AppTec360 Enterprise Mobile Manager & ContentBox

Посібник з адміністрування | Версія 5.0 (202110)

Зміст

Конфігурація iOS

Генерал

- Огляд профілю групи (тільки на рівні групи)
- Загальна інформація
- Налаштування
- Ревізія конфігурації
- Журнал пристрою (тільки на рівні пристрою)
  - Командний журнал
  - Можливі стани команди

Управління активами (тільки на рівні пристрою)

- Управління активами (тільки на рівні пристрою)
  - Інформація про пристрій
  - Wi-Fi
  - Стільниковий зв’язок
  - Bluetooth

Управління безпекою

- Захист від крадіжок (лише на рівні пристрою)
  - Інформація про GPS (лише на рівні пристрою)
  - Wipe & Lock (тільки на рівні пристрою)
  - Повідомлення (тільки на рівні пристрою)
- Конфігурація безпеки
  - Пароль
  - Сертифікат (тільки на рівні пристрою)
  - Шифрування
  - Єдиний вхід
- Кінець життя (тільки на рівні пристрою)
  - Витирання (тільки на рівні пристрою)
- Налаштування обмежень
  - Функціональність пристрою
  - iCloud
  - Безпека та конфіденційність

BYOD

- Вбудований захист iOS (контейнер)
  - Активація

- Пароль SecurePIM
- Безпека SecurePIM
- Браузер SecurePIM
- Обмін

Керування з’єднаннями

- Wi-Fi
  - Налаштування проксі-сервера
  - Тип безпеки
- VPN
  - Тип VPN
    - VPN
    - Per-App VPN
  - Налаштування проксі-сервера
- APN
- Стільниковий зв’язок
- HTTP-проксі-сервер
- AirPrint
- AirPlay

Менеджмент ПІМ

- Активна синхронізація Exchange Active Sync
- Електронна пошта
  - Вхідна пошта
  - Вихідна пошта
- CalDav
- Календарі за передплатою
- LDAP

Керування сайтом

- Веб-кліпи
- Фільтр веб-вмісту

Керування додатками

- Enterprise App Manager
  - Встановлені програми (лише на рівні пристрою)
  - Обов’язкові програми
    - Параметри встановлення

- Веб-додатки
- Обмеження та налаштування
  - Додатки з чорного списку / білого списку
  - Обмеження SysApp
  - App-VPN
  - Налаштування програми
- Enterprise App Store
  - Програми iTunes
  - Власні сили
- Режим кіоску
  - Тип програми
    - Пакет
    - URL
  - Налаштування режиму кіоску

Android Enterprise – повністю керована конфігурація пристрою

Генерал

- Огляд профілю групи (тільки на рівні групи)
- Огляд пристрою (тільки на рівні пристрою)
- Ревізія конфігурації (лише на рівні пристрою)
- Журнал пристрою (тільки на рівні пристрою)
  - Командний журнал
  - Можливі стани команди
- Налаштування пристрою
  - Конфігурація клієнта
  - Шпалери

Управління активами (тільки на рівні пристрою)

- Інформація про пристрій
  - Wi-Fi
- Стільниковий зв’язок
- Bluetooth

Управління безпекою

- Захист від крадіжок (лише на рівні пристрою)
  - Інформація про GPS (лише на рівні пристрою)

- Wipe & Lock (тільки на рівні пристрою)
- Повідомлення (тільки на рівні пристрою)
- Конфігурація безпеки
  - Код доступу до пристрою
  - Антивірус
- Кінець життя (тільки на рівні пристрою)
  - Витирання (тільки на рівні пристрою)
- Налаштування обмежень
  - Обмеження
- Управління сертифікатами

Керування з’єднаннями

- Wi-Fi
  - Тип безпеки
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Тип VPN
    - VPN
    - Per-App VPN
- Обмеження

Менеджмент ПІМ

- Обмін Gmail

Керування додатками

- Enterprise App Manager
  - Встановлені програми (лише на рівні пристрою)
  - Системні програми (лише на рівні пристрою)
  - Обов’язкові програми
  - Чорні та білі списки
  - Додатки для системи AE
- Обмеження та налаштування
  - Налаштування керування програмами
- Enterprise App Store
  - Власні сили
- Enterprise Play Store

- Налаштування пристрою
  - Конфігурація клієнта
  - Шпалери
- Управління активами (тільки на рівні пристрою)
- Інформація про пристрій
  - Wi-Fi
- Стільниковий зв’язок
- Bluetooth
- Управління безпекою
- Захист від крадіжок (лише на рівні пристрою)
  - Інформація про GPS (лише на рівні пристрою)
  - Wipe & Lock (тільки на рівні пристрою)
  - Повідомлення (тільки на рівні пристрою)
- Конфігурація безпеки
  - Код доступу до пристрою
  - Код доступу до контейнера
  - Антивірус
- Кінець життя (тільки на рівні пристрою)
  - Витирання (тільки на рівні пристрою)
- Налаштування обмежень
  - Обмеження
- Управління сертифікатами
- Керування з’єднаннями
- Wi-Fi
  - Тип безпеки
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Тип VPN
    - VPN
    - Per-App VPN
- Обмеження
- Менеджмент ПІМ
- Обмін Gmail

- Інформація про GPS (лише на рівні пристрою)
- Wipe & Lock (тільки на рівні пристрою)
- Повідомлення (тільки на рівні пристрою)
- Конфігурація безпеки
  - Пароль
  - Шифрування
  - Антивірус
- Кінець життя (тільки на рівні пристрою)
  - Витирання (тільки на рівні пристрою)
- Налаштування обмежень
  - Обмеження
  - Власник пристрою AE

Контейнер BYOD

- Android Enterprise
  - Android Enterprise
  - Обмін Gmail
  - Додатки для системи AE
  - Код доступу до контейнера
- Samsung KNOX
  - Активація
  - Пароль Нокса
  - Нокс Секьюріті
  - Knox Exchange
  - Knox eMail
  - Knox Apps

Керування з’єднаннями

- Wi-Fi
  - Тип безпеки
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Обмеження
- APN
- Bluetooth

- Менеджмент ПІМ
  - Обмін
  - Електронна пошта
  - AE Gmail Exchange
- Керування додатками
  - Enterprise App Manager
    - Встановлені програми (лише на рівні пристрою)
    - Системні програми (лише на рівні пристрою)
    - Обов’язкові програми
    - Додатки для системи AE
  - Обмеження та налаштування
    - Чорні та білі списки
    - Обмеження системних додатків
      - Програми Samsung
      - Програми Huawei
    - Налаштування керування програмами
  - Enterprise App Store
    - Playstore
    - Власні сили
  - Enterprise Play Store
  - Режим кіоску та лаунчер
    - Режим кіоску
    - AppTec360 Launcher
    - Налаштування AppTec360
- Пульт дистанційного керування
  - Splashtop
  - Teamviewer
- Управління контентом
  - Вміст
  - Безпечний браузер

Конфігурація ПК з Windows 10

- Генерал
  - Огляд профілю групи (тільки на рівні групи)
  - Огляд пристрою (тільки на рівні пристрою)

- Налаштування
- Ревізія конфігурації (лише на рівні пристрою)
- Журнал пристрою (тільки на рівні пристрою)
  - Командний журнал
  - Можливі стани команди
- Управління активами (тільки на рівні пристрою)
  - Інформація про пристрій
  - Стільниковий зв’язок
  - Інформація про синхронізацію
- Управління безпекою
  - Захист від крадіжок (лише на рівні пристрою)
    - Інформація про GPS (лише на рівні пристрою)
    - Налаштування GPS
  - Конфігурація безпеки
    - Пароль
    - Антивірус
    - Центр безпеки
    - Налаштування брандмауера
    - Правила брандмауера
  - Налаштування обмежень
    - Функціональність пристрою
  - BitLocker
    - Конфігурація BitLocker
    - Стан BitLocker
  - Управління сертифікатами
    - Список сертифікатів
    - Конфігурація сертифіката
    - SCEP
- Керування з’єднаннями
  - Wi-Fi
    - Тип безпеки
    - Використання проксі-сервера
  - Обмеження Wifi
  - VPN
    - Тип підключення
    - Типові конфігурації VPN
  - Обмеження VPN

- Bluetooth
- Менеджмент ПІМ
  - Активна синхронізація Exchange Active Sync
  - Електронна пошта
- Керування додатками
  - Enterprise App Manager
    - Встановлені програми
    - Обов’язкові програми
    - Обмеження системних додатків
    - Чорні та білі списки

Конфігурація MacOS

Генерал

- Огляд профілю групи (тільки на рівні групи)
- Огляд пристрою (тільки на рівні пристрою)
- Ревізія конфігурації (лише на рівні пристрою)
- Журнал пристрою (тільки на рівні пристрою)
  - Командний журнал
  - Можливі стани команди

Управління активами (тільки на рівні пристрою)

- Інформація про пристрій
- WiFi
- Стільниковий зв’язок
- Bluetooth

Керування оновленнями (лише на рівні пристрою)

- Інформація про оновлення

Управління безпекою

- Захист від крадіжок
  - Wipe & Lock
- Конфігурація безпеки
  - Пароль
  - Сертифікат
- Налаштування обмежень
  - Функціональність пристрою
  - iCloud

Загальний огляд

Вступ до AppTec360

Рішення для управління мобільними пристроями від AppTec пропонує можливість керувати та налаштовувати всіма мобільними пристроями за допомогою інтуїтивно зрозумілої консолі управління. У цьому сценарії сервер EMM може працювати у вашому власному середовищі або ви можете використовувати наше хмарне рішення.

Навіть у питанні централізованого встановлення корпоративних додатків на смартфони ви потрапили в потрібне місце. За допомогою Enterprise Mobile Manager ви можете розповсюджувати корпоративні програми та документи на пристрої за лічені секунди або блокувати небажані програми за допомогою білих/чорних списків.

Використання приватних пристроїв у компаніях створює нові виклики для захисту смартфонів та планшетів. У зв'язку з тим, що співробітники хочуть використовувати свої смартфони все більше і більше, IT-адміністратори повинні захищати велику кількість різних типів пристроїв. Ми допоможемо вам захистити всі пристрої та конфіденційні дані, що зберігаються на них, і керувати ними за допомогою інтуїтивно зрозумілої консолі.

Підтримувані операційні системи пристроїв

AppTec360 пропонує підтримку пристроїв на iOS, Android та Windows. Зверніть увагу, що функціональні можливості згаданих платформ можуть відрізнятися в різних ОС.

- Apple iOS 11.0 або новішої версії*.
- Apple macOS 10.11 або новішої версії
- Google Android 4.4 або новішої версії** у хмарній версії
- Google Android 4.1 або новішої версії** у версії OnPrem
- MS Windows 10 або новішої версії*** (настільний комп'ютер, ноутбук та планшет)

**Зверніть увагу, що пристрої з iOS 10 або більш ранніми версіями не можуть бути зареєстровані через радикальні зміни, внесені компанією Apple у процес реєстрації.*

***Пристрої можна підключати та налаштовувати, навіть якщо вони використовують версію, яка більше не підтримується виробником. Зверніть увагу, що деякі функції можуть потребувати певної версії Android. У випадках підтримки ми користуємося офіційною підтримкою виробника. У разі виникнення проблем або помилок, спричинених застарілою версією, яка більше не підтримується виробником, ми залишаємо за собою право надавати лише обмежену підтримку.*

****Домашні версії Windows не підтримуються через обмеження операційної системи. Ми наполегливо рекомендуємо використовувати версію ОС, яка все ще підтримується виробником. Не тільки для сумісності, але й з міркувань безпеки. Тому ми рекомендуємо iOS 12 або новішої версії та Android 9 або новішої версії.*

Підтримувані каталоги LDAP

- Microsoft Active Directory
- Відкрити LDAP

Актуальну інформацію про "Підтримувані операційні системи пристроїв" та "Підтримувані каталоги LDAP" можна знайти тут:

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

Пояснення “Режиму під наглядом” на пристроях Apple

Режим під наглядом являє собою розширений інтерфейс для пристроїв iOS.

На відповідно сконфігурованому пристрої можуть бути застосовані додаткові обмеження, що стосуються функціональності пристрою кінцевого користувача. Вони також містяться в посібнику з адміністрування і позначені відповідним банером.

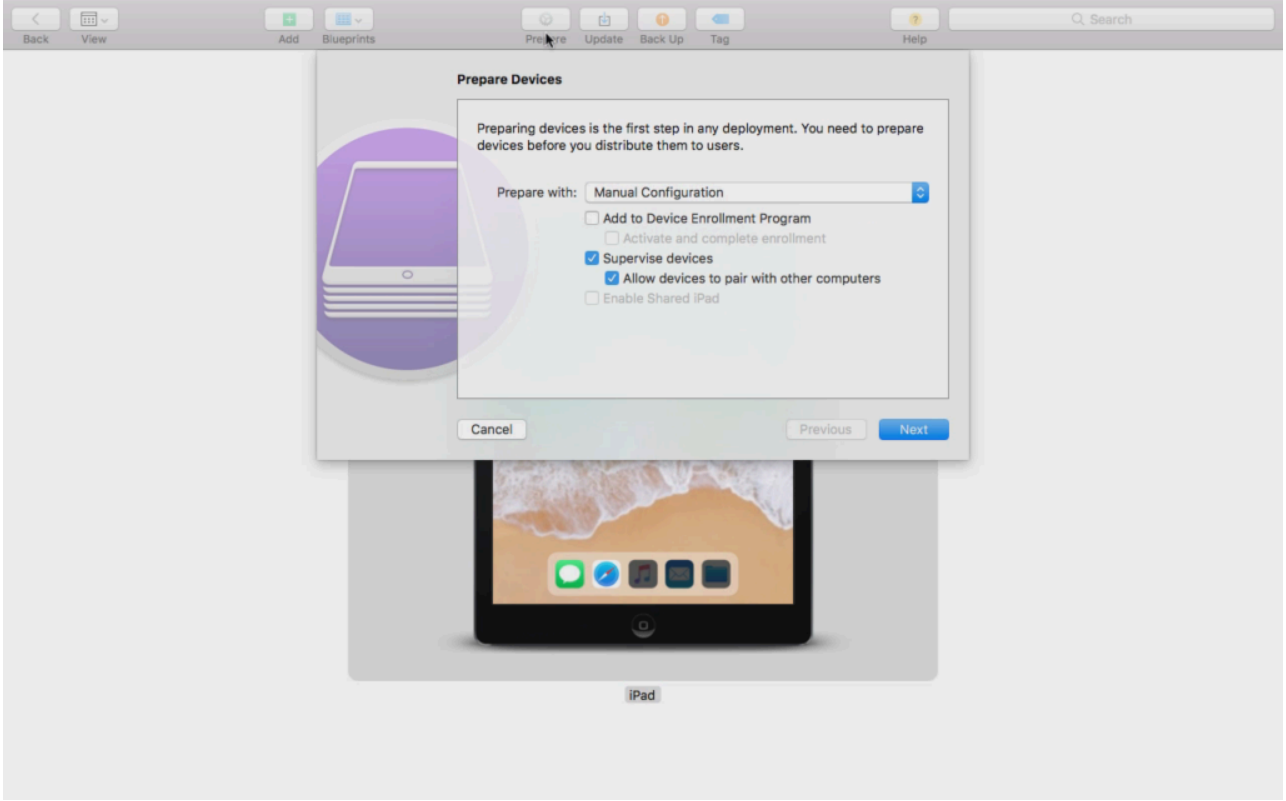
Доступно в режимі під наглядом

"Режим під наглядом" можна активувати за допомогою програми "Apple Configurator". Apple Configurator може встановлювати налаштування за замовчуванням на нових пристроях iOS як інструмент конфігурації (через інтерфейс USB).

Інструмент може встановлювати не лише конфігураційні профілі, але й програми. Це безкоштовно, але для цього потрібен комп'ютер Mac.

Увімкніть контрольований режим

1. Відкрийте Apple Configurator



2. Натисніть на пристрій і виберіть "Підготувати"
3. Виберіть "Конфігурація вручну" та "Наглядати за пристроями"
4. Натисніть "Далі"
5. (Необов'язково) Тепер ви можете додати сервер MDM, на якому буде зареєстровано пристрій. Посилання для цього можна знайти в "Загальні налаштування - Конфігурація iOS - Конфігуратор та URL-адреса" Виберіть свою організацію або створіть нову
6. Виберіть свою організацію або створіть нову
7. Виберіть, які кроки слід пропустити під час початкового налаштування, і натисніть "Далі" (УВАГА: Продовження призведе до видалення вашого пристрою!).

Тепер ваш пристрій буде переведено в режим нагляду. Це може зайняти кілька хвилин. Після цього пристрій перезавантажиться.

Тепер ваш пристрій під наглядом!

Додавання пристрою до DEP

Ви також можете додати пристрої до DEP (Програма реєстрації пристроїв) за допомогою Apple Configurator, якщо ваші пристрої працюють на iOS 11 або новішої версії.

Більше інформації про DEP: https://www.apple.com/business/dep/

Виконайте ті самі кроки, що й для нагляду за пристроєм, і додатково встановіть прапорець "Додати до програми реєстрації пристроїв". Вам буде запропоновано ввести дані для входу в DEP, якщо ви ніколи раніше не входили в DEP за допомогою Apple Configurator.

Після завершення процесу пристрій можна знайти на сервері DEP у розділі "Пристрої, додані Apple Configurator 2". Тепер ви можете використовувати цей сервер і підключити його до консолі керування або перенести пристрій на вже існуючий сервер.

Ви успішно додали пристрій до DEP!

Пояснення Android Enterprise

Що таке Android Enterprise?

Android Enterprise пропонує кращий контроль над робочими пристроями, які управляються за допомогою MDM. Це дозволяє адміністраторам мати повний контроль над своїми Android-пристроями або відокремлювати дані компанії від приватних даних на контейнерних пристроях. Крім того, Android Enterprise дозволяє легше реєструвати пристрої та розповсюджувати додатки.

Які вимоги для використання Android Enterprise?

Android Enterprise може безкоштовно використовуватись усіма бажаючими. Вам потрібно лише підключити обліковий запис Google до MDM, щоб увімкнути всі функції Android Enterprise. Більше про це можна дізнатися в розділі Android Enterprise.

Android Enterprise можна використовувати на пристроях з Android 5.1 або новішої версії, за винятком розширеного робочого профілю (див. нижче). Ми рекомендуємо використовувати принаймні Android 7 або новішу версію для спрощення реєстрації або Android 11, щоб скористатися всіма доступними функціями.

Які режими доступні в Android Enterprise?

Існує 3 різних режими, які можна використовувати при роботі з Android Enterprise.

AE Повністю керований пристрій (Work Managed): Повністю керований пристрій, який використовується лише для роботи. Це дозволяє адміністратору повністю контролювати пристрій. Це не дозволяє приватне використання пристрою. Щоб зареєструвати пристрої в цьому режимі, їх потрібно скинути і зареєструвати за допомогою QR-коду (див. Реєстрація AE) або зареєструвати за допомогою Knox Enrollment чи Zero Touch.

AE BYOD Container: Контейнер BYOD (принеси свій власний пристрій) дозволяє користувачам отримувати доступ до даних компанії на своєму особистому телефоні в окремому контейнері. У цьому режимі приватні програми не можуть бачити дані та програми компанії і навпаки. Щоб зареєструвати пристрої в цьому режимі, потрібно завантажити додаток AppTec і відсканувати QR-код. Створіть пристрій в консолі і виберіть "AE Container (BYOD & Enahnced Work Profile)" як тип пристрою. Натисніть на QR-код на щойно створеному пристрої, щоб отримати QR-код, і встановіть перший перемикач на "Legacy & BYOD".

AE Enhanced Work Profile: (вимагає Android 11 або новішої версії) У той час як вищезгаданий BYOD Container приносить дані компанії на приватний пристрій, Enhanced Work Profile робить те ж саме, але для пристрою, що належить компанії. Він створює той самий контейнер, але дає адміністратору трохи більше контролю над пристроєм, тому користувач не може просто

видалити MDM з пристрою. Створіть пристрій в консолі і виберіть "AE Container (BYOD & Enahnced Work Profile)" як тип пристрою. Натисніть на QR-код на щойно створеному пристрої, щоб отримати QR-код, і встановіть перший перемикач на "Розширений робочий профіль". Цей QR-код можна відсканувати після перезавантаження пристрою та 6 разів постукавши по екрану, як описано в Методі 1 в розділі Реєстрація AE.

Як призначити програми на пристрої Android Enterprise?

Спочатку ви маєте затвердити додатки, які хочете використовувати, у Загальних налаштуваннях → Керування додатками → AE Play Store → Додатки Play Store. Після схвалення програми ви можете додати її до списку обов'язкових програм → вашого профілю, натиснувши на "+" і вибравши програму на вкладці "AE Play Store". Це призведе до автоматичного завантаження та встановлення програми. Для цього не потрібен обліковий запис Google на пристрої, і користувачеві не потрібно підтверджувати або дозволяти це.

Завантажуйте власні програми в Google Play Store

Ви можете завантажити свої внутрішні додатки в Google Play Store. Таким чином ви можете скористатися різними перевагами, наприклад, механізмом оновлення Play Store.

Для цього вам потрібен обліковий запис розробника Google. Увійдіть за допомогою консолі Google Play(https://play.google.com/apps/publish)

Натисніть "Створити додаток". Виберіть мову за замовчуванням і назву програми.

Create application

Default language *

English (United Kingdom) – en-GB ▾

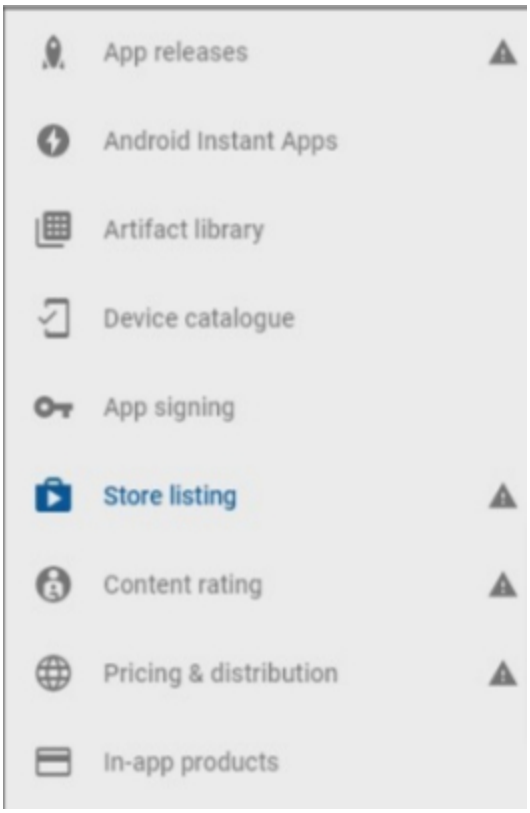
Title *

AppTec Demo App

15/50

CANCEL CREATE

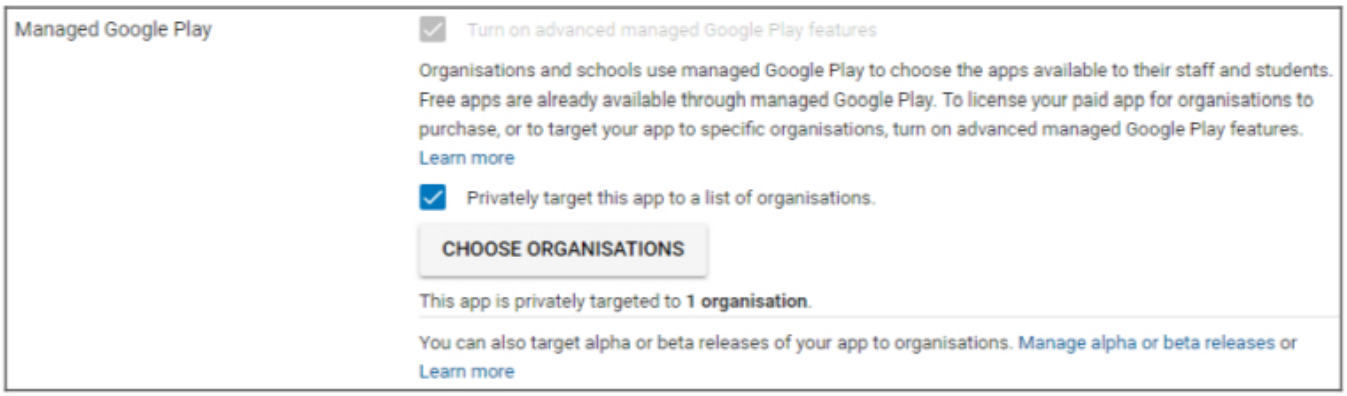
На наступній сторінці вам буде запропоновано ввести різні дані про ваш додаток.



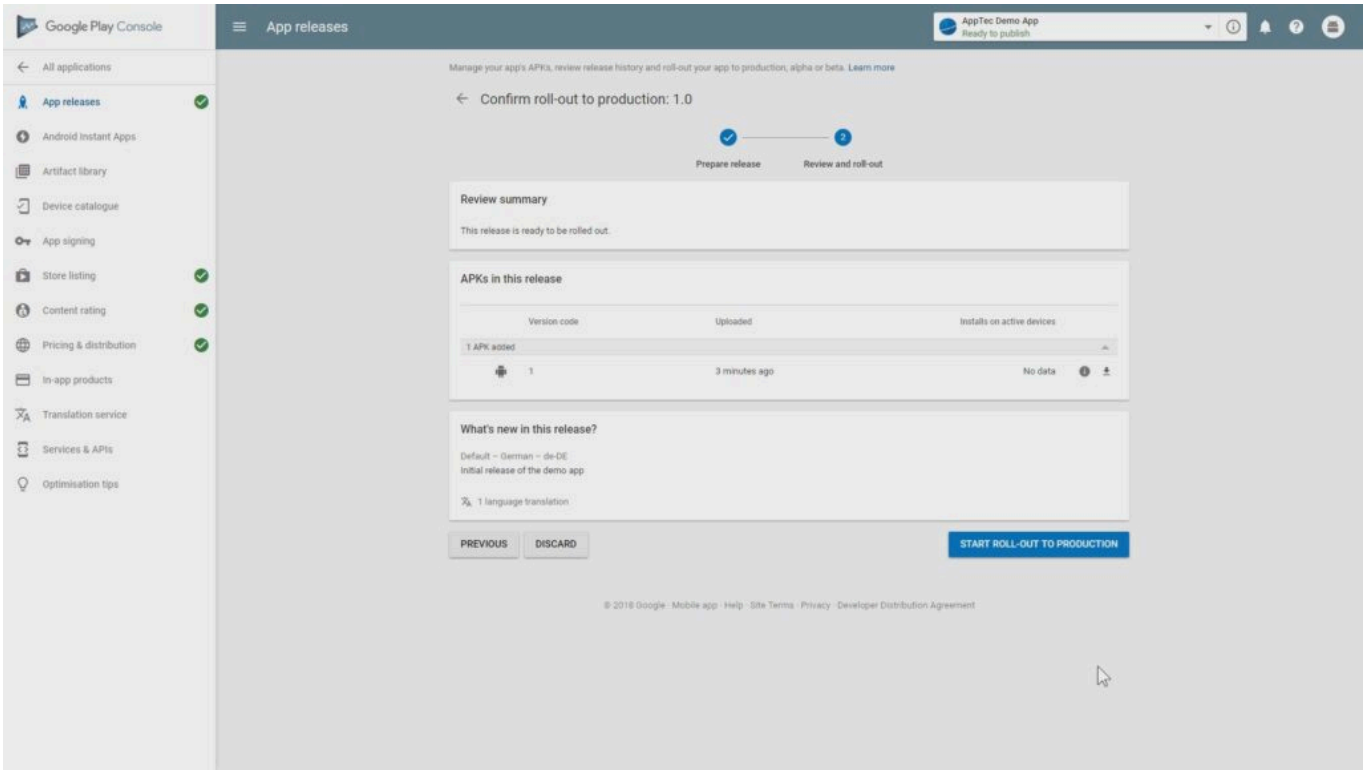
Після того, як ви ввели всі дані, зліва ви побачите різні символи-підказки.

Наведіть на них курсор, щоб побачити, які кроки залишилися, і виконайте їх у будь-якому порядку.

Примітка: Переконайтеся, що ви встановили дві галочки в "Керованому Google Play" в розділі "Ціноутворення та розповсюдження". В іншому випадку додаток буде загальнодоступним і його зможуть завантажити всі бажаючі. Також не забудьте вибрати країну для розповсюдження.



Після того, як ви виконали всі кроки, ви можете перейти до розділу "Випуски додатків". Натисніть на "Review" і "Start Roll-Out to Production", щоб завершити роботу над проєктом і опублікувати додаток.



Це може зайняти деякий час, перш ніж додаток стане доступним у Play Store. Після завершення процесу ви можете знайти свою програму в магазині Play for Work і затвердити її. Після цього ви можете просто призначити додаток на пристрої за допомогою консолі EMM так само, як ви робите це з іншими додатками.

Вимоги та встановлення

Вимоги

Системні вимоги

Віртуальний пристрій доступний у форматі відкритої віртуалізації (VMWare, VirtualBox, Citrix Xen Server) та у вигляді стисненого файлу .vhdx (Hyper-V)*.

*Примітка: У разі використання Hyper-V машина має бути створена з версією 1-го покоління.

Віртуальний диск має цільовий розмір 20 ГБ, а машина потребує 4 ГБ оперативної пам'яті.

Пристрій працює на базі Debian 9 64bit

Оновіть імпортовану машину до найновішої версії сумісності (наприклад, у VMWare) і переконайтеся, що у вашому гіпервізорі правильно встановлено тип ОС машини.

Ліцензійний ключ

Для успішної активації та встановлення сервера вам знадобиться дійсний файл ліцензії. Ви можете отримати його безпосередньо у AppTec360 та/або у вашого відповідного реселлера.

Розширення IP-адреси та DNS

Пристрій AppTec360 повинен бути доступний за допомогою хост-імені, на яке видано ліцензію.

Щоб зареєструвати пристрої з Windows 10, вам також потрібно налаштувати додатковий субдомен у вигляді "enterpriseenrollment.", що вказує на пристрій.

SSL-сертифікат

Оскільки всі з'єднання з пристроями повинні бути захищені за допомогою SSL, вам потрібен дійсний сертифікат для імені хоста, виданий центром сертифікації, якому довіряє пристрій. Закритий ключ для сертифіката повинен бути завантажений без захисту паролем. У більшості випадків потрібен проміжний сертифікат для центру сертифікації, щоб пристрої могли розпізнати сертифікат сервера.

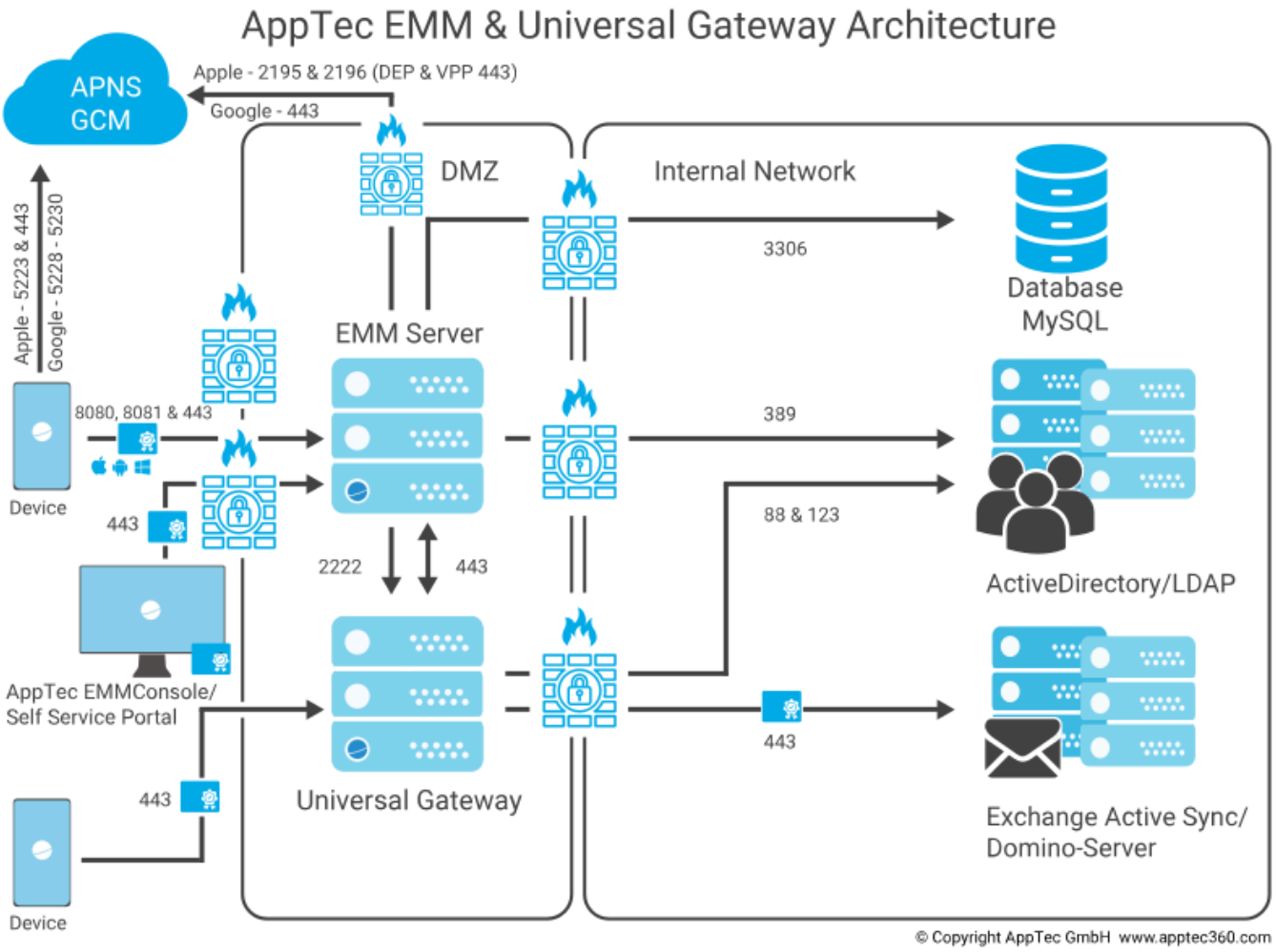
Пристроям з Windows 10 знадобиться спеціальний сертифікат для вашого субдомену корпоративної реєстрації.

Починаючи з версії пристрою 202104, ви також можете використовувати сертифікати Let's Encrypt, які генеруються автоматично (описано в розділі Крок другий - Сертифікат SSL).

Сервер SMTP

Для того, щоб AppTec360 EMM міг надсилати електронні листи (наприклад, для реєстрації пристрою та підтвердження облікового запису), потрібен сервер електронної пошти та/або ретранслятор електронної пошти.

Правила брандмауера



На цій схемі показано, яке з'єднання потрібне залежно від того, якими послугами ви хочете користуватися.

Більш детальний опис див. у таблиці на наступній сторінці.

Будь-який (зовнішній/ пристрої)	→	**Прилад AppTec360 / emmconsole.com**
Порти	443	Управління, корпоративний AppStore та комунікація з Windows Phone
	8080	Зв'язок з Android та iOS
	80	Перше налаштування Let's Encrypt. Надалі використовує 443.
Будь-який (Пристрої)	→	**Будь-який (зовнішній)**
Порти	5223, 443	Apple Push Service, має бути доступний без проксі, 443 як резервний варіант, див. https://support.apple.com/en-us/HT203609.
	5228-5230	Android Push Service (FCM), повинен бути доступний без проксі
Прилад AppTec360	→	**Контролер домену**
Порти	389, (LDAPS 636)	Синхронізація користувачів з LDAP
Прилад AppTec360	→	**Будь-який**
Порт	443	Використовується для Android Push Service (GCM) Пошук в AppStore / Play Store
Прилад AppTec360	→	**emmconsole.com**
Порти	443	Оновлення пристроїв AppTec360, генерація сертифікатів APNS
Прилад AppTec360	→	**Мережа Apple (17.0.0.0.0/8)**
Порти	2195, 2196	Apple Push Service та служба зворотного зв'язку
	443	DEP TA VPP

Оновлення безпеки

Операційну систему Debian слід регулярно оновлювати, щоб отримати найновіші виправлення безпеки. Однак переконайтеся, що ви не оновлюєтесь до новішої основної версії Debian вручну. Коли AppTec360 EMM буде сумісний з новішою версією, ми додамо спосіб оновлення в оновлення пристрою.

Паролі віртуального пристрою за замовчуванням

Логін Користувач (Root-логін вимкнено. Використовуйте "sudo" для завдань адміністрування)

apptec

Логін Пароль

apptec

Root-користувач MySQL

корінь

Root-пароль MySQL

apptec

Користувач MySQL за замовчуванням

AppTec

Пароль користувача MySQL за замовчуванням

AppTec

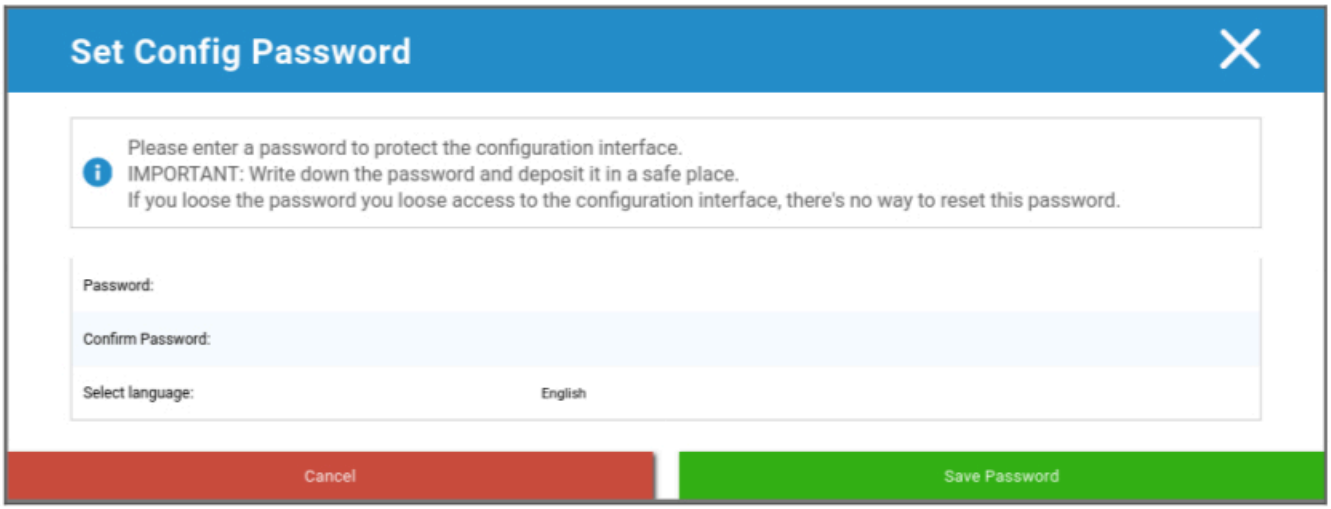
Конфігурація віртуального приладу

Важливо: Перед початком налаштування віртуального приладу слід встановити роздільну здатність дисплея щонайменше 1280 x 800 пікселів.

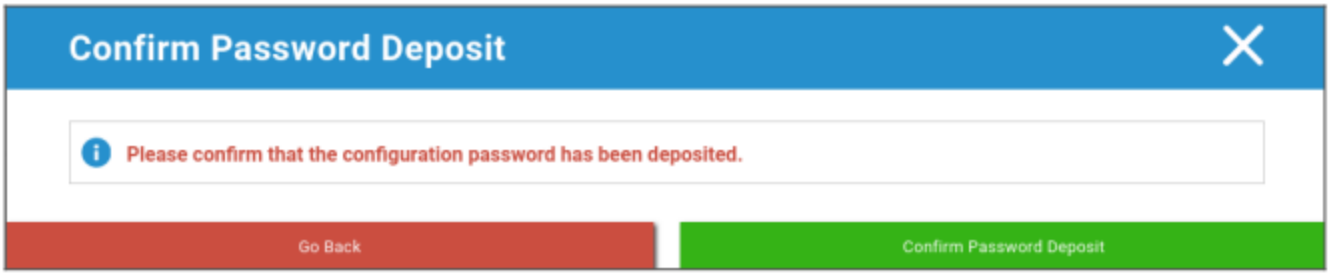
Після входу до Пристрою Firefox повинен автоматично запуститися і відобразити інтерфейс конфігурації.

Підготовка

Спочатку вам потрібно вказати пароль для інтерфейсу конфігурації. Цей пароль використовується для шифрування всієї інформації та файлів, що вводяться в інтерфейсі конфігурації. Тут ви також можете встановити мову, якою буде відображатися інтерфейс (її можна змінити пізніше).

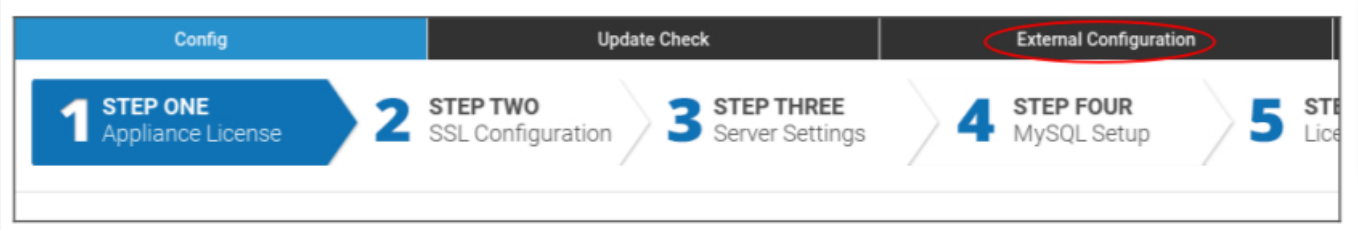


Пароль може бути скинутий тільки службою підтримки AppTec360, тому переконайтеся, що ви зберегли його в безпечному місці і підтвердіть спливаюче вікно.



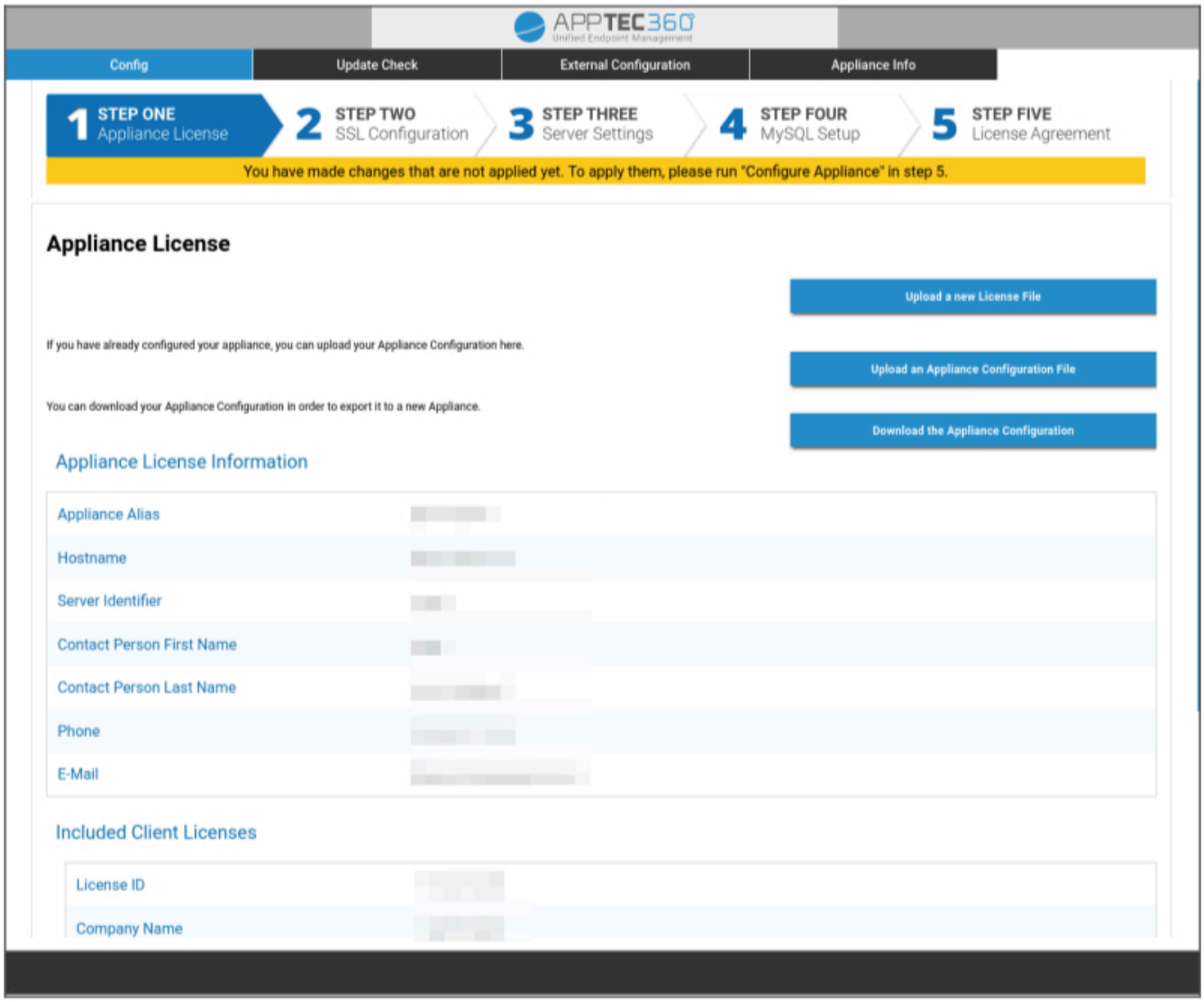
Налаштування із зовнішнього хосту

Щоб полегшити процес налаштування, ви можете зробити сторінку конфігурації доступною віддалено. Для цього виконайте кроки з розділу "Налаштування із зовнішнього хосту".



Крок перший – Ліцензія на використання приладу

1. Будь ласка, завантажте файл ліцензії, який ви отримали від AppTec.
2. Якщо файл ліцензії було успішно завантажено, ви побачите інформацію про ліцензію на пристрій, як на скріншоті нижче.



Крок другий – SSL-сертифікат

Ви можете скористатися автоматичним встановленням сертифікатів за допомогою Let's Encrypt або надати сертифікати самостійно (див. розділ SSL-сертифікат для отримання додаткової інформації).

Автоматично

Сертифікат буде автоматично згенеровано за допомогою сервісу Let's Encrypt.

AppTec360 EMM використовує HTTP-01 виклик для перевірки домену, що означає, що HTTP-порт повинен бути відкритий з Інтернету для першого запиту сертифікату. Наступні запити на поновлення можуть бути підтверджені через HTTPS.

Перемкніть перемикачі на "Автоматично (Шифрувати)" і натисніть "Зберегти значення". Сертифікат буде автоматично запитано під час застосування конфігурації на п'ятому кроці - Ліцензійна угода. Сертифікат буде автоматично поновлюватися при необхідності, і ви отримаєте електронного листа, якщо термін дії сертифіката закінчується (що означає, що поновлення могло бути невдалим).

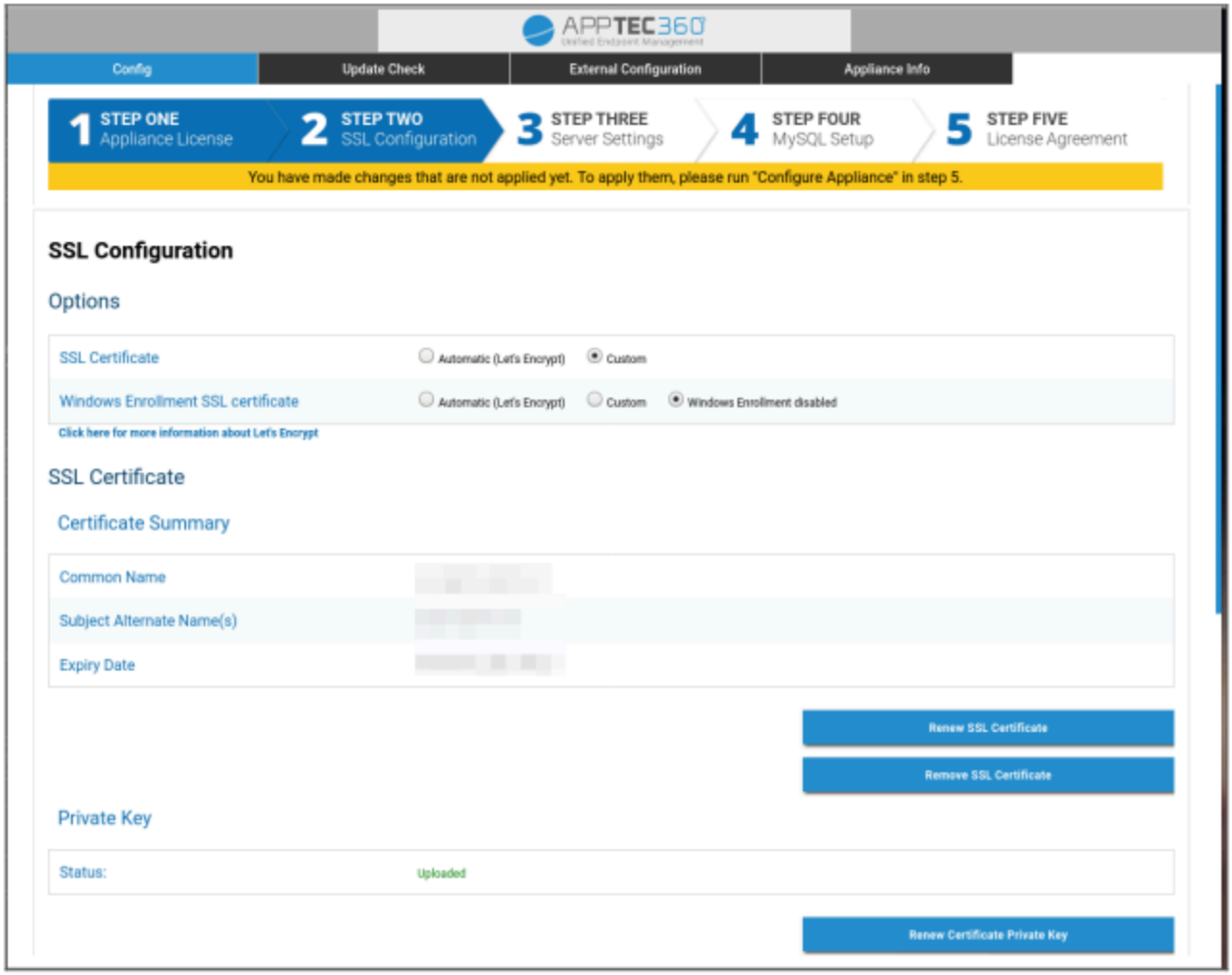
Нестандартний

1. Завантажте SSL-сертифікат для вашого ліцензованого імені хоста. Ви можете побачити ім'я хоста в Крок перший - Ліцензія на пристрій.

2. Також завантажте закритий ключ для сертифіката і, за необхідності, проміжний сертифікат.

Важливо: Ключ не повинен бути захищений паролем. Якщо це так, будь ласка, зніміть пароль перед завантаженням.

Підказка: Якщо ви також хочете використовувати пристрої з Windows 10, вам потрібно увімкнути "SSL-сертифікат реєстрації Windows" і завантажити сертифікат, приватний ключ і проміжний сертифікат для вашого субдомену (як описано в розділі "IP-адреса та DNS-дозвіл"), завантаживши їх у нижній частині сторінки.



Крок третій – Налаштування сервера

1. Будь ласка, введіть глобальну адресу електронної пошти служби підтримки. Ця адреса буде використовуватися в електронних листах вашим користувачам, щоб вони знали, до кого звертатися в разі виникнення будь-яких проблем з їхнім пристроєм.

2. Надайте налаштування електронної пошти, які будуть використовуватися системою для надсилання електронних листів. Налаштування будуть використовуватися для надсилання електронних листів користувачеві, а також для надсилання повідомлень про помилки та запитів на розробку на адресу"support@apptec360.com".Після збереження налаштувань електронної пошти вам необхідно перевірити їх, натиснувши на "Test E-Mail Configuration" і дотримуючись інструкцій.

Крок четвертий – Налаштування MySQL

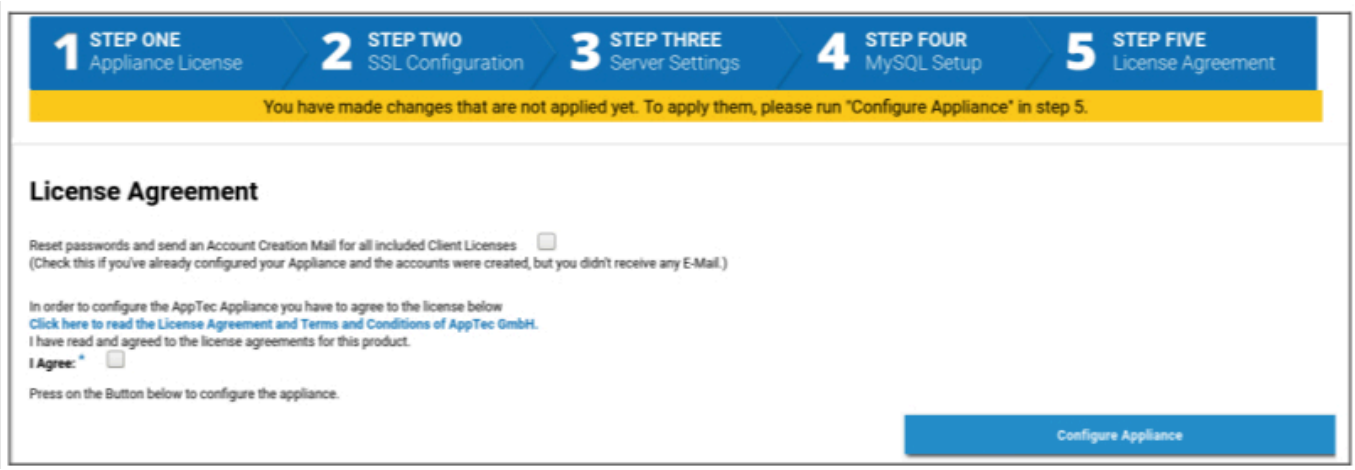
1. Якщо ви хочете використовувати внутрішню базу даних, ви можете пропустити цей крок. В іншому випадку ви можете ввести інформацію про підключення до зовнішнього сервера бази даних.


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)

Крок п’ятий – Ліцензійна угода

1. Будь ласка, прочитайте ліцензійну угоду.
2. Поставте галочку "Я згоден" і натисніть кнопку "Налаштувати пристрій", щоб застосувати налаштування.

Підказка: Вам потрібно буде запускати "Configure Appliance" щоразу, коли ви змінюєте налаштування в 5 кроках, щоб застосувати налаштування.



Вітаю!

Ви завершили налаштування віртуального пристрою.

Електронний лист із паролем було надіслано на адресу, яку ви вказали для отримання ліцензії (її видно в розділі "Включені клієнтські ліцензії" на першому кроці - Ліцензія на програмне забезпечення).

Тепер ви можете увійти в консоль, використовуючи цей пароль та адресу електронної пошти, на яку ви його отримали.

Для входу в консоль, будь ласка, введіть ім'я хоста консолі в адресний рядок вашого браузера.

Ви можете знайти ім'я хоста вашого пристрою в Крок перший - Ліцензія на пристрій.

Усунення несправностей

1. Ви не отримали електронного листа під час налаштування приладу на п'ятому кроці - Ліцензійна угода:

Переконайтеся, що ваші налаштування електронної пошти в Крок третій - Налаштування сервера - правильні. Щоб повторно надіслати пароль, поставте галочку біля пункту "Скинути паролі та надіслати повідомлення про створення облікового запису для всіх включених клієнтських ліцензій" у Крок п'ятий - Ліцензійна угода, перш ніж знову запускати "Налаштувати пристрій".

2. Ви отримали помилку щодо Let's Encrypt під час налаштування на п'ятому кроці - Ліцензійна угода:

Переконайтеся, що пристрій доступний за доменним ім'ям через порт 80. Давайте зашифруємо також запишемо лог до "/var/log/letsencrypt", що може допомогти у подальшому пошуку та усуненні несправностей.

Рекомендації з безпеки

Рекомендується виконати наступні кроки для захисту вашого пристрою AppTec360.

Це не повний набір інструкцій, а лише рекомендація для базової конфігурації.

- Зміна пароля для користувача AppTec360
- Змініть пароль для користувачів MySQL "root" і "AppTec" та оновіть Крок четвертий - Налаштування MySQL відповідно
- Зміна порту SSH-сервера за замовчуванням
- Заблокуйте порт 80 у вашій консолі і забороніть вхідний HTTP-трафік, використовуйте тільки HTTPS. Після налаштування можливе також зовнішнє конфігурування через HTTPS.
- Обмежте доступ до інтерфейсу керування лише певними IP-адресами внизу Крок третій - Налаштування сервера
- Налаштування брандмауера

Загальні налаштування

Огляд рахунку

Інформація про обліковий запис

Огляд

Тут ви можете побачити огляд вашого облікового запису AppTec360.

Назва компанії	Назва вашої компанії
Дата створення	Дата створення облікового запису
Тип ліцензії	Платна = платна ліцензія Безкоштовна = безоплатна ліцензія Примітка: Рахунки на локальному пристрої завжди відображатимуться як оплачені з технічних причин
Ідентифікатор клієнта	Ідентифікатор вашого облікового запису (це НЕ ваш номер клієнта)
Дата закінчення терміну дії ліцензії	Дата закінчення терміну дії вашої ліцензії AppTec360
Ліцензія ContentBox	Безкоштовно = безкоштовна ліцензія на 25 пристроїв Платна = платна ліцензія для x пристроїв
Launcher	Показує, чи можна використовувати кастомний лаунчер для Android
Пристрої	Кількість ліцензій, що використовуються в даний час / загальна кількість ліцензій
Контактна особа	Вказана контактна особа
Телефон	Наданий номер телефону
Електронна пошта*	Надана адреса електронної пошти
Root-користувач	Root-користувачі, які можуть увійти в систему
Версія програмного забезпечення	Поточна версія програмного забезпечення

**Примітка: Тут показано адресу електронної пошти, яку ви ввели під час реєстрації облікового запису. На основі цієї адреси буде створено користувача в дереві користувачів/ пристроїв, якого можна буде змінювати. Редагування цього користувача змінить адресу*

електронної пошти, яку ви маєте використовувати для входу, але не інформацію в огляді облікового запису .

Звіт про помилку

Звіт про помилку можна надіслати безпосередньо до служби підтримки, щоб повідомити про проблеми або помилки, і він містить інформацію та журнали про ваш обліковий запис і налаштування.

Тема	Тема повідомлення про ваду. Додайте номер тікета, якщо ви хочете додати його до існуючого тікета підтримки.
Очікувана поведінка	Детально опишіть, що ви робили і чого очікували
Фактична поведінка	Детально опишіть, що саме відбувається. Будь ласка, цитуйте повідомлення про помилки ТОЧНО. Також допоможе, якщо ви додасте скріншоти до вкладення.
Коли ви зіткнулися з цією проблемою?	Будь ласка, вкажіть точний час, коли ви отримали конкретне повідомлення про помилку/проблему. У кращому випадку додайте секунди, наприклад, 18:55:27
Чи можна повторити цю проблему? Якщо так, то як (детально)?	Детально опишіть, як ви можете відтворити проблему.
Чи працювала ця функція раніше так, як ви очікували? Якщо так, то до якого часу?	Залиште порожнім, якщо не знаєте.
Чи були внесені якісь конкретні зміни до системи до того, як з'явилася ця проблема? Якщо так, то які саме зміни (детально)?	Завжди згадуйте, які ваші останні зміни або дії були перед тим, як з'явилася проблема, навіть якщо ви вважаєте, що це не має відношення до справи.
Якщо застосовно: На які моделі пристроїв та версії ОС це впливає?	Будь ласка, завжди вказуйте точну версію ОС (наприклад, iOS 14.7.1 або Android 11)
Якщо застосовно: Яка публічна IP-адреса та/або серійний номер пристрою?	Назвіть хоча б один, навіть якщо це стосується всіх пристроїв.
Включити лог-файли	Позначте цей пункт, щоб надіслати файл журналу разом із повідомленням про ваду. Це рекомендується зробити.
Отримати поточний стан VPP від Apple та додати до багрепорту	Містить інформацію про призначення ліцензій VPP. Активуйте цю опцію, тільки якщо вас попросить про

	це служба підтримки або якщо ваша проблема пов'язана з VPP.
Вкладення	Прикріпіть будь-який файл, який може бути корисним (наприклад, скріншоти повідомлення про помилку)

Запит на функцію

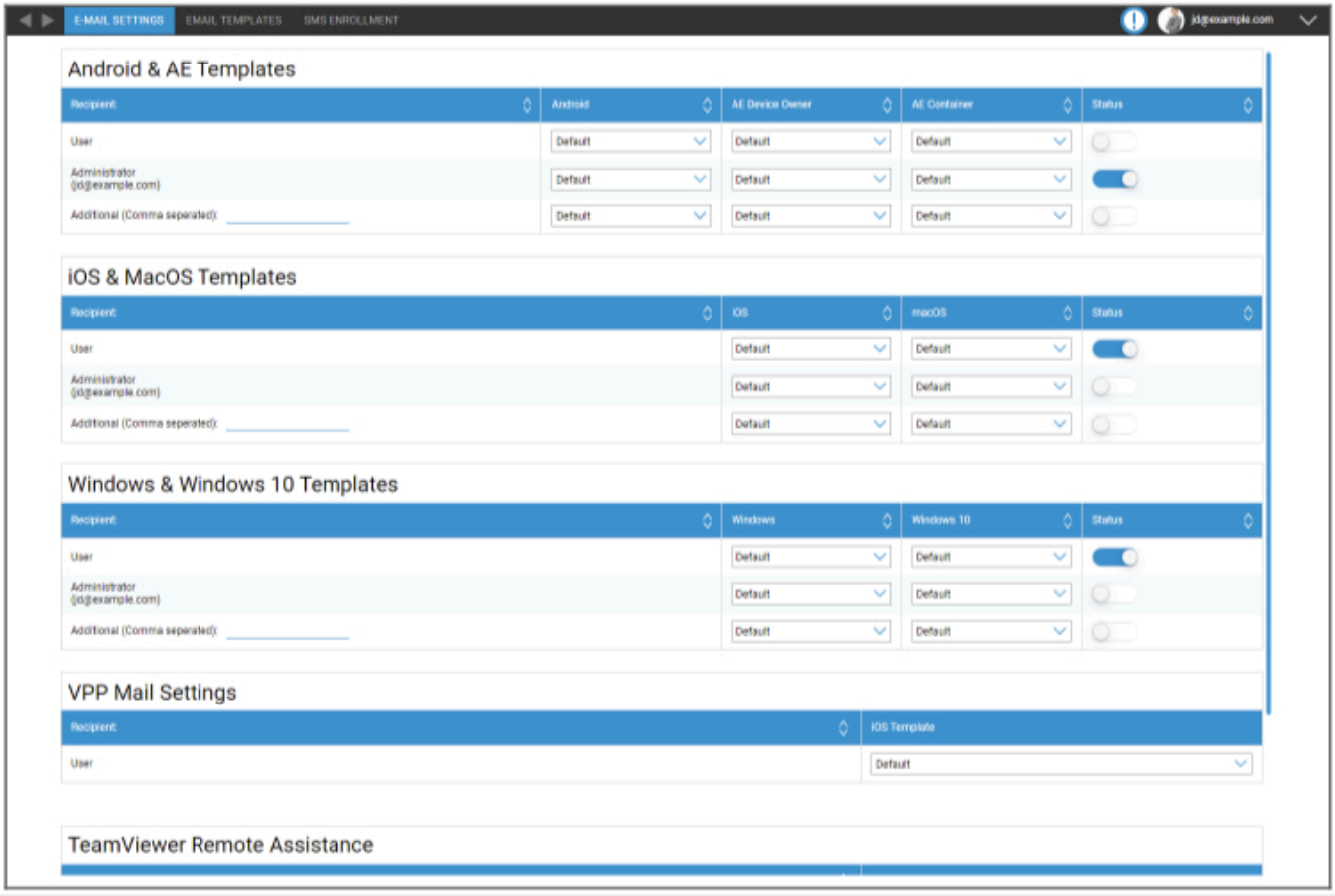
Запит на функцію можна надіслати безпосередньо до служби підтримки. Він може містити запит на певну функцію або поліпшення для

Підсумок	Короткий опис вашої проблеми
Опис	Детальний опис вашої проблеми, будь ласка, будьте максимально конкретними
Вкладення	Прикріпіть файли до повідомлення про ваду

Глобальна конфігурація

Налаштування електронної пошти

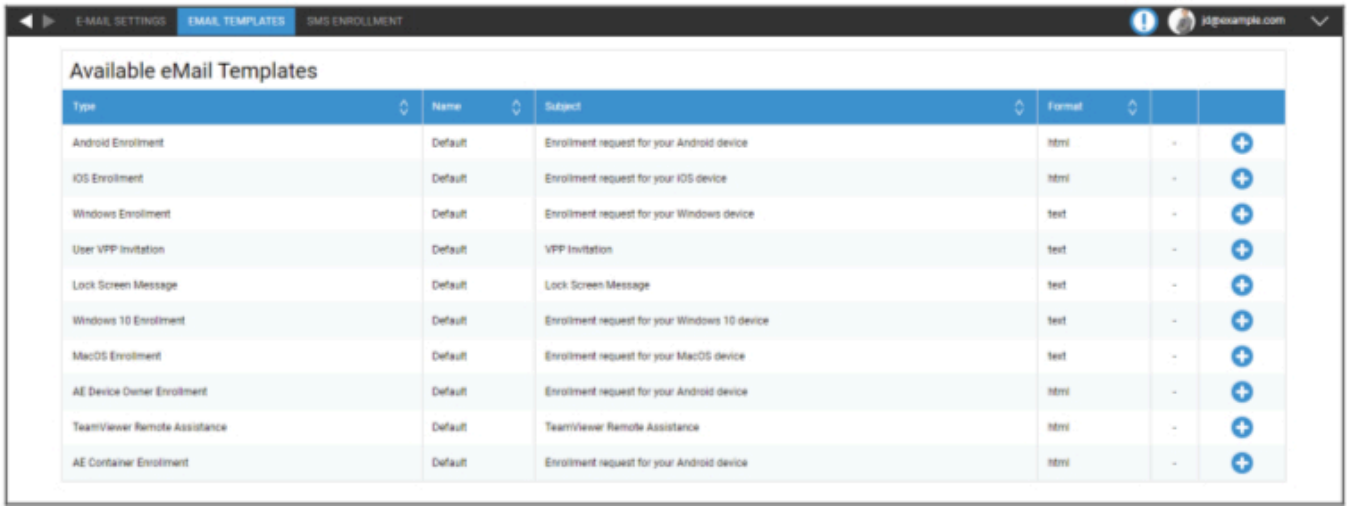
Тут ви можете вказати, хто отримає лист, коли буде створено запит на реєстрацію, і який текстовий шаблон буде використано для цього листа.



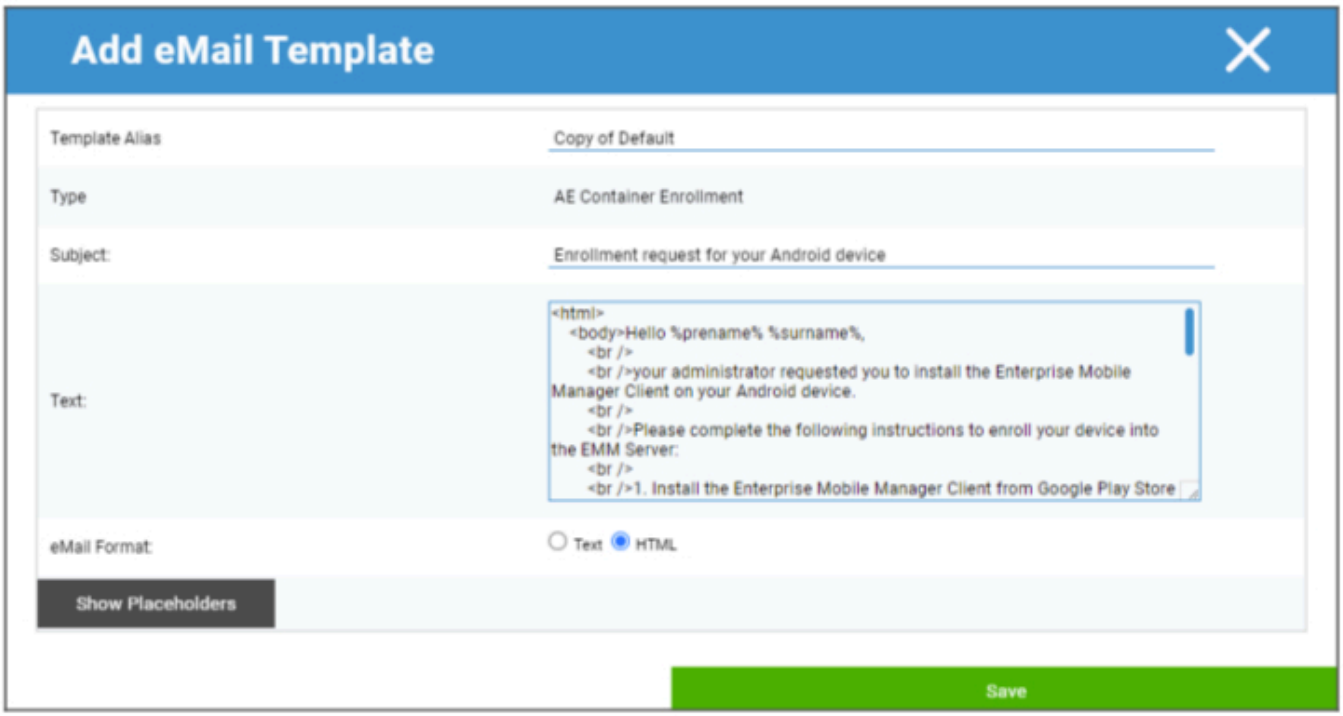
Шаблони електронної пошти

Тут ви можете створювати і редагувати свої шаблони для різних сценаріїв. Вони можуть бути у вигляді звичайного тексту або у форматі HTML. За допомогою HTML ви можете краще контролювати форматування тексту.

Шаблони за замовчуванням не можна редагувати або видаляти.



Ви також можете використовувати заповнювачі як змінні, які будуть автоматично замінені. Натисніть "Показати заповнювачі" під час редагування, щоб побачити доступні заповнювачі. Різні категорії мають різні заповнювачі.



Реєстрація за допомогою SMS

Тут ви можете активувати/деактивувати процес SMS-реєстрації.

(За замовчуванням: вимкнено)

Ви також побачите дисплей, на якому буде вказано, скільки SMS-кредитів залишилося в наявності.

SMS-кредити потрібно купувати окремо.

Конфіденційність

Доступ до GPS

Тут ви можете захистити Перегляд GPS для кожного пристрою за допомогою 1 або 2 паролів (принцип "чотирьох очей"). Вам буде запропоновано ввести пароль (паролі) щоразу, коли ви намагатиметеся отримати доступ до місцезнаходження пристрою.

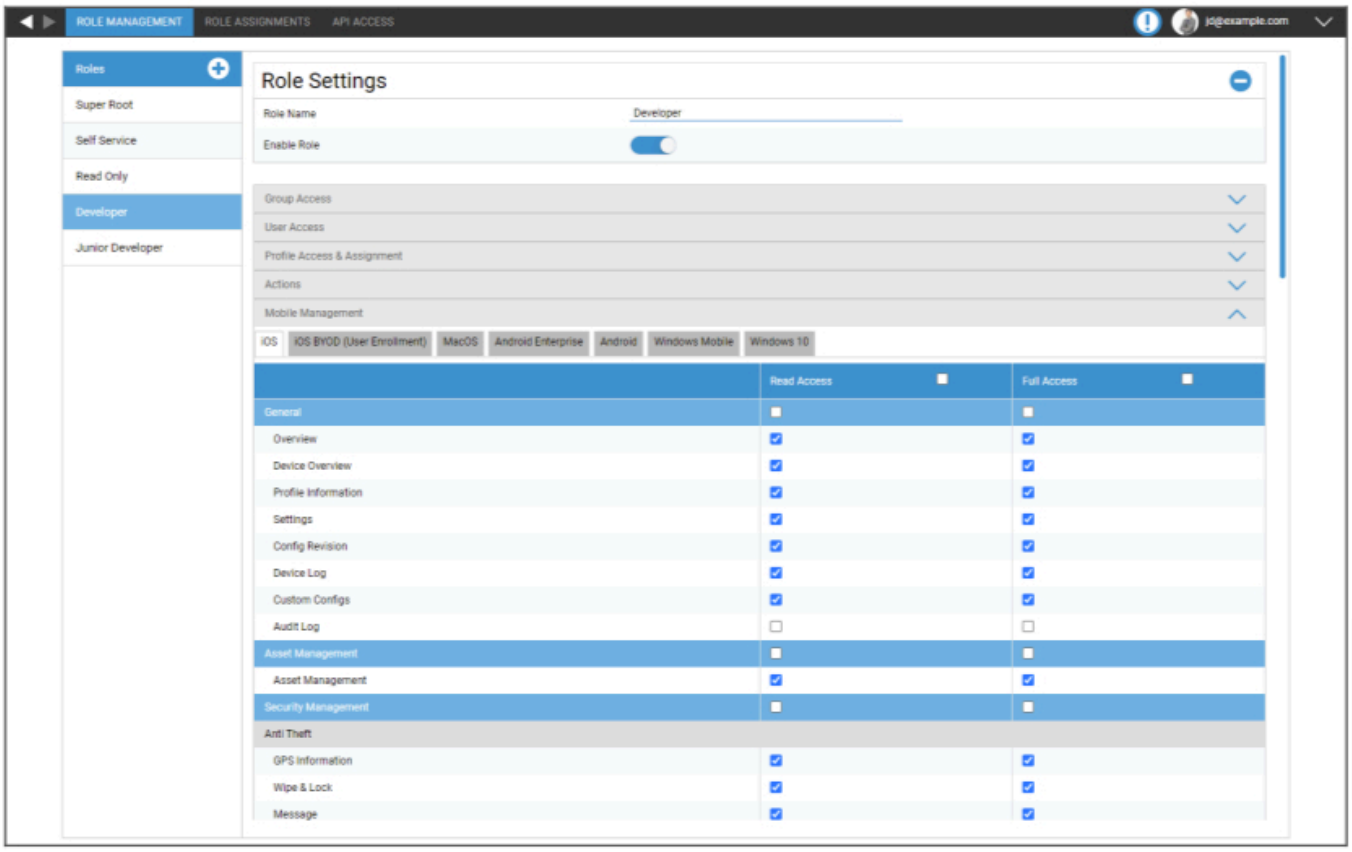
Обмежити доступ до налаштувань GPS	Вимкнено = функція вимкнена і пароль для локалізації не потрібен
	Увімкнено = функція увімкнена і для локалізації потрібен пароль
Спосіб захисту	Використовувати один пароль = використовувати один пароль для локалізації
	Використовувати два паролі = використовувати два паролі для локалізації
Введіть пароль (1)	Введіть обраний пароль
Повторити пароль (1)	Повторно введіть обраний пароль
необов'язково: Введіть пароль 2	Введіть 2-й обраний пароль
за бажанням: Повторити пароль 2	Повторно введіть 2-й обраний пароль

Примітка: Після встановлення пароля(ів) вам потрібно буде ввести його ще раз, перш ніж він буде повністю увімкнений.

Доступ на основі ролей

Управління ролями

Ролі визначають, що користувач може бачити і робити, коли він входить в консоль управління. Це дозволяє створювати користувачів, які можуть входити в систему, але мають обмежену функціональність.



Суперкоренева роль - це роль за замовчуванням, яка завжди може бачити і змінювати все. Її не можна змінити або видалити. Роль самообслуговування може бачити лише своїх користувачів і пристрої. Ви можете поєднати роль самообслуговування і користувацьку роль, щоб, наприклад, дозволити користувачам входити і реєструвати пристрої самостійно і тільки для свого користувача.

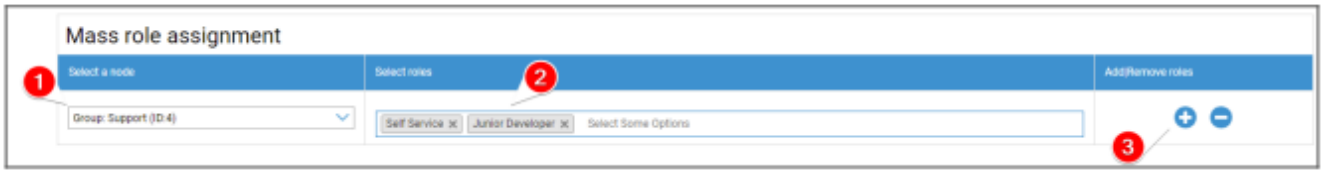
Користувацькі ролі можна ввімкнути або вимкнути вручну. Нові ролі за замовчуванням вимкнено. Користувачі з вимкненою роллю працюють так, ніби вони не мають цієї ролі. Це дозволяє, наприклад, тимчасово обмежити певну роль у діях.

Усі дозволи поділяються на "Доступ для читання" та "Повний доступ". Надання ролям доступу на читання дозволяє їм бачити певну частину консолі. Надання повного доступу дозволяє ролі

бачити і змінювати певну частину консолі.

Розподіл ролей

Тут ви отримаєте огляд всіх користувачів, які мають роль, і побачите, яку саме роль вони мають. Ви також можете призначити роль користувачам або цілим групам:

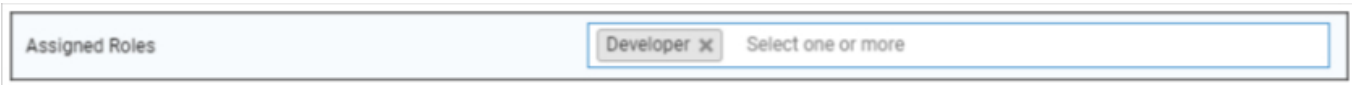


1. Виберіть, для якої групи або користувача ви хочете додати або видалити ролі. Ви можете вибрати окремого користувача або групу. Якщо ви виберете групу, ваші зміни вплинуть на всіх користувачів у цій групі і на всіх користувачів підгруп у вибраній групі.
2. Виберіть, яку роль ви хочете додати або видалити. Ви можете вибрати одну або декілька ролей.
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. Збережіть, щоб завершити процес. Користувачі, у яких раніше не було жодної ролі та відключена опція "Можна увійти", автоматично отримають лист із посиланням для встановлення паролю.

Під масовим призначенням ролей ви можете знайти огляд призначених ролей. Ви також можете вручну змінити ролі для певних користувачів.

Розподіл ролей

Щоб призначити роль користувачеві, перейдіть до Мобільного управління, де ви знайдете дерево ваших груп, користувачів і пристроїв. Відредагуйте користувача, щоб призначити йому роль. Крім того, ви можете використовувати вищезгаданий метод лише для одного користувача.



Доступ до API

Доступ до AppTec360 REST API

AppTec360 REST API вимагає токен автентифікації (ключ API) і приватний ключ, які повинні бути згенеровані в консолі управління.

Для цього увійдіть в AppTec360 EMM і перейдіть до

Загальні налаштування → Доступ на основі ролей → Доступ до API та додайте новий ключ.

Ви повинні вибрати користувача, чиї права будуть застосовані до ключа API.

Приватний ключ можна завантажити лише один раз. Після початку завантаження ключ буде видалено, а кнопка "Завантажити" зникне.

Якщо ви втратите приватний ключ, вам доведеться згенерувати новий API-ключ.

Загальні правила

- REST API доступний під основною URL-адресою:

/public/external/api

- Усі запити мають бути надіслані через POST.
- REST API підтримує запити тільки через HTTPS.
- Запити повинні містити такі заголовки:

Назва заголовка	Значення заголовка	Опис
Тип вмісту	application/json	фіксований
авт.	123...xyz	Ключ API у вкладці "Доступ до API"
підпис	Підпис, закодований Base64	Підпис корисного навантаження, згенерованого за допомогою приватний ключ у вкладці "Доступ до API"

- Тіло запиту має бути об'єктом у форматі json, який повинен містити наступні значення:

Поле	Приклад поля Значення	Опис
api	v2/device/listdevices	Назва API
час	1529662725	Мітка часу Unix (UTC) клієнтської машини. Максимально допустима різниця в часі між клієнтом і сервером дорівнює 30 хвилин.

- У разі успіху API повертає запитувані дані (див. Запити нижче) і код статусу HTTP 200.
- У разі виникнення помилки HTTP-код статусу буде мати значення від 4xx до 5xx залежно від помилки, а об'єкт відповіді міститиме масив з ключем "errors", який містить список повідомлень про помилки, які можна прочитати людиною.
- Якщо для пристрою немає відповідних даних, буде повернуто порожній масив.
- Якщо ідентифікатор пристрою не існує, дані, що повертаються, будуть нульовими.

Приклад запиту

```
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]}}
```

Запити

Перерахувати всі пристрої

Функціональність: Повертає список всіх пристроїв, що містить ідентифікатор пристрою, IMEI та серійний номер
API URI: v2/device/listdevices
Обов'язкові параметри: немає
Необов'язкові параметри: немає

Приклад тіла запиту


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


Приклад органу реагування


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

Отримати список (GPS) позицій

Функціонал: Повертає список всіх збережених записів журналу позицій для ідентифікаторів пристроїв
API URI: v2/device/listposition
Обов'язкові параметри: "ids" - Масив ідентифікаторів пристроїв
Необов'язкові параметри: немає

Приклад тіла запиту


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


Приклад органу реагування


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

Отримати карту активів

Функціональність:
Повертає список усіх збережених можливих активів, які можна запросити за допомогою функції Get any asset data.
Для запиту даних можна використовувати зручну для читання форму або тег активу.
API URI: v2/device/getassetmap
Обов'язкові параметри: немає
Необов'язкові параметри: немає

Приклад тіла запиту

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

Приклад органу реагування

Ця відповідь була скорочена для зручності читання.

{
"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": []
}

Отримуйте будь-які дані про активи

Функціональність: Повертає список запитаних даних активів для ідентифікаторів пристроїв
API URI: v2/device/getassetdata
Обов'язкові параметри: "ids" - Масив ідентифікаторів пристроїв
Необов'язкові параметри:
"assetkeys" - Ключі даних активів для повернення. Якщо не вказано, будуть повернуті всі доступні дані активів. Ви можете отримати список ключів активів за допомогою кнопки Отримати карту активів.

Приклад тіла запиту


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


Приклад органу реагування


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

Приклад коду на 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)
```

Конфігурація Apple

Сертифікат APNS

Тут ви можете завантажити сертифікат APNS. Він необхідний для керування пристроями на iOS та MacOS.

Примітка: Сертифікат APNS дійсний лише один рік. Його необхідно поновити до закінчення терміну дії. Процес поновлення ідентичний процесу створення (див. нижче) і займає лише кілька хвилин.

Якщо ви забудете поновити його вчасно, ви не зможете вносити зміни до вже зареєстрованих пристроїв **і вам доведеться зареєструвати всі пристрої заново**.

Крок 1

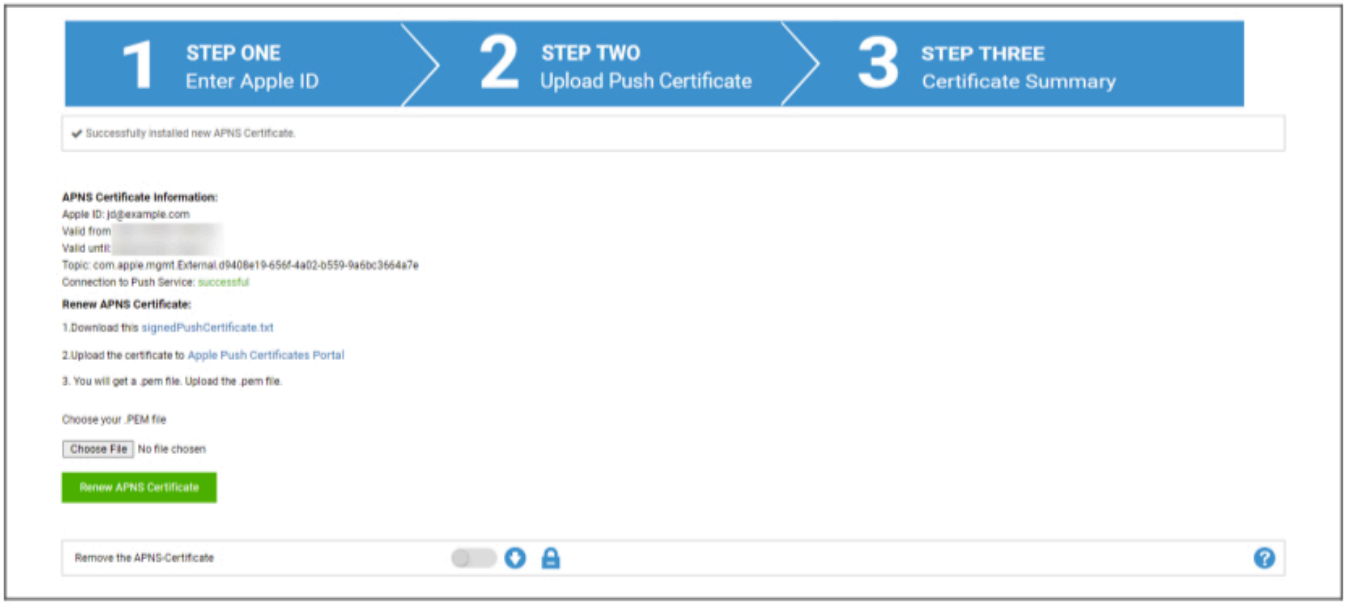
- Спочатку введіть свій Apple ID, який ви хочете використовувати для створення сертифіката APNS.

Примітка: Цей Apple ID використовується лише для створення сертифікату APNS. Цей Apple ID не має нічого спільного з пристроями, і пристрої не будуть знати про цей Apple ID. Крім того, вам також потрібен доступ до цього Apple ID для поновлення сертифіката APNS. Тому рекомендується використовувати якийсь загальний Apple ID і задокументувати дані для входу. Перед закінченням терміну дії сертифікату APNS на використану поштову адресу Apple ID буде надіслано нагадування.

- Натисніть "Наступний крок", щоб продовжити.
- (необов'язково) Ви також можете відновити раніше видалений сертифікат APNS, якщо ви видалили його випадково

Крок 2

- Завантажте файл signedPushCertificate.txt
- Перейдіть на сайт https://identity.apple.com/pushcert/ та увійдіть за допомогою Apple ID з кроку 1
- Натисніть "Створити сертифікат"
- (необов'язково) введіть Примітку. Це може бути корисно, якщо ви керуєте кількома орендарями, щоб легко їх ідентифікувати.
- Натисніть "Вибрати файл", щоб вибрати раніше завантажений файл signedPushCertificate.txt
- Натисніть на кнопку "Завантажити".
- Тепер ви побачите підтвердження того, що ви створили сертифікат APNS.
- Натисніть "Завантажити" та збережіть його.
- Поверніться до консолі керування.
- Натисніть "Вибрати файл" і виберіть сертифікат APNS, який ви хочете завантажити.
- Натисніть на кнопку "Завантажити"



Крок 3

Ви успішно налаштували сертифікат APNS і тепер можете керувати пристроями на iOS і MacOS.

На кроці 3 ви побачите огляд вашого поточного сертифіката APNS.

Також у вас є можливість поновити сертифікат APNS, виконавши кроки, показані на екрані. Не забудьте поновити його до закінчення терміну дії.

Поновлюючи сертифікат APNS, пам'ятайте, що потрібно входити за допомогою Apple ID, показаного в Кроці 3, а також поновлювати раніше використаний сертифікат, а НЕ створювати новий. Ви побачите "тему" сертифіката APNS у Кроці 3 та при натисканні на "i" на порталі Apple Push Certificate Portal. Це унікальний ідентифікатор, який ідентифікує сертифікат. Це допоможе вам визначити правильний сертифікат і поновити його.

Коли ви отримуєте повідомлення "Помилка: Push-сертифікат має іншу тему!" під час поновлення, це означає, що ви поновили інший сертифікат або створили новий.

Якщо ви хочете завантажити новий сертифікат, наприклад, якщо ви більше не можете отримати доступ до Apple ID, який використовували раніше, спочатку видаліть поточний завантажений сертифікат.

У будь-якому разі видалення сертифіката APNS означає, що ви більше не зможете вносити зміни для зареєстрованих пристроїв, доки не зареєструєте їх знову. Тому переконайтеся, що ви готові до цього, і видаляйте сертифікат лише у випадку, якщо немає іншого виходу.

Керований доступ

Тут ви можете ввімкнути реєстрацію користувачів для пристроїв iOS та спільний доступ до iPad для пристроїв iOS.

Реєстрація користувачів

"Реєстрація користувачів" вмикає спеціальний режим для пристроїв BYOD.

Для кожного користувача необхідно створити керований Apple-ID на бізнес-порталі Apple Business Portal.

Під час реєстрації користувачам буде запропоновано ввести свої облікові дані Apple-ID.

"Реєстрація користувача" гарантує максимальну безпеку для користувача, оскільки дозволяє лише обмежений набір налаштувань та обмежень, які можуть бути налаштовані MDM.

Керований домен:

Домен, який використовується для зіставлення адреси електронної пошти користувача з його керованим Apple-ID (має бути у форматі: "@appleid.company.com"). Наприклад, john.doe@example.com буде зіставлено з john.doe@appleid.company.com.

Перевірте свій керований домен у бізнес-менеджері Apple Business Manager

Спільний iPad

Спільний iPad - це пристрій DEP, налаштований за допомогою спеціального профілю DEP.

Це дозволяє декільком користувачам входити на пристрій за допомогою керованого Apple-ID.

Керований Apple-ID має бути створений в Apple Business Portal або в Apple School Manager.

Користувачам, які заходять на спільний iPad, пропонується ввести свої керовані облікові дані Apple-ID.

Керований домен:

Домен, який використовується для зіставлення адреси електронної пошти користувача з його керованим Apple-ID (має бути у форматі: "@appleid.company.com"). Наприклад, john.doe@example.com буде зіставлено з john.doe@appleid.company.com.

Перевірте свій керований домен у бізнес-менеджері Apple Business Manager

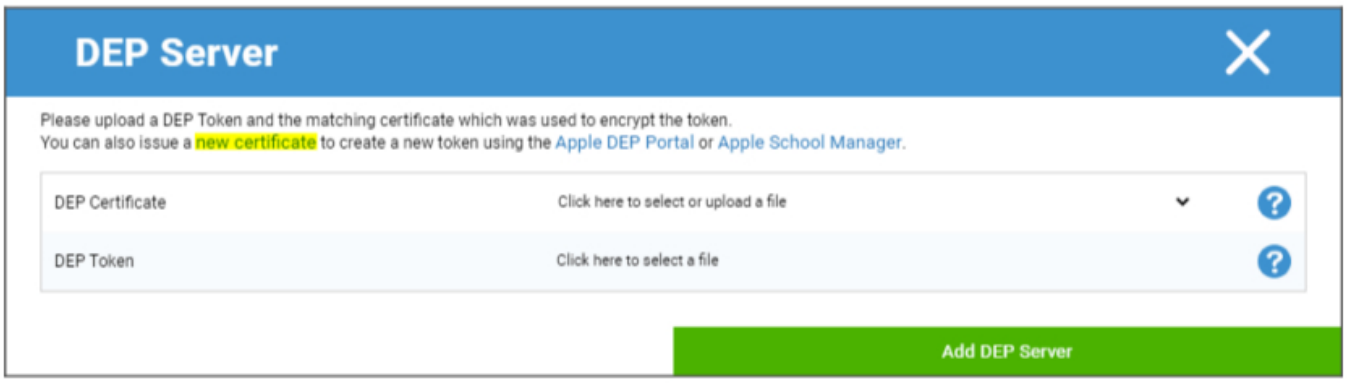
DEP

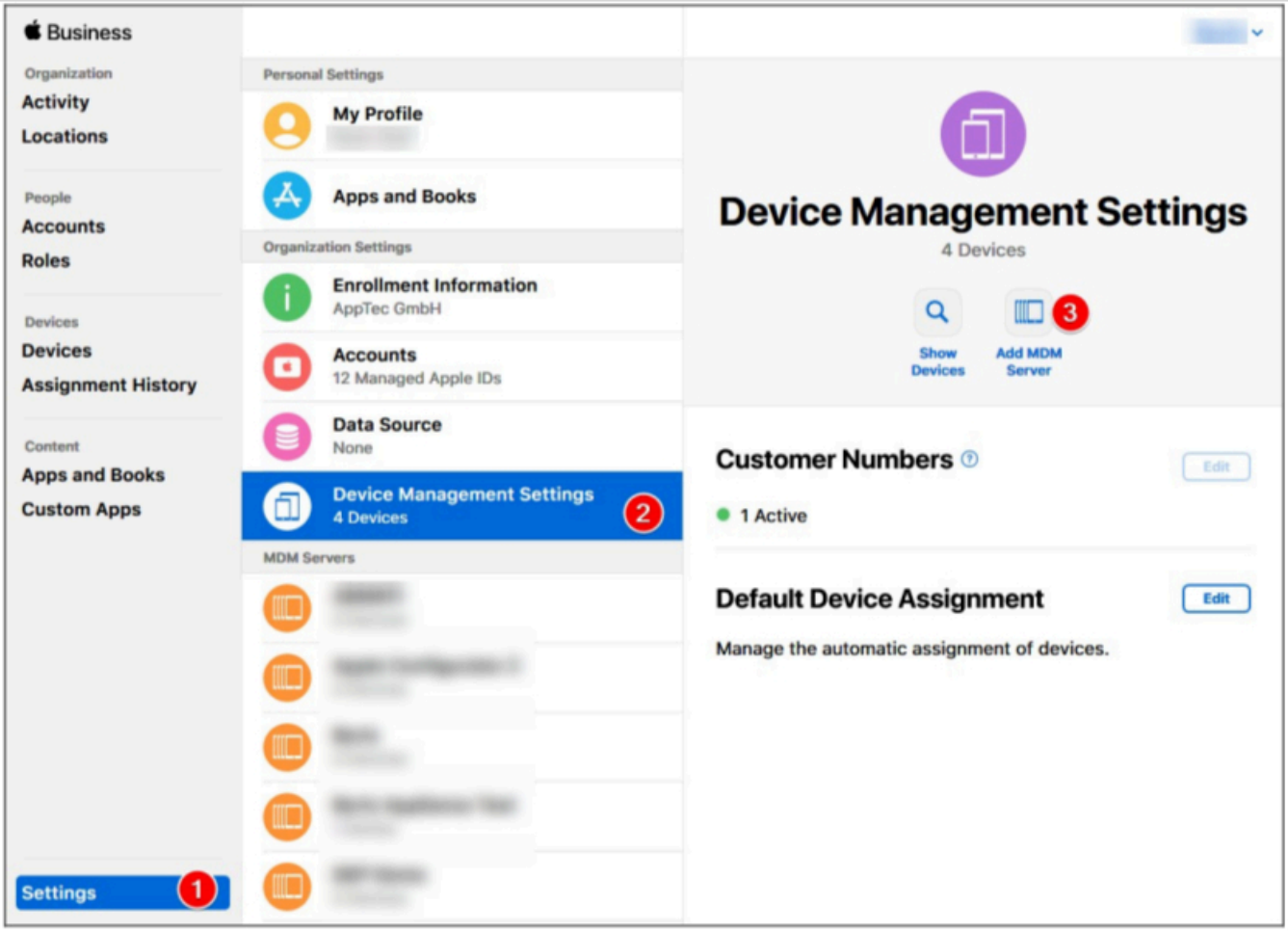
DEP (Device Enrollment Program - програма реєстрації пристроїв) дозволяє легко реєструвати пристрої в MDM. При використанні DEP пристрої будуть автоматично підключені до MDM під час налаштування пристрою. Ви також можете пропустити майже всі кроки налаштування, які зазвичай є обов'язковими в iOS.

Майте на увазі, що пристрої потрібно купувати у реселера, який підтримує DEP. Для отримання додаткової інформації зверніться до свого реселлера або до Apple.

Більше інформації про DEP: https://www.apple.com/business/dep/

Натисніть на "+", щоб додати DEP Token. У спливаючому вікні натисніть на "новий сертифікат" у тексті (позначений жовтим кольором на зображенні нижче). Це призведе до створення та завантаження сертифікату DEP. Після цього перейдіть до Apple Business Manager(https://business.apple.com/) або Apple School Manager(https://school.apple.com/).

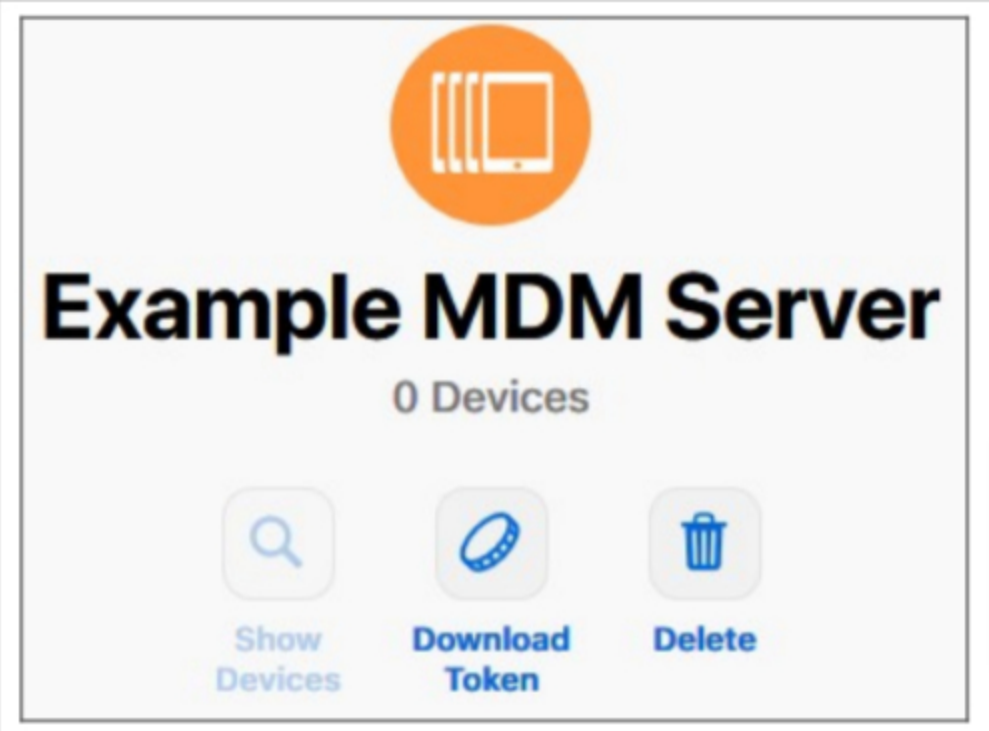




В Apple Business Manager виконайте кроки, як показано на зображенні вище. Налаштування → Налаштування керування пристроями → Додати сервер MDM.

Дайте серверу будь-яке ім'я і завантажте раніше завантажений DEP-сертифікат у розділі Налаштування сервера MDM → Завантажити відкритий ключ і натисніть кнопку "Зберегти".

Тепер у вас буде опція "Завантажити токен". Натисніть на нього і збережіть його. Токен дійсний лише 1 рік. Але при повторному натисканні кнопки "Завантажити токен" ви отримаєте новий токен, що робить поновлення токена дуже простим.



Тепер ви можете повернутися до MDM, звідки раніше завантажили DEP-сертифікат. Якщо ви не закрили вкладку, спливаюче вікно для додавання DEP-сервера все ще має бути відкрите, а DEP-сертифікат вже має бути вибраний. Тепер ви можете завантажити свій токен в поле "DEP Token" і натиснути на DEP Server.

У колонці "**Пристрої**" ви побачите кількість пристроїв, призначених для цього сервера DEP. Пристрої, додані до цього сервера DEP, будуть автоматично створені в пулі DEP в Мобільному менеджменті.

Ви можете натиснути на цей номер, щоб отримати огляд усіх ваших пристроїв DEP та їхнього стану.

Примітка: Залежно від вашого робочого процесу або конфігурації в Business Manager, можливо, вам доведеться вручну призначити ці пристрої на сервер DEP. Ви також можете встановити сервер DEP за замовчуванням в Apple Business Manager для нових пристроїв.

У колонці "**Профілі**" ви бачите кількість наявних у вас DEP-профілів. Ви також можете натиснути на це число, щоб переглянути детальну інформацію про ваші DEP-профілі, і ви можете видалити старі/невикористовувані профілі тут. Наразі змінити їх неможливо. Якщо ви хочете внести зміни, вам доведеться створити новий профіль.

У колонці "**Остання синхронізація**" ви можете вручну синхронізувати сервер DEP (наприклад, якщо ви щойно додали новий пристрій до DEP) і побачити дату останньої успішної синхронізації.

У колонці "Автоматичний**профіль**" ви можете встановити профіль DEP як автоматичний за замовчуванням. Цей профіль буде автоматично призначатися новим пристроям. Якщо ви не встановите автоматичний профіль, вам доведеться щоразу призначати профіль новим пристроям вручну.

У колонці "**Додати профіль**" ви можете додати новий профіль DEP. Пристрій отримає його на початку налаштування пристрою. Профіль DEP визначає спосіб налаштування пристрою і те, які кроки налаштування будуть пропущені.

Примітка: після реєстрації пристрою ці налаштування можна змінити, лише виконавши скидання до заводських налаштувань і зареєструвавши пристрій з новим профілем. Це особливо актуально для параметрів "**Знімний**" і "Дозволити**сполучення**". У випадку "**Дозволити**сполучення" рекомендується увімкнути цю опцію, оскільки її можна вимкнути за допомогою обмежень MDM, але її не можна увімкнути знову, якщо її вимкнено у профілі DEP.

У колонці "**Редагувати**" ви можете завантажити новий токен, наприклад, при поновленні токена.

Конфігуратор та URL-адреса

URL-адреси для реєстрації в пулі

Тут ви можете створити URL-адресу для реєстрації та QR-код для реєстрації, які будуть дійсні протягом певної кількості реєстрацій і до певної дати. Це дозволить вам зареєструвати декілька пристроїв, які мають лише одне посилання або QR-код.

Пристрої, зареєстровані за допомогою цієї URL-адреси або QR-коду, будуть у пулі в Мобільному управлінні, і вам потрібно буде вручну призначити їх групі або користувачеві.

Примітка: це лише для реєстрації вручну. Не використовуйте цю URL-адресу, якщо ви реєструєте пристрої за допомогою Apple Configurator

Профіль MDM – Apple Configurator

Тут ви можете отримати URL-адресу, необхідну для реєстрації пристроїв через Apple Configurator. Під час підготовки пристроїв за допомогою Apple Configurator ви можете додати пристрої до MDM в тому ж процесі. Для цього Apple Configurator вимагає цю URL-адресу.

Пристрої, додані через Apple Configurator, будуть у пулі в Мобільному управлінні, і вам потрібно буде вручну призначити їх групі або користувачеві.

Тут ви також знайдете файл .mobileconfig, який можна використовувати для реєстрації пристроїв через Apple Configurator. У будь-якому випадку рекомендується використовувати URL-адресу.

Конфігурація Android

Конфігурація Android

Видалити захист	Якщо цю функцію увімкнено, користувач не може деактивувати адміністратора пристрою без введення пароля, встановленого адміністратором MDM. Пароль встановлюється під час реєстрації, тому для оновлення пароля необхідно повторно зареєструвати пристрої. Існує два варіанти видалення адміністраторів пристроїв: 1. Вручну на пристрої ◦ Відкрийте програму EMM на пристрої ◦ Перейдіть на вкладку Статус ◦ Натисніть "Видалити захист" ◦ Введіть пароль Ви можете скористатися ревізією, щоб отримати правильний пароль з "Історії паролів" у консолі. ◦ Прокрутіть вниз і торкніться нещодавно доданого пункту "Натисніть, щоб видалити додаток AppTec360 MDM" (у вас є 20 секунд на виконання цього завдання) ◦ Підтвердіть діалог "Видалити AppTec360 MDM App", натиснувши "ok". Це призведе до видалення пристрою з консолі. ◦ Щоб видалити програму з пристрою, підтвердіть діалог "AppTec360 MDM буде деінстальовано", натиснувши "ВИДАЛИТИ". 2. автоматичний (Console) ◦ Виберіть Пристрій в консолі ◦ Натисніть на синій значок шестерні та виберіть "Enterprise Wipe" Примітка: Доступно лише на Android 4.x і новіших версіях або на пристроях з KNOX API (пристрої Samsung)

Видалити пароль (версія x)	Встановлений пароль, за допомогою якого користувач може відсторонити адміністратора пристрою Ревізія x = лічильник, як часто пароль вже змінювався Важливо, який пароль потрібен користувачеві, оскільки можливо, що пристрій не зв'язувався з сервером AppTec360 і тому найновіший пароль ще не був переданий
Історія паролів	При натисканні на синю кнопку ("Показати історію") ви зможете переглянути раніше встановлені паролі
Розширений захист від видалення	Ця опція забезпечує захист від небезпечних пристроїв Поки цей параметр активовано, неможливо легко деактивувати адміністратора пристрою
Запропонувати користувачеві видалити заблоковані програми?	Якщо це можливо, заблоковані Програми будуть не лише заблоковані, але й автоматично видалені. Користувачеві буде запропоновано видалити заблоковані програми, якщо автоматичне видалення неможливе.
Блокування додатків інтелектуальної системи	Якщо увімкнено Білий список, клієнт Android MDM блокує всі встановлені користувачем програми. Увімкніть цей параметр, щоб блокувати всі системні програми, що запускаються, у режимі білих списків.

Автоматична реєстрація

Тут ви можете увімкнути функцію автоматичної реєстрації, щоб автоматично реєструвати ваші пристрої, коли клієнт AppTec360 MDM відкривається на пристрої.

Важливо: Цей метод реєстрації застарілий і більше не працює на Android 10 або новіших версіях. У будь-якому випадку, якщо ви використовуєте Android 7 або новішу версію, вам слід зареєструвати пристрої як Android Enterprise з повним керуванням. Якщо ви хочете використовувати контейнер Android Enterprise BYOD на Android 10 або новішої версії, вам потрібно вручну зареєструвати пристрій за допомогою облікових даних, QR-коду або SMS. У будь-якому випадку, список автоматичної реєстрації все ще використовується для автоматизації процесу реєстрації, наприклад, AE Enrollment, Knox Enrollment тощо.

Так чи інакше, список автоматичного зарахування все ще використовується для автоматизації процесу зарахування, наприклад, AE зарахування, Knox зарахування тощо.

Натиснувши на "Менеджер серій" або "Менеджер IMEI", ви можете додати серійний номер або IMEI ваших пристроїв відповідно. Не обов'язково робити це для обох пристроїв, достатньо лише одного.

Дія визначає, хто буде вносити пристрої до пулу - користувач або група.

Ви також можете експортувати та імпортувати файл .csv і фільтрувати записи за ключовими словами.

Android Enterprise

Тут ви можете налаштувати Android Enterprise. Це необхідно для використання всіх функцій Android Enterprise.

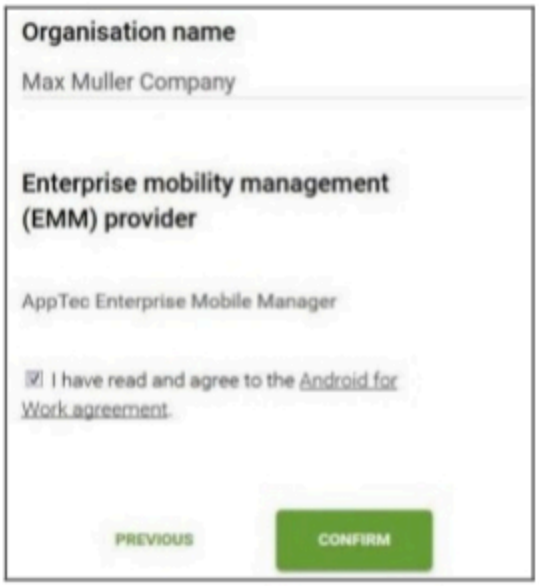
Перший спосіб: Корпоративний обліковий запис Android (обліковий запис Google)

Спочатку натисніть "Prepare Setup", після чого через деякий час повинна з'явитися кнопка "Start Setup".

Ви потрапите на сторінку налаштувань Android для підприємств від Google.

Увійдіть у свій обліковий запис Google, якщо ви ще не ввійшли, і натисніть "Почати".

Тепер ви можете ввести назву вашої компанії. Після цього встановіть прапорець і натисніть "Підтвердити"



На останньому кроці ви можете завершити реєстрацію і повернутися до консолі. Якщо все пройшло успішно, вона повинна виглядати так:

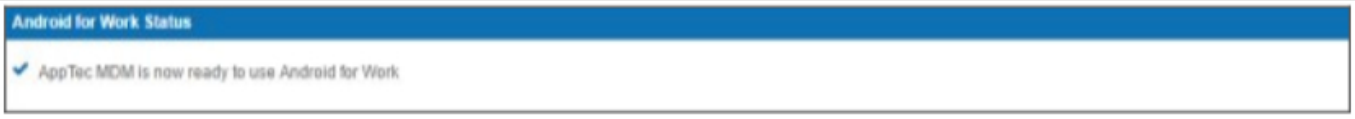
Тепер ви можете приступити до налаштування вашого Android Enterprise Container.

Другий спосіб: Обліковий запис G-Suite

Натисніть "Використовувати G-Suite" і увійдіть до свого облікового запису адміністратора Google. Там перейдіть до "Безпека" -> "Показати більше" -> "Керування постачальником EMM для Android" і згенеруйте токен. Примітка: Якщо ви не бачите корпоративних налаштувань Android у вашому обліковому записі G-Suite, вам потрібно перейти до "Отримати більше додатків і служб" і додати управління пристроями Android. Тепер введіть токен і ваш основний домен у нашій консолі та натисніть "Зберегти зміни". Закінчивши, натисніть "Використовувати корпоративний обліковий запис Android".

Тепер ви повинні побачити кнопку "Створити обліковий запис". Натисніть на неї. Цей процес може зайняти кілька хвилин.

Якщо все працювало, це має виглядати так:



Тепер ви можете приступити до налаштування вашого Android Enterprise Container.

Захист від скидання до заводських налаштувань

За допомогою функції захисту від скидання до заводських налаштувань ви можете прив'язати свій пристрій до обраного вами облікового запису Google, що також замінить будь-яку існуючу прив'язку до облікового запису Google. Щоб використовувати захист від скидання до заводських налаштувань, вам потрібно спочатку налаштувати його тут, а потім активувати у своїх профілях.

Щоб налаштувати захист від скидання до заводських налаштувань, натисніть "Налаштування FRP" і дотримуйтесь інструкцій на екрані.

ПРИМІТКА: Уважно прочитайте та виконайте кроки. Ми рекомендуємо робити це в новому вікні браузера інкогніто, щоб уникнути автоматичного входу в неправильний обліковий запис Google. Ви можете повністю заблокувати себе на пристрої, якщо введете неправильний ідентифікатор або втратите доступ до використовуваного облікового запису Google!

Зарахування на AE

Тут ви можете активувати Android Enterprise Ernollment. Використання цього методу переведе ваші пристрої в режим власника Android Enterprise Device Owner Mode. У цьому режимі ви матимете повний контроль над пристроєм.

Увімкнути реєстрацію AE	Активує попередження про реєстрацію AE: Якщо ви вимкнете функцію AE Enrollment, наявні QR-коди та вже налаштовані пристрої NFC-програматори перестануть працювати. Якщо ви знову увімкнете AE Enrollment, вам доведеться повторно надіслати конфігурації NFC push / згенерувати нові QR-коди.
Увімкнути автоматичне виявлення	Коли пристрій реєструється через "AE Enrollment", система спробує призначити його користувачеві на основі інформації, встановленої в Білому списку серійних номерів / IMEI ("Загальні налаштування" > "Конфігурація Android" > "Автоматична реєстрація").
Блокувати невідомі пристрої	Дозволяється реєструвати лише ті пристрої, які були внесені до білого списку серійних номерів / IMEI ("Загальні налаштування" > "Конфігурація Android" > "Автоматичне реєстрування").

Примітка до методів 1 і 2: "Екран привітання" - це перший екран, який ви бачите після скидання до заводських налаштувань. Він може виглядати по-різному залежно від версії Android та/або моделі пристрою, який ви використовуєте.

Спосіб 1: Реєстрація за допомогою QR-коду

(вимагає Android 7.0 або новішої версії) Ми рекомендуємо завжди використовувати цей метод, якщо ви використовуєте Android 7 або новішу версію.

1. Скидання пристрою до заводських налаштувань
2. Згенеруйте QR-код для реєстрації за допомогою одного з двох наступних методів:
    - Натисніть у "Загальні налаштування -> Конфігурація Android -> Реєстрація AE" на "Згенерувати QR-код". Виберіть, чи хочете ви пропустити шифрування сховища та/або видалити всі системні програми.
    - (альтернативно) Виберіть існуючий Пристрій. В "Огляді пристрою" натисніть на QR-код, який там відобразиться. Виберіть, чи хочете ви пропустити шифрування сховища та/або видалити всі системні програми.
3. Тепер торкніться 6 разів на екрані привітання вашого пристрою. Це має запустити режим реєстрації за допомогою QR.
4. Тепер підключіться до бездротової мережі та зачекайте деякий час, поки зчитувач QR-кодів встановиться
5. Тепер відскануйте QR-код

6. Це все. Ваш пристрій тепер зареєстровано в режимі корпоративного пристрою Android.
    - a. Якщо ви використовували QR-код у "Загальних налаштуваннях", ви можете знайти свій пристрій у розділі "Пул -> Пристрої власників AE-пристроїв". (Підказка: Можливо, вам доведеться перезавантажити сайт, щоб побачити пристрої). Якщо ви поставили галочку "Увімкнути авторозпізнавання", ви знайдете його у вашому користувачеві авторозпізнавання.
    - Якщо ви використали QR-код існуючого профілю пристрою, пристрій буде зареєстровано в цьому профілі.

Спосіб 2: Реєстрація за допомогою NFC

(потрібен NFC та Android 6.0 або новішої версії)

Підготовка: Введіть інформацію про ваш WiFi у "Загальні налаштування -> Конфігурація Android -> Реєстрація AE -> Дані для налаштування NFC". Тепер за допомогою "Пристрій NFC" знайдіть пристрій, який стане програматором. Цей пристрій буде використовуватися для надсилання інформації про реєстрацію на інші пристрої через NFC.

1. Скидання до заводських налаштувань
2. Відкрийте програму для створення пари NFC з AppTec360 на вашому програматорі
3. Виберіть, чи хочете ви пропустити шифрування сховища та/або видалити всі системні програми.
4. Тримайте обидва пристрої спиною до спини
5. Тепер Android Enterprise Enrollment має стати
6. Тепер ви знайдете свій пристрій у консолі
    - a. У пулі, якщо ви не налаштували автоматичне виявлення
    - b. Для користувача, якого ви налаштували для автоматичного виявлення
    - c. Підказка: Можливо, вам доведеться перезавантажити сайт, щоб побачити пристрої

Спосіб 3: Акаунт Google

(потрібна Android 5.1 або новіша версія)

(Примітка: Якщо ви використовуєте цей метод, пристрій не буде автоматично зареєстровано. Замість цього вам доведеться зареєструвати його вручну або автоматизувати процес за допомогою функції автоматичної реєстрації).

1. Скидання до заводських налаштувань
2. Пройдіть кроки налаштування, поки не зможете увійти за допомогою облікового запису Google
3. Введіть "afw#apptec" як ім'я користувача/пошту
4. Натисніть "Далі"

5. Ваш пристрій тепер є корпоративним пристроєм Android

Вступ до KNOX

Тут ви можете активувати реєстрацію KNOX і знайти інформацію, необхідну для створення профілю реєстрації KNOX на порталі розгортання KNOX. Щоб налаштувати і використовувати цей інструмент, вам потрібен обліковий запис на порталі розгортання KNOX.

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

Увімкнути реєстрацію в KNOX	Активує реєстрацію в KNOX. Увага: Якщо ви вимкнете реєстрацію KNOX, існуючі профілі MDM перестануть працювати. Якщо ви знову увімкнете реєстрацію KNOX, вам потрібно буде оновити поле "Спеціальні JSON-дані" у вашому профілі MDM
Увімкнути автоматичне виявлення	Коли пристрій реєструється через "Реєстрація KNOX", система спробує призначити його користувачеві на основі інформації, встановленої в Білому списку серійних номерів / IMEI ("Загальні налаштування" > "Конфігурація Android" > "Автоматична реєстрація").

1. Увійдіть на мобільний портал Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Перейдіть до "Профілі MDM"
3. Натисніть на кнопку "Додати"
4. Виберіть "URI сервера не потрібен для мого MDM" і натисніть "Далі"
5. Тепер створіть профіль з інформацією, показаною в консолі керування

Тепер цей профіль реєстрації KNOX може бути безпосередньо встановлений на пристрій Samsung, якщо ви купуєте пристрої безпосередньо у Samsung.

Крім того, ви можете завантажити додаток KNOX Deployment App, увійти за допомогою свого облікового запису розгортання KNOX і відправити профіль реєстрації KNOX за допомогою NFC на інші пристрої.

Якщо на пристрої встановлено профіль реєстрації KNOX, він завантажить наш додаток і зареєструє пристрій, якщо у нього є доступ до Інтернету.

Пристрої, що реєструються через KNOX, можна знайти в "Пул -> Реєстрація KNOX" або у користувача, якого ви вказали у вікні Автоматичного виявлення.

Нульовий дотик

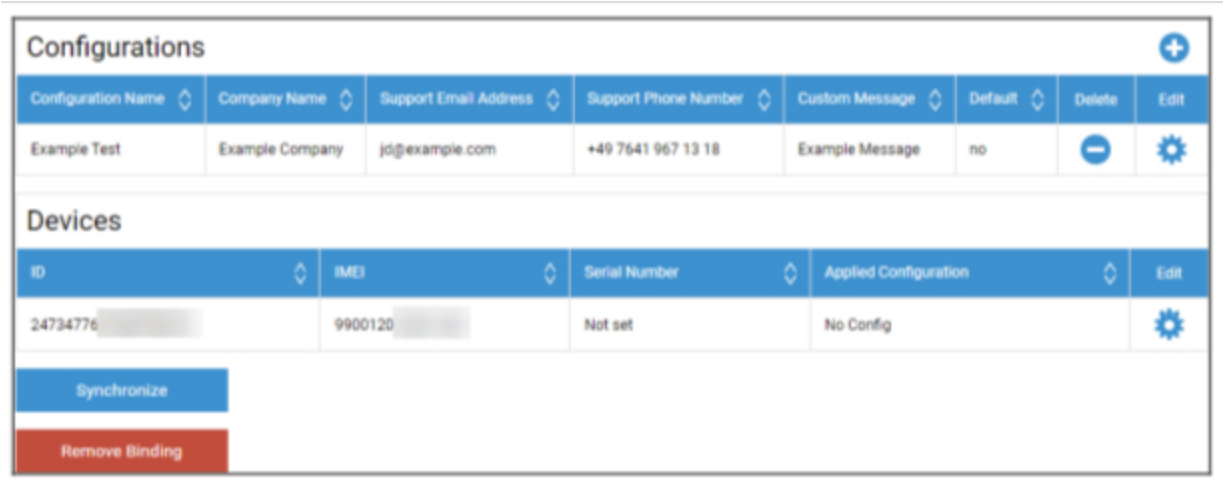
За допомогою Zero-Touch ви можете легко реєструвати свої пристрої, не торкаючись їх і не налаштовуючи нічого на самому пристрої. Вам просто потрібно увімкнути його, виконати конфігурацію, як зазвичай, і пристрій отримає всю інформацію про те, як налаштувати і підключитися до MDM, повністю автоматично.

Щоб користуватися Zero-Touch, ви повинні придбати свої пристрої у дилера, який підтримує Zero-Touch. Той самий дилер також створить для вас обліковий запис на порталі Zero-Touch. Зверніться до свого дилера, щоб отримати додаткову інформацію про процедуру або якщо у вас виникли проблеми з доступом до порталу Zero-Touch.

Натисніть на "Почати налаштування", щоб розпочати налаштування. Вас буде перенаправлено на сторінку входу, де ви повинні вибрати свій обліковий запис Google, який має доступ до порталу Zero-Touch.

ПРИМІТКА: Можна вибрати БУДЬ-ЯКИЙ обліковий запис. Тому переконайтеся, що ви вибрали правильний обліковий запис на цьому кроці. Якщо ви не бачите свої пристрої/конфігурації, швидше за все, ви вибрали неправильний обліковий запис.

Після завершення входу він матиме такий вигляд:



Натисніть на "+", щоб додати конфігурацію і заповніть поля, як показано на екрані. Якщо ви ввімкнете конфігурацію як конфігурацію за замовчуванням, вона буде призначена новим пристроям автоматично. Створення або встановлення конфігурації за замовчуванням не призначає її вже існуючим пристроям.

Якщо пристрій не має призначеної конфігурації, він буде налаштований як звичайний пристрій і не підключиться до MDM. Тому переконайтеся, що вашим пристроям призначено конфігурацію.

Після того, як ви підключили свій обліковий запис, ваші пристрої стали видимими, і для них призначено конфігурацію, ви можете почати налаштування пристроїв.

Ви можете додати пристрої до списку автоматичного входу, щоб вони автоматично входили до вказаної групи або користувача. Якщо ви нічого не налаштували у списку автоматичного зарахування, пристрої буде зараховано до пулу.

Конфігурація Windows

Конфігурація Windows

Тут у вас є можливість увімкнути наступні конфігурації на вашому комп'ютері з Windows 10:

Миттєве підключення DM	
Початковий час повторної спроби	Встановлює першу спробу підключення до пристрою, це значення збільшується в геометричній прогресії
Повторні спроби з'єднання	Вказує, скільки спроб з'єднання повинен виконати DM-клієнт під час помилки з'єднання
Максимальний час сну	Показує максимальний час очікування після помилки з'єднання
Перші спроби синхронізації	Інтервали, через які пристрій має виходити на зв'язок із сервером після першого з'єднання
Перший інтервал повторної спроби	Пов'язано з "Перші спроби синхронізації" Тут час вказано в хвилинах Наприклад, у полі "Перші спроби синхронізації" вказано значення "2", а в полі "Інтервал перших спроб" вказано значення "4 хвилини", таким чином, пристрій зв'язується 2 рази кожні 4 хвилини, після першого з'єднання.
Друга спроба синхронізації	Інтервали, з якими пристрій повинен виходити на зв'язок із сервером після завершення "Перших спроб синхронізації"
Другий інтервал повторної спроби	Той самий принцип, що й для "Інтервалу першої спроби" - тільки тут він застосовується до "Других спроб синхронізації"
Регулярні спроби синхронізації	Інтервали, як часто пристрій повинен зв'язуватися з сервером у майбутньому За замовчуванням: "Нескінченно" Ми рекомендуємо не змінювати це значення, тому що якщо ви введете "10", пристрій зв'яжеться з сервером 10 разів, а потім зупиниться Таким чином, зв'язок з сервером AppTec360 буде розірвано!
Регулярний інтервал повторних спроб	Той самий принцип, що й для "Інтервал першої/другої спроби" - тільки тут застосовуються налаштування на майбутнє
Регулярний інтервал повторних спроб	Той самий принцип, що й для "Інтервал першої/другої спроби" - тільки тут застосовуються налаштування на майбутнє

ContentBox

Конфігурація

Тут ви можете налаштувати ContentBox. Ви можете розмістити файли для груп у ContentBox, до яких можна отримати доступ за допомогою програми ContentBox на пристрої.

Увімкнути ContentBox	Увімкнути ContentBox. Вимкнення цього параметра, якщо ви не використовуєте ContentBox, може заощадити ресурси на локальних машинах.
Використовуйте зовнішнє встановлення ContentBox	ContentBox також може працювати з вашим власним Nextcloud.
URL	Повна URL-адреса сутності Nextcloud
Root-користувач	Root-користувач облікового запису Nextcloud
Root Пароль	Root-пароль облікового запису Nextcloud
Типові права доступу до групових папок	Дозволи на групові папки за замовчуванням, можуть бути індивідуально змінені для кожної групи (у Мобільному управлінні)
Спільний доступ до папки групи з підгрупами	Якщо активовано, кожна підгрупа може читати всі папки основної групи, а також може бути індивідуально налаштована для кожної групи (Мобільне управління)
Дозволи для підгруп	Дозволи для підгруп можна налаштувати індивідуально для кожної групи (Mobile Management)
Дозволити спільний доступ	Дозволяє користувачеві ділитися контентом за допомогою посилань, може бути індивідуально налаштований для кожної групи
Максимальний розмір завантажуваного файлу в МБ	Максимальний розмір файлу Стандартний: 512 МБ Максимальна конфігурація: 2048
Облікові дані WebDAV	
URL-адреса WebDAV	Ви також можете відкрити ContentBox за допомогою WebDAV. Будь ласка, не видаляйте наступні папки за жодних обставин: /apptecgroups /apptecgroups/AppTecGroup-X
Root-користувач	Ім'я кореневого користувача
Пароль	Пароль Root-користувача

Синхронізація з ContentBox відбувається автоматично. Однак ви можете виконати синхронізацію вручну за допомогою "Синхронізувати ContentBox".

Крім того, тут ви можете активувати/деактивувати ContentBox на кожному окремому пристрої.

Це актуально лише в тому випадку, якщо ви не придбали додаткову ліцензію на ContentBox, тоді у вас все ще є доступ до 25 пристроїв, за допомогою яких ви можете протестувати ContentBox - тут ви можете активувати це для відповідних пристроїв.

Конфігурація LDAP

Огляд LDAP

Тут ви можете встановити з'єднання з Active Directory через LDAP для масового імпорту користувачів і груп. Синхронізація виконується вручну. Ви можете налаштувати декілька LDAP-з'єднань до різних систем або з різними конфігураціями/фільтрами.

Ім'я сервера	Відображення імені сервера
Тип	Наразі підтримуються лише активні каталоги, які підтримують LDAP
Домен LDAP	Основний домен LDAP (наприклад, example.com)
Хост LDAP	Необхідно лише в тому випадку, якщо хост LDAP недоступний в даному домені LDAP.
Порт	Залиште порожнім, щоб використовувати стандартний порт (389 або 636 для SSL)
Ім'я користувача	Наприклад, CN=John,OU=Users,DC=EXAMPLE,DC=COM Примітка: Більшість систем вимагають введення імені користувача у цьому форматі і не приймають "John" як ім'я користувача
Пароль	
Підтвердити пароль	
Безпека з'єднання	Примітка: при використанні SSL або TLS буде перевірено сертифікат Active Directory. Якщо він самопідписаний, вам потрібно додати кореневий центр сертифікації до сховища довіри на локальній машині. Якщо ви працюєте в хмарі, Active Directory має надати довірений сертифікат, інакше з'єднання працюватиме лише без шифрування
Автоматична синхронізація.	Вмикає автоматичну синхронізацію LDAP-каталогу з інтервалом часу, вказаним у загальних налаштуваннях LDAP.
Базовий DN	Якщо ви не хочете синхронізувати весь каталог, ви можете вказати OU тут, наприклад, OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Член	Всі імпортовані користувачі будуть додані до обраної групи
Тільки активовані користувачі?	Якщо увімкнено, буде враховано атрибут userAccountControl, користувачі без цього атрибуту не будуть імпортовані.

LDAP-фільтр	Ви можете використовувати LDAP-фільтр, щоб відфільтрувати користувачів, яких буде імпортовано
Регекс-фільтр	Ви можете використовувати Regex-фільтр, щоб відфільтрувати користувачів, яких буде імпортовано
Тестове підключення	Тестує з'єднання під час збереження конфігурації
Скинути структуру каталогів при синхронізації?	Якщо встановлено, всі записи LDAP будуть повернуті до їх початкового розташування у дереві LDAP. Рекомендується ввімкнути.
Повторний імпорт видалених користувачів і груп?	Якщо увімкнено, користувачі та групи, які були видалені, будуть відновлені. Рекомендується ввімкнути.
Видалення синхронізації?	Якщо увімкнено, групи і користувачі будуть видалятися, коли їх буде видалено на LDAP-сервері. Також буде видалено пристрої видалених користувачів.

Під списком ваших конфігурацій LDAP ви можете визначити період, через який система буде автоматично синхронізуватися. Для автоматичної синхронізації використовуються лише ті конфігурації LDAP, у яких активовано відповідну опцію.

Керування додатками

Внутрішня база даних додатків

Android

Тут ви можете завантажити додатки для Android, які розробила ваша компанія, і поширювати їх пізніше в Мобільному управлінні в профілях пристроїв або груп.

Зверніть увагу, що ми рекомендуємо розповсюджувати таким чином лише ті програми, які не доступні в Google Play Маркеті.

Натисніть на "+", щоб завантажити APK програми, яку ви хочете завантажити. Наразі підтримується лише формат APK.

Ліміт завантаження на локальних пристроях можна збільшити на кроці 3 конфігурації пристрою. Якщо ви хочете збільшити ліміт завантаження у хмарі, зверніться до служби підтримки для отримання додаткової інформації.

Майте на увазі, що зазвичай APK-файли мають трохи менший розмір, ніж їхній вміст. Можливо, через це завантаження не вдасться, оскільки APK розпаковується в процесі. Наприклад, може статися так, що APK розміром 95 МБ не вдасться завантажити при ліміті на завантаження 100 МБ. У цьому випадку збільште ліміт завантаження, як зазначено вище.

Ми також радимо спочатку вручну перенести APK на один тестовий пристрій (наприклад, через USB) і спробувати встановити його вручну за допомогою програми "Файли" на цьому пристрої. Якщо це з якихось причин не спрацює, то через MDM також не вдасться.

Оновити ціль

За допомогою функції "Мета оновлення" ви можете вибрати, яку версію програми слід встановити або до якої версії слід оновити програму, якщо ви активували функцію "Оновлення" для програми.

Якщо ви не вибрали ціль оновлення, буде використано найновішу версію.

Майте на увазі, що Android не може понижувати версії програм. Також майте на увазі, що "Код версії" визначає, чи є версія вищою, нижчою або такою ж самою. Тому переконайтеся, що ви правильно збільшили цю версію у вашому додатку під час створення оновлення.

iOS

Тут ви можете завантажити розроблені вами додатки для iOS і поширювати їх пізніше в Мобільному управлінні на вашому пристрої або в профілі групи.

Натисніть на "+", щоб завантажити IPA додатку, який ви хочете завантажити. Наразі підтримується лише формат IPA.

Ліміт завантаження на локальних пристроях можна збільшити на кроці 3 конфігурації пристрою. Якщо ви хочете збільшити ліміт завантаження у хмарі, зверніться до служби підтримки для отримання додаткової інформації.

Оновити ціль

За допомогою функції "Мета оновлення" ви можете вибрати, яку версію програми слід встановити або до якої версії слід оновити програму, якщо ви активували функцію "Оновлення" для програми.

Якщо ви не вибрали ціль оновлення, буде використано найновішу версію.

MacOS

Тут ви можете завантажити програми для MacOS, які ви розробили, і поширювати їх пізніше в "Мобільному управлінні" у профілі вашого пристрою або групи.

Натисніть на "+", щоб завантажити PKG програми, яку ви хочете завантажити. Наразі підтримується лише формат PKG.

Ліміт завантаження на локальних пристроях можна збільшити на кроці 3 конфігурації пристрою. Якщо ви хочете збільшити ліміт завантаження у хмарі, зверніться до служби підтримки для отримання додаткової інформації.

Оновити ціль

За допомогою функції "Мета оновлення" ви можете вибрати, яку версію програми слід встановити або до якої версії слід оновити програму, якщо ви активували функцію "Оновлення" для програми.

Якщо ви не вибрали ціль оновлення, буде використано найновішу версію.

Windows 10

Тут ви можете завантажити програми для Windows 10 і поширювати їх пізніше в Мобільному управлінні на своєму пристрої або в профілі групи.

Натисніть на "+", щоб завантажити APPX, APPXBUNDLE або MSI програми, яку ви хочете завантажити. Наразі підтримується лише формат APPX, APPXBUNDLE або MSI.

Ви також можете завантажити і визначити залежності для програми, які будуть автоматично поширюватися і встановлюватися перед встановленням потрібної програми.

Ліміт завантаження на локальних пристроях можна збільшити на кроці 3 конфігурації пристрою. Якщо ви хочете збільшити ліміт завантаження у хмарі, зверніться до служби підтримки для отримання додаткової інформації.

Оновити ціль

За допомогою функції "Мета оновлення" ви можете вибрати, яку версію програми слід встановити або до якої версії слід оновити програму, якщо ви активували функцію "Оновлення" для програми.

Якщо ви не вибрали ціль оновлення, буде використано найновішу версію.

Win32 Пакет (.exe)

Ви також можете розповсюджувати .exe-файли/інсталятори на ваші пристрої.

Назва пакета	Ім'я, яке буде відображатися в MDM
Опис	Опис, показаний в MDM
Файл пакету	Допускаються лише файли .zip. Помістіть файли, які ви хочете розгорнути, у цей zip-архів.
Контекст розгортання	**Система**: Команда install виконується з системними привілеями, які є вищими, ніж "Користувач". Також при використанні "System" процес не має інтерфейсу користувача, тому він буде беззвучним, а профіль користувача, наприклад, змінні оточення, такі як %AppDat%, будуть недоступні. **Користувач**: Команда install має доступ до профілю користувача і за необхідності може відобразити інтерфейс користувача. Примітка: Деякі процеси можуть працювати лише в одному контексті. Наприклад, якщо програма встановлює себе у AppData, вона працюватиме лише при виборі "Користувач"
Команда встановлення	Команда, яка використовується для встановлення програми. Наприклад, команда встановлення для zip-файлу, що містить "setup.exe" у корені, який підтримує параметр "/s", для тихого встановлення команда встановлення буде "setup.exe /s". Зауважте, що різні програми можуть мати різні параметри.
Команда видалення	Команда, яку слід запустити для видалення програмного забезпечення через MDM. Зазвичай вказує на програму видалення. Наприклад, "C:\Program Files\ExampleSoftware\uninstall.exe".
Вимоги	
Примітка: Для встановлення програмного забезпечення необхідно виконати всі встановлені вимоги. В іншому випадку його не буде встановлено. Деякі поля можуть бути обов'язковими. Якщо для вимоги не встановлено жодного значення, вимогу буде проігноровано.	
Архітектура ОС	Архітектура ОС
Мінімальна версія ОС	Мінімальна версія ОС
Мінімальний обсяг вільного місця на диску (МБ)	Мінімальний обсяг вільного місця на диску (МБ)
Мінімальна фізична пам'ять (МБ)	Мінімальна фізична пам'ять (МБ)

Мінімальна кількість логічних процесорів	Мінімальна кількість логічних процесорів
Мінімальна частота процесора (МГц)	Мінімальна частота процесора (МГц)
Додаткові вимоги	Ви також можете вручну визначити правила або завантажити скрипт для виконання додаткових перевірок, якщо хочете.
Правила виявлення	
Метод виявлення	Тут ви можете вказати, як визначати, чи встановлено програму на пристрої. Команди встановлення будуть виконуватися лише тоді, коли ці правила виявлять, що програму НЕ встановлено. Команди видалення виконуватимуться лише тоді, коли ці правила визначать, що програму не встановлено. **Визначити правила вручну**: Дозволяє вам вручну визначити одне або декілька правил для перевірки, наприклад, наявності певного файлу, теки, MSI або ключа реєстру. Якщо всі вказані правила перевірки відповідають дійсності, програма вважатиметься встановленою. **Використовувати скрипт**: Завантажте власний скрипт з вашими власними перевірками. Якщо скрипт повертає "$TRUE", програма буде вважатися присутньою.
Правила виявлення	

Налаштування програми

Налаштування програми для iOS

Тут ви можете визначити налаштування за замовчуванням для додавання програми до обов'язкових додатків або корпоративного магазину додатків.

Примітка: Це лише налаштування того, що буде вибрано за замовчуванням під час додавання програм. Це НЕ змінює існуючі налаштування для програм, які вже додано до обов'язкових програм або корпоративної крамниці програм.

Будьте в курсі подій	Автоматично підтримує додаток в актуальному стані. Будь ласка, зауважте, що після виходу оновлення може пройти до 7 днів, перш ніж додаток оновиться.
Обганяють, коли некеровані	Якщо додаток вже встановлено як некерований (користувачем), він буде перехоплений і керований MDM.
Видалення програми після видалення профілю MDM	Видаляє програму після видалення MDM.
Заборонити резервне копіювання даних програми	Перешкоджає резервному копіюванню даних програми.

Налаштування програми для Android

Тут ви можете визначити налаштування за замовчуванням для додавання програми до обов'язкових додатків або корпоративного магазину додатків.

Примітка: Це лише налаштування того, що буде вибрано за замовчуванням під час додавання. Це НЕ змінює налаштування програм, які вже додано до обов'язкових програм або корпоративної крамниці програм.

Будьте в курсі подій	Автоматично оновлює додаток. Доступно лише для власних додатків.
Контрольоване оновлення клієнта AppTec360 EMM	Якщо увімкнено, адміністратори можуть вказати ціль оновлення для клієнта AppTec360 EMM. Список всіх доступних версій AppTec360 EMM Client буде показано в "Загальні налаштування" → "Керування додатками" → "Внутрішня база даних додатків" → "Android".

Сторонні додатки

Android

Тут ви можете встановити код активації для Ikarus.

Встановіть значення "Використовувати код активації" і введіть свій код активації тут.

Примітка: Після введення та збереження коду, він ще не буде доданий до профілю, який буде надіслано на пристрій. Для того, щоб код було додано до профілю, вам потрібно виконати будь-які зміни у вашому профілі. Наприклад, змінити будь-який перемикач у профілі з вимкнено → увімкнено → вимкнено - Зберегти → Призначити зараз.

iOS

Тут ви можете ввести вашу ліцензію SecurePIM. Після введення ліцензії натисніть "Зберегти зміни" і ви зможете користуватися опціями SecurePIM.

VPP / KNOX Premium

Програма Apple Volume Purchase Program (VPP) дозволяє вам легко розповсюджувати платні та безкоштовні додатки на ваших пристроях. Це дуже рекомендується, оскільки вам не потрібен Apple ID на пристроях, користувачам не потрібно підтверджувати встановлення (під контролем), користувачам не потрібно вводити пароль Apple ID, і ви можете легко розповсюджувати платні програми, не купуючи їх знову на кожен пристрій.

Щоб користуватися VPP, вам потрібно зареєструватися в Apple Business Manager.

Ліцензії VPP

Тут ви можете отримати огляд ваших додатків VPP, дізнатися, скільки ліцензій використовується і скільки з них доступні.

Натиснувши на коліщатко, ви побачите, яким пристроям призначено ліцензію і який статус цього призначення.

Натискання на кнопку оновлює кеш VPP, який порівнює ліцензії, призначені в MDM, з ліцензіями, призначеними на стороні Apple. У деяких випадках це може вирішити проблеми з ліцензіями.

Токен VPP

Тут ви можете завантажити свій токен VPP, який можна знайти в Apple Business Manager у розділі "Налаштування" → "Програми та книги". Ви можете завантажити кілька токенів VPP.

Ви можете поновити Токен, просто завантаживши новий в Apple Business Manager, натиснувши на колесо "Редагувати" і завантаживши новий.

Режим VPP визначає, як буде оброблятися призначення ліцензії. Залежно від вашого сценарію, вам доведеться використовувати різні режими:

"На основі пристрою" слід використовувати при реєстрації пристроїв за допомогою QR-коду, посилання, Apple Configurator або DEP.

"На основі користувача" потрібно, якщо Пристрої зареєстровано за допомогою реєстрації користувача або як спільний iPad.

Якщо ви ввімкнули "Автоматизоване керування ліцензіями", користувачам, яких переміщено з однієї групи до іншої, буде автоматично призначено ліцензії Apple VPP на основі профілю групи, до якої їх також переміщено.

Існуючі ліцензії Apple VPP від групи, з якої вони перейшли, не будуть відкликані.

Новим користувачам, доданим до групи, будуть автоматично призначені ліцензії Apple VPP на основі профілю відповідної групи.

KNOX Premium Key

Тут ви можете ввести свій ключ KNOX Premium Key для використання Samsung KNOX Container.

Зверніть увагу, що ця функція більше не підтримується, починаючи з Android 10. Замість цього використовуйте Android Enterprise Container.

Налаштування App Store

Регіон та мова

Тут ви можете встановити мову та регіон за замовчуванням для пошуку додатків у Керуванні додатками.

Зверніть увагу, що налаштування iTunes також визначають, як система отримує інформацію про певні програми. Якщо у вашому списку є програми, які відображаються у дивний спосіб (наприклад, відсутня піктограма), можливо, ви встановили регіон, в якому певна програма недоступна.

AE Play Store

Тут ви можете знайти всі параметри Play Store для корпоративних пристроїв Android, щоб затверджувати додатки, завантажувати власні додатки до Play Store або створювати власні веб-додатки.

Схвалені програми

Тут ви можете отримати огляд усіх програм, які ви схвалили.

Додатки Play Store

Це призведе до завантаження iFrame із зображенням Play Store. Знайдіть потрібний додаток, натисніть на нього та затвердьте. Під час схвалення програми ви також можете вказати, що схвалення буде скасовано, якщо дозволи буде змінено. Ми рекомендуємо залишати ці налаштування за замовчуванням при затвердженні додатків.

Після того, як додаток буде схвалено, ви можете додати його до своїх профілів.

Після затвердження кнопка "Затвердити" зміниться на "Відкликати затвердження", тому ви завжди можете видалити додатки, якщо вони вам більше не потрібні.

Приватні додатки

Тут ви можете завантажити власний додаток як приватний додаток до Google Play Store. Це дозволить вам поширювати додаток через Сервіси Google і оновлювати його через них. Це також має ту перевагу, що ваші власні додатки можуть бути встановлені без підтвердження користувача, яке зазвичай є необхідним.

Веб-додатки

Тут ви можете створювати веб-програми, які є посиланнями на певні веб-сторінки, які можна призначити як програми.

Ви також можете створити власну піктограму і визначити, як саме вона буде відображатися.

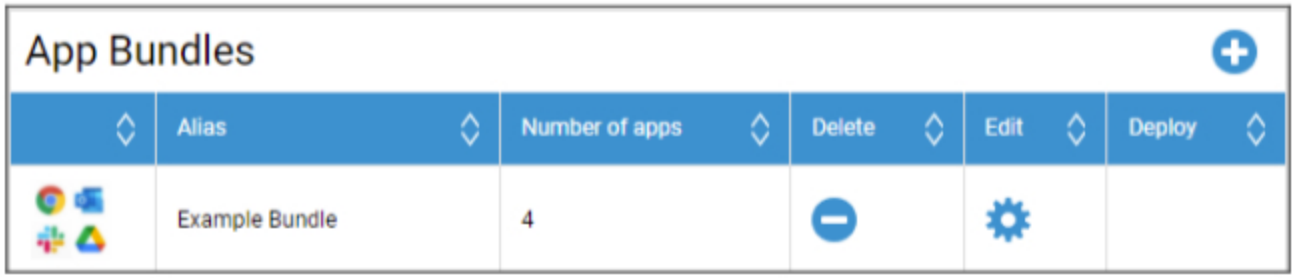
Макет магазину

Макет магазину визначає, як програми відображатимуться в Play Маркеті і чи відображатимуться взагалі.

Майте на увазі, якщо ви хочете показувати додатки в Play Store, щоб користувач міг встановити їх вручну, їх потрібно додати тут, у макеті **I** у профілі до Enterprise Play Store. Якщо ви додасте програму лише до одного з них, вона не відображатиметься.

Пакет додатків

За допомогою пакетів програм ви можете визначити групи програм, які можна призначити профілям пристроїв або груп одним клацанням миші.



Натисніть на "+", щоб створити новий Пакет додатків. Після створення пакету програм ви можете натиснути "Редагувати", щоб додати до нього програми з різних джерел.

Пакет можна додати до профілю так само, як і будь-яку іншу програму. При додаванні додатків у вас з'явиться додаткова вкладка "Пакети додатків", де ви зможете знайти свої пакети.

Якщо ви вносите будь-які зміни до пакету додатків, у колонці "Розгорнути" з'явиться кнопка "Розгорнути". Це дозволить вам застосувати ці зміни до всіх профілів, що містять цей пакет. Майте на увазі, що вам доведеться робити це вручну після додавання або видалення програм у пакеті.

Пульт дистанційного керування

TeamViewer

Конектор TeamViewer

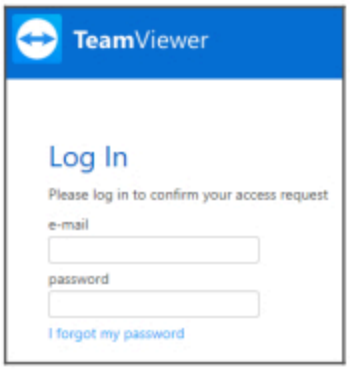
Примітка: Під час безкоштовної пробної версії нашої хмарної версії ви не можете підключити свій обліковий запис TeamViewer. Замість цього вам буде автоматично підключено безкоштовний демо-рахунок.

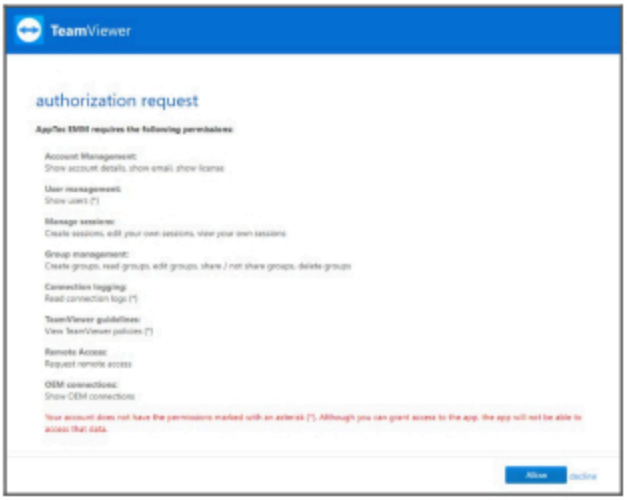
Перейдіть до Загальних налаштувань -> Пульт дистанційного керування -> TeamViewer. Тут ви можете зв'язати свій обліковий запис TeamViewer з консоллю або переглянути інформацію про поточний підключений обліковий запис. Також ви можете переглянути всі поточні активні сеанси, якщо перейдете до розділу "Активні сеанси".

Щоб прив'язати свій обліковий запис, натисніть "Почати налаштування".

Після цього ви потрапите на нову сторінку, де вам потрібно буде увійти за допомогою свого облікового запису TeamViewer.

Після входу ви дозволите AppTec360 MDM використовувати цей обліковий запис. Після підтвердження вам потрібно почекати кілька секунд, і обліковий запис буде підключено.


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


TeamViewer
authorization request

Інсталяція TeamViewer QuickSupport

Додайте додаток "TeamViewer QuickSupport" до обов'язкових додатків вашого профілю пристрою або профілю групи і натисніть "Призначити зараз". Зачекайте, поки додаток буде встановлено на пристрої.

Якщо ви спробуєте отримати доступ до пристрою, на якому програма не встановлена, її буде встановлено або з'явиться запит на встановлення, залежно від конфігурації пристрою.

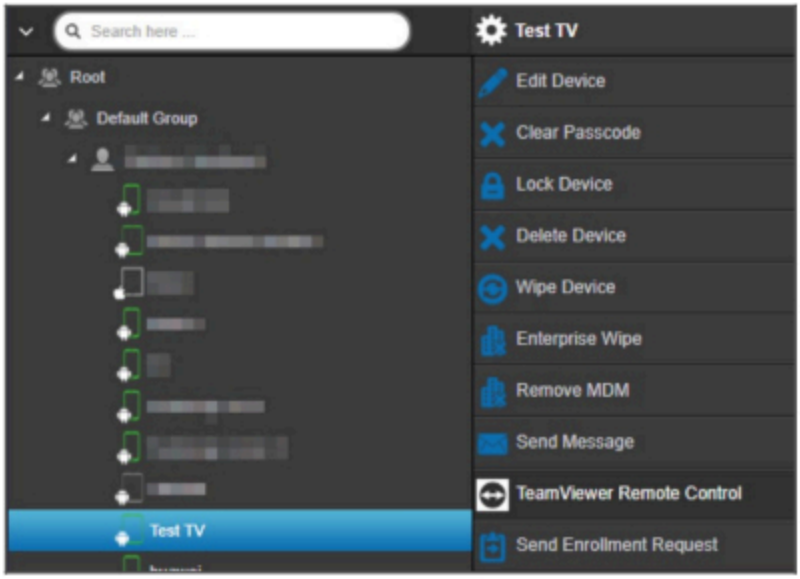
Дистанційне керування пристроєм

Щоб дистанційно керувати пристроєм, виберіть пристрій, натисніть на коліщатко і виберіть "Дистанційне керування TeamViewer"

Якщо вже існує активна сесія, ви можете використовувати стару сесію або створити нову.

Підтвердіть, що ви хочете створити новий сеанс TeamViewer.

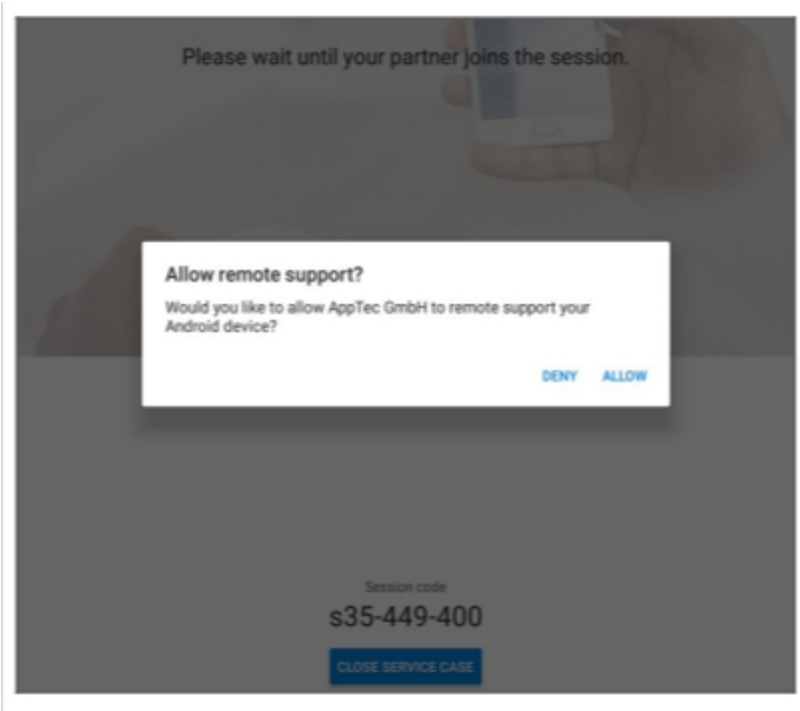
Через кілька секунд ви отримаєте посилання на сеанс TeamViewer. Ви можете натиснути на кнопку "Почати", щоб відкрити це посилання в новому вікні.


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

За цим посиланням відкриється встановлений TeamViewer і з'єднає вас з вашим пристроєм.

Тепер вам потрібно підтвердити з'єднання на самому пристрої, щоб дистанційно керувати ним.

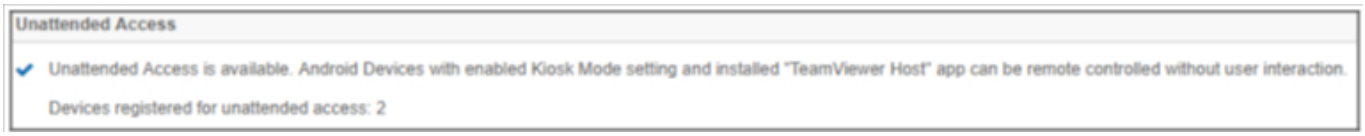


Якщо ви використовуєте iOS, ви отримаєте повідомлення в клієнті AppTec360 MDM. За цим посиланням пристрій приєднається до віддаленого сеансу. Залежно від налаштувань сповіщень на пристрої, можливо, ви не отримаєте сповіщення і вам доведеться відкрити клієнт AppTec360 MDM вручну.

На деяких пристроях Android (наприклад, Samsung) потрібно встановити додатковий додаток як аддон. Додаток TeamViewer на пристрої повідомить вас про це, якщо це необхідно на вашому пристрої.

Доступ без нагляду

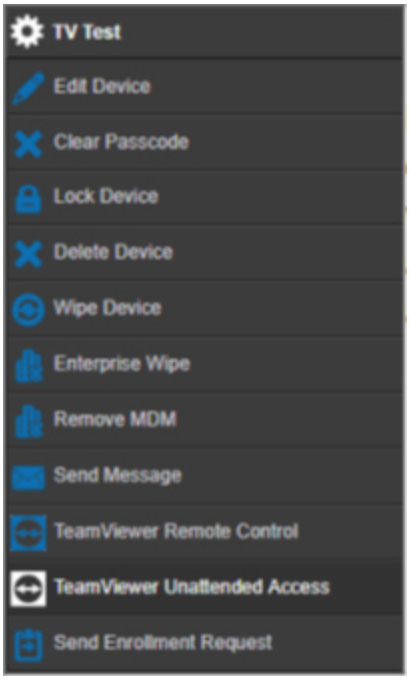
Примітка: Безконтрольний доступ можливий лише на пристроях Android.



Ви можете підключатися до пристроїв, не приймаючи з'єднання на пристрої, тільки якщо ваш обліковий запис TeamViewer використовує ліцензію "Тензор" або "Корпоративну".

Перевірити це можна після прив'язки облікового запису в "Загальних налаштуваннях"

Для того, щоб користуватися доступом без нагляду, вам потрібно встановити додаток "TeamViewer Host" та активувати "Enable Unattended Access" у розділі "Kiosk Mode & Launcher" у вашому профілі. Будь ласка, зверніть увагу, що це можливо, тільки якщо ви використовуєте режим кіоску.



Тепер ви можете вибрати автоматичний доступ, вибравши свій пристрій і натиснувши на коліщатко. Це з'єднає вас з вашим пристроєм без необхідності підтвердження на самому пристрої. Будь ласка, зауважте, що це може зайняти деякий час, поки ви отримаєте посилання для доступу до вашого пристрою.

Splashtop

Якщо ви ввімкнули опцію Splashtop, ви побачите параметри конфігурації Splashtop у ваших профілях.

Щоб використовувати Splashtop, вам потрібно встановити Splashtop Streamer (com.splashtop.streamer.csrs) як обов'язковий додаток у вашому профілі. Після цього ви можете увімкнути конфігурацію Splashtop у вашому профілі в розділі "Пульт дистанційного керування". Це дозволить налаштувати додаток Splashtop Streamer. Якщо ви використовуєте Splashtop Streamer, але не в поєднанні з MDM, вам слід залишити цю опцію вимкненою.

У вашому профілі в розділі "Пульт дистанційного керування" ви також маєте встановити код розгортання. Перейдіть на https://my.splashtop.com і увійдіть у свій обліковий запис Splashtop. Натисніть "Додати комп'ютер" і скопіюйте 12-значний код розгортання зі сторінки, що з'явиться.

Без коду розгортання дистанційне керування НЕ можливе.

Після цього ви можете клацнути правою кнопкою миші на своєму пристрої та розпочати віддалений сеанс, натиснувши "Дистанційне керування Splashtop"

Керування сім-картками

Масовий імпорт CSV

Тут відображається огляд призначених вам SIM-карт і вся інформація про них. Це допоможе вам мати всю інформацію не тільки про ваші пристрої, але й про ваші SIM-картки в одній системі.

ПРИМІТКА: Це ручне управління/документування. Неможливо отримати ці дані автоматично з пристроїв через механізми конфіденційності/безпеки операційних систем.

Ви також можете експортувати та імпортувати цей список у форматі CSV.

Перевізник і тариф

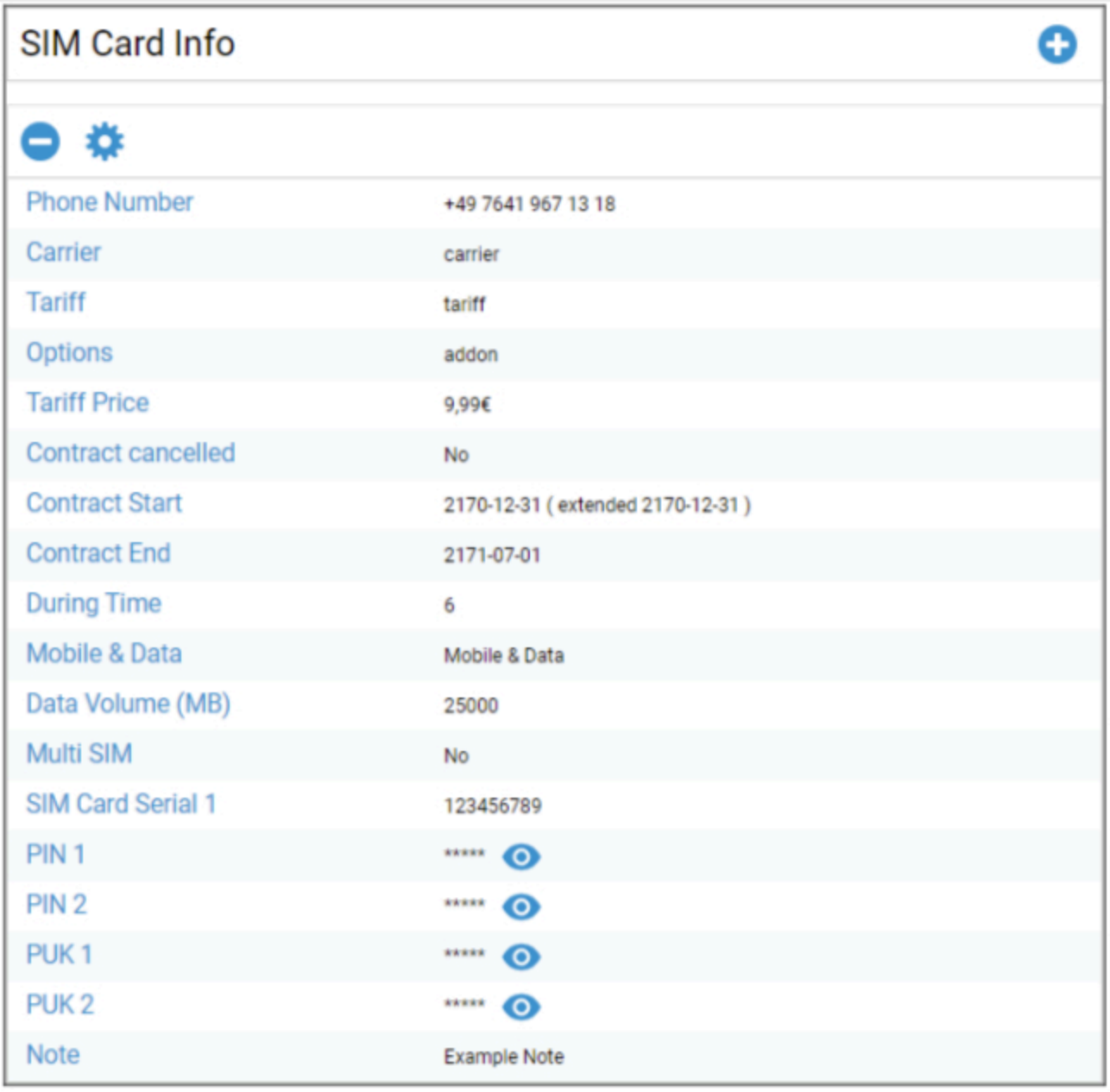
Щоб додати Sim-карту, спочатку натисніть на кнопку , щоб додати одного або декількох операторів.

Після цього натисніть на "+" в розділі "Інформація про тарифи", щоб додати тариф до перевізника.

Якщо у вас є щось подібне, ви можете додати опціональні доповнення нижче, якщо у вас є щось подібне.

Це підготувало все необхідне для додавання фактичної SIM-карти. Наразі Sim-картки призначені Користувачеві. Тому перейдіть до Керування мобільними пристроями, виберіть Користувача і перейдіть до "Огляд SIM-карт.

Тут ви бачите сім-карти цього користувача. Якщо вона є, ви можете відредагувати або видалити її. Користувачі можуть мати кілька Sim-карт.

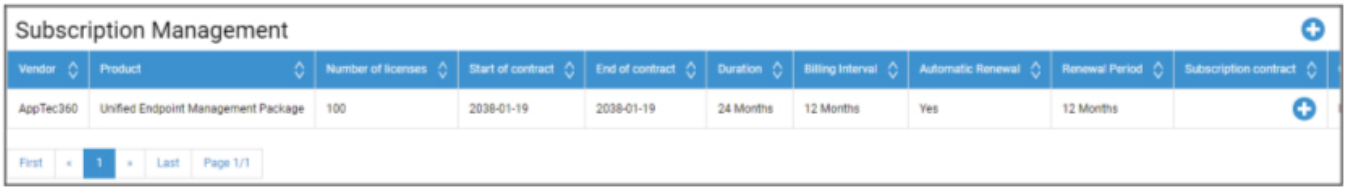


Натисніть на "+", щоб додати Sim-карту і додайте всю необхідну інформацію. Ці сім-карти також будуть перераховані в списку всіх ваших сім-карт у Загальних налаштуваннях → Керування сім-картами.

Керування підпискою

Керування підпискою

Тут ви можете документувати поточні підписки, їхні деталі, а також зберігати різні файли, наприклад, підписаний договір, лист про розірвання тощо. Ви також можете налаштувати нагадування, які нагадуватимуть вам на пошту перед закінченням підписки і, можливо, автоматично продовжуватимуть її.



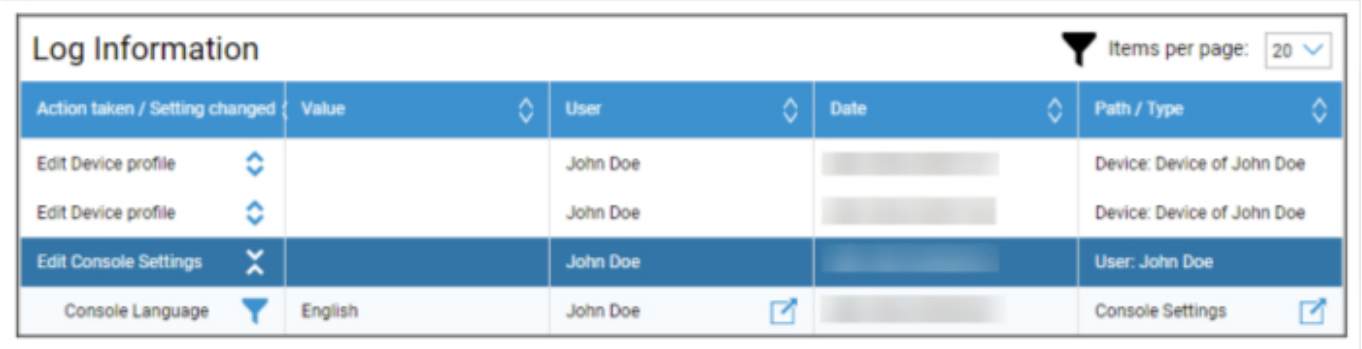
Натисніть на "+" вгорі, щоб додати підписку. Ви можете додати стільки підписок, скільки хочете.

Натисніть на "+" у різних полях, щоб завантажити файли, що стосуються цієї підписки. Технічно ви можете завантажити будь-який тип файлів, але майте на увазі, що не всі типи файлів можна попередньо переглянути в браузері.

Загальний журнал аудиту

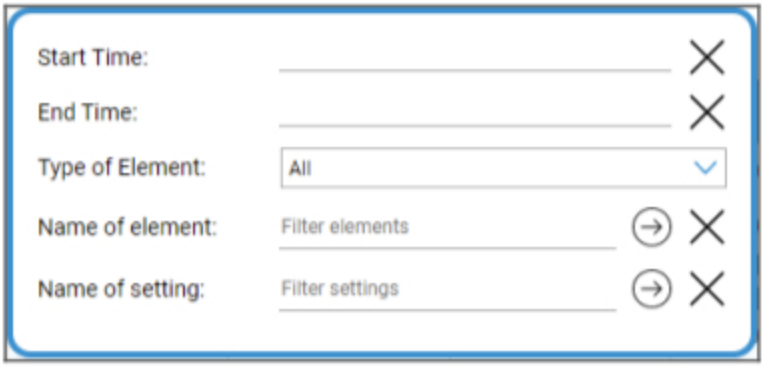
Журнал аудиту

Тут ви бачите загальний журнал аудиту, який показує всі внесені зміни. У той час як журнал аудиту користувача або групи показує лише зміни, що стосуються цього користувача або групи, цей журнал показує КОЖНУ зміну, зроблену будь-де в консолі.



Ви можете побачити, що було змінено, ким, коли і де. У деяких випадках ви також можете розгорнути запис, щоб побачити більше деталей.

Можна натиснути на користувача або на запис у полі "Шлях / Тип", щоб перейти до місця, де було зроблено зміну.



У верхньому правому куті ви також можете визначити фільтр, який може допомогти знайти певні зміни в середовищі, де відбувається багато змін.

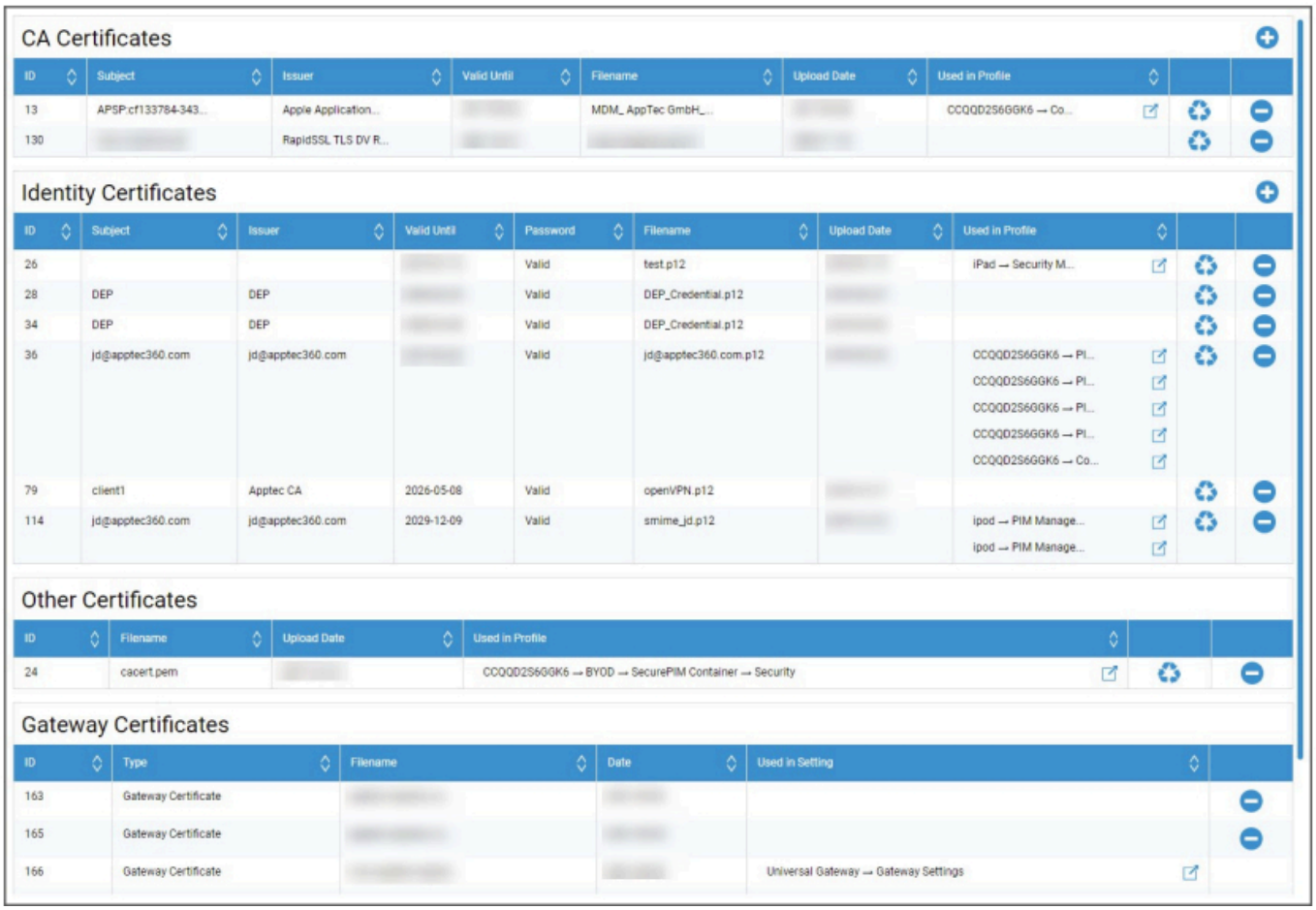
Налаштування журналу аудиту

"Період зберігання журналів аудиту" визначає, як довго слід зберігати журнали аудиту перед видаленням.

Управління сертифікатами

Тут ви отримаєте огляд усіх сертифікатів, завантажених і використовуваних в консолі. Це лише огляд. Фактична конфігурація, наприклад, сертифікатів Wi-Fi, як і раніше, виконується в профілі у відповідному місці.

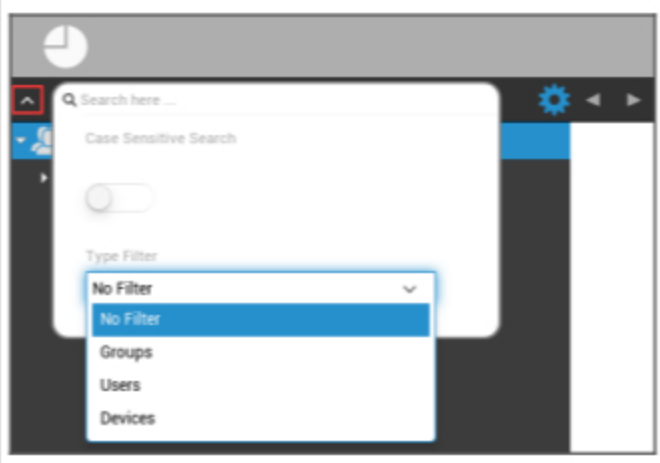
Тут ви також можете видалити або оновити сертифікати, що буде автоматично відображено у відповідних профілях. Натисніть на інформацію в розділі "Використовується в профілі", щоб побачити, де саме все ще призначено сертифікат.



Мобільне управління

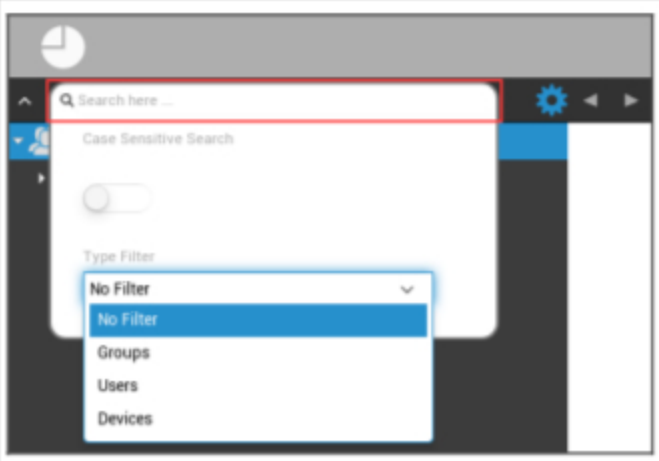
Екран мобільного керування

Фільтр пристрою



Клікнувши у верхньому лівому кутку екрана, ви можете знайти різноманітні фільтри для відображення пристроїв.

Вікно пошуку



Вікно пошуку дозволяє шукати всі пристрої та/або користувачів за певним ключовим словом.

Додаткове обладнання

Після натискання на відповідний символ з'явиться список варіантів, які вам доступні.

Вони змінюються з кожним поточним вікном і пояснюються у відповідних розділах.

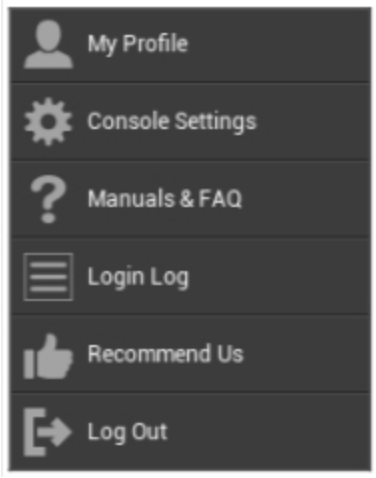
Навігаційні стрілки

Натиснувши на стрілку вліво, ви перейдете на попередню сторінку.

Після цього, натиснувши на стрілку вправо, ви потрапите на сторінку, з якої щойно вийшли.

Налаштування облікового запису адміністратора

Натиснувши на адресу електронної пошти, як показано вище, ви побачите наступне меню:



Мій профіль	Відредагуйте дані облікового запису адміністратора
Налаштування консолі	Налаштування параметрів консолі для облікового запису Адміністратора
Посібники та поширені запитання	Перегляньте сторінку "Посібники та поширені запитання" в розділі "Загальні налаштування"
Вхід в систему	Доступ до "Журналу входу"
Рекомендуйте нас	Перегляньте сторінку "Рекомендувати нас" в "Загальних налаштуваннях"
Вийти з системи	Вийдіть з консолі MDM

Інформація про користувача

Тут ви можете редагувати дані облікового запису поточного адміністратора.

Ім'я користувача	Ім'я користувача та/або адреса електронної пошти облікового запису
Ім'я	Ім'я адміністратора
Прізвище	Прізвище адміністратора
Ім'я користувача Ім'я користувача	Ім'я для входу адміністратора
Адреса електронної пошти	Адреса електронної пошти адміністраторів
Альтернативна адреса електронної пошти	Альтернативна адреса електронної пошти адміністраторів
Зображення	Зображення профілю
Номер телефону	Номер телефону адміністратора
Номер мобільного телефону	Номер мобільного адміністратора
Внутрішній номер телефону	Внутрішній номер телефону
Місцезнаходження	Місцезнаходження
Посада	Посада в компанії
Група користувачів	Виберіть, якій групі користувачів ви хочете призначити обліковий запис адміністратора
Коментар	Введіть коментар
Введіть новий пароль	Введіть пароль для зміни пароля
Повторіть новий пароль	Повторіть новий пароль для підтвердження

Зверніть увагу, що доступ до адміністрування також може бути поданий як локальний обліковий запис користувача в структурі ієрархії. Без створення додаткового адміністратора цей обліковий запис не можна видаляти!

Налаштування консолі

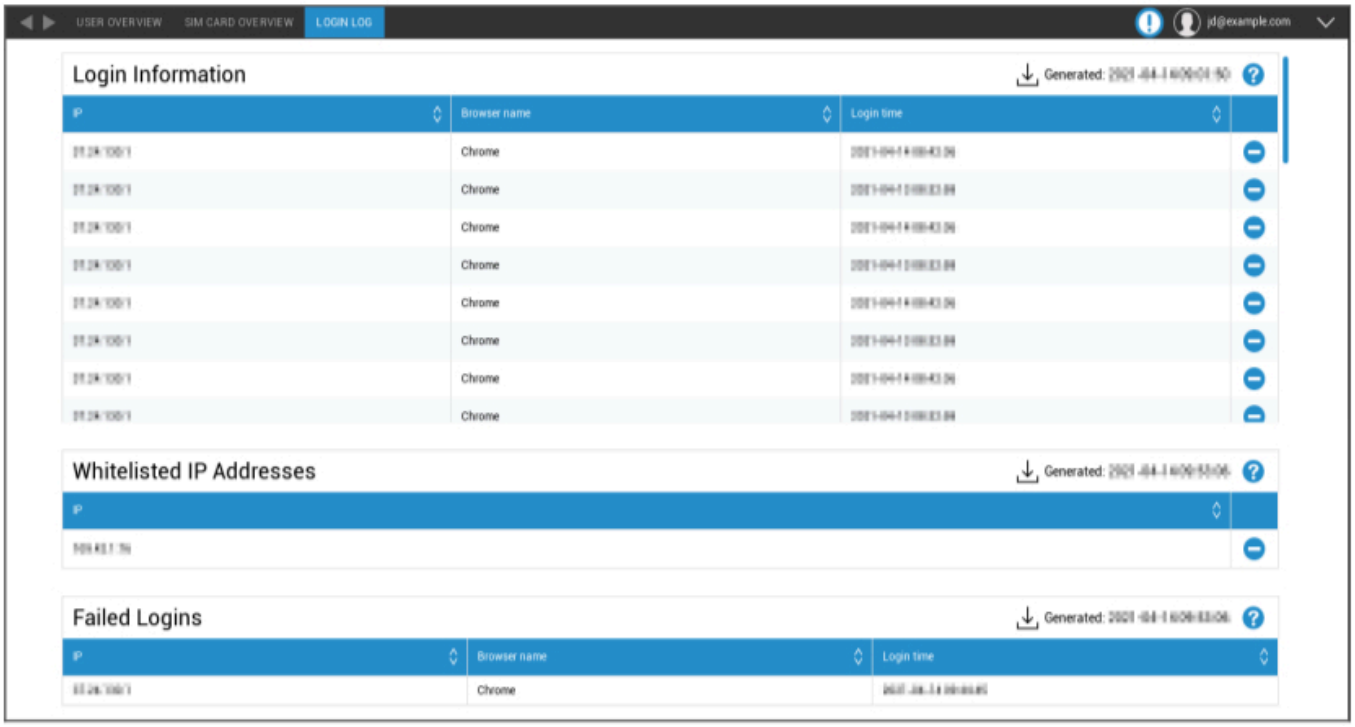
Тут ви можете налаштувати наступні параметри консолі для облікового запису адміністратора:

Параметри відображення користувача каталогу	Визначте, як користувачі повинні бути позначені в дереві
Параметри відображення пристроїв каталогу	Визначте, як пристрої мають бути позначені в дереві
Тайм-аут сеансу	Якщо користувач нічого не зробить протягом зазначеного часу, він вийде з системи. Значення за замовчуванням - 60 хвилин. Будь ласка, вийдіть і увійдіть знову після зміни цього налаштування.
Часовий пояс	Виберіть часовий пояс, який використовується
Формат часу	Виберіть спосіб відображення міток часу
Мова консолі	Виберіть мову, якою має відображатися консоль. Доступні англійська та німецька мови.
Основний колір	Ви можете задати колір, який буде використовуватися як основа для колірної схеми консолі. Ви можете скористатися палітрою кольорів або ввести колір у HTML HEX-нотації. RGB-форматори, такі як "рожевий", "жовтий", також працюють.
Зберегти команду	Комбінація клавіш для запуску збереження без натискання кнопки "Зберегти".
Використовуйте двофакторну автентифікацію	Увімкніть використання двофакторної автентифікації при вході в систему. Після входу ви отримаєте електронного листа з кодом, який потрібно буде ввести для входу.
Тайм-аут двофакторної автентифікації	Встановіть період часу, протягом якого не буде запитуватися двофакторна автентифікація після вже успішної автентифікації.
Надішліть код підтвердження через	Код підтвердження буде надіслано на вибрані опції. Повідомлення пристрою буде показано в додатку AppTec360 MDM на всіх пристроях Android та iOS, які вам належать.
Надіслати повідомлення після входу в систему	Якщо увімкнено, при кожному вході з IP-адреси, яка не входить до білого списку, буде надіслано електронний лист.

	В електронному листі міститься інформація про вхід в систему (наприклад, IP, браузер).

Вхід в систему

Тут ви можете побачити інформацію про логіни поточного облікового запису адміністратора.



Інформація для входу	Список, що містить логіни поточного облікового запису адміністратора, які було записано консоллю. Цей список показує всі ваші успішні входи за останні 30 днів.
Білі списки IP-адрес	Це список усіх ваших білих IP-адрес. Якщо ви ввійдете з IP-адреси, яка вказана тут, ви не отримаєте повідомлення про вхід. Ви можете додати IP-адресу до цього списку, натиснувши на кнопку поруч із записом у списку "Інформація для входу" вище. Ви можете видалити IP-адресу з цього списку, натиснувши на кнопку поруч із записом у цьому списку або у списку "Інформація для входу" вище.
Невдалі входи	Це список всіх невдалих спроб входу за останні 30 днів. Якщо ви не змогли ввести правильний пароль принаймні 3 рази протягом 20 хвилин, запис з'явиться в цьому списку. Про невдалі спроби входу ви також будете поінформовані електронною поштою.

Корпоративне адміністрування (Root-Node) в мобільному управлінні

Коли ви досягли кореневого вузла (перша група), ви можете виконати різноманітні налаштування для вашої компанії, що стосуються управління мобільними пристроями.

Створити підгрупу	Створити підгрупу
Перейменувати кореневий вузол	Перейменування кореневого вузла (наприклад, назва вашої компанії)
Масовий набір на навчання	Одночасна реєстрація декількох пристроїв/користувачів
Масове призначення	Призначте профіль для відповідних груп, одним поглядом
Швидке адміністрування додатків	Надсилайте запити на (Видалення) встановлення програми на пристрої відповідних груп
Імпорт користувачів у форматі CSV	Імпортувати користувачів з CSV у відповідну групу

Створити підгрупу

За допомогою кнопки "Створити підгрупу" ви можете створити додаткову підгрупу.

Ви можете визначити, до якої групи слід віднести підгрупу.

(За замовчуванням створюється нова група, яка призначається як підгрупа у кореневому вузлі)

Перейменувати кореневий вузол

Тут ви можете перейменувати своє кореневе ім'я. Зазвичай у цьому випадку використовується назва компанії.

Масовий набір на навчання

За допомогою функції "Масова реєстрація" ви можете зареєструвати кілька пристроїв і користувачів.

Ви можете безпосередньо вибрати спосіб, у який користувач повинен отримати повідомлення про реєстрацію (електронна пошта; альтернативна електронна пошта; SMS)

Залежно від того, який пристрій збирається отримати користувач (iOS, Android, Windows Phone), ви можете безпосередньо позначити це тут.

Тут також можна налаштувати різницю між смартфоном і планшетом, яку потрібно буде правильно вибрати, поставивши галочку.

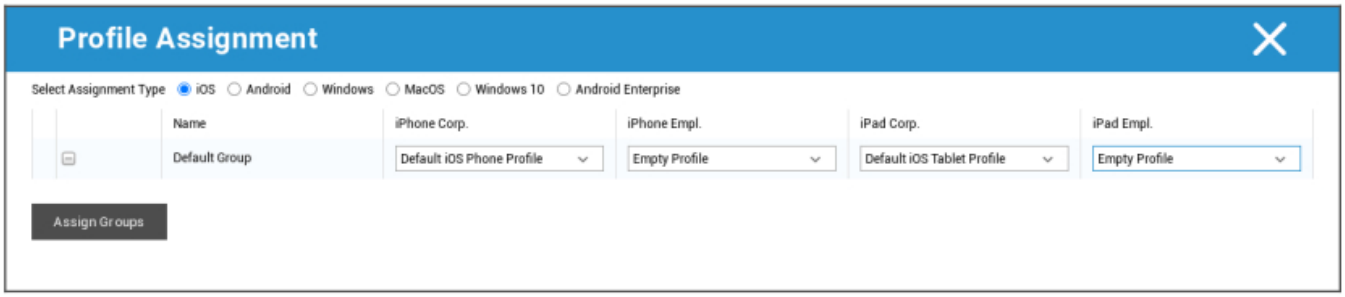
На останньому етапі ви можете встановити, чи є відповідний пристрій корпоративним або приватним (BYOD).

За допомогою кнопки "Експортувати як CSV" ви можете експортувати інформацію у вигляді файлу даних CSV. У свою чергу, ви також можете імпортувати файл даних CSV за допомогою "Імпортувати CSV", файл повинен виглядати як у прикладі нижче:

Філіп Райсс; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;

Масове призначення

У розділі Масове призначення ви можете призначити профіль усім групам, які поділяються на iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

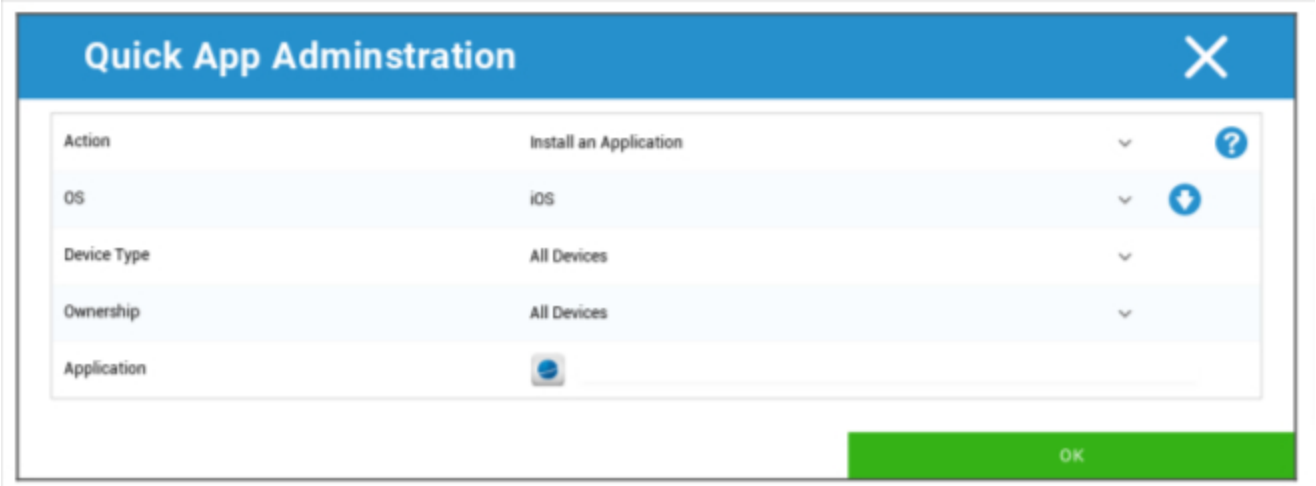


Windows - MacOS - Windows 10 - Android Enterprise

Швидке адміністрування додатків

У розділі Швидке адміністрування додатків ви можете надсилати запити на встановлення або видалення певної програми до обраної вами ОС.

Ви також можете вказати, чи слід надсилати запит на всі типи пристроїв з вибраною ОС, чи лише на певний тип пристрою.



Імпорт користувачів у форматі CSV

Імпортуйте користувачів з CSV у відповідну групу.

За допомогою кнопки "Завантажити шаблон CSV" ви можете експортувати файл шаблону CSV, який можна заповнити (або використовувати як зразок).

Ви також можете використовувати опції "Показувати ідентифікатори ролей" і "Показувати ідентифікатори груп" як посилання для створення власного CSV-файлу.

Файл CSV можна завантажити в MDM за допомогою кнопки "Завантажити CSV".

На останньому етапі ви можете розпочати імпорт, натиснувши на кнопку "Почати імпорт".

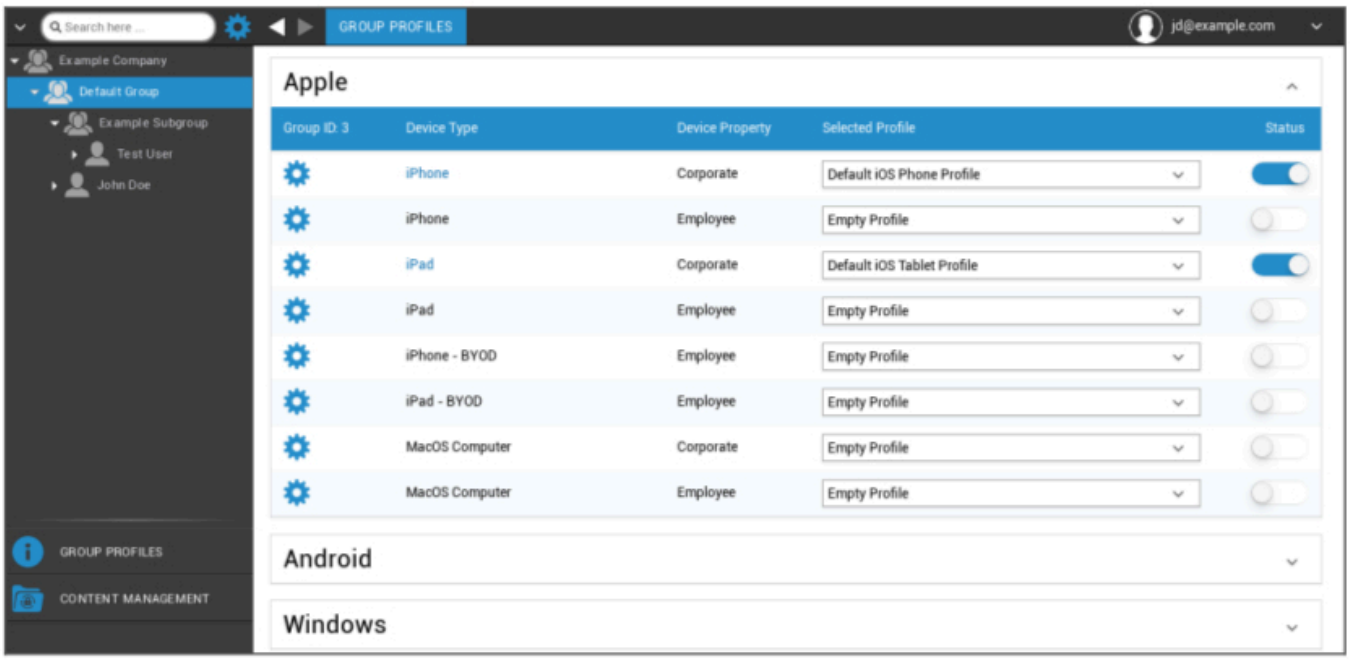
Управління групами в мобільному менеджменті

Один клік на огляді відображає різні профілі конфігурації для відповідних платформ.

Один профіль містить всі параметри налаштувань, які можна заздалегідь встановити за допомогою AppTec360 на пристрої кінцевого користувача. На кожній платформі ви можете створювати профілі для корпоративних пристроїв (Corporate) або для пристроїв з власними пристроями (Employee).

Щоб диференціювати конфігурації для груп пристроїв, наприклад, за місцем розташування або функціями, рекомендується створити кілька підгруп.

Будь ласка, зверніть увагу на Керування профілем у розділі Керування мобільними пристроями



За допомогою меню передач ви встановлюєте різноманітні налаштування для відповідної (під)групи.

Створити підгрупу	Створити підгрупу для відповідної (під)групи
Редагування вибраної групи	Редагування вибраної групи
Видалити вибрану групу	Видалити вибрану групу
Масовий набір	Зареєструйте кілька пристроїв/користувачів одночасно для вибраного профілю
Масове призначення	Призначити профілі до групи, яка вибрана в даний момент

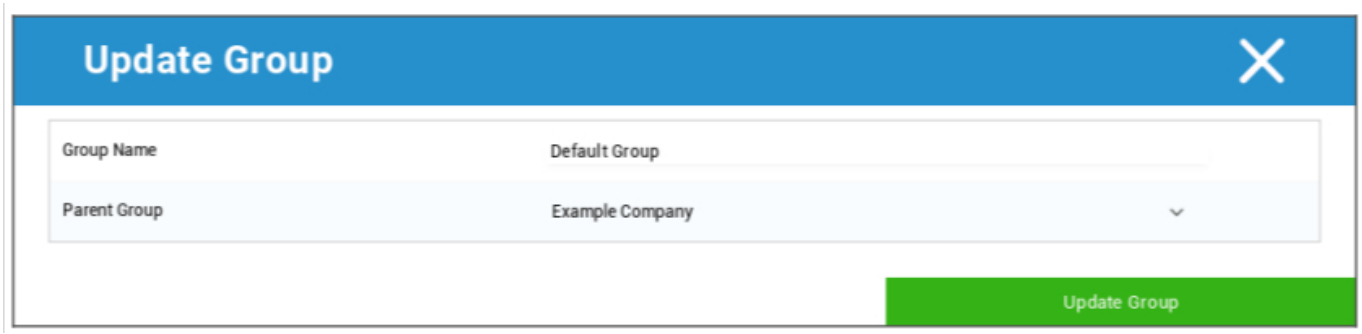
Створити підгрупу	Створити підгрупу для відповідної (під)групи
Створити користувача	Створіть користувача для відповідної (під)групи

Створити підгрупу

За допомогою кнопки "Створити підгрупу" ви можете створити додаткову підгрупу.

Ви можете вказати, до якої групи буде призначена підгрупа (за замовчуванням підгрупа призначається до групи, яка вибрана в даний момент).

Редагування вибраної групи



Тут ви можете редагувати профіль - тут можливі наступні налаштування:

- Назву групи можна змінити
- Батьківську групу можна змінити

Видалити вибрану групу

У розділі "Видалити вибрану групу" перераховані всі користувачі та пристрої, які входять до відповідної групи. Тут ви можете їх видалити.

Для одного користувача ви можете виконати наступні команди видалення:

Видалити користувача	Користувача видалено
Перемістити користувача до групи:	Ви можете перемістити користувача в іншу групу (наступний стовпчик, наприклад, "Адміни")

Для одного пристрою можна виконати такі команди видалення:

Витирання та видалення	Витирання та видалення пристрою
Видалити з системи	Видаляйте пристрій лише з AppTec

Довідка: Масовий набір на навчання

Довідка: Масове призначення

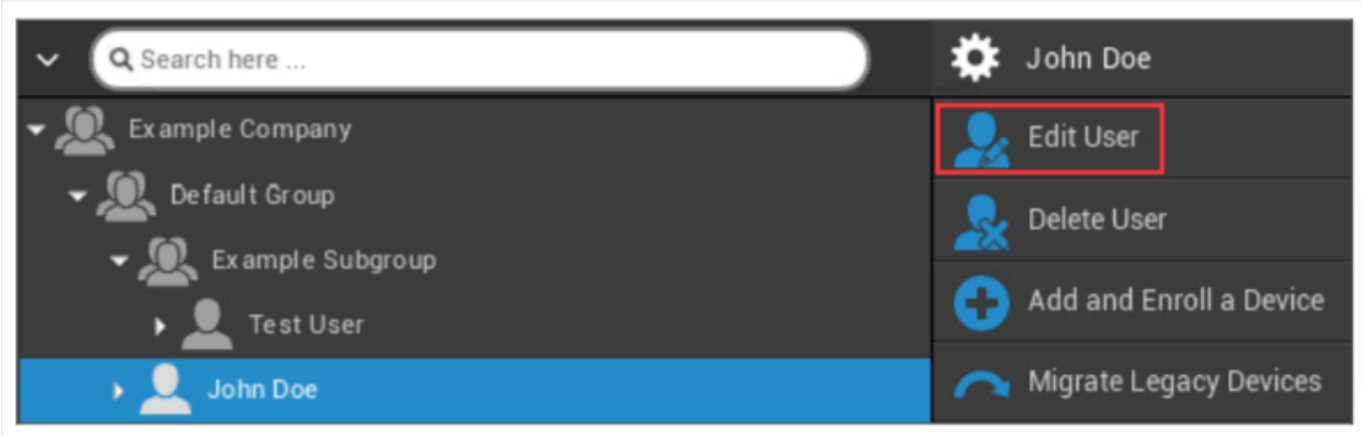
Створити користувача

За допомогою кнопки "Створити користувача" ви можете додати нового користувача.

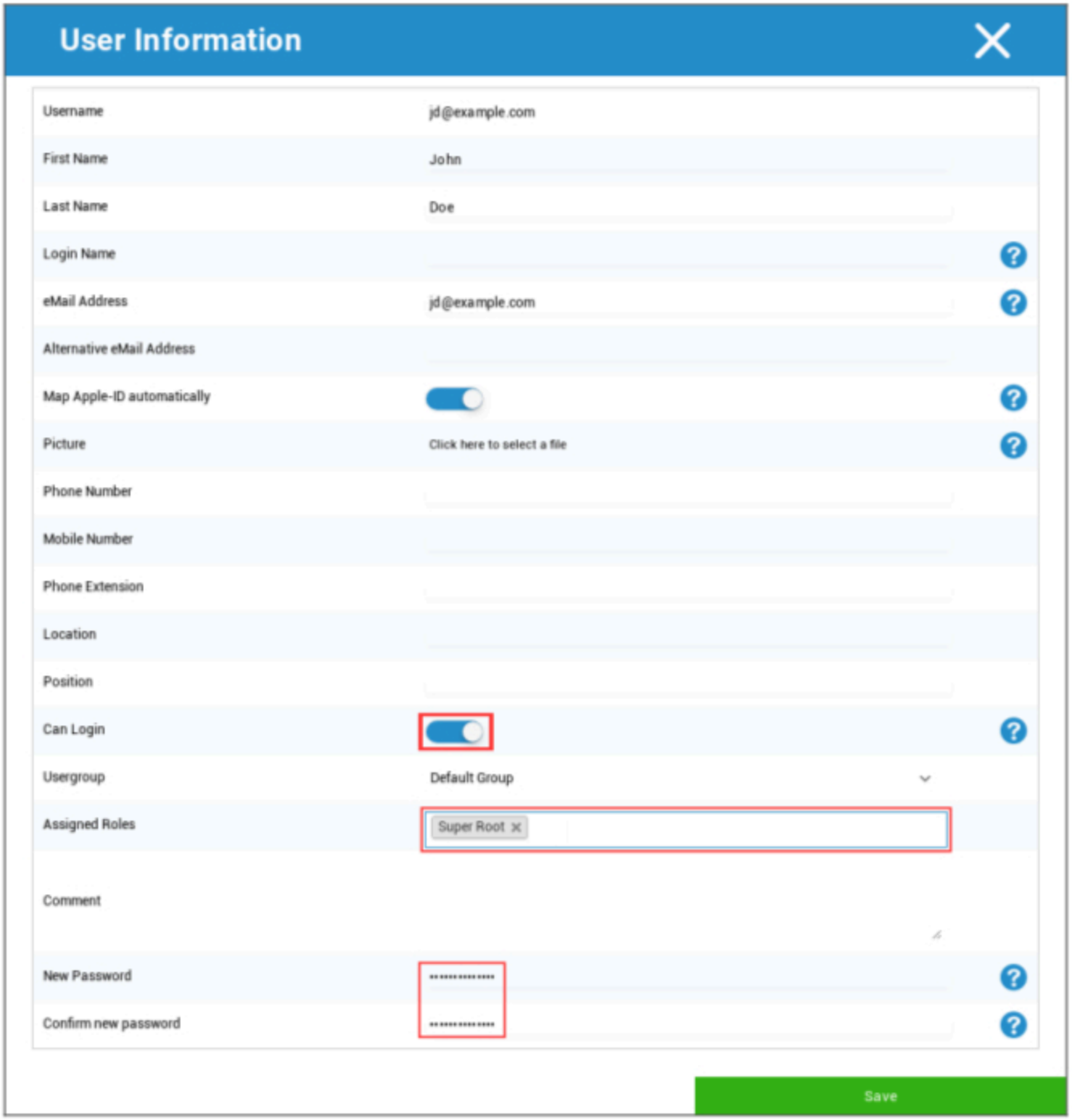
Створіть нового адміністратора-користувача

Ви можете призначити користувачеві права Адміністратора-користувача. Це дасть йому права на вхід до консолі, а також на зміну користувачів/груп/пристроїв.

Створіть звичайного користувача або скористайтеся вже існуючим. Виберіть Користувача, якому ви хочете надати права адміністратора, натисніть на коліщатко і виберіть "Редагувати користувача":



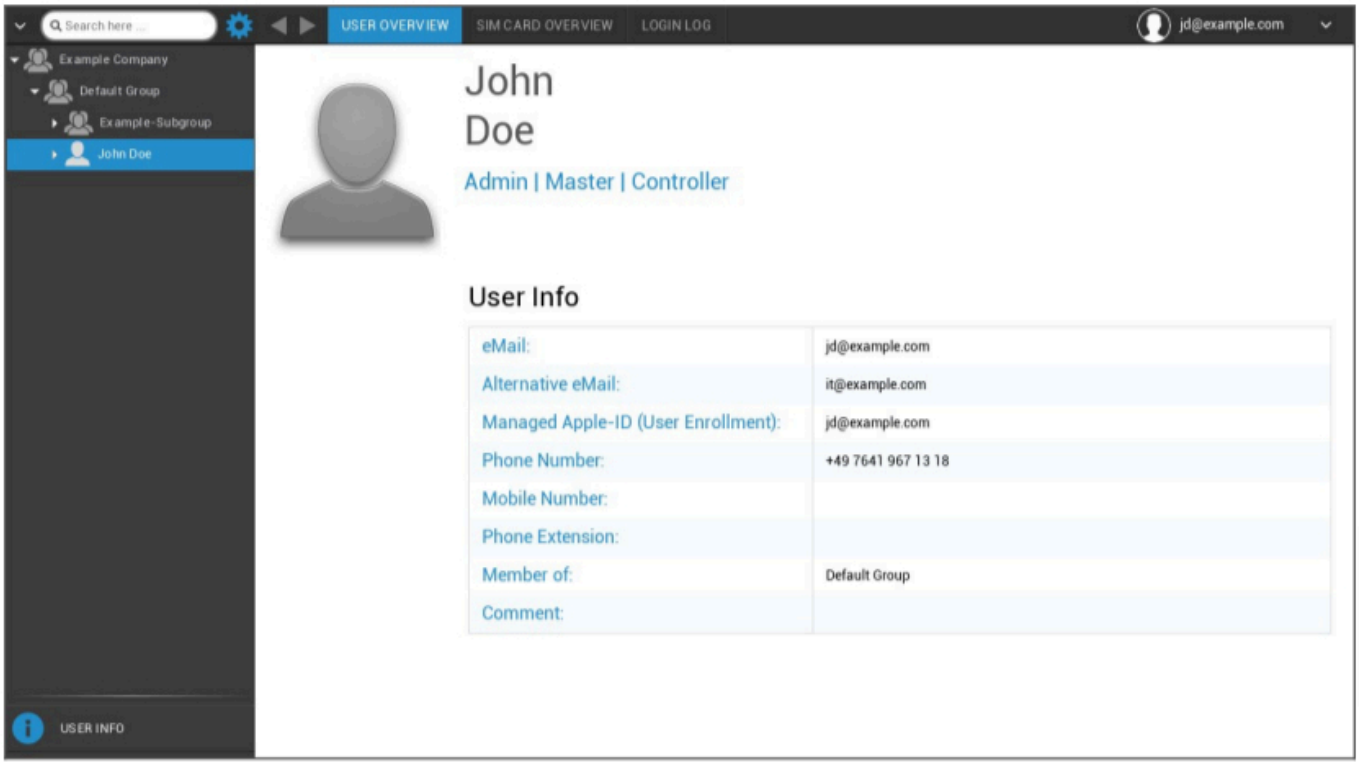
Увімкніть перемикач "Can Login", призначте користувачеві роль "Super-Root" і встановіть пароль.



Збережіть це, і тепер користувач може увійти за допомогою імені користувача та пароля.

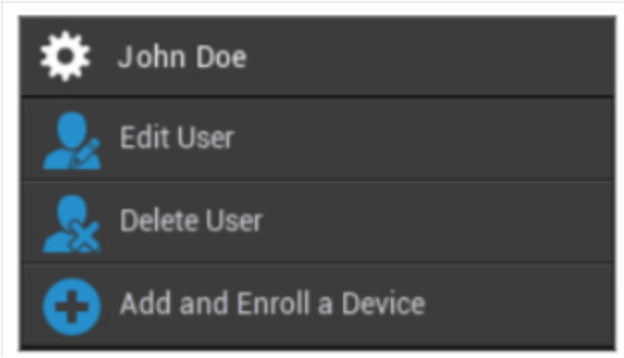
Керування користувачами в мобільному управлінні

Коли ви виберете певного користувача, ви побачите наступний огляд:



Ви отримаєте огляд всієї інформації, яку ви ввели раніше в розділі "Створити користувача".

За допомогою шестерні, встановленої зверху, ви можете виконати наступні конфігурації:



Ім'я користувача	Ім'я користувача вибраного користувача
Редагувати користувача	Редагування інформації про користувача
Видалити користувача	Видалити користувача • Видалити з системи = Пристрій буде видалено з AppTec

	• Wipe & Delete = Пристрій буде відновлено до заводських налаштувань і видалено з AppTec
Додавання та реєстрація Пристрою	Зареєструвати пристрій для вибраного користувача

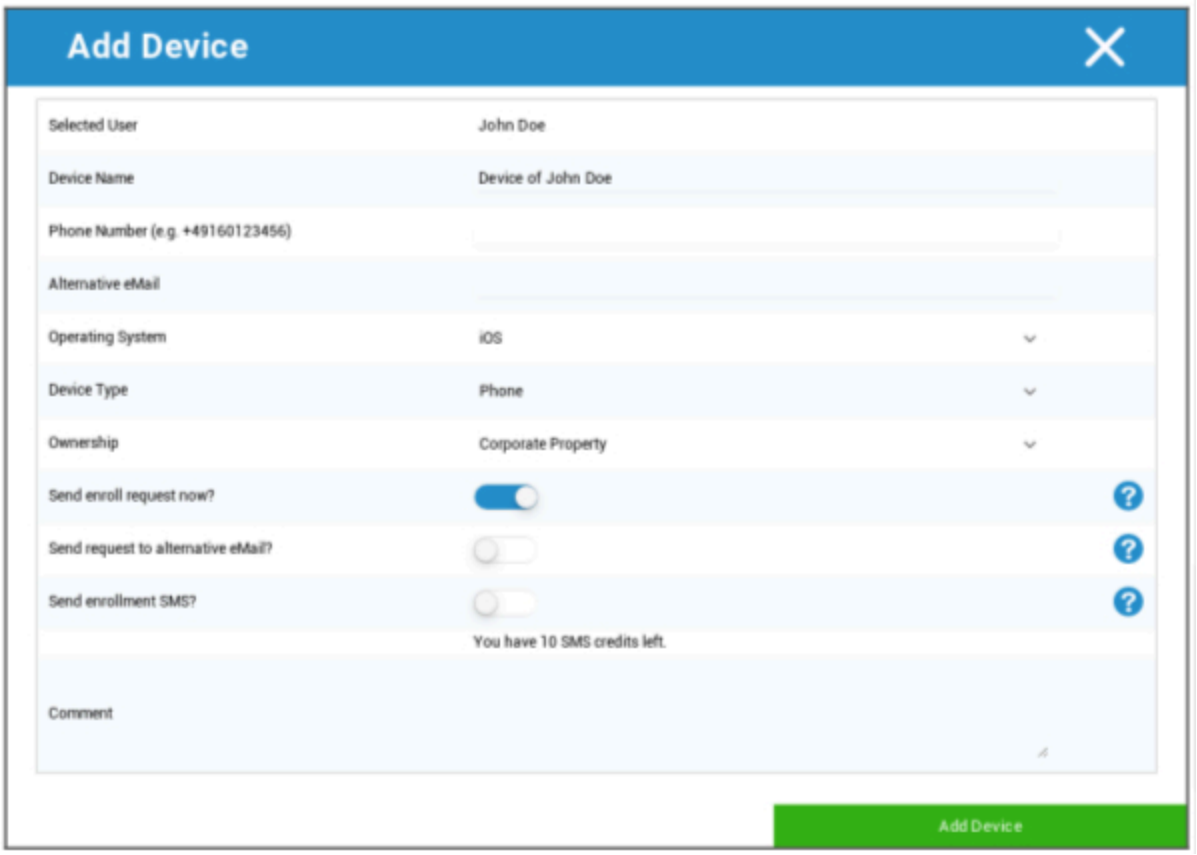
Зверніть увагу, що доступ до адміністрування також може бути поданий як локальний обліковий запис користувача в структурі ієрархії. Без створення додаткового адміністратора цей обліковий запис не можна видаляти!

Додавання та реєстрація Пристрою

Тут ви можете вибрати пристрій для обраного використання.

Крім того, ви можете вносити пристрої до групи безпосередньо. Для цього натисніть на групу, натисніть на коліщатко і виберіть "Додати та зареєструвати пристрій".

Вам варто ознайомитися з наступним оглядом:



Залежно від типу пристрою, який ви хочете зареєструвати, ви повинні виконати наступні налаштування:

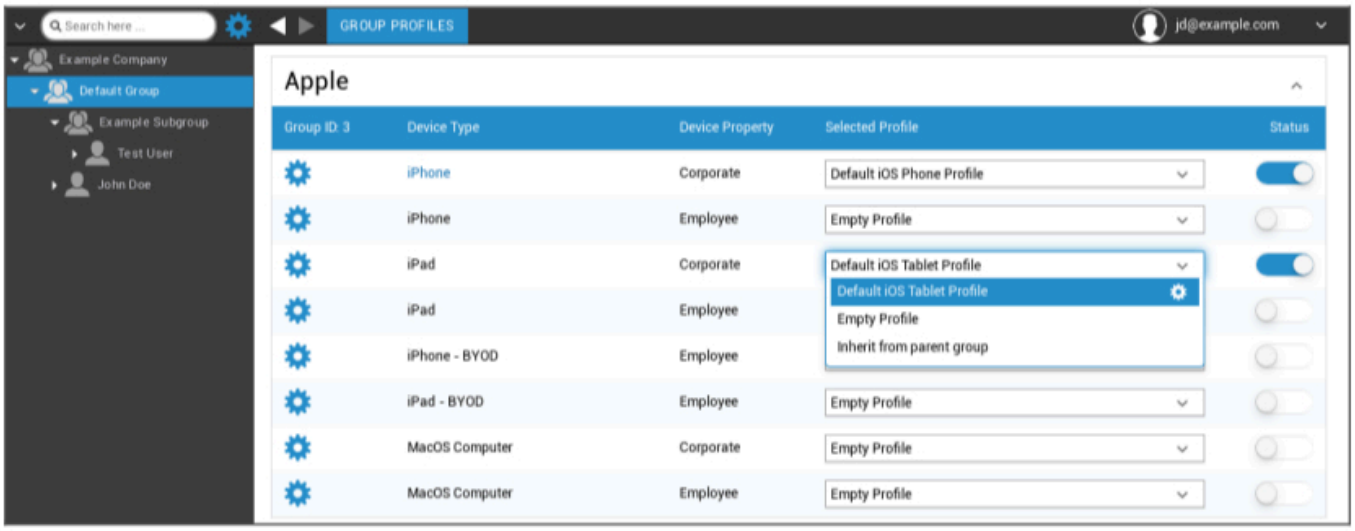
Вибраний користувач	Обраний користувач (заповнюється автоматично)
Назва пристрою	Буде заповнено автоматично (пристрій для "імені користувача") - можна, однак, змінити
Номер телефону	Номер телефону, буде заповнений автоматично (якщо він був наданий користувачем) - тут, однак, його можна додати або змінити
Альтернативна електронна пошта	Альтернативна електронна пошта, буде заповнена автоматично (якщо вона була надана користувачем) - тут, однак, її можна додати або змінити
Власник пристрою	Корпоративна власність = корпоративний пристрій Власність працівника = пристрій BYOD
Виберіть операційну систему	Тут ви можете вибрати одну з наступних операційних систем: • iOS • iOS BYOD (реєстрація користувачів) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Надіслати запит на реєстрацію?	Електронний лист одразу надсилається на основну адресу електронної пошти, а користувачеві пропонується підключити свій пристрій
Надіслати запит на альтернативну електронну пошту?	Надішліть лист додатково або виключно (якщо опція "Надіслати запит на реєстрацію?" була деактивована) на альтернативну електронну адресу (електронна адреса відрізняється від "звичайної" електронної адреси для запиту на реєстрацію)
Надіслати SMS для реєстрації?	Надішліть запит на реєстрацію за допомогою SMS (необхідно ввести "Номер телефону")

Після відправлення запиту на реєстрацію пристрій одразу з'явиться на екрані (позначений червоним кольором).

Після успішного підключення пристрій буде позначено зеленим кольором, що означає, що він готовий до отримання обмежень, додатків тощо.

Керування профілями в мобільному управлінні

Після натискання на групу ви отримаєте огляд всіх платформ пристроїв, які потрібно налаштувати, і відповідно призначених профілів.



	Виконайте конфігурацію для обраного профілю
Тип пристрою	Тип та/або модель пристрою
Властивості пристрою	Власник пристрою (Corporate = корпоративна власність, Employee = приватний пристрій працівника)
Обраний профіль	Вибраний профіль (перемикач відкриває діалогове вікно конфігурації профілю)
Статус	Увімкнено/вимкнено (профіль увімкнено/вимкнено)

Коли ви виберете передачу, ви отримаєте наступні варіанти:

Створіть профіль

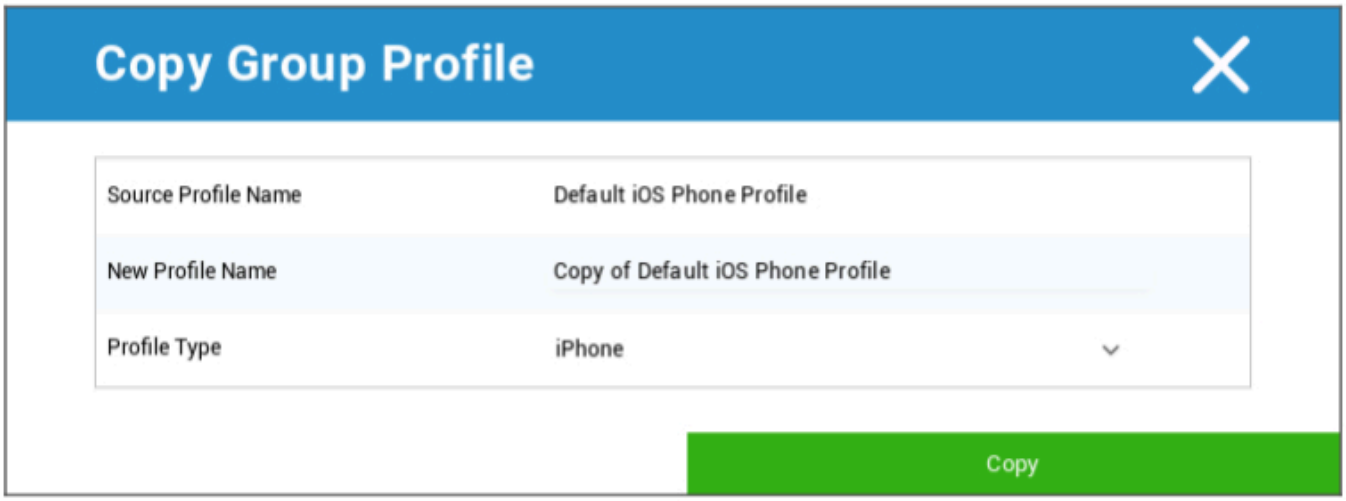
Ви можете створити та налаштувати новий профіль для кожного запису та/або платформи. Після натискання на цей підпункт профіль буде негайно створено, і ви зможете одразу ж розпочати конфігурацію для iOS, Android та Windows Phone.

Редагувати профіль

Після натискання на "Редагувати профіль" ви потрапите на сторінку конфігурації відповідного профілю, де ви можете встановити конфігурацію.

Копіювати профіль

За допомогою функції "Копіювати профіль" ви можете скопіювати налаштування/конфігурації з уже існуючого профілю і додати їх до нового профілю.

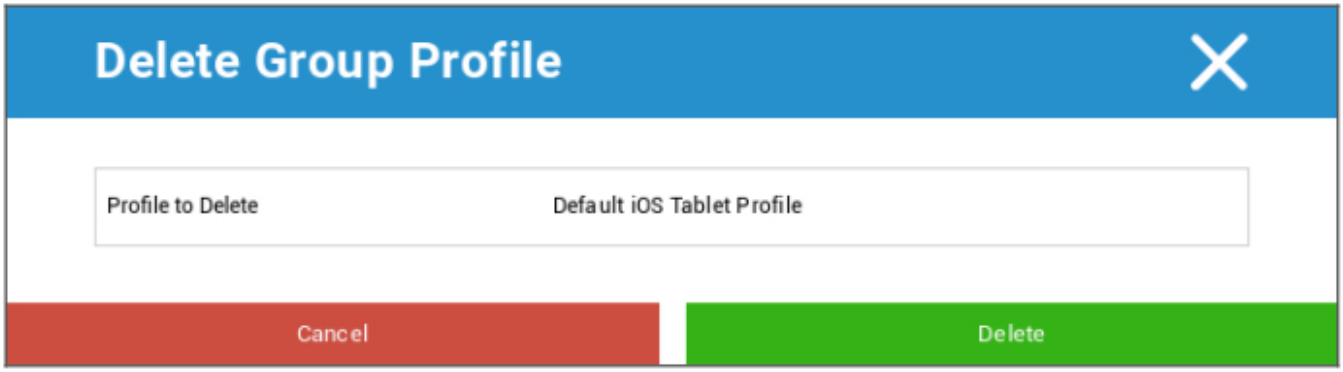


Назва вихідного профілю Ім'я профілю	Назва профілю, який потрібно скопіювати
Нова назва профілю	Назва нового профілю
Тип профілю	Тип профілю (Телефон/планшет)

Після натискання кнопки "Копіювати" профіль буде створено, і тепер його можна буде призначити групі

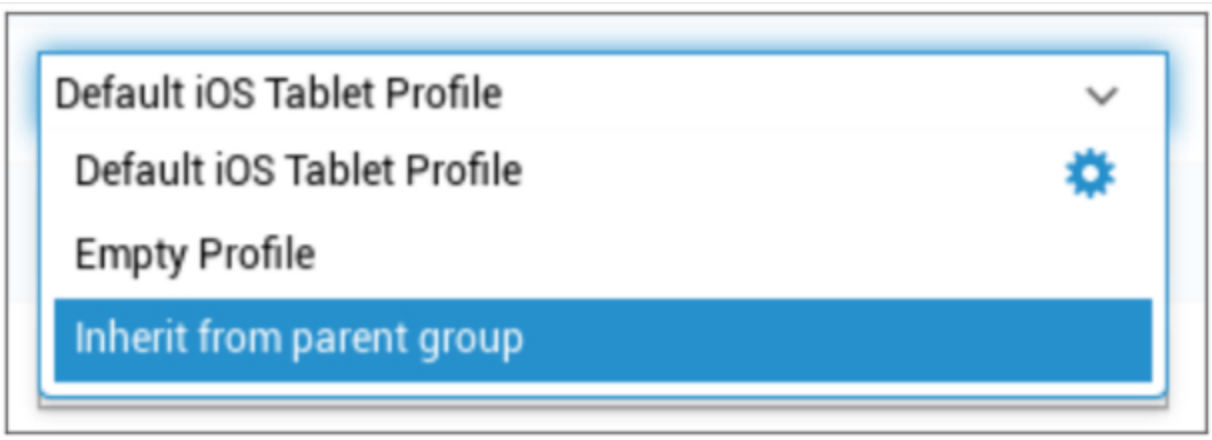
Видалити профіль

Тут ви можете назавжди видалити профіль. Зверніть увагу, що під час процесу видалення і наступного процесу "Призначити зараз" для профілю, конфігурація зникне на відповідних пристроях ураженої групи і не може бути відновлена!


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

Спадкування профілів

Під час вибору профілів доступна опція "Успадкувати від батьківської групи".



Якщо профіль активовано, то для відповідного вибраного пристрою (і відповідного типу пристрою) буде використано профіль батьківської групи. Зауважте також, що зміни у цьому профілі можуть вплинути на багато груп.

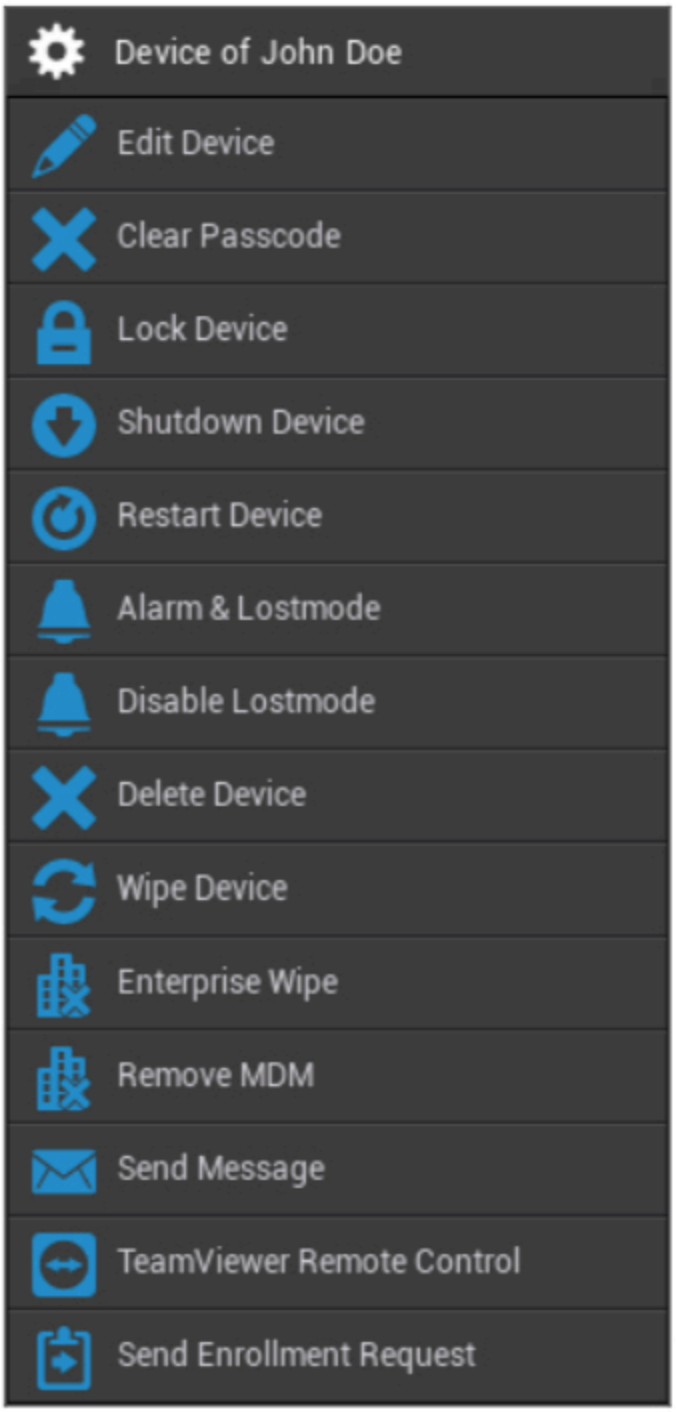
Ця конфігурація встановлюється як значення за замовчуванням, коли створюється нова підгрупа.

Також доступна конфігурація "Порожній профіль", яка відповідає порожньому профілю, що означає, що в кінцевому підсумку на пристрої кінцевого користувача не буде виконано жодних нових конфігурацій.

Керування пристроями в мобільному управлінні

Коли ви обираєте пристрій, ви можете виконувати різноманітні завдання за допомогою "шестерні". Вони відрізняються залежно від платформ ОС (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

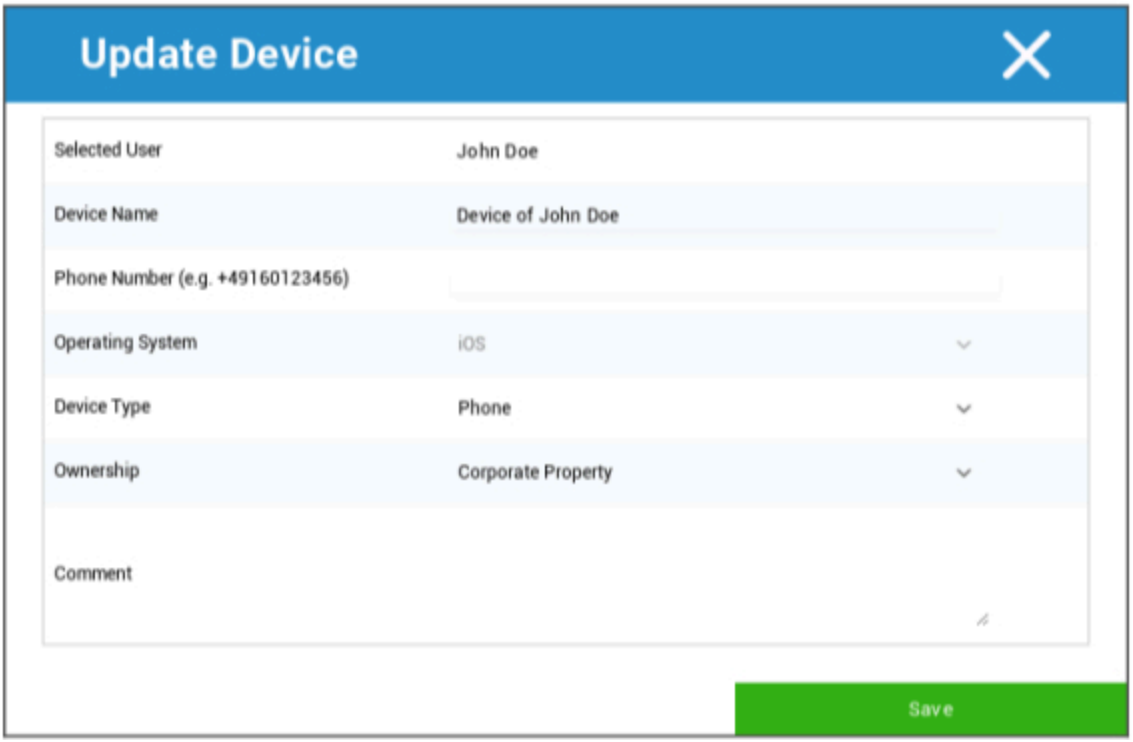
IOS



Редагувати пристрій	Редагувати пристрій
Очистити пароль	Парольний код пристрою стерто
Пристрій блокування	Блокування пристрою (екран блокування)
Пристрій вимкнення	Пристрій вимкнення

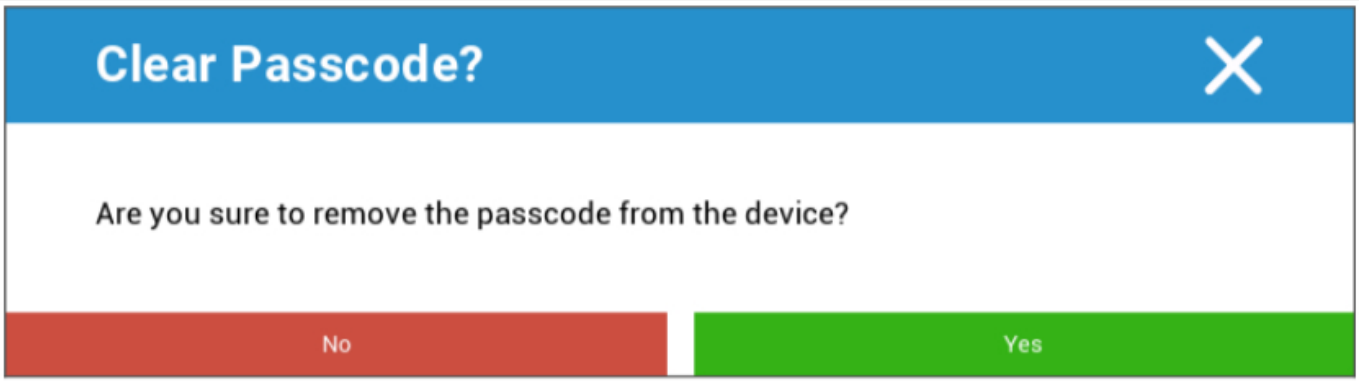
Перезавантажити пристрій	Перезавантажити пристрій
Тривога та режим втрати	Початок сигналу тривоги та режим "Загублений
Вимкнути Lostmode	Вимкнути Lostmode
Видалити пристрій	Видалити пристрій з AppTec
Пристрій для витирання	Відновлення заводських налаштувань пристрою
Enterprise Wipe	Інформація, програми та профілі, надані AppTec360, видаляються (пристрій відокремлюється від MDM)
Видалити MDM	
Надіслати повідомлення	Надсилання пуш-сповіщень на пристрій Повідомлення буде відображено в додатку AppTec360 (вкладка "Повідомлення")
Пульт дистанційного керування TeamViewer	Запуск сеансу дистанційного керування за допомогою TeamViewer
Надіслати запит на реєстрацію	Надіслати (повторний) запит на зарахування

Редагувати пристрій



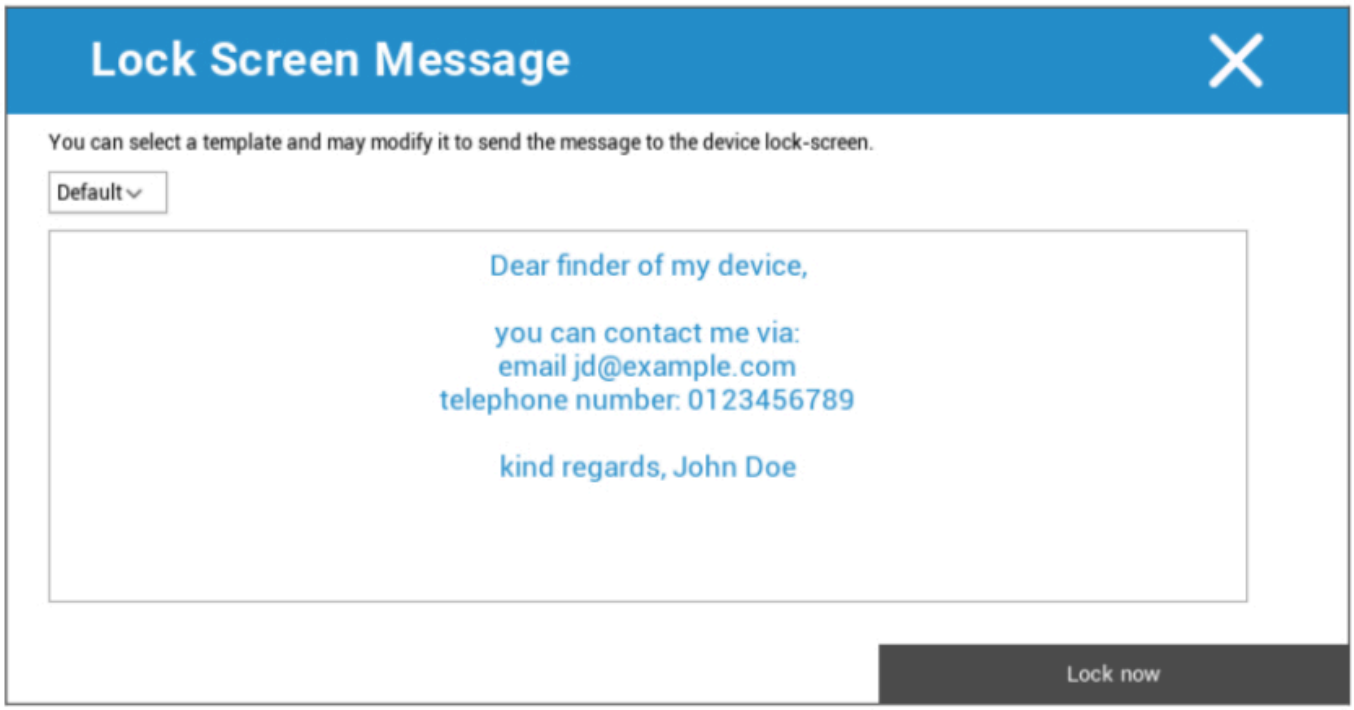
Тут ви можете оновити різноманітну інформацію про пристрій.

Очистити пароль



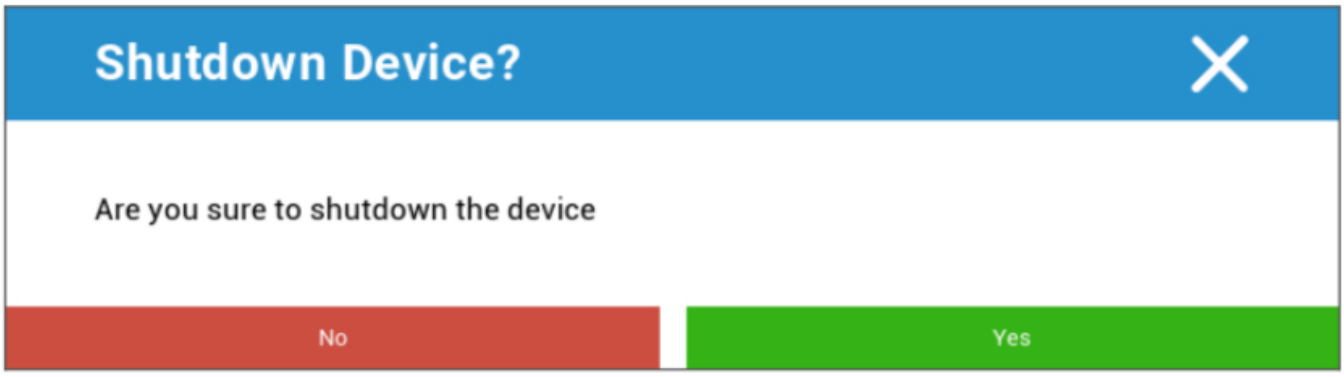
У розділі "Очистити пароль" ви можете віддалено видалити пароль з пристрою. Згодом користувачеві буде запропоновано ввести новий пароль (залежно від інструкцій з використання пароля).

Пристрій блокування



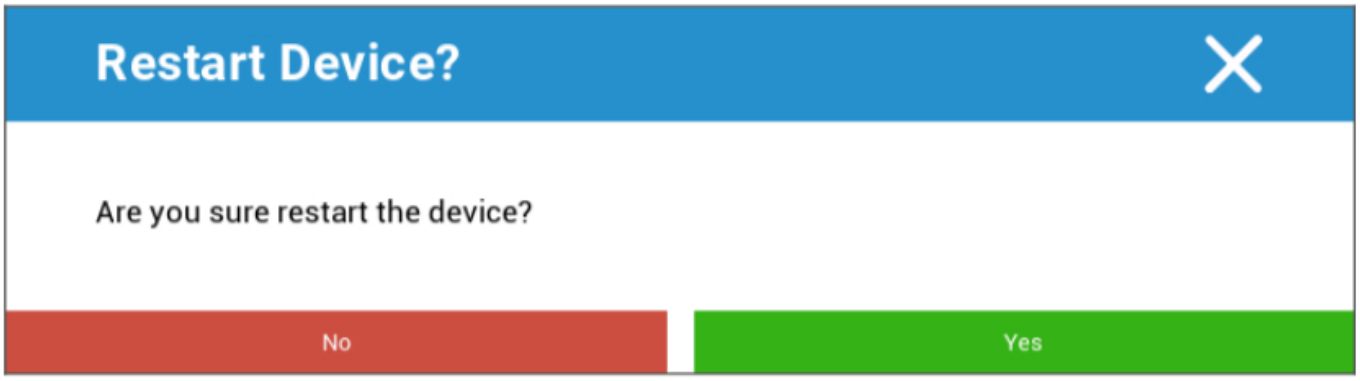
Тут команда блокування надсилається на пристрій кінцевого користувача (екран блокування).

Пристрій вимкнення



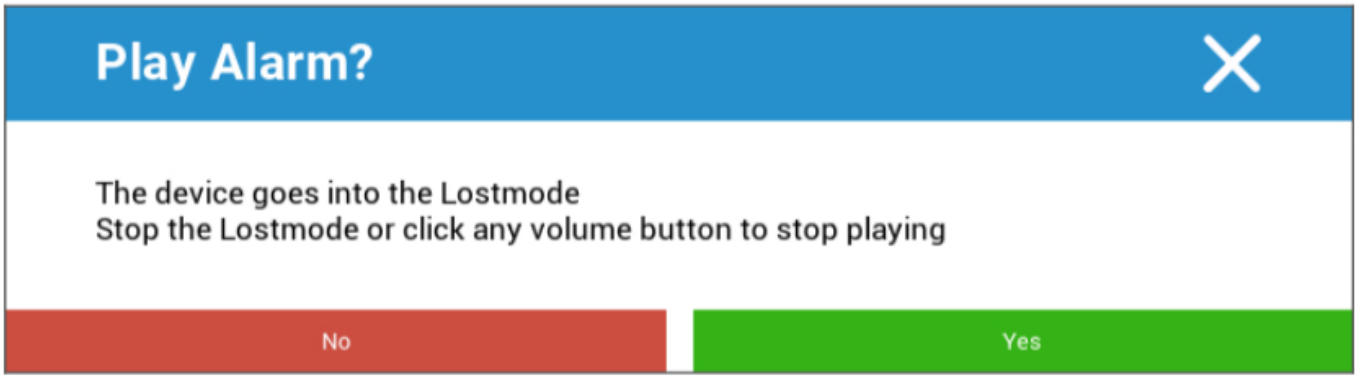
Тут на кінцевий пристрій користувача надсилається команда вимкнення.

Перезавантажити пристрій

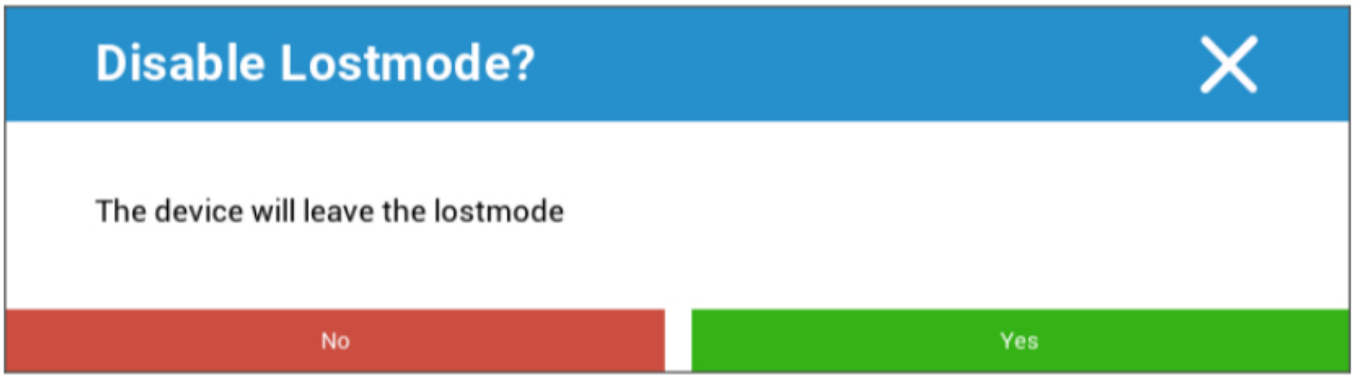


Тут на пристрій кінцевого користувача надсилається команда перезапуску.

Сигналізація та режим втрати | Вимкнути режим втрати



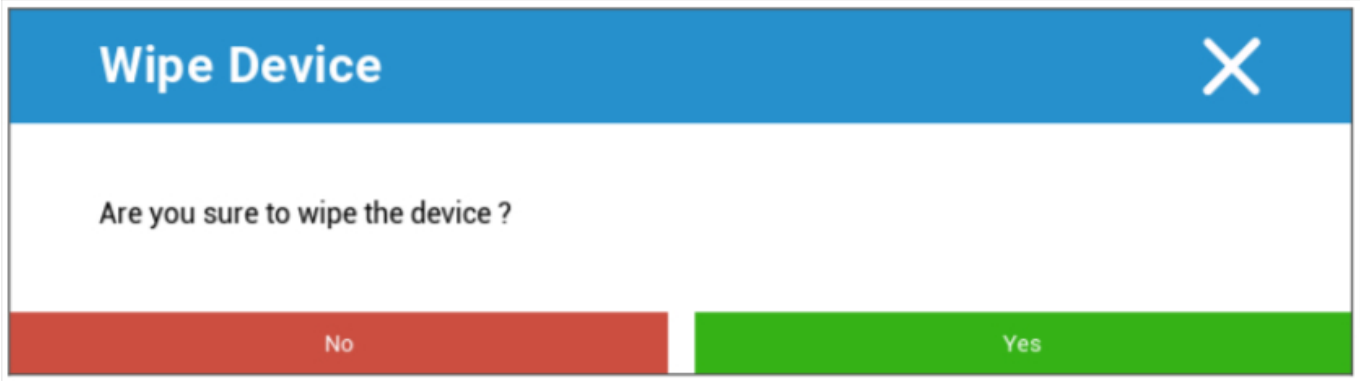
Тут пристрій можна перевести в режим "Загублений", в якому пристрій буде постійно відтворювати звуковий сигнал будильника. Режим "Загублений" можна вимкнути, натиснувши будь-яку кнопку гучності пристрою або віддалено, натиснувши на "Вимкнути режим "Загублений"":



Видалити пристрій

Тут можна виконати команду видалення. Ви можете ще раз вирішити, чи потрібно видалити пристрій лише з AppTec360 ("Видалити з системи"), чи потрібно видалити пристрій з AppTec360, а також відновити його заводські налаштування ("Витерти і видалити").

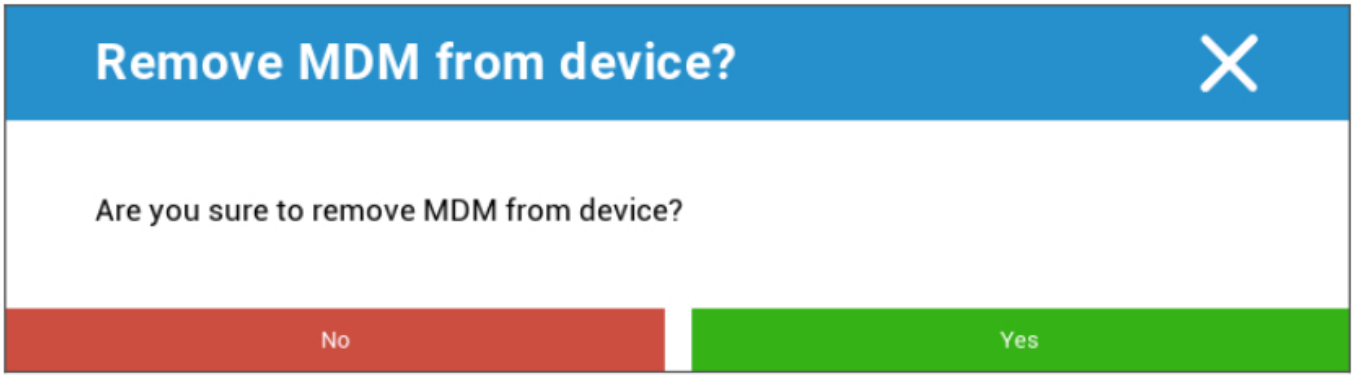
Пристрій для витирання



У розділі "Очистити пристрій" ви можете виконати повне очищення пристрою. Пристрій буде відновлено до заводських налаштувань.

Enterprise Wipe | Видалення MDM

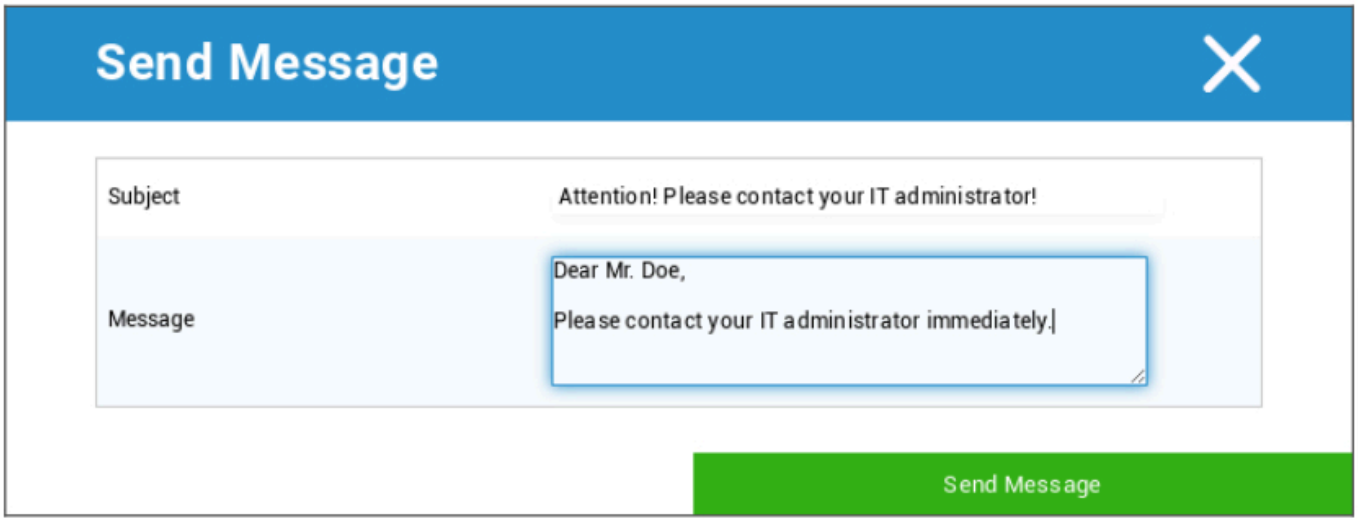
Видаляється лише інформація, програми та профілі, надані AppTec360. Таким чином, корпоративні дані більше не будуть доступні на пристрої кінцевого користувача. Приватна зона не зачіпається і продовжує залишатися на пристрої кінцевого користувача.



За допомогою "Видалити MDM" ви можете видалити профіль MDM на кінцевому пристрої користувача і всі інші елементи, надані AppTec.

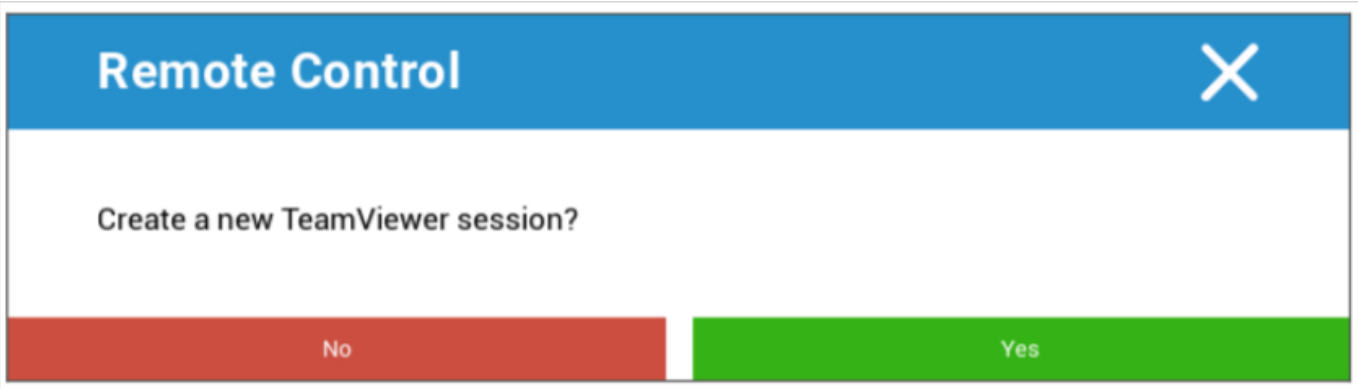
Ця команда виконує ті ж дії, що і "Enterprise Wipe".

Надіслати повідомлення



Тут ви можете надіслати Push-сповіщення на відповідний пристрій.

Пульт дистанційного керування TeamViewer



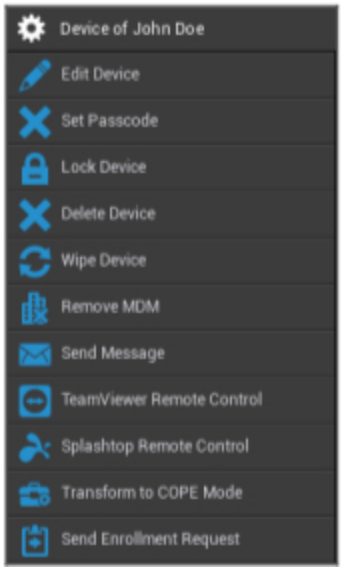
Тут можна розпочати сеанс віддаленого керування Teamviewer.

Надіслати запит на реєстрацію

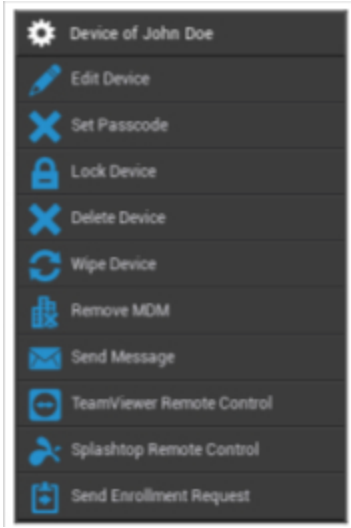
За допомогою "Надіслати запит на реєстрацію" ви можете надіслати запит на реєстрацію (ще раз) відповідному користувачеві.

Android

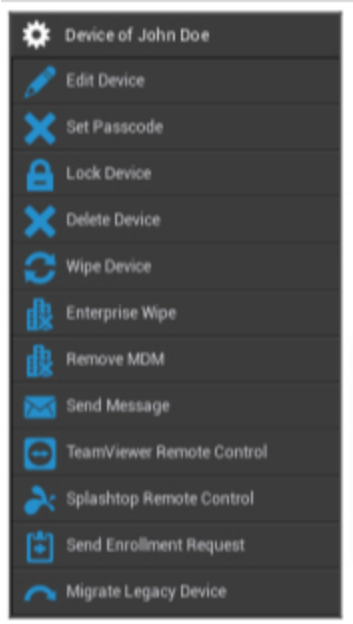
AE Повністю керований пристрій (керування роботою)



Профіль роботи AE (контейнер)



Телефон Android | Планшет

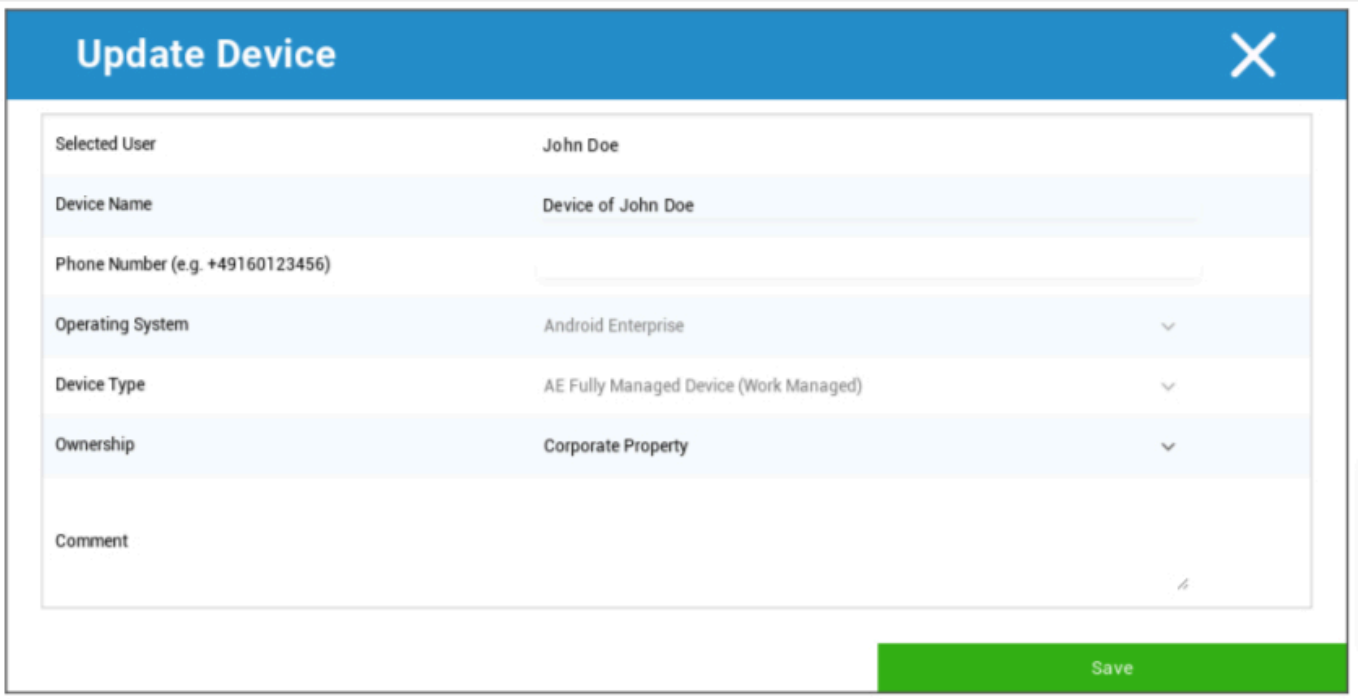


Редагувати пристрій	Редагування інформації про пристрій
Встановити пароль	Встановіть пароль пристрою
Пристрій блокування	Блокування пристрою (екран блокування)
Видалити пристрій	Видалити пристрій з AppTec
Пристрій для витирання	Відновлення заводських налаштувань пристрою
Enterprise Wipe	Інформація, Програми, Профілі, які надаються AppTec360, видаляються (пристрій буде відокремлено від MDM)
Видалити MDM	
Надіслати повідомлення	Надсилайте Push-сповіщення на пристрій Повідомлення буде відображено в додатку AppTec360 (вкладка "Повідомлення")
Пульт дистанційного керування TeamViewer	Запустіть сеанс віддаленого керування для цього пристрою за допомогою TeamViewer
Пульт дистанційного керування Splashtop	Запустіть сеанс дистанційного керування для цього пристрою за допомогою Splashtop
Перехід у режим COPE (тільки на повністю керованому пристрої AE (Work Managed))	Створіть робочий профіль на цьому пристрої з повним керуванням AE (Work

	Managed)
Надіслати запит на реєстрацію	Надіслати (повторний) запит на реєстрацію
Перенести застарілий пристрій (тільки на телефоні/планшеті Android, якщо ви зареєструвалися за допомогою надання режиму власника пристрою)	Перенесіть профіль телефону/планшета Android на профіль повністю керованого пристрою AE (Work Managed)

Редагувати пристрій

Тут ви можете оновити різноманітну інформацію про пристрій.



Вибраний користувач	Користувач пристрою
Назва пристрою	Назва пристрою
Номер телефону	Номер телефону пристрою
Операційна система	Android Enterprise Android
Тип пристрою	Андроїд Ентерпрайз: • AE Повністю керований пристрій (керування роботою) • Режим робочого профілю AE (лише для контейнера) • AE Повністю керований пристрій з робочим профілем (COPE) Андроїд: • Телефон • Планшет
Право власності	Корпоративна = корпоративна власність

	Працівник = власність працівника
Коментар	Додаткові описи для пристрою

Очистити пароль

Тут ви можете видалити пароль пристрою на вибраному пристрої. За замовчуванням на Android пароль буде встановлено на "123456" - користувач може і повинен змінити його згодом.

Пристрій блокування

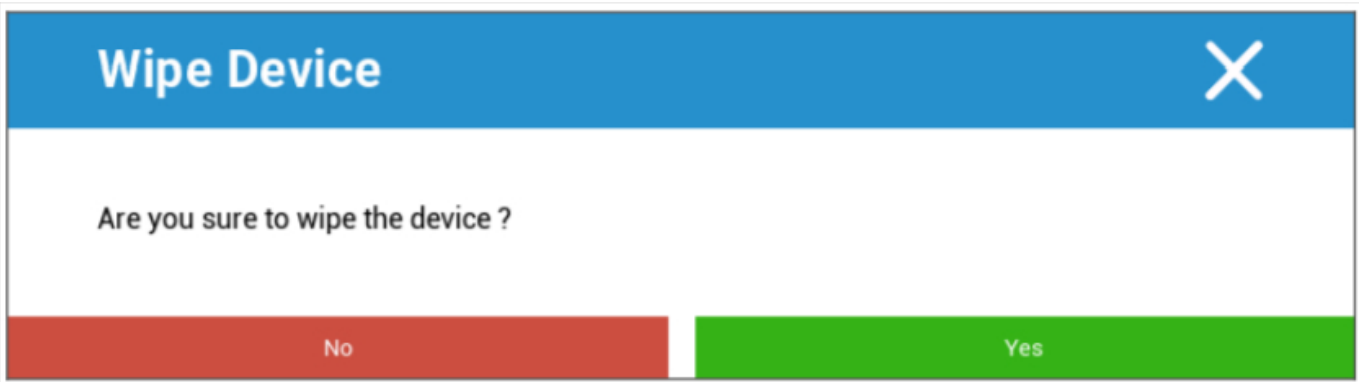
Тут на пристрій буде надіслано команду блокування пристрою (екран блокування).

Видалити пристрій

Тут можна виконати команду видалення. Ви можете ще раз вирішити, чи потрібно видалити пристрій лише з AppTec360 ("Видалити з системи"), чи потрібно видалити пристрій з AppTec360 і додатково відновити його до заводських налаштувань ("Витерти і видалити").

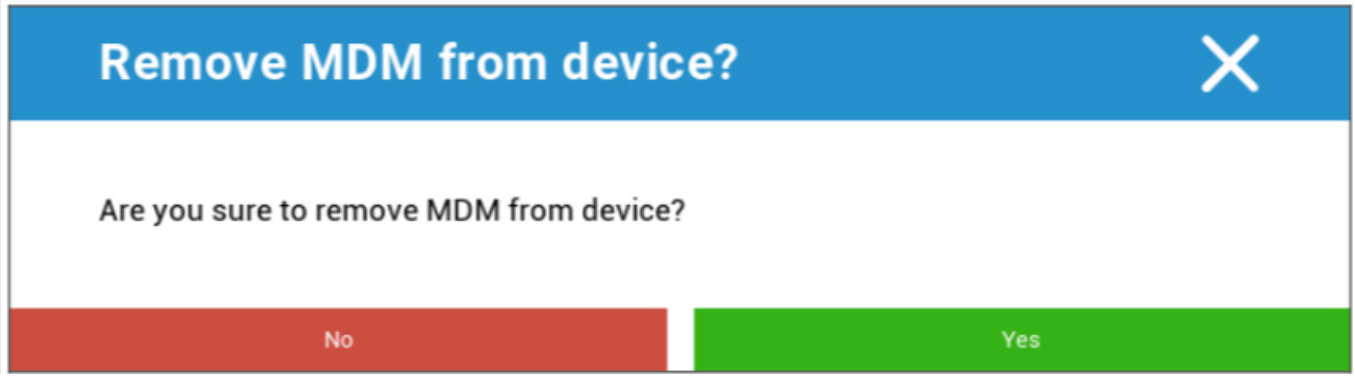
Пристрій для витирання

У розділі "Очистити пристрій" ви можете виконати повне очищення пристрою. Після цього пристрій буде відновлено до заводських налаштувань.



Крім того, якщо пристрій містить SD-карту, ви можете стерти SD-карту. Це можна зробити, встановивши для параметра "Wipe SD Card too? " на "Увімкнено".

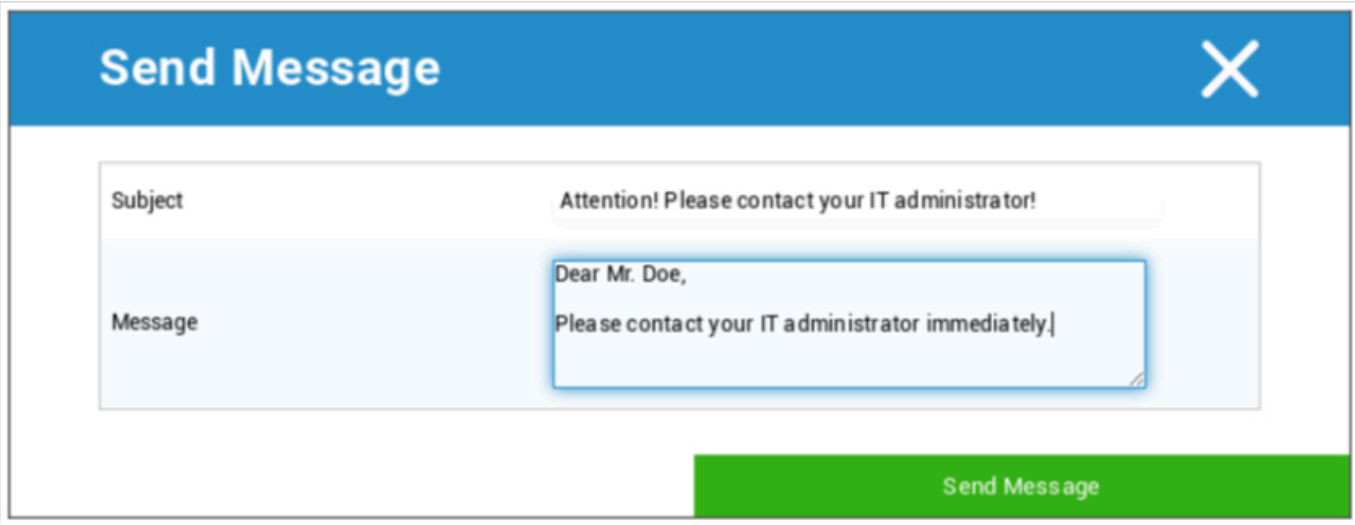
Видалити MDM



Це рекомендований метод для створення відокремлення від MDM.

Видаляється лише інформація, додатки та профілі, надані AppTec360, а це означає, що всі корпоративні дані більше не будуть доступні на пристрої кінцевого користувача. Приватна сфера, однак, не зачіпається і продовжує залишатися на пристрої кінцевого користувача.

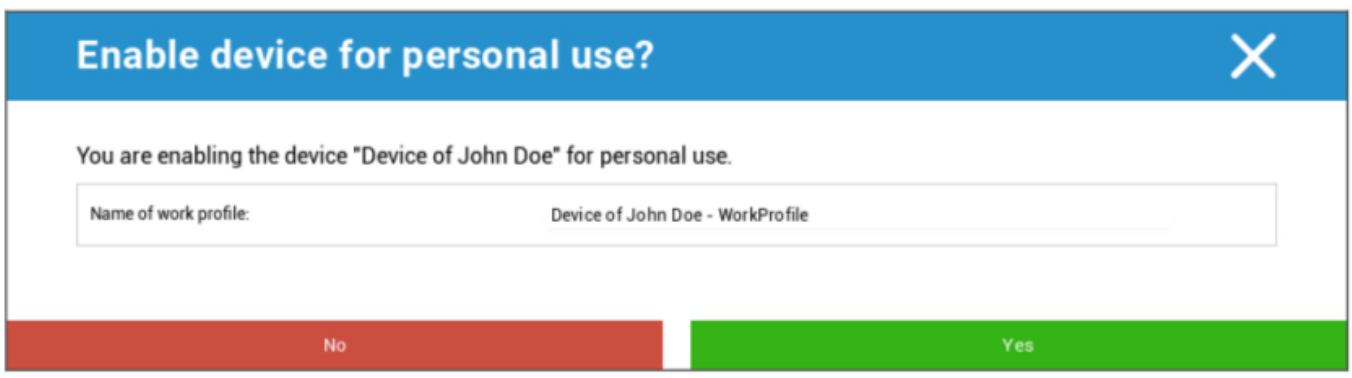
Надіслати повідомлення



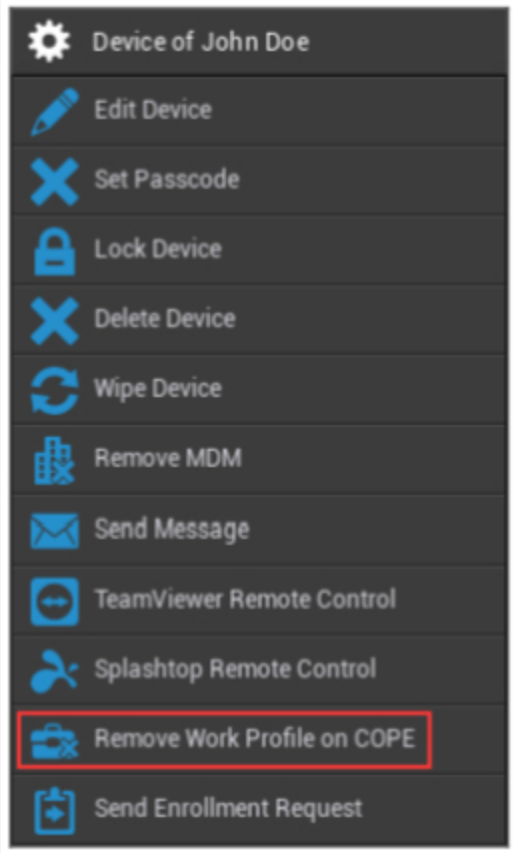
Тут ви можете надіслати Push-сповіщення на відповідний пристрій кінцевого користувача.

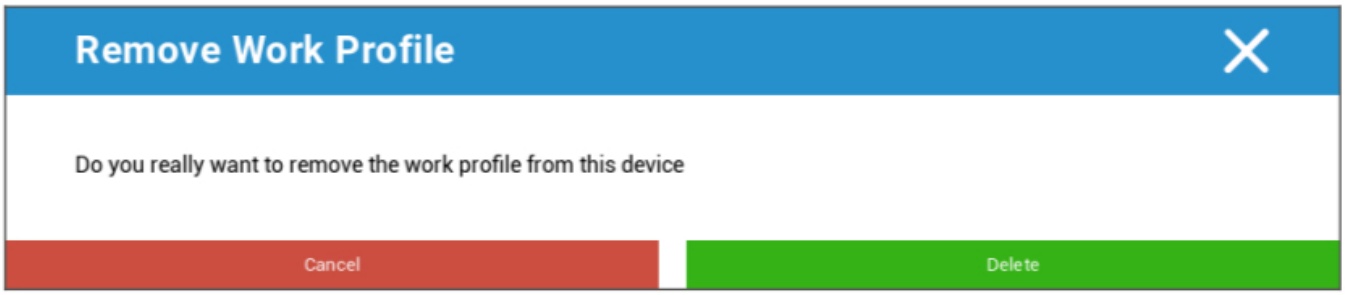
Перехід у режим COPE

Створіть робочий профіль на цьому пристрої з повним керуванням AE (Work Managed)



Після переведення пристрою в режим COPE ви можете видалити робочий профіль, натиснувши на опцію шестерні **Видалити робочий профіль на COPE:**




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

Надіслати запит на реєстрацію

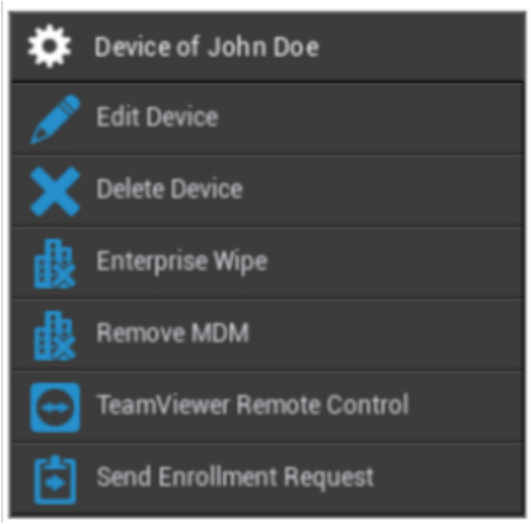
За допомогою "Надіслати запит на реєстрацію" ви можете надіслати запит на реєстрацію (ще раз) відповідному користувачеві.

Будь ласка, зверніть увагу, що дійсною є лише найновіша заявка на реєстрацію.

Перенести застарілий пристрій

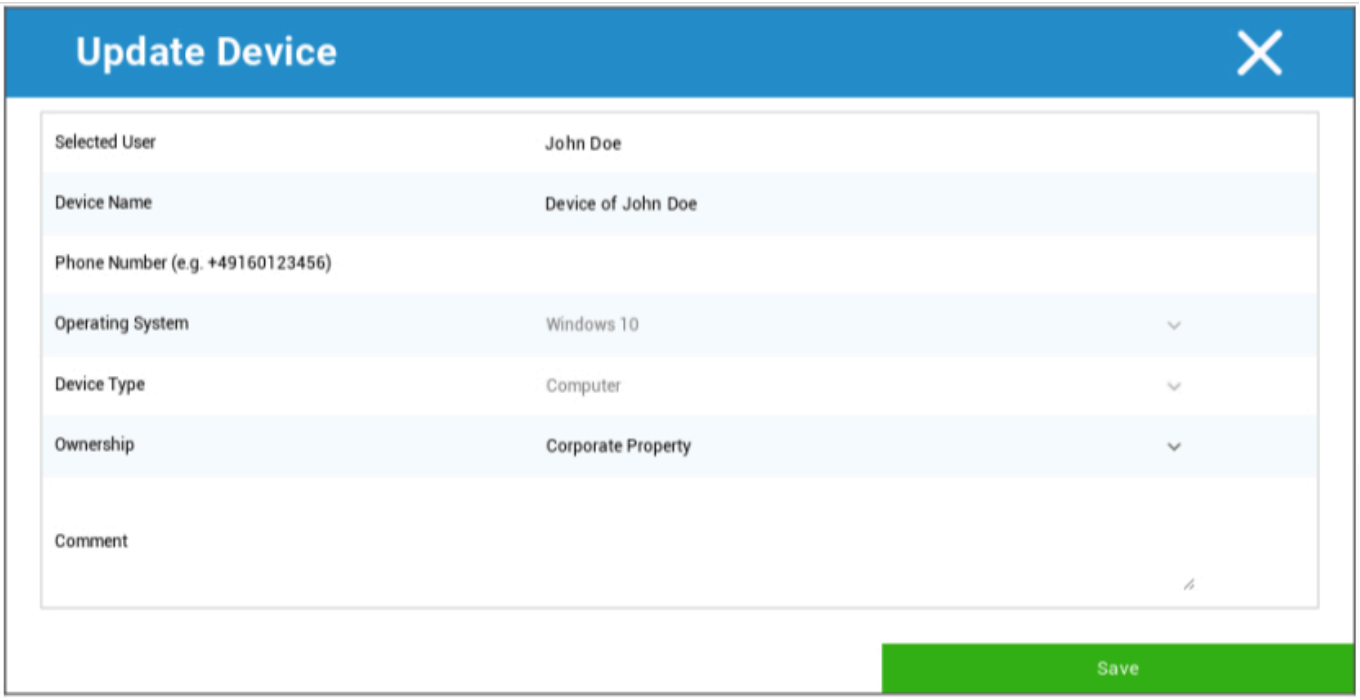
Перенесіть профіль телефону/планшета Android на профіль повністю керованого пристрою AE (Work Managed)

Windows



Назва пристрою	Назва вибраного пристрою
Редагувати пристрій	Редагувати пристрій
Видалити пристрій	Видалити пристрій з AppTec
Enterprise Wipe	Інформація, програми та профіль, надані AppTec360, видаляються
Видалити MDM	
Пульт дистанційного керування TeamViewer	Віддалене керування пристроєм за допомогою TeamViewer
Надіслати запит на реєстрацію	Надішліть запит на реєстрацію (ще раз)

Редагувати пристрій

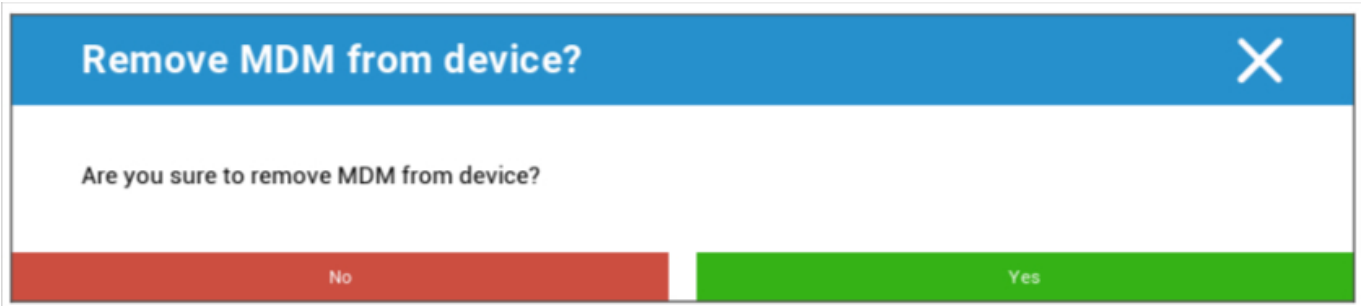


Тут ви можете оновити різноманітну інформацію про пристрій.

Видалити пристрій

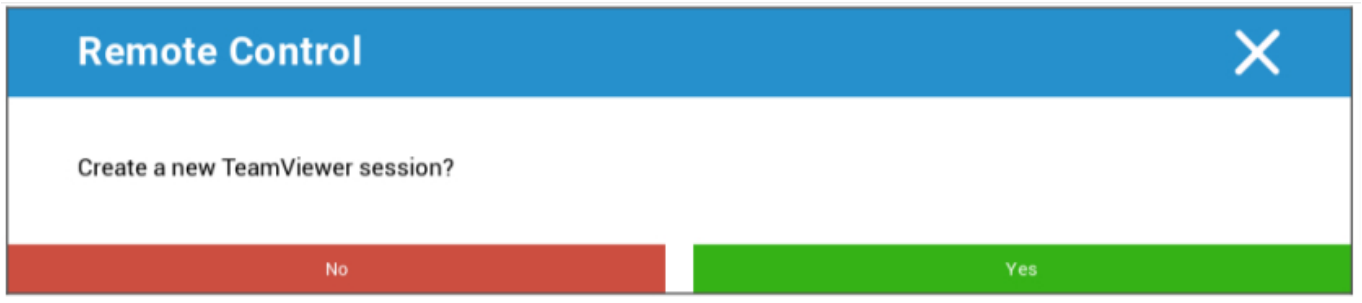
Тут можна виконати команду видалення, яка лише видаляє пристрій з AppTec360.

Enterprise Wipe | Видалення MDM



Видаляється лише інформація, програми та профілі, надані AppTec360. Таким чином, корпоративні дані більше не будуть доступні на пристрої кінцевого користувача. Приватна зона не зачіпається і продовжує залишатися на пристрої кінцевого користувача.

Пульт дистанційного керування TeamViewer



Тут ви можете розпочати сеанс віддаленого керування TeamViewer для цього пристрою.

Надіслати запит на реєстрацію

За допомогою "Надіслати запит на реєстрацію" ви можете надіслати запит на реєстрацію (ще раз) відповідному користувачеві.

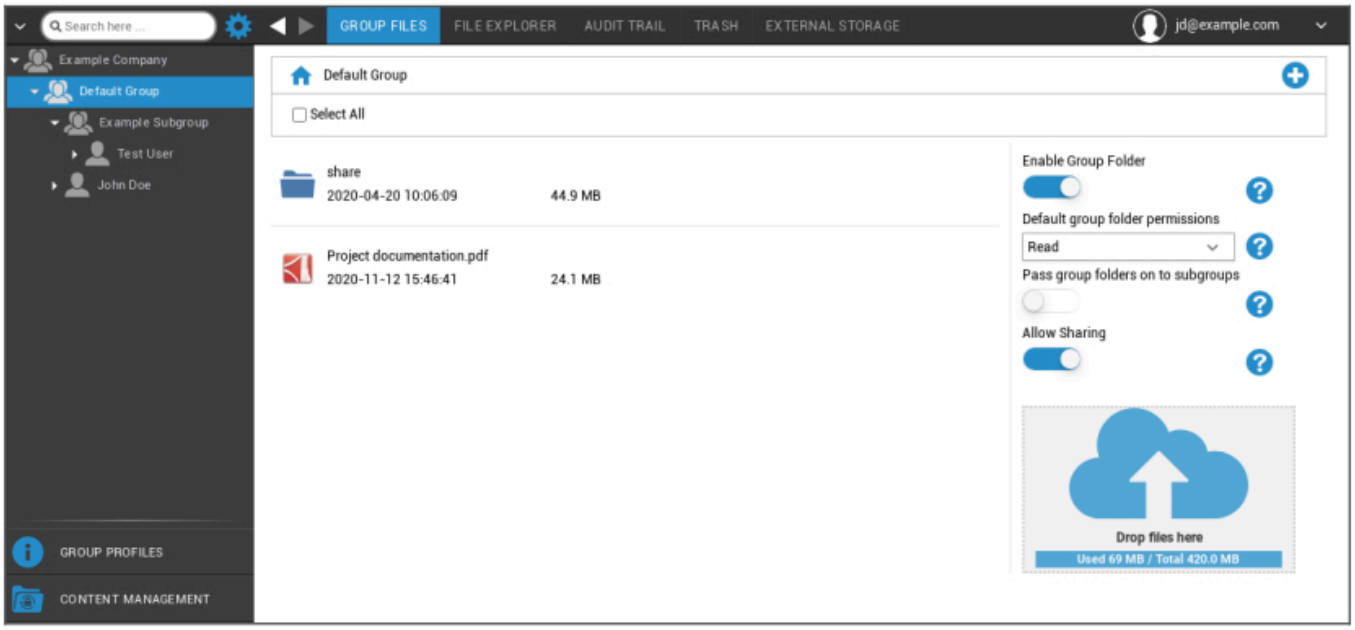
Управління контентом

Коли ви перебуваєте в групі, ви можете керувати ContentBox AppTec за допомогою "Керування вмістом".

За допомогою Content Box ви можете безпечно поширювати документи та інші корпоративні дані на пристрої кінцевих користувачів.

Файли групи

"Групові файли" є фундаментальною частиною ContentBox. Тут ви встановлюєте налаштування, завантажуєте документи, створюєте нові папки тощо.



За допомогою символу у верхньому правому куті ви можете створювати нові папки, які призначаються до відповідної групи за допомогою кнопки "Додати папку".

За допомогою символу у верхньому правому куті ви можете створити нову папку через "Додати папку", яку слід призначити до відповідної групи.

Ви можете назвати папку як завгодно.

Через "Завантажити файли" ви можете завантажити дані. Тут буде відкрито ваш Standard-Explorer. Звичайно, ви можете виконати ці дві дії у кожній (під)теці.

За допомогою символу у верхньому лівому кутку ви можете повернутися до головного меню.

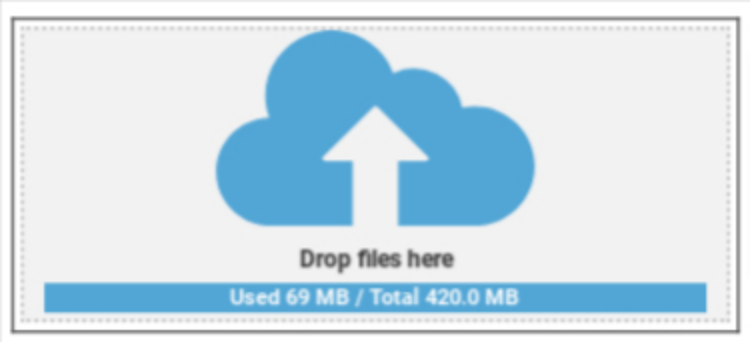
Ви можете вибрати кілька папок і файлів і завантажити їх за допомогою кнопки "Завантажити" або видалити, натиснувши кнопку "Видалити".

Ви також можете виділити всі файли і папки з і виконати команди "Завантажити" і "Видалити".

Коли ви наведете курсор миші на папку або файл, ви побачите наступний огляд:

- За допомогою кнопки "Перейменувати" ви можете перейменувати папку/файл
- За допомогою кнопки "Завантажити" ви можете завантажити папку/файл
- За допомогою кнопки "Видалити" ви можете видалити папку/файл

Увімкнути групову папку	Якщо ця опція активована, всі учасники групи мають доступ до відповідної папки
Типові права доступу до групових папок	Дозволи користувачів у вибраній групі: Read = дозвіл тільки на читання Оновлення = дозвіл на оновлення Створити = створити дозвіл Видалити = дозвіл на видалення
Передача групових папок підгрупам	Якщо ця опція активована, відповідні підгрупи можуть мати доступ до батьківських файлів даних
Дозволи для підгруп	Дозволи користувачів у вибраній підгрупі: Read = дозвіл тільки на читання Оновлення = дозвіл на оновлення Створити = створити дозвіл Видалити = дозвіл на видалення
Дозволити спільний доступ	Якщо ця опція активована, користувач може ділитися файлами за посиланням



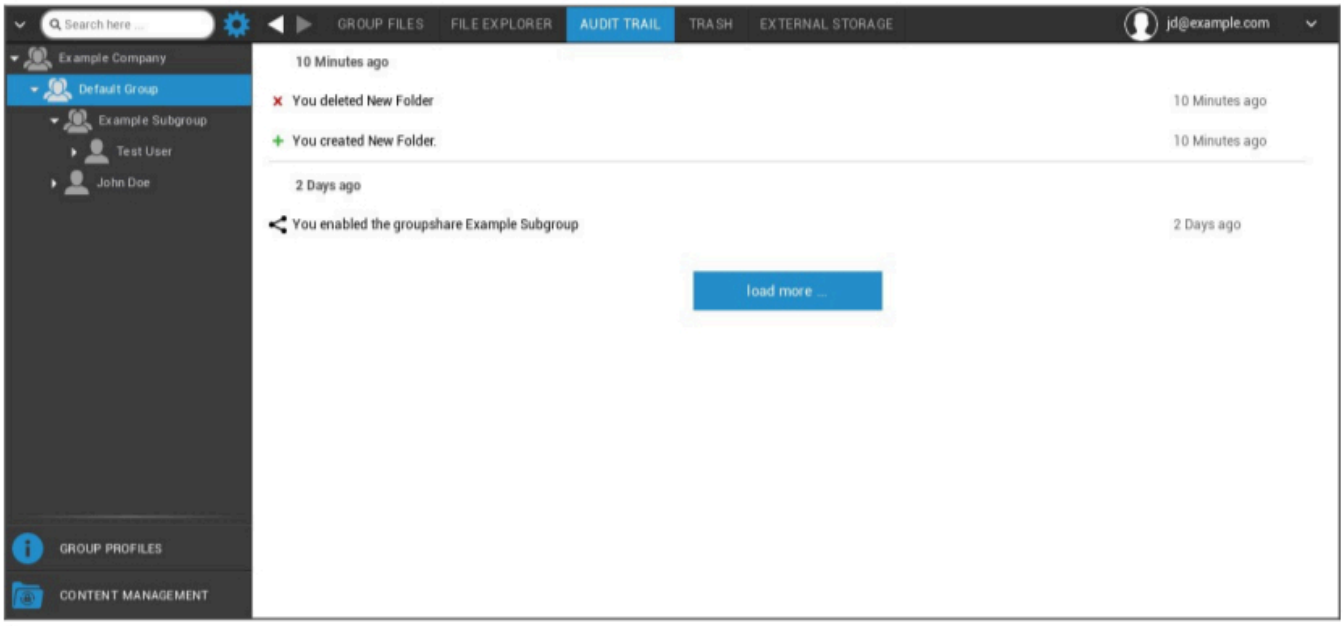
Для завантаження файлів ви можете скористатися цим полем, перетягнувши файл за допомогою Drag & Drop до цього вікна. Ви також можете натиснути на це поле, щоб вибрати і завантажити файл за допомогою Internet Explorer.

Провідник файлів

За допомогою "Провідника файлів" ви можете керувати всіма папками і файлами - незалежно від того, в якій групі вони знаходяться.

Ви також знайдете налаштування і кнопки, про які ви дізналися в розділі "Файли групи".

Аудиторський слід



В "Аудиторському сліді" ви можете побачити з історії, який користувач що створив, видалив або поділився. Таким чином, ви можете в будь-який момент встановити, що було зроблено з корпоративними даними.

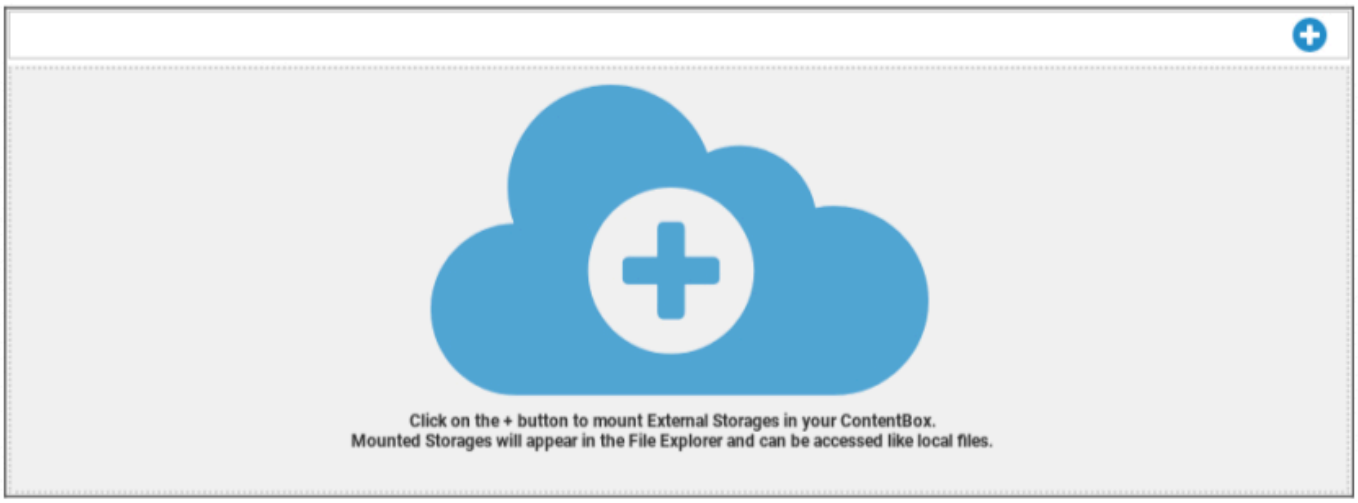
Сміття.

Якщо ви щось видалили (випадково), ви можете переглянути папки і файли в розділі "Смітник" і відновити їх відповідно до ваших побажань.

- За допомогою кнопки "Видалити" ви можете відновити дані/теку.
- За допомогою кнопки "Видалити" ви можете назавжди видалити дані/теку - для цього потрібно ще раз підтвердити команду "Видалити".

Зверніть увагу, що обсяг пам'яті, який використовується в кошику, зменшує доступний "Загальний простір" - це вимога ownCloud.

Зовнішня пам’ять



Під заголовком "Зовнішній накопичувач" ви можете підключити зовнішній накопичувач.

За допомогою символу можна додати (додаткове) сховище.

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

Amazon S3	
Ім'я користувача	Відображати ім'я
Ключ доступу	Ключ доступу
Секретний ключ	Ключ безпеки
Відро.	Точна ідентичність підпапки, яка була вам призначена
Ім'я хоста (необов'язково)	Ім'я хоста (необов'язково)
Порт (необов'язково)	Порт (необов'язково)
Регіон	Регіон (необов'язково)
Увімкнути SSL	Увімкнути SSL
Увімкнути стиль контуру	Очистити призначену вам адресу шляху

FTP	
Ім'я користувача	Відображати ім'я
Ведучий	Адреса хоста
Ім'я користувача	Ім'я користувача
Пароль	Пароль
Корінь	Головне меню
Безпечний ftps://	

SFTP	
Ім'я користувача	Відображати ім'я
Ведучий	Адреса хоста
Ім'я користувача	Ім'я користувача
Пароль	Пароль
Корінь	Головне меню

ownCloud	
Ім'я користувача	Відображати ім'я
URL	URL-адреса власної хмари
Ім'я користувача	Ім'я користувача
Пароль	Пароль
Віддалена підпапка	Стандартна папка
Захистіть https://	

WebDAV	
Ім'я користувача	Відображати ім'я
URL	URL-адреса WebDAV
Ім'я користувача	Ім'я користувача
Пароль	Пароль
Корінь	Головне меню
Захистіть https://	
Спільний доступ до Windows	Підтримка Windows Share буде доступна найближчим часом
SharePoint	Підтримка Microsoft SharePoint буде доступна найближчим часом

Журнал аудиту

Тут ви можете знайти журнал, який записує інформацію про дії, що виконуються в консолі MDM.

За допомогою іконки фільтра ви можете застосувати фільтри до відображуваного списку.

За допомогою випадаючого меню **Елементи на сторінці**: ви можете вибрати кількість елементів, які будуть відображатися на одній сторінці списку.

Вжито заходів / Змінено налаштування	Дія, яку було вжито / Налаштування, яке було змінено
Значення	Значення виконаної дії / зміненого налаштування
Користувач	Ім'я користувача, який виконав дію / змінив налаштування
Дата	Мітка часу, коли було виконано цю дію / змінено це налаштування
Шлях / Тип	Шлях до місця, де було виконано цю дію / змінено цей параметр

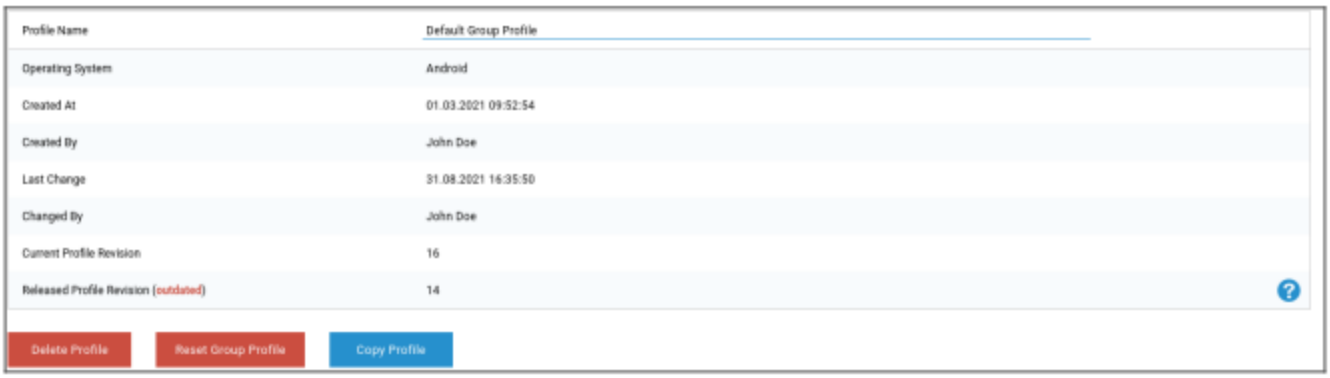
Конфігурація iOS

Генерал

Залежно від того, яку групу або пристрій ви вибрали, дисплей та його підпункти відрізняються - будь ласка, зверніть на це увагу!

Огляд профілю групи (тільки на рівні групи)

При відкритті профілю групи ви отримаєте швидкий огляд профілю



Ім'я профілю Ім'я профілю	Назва профілю (можна змінити тут)
Операційна система	Операційна система, для якої призначений профіль
Створено в	Час створення
Створено	Творець профілю
Остання зміна	Час останньої зміни профілю
Змінено	Обліковий запис, який вніс останні зміни
Поточна редакція профілю	Перегляд стану збереженого профілю
Випущено ревізію профілю	Призначена версія профілю ("Призначити зараз"). Якщо за текстом мітки вказано "(застаріла)", це означає, що ви зберегли профіль, але ще не призначили його, тому пристрої все одно отримають старішу версію.

Загальна інформація

Якщо ви перебуваєте безпосередньо на пристрої, ви отримаєте короткий огляд вибраного пристрою.

Назва пристрою	Назва пристрою
Номер телефону	Номер телефону пристрою
Модель	Номер моделі
Операційна система	ОС
Серійний номер	Серійний номер пристрою
Право власності на пристрій	Корпоративний або приватний пристрій Корпоративний = корпоративний пристрій Працівник = приватний пристрій
Тип пристрою	Тип пристрою (планшет або телефон)
Зламана в'язниця.	Якщо на пристрої є джейлбрейк
Під наглядом	Вказує, чи це пристрій під наглядом
Дотримується	Якщо були порушені будь-які правила
Востаннє бачили	Статус, коли пристрій востаннє виходив на зв'язок із сервером AppTec360

Налаштування

Ці налаштування містять ім'я пристрою та попередньо визначений фон.

Назвати пристрій на ім'я системи	Ім'я, яке буде видано в консолі AppTec360 (в лівій ієрархічній структурі), буде таким же, як і на відповідному пристрої кінцевого користувача (можна переглянути в налаштуваннях пристрою)
Використовуйте власні шпалери (лише для пристроїв під наглядом)	Тут ви можете заздалегідь визначити фон, який буде відображатися на пристрої кінцевого користувача (наприклад, для корпоративного брендування пристрою) Доступно тільки в режимі під наглядом!
Автоматичне оновлення ОС	Примушує оновлювати ОС, якщо це можливо. Тільки для пристроїв DEP у контрольованому режимі.
Користувацькі шрифти	Тут ви можете додати власні шрифти.
Ім'я	Необов'язково. Видима користувачеві назва шрифту. Це поле буде замінено на справжню назву шрифту після встановлення.
Шрифт	Завантажте файл шрифту (.otf або .ttf).

Ревізія конфігурації

Тут ви отримаєте огляд того, який профіль групи призначено пристрою.

Якщо ви натиснете на профіль групи, ви отримаєте доступ безпосередньо до профілю і зможете виконати налаштування.

За допомогою цього символу ви можете повернути призначені програми до налаштувань профілю групи.

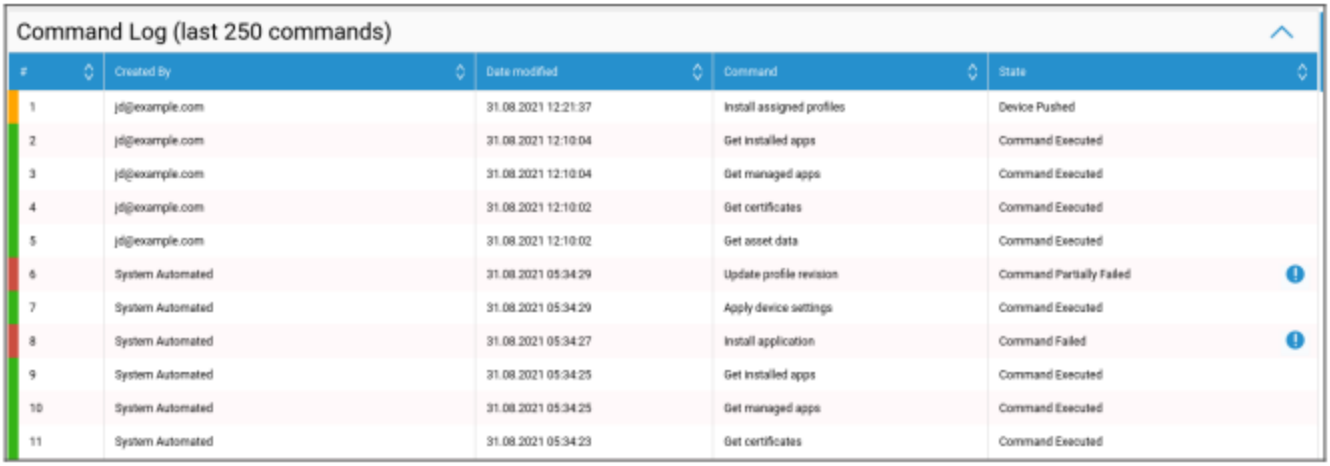
За допомогою цього символу ви можете скинути профіль пристрою, щоб він не мав жодних налаштувань.

"Доступна новіша версія" вказує на те, що профіль групи було змінено та збережено, але не призначено. Щоб застосувати зміни до пристроїв, профіль групи потрібно призначити за допомогою "Призначити зараз" на рівні групи.

Журнал пристрою (тільки на рівні пристрою)

Командний журнал

Тут ви можете побачити, які команди були видані для пристрою і який їхній статус.



Команди, створені за допомогою "Автоматизації системи", автоматично створюються системою.

Можливі стани команди

Пристрій натиснуто	До служби push (наприклад, APNS) було надіслано push-запит, щоб повідомити пристрій про необхідність з'єднатися з сервером EMM.
Команду створено	Команда була створена в системі.
Команду відправлено.	Команда була надіслана на пристрій після того, як він підключився до сервера.
Команду виконано	Команда була успішно виконана.
Команда не спрацювала	Команда не спрацювала. *
Команда частково не виконана	Залежно від операційної системи пристрою деякі команди можуть бути згруповані разом. У цьому деякі частини цієї командної групи зазнали невдачі. *
Команда виконана, але зрештою не спрацювала	Команда була виконана, але, можливо, не була.
Команда "Відсіч	Команду було перевиконано користувачем.
Викинуто	Команду було відкинуто. Наприклад, її було замінено іншою командою або пристрій було перереєстровано, а старі команди видалено

Якщо за повідомленням стоїть знак оклику, ви можете отримати додаткову інформацію, навівши курсор на іконку.

Управління активами (тільки на рівні пристрою)

Управління активами (тільки на рівні пристрою)

Інформація про пристрій

Модель	Номер моделі пристрою
Операційна система	ОС
Версія ОС	Версія операційної системи
Серійний номер	Серійний номер
UDID	UDID пристрою
Назва пристрою	Назва пристрою
Під наглядом	Показує, чи перебуває пристрій під наглядом
Стан акумулятора	Стан акумулятора

Wi-Fi

IP-адреса	IP-адреса пристрою
MAC-адреса WiFi	MAC-адреса WiFi

Стільниковий зв’язок

Статус	Статус (наявність SIM-карти)
Номер телефону	Номер телефону
Статус роумінгу	Поточний статус у роумінгу
Роумінг (голос/дані)	Статус роумінгу для голосу/даних
IP-адреса	IP-адреса
IMEI	IMEI-номер
Оператор/перевізник	Постачальник послуг стільникового зв'язку
Мережа оператора SIM-карти	Мережа оператора SIM-карти
Версія для носія	Версія для носія
Прошивка модему	Прошивка модему
Поточний ГХК/МНК	Див. розділ "SIM MCC/MNC"
SIM MCC/MNC	Мобільний код країни - це встановлена МСЕ ідентифікація країни відповідно до стандарту E.212, яка разом з кодом мобільної мережі (MNC) використовується для ідентифікації стільникової мережі (=код країни). Коли ви переходите в іншу стільникову мережу, "Поточний MCC/MNC" і "SIM MCC/MNC" будуть відрізнятися.

Bluetooth

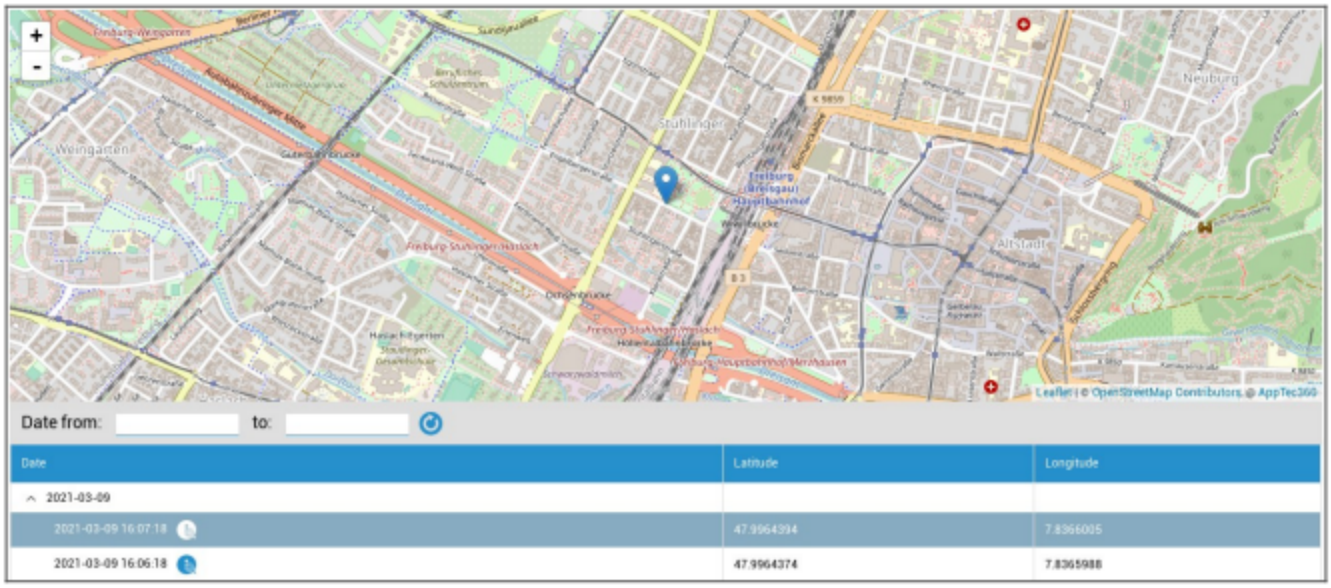
MAC-адреса Bluetooth	MAC-адреса Bluetooth

Управління безпекою

Захист від крадіжок (лише на рівні пристрою)

Інформація про GPS (лише на рівні пристрою)

Тут ви можете оцінити поточне/останнє місцезнаходження пристрою. Локалізацію можна захистити одним або навіть двома паролями - Див: Загальні налаштування - Конфіденційність - Доступ до GPS



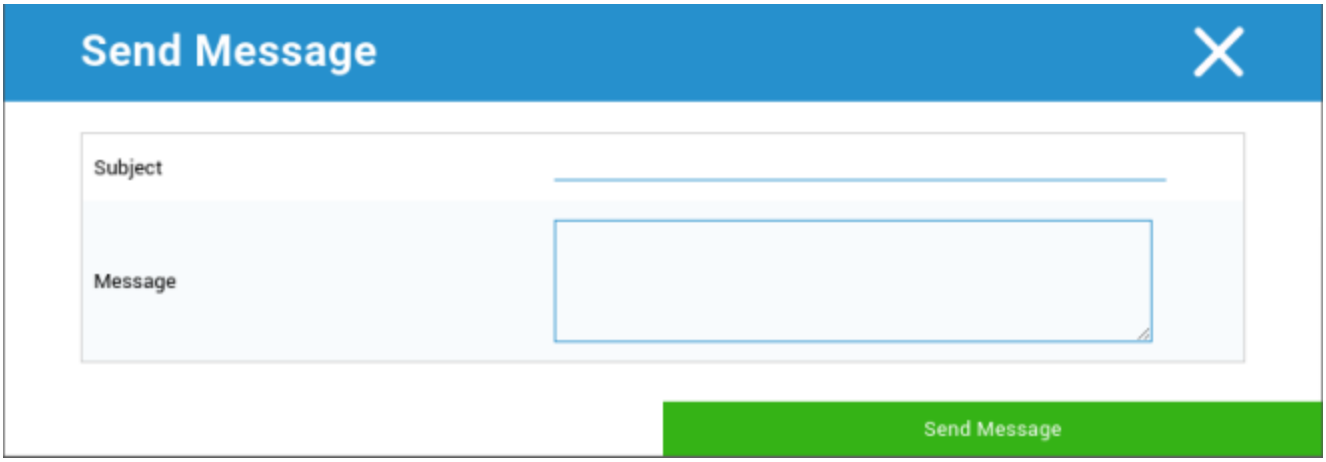
Wipe & Lock (тільки на рівні пристрою)

У розділі "Витирання та блокування" ви можете виконати наступні три дії:

Повне витирання	Пристрій відновлюється до заводських налаштувань (видаляються корпоративні, а також особисті дані)
Enterprise Wipe	З пристрою кінцевого користувача видаляються лише корпоративні дані (всі додатки, дані тощо, які були надані AppTec)
Екран блокування	Блокування екрану активоване, достатньо розблокувати пристрій за допомогою пароля/коду пристрою
Блокування для судмедекспертів (лише для пристроїв під наглядом)	Якщо цю функцію активувати за допомогою символу  , пристрій буде заблоковано, з'явиться повідомлення, яке неможливо закрити. Працівник також не зможе розблокувати пристрій. Тільки адміністратор може розблокувати пристрій у консолі за допомогою символу розблокування  .
Увімкнути блокування активації (лише для пристроїв під наглядом)	Якщо цю функцію увімкнено, пристрій буде заблоковано, щойно в налаштуваннях iCloud буде увімкнено функцію "Знайти мій iPhone".

Повідомлення (тільки на рівні пристрою)

У наступному вікні ви можете заповнити тему і текст повідомлення та надіслати його на пристрій кінцевого користувача:



Конфігурація безпеки

Пароль

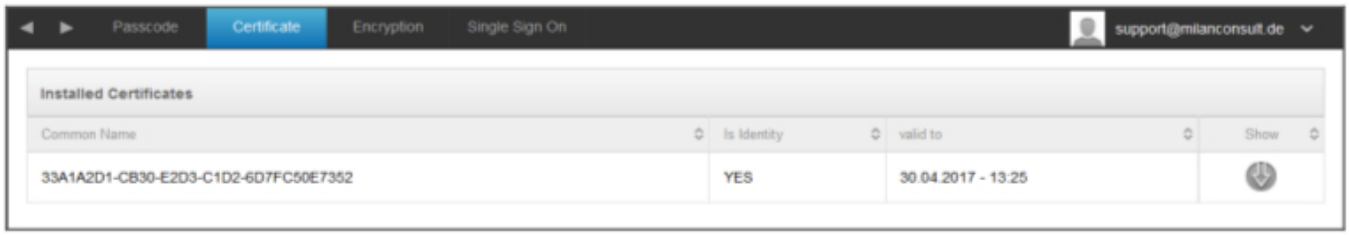
Тут ви встановлюєте налаштування пароля пристрою

Деактивація коду дозволена	Коли цей параметр активовано, запит на введення пароля не з'являється Після встановлення пароля його неможливо деактивувати
Дозволити просте значення	Дозвольте користувачеві використовувати однакові, зростаючі та спадаючі рядки чисел (наприклад, 1234, 1111)
Потрібне буквено-цифрове значення	Паролі повинні містити принаймні одну літеру
Мінімальна довжина пароля	Мінімальна довжина пароля
Мінімальна кількість складних символів	Мінімальна кількість алфавітно-цифрових символів у паролі
Максимальний вік пароля	Кількість днів, після закінчення яких необхідно змінити пароль
Максимальне автоматичне блокування	Максимальний час, після якого пристрій буде заблоковано
Максимальний пільговий період для блокування пристрою	Час, після якого пристрій переходить у заблокований режим очікування
Максимальна кількість невдалих спроб	Визначає, як часто можна вводити пароль неправильно, перш ніж буде виконано повне очищення пристрою
Максимальний вік паролю (1-730 днів)	Максимальний вік пароля
Історія паролів (1-50 паролів)	Після цього номера дозволяється використовувати старий пароль

Натискання на смітник відкриває діалогове вікно "Скидання пароля", за допомогою якого можна стерти забутий пароль пристрою.

Сертифікат (тільки на рівні пристрою)

Відображає сертифікати, доступні на пристрої


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

Шифрування

Вимагати шифрування сховища	Увімкніть функцію шифрування встановленого пристрою

Єдиний вхід

У пункті "Single Sign-On" ви можете налаштувати аутентифікацію Kerberos.

Тут ви встановлюєте облікові дані доступу та відповідні URL-адреси/програми, яким дозволено використовувати токени Kerberos.

Доступно в контрольованому режимі	
Назва облікового запису	Назва облікового запису
Ім'я керівника	Унікальна ідентичність, на яку можна розповсюджувати квитки Kerberos
Царство	Ваша область Kerberos, яка буде використовуватися (наприклад, ваш домен)

За допомогою символу ви можете створювати додаткові URL-адреси.

Шаблон URL-адреси, що використовується для обмеження цього облікового запису	Потрібно визначити URL-адреси, на які можна розповсюджувати Kerberos Tickets

За допомогою Символу ви можете встановити додаткові програми.

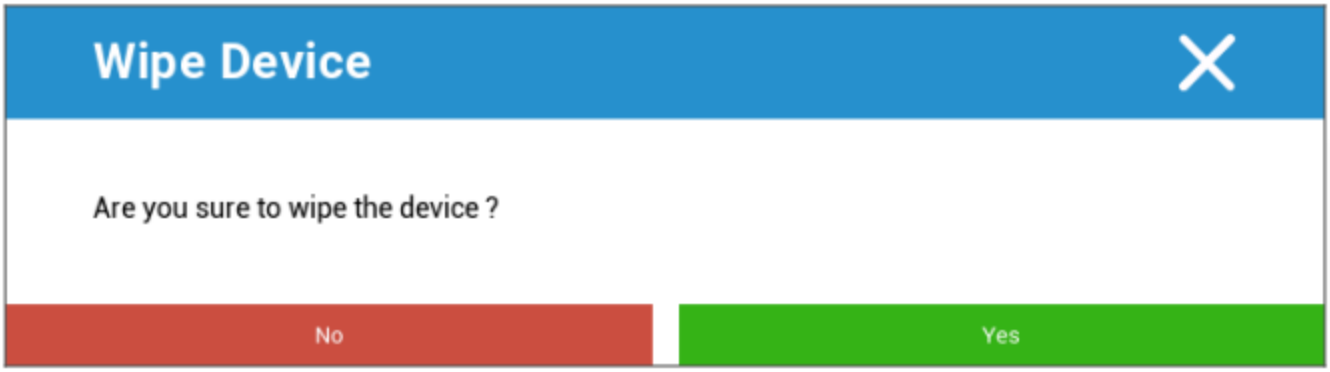
Додатки для обмеження цього облікового запису	Буде визначено додатки, на які можна розповсюджувати квитки Kerberos

Кінець життя (тільки на рівні пристрою)

Витирання (тільки на рівні пристрою)

У розділі "Видалити" ви можете відновити заводські налаштування пристрою. При цьому на пристрої кінцевого користувача будуть видалені як корпоративні, так і приватні дані.

При натисканні на "Символ мінус" ви повинні отримати наступне повідомлення



За допомогою "Так" ви можете виконати стирання.

У розділі "Звіт про витирання" можуть відображатися такі елементи

Витерто	Історія про те, хто виконував стирання
Дата	Дата
Статус	Статус (наприклад, якщо очищення було виконано успішно)

Налаштування обмежень

Функціональність пристрою

Тут ви можете заблокувати окремі функції пристрою кінцевого користувача

Дозволити встановлення програм	Дозволити встановлення додатків
Увімкнути камеру	Дозвольте використовувати камеру
Увімкнути FaceTime	Увімкнути FaceTime
Дозволити знімок екрана	Дозволити знімок екрана
Дозволити автоматичну синхронізацію в роумінгу	Дозволити автоматичну синхронізацію в роумінгу
Дозволити Siri	Дозволити Siri
Дозволити голосовий набір	Дозволити голосовий набір
Дозволити покупку в додатку	Дозволити покупку в додатку
Вимагати пароль від iTunes Store для всіх покупок	Вимагати пароль від iTunes Store для всіх покупок
Дозволити багатокористувацьку гру	Дозволити багатокористувацьку гру
Дозволити додавання друзів Game Center	Дозволити додавання друзів Game Center
Дозволити відкриття з керованого на некерований	Дозволити відкриття вмісту в керованих програмах у некерованих програмах
Дозволити відкриття з некерованого на керований	Дозволити відкриття вмісту в некерованих програмах у керованих програмах
Дозволити перегляд сьогоднішнього дня на екрані блокування	Коли цей параметр активний, подання "Сьогодні" відображатиметься в Центрі сповіщень на екрані блокування
Дозволити центр керування на екрані блокування	Увімкнути Центр керування на екрані блокування
Дозволити TouchID	Дозволити TouchID
Дозволити бездротове оновлення PKI	Дозволити бездротове оновлення PKI

Дозволити пропуск, коли він заблокований	Дозволити доступ до пароля, коли пристрій заблоковано
Обмежити відстеження реклами	Ця функція деактивує відстеження реклами (наприклад, рекламодавці не можуть використовувати відстеження реклами для розповсюдження персоналізованої реклами)
Дозволити передачу	Дозволити передачу
Дозвольте інтернет-результатам бути в центрі уваги	Дозвольте інтернет-результатам бути в центрі уваги (наприклад, Bing або Вікіпедія)
Вимагати пароль під час першого створення пари AirPlay	Вимагати пароль під час першого створення пари AirPlay
Захист зап'ястя годинника Force Watch	Якщо ця функція активована, Apple Watch змушений використовувати "Захист зап'ястя" (розпізнавання зап'ястя)
Увімкнути фототеку iCloud	Дозволяє використовувати медіатеку iCloud. Якщо не дозволено, то всі фотографії, які не були повністю завантажені з iCloud, будуть стерті на локальному сховищі
Доступно в режимі під наглядом	
Дозволити зміну облікового запису	Дозволити модифікацію "пошти, контактів, календаря"
Дозволити AirDrop	Дозволити AirDrop
Дозволити модифікацію клітин додатку	Цей параметр блокує налаштування, для яких програмам дозволено використовувати мобільні дані Цей параметр можна, наприклад, встановити вручну на пристрої кінцевого користувача, а потім активувати це обмеження
Дозвольте Siri запитувати створений користувачем вміст з Інтернету	Веб-пошук на певних сайтах заблоковано, наприклад, у Вікіпедії, оскільки кожен може вносити зміни на свій розсуд
Увімкнути фільтр ненормативної лексики Siri	Ненормативна лексика, спрямована на Siri, цензурується
Дозволити iBook Store	Дозволити iBook Store
Дозволити iBook Store Еротика	Дозволити iBook Store Еротика

Дозволити зміну налаштувань "Знайти моїх друзів	Дозволити зміну налаштувань "Знайти моїх друзів
Увімкнути ігровий центр	Увімкнути ігровий центр
Дозволити створення пари з хостом	Керуйте сполученням комп'ютера
Дозволити встановлення профілів конфігурації	Дозволяє встановлювати профілі конфігурації
Дозволити видалення програми	Видалення програм керування
Дозволити iMessage	Дозволити iMessage
Дозволити видалити весь вміст і налаштування	Дозволяє видаляти весь вміст і налаштування
Дозволити налаштування обмежень	Дозволити налаштування обмежень
Дозволити подкаст	Дозволити подкаст
Дозволити пошук визначень	Дозволити пошук визначень
Увімкнути предиктивну клавіатуру	Увімкнути предиктивну клавіатуру
Дозволити автокорекцію	Дозволити автокорекцію
Дозволити встановлення додатку UI	Якщо цю функцію вимкнено, програми не можна буде інсталювати з загальнодоступного магазину AppStore (піктограма більше не відображатиметься). Однак програми все ще можна інсталювати за допомогою iTunes та Конфігуратора
Дозволити комбінації клавіш	Дозволити комбінації клавіш, якщо пристрій підключено до фізичної клавіатури
Дозволити сполучення з Apple Watch	Забороняє сполучення між пристроєм та Apple Watch, існуючі з'єднання будуть розірвані
Дозволити зміну пароля	Якщо це заборонено, жоден пароль пристрою не може бути доданий, змінений або видалений
Дозволити зміну назви пристрою	Вказівки щодо визначення того, чи можна змінювати назву пристрою
Дозволити зміну шпалер	Як визначити, чи можна змінювати шпалери
Дозвольте автоматичне завантаження додатків	Якщо деактивувати цю функцію, придбана програма не буде автоматично встановлюватися на інші пристрої. Не стосується

	оновлень для наявних програм
Дозволити новини	Дозволити новини на пристрої iOS
Дозволити довіру до корпоративних додатків	Якщо встановлено значення false, забороняє довіряти корпоративним програмам

iCloud

Блокування певних функцій під час створення пари з iCloud

Дозволити резервне копіювання	Дозволити резервне копіювання
Дозволити синхронізацію документів	Дозволити синхронізацію документів
Дозволити фотопотік	Дозволити фотопотік
Дозволити спільний потік фотографій	Дозволити спільний потік фотографій
Дозволити хмарну синхронізацію брелока	Дозволити хмарну синхронізацію брелока
Дозвольте керованим програмам зберігати дані	Дозвольте керованим програмам зберігати дані
Дозволити синхронізацію нотаток і виділень для корпоративних книг	Дозволити синхронізацію нотаток і виділень для корпоративних книг
Дозволити резервне копіювання книг підприємства	Дозволити резервне копіювання книг підприємства

Безпека та конфіденційність

Блокування цих функцій, пов'язаних з діагностичними даними

Дозволити надсилання діагностичних даних до Apple	Дозволити надсилання діагностичних даних до Apple
Дозволити користувачеві приймати ненадійні сертифікати TLS	Дозволити користувачеві приймати ненадійні сертифікати TLS
Примусове шифрування резервних копій	Примусове шифрування резервних копій

BYOD

Вбудований захист iOS (контейнер)

iOS завжди вміла розрізняти керовані (ділові) та некеровані (приватні) дані. Все, що надходить з системи MDM, вважається керованим. Наприклад, якщо ви встановлюєте додаток через MDM або налаштовуєте обліковий запис Exchange, це буде вважатися керованим iOS.

Все інше, що налаштовується/встановлюється на пристрій вручну, буде вважатися некерованим. Наприклад, якщо користувач самостійно встановлює WhatsApp або додає обліковий запис Exchange. Однак цей поділ ніколи не впливав на контакти. Але починаючи з iOS 11.3 (і вище) це також було додано для контактів.

Оскільки це базова функція операційної системи, вам не потрібно нічого встановлювати або налаштовувати спеціальний контейнер.

Увімкніть вбудовану функцію для розділення приватних і службових програм/інформації/файлів. Цей параметр також вимкне деякі інші функції, які можуть помилково вимкнути частину цього поділу.

Активація

Активуйте контейнерні рішення, які підтримуються AppTec360

Увімкнути Google Divide Container	Увімкнути Google Divide Container
Увімкнути контейнер SecurePIM	Увімкнути контейнер SecurePIM

Якщо ви активували SecurePIM Container, ви також знайдете наступний пункт у розділі "Активація". Крім того, одразу відкриються ще чотири вкладки, які описані нижче.

Адреса електронної пошти служби підтримки	Адреса електронної пошти підтримки, куди користувач може звернутися з проблемами

Пароль SecurePIM

У розділі "Пароль SecurePIM" ви можете встановити рекомендації щодо надійності пароля.

Тайм-аут сеансу	Тут ви можете встановити, через скільки хвилин потрібно ввести новий пароль, коли SecurePIM працює у фоновому режимі
Довжина пароля	Довжина пароля для доступу до контейнера SecurePIM
Символи верхнього регістру	Мінімум символів верхнього регістру
Малі літери	Мінімум символів нижнього регістру
Спеціальні символи	Мінімум спеціальних символів
Цифри	Мінімальні цифри
Застосування для протирання	Скільки разів можна ввести пароль неправильно, перш ніж вміст SecurePIM буде видалено (Додаток, однак, залишається на пристрої кінцевого користувача)

Безпека SecurePIM

У розділі "Безпека SecurePIM" ви можете встановити різні налаштування безпеки.

Виявлення зламаних пристроїв	Якщо цей параметр увімкнено, доступ до SecurePIM Container буде заблоковано, як тільки пристрій буде виявлено як зламаний
Захищені текстові поля	Вміст полів відправки буде зашифровано, ніяка інформація не потрапить до ОС (iOS) Примітка: Поки цей параметр активний, автокорекція буде недоступна
Експорт контактних даних на пристрій	Якщо цей параметр увімкнено, користувачеві буде дозволено експортувати контакти Exchange на локальний пристрій Примітка: Експортуються лише ім'я та номер телефону
Показати місце проведення заходу	Якщо цей параметр увімкнено, місцезнаходження майбутніх подій буде відображатися в панелі сповіщень
Показати назву події	Якщо цей параметр увімкнено, то в рядку сповіщень буде відображатися місце розташування назви майбутньої події

Браузер SecurePIM

Тут ви можете налаштувати браузер SecurePIM.

За допомогою цього символу ви можете визначити нову URL-адресу.

За допомогою символу ви можете знову видалити визначену URL-адресу.

"Білі URL-адреси" - це URL-адреси, які можна завантажувати.

"URL-адреси з чорного списку" - це URL-адреси, які не можуть бути завантажені і, таким чином, заблоковані.

Зверніть увагу, що записи Білого списку мають вищий пріоритет, ніж записи Чорного списку. У полі "Назва закладки" ви можете вказати назву. За допомогою "URL-адреси закладки" ви можете пов'язати URL-адресу з назвою закладки - таким чином ви можете розподіляти індивідуальні закладки серед відповідних користувачів.

Обмін

У розділі "Exchange" ви можете налаштувати обліковий запис Exchange.

Адреса електронної пошти ActiveSync	Обмін електронною адресою (зверніть увагу на "Заповнювачі")
ActiveSync Exchange Логін для входу в систему	Обміняйтеся іменами користувачів (зверніть увагу на "Заповнювачі")
Сервер обміну ActiveSync	Адреса сервера обміну (FQDN)
Домен обміну ActiveSync	Адреса домену для обміну
Сертифікат користувача	Сертифікат користувача
Автентифікація на основі сертифікатів	Користувач автентифікується за допомогою сертифіката
Дозволити шифрування S/MIME	Дозволяє користувачеві шифрувати свою пошту
Дозволити S/MIME підпис	Дозволяє користувачеві підписувати свою пошту
Перевірка CRL.	Якщо він активний, приватний сертифікат буде порівняно з CRL (списком відкликання сертифікатів)

Керування з’єднаннями

Wi-Fi

Ідентифікатор набору послуг (SSID)	SSID мережі, до якої потрібно підключитися
Автоматичне приєднання	Увімкнути автоматичне приєднання при приєднанні до мережі
Прихована мережа	Активувати, якщо точка доступу не передає SSID

Налаштування проксі-сервера

Налаштування проксі для кожної точки доступу

Ні.	Не створювати проксі-сервер
Посібник	Налаштуйте проксі вручну
URL-адреса проксі-сервера	Адреса для доступу до налаштувань проксі-сервера
Порт	Встановіть порт для проксі-сервера
Аутентифікація	Ім'я користувача для автентифікації на проксі
Пароль	Пароль для автентифікації на проксі
Автоматично	Автоматичне створення проксі-сервера
URL-адреса проксі-сервера	URL для доступу до налаштувань проксі-сервера

Тип безпеки

Встановіть тип безпеки для точки доступу

WEP	
Пароль	Пароль для точки доступу

WPA/WPA2	
Пароль	Пароль для точки доступу

WEP Enterprise - WPA / WPA2 Enterprise - будь-яке підприємство		
Протоколи		
TLS	Активувати/деактивувати	
TTLS	Активувати/деактивувати	
ПІК!	Активувати/деактивувати	
PEAP	Активувати/деактивувати	
EAP-FAST	Активувати/деактивувати	
EAP-SIM	Активувати/деактивувати	
Використовуйте PAC		Використання PAC (Protected Access Control)
Положення PAC	Конфігурація Provision PAC	
Надання PAC Анонімно	Анонімне надання ГРД	
Внутрішні автентифікації	Протокол автентифікації, який слід використовувати: PAP, CHAP, MSCHAP, MSCHAPv2	
Ім'я користувача	Ім'я користувача для аутентифікації	
Не використовуйте пароль для кожного з'єднання	Не використовуйте пароль для кожного з'єднання	
Посвідчення особи	Завантаження/вибір сертифіката автентифікації	
Зовнішня ідентичність	Ідентичність, яку можна побачити ззовні	
Довіра		
Довірений сертифікат 1	Завантажте перший довірений сертифікат	
Довірений сертифікат 2	Завантажте другий довірений сертифікат	
Сертифікат довіри 3	Завантажте третій довірений сертифікат	
Імена сертифікатів довірених серверів	Назви очікуваних сертифікатів сервера (у списку через кому)	

Ні.	Не встановлюйте жодних заходів безпеки

VPN

Ім'я з'єднання Ім'я з'єднання	Назва VPN-профілю

Тип VPN

VPN

Весь мережевий трафік пристрою буде маршрутизуватися через VPN-з'єднання.

Тип підключення	Встановити тип VPN-з'єднання
IPsec (cisco)	Протокол IPsec від cisco
PPTP	Протокол PPTP
L2TP	Протокол L2TP
Cisco AnyConnect	Протокол AnyConnect
Juniper SSL	Протокол Juniper SSL
F5 SSL	F5 Протокол SSL
SonicWall mConnect	SonicWall mobile Connect
Аруба VIA	Протокол Аруба VIA
Спеціальний SSL	Підключення через спеціальний SSL
OpenVPN	Протокол OpenVPN

Per-App VPN

При відкритті певного додатку буде встановлено VPN-з'єднання

Автоматично запускати VPN-з'єднання Per-App		Автоматично запускати VPN-з'єднання Per-App
Тип підключення		Встановити тип VPN-з'єднання
	Cisco AnyConnect	Протокол AnyConnect
	Juniper SSL	Протокол Juniper SSL
	F5 SSL	F5 Протокол SSL
	SonicWall mConnect	SonicWall mobile Connect
	Аруба VIA	Протокол Аруба VIA
	Спеціальний SSL	Підключення через спеціальний SSL
	OpenVPN	Протокол OpenVPN

Налаштування проксі-сервера

Налаштування проксі для VPN-з'єднання

Ні.	Не створювати проксі-сервер
Посібник	Встановлення проксі вручну
URL-адреса проксі-сервера	Адреса для доступу до налаштувань проксі-сервера
Порт	Встановіть порт для проксі-сервера
Аутентифікація	Ім'я користувача для автентифікації на проксі
Пароль	Пароль для автентифікації на проксі
Автоматично	Автоматичне створення проксі-сервера
URL-адреса проксі-сервера	URL для доступу до налаштувань проксі-сервера

Показати заповнювачі	Відображає всі доступні користувацькі змінні, які може використовувати AppTec360

APN

Назва точки доступу Ім'я точки доступу	Назва точки доступу
Ім'я користувача точки доступу	Ім'я користувача точки доступу
Пароль точки доступу	Пароль точки доступу
Проксі-сервер	Адреса проксі-сервера
Порт	Відповідний порт проксі-сервера

Стільниковий зв’язок

Увімкнути роумінг даних	Увімкнути роумінг даних
Увімкнути голосовий роумінг	Увімкнути голосовий роумінг
Увімкнути точку доступу	Увімкнути точку доступу

HTTP-проксі-сервер

Тип проксі	
Посібник	Створіть проксі вручну
URL-адреса проксі-сервера	Адреса для доступу до налаштувань проксі-сервера
Порт	Встановіть проксі-порт
Аутентифікація	Ім'я користувача для автентифікації на проксі
Пароль	Пароль для автентифікації на проксі
Автоматично	Автоматичне створення проксі-сервера
URL-адреса проксі-сервера PAC	URL-адреса проксі-сервера PAC
Дозволити пряме з'єднання, якщо PAC недоступний	Дозволити пряме підключення (без VPN), якщо PAC недоступний
Дозволити обхід проксі для доступу до кептивних мереж	Дозволити обхід проксі для доступу до внутрішніх мереж

AirPrint

IP-адреса	IP-адреса принтера
Шлях до ресурсів	Визначений шлях до пристрою AirPrint

AirPlay

Назва пристрою	Назва пристрою
Пароль	Пароль для створення пари
Білий список	Визначте список пристроїв, з якими пристрій може сполучатися виключно самостійно

Менеджмент ПІМ

Активна синхронізація Exchange Active Sync

Назва облікового запису	Ім'я облікового запису електронної пошти
Хост Exchange ActiveSync	Адреса / FQDN сервера
Дозволити рух	Дозволити переміщення імейлів
Використовувати тільки в пошті	Взаємодія може відбуватися лише у власному додатку Mail
Використовуйте SSL	Використовуйте SSL-шифрування
Домен	Домен сервера
Користувач	Ім'я користувача
Адреса електронної пошти	адреса електронної пошти (тільки на рівні пристрою)
Пароль (тільки на рівні пристрою)	Пароль користувача
Посвідчення особи	Виберіть відповідний сертифікат для автентифікації на сервері
Синхронізація пошти за минулі дні	Кількість днів, протягом яких імейли мають бути знову синхронізовані. Без обмежень = необмежений
Увімкнути S/MIME	Увімкнути шифрування S/MIME
Свідоцтво про підписання	Завантажте відповідний сертифікат підписання
Сертифікат шифрування	Завантажте відповідний сертифікат шифрування

Електронна пошта

Налаштування облікових записів POP3 / IMAP на пристрої кінцевого користувача

Опис рахунку	Ім'я облікового запису електронної пошти		
Тип рахунку	IMAP	Префікс шляху	Префікс шляху для спеціальних папок
	POP		
Ім'я користувача	Ім'я користувача		
Адреса електронної пошти	Адреса електронної пошти користувача		
Дозволити рух	Дозволити переміщення імейлів		
Увімкнути S/MIME	Увімкнути шифрування S/MIME		
Свідоцтво про підписання	Завантажте відповідний сертифікат підписання		
Сертифікат шифрування	Завантажте відповідний сертифікат шифрування		

Вхідна пошта

Вхідні налаштування сервера

Адреса поштового сервера	Адреса поштового сервера
Порт поштового сервера	Порт поштового сервера
Ім'я користувача	Відповідне ім'я користувача
Тип автентифікації	Тип автентифікації
Ні.	Немає типу автентифікації
Пароль (тільки на рівні пристрою)	Запит на введення пароля
Виклик-відповідь МДМ	
NTLM	NTLM-автентифікація
Дайджест HTTP MD5	
Використовуйте SSL	Використовуйте SSL, якщо потрібно

Вихідна пошта

Налаштування вихідного сервера

Адреса поштового сервера	Адреса поштового сервера
Порт поштового сервера	Порт поштового сервера
Ім'я користувача	Відповідне ім'я користувача
Тип автентифікації	
Ні.	Немає методу автентифікації
Пароль (тільки на рівні пристрою)	Запит на введення пароля
Виклик-відповідь МДМ	
NTLM	NTLM-автентифікація
Дайджест HTTP MD5	
Використовуйте SSL	Використовуйте SSL, якщо потрібно
Вихідний пароль такий самий, як і вхідний	Вихідний пароль такий самий, як і вхідний
Використовуйте тільки в пошті	Активуйте, якщо всі вихідні імейли мають надсилатися через Mail-App

CalDav

Налаштування створення та розповсюдження облікового запису CalDav

Опис рахунку	Відображення назви облікового запису
Ім'я хоста	Ім'я хоста та/або IP-адреса
Порт	Порт облікового запису CalDav
Основна URL-адреса	Основна URL-адреса облікового запису
Ім'я користувача	Відповідне ім'я користувача CalDav
Пароль (тільки на рівні пристрою)	Відповідний пароль CalDav
Використовуйте SSL	Використовуйте SSL, якщо потрібно

Календарі за передплатою

Створення та розповсюдження передплачених календарів

Опис	Відображення назви облікового запису
URL	URL бази даних календаря
Ім'я користувача	Ім'я користувача підписки на календар
Пароль (тільки на рівні пристрою)	Пароль підписки на календар
Використовуйте SSL	Використовуйте SSL, якщо потрібно

LDAP

У цій області налаштуйте LDAP-з'єднання, щоб дозволити динамічний обмін сертифікатами між пристроєм кінцевого користувача та Active Directory.

Зверніть увагу, що обраному користувачеві потрібен відповідний дозвіл на читання.

Опис рахунку	Опис рахунку
Ім'я користувача облікового запису	Користувач для LDAP-доступу
Пароль облікового запису	Пароль для LDAP-доступу
Ім'я хоста облікового запису	Ім'я хоста/IP-адреса сервера LDAP
Використовуйте SSL	Використовуйте SSL, якщо потрібно

У другій частині ви можете задати індивідуальні фільтри для пошуку в реєстрі LDAP.

Опис	Сфера застосування	База пошуку
Опис фільтра	Рівень пошуку в реєстрі LDAP	Визначте індивідуальний фільтр

Керування сайтом

Веб-кліпи

У цьому місці визначте закладки з посиланнями на веб-сторінки, інтранет-портали тощо, які будуть видимі як додаток на пристрої кінцевого користувача.

Етикетка	Назва з'єднання на пристрої кінцевого користувача
URL	Посилання на відповідний веб-сайт
Знімний	Якщо ця опція активована, користувач може видалити веб-кліп
Ікона	Через цей діалог завантажте логотип для з'єднання: Розміри 180x180, формат png
Готова піктограма	Якщо увімкнено, на іконці не відображатимуться додаткові ефекти (тінь, віддзеркалення)
На весь екран	При відкритті веб-кліпів браузер відкривається в повноекранному режимі

Фільтр веб-вмісту

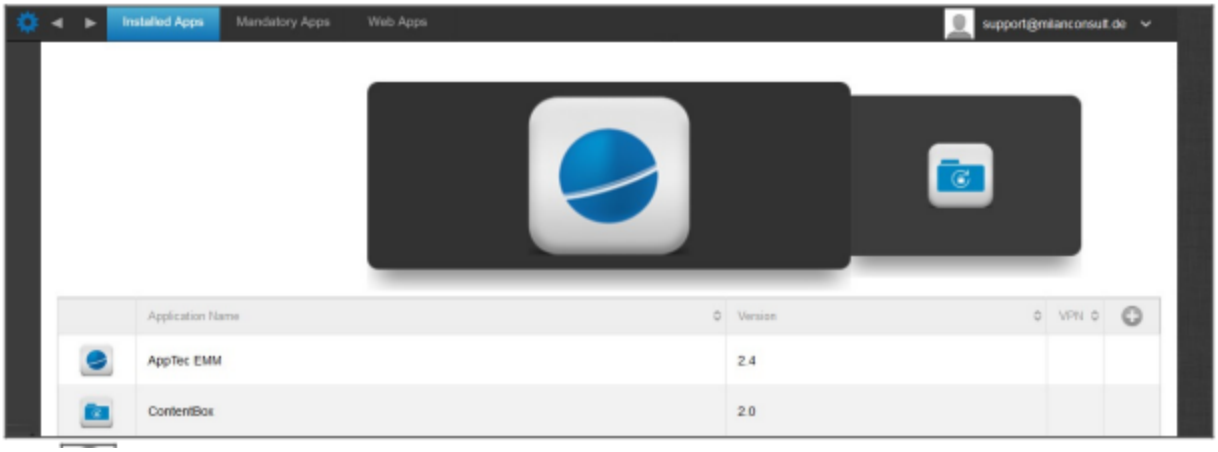
Фільтр веб-вмісту дозволяє обмежити доступ до певних інтернет-сторінок.

Дозволені веб-сайти	
Обмежити вміст для дорослих	Веб-фільтр автоматично застосовується для вмісту для дорослих
Дозволені URL-адреси	За допомогою символу + додайте дозволені сторінки
URL-адреси в чорному списку	За допомогою символу + додайте заблоковані сторінки
Тільки для певних веб-сайтів	Відображається лише певний вміст, який ви можете додати за допомогою символу +.

Керування додатками

Enterprise App Manager

Встановлені програми (лише на рівні пристрою)



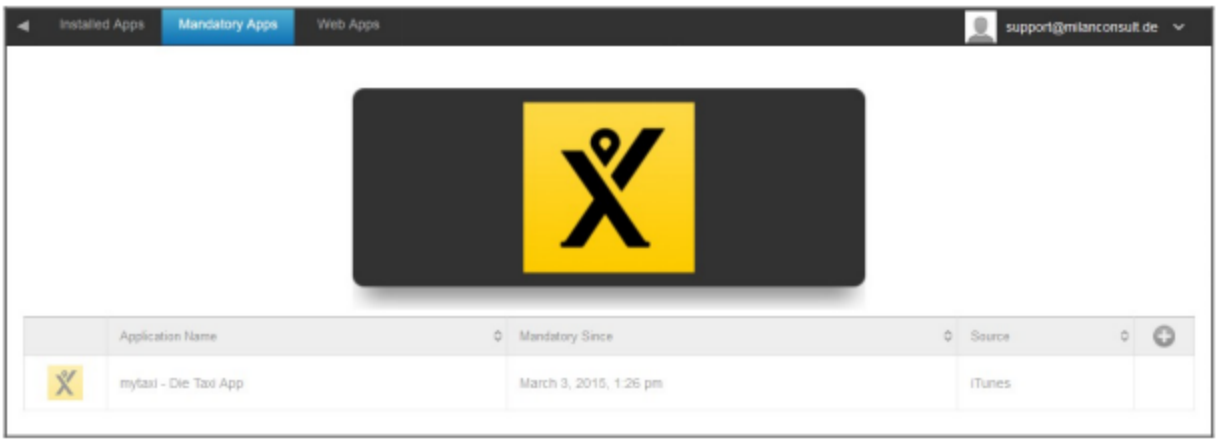
Тут ви можете побачити програми, які наразі встановлені на пристрої.

Обов’язкові програми

У розділі "Обов'язкові програми" ви можете вказати необхідні програми.

Користувач буде постійно отримувати нагадування про необхідність встановлення цього додатку.

За допомогою , можна визначити необхідний додаток.



Це може бути як додаток для Apple App Store, так і внутрішній додаток.

Якщо це стосується пристрою під наглядом, додаток буде встановлено автоматично.

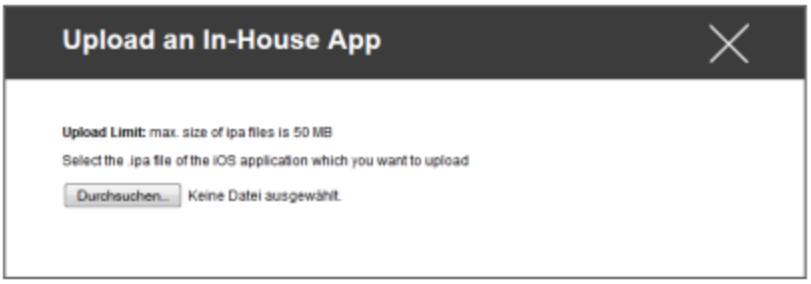
Ви можете завантажити на пристрій додаток "Apple AppStore" із загальнодоступного магазину AppStore, а також внутрішньо розроблений власний додаток.

Або ви можете вибрати категорію "Власні додатки iOS" і вибрати власний додаток, який ви завантажили в Загальних налаштуваннях.

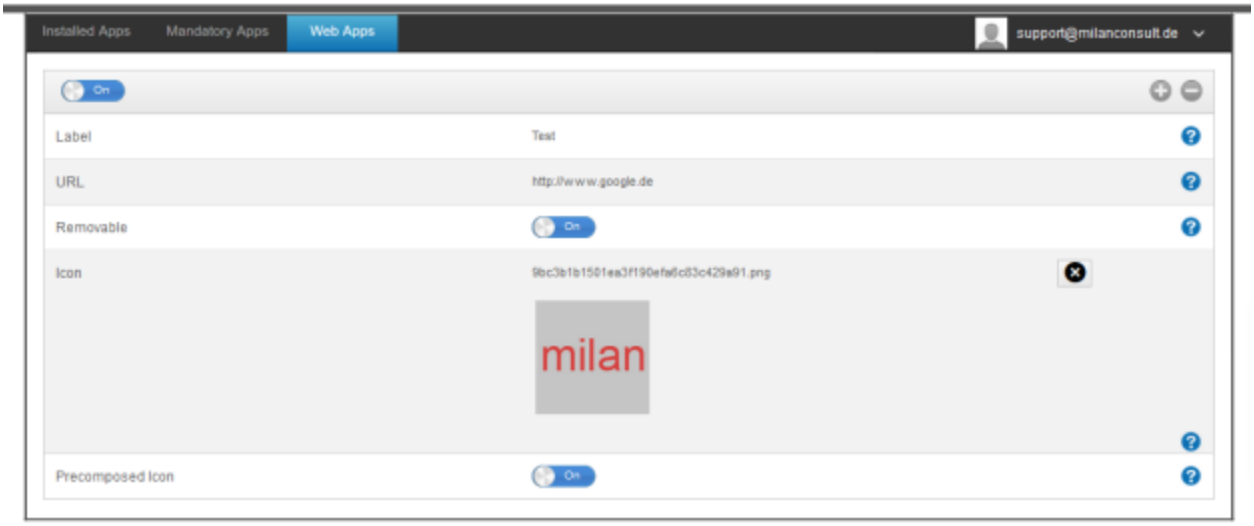
Параметри встановлення

Будьте в курсі подій (підтримується лише для VPP на пристрій)	Раз на тиждень буде визначатися, чи є оновлення для додатку. Якщо так, це оновлення буде встановлено Для власних програм буде використано ціль оновлення, яку ви налаштували у Загальних налаштуваннях.
Обганяють, коли некеровані	Якщо програма вже встановлена, MDM візьме її на себе і буде керувати нею
Видалення програми після видалення профілю MDM	У разі видалення керування пристроєм додаток буде видалено
Заборонити резервне копіювання даних програми	Резервна копія специфічних даних програми не буде створена
Налаштування програми	У розділі "Налаштування програми" ви можете призначити програмі певні значення на передньому плані (якщо програма це підтримує, за необхідності зверніться до розробника програми).

Ви також можете безпосередньо вибрати і завантажити ipa-файл через "Завантажити власний додаток".



Веб-додатки



У пункті "Веб-програми" ви можете, як і у випадку з "Веб-кліпами", перенести інтернет-сторінки або портали інтрамережі у вигляді програми на пристрій кінцевого користувача в області "Керування веб-сторінками". За замовчуванням веб-програми відображатимуться в повноекранному режимі, який можна налаштувати в пункті "Веб-кліпи".

Етикетка	Назва з'єднання на пристрої кінцевого користувача
URL	Посилання на відповідний веб-сайт
Знімний	Якщо ця опція активована, користувач може видалити веб-кліп
Ікона	Через цей діалог завантажте логотип для з'єднання: Розміри 180x180, формат png
Готова піктограма	Якщо увімкнено, на іконці не відображатимуться додаткові ефекти (тінь, віддзеркалення)

Обмеження та налаштування

Додатки з чорного списку / білого списку

Тут ви можете встановити програми, які будуть заблоковані (або дозволені) залежно від ваших налаштувань у "Загальних налаштуваннях". Натиснувши на кнопку, ви побачите вже знайомий вам пошук додатків. Там ви можете шукати програми, які хочете додати.

Зверніть увагу, що для виконання цієї функції потрібен пристрій під наглядом

Обмеження SysApp

Блокування певних програм або функцій вашого пристрою

Дозволити використання YouTube	Дозволити використання YouTube
Дозволити використання iTunes Store	Дозволити використання iTunes Store
Дозволити використання Safari	Дозволити використання Safari
Увімкнути автозаповнення	Дозволяє автозаповнення
Попередження про примусове шахрайство	Попередження про шахрайство
Увімкнути JavScript	Дозволяє використовувати JavaScript
Блокувати спливаючі вікна	Блокує всі види пуп-апів
Дозволити файли cookie	Виберіть, коли Safari прийматиме файли cookie

App-VPN

За допомогою символу ви можете визначити програми, які автоматично запускатимуть вибране VPN-з'єднання під час запуску.

Налаштування програми

У розділі "Налаштування програми" ви можете призначити програмі певні значення на передньому плані (якщо програма це підтримує, за необхідності зверніться до розробника програми).

За допомогою символу ви додаєте (додатковий) додаток. Ви знову побачите знайоме представлення AppTec360 для імпорту додатків.

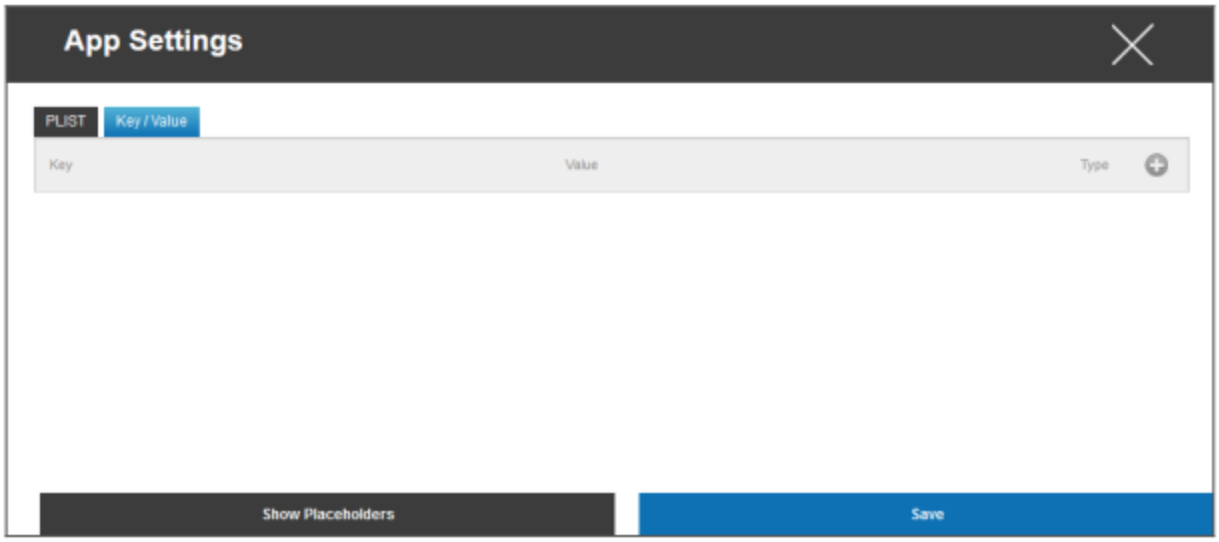
Знайдіть тут програму, яку ви хочете налаштувати, і виберіть її. Налаштування застосовуватимуться лише до програм, якими ви керуєте.

Якщо імпорт пройшов успішно, ви побачите наступне повідомлення:

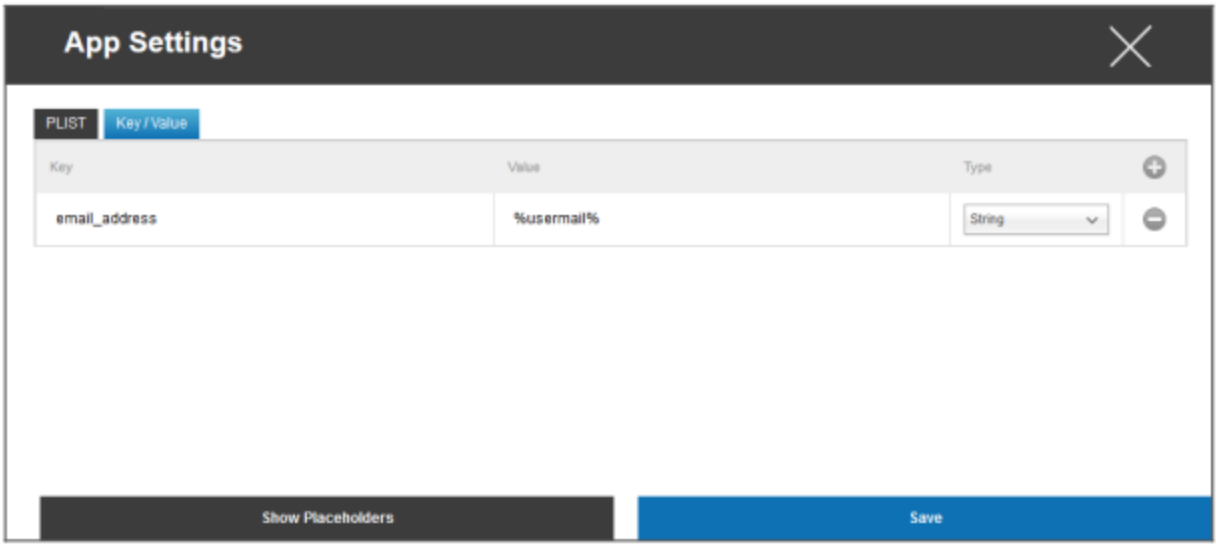
Тепер, натиснувши на , ви можете виконати різноманітні конфігурації. Після цього ви отримаєте наступний огляд:

Якщо у вас вже є PLIST (вихідний текст конфігурації), ви можете додати його сюди і зберегти все за допомогою кнопки "Зберегти".

У розділі "Ключ/Значення" ви можете прикріпити певні конфігурації до додатку



Тут ви можете встановити новий ключ і його значення за допомогою символу.



Звичайно, всі плейсхолдери AppTec у вашому розпорядженні

"Тип" пояснення:

Рядок	Текст
Булевий	Правда/Неправда
Номер	Номер

За допомогою цього символу ви можете знову видалити програму.

Enterprise App Store

Програми iTunes

У цьому пункті ви можете розповсюджувати необов'язкові програми для своїх користувачів.

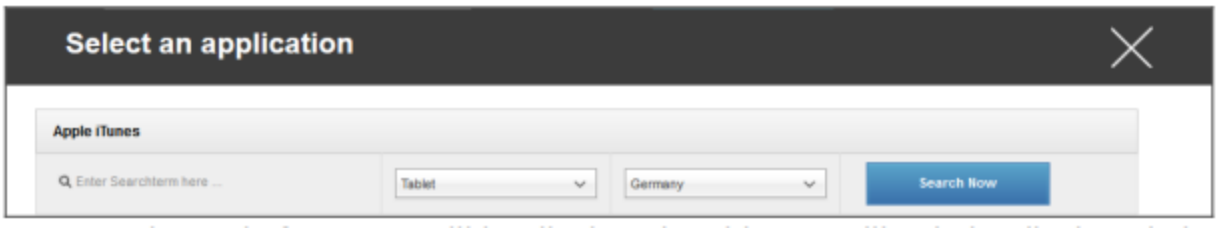
Якщо тут є додаток, він буде автоматично встановлений на кінцевий пристрій користувача в AppTec360 Store.

Це просто посилання на офіційний магазин додатків Apple. З цієї причини кожен пристрій кінцевого користувача повинен бути оснащений Apple ID.

На цьому етапі ми рекомендуємо кожному користувачеві мати власний Apple ID.

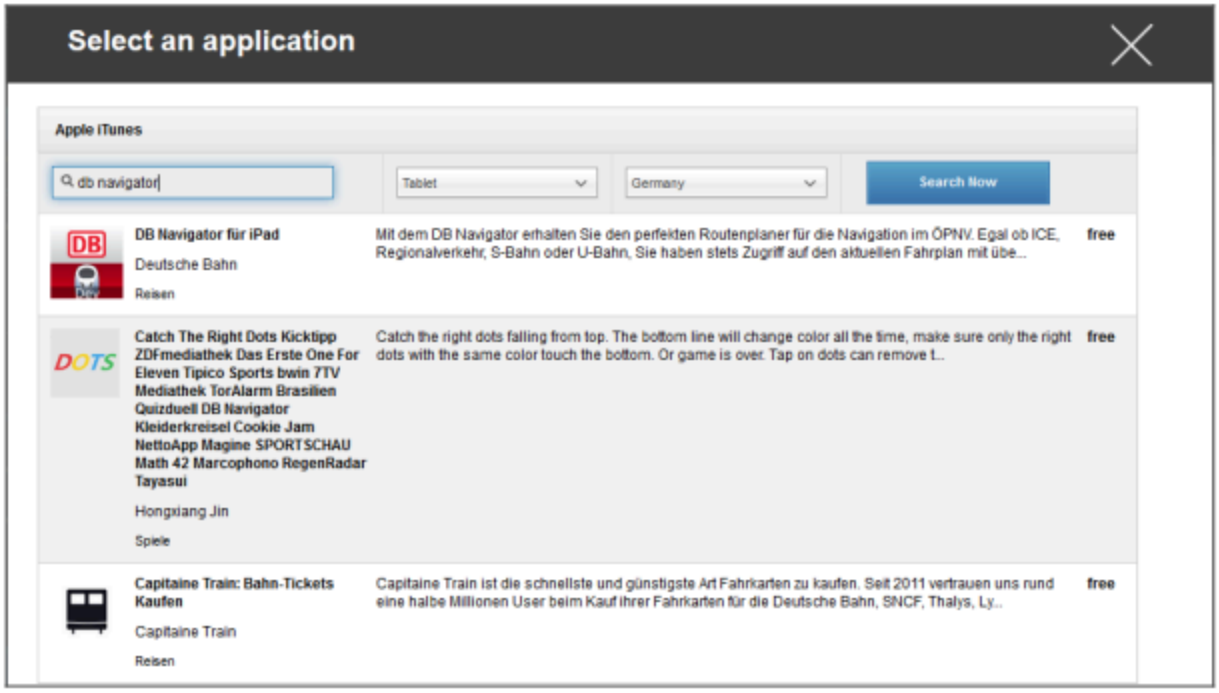
За допомогою цього символу ви можете додавати додаткові програми.

Після цього має відкритися вікно з наступним оглядом.



Зверніть увагу, що відображатимуться лише безкоштовні програми, платні програми відображатимуться лише через VPN.

У розділі "Введіть пошуковий термін тут..." ви можете шукати програму, яка є в Apple App Store.



Щойно ви натиснете на іконку або на назву програми, вам знову буде запропоновано виконати додаткові налаштування.

Будьте в курсі подій	Раз на тиждень буде визначатися, чи є оновлення для додатку. Якщо так, це оновлення буде встановлено
Видалення програми після видалення профілю MDM	У разі видалення керування пристроєм додаток буде видалено
Заборонити резервне копіювання даних програми	Резервна копія специфічних даних програми не буде створена
App-VPN	Виберіть VPN-з'єднання, яке буде запускатися при відкритті програми

Після натискання кнопки "Встановити" додаток буде додано до Enterprise App Store, а потім його можна буде встановити на пристрої кінцевого користувача через AppTec360 AppStore.

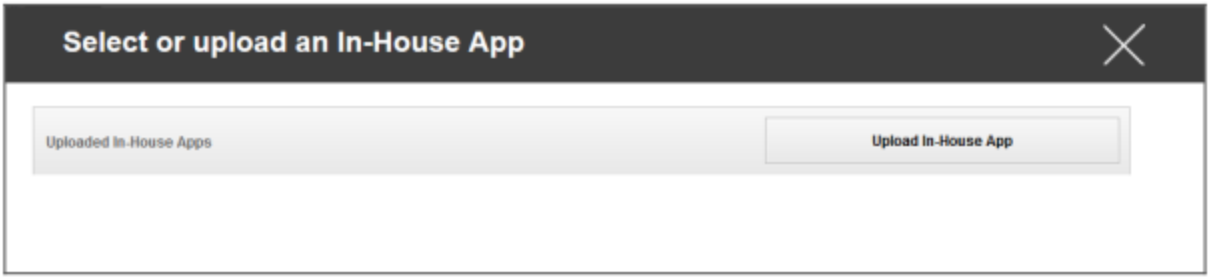
Якщо імпорт з App-Store пройшов успішно, ви отримаєте наступний огляд:

Власні сили

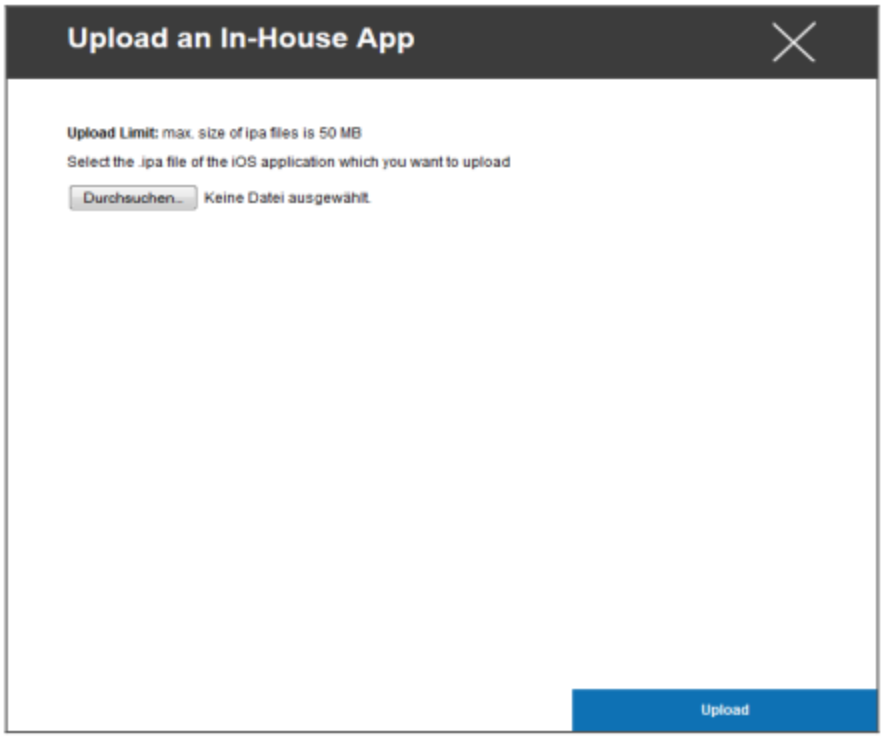
У пункті "In-house" ви можете завантажувати додатки, розроблені власними силами, і поширювати їх.

За допомогою цього символу ви можете розповсюджувати додаткові Внутрішні програми.

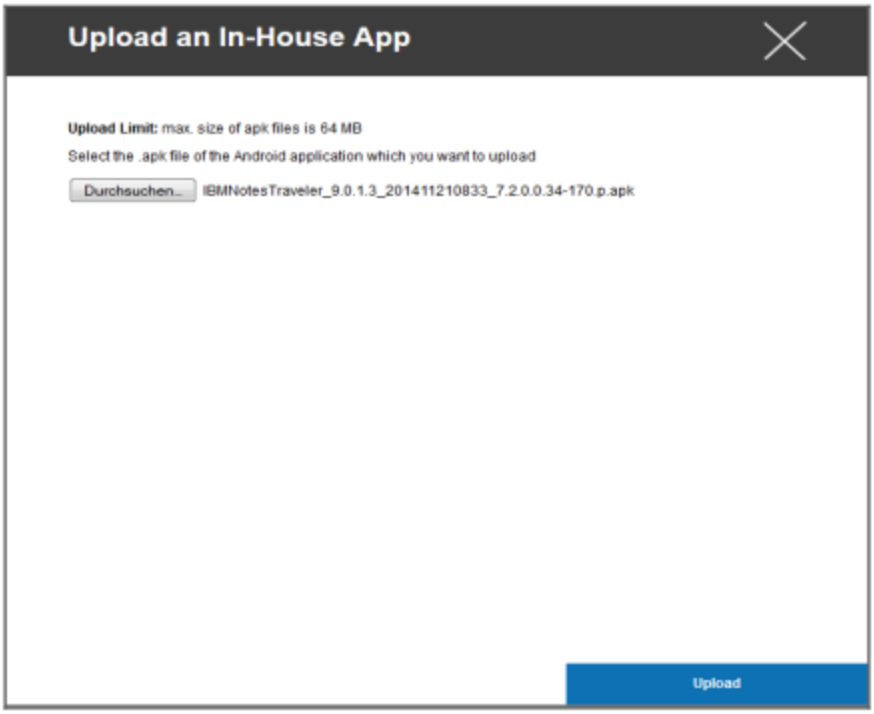
Якщо ви ніколи не розповсюджували In-House App, ви отримаєте наступний огляд:



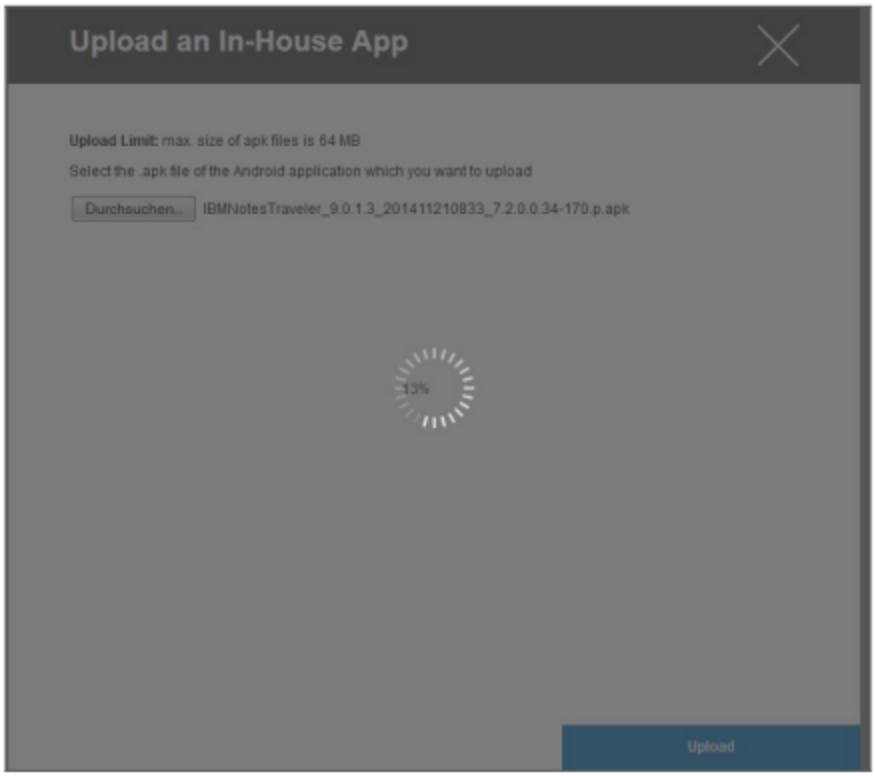
Для цього натисніть "Завантажити власний додаток", після чого ви отримаєте наступний огляд:



Тепер виберіть за допомогою "Пошук..." файл .ipa, а потім натисніть "Завантажити"



Ваш додаток буде завантажено. Посередині кола ви можете побачити відсоток того, яку частину вашого додатку вже завантажено.



Якщо завантаження Внутрішнього додатку пройшло успішно, ви побачите щойно завантажений додаток у вашому Каталозі додатків.

Тепер користувач має можливість переглянути та встановити цей додаток в AppTec360 Store на пристрої кінцевого користувача в категорії "In-House".

Оскільки це не пов'язано з публічним додатком Apple AppStore, користувачеві не потрібно зберігати ідентифікатор Apple ID на кінцевому пристрої.

Режим кіоску

Режим кіоску iOS доступний лише в режимі під наглядом

Режим кіоску дозволяє вам попередньо визначити програму або URL-адресу, щоб можна було запускати/відвідувати виключно цю програму/URL-адресу.

Крім того, ви можете деактивувати різні апаратні кнопки в режимі кіоску.

Тип програми

Пакет

Якщо ви хочете запустити програму в режимі кіоску, виберіть "Пакет" у розділі "Тип програми"

Додаток для кіоску	Натисніть тут, щоб вибрати програму, яка має запускатися в режимі кіоску Ви знайдете поточний огляд управління додатками Ви можете вибрати між "Додатками Apple iTunes" та "Власними додатками iOS"

URL

Якщо ви хочете запустити URL-адресу в режимі кіоску, виберіть "URL" у розділі "Тип програми"

URL	Тепер визначте потрібну URL-адресу
Політика однакового походження	Якщо ця функція активна, користувач може переглядати лише підсторінки за попередньо визначеною URL-адресою Наприклад, якщо ви визначили наступну URL-адресу: www.mypage.com, після чого користувач може перейти на www.mypage.com/subpage
Білі списки URL-адрес	Тут ви можете вести білий список, всі ці URL-адреси дозволені Не більше 1 URL-адреси в рядку URL-адреса повинна починатися з http:/ або https://
URL-адреси в чорному списку	Тут ви можете вести чорний список, всі ці URL-адреси заборонені Не більше 1 URL-адреси в рядку URL-адреса повинна починатися з http:/ або https://
Очистити браузер після бездіяльності	Після бездіяльності кеш браузера буде очищено
Увімкнено пароль на вихід	Якщо ви активуєте цю функцію, користувач має можливість завершити роботу в режимі кіоску за допомогою пароля, який ви визначили заздалегідь
Пароль для виходу	Це пароль, який ви визначили заздалегідь

Налаштування режиму кіоску

Режим роботи кіоску за розкладом	Залежно від часу доби, ви можете налаштувати режим кіоску, щоб він автоматично запускався і завершувався в заздалегідь визначений час.
Час початку	Час початку
Час у хвилинах	Час у хвилинах, після якого режим кіоску має бути знову завершений
Вимкнути дотик	Якщо увімкнено, сенсорний екран вимкнено
Вимкнути обертання пристрою	Якщо увімкнено, автоматичну адаптацію екрана вимкнено
Вимкнути перемикач дзвінка	Якщо її увімкнути, дзвінок буде вимкнено. З цього моменту поведінка залежить від попередньо встановленої функції
Вимкнення кнопок гучності	Якщо увімкнено, кнопки гучності буде вимкнено
Вимкнути кнопку "Сон" - "Пробудження	Якщо активовано, перемикач увімкнення/вимкнення буде деактивовано
Вимкнути автоматичне блокування	Якщо увімкнено, пристрій не буде переходити в режим очікування
Ввімкнути голосовий супровід	Якщо увімкнено, буде активовано голосовий помічник
Увімкнути масштабування	Якщо увімкнено, буде активовано зум
Увімкнути інвертування кольорів	Якщо увімкнено, буде активовано режим інвертованого відображення
Ввімкнути допоміжний сенсорний дотик	Якщо увімкнено, AssistiveTouch буде активовано
Увімкнути вибір мови	Якщо увімкнено, буде активовано вибір мови
Увімкнути монофонічний звук	Якщо увімкнено, буде активовано монофонічний звук
Голос за кадром	Якщо активовано, користувач може ввімкнути VoiceOver
Збільшити	Якщо ця опція активована, користувач може ввімкнути Zoom
Інвертувати кольори	Якщо активовано, користувач може ввімкнути інвертовані кольори
Асистентний дотик	Якщо увімкнено, користувач може увімкнути допоміжний дотик

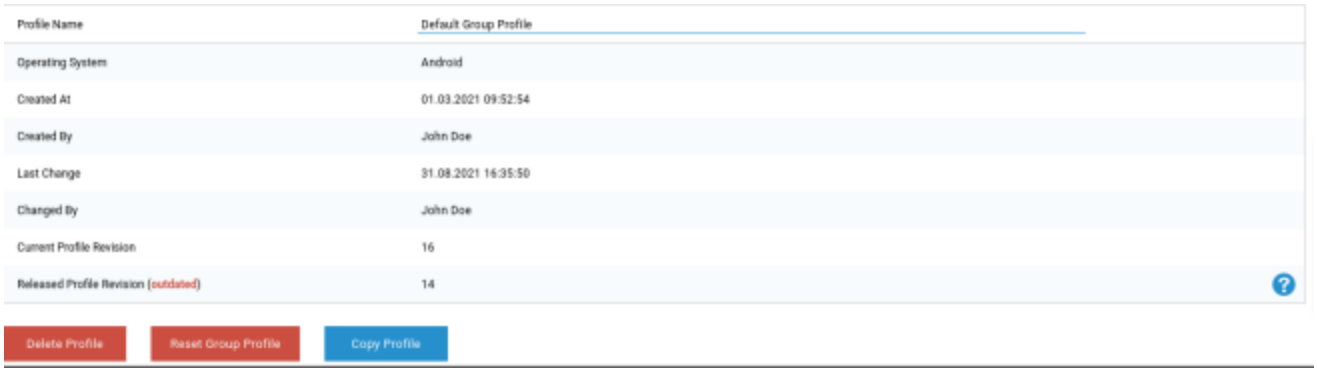
Android Enterprise – повністю керована конфігурація пристрою

Залежно від того, який профіль групи або пристрою ви вибрали, огляд і його підпункти відрізняються - будь ласка, зверніть на це увагу!

Генерал

Огляд профілю групи (тільки на рівні групи)

Відкривши профіль групи, ви отримаєте короткий огляд профілю.



Ім'я профілю Ім'я профілю	Назва профілю (можна змінити тут)
Операційна система	Операційна система, для якої призначений профіль
Створено в	Час створення
Створено	Творець профілю
Остання зміна	Час останньої зміни профілю
Змінено	Обліковий запис, який вніс останні зміни
Поточна редакція профілю	Перегляд стану збереженого профілю
Випущено ревізію профілю	Призначена версія профілю ("Призначити зараз"). Якщо за текстом мітки вказано "(застаріла)", це означає, що ви зберегли профіль, але ще не призначили його, тому пристрої все одно отримають стару версію.

Огляд пристрою (тільки на рівні пристрою)

Якщо ви перебуваєте на пристрої, ви отримаєте оглядову інформацію про вибраний пристрій, яка міститься тут:

Назва пристрою	Назва пристрою
Місцезнаходження	Координати розташування
Номер телефону	Номер телефону
Призначені обов'язкові програми	Кількість призначених Обов'язкових додатків
Версія ОС	Версія операційної системи пристрою
Операційна система	Операційна система (Android Enterprise)
Серійний номер	Серійний номер пристрою
Право власності на пристрій	Корпоративний або приватний пристрій
Тип пристрою	Пристрій керування роботою AE
Укорінений	Статус, що вказує на те, чи був пристрій вкорінений
Дотримується	Відповідає настановам
IP-адреса	IP-адреса пристрою
Востаннє бачили	Момент часу, коли пристрій востаннє підключався до AppTec
Останній поштовх	Момент часу, коли на пристрій було надіслано останнє push-повідомлення
Режим власника пристрою AE	Так.
Призначення користувача	Користувач або група, якій призначено цей пристрій

Ревізія конфігурації (лише на рівні пристрою)

Тут ви отримаєте огляд того, який профіль групи призначено пристрою.

Якщо ви натиснете на профіль групи, ви отримаєте прямий доступ до цього профілю і зможете виконати налаштування.

За допомогою цього символу ви можете повернути розподілені програми до налаштувань профілю групи.

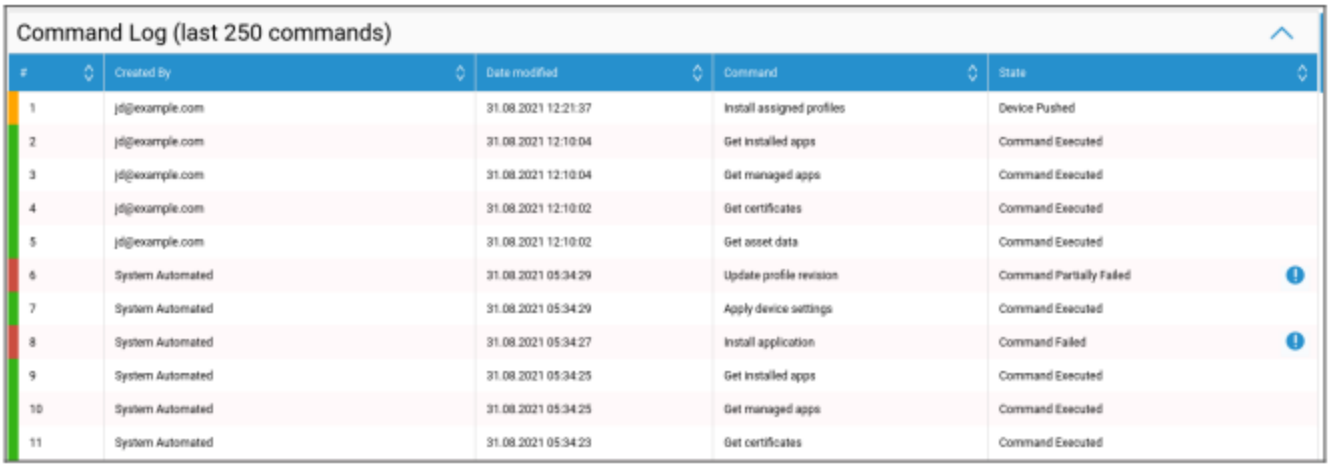
За допомогою цього символу ви можете повернути всі використовувані програми до налаштувань профілю групи.

"Доступна новіша версія" вказує на те, що профіль групи було змінено та збережено, але не призначено. Щоб застосувати зміни до пристроїв, профіль групи потрібно призначити за допомогою "Призначити зараз" на рівні групи.

Журнал пристрою (тільки на рівні пристрою)

Командний журнал

Тут ви можете побачити, які команди були видані для пристрою і який їхній статус.



Команди, створені за допомогою "Автоматизації системи", автоматично створюються системою.

Можливі стани команди

Пристрій натиснуто	До служби push (наприклад, APNS) було надіслано push-запит, щоб повідомити пристрій про необхідність з'єднатися з сервером EMM.
Команду створено	Команда була створена в системі.
Команду відправлено.	Команда була надіслана на пристрій після того, як він підключився до сервера.
Команду виконано	Команда була успішно виконана.
Команда не спрацювала	Команда не спрацювала. *
Команда частково не виконана	Залежно від операційної системи пристрою деякі команди можуть бути згруповані разом. У цьому деякі частини цієї командної групи зазнали невдачі. *
Команда виконана, але зрештою не спрацювала	Команда була виконана, але, можливо, не була.
Команда "Відсіч	Команду було перевиконано користувачем.
Викинуто	Команду було відкинуто. Наприклад, її було замінено іншою командою або пристрій було перереєстровано, а старі команди видалено

Якщо за повідомленням стоїть знак оклику, ви можете отримати додаткову інформацію, навівши курсор на іконку.

Налаштування пристрою

Конфігурація клієнта

Тут ви можете виконати наступні конфігурації на вашому пристрої Android:

Порушення термінів дотримання вимог	Граничний таймаут відповіді користувача, після якого застосовується дія примусового виконання.
Примусові заходи після закінчення терміну виконання	Примусова дія, коли користувач не виконує дії, які призводять до сумісного статусу пристрою
Частота збору даних	Частота, з якою пристрій / GPS-інформація повинна збиратися
Частота серцебиття пристрою	Інтервал, через який пристрій повинен зв'язуватися з сервером AppTec360 Хвилина. 1 хвилина Максимум. 24 години
Увімкнути оновлення місцезнаходження	Якщо увімкнено, пристрій надсилає оновлення місцезнаходження на сервер AppTec360
Час оновлення місцезнаходження	Визначає, через які проміжки часу пристрій надсилає оновлення місцезнаходження до AppTec360
Використовуйте Google Location Accuracy для оновлення місцезнаходження	Якщо увімкнено, то для оновлення місцезнаходження буде використовуватися мережеве розташування (якщо це було деактивовано в розділі "Обмеження", то це налаштування ні на що не вплине)
Використовуйте GPS-локацію для оновлення місцезнаходження	Якщо увімкнено, GPS буде використовуватися для оновлення місцезнаходження
Дозволити імітацію (фейкові) локації	Дозволяє підробляти інформацію про місцезнаходження за допомогою сторонніх додатків
Дія "Втрата зв'язку	Якщо увімкнено, ви можете вказати дію на випадок, якщо пристрій не отримає з'єднання з MDM-сервером протягом інтервалу серцебиття. Наприклад, якщо час серцебиття пристрою становить 5 хвилин, він з'єднається з сервером о 10:35 ранку. Після цього пристрій виходить з діапазону Wi-Fi. Наступне серцебиття о 10:40 буде невдалим, і вказана дія буде виконана.
Дія	Дії, які необхідно вжити, як тільки пристрій стає невідповідним.

	• Lock Device = пристрій блокування • Очистити пристрій = пристрій буде відновлено до заводських налаштувань • Wipe Device & SD Card = пристрій буде відновлено до заводських налаштувань, а пам'ять на SD-карті буде видалено
Поріг	Ви можете вказати поріг кількості невдалих серцевих скорочень, які необхідні для запуску вказаної дії.

Режим застосування політики	За замовчуванням:	Користувачі будуть періодично отримувати запити на виконання незавершених дій
	Ліниве впровадження політики:	Користувачам ніколи не буде запропоновано виконати незавершені дії. Всі відкриті дії будуть показані в клієнті AppTec360
	Агресивне впровадження політики:	Користувачам будуть постійно пропонувати виконати незавершені дії
AppTec360 Блокування версії	Якщо увімкнено, можна вказати код версії для клієнта AppTec360 MDM. Клієнт AppTec360 буде оновлюватися лише до вказаної версії. Більш нові версії будуть ігноруватися. Пониження версії НЕ можливе.	
Код версії	Код версії MDM-клієнта AppTec360, до якого потрібно прив'язати AppTec360 MDM.	
Вимкнути сповіщення AppTec360	Якщо вимкнено, клієнт AppTec360 не показуватиме сповіщення в панелі сповіщень. Таким чином, користувачі можуть закрити клієнт AppTec360 через диспетчер завдань. Якщо клієнт AppTec360 закрито, деякі функції, включаючи режим кіоску та чорний/білий список додатків, не працюватимуть належним чином. Пристрої Samsung пропонують механізм захисту для клієнта AppTec360. Сповіщення за замовчуванням вимкнено на пристроях Samsung, які підтримують KNOX API. Сповіщення не повинно відключати пристрої з Android 8.0 або новішої версії.	

Шпалери

Встановіть власні шпалери	Увімкнути/вимкнути кастомні шпалери
Шпалери	Налаштуйте режим шпалер для використання кольорового коду або зображення
Вкажіть колір	Вкажіть колір бекграунду як шістнадцяткове значення, наприклад, #000000 для чорного або #ffffff для білого.
Встановити зображення як шпалери	Завантажте файл зображення, який ви хочете використовувати як шпалери

Управління активами (тільки на рівні пристрою)

Інформація про пристрій

Модель	Позначення моделі пристрою
Операційна система	ОС
Версія ОС	Версія операційної системи
Серійний номер	Серійний номер
Назва пристрою	Назва пристрою
Стан акумулятора	Стан акумулятора
Вільна / загальна пам'ять	Вільна / Загальна пам'ять
Samsung Safe	Інтерфейс Samsung SAFE, необхідний для різноманітних налаштувань
Доступна SD-карта	Доступна SD-карта
Емуляція SD-карти	Емуляція SD-карти
Знімна SD-карта	Знімна SD-карта
Вільна пам'ять SD / загальна пам'ять	Вільна пам'ять на SD / Загальна пам'ять на SD-карті

Wi-Fi

IP-адреса	IP-адреса пристрою
MAC-адреса WiFi	MAC-адреса WiFi

Стільниковий зв’язок

Статус	Статус (встановлена SIM-карта)
Номер телефону	Номер телефону
Роумінг (голосовий зв'язок / передача даних)	Роумінг для передачі голосу/даних
Статус роумінгу	Поточний статус у роумінгу
IP-адреса	IP-адреса
Оператор/перевізник	Оператор/перевізник
Стільникові технології	Стільникові технології
IMEI	Номер IMEI
ICCID	Це ідентифікатор SIM-картки, часто також смарт-картки або картки з інтегральною схемою (ICC)
IMSI	Міжнародна мобільна ідентифікація абонента (IMSI) забезпечує в GSM- і UMTS-мережах однозначну ідентифікацію користувачів мережі IMSI складається максимум з 15 цифр і налаштовується наступним чином: • Мобільний код країни (MCC), 3 цифри • Код мобільної мережі (MNC), 2 або 3 цифри • Ідентифікаційний номер абонента мобільного зв'язку (MSIN), 1-10 цифр
Поточний ГХК/МНК	Див. розділ "SIM MCC/MNC"
SIM MCC/MNC	Мобільний код країни - це визнаний ідентифікатор країни, встановлений MCE відповідно до стандарту E.212. Він працює разом з кодом мобільної мережі (MNC) для ідентифікації мобільної мережі. Означає код країни/мобільної мережі SIM-карти. Якщо ви перебуваєте в роумінгу в іншій мобільній мережі, то логічно, що "Поточний MCC/MNC" і "MCC/MNC SIM" будуть відрізнятися.

Bluetooth

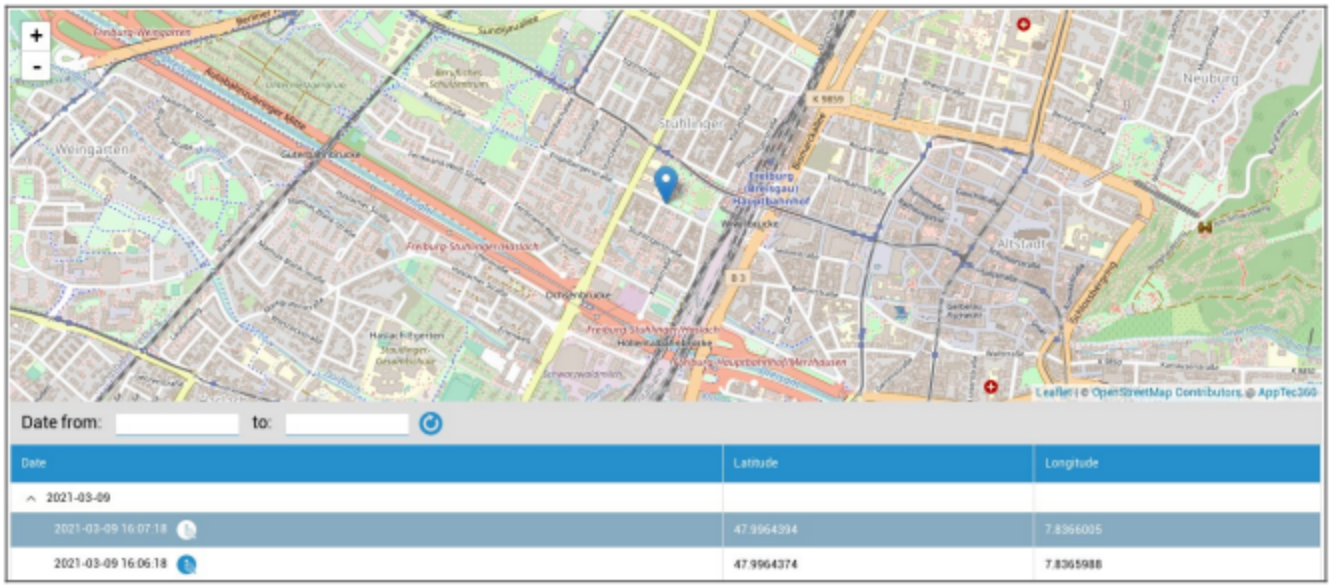
MAC-адреса Bluetooth	MAC-адреса Bluetooth

Управління безпекою

Захист від крадіжок (лише на рівні пристрою)

Інформація про GPS (лише на рівні пристрою)

Тут ви можете встановити поточне/останнє місцезнаходження пристрою. Локалізацію можна захистити одним або навіть двома паролями - Див: Загальні налаштування - Конфіденційність - Доступ до GPS



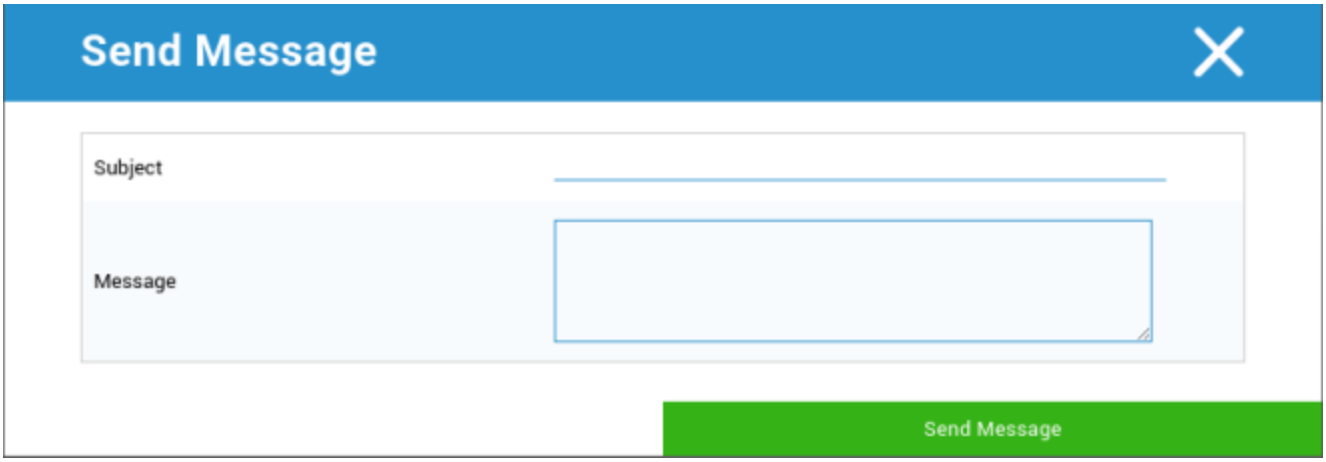
Wipe & Lock (тільки на рівні пристрою)

У розділі "Витирання та блокування" ви можете виконати наступні три дії:

Повне витирання	Пристрій відновлюється до заводських налаштувань (видаляються корпоративні, а також особисті дані)
Enterprise Wipe	З пристрою кінцевого користувача видаляються лише корпоративні дані (всі додатки, дані тощо, які були надані AppTec360).
Екран блокування	Блокування екрану активоване, достатньо розблокувати пристрій за допомогою пароля/коду пристрою

Повідомлення (тільки на рівні пристрою)

Тут ви можете заповнити тему та повідомлення і відправити його на пристрій кінцевого користувача.



Конфігурація безпеки

Код доступу до пристрою

У розділі "Пароль" ви можете встановити пароль пристрою, вам доступні наступні варіанти налаштувань

Мінімальна довжина пароля	Визначає мінімальну кількість символів, які повинен містити пароль	
Якість пароля	Не визначено	Ця політика не містить вимог до пароля.
	Біометричні слабкі	Ця політика дозволяє використовувати технології біометричного розпізнавання з низьким рівнем безпеки. Це означає технології, які можуть розпізнати особу приблизно до 3-значного PIN-коду (ймовірність помилкового розпізнавання - менше ніж 1 на 1000).
	Щось.	Ця політика вимагає встановлення певного пароля або шаблону, але не запроваджує жодних конкретних правил.
	Алфавітний	Користувач повинен ввести пароль, що містить принаймні літерні (або інші символи) символи.
	Буквено-цифровий	Користувач повинен ввести пароль, що містить принаймні обидва символи - цифри та літери (або інші символи).
	Комплекс	За замовчуванням користувач повинен ввести пароль, що містить щонайменше літеру, цифру та спеціальний символ. З такою якістю пароля можна обмежити його вміст різними наборами символів, наприклад, принаймні великими літерами тощо.
Мінімальна довжина пароля	Встановіть необхідну кількість символів для пароля. Наприклад, ви можете вимагати, щоб PIN-код або пароль містив щонайменше шість символів.	
Мінімальна кількість цифр у паролі	Мінімальна кількість цифр у паролі	
Мінімум малих літер у паролі	Мінімум малих літер у паролі	
Мінімальна кількість великих літер у паролі	Мінімальна кількість великих літер у паролі	

Мінімальна кількість нелітерних символів у паролі	Мінімальна кількість нелітерних символів у паролі
Мінімальна кількість символів у паролі	Мінімальна кількість символів у паролі

Блокування максимального часу бездіяльності	Максимальна бездіяльність користувача до моменту блокування часу
Таймаут терміну дії пароля	Встановлює, через який проміжок часу закінчується термін дії пароля і потрібно видати новий пароль
Обмеження історії паролів	Кількість раніше використаних паролів, які не допускаються
Максимальна кількість невдалих спроб введення пароля	Визначає, як часто можна вводити пароль неправильно, перш ніж буде виконано повне очищення пристрою
Дозволити біометричну автентифікацію	Дозволяє автентифікацію за допомогою сканування відбитка пальця або райдужної оболонки ока. Тільки для Samsung KNOX 2.1 і вище

Антивірус

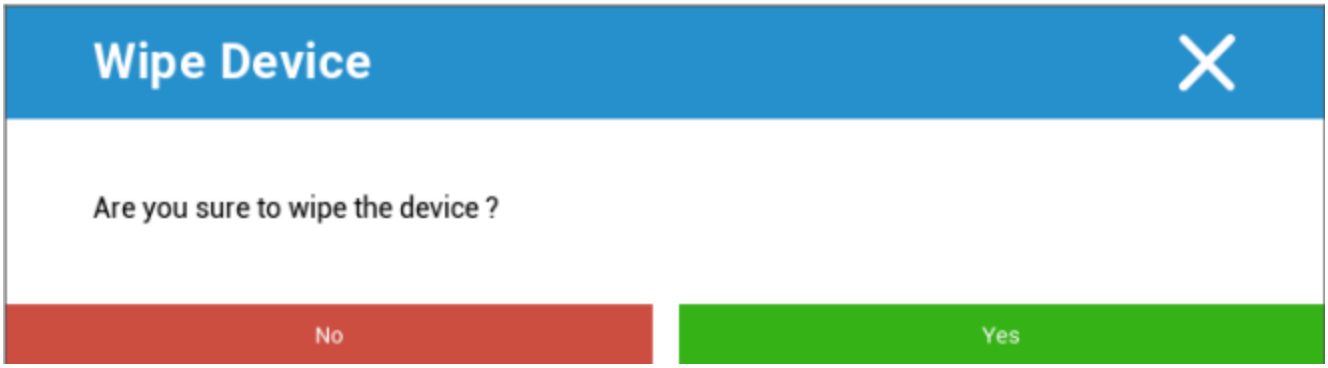
Автоматичне сканування	Увімкнути періодичне автоматичне сканування
Інтервал сканування	Інтервал для обстеження (Швидкий / Повний)
Повне автоматичне сканування	Увімкнути повне автоматичне сканування
Автоматичні оновлення	Увімкнути автоматичні оновлення
Інтервал перевірки оновлення	Як часто потрібно оновлювати додаток та його базу даних (віруси / пошкоджений код)
Захист додатків	Увімкнути автоматичне сканування програм
Захист SD-карти	Увімкнути автоматичне сканування SD-карти
Оновлення тільки для Wi-Fi	Якщо увімкнено, оновлення будуть застосовуватися лише тоді, коли пристрій успішно підключено до мережі Wi-Fi

Кінець життя (тільки на рівні пристрою)

Витирання (тільки на рівні пристрою)

У розділі "Видалити" ви можете відновити заводські налаштування пристрою. При цьому на пристрої кінцевого користувача будуть видалені як корпоративні, так і приватні дані.

При натисканні на "Символ мінус" ви отримаєте наступне повідомлення:



За допомогою "Так" ви можете виконати стирання.

У розділі "Звіт про витирання" можуть відображатися такі елементи

Витерто	Історія про те, хто виконував стирання
Дата	Дата
Статус	Статус (наприклад, якщо очищення було виконано успішно)

Налаштування обмежень

Обмеження

Тут можна обмежити та заблокувати безліч речей.

Увімкнути камеру	Дозволити використовувати камеру	
Ввімкнути автосинхронізацію	На	Синхронізація постійно активована
	Вимкнено	Синхронізація назавжди вимкнена
	Вибір користувача	Вибрано користувачем
Ввімкнути Bluetooth	Увімкнено	Bluetooth постійно активовано
	Вимкнено	Bluetooth назавжди вимкнено
	Вибір користувача	Вибрано користувачем
Примусьте GPS	Увімкнено	GPS постійно активовано
	Вимкнено	GPS назавжди вимкнено
	Вибір користувача	Вибрано користувачем
Розташування силової мережі	Увімкнено	Постійна інтернет-локалізація
	Вимкнено	Постійна деактивація інтернет-локалізації
	Вибір користувача	Вибрано користувачем

Безпека		
Заборонити розташування спільного доступу	Вказує, чи користувачеві заборонено вмикати спільний доступ до місцезнаходження.	
Заборонити безпечне завантаження	Вказує, чи користувачеві заборонено перезавантажувати пристрій у безпечний режим завантаження.	
Заборонити скидання мережі	Вказує, чи користувачеві заборонено скидати налаштування мережі з Налаштувань.	
Заборонити скидання до заводських налаштувань	Вказує, чи користувачеві заборонено скидати пристрій.	
Увімкнути АБР	Дозволяє підключатись до ПК через ADB	
Вимкнути Keyguard	Вимкнення Keyguard	
Інформація про власника пристрою на екрані блокування	Дозволяє встановити інформацію про власника пристрою для відображення на екрані блокування.	
Забезпечення комплаєнсу	Режим Підказка користувачеві	Користувачеві буде запропоновано виконати необхідні дії.
	Контейнер для блокування режиму	Приховати всі програми, доки не будуть виконані всі вимоги

Керування додатками	
Дозволити зв'язування міжпрофільних додатків	Дозволяє програмам у батьківському профілі обробляти веб-посилання з керованого профілю.
Заборонити керування програмами	Вказує, чи користувачеві заборонено змінювати програми у Налаштуваннях або лаунчерах.
Заборонити встановлення програми	Вказує, чи заборонено користувачеві встановлювати програми.
Заборонити видалення програм	Вказує, чи користувачеві заборонено видаляти програми.
Політика дозволів на виконання	Вказує, як будуть оброблятися нові запити на дозволи від програм.
Дозволити невідомі джерела	Якщо увімкнено, користувачі можуть завантажувати програми, встановивши файл .apk.

Зв'язок	
Заборонити конфігурацію мобільної мережі	Вказує, чи користувачеві заборонено налаштовувати мобільні мережі.
Заборонити прив'язку Конфігурація	Вказує, чи користувачеві заборонено налаштовувати Tethering та портативні хот-споти.
Заборонити конфігурацію VPN	Вказує, чи користувачеві заборонено налаштовувати VPN.
Заборонити конфігурацію Wifi	Вказує, чи користувачеві заборонено змінювати точки доступу WiFi.
Заборонити вихідний промінь NFC	Вказує, чи дозволено користувачеві використовувати NFC для передачі даних з програм.
Блокування конфігурації WiFi	Цей параметр визначає, чи слід блокувати конфігурації WiFi, створені у програмі Власника пристрою (тобто, чи можна їх редагувати або видаляти лише у програмі Власника пристрою, а не у програмі Налаштування).
Увімкнути роумінг даних	Активує роумінг даних

Bluetooth	
Заборонити Bluetooth	Вказує, чи заборонено Bluetooth на пристрої. Потрібна версія Android 8.0
Заборонити спільний доступ через Bluetooth	Вказує, чи заборонено на пристрої вихідний обмін даними через Bluetooth. Потрібна Android 8.0
Заборонити конфігурацію Bluetooth	Вказує, чи користувачеві заборонено налаштовувати bluetooth.

Управління рахунками	
Заборонити додавання керованого профілю	Вказує, чи користувачеві заборонено додавати керовані профілі. Потрібна версія Android 8.0
Заборонити додавання користувачів	Вказує, чи користувачеві заборонено додавати нових користувачів.
Заборонити видалення керованого профілю	Вказує, чи можна видаляти керовані профілі цього користувача, окрім власника профілю. Потрібна Android 8.0
Заборонити зміну облікового запису	Вказує, чи користувачеві заборонено додавати та видаляти облікові записи, якщо вони не додані програмно за допомогою автентифікатора.

Телефонія	
Заборонити вихідні дзвінки	Вказує, що користувачеві заборонено здійснювати вихідні телефонні дзвінки.
Заборонити SMS	Вказує, що користувачеві заборонено надсилати або отримувати SMS-повідомлення.

Система	
Заборонити створення вікон	Вказує, що не слід створювати вікна, окрім вікон програми.
Заборонити встановлену піктограму користувача	Вказує, чи дозволено користувачеві змінювати свою іконку.
Заборонити встановлення шпалер	Обмеження користувача для заборони встановлення шпалер.
Вимкнути рядок стану	Вимкнення рядка стану блокує сповіщення, швидкі налаштування та інші екранні накладки, які дозволяють втекти з одноразового пристрою.
Увімкнути автоматичний час	Встановлює час автоматично.
Увімкнути автоматичний часовий пояс	Автоматично встановлює часовий пояс.
Залишайтеся увімкненими, коли ви підключені до мережі	Пристрій залишатиметься активним, поки підключений до джерела живлення.

Зберігання	
Заборонити вимкнути перевірку додатків	Вказує, чи користувачеві заборонено вимикати перевірку додатків.
Заборонити монтування фізичних носіїв	Вказує, чи користувачеві заборонено монтувати фізичні зовнішні носії.
Увімкнути службу резервного копіювання	Служба резервного копіювання керує всіма механізмами резервного копіювання та відновлення на пристрої. Якщо встановити значення false, резервне копіювання або відновлення даних буде неможливим. За замовчуванням службу резервного копіювання вимкнено. Потрібна Android 8.0
Увімкнути USB-накопичувач	Дозволяє використовувати USB-накопичувач.

Клавіатура	
Заборонити автозаповнення	Вказує, чи користувачеві заборонено використовувати служби автозаповнення. Потрібна версія Android 8.0
Заборонити копіювання та вставку між профілями	Вказує, чи можна вставляти скопійоване у буфер обміну цього профілю у пов'язані профілі.

Звук	
Заборонити регулювання гучності	Дозволяє вказати, чи користувачеві заборонено регулювати загальний рівень гучності.
Заборонити вимкнення мікрофона	Вказує, чи користувачеві заборонено регулювати гучність мікрофона.
Вимкнення звуку пристрою	Вимкнути звук.

Управління сертифікатами

Тут ви можете розповсюджувати довірені сертифікати та ідентифікаційні сертифікати на ваші пристрої.

Для розповсюдження довірених сертифікатів потрібна Android 8 або новіша версія, а для розповсюдження ідентифікаційних сертифікатів - Android 9 або новіша версія.

За допомогою "+" ви можете додати кілька сертифікатів.

Довірені сертифікати повинні бути у форматі PEM.

Посвідчення особи повинні бути у форматі PKCS12

Керування з’єднаннями

Wi-Fi

Для цього налаштування виконайте попередню конфігурацію пристроїв кінцевих користувачів для доступу до внутрішніх точок доступу

Ідентифікатор набору послуг (SSID)	SSID мережі, до якої потрібно підключитися
Прихована мережа	Активувати, якщо точка доступу не передає SSID

Тип безпеки

Встановіть тип захисту точки доступу

WEP

Пароль	Пароль для точки доступу

WPA/WPA2

Пароль	Пароль для точки доступу

802.1x EAP

EAP-метод

PWD	Ідентичність	Ідентичність
	Пароль	Пароль

PEAP	Етап 2 Протокол автентифікації	ні	Без додаткового протоколу
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертифікат центру сертифікації	Сертифікат центру сертифікації	
	Ідентичність	Ідентичність	
	Анонімна ідентичність	Анонімна особистість	
	Пароль	Пароль	

TTLS	Етап 2 Протокол автентифікації	ні	Без додаткового протоколу
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертифікат центру сертифікації	Сертифікат центру сертифікації	
	Ідентичність	Ідентичність	
	Анонімна ідентичність	Анонімна ідентичність	
	Пароль	Пароль	

TLS	Сертифікат центру сертифікації	Сертифікат центру сертифікації
	Ідентичність	Ідентичність
	Пароль	Пароль

VPN

Ім'я з'єднання Ім'я з'єднання	Назва VPN-з'єднання

Тип VPN

VPN

Клієнт VPN

AppTec360 VPN клієнт	
Конфігурація шлюзу	Виберіть конфігурацію шлюзу VPN (див. **Загальні налаштування > Універсальний шлюз > Налаштування VPN**)
Завжди увімкнений VPN	Увімкнути власне блокування
Увімкнути блокування AppTec360	Увімкнути блокування AppTec360

Вбудований (доступний лише на пристроях Samsung)			
Тип підключення	PPTP	Сервер	Сервер
		Увімкнути шифрування PPTP	Увімкнути шифрування PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Увімкнути секрет L2TP	Увімкнути секрет L2TP
		Секрет L2TP	Секрет L2TP
	IPSec XAuth PSK	Сервер	Сервер
		Ідентифікатор IPSec	Ідентифікатор IPSec
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
Пошукові домени DNS	Пошукові домени DNS		
Налаштування експерта	DNS-сервери	DNS-сервери	
	Маршрути переадресації	Маршрути переадресації	

Відкрити VPN		
Сервер	Сервер	
Профіль OpenVPN	Профіль OpenVPN	
Додаток OpenVPN	OpenVPN для Android (рекомендовано)	
	OpenVPN Connect	
Налаштування експерта	DNS-сервери	DNS-сервери
	Маршрути переадресації	Маршрути переадресації

Samsung / Сильний лебідь			
Тип підключення	PPTP	Сервер	Сервер
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути шифрування PPTP	Увімкнути шифрування PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути секрет L2TP	Секрет L2TP
	IPSec XAuth PSK	Сервер	Сервер
		Ідентифікатор IPSec	Ідентифікатор IPSec
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
Налаштування експерта	DNS-сервери	DNS-сервери	
	Маршрути переадресації	Маршрути переадресації	

Cisco Any Connect		
Сервер	Сервер	
Режим сертифіката	Інваліди	Інваліди
	Автоматично	Автоматично
Налаштування експерта	DNS-сервери	DNS-сервери
	Маршрути переадресації	Маршрути переадресації

Per-App VPN

Клієнт VPN

AppTec360 VPN клієнт		
Конфігурація шлюзу	Виберіть конфігурацію шлюзу VPN (див. **Загальні налаштування > Універсальний шлюз > Налаштування VPN**)	
Програми VPN	Програми VPN	
Завжди увімкнений VPN	Увімкнути власне блокування	Завжди увімкнений VPN
Увімкнути блокування AppTec360	Увімкнути блокування AppTec360	

Samsung / Сильний лебідь			
Тип підключення	PPTP	Сервер	Сервер
		Програми VPN	Програми VPN
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути шифрування PPTP	Увімкнути шифрування PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Програми VPN	Програми VPN
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути секрет L2TP	Секрет L2TP
	IPSec XAuth PSK	Сервер	Сервер
		Програми VPN	Програми VPN
		Ідентифікатор IPSec	Ідентифікатор IPSec
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
Налаштування експерта	DNS-сервери	DNS-сервери	
	Маршрути переадресації	Маршрути переадресації	

Обмеження

Тут ви можете встановити обмеження щодо управління з'єднаннями.

Дозволити роумінг даних	Дозволити мобільні дані в роумінгу
Примусити роумінг даних	Якщо увімкнено, роумінг для мобільних даних активується назавжди (не рекомендується!). Цей параметр замінює параметр "Дозволити роумінг даних"!
Наступні налаштування доступні лише в SAFE 2.x або новішої версії	
Дозволити лише екстрені виклики	Дозволити лише екстрені виклики
Увімкнути WiFi	Увімкнути WiFi
Мінімальний рівень безпеки мережі WiFi	Мінімальний рівень безпеки мережі WiFi Відкрито = дозволені всі типи WiFi
Заборонити користувачеві додавати мережі WiFi	Користувач не може самостійно додати мережу WiFi Це налаштування можливе лише в тому випадку, якщо в розділі "Керування з'єднаннями" було визначено профіль WiFi
Дозволити SMS та MMS	Всі = Весь SMS та MMS трафік дозволено Incoming SMS Only = Дозволено лише вхідні SMS-повідомлення Тільки вихідні SMS = дозволені тільки вихідні SMS-повідомлення Немає = трафік SMS / MMS заборонено
Дозволити синхронізацію в роумінгу	Дозволити синхронізацію в роумінгу Увімкнено = активовано Вимкнено = деактивовано Вибір користувача = вибір користувача
Дозволити голосовий роумінг	Дозволити голосовий роумінг Увімкнено = активовано Вимкнено = деактивовано User Choice = вибір користувача
Використання системного проксі-сервера http	Використання HTTP-проксі-сервера, яке передбачено налаштуваннями системи в налаштуваннях, залежить від підключеної мережі (WiFi або APN)

Менеджмент ПІМ

Обмін Gmail

Info: Ця конфігурація буде застосована до програми Gmail. Тому вам потрібно схвалити та встановити Gmail.

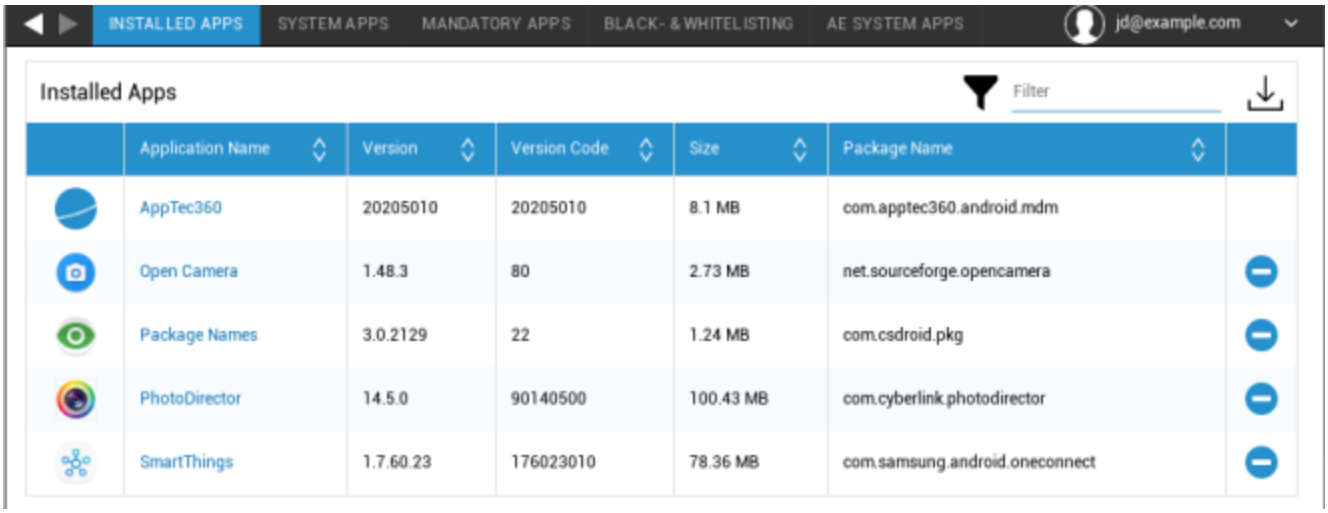
Адреса електронної пошти	Надана адреса електронної пошти користувача Зверніть увагу на "Заповнювачі", які можна використовувати для роботи з обліковими даними і не виконувати зміни вручну на кожному пристрої Натиснувши на них, ви можете переглянути їх для себе
Ім'я хосту сервера	Адреса сервера ваших Exchange-серверів
Ім'я користувача	Ім'я для входу для відповідного пристрою кінцевого користувача, також зверніть увагу на "Заповнювачі тут
Підпис	Можна додати підпис (Підказка: деякі пристрої вимагають HTML-форматування для підпису)
Кількість попередніх днів для синхронізації	Кількість днів, які визначають, коли імейли будуть синхронізовані знову
Ідентифікатор пристрою	Рядок, який містить ідентифікатор пристрою EAS. Він є частиною протоколу EAS і потрібен в окремих випадках
Використовуйте протокол захищених сокетів (SSL)	Використовуйте SSL-з'єднання
Приймаємо всі сертифікати	Приймаються всі сертифікати. Виберіть цю опцію, якщо ваш Exchange-сервер використовує самопідписаний сертифікат

Керування додатками

Enterprise App Manager

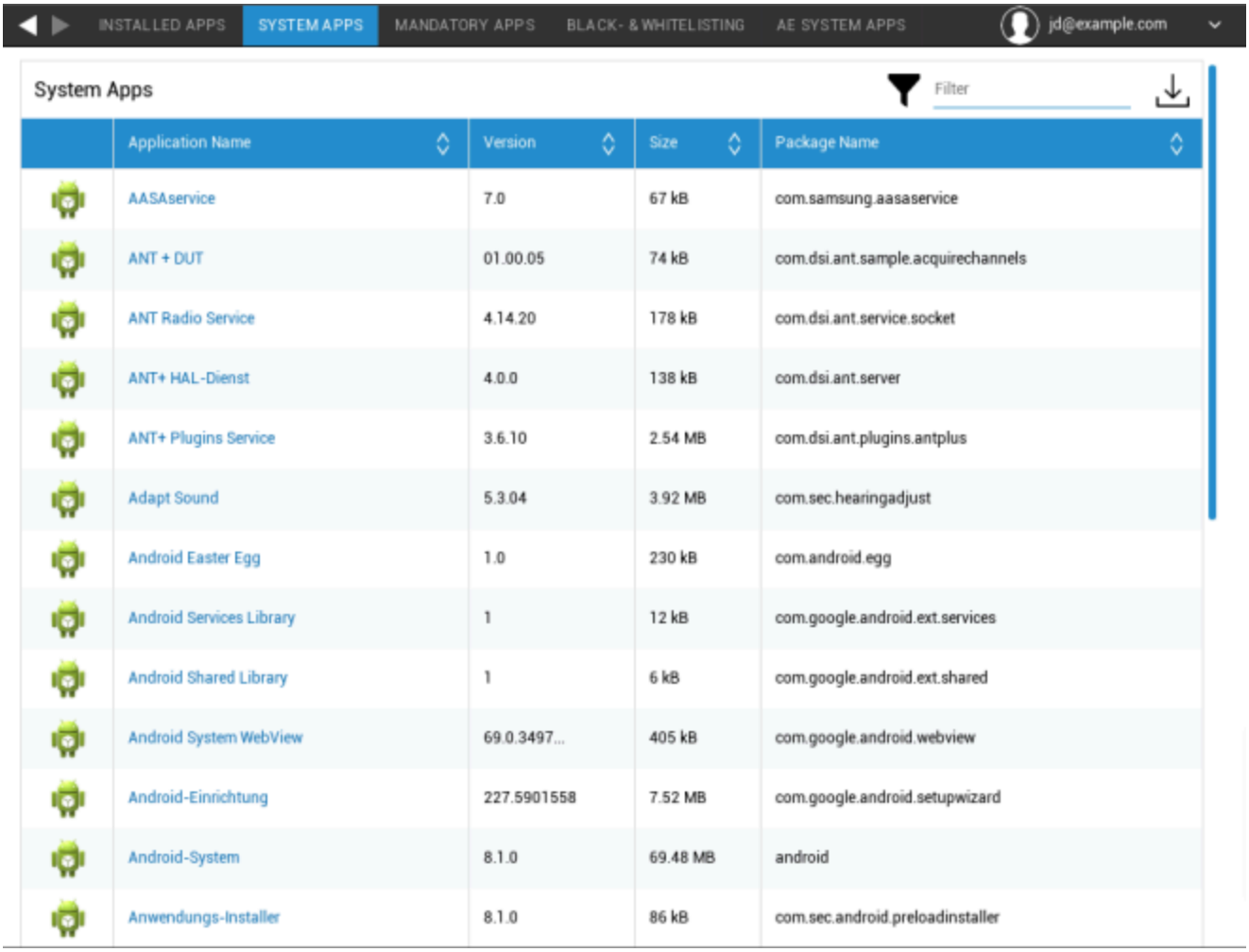
Встановлені програми (лише на рівні пристрою)

Тут будуть показані всі програми, які наразі встановлені на пристрої кінцевого користувача.



Системні програми (лише на рівні пристрою)

У розділі "Системні програми" будуть перераховані всі програми та служби, які вже встановлені на кінцевому пристрої користувача виробником пристрою.

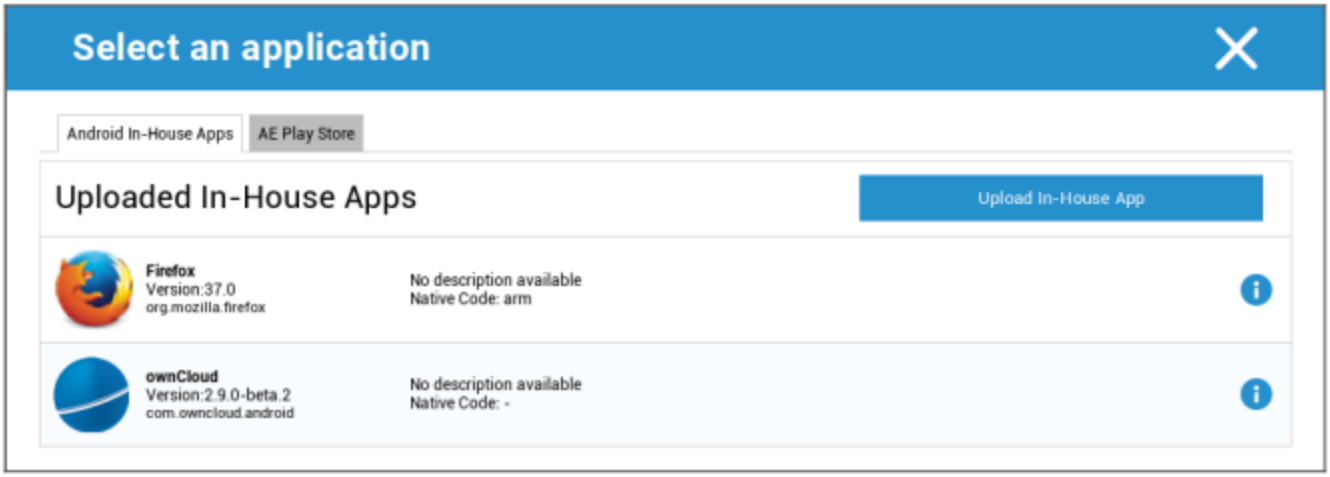


Обов’язкові програми

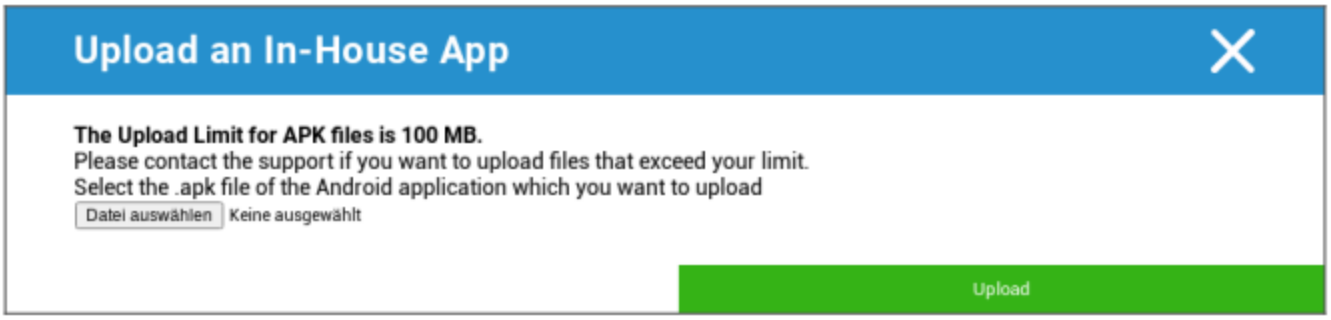
У розділі Обов'язкові програми ви можете встановити обов'язкові програми. Користувачеві буде постійно пропонуватися встановити цю програму.

За допомогою , можна визначити необхідний додаток.

Це може бути власний додаток з папки "Власні додатки Android", який ви завантажили в Загальних налаштуваннях.

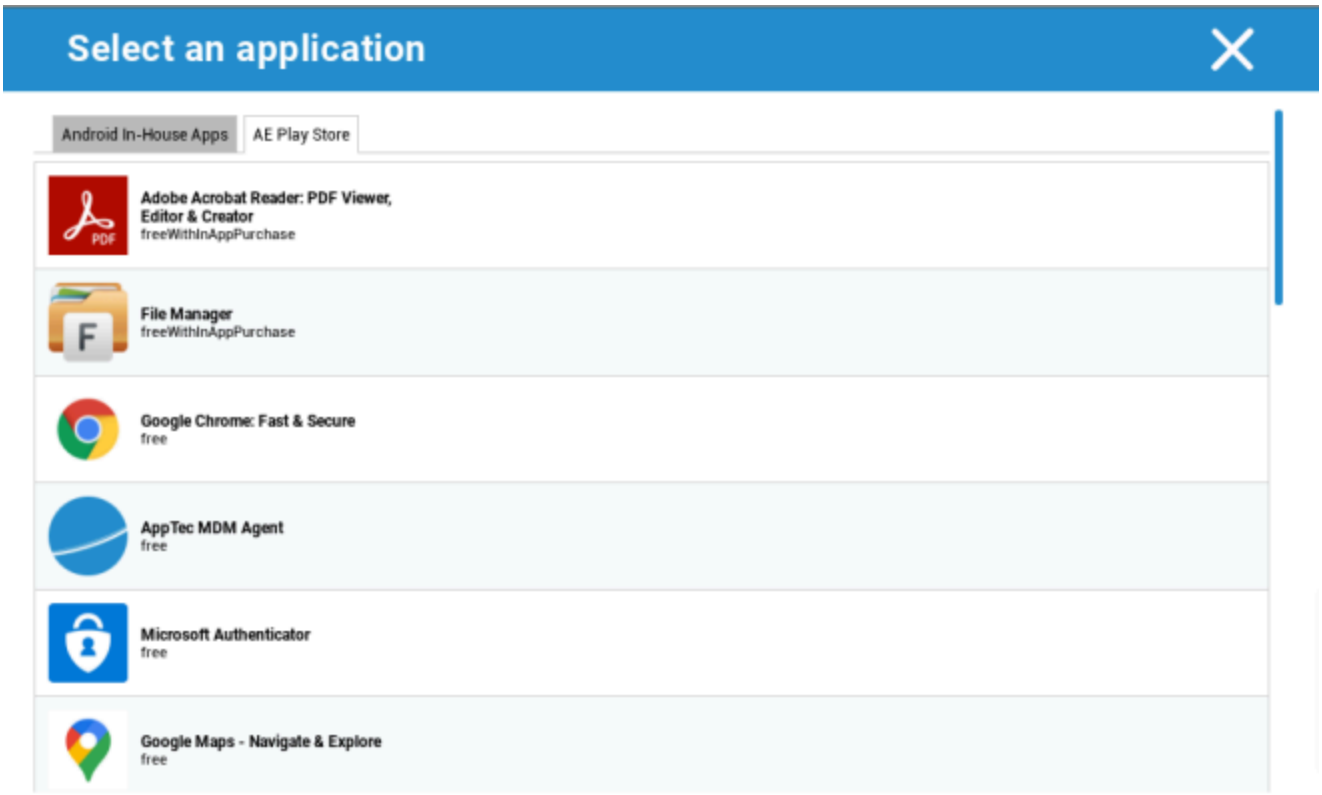


Ви також можете безпосередньо вибрати і завантажити apk-файл за допомогою функції "Завантажити власний додаток".



Якщо ви встановлюєте власний додаток, у вас буде можливість активувати функцію "Оновлювати". Якщо вона активована і ви визначили нову версію в базі даних власних додатків, додаток буде оновлено на пристрої.

Або це може бути додаток "AE Play Store" з Google Work Play Store.



На цій вкладці будуть показані лише схвалені додатки "AE Play Store Apps".

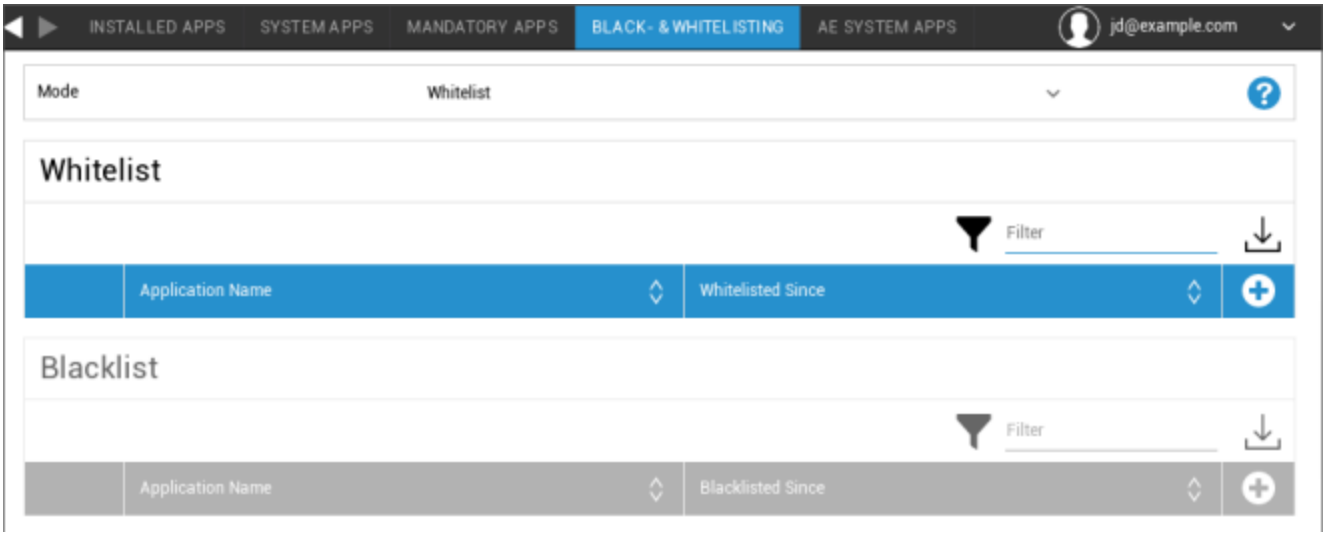
Щоб затвердити "AE Play Store App", перейдіть в "Загальні налаштування" > "Керування додатками" > "AE Play

Store" і додайте додаток за допомогою кнопки, яка перенаправить вас на вкладку "Play Store Apps" (або ви
можете безпосередньо перейти на вкладку "Play Store Apps").

На вкладці "Додатки Play Store" ви можете шукати додатки. Коли ви натискаєте на програму, відкривається сторінка програми
, де ви можете затвердити програму, натиснувши на кнопку "Затвердити".

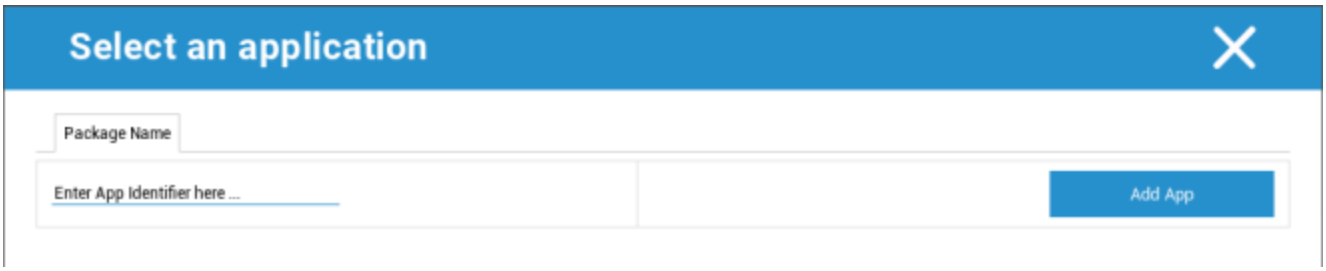
Чорні та білі списки

У розділі "Чорні та білі списки" ви можете вибрати між режимом "Білий список" та режимом "Чорний список".



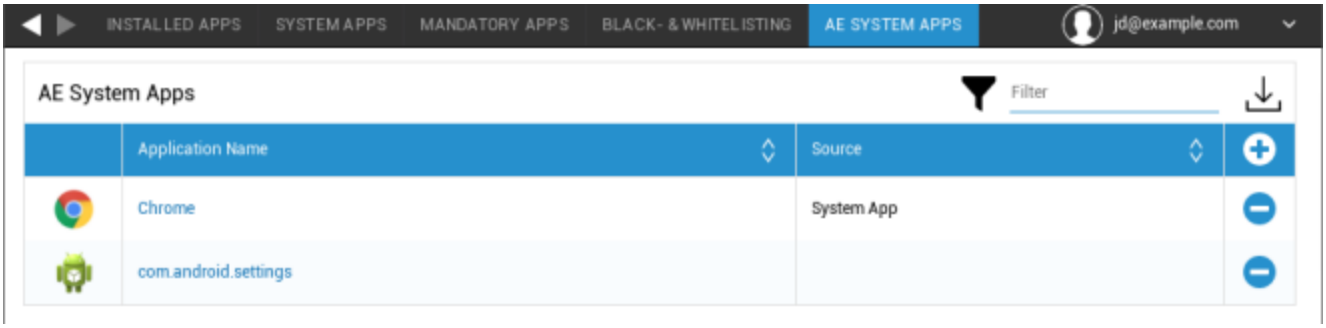
Білий список	На кінцевий пристрій користувача можна встановити лише додані до списку програми та сервіси. Якщо вони вже встановлені на пристрої кінцевого користувача, вони будуть активовані та налаштовані, щоб користувач міг їх запустити.
	Всі інші програми, які не додані до списку, не можуть бути встановлені на кінцевий пристрій користувача. Якщо вони вже встановлені на пристрої кінцевого користувача, їх буде деактивовано і встановлено так, що користувач не зможе їх запустити.
Чорний список	Додані до списку програми та сервіси не можуть бути встановлені на пристрої кінцевого користувача. Якщо вони вже встановлені на пристрої кінцевого користувача, їх буде деактивовано і налаштовано так, що користувач не зможе їх запустити.
	Всі інші програми, які не додані до списку, можуть бути встановлені на пристрої кінцевого користувача. Якщо вони вже встановлені на пристрої кінцевого користувача, вони будуть активовані та налаштовані, щоб користувач міг їх запустити.

За допомогою кнопок , ви можете додати додаткові програми або сервіси до поточно використовуваного списку.
За допомогою кнопок , ви можете додати додаткові програми або сервіси до поточно неактивного списку.
Ви можете визначити "Ім'я пакета":

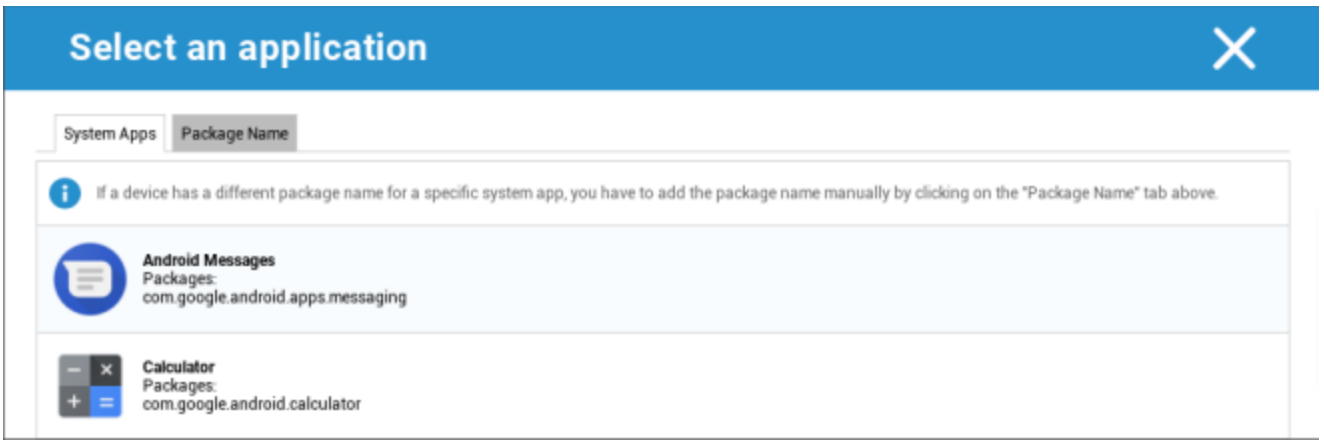

Select an application
Package Name
Enter App Identifier here ...
Add App

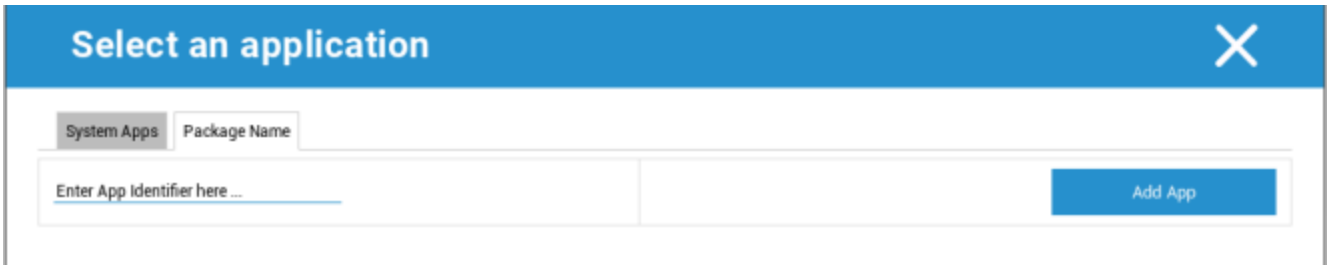
Додатки для системи AE

Тут ви можете визначити список, який містить певні системні програми, що мають бути активовані на пристроях.



Якщо ви натиснете на кнопку, ви зможете вибрати зі списку можливих системних додатків, наданих Google, або безпосередньо ввести назву пакета системного додатка, який потрібно активувати.





Будь ласка, майте на увазі, що системні програми у списку, наданому Google, - це лише програми, які можуть бути системними, але не обов'язково мають бути системними на ваших пристроях.

Однак цей список стосується лише тих програм, які вже встановлені.

Додавання додатків, які не є попередньо встановленими на ваших пристроях, не вплине на їхню роботу, незалежно від того, чи це додаток зі списку, наданого Google, чи ім'я пакунка додатка введено безпосередньо.

Обмеження та налаштування

Налаштування керування програмами

Тут ви можете налаштувати поведінку пристрою щодо оновлень програм.

Частота перевірки оновлення	Вкажіть, з яким інтервалом клієнт AppTec360 буде шукати оновлення програми. Значення за замовчуванням - 24 години.
Поріг Wi-Fi	Програми, розмір яких перевищує вказаний, буде завантажено через Wi-Fi. Якщо вибрано "Тільки Wi-Fi", всі програми буде завантажено через Wi-Fi.

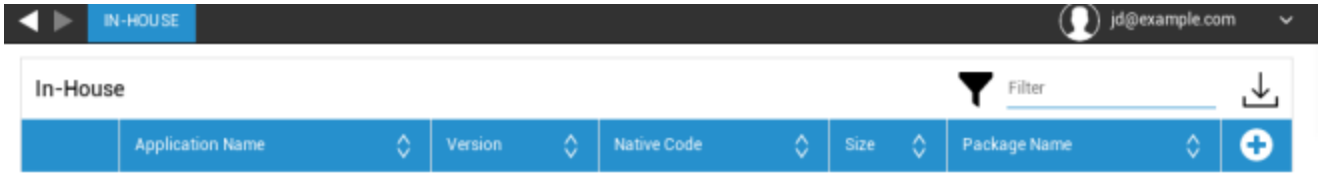
Enterprise App Store

Власні сили

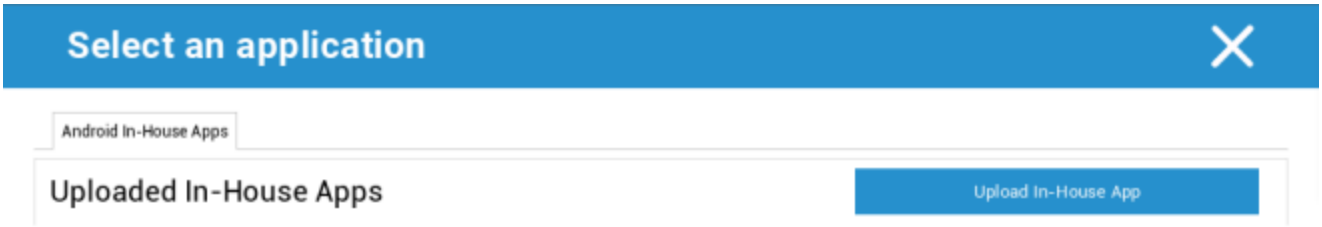
У пункті "In-House" ви можете завантажувати та розповсюджувати додатки, розроблені власними силами.

За допомогою цього символу ви можете розповсюджувати додаткові Внутрішні програми.

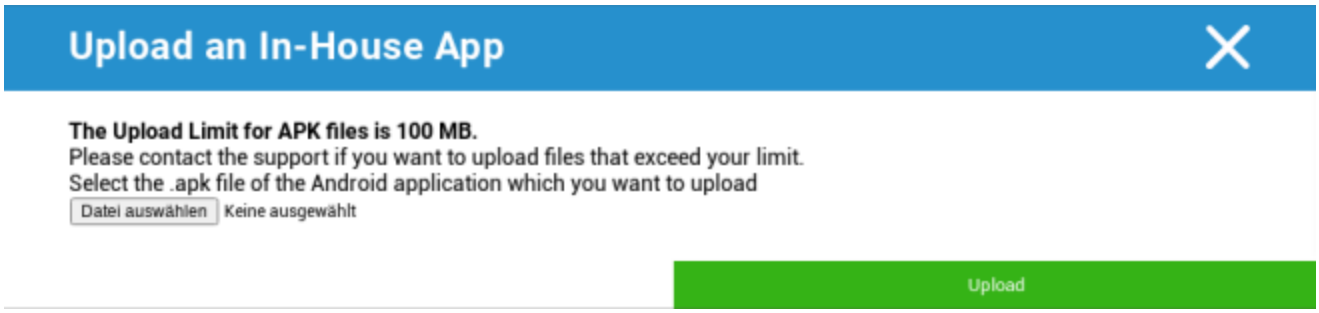
Якщо ви встановлюєте власний додаток, у вас буде можливість активувати функцію "Оновлювати". Якщо
ця функція активована і ви визначили новішу версію в базі даних власних додатків, додаток буде оновлюватися на пристрої.



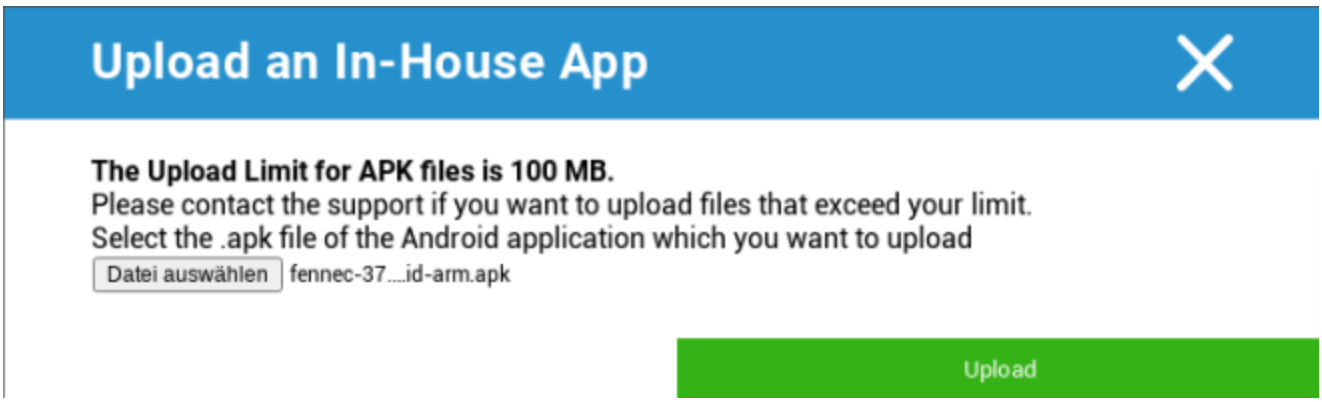
Якщо ви не розповсюджували внутрішні програми, ви отримаєте наступний огляд:



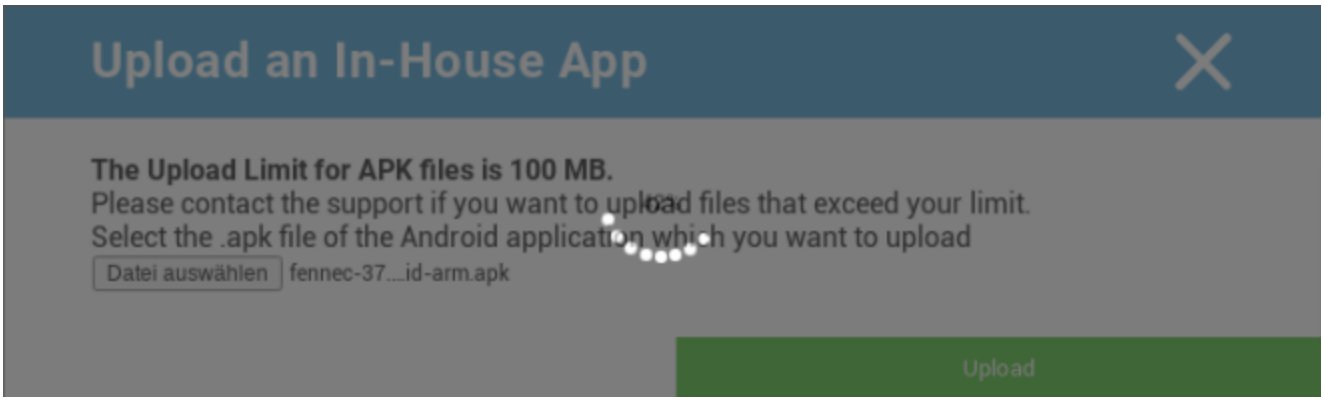
Для цього натисніть на "Завантажити власний додаток", після чого ви отримаєте наступний огляд:



Тепер виберіть за допомогою "Пошук..." файл .apk, а потім натисніть "Завантажити".



Ваш додаток буде завантажено, в середині кола ви побачите індикатор у відсотках, який показує, яку частину вашого додатку вже завантажено.



Якщо завантаження вашого внутрішнього додатку пройшло успішно, ви зможете знайти завантажений додаток
у вашому Каталозі додатків.

Тепер користувач має можливість переглянути та встановити цей додаток в AppTec360 Store на пристрої кінцевого користувача
в категорії "In-House".

Оскільки це не пов'язано з додатком Google PlayStore, користувачеві не потрібно зберігати ідентифікатор Google
на своєму кінцевому пристрої.

Enterprise Play Store

AE Play Store

Тут ви можете додавати програми до Android Enterprise Playstore. Зверніть увагу, що перед додаванням ви повинні схвалити додатки
у своєму обліковому записі адміністратора AE.

Щоб затвердити додаток, будь ласка, зверніться до інструкцій у розділі "Обов'язкові додатки".

Режим кіоску та лаунчер

Режим кіоску

Режим кіоску дозволяє вам попередньо визначити програму або URL-адресу. Тоді можна буде виключно
запустити/відвідати цю програму та/або URL-адресу.

Аналогічно, різні апаратні кнопки можна деактивувати в режимі "Кіоск".

Автоматичний запуск	Автоматично запускає режим кіоску, щойно профіль потрапляє на пристрій кінцевого користувача
Режим кіоску за розкладом?	Ви можете запланувати час для роботи в режимі кіоску, тоді він почнеться і завершиться автоматично, у встановлений вами час
Час початку	Час початку
Час у хвилинах	Час у хвилинах, після якого режим кіоску повинен знову завершитися

Тип програми

Єдиний додаток	Якщо ви хочете запустити програму в режимі кіоску, виберіть "Пакет" у розділі "Тип програми"
Додаток для кіоску	Натисніть тут, щоб вибрати програму, яку слід запустити в режимі кіоску Ви знайдете звичайний огляд управління додатками Ви можете вибрати між "Магазином Google Play", "Власними програмами Android" та "Ім'ям пакету"

Тип програми

URL	Якщо ви хочете запустити URL-адресу в режимі кіоску, виберіть "URL" у розділі "Тип програми" Потім визначте бажану URL-адресу
Очистити браузер після бездіяльності	Тут ви можете визначити інтервал часу в хвилинах, через який режим кіоску має бути перезапущено
Очистити веб-кеш і файли cookie	Якщо ви активуєте цю функцію, то після перезапуску режиму кіоску веб-кеш (файли cookie та кешовані зображення) буде стерто
Політика однакового походження	Якщо ця функція активна, то користувач може переглядати лише підсторінки визначеної URL-адреси Наприклад, ви визначили таку URL-адресу: www.mypage.com Тоді користувач може перейти за адресою: www.mypage.com/subpage
Білі списки URL-адрес	Тут ви можете вести білий список, всі ці URL-адреси дозволені Не більше 1 URL-адреси в рядку URL-адреса повинна починатися з http:/ або https://
URL-адреси в чорному списку	Тут ви можете вести чорний список, всі ці URL-адреси заборонені Не більше 1 URL-адреси в рядку URL-адреса повинна починатися з http:/ або https://
Орієнтація екрана	Цей параметр стосується налаштувань екрана Автоматичний = автоматичний Портрет = вертикальний формат Ландшафт = ландшафтний режим

Багатофункціональний додаток	Якщо ви виберете режим кіоску "Multi App", використання AppTec360 Launcher буде обов'язковим.
Додатки	Додаток: Виберіть Playstore або власний додаток як додаток для кіоску. Також можна ввести ім'я пакету. Вибраний додаток Kiosk повинен бути встановлений на пристрої. Не забудьте встановити додаток Kiosk як обов'язковий. Ярлик на головному екрані: Якщо увімкнено, буде створено ярлик на головному екрані. Якщо встановлено значення "Вимкнено", програма все одно відображатиметься у списку програм.

Увімкнено пароль на вихід	Якщо ви активуєте цю функцію, то користувач може завершити роботу в режимі кіоску за допомогою пароля, який ви попередньо визначили
Пароль для виходу	Це пароль, який ви визначили заздалегідь
Автоматичне згортання рядка стану	Якщо цей параметр увімкнено, рядок стану буде автоматично згорнуто. З цією опцією користувачі можуть бачити інформацію в рядку стану, але не можуть отримати доступ до його функцій
Вимкнути рядок стану	Рядок стану містить сповіщення, ярлики та інформацію. Доступно лише для пристроїв Samsung з версією SAFE 4.0 або вище.
Вимкнення клавіш гучності	Вимкнути клавіші гучності (доступно лише на пристроях Samsung з версією SAFE 3.0 або вище)
Вимкнути перемикач увімкнення / вимкнення	Вимкнути перемикач увімкнення / вимкнення (доступно лише на пристроях Samsung з версією SAFE 3.0 або вище)
Вимкнути кнопку "Додому	Вимкнути кнопку "Додому". Якщо ця функція активована, то режим кіоску можна завершити тільки в консолі AppTec360 (доступно лише на пристроях Samsung з версією SAFE 3.0 або вище)
Вимкнути панель навігації	За допомогою цього пункту ви можете вимкнути панель навігації (Назад / Меню) Якщо ця функція активована, то режим кіоску можна завершити тільки в консолі AppTec360 (доступно лише на пристроях Samsung з версією SAFE 3.0 або вище)

AppTec360 Launcher

Увімкніть AppTec360 Launcher	Увімкнено: Увімкнути програму запуску AppTec360. Користувач повинен встановити його як лаунчер за замовчуванням один раз. Примітка: Якщо увімкнено режим "Кіоск", а режим "Кіоск" встановлено на "Багато додатків", використання лаунчера AppTec360 буде обов'язковим.
Великі іконки	Увімкнено: Показує збільшену версію іконок програм на панелі запуску
Приховати піктограму програми AppTec360	Увімкнено: Повністю приховує програму AppTec360
Приховати іконку магазину AppTec360	Увімкнено: Повністю приховує AppTec360 Enterprise AppStore

Налаштування AppTec360

Увімкнути програму налаштувань AppTec360	Додаток AppTec360 Settings забезпечує контроль над з'єднаннями WiFi і Bluetooth
Увімкнення налаштувань у декількох додатках Режим кіоску	Якщо увімкнено, користувачі можуть отримати доступ до програми налаштувань AppTec360, коли активний режим кіоску з декількома додатками

Пульт дистанційного керування

Splashtop

Щоб розпочати сеанс дистанційного керування вашим пристроєм, необхідно встановити додаток "Splashtop Streamer" на пристрій, додавши його в **Керування додатками** → **Менеджер корпоративних додатків** → **Обов'язкові додатки**.

Після цього налаштуйте наступні параметри для Splashtop:

Увімкнути Splashtop	Якщо увімкнено, AppTec360 налаштує додаток Splashtop для дистанційного керування
Розгорнути код	Перейдіть на https://my.splashtop.com та увійдіть у свій обліковий запис Splashtop. Натисніть "Додати комп'ютер" і скопіюйте 12-значний код розгортання зі сторінки, що з'явиться.
Встановити користувацький шлюз для розгортання?	Розгортання шлюзу
Розгортання домену / хосту шлюзу	Розгортання шлюзу
Верифікація сертифікатів	Верифікація сертифікатів

Потім ви можете скористатися пунктом Пульт дистанційного керування Splashtop контекстного меню (шестірня поруч із рядком пошуку, коли пристрій вибрано, або клацніть правою кнопкою миші на пристрої в дереві), щоб розпочати сеанс дистанційного керування.

TeamViewer

Щоб розпочати сеанс дистанційного керування вашим пристроєм, необхідно встановити на ньому додаток "TeamViewer QuickSupport", додавши його в **Керування додатками** → **Менеджер корпоративних додатків** → **Обов'язкові додатки**.

Потім ви можете скористатися опцією **TeamViewer Remote Control** контекстного меню (шестерня поруч з рядком пошуку, коли пристрій вибрано, або клацнути правою кнопкою миші на пристрої в дереві), щоб розпочати сеанс віддаленого керування.

Управління контентом

ContentBox

Тут ви можете активувати ContentBox.

Як тільки ви перемкнете "Увімкнути ContentBox" на "Увімкнено", окремий додаток ContentBox буде автоматично встановлений
на пристрої кінцевого користувача.

Безпечний браузер

Тут ви можете налаштувати параметри безпечного браузера AppTec360.

Як тільки ви перемкнете розділ "Безпечний браузер" на "Увімкнено", окремий додаток для браузера
буде автоматично встановлений на пристрої кінцевого користувача.

Вимагати пароль	Вимагати від користувача встановлення та використання пароля для доступу до браузера.
Мінімальна необхідна довжина пароля	Встановіть необхідну кількість символів для пароля
Необхідна якість пароля	Встановіть необхідну якість пароля
Обмежити завантаження/відкриття	
Обмежити завантаження	
Завантажити білий список	Список URL-адрес, для яких завантаження завжди буде дозволено.
Дозволити копіювання	Дозволяє копіювати, вирізати або ділитися текстом всередині веб-сторінок.
Дозволити захоплення екрана	Дозволити створення скріншотів.
Частота очищення даних	Виберіть, з якою періодичністю слід автоматично видаляти BCI дані користувача (історію, кеш тощо).
Закладки компанії	Закладки з'являться в папці "Закладки компанії" в закладках браузера. Вони не можуть бути відредаговані користувачем.
Приховати адресний рядок	
Внутрішньобраузерний білий список (без універсального шлюзу)	Вмикає білі списки URL-адрес на стороні клієнта. • Закладки компанії завжди в білому списку • Підтримується лише для 100 URL-адрес • Будь ласка, використовуйте Універсальний шлюз для необмеженої кількості чорних та білих списків
Білі списки URL-адрес	Список дозволених URL-адрес.

Чорні та білі списки на основі шлюзу	До чорного списку висуваються наступні вимоги: • Працюючий універсальний шлюз AppTec360 ("Загальні налаштування" → "Універсальний шлюз") • Робоча конфігурація VPN із зазначеним DNS-сервером ("Загальні налаштування" → "Універсальний шлюз" → "Налаштування VPN") • Налаштування чорного списку ("Загальні налаштування" → "Універсальний шлюз" → "Чорний список доменів") • Дійсне VPN-з'єднання в профілі ("Управління з'єднаннями" → "VPN")

Додатковий API

Samsung KNOX

Обмеження

Дозволити SD-карту	
Дозволити запис на SD-карту	
Дозволити захоплення екрана	
Дозволити буфер обміну	
Резервне копіювання налаштувань і даних програм у Google Cloud	
Відновлення налаштувань з Google Cloud під час перевстановлення програми	
Дозволити налагодження USB	
Дозволити Google Crash Report	
Дозволити скидання до заводських налаштувань	
Дозволити оновлення OTA	
Дозволити хост-накопичувач USB	Якщо увімкнено, користувач може підключити будь-який флеш-накопичувач (портативний USB-накопичувач), зовнішній кардрідер HD або Secure Digital (SD), і він буде встановлений як накопичувач на пристрої.
Дозволити USB медіаплеєр (MTP, PTP)	
Увімкнути мікрофон	Вимикає мікрофон для сторонніх програм
Дозволити NFC (ближній радіозв'язок)	
Дозволити невідомі джерела (APK Sideloading)	Якщо увімкнено, дозволено бічне завантаження додатків (APK-файлів). Якщо цей параметр вимкнено, користувачеві доведеться увімкнути його вручну, коли ви дозволите встановлення APK з невідомих джерел.

Дозволити створення користувачів	Якщо увімкнено, користувачеві дозволено створювати кілька облікових записів на пристрої, наприклад, гостьові облікові записи

Електронна пошта

Адреса електронної пошти	
Вхідний протокол сервера	
Вхідна адреса сервера	
Вхідний порт сервера	
Вхідний логін/ім'я користувача на сервері	
Вхідний пароль сервера	
Вхідний сервер використовує SSL	
Вхідний сервер використовує TLS	
Вхідний сервер приймає всі сертифікати	
Протокол вихідного сервера	
Адреса вихідного сервера	
Вихідний порт сервера	
Вихідний сервер використовує додаткові облікові дані	Якщо цю опцію вимкнено, система використовує вхідні облікові дані і для вихідного сервера.
Логін/ім'я користувача вихідного сервера	
Пароль вихідного сервера	
Вихідний сервер використовує SSL	
Вихідний сервер використовує TLS	
Вихідний сервер приймає всі сертифікати	
Встановити підпис	
Підпис	Примітка: Для деяких пристроїв підпис потрібно вказувати у форматі HTML.
Сповіщати користувача про отримання нової електронної пошти	

Обмін

Адреса електронної пошти	
Ім'я хосту сервера	Ім'я хоста Exchange-сервера
Ім'я користувача Ім'я користувача	Ім'я користувача, яке використовується для входу на сервер Exchange Server
Домен	Якщо конфігурація шлюзу ACL увімкнена і поле Домен не порожнє, універсальний шлюз AppTec360 буде аутентифікувати пристрій з наступним ім'ям "Домен\Ім'я для входу
Пароль	
Кількість попередніх днів для синхронізації	
Частота для синхронізації електронної пошти	
Синхронізація в роумінгу	
Встановити підпис	
Підпис	Примітка: Для деяких пристроїв підпис потрібно вказувати у форматі HTML.
Обліковий запис за замовчуванням	
Використовуйте протокол захищених сокетів (SSL)	
Використовуйте захист на транспортному рівні (TLS)	
Приймаємо всі сертифікати	

APN

APN Відображуване ім'я	
Назва точки доступу Ім'я точки доступу	Назва APN
Протокол вихідного сервера	
MCC - мобільний код країни	Залиште порожнім, щоб використовувати mmc встановленої SIM-карти
MNC - код мобільної мережі	Залиште порожнім, щоб використовувати mnc встановленої SIM-карти
Адреса сервера	
Номер порту сервера	
Проксі-адреса сервера	
Адреса сервера MMS	Залиште порожнім за замовчуванням
Номер порту MMS	Залиште порожнім за замовчуванням
Адреса проксі-сервера MMS	Залиште порожнім за замовчуванням
Ім'я користувача	
Пароль	
Тип точки доступу	Допустимі типи: "default", "mms", "supl".
	Якщо передано null або порожньо, за замовчуванням використовується "default,supl,mms".
	Залиште порожнім за замовчуванням.
Бажаний APN	

Bluetooth

Дозволити виявлення пристрою через Bluetooth	
Дозволити створення пари Bluetooth	
Дозволити пристрої з Bluetooth-гарнітурою	
Дозволити Bluetooth-пристрої гучного зв'язку	
Дозволити пристрої Bluetooth A2DP	A2DP, розширений профіль розподілу аудіо, дозволяє передавати аудіопотоки між пристроями
Дозволити вихідні дзвінки	
Дозволити передачу даних через Bluetooth	
Увімкнути прив'язку Bluetooth	
Дозволити підключення до комп'ютера через Bluetooth	

Підключення

Дозволити лише екстрені викликиДозволити Wi-Fi	
Мінімальний рівень безпеки мережі Wi-Fi	
Заборонити користувачеві додавати мережі Wi-Fi	Це обмеження можна активувати, лише якщо в розділі Керування підключеннями визначено принаймні один активний профіль Wi-Fi
Дозволити SMS та MMS	
Дозволити синхронізацію в роумінгу	
Дозволити голосовий роумінг	

Android Enterprise – повністю керований пристрій з робочим профілем (COPE)

Загальне пояснення COPE

COPE - це абревіатура від **Corporate Owned Personally Enabled**.

Режим COPE дозволяє зареєструвати пристрій Android як **Android Enterprise - Повністю керований пристрій** з інтегрованим профілем **Android Enterprise - Контейнер**.

Це може бути або пристрій Android, який вже зареєстрований як **Android Enterprise - Fully Managed Device** і на якому додатково налаштовано **Android Enterprise - Container**, або новий пристрій Android, який безпосередньо зареєстрований як **Android Enterprise - Fully Managed Device** разом з **Android Enterprise - Container**, встановленим на ньому.

Режим COPE доступний лише для пристроїв з Android 8, 9 і 10

Конфігурація профілів для пристроїв COPE

Оскільки для самого режиму COPE немає профілю конфігурації, конфігурація **Android Enterprise - Повністю керований пристрій** і **Android Enterprise - Контейнер** розділена на два профілі в межах профілю COPE. Можна перемикатися між двома профілями для конфігурації кожного з них, натиснувши на відповідну кнопку в лівій частині консолі:

Обидва профілі можна налаштувати, як описано для кожного окремого профілю:

Android Enterprise - повністю керований пристрій

Android Enterprise - Контейнер

Повернення до повністю керованого пристрою AE

Профіль **Android Enterprise - Container** можна видалити, як описано в розділі **Керування мобільними** пристроями.

Якщо видалити профіль Container, профіль COPE буде перетворено на профіль **Android Enterprise - Fully Managed Device**.

Android Enterprise – Конфігурація контейнера

Залежно від того, який профіль групи або пристрою ви вибрали, огляд і його підпункти відрізняються - будь ласка, зверніть на це увагу!

Генерал

Огляд профілю (тільки на рівні профілю)

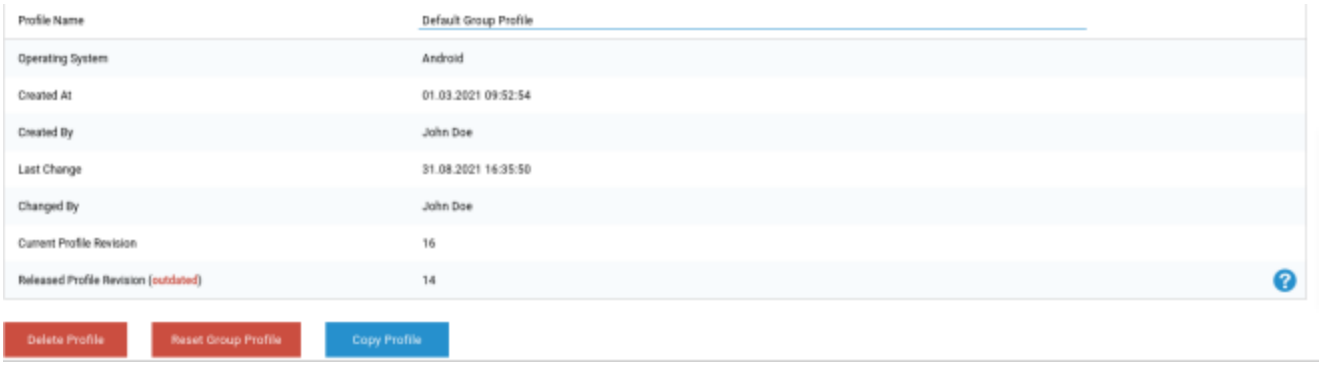
Якщо у вас є профіль, ви отримаєте короткий огляд профілю: ім'я, операційна система, дата створення, автор тощо.

Ім'я профілю Ім'я профілю	Назва профілю - можна безпосередньо перейменувати тут
Операційна система	Допустима операційна система для профілю
Створено в	Дата створення
Створено	Створено
Остання зміна	Дата останньої зміни
Змінено	Користувач, який вносив останні зміни до цього профілю
Поточна редакція профілю	Кількість разів, коли профіль вже оновлювався
Випущено ревізію профілю	Кількість разів, коли профіль вже оновлювався і йому були призначені пристрої

Видалити профіль	Видалити профіль
Скинути профіль групи	Скинути профіль групи
Копіювати профіль	Копіювати профіль

Огляд профілю групи (тільки на рівні групи)

Відкривши профіль групи, ви отримаєте короткий огляд профілю.



Ім'я профілю Ім'я профілю	Назва профілю (можна змінити тут)
Операційна система	Операційна система, для якої призначений профіль
Створено в	Час створення
Створено	Творець профілю
Остання зміна	Час останньої зміни профілю
Змінено	Обліковий запис, який вніс останні зміни
Поточна редакція профілю	Перегляд стану збереженого профілю
Випущено ревізію профілю	Призначена версія профілю ("Призначити зараз"). Якщо за текстом мітки вказано "(застаріла)", це означає, що ви зберегли профіль, але ще не призначили його, тому пристрої все одно отримають стару версію.

Огляд пристрою (тільки на рівні пристрою)

Якщо ви перебуваєте на пристрої, ви отримаєте оглядову інформацію про вибраний пристрій, яка міститься тут:

Назва пристрою	Назва пристрою
Місцезнаходження	Координати розташування
Номер телефону	Номер телефону
Призначені обов'язкові програми	Кількість призначених Обов'язкових додатків
Версія ОС	Версія операційної системи пристрою
Операційна система	Операційна система (Android Enterprise)
Серійний номер	Серійний номер пристрою
Право власності на пристрій	Корпоративний або приватний пристрій
Тип пристрою	Пристрій керування роботою AE
Укорінений	Статус, що вказує на те, чи був пристрій вкорінений
Дотримується	Відповідає настановам
IP-адреса	IP-адреса пристрою
Востаннє бачили	Момент часу, коли пристрій востаннє підключався до AppTec
Останній поштовх	Момент часу, коли на пристрій було надіслано останнє push-повідомлення
Призначення користувача	Користувач або група, якій призначено цей пристрій

Ревізія конфігурації

Тут ви отримаєте огляд того, який профіль групи призначено пристрою.

Якщо ви натиснете на профіль групи, ви отримаєте прямий доступ до цього профілю і зможете виконати налаштування.

За допомогою цього символу ви можете повернути розподілені програми до налаштувань профілю групи.

За допомогою цього символу ви можете повернути всі використовувані програми до налаштувань профілю групи.

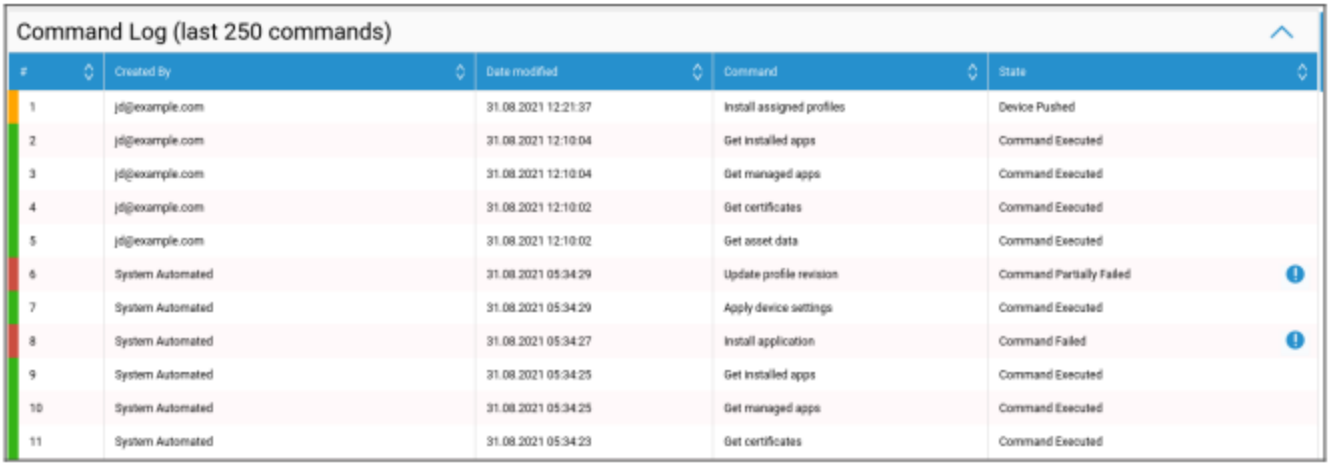
"Доступна новіша версія" вказує на те, що профіль групи було змінено та збережено, але не призначено. Щоб застосувати зміни до пристроїв, профіль групи потрібно призначити за допомогою "Призначити зараз" на рівні групи.

Журнал пристрою (тільки на рівні пристрою)

Тут ви отримаєте різні логи пристрою. Якщо потрібно, ви можете безпосередньо дізнатися причину помилки тут.

Командний журнал

Тут ви можете побачити, які команди були видані для пристрою і який їхній статус.



Можливі стани команди

Пристрій натиснуто	До служби push (наприклад, APNS) було надіслано push-запит, щоб повідомити пристрій про необхідність з'єднатися з сервером EMM.
Команду створено	Команда була створена в системі.
Команду відправлено.	Команда була надіслана на пристрій після того, як він підключився до сервера.
Команду виконано	Команда була успішно виконана.
Команда не спрацювала	Команда не спрацювала. *
Команда частково не виконана	Залежно від операційної системи пристрою деякі команди можуть бути згруповані разом. У цьому деякі частини цієї командної групи зазнали невдачі. *
Команда виконана, але зрештою не спрацювала	Команда була виконана, але, можливо, не була.
Команда "Відсіч	Команду було перевиконано користувачем.
Викинуто	Команду було відкинуто. Наприклад, її було замінено іншою командою або пристрій було перереєстровано, а старі команди видалено

*Якщо за повідомленням стоїть знак оклику, ви можете отримати додаткову інформацію, навівши курсор на іконку.

Налаштування пристрою

Конфігурація клієнта

Тут ви можете виконати наступні конфігурації на вашому пристрої Android:

Порушення термінів дотримання вимог	Граничний таймаут відповіді користувача, після якого застосовується дія примусового виконання.
Примусові заходи після закінчення терміну виконання	Примусова дія, коли користувач не виконує дій, які призводять до сумісного стану пристрою
Частота збору даних	Частота, з якою пристрій / GPS-інформація повинна збиратися
Частота серцебиття пристрою	Інтервал, через який пристрій повинен зв'язуватися з сервером AppTec Server Хвилина. 1 хвилина Максимум. 24 години
Увімкнути оновлення місцезнаходження	Якщо увімкнено, пристрій надсилає оновлення місцезнаходження на сервер AppTec Server
Час оновлення місцезнаходження	Визначає, через які проміжки часу пристрій надсилає оновлення місцезнаходження до AppTec
Використовуйте Google Location Accuracy для оновлення місцезнаходження	Якщо увімкнено, то для оновлення місцезнаходження буде використовуватися мережеве розташування (якщо це було деактивовано в розділі "Обмеження", то це налаштування ні на що не вплине)
Використовуйте GPS-локацію для оновлення місцезнаходження	Якщо увімкнено, GPS буде використовуватися для оновлення місцезнаходження
Дозволити імітацію (фейкові) локації	Дозволяє підробляти інформацію про місцезнаходження за допомогою сторонніх додатків
Дія "Втрата зв'язку	Якщо увімкнено, ви можете вказати дію на випадок, якщо пристрій не отримає з'єднання з MDM-сервером протягом інтервалу серцебиття. Наприклад, якщо час серцебиття пристрою становить 5 хвилин, він з'єднається з сервером о 10:35 ранку. Після цього пристрій виходить з діапазону Wi-Fi. Наступне серцебиття о 10:40 буде невдалим, і вказана дія буде виконана.
Дія	Дії, які необхідно вжити, як тільки пристрій стає невідповідним.

		• Lock Пристрій = пристрій блокування • Очистити пристрій = пристрій буде відновлено до заводських налаштувань • Wipe Device & SD Card = пристрій буде відновлено до заводських налаштувань, а пам'ять на SD-карті буде видалено
	Поріг	Ви можете вказати поріг кількості невдалих серцевих скорочень, які необхідні для запуску вказаної дії.

Режим застосування політики	За замовчуванням:	Користувачі будуть періодично отримувати запити на виконання незавершених дій
	Ліниве впровадження політики:	Користувачам ніколи не буде запропоновано виконати незавершені дії. Всі відкриті дії будуть показані в клієнті AppTec
	Агресивне впровадження політики:	Користувачам будуть постійно пропонувати виконати незавершені дії
AppTec Блокування версій	Якщо увімкнено, можна вказати код версії програми AppTec. Клієнт AppTec оновлюватиметься лише до вказаної версії. Новіші версії будуть ігноруватися. Пониження версії НЕ можливе.	
Код версії	Код версії програми AppTec, до якої потрібно прив'язати додаток.	
Вимкнути сповіщення AppTec	Якщо цей параметр вимкнено, клієнт AppTec не показуватиме сповіщення у панелі сповіщень. Таким чином, користувачі можуть закрити клієнт AppTec за допомогою диспетчера завдань. Якщо клієнт AppTec закрито, деякі функції, включно з режимом кіоску та чорним/білим списком додатків, не працюватимуть належним чином. Пристрої Samsung пропонують механізм захисту для клієнта AppTec. Сповіщення за замовчуванням вимкнено на пристроях Samsung, які підтримують KNOX API. Сповіщення не повинно відключати пристрої з Android 8.0 або новішої версії.	

Шпалери

Встановіть власні шпалери	Увімкнути/вимкнути кастомні шпалери
Шпалери	Налаштуйте режим шпалер для використання кольорового коду або зображення
Вкажіть колір	Вкажіть колір фону у вигляді шістнадцяткового значення, наприклад, #000000 для чорного або #ffffff для білого.
Встановити зображення як шпалери	Завантажте файл зображення, який ви хочете використовувати як шпалери

Управління активами (тільки на рівні пристрою)

Інформація про пристрій

Модель	Позначення моделі пристрою
Операційна система	ОС
Версія ОС	Версія операційної системи
Серійний номер	Серійний номер
Назва пристрою	Назва пристрою
Стан акумулятора	Стан акумулятора
Вільна / загальна пам'ять	Вільна / Загальна пам'ять
Samsung Safe	Інтерфейс Samsung SAFE, необхідний для різноманітних налаштувань
Доступна SD-карта	Доступна SD-карта
Емуляція SD-карти	Емуляція SD-карти
Знімна SD-карта	Знімна SD-карта
Вільна пам'ять SD / загальна пам'ять	Вільна пам'ять на SD / Загальна пам'ять на SD-карті

Wi-Fi

IP-адреса	IP-адреса пристрою
MAC-адреса WiFi	MAC-адреса WiFi

Стільниковий зв’язок

Статус	Статус (встановлена SIM-карта)
Номер телефону	Номер телефону
Роумінг (голосовий зв'язок / передача даних)	Роумінг для передачі голосу/даних
Статус роумінгу	Поточний статус у роумінгу
IP-адреса	IP-адреса
Оператор/перевізник	Оператор/перевізник
Стільникові технології	Стільникові технології
IMEI	Номер IMEI
ICCID	Це ідентифікатор SIM-картки, часто також смарт-картки або картки з інтегральною схемою (ICC)
IMSI	Міжнародна мобільна ідентифікація абонента (IMSI) забезпечує в GSM- і UMTS-мережах однозначну ідентифікацію користувачів мережі IMSI складається максимум з 15 цифр і налаштовується наступним чином: • Мобільний код країни (MCC), 3 цифри • Код мобільної мережі (MNC), 2 або 3 цифри • Ідентифікаційний номер абонента мобільного зв'язку (MSIN), 1-10 цифр
Поточний ГХК/МНК	Див. розділ "SIM MCC/MNC"
SIM MCC/MNC	Мобільний код країни - це визнаний ідентифікатор країни, встановлений MCE відповідно до стандарту E.212. Він працює разом з кодом мобільної мережі (MNC) для ідентифікації мобільної мережі. Означає код країни/мобільної мережі SIM-карти. Якщо ви перебуваєте в роумінгу в іншій мобільній мережі, то логічно, що "Поточний MCC/MNC" і "MCC/MNC SIM" будуть відрізнятися.

Bluetooth

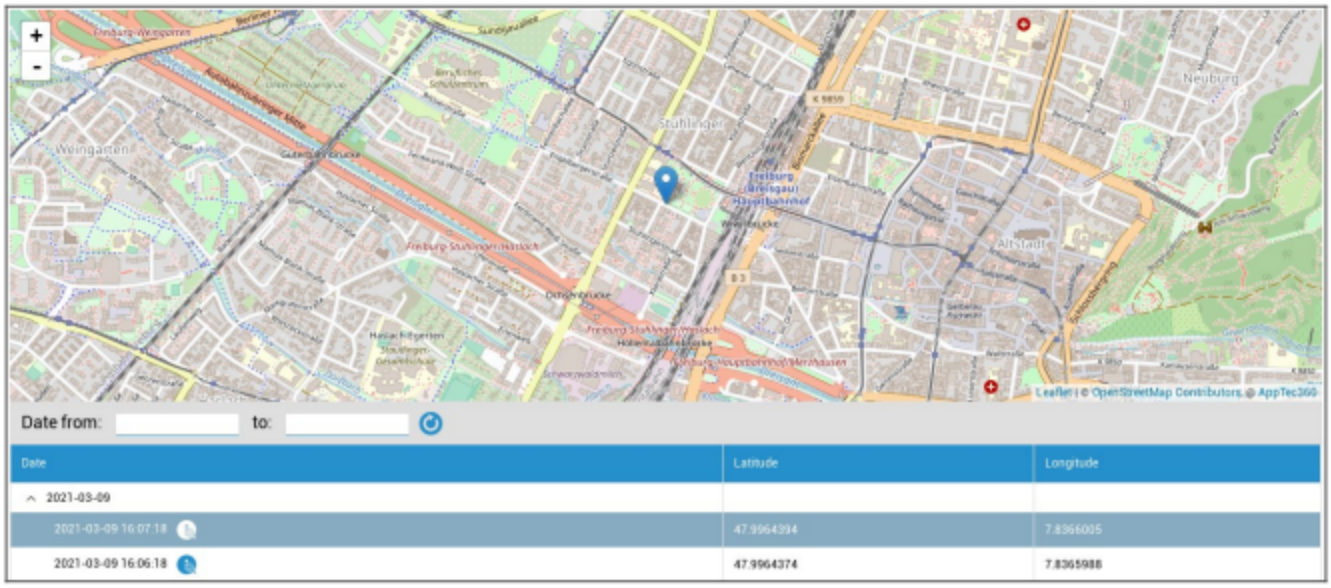
MAC-адреса Bluetooth	MAC-адреса Bluetooth

Управління безпекою

Захист від крадіжок (лише на рівні пристрою)

Інформація про GPS (лише на рівні пристрою)

Тут ви можете встановити поточне/останнє місцезнаходження пристрою. Локалізацію можна захистити одним або навіть двома паролями - Див: Загальні налаштування - Конфіденційність - Доступ до GPS



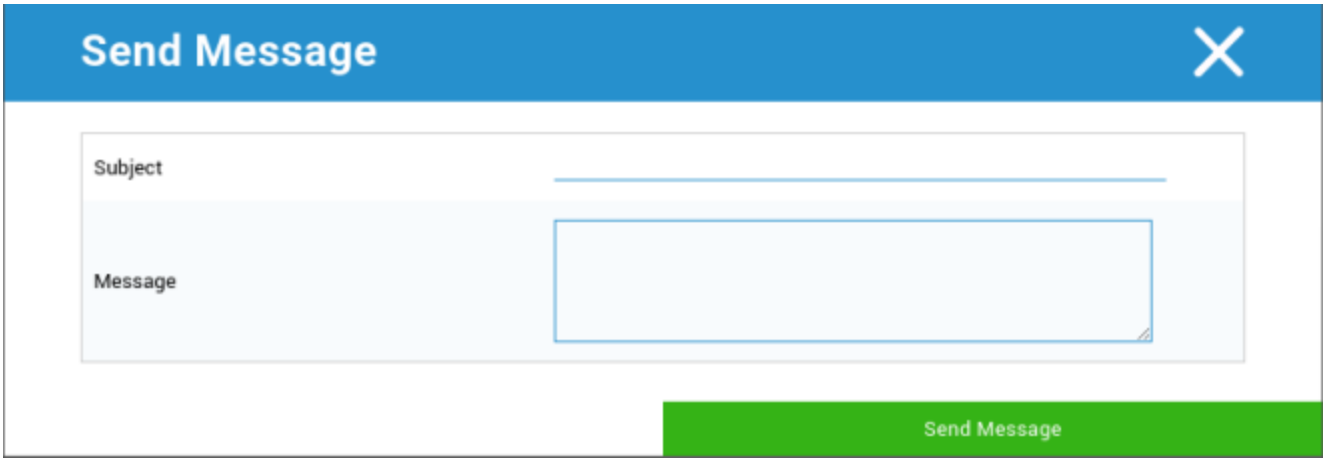
Wipe & Lock (тільки на рівні пристрою)

У розділі "Витирання та блокування" ви можете виконати наступні три дії:

Повне витирання	Пристрій відновлюється до заводських налаштувань (корпоративні, а також особисті дані видаляються). Працює тільки для Розширеного робочого профілю
Enterprise Wipe	З пристрою кінцевого користувача видаляються лише корпоративні дані (всі додатки, дані тощо, які були надані AppTec)
Екран блокування	Блокування екрану активоване, достатньо розблокувати пристрій за допомогою пароля/коду пристрою

Повідомлення (тільки на рівні пристрою)

Тут ви можете заповнити тему та повідомлення і відправити його на пристрій кінцевого користувача



Конфігурація безпеки

Код доступу до пристрою

У розділі "Пароль" ви можете встановити пароль пристрою, вам доступні наступні варіанти налаштувань

Мінімальна довжина пароля	Визначає мінімальну кількість символів, які повинен містити пароль	
Якість пароля	Не визначено	Ця політика не містить вимог до пароля.
	Біометричні слабкі	Ця політика дозволяє використовувати технології біометричного розпізнавання з низьким рівнем безпеки. Це означає технології, які можуть розпізнати особу приблизно до 3-значного PIN-коду (ймовірність помилкового розпізнавання - менше ніж 1 на 1000).
	Щось.	Ця політика вимагає встановлення певного пароля або шаблону, але не запроваджує жодних конкретних правил.
	Алфавітний	Користувач повинен ввести пароль, що містить принаймні літерні (або інші символи) символи.
	Буквено-цифровий	Користувач повинен ввести пароль, що містить принаймні обидва символи - цифри та літери (або інші символи).
	Комплекс	За замовчуванням користувач повинен ввести пароль, що містить щонайменше літеру, цифру та спеціальний символ. З такою якістю пароля можна обмежити його вміст різними наборами символів, наприклад, принаймні великими літерами тощо.
Мінімальна довжина пароля	Встановіть необхідну кількість символів для пароля. Наприклад, ви можете вимагати, щоб PIN-код або пароль містив щонайменше шість символів.	
Мінімальна кількість цифр у паролі	Мінімальна кількість цифр у паролі	
Мінімум малих літер у паролі	Мінімум малих літер у паролі	
Мінімальна кількість великих літер у паролі	Мінімальна кількість великих літер у паролі	

Мінімальна кількість нелітерних символів у паролі	Мінімальна кількість нелітерних символів у паролі
Мінімальна кількість символів у паролі	Мінімальна кількість символів у паролі

Блокування максимального часу бездіяльності	Максимальна бездіяльність користувача до моменту блокування часу
Таймаут терміну дії пароля	Встановлює, через який проміжок часу закінчується термін дії пароля і потрібно видати новий пароль
Обмеження історії паролів	Кількість раніше використаних паролів, які не допускаються
Максимальна кількість невдалих спроб введення пароля	Визначає, як часто можна вводити пароль неправильно, перш ніж буде виконано повне очищення пристрою
Дозволити біометричну автентифікацію	Дозволяє автентифікацію за допомогою сканування відбитка пальця або райдужної оболонки ока. Тільки для Samsung KNOX 2.1 і вище

Код доступу до контейнера

У розділі "Пароль" ви можете задати пароль контейнера, вам доступні наступні варіанти налаштувань

Мінімальна довжина пароля	Визначає мінімальну кількість символів, які повинен містити пароль	
Якість пароля	Не визначено	Ця політика не містить вимог до пароля.
	Біометричні слабкі	Ця політика дозволяє використовувати технології біометричного розпізнавання з низьким рівнем безпеки. Це означає технології, які можуть розпізнати особу приблизно до 3-значного PIN-коду (ймовірність помилкового розпізнавання - менше ніж 1 на 1000).
	Щось.	Ця політика вимагає встановлення певного пароля або шаблону, але не запроваджує жодних конкретних правил.
	Алфавітний	Користувач повинен ввести пароль, що містить принаймні літерні (або інші символи) символи.
	Буквено-цифровий	Користувач повинен ввести пароль, що містить принаймні обидва символи - цифри та літери (або інші символи).
	Комплекс	За замовчуванням користувач повинен ввести пароль, що містить щонайменше літеру, цифру та спеціальний символ. З такою якістю пароля можна обмежити його вміст різними наборами символів, наприклад, принаймні великими літерами тощо.
Мінімальна довжина пароля	Встановіть необхідну кількість символів для пароля. Наприклад, ви можете вимагати, щоб PIN-код або пароль містив щонайменше шість символів.	
Мінімальна кількість цифр у паролі	Мінімальна кількість цифр у паролі	
Мінімум малих літер у паролі	Мінімум малих літер у паролі	
Мінімальна кількість великих літер у паролі	Мінімальна кількість великих літер у паролі	
Мінімальна кількість	Мінімальна кількість нелітерних символів у паролі	

нелітерних символів у паролі	
Мінімальна кількість символів у паролі	Мінімальна кількість символів у паролі

Блокування максимального часу бездіяльності	Максимальна бездіяльність користувача до моменту блокування часу
Таймаут терміну дії пароля	Встановлює, через який проміжок часу закінчується термін дії пароля і потрібно видати новий пароль
Обмеження історії паролів	Кількість раніше використаних паролів, які не допускаються
Максимальна кількість невдалих спроб введення пароля	Визначає, як часто можна вводити пароль неправильно, перш ніж буде виконано повне очищення пристрою

Антивірус

Автоматичне сканування	Увімкнути періодичне автоматичне сканування
Інтервал сканування	Інтервал для обстеження (Швидкий / Повний)
Повне автоматичне сканування	Увімкнути повне автоматичне сканування
Автоматичні оновлення	Увімкнути автоматичні оновлення
Інтервал перевірки оновлення	Як часто потрібно оновлювати додаток та його базу даних (віруси / пошкоджений код)
Захист додатків	Увімкнути автоматичне сканування програм
Захист SD-карти	Увімкнути автоматичне сканування SD-карти
Оновлення тільки для Wi-Fi	Якщо увімкнено, оновлення будуть застосовуватися лише тоді, коли пристрій успішно підключено до мережі Wi-Fi

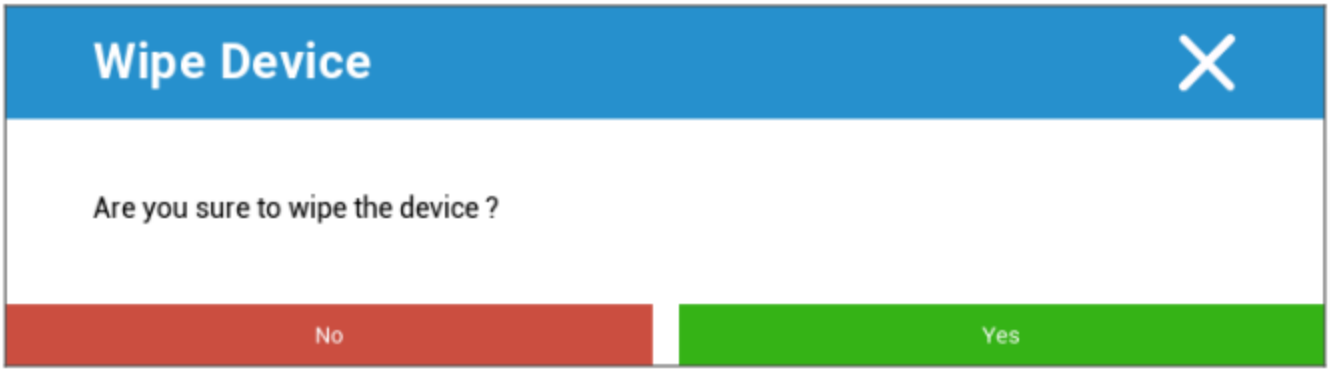
Кінець життя (тільки на рівні пристрою)

Витирання (тільки на рівні пристрою)

У розділі "Очищення" ви можете відновити заводські налаштування пристрою (лише у розширеному робочому профілі).

При цьому корпоративні, а також приватні дані будуть видалені на пристрої кінцевого користувача.

При натисканні на "Символ мінус" ви отримаєте наступне повідомлення:



За допомогою "Так" ви можете виконати стирання.

У розділі "Звіт про витирання" можуть відображатися такі елементи

Витерто	Історія про те, хто виконував стирання
Дата	Дата
Статус	Статус (наприклад, якщо очищення було виконано успішно)

Налаштування обмежень

Обмеження

Тут можна обмежити та заблокувати безліч речей.

Забезпечення комплаєнсу	Режим Підказка користувачеві - Користувачеві буде запропоновано виконати необхідні дії. Режим Lock-Down Container - приховати всі програми, поки не будуть виконані всі вимоги
Політика дозволів на виконання	Підказка користувачеві про нові запити на дозволи Завжди надавайте нові запити на отримання дозволів Завжди відхиляйте нові запити на отримання дозволів Попередження: Деякі програми мають проблеми з розпізнаванням дозволів, якщо вони встановлені автоматично. Якщо ви завжди надаєте дозволи і стикаєтеся з проблемами, коли програми повідомляють, що дозволів не вистачає, встановіть для цього параметра значення "запитувати користувача" і переінсталюйте програму
Дозволити вихідний буфер обміну	Дозволяє копіювати та вставляти зсередини контейнера назовні
Дозволити дозвіл ідентифікатора абонента	Показує ім'я для вхідного дзвінка на основі контактів у контейнері
Дозволити роздільну здатність пошуку контактів	Дозволяє шукати імена в контактах контейнера при здійсненні дзвінків
Дозволити обмін контактами через Bluetooth	Дозволяє отримати доступ до контакту контейнера в автомобілі
Заборонити вихідний промінь NFC	Вимкнення NFC для контейнера
Дозволити невідомі джерела	Якщо увімкнено, користувачі можуть завантажувати програми, встановивши файл .apk.
Дозволити налагодження USB	Якщо увімкнено, користувачі можуть увімкнути налагодження USB.
Заборонити зміну облікового запису	Забороняє створення, видалення та модифікацію облікових записів у контейнері

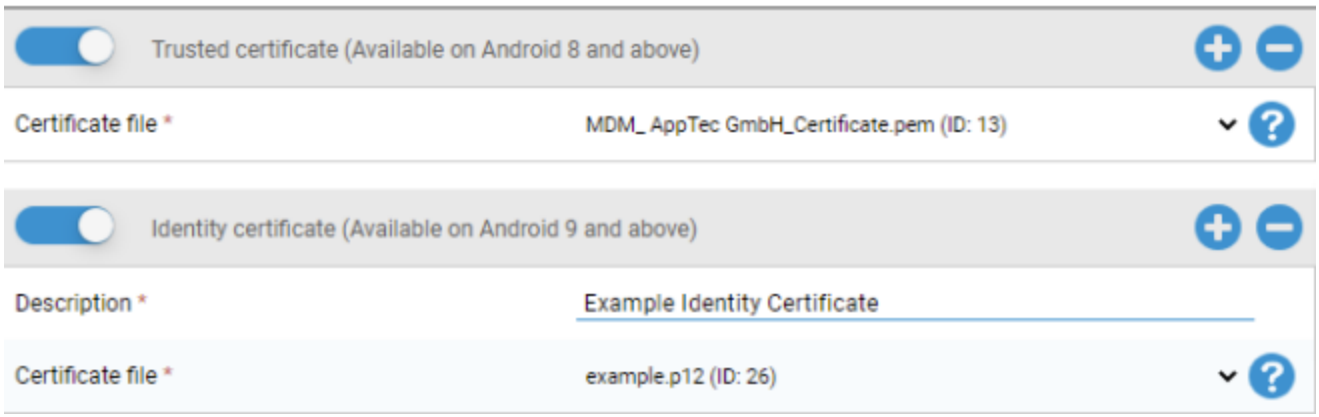
	Майте на увазі, що деякі програми потребують створення або зміни облікових записів, щоб працювати належним чином

Обмеження робочого профілю. Доступно лише на пристроях Android 11 і вище з розширеним робочим профілем	
Заборонити камеру	Вказує, чи заборонено камеру у робочому профілі.
Заборонити Bluetooth	Вказує, чи заборонено Bluetooth у робочому профілі.
Увімкнути захист від скидання до заводських налаштувань	Увімкніть цю функцію, щоб обійти захист Android від скидання до заводських налаштувань для облікового запису Google, який ви визначили в "Загальні налаштування" → "Конфігурація Android" → "Android Enterprise" → "Захист від скидання до заводських налаштувань" Якщо цю функцію увімкнено і ви скинете пристрій, вам потрібно буде надати налаштований обліковий запис Google, щоб налаштувати пристрій знову.
Керування оновленням ОС	Увімкніть цей параметр, щоб встановити поведінку оновлення: автоматичне, у вікні або відкладене.
Політика оновлення	Автоматично: Інсталювати автоматично, щойно стане доступним оновлення. Через вікно: Інсталювати автоматично у вікні щоденного обслуговування. Це також налаштовує програми Play на оновлення у вікні. Наполегливо рекомендується для кіоскових пристроїв, оскільки це єдиний спосіб оновити програми, постійно закріплені на передньому плані, за допомогою Play. Відкласти: Відкласти автоматичну інсталяцію максимум на 30 днів.

Обмеження особистого профілю. Доступно лише на пристроях Android 11 і вище з розширеним робочим профілем	
Заборонити камеру	Вказує, чи заборонено камеру в особистому профілі.
Заборонити Bluetooth	Вказує, чи заборонено Bluetooth в особистому профілі.
Дозволити невідомі джерела	Якщо увімкнено, користувачі робочого профілю можуть завантажувати програми, встановивши файл .apk.

Управління сертифікатами

Тут ви можете розповсюджувати довірені сертифікати та ідентифікаційні сертифікати на ваші пристрої. Для розповсюдження довірених сертифікатів потрібна Android 8 або новіша версія, а для розповсюдження ідентифікаційних сертифікатів - Android 9 або новіша версія.



За допомогою "+" ви можете додати кілька сертифікатів.

Довірені сертифікати повинні бути у форматі PEM.

Посвідчення особи повинні бути у форматі PKCS12.

Керування з’єднаннями

Wi-Fi

Для цього налаштування виконайте попередню конфігурацію пристроїв кінцевих користувачів для доступу до внутрішніх точок доступу

Ідентифікатор набору послуг (SSID)	SSID мережі, до якої потрібно підключитися
Прихована мережа	Активувати, якщо точка доступу не передає SSID

Тип безпеки

Встановіть тип захисту точки доступу

WEP

Пароль	Пароль для точки доступу

WPA/WPA2

Пароль	Пароль для точки доступу

802.1x EAP

EAP-метод

PWD	Ідентичність	Ідентичність
	Пароль	Пароль

PEAP	Етап 2 Протокол автентифікації	ні	Без додаткового протоколу
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертифікат центру сертифікації	Сертифікат центру сертифікації	
	Ідентичність	Ідентичність	
	Анонімна ідентичність	Анонімна особистість	
	Пароль	Пароль	

TTLS	Етап 2 Протокол автентифікації	ні	Без додаткового протоколу
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертифікат центру сертифікації	Сертифікат центру сертифікації	
	Ідентичність	Ідентичність	
	Анонімна ідентичність	Анонімна ідентичність	
	Пароль	Пароль	

TLS	Сертифікат центру сертифікації	Сертифікат центру сертифікації
	Ідентичність	Ідентичність
	Пароль	Пароль

VPN

Ім'я з'єднання Ім'я з'єднання	Назва VPN-з'єднання

Тип VPN

VPN

Клієнт VPN

AppTec VPN клієнт	
Конфігурація шлюзу	Виберіть конфігурацію шлюзу VPN (див. **Загальні налаштування > Універсальний шлюз > Налаштування VPN**)
Завжди увімкнений VPN	Увімкнути власне блокування
Увімкнути блокування AppTec	Увімкнути блокування AppTec

Вбудований (доступний лише на пристроях Samsung)			
Тип підключення	PPTP	Сервер	Сервер
		Увімкнути шифрування PPTP	Увімкнути шифрування PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Увімкнути секрет L2TP	Увімкнути секрет L2TP
		Секрет L2TP	Секрет L2TP
	IPSec XAuth PSK	Сервер	Сервер
		Ідентифікатор IPSec	Ідентифікатор IPSec
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
Пошукові домени DNS	Пошукові домени DNS		
Налаштування експерта	DNS-сервери	DNS-сервери	
	Маршрути переадресації	Маршрути переадресації	

Відкрити VPN		
Сервер	Сервер	
Профіль OpenVPN	Профіль OpenVPN	
Додаток OpenVPN	OpenVPN для Android (рекомендовано)	
	OpenVPN Connect	
Налаштування експерта	DNS-сервери	DNS-сервери
	Маршрути переадресації	Маршрути переадресації

Samsung / Сильний лебідь			
Тип підключення	PPTP	Сервер	Сервер
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути шифрування PPTP	Увімкнути шифрування PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути секрет L2TP	Секрет L2TP
	IPSec XAuth PSK	Сервер	Сервер
		Ідентифікатор IPSec	Ідентифікатор IPSec
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
Налаштування експерта	DNS-сервери	DNS-сервери	
	Маршрути переадресації	Маршрути переадресації	

Cisco Any Connect		
Сервер	Сервер	
Режим сертифіката	Інваліди	Інваліди
	Автоматично	Автоматично
Налаштування експерта	DNS-сервери	DNS-сервери
	Маршрути переадресації	Маршрути переадресації

Per-App VPN

Клієнт VPN

AppTec VPN клієнт		
Конфігурація шлюзу	Виберіть конфігурацію шлюзу VPN (див. **Загальні налаштування > Універсальний шлюз > Налаштування VPN**)	
Програми VPN	Програми VPN	
Завжди увімкнений VPN	Увімкнути власне блокування	Завжди увімкнений VPN
Увімкнути блокування AppTec	Увімкнути блокування AppTec	

Samsung / Сильний лебідь			
Тип підключення	PPTP	Сервер	Сервер
		Програми VPN	Програми VPN
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути шифрування PPTP	Увімкнути шифрування PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Програми VPN	Програми VPN
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
		Увімкнути секрет L2TP	Секрет L2TP
	IPSec XAuth PSK	Сервер	Сервер
		Програми VPN	Програми VPN
		Ідентифікатор IPSec	Ідентифікатор IPSec
		Ключ IPSec Pre-Shared Key	Ключ IPSec Pre-Shared Key
		Ім'я користувача	Ім'я користувача
		Пароль	Пароль
Налаштування експерта	DNS-сервери	DNS-сервери	
	Маршрути переадресації	Маршрути переадресації	

Обмеження

Тут ви можете встановити обмеження щодо управління з'єднаннями

Дозволити роумінг даних	Дозволити мобільні дані в роумінгу
Примусити роумінг даних	Якщо увімкнено, роумінг для мобільних даних активується назавжди (не рекомендується!). Цей параметр замінює параметр "Дозволити роумінг даних"!
Використання системного проксі-сервера http	Використання HTTP-проксі-сервера, яке передбачено налаштуваннями системи в налаштуваннях, залежить від підключеної мережі (WiFi або APN)

Менеджмент ПІМ

Обмін Gmail

Info: Ця конфігурація буде застосована до програми Gmail. Тому вам потрібно схвалити та встановити Gmail.

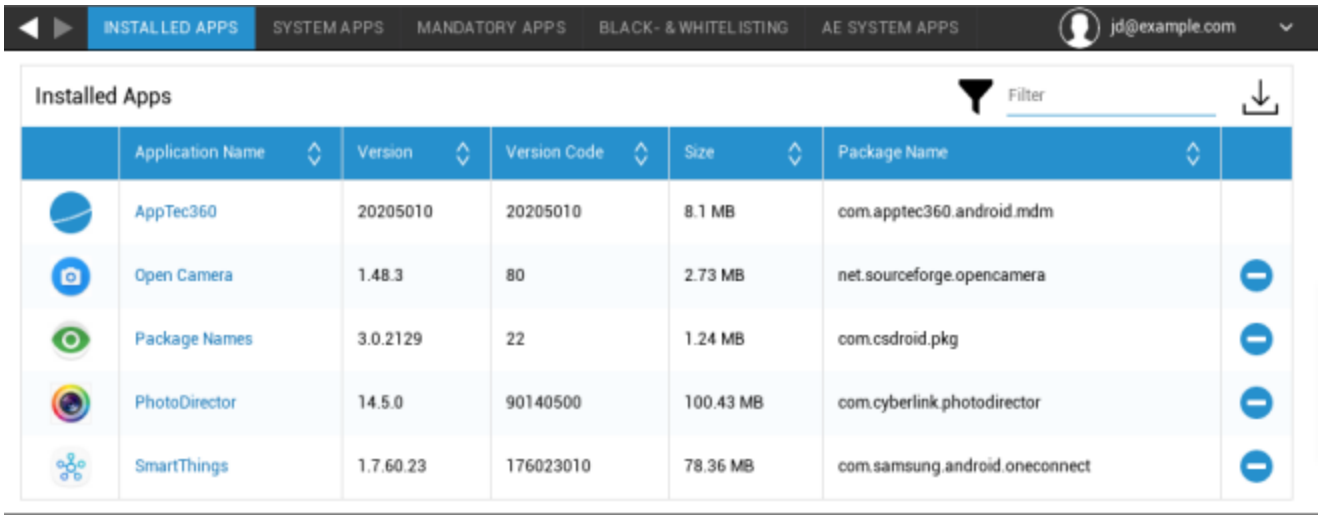
Адреса електронної пошти	Надана адреса електронної пошти користувача Зверніть увагу на "Заповнювачі", які можна використовувати для роботи з обліковими даними і не виконувати зміни вручну на кожному пристрої Натиснувши на них, ви можете переглянути їх для себе
Ім'я хосту сервера	Адреса сервера ваших Exchange-серверів
Ім'я користувача	Ім'я для входу для відповідного пристрою кінцевого користувача, також зверніть увагу на "Заповнювачі тут
Підпис	Можна додати підпис (Підказка: деякі пристрої вимагають HTML-форматування для підпису)
Кількість попередніх днів для синхронізації	Кількість днів, які визначають, коли імейли будуть синхронізовані знову
Ідентифікатор пристрою	Рядок, який містить ідентифікатор пристрою EAS. Він є частиною протоколу EAS і потрібен в окремих випадках
Використовуйте протокол захищених сокетів (SSL)	Використовуйте SSL-з'єднання
Приймаємо всі сертифікати	Приймаються всі сертифікати. Виберіть цю опцію, якщо ваш Exchange-сервер використовує самопідписаний сертифікат
Дозволити некеровані акаунти	Дозволити користувачам додавати або видаляти будь-які облікові записи Exchange, окрім облікового запису, вказаного в цій керованій конфігурації. Якщо цей параметр увімкнено, ви не зможете заборонити користувачам додавати інші облікові записи Exchange до Gmail. Ви також не зможете контролювати обмін даними між іншими програмами та акаунтами Exchange, доданими користувачами. Цей параметр слід увімкнути, лише якщо вашим користувачам потрібно мати більше одного робочого акаунта Exchange у Gmail.
Сертифікат клієнта	Сертифікат клієнта. Потрібен лише в тому випадку, якщо ваш поштовий сервер очікує його наявності.

Керування додатками

Enterprise App Manager

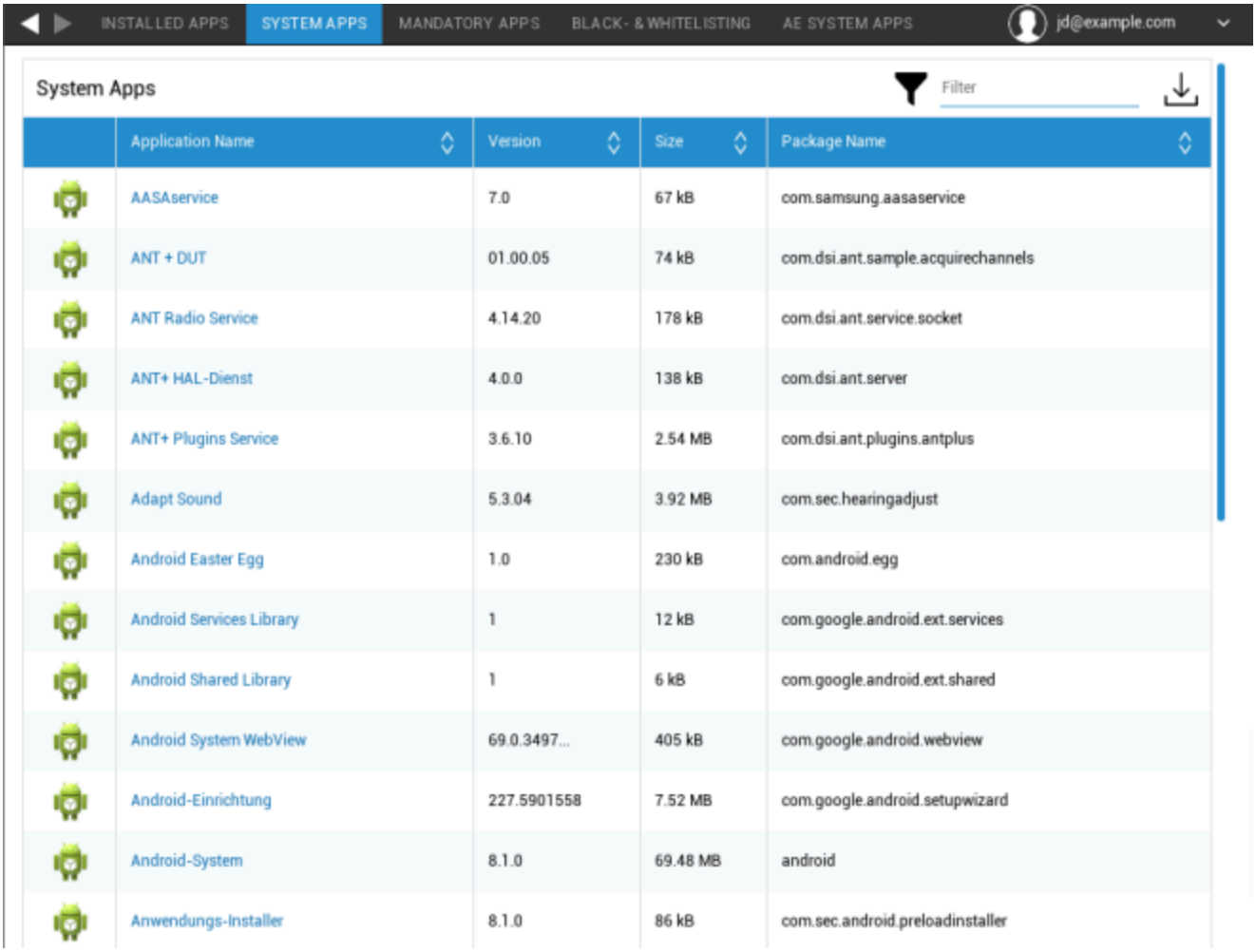
Встановлені програми (лише на рівні пристрою)

Тут будуть показані всі програми, які наразі встановлені в контейнері.



Системні програми (лише на рівні пристрою)

У розділі "Системні програми" будуть перераховані всі програми та служби, які вже встановлені на кінцевому пристрої користувача виробником пристрою.

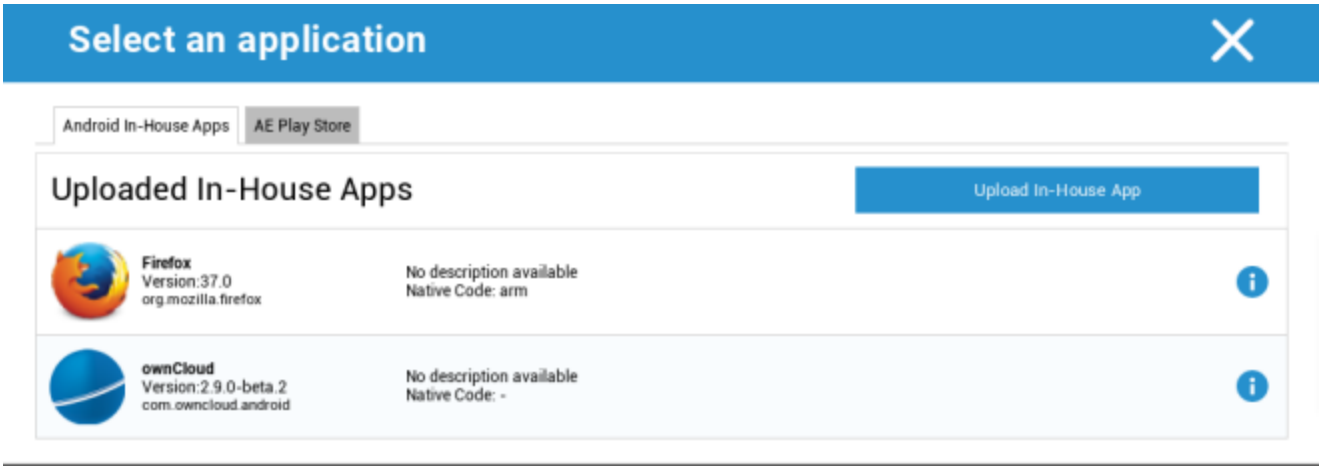


Обов’язкові програми

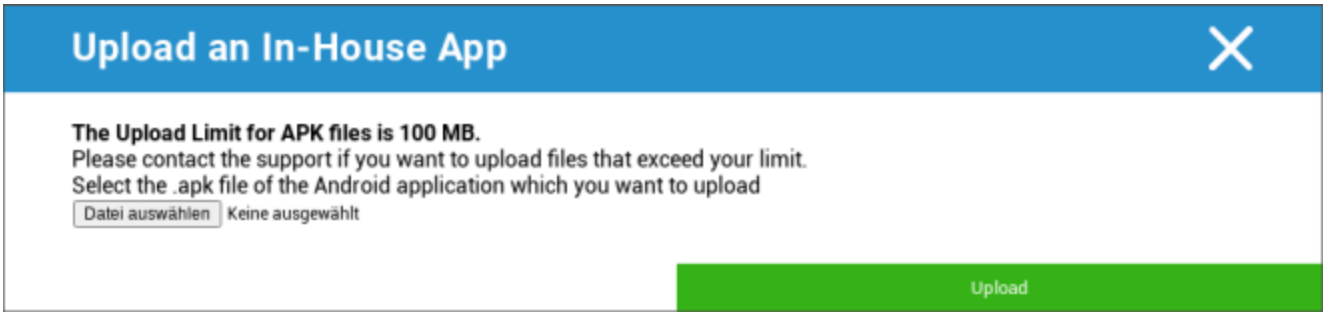
У розділі Обов'язкові програми ви можете встановити обов'язкові програми. Користувачеві буде постійно пропонуватися встановити цю програму, якщо вона є власною розробкою. Додатки з Play Store будуть встановлені автоматично.

За допомогою , можна визначити необхідний додаток.

Це може бути власний додаток з папки "Власні додатки Android", який ви завантажили в Загальних налаштуваннях.

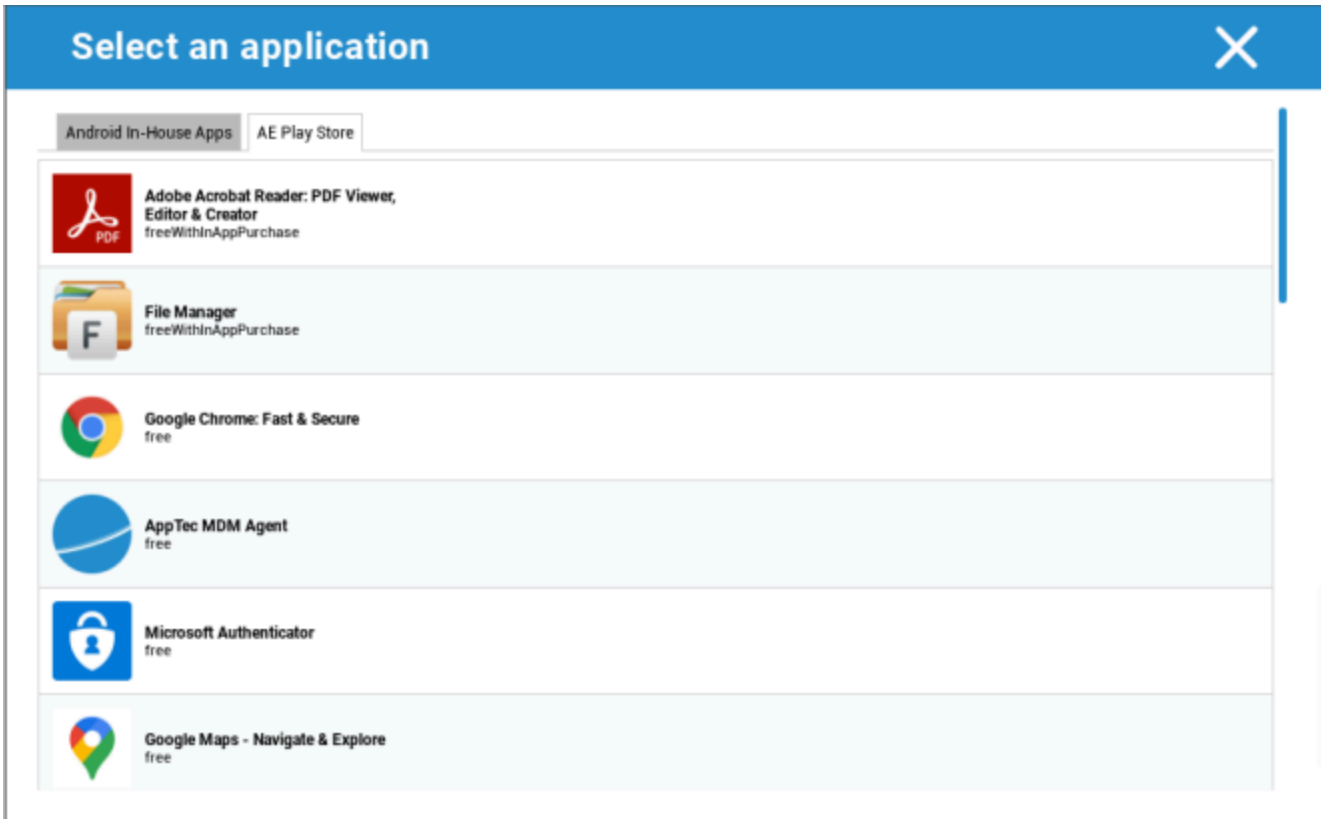


Ви також можете безпосередньо вибрати і завантажити apk-файл за допомогою функції "Завантажити власний додаток".



Якщо ви встановлюєте власний додаток, у вас буде можливість активувати функцію "Оновлювати". Якщо вона активована і ви визначили нову версію в базі даних власних додатків, додаток буде оновлено на пристрої.

Або це може бути додаток "AE Play Store" з Google Work Play Store.



На цій вкладці будуть показані лише схвалені додатки "AE Play Store Apps".

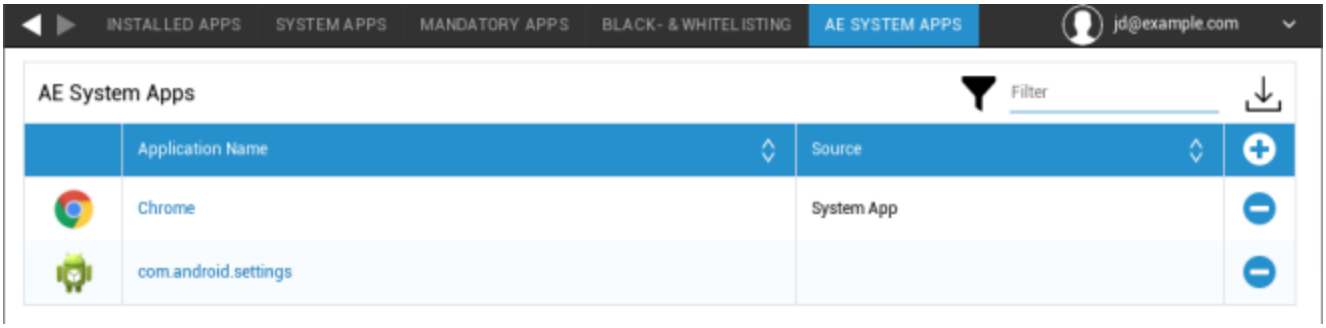
Щоб затвердити "AE Play Store App", перейдіть в "Загальні налаштування" > "Керування додатками" > "AE Play

Store" і додайте додаток за допомогою кнопки, яка перенаправить вас на вкладку "Play Store Apps" (або ви можете безпосередньо перейти на вкладку "Play Store Apps").

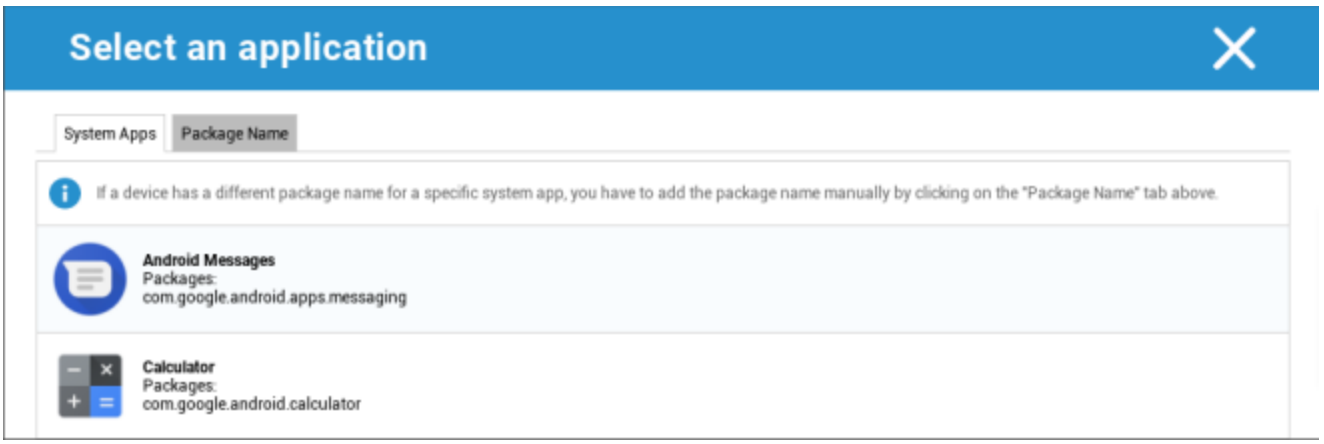
На вкладці "Додатки Play Store" ви можете шукати додатки. Коли ви натискаєте на програму, відкривається сторінка програми, де ви можете затвердити програму, натиснувши на кнопку "Затвердити".

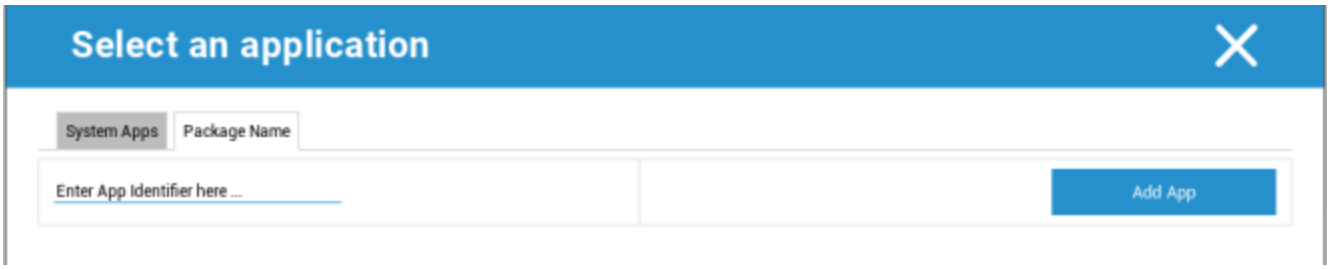
Додатки для системи AE

Тут ви можете визначити список, який містить певні системні програми, що мають бути активовані на пристроях.



Якщо ви натиснете на кнопку, ви зможете вибрати зі списку можливих системних додатків, наданих Google, або безпосередньо ввести назву пакета системного додатка, який потрібно активувати.





Будь ласка, майте на увазі, що системні програми у списку, наданому Google, - це лише програми, які можуть бути системними, але не обов'язково мають бути системними на ваших пристроях.

Однак цей список стосується лише тих програм, які вже встановлені.

Додавання додатків, які не є попередньо встановленими на ваших пристроях, не вплине на їхню роботу, незалежно від того, чи це додаток зі списку, наданого Google, чи ім'я пакунка додатка введено безпосередньо.

Обмеження та налаштування

Налаштування керування програмами

Тут ви можете налаштувати поведінку пристрою щодо оновлень програм.

Частота перевірки оновлення	Вкажіть, з яким інтервалом AppTec Client буде шукати оновлення програми. Значення за замовчуванням - 24 години.
Поріг Wi-Fi	Програми, розмір яких перевищує вказаний, буде завантажено через Wi-Fi. Якщо вибрано "Тільки Wi-Fi", всі програми буде завантажено через Wi-Fi.

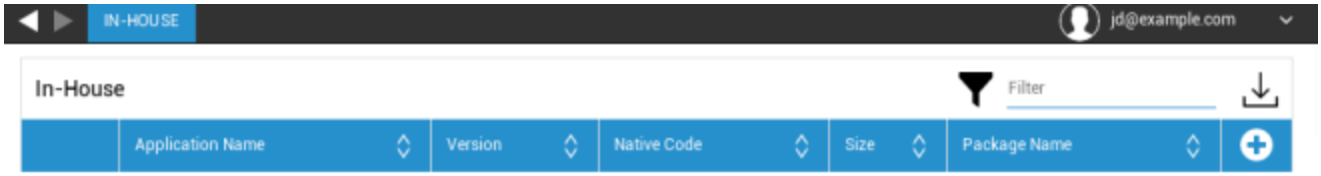
Enterprise App Store

Власні сили

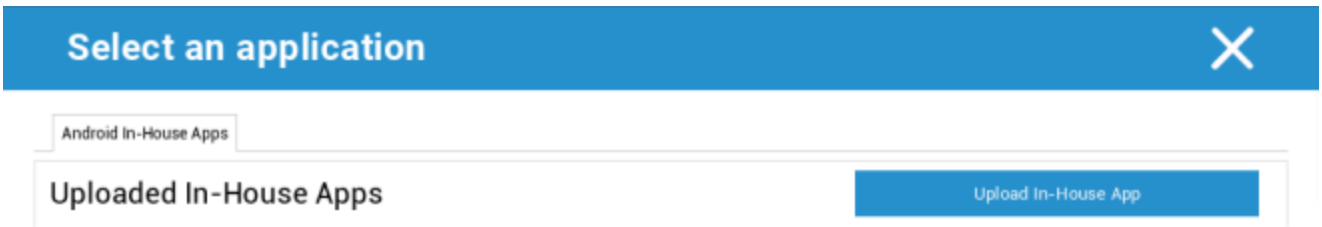
У пункті "In-House" ви можете завантажувати та розповсюджувати додатки, розроблені власними силами.

За допомогою цього символу ви можете розповсюджувати додаткові Внутрішні програми.

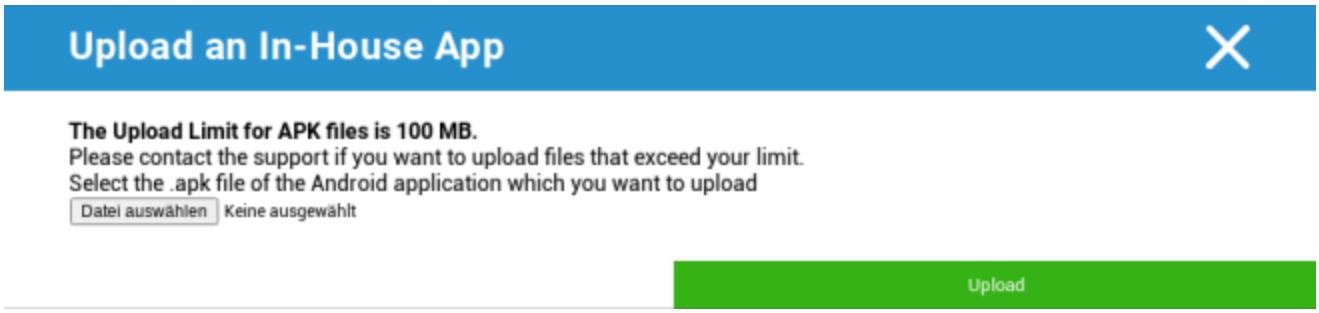
Якщо ви встановлюєте власний додаток, у вас буде можливість активувати функцію "Оновлювати". Якщо вона активована і ви визначили нову версію в базі даних власних додатків, додаток буде оновлено на пристрої.



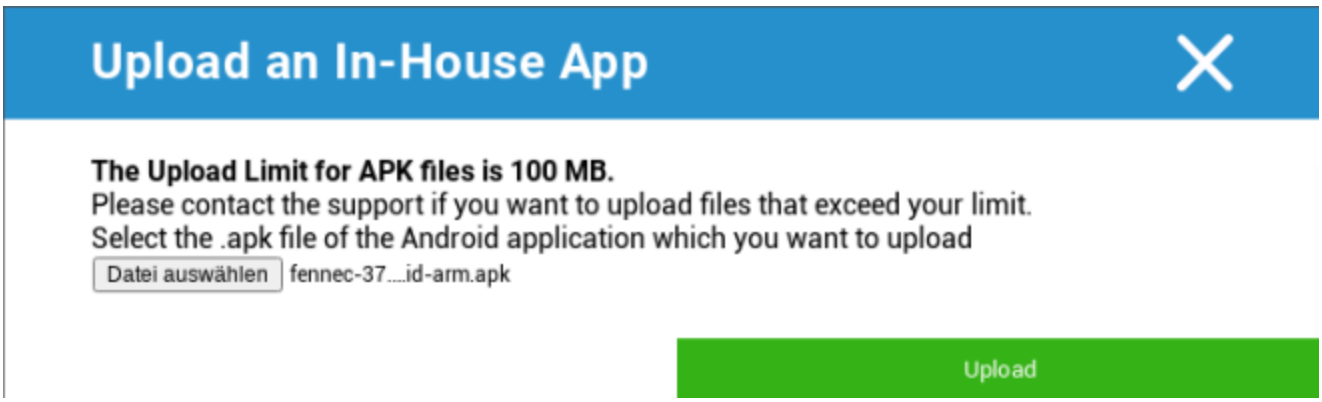
Якщо ви не розповсюджували внутрішні програми, ви отримаєте наступний огляд:



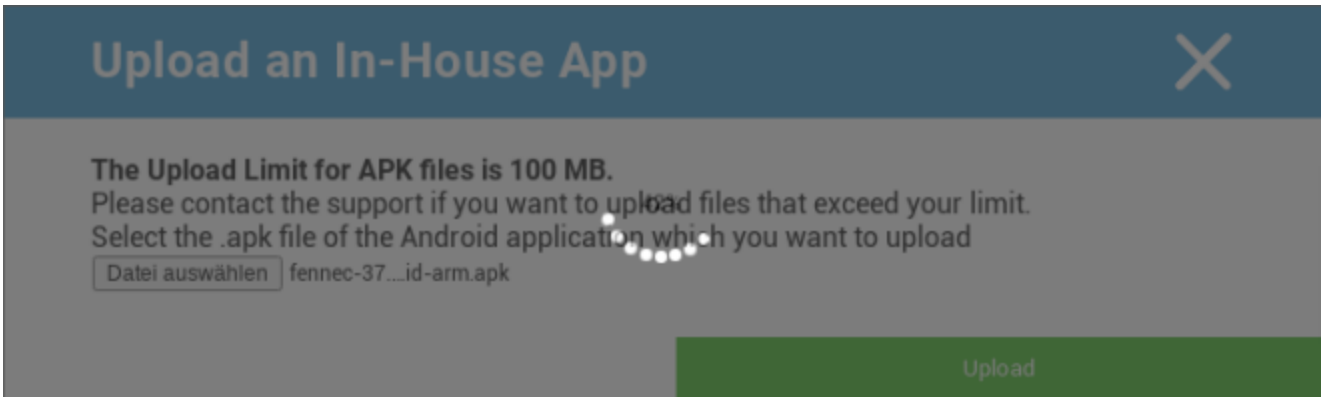
Для цього натисніть на "Завантажити власний додаток", після чого ви отримаєте наступний огляд:



Тепер виберіть за допомогою "Пошук..." файл .apk, а потім натисніть "Завантажити".



Ваш додаток буде завантажено, в середині кола ви побачите індикатор у відсотках, який показує, яку частину вашого додатку вже завантажено.



Якщо завантаження вашого внутрішнього додатку пройшло успішно, ви зможете знайти завантажений додаток у вашому Каталозі додатків.

Тепер користувач має можливість переглянути та встановити цей додаток в AppTec Store на пристрої кінцевого користувача в категорії "In-House".

Оскільки це не пов'язано з додатком Google PlayStore, користувачеві не потрібно зберігати ідентифікатор Google ID на своєму кінцевому пристрої.

Enterprise Play Store

AE Play Store

Тут ви можете додавати програми до Android Enterprise Playstore. Зверніть увагу, що перш ніж додавати програми, ви повинні схвалити їх у своєму обліковому записі адміністратора AE.

Щоб затвердити додаток, будь ласка, зверніться до інструкцій у розділі "Обов'язкові додатки".

Управління контентом

ContentBox

Тут ви можете активувати ContentBox.

Щойно ви перемкнете "Увімкнути ContentBox" на "Увімкнено", окремий додаток ContentBox буде автоматично інстальовано на пристрої кінцевого користувача.

Безпечний браузер

Тут ви можете налаштувати параметри AppTec Secure Browser.

Як тільки ви перемкнете розділ "Безпечний браузер" на "Увімкнено", на кінцевий пристрій користувача буде автоматично встановлено окремий додаток для браузера.

Вимагати пароль	Вимагати від користувача встановлення та використання пароля для доступу до браузера.
Мінімальна необхідна довжина пароля	Встановіть необхідну кількість символів для пароля
Необхідна якість пароля	Встановіть необхідну якість пароля
Обмежити завантаження/відкриття	
Обмежити завантаження	
Завантажити білий список	Список URL-адрес, для яких завантаження завжди буде дозволено.
Дозволити копіювання	Дозволяє копіювати, вирізати або ділитися текстом всередині веб-сторінок.
Дозволити захоплення екрана	Дозволити створення скріншотів.
Частота очищення даних	Виберіть, з якою періодичністю слід автоматично видаляти BCI дані користувача (історію, кеш тощо).
Закладки компанії	Закладки з'являться в папці "Закладки компанії" в закладках браузера. Вони не можуть бути відредаговані користувачем.
Приховати адресний рядок	
Внутрішньобраузерний білий список (без універсального шлюзу)	Вмикає білі списки URL-адрес на стороні клієнта. • Закладки компанії завжди в білому списку • Підтримується лише для 100 URL-адрес • Будь ласка, використовуйте Універсальний шлюз для необмеженої кількості чорних та білих списків
Білі списки URL-адрес	Список дозволених URL-адрес.
Чорні та білі списки на основі шлюзу	До чорного списку висуваються наступні вимоги:

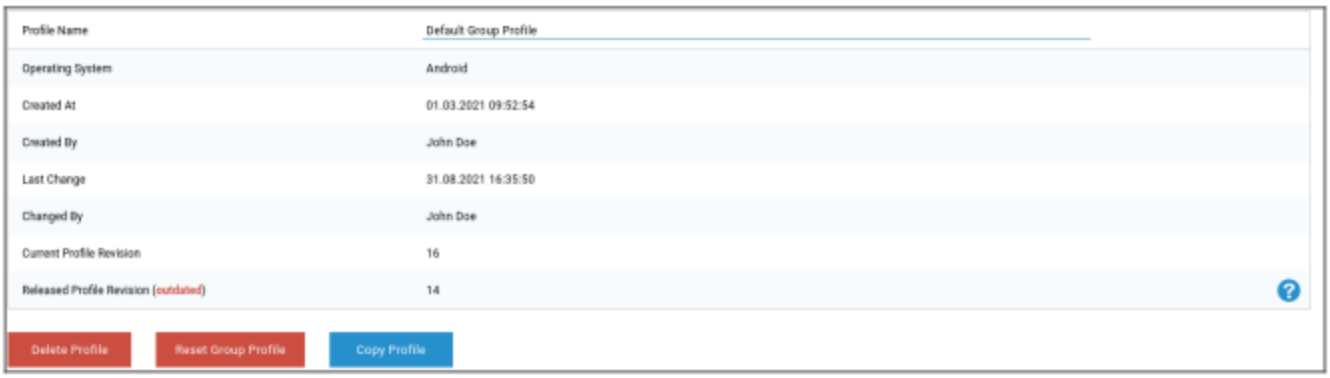
	• Працюючий універсальний шлюз AppTec ("Загальні налаштування" → "Універсальний шлюз") • Робоча конфігурація VPN із зазначеним DNS-сервером ("Загальні налаштування" → "Універсальний шлюз" → "Налаштування VPN") • Налаштування чорного списку ("Загальні налаштування" → "Універсальний шлюз" → "Чорний список доменів") • Дійсне VPN-з'єднання в профілі ("Управління з'єднаннями" → "VPN")

Конфігурація Android

Генерал

Огляд профілю групи (тільки на рівні групи)

Відкривши профіль групи, ви отримаєте короткий огляд профілю.



Ім'я профілю Ім'я профілю	Назва профілю (можна змінити тут)
Операційна система	Операційна система, для якої призначений профіль
Створено в	Час створення
Створено	Творець профілю
Остання зміна	Час останньої зміни профілю
Змінено	Обліковий запис, який вніс останні зміни
Поточна редакція профілю	Перегляд стану збереженого профілю
Випущено ревізію профілю	Призначена версія профілю ("Призначити зараз"). Якщо за текстом мітки вказано "(застаріла)", це означає, що ви зберегли профіль, але ще не призначили його, тому пристрої все одно отримають стару версію.

Огляд пристрою (тільки на рівні пристрою)

Якщо ви перебуваєте на пристрої, ви отримаєте оглядову інформацію про вибраний пристрій, яка міститься тут:

Назва пристрою	Назва пристрою
Останнє відоме місцезнаходження	Останні відомі GPS-координати
Номер телефону	Номер телефону
Призначені обов'язкові програми	Кількість призначених обов'язкових додатків
Версія ОС	Версія операційної системи пристрою
Операційна система	Операційна система (Android / iOS / Windows Phone)
Серійний номер	Серійний номер пристрою
Право власності на пристрій	Корпоративний або приватний пристрій
Тип пристрою	Телефон або планшет
Укорінений	Статус, що вказує на те, чи був пристрій вкорінений
Дотримується	Відповідає настановам
IP-адреса	IP-адреса
Востаннє бачили	Момент часу, коли пристрій востаннє підключався до AppTec
Останній поштовх	Момент часу, коли сервер відправив пуш на пристрій
Призначення користувача	Випадаючий список для призначення пристрою іншому користувачеві

Ревізія конфігурації (лише на рівні пристрою)

Тут ви отримаєте огляд того, який профіль групи призначено пристрою.

Якщо ви натиснете на профіль групи, ви отримаєте доступ безпосередньо до профілю і зможете виконати налаштування.

За допомогою цього символу ви можете повернути призначені програми до налаштувань профілю групи.

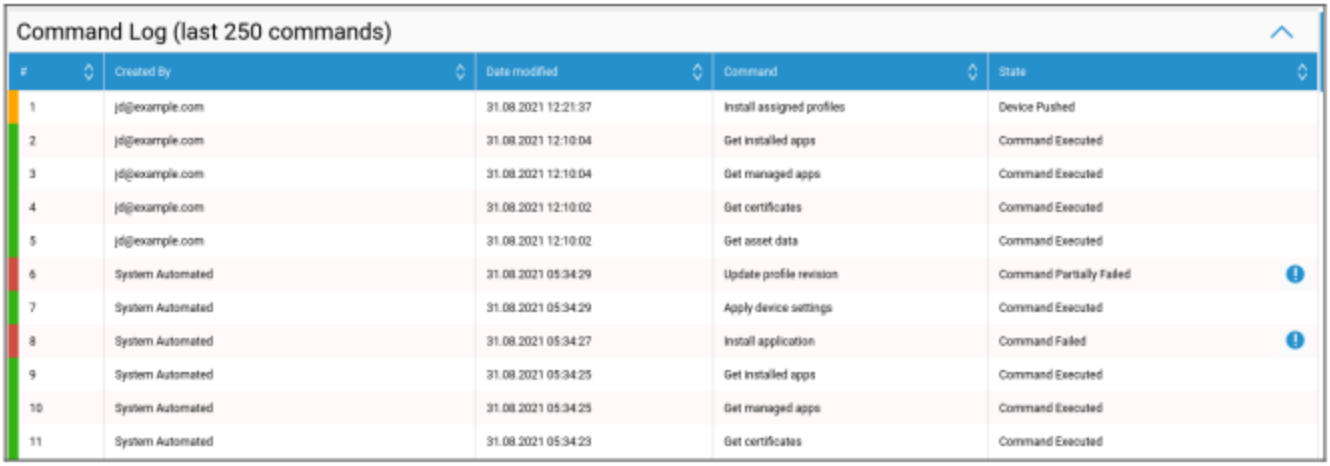
За допомогою цього символу ви можете скинути профіль пристрою, щоб він не мав жодних налаштувань.

"Доступна новіша версія" вказує на те, що профіль групи було змінено та збережено, але не призначено. Щоб застосувати зміни до пристроїв, профіль групи потрібно призначити за допомогою "Призначити зараз" на рівні групи.

Журнал пристрою (тільки на рівні пристрою)

Командний журнал

Тут ви можете побачити, які команди були видані для пристрою і який їхній статус.



Команди, створені за допомогою "Автоматизації системи", автоматично створюються системою.

Можливі стани команди

Пристрій натиснуто	До служби push (наприклад, APNS) було надіслано push-запит, щоб повідомити пристрій про необхідність з'єднатися з сервером EMM.
Команду створено	Команда була створена в системі.
Команду відправлено.	Команда була надіслана на пристрій після того, як він підключився до сервера.
Команду виконано	Команда була успішно виконана.
Команда не спрацювала	Команда не спрацювала. *
Команда частково не виконана	Залежно від операційної системи пристрою деякі команди можуть бути згруповані разом. У цьому деякі частини цієї командної групи зазнали невдачі. *
Команда виконана, але зрештою не спрацювала	Команда була виконана, але, можливо, не була.
Команда "Відсіч	Команду було перевиконано користувачем.
Викинуто	Команду було відкинуто. Наприклад, її було замінено іншою командою або пристрій було перереєстровано, а старі команди видалено

*Якщо за повідомленням стоїть знак оклику, ви можете отримати додаткову інформацію, навівши курсор на іконку.

Налаштування пристрою

Конфігурація клієнта

Тут ви можете виконати наступні конфігурації на вашому пристрої Android:

Попередження після вимкнення Керування пристроями	Установлене попереджувальне повідомлення після вимкнення Керування пристроями
Порушення термінів дотримання вимог	Обмеження часу, після якого буде виконано "Дію примусового виконання після відповідності", якщо пристрій не відповідає вимогам. Хвилина. 1 хвилина Максимум. 24 години
Примусові заходи після закінчення терміну виконання	Дії, які необхідно вжити, як тільки пристрій стає невідповідним. • нічого не робити = ніяких дій • Lock Device = пристрій блокування • Очистити пристрій = пристрій буде відновлено до заводських налаштувань
Частота збору даних	Частота, з якою пристрій / GPS-інформація повинна збиратися
Частота серцебиття пристрою	Інтервал, через який пристрій повинен зв'язуватися з сервером AppTec360 Хвилина. 1 хвилина Максимум. 24 години
Увімкнути оновлення місцезнаходження	Якщо увімкнено, пристрій надсилає оновлення місцезнаходження на сервер AppTec360
Час оновлення місцезнаходження	Визначає, через які проміжки часу пристрій надсилає оновлення місцезнаходження до AppTec
Використовуйте Google Location Accuracy для оновлення місцезнаходження	Якщо увімкнено, для оновлення місцезнаходження буде використовуватися точність визначення місцезнаходження Google (раніше відома як мережеве місцезнаходження) (якщо це було деактивовано в розділі "Обмеження", то це налаштування ні на що не вплине).
Використовуйте GPS-локацію для оновлення	Якщо увімкнено, GPS буде використовуватися для оновлення місцезнаходження

місцезнаходження	
Дозволити імітацію (фейкові) локації	Дозволяє підробляти інформацію про місцезнаходження за допомогою сторонніх додатків
Дія "Втрата зв'язку	Дозволяє встановити певну дію, яка буде виконана після певної кількості невдалих серцевих скорочень
Режим застосування політики	Визначає, наскільки агресивно клієнт AppTec360 просить користувача виконати певні дії, які вимагають введення даних. Інтервал (за замовчуванням) = запитувати через певні проміжки часу, щоб користувач міг відкласти це на деякий час у фоновому режимі. Без сповіщення = немає спливаючого вікна для будь-якої необхідної взаємодії. Вам доведеться відкрити клієнт AppTec360 вручну, щоб перевірити, чи є необхідна дія Постійне попередження = Користувач може виконати лише необхідну дію. Клієнт AppTec360 витіснить себе на передній план, якщо користувач спробує його уникнути
AppTec360 Блокування версії	Дозволяє визначити версію клієнта AppTec360, яка є максимальною версією, до якої оновлюється клієнт.

Шпалери

Тут ви можете визначити власні шпалери.

"Вказати колір" дозволяє задати колір у шістнадцятковому форматі (наприклад, #000000). Допускаються лише шістнадцяткові значення.

"Встановити зображення як шпалери" дозволяє завантажити зображення. Зверніть увагу, що на різних пристроях з різними лаунчерами та версіями ОС це працює по-різному. Не існує загальних рекомендацій щодо розміру та співвідношення, оскільки це залежить від пристрою.

Використовуйте JPG (або JPEG) або PNG як формат файлу.

Управління активами (тільки на рівні пристрою)

Управління активами

Інформація про пристрій

Модель	**Позначення моделі пристрою**
Операційна система	ОС
Версія ОС	Версія операційної системи
Підтримка AE	Підтримка Android Enterprise (контейнерна та повністю керована)
Серійний номер	Серійний номер
Назва пристрою	Назва пристрою
Стан акумулятора	Стан акумулятора
Вільна / загальна пам'ять	Вільна / Загальна пам'ять
Samsung KNOX	Рівень API Samsung KNOX
Доступна SD-карта	Доступна SD-карта
Емуляція SD-карти	Емуляція SD-карти
Знімна SD-карта	Знімна SD-карта
Вільна пам'ять SD / загальна пам'ять	Вільна пам'ять на SD / Загальна пам'ять на SD-карті

Wi-Fi

IP-адреса	IP-адреса пристрою
MAC-адреса WiFi	MAC-адреса WiFi

Стільниковий зв’язок

Статус	Статус (встановлена SIM-карта)
Номер телефону	Номер телефону
Роумінг (голосовий зв'язок / передача даних)	Роумінг для передачі голосу/даних
Статус роумінгу	Поточний статус у роумінгу
IP-адреса	IP-адреса
Оператор/перевізник	Оператор/перевізник
Стільникові технології	Стільникові технології
IMEI	Номер IMEI
ICCID	Це ідентифікатор SIM-картки, часто також смарт-картки або картки з інтегральною схемою (ICC)
IMSI	Міжнародна мобільна ідентифікація абонента (IMSI) забезпечує в GSM- і UMTS-мережах однозначну ідентифікацію користувачів мережі IMSI складається максимум з 15 цифр і налаштовується наступним чином: • Мобільний код країни (MCC), 3 цифри • Код мобільної мережі (MNC), 2 або 3 цифри • Ідентифікаційний номер абонента мобільного зв'язку (MSIN), 1-10 цифр
Поточний ГХК/МНК	Див. розділ "SIM MCC/MNC"
SIM MCC/MNC	Мобільний код країни - це визнаний ідентифікатор країни, встановлений МСЕ відповідно до стандарту E.212. Він працює разом з кодом мобільної мережі (MNC) для ідентифікації мобільної мережі. Означає код країни/мобільної мережі SIM-карти. Якщо ви перебуваєте в роумінгу в іншій мобільній мережі, то логічно, що "Поточний MCC/MNC" і "MCC/MNC SIM" будуть відрізнятися.

Bluetooth

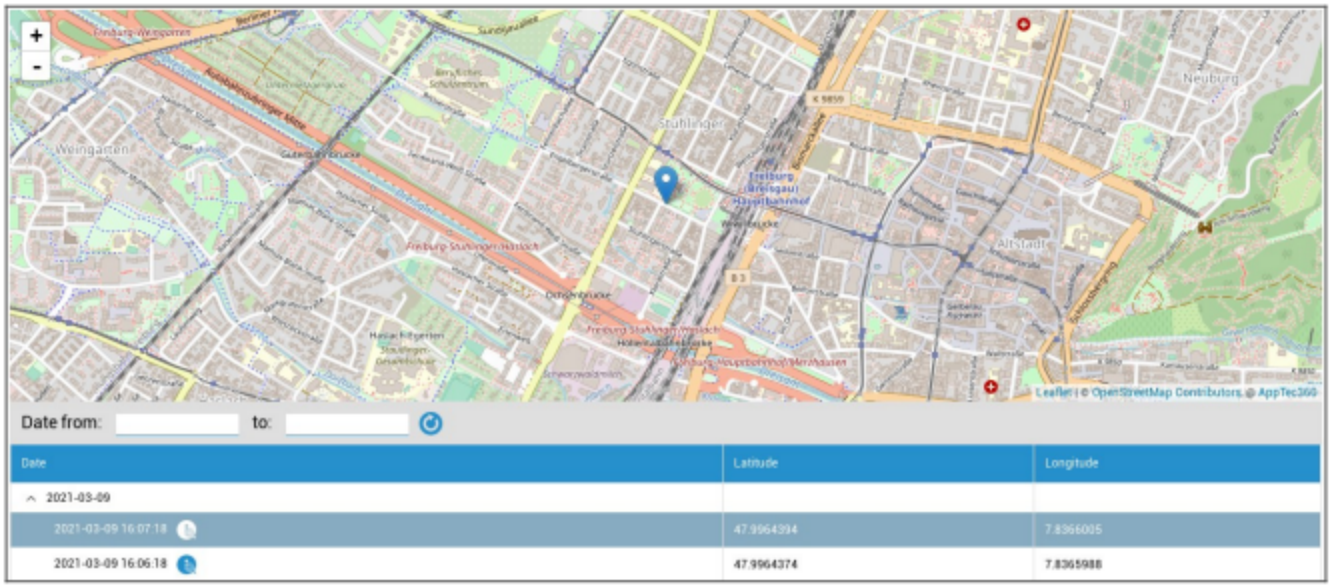
MAC-адреса Bluetooth	MAC-адреса Bluetooth

Управління безпекою

Захист від крадіжок (лише на рівні пристрою)

Інформація про GPS (лише на рівні пристрою)

Тут ви можете встановити поточне/останнє місцезнаходження пристрою. Локалізацію можна захистити одним або навіть двома паролями - Див: Загальні налаштування - Конфіденційність - Доступ до GPS



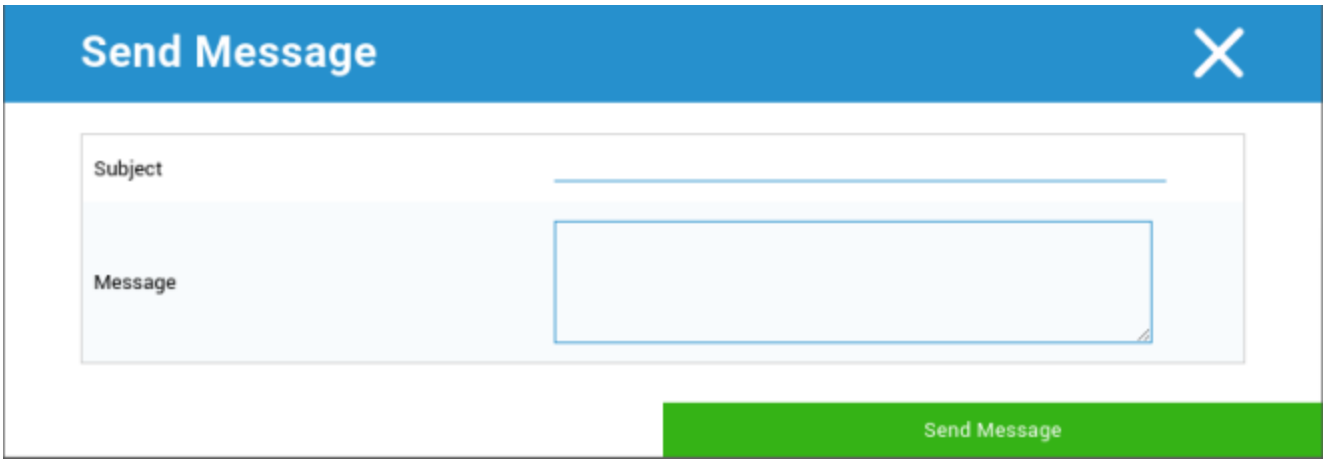
Wipe & Lock (тільки на рівні пристрою)

У розділі "Витирання та блокування" ви можете виконати наступні три дії:

Повне витирання	Пристрій відновлюється до заводських налаштувань (видаляються корпоративні, а також особисті дані)
Enterprise Wipe	З пристрою кінцевого користувача видаляються лише корпоративні дані (всі додатки, дані тощо, які були надані AppTec360).
Екран блокування	Блокування екрану активоване, достатньо розблокувати пристрій за допомогою пароля/коду пристрою

Повідомлення (тільки на рівні пристрою)

Ви можете заповнити тему і текст повідомлення та надіслати його на пристрій кінцевого користувача. Це повідомлення буде відображено в клієнті AppTec360.



Конфігурація безпеки

Пароль

У розділі "Пароль" ви можете встановити пароль пристрою, вам доступні наступні варіанти налаштувань

Мінімальна довжина пароля	Визначає мінімальну кількість символів, які повинен містити пароль
Якість пароля	Надійність пароля Unspecified = не вказано Every password is ok = кожен пароль прийнятний принаймні числові символи = має містити принаймні числові символи принаймні складні символи = має містити принаймні спеціальні символи принаймні алфавітно-цифрові символи = має містити принаймні алфавітно-цифрові символи принаймні літерні символи = має містити принаймні літерні символи
Блокування максимального часу бездіяльності	Максимальний таймаут екрану. Тут налаштовується лише максимальне значення, яке може вибрати користувач
Мінімум малих літер у паролі	Мінімум малих літер у паролі
Мінімальна кількість великих літер у паролі	Мінімальна кількість великих літер у паролі
Мінімальна кількість нелітерних символів у паролі	Мінімальна кількість нелітерних символів у паролі
Мінімальна кількість цифр у паролі	Мінімальна кількість цифр у паролі
Мінімальна кількість символів у паролі	Мінімальна кількість символів у паролі
Таймаут терміну дії пароля	Встановлює, через який проміжок часу закінчується термін дії пароля і потрібно видати новий пароль
Обмеження історії паролів	Кількість раніше використаних паролів, які не допускаються
Максимальна кількість невдалих спроб введення пароля	Визначає, як часто можна вводити пароль неправильно, перш ніж буде виконано повне очищення пристрою

Шифрування

У цьому пункті ви можете зашифрувати внутрішню пам'ять пристрою, а також пам'ять SD-карти.

Вимагати шифрування сховища	Якщо цей параметр увімкнено, пам'ять пристрою буде зашифровано, якщо пристрій підтримує цю функцію. Після того, як пам'ять пристрою буде зашифровано вперше, її вже неможливо буде розшифрувати. Аналогічно, політику паролів буде автоматично переключено на 6 алфавітно-цифрових символів
Вимагати шифрування SD-карти	Цей параметр застосовується лише до пристроїв Samsung! Якщо цей параметр активовано, зовнішню SD-карту буде зашифровано, і її можна буде розшифрувати лише вручну на кінцевому пристрої користувача. Аналогічно, політику паролів буде автоматично переключено на 6 алфавітно-цифрових символів

Антивірус

Увімкнувши Антивірус, ви встановите Ikarus на пристрої. Зверніть увагу, що для цього потрібна окрема ліцензія, яку можна ввести в Загальних налаштуваннях → Керування програмами → Сторонні програми.

Автоматичне сканування	Визначає, чи виконує Ikarus автоматичне сканування і як часто він виконує це сканування Якщо увімкнути "Повне автоматичне сканування", буде виконано повне сканування. В іншому випадку буде виконано швидке сканування
Автоматичні оновлення	Увімкнення автоматичного оновлення вірусної бази та налаштування частоти оновлення
Захист додатків	Увімкнення сканування програм на додаток до звичайного сканування, яке сканує лише файли
Захист SD-карти	Увімкнення захисту SD-карти. Без цього параметра сканування обмежується локальним сховищем
Оновлення тільки для Wi-Fi	Обмеження оновлення до Wi-Fi

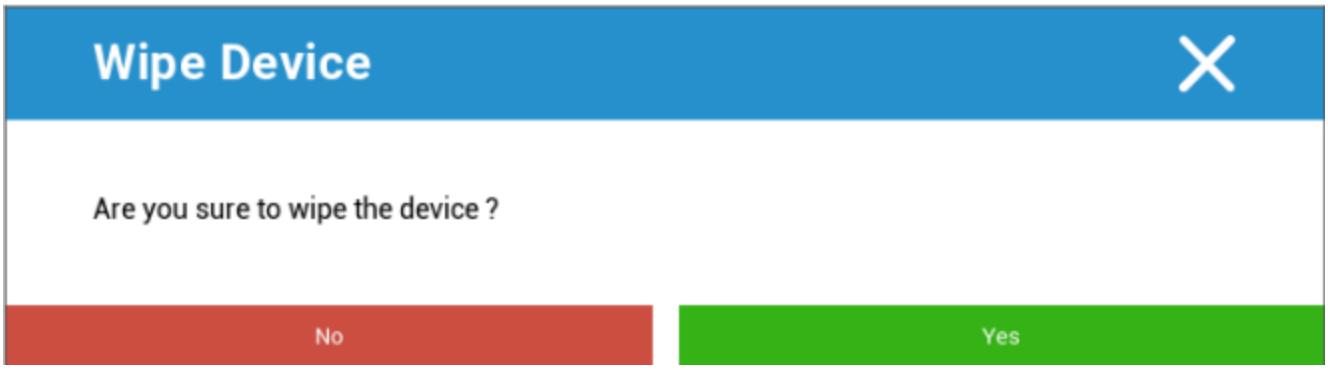
Кінець життя (тільки на рівні пристрою)

Витирання (тільки на рівні пристрою)

У розділі "Видалити" ви можете відновити заводські налаштування пристрою. При цьому на пристрої кінцевого користувача будуть видалені як корпоративні, так і приватні дані.

При натисканні на "Символ мінус" ви повинні отримати наступне повідомлення

Витирати SD-карту теж?	Пам'ять SD-карти також буде стерто



За допомогою "Так" ви можете виконати стирання.

У розділі "Звіт про витирання" можуть відображатися такі елементи

Витерто	Історія про те, хто виконував стирання
Дата	Дата
Статус	Статус (наприклад, якщо очищення було виконано успішно)

Налаштування обмежень

Обмеження

Тут можна обмежити та заблокувати безліч речей.

Увімкнути камеру	Дозволити використовувати камеру
Ввімкнути автосинхронізацію	Стосується інтерфейсу "Синхронізація" Увімкнено = синхронізація постійно активована Вимкнено = синхронізація вимкнена назавжди Вибір користувача = вибрано користувачем
Ввімкнути Bluetooth	Увімкнено = Bluetooth постійно активовано Вимкнено = Bluetooth назавжди вимкнено Вибір користувача = вибрано користувачем
Примусьте GPS	Увімкнено = GPS постійно активовано Вимкнено = GPS назавжди вимкнено Вибір користувача = вибрано користувачем
Примусити Google визначати місцезнаходження	Увімкнено = Постійна інтернет-локалізація Вимкнено = постійне вимкнення інтернет-локалізації Вибір користувача = вибрано користувачем

Для пристроїв Samsung з інтерфейсом KNOX 1.0 або вище доступні наступні варіанти налаштувань.

Дозволити SD-карту	Дозволити SD-карту
Дозволити запис на SD-карту	Дозволити "запис" на SD-карту
Дозволити захоплення екрана	Дозволити знімок екрана
Дозволити буфер обміну	Дозволити буфер обміну
Резервне копіювання налаштувань і даних програм у Google Cloud	Вимкнено = вимкнути резервне копіювання Google Увімкнено = активувати Google Резервне копіювання Вибір користувача = вибрано користувачем
Дозволити налагодження USB	Дозволити налагодження USB (використовується, наприклад, для створення журналів пристроїв (ADB))
Дозволити Google Crash Report	Дозволити надсилання звіту Google Crash Report з додатків
Дозволити скидання до заводських налаштувань	Дозволяє користувачеві відновити заводські налаштування пристрою
Дозволити оновлення OTA	Дозволити оновлення "по повітрю"
Дозволити хост-накопичувач USB	Якщо активовано, можна підключити USB-накопичувач у вигляді зчитувача HD або SD-карт
Дозволити USB медіаплеєр (MTP, PTP)	Дозволити USB медіаплеєр (MTP, PTP)
Увімкнути мікрофон	Увімкнено = дозволити мікрофон для сторонніх додатків Вимкнено = заблокувати мікрофон для сторонніх програм Вибір користувача = користувачі можуть вибрати, чи має сторонній додаток доступ до мікрофона
Дозволити NFC (ближній радіозв'язок)	Увімкнути NFC
Дозволити невідомі джерела (APK Sideloading)	Якщо увімкнено, дозволено бічне завантаження додатків (APK-файлів). Якщо цей параметр вимкнено, користувачеві доведеться увімкнути його вручну, коли ви дозволите встановлення APK з невідомих джерел.
Дозволити створення користувачів	Дозволяє створювати кілька користувачів

Власник пристрою AE

(Пристрій має бути в режимі власника пристрою Android Enterprise) Рекомендується створювати пристрої як пристрої "Android Enterprise", а не як пристрої "Android".

Безпека	
Заборонити розташування спільного доступу	Вказує, чи користувачеві заборонено вмикати спільний доступ до місцезнаходження.
Заборонити безпечне завантаження	Вказує, чи користувачеві заборонено перезавантажувати пристрій у безпечний режим завантаження.
Заборонити скидання мережі	Вказує, чи користувачеві заборонено скидати налаштування мережі з Налаштувань.
Заборонити скидання до заводських налаштувань	Вказує, чи користувачеві заборонено скидати пристрій.
Увімкнути АБР	Дозволяє підключатись до ПК через ADB
Вимкнути Keyguard	Вимкнення Keyguard
Інформація про власника пристрою на екрані блокування	Дозволяє встановити інформацію про власника пристрою для відображення на екрані блокування.
Забезпечення комплаєнсу	Режим Підказка користувачеві - Користувачеві буде запропоновано виконати необхідні дії. Режим Lock-Down Container - приховати всі програми, поки не будуть виконані всі вимоги

Керування додатками	
Дозволити зв'язування міжпрофільних додатків	Дозволяє програмам у батьківському профілі обробляти веб-посилання з керованого профілю.
Заборонити керування програмами	Вказує, чи користувачеві заборонено змінювати програми у Налаштуваннях або лаунчерах.
Заборонити встановлення програми	Вказує, чи заборонено користувачеві встановлювати програми.
Заборонити видалення програм	Вказує, чи користувачеві заборонено видаляти програми.
Політика дозволів на виконання	Вказує, як будуть оброблятися нові запити на дозволи від програм.
Дозволити невідомі джерела	Якщо увімкнено, користувачі можуть завантажувати програми, встановивши файл .apk.

Зв'язок	
Заборонити конфігурацію мобільної мережі	Вказує, чи користувачеві заборонено налаштовувати мобільні мережі.
Заборонити прив'язку Конфігурація	Вказує, чи користувачеві заборонено налаштовувати Tethering та портативні хот-споти.
Заборонити конфігурацію VPN	Вказує, чи користувачеві заборонено налаштовувати VPN.
Заборонити конфігурацію Wifi	Вказує, чи користувачеві заборонено змінювати точки доступу WiFi.
Заборонити вихідний промінь NFC	Вказує, чи дозволено користувачеві використовувати NFC для передачі даних з програм.
Блокування конфігурації WiFi	Цей параметр визначає, чи слід блокувати конфігурації WiFi, створені у програмі Власника пристрою (тобто, чи можна їх редагувати або видаляти лише у програмі Власника пристрою, а не у програмі Налаштування).
Увімкнути роумінг даних	Активує роумінг даних

Bluetooth	
Заборонити Bluetooth	Вказує, чи заборонено Bluetooth на пристрої. Потрібна версія Android 8.0
Заборонити спільний доступ через Bluetooth	Вказує, чи заборонено на пристрої вихідний обмін даними через Bluetooth. Потрібна Android 8.0
Заборонити конфігурацію Bluetooth	Вказує, чи користувачеві заборонено налаштовувати bluetooth.

Управління рахунками	
Заборонити додавання керованого профілю	Вказує, чи користувачеві заборонено додавати керовані профілі. Потрібна версія Android 8.0
Заборонити додавання користувачів	Вказує, чи користувачеві заборонено додавати нових користувачів.
Заборонити видалення керованого профілю	Вказує, чи можна видаляти керовані профілі цього користувача, окрім власника профілю. Потрібна Android 8.0
Заборонити зміну облікового запису	Вказує, чи користувачеві заборонено додавати та видаляти облікові записи, якщо вони не додані програмно за допомогою автентифікатора.

Телефонія	
Заборонити вихідні дзвінки	Вказує, що користувачеві заборонено здійснювати вихідні телефонні дзвінки.
Заборонити SMS	Вказує, що користувачеві заборонено надсилати або отримувати SMS-повідомлення.

Система	
Заборонити створення вікон	Вказує, що не слід створювати вікна, окрім вікон програми.
Заборонити встановлену піктограму користувача	Вказує, чи дозволено користувачеві змінювати свою іконку.
Заборонити встановлення шпалер	Обмеження користувача для заборони встановлення шпалер.
Вимкнути рядок стану	Вимкнення рядка стану блокує сповіщення, швидкі налаштування та інші екранні накладки, які дозволяють втекти з одноразового пристрою.
Увімкнути автоматичний час	Встановлює час автоматично.
Увімкнути автоматичний часовий пояс	Автоматично встановлює часовий пояс.
Залишайтеся увімкненими, коли ви підключені до мережі	Пристрій залишатиметься активним, поки підключений до джерела живлення.

Зберігання

Заборонити вимкнути перевірку додатків	Вказує, чи користувачеві заборонено вимикати перевірку додатків.
Заборонити монтування фізичних носіїв	Вказує, чи користувачеві заборонено монтувати фізичні зовнішні носії.
Увімкнути службу резервного копіювання	Служба резервного копіювання керує всіма механізмами резервного копіювання та відновлення на пристрої. Якщо встановити значення false, резервне копіювання або відновлення даних буде неможливим. За замовчуванням службу резервного копіювання вимкнено. Потрібна Android 8.0
Увімкнути USB-накопичувач	Дозволяє використовувати USB-накопичувач.

Клавіатура	
Заборонити автозаповнення	Вказує, чи користувачеві заборонено використовувати служби автозаповнення. Потрібна версія Android 8.0
Заборонити копіювання та вставку між профілями	Вказує, чи можна вставляти скопійоване у буфер обміну цього профілю у пов'язані профілі.

Звук	
Заборонити регулювання гучності	Дозволяє вказати, чи користувачеві заборонено регулювати загальний рівень гучності.
Заборонити вимкнення мікрофона	Вказує, чи користувачеві заборонено регулювати гучність мікрофона.
Вимкнення звуку пристрою	Вимкнути звук.

Політика оновлення системи	
Керування оновленнями ОС	Увімкніть цей параметр, щоб встановити поведінку оновлення: автоматичне, у вікні або відкладене.

Контейнер BYOD

Android Enterprise

Android Enterprise

Увімкнути Android Enterprise	Увімкніть Android Enterprise (AE). AE підтримується починаючи з Android 5.1 і вище.
Забезпечення комплаєнсу	Режим Підказка користувачеві - Користувачеві буде запропоновано виконати необхідні дії. Режим Lock-Down Container - приховати всі програми, поки не будуть виконані всі вимоги
Політика дозволів на виконання	Підказка користувачеві про нові запити на дозволи Завжди надавайте нові запити на отримання дозволів Завжди відхиляйте нові запити на отримання дозволів Попередження: Деякі програми мають проблеми з розпізнаванням дозволів, якщо вони встановлені автоматично. Якщо ви завжди надаєте дозволи і стикаєтеся з проблемами, коли програми повідомляють, що дозволів не вистачає, встановіть для цього параметра значення "запитувати користувача" і переінсталюйте програму
Дозволити вихідний буфер обміну	Дозволяє копіювати та вставляти зсередини контейнера назовні
Дозволити дозвіл ідентифікатора абонента	Показує ім'я для вхідного дзвінка на основі контактів у контейнері
Дозволити роздільну здатність пошуку контактів	Дозволяє шукати імена в контактах контейнера при здійсненні дзвінків
Дозволити обмін контактами через Bluetooth	Дозволяє отримати доступ до контакту контейнера в автомобілі
Заборонити вихідний промінь NFC	Вимкнення NFC для контейнера
Дозволити невідомі джерела	Якщо увімкнено, користувачі можуть завантажувати програми, встановивши файл .apk.

Дозволити налагодження USB	Якщо увімкнено, користувачі можуть увімкнути налагодження USB.
Заборонити зміну облікового запису	Забороняє створення, видалення та модифікацію облікових записів у контейнері Майте на увазі, що деякі програми потребують створення або зміни облікових записів, щоб працювати належним чином

Обмін Gmail

Дозволяє налаштувати Gmail у Контейнері. Зауважте, що ввімкнення цього параметра не означає автоматичного встановлення програми. Вам все одно доведеться додати цю програму як обов'язкову.

Адреса електронної пошти	Адреса електронної пошти
Ім'я хосту сервера	Ім'я хосту сервера
Ім'я користувача Ім'я користувача	Ім'я користувача Ім'я користувача
Підпис	Підпис
Кількість попередніх днів для синхронізації	Кількість попередніх днів для синхронізації.
Ідентифікатор пристрою	Ідентифікатор EAS. Залиште це поле порожнім, якщо ваше середовище не вимагає цього
Використовуйте протокол захищених сокетів (SSL)	Дозволяє використання SSL. Вимкнення може знизити рівень безпеки
Приймаємо всі сертифікати	Приймає всі сертифікати. Увімкнення цієї опції може знизити рівень безпеки
Дозволити некеровані акаунти	Дозволяє користувачеві додавати додаткові облікові записи
Сертифікат клієнта	Завантажте клієнтський сертифікат, якщо цього вимагає ваш Exchange-сервер

Додатки для системи AE

Тут ви можете увімкнути системні програми для Android Enterprise Container. Будь ласка, майте на увазі, що вказаний додаток має бути у сховищі системи, інакше нічого не відбудеться.

Код доступу до контейнера

Тільки для Android 7.0 або новішої версії

Дозволяє встановити певну вимогу до пароля для контейнера.

Мінімальна довжина пароля	Визначає мінімальну кількість символів, які повинен містити пароль
Якість пароля	Надійність пароля Unspecified = не вказано Every password is ok = кожен пароль прийнятний принаймні числові символи = має містити принаймні числові символи принаймні складні символи = має містити принаймні спеціальні символи принаймні алфавітно-цифрові символи = має містити принаймні алфавітно-цифрові символи принаймні літерні символи = має містити принаймні літерні символи
Блокування максимального часу бездіяльності	Максимальний час до блокування контейнера. Тут налаштовується лише максимальне значення, яке може вибрати користувач
Мінімум малих літер у паролі	Мінімум малих літер у паролі
Мінімальна кількість великих літер у паролі	Мінімальна кількість великих літер у паролі
Мінімальна кількість нелітерних символів у паролі	Мінімальна кількість нелітерних символів у паролі
Мінімальна кількість цифр у паролі	Мінімальна кількість цифр у паролі
Мінімальна кількість символів у паролі	Мінімальна кількість символів у паролі
Таймаут терміну дії пароля	Встановлює, через який проміжок часу закінчується термін дії пароля і потрібно видати новий пароль
Обмеження історії паролів	Кількість раніше використаних паролів, які не допускаються
Максимальна кількість невдалих спроб введення пароля	Визначає, як часто можна вводити пароль неправильно, перш ніж контейнер буде видалено

Samsung KNOX

Активація

Тут ви можете увімкнути контейнер Samsung KNOX. Зверніть увагу, що ця функція більше не підтримується компанією Samsung на Android 10 або новіших версіях. Використання Android Enterprise Container на Android 10 або новішої версії

Пароль Нокса

Встановіть правила, які стосуються налаштувань пароля пристрою

Мінімальна довжина пароля	Визначає, скільки символів повинен містити пароль
Якість пароля	Надійність пароля Кожен пароль підходить = Кожен пароль підходить Щонайменше цифрові символи = Мінімум цифрових символів має бути присутнім Щонайменше складні символи = Повинні бути присутніми мінімум спеціальних символів Принаймні алфавітно-цифрові символи = Мінімум алфавітно-цифрових символів має бути присутнім Принаймні алфавітні символи = Мінімум алфавітних символів має бути присутнім
Потрібно мінімум складних символів	Мінімум складних символів має бути присутнім
Максимальний тайм-аут бездіяльності	Максимальний таймаут бездіяльності користувача перед блокуванням клавіатури
Дозволити автентифікацію за відбитками пальців	Дозволити автентифікацію за відбитками пальців
Дозволити автентифікацію діафрагми	Дозволити автентифікацію за райдужною оболонкою ока
Максимальний вік пароля	Визначає, через який час закінчується термін дії пароля і потрібно видати новий пароль
Історія збережених паролів	Кількість колишніх паролів, які не дозволені
Максимальна кількість невдалих спроб введення пароля	Визначає, як часто можна вводити неправильний пароль, перш ніж відбудеться повне очищення пристрою

Нокс Секьюріті

Обмеження певних функцій пристрою

Увімкнути камеру	Дозвольте використовувати камеру

Дозволити Samsung KNOX App Store	Дозволити використання Samsung KNOX App Store
Увімкнути служби Google Play	Увімкнути служби Google Play
Дозволити браузер	Дозволити використання рідного браузера
Дозволити скріншоти	Дозволити створення скріншотів
Дозволити імпорт контактів	Якщо активовано, доступ до контактів пристрою з KNOX Container дозволено
Дозволити експорт контактів	Якщо увімкнено, доступ до контактів KNOX з пристрою дозволено
Дозволити імпорт календаря	Якщо увімкнено, доступ до календаря пристроїв з Контейнера KNOX дозволено
Дозволити експорт календаря	Якщо увімкнено, доступ до календаря KNOX з пристрою дозволено
Дозволити незахищену клавіатуру	Дозволити використання незахищеної клавіатури
Увімкнути імпорт файлів	Увімкнути імпорт файлів до контейнера KNOX
Увімкнути експорт файлів	Увімкнути експорт файлів з контейнера KNOX

Knox Exchange

Тут ви можете налаштувати Exchange-профіль для KNOX-контейнера

Адреса електронної пошти	Надана адреса електронної пошти користувача Зверніть увагу на "Заповнювачі", які можна використовувати для роботи з обліковими даними і не виконувати зміни вручну на кожному пристрої Натиснувши на кнопку **Показати заповнювачі**, ви можете відобразити їх для себе
Ім'я хосту сервера	Адреса сервера ваших Exchange-серверів
Ім'я користувача	Ім'я для входу для відповідного пристрою кінцевого користувача, також зверніть увагу на "Заповнювачі" тут
Домен	Адреса домену
Пароль (тільки на рівні пристрою)	За бажанням окремому пристрою може бути надано пароль, якщо він залишиться порожнім, користувачеві буде запропоновано ввести свій Exchange Password
Кількість попередніх днів для синхронізації	Кількість днів, які визначають, коли імейли будуть синхронізовані знову
Підпис	Можна додати підпис
Обліковий запис за замовчуванням	Встановлює, що цей акаунт електронної пошти є стандартним акаунтом
Використовуйте протокол захищених сокетів (SSL)	Використовуйте SSL-з'єднання
Використовуйте захист на транспортному рівні (TLS)	Використовуйте з'єднання TLS
Приймаємо всі сертифікати	Приймаються всі сертифікати. Виберіть цю опцію, якщо ваш Exchange-сервер використовує самопідписаний сертифікат

Knox eMail

Адреса електронної пошти	Надана адреса електронної пошти користувача Зверніть увагу на "Заповнювачі", які можна використовувати для роботи з обліковими даними і не виконувати зміни вручну на кожному пристрої Натиснувши на кнопку **Показати заповнювачі**, ви можете відобразити їх для себе
Вхідний протокол сервера	Вхідний протокол сервера IMAP або POP
Вхідна адреса сервера	Вхідна адреса сервера
Вхідний порт сервера	Вхідний порт сервера
Вхідний логін/ім'я користувача на сервері	Вхідний логін/ім'я користувача на сервері
Вхідний пароль сервера	Вхідний пароль сервера
Вхідний сервер використовує SSL	Вхідний сервер використовує SSL
Вхідний сервер використовує TLS	Вхідний сервер використовує TLS
Вхідний сервер приймає всі сертифікати	Вхідні сервери приймають всі типи сертифікатів
Протокол вихідного сервера	Протокол вихідного сервера SMTP
Вихідний порт сервера	Вихідний порт сервера
Вихідний сервер використовує додаткові облікові дані	Додаткові облікові дані для вихідного сервера. Якщо цей параметр вимкнено, то будуть використовуватися налаштування вхідного сервера
Логін/ім'я користувача вихідного сервера	Логін/ім'я користувача вихідного сервера
Пароль вихідного сервера	Пароль вихідного сервера
Вихідний сервер використовує SSL	Вихідний сервер використовує SSL
Вихідний сервер використовує TLS	Вихідний сервер використовує TLS
Вихідний сервер приймає всі сертифікати	Вихідний сервер приймає всі типи сертифікатів

Підпис	Тут можна додати підпис
Сповіщати користувача про отримання нової електронної пошти	Сповіщати користувача про отримання нової електронної пошти

Knox Apps

Створіть тут програми, які ви хочете розповсюдити на пристрої кінцевих користувачів. Після цього вони будуть доступні в KNOX-Container. Для того, щоб додати додаток, будь ласка, дійте так само, як у меню Обов'язкові додатки

Назва заявки	Назва заявки
Обов'язково, оскільки	Момент часу, коли додаток було додано
Джерело	Джерело додатку (Play Store | In-house)

Натиснувши на символ, відповідну програму можна знову видалити

Керування з’єднаннями

Wi-Fi

Для цього налаштування виконайте попереднє налаштування пристроїв кінцевих користувачів для доступу до внутрішніх точок доступу

Ідентифікатор набору послуг (SSID)	SSID мережі, до якої потрібно підключитися
Прихована мережа	Активувати, якщо точка доступу не передає SSID
Тип безпеки	Встановіть тип захисту точки доступу

Тип безпеки

WEP

Пароль	Пароль для точки доступу

WPA/WPA2

Пароль	Пароль для точки доступу

802.1x EAP

EAP-метод	

PWD	Ідентичність	Ідентичність
	Пароль	Пароль

PEAP	Етап 2 Протокол автентифікації	ні	Без додаткового протоколу
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертифікат центру сертифікації	Сертифікат центру сертифікації	
	Ідентичність	Ідентичність	
	Анонімна ідентичність	Анонімна особистість	
	Пароль	Пароль	

EAP-метод	

TTLS	Етап 2 Протокол автентифікації	ні	Без додаткового протоколу
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертифікат центру сертифікації	Сертифікат центру сертифікації	
	Ідентичність	Ідентичність	
	Анонімна ідентичність	Анонімна ідентичність	
	Пароль	Пароль	

TLS	Сертифікат центру сертифікації	Сертифікат центру сертифікації
	Ідентичність	Ідентичність
	Пароль	Пароль

VPN

Тип підключення	**Встановити тип VPN-з'єднання**

Якщо ви виберете "Per-App VPN" як тип VPN, доступні VPN-клієнти зміняться. Per-App VPN обмежує VPN певними програмами і запускає VPN-з'єднання автоматично, якщо запускається певна програма.

AppTec360 VPN клієнт	Використовує VPN-клієнт AppTec360 у поєднанні з універсальним шлюзом
Ім'я з'єднання Ім'я з'єднання	Ім'я VPN-з'єднання
Конфігурація шлюзу	Виберіть конфігурацію VPN універсального шлюзу
Завжди на VPN	Змушує VPN бути завжди активним, тому весь трафік проходить через VPN.
Увімкнути власне блокування	Блокує всі мережеві підключення, коли пристрій не підключено до VPN. Використовуйте цю функцію обережно, оскільки неправильне налаштування може призвести до повної втрати з'єднання. Тільки для Android Enterprise на Android 7 або новішої версії
Увімкнути блокування AppTec360	Блокує використання всіх програм, поки не буде запущено VPN-з'єднання

Cisco AnyConnect	
Ім'я з'єднання Ім'я з'єднання	Ім'я VPN-з'єднання
Сервер	Адреса сервера
Режим сертифіката	Відключено = деактивовано Автоматичний = автоматичний

L2TP (тільки KNOX)	Доступно лише на пристроях Samsung
Ім'я з'єднання Ім'я з'єднання	Назва з'єднання
Сервер	Адреса сервера
Увімкнути секрет L2TP	
Пошукові домени DNS	Пошук доменів DNS

Тип підключення	**Встановити тип VPN-з'єднання**

PPTP (тільки для KNOX)	Доступно лише на пристроях Samsung
Ім'я з'єднання Ім'я з'єднання	Ім'я VPN-з'єднання
Сервер	Адреса сервера
Увімкнути шифрування	Увімкнути шифрування
Пошукові домени DNS	Пошук доменів DNS

L2TP / IPSec PSK (тільки KNOX)	Доступно лише на пристроях Samsung
Ім'я з'єднання Ім'я з'єднання	Ім'я VPN-з'єднання
Сервер	Адреса сервера
Ключ IPSec Pre-Shared Key	Попередньо наданий ключ для автентифікації
Увімкнути секрет L2TP	
Секрет L2TP	
Пошукові домени DNS	Пошук доменів DNS

IPSec XAuth PSK (тільки KNOX)	Доступно лише на пристроях Samsung
Ім'я з'єднання Ім'я з'єднання	Ім'я VPN-з'єднання
Сервер	Адреса сервера
Ідентифікатор IPSec	Ім'я користувача для підключення
Ключ IPSec Pre-Shared Key	Пароль для підключення
Пошукові домени DNS	Пошук доменів DNS

OpenVPN	

Ім'я з'єднання Ім'я з'єднання	Назва з'єднання
Профіль OpenVPN	Сюди буде скопійовано вміст файлу .ovpn
Додаток OpenVPN	Існує два різних додатки для використання OpenVPN Ми рекомендуємо додаток "OpenVPN для Android". Але в якості альтернативи можна використовувати додаток "OpenVPN Connect"

Обмеження

Тут ви можете встановити обмеження щодо управління з'єднаннями.

Дозволити роумінг даних	Дозволити мобільні дані в роумінгу
Примусити роумінг даних	Якщо увімкнено, роумінг для мобільних даних активується назавжди (не рекомендується!). Цей параметр замінює параметр "Дозволити роумінг даних"!
Наступні налаштування доступні лише на Samsung KNOX 2.0 або новішої версії	
Дозволити лише екстрені виклики	Дозволити лише екстрені виклики
Увімкнути WiFi	Увімкнути WiFi
Мінімальний рівень безпеки мережі WiFi	Мінімальний рівень безпеки мережі WiFi Відкрито = дозволені всі типи WiFi
Заборонити користувачеві додавати мережі WiFi	Користувач не може самостійно додати мережу WiFi Це налаштування можливе лише в тому випадку, якщо в розділі "Керування з'єднаннями" було визначено профіль WiFi
Дозволити SMS та MMS	Всі = Весь SMS та MMS трафік дозволено Incoming SMS Only = Дозволено лише вхідні SMS-повідомлення Тільки вихідні SMS = дозволені тільки вихідні SMS-повідомлення Немає = трафік SMS / MMS заборонено
Дозволити синхронізацію в роумінгу	Дозволити синхронізацію в роумінгу Увімкнено = активовано Вимкнено = деактивовано Вибір користувача = вибір користувача
Дозволити голосовий роумінг	Дозволити голосовий роумінг Увімкнено = активовано Вимкнено = деактивовано User Choice = вибір користувача
Використання системного проксі-сервера http	Використання HTTP-проксі-сервера, яке передбачено налаштуваннями системи в налаштуваннях, залежить від підключеної мережі (WiFi або APN)

APN

Наступні налаштування доступні лише на Samsung SAFE 2.0 або новішої версії!

APN Відображуване ім'я	APN Відображуване ім'я	
Назва точки доступу Ім'я точки доступу	Ім'я APN	
Протокол вихідного сервера	Не встановлено	
	Ні.	
	PAP	Протокол PAP
	ЧЕП	Протокол CHAP
	PAP або CHAP	Протокол PAP або CHAP
MCC - мобільний код країни	Тут вводиться MCC, залиште це поле порожнім, якщо потрібно використовувати MCC вставленої SIM-карти	
MNC - код мобільної мережі	Тут вводиться MNC, залиште це поле порожнім, якщо потрібно використовувати MCC вставленої SIM-карти	
Адреса сервера	Адреса сервера	
Номер порту сервера	Номер порту сервера	
Проксі-адреса сервера	Проксі-адреса сервера	
Адреса сервера MMS	Адреса MMS-сервера, для Стандартного залиште порожнім	
Номер порту MMS	Номер порту MMS	
Адреса проксі-сервера MMS	Адреса проксі-сервера MMS	
Ім'я користувача	Ім'я користувача	
Пароль	Пароль	
Тип точки доступу	Допустимі типи "default", "mms", "supl" Якщо це поле залишити порожнім, то буде використано "default,supl,mms"	
Бажаний APN	Перевага надається APN	

Bluetooth

Тут можна виконати різноманітні налаштування Bluetooth.

Наступні налаштування доступні лише на Samsung KNOX 1.0 або новішої версії!

Дозволити виявлення пристрою через Bluetooth	Дозволити виявлення пристрою через Bluetooth
Дозволити створення пари Bluetooth	Увімкнути сполучення Bluetooth
Дозволити пристрої з Bluetooth-гарнітурою	Дозволити пристрої з Bluetooth-гарнітурою
Дозволити Bluetooth-пристрої гучного зв'язку	Дозволити Bluetooth-пристрої гучного зв'язку
Дозволити пристрої Bluetooth A2DP	Дозволити аудіопотоки Bluetooth A2DP між пристроями
Дозволити вихідні дзвінки	Дозволити вихідні дзвінки через BT
Дозволити передачу даних через Bluetooth	Дозволити передачу даних через Bluetooth
Увімкнути прив'язку Bluetooth	Дозволяє використовувати пристрій як модем (інтернет-з'єднання Bluetooth)
Дозволити підключення до комп'ютера через Bluetooth	Дозволити підключення до комп'ютера через Bluetooth

Менеджмент ПІМ

Обмін

Доступно лише для Samsung KNOX 1.0 або новішої версії!

Адреса електронної пошти	Надана адреса електронної пошти користувача Зверніть увагу на "Заповнювачі", які можна використовувати для роботи з обліковими даними і не виконувати зміни вручну на кожному пристрої Натиснувши на кнопку **Показати заповнювачі**, ви можете відобразити їх для себе
Ім'я хосту сервера	Адреса сервера ваших Exchange-серверів
Ім'я користувача	Ім'я для входу для відповідного пристрою кінцевого користувача, також зверніть увагу на "Заповнювачі тут
Домен	Адреса домену
Пароль (тільки на рівні пристрою)	За бажанням, окремому пристрою може бути надано пароль, якщо він залишиться порожнім, користувачеві буде запропоновано ввести свій Exchange Password
Кількість попередніх днів для синхронізації	Кількість днів, які визначають, коли імейли будуть синхронізовані знову
Підпис	Можна додати підпис (Підказка: деякі пристрої вимагають HTML-форматування для підпису)
Обліковий запис за замовчуванням	Встановлює, що цей поштовий акаунт є стандартним акаунтом
Використовуйте протокол захищених сокетів (SSL)	Використовуйте SSL-з'єднання
Використовуйте захист на транспортному рівні (TLS)	Використовуйте з'єднання TLS
Приймаємо всі сертифікати	Приймаються всі сертифікати. Виберіть цю опцію, якщо ваш Exchange-сервер використовує самопідписаний сертифікат

Електронна пошта

Тут ви можете розподілити облікові записи IMAP і POP на відповідні пристрої кінцевих користувачів.

Наступні налаштування доступні лише на Samsung KNOX 1.0 або новішої версії!		
Адреса електронної пошти	Надана адреса електронної пошти користувача Зверніть увагу на "Заповнювачі", які можна використовувати для роботи з обліковими даними і не виконувати зміни вручну на кожному пристрої Натиснувши на кнопку **Показати заповнювачі**, ви можете відобразити їх для себе	
Вхідний протокол сервера	Вхідний протокол сервера	IMAP або POP
Вхідна адреса сервера	Вхідна адреса сервера	
Вхідний порт сервера	Вхідний порт сервера	
Вхідний логін/ім'я користувача на сервері	Вхідний логін/ім'я користувача на сервері	
Пароль вхідного сервера (тільки на рівні пристрою)	Пароль вхідного сервера (тільки на рівні пристрою)	
Вхідний сервер використовує SSL	Вхідний сервер використовує SSL	
Вхідний сервер використовує TLS	Вхідний сервер використовує TLS	
Вхідний сервер приймає всі сертифікати	Вхідні сервери приймають всі типи сертифікатів	
Протокол вихідного сервера	Протокол вихідного сервера	SMTP
Вихідний порт сервера	Вихідний порт сервера	
Вихідний сервер використовує додаткові облікові дані	Додаткові облікові дані для вихідного сервера. Якщо цей параметр вимкнено, то будуть використовуватися налаштування вхідного сервера	
Логін/ім'я користувача вихідного сервера	Логін/ім'я користувача вихідного сервера	
Пароль вихідного сервера (тільки на рівні пристрою)	Пароль вихідного сервера	

Вихідний сервер використовує SSL	Вихідний сервер використовує SSL
Вихідний сервер використовує TLS	Вихідний сервер використовує TLS
Вихідний сервер приймає всі сертифікати	Вихідний сервер приймає всі типи сертифікатів
Підпис	Підпис можна прикріпити тут (Підказка: деякі пристрої вимагають HTML-форматування для підпису)
Сповіщати користувача про отримання нової електронної пошти	Сповіщає користувача про отримання нового листа

AE Gmail Exchange

Info: Ця конфігурація буде застосована до програми Gmail. Тому вам потрібно схвалити та встановити Gmail.

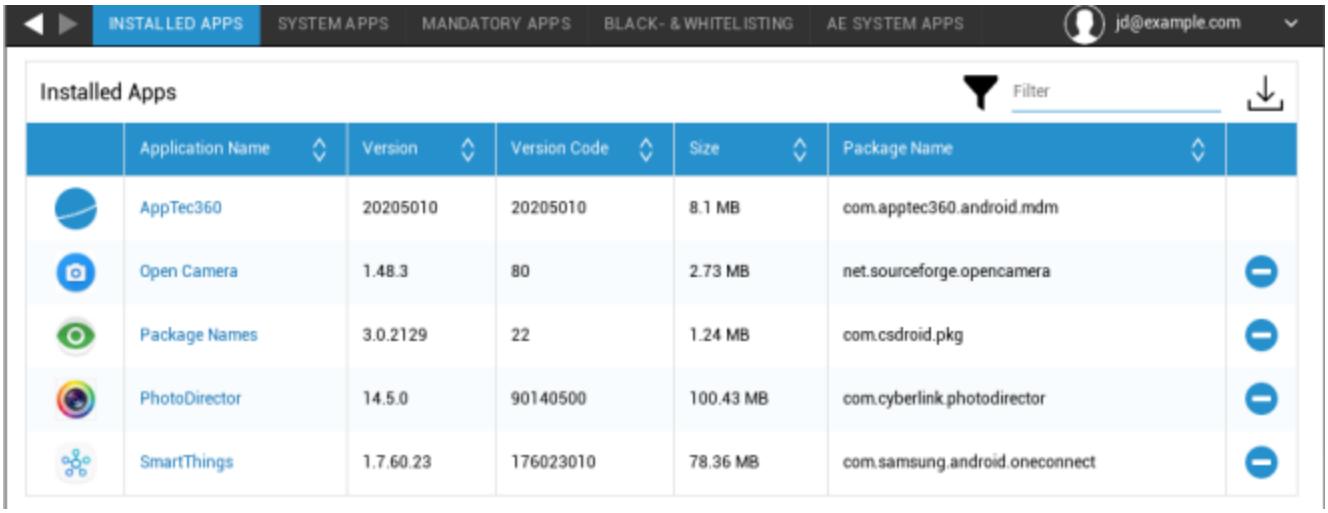
Адреса електронної пошти	Надана адреса електронної пошти користувача Зверніть увагу на "Заповнювачі", які можна використовувати для роботи з обліковими даними і не виконувати зміни вручну на кожному пристрої Натиснувши на кнопку Показати заповнювачі, ви можете відобразити їх для себе
Ім'я хосту сервера	Адреса сервера ваших Exchange-серверів
Ім'я користувача	Ім'я для входу для відповідного пристрою кінцевого користувача, також зверніть увагу на "Заповнювачі тут
Підпис	Можна додати підпис (Підказка: деякі пристрої вимагають HTML-форматування для підпису)
Кількість попередніх днів для синхронізації	Кількість днів, які визначають, коли імейли будуть синхронізовані знову
Ідентифікатор пристрою	Ідентифікатор EAS. Залиште це поле порожнім, якщо ваше середовище не вимагає цього
Використовуйте протокол захищених сокетів (SSL)	Використовуйте SSL-з'єднання
Приймаємо всі сертифікати	Приймаються всі сертифікати. Виберіть цю опцію, якщо ваш Exchange-сервер використовує самопідписаний сертифікат
Дозволити некеровані акаунти	Дозволяє користувачеві додавати додаткові облікові записи
Сертифікат клієнта	Завантажте клієнтський сертифікат, якщо цього вимагає ваш Exchange-сервер

Керування додатками

Enterprise App Manager

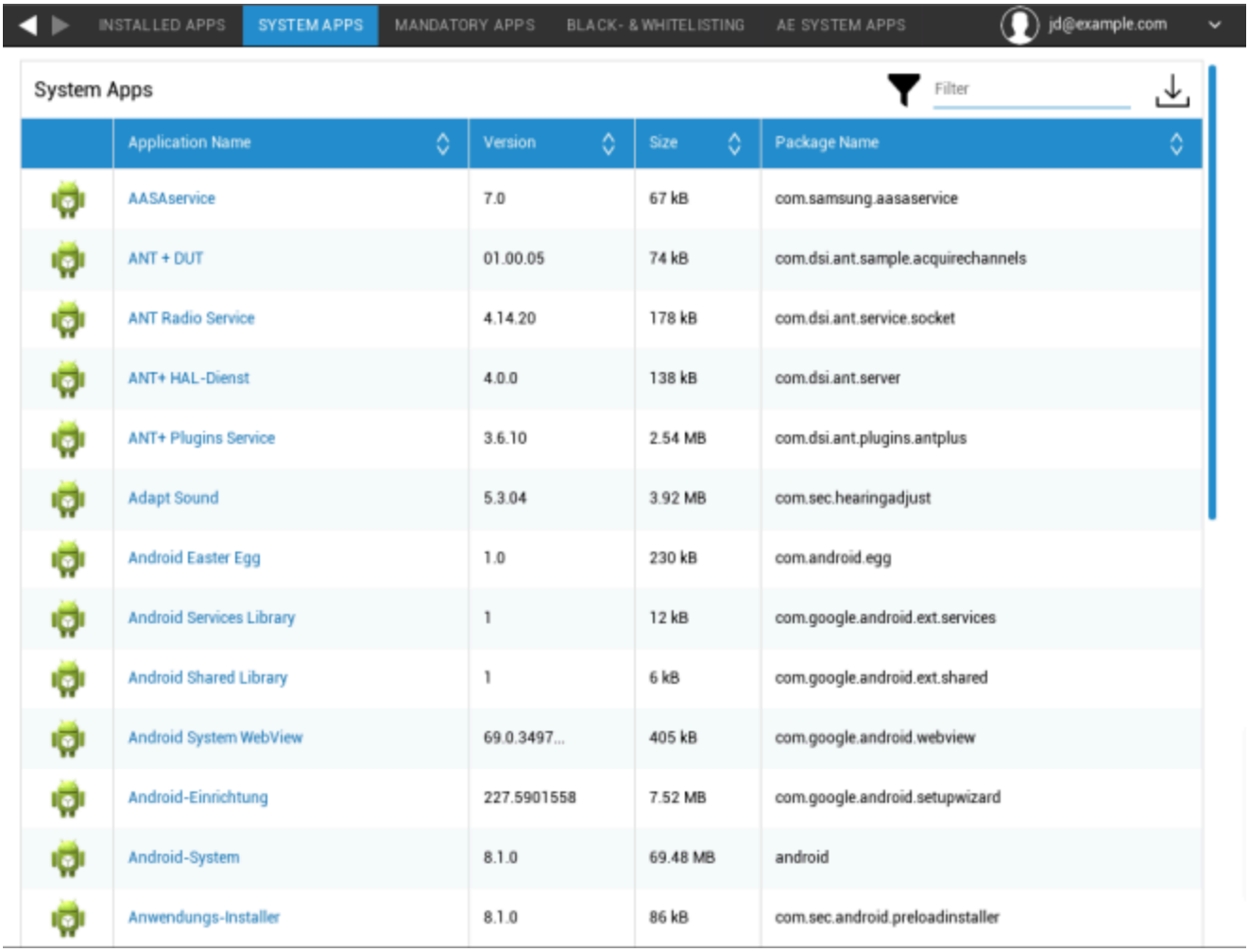
Встановлені програми (лише на рівні пристрою)

Тут будуть показані всі програми, які наразі встановлені на пристрої кінцевого користувача.


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

Системні програми (лише на рівні пристрою)

У розділі "Системні програми" буде перелічено всі попередньо встановлені системні програми з назвою пакунків та їхньою версією.



Обов’язкові програми

У розділі Обов'язкові програми ви можете визначити, які програми мають бути встановлені на пристрої. Залежно від конфігурації та пристрою додаток буде встановлено автоматично або користувачеві буде запропоновано встановити його.

Зверніть увагу, що для зручного керування програмами рекомендується використовувати Android Enterprise.

Сценарії наведені нижче:

Звичайні додатки Play Store

Встановлення додатків з Playstore завжди потребує втручання користувача. Крім того, на пристрої має бути налаштований обліковий запис Google.

Внутрішнє встановлення додатків

На пристроях Samsung ці програми будуть встановлені беззвучно. Єдиний виняток - контейнер, де користувач має підтвердити встановлення.

У будь-якому іншому випадку користувач повинен підтвердити встановлення програми.

Додатки для Android Enterprise Play Store

Ці програми завжди встановлюються безшумно, без втручання користувача.

Щоб додати обов'язковий додаток, натисніть на "+" і виберіть потрібний додаток зі списку. Зверніть увагу, що ви не можете встановлювати додатки з вкладки "Google Play Store", якщо пристрій налаштовано з Android Enterprise як повністю керований або як контейнер.

Якщо ви використовуєте Android Enterprise, виберіть програми з розділу "AE Play Store". Щоб зробити програми доступними тут, підтвердіть їх у магазині Google Enterprise Play, перейшовши до Загальних налаштувань → AE Play Store → Програми Play Store.

При видаленні обов'язкового додатка, він також буде видалений з пристрою.

Ви можете натиснути на назву програми у списку обов'язкових програм і перейти на вкладку "конфігурація", щоб налаштувати програму. Для цього потрібно використовувати Android Enterprise, і програма повинна це підтримувати. Тому доступні опції залежать від обраної програми.

Додатки для системи AE

Тут ви можете увімкнути системні програми для пристроїв Android Enterprise. Будь ласка, майте на увазі, що вказаний додаток має бути у сховищі системи, інакше нічого не відбудеться. 296

Обмеження та налаштування

Чорні та білі списки

Тут ви можете визначити чорний або білий список. Всі програми з чорного списку будуть заблоковані. Усі програми, яких немає в білому списку, будуть заблоковані. Порожній чорний список нічого не блокує, тоді як порожній білий список блокує все*.

**Усі обов'язкові програми та програми з Enterprise App Store будуть автоматично додані до білого списку. Вам не потрібно додавати їх вручну*

Натиснувши на "+", ви можете або знайти програму, яку хочете додати до чорного чи білого списку, або ввести назву пакета вручну.

Обмеження системних додатків

У розділі "Обмеження системних програм" ви можете, серед іншого, заблокувати попередньо встановлені програми та служби за власним бажанням.

Вимкнути браузер	Вимкнути стандартний браузер
Вимкнути календар	Вимкнути рідний календар
Вимкнути калькулятор	Відключити калькулятор
Вимкнути браузер Chrome	Вимкніть браузер Chrome
Вимкнути годинник	Вимкнути годинник
Вимкнути контакти	Вимкнути контакти
Вимкнути дозвон	Вимкнути рідний набір номера
Вимкнути електронну пошту	Вимкнути електронну пошту
Вимкнути обмін	Вимкнення облікових записів Exchange
Вимкнути Facebook	Вимкнути додаток Facebook
Вимкнути галерею	Вимкнути рідну програму галереї
Вимкнути Gmail	Вимкнути Gmail
Вимкнути Google Books	Вимкнути Google Books
Вимкнути Кіоск Google Play	Вимкнути Кіоск Google Play
Вимкнути Google Maps	Вимкнути Google Maps
Вимкнути Google Music	Вимкнути Google Music
Вимкнути фільми Google	Вимкнути фільми Google
Вимкнути Google Play Store	Вимкнути Google Play Store (загальнодоступний магазин додатків)
Вимкнути Google Plus	Вимкнути Google Plus
Вимкнути пошук Google	Вимкнути пошук Google
Вимкнути Google Talk / Google Hangouts	Вимкнути Google Talk / Google Hangouts
Вимкнути музичний програвач	Вимкнути рідну програму музичного плеєра
Вимкнути налаштування	Вимкнути налаштування пристрою
Вимкнути Sim Toolkit	Вимкнути служби Sim Toolkit
Вимкнути SMS / MMS	Вимкнути SMS / MMS
Вимкнути режим перегляду вулиць	Вимкнути служби перегляду вулиць
Вимкнути Youtube	Вимкнути Youtube

Програми Samsung

У розділі "Програми Samsung" ви можете визначити додаткові налаштування та/або обмеження для пристроїв Samsung.

Вимкнути AllShare Play / Samsung Link	Вимкнути AllShare Play / Samsung Link
Вимкнути ChatON	Вимкнути ChatON
Вимкнути Game Hub	Вимкнути Game Hub
Вимкнути групову гру	Вимкнути групову гру
Вимкнути довідку	Вимкнення довідки Samsung
Вимкнути KNOX	Вимкнути контейнер Samsung KNOX
Вимкнути пам'ятку	Вимкнути голосову нагадування
Вимкнути "Мої файли	Вимкнути "Мої файли
Вимкнути оптичний зчитувач	Вимкнути оптичний зчитувач
Вимкнути Polaris Office	Вимкнути Polaris Office
Вимкнути Readers Hub / Samsung Books	Вимкнути Readers Hub / Samsung Books
Вимкнути пам'ятку S	Вимкнення програми Samsung Memo
Вимкнути перекладач S	Вимкнути програму Samsung Translator
Вимкнути голос S	Вимкнути голосовий помічник S
Вимкнення програм Samsung	Вимкнути Samsung App Store
Вимкнути Samsung Hub	Вимкнення розважальних магазинів Samsung
Вимкнути відеопрогравач	Вимкнути відеопрогравач
Вимкнути диктофон	Вимкнути диктофон
Вимкнути WatchON	Вимкнути WatchON (імітує пульт дистанційного керування)

Програми Huawei

У розділі "Програми Huawei" ви можете визначити додаткові налаштування та/або обмеження для пристрою Huawei.

Вимкнення DLNA	Вимкнення DLNA
Вимкнути інсталятор додатків	Вимкнути інсталятор додатків
Вимкнути диспетчер файлів	Вимкнути диспетчер файлів
Вимкнути Диспетчер резервного копіювання	Вимкнути Диспетчер резервного копіювання
Вимкнути оновлення системи	Вимкнути оновлення системи
Вимкнути панель інструментів	Вимкнути панель інструментів
Вимкнути погоду	Вимкнути погоду
Вимкнути FM-радіо	Вимкнути FM-радіо

Налаштування керування програмами

Тут ви можете визначити поведінку оновлень для внутрішніх додатків.

Частота перевірки оновлень визначає, як часто додаток AppTec360 шукає оновлення для внутрішніх додатків. Як тільки буде виявлено нову версію, вона буде завантажена та встановлена.

Поріг Wi-Fi визначає, чи слід обмежувати завантаження з'єднаннями Wi-Fi, якщо додаток більший за встановлений вами поріг. Якщо він менший або ви не визначили поріг, додаток буде завантажуватися як через Wi-Fi, так і через стільникову мережу.

Enterprise App Store

Зверніть увагу, що додавання додатків тут (Enterprise App Store) НЕ призведе до їхнього автоматичного встановлення на пристрої. Користувач повинен відкрити Enterprise App Store на своєму пристрої та встановити програму вручну.

Якщо ви хочете автоматично встановлювати програми на пристрій, перейдіть до "Керування програмами" → "Enterprise App Manager" → "Обов'язкові програми" і додайте туди потрібні програми.

У цьому пункті ви можете розповсюджувати необов'язкові програми серед своїх користувачів.

Playstore

Натисніть на "+", щоб додати додаток з Play Store до магазину. Якщо ви використовуєте Android Enterprise, перейдіть до "Керування програмами Enterprise Play Store". Також майте на увазі, що для встановлення вказаних тут додатків на → пристрої має бути налаштований обліковий запис Google.

Власні сили

У пункті "In-House" ви можете завантажувати та розповсюджувати додатки, розроблені власними силами.

Натисніть на "+", щоб додати внутрішній додаток до корпоративного магазину додатків, який потім може бути встановлений користувачем. У цьому діалозі ви також можете завантажити новий внутрішній додаток.

Enterprise Play Store

Зверніть увагу, що додавання додатків тут (Enterprise Play Store) НЕ призведе до їх автоматичного встановлення на пристрій(и). Користувач повинен відкрити Play Store на своєму пристрої та встановити програму вручну.

Якщо ви хочете автоматично встановлювати програми на пристрій, перейдіть до "Керування програмами" → "Enterprise App Manager" → "Обов'язкові програми" і додайте туди потрібні програми.

У цьому пункті ви можете розповсюджувати необов'язкові програми серед своїх користувачів.

Тут ви можете додати програми до Android Enterprise Playstore. Зверніть увагу, що ви повинні схвалити додатки в Загальних налаштуваннях → AE Play Store → Додатки Play Store. Ці програми будуть додані до звичайного магазину Google Play.

Також майте на увазі, що спочатку потрібно визначити макет з програмами у Загальних налаштуваннях → Керування програмами → AE Play Store → Макет магазину.

Додатки повинні бути в макеті, перш ніж ви зможете успішно додати їх до магазину.

Режим кіоску та лаунчер

Режим кіоску

Режим кіоску дозволяє вам попередньо визначити програму або URL-адресу. Після цього можна буде запускати/відвідувати лише цю програму та/або URL-адресу.

Аналогічно, різні апаратні кнопки можна деактивувати в режимі "Кіоск".

Автоматичний запуск	Автоматично запускає режим кіоску, щойно профіль потрапляє на пристрій кінцевого користувача
Режим кіоску за розкладом?	Ви можете запланувати час для роботи в режимі кіоску, тоді він почнеться і завершиться автоматично, у встановлений вами час
Час початку	Час початку
Час у хвилинах	Час у хвилинах, після якого режим кіоску повинен знову завершитися

Тип програми

Єдиний додаток	Якщо ви хочете запустити програму в режимі кіоску, виберіть "Пакет" у розділі "Тип програми"
Додаток для кіоску	Натисніть тут, щоб вибрати програму, яку слід запустити в режимі кіоску Ви знайдете звичайний огляд управління додатками Ви можете вибрати між "Магазином Google Play", "Власними програмами Android" та "Ім'ям пакету"

Тип програми

URL	Якщо ви хочете запустити URL-адресу в режимі кіоску, виберіть "URL" у розділі "Тип програми" Потім визначте бажану URL-адресу
Очистити браузер після бездіяльності	Тут ви можете визначити інтервал часу в хвилинах, через який режим кіоску має бути перезапущено
Очистити веб-кеш і файли cookie	Якщо ви активуєте цю функцію, то після перезапуску режиму кіоску веб-кеш (файли cookie та кешовані зображення) буде стерто
Політика однакового походження	Якщо ця функція активна, то користувач може переглядати лише підсторінки визначеної URL-адреси Наприклад, ви визначили таку URL-адресу: www.mypage.com Тоді користувач може перейти за адресою: www.mypage.com/subpage
Білі списки URL-адрес	Тут ви можете вести білий список, всі ці URL-адреси дозволені Не більше 1 URL-адреси в рядку URL-адреса повинна починатися з http:/ або https://
URL-адреси в чорному списку	Тут ви можете вести чорний список, всі ці URL-адреси заборонені Не більше 1 URL-адреси в рядку URL-адреса повинна починатися з http:/ або https://
Орієнтація екрана	Цей параметр стосується налаштувань екрана Автоматичний = автоматичний Портрет = вертикальний формат Ландшафт = ландшафтний режим

Багатофункціональний додаток	Якщо ви виберете режим кіоску "Multi App", використання AppTec360 Launcher буде обов'язковим.
Додатки	Додаток: Виберіть Playstore або власний додаток як додаток для кіоску. Також можна ввести ім'я пакету. Вибраний додаток Kiosk повинен бути встановлений на пристрої. Не забудьте встановити додаток Kiosk як обов'язковий. Ярлик на головному екрані: Якщо увімкнено, буде створено ярлик на головному екрані. Якщо встановлено значення "Вимкнено", програма все одно відображатиметься у списку програм.

Увімкнено пароль на вихід	Якщо ви активуєте цю функцію, то користувач може завершити роботу в режимі кіоску за допомогою пароля, який ви попередньо визначили
Пароль для виходу	Це пароль, який ви визначили заздалегідь
Автоматичне згортання рядка стану	Якщо цей параметр увімкнено, рядок стану буде автоматично згорнуто. З цією опцією користувачі можуть бачити інформацію в рядку стану, але не можуть отримати доступ до його функцій
Вимкнути рядок стану	Рядок стану містить сповіщення, ярлики та інформацію. Доступно лише для пристроїв Samsung з KNOX 1.0 або новішої версії.
Вимкнення клавіш гучності	Вимкнути клавіші гучності (доступно лише на пристроях Samsung з KNOX 1.0 або новішої версії)
Вимкнути перемикач увімкнення / вимкнення	Вимкнути перемикач увімкнення / вимкнення (доступно лише на пристроях Samsung з KNOX 1.0 або новішої версії)
Вимкнути кнопку "Додому	Вимкнути кнопку "Додому". Якщо ця функція активована, то режим кіоску можна завершити лише в консолі AppTec360 (доступно лише на пристроях Samsung з версією KNOX 1.0 або вище)
Вимкнути панель навігації	За допомогою цього пункту ви можете вимкнути панель навігації (Назад / Меню) Якщо ця функція активована, то режим кіоску можна завершити тільки в консолі AppTec360 (доступно лише на пристроях Samsung з версією KNOX 1.0 або вище)

Налаштування оновлення програми	
Дозволити оновлення програми	Користувачам буде запропоновано оновити програми, навіть якщо активовано режим кіоску. На пристроях з Samsung KNOX програми оновлюватимуться безшумно.
Вікно оновлення	Встановіть інтервал, через який користувачам буде запропоновано встановити оновлення програми.

TeamViewer	
Увімкнути доступ без нагляду	Якщо увімкнено, адміністратори можуть віддалено керувати пристроєм без участі користувача. На пристрої потрібно встановити програму TeamViewer Host.

AppTec360 Launcher

Увімкніть AppTec360 Launcher	Увімкнено: Увімкнути програму запуску AppTec360. Користувач повинен встановити його як лаунчер за замовчуванням один раз. Примітка: Якщо увімкнено режим "Кіоск", а режим "Кіоск" встановлено на "Багато додатків", використання лаунчера AppTec360 буде обов'язковим.
Великі іконки	Увімкнено: Показує збільшену версію іконок програм на панелі запуску
Приховати піктограму програми AppTec360	Увімкнено: Повністю приховує програму AppTec360
Приховати іконку магазину AppTec360	Увімкнено: Повністю приховує AppTec360 Enterprise AppStore

Налаштування AppTec360

Увімкнути програму налаштувань AppTec360	Додаток AppTec360 Settings забезпечує контроль над з'єднаннями WiFi і Bluetooth
Увімкнення налаштувань у декількох додатках Режим кіоску	Якщо увімкнено, користувачі можуть отримати доступ до програми налаштувань AppTec360, коли активний режим кіоску з декількома додатками

Пульт дистанційного керування

Splashtop

Показує поточний стан налаштування Splashtop. Тут ви побачите кроки, які потрібно виконати для віддаленого доступу до пристрою через Splashtop. Тут також потрібно ввести код розгортання, який ви можете отримати на веб-сайті Splashtop. Код розгортання необхідний для підключення до пристрою.

Teamviewer

Показує поточний стан налаштування Teamviewer. Тут ви побачите кроки, які потрібно виконати, щоб отримати віддалений доступ до пристрою через Teamviewer.

Управління контентом

Вміст

Тут ви можете активувати Contentbox для цього пристрою. Після активації додаток Contentbox буде інстальовано на пристрій.

Безпечний браузер

Тут ви можете ввімкнути Безпечний браузер для цього пристрою. Після активації на пристрій буде інстальовано додаток Безпечний браузер. Цей браузер можна налаштувати так, щоб він пропонував на пристрої веб-браузер, який відповідає вашим потребам.

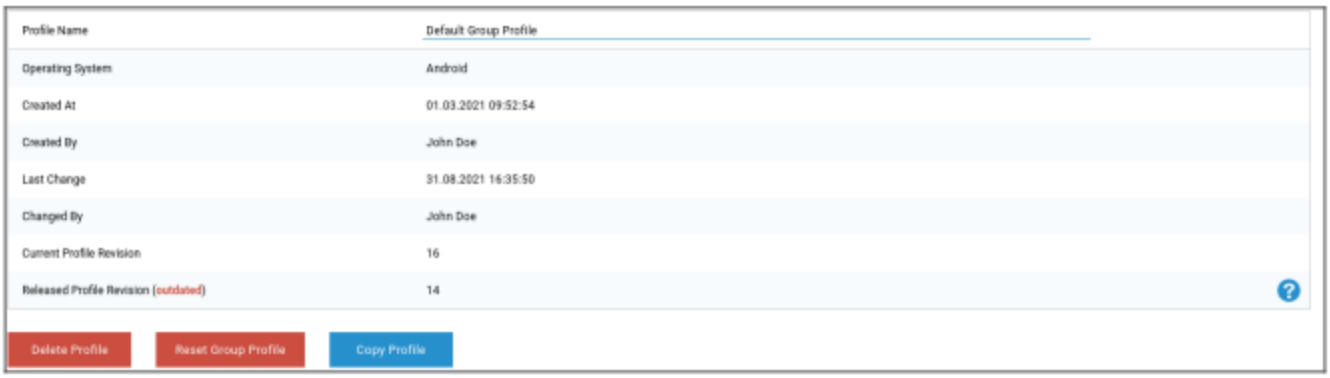
Вимагати пароль	Вимагати від користувача встановлення та використання пароля для доступу до браузера.
Обмежити завантаження/ відкриття	Блокує завантаження з веб-сайтів
Обмежити завантаження	Обмежує завантаження певними URL-адресами. Не вказуйте жодної URL-адреси, щоб повністю заблокувати завантаження
Дозволити копіювання	Дозволяє копіювати, вирізати або ділитися текстом всередині веб-сторінок.
Дозволити захоплення екрана	Дозволити створення скріншотів.
Частота очищення даних	Виберіть, з якою періодичністю слід автоматично видаляти BCI дані користувача (історію, кеш тощо).
Закладки компанії	Закладки з'являться в папці "Закладки компанії" в закладках браузера. Вони не можуть бути відредаговані користувачем.
Приховати адресний рядок	Приховує адресний рядок, щоб користувач не бачив URL-адресу, яку він відвідує
Внутрішньобраузерний білий список (без універсального шлюзу)	Вмикає білі списки URL-адрес на стороні клієнта. - Закладки компанії завжди в білому списку - Підтримується лише 100 URL-адрес - Використовуйте Універсальний шлюз для необмеженої кількості чорних та білих списків
Чорні та білі списки на основі шлюзу	До чорного списку висуваються наступні вимоги: - Працюючий універсальний шлюз AppTec360 ("Загальні налаштування" → "Універсальний шлюз") - Працююча конфігурація VPN із зазначеним DNS-сервером ("Загальні налаштування" → "Універсальний шлюз" → "Налаштування VPN") - Конфігурація чорного списку ("Загальні налаштування" → "Універсальний шлюз" → "Чорний список доменів") - Дійсне VPN-з'єднання в профілі ("Управління з'єднаннями" → "VPN")

Конфігурація ПК з Windows 10

Генерал

Огляд профілю групи (тільки на рівні групи)

Відкривши профіль групи, ви отримаєте короткий огляд профілю.



Ім'я профілю Ім'я профілю	Назва профілю (можна змінити тут)
Операційна система	Операційна система, для якої призначений профіль
Створено в	Час створення
Створено	Творець профілю
Остання зміна	Час останньої зміни профілю
Змінено	Обліковий запис, який вніс останні зміни
Поточна редакція профілю	Перегляд стану збереженого профілю
Випущено ревізію профілю	Призначена версія профілю ("Призначити зараз"). Якщо за текстом мітки вказано "(застаріла)", це означає, що ви зберегли профіль, але ще не призначили його, тому пристрої все одно отримають стару версію.

Огляд пристрою (тільки на рівні пристрою)

Короткий огляд пристрою, який містить наступне:

Назва комп'ютера	Назва комп'ютера
Клієнт	Пристрої типу Windows
Останнє відоме місцезнаходження	Широта і довгота останнього відомого місцезнаходження пристроїв
Призначені обов'язкові програми	Кількість обов'язкових програм, призначених для пристрою
ІДЕНТИФІКАТОР КОМП'ЮТЕРА	UID комп'ютера
Редакція ОС	Показує вашу версію Windows
Версія ОС	Поточна встановлена версія Windows
Збірка ОС	Поточна збірка Windows
Операційна система	Встановлена операційна система
Серійний номер	Серійний номер пристрою
Право власності на пристрій	Налаштований тип власності
Тип пристрою	Тип пристрою
Укорінений	Показує, чи є Пристрій рутованим
Дотримується	Показує, чи відповідає пристрій вимогам
Востаннє бачили	Дата і час, коли були внесені зміни до профілю
Призначення користувача	Відображає користувача або групу, якій наразі призначено цей пристрій. Ви можете перемістити пристрій, вибравши іншого користувача або групу зі спадного списку.

Налаштування

Дозволити автоматичне оновлення	Дозволити або заборонити автоматичне оновлення ОС.

Ревізія конфігурації (лише на рівні пристрою)

Тут ви отримаєте огляд того, який профіль групи призначено пристрою.

Якщо ви натиснете на профіль групи, ви отримаєте доступ безпосередньо до профілю і зможете виконати налаштування.

За допомогою цього символу ви можете повернути призначені програми до налаштувань профілю групи.

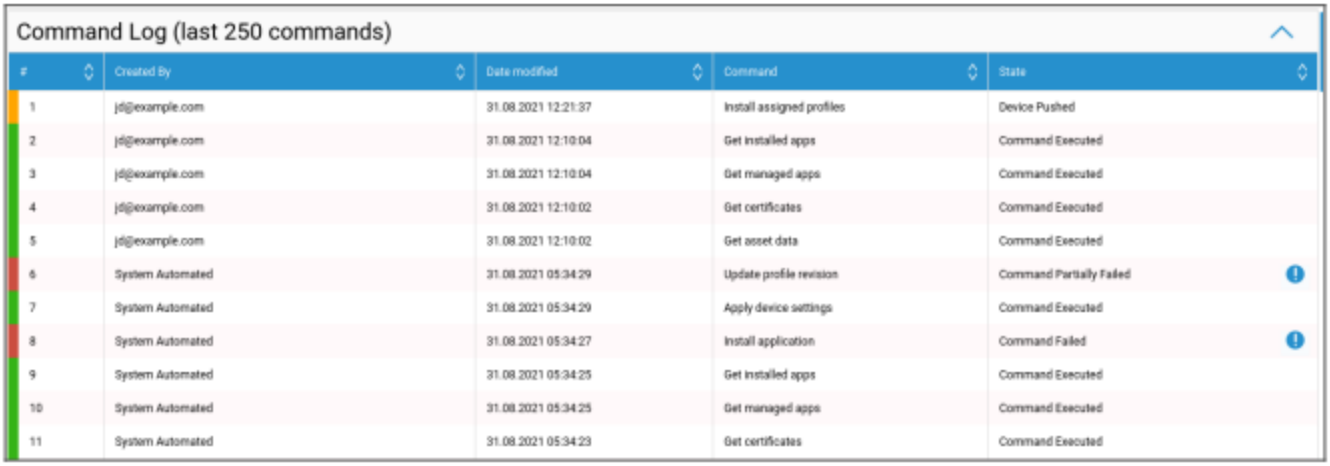
За допомогою цього символу ви можете скинути профіль пристрою, щоб він не мав жодних налаштувань.

"Доступна новіша версія" вказує на те, що профіль групи було змінено та збережено, але не призначено. Щоб застосувати зміни до пристроїв, профіль групи потрібно призначити за допомогою "Призначити зараз" на рівні групи.

Журнал пристрою (тільки на рівні пристрою)

Командний журнал

Тут ви можете побачити, які команди були видані для пристрою і який їхній статус.



Команди, створені за допомогою "Автоматизації системи", автоматично створюються системою.

Можливі стани команди

Пристрій натиснуто	До служби push (наприклад, APNS) було надіслано push-запит, щоб повідомити пристрій про необхідність з'єднатися з сервером EMM.
Команду створено	Команда була створена в системі.
Команду відправлено.	Команда була надіслана на пристрій після того, як він підключився до сервера.
Команду виконано	Команда була успішно виконана.
Команда не спрацювала	Команда не спрацювала. *
Команда частково не виконана	Залежно від операційної системи пристрою деякі команди можуть бути згруповані разом. У цьому деякі частини цієї командної групи зазнали невдачі. *
Команда виконана, але зрештою не спрацювала	Команда була виконана, але, можливо, не була.
Команда "Відсіч	Команду було перевиконано користувачем.
Викинуто	Команду було відкинуто. Наприклад, її було замінено іншою командою або пристрій було перереєстровано, а старі команди видалено

*Якщо за повідомленням стоїть знак оклику, ви можете отримати додаткову інформацію, навівши курсор на іконку.

Управління активами (тільки на рівні пристрою)

Інформація про пристрій

Виробник	Виробник пристрою
Модель	Модель пристрою
Номер моделі	Номер моделі
Операційна система	Операційна система
Версія ОС	Версія операційної системи
Серійний номер	Серійний номер
ExchangeID	ExchangeID
Загальна оперативна пам'ять	Загальна оперативна пам'ять
Роздільна здатність дисплея	Роздільна здатність дисплея
Мова телефону	Мова пристрою
Версія прошивки	Версія прошивки
Клієнтська версія DM	Керування пристроями Клієнтська версія
Апаратна версія	Версія апаратного забезпечення пристрою
Архітектура процесора	Архітектура процесора (тип процесора)

Стільниковий зв’язок

Мережа оператора SIM-карти	Мережа операторів
Номер телефону	Номер телефону
Статус роумінгу	Статус роумінгу
IMEI	IMEI
IMSI	IMSI
Прошивка модему	Прошивка модему

Інформація про синхронізацію

Миттєве підключення DM	Пристрій повинен негайно створити з'єднання з AppTec
Початковий час повторної спроби	Початковий час повторної спроби для цього першого з'єднання
Повторні спроби з'єднання	Кількість нових спроб з'єднання після розриву з диспетчером з'єднань або помилки на рівні WinInet
Максимальний час сну	Максимальний час сну після помилки відправки пакета
Перші спроби синхронізації	Час для першого етапу після зарахування
Перший інтервал повторної спроби	Час для першого етапу після зарахування
Друга спроба синхронізації	Час для другого етапу після зарахування
Другий інтервал повторної спроби	Час для другого етапу після зарахування
Регулярні спроби синхронізації	Час для додаткових етапів після зарахування
Регулярний інтервал повторних спроб	Час для додаткових етапів після зарахування

Управління безпекою

Захист від крадіжок (лише на рівні пристрою)

Інформація про GPS (лише на рівні пристрою)

Тут ви можете встановити поточне/останнє місцезнаходження пристрою. Локалізацію можна захистити одним або навіть двома паролями - Див: "Загальні налаштування" > "Конфіденційність" > "Доступ до GPS"

Налаштування GPS

Увімкнути GPS-відстеження	Увімкніть регулярну синхронізацію інформації GPS.
Інтервал відстеження	Встановіть інтервал синхронізації інформації GPS.

Конфігурація безпеки

Пароль

Мінімальна довжина пароля	Мінімальна довжина пароля	
Склад пароля	Вказує кількість певних символів, які повинен містити пароль Вони складаються з великих і малих літер, цифр і спеціальних символів	
Якість пароля	Тут ви можете налаштувати якість пароля	
	Буквено-цифровий	Тільки цифри та літери
	Числовий	Тільки цифри
	Цифровий або буквено-цифровий	Цифри або цифри та літери
Блокування максимального часу бездіяльності	Кількість хвилин бездіяльності користувача на пристрої, після чого пристрій буде заблоковано. Користувач повинен розблокувати пристрій після закінчення цього часу, ввівши свій пароль від пристрою.	
Закінчення терміну дії пароля	Встановіть час, через який потрібно встановити новий пароль	
Обмеження історії паролів	Кількість раніше використаних паролів, які не допускаються	
Максимальна кількість невдалих спроб введення пароля	Кількість разів, коли пароль може бути введений неправильно, перш ніж буде виконано повне очищення пристрою	

Антивірус

Налаштування антивірусу - Задати конфігурацію сканування	
Тип сканування	Дозволяє вибрати швидке або повне сканування
Встановити початок сканування	Дозволяє вибрати час доби, коли Захисник Windows почне сканування
Частота сканування	Дозволяє вибрати день запуску сканування захисником Windows
Частота оновлення підписів	Вказує інтервал у годинах, який буде використовуватися для перевірки підписів

Тип конфігурації файлів для сканування	
Дозволити сканування архівних файлів	Дозволити або заборонити сканування архівів (наприклад, .zip) під час доступу до них.
Дозволити сканування скриптів	Дозволяє або забороняє функцію сканування сценаріїв Windows Defender.
Дозволити сканування електронних листів	Дозволити або заборонити сканування електронних листів.
Дозволити сканування мережевих файлів	Дозволити або заборонити сканування мережевих файлів.
Дозволяє повністю сканувати зіставлені мережеві диски	Дозволити або заборонити сканування зіставлених мережевих дисків (увімкнено лише тоді, коли увімкнено повне сканування).
Керування двонаправленим скануванням	Контролює, які набори файлів слід відстежувати.
Дозволяє повністю сканувати знімні диски	Дозволити або заборонити повне сканування знімних дисків. Ініціюється лише під час повного сканування.

Тип файлів, які буде виключено з сканування	
Ігнорувати типи файлів для сканування	Визначте набір типів розширень файлів. Кожне розширення файлу для кожного поля.
Ігнорувати шляхи до каталогів	Визначте набір шляхів до каталогів, щоб не сканувати їх. Один шлях на одне поле. Приклади: "C:\Example", "C:\Windows" або "C:\Users".
Виключити процеси зі сканування	Виключити файли, відкриті певними процесами, з перевірки антивірусом Microsoft Defender. . Один шлях на поле. Приклади: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Додаткові налаштування	
Дозволити моніторинг в режимі реального часу	Увімкнення або вимкнення функції моніторингу в режимі реального часу Windows Defender
Дозволити моніторинг поведінки	Увімкнення або вимкнення функції моніторингу поведінки Windows
Увімкнути хмарний захист	Дозвольте або забороніть Захиснику Windows надсилати інформацію в корпорацію Майкрософт про будь-яку знайдену проблему. Корпорація Майкрософт проаналізує ці відомості, дізнається більше про проблему, яка впливає на пристрій, і запропонує кращі рішення
	Поведінка при надсиланні зразків
Увімкнути захист Windows Defender IOAV	Увімкнення або вимкнення захисту Windows Defender IOAV
Дозволити доступ до інтерфейсу захисників "Про захист доступу"	
Середній коефіцієнт завантаження процесора	Відображає середній коефіцієнт завантаження процесора для сканування Windows Defender (у відсотках)

Робота зі шкідливим програмним забезпеченням	
Низький ступінь тяжкості	Для кожного рівня небезпеки ви можете визначити, як пристрій буде поводитися зі шкідливим програмним забезпеченням. Доступні наступні варіанти: • Чистий • Карантин. • Видалити • Дозвольте • Визначено користувачем • Блок
Помірний ступінь тяжкості	
Високий ступінь тяжкості	
Високий ступінь тяжкості	
Скільки днів зберігати очищене шкідливе програмне забезпечення	Період часу в днях, протягом якого карантинні файли/елементи зберігатимуться в системі. Значення за замовчуванням - 0, що

	означає, що об'єкти зберігаються в карантині, але не видаляються автоматично. Максимальне значення - 90.

Центр безпеки

Центр безпеки Windows - Налаштування безпеки Windows	
Вимкнути інтерфейс захисту від вірусів та загроз	
Приховати інтерфейс відновлення даних за допомогою програм-вимагачів	
Вимкнути інтерфейс захисту облікового запису	
Вимкнути брандмауер та інтерфейс мережевого захисту	
Вимкнути інтерфейс управління додатками та браузером	
Заборонити зміни в захисті від експлойтів	Заборонити користувачеві вносити зміни до налаштувань захисту від експлойтів
Вимкнути інтерфейс безпеки пристрою	
Приховати усунення несправностей TPM	Приховати налаштування усунення несправностей TPM
Вимкнути кнопку Очистити TPM	
Вимкнення інтерфейсу продуктивності та стану пристрою	
Вимкнути сімейні опції інтерфейсу	

Налаштувати тости	
Увімкнути індивідуальну інформацію про підтримку	Увімкнення відображення контактної інформації служби підтримки вашої компанії в правому нижньому куті програми центру безпеки.
Адреса електронної пошти	Встановити адресу електронної пошти компанії
Назва компанії	Встановити назву компанії
Телефон компанії	Встановити телефон компанії
URL-адреса довідки	Встановити URL-адресу довідки компанії

Додаткові налаштування	
Вимкнути сповіщення	Вимкнути відображення сповіщень Центру безпеки Windows Defender.
Приховати рекомендації щодо оновлення мікропрограми TPM	Приховати рекомендацію оновити прошивку TPM у разі виявлення вразливої прошивки.
Відображати назву компанії та контактні дані	Відображайте назву компанії та контактні дані у спливаючій картці контакту в Центрі безпеки Windows Defender.
Приховати безпечне завантаження	Приховати область завантаження безпеки.
Приховати Керування областю сповіщень про безпеку	Приховати керування областю сповіщень Windows Security.

Налаштування брандмауера

Конфігурація брандмауера - Глобальні налаштування	
Ігнорувати набір автентифікації	Ігнорувати весь набір автентифікації, якщо вони не підтримують всі набори автентифікації, вказані в наборі
Тип черги пакетів	Вказує, як увімкнено масштабування для програмного забезпечення на стороні приймача як для зашифрованого приймання, так і для очищення прямого шляху для сценарію тунельного шлюзу IPsec.
Вимкнути фільтрацію FTP за станом	Якщо його вимкнено, він не виконуватиме фільтрацію протоколу передачі файлів (FTP) за станом, щоб дозволити вторинні з'єднання
Час простою охоронної асоціації	У цьому полі задається час простою асоціацій безпеки у секундах. Асоціації безпеки видаляються після того, як мережевий трафік не з'являється протягом вказаного періоду часу.
Кодування попередньо наданих ключів	Встановіть кодування попередньо наданого ключа
Винятки IPSec	Налаштування винятків інтернет-протоколу
Перевірка списку відкликання сертифікатів	

Профілі брандмауера (Профіль домену / Приватний профіль / Загальнодоступний профіль)	
Увімкнути брандмауер для цього профілю	
Вимкнути сповіщення	Вимкнути відображення сповіщення користувачеві, коли програмі заблоковано прослуховування порту.
Блокування одноадресних відповідей на багатоадресні розсилки	
Застосовуйте правила брандмауера для дозволених додатків	Якщо його не застосовано, правила брандмауера авторизованих програм у локальному сховищі ігноруються і не застосовуються
Впровадження правил брандмауера глобального порту	Якщо його не застосовано, правила брандмауера глобального порту у локальному сховищі ігноруються і не застосовуються. Параметр має значення, лише якщо його задано або перелічено у сховищі групової політики або якщо його перелічено зі сховища GroupPolicyRSoPStore
Застосовуйте правила брандмауера	Якщо його не застосовано, правила брандмауера з локального сховища ігноруються і не застосовуються
Впроваджуйте правила безпеки з'єднання	Якщо його не ввімкнено, правила безпеки з'єднання з локального сховища ігноруються і не застосовуються
Вихідна дія за замовчуванням	Дія, яку брандмауер виконує за замовчуванням на вихідних з'єднаннях
Дія за замовчуванням при вхідному дзвінку	Дія, яку брандмауер виконує за замовчуванням на вхідних з'єднаннях
Вимкнути режим "Стелс	Невидимий режим - це механізм у брандмауері Windows, який допомагає запобігти отриманню зловмисниками інформації про мережеві комп'ютери та запущені на них служби.
Вимкнути запобігання відповіді на небажаний трафік	Якщо вимкнено, правила невидимого режиму брандмауера не повинні перешкоджати хост-комп'ютеру відповідати на небажаний мережевий трафік, якщо цей трафік захищено за допомогою IPsec.

Правила брандмауера

Правила брандмауера	
Ім'я	Назва правила
Опис	Опис правила
Дія	Вкажіть, чи буде це правило блокувати трафік, чи дозволяти його. Зверніть увагу, що опція Блокувати може також блокувати трафік (залежно від решти налаштувань) між MDM-сервером і Пристроєм
Напрямок	
Увімкнути обхід кордону (доступно лише тоді, коли для параметра **Напрямок** встановлено значення "**Вхідний трафік**")	Вказує, що певному вхідному трафіку дозволено тунелювати через NAT та інші граничні пристрої з використанням технології тунелювання Teredo.

Програми та послуги	
Визначте програми, все інше	Якщо не ввімкнено, то будуть розглядатися всі заявки
Ім'я пакунка Назва пакунка	Ім'я сімейства пакунків, до якого буде застосовано правило.
Шлях до файлу програми	Повна програма, наприклад, C:\Windows\System\Notepad.exe, до якої буде застосовано правило
Повноцінне бінарне ім'я	Повне кваліфіковане бінарне ім'я, до якого застосовуватиметься правило. FQBN - це рядок у наступному вигляді: {Видавець\Продукт\Ім'я файлу,Версія}
Назва послуги	Введіть ім'я служби (наприклад, "EventLog"). Ви можете отримати список імен служб у Powershell, виконавши команду "Get-Service".

Протоколи та порти				
Протокол	Протокол, який використовується правилом.			
	Доступні значення: - Будь-який - Нестандартний - ПОРТ - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-маршрут - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Options - VRRP - PGM - L2TP	Якщо встановлено значення "Користувацьке	Введіть номер протоколу в діапазоні від 0 до 255	Номер протоколу
		Якщо налаштовано на TCP або UDP	Вкажіть локальні порти, інакше будуть використані всі	Локальні порти, які будуть використовуватися правилом, також дозволено вказувати в діапазоні портів
			Місцевий порт	Один порт або ряд портів. Наприклад, 100-120, 200, 300-320.
			Вкажіть віддалені порти, інакше будуть використані всі	Віддалені порти, які буде використовувати правило, також дозволено вказувати в діапазоні портів
			Віддалений порт	Один порт або ряд портів. Наприклад, 100-120, 200, 300-320.

Сфера застосування	
Вказуйте локальні IP-адреси, в іншому випадку - будь-які	Набір локальних IP-адрес, це також може бути діапазон IP-адрес, розділених символом -.
Локальна IP-адреса	Набір окремих IP-адрес або діапазон IP-адрес, розділених - -.
Вкажіть віддалені IP-адреси, в іншому випадку будь-який віддалений IP	Вкажіть набір віддалених IP-адрес, це може бути також діапазон IP-адрес, розділених знаком "-".
Віддалена IP-адреса	Вкажіть окремі IP-адреси або діапазон IP-адрес
Жетони.	Токени, які можна встановити разом з віддаленими адресами. Токени Intranet, RmtIntranet і Ply2Renders підтримуються у Windows 10 версії 1809 і вище.

Додаткові налаштування

Вкажіть профілі, інакше будуть використані всі	Якщо вимкнено, будуть використовуватися всі профілі
Домен	Профіль домену
Рядовий	Особистий профіль
Громадськість	Публічний профіль
Вкажіть інтерфейси, інакше будуть використані всі	Якщо вимкнено, будуть використовуватися всі інтерфейси
Локальна мережа	Інтерфейс локальної мережі
Віддалений доступ	Інтерфейс віддаленого доступу
Бездротовий	Бездротовий інтерфейс

Місцеві директори	
Додавання авторизованих локальних користувачів	Дозволити додавання списку локальних користувачів, які будуть використовувати це правило
Авторизовані користувачі	Список авторизованих локальних користувачів для цього правила. Ім'я користувача має бути у форматі Security Description Definition Language (SDDL), наприклад, PC_NAME\USERNAME. Це поле не повинно бути заповнене, якщо для цього правила встановлено ім'я служби

Налаштування обмежень

Функціональність пристрою

Дозволити SD-карту	Дозволити використання SD-карти
Дозволити камеру	Дозвольте використовувати камеру
Дозволити службу визначення місцезнаходження	Увімкнути службу визначення місцезнаходження пристрою
Дозволити бічне завантаження додатків	Дозволити встановлення програм з невідомих джерел
Увімкнути режим розробника	Дозволяє режим розробника
Дозволити роумінг мобільних даних	Дозволити роумінг мобільних даних
Увімкнути Cortana	Увімкнути голосовий помічник Cortana
Дозволити пошуку використовувати місцезнаходження	Дозволити пошук за місцезнаходженням
Дозволити додавання облікового запису електронної пошти не від Microsoft	Вкажіть, чи дозволено користувачеві додавати поштові скриньки, що не належать до MSA.
Дозволити підключення облікового запису Microsoft	Вкажіть, чи дозволити використання облікового запису MSA для автентифікації з'єднань і служб, не пов'язаних з електронною поштою.
Дозволити синхронізацію моїх налаштувань	Дозволяє синхронізувати налаштування на всьому пристрої
Доменні імена, захищені для підприємств	Вказує доменні імена підприємства, розділені символом ";".
Дозволити користувачеві вимкнути відновлення системи	Дозволяє користувачеві вимкнути Відновлення системи. **УВАГА!** Цю функцію слід використовувати лише на пристроях, які належать або надані корпоративною компанією чи організацією, або на

	пристроях, що належать користувачеві, якщо користувач дозволив, щоб пристрій повністю керувався корпоративною компанією. Якщо вимкнути цей параметр політики, Відновлення системи буде вимкнено, а доступ до Майстра відновлення системи буде неможливим. Також буде вимкнено можливість налаштувати Відновлення системи або створити точку відновлення за допомогою Захисту системи.
Дозволити відмову від реєстрації користувача	Дозволяє користувачеві видалити корпоративну частину з пристрою і таким чином від'єднатися від серверів AppTec360. Якщо це станеться, керувати пристроєм буде неможливо **УВАГА!** Цю функцію слід використовувати лише на пристроях, які належать або надані корпоративною компанією чи організацією, або на пристроях, що належать користувачеві, якщо користувач дозволив, щоб пристрій повністю керувався корпоративною компанією. Якщо ви вимкнете цей параметр політики, користувачі не зможуть видаляти реєстрації MDM. Вкажіть, чи дозволено користувачеві видаляти обліковий запис робочого місця через панель керування робочим місцем. Сервер MDM завжди може віддалено видалити обліковий запис.

BitLocker

Конфігурація BitLocker

Загальні налаштування	
Вимагати шифрування пристрою	Запропонувати користувачам увімкнути шифрування пристрою. Залежно від версії Windows і конфігурації системи, користувачам може бути запропоновано це зробити: - Щоб переконатися, що шифрування від іншого провайдера не ввімкнено. - Вимкнути BitLocker Drive Encryption, а потім знову увімкнути BitLocker.
Методи шифрування	
Метод шифрування дисків операційної системи	
Метод шифрування для стаціонарних накопичувачів даних	
Метод шифрування знімних накопичувачів даних	
Вимкнути попередження про стороннє шифрування диска	Вимкнути попередження про використання на пристрої сторонньої служби шифрування дисків. Починаючи з Windows 10, версії 1803, цей параметр підтримується лише для пристроїв, приєднаних до Azure Active Directory.
Дозволити запуск шифрування під час входу користувача, який не є адміністратором	Підтримується лише для пристроїв, приєднаних до Azure Active Directory

Розширення AppTec360	
Безшумне шифрування	Якщо вибрати опцію "Вимагати шифрування пристрою", служба управління AppTec360 запустить автоматичне безшумне шифрування дисків пристрою.
Автоматично генерувати облікові дані користувача	Зашифрований диск з ОС буде захищено автоматично згенерованими обліковими даними користувача. PIN-код TPM, якщо доступний TPM, або 6-значний текстовий пароль. Згенеровані облікові дані будуть надіслані на електронну адресу, зареєстровану для даного пристрою. Якщо цю опцію вимкнено, єдиним можливим захистом для тихого шифрування є використання TPM. У такому випадку для пристроїв без TPM шифрування безшумним способом не вдасться.
Шифрування стаціонарних дисків	Будь-які доступні стаціонарні диски з даними також будуть зашифровані та захищені функцією "Автоматичне розблокування" за допомогою ключа, що зберігається на диску з операційною системою.

Налаштування диска ОС

Вимагати додаткову автентифікацію під час запуску	Цей параметр дозволяє вам налаштувати, чи буде BitLocker вимагати автентифікацію при кожному запуску комп'ютера. Цей параметр застосовується під час налаштування BitLocker. Якщо ви увімкнете цей параметр, користувачі зможуть налаштувати розширені параметри запуску у майстрі налаштування BitLocker.
Блокування BitLocker без сумісного TPM	
Тільки TPM.	
TPM та PIN-код	
TPM і ключ	
TPM, ключ та PIN-код	Якщо ви хочете вимагати використання PIN-коду та USB-накопичувача (ключа), користувач повинен налаштувати BitLocker за допомогою інструменту командного рядка "manage-bde" замість майстра налаштування BitLocker Drive Encryption.

Вимагати мінімальну довжину PIN-коду

	Мінімум символів

Налаштуйте повідомлення та URL-адресу для відновлення перед завантаженням	Налаштуйте все повідомлення про відновлення або замініть існуючу URL-адресу, яка відображається на екрані відновлення ключа перед завантаженням, коли диск з ОС заблоковано. Примітка: Не всі символи і мови підтримуються у попередньому завантаженні. Наполегливо рекомендуємо перевірити правильність відображення символів, які ви використовуєте, на екрані відновлення перед завантаженням.
	Параметр повідомлення про відновлення перед завантаженням
	Користувацьке повідомлення про відновлення
	Спеціальна URL-адреса відновлення

Варіанти відновлення диска з ОС		Цей параметр дозволяє контролювати відновлення дисків операційних систем, захищених BitLocker, за відсутності необхідних облікових даних. Цей параметр застосовується під час налаштування BitLocker. За замовчуванням дозволено використання агента відновлення даних на основі сертифікатів, параметри відновлення можуть бути вказані користувачем, включаючи пароль і ключ відновлення, а інформація для відновлення не зберігається в резервній копії в AD DS.
	Агент для відновлення даних на основі сертифікатів Block	Вкажіть, чи можна використовувати агент відновлення даних з дисками операційної системи, захищеними BitLocker. Перш ніж використовувати агент відновлення даних, його потрібно додати з елемента Політики відкритих ключів в Консолі керування груповою політикою або локальному редакторі групової політики. Щоб дізнатися більше про додавання агентів відновлення даних, зверніться до посібника з розгортання BitLocker Drive Encryption на Microsoft TechNet.
	Налаштування відновлення пароля BitLocker	
	Налаштування ключа відновлення BitLocker	
	Збережіть інформацію про відновлення BitLocker у службі доменів Active Directory	
	Конфігурація сховища для відновлення AD DS BitLocker	Зберігання пакету ключів дозволяє відновити дані з фізично пошкодженого диска.
	Вимагати збереження даних відновлення в AD DS	Заборонити користувачам вмикати BitLocker, якщо комп'ютер не підключено до домену та

Виправлені налаштування накопичувача	
Можливості відновлення фіксованих дисків	Цей параметр дозволяє контролювати відновлення стаціонарних дисків, захищених BitLocker, за відсутності необхідних облікових даних. Цей параметр застосовується під час налаштування BitLocker. За замовчуванням дозволено використання агента відновлення даних на основі сертифікатів, параметри відновлення можуть бути вказані користувачем, включаючи пароль і ключ відновлення, а інформація для відновлення не зберігається в AD DS.
Агент для відновлення даних на основі сертифікатів Block	
Налаштування відновлення пароля BitLocker	
Налаштування ключа відновлення BitLocker	
Збережіть інформацію про відновлення BitLocker у службі доменів Active Directory	
Конфігурація сховища для відновлення AD DS BitLocker	Зберігання пакету ключів дозволяє відновити дані з фізично пошкодженого диска.
Вимагати збереження даних відновлення в AD DS	Заборонити користувачам вмикати BitLocker, якщо комп'ютер не підключено до домену і резервне копіювання інформації для відновлення BitLocker в AD DS не вдалося. Примітка: Пароль для відновлення буде згенеровано автоматично.
Заборонити доступ на запис до незахищених фіксованих дисків	

Налаштування знімних дисків	
Заборонити доступ на запис до незахищених знімних дисків	Заборонити доступ на запис до знімних дисків, не захищених Bitlocker. Примітка: Якщо параметр "Знімні диски: Заборонити доступ на запис" увімкнено у груповій політиці, цей параметр політики буде проігноровано.
Заборонити доступ на запис до пристроїв, налаштованих в іншій організації	Доступ на запис буде надано лише тим дискам, ідентифікаційні поля яких збігаються з ідентифікаційними полями комп'ютера. Ці поля визначаються параметром групової політики "Надавати унікальні ідентифікатори для вашої організації".

Стан BitLocker

Тут ви можете побачити поточний стан зашифрованих BitLocker дисків

C [OS Drive]
Статус шифрування
Зашифровано (%)
Статус захисту
Метод шифрування
Основні засоби захисту
Пароль для відновлення

Натиснувши на кнопку "Змінити пароль відновлення", ви можете змінити пароль відновлення BitLocker.

Управління сертифікатами

Список сертифікатів

Тут відображається список сертифікатів, які встановлені на пристрої.

Конфігурація сертифіката

Тут ви можете налаштувати сертифікати і те, як вони будуть встановлені на пристрої.

Довірений сертифікат	
Опис	Опис сертифікату
Сфера застосування	Сфера розгортання сертифікатів: Поточний користувач проти пристрою
Магазин сертифікатів	"Ненадійні сертифікати" доступні лише починаючи з Windows 10, версія 1803
Файл сертифіката	Завантажте файл PKCS#1

Посвідчення особи			
Опис	Опис сертифікату		
Сфера застосування	Сфера розгортання сертифікатів: Поточний користувач проти пристрою		
Ключове розташування	Постачальник сховища ключів для встановлення приватного ключа.		
		ППМ. Не вдасться, якщо немає TPM	
	TPM. Якщо TPM відсутній, поверніться до програмного KSP		
	Постачальник сховища програмних ключів		Позначте приватний ключ як експортований
	Windows Hello для бізнесу	Назва контейнера	Вказує ім'я контейнера Windows Hello для бізнесу (раніше відомого як Microsoft Passport for Work).
		Текст підказки PIN-коду	Дозволяє вказати спеціальний текст, який відображатиметься у запиті PIN-коду Windows Hello для бізнесу під час реєстрації сертифіката.
Облікові дані	Завантажити файл PKCS#12		

SCEP

Опис	Опис сервера SCEP		
Сфера розгортання	Сфера розгортання сертифікатів: Поточний пристрій проти користувача		
URL-адреси серверів SCEP	Один або декілька серверів, які видають сертифікати через SCEP		
Тема	Представлення імені у форматі X.500. Наприклад, "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Альтернативні назви теми	Тип	Адреса електронної пошти	
		DNS	
		URI	
		Основне ім'я користувача (UPN)	
CA Fingerprint	SHA1-відбиток сертифіката центру сертифікації. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Термін дії одиниці виміру	Дні, місяці або роки		
Термін дії			
Виклик	Використовується як попередньо наданий секрет для автоматичної реєстрації		
Повторні спроби	Кількість разів, яку пристрій повинен повторити спробу, якщо сервер надсилає відповідь PENDING. Значення за замовчуванням - 5, максимальне значення - 30.		
Затримка на повторну спробу	Кількість хвилин для очікування перед повторною спробою. Значення за замовчуванням - 5, мінімальне значення - 1.		
Ключовий розмір	Розмір ключа в бітах		
Алгоритм хешування	Сімейство хеш-алгоритмів		
Ключове використання	Розширення використання ключа визначає призначення (наприклад, шифрування, підпис) ключа, що міститься в сертифікаті. Необхідно вибрати принаймні один з варіантів "Цифровий підпис" або "Шифрування ключа".		
Розширене використання	Вказує розширене використання ключів. Залежно від конфігурації сервера SCEP. Вкажіть список відповідних OID, наприклад, 1.3.6.1.5.5.7.3.2		

клавіш	(Автентифікація клієнта)		
Ключове розташування	Постачальник сховища ключів для встановлення приватного ключа.		
		ППМ. Не вдасться, якщо немає TPM	
	TPM. Якщо TPM відсутній, поверніться до програмного KSP		
	Постачальник сховища програмних ключів		
	Windows Hello для бізнесу	Назва контейнера	Вказує ім'я контейнера Windows Hello для бізнесу (раніше відомого як Microsoft Passport for Work).
		Текст підказки PIN-коду	Дозволяє вказати спеціальний текст, який відображатиметься у запиті PIN-коду Windows Hello для бізнесу під час реєстрації сертифіката.

Керування з’єднаннями

Wi-Fi

На цьому етапі виконується попереднє налаштування пристроїв кінцевих користувачів для доступу до внутрішніх Точок доступу

Ідентифікатор набору послуг (SSID)	SSID мережі, до якої буде встановлено з'єднання
Автоматичне приєднання	Увімкнути автоматичне приєднання до мережі
Прихована мережа	Активувати, якщо точка доступу не передає SSID

Тип безпеки

Встановіть тип захисту точки доступу

Відкрита система WEP	
Пароль	Пароль для точки доступу

WPA PSK	
Пароль	Пароль для точки доступу

WPA EAP	
Тип автентифікації	Тип автентифікації, можливий лише з "PEAP-MSCAHPv2"
Швидке перепідключення	Пристрої можуть перемикатися між точками доступу без необхідності повторної автентифікації
Гостьовий доступ	Користувач не має облікового запису і тому повинен зареєструватися як гість
Карантинні перевірки	Клієнт повинен виконати перевірку NAP (захист доступу до мережі) і надати результати системі, яка потім вирішить, чи може клієнт підключитися.
Вимагає криптографічної прив'язки	Аутентифікація можлива лише за допомогою Crypto Binding
Перевірка сервера	Клієнт перевіряє, чи дійсний сертифікат сервера. Якщо це так, з'єднання буде встановлено
Запит на отримання сертифікатів	Дозволяє користувачеві приймати ненадійні сертифікати
Імена серверів	Дозволяє відобразити ім'я RADIUS-сервера, який пропонує мережеву автентифікацію та авторизацію

WPA2-PSK	
Пароль	Пароль точки доступу

WPA2 EAP	
Тип автентифікації	Тип автентифікації, можливий лише з "PEAP-MSCAHPv2"
Швидке перепідключення	
Гостьовий доступ	
Карантинні перевірки	Активує захист доступу до мережі NAP
Вимагає криптографічної прив'язки	Аутентифікація можлива лише за допомогою Crypto Binding
Перевірка сервера	
Запит на отримання сертифікатів	Підказки щодо підтвердження сертифіката сервера, імені або автентифікації кореневого сертифіката (CA)
Імена серверів	Список серверів, яким повинні довіряти пристрої
Ні.	Відсутність встановленої системи безпеки
Використання проксі-сервера	Використання проксі-сервера
Адреса сервера	Адреса проксі-сервера
Порт сервера	Порт сервера проксі-сервера

Використання проксі-сервера

Увімкніть використання проксі-сервера.

Адреса сервера	Адреса проксі-сервера, що використовується цією мережею.
Порт сервера	Порт проксі-сервера, що використовується цією мережею.

Обмеження Wifi

Тут ви можете визначити різні обмеження Wifi.

Увімкнути WiFi	Дозволити/заборонити WiFi
Дозволити спільний доступ до Інтернету	Дозволити використання точки доступу
Дозволити автоматичне підключення до точок доступу WiFi Sense	Дозволити автоматичне підключення до точок доступу WiFi Sense
Дозволити ручне налаштування WiFi	Дозволити користувачеві підключатися до мереж WiFi, які не були визначені AppTec
Частота сканування бездротової мережі	Дозволяє встановити інтервал сканування WLAN. Тут більше значення підвищує здатність розпізнавання WIFI-мереж.

VPN

Виконайте відповідні налаштування тут, щоб налаштувати VPN-з'єднання

Ім'я з'єднання Ім'я з'єднання	Вказана назва з'єднання		
Тип VPN	VPN-з'єднання Per-App використовується для захисту трафіку певних додатків.		
	VPN	Завжди увімкнено	Це автоматично підключить VPN при вході в систему і залишиться підключеним до тих пір, поки користувач не відключить його вручну.
	Per-App VPN	Програми VPN	Визначте програми, які використовують це VPN-з'єднання
		Блокування кожного додатка	Блокування на додаток дозволяє вибраним програмам мати доступ лише через це VPN-з'єднання. Ця функція залежить від брандмауера Windows Defender.
	Профіль WIP	Домен WIP для цього з'єднання	Ідентифікатор підприємства, необхідний для підключення цього VPN-профілю до політики захисту інформації Windows (WIP)

Тип підключення

AppTec360 VPN	
Для "AppTec360 VPN" потрібно, щоб завантаження додатків було дозволено. Будь ласка, увімкніть "Дозволити завантаження додатків" у "Керування безпекою" → "Налаштування обмежень" → "Функціональність пристрою".	
Конфігурація шлюзу	Щоб налаштувати VPN-з'єднання з чорним списком, виберіть конфігурацію VPN із зазначеним DNS-сервером. Налаштувати конфігурацію VPN можна в "Загальні налаштування" → "Універсальний шлюз" → "Налаштування VPN".

IKEv2		
Сервери	Список VPN серверів	
Тунель пристроїв	Увімкніть з'єднання перед входом користувача.	
Метод автентифікації	EAP	EAP XML
	Сертифікати машин	
Алгоритм шифрування		
Алгоритм перевірки цілісності		
Diffie-Hellman Group		
Алгоритм шифрування		
Алгоритм перетворення автентифікації		
Група досконалої передової секретності (PFS)		

PPTP		
Сервери	Список VPN серверів	
Метод автентифікації	EAP	EAP XML

L2TP		
Сервери	Список VPN серверів	
Метод автентифікації	EAP	EAP XML
Алгоритм шифрування		
Алгоритм перевірки цілісності		
Diffie-Hellman Group		
Алгоритм шифрування		
Алгоритм перетворення автентифікації		
Група досконалої передової секретності (PFS)		

Автоматично		
Сервери	Список VPN серверів	
Метод автентифікації	EAP	EAP XML

Типові конфігурації VPN

Запам'ятовуйте облікові дані під час кожного входу	
Реєстрація IP-адрес у внутрішньому DNS	
Правила фільтрації мережевого трафіку	Обмежте VPN-з'єднання визначеним набором правил.
Список пошуку за суфіксом DNS	Суфікси DNS для додавання до списку пошуку DNS для маршрутизації коротких імен.
Правила таблиці політики дозволу імен (NRPT)	Правила таблиці політики дозволу імен (NRPT) визначають, як DNS вирішує імена при підключенні до VPN.
Виявлення надійних мереж	Список суфіксів DNS для визначення довіреної мережі.
Роздільна проходка тунелів	Розділене тунелювання означає, що трафік може проходити через будь-який інтерфейс, визначений мережевим стеком.
Розділення маршрутів проходки тунелів	Список маршрутів, які буде додано до таблиці маршрутизації для VPN-інтерфейсу.
Налаштування проксі-сервера	Налаштування проксі, що використовується з цією мережею
Адреса проксі-сервера	Адреса проксі-сервера як повне ім'я хоста або IP-адреса.
Порт	Порт проксі-сервера.
URL-адреса автоматичного налаштування проксі-сервера	URL-адреса для автоматичного отримання налаштувань проксі-сервера.

Обмеження VPN

Тут ви можете визначити різні обмеження VPN.

Дозволити налаштування VPN	Ця настанова дозволяє/забороняє користувачеві деактивувати та змінювати налаштування VPN
Дозволити VPN через стільниковий зв'язок	Дозволяє/забороняє пристрою встановлювати VPN-з'єднання, якщо пристрій використовує мобільні дані
Дозволити роумінг VPN через мобільний зв'язок	Дозволяє/забороняє пристрою встановлювати VPN-з'єднання, якщо пристрій перебуває в роумінгу

Bluetooth

Тут ви можете встановити, чи слід дозволити/заборонити Bluetooth.

Увімкнути Bluetooth	Увімкнення/вимкнення Bluetooth

Менеджмент ПІМ

Активна синхронізація Exchange Active Sync

Налаштування облікового запису ActiveSync на кінцевому пристрої користувача

Назва облікового запису	Ім'я облікового запису електронної пошти
Ім'я хоста сервера	Адреса сервера/FQDN
Доменне ім'я	Домен сервера
Адреса електронної пошти	Адреса електронної пошти
Ім'я користувача	Ім'я користувача
Пароль користувача	За бажанням, ви вже можете прикріпити пароль до користувача тут
Використовуйте SSL	Використовуйте SSL-з'єднання
Інтервал синхронізації	Тут можна встановити інтервал синхронізації Ручна синхронізація = Користувач повинен завантажити свої електронні листи та виконати синхронізацію вручну
Фільтр віку пошти	Час, до якого потрібно синхронізувати імейли Без фільтра = необмежений
Рівень журналу	Налаштування рівнів журналювання для трафіку ActiveSync
Синхронізувати електронну пошту	Активовано = імейли синхронізовано
Синхронізація Контакти	Активовано = контакти синхронізовані
Синхронізація календаря	Активовано = календар синхронізовано
Завдання синхронізації	Активовано = завдання синхронізовано

Електронна пошта

Створення облікових записів POP3/IMAP4 на пристрої кінцевого користувача.

Опис рахунку	Ім'я облікового запису електронної пошти
Ім'я відправника	Відображене ім'я відправника
Доменне ім'я	Доменне ім'я для облікового запису електронної пошти
Адреса електронної пошти	Адреса електронної пошти користувача
Ім'я користувача	Ім'я користувача
Пароль користувача	За бажанням, ви вже можете прикріпити пароль до користувача тут
Альтернативні облікові дані вихідного сервера	Тут можна вказати, якщо для вихідного сервера потрібні інші облікові дані
Вихідне доменне ім'я	Вихідне доменне ім'я
Ім'я користувача вихідного сервера	Ім'я користувача вихідного сервера
Пароль вихідного сервера	Пароль вихідного сервера
Протокол електронної пошти	POP3 або IMAP4, можна використовувати як протокол
Ім'я хоста сервера вхідної пошти	Ім'я хоста сервера вхідної пошти
Використовуйте SSL для вхідної пошти	Використовуйте SSL для вхідних листів
Ім'я хоста сервера вихідної пошти	Ім'я хосту сервера вихідної пошти
Використовуйте SSL для вихідних повідомлень	Використовуйте SSL для вихідних листів
Автентифікація вихідного сервера	Потрібна автентифікація вихідного сервера
Інтервал синхронізації	Тут можна встановити інтервал синхронізації Ручна синхронізація = Користувач повинен завантажити свої електронні листи та виконати синхронізацію вручну
Фільтр віку пошти	Час, до якого потрібно синхронізувати імейли Без фільтра = необмежений

Керування додатками

Enterprise App Manager

Встановлені програми

Тут наведено список програм, які наразі встановлені на пристрої, що відображається.

Обов’язкові програми

Тут ви можете налаштувати список програм, які є обов'язковими для використання на пристрої.

Цей список буде перевірятися щоразу, коли пристрій підключається до MDM, і інсталюватиме всі програми з цього списку, які не були встановлені на пристрої, незалежно від того, чи було їх видалено, чи вони ніколи не встановлювалися раніше.

Ви можете завантажити власні програми Windows 10, а потім додати їх до цього списку або додати конфігурації Microsoft Office, які потрібно попередньо налаштувати в "Загальні налаштування" > "Керування програмами" > "Microsoft Office".

Обмеження системних додатків

Програми вхідних повідомлень
Дозволити будильники та годинник
Дозволити калькулятор
Дозволити камеру
Дозволити зв'язок зі службою підтримки
Увімкнути Cortana
Дозволити провідник файлів
Дозволити розпочати роботу
Дозволити грув-музику
Дозволити карти
Дозволити обмін повідомленнями
Дозволити Microsoft Edge
Дозволити фільми та телебачення
Дозволити гроші
Дозволити новини
Увімкнути OneDrive
Дозволити OneNote
Дозволити календар і пошту Outlook
Дозвольте людям
Дозволити телефон
Дозволити фото
Дозволити Powerpoint
Дозволити налаштування
Увімкнути Skype
Дозволити спорт
Дозволити зберігання
Увімкнути диктофон
Дозволити гаманець
Дозволити погоду

Увімкнути Windows Feedback Hub
Дозволити слово
Увімкнути Xbox

Налаштування сторінок
Дозволити облікові записи на робочому місці
Дозволити розширену інформацію
Дозволити Куточок додатків
Блокування та фільтрація дозволів
Дозволити колірний профіль
Увімкнути режим водіння
Дозволити електронну пошту та акаунти
Увімкнути еквалайзер
Дозволити клавіатуру
Дозволити панель навігації
Увімкнути режим мережевого літака
Дозволити спільний доступ до мережі Інтернет
Дозволити мережеві служби
Увімкнути мережевий Wi-Fi
Увімкнути Bluetooth системи ПК
Дозволити оцінку вашого пристрою
Дозволити відновлення оновлення
Дозволити спільний доступ
Дозволити запуск
Дозволити мову часу
Дозволити час Регіон
Дозволити екран блокування Windows за замовчуванням
Дозволити робочий або навчальний рахунок

Чорні та білі списки

У розділі "Чорні та білі списки" ви можете вибрати між режимом "Білий список" та режимом "Чорний список".

Білий список	На кінцевий пристрій користувача можна встановити лише додані до списку програми та сервіси. Якщо вони вже встановлені на пристрої кінцевого користувача, вони будуть активовані та налаштовані, щоб користувач міг їх запустити.
	Всі інші програми, які не додані до списку, не можуть бути встановлені на кінцевий пристрій користувача. Якщо вони вже встановлені на пристрої кінцевого користувача, їх буде деактивовано і встановлено так, що користувач не зможе їх запустити.
Чорний список	Додані до списку програми та сервіси не можуть бути встановлені на пристрої кінцевого користувача. Якщо вони вже встановлені на пристрої кінцевого користувача, їх буде деактивовано і налаштовано так, що користувач не зможе їх запустити.
	Всі інші програми, які не додані до списку, можуть бути встановлені на пристрої кінцевого користувача. Якщо вони вже встановлені на пристрої кінцевого користувача, вони будуть активовані та налаштовані, щоб користувач міг їх запустити.

За допомогою кнопок , ви можете додати додаткові програми або сервіси до поточного списку.

За допомогою кнопок , ви можете додати додаткові програми або сервіси до неактивного на даний момент списку.

Ви можете додати програму з "Магазину додатків Windows" або безпосередньо ввести "Ідентифікатор програми", щоб додати її до чорного або білого списку.

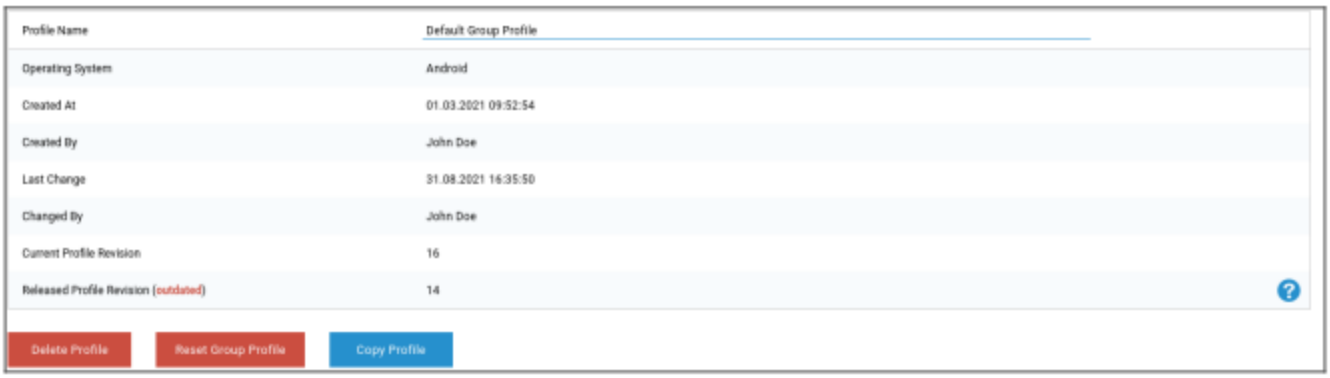
Конфігурація MacOS

Залежно від того, вибрали ви профіль або пристрій, відображення та його підпункти відрізняються - будь ласка, зверніть на це увагу!

Генерал

Огляд профілю групи (тільки на рівні групи)

Відкривши профіль групи, ви отримаєте короткий огляд профілю.



Ім'я профілю Ім'я профілю	Назва профілю (можна змінити тут)
Операційна система	Операційна система, для якої призначений профіль
Створено в	Час створення
Створено	Творець профілю
Остання зміна	Час останньої зміни профілю
Змінено	Обліковий запис, який вніс останні зміни
Поточна редакція профілю	Перегляд стану збереженого профілю
Випущено ревізію профілю	Призначена версія профілю ("Призначити зараз"). Якщо за текстом мітки вказано "(застаріла)", це означає, що ви зберегли профіль, але ще не призначили його, тому пристрої все одно отримають стару версію.

Огляд пристрою (тільки на рівні пристрою)

Короткий огляд пристрою.

Назва пристрою	Назва пристрою
Модель	Модель
Операційна система	Операційна система
Серійний номер	Серійний номер пристрою
Право власності на пристрій	Налаштований тип власності
Тип пристрою	Тип пристрою
Дотримується	Показує, чи відповідає пристрій вимогам
IP-адреса	IP-адреса, з якої пристрій підключився до сервера
Востаннє бачили	Час останнього з'єднання з пристроєм
Останній поштовх	Час останнього відправленого на пристрій поштовху
Завдання	Тут ви можете передати пристрій іншому користувачеві або групі

Ревізія конфігурації (лише на рівні пристрою)

Тут ви отримаєте огляд того, який профіль групи призначено пристрою.

Якщо ви натиснете на профіль групи, ви отримаєте доступ безпосередньо до профілю і зможете виконати налаштування.

За допомогою цього символу ви можете повернути призначені програми до налаштувань профілю групи.

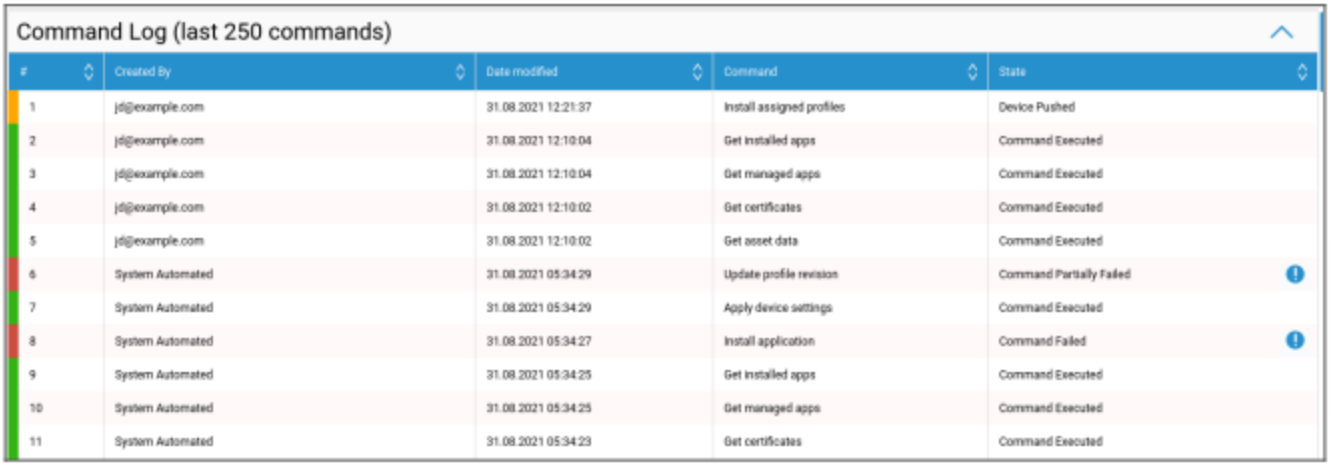
За допомогою цього символу ви можете скинути профіль пристрою, щоб він не мав жодних налаштувань.

"Доступна новіша версія" вказує на те, що профіль групи було змінено та збережено, але не призначено. Щоб застосувати зміни до пристроїв, профіль групи потрібно призначити за допомогою "Призначити зараз" на рівні групи.

Журнал пристрою (тільки на рівні пристрою)

Командний журнал

Тут ви можете побачити, які команди були видані для пристрою і який їхній статус.



Команди, створені за допомогою "Автоматизації системи", автоматично створюються системою.

Можливі стани команди

Пристрій натиснуто	До служби push (наприклад, APNS) було надіслано push-запит, щоб повідомити пристрій про необхідність з'єднатися з сервером EMM.
Команду створено	Команда була створена в системі.
Команду відправлено.	Команда була надіслана на пристрій після того, як він підключився до сервера.
Команду виконано	Команда була успішно виконана.
Команда не спрацювала	Команда не спрацювала. *
Команда частково не виконана	Залежно від операційної системи пристрою деякі команди можуть бути згруповані разом. У цьому деякі частини цієї командної групи зазнали невдачі. *
Команда виконана, але зрештою не спрацювала	Команда була виконана, але, можливо, не була.
Команда "Відсіч	Команду було перевиконано користувачем.
Викинуто	Команду було відкинуто. Наприклад, її було замінено іншою командою або пристрій було перереєстровано, а старі команди видалено

*Якщо за повідомленням стоїть знак оклику, ви можете отримати додаткову інформацію, навівши курсор на іконку.

Управління активами (тільки на рівні пристрою)

Інформація про пристрій

Номер моделі	Номер моделі
Ім'я хоста	Ім'я хоста
Локальне ім'я хоста	Локальне ім'я хоста
Операційна система	Операційна система
Версія ОС	Версія операційної системи
UDID	UDID
Вільна / загальна пам'ять	Вільна / загальна пам'ять

WiFi

IP-адреса	IP-адреса
MAC-адреса WiFi	MAC-адреса WiFi

Стільниковий зв’язок

Номер телефону	Номер телефону
Статус роумінгу	Статус роумінгу
Роумінг (голосовий зв'язок / передача даних)	Роумінг (голосовий зв'язок / передача даних)
IP-адреса	IP-адреса
Оператор/перевізник	Оператор/перевізник
Мережа оператора SIM-карти	Мережа операторів
Версія для носія	Версія для носія
ICCID	ICCID
Поточний ГХК/МНК	Поточний ГХК/МНК
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

MAC-адреса Bluetooth	MAC-адреса Bluetooth

Керування оновленнями (лише на рівні пристрою)

Інформація про оновлення

На цій вкладці відображається інформація про налаштування оновлення системи на пристрої.

Увімкнено автоперевірку	Якщо система перевіряє наявність оновлень автоматично.
Автоматичне оновлення програми увімкнено	Якщо система буде встановлювати оновлення програми автоматично.
Увімкнено автоматичне оновлення ОС	Якщо система встановить оновлення ОС автоматично.
Увімкнено автоматичні оновлення безпеки	Якщо система встановить оновлення безпеки автоматично.
Ввімкнено фонове завантаження оновлення програми	Якщо система буде завантажувати оновлення програми у фоновому режимі.
URL-адреса каталогу	URL-адреса каталогу оновлень програмного забезпечення, який використовує клієнт.
Каталог за замовчуванням	Якщо "так", Catalog буде каталогом за замовчуванням.
Виконуйте періодичну перевірку	Якщо "так", почніть нове сканування.
Дата попереднього сканування	Дата останньої перевірки на наявність оновлень програмного забезпечення.
Попередній результат сканування	Код результату останньої перевірки на наявність оновлень програмного забезпечення.

Управління безпекою

Захист від крадіжок

Wipe & Lock

Повне витирання	Надіслати команду для скидання пристрою до заводських налаштувань
Enterprise Wipe	Вийміть MDM з пристрою та видаліть усі дані MDM (наприклад, облікові записи, програми)
Екран блокування	Змусьте пристрій повернутися до екрана блокування

Конфігурація безпеки

Пароль

Деактивація коду дозволена	Визначає, чи буде користувач змушений вводити PIN-код. Просте встановлення цього значення (а не інших) змушує користувача вводити пароль, не обмежуючи його довжину або якість.
Дозволити просте значення	Дозвольте користувачеві використовувати однакові, зростаючі та спадаючі рядки чисел (наприклад, 1234, 1111)
Потрібне буквено-цифрове значення	Паролі повинні містити принаймні одну літеру
Мінімальна довжина пароля	Мінімальна довжина пароля
Мінімальна кількість складних символів	Мінімальна кількість алфавітно-цифрових символів у паролі
Максимальний вік пароля	Кількість днів, після закінчення яких необхідно змінити пароль
Максимальне автоматичне блокування	Максимальний час, після якого пристрій буде заблоковано
Максимальний пільговий період для блокування пристрою	Час, протягом якого пристрій може бути заблоковано без запиту пароля для розблокування
Максимальний вік паролю (1-730 днів, або жодного)	Дні, після яких необхідно змінити пароль
Історія паролів (1-50 паролів або жодного)	Кількість унікальних паролів перед повторним використанням

Сертифікат

PKCS#1	
Опис	Введіть опис для сертифіката
Облікові дані	Завантажити файл pkcs1

PKCS#12	
Опис	Введіть опис для сертифіката
Облікові дані	Завантажити файл pkcs12

Налаштування обмежень

Функціональність пристрою

Дозволити камеру	Дозвольте використовувати камеру
Увімкнути ігровий центр	Якщо значення хибне, ігровий центр вимкнено, а його піктограму прибрано з головного екрана.
Дозволити багатокористувацьку гру	Якщо значення false, забороняє багатокористувацьку гру.
Дозволити додавання друзів Game Center	Якщо неправда, забороняє додавання друзів до Game Center.
Увімкнути фототеку iCloud	Якщо встановлено значення false, вимикає медіатеку iCloud. Усі фотографії, не повністю викачані з медіатеки iCloud на пристрій, буде вилучено з локального сховища.
Дозволити Touch ID	Якщо значення false, забороняє розблокування пристрою за допомогою Touch ID.

iCloud

Блокування певних функцій під час створення пари з iCloud

Дозволити синхронізацію документів	Дозволити синхронізацію документів
Увімкнути синхронізацію брелока iCloud	Увімкнути синхронізацію брелока iCloud
Дозволити нотатки в iCloud	Якщо значення false, вимикає служби MacOS iCloud Notes
Дозволити iCloud BTMM	Якщо значення false, вимикає службу MacOS Back to My Mac iCloud.
Дозволити iCloud FMM	Якщо значення false, вимикає службу MacOS Find My Mac iCloud.
Дозволити закладки iCloud	Якщо значення false, вимикає синхронізацію закладок iCloud у MacOS.
Увімкнути пошту iCloud	Якщо значення false, вимикає служби MacOS Mail та iCloud.
Увімкнути календар iCloud	Якщо значення false, вимикає сервіси MacOS Cloud iCloud.
Увімкнути нагадування в iCloud	Якщо значення хибне, вимикає служби нагадувань iCloud.

Увімкнути адресну книгу iCloud	Якщо значення false, вимикає служби адресної книги MacOS iCloud Address Book.

Медіа-менеджмент

Видалити при виході з системи	Вийміть усі знімні носії під час виходу з системи
Дозволити мережу	Дозволити доступ для мережевих носіїв
Дозволити внутрішній диск	Дозволити доступ до внутрішнього диска.
Вимагати автентифікації	Вимагати автентифікацію для використання цього носія
Тільки для читання	Користувач може лише зчитувати дані з носія
Дозволити зовнішній диск	Дозволити доступ до зовнішнього диска.
Вимагати автентифікації	Вимагати автентифікацію для використання цього носія
Тільки для читання	Користувач може лише зчитувати дані з носія
Дозволити використання образів дисків	Дозволити доступ для зображень.
Вимагати автентифікації	Вимагати автентифікацію для використання цього носія
Тільки для читання	Користувач може лише зчитувати дані з носія
Дозволити використання DVD-RAM	Дозволити доступ для диска DVD-RAM.
Вимагати автентифікації	Вимагати автентифікацію для використання цього носія
Тільки для читання	Користувач може лише зчитувати дані з носія
Дозволити використання DVD-дисків	Дозволити доступ для DVD-диска.
Вимагати автентифікації	Вимагати автентифікацію для використання цього носія
Дозволити використання компакт-дисків	Дозвольте доступ для CD-диска.
Вимагати автентифікації	Вимагати автентифікацію для використання цього носія

Керування з’єднаннями

Wi-Fi

Тут ви можете додавати та налаштовувати Wi-Fi з'єднання

Ідентифікатор набору послуг (SSID)	SSID мережі, до якої буде встановлено з'єднання
Автоматичне приєднання	Увімкнути автоматичне приєднання до мережі
Прихована мережа	Увімкнути, якщо точка доступу не транслює SSID
Налаштування проксі-сервера	Налаштування проксі для кожної точки доступу
Ні.	Не використовуйте проксі-сервер
Посібник	Налаштуйте проксі вручну
URL-адреса проксі-сервера	Адреса для доступу до налаштувань проксі-сервера
Порт	Встановіть порт для проксі-сервера
Аутентифікація	Ім'я користувача для автентифікації на проксі
Пароль	Пароль для автентифікації на проксі
Автоматично	Автоматичне створення проксі-сервера
URL-адреса проксі-сервера	URL-адреса файлу налаштувань проксі-сервера
Тип безпеки	Встановіть тип безпеки для точки доступу
WEP	
Пароль	Пароль для точки доступу
WPA/WPA2	
Пароль	Пароль для точки доступу
WEP Enterprise - WPA/ WPA2 Enterprise / Будь-яке підприємство	Див. помилку в таблиці: Джерело посилання не знайдено нижче

Ні.	Не встановлюйте жодних заходів безпеки
Вимкнути рандомізацію MAC-адрес	Вимикає рандомізацію MAC-адрес для цієї мережі Wi-Fi під час підключення до неї. Це також показує попередження про конфіденційність у Налаштуваннях, яке вказує на те, що мережа має знижений рівень захисту конфіденційності.

Конфігурація Wi-Fi на підприємстві

Примітка: Доступно лише тоді, коли для параметра "Тип безпеки" встановлено значення "Тип підприємства".

Протоколи	Протокол автентифікації, що підтримується в цільовій мережі
TLS	Увімкнути / вимкнути використання
TTLS	Увімкнути / вимкнути використання
Внутрішні автентифікації	Протокол автентифікації, який слід використовувати: PAP, CHAP, MSCHAP, MSCHAPv2
ПІК!	Увімкнути / вимкнути використання
PEAP	Увімкнути / вимкнути використання
EAP-FAST	Увімкнути / вимкнути використання
EAP-SIM	Увімкнути / вимкнути використання
Використовуйте PAC	Використання PAC (захищений контроль доступу)
Положення PAC	Конфігурація Provision PAC
Надання PAC Анонімно	Анонімне надання ГРД
Аутентифікація	
Ім'я користувача	Ім'я користувача для аутентифікації
Не використовуйте За кожне з'єднання Пароль	Не використовуйте пароль для кожного з'єднання
Пароль	Пароль для використання
Посвідчення особи	Завантаження/вибір сертифіката автентифікації
Зовнішня ідентичність	Ідентичність, яку можна побачити ззовні
Довіра	

Довірений сертифікат 1	Завантажте перший довірений сертифікат
Довірений сертифікат 2	Завантажте другий довірений сертифікат
Сертифікат довіри 3	Завантажте третій довірений сертифікат
Довірений сервер Назви сертифікатів	Назви очікуваних сертифікатів сервера (у списку через кому)

VPN

Залежно від обраного типу з'єднання можуть відображатися різні поля.

Ім'я з'єднання Ім'я з'єднання	Назва VPN-профілю
Тип VPN	
VPN	Весь мережевий трафік пристрою буде маршрутизуватися через VPN-з'єднання.
Тип підключення	Встановити тип VPN-з'єднання
IPsec (cisco)	Протокол IPsec від cisco
L2TP	Протокол L2TP
Спеціальний SSL	Підключення через спеціальний SSL
IKEv2	Протокол IKEv2
Налаштування проксі-сервера	Налаштування проксі для VPN-з'єднання
Ні.	Не створювати проксі-сервер
Посібник	Встановлення проксі вручну
URL-адреса проксі-сервера	Адреса для доступу до налаштувань проксі-сервера
Порт	Встановіть порт для проксі-сервера
Аутентифікація	Ім'я користувача для автентифікації на проксі
Пароль	Пароль для автентифікації на проксі
Автоматично	Автоматичне створення проксі-сервера
URL-адреса проксі-сервера	URL для доступу до налаштувань проксі-сервера

HTTP-проксі-сервер

Тип проксі	
Посібник	Створіть проксі вручну
URL-адреса проксі-сервера	Адреса для доступу до налаштувань проксі-сервера
Порт	Встановіть проксі-порт
Аутентифікація	Ім'я користувача для автентифікації на проксі
Пароль	Пароль для автентифікації на проксі
Автоматично	Автоматичне створення проксі-сервера
URL-адреса проксі-сервера PAC	URL-адреса проксі-сервера PAC
Дозволити пряме з'єднання, якщо PAC недоступний	Дозволити пряме підключення (без VPN), якщо PAC недоступний
Дозволити обхід проксі для доступу до кептивних мереж	Дозволити обхід проксі для доступу до внутрішніх мереж

AirPrint

IP-адреса	IP-адреса принтера
Шлях до ресурсів	Визначений шлях до пристрою AirPrint

AirPlay

Назва пристрою	Назва пристрою
Пароль	Пароль для створення пари
Білий список	Визначте список пристроїв, з якими пристрій може сполучатися виключно самостійно

Менеджмент ПІМ

Активна синхронізація Exchange Active Sync

Назва облікового запису	Назва рахунку.
Адреса електронної пошти	Адреса облікового запису (наприклад, max@company.com)
Ім'я хосту сервера	Внутрішнє ім'я хоста
Ім'я користувача Ім'я користувача	"Домен" та "Ім'я користувача" повинні бути порожніми, щоб пристрій запитав користувача.
Домен	"Домен" та "Ім'я користувача" повинні бути порожніми, щоб пристрій запитав користувача. Якщо конфігурація шлюзу ACL включена і поле Домен не порожнє, універсальний шлюз AppTec360 буде аутентифікувати пристрій з наступним ім'ям "Домен\Ім'я для входу"
Пароль	Пароль для облікового запису (наприклад, secretUserPassword)
Синхронізація пошти за минулі дні	Кількість останніх днів, за які потрібно синхронізувати пошту
Використовуйте SSL	Використання SSL для внутрішнього хоста обміну
Розширена опція	Показати додаткові параметри
Порт сервера	Внутрішній порт
Шлях до сервера	Внутрішній шлях
Зовнішнє ім'я хоста	Зовнішній хост
Зовнішній порт	Зовнішній порт
Зовнішній шлях	Зовнішній шлях
Використовуйте SSL для зовнішніх Хост обміну	Використання SSL для зовнішнього хоста обміну

Електронна пошта

Налаштування облікових записів POP3 / IMAP на пристрої кінцевого користувача

Опис рахунку	Ім'я облікового запису електронної пошти
Тип рахунку	
IMAP	
Префікс шляху	Префікс шляху для спеціальних папок
POP	
Ім'я користувача	Ім'я користувача
Адреса електронної пошти	Адреса електронної пошти користувача

Вхідна пошта	Вхідні налаштування сервера
Адреса поштового сервера	Адреса поштового сервера
Порт поштового сервера	Порт поштового сервера
Ім'я користувача	Відповідне ім'я користувача
Тип автентифікації	Тип автентифікації
Ні.	Немає типу автентифікації
Пароль (тільки на рівні пристрою)	Запит на введення пароля
Виклик-відповідь МДМ	
NTLM	NTLM-автентифікація
Дайджест HTTP MD5	
Використовуйте SSL	Використовуйте SSL, якщо потрібно

Вихідна пошта	Налаштування вихідного сервера
Адреса поштового сервера	Адреса поштового сервера
Порт поштового сервера	Порт поштового сервера
Ім'я користувача	Відповідне ім'я користувача
Тип автентифікації	
Ні.	Немає методу автентифікації
Пароль (тільки на рівні пристрою)	Запит на введення пароля
Виклик-відповідь МДМ	
NTLM	NTLM-автентифікація
Дайджест HTTP MD5	
Використовуйте SSL	Використовуйте SSL, якщо потрібно
Вихідний пароль такий самий, як і вхідний	Вихідний пароль такий самий, як і вхідний
Використовуйте тільки в пошті	Активуйте, якщо всі вихідні імейли мають надсилатися через Mail-App

CalDav

Налаштування створення та розповсюдження облікового запису CalDav

Опис рахунку	Відображення назви облікового запису
Ім'я хоста	Ім'я хоста та/або IP-адреса
Порт	Порт облікового запису CalDav
Основна URL-адреса	Основна URL-адреса облікового запису
Ім'я користувача	Відповідне ім'я користувача CalDav
Пароль (тільки на рівні пристрою)	Відповідний пароль CalDav
Використовуйте SSL	Використовуйте SSL, якщо потрібно

CardDav

Налаштування створення та розповсюдження облікового запису CardDav

Опис рахунку	Відображення назви облікового запису
Ім'я хоста	Ім'я хоста та/або IP-адреса
Порт	Порт облікового запису CardDav
Основна URL-адреса	Основна URL-адреса облікового запису
Ім'я користувача	Відповідне ім'я користувача CardDav
Пароль (тільки на рівні пристрою)	Відповідний пароль CardDav
Використовуйте SSL	Використовуйте SSL, якщо потрібно

LDAP

У цій області налаштуйте LDAP-з'єднання, щоб дозволити динамічний обмін сертифікатами між пристроєм кінцевого користувача та Active Directory.

Зверніть увагу, що обраному користувачеві потрібен відповідний дозвіл на читання.

Опис рахунку	Опис рахунку
Ім'я користувача облікового запису	Користувач для LDAP-доступу
Пароль облікового запису	Пароль для LDAP-доступу
Ім'я хоста облікового запису	Ім'я хоста/IP-адреса сервера LDAP
Використовуйте SSL	Використовуйте SSL, якщо потрібно

У другій частині ви можете задати індивідуальні фільтри для пошуку в реєстрі LDAP.

Опис	Сфера застосування	База пошуку
Опис фільтра	Рівень пошуку в реєстрі LDAP	Визначте індивідуальний фільтр

Інформаційна панель та звітність

Налаштування інформаційної панелі

Тут ви можете побачити, які дашборди існують, редагувати їх або створювати нові. Кожна дашборд має свій власний набір даних для відображення та графічної конфігурації.

Керування налаштуваннями інформаційної панелі

Громадськість	Робить Дэшборд публічним, щоб інші користувачі могли його бачити. Звичайно, користувачі повинні мати можливість увійти і переглядати дашборди. Якщо опція "Публічний" не активована, її може бачити лише автор.
За замовчуванням	Встановлює Панель за замовчуванням, щоб вона автоматично відкривалася наступного разу, коли ви звертаєтеся до подання Панелі керування.
	Показати Панель моніторингу та її графіки
	Видалити інформаційну панель
	Редагування назви та налаштувань інформаційної панелі
	Зробіть копію Dashboard
	Додайте абсолютно нову інформаційну панель

Вигляд інформаційної панелі

Тут відображаються дані та графіки вибраної інформаційної панелі, а також ви можете їх змінити.

Керування на панелі приладів

	Дозволяє визначити, які дані відображатимуться на Панелі моніторингу, кількість даних, що відображатимуться, та розмір цих даних.
	Повертає вас до огляду інформаційної панелі
	Повертає поточну відкриту інформаційну панель до значень за замовчуванням
	Зберігає всі зміни, які ви внесли до поточної відкритої Панелі моніторингу (наприклад, які дані показувати)
	Змінити тип діаграми на стовпчасту
	Змінити тип діаграми на кругову діаграму
	Змінити тип діаграми на кругову діаграму
	Змінити тип діаграми на діаграму полярних областей
	Змінити порядок сортування

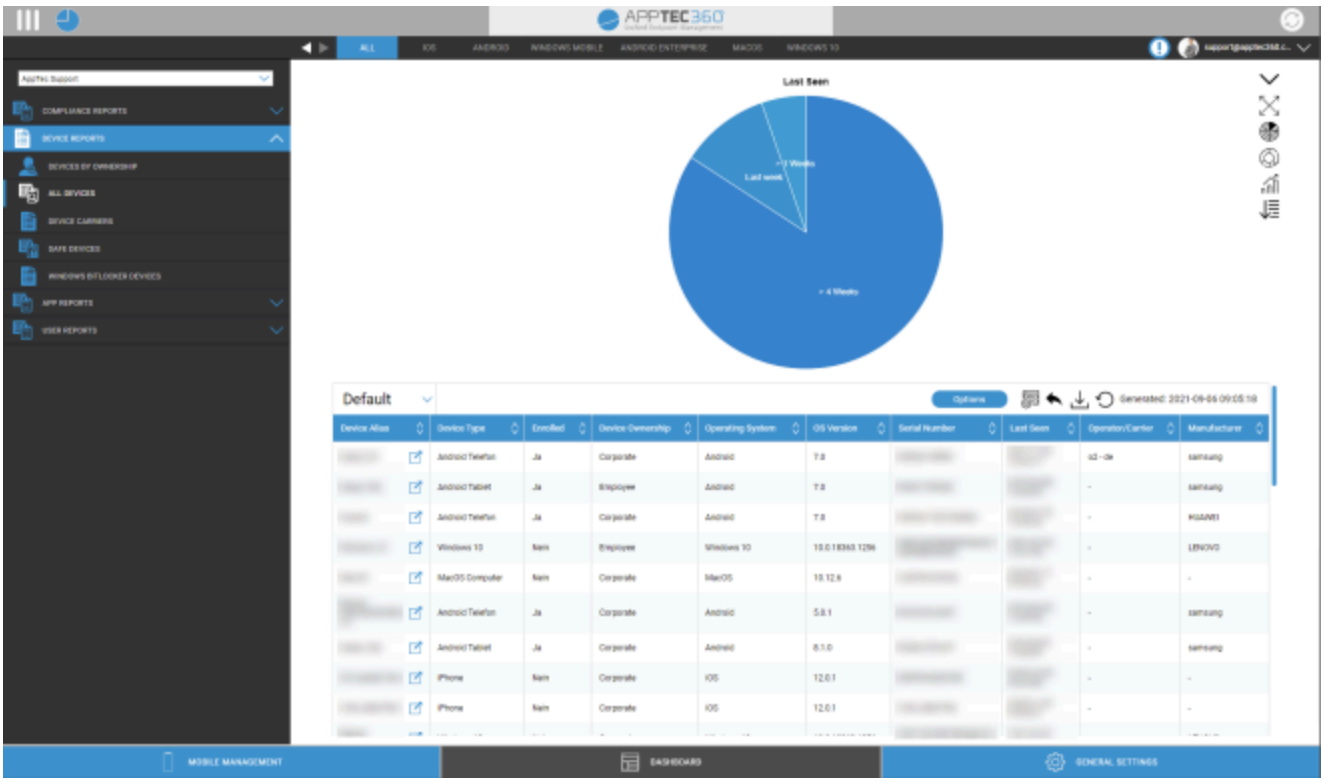
Розширена звітність

"Розширені звіти" пропонують детальні огляди та графіки інформації про пристрої та користувачів.

Існує кілька стандартних звітів, але всі вони можуть бути змінені вручну, щоб додати або видалити дані для відображення.

Зверніть увагу, що ви можете лише вручну змінити дані, які будуть показані. Вибрана категорія звіту визначає дані, на яких він базується. Наприклад, ви ніколи не зможете побачити пристрої Android у звіті для iOS у розділі Звіти про пристрої Всі пристрої iOS

У верхньому лівому кутку ви можете обмежити дані звіту певною групою (і всіма її підгрупами). За замовчуванням цей параметр встановлено для вашого кореневого вузла, тому він враховує ВСІ пристрої та користувачів.



Розширений контроль звітності

У кожному огляді ви можете використовувати наступні функції, щоб змінити звіт у будь-який спосіб:

	Приховати діаграму (якщо діаграма відображається)
	Показати графік (якщо графік приховано)
	Розгорнути діаграму (якщо діаграма згорнута)
	Згорнути діаграму (якщо діаграма розгорнута)
	Змінити тип діаграми на стовпчасту
	Змінити тип діаграми на кругову діаграму
	Змінити тип діаграми на кругову діаграму
	Змінити тип діаграми на діаграму полярних областей
	Змінити порядок сортування
	Змініть наступні частини огляду, що відображаються на екрані: • Додавання/видалення стовпців • Вкажіть порядок відображення стовпців • Показати/приховати діаграму над таблицею • Виберіть стовпець, який використовується для діаграми • Фільтруйте дані вашої таблиці
	Відкрийте менеджер налаштувань, щоб зберегти та завантажити різні звіти
	Скидає поточний відкритий звіт до значення за замовчуванням
	Експортуйте поточний звіт у файл .csv
	Регенеруйте дані та перезавантажте поточний звіт

На наступних сторінках ви знайдете список усіх звітів за замовчуванням.

Звіти про комплаєнс

Вкорінені пристрої

Огляд пристроїв, які були рутовані / зламані.

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта
Операційна система
Номер телефону
Востаннє бачили
Виробник

Пристрої в роумінгу

Огляд усіх пристроїв, які перебувають у роумінгу

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта
Тип пристрою
Операційна система
Номер телефону
Востаннє бачили

Пристрої з підтримкою роумінгу

Огляд усіх пристроїв, які активували роумінг, але не обов'язково перебувають у роумінгу.

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта
Тип пристрою
Операційна система
Номер телефону
Востаннє бачили

Пристрої під наглядом

Огляд усіх пристроїв, які перебувають під наглядом у режимі нагляду (лише для iOS)

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта
Тип пристрою
Востаннє бачили

Неактивні пристрої

Огляд усіх пристроїв, які не підключалися до сервера за останні 7 днів

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта
Тип пристрою
Операційна система
Востаннє бачили

Звіти про пристрої

Пристрої за формами власності

Тут ви можете побачити, скільки пристроїв наразі розгорнуто як корпоративні (корпоративні пристрої) та особисті (особисті пристрої).

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Тип пристрою
Право власності на пристрій
Операційна система

Всі пристрої

Тут ви можете побачити огляд усіх пристроїв з найважливішою інформацією.

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Тип пристрою
Зараховано.
Право власності на пристрій
Операційна система
Версія ОС
Серійний номер
Востаннє бачили
Оператор/перевізник
Виробник

Носії пристроїв

Тут ви можете побачити огляд щодо оператора (стільникового провайдера).

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта
Операційна система
Версія ОС
Оператор/перевізник

БЕЗПЕЧНІ ПРИСТРОЇ

Тут ви можете побачити огляд того, які пристрої використовують SAFE Version.

Оскільки огляд та/або SAFE доступні лише для пристроїв Samsung, ви не побачите звичних вкладок під цим пунктом.

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта
Тип пристрою
Востаннє бачили
Безпечна версія

Пристрої Windows BitLocker

Тут ви можете переглянути огляд пристроїв Windows, які використовують BitLocker.

Стовпці за замовчуванням у цьому звіті:

Псевдонім пристрою
Власник пристрою
Електронна пошта

Стан BitLocker

Звіти про додатки

Тут ви отримуєте різноманітні огляди щодо програм. У всіх цих звітах ви можете натиснути на запис, щоб побачити, які версії встановлені на пристроях і як часто. У цьому поданні ви можете знову натиснути на певну версію, щоб побачити, на яких пристроях встановлено цю версію.

Примітка: Може знадобитися деякий час, поки система отримає актуальну інформацію від пристрою. Крім того, звіти не оновлюються щохвилини. Можливо, вам доведеться набратися терпіння, щоб побачити поточний стан, якщо ви щойно призначили нову програму або версію. Перезавантаження звіту вручну змусить його відображати найсвіжіші доступні дані

Встановлені програми

Тут ви отримаєте огляд усіх встановлених програм.

Стовпці за замовчуванням у цьому звіті:

Ім'я	Назва відповідного додатку та/або сервісу
Ідентифікатор	Визначений ідентифікатор програми/сервісу
Загальна кількість	Як часто цей додаток/сервіс був встановлений на пристроях кінцевих користувачів

Найбільше встановлених програм

Тут ви отримаєте огляд додатків, які були встановлені найчастіше.

Стовпці за замовчуванням у цьому звіті:

Ім'я	Назва відповідного додатку та/або сервісу
Ідентифікатор	Визначений ідентифікатор програми/сервісу
Загальна кількість	Як часто цей додаток/сервіс був встановлений на пристроях кінцевих користувачів

Обов’язкові програми

Тут ви знайдете огляд обов'язкових (mandatory required) додатків.

Стовпці за замовчуванням у цьому звіті:

Ім'я	Назва відповідного додатку та/або сервісу
Ідентифікатор	Визначений ідентифікатор програми/сервісу
Джерело програми	Який AppStore бере участь: • Google PlayStore (Android) • iTunes AppStore (iOS)
ОС	Операційна система

Додатки в чорному списку

Тут ви отримаєте огляд усіх визначених програм з чорного списку.

Стовпці за замовчуванням у цьому звіті:

Ім'я	Назва відповідного додатку та/або сервісу
Ідентифікатор	Визначений ідентифікатор програми/сервісу
Джерело програми	Який AppStore бере участь: • Google PlayStore (Android) • iTunes AppStore (iOS)
ОС	Операційна система

Звіти користувачів

Тариф

Тут ви отримаєте огляд телефонних тарифів і SIM-карт ваших користувачів.

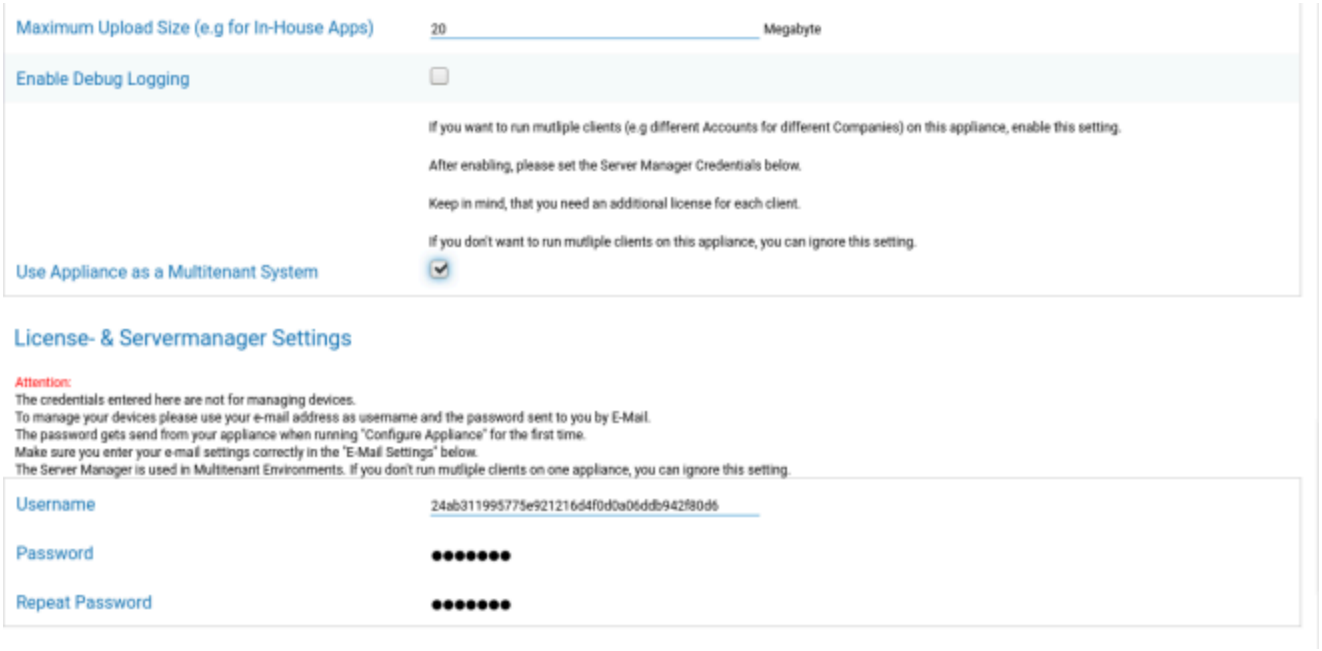
Стовпці за замовчуванням у цьому звіті:

Електронна пошта
Ім'я
номер телефону
перевізник
тариф
варіант
ціна
контрактСкасовано
contractStart
duringTime
мобільний зв'язок та дані
dataVolume
multiSIM
тип
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
примітка

Управління декількома орендарями

AppTec360 EMM може приймати кілька окремих орендарів, кожен з яких має власних користувачів і групи, дозволи та глобальні налаштування.

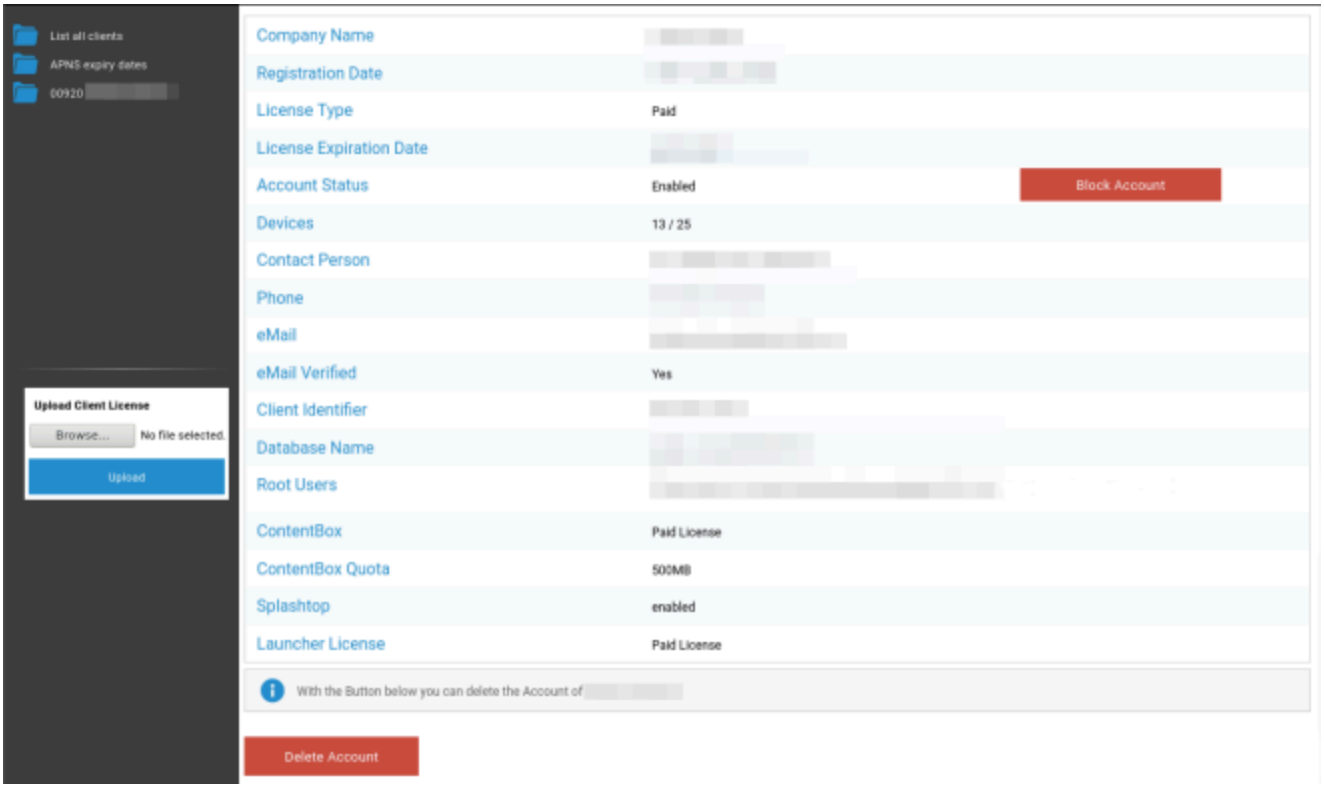
Щоб увімкнути багатокористувацькі можливості, вам потрібно увімкнути їх в інтерфейсі конфігурації Пристрою в розділі "Крок третій - Налаштування сервера".



У новому меню встановіть ім'я користувача та пароль для Servermanager. Збережіть налаштування і запустіть "Налаштувати пристрій" у розділі "Крок п'ятий - Ліцензійна угода", щоб застосувати налаштування.

Коли налаштування завершено, ви можете увійти за допомогою встановлених облікових даних через звичайний інтерфейс мобільного управління.

Після входу ви побачите наступний вигляд.



Зліва ви можете побачити всіх орендарів (в даному випадку тільки одного з ідентифікатором 920), а праворуч - інформацію про цього клієнта. У вас також є можливість заблокувати доступ до облікового запису, а також видалити клієнта (УВАГА: при цьому будуть видалені всі дані, пов'язані з цим клієнтом).

Зліва ви можете завантажити нову ліцензію клієнта, яка може бути як оновленням ліцензії для існуючого клієнта, так і новою ліцензією, яка автоматично створює нового клієнта. При створенні нового клієнта на адресу електронної пошти, на яку було видано ліцензію, автоматично надсилається лист, що містить логін і пароль для входу в систему.

Щоб отримати нову або оновлену клієнтську ліцензію (наприклад, якщо вам потрібна більша кількість ліцензій на пристрої), зверніться до свого торгового представника.

Додаткові види

Перерахувати всіх клієнтів

Показує огляд всіх клієнтів в системі.

Ідентифікатор клієнта	Ідентифікатор клієнта
Ідентифікатор	Ідентифікатор клієнта
База даних	База даних
Назва компанії	Назва компанії
Електронна пошта	Контактна особа електронна пошта
Перевірено	Чи перевірено електронну пошту контактних осіб
Країна	Країна
Пристрої	Кількість зареєстрованих пристроїв
Дата реєстрації	Момент передачі ліцензії
Останній вхід	Останній вхід в обліковий запис адміністратора
Ліцензія	Відображення типу ліцензії (Безкоштовна|Платна)
Ліцензія ЦБ	Тип ліцензії ContentBox (безкоштовна|платна)
Статус	Поточний статус AppTec-клієнта
Закінчився	Відображається, якщо термін дії ліцензії закінчився
iOS	Кількість пристроїв iOS
Android	Кількість пристроїв Android
Windows Mobile	Кількість пристроїв Windows Mobile
MacOS	Кількість пристроїв MacOS
Windows 10	Кількість пристроїв з Windows 10
Android Enterprise	Кількість корпоративних пристроїв Android
IOS BYOD (реєстрація користувачів)	Кількість пристроїв IOS BYOD (реєстрація користувачів)
IoT	Кількість пристроїв Інтернету речей

Терміни дії APNS

Відображає огляд всіх дат закінчення терміну дії сертифікатів APNS для всіх клієнтів.

Ідентифікатор клієнта	Ідентифікатор клієнта
Назва компанії	Назва компанії
Дата закінчення терміну дії	Термін дії APNS-сертифікату Apple
Інформація	Інформація про закінчення терміну придатності

Контакти

Виникли додаткові запитання? Просто зв'яжіться з нами за посиланням:

Для загальних технічних питань

support@apptec360.com

+41 61 511 3210

З питань, пов’язаних з установкою віртуального приладу

consulting@apptec360.com

+41 61 511 3214

Відмова від відповідальності