AppTec360 Enterprise Mobile Manager & ContentBox

Руководство по администрированию | Версия 5.0 (202110)

Оглавление

- Очистить код доступа
- Устройство блокировки
- Устройство выключения
- Перезагрузка устройства
- Сигнализация и режим Lostmode | Отключить режим Lostmode
- Удалить устройство
- Стирание устройства
- Enterprise Wipe | Remove MDM
- Отправить сообщение
- Удаленное управление TeamViewer
- Отправить запрос на зачисление

Android

- Редактировать устройство
- Очистить код доступа
- Устройство блокировки
- Удалить устройство
- Стирание устройства
- Удалите MDM
- Отправить сообщение
- Переход в режим COPE
- Отправить запрос на зачисление
- Перенос устаревшего устройства

Windows

- Редактировать устройство
- Удалить устройство
- Enterprise Wipe | Remove MDM
- Удаленное управление TeamViewer
- Отправить запрос на зачисление

Управление контентом

- Групповые файлы
- Проводник файлов
- Аудиторский журнал
- Мусор
- Внешнее хранилище

Журнал аудита

Конфигурация iOS

Общие сведения

- Обзор профиля группы (только на уровне группы)
- Общая информация
- Настройки
- Пересмотр конфигурации
- Журнал устройства (только на уровне устройства)
  - Журнал команд
  - Возможные статусы команд

Управление активами (только на уровне устройств)

- Управление активами (только на уровне устройств)
  - Информация об устройстве
  - Wi-Fi
  - Клетчатка
  - Bluetooth

Управление безопасностью

- Защита от кражи (только на уровне устройства)
  - Информация GPS (только на уровне устройства)
  - Wipe & Lock (только на уровне устройства)
  - Сообщение (только на уровне устройства)
- Конфигурация безопасности
  - Пасскод
  - Сертификат (только на уровне устройства)
  - Шифрование
  - Единый вход в систему
- Окончание срока службы (только на уровне устройства)
  - Стирание (только на уровне устройства)
- Настройки ограничений
  - Функциональность устройства
  - iCloud
  - Безопасность и конфиденциальность

BYOD

- Встроенная система безопасности iOS (контейнер)
  - Активация

- Пароль SecurePIM
- SecurePIM Безопасность
- SecurePIM Browser
- Обмен

Управление соединениями

- Wi-Fi
  - Настройка прокси
  - Тип безопасности
- VPN
  - Тип VPN
    - VPN
    - VPN для каждого приложения
  - Настройка прокси
- APN
- Клетчатка
- HTTP-прокси
- AirPrint
- AirPlay

Управление PIM

- Exchange Active Sync
- eMail
  - Входящая почта
  - Исходящая почта
- CalDav
- Календари с подпиской
- LDAP

Веб-менеджмент

- Webclips
- Фильтр веб-контента

Управление приложениями

- Enterprise App Manager
  - Установленные приложения (только на уровне устройства)
  - Обязательные приложения
    - Опции установки

- Веб-приложения
- Ограничения и настройки
  - Приложения в черном списке / в белом списке
  - Ограничения SysApp
  - App-VPN
  - Настройки приложения
- Магазин приложений для предприятий
  - Приложения iTunes
  - In-House
- Режим киоска
  - Тип применения
    - Пакет
    - URL
  - Настройки режима киоска

Android Enterprise — полностью управляемая конфигурация устройств

Общие сведения

- Обзор профиля группы (только на уровне группы)
- Обзор устройства (только на уровне устройства)
- Пересмотр конфигурации (только на уровне устройства)
- Журнал устройства (только на уровне устройства)
  - Журнал команд
  - Возможные статусы команд
- Настройки устройства
  - Конфигурация клиента
  - Обои

Управление активами (только на уровне устройств)

- Информация об устройстве
  - Wi-Fi
- Клетчатка
- Bluetooth

Управление безопасностью

- Защита от кражи (только на уровне устройства)
  - Информация GPS (только на уровне устройства)

- Wipe & Lock (только на уровне устройства)
- Сообщение (только на уровне устройства)
- Конфигурация безопасности
  - Пасскод устройства
  - Антивирус
- Окончание срока службы (только на уровне устройства)
  - Стирание (только на уровне устройства)
- Настройки ограничений
  - Ограничения
- Управление сертификатами

Управление соединениями

- Wifi
  - Тип безопасности
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Тип VPN
    - VPN
    - VPN для каждого приложения
- Ограничения

Управление PIM

- Gmail Exchange

Управление приложениями

- Enterprise App Manager
  - Установленные приложения (только на уровне устройства)
  - Системные приложения (только на уровне устройства)
  - Обязательные приложения
  - Черные и белые списки
  - Системные приложения AE
- Ограничения и настройки
  - Настройки управления приложениями
- Магазин приложений для предприятий
  - In-House
- Enterprise Play Store

- Настройки устройства
  - Конфигурация клиента
  - Обои
- Управление активами (только на уровне устройств)
- Информация об устройстве
  - Wi-Fi
- Клетчатка
- Bluetooth
- Управление безопасностью
- Защита от кражи (только на уровне устройства)
  - Информация GPS (только на уровне устройства)
  - Wipe & Lock (только на уровне устройства)
  - Сообщение (только на уровне устройства)
- Конфигурация безопасности
  - Passкод устройства
  - Passкод контейнера
  - Антивирус
- Окончание срока службы (только на уровне устройства)
  - Стирание (только на уровне устройства)
- Настройки ограничений
  - Ограничения
- Управление сертификатами
- Управление соединениями
- Wifi
  - Тип безопасности
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Тип VPN
    - VPN
    - VPN для каждого приложения
- Ограничения
- Управление PIM
- Gmail Exchange

- Информация GPS (только на уровне устройства)
- Wipe & Lock (только на уровне устройства)
- Сообщение (только на уровне устройства)
- Конфигурация безопасности
  - Passкод
  - Шифрование
  - Антивирус
- Окончание срока службы (только на уровне устройства)
  - Стирание (только на уровне устройства)
- Настройки ограничений
  - Ограничения
  - Владелец устройства AE

Контейнер для BYOD

- Android Enterprise
  - Android Enterprise
  - Gmail Exchange
  - Системные приложения AE
  - Passкод контейнера
- Samsung KNOX
  - Активация
  - Пасс-код Knox
  - Knox Security
  - Knox Exchange
  - Knox eMail
  - Knox Apps

Управление соединениями

- Wifi
  - Тип безопасности
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Ограничения
- APN
- Bluetooth

- Настройки
- Пересмотр конфигурации (только на уровне устройства)
- Журнал устройства (только на уровне устройства)
  - Журнал команд
  - Возможные статусы команд
- Управление активами (только на уровне устройств)
  - Информация об устройстве
  - Клетчатка
  - Информация о синхронизации
- Управление безопасностью
  - Защита от кражи (только на уровне устройства)
    - Информация GPS (только на уровне устройства)
    - Настройки GPS
  - Конфигурация безопасности
    - Пасскод
    - Антивирус
    - Центр безопасности
    - Конфигурация брандмауэра
    - Правила брандмауэра
  - Настройки ограничений
    - Функциональность устройства
  - BitLocker
    - Конфигурация BitLocker
    - Состояние BitLocker
  - Управление сертификатами
    - Список сертификатов
    - Конфигурация сертификата
    - SCEP
- Управление соединениями
  - Wifi
    - Тип безопасности
    - Используйте прокси-сервер
  - Ограничения Wifi
  - VPN
    - Тип соединения
    - Общие конфигурации VPN
  - Ограничения VPN

- Bluetooth
- Управление PIM
  - Exchange Active Sync
  - eMail
- Управление приложениями
  - Enterprise App Manager
    - Установленные приложения
    - Обязательные приложения
    - Ограничения системных приложений
    - Черные и белые списки

Конфигурация MacOS

Общие сведения

- Обзор профиля группы (только на уровне группы)
- Обзор устройства (только на уровне устройства)
- Пересмотр конфигурации (только на уровне устройства)
- Журнал устройства (только на уровне устройства)
  - Журнал команд
  - Возможные статусы команд

Управление активами (только на уровне устройств)

- Информация об устройстве
- WiFi
- Клетчатка
- Bluetooth

Управление обновлениями (только на уровне устройства)

- Обновленная информация

Управление безопасностью

- Защита от краж
  - Вытрите и заблокируйте
- Конфигурация безопасности
  - Пасскод
  - Сертификат
- Настройки ограничений
  - Функциональность устройства
  - iCloud

Общий обзор

Введение в AppTec360

Решение AppTec для корпоративного управления мобильными устройствами предлагает возможность управлять и настраивать все мобильные устройства с помощью интуитивно понятной консоли управления. В этом случае сервер EMM может работать либо в Вашем собственном окружении, либо Вы можете воспользоваться нашим облачным решением.

Даже если речь идет о централизованной установке корпоративных приложений на смартфоны, Вы попали по адресу. С помощью Enterprise Mobile Manager Вы можете в считанные секунды распространять корпоративные приложения и документы на устройствах или блокировать нежелательные приложения с помощью белых/черных списков.

Использование личных устройств в компаниях ставит новую задачу по обеспечению безопасности смартфонов и планшетов. Из-за того, что сотрудники все чаще хотят использовать свои смартфоны, ИТ-администраторам приходится защищать большое количество различных типов устройств. Мы поможем Вам защитить все устройства и хранящиеся на них конфиденциальные данные и управлять ими с помощью интуитивно понятной консоли.

Поддерживаемые операционные системы устройств

AppTec360 предлагает поддержку устройств на базе iOS, Android и Windows. Обратите внимание, что функциональные возможности упомянутых платформ могут отличаться от одной ОС к другой.

- Apple iOS 11.0 или выше*
- Apple macOS 10.11 или выше
- Google Android 4.4 или выше** в облачной версии
- Google Android 4.1 или выше** на версии OnPrem
- MS Windows 10 или выше*** (настольный компьютер, ноутбук и планшет)

**Примите во внимание, что устройства с iOS 10 или более ранней версией не могут быть зарегистрированы из-за радикальных изменений, внесенных компанией Apple в процесс регистрации.*

***Устройства можно подключать и настраивать, даже если они используют версию, которая больше не поддерживается производителем. Обратите внимание, что некоторые функции могут требовать определенной версии Android. В случаях поддержки мы следуем официальной поддержке производителя. В случае проблем или ошибок, вызванных устаревшей версией, которая больше не поддерживается производителем, мы оставляем за собой право предложить лишь ограниченную поддержку.*

****Домашние версии Windows не поддерживаются из-за ограничений операционной системы. Мы настоятельно рекомендуем использовать версию ОС, которая все еще поддерживается производителем. Не только для совместимости, но и по соображениям безопасности. Поэтому мы рекомендуем iOS 12 или выше и Android 9 или выше.*

Поддерживаемые каталоги LDAP

- Microsoft Active Directory
- Откройте LDAP

Актуальную информацию о "Поддерживаемых операционных системах устройств" и "Поддерживаемых LDAP-каталогах" можно найти здесь:

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

Объяснение «Режима под наблюдением» на устройствах Apple

Режим Supervised-Mode представляет собой расширенный интерфейс для устройств iOS.

К устройству, настроенному соответствующим образом, могут быть применены дополнительные ограничения, относящиеся к функциональности конечного пользовательского устройства. Они также содержатся в руководстве для администрации и отмечены соответствующим баннером.

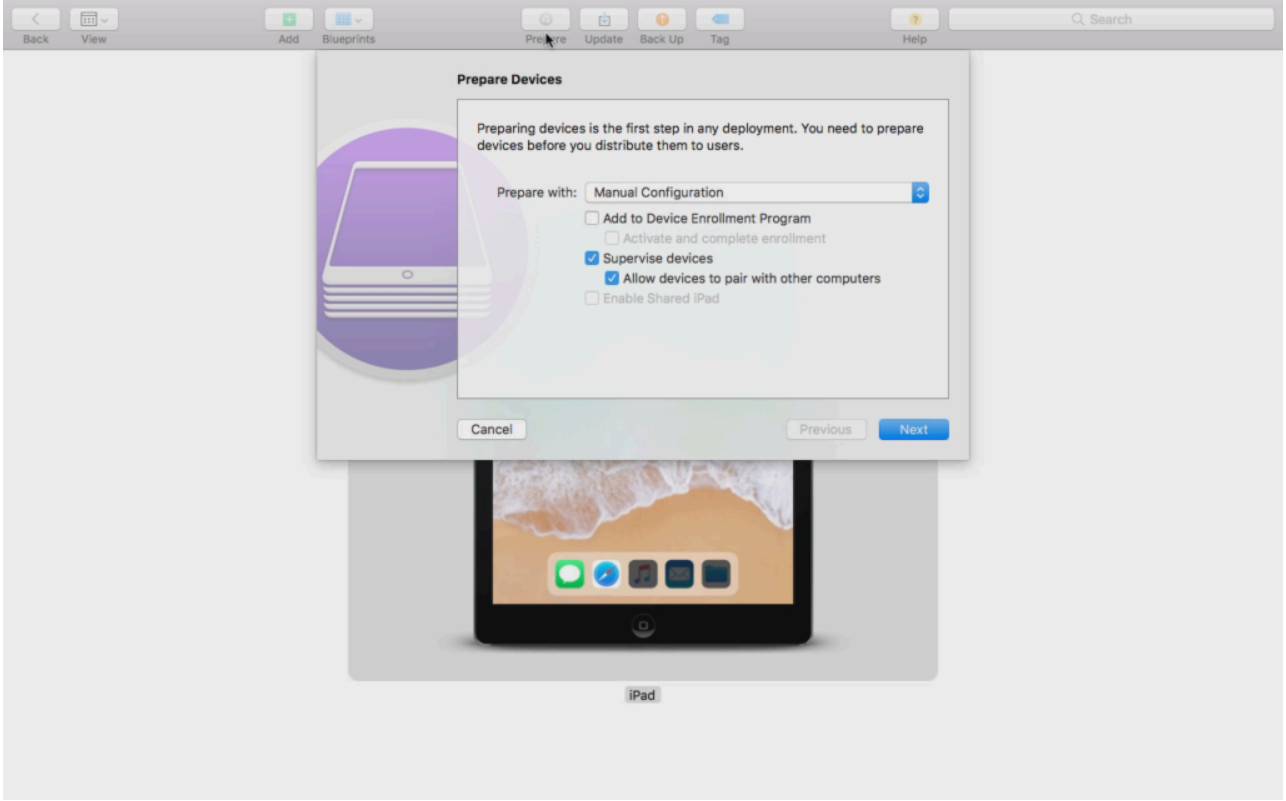
Доступно в режиме «Под наблюдением

Режим "Supervised-Mode" можно активировать с помощью программы "Apple Configurator". Apple Configurator может устанавливать настройки по умолчанию на новых iOS-устройствах в качестве инструмента для настройки (через USB-интерфейс).

Инструмент может устанавливать не только профили конфигурации, но и приложения. Это бесплатно, но требует наличия компьютера Mac.

Активируйте режим под наблюдением

1. Откройте Конфигуратор Apple



2. Нажмите на устройство и выберите "Подготовить".
3. Выберите "Ручная конфигурация" и "Контролировать устройства".
4. Нажмите "Далее".
5. (Необязательно) Теперь Вы можете добавить MDM-сервер, на котором будет зарегистрировано устройство. Ссылку для этого можно найти в разделе "Общие настройки - Конфигурация iOS - Конфигуратор и URL" Выберите свою организацию или создайте новую
6. Выберите свою организацию или создайте новую
7. Выберите, какие шаги следует пропустить при первоначальной настройке, и нажмите "Далее" (ВНИМАНИЕ: продолжение работы приведет к удалению Вашего устройства!)

Теперь Ваше устройство будет переведено в режим наблюдения. Это может занять несколько минут. После этого устройство перезагрузится.

Теперь Ваше устройство под присмотром!

Добавление устройства в DEP

Вы также можете добавить устройства в программу DEP (Device Enrollment Programm) с помощью Apple Configurator, если Ваши устройства работают под управлением iOS 11 или выше.

Дополнительная информация о DEP: https://www.apple.com/business/dep/

Выполните те же действия, что и при контроле устройства, и дополнительно отметьте "Add to Device Enrollment Programm". Вам будет предложено ввести данные для входа в DEP, если Вы никогда ранее не входили в DEP с помощью Apple Configurator.

После завершения процесса устройство можно найти в сервере DEP Server "Devices Added by Apple Configurator 2". Теперь Вы можете использовать этот сервер и подключить его к консоли управления или перенести устройство на уже существующий сервер.

Теперь Вы успешно добавили устройство в DEP!

Объяснение Android Enterprise

Что такое Android Enterprise?

Android Enterprise предлагает лучший контроль над рабочими устройствами, которые управляются с помощью MDM. Это позволяет администраторам либо полностью контролировать андроид-устройства, либо отделить данные компании от личных данных на контейнерных устройствах. Кроме того, Android Enterprise позволяет проще регистрировать устройства и легко распространять приложения.

Каковы требования для использования Android Enterprise?

Android Enterprise может использоваться бесплатно всеми желающими. Вам нужно только подключить учетную запись google к MDM, чтобы включить все функции Android Enterprise. Подробнее об этом можно прочитать в разделе Android Enterprise.

Android Enterprise можно использовать на устройствах с Android 5.1 или выше, за исключением Enhanced Work Profile (см. ниже). Мы рекомендуем использовать как минимум Android 7 или выше для более легкой регистрации или Android 11, чтобы использовать все доступные функции.

Какие режимы доступны в Android Enterprise?

Существует 3 различных режима, которые можно использовать при работе с Android Enterprise.

AE Полностью управляемое устройство (Work Managed): Полностью управляемое устройство, которое используется только для работы. Это позволяет администратору полностью контролировать устройство. Это не позволяет использовать устройство в личных целях. Чтобы зачислить устройства в этот режим, их необходимо сбросить и зачислить с помощью QR-кода (см. AE Enrollment) или зачислить с помощью Knox Enrollment или Zero Touch.

AE BYOD Container: Контейнер BYOD (bring your own device) позволяет пользователям получать доступ к данным компании на своем личном телефоне в отдельном контейнере. В этом режиме личные приложения не могут видеть данные и приложения компании, и наоборот. Чтобы зарегистрировать устройства в этом режиме, необходимо загрузить приложение AppTec и отсканировать QR-код. Создайте устройство в консоли и выберите в качестве типа устройства "AE Container (BYOD & Enahnced Work Profile)". Нажмите на QR-код на только что созданном устройстве, чтобы получить QR-код, и установите первый переключатель на "Legacy & BYOD".

AE Enhanced Work Profile: (требуется Android 11 или выше) В то время как вышеупомянутый BYOD Container переносит данные компании на частное устройство, Enhanced Work Profile делает то же самое, но для устройства, принадлежащего компании. Он создает тот же

контейнер, но дает администратору немного больше контроля над устройством, поэтому пользователь не может просто удалить MDM с устройства. Создайте устройство в консоли и выберите в качестве типа устройства "AE Container (BYOD & Enahnced Work Profile)". Нажмите на QR-код на только что созданном устройстве, чтобы получить QR-код, и установите первый переключатель на "Enhanced Work Profile". Этот QR-код можно отсканировать после перезагрузки устройства и 6-кратного нажатия на экран, как описано в Методе 1 в разделе Регистрация AE.

Как назначить приложения на устройства Android Enterprise?

Сначала Вам необходимо одобрить приложения, которые Вы хотите использовать, в разделе Общие настройки → Управление приложениями → AE Play Store → Play Store Apps. После одобрения приложений Вы можете назначить их в список обязательных приложений → Вашего профиля, нажав на "+" и выбрав приложение на вкладке "AE Play Store". Это приведет к автоматической загрузке и установке приложения. Учетная запись google на устройстве не требуется, и пользователю не нужно подтверждать или разрешать это.

Загружайте собственные приложения в Google Play Store

Вы можете загрузить свои собственные приложения в Google Play Store. Таким образом, Вы сможете воспользоваться различными преимуществами, например, механизмом обновления Play Store.

Для этого Вам нужен аккаунт разработчика Google. Войдите в систему, используя Google Play Console(https://play.google.com/apps/publish).

Нажмите на "Создать приложение". Выберите язык по умолчанию и название приложения.

Create application

Default language *

English (United Kingdom) – en-GB ▾

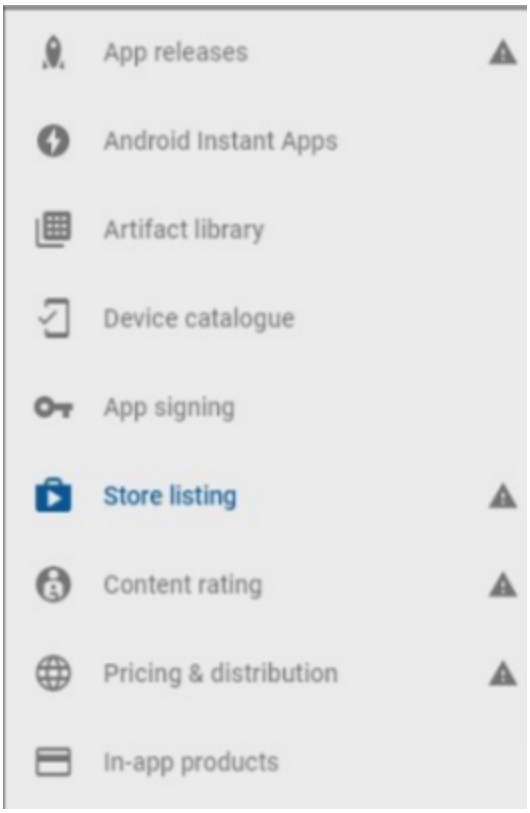
Title *

AppTec Demo App

15/50

CANCEL CREATE

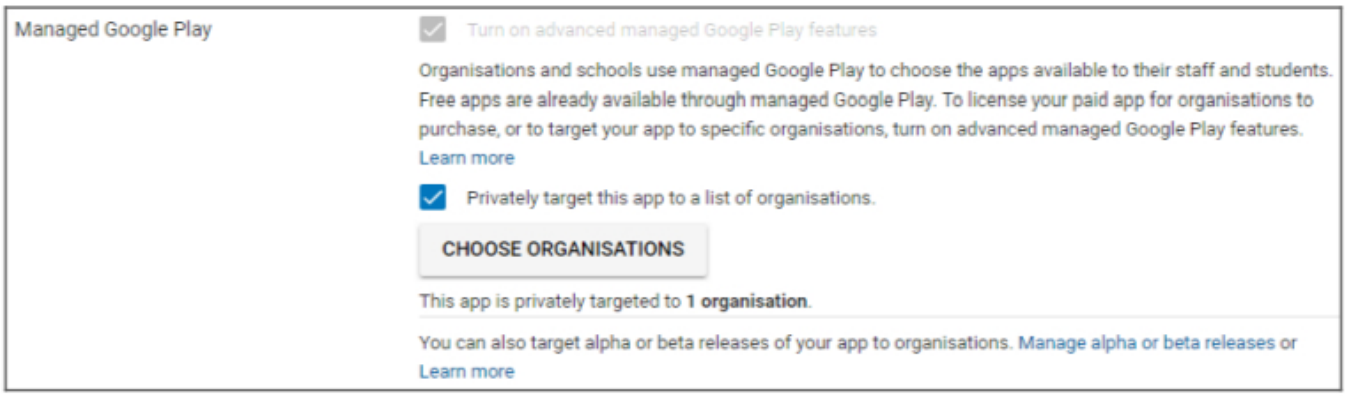
На следующей странице Вам будет предложено ввести различные сведения о Вашем приложении.



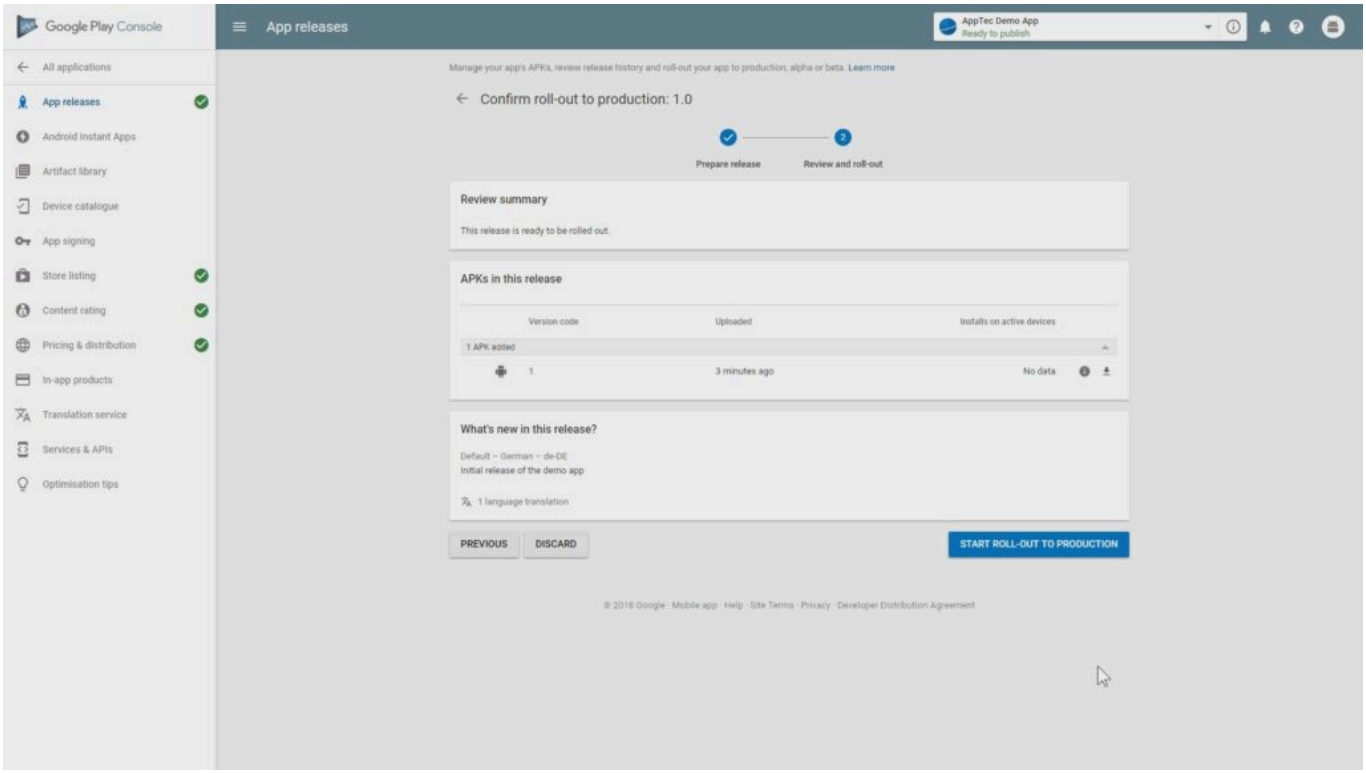
После того, как Вы ввели все данные, Вы увидите различные символы-подсказки в левой части экрана.

Наведите на них курсор, чтобы увидеть, какие шаги остались, и выполните их в любом порядке.

Примечание: Обязательно отметьте два флажка в пункте "Managed Google Play" в разделе "Pricing & Distribution". В противном случае приложение будет общедоступным, и доступ к нему смогут получить все желающие. Также не забудьте выбрать страну для распространения.



После того, как Вы выполнили все шаги, Вы можете перейти в раздел "Выпуск приложений". Нажмите на "Review" и "Start Roll-Out to Production", чтобы завершить работу над своим проектом и опубликовать приложение.



Это может занять некоторое время, пока приложение будет доступно в Play Store. После завершения процесса Вы можете найти свое приложение в магазине Play for Work и одобрить его. После этого Вы можете просто назначить приложение на устройства с помощью консоли EMM так же, как Вы делаете это с другими приложениями.

Требования и установка

Требования

Системные требования

Виртуальное устройство доступно в формате Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) и в виде сжатого файла .vhdx (Hyper-V)*.

*Примечание: При использовании Hyper-V машина должна быть создана с Generation 1.

Целевой размер виртуального диска составляет 20 ГБ, а машине требуется 4 ГБ оперативной памяти.

Устройство работает на базе Debian 9 64bit.

Обновите импортированную машину до новейшей совместимости (например, в VMWare) и убедитесь, что тип ОС машины установлен правильно в Вашем гипервизоре.

Лицензионный ключ

Для того чтобы успешно активировать и установить сервер, Вам потребуется действующий файл лицензии. Вы можете получить его непосредственно у AppTec360 и/или у Вашего соответствующего реселлера.

Разрешение IP-адресов и DNS

Прибор AppTec360 должен быть доступен устройству, использующему имя хоста, на который выдана лицензия.

Для регистрации устройств с Windows 10 Вам также необходимо настроить дополнительный поддомен в виде "enterpriseenrollment.", указывающий на устройство.

SSL-сертификат

Поскольку все соединения с устройствами и обратно должны быть защищены с помощью SSL, Вам необходим действительный сертификат для имени хоста, выданный центром сертификации, которому доверяет устройство. Закрытый ключ сертификата должен быть загружен без защиты паролем. В большинстве случаев для того, чтобы устройства распознали сертификат сервера, требуется промежуточный сертификат для центра сертификации.

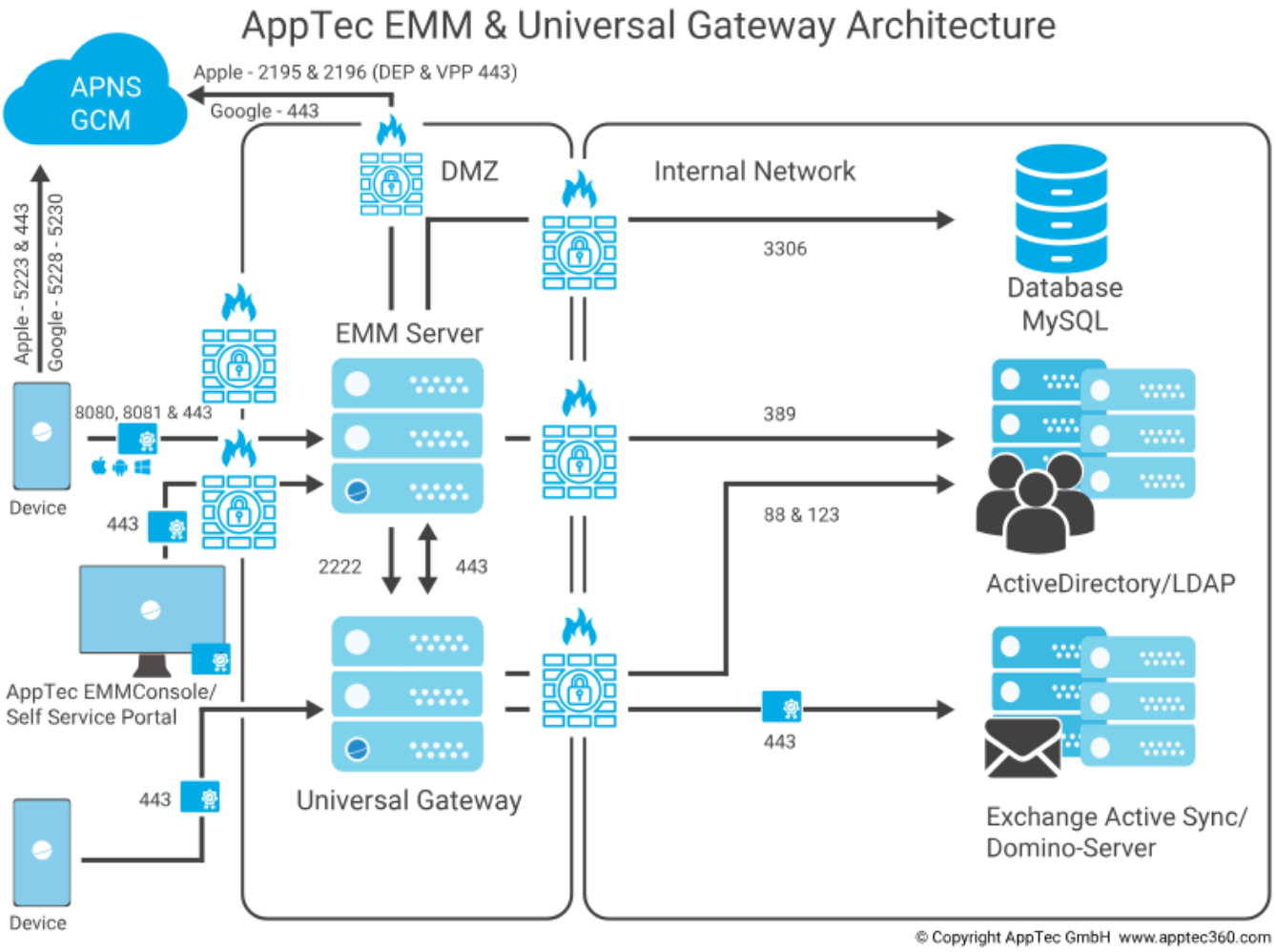
Устройствам с Windows 10 потребуется специальный сертификат для поддомена enterpriseenrollment.

Начиная с версии устройства 202104 Вы также можете использовать сертификаты Let's Encrypt, которые генерируются автоматически (описано в Шаге втором - SSL-сертификат).

SMTP-сервер

Для того чтобы AppTec360 EMM мог отправлять электронные письма (например, для регистрации устройств и подтверждения учетных записей), необходим сервер электронной почты и/или почтовый ретранслятор.

Правила брандмауэра



На этой схеме показано, какое подключение необходимо в зависимости от того, какие услуги Вы хотите использовать.

Более подробное описание см. в таблице на следующей странице.

Любые (внешние/ устройства)	→	**AppTec360 Appliance / emmconsole.com**
Порты	443	Управление, корпоративный AppStore и Windows Phone Communication
	8080	Общение с Android и iOS
	80	Первый раз установите Let´s Encrypt. После этого используется 443.
Любой (устройства)	→	**Любой (внешний)**
Порты	5223, 443	Apple Push Service, должен быть доступен без прокси, 443 как Fallback, см. https://support.apple.com/en-us/HT203609.
	5228-5230	Android Push Service (FCM), должен быть доступен без прокси-сервера
AppTec360 Appliance	→	**Контроллер домена**
Порты	389, (LDAPS 636)	Синхронизация пользователей с LDAP
AppTec360 Appliance	→	**Любой**
Порт	443	Используется для службы Android Push Service (GCM) Поиск в AppStore / Play Store
AppTec360 Appliance	→	**emmconsole.com**
Порты	443	Обновления AppTec360 Appliance, генерация сертификатов APNS
AppTec360 Appliance	→	**Сеть Apple (17.0.0.0/8)**
Порты	2195, 2196	Служба Apple Push Service и служба обратной связи
	443	DEP & VPP

Обновления системы безопасности

Операционную систему Debian следует регулярно обновлять, чтобы получить самые новые исправления безопасности. Однако убедитесь, что Вы не переходите на новую основную версию Debian вручную. Когда AppTec360 EMM будет совместим с новой основной версией, мы добавим возможность обновления в обновление устройства.

Пароли по умолчанию для виртуального устройства

Логин пользователя (вход Root отключен. Используйте "sudo" для административных задач)

apptec

Пароль для входа

apptec

Корневой пользователь MySQL

корень

Корневой пароль MySQL

apptec

Пользователь MySQL по умолчанию

AppTec

Пароль пользователя MySQL по умолчанию

AppTec

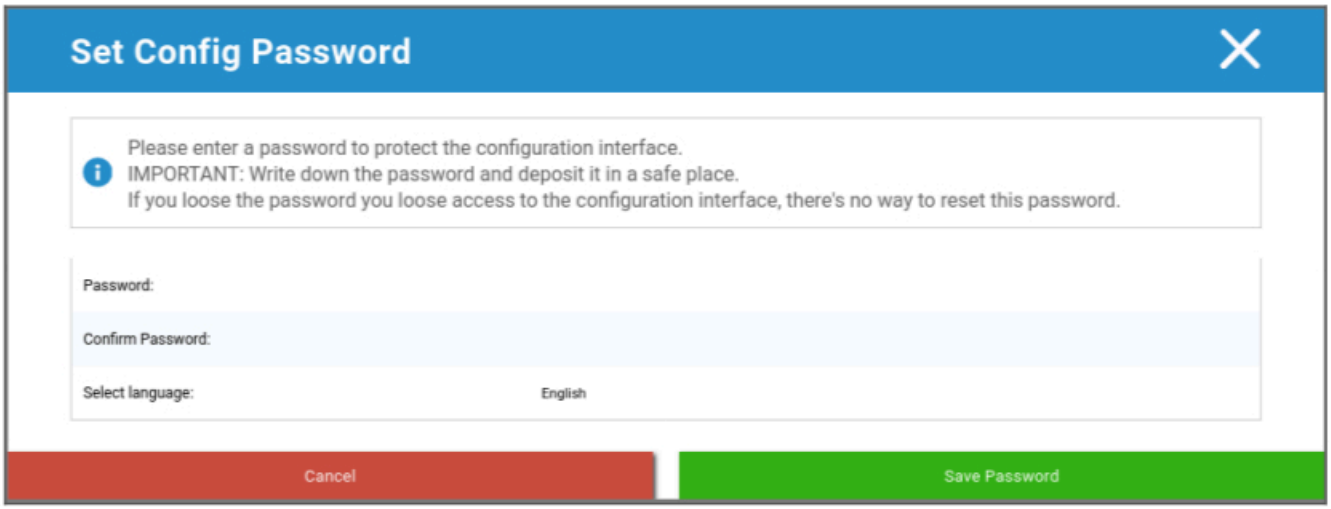
Конфигурация виртуального устройства

Важно: Прежде чем приступить к настройке виртуального устройства, разрешение дисплея должно быть установлено не менее 1280 x 800 пикселей.

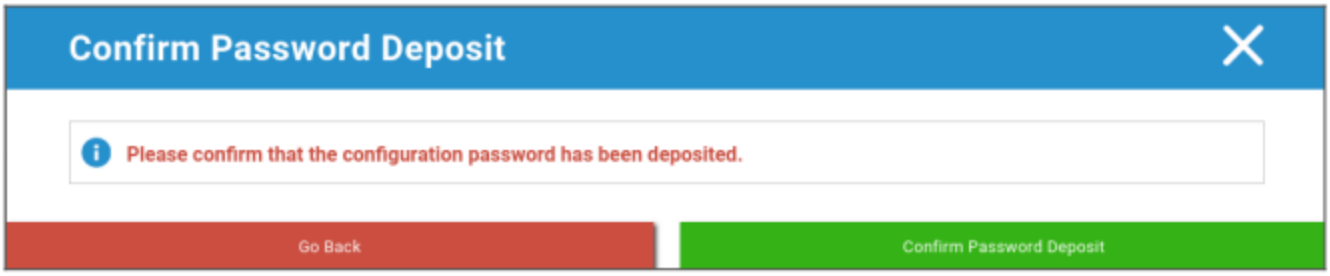
После входа в устройство Firefox должен автоматически запуститься и отобразить интерфейс конфигурации.

Подготовка

Сначала Вам необходимо задать пароль для интерфейса конфигурации. Этот пароль используется для шифрования всей информации и файлов, вводимых в интерфейс конфигурации. Здесь же Вы можете задать язык, на котором будет отображаться интерфейс (его можно изменить позже).

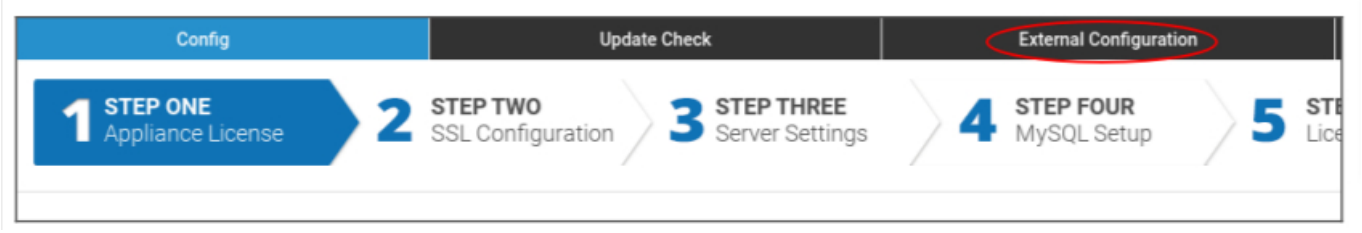


Пароль может быть сброшен только службой поддержки AppTec360, поэтому убедитесь, что Вы положили его в надежное место и подтвердили предстоящее всплывающее окно.



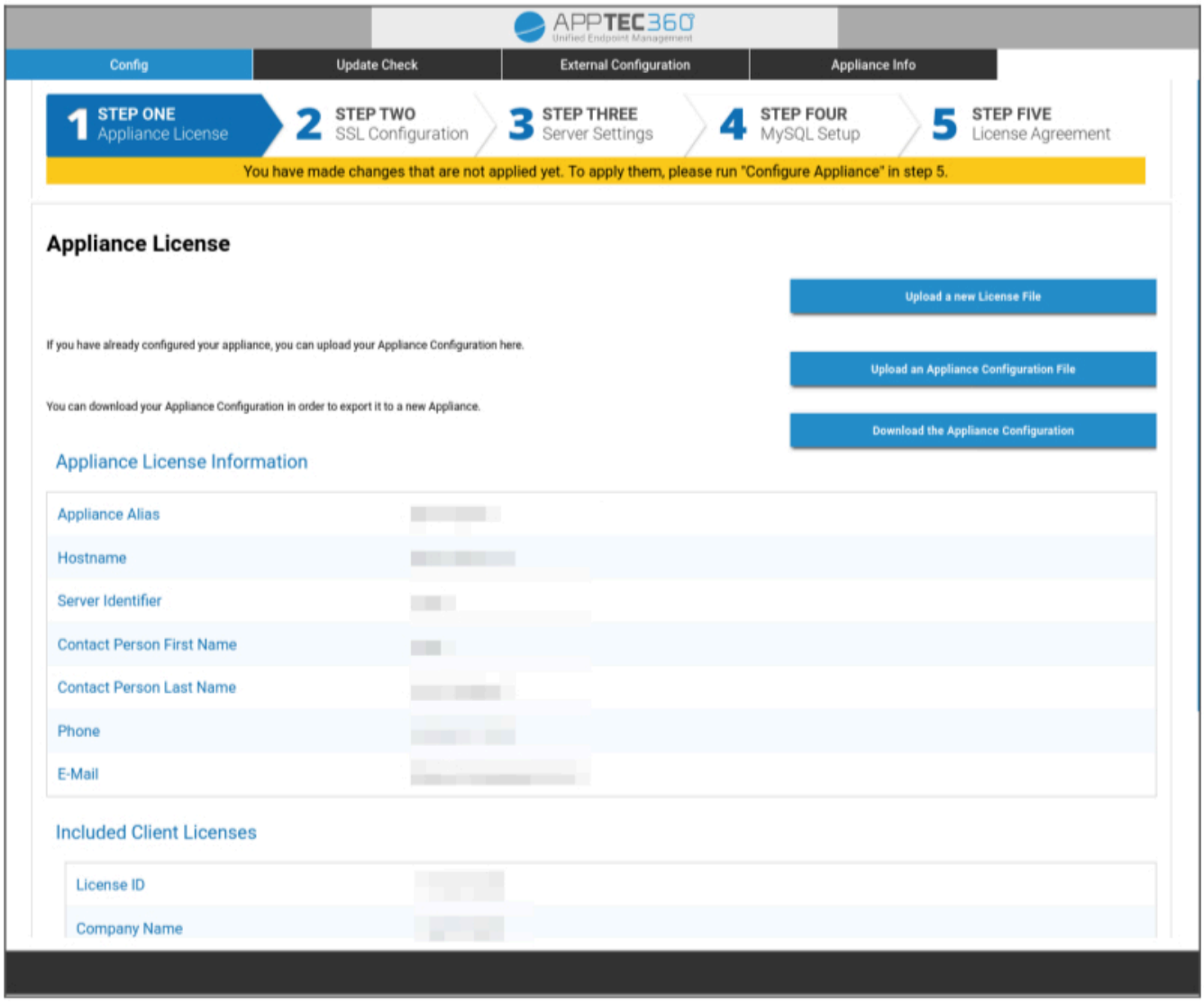
Настройка с внешнего хоста

Чтобы облегчить процесс настройки, Вы можете сделать страницу конфигурации доступной удаленно. Для этого выполните действия, описанные в разделе "Настройка с внешнего хоста".



Шаг первый — Лицензия на прибор

1. Пожалуйста, загрузите файл лицензии, который Вы получили от AppTec.
2. Если файл лицензии был успешно загружен, Вы можете увидеть информацию о лицензии прибора, как на скриншоте ниже.



Шаг второй — SSL-сертификат

Вы можете либо воспользоваться автоматической установкой сертификатов с помощью Let's Encrypt, либо предоставить сертификаты самостоятельно (см. раздел SSL-Certificate для получения дополнительной информации).

Автоматический

Сертификат будет сгенерирован автоматически с помощью службы Let's Encrypt.

AppTec360 EMM использует вызов HTTP-01 для проверки домена, что означает, что для первого запроса сертификата порт HTTP должен быть открыт из Интернета. Последующие запросы на продление могут быть подтверждены через HTTPS.

Переключите радиокнопки на "Automatic (Let's Encrypt)" и нажмите "SAVE VALUES". Сертификат будет автоматически запрошен при применении конфигурации в Шаге 5 - Лицензионное соглашение. При необходимости сертификат будет автоматически обновляться, и Вы получите электронное письмо, если срок действия сертификата истечет (что означает, что обновление могло быть неудачным).

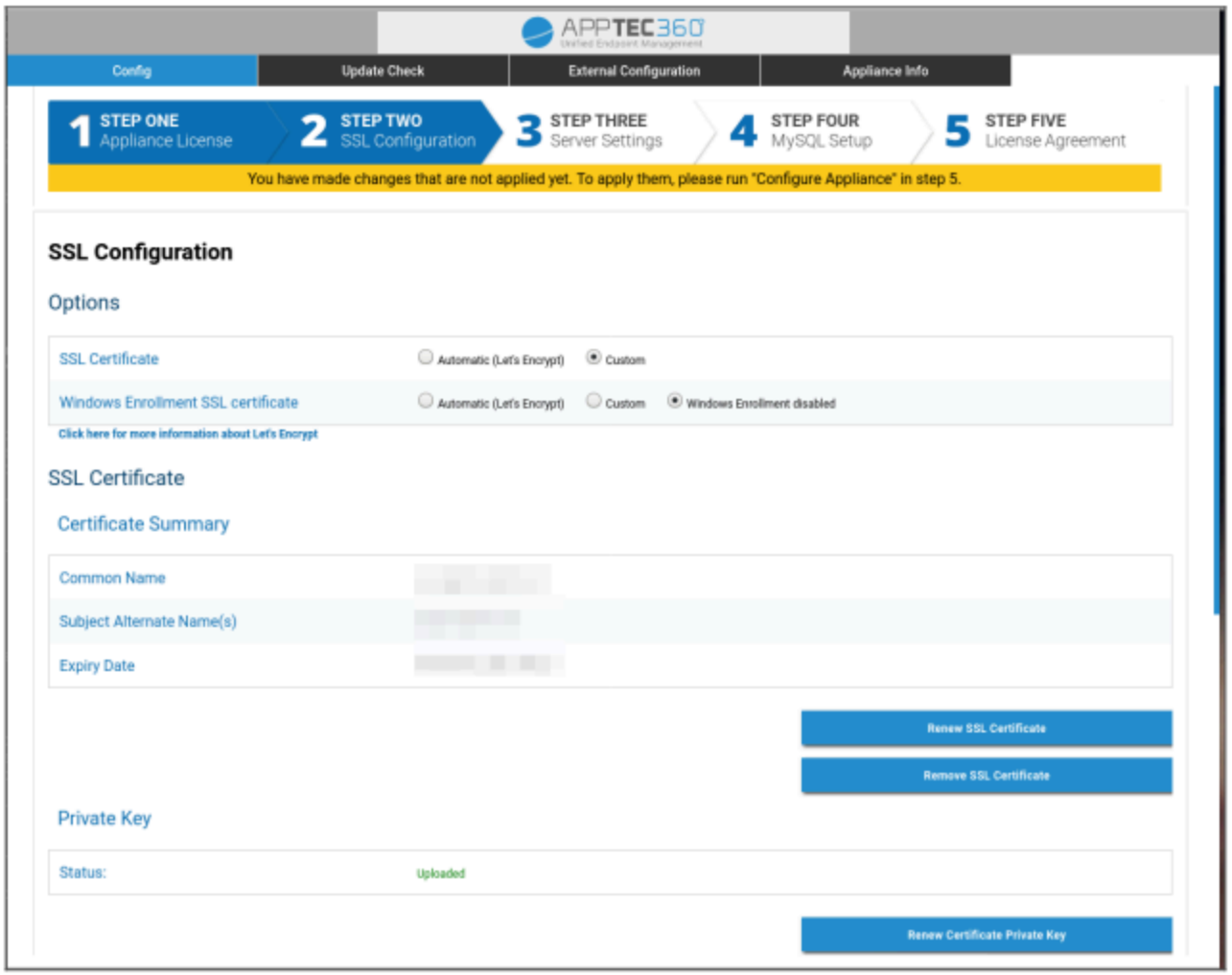
Пользовательский

1. Загрузите SSL-сертификат для Вашего лицензированного имени хоста. Вы можете увидеть имя хоста в Шаге первом - Лицензия прибора.

2. Загрузите также закрытый ключ сертификата и, при необходимости, промежуточный сертификат.

Важно: Ключ не должен быть защищен паролем. Если он защищен, пожалуйста, удалите пароль перед загрузкой.

Совет: Если Вы также хотите использовать устройства с Windows 10, Вам необходимо включить "Windows Enrollment SSL certificate" и загрузить сертификат, закрытый ключ и промежуточный сертификат для Вашего поддомена (описано в разделе Загрузка IP-адреса и разрешения DNS) в нижней части страницы.



Шаг третий — Настройки сервера

1. Пожалуйста, введите глобальный адрес электронной почты службы поддержки. Этот адрес будет использоваться в письмах, отправляемых Вашим пользователям, чтобы они знали, к кому обращаться в случае возникновения каких-либо проблем с их устройством.
2. Задайте настройки электронной почты, которые будут использоваться системой для отправки писем. Эти настройки будут использоваться для отправки электронных писем пользователю, а также для отправки сообщений об ошибках и запросов о возможностях на"support@apptec360.com".После сохранения настроек электронной почты Вам необходимо проверить их, нажав на "Test E-Mail Configuration" и следуя инструкциям.

Шаг четвертый — Настройка MySQL

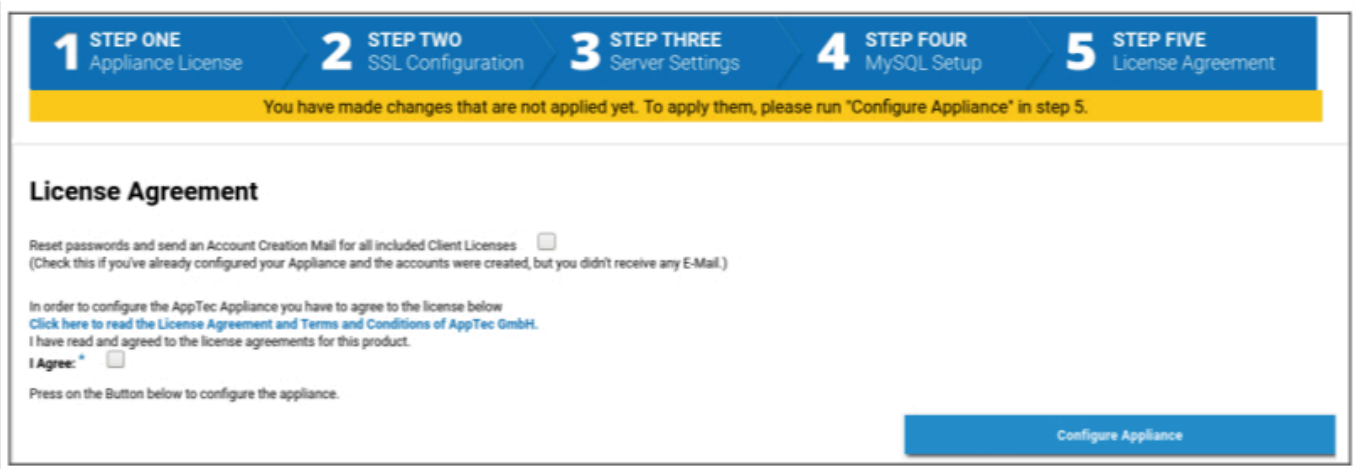
1. Если Вы хотите использовать внутреннюю базу данных, Вы можете пропустить этот шаг. В противном случае Вы можете ввести информацию о подключении к внешнему серверу базы данных.


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)

Шаг пятый — Лицензионное соглашение

1. Пожалуйста, прочтите лицензионное соглашение.
2. Отметьте "I Agree" и нажмите кнопку "Configure Appliance", чтобы применить настройки.

Подсказка: Вам нужно будет запускать "Configure Appliance" каждый раз, когда Вы изменяете настройки в 5 шагах, чтобы применить их.



Поздравляю!

Вы закончили настройку виртуального устройства.

На адрес, который Вы указали для получения лицензии (см. раздел "Включенные клиентские лицензии" в Шаге 1 - Лицензия устройства), было отправлено письмо с паролем.

Теперь Вы можете войти в консоль, используя этот пароль и адрес электронной почты, на который Вы его получили.

Чтобы войти в консоль, пожалуйста, введите имя хоста консоли в адресную строку Вашего браузера.

Имя хоста Вашего устройства Вы можете найти в Шаге первом - Лицензия устройства.

Устранение неполадок

1. Вы не получили электронное письмо при настройке устройства на пятом шаге - Лицензионное соглашение:

Убедитесь, что настройки электронной почты в Шаге 3 - Настройки сервера верны. Для повторной отправки пароля отметьте "Сбросить пароли и отправить письмо о создании учетной записи для всех включенных клиентских лицензий" в Шаге пятом - Лицензионное соглашение, прежде чем снова запускать "Configure Appliance".

2. Вы получили ошибку в отношении Let's Encrypt во время настройки в Шаге 5 - Лицензионное соглашение:

Убедитесь, что устройство доступно по своему доменному имени на порту 80. Let's encrypt также пишет журнал в "/var/log/letsencrypt", который может помочь в дальнейшем поиске неисправностей.

Рекомендации по безопасности

Рекомендуется выполнить следующие шаги, чтобы обезопасить устройство AppTec360.

Это не полный набор инструкций, а лишь рекомендации по базовой конфигурации.

- Измените пароль для пользователя AppTec360
- Измените пароль для пользователей MySQL "root" и "AppTec" и обновите Шаг 4 - Настройка MySQL соответствующим образом.
- Измените порт SSH-сервера по умолчанию
- Заблокируйте порт 80 в Вашей консоли и запретите входящий HTTP-трафик, используйте только HTTPS. После настройки возможна также внешняя конфигурация по HTTPS.
- Ограничьте доступ к интерфейсу управления только для определенных Ips в нижней части Шага 3 - Настройки сервера
- Настройте брандмауэр

Общие настройки

Обзор аккаунта

Информация о счете

Обзор

Здесь Вы можете увидеть обзор Вашей учетной записи AppTec360.

Название компании	Название Вашей компании
Дата создания	Дата создания Вашего счета
Тип лицензии	Paid = платная лицензия Бесплатно = неоплачиваемая лицензия Примечание: Учетные записи на OnPremise Appliance всегда будут отображаться как оплаченные по техническим причинам
Идентификатор клиента	Идентификатор Вашего счета (это НЕ номер Вашего клиента)
Дата истечения срока действия лицензии	Дата истечения срока действия Вашей лицензии AppTec360
Лицензия ContentBox	Бесплатно = бесплатная лицензия на 25 устройств Paid = платная лицензия для x устройств
Launcher	Показывает, можете ли Вы использовать пользовательскую пусковую установку для Android.
Устройства	Количество используемых в настоящее время лицензий / общее количество лицензий
Контактное лицо	Предоставленное контактное лицо
Телефон	Предоставленный номер телефона
eMail*	Предоставленный адрес электронной почты
Корневой пользователь	Корневые пользователи, которые могут войти в систему
Версия программного обеспечения	Текущая версия программного обеспечения

**Примечание: Здесь указывается адрес электронной почты, который Вы ввели при регистрации аккаунта. На его основе в дереве пользователей/устройств будет создан пользователь, которого можно будет изменить. Редактирование этого пользователя*

изменит адрес электронной почты, который Вы должны использовать для входа в систему, но не изменит информацию в обзоре аккаунта. .

Сообщение об ошибке

Сообщение об ошибке может быть отправлено непосредственно в службу поддержки, чтобы сообщить о проблемах или ошибках, и включает в себя информацию и журналы о Вашей учетной записи и настройках.

Тема	Тема сообщения об ошибке. Укажите номер тикета, если Вы хотите добавить его к существующему тикету поддержки.
Ожидаемое поведение	Подробно опишите, что Вы делали и что, по Вашему мнению, должно было произойти.
Фактическое поведение	Опишите в деталях, что именно произошло. Пожалуйста, цитируйте сообщения об ошибках ТОЧНО. Также будет полезно, если Вы добавите скриншоты во вложение.
В какое время у Вас возникла эта проблема?	Пожалуйста, укажите точное время, когда Вы получили конкретное сообщение об ошибке/ проблеме. В лучшем случае включите и секунды, например, 18:55:27
Можно ли воспроизвести эту проблему? Если да, то как (подробно)?	Подробно опишите, как Вы можете воспроизвести проблему.
Работала ли эта функция раньше так, как Вы ожидали? Если да, то до какого момента?	Оставьте пустым, если Вы не знаете.
Были ли внесены какие-либо изменения в систему до появления этой проблемы? Если да, то какие изменения (подробно)?	Всегда упоминайте, какое последнее изменение или действие Вы совершили до появления этой проблемы, даже если Вы считаете, что это не имеет отношения к делу.
Если применимо: Какие модели устройств и версии ОС затронуты?	Пожалуйста, всегда называйте точную версию ОС (например, iOS 14.7.1 или Android 11).
Если применимо: Каков публичный IP-адрес или/и серийный номер устройства?	Назовите хотя бы одно, даже если затронуты все устройства.
Включите журнальные файлы	Установите этот флажок, чтобы отправить файл журнала вместе с сообщением об ошибке. Это рекомендуется сделать.

Получите текущее состояние VPP от Apple и включите в сообщение об ошибке	Содержит информацию о назначении лицензий VPP. Активируйте его, только если Вас попросит об этом служба поддержки или если Ваша проблема связана с VPP.
Вложение	Прикрепите любой файл, который может быть полезен (например, скриншоты сообщения об ошибке).

Запрос функции

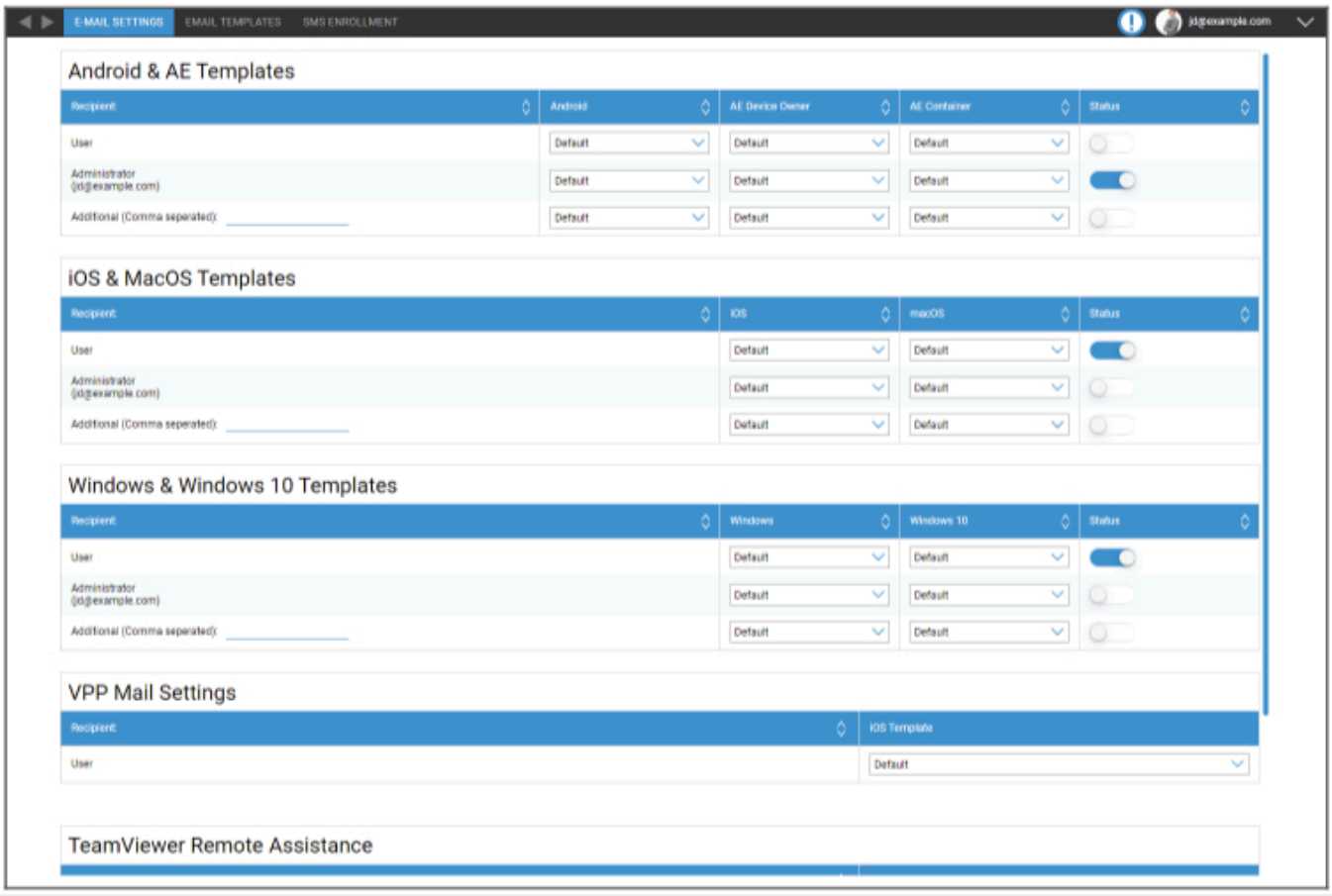
Запрос о функциях можно отправить непосредственно в службу поддержки. Это может содержать запрос на конкретную функцию или улучшение для

Резюме	Краткое описание вашей проблемы
Описание	Подробное описание вашей проблемы, пожалуйста, будьте как можно более конкретными
Вложение	Прикрепление файлов к сообщению об ошибке

Глобальная конфигурация

Настройки eMail

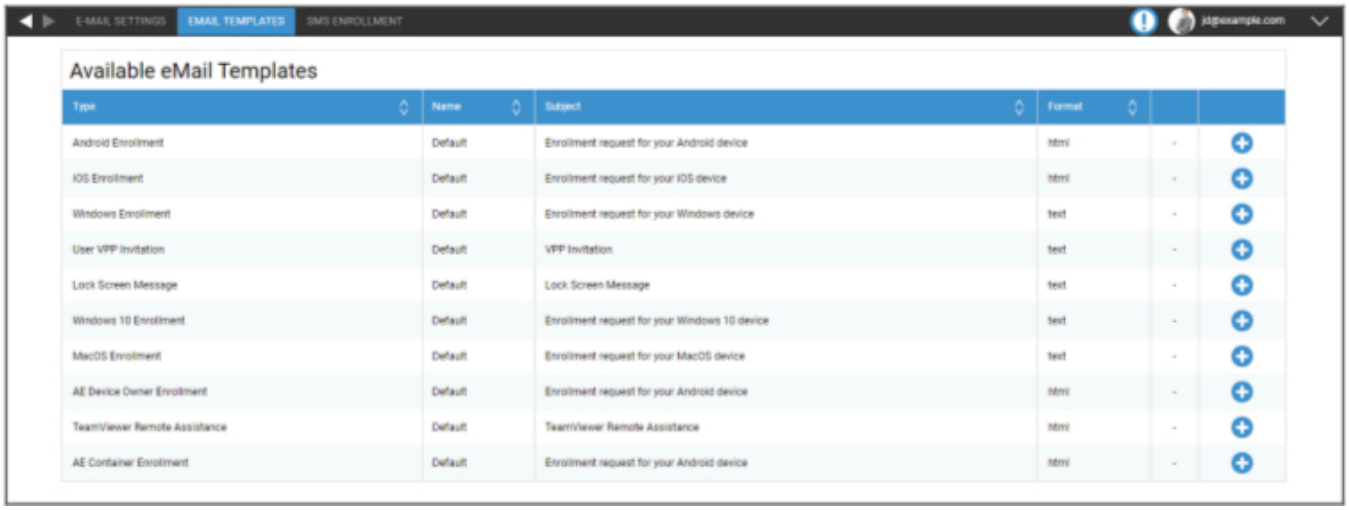
Здесь Вы можете определить, кто получит письмо, когда будет создан запрос на зачисление, и какой текстовый шаблон будет использоваться для этого письма.



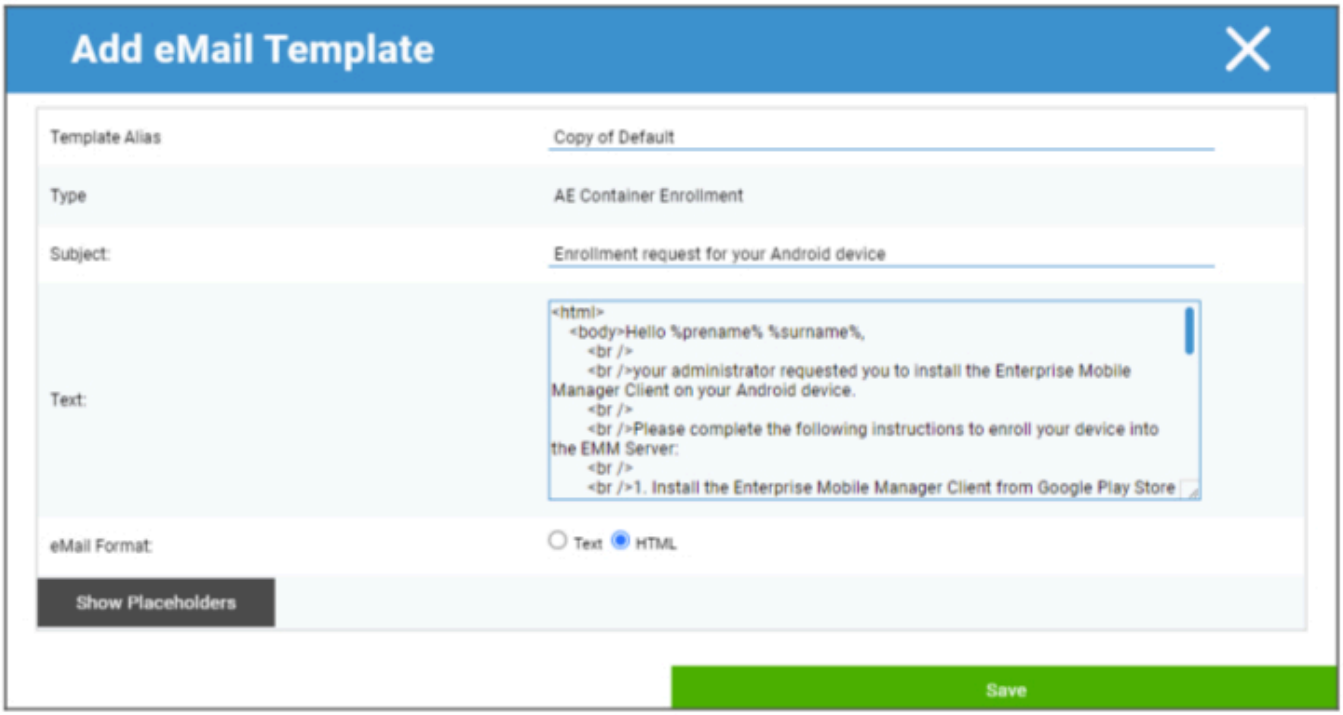
Шаблоны электронной почты

Здесь Вы можете создавать и редактировать свои шаблоны для различных сценариев. Они могут быть в виде обычного текста или в формате HTML. С помощью HTML Вы можете лучше контролировать форматирование текста.

Шаблоны по умолчанию нельзя редактировать или стирать.



Вы также можете использовать Placeholders в качестве переменной, которая будет автоматически заменяться. Нажмите на "Show Placeholders" во время редактирования, чтобы увидеть доступные Placeholders. Разные категории имеют разные плейсхолдеры.



SMS-регистрация

Здесь Вы можете отключить/активировать процесс SMS-регистрации.

(По умолчанию: деактивировано)

Вы также увидите индикацию, указывающую, сколько SMS-кредитов еще доступно.

Кредиты SMS необходимо приобретать отдельно.

Конфиденциальность

Доступ к GPS

Здесь Вы можете защитить просмотр GPS для каждого устройства с помощью 1 или 2 паролей (принцип "четырех глаз"). Вам будет предложено ввести пароль (пароли) каждый раз, когда Вы попытаетесь получить доступ к местоположению устройства.

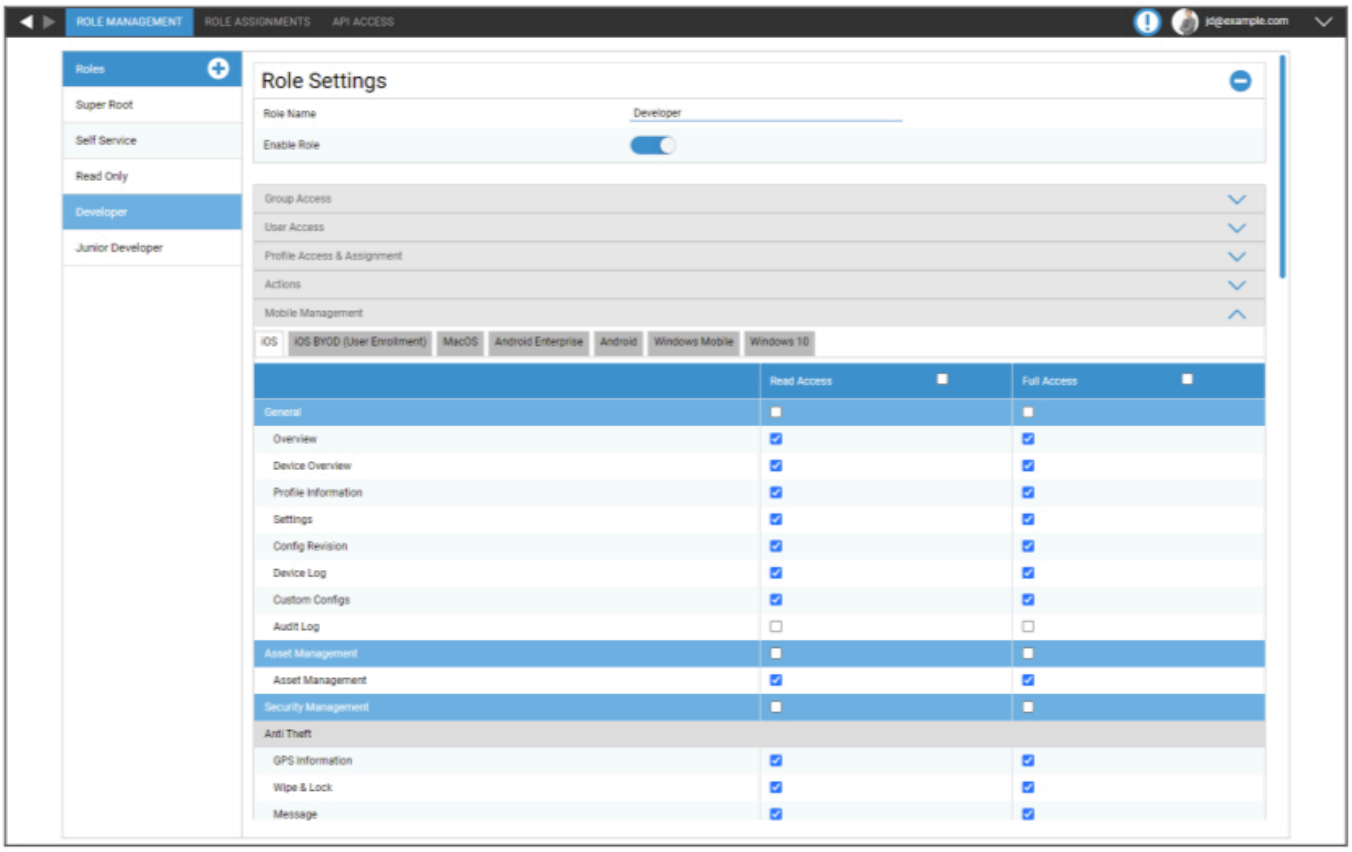
Ограничьте доступ к настройкам GPS	Выкл = функция выключена, и пароль для локализации не требуется
	Вкл = функция включена, и для локализации требуется пароль
Метод защиты	Использовать один пароль = использовать один пароль для локализации
	Использовать два пароля = использовать два пароля для локализации
Введите пароль (1)	Введите выбранный пароль
Повторите пароль (1)	Повторно введите выбранный пароль
необязательно: Введите пароль 2	Введите второй выбранный пароль
необязательно: Повторите пароль 2	Повторно введите второй выбранный пароль

Примечание: После установки пароля (паролей) Вам придется ввести его еще раз, прежде чем он будет полностью включен.

Доступ на основе ролей

Управление ролями

Роли определяют, что пользователь может видеть и делать, когда он входит в консоль управления. Это позволяет Вам создавать пользователей, которые могут входить в систему, но имеют ограниченную функциональность.



Роль Super Root - это роль по умолчанию, которая всегда может видеть и изменять все. Она не может быть изменена или удалена. Роль самообслуживания может видеть только своих пользователей и устройства. Вы можете объединить Самообслуживание и пользовательскую роль, чтобы, например, позволить пользователям самостоятельно входить в систему и регистрировать устройства только для своего пользователя.

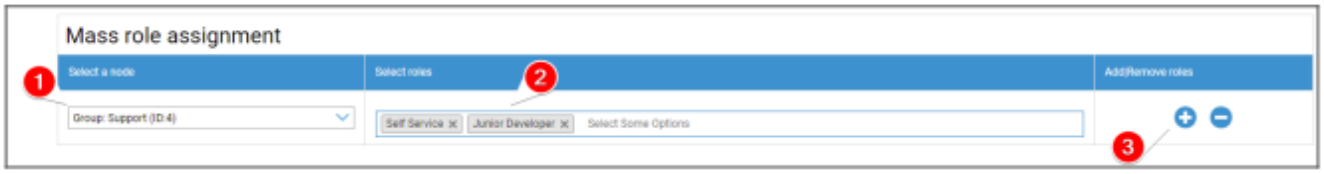
Пользовательские роли могут быть вручную включены или отключены. Новые роли по умолчанию отключены. Пользователи с отключенной ролью работают так, как будто у них нет этой роли. Это позволяет Вам, например, временно ограничить действия данной роли.

Все разрешения делятся на "Доступ для чтения" и "Полный доступ". Предоставление роли доступа на чтение позволяет ей видеть определенную часть консоли. Предоставление полного

доступа позволяет роли видеть и изменять определенную часть консоли.

Назначение ролей

Здесь Вы получите обзор всех пользователей, у которых есть роль, и увидите, какая у них роль. Здесь Вы также можете назначить роль пользователям или целым группам:

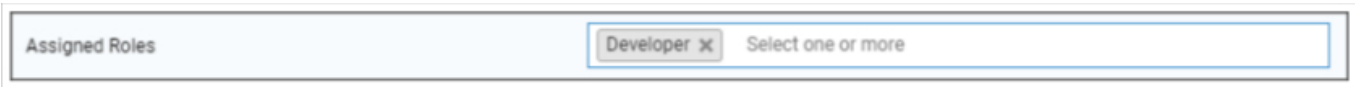


1. Выберите, для какой группы или пользователя Вы хотите добавить или удалить роли. Вы можете выбрать либо отдельного пользователя, либо группу. При выборе группы Ваши изменения затронут всех пользователей в этой группе и всех пользователей подгрупп, входящих в выбранную группу.
2. Выберите роль, которую Вы хотите добавить или удалить. Вы можете выбрать одну или несколько 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. Сохраните, чтобы завершить процесс. Пользователи, у которых ранее не было роли и была отключена опция "Can Login", автоматически получат письмо со ссылкой для установки пароля.

Под массовым назначением ролей Вы можете найти обзор назначенных ролей. Вы также можете вручную изменить там роли для конкретных пользователей.

Назначение роли

Чтобы назначить роль пользователю, Вам нужно перейти в раздел Mobile Management, где находится дерево Ваших групп, пользователей и устройств. Отредактируйте пользователя, чтобы назначить ему роль. В качестве альтернативы Вы можете использовать описанный выше метод только для отдельных пользователей.



Доступ к API

Доступ к AppTec360 REST API

Для работы с AppTec360 REST API требуется токен аутентификации (ключ API) и закрытый ключ, которые необходимо сгенерировать в консоли управления.

Для этого войдите в AppTec360 EMM и перейдите в раздел

Общие настройки → Доступ на основе ролей → Доступ к API и добавьте новый ключ.

Вы должны выбрать пользователя, чьи права будут применяться к ключу API.

Закрытый ключ можно загрузить только один раз. После начала загрузки ключ будет удален, а кнопка "Загрузить" исчезнет.

Если Вы потеряете свой закрытый ключ, Вам придется сгенерировать новый API-ключ.

Общие правила

- REST API доступен ниже базового URL:

/public/external/api

- Все запросы должны быть отправлены через POST.
- API REST поддерживает запросы только через HTTPS.
- Запросы должны содержать следующие заголовки:

Название заголовка	Значение заголовка	Описание
Тип содержимого	приложение/json	исправлено
auth	123...xyz	Ключ API на вкладке "Доступ к API"
подпись	Подпись в кодировке Base64	Подпись полезной нагрузки, созданной с помощью закрытый ключ на вкладке "Доступ к API"

- Тело запроса должно представлять собой объект в кодировке json, который должен содержать следующие значения:

Поле	Поле Пример Значение	Описание
api	v2/device/listdevices	Название API
время	1529662725	Unix Timestamp (UTC) клиентской машины. Максимально допустимая разница во времени между клиентом и сервером составляет 30 минут.

- В случае успеха API возвращает запрошенные данные (см. раздел "Запросы" ниже) и HTTP-код состояния 200.
- Если произошла ошибка, код состояния HTTP будет от 4xx до 5xx в зависимости от ошибки, а объект ответа будет содержать массив с ключом "errors", который содержит список человекочитаемых сообщений об ошибках.
- Если для устройства нет подходящих данных, будет возвращен пустой массив.
- Если Id устройства не существует, то возвращаемые данные будут равны null.

Пример запроса

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]}}

Запросы

Перечислите все устройства

Функциональность: Возвращает список всех устройств, содержащий ID устройства, IMEI и серийный
API URI: v2/device/listdevices
Обязательные параметры: нет
Необязательные параметры: нет

Пример тела запроса

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

Пример тела ответа

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

Получите список позиций (GPS)

Функциональность: Возвращает список всех сохраненных записей журнала положения для идентификаторов устройств
API URI: v2/device/listposition
Обязательные параметры: "ids" - массив идентификаторов устройств
Дополнительные параметры: нет

Пример тела запроса

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

Пример тела ответа

{
"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":[],
]
}

Получите карту активов

Функциональность:
Возвращает список всех сохраненных возможных активов, которые можно запросить с помощью функции Get any asset data.
Вы можете использовать либо человекочитаемую форму, либо тег актива для запроса данных.
API URI: v2/device/getassetmap
Обязательные параметры: нет
Необязательные параметры: нет

Пример тела запроса

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

Пример тела ответа

Этот ответ был сокращен для удобства чтения.

{
"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": []
}

Получите любые данные об активах

Функциональность: Возвращает список запрошенных данных об активах для идентификаторов устройств
API URI: v2/device/getassetdata
Обязательные параметры: "ids" - Массив идентификаторов устройств
Дополнительные параметры:
"assetkeys" - Ключи данных об активах, которые необходимо вернуть. Если не указано, будут возвращены все доступные данные об активах
. Вы можете получить список ключей активов с помощью Get asset map.

Пример тела запроса

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

Пример тела ответа

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

Пример кода в 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)
```

Конфигурация Apple

Сертификат APNS

Здесь Вы можете загрузить сертификат APNS. Он необходим для управления устройствами iOS и MacOS.

Примечание: Сертификат APNS действителен только в течение одного года. Его необходимо обновить до истечения срока действия. Процесс продления идентичен процессу создания (см. ниже) и занимает всего несколько коротких минут.

Если Вы забудете вовремя продлить регистрацию, Вы не сможете внести изменения в уже зарегистрированные устройства **и Вам придется регистрировать все устройства заново.**.

Шаг 1

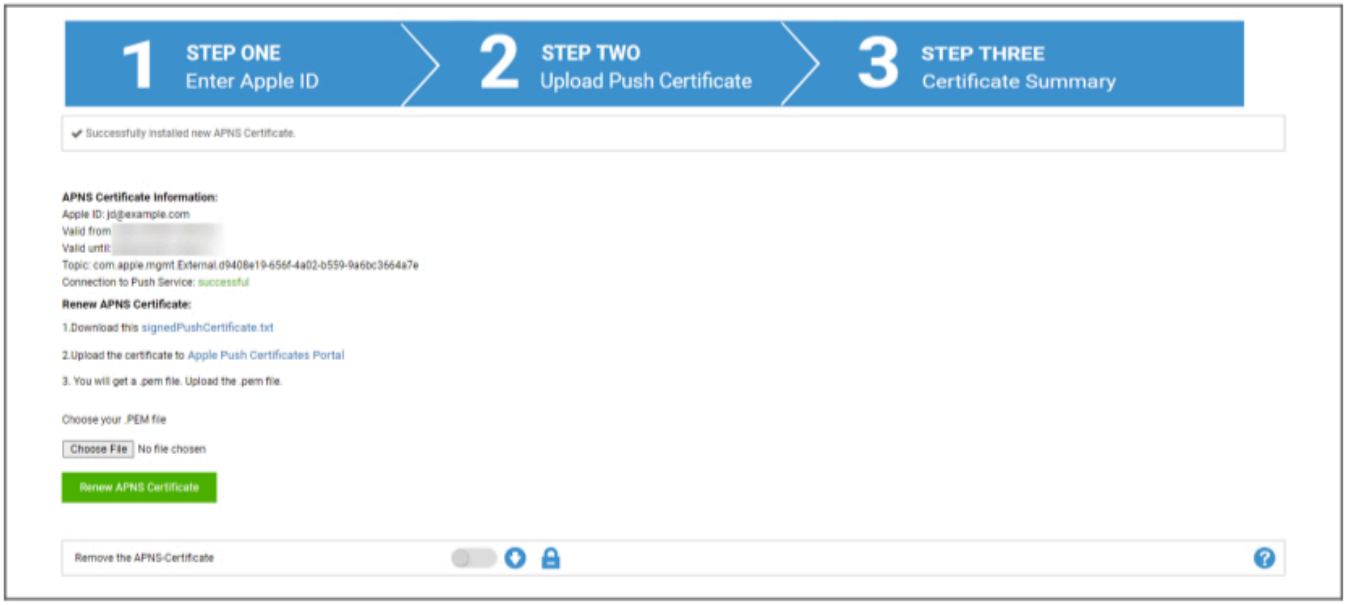
- Сначала введите свой Apple ID, который Вы хотите использовать для создания сертификата APNS.

Примечание: Этот Apple ID используется только для создания сертификата APNS. Этот Apple ID не имеет никакого отношения к устройствам, и устройства не будут знать об этом Apple ID. Кроме того, Вам нужен доступ к этому Apple ID для обновления сертификата APNS. Поэтому рекомендуется использовать какой-нибудь общий Apple ID и задокументировать данные для входа. Напоминание отправляется на используемый почтовый адрес Apple ID до истечения срока действия сертификата APNS.

- Нажмите "Следующий шаг", чтобы продолжить.
- (опционально) Вы также можете восстановить ранее удаленный сертификат APNS, если Вы удалили его случайно.

Шаг 2

- Загрузите файл signedPushCertificate.txt
- Перейдите на сайт https://identity.apple.com/pushcert/ и войдите в систему, используя Apple ID из Шага 1.
- Нажмите на "Создать сертификат".
- (необязательно) введите примечание. Это может быть полезно, если Вы управляете несколькими арендаторами, чтобы легко идентифицировать их.
- Нажмите "Выбрать файл", чтобы выбрать ранее загруженный файл signedPushCertificate.txt
- Нажмите на кнопку "Загрузить".
- Теперь Вы увидите подтверждение того, что Вы создали сертификат APNS.
- Нажмите "Загрузить" и сохраните его.
- Вернитесь в консоль управления.
- Нажмите на "Choose File" и выберите сертификат APNS, который Вы хотите загрузить.
- Нажмите на "Загрузить".



Шаг 3

Теперь Вы успешно настроили сертификат APNS и можете управлять устройствами iOS и MacOS.

В Шаге 3 Вы увидите обзор Ваших текущих используемых сертификатов APNS.

Также у Вас есть возможность продлить срок действия сертификата APNS, выполнив указанные на экране действия. Не забудьте обновить его до истечения срока действия.

При обновлении сертификата APNS не забудьте войти в систему с Apple ID, указанным в Шаге 3, а также обновить ранее использованный сертификат и НЕ создавать новый. Вы увидите "тему" сертификата APNS в Шаге 3 и при нажатии на "i" на портале сертификатов Apple Push. Это уникальный ID, который идентифицирует сертификат. Это поможет Вам определить правильный и обновить его.

Когда Вы получаете сообщение "Ошибка: Сертификат Push имеет другую тему!" при обновлении, это означает, что Вы обновили другой сертификат или создали новый.

Если Вы хотите загрузить новый сертификат, например, если Вы больше не можете получить доступ к ранее использовавшемуся Apple ID, Вам сначала нужно удалить текущий загруженный сертификат.

В любом случае, удаление сертификата APNS означает, что Вы больше не сможете вносить изменения в текущие зарегистрированные устройства, пока не зарегистрируете их снова. Поэтому убедитесь, что Вы готовы к этому, и удаляйте сертификат только в том случае, если нет другого выхода.

Управляемый доступ

Здесь Вы можете включить функцию User-Enrollment для iOS-устройств и Shared iPad для iOS-устройств.

Зачисление пользователей

'User Enrollment' включает специальный режим для устройств BYOD.

Для каждого пользователя в Apple Business Portal должен быть создан управляемый Apple-ID.

В процессе регистрации пользователей попросят ввести учетные данные Apple-ID.

'User Enrollment' гарантирует максимальную безопасность для пользователя, поскольку позволяет MDM настраивать только ограниченный набор параметров и ограничений.

Управляемый домен:

Домен, используемый для сопоставления адреса электронной почты пользователя с его управляемым Apple-ID (должен быть в формате: '@appleid.company.com'). Например, john.doe@example.com будет сопоставлен с john.doe@appleid.company.com.

Проверьте Apple Business Manager, чтобы увидеть Ваш управляемый домен.

Совместное использование iPad

Общий iPad - это устройство DEP, сконфигурированное со специальным профилем DEP.

Это позволит нескольким пользователям входить в устройство, используя свой управляемый Apple-ID.

Управляемый Apple-ID должен быть создан в Apple Business Portal или Apple School Manager.

Пользователей, которые входят в общий iPad, просят ввести их управляемые учетные данные Apple-ID.

Управляемый домен:

Домен, используемый для сопоставления адреса электронной почты пользователя с его управляемым Apple-ID (должен быть в формате: '@appleid.company.com'). Например, john.doe@example.com будет сопоставлен с john.doe@appleid.company.com.

Проверьте Apple Business Manager, чтобы увидеть Ваш управляемый домен.

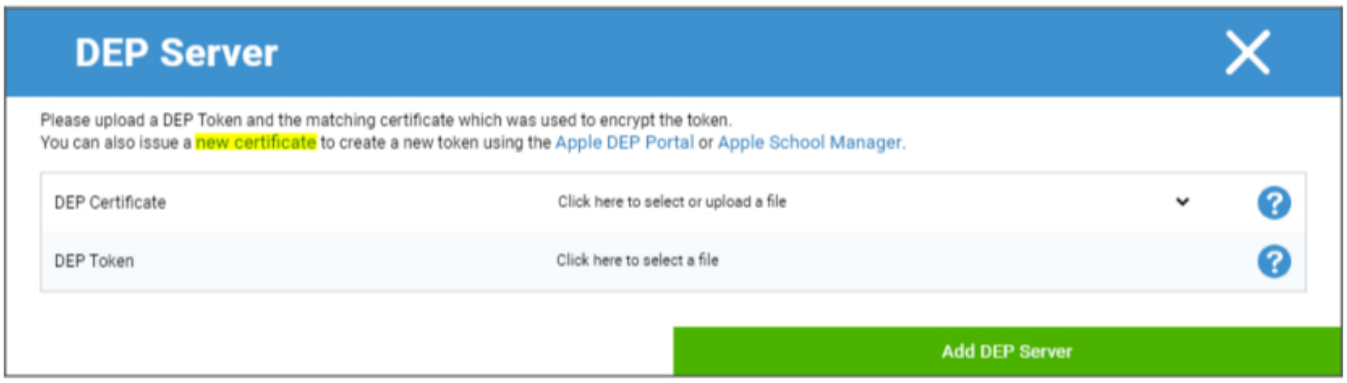
DEP

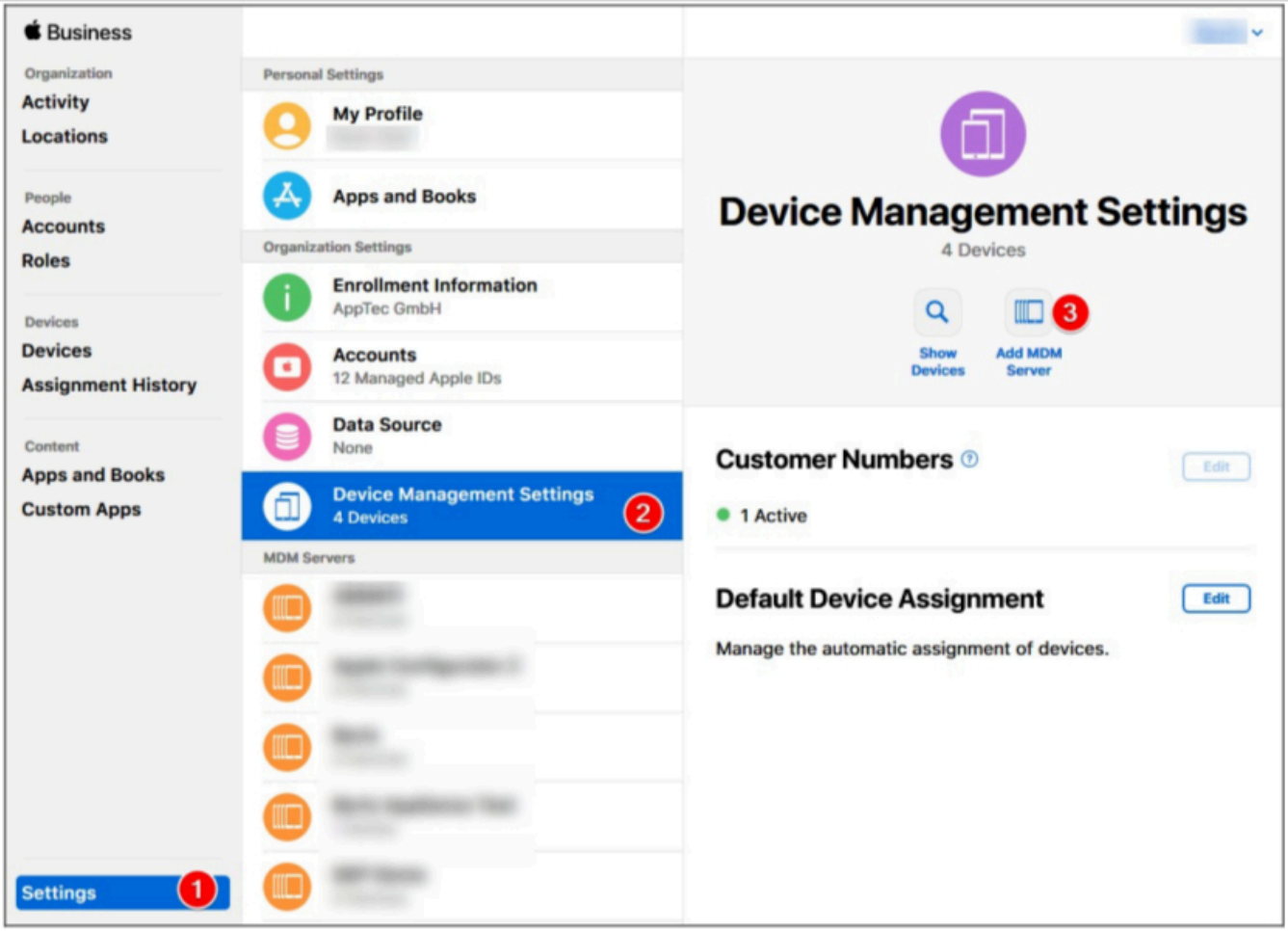
DEP (Device Enrollment Program) позволяет Вам легко регистрировать устройства в MDM. При использовании DEP устройства будут автоматически подключаться к MDM при настройке устройства. Вы также можете пропустить почти все этапы настройки, которые обычно являются обязательными в iOS.

Имейте в виду, что Вам необходимо покупать устройства у реселлера, который поддерживает DEP. За дополнительной информацией обращайтесь к своему реселлеру или в Apple.

Дополнительная информация о DEP: https://www.apple.com/business/dep/

Нажмите на "+", чтобы добавить DEP-токен. Во всплывающем окне нажмите на "новый сертификат" в тексте (выделено желтым на изображении ниже). В результате будет сгенерирован и загружен сертификат DEP. После этого перейдите в Apple Business Manager(https://business.apple.com/) или Apple School Manager(https://school.apple.com/).

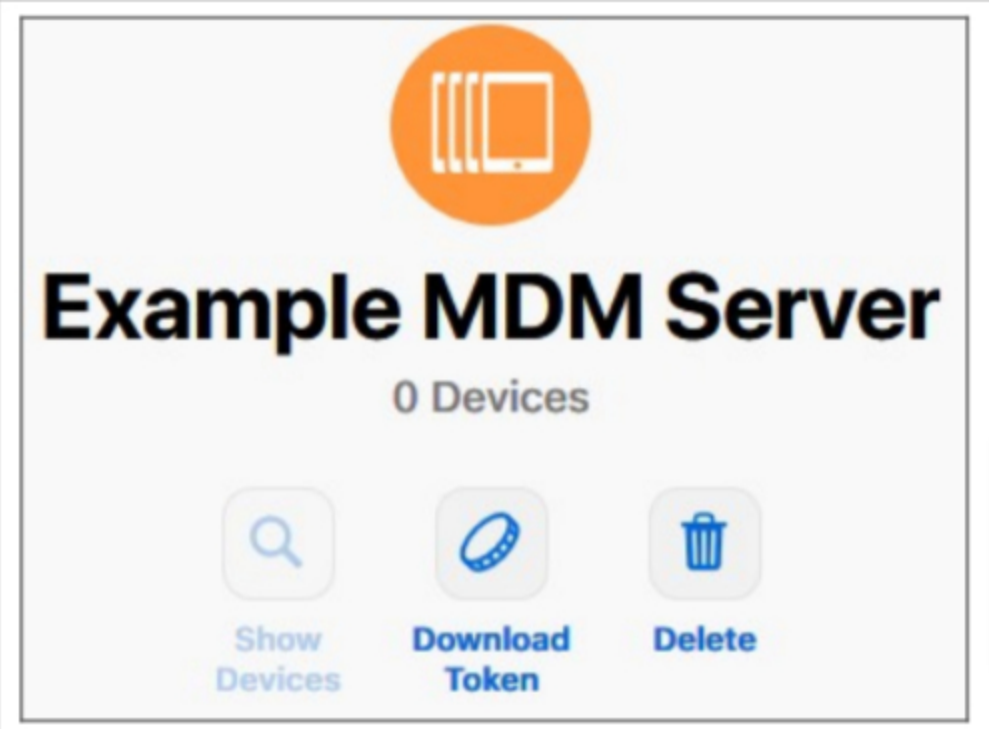




В Apple Business Manager выполните действия, как показано на изображении выше. Настройки → Настройки управления устройствами → Добавить MDM-сервер.

Дайте серверу любое имя и загрузите ранее скачанный DEP-сертификат в разделе MDM Server Settings → Upload Public Key и нажмите "Save".

Теперь у Вас появится опция "Загрузить токен". Нажмите на нее и сохраните. Токен действителен только в течение 1 года. Но просто нажав "Загрузить токен" еще раз, Вы получите новый, что значительно упрощает продление срока действия токена.



Теперь Вы можете вернуться в MDM, где Вы ранее загрузили сертификат DEP. Если Вы не закрыли вкладку, всплывающее окно для добавления сервера DEP должно быть по-прежнему открыто, а сертификат DEP уже должен быть выбран. Теперь Вы можете загрузить свой токен в поле "DEP Token" и нажать на DEP Server.

В колонке "**Устройства**" Вы увидите количество устройств, назначенных этому серверу DEP. Устройства, добавленные к этому серверу DEP, будут автоматически созданы в пуле DEP в Mobile Management.

Вы можете нажать на этот номер, чтобы получить обзор всех Ваших устройств DEP и их состояния.

Примечание: В зависимости от Вашего рабочего процесса или конфигурации в Business Manager может оказаться, что Вам придется вручную назначить эти устройства на сервер DEP Server. Вы также можете установить сервер DEP по умолчанию в Apple Business Manager для новых устройств.

В колонке "**Профили**" Вы видите количество имеющихся у Вас профилей DEP. Вы также можете нажать на это число, чтобы просмотреть подробную информацию о Ваших профилях DEP, и

здесь же Вы можете удалить старые/неиспользуемые профили. В настоящее время изменить их невозможно. Если Вы хотите внести изменения, Вам необходимо создать новый профиль.

В колонке "**Последняя синхронизация**" Вы можете вручную синхронизировать сервер DEP (например, если Вы только что добавили новое устройство в DEP) и увидеть дату последней успешной синхронизации.

В колонке "**Автопрофиль**" Вы можете установить профиль DEP в качестве автоматического по умолчанию. Этот профиль будет автоматически назначаться новым устройствам. Если Вы не установите автопрофиль, Вам придется каждый раз вручную назначать профиль новым устройствам.

В колонке "**Добавить профиль**" Вы можете добавить новый профиль DEP. Устройство получит его в начале настройки устройства. Профиль DEP определяет, как настраивается устройство и какие этапы настройки будут пропущены.

Примечание: после регистрации устройства эти настройки можно изменить, только выполнив сброс к заводским настройкам и зарегистрировав устройство в новом профиле. Это особенно актуально для параметров "**Съемный**" и "**Разрешить сопряжение**". В случае с "**Разрешить сопряжение**" рекомендуется включить эту настройку, поскольку ее можно отключить с помощью MDM-ограничений, но ее нельзя включить снова, если она была отключена в профиле DEP.

В колонке "**Редактировать**" Вы можете загрузить новый токен, например, при обновлении токена.

Конфигуратор и URL

URL-адрес записи в бассейн

Здесь Вы можете создать URL-адрес регистрации и QR-код регистрации, которые будут действительны в течение определенного времени и до определенной даты. Это позволит Вам зарегистрировать несколько устройств, используя только одну ссылку или QR-код.

Устройства, зарегистрированные с помощью этого URL или QR-кода, попадут в пул в Mobile Management, и Вам придется вручную назначить их группе или пользователю.

Примечание: это только для ручной регистрации. Не используйте этот URL, если Вы регистрируете устройства через Apple Configurator

Профиль MDM — Apple Configurator

Здесь Вы можете получить URL, необходимый для регистрации устройств с помощью Apple Configurator. При подготовке устройств с помощью Apple Configurator Вы можете добавить устройства в MDM в том же процессе. Apple Configurator требует для этого данный URL.

Устройства, добавленные через Apple Configurator, будут находиться в пуле в Mobile Management, и Вам придется вручную назначить их группе или пользователю.

Вы также найдете здесь файл .mobileconfig, который можно использовать для регистрации устройств через Apple Configurator. В любом случае, рекомендуется использовать URL.

Конфигурация Android

Конфигурация Android

Удаление защиты	Если эта функция активирована, пользователь не сможет деактивировать администратора устройства, не введя пароль, установленный администратором MDM. Пароль задается во время регистрации, поэтому для обновления пароля устройства должны быть зарегистрированы заново. Есть два варианта удаления администраторов устройства: 1. Вручную на устройстве ◦ Откройте приложение EMM на устройстве ◦ Переключитесь на вкладку Статус ◦ Нажмите на "Удалить защиту". ◦ Введите пароль Вы можете использовать Ревизию для получения правильного пароля из "Истории паролей" в консоли. ◦ Прокрутите страницу вниз и нажмите на недавно добавленный пункт "Нажмите, чтобы удалить AppTec360 MDM App" (у Вас есть 20 секунд на выполнение этой задачи) ◦ Подтвердите диалог "Uninstall AppTec360 MDM App" нажатием "ok". В результате устройство будет удалено из консоли. ◦ Чтобы удалить приложение с устройства, подтвердите диалог "AppTec360 MDM будет удалено" нажатием кнопки "UNINSTALL". 2. автоматический (Консоль) ◦ Выберите устройство в консоли ◦ Нажмите на синий значок шестеренки и выберите "Enterprise Wipe".

	Примечание: Доступно только с Android 4.x и более низкими версиями или на устройствах с KNOX API (устройства Samsung).
Пароль деинсталляции (Пересмотр x)	Установленный пароль, с помощью которого пользователь может удалить администратора устройства Revision x = счетчик, сколько раз пароль уже менялся Важно, какой пароль нужен пользователю, потому что возможно, что устройство не связалось с AppTec360 Server и поэтому самый новый пароль еще не был передан.
История паролей	Когда Вы нажмете на синюю кнопку ("Показать историю"), Вы сможете просмотреть ранее установленные пароли
Расширенная защита от деинсталляции	Эта опция обеспечивает защиту от устройств, не относящихся к классу SAFE Пока эта настройка активирована, невозможно легко деактивировать администратора устройства.
Предложить пользователю удалить заблокированные приложения?	Если возможно, заблокированные приложения будут не только заблокированы, но и автоматически удалены. Если автоматическое удаление невозможно, пользователю будет предложено удалить заблокированные приложения.
Интеллектуальная система блокировки приложений	Если включен режим Whitelisting, Android MDM Client блокирует все установленные пользователем приложения. Включите эту настройку, чтобы блокировать все запускаемые системные приложения в режиме Whitelisting.

Автоматическое зачисление

Здесь Вы можете включить функцию Auto Enrollment, чтобы Ваши устройства регистрировались автоматически при открытии AppTec360 MDM Client на устройстве.

Важно: Этот метод регистрации устарел и больше не работает на Android 10 и выше. В любом случае, если Вы используете Android 7 или выше, Вы должны регистрировать устройства как полностью управляемые Android Enterprise. Если Вы хотите использовать контейнер Android Enterprise BYOD и работаете на Android 10 или выше, Вам придется вручную зарегистрировать устройство с помощью учетных данных, QR-кода или SMS. В любом случае, список авторегистрации по-прежнему используется для автоматизации процесса регистрации, например, AE Enrollment, Knox Enrollment и т.д.

В любом случае, список автоматического зачисления по-прежнему используется для автоматизации процесса зачисления, например, AE Enrollment, Knox Enrollment и т.д.

Щелкнув на "Serial Manager" или "IMEI Manager", Вы можете добавить серийный номер или IMEI Ваших устройств соответственно. Не обязательно делать оба варианта для Ваших устройств, достаточно одного.

Действие определяет, будут ли устройства зачислены в пул, пользователя или группу.

Вы также можете экспортировать и импортировать файл .csv и фильтровать записи по ключевым словам.

Android Enterprise

Здесь Вы можете настроить Android Enterprise. Это необходимо для использования всех возможностей Android Enterprise.

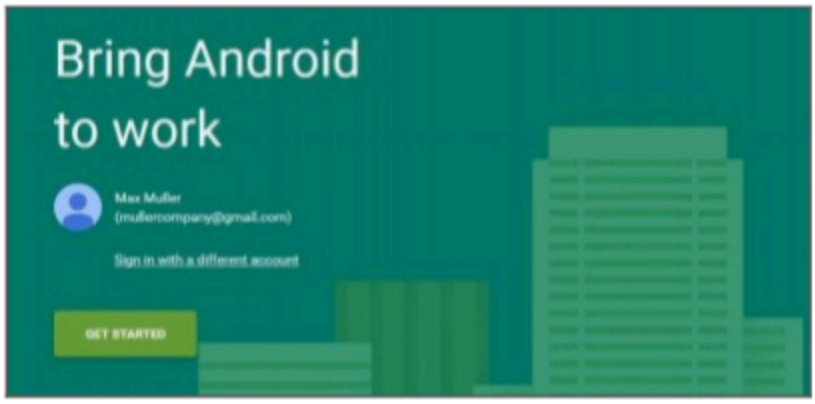
Первый способ: Корпоративная учетная запись Android (Google Account)

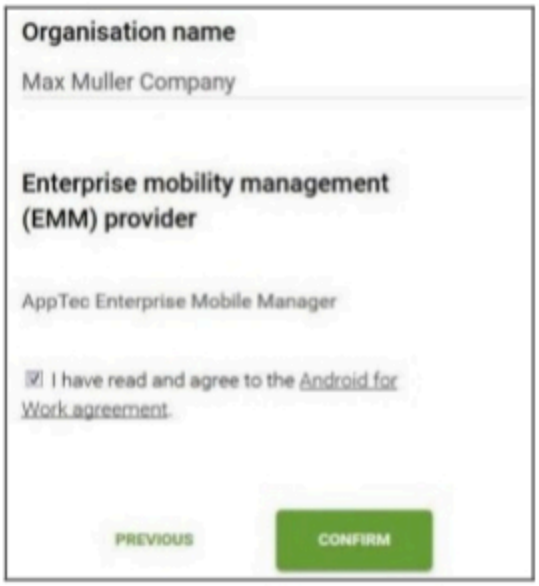
Сначала нажмите кнопку "Prepare Setup", а через некоторое время должна появиться кнопка "Start Setup".

Это приведет Вас на страницу настроек Google Android Enterprise.

Войдите в аккаунт Google, который Вы хотите использовать, если Вы еще не вошли в него, и нажмите "Начать".

Теперь Вы можете ввести название Вашей компании. После этого установите флажок и нажмите "Подтвердить".





На последнем шаге Вы можете завершить регистрацию и должны вернуться в консоль. Если все получилось, она должна выглядеть следующим образом:

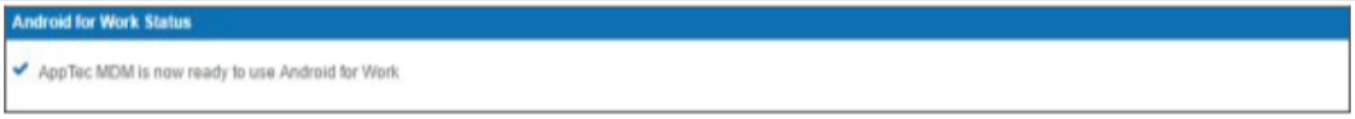
Теперь Вы можете приступить к настройке Вашего Android Enterprise Container.

Второй способ: Учетная запись G-Suite

Нажмите "Use G-Suite" и войдите в свою учетную запись Google Admin. Там Вы перейдете в раздел "Безопасность" -> "Показать больше" -> "Управление EMM-провайдером для Android" и сгенерируете токен. Примечание: Если в Вашем аккаунте G-Suite не отображаются корпоративные настройки Android, Вам необходимо перейти в раздел "Получить больше приложений и сервисов" и добавить управление устройствами Android. Теперь введите Токен и Ваш основной Домен в нашей консоли и нажмите на "Сохранить изменения". Когда Вы закончите, нажмите на "Использовать учетную запись Android Enterprise".

Теперь Вы должны увидеть кнопку "Создать учетную запись сервиса". Нажмите на нее. Этот процесс может занять несколько мгновений.

Если все работает, то это должно выглядеть следующим образом:



Теперь Вы можете приступить к настройке Вашего Android Enterprise Container.

Защита от сброса к заводским настройкам

С помощью функции Factory Reset Protection Вы можете привязать свое устройство к выбранной Вами учетной записи google, которая также отменяет все существующие привязки к учетным записям google. Чтобы использовать Factory Reset Protection, Вам необходимо сначала настроить ее здесь, а затем активировать в своих профилях.

Чтобы настроить защиту от сброса к заводским настройкам, нажмите на "FRP Setup" и следуйте инструкциям на экране.

ПРИМЕЧАНИЕ: Внимательно прочитайте и выполните все шаги. Мы рекомендуем делать это в новом окне браузера инкогнито, чтобы избежать автоматического входа в неправильный аккаунт Google. Вы можете полностью лишить себя доступа к устройству, если введете неправильный ID или потеряете доступ к используемому Аккаунту Google!

Зачисление AE

Здесь Вы можете активировать Android Enterprise Ernollment. Использование этого метода переведет Ваши устройства в режим владельца устройства Android Enterprise. В этом режиме у Вас будет полный контроль над устройством.

Включить регистрацию AE	Активирует AE Enrollment Внимание: Если Вы отключите AE Enrollment, существующие QR-коды и уже настроенные устройства NFC-программатора перестанут работать. Если Вы снова включите AE Enrollment, Вам придется заново отправлять конфигурации NFC push / генерировать новые QR-коды.
Включить автоматическое обнаружение	Когда устройство регистрируется с помощью "AE Enrollment", система попытается назначить его пользователю на основе информации, заданной в Серийном / IMEI белом списке ("Общие настройки" > "Конфигурация Android" > "Авторегистрация").
Блокировка неизвестных устройств	Только устройствам, внесенным в белый список серийного номера / IMEI ("Общие настройки" > "Конфигурация Android" > "Автозачисление"), разрешено зачисление.

Примечание к Методу 1 и 2: "Экран приветствия" означает первый экран, который Вы видите после сброса настроек на заводские. Он может выглядеть по-разному в зависимости от версии андроида и/или модели устройства, которое Вы используете.

Способ 1: Зачисление по QR-коду

(требуется Android 7.0 или выше) Мы рекомендуем всегда использовать этот метод, если Вы работаете под управлением Android 7 или выше.

1. Сброс настроек устройства к заводским установкам
2. Сгенерируйте QR-код для регистрации, используя один из двух следующих методов:
   - Нажмите в разделе "Общие настройки -> Конфигурация Android -> AE Enrollment" на "Сгенерировать QR-код". Выберите, хотите ли Вы пропустить шифрование памяти и/или удалить все системные приложения.
   - (альтернативный вариант) Выберите существующее устройство. В разделе "Обзор устройства" нажмите на отображаемый там QR-код. Выберите, хотите ли Вы пропустить шифрование хранилища и/или удалить все системные приложения.
3. Теперь нажмите 6 раз на экране приветствия Вашего устройства. Это запустит режим QR-регистрации.
4. Теперь подключитесь к беспроводной сети и подождите некоторое время, пока не установится устройство для считывания QR-кодов
5. Теперь отсканируйте QR-код

6. Вот и все. Теперь Ваше устройство включено в режим Android Enterprise Device Mode.
    - a. Если Вы использовали QR-код в "Общих настройках", Вы можете найти свое устройство в разделе "Пул -> Устройства владельца устройства AE". (Подсказка: возможно, Вам придется перезагрузить сайт, чтобы увидеть устройства). Если Вы отметили "Включить автообнаружение", Вы найдете его внутри пользователя Auto Discover.
    - Если Вы использовали QR-код существующего профиля устройства, устройство будет занесено в этот профиль.

Способ 2: Регистрация NFC

(требуется NFC и Android 6.0 или выше)

Подготовка: Введите информацию о Вашем WiFi в "General Settings -> Android Configuration -> AE Enrollment -> Data for NFC provisioning". Теперь используйте "NFC Device" для поиска устройства, которое станет программатором. Это устройство будет использоваться для передачи информации о зачислении на другие устройства через NFC.

1. Сброс настроек на заводские параметры Вашего устройства
2. Откройте приложение для сопряжения NFC из AppTec360 на Вашем программаторе
3. Выберите, хотите ли Вы пропустить шифрование памяти и/или удалить все системные приложения.
4. Держите оба устройства спиной друг к другу
5. Теперь Android Enterprise Enrollment должен стать ярким
6. Теперь Вы найдете свое устройство в консоли
    - a. В пуле, если Вы не настроили Автообнаружение
    - b. Внутри пользователя, которого Вы настроили на автообнаружение
    - c. Подсказка: Возможно, Вам придется перезагрузить сайт, чтобы увидеть устройства

Способ 3: Аккаунт Google

(требуется Android 5.1 или выше)

(Примечание: Если Вы используете этот метод, устройство не будет зачислено автоматически. Вместо этого Вам придется зарегистрировать его вручную или автоматизировать процесс с помощью Авторегистрации).

1. Сброс настроек на заводские параметры Вашего устройства
2. Пройдите все шаги по настройке, пока не сможете войти в систему с помощью учетной записи google.
3. Введите "afw#apptec" в качестве имени пользователя/почты
4. Нажмите "Далее".

5. Теперь Ваше устройство является устройством Android Enterprise Device

Зачисление в KNOX

Здесь Вы можете активировать KNOX Enrollment и найти информацию, необходимую для создания профиля KNOX Enrollment Profile в KNOX Deployment Portal. Для настройки и использования этой функции Вам необходима учетная запись на KNOX Deployment Portal.

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

Включить регистрацию KNOX	Активирует функцию KNOX Enrollment. Внимание: Если Вы отключите KNOX Enrollment, существующие профили MDM перестанут работать. Если Вы снова включите KNOX Enrollment, Вам придется обновить поле "Custom JSON Data" в Вашем MDM-профиле.
Включить автоматическое обнаружение	Когда устройство регистрируется через "KNOX Enrollment", система попытается назначить его пользователю, основываясь на информации, заданной в Серийном / IMEI белом списке ("Общие настройки" > "Конфигурация Android" > "Авторегистрация").

1. Войдите в портал Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin.
2. Перейдите в раздел "Профили MDM".
3. Нажмите "Добавить".
4. Выберите "Server URI not required for my MDM" и нажмите "Next".
5. Теперь создайте профиль с информацией, показанной в консоли управления

Теперь этот профиль регистрации KNOX может быть установлен на устройство непосредственно компанией Samsung, если Вы приобретаете устройства непосредственно у Samsung.

В качестве альтернативы Вы можете скачать приложение KNOX Deployment App, войти в систему под своей учетной записью KNOX Deployment Account и отправить профиль регистрации KNOX Enrollment Profile через NFC на другие устройства.

Если на устройстве установлен KNOX Enrollment Profile, оно загрузит наше приложение и зарегистрирует устройство, если у него есть рабочее подключение к Интернету.

Регистрация устройств с помощью KNOX Enrollment находится в разделе "Pool -> KNOX Enrollment", или под пользователем, которого Вы указали в Auto Discover.

Zero-Touch

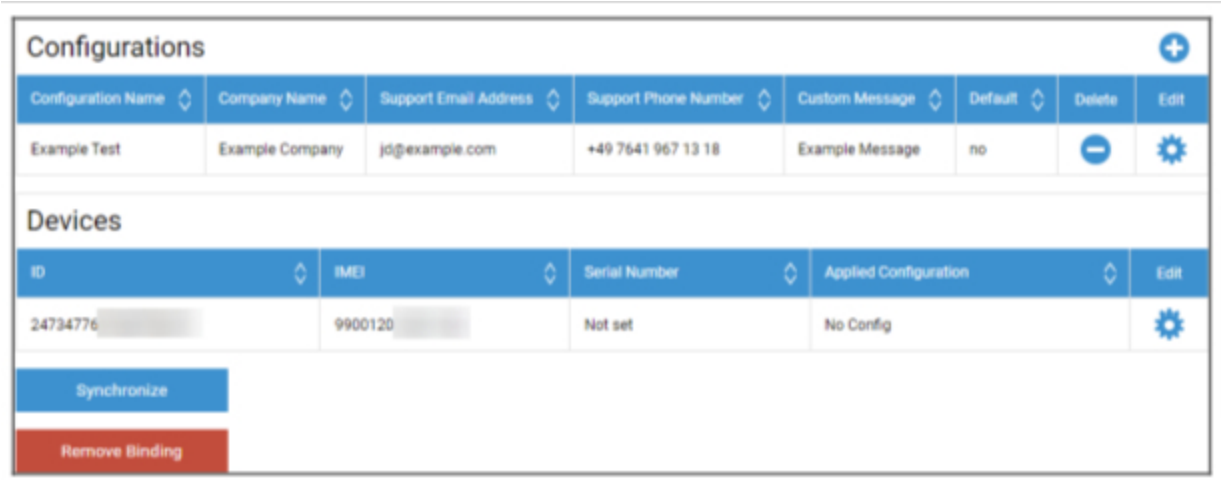
С помощью Zero-Touch Вы можете легко регистрировать свои устройства, не прикасаясь к ним и не настраивая ничего на самом устройстве. Вам просто нужно включить его, выполнить обычную настройку, и устройство получит всю информацию о том, как настроить и подключиться к MDM, совершенно автоматически.

Чтобы использовать Zero-Touch, Вы должны купить свои устройства у реселлера, который поддерживает Zero-Touch. Этот же реселлер создает для Вас учетную запись на Портале Zero-Touch. Свяжитесь с Вашим дилером, чтобы получить дополнительную информацию о процедуре или если у Вас возникли проблемы с доступом к Порталу Zero-Touch.

Нажмите на кнопку "Начать настройку", чтобы начать настройку. Вы будете перенаправлены на страницу входа в систему, где Вам необходимо выбрать Вашу учетную запись Google, которая имеет доступ к порталу Zero-Touch.

ПРИМЕЧАНИЕ: Можно выбрать ЛЮБУЮ учетную запись. Поэтому убедитесь, что выбрали правильную Учетную запись на этом шаге. Если Вы не видите своих устройств/настроек, скорее всего, Вы использовали неправильную Учетную запись.

После завершения входа в систему она будет выглядеть следующим образом:



Нажмите на "+", чтобы добавить конфигурацию, и заполните поля, как показано на экране. Если Вы включите конфигурацию в качестве конфигурации по умолчанию, она будет назначена новым устройствам автоматически. Создание или установка конфигурации по умолчанию не назначает ее уже существующим устройствам.

Если устройству не назначена Конфигурация, оно будет настроено как обычное устройство и не подключится к MDM. Поэтому убедитесь, что Вашим устройствам назначена Конфигурация.

После того, как Вы подключили свою учетную запись, Ваши устройства стали видимыми и им назначена конфигурация, Вы можете приступить к настройке устройств.

Вы можете добавить устройства в список автозачисления, чтобы они автоматически зачислялись в указанную группу или пользователя. Если Вы ничего не настроили в списке Автозачисление, устройства будут зачислены в Пул.

Конфигурация Windows

Конфигурация Windows

Здесь у Вас есть возможность включить следующие конфигурации на Вашем ПК с Windows 10:

Мгновенное подключение DM	
Начальное время повтора	Устанавливает первую попытку соединения с устройством, это значение увеличивается экспоненциально
Повторные попытки подключения	Указывает, сколько попыток соединения должен выполнить DM-клиент во время ошибки соединения
Максимальное время сна	Указывает максимальное время сна после ошибки соединения
Первые повторные попытки синхронизации	Интервалы, через которые устройство должно связываться с сервером после первого соединения
Первый интервал повторных попыток	Относится к "Первым повторным попыткам синхронизации". Здесь время указано в минутах. Например, в разделе "First Sync Retries" указано значение "2", а в разделе "First Retry Interval" указано значение "4 Minutes", таким образом, устройство будет связываться 2 раза каждые 4 минуты, после первого соединения.
Повторные попытки синхронизации	Интервалы, через которые устройство должно связываться с сервером после завершения "First Sync Retries".
Второй интервал повторных попыток	Тот же принцип, что и для "First Retry Interval" - только здесь он применяется к "Second Sync Retries".
Регулярные повторные попытки синхронизации	Интервалы, как часто устройство должно общаться с сервером в будущем По умолчанию: "Бесконечный" Мы не рекомендуем изменять это значение, потому что если Вы введете "10", устройство будет общаться с сервером 10 раз, а затем остановится. Таким образом, связь с сервером AppTec360 прервется!
Регулярный интервал повторных попыток	Принцип тот же, что и для "Первого/второго интервала повторных попыток" - просто здесь применяются настройки на будущее

Регулярный интервал повторных попыток	Принцип тот же, что и для "Первого/второго интервала повторных попыток" - просто здесь применяются настройки на будущее

ContentBox

Конфигурация

Здесь Вы можете настроить ContentBox. Вы можете поместить в ContentBox файлы для групп, доступ к которым можно получить с помощью приложения ContentBox App на устройстве.

Включить ContentBox	Включите ContentBox. Отключение этого параметра, если Вы не используете ContentBox, может сэкономить ресурсы на машинах OnPremise.
Используйте внешнюю установку ContentBox	ContentBox также может работать с Вашим собственным облаком Nextcloud.
URL	Полный URL-адрес объекта Nextcloud
Корневой пользователь	Корневой пользователь учетной записи Nextcloud
Корневой пароль	Корневой пароль учетной записи Nextcloud
Разрешения групповых папок по умолчанию	Разрешения групповых папок по умолчанию, могут быть индивидуально изменены группой (в Mobile Management)
Совместное использование групповой папки с подгруппами	Если эта функция активна, каждая подгруппа может читать все папки основной группы, также может быть индивидуально настроена для каждой группы (Управление мобильными устройствами).
Разрешения для подгрупп	Разрешения для подгрупп может быть индивидуально настроен для каждой группы (Управление мобильными устройствами)
Разрешить совместное использование	Позволяет пользователю делиться содержимым с помощью ссылок, может быть индивидуально настроен для каждой группы
Максимальный размер загружаемого файла в МБ	Максимальный размер файла Стандарт: 512 МБ Максимальная конфигурация: 2048
Учетные данные WebDAV	
URL WebDAV	Вы также можете открыть ContentBox с помощью WebDAV. Пожалуйста, ни при каких обстоятельствах не удаляйте следующие папки: /apptecgroups /apptecgroups/AppTecGroup-X
Корневой пользователь	Имя корневого пользователя

Пароль	Пароль корневого пользователя

Синхронизация с ContentBox происходит автоматически. Однако Вы можете выполнить синхронизацию вручную с помощью команды "Synchronize ContentBox".

Кроме того, здесь Вы можете активировать/деактивировать ContentBox на каждом отдельном устройстве.

Это актуально только в том случае, если у Вас нет дополнительной лицензии на ContentBox, тогда у Вас все еще есть доступ к 25 устройствам, с помощью которых Вы можете протестировать ContentBox - здесь Вы можете активировать это для соответствующих устройств.

Конфигурация LDAP

Обзор LDAP

Здесь Вы можете установить соединение с Вашей Active Directory через LDAP для массового импорта пользователей и групп. Синхронизация должна быть выполнена вручную. Вы можете настроить несколько LDAP-соединений с разными системами или с разными конфигурациями/ фильтрами.

Имя сервера	Отображаемое имя сервера
Тип	В настоящее время поддерживаются только Active Directories, которые поддерживают LDAP
Домен LDAP	Основной домен LDAP (например, example.com)
LDAP Host	Это необходимо только в том случае, если хост LDAP недоступен для данного домена LDAP.
Порт	Оставьте пустым, чтобы использовать стандартный порт (389 или 636 для SSL).
Имя пользователя	Например, CN=John,OU=Users,DC=EXAMPLE,DC=COM Примечание: Большинство систем требуют имя пользователя в этом формате и не принимают "John" в качестве имени пользователя.
Пароль	
Подтверждение пароля	
Безопасность соединения	Примечание: при использовании SSL или TLS будет проверен сертификат Active Directory. Если он самоподписанный, Вам необходимо добавить корневой центр сертификации в хранилище доверия на локальной машине. Если Вы находитесь в облаке, Active Directory должна предоставить доверенный сертификат, иначе соединение будет работать только без шифрования.
Автоматическая синхронизация.	Включает автоматическую синхронизацию каталога LDAP через временной интервал, указанный в общих настройках LDAP.
Базовый DN	Если Вы не хотите синхронизировать всю директорию, Вы можете указать здесь OU. Например, OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Член	Все импортированные пользователи будут добавлены в выбранную группу

Только активированные пользователи?	При включении будет учитываться атрибут userAccountControl, пользователи без этого атрибута не будут импортированы.
Фильтр LDAP	Вы можете использовать фильтр LDAP Filter, чтобы отфильтровать, какие пользователи будут импортированы
Регекс-фильтр	Вы можете использовать фильтр Regex Filter, чтобы отфильтровать, какие пользователи будут импортированы
Тестовое соединение	Проверяет соединение при сохранении конфигурации
Сбросить структуру каталогов при синхронизации?	Если значение true, все записи LDAP будут перемещены обратно в исходное положение в дереве LDAP. Рекомендуется включить.
Повторно импортировать удаленных пользователей и группы?	Когда эта функция включена, пользователи и группы, которые были удалены, будут созданы заново. Рекомендуется включить.
Синхронизировать удаления?	Если эта опция включена, группы и пользователи будут удалены, когда они будут удалены на сервере LDAP. Также будут удалены устройства удаленных пользователей.

Под списком Ваших LDAP-конфигураций Вы можете определить период, в течение которого система будет автоматически синхронизироваться. Для автоматической синхронизации используются только те LDAP-конфигурации, у которых активирована соответствующая опция.

Управление приложениями

Внутренняя база данных приложений

Android

Здесь Вы можете загрузить приложения для Android, которые разработала Ваша компания, и позже распределить их в Mobile Management в профилях устройств или групп.

Пожалуйста, имейте в виду, что мы советуем распространять таким образом только те приложения, которые не доступны в Google Play Store.

Нажмите на "+", чтобы загрузить APK приложения, которое Вы хотите загрузить. В настоящее время поддерживается только формат APK.

Лимит загрузки на OnPremise Appliances может быть увеличен на Шаге 3 конфигурации Appliance Configuration. Если Вы хотите увеличить лимит загрузки на облачных устройствах, пожалуйста, обратитесь в службу поддержки для получения дополнительной информации.

Имейте в виду, что обычно APK немного меньше, чем их содержимое. Возможно, что загрузка не удастся из-за этого, поскольку APK распаковывается в процессе. Например, возможно, что APK размером 95 МБ не удастся загрузить при лимите загрузки 100 МБ. В этом случае увеличьте лимит загрузки, как указано выше.

Мы также советуем сначала вручную перенести APK на одно тестовое устройство (например, через USB) и попытаться установить его вручную с помощью приложения "Файлы" на устройстве. Если по какой-то причине это не сработает, то не получится и с помощью MDM.

Обновление цели

С помощью функции "Update Target" Вы можете выбрать, какая версия приложения должна быть установлена или до какой версии должно быть обновлено приложение, если Вы активировали функцию "Keep up to date" для приложения.

Если Вы не выбрали цель обновления, будет использоваться самая высокая версия.

Имейте в виду, что Android не может понижать версии приложений. Также имейте в виду, что "Код версии" определяет, является ли версия выше, ниже или такой же. Поэтому при создании обновления убедитесь, что Вы правильно увеличили эту версию в своем приложении.

iOS

Здесь Вы можете загрузить разработанные Вами приложения для iOS и распространить их позже в Mobile Management в профиле Вашего устройства или группы.

Нажмите на "+", чтобы загрузить IPA приложения, которое Вы хотите загрузить. На данный момент поддерживается только формат IPA.

Лимит загрузки на OnPremise Appliances может быть увеличен на Шаге 3 конфигурации Appliance Configuration. Если Вы хотите увеличить лимит загрузки на облачных устройствах, пожалуйста, обратитесь в службу поддержки для получения дополнительной информации.

Обновление цели

С помощью функции "Update Target" Вы можете выбрать, какая версия приложения должна быть установлена или до какой версии должно быть обновлено приложение, если Вы активировали функцию "Keep up to date" для приложения.

Если Вы не выбрали цель обновления, будет использоваться самая высокая версия.

MacOS

Здесь Вы можете загрузить разработанные Вами приложения для MacOS и распространить их позже в Mobile Management в профиле Вашего устройства или группы.

Нажмите на "+", чтобы загрузить PKG приложения, которое Вы хотите загрузить. На данный момент поддерживается только формат PKG.

Лимит загрузки на OnPremise Appliances может быть увеличен на Шаге 3 конфигурации Appliance Configuration. Если Вы хотите увеличить лимит загрузки на облачных устройствах, пожалуйста, обратитесь в службу поддержки для получения дополнительной информации.

Обновление цели

С помощью функции "Update Target" Вы можете выбрать, какая версия приложения должна быть установлена или до какой версии должно быть обновлено приложение, если Вы активировали функцию "Keep up to date" для приложения.

Если Вы не выбрали цель обновления, будет использоваться самая высокая версия.

Windows 10

Здесь Вы можете загрузить приложения Windows 10 Apps и распространить их позже в Mobile Management в профиле Вашего устройства или группы.

Нажмите на "+", чтобы загрузить APPX, APPXBUNDLE или MSI приложения, которое Вы хотите загрузить. На данный момент поддерживается только формат APPX, APPXBUNDLE или MSI.

Вы также можете загрузить и определить Зависимости для приложения, которые будут автоматически распространяться и устанавливаться перед установкой нужного приложения.

Лимит загрузки на OnPremise Appliances может быть увеличен на Шаге 3 конфигурации Appliance Configuration. Если Вы хотите увеличить лимит загрузки на облачных устройствах, пожалуйста, обратитесь в службу поддержки для получения дополнительной информации.

Обновление цели

С помощью функции "Update Target" Вы можете выбрать, какая версия приложения должна быть установлена или до какой версии должно быть обновлено приложение, если Вы активировали функцию "Keep up to date" для приложения.

Если Вы не выбрали цель обновления, будет использоваться самая высокая версия.

Пакет Win32 (.exe)

Вы также можете распространять файлы .exe/установщики на своих устройствах.

Название пакета	Имя, которое будет отображаться в MDM
Описание	Описание, показанное в MDM
Файл пакета	Разрешается использовать только файлы .zip. Поместите файлы, которые Вы хотите развернуть, в этот zip-файл.
Контекст развертывания	**Система**: Команда установки выполняется с системными привилегиями, которые выше, чем "Пользователь". Также при использовании "System" у процесса нет пользовательского интерфейса, поэтому он будет беззвучным, а профиль пользователя, например, переменные окружения, такие как %AppDat%, будут недоступны. **User**: Команда установки имеет доступ к профилю пользователя и может отображать пользовательский интерфейс, если это необходимо. Примечание: Некоторые процессы могут работать только в одном контексте. Например, если программа установится в AppData, она будет работать только при выборе "Пользователь".
Установите команду	Команда, используемая для установки программы. Например, команда установки для zip-файла, содержащего в корне "setup.exe", который поддерживает параметр "/s" для бесшумной установки, будет выглядеть так: "setup.exe /s". Имейте в виду, что у разных программ могут быть разные параметры.
Команда удаления	Команда, которую нужно выполнить для удаления программного обеспечения через MDM. Обычно она указывает на программу деинсталляции. Например, "C:\Program Files\ExampleSoftware\uninstall.exe".
Требования	
Примечание: Для установки программного обеспечения должны быть выполнены все установленные требования. В противном случае оно не будет установлено. Некоторые поля могут быть обязательными. Если для какого-либо требования не задано значение, оно будет проигнорировано.	
Архитектура ОС	Архитектура ОС
Минимальная версия ОС	Минимальная версия ОС
Минимальное свободное дисковое пространство (МБ)	Минимальное свободное дисковое пространство (МБ)

Минимальная физическая память (МБ)	Минимальная физическая память (МБ)
Минимальное количество логических процессоров	Минимальное количество логических процессоров
Минимальная скорость процессора (МГц)	Минимальная скорость процессора (МГц)
Дополнительные требования	Вы также можете вручную определить правила или загрузить сюда сценарий для выполнения дополнительных проверок требований, если Вам это необходимо.
Правила обнаружения	
Метод обнаружения	Здесь Вы можете определить, как определить, установлено ли приложение на устройстве. Команды установки будут выполняться только в том случае, если эти правила определят, что приложение НЕ установлено. Команды удаления будут выполняться только в том случае, если эти правила определят, что приложение не установлено. **Вручную определить правила**: Позволяет Вам вручную определить одно или несколько правил, чтобы проверить, например, наличие определенного файла, папки, MSI или ключа реестра. Если все заданные правила обнаружения верны, приложение будет считаться установленным. **Использовать скрипт**: Загрузите собственный скрипт с собственными проверками. Если сценарий вернет "$TRUE", приложение будет считаться присутствующим.
Правила обнаружения	

Настройки приложения

Настройки приложений для iOS

Здесь Вы можете определить настройки по умолчанию для добавления приложения в обязательные приложения или в магазин корпоративных приложений.

Примечание: Это только устанавливает то, что выбрано по умолчанию при добавлении приложений. Это НЕ изменит существующие настройки для приложений, которые уже добавлены в обязательные приложения или в магазин корпоративных приложений.

Будьте в курсе событий	Автоматически поддерживает приложение в актуальном состоянии. Пожалуйста, имейте в виду, что после выхода обновления может пройти до 7 дней, прежде чем приложение будет обновлено.
Обгоните, если не управлять	Если приложение уже установлено как неуправляемое (пользователем), оно перейдет под управление MDM.
Удалите приложение при удалении профиля MDM	Удалите приложение, когда MDM будет удален.
Предотвращение резервного копирования данных приложения	Предотвращает резервное копирование данных приложения.

Настройки приложения для Android

Здесь Вы можете определить настройки по умолчанию для добавления приложения в обязательные приложения или в магазин корпоративных приложений.

Примечание: Здесь задается только то, что выбрано по умолчанию при добавлении. Это НЕ изменяет настройки для приложений, которые уже добавлены в обязательные приложения или в магазин корпоративных приложений.

Будьте в курсе событий	Автоматически поддерживает приложение в актуальном состоянии. Доступно только для приложений InHouse Apps.
Обновление клиента Controlled AppTec360 EMM	Если эта опция включена, администраторы могут указать цель обновления для AppTec360 EMM Client. Список всех доступных версий AppTec360 EMM Client будет показан в разделе "Общие настройки" → "Управление приложениями" → "In-House App DB" → "Android".

Сторонние приложения

Android

Здесь Вы можете установить код активации для Ikarus.

Установите значение "Использовать код активации" и введите здесь свой код активации.

Примечание: После ввода кода и сохранения код еще не добавлен в профиль, который отправляется на устройство. Чтобы код был добавлен в профиль, необходимо произвести какие-либо изменения в профиле. Например, измените любой переключатель в профиле с Выкл → Вкл → Выкл - Сохранить → Назначить сейчас.

iOS

Здесь Вы можете ввести свою лицензию SecurePIM. После ввода лицензии нажмите "Сохранить изменения", и Вы сможете пользоваться опциями SecurePIM.

VPP / KNOX Premium

Программа Apples Volume Purchase Program (VPP) позволяет Вам легко распространять платные и бесплатные приложения на своих устройствах. Это очень рекомендуется, поскольку Вам не нужен Apple ID на устройствах, пользователям не нужно подтверждать установку (под наблюдением), пользователям не нужно вводить пароль Apple ID, и Вы можете легко распространять платные приложения, не покупая их на каждом устройстве заново.

Чтобы использовать VPP, Вам необходимо зарегистрироваться в Apple Business Manager.

Лицензии VPP

Здесь Вы можете получить обзор Ваших приложений VPP Apps, узнать, сколько лицензий используется и сколько доступно.

Нажав на колесико, Вы увидите, каким устройствам назначена лицензия и каков статус этого назначения.

При нажатии на кнопку обновляется кэш VPP, который сравнивает лицензии, назначенные в MDM, с лицензиями, назначенными на стороне Apples. В некоторых случаях это может решить проблемы с лицензиями.

Токен VPP

Здесь Вы можете загрузить свой VPP Token, который можно найти в Apple Business Manager в Настройках → Приложения и книги. Вы можете загрузить несколько VPP-токенов.

Вы можете обновить токен, просто загрузив новый в Apple Business Manager, нажав на колесико "Редактировать" и загрузив новый токен.

Режим "VPP Mode" определяет, как будет обрабатываться назначение лицензии. В зависимости от Вашего сценария, Вы должны использовать различные режимы:

"Device based" следует использовать при регистрации устройств с помощью QR-кода, ссылки, Apple Configurator или DEP.

"User based" требуется, если устройства зарегистрированы с помощью User Enrollment или как Shared iPad.

Если Вы включите "Автоматическое управление лицензиями", пользователям, перемещаемым из одной группы в другую, будут автоматически назначены лицензии Apple VPP на основе профиля группы, в которую они перемещены.

Существующие лицензии Apple VPP той группы, из которой они перешли, не будут аннулированы.

Новым пользователям, добавленным в группу, будут автоматически назначены лицензии Apple VPP на основе соответствующего профиля группы.

KNOX Premium Key

Здесь Вы можете ввести свой KNOX Premium Key для использования контейнера Samsung KNOX.

Пожалуйста, имейте в виду, что начиная с Android 10 эта функция больше не поддерживается. Вместо этого используйте Android Enterprise Container.

Настройки App Store

Регион и язык

Здесь Вы можете установить язык и регион по умолчанию для поиска приложений в App Management.

Пожалуйста, имейте в виду, что настройка iTunes также определяет, как система получает информацию об определенных приложениях. Если в Ваших списках есть приложения, которые отображаются странным образом (например, отсутствует значок), возможно, Вы установили регион, в котором данное приложение недоступно.

AE Play Store

Здесь Вы найдете все возможности Play Store для корпоративных устройств Android, чтобы одобрить приложения, загрузить собственные приложения в Play Store или создать собственные веб-приложения.

Утвержденные приложения

Здесь Вы можете получить обзор всех одобренных Вами приложений.

Приложения Play Store

В результате загрузится iFrame, показывающий Play Store. Найдите любое нужное Вам приложение, щелкните на нем и одобрите его. При одобрении приложения Вы также можете указать, что одобрение будет отменено, если необходимые разрешения изменятся. Мы рекомендуем оставить эти настройки по умолчанию при утверждении приложений.

После того, как приложение будет одобрено, Вы сможете добавить его в свои профили.

После одобрения кнопка "Одобрить" сменится на "Отменить одобрение", так что Вы всегда сможете удалить приложения, если они Вам больше не нужны.

Частные приложения

Здесь Вы можете загрузить свое собственное приложение в качестве частного приложения в Google Play Store. Это позволит Вам распространять приложение через службы Googles и обновлять его через них. Преимуществом этого способа является то, что Ваши собственные приложения могут быть установлены без подтверждения пользователя, которое обычно необходимо.

Веб-приложения

Здесь Вы можете создавать Web Apps, которые представляют собой ссылки на определенные веб-страницы, которые можно назначать как Apps.

Вы также можете присвоить этому значку свой собственный значок и дополнительно определить, как именно он будет отображаться.

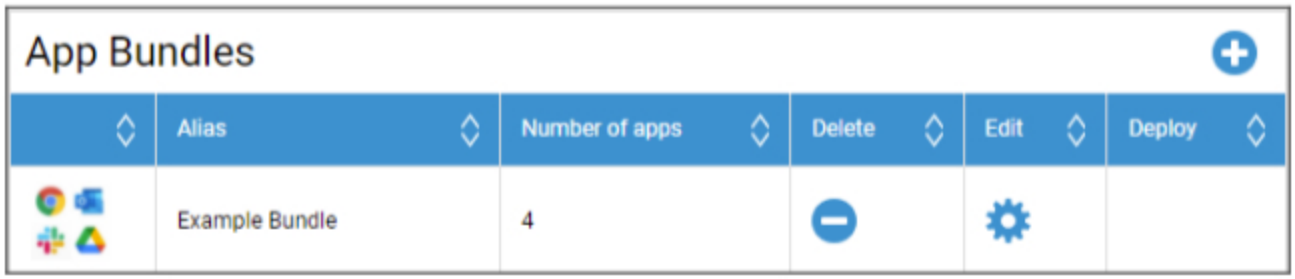
Планировка магазина

Макет магазина определяет, как будут отображаться приложения в Play Store, и будут ли они отображаться вообще.

Помните, что если Вы хотите показать приложения в Play Store, которые пользователь может установить вручную, их необходимо добавить здесь, в макете **И** в профиле в Enterprise Play Store. Если Вы добавите приложение только в один из них, оно не будет отображаться.

Пакет приложений

С помощью App Bundles Вы можете определять группы приложений, которые можно назначить профилю устройства или группы одним щелчком мыши.



Нажмите на "+", чтобы создать новый App Bundle. После создания App Bundle Вы можете нажать на "Edit", чтобы добавить в него приложения из различных источников.

Пакет можно добавить в профиль, как и любое другое приложение. При добавлении приложений у Вас появится дополнительная вкладка под названием "App Bundles", на которой будут располагаться Ваши пакеты.

Если Вы внесете какие-либо изменения в App Bundle, появится кнопка в колонке "Развернуть". Это позволит Вам распространить эти изменения на все профили, содержащие этот пакет. Поэтому имейте в виду, что Вам придется делать это вручную после добавления или удаления приложений в пакете.

Пульт дистанционного управления

TeamViewer

Коннектор TeamViewer

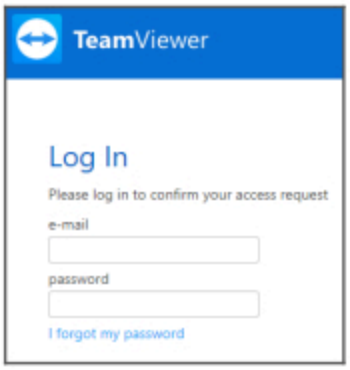
Примечание: В бесплатной пробной версии нашей облачной системы Вы не сможете подключить свой аккаунт TeamViewer. Вместо этого у Вас будет автоматически подключен бесплатный демо-аккаунт.

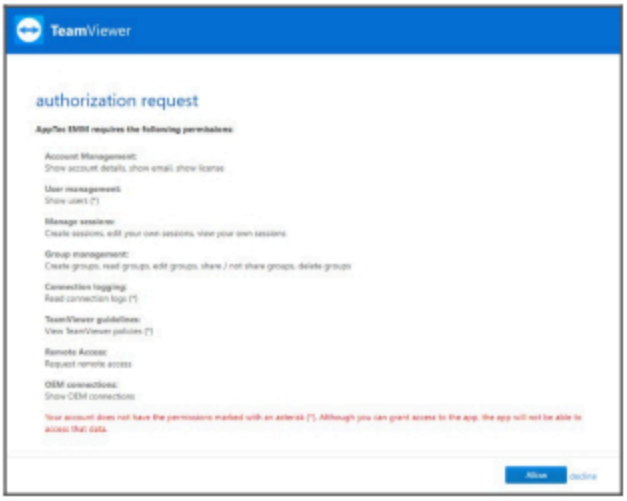
Перейдите в Общие настройки -> Дистанционное управление -> TeamViewer. Здесь Вы можете связать свою учётную запись TeamViewer с консолью или просмотреть информацию о Вашей текущей подключённой учётной записи. Также Вы можете просмотреть все активные в данный момент сеансы, если перейдете в раздел "Активные сеансы".

Чтобы связать свой аккаунт, нажмите на кнопку "Начать настройку".

В результате Вы попадёте на новую страницу, где Вам нужно будет войти в систему, используя свою учётную запись TeamViewer.

После входа в систему Вы должны разрешить AppTec360 MDM использовать эту учетную запись. После подтверждения Вам нужно подождать несколько секунд, и Учетная запись будет подключена.


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


TeamViewer
authorization request

Установите TeamViewer QuickSupport

Добавьте приложение "TeamViewer QuickSupport" в список обязательных приложений Вашего профиля устройства или профиля группы и нажмите кнопку "Назначить сейчас". Подождите, пока приложение не будет установлено на устройство.

Если Вы попытаетесь получить доступ к устройству, на котором это приложение не установлено, оно будет установлено или Вам будет предложено установить его, в зависимости от конфигурации устройства.

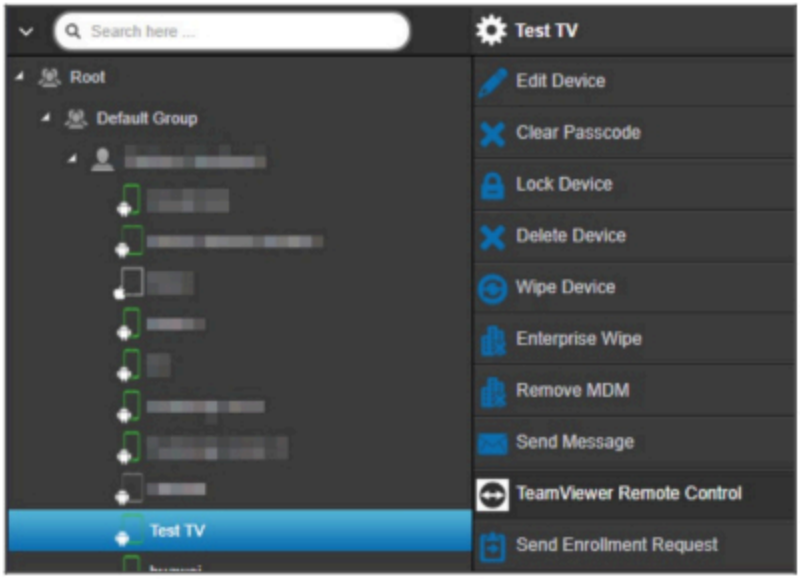
Дистанционное управление Вашим устройством

Чтобы удаленно управлять устройством, выберите устройство, нажмите на колесико и выберите "TeamViewer Remote Control".

Если уже есть активная сессия, Вы можете либо использовать старую, либо создать новую.

Подтвердите, что Вы хотите создать новую сессию TeamViewer.

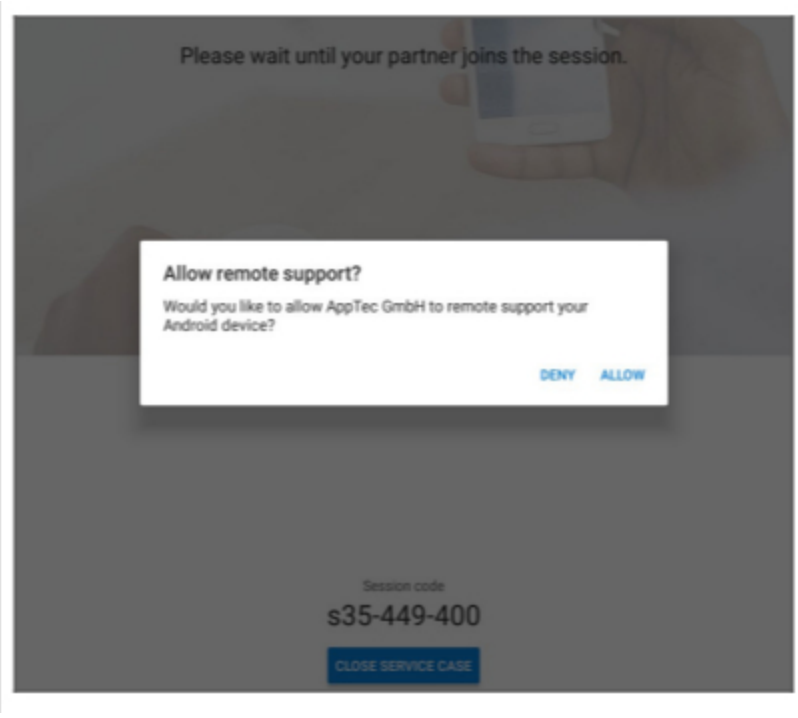
Через несколько секунд Вы получите ссылку на Вашу сессию TeamViewer. Вы можете нажать на "Начать", чтобы открыть эту ссылку в новом окне.


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

Эта ссылка откроет установленную Вами программу TeamViewer и подключит Вас к устройству.

Теперь Вам нужно подтвердить соединение на самом устройстве, чтобы управлять им дистанционно.



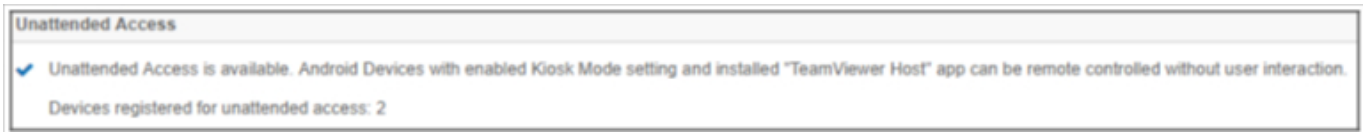
Если Вы используете iOS, Вы получите сообщение в AppTec360 MDM Client. С помощью этой ссылки устройство присоединится к удаленной сессии. В зависимости от настроек уведомлений

на устройстве возможно, что Вы не получите уведомление и Вам придется открывать AppTec360 MDM Client вручную.

На некоторых устройствах Android (например, Samsung) необходимо установить дополнительное приложение в качестве аддона. Приложение TeamViewer на устройстве сообщит Вам об этом, если это необходимо на Вашем устройстве.

Неуправляемый доступ

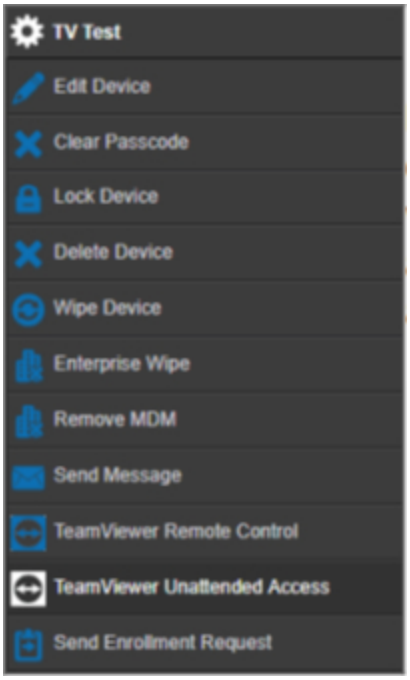
Примечание: Неавторизованный доступ возможен только на устройствах Android.



Вы можете подключаться к своим устройствам, не принимая соединение на устройстве, только если ваша учётная запись TeamViewer использует лицензию "Tensor" или "Corporate".

Вы можете проверить это после привязки Вашей учетной записи в разделе "Общие настройки".

Чтобы воспользоваться неуправляемым доступом, Вам необходимо установить приложение "TeamViewer Host" и активировать "Enable Unattended Access" в разделе "Kiosk Mode & Launcher" в Вашем профиле. Пожалуйста, имейте в виду, что это возможно только в том случае, если Вы используете режим "Киоск".



Теперь Вы можете выбрать неуправляемый доступ, если выберете свое устройство и нажмете на колесико. Это позволит Вам подключиться к устройству без необходимости подтверждения на самом устройстве. Пожалуйста, имейте в виду, что может пройти несколько минут, прежде чем Вы получите Ссылку для доступа к Вашему устройству.

Splashtop

Если Вы включите опцию Splashtop, Вы увидите параметры настройки Splashtop в своих профилях.

Чтобы использовать Splashtop, Вам необходимо установить Splashtop Streamer (com.splashtop.streamer.csrs) в качестве обязательного приложения в Вашем профиле. После этого Вы можете включить конфигурацию Splashtop в своем профиле в разделе "Удаленное управление". Включение этой опции настроит приложение Splashtop Streamer. Если Вы используете Splashtop Streamer, но не в сочетании с MDM, Вам следует оставить эту опцию выключенной.

В Вашем профиле в разделе "Удаленное управление" Вы также должны задать код развертывания. Перейдите на https://my.splashtop.com и войдите в свою учетную запись Splashtop. Нажмите на "Добавить компьютер" и скопируйте 12-значный код развертывания с открывшейся страницы.

Без кода развертывания дистанционное управление НЕ возможно.

После этого Вы можете щелкнуть правой кнопкой мыши на своем устройстве и запустить удаленный сеанс, нажав на "Splashtop Remote Control".

Управление сим-картой

Массовый импорт CSV

Здесь показан обзор назначенных Вам Sim-карт и вся информация о них. Это поможет Вам иметь всю информацию не только о Ваших устройствах, но и о Ваших Sim-картах в одной системе.

ПРИМЕЧАНИЕ: Это ручное управление/документирование. Невозможно получить эти данные автоматически с устройств из-за механизмов конфиденциальности/безопасности операционных систем.

Вы также можете импортировать этот список в формате CSV.

Перевозчик и тариф

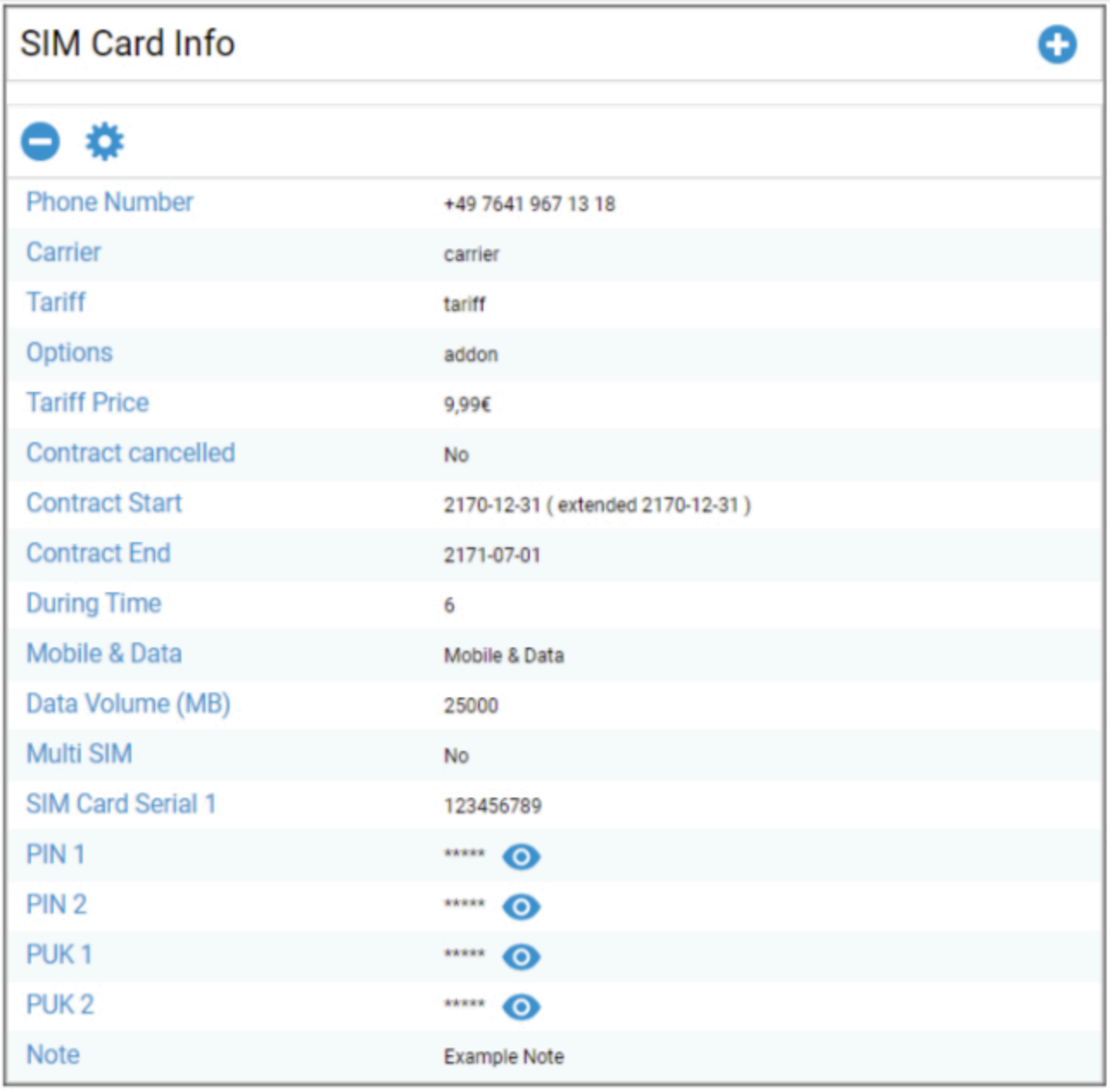
Чтобы добавить Sim-карту, сначала нажмите на кнопку, чтобы добавить одного или нескольких операторов.

Затем нажмите на "+" в разделе "Информация о тарифах", чтобы добавить тариф к перевозчику.

По желанию Вы можете добавить дополнительные опции ниже, если у Вас есть что-то подобное.

Здесь подготовлено все, что нужно для добавления настоящей Sim-карты. В настоящее время Sim-карты назначаются Пользователю. Поэтому зайдите в Управление мобильными устройствами, выберите пользователя и перейдите в раздел "Обзор Sim-карт".

Здесь Вы видите Sim-карты этого пользователя. Если таковая имеется, Вы можете отредактировать или удалить её. У пользователей может быть несколько Sim-карт.

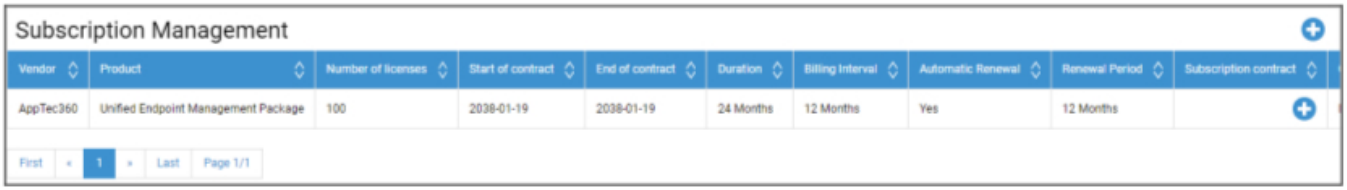


Нажмите на "+", чтобы добавить Sim-карту, и добавьте всю необходимую информацию. Эти Sim-карты также будут перечислены в списке всех Ваших Sim-карт в разделе Общие настройки → Управление Sim-картами.

Управление подпиской

Управление подпиской

Здесь Вы можете документировать текущие подписки, их детали, а также хранить различные файлы, например, подписанный контракт, письмо о расторжении и т.д. Вы также можете настроить напоминания, которые будут напоминать Вам по почте до окончания подписки и, возможно, продлевать ее автоматически.



Нажмите на "+" вверху, чтобы добавить подписку. Вы можете добавить столько подписок, сколько захотите.

Нажмите на "+" в различных полях, чтобы загрузить файлы, относящиеся к этой Подписке. Технически Вы можете загружать файлы любого типа, но имейте в виду, что не все типы файлов могут быть предварительно просмотрены в браузере.

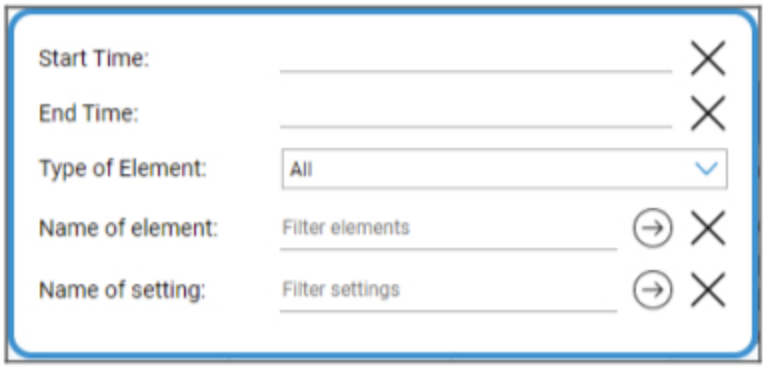
Общий журнал аудита

Журнал аудита

Здесь у Вас есть общий Журнал аудита, который показывает все сделанные изменения. В то время как журнал аудита для пользователя или группы показывает только изменения, относящиеся к этому пользователю или группе, этот журнал показывает КАЖДОЕ изменение, сделанное в любом месте консоли.

Вы можете увидеть, что было изменено, кем, когда и где. В некоторых случаях Вы также можете расширить запись, чтобы увидеть дополнительные детали.

Можно нажать на пользователя или на запись в "Path / Type", чтобы перейти к месту, где было сделано изменение.



В правом верхнем углу Вы также можете задать фильтр, который поможет найти определенные изменения в среде, где происходит множество изменений.

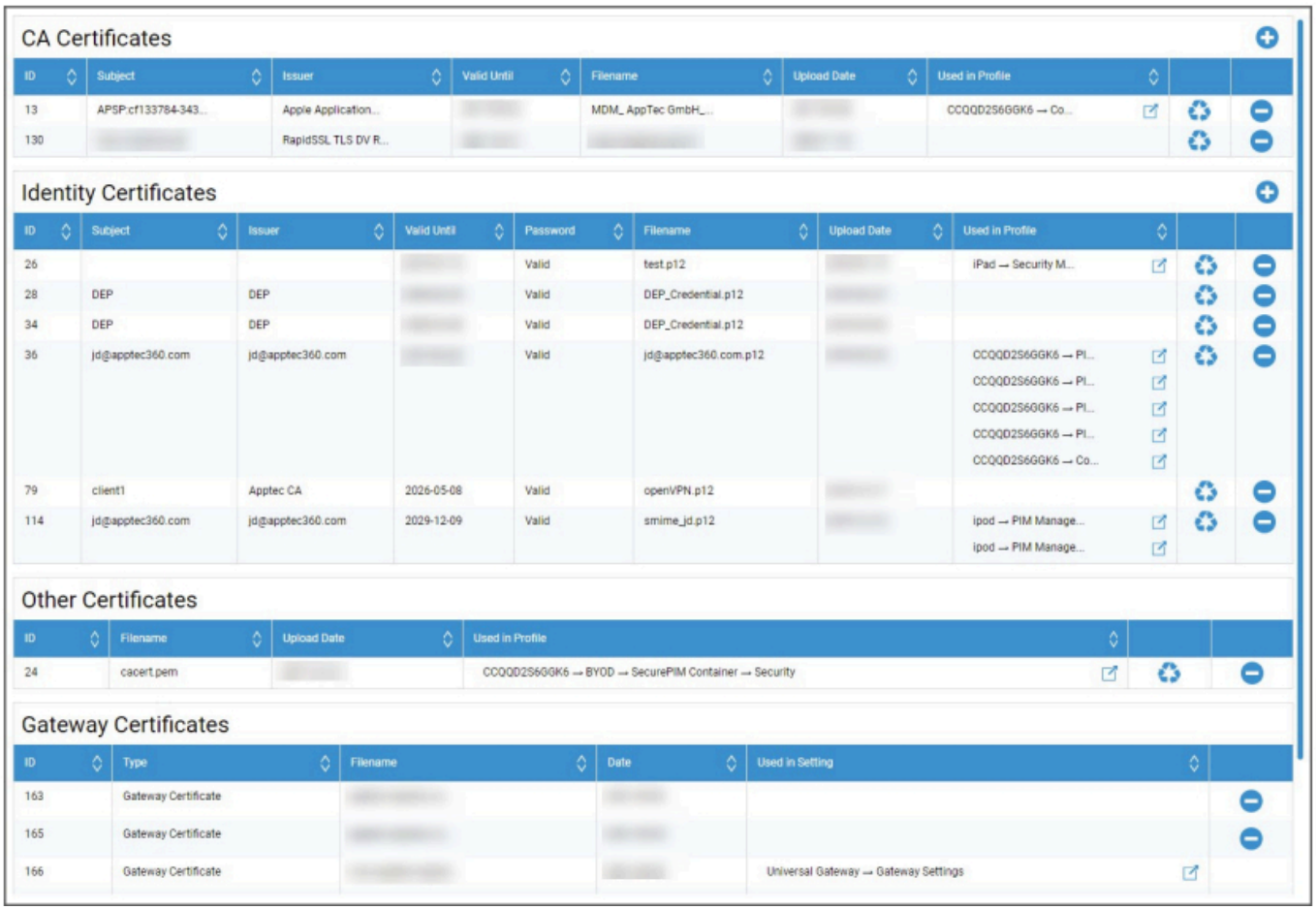
Настройки журнала аудита

"Период хранения журналов аудита" определяет, как долго журналы аудита должны храниться перед удалением.

Управление сертификатами

Здесь Вы получите обзор всех сертификатов, загруженных и используемых в Консоли. Это только обзор. Фактическая настройка сертификатов, например, Wi-Fi, по-прежнему выполняется в профиле в соответствующем месте.

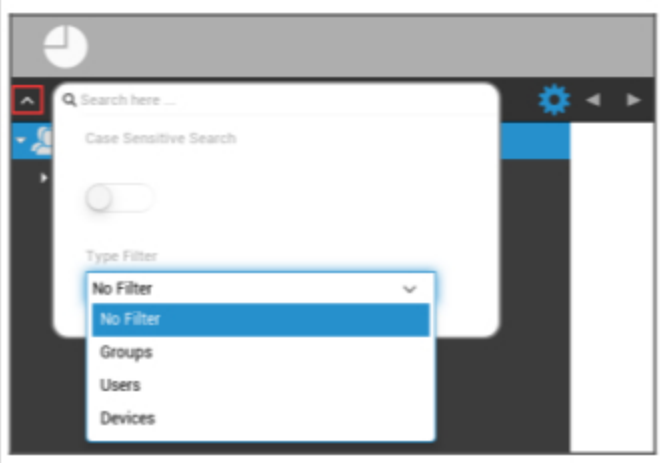
Здесь Вы также можете удалить или обновить сертификаты, что автоматически отразится в затронутых профилях. Щелкните на информации в разделе "Используется в профиле", чтобы увидеть, где именно какой-либо сертификат все еще назначен.



Управление мобильными устройствами

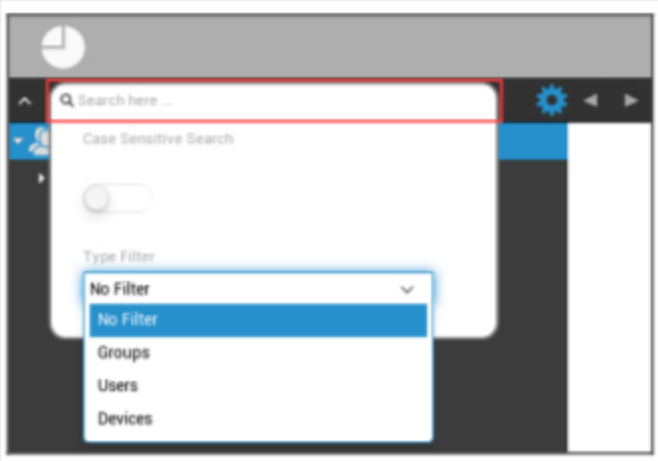
Экран управления мобильными устройствами

Фильтр устройства



Щелкнув мышью в левом верхнем углу экрана, Вы найдете множество фильтров для отображения устройств.

Окно поиска



Окно поиска позволяет Вам найти все устройства и/или пользователей по определенному ключевому слову.

Опциональные шестеренки

После нажатия на соответствующий символ появится список доступных Вам опций.

Они меняются с каждым текущим окном и объясняются в соответствующих главах.

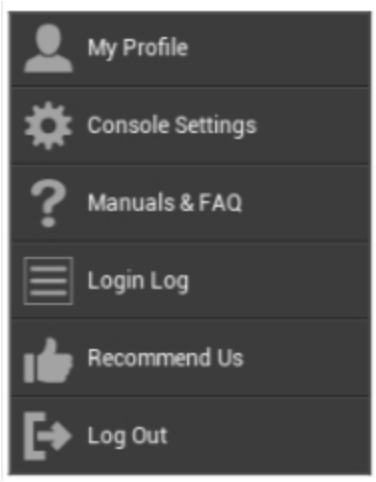
Навигационные стрелки

Щелкнув на стрелке влево, Вы перейдете на предыдущую страницу.

После этого, нажав на стрелку вправо, Вы перейдете на страницу, которую только что покинули.

Администрирование учетной записи — настройки

Щелкнув на адресе электронной почты, как показано выше, Вы увидите следующее меню:



Мой профиль	Отредактируйте данные учетной записи администратора
Настройки консоли	Настройте параметры консоли для учетной записи Admins
Руководства и часто задаваемые вопросы	Просмотрите страницу "Руководства и часто задаваемые вопросы" в разделе "Общие настройки".
Журнал регистрации	Доступ к "Журналу входа в систему"
Рекомендуйте нас	Просмотрите страницу "Рекомендуйте нас" в разделе "Общие настройки".
Выйти из системы	Выйдите из консоли MDM

Информация о пользователе

Здесь Вы можете отредактировать данные учетной записи администратора, вошедшего в систему в данный момент.

Имя пользователя	Имя пользователя и/или адрес электронной почты учетной записи
Имя	Имя администратора
Фамилия	Фамилия администратора
Имя пользователя	Имя пользователя администратора
Адрес электронной почты	Адрес электронной почты администратора
Альтернативный адрес электронной почты	Альтернативный адрес электронной почты администратора
Изображение	Изображение профиля
Номер телефона	Номер телефона администратора
Номер мобильного телефона	Номер мобильного телефона администратора
Расширение телефона	Расширение телефона
Расположение	Расположение
Позиция	Должность в компании
Группа пользователей	Выберите, какой группе пользователей Вы хотите назначить учетную запись администратора.
Комментарий	Введите комментарий
Введите новый пароль	Введите пароль для изменения пароля
Повторите новый пароль	Повторите новый пароль для подтверждения

Обратите внимание, что доступ к администрированию также может быть оформлен как учетная запись локального пользователя в структуре иерархии. Без создания дополнительного администратора эту учетную запись удалять не следует!

Настройки консоли

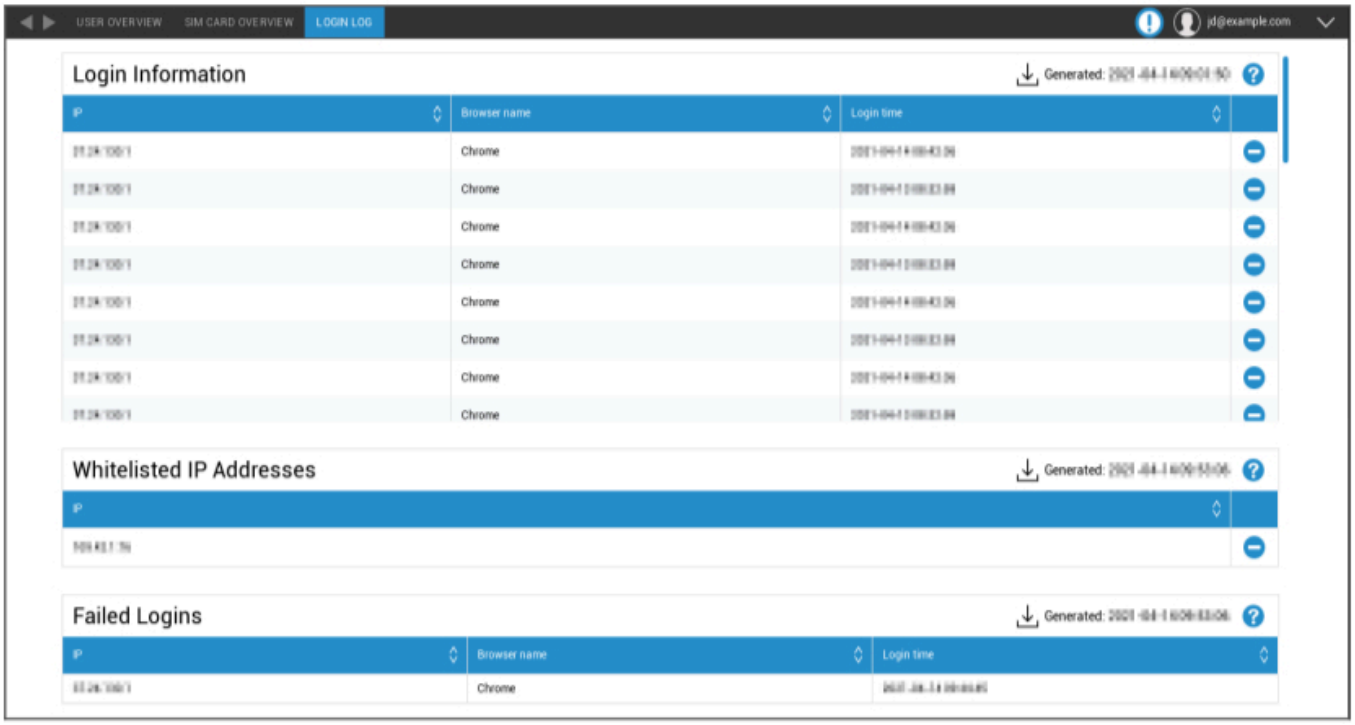
Здесь Вы можете настроить следующие параметры консоли для учетной записи Admins:

Параметры отображения пользователя в каталоге	Определите, как пользователи должны быть помечены в дереве
Параметры отображения устройства каталога	Определите, как устройства должны быть обозначены в дереве
Таймаут сессии	Если пользователь ничего не сделает в течение указанного времени, он выйдет из системы. Значение по умолчанию - 60 минут. Пожалуйста, выйдите из системы и войдите в нее снова после изменения этой настройки.
Часовой пояс	Выберите часовой пояс, который будет использоваться
Формат времени	Выберите способ отображения временных меток
Язык консоли	Выберите язык, на котором будет отображаться консоль. Доступны английский и немецкий.
Основной цвет	Вы можете задать цвет, который будет использоваться в качестве базового для цветовой схемы консоли. Вы можете либо воспользоваться палитрой выбора цвета, либо ввести цвет в HTML HEX-нотации. RGB-форматоры, такие как "розовый", "желтый", тоже работают.
Команда сохранения	Комбинация клавиш для запуска сохранения без нажатия кнопки "Сохранить".
Используйте двухфакторную аутентификацию	Включите использование двухфакторной аутентификации при входе в систему. После входа в систему Вы получите электронное письмо с кодом, который нужно будет ввести, чтобы войти в систему.
Таймаут двухфакторной аутентификации	Установите период времени, в течение которого Вас не будут просить пройти двухфакторную аутентификацию после уже успешной аутентификации.
Отправьте код проверки через	Код проверки будет отправлен на выбранные варианты. Сообщение об устройстве будет показано в AppTec360 MDM App на всех принадлежащих Вам устройствах Android и iOS.
Отправьте сообщение о входе в систему после входа	Если эта опция включена, то при каждом входе в систему с ip-адреса, не внесенного в белый список, будет отправлено письмо.

	В письме содержится информация о входе в систему (например, IP, браузер).

Журнал регистрации

Здесь Вы можете увидеть информацию о входах в систему для текущей учетной записи администратора.



Информация для входа	Список, содержащий логины текущей учетной записи администратора, которые были записаны консолью. В этом списке показаны все Ваши успешные входы в систему за последние 30 дней.
IP-адреса в белом списке	Это список всех Ваших IP-адресов, внесенных в белый список. Если Вы войдете в систему с IP, который указан в этом списке, Вы не получите сообщение о входе. Вы можете добавить IP-адрес в этот список, нажав на кнопку рядом с записью в списке "Информация для входа" выше. Вы можете удалить IP-адрес из этого списка, нажав на кнопку рядом с записью в этом списке или в списке "Информация для входа" выше.
Неудачные входы в систему	Это список всех неудачных попыток входа в систему за последние 30 дней. Если Вам не удалось ввести правильный пароль хотя бы 3 раза за 20 минут, запись появится в этом списке. Вы также будете получать информацию о неудачных попытках входа в систему по электронной почте.

Корпоративная администрация (корневой узел) в управлении мобильными устройствами

Когда Вы доберетесь до корневого узла (первая группа), Вы сможете выполнить множество настроек для Вашей компании, касающихся управления мобильными устройствами.

Создайте подгруппу	Создайте подгруппу
Переименование корневого узла	Переименование корневого узла (например, название Вашей компании)
Массовое зачисление	Одновременная регистрация нескольких устройств/ пользователей
Назначение массы	Назначьте профиль для соответствующих групп с помощью одного взгляда
Быстрое администрирование приложений	Отправляйте запросы на (Не)установку приложения на соответствующие групповые устройства
Импорт пользователей в формате CSV	Импортируйте пользователей из CSV в соответствующую группу

Создайте подгруппу

С помощью "Create a Subgroup" Вы можете создать дополнительную подгруппу.

Вы можете установить, к какой группе должна быть отнесена подгруппа.

(По умолчанию создается новая группа, которая назначается в качестве подгруппы в корневом узле)

Переименование корневого узла

Здесь Вы можете переименовать свое корневое имя. Обычно в этом случае используется название компании.

Массовое зачисление

С помощью "Mass Enrollment" Вы можете зарегистрировать несколько устройств и пользователей.

Вы можете напрямую выбрать, каким способом пользователь должен получить информацию о зачислении (eMail; альтернативная eMail; SMS).

В зависимости от того, какое устройство получит пользователь (iOS, Android, Windows Phone), Вы можете прямо отметить это здесь.

Здесь также можно настроить различие между смартфоном и планшетом, которое нужно правильно выбрать, поставив галочку.

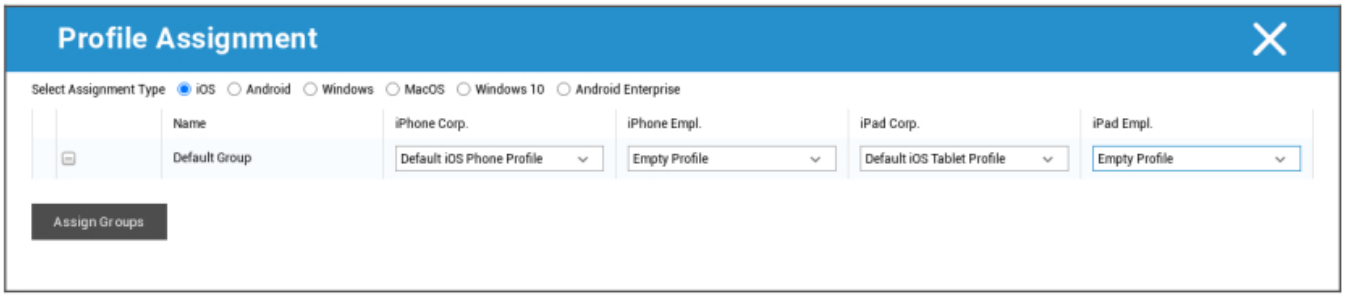
В качестве последнего шага Вы можете определить, является ли соответствующее устройство корпоративным или личным (BYOD).

С помощью "Export as CSV" Вы можете экспортировать информацию в файл данных CSV. В свою очередь, Вы также можете импортировать файл данных CSV с помощью "Import CSV", файл должен выглядеть так, как показано ниже:

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

Назначение массы

В разделе "Массовое назначение" Вы можете назначить профиль всем группам, которые делятся на iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

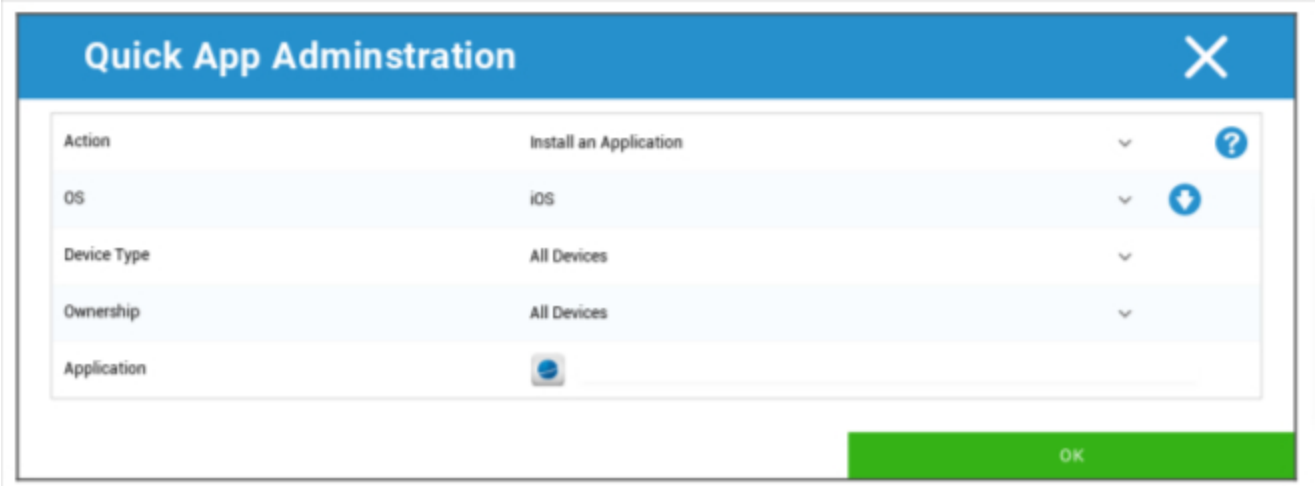


Windows - MacOS - Windows 10 - Android Enterprise

Быстрое администрирование приложений

В разделе Быстрое администрирование приложений Вы можете отправить запросы на установку или удаление указанного приложения в выбранную Вами ОС.

Вы также можете определить, должен ли запрос быть отправлен на все типы устройств выбранной ОС или только на определенный тип устройства.



Импорт пользователей в формате CSV

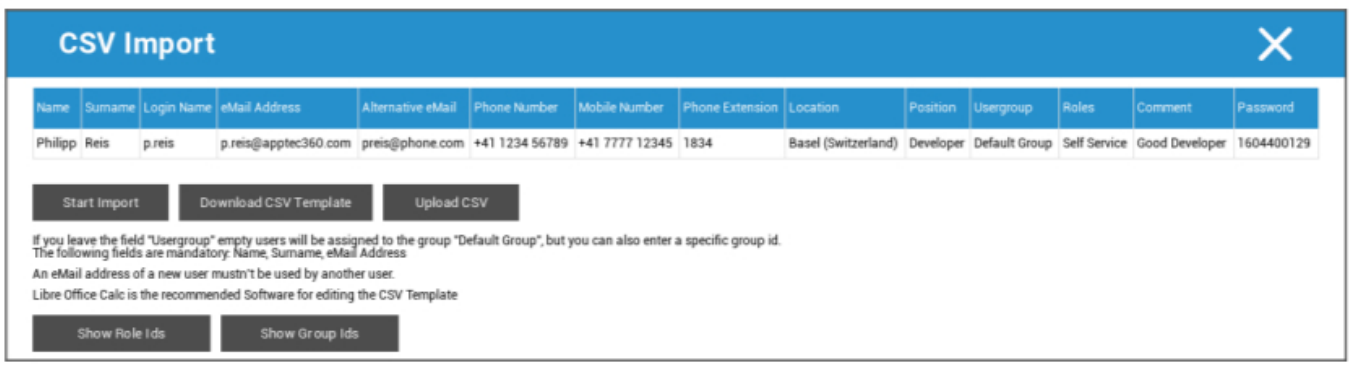
Импортируйте пользователей из CSV в соответствующую группу.

С помощью "Download CSV Template" Вы можете экспортировать файл-шаблон CSV, который можно заполнить (или использовать в качестве справочника).

Вы также можете использовать опции "Show Role Ids" и "Show Group Ids" в качестве ссылки для создания собственного CSV-файла.

CSV-файл можно загрузить в MDM с помощью команды "Upload CSV".

В качестве последнего шага Вы можете начать импорт, нажав на кнопку "Начать импорт".



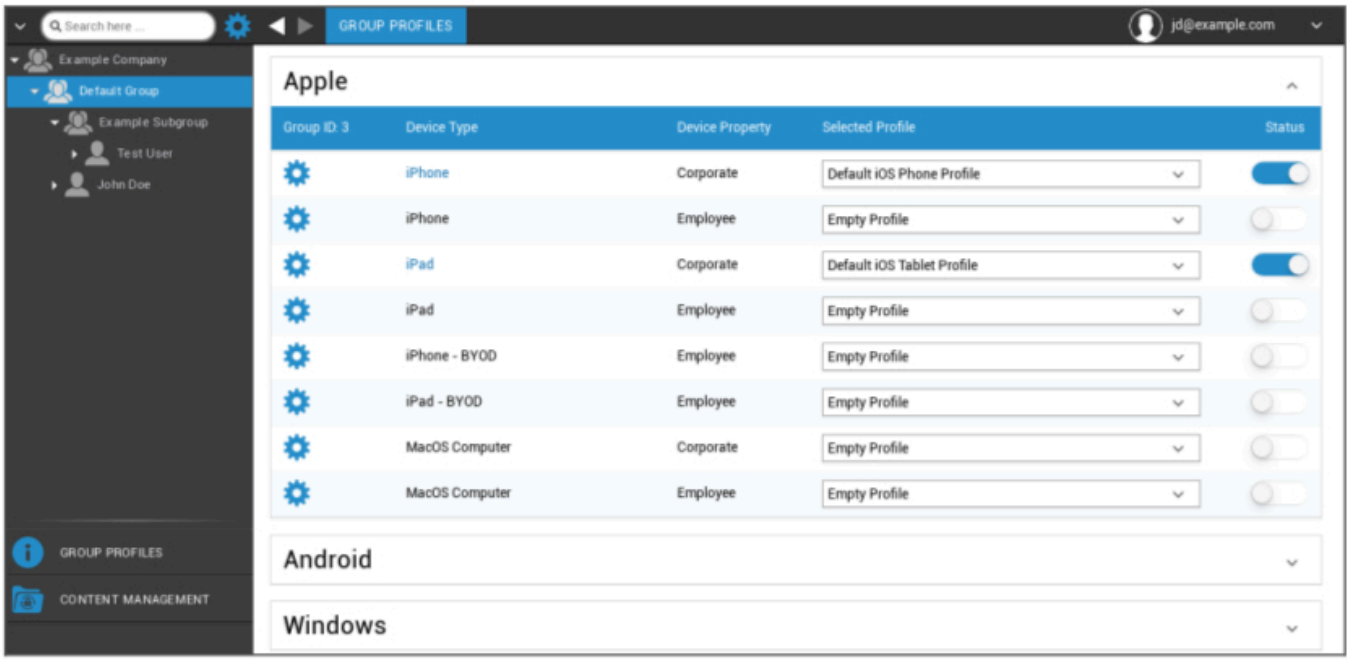
Управление группами в мобильном менеджменте

Один щелчок на обзоре отображает различные профили конфигурации для соответствующих платформ.

Один профиль содержит все параметры, которые можно заранее установить с помощью AppTec360 на устройстве конечного пользователя. На каждой платформе Вы можете создать профили для корпоративных устройств (Corporate) или для устройств, которые Вы приносите с собой (Employee).

Для того чтобы разграничить конфигурации групп устройств, например, по местоположению или функциям, рекомендуется создать несколько подгрупп.

Обратите внимание на Управление профилем в разделе Управление мобильными устройствами



С помощью меню передач Вы устанавливаете различные настройки для соответствующей (под)группы.

Создайте подгруппу	Создайте подгруппу для соответствующей (под)группы
Редактирование выбранной группы	Редактирование выбранной группы
Удалить выбранную группу	Удалить выбранную группу
Массовое зачисление	Регистрируйте сразу много устройств/пользователей для выбранного профиля

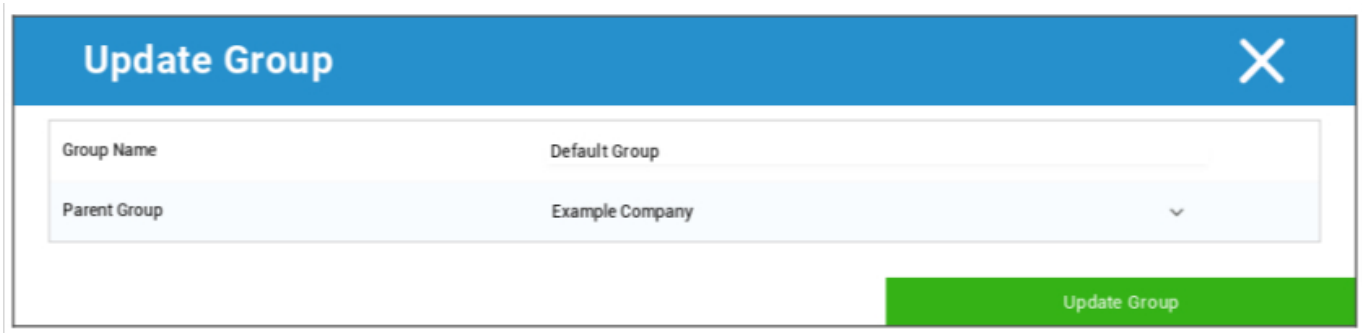
Назначение массы	Назначьте профили группе, которая выбрана в данный момент.
Создайте подгруппу	Создайте подгруппу для соответствующей (под)группы
Создать пользователя	Создайте пользователя для соответствующей (под)группы

Создайте подгруппу

С помощью "Create a Subgroup" Вы можете создать дополнительную подгруппу.

Вы можете установить, к какой группе будет отнесена подгруппа (по умолчанию подгруппа будет отнесена к группе, которая выбрана в данный момент).

Редактирование выбранной группы



Здесь Вы можете редактировать профиль - здесь возможны следующие настройки:

- Название группы можно изменить
- Родительская группа может быть изменена

Удалить выбранную группу

В разделе "Удалить выбранную группу" Вам будут перечислены все пользователи и устройства, входящие в соответствующую группу. Здесь у Вас есть возможность удалить их.

Для одного пользователя Вы можете выполнить следующие команды удаления:

Удалить пользователя	Пользователь удален
Переместить пользователя в группу:	Вы можете переместить пользователя в другую группу (следующая колонка, например, "Администраторы).

Для одного устройства Вы можете выполнить следующие команды удаления:

Стирание и удаление	Стирание и удаление устройства
Удалить из системы	Извлеките устройство только из AppTec

Ссылка: Массовое зачисление

Ссылка: Назначение массы

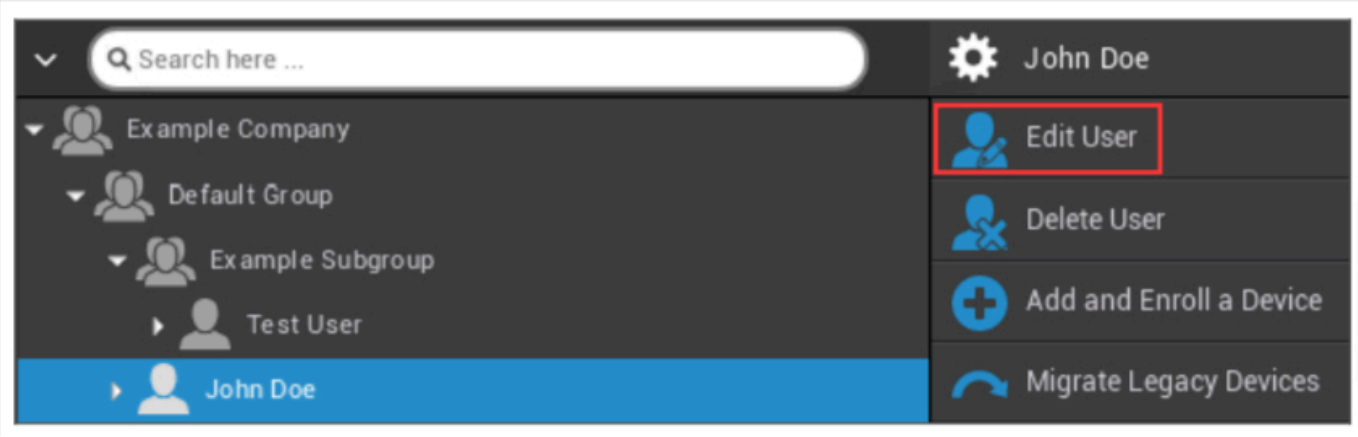
Создать пользователя

С помощью "Create a User" Вы можете добавить нового пользователя.

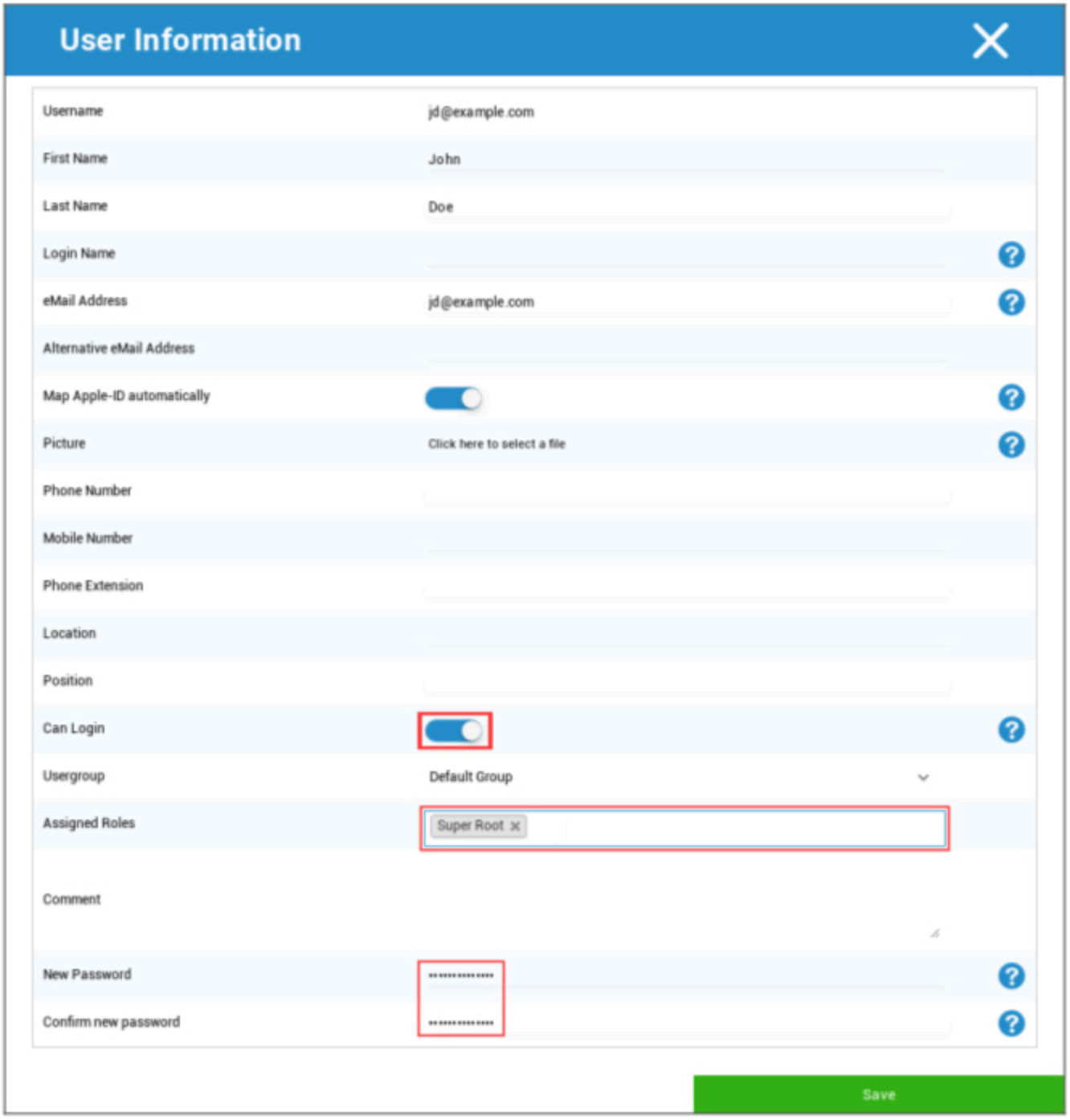
Создайте нового пользователя-администратора

Вы можете установить для пользователя статус Admin-User. Это даст ему права на вход в консоль, а также на изменение пользователей/групп/устройств.

Создайте обычного пользователя или используйте уже существующего. Выберите пользователя, которому Вы хотите предоставить права администратора, нажмите на колесико и выберите "Редактировать пользователя":



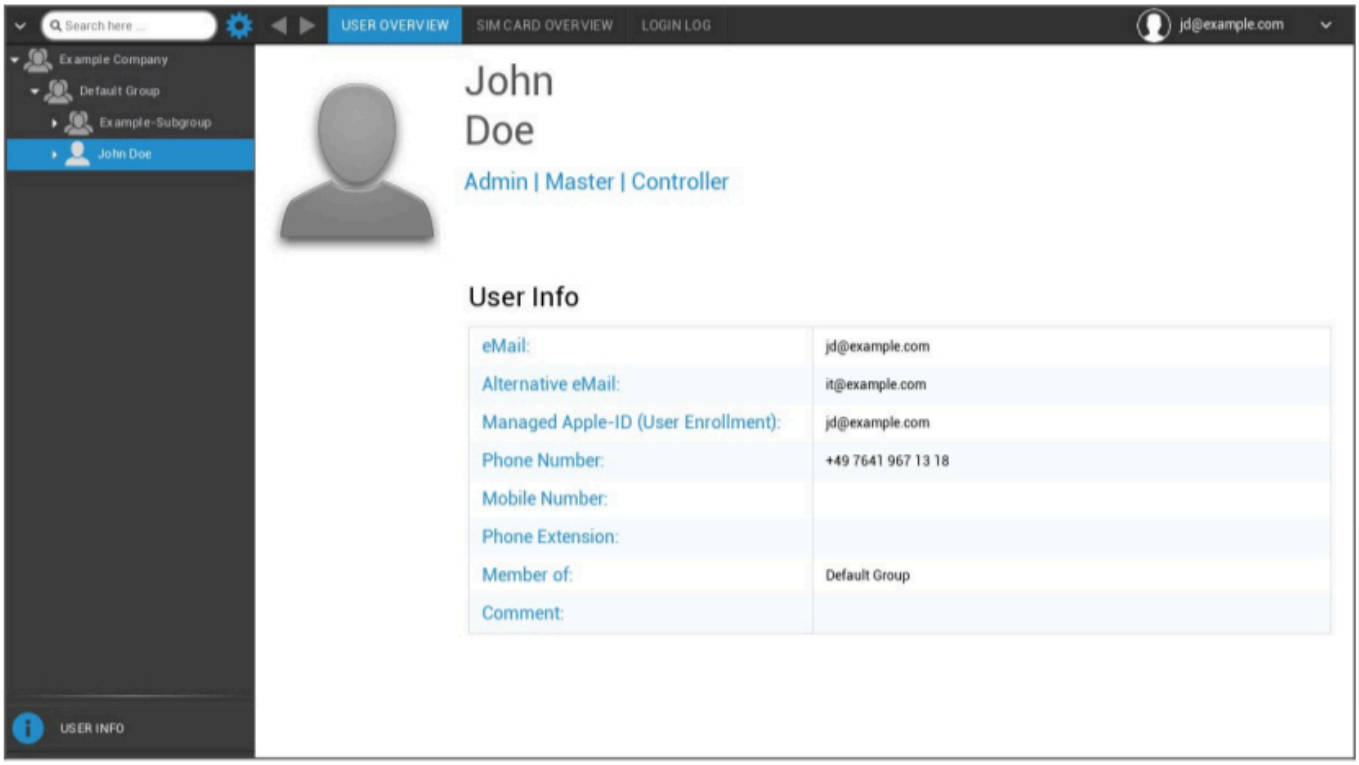
Активируйте переключатель "Can Login", назначьте пользователю роль "Super-Root" и установите пароль.



Сохраните это, и теперь пользователь может войти в систему, указав имя пользователя и пароль.

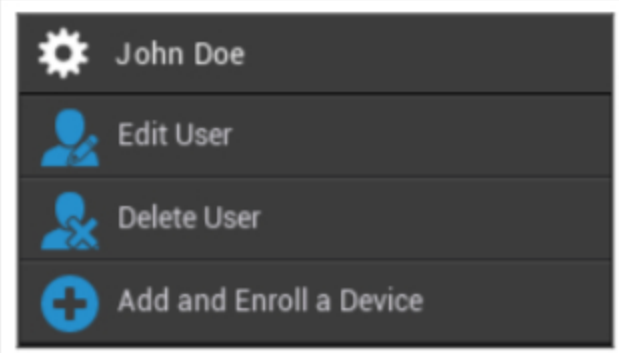
Управление пользователями в мобильном менеджменте

Когда Вы выбираете определенного пользователя, Вы видите следующий обзор:



Вы получите обзор всей информации, которую Вы ввели ранее в разделе "Создать пользователя".

С помощью шестеренки, установленной сверху, Вы можете выполнить следующие конфигурации:



Имя пользователя	Имя пользователя выбранного пользователя
Редактировать пользователя	Редактирование информации о пользователе

Удалить пользователя	Удалить пользователя • Удалить из системы = Устройство будет удалено из AppTec • Wipe & Delete = Устройство будет восстановлено до заводских настроек и удалено из AppTec
Добавьте и зарегистрируйте устройство	Зарегистрируйте устройство для выбранного пользователя

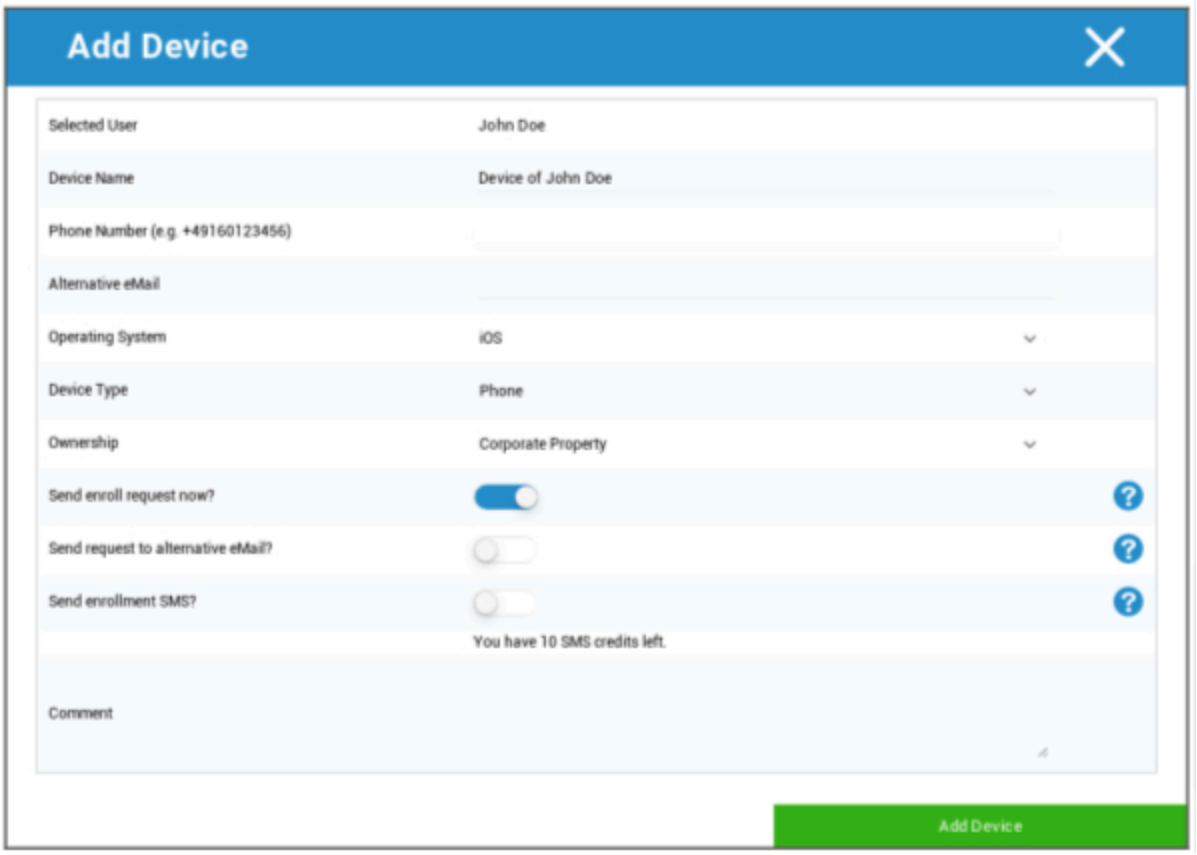
Обратите внимание, что доступ к администрированию также может быть оформлен как учетная запись локального пользователя в структуре иерархии. Без создания дополнительного администратора эту учетную запись удалять не следует!

Добавьте и зарегистрируйте устройство

Здесь Вы можете выбрать устройство для выбранного использования.

Кроме того, Вы можете зачислить устройства в группу напрямую. Для этого щелкните на группе, нажмите на колесико и выберите "Добавить и зачислить устройство".

Вы должны увидеть следующий обзор:



В зависимости от того, какое устройство Вы хотите зарегистрировать, Вы должны выполнить следующие настройки:

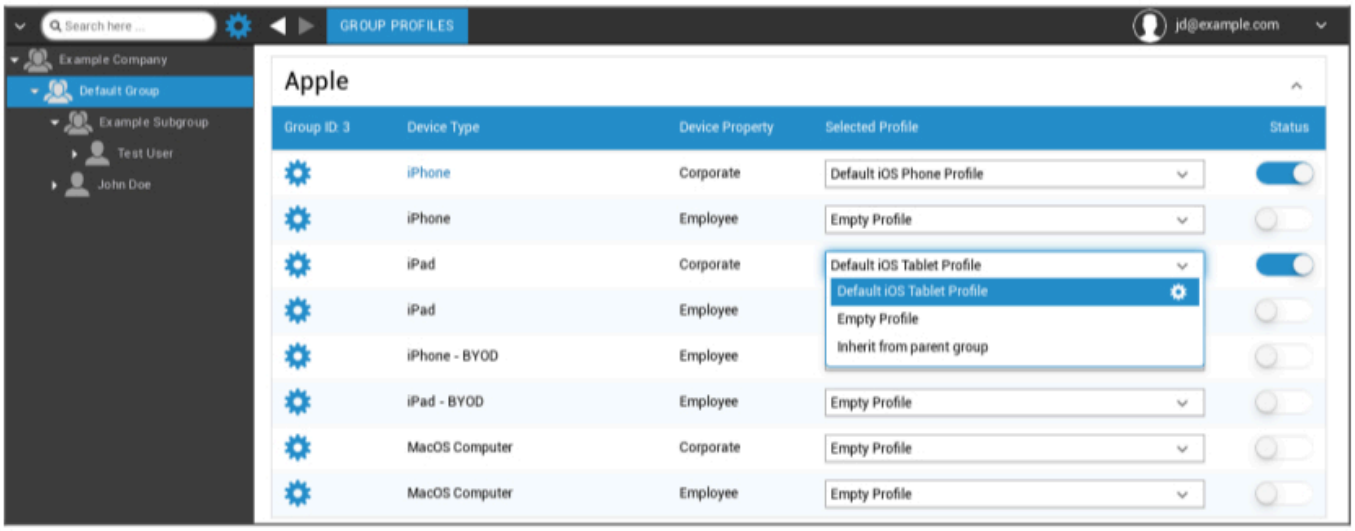
Выбранный пользователь	Выбранный пользователь (будет заполнено автоматически)
Имя устройства	Будет заполнено автоматически (устройство для "имени пользователя") - однако, может быть изменено
Номер телефона	Номер телефона, будет заполнен автоматически (если он был предоставлен пользователем) - здесь, однако, его можно добавить или изменить
Альтернативная электронная почта	Альтернативный e-mail, будет заполнен автоматически (если он был предоставлен пользователем) - здесь, однако, его можно добавить или изменить
Владелец устройства	Корпоративная собственность = корпоративное устройство Собственность сотрудника = устройство BYOD
Выберите операционную систему	Здесь Вы можете выбрать одну из следующих операционных систем: • iOS • iOS BYOD (регистрация пользователей) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Отправить запрос на зачисление?	Письмо немедленно отправляется на основной адрес электронной почты, и пользователю предлагается подключить свое устройство
Отправить запрос на альтернативный eMail?	Отправьте письмо дополнительно или исключительно (в случае, если функция "Отправить запрос на зачисление?" была деактивирована) на альтернативный адрес электронной почты (письмо отличается от "обычного" письма с запросом на зачисление)
Отправить SMS о зачислении?	Отправьте запрос на зачисление через SMS (необходимо ввести "Номер телефона")

После отправки запроса на регистрацию устройство сразу же появится на экране (выделено красным).

Как только устройство будет успешно подключено, вскоре оно будет отмечено зеленым цветом и, таким образом, будет готово к приему ограничений, приложений и т.д.

Управление профилем в мобильном менеджменте

После нажатия на группу Вы получите обзор всех платформ устройств, которые необходимо настроить, и соответственно назначенных профилей.



	Выполните настройку для выбранного профиля
Тип устройства	Тип устройства и/или модель
Свойства устройства	Владелец устройства (Корпоративный = корпоративная собственность, Сотрудник = устройство частного сотрудника)
Избранный профиль	Выбранный профиль (шестеренка открывает диалог настройки профиля)
Статус	Вкл/Выкл (профиль активирован/деактивирован)

Когда Вы выберите передачу, Вы получите следующие варианты:

Создайте профиль

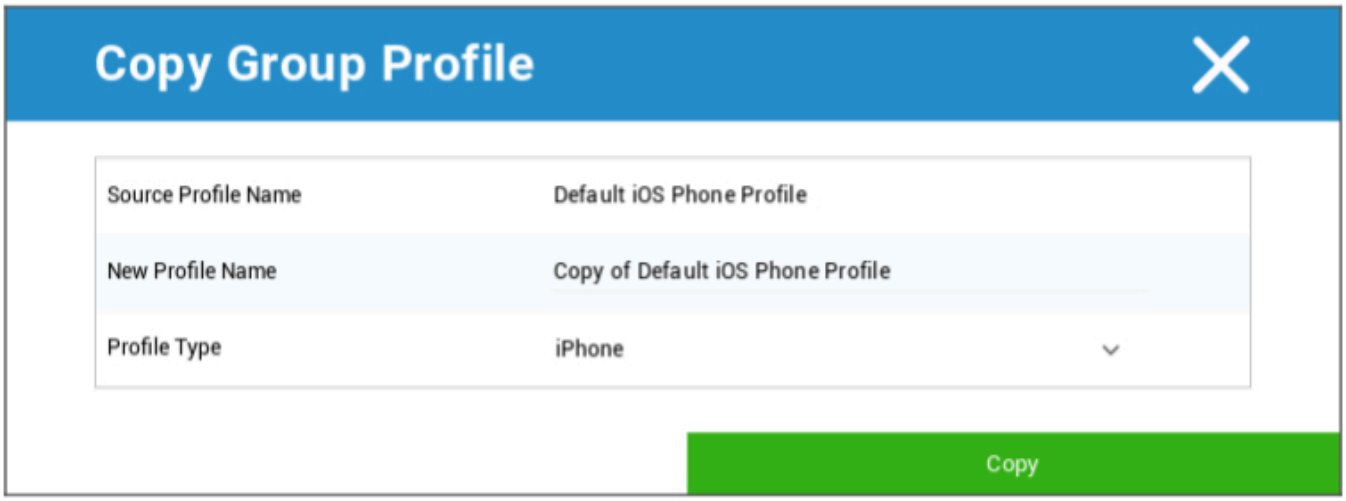
Вы можете создать и настроить новый профиль для каждой записи и/или платформы. После нажатия на этот подпункт профиль будет создан немедленно, и Вы сможете сразу же приступить к настройке iOS, Android и Windows Phone.

Редактировать профиль

После нажатия на кнопку "Редактировать профиль" Вы попадете в окно конфигурации соответствующего профиля, где сможете задать настройки.

Профиль копирования

С помощью функции "Копировать профиль" Вы можете скопировать настройки/конфигурации из уже существующего профиля и добавить их в новый профиль.

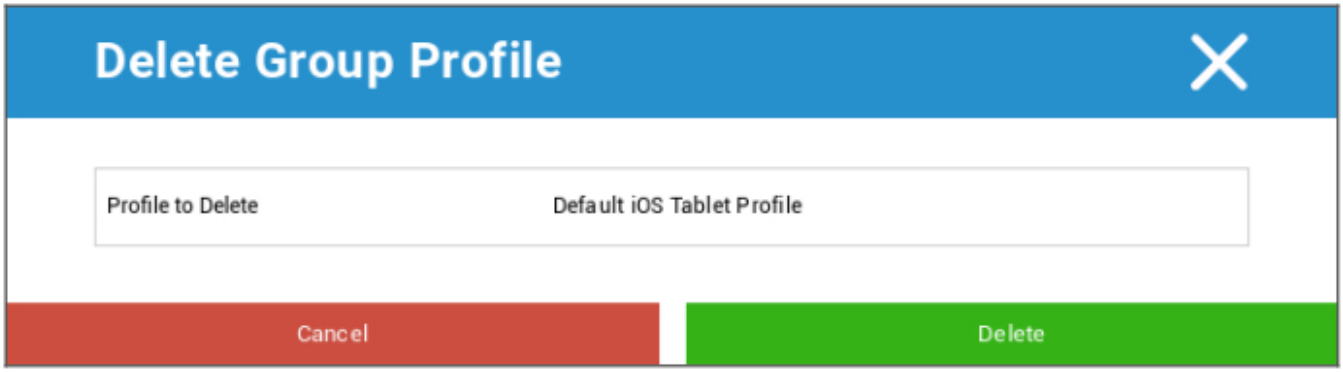


Источник Имя профиля	Имя профиля, который необходимо скопировать
Новое имя профиля	Имя нового профиля
Тип профиля	Тип профиля (телефон/планшет)

Как только Вы нажмете "Копировать", профиль будет создан и теперь может быть назначен группе

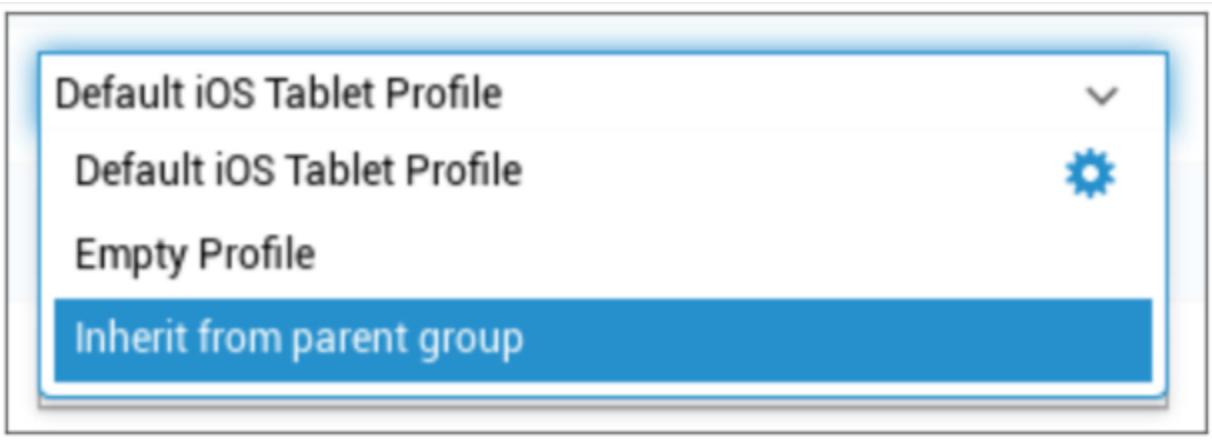
Удалить профиль

Здесь Вы можете навсегда удалить профиль. Обратите внимание, что во время процесса удаления и последующего процесса "Назначить сейчас" для профиля, конфигурация исчезнет на соответствующих устройствах затронутой группы и не сможет быть восстановлена!


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

Наследование профилей

Во время выбора профилей доступна опция "Унаследовать от родительской группы".



Если профиль активирован, то для соответственно выбранного устройства (и соответствующего типа устройства) будет использоваться профиль родительской группы. Обратите внимание, что изменения в этом профиле могут повлиять на множество групп.

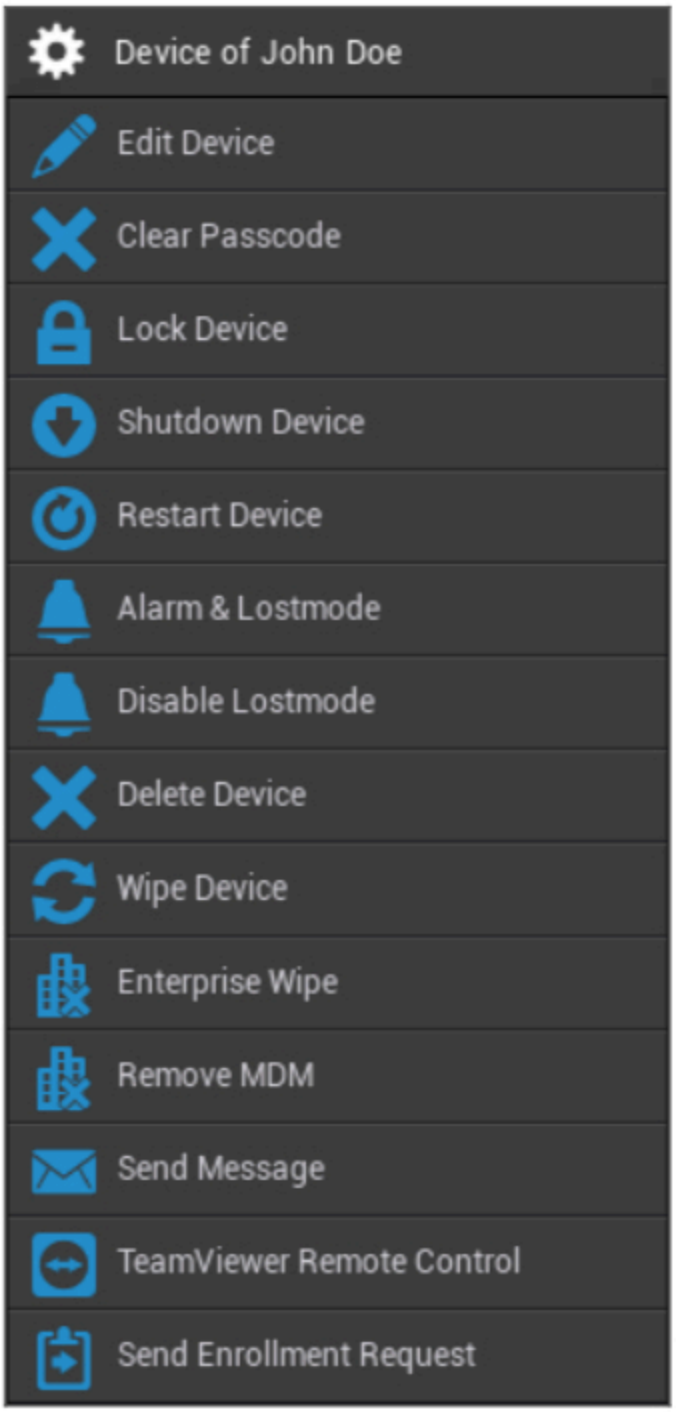
Эта конфигурация устанавливается как значение по умолчанию при создании новой подгруппы.

Также доступна конфигурация "Пустой профиль", которая соответствует пустому профилю, что означает, что в конечном итоге на устройстве конечного пользователя не будет производиться никаких новых конфигураций.

Управление устройствами в мобильном менеджменте

Когда Вы выбираете устройство, Вы можете выполнять различные задачи с помощью "шестеренки". Они различаются в зависимости от платформ ОС (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

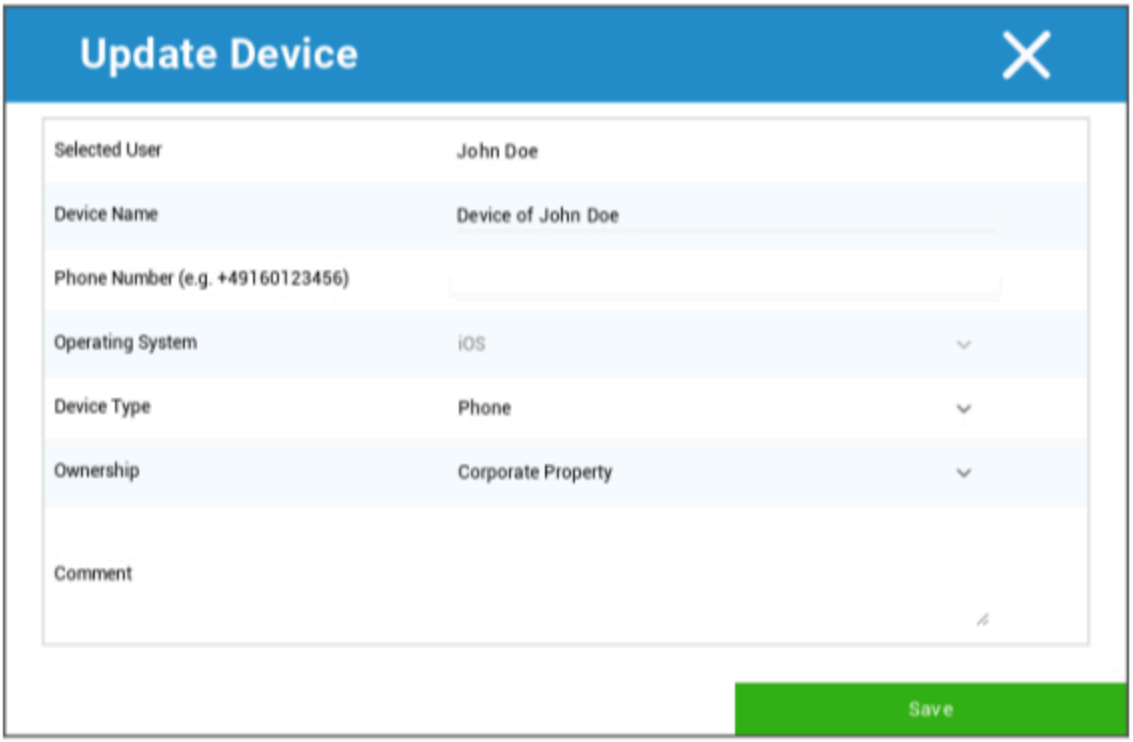
IOS



Редактировать устройство	Редактирование устройства
Очистить код доступа	Пароль устройства стирается
Устройство блокировки	Блокировка устройства (экран блокировки)

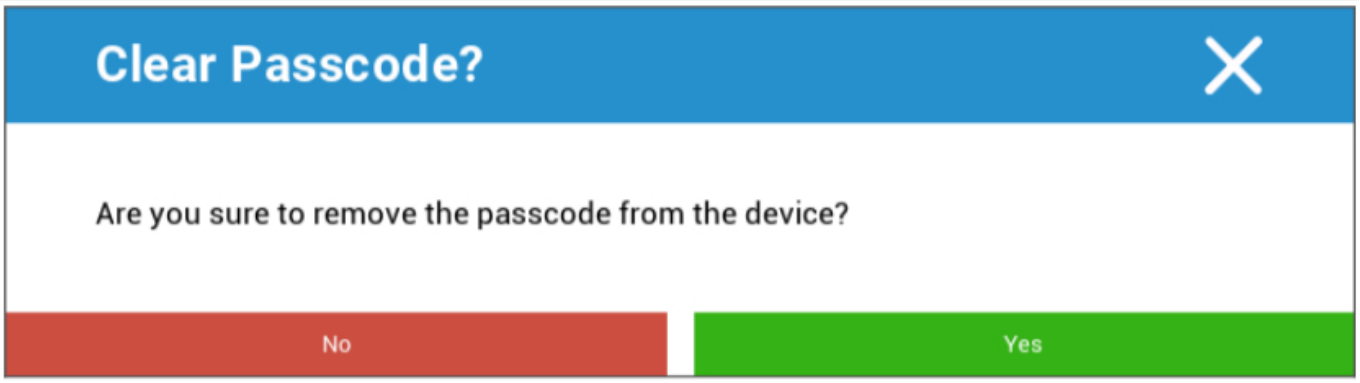
Устройство выключения	Устройство выключения
Перезагрузка устройства	Перезапустите устройство
Alarm & Lostmode	Start Alarm & Lostmode
Отключите режим Lostmode	Отключите режим Lostmode
Удалить устройство	Извлеките устройство из AppTec
Стирание устройства	Восстановление заводских настроек устройства
Enterprise Wipe	Информация, приложения и профили, предоставленные AppTec360, удаляются (устройство отделяется от MDM)
Удалите MDM	
Отправить сообщение	Отправляйте Push-уведомления на устройство Сообщение будет отображено в приложении AppTec360 (вкладка "Сообщение")
Удаленное управление TeamViewer	Начните сеанс удаленного управления с помощью TeamViewer
Отправить запрос на зачисление	Отправьте (повторно) запрос на зачисление

Редактировать устройство



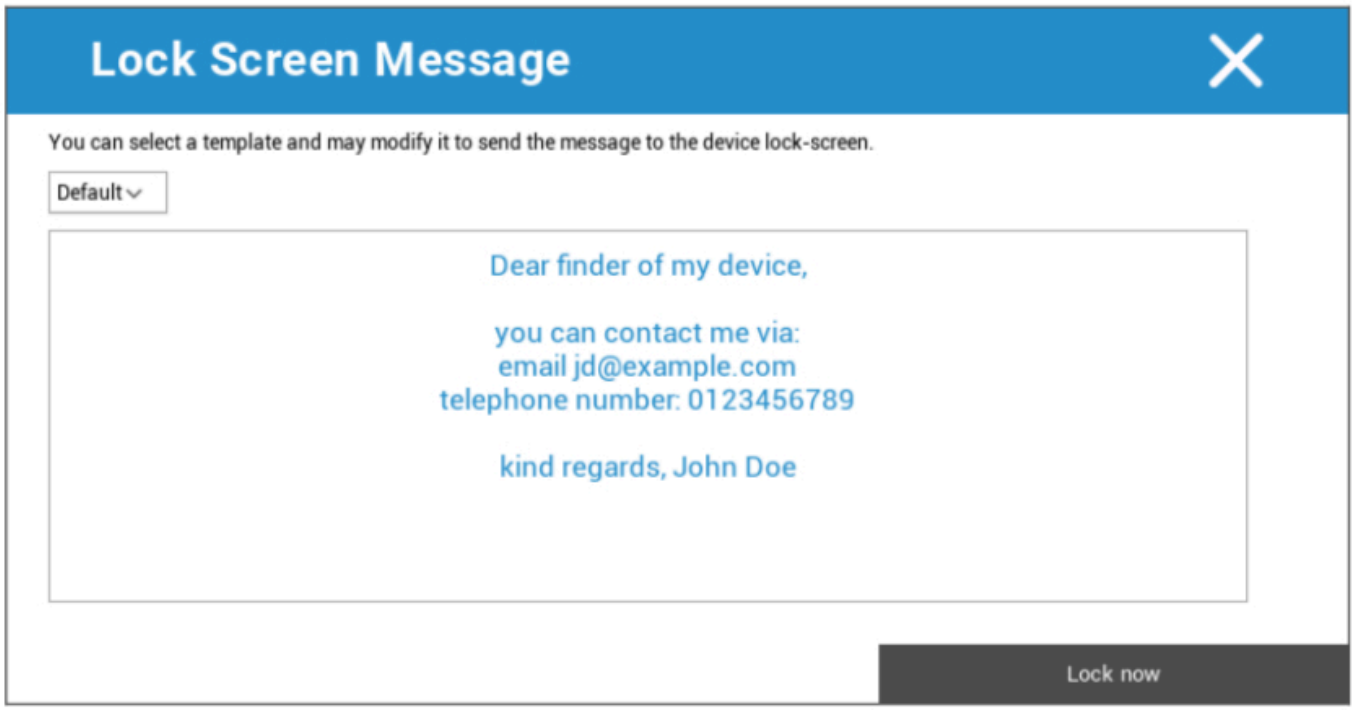
Здесь Вы можете обновить различную информацию об устройстве.

Очистить код доступа



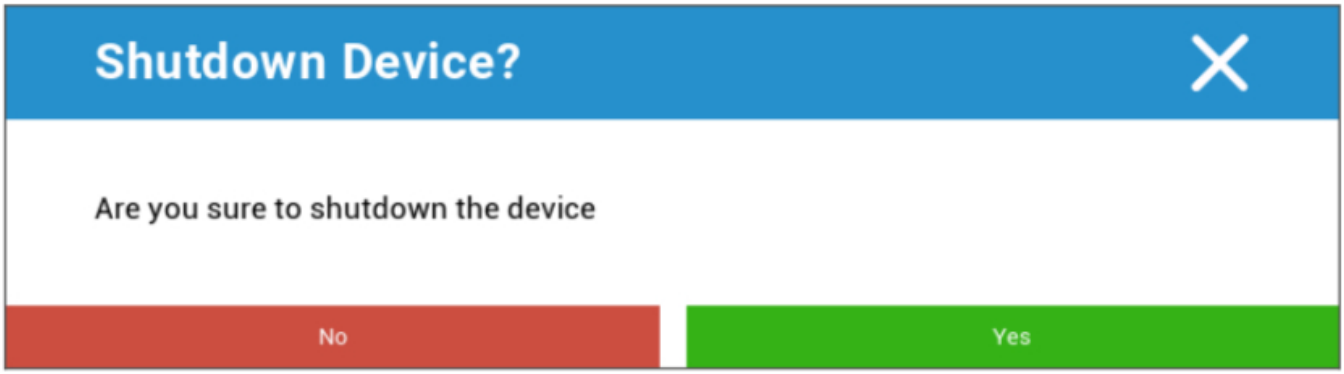
В разделе "Clear Passcode" Вы можете удаленно удалить пароль с устройства. Впоследствии пользователю будет предложено ввести новый пароль (в зависимости от рекомендаций по использованию Passcode).

Устройство блокировки



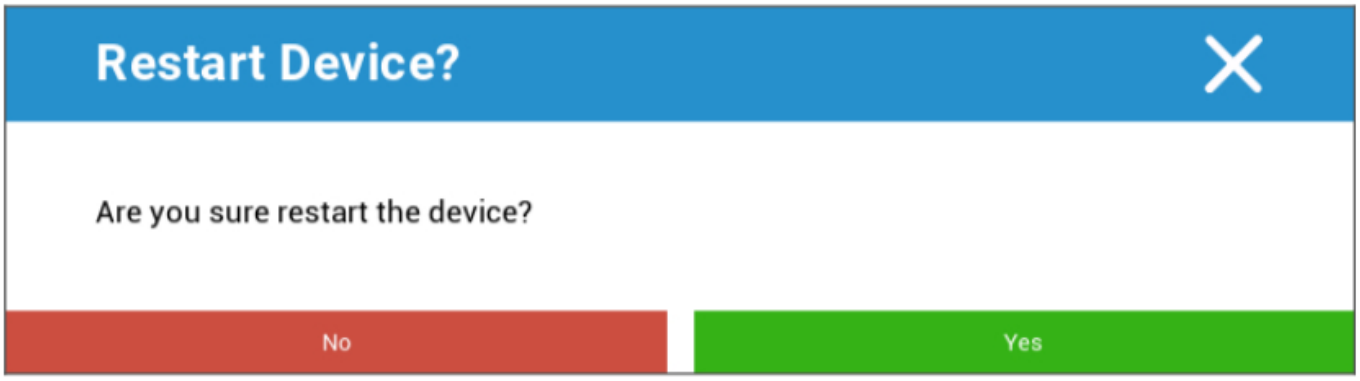
Здесь на устройство конечного пользователя отправляется команда блокировки (экран блокировки).

Устройство выключения



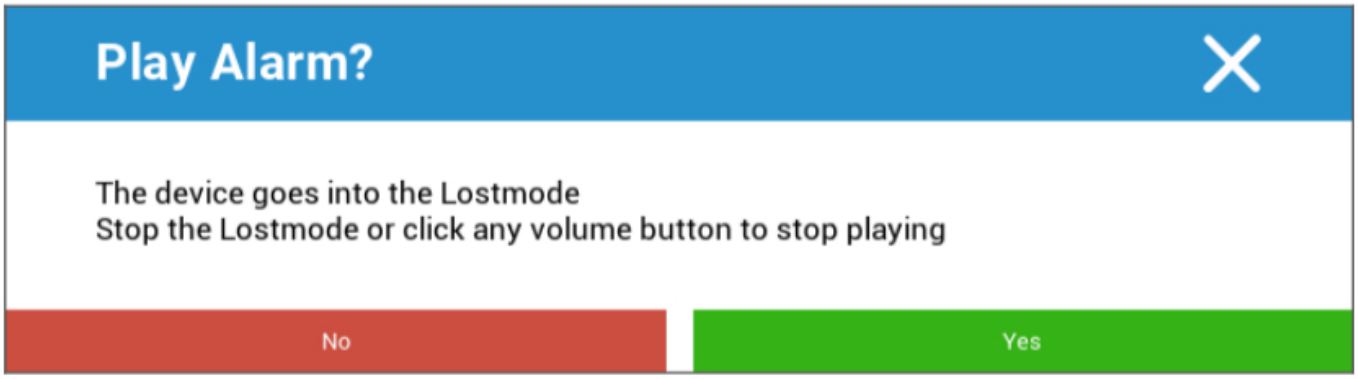
Здесь на устройство конечного пользователя отправляется команда выключения.

Перезагрузка устройства

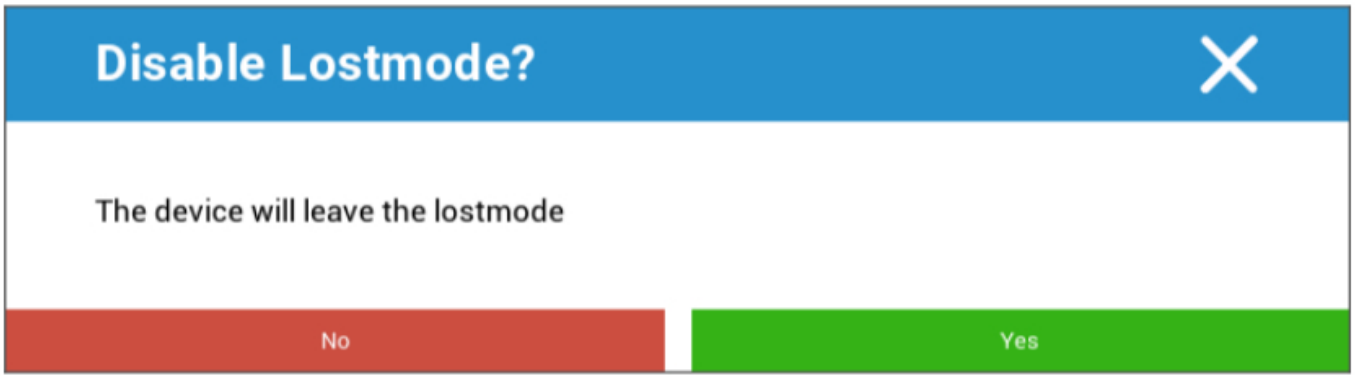


Здесь на конечное пользовательское устройство отправляется команда перезапуска.

Сигнализация и режим Lostmode | Отключить режим Lostmode



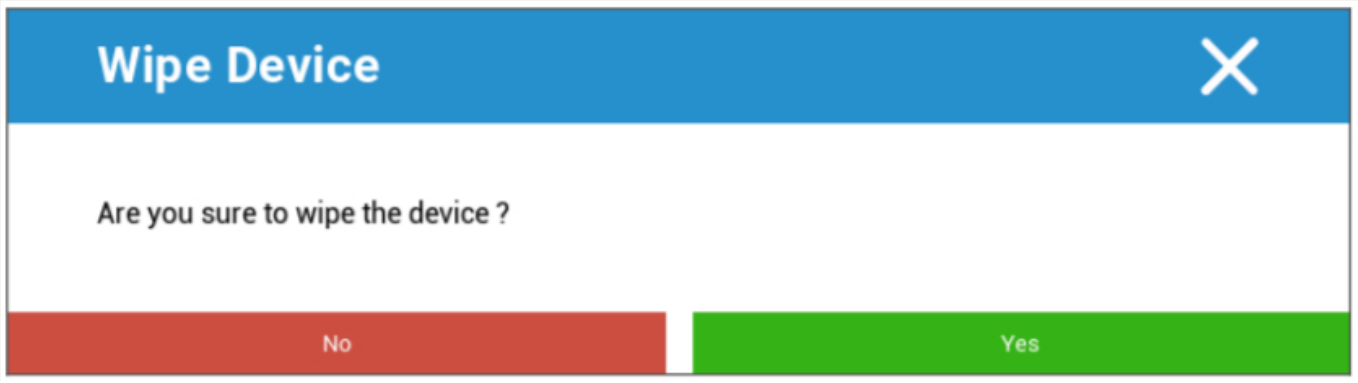
Здесь устройство может быть переведено в режим Lostmode, при котором устройство будет постоянно воспроизводить звук тревоги. Режим Lostmode можно остановить, нажав на любую кнопку громкости устройства или удаленно, нажав на кнопку "Disable Lostmode":



Удалить устройство

Здесь можно выполнить команду удаления. Вы можете еще раз решить, следует ли удалить устройство только из AppTec360 ("Delete from System") или удалить устройство из AppTec360, а также восстановить его заводские настройки ("Wipe & Delete").

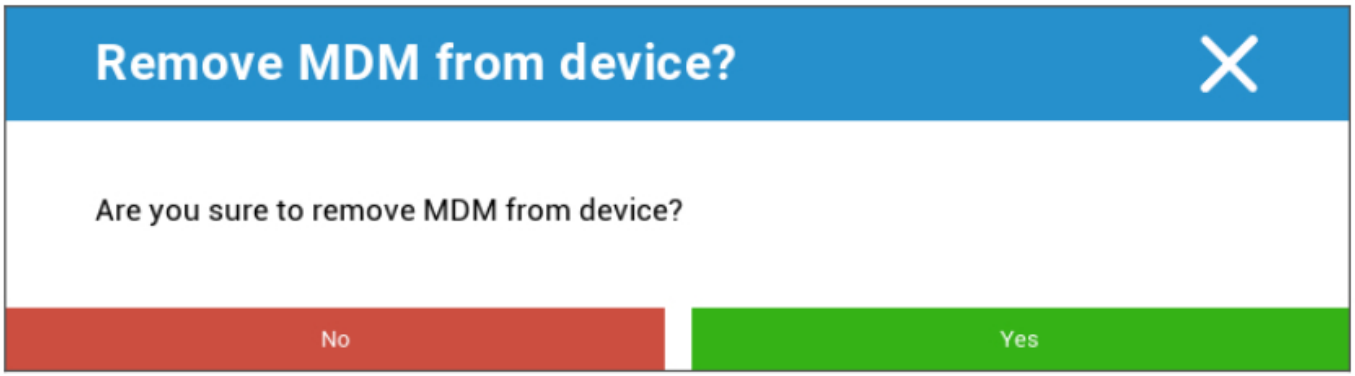
Стирание устройства



В разделе "Wipe Device" Вы можете полностью стереть устройство. Устройство будет восстановлено до заводских настроек.

Enterprise Wipe | Remove MDM

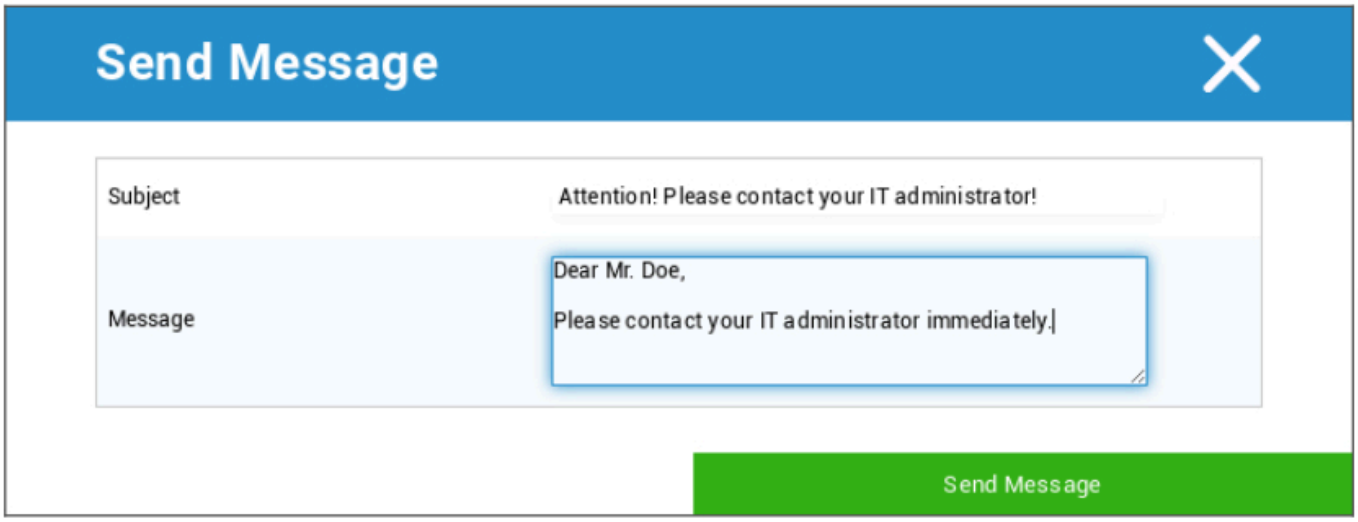
Удаляется только информация, приложения и профили, предоставленные AppTec360. Таким образом, корпоративные данные больше не будут доступны на устройстве конечного пользователя. Личная зона не затрагивается и продолжает оставаться на устройстве конечного пользователя.



С помощью команды "Remove MDM" Вы можете удалить профиль MDM на устройстве конечного пользователя и все остальные элементы, предоставленные AppTec.

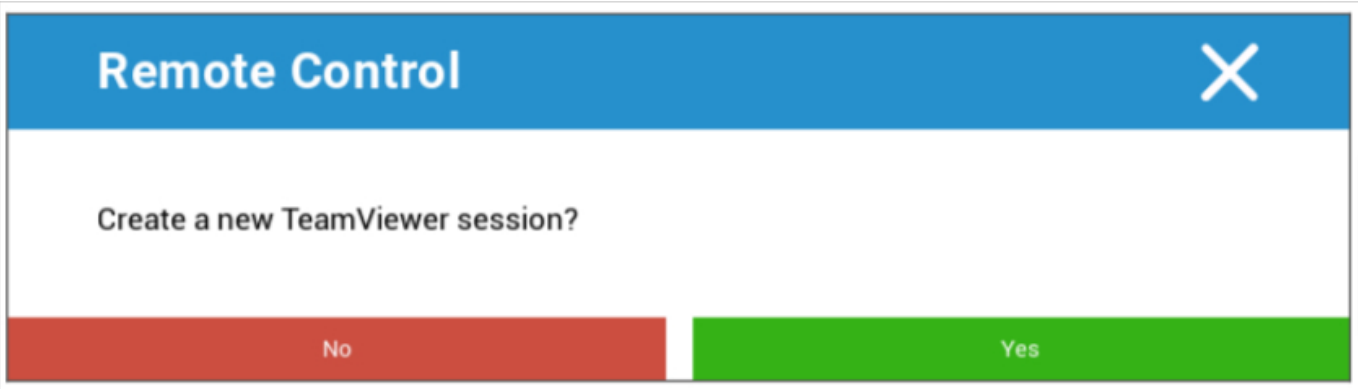
Эта команда выполняет то же действие, что и "Enterprise Wipe".

Отправить сообщение



Здесь Вы можете отправить Push-уведомление на соответствующее устройство.

Удаленное управление TeamViewer



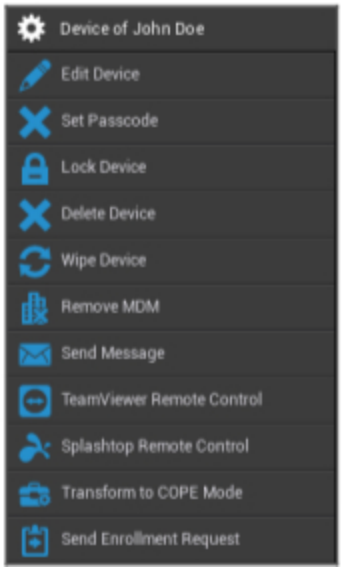
Здесь можно начать сеанс удаленного управления Teamviewer.

Отправить запрос на зачисление

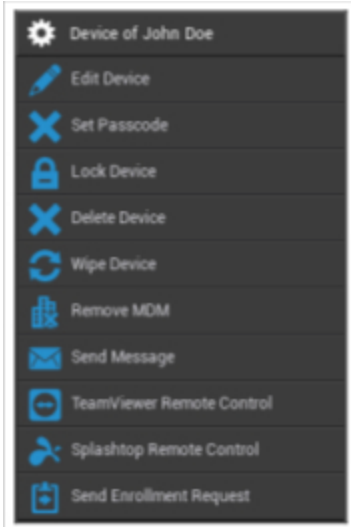
С помощью "Send Enrollment Request" Вы можете отправить запрос на зачисление (повторно) соответствующему пользователю.

Android

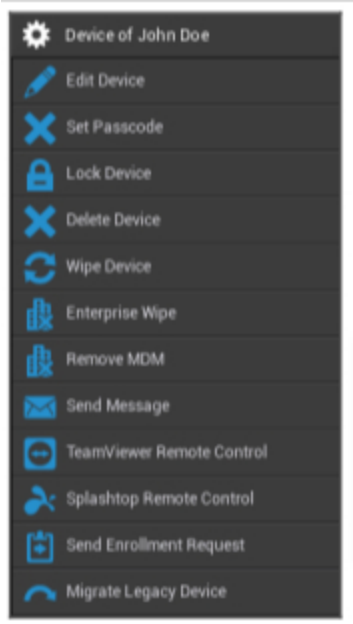
AE Полностью управляемое устройство (Work Managed)



Рабочий профиль AE (контейнер)



Телефон Android | Планшет

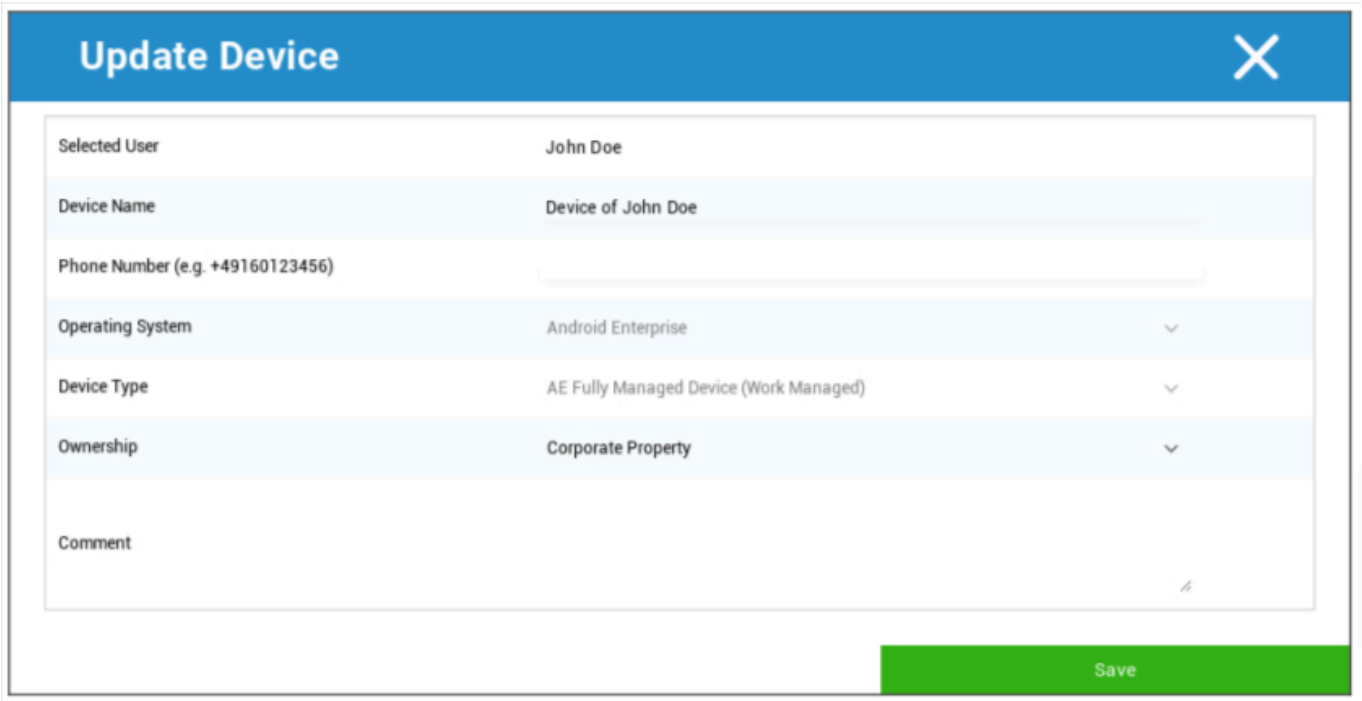


Редактировать устройство	Редактирование информации об устройстве
Установите пароль	Установите пароль устройства
Устройство блокировки	Блокировка устройства (экран блокировки)
Удалить устройство	Удалите устройство из AppTec
Стирание устройства	Восстановление заводских настроек устройства
Enterprise Wipe	Информация, приложения, профили, предоставленные AppTec360, будут удалены (устройство будет отделено от MDM)
Удалите MDM	
Отправить сообщение	Отправляйте Push-уведомления на устройство Сообщение будет отображено в приложении AppTec360 (вкладка "Сообщение")
Удаленное управление TeamViewer	Начните сеанс удаленного управления этим устройством с помощью TeamViewer
Пульт дистанционного управления Splashtop	Запустите сеанс удаленного управления этим устройством с помощью Splashtop

Переход в режим COPE (только на полностью управляемом устройстве AE (Work Managed))	Создайте рабочий профиль на этом устройстве AE с полным управлением (Work Managed)
Отправить запрос на зачисление	Отправьте (повторный) запрос на зачисление
Перенос устаревшего устройства (только для телефонов/планшетов Android, если они зарегистрированы с использованием режима обеспечения владельца устройства)	Перенесите профиль телефона/планшета Android в профиль AE Fully Managed Device (Work Managed).

Редактировать устройство

Здесь Вы можете обновить различную информацию об устройстве.



Выбранный пользователь	Пользователь устройства
Имя устройства	Имя устройства
Номер телефона	Номер телефона устройства
Операционная система	Android Enterprise Android

Тип устройства	Android Enterprise: • AE Полностью управляемое устройство (Work Managed) • Режим рабочего профиля AE (только для контейнеров) • Полностью управляемое устройство AE с рабочим профилем (COPE) Android: • Телефон • Планшет
Собственность	Корпоративный = корпоративная собственность Сотрудник = свойство сотрудника
Комментарий	Дополнительные описания для устройства

Очистить код доступа

Здесь Вы можете удалить пароль устройства на выбранном устройстве. По умолчанию на Android пароль будет установлен на "123456"- впоследствии он может и должен быть изменен пользователем.

Устройство блокировки

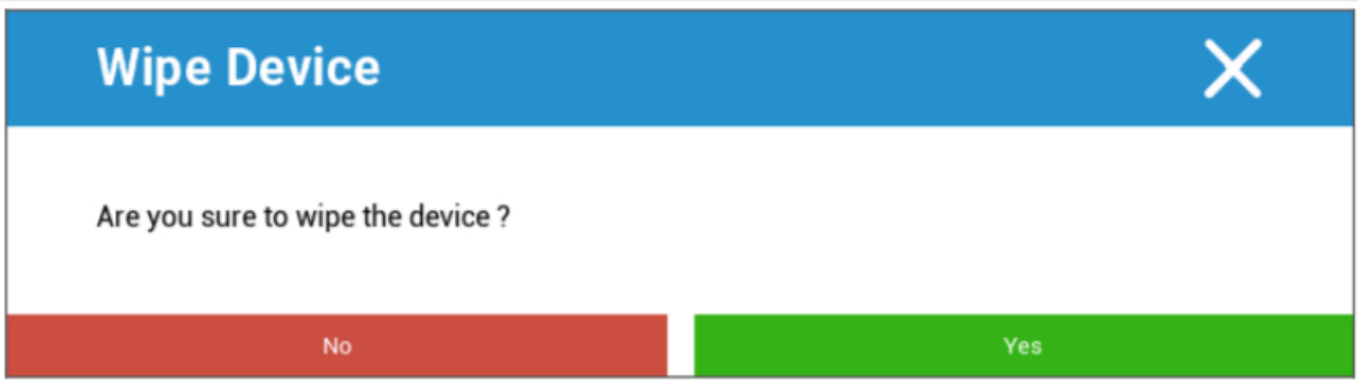
Здесь на устройство будет отправлена команда блокировки устройства (экран блокировки).

Удалить устройство

Здесь можно выполнить команду удаления. Вы можете еще раз решить, следует ли удалить устройство только из AppTec360 ("Delete from System") или удалить устройство из AppTec360 и дополнительно восстановить его заводские настройки ("Wipe & Delete").

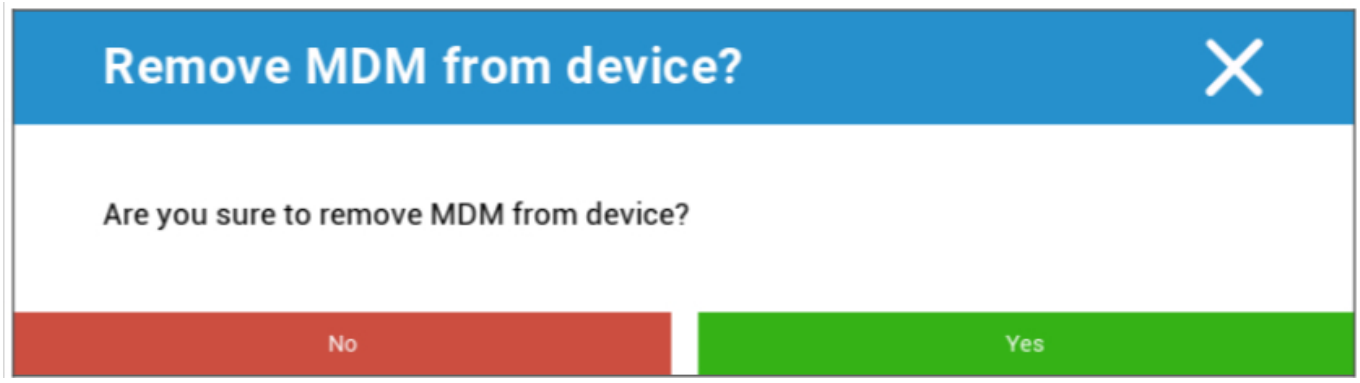
Стирание устройства

В разделе "Wipe Device" Вы можете выполнить полное стирание устройства. После этого устройство будет восстановлено до заводских настроек.



Кроме того, если устройство содержит SD-карту, Вы можете стереть SD-карту. Вы можете сделать это, установив для параметра "Wipe SD Card too? " в положение "Вкл.".

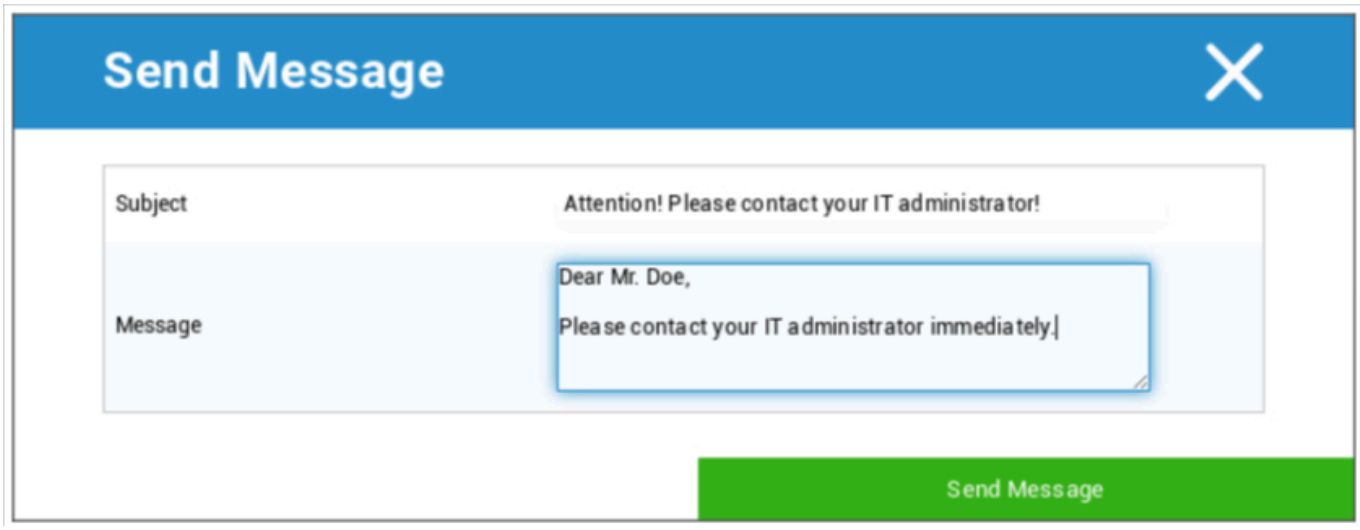
Удалите MDM



Это рекомендуемый метод для создания отделения от MDM.

Удаляется только информация, приложения и профили, предоставленные AppTec360, а это значит, что все корпоративные данные больше не будут доступны на устройстве конечного пользователя. Однако частная сфера не затрагивается и продолжает оставаться на устройстве конечного пользователя.

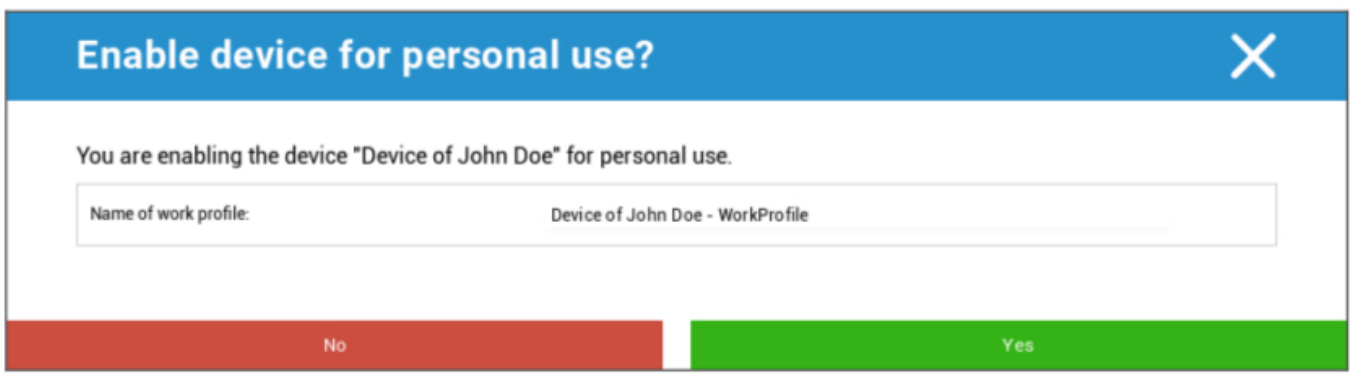
Отправить сообщение



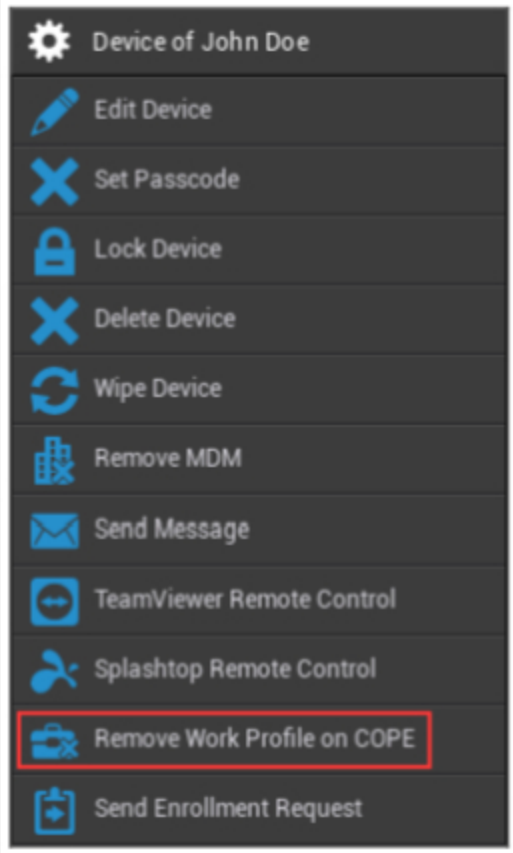
Здесь Вы можете отправить Push-уведомление на соответствующее устройство конечного пользователя.

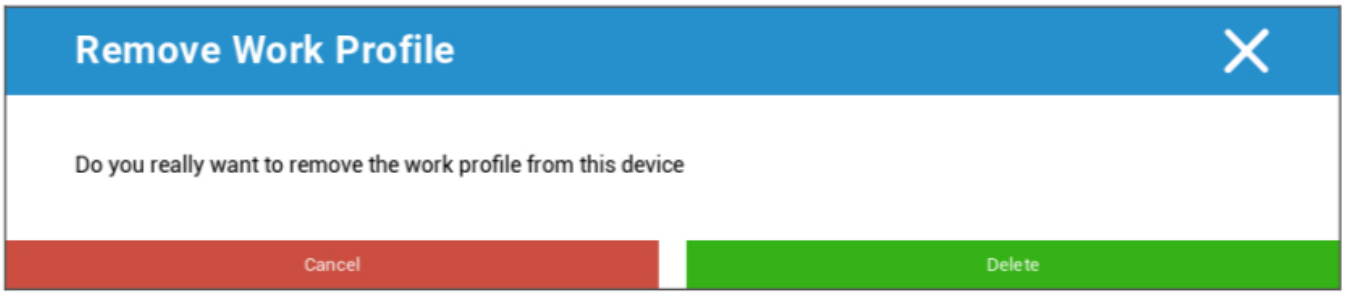
Переход в режим COPE

Создайте рабочий профиль на этом устройстве AE с полным управлением (Work Managed)



После перевода устройства в режим COPE Mode Вы можете удалить рабочий профиль, нажав на шестеренку **Remove Work Profile on COPE**:




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

Отправить запрос на зачисление

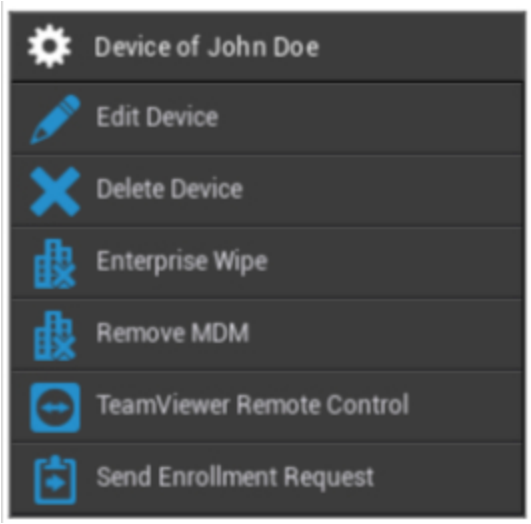
С помощью "Send Enrollment Request" Вы можете отправить запрос на зачисление (повторно) соответствующему пользователю.

Обратите внимание, что действителен только самый новый Запрос на зачисление.

Перенос устаревшего устройства

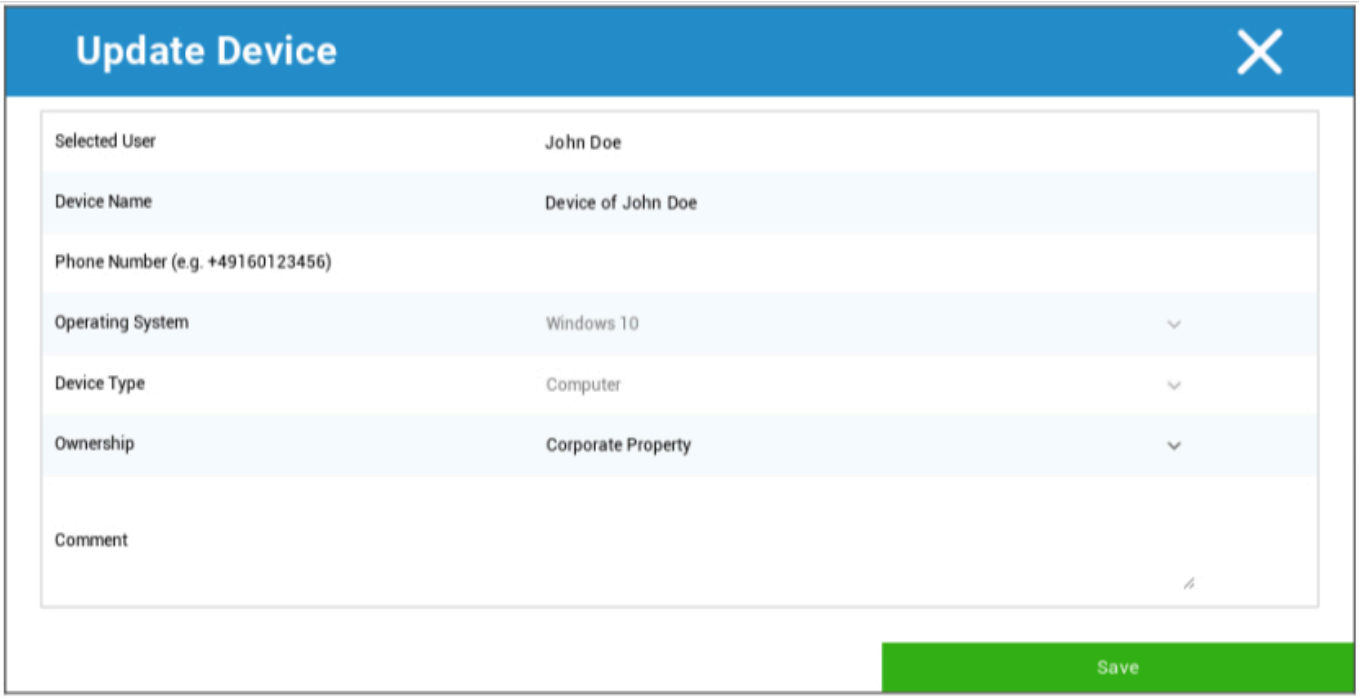
Перенесите профиль телефона/планшета Android в профиль AE Fully Managed Device (Work Managed).

Windows



Имя устройства	Имя выбранного устройства
Редактировать устройство	Редактирование устройства
Удалить устройство	Извлеките устройство из AppTec
Enterprise Wipe	Информация, приложения и профиль, предоставленные AppTec360, удаляются
Удалите MDM	
Удаленное управление TeamViewer	Удаленное управление устройством с помощью TeamViewer
Отправить запрос на зачисление	Отправьте запрос на зачисление (еще раз)

Редактировать устройство

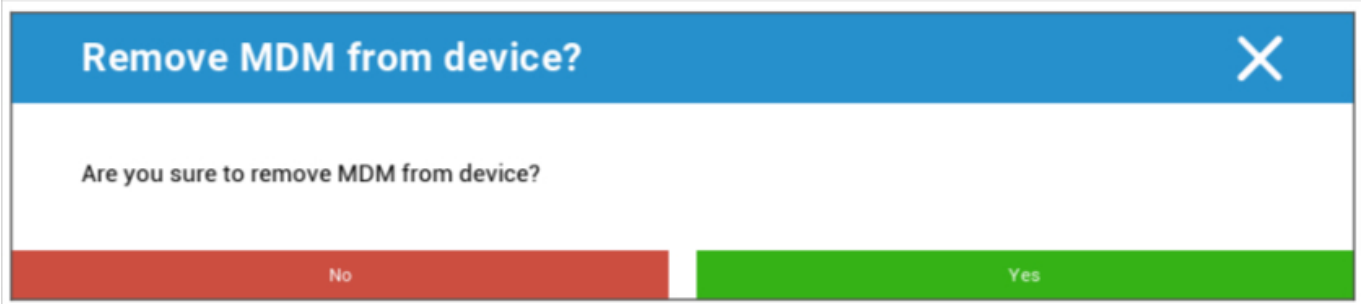


Здесь Вы можете обновить различную информацию об устройстве.

Удалить устройство

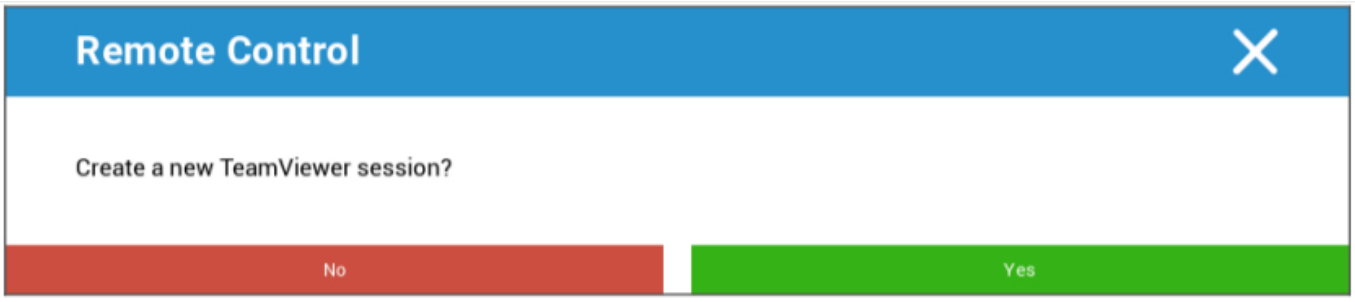
Здесь можно выполнить команду delete, которая только удаляет устройство из AppTec360.

Enterprise Wipe | Remove MDM



Удаляется только информация, приложения и профили, предоставленные AppTec360. Таким образом, корпоративные данные больше не будут доступны на устройстве конечного пользователя. Личная зона не затрагивается и продолжает оставаться на устройстве конечного пользователя.

Удаленное управление TeamViewer



Здесь Вы можете начать сеанс удалённого управления TeamViewer для этого устройства.

Отправить запрос на зачисление

С помощью "Send Enrollment Request" Вы можете отправить запрос на зачисление (повторно) соответствующему пользователю.

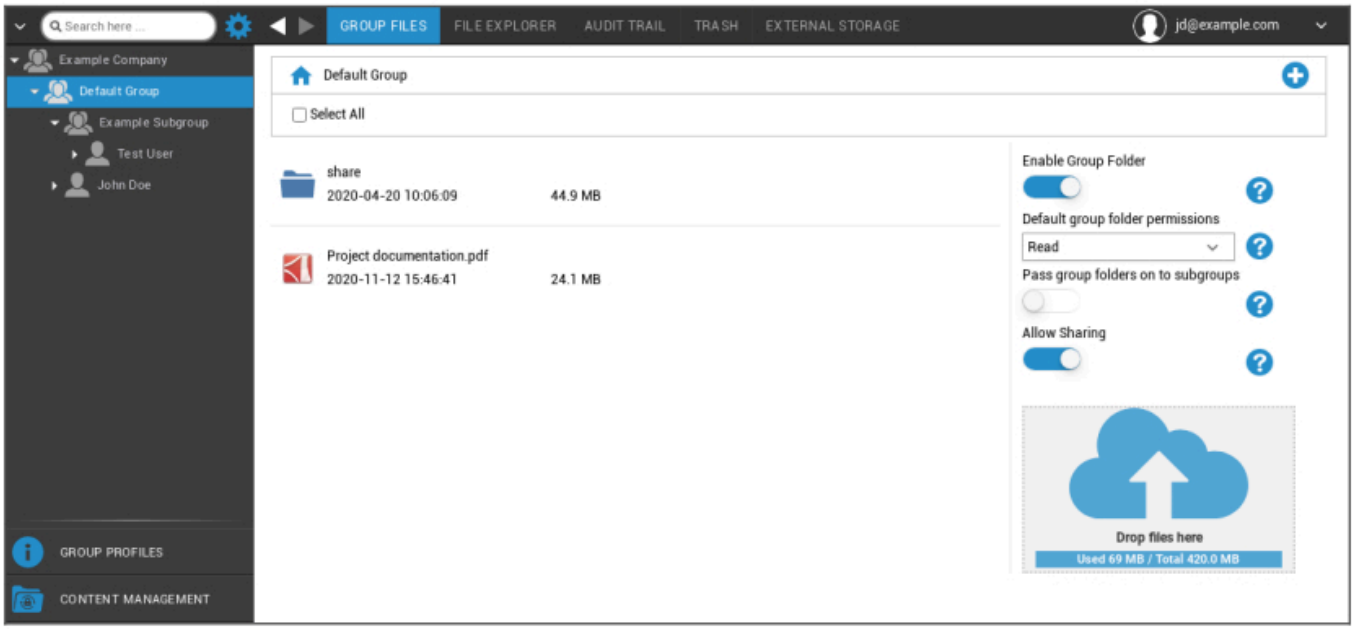
Управление контентом

Когда Вы находитесь в группе, Вы можете управлять AppTec's ContentBox с помощью "Content Management".

С помощью Content Box Вы можете безопасно распространять документы и другие корпоративные данные на устройствах конечных пользователей.

Групповые файлы

"Group Files" представляет собой фундаментальную часть ContentBox. Здесь Вы устанавливаете настройки, загружаете документы, создаете новые папки и т.д.



С помощью символа в правом верхнем углу Вы можете создавать новые папки, которые назначаются соответствующей группе с помощью "Add Folder".

С помощью символа в правом верхнем углу Вы можете создать новую папку через "Add Folder", которая должна быть назначена соответствующей группе.

Вы можете назвать папку как угодно.

Через "Upload Files" Вы можете загрузить данные. Здесь откроется Ваш Standard-Explorer. Разумеется, Вы можете выполнить эти два действия в каждой (под)папке.

С помощью символа в левом верхнем углу Вы можете вернуться в главное меню.

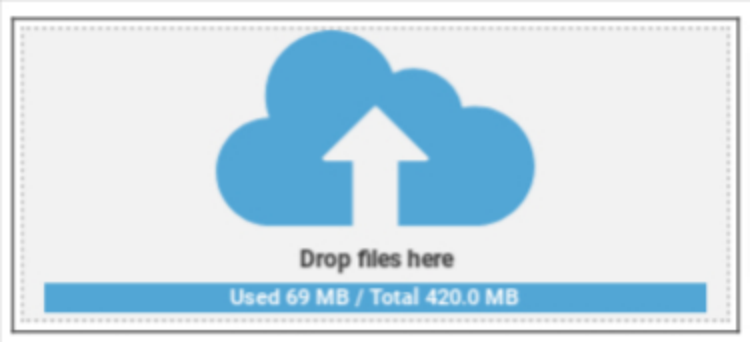
Вы можете выбрать несколько папок и файлов и загрузить их с помощью кнопки "Загрузить" или стереть их, нажав "Удалить".

Вы также можете выбрать все файлы и папки и выполнить команды "Загрузить" и "Удалить".

Когда Вы наводите курсор на папку или файл, Вы видите следующий обзор:

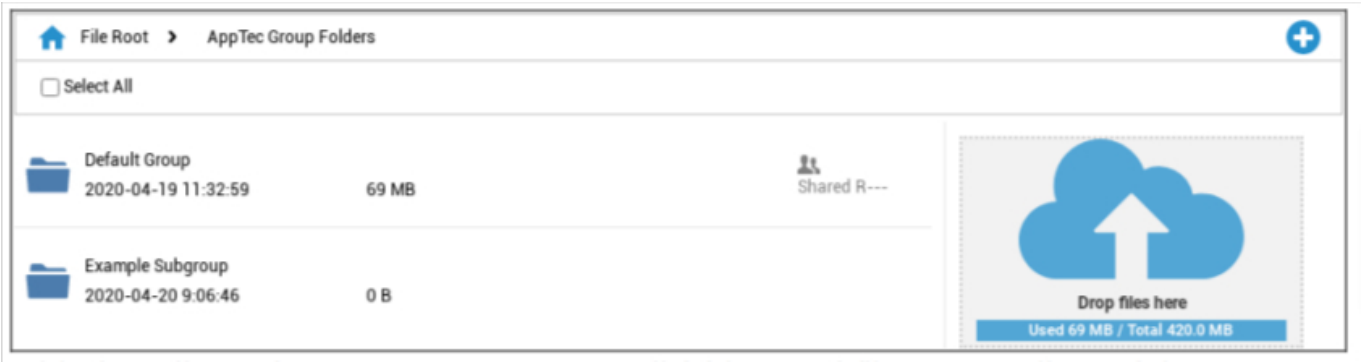
- С помощью "Rename" Вы можете переименовать папку/файл.
- С помощью "Download" Вы можете загрузить папку/файл.
- С помощью "Delete" Вы можете удалить папку/файл.

Включить групповую папку	Если эта функция активирована, все члены группы получают доступ к соответствующей папке
Разрешения групповых папок по умолчанию	Разрешения пользователей в выбранной группе: Чтение = разрешение только на чтение Обновить = разрешение на обновление Создать = разрешение на создание Удалить = разрешение на удаление
Передавайте групповые папки подгруппам	Если эта функция активирована, соответствующие подгруппы могут иметь доступ к родительским файлам данных
Разрешения для подгрупп	Разрешения пользователей в выбранной подгруппе: Чтение = разрешение только на чтение Обновить = разрешение на обновление Создать = разрешение на создание Удалить = разрешение на удаление
Разрешить совместное использование	Если эта функция активирована, пользователь может обмениваться файлами по ссылке



Для загрузки файлов Вы можете воспользоваться этим полем, перетащив файл с помощью Drag & Drop в это окно. Вы также можете нажать на это поле, чтобы выбрать и загрузить файл с помощью Internet Explorer.

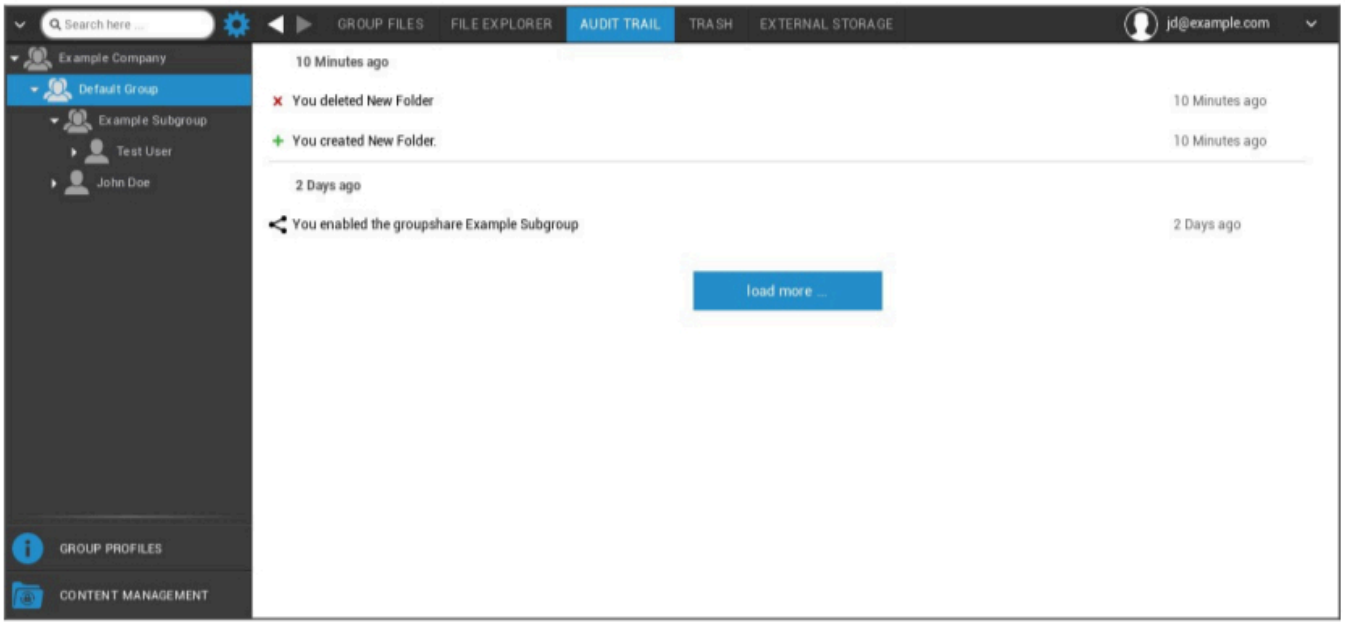
Проводник файлов



С помощью "Проводника файлов" Вы можете управлять всеми папками и файлами - независимо от группы, в которой они хранятся.

Вы также найдете настройки и кнопки, о которых Вы узнали в разделе "Групповые файлы".

Аудиторский журнал



В "Аудиторском журнале" Вы можете увидеть из истории, кто из пользователей что создал, удалил или поделился. Таким образом, Вы в любой момент сможете установить, что было сделано с корпоративными данными.

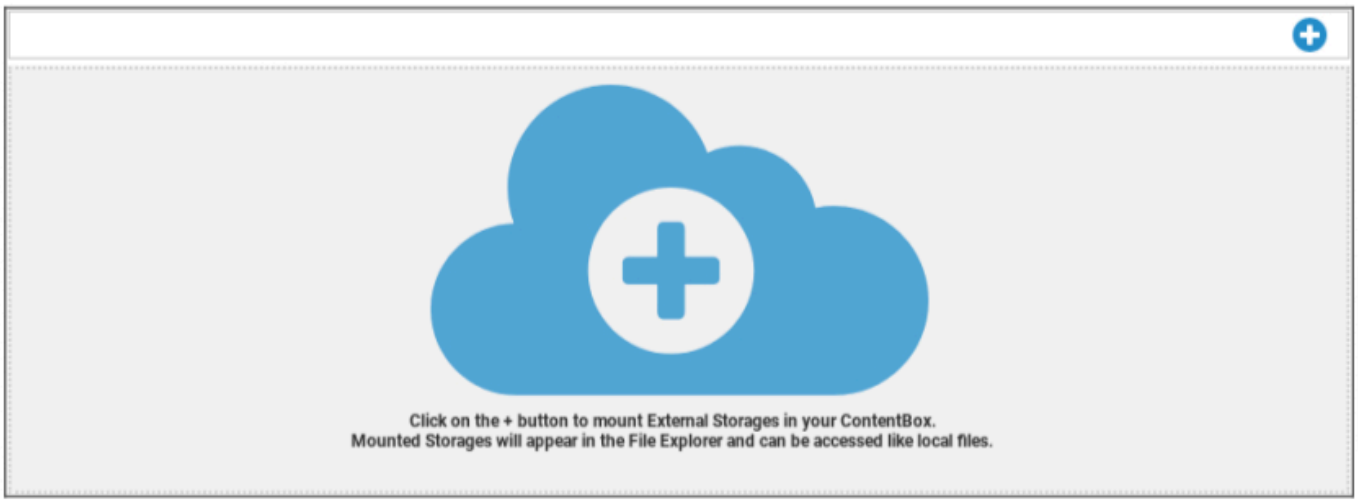
Мусор

Если Вы что-то удалили (случайно), Вы можете просмотреть папки и файлы в разделе "Корзина" и восстановить их, в соответствии с Вашими пожеланиями.

- С помощью "Undelete" Вы можете восстановить данные/папку.
- С помощью команды "Удалить" Вы можете навсегда удалить данные/папку - для этого Вам необходимо еще раз подтвердить команду удаления.

Обратите внимание, что объем памяти, используемый в корзине, уменьшает доступное "Общее пространство" - это требование ownCloud.

Внешнее хранилище



Под заголовком "Внешнее хранилище" Вы можете подключить внешнее хранилище.

С помощью символа можно добавить (дополнительное) хранилище.

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

Amazon S3	
Отображаемое имя	Отображаемое имя
Ключ доступа	Ключ доступа
Секретный ключ	Ключ безопасности
Ведро	Определенная идентификация подпапки, которая была назначена Вам
Имя хоста (необязательно)	Имя хоста (необязательно)
Порт (опционально)	Порт (опционально)
Регион	Регион (необязательно)
Включить SSL	Включить SSL
Включить стиль контура	Clear Path Адрес, который был присвоен Вам

FTP	
Отображаемое имя	Отображаемое имя
Хозяин	Хост-адрес
Имя пользователя	Имя пользователя
Пароль	Пароль
Корень	Главное меню
Безопасный ftps://	

SFTP	
Отображаемое имя	Отображаемое имя
Хозяин	Хост-адрес
Имя пользователя	Имя пользователя
Пароль	Пароль
Корень	Главное меню

ownCloud	
Отображаемое имя	Отображаемое имя
URL	URL-адрес ownCloud
Имя пользователя	Имя пользователя
Пароль	Пароль
Удаленная подпапка	Стандартная папка
Безопасный https://	

WebDAV	
Отображаемое имя	Отображаемое имя
URL	URL WebDAV
Имя пользователя	Имя пользователя
Пароль	Пароль
Корень	Главное меню
Безопасный https://	
Windows Share	Поддержка Windows Share появится в ближайшее время
SharePoint	Поддержка Microsoft SharePoint будет доступна в ближайшее время

Журнал аудита

Здесь Вы можете найти журнал, в котором записывается информация о действиях, выполняемых в консоли MDM.

С помощью значка фильтра Вы можете применить фильтры к отображаемому списку.

С помощью выпадающего меню **"Элементы на страницу"**: Вы можете выбрать количество элементов, которые будут отображаться на одной странице списка.

Принятые меры / Изменение настроек	Действие, которое было предпринято / Настройка, которая была изменена
Значение	Значение предпринятого действия / измененной настройки
Пользователь	Имя пользователя, который выполнил действие / изменил настройку
Дата	Временная метка того, когда это действие было выполнено / эта настройка была изменена
Путь / Тип	Путь к месту, где было выполнено это действие / изменена эта настройка

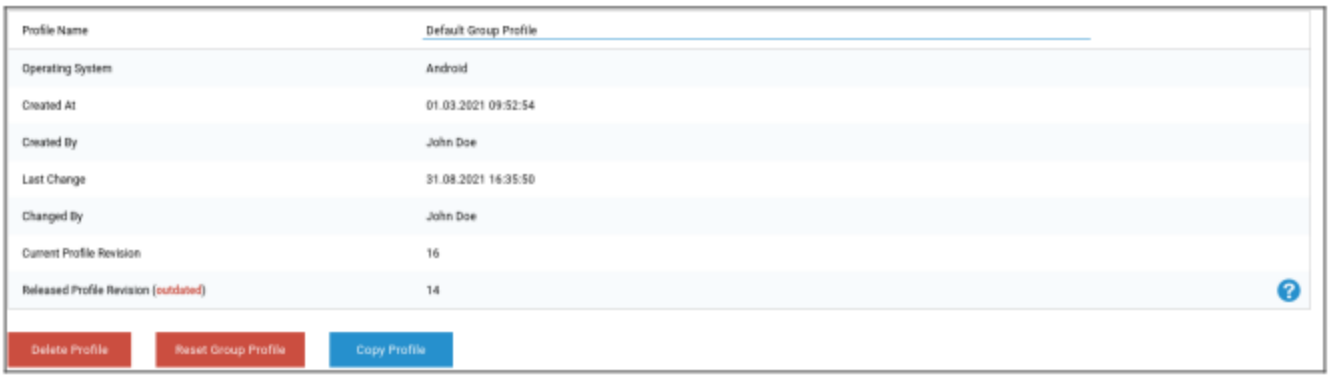
Конфигурация iOS

Общие сведения

В зависимости от того, что Вы выбрали в данный момент - группу или устройство, дисплей и его подпункты будут отличаться - обратите на это внимание!

Обзор профиля группы (только на уровне группы)

Открыв профиль группы, Вы получите краткий обзор профиля



Имя профиля	Название профиля (может быть изменено здесь)
Операционная система	Операционная система, для которой предназначен профиль
Создано в	Время создания
Created By	Создатель профиля
Последнее изменение	Время последнего изменения профиля
Изменено	Учетная запись, которая внесла последние изменения
Текущий пересмотр профиля	Пересмотр сохраненного состояния профиля
Выпущенный пересмотр профиля	Назначенная ревизия профиля ("Назначить сейчас"). Если за текстом на ярлыке отображается "(устаревший)", это означает, что Вы сохранили профиль, но еще не назначили его, поэтому устройства все еще будут получать старую версию.

Общая информация

Если Вы находитесь непосредственно на устройстве, Вы получите краткий обзор выбранного Вами устройства.

Имя устройства	Имя устройства
Номер телефона	Номер телефона устройства
Модель	Номер модели
Операционная система	OS
Серийный номер	Серийный номер устройства
Владение устройством	Корпоративное или частное устройство Корпоративный = корпоративное устройство Сотрудник = личное устройство
Тип устройства	Тип устройства (планшет или телефон)
Взломанный	Если на устройстве есть джейлбрейк
Под наблюдением	Указывает, является ли это устройство контролируемым.
Соответствующий	Если были нарушены какие-либо рекомендации
Последний раз видели	Состояние, когда устройство в последний раз связывалось с сервером AppTec360 Server

Настройки

Эти настройки содержат имя устройства и предопределенный фон.

Назовите устройство системным именем	Имя, которое будет выдано в AppTec360 Console (в левой иерархической структуре), будет таким же, как и на соответствующем устройстве конечного пользователя (можно посмотреть в настройках устройства)
Используйте пользовательские обои (только для устройств под наблюдением)	Здесь Вы можете предварительно определить фон, который должен отображаться на устройстве конечного пользователя (например, для типа корпоративного брендинга устройства). Доступно только в режиме "Под наблюдением"!
Автоматические обновления ОС	Принудительное обновление ОС, если оно доступно. Только для устройств DEP в контролируемом режиме.
Пользовательские шрифты	Здесь Вы можете добавить пользовательские шрифты.
Имя	Необязательно. Видимое пользователю имя шрифта. Это поле заменяется реальным именем шрифта после установки.
Шрифт	Загрузите файл шрифта (.otf или .ttf).

Пересмотр конфигурации

Здесь Вы получите обзор того, какой групповой профиль назначен для данного устройства.

Если Вы нажмете на профиль группы, Вы получите прямой доступ к нему и сможете выполнить настройки.

С помощью этого символа Вы можете вернуть назначенные приложения к настройкам группового профиля.

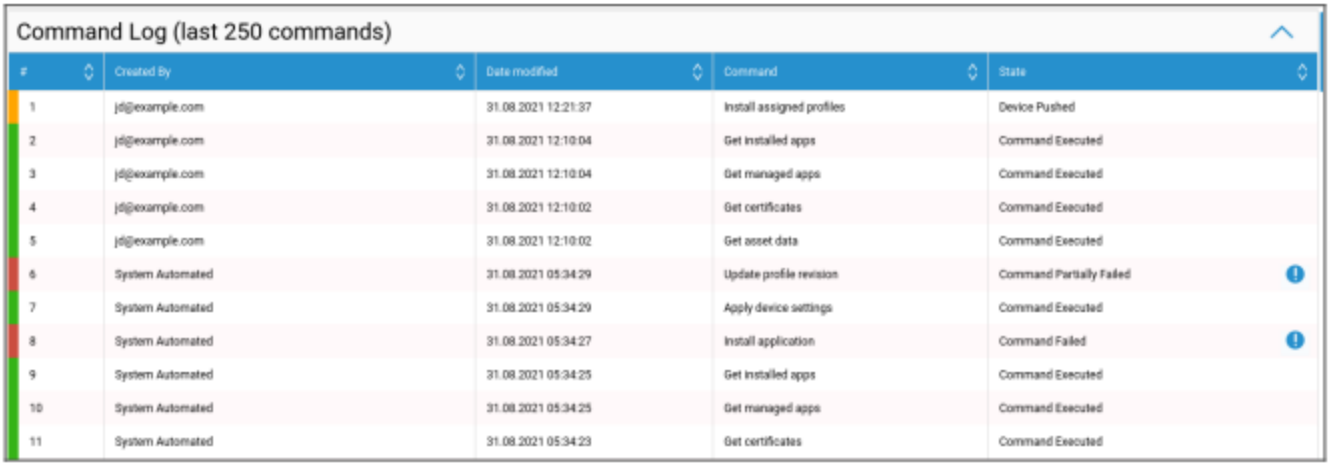
С помощью этого символа Вы можете сбросить профиль устройства, чтобы он вообще не имел никаких настроек.

"Доступна более новая редакция" означает, что профиль группы был изменен и сохранен, но не назначен. Чтобы применить изменения к устройствам, групповой профиль должен быть назначен с помощью "Назначить сейчас" на уровне группы.

Журнал устройства (только на уровне устройства)

Журнал команд

Здесь Вы можете увидеть, какие команды были отданы устройству и каков их статус.



Команды, созданные с помощью "System Automated", автоматически создаются системой.

Возможные статусы команд

Устройство нажимается	Запрос push был отправлен в службу push (например, APNS), чтобы сообщить устройству о необходимости подключиться обратно к серверу EMM.
Команда Создана	Команда была создана в системе.
Команда отправлена	Команда была отправлена на устройство после того, как оно подключилось к серверу.
Команда выполнена	Команда была успешно выполнена.
Команда не выполнена	Команда завершилась неудачно. *
Команда частично не выполнена	В зависимости от ОС устройства некоторые команды могут быть сгруппированы вместе. В этом случае некоторые части этой группы команд оказались неудачными. *
Команда выполнена, в итоге - отказ	Команда была выполнена, но, возможно, она не была выполнена.
Command Repushed	Команда была повторно запущена пользователем.
Выброшенные	Команда была отменена. Например, потому что она была заменена другой командой или устройство было перерегистрировано, и старые команды были удалены.

Если за сообщением стоит восклицательный знак, Вы можете получить дополнительную информацию, наведя курсор на значок.

Управление активами (только на уровне устройств)

Управление активами (только на уровне устройств)

Информация об устройстве

Модель	Номер модели устройства
Операционная система	OS
Версия ОС	Версия ОС
Серийный номер	Серийный номер
UDID	UDID устройства
Имя устройства	Имя устройства
Под наблюдением	Отображает, находится ли устройство под наблюдением
Состояние батареи	Состояние батареи

Wi-Fi

IP-адрес	IP-адрес устройства
WiFi MAC	MAC-адрес WiFi

Клетчатка

Статус	Статус (SIM-карта присутствует)
Номер телефона	Номер телефона
Статус роуминга	Текущий статус роуминга
Роуминг (голос/данные)	Статус роуминга для голоса/данных
IP-адрес	IP-адрес
IMEI	IMEI-номер
Оператор/ перевозчик	Поставщик услуг сотовой связи
Сеть оператора SIM	Сеть оператора SIM
Версия для носителей	Версия для носителей
Встроенное ПО модема	Встроенное ПО модема
Текущий MCC/MNC	См. раздел "SIM MCC/MNC".
SIM MCC/MNC	Код страны мобильной связи - это установленная МСЭ идентификация страны в соответствии со стандартом E.212, которая в сочетании с кодом мобильной сети (MNC) используется для идентификации сотовой сети (=код страны). Когда Вы переходите в другую сотовую сеть, "Current MCC/MNC" и "SIM MCC/MNC", соответственно, отличаются.

Bluetooth

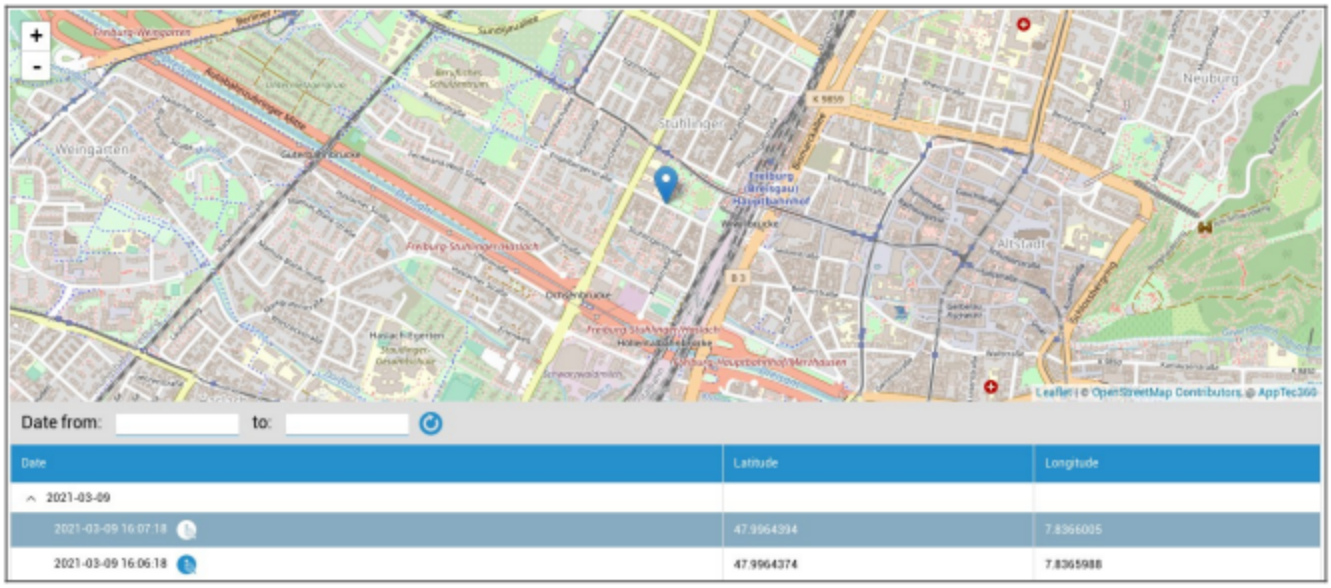
Bluetooth MAC	MAC-адрес Bluetooth

Управление безопасностью

Защита от кражи (только на уровне устройства)

Информация GPS (только на уровне устройства)

Здесь Вы можете оценить текущее/последнее местоположение устройства. Локализация может быть защищена одним или даже двумя паролями - см: Общие настройки - Конфиденциальность - Доступ к GPS



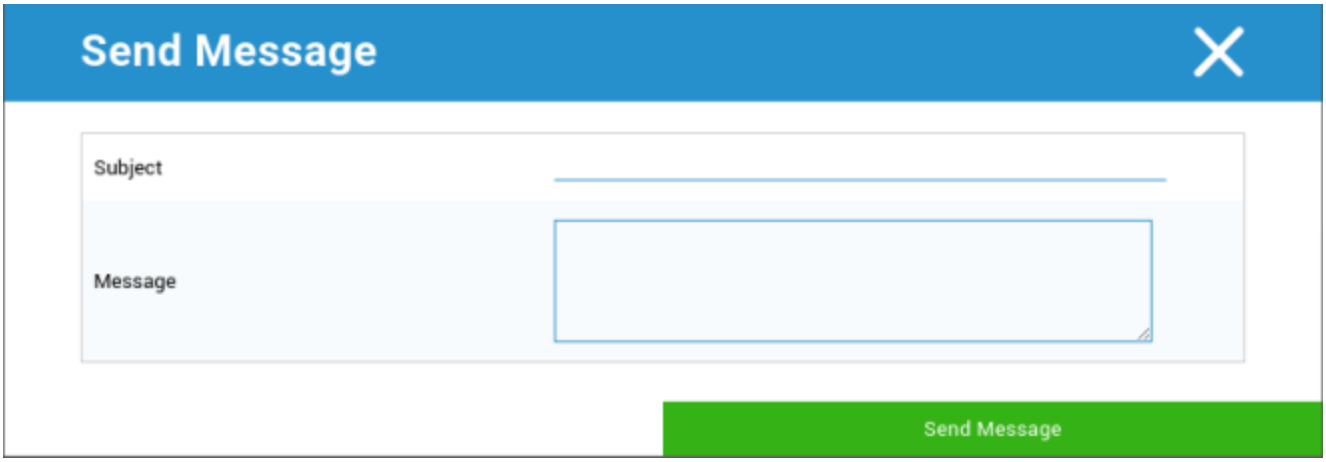
Wipe & Lock (только на уровне устройства)

В разделе "Wipe & Lock" Вы можете выполнить следующие три действия:

Полное вытирание	Устройство возвращается к заводским настройкам (корпоративные, а также личные данные удаляются)
Enterprise Wipe	С устройства конечного пользователя удаляются только корпоративные данные (все приложения, данные и т.д., которые были предоставлены AppTec)
Экран блокировки	Активирована блокировка экрана, достаточно разблокировать устройство с помощью пароля устройства/PIN-кода
Криминалистическая блокировка (только для контролируемых устройств)	Если эта функция активирована с помощью символа  , устройство будет заблокировано, на экране появится сообщение, которое нельзя будет закрыть. Сотрудник также не сможет разблокировать устройство. Только администратор может разблокировать устройство в консоли с помощью символа разблокировки  .
Разрешить блокировку активации (только для контролируемых устройств)	Если эта функция активирована, устройство будет заблокировано, как только в настройках iCloud будет активирована функция "Найти мой iPhone".

Сообщение (только на уровне устройства)

В следующем окне Вы можете заполнить тему и сообщение и отправить его на устройство конечного пользователя:



Конфигурация безопасности

Passкод

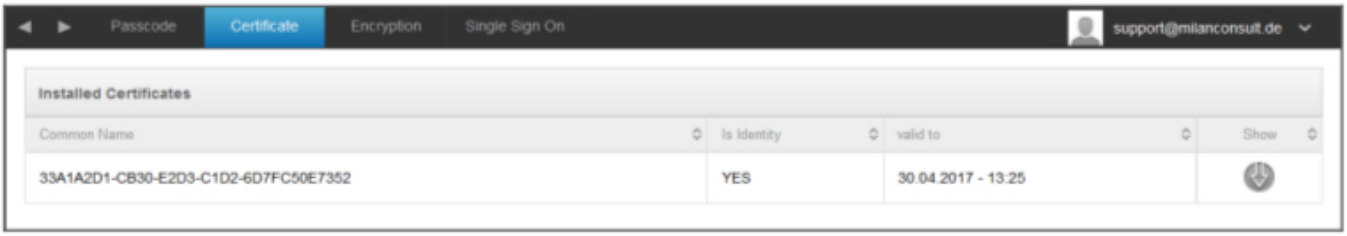
Здесь Вы устанавливаете настройки для пароля устройства

Разрешена деактивация кода	Когда эта настройка активирована, запрос на ввод пароля отсутствует. Как только пароль установлен, его невозможно деактивировать
Разрешить простое значение	Разрешите пользователю использовать одинаковые, возрастающие и уменьшающиеся строки номеров (например, 1234, 1111).
Требуется буквенно-цифровое значение	Пароли должны содержать хотя бы одну букву
Минимальная длина пароля	Минимальная длина пароля
Минимальное количество сложных символов	Минимальное количество буквенно-цифровых символов в пароле
Максимальный возраст пароля	Количество дней, по истечении которых пароль должен быть изменен
Максимальная автоблокировка	Максимальное время, по истечении которого устройство будет заблокировано
Максимальный льготный период для блокировки устройства	Время, по истечении которого устройство переходит в заблокированный режим Stand-By
Максимальное количество неудачных попыток	Устанавливает, как часто пароль может быть введен неверно, прежде чем будет произведено полное стирание устройства
Максимальный срок действия пароля (1-730 дней)	Максимальный возраст пароля
История passкодов (1-50 passкодов)	После этого числа разрешается использовать старый пароль

Щелчок по корзине открывает диалог сброса пароля, с помощью которого можно стереть забытый пароль устройства.

Сертификат (только на уровне устройства)

Отображает сертификаты, которые доступны на устройстве



Шифрование

Требуйте шифрования при хранении	Активируйте функцию шифрования установленного устройства

Единый вход в систему

В пункте "Single Sign-On" Вы можете настроить аутентификацию Kerberos.

Здесь Вы устанавливаете учетные данные доступа и соответствующие URL / приложения, которым разрешено использовать токены Kerberos.

Доступно в режиме под наблюдением	
Название счета	Название счета
Основное имя	Уникальный идентификатор, на который можно распространять билеты Kerberos.
Realm	Ваш Kerberos Realm, который будет использоваться (например, Ваш домен)

С помощью Символа Вы можете создать дополнительные URL-адреса.

Шаблон URL, используемый для ограничения этой учетной записи	URL, по которым можно распространять билеты Kerberos, будет определен.

С помощью Символа Вы можете установить дополнительные Приложения.

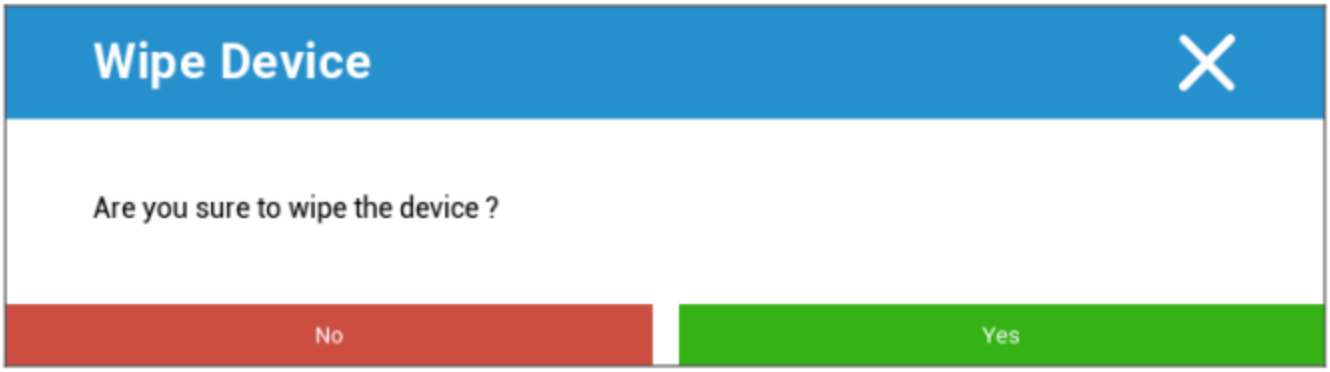
Приложения для ограничения этой учетной записи	Будет определено Приложения, на которые можно распространять билеты Kerberos

Окончание срока службы (только на уровне устройства)

Стирание (только на уровне устройства)

В разделе "Wipe" Вы можете восстановить заводские настройки устройства. При этом корпоративные, а также личные данные будут удалены с устройства конечного пользователя.

При нажатии на символ "Минус" Вы должны получить следующее сообщение



Ответив "Да", Вы можете выполнить стирание.

В разделе "Отчет о стирании" отображаются следующие пункты

Стерто	История о том, кто выполнял протирание
Дата	Дата
Статус	Статус (например, успешно ли выполнено стирание)

Настройки ограничений

Функциональность устройства

Здесь Вы можете заблокировать отдельные функциональные возможности устройства конечного пользователя

Разрешите установку приложений	Разрешите установку приложений
Разрешить камеру	Разрешите использовать фотоаппарат
Разрешить FaceTime	Разрешить FaceTime
Разрешить захват экрана	Разрешить захват экрана
Разрешите автосинхронизацию в роуминге	Разрешите автосинхронизацию в роуминге
Разрешить Siri	Разрешить Siri
Разрешите голосовой набор	Разрешите голосовой набор
Разрешите покупки в приложении	Разрешите покупки в приложении
Требуйте пароль iTunes Store для всех покупок	Требуйте пароль iTunes Store для всех покупок
Разрешить многопользовательские игры	Разрешить многопользовательские игры
Разрешите добавлять друзей из Game Center	Разрешите добавлять друзей из Game Center
Разрешить открывать из управляемых в неуправляемые	Разрешите открывать содержимое управляемых приложений в неуправляемых приложениях
Разрешить открывать из неуправляемых в управляемые	Разрешите открывать содержимое неуправляемых приложений в управляемых приложениях
Разрешить просмотр сегодняшнего дня на экране блокировки	Когда эта настройка активна, вид "Сегодня" будет отображаться в Центре уведомлений на экране блокировки.
Разрешите центр управления на экране блокировки	Разрешите Центр управления на экране блокировки
Разрешить TouchID	Разрешить TouchID

Разрешите обновления PKI по воздуху	Разрешите обновления PKI по воздуху
Разрешите пользоваться записной книжкой при блокировке	Разрешите пользоваться записной книжкой, когда устройство заблокировано
Ограничьте отслеживание рекламы	Эта функция отключает отслеживание рекламы (например, рекламодатели не могут использовать отслеживание рекламы для распространения персонализированных объявлений)
Разрешить передачу	Разрешить передачу
Позволить интернет-результатам быть в центре внимания	Разрешите результаты Интернета в прожекторе (например, Bing или Wikipedia)
Требуйте ввод пароля при первом сопряжении AirPlay	Требуйте ввод пароля при первом сопряжении AirPlay
Защита запястья Force Watch	Если эта функция активирована, Apple Watch будут вынуждены использовать "Wrist Protection" (распознавание запястья).
Разрешить фотобиблиотеку iCloud	Разрешает использование фотобиблиотеки iCloud. Если не разрешить, то все фотографии, которые не были полностью загружены из iCloud, будут стерты на локальном хранилище
Доступно в режиме "Под наблюдением	
Разрешить изменение учетной записи	Разрешите модификацию "почта, контакты, календарь".
Разрешить AirDrop	Разрешить AirDrop
Разрешить модификацию приложений для сотовых телефонов	Этот параметр блокирует настройку того, каким приложениям разрешено использовать мобильные данные Этот параметр можно, например, установить вручную на устройстве конечного пользователя, а затем активировать это ограничение
Разрешите Siri запрашивать пользовательский контент из Интернета	Веб-поиск на определенных сайтах заблокирован, например, в Википедии, потому что каждый может вносить изменения по своему усмотрению
Включите фильтр ненормативной лексики в Siri	Ненормативная лексика, направленная на Siri, подвергается цензуре
Разрешить iBook Store	Разрешить iBook Store

Разрешить эротику в iBook Store	Разрешить эротику в iBook Store
Разрешите изменять настройки "Найти моих друзей	Разрешите изменять настройки "Найти моих друзей
Разрешить Game Center	Разрешить Game Center
Разрешить сопряжение с хостом	Сопряжение с управляющим компьютером
Разрешите устанавливать профили конфигурации	Разрешите установку профилей конфигурации
Разрешить Удалить приложение	Удаление управляющих приложений
Разрешить iMessage	Разрешить iMessage
Разрешите стереть все содержимое и настройки	Позволяет стирать все содержимое и настройки
Позволяет настраивать ограничения	Позволяет настраивать ограничения
Разрешить подкаст	Разрешить подкаст
Разрешить поиск определений	Разрешить поиск определений
Разрешить предиктивную клавиатуру	Разрешить предиктивную клавиатуру
Разрешить автокоррекцию	Разрешить автоматическую коррекцию
Разрешить установку приложений UI	Если эта функция деактивирована, приложения не могут быть установлены из публичного AppStore (значок больше не будет отображаться). Однако приложения по-прежнему можно устанавливать через iTunes и Конфигуратор
Разрешить сочетания клавиш	Разрешите сочетания клавиш, если устройство подключено к физической клавиатуре
Разрешите сопряжение с Apple Watch	Запрещает сопряжение между устройством и Apple Watch, существующие соединения будут прерваны
Разрешите модификацию пароля	Если это не разрешено, ни один пароль устройства не может быть добавлен, изменен или удален
Разрешите изменять имя устройства	Рекомендации по определению того, можно ли изменить имя устройства
Позволяет изменять обои	Рекомендации по определению того, можно ли менять обои

Разрешите автоматическую загрузку приложений	При деактивации купленное приложение не будет автоматически устанавливаться на другие устройства. Не относится к обновлениям для существующих приложений
Разрешить новости	Разрешить новости на устройстве iOS
Разрешите доверять корпоративным приложениям	Если установлено значение false, это предотвращает доверие к корпоративным приложениям

iCloud

Блокируйте определенные функции во время сопряжения с iCloud

Разрешить резервное копирование	Разрешить резервное копирование
Разрешите синхронизацию документов	Разрешите синхронизацию документов
Разрешить фотопоток	Разрешить фотопоток
Разрешить общий фотопоток	Разрешить общий фотопоток
Разрешить синхронизацию облачной связки ключей	Разрешить синхронизацию облачной связки ключей
Разрешите управляемым приложениям хранить данные	Разрешите управляемым приложениям хранить данные
Разрешите синхронизацию заметок и основных моментов для корпоративных книг	Разрешите синхронизацию заметок и основных моментов для корпоративных книг
Разрешить резервное копирование книг предприятия	Разрешить резервное копирование книг предприятия

Безопасность и конфиденциальность

Блокируйте эти функциональные возможности, связанные с диагностическими данными

Разрешите отправлять диагностические данные в Apple	Разрешите отправлять диагностические данные в Apple
Разрешите пользователю принимать недоверенные сертификаты TLS	Разрешите пользователю принимать недоверенные сертификаты TLS
Принудительное зашифрованное резервное копирование	Принудительное зашифрованное резервное копирование

BYOD

Встроенная система безопасности iOS (контейнер)

iOS всегда различала управляемые (бизнес) и неуправляемые (частные) устройства. Все, что поступает из системы MDM, рассматривается как управляемое. Например, если Вы установите приложение через MDM или настроите учетную запись Exchange, это будет рассматриваться iOS как управляемое.

Все остальное, что настраивается/устанавливается на устройство вручную, будет считаться неуправляемым. Например, если пользователь самостоятельно установит WhatsApp или если он добавит учетную запись Exchange. Однако такое разделение никогда не влияло на контакты. Но начиная с iOS 11.3 (и выше) это было добавлено и для контактов.

Поскольку это базовая функциональность операционной системы, Вам не нужно что-то устанавливать или настраивать специальный контейнер.

Активируйте встроенную функцию для разделения личных и рабочих приложений/информации/файлов. Эта настройка также отключит некоторые другие функции, которые могут по ошибке отключить часть этого разделения.

Активация

Активируйте контейнерные решения, которые поддерживаются AppTec360

Включите разделение контейнера Google	Включите разделение контейнера Google
Включите SecurePIM Container	Включите SecurePIM Container

Если Вы активировали SecurePIM Container, Вы также найдете следующий пункт в разделе "Активация". Кроме того, сразу же откроются еще четыре вкладки, которые описаны ниже.

Адрес электронной почты службы поддержки	Адрес электронной почты службы поддержки, куда пользователь может обратиться с проблемами

Пароль SecurePIM

В разделе "SecurePIM Password" Вы можете установить рекомендации по надежности пароля.

Таймаут сессии	Здесь Вы можете установить, через сколько минут необходимо снова ввести новый пароль, если SecurePIM работает в фоновом режиме.
Длина пароля	Длина пароля для доступа к контейнеру SecurePIM
Символы верхнего регистра	Минимальное количество символов верхнего регистра
Символы нижнего регистра	Минимальное количество символов нижнего регистра
Специальные символы	Минимальное количество специальных символов
Цифры	Минимальное количество цифр
Применение салфеток	Количество раз, когда пароль может быть введен неверно, прежде чем содержимое SecurePIM будет удалено (Приложение, однако, по-прежнему остается на устройстве конечного пользователя).

SecurePIM Безопасность

В разделе "SecurePIM Security" Вы можете установить различные настройки безопасности.

Обнаружение устройств с джейлбрейком	Если эта настройка активирована, доступ к контейнеру SecurePIM будет заблокирован, как только устройство будет определено как взломанное.
Защищенные текстовые поля	Содержимое полей отправки будет зашифровано, никакая информация не попадет в ОС (iOS). Примечание: Пока эта настройка активна, автокоррекция больше не доступна
Экспорт контактных данных на устройство	Если эта настройка активирована, то пользователю разрешается экспортировать Контакты Exchange на свое локальное устройство Примечание: Экспортируются только имя и номер телефона.
Место проведения шоу	Если эта настройка активирована, местоположение предстоящих событий будет отображаться в панели уведомлений
Показать название события	Если эта настройка активирована, заголовок предстоящего события будет отображаться в панели уведомлений

SecurePIM Browser

Здесь Вы можете настроить браузер SecurePIM.

С помощью этого символа Вы можете определить новый URL.

С помощью этого символа Вы сможете снова удалить определенный URL.

"URL из белого списка" - это URL, которые могут быть загружены.

URL-адреса в "черном списке" - это URL-адреса, которые не могут быть загружены и, таким образом, блокируются.

Обратите внимание, что записи в "Белом списке" имеют более высокий приоритет, чем записи в "Черном списке". В разделе "Bookmark Title" Вы можете указать название. С помощью "Bookmark URL" Вы можете связать URL-адрес с названием закладки - таким образом, Вы сможете раздавать индивидуальные закладки соответствующим пользователям.

Обмен

В разделе "Exchange" Вы можете настроить учетную запись Exchange.

Адрес электронной почты ActiveSync	Адрес электронной почты (обратите внимание на "Placeholders")
Вход в систему ActiveSync Exchange	Имена пользователей Exchange (обратите внимание на "Placeholders")
ActiveSync Exchange Server	Адрес сервера Exchange (FQDN)
ActiveSync Домен Exchange	Доменный адрес Exchange
Сертификат пользователя	Сертификат пользователя
Аутентификация на основе сертификата	Пользователь аутентифицирует себя с помощью сертификата
Разрешить шифрование S/MIME	Позволяет пользователю шифровать свою почту
Разрешить подписание S/MIME	Позволяет пользователю подписывать свою почту
Проверка CRL	Если он активен, частный сертификат будет сравнен с CRL (Certificate Revocation List).

Управление соединениями

Wi-Fi

Идентификатор набора услуг (SSID)	SSID подключаемой сети
Автоматическое присоединение	Активируйте автоматическое присоединение при подключении к сети
Скрытая сеть	Активировать, в случае если точка доступа не передает SSID

Настройка прокси

Настройка прокси для каждой точки доступа

Нет	Установить отсутствие прокси
Руководство	Установите ручной прокси-сервер
URL-адрес прокси-сервера	Адрес для доступа к настройкам прокси-сервера
Порт	Установите порт для прокси-сервера
Аутентификация	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Автоматический	Установите прокси автоматически
URL-адрес прокси-сервера	URL для доступа к настройкам прокси-сервера

Тип безопасности

Установите тип безопасности для точки доступа

WEP	
Пароль	Пароль для точки доступа

WPA/WPA2	
Пароль	Пароль для точки доступа

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise		
Протоколы		
TLS	Активировать/деактивировать	
TTLS	Активировать/деактивировать	
LEAP	Активировать/деактивировать	
PEAP	Активировать/деактивировать	
EAP-FAST	Активировать/деактивировать	
EAP-SIM	Активировать/деактивировать	
Используйте PAC		Использование PAC (Protected Access Controll)
Положение PAC	Конфигурация Provision PAC	
Предоставление PAC анонимно	Анонимное предоставление PAC	
Внутренняя аутентификация	Протокол аутентификации, который должен быть использован: PAP, CHAP, MSCHAP, MSCHAPv2	
Имя пользователя	Имя пользователя для аутентификации	
Не используйте пароль для каждого соединения	Не используйте пароль для каждого соединения	
Сертификат личности	Загрузите/выберите сертификат аутентификации	
Внешняя идентичность	Идентичность, которую можно увидеть снаружи	
Trust		
Доверенный сертификат 1	Загрузите первый доверенный сертификат	
Доверенный сертификат 2	Загрузите второй доверенный сертификат	
Доверенный сертификат 3	Загрузите третий доверенный сертификат	
Имена сертификатов доверенных серверов	Имена ожидаемых сертификатов сервера	

		(в списке, разделенном запятыми)	

Нет	Не создавайте никакой безопасности

VPN

Имя соединения	Имя VPN-профиля

Тип VPN

VPN

Весь сетевой трафик устройства будет направляться через VPN-соединение.

Тип соединения	Установите тип VPN-соединения
IPsec (cisco)	Протокол IPsec от компании cisco
PPTP	Протокол PPTP
L2TP	Протокол L2TP
Cisco AnyConnect	Протокол AnyConnect
Juniper SSL	Протокол SSL от Juniper
F5 SSL	Протокол F5 SSL
SonicWall mConnect	SonicWall mobile Connect
Аруба VIA	Протокол Aruba VIA
Пользовательский SSL	Подключение через пользовательский SSL
OpenVPN	Протокол OpenVPN

VPN для каждого приложения

При открытии определенного приложения будет установлено VPN-соединение

Автоматически запускайте VPN-соединение для каждого приложения	Автоматически запускайте VPN-соединение для каждого приложения
Тип соединения	Установите тип VPN-соединения
Cisco AnyConnect	Протокол AnyConnect
Juniper SSL	Протокол SSL от Juniper
F5 SSL	Протокол F5 SSL
SonicWall mConnect	SonicWall mobile Connect
Аруба VIA	Протокол Aruba VIA
Пользовательский SSL	Подключение через пользовательский SSL
OpenVPN	Протокол OpenVPN

Настройка прокси

Настройка прокси для VPN-соединения

Нет	Установить отсутствие прокси
Руководство	Установите прокси вручную
URL-адрес прокси-сервера	Адрес для доступа к настройкам прокси-сервера
Порт	Установите порт для прокси-сервера
Аутентификация	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Автоматический	Установите прокси автоматически
URL-адрес прокси-сервера	URL для доступа к настройкам прокси-сервера

Показать держатели	Отображает все доступные пользовательские переменные, которые AppTec360 может использовать

APN

Имя точки доступа	Имя точки доступа
Имя пользователя точки доступа	Имя пользователя точки доступа
Пароль точки доступа	Пароль точки доступа
Прокси-сервер	Адрес прокси-сервера
Порт	Соответствующий порт прокси-сервера

Клетчатка

Включить роуминг данных	Включить роуминг данных
Включить голосовой роуминг	Включить голосовой роуминг
Включить точку доступа	Включить точку доступа

HTTP-прокси

Тип прокси	
Руководство	Установите прокси вручную
URL-адрес прокси-сервера	Адрес для доступа к настройкам прокси-сервера
Порт	Установите порт прокси-сервера
Аутентификация	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Автоматический	Установите прокси автоматически
URL прокси PAC	URL прокси PAC
Разрешите прямое соединение, если PAC недоступен	Разрешите прямое соединение (без VPN), если PAC недоступен
Позволяет обходить прокси-сервер для доступа к сетям захвата	Позволяет обходить прокси для доступа к внутренним сетям.

AirPrint

IP-адрес	IP-адрес принтера
Путь к ресурсам	Определенный путь к устройству AirPrint

AirPlay

Имя устройства	Имя устройства
Пароль	Пароль сопряжения
Белый список	Определите список устройств, с которыми устройство может сопрягаться исключительно

Управление PIM

Exchange Active Sync

Название счета	Имя учетной записи электронной почты
Exchange ActiveSync Host	Адрес/FQDN сервера
Разрешить перемещение	Позволяет перемещать электронные письма
Используйте только в почте	Взаимодействие может происходить только в родном приложении Mail App
Используйте SSL	Используйте SSL-шифрование
Домен	Домен сервера
Пользователь	Имя пользователя
Адрес электронной почты	адрес электронной почты (только на уровне устройства)
Пароль (только на уровне устройства)	Пароль пользователя
Сертификат личности	Выберите соответствующий сертификат для аутентификации на сервере
Прошлые дни Mail to Sync	Количество дней, в течение которых электронная почта должна быть синхронизирована обратно. Без ограничений = неограниченно
Включить S/MIME	Включите шифрование S/MIME
Сертификат подписи	Загрузите соответствующий сертификат подписи
Сертификат шифрования	Загрузите соответствующий сертификат шифрования

eMail

Настройка учетных записей POP3 / IMAP на устройстве конечного пользователя

Описание счета	Учетные записи электронной почты		
Тип счета	IMAP	Префикс пути	Префикс пути для специальных папок
	POP		
Отображаемое имя пользователя	Отображаемое имя пользователя		
Адрес электронной почты	Адрес электронной почты пользователя		
Разрешить перемещение	Позволяет перемещать электронные письма		
Включить S/MIME	Включите шифрование S/MIME		
Сертификат подписи	Загрузите соответствующий сертификат подписи		
Сертификат шифрования	Загрузите соответствующий сертификат шифрования		

Входящая почта

Настройки сервера входящих сообщений

Адрес почтового сервера	Адрес почтового сервера
Порт почтового сервера	Порт почтового сервера
Имя пользователя	Соответствующее имя пользователя
Тип аутентификации	Тип аутентификации
Нет	Нет Тип аутентификации
Пароль (только на уровне устройства)	Запрос пароля
MDM Challenge-Response	
NTLM	NTLM-аутентификация
HTTP MD5 Digest	
Используйте SSL	Используйте SSL, если необходимо

Исходящая почта

Настройки исходящего сервера

Адрес почтового сервера	Адрес почтового сервера
Порт почтового сервера	Порт почтового сервера
Имя пользователя	Соответствующее имя пользователя
Тип аутентификации	
Нет	Нет метода аутентификации
Пароль (только на уровне устройства)	Запрос пароля
MDM Challenge-Response	
NTLM	NTLM-аутентификация
HTTP MD5 Digest	
Используйте SSL	Используйте SSL, если необходимо
Исходящий пароль такой же, как и входящий	Исходящий пароль такой же, как и входящий
Используйте только в почтовых отправлениях	Активировать, если все исходящие сообщения электронной почты должны отправляться через Mail-App

CalDav

Настройка и распределение учетной записи CalDav

Описание счета	Отображаемое имя учетной записи
Имя хоста	Имя хоста и/или IP-адрес
Порт	Порт учетной записи CalDav
Основной URL	Основной URL-адрес счета
Имя пользователя	Соответствующее имя пользователя CalDav
Пароль (только на уровне устройства)	Соответствующий пароль CalDav
Используйте SSL	Используйте SSL, если необходимо

Календари с подпиской

Настройка и распределение календарей с подпиской

Описание	Отображаемое имя учетной записи
URL	URL базы данных календаря
Имя пользователя	Имя пользователя подписки на календарь
Пароль (только на уровне устройства)	Пароль подписки на календарь
Используйте SSL	Используйте SSL, если необходимо

LDAP

В этой области настройте LDAP-соединение, чтобы обеспечить динамический обмен сертификатами между устройством конечного пользователя и Active Directory.

Обратите внимание, что выбранному пользователю требуется соответствующее разрешение на чтение.

Описание счета	Описание счета
Имя пользователя аккаунта	Пользователь для LDAP-доступа
Пароль учетной записи	Пароль для LDAP-доступа
Имя хоста учетной записи	Имя хоста/IP-адрес сервера LDAP
Используйте SSL	Используйте SSL, если необходимо

Во второй части Вы можете определить индивидуальные фильтры для поиска в реестре LDAP.

Описание	Область применения	База поиска
Описание фильтра	Уровень поиска в реестре LDAP	Определите индивидуальный фильтр

Веб-менеджмент

Webclips

В этом месте определите закладки со ссылками на веб-страницы, интранет-порталы и т.д., которые будут видны как приложение на устройстве конечного пользователя.

Этикетка	Имя соединения на устройстве конечного пользователя
URL	Ссылка на соответствующий веб-сайт
Съемный	Если он активирован, пользователь может удалить веб-клипсу
Иконка	В этом диалоге загрузите логотип для соединения: Размеры 180x180, формат png
Предварительно составленный значок	Если эта функция активирована, на иконке не будет отображаться никаких дополнительных эффектов (тень, отражение).
Полный экран	При открытии веб-клипов браузер открывается в полноэкранном режиме

Фильтр веб-контента

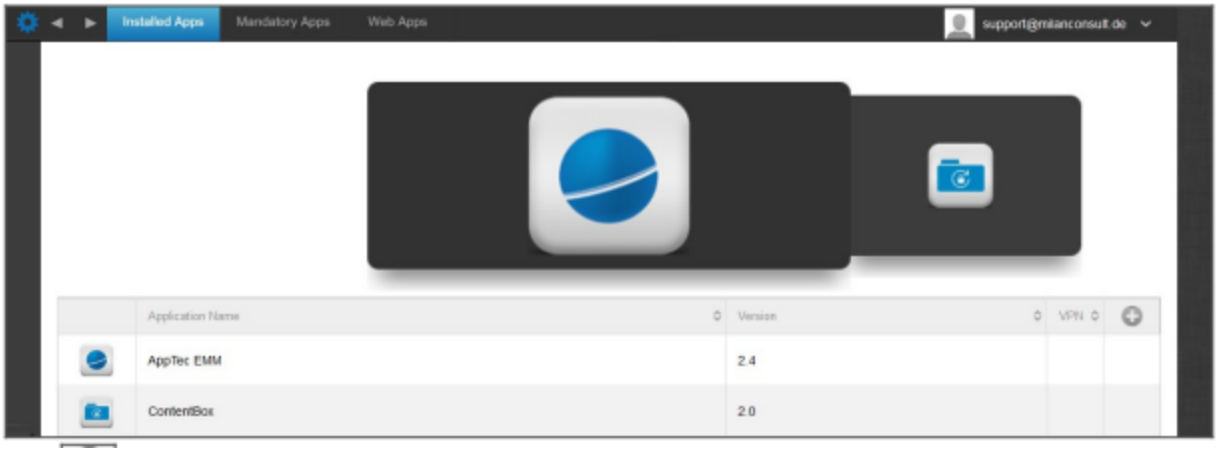
Фильтр веб-содержимого позволяет ограничить доступ к определенным интернет-страницам.

Разрешенные веб-сайты	
Ограничьте содержание для взрослых	Веб-фильтр автоматически применяется к контенту для взрослых
Разрешенные URL-адреса	С помощью символа + добавьте разрешенные страницы
URL-адреса, занесенные в черный список	С помощью символа + добавьте заблокированные страницы
Только конкретные веб-сайты	Можно отображать только определенный контент, который Вы можете добавить с помощью символа +.

Управление приложениями

Enterprise App Manager

Установленные приложения (только на уровне устройства)



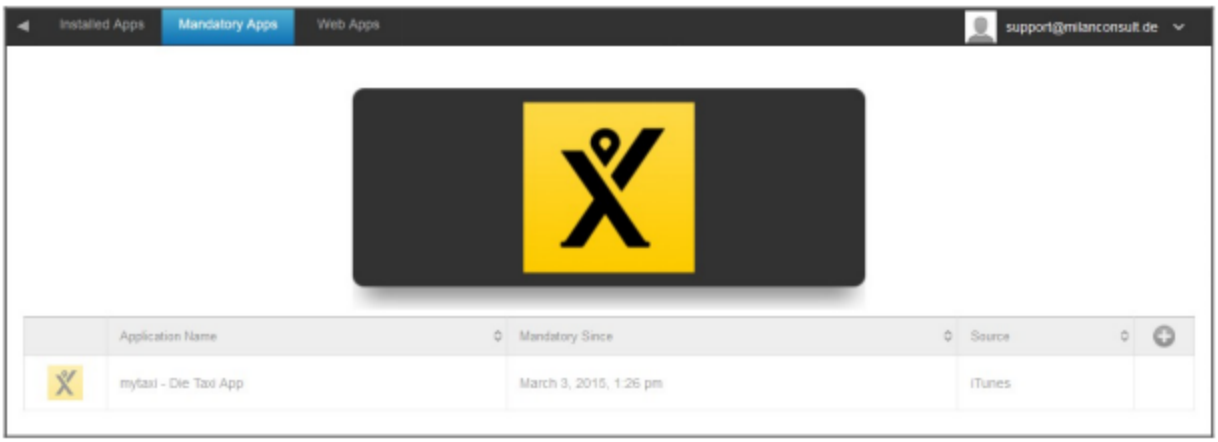
Здесь Вы можете увидеть приложения, которые в настоящее время установлены на устройстве.

Обязательные приложения

В разделе Обязательные приложения Вы можете установить необходимые приложения.

Пользователю постоянно будет напоминаться о необходимости установить это приложение.

С помощью , можно определить обязательное приложение.



Это может быть не только приложение из Apple App Store, но и собственное приложение.

Если речь идет о контролируемом устройстве, то приложение будет установлено автоматически.

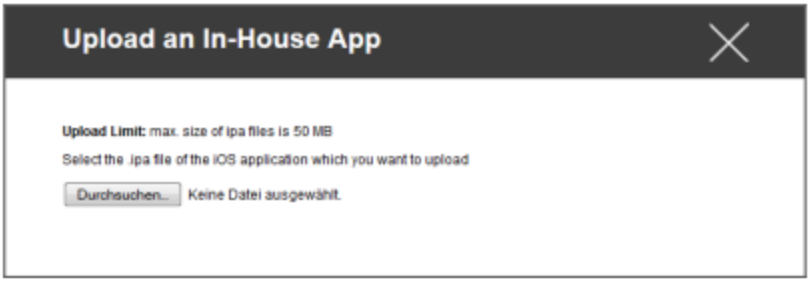
Вы можете установить на устройство приложение "Apple AppStore" из публичного AppStore, а также внутреннее приложение, разработанное собственными силами.

Или Вы можете выбрать категорию "Внутренние приложения iOS" и выбрать внутреннее приложение, которое Вы загрузили в разделе "Общие настройки".

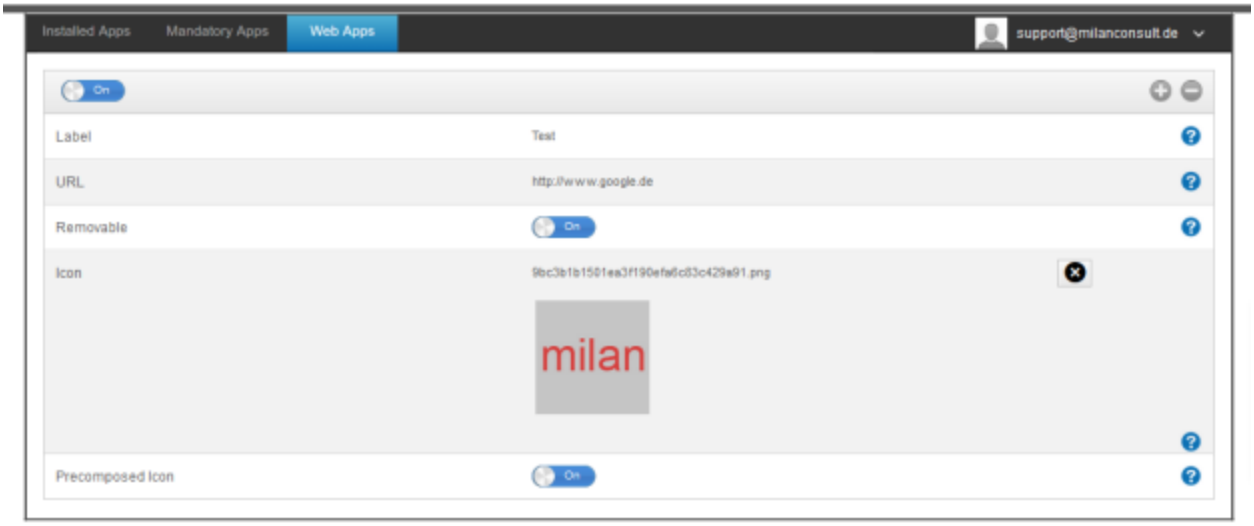
Опции установки

Постоянно обновляйте информацию (поддерживается только для VPP на устройство)	Раз в неделю будет определяться, есть ли обновление для приложения. Если да, то это обновление будет установлено Для приложений In-House Apps в процессе обновления будет использоваться цель обновления, которую Вы настроили в Общих настройках.
Обгоните, если не управлять	Если приложение уже установлено, MDM возьмет его на себя и будет управлять им
Удалите приложение при удалении профиля MDM	В случае удаления управления устройством приложение будет деинсталлировано
Предотвращение резервного копирования данных приложений	Резервная копия данных, относящихся к конкретному приложению, не будет создана
Настройка приложения	В разделе "Настройки приложения" Вы можете назначить приложению определенные значения на переднем плане (если приложение поддерживает это, при необходимости обратитесь к разработчику приложения).

Вы также можете напрямую выбрать и загрузить ipa-файл, воспользовавшись командой "Upload In-House App".



Веб-приложения



В пункте "Web Apps" Вы можете, как и в случае с "Web Clips", вывести интернет-страницы или интранет-порталы в виде приложения на конечное пользовательское устройство в области Web Management. По умолчанию Web Apps будут отображаться в полноэкранном режиме, который можно настроить в разделе "Webclips".

Этикетка	Имя соединения на устройстве конечного пользователя
URL	Ссылка на соответствующий веб-сайт
Съемный	Если он активирован, пользователь может удалить Webclip
Иконка	В этом диалоге загрузите логотип для соединения: Размеры 180x180, формат png
Предварительно составленный значок	Если эта функция активирована, на иконке не будет отображаться никаких дополнительных эффектов (тень, отражение).

Ограничения и настройки

Приложения в черном списке / в белом списке

Здесь Вы можете задать приложения, которые будут заблокированы (или разрешены) в зависимости от Ваших настроек в "Общих настройках". При нажатии откроется поиск известных приложений. Там Вы можете найти приложения, которые хотите добавить.

Обратите внимание, что для этой функции необходимо контролируемое устройство

Ограничения SysApp

Блокируйте определенные приложения или функции Вашего устройства

Разрешите использовать YouTube	Разрешите использовать YouTube
Разрешите использовать iTunes Store	Разрешите использовать iTunes Store
Разрешите использовать Safari	Разрешите использовать Safari
Включить автозаполнение	Позволяет автозаполнение
Предупреждение о принудительном мошенничестве	Принудительное предупреждение о мошенничестве
Включить JavScript	Позволяет использовать JavaScript
Блокируйте всплывающие окна	Блокирует все виды пупсов
Разрешить Cookies	Выберите, когда Safari будет принимать файлы cookie

App-VPN

С помощью этого символа Вы можете определить приложения, которые будут автоматически запускать выбранное VPN-соединение при запуске.

Настройки приложения

В разделе "Настройки приложения" Вы можете назначить приложению определенные значения на переднем плане (если приложение поддерживает это, при необходимости обратитесь к разработчику приложения).

С помощью этого символа Вы добавляете (дополнительное) приложение. Вы снова увидите знакомое по AppTec360 представление App-Import.

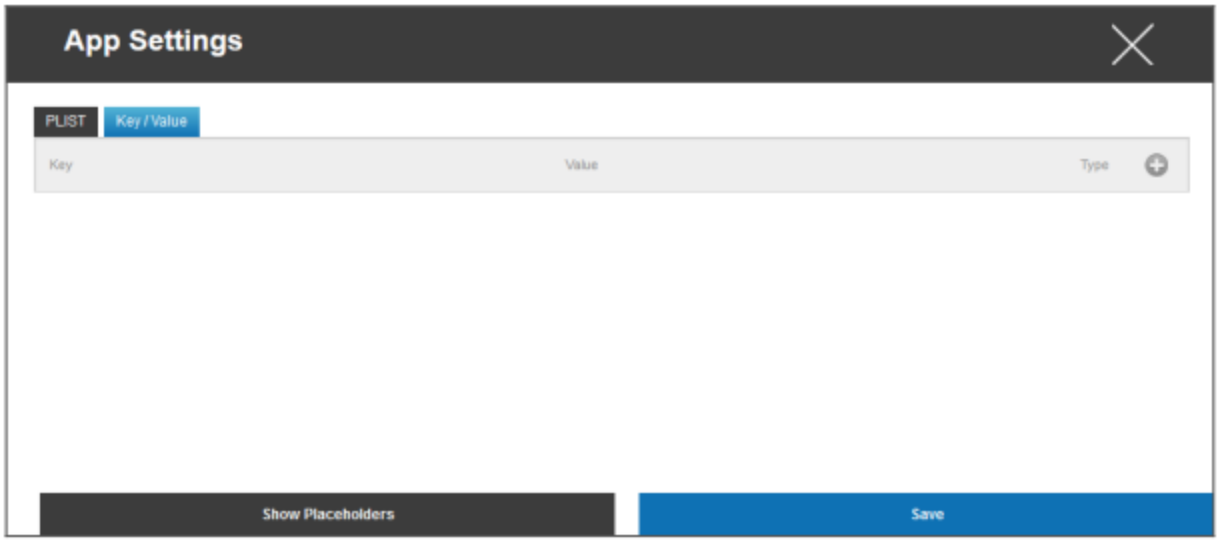
Найдите здесь приложение, которое Вы хотите настроить, и выберите его. Настройки будут применяться только к управляемым приложениям.

Если импорт прошел успешно, Вы увидите следующее окно:

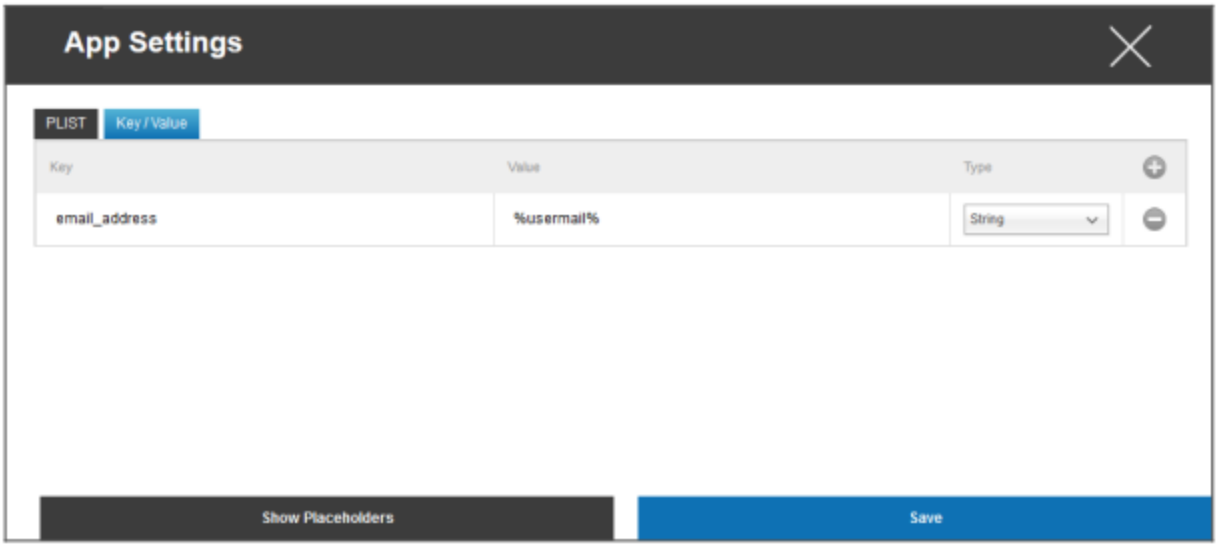
Теперь, нажав на кнопку , Вы можете выполнить различные конфигурации. Затем Вы получите следующий обзор:

Если у Вас уже есть PLIST (исходный текст конфигурации), Вы можете добавить его сюда и сохранить все это с помощью кнопки "Save".

В разделе "Ключ / Значение" Вы можете прикрепить определенные конфигурации к приложению



Здесь Вы можете установить новый ключ и его значение с помощью символа.



Конечно же, в Вашем распоряжении все возможности AppTec

Объяснение "Тип":

Строка	Текст
Булево	Правда/Ложь
Номер	Номер

С помощью этого символа Вы можете снова удалить приложение.

Магазин приложений для предприятий

Приложения iTunes

В этом пункте Вы можете распространять дополнительные Приложения для Вашего Пользователя.

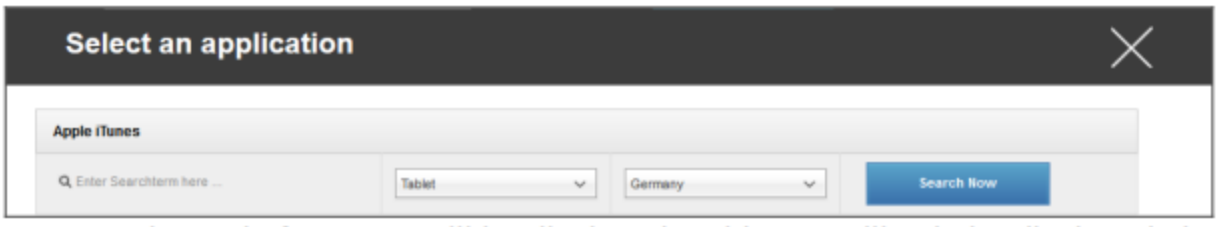
Если здесь есть приложение, оно будет автоматически установлено на устройство конечного пользователя AppTec360 Store.

Это просто ссылки на официальный магазин приложений Apple App Store. По этой причине каждое устройство конечного пользователя должно быть оснащено Apple ID.

На данном этапе мы рекомендуем каждому пользователю иметь свой собственный Apple ID.

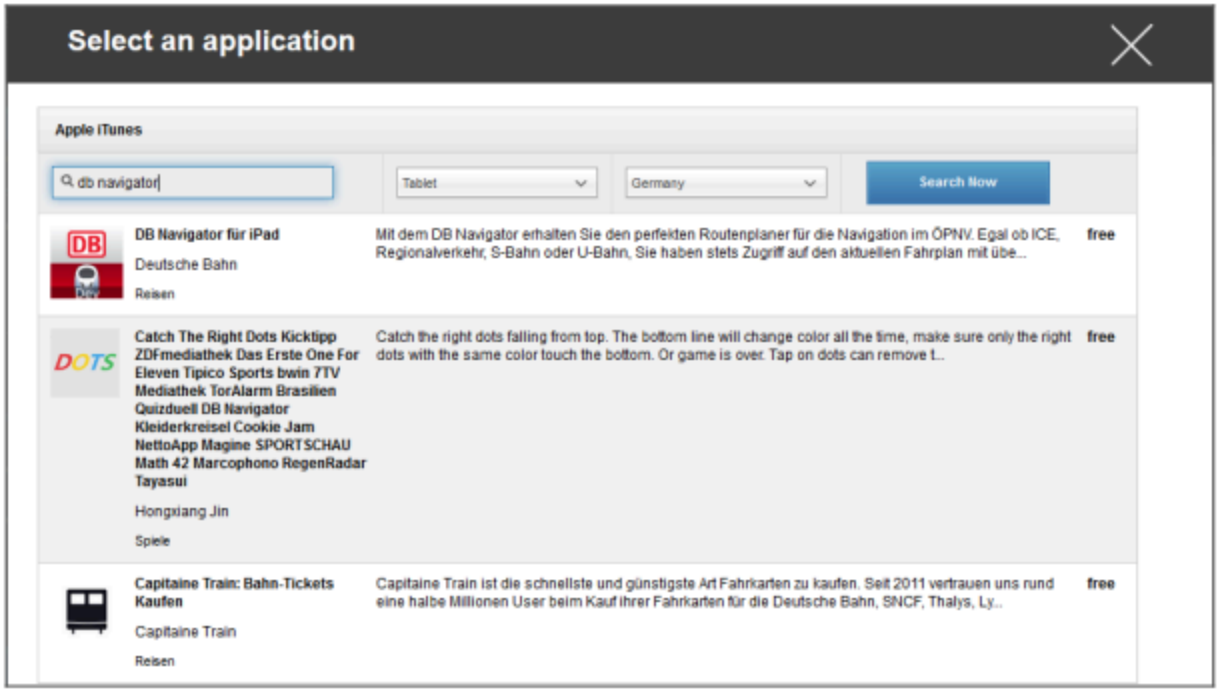
С помощью символа Вы можете добавить дополнительные Приложения.

После этого должно открыться окно со следующим обзором.



Обратите внимание, что будут отображаться только бесплатные приложения, платные приложения будут отображаться только через VPN.

В разделе "Введите поисковый запрос здесь ..." Вы можете найти приложение, которое находится в Apple App Store.



Как только Вы нажмете на значок или на название приложения, Вам снова будет предложено выполнить дополнительные настройки.

Будьте в курсе событий	Раз в неделю будет определяться, есть ли обновление для приложения. Если да, то это обновление будет установлено
Удалите приложение при удалении профиля MDM	В случае удаления управления устройством приложение будет деинсталлировано
Предотвращение резервного копирования данных приложений	Резервная копия данных, относящихся к конкретному приложению, не будет создана

App-VPN	Выберите VPN-соединение, которое будет запущено при открытии приложения

После нажатия на кнопку "Установить" приложение будет добавлено в Enterprise App Store и затем может быть установлено на устройство конечного пользователя через AppTec360 AppStore.

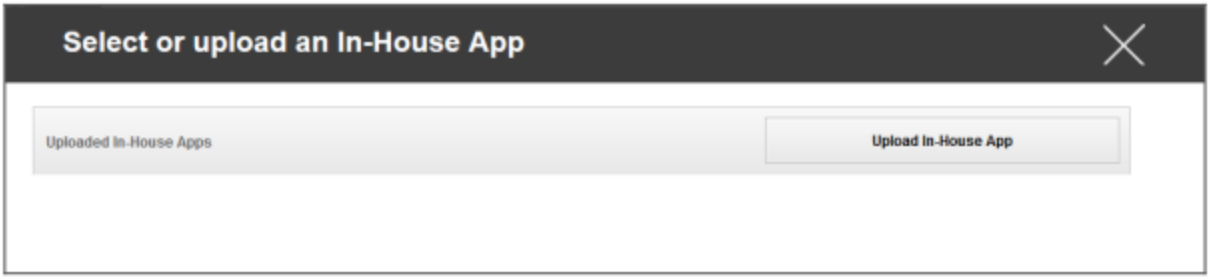
Если импорт в App-Store прошел успешно, Вы получите следующий обзор:

In-House

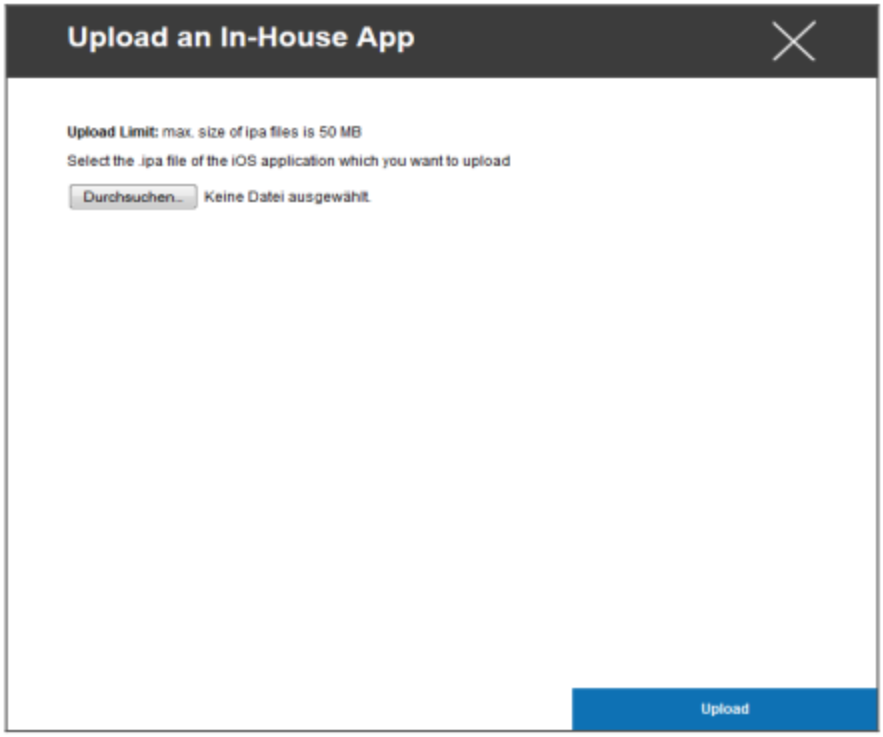
В пункте "In-House" Вы можете загружать приложения, разработанные внутри компании, и распространять их.

С помощью символа Вы можете распространять дополнительные приложения In-House Apps.

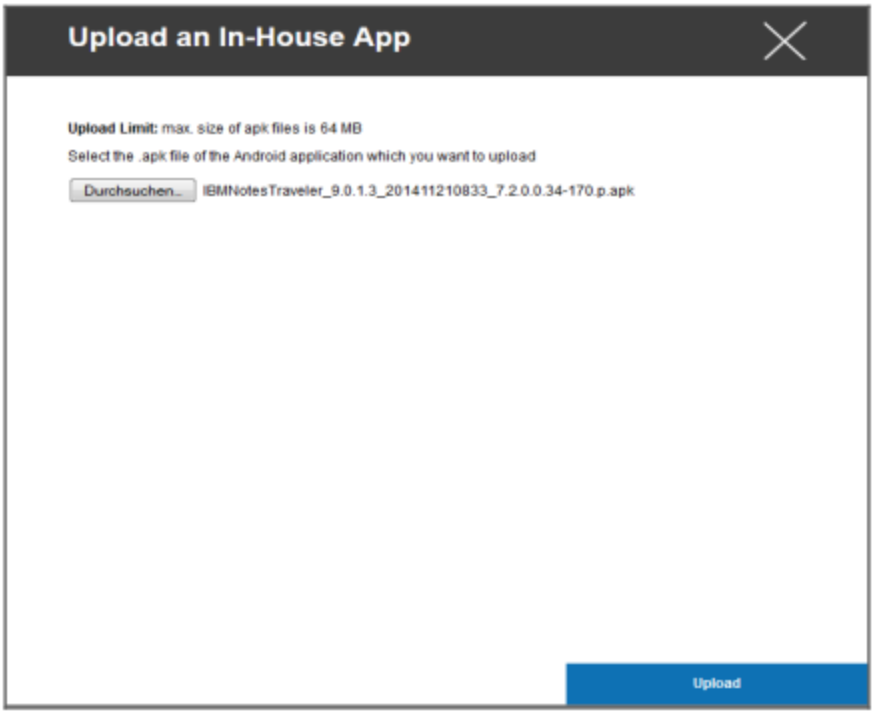
Если Вы никогда не занимались распространением In-House App, Вы получите следующий обзор:



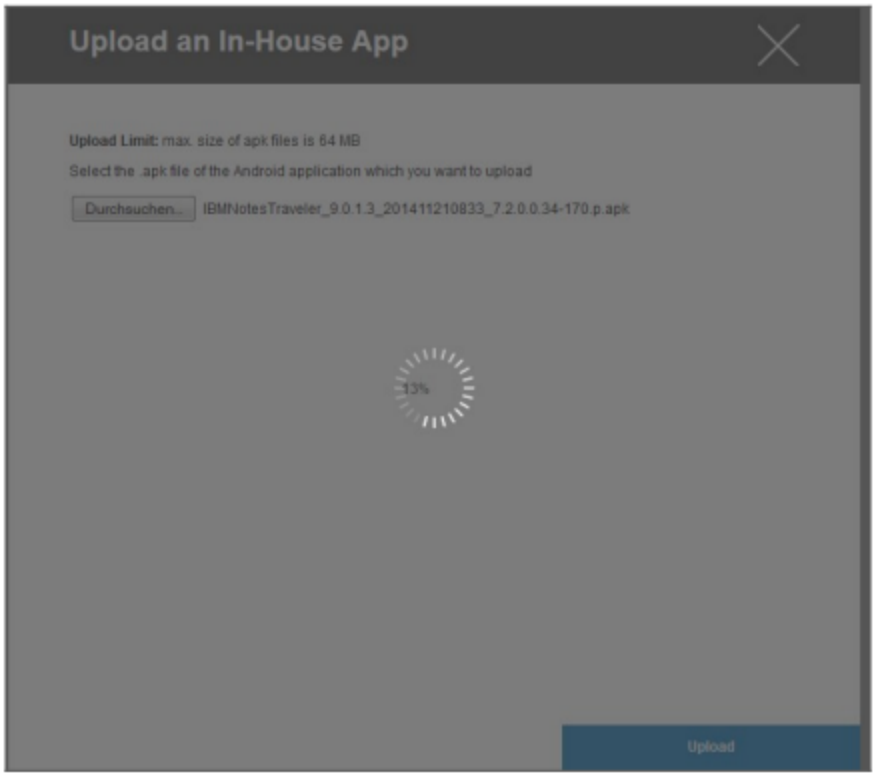
Для этого нажмите "Upload In-House App", после чего Вы получите следующий обзор:



Теперь выберите с помощью "Search... "файл .ipa и нажмите "Upload".



Теперь Ваше приложение будет загружено. В центре круга Вы можете увидеть процентное соотношение того, сколько частей Вашего приложения уже загружено.



Если загрузка приложения In-House App прошла успешно, Вы увидите новое загруженное приложение в Вашем каталоге приложений.

Теперь у пользователя есть возможность увидеть и установить это приложение в AppTec360 Store на устройстве конечного пользователя, в категории "In-House".

Поскольку в этом случае не используется общедоступное приложение Apple AppStore, пользователю не нужен сохраненный Apple ID на конечном устройстве пользователя.

Режим киоска

Режим киоска для iOS доступен только в режиме под наблюдением

Режим киоска позволяет Вам предварительно определить приложение или URL, чтобы можно было запускать/посещать только это приложение/URL.

Кроме того, Вы можете отключить различные аппаратные кнопки в режиме киоска.

Тип применения

Пакет

Если Вы хотите запустить приложение в режиме киоска, выберите "Пакет" в разделе "Тип приложения".

Применение киосков	Нажмите здесь, чтобы выбрать приложение, которое должно запускаться в режиме киоска Вы найдете текущий обзор App Management Вы можете выбрать между "Apple iTunes Apps" и "iOS In-House Apps".

URL

Если Вы хотите запустить URL в режиме киоска, выберите "URL" в разделе "Тип приложения".

URL	Теперь определите нужный адрес URL
Политика одинакового происхождения	Если эта функция активна, пользователь сможет просматривать только подстраницы заданного URL. Например, если Вы определили следующий URL: www.mypage.com, то пользователь может перейти на www.mypage.com/subpage.
URL-адреса, внесенные в белый список	Здесь Вы можете создать белый список, в котором все эти URL будут разрешены Не более 1 URL в строке URL должен начинаться с http:/ или https://.
URL-адреса, занесенные в черный список	Здесь Вы можете вести Черный список, в котором все эти URL будут запрещены. Не более 1 URL в строке URL должен начинаться с http:/ или https://.
Очистка браузера после бездействия	После бездействия кэш браузера будет очищен.
Пароль выхода Включен	Если Вы активируете эту функцию, у пользователя будет возможность завершить режим киоска с помощью пароля, который был предварительно определен Вами
Пароль выхода	Это пароль, который был предварительно определен Вами

Настройки режима киоска

Режим киоска по расписанию	В зависимости от времени суток Вы можете установить режим киоска, чтобы режим запускался и завершался автоматически в заранее установленное время
Время начала	Время начала
Время в минутах	Время в минутах, по истечении которого режим киоска должен быть снова завершен
Отключить сенсорное управление	Если активирован, сенсорный экран отключен
Отключить вращение устройства	Если активирована, автоматическая адаптация экрана отключается
Выключатель звонка	Если он активирован, переключатель звонка будет отключен. С этого момента поведение зависит от ранее установленной функции
Отключите кнопки регулировки громкости	Если активировать эту функцию, кнопки громкости будут отключены
Отключите кнопку пробуждения во время сна	При активации переключатель включения/выключения будет деактивирован
Отключить автоматическую блокировку	Если эта функция активирована, устройство не будет переводиться в режим ожидания
Включить передачу голоса	Если он активирован, будет включен голосовой помощник
Включить масштабирование	Если активировать, то будет активирован зум.
Включить инверсию цветов	Если он активирован, будет включен режим инвертированного дисплея
Включите функцию Assistive Touch	Если он активирован, AssistiveTouch будет активирован
Включить выбор речи	Если активирован, будет активирован выбор речи
Включить монофонический звук	Если он активирован, будет включено монофоническое звучание
VoiceOver	Если эта функция активирована, пользователь может включить VoiceOver

Zoom	Если эта функция активирована, пользователь может включить Zoom
Инвертировать цвета	Если эта функция активирована, пользователь может включить инвертированные цвета
Assistive Touch	Если эта функция активирована, пользователь может включить вспомогательные сенсорные функции

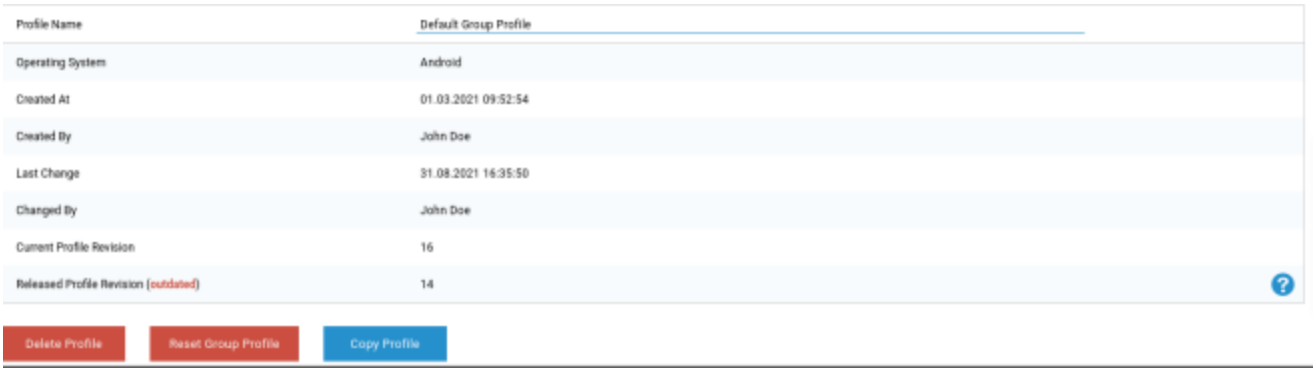
Android Enterprise — полностью управляемая конфигурация устройств

В зависимости от того, выбрали ли Вы в данный момент групповой профиль или устройство, обзор и его подпункты будут отличаться - пожалуйста, внимательно изучите это!

Общие сведения

Обзор профиля группы (только на уровне группы)

Открыв профиль группы, Вы получите краткий обзор профиля.



Имя профиля	Название профиля (может быть изменено здесь)
Операционная система	Операционная система, для которой предназначен профиль
Создано в	Время создания
Created By	Создатель профиля
Последнее изменение	Время последнего изменения профиля
Изменено	Учетная запись, которая внесла последние изменения

Текущий пересмотр профиля	Пересмотр сохраненного состояния профиля
Выпущенный пересмотр профиля	Назначенная ревизия профиля ("Назначить сейчас"). Если за текстом на ярлыке отображается "(устаревший)", это означает, что Вы сохранили профиль, но еще не назначили его, поэтому устройства все еще будут получать старую версию.

Обзор устройства (только на уровне устройства)

Если Вы находитесь на устройстве, Вы получите обзорную информацию о выбранном устройстве, в которой содержится следующее:

Имя устройства	Имя устройства
Расположение	Координаты местоположения
Номер телефона	Номер телефона
Назначение Обязательные приложения	Количество назначенных обязательных приложений
Версия ОС	Версия ОС устройства
Операционная система	Операционная система (Android Enterprise)
Серийный номер	Серийный номер устройства
Владение устройством	Корпоративное или личное устройство
Тип устройства	Управляемое устройство AE Work
Rooted	Статус, указывающий, было ли устройство рутировано
Соответствующий	Соответствие рекомендациям
IP-адрес	IP-адрес устройства
Последний раз видели	Точка во времени, когда устройство в последний раз подключалось к AppTec
Последний рывок	Точка во времени, когда последний толчок был отправлен на устройство
Режим владельца устройства AE	Да
Назначение пользователя	Пользователь или группа, которой назначено это устройство

Пересмотр конфигурации (только на уровне устройства)

Здесь Вы получите обзор того, какой групповой профиль назначен устройству.

Если Вы нажмете на профиль группы, Вы получите прямой доступ к этому профилю и сможете выполнить настройки.

С помощью этого символа Вы можете вернуть распределенные приложения к настройкам группового профиля.

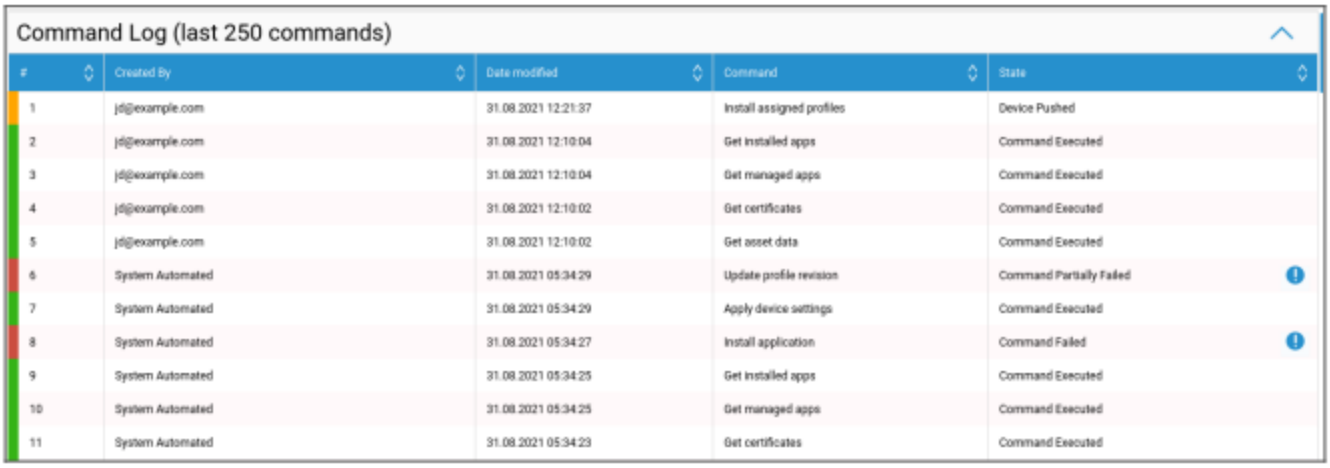
С помощью этого символа Вы можете вернуть все используемые приложения к настройкам группового профиля.

"Доступна более новая редакция" означает, что профиль группы был изменен и сохранен, но не назначен. Чтобы применить изменения к устройствам, групповой профиль должен быть назначен с помощью "Назначить сейчас" на уровне группы.

Журнал устройства (только на уровне устройства)

Журнал команд

Здесь Вы можете увидеть, какие команды были отданы устройству и каков их статус.



Команды, созданные с помощью "System Automated", автоматически создаются системой.

Возможные статусы команд

Устройство нажимается	Запрос push был отправлен в службу push (например, APNS), чтобы сообщить устройству о необходимости подключиться обратно к серверу EMM.
Команда Создана	Команда была создана в системе.
Команда отправлена	Команда была отправлена на устройство после того, как оно подключилось к серверу.
Команда выполнена	Команда была успешно выполнена.
Команда не выполнена	Команда завершилась неудачно. *
Команда частично не выполнена	В зависимости от ОС устройства некоторые команды могут быть сгруппированы вместе. В этом случае некоторые части этой группы команд оказались неудачными. *
Команда выполнена, в итоге - отказ	Команда была выполнена, но, возможно, она не была выполнена.
Command Repushed	Команда была повторно запущена пользователем.
Выброшенные	Команда была отменена. Например, потому что она была заменена другой командой или устройство было перерегистрировано, и старые команды были удалены.

Если за сообщением стоит восклицательный знак, Вы можете получить дополнительную информацию, наведя курсор на значок.

Настройки устройства

Конфигурация клиента

Здесь Вы можете выполнить следующие настройки Вашего устройства Android:

Время несоблюдения	Предельное время ожидания ответа пользователя, после которого применяется принудительное действие.
Принудительные действия после истечения времени выполнения	Принудительные действия, когда пользователь не выполняет действия, которые приводят к состоянию устройства, соответствующему требованиям
Частота сбора данных	Частота сбора информации об устройстве/GPS
Частота сердцебиения устройства	Интервал, через который устройство должно связаться с сервером AppTec360 Server Мин. 1 минута Макс. 24 часа
Включите обновление местоположения	Если активирована, устройство отправляет обновления местоположения на сервер AppTec360 Server
Расположение Время обновления	Определяет, через какие временные интервалы устройство отправляет обновления местоположения в AppTec360
Используйте точность определения местоположения Google для обновления местоположения	Если эта настройка активирована, то для обновления местоположения будет использоваться сетевое местоположение (если эта настройка была отключена в разделе "Ограничения", то она ни на что не повлияет)
Используйте GPS для обновления местоположения	Если активировано, GPS будет использоваться для обновления местоположения
Разрешить имитацию (подделку) местоположения	Позволяет подделывать информацию о местоположении с помощью сторонних приложений
Действие при потере соединения	Если эта опция включена, Вы можете указать действие для случая, когда устройство не получает соединения с MDM-сервером в интервале сердцебиения. Например, если устройство имеет интервал сердцебиения 5 минут, оно подключится к серверу в 10:35 утра. После этого устройство выходит из зоны действия Wi-

	Fi. Следующее сердцебиение в 10:40 утра будет неудачным, и указанное действие будет выполнено.
Действие	Действия, которые необходимо предпринять, как только устройство становится несоответствующим требованиям. • Устройство блокировки = устройство блокировки • Wipe Device = устройство будет восстановлено до заводских настроек • Wipe Device & SD Card = устройство будет восстановлено до заводских настроек, а память SD Card будет удалена.
Порог	Вы можете указать пороговое количество неудачных сердцебиений, которое необходимо для запуска указанного действия.

Режим внедрения политики	По умолчанию:	Пользователям будет периодически предлагаться выполнить невыполненные действия
	Ленивое внедрение политики:	Пользователям никогда не будет предложено выполнить незавершенные действия. Все открытые действия будут отображаться в AppTec360 Client
	Агрессивное применение политики:	Пользователям будет постоянно предлагаться выполнить невыполненные действия
AppTec360 Блокировка версий	Если эта опция включена, можно указать код версии для AppTec360 MDM Client. Клиент AppTec360 будет обновляться только до указанной версии. Более новые версии будут игнорироваться. Понижение версии НЕ возможно.	
Код версии	Код версии клиента AppTec360 MDM Client, к которому необходимо подключиться.	
Отключение уведомлений AppTec360	Если отключить эту функцию, клиент AppTec360 не будет показывать уведомление на панели уведомлений. Таким образом, пользователи могут закрыть клиент AppTec360 через диспетчер задач. Если клиент AppTec360 закрыт, некоторые функции, включая режим киоска и черный/белый список приложений, не будут работать должным образом. Устройства Samsung предлагают механизм защиты для AppTec360 Client. Уведомление отключено по умолчанию на устройствах Samsung, поддерживающих API KNOX. Уведомление не должно отключаться на устройствах с Android 8.0 и выше.	

Обои

Установите пользовательские обои	Включение/выключение пользовательских обоев
Обои	Установите режим обоев, чтобы использовать цветовой код или изображение
Укажите цвет	Укажите цвет заднего плана в виде шестнадцатеричного значения, например, #000000 для черного или #ffffff для белого.
Установите изображение в качестве обоев	Загрузите файл с изображением, которое Вы хотите использовать в качестве обоев.

Управление активами (только на уровне устройств)

Информация об устройстве

Модель	Обозначение модели устройства
Операционная система	OS
Версия ОС	Версия ОС
Серийный номер	Серийный номер
Имя устройства	Имя устройства
Состояние батареи	Состояние батареи
Свободная / общая память	Свободная / общая память
Samsung Safe	Интерфейс Samsung SAFE, необходимый для различных настроек
Доступна карта памяти SD	Доступна карта SD
Эмулированная SD-карта	Эмулированная SD-карта
Съемная SD-карта	Съемная SD-карта
Свободная / общая память SD	Свободная память SD / Общая память SD-карты

Wi-Fi

IP-адрес	IP-адрес устройства
WiFi MAC	MAC-адрес WiFi

Клетчатка

Статус	Состояние (SIM-карта установлена)
Номер телефона	Номер телефона
Роуминг (голос / данные)	Роуминг для голоса / данных
Статус роуминга	Текущий статус роуминга
IP-адрес	IP-адрес
Оператор/ перевозчик	Оператор/перевозчик
Клеточные технологии	Клеточные технологии
IMEI	Номер IMEI
ICCID	Это идентификатор SIM-карты, часто также называемой Smartcard или Integrated Circuit Card (ICC).
IMSI	Международный идентификатор мобильного абонента (IMSI) обеспечивает в GSM- и UMTS-мобильных сетях однозначную идентификацию пользователей сети. IMSI состоит максимум из 15 цифр и настраивается следующим образом: • Код страны мобильного телефона (MCC), 3 цифры • Код мобильной сети (MNC), 2 или 3 цифры • Идентификационный номер мобильного абонента (MSIN), 1-10 цифр
Текущий MCC/MNC	См. раздел "SIM MCC/MNC".
SIM MCC/MNC	Код страны мобильной связи - это установленный идентификатор страны, установленный МСЭ в соответствии со стандартом E.212. Он работает в сочетании с кодом мобильной сети (MNC) для идентификации мобильной сети. Означает код страны/мобильной сети SIM-карты. Если Вы переходите в другую мобильную сеть, то, по логике вещей, "Current MCC/MNC" и "SIM MCC/MNC" будут разными.

Bluetooth

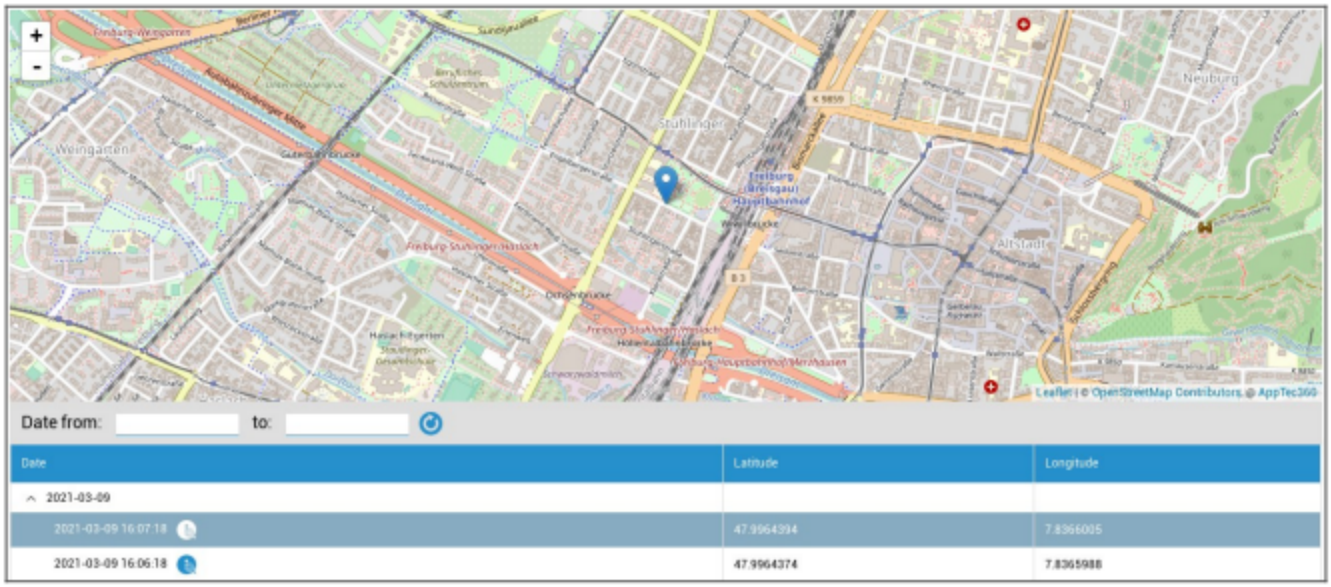
Bluetooth MAC	MAC-адрес Bluetooth

Управление безопасностью

Защита от кражи (только на уровне устройства)

Информация GPS (только на уровне устройства)

Здесь Вы можете установить текущее/последнее местоположение устройства. Локализация может быть защищена одним или даже двумя паролями - См: Общие настройки - Конфиденциальность - Доступ к GPS



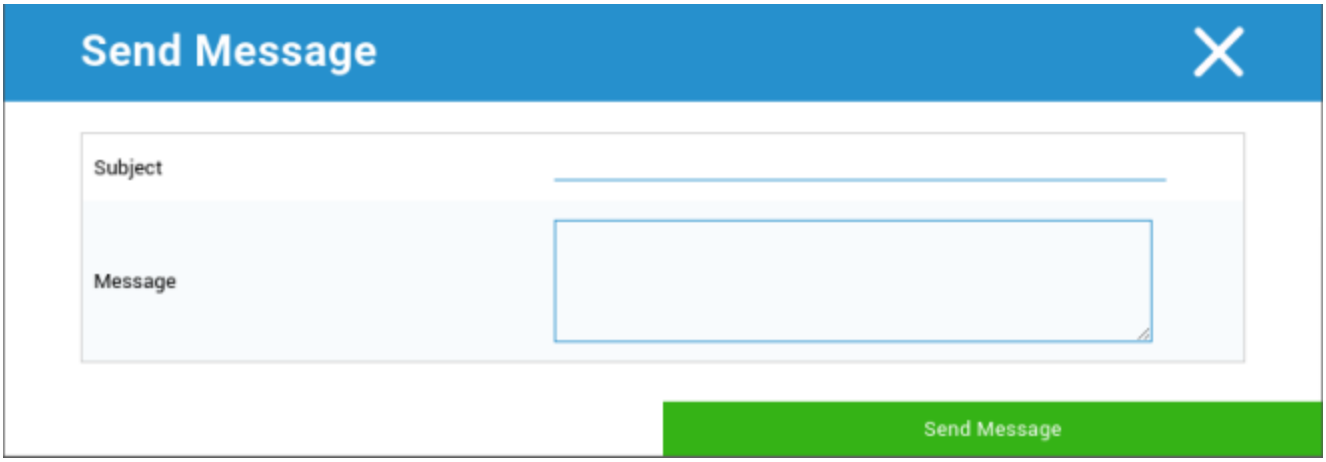
Wipe & Lock (только на уровне устройства)

В разделе "Wipe & Lock" Вы можете выполнить следующие три действия:

Полное вытирание	Устройство возвращается к заводским настройкам (корпоративные, а также личные данные удаляются)
Enterprise Wipe	С устройства конечного пользователя удаляются только корпоративные данные (все приложения, данные и т.д., которые были предоставлены AppTec360).
Экран блокировки	Активирована блокировка экрана, достаточно разблокировать устройство с помощью пароля устройства/PIN-кода

Сообщение (только на уровне устройства)

Здесь Вы можете заполнить тему и сообщение и отправить его на устройство конечного пользователя.



Конфигурация безопасности

Пасскод устройства

В разделе "Пароль" Вы можете задать пароль устройства, Вам доступны следующие опции настройки

Минимальная длина пароля	Устанавливает минимальное количество символов, которое должно быть в пароле	
Качество пароля	Неопределенный	В этой политике нет требований к паролю.
	Биометрическая слабость	Эта политика позволяет использовать технологии биометрического распознавания с низким уровнем безопасности. Под этим подразумеваются технологии, способные распознать личность человека примерно до 3-значного PIN-кода (ложное обнаружение составляет менее 1 из 1 000).
	Кое-что	Эта политика требует установки какого-либо пароля или шаблона, но не устанавливает никаких конкретных правил.
	Алфавитный	Пользователь должен ввести пароль, содержащий как минимум алфавитные (или другие символы) символы.
	Буквенно-цифровой	Пользователь должен ввести пароль, содержащий как минимум оба цифровых и буквенных (или других символа) символа.
	Комплекс	По умолчанию пользователь должен ввести пароль, содержащий как минимум букву, цифру и специальный символ. С помощью этого качества пароли можно ограничить, чтобы они содержали различные наборы символов, например, хотя бы заглавную букву и т.д.
Минимальная длина пароля	Установите необходимое количество символов для пароля. Например, Вы можете потребовать, чтобы PIN-код или пароль состояли как минимум из шести символов.	
Минимальное количество цифр в пароле	Минимальное количество цифр в пароле	

Минимальное количество строчных букв в пароле	Минимальное количество строчных букв в пароле
Минимальное количество заглавных букв в пароле	Минимальное количество заглавных букв в пароле
Минимальное количество небуквенных символов, необходимых для пароля	Минимальное количество небуквенных символов, необходимых для пароля
Минимальное количество символов в пароле	Минимальное количество символов в пароле

Максимальная блокировка времени бездействия	Максимальное время бездействия пользователя до временной блокировки
Таймаут истечения срока действия пароля	Устанавливает, через какой промежуток времени срок действия пароля истекает, и необходимо выдать новый пароль
Ограничение истории паролей	Количество ранее использованных паролей, которые не разрешены
Максимальное количество неудачных попыток ввода пароля	Устанавливает, как часто пароль может быть введен неверно, прежде чем будет произведено полное стирание устройства
Разрешить биометрическую аутентификацию	Обеспечивает аутентификацию с помощью отпечатка пальца или сканирования радужной оболочки глаза. Только для Samsung KNOX 2.1 и выше

Антивирус

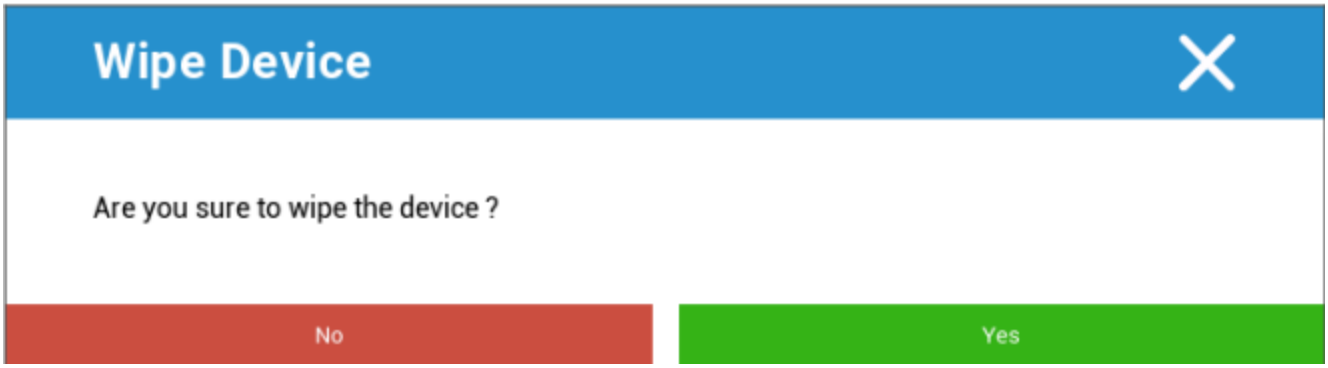
Автоматическое сканирование	Включите периодическое автоматическое сканирование
Интервал сканирования	Интервал для обследования (Быстрое / Полное)
Полное автоматическое сканирование	Включите полное автоматическое сканирование
Автоматические обновления	Включите автоматические обновления
Интервал проверки обновлений	Как часто следует обновлять приложение и его базу данных (вирусы / поврежденный код)
Защита приложений	Включите автоматическое сканирование приложений
Защита SD-карты	Включите автоматическое сканирование SD-карты
Обновление только через Wi-Fi	Если эта функция включена, обновления будут применяться только при успешном подключении устройства к сети Wi-Fi.

Окончание срока службы (только на уровне устройства)

Стирание (только на уровне устройства)

В разделе "Wipe" Вы можете восстановить заводские настройки устройства. При этом корпоративные, а также личные данные будут удалены с устройства конечного пользователя.

При нажатии на "Символ минуса" Вы получите следующее сообщение:



Ответив "Да", Вы можете выполнить стирание.

В разделе "Отчет о стирании" отображаются следующие пункты

Стерто	История о том, кто выполнял протирание
Дата	Дата
Статус	Статус (например, успешно ли выполнено стирание)

Настройки ограничений

Ограничения

Здесь можно ограничить и заблокировать множество вещей.

Включить камеру	Разрешите использовать фотоаппарат	
Принудительная автоматическая синхронизация	На сайте	Синхронизация постоянно активирована
	С сайта	Синхронизация отключена навсегда
	Выбор пользователя	Выбирается пользователем
Force Bluetooth	На сайте	Bluetooth постоянно активирован
	С сайта	Bluetooth отключен навсегда
	Выбор пользователя	Выбирается пользователем
Force GPS	На сайте	GPS постоянно активирован
	С сайта	GPS постоянно отключен
	Выбор пользователя	Выбирается пользователем
Расположение сети сил	На сайте	Постоянная интернет-локализация
	С сайта	Постоянная деактивация интернет-локализации
	Выбор пользователя	Выбирается пользователем

Безопасность		
Запретить совместное использование местоположения	Указывает, запрещено ли пользователю включать совместное использование местоположения.	
Запретить безопасную загрузку	Указывает, запрещено ли пользователю перезагружать устройство в безопасный режим загрузки.	
Запретить сетевой сброс	Указывает, запрещено ли пользователю сбрасывать сетевые настройки из Настроек.	
Запретить сброс к заводским настройкам	Указывает, запрещено ли пользователю сбрасывать устройство.	
Включите ADB	Позволяет подключаться к ПК через ADB	
Отключите охрану ключей	Отключает охрану ключей	
Информация о владельце устройства на запорном экране	Устанавливает информацию о владельце устройства, которая будет отображаться на экране блокировки.	
Обеспечение соответствия	Режим Подсказка Пользователю	Пользователю будет предложено выполнить необходимые действия.
	Режим блокировки контейнера	Скрывайте все приложения до тех пор, пока не будут выполнены все требования

Управление приложениями	
Разрешите межпрофильные ссылки на приложения	Позволяет приложениям в родительском профиле обрабатывать веб-ссылки из управляемого профиля.
Запретить управление приложениями	Определяет, запрещено ли пользователю изменять приложения в Настройках или пусковых установках.
Запретить установку приложений	Указывает, запрещено ли пользователю устанавливать приложения.
Запретить удаление приложений	Указывает, запрещено ли пользователю удалять приложения.
Политика разрешений во время выполнения	Определяет, как будут обрабатываться новые запросы на разрешение от приложений.
Разрешить неизвестные источники	Если эта функция включена, пользователи могут загружать приложения с боковой стороны, устанавливая файл .apk.

Возможность подключения	
Запретить настройку мобильной сети	Указывает, запрещено ли пользователю настраивать мобильные сети.
Настройка запрета привязки	Указывает, запрещено ли пользователю настраивать Tethering & portable hotspots.
Запретить настройку VPN	Указывает, запрещено ли пользователю настраивать VPN.
Запретить настройку Wifi	Указывает, запрещено ли пользователю менять точки доступа WiFi.
Запретить исходящий луч NFC	Указывает, запрещено ли пользователю использовать NFC для передачи данных из приложений.
Блокировка конфигурации WiFi	Этот параметр определяет, должны ли конфигурации WiFi, созданные приложением владельца устройства, быть заблокированы (то есть, редактироваться или удаляться только приложением владельца устройства, даже не приложением Settings).
Включить роуминг данных	Активирует роуминг данных

Bluetooth	
Запретить Bluetooth	Указывает, запрещен ли bluetooth на устройстве. Требуется Android 8.0
Запретите совместный доступ к Bluetooth	Указывает, запрещен ли на устройстве исходящий совместный доступ по bluetooth. Требуется Android 8.0
Запретить настройку Bluetooth	Указывает, запрещено ли пользователю настраивать bluetooth.

Управление счетами	
Запретите добавление управляемого профиля	Указывает, запрещено ли пользователю добавлять управляемые профили. Требуется Android 8.0
Запретить добавление пользователей	Указывает, запрещено ли пользователю добавлять новых пользователей.
Запретить удаление управляемого профиля	Указывает, могут ли управляемые профили этого пользователя быть удалены, кроме как владельцем профиля. Требуется Android 8.0
Запретить изменение учетной записи	Определяет, запрещено ли пользователю добавлять и удалять учетные записи, если они не были добавлены Authenticator программно.

Телефония	
Запрет исходящих вызовов	Указывает, что пользователю запрещено совершать исходящие телефонные звонки.
Запретить SMS	Указывает, что пользователю не разрешено отправлять или получать SMS-сообщения.

Система	
Запретить создание окон	Указывает, что окна, кроме окон приложений, не должны создаваться.
Запретить установку значка пользователя	Указывает, запрещено ли пользователю менять свой значок.
Запретить установку обоев	Ограничение пользователя, запрещающее устанавливать обои.
Отключите строку состояния	Отключение строки состояния блокирует уведомления, быстрые настройки и другие экранные накладки, которые позволяют уйти от одноразового использования устройства.
Включить автоматическое время	Установите время автоматически.
Включить автоматический часовой пояс	Установите часовой пояс автоматически.

Остается включенным в розетку	Устройство будет оставаться активным, пока подключено к источнику питания.

Хранение	
Запретите отключать проверку приложений	Указывает, запрещено ли пользователю отключать проверку приложений.
Запретить монтировать физические носители	Указывает, запрещено ли пользователю монтировать физические внешние носители.
Включите службу резервного копирования	Служба резервного копирования управляет всеми механизмами резервного копирования и восстановления на устройстве. Если установить значение false, резервное копирование или восстановление данных будет запрещено. По умолчанию служба резервного копирования отключена. Требуется Android 8.0
Включите USB-накопитель	Включает использование USB Mass Storage.

Клавиатура	
Запретить автозаполнение	Указывает, запрещено ли пользователю использовать службы автозаполнения. Требуется Android 8.0
Запретите копирование и вставку между профилями	Указывает, можно ли скопированное в буфер обмена этого профиля вставить в соседние профили.

Звук	
Запретить корректировку объема	Указывает, запрещено ли пользователю регулировать основную громкость.
Запретить отключение микрофона	Указывает, запрещено ли пользователю регулировать громкость микрофона.
Выключите устройство	Отключите звук.

Управление сертификатами

Здесь Вы можете распространять Доверенные сертификаты и Сертификаты идентичности среди Ваших устройств.

Для распространения Доверенных сертификатов требуется Android 8 или выше, а для распространения Идентификационных сертификатов - Android 9 или выше.

С помощью "+" Вы можете добавить несколько сертификатов.

Доверенные сертификаты должны быть в формате PEM.

Сертификаты личности должны быть в формате PKCS12

Управление соединениями

Wifi

Для этой настройки выполните предварительную конфигурацию устройств конечных пользователей для доступа к внутренним точкам доступа
.

Идентификатор набора услуг (SSID)	SSID для подключаемой сети
Скрытая сеть	Активировать, в случае если точка доступа не передает SSID

Тип безопасности

Установите тип безопасности точки доступа

WEP

Пароль	Пароль для точки доступа

WPA/WPA2

Пароль	Пароль для точки доступа

802.1x EAP

EAP-метод

PWD	Идентичность	Идентичность
	Пароль	Пароль

PEAP	Протокол аутентификации Фазы 2	нет	Никакого дополнительного протокола
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертификат CA	Сертификат ЦС	
	Идентичность	Идентичность	
	Анонимная личность	Анонимная личность	
	Пароль	Пароль	

TTLS	Протокол аутентификации Фазы 2	нет	Никакого дополнительного протокола
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертификат CA	Сертификат CA	
	Идентичность	Идентичность	
	Анонимная личность	Анонимная личность	
	Пароль	Пароль	

TLS	Сертификат CA	Сертификат ЦС
	Идентичность	Идентичность
	Пароль	Пароль

VPN

Имя соединения	Имя VPN-соединения

Тип VPN

VPN

VPN-клиент

AppTec360 VPN Client	
Конфигурация шлюза	Выберите конфигурацию VPN шлюза (см. **Общие настройки > Универсальный шлюз > Настройки VPN**).
Always On VPN	Включить нативную блокировку
Включите блокировку AppTec360	Включите блокировку AppTec360

Встроенный (доступно только на устройствах Samsung)			
Тип соединения	PPTP	Сервер	Сервер
		Включить шифрование PPTP	Включить шифрование PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Включить секрет L2TP	Включить секрет L2TP
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сервер	Сервер
		Идентификатор IPSec	Идентификатор IPSec
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
DNS Поиск доменов	DNS Поиск доменов		
Экспертные настройки	Серверы DNS	Серверы DNS	
	Маршруты переадресации	Маршруты переадресации	

Открытый VPN		
Сервер	Сервер	
Профиль OpenVPN	Профиль OpenVPN	
Приложение OpenVPN	OpenVPN для Android (рекомендуется)	
	OpenVPN Connect	
Экспертные настройки	Серверы DNS	Серверы DNS
	Маршруты переадресации	Маршруты переадресации

Samsung / Strong Swan			
Тип соединения	PPTP	Сервер	Сервер
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить шифрование PPTP	Включить шифрование PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить секрет L2TP	L2TP Secret
	IPSec XAuth PSK	Сервер	Сервер
		Идентификатор IPSec	Идентификатор IPSec
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
Экспертные настройки	Серверы DNS	Серверы DNS	
	Маршруты переадресации	Маршруты переадресации	

Cisco Any Connect		
Сервер	Сервер	
Режим сертификата	Отключено	Отключено
	Автоматический	Автоматический
Экспертные настройки	Серверы DNS	Серверы DNS
	Маршруты переадресации	Маршруты переадресации

VPN для каждого приложения

VPN-клиент

AppTec360 VPN Client		
Конфигурация шлюза	Выберите конфигурацию VPN шлюза (см. **Общие настройки > Универсальный шлюз > Настройки VPN**).	
Приложения VPN	Приложения VPN	
Always On VPN	Включить нативную блокировку	Always On VPN
Включите блокировку AppTec360	Включите блокировку AppTec360	

Samsung / Strong Swan			
Тип соединения	PPTP	Сервер	Сервер
		Приложения VPN	Приложения VPN
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить шифрование PPTP	Включить шифрование PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Приложения VPN	Приложения VPN
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить секрет L2TP	L2TP Secret
	IPSec XAuth PSK	Сервер	Сервер
		Приложения VPN	Приложения VPN
		Идентификатор IPSec	Идентификатор IPSec
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
Экспертные настройки	Серверы DNS	Серверы DNS	
	Маршруты переадресации	Маршруты переадресации	

Ограничения

Здесь Вы можете установить ограничения, связанные с управлением соединениями.

Разрешить роуминг данных	Разрешите передачу мобильных данных в роуминге
Принудительный роуминг данных	Если эта функция активирована, роуминг для мобильных данных будет постоянно включен (не рекомендуется!). Эта настройка заменяет настройку "Разрешить роуминг данных"!
Следующие настройки доступны только в SAFE 2.x или выше	
Разрешить только экстренные вызовы	Разрешить только экстренные вызовы
Разрешить WiFi	Разрешить WiFi
Минимальный уровень безопасности сети WiFi	Минимальный уровень безопасности сети WiFi Открыто = разрешены все типы WiFi
Запретите пользователю добавлять сети WiFi	Пользователь не может самостоятельно добавить сеть WiFi Эта настройка возможна только в том случае, если профиль WiFi был определен в разделе "Управление подключением".
Разрешить SMS и MMS	Все = Весь SMS и MMS трафик разрешен Incoming SMS Only = Разрешены только входящие SMS-сообщения Только исходящие SMS = Разрешены только исходящие SMS-сообщения Нет = Трафик SMS / MMS не разрешен
Разрешить синхронизацию во время роуминга	Разрешить синхронизацию во время роуминга Вкл = активировано Выключено = деактивировано Выбор пользователя = выбор пользователя
Разрешить голосовой роуминг	Разрешить голосовой роуминг Вкл = активировано Выключено = деактивировано Выбор пользователя = выбор пользователя
Используйте системный http-прокси-сервер	Использование HTTP-прокси-сервера, которое предусмотрено настройками системы в разделе "Настройки", зависит от подключенной сети (WiFi или APN).

Управление PIM

Gmail Exchange

Информация: Эта настройка будет применена к приложению Gmail. Поэтому Вам необходимо одобрить и установить Gmail.

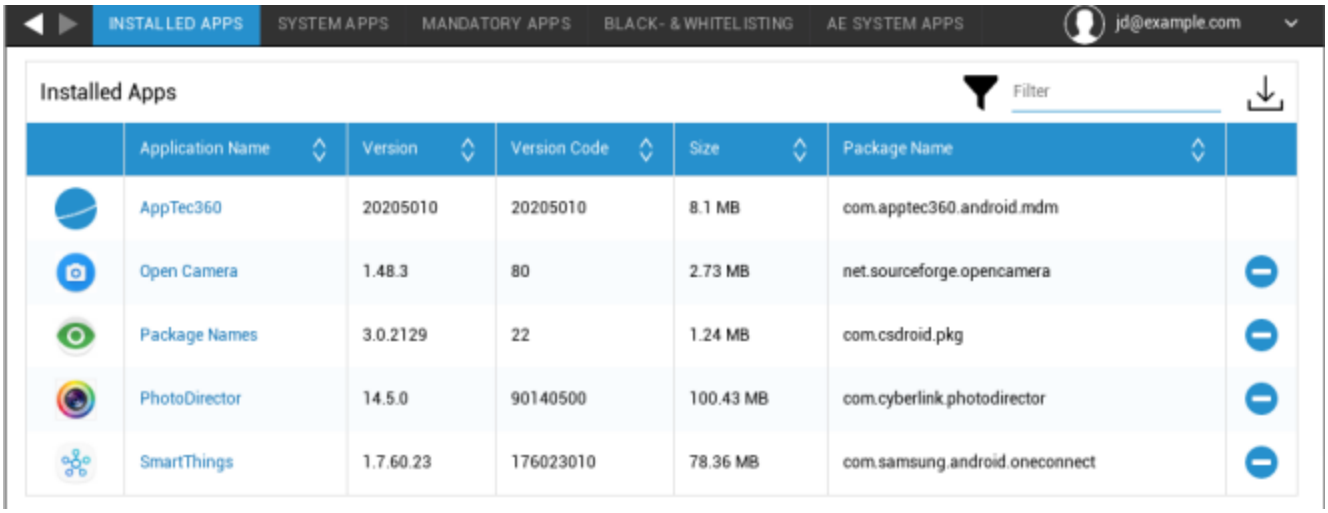
Адрес электронной почты	Адрес электронной почты пользователя Обратите внимание на "Placeholders", которые Вы можете использовать для работы с учетными данными и не выполнять изменения вручную на каждом устройстве Щелкнув мышью, Вы можете сами показать их.
Имя хоста сервера	Адрес сервера Ваших серверов Exchange
Имя пользователя	Имя входа в систему для соответствующего устройства конечного пользователя, пожалуйста, также обратите внимание на "Placeholders here
Подпись	Можно прикрепить подпись (Подсказка: некоторые устройства требуют HTML-форматирования подписи)
Количество предыдущих дней для синхронизации	Количество дней, определяющее, когда электронная почта будет синхронизирована обратно
Идентификатор устройства	Ein String der die EAS DeviceID enthält. Это Teil des EAS Protokols и может быть использован в некоторых регионах.
Используйте Secure Sockets Layer (SSL)	Используйте SSL-соединение
Принимайте все сертификаты	Все сертификаты принимаются. Пожалуйста, выберите эту опцию, если Ваш Exchange Server использует самоподписанный сертификат

Управление приложениями

Enterprise App Manager

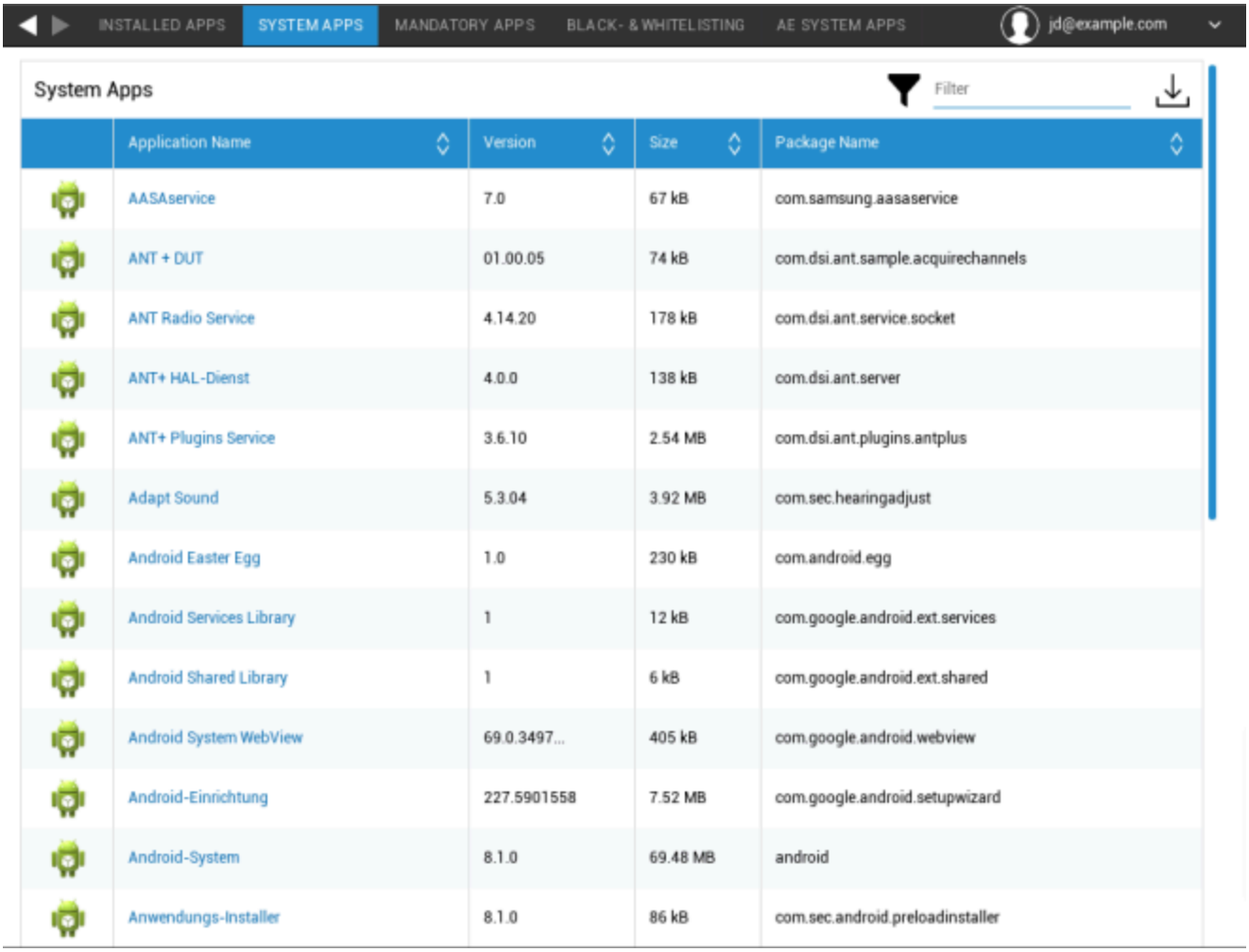
Установленные приложения (только на уровне устройства)

Здесь будут показаны все приложения, которые в данный момент установлены на устройстве конечного пользователя.



Системные приложения (только на уровне устройства)

В разделе "Системные приложения" будут перечислены все приложения и службы, которые уже были установлены на устройство конечного пользователя производителем Вашего устройства.

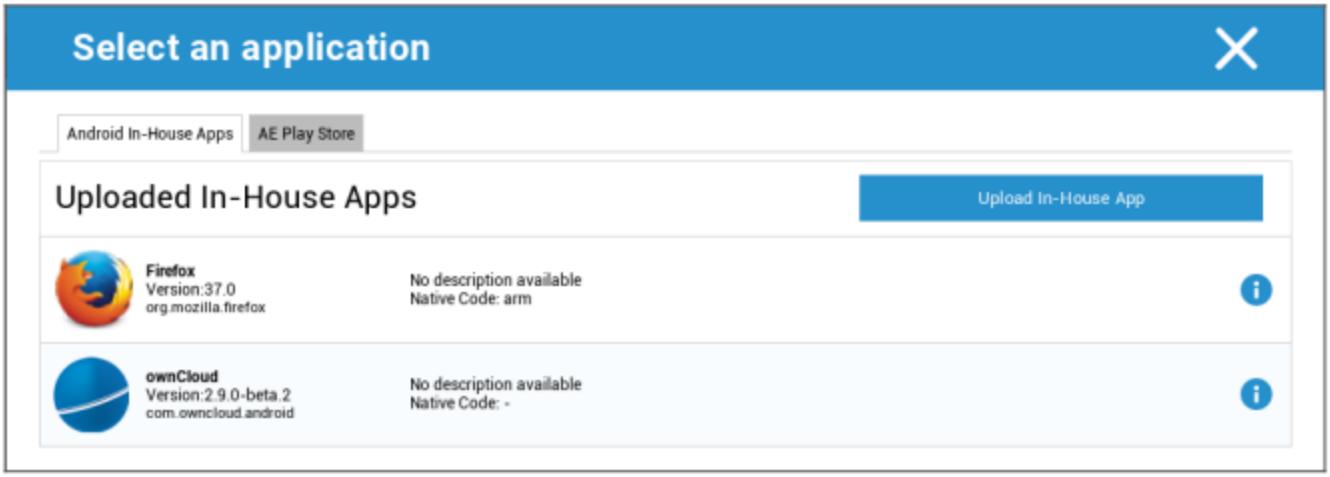


Обязательные приложения

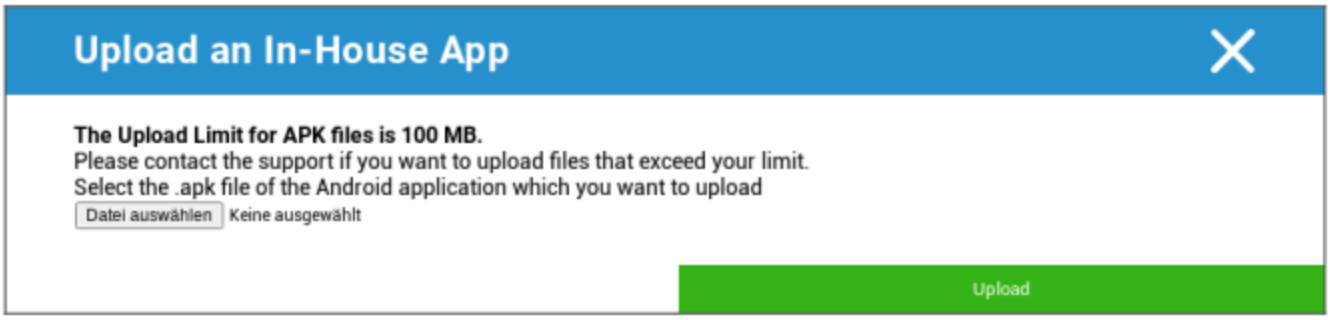
В разделе Обязательные приложения Вы можете установить обязательные приложения. Пользователю будет постоянно предложено установить это приложение.

С помощью , можно определить обязательное приложение.

Это может быть внутреннее приложение из списка "Внутренние приложения Android", который Вы загрузили в Общие настройки.

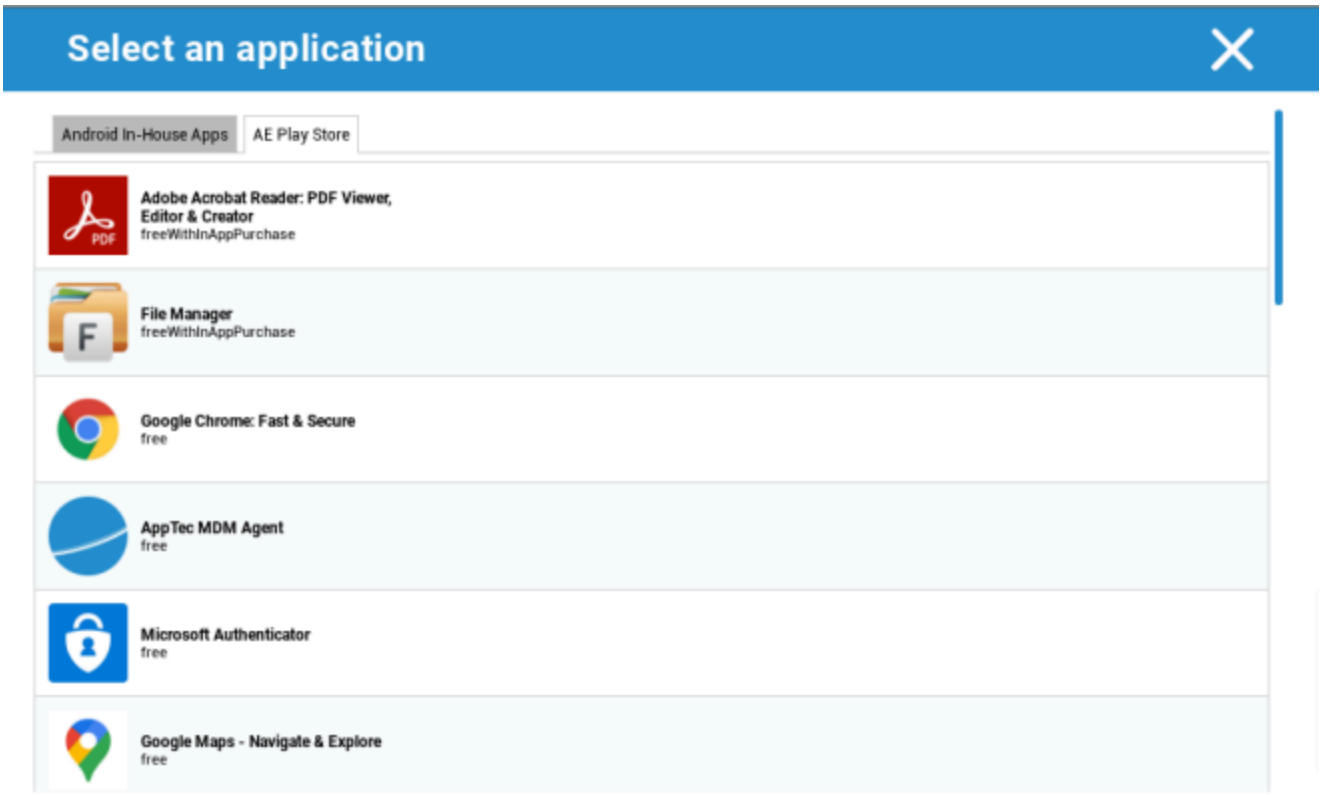


Вы также можете напрямую выбрать и загрузить apk-файл с помощью функции "Upload In-House App".



Если Вы устанавливаете приложение In-House App, у Вас будет возможность активировать функцию "Keep up to date". Если эта функция активирована, и Вы определили более новую версию в In-House App DB, приложение будет обновлено на устройстве.

Или это может быть приложение "AE Play Store" из Google Work Play Store.



На этой вкладке будут отображаться только одобренные приложения "AE Play Store Apps".

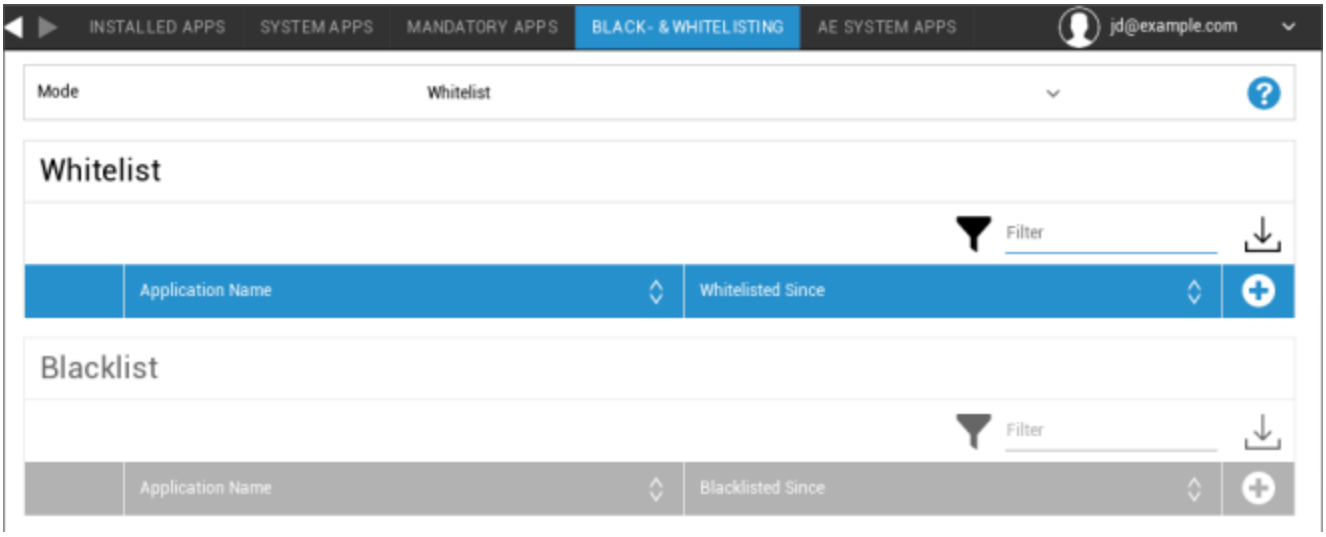
Чтобы одобрить приложение "AE Play Store App", перейдите в раздел "Общие настройки" > "Управление приложениями" > "AE Play

Store" и добавьте приложение с помощью кнопки, которая перенаправит Вас на вкладку "Play Store Apps" (или Вы
можете напрямую перейти на вкладку "Play Store Apps").

На вкладке "Play Store Apps" Вы можете искать приложения. Когда Вы нажимаете на приложение, открывается страница приложения
, и здесь Вы можете одобрить приложение, нажав на кнопку "Одобрить".

Черные и белые списки

В разделе "Черный и белый список" Вы можете выбрать режим "Белый список" или режим "Черный список".

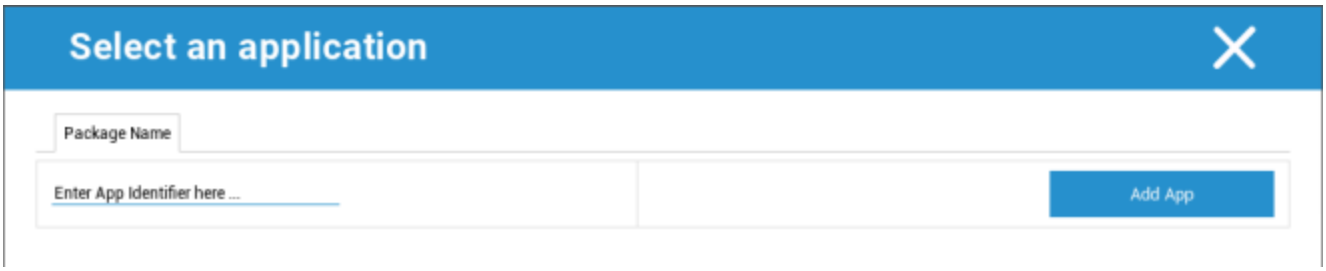


Белый список	Только те приложения и службы, которые добавлены в список, могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут активированы и установлены, чтобы пользователь мог их запускать.
	Все остальные приложения, не добавленные в список, не могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут деактивированы и установлены, так что пользователь не сможет их запустить.
Черный список	Приложения и службы, добавленные в список, не могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут деактивированы и настроены так, что пользователь не сможет их запустить.
	Все остальные приложения, не добавленные в список, могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут активированы и установлены, чтобы пользователь мог их запустить.

С помощью кнопки , Вы добавляете дополнительные приложения или услуги в список используемых в данный момент.
С помощью кнопки , Вы добавляете дополнительные приложения или услуги в список

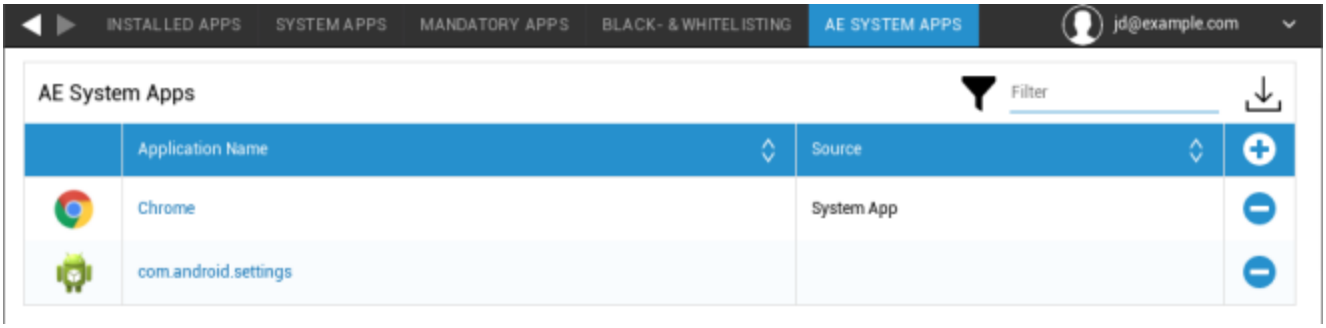
неактивных.

Вы можете определить "Имя пакета":

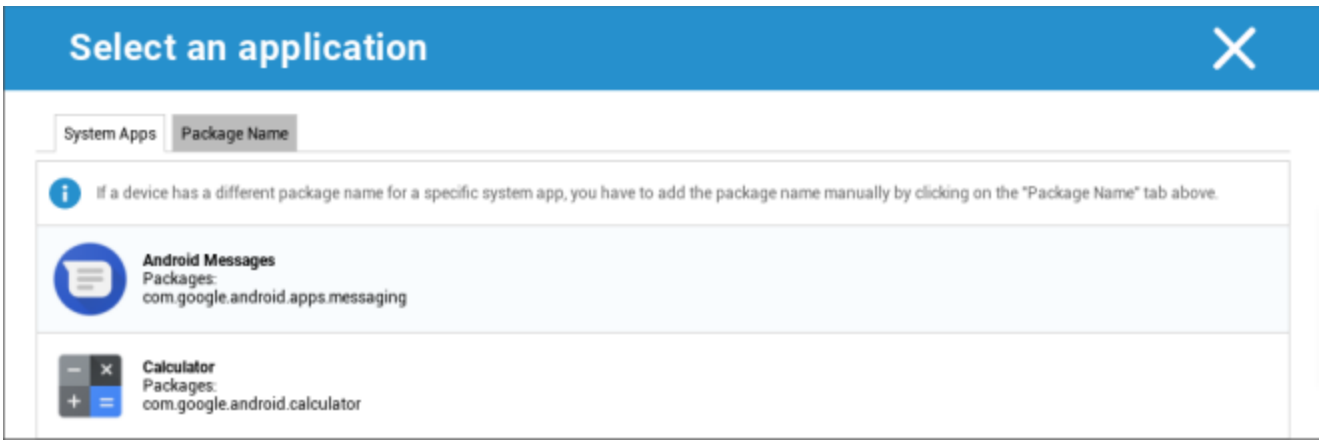


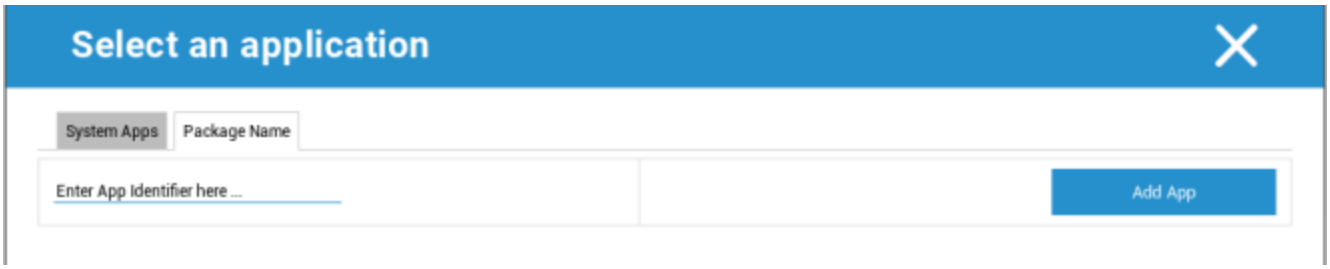
Системные приложения AE

Здесь Вы можете определить список, содержащий определенные системные приложения, которые должны быть активированы на устройствах.



Если Вы нажмете на кнопку, Вы можете выбрать из списка возможных системных приложений, предоставленного Google, или напрямую ввести название пакета системного приложения, которое необходимо активировать.





Имейте в виду, что системные приложения в списке, предоставленном Google, - это только те приложения, которые могут быть системными, но не обязательно должны быть системными на Ваших устройствах.

Однако этот список затрагивает только те приложения, которые уже предустановлены.

Добавление приложений, которые не были предварительно установлены на Ваших устройствах, не повлияет на работу устройств, независимо от того, будет ли это приложение из списка, предоставленного Google, или название пакета приложения будет введено напрямую.

Ограничения и настройки

Настройки управления приложениями

Здесь Вы можете настроить поведение устройства в отношении обновлений приложений.

Частота проверки обновлений	Укажите, через какой промежуток времени AppTec360 Client будет искать обновления приложений. Значение по умолчанию - 24 часа.
Порог Wi-Fi	Приложения, размер которых превышает указанный, будут загружаться по Wi-Fi. Если выбрано "Только Wi-Fi", все приложения будут загружаться через Wi-Fi.

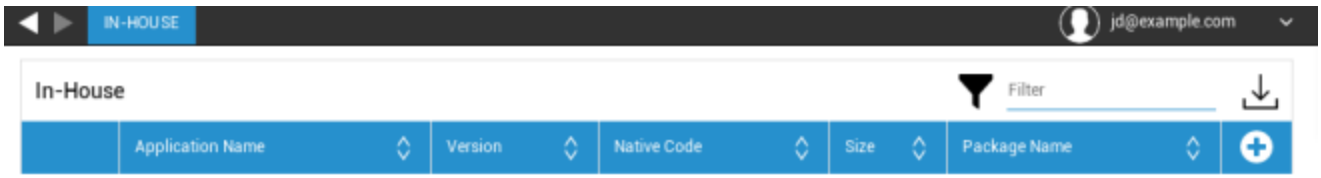
Магазин приложений для предприятий

In-House

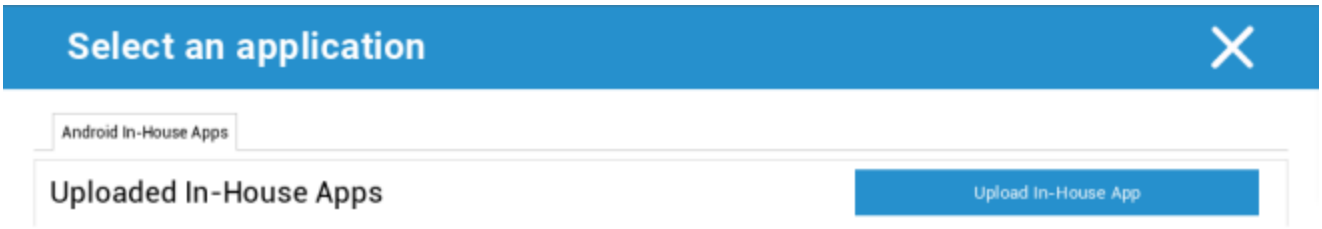
В пункте "In-House" Вы можете загружать и распространять приложения, разработанные внутри компании.

С помощью символа Вы можете распространять дополнительные приложения In-House Apps.

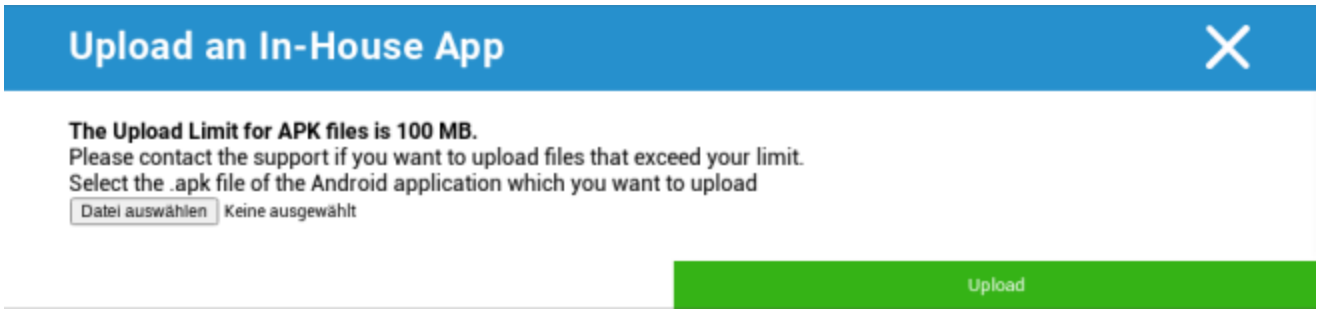
Если Вы устанавливаете приложение In-House App, у Вас будет возможность активировать опцию "Keep up to date". Если
активирована эта опция, и Вы определили более новую версию в In-House App DB, приложение будет
обновлено на устройстве.



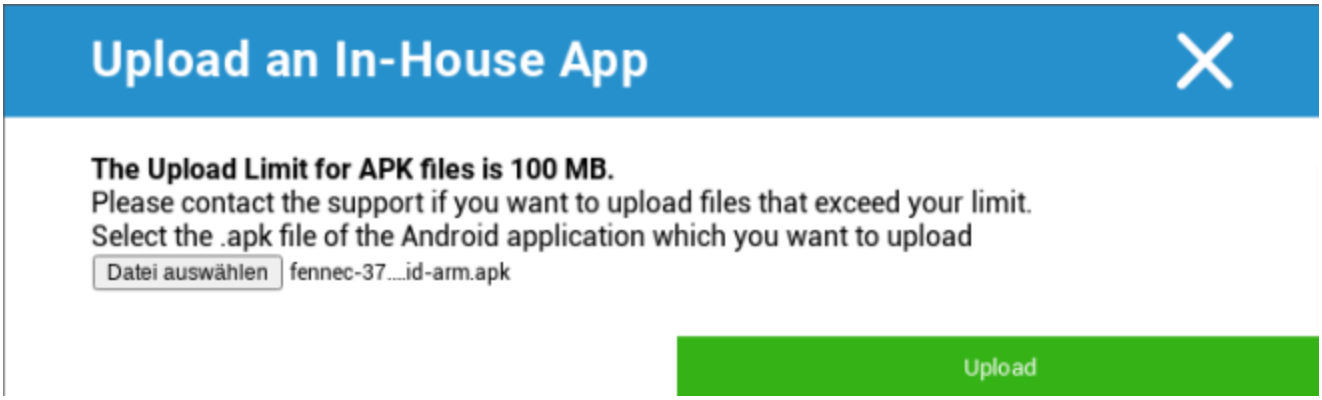
Если Вы не занимались распространением In-House Apps, Вы получите следующий обзор:



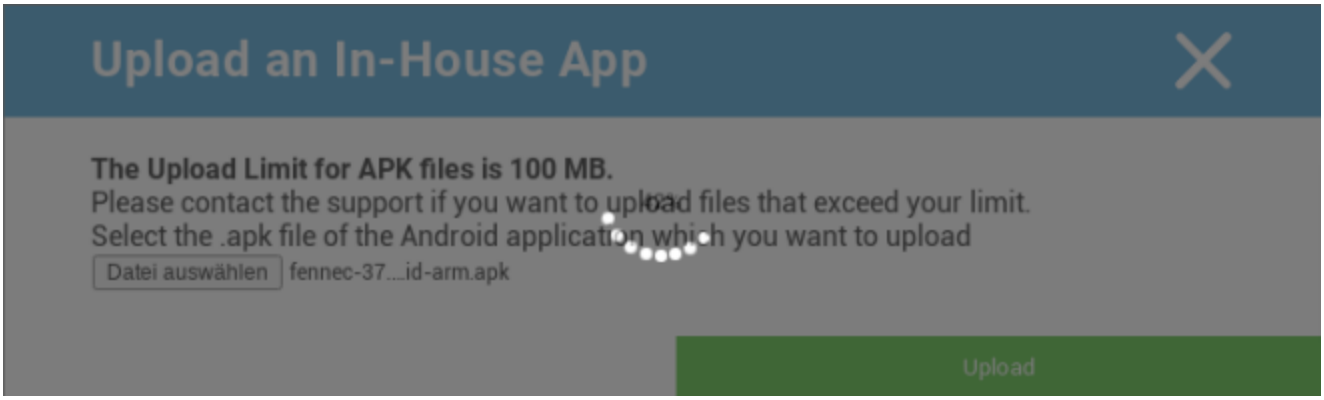
Для этого нажмите на "Upload In-House App", после чего Вы получите следующий обзор:



Теперь выберите с помощью "Search... "файл .apk, а затем нажмите "Upload".



Теперь Ваше приложение будет загружено, в центре круга Вы увидите процентный индикатор, , показывающий, какая часть Вашего приложения уже загружена.



Если загрузка Вашего внутреннего приложения прошла успешно, Вы можете найти загруженное приложение
в Вашем каталоге приложений.

Теперь у пользователя есть возможность увидеть и установить это приложение в AppTec360 Store на устройстве конечного пользователя
, в категории "In-House".

Благодаря тому, что это не приложение Google PlayStore, пользователю не нужен сохраненный Google
ID на соответствующем устройстве конечного пользователя.

Enterprise Play Store

AE Play Store

Здесь Вы можете добавлять приложения в Android Enterprise Playstore. Обратите внимание, что перед тем, как добавлять приложения, Вы должны одобрить
Apps с помощью учетной записи администратора AE.

Чтобы одобрить приложение, пожалуйста, ознакомьтесь с инструкциями в разделе Обязательные приложения.

Режим киоска и пусковая установка

Режим киоска

Режим киоска позволяет Вам предварительно определить приложение или URL. После этого на сайте
можно будет запускать/посещать только это приложение или URL.

Аналогично, различные аппаратные кнопки могут быть отключены в различных режимах Kiosk Mode.

Автоматический старт	Автоматический запуск режима киоска, как только профиль достигнет конечного пользовательского устройства
Режим киоска по расписанию?	Вы можете запланировать время для режима киоска, который будет автоматически начинаться и заканчиваться в установленное Вами время.
Время начала	Время начала
Время в минутах	Время в минутах, по истечении которого режим киоска должен снова завершиться

Тип применения

Одно приложение	Если Вы хотите запустить приложение в режиме киоска, выберите "Пакет" в разделе "Тип приложения".
Применение киосков	Нажмите здесь, чтобы выбрать приложение, которое должно быть запущено в режиме киоска Вы найдете обычный обзор App Management Вы можете выбрать между "Google Play Store", "Android In-House Apps" и "Packagename".

Тип применения	
URL	Если Вы хотите запустить URL в режиме киоска, выберите "URL" в разделе "Тип приложения". Затем определите желаемый адрес URL
Очистите браузер после бездействия	Здесь Вы можете задать временной интервал в минутах, по истечении которого режим киоска должен быть перезапущен.
Очистите веб-кэш и файлы cookie	Если Вы активируете эту функцию, то после перезапуска режима киоска веб-кэш (куки и кэшированные изображения) будет удален.
Политика одинакового происхождения	Если эта функция активна, то пользователь может просматривать только подстраницы определенного URL. Например, Вы определили следующий URL:www.mypage.com Затем пользователь может перейти на сайт: www.mypage.com/subpage.
URL-адреса, внесенные в белый список	Здесь Вы можете создать белый список, в котором все эти URL будут разрешены Не более 1 URL в строке URL должен начинаться с http:/ или https://.
URL-адреса, занесенные в черный список	Здесь Вы можете вести Черный список, в котором все эти URL будут запрещены. Не более 1 URL в строке URL должен начинаться с http:/ или https://.
Ориентация экрана	Эта настройка относится к настройкам экрана Автоматический = автоматический Портрет = вертикальный формат Пейзаж = ландшафтный режим

Мультиприложение	Если Вы выбрали режим киоска "Multi App", использование AppTec360 Launcher будет обязательным.
Приложения	Приложение: Выберите Playstore или собственное приложение в качестве приложения для киоска. Также можно ввести название пакета. Выбранное приложение для киоска должно быть установлено на устройстве. Не забудьте установить приложение для киоска как обязательное. Ярлык на домашнем экране: Если установлено значение "Вкл.", будет создан ярлык на домашнем экране. Если установить значение "Выкл.", приложение по-прежнему будет отображаться в Списке приложений.

Пароль выхода Включен	Если Вы активируете эту функцию, то пользователь сможет завершить режим киоска с помощью пароля, который был предварительно определен Вами
Пароль выхода	Это пароль, который был предварительно определен Вами
Автоматическое сворачивание строки состояния	Если эта опция включена, Строка состояния будет автоматически закрашиваться. С этой опцией пользователи смогут видеть информацию в Строке состояния, но не смогут получить доступ к ее функциям
Отключите строку состояния	Строка состояния содержит Уведомления, Ярлыки и Информацию. Доступно только для устройств Samsung с SAFE 4.0 или выше.
Отключите клавиши регулировки громкости	Отключите клавиши регулировки громкости (доступно только на устройствах Samsung с SAFE 3.0 или выше)
Отключить переключатель включения/выключения	Отключите переключатель Вкл/Выкл (доступно только на устройствах Samsung с SAFE 3.0 или выше)
Отключите кнопку Home	Отключите кнопку "Домой". Если эта функция была активирована, то режим киоска может быть завершен только в консоли AppTec360 (доступно только на устройствах Samsung с SAFE 3.0 или выше)
Отключить панель навигации	С ее помощью Вы можете отключить панель навигации (Назад / Меню). Если эта функция активирована, то режим киоска может быть прерван только в консоли AppTec360. (доступно только на устройствах Samsung с SAFE 3.0 или выше)

AppTec360 Launcher

Включите AppTec360 Launcher	Вкл: Включает AppTec360 Launcher. Пользователь должен один раз установить его в качестве пусковой установки по умолчанию. Примечание: Если режим киоска включен, а для режима киоска установлено значение "Multi App", использование программы запуска AppTec360 будет принудительным.
Большие иконки	Вкл: Показывает увеличенную версию значков приложений в лаунчере.
Скрыть значок приложения AppTec360	Вкл: Полностью скрывает приложение AppTec360
Скрыть значок магазина AppTec360	Вкл: Полностью скрывает AppTec360 Enterprise AppStore

Настройки AppTec360

Включите приложение AppTec360 Settings	Приложение AppTec360 Settings App обеспечивает контроль над соединениями WiFi и Bluetooth
Включите настройки в Multi App Режим киоска	Если эта функция включена, пользователи могут получить доступ к приложению AppTec360 Settings App, пока активен режим киоска с несколькими приложениями

Пульт дистанционного управления

Splashtop

Чтобы начать сеанс удаленного управления Вашим устройством, необходимо установить на него приложение "Splashtop Streamer", добавив его в **App Management** → **Enterprise App Manager** → **Mandatory Apps**.

После этого настройте следующие параметры для Splashtop:

Включите Splashtop	Если включено, AppTec360 настроит приложение Splashtop на удаленное управление
Развертывание кода	Перейдите на сайт https://my.splashtop.com и войдите в свою учетную запись Splashtop. Нажмите на "Добавить компьютер" и скопируйте 12-значный код развертывания с появившейся страницы.
Установить пользовательский шлюз развертывания?	Развертывание шлюза
Развертывание шлюза Домен / Хост	Развертывание шлюза
Проверка сертификата	Проверка сертификата

Затем Вы можете воспользоваться опцией Splashtop Remote Control контекстного меню (шестеренка рядом со строкой поиска, когда устройство выбрано, или щелчок правой кнопкой мыши на устройстве в дереве), чтобы начать сеанс удаленного управления.

TeamViewer

Чтобы начать сеанс удаленного управления Вашим устройством, необходимо установить на него приложение "TeamViewer QuickSupport", добавив его в **App Management** → **Enterprise App Manager** → **Mandatory Apps**.

Затем Вы можете воспользоваться опцией **TeamViewer Remote Control** контекстного меню (шестеренка рядом со строкой поиска, когда устройство выбрано, или щелчок правой кнопкой мыши на устройстве в дереве), чтобы начать сеанс удаленного управления.

Управление контентом

ContentBox

Здесь Вы можете активировать ContentBox.

Как только Вы переключите "Включить ContentBox" на "Вкл.", отдельное приложение ContentBox App будет установлено
автоматически на устройство конечного пользователя.

Безопасный браузер

Здесь Вы можете настроить параметры AppTec360 Secure Browser.

Как только Вы переключите раздел "Безопасный браузер" в положение "Вкл.", отдельное приложение для браузера будет
автоматически установлено на устройство конечного пользователя.

Требуется пароль	Требуйте, чтобы пользователь установил и использовал пароль для доступа к браузеру.
Минимальная требуемая длина пароля	Установите необходимое количество символов для пароля
Требуемое качество пароля	Установите необходимое качество пароля
Ограничить загрузку / Открыть в	
Ограничение загрузки	
Загрузите белый список	Список URL-адресов, для которых всегда будет разрешена загрузка.
Разрешить копирование	Позволяет копировать, вырезать или делиться текстом внутри веб-страниц.
Разрешить захват экрана	Позволяет делать скриншоты.
Частота очистки данных	Выберите, с какой периодичностью должны автоматически удаляться ВСЕ пользовательские данные (история, кэш и т.д.).
Закладки компании	Закладки появятся в папке "Закладки компании" в закладках браузера. Они не редактируются пользователем.
Скрыть адресную строку	
Белые списки в браузере (без Universal Gateway)	Включает "белые списки" URL на стороне клиента. • Закладки компании всегда в белом списке • Поддерживается только для 100 URL-адресов • Пожалуйста, используйте Универсальный шлюз для неограниченного использования черных и белых списков.

URL-адреса, внесенные в белый список	Список разрешенных URL-адресов.
Черные и белые списки на основе шлюза	К черному списку предъявляются следующие требования: • Работающий Универсальный шлюз AppTec360 ("Общие настройки" → "Универсальный шлюз") • Рабочая конфигурация VPN с указанным DNS-сервером ("Общие настройки" → "Универсальный шлюз" → "Настройки VPN") • Конфигурация черного списка ("Общие настройки" → "Универсальный шлюз" → "Черный список доменов") • Действующее VPN-соединение в профиле ("Управление соединениями" → "VPN")

Дополнительный API

Samsung KNOX

Ограничения

Разрешить SD-карту	
Разрешить запись на SD-карту	
Разрешить захват экрана	
Разрешить буфер обмена	
Резервное копирование настроек и данных приложений в Google Cloud	
Восстановление настроек из Google Cloud при переустановке приложения	
Разрешить отладку по USB	
Разрешить Google Crash Report	
Разрешить сброс к заводским настройкам	
Разрешить OTA-обновление	
Разрешить хранение данных на USB-хосте	Если эта функция включена, пользователь может подключить любой накопитель (портативный USB-накопитель), внешний HD-накопитель или устройство для чтения карт памяти Secure Digital (SD), и он будет смонтирован на устройстве как накопитель.
Разрешить USB-медиаплеер (MTP,PTP)	
Разрешить микрофон	Отключите микрофон для приложений сторонних разработчиков
Разрешить NFC (связь ближнего поля)	
Разрешить неизвестные источники (боковая загрузка APK)	Если включено, то разрешена боковая загрузка приложений (APK-файлов).

	Если эта настройка отключена, пользователю придется включить ее вручную, когда Вы разрешите установку APK из неизвестных источников.
Разрешить создание пользователей	Если эта опция включена, пользователю разрешается создавать несколько учетных записей на устройстве, например, гостевые учетные записи.

Электронная почта

Адрес электронной почты	
Протокол входящего сервера	
Адрес входящего сервера	
Порт входящего сервера	
Логин/имя пользователя входящего сервера	
Пароль входящего сервера	
Входящий сервер использует SSL	
Входящий сервер использует TLS	
Входящий сервер принимает все сертификаты	
Протокол исходящего сервера	
Адрес исходящего сервера	
Порт исходящего сервера	
Исходящий сервер использует дополнительные учетные данные	Если отключено, система использует входящие учетные данные и для исходящего сервера.
Логин/имя пользователя исходящего сервера	
Пароль исходящего сервера	
Исходящий сервер использует SSL	
Исходящий сервер использует TLS	
Исходящий сервер принимает все сертификаты	
Установите подпись	
Подпись	Примечание: Для некоторых устройств подпись должна быть указана в формате HTML.
Уведомление пользователя о получении новой электронной почты	

Обмен

Адрес электронной почты	
Имя хоста сервера	Имя хоста сервера Exchange Server
Имя пользователя	Имя пользователя, которое используется для входа на сервер Exchange Server
Домен	Если конфигурация шлюза ACL включена и поле Домен не пустое, Универсальный шлюз AppTec360 будет аутентифицировать устройство со следующим именем "Domain\Login Name
Пароль	
Количество предыдущих дней для синхронизации	
Частота синхронизации электронной почты	
Синхронизация в роуминге	
Установите подпись	
Подпись	Примечание: Для некоторых устройств подпись должна быть указана в формате HTML.
Счет по умолчанию	
Используйте Secure Sockets Layer (SSL)	
Используйте защиту транспортного уровня (TLS)	
Принимайте все сертификаты	

APN

Отображаемое имя APN	
Имя точки доступа	Имя APN
Протокол исходящего сервера	
MCC - Код страны мобильного телефона	Оставьте пустым, чтобы использовать mmc установленной SIM
MNC - код мобильной сети	Оставьте пустым, чтобы использовать mnc установленной SIM
Адрес сервера	
Номер порта сервера	
Адрес прокси-сервера	
Адрес MMS-сервера	Оставьте пустым по умолчанию
Номер порта MMS	Оставьте пустым по умолчанию
Адрес MMS-прокси	Оставьте пустым по умолчанию
Имя пользователя	
Пароль	
Тип точки доступа	Принятые типы: "default", "mms", "supl".
	Если передано null или пусто, по умолчанию используется значение "default,supl,mms".
	Оставьте пустым по умолчанию.
Предпочтительный APN	

Bluetooth

Разрешите обнаружение устройства через Bluetooth	
Разрешить сопряжение с Bluetooth	
Разрешить устройства с Bluetooth-гарнитурой	
Разрешите устройства громкой связи Bluetooth	
Разрешите устройства Bluetooth A2DP	A2DP, Advanced Audio Distribution Profile позволяет передавать потоковое аудио между устройствами.
Разрешить исходящие вызовы	
Разрешите передачу данных через Bluetooth	
Разрешите Bluetooth Tethering	
Разрешите подключение к компьютеру через Bluetooth	

Соединение

Разрешить только экстренные вызовыРазрешить Wi-Fi	
Минимальный уровень безопасности сети Wi-Fi	
Запретите пользователю добавлять сети Wi-Fi	Это ограничение может быть активировано только в том случае, если в разделе Управление подключением задан хотя бы один активный профиль Wi-Fi
Разрешить SMS и MMS	
Разрешить синхронизацию во время роуминга	
Разрешить голосовой роуминг	

Android Enterprise — полностью управляемое устройство с рабочим профилем (COPE)

Общее объяснение COPE

COPE - это аббревиатура от **Corporate Owned Personally Enabled**(**"Корпоративная персональная поддержка"**).

Режим COPE позволяет зарегистрировать устройство Android как **Android Enterprise - Fully Managed Device** с интегрированным профилем **Android Enterprise - Container**.

Это может быть либо устройство Android, которое уже зарегистрировано как **Android Enterprise - Fully Managed Device** и на котором дополнительно установлен **Android Enterprise - Container**, либо новое устройство Android, которое непосредственно зарегистрировано как **Android Enterprise - Fully Managed Device** вместе с **Android Enterprise - Container**, установленным поверх него.

Режим COPE доступен только для устройств с Android 8, 9 и 10

Конфигурация профилей для устройств COPE

Поскольку для самого режима COPE не существует профиля конфигурации, конфигурация **Android Enterprise - Fully Managed Device** и **Android Enterprise - Container** разделена на два профиля в рамках профиля COPE. Переключаться между этими двумя профилями для настройки каждого профиля можно, нажав на соответствующую кнопку в левой части консоли:

Оба профиля могут быть настроены, как описано для каждого отдельного профиля:

Android Enterprise - полностью управляемое устройство

Android Enterprise - контейнер

Возврат к полностью управляемому устройству AE

Профиль **Android Enterprise - Container** можно удалить, как описано в разделе **Управление мобильными устройства**ми.

Если удалить профиль Container, профиль COPE будет преобразован в профиль **Android Enterprise - Fully Managed Device**.

Android Enterprise — Конфигурация контейнера

В зависимости от того, выбрали ли Вы в данный момент групповой профиль или устройство, обзор и его подпункты будут отличаться - пожалуйста, внимательно изучите это!

Общие сведения

Обзор профиля (только на уровне профиля)

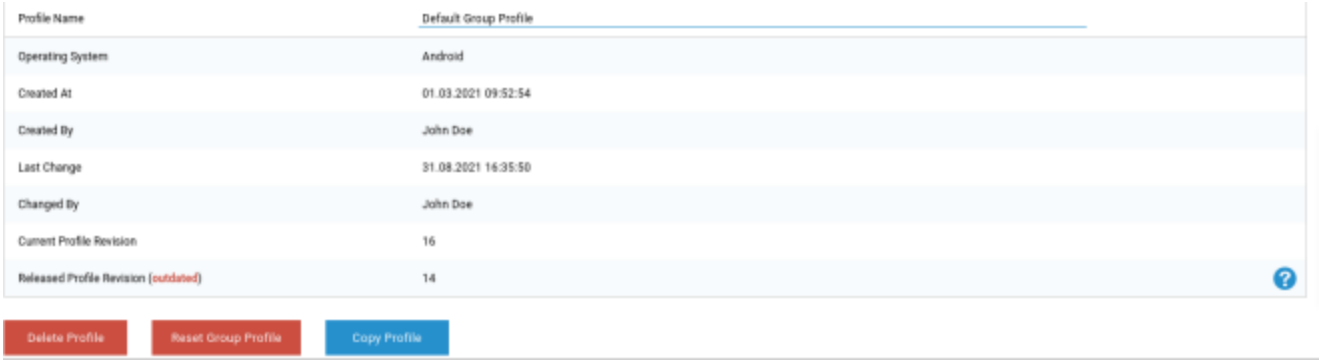
Если Вы находитесь в профиле, Вы получите краткую информацию о нем: название, ОС, дата создания, автор и т.д.

Имя профиля	Имя профиля - может быть непосредственно переименовано здесь
Операционная система	Действительная ОС для профиля
Создано в	Дата создания
Created By	Создано
Последнее изменение	Дата последнего изменения
Изменено	Пользователь, который вносил последние изменения в этот профиль
Текущий пересмотр профиля	Количество раз, когда профиль уже обновлялся
Выпущенный пересмотр профиля	Количество раз, когда профиль уже был обновлен и ему были назначены устройства

Удалить профиль	Удалить профиль
Сброс группового профиля	Сброс группового профиля
Профиль копирования	Профиль копирования

Обзор профиля группы (только на уровне группы)

Открыв профиль группы, Вы получите краткий обзор профиля.



Имя профиля	Название профиля (может быть изменено здесь)
Операционная система	Операционная система, для которой предназначен профиль
Создано в	Время создания
Created By	Создатель профиля
Последнее изменение	Время последнего изменения профиля
Изменено	Учетная запись, которая внесла последние изменения
Текущий пересмотр профиля	Пересмотр сохраненного состояния профиля
Выпущенный пересмотр профиля	Назначенная ревизия профиля ("Назначить сейчас"). Если за текстом на ярлыке отображается "(устаревший)", это означает, что Вы сохранили профиль, но еще не назначили его, поэтому устройства все еще будут получать старую версию.

Обзор устройства (только на уровне устройства)

Если Вы находитесь на устройстве, Вы получите обзорную информацию о выбранном устройстве, в которой содержится следующее:

Имя устройства	Имя устройства
Расположение	Координаты местоположения
Номер телефона	Номер телефона
Назначение Обязательные приложения	Количество назначенных обязательных приложений
Версия ОС	Версия ОС устройства
Операционная система	Операционная система (Android Enterprise)
Серийный номер	Серийный номер устройства
Владение устройством	Корпоративное или личное устройство
Тип устройства	Управляемое устройство AE Work
Rooted	Статус, указывающий, было ли устройство рутировано
Соответствующий	Соответствие рекомендациям
IP-адрес	IP-адрес устройства
Последний раз видели	Точка во времени, когда устройство в последний раз подключалось к AppTec
Последний рывок	Точка во времени, когда последний толчок был отправлен на устройство
Назначение пользователя	Пользователь или группа, которой назначено это устройство

Пересмотр конфигурации

Здесь Вы получите обзор того, какой групповой профиль назначен устройству.

Если Вы нажмете на профиль группы, Вы получите прямой доступ к этому профилю и сможете выполнить настройки.

С помощью этого символа Вы можете вернуть распределенные приложения к настройкам группового профиля.

С помощью этого символа Вы можете вернуть все используемые приложения к настройкам группового профиля.

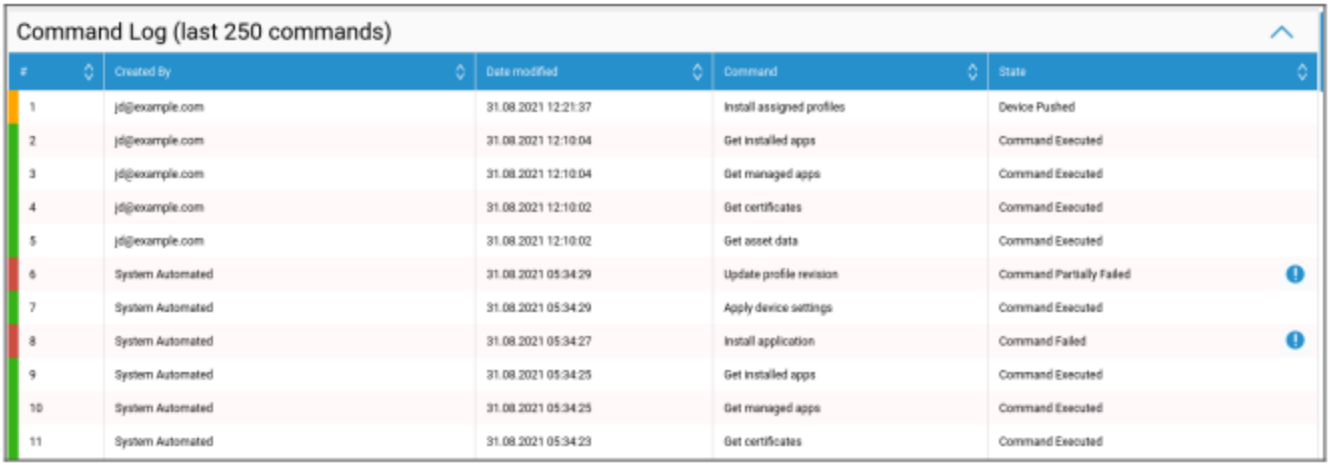
"Доступна более новая редакция" означает, что профиль группы был изменен и сохранен, но не назначен. Чтобы применить изменения к устройствам, групповой профиль должен быть назначен с помощью "Назначить сейчас" на уровне группы.

Журнал устройства (только на уровне устройства)

Здесь Вы получите различные журналы устройств. При необходимости здесь можно напрямую выяснить причину ошибки.

Журнал команд

Здесь Вы можете увидеть, какие команды были отданы устройству и каков их статус.



Возможные статусы команд

Устройство нажимается	Запрос push был отправлен в службу push (например, APNS), чтобы сообщить устройству о необходимости подключиться обратно к серверу EMM.
Команда Создана	Команда была создана в системе.
Команда отправлена	Команда была отправлена на устройство после того, как оно подключилось к серверу.
Команда выполнена	Команда была успешно выполнена.
Команда не выполнена	Команда завершилась неудачно. *
Команда частично не выполнена	В зависимости от ОС устройства некоторые команды могут быть сгруппированы вместе. В этом случае некоторые части этой группы команд оказались неудачными. *
Команда выполнена, в итоге - отказ	Команда была выполнена, но, возможно, она не была выполнена.
Command Repushed	Команда была повторно запущена пользователем.
Выброшенные	Команда была отменена. Например, потому что она была заменена другой командой или устройство было перерегистрировано, и старые команды были удалены.

*Если за сообщением стоит восклицательный знак, Вы можете получить дополнительную информацию, наведя курсор на значок.

Настройки устройства

Конфигурация клиента

Здесь Вы можете выполнить следующие настройки Вашего устройства Android:

Время несоблюдения	Предельное время ожидания ответа пользователя, после которого применяется принудительное действие.
Принудительные действия после истечения времени выполнения	Принудительные действия, когда пользователь не выполняет действия, которые приводят к состоянию устройства, соответствующему требованиям
Частота сбора данных	Частота сбора информации об устройстве/GPS
Частота сердцебиения устройства	Интервал, через который устройство должно связаться с сервером AppTec Server Мин. 1 минута Макс. 24 часа
Включите обновление местоположения	Если устройство активировано, оно отправляет обновления местоположения на сервер AppTec Server
Расположение Время обновления	Определяет, через какие временные интервалы устройство отправляет обновления местоположения в AppTec
Используйте точность определения местоположения Google для обновления местоположения	Если эта настройка активирована, то для обновления местоположения будет использоваться сетевое местоположение (если эта настройка была отключена в разделе "Ограничения", то она ни на что не повлияет)
Используйте GPS для обновления местоположения	Если активировано, GPS будет использоваться для обновления местоположения
Разрешить имитацию (подделку) местоположения	Позволяет подделывать информацию о местоположении с помощью сторонних приложений
Действие при потере соединения	Если эта опция включена, Вы можете указать действие для случая, когда устройство не получает соединения с MDM-сервером в интервале сердцебиения. Например, если устройство имеет интервал сердцебиения 5 минут, оно подключится к серверу в

	10:35 утра. После этого устройство выходит из зоны действия Wi-Fi. Следующее сердцебиение в 10:40 утра будет неудачным, и указанное действие будет выполнено.
Действие	Действия, которые необходимо предпринять, как только устройство становится несоответствующим требованиям. • Lock Устройство = устройство блокировки • Wipe Device = устройство будет восстановлено до заводских настроек • Wipe Device & SD Card = устройство будет восстановлено до заводских настроек, а память SD Card будет удалена.
Порог	Вы можете указать пороговое количество неудачных сердцебиений, которое необходимо для запуска указанного действия.

Режим внедрения политики	По умолчанию:	Пользователям будет периодически предлагаться выполнить невыполненные действия
	Ленивое внедрение политики:	Пользователям никогда не будет предложено выполнить незавершенные действия. Все открытые действия будут отображаться в AppTec Client
	Агрессивное применение политики:	Пользователям будет постоянно предлагаться выполнить невыполненные действия
AppTec Version Lock	Если эта опция включена, можно указать код версии для приложения AppTec. Клиент AppTec будет обновляться только до указанной версии. Более новые версии будут игнорироваться. Понижение версии НЕ возможно.	
Код версии	Код версии для приложения AppTec, к которому нужно привязаться.	
Отключение уведомлений AppTec	Если отключить эту функцию, клиент AppTec не будет показывать уведомление на панели уведомлений. Таким образом, пользователи могут закрыть клиент AppTec через диспетчер задач. Если клиент AppTec закрыт, некоторые функции, включая режим киоска и черный/белый список приложений, не будут работать должным образом. Устройства Samsung предлагают механизм защиты для AppTec Client. Уведомление отключено по умолчанию на устройствах Samsung, поддерживающих API KNOX. Уведомление не должно отключаться на устройствах с Android 8.0 и выше.	

Обои

Установите пользовательские обои	Включение/выключение пользовательских обоев
Обои	Установите режим обоев, чтобы использовать цветовой код или изображение
Укажите цвет	Укажите цвет фона в виде шестнадцатеричного значения, например, #000000 для черного или #ffffff для белого.
Установите изображение в качестве обоев	Загрузите файл с изображением, которое Вы хотите использовать в качестве обоев.

Управление активами (только на уровне устройств)

Информация об устройстве

Модель	Обозначение модели устройства
Операционная система	OS
Версия ОС	Версия ОС
Серийный номер	Серийный номер
Имя устройства	Имя устройства
Состояние батареи	Состояние батареи
Свободная / общая память	Свободная / общая память
Samsung Safe	Интерфейс Samsung SAFE, необходимый для различных настроек
Доступна карта памяти SD	Доступна карта SD
Эмулированная SD-карта	Эмулированная SD-карта
Съемная SD-карта	Съемная SD-карта
Свободная / общая память SD	Свободная память SD / Общая память SD-карты

Wi-Fi

IP-адрес	IP-адрес устройства
WiFi MAC	MAC-адрес WiFi

Клетчатка

Статус	Состояние (SIM-карта установлена)
Номер телефона	Номер телефона
Роуминг (голос / данные)	Роуминг для голоса / данных
Статус роуминга	Текущий статус роуминга
IP-адрес	IP-адрес
Оператор/ перевозчик	Оператор/перевозчик
Клеточные технологии	Клеточные технологии
IMEI	Номер IMEI
ICCID	Это идентификатор SIM-карты, часто также называемой Smartcard или Integrated Circuit Card (ICC).
IMSI	Международный идентификатор мобильного абонента (IMSI) обеспечивает в GSM- и UMTS-мобильных сетях однозначную идентификацию пользователей сети. IMSI состоит максимум из 15 цифр и настраивается следующим образом: • Код страны мобильного телефона (MCC), 3 цифры • Код мобильной сети (MNC), 2 или 3 цифры • Идентификационный номер мобильного абонента (MSIN), 1-10 цифр
Текущий MCC/MNC	См. раздел "SIM MCC/MNC".
SIM MCC/MNC	Код страны мобильной связи - это установленный идентификатор страны, установленный МСЭ в соответствии со стандартом E.212. Он работает в сочетании с кодом мобильной сети (MNC) для идентификации мобильной сети. Означает код страны/мобильной сети SIM-карты. Если Вы переходите в другую мобильную сеть, то, по логике вещей, "Current MCC/MNC" и "SIM MCC/MNC" будут разными.

Bluetooth

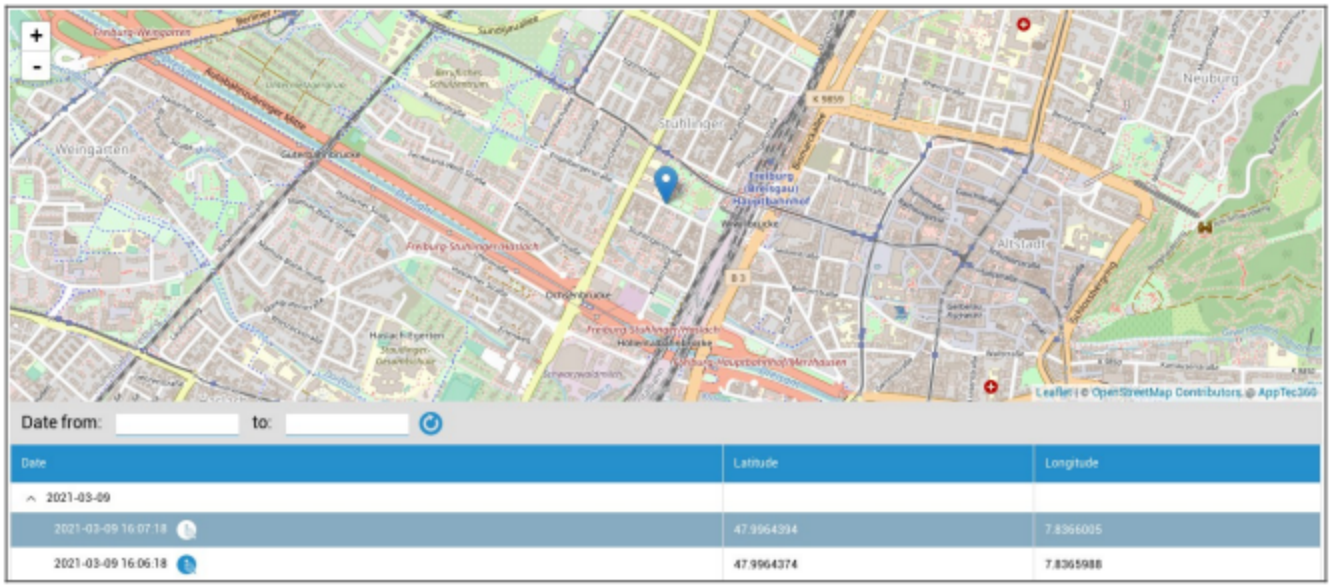
Bluetooth MAC	MAC-адрес Bluetooth

Управление безопасностью

Защита от кражи (только на уровне устройства)

Информация GPS (только на уровне устройства)

Здесь Вы можете установить текущее/последнее местоположение устройства. Локализация может быть защищена одним или даже двумя паролями - См: Общие настройки - Конфиденциальность - Доступ к GPS



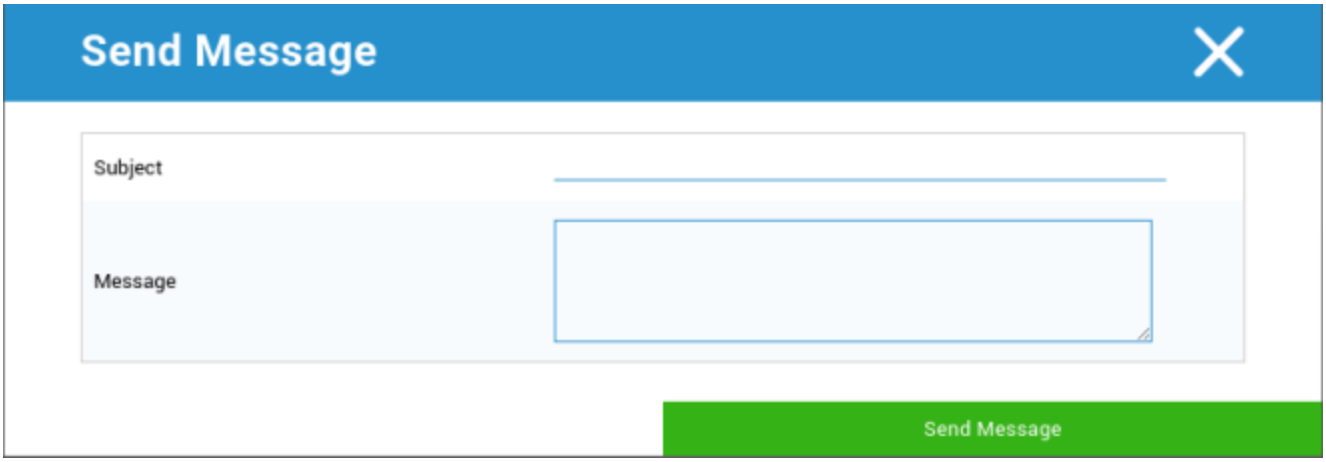
Wipe & Lock (только на уровне устройства)

В разделе "Wipe & Lock" Вы можете выполнить следующие три действия:

Полное вытирание	Устройство возвращается к заводским настройкам (корпоративные, а также личные данные удаляются). Работает только для расширенного рабочего профиля
Enterprise Wipe	С устройства конечного пользователя удаляются только корпоративные данные (все приложения, данные и т.д., которые были предоставлены AppTec)
Экран блокировки	Активирована блокировка экрана, достаточно разблокировать устройство с помощью пароля устройства/PIN-кода

Сообщение (только на уровне устройства)

Здесь Вы можете заполнить тему и сообщение и отправить его на устройство конечного пользователя.



Конфигурация безопасности

Passкод устройства

В разделе "Пароль" Вы можете задать пароль устройства, Вам доступны следующие опции настройки

Минимальная длина пароля	Устанавливает минимальное количество символов, которое должно быть в пароле	
Качество пароля	Неопределенный	В этой политике нет требований к паролю.
	Биометрическая слабость	Эта политика позволяет использовать технологии биометрического распознавания с низким уровнем безопасности. Под этим подразумеваются технологии, способные распознать личность человека примерно до 3-значного PIN-кода (ложное обнаружение составляет менее 1 из 1 000).
	Кое-что	Эта политика требует установки какого-либо пароля или шаблона, но не устанавливает никаких конкретных правил.
	Алфавитный	Пользователь должен ввести пароль, содержащий как минимум алфавитные (или другие символы) символы.
	Буквенно-цифровой	Пользователь должен ввести пароль, содержащий как минимум оба цифровых и буквенных (или других символа) символа.
	Комплекс	По умолчанию пользователь должен ввести пароль, содержащий как минимум букву, цифру и специальный символ. С помощью этого качества пароли можно ограничить, чтобы они содержали различные наборы символов, например, хотя бы заглавную букву и т.д.
Минимальная длина пароля	Установите необходимое количество символов для пароля. Например, Вы можете потребовать, чтобы PIN-код или пароль состояли как минимум из шести символов.	
Минимальное количество цифр в пароле	Минимальное количество цифр в пароле	

Минимальное количество строчных букв в пароле	Минимальное количество строчных букв в пароле
Минимальное количество заглавных букв в пароле	Минимальное количество заглавных букв в пароле
Минимальное количество небуквенных символов, необходимых для пароля	Минимальное количество небуквенных символов, необходимых для пароля
Минимальное количество символов в пароле	Минимальное количество символов в пароле

Максимальная блокировка времени бездействия	Максимальное время бездействия пользователя до временной блокировки
Таймаут истечения срока действия пароля	Устанавливает, через какой промежуток времени срок действия пароля истекает, и необходимо выдать новый пароль
Ограничение истории паролей	Количество ранее использованных паролей, которые не разрешены
Максимальное количество неудачных попыток ввода пароля	Устанавливает, как часто пароль может быть введен неверно, прежде чем будет произведено полное стирание устройства
Разрешить биометрическую аутентификацию	Обеспечивает аутентификацию с помощью отпечатка пальца или сканирования радужной оболочки глаза. Только для Samsung KNOX 2.1 и выше

Passcode контейнера

В разделе "Passcode" Вы можете задать пароль для контейнера, следующие опции настройки доступны для Вас

Минимальная длина пароля	Устанавливает минимальное количество символов, которое должно быть в пароле	
Качество пароля	Неопределенный	В этой политике нет требований к паролю.
	Биометрическая слабость	Эта политика позволяет использовать технологии биометрического распознавания с низким уровнем безопасности. Под этим подразумеваются технологии, способные распознать личность человека примерно до 3-значного PIN-кода (ложное обнаружение составляет менее 1 из 1 000).
	Кое-что	Эта политика требует установки какого-либо пароля или шаблона, но не устанавливает никаких конкретных правил.
	Алфавитный	Пользователь должен ввести пароль, содержащий как минимум алфавитные (или другие символы) символы.
	Буквенно-цифровой	Пользователь должен ввести пароль, содержащий как минимум оба цифровых и буквенных (или других символа) символа.
	Комплекс	По умолчанию пользователь должен ввести пароль, содержащий как минимум букву, цифру и специальный символ. С помощью этого качества пароли можно ограничить, чтобы они содержали различные наборы символов, например, хотя бы заглавную букву и т.д.
Минимальная длина пароля	Установите необходимое количество символов для пароля. Например, Вы можете потребовать, чтобы PIN-код или пароль состояли как минимум из шести символов.	
Минимальное количество цифр в пароле	Минимальное количество цифр в пароле	
Минимальное количество строчных	Минимальное количество строчных букв в пароле	

букв в пароле	
Минимальное количество заглавных букв в пароле	Минимальное количество заглавных букв в пароле
Минимальное количество небуквенных символов, необходимых для пароля	Минимальное количество небуквенных символов, необходимых для пароля
Минимальное количество символов в пароле	Минимальное количество символов в пароле

Максимальная блокировка времени бездействия	Максимальное время бездействия пользователя до временной блокировки
Таймаут истечения срока действия пароля	Устанавливает, через какой промежуток времени срок действия пароля истекает, и необходимо выдать новый пароль
Ограничение истории паролей	Количество ранее использованных паролей, которые не разрешены
Максимальное количество неудачных попыток ввода пароля	Устанавливает, как часто пароль может быть введен неверно, прежде чем будет произведено полное стирание устройства

Антивирус

Автоматическое сканирование	Включите периодическое автоматическое сканирование
Интервал сканирования	Интервал для обследования (Быстрое / Полное)
Полное автоматическое сканирование	Включите полное автоматическое сканирование
Автоматические обновления	Включите автоматические обновления
Интервал проверки обновлений	Как часто следует обновлять приложение и его базу данных (вирусы / поврежденный код)
Защита приложений	Включите автоматическое сканирование приложений
Защита SD-карты	Включите автоматическое сканирование SD-карты
Обновление только через Wi-Fi	Если эта функция включена, обновления будут применяться только при успешном подключении устройства к сети Wi-Fi.

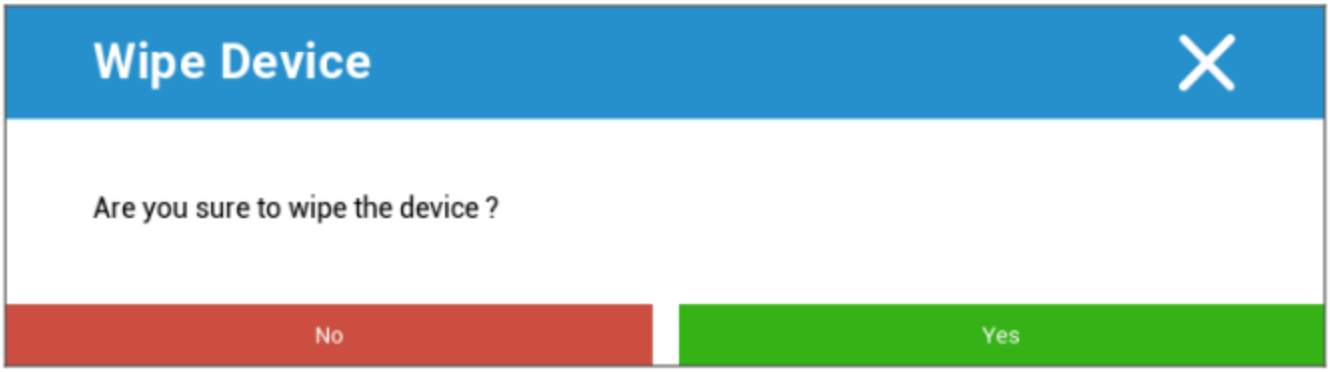
Окончание срока службы (только на уровне устройства)

Стирание (только на уровне устройства)

В разделе "Wipe" Вы можете восстановить заводские настройки устройства (только в режиме Enhanced Work Profile).

Здесь корпоративные, а также личные данные будут удалены на устройстве конечного пользователя.

При нажатии на "Символ минуса" Вы получите следующее сообщение:



Ответив "Да", Вы можете выполнить стирание.

В разделе "Отчет о стирании" отображаются следующие пункты

Стерто	История о том, кто выполнял протирание
Дата	Дата
Статус	Статус (например, успешно ли выполнено стирание)

Настройки ограничений

Ограничения

Здесь можно ограничить и заблокировать множество вещей.

Обеспечение соответствия	Режим Prompt User - Пользователю будет предложено выполнить необходимые действия. Контейнер блокировки режима - скройте все приложения, пока не будут выполнены все требования
Политика разрешений во время выполнения	Предложите пользователю запросить новые разрешения Всегда удовлетворяйте новые запросы на разрешение Всегда отклоняйте новые запросы на разрешение Внимание: У некоторых приложений возникают проблемы с распознаванием разрешений, если они установлены автоматически. Если Вы всегда предоставляете разрешения и сталкиваетесь с проблемами, когда приложения говорят, что разрешения отсутствуют, установите значение "подсказать пользователю" и переустановите приложение.
Разрешить исходящий буфер обмена	Позволяет копировать и вставлять из внутреннего контейнера во внешний
Разрешить разрешение идентификатора вызывающего абонента	Показывает имя для входящего вызова на основе контактов в контейнере
Разрешить разрешение поиска контактов	Позволяет искать имена в контактах контейнера при совершении звонков
Разрешите обмен контактами через Bluetooth	Позволяет получить доступ к контакту контейнера в автомобиле
Запретить исходящий луч NFC	Отключение NFC для контейнера
Разрешить неизвестные источники	Если эта функция включена, пользователи могут загружать приложения с боковой стороны, устанавливая файл .apk.
Разрешить отладку по USB	Если эта опция включена, пользователи могут включить отладку по USB.
Запретить изменение учетной записи	Запрещает создание, удаление и изменение учетных записей в контейнере

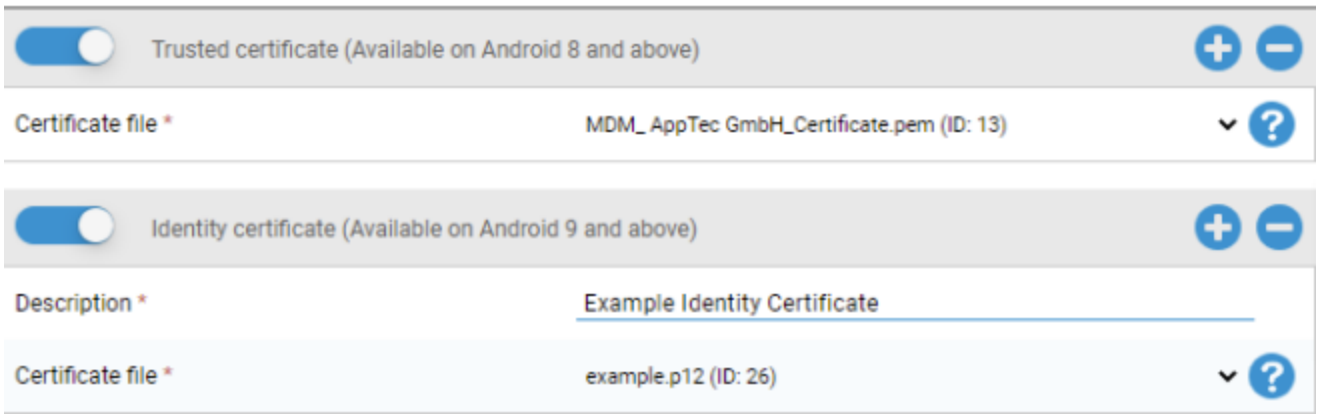
	Имейте в виду, что некоторым приложениям необходимо создать или изменить учетные записи, чтобы они работали как положено.

Ограничения рабочего профиля. Доступно только на устройствах с ОС Android 11 и выше, с расширенным рабочим профилем	
Запретить камеру	Указывает, запрещена ли камера в рабочем профиле.
Запретить Bluetooth	Указывает, запрещен ли bluetooth в рабочем профиле.
Включите защиту от сброса к заводским настройкам	Активируйте эту функцию, чтобы отменить защиту от сброса к заводским настройкам Android на аккаунт Google, который Вы задали в разделе "Общие настройки" → "Конфигурация Android" → "Android Enterprise" → "Защита от сброса к заводским настройкам" Если эта функция включена и Вы сбросили устройство, Вам придется указать настроенный аккаунт Google, чтобы настроить устройство снова.
Контроль обновления ОС	Включите эту опцию, чтобы установить автоматическое, оконное или отложенное обновление.
Политика обновления	Автоматически: Устанавливайте автоматически, как только появится обновление. Оконная: Автоматическая установка в течение ежедневного окна обслуживания. При этом также настраивается обновление приложений Play в пределах окна. Это настоятельно рекомендуется для киосковых устройств, поскольку только так приложения, постоянно находящиеся на переднем плане, могут быть обновлены Play. Отложить: Отложите автоматическую установку максимум на 30 дней.

Ограничения личного профиля. Доступно только на устройствах с ОС Android 11 и выше, с расширенным рабочим профилем	
Запретить камеру	Указывает, запрещена ли камера в личном профиле.
Запретить Bluetooth	Указывает, запрещен ли bluetooth в личном профиле.
Разрешить неизвестные источники	Если эта функция включена, пользователи рабочего профиля могут загружать приложения с помощью установки .apk-файла.

Управление сертификатами

Здесь Вы можете распространять Доверенные сертификаты и Сертификаты идентичности на своих устройствах. Для распространения Доверенных сертификатов требуется Android 8 или выше, а для распространения Идентификационных сертификатов - Android 9 или выше.



С помощью "+" Вы можете добавить несколько сертификатов.

Доверенные сертификаты должны быть в формате PEM.

Сертификаты личности должны быть в формате PKCS12.

Управление соединениями

Wifi

Для этой настройки выполните предварительную конфигурацию устройств конечных пользователей для доступа к внутренним точкам доступа
.

Идентификатор набора услуг (SSID)	SSID для подключаемой сети
Скрытая сеть	Активировать, в случае если точка доступа не передает SSID

Тип безопасности

Установите тип безопасности точки доступа

WEP

Пароль	Пароль для точки доступа

WPA/WPA2

Пароль	Пароль для точки доступа

802.1x EAP

EAP-метод

PWD	Идентичность	Идентичность
	Пароль	Пароль

PEAP	Протокол аутентификации Фазы 2	нет	Никакого дополнительного протокола
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертификат CA	Сертификат ЦС	
	Идентичность	Идентичность	
	Анонимная личность	Анонимная личность	
	Пароль	Пароль	

TTLS	Протокол аутентификации Фазы 2	нет	Никакого дополнительного протокола
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертификат CA	Сертификат CA	
	Идентичность	Идентичность	
	Анонимная личность	Анонимная личность	
	Пароль	Пароль	

TLS	Сертификат CA	Сертификат ЦС
	Идентичность	Идентичность
	Пароль	Пароль

VPN

Имя соединения	Имя VPN-соединения

Тип VPN

VPN

VPN-клиент

AppTec VPN Client	
Конфигурация шлюза	Выберите конфигурацию VPN шлюза (см. **Общие настройки > Универсальный шлюз > Настройки VPN**).
Always On VPN	Включить нативную блокировку
Включите блокировку AppTec	Включите блокировку AppTec

Встроенный (доступно только на устройствах Samsung)			
Тип соединения	PPTP	Сервер	Сервер
		Включить шифрование PPTP	Включить шифрование PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Включить секрет L2TP	Включить секрет L2TP
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сервер	Сервер
		Идентификатор IPSec	Идентификатор IPSec
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
DNS Поиск доменов	DNS Поиск доменов		
Экспертные настройки	Серверы DNS	Серверы DNS	
	Маршруты переадресации	Маршруты переадресации	

Открытый VPN		
Сервер	Сервер	
Профиль OpenVPN	Профиль OpenVPN	
Приложение OpenVPN	OpenVPN для Android (рекомендуется)	
	OpenVPN Connect	
Экспертные настройки	Серверы DNS	Серверы DNS
	Маршруты переадресации	Маршруты переадресации

Samsung / Strong Swan			
Тип соединения	PPTP	Сервер	Сервер
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить шифрование PPTP	Включить шифрование PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить секрет L2TP	L2TP Secret
	IPSec XAuth PSK	Сервер	Сервер
		Идентификатор IPSec	Идентификатор IPSec
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
Экспертные настройки	Серверы DNS	Серверы DNS	
	Маршруты переадресации	Маршруты переадресации	

Cisco Any Connect		
Сервер	Сервер	
Режим сертификата	Отключено	Отключено
	Автоматический	Автоматический
Экспертные настройки	Серверы DNS	Серверы DNS
	Маршруты переадресации	Маршруты переадресации

VPN для каждого приложения

VPN-клиент

AppTec VPN Client		
Конфигурация шлюза	Выберите конфигурацию VPN шлюза (см. **Общие настройки > Универсальный шлюз > Настройки VPN**).	
Приложения VPN	Приложения VPN	
Always On VPN	Включить нативную блокировку	Always On VPN
Включите блокировку AppTec	Включите блокировку AppTec	

Samsung / Strong Swan			
Тип соединения	PPTP	Сервер	Сервер
		Приложения VPN	Приложения VPN
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить шифрование PPTP	Включить шифрование PPTP
	L2TP / IPSec PSK	Сервер	Сервер
		Приложения VPN	Приложения VPN
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
		Включить секрет L2TP	L2TP Secret
	IPSec XAuth PSK	Сервер	Сервер
		Приложения VPN	Приложения VPN
		Идентификатор IPSec	Идентификатор IPSec
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Имя пользователя	Имя пользователя
		Пароль	Пароль
Экспертные настройки	Серверы DNS	Серверы DNS	
	Маршруты переадресации	Маршруты переадресации	

Ограничения

Здесь Вы можете установить ограничения, связанные с управлением соединениями

Разрешить роуминг данных	Разрешите передачу мобильных данных в роуминге
Принудительный роуминг данных	Если эта функция активирована, роуминг для мобильных данных будет постоянно включен (не рекомендуется!). Эта настройка заменяет настройку "Разрешить роуминг данных"!
Используйте системный http-прокси-сервер	Использование HTTP-прокси-сервера, которое предусмотрено настройками системы в разделе "Настройки", зависит от подключенной сети (WiFi или APN).

Управление PIM

Gmail Exchange

Информация: Эта настройка будет применена к приложению Gmail. Поэтому Вам необходимо одобрить и установить Gmail.

Адрес электронной почты	Адрес электронной почты пользователя Обратите внимание на "Placeholders", которые Вы можете использовать для работы с учетными данными и не выполнять изменения вручную на каждом устройстве Щелкнув мышью, Вы можете сами показать их.
Имя хоста сервера	Адрес сервера Ваших серверов Exchange
Имя пользователя	Имя входа в систему для соответствующего устройства конечного пользователя, пожалуйста, также обратите внимание на "Placeholders here
Подпись	Можно прикрепить подпись (Подсказка: некоторые устройства требуют HTML-форматирования подписи)
Количество предыдущих дней для синхронизации	Количество дней, определяющее, когда электронная почта будет синхронизирована обратно
Идентификатор устройства	Ein String der die EAS DeviceID enthält. Это Teil des EAS Protokols и может быть использован в некоторых регионах.
Используйте Secure Sockets Layer (SSL)	Используйте SSL-соединение
Принимайте все сертификаты	Все сертификаты принимаются. Пожалуйста, выберите эту опцию, если Ваш Exchange Server использует самоподписанный сертификат
Разрешить неуправляемые учетные записи	Разрешите пользователям добавлять или удалять любую учетную запись Exchange, кроме той, которая указана в этой управляемой конфигурации. Если этот параметр включен, Вы не можете запретить пользователям добавлять другие учетные записи Exchange в Gmail. Вы также не можете контролировать обмен данными между другими приложениями и учетными записями Exchange, добавленными пользователями. Этот параметр следует включать только в том случае, если Вашим пользователям необходимо поддерживать более одной рабочей учетной записи Exchange в Gmail.

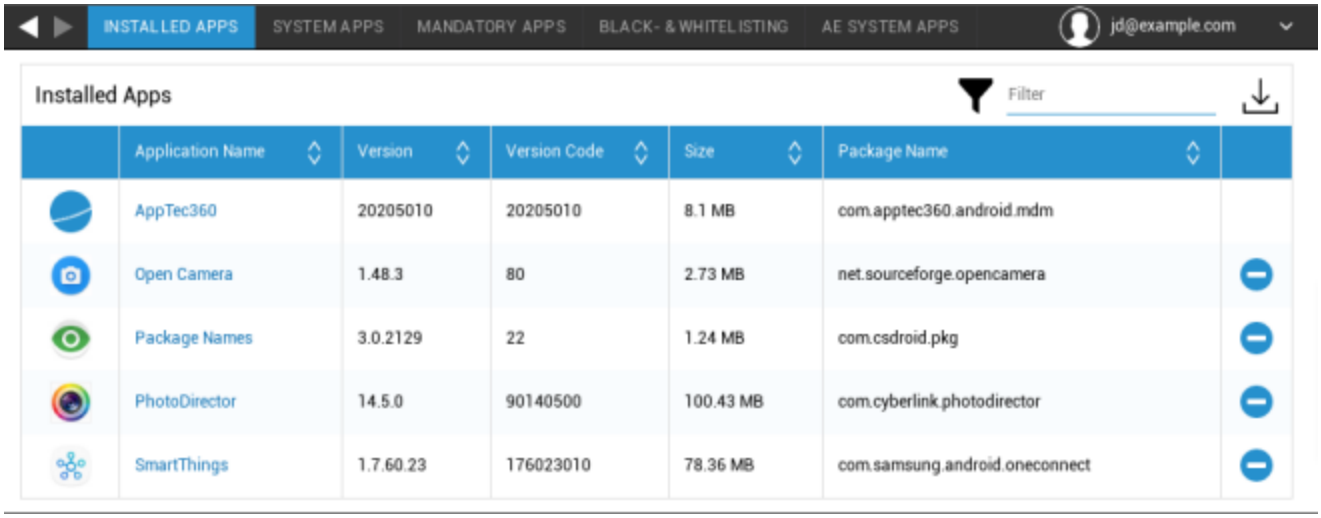
Сертификат клиента	Сертификат клиента. Требуется только в том случае, если Ваш почтовый сервер ожидает его наличия.

Управление приложениями

Enterprise App Manager

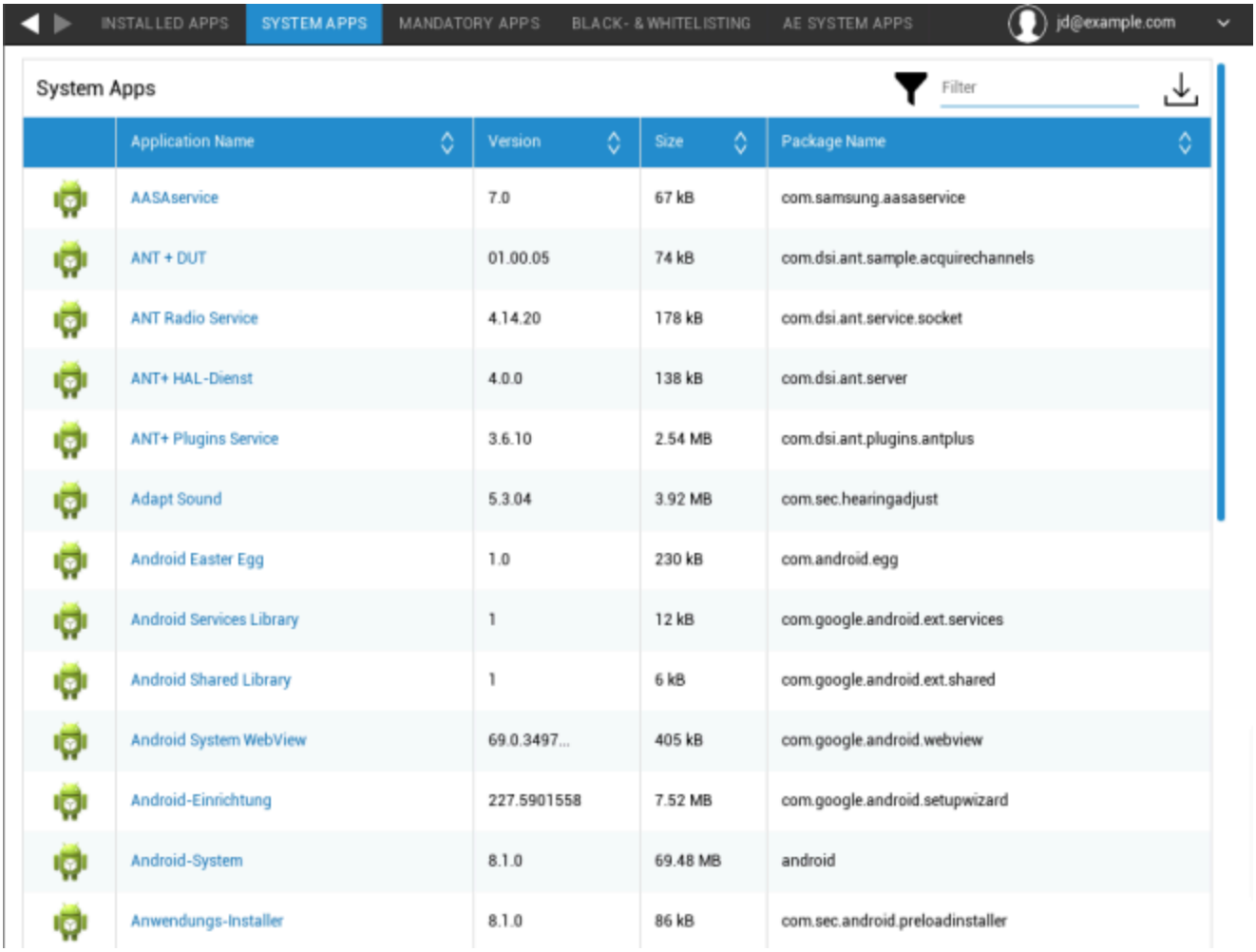
Установленные приложения (только на уровне устройства)

Здесь будут показаны все приложения, которые в данный момент установлены в контейнере.



Системные приложения (только на уровне устройства)

В разделе "Системные приложения" будут перечислены все приложения и службы, которые уже были установлены на устройство конечного пользователя производителем Вашего устройства.

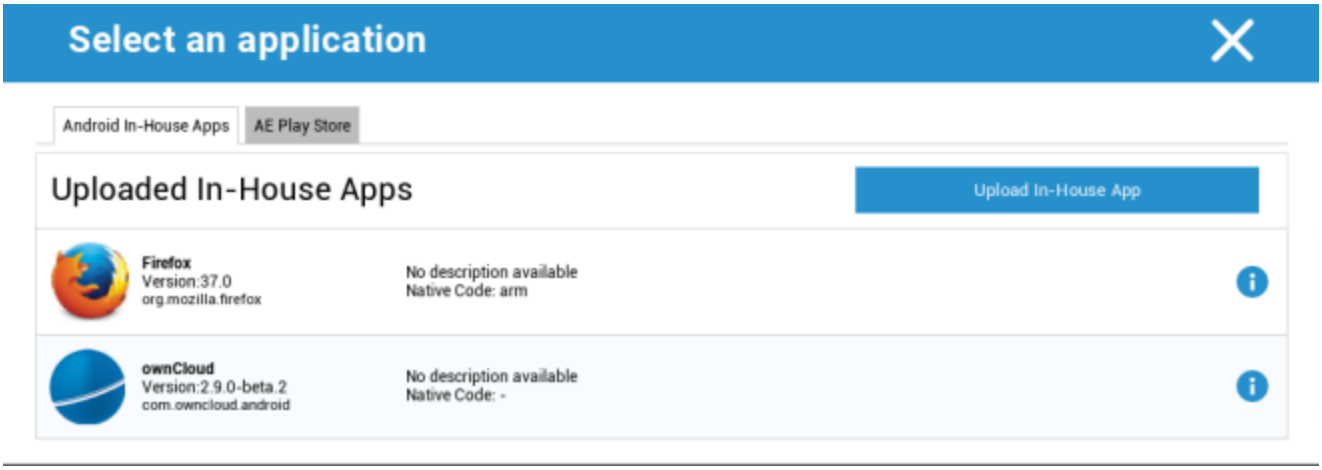


Обязательные приложения

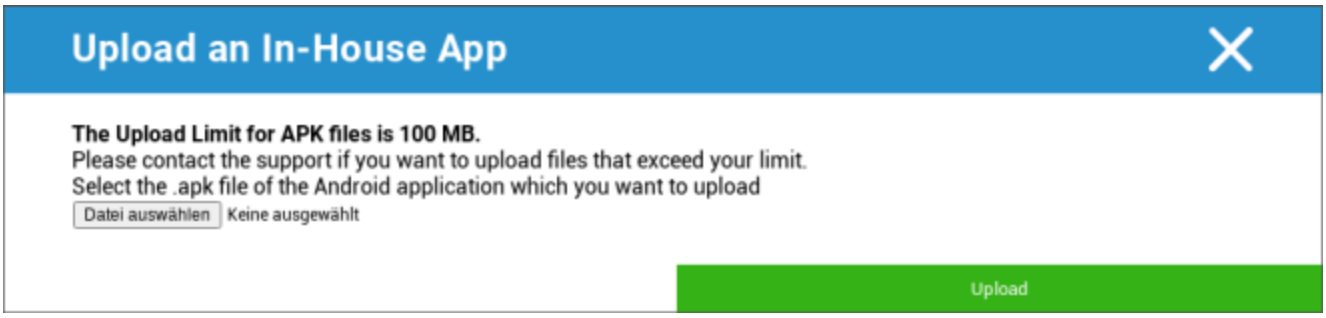
В разделе Обязательные приложения Вы можете установить обязательные приложения. Пользователю будет постоянно предложено установить это приложение, если это приложение InHouse. Приложения из Play Store будут установлены автоматически.

С помощью , можно определить обязательное приложение.

Это может быть внутреннее приложение из списка "Внутренние приложения Android", который Вы загрузили в Общие настройки.

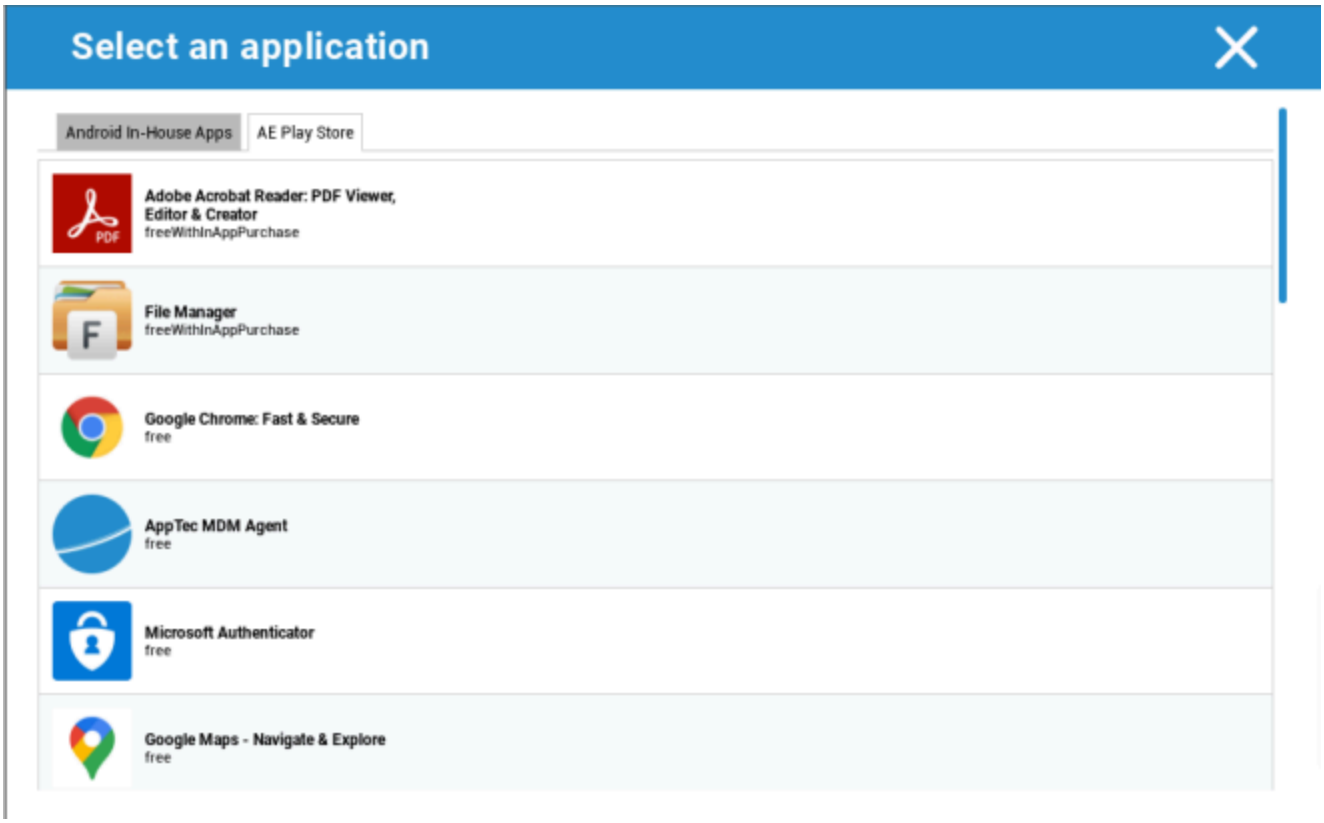


Вы также можете напрямую выбрать и загрузить apk-файл с помощью функции "Upload In-House App".



Если Вы устанавливаете приложение In-House App, у Вас будет возможность активировать функцию "Keep up to date". Если эта функция активирована, и Вы определили более новую версию в In-House App DB, приложение будет обновлено на устройстве.

Или это может быть приложение "AE Play Store" из Google Work Play Store.



На этой вкладке будут отображаться только одобренные приложения "AE Play Store Apps".

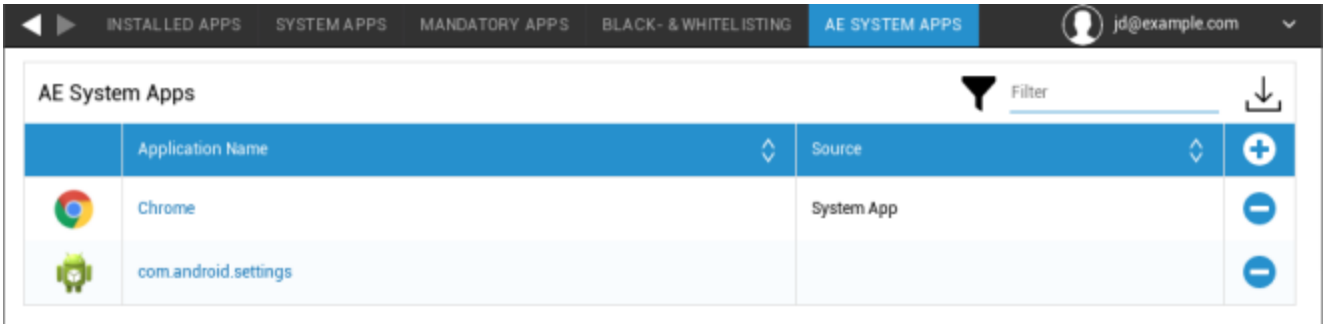
Чтобы одобрить приложение "AE Play Store App", перейдите в раздел "Общие настройки" > "Управление приложениями" > "AE Play

Магазин" и добавьте приложение с помощью кнопки, которая перенаправит Вас на вкладку "Play Store Apps" (или Вы можете перейти непосредственно на вкладку "Play Store Apps").

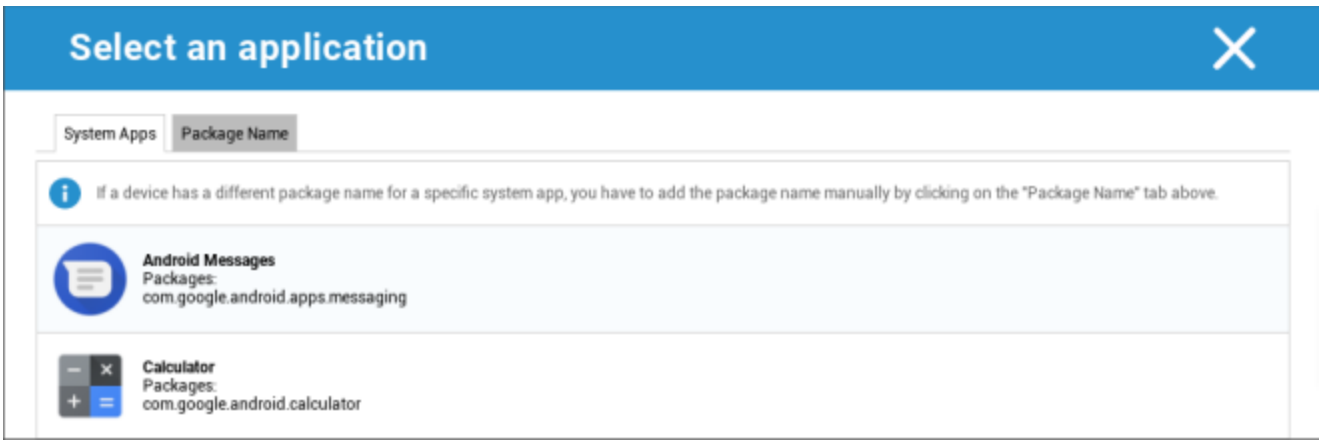
На вкладке "Play Store Apps" Вы можете искать приложения. Когда Вы нажимаете на приложение, открывается страница приложения, и здесь Вы можете одобрить приложение, нажав на кнопку "Одобрить".

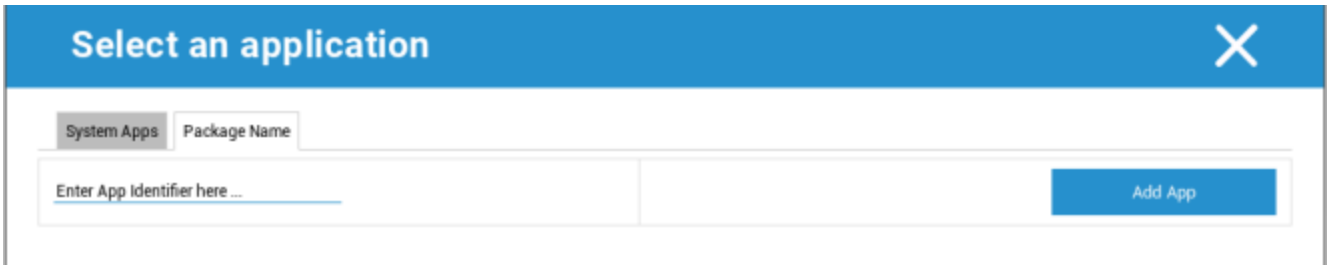
Системные приложения AE

Здесь Вы можете определить список, содержащий определенные системные приложения, которые должны быть активированы на устройствах.



Если Вы нажмете на кнопку, Вы можете выбрать из списка возможных системных приложений, предоставленного Google, или напрямую ввести название пакета системного приложения, которое необходимо активировать.





Имейте в виду, что системные приложения в списке, предоставленном Google, - это только те приложения, которые могут быть системными, но не обязательно должны быть системными на Ваших устройствах.

Однако этот список затрагивает только те приложения, которые уже предустановлены.

Добавление приложений, которые не были предварительно установлены на Ваших устройствах, не повлияет на работу устройств, независимо от того, будет ли это приложение из списка, предоставленного Google, или название пакета приложения будет введено напрямую.

Ограничения и настройки

Настройки управления приложениями

Здесь Вы можете настроить поведение устройства в отношении обновлений приложений.

Частота проверки обновлений	Укажите, через какой промежуток времени AppTec Client будет искать обновления приложений. Значение по умолчанию - 24 часа.
Порог Wi-Fi	Приложения, размер которых превышает указанный, будут загружаться по Wi-Fi. Если выбрано "Только Wi-Fi", все приложения будут загружаться через Wi-Fi.

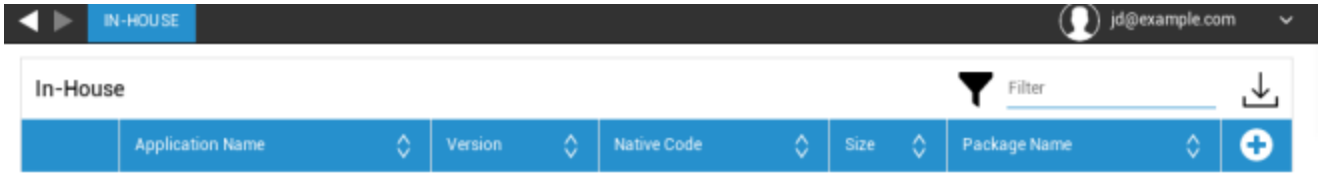
Магазин приложений для предприятий

In-House

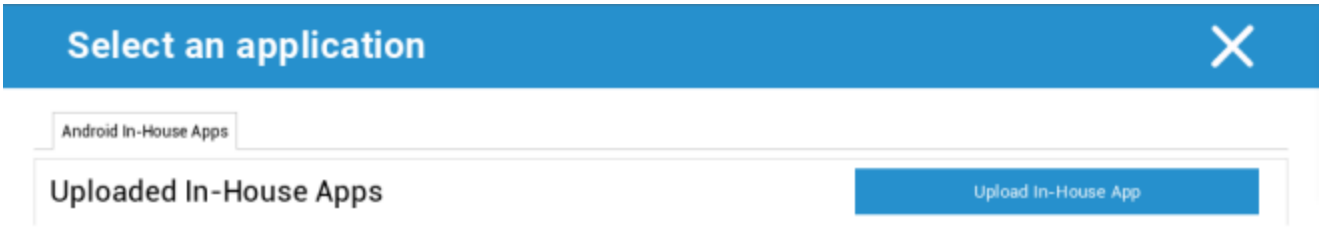
В пункте "In-House" Вы можете загружать и распространять приложения, разработанные внутри компании.

С помощью символа Вы можете распространять дополнительные приложения In-House Apps.

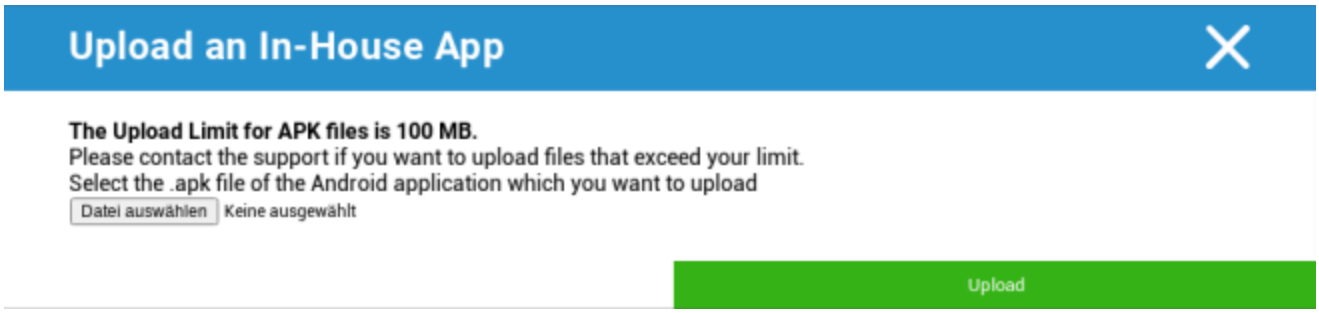
Если Вы устанавливаете приложение In-House App, у Вас будет возможность активировать функцию "Keep up to date". Если эта функция активирована, и Вы определили более новую версию в In-House App DB, приложение будет обновлено на устройстве.



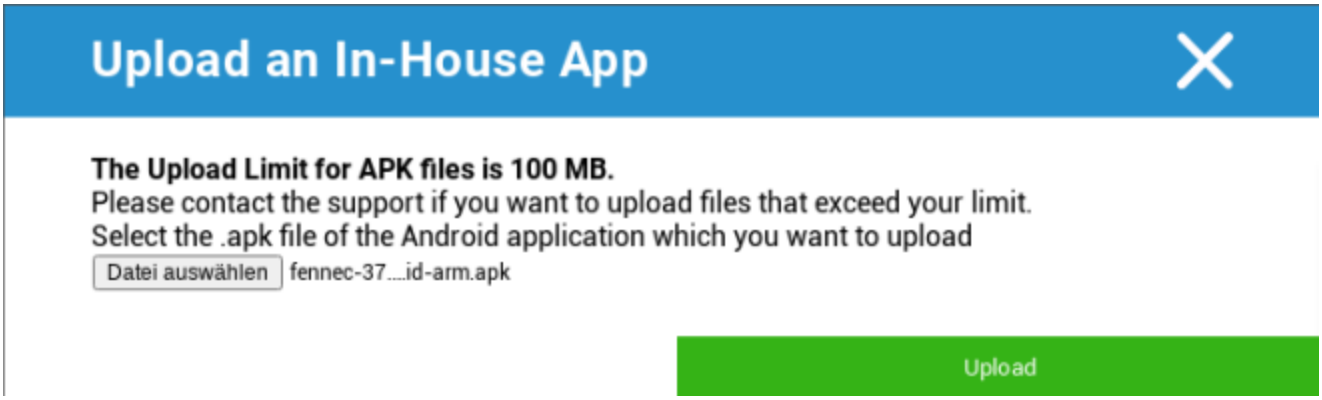
Если Вы не занимались распространением In-House Apps, Вы получите следующий обзор:



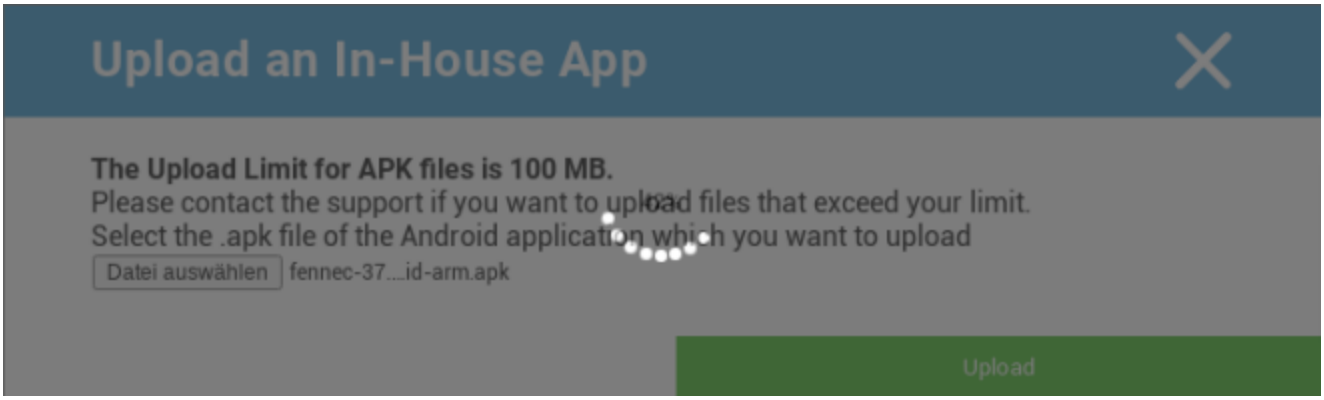
Для этого нажмите на "Upload In-House App", после чего Вы получите следующий обзор:



Теперь выберите с помощью "Search... "файл .apk, а затем нажмите "Upload".



Теперь Ваше приложение будет загружено, в центре круга Вы увидите процентный индикатор, показывающий, какая часть Вашего приложения уже загружена.



Если загрузка Вашего приложения In-House App прошла успешно, Вы сможете найти его в Вашем каталоге приложений.

Теперь у пользователя есть возможность увидеть и установить это приложение в AppTec Store на устройстве конечного пользователя в категории "In-House".

Благодаря тому, что это не приложение Google PlayStore, пользователю не нужен сохраненный Google ID на его соответствующем конечном устройстве.

Enterprise Play Store

AE Play Store

Здесь Вы можете добавить приложения в Android Enterprise Playstore. Обратите внимание, что перед добавлением приложений Вы должны одобрить их с помощью учетной записи администратора AE.

Чтобы одобрить приложение, пожалуйста, ознакомьтесь с инструкциями в разделе Обязательные приложения.

Управление контентом

ContentBox

Здесь Вы можете активировать ContentBox.

Как только Вы переключите "Enable ContentBox" на "On", отдельное приложение ContentBox будет автоматически установлено на устройство конечного пользователя.

Безопасный браузер

Здесь Вы можете настроить параметры AppTec Secure Browser.

Как только Вы переключите раздел "Безопасный браузер" в положение "Вкл.", на устройство конечного пользователя будет автоматически установлено отдельное приложение для браузера.

Требуется пароль	Требуйте, чтобы пользователь установил и использовал пароль для доступа к браузеру.
Минимальная требуемая длина пароля	Установите необходимое количество символов для пароля
Требуемое качество пароля	Установите необходимое качество пароля
Ограничить загрузку / Открыть в	
Ограничение загрузки	
Загрузите белый список	Список URL-адресов, для которых всегда будет разрешена загрузка.
Разрешить копирование	Позволяет копировать, вырезать или делиться текстом внутри веб-страниц.
Разрешить захват экрана	Позволяет делать скриншоты.
Частота очистки данных	Выберите, с какой периодичностью должны автоматически удаляться ВСЕ пользовательские данные (история, кэш и т.д.).
Закладки компании	Закладки появятся в папке "Закладки компании" в закладках браузера. Они не редактируются пользователем.
Скрыть адресную строку	
Белые списки в браузере (без Universal Gateway)	Включает "белые списки" URL на стороне клиента. • Закладки компании всегда в белом списке • Поддерживается только для 100 URL-адресов • Пожалуйста, используйте Универсальный шлюз для неограниченного использования черных и белых списков.
URL-адреса, внесенные в белый список	Список разрешенных URL-адресов.

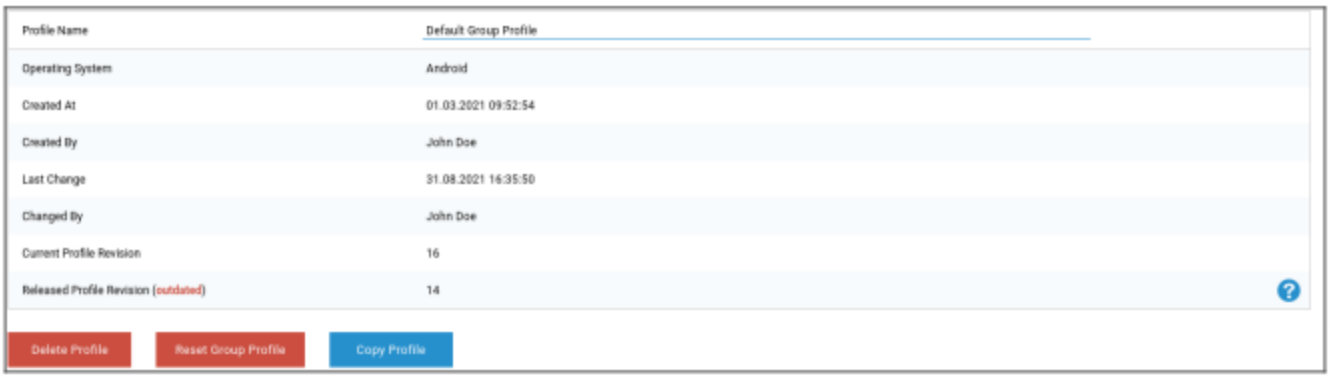
Черные и белые списки на основе шлюза	К черному списку предъявляются следующие требования: • Работающий Универсальный шлюз AppTec ("Общие настройки" → "Универсальный шлюз") • Рабочая конфигурация VPN с указанным DNS-сервером ("Общие настройки" → "Универсальный шлюз" → "Настройки VPN") • Конфигурация черного списка ("Общие настройки" → "Универсальный шлюз" → "Черный список доменов") • Действующее VPN-соединение в профиле ("Управление соединениями" → "VPN")

Конфигурация Android

Общие сведения

Обзор профиля группы (только на уровне группы)

Открыв профиль группы, Вы получите краткий обзор профиля.



Имя профиля	Название профиля (может быть изменено здесь)
Операционная система	Операционная система, для которой предназначен профиль
Создано в	Время создания
Created By	Создатель профиля
Последнее изменение	Время последнего изменения профиля
Изменено	Учетная запись, которая внесла последние изменения
Текущий пересмотр профиля	Пересмотр сохраненного состояния профиля
Выпущенный пересмотр профиля	Назначенная ревизия профиля ("Назначить сейчас"). Если за текстом на ярлыке отображается "(устаревший)", это означает, что Вы сохранили профиль, но еще не назначили его, поэтому устройства все еще будут получать старую версию.

Обзор устройства (только на уровне устройства)

Если Вы находитесь на устройстве, Вы получите обзорную информацию о выбранном устройстве, в которой содержится следующее:

Имя устройства	Имя устройства
Последнее известное местонахождение	Последние известные GPS-координаты
Номер телефона	Номер телефона
Назначение Обязательные приложения	Количество назначенных обязательных приложений
Версия ОС	Версия ОС устройства
Операционная система	Операционная система (Android / iOS / Windows Phone)
Серийный номер	Серийный номер устройства
Владение устройством	Корпоративное или личное устройство
Тип устройства	Телефон или планшет
Rooted	Статус, указывающий, было ли устройство рутировано
Соответствующий	Соответствие рекомендациям
IP-адрес	IP-адрес
Последний раз видели	Точка во времени, когда устройство в последний раз подключалось к AppTec
Последний рывок	Точка во времени, когда сервер отправил push на устройство
Назначение пользователя	Выпадающий список для назначения устройства другому пользователю

Пересмотр конфигурации (только на уровне устройства)

Здесь Вы получите обзор того, какой групповой профиль назначен устройству.

Если Вы нажмете на профиль группы, Вы получите прямой доступ к нему и сможете выполнить настройки.

С помощью этого символа Вы можете вернуть назначенные приложения к настройкам группового профиля.

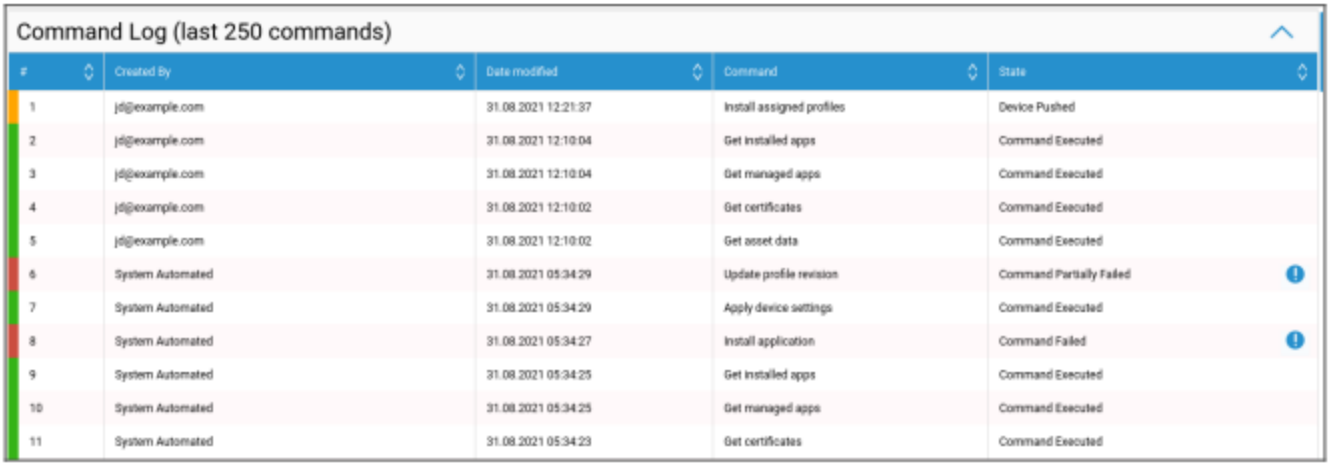
С помощью этого символа Вы можете сбросить профиль устройства, чтобы он вообще не имел никаких настроек.

"Доступна более новая редакция" означает, что профиль группы был изменен и сохранен, но не назначен. Чтобы применить изменения к устройствам, групповой профиль должен быть назначен с помощью "Назначить сейчас" на уровне группы.

Журнал устройства (только на уровне устройства)

Журнал команд

Здесь Вы можете увидеть, какие команды были отданы устройству и каков их статус.



Команды, созданные с помощью "System Automated", автоматически создаются системой.

Возможные статусы команд

Устройство нажимается	Запрос push был отправлен в службу push (например, APNS), чтобы сообщить устройству о необходимости подключиться обратно к серверу EMM.
Команда Создана	Команда была создана в системе.
Команда отправлена	Команда была отправлена на устройство после того, как оно подключилось к серверу.
Команда выполнена	Команда была успешно выполнена.
Команда не выполнена	Команда завершилась неудачно. *
Команда частично не выполнена	В зависимости от ОС устройства некоторые команды могут быть сгруппированы вместе. В этом случае некоторые части этой группы команд оказались неудачными. *
Команда выполнена, в итоге - отказ	Команда была выполнена, но, возможно, она не была выполнена.
Command Repushed	Команда была повторно запущена пользователем.
Выброшенные	Команда была отменена. Например, потому что она была заменена другой командой или устройство было перерегистрировано, и старые команды были удалены.

*Если за сообщением стоит восклицательный знак, Вы можете получить дополнительную информацию, наведя курсор на значок.

Настройки устройства

Конфигурация клиента

Здесь Вы можете выполнить следующие настройки Вашего устройства Android:

Предупреждающее сообщение после отключения управления устройствами	Установленное предупреждение после отключения управления устройствами
Время несоблюдения	Ограничение по времени, по истечении которого будет выполнено "Действие по принуждению после соответствия", если устройство не соответствует требованиям. Мин. 1 минута Макс. 24 часа
Принудительные действия после истечения времени выполнения	Действия, которые необходимо предпринять, как только устройство становится несоответствующим требованиям. • Ничего не делать = не действовать • Устройство блокировки = устройство блокировки • Wipe Device = устройство будет восстановлено до заводских настроек
Частота сбора данных	Частота сбора информации об устройстве/GPS
Частота сердцебиения устройства	Интервал, через который устройство должно связаться с сервером AppTec360 Server Мин. 1 минута Макс. 24 часа
Включите обновление местоположения	Если активирована, устройство отправляет обновления местоположения на сервер AppTec360 Server
Расположение Время обновления	Определяет, через какие временные интервалы устройство отправляет обновления местоположения в AppTec
Используйте точность определения местоположения Google для обновления местоположения	Если эта настройка активирована, то для обновления местоположения будет использоваться функция Google Location Accuracy (ранее известная как сетевое местоположение) (если она была отключена в разделе "Ограничения", то эта настройка ни на что не повлияет)

Используйте GPS для обновления местоположения	Если активировано, GPS будет использоваться для обновления местоположения
Разрешить имитацию (подделку) местоположения	Позволяет подделывать информацию о местоположении с помощью сторонних приложений
Действие при потере соединения	Позволяет Вам задать определенное действие, которое будет выполнено после определенного количества неудачных ударов сердца.
Режим внедрения политики	Определяет, насколько агрессивно AppTec360 Client просит пользователя выполнить определенные действия, требующие его ввода. Интервал (по умолчанию) = спрашивать через определенные промежутки времени, чтобы пользователь мог на некоторое время оставить это занятие в фоновом режиме. Нет оповещения = нет всплывающего окна для требуемого действия. Вам придется открыть AppTec360 Client вручную, чтобы проверить, есть ли требуемое действие. Постоянное оповещение = Пользователь может выполнять только необходимые действия. Клиент AppTec360 будет принудительно выводиться на передний план, если пользователь попытается этого избежать
AppTec360 Блокировка версий	Позволяет определить версию AppTec360 Client, которая является максимальной версией, до которой обновляется клиент.

Обои

Здесь Вы можете задать пользовательские обои.

"Specify a Color" позволяет Вам задать цвет в шестнадцатеричном формате (например, #000000). Допускаются только шестнадцатеричные значения.

"Установить изображение в качестве обоев" позволяет Вам загрузить изображение. Пожалуйста, имейте в виду, что разные устройства с разными пусковыми установками и версиями ОС работают по-разному. Общего руководства по размеру и соотношению сторон не существует, поскольку это зависит от устройства.

Используйте JPG (или JPEG) или PNG для формата файла.

Управление активами (только на уровне устройств)

Управление активами

Информация об устройстве

Модель	**Обозначение модели устройства**
Операционная система	OS
Версия ОС	Версия ОС
Поддержка AE	Поддержка Android Enterprise (контейнерная и полностью управляемая)
Серийный номер	Серийный номер
Имя устройства	Имя устройства
Состояние батареи	Состояние батареи
Свободная / общая память	Свободная / общая память
Samsung KNOX	Уровень API Samsung KNOX
Доступна карта памяти SD	Доступна карта SD
Эмулированная SD-карта	Эмулированная SD-карта
Съемная SD-карта	Съемная SD-карта
Свободная / общая память SD	Свободная память SD / Общая память SD-карты

Wi-Fi

IP-адрес	IP-адрес устройства
WiFi MAC	MAC-адрес WiFi

Клетчатка

Статус	Состояние (SIM-карта установлена)
Номер телефона	Номер телефона
Роуминг (голос / данные)	Роуминг для голоса / данных
Статус роуминга	Текущий статус роуминга
IP-адрес	IP-адрес
Оператор/ перевозчик	Оператор/перевозчик
Клеточные технологии	Клеточные технологии
IMEI	Номер IMEI
ICCID	Это идентификатор SIM-карты, часто также называемой Smartcard или Integrated Circuit Card (ICC).
IMSI	Международный идентификатор мобильного абонента (IMSI) обеспечивает в GSM- и UMTS-мобильных сетях однозначную идентификацию пользователей сети. IMSI состоит максимум из 15 цифр и настраивается следующим образом: • Код страны мобильного телефона (MCC), 3 цифры • Код мобильной сети (MNC), 2 или 3 цифры • Идентификационный номер мобильного абонента (MSIN), 1-10 цифр
Текущий MCC/MNC	См. раздел "SIM MCC/MNC".
SIM MCC/MNC	Код страны мобильной связи - это установленный идентификатор страны, установленный МСЭ в соответствии со стандартом E.212. Он работает в сочетании с кодом мобильной сети (MNC) для идентификации мобильной сети. Означает код страны/мобильной сети SIM-карты. Если Вы переходите в другую мобильную сеть, то, по логике вещей, "Current MCC/MNC" и "SIM MCC/MNC" будут разными.

Bluetooth

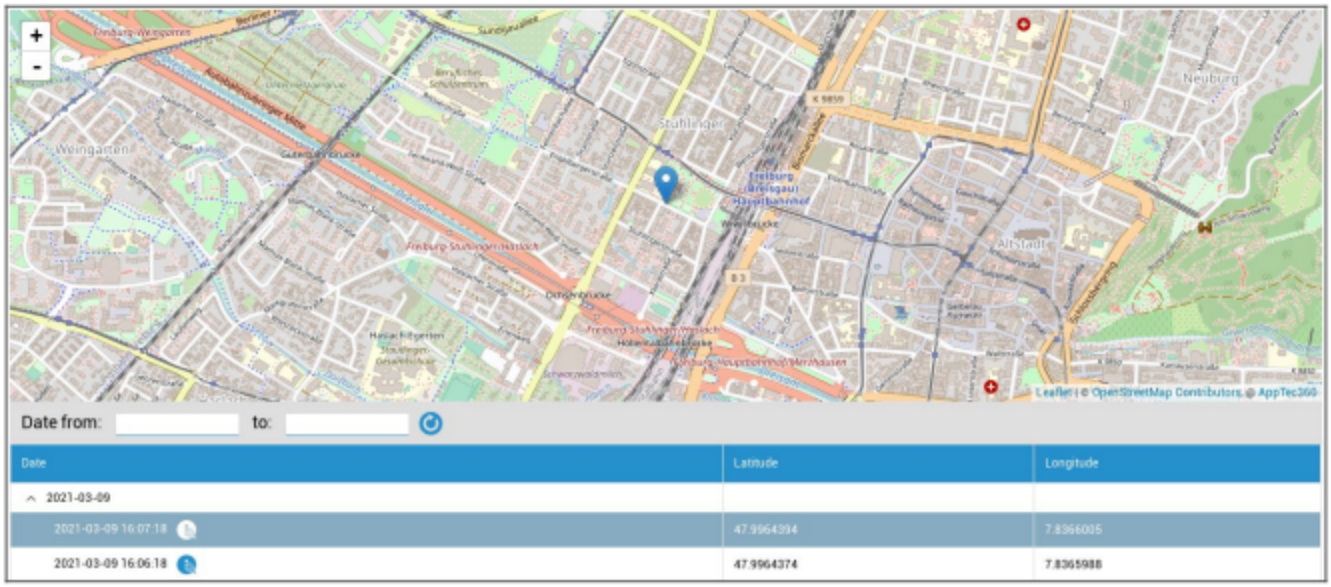
Bluetooth MAC	MAC-адрес Bluetooth

Управление безопасностью

Защита от кражи (только на уровне устройства)

Информация GPS (только на уровне устройства)

Здесь Вы можете установить текущее/последнее местоположение устройства. Локализация может быть защищена одним или даже двумя паролями - См: Общие настройки - Конфиденциальность - Доступ к GPS



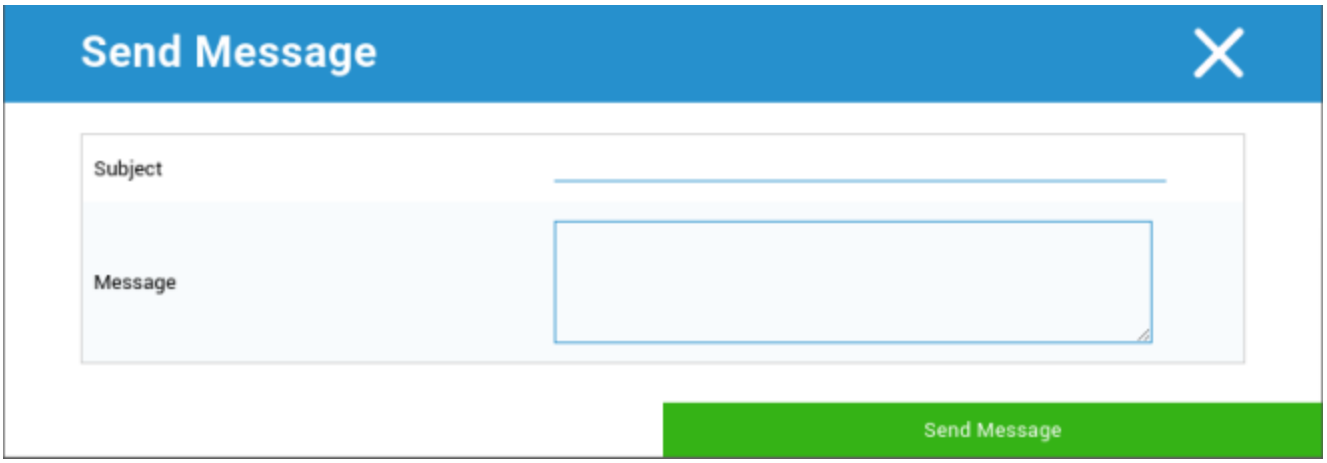
Wipe & Lock (только на уровне устройства)

В разделе "Wipe & Lock" Вы можете выполнить следующие три действия:

Полное вытирание	Устройство возвращается к заводским настройкам (корпоративные, а также личные данные удаляются)
Enterprise Wipe	С устройства конечного пользователя удаляются только корпоративные данные (все приложения, данные и т.д., которые были предоставлены AppTec360).
Экран блокировки	Активирована блокировка экрана, достаточно разблокировать устройство с помощью пароля устройства/PIN-кода

Сообщение (только на уровне устройства)

Вы можете заполнить тему и сообщение и отправить его на устройство конечного пользователя. Это сообщение будет отображено в AppTec360 Client.



Конфигурация безопасности

Passcode

В разделе "Пароль" Вы можете задать пароль устройства, Вам доступны следующие опции настройки

Минимальная длина пароля	Устанавливает минимальное количество символов, которое должно быть в пароле
Качество пароля	Стойкость пароля Неопределенный = не определенный Все пароли в порядке = все пароли приемлемы хотя бы числовые символы = должен содержать хотя бы числовые символы не менее сложных символов = должен содержать не менее специальных символов не менее буквенно-цифровых символов = должен содержать не менее буквенно-цифровых символов не менее алфавитных символов = должен содержать не менее алфавитных символов
Максимальная блокировка времени бездействия	Максимальный тайм-аут экрана. Здесь настраивается только максимальное значение, которое может быть выбрано пользователем
Минимальное количество строчных букв в пароле	Минимальное количество строчных букв в пароле
Минимальное количество заглавных букв в пароле	Минимальное количество заглавных букв в пароле
Минимальное количество небуквенных символов, необходимых для пароля	Минимальное количество небуквенных символов, необходимых для пароля
Минимальное количество цифр в пароле	Минимальное количество цифр в пароле
Минимальное количество символов в пароле	Минимальное количество символов в пароле
Таймаут истечения срока действия пароля	Устанавливает, через какой промежуток времени срок действия пароля истекает, и необходимо выдать новый пароль
Ограничение истории паролей	Количество ранее использованных паролей, которые не разрешены
Максимальное количество неудачных попыток ввода пароля	Устанавливает, как часто пароль может быть введен неверно, прежде чем будет произведено полное стирание устройства

Шифрование

В этом пункте Вы можете зашифровать внутреннюю память устройства, а также память SD-карты.

Требуйте шифрования хранилища	Если эта настройка активирована, память устройства будет зашифрована, если устройство поддерживает эту функцию. После того, как память устройства была зашифрована в первый раз, ее уже невозможно не зашифровать. Аналогичным образом, политика паролей будет автоматически переключена на 6 буквенно-цифровых символов
Требуется шифрование SD-карты	Эта настройка применима только к устройствам Samsung! Если эта настройка активирована, внешняя SD-карта может быть зашифрована и может быть разшифрована только вручную на устройстве конечного пользователя. Аналогичным образом, политика паролей будет автоматически переключена на 6 буквенно-цифровых символов

Антивирус

Включение Антивируса установит Ikarus на устройства. Пожалуйста, имейте в виду, что для этого требуется отдельная лицензия, которую можно ввести в разделе Общие настройки → Управление приложениями → Сторонние приложения.

Автоматическое сканирование	Определяет, будет ли Ikarus выполнять автоматическое сканирование и как часто оно будет выполняться. Если включить "Полное автоматическое сканирование", будет выполнено полное сканирование. В противном случае будет выполнено быстрое сканирование
Автоматические обновления	Включите автоматическое обновление вирусной базы данных и установите, как часто это происходит.
Защита приложений	Включает сканирование приложений в дополнение к обычному сканированию, которое сканирует только файлы.
Защита SD-карты	Включает защиту SD-карты. Без этого сканирование ограничивается локальным хранилищем.
Обновление только через Wi-Fi	Ограничение обновления до Wi-Fi

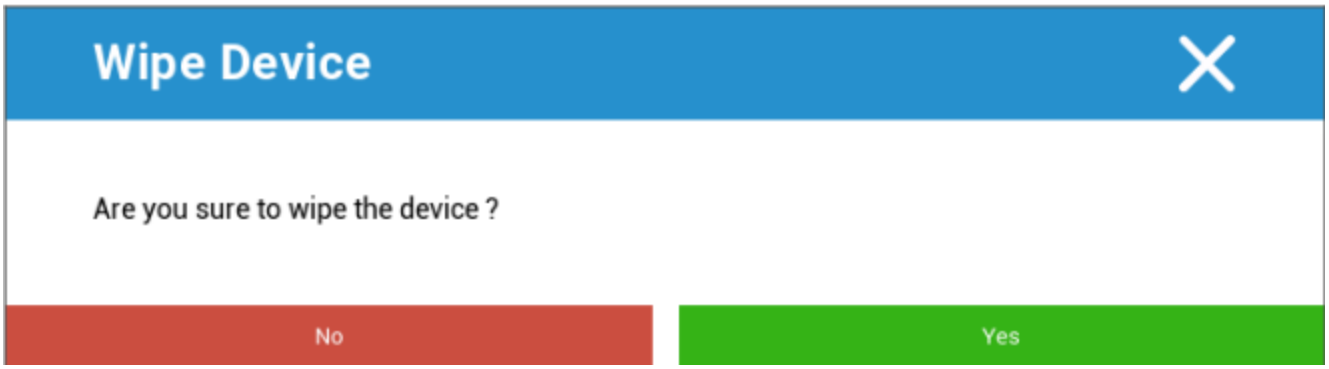
Окончание срока службы (только на уровне устройства)

Стирание (только на уровне устройства)

В разделе "Wipe" Вы можете восстановить заводские настройки устройства. При этом корпоративные, а также личные данные будут удалены с устройства конечного пользователя.

При нажатии на "Символ минуса" Вы должны получить следующее сообщение

Затереть SD-карту тоже?	Память SD-карты также будет удалена



Ответив "Да", Вы можете выполнить стирание.

В разделе "Отчет о стирании" отображаются следующие пункты

Стерто	История о том, кто выполнял протирание
Дата	Дата
Статус	Статус (например, успешно ли выполнено стирание)

Настройки ограничений

Ограничения

Здесь можно ограничить и заблокировать множество вещей.

Включить камеру	Разрешите использовать фотоаппарат
Принудительная автоматическая синхронизация	Относится к интерфейсу "Sync". Вкл = синхронизация постоянно активирована Выкл = синхронизация постоянно отключена Выбор пользователя = выбранный пользователем
Force Bluetooth	Вкл = Bluetooth постоянно активирован Выкл = Bluetooth постоянно отключен Выбор пользователя = выбранный пользователем
Force GPS	Вкл = GPS постоянно активирован Выкл = GPS постоянно отключен Выбор пользователя = выбранный пользователем
Принудительная точность определения местоположения Google	Вкл = Постоянная интернет-локализация Выкл = Постоянная деактивация интернет-локализации Выбор пользователя = выбранный пользователем

Для устройств Samsung с интерфейсом KNOX 1.0 или выше доступны следующие опции настройки.

Разрешить SD-карту	Разрешить SD-карту
Разрешить запись на SD-карту	Разрешите "запись" на SD-карту
Разрешить захват экрана	Разрешить захват экрана
Разрешить буфер обмена	Разрешить буфер обмена
Резервное копирование настроек и данных приложений в Google Cloud	Выкл = деактивировать резервное копирование Google Вкл = активировать резервное копирование Google Выбор пользователя = выбирается пользователем
Разрешить отладку по USB	Разрешить отладку USB (используется, например, для создания журналов устройств (ADB))
Разрешить Google Crash Report	Разрешите отправлять Google Crash Report из приложений
Разрешить сброс к заводским настройкам	Позволяет пользователю восстановить заводские настройки устройства
Разрешить OTA-обновление	Разрешите обновления "по воздуху"
Разрешить хранение данных на USB-хосте	Если активировать эту функцию, можно подключить USB-накопитель в виде HD-накопителя или устройства для чтения SD-карт.
Разрешить USB-медиаплеер (MTP,PTP)	Разрешить USB-медиаплеер (MTP,PTP)
Разрешить микрофон	Вкл = разрешить микрофон для сторонних приложений Выкл = блокировать микрофон для сторонних приложений Выбор пользователя = пользователи могут выбирать, если стороннее приложение имеет доступ к микрофону
Разрешить NFC (связь ближнего поля)	Разрешить NFC
Разрешить неизвестные источники (боковая загрузка APK)	Если включено, то разрешена боковая загрузка приложений (APK-файлов). Если эта настройка отключена, пользователю придется включить ее вручную, когда Вы разрешите установку APK из неизвестных источников.
Разрешить создание пользователей	Позволяет создавать несколько пользователей

Владелец устройства AE

(Устройство должно находиться в режиме владельца устройства Android Enterprise)
Рекомендуется создавать устройства как устройства "Android Enterprise", а не как устройства "Android".

Безопасность	
Запретить совместное использование местоположения	Указывает, запрещено ли пользователю включать совместное использование местоположения.
Запретить безопасную загрузку	Указывает, запрещено ли пользователю перезагружать устройство в безопасный режим загрузки.
Запретить сетевой сброс	Указывает, запрещено ли пользователю сбрасывать сетевые настройки из Настроек.
Запретить сброс к заводским настройкам	Указывает, запрещено ли пользователю сбрасывать устройство.
Включите ADB	Позволяет подключаться к ПК через ADB
Отключите охрану ключей	Отключает охрану ключей
Информация о владельце устройства на запорном экране	Устанавливает информацию о владельце устройства, которая будет отображаться на экране блокировки.
Обеспечение соответствия	Режим Prompt User - Пользователю будет предложено выполнить необходимые действия. Контейнер блокировки режима - скройте все приложения, пока не будут выполнены все требования

Управление приложениями	
Разрешите межпрофильные ссылки на приложения	Позволяет приложениям в родительском профиле обрабатывать веб-ссылки из управляемого профиля.
Запретить управление приложениями	Определяет, запрещено ли пользователю изменять приложения в Настройках или пусковых установках.
Запретить установку приложений	Указывает, запрещено ли пользователю устанавливать приложения.
Запретить удаление приложений	Указывает, запрещено ли пользователю удалять приложения.
Политика разрешений во время выполнения	Определяет, как будут обрабатываться новые запросы на разрешение от приложений.

Разрешить неизвестные источники	Если эта функция включена, пользователи могут загружать приложения с боковой стороны, устанавливая файл .apk.

Возможность подключения	
Запретить настройку мобильной сети	Указывает, запрещено ли пользователю настраивать мобильные сети.
Настройка запрета привязки	Указывает, запрещено ли пользователю настраивать Tethering & portable hotspots.
Запретить настройку VPN	Указывает, запрещено ли пользователю настраивать VPN.
Запретить настройку Wifi	Указывает, запрещено ли пользователю менять точки доступа WiFi.
Запретить исходящий луч NFC	Указывает, запрещено ли пользователю использовать NFC для передачи данных из приложений.
Блокировка конфигурации WiFi	Этот параметр определяет, должны ли конфигурации WiFi, созданные приложением владельца устройства, быть заблокированы (то есть, редактироваться или удаляться только приложением владельца устройства, даже не приложением Settings).
Включить роуминг данных	Активирует роуминг данных

Bluetooth	
Запретить Bluetooth	Указывает, запрещен ли bluetooth на устройстве. Требуется Android 8.0
Запретите совместный доступ к Bluetooth	Указывает, запрещен ли на устройстве исходящий совместный доступ по bluetooth. Требуется Android 8.0
Запретить настройку Bluetooth	Указывает, запрещено ли пользователю настраивать bluetooth.

Управление счетами	
Запретите добавление управляемого профиля	Указывает, запрещено ли пользователю добавлять управляемые профили. Требуется Android 8.0
Запретить добавление пользователей	Указывает, запрещено ли пользователю добавлять новых пользователей.
Запретить удаление управляемого профиля	Указывает, могут ли управляемые профили этого пользователя быть удалены, кроме как владельцем профиля. Требуется Android 8.0
Запретить изменение учетной записи	Определяет, запрещено ли пользователю добавлять и удалять учетные записи, если они не были добавлены Authenticator программно.

Телефония	
Запрет исходящих вызовов	Указывает, что пользователю запрещено совершать исходящие телефонные звонки.
Запретить SMS	Указывает, что пользователю не разрешено отправлять или получать SMS-сообщения.

Система	
Запретить создание окон	Указывает, что окна, кроме окон приложений, не должны создаваться.
Запретить установку значка пользователя	Указывает, запрещено ли пользователю менять свой значок.
Запретить установку обоев	Ограничение пользователя, запрещающее устанавливать обои.
Отключите строку состояния	Отключение строки состояния блокирует уведомления, быстрые настройки и другие экранные накладки, которые позволяют уйти от одноразового использования устройства.
Включить автоматическое время	Установите время автоматически.
Включить автоматический часовой пояс	Установите часовой пояс автоматически.

Остается включенным в розетку	Устройство будет оставаться активным, пока подключено к источнику питания.

Хранение	
Запретите отключать проверку приложений	Указывает, запрещено ли пользователю отключать проверку приложений.
Запретить монтировать физические носители	Указывает, запрещено ли пользователю монтировать физические внешние носители.
Включите службу резервного копирования	Служба резервного копирования управляет всеми механизмами резервного копирования и восстановления на устройстве. Если установить значение false, резервное копирование или восстановление данных будет запрещено. По умолчанию служба резервного копирования отключена. Требуется Android 8.0
Включите USB-накопитель	Включает использование USB Mass Storage.

Клавиатура	
Запретить автозаполнение	Указывает, запрещено ли пользователю использовать службы автозаполнения. Требуется Android 8.0
Запретите копирование и вставку между профилями	Указывает, можно ли скопированное в буфер обмена этого профиля вставить в соседние профили.

Звук	
Запретить корректировку объема	Указывает, запрещено ли пользователю регулировать основную громкость.
Запретить отключение микрофона	Указывает, запрещено ли пользователю регулировать громкость микрофона.
Выключите устройство	Отключите звук.

Политика обновления системы

Контролируйте обновления ОС	Включите эту опцию, чтобы установить автоматическое, оконное или отложенное обновление.

Контейнер для BYOD

Android Enterprise

Android Enterprise

Включите Android Enterprise	Включите Android Enterprise (AE). AE поддерживается начиная с версии Android 5.1 и выше.
Обеспечение соответствия	Режим Prompt User - Пользователю будет предложено выполнить необходимые действия. Контейнер блокировки режима - скройте все приложения, пока не будут выполнены все требования
Политика разрешений во время выполнения	Предложите пользователю запросить новые разрешения Всегда удовлетворяйте новые запросы на разрешение Всегда отклоняйте новые запросы на разрешение Внимание: У некоторых приложений возникают проблемы с распознаванием разрешений, если они установлены автоматически. Если Вы всегда предоставляете разрешения и сталкиваетесь с проблемами, когда приложения говорят, что разрешения отсутствуют, установите значение "подсказать пользователю" и переустановите приложение.
Разрешить исходящий буфер обмена	Позволяет копировать и вставлять из внутреннего контейнера во внешний
Разрешить разрешение идентификатора вызывающего абонента	Показывает имя для входящего вызова на основе контактов в контейнере
Разрешить разрешение поиска контактов	Позволяет искать имена в контактах контейнера при совершении звонков
Разрешите обмен контактами через Bluetooth	Позволяет получить доступ к контакту контейнера в автомобиле
Запретить исходящий луч NFC	Отключение NFC для контейнера
Разрешить неизвестные источники	Если эта функция включена, пользователи могут загружать приложения с боковой стороны, устанавливая файл .apk.

Разрешить отладку по USB	Если эта опция включена, пользователи могут включить отладку по USB.
Запретить изменение учетной записи	Запрещает создание, удаление и изменение учетных записей в контейнере Имейте в виду, что некоторым приложениям необходимо создать или изменить учетные записи, чтобы они работали как положено.

Gmail Exchange

Позволяет Вам настроить Gmail в контейнере. Имейте в виду, что включение этой конфигурации не приводит к автоматической установке приложения. Вам все равно придется добавить это приложение в качестве обязательного.

Адрес электронной почты	Адрес электронной почты
Имя хоста сервера	Имя хоста сервера
Имя пользователя	Имя пользователя
Подпись	Подпись
Количество предыдущих дней для синхронизации	Количество предыдущих дней для синхронизации.
Идентификатор устройства	Идентификатор EAS. Оставьте этот параметр пустым, если в Вашей среде он не требуется
Используйте Secure Sockets Layer (SSL)	Включает использование SSL. Отключение этой опции может снизить уровень безопасности
Принимайте все сертификаты	Принимает все сертификаты. Включение этой опции может снизить уровень безопасности
Разрешить неуправляемые учетные записи	Позволяет пользователю добавлять дополнительные учетные записи
Сертификат клиента	Загрузите сертификат клиента, если Ваш сервер Exchange требует этого

Системные приложения AE

Здесь Вы можете включить системные приложения для контейнера Android Enterprise Container. Имейте в виду, что указанное приложение должно находиться в системном хранилище, иначе ничего не произойдет.

Пасскод контейнера

Только для Android 7.0 или выше

Позволяет Вам установить особое требование к паролю для контейнера.

Минимальная длина пароля	Устанавливает минимальное количество символов, которое должно быть в пароле
Качество пароля	Стойкость пароля Неопределенный = не определенный Все пароли в порядке = все пароли приемлемы хотя бы числовые символы = должен содержать хотя бы числовые символы не менее сложных символов = должен содержать не менее специальных символов не менее буквенно-цифровых символов = должен содержать не менее буквенно-цифровых символов не менее алфавитных символов = должен содержать не менее алфавитных символов
Максимальная блокировка времени бездействия	Максимальное время, пока контейнер не будет заперт. Здесь настраивается только максимальное значение, которое может быть выбрано пользователем
Минимальное количество строчных букв в пароле	Минимальное количество строчных букв в пароле
Минимальное количество заглавных букв в пароле	Минимальное количество заглавных букв в пароле
Минимальное количество небуквенных символов, необходимых для пароля	Минимальное количество небуквенных символов, необходимых для пароля
Минимальное количество цифр в пароле	Минимальное количество цифр в пароле
Минимальное количество символов в пароле	Минимальное количество символов в пароле
Таймаут истечения срока действия пароля	Устанавливает, через какой промежуток времени срок действия пароля истекает, и необходимо выдать новый пароль
Ограничение истории паролей	Количество ранее использованных паролей, которые не разрешены
Максимальное количество неудачных попыток ввода пароля	Устанавливает, как часто пароль может быть введен неправильно, прежде чем контейнер будет удален

Samsung KNOX

Активация

Здесь Вы можете включить контейнер Samsung KNOX. Пожалуйста, имейте в виду, что он больше не поддерживается компанией Samsung на Android 10 и выше. Использование контейнера Android Enterprise Container на Android 10 или выше

Пасс-код Knox

Установите рекомендации по настройке пароля устройства

Минимальная длина пароля	Устанавливает, сколько символов должно быть в пароле.
Качество пароля	Стойкость пароля Каждый пароль в порядке = Каждый пароль в порядке Минимум цифровых символов = Минимум цифровых символов должен присутствовать Не менее сложных символов = Должны присутствовать минимальные специальные символы Минимум буквенно-цифровых символов = Минимум буквенно-цифровых символов должно присутствовать Минимум буквенных символов = Должно присутствовать минимум буквенных символов
Требуется минимум сложных символов	Должны присутствовать минимальные сложные символы
Максимальное время бездействия	Максимальное время бездействия пользователя, до блокировки клавиатуры
Разрешить аутентификацию по отпечаткам пальцев	Разрешите аутентификацию по отпечатку пальца
Разрешить аутентификацию по радужной оболочке глаза	Разрешите аутентификацию с помощью распознавания радужной оболочки глаза
Максимальный возраст пароля	Устанавливает, через какое время срок действия пароля истекает и необходимо выдать новый пароль
История сохраненных паролей	Количество прежних паролей, которые не разрешены
Максимальное количество неудачных попыток ввода пароля	Устанавливает, как часто пароль может быть введен неверно, прежде чем произойдет полное стирание устройства

Knox Security

Ограничьте определенные функциональные возможности устройства

Включить камеру	Разрешите использовать фотоаппарат
Разрешите Samsung KNOX App Store	Разрешите использовать магазин приложений Samsung KNOX App Store
Разрешить Службы Google Play	Разрешить Службы Google Play
Разрешить браузер	Разрешите использовать родной браузер
Разрешить скриншоты	Разрешите создавать скриншоты
Разрешить импорт контактов	Если активировано, разрешен доступ к контактам устройства из контейнера KNOX
Разрешить экспорт контактов	Если активировано, доступ к контактам KNOX с устройства разрешен
Разрешить импорт календаря	Если активировано, то разрешен доступ к календарю устройства из контейнера KNOX.
Разрешить экспорт календаря	Если он активирован, доступ к календарю KNOX с устройства разрешен
Разрешить небезопасную клавиатуру	Разрешите использовать небезопасную клавиатуру
Включить импорт файлов	Включите импорт файлов в контейнер KNOX
Включить экспорт файлов	Включите экспорт файлов из контейнера KNOX

Knox Exchange

Здесь Вы можете настроить профиль Exchange-Profile для контейнера KNOX.

Адрес электронной почты	Адрес электронной почты пользователя Обратите внимание на "Placeholders", которые Вы можете использовать для работы с учетными данными и не выполнять изменения вручную на каждом устройстве Щелкнув на **Show Placeholders**, Вы можете отобразить их для себя
Имя хоста сервера	Адрес сервера Ваших серверов Exchange
Имя пользователя	Имя входа в систему для соответствующего устройства конечного пользователя, пожалуйста, также обратите внимание на "Placeholders" здесь
Домен	Доменный адрес
Пароль (только на уровне устройства)	В качестве опции индивидуальному устройству может быть предоставлен пароль, если он останется пустым, пользователю будет предложено ввести свой пароль Exchange.
Количество предыдущих дней для синхронизации	Количество дней, определяющее, когда электронная почта будет синхронизирована обратно
Подпись	Можно прикрепить подпись
Счет по умолчанию	Устанавливает, что эта учетная запись электронной почты является стандартной учетной записью
Используйте Secure Sockets Layer (SSL)	Используйте SSL-соединение
Используйте защиту транспортного уровня (TLS)	Используйте TLS-соединение
Принимайте все сертификаты	Все сертификаты принимаются. Пожалуйста, выберите эту опцию, если Ваш Exchange Server использует самоподписанный сертификат

Knox eMail

Адрес электронной почты	Адрес электронной почты пользователя Обратите внимание на "Placeholders", которые Вы можете использовать для работы с учетными данными и не выполнять изменения вручную на каждом устройстве Щелкнув на **Show Placeholders**, Вы можете отобразить их для себя
Протокол входящего сервера	Протокол входящего сервера IMAP или POP
Адрес входящего сервера	Адрес входящего сервера
Порт входящего сервера	Порт входящего сервера
Логин/имя пользователя входящего сервера	Логин/имя пользователя входящего сервера
Пароль входящего сервера	Пароль входящего сервера
Входящий сервер использует SSL	Входящий сервер использует SSL
Входящий сервер использует TLS	Входящий сервер использует TLS
Входящий сервер принимает все сертификаты	Входящий сервер принимает все типы сертификатов
Протокол исходящего сервера	Протокол исходящего сервера SMTP
Порт исходящего сервера	Порт исходящего сервера
Исходящий сервер использует дополнительные учетные данные	Дополнительные учетные данные для исходящего сервера. Если это значение установлено в "off", то будут использоваться настройки входящего сервера
Логин/имя пользователя исходящего сервера	Логин/имя пользователя исходящего сервера
Пароль исходящего сервера	Пароль исходящего сервера
Исходящий сервер использует SSL	Исходящий сервер использует SSL
Исходящий сервер использует TLS	Исходящий сервер использует TLS
Исходящий сервер принимает все сертификаты	Исходящий сервер принимает все типы сертификатов

Подпись	Здесь можно прикрепить подпись
Уведомление пользователя о получении новой электронной почты	Уведомление пользователя о получении новой электронной почты

Knox Apps

Создайте здесь приложения, которые Вы хотите распространить на устройствах конечных пользователей. Затем они будут доступны в KNOX-контейнере. Чтобы добавить приложение, действуйте, как в меню Обязательные приложения

Имя приложения	Имя приложения
Обязательно с тех пор, как	Момент времени, когда приложение было добавлено
Источник	Источник приложения (Play Store | In-House)

Нажав на символ, можно снова удалить соответствующее приложение.

Управление соединениями

Wifi

Для этой настройки выполните предварительную конфигурацию устройств конечных пользователей для доступа к внутренним точкам доступа

Идентификатор набора услуг (SSID)	SSID для подключаемой сети
Скрытая сеть	Активировать, в случае если точка доступа не передает SSID
Тип безопасности	Установите тип безопасности точки доступа

Тип безопасности

WEP

Пароль	Пароль для точки доступа

WPA/WPA2

Пароль	Пароль для точки доступа

802.1x EAP

EAP-метод	

PWD	Идентичность	Идентичность
	Пароль	Пароль

PEAP	Протокол аутентификации Фазы 2	нет	Никакого дополнительного протокола
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертификат CA	Сертификат ЦС	
	Идентичность	Идентичность	
	Анонимная личность	Анонимная личность	
	Пароль	Пароль	

EAP-метод	

TTLS	Протокол аутентификации Фазы 2	нет	Никакого дополнительного протокола
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол GTC
	Сертификат CA	Сертификат ЦС	
	Идентичность	Идентичность	
	Анонимная личность	Анонимная личность	
	Пароль	Пароль	

TLS	Сертификат CA	Сертификат ЦС
	Идентичность	Идентичность
	Пароль	Пароль

VPN

Тип соединения	Установите тип VPN-соединения

Если Вы выберете "Per-App VPN" в качестве типа VPN, доступные VPN-клиенты изменятся. Per-App VPN ограничивает VPN определенными приложениями и автоматически запускает VPN-соединение при запуске определенного приложения.

AppTec360 VPN Client	Использование AppTec360 VPN Client в сочетании с универсальным шлюзом
Имя соединения	Имя VPN-соединения
Конфигурация шлюза	Выберите Конфигурация VPN универсального шлюза
Всегда на VPN	Заставляет VPN быть всегда активным, поэтому весь трафик проходит через VPN.
Включить нативную блокировку	Блокируйте все сетевые соединения, когда устройство не подключено к VPN. Используйте этот параметр с осторожностью, поскольку при неправильной настройке он может привести к полной потере соединения. Только для Android Enterprise на Android 7 или выше
Включите блокировку AppTec360	Блокируйте использование всех приложений до тех пор, пока не будет запущено VPN-соединение

Cisco AnyConnect	
Имя соединения	Имя VPN-соединения
Сервер	Адрес сервера
Режим сертификата	Disabled = деактивировано Автоматический = автоматический

L2TP (только KNOX)	Доступно только на устройствах Samsung
Имя соединения	Имя соединения
Сервер	Адрес сервера
Включить секрет L2TP	
DNS Поиск доменов	DNS поиск доменов

Тип соединения	**Установите тип VPN-соединения**

PPTP (только KNOX)	Доступно только на устройствах Samsung
Имя соединения	Имя VPN-соединения
Сервер	Адрес сервера
Включить шифрование	Включите шифрование
DNS Поиск доменов	DNS поиск доменов

L2TP / IPSec PSK (только KNOX)	Доступно только на устройствах Samsung
Имя соединения	Имя VPN-соединения
Сервер	Адрес сервера
IPSec Pre-Shared Key	Предварительный ключ для аутентификации
Включить секрет L2TP	
L2TP Secret	
DNS Поиск доменов	DNS поиск доменов

IPSec XAuth PSK (только KNOX)	Доступно только на устройствах Samsung
Имя соединения	Имя VPN-соединения
Сервер	Адрес сервера
Идентификатор IPSec	Имя пользователя для подключения
IPSec Pre-Shared Key	Пароль для подключения
DNS Поиск доменов	DNS поиск доменов

OpenVPN	
Имя соединения	Имя соединения

Профиль OpenVPN	Вот куда будет скопировано содержимое файла .ovpn
Приложение OpenVPN	Существует два различных приложения для использования OpenVPN Мы рекомендуем приложение "OpenVPN for Android". Но в качестве альтернативы можно использовать приложение "OpenVPN Connect".

Ограничения

Здесь Вы можете установить ограничения, связанные с управлением соединениями.

Разрешить роуминг данных	Разрешите передачу мобильных данных в роуминге
Принудительный роуминг данных	Если эта функция активирована, роуминг для мобильных данных будет постоянно включен (не рекомендуется!). Эта настройка заменяет настройку "Разрешить роуминг данных"!
Следующие настройки доступны только на Samsung KNOX 2.0 или выше	
Разрешить только экстренные вызовы	Разрешить только экстренные вызовы
Разрешить WiFi	Разрешить WiFi
Минимальный уровень безопасности сети WiFi	Минимальный уровень безопасности сети WiFi Открыто = разрешены все типы WiFi
Запретите пользователю добавлять сети WiFi	Пользователь не может самостоятельно добавить сеть WiFi Эта настройка возможна только в том случае, если профиль WiFi был определен в разделе "Управление подключением".
Разрешить SMS и MMS	Все = Весь SMS и MMS трафик разрешен Incoming SMS Only = Разрешены только входящие SMS-сообщения Только исходящие SMS = Разрешены только исходящие SMS-сообщения Нет = Трафик SMS / MMS не разрешен
Разрешить синхронизацию во время роуминга	Разрешить синхронизацию во время роуминга Вкл = активировано Выключено = деактивировано Выбор пользователя = выбор пользователя
Разрешить голосовой роуминг	Разрешить голосовой роуминг Вкл = активировано Выключено = деактивировано Выбор пользователя = выбор пользователя
Используйте системный http-прокси-сервер	Использование HTTP-прокси-сервера, которое предусмотрено настройками системы в разделе "Настройки", зависит от подключенной сети (WiFi или APN).

APN

Следующие настройки доступны только на Samsung SAFE 2.0 или выше!

Отображаемое имя APN	Отображаемое имя APN	
Имя точки доступа	Имя APN	
Протокол исходящего сервера	Не установлено	
	Нет	
	PAP	Протокол PAP
	CHAP	Протокол CHAP
	PAP или CHAP	Либо протокол PAP, либо протокол CHAP
MCC - Код страны мобильного телефона	Здесь вводится MCC, оставьте это поле пустым, если следует использовать MCC вставленной SIM-карты.	
MNC - код мобильной сети	Здесь вводится MNC, оставьте это поле пустым, если следует использовать MCC установленной SIM-карты.	
Адрес сервера	Адрес сервера	
Номер порта сервера	Номер порта сервера	
Адрес прокси-сервера	Адрес прокси-сервера	
Адрес MMS-сервера	Адрес MMS-сервера, для Стандартного оставьте пустым	
Номер порта MMS	Номер порта MMS	
Адрес MMS-прокси	Адрес MMS-прокси	
Имя пользователя	Имя пользователя	
Пароль	Пароль	
Тип точки доступа	Разрешенными типами являются: "default", "mms", "supl". Если это поле оставить пустым, то будут использоваться "default,supl,mms".	
Предпочтительный APN	APN предпочтительнее	

Bluetooth

Здесь можно выполнить различные настройки Bluetooth.

Следующие настройки доступны только на Samsung KNOX 1.0 или выше!

Разрешите обнаружение устройства через Bluetooth	Разрешите обнаружение устройства через Bluetooth
Разрешить сопряжение с Bluetooth	Разрешите сопряжение с Bluetooth
Разрешить устройства с Bluetooth-гарнитурой	Разрешить устройства с Bluetooth-гарнитурой
Разрешите устройства громкой связи Bluetooth	Разрешите устройства громкой связи Bluetooth
Разрешите устройства Bluetooth A2DP	Разрешите потоковую передачу звука Bluetooth A2DP между устройствами
Разрешить исходящие вызовы	Разрешите исходящие звонки через BT
Разрешите передачу данных через Bluetooth	Разрешите передачу данных через Bluetooth
Разрешите Bluetooth Tethering	Позволяет использовать устройство в качестве модема (подключение к Интернету через Bluetooth)
Разрешите подключение к компьютеру через Bluetooth	Разрешите подключение к компьютеру через Bluetooth

Управление PIM

Обмен

Доступно только для Samsung KNOX 1.0 или выше!

Адрес электронной почты	Адрес электронной почты пользователя Обратите внимание на "Placeholders", которые Вы можете использовать для работы с учетными данными и не выполнять изменения вручную на каждом устройстве Щелкнув на **Show Placeholders**, Вы можете отобразить их для себя
Имя хоста сервера	Адрес сервера Ваших серверов Exchange
Имя пользователя	Имя входа в систему для соответствующего устройства конечного пользователя, пожалуйста, также обратите внимание на "Placeholders here
Домен	Доменный адрес
Пароль (только на уровне устройства)	По желанию, индивидуальному устройству может быть предоставлен пароль, если он останется пустым, пользователю будет предложено ввести свой пароль Exchange.
Количество предыдущих дней для синхронизации	Количество дней, определяющее, когда электронная почта будет синхронизирована обратно
Подпись	Можно прикрепить подпись (Подсказка: некоторые устройства требуют HTML-форматирования подписи)
Счет по умолчанию	Устанавливает, что эта почтовая учетная запись является стандартной учетной записью
Используйте Secure Sockets Layer (SSL)	Используйте SSL-соединение
Используйте защиту транспортного уровня (TLS)	Используйте TLS-соединение
Принимайте все сертификаты	Все сертификаты принимаются. Пожалуйста, выберите эту опцию, если Ваш Exchange Server использует самоподписанный сертификат

eMail

Здесь Вы можете распределить учетные записи IMAP и POP по соответствующим устройствам конечных пользователей.

Следующие настройки доступны только на Samsung KNOX 1.0 или выше!		
Адрес электронной почты	Адрес электронной почты пользователя Обратите внимание на "Placeholders", которые Вы можете использовать для работы с учетными данными и не выполнять изменения вручную на каждом устройстве Щелкнув на **Show Placeholders**, Вы можете отобразить их для себя	
Протокол входящего сервера	Протокол входящего сервера	IMAP или POP
Адрес входящего сервера	Адрес входящего сервера	
Порт входящего сервера	Порт входящего сервера	
Логин/имя пользователя входящего сервера	Логин/имя пользователя входящего сервера	
Пароль входящего сервера (только на уровне устройства)	Пароль входящего сервера (только на уровне устройства)	
Входящий сервер использует SSL	Входящий сервер использует SSL	
Входящий сервер использует TLS	Входящий сервер использует TLS	
Входящий сервер принимает все сертификаты	Входящий сервер принимает все типы сертификатов	
Протокол исходящего сервера	Протокол исходящего сервера	SMTP
Порт исходящего сервера	Порт исходящего сервера	
Исходящий сервер использует дополнительные учетные данные	Дополнительные учетные данные для исходящего сервера. Если установить значение "off", то будут использоваться настройки входящего сервера	
Логин/имя пользователя исходящего сервера	Логин/имя пользователя исходящего сервера	
Пароль исходящего сервера (только на уровне устройства)	Пароль исходящего сервера	

Исходящий сервер использует SSL	Исходящий сервер использует SSL
Исходящий сервер использует TLS	Исходящий сервер использует TLS
Исходящий сервер принимает все сертификаты	Исходящий сервер принимает все типы сертификатов
Подпись	Подпись можно прикрепить здесь (Подсказка: некоторые устройства требуют HTML-форматирования подписи)
Уведомление пользователя о получении новой электронной почты	Уведомляет пользователя о получении нового письма

AE Gmail Exchange

Информация: Эта настройка будет применена к приложению Gmail. Поэтому Вам необходимо одобрить и установить Gmail.

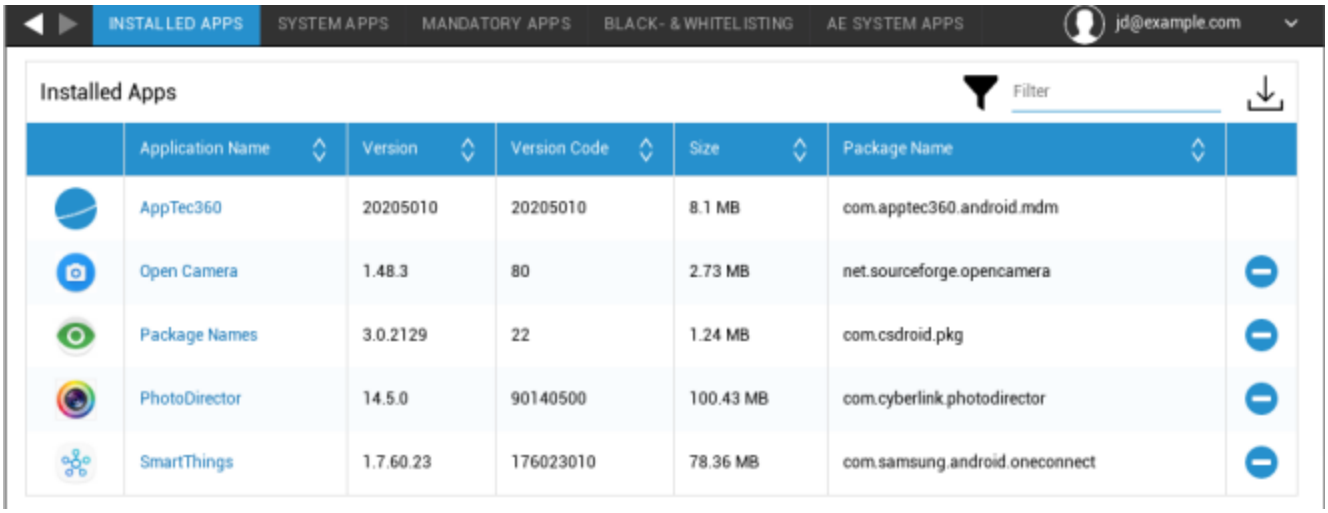
Адрес электронной почты	Адрес электронной почты пользователя Обратите внимание на "Placeholders", которые Вы можете использовать для работы с учетными данными и не выполнять изменения вручную на каждом устройстве Щелкнув на Show Placeholders, Вы можете отобразить их для себя
Имя хоста сервера	Адрес сервера Ваших серверов Exchange
Имя пользователя	Имя входа в систему для соответствующего устройства конечного пользователя, пожалуйста, также обратите внимание на "Placeholders here
Подпись	Можно прикрепить подпись (Подсказка: некоторые устройства требуют HTML-форматирования подписи)
Количество предыдущих дней для синхронизации	Количество дней, определяющее, когда электронная почта будет синхронизирована обратно
Идентификатор устройства	Идентификатор EAS. Оставьте этот параметр пустым, если в Вашей среде он не требуется
Используйте Secure Sockets Layer (SSL)	Используйте SSL-соединение
Принимайте все сертификаты	Все сертификаты принимаются. Пожалуйста, выберите эту опцию, если Ваш Exchange Server использует самоподписанный сертификат
Разрешить неуправляемые учетные записи	Позволяет пользователю добавлять дополнительные учетные записи
Сертификат клиента	Загрузите сертификат клиента, если Ваш сервер Exchange требует этого

Управление приложениями

Enterprise App Manager

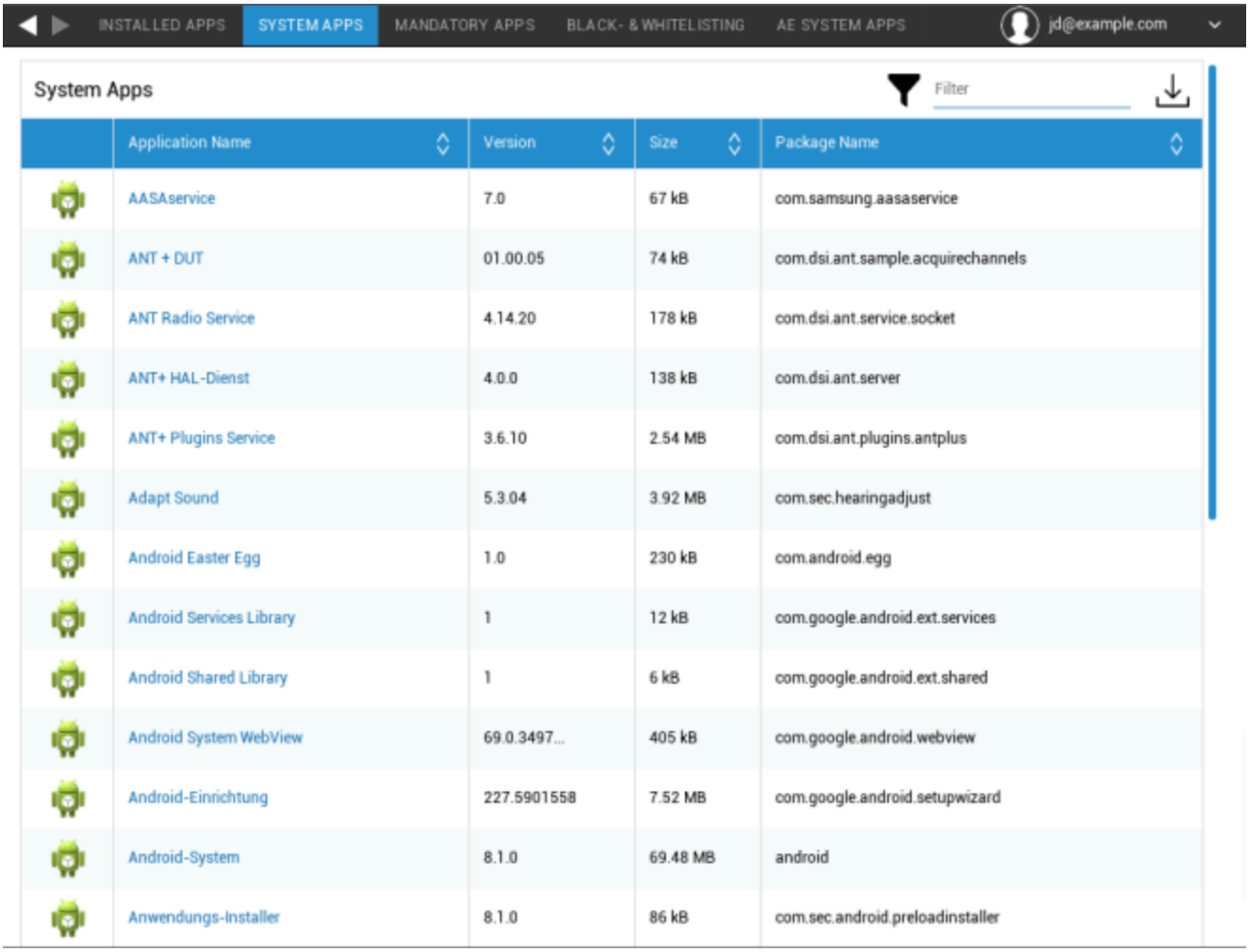
Установленные приложения (только на уровне устройства)

Здесь будут показаны все приложения, которые в данный момент установлены на устройстве конечного пользователя.


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

Системные приложения (только на уровне устройства)

В разделе "Системные приложения" будут перечислены все предустановленные системы с указанием названия и версии пакета.



Обязательные приложения

В разделе Обязательные приложения Вы можете определить, какие приложения должны быть установлены на устройстве. В зависимости от Вашей конфигурации и устройства приложение будет установлено автоматически или пользователю будет предложено установить его.

Пожалуйста, имейте в виду, что для удобства управления приложениями рекомендуется использовать Android Enterprise.

Сценарии приведены ниже:

Обычные приложения Play Store

Установка приложений в Playstore всегда требует вмешательства пользователя. Кроме того, на устройстве должна быть настроена учетная запись Google.

Установка приложений InHouse

На устройствах Samsung эти приложения будут установлены беззвучно. Единственное исключение - контейнер, где пользователь должен подтвердить установку.

В любом другом случае пользователь должен подтвердить установку приложения.

Android Enterprise Play Store Apps

Эти приложения всегда будут устанавливаться бесшумно, без участия пользователя.

Чтобы добавить обязательное приложение, нажмите на "+" и выберите нужное приложение из списка. Пожалуйста, помните, что Вы не сможете установить приложения из вкладки "Google Play Store", если устройство настроено на Android Enterprise как полностью управляемое или как контейнер.

Если Вы используете Android Enterprise, выберите приложения из раздела "AE Play Store". Чтобы приложения были доступны здесь, подтвердите их в магазине Google Enterprise Play, перейдя в Общие настройки → AE Play Store → Play Store Apps.

При удалении обязательного приложения оно также будет деинсталлировано с устройства.

Вы можете нажать на название приложения в списке обязательных приложений и перейти на вкладку "конфигурация", чтобы настроить приложение. Для этого требуется использование Android Enterprise, и приложение должно его поддерживать. Поэтому доступные опции зависят от выбранного приложения.

Системные приложения AE

Здесь Вы можете включить системные приложения для устройств Android Enterprise. Имейте в виду, что указанное приложение должно быть в системном хранилище, иначе ничего не произойдет. 296

Ограничения и настройки

Черные и белые списки

Здесь Вы можете определить черный или белый список. Все приложения из черного списка будут заблокированы. Все приложения, которых нет в белом списке, будут заблокированы. Пустой черный список не блокирует ничего, а пустой белый список блокирует все*.

**Все обязательные приложения и приложения из Enterprise App Store будут внесены в белый список автоматически. Вам не нужно добавлять их вручную*

Нажав на "+", Вы можете либо найти приложение, которое хотите добавить в черный или белый список, либо ввести название пакета вручную.

Ограничения системных приложений

В разделе "Sys App Restrictions" Вы можете, помимо прочего, блокировать предустановленные приложения и службы по своему усмотрению.

Отключить браузер	Отключите стандартный браузер
Отключить календарь	Отключите родной календарь
Отключить калькулятор	Отключите калькулятор
Отключите браузер Chrome	Отключите браузер Chrome
Отключить часы	Отключите часы
Отключить контакты	Отключить контакты
Отключить номеронабиратель	Отключите родной дозвон
Отключить электронную почту	Отключить электронную почту
Отключить обмен	Отключите учетные записи Exchange
Отключите Facebook	Отключите приложение Facebook
Отключить галерею	Отключите родное приложение галереи
Отключите Gmail	Отключите Gmail
Отключите Google Книги	Отключите Google Книги
Отключите Google Play Kiosk	Отключите Google Play Kiosk
Отключите Google Maps	Отключите Google Maps
Отключите Google Музыку	Отключите Google Музыку
Отключите Google Фильмы	Отключите Google Фильмы
Отключите Google Play Store	Отключите Google Play Store (публичный App Store)
Отключите Google Plus	Отключите Google Plus
Отключите поиск Google	Отключите поиск Google
Отключите Google Talk / Google Hangouts	Отключите Google Talk / Google Hangouts
Отключите музыкальный проигрыватель	Отключите родное приложение музыкального плеера
Отключить настройки	Отключите настройки устройства
Отключите Sim Toolkit	Отключите службы Sim Toolkit
Отключить SMS / MMS	Отключите SMS / MMS
Отключите просмотр улиц	Отключите сервисы Street View
Отключите Youtube	Отключите Youtube

Приложения Samsung

В разделе "Samsung Apps" Вы можете задать дополнительные настройки и/или ограничения для устройств Samsung.

Отключите AllShare Play / Samsung Link	Отключите AllShare Play / Samsung Link
Отключите ChatON	Отключите ChatON
Отключите игровой концентратор	Отключите игровой концентратор
Отключите групповую игру	Отключите групповую игру
Отключить помощь	Отключить справку Samsung
Отключите KNOX	Отключите контейнер Samsung KNOX
Отключить памятку	Отключите голосовые заметки
Отключить "Мои файлы	Отключить "Мои файлы
Отключите оптический считыватель	Отключите оптический считыватель
Отключите Polaris Office	Отключите Polaris Office
Отключите Readers Hub / Samsung Books	Отключите Readers Hub / Samsung Books
Отключите функцию S Memo	Отключите приложение Samsung Memo
Отключить S-переводчик	Отключите приложение Переводчик Samsung
Отключите функцию S Voice	Отключите голосовой помощник S Voice
Отключите приложения Samsung	Отключите магазин приложений Samsung App Store
Отключите концентратор Samsung	Отключите развлекательные магазины Samsung
Отключите видеоплеер	Отключите видеоплеер
Отключить диктофон	Отключить диктофон
Отключите WatchON	Отключите WatchON (имитирует пульт дистанционного управления)

Приложения Huawei

В разделе "Huawei Apps" Вы можете задать дополнительные настройки и/или ограничения для устройства Huawei.

Отключите DLNA	Отключите DLNA
Отключите установщик приложений	Отключите установщик приложений
Отключите диспетчер файлов	Отключите диспетчер файлов
Отключите диспетчер резервного копирования	Отключите диспетчер резервного копирования
Отключите программу обновления системы	Отключите программу обновления системы
Отключите панель инструментов	Отключите панель инструментов
Отключить погоду	Отключить погоду
Отключите FM-радио	Отключите FM-радио

Настройки управления приложениями

Здесь Вы можете определить поведение обновлений InHouse Apps.

Частота проверки обновлений определяет, как часто приложение AppTec360 ищет обновления для приложений InHouse. Как только новая версия будет обнаружена, она будет загружена и установлена.

Порог Wi-Fi определяет, следует ли ограничивать загрузку Wi-Fi соединениями, если размер приложения превышает настроенный Вами порог. Если приложение меньше или Вы не задали порог, оно будет загружаться и в Wi-Fi, и в сотовой сети.

Магазин приложений для предприятий

Пожалуйста, имейте в виду, что приложения, добавленные сюда (Enterprise App Store), НЕ будут автоматически установлены на устройство (устройства). Пользователь должен открыть Enterprise App Store на устройстве и установить приложение вручную.

Если Вы хотите автоматически устанавливать приложения на устройство, перейдите в раздел "App Management" → "Enterprise App Manager" → "Mandatory Apps" и добавьте туда нужные приложения.

На этом этапе Вы можете распространять дополнительные приложения среди своих пользователей.

Playstore

Нажмите на "+", чтобы добавить приложение в магазин Play Store. Если Вы используете Android Enterprise, пожалуйста, перейдите в раздел "Управление приложениями Enterprise Play Store". Также имейте в виду, что для установки указанных здесь приложений на → устройстве должна быть настроена учетная запись Google.

In-House

В пункте "In-House" Вы можете загружать и распространять приложения, разработанные внутри компании.

Нажмите на "+", чтобы добавить приложение InHouse в магазин корпоративных приложений, которое затем может быть установлено пользователем. В этом диалоге Вы также можете загрузить новое приложение InHouse.

Enterprise Play Store

Пожалуйста, имейте в виду, что приложения, добавленные сюда (Enterprise Play Store), НЕ будут автоматически установлены на устройство (устройства). Пользователю придется открыть Play Store на устройстве и установить приложение вручную.

Если Вы хотите автоматически устанавливать приложения на устройство, перейдите в раздел "App Management" → "Enterprise App Manager" → "Mandatory Apps" и добавьте туда нужные приложения.

На этом этапе Вы можете распространять дополнительные приложения среди своих пользователей.

Здесь Вы можете добавлять приложения в Android Enterprise Playstore. Обратите внимание, что Вы должны одобрить приложения в разделе Общие настройки → AE Play Store → Play Store

Apps. Эти приложения будут добавлены в обычный Google Play Store.

Также имейте в виду, что сначала Вам нужно определить макет с приложениями в разделе Общие настройки → Управление приложениями → AE Play Store → Макет магазина.

Приложения должны быть в Layout, прежде чем Вы сможете успешно добавить их в магазин.

Режим киоска и пусковая установка

Режим киоска

Режим киоска позволяет Вам предварительно определить приложение или URL. После этого можно будет запускать/посещать только это приложение или URL.

Аналогично, различные аппаратные кнопки могут быть отключены в различных режимах Kiosk Mode.

Автоматический старт	Автоматический запуск режима киоска, как только профиль достигнет конечного пользовательского устройства
Режим киоска по расписанию?	Вы можете запланировать время для режима киоска, который будет автоматически начинаться и заканчиваться в установленное Вами время.
Время начала	Время начала
Время в минутах	Время в минутах, по истечении которого режим киоска должен снова завершиться

Тип применения

Одно приложение	Если Вы хотите запустить приложение в режиме киоска, выберите "Пакет" в разделе "Тип приложения".
Применение киосков	Нажмите здесь, чтобы выбрать приложение, которое должно быть запущено в режиме киоска Вы найдете обычный обзор App Management Вы можете выбрать между "Google Play Store", "Android In-House Apps" и "Packagename".

Тип применения

URL	Если Вы хотите запустить URL в режиме киоска, выберите "URL" в разделе "Тип приложения". Затем определите желаемый адрес URL
Очистите браузер после бездействия	Здесь Вы можете задать временной интервал в минутах, по истечении которого режим киоска должен быть перезапущен.
Очистите веб-кэш и файлы cookie	Если Вы активируете эту функцию, то после перезапуска режима киоска веб-кэш (куки и кэшированные изображения) будет удален.
Политика одинакового происхождения	Если эта функция активна, то пользователь может просматривать только подстраницы определенного URL. Например, Вы определили следующий URL:www.mypage.com Затем пользователь может перейти на сайт: www.mypage.com/subpage.
URL-адреса, внесенные в белый список	Здесь Вы можете создать белый список, в котором все эти URL будут разрешены Не более 1 URL в строке URL должен начинаться с http:/ или https://.
URL-адреса, занесенные в черный список	Здесь Вы можете вести Черный список, в котором все эти URL будут запрещены. Не более 1 URL в строке URL должен начинаться с http:/ или https://.
Ориентация экрана	Эта настройка относится к настройкам экрана Автоматический = автоматический Портрет = вертикальный формат Пейзаж = ландшафтный режим

Мультиприложение	Если Вы выбрали режим киоска "Multi App", использование AppTec360 Launcher будет обязательным.
Приложения	Приложение: Выберите Playstore или собственное приложение в качестве приложения для киоска. Также можно ввести название пакета. Выбранное приложение для киоска должно быть установлено на устройстве. Не забудьте установить приложение для киоска как обязательное. Ярлык на домашнем экране: Если установлено значение "Вкл.", будет создан ярлык на домашнем экране. Если установить значение "Выкл.", приложение по-прежнему будет отображаться в Списке приложений.

Пароль выхода Включен	Если Вы активируете эту функцию, то пользователь сможет завершить режим киоска с помощью пароля, который был предварительно определен Вами
Пароль выхода	Это пароль, который был предварительно определен Вами
Автоматическое сворачивание строки состояния	Если эта опция включена, Строка состояния будет автоматически закрашиваться. С этой опцией пользователи смогут видеть информацию в Строке состояния, но не смогут получить доступ к ее функциям
Отключите строку состояния	Строка состояния содержит Уведомления, Ярлыки и Информацию. Доступно только для устройств Samsung с KNOX 1.0 или выше.
Отключите клавиши регулировки громкости	Отключите клавиши регулировки громкости (доступно только на устройствах Samsung с KNOX 1.0 или выше)
Отключить переключатель включения/выключения	Отключите переключатель Вкл/Выкл (доступно только на устройствах Samsung с KNOX 1.0 или выше)
Отключите кнопку Home	Отключите кнопку "Домой". Если эта функция была активирована, то режим киоска может быть завершен только в консоли AppTec360 (доступно только на устройствах Samsung с KNOX 1.0 или выше)
Отключить панель навигации	С ее помощью Вы можете отключить панель навигации (Назад / Меню). Если эта функция активирована, то режим киоска может быть прерван только в консоли AppTec360. (доступно только на устройствах Samsung с KNOX 1.0 или выше)

Настройки обновления приложений	
Разрешить обновления приложений	Пользователям будет предложено выполнить обновление приложений, даже если активен режим "Киоск". На устройствах с Samsung KNOX приложения будут обновляться беззвучно.
Окно обновления	Установите интервал, через который пользователям будет предложено установить обновления приложений.

TeamViewer	
Включить неуправляемый доступ	Если эта функция включена, администраторы могут удаленно управлять устройством без участия пользователя. На устройстве должно быть установлено приложение TeamViewer Host.

AppTec360 Launcher

Включите AppTec360 Launcher	Вкл: Включает AppTec360 Launcher. Пользователь должен один раз установить его в качестве пусковой установки по умолчанию. Примечание: Если режим киоска включен, а для режима киоска установлено значение "Multi App", использование программы запуска AppTec360 будет принудительным.
Большие иконки	Вкл: Показывает увеличенную версию значков приложений в лаунчере.
Скрыть значок приложения AppTec360	Вкл: Полностью скрывает приложение AppTec360
Скрыть значок магазина AppTec360	Вкл: Полностью скрывает AppTec360 Enterprise AppStore

Настройки AppTec360

Включите приложение AppTec360 Settings	Приложение AppTec360 Settings App обеспечивает контроль над соединениями WiFi и Bluetooth
Включите настройки в Multi App Режим киоска	Если эта функция включена, пользователи могут получить доступ к приложению AppTec360 Settings App, пока активен режим киоска с несколькими приложениями

Пульт дистанционного управления

Splashtop

Показывает текущий статус настройки Splashtop. Здесь Вы увидите шаги, которые необходимо выполнить для удаленного доступа к устройству через Splashtop. Здесь Вам также нужно ввести код развертывания, который Вы можете получить на сайте Splashtop. Код развертывания необходим для подключения к устройству.

Teamviewer

Показывает текущий статус настройки Teamviewer. Здесь Вы увидите шаги, которые необходимо выполнить для удаленного доступа к устройству через Teamviewer.

Управление контентом

Contentbox

Здесь Вы можете включить Contentbox для этого устройства. После активации приложение Contentbox будет установлено на устройство.

Безопасный браузер

Здесь Вы можете включить Безопасный браузер для этого устройства. После активации на устройстве будет установлено приложение Secure Browser App. Этот браузер можно настроить так, чтобы он предлагал на устройстве веб-браузер, ограниченный Вашими потребностями.

Требуется пароль	Требуйте, чтобы пользователь установил и использовал пароль для доступа к браузеру.
Ограничить загрузку / Открыть в	Блокировка загрузок с веб-сайтов
Ограничение загрузки	Ограничивает загрузку на определенные URL. Укажите URL-адрес, чтобы полностью заблокировать загрузку
Разрешить копирование	Позволяет копировать, вырезать или делиться текстом внутри веб-страниц.
Разрешить захват экрана	Позволяет делать скриншоты.
Частота очистки данных	Выберите, с какой периодичностью должны автоматически удаляться ВСЕ пользовательские данные (история, кэш и т.д.).
Закладки компании	Закладки будут отображаться в папке "Закладки компании" в закладках браузера. Пользователь не может их редактировать.
Скрыть адресную строку	Скрывает адресную строку, чтобы пользователь не видел URL, который он посещает.
Белые списки в браузере (без Universal Gateway)	Обеспечивает "белый список" URL на стороне клиента. - Закладки компании всегда заносятся в белый список - Поддерживается только для 100 URL - Пожалуйста, используйте Универсальный шлюз для неограниченного количества черных и белых списков
Черные и белые списки на основе шлюза	Для внесения в черный список необходимы следующие требования: - Работающий Универсальный шлюз AppTec360 ("Общие настройки" → "Универсальный шлюз") - Работающая конфигурация VPN с указанным DNS-сервером ("Общие настройки" → "Универсальный шлюз" → "Настройки VPN") - Конфигурация Черного списка ("Общие настройки" →

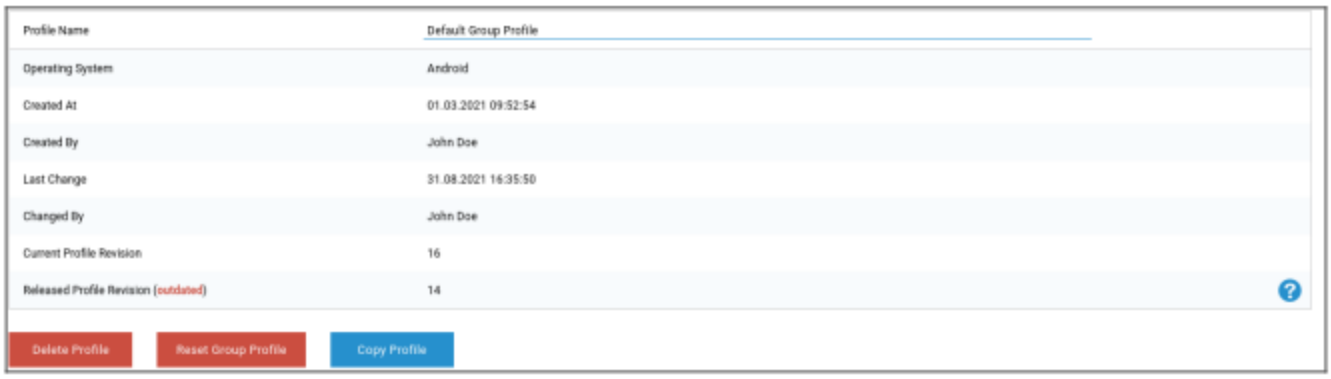
	"Универсальный шлюз" → "Черный список доменов") - Действующее VPN-соединение в профиле ("Управление соединениями" → "VPN").

Конфигурация ПК с Windows 10

Общие сведения

Обзор профиля группы (только на уровне группы)

Открыв профиль группы, Вы получите краткий обзор профиля.



Имя профиля	Название профиля (может быть изменено здесь)
Операционная система	Операционная система, для которой предназначен профиль
Создано в	Время создания
Created By	Создатель профиля
Последнее изменение	Время последнего изменения профиля
Изменено	Учетная запись, которая внесла последние изменения
Текущий пересмотр профиля	Пересмотр сохраненного состояния профиля
Выпущенный пересмотр профиля	Назначенная ревизия профиля ("Назначить сейчас"). Если за текстом на ярлыке отображается "(устаревший)", это означает, что Вы сохранили профиль, но еще не назначили его, поэтому устройства все еще будут получать старую версию.

Обзор устройства (только на уровне устройства)

Сводный обзор устройства, который содержит следующее:

Имя ПК	Название ПК
Клиент	Устройства типа Windows
Последнее известное местонахождение	Широта и долгота последнего известного местоположения устройства
Назначение Обязательные приложения	Количество обязательных приложений, назначенных устройству
UID ПК	UID компьютера
OS Edition	Показывает Вашу редакцию Windows
Версия ОС	Текущая установленная версия Windows
Сборка ОС	Текущая сборка Windows
Операционная система	Установленная в настоящее время операционная система
Серийный номер	Серийный номер устройства
Владение устройством	Настроенный тип владения
Тип устройства	Тип устройства
Rooted	Показывает, является ли устройство рутованным
Соответствующий	Показывает, соответствует ли устройство требованиям
Последний раз видели	Дата и время, когда были сделаны изменения в профиле
Назначение пользователя	Отображает пользователя или группу, к которой в данный момент приписано это устройство. Вы можете переместить устройство, выбрав другого пользователя или группу из выпадающего списка.

Настройки

Разрешить автоматическое обновление	Разрешите или запретите автоматическое обновление ос.

Пересмотр конфигурации (только на уровне устройства)

Здесь Вы получите обзор того, какой групповой профиль назначен устройству.

Если Вы нажмете на профиль группы, Вы получите прямой доступ к нему и сможете выполнить настройки.

С помощью этого символа Вы можете вернуть назначенные приложения к настройкам группового профиля.

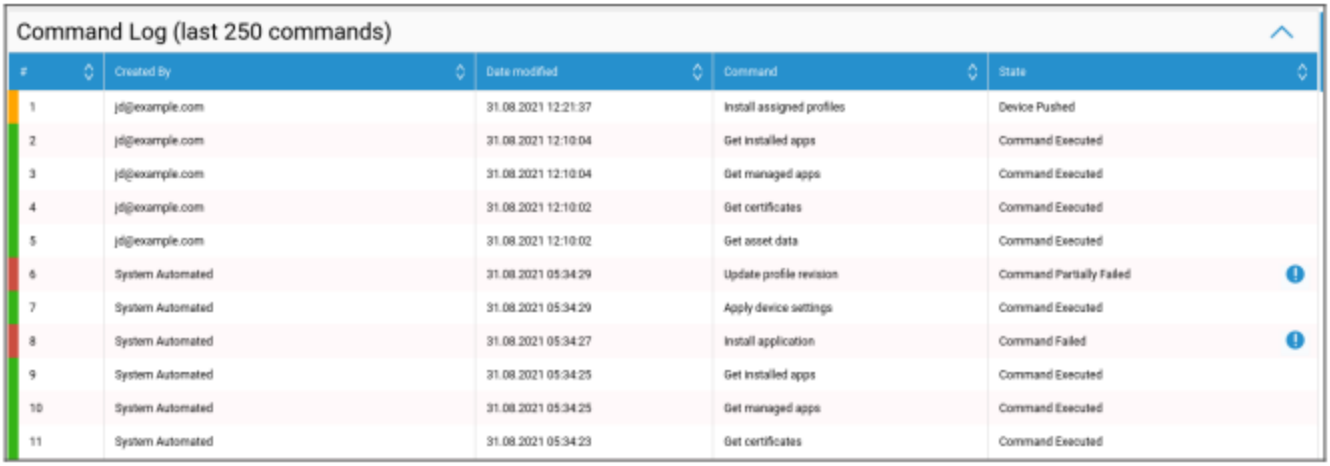
С помощью этого символа Вы можете сбросить профиль устройства, чтобы он вообще не имел никаких настроек.

"Доступна более новая редакция" означает, что профиль группы был изменен и сохранен, но не назначен. Чтобы применить изменения к устройствам, групповой профиль должен быть назначен с помощью "Назначить сейчас" на уровне группы.

Журнал устройства (только на уровне устройства)

Журнал команд

Здесь Вы можете увидеть, какие команды были отданы устройству и каков их статус.



Команды, созданные с помощью "System Automated", автоматически создаются системой.

Возможные статусы команд

Устройство нажимается	Запрос push был отправлен в службу push (например, APNS), чтобы сообщить устройству о необходимости подключиться обратно к серверу EMM.
Команда Создана	Команда была создана в системе.
Команда отправлена	Команда была отправлена на устройство после того, как оно подключилось к серверу.
Команда выполнена	Команда была успешно выполнена.
Команда не выполнена	Команда завершилась неудачно. *
Команда частично не выполнена	В зависимости от ОС устройства некоторые команды могут быть сгруппированы вместе. В этом случае некоторые части этой группы команд оказались неудачными. *
Команда выполнена, в итоге - отказ	Команда была выполнена, но, возможно, она не была выполнена.
Command Repushed	Команда была повторно запущена пользователем.
Выброшенные	Команда была отменена. Например, потому что она была заменена другой командой или устройство было перерегистрировано, и старые команды были удалены.

*Если за сообщением стоит восклицательный знак, Вы можете получить дополнительную информацию, наведя курсор на значок.

Управление активами (только на уровне устройств)

Информация об устройстве

Производитель	Производитель устройства
Модель	Модель устройства
Номер модели	Номер модели
Операционная система	Операционная система
Версия ОС	Версия ОС
Серийный номер	Серийный номер
ExchangeID	ExchangeID
Общее количество оперативной памяти	Общее количество оперативной памяти
Разрешение дисплея	Разрешение дисплея
Язык телефона	Язык устройства
Версия микропрограммы	Версия микропрограммы
Версия DM Client	Версия клиента управления устройством
Версия аппаратного обеспечения	Версия аппаратного обеспечения устройства
Архитектура процессора	Архитектура процессора (тип процессора)

Клетчатка

Сеть оператора SIM	Сеть операторов связи
Номер телефона	Номер телефона
Статус роуминга	Статус роуминга
IMEI	IMEI
IMSI	IMSI
Встроенное ПО модема	Встроенное ПО модема

Информация о синхронизации

Мгновенное подключение DM	Устройство должно немедленно создать соединение с AppTec
Начальное время повтора	Начальное время повторной попытки для этого первого соединения
Повторные попытки подключения	Количество повторных попыток установить новое соединение после разрыва связи с диспетчером соединений или ошибки на уровне WinInet
Максимальное время сна	Максимальное время сна после ошибки отправки пакета
Первые повторные попытки синхронизации	Время для первого этапа после зачисления
Первый интервал повторных попыток	Время для первого этапа после зачисления
Повторные попытки синхронизации	Время для второго этапа после зачисления
Второй интервал повторных попыток	Время для второго этапа после зачисления
Регулярные повторные попытки синхронизации	Время на дополнительные этапы после зачисления
Регулярный интервал повторных попыток	Время на дополнительные этапы после зачисления

Управление безопасностью

Защита от кражи (только на уровне устройства)

Информация GPS (только на уровне устройства)

Здесь Вы можете установить текущее/последнее местоположение устройства. Локализация может быть защищена одним или даже двумя паролями - см: "Общие настройки" > "Конфиденциальность" > "Доступ к GPS".

Настройки GPS

Включите GPS-слежение	Включите регулярную синхронизацию GPS-информации.
Интервал отслеживания	Установите интервал синхронизации GPS-информации.

Конфигурация безопасности

Пасскод

Минимальная длина пароля	Минимальная длина пароля	
Состав пароля	Указывает количество определенных символов, которые должен содержать пароль Они состоят из заглавных и строчных букв, цифр и специальных символов.	
Качество паролей	Здесь Вы можете установить качество пароля	
	Буквенно-цифровой	Только цифры и буквы
	Числовой	Только числа
	Цифровой или буквенно-цифровой	Цифры или цифры и буквы
Максимальная блокировка времени бездействия	Количество минут бездействия пользователя на устройстве, по истечении которых устройство будет заблокировано. По истечении этого времени пользователь должен разблокировать устройство, введя свой пароль.	
Срок действия пароля	Установите время, в течение которого необходимо установить новый пароль	
Ограничение истории паролей	Количество ранее использованных паролей, которые не разрешены	
Максимальное количество неудачных попыток ввода пароля	Количество раз, когда пароль может быть введен неправильно, прежде чем будет произведено полное стирание устройства	

Антивирус

Настройки антивируса - Настройка конфигурации сканирования	
Тип сканирования	Выбирает, выполнять ли быстрое или полное сканирование
Установите начало сканирования	Выбор времени суток, когда Windows Defender будет начинать сканирование
Частота сканирования	Выбирает день, когда должно выполняться сканирование Windows Defender
Частота обновления подписи	Указывает интервал в часах, который будет использоваться для проверки наличия подписей

Настройте тип файлов для сканирования	
Разрешите сканирование архивных файлов	Разрешите или запретите сканирование архивов (например, .zip) при обращении к ним.
Разрешите сканирование скриптов	Разрешает или запрещает функцию сканирования сценариев Windows Defender.
Разрешите сканирование электронной почты	Разрешите или запретите сканирование электронной почты.
Разрешите сканирование сетевых файлов	Разрешите или запретите сканирование сетевых файлов.
Разрешите полное сканирование сопоставленных сетевых дисков	Разрешите или запретите сканирование сопоставленных сетевых дисков (включается, только если включено полное сканирование).
Управление двунаправленным сканированием	Контролирует, какие наборы файлов должны отслеживаться.
Разрешите полное сканирование съемных дисков	Разрешите или запретите полное сканирование съемных дисков. Только при запуске полного сканирования.

Тип файлов, которые нужно исключить из сканирования	
Игнорируйте типы файлов для сканирования	Определите набор типов расширений файлов. Каждое расширение файла для каждого поля.
Игнорируйте пути к директориям	Определите набор путей к каталогам, чтобы не сканировать их. По одному пути на поле. Примеры: "C:\Example", "C:\Windows" или "C:\Users".
Исключите процессы из сканирования	Исключите файлы, которые были открыты определенными процессами, из сканирования антивирусом Microsoft Defender. . Один путь на поле. Примеры: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Дополнительные настройки	
Разрешить мониторинг в режиме реального времени	Разрешите или запретите функцию Windows Defender Realtime Monitoring
Разрешить мониторинг поведения	Разрешите или запретите функцию мониторинга поведения Windows
Разрешить облачную защиту	Разрешите или запретите Защитнику Windows отправлять информацию в Microsoft о любой найденной им проблеме. Microsoft проанализирует эту информацию, узнает больше о проблеме, влияющей на устройство, и предложит улучшенные решения.
	Поведение при отправке образцов
Разрешите защиту Windows Defender IOAV	Разрешите или запретите защиту Windows Defender IOAV
Разрешите доступ к пользовательскому интерфейсу Defenders "Защита при доступе"	
Средний коэффициент загрузки процессора	Представляет собой средний коэффициент загрузки процессора при сканировании Windows Defender (в процентах).

Работа с вредоносным ПО	
Низкая степень тяжести	Вы можете определить для каждого уровня серьезности, как устройство будет обрабатывать вредоносное ПО. Доступны следующие варианты: • Clean • Карантин • Удалить • Разрешить • Определено пользователем • Блок
Умеренная степень тяжести	
Высокая степень тяжести	
Тяжелая степень тяжести	
Дни для сохранения очищенного вредоносного ПО	Период времени в днях, в течение которого файлы/элементы в карантине будут храниться в системе. Значение по умолчанию - 0, при

	этом элементы остаются в карантине и не удаляются автоматически. Максимальное значение - 90.

Центр безопасности

Центр безопасности Windows - Настройки безопасности Windows	
Отключите пользовательский интерфейс защиты от вирусов и угроз	
Hide Ransomware Data Recovery UI	
Отключите защиту учетной записи в пользовательском интерфейсе	
Отключите брандмауэр и сетевую защиту UI	
Отключите пользовательский интерфейс управления приложениями и браузером	
Запретите изменения в защите от эксплойтов	Запретите пользователю вносить изменения в настройки защиты от эксплойтов
Отключите пользовательский интерфейс безопасности устройства	
Устранение неисправностей TPM	Скрыть настройки устранения неисправностей TPM
Отключите кнопку Clear TPM	
Отключите пользовательский интерфейс производительности и здоровья устройства	
Отключите пользовательский интерфейс семейных опций	

Настройте тосты	
Включите настраиваемую информацию о поддержке	Включите отображение настроенной контактной информации службы поддержки для Вашей компании в правом нижнем углу приложения центра безопасности.
Адрес электронной почты	Установите адрес электронной почты компании
Название компании	Установите название компании
Телефон компании	Установите телефон компании
URL-адрес справки	Установите URL-адрес справки компании

Дополнительные настройки	
Отключите уведомления	Отключите отображение уведомлений Центра безопасности Windows Defender.
Скрыть рекомендации по обновлению прошивки TPM	Скройте рекомендацию по обновлению микропрограммы TPM при обнаружении уязвимой микропрограммы.
Отображайте название компании и контактные данные	Отобразите название Вашей компании и контактные данные во всплывающей карточке контактов в Центре безопасности Windows Defender.
Скрыть Secure Boot	Скройте область Security Boot.
Управление областью уведомлений Hide Security	Скрыть управление областью уведомлений Windows Security.

Конфигурация брандмауэра

Конфигурация брандмауэра - Глобальные настройки	
Игнорируйте набор аутентификации	Игнорируйте весь набор аутентификации, если он не поддерживает все наборы аутентификации, указанные в наборе
Тип очереди пакетов	Указывает, как включается масштабирование программного обеспечения на стороне приема как для зашифрованного приема, так и для очищенного прямого пути для сценария туннельного шлюза IPsec.
Отключите фильтрацию FTP с учетом состояния	Если эта функция отключена, она не будет выполнять фильтрацию по протоколу передачи файлов (FTP) с учетом состояния, чтобы разрешить вторичные соединения.
Время простоя ассоциации безопасности	В этом поле настраивается время простоя ассоциаций безопасности в секундах. Ассоциации безопасности удаляются после того, как сетевой трафик не наблюдается в течение указанного периода времени.
Кодирование ключей с предварительной защитой	Установите кодировку предварительно распределенного ключа
Исключения IPSec	Настройте исключения Интернет-протокола
Проверка списка отзыва сертификатов	

Профили брандмауэра (Профиль домена / Частный профиль / Публичный профиль)	
Включите брандмауэр для этого профиля	
Отключите уведомления	Отключите отображение уведомления для пользователя, когда приложение блокируется от прослушивания порта.
Блокируйте одноадресные ответы на многоадресные передачи	
Применяйте правила брандмауэра авторизованных приложений	Если он не установлен, авторизованные правила брандмауэра приложений в локальном хранилище игнорируются и не выполняются
Применяйте глобальные правила брандмауэра портов	Если этот параметр не установлен, правила брандмауэра глобальных портов в локальном хранилище игнорируются и не применяются. Параметр имеет значение, только если он установлен или перечисляется в хранилище групповой политики или если он перечисляется из хранилища GroupPolicyRSoPStore
Обеспечьте выполнение правил брандмауэра	Если он не установлен, правила брандмауэра из локального хранилища игнорируются и не выполняются
Применяйте правила безопасности соединений	Если это правило не выполняется, правила безопасности соединения из локального магазина игнорируются и не выполняются
Действие по умолчанию для исходящих сообщений	Действие, которое брандмауэр выполняет по умолчанию при исходящих соединениях
Входящее действие по умолчанию	Действие, которое брандмауэр выполняет по умолчанию при входящих соединениях
Отключите режим "Скрытность	Скрытый режим - это механизм в Брандмауэре Windows, который помогает предотвратить обнаружение злоумышленниками информации о компьютерах сети и запускаемых ими службах.
Отключите предотвращение ответа на незапрашиваемый трафик	Если отключено, правила скрытого режима брандмауэра не должны запрещать хост-компьютеру отвечать на незапрашиваемый сетевой трафик, если этот трафик защищен с помощью IPsec.

Правила брандмауэра

Правила брандмауэра	
Имя	Название правила
Описание	Описание правила
Действие	Укажите, будет ли это правило блокировать трафик или разрешать его. Пожалуйста, примите во внимание, что опция Block может также блокировать трафик (в зависимости от остальной конфигурации) между MDM-сервером и Устройством
Направление	
Включить обход границы (доступно только в том случае, если параметр **Направление** установлен на **входящий трафик**)	Указывает, что определенному входящему трафику разрешено туннелирование через NAT и другие пограничные устройства с помощью технологии туннелирования Teredo.

Программы и услуги	
Определите приложения, во всех остальных случаях	Если эта опция не включена, то будут рассматриваться все приложения
Название семейства пакетов	Имя семейства пакетов, к которому будет применяться правило.
Путь к файлу приложения	Полное приложение, например, C:\Windows\System\Notepad.exe, к которому будет применено правило
Полностью квалифицированное двоичное имя	Полностью квалифицированное двоичное имя, к которому будет применяться правило. FQBN - это строка в следующем виде: {Publisher\Product\Filename,Version}
Название услуги	Введите имя службы (например, "EventLog"). Вы можете получить список имен служб в Powershell, выполнив команду "Get-Service".

Протоколы и порты				
Протокол	Протокол, используемый правилом.			
	Доступные значения: - Любой - Пользовательский - ХОПОРТ - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-маршрут - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	При установке значения Пользовательский	Вставьте номер протокола от 0 до 255	Номер протокола
		Если выбрано значение TCP или UDP	Укажите локальные порты, в противном случае будут использоваться все.	Локальные порты, которые будет использовать правило, порты диапазона также разрешены
			Местный порт	Один порт или диапазон портов. Например, 100-120, 200, 300-320.
			Укажите удаленные порты, в противном случае будут использоваться все.	Удаленные порты, которые будет использовать правило, порты диапазона также разрешены
			Удаленный порт	Один порт или диапазон портов. Например, 100-120, 200, 300-320.

Область применения	
Укажите локальные IP-адреса, в противном случае - любой IP-адрес	Набор локальных IP-адресов, это также может быть диапазон IP-адресов, разделенных символом -.
Локальный IP-адрес	Набор отдельных IP-адресов или диапазон IP-адресов, разделенных символом -.
Укажите удаленные IP-адреса, в противном случае - любой удаленный IP-адрес	Укажите набор удаленных IP-адресов, это также может быть диапазон IP-адресов, разделенных знаком "-".
Удаленный IP-адрес	Укажите один IP-адрес или диапазон IP-адресов

	Жетоны	Токены, которые можно установить вместе с удаленными адресами. Токены Intranet, RmtIntranet и Ply2Renders поддерживаются в Windows 10, версии 1809 и более поздних.

Дополнительные настройки	
Укажите профили, в противном случае будут использоваться все	Если отключить, будут использоваться все профили
Домен	Профиль домена
Частный	Личный профиль
Общественность	Публичный профиль
Укажите интерфейсы, в противном случае будут использоваться все.	Если отключить, будут использоваться все интерфейсы
Локальная сеть	Интерфейс локальной сети
Удаленный доступ	Интерфейс удаленного доступа
Беспроводной	Беспроводной интерфейс

Местные директора	
Добавьте авторизованных локальных пользователей	Разрешите добавить список локальных пользователей, которые будут использовать это правило
Авторизованные пользователи	Список авторизованных локальных пользователей для этого правила. Пользователь должен быть в формате языка описания безопасности (SDDL), например, PC_NAME\USERNAME. Это поле не должно быть заполнено, если имя службы настроено на использование этого правила

Настройки ограничений

Функциональность устройства

Разрешить SD-карту	Позволяет использовать SD-карту
Разрешить камеру	Разрешите использовать фотоаппарат
Разрешить службу определения местоположения	Разрешите службу определения местоположения устройства
Разрешить боковую загрузку приложений	Разрешите установку приложений из неизвестных источников
Разрешить режим разработчика	Позволяет использовать режим разработчика
Разрешить роуминг сотовых данных	Разрешите роуминг сотовых данных
Разрешить Cortana	Разрешите голосовому помощнику Cortana
Разрешите поиску использовать местоположение	Разрешите поиску использовать местоположение
Разрешить добавление учетной записи электронной почты, не принадлежащей Microsoft	Укажите, разрешено ли пользователю добавлять учетные записи электронной почты, не относящиеся к MSA.
Разрешить подключение учетной записи Microsoft	Укажите, разрешено ли использовать учетную запись MSA для аутентификации и услуг, не связанных с электронной почтой.
Разрешить синхронизацию Мои настройки	Позволяет синхронизировать настройки всего устройства.
Защищенные доменные имена предприятия	Укажите имена доменов предприятия, разделенные символом ";".
Разрешите пользователю отключить	Позволяет пользователю отключить Восстановление системы. **ВНИМАНИЕ!**

восстановление системы	Эту функцию следует использовать только на устройствах, которые принадлежат или предоставляются корпоративной компанией или организацией, или на устройствах, принадлежащих пользователю, когда пользователь разрешает, чтобы устройство полностью управлялось корпоративной компанией. Если Вы отключите этот параметр политики, Восстановление системы будет отключено, а мастер восстановления системы будет недоступен. Возможность настроить Восстановление системы или создать точку восстановления через Защиту системы также отключена.
Разрешить отмену регистрации пользователей	Позволяет пользователю удалить корпоративную часть с устройства и тем самым отключиться от серверов AppTec360. Если это произойдет, управлять устройством будет уже невозможно **ВНИМАНИЕ!** Эту функцию следует использовать только на устройствах, которые принадлежат или предоставляются корпоративной компанией или организацией, или на устройствах, принадлежащих пользователю, когда пользователь разрешает, что устройство будет полностью управляться корпоративной компанией. Если Вы отключите этот параметр политики, пользователи не смогут удалять записи MDM. Укажите, разрешено ли пользователю удалять учетную запись на рабочем месте через панель управления рабочим местом. Сервер MDM всегда может удаленно удалить учетную запись.

BitLocker

Конфигурация BitLocker

Общие настройки	
Требуйте шифрования устройств	Предложите пользователям включить шифрование устройства.В зависимости от редакции Windows и конфигурации системы, пользователям может быть предложено включить шифрование: - Чтобы убедиться, что шифрование от другого провайдера не включено. - Чтобы отключить BitLocker Drive Encryption, а затем снова включить BitLocker.
Методы шифрования	
Метод шифрования дисков операционной системы	
Метод шифрования для фиксированных накопителей данных	
Метод шифрования для съемных накопителей данных	
Отключите предупреждение о шифровании дисков сторонних производителей	Отключите предупреждение о том, что на устройстве используется сторонняя служба шифрования дисков. Начиная с Windows 10, версия 1803, этот параметр поддерживается только для устройств, подключенных к Azure Active Directory.
Разрешите выполнять шифрование при входе в систему пользователя, не являющегося администратором	Поддерживается только для устройств, подключенных к Azure Active Directory

Расширения AppTec360	
Бесшумное шифрование	Если выбрать этот пункт вместе с "Требовать шифрования устройств", служба управления AppTec360 запустит автоматическое бесшумное шифрование дисков устройств.
Автоматически генерируйте учетные данные пользователя	Зашифрованный диск ОС будет защищен автоматически сгенерированными учетными данными пользователя. Либо PIN-код TPM, если TPM доступен, либо текстовый пароль из 6 цифр. Сгенерированные учетные данные отправляются на адрес электронной почты, зарегистрированный для данного устройства. Если эта опция выключена, единственной возможной защитой для бесшумного шифрования будет использование TPM. В этом случае на устройствах без TPM бесшумное шифрование не сработает.
Шифруйте фиксированные диски	Все имеющиеся стационарные диски с данными также будут зашифрованы и защищены "Автоматической разблокировкой" с помощью ключа, хранящегося на диске ОС.

Настройки диска ОС

Требуйте дополнительной аутентификации при запуске	Этот параметр позволяет Вам настроить, требует ли BitLocker аутентификации при каждом запуске компьютера. Эта настройка применяется во время установки BitLocker. Если Вы включите этот параметр, пользователи смогут настраивать расширенные параметры запуска в мастере установки BitLocker.
Блокировка BitLocker без совместимого TPM	
Только TPM	
TPM и PIN-код	
TPM и ключ	
TPM, ключ и PIN-код	Если Вы хотите потребовать использования PIN-кода и USB-накопителя (ключа), пользователь должен настроить BitLocker с помощью инструмента командной строки "manage-bde", а не с помощью мастера настройки BitLocker Drive Encryption.

Требуется минимальная длина PIN-кода

	Минимальное количество символов

Настройте сообщение и URL для предзагрузочного восстановления	Настройте все сообщение о восстановлении или замените существующий URL, который отображается на экране восстановления ключа перед загрузкой, когда диск ОС заблокирован. Примечание: Не все символы и языки поддерживаются в предварительной загрузке. Настоятельно рекомендуется проверить, правильно ли отображаются используемые Вами символы на экране восстановления перед загрузкой.
	Вариант сообщения перед загрузкой восстановления
	Пользовательское сообщение о восстановлении
	Пользовательский URL-адрес восстановления

Варианты восстановления диска ОС		Этот параметр позволяет Вам управлять тем, как восстанавливать диски с операционной системой, защищенной BitLocker, при отсутствии необходимых учетных данных. Эта настройка применяется во время установки BitLocker. По умолчанию разрешен агент восстановления данных на основе сертификатов, параметры восстановления могут быть указаны пользователем, включая пароль и ключ восстановления, а информация о восстановлении не резервируется в AD DS.
	Агент для восстановления данных на основе блочного сертификата	Укажите, можно ли использовать средство восстановления данных с дисками, защищенными операционной системой BitLocker. Перед использованием агента восстановления данных его необходимо добавить из пункта Политики открытых ключей в консоли управления групповой политикой или в редакторе локальной групповой политики. Обратитесь к Руководству по развертыванию BitLocker Drive Encryption на сайте Microsoft TechNet за дополнительной информацией о добавлении агентов восстановления данных.
	Настройки пароля восстановления BitLocker	
	Настройки ключа восстановления BitLocker	
	Сохраните информацию о восстановлении BitLocker в доменных службах Active Directory	
	Конфигурация хранилища для восстановления AD DS BitLocker	Хранение пакета ключей позволяет восстановить данные с диска, который был физически поврежден.
	Требуйте хранения данных восстановления в AD DS	Запретите пользователям включать BitLocker, если компьютер не подключен к домену и

Фиксированные настройки привода	
Варианты восстановления фиксированных дисков	Этот параметр позволяет Вам контролировать, как будут восстанавливаться защищенные BitLocker фиксированные диски при отсутствии необходимых учетных данных. Эта настройка применяется во время установки BitLocker. По умолчанию разрешен агент восстановления данных на основе сертификатов, параметры восстановления могут быть указаны пользователем, включая пароль и ключ восстановления, а информация о восстановлении не резервируется в AD DS.
Агент для восстановления данных на основе блочного сертификата	
Настройки пароля восстановления BitLocker	
Настройки ключа восстановления BitLocker	
Сохраните информацию о восстановлении BitLocker в доменных службах Active Directory	
Конфигурация хранилища для восстановления AD DS BitLocker	Хранение пакета ключей позволяет восстановить данные с диска, который был физически поврежден.
Требуйте хранения данных восстановления в AD DS	Запретите пользователям включать BitLocker, если компьютер не подключен к домену и резервное копирование информации о восстановлении BitLocker в AD DS прошло успешно. Примечание: Пароль для восстановления генерируется автоматически.
Запрет на запись на незащищенные фиксированные диски	

Настройки съемного диска	
Запретите запись на незащищенные съемные диски	Запретите доступ на запись к съемным дискам, которые не защищены Bitlocker. Примечание: Если в групповой политике включен параметр "Съемные диски: Запретить доступ на запись" включен в групповой политике, этот параметр политики будет проигнорирован.
Запретить доступ на запись устройствам, настроенным в другой организации	Доступ на запись будет предоставлен только тем дискам, идентификационные поля которых совпадают с идентификационными полями компьютера. Эти поля определяются параметром групповой политики "Предоставлять уникальные идентификаторы для Вашей организации".

Состояние BitLocker

Здесь Вы можете увидеть текущее состояние зашифрованных дисков BitLocker

C [OS Drive]
Статус шифрования
Зашифровано (%)
Статус защиты
Метод шифрования
Протекторы для ключей
Восстановление пароля

Щелкнув на кнопке "Повернуть пароль восстановления", Вы можете повернуть пароль восстановления BitLocker.

Управление сертификатами

Список сертификатов

Здесь представлен список сертификатов, установленных на отображаемом устройстве.

Конфигурация сертификата

Здесь Вы можете настроить сертификаты и то, как они будут устанавливаться на устройство.

Доверенный сертификат	
Описание	Описание сертификата
Область применения	Область развертывания сертификата: Текущий пользователь против устройства
Хранилище сертификатов	"Недоверенные сертификаты" доступны только в Windows 10, версия 1803
Файл сертификата	Загрузите файл PKCS#1

Сертификат личности			
Описание	Описание сертификата		
Область применения	Область развертывания сертификата: Текущий пользователь против устройства		
Ключевое местоположение	Поставщик хранилища ключей для установки закрытого ключа.		
		TPM. Отказ, если TPM отсутствует	
	TPM. Если TPM отсутствует, перейдите на программный KSP		
	Поставщик программного обеспечения для хранения ключей		Пометьте закрытый ключ как экспортируемый
	Windows Hello для бизнеса	Название контейнера	Укажите имя контейнера Windows Hello for Business (ранее известного как Microsoft Passport for Work).
		Текст подсказки PIN-кода	Определяет пользовательский текст, который будет отображаться в подсказке Windows Hello for Business PIN во время регистрации сертификата.
Кредит	Загрузка файла PKCS#12		

SCEP

Описание	Описание сервера SCEP		
Область развертывания	Область развертывания сертификата: Текущее устройство против пользователя		
URL-адреса серверов SCEP	Один или несколько серверов, выдающих сертификаты через SCEP		
Тема	Представление имени X.500. Например, "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar".		
Альтернативные названия предметов	Тип	Адрес электронной почты	
		DNS	
		URI	
		Основное имя пользователя (UPN)	
Отпечатки пальцев CA	Отпечаток SHA1 сертификата центра сертификации. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Единицы срока действия	Дни, месяцы или годы		
Срок действия			
Вызов	Используется как предварительный секрет для автоматической регистрации		
Повторные попытки	Количество повторных попыток устройства, если сервер посылает ответ PENDING. Значение по умолчанию - 5. Максимальное значение - 30.		
Задержка повторной попытки	Количество минут ожидания перед повторной попыткой. Значение по умолчанию - 5. Минимальное значение - 1.		
Размер ключа	Размер ключа в битах		
Алгоритм хэширования	Семейство хэш-алгоритмов		
Использование ключей	Расширение "Использование ключа" определяет назначение (например, шифрование, подпись) ключа, содержащегося в сертификате. Необходимо выбрать хотя бы один из вариантов "Цифровая подпись" или "Шифрование ключа".		
Расширенное использование	Определяет расширенные возможности использования ключей. Зависит от конфигурации сервера SCEP. Укажите список соответствующих OID,		

ключей	например, 1.3.6.1.5.5.7.3.2 (Аутентификация клиента).		
Ключевое местоположение	Поставщик хранилища ключей для установки закрытого ключа.		
		TPM. Отказ, если TPM отсутствует	
	TPM. Если TPM отсутствует, перейдите на программный KSP		
	Поставщик программного обеспечения для хранения ключей		
	Windows Hello для бизнеса	Название контейнера	Укажите имя контейнера Windows Hello for Business (ранее известного как Microsoft Passport for Work).
		Текст подсказки PIN-кода	Определяет пользовательский текст, который будет отображаться в подсказке Windows Hello for Business PIN во время регистрации сертификата.

Управление соединениями

Wifi

При этой настройке выполните предварительную конфигурацию устройств конечных пользователей для доступа к внутренним точкам доступа

Идентификатор набора услуг (SSID)	SSID сети, к которой будет установлено соединение
Автоматическое присоединение	Активация автоматического присоединения к сети
Скрытая сеть	Активировать, в случае если точка доступа не передает SSID

Тип безопасности

Установите тип безопасности точки доступа

Открытая система WEP	
Пароль	Пароль для точки доступа

WPA PSK	
Пароль	Пароль для точки доступа

WPA EAP	
Тип аутентификации	Тип аутентификации, возможен только при использовании "PEAP-MSCAHPv2".
Быстрое повторное подключение	Устройства могут переключаться между точками доступа без необходимости повторной аутентификации
Гостевой доступ	У пользователя нет учетной записи, поэтому он должен зарегистрироваться как гость
Проверки карантина	Клиент должен выполнить проверку NAP (Network Access Protection) и поделиться результатами с системой, которая затем решит, может ли клиент подключиться.
Требуется привязка к криптовалюте	Аутентификация возможна только через Crypto Binding
Валидация сервера	Клиент проверяет, действителен ли сертификат сервера. Если это так, будет установлено соединение
Запрос на получение сертификатов	Позволяет пользователю принимать недоверенные сертификаты
Имена серверов	Предлагает возможность отобразить имя RADIUS-сервера, который обеспечивает сетевую аутентификацию и авторизацию

WPA2-PSK	
Пароль	Пароль точки доступа

WPA2 EAP	
Тип аутентификации	Тип аутентификации, возможен только при использовании "PEAP-MSCAHPv2".
Быстрое повторное подключение	
Гостевой доступ	
Проверки карантина	Активирует защиту доступа к сети NAP
Требуется привязка к криптовалюте	Аутентификация возможна только через Crypto Binding
Валидация сервера	
Запрос на получение сертификатов	Предлагает ввести подтвержденный сертификат сервера, имя или корневой сертификат аутентификации (CA)
Имена серверов	Список серверов, которым должны доверять устройства
Нет	Отсутствие установленной безопасности
Используйте прокси-сервер	Использование прокси-сервера
Адрес сервера	Адрес прокси-сервера
Порт сервера	Порт сервера прокси-сервера

Используйте прокси-сервер

Включите использование прокси-сервера.

Адрес сервера	Адрес прокси-сервера, используемого в этой сети.
Порт сервера	Порт прокси-сервера, используемый в этой сети.

Ограничения Wifi

Здесь Вы можете задать различные ограничения Wifi.

Разрешить WiFi	Разрешить/запретить WiFi
Разрешить общий доступ к Интернету	Разрешить использование точки доступа
Разрешить автоматическое подключение к горячим точкам WiFi Sense Hot Spots	Разрешить автоматическое подключение к горячим точкам WiFi Sense Hot Spots
Разрешить ручную настройку WiFi	Разрешить пользователю подключаться к сетям WiFi, которые не были определены AppTec
Частота сканирования WLAN	Устанавливает интервал сканирования WLAN. Здесь более высокое значение повышает способность распознавать сети WIFI.

VPN

Выполните здесь соответствующие настройки, чтобы сконфигурировать VPN-соединения

Имя соединения	Указанное имя соединения		
Тип VPN	VPN-соединение Per-App используется для защиты трафика определенных приложений.		
	VPN	Всегда включен	Это автоматически подключит VPN при входе в систему и будет оставаться подключенным до тех пор, пока пользователь не отключится вручную.
	VPN для каждого приложения	Приложения VPN	Определите приложения, которые будут использовать это VPN-соединение
		Блокировка каждого приложения	Per-App Lockdown заставляет выбранные приложения иметь возможность подключения только через это VPN-соединение. Эта функция зависит от брандмауэра Windows Defender.
	Профиль WIP	Домен WIP для этого соединения	Идентификатор предприятия, который необходим для соединения этого VPN-профиля с политикой защиты информации Windows (WIP)

Тип соединения

AppTec360 VPN	
Для "AppTec360 VPN" необходимо, чтобы была разрешена боковая загрузка приложений. Пожалуйста, включите опцию "Разрешить боковую загрузку приложений" в разделе "Управление безопасностью" → "Настройки ограничений" → "Функциональность устройства".	
Конфигурация шлюза	Чтобы настроить VPN-соединение с черным списком, выберите конфигурацию VPN с указанным DNS-сервером. Вы можете настроить конфигурацию VPN в разделе "Общие настройки" → "Универсальный шлюз" → "Настройки VPN".

IKEv2		
Серверы	Список VPN-серверов	
Туннель устройства	Включите соединение перед входом пользователя в систему.	
Метод аутентификации	EAP	EAP XML
	Сертификаты на машины	
Алгоритм шифрования		
Алгоритм проверки целостности		
Группа Диффи-Хеллмана		
Алгоритм преобразования шифра		
Алгоритм преобразования аутентификации		
Группа совершенной прямой секретности (PFS)		

PPTP		
Серверы	Список VPN-серверов	
Метод аутентификации	EAP	EAP XML

L2TP		
Серверы	Список VPN-серверов	
Метод аутентификации	EAP	EAP XML
Алгоритм шифрования		
Алгоритм проверки целостности		
Группа Диффи-Хеллмана		
Алгоритм преобразования шифра		
Алгоритм преобразования аутентификации		
Группа совершенной прямой секретности (PFS)		

Автоматический		
Серверы	Список VPN-серверов	
Метод аутентификации	EAP	EAP XML

Общие конфигурации VPN

Запоминайте учетные данные при каждом входе в систему	
Зарегистрируйте IP-адреса во внутреннем DNS	
Правила фильтрации сетевого трафика	Ограничьте VPN-соединение определенным набором правил.
Список поиска суффиксов DNS	DNS-суффиксы для добавления в список поиска DNS для маршрутизации коротких имен.
Правила таблицы политики разрешения имен (NRPT)	Правила таблицы политики разрешения имен (NRPT) определяют, как DNS разрешает имена при подключении к VPN.
Обнаружение доверенных сетей	Список DNS-суффиксов для идентификации доверенной сети.
Раздельное туннелирование	Раздельное туннелирование означает, что трафик может проходить через любой интерфейс, определяемый сетевым стеком.
Разделение туннельных маршрутов	Список маршрутов, которые должны быть добавлены в таблицу маршрутизации для интерфейса VPN.
Настройка прокси-сервера	Настраивает Proxy, используемый в этой сети
Адрес прокси-сервера	Адрес прокси-сервера в виде полного имени хоста или IP-адреса.
Порт	Порт прокси-сервера.
URL-адрес автоконфигурации прокси	URL-адрес для автоматического получения настроек прокси.

Ограничения VPN

Здесь Вы можете определить различные ограничения VPN.

Разрешить настройки VPN	Это руководство позволяет/запрещает пользователю деактивировать и изменять настройки VPN
Разрешить VPN через сотовую связь	Разрешает/запрещает устройству устанавливать VPN-соединение, если устройство использует мобильные данные
Разрешить VPN-роуминг через сотовую связь	Разрешает/запрещает устройству устанавливать VPN-соединение, если устройство находится в роуминге

Bluetooth

Здесь Вы можете установить, должен ли Bluetooth быть разрешен/запрещен.

Разрешить Bluetooth	Активируйте/деактивируйте Bluetooth

Управление PIM

Exchange Active Sync

Настройка учетной записи ActiveSync на устройстве конечного пользователя

Название счета	Имя учетной записи электронной почты
Имя хоста сервера	Адрес сервера/FQDN
Доменное имя	Домен сервера
Адрес электронной почты	Адрес электронной почты
Имя пользователя	Имя пользователя
Пароль пользователя	По желанию, Вы можете прикрепить пароль к пользователю здесь
Используйте SSL	Используйте SSL-соединение
Интервал синхронизации	Здесь можно установить интервал синхронизации Ручная синхронизация = Пользователь должен загрузить свою электронную почту и выполнить ручную синхронизацию
Фильтр возраста почты	Количество времени, в течение которого электронная почта должна быть синхронизирована Без фильтра = неограниченно
Уровень журнала	Установка уровней протоколирования для трафика ActiveSync
Синхронизация электронной почты	Активировано = электронная почта синхронизируется
Синхронизация контактов	Активировано = контакты синхронизированы
Синхронизация календаря	Активировано = календарь синхронизирован
Синхронизация задач	Активировано = задания синхронизированы

eMail

Создание учетных записей POP3/IMAP4 на устройстве конечного пользователя.

Описание счета	Имя учетной записи электронной почты
Имя отправителя	Отображаемое имя отправителя
Доменное имя	Доменное имя для учетной записи электронной почты
Адрес электронной почты	Адрес электронной почты пользователя
Имя пользователя	Имя пользователя
Пароль пользователя	По желанию, Вы можете прикрепить пароль к пользователю здесь
Альтернативные учетные данные исходящего сервера	Здесь можно указать, если для исходящего сервера требуются другие учетные данные.
Исходящее доменное имя	Исходящее доменное имя
Имя пользователя исходящего сервера	Имя пользователя исходящего сервера
Пароль исходящего сервера	Пароль исходящего сервера
Протокол электронной почты	POP3 или IMAP4, может использоваться в качестве протокола
Имя хоста сервера входящей почты	Имя хоста сервера входящей почты
Используйте SSL для входящей почты	Используйте SSL для входящих сообщений электронной почты
Имя хоста сервера исходящей почты	Имя хоста сервера исходящей почты
Используйте SSL для исходящих писем	Используйте SSL для исходящих сообщений электронной почты
Аутентификация исходящего сервера	Требуется аутентификация исходящего сервера
Интервал синхронизации	Здесь можно установить интервал синхронизации Ручная синхронизация = Пользователь должен загрузить свою электронную почту и выполнить ручную синхронизацию

Фильтр возраста почты	Количество времени, в течение которого электронная почта должна быть синхронизирована Без фильтра = неограниченно

Управление приложениями

Enterprise App Manager

Установленные приложения

Здесь представлен список приложений, которые в настоящее время установлены на отображаемом устройстве.

Обязательные приложения

Здесь Вы можете настроить список приложений, обязательных для использования на устройстве.

Этот список будет проверяться каждый раз, когда устройство подключается к MDM, и устанавливать все приложения из этого списка, которые не были установлены на устройстве, независимо от того, было ли приложение удалено или никогда не было установлено ранее.

Вы можете загрузить приложения Windows 10 In-House Apps и затем добавить их в этот список или добавить конфигурации Microsoft Office, которые необходимо предварительно настроить в разделе "Общие настройки" > "Управление приложениями" > "Microsoft Office".

Ограничения системных приложений

Приложения Inbox
Разрешить будильники и часы
Калькулятор разрешений
Разрешить камеру
Разрешить контактную поддержку
Разрешить Cortana
Разрешить File Explorer
Разрешить приступить к работе
Allow Groove Music
Разрешить карты
Разрешить обмен сообщениями
Разрешить Microsoft Edge
Разрешить фильмы и телевидение
Разрешить деньги
Разрешить новости
Разрешить OneDrive
Разрешить OneNote
Разрешить календарь и почту Outlook
Разрешить людям
Разрешить телефон
Разрешить фотографии
Разрешить Powerpoint
Разрешить настройки
Разрешить Skype
Разрешить спорт
Разрешить магазин
Разрешить диктофон
Разрешить кошелек
Разрешить погоду

Разрешить концентратор отзывов Windows
Разрешить слово
Разрешить Xbox

Настройка страниц
Разрешить учетные записи на рабочем месте
Разрешить расширенную информацию
Уголок разрешенных приложений
Разрешить блокировать и фильтровать
Разрешить цветовой профиль
Разрешить режим вождения
Разрешить электронную почту и учетные записи
Разрешить эквалайзер
Разрешить клавиатуру
Разрешить панель навигации
Разрешить сетевой авиарежим
Разрешить общий доступ к сети Интернет
Разрешить сетевые службы
Разрешить сеть Wi-Fi
Разрешить системе ПК Bluetooth
Разрешите оценить Ваше устройство
Разрешить восстановление обновления
Разрешить совместное использование
Разрешить запуск
Уделите время языку
Разрешить Время Регион
Разрешить экран блокировки Windows по умолчанию
Разрешить учетную запись на работе или в школе

Черные и белые списки

В разделе "Черный и белый список" Вы можете выбрать режим "Белый список" или режим "Черный список".

Белый список	Только те приложения и службы, которые добавлены в список, могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут активированы и установлены, чтобы пользователь мог их запускать.
	Все остальные приложения, не добавленные в список, не могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут деактивированы и установлены, так что пользователь не сможет их запустить.
Черный список	Приложения и службы, добавленные в список, не могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут деактивированы и настроены так, что пользователь не сможет их запустить.
	Все остальные приложения, не добавленные в список, могут быть установлены на устройство конечного пользователя. Если они уже предустановлены на устройстве конечного пользователя, они будут активированы и установлены, чтобы пользователь мог их запустить.

С помощью кнопки , Вы добавляете дополнительные приложения или службы в список используемых в данный момент.

С помощью кнопки , Вы добавляете дополнительные приложения или службы в список неактивных.

Вы можете добавить приложение из "Магазина приложений Windows" или напрямую ввести "Идентификатор приложения", чтобы добавить его в черный или белый список.

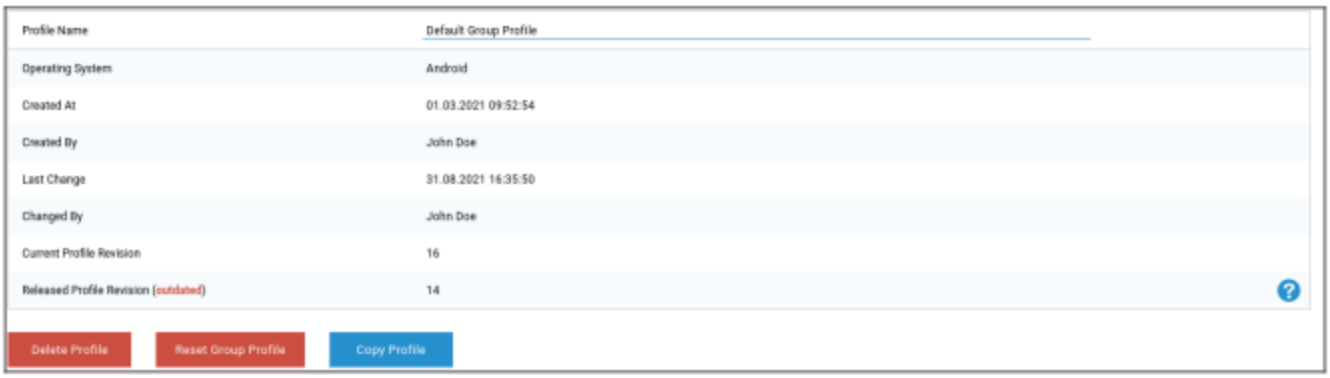
Конфигурация MacOS

В зависимости от того, выбрали ли Вы профиль или устройство, дисплей и его подпункты будут отличаться - обратите на это внимание!

Общие сведения

Обзор профиля группы (только на уровне группы)

Открыв профиль группы, Вы получите краткий обзор профиля.



Имя профиля	Название профиля (может быть изменено здесь)
Операционная система	Операционная система, для которой предназначен профиль
Создано в	Время создания
Created By	Создатель профиля
Последнее изменение	Время последнего изменения профиля
Изменено	Учетная запись, которая внесла последние изменения
Текущий пересмотр профиля	Пересмотр сохраненного состояния профиля
Выпущенный пересмотр профиля	Назначенная ревизия профиля ("Назначить сейчас"). Если за текстом на ярлыке отображается "(устаревший)", это означает, что Вы сохранили профиль, но еще не назначили его, поэтому устройства все еще будут получать старую версию.

Обзор устройства (только на уровне устройства)

Краткий обзор устройства.

Имя устройства	Имя устройства
Модель	Модель
Операционная система	Операционная система
Серийный номер	Серийный номер устройства
Владение устройством	Настроенный тип владения
Тип устройства	Тип устройства
Соответствующий	Показывает, соответствует ли устройство требованиям
IP-адрес	IP-адрес, с которого устройство подключено к серверу
Последний раз видели	Время последнего соединения с устройством
Последний рывок	Время последнего толчка, отправленного на устройство
Задание	Здесь Вы можете переместить устройство к другому пользователю или группе.

Пересмотр конфигурации (только на уровне устройства)

Здесь Вы получите обзор того, какой групповой профиль назначен устройству.

Если Вы нажмете на профиль группы, Вы получите прямой доступ к нему и сможете выполнить настройки.

С помощью этого символа Вы можете вернуть назначенные приложения к настройкам группового профиля.

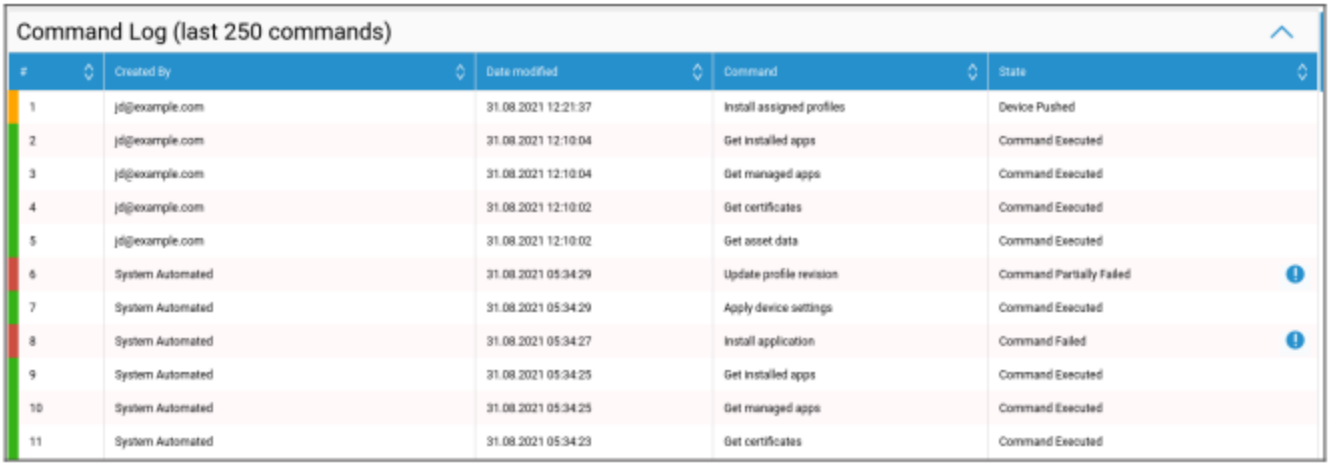
С помощью этого символа Вы можете сбросить профиль устройства, чтобы он вообще не имел никаких настроек.

"Доступна более новая редакция" означает, что профиль группы был изменен и сохранен, но не назначен. Чтобы применить изменения к устройствам, групповой профиль должен быть назначен с помощью "Назначить сейчас" на уровне группы.

Журнал устройства (только на уровне устройства)

Журнал команд

Здесь Вы можете увидеть, какие команды были отданы устройству и каков их статус.



Команды, созданные с помощью "System Automated", автоматически создаются системой.

Возможные статусы команд

Устройство нажимается	Запрос push был отправлен в службу push (например, APNS), чтобы сообщить устройству о необходимости подключиться обратно к серверу EMM.
Команда Создана	Команда была создана в системе.
Команда отправлена	Команда была отправлена на устройство после того, как оно подключилось к серверу.
Команда выполнена	Команда была успешно выполнена.
Команда не выполнена	Команда завершилась неудачно. *
Команда частично не выполнена	В зависимости от ОС устройства некоторые команды могут быть сгруппированы вместе. В этом случае некоторые части этой группы команд оказались неудачными. *
Команда выполнена, в итоге - отказ	Команда была выполнена, но, возможно, она не была выполнена.
Command Repushed	Команда была повторно запущена пользователем.
Выброшенные	Команда была отменена. Например, потому что она была заменена другой командой или устройство было перерегистрировано, и старые команды были удалены.

*Если за сообщением стоит восклицательный знак, Вы можете получить дополнительную информацию, наведя курсор на значок.

Управление активами (только на уровне устройств)

Информация об устройстве

Номер модели	Номер модели
Имя хоста	Имя хоста
Локальное имя хоста	Локальное имя хоста
Операционная система	Операционная система
Версия ОС	Версия ОС
UDID	UDID
Свободная / общая память	Свободная / общая память

WiFi

IP-адрес	IP-адрес
WiFi MAC	WiFi MAC

Клетчатка

Номер телефона	Номер телефона
Статус роуминга	Статус роуминга
Роуминг (голос / данные)	Роуминг (голос / данные)
IP-адрес	IP-адрес
Оператор/перевозчик	Оператор/перевозчик
Сеть оператора SIM	Сеть операторов связи
Версия для носителей	Версия для носителей
ICCID	ICCID
Текущий MCC/MNC	Текущий MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Управление обновлениями (только на уровне устройства)

Обновленная информация

На этой вкладке отображается информация о настройках обновления системы на устройстве.

Автопроверка включена	Если система проверяет наличие обновлений автоматически.
Автоматическое обновление приложений включено	Если система будет устанавливать обновления приложений автоматически.
Автоматическое обновление ОС включено	Если система будет устанавливать обновления os автоматически.
Автоматическое обновление системы безопасности включено	Если система будет устанавливать обновления безопасности автоматически.
Включена фоновая загрузка обновлений приложений	Если система будет загружать обновления приложений в фоновом режиме.
URL-адрес каталога	URL-адрес каталога обновлений программного обеспечения, который использует клиент.
Каталог по умолчанию	Если "да", то Catalog - это каталог по умолчанию.
Выполните периодическую проверку	Если "Да", начните новое сканирование.
Дата предыдущего сканирования	Дата последнего сканирования обновления программного обеспечения.
Предыдущий результат сканирования	Код результата последнего сканирования обновления программного обеспечения.

Управление безопасностью

Защита от краж

Вытрите и заблокируйте

Полное вытирание	Отправьте команду на сброс устройства к заводским настройкам
Enterprise Wipe	Удалите MDM с устройства и удалите все данные MDM (например, учетные записи, приложения).
Экран блокировки	Заставьте устройство вернуться на экран блокировки

Конфигурация безопасности

Пасскод

Разрешена деактивация кода	Определяет, должен ли пользователь вводить PIN-код. Простая установка этого значения (а не других) заставляет пользователя вводить код доступа, не устанавливая при этом его длину или качество.
Разрешить простое значение	Разрешите пользователю использовать одинаковые, возрастающие и уменьшающиеся строки номеров (например, 1234, 1111).
Требуется буквенно-цифровое значение	Пароли должны содержать хотя бы одну букву
Минимальная длина пароля	Минимальная длина пароля
Минимальное количество сложных символов	Минимальное количество буквенно-цифровых символов в пароле
Максимальный возраст пароля	Количество дней, по истечении которых пароль должен быть изменен
Максимальная автоблокировка	Максимальное время, по истечении которого устройство будет заблокировано
Максимальный льготный период для блокировки устройства	Сколько времени устройство может быть заблокировано без запроса пароля при разблокировке
Максимальный срок действия пароля (1-730 дней или нет)	Дни, по истечении которых пароль должен быть изменен
История паролей (1-50 паролей или ни одного)	Количество уникальных кодов до повторного использования

Сертификат

PKCS#1	
Описание	Введите описание для сертификата
Удостоверение	Загрузите файл pkcs1

PKCS#12	
Описание	Введите описание для сертификата
Кредит	Загрузить файл pkcs12

Настройки ограничений

Функциональность устройства

Разрешить камеру	Разрешите использовать фотоаппарат
Разрешить Game Center	Если значение false, Game Center отключается, а его значок удаляется с Главного экрана.
Разрешить многопользовательские игры	Если значение false, это запрещает многопользовательские игры.
Разрешите добавлять друзей из Game Center	Если значение false, это запрещает добавлять друзей в Game Center.
Разрешить фотобиблиотеку iCloud	Если установлено значение false, отключается iCloud Photo Library. Все фотографии, которые не были полностью загружены из iCloud Photo Library на устройство, будут удалены из локального хранилища.
Разрешить Touch ID	Если значение равно false, то Touch ID не сможет разблокировать устройство.

iCloud

Блокируйте определенные функции во время сопряжения с iCloud

Разрешите синхронизацию документов	Разрешите синхронизацию документов
Разрешить синхронизацию связки ключей iCloud	Разрешить синхронизацию связки ключей iCloud
Разрешить заметки iCloud	Если значение false, запрещает MacOS службы iCloud Notes.
Разрешить iCloud BTMM	Если значение равно false, это означает, что служба MacOS Back to My Mac iCloud запрещена.
Разрешить iCloud FMM	Если значение равно false, это означает, что служба iCloud MacOS Find My Mac запрещена.
Разрешить закладки iCloud	Если значение равно false, запрещается синхронизация закладок iCloud с MacOS.
Разрешить iCloud Mail	Если значение равно false, то запрещает MacOS Mail сервисы iCloud.

Разрешить календарь iCloud	Если значение равно false, это запрещает работу служб iCloud в MacOS Cloud.
Разрешить напоминания iCloud	Если значение равно false, это означает, что службы напоминаний iCloud запрещены.
Разрешить адресную книгу iCloud	Если значение равно false, это означает запрет на использование служб MacOS iCloud Address Book.

Управление средствами массовой информации

Извлечение при выходе из системы	Извлеките все съемные носители при выходе из системы
Разрешить сеть	Разрешите доступ для сетевых носителей
Разрешить внутренний диск	Разрешите доступ для внутреннего диска.
Требуется аутентификация	Требуется аутентификация для использования этого носителя
Только чтение	Пользователь может только считывать данные с носителя.
Разрешить внешний диск	Разрешите доступ для внешнего диска.
Требуется аутентификация	Требуется аутентификация для использования этого носителя
Только чтение	Пользователь может только считывать данные с носителя.
Разрешите использовать образы дисков	Разрешите доступ для изображений.
Требуется аутентификация	Требуется аутентификация для использования этого носителя
Только чтение	Пользователь может только считывать данные с носителя.
Разрешите использовать диски DVD-RAM	Разрешите доступ для диска DVD-RAM.
Требуется аутентификация	Требуется аутентификация для использования этого носителя
Только чтение	Пользователь может только считывать данные с носителя.
Разрешите использование DVD-дисков	Разрешите доступ к DVD-диску.
Требуется аутентификация	Требуется аутентификация для использования этого носителя
Разрешите использовать компакт-диски	Разрешите доступ к CD-диску.

Требуется аутентификация	Требуется аутентификация для использования этого носителя

Управление соединениями

Wi-Fi

Здесь Вы можете добавлять и настраивать Wi-Fi соединения

Идентификатор набора услуг (SSID)	SSID сети, к которой будет установлено соединение
Автоматическое присоединение	Включите автоматическое присоединение к сети
Скрытая сеть	Включить, в случае, если точка доступа не передает SSID
Настройка прокси	Настройка прокси для каждой точки доступа
Нет	Не используйте прокси-сервер
Руководство	Установите ручной прокси-сервер
URL-адрес прокси-сервера	Адрес для доступа к настройкам прокси-сервера
Порт	Установите порт для прокси-сервера
Аутентификация	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Автоматический	Установите прокси автоматически
URL-адрес прокси-сервера	URL-адрес файла настроек прокси-сервера
Тип безопасности	Установите тип безопасности для точки доступа
WEP	
Пароль	Пароль для точки доступа
WPA/WPA2	
Пароль	Пароль для точки доступа
WEP Enterprise - WPA / WPA2 Enterprise / Любое предприятие	См. таблицу Ошибка: Источник ссылки не найден
Нет	Не создавайте никакой безопасности
Отключите рандомизацию MAC-	Отключает рандомизацию MAC-адресов для данной сети Wi-Fi, пока она ассоциирована с ней. При этом также появляется предупреждение о

адресов	конфиденциальности в Настройках, указывающее на то, что сеть имеет пониженную защиту конфиденциальности.

Конфигурация Wi-Fi на предприятии

Примечание: Доступно только в том случае, если для параметра "Тип безопасности" установлено значение "Тип предприятия".

Протоколы	Протокол аутентификации, поддерживаемый в целевой сети
TLS	Включить / Выключить использование
TTLS	Включить / Выключить использование
Внутренняя аутентификация	Протокол аутентификации, который должен быть использован: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Включить / Выключить использование
PEAP	Включить / Выключить использование
EAP-FAST	Включить / Выключить использование
EAP-SIM	Включить / Выключить использование
Используйте PAC	Использование PAC (защищенный контроль доступа)
Положение PAC	Конфигурация Provision PAC
Предоставление PAC анонимно	Анонимное предоставление PAC
Аутентификация	
Имя пользователя	Имя пользователя для аутентификации
Не используйте За подключение Пароль	Не используйте пароль для каждого соединения
Пароль	Пароль для использования
Сертификат личности	Загрузите/выберите сертификат аутентификации
Внешняя идентичность	Идентичность, которую можно увидеть снаружи
Trust	
Доверенный сертификат 1	Загрузите первый доверенный сертификат
Доверенный сертификат 2	Загрузите второй доверенный сертификат

Доверенный сертификат 3	Загрузите третий доверенный сертификат
Доверенный сервер Имена сертификатов	Имена ожидаемых сертификатов сервера (в списке, разделенном запятыми)

VPN

В зависимости от выбранного типа соединения, могут быть видны разные поля.

Имя соединения	Имя VPN-профиля
Тип VPN	
VPN	Весь сетевой трафик устройства будет направляться через VPN-соединение.
Тип соединения	Установите тип VPN-соединения
IPsec (cisco)	Протокол IPsec от компании cisco
L2TP	Протокол L2TP
Пользовательский SSL	Подключение через пользовательский SSL
IKEv2	Протокол IKEv2
Настройка прокси	Настройка прокси для VPN-соединения
Нет	Установить отсутствие прокси
Руководство	Установите прокси вручную
URL-адрес прокси-сервера	Адрес для доступа к настройкам прокси-сервера
Порт	Установите порт для прокси-сервера
Аутентификация	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Автоматический	Установите прокси автоматически
URL-адрес прокси-сервера	URL для доступа к настройкам прокси-сервера

HTTP-прокси

Тип прокси	
Руководство	Установите прокси вручную
URL-адрес прокси-сервера	Адрес для доступа к настройкам прокси-сервера
Порт	Установите порт прокси-сервера
Аутентификация	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Автоматический	Установите прокси автоматически
URL прокси PAC	URL прокси PAC
Разрешите прямое соединение, если PAC недоступен	Разрешите прямое соединение (без VPN), если PAC недоступен
Позволяет обходить прокси-сервер для доступа к сетям захвата	Позволяет обходить прокси для доступа к внутренним сетям.

AirPrint

IP-адрес	IP-адрес принтера
Путь к ресурсам	Определенный путь к устройству AirPrint

AirPlay

Имя устройства	Имя устройства
Пароль	Пароль сопряжения
Белый список	Определите список устройств, с которыми устройство может сопрягаться исключительно

Управление PIM

Exchange Active Sync

Название счета	Название счета.
Адрес электронной почты	Адрес счета (например, max@company.com)
Имя хоста сервера	Внутреннее имя хоста
Имя пользователя	"Домен" и "Имя входа" должны быть пустыми, чтобы устройство запрашивало пользователя.
Домен	"Домен" и "Имя входа" должны быть пустыми, чтобы устройство запрашивало пользователя. Если конфигурация шлюза ACL включена и поле "Домен" не пустое, универсальный шлюз AppTec360 будет аутентифицировать устройство со следующим именем "Domain\Login Name".
Пароль	Пароль для учетной записи (например, secretUserPassword)
Прошлые дни Mail to Sync	Количество последних дней почты, которую нужно синхронизировать
Используйте SSL	Используйте SSL для внутреннего хоста Exchange
Расширенный вариант	Показать дополнительные опции
Порт сервера	Внутренний порт
Путь к серверу	Внутренний путь
Имя внешнего хоста	Внешний хозяин
Внешний порт	Внешний порт
Внешний путь	Внешний путь
Используйте SSL для внешних Exchange Host	Используйте SSL для внешнего хоста Exchange

eMail

Настройка учетных записей POP3 / IMAP на устройстве конечного пользователя

Описание счета	Учетные записи электронной почты
Тип счета	
IMAP	
Префикс пути	Префикс пути для специальных папок
POP	
Отображаемое имя пользователя	Отображаемое имя пользователя
Адрес электронной почты	Адрес электронной почты пользователя

Входящая почта	Настройки сервера входящих сообщений
Адрес почтового сервера	Адрес почтового сервера
Порт почтового сервера	Порт почтового сервера
Имя пользователя	Соответствующее имя пользователя
Тип аутентификации	Тип аутентификации
Нет	Нет Тип аутентификации
Пароль (только на уровне устройства)	Запрос пароля
MDM Challenge-Response	
NTLM	NTLM-аутентификация
HTTP MD5 Digest	
Используйте SSL	Используйте SSL, если необходимо

Исходящая почта	Настройки исходящего сервера
Адрес почтового сервера	Адрес почтового сервера
Порт почтового сервера	Порт почтового сервера
Имя пользователя	Соответствующее имя пользователя
Тип аутентификации	
Нет	Нет метода аутентификации
Пароль (только на уровне устройства)	Запрос пароля
MDM Challenge-Response	
NTLM	NTLM-аутентификация
HTTP MD5 Digest	
Используйте SSL	Используйте SSL, если необходимо
Исходящий пароль такой же, как и входящий	Исходящий пароль такой же, как и входящий
Используйте только в почтовых отправлениях	Активировать, если все исходящие сообщения электронной почты должны отправляться через Mail-App

CalDav

Настройка и распределение учетной записи CalDav

Описание счета	Отображаемое имя учетной записи
Имя хоста	Имя хоста и/или IP-адрес
Порт	Порт учетной записи CalDav
Основной URL	Основной URL-адрес счета
Имя пользователя	Соответствующее имя пользователя CalDav
Пароль (только на уровне устройства)	Соответствующий пароль CalDav
Используйте SSL	Используйте SSL, если необходимо

CardDav

Настройка и распределение учетной записи CardDav

Описание счета	Отображаемое имя учетной записи
Имя хоста	Имя хоста и/или IP-адрес
Порт	Порт учетной записи CardDav
Основной URL	Основной URL-адрес счета
Имя пользователя	Соответствующее имя пользователя CardDav
Пароль (только на уровне устройства)	Соответствующий пароль CardDav
Используйте SSL	Используйте SSL, если необходимо

LDAP

В этой области настройте LDAP-соединение, чтобы обеспечить динамический обмен сертификатами между устройством конечного пользователя и Active Directory.

Обратите внимание, что выбранному пользователю требуется соответствующее разрешение на чтение.

Описание счета	Описание счета
Имя пользователя аккаунта	Пользователь для LDAP-доступа
Пароль учетной записи	Пароль для LDAP-доступа
Имя хоста учетной записи	Имя хоста/IP-адрес сервера LDAP
Используйте SSL	Используйте SSL, если необходимо

Во второй части Вы можете определить индивидуальные фильтры для поиска в реестре LDAP.

Описание	Область применения	База поиска
Описание фильтра	Уровень поиска в реестре LDAP	Определите индивидуальный фильтр

Приборная панель и отчетность

Настройки приборной панели

Здесь Вы можете посмотреть, какие приборные панели существуют, отредактировать их или создать новые. Каждая приборная панель имеет свой собственный набор данных для отображения и конфигурацию графиков.

Управление настройками приборной панели

Общественность	Устанавливает приборную панель публичной, чтобы другие пользователи могли видеть ее. Разумеется, пользователи должны иметь возможность входить в систему и просматривать приборные панели. Если опция "Public" не активирована, её может видеть только создатель.
По умолчанию	Установите приборную панель по умолчанию, чтобы она автоматически открывалась при следующем обращении к представлению приборной панели.
	Покажите приборную панель и ее графики
	Удалить приборную панель
	Редактирование названия и настроек приборной панели
	Сделайте копию приборной панели
	Добавьте совершенно новую приборную панель

Вид приборной панели

Здесь показаны данные и графики выбранной приборной панели, а также Вы можете их изменить.

Управление приборной панелью

	Позволяет Вам определить, какие данные будут отображаться на приборной панели, в каком количестве и в каком размере показывать эти данные.
	Возвращает Вас к обзору приборной панели
	Сбросьте открытую в данный момент приборную панель на панель по умолчанию
	Сохраняет все изменения, которые Вы внесли в открытую в данный момент панель (например, какие данные показывать).
	Измените тип графика на столбчатый
	Измените тип диаграммы на круговую диаграмму
	Измените тип графика на график пончика
	Измените тип графика на график полярной области
	Измените порядок сортировки

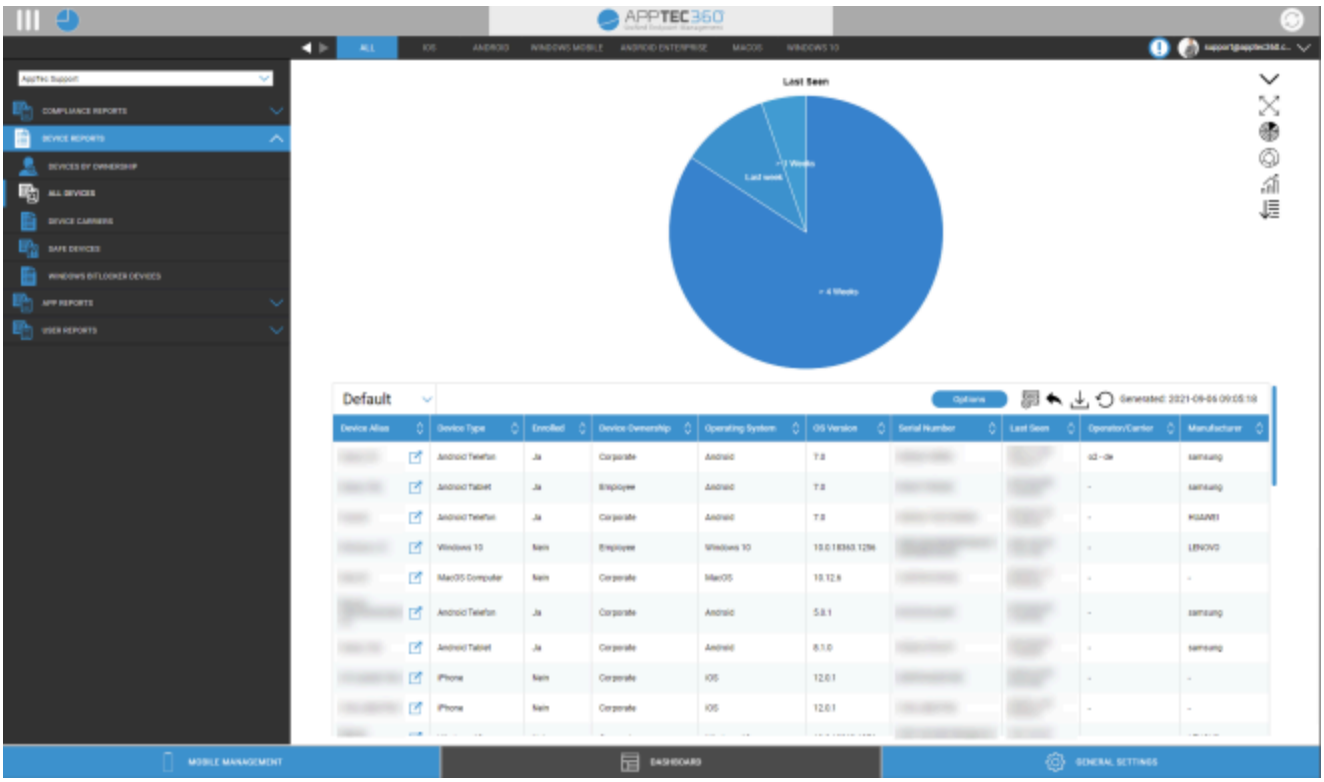
Расширенная отчетность

Расширенная отчетность" предлагает подробные обзоры и графики информации об устройствах и пользователях.

Есть несколько отчетов по умолчанию, но все они могут быть изменены вручную, чтобы добавить или удалить данные для показа.

Обратите внимание, что Вы можете только вручную изменить, какие данные будут показаны. Выбранная категория отчета определяет, на каких данных он основан. Например, Вы никогда не сможете увидеть устройства Android в отчете по iOS в Device Reports All Devices iOS.

В левом верхнем углу Вы можете ограничить данные отчетов определенной группой (и всеми ее подгруппами). По умолчанию эта группа установлена для Вашего корневого узла, поэтому учитываются ВСЕ устройства и пользователи.



Расширенное управление отчетностью

В каждом обзоре Вы можете использовать следующие функции, чтобы изменить отчет так, как Вы хотите:

	Скрыть график (если график показан)
	Показать график (если график скрыт)
	Разверните график (если график свернут).
	Сверните график (если график развернут)
	Измените тип графика на столбчатый
	Измените тип диаграммы на круговую диаграмму
	Измените тип графика на график пончика
	Измените тип графика на график полярной области
	Измените порядок сортировки
	Измените следующие детали отображаемого обзора: • Добавление/удаление колонок • Укажите порядок, в котором будут отображаться колонки • Показать/скрыть график над таблицей • Выберите колонку, которая будет использоваться для графика • Отфильтруйте данные Вашей таблицы
	Откройте менеджер настроек, чтобы сохранять и загружать различные отчеты
	Сбросьте текущий открытый Отчет на значение по умолчанию
	Экспортируйте текущий отчет в файл .csv
	Регенерируйте данные и перезагрузите текущий отчет

Список всех отчетов по умолчанию Вы найдете на следующих страницах.

Отчеты о соответствии

Откорректированные устройства

Обзор устройств, которые были рутированы/взломаны.

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта
Операционная система
Номер телефона
Последний раз видели
Производитель

Роуминговые устройства

Обзор всех устройств, которые находятся в роуминге

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта
Тип устройства
Операционная система
Номер телефона
Последний раз видели

Устройства с поддержкой роуминга

Обзор всех устройств, которые активировали роуминг, но не обязательно находятся в роуминге в данный момент.

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта
Тип устройства
Операционная система
Номер телефона
Последний раз видели

Контролируемые устройства

Обзор всех устройств, которые находятся под наблюдением в режиме наблюдения (только для iOS)

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта
Тип устройства
Последний раз видели

Неактивные устройства

Обзор всех устройств, которые не подключались к серверу в течение последних 7 дней

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта
Тип устройства
Операционная система
Последний раз видели

Отчеты об устройствах

Устройства по владению

Здесь Вы можете увидеть, сколько устройств на данный момент развернуто в качестве корпоративных (корпоративные устройства) и личных (личные устройства).

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Тип устройства
Владение устройством
Операционная система

Все устройства

Здесь Вы можете увидеть обзор всех устройств с наиболее важной информацией.

Колонки по умолчанию этого отчета:

Псевдоним устройства
Тип устройства
Записался
Владение устройством
Операционная система
Версия ОС
Серийный номер
Последний раз видели
Оператор/перевозчик
Производитель

Носители устройств

Здесь Вы можете посмотреть обзор, касающийся оператора (провайдера сотовой связи).

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта
Операционная система
Версия ОС
Оператор/перевозчик

Устройства SAFE

Здесь Вы можете посмотреть обзор того, какие устройства используют SAFE Version.

Поскольку обзор и/или SAFE доступен только для устройств Samsung, Вы не увидите привычных вкладок в этом пункте.

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта
Тип устройства
Последний раз видели
Версия SAFE

Устройства Windows BitLocker

Здесь Вы можете посмотреть обзор устройств Windows, на которых используется BitLocker.

Колонки по умолчанию этого отчета:

Псевдоним устройства
Владелец устройства
Электронная почта

Состояние BitLocker

Отчеты о приложениях

Здесь Вы получите разнообразные обзоры по приложениям. Во всех этих отчетах Вы можете щелкнуть по записи, чтобы посмотреть, какие версии установлены на устройствах и как часто. В этом обзоре Вы можете снова щелкнуть на конкретной версии, чтобы увидеть, на каких устройствах установлена эта версия.

Примечание: Может пройти некоторое время, пока система получит актуальную информацию от устройства. Кроме того, отчеты не обновляются каждую минуту. Вам может потребоваться терпение, чтобы увидеть текущий статус, если Вы только что назначили новое приложение или версию. Ручная перезагрузка отчета заставит его отобразить самые актуальные данные.

Установленные приложения

Здесь Вы получите обзор всех установленных приложений.

Колонки по умолчанию этого отчета:

Имя	Название соответствующего приложения и/или сервиса
Идентификатор	Определенный идентификатор приложения/сервиса
Общее количество	Как часто это приложение / сервис устанавливалось на устройствах конечных пользователей

Самые устанавливаемые приложения

Здесь Вы получите обзор приложений, которые были установлены чаще всего.

Колонки по умолчанию этого отчета:

Имя	Название соответствующего приложения и/или сервиса
Идентификатор	Определенный идентификатор приложения/сервиса
Общее количество	Как часто это приложение/сервис устанавливалось на устройствах конечных пользователей

Обязательные приложения

Здесь Вы получите обзор обязательных (требуемых в обязательном порядке) приложений.

Колонки по умолчанию этого отчета:

Имя	Название соответствующего приложения и/или сервиса
Идентификатор	Определенный идентификатор приложения/сервиса
Источник приложений	Какой AppStore участвует: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Операционная система

Приложения в черном списке

Здесь Вы получите обзор всех определенных приложений, внесенных в черный список.

Колонки по умолчанию этого отчета:

Имя	Название соответствующего приложения и/или сервиса
Идентификатор	Определенный идентификатор приложения/сервиса
Источник приложений	Какой AppStore участвует: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Операционная система

Отчеты пользователей

Тариф

Здесь Вы получите обзор телефонных тарифов и SIM-карт Ваших пользователей.

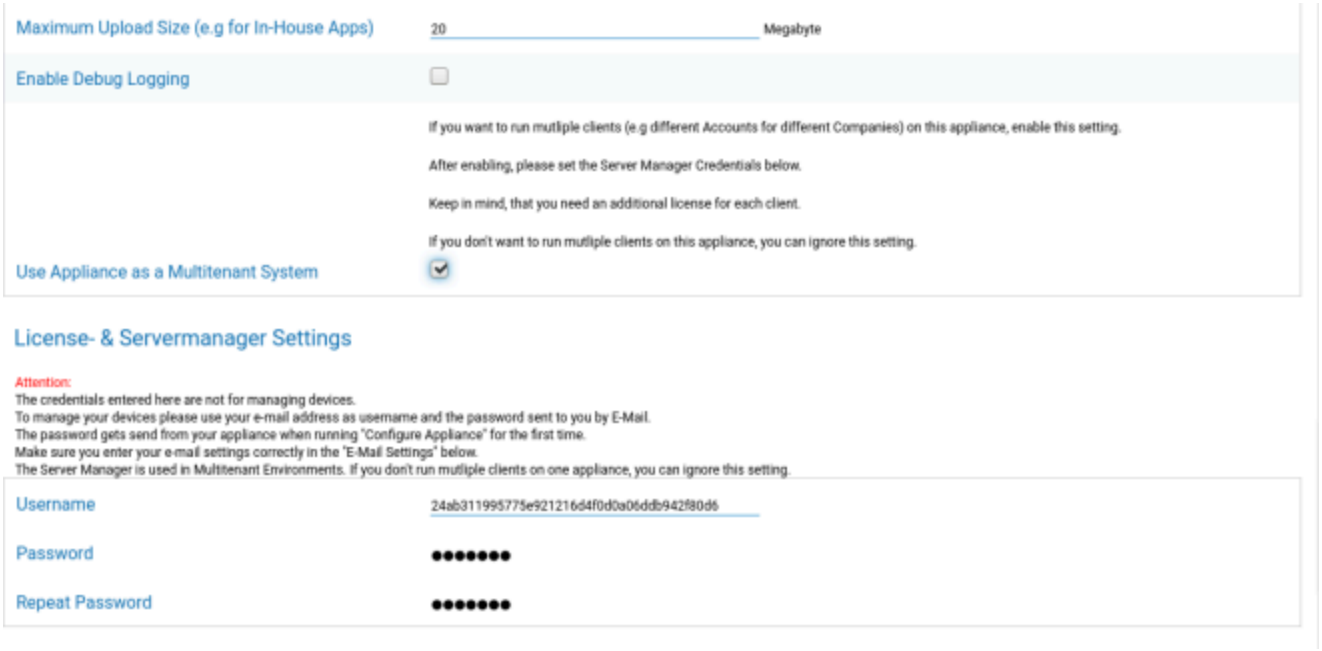
Колонки по умолчанию этого отчета:

Электронная почта
Имя
phoneNumber
носитель
тариф
вариант
цена
контрактОтменен
contractStart
duringTime
mobileAndData
dataVolume
multiSIM
тип
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
Примечание

Управление несколькими арендаторами

AppTec360 EMM может содержать несколько отдельных арендаторов, каждый со своими пользователями и группами, разрешениями и глобальными настройками.

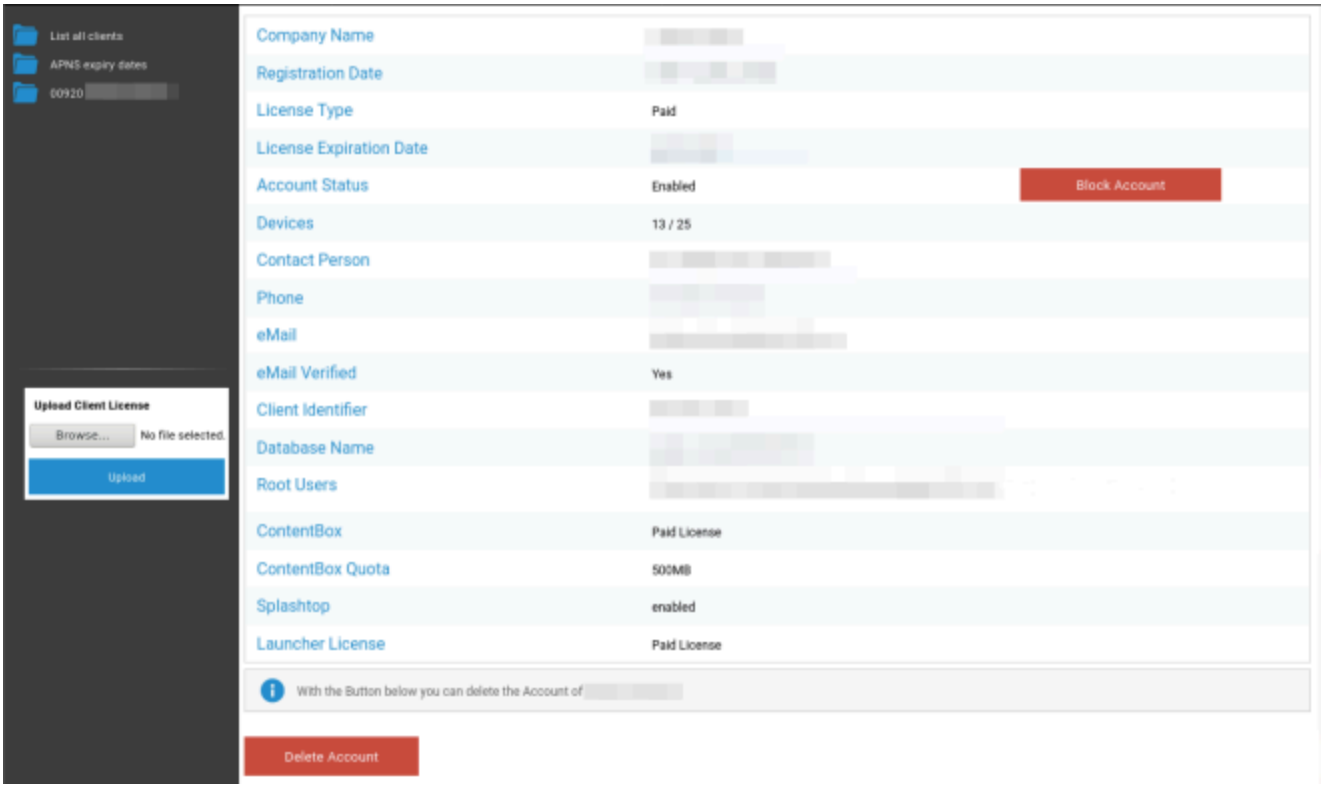
Чтобы включить возможности Multitenant, Вам необходимо включить их в интерфейсе конфигурации устройства в разделе "Шаг третий - Настройки сервера".



В новом меню задайте имя пользователя и пароль для Servermanager. Сохраните настройки и выполните команду "Configure Appliance" в разделе "Шаг пятый - Лицензионное соглашение", чтобы применить настройки.

Когда настройка будет завершена, Вы сможете войти в систему с заданными учетными данными через обычный интерфейс Mobile Management.

После входа в систему Вы можете увидеть следующий вид.



Слева Вы можете увидеть всех арендаторов (в данном случае только одного с id 920), а справа - информацию об этом клиенте. У Вас также есть возможность заблокировать доступ к аккаунту, а также удалить клиента (ВНИМАНИЕ: при этом будут удалены все данные, связанные с этим клиентом).

Слева Вы можете загрузить новую клиентскую лицензию, которая может быть либо обновлением лицензии для существующего клиента, либо новой лицензией, автоматически создающей нового клиента. При создании нового клиента письмо с паролем для входа в систему автоматически отправляется на адрес электронной почты, на который была выдана лицензия.

Чтобы получить новую или обновленную клиентскую лицензию (например, если требуется больше лицензий на устройства), свяжитесь с Вашим торговым представителем.

Дополнительные виды

Перечислите всех клиентов

Показывает обзор всех клиентов в системе.

ID клиента	ID клиента
Идентификатор	Идентификатор клиента
База данных	База данных
Название компании	Название компании
eMail	Контактное лицо eMail
Проверено	Проверена ли электронная почта контактного лица или нет
Страна	Страна
Устройства	Количество зарегистрированных устройств
Дата регистрации	Точка во времени назначения лицензии
Последний вход в систему	Последний вход в учетную запись администратора
Лицензия	Отображение типа лицензии (Бесплатная|Платная)
Лицензия CB	Тип лицензии ContentBox (Free|Paid)
Статус	Текущий статус AppTec-Client
Просроченный	Отображается, если срок действия лицензии истек
iOS	Количество устройств iOS
Android	Количество устройств Android
Windows Mobile	Количество устройств Windows Mobile
MacOS	Количество устройств MacOS
Windows 10	Количество устройств с Windows 10
Android Enterprise	Количество корпоративных устройств Android
IOS BYOD (регистрация пользователей)	Количество устройств IOS BYOD (регистрация пользователей)
IoT	Количество устройств IoT

Сроки годности APNS

Показывает обзор всех дат истечения срока действия сертификатов APNS для всех клиентов.

ID клиента	ID клиента
Название компании	Название компании
Дата истечения срока действия	Дата истечения срока действия APNS-сертификата Apple
Информация	Информация об истечении срока действия

Свяжитесь с

Дополнительные вопросы? Просто свяжитесь с нами по ссылке:

Для общих технических вопросов

support@apptec360.com

+41 61 511 3210

Для вопросов, связанных с установкой виртуального устройства

consulting@apptec360.com

+41 61 511 3214

Отказ от ответственности