IBM MaaS360 Mobile Device Management for iOS

Предоставление, управление и защита новых устройств, приложений и контента iOS

Основные преимущества

- Предоставление, защита и управление устройствами, приложениями и контентом из одной консоли
- Беспроводная настройка электронной почты, календаря, списка контактов, профилей Wi-Fi и VPN для быстрого подключения пользователей
- Поддержка в день выпуска новых версий мобильных операционных систем для устройств iOS
- Настройка политик безопасности и их реализация с помощью автоматических действий по обеспечению соответствия, таких как требование пароля к устройству и блокировка скомпроментированного устройства
- Использование надежных инструментальных панелей и отчетов для управления корпоративными и личными устройствами

Apple + IBM® MaaS360® = лучше работают вместе

Apple продолжает внедрять инновации в области корпоративных технологий, благодаря которым iOS 9 стала мощной офисной платформой. И MaaS360 обеспечивает быструю и надежную поддержку iOS 9 и предыдущих версий. Работая совместно, Apple и IBM помогают организациям использовать весь потенциал мобильных устройств и приложений для своих сотрудников, клиентов и партнеров.

Можно развернуть устройства и выполнять обновление до последней версии iOS мгновенно и легко в день выпуска компанией Apple, не нарушая работу пользователей и не создавая проблем для ИТ-персонала. Не окажитесь на обочине вместе с другими поставщиками систем управления мобильными устройствами (MDM); воспользуйтесь множеством новых возможностей iOS 9 с помощью MaaS360 уже сегодня!

Моментальное управление Apple iOS

IBM MaaS360 for iOS обеспечивает обширный обзор и контроль для устройств iPhone и iPad на предприятии, поддерживая iOS 4.3 и более поздних версий. Сегодня поддерживается версия iOS 9 и предоставляются инструменты, с помощью которых можно проводить анализ, выполнять действия, настраивать и распространять политики, управлять приложениями и документами и так далее.

Решение предоставляет быстрый и легкий способ для защиты этих устройств и содержащихся на них корпоративных данных. Можно развертывать их по беспроводной сети и использовать политики безопасности и правила соответствия нормативным требованиям, чтобы обеспечить использование паролей и шифрования, обнаруживать устройства с несанкционированно измененной микропрограммой и ограничивать их использование, создавать белые и черные списки приложений, управлять резервным копированием файлов и так далее.

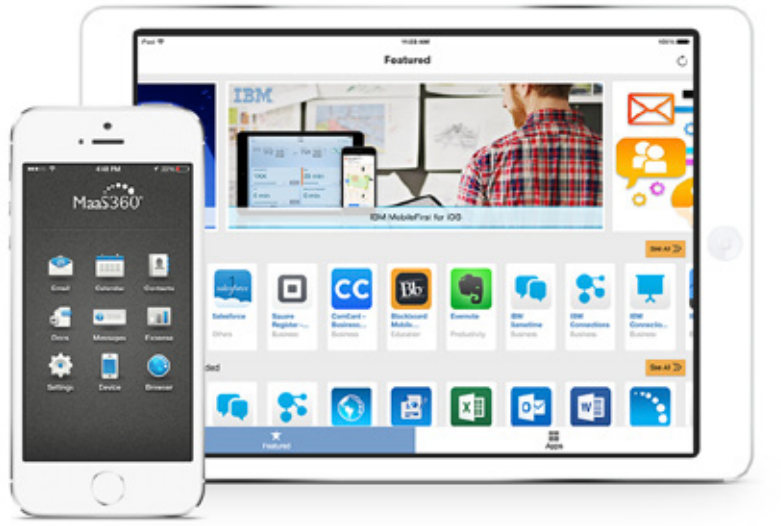

Рис. 1. Простое развертывание приложений и контента для устройств iOS организации

Анализ информации

- Модель, серийный номер, операционная система
- Домашняя/текущая сеть
  - Статус роуминга, MAC-адрес
- Объем свободной памяти
- Приложения, версии и размер
- ИД устройства (номер телефона, IMEI, адрес электронной почты)
  - Уровень шифрования, обнаружение несанкционированного изменения микропрограммы, статус пароля, ограничения устройства,установленные профили, политики безопасности и так далее
- Использование DEP для автоматического развертывания конфигураций и политик на принадлежащих предприятию устройствах во время активации
- Включена функция Activation Lock в Find My iPhone, закрепляющая устройство за ИД Apple пользователя
- Отправка сообщения в случае, если на устройстве существует учетная запись iTunes
- Просмотр подробной отчетности по документам, пользователям, устройствам, приложениям и так далее

Выполнение действий

- Настройка параметров и профилей Wi-Fi, VPN и электронной почты
- Обнаружение, вызов, блокировка устройства или сброс забытых паролей
- Выборочная очистка корпоративных данных при сохранении личных данных на устройстве, принадлежащем сотруднику
- Выполнение полной очистки утерянного или украденного устройства
- Изменение политики iOS
- Включение и отключение средств управления роумингом голоса и данных

Каталог корпоративных приложений

- Управление корпоративными приложениями: полное управление мобильными приложениями, распространяемыми MaaS360 на устройства iOS; развертывание приложений упрощается, а безопасность улучшается
  - Рекомендации приложений iTunes для сотрудников
  - Распространение собственных приложений и публикация обновлений
  - Удаленное развертывание приложения на устройстве; бесшумная установка на контролируемых устройствах
  - Управление средствами контроля Open In, чтобы ограничить открытие файлов из корпоративных приложений в личных и наоборот
  - Подключение управляемых приложений к VPN для обеспечения защищенного доступа к сети
  - Поддержка единого входа в систему в рамках всех приложений для аутентификации
  - Автоматическое применение шифрования для данных сторонних приложений
- Поддержка Apple VPP
  - Распространение и установка заранее оплаченных приложений без входа в Apple App Store
  - Экономия средств благодаря сохранению полного владения и управления лицензиями VPP на приложения и книги, когда пользователям они больше не нужны

Настройка и распространение политик

- Обеспечение выполнения требований к паролям
- Настройка ограничений для устройств
  - Обеспечение создания зашифрованных резервных копий
  - Ограничение использования камеры, FaceTime, Touch ID и так далее
  - Ограничение установки приложений, использования общего фотопотока (Photo Stream) и так далее
  - Принудительная отправка интернет-трафика через глобальный прокси-сервер HTTP
  - Распространение профилей Wi-Fi, VPN и электронной почты, например параметров Exchange ActiveSync
- Управление средствами контроля iCloud
  - Управление резервным копированием документов, данных приложений и устройств и синхронизацией фотографий с iCloud для пользователя, группы или всех устройств
- Повышение безопасности электронной почты
  - Ограничение передачи пользователями сообщений электронной почты между учетными записями; это помогает обеспечить защиту от утечки корпоративных данных
  - Предотвращение отправки сообщений электронной почты сторонними приложениями
- Расширенная настройка Wi-Fi
  - Управление настройками прокси-сервера и их распространение, а также автоматическое соединение с идентификатором SSID
- Обязательное использование паролей iTunes
  - Требование ввода паролей пользователей iTunes для доступак контенту, приложениям и данным в iTunes
- Отправка сообщения и номера на экран блокировки в случае утери устройства
- Поддержка функции Handoff, которая обеспечивает непрерывность работы, просмотр веб-результатов в Spotlight и синхронизацию с iCloud для управляемых приложений

Поддержка в день выпуска новых версий

iOS 9 и MaaS360 совместно готовы обеспечить совершенно новый уровень безопасности, эффективности работы и функций управления устройствами и данными, которые помогут вашей организации сделать очередной шаг в области мобильности.

Новые функции iOS 9 для обеспечения корпоративной безопасности

- Ограничение AirDrop для управляемых приложений и библиотеки iCloud Photo Library
- Настройка новых ограничений в контролируемом режиме (Supervised) для использования магазина приложений App Store, ярлыков клавиатуры, Apple Watch, изменения пароля, автоматической загрузки приложений и так далее
- Выключение доверительного выполнения корпоративных приложений на контролируемых устройствах

Новые функции распространения приложений iOS 9

- Распространение приложений на основе устройства развертывает приложения непосредственно на устройствах, используя программу оптовой покупки (VPP) и MaaS360 для назначения приложений устройству с данным серийным номером, не требуя ИД Apple
- Установка общедоступных приложений на большом количестве устройств («push») или по запросу («pull»), не требуя доступа пользователя к магазину App Store
- Корпоративные приложения, устанавливаемые с помощью MaaS360, являются очевидно доверенными и не требуют подтверждения доверенности со стороны пользователя
- Если приложения были установлены на устройстве до его передачи под управление, то когда устройство станет контролируемым, управление ими будет осуществляться незаметно
- Приложения, приобретенные и распространяемые посредством VPP, могут назначаться устройствам или пользователям в любой стране, где эти приложения доступны

Новые функции iOS 9 для управления устройствами и данными

- MaaS360 может инициировать обновление любых устройств в программе Device Enrollment Program (DEP) до новых версий iOS
- С помощью Apple Configurator можно заранее развертывать приложения и обеспечить потоковое развертывание на устройствах с помощью MaaS360 по программе DEP
- VPN на основе приложений поддерживает UDP и TCP для потоковой загрузки аудио и видео

Чтобы узнать подробнее о решении IBM MaaS360 и начать 30-дневный бесплатный период пробного использования, посетите веб-сайт www.**ibm.com**/maas360

IBM Восточная Европа/Азия
123317, Москва
Пресненская наб., 10
Тел.: +7 (495) 775-8800
Факс: + 7 (495) 258-6468, 258-6404
ibm.com/ru

Произведено в США.
Апрель 2016 г.

Подлежит переработке и вторичному использованию

WGD03066-RURU-00