За гранью AppStore

MDM, Supervised и другие возможности для разработки в бизнес-сегменте

Кудинов Денис

@kudinovdw

@kudinovdenis

kaspersky

План встречи

Кому полезен этот доклад

Профили конфигурации

Mobile Device Management

Supervised-режим

BYOD-режим

Кому это может пригодиться?

Разработчики B2B iOS приложений

Product-owner

Backend разработчики

Разработчики B2C iOS приложений

План встречи

Кому полезен этот доклад

Профили конфигурации

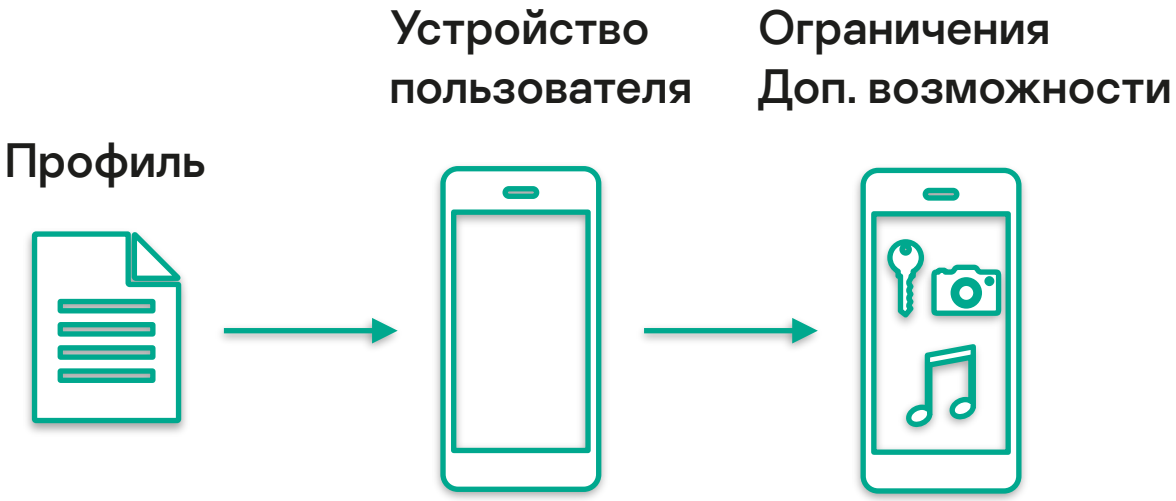
Mobile Device Management

Supervised-режим

BYOD-режим

Configuration profiles

Configuration profile



Configuration Profile

Введение

XML-файл

Содержит политики для управления устройством

Пароли
Сети Wi-Fi
Принтеры
VPN
Контакты
Сертификаты
...

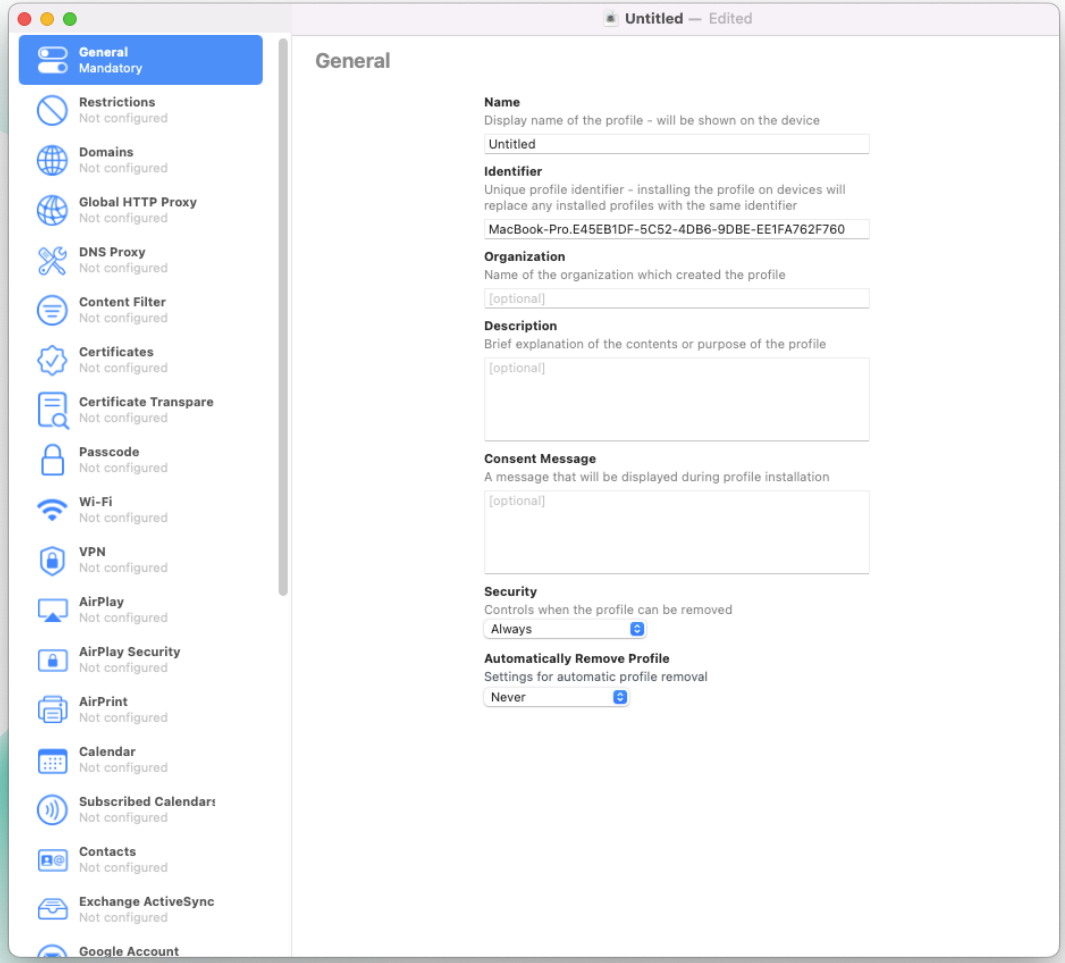
Configuration Profile

Способы создания

Apple configurator

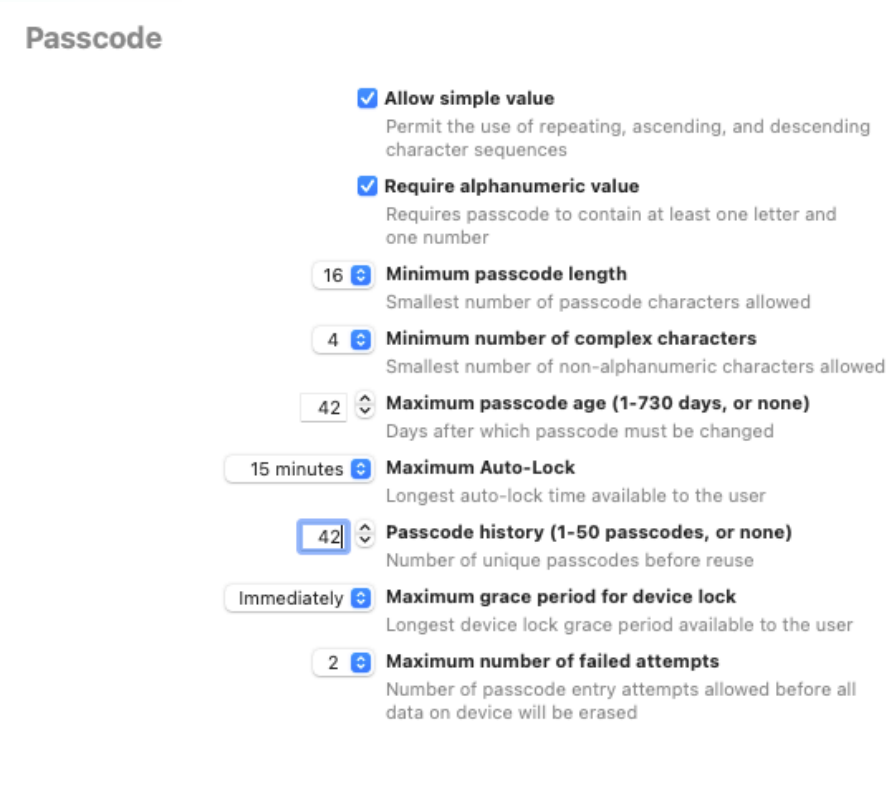
Создать XML руками

Apple configurator



Apple configurator

Политика пароля



Configuration Profile

Способы создания

Apple configurator

Создать XML руками

Создание XML руками

Политика пароля

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist … >
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            ...
        </dict>
    </array>
    <key>PayloadDisplayName</key>
    <string>Untitled</string>
    <key>PayloadIdentifier</key>
    <string>MacBook-Pro….</string>
    <key>PayloadRemovalDisallowed</key>
    <false/>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>3DD756B4-52D5-4416-8F4D-5C167BD2AA68</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
</plist>
```

Создание XML руками

Политика пароля

```xml
<key>PayloadContent</key>
<array>
    <dict>
        <key>PayloadDescription</key>
        <string>Configures passcode settings</string>
        <key>PayloadDisplayName</key>
        <string>Passcode</string>
        <key>PayloadIdentifier</key>
        <string>com.apple.mobiledevice.passwordpolicy….>
        <key>PayloadType</key>
        <string>com.apple.mobiledevice.passwordpolicy</string>
        <key>PayloadUUID</key>
        <string>24A53A9C-C449-4500-AA10-99044DEB514D</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>allowSimple</key>
        <true/>
        <key>forcePIN</key>
        <true/>
        <key>maxFailedAttempts</key>
        <integer>2</integer>
        <key>maxGracePeriod</key>
        <integer>0</integer>
        <key>maxInactivity</key>
        <integer>15</integer>
        <key>maxPINAgeInDays</key>
        <integer>42</integer>
        <key>minComplexChars</key>
        <integer>4</integer>
        <key>minLength</key>
        <integer>16</integer>
        <key>pinHistory</key>
        <integer>42</integer>
        <key>requireAlphanumeric</key>
        <true/>
    </dict>
</array>
```

Configuration Profile

Как установить на устройство?

Apple Configurator

Скачать по ссылке

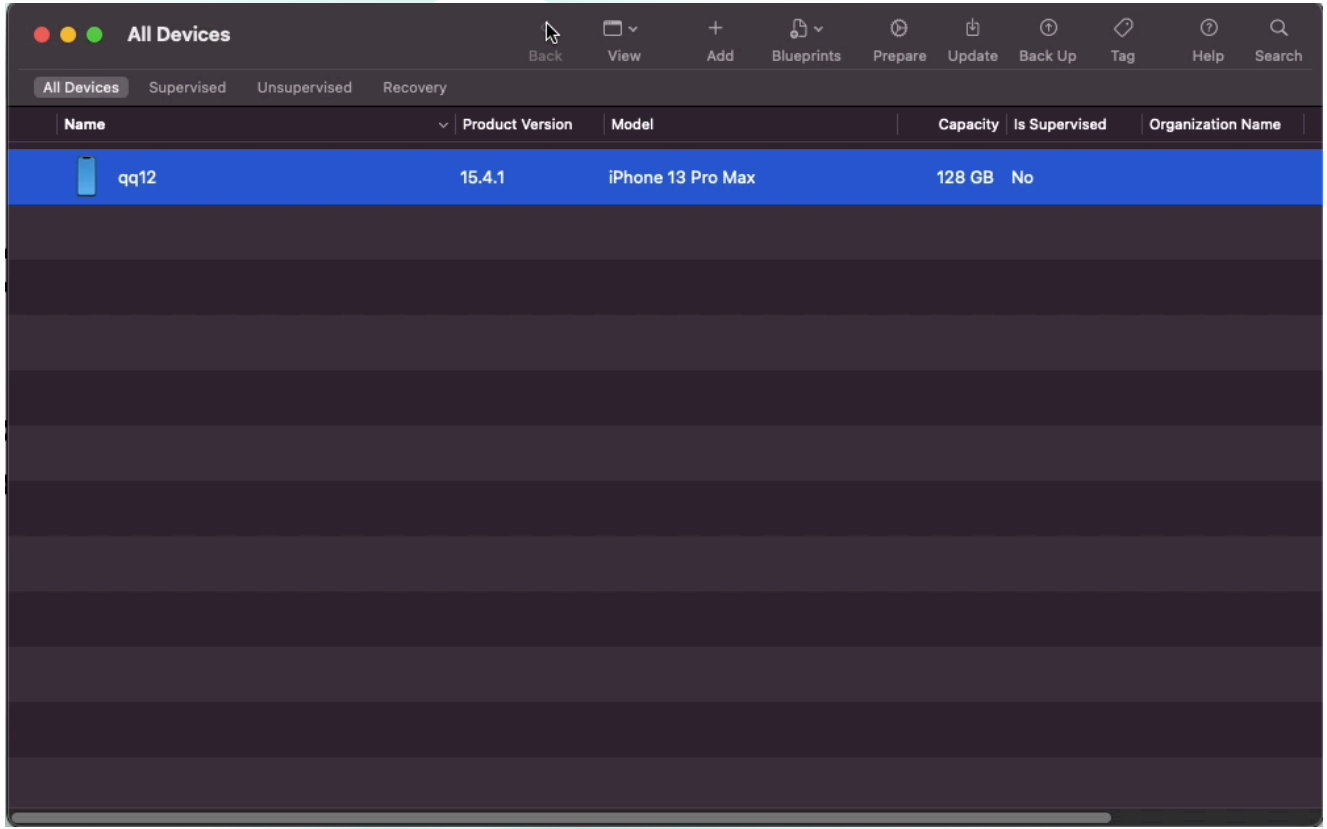
Силами MDM-сервера

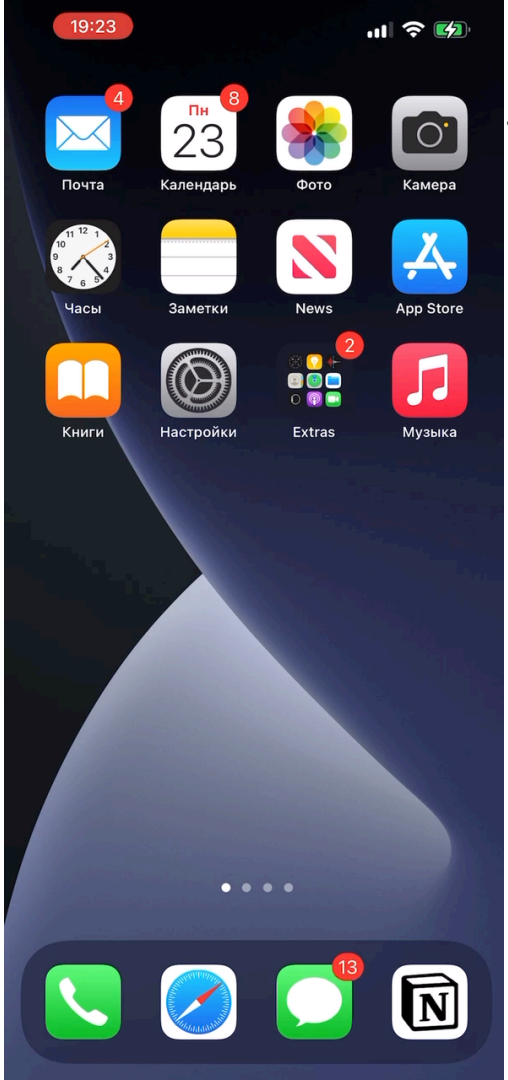
Configuration Profile

Как установить на устройство?

ДЕМО

Процесс установки профиля на устройство с помощью Apple configurator


All Devices
Back
View
Add
Blueprints
Prepare
Update
Back Up
Tag
Help
Search
All Devices
Supervised
Unsupervised
Recovery
Name
Product Version
Model
Capacity
Is Supervised
Organization Name
qq12
15.4.1
iPhone 13 Pro Max
128 GB
No


19:23
Почта
Календарь
Фото
Камера
Часы
Заметки
News
App Store
Книги
Настройки
Extras
Музыка

16

Configuration Profile

Как установить на устройство?

ДЕМО

Процесс установки профиля на устройство по ссылке


Install profile
AA
m1553d.com

Configuration Profile

Насколько легко установить профиль?

Для разработчиков выглядит просто

А для пользователей?

15:47

Safari не удается открыть страницу, так как браузеру не удалось подключиться к серверу.

Веб-сайт пытается загрузить профиль конфигурации. Разрешить?

Игнорировать Разрешить

AA m1553d.com

15:47

Safari не удается открыть страницу, так как браузеру не удалось подключиться к серверу.

Профиль загружен

Если Вы хотите установить профиль, просмотрите его в приложении «Настройки».

Закрыть

AA m1553d.com

15:47

VPN и управление устройством

VPN Не подключено

Войти в учетную запись учебного учреждения или организации...

ЗАГРУЖЕННЫЙ ПРОФИЛЬ

WorkspaceDefender
WD

ПРОФИЛИ КОНФИГУРАЦИИ

Charles Proxy CA (14 May 2018,...

Denis Kudinov
Kaspersky Lab

15:47

Отменить Установка профиля Установить

WorkspaceDefender
WD

Подпись m1553d.com
Проверен ✓

Описание This is an example of workspace defender app profile. Enjoy!

Содержание Управление мобильными устройствами
Сертификаты (5)

Более подробно

Удалить загруженный профиль

15:47

Отменить | Ввод код-пароля | Готово

Введите код-пароль

15:47

Отменить | Согласие | Далее

СООБЩЕНИЕ ОТ «WD»

Installing Workspace Defender (c) profile

15:47

Отменить | Предупреждение | Установить

КОРНЕВОЙ СЕРТИФИКАТ

При установке сертификата «Apple Root CA - G3» он будет добавлен в список надежных сертификатов на iPhone.

КОРНЕВОЙ СЕРТИФИКАТ

При установке сертификата «Apple Root CA - G2» он будет добавлен в список надежных сертификатов на iPhone.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Установка этого профиля позволит администратору «https://m1553d.com/api/server» удаленно управлять Вашим iPhone.

Администратор может собирать личные данные, добавлять и удалять учетные записи, задавать ограничения, просматривать, упорядочивать и устанавливать приложения, а также удаленно стирать данные на Вашем iPhone.

15:47

Отменить | Предупреждение | Установить

КОРНЕВОЙ СЕРТИФИКАТ

При установке сертификата «Apple Root CA - G3» он будет добавлен в список надежных сертификатов на iPhone.

КОРНЕВОЙ СЕРТИФИКАТ

При установке сертификата «Apple Root CA - G2» он будет добавлен в список надежных сертификатов на iPhone.

Удаленное управление

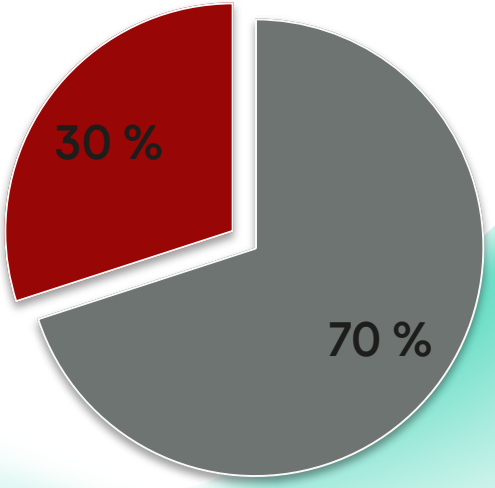
Вы доверяете источнику этого профиля для принятия данного iPhone под удаленное управление?

Отменить | Доверять

server» удаленно управлять Вашим iPhone.

Администратор может собирать личные данные, добавлять и удалять учетные записи, задавать ограничения, просматривать, упорядочивать и устанавливать приложения, а также удаленно стирать данные на Вашем iPhone.

Configuration Profile



Установили

Запретили установку

Провели мини-исследование

Все опрошенные были мотивированы на установку

Установить рядовым пользователям сложно

Configuration Profile

Что ещё умеют профили?

Конфигурировать календари и контакты

Конфигурировать почтовые клиенты

Настраивать сеть (Wi-Fi)

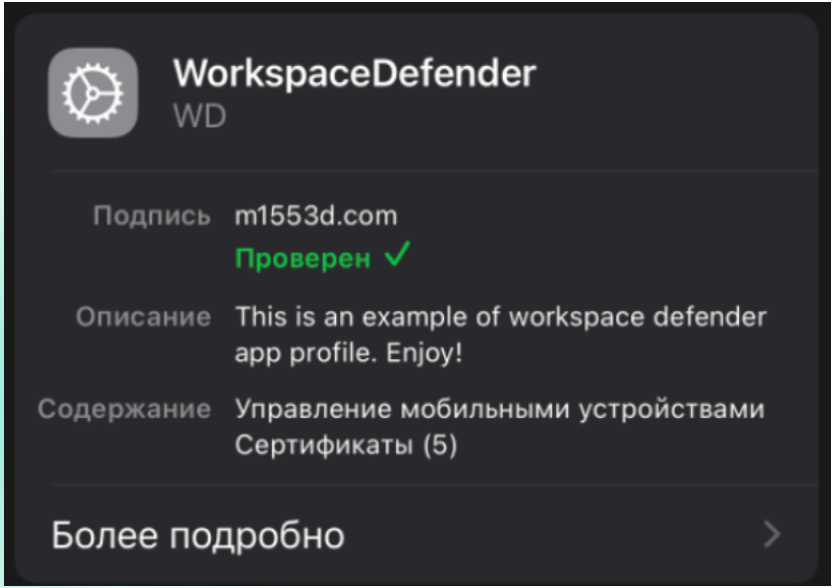
Устанавливать веб- и dns-прокси

Настраивать принтеры

Устанавливать дополнительные сертификаты

Configuration Profile

Как получить галочку “Проверен”?



Configuration Profile

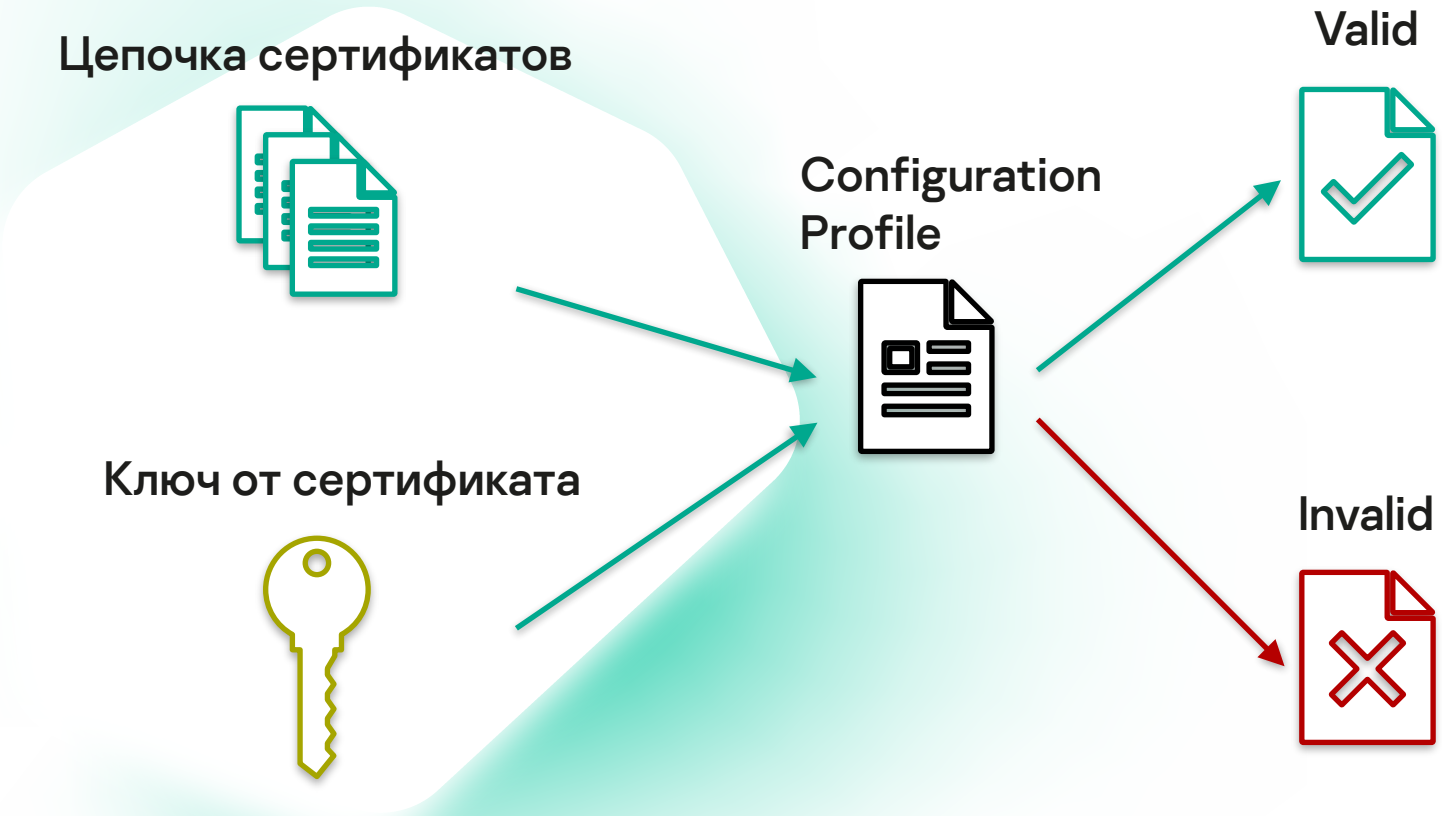
Как получить галочку “Проверен”?

Профиль можно подписать

Неподписанный профиль всё ещё будет работать

Зелёная галочка означает валидность SSL-сертификата

Теория


Цепочка сертификатов
Ключ от сертификата
Configuration Profile
Valid
Invalid

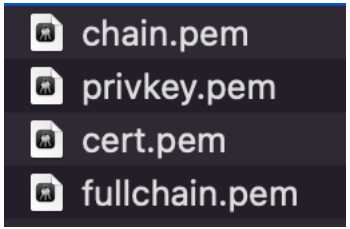
Практика (let’s encrypt)

1. Конвертим сертификат в .crt

```
openssl x509 -inform DER -in cert.pem -out server.crt
```

2. Подписываем профиль

```
openssl smime -sign
-signer server.crt
-inkey privkey.pem
-certfile fullchain.pem
-nodetach
-outform der
-in Enroll.mobileconfig
-out EnrollSigned.mobileconfig
```



План встречи

Кому полезен этот доклад

Профили конфигурации

Mobile Device Management

Supervised-режим

BYOD-режим

Mobile Device Management (MDM)

MDM

Введение

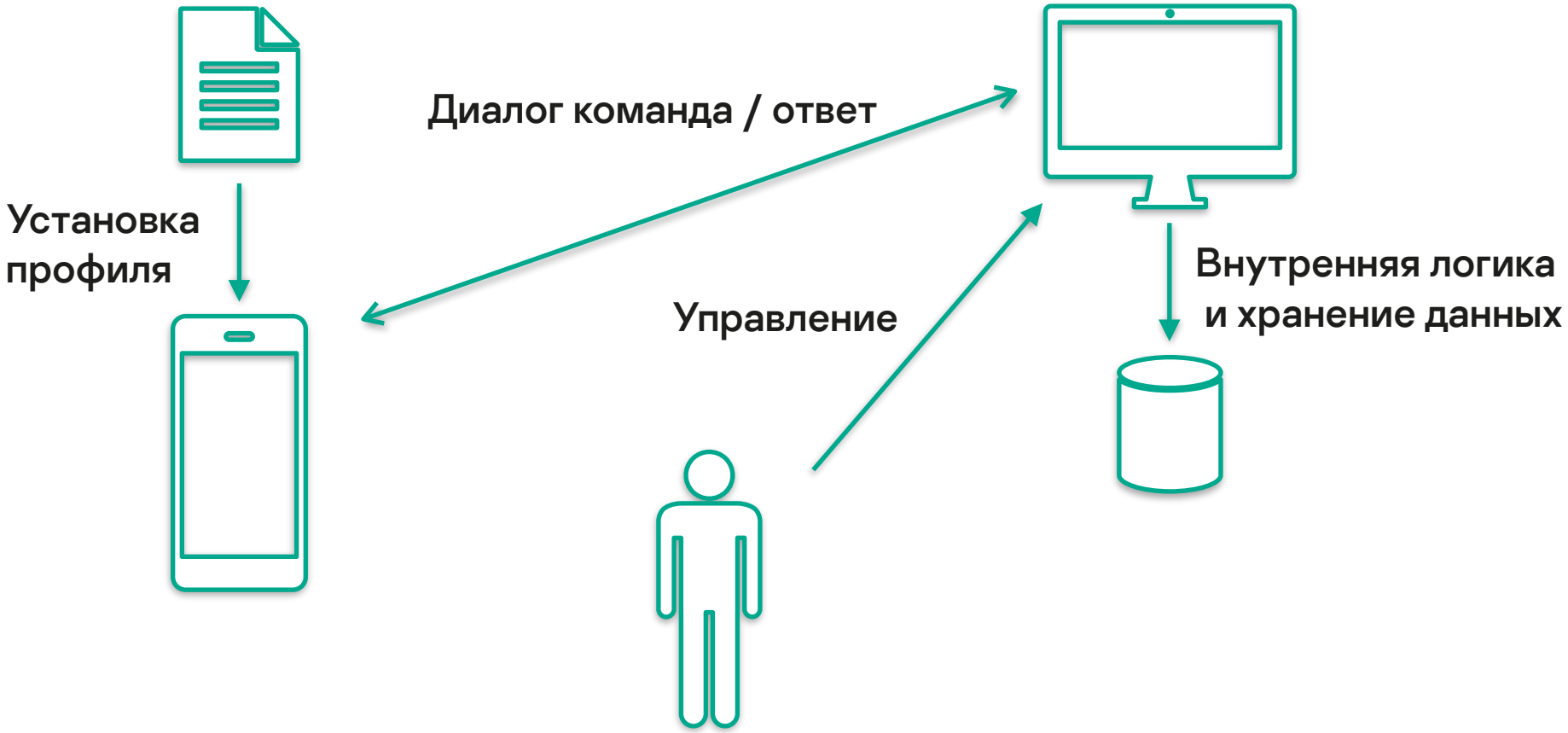
Технология для удалённого управления устройством

Частично основана на Configuration profile

Позволяет получать недоступную из iOS-приложения информацию

Позволяет устанавливать на устройство профили и приложения

Механизм работы MDM



MDM

Основные возможности

Просмотр информации об устройстве

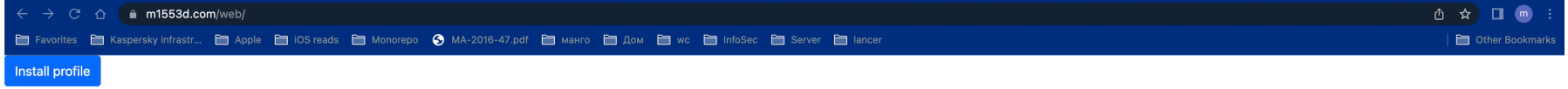
Установка и удаление приложений

Просмотр информации о других профилях

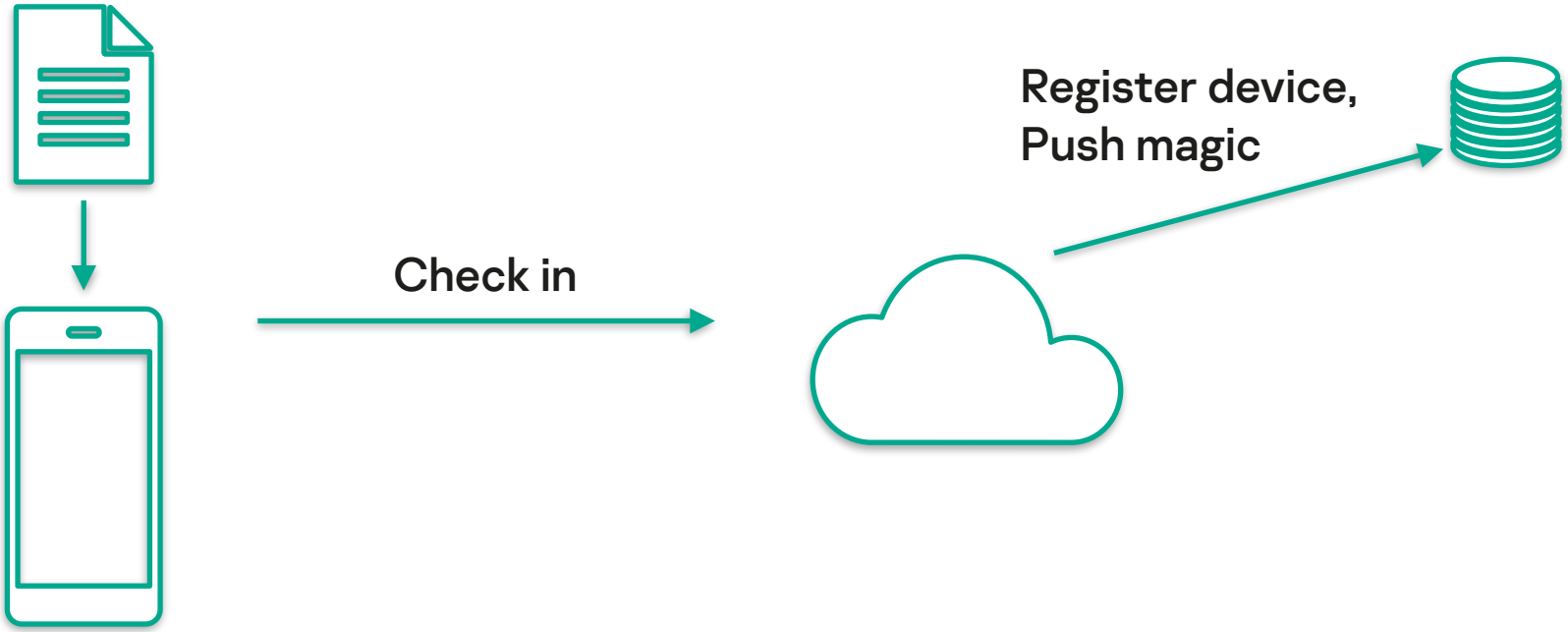
Планирование команд на основе собственной логики

MDM

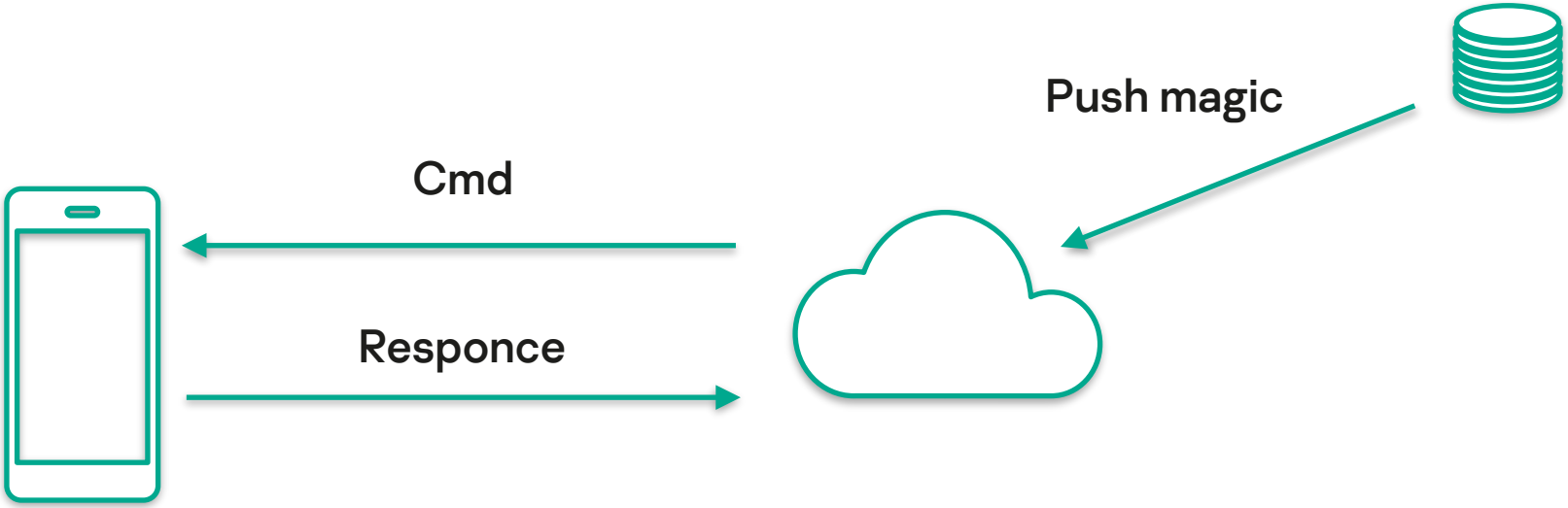
Демо Device info


m1553d.com/web/
Favorites
Kaspersky infrastr...
Apple
iOS reads
Monorepo
MA-2016-47.pdf
манго
Дом
wc
InfoSec
Server
lancer
Other Bookmarks
Install profile

Механизм Enroll устройства в MDM программе



Механизм управления устройством



Что такое команды в MDM?

XML в специальном формате

Всегда отправляется с использованием Push сообщений

Могут быть растянуты во времени

Всегда должен быть получен ответ от устройства

Позволяет получать недоступную из iOS-приложения информацию

Позволяет устанавливать на устройство профили и приложения

Пример команды в MDM (raw Checkin)


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "…">
<plist version="1.0">
  <dict>
   <key>MessageType</key>
   <string>Authenticate</string>
   <key>Topic</key>
   <string>...</string>
   <key>UDID</key>
   <string>...</string>
  </dict>
</plist>
```

Дополнительная информация об устройстве

Wi-Fi оборудование (Mac-адрес)

Bluetooth

iTunes (хэш аккаунта)

Информация о сим-картах (в том числе номер телефона)

Информация об уникальных id (UDID/IMEI)

Результат команд Check-in и TokenUpdate

Device info

Basic info | Applications | Profiles

Parameter	Value	Description
Identifier	00008101-	UDID
Push token	n0EZmTGmWsN1J	Used to send push
Push magic	3890A20D-CE99-	Used to send MDM payloads
Topic		Unique string describing client-server interaction
CheckedOut	false	Is device removed from MDM

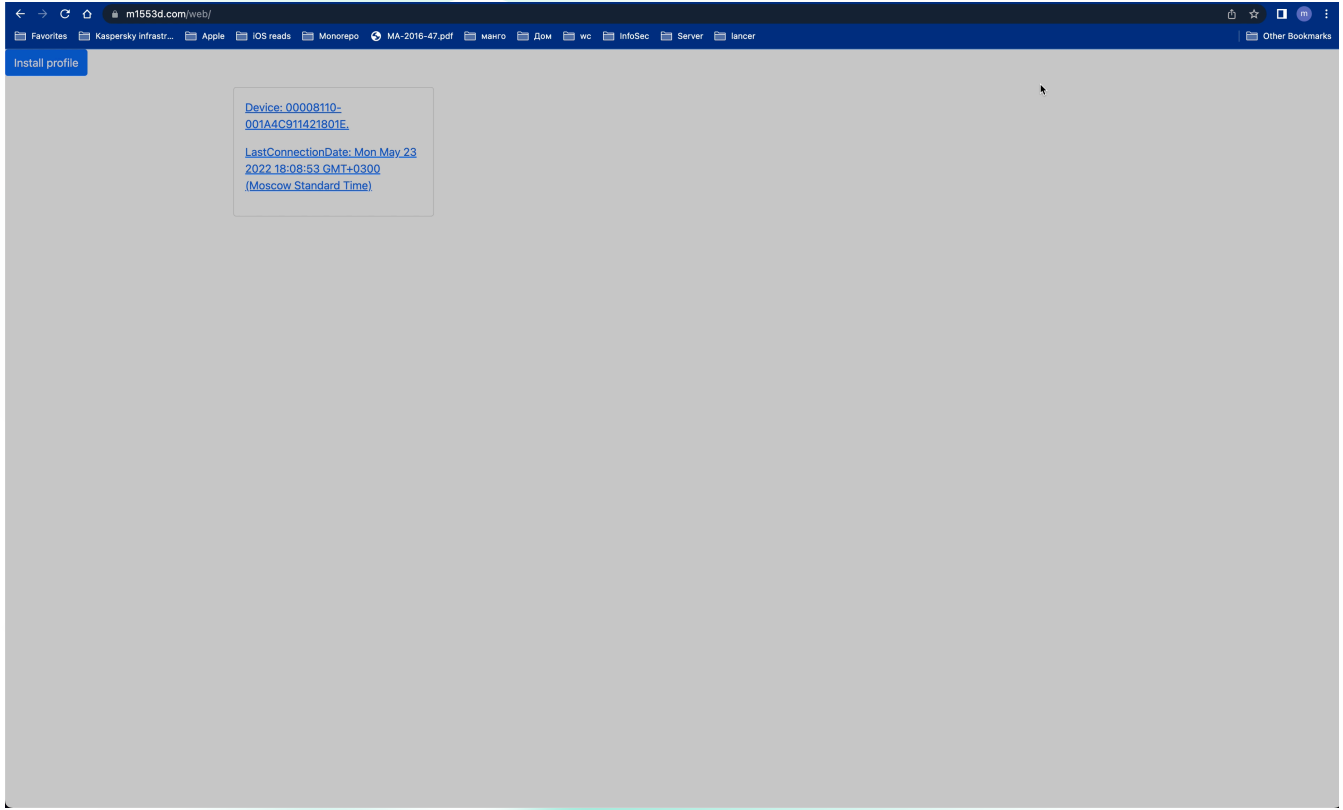
Query additional device information

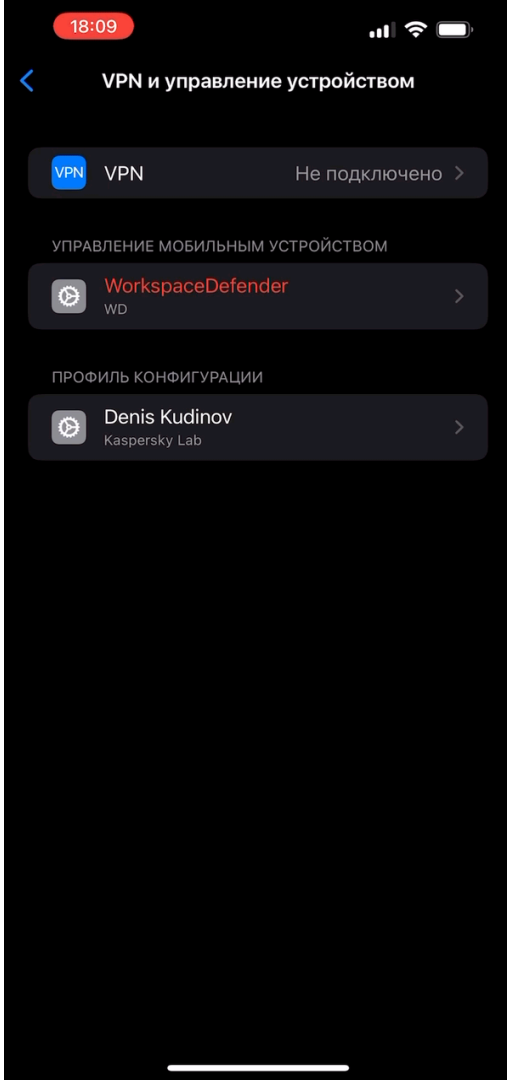
Ответ от команды DeviceInfo

DeviceName	"qq12"
OSVersion	"15.0.2"
BuildVersion	"19A404"
ModelName	"iPhone"
ProductName	"iPhone13,3"
SerialNumber	“F17DVXXXXXX"
BatteryLevel	1
IMEI	"35 717185 xxxxxxx”
IsDeviceLocatorServiceEnabled	TRUE
IsActivationLockEnabled	TRUE
IsDoNotDisturbInEffect	FALSE
BluetoothMAC	“B0:8c:xx:xx:xx:xx”
WiFiMAC	“B0:8c:xx:xx:xx:xx”

MDM

Демо Applications


m1553d.com/web/
Favorites
Kaspersky infrastr...
Apple
iOS reads
Monorepo
MA-2016-47.pdf
манго
Дом
wc
InfoSec
Server
lancer
Other Bookmarks
Install profile
Device: 00008110-001A4C911421801E.
LastConnectionDate: Mon May 23 2022 18:08:53 GMT+0300 (Moscow Standard Time)


18:09
VPN и управление устройством
VPN
Не подключено
УПРАВЛЕНИЕ МОБИЛЬНЫМ УСТРОЙСТВОМ
WorkspaceDefender
WD
ПРОФИЛЬ КОНФИГУРАЦИИ
Denis Kudinov
Kaspersky Lab

MDM

Демо Profiles

m1553d.com/web/

Install profile

Device info

Basic info | Applications | Profiles

Load list of device profiles

Will load all profiles on device.

Load list of profiles


```
0
  HasRemovalPasscode   false
  IsEncrypted          false
  IsManaged            true
  PayloadContent
    0
      PayloadDisplayName   "Apple Worldwide Developer Relations CA - G2"
      PayloadIdentifier    "com.apple.security.pkcs1.40C19302-FB51-4766-B9A6-DFCD19DCB76D"
      PayloadType          "com.apple.security.pkcs1"
      PayloadVersion       1
      PayloadOrganization  ""
      PayloadDescription   "Adds a PKCS#1-formatted certificate"
      PayloadUUID          ""
    1
      PayloadDisplayName   "m1553d.com"
      PayloadIdentifier    "com.apple.security.pkcs12.7F15DCD5-62D9-4A39-BDE5-62B19F88E808"
      PayloadType          "com.apple.security.pkcs12"
      PayloadVersion       1
      PayloadOrganization  ""
```

Применения MDM

Отслеживание роуминга

Обеспечение политик безопасности доступа к устройству (Face ID, pass, ...)

Раскатка корпоративных приложений

Автообновление ОС

Lost mode

Контроль новых установленных приложений

Отслеживание установленных рутовых сертификатов

План встречи

Кому полезен этот доклад

Профили конфигурации

Mobile Device Management

Supervised-режим

BYOD-режим

Supervised mode

Что такое Supervised?

Режим “полного” управления устройством

Расширенный набор команд с сервера MDM

Снятие ограничения на использование некоторых API из клиента

Возможна только установка при активации iPhone

Требует выполнения Erase All Content and Settings

Невозможно накатить режим supervised“по воздуху”

Возможности Supervised в MDM

Незаметная установка профилей и приложений

Большие возможности для ограничений: установка приложений, подключение к сетям

Wipe device

Различные системные возможности (шорткаты, find my, ...)

Lock Screen message

Content filter

Возможности Supervised в MDM

Kiosk mode

Activation lock

Unroll deny (нельзя выйти из режима управления)

Полный список отличий от non-supervised: https://support.apple.com/ru-ru/guide/deployment/dep6b5ae23e9/web

План встречи

Кому полезен этот доклад

Профили конфигурации

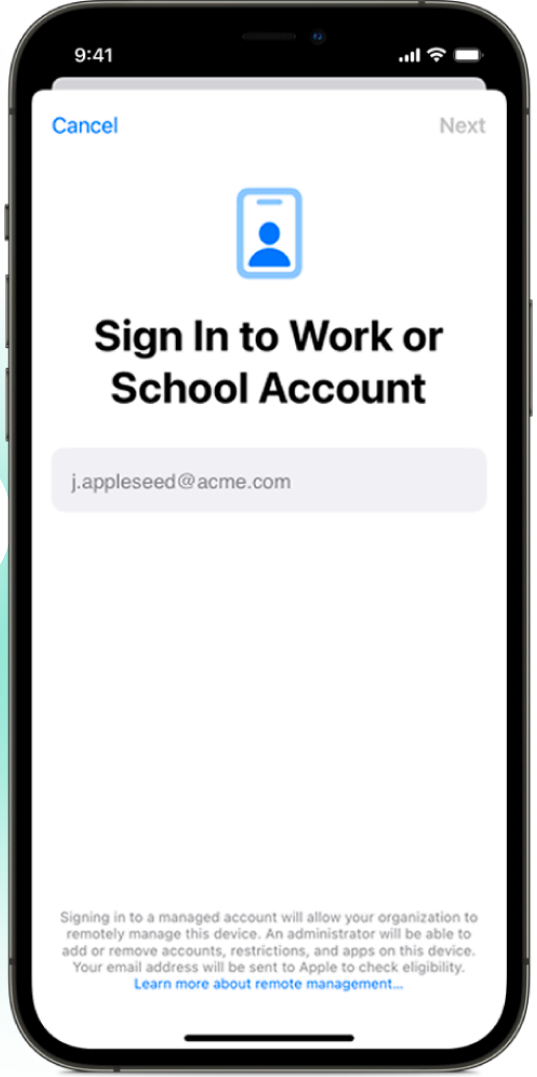
Mobile Device Management

Supervised-режим

BYOD-режим

Bring Your Own Device (BYOD)

BYOD


9:41
Cancel
Next
Sign In to Work or School Account
j.appleseed@acme.com
Signing in to a managed account will allow your organization to remotely manage this device. An administrator will be able to add or remove accounts, restrictions, and apps on this device. Your email address will be sent to Apple to check eligibility.
Learn more about remote management...

BYOD

Заводит дополнительную рабочую учётку apple id

Частично доступны методы из Supervised-режима

Смесь обычного режима использования устройства и Supervised-режима

Возможна раскатка в любой момент времени

Не требует удаления всего контента

Не требует “корпоративного” устройства

BYOD

Ограничения

Нет доступа к IMEI / UDID

Мягче политики паролей

Не может устанавливать Lost Mode

Не может удалять данные пользователя

Не может выполнять Wipe device

Не имеет доступа к данным о роуминге

Полезные ссылки

Описание команд

https://developer.apple.com/documentation/devicemanagement/commands_and_queries

BYOD

https://support.apple.com/ru-ru/guide/deployment/dep23db2037d/web

Статья про подпись профиля

https://medium.com/developerinsider/how-to-create-a-verified-ios-mobile-device-management-mdm-profile-9d6739b92cc1

MDM Protocol reference

https://developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf

Спасибо за внимание. Вопросы?

Кудинов Денис

@kudinovdw

@kudinovdenis

kaspersky