Apple iPhone Configuration Utility (iPCU) and Profile Manager

@rojoroboto
#iPCU&PM

What we will cover:

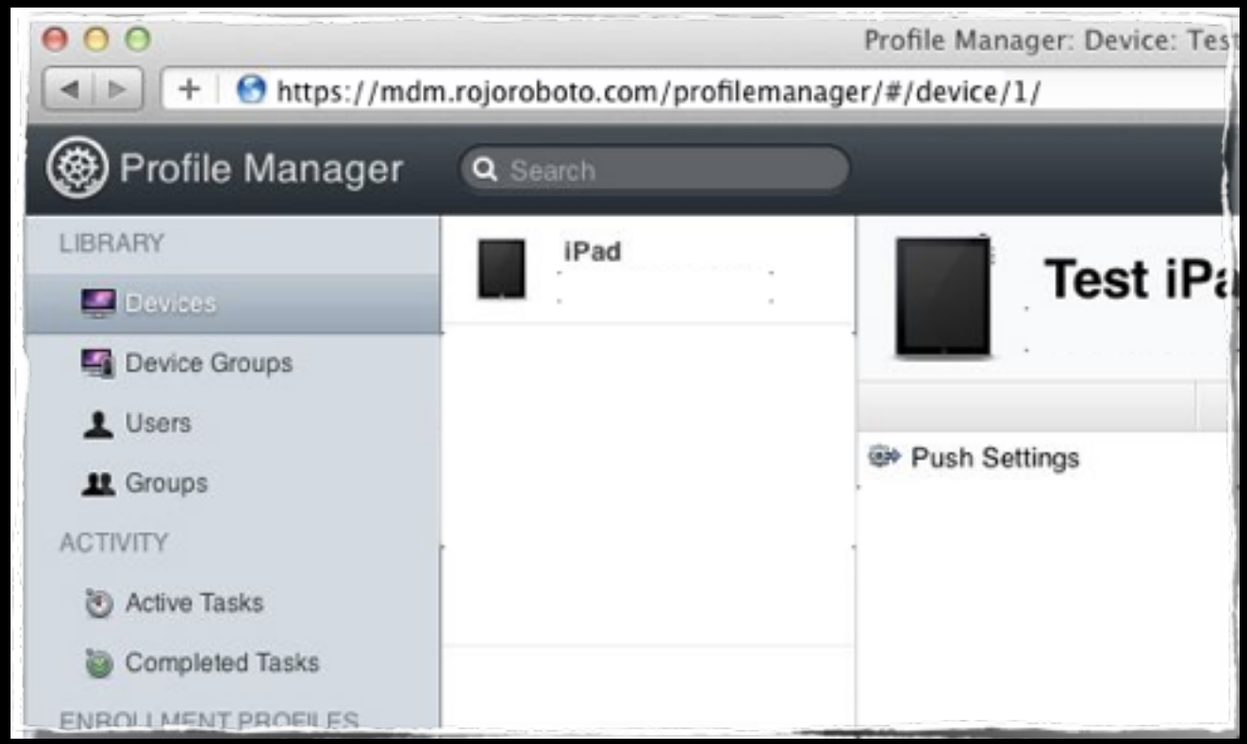
What we will cover:

What we will cover:

Fundamentals
Configuration
Deployment

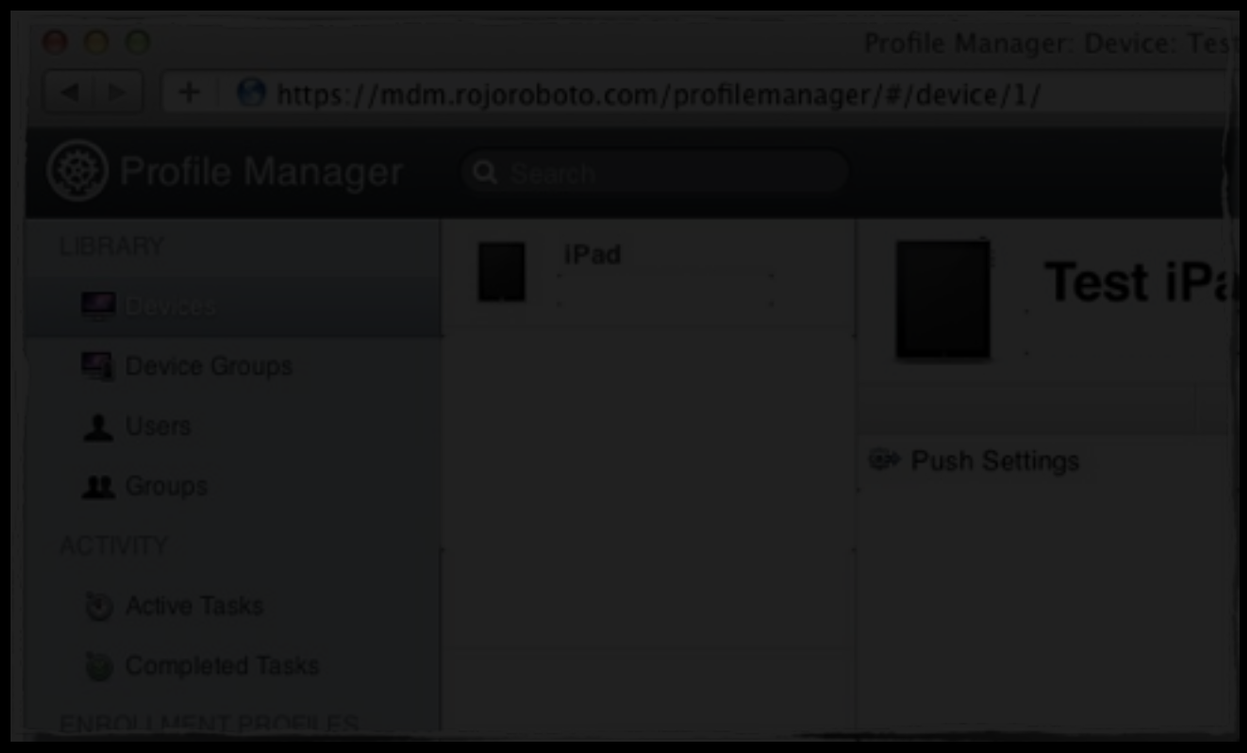
The Fundamentals

iPCU



Profile Manager

iPCU



Profile Manager

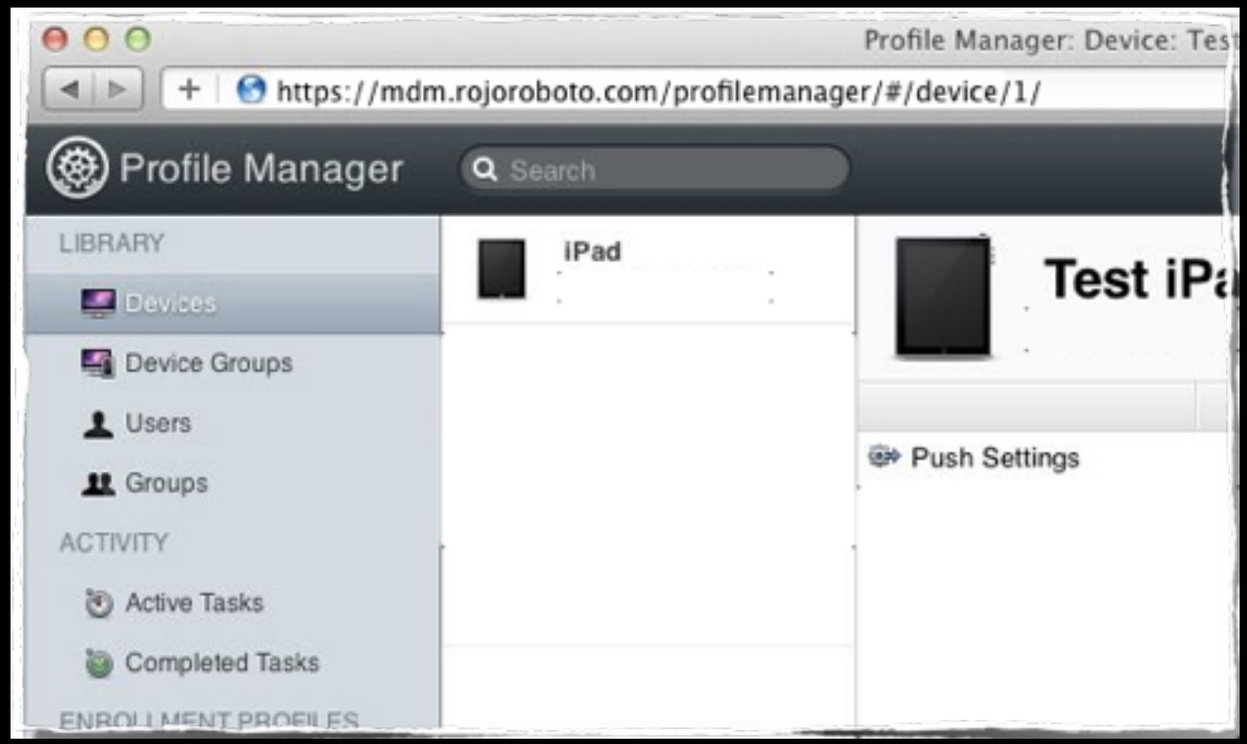
iPCU

- Builds Configuration Profiles for iOS Devices
- Tether Sync of Profiles & Apps*
- Export Configuration Profiles
- Tethered Device Management

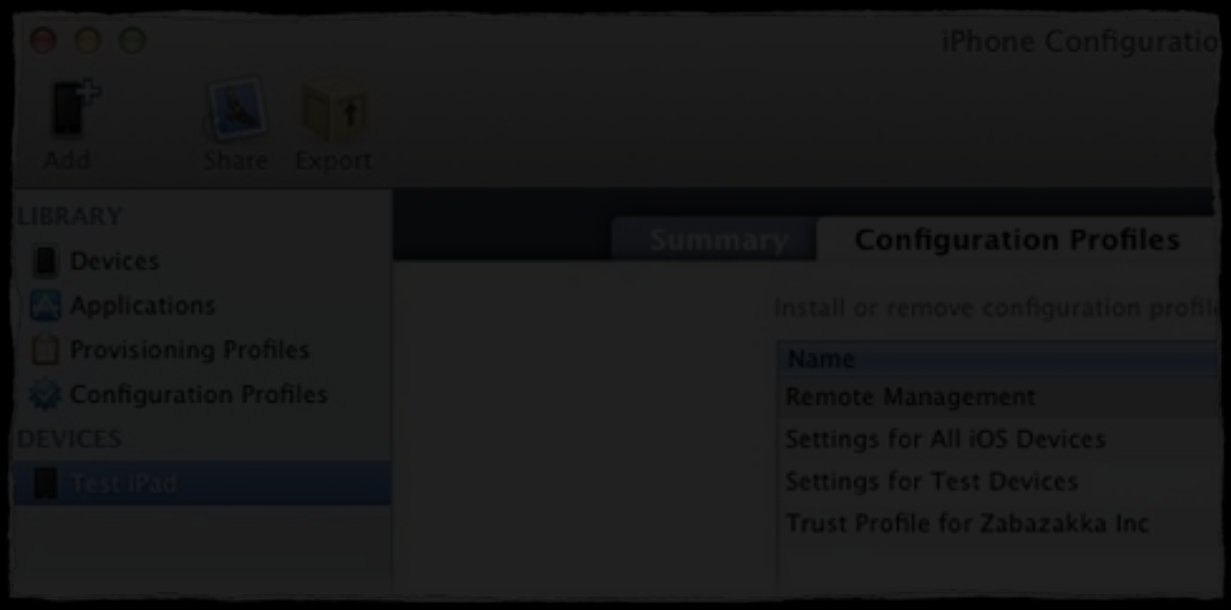
Profile Manager

* Enterprise (in-house) or Development Apps

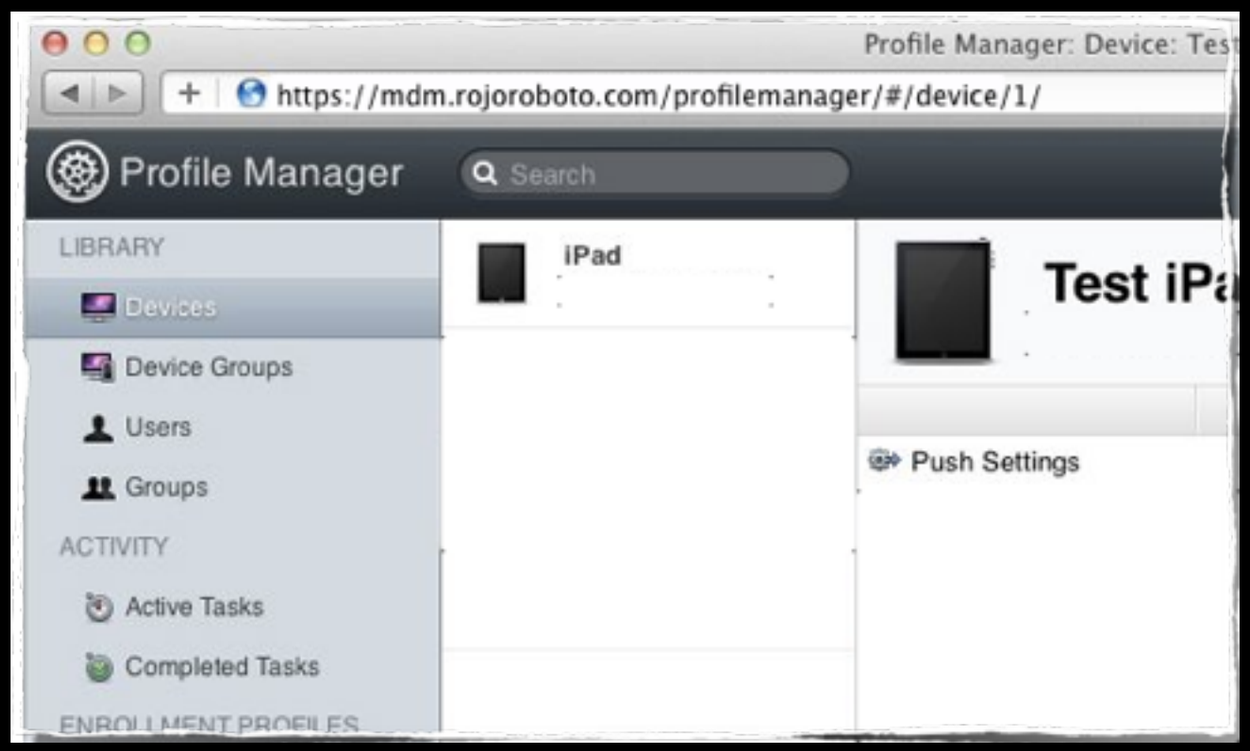
iPCU



Profile Manager

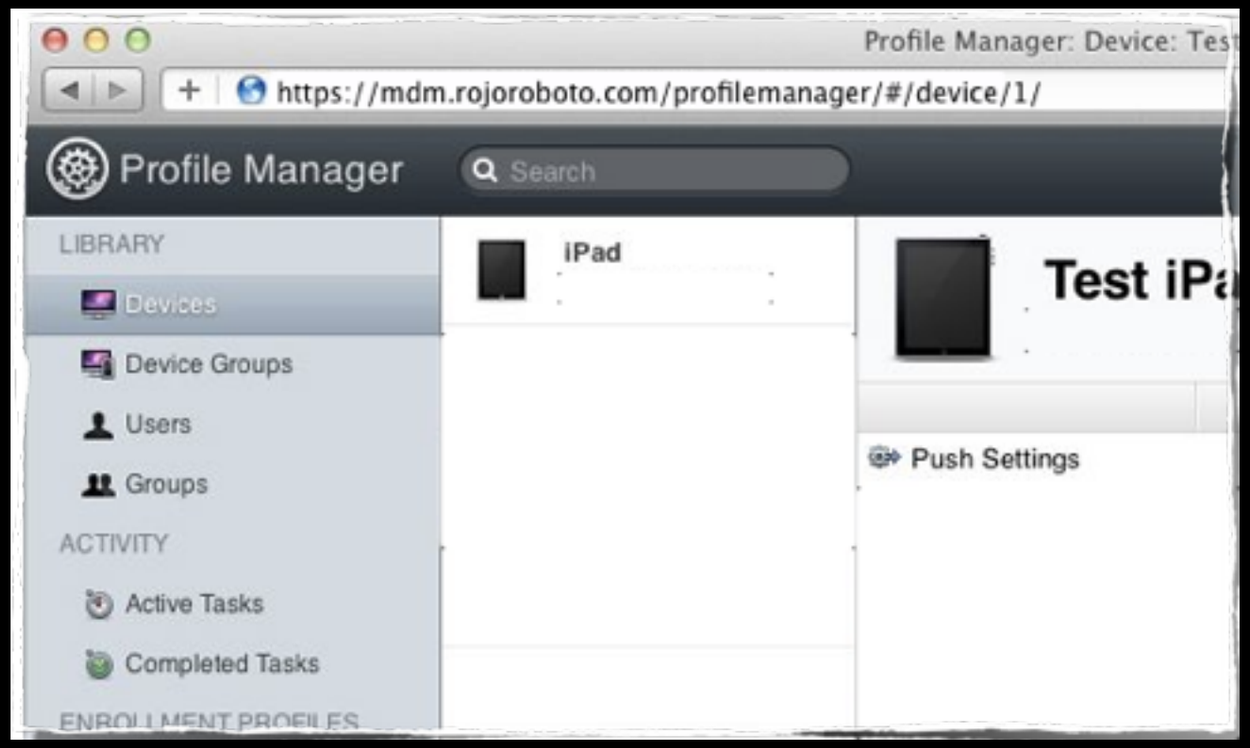


iPCU



Profile Manager

- Builds Configuration Profiles for iOS & OS X 10.7
- Over-The-Air Enrollment
- Over-The-Air Sync of Profiles & In-House Apps
- Web Based Device & Device Group Management
- Web Based User & Group Management



Profile Manager

Configuration Profiles

What are configuration profiles?

What are configuration profiles?

What are configuration profiles?

“Configuration Profiles are XML files that contain settings that permit the device to work with your enterprise systems, including account information, passcode policies, restrictions, and other device settings.”

iPhone and iPad in Business Deployment Scenarios, p.23

What are configuration profiles?

- XML File (.mobileconfig)
- Contains Payload Data
- Plain text, Signed or Signed & Encrypted

What are configuration profiles?

- XML File (.mobileconfig)
- Contains Payload Data
- Plain text, Signed or Signed & Encrypted

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadUUID</key>
        <string>Ignored</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadIdentifier</key>
        <string>Ignored</string>
```

Supported Configurable Settings

Supported Configurable Settings

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Exchange ActiveSync
- IMAP/POP Email
- Wi-Fi
- VPN
- LDAP
- CardDAV
- CalDAV
- Subscribed calendars

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Require passcode on device
- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Time before auto-lock
- Passcode history
- Grace period for device lock
- Maximum number of failed attempts

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Allow diagnostic data to be sent to Apple
- Allow user to accept untrusted certificates
- Force encrypted backups

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Allow installing apps
- Allow Siri
- Allow use of camera
- Allow FaceTime
- Allow screen capture
- Allow automatic syncing while roaming
- Allow voice dialing
- Allow In-App Purchase
- Require store password for all purchases
- Allow multiplayer gaming
- Allow adding Game Center friends

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Allow use of YouTube
- Allow use of iTunes Store
- Allow use of Safari
- Set Safari security preferences

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Allow backup
- Allow document sync and key-value sync
- Allow Photo Stream

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Allow explicit music and podcasts
- Set ratings region
- Set allowed content ratings

Supported Configurable Settings

Accounts
PasscodePolicies
Security and Privacy
Device Functionality
Applications
iCloud
Content Ratings
Other Settings

- Credentials
- Web clips
- SCEP settings
- APN settings

A Note on Signing & Encrypting Profiles

A Note on Signing & Encrypting Profiles

A Note on Signing & Encrypting Profiles

Profiles can be exported as:
clear text
signed
signed and encrypted

A Note on Singing & Encrypting Profiles

Clear Text and Signed Profiles
generated to install on <u>any</u> device

Signed & Encrypted
generated to install on a <u>single</u> device

Setting up iPCU and Profile Manager

iPCU

iPCU

- Trivial to install from .pkg or .exe
- Works well on 10.6 & 10.7, and XP
- Great “one off” config management

Profile Manager

Profile Manager

- Properly Configured Lion Server DNS
- Bound to AD or OD (or OD master)
- Properly Configured Certificates
- Apple Push Notification Service Account

Setting up Profile Manager

Setting up Profile Manager

Prep-work

Certificates, DNS, Directory,

Apple Push Notification Service & Ports

Setting up Profile Manager

DNS:

For proper TLS configure your server with a proper FQDN.

Setting up Profile Manager

Certificates:

It is best practices to snag a certificate from a trusted CA.

Setting up Profile Manager

Directory:

Your Server will need to host an OD master/replica or bind to an existing OD or AD in your deployment

Setting up Profile Manager

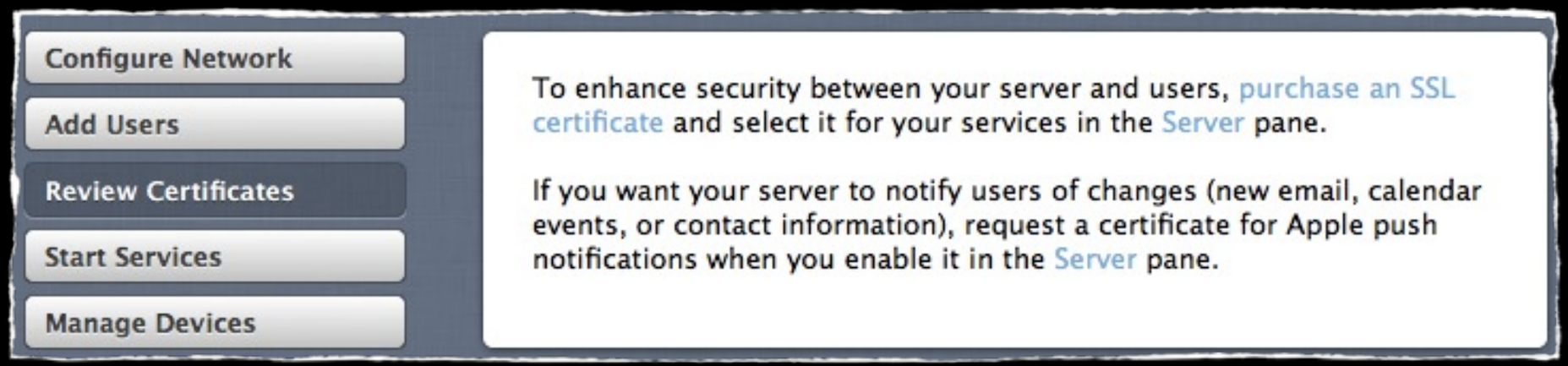
Apple Push Notification Service:
To allow over-the-air management, you will need an AppleID dedicated to APNS.

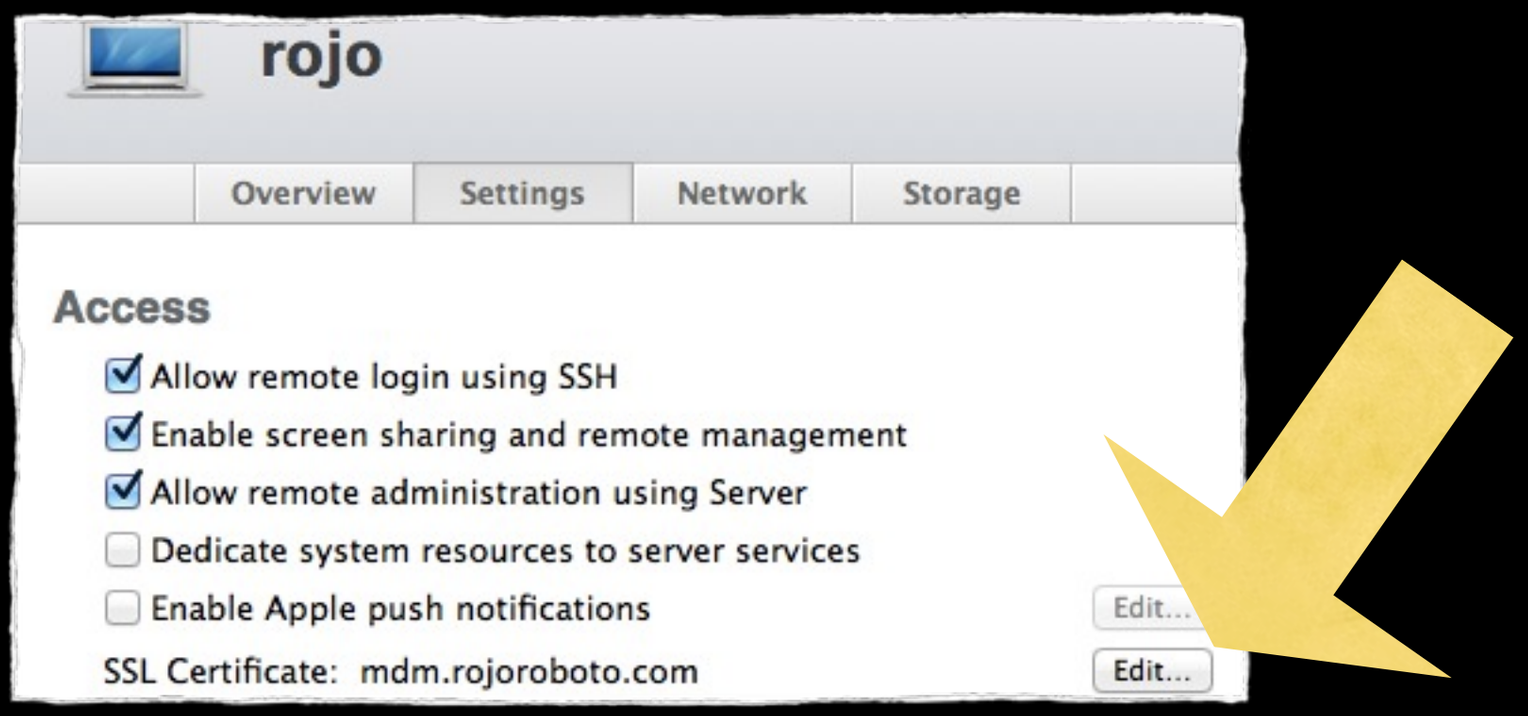
Setting up Profile Manager

Ports:

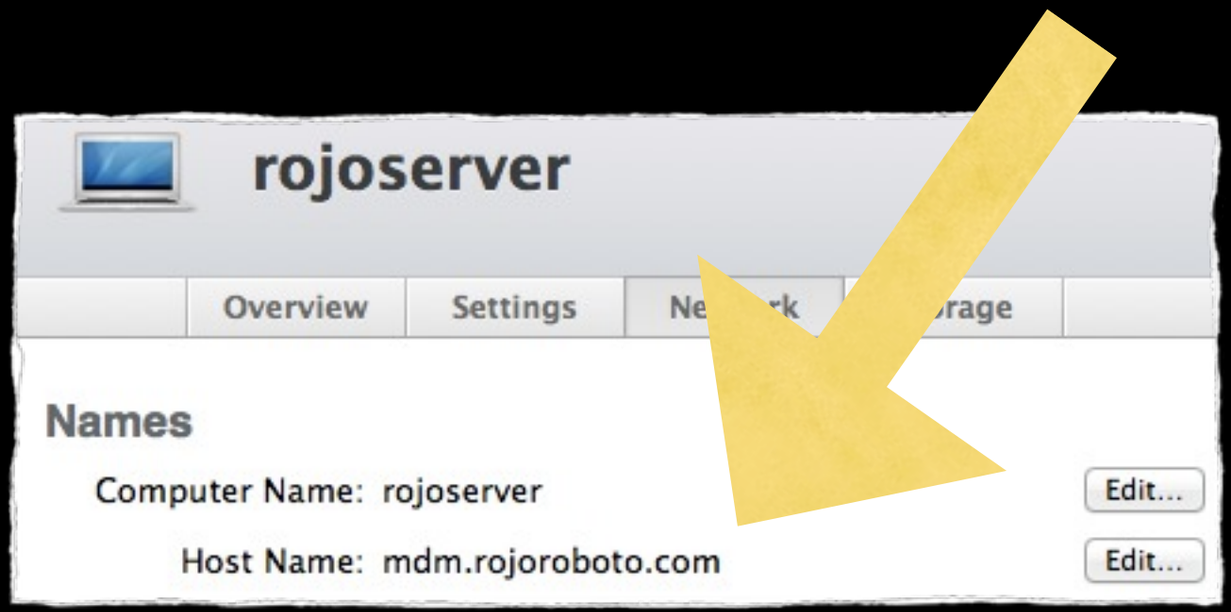
You will need to open TCP ports 443, 1640, and 5223 in your firewall and NAT router (if you are behind one)

Check (or load) your certificate

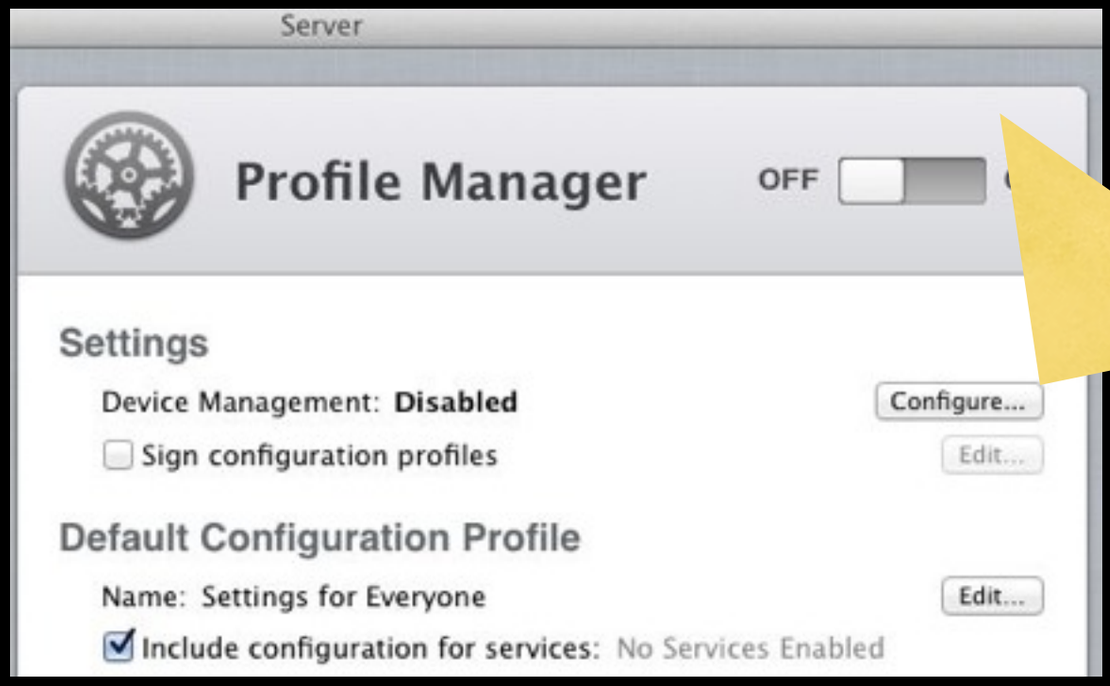




Check to make sure your Host name matches your FQDN



Activating Device Management

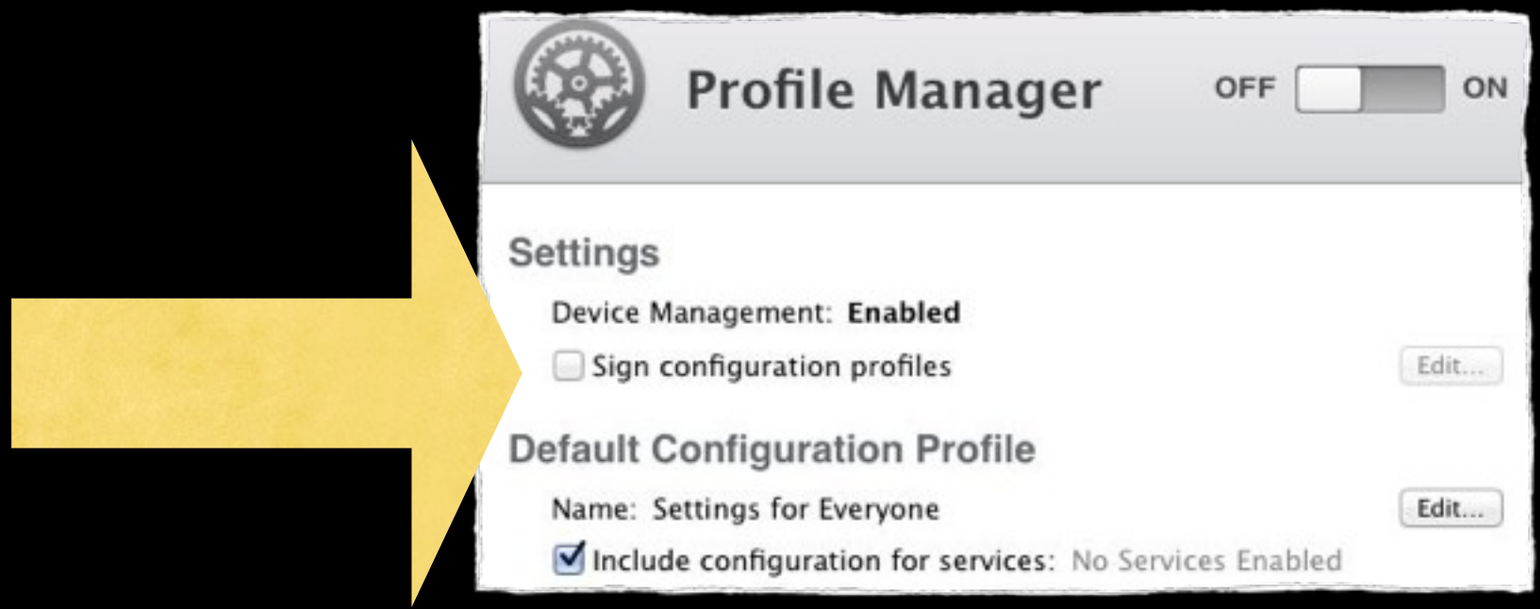


NOTE: If you aren't already bound to a directory, you will be asked to create a diradmin account for your new OD network users.

Activating Device Management

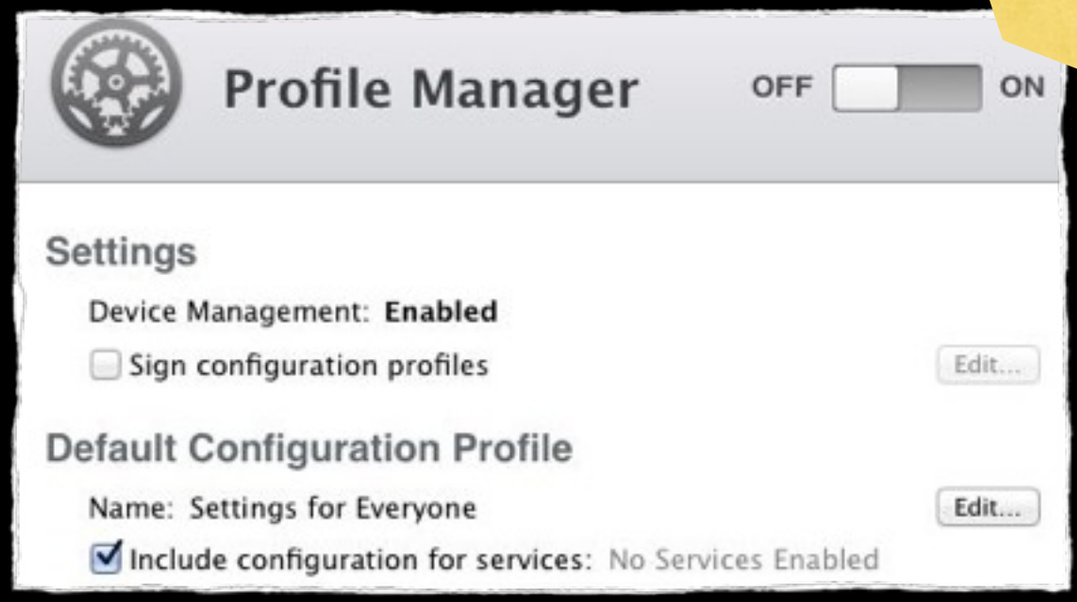
Activating Device Management

Activating Device Management



Enable “Sign configuration profiles”

Activating Device Management



Switch Profile Manager to “On”

Checking the Web App

Deployment & Enrollment

Wired vs Over-the-Air

Wired vs Over-the-Air

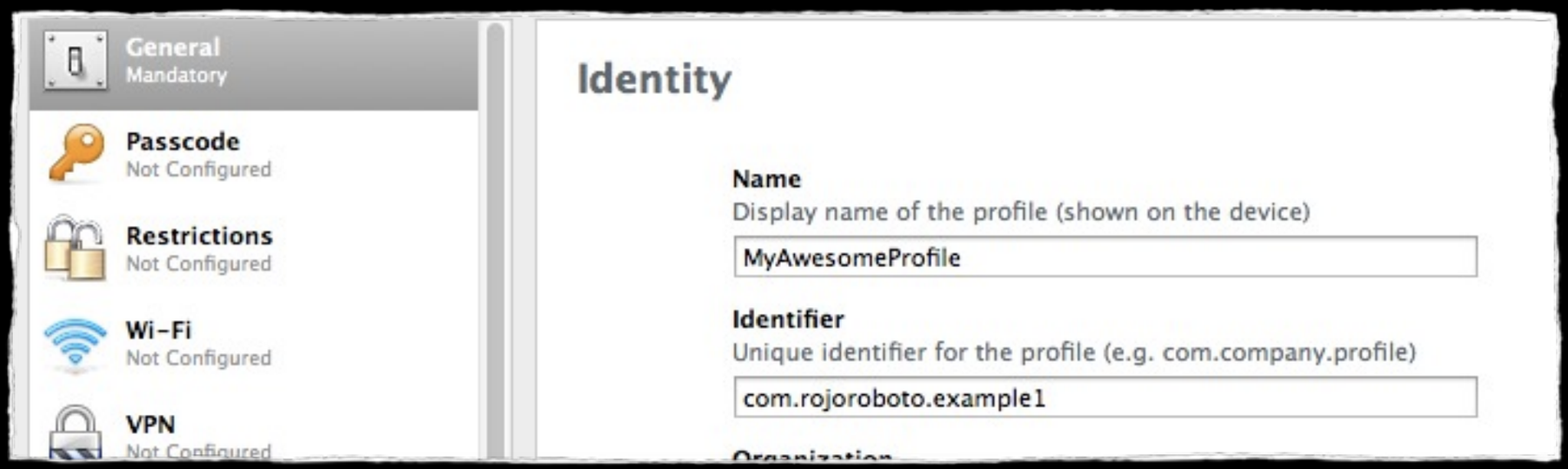
Wired,	Over-the-Air	Export for Web & Email
iPCU	Profile Manager	Both

Wired

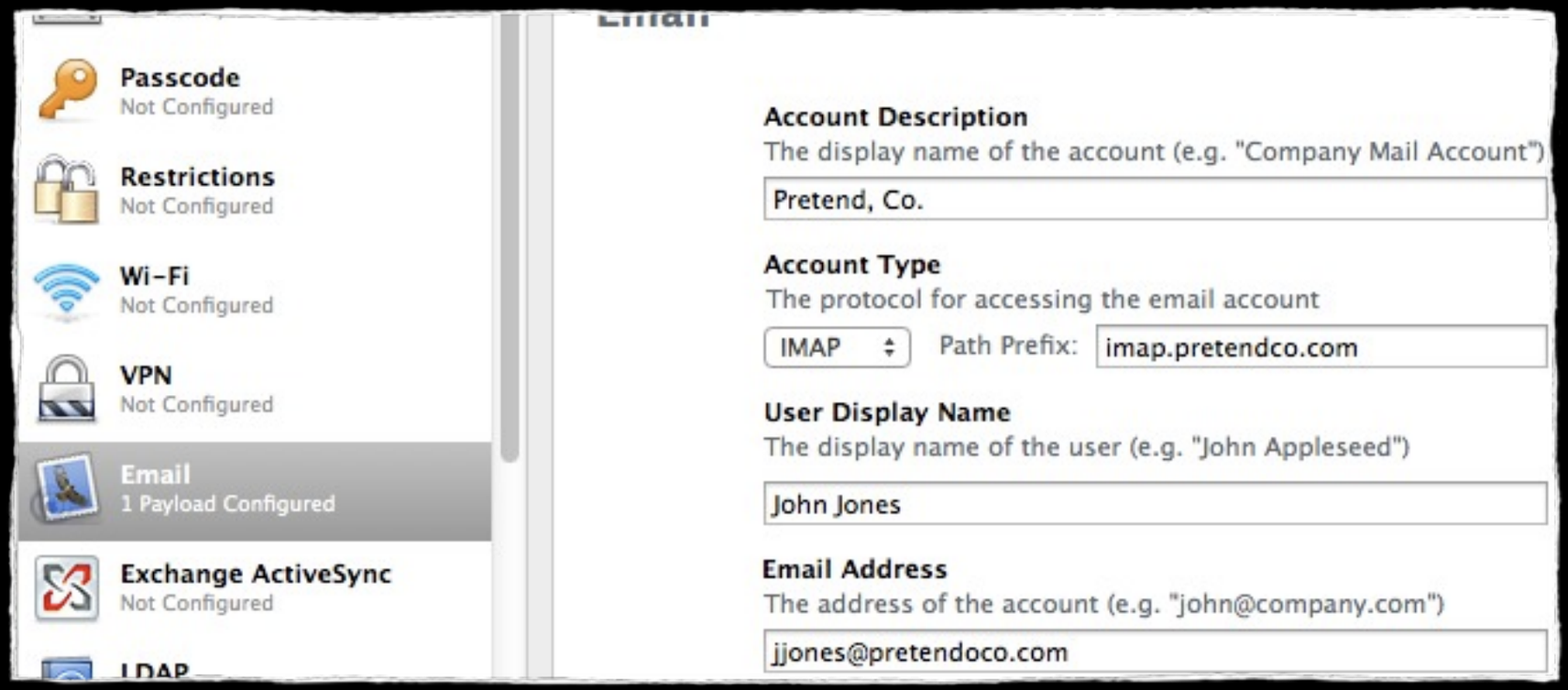
Wired

Add
Share
Export
Hide Detail
All
Search
BRARY
Devices
Applications
Provisioning Profiles
Configuration Profiles
EVICES
iPhone
Name
Serial Number
Identifier
Phone Number
Owner Nar
iPhone
+1 (512)
Summary
Configuration Profiles
Provisioning Profiles
Applications
Device
Name: iPhone
Capacity: 13.59 GB
Software Version: 5.0.1 (9A405)
Serial Number:
Identifier:
ECID:
IMEI:
MEID: Unknown
WiFi MAC Address:
Bluetooth MAC Address:
Last Connected:

Wired


General
Mandatory
Passcode
Not Configured
Restrictions
Not Configured
Wi-Fi
Not Configured
VPN
Not Configured
Identity
Name
Display name of the profile (shown on the device)
MyAwesomeProfile
Identifier
Unique identifier for the profile (e.g. com.company.profile)
com.rojoroboto.example1

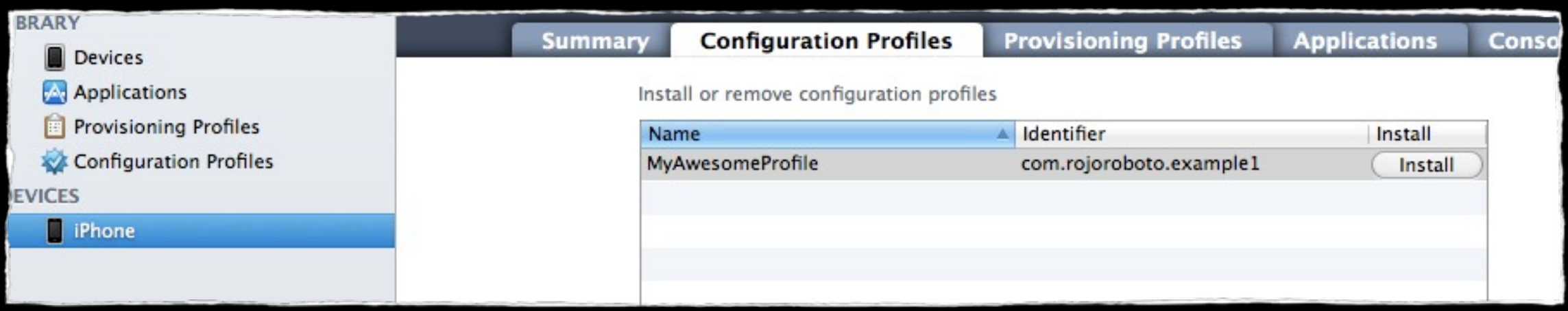
Wired


Passcode
Not Configured
Restrictions
Not Configured
Wi-Fi
Not Configured
VPN
Not Configured
Email
1 Payload Configured
Exchange ActiveSync
Not Configured
LDAP
Account Description
The display name of the account (e.g. "Company Mail Account")
Pretend, Co.
Account Type
The protocol for accessing the email account
IMAP
Path Prefix:
imap.pretendco.com
User Display Name
The display name of the user (e.g. "John Appleseed")
John Jones
Email Address
The address of the account (e.g. "john@company.com")
jjones@pretendoco.com

Wired

1 Payload Configured
Exchange ActiveSync
Not Configured
LDAP
Not Configured
CalDAV
Not Configured
CardDAV
Not Configured
Subscribed Calendars
Not Configured
Web Clips
1 Payload Configured
Credentials
Not Configured
Web Clip
Label
The name to display for the Web Clip
rojoroboto
URL
The URL to be displayed when opening the Web Clip
http://rojoroboto.com
Removable
Enable removal of the Web Clip
Icon
The icon to use for the Web Clip

Wired


BRARY
Devices
Applications
Provisioning Profiles
Configuration Profiles
EVICES
iPhone
Summary
Configuration Profiles
Provisioning Profiles
Applications
Conso
Install or remove configuration profiles
Name
Identifier
Install
MyAwesomeProfile
com.rojoroboto.example1
Install

Wired

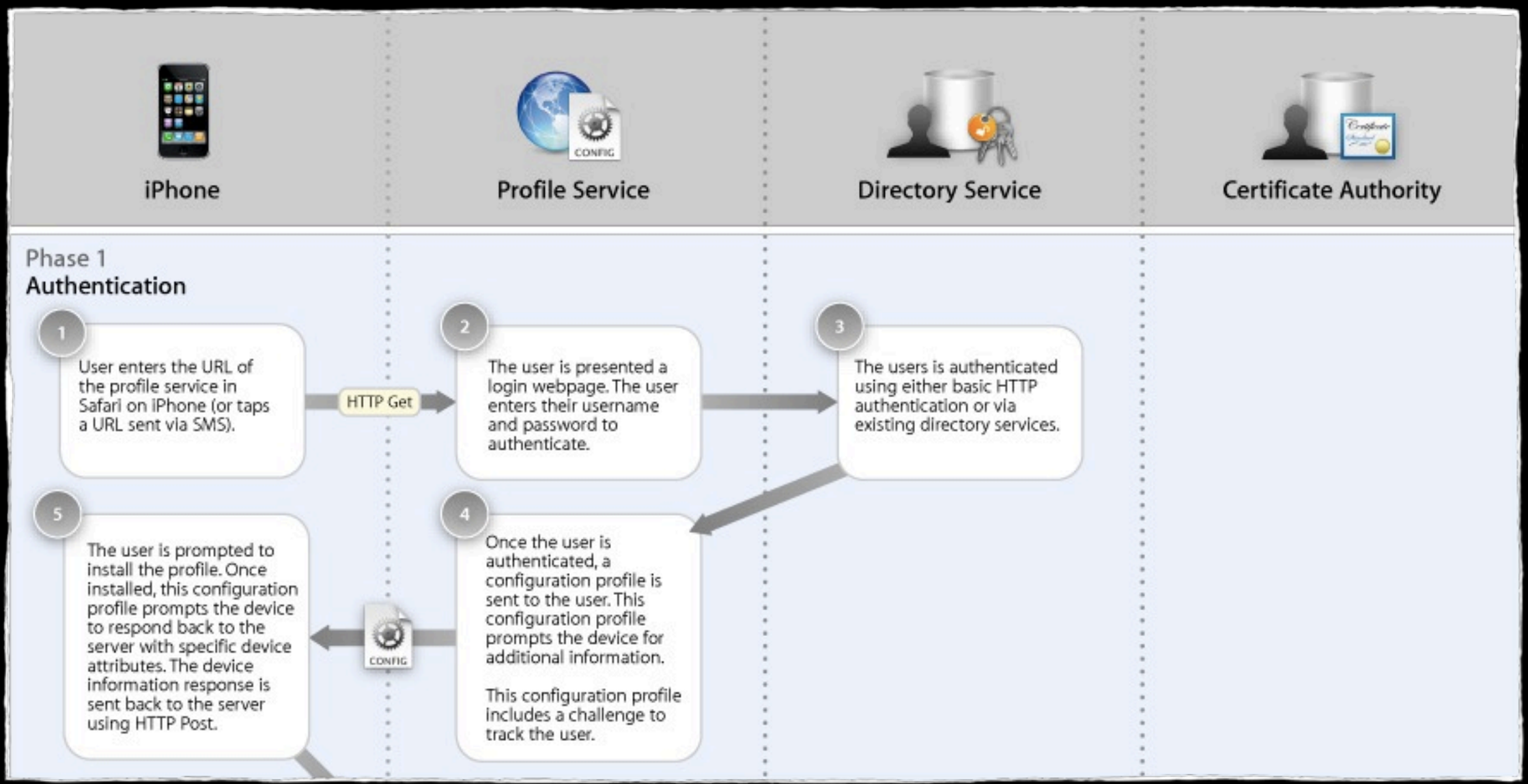
AT&T 3G
9:50
91%
Personal Hotspot: 1 Connection
Cancel
Install Profile
MyAwesomeProfile
Rojoroboto, LLC
Verified
Install
Description
Profile description.
Signed
iPhone Configuration Utility (1B783C0E-2C69-4A4A-8B99-B797151015F5)
Received
Dec 7, 2011
Contains
Web Clip
Email Account
More Details

Over-The-Air

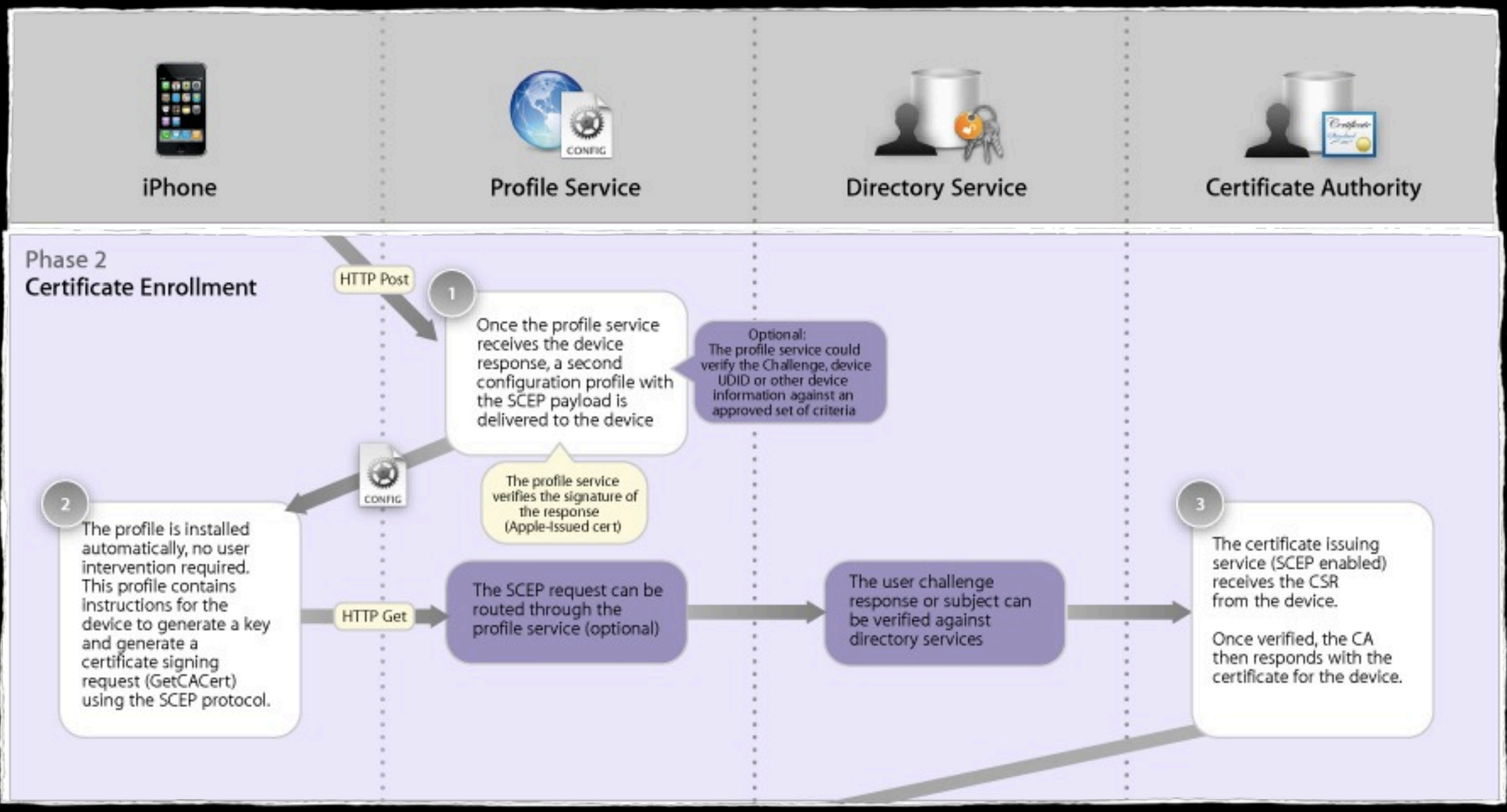
Over-The-Air

How the Profile Manager enrolls new devices

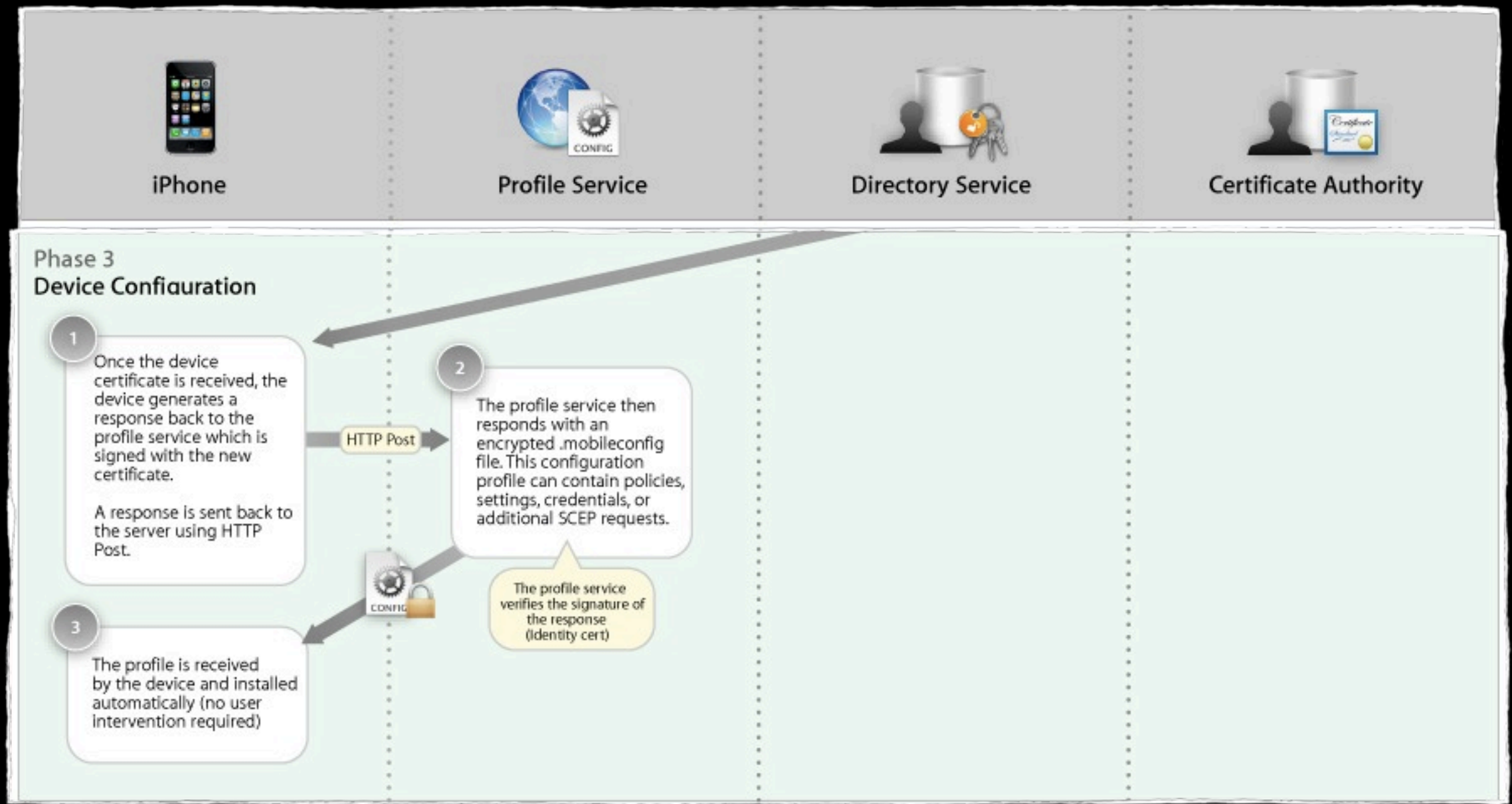
Over-The-Air


iPhone
Profile Service
CONFIG
Directory Service
Certificate Authority
Phase 1
Authentication
1
User enters the URL of the profile service in Safari on iPhone (or taps a URL sent via SMS).
HTTP Get
2
The user is presented a login webpage. The user enters their username and password to authenticate.
3
The users is authenticated using either basic HTTP authentication or via existing directory services.
4
Once the user is authenticated, a configuration profile is sent to the user. This configuration profile prompts the device for additional information.
This configuration profile includes a challenge to track the user.
CONFIG
5
The user is prompted to install the profile. Once installed, this configuration profile prompts the device to respond back to the server with specific device attributes. The device information response is sent back to the server using HTTP Post.

Over-The-Air


iPhone
Profile Service
Directory Service
Certificate Authority
Phase 2
Certificate Enrollment
HTTP Post
1
Once the profile service receives the device response, a second configuration profile with the SCEP payload is delivered to the device
Optional:
The profile service could verify the Challenge, device UDID or other device information against an approved set of criteria
CONFIG
The profile service verifies the signature of the response (Apple-Issued cert)
2
The profile is installed automatically, no user intervention required. This profile contains instructions for the device to generate a key and generate a certificate signing request (GetCACert) using the SCEP protocol.
HTTP Get
The SCEP request can be routed through the profile service (optional)
The user challenge response or subject can be verified against directory services
3
The certificate issuing service (SCEP enabled) receives the CSR from the device.
Once verified, the CA then responds with the certificate for the device.

Over-The-Air


iPhone
Profile Service
Directory Service
Certificate Authority
Phase 3
Device Configuration
1
Once the device certificate is received, the device generates a response back to the profile service which is signed with the new certificate.
A response is sent back to the server using HTTP Post.
HTTP Post
2
The profile service then responds with an encrypted .mobileconfig file. This configuration profile can contain policies, settings, credentials, or additional SCEP requests.
CONFIG
The profile service verifies the signature of the response (identity cert)
3
The profile is received by the device and installed automatically (no user intervention required)

Over-The-Air

Login with user account to see enroll screen

Over-The-Air

Here the end user sees the Install Profile Screen

Over-The-Air

Verified
Install
Install Profile
Installing this profile will change settings on your iPhone.
Cancel
Install Now

Over-The-Air

Cancel
Warning
Install
Mobile Device Management
Installing this profile will allow the administrator at "https://mdm.rojoroboto.com/devicemanagement/api/device/connect" to remotely manage your iPhone.
The administrator may collect personal data, list of apps, add/remove accounts and restrictions, and remotely erase data on your iPhone.

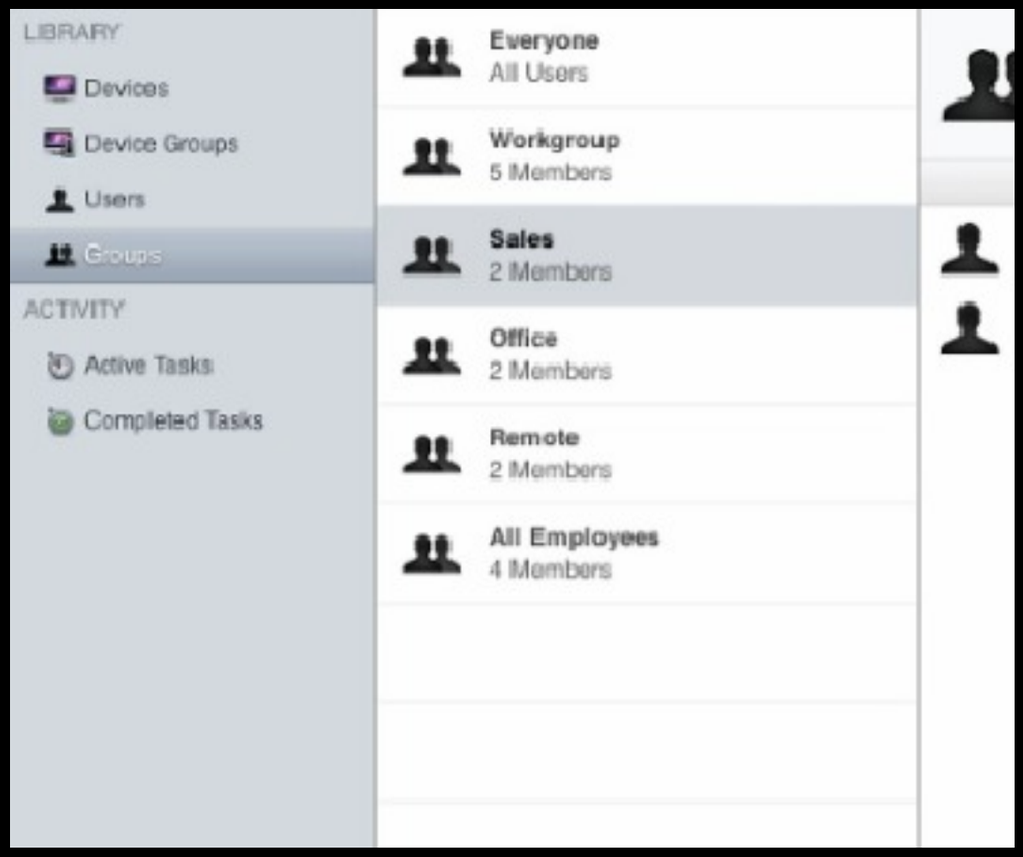
Over-The-Air

Profile Installed
Done
Device Enrollment
Rojoroboto, LLC
Verified
Description
Enrolls your device with the management server.
Signed
mdm.rojoroboto.com Code Signing Certificate
Received
Contains
Device enrollment challenge
More Details

Over-The-Air

Web Administration

Web Administration



Manage Access & Profiles by User & Groups

Web Administration

Manage Access & Profiles by Device & Device Groups

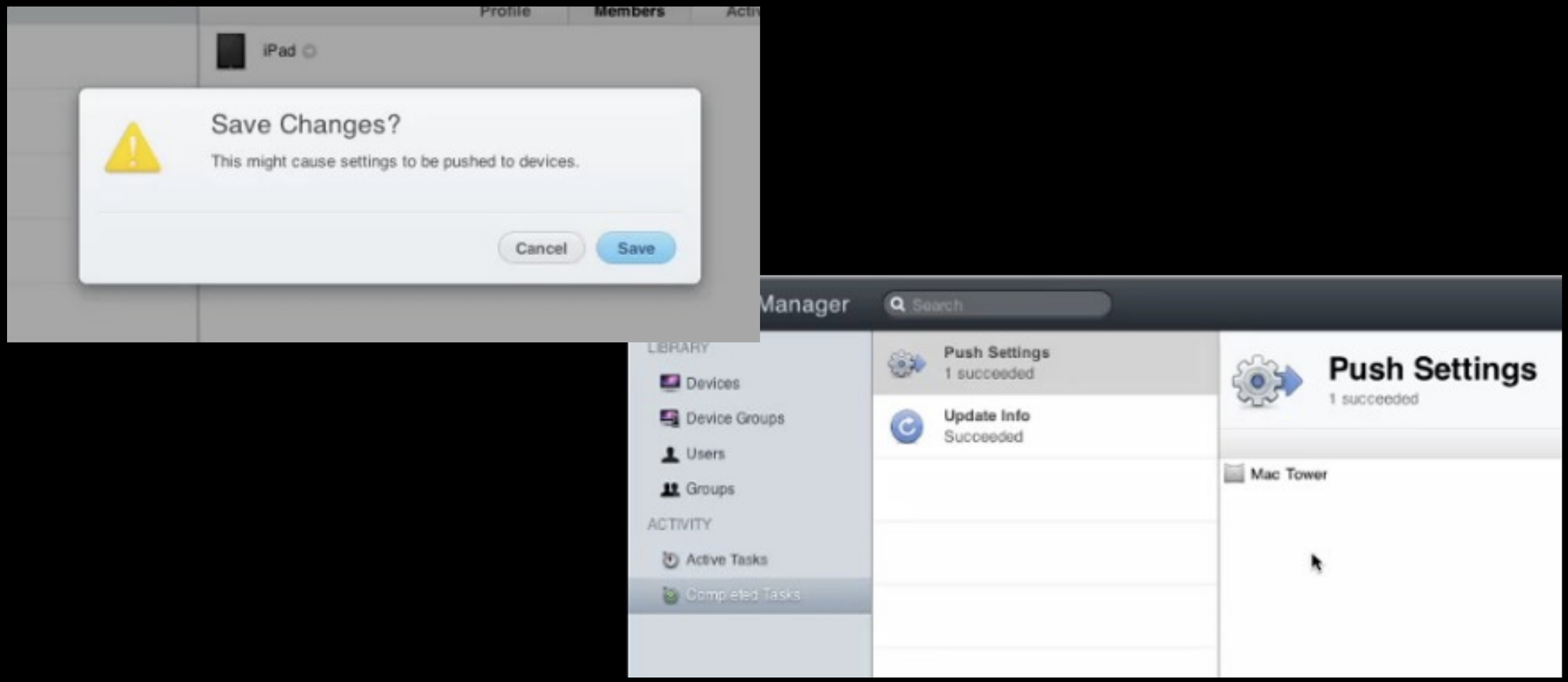
Web Administration

Configuration Profiles are almost identical to iPCU

Web Administration

Export Trust, Configuration, and Enrollment Profiles

Web Administration



Pushing Profile Changes

Web Administration

Lock, Wipe, etc

Web Administration

Monitor Activity

Web Administration

Remote Wipe & Lock

Known Limitations

Questions?

Additional reading:
http://tinyurl.com/mt-ipcu-pm

@rojoroboto
#ipcu&pm