Ahmed Kufaishi

- Supporting Mac systems for the last 20 years.
- Started manning Mac systems using At Ease.
- An early adopter of the Apple OS X Server 10.0.
- Founded Alary Technologies in Oshawa Ontario as the only ACN member and an AASP in the region.
- An avid Apple Scripter, he specializes mass deployment on OS X and iOS devices.

Why Profiles?

- Because we don’t have directory based management anymore
- Profile based management replaced Directory based management because of the advent of iOS which couldn’t be managed via a directory system

What are profiles?

Settings similar to Windows Group Policy restrictions/ configurations

Simple text files saved as *.mobileconfig in XML formatting just like Plist files

Configures iOS and OS X

Can contain multiple payloads

Evolution from MCX (Managed Preferences)

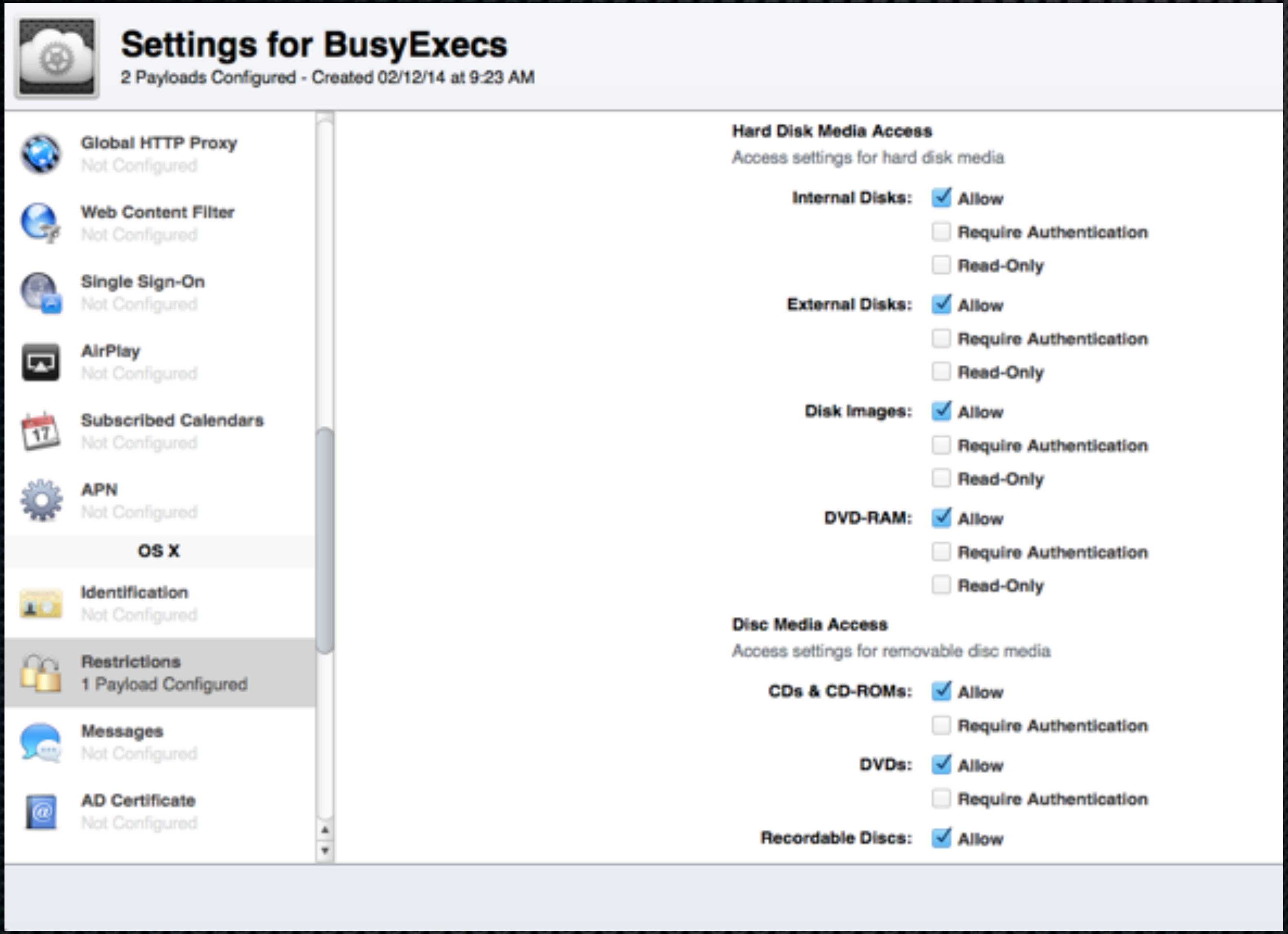
Profile Basics

- Profiles contain settings and preference bundles for devices including:
  - Restrictions on device features
  - Wi-Fi settings
  - VPN settings
  - Email server settings
  - Exchange settings
  - LDAP directory service settings
  - CalDAV calendar service settings
  - Wallpaper
  - Web clips
  - Credentials and keys

Terms and things you need to know:

- .mobileconfig
  - xml files that store profile info
- Trust profile
  - needed for self-signed servers
- Enrollment profile
  - provided by MDM for enrollment

Profile.mobileconfig…



Settings for BusyExecs

2 Payloads Configured - Created 02/12/14 at 9:23 AM

Hard Disk Media Access

Access settings for hard disk media

Internal Disks: ☑ Allow
☐ Require Authentication
☐ Read-Only

External Disks: ☑ Allow
☐ Require Authentication
☐ Read-Only

Disk Images: ☑ Allow
☐ Require Authentication
☐ Read-Only

DVD-RAM: ☑ Allow
☐ Require Authentication
☐ Read-Only

Disc Media Access

Access settings for removable disc media

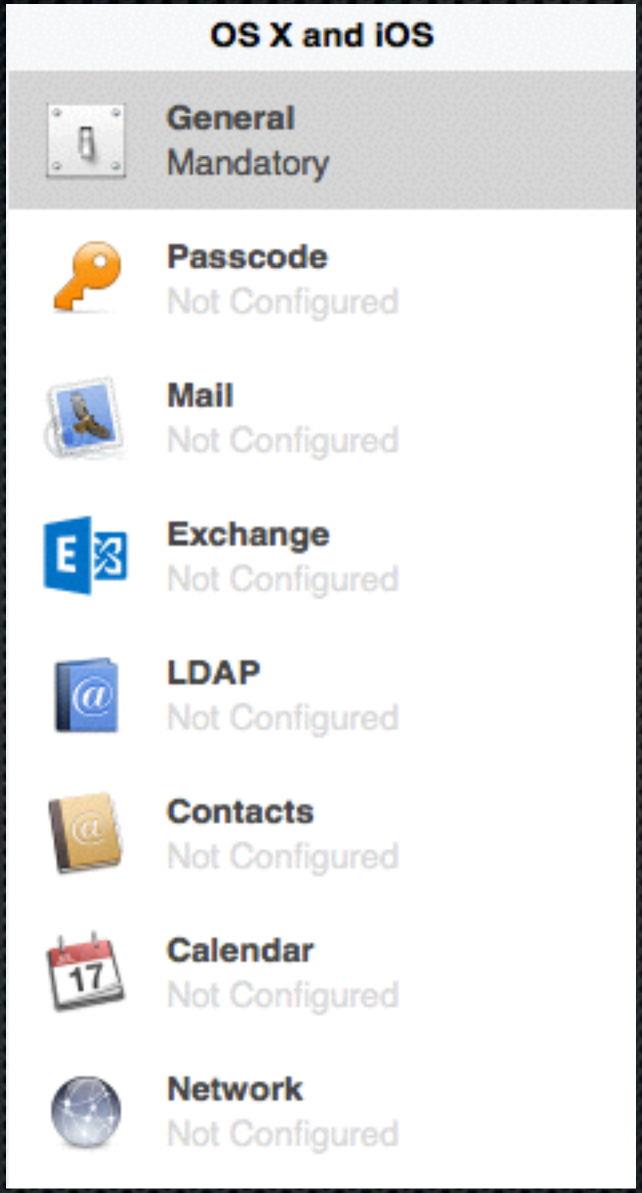
CDs & CD-ROMs: ☑ Allow
☐ Require Authentication

DVDs: ☑ Allow
☐ Require Authentication

Recordable Discs: ☑ Allow

```
  <key>PayloadDisplayName</key>
  <string>Restrictions</string>
  <key>logout-eject</key>
  <dict/>
  <key>mount-controls</key>
  <dict>
    <key>blankcd</key>
    <array/>
    <key>blankdvd</key>
    <array/>
    <key>cd</key>
    <array/>
    <key>dvd</key>
    <array/>
    <key>dvdram</key>
    <array/>
    <key>disk-image</key>
    <array/>
    <key>harddisk-external</key>
    <array/>
    <key>harddisk-internal</key>
    <array/>
  </dict>
</dict>
<dict>
  <key>PayloadType</key>
  <string>com.apple.DiscRecording</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>PayloadIdentifier</key>
  <string>com.apple.mdm.ml.kkheconsulting.com.8aca65e0-7032-013
  <key>PayloadEnabled</key>
  <true/>
  <key>PayloadUUID</key>
  <string>60c20226-fa71-aafc-8332-1302aa02d6bc</string>
  <key>PayloadDisplayName</key>
  <string>Media Access:  Disc Recording</string>
  <key>BurnSupport</key>
  <string>on</string>
</dict>
<dict>
```

USER Profile 1 - OS X & iOS



OS X and iOS

General
Mandatory

Passcode
Not Configured

Mail
Not Configured

Exchange
Not Configured

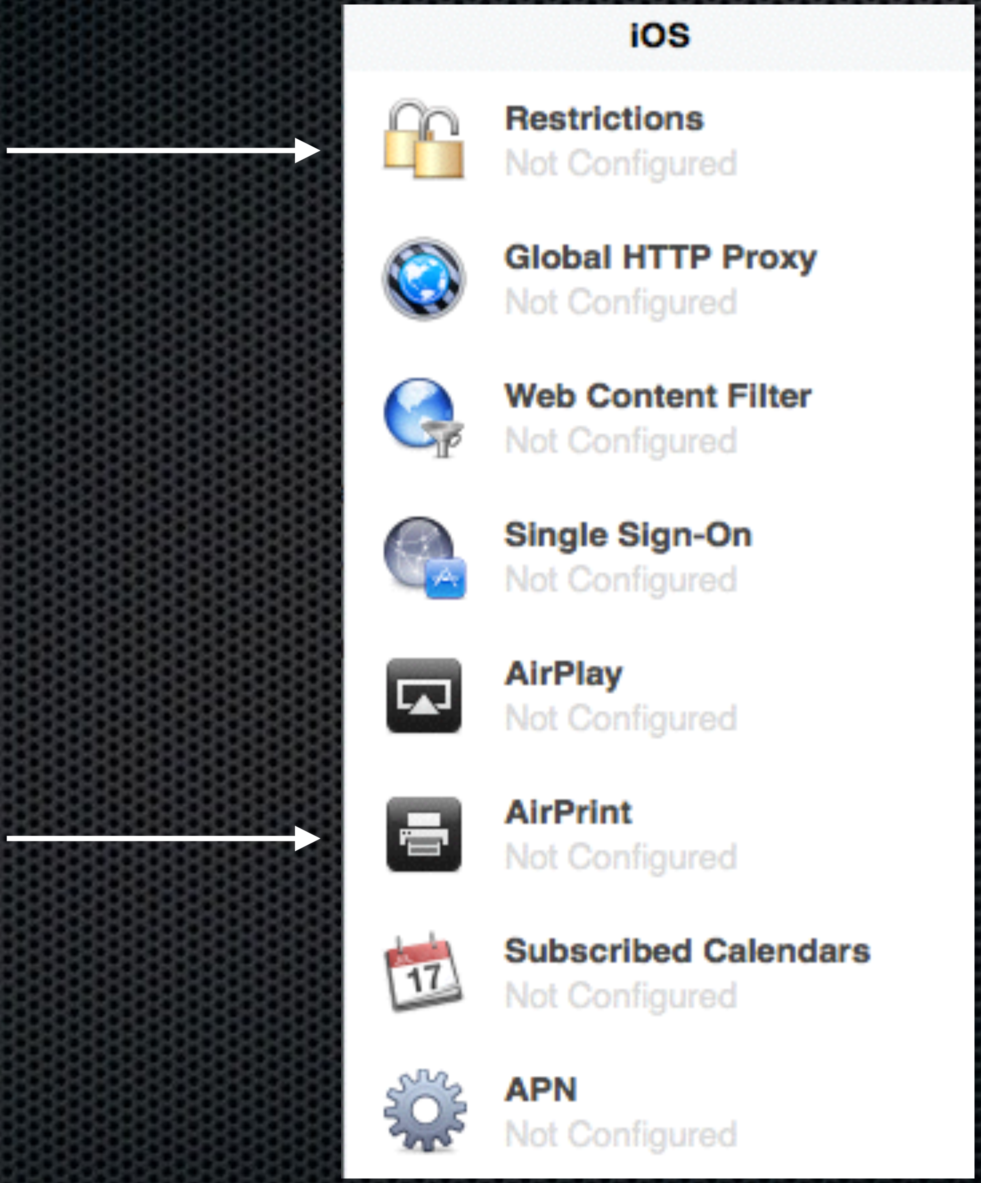
LDAP
Not Configured

Contacts
Not Configured

Calendar
Not Configured

Network
Not Configured

USER Profile 2 - iOS only



iOS

Restrictions
Not Configured

Global HTTP Proxy
Not Configured

Web Content Filter
Not Configured

Single Sign-On
Not Configured

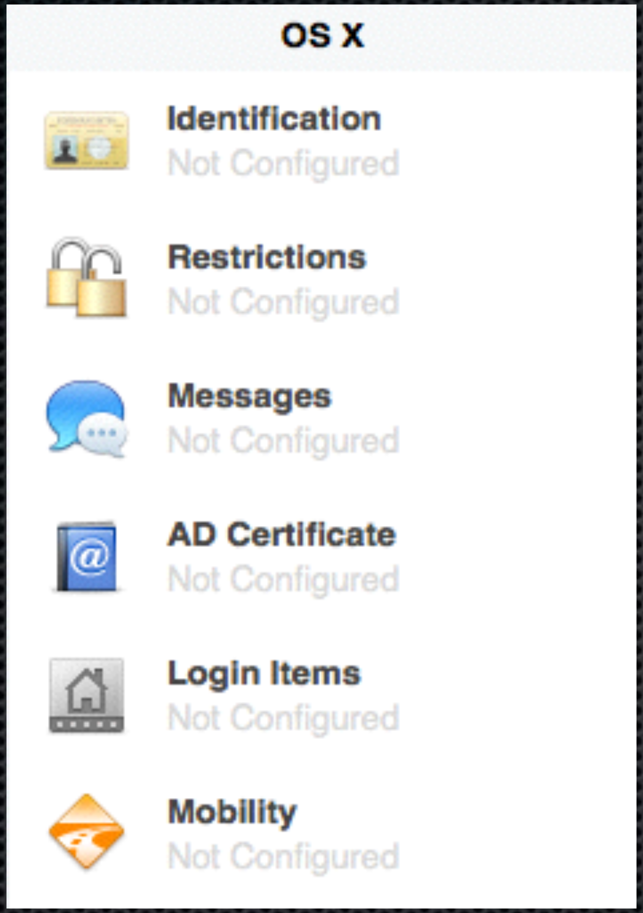
AirPlay
Not Configured

AirPrint
Not Configured

Subscribed Calendars
Not Configured

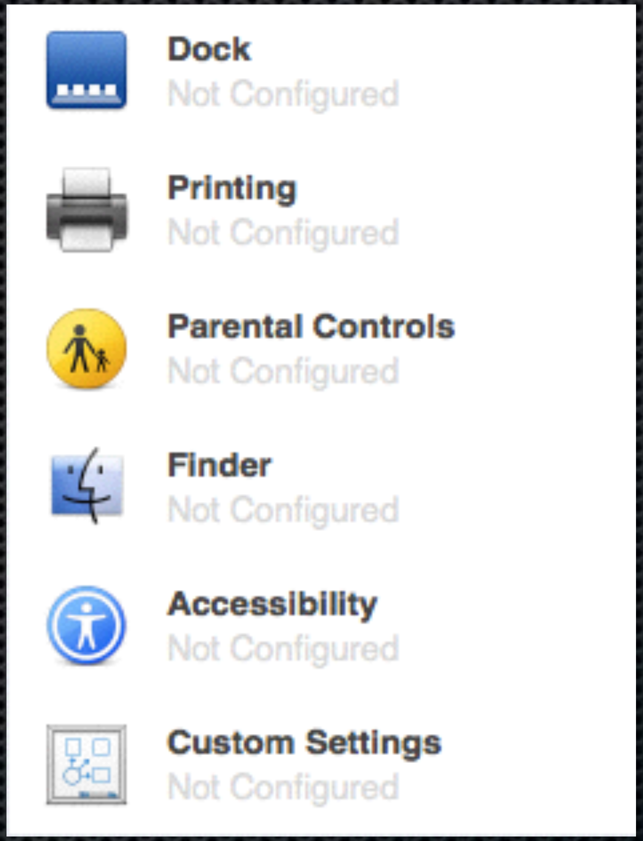
APN
Not Configured

USER Profile 3 - OS X only



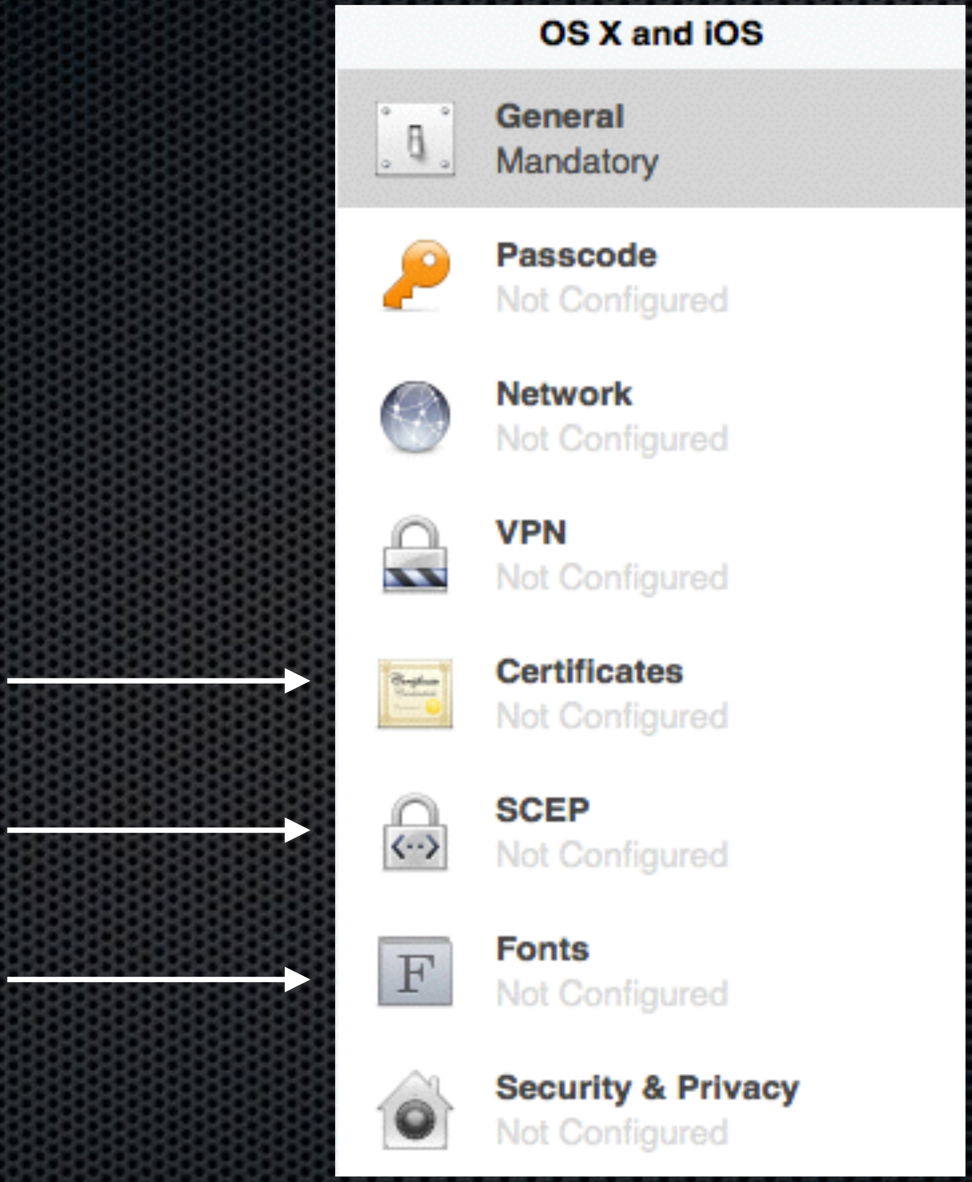
OS X

- **Identification** Not Configured
- **Restrictions** Not Configured
- **Messages** Not Configured
- **AD Certificate** Not Configured
- **Login Items** Not Configured
- **Mobility** Not Configured



- **Dock** Not Configured
- **Printing** Not Configured
- **Parental Controls** Not Configured
- **Finder** Not Configured
- **Accessibility** Not Configured
- **Custom Settings** Not Configured

DEVICE Profile 1 - OS X & iOS



OS X and iOS

General
Mandatory

Passcode
Not Configured

Network
Not Configured

VPN
Not Configured

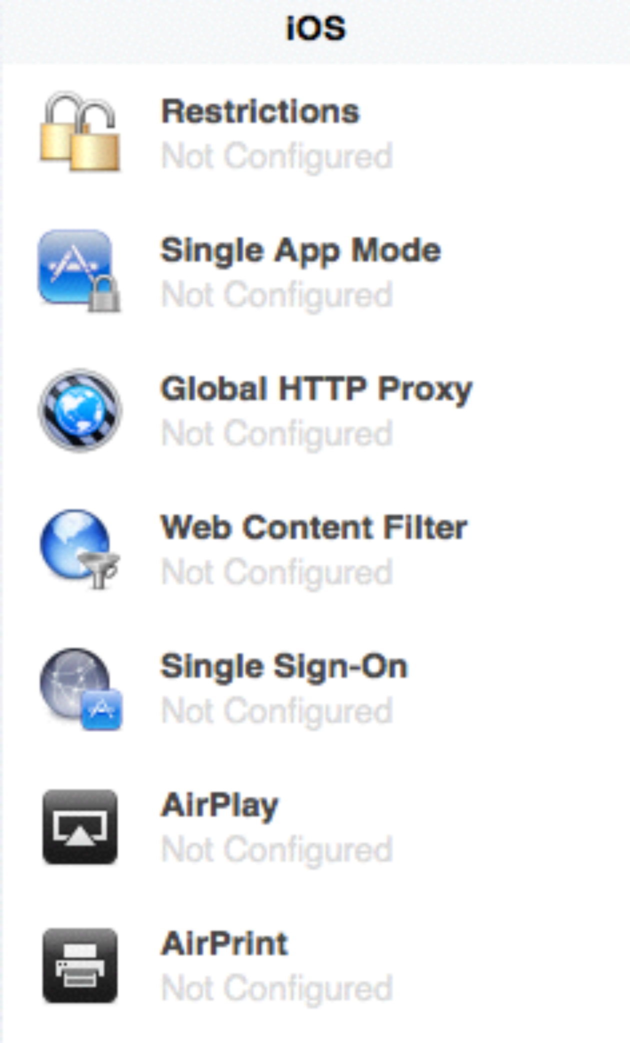
Certificates
Not Configured

SCEP
Not Configured

Fonts
Not Configured

Security & Privacy
Not Configured

DEVICE Profile 2 - iOS only



iOS

Restrictions
Not Configured

Single App Mode
Not Configured

Global HTTP Proxy
Not Configured

Web Content Filter
Not Configured

Single Sign-On
Not Configured

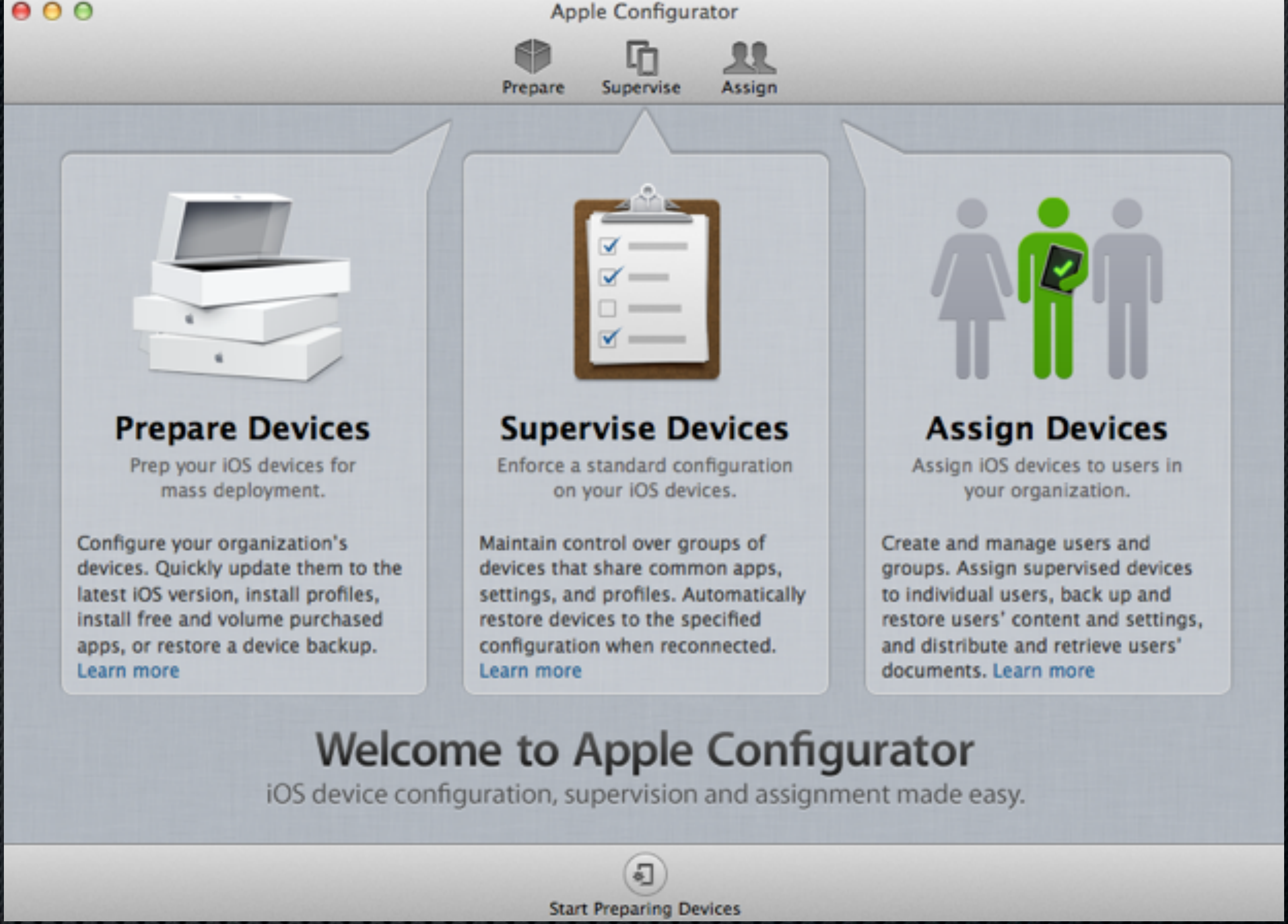
AirPlay
Not Configured

AirPrint
Not Configured

Profile Delivery

- Manually - via email, file server, website, or ARD
- Manually - via tethering (iPCU or Apple Configurator)
- Manually by user - via a self-service portal
- Automatically - via a MDM solution

Apple Configurator



Prepare Devices

Prep your iOS devices for mass deployment.

Configure your organization's devices. Quickly update them to the latest iOS version, install profiles, install free and volume purchased apps, or restore a device backup. Learn more

Supervise Devices

Enforce a standard configuration on your iOS devices.

Maintain control over groups of devices that share common apps, settings, and profiles. Automatically restore devices to the specified configuration when reconnected. Learn more

Assign Devices

Assign iOS devices to users in your organization.

Create and manage users and groups. Assign supervised devices to individual users, back up and restore users' content and settings, and distribute and retrieve users' documents. Learn more

Welcome to Apple Configurator

iOS device configuration, supervision and assignment made easy.

Apple Configurator

- Three modes:
  - Prepare
  - Supervise
  - Assign
- Knowing when devices are in danger of being erased.
- Integration of assignment with a directory service.

Why Apple Configurator (still)

- No way to "Supervise" a device over the air
  - Certain attributes can only be managed if device is supervised (Airdrop)
- No way to lock an over the air MDM enrollment profile so user can't remove it
- No way to distribute and then revoke apps using just one Apple ID.
- Great way to generate Profiles for use in other tools…

Demo…

Configurator

OTA
(Over The Air)

Main Players

- Meraki
- Absolute
- Apple Profile Manager
- BoxTone
- Centrify
- Filewave
- JAMF Casper Suite
- MaaS360 by Fiberlink
- MobileIron
- SOTI

and on and on...

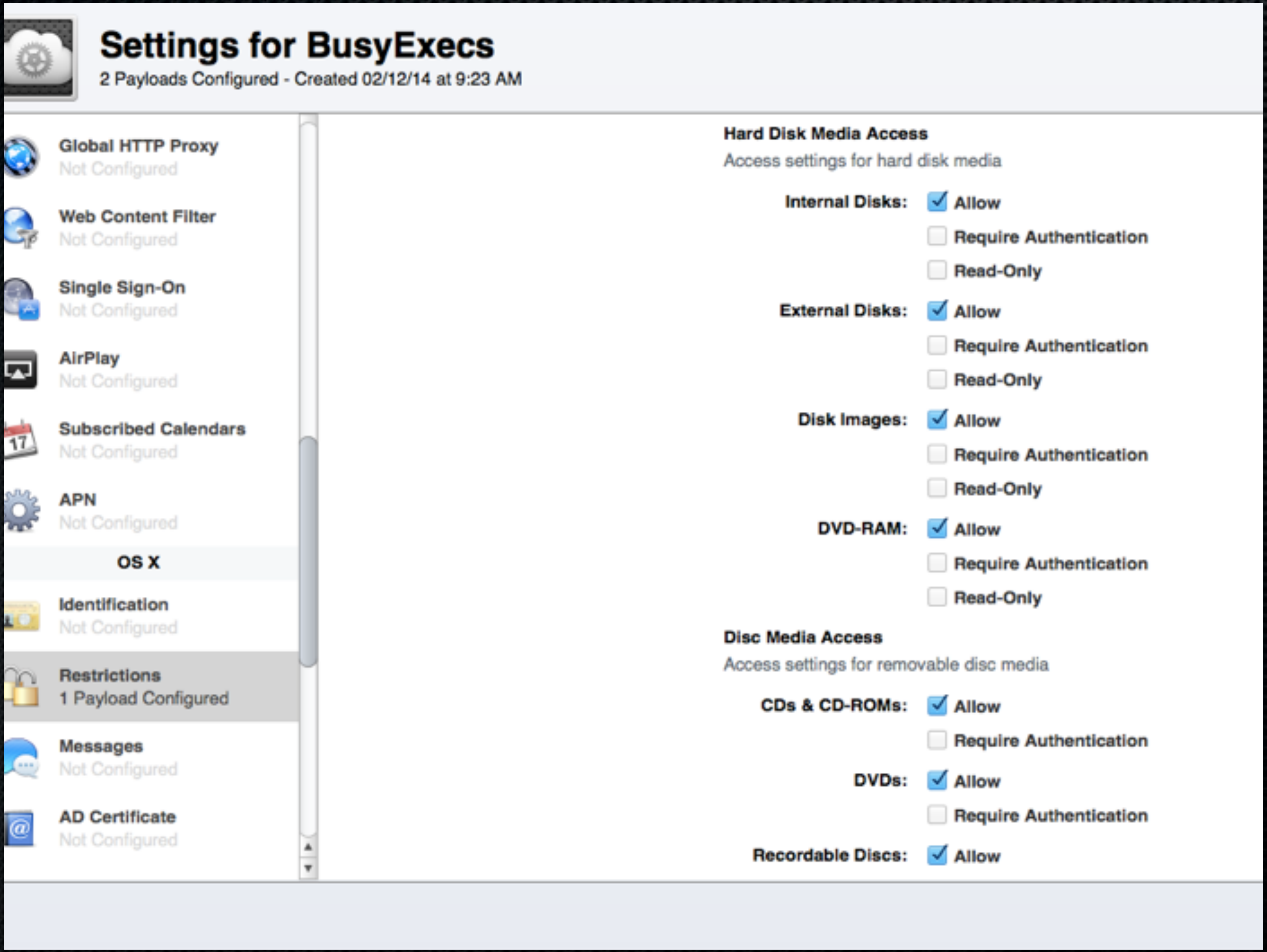
Main Uses and Differences

- What features should you be looking for?
- What size solution do you need?
- Who will maintain it?
- Where do they excel?
- How do you choose?

Apple's Profile Manager

(http://help.apple.com/profilemanager/mac/3.0/#)

Apple Profile Manager



Settings for BusyExecs

2 Payloads Configured - Created 02/12/14 at 9:23 AM

Hard Disk Media Access

Access settings for hard disk media

Internal Disks: ☑ Allow
☐ Require Authentication
☐ Read-Only

External Disks: ☑ Allow
☐ Require Authentication
☐ Read-Only

Disk Images: ☑ Allow
☐ Require Authentication
☐ Read-Only

DVD-RAM: ☑ Allow
☐ Require Authentication
☐ Read-Only

Disc Media Access

Access settings for removable disc media

CDs & CD-ROMs: ☑ Allow
☐ Require Authentication

DVDs: ☑ Allow
☐ Require Authentication

Recordable Discs: ☑ Allow

Apple’s Profile Manager:

- Components of Profile Manager
    - Administration portal
    - Self-service user portal
    - MDM service
    - App and book distribution
- User and Device groups
- Distribute configuration profiles
    - Manual distribution
    - User self-service
    - Remote device management

Apple's Profile Manager:

- Distributing Apps and Books
  - VPP app distribution for education and enterprise
- Enrolling devices and computers
- Importing device and computer lists
- Associating devices with users
- Deploying a trust profile

Apple’s Profile Manager (more):

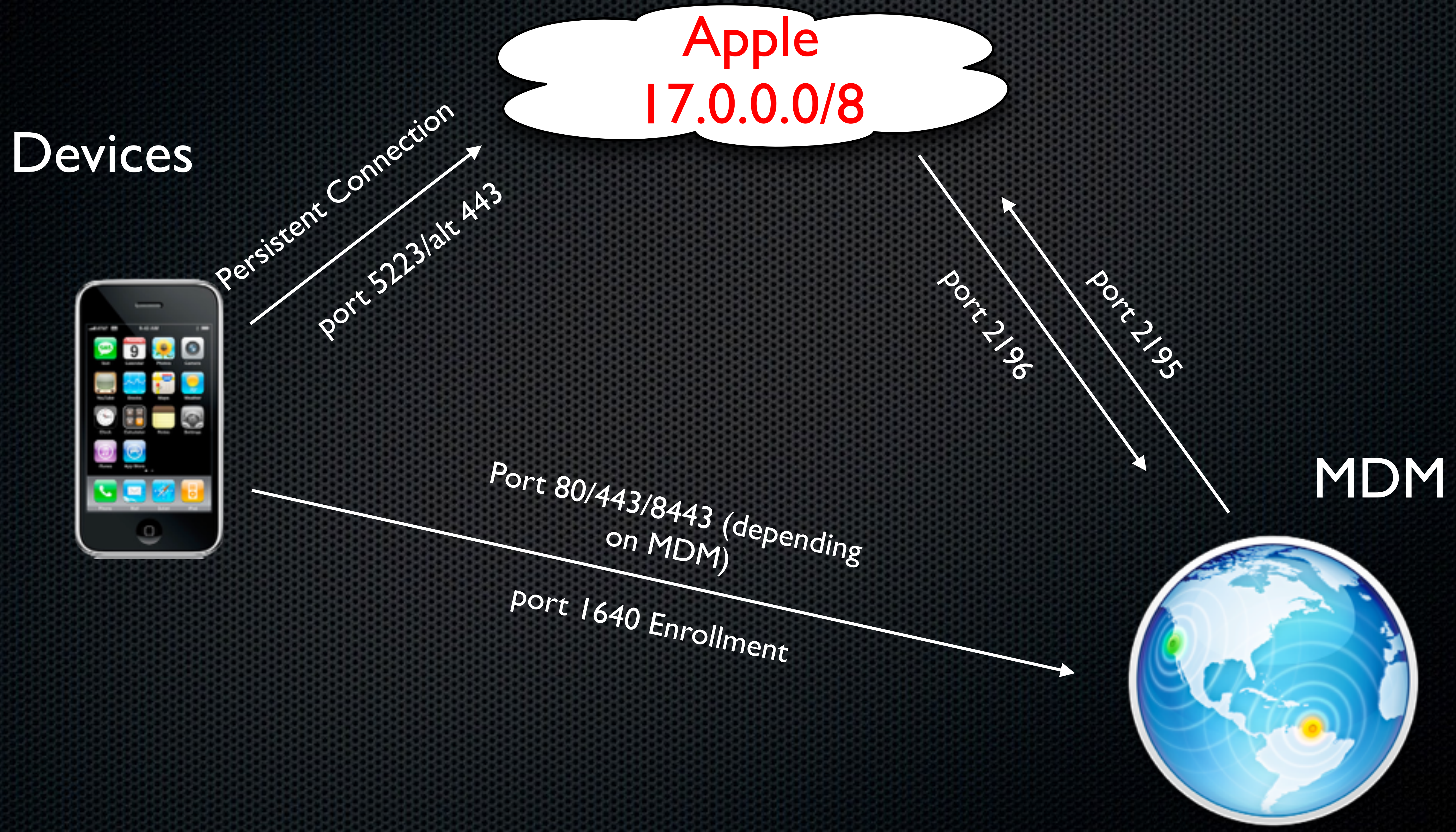
- Creating an enrollment profile
- Creating and installing configuration profiles
    - Apply payloads effectively
    - Payload interactions
    - Payload variables
- User and group management
- Managing in-house enterprise apps for users and user groups

Apple’s Profile Manager (more):

- iOS management options
- Mac OS management options
- Generic management options

Apple Push Notification Service (APNs)

APNS



Apple
17.0.0.0/8

Devices

Persistent Connection
port 5223/alt 443

port 2196

port 2195

MDM

Port 80/443/8443 (depending on MDM)

port 1640 Enrollment

MACTECH

APNs: Load Balancing

- Apple Push Notification Service (APNs) servers use load balancing.
- Your devices will not always connect to the same public IP address for notification.
- The entire 17.0.0.0/8 address block is assigned to Apple, so it's best to allow this range in your firewall settings.

Firewalls

- For APNs traffic to get past your firewall, you'll need to open these ports:
  - OutBound
    - TCP port 5223 (used by devices to communicate to the APNs Servers)
    - TCP port 2195 (used to send notifications to the APNs)
    - TCP port 443 (used as a fallback on Wi-Fi only, when devices are unable to communicate to APNs on port 5223)
  - InBound
    - TCP port 1690 (
    - TCP port 2196 (used by the APNs feedback service)

Compare and Contrast leading MDM solutions

- Countless players
- Compare and contrast
- Find the features you need
- Great resource at: http://www.enterpriseios.com/wiki/Comparison_MDM_Providers

Demo…

Profile Manager

New in iOS 8

- Reset activation lock
- Hides all profiles installed via MDM
- Categorizes profiles by type
- Users can not remove individual profiles installed via MDM
- Query date of last iCloud backup
- Query which iTunes account is configured

New in OS X 10.10

- Deploy flat packages
- Deploy managed apps
- Managed Domains
- MDM command to begin AirPlay
- Query which iTunes account is configured

Questions?

Ahmed Kufaishi
ahmed@alarytech.ca