Profiles

LeRoy Dennison
Dennison Consulting
LeRoy@dennison.com

MACTECH

LeRoy Dennison

- Over 30 years of IT experience, starting with service in the U.S. Coast Guard.
- Employers since USCG:
  - Christopher Newport University
  - Computer Sciences Corp. @ NASA Langley Research Center
  - MacCenter
  - Apple
  - Active Storage
  - PC Mall Services / PCM
- LeRoy is now doing contract work, specializing in Technical Learning & Development, Mac System Administration, and MDM.

What are Profiles?

```
<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>
```

Questions?

Profile Basics

- Categories:
  - User (and user group) profiles
  - Device (and device group) profiles
- Profile types
  - Configuration profiles
  - Managed profiles
  - Trust profiles
  - Provisioning profiles

Configuration Profiles

- A configuration profile is an XML file that allows you to distribute configuration information.

- A configuration profile contains a number of settings that you can specify, including:
  - Restrictions on device features
  - Wi-Fi settings
  - VPN settings
  - Email server settings
  - Exchange settings
  - LDAP directory service settings
  - CalDAV calendar service settings
  - Web clips
  - Credentials and keys

- Configuration profiles are in property list format, with ***Data*** values stored in Base64 encoding. The ***.plist*** format can be read and written by any XML library.

Managed Profiles

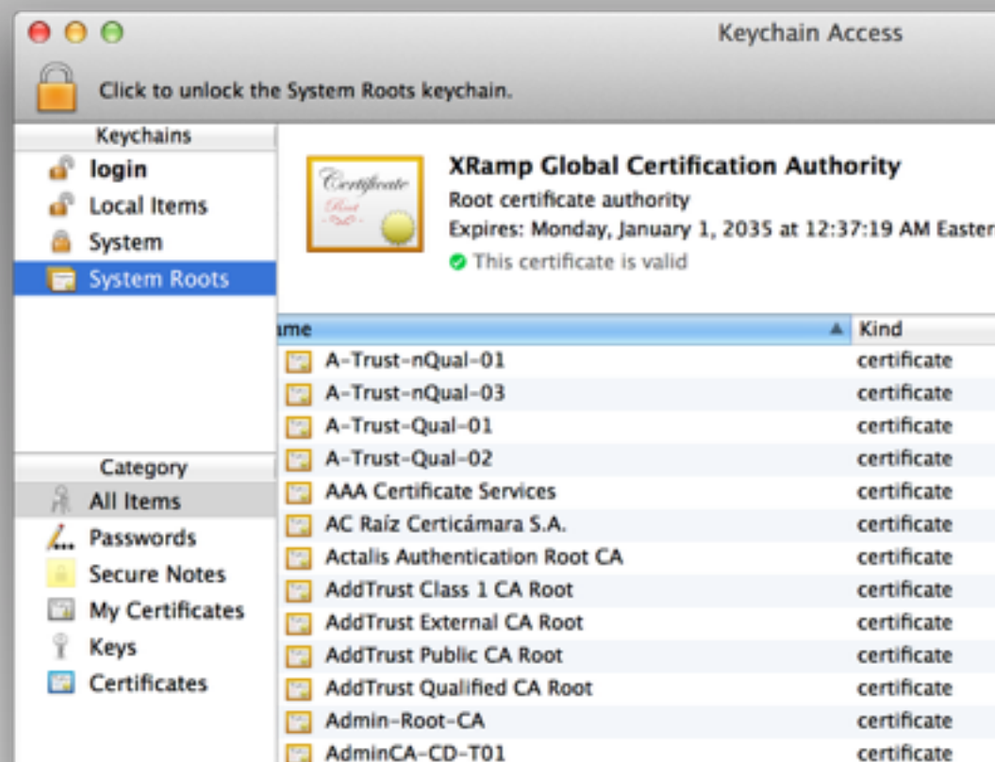
- A configuration profile that has been installed by an MDM solution
- The primary MDM profile manages anything delivered by MDM after enrollment and contains several “rights” to the system, including:
  - Erase all data on the computer/wipe device
  - Add or remove configuration profiles
  - Add or remove provisioning profiles
  - Lock screen
  - Query information about different settings including security, computer, network, installed applications, and installed profiles

Trust Profiles

- A profile that tells an iOS device to “trust” the MDM server for SSL communication
- For use when you are using an SSL or code signing certificate that is self-signed, or is signed by an authority not in Apple's default trust chain.
- Typically installed along with an enrollment profile on mobile devices

iOS 7: List of available trusted root certificates

http://support.apple.com/kb/HT5012



Provisioning Profiles

- A provisioning profile is a collection of digital entities that uniquely ties developers and devices to an authorized iPhone Development Team and enables a device to be used for testing.
- This allows an application to be installed without downloading it from the iTunes App Store.
- Common for testing of apps under development that will either be distributed via the App Store when complete or managed as In-House apps via an MDM solution.

Profile Structure & Format

- XML files that store key-value pairs in a property list (.plist) format and have a ***.mobileconfig*** suffix
- Both OS X and iOS use the same file format for configuration profiles
- Each configuration profile contains one or more payloads

```
<key>PayloadContent</key>
<array>
    <dict>
        <key>ABT_PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadDescription</key>
        <string>Configures security-related items.</string>
        <key>PayloadDisplayName</key>
        <string>Passcode</string>
        <key>PayloadIdentifier</key>
        <string>FB60D71D-2F0F-4678-A30C-281E4E37A8BB.passwordpolicy
        <key>PayloadOrganization</key>
        <string>Pharmetrics</string>
        <key>PayloadType</key>
        <string>com.apple.mobiledevice.passwordpolicy</string>
        <key>PayloadUUID</key>
        <string>1A264C7C-EE3A-45B5-98DD-5C4A1DA369F7</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>allowSimple</key>
        <true/>
        <key>forcePIN</key>
        <true/>
        <key>maxInactivity</key>
        <integer>5</integer>
        <key>minLength</key>
        <integer>4</integer>
        <key>requireAlphanumeric</key>
        <false/>
    </dict>
</array>
```

Mandatory Keys

- The ***PayloadVersion*** key describes the version of the profile as a whole
- The ***PayloadUUID*** key is a globally unique identifier for the profile
  - In OS X, you can use the command `uuidgen(1)` to generate UUIDs
- The ***PayloadType*** key supports only the value *Configuration*
- The ***PayloadIdentifier*** key determines whether a new profile should replace an existing profile or be added
- The ***General settings* payload** is the only required payload in a configuration profile; it sets the name & identifier of the config profile

Configuration Profile Key Reference:

https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html

%Variables% in Profiles

- *User info variables*
  - full_name, first_name, last_name, email, job_title, mobile_phone, short_name, guid
- *Device info variables*
  - ICCID, OSVersion, SerialNumber, ProductName, BuildVersion, IMEI, WIFIMAC
- *802.1X network variables*
  - AD_ComputerID, AD_Domain, AD_DomainForrestName, AD_DomainNameDNS, AD_KerberosID, ComputerName, HardwareUUID, HostName, LocalHostName, MACAddress, SerialNumber

Signed Profiles

- The payload data on a configuration profile can contain sensitive information
- A signed profile can be encrypted
- A profile that's signed can be replaced only by another profile with the same ***identifier*** that's also ***signed*** by the same source

Creating Profiles

- Text Editor
- iPhone Configuration Utility (iPCU)
- Apple Configurator
- Profile Manager
- 3rd party MDM solution

More on this after a couple of additional slides

Distributing Profiles

- Manually, via tethering (iPCU or Apple Configurator)

  With these two tools, they get installed as well

- Manually, via email, file server, website, or ARD

- Manually by user, via a self-service portal

- Automatically, via a MDM solution

  After initial enrollment, they get installed as well with a MDM solution

Installing Profiles

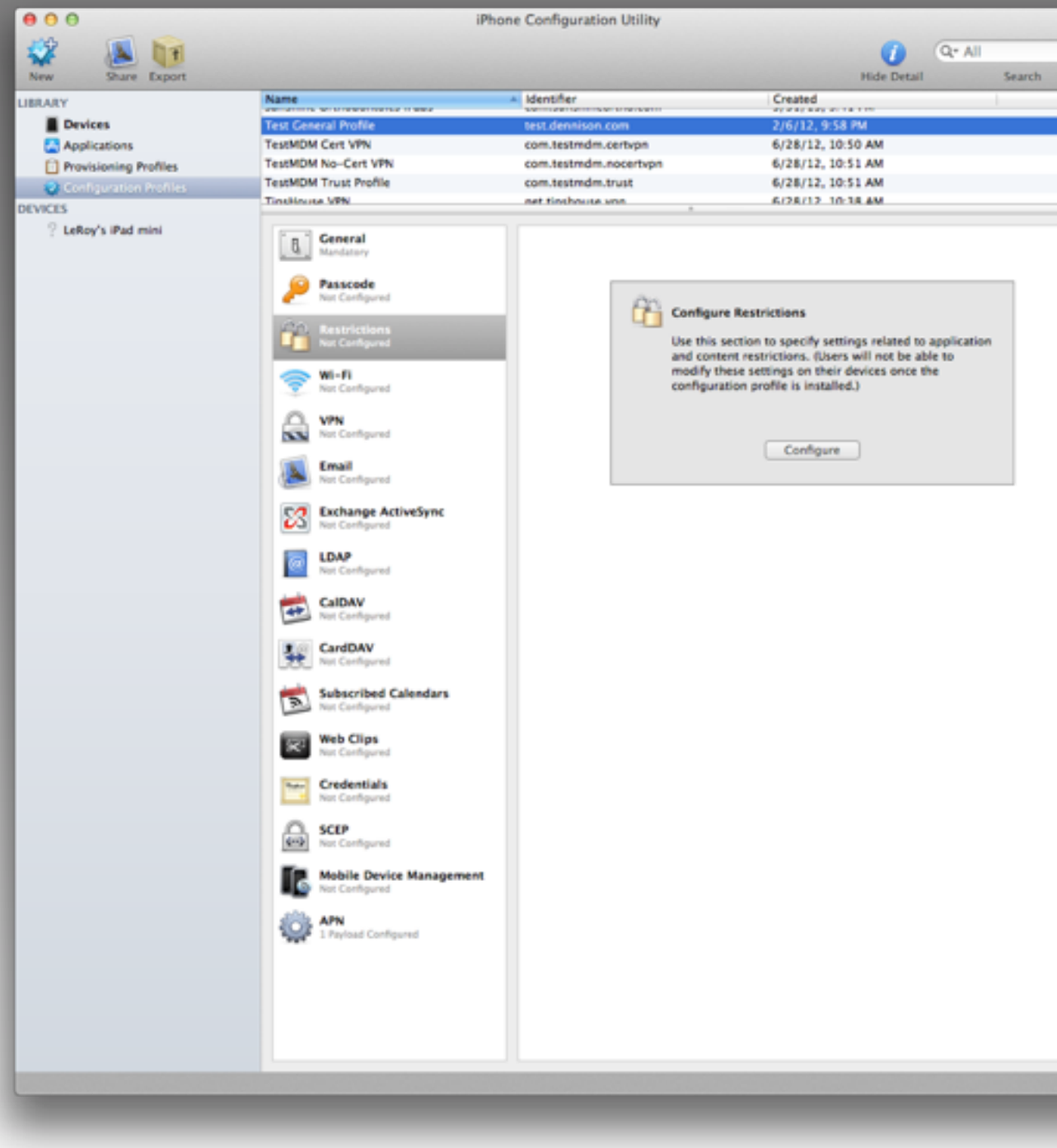
- Manually via Finder
- Automatically via ARD (or other client management solution)
- Automatically via System Image Utility (or other imaging solution)
- Automatically via Terminal using the *`profiles`* command
- Automatically via MDM solution once device is enrolled

Three Apple Tools

MACTECH

iPhone Configuration Utility (iPCU)

- Utility for creating and installing profiles and apps
- Available for Mac OS X and Windows
- Mac Download: http://support.apple.com/kb/DL1465
  - Note: for use with Lion & Mountain Lion; for Mavericks, use Apple Configurator



Apple Configurator

- Three modes:
  - Prepare
  - Supervise
  - Assign

Profile Manager

MACTECH

Mobile Device Management

a quick overview

MACTECH

MDM Tiers

- Tier 4 - 3rd party MDM (needed for any MDM scenarios that are not all iOS)
- Tier 3 - Profile Manager (OS X Server), over-the-air updates
- Tier 2 - Profiles distributed via email, file server, or HTTP
- Tier 1 - iPCU or Apple Configurator, tethered
- Tier 0 - Manual, on the device itself

Apple's new Device Enrollment Program

- The Device Enrollment Program simplifies initial setup by
  - **Automating Mobile Device Management (MDM) enrollment** and supervision of devices during setup and
  - Enabling management of devices **without touching them**.
- To further simplify the process, it's now even easier to **skip certain Setup Assistant screens** so users can start using their devices right out of the box.

Note: As of today, this is only available on iOS devices purchased directly from Apple

Apple has a PDF guide on this available at:
https://www.apple.com/iphone/business/docs/DEP_Business_Guide_EN_Feb14.pdf

DEP: Mandatory & Lockable MDM Enrollment

- The Device Enrollment Program enables automatic management all institutionally-owned devices.
- While completing the Setup Assistant, **the device can be preconfigured to require automatic enrollment into MDM**.
  - This ensures that devices are configured based on the institution's requirements, and guarantees that all users get the same setup on their devices.
- Can also lock device in MDM for ongoing management
  - i.e., **users can't remove the management config profile**

DEP: Wireless Supervision

- Supervision mode provides a higher level of device management for institutionally-owned iOS devices.
  - It allows additional restrictions, such as turning off iMessage or Game Center, and it provides additional device configurations and features, such as web content filtering and **single-app mode**.
- Can **wirelessly enable Supervision mode** on a device as a part of the setup process.

DEP: Streamlined Setup Assistant

- The Device Enrollment Program makes it even easier to set up users on iPad, iPhone, or Mac.
- After you've configured devices through your MDM solution, users are guided through the activation process with the built-in Setup Assistant.
- Can streamline the Setup Assistant even further by **specifying that certain screens be skipped**.
  - Passcode. *Hides and disables the passcode pane.*
  - Location. *Does not enable Location Services.*
  - Restore from backup. *Disables restoring from backup.*
  - Apple ID. *Does not allow you to sign in with an Apple ID.*
  - Terms of Service. *Skips the Terms of Service.*
  - Siri. *Disables Sir*i.
  - Sending diagnostics. *Disables automatically sending diagnostic information.*

Mobile Device Management

Configure

Enroll

Query

Manage

Apple Push Notification service (APNs)

- Apple Push Notification service (APNs) servers use load balancing
- Devices will not always connect to the same 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 firewall settings

Ports Used

Service	TCP Ports
HTTP	80
HTTPS	443
SCEP	1640
APNs	5223, 2195, 2196

Profile Manager

some details

MACTECH

Profile Manager's 3 parts

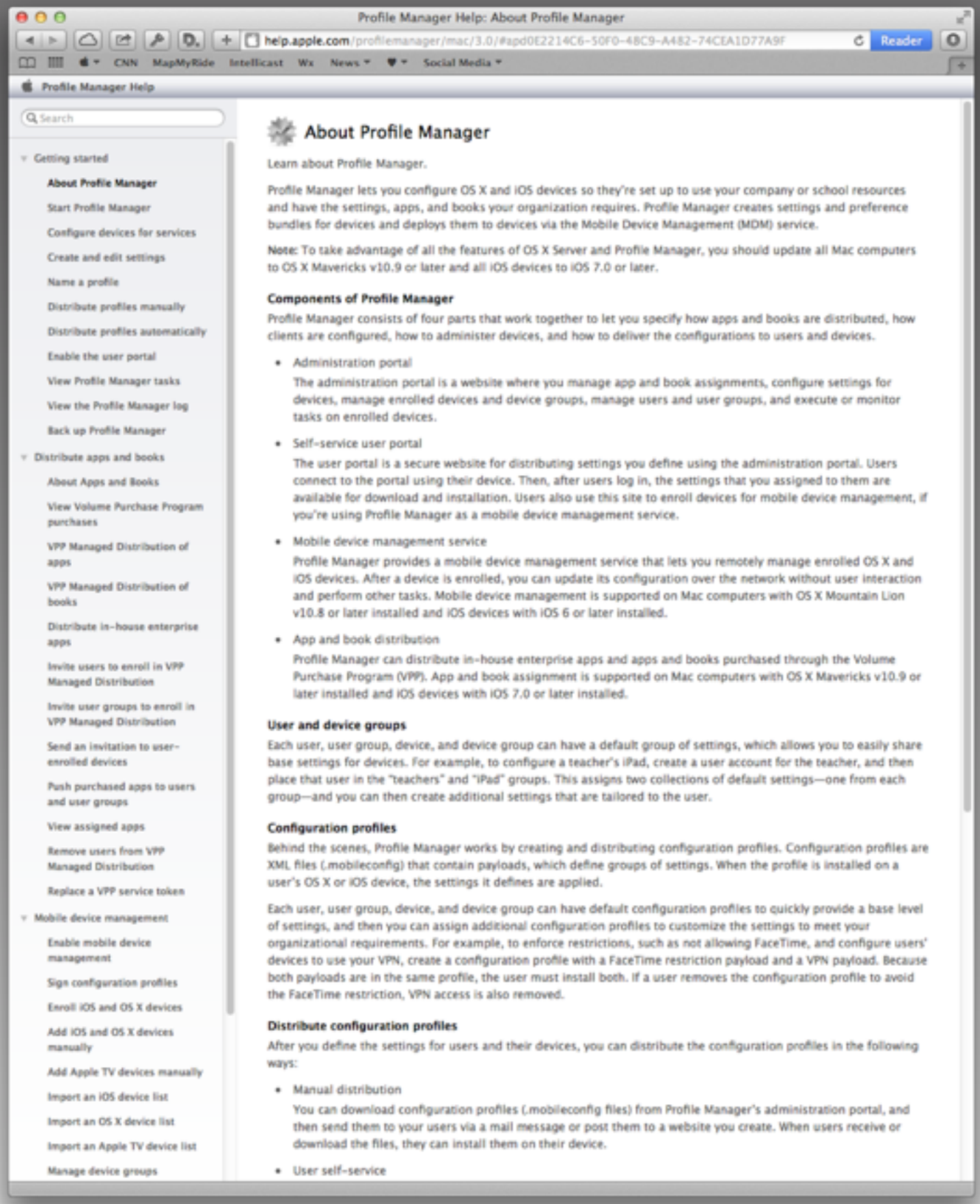
- **Profile Manager web tool**
  - *https://server.domain.com/profilemanager/*
- **User Portal website**
  - *https://server.domain.com/mydevices/*
- **MDM Server**
  - *For Lion and later computers & iOS 4 and later devices*

Profile Manager

- Distributing Apps and Books
  - *VPP distribution for education and enterprise*
  - *Distributing in-house apps*
- Enrolling devices and computers
- Importing device and computer lists
- Associating devices with users

http://www.apple.com/ipad/business/it/

http://help.apple.com/profilemanager/mac/3.0/



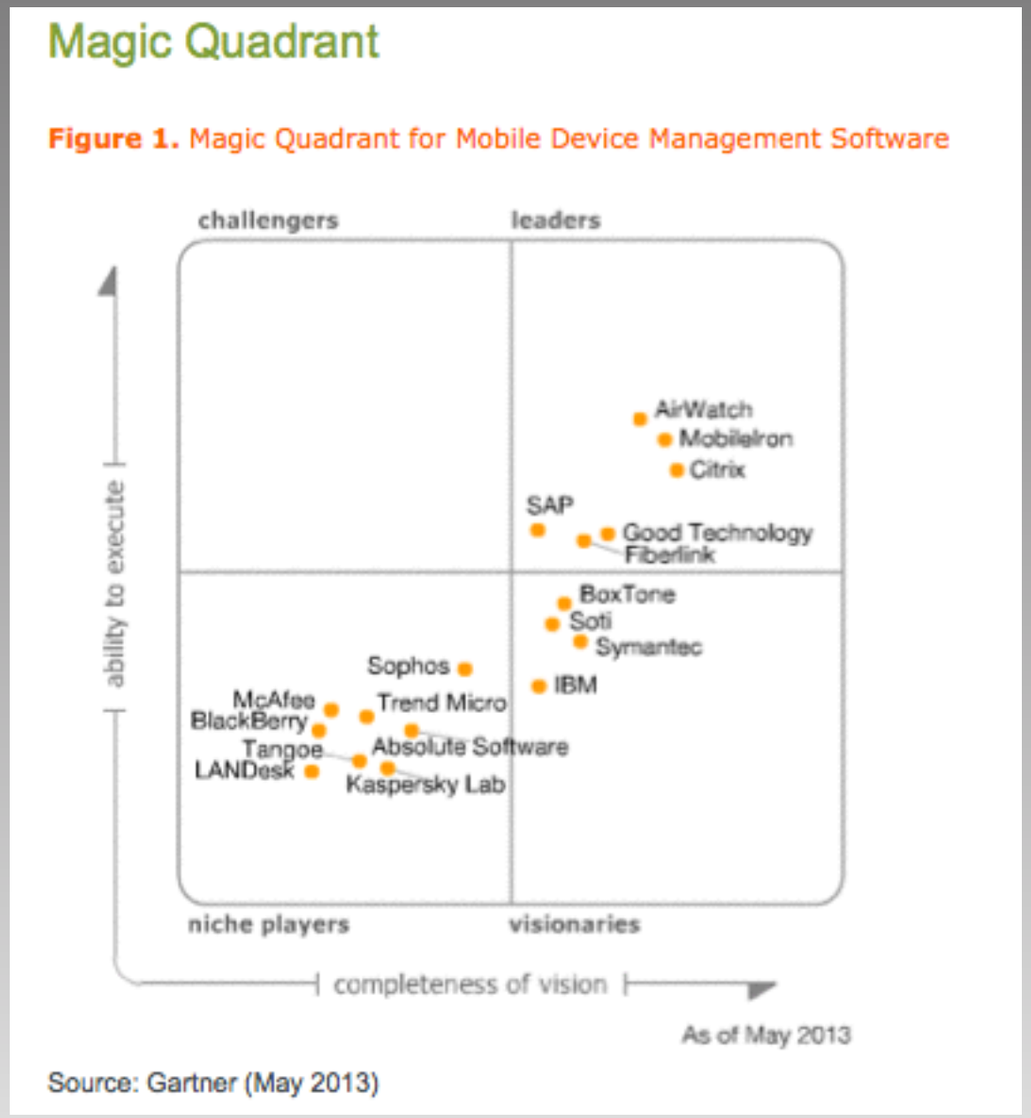
MACTECH

MDM Players

MACTECH

MDM Leaders

- MobileIron
- AirWatch
- MaaS360, by Fiberlink



Source: Gartner (May 2013)

MACTECH

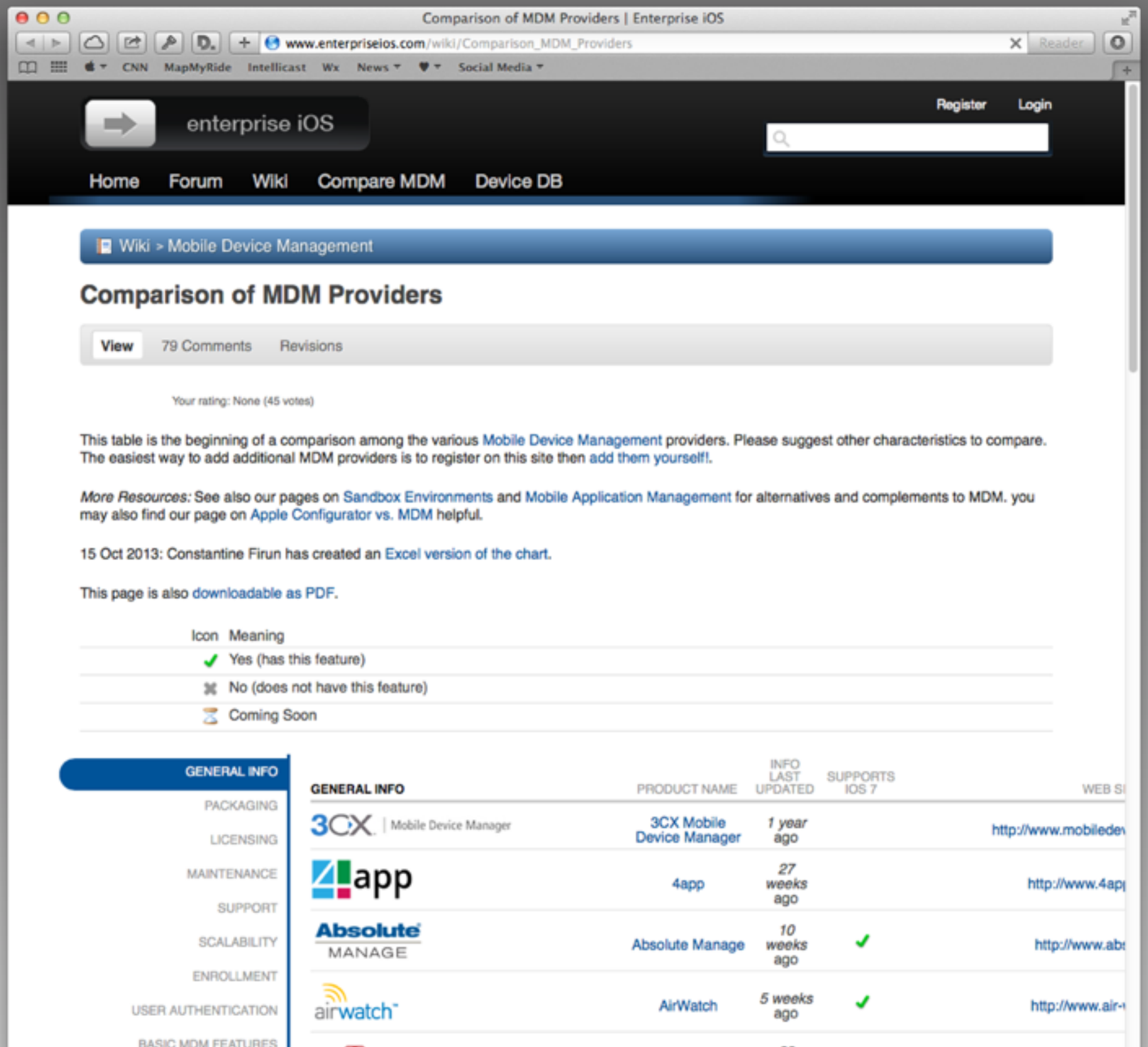
Client Mgmt. solutions that do MDM

- Casper Suite, by JAMF Software
- Absolute Manage
- FileWave

Network solutions that do MDM

- Meraki
- Aruba Networks
- Juniper Networks

http://enterpriseios.com (by TekServe)



MACTECH

Questions?