

Profiles

LeRoy Dennison
Dennison Consulting
LeRoy@dennison.com

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

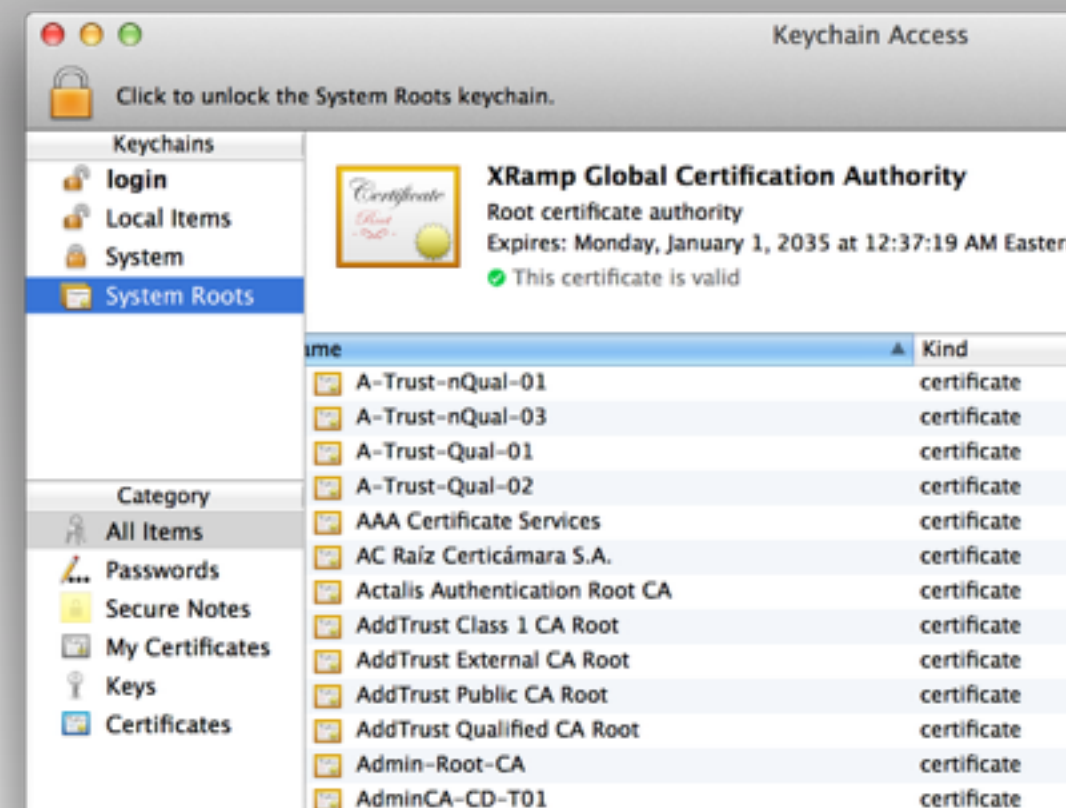
- A configuration profile that has been installed by an MDM solution
- The primary MDM profile manages anything delivered by MDM after enrollment and contains several “rights” to the system, including:
 - Erase all data on the computer/wipe device
 - Add or remove configuration profiles
 - Add or remove 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</string>
    <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

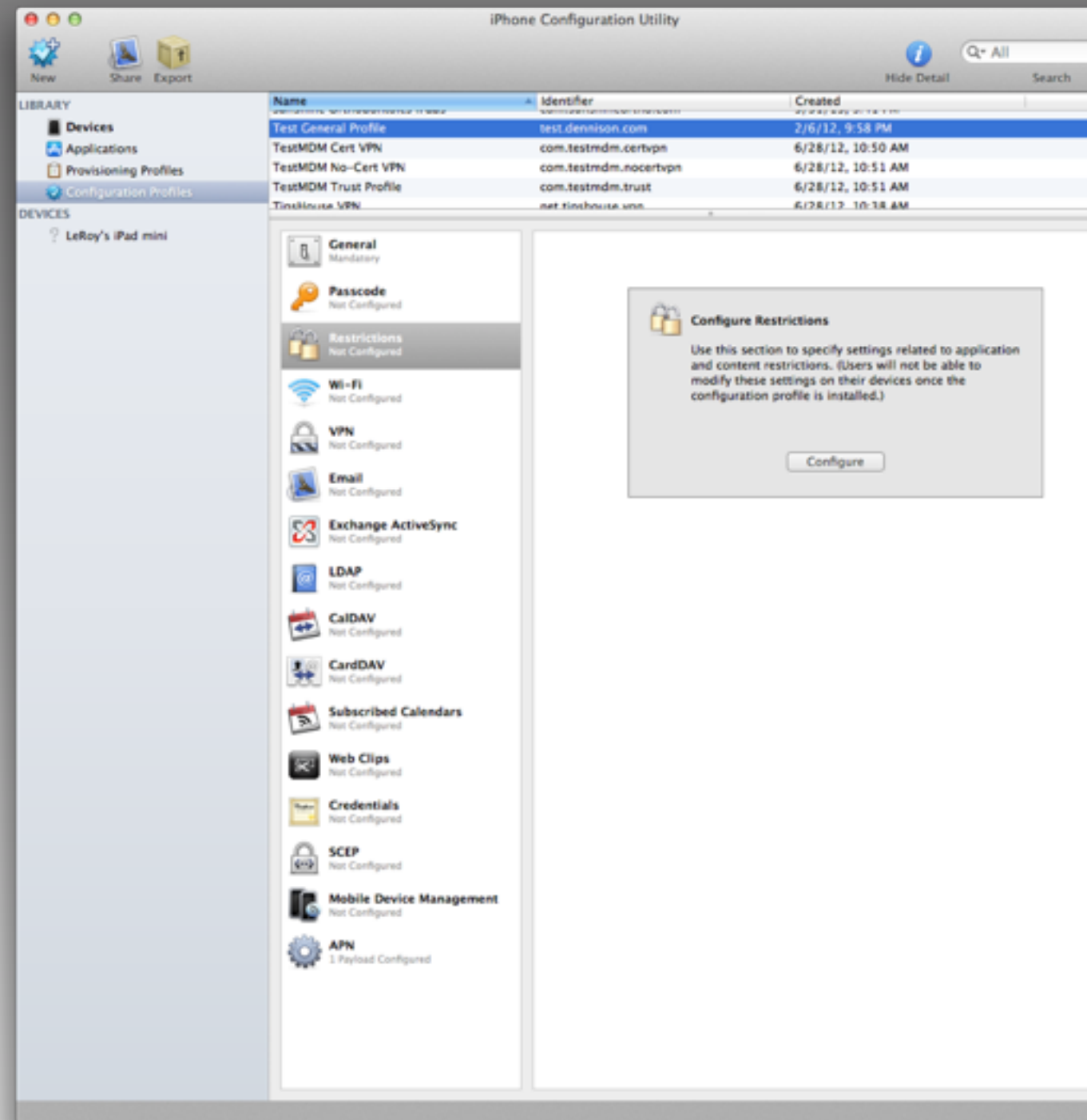
Installing Profiles

- 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

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



Settings for iPhones

2 Payloads Configured – Updated 03/05/13 at 4:41 PM

OS X and iOS

General

1 Payload Configured

Passcode

1 Payload Configured

Network

Not Configured

VPN

Not Configured

Certificate

Not Configured

SCEP

Not Configured

Security & Privacy

Not Configured

iOS

Restrictions

Not Configured

Accessibility

Not Configured

Global HTTP Proxy

☒ **Allow simple value**
Permit the use of repeating, ascending, and descending character sequences

☐ **Require alphanumeric value**
Requires passcode to contain at least one letter

4

Minimum passcode length
Minimum number of passcode characters allowed

--

Minimum number of complex characters
Minimum number of non-alphanumeric characters allowed

730

Maximum passcode age
Days (1-730) after which the passcode must be changed

--

Maximum Auto-Lock
Device automatically locks when minutes elapse

Passcode history (iOS only)
Number (1-50) of unique passcodes before reuse

--

Maximum grace period for device lock (iOS only)
Maximum amount of time the device can be locked without prompting for passcode on unlock

--

Maximum number of failed attempts
Number of passcode entry attempts allowed before all data on device will be erased

Cancel

OK

Mobile Device Management

a quick overview

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 Siri.*
 - 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

Profile Manager's 3 parts

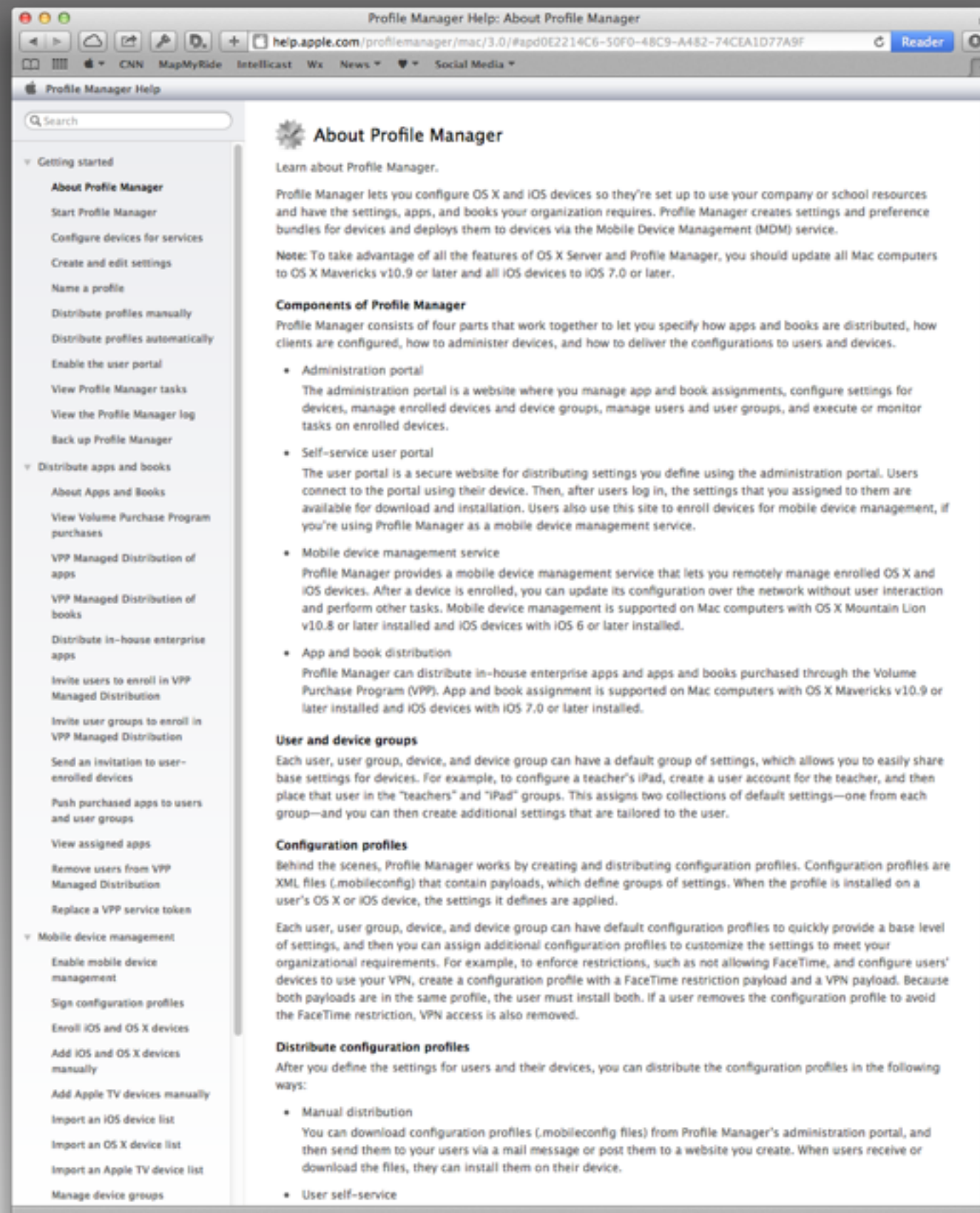
- **Profile Manager web tool**
 - *<https://server.domain.com/profilemanager/>*
- **User Portal website**
 - *<https://server.domain.com/mydevices/>*
- **MDM Server**
 - *For Lion and later computers & iOS 4 and later devices*

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/>



MDM Players

MDM Leaders

- MobileIron
- AirWatch
- MaaS360, by Fiberlink



Magic Quadrant

Figure 1. Magic Quadrant for Mobile Device Management Software



Source: Gartner (May 2013)

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)

The screenshot shows a web browser window with the URL www.enterpriseios.com/wiki/Comparison_MDM_Providers. The page title is "Comparison of MDM Providers | Enterprise iOS". The navigation bar includes links for Home, Forum, Wiki, Compare MDM, and Device DB. The main content area is titled "Comparison of MDM Providers" and includes a "View" button, "79 Comments", and "Revisions". Below this, there is a section for "Your rating: None (45 votes)". The text explains that the table is the beginning of a comparison among various Mobile Device Management providers and encourages users to suggest other characteristics to compare. It also provides more resources, including pages on Sandbox Environments, Mobile Application Management, and Apple Configurator vs. MDM. A note mentions that Constantine Firun created an Excel version of the chart on October 15, 2013. The page is also downloadable as a PDF. A legend defines the icons used in the table: a green checkmark for "Yes (has this feature)", a crossed-out circle for "No (does not have this feature)", and a clock for "Coming Soon". The table itself has columns for General Info, Product Name, Info Last Updated, Supports iOS 7, and Web Site. The providers listed are 3CX Mobile Device Manager, 4app, Absolute Manage, and AirWatch.

enterprise iOS

Register Login

Home Forum Wiki Compare MDM Device DB

Wiki > Mobile Device Management

Comparison of MDM Providers

View 79 Comments Revisions

Your rating: None (45 votes)

This table is the beginning of a comparison among the various [Mobile Device Management](#) providers. Please suggest other characteristics to compare. The easiest way to add additional MDM providers is to register on this site then [add them yourself!](#).

More Resources: See also our pages on [Sandbox Environments](#) and [Mobile Application Management](#) for alternatives and complements to MDM. you may also find our page on [Apple Configurator vs. MDM](#) helpful.

15 Oct 2013: Constantine Firun has created an [Excel version of the chart](#).

This page is also [downloadable as PDF](#).

Icon	Meaning
✓	Yes (has this feature)
✗	No (does not have this feature)
🕒	Coming Soon

GENERAL INFO	PRODUCT NAME	INFO LAST UPDATED	SUPPORTS IOS 7	WEB SITE
3CX Mobile Device Manager	3CX Mobile Device Manager	1 year ago		http://www.mobileden.com
4app	4app	27 weeks ago		http://www.4app.com
Absolute MANAGE	Absolute Manage	10 weeks ago	✓	http://www.absolute.com
airwatch	AirWatch	5 weeks ago	✓	http://www.airwatch.com

Questions?