Managing Apple Devices

Session 702
Todd Fernandez
Senior Manager, Device Management
“Why can’t it be as easy as opening the box and handing the iPad to the user?”
“Why can’t it be as easy as opening the box and handing the iPad to the user?”

“Apple turned the dream into reality.”

“600 iPads, 2.5 hours.”

“With the Device Enrollment Program, the process was effortless.”

A Fresh Start, Immaculata-La Salle High School, Miami, Florida

http://www.youtube.com/watch?v=H4WqTJzZGh4
New restrictions

New MDM commands
IKEv2 VPN
New Settings UI for MDM, profiles, and certs
Managed Books
Managed Domains
Managed Distribution
Activation Lock bypass codes
Content Filter Plug-ins
Enroll
Enroll

Device Enrollment Program (DEP)
Apple Configurator
Activation Lock
What’s New in iOS 8 and OS X Yosemite
Device Enrollment Program

DEP  ->  MDM
Device Enrollment Program

Easy
Device Enrollment Program

Administrators provide enrollment settings to DEP
Device Enrollment Program

Administrators provide enrollment settings to DEP
End users complete enrollment in Setup Assistant
Device Enrollment Program

Administrators provide enrollment settings to DEP
End users complete enrollment in Setup Assistant
Available for US direct sales
Device Enrollment Program

Administrators provide enrollment settings to DEP
End users complete enrollment in Setup Assistant
Available for US direct sales
…and now in Canada
Device Enrollment Program
What’s new since launch

Available now

Orders within last three years now eligible
Set default MDM server for automatic device assignment
See who assigned devices to servers
Device Enrollment Program

What’s new since launch

Available now

Orders within last three years now eligible
Set default MDM server for automatic device assignment
See who assigned devices to servers

Coming Soon

Service replacement devices remain in DEP
- Including last three years of service events
Apple

Device Enrollment Program
Device Enrollment Program

Apple

MDM Server
Device Enrollment Program

1. Apple

2. MDM Server

3. Unboxed iPads and Macs

4. Device Enrollment Program

5. MDM Server
MDM Server → Unboxed iPads and Macs
Device Enrollment Program

Topics

Where is the truth?
Disowning devices
Supervised vs. removable
Device Enrollment Program

Where does the truth lie?

DEP for devices in the program
MDM server for device profiles
Device gets new profile only at activation
Device Enrollment Program

Disowning devices
Device Enrollment Program
Disowning devices

Here Be Dragons
Are you really, really, really, really, really, really sure you want to disown the device "Cart iPad 10"?
Device Enrollment Program

Disowning devices

Rule #1—Don’t implement this feature
Rule #1—Don’t implement this feature
Rule #2—If you break Rule #1, strongly warn the user

Are you really, really, really, really, really, really, really sure you want to disown the device “Cart iPad 10”?

[Cancel]  [OK]
Rule #1—Don’t implement this feature
Rule #2—If you break Rule #1, strongly warn the user
Rule #3—There is no way to undo this action
# Device Enrollment Program

## Supervised vs. removable

<table>
<thead>
<tr>
<th>Supervised</th>
<th>Removable</th>
<th>Not Removable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>?</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Install enrollment settings over USB

Enrollment looks the same to MDM server as using DEP

• Requests to server are indistinguishable
• Server can distinguish if device is not in DEP
• Configurator will not install enrollment settings on devices with DEP profile
• Cannot be made non-removable

✅ Allow administrators to control whether this is allowed
Activation Lock

Management

Activation Lock cannot be enabled on supervised devices by default
Request and delete bypass code after enrollment
Allow Activation Lock if desired
Provide access to the bypass code in the UI
• Can be used for manual entry on devices unreachable via MDM
Activation Lock

Bypass codes

Retrieve bypass code using `ActivationLockBypassCode`
Delete bypass code from device using `ClearActivationLockBypassCode`
Allow Activation Lock using `ActivationLockAllowedWhileSupervised`

- Always retrieve and clear bypass code
  - Available for 15 days after supervision

- Save bypass code when device is removed from MDM
  - Activation Lock may still be enabled
  - Device can reenroll
What’s New in iOS 8 and OS X Yosemite

Device returns NotNow while in Setup Assistant

• InviteToProgram
• InstallApplication
• InstallMedia
• ApplyRedemptionCode
• DeviceLock
• RequestMirroring
Demo
Enrolling Devices

Jussi-Pekka Mantere
Mark Whittemore
Enroll Demo Recap

Enroll and supervise iOS device using DEP
Configure DEP settings
Retrieve Activation Lock bypass code from iOS device
Allow Activation Lock to be enabled on a supervised iOS device
Distribute

Volume Purchase Program (VPP)
Managed Apps
What’s New in iOS 8
What’s New in OS X Yosemite
Volume Purchase Program
Managed Distribution
Volume Purchase Program

Managed Distribution

Buy licenses instead of codes
Volume Purchase Program
Managed Distribution
Buy licenses instead of codes
Apps
Volume Purchase Program
Managed Distribution

Buy licenses instead of codes
Apps
Books
Volume Purchase Program

Managed Distribution

Buy licenses instead of codes
Apps
Books
APIs for MDM integration
Volume Purchase Program

Managed Distribution

Buy licenses instead of codes

Apps

Books

APIs for MDM integration

Available in 10 countries
Volume Purchase Program

Topics

Where is the truth?
Account management
Invitations
User IDs
App metadata
Volume Purchase Program
Where does the truth lie?

VPP for
• User enrollment status
• Purchased licenses
• Irrevocable book assignments
MDM server for everything else
• Revocable app assignments
Volume Purchase Program

Account management—Initial configuration

Check clientContext attribute from VPPClientConfigSrv request if empty

- Claim account by setting to JSON string
  
  ```json
  {"hostname":<my.servername.com>, "guid":<random_uuid>}
  ```

  If does not match guid of your server

- Report hostname from clientContext

- Ask administrator to confirm that your server should take over
Volume Purchase Program

Account management—Every session

Check clientContext to ensure it still refers to your MDM server
If clientContext no longer refers to your server guid
• Do not make any further requests to VPP for that account
• Report the hostname of the server to an administrator
Volume Purchase Program

Invitations

Invite via MDM
Use email as a fallback for users without enrolled devices

https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/associateVPPUserWithITSAccount?cc=us&inviteCode=ad9dd59ecf3a45fdaf005602be76ed09&mt=8

Create custom URL to MDM server, then redirect to VPP URL
Integrate invitation into your user portal
Volume Purchase Program

User IDs

MDM User Account

VPP User Account

End User’s Apple ID

clientUserIdStr

userId

itsIdHash

John Appleseed

John Appleseed

John Appleseed
Volume Purchase Program

User IDs—Ideal world

Each user has one Apple ID associated with VPP
That Apple ID never changes
One-to-one mapping between all three user representations
Volume Purchase Program

User IDs—Real world

Multiple VPP users can be associated with the same Apple ID
Users can disassociate and associate with a new Apple ID
Any of these users may have irrevocable books assigned
Volume Purchase Program

User IDs—clientUserIdStr

Pick a value that will never change

☑ Directory's GeneratedUID
☒ Email address

Find the “active” VPP entry for a user

WHERE clientUserIdStr = guid AND status IN ('Registered', 'Associated')
Volume Purchase Program

User IDs—itsIdHash

Track itsIdHash once a user is “Associated”

MDM query for this value

May also want to track “Retired” itsIdHash values

• Primarily useful for tracking irrevocable book assignments
Volume Purchase Program

App metadata

countryCode now added to response from VPPClientConfigSrv

Get app metadata using public iTunes API in non-US iTunes stores

Managed Apps

Managed apps

App Store and enterprise apps
Install using `InstallApplication` with management flag set
- Cannot retroactively manage app
Server can detect if app not managed
Work with Managed Open In to prevent data leakage
What’s New in iOS 8

Managed books
What’s New in iOS 8
Managed books
Managed Books

Features—iBooks Store books

Can manage iBooks Store book and tell device to download it
- Book must be purchased via VPP whether user purchased or not
- Can manage book even if already installed
  - Useful to ensure book is installed
Managed Books

Features—Enterprise books

Can install and remove enterprise books (PDF, ePub, iBooks Author)

• Stored with Class C data protection

Restrictions

• iCloud backups

• Highlights and notes sync
Managed Books

Commands

InstallMedia
- iTunesStoreID
- MediaURL
  - PersistentID – com.example.manuals.training
  - Kind – pdf, epub, ibooks

RemoveMedia
Managed Books

Limitations

Requires App Installation right
iBooks Store books require VPP and App Store enabled
List of installed books shows only managed books
Enterprise books can’t be synced using iTunes
What’s New in OS X Yosemite

Installation of non-App Store signed flat .pkg containing app
Profile Manager also supports installing .app bundles
Demo
Installing Enterprise Apps and Books
Distribute Demo Recap

Install enterprise book on device running iOS 8
Remove enterprise book from iOS device
Install enterprise app on iOS device
Install enterprise app on Mac running OS X Yosemite
Manage

Activation Lock
Integration with external data sources
MDMServiceConfig
What’s new in iOS 8
What’s new in OS X Yosemite
Activation Lock
Schrödinger’s iPad

Check IsActivationLockEnabled key from DeviceInformation query

Clear Activation Lock via https://deviceservices-external.apple.com/deviceservicesworkers/escrowKeyUnlock request

Device will continue to report IsActivationLockEnabled = true

Even after clearing Activation Lock, device's owner can reenable it

Same bypass code can be used again to clear Activation Lock
Integration with External Data Sources

Directory Services

Active Directory, LDAP, OpenDirectory, etc.

Some database packages don’t support external data references

Compared to database DS have severely limited capabilities

- Don’t support full enumeration of contents
- No easy way to discover changes
- Slow
- Intermittently available
Integration with External Data Sources
DEP and VPP

Easy to fully enumerate
Provide changes
Simple and efficient to mirror data they hold in your database

✔ Mirror into your database
✘ Do not use these services for live access
Integration with Directory Services

Mirroring DS data

- Performance
- Reliability
- Relational integrity

- Leave authentication in DS
- Mirror only records with MDM-related data associated
MDMServiceConfig

Equivalent to Storebag from iTunes Store
Informs tools what info they can obtain from your server
Unauthenticated HTTPS request at URI MDMServiceConfig
UTF8 JSON-encoded hash

- dep_enrollment_url
- dep_anchor_certs_url
- trust_profile_url
What’s New in iOS 8
MDM commands and queries

- Set device name
- Clear restrictions passcode
  - Install media
  - Remove media

Date of last iCloud backup
Which iTunes account is configured (itsIdHash)
What’s New in iOS 8

Configuration profile payloads

- VPN—IKEv2 connection type and Always On
- Content Filter—Plug-in type
  - Managed Domains
  - Email, Exchange—Per-message S/MIME switch
  - Single Sign On—Certificate
  - Wi-Fi—One time password
- Restrictions
What’s New in iOS 8

Configuration profile restrictions

- Allow Handoff
- Allow Internet results in Spotlight
- Allow iCloud sync for managed apps
- Allow backup of enterprise books
- Allow notes and highlights sync for enterprise books

- Allow Erase All Content and Settings
- Allow configuring restrictions
What’s New in iOS 8
End user experience of profiles and MDM

New UI for profile installation and management
MDM relationship represented with one item
• Hides all profiles installed via MDM
• Shows all settings installed via profile, apps, and books in one place
  - Accounts, apps, books, restrictions shown at top
• Users can no longer remove individual profiles installed via MDM
Restrictions UI indicates features disabled by profiles
See all certificate details
Provisioning profiles handled automatically
What’s New in OS X Yosemite

- VPN—IKEv2 connection type and Always On
- Content Filter—Plug-in type
  
- Managed Domains
  
  MDM command to begin mirroring to AirPlay destination
  
  MDM query which iTunes account is configured (itsIdHash)
Demo
Managing Device Duty Cycle
Manage Demo Recap

Easier to understand end user UI in Settings in iOS 8
How Managed Domains help prevent data leakage
Using an Activation Lock bypass code to erase a device
Completing a duty cycle using DEP
Summary

Use DEP (wireless) or Configurator (wired) to enroll devices in MDM
Use VPP and Managed Apps and Books to distribute content

Support DEP, VPP, and Activation Lock management
Support new features in iOS 8 and OS X Yosemite
Reinvent your enterprise with iOS.

iOS 8 is more advanced than ever for every line of business. Get the latest content from WWDC14 geared to IT and enterprise developers. Learn about key technologies in iOS including how to deploy devices, secure corporate data, and build breakthrough custom apps.
More Information

Developers

Paul Danbold
Core OS Technologies Evangelist
danbold@apple.com

Documentation
Apple MDM Protocol

Configuration Profile Reference
https://developer.apple.com/library/ios/#featuredarticles/iPhoneConfigurationProfileRef

Apple Developer Forums
MDM Developer Forum
http://devforums.apple.com/community/ios/mdmdev
More Information

Administrators

Documentation
Device Enrollment Program Guide

Apple Configurator Help
http://help.apple.com/configurator/mac/1.5

Apple Discussion Boards
iPad in Business and Education
http://discussions.apple.com/community/ipad/ipad_in_business_and_education

iPhone in Business and Education
http://discussions.apple.com/community/iphone/iphone_in_business_and_education
## Related Sessions

<table>
<thead>
<tr>
<th>Session</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Apps for Enterprise and Education</td>
<td>Pacific Heights</td>
<td>Tuesday 10:15AM</td>
</tr>
<tr>
<td>Distributing Enterprise Apps</td>
<td>Pacific Heights</td>
<td>Tuesday 11:30AM</td>
</tr>
<tr>
<td>Apps for Enterprise Get Together</td>
<td>Broadway</td>
<td>Tuesday 4:30PM</td>
</tr>
<tr>
<td>User Privacy in iOS and OS X</td>
<td>Nob Hill</td>
<td>Thursday 2:00PM</td>
</tr>
</tbody>
</table>
Labs

<table>
<thead>
<tr>
<th>Topic</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing Apps for Enterprise and Education</td>
<td>Core OS Lab A</td>
<td>Wednesday 2:00PM</td>
</tr>
<tr>
<td>Managing Apple Devices</td>
<td>Core OS Lab B</td>
<td>Thursday 9:00AM</td>
</tr>
<tr>
<td>Security and Privacy</td>
<td>Core OS Lab B</td>
<td>Thursday 3:15PM</td>
</tr>
</tbody>
</table>