What’s New in Apple Device Management

Session 303

Todd Fernandez Senior Manager, Device Management & Server
Evaluate

Tools
Spring 2016
Jane Appleseed

ID Number
1847664

Role / Location
Student at Township Schools

Grade Level
1

Email Address
jappleseed2@townshipschools.org
“Apple School Manager will save our tech staff lots of time—we can manage devices, content, and our student accounts all from one place.”

Patrick Scanlan
Supervisor of Technology & Information Services
San Jose Unified School District
Getting Ready
“Shared iPad will allow our district to transform a cart of shared devices into a personalized learning experience for each student.”

Eric Culpepper
Technology Support Specialist
Goose Creek CISD
“Classroom has been an extremely useful tool throughout the school day ... to enhance the Project Based Learning that is going on in my classroom. Classroom helps me to keep all my students accountable for their work, while also keeping them extremely engaged in their assignments.”

Ryan Garcia-Ganan
Fourth Grade Teacher
San Jose Unified School District
Getting Started

Distribution

Management

Tools
Getting Started
Getting Started

Apple deployment programs
Apple School Manager
Managed Apple ID
Enrollment
Shared iPad
Getting Started
Enterprise

Apple deployment programs
Device Enrollment Program (DEP)
Volume Purchase Program (VPP)
Many new settings and commands
Getting Started
Apple School Manager

People
Devices
Content
Apple School Manager

People

Input

• SIS integration
• CSV upload

Managed Apple ID

• Students
• Teachers

Classes
Apple School Manager
Managed Apple ID

Admin accounts
- Tiered administration
- Roles and privileges

Student accounts
- Required for Shared iPad
- Passcode options
- Disabled services
  - Commerce, FaceTime, iMessage, iCloud Mail, …
Apple School Manager

API

Roster Service

Users
• Students
• Teachers

Classes
Apple School Manager
API: Transition

Check during syncs if token is now ASM type (API v3)
Tell DEP you support API v3 by including in header

Customers do not need to download new tokens
Apple School Manager

API: Best practices

Handle duplicate records from multiple sources (e.g., LDAP + API)

- Allow admin to configure automatic policy matching criteria
- Allow admin to manually merge records

source_system_identifier corresponds to CSV “PersonNumber”

- Field is mutable and not guaranteed to be unique!
Apple School Manager

API: Best practices

No delta API

- SIS syncing only once per day
- Don’t automatically perform “full sync” more than once per day

- Consider throttling admin-initiated syncs
Apple School Manager

Devices

Device Enrollment Program

- Find purchases
- Configure MDM servers
- Assign devices to MDM servers
Apple School Manager

Content

Volume Purchase Program
iTunes U
Getting Started

Enrollment

Enrollment optimization
Security best practices
Configure Setup Assistant
MDMServiceConfig
Shared iPad
Enrollment

Enrollment optimization
Enrollment optimization

MDM Server

Device Enrollment Program

iOS Device or Mac
Enrollment optimization

MDM Server

await_device_configured

Device Enrollment Program

DEP Settings

iOS Device or Mac
Enrollment optimization

1. MDM Server
   - await_device_configured

2. iOS Device or Mac

Device Enrollment Program
- DEP Settings
Enrollment optimization

1. MDM Server
   - `await_device_configured`

2. Device Enrollment Program
   - DEP Settings

3. iOS Device or Mac
   - `TokenUpdate (AwaitingConfiguration)`
Enrollment

Enrollment optimization

1. MDM Server
   - await_device_configured
   - Commands
   - Configuration Profiles

2. Device Enrollment Program
   - DEP Settings

3. iOS Device or Mac
   - TokenUpdate (AwaitingConfiguration)

4. Connections between MDM Server and DEP Settings

Diagram showing the process of enrollment optimization with key components and connections.
Enrollment optimization

1. MDM Server
   - await_device_configured
   - Commands
     - Configuration Profiles
   - DeviceConfigured

2. Device Enrollment Program
   - DEP Settings

3. iOS Device or Mac
   - TokenUpdate (AwaitingConfiguration)

4. DeviceConfigured

5. Exit Setup Assistant
Enrollment

Enrollment optimization: Shared iPad
Enrollment

Enrollment optimization: Shared iPad

MDM Server

Shared iPad
Enrollment

Enrollment optimization: Shared iPad

User signs in

MDM Server

Shared iPad
Enrollment optimization: Shared iPad

User signs in

1

MDM Server

2

Shared iPad

TokenUpdate
Enrollment
Enrollment optimization: Shared iPad

MDM Server
Commands
Configuration Profiles

Shared iPad
TokenUpdate

User signs in
1

2

3
Enrollment

Security best practices

iOS 9.3.2 no longer supports MD5
DES deprecated
iOS 10 adds AES support

SCEP servers need to support 3DES or AES as soon as possible
Enrollment
Configure Setup Assistant

True Tone
Enrollment
Configure Setup Assistant

Siri
iCloud Desktop
Device Enrollment Program

MDMServiceConfig

Equivalent to VPP 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
Device Enrollment Program

MDMServiceConfig

Equivalent to VPP 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`

Profile Manager has implemented
Configurator 2 now supports
Shared iPad

Support multiple users
Install apps
Preserve user data
Shared iPad

Multiple users

Requires Managed Apple ID to sign in

Signs in to iCloud and iTunes
Shared iPad

Installing apps

Device assigned

MDM vendors use PurchaseMethod 1

All app types supported

• App Store developers must allow device assignment
Shared iPad

Architecture

Student data truth in the cloud

- Data is cached, but may be purged when needed
- User data separation
- Data will continue to upload after sign out if necessary

Apps should be education ready
Goodbye, Mia
Uploading Mia’s Data
Uploading Mia’s Data
Uploading Mia’s Data
Uploading Mia’s Data
Uploading Mia’s Data
Uploading Mia's Data
Uploading Mia’s Data

Downloading Gabriel’s Data
Shared iPad
Support in MDM servers

New DEP setting to enable
Use Enrollment Optimization to set options before student use
• User quota
• Lock screen grace period
Shared iPad
User quota
Shared iPad

User quota

Maximum numbers of users cached locally
Shared iPad

User quota

Maximum numbers of users cached locally

Storage allocated to each user calculated automatically
Shared iPad

User quota

Maximum numbers of users cached locally

Storage allocated to each user calculated automatically
Shared iPad

User quota

Maximum numbers of users cached locally
Storage allocated to each user calculated automatically
After limit reached, new user purges the cache of the LRU user
Shared iPad

User quota

Maximum numbers of users cached locally
Storage allocated to each user calculated automatically
After limit reached, new user purges the cache of the LRU user
Shared iPad

User quota

Maximum numbers of users cached locally
Storage allocated to each user calculated automatically
After limit reached, new user purges the cache of the LRU user
Shared iPad
Lock screen grace period

Time after screen locks that device will prompt for user passcode
Before time limit reached, student can wake device with just a swipe
Hello, Mia

› slide to unlock

This iPad is managed by Township Schools.
Learn more.
Shared iPad

User channel

Allows MDM server to configure per-user settings

• Similar to macOS
• iOS devices running 9.3 and later don’t ignore it
• Some payloads now supported

No user authentication on iOS

• Never send sensitive information over user channel
  - User channel enforces no credentials
  - Google OAuth supported, but without credentials
Shared iPad

User channel: Supported payloads

- Accounts, including Google OAuth account
- Notifications
- Home screen layout
- Managed Domains: Safari autofill domains
- Restrictions, including Show/Hide Apps
Shared iPad

User channel: Restrictions payloads

Most restrictive wins

Combined to compute effective restrictions
• Just like multiple profiles
Demo
Shared iPad

David Steinberg
Device Management Engineer
Demo Recap

Shared iPad

Classes preconfigured on login screen

Recent users

Sign in with Managed Apple ID and passcode

Sign in choosing recent user

Apps show only current user’s data

Different users see different apps and home screen layout
Distribution

Managed Apple ID
Books for Shared iPad
Enterprise Apps
Managed Apple ID association

Programmatically associate Managed Apple IDs for VPP

Requires DEP/ASM token and VPP tokens from same organization

• Customer doesn’t need new tokens after transition to ASM

• DEP and VPP use different tokens so could be different organizations
  - Dedicated error code for this failure mode; try and fail

Requires MDM solution adopt API

Important for iBooks Store books
VPP

Books for Shared iPad

iBooks Store VPP books
• Assigned to users
• Cannot be distributed to devices
• Shared iPad user must “download” in iBooks
  - Downloaded only once per device

Non-iBooks Store books
• PDF, IBA, EPUB
• Device assigned
Enterprise Apps

UPPs

Allow non-App Store app to run on device not defined in provisioning profile

Require trust and validation

User must explicitly trust apps from that signer to run on this device

• Apps installed via MDM implicitly trusted

Apple must consider this UPP still valid

• Periodic checks via online connection to validation server

• MDM installed apps still require periodic validation

• MDM can trigger validation for any app

• Automatically validate any applications that it discovers are not validated
Management
Management

Shubham Kedia
iOS Engineer
What’s New in iOS 9.3
MDM commands and queries

- Settings now allows setting max users, diagnostic submission
- User List
- Logout user
- Delete User
- MDM Lost Mode (including device location)
- MDM Activation Lock
What’s New in iOS 9.3

Configuration profile payloads

Education
Notifications
Home Screen Layout
Lock Screen Message

Exchange, Mail: Allow Mail Drop
Managed Domains: Safari autofill passwords
VPN: Many new IKEv2 settings
Restrictions: Many new settings
What’s New in iOS 9.3

Configuration profile payloads: Restrictions

- Apple Music
- Classroom Screen View
- iCloud Photo Library
- iTunes Radio
- Modify Notifications
- Show/Hide Apps
What’s New in iOS 9.3

Configuration profile payloads: Education

Students
Teachers
Classes
Photos
  • URLs
  • Get required HTTPS
Used by Shared iPad login screen and Classroom
Only one allowed per device
Student devices and teacher devices need different payloads
What’s New in iOS 9.3

Configuration profile payloads: Per-user on Shared iPad

Five payloads can now apply per-user on Shared iPad

Accounts
  • Google OAuth account

Notifications

Home screen layout

Managed Domains: Safari autofill domains

Restrictions
  • Show/Hide Apps
What’s New in iOS 9.3.2

MDM commands and queries

- Enable/Disable App Analytics
- Set lock screen grace period

- DeviceInformation returns App Analytics enabled/disabled
- SecurityInfo returns lock screen grace period
What’s New in iOS 9.3.2

Automatic Assessment Configuration

Continues to work same way on supervised devices

New entitlement

API then disables five features while app is running:

• Auto correction, Define, keyboard shortcuts, predictive keyboard, spell check

Safe escape behavior on unmanaged devices
What's New in iOS 9.3.2

Configuration profile restrictions

Modify diagnostics submission
What’s New in iOS 10

Configuration profile payloads

Contacts, Exchange, Google, LDAP: Communication service rules for audio
Lock Screen Message: Updated key names
VPN: IKEv2 EAP only authentication method, timeout for IPSec
VPN: PPTP has been removed from iOS 10
• Existing payloads will not work
Wi-Fi: Captive bypass
Wi-Fi: Cisco fast lane QoS marking

Restrictions: Modify Bluetooth
Deprecations

Configuration profile restrictions

App installation
App removal
FaceTime
Safari
iTunes
Explicit content
iCloud documents and data
Multiplayer gaming
Add GameCenter Friends
Deprecations

Configuration profile restrictions

- App installation
- App removal
- FaceTime
- Safari
- iTunes
- Explicit content
- iCloud documents and data
- Multiplayer gaming
- Add GameCenter Friends
What’s New in OS X 10.11.4

MDM commands and queries

Install major update (DEP Macs)
What’s New in macOS Sierra

Configuration profile payloads

IP firewall

Restrictions

- Apple Music
- iCloud keychain sync
- iCloud Photo Library
- Back to my Mac
- Find My Mac
- Sharing to Notes, Reminders, or LinkedIn
Assign Shared iPad
Launch app
Navigate to location
AirPlay to Apple TV
Lock iPad
View screen
Demo
Classroom

Shruti Gupta
Device Management Engineer
Demo Recap

Classroom

Open app
Create and edit groups
Lock to app
View screen
Lock device
Tools

DEP and VPP Simulators

Simulate DEP and VPP services
Test handling of service errors

Now supports all the new DEP and VPP features

Available for download on developer portal
Support new features
Summary

Administrators

Use Apple School Manager to manage people, devices, content
Use DEP (wireless) or Configurator (wired) to enroll devices in MDM
Use Shared iPad with Managed Apple ID on shared devices
Use VPP Managed Distribution to distribute apps to devices or users
Summary

MDM developers

Support VPP Managed Apple ID association
Support new features in iOS 10 and macOS Sierra

• Documentation available now

Test with DEP and VPP simulators
Summary

App developers

Store data and preferences in cloud
Test using app with two iPads
Related Sessions

Best Practices for Building Apps Used in Business and Education

Nob Hill

Wednesday 1:40PM
<table>
<thead>
<tr>
<th>Labs</th>
<th>Graphics, Games, and Media Lab C</th>
<th>Tuesday 1:30PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education and Enterprise Deployment and Development Lab</td>
<td>Fort Mason</td>
<td>Wednesday 3:00PM</td>
</tr>
<tr>
<td>Education and Enterprise Deployment and Development Lab</td>
<td>Fort Mason</td>
<td>Thursday 11:00AM</td>
</tr>
</tbody>
</table>
Create more a-ha moments.

Something magical happens when you put Apple products in your classroom. You can create unique opportunities for personal learning at every level. Lessons become more immersive through the power of touch, motion, and sound. Assignments can be sketched, scored, charted, coded, or performed. And the work your students need to do becomes the work they love to do.
Build apps that transform how business works.

iOS makes it easy to build amazing and powerful apps for business. By leveraging the latest iOS technology, you can create even more engaging experiences for your employees and customers.
More Information

https://developer.apple.com/wwdc16/303