Core OS

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

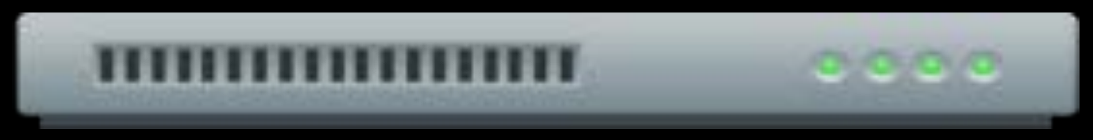
Managed Books

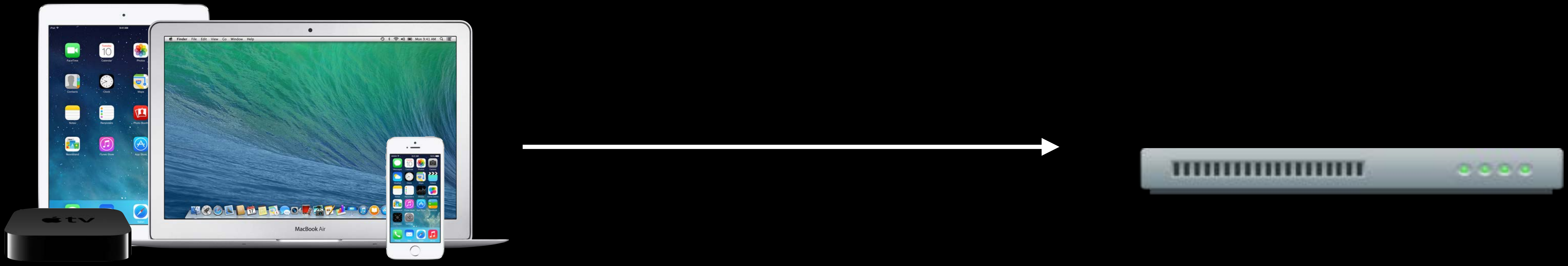
Managed Domains

Managed Distribution

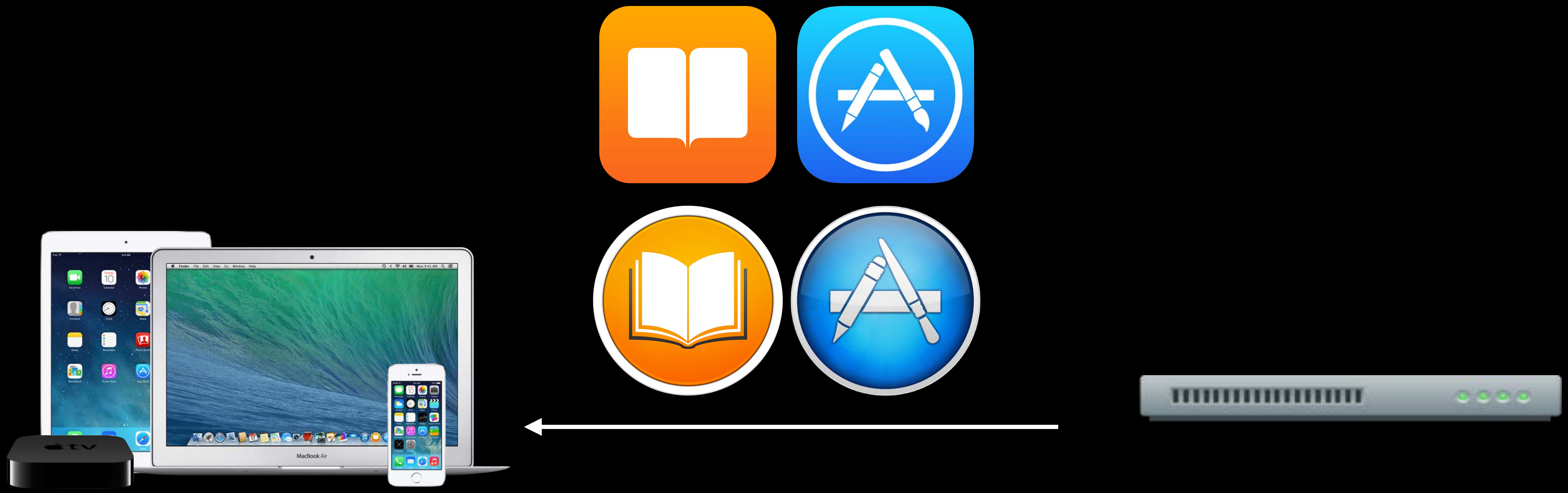
Activation Lock bypass codes

Content Filter Plug-ins



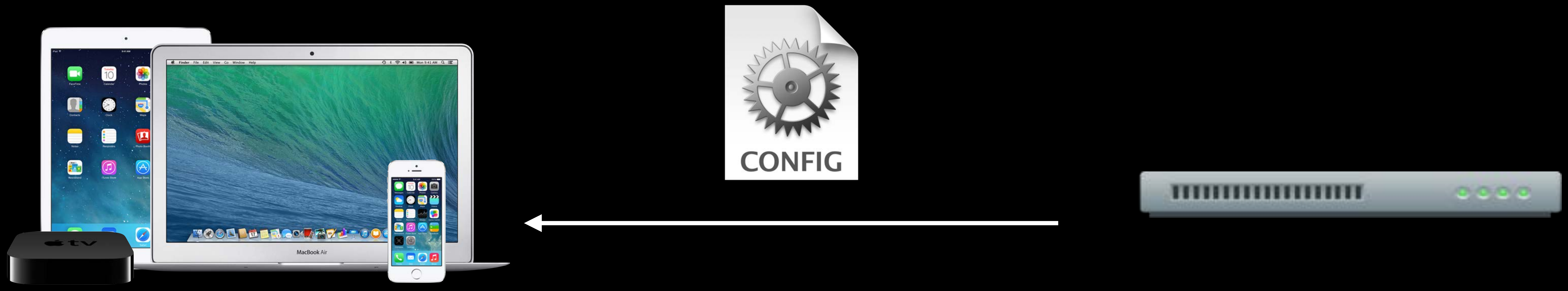


Enroll



Enroll

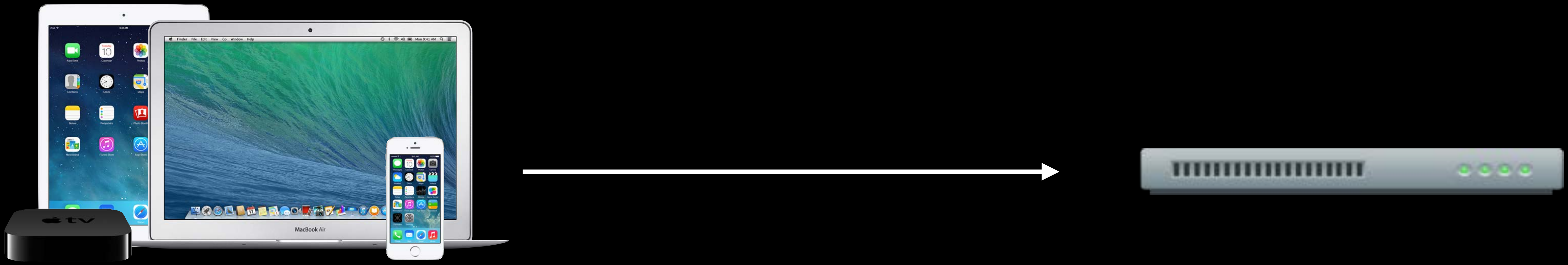
Distribute



Enroll

Distribute

Manage



Enroll

Distribute

Manage

Enroll

Device Enrollment Program (DEP)

Apple Configurator

Activation Lock

What’s New in iOS 8 and OS X Yosemite

Device Enrollment Program

DEP != MDM

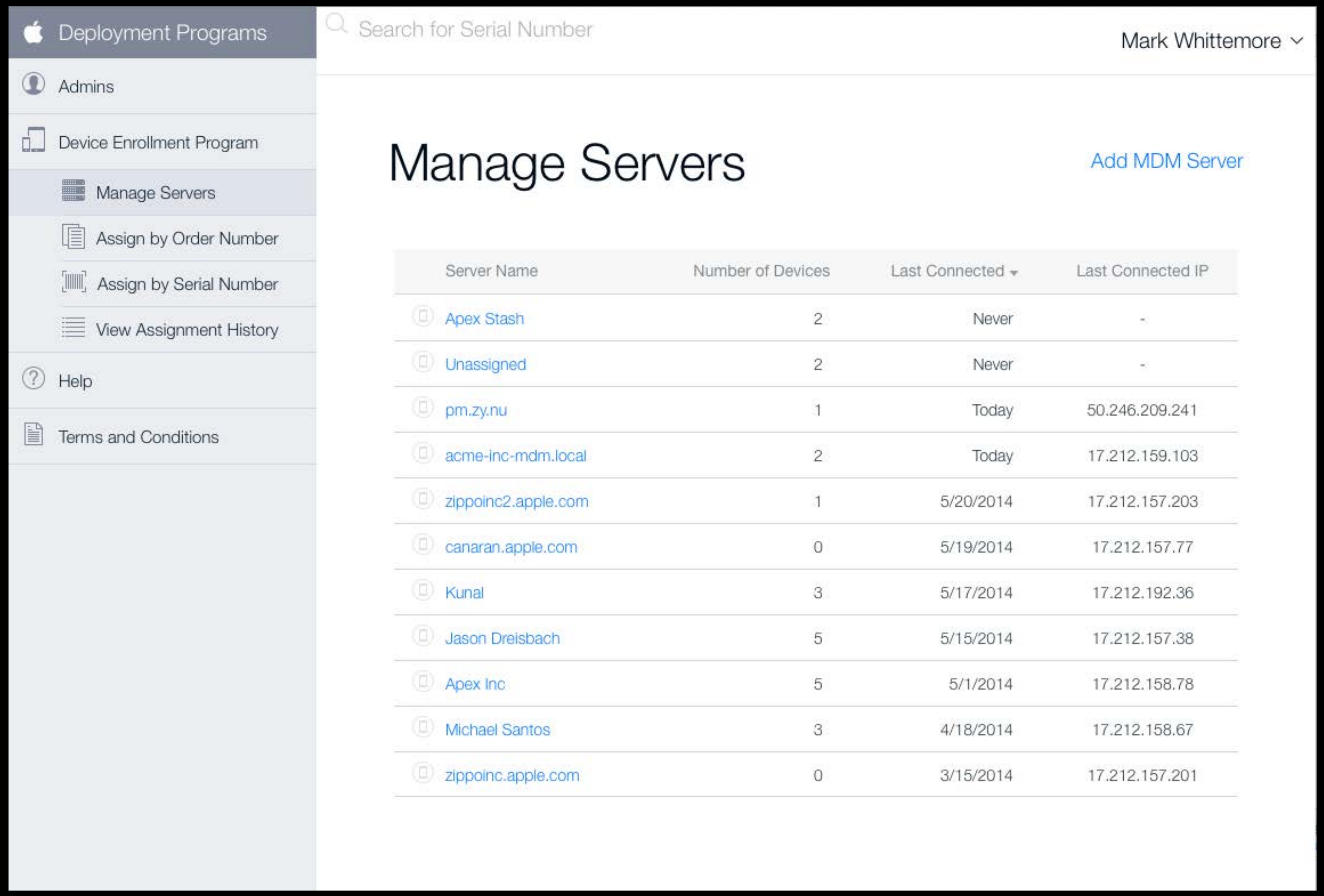
Device Enrollment Program

DEP -> MDM

Device Enrollment Program

Device Enrollment Program

Administrators provide enrollment settings to DEP



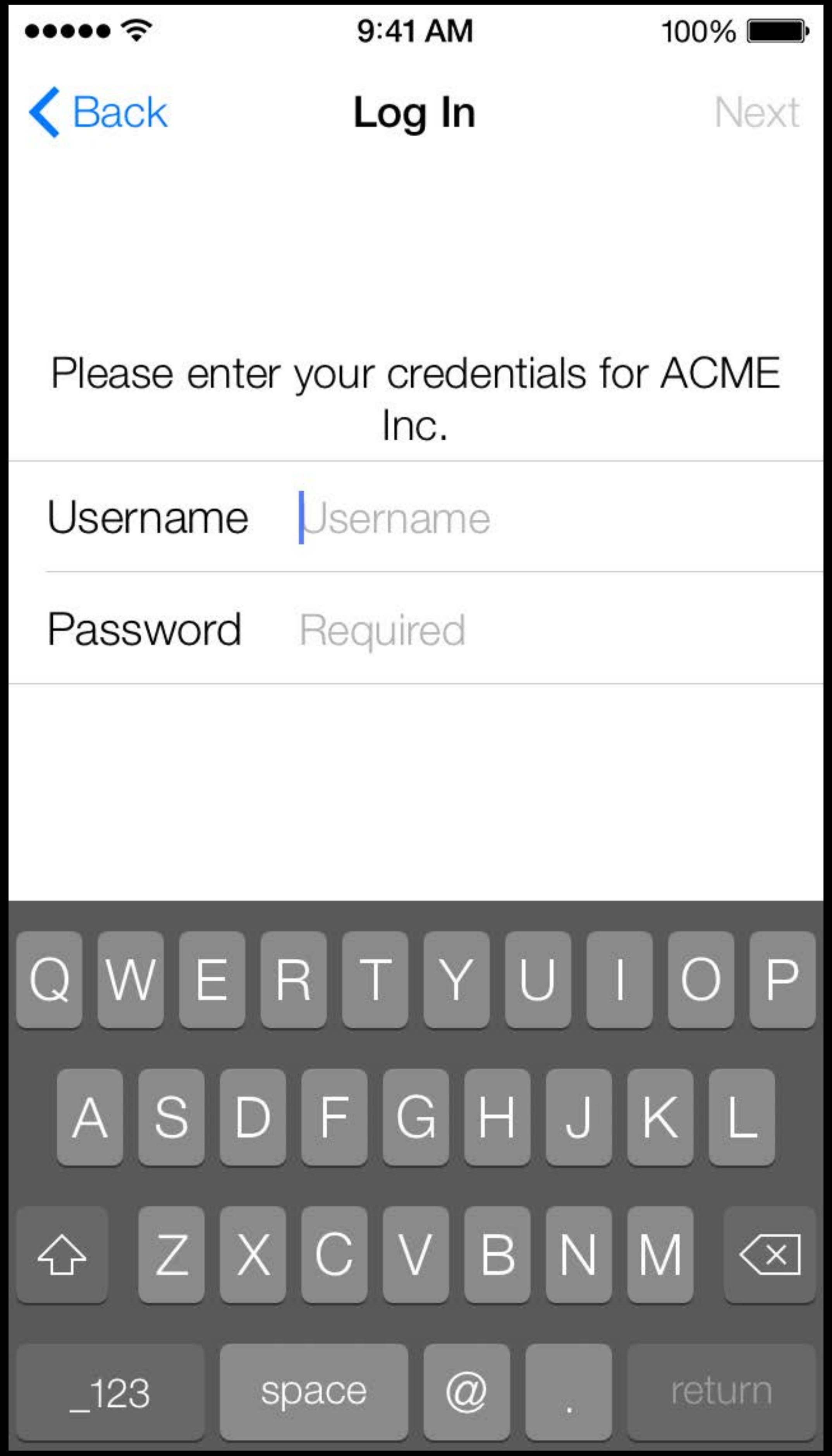
Manage Servers

Server Name	Number of Devices	Last Connected ▾	Last Connected IP
Apex Stash	2	Never	-
Unassigned	2	Never	-
pm.zy.nu	1	Today	50.246.209.241
acme-inc-mdm.local	2	Today	17.212.159.103
zippoinc2.apple.com	1	5/20/2014	17.212.157.203
canaran.apple.com	0	5/19/2014	17.212.157.77
Kunal	3	5/17/2014	17.212.192.36
Jason Dreisbach	5	5/15/2014	17.212.157.38
Apex Inc	5	5/1/2014	17.212.158.78
Michael Santos	3	4/18/2014	17.212.158.67
zippoinc.apple.com	0	3/15/2014	17.212.157.201

Device Enrollment Program

Administrators provide enrollment settings to DEP

End users complete enrollment in Setup Assistant



Please enter your credentials for ACME Inc.

Username: Username

Password: Required

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

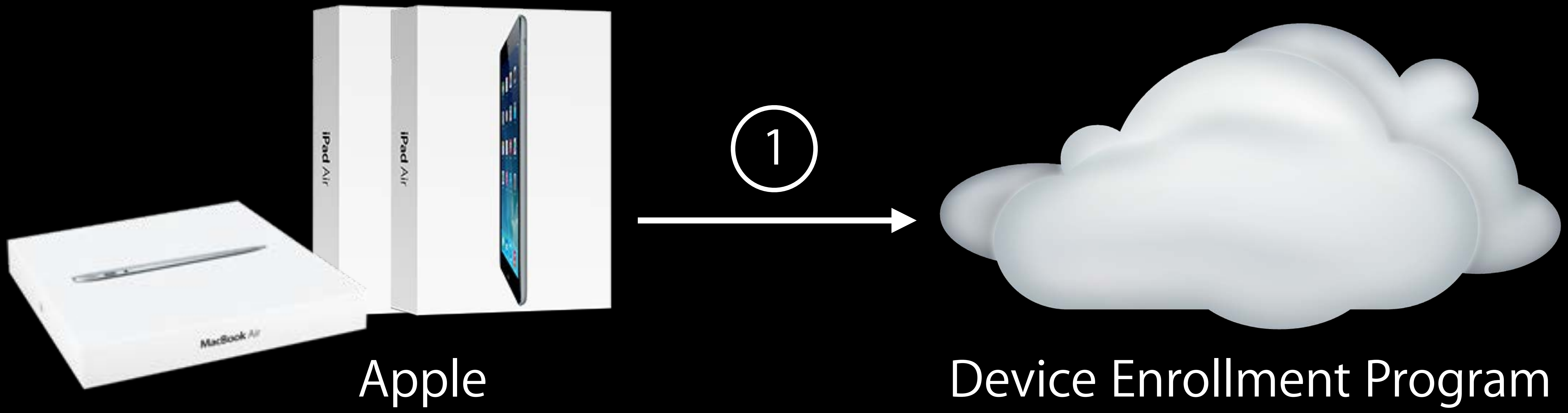
Coming Soon

Service replacement devices remain in DEP

- Including last three years of service events

Apple

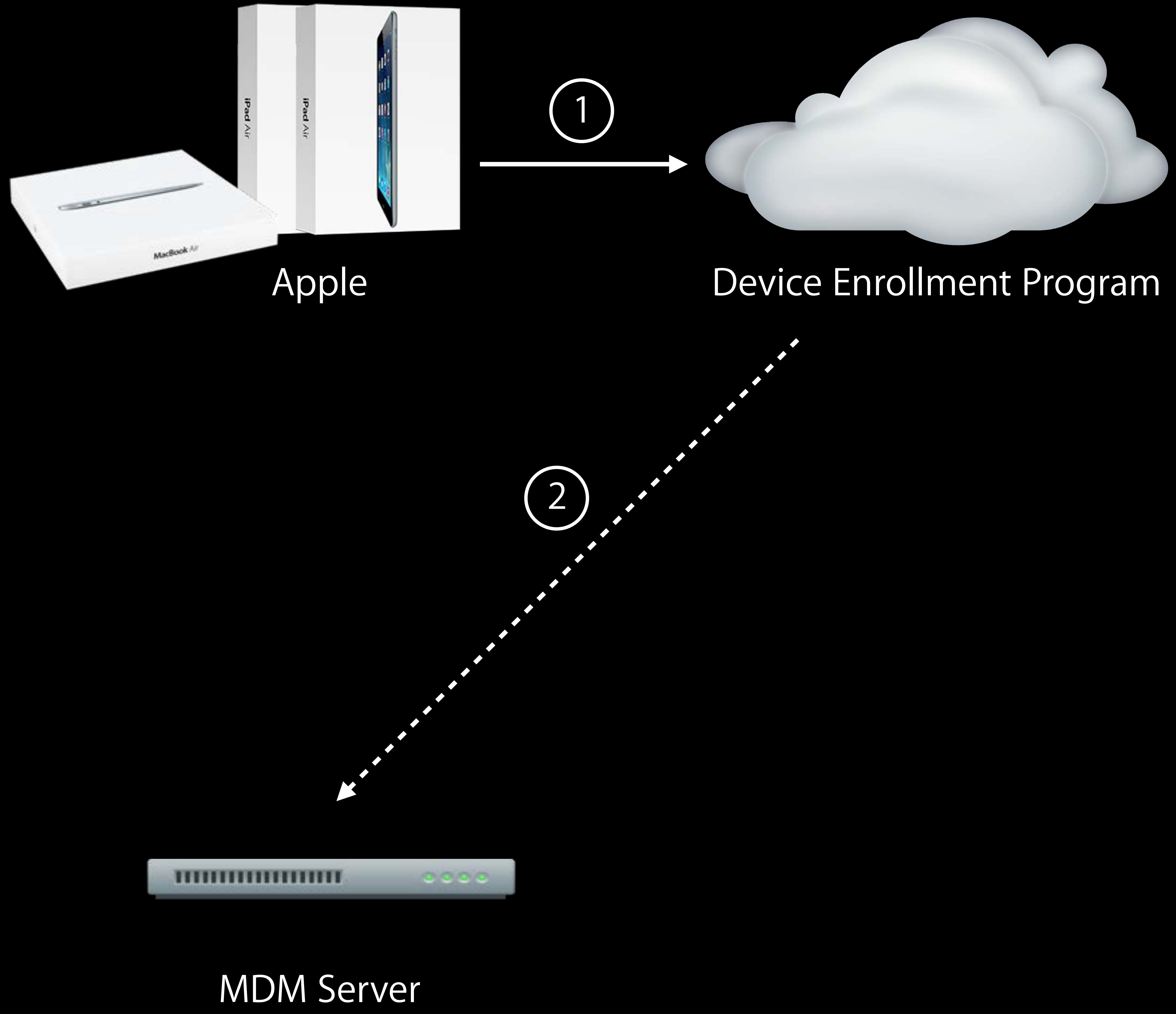
Device Enrollment Program



Apple

1

Device Enrollment Program



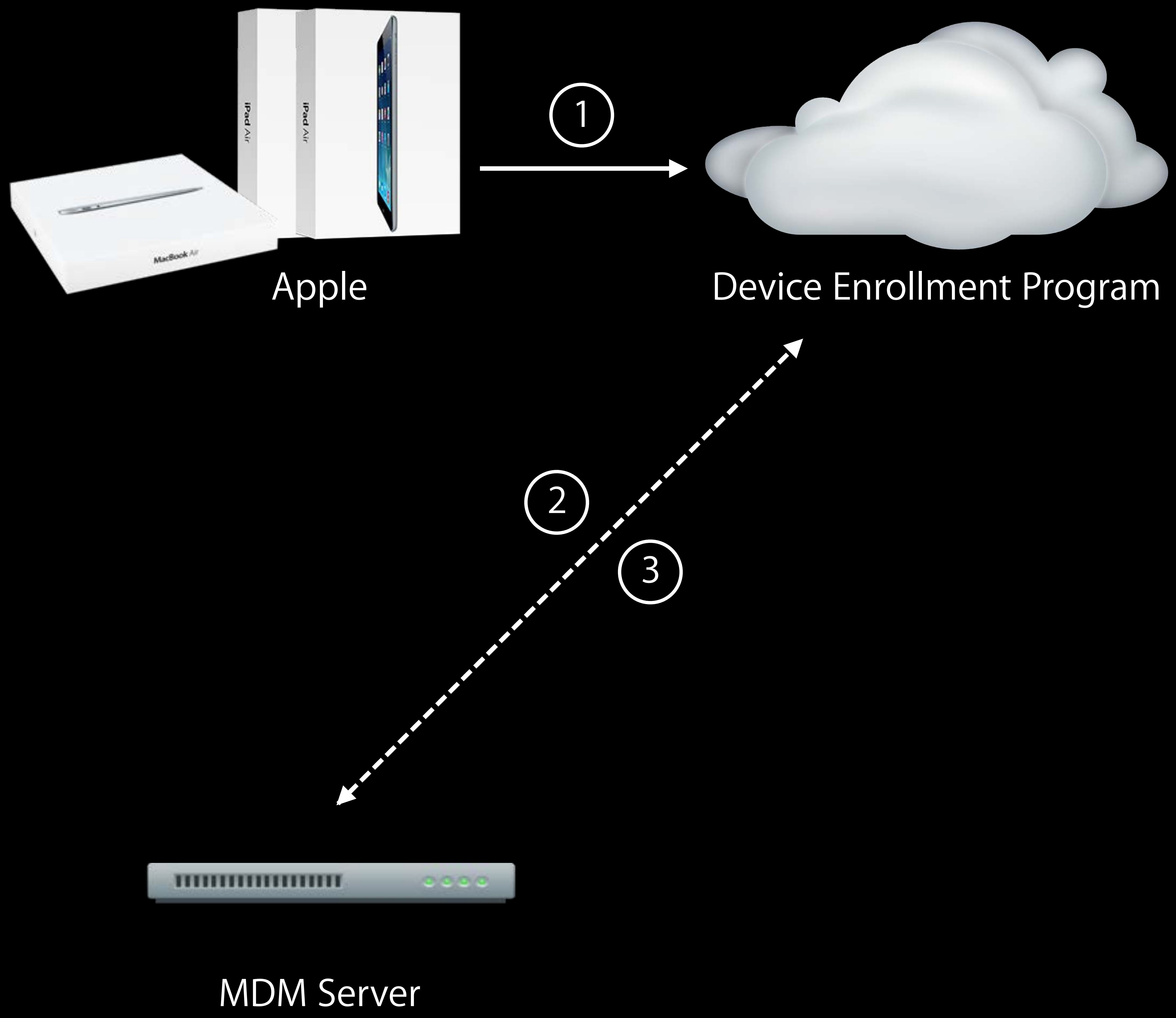
Apple

1

Device Enrollment Program

2

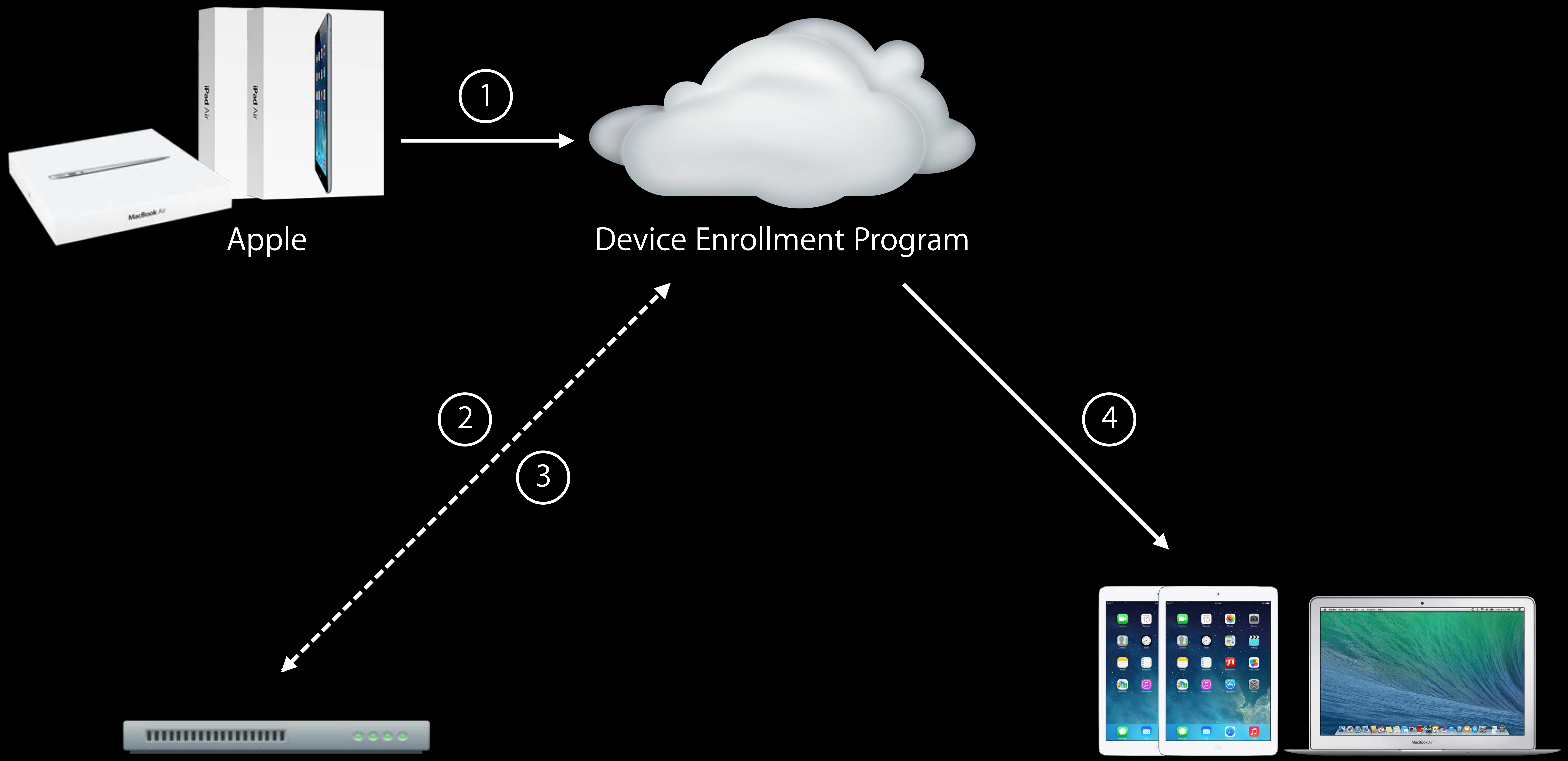
MDM Server



Apple

Device Enrollment Program

MDM Server

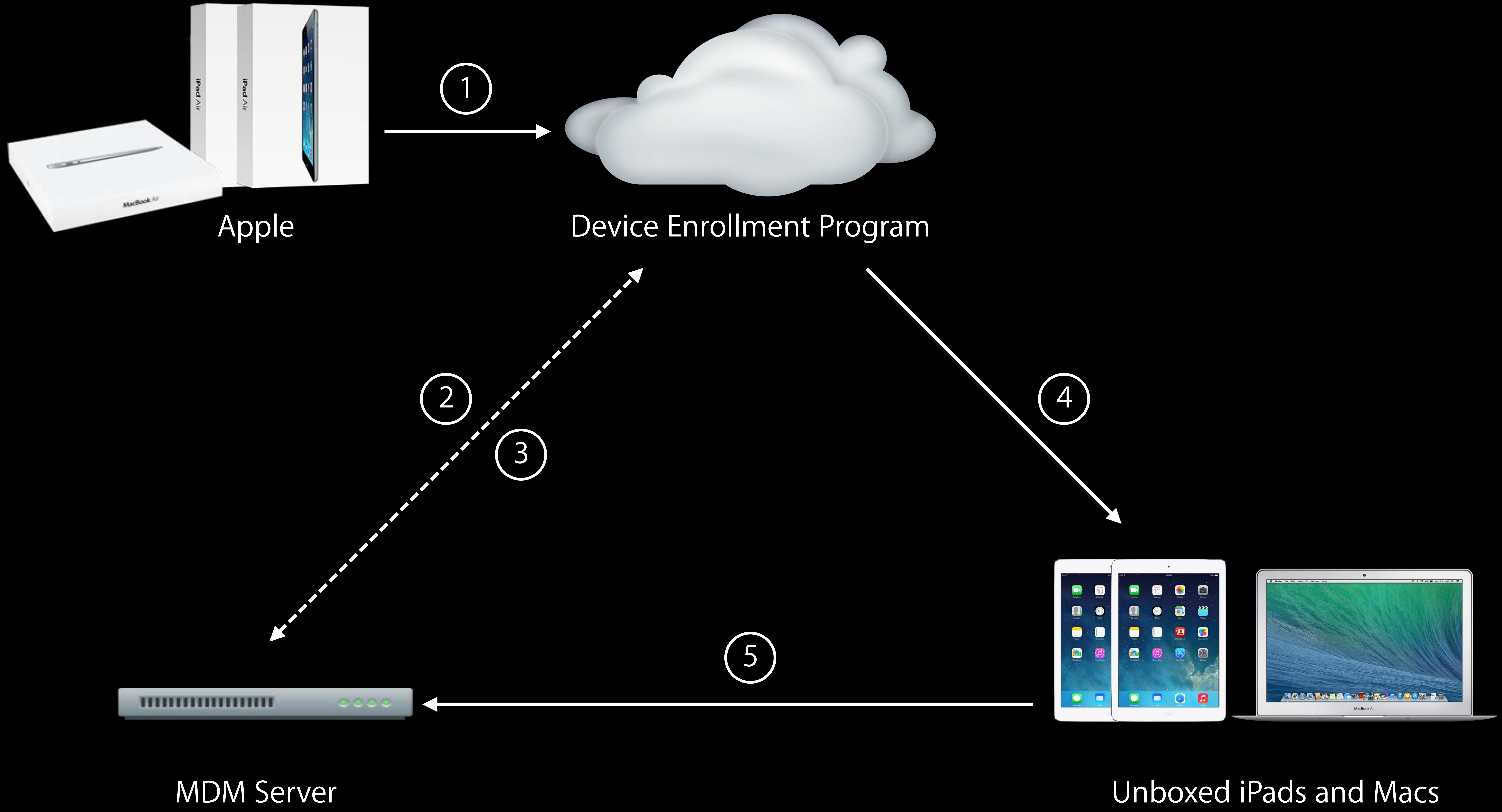


Apple

Device Enrollment Program

MDM Server

Unboxed iPads and Macs

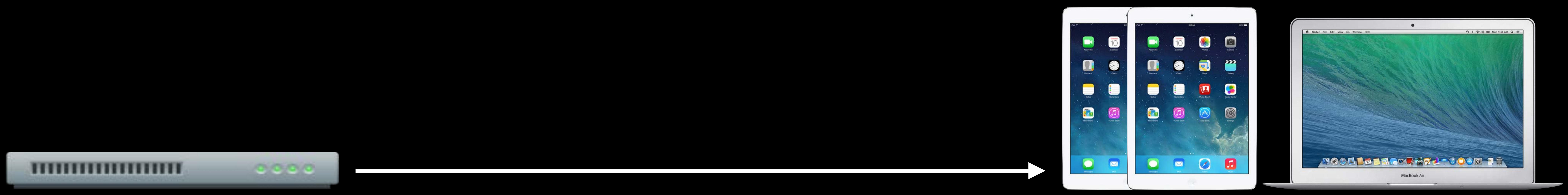


Apple

Device Enrollment Program

MDM Server

Unboxed iPads and Macs



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

Device Enrollment Program

Disowning devices ✓

Device Enrollment Program

Disowning devices

Rule #1—Don’t implement this feature

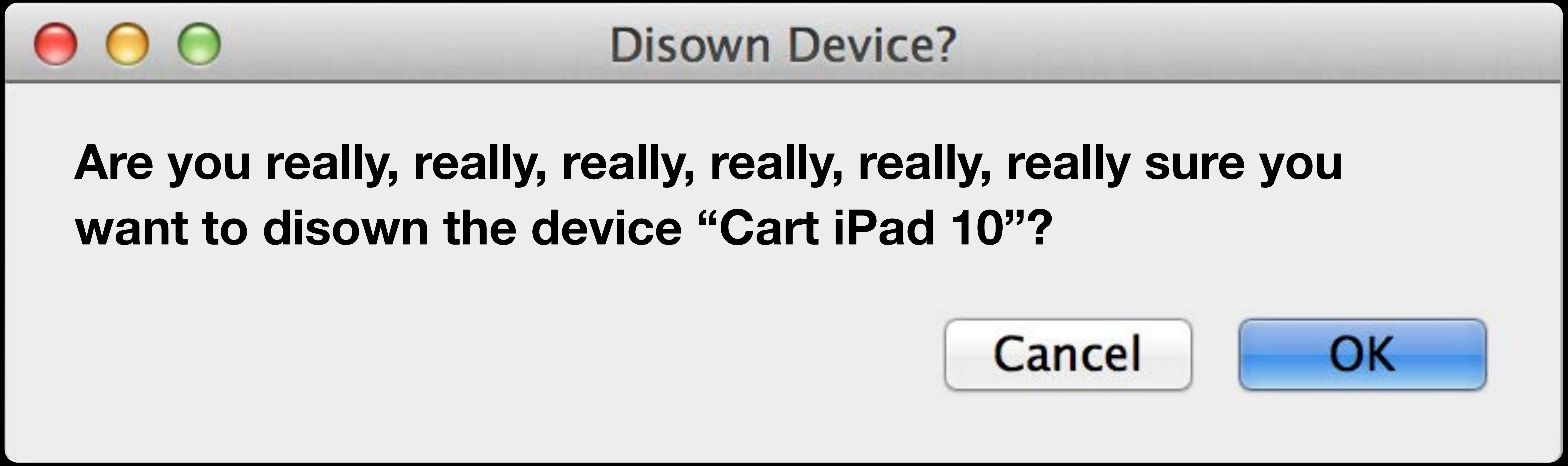
Device Enrollment Program

Disowning devices

✓

Rule #1—Don’t implement this feature

Rule #2—If you break Rule #1, strongly warn the user



Disown Device?

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

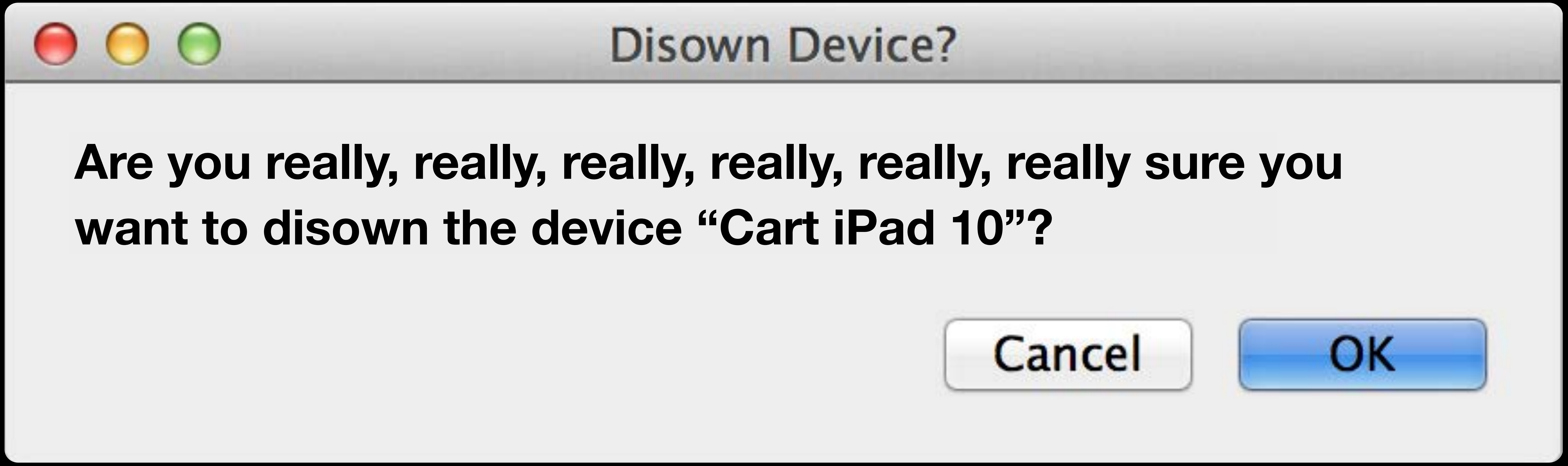
Device Enrollment Program

Disowning devices

✓

Rule #1—Don’t implement this feature

Rule #2—If you break Rule #1, strongly warn the user



Disown Device?

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

Rule #3—There is no way to undo this action

Device Enrollment Program

Supervised vs. removable

	Removable	Not Removable
Supervised	?	✓
Not Supervised	✓	✗

Apple Configurator

Enrollment

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

NEW

Device returns NotNow while in Setup Assistant

- InviteToProgram
- InstallApplication
- InstallMedia
- ApplyRedemptionCode
- DeviceLock
- RequestMirroring

Demo

Enrolling Devices

Jussi-Pekka Mantere
Mark Whittemore

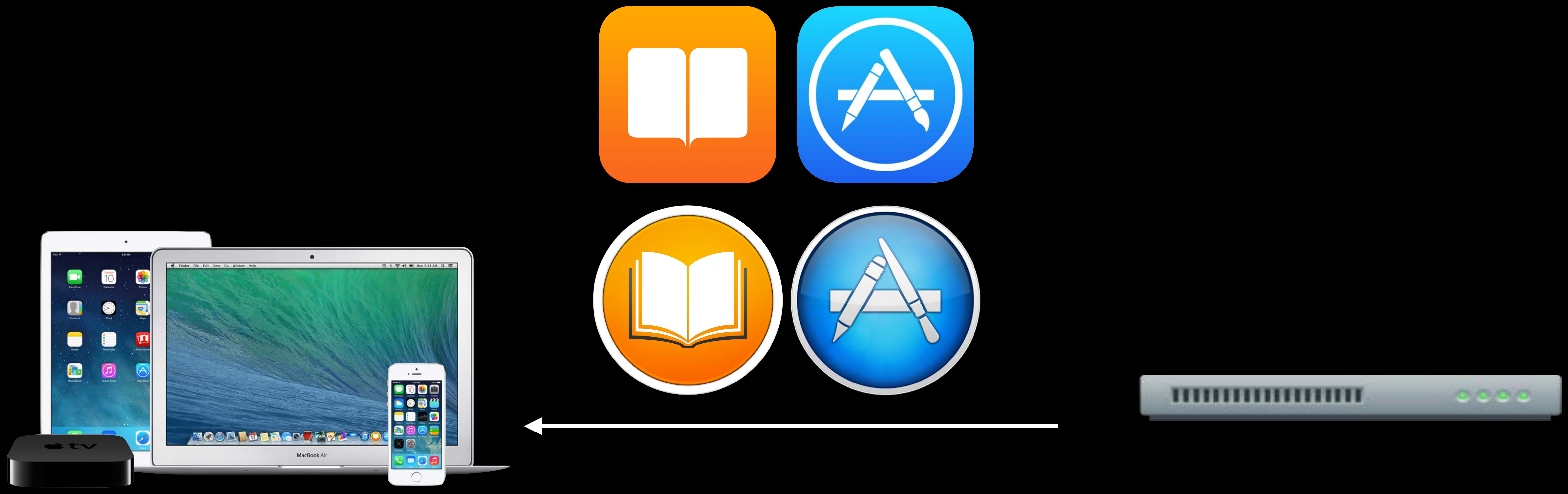
Enroll Demo Recap

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



Enroll

Distribute

Manage

Distribute

Volume Purchase Program (VPP)

Managed Apps

What’s New in iOS 8

What’s New in OS X Yosemite

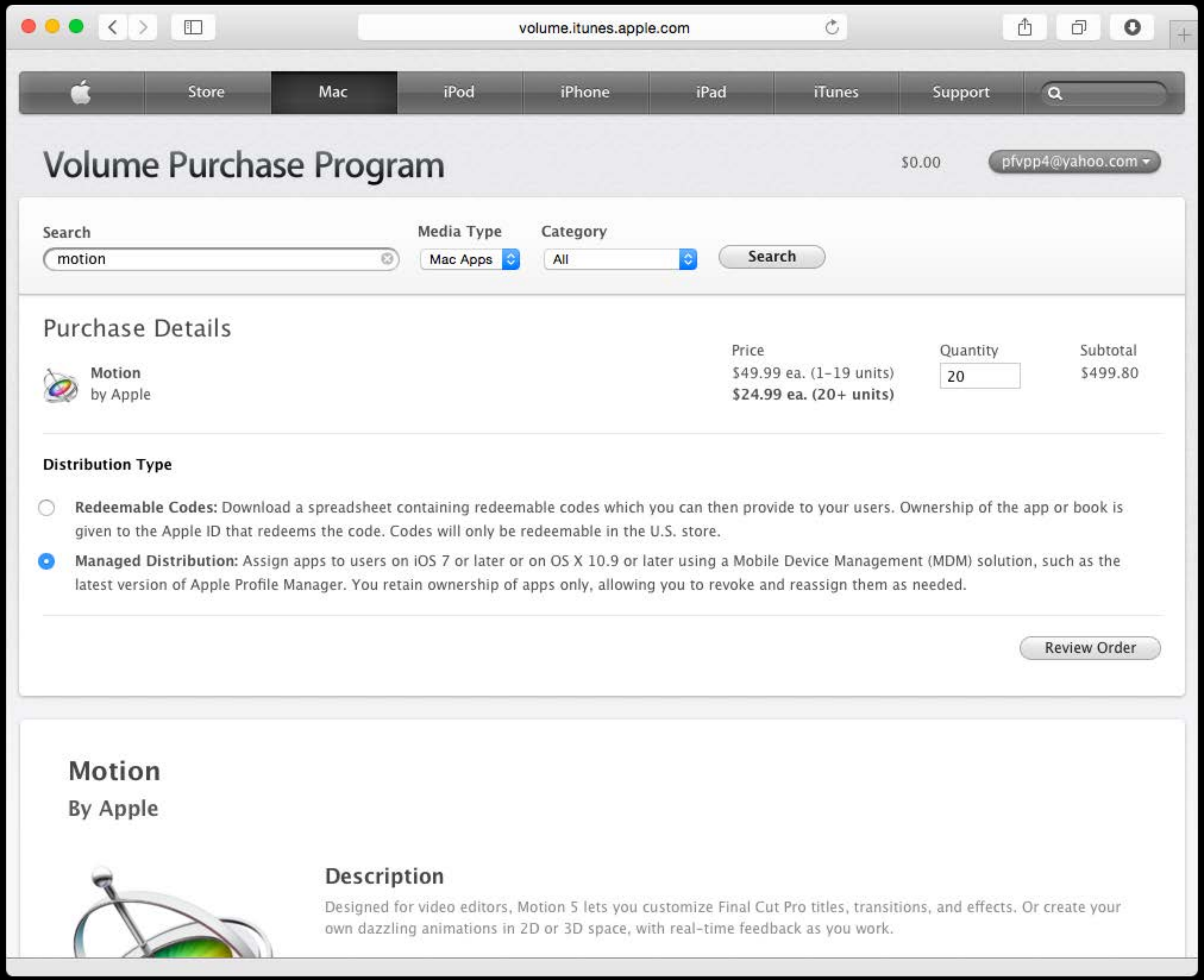
Volume Purchase Program

Managed Distribution

Volume Purchase Program

Managed Distribution

Buy licenses instead of codes



Volume Purchase Program

Search: motion

Media Type: Mac Apps

Category: All

Purchase Details

	Price	Quantity	Subtotal
Motion by Apple	$49.99 ea. (1-19 units) **$24.99 ea. (20+ units)**	20	$499.80

Distribution Type

○ **Redeemable Codes:** Download a spreadsheet containing redeemable codes which you can then provide to your users. Ownership of the app or book is given to the Apple ID that redeems the code. Codes will only be redeemable in the U.S. store.

● **Managed Distribution:** Assign apps to users on iOS 7 or later or on OS X 10.9 or later using a Mobile Device Management (MDM) solution, such as the latest version of Apple Profile Manager. You retain ownership of apps only, allowing you to revoke and reassign them as needed.

Motion

By Apple

Description

Designed for video editors, Motion 5 lets you customize Final Cut Pro titles, transitions, and effects. Or create your own dazzling animations in 2D or 3D space, with real-time feedback as you work.

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

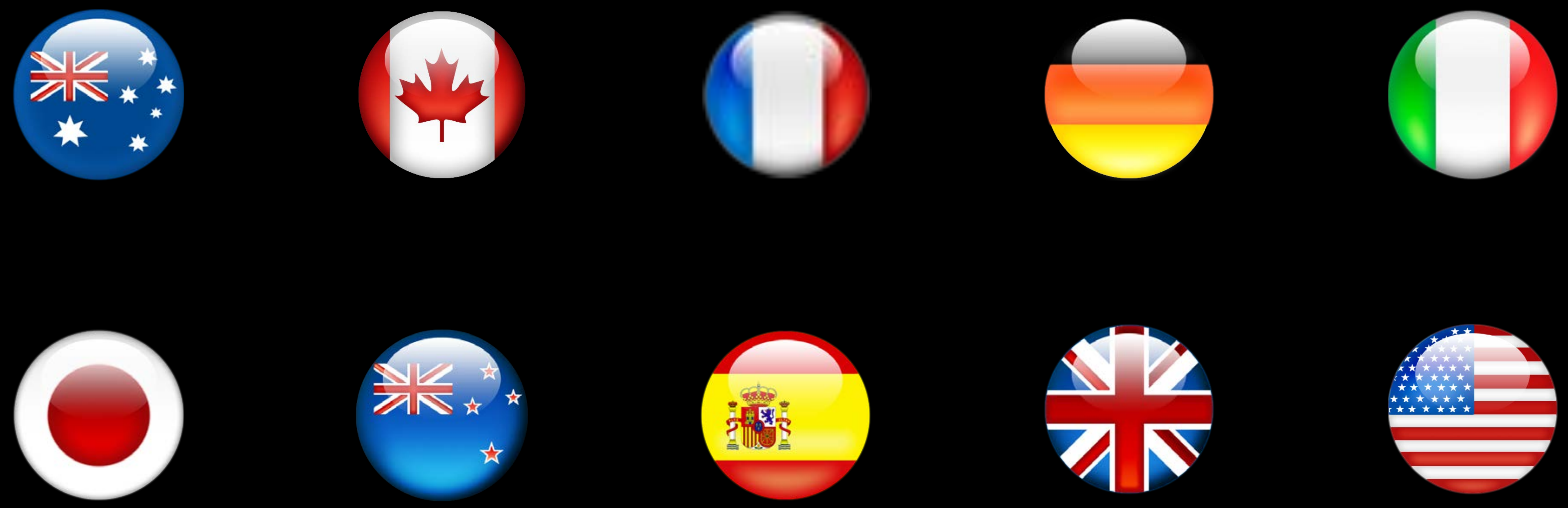
Buy licenses instead of codes

Apps

Books

APIs for MDM integration

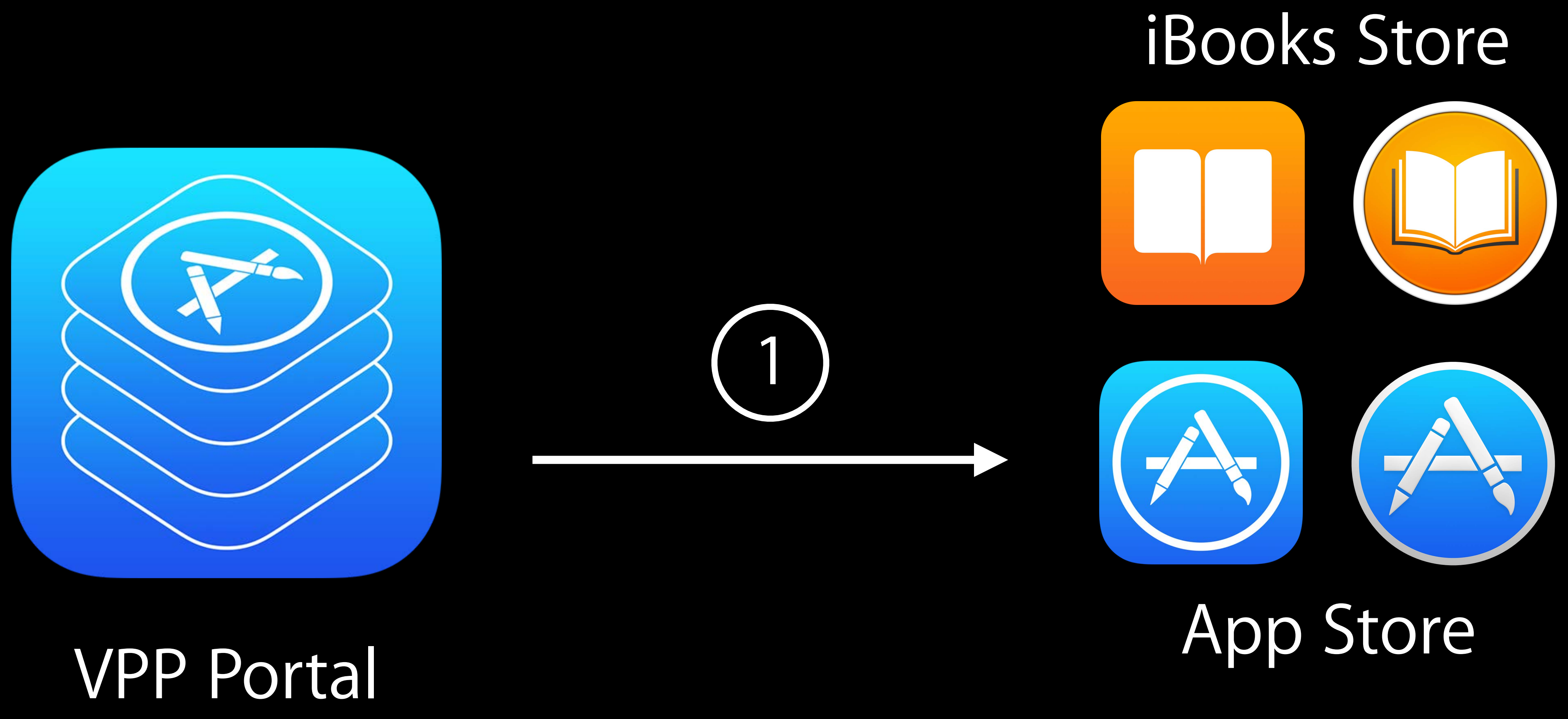
Available in 10 countries



iBooks Store

VPP Portal

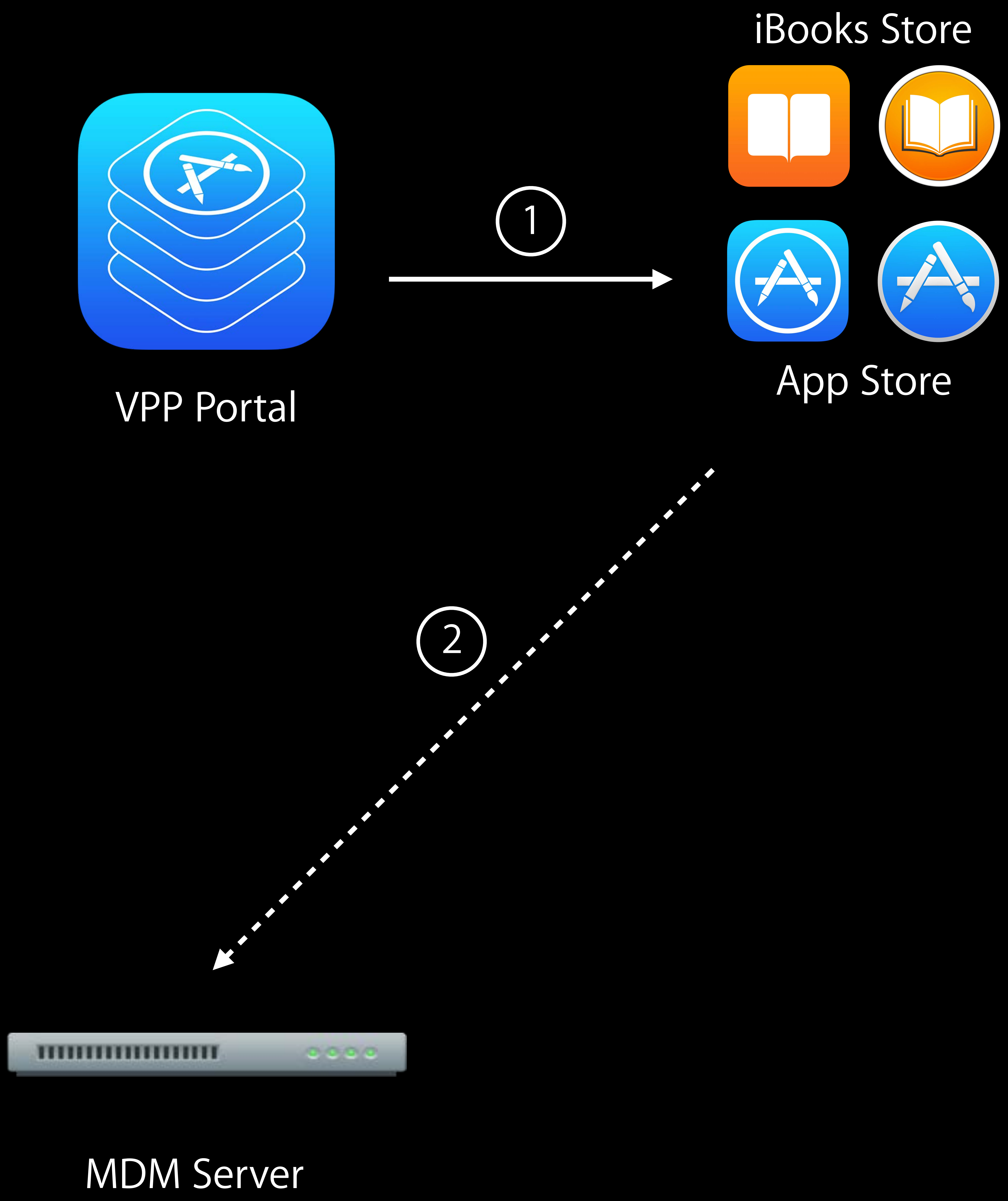
App Store

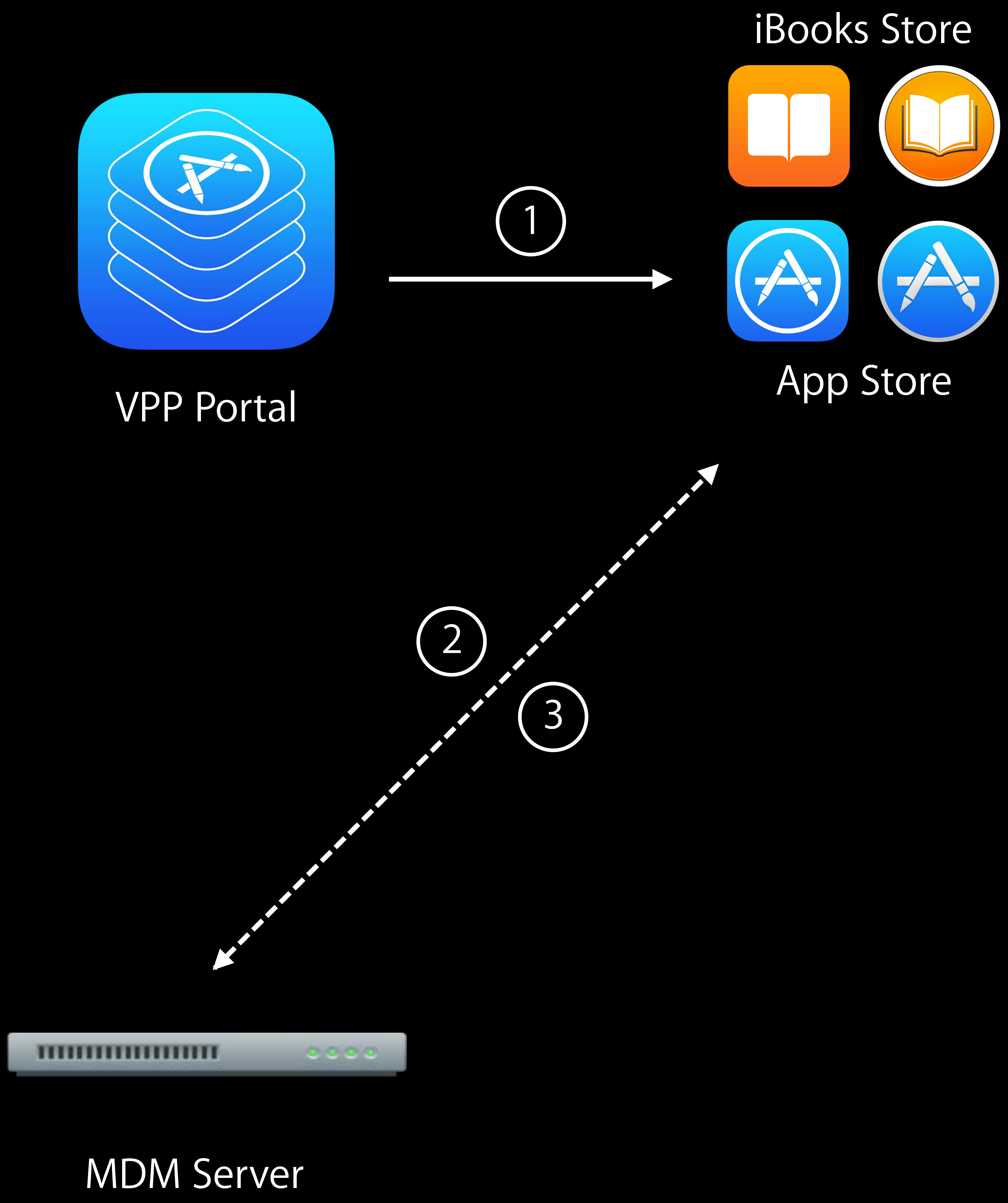

VPP Portal

1

iBooks Store

App Store


iBooks Store
VPP Portal
1
App Store
2
MDM Server

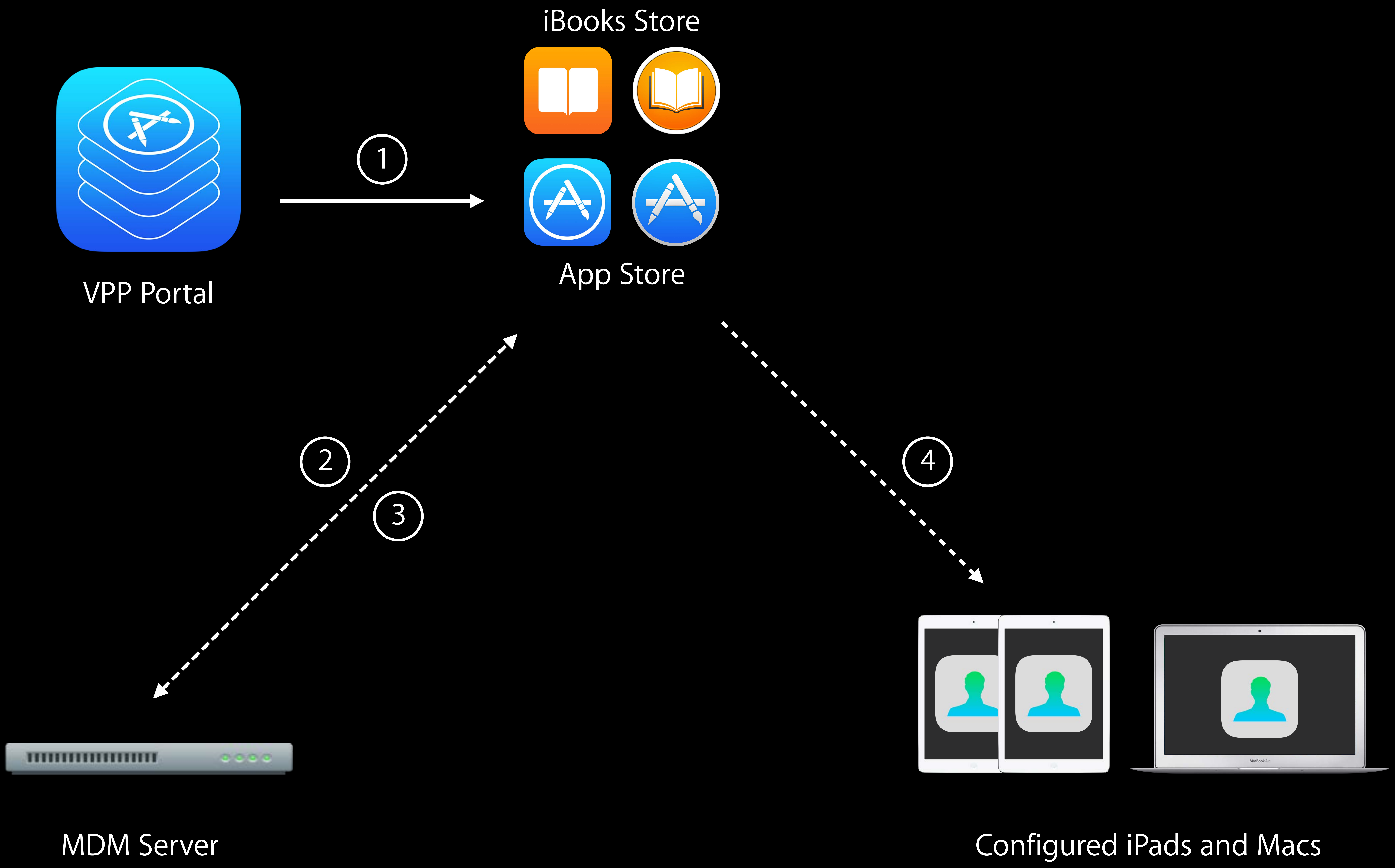


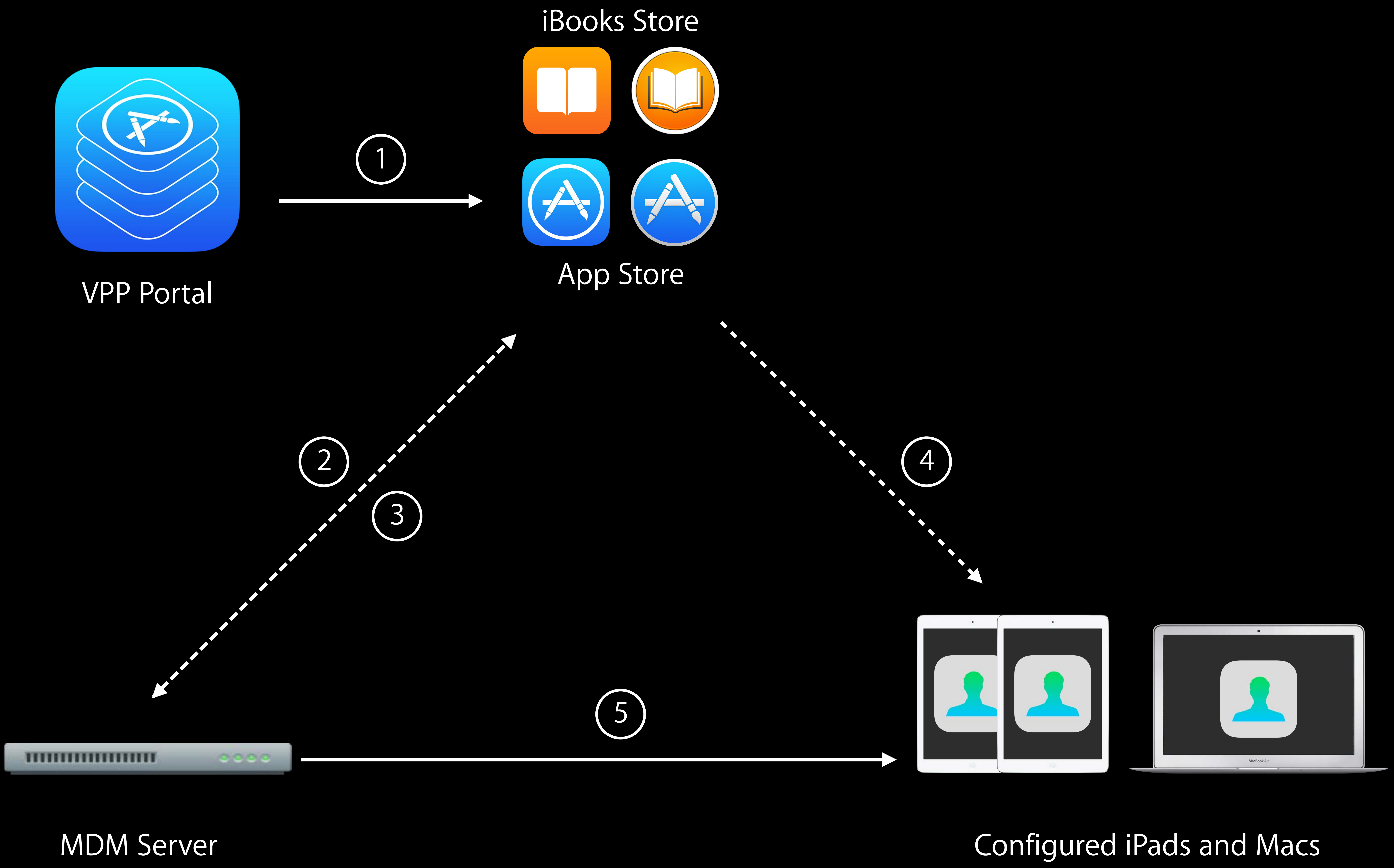
iBooks Store

VPP Portal

App Store

MDM Server


iBooks Store
VPP Portal
1
App Store
2
3
4
MDM Server
Configured iPads and Macs


iBooks Store
VPP Portal
1
App Store
2
3
4
5
MDM Server
Configured iPads and Macs

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

```
{"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&amp;inviteCode=ad9dd59ecf3a45fdaf005602be76ed09&amp;mt=8

Create custom URL to MDM server, then redirect to VPP URL

Integrate invitation into your user portal

Volume Purchase Program

User IDs

John
Appleseed
John
Appleseed
John
Appleseed

MDM User Account	VPP User Account	End User’s Apple ID
`clientUserIdStr`	`userId`	`itsIdHash`

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”

8 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

NEW

`countryCode` now added to response from VPPClientConfigSrv

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

http://www.apple.com/itunes/affiliates/resources/documentation/itunes-store-web-service-search-api.html

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

NEW

Installation of non-App Store signed flat .pkg containing app

Profile Manager also supports installing .app bundles

Demo

Installing Enterprise Apps and Books

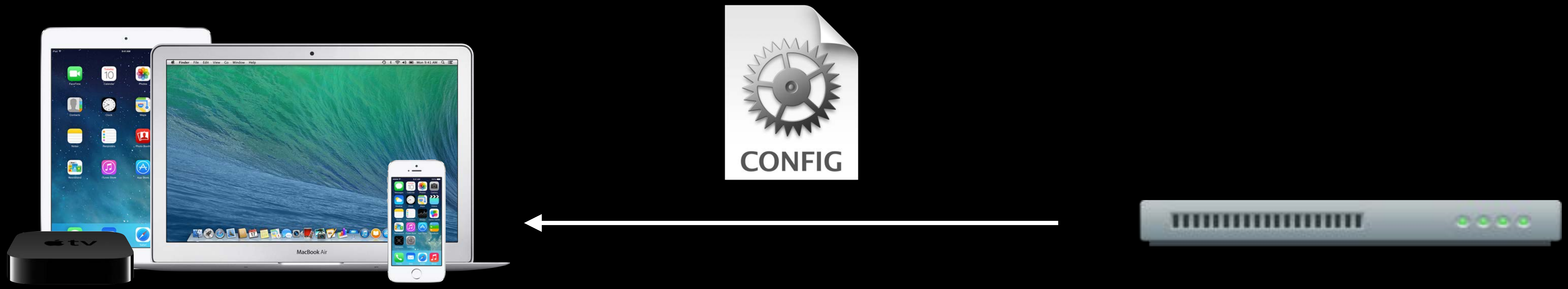
Distribute Demo Recap

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



Enroll

Distribute

Manage

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

NEW

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

NEW

- 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

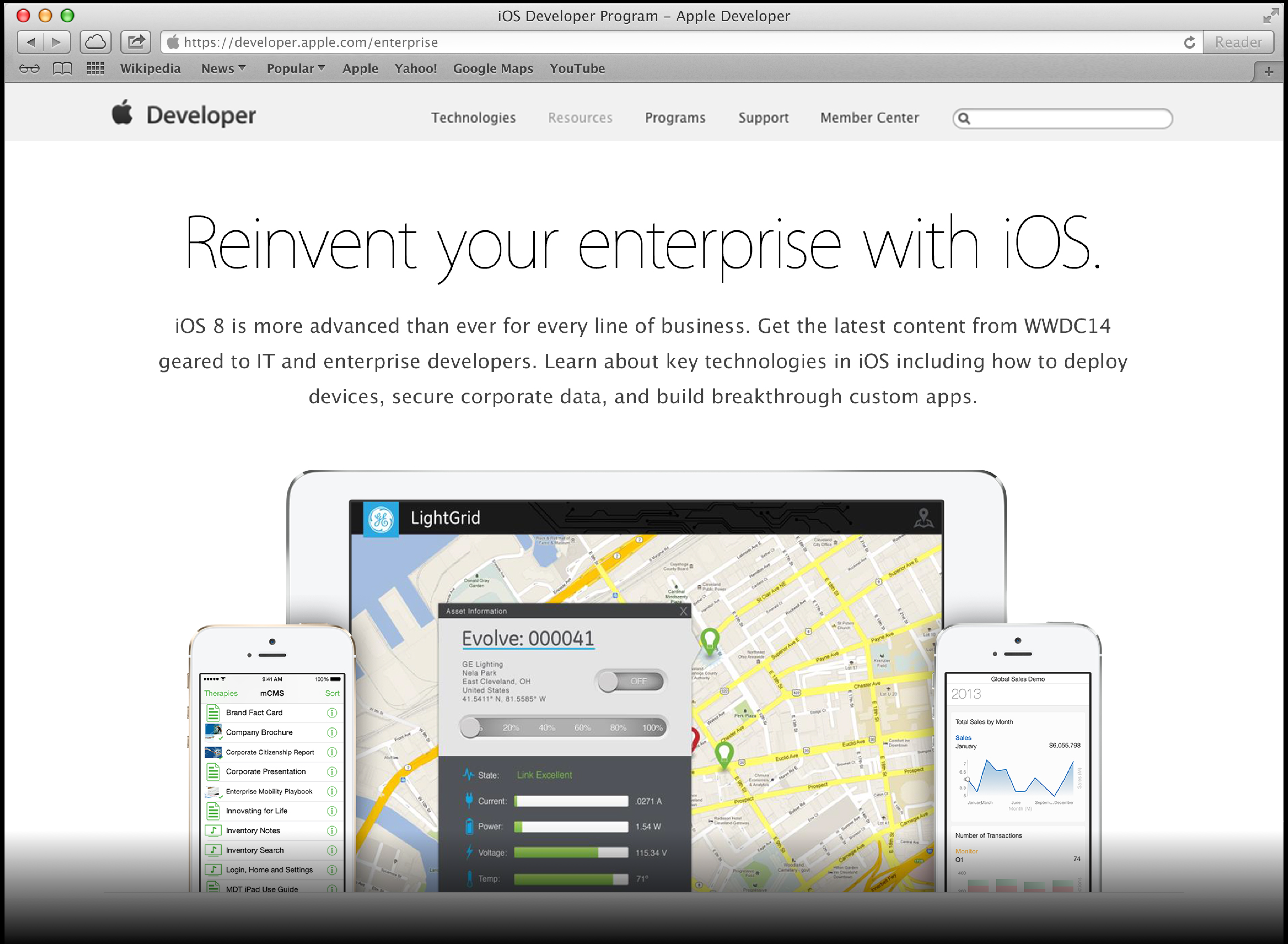
Summary

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 developer.apple.com/enterprise



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
https://developer.apple.com/account/ios/certificate/certificateCreate.action

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

https://deploy.apple.com/enroll/files/dep_help.pdf

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

● Building Apps for Enterprise and Education	Pacific Heights	Tuesday 10:15AM
● Distributing Enterprise Apps	Pacific Heights	Tuesday 11:30AM
● Apps for Enterprise Get Together	Broadway	Tuesday 4:30PM
● User Privacy in iOS and OS X	Nob Hill	Thursday 2:00PM

Labs

Developing Apps for Enterprise and Education	Core OS Lab A	Wednesday 2:00PM
Managing Apple Devices	Core OS Lab B	Thursday 9:00AM
Security and Privacy	Core OS Lab B	Thursday 3:15PM

WWDC14