Open Source MDM

… or how to embrace your inner 

Jesse Peterson @jessecpeterson @jessepeterson

Open Source MDM

… or how to embrace your inner 

Jesse Peterson
Victor Vrantchan

@jessecpeterson
@wikiwalk

@jessepeterson
@groob

Agenda for Today

Part I

MDM+DEP

Under the hood

What it means for Macs

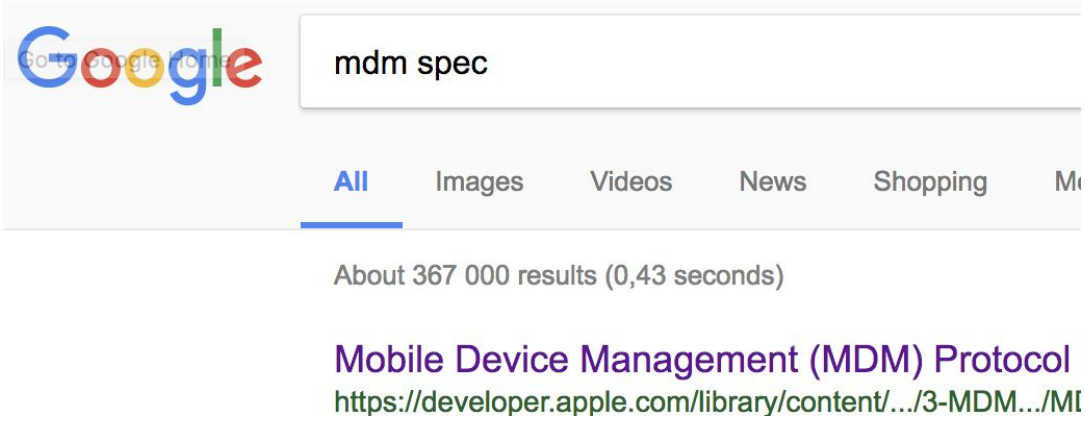
Part II

MicroMDM

Getting it up and running

Part I: MDM+DEP

Protocol, Spec, etc.



Why? What does MDM on Macs do for me?

Why? What does MDM on Macs do for me?

… or: what can't I do with other, better tools?

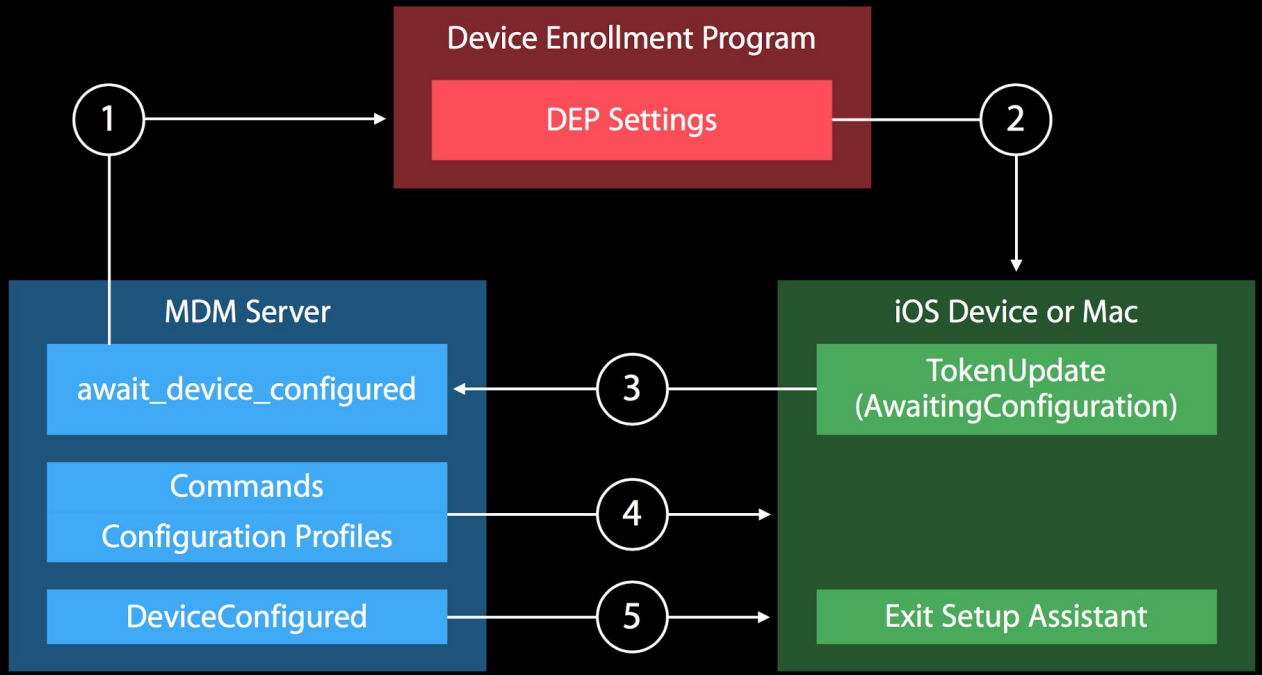
DEP bootstrapping
Remote Wipe*
VPP app distribution

DEP bootstrapping
Remote Wipe*
VPP app distribution
SKEL (UAKEL)

Device Enrollment Program

Device Enrollment Program

Enrollment optimization



Device Enrollment Program

deploy.apple.com

DEP API

Profile Fetch (Device)

DEP API:

- Most HTTP bodies are JSON
- Authenticated with OAuth tokens (with a PKI exchange to get them)
- MDM server periodically syncs devices from the DEP service
    - How MDM learns about devices to send DEP profile to

MDM Protocol & Specification

MDM: Bits on the wire

- Just an HTTPS server
- Prolific XML Plist passing: most HTTPS bodies are plists
- Sometimes responses are wrapped in encrypted or signed CMS (PKCS#7) messages or have detached signatures
- APNs or APNs HTTP/2 (but not yet new JWT APNs auth)
- SCEP protocol also HTTP but is largely CMS/PKCS#7 messages being passed

Enrollment

https://mdm.myorg.com/enroll
/scep
/ota/enroll

Checkin

/checkin

Command Queue

`/mdm/connect`

Commands: InstallApplication

DEP ~~-boot~~strap process

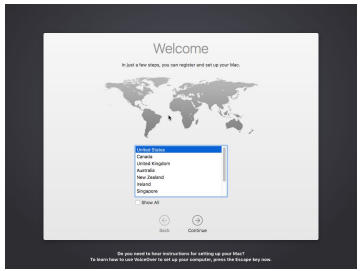
Power-on

DEP profile fetched from Apple

:00

:05

:07



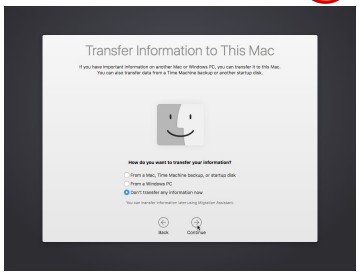
DEP enrollment presented

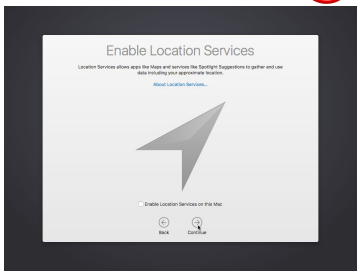
DEP MDM enrollment

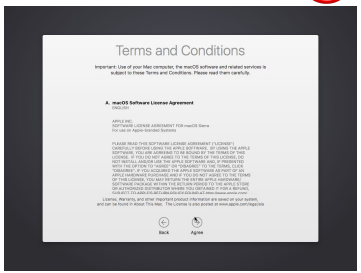
Await DeviceConfigured state

Can set to skip in DEP profile

:10 :12 :14 :16







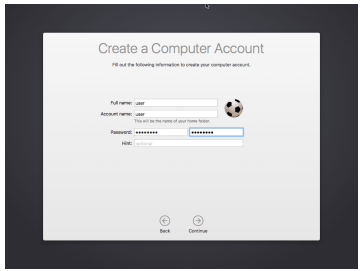
Per-user MDM token update

DEP enrollment done

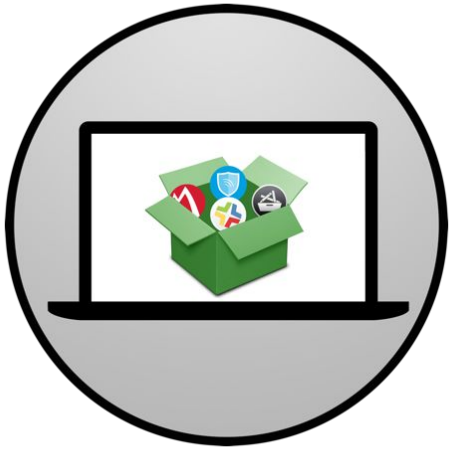
User account creation (can skip/can auto-create admin user)

Can't disable. Probably don't want to.

:20 :25 :30 :35



InstallApplications



github.com/erikng/installapplications

DEPNotify

gitlab.com/Mactroll/DEPNotify

Virtualize your DEP testing!

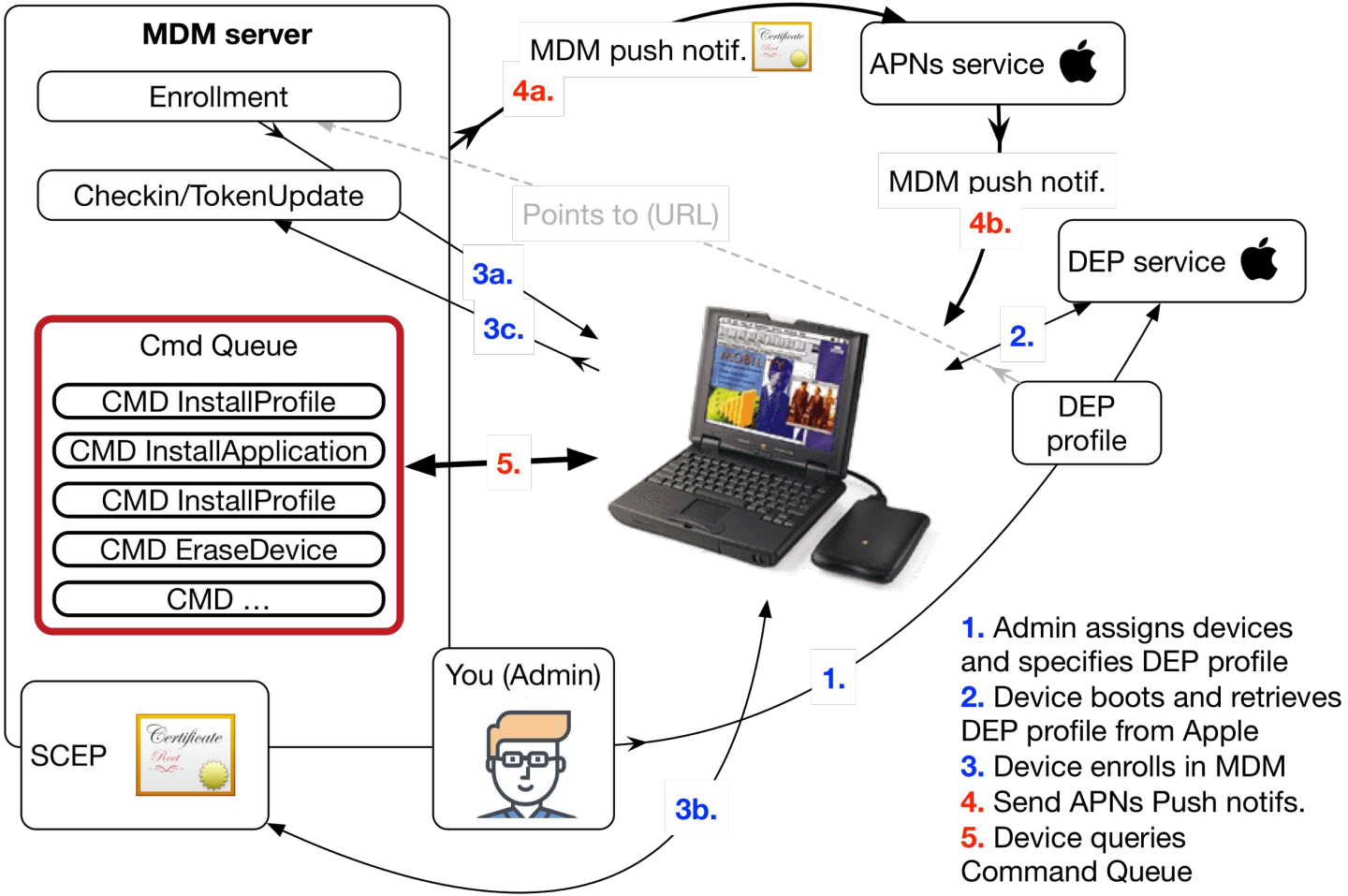
https://goo.gl/XuLWYB

https://www.rderewianko.com/how-to-create-a-vm-thatll-work-with-dep-on-vmware-fusion/

Thanks @rderewianko!

The bigger picture: DEP + MDM

MDM+DEP Operation in a nutshell

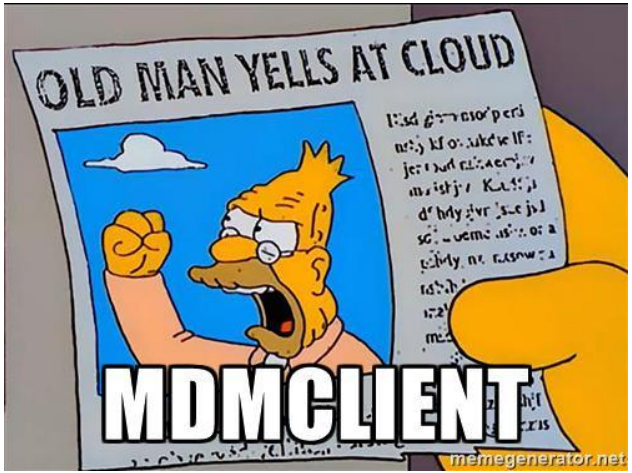


MDM: The Bad Parts

- APNs & DEP network requirement
- APNs & DEP availability, reliability, scalability
- Lack of adequate **desired state** inspection
- Complexity & restrictions of setting up an MDM
- MDM spec itself is terrible & vague in many areas
- MDM spec/features are glacial

MDM: The Bugs

- mdmclient terribly documented & buggy
- storedownloadd extremely fragile
- ever-evolving DEP InstallApplication context
- ScheduleOSUpdate & friends utterly unreliable



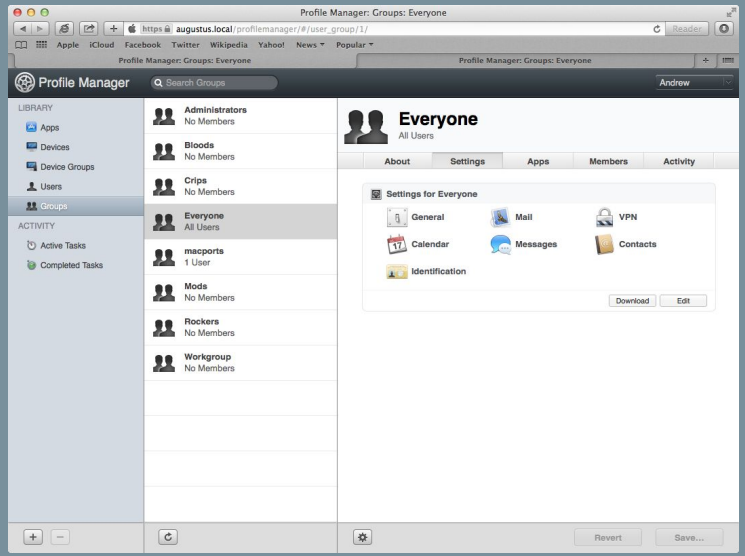
Part II: MicroMDM

Philosophy, getting up and running, etc.

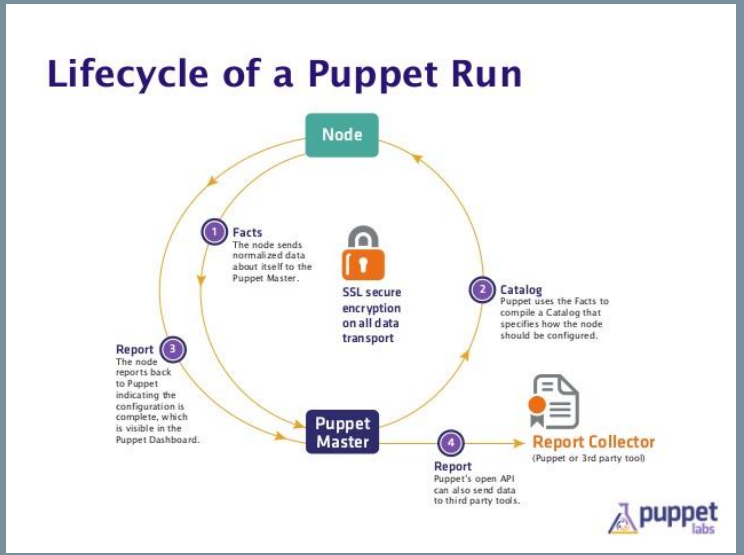
Why *Open Source* MDM?

- Curiosity
- Commercial MDM ain’t cutting it
- Extensibility/expandability/API/hooks
- Source is.. Open!
- Community support
- Not *just* a GUI/WEB UI
- Cost

The DevOps way



vs.



nmcspadden / Profiles

Watch 30 Star 119 Fork 19

Code Issues 4 Pull requests 0 Projects 0 Insights

Updated SetupAssistant for Yosemite

Browse files

master

nmcspadden committed on Apr 21, 2015 1 parent a5d296c commit fa192be17ae831266edd4bcb7aff89ee793e1cb5

Showing 1 changed file with 2 additions and 2 deletions. Unified Split

4 SetupAssistant_10.10.2.mobileconfig → SetupAssistant-10.10.3.mobileconfig View

```
@@ -45,11 +45,11 @@
45 45                                                    <key>DidSeeCloudSetup</key>
46 46                                                    <true/>
47 47                                                    <key>LastSeenCloudProductVersion</key>
48    -                                                  <string>10.10.2</string>
   48 +                                                  <string>10.10.3</string>
49 49                                                    <key>RunNonInteractive</key>
50 50                                                    <true/>
51 51                                                    <key>LastSeenBuddyBuildVersion</key>
52    -                                                  <string>14C109</string>
   52 +                                                  <string>14D136</string>
53 53                                                </dict>
54 54                                            </dict>
55 55                                        </array>
```

0 comments on commit fa192be

Please sign in to comment.

MicroMDM

https://micromdm.io

MicroMDM https://micromdm.io

MicroMDM is an experimental project to build a Mobile Device Management server for Apple devices. Our goal is to create a performant and extensible device management solution for enterprise and education environments.

Links

micromdm.io
MicroMDM on GitHub
Releases

Getting Started
Documentation
Issue Tracker

Contact Us

Blog Archive

News

Understanding MDM Certificates

Mobile Device Management (MDM) requires the use of various digital certificates for its operation. But exactly which certificates and the various ways in which they are generated, acquired, signed, used, exported, imported, and managed within an MDM product may not be so clear. Generally speaking a commercial MDM product or service manages most of the complexity related to these certificates for you but in the case of an open source MDM much of that responsibility will land on you. In this post I hope to bring a better understanding of these certificates with the aim that you'll be managing at least a few of them yourself.

Read More…

Documentation

- The Quickstart has instructions for getting started.
- The MicroMDM organization on GitHub has the source code for MicroMDM and related repositories.
- The contribution guide describes how you can contribute.

Community

The community around open source MDM is small but growing. If you're interested in the project and looking to chat with other MDM developers(and users), the best place to start is the MacAdmins Slack Team. Some of the channels you can join are #micromdm, #dep and #mdm.

We also maintain a list of related projects, blog posts and talks on the micromdm wiki page.

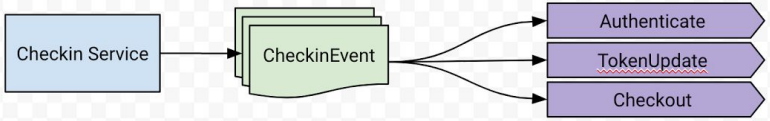
The Checkin Service is an http service which accep ts mdm checkin messages.

Devices send **Authenticate** message to establish a relationship.

TokenUpdate messages include the tokens necessary to send APNS payloads to the device.

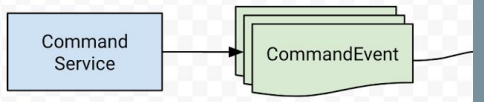
Checkout sent when the device un-enrolls.
Not guaranteed to be received.

A MDM Checkin message is wrapped in an "Event" which has uuid and timestamp fields. The event is serialized and sent on a message queue for other consumers to pick up.



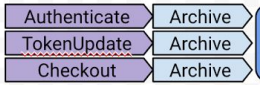
The service bus is a pub/sub message queue(NSQ) that works over TCP.
The services can either be embedded in a single binary application or distributed across multiple hosts.

Delivery is guaranteed at least once to each consumer group.

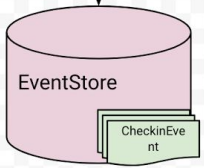


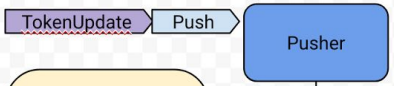
The Command Service creates MDM Payloads from command requests.

Service Bus (Pub/Sub message queue)

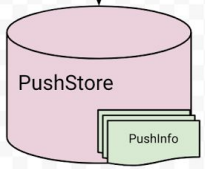


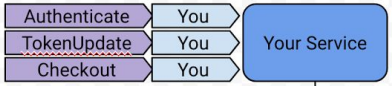
The Archiver service subscribes to topics on an "Archive" channel. It saves checkin events to an append-only datastore using the event timestamp as the key.



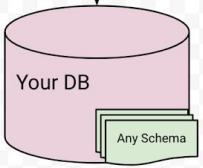


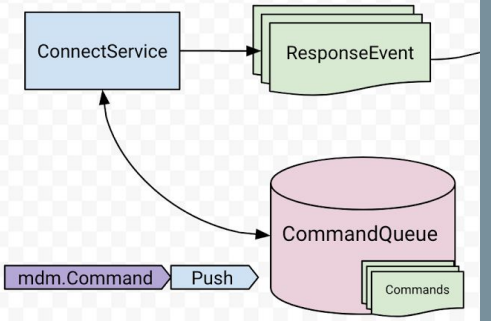
The Pusher service subscribes to TokenUpdate messages on a Push channel. It extracts the UDID, PushMagic and PushToken values and stores them for it's own use.
The PushStore knows how to create and send APNS messages and exposes an API for sending a push notification to a UDID.





You can subscribe to topics from the service bus to create any number of additional services/service workers.

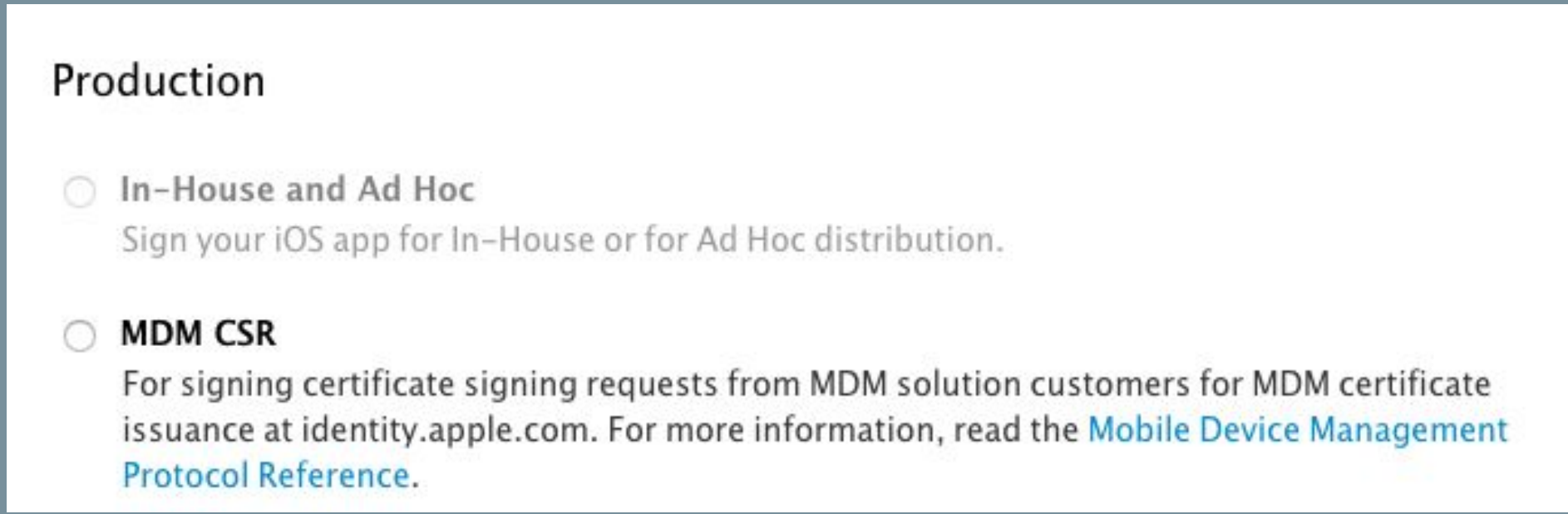




Getting up and running with MicroMDM: Things you'll need first

Read micromdm.io/blog for full write-up...

Vendor Certificate

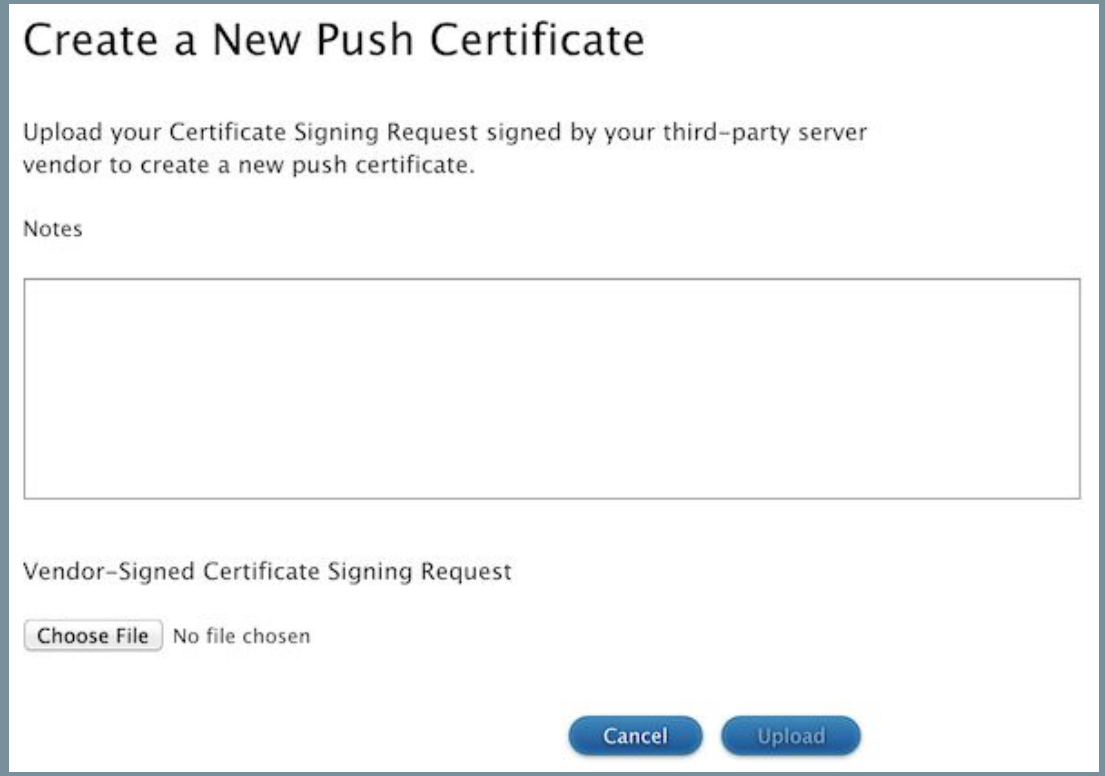


Vendor Certificate (other options)

Export from Server App

https://mdmcert.download

Push Certificate



identity.apple.com

Signing up for DEP

Read micromdm.io/blog for full write-up...

Video Demo

InstallApplications

github.com/erikng/installapplications

DEPNotify

gitlab.com/Mactroll/DEPNotify

Thank you & QA!

And happy MDMing!
Join us in **#micromdm** on Slack

Jesse Peterson

@jessecpeterson

@jessepeterson