

OPEN SOURCE MDM

STATE OF THE UNION

2018



WHERE WE WERE
WHERE WE ARE
WHERE WE'RE GOING

IF YOU'VE BEEN WAITING TO DEPLOY MDM:

NOW'S THE TIME

WHERE WE WERE



SOME CONTEXT: 2010, IOS 4, MDM ANNOUNCED

- ▶ MDM: Hooray!
- ▶ MDM specification paywalled
- ▶ Requires paywalled "vendor" certificate
 - ▶ Can use Server.app certificate (when macOS arrived)
- ▶ Very little documentation & reference code
- ▶ Of the documentation that existed: ~~poor quality & ambiguous~~ just terrible

2010—2014: VENDORS & RESEARCHERS

- ▶ 2010: MDM protocol arrives (2011 on macOS)
- ▶ 2011: David Shuetz Black Hat presentation
- ▶ 2013: Project iMAS mdm-server
- ▶ 2014: DEP arrives
- ▶ Vendor solutions

2015: OPEN SOURCE MDM BEGINS

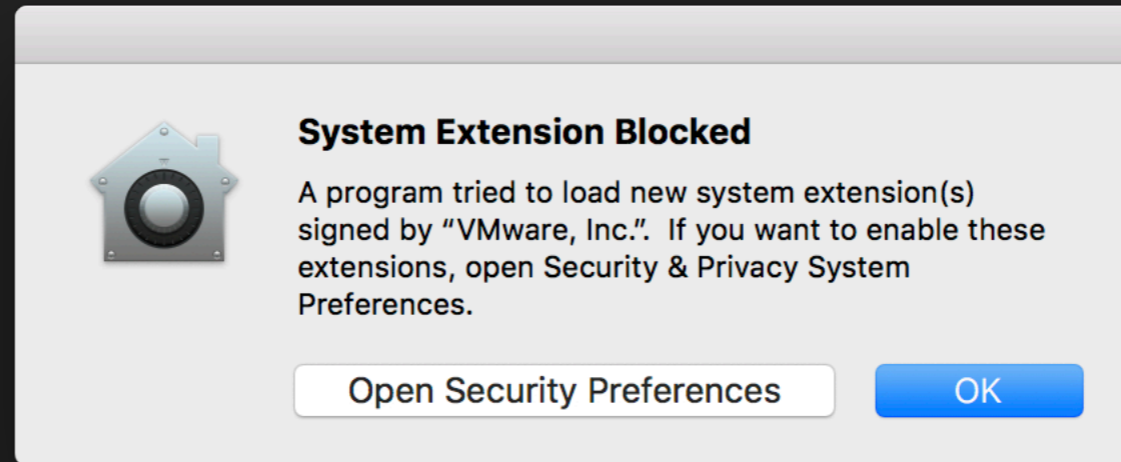
- ▶ June: @ygini starts Open Source MDM profile editor
- ▶ June: @bruienne MDM-amazing blog using mdm-server
- ▶ July: PSU MacAdmins BoF table
- ▶ July: @jessepeterson releases Commandment MDM server
- ▶ November: @groob (@wikiwalk) starts MDM blogs & dev
- ▶ November: community R&D into InstallApplications

2016—2017: REFINEMENT

- ▶ March 2016: @groob releases MicroMDM
- ▶ May 2016: @groob presents **right here** on MicroMDM
- ▶ 2016 OSS MDM dev work: SCEP, DEP, InstallApplications
- ▶ April 2017: micromdm reboots from nanomdm
- ▶ June 2017: **MVP for MicroMDM** (just in time!)
- ▶ June, July, October 2017: YVR, PSU, and MSA talks
- ▶ November 2017: @mosen takes over Commandment

**I BET THAT SYSTEM IMAGING
WILL END WITH APFS. YOU
SHOULD FOCUS ON DEP, MDM [...]**

@deploystudio



USER APPROVED

- MDM ENROLLMENT (+DEP)
- "SECURITY-SENSITIVE" SETTINGS

**IMAC PRO COMPUTERS DON'T
SUPPORT STARTING UP FROM
NETWORK VOLUMES.**

Apple HT202770

WHERE WE ARE



2018

NETBOOT: DEAD

IMAGING: DEAD*

* 99% sure its a non-starter

IF YOU'VE BEEN WAITING TO DEPLOY MDM:

~~NOW'S~~ YESTERDAY WAS
THE TIME

**OKAY, BUT WHAT'S THE
STATE OF OSS MDM?**

MICROMDM



COMMANDMENT

MicroMDM

Commandment

Goal/Design	MDM "platform"	Traditional MDM
Getting started	Easier	Harder (getting much better!)
Using	Harder (API+CLI)	Easier (Web UI)
Scalability	Good (potential)	Traditional
Extensibility	Very good	Traditional
iOS Support	Sorta (but planned)	No (but planned)

	MicroMDM	Commandment
Device Enrollment	✓	✓
DEP	✓	✓
VPP	-	-
User Enrollment	✓	-
SCEP	✓	✓ (macOS)
Web GUI	-	✓
HTTP API	✓	✓
Alt. Database	(In dev)	✓
Language	Go	Python
Community	Larger	Smaller
Code Contributors	12+	2+
Status	Active	Active
Cmd. Support	https://goo.gl/vQNeME	

DEMO

COMMANDMENT: SETTINGS

The screenshot shows the 'Settings' page in the COMMANDMENT interface. The navigation bar at the top includes 'CMDMNT', 'Devices', 'Profiles', 'Applications', 'Settings' (which is highlighted), and 'Groups'. The main content area contains five configuration cards:


- Organization**: Configure your organization
- SCEP**: Configure how communication is secured between your devices and this MDM
- Authentication**: Configure authentication sources
- VPP**: Configure access to the Volume Purchasing Programme
- DEP**: Configure the Device Enrollment Programme

COMMANDMENT: PROFILES

CMDMNT Devices **Profiles** Applications Settings Groups

Profiles

Drop configuration profile or Click to upload

Search... 

id	Name	Scope	UUID
1	iBooks	PayloadScope.System	a59201f6-a116-4fce-a7b0-a1caad3307cb
2	Commandment Enrollment Profile	PayloadScope.System	4b69552c-5cb5-48e3-ac37-527acd171237
3	Commandment Enrollment Profile	PayloadScope.System	6ef37216-7d8d-46a3-8716-c7f436eaf41a
4	MCX debug mode and logging	PayloadScope.System	d30c25bd-e0c1-44c8-830a-964f27dad4ba

< 1 >

COMMANDMENT: DEVICES

The screenshot displays the CDMNT web interface. At the top, there is a navigation bar with tabs for 'CMDMNT', 'Devices', 'Profiles', 'Applications', 'Settings', and 'Groups'. Below the navigation bar, there is an 'action' dropdown menu currently set to 'desktop'. The main content area shows the details for a device named 'elhack'. The device name 'elhack' is displayed in a large font, with a 'Rename' button next to it. To the right of the name, the storage capacity '20G' is shown. Below the name, the domain 'elhack.local' is listed. The device's status is shown as 'Last Seen' with a heart icon. The operating system is 'macOS 10.12.6 (16G29)'. The UDID is partially visible as '735-85B4-'. The Model is also partially visible. On the right side of the device details, there are icons for Bluetooth MAC (Not Available), Wifi MAC, and SIP (Disabled). Below the device details, there is a purple navigation bar with tabs for 'Detail', 'Certificates', 'Commands', 'Applications', 'Profiles', and 'Updates'. The 'Detail' tab is currently selected. Below the navigation bar, there are two sections: 'Security' and 'iTunes and iCloud'. The 'Security' section lists several security features that are enabled, each with a red 'X' icon: Firewall Enabled, Stealth Mode, Block all incoming, Has Passcode, Passcode is compliant, Passcode is compliant with profiles, Full Disk Encryption Enabled, With Personal Recovery Key, and With Institutional Recovery Key. The 'iTunes and iCloud' section lists 'Store account active' with a red 'X' icon.

CMDMNT Devices Profiles Applications Settings Groups

action ▾ desktop × ▾

elhack Rename **20G**

elhack.local

♥ Last Seen

🖥️ macOS 10.12.6 (16G29)

🏷️ UDID 735-85B4-

🖨️ Model

📶 Bluetooth MAC Not Available

📶 Wifi MAC

🛡️ SIP Disabled

Detail Certificates Commands Applications Profiles Updates

Security

- ✗ Firewall Enabled
 - ✗ Stealth Mode
 - ✗ Block all incoming
- ✗ Has Passcode
 - ✗ Passcode is compliant
 - ✗ Passcode is compliant with profiles
- ✗ Full Disk Encryption Enabled
 - ✗ With Personal Recovery Key
 - ✗ With Institutional Recovery Key

iTunes and iCloud

- ✗ Store account active

WHERE WE'RE GOING



MACOS: SOME PREDICTIONS

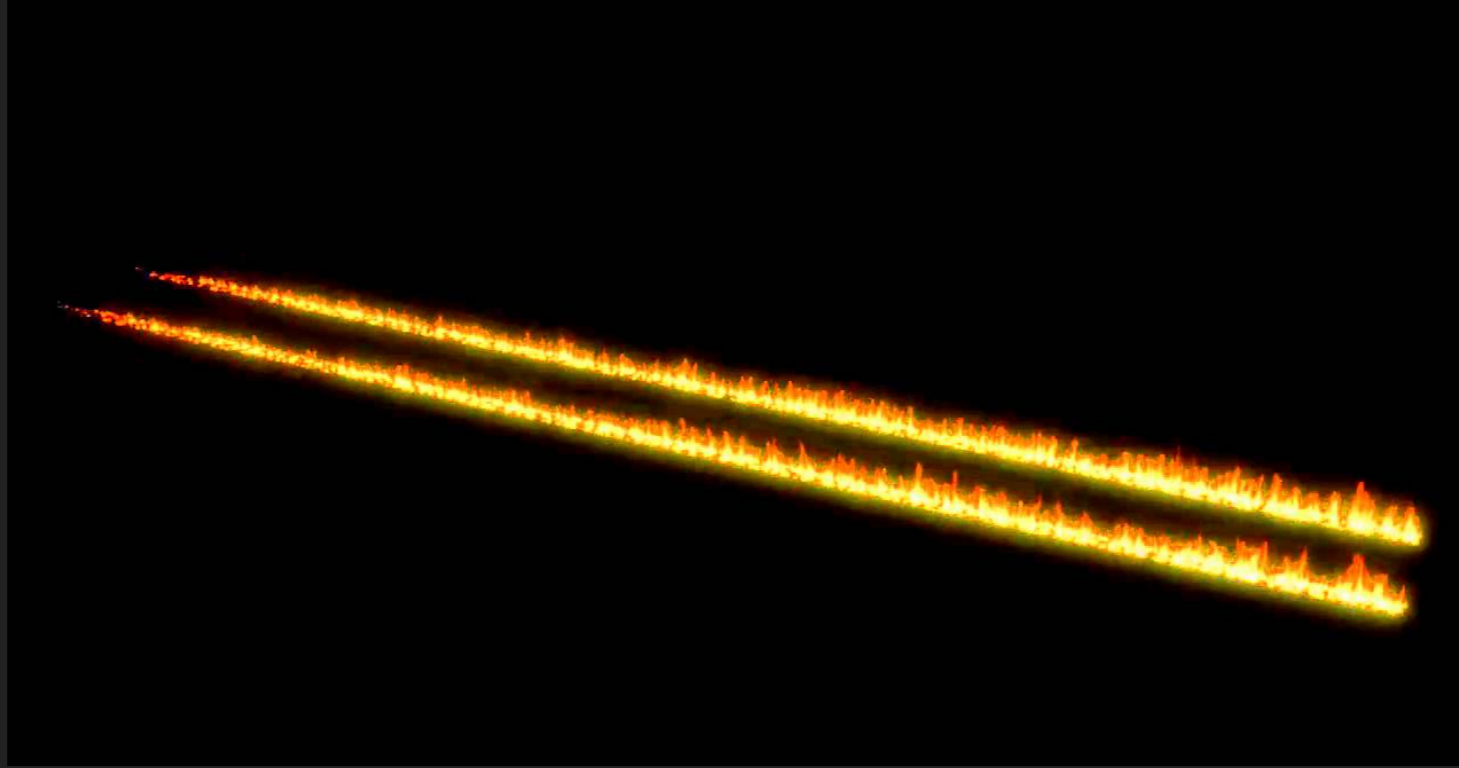
- ▶ More "security-sensitive"-ONLY settings
 - ▶ I.e. more dependence on User Approved/DEP MDM
 - ▶ Root launch daemons UA some day?

MICROMDM: FUTURE PLANS

- ▶ Better iOS support
- ▶ Better documentation
- ▶ More API features (no GUI on roadmap)
- ▶ High-availability/stateless/database abstraction (in dev)
- ▶ Auto-assignment of DEP registrations to profiles (in dev)
- ▶ Expose message bus (for integrations)
- ▶ More (& dynamic) Blueprint assignments (Workflows)

COMMANDMENT: FUTURE PLANS

- ▶ Adding non-Apple Store apps for installation
- ▶ Authentication to web UI



THANK YOU!

JOIN US ON SLACK!

#micromdm • micromdm.io

#commandment • github.com/cmdmnt/commandment