Custom PED

Performance Enhancing Deployments

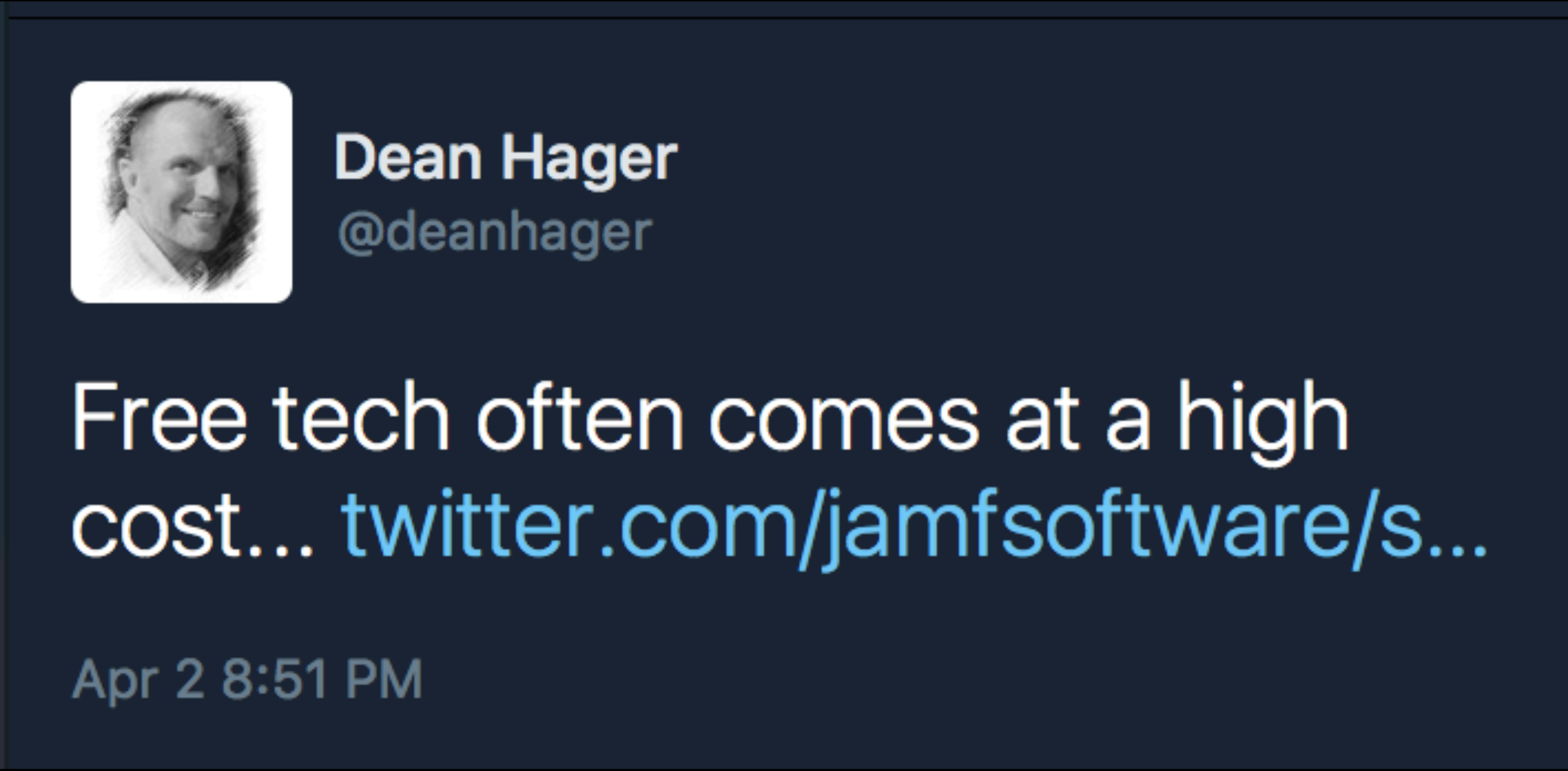
Achieving massive gains through MDM & OSS

Open Source

~~vs~~ *and*

Vendor MDM

(Custom DEP)



Dean Hager
@deanhager

Free tech often comes at a high cost... twitter.com/jamfsoftware/s...

Apr 2 8:51 PM

Freeware vs. Paid

The high cost of a cheap solution

Why?

1. The core of Jamf Pro is built on free, open source technologies
    - MySQL
    - Tomcat
2. Most Jamf Pro environments use other macadmin open source projects
    - auto-update-magic
    - AutoCasperNBI
    - AutoDMG
    - AutoPkg
    - Community Blog Posts / Scripts
    - createOSXInstallPkg
    - dockutil
    - jss-recipes
    - JSSImporter
    - outset
    - Rich Trouton Scripts
    - SplashBuddy/CasperSplash

Open source isn't *cheap* - it's ***free***

Cheap: *of inferior quality or worth*

Why did we leave Jamf Pro?

1. Platform Limitations
   - Profiles (.mobileconfig) are neither dynamic nor singular in scope.
   - No native support for .dmg compressed Applications or Choice Changes XML
   - No native support for managing/installing Apple updates, updating applications or detecting app state
   - Outstanding bugs that were not fixed and no bug tracking
   - No alpha -> beta -> production promotion
   - Extension Attributes/Smart Groups only support strings and Extension Attributes cannot be scoped
   - iOS and macOS only
2. Employee Extensibility / Trust
   - Management framework is not code-reviewable/logged nor audited [N].
   - Management framework cannot be augmented by the user.

[N] Audit log causes swelling of the database, leading to lower performance

Platform Limitations

Profile deployments are terrible on *all* traditional MDM platforms

Payload Best Practices

If you have multiple profiles containing similar payloads with different settings, the resulting behavior is undefined.

— *Apple*

Managing the screensaver lock shouldn't result in managing extra payloads:

Tool	Total Payloads	Total Keys Managed
Chef	1	2
AirWatch	6	7
Profile Manager	8	12 ❕
Jamf Pro	9	14 😱

com.apple.screensaver

- askForPassword
- askForPasswordDelay

Managing the screensaver lock shouldn't result in managing extra payloads:

Payload	Chef	AirWatch	Profile Manager	Jamf Pro
com.apple.screensaver	✓	✓	✓	✓
com.apple.applicationaccess		✓	✓	✓
com.apple.loginwindow		✓	✓	✓
com.apple.MCX			✓	✓
com.apple.preference.security			✓	✓
com.apple.security.firewall			✓	✓
com.apple.SubmitDiagInfo		✓	✓	✓
com.apple.systempolicy.control		✓	✓	✓
com.apple.systempolicy.managed		✓		✓

More ✓ is not a good thing...

Creating profiles through a paid MDM solution may result in *undefined* behavior.

Deploying profiles through Chef is incredibly precise.

Empowering your employees with Chef:

company_wide.rb

```ruby
# Manage the screensaver with cpe_screensaver Chef cookbook
begin
  node.default['cpe_screensaver']['idleTime'] = 600
  node.default['cpe_screensaver']['askForPassword'] = true
  node.default['cpe_screensaver']['askForPasswordDelay'] = 0
end
```

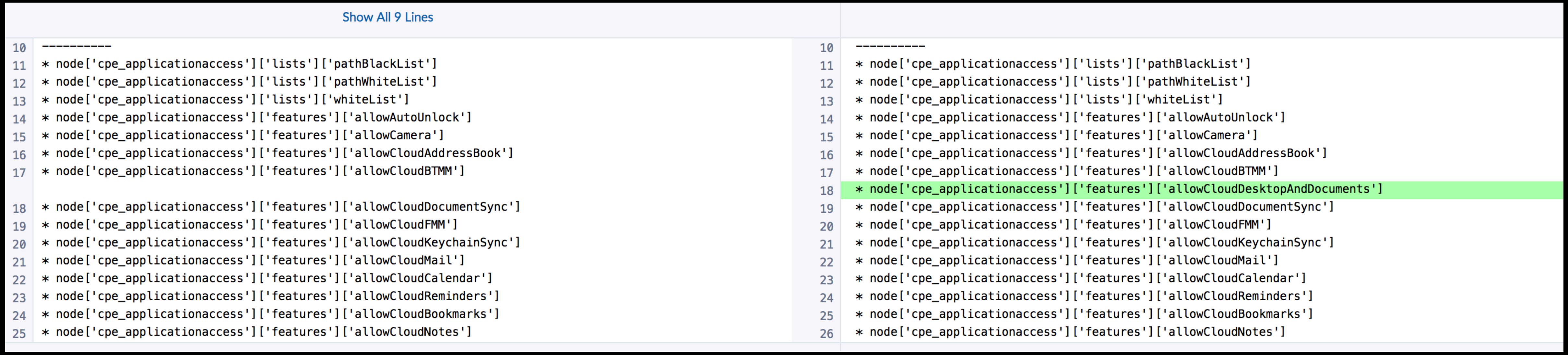
egomez.rb

```ruby
# Override delay to 5 seconds for egomez
begin
  node.default['cpe_screensaver']['askForPasswordDelay'] = 5
end
```

Adding new functionality to Chef is pretty easy.

Example 10.12.4 iCloud Drive

```ruby
# Add 10.12.4 iCloud Drive functionality
begin
  node.default['cpe_applicationaccess']['features']['allowCloudDesktopAndDocuments'] = false
end
```



```
----------
* node['cpe_applicationaccess']['lists']['pathBlackList']
* node['cpe_applicationaccess']['lists']['pathWhiteList']
* node['cpe_applicationaccess']['lists']['whiteList']
* node['cpe_applicationaccess']['features']['allowAutoUnlock']
* node['cpe_applicationaccess']['features']['allowCamera']
* node['cpe_applicationaccess']['features']['allowCloudAddressBook']
* node['cpe_applicationaccess']['features']['allowCloudBTMM']

* node['cpe_applicationaccess']['features']['allowCloudDocumentSync']
* node['cpe_applicationaccess']['features']['allowCloudFMM']
* node['cpe_applicationaccess']['features']['allowCloudKeychainSync']
* node['cpe_applicationaccess']['features']['allowCloudMail']
* node['cpe_applicationaccess']['features']['allowCloudCalendar']
* node['cpe_applicationaccess']['features']['allowCloudReminders']
* node['cpe_applicationaccess']['features']['allowCloudBookmarks']
* node['cpe_applicationaccess']['features']['allowCloudNotes']
```

```
----------
* node['cpe_applicationaccess']['lists']['pathBlackList']
* node['cpe_applicationaccess']['lists']['pathWhiteList']
* node['cpe_applicationaccess']['lists']['whiteList']
* node['cpe_applicationaccess']['features']['allowAutoUnlock']
* node['cpe_applicationaccess']['features']['allowCamera']
* node['cpe_applicationaccess']['features']['allowCloudAddressBook']
* node['cpe_applicationaccess']['features']['allowCloudBTMM']
* node['cpe_applicationaccess']['features']['allowCloudDesktopAndDocuments']
* node['cpe_applicationaccess']['features']['allowCloudDocumentSync']
* node['cpe_applicationaccess']['features']['allowCloudFMM']
* node['cpe_applicationaccess']['features']['allowCloudKeychainSync']
* node['cpe_applicationaccess']['features']['allowCloudMail']
* node['cpe_applicationaccess']['features']['allowCloudCalendar']
* node['cpe_applicationaccess']['features']['allowCloudReminders']
* node['cpe_applicationaccess']['features']['allowCloudBookmarks']
* node['cpe_applicationaccess']['features']['allowCloudNotes']
```

Platform Limitations

Traditional MDM is *not* Desired State.

(If someone tells you this, they are *wrong*.)

Traditional MDM is *not* Desired State

Desired State: Defining your machine state with code.

Machines often and easily “drift” through various states.

- While some MDM's can push scripts/packages, they cannot adequately ensure a machine is in an accurate state. The *script* is the underlying method of detection/resolution.
- Devices could change state *during* Recons.
- Dynamic MDM Smart Groups are often "too late" - It takes multiple policy runs to bring a device back into an expected state. This is too long.

Traditional MDM is *not* Desired State

```
# Traditional MDM Demo Script
#!/bin/bash

# Create MDM Folder
/bin/mkdir -p “/Library/Application Support/MDM”

# Set MDM Permissions
/bin/chown -R root:wheel “/Library/Application Support/MDM”

--------------------------------------------------------------------------------------------------------

# Chef Demo Code
directory "Create /Library/Application Support/MDM" do
    owner 'root'
    group 'wheel'
    mode '0755'
    path "/Library/Application Support/MDM"
    action :create
end
```

The Jamf Free vs. Paid ebook was right about two things:

It takes time and effort to build a system from the ground up…

...but Rome wasn't built in a day

- GitHub
- Google Groups
- IT Think Tank
- Jamfnation (yep)
- MacAdmin Slack
- MacBrained
- Twitter

Our community is incredibly strong

And zero-touch deployments weren't possible...

…until now.

Unique Partnership

Paid MDM + Open source

Pinterest

&

vmware®

airwatch®

Choosing a "Best of Breed, Hybrid" Model

Tool	DEP	Remote Wipe	Apps	Machine State	Profiles	FileVault
AirWatch	✅	✅	✓[3]	-	✓[2]	✓[1]
Chef	-	-	✓[1]	✅	✅	-
Crypt	-	-	-	-	-	✅
Munki	-	-	✅	-	✓[1]	-

[1] Available but not utilized by Pinterest

[2] Signed/Encrypted Certificate Payloads

[3] App Store apps

There's not enough money in the world to make me use AirWatch again.

— Erik Gomez, 2012 - 2016

AirWatch isn't perfect

- API
  - Does not return all logged machine data
- Enterprise Integrations
  - Poor OpenLDAP documentation
  - Requires two SAML connections (admin and user)
- UI
  - Many things are buried within multiple sub-menus

So why AirWatch?

- Active in the macadmin Slack (#airwatch)
- Laser Focus on MDM/DEP
- Multi-platform support
    - Android, iOS, macOS, Windows
- Multi-tenancy
    - Can give helpdesk / admins granular access
    - Multiple DEP profiles both globally and per tenant
- Partnerships
    - Custom DEP
    - Custom Android functionality

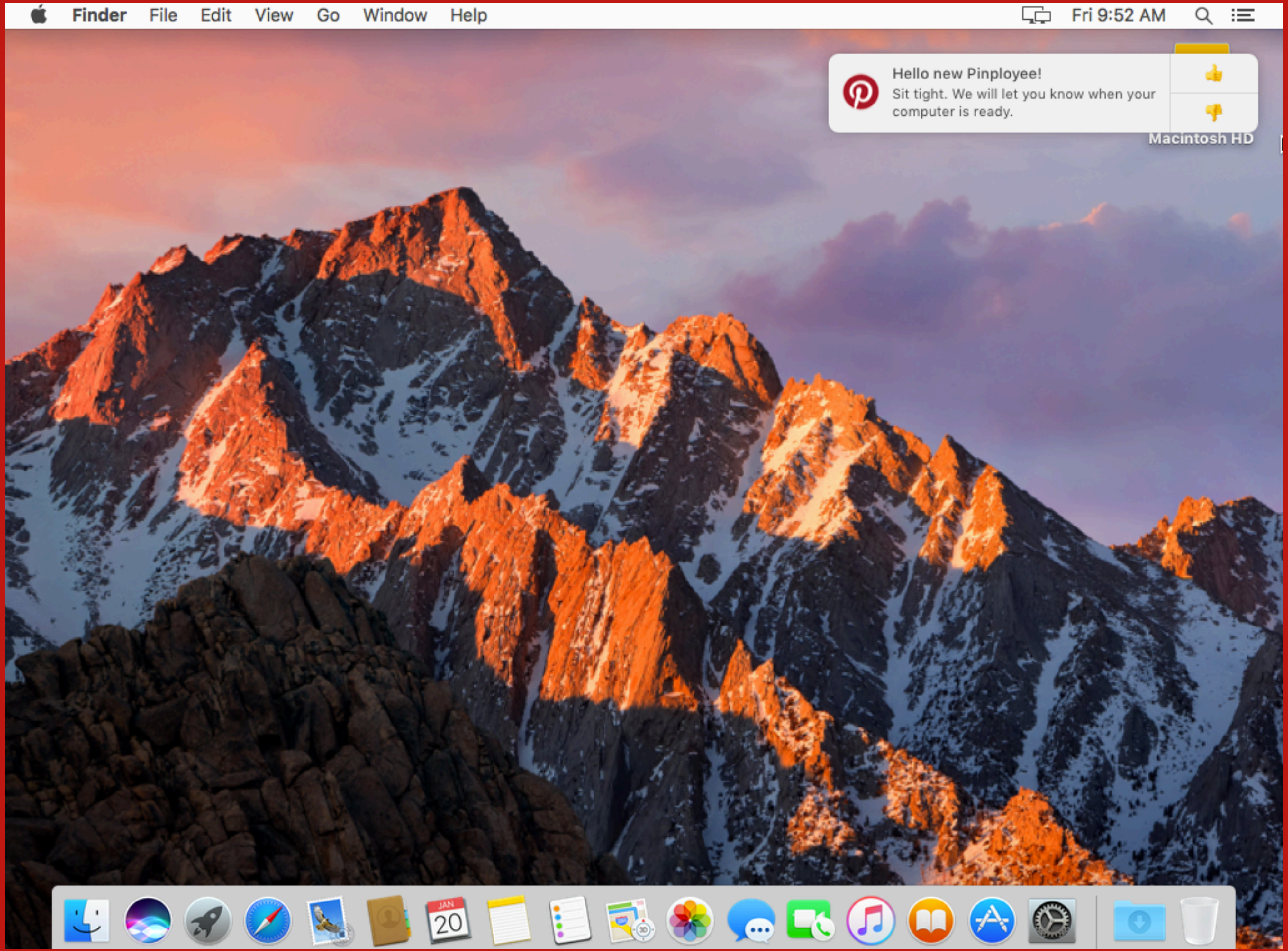
Instead of posting ebooks about the dangers of open source,

AirWatch *embraced* it.

Within a week of our partnership, we had the ability to deliver our custom DEP package.

But it took a lot of brainstorming (and code) to come up with our deployment.

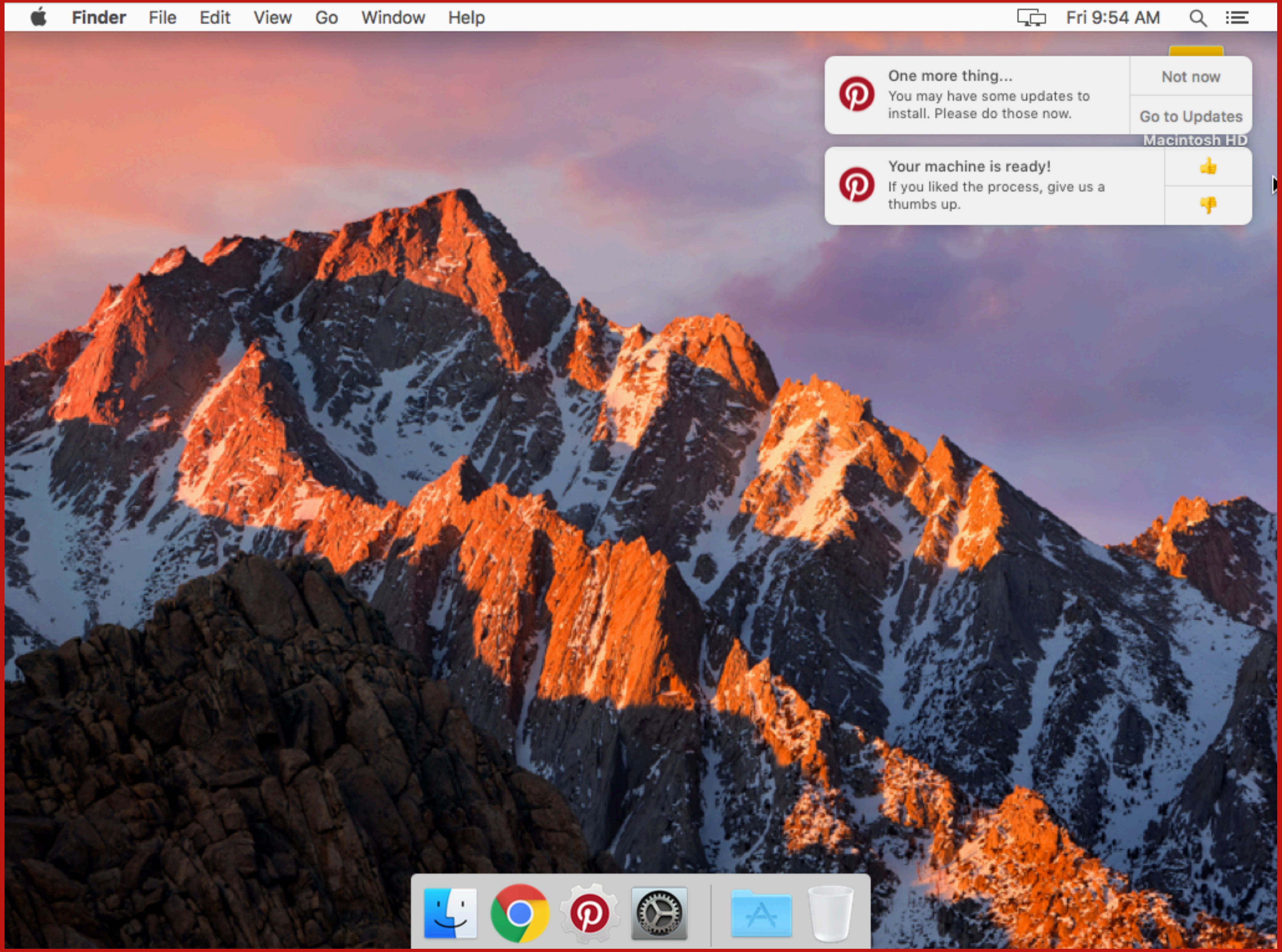
DEP Beta v.01



Hello new Pinployee!

Sit tight. We will let you know when your computer is ready.

DEP Beta v.01 (cont)



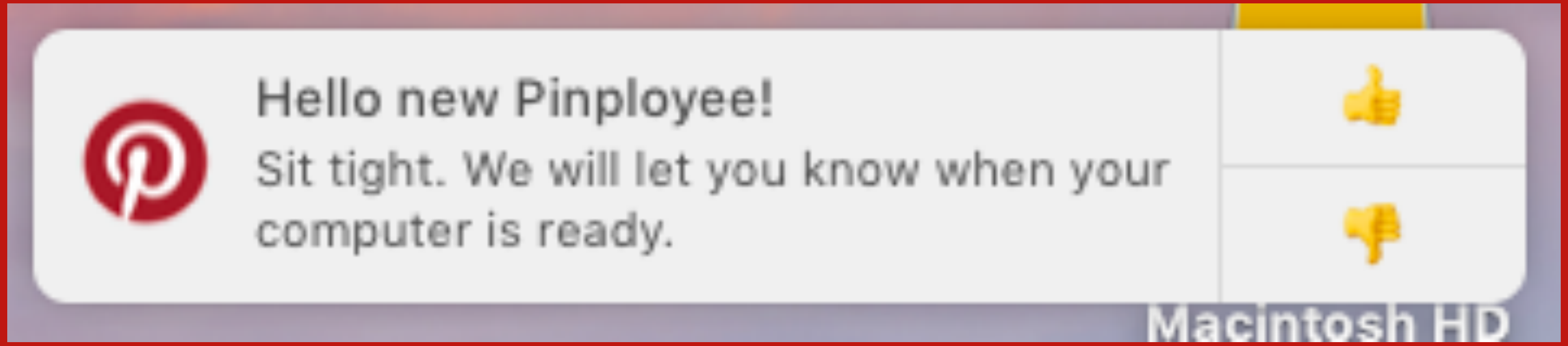
One more thing...

You may have some updates to install. Please do those now.

Your machine is ready!

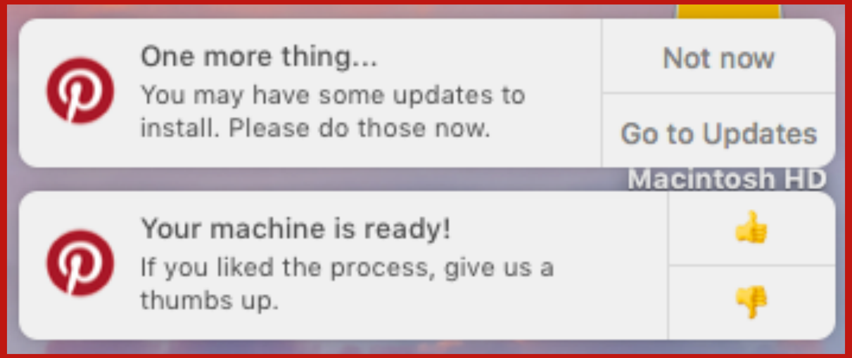
If you liked the process, give us a thumbs up.

Other UI tests



Hello new Pinployee!

Sit tight. We will let you know when your computer is ready.

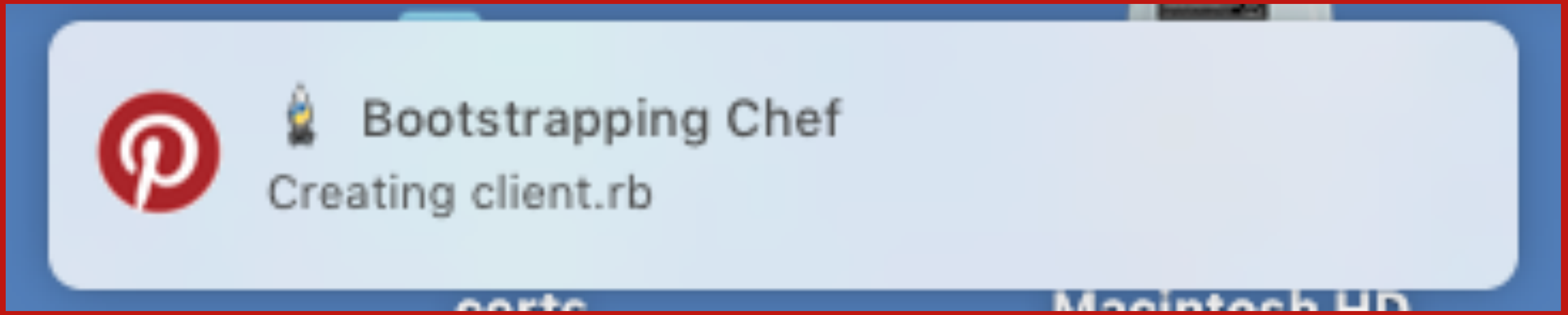


One more thing...

You may have some updates to install. Please do those now.

Your machine is ready!

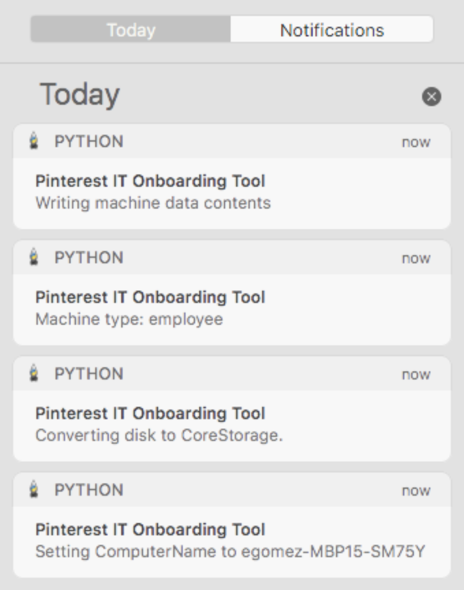
If you liked the process, give us a thumbs up.



Bootstrapping Chef

Creating client.rb

Other UI tests



PYTHON now

Pinterest IT Onboarding Tool
Writing machine data contents

PYTHON now

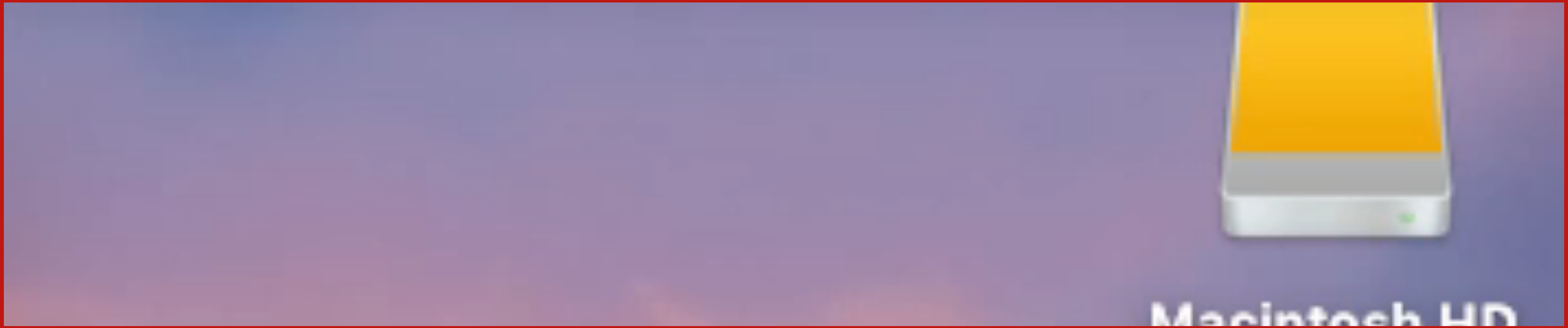
Pinterest IT Onboarding Tool
Machine type: employee

PYTHON now

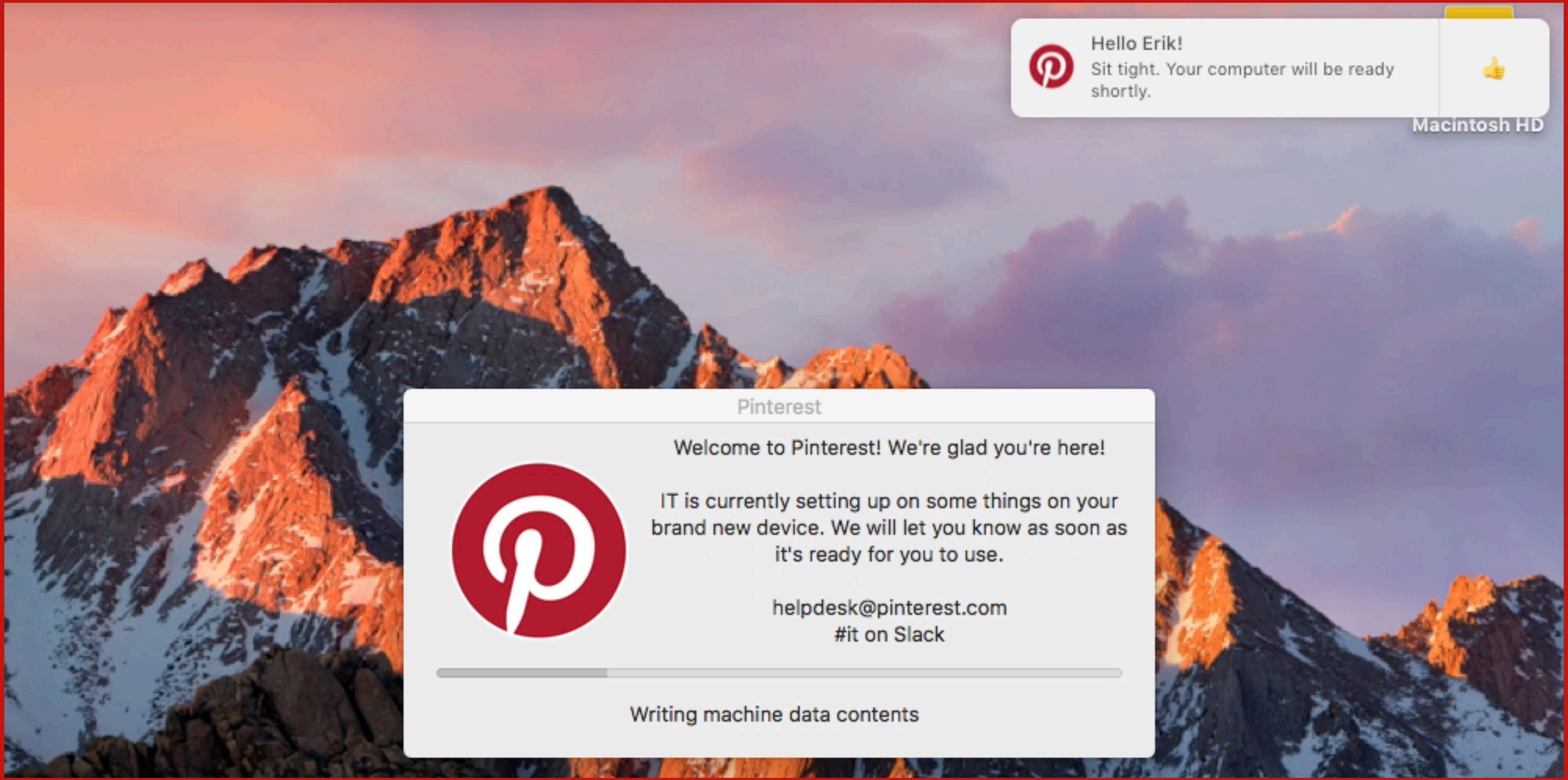
Pinterest IT Onboarding Tool
Converting disk to CoreStorage.

PYTHON now

Pinterest IT Onboarding Tool
Setting ComputerName to egomez-MBP15-SM75Y



User Experience 1.0



Hello Erik!
Sit tight. Your computer will be ready shortly.

Pinterest

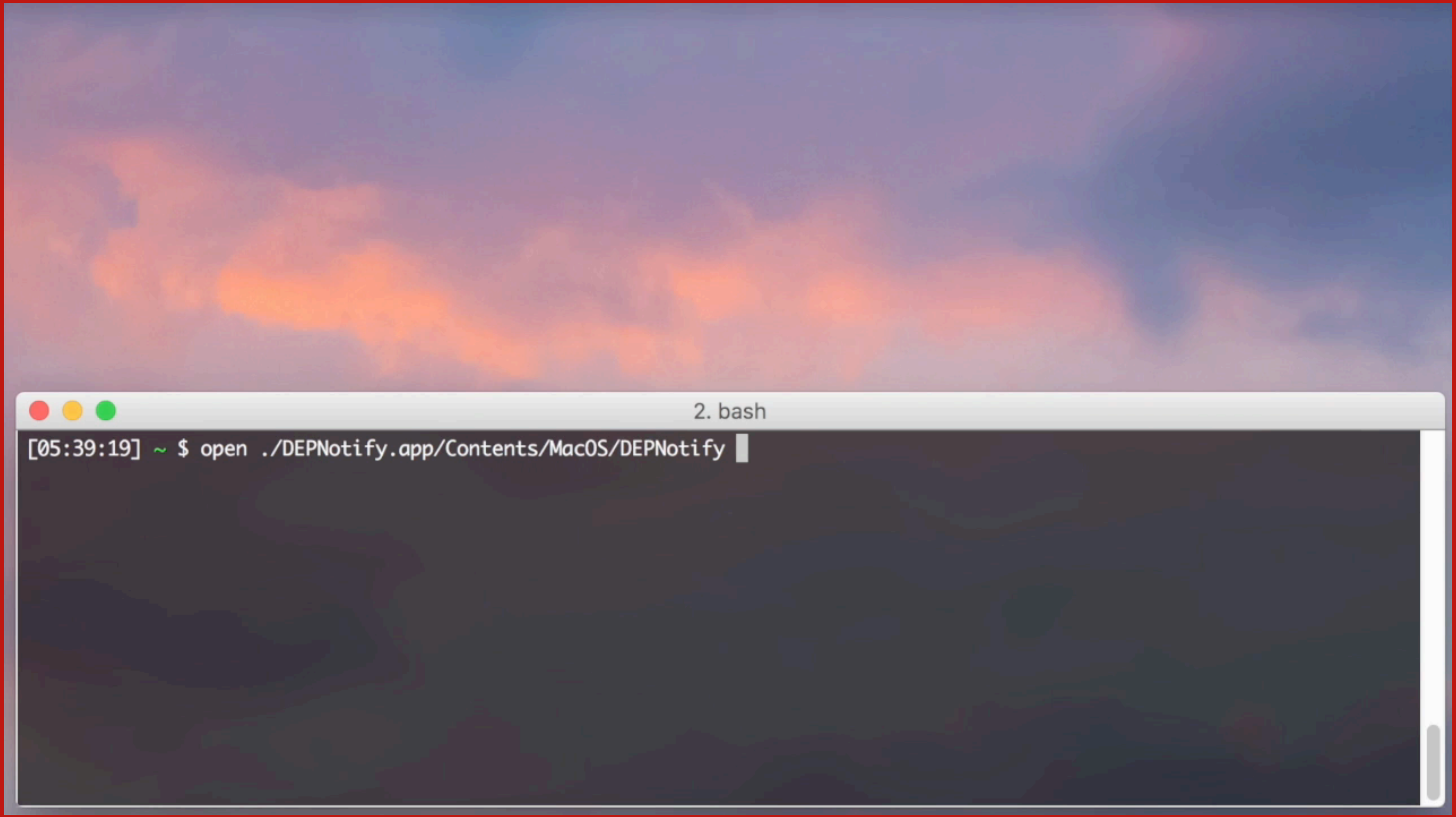
Welcome to Pinterest! We're glad you're here!

IT is currently setting up on some things on your brand new device. We will let you know as soon as it's ready for you to use.

helpdesk@pinterest.com
#it on Slack

Writing machine data contents

DEPNotify



```
[05:39:19] ~ $ open ./DEPNotify.app/Contents/MacOS/DEPNotify
```

DEPNotify

https://gitlab.com/Mactroll/DEPNotify

#depnotify on Slack MacAdmins

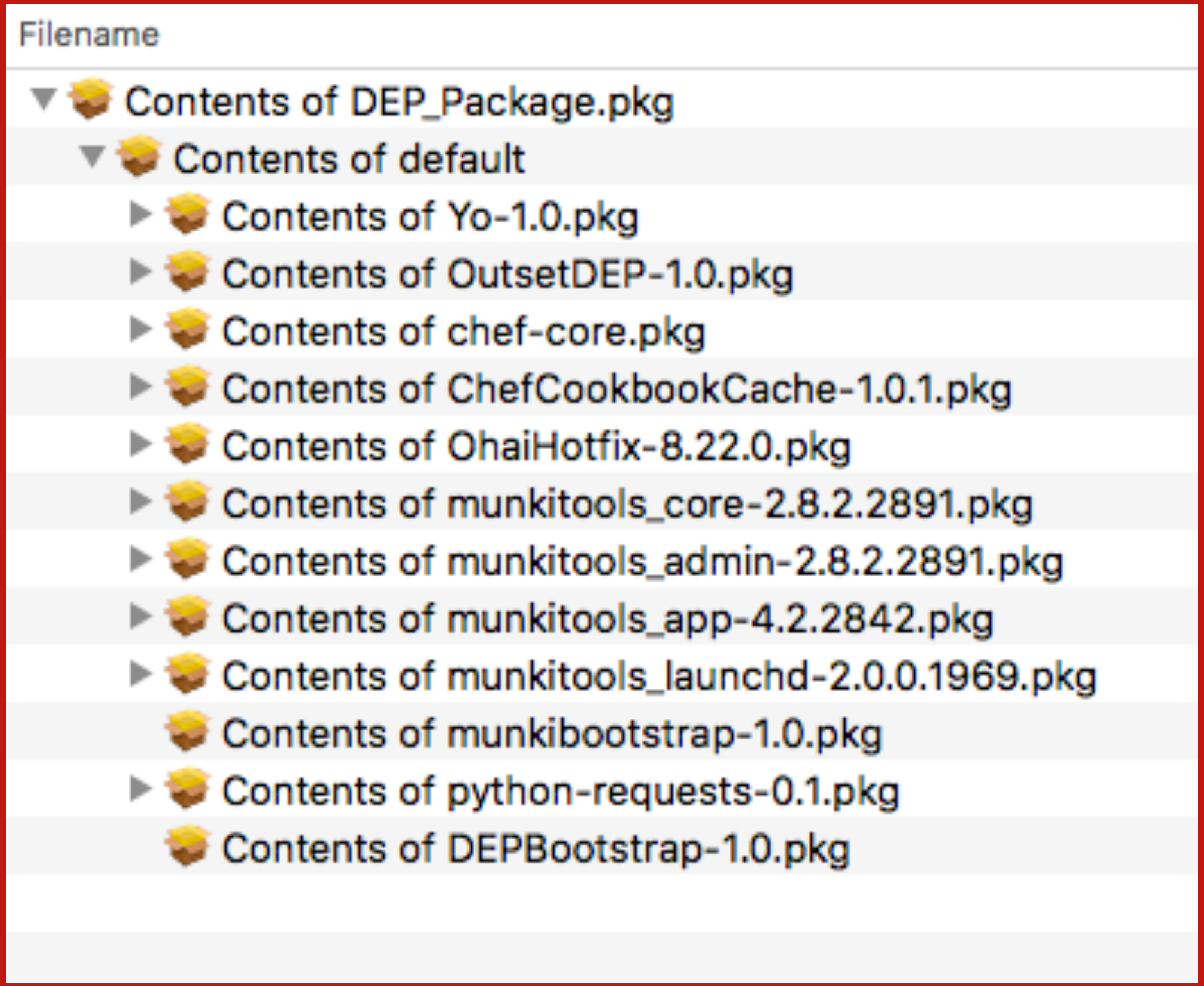
InstallApplication requirements

- Distribution Package
  - Signed by Developer Account
  - Sub packages optionally signed, but *cannot* be distribution packages
- AppManifest.plist
  - URL to signed distribution package
  - md5/md5s (split into 10MB chunks)

Custom DEP Package

Version	Size
0.1	3.5 MB
0.2	10.1 MB
0.3	22.5 MB
0.4	43.9 MB
0.5	58.6 MB
0.6	57.9 MB
0.7	57.0 MB
0.8	71.4 MB
0.9	72.8 MB

Monolithic Packaging 😱

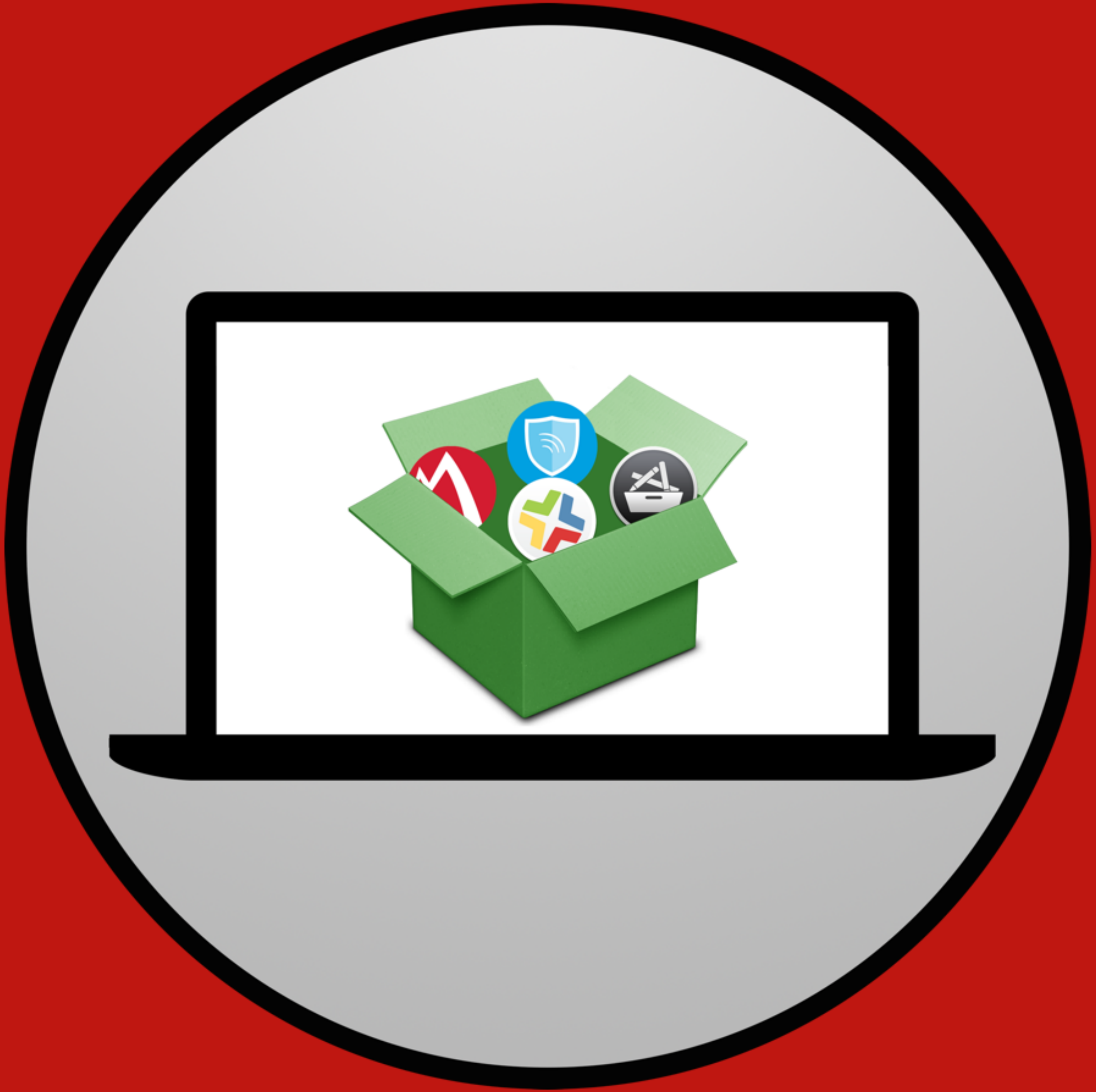


```
Filename
▼ Contents of DEP_Package.pkg
    ▼ Contents of default
        ▶ Contents of Yo-1.0.pkg
        ▶ Contents of OutsetDEP-1.0.pkg
        ▶ Contents of chef-core.pkg
        ▶ Contents of ChefCookbookCache-1.0.1.pkg
        ▶ Contents of OhaiHotfix-8.22.0.pkg
        ▶ Contents of munkitools_core-2.8.2.2891.pkg
        ▶ Contents of munkitools_admin-2.8.2.2891.pkg
        ▶ Contents of munkitools_app-4.2.2842.pkg
        ▶ Contents of munkitools_launchd-2.0.0.1969.pkg
          Contents of munkibootstrap-1.0.pkg
        ▶ Contents of python-requests-0.1.pkg
          Contents of DEPBootstrap-1.0.pkg
```

Custom DEP Package v1.0

30 KB

(99.95% reduction in size)



InstallApplications

https://github.com/erikng/installapplications

#installapplications on Slack MacAdmins

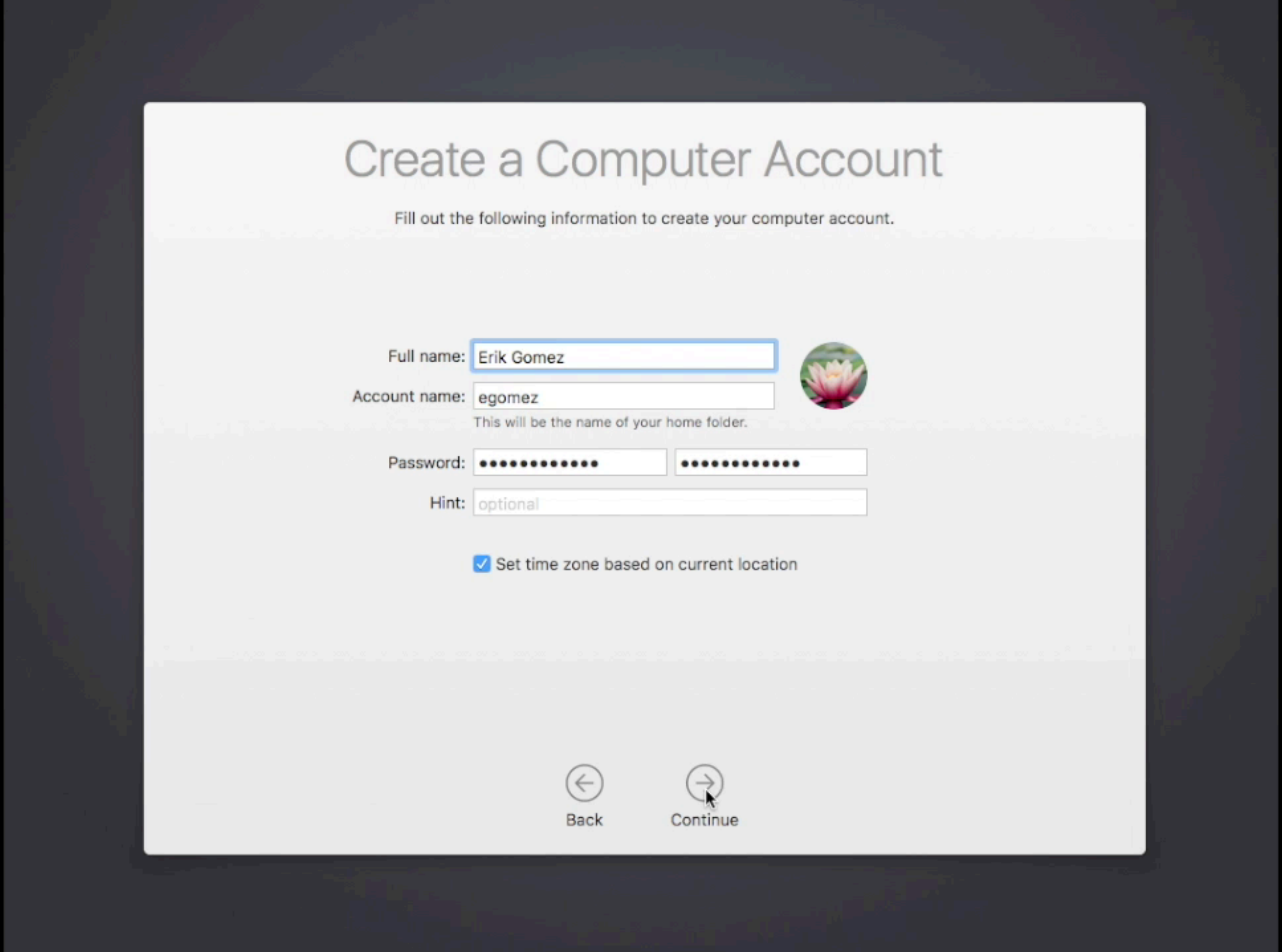
InstallApplications solves many limitations

- DEP
  - Ability to install more than one package
  - Install packages *during* SetupAssistant and *after* (requires 10.12.4+)
  - Do not have to update your DEP package each time there is an update
- Support for non-MDM/DEP capable devices
  - Virtual Machines
  - Pre-DEP devices through imaging

```
python ./installapplications.py --jsonurl https://domain.tld/dep.json
```

```
{
  "prestage": [
    {
      "file": "/private/tmp/installapplications/depnotify.pkg",
      "url": "https://domain.tld/depnotify.pkg",
      "hash": "71fec9a93119e8649a8e6f601720c6d44d7b19cbccc1a0e29609bd9732b701eb"
    }
  ],
  "stage1": [
    {
      "file": "/private/tmp/installapplications/bootstrap_ui.pkg",
      "url": "https://domain.tld/bootstrap_ui.pkg",
      "hash": "a2e29c3594f63ef2a39dc5591cc725b67c9b528e707f1db159a2391719d72539"
    }
  ],
  "stage2": [
    {
      "file": "/private/tmp/installapplications/chef.pkg",
      "url": "https://domain.tld/chef.pkg",
      "hash": "82502191c9484b04d685374f9879a0066069c49b8acae7a04b01d38d07e8eca0"
    }
  ]
}
```

With AirWatch, InstallApplications and macOS 10.12.4, you can create an almost instant UI prompt for your DEP devices.



Create a Computer Account

Fill out the following information to create your computer account.

Full name: Erik Gomez

Account name: egomez

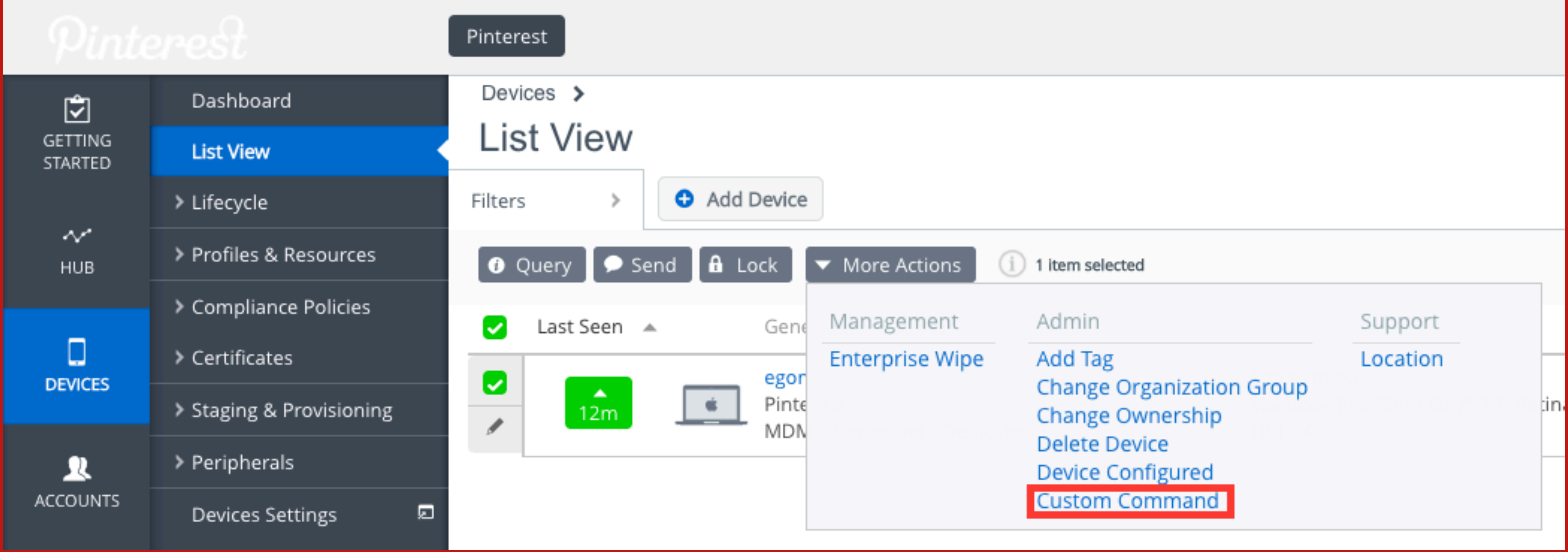
This will be the name of your home folder.

Password: ●●●●●●●●●●●●● ●●●●●●●●●●●●●

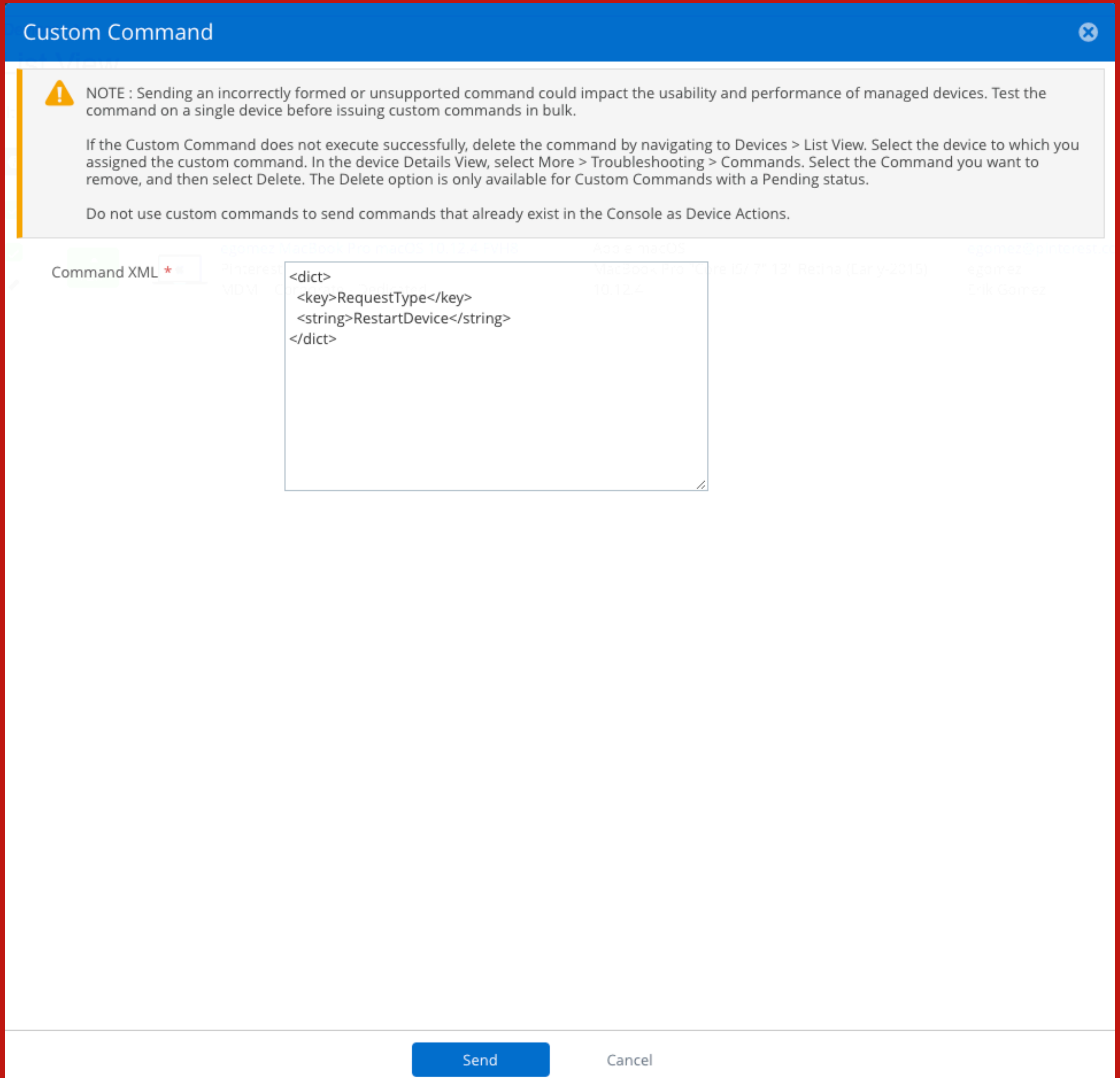
Hint: optional

☑ Set time zone based on current location

With AirWatch 9.1, you can send arbitrary mdmclient commands through the GUI.



With AirWatch 9.1, you can send arbitrary mdmclient commands through the GUI.



NOTE : Sending an incorrectly formed or unsupported command could impact the usability and performance of managed devices. Test the command on a single device before issuing custom commands in bulk.

If the Custom Command does not execute successfully, delete the command by navigating to Devices > List View. Select the device to which you assigned the custom command. In the device Details View, select More > Troubleshooting > Commands. Select the Command you want to remove, and then select Delete. The Delete option is only available for Custom Commands with a Pending status.

Do not use custom commands to send commands that already exist in the Console as Device Actions.

Command XML *

```
<dict>
  <key>RequestType</key>
  <string>RestartDevice</string>
</dict>
```

With AirWatch 9.1, you can send also arbitrary mdmclient commands through the *API*.

https://github.com/erikng/mdmscripts

```
python ./aw_api_installapplication.py \
--authorization 'dXNlcm5hbWU6cGFzc3dvcmQ=' \
--baseurl 'https://cn.awmdm.com'
--manifesturl 'https://s3.amazonaws.com/appmanifest.plist' \
--tenantcode 'YWlyd2F0Y2h0ZW5hbnRjb2Rl' \
--machineserial "CXXXXXXXX"
```

AppManifest.plist

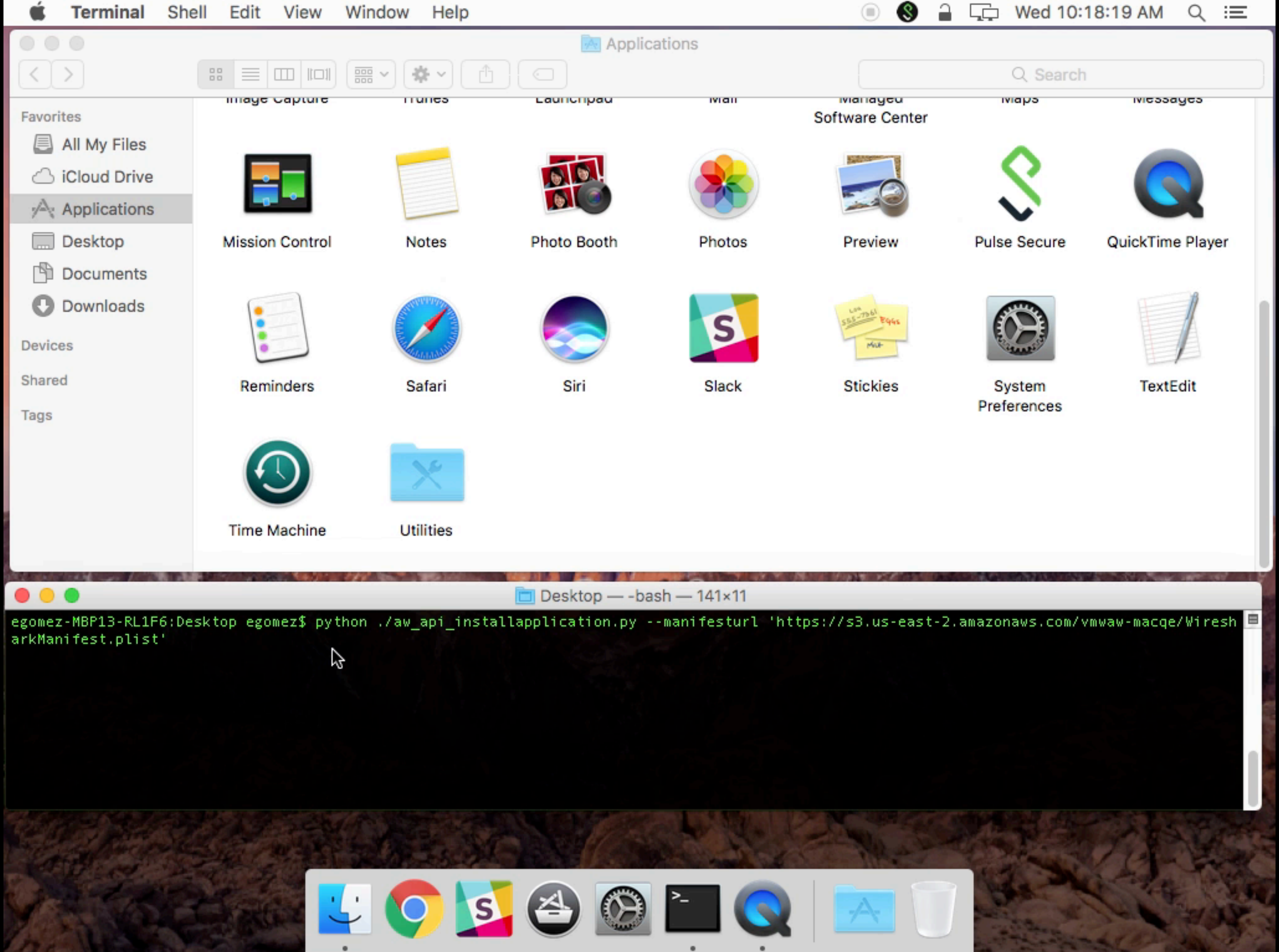
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>items</key>
    <array>
      <dict>
        <key>assets</key>
        <array>
          <dict>
            <key>kind</key>
            <string>software-package</string>
            <key>md5-size</key>
            <integer>10485760</integer>
            <key>md5s</key>
            <array>
              <string>2e4ad4a42e2466cf0747fae916cb0b93</string>
              <string>8b03be431ea627c1ed3462decc8c80d1</string>
              <string>a40c97bb6acf0a0e45cc45ae22b207b2</string>
              <string>0d43b6f06b281860a2988e689b7b342b</string>
            </array>
            <key>url</key>
            <string>https://s3.us-west-2.amazonaws.com/nope/Wireshark.pkg</string>
          </dict>
        </array>
      </dict>
    </array>
  </dict>
</plist>
```

MicroMDM's appmanifest

Tool to easily make a manifest.plist for use with InstallApplication

```
./appmanifest /path/to/pkg > ./appmanifest.plist
```

https://github.com/micromdm/tools/releases



```
egomez-MBP13-RL1F6:Desktop egomez$ python ./aw_api_installapplication.py --manifesturl 'https://s3.us-east-2.amazonaws.com/vmwaw-macqe/Wiresh
arkManifest.plist'
```

MDM Availability

Tool	Basic MDM	Custom InstallApplication	Custom DEP
AirWatch	✓	✓ v9.1+	✓ Coming soon!
Fleetsmith	-	-	-
jamf Pro	✓	-	-
MicroMDM	✓	✓	✓
Microsoft Intune	✓	-	-
MobileIron	✓	-	-
Meraki Systems Manager	✓	-	-
Simple MDM	✓	✓	✓

Greater control of MDM benefits everyone.

- Apple
  - Gets feedback regarding `mdmclient` that they desperately need
  - Radars / Feature Enhancements
- Customers
  - Full control of DEP
  - Ability to interact directly with MDM commands vs vendor agents
- Vendors
  - **You still get paid!**
  - Support customers who want more control over their deployments

Hello MDM vendors,

Greater control of MDM benefits everyone. Please support these features.

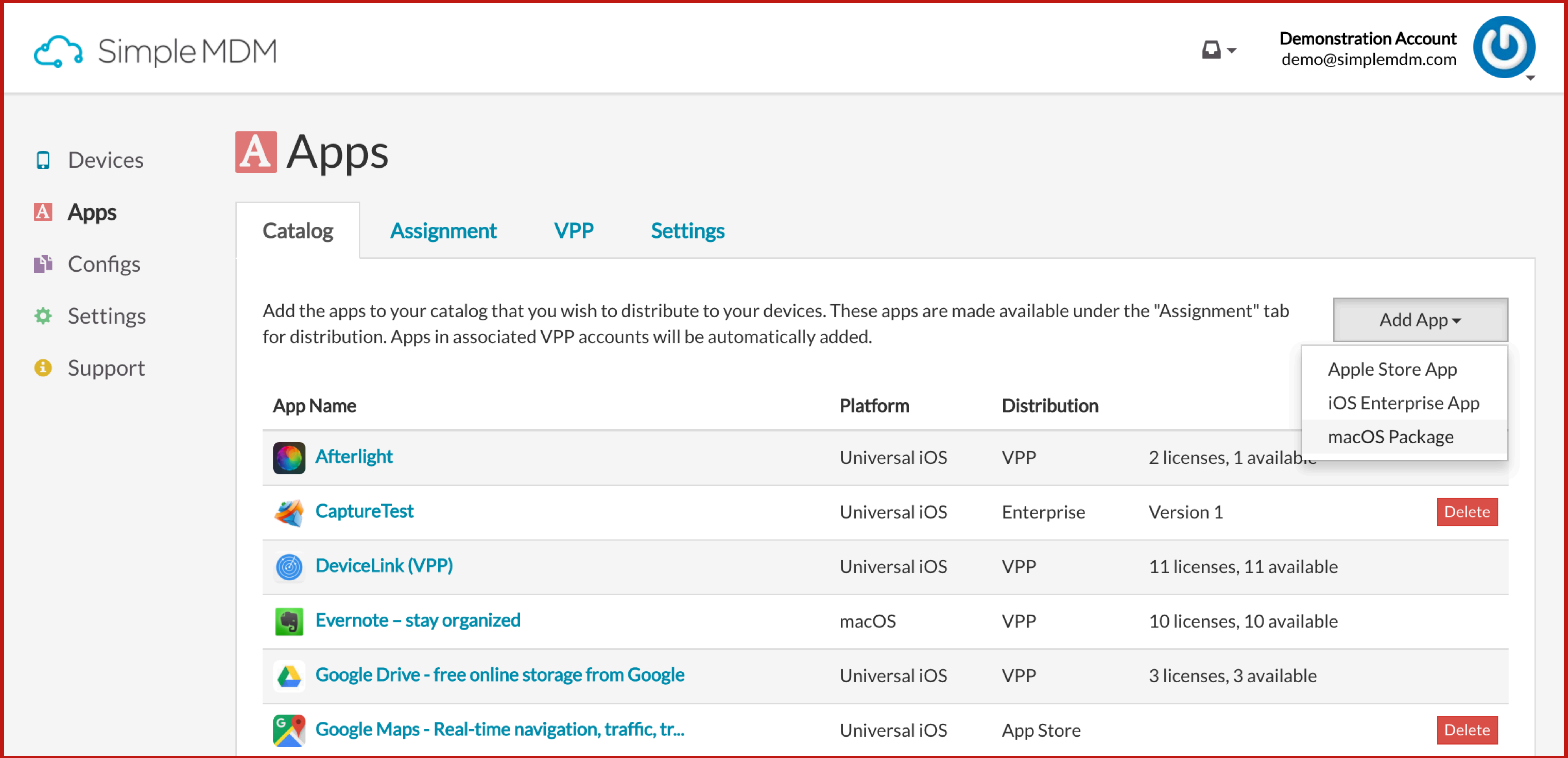
Sincerely, your paying customers

Thank you, AirWatch!

Honorable mentions:

- Centrify
  - New Mac App Management (v17.4) powered by munki/autopkg
- MicroMDM - Not production ready, but getting very close
  - Deepest admin control of any MDM
  - Robust API to interact with mdmclient
  - macOS focus, but can work with iOS
- SimpleMDM
  - UI for custom packages using InstallApplication
  - API for adding multiple packages

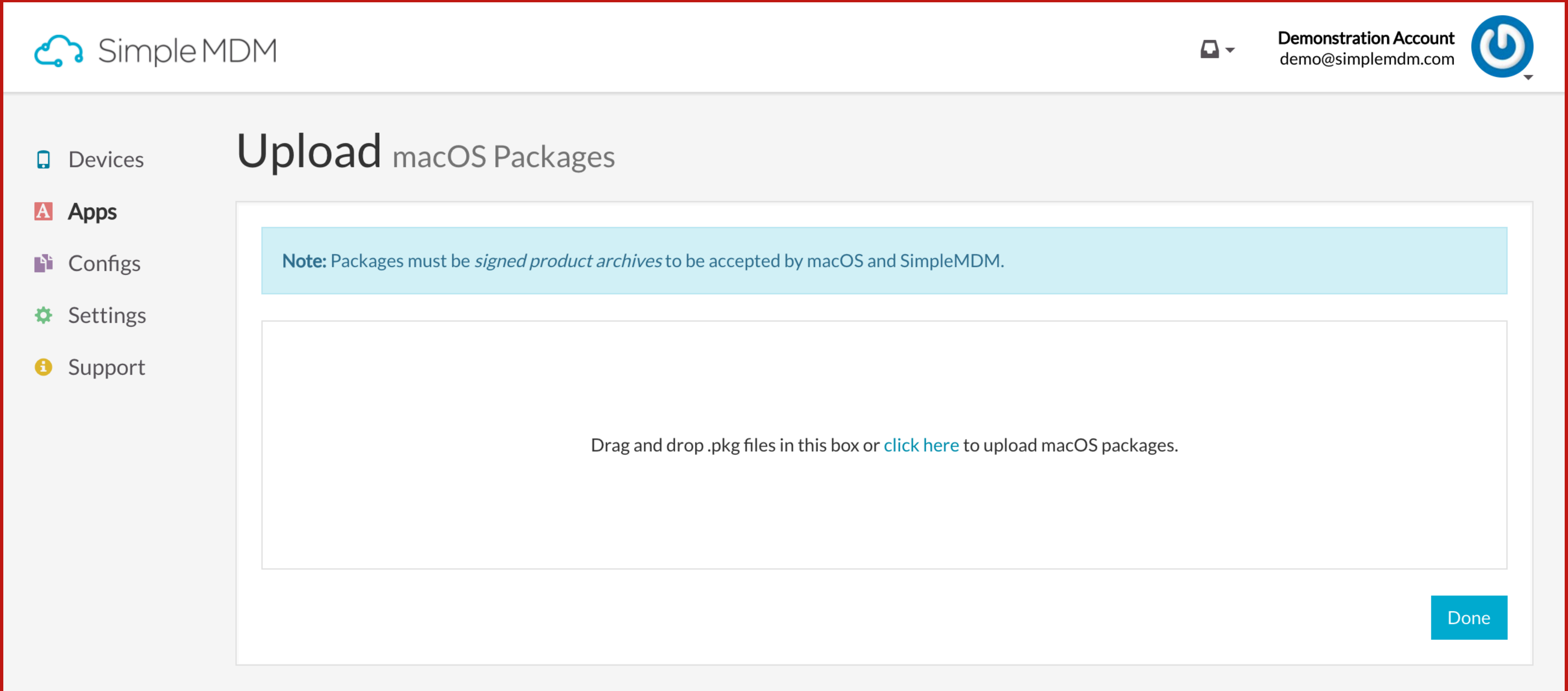
SimpleMDM Custom Package



Add the apps to your catalog that you wish to distribute to your devices. These apps are made available under the "Assignment" tab for distribution. Apps in associated VPP accounts will be automatically added.

App Name	Platform	Distribution		
Afterlight	Universal iOS	VPP	2 licenses, 1 availab	
CaptureTest	Universal iOS	Enterprise	Version 1	Delete
DeviceLink (VPP)	Universal iOS	VPP	11 licenses, 11 available	
Evernote – stay organized	macOS	VPP	10 licenses, 10 available	
Google Drive - free online storage from Google	Universal iOS	VPP	3 licenses, 3 available	
Google Maps - Real-time navigation, traffic, tr...	Universal iOS	App Store		Delete

SimpleMDM Custom Package



Upload macOS Packages

Note: Packages must be *signed product archives* to be accepted by macOS and SimpleMDM.

Drag and drop .pkg files in this box or click here to upload macOS packages.

Zentral

Event Stream processing and alerting

Pinterest

We're hiring...

😄

Client Platform Engineer

goo.gl/gEWQ5C

Corporate Security Engineer

goo.gl/pg1Dpb

Two more things…

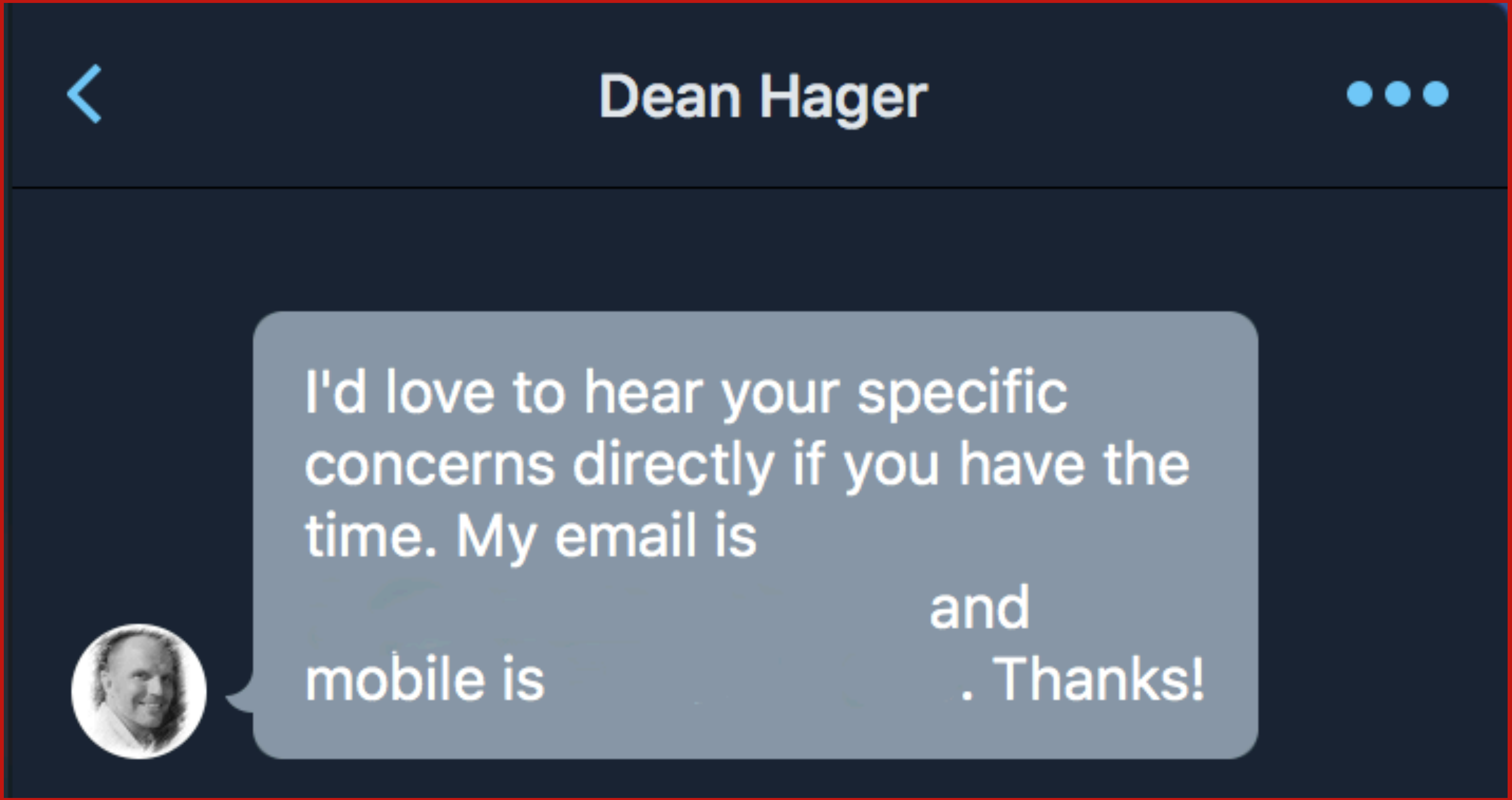
AirWatch is **here**!

No marketing speeches, no sales numbers

Just some passionate engineers.

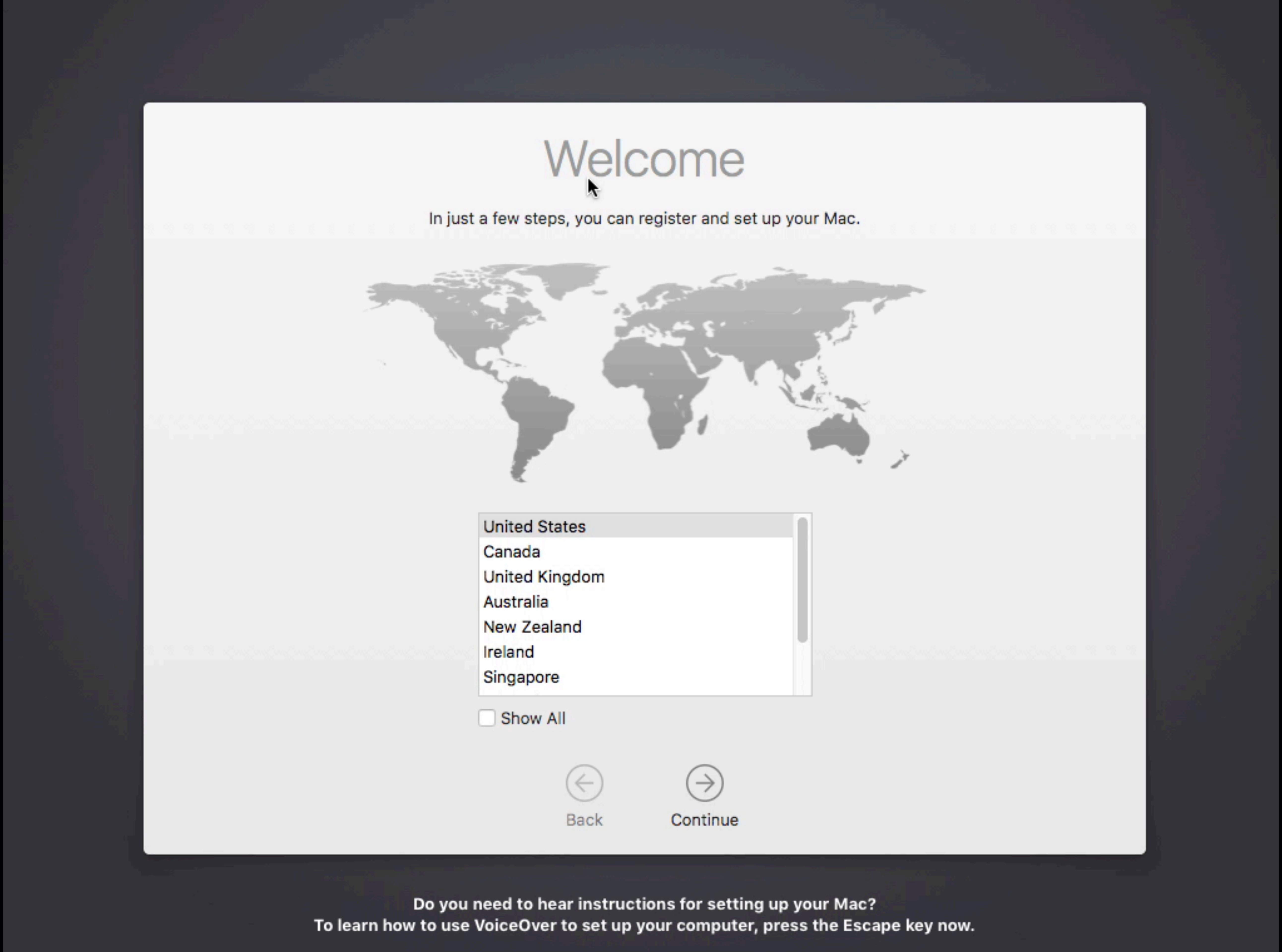
Find them and ask some questions.

Dean and Jamf are good people.



I'd love to hear your specific concerns directly if you have the time. My email is [redacted] and mobile is [redacted]. Thanks!

Q & A



Welcome

In just a few steps, you can register and set up your Mac.

United States
Canada
United Kingdom
Australia
New Zealand
Ireland
Singapore

☐ Show All

Do you need to hear instructions for setting up your Mac?
To learn how to use VoiceOver to set up your computer, press the Escape key now.