



From Imaging to Installation in 1 Semester

Dylan McKenna and James Chiaramonte





`https://github.com/mckmatter/MacAdmins.git`

`$ cd ~/Desktop/`

`$ git clone https://github.com/mckmatter/macadmins.git`



Our Deployment

- Total Enrollment: ~5,000
- Faculty: ~450
- iMac: 138
- MacBook: 83
- Other macOS: 9
- iOS: 74



Where we were

Deploy Studio
Munki
Xserve



Where we are now

jamf | PRO

- On Premise - 10.12
- 2 Servers
 - RedDelicious can be reached from the internet
 - GoldenDelicious can be reached only from internal networks and contains the database
- Admin UI can be reached from internal networks - access control via F5 iRule

Provisioning macOS



Manage your institution's devices, apps,
and accounts.

Apple ID



☐ Remember me

Forgot Managed Apple ID or password?

Not yet an Apple School? [Enroll now.](#)

1. Choose Devices

☒ Serial Number ☐ Order Number ☐ Upload CSV File

Serial Numbers

aserialnumber

2. Choose Action

Perform Action

Assign to Server



MDM Server

Jamf Pro



PreStage Enrollments

NAME	LAST SYNC
Apple DEP Employees	06/05/2019 at 3:56 PM
Apple DEP Kiosks	06/05/2019 at 3:56 PM
Apple DEP Lab Machines	06/05/2019 at 3:56 PM




Installing macOS

- Internet Recovery
 - Command + Option + R -> Latest macOS
 - Used to get existing machines from HFS+ to APFS
- `startosinstall -eraseinstall`
 - Good for Remotely Re-Provisioning a Mac
 - Erase Install only works if the Disk is already on APFS
- `createosinstall --volume --applicationpath`
 - Good for one-off machines

Apple DEP Lab Machines

Options Scope

 General >

 Account Settings

 Configuration Profiles
0 Profiles

 User and Location

 Purchasing

 Attachments
0 Attachments

 Certificates

Setup Assistant Options Selected items are not displayed in the Setup Assistant during enrollment

None

- ☒ Location Services
- ☒ Transfer Information
- ☒ Apple ID
- ☒ Terms and Conditions
- ☒ Siri
- ☒ App Analytics
- ☒ Touch ID / Face ID
- ☒ Apple Pay

Select Language

Select Country

Allow Remote Management

Select Timezone

Done

History

Clone

Delete

Edit



Policies @ Enrollment

- Policies set to run @_Enrollment
- Scoped to Smart Groups based on PreStage Enrollment

06 Sophos

Options

Scope

Self Service

User Interaction



General



Packages

1 Package

General

DISPLAY NAME Display name for the policy

06 Sophos



Enabled

CATEGORY Category to add the policy to

@_Enrollment



Trigger Event(s) to use to initiate the policy

06 Sophos

Options

Scope

Self Service

User Interaction

☐ Show in Jamf Pro Dashboard

Targets	Limitations	Exclusions
---------	-------------	------------

TARGET COMPUTERS

Computers to deploy the policy to

Specific Computers

▼

TARGET USERS

Users to deploy the policy to

Specific Users

▼

TARGET	TYPE
Basic Enrollment with AD Binding	Smart Computer Group
First Run EMPLOYEE	Smart Computer Group
First Run KIOSKS	Smart Computer Group
First Run LABS	Smart Computer Group

















FirstRun Smart Groups

- Machines Fall into a 'FirstRun' Smart Group based on their PreStage Enrollment
- They leave the FirstRun smart group once the last @_Enrollment Policy executes
- Two Purposes
 - If enrollment doesn't go well, you can use `jamf enroll` and the software packages will not be re-installed
 - Smart Group email notifications as a machine enrolls

Policies

 @_Enrollment

	 01 Please Wait	Ongoing	Enrollment	3 computer groups
	 05 SplashBuddyBASE	Ongoing	Enrollment	First Run EMPLOYEE
	 06 Sophos	Ongoing	Enrollment	4 computer groups
	 09 Set Computer Name	Ongoing	Enrollment	Basic Enrollment with AD Binding
	 10 EnrollmentScripts	Ongoing	Enrollment, enrollscripts	3 computer groups
	 12 AdobeFlashPlayer	Ongoing	Enrollment	2 computer groups
	 13 AdobeReader	Ongoing	Enrollment	2 computer groups

Apple DEP Lab Machines

Options

Scope



General



Account Settings >



Configuration Profiles

0 Profiles



User and Location



Purchasing



Attachments

0 Attachments



Certificates

Account Settings

Management Account

Local administrator account to use for managing computers enrolled via user-initiated enrollment

ACCOUNT USERNAME

jssadmin



Create an additional local administrator account

Additional local administrator account to create for computers enrolled via user-initiated enrollment

USERNAME

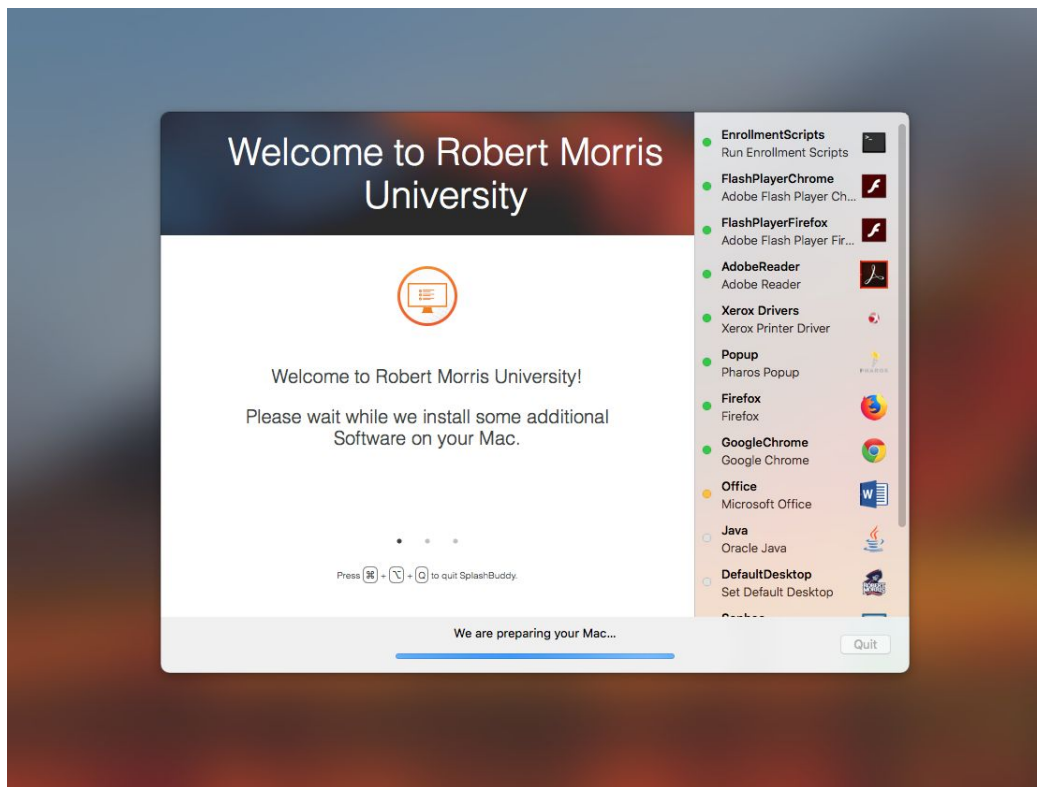
admin

PASSWORD

.....

VERIFY PASSWORD

.....



<https://github.com/Shufflepuck/SplashBuddy.git>

`tail -f /var/log/jamf.log`



setComputerName.sh

BLD-100-M01

```
jamf setComputerName -fromFile /tmp/labNames.csv
```

```
if [ "$MODEL" == "MacBookPro" ];
```

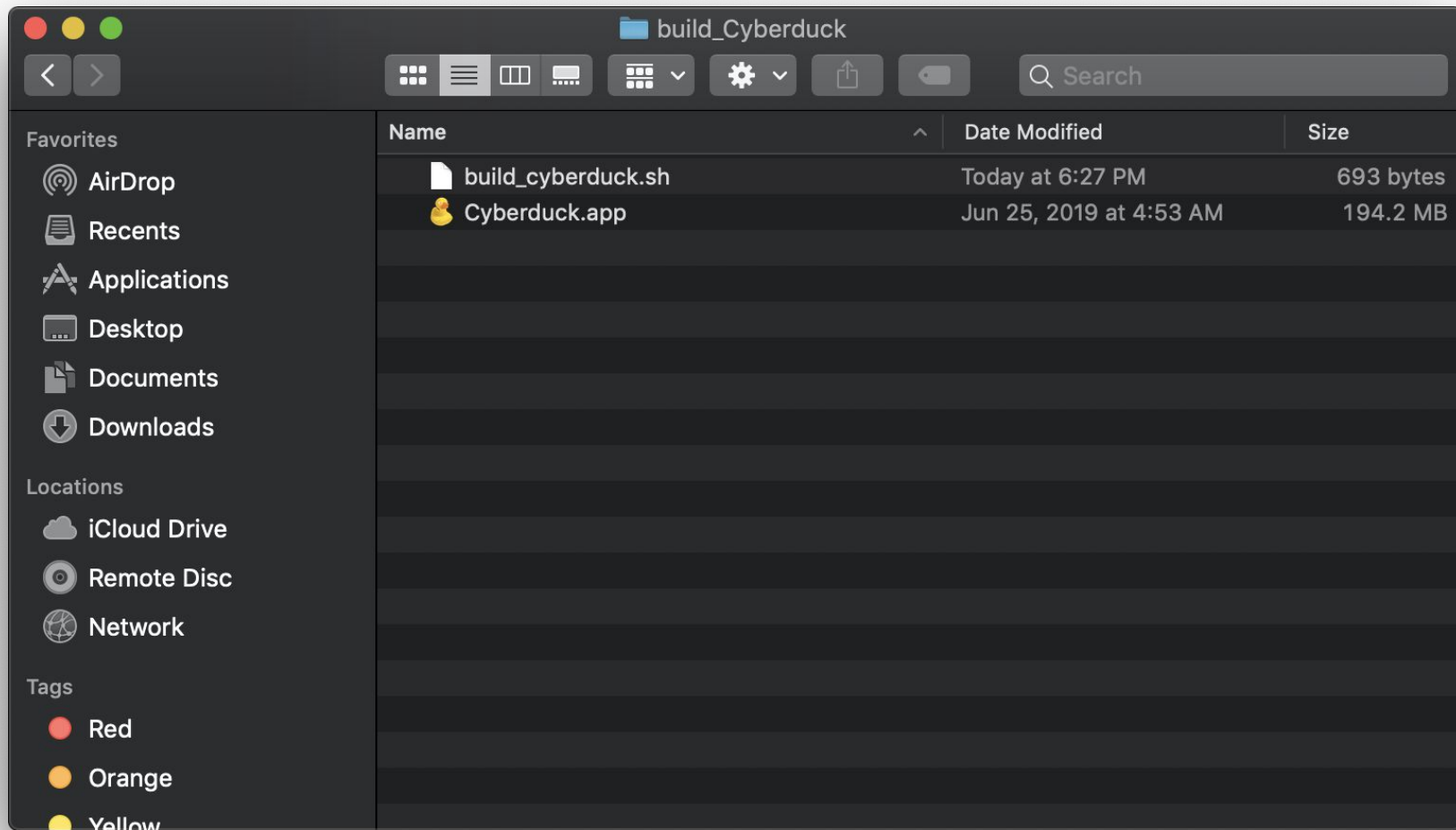
```
    then
```

```
        NAME="MBP"$SERIAL
```



Packaging .app

- Some Apps come off the internet in the form of DMG's
- Other come just as zipped up .app files
- Scripts for .app
- AutoPkg where Recipes Exist



build_cyberduck.shUNREGISTERED

setComputerName.sh xbuild_cyberduck.sh x

```
1  #!/bin/bash
2
3  # Path relative to this script
4  PATH=`pwd`
5
6  # Bundle identifier to use for Cyberduck
7  BUNDLE_ID="edu.abc.cyberduck.pkg"
8
9  # Location of vmware application, assuming default location
10 APP="Cyberduck.app"
11
12 # The version number of the app
13 VERSION="7.0.1"
14
15 # What to call the installer package
16 INSTALLER_PKG="cyberduck_${VERSION}.pkg"
17
18 # Developer ID must be provided or package creation will fail since it cannot be signed
19 DEVELOPER_ID="Developer ID Installer: Your Name"
20
21 # Package the UTC Installer
22 /usr/bin/pkgbuild --sign "${DEVELOPER_ID}" \
23   --install-location "/Applications" \
24   --identifier "${BUNDLE_ID}" \
25   --component "${APP}" \
26   --quiet \
27   "${PATH}/${INSTALLER_PKG}"
28
29
30
31
```

Line 16, Column 41

master 1921

Tab Size: 4

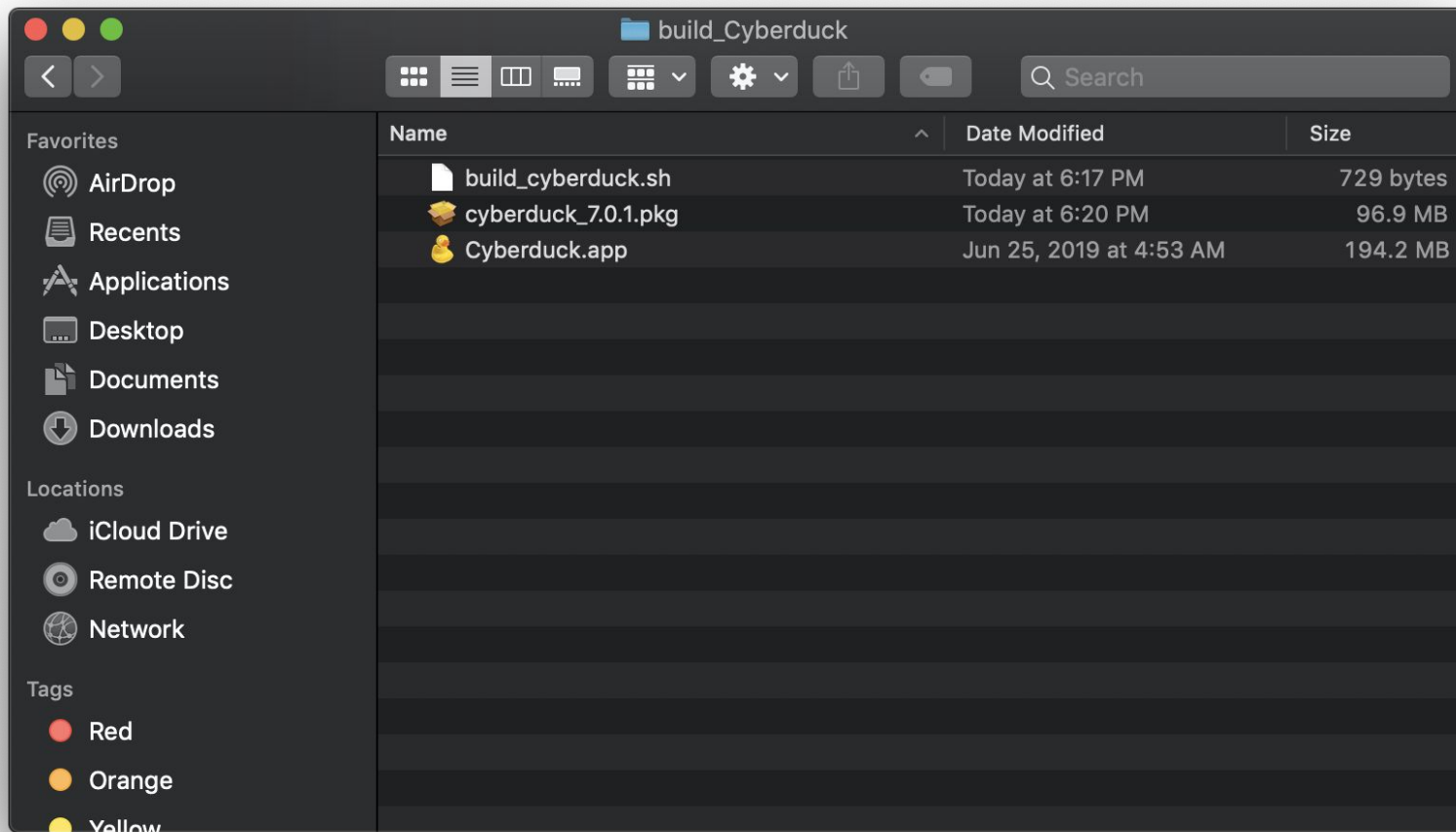
Bourne Again Shell (bash)



```
cd build_Cyberduck/
```

```
chmod +x build_cyberduck.sh
```

```
:build_Cyberduck username$ ./build_cyberduck.sh
```



To Bind or Not To Bind

- We Bind
 - SSO Type Experience in Labs
 - DFS Namespace Mapping to User Account in Labs
 - Set Search Domains on the network adapter
 - AD does not lock accounts



Lab Configuration Profiles

- Lab Configuration Profiles have the following Payloads
 - Network - Cisco ISE Integration
 - Certificate
 - Restrictions - Disables App Installation
 - Login Window - Disclaimer on Login Window
 - Mobility - Delete User Profile as Soon As Possible



Lab Configuration Profiles (cont.)

- Lab Configuration Profiles have the following Payloads
 - Security and Privacy - Enables the Firewall
 - Energy Saver - Schedules a Startup Time
 - Custom Settings - `askForSecureTokenAuthBypass=true`
 - Finder - Enables Desktop Icons for drives
 - Approved Kernel Extensions - Avid ProTools



Provisioning Rogue Devices

- Devices not purchased from our Apple Representative can't be claimed in School Manager or assigned a PreStage Enrollment
- Visit jamfinstance.com/enroll
- Create a Smart Computer Group based on Serial Number

Basic Enrollment with AD Binding

Computer Group		Criteria	
AND/OR		CRITERIA	OPERATOR
		Serial Number	is
or		Serial Number	is



Identity Services Engine

Username

Password

Identity Source

Internal



Login

[Problem logging in?](#)



Cisco ISE

- Puts a machine on a transient network for 15 seconds before MAC Address Bypass
 - Prevents Internet Recovery from working
- Temporarily change the switchport access vlan from the transient vlan to the proper vlan



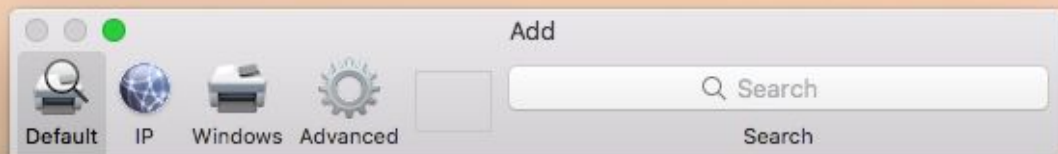
Adobe Shared Device Licensing

- Volume License Packages no longer exist
- Use Adobe Provided Python Scripts to sync AD groups with Adobe
- Students Sign In to all Adobe Creative Cloud Products with our SSO



Printing with MacOS

- Pharos Popup and Xerox/HP Drivers deployed @_Enrollment
- Jamf Policies that add Printers have custom PPD Files
- Labs get Lab Printers based on Smart Group
- Employees can add printers via Self Service
- Create Disk Images with the Popup and a custom PPD for BYOD Macs



Drag your favorite items into the toolbar...



Windows



IP



Default



Advanced



Search



Space



Flexible Space

... or drag the default set into the toolbar.



Default



IP



Windows



Search

Search

Show

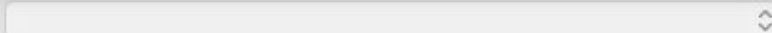
Icon and Text



Use small size

Done

Use:



Add



KEXT Policy Identification

- Some Applications (Sophos) require KEXT Policies to run properly
- Identify these policies ahead of time by allowing them on your test machine
- Look up the Identifiers in the Kext Policy sqlite3 Table



KEXT Policy Identification

```
cd /var/db/SystemPolicyConfiguration/
```

```
sudo sqlite3 KextPolicy
```

```
SELECT * FROM kext_policy;
```

```
73YQY62QM3|com.displaylink.driver.DisplayLinkDriver|1|Display  
Link Corp|1
```

Lab Machines

Options

Scope



Mobility

1 Payload Configured



Security & Privacy

1 Payload Configured



Energy Saver

1 Payload Configured



Custom Settings

1 Payload Configured



Finder

1 Payload Configured



Approved Kernel Extensions >

1 Payload Configured

Approved Team IDs and Kernel Extensions



Approved Team ID

DISPLAY NAME

Avid Pro Tools

TEAM ID

4UYUA773XD

Approved Kernel Extensions (Optional) Approve the following bundle IDs only

DISPLAY NAME

KERNEL EXTENSION B...

MBoxPro Driver

com.avid.driver.firewire.
mboxpro

AvidHDDriver

com.digidesign.iokit.Di
giDal

iOS Provisioning



Restore iOS

- Claim in Apple School Manager
- Assign a PreStage Enrollment
- Get the device into Restore Mode
- Plug into iTunes and reinstall iOS

PreStage Enrollments

+ New

NAME	LAST SYNC
EAB Kiosk iPad DEP Enrollment	06/05/2019 at 3:56 PM
Employee iPad DEP Enrollment	06/05/2019 at 3:56 PM
Employee iPhone DEP Enrollment	06/05/2019 at 3:56 PM
Facilities iPad DEP Enrollment	06/05/2019 at 3:56 PM
SESS iPad DEP Enrollment	06/05/2019 at 3:56 PM
SNHS RISE Simulation iPhone DEP Enrollment	06/05/2019 at 3:56 PM
Square iPad DEP Enrollment	06/05/2019 at 3:56 PM
Test iPad DEP Enrollment	06/05/2019 at 3:56 PM
Titanium Counseling Center iPad DEP Enrollment	06/05/2019 at 3:56 PM
UEC iPad DEP Enrollment	06/05/2019 at 3:56 PM

Mobile Device Apps

<div><div>▼</div><div>Filter Re</div><div>1 - 33 of 33</div><div>+ New</div></div>							
NAME	VERSION	SOURCE	VPP TYPE	TOTAL PURCHASED	IN USE	REMAINING	SCOPE
<div><div>▼</div>No category assigned</div>							
Adobe Illustrator Draw	4.7.1	App Store	License	50	13	37	SESS iPad
AppInventor2 Tutorials	1.0	App Store	License	20	13	7	SESS iPad
Blue-Bot	1.17	App Store	License	25	13	12	SESS iPad
CellScope - Oto For Clinicians	1.5.9	App Store	License	10	3	7	SNHS RISE Simulation iPhone
Cisco AnyConnect	4.8.00801	App Store	License	200	74	126	All mobile devices

Questions?