iPad Automation

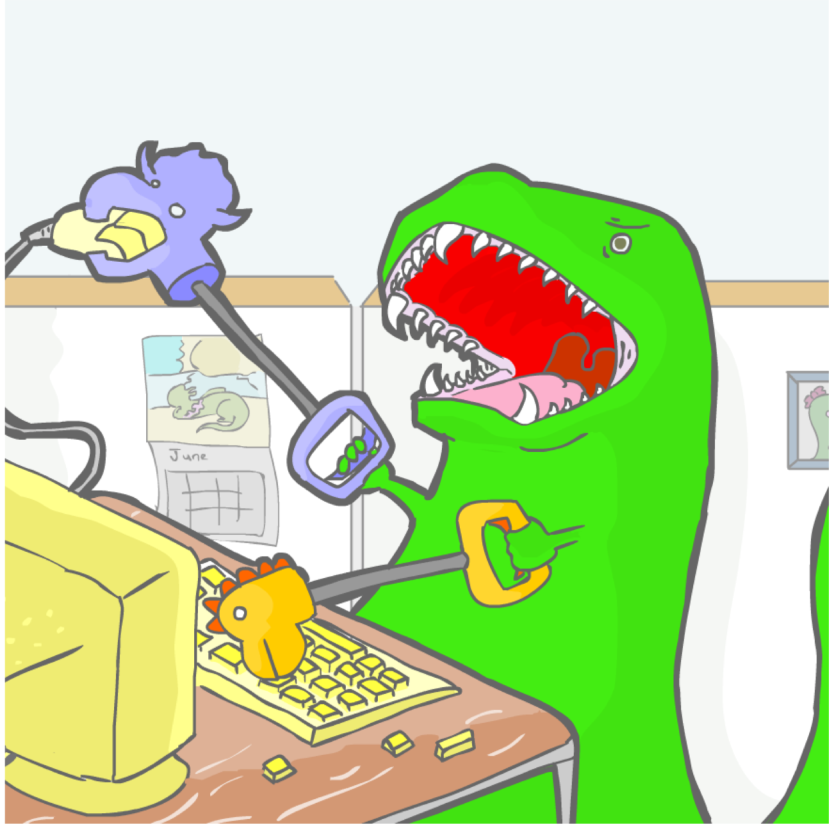
J. Willard Marriott Library
THE UNIVERSITY OF UTAH

ALL U
NEED

About Me

- Sam Forester
- Mac Systems Administrator
  - Tinkering, Scripting, Automation

- Marriott Library, University of Utah
- Contact:
  - Email: sam.forester@utah.edu
  - MacAdmins Slack: @sam



J. Willard Marriott Library
THE UNIVERSITY OF UTAH

ALL U
NEED

Overview

- Our Environment
- Goals/Reasoning
- Workflow
- Available Solutions
- Hardware
- Automation
- Additional Resources

Our Environment

- 3 full-time Mac SysAdmins and student staff
  - Multiple management systems (Radmind + Jamf)
  - ~850 Mac systems (Staff + Labs)
  - Software distribution, security, updates, QA, research, e-tickets, troubleshooting, hardware upgrades, bug-reports, training, long-term projects, and community contribution
- 33,023 Students enrolled (fall 2018)
- Student consultants
- Growing checkout program (we are a library after all!)

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

ALL U NEED

Goals

- Quick Turn-around
- Secure User Data
- Minimal Restrictions
- Minimal Training
- Pre-Installed Apps

Goals – Quick Turn-Around

- Maximum 24 hour checkout (usually 1-5 hours)
- iPads checkouts have been available since start of semester (8/20/18)
  - 12 iPads have been checked out 299 times
  - ~3 checkouts per day on (total average)
  - 1st month only ~20 checkouts
- Manual refresh of device takes ~10-20 minutes

Goals – Securing User Data

- Many-to-one Environment
  - 33,023 students and 12 iPads
- iCloud:
  - Photos, Keychain, and Files (oh my!)
  - Can be accessed by other patrons or staff between checkouts
- Two Options:
  - No iCloud
  - Erase All Content and Settings (every time)
- What about Shared iPad?
  - Only supports maximum of 10 users…

Goals – Minimize Restrictions

- Restrict only the unfixable, unbearable, and malicious:
  - iOS Updates (unfixable)
    - I miss 11.4.1 😢
  - Activation Lock (unbearable)
    - If I have to manually by-pass activation lock one more time… 😡
  - MDM Profile Removal (malicious)
    - I wonder what happens if I remove this… 🤔
- “Let them play!” and figure out how to best facilitate (within reason)

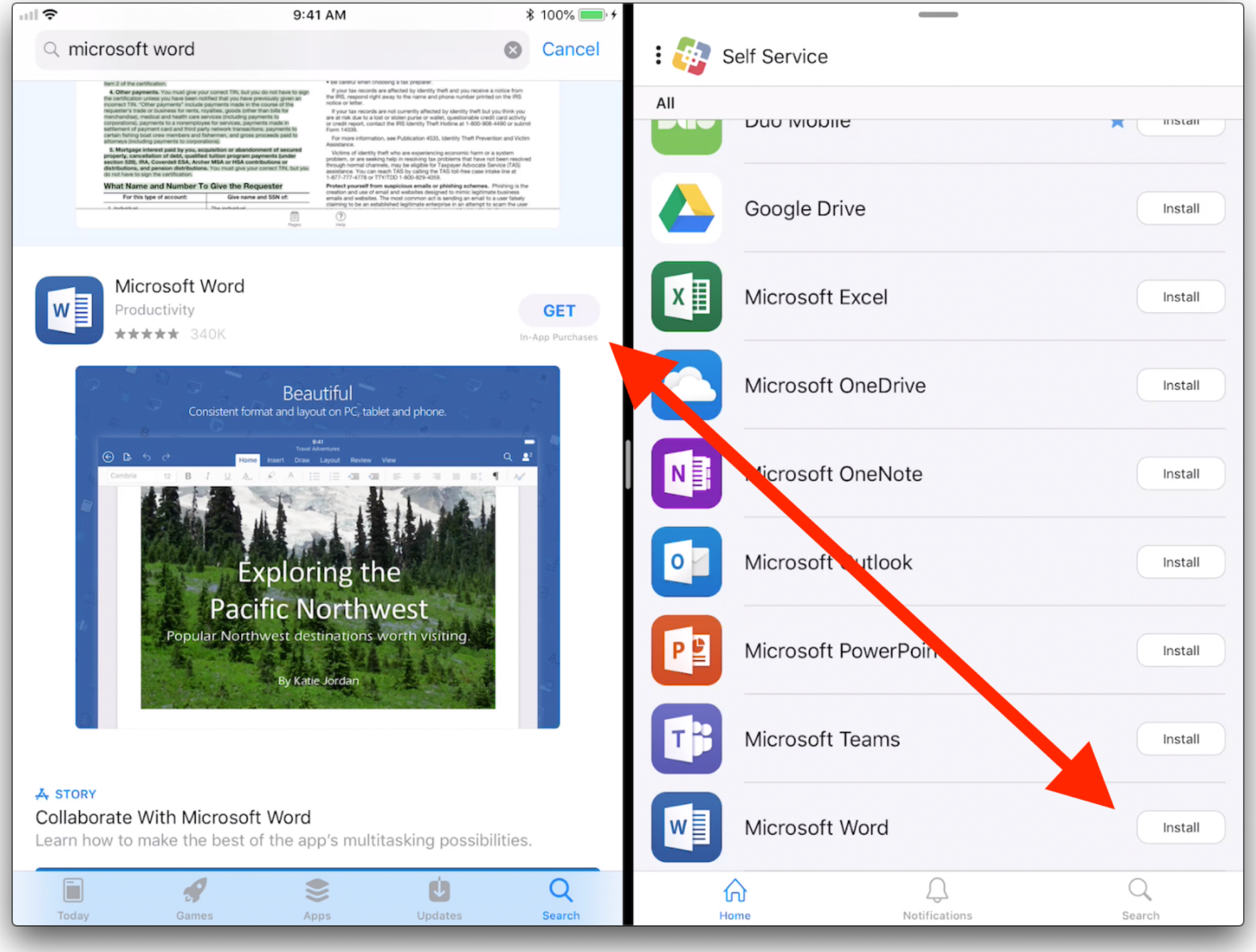
Goals – Minimize Staff Training

- “If you want something done right…” *sigh...
- More “required” user interaction == more work == more time
- Student staff turnover == lots of training

Goals – Pre-Installed Apps

- Self Service vs Automatic Install
  - Users don’t have to search for apps
  - Minimal re-installation of popular apps

- Self Service vs App Store
  - iOS Searches don’t yield Self Service results (App Store)
  - Users tend to default to App Store
  - No mechanism to instruct users that the app is available via Self Service



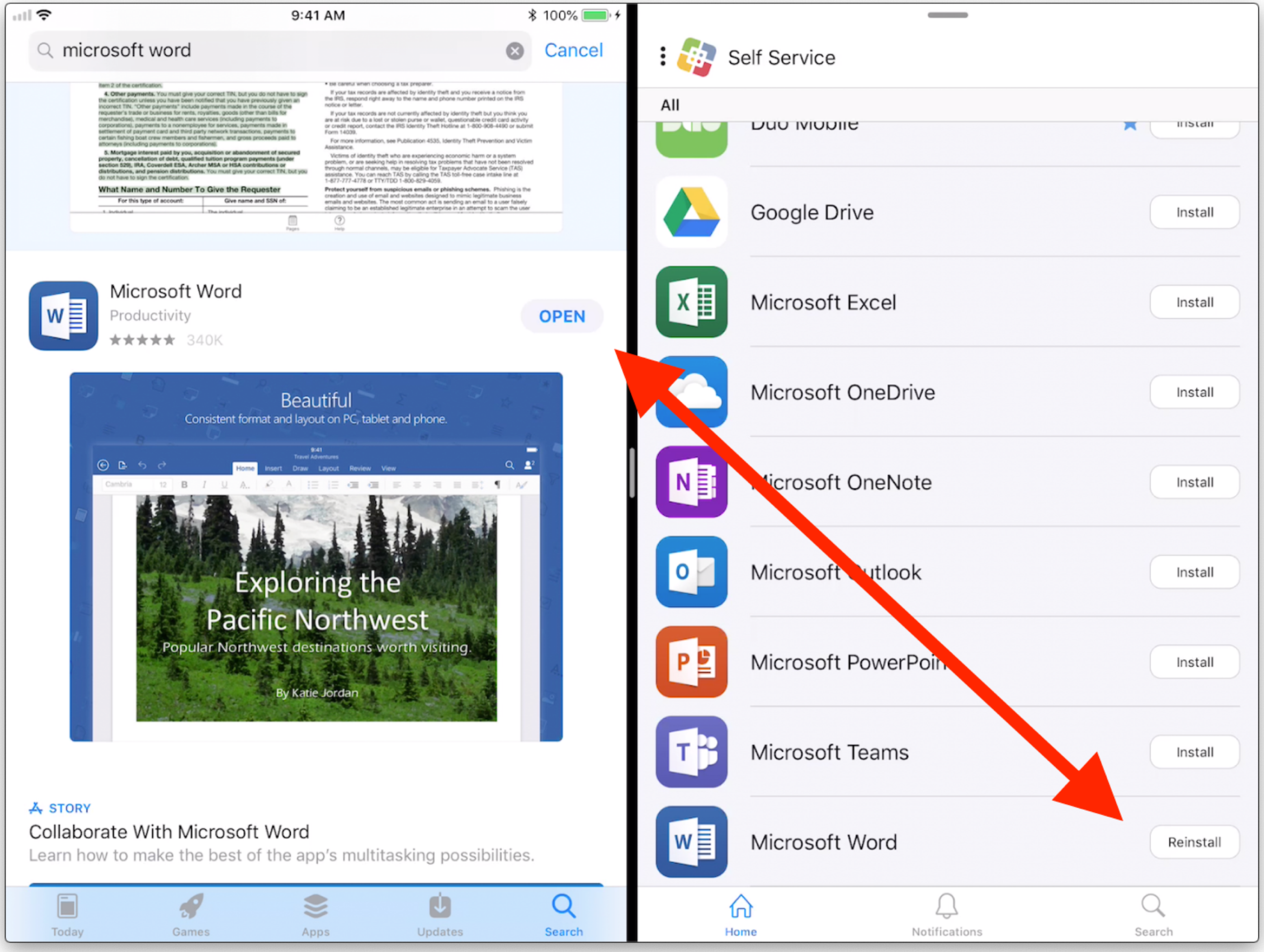
microsoft word

Collaborate With Microsoft Word

Learn how to make the best of the app's multitasking possibilities.

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

ALL U
NEED



9:41 AM 100%

microsoft word Cancel

Microsoft Word
Productivity
★★★★★ 340K
OPEN

Beautiful
Consistent format and layout on PC, tablet and phone.

Exploring the Pacific Northwest
Popular Northwest destinations worth visiting.
By Katie Jordan

STORY
Collaborate With Microsoft Word
Learn how to make the best of the app's multitasking possibilities.

Today Games Apps Updates Search

Self Service

All

Duo Mobile — Install
Google Drive — Install
Microsoft Excel — Install
Microsoft OneDrive — Install
Microsoft OneNote — Install
Microsoft Outlook — Install
Microsoft PowerPoint — Install
Microsoft Teams — Install
Microsoft Word — Reinstall

Home Notifications Search

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

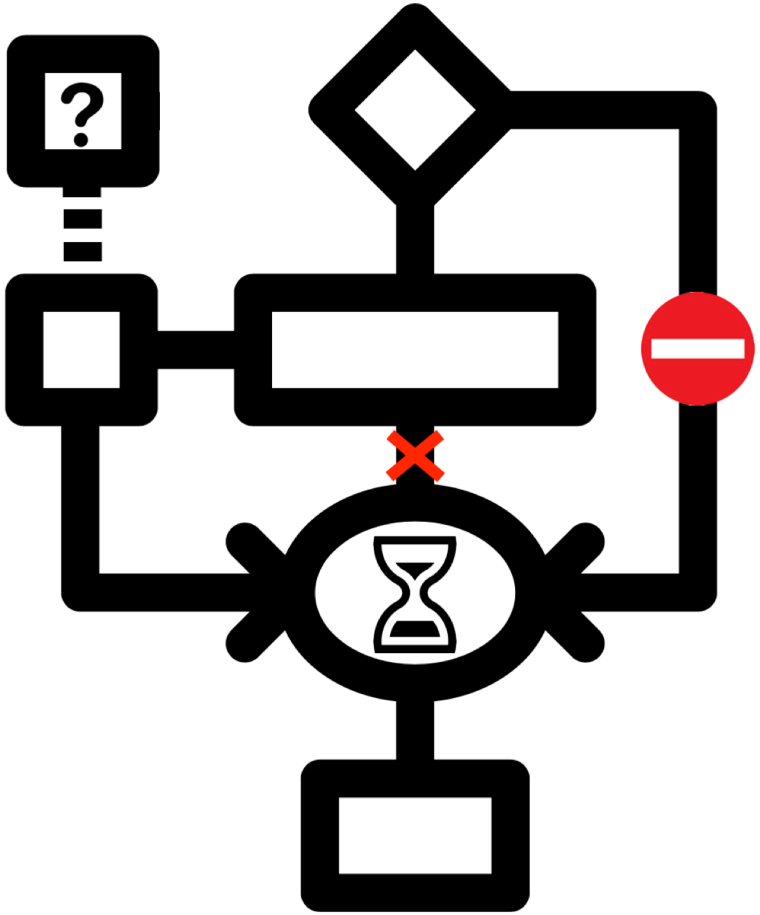
ALL U
NEED

Workflow

- Checkout Erased Device
- DEP Zero-Touch + MDM
- Apps Installed
- Check-In
- Reset Device (Erase All Content and Settings)

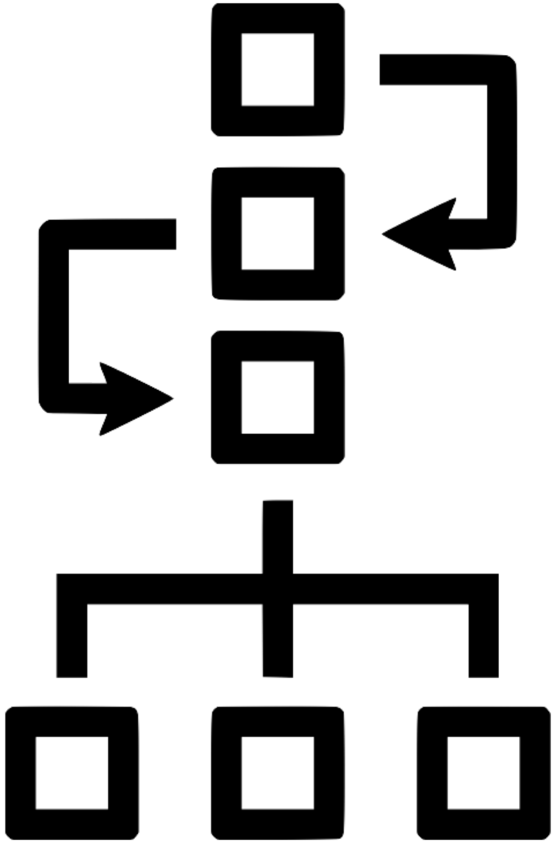
Workflow – Reality

- Checkout Pre-Erased Device
- DEP Zero-Touch == “Minimal Touch”
  - Language + Region
  - Wi-Fi
  - Remote Management
  - … waiting
- Automatic Apps installed via MDM (wireless)
  - … more waiting
  - Wrong Wi-Fi? (Hahahahaha… more waiting)
- Check-In Manually Erase All Content and Settings
  - … hopefully… ¯_(ツ)_/¯
- Rinse and Repeat



Workflow – Ideal

- True Zero-Touch
  - No interaction with device UI
- Check-In:
  - Automatic Erase
  - Automatic App Installation
  - Re-Enroll Device into MDM
- Device is fully prepped and ready for checkout



Challenges

- Assuring user data is erased automatically
  - Easy to solve using `cfgutil` … more on this later
  - Unable to specifically target user data
  - Entire device must be set to default
- Raises additional issues:
  - Re-enrollment
  - Re-installing applications

Additional Challenges

- MDM Re-enrollment
  - DEP to the rescue!
  - Challenges: device requires network to re-enroll via DEP

- Re-install Applications:
  - MDM vs Apple Configurator
  - Challenges: Varies depending on the chosen solution

Various Methods

- History
- MDM + DEP
- Apple Configurator
- Hybrid Solution

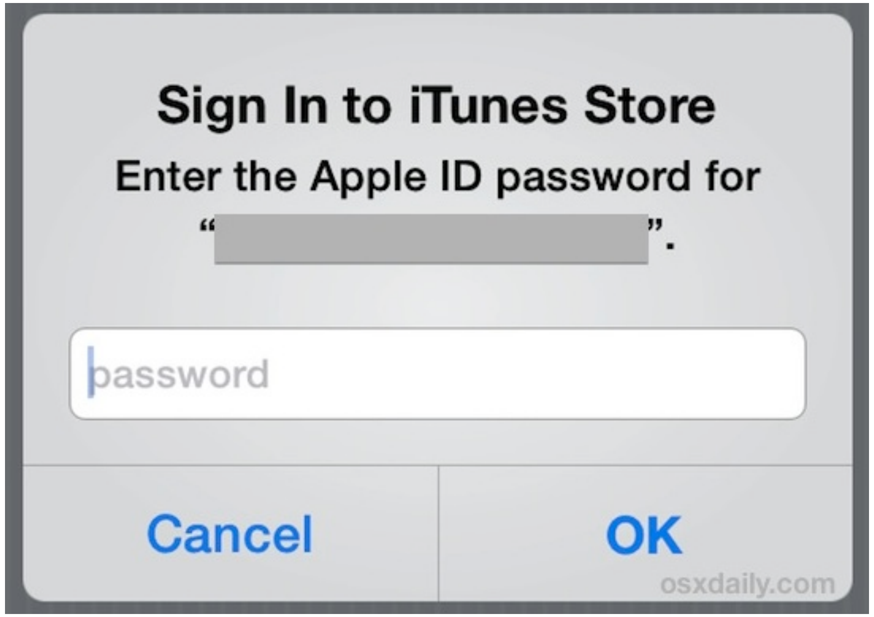
History – Legacy iOS Imaging

- Create a backup for the device (Apps, configuration, etc.)
- Erase the device
- Re-Activate Device
- Use Apple Configurator 1 to restore the backup and apps
- Keep single Apple ID logged into device

Legacy Imaging

- Can still create and restore backups
  - Settings are restored
  - Apps can be distributed via local .IPA files

- Apple ID password required after installation of .IPA files



Sign In to iTunes Store

Enter the Apple ID password for "[redacted]".

Volume Purchase Program (VPP)

- Application distribution
- Device Based Licenses
  - No Apple ID required
  - 1 license per device
- User Based Licenses
  - Apple ID required
  - 1 license per user (any number of devices)
- Can’t be personal Apple ID

MDM + DEP

- Configuration Management
- Highly Suggested
- General Witchcraft and Wizardry
- Caveats:
  - DEP is designed to work with MDM
  - Limits configuration options with Apple Configurator 2

MDM – Jamf Pro

- Perfect for long-term, 1-to-1 iOS management
- Remote management/Active updates
- Pre-installed apps not necessary
  - Few “required” apps can be installed automatically via MDM
  - All other apps available via Self Service
    - Users can install what they need, when/if they need it
    - Intuitive solution (“Think of it as our own little App Store.”)
    - Easy to distribute additional apps or add additional licenses
- Device can be manually reset before being re-assigned
  - DEP takes care of the rest

MDM – Jamf Pro – Caveats

- MDM & iOS Setup Assistant don't mix
  - Automatic app installation doesn't take place until user interacts with device
- "Best Effort" Mechanisms:
  - Attempts to do what it can, when it can, except for when it doesn't, or thinks it did, but didn't really…
  - Requires active device network connection
- Zero-day support for iOS is fuzzy-ish…
- Zero-Touch != Zero-Touch

Apple Configurator

- Apple’s original tool for enterprise iOS support
- Pre-cursor to MDM (deep magic)
  - Automation Tools
  - Additional Resources

Apple Configurator

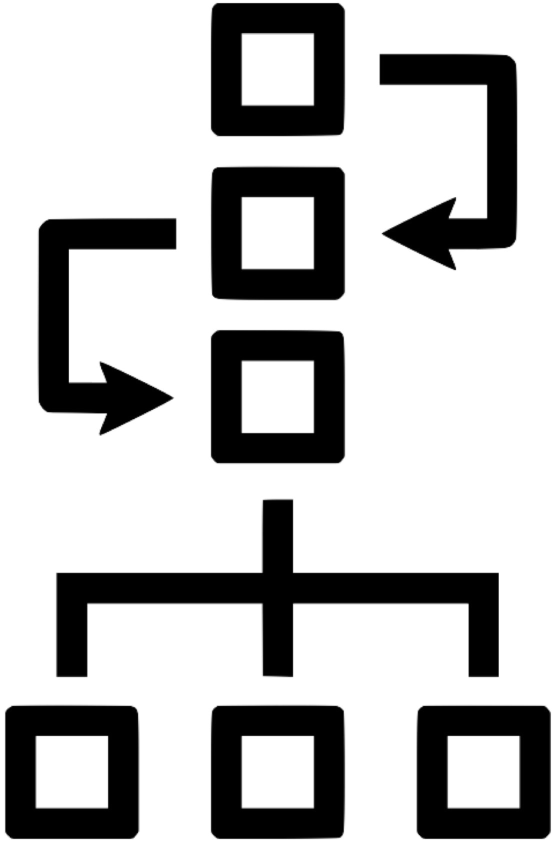
- Actively maintained by Apple
- Provides automation tools
- Works with/without MDM
- Zero-day support for iOS
- Completely bypasses Setup Assistant (allowing MDM to take over)
- VPP App Installation on non-supervised devices
- No device network required, except for Automated Enrollment (DEP)

Apple Configurator – Caveats

- VPP Accounts:
    - VPP accounts cannot be shared between supervising entities
    - One account per station (+MDM)
- No ability to manage devices beyond setup
- UI is contextually frustrating (intuitive, but only in relation to itself)
- Hands-on management
- Configuration profile management gets messy when mixed with MDM
- No automation for VPP app installation

Workflow – Revisited

- Automatic app installation
  - Multiple options
  - Jamf Pro vs Apple Configurator
- Re-enrolling devices into MDM
  - Device network
- Automated erase:
  - Automation tools
  - Under the hood



Application Installation

- Challenges
- MDM vs Apple Configurator
- Demo

Challenges – Applications

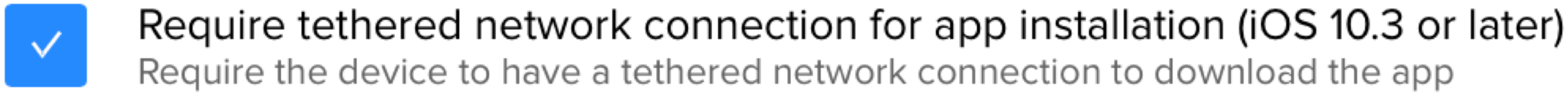
- Multiple Methods for installing Apps
- MDM requires device network
  - Tethered caching can be a bust
- Apple Configurator doesn't have any automated means of installing VPP apps (by default)

Applications – MDM

- Pros:
  - Centralized and remote management
  - App Configuration
  - Hands-off
  - Cached Content (kind of)
- Cons:
  - Prone to Error
  - Eventual (best effort) app installation
  - Requires complete setup assistant
  - Requires device network to function

Applications – MDM – Caveats

- Installation via Tethered Caching vs. Wi-Fi



☑ Require tethered network connection for app installation (iOS 10.3 or later)
Require the device to have a tethered network connection to download the app

- But, if an app fails to install while tethered… it won’t
- Can only be installed **AFTER** Setup Assistant is finished

Applications – Apple Configurator 2

- Pros:
  - No Requirements
  - Scriptable
  - Takes advantage of Cached Content
- Cons:
  - Prone to errors
  - Multiple VPP accounts
  - Decentralized configuration
  - No app configuration

Video Demo

- MDM Auto Install vs Apple Configurator

Challenges – Device Network

- Device network is an absolute requirement for DEP Enrollment
- Two ways to give network to a device:
  - Tethered Caching
  - Wi-Fi Profile

iOS Device Network

- Wi-Fi Profile:
  - tried and true (very stable)
- Tethering:
  - 10.12.4: tethered-caching
    - Network works well, caching doesn't…
  - 10.13 – 10.14: Content Caching
    - Major improvements for App Caching
- Utilities:
  - `ifconfig`
  - `AssetCacheTetheratorUtil`

iOS Device Network – Caveats

- Wi-Fi Profile:
  - Wi-Fi profile are difficult to removed after enrollment
  - Still testing “expiring profiles”

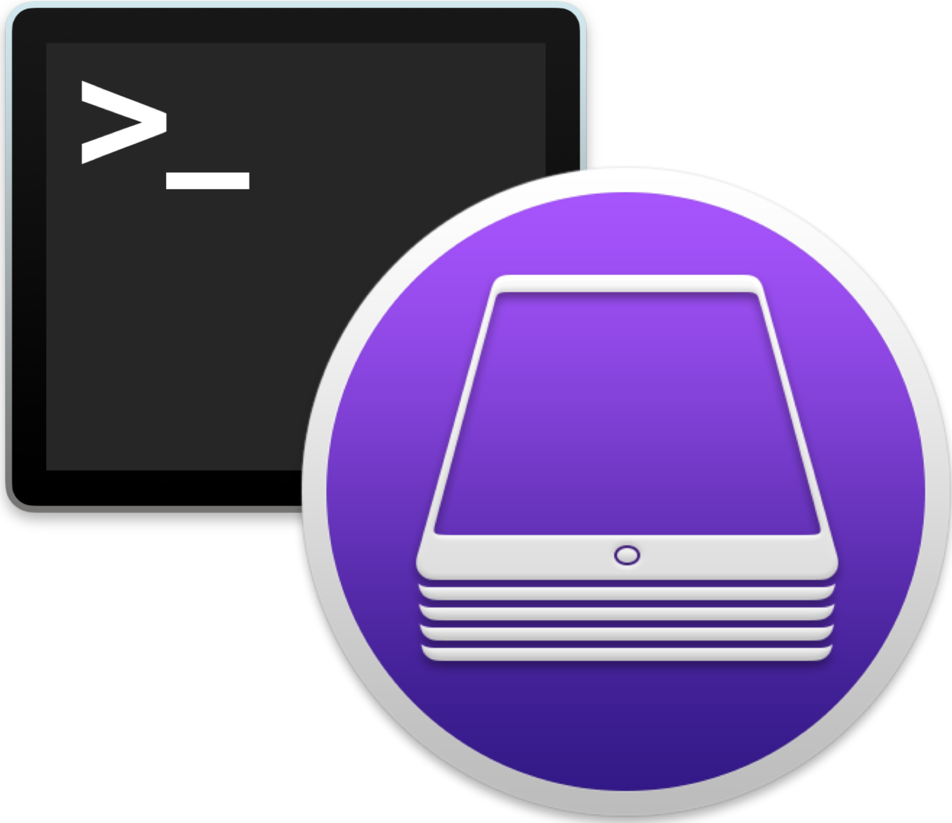
- Tethering:
  - 10.12.4: tethered-caching
    - Breaks sometimes, but can be restarted
  - 10.13 – 10.14: Content Caching
    - Also breaks sometimes, haven’t figured out how to restart it
    - Open ticket with Apple about no network after erase (iOS 12.1)
      - Manually restarting iPad fixes it

iOS Device Network – More Caveats

- Sometimes Devices refuse to utilize tethered connection
- iOS 12.1 refuses to work with tethered connection until device is physically restarted (bug submitted)
- Used to be able to manually remove Wi-Fi profiles after re-enrollment with `cfgutil`
  - doesn’t seem to work anymore…

Apple Configurator 2 – Deeper Look

- Abilities:
  - Install VPP apps
  - Blueprints
  - Configuration Profiles
- Automation tools:
  - Automator Workflows
  - AppleScript Additions
  - `cfgutil`



$ cfgutil

- Command-line tool for iOS devices
- Install Automation tools via Apple Configurator 2
- Sub-commands:
  - erase, restart, set-wallpaper, prepare, exec
- Easy to parse output (JSON)

$ cfgutil exec

```
[presentation:~] sam$ cfgutil help exec
exec
    Usage: exec [-a <path to attach script>] [-d <path to detach script>]
    Run a script when devices attach or detach.
```

- Allows script (or any executable) to be run each time a device attaches/detaches from the system
- Device information set as environment variables
  - ECID, UDID, deviceName, deviceType, buildVersion, firmwareVersion,

```
$ cfgutil prepare
```

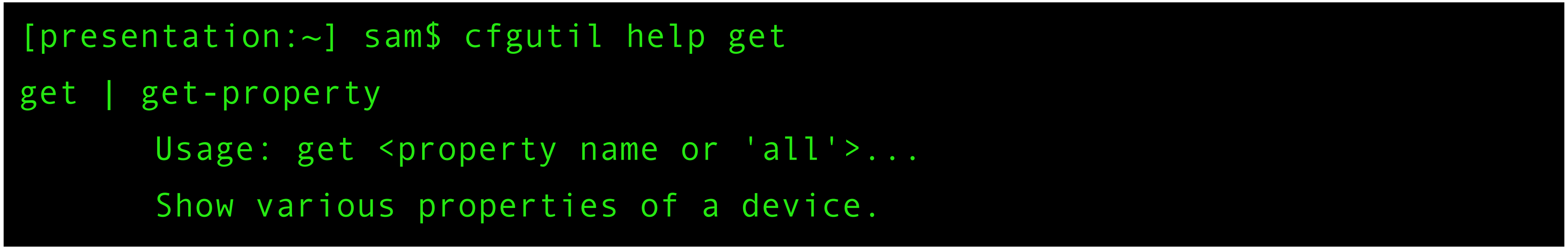
```
$ cfgutil prepare --dep --skip-region --skip-language
```

- Completely by-passes Setup Assistant* and lands on home screen
  - *If MDM is set to “Skip all steps”
- MDM takes over configuration (and can actually perform tasks)
- Caveats:
  - Requires erased device
  - Device requires network connection (tethering or Wi-Fi profile)

```
$ cfgutil prepare
```

- Manual configuration options for non-MDM environments
  - --skip-all, --supervised, --shared-ipad, etc.
- Devices Enrolled in DEP cannot use non-MDM options
  - Warning: DEP without MDM will always fail
    - A device in DEP cannot be modified via manual configuration

$ cfgutil get



```
[presentation:~] sam$ cfgutil help get
get | get-property
        Usage: get <property name or 'all'>...
        Show various properties of a device.
```

- Provides various information about the specified device
- Useful for determining automation actions or verifying completion

```
$ cfgutil get
```

- Storage:
  - totalDiskCapacity, totalSpaceAvailable, freeDiskSpace
  - appDiskUsage, audioDiskUsage, logsDiskUsage, otherDiskUsage, photosDiskUsage, videoDiskUsage, documentsDiskUsage, booksDiskUsage
- State:
  - installedApps, isSupervised, passcodeProtected, configurationProfiles, batteryCurrentCapacity, batteryIsCharging, name
- Misc:
  - serialNumber, tags, passcodeProtected, installedApps, cloudBackupsAreEnabled

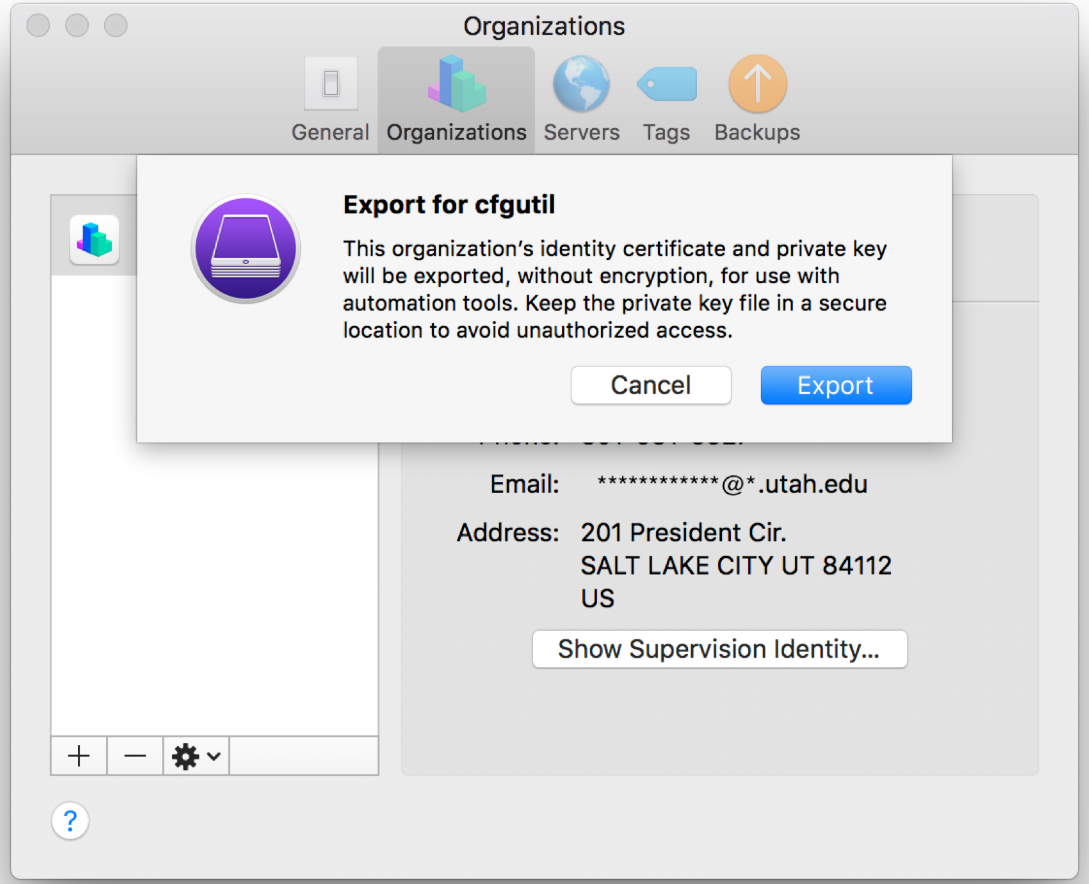
```
$ cfgutil get
```

- Useless:
  - bootState: device is unable to be accessed if it is not powered on
- Weird:
  - color, enclosureColor, ethernetAddress
- Missing:
  - Networking State (Wi-Fi and Bluetooth MAC addresses are available)
  - Activation Lock
  - More iCloud Information

`cfgutil` – Caveats

- Activation Lock:
  - No way to bypass activation lock (even with supervised erase)
  - Disable with MDM, if possible (Thank you Jamf Pro 10.7.1)
- Exec re-triggers attach and detach on device restart
- No VPP support for app installation
- Some supervision required
  - wallpaper, set-icon-layout, restart, shutdown
  - Requires unencrypted .DER certificate

cfgutil – Supervision Export



Export for cfgutil

This organization's identity certificate and private key will be exported, without encryption, for use with automation tools. Keep the private key file in a secure location to avoid unauthorized access.

Email: ************@*.utah.edu

Address: 201 President Cir.
SALT LAKE CITY UT 84112
US

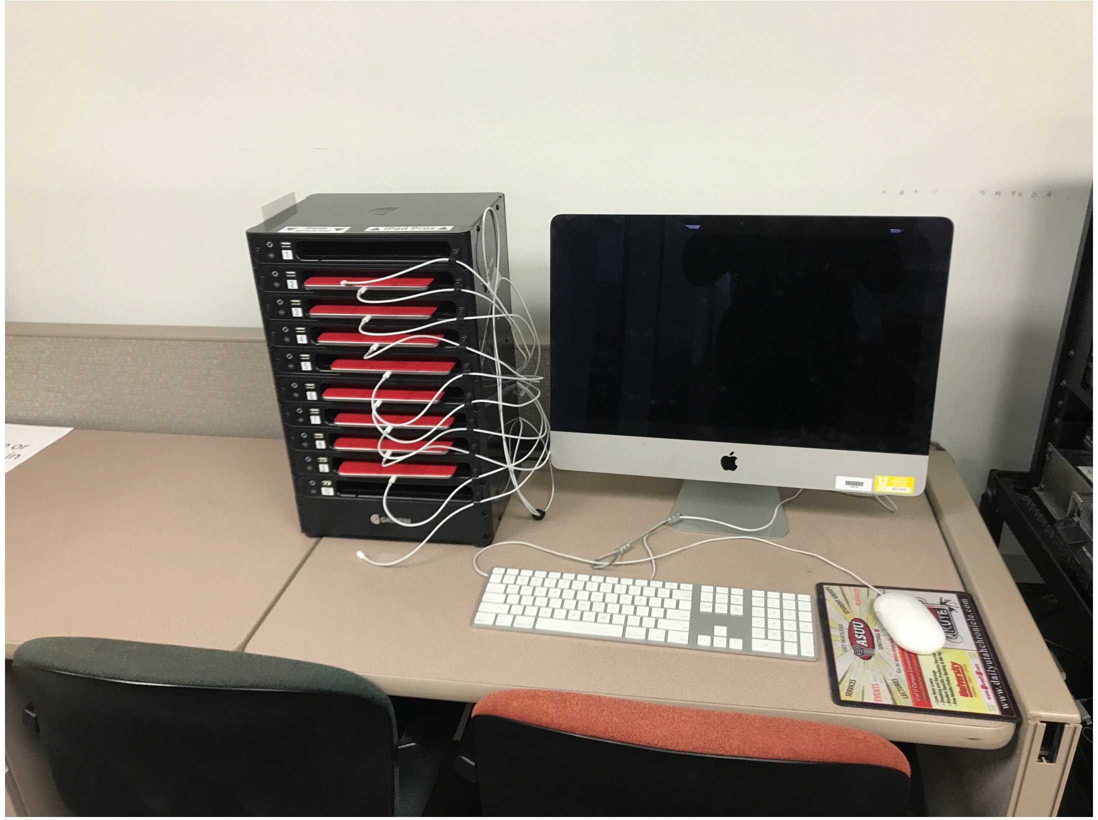
Our Solution

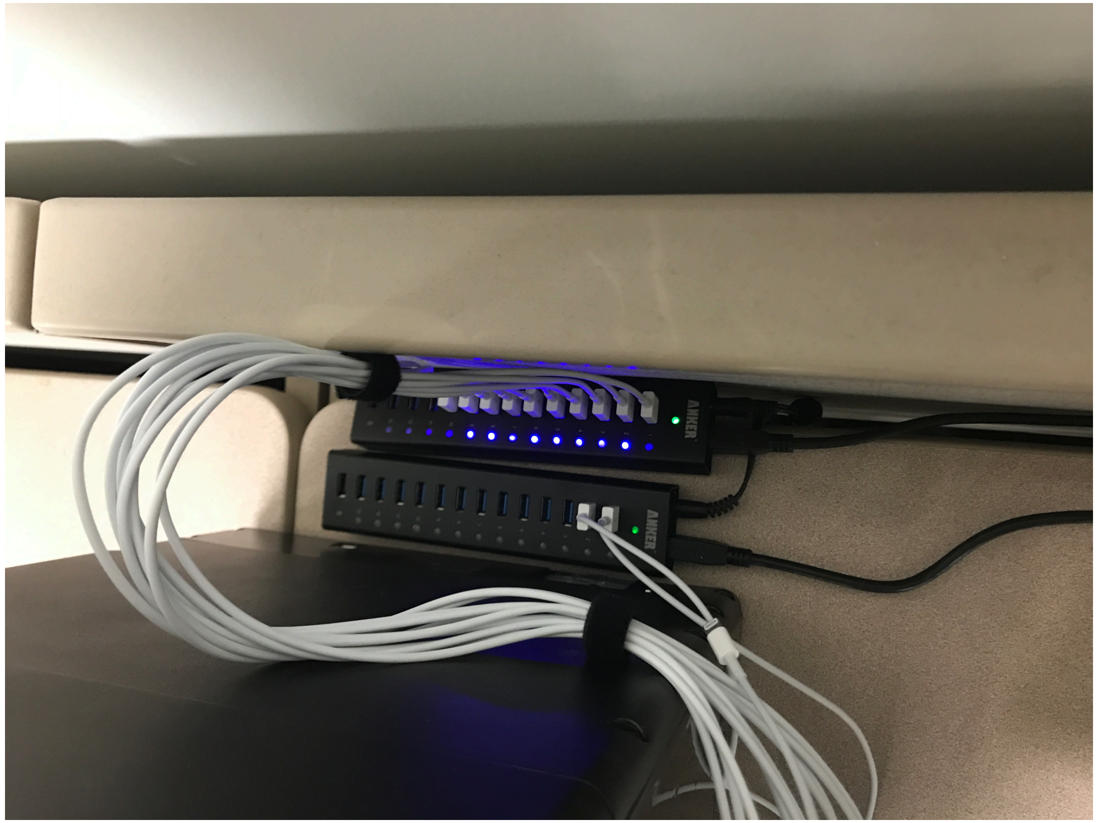
- Hardware (on a budget)
- macOS
- Custom Software

Hardware

- iMac Late 2012
  - macOS 10.12.6
- Powered USB 3.0 Hubs
- Shelf

Pictures





macOS

- macOS 10.12:
  - Network: tethered-caching (Sharing > Content Caching not available)
  - Apple Configurator: v.2.7.1
- macOS 10.13:
  - Network: Content Caching (/usr/bin/tethered-caching not distributed)
  - Apple Configurator v.2.7.1
- macOS 10.14:
  - Network: Content Caching
  - Apple Configurator 2.8.2

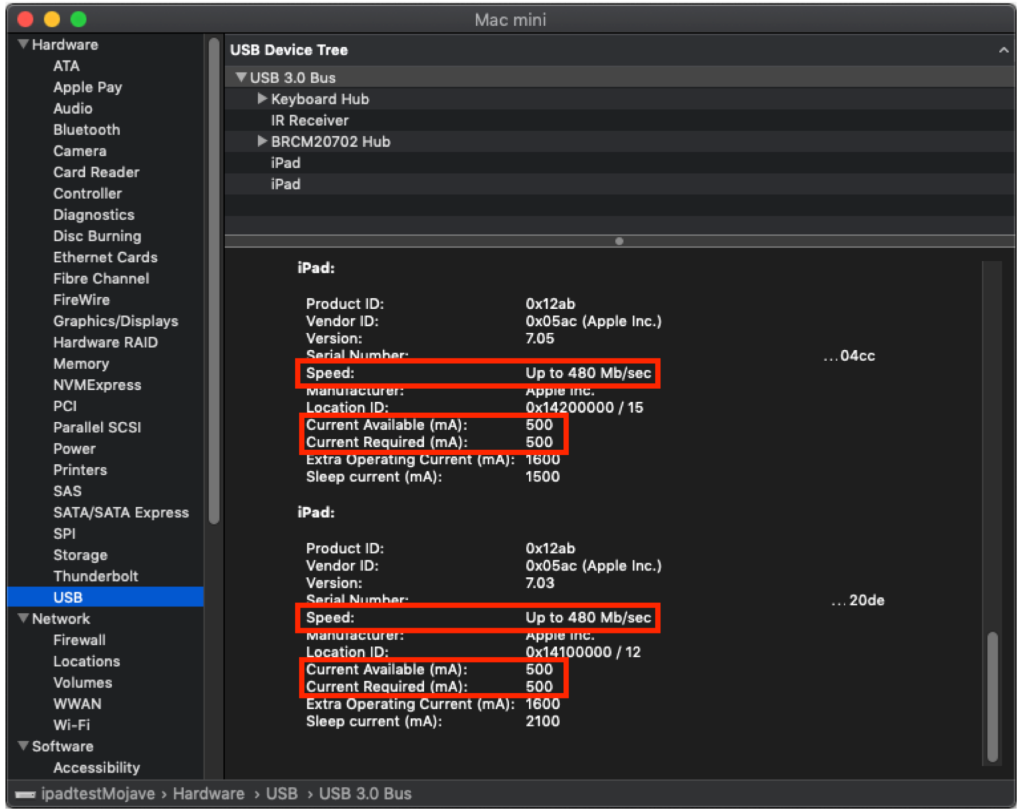
iOS Device Power

- Difficult to find specific specs
- Apple Adapters:
  - 5W USB Power Adapter (5V ⎓ 1A)
    - iPhone (4-6+), iPad mini
  - 10W USB Power Adapter (5.1V ⎓ 2.1A)
    - iPad 2, iPad Air (2), iPad mini (2-3)
  - 12W USB Power Adapter (5.2V ⎓ 2.4A)
    - iPad with Retina

Designed by Apple in California Assembled in China
10W USB Power Adapter
Model A1357 Input: 100-240V~ 0.45A (0,45A) 50-60Hz
Output: 5.1V ⎓ 2.1A Foxlink Technology Ltd. W010A051
NSW24363 LPS
JET
Apple Japan
TÜV
GS
ITE Power Supply
1RW0
LISTED
E211458

iOS Device Limitations

- iPad Pro and iPad Retina
- USB 2.0 (480Mb/s)
- 5V ⎓ .5A
- Warning:
  - Don’t overload USB hub with too many devices



```
▼Hardware
   ATA
   Apple Pay
   Audio
   Bluetooth
   Camera
   Card Reader
   Controller
   Diagnostics
   Disc Burning
   Ethernet Cards
   Fibre Channel
   FireWire
   Graphics/Displays
   Hardware RAID
   Memory
   NVMExpress
   PCI
   Parallel SCSI
   Power
   Printers
   SAS
   SATA/SATA Express
   SPI
   Storage
   Thunderbolt
   USB
▼Network
   Firewall
   Locations
   Volumes
   WWAN
   Wi-Fi
▼Software
   Accessibility
```

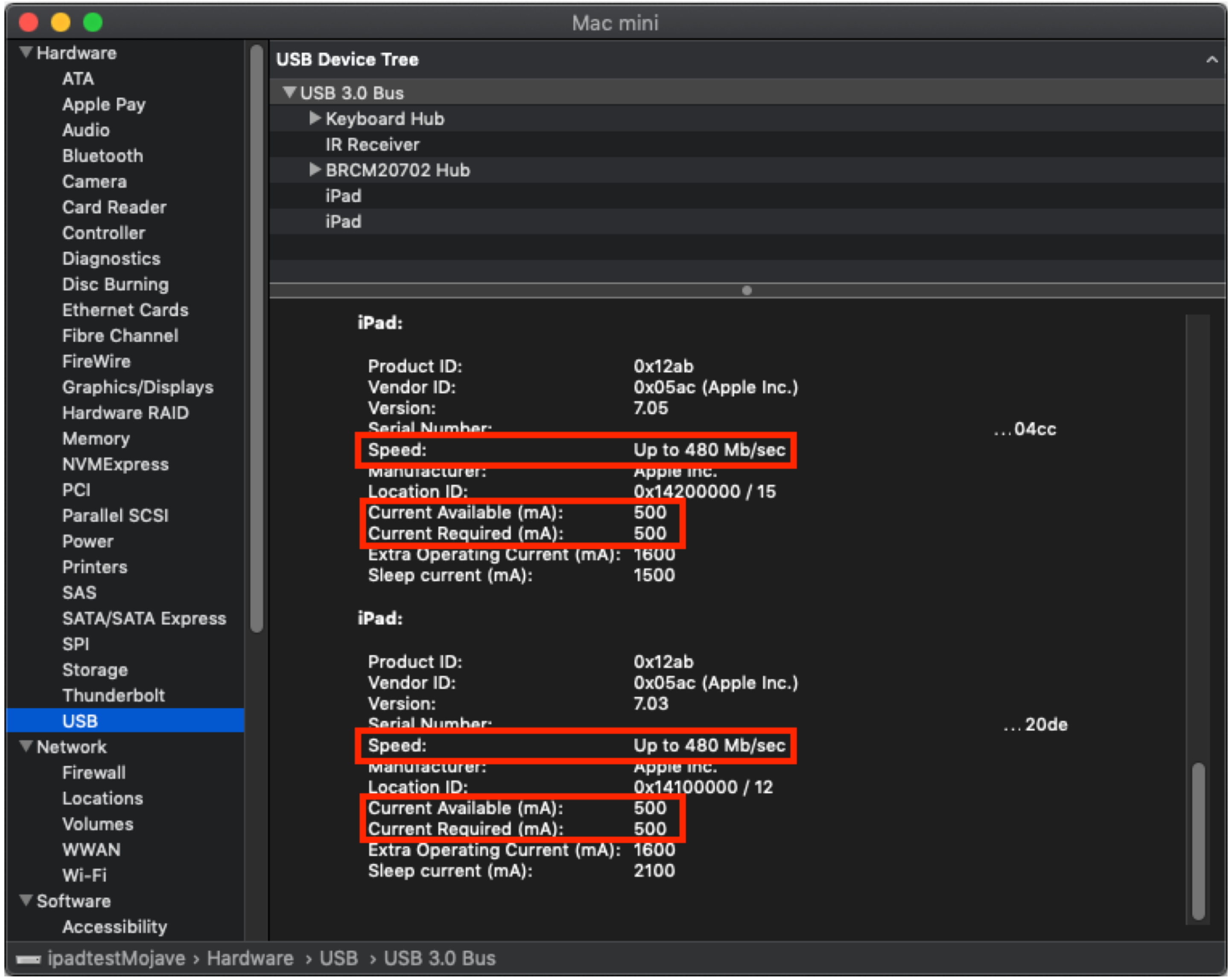
```
USB Device Tree
▼USB 3.0 Bus
   ▶Keyboard Hub
    IR Receiver
   ▶BRCM20702 Hub
    iPad
    iPad
```

```
iPad:

  Product ID:                    0x12ab
  Vendor ID:                     0x05ac (Apple Inc.)
  Version:                       7.05
  Serial Number:                                                   ...04cc
  Speed:                         Up to 480 Mb/sec
  Manufacturer:                  Apple Inc.
  Location ID:                   0x14200000 / 15
  Current Available (mA):        500
  Current Required (mA):         500
  Extra Operating Current (mA):  1600
  Sleep current (mA):            1500

iPad:

  Product ID:                    0x12ab
  Vendor ID:                     0x05ac (Apple Inc.)
  Version:                       7.03
  Serial Number:                                                   ...20de
  Speed:                         Up to 480 Mb/sec
  Manufacturer:                  Apple Inc.
  Location ID:                   0x14100000 / 12
  Current Available (mA):        500
  Current Required (mA):         500
  Extra Operating Current (mA):  1600
  Sleep current (mA):            2100
```



USB Device Tree

```
▼USB 3.0 Bus
   ▶Keyboard Hub
    IR Receiver
   ▶BRCM20702 Hub
    iPad
    iPad
```

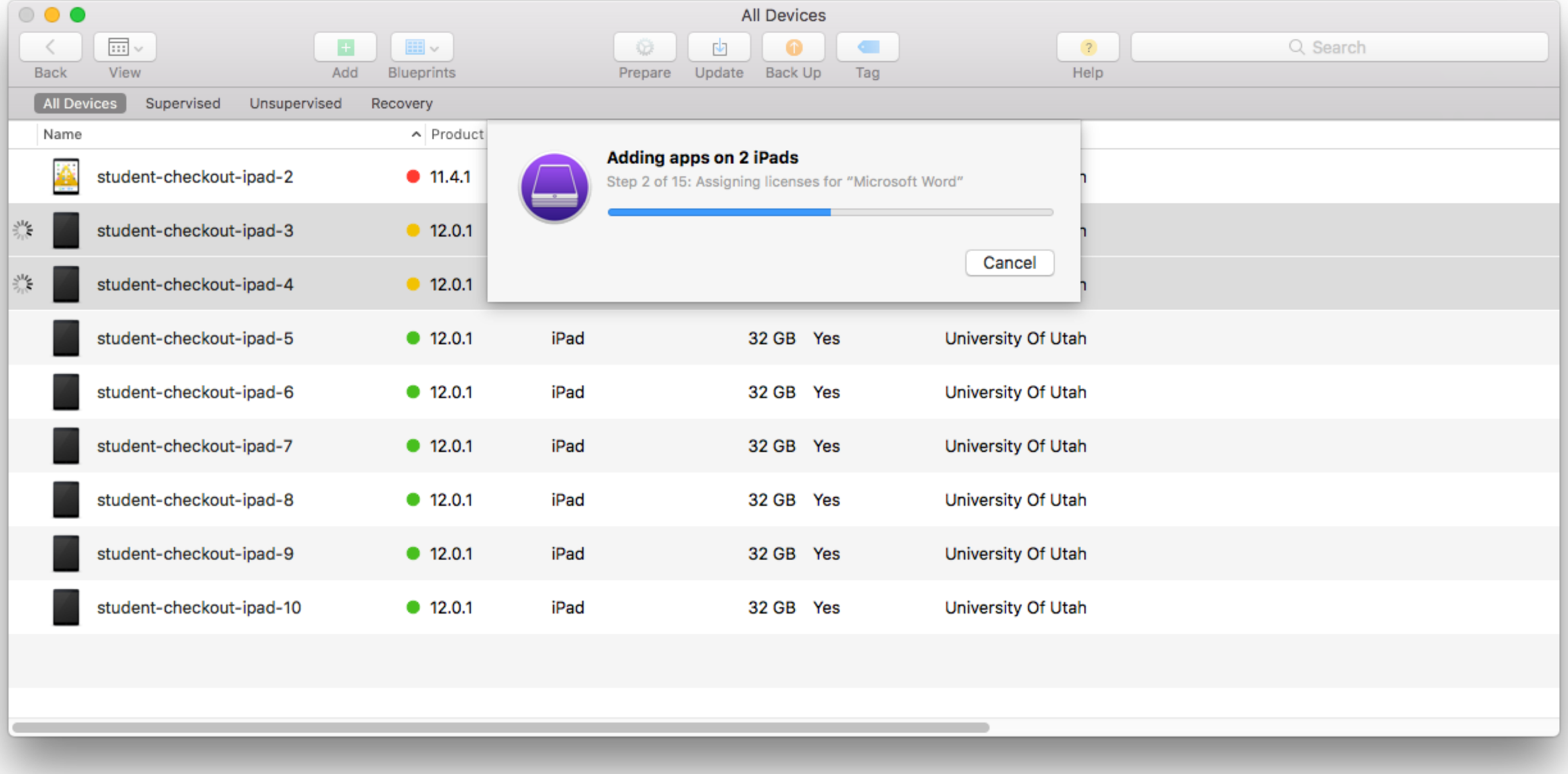
```
iPad:

  Product ID:                       0x12ab
  Vendor ID:                        0x05ac (Apple Inc.)
  Version:                          7.05
  Serial Number:                                                 ...04cc
  Speed:                            Up to 480 Mb/sec
  Manufacturer:                     Apple Inc.
  Location ID:                      0x14200000 / 15
  Current Available (mA):           500
  Current Required (mA):            500
  Extra Operating Current (mA):     1600
  Sleep current (mA):               1500

iPad:

  Product ID:                       0x12ab
  Vendor ID:                        0x05ac (Apple Inc.)
  Version:                          7.03
  Serial Number:                                                 ...20de
  Speed:                            Up to 480 Mb/sec
  Manufacturer:                     Apple Inc.
  Location ID:                      0x14100000 / 12
  Current Available (mA):           500
  Current Required (mA):            500
  Extra Operating Current (mA):     1600
  Sleep current (mA):               2100
```

Our Solution



Adding apps on 2 iPads

Step 2 of 15: Assigning licenses for “Microsoft Word”

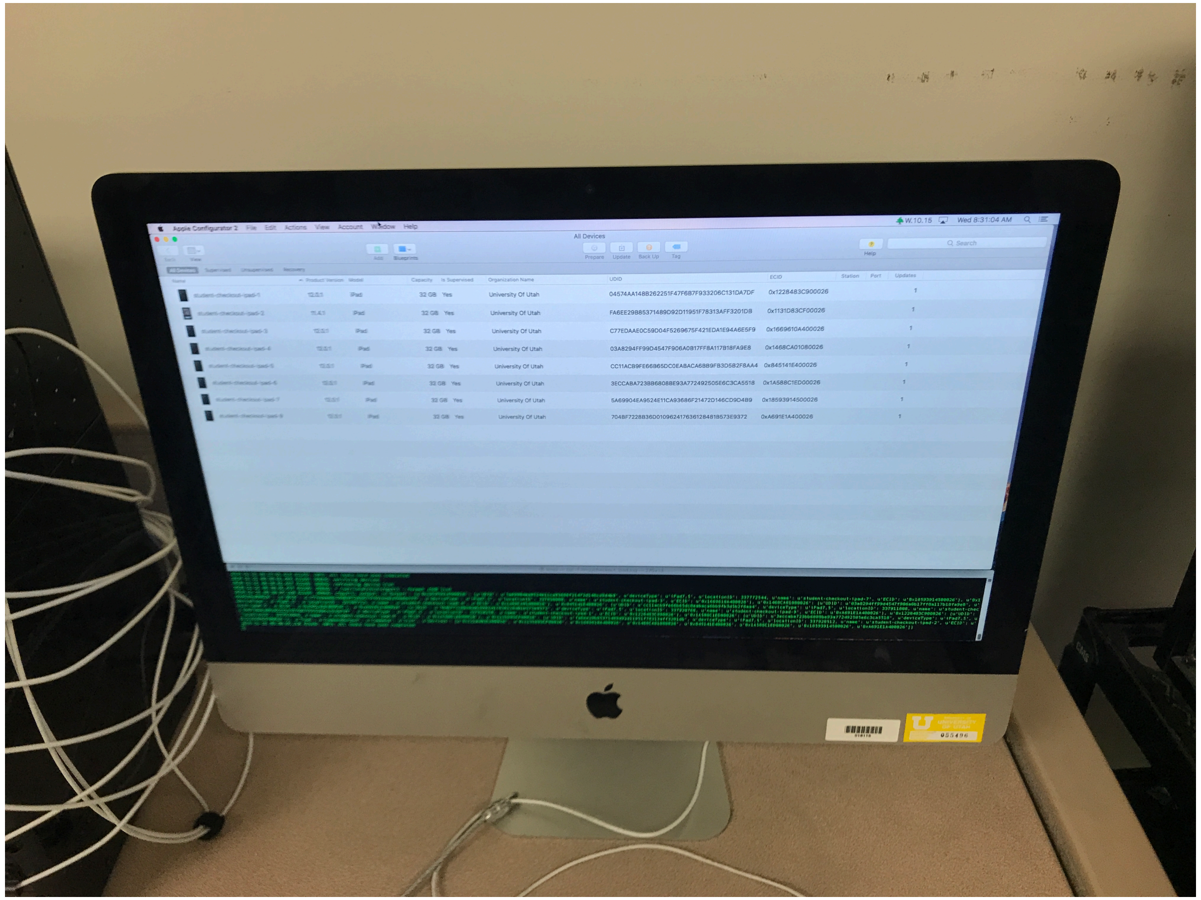
Cancel

Name	Product				
student-checkout-ipad-2	● 11.4.1				h
student-checkout-ipad-3	● 12.0.1				h
student-checkout-ipad-4	● 12.0.1				h
student-checkout-ipad-5	● 12.0.1	iPad	32 GB	Yes	University Of Utah
student-checkout-ipad-6	● 12.0.1	iPad	32 GB	Yes	University Of Utah
student-checkout-ipad-7	● 12.0.1	iPad	32 GB	Yes	University Of Utah
student-checkout-ipad-8	● 12.0.1	iPad	32 GB	Yes	University Of Utah
student-checkout-ipad-9	● 12.0.1	iPad	32 GB	Yes	University Of Utah
student-checkout-ipad-10	● 12.0.1	iPad	32 GB	Yes	University Of Utah

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

ALL U NEED

Our Solution



Name	Product Version	Model	Capacity	Is Supervised	Organization Name	UDID	ECID	Station	Port	Updates
student-checkout-ipad-1	12.0.1	iPad	32 GB	Yes	University Of Utah	04574AA148B262251F47F6B7F933206C131DA7DF	0x1228483C900026			1
student-checkout-ipad-2	11.4.1	iPad	32 GB	Yes	University Of Utah	FA6EE29B85371489D92D11951F78313AFF3201DB	0x1131D83CF00026			1
student-checkout-ipad-3	12.0.1	iPad	32 GB	Yes	University Of Utah	C77EDAAE0C59D04F5269675F421EDA1E94A6E5F9	0x1669610A400026			1
student-checkout-ipad-4	12.0.1	iPad	32 GB	Yes	University Of Utah	03A8294FF99D4547F906A0B17FF8A117B18FA9E8	0x1468CA01080026			1
student-checkout-ipad-5	12.0.1	iPad	32 GB	Yes	University Of Utah	CC11ACB9FE66B65DC0EABACA6BB9FB3D5B2F8AA4	0x845141E400026			1
student-checkout-ipad-6	12.0.1	iPad	32 GB	Yes	University Of Utah	3ECCABA723BB6808BE93A772492505E6C3CA5518	0x1A588C1ED00026			1
student-checkout-ipad-7	12.0.1	iPad	32 GB	Yes	University Of Utah	5A69904EA9524E11CA93686F21472D146CD9D4B9	0x18593914500026			1
student-checkout-ipad-9	12.0.1	iPad	32 GB	Yes	University Of Utah	704BF7228B36D010962417636128481B573E9372	0xA691E1A400026			1

Our Solution – Software

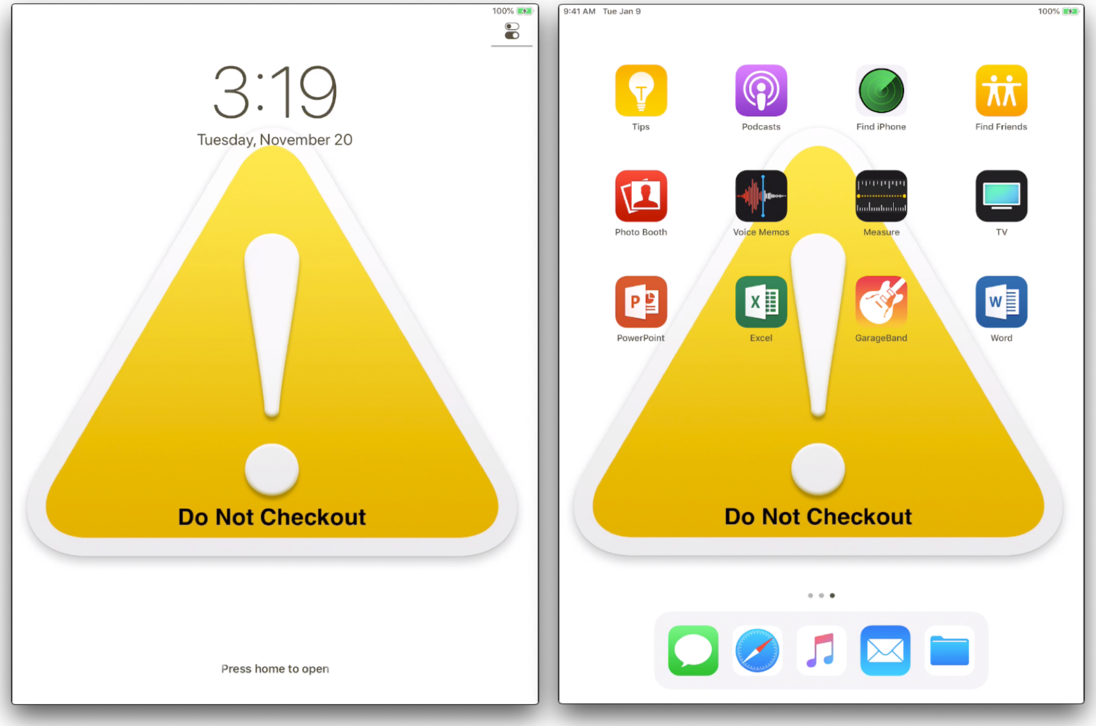
- Mix and match!
- Play to DEP + MDM’s unparalleled configuration management
- Leverage Apple Configurator’s automation tools and Setup Assistant bypass mechanisms
- Scripts to install VPP apps via GUI
- TRUELY Zero-Touch

Automation

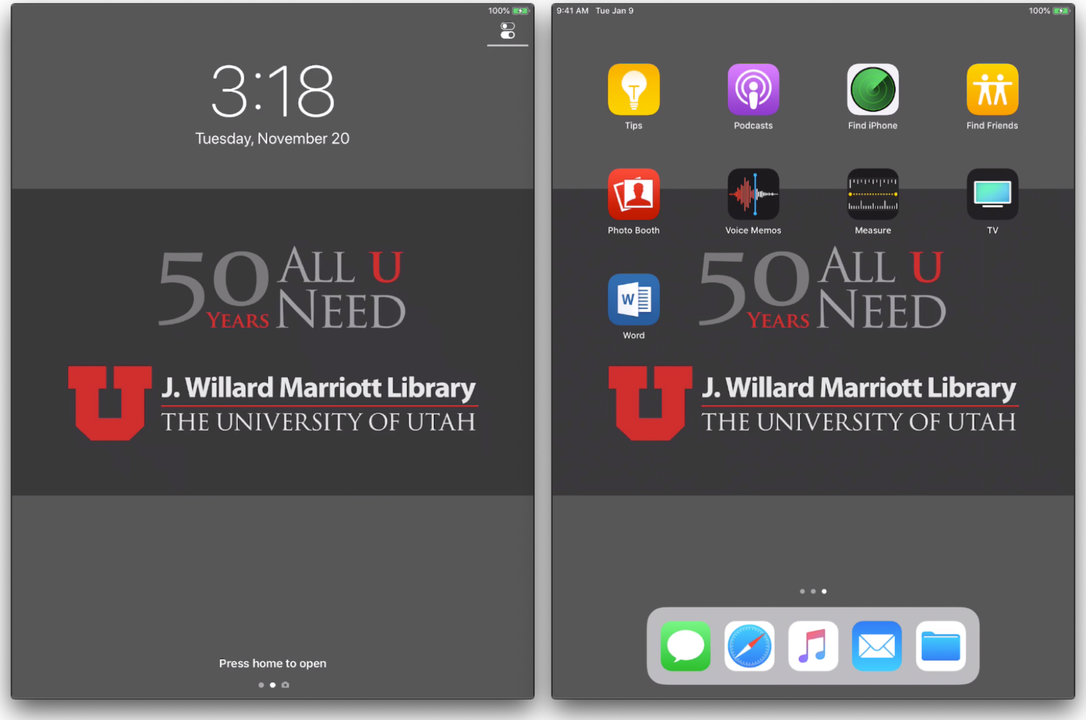
- Use `cfgutil exec` to trigger our scripts on device attachment and detachment
- Connection of iOS device to the station triggers check-in processes
    - Device queries, erase, re-enrollment, and app installation
- Configurable list of VPP apps to install
- Additionally modify background as an indicator to device state

Backgrounds as Indicators

Failed or In Progress



Successfully Finished



J. Willard Marriott Library
THE UNIVERSITY OF UTAH

ALL U NEED

ACAdapter

- Built to interact with Apple Configurator 2 GUI (AppleScript)
- Designed to bridge shortcomings in `cfgutil`
  - Blueprint Support
  - VPP App installation
- GUI Interaction:
  - Errors, Prompts, Status
- Caveats:
  - Running application requires Accessibility access
  - Non-default column UDID and ECID
  - Still in beta (not publicly available… yet)

Reporting

- Currently using Slack to report issues
- App installation:
  - List of apps that were installed by the user
  - Used to keep auto installed apps relevant
- New Errors as they occur

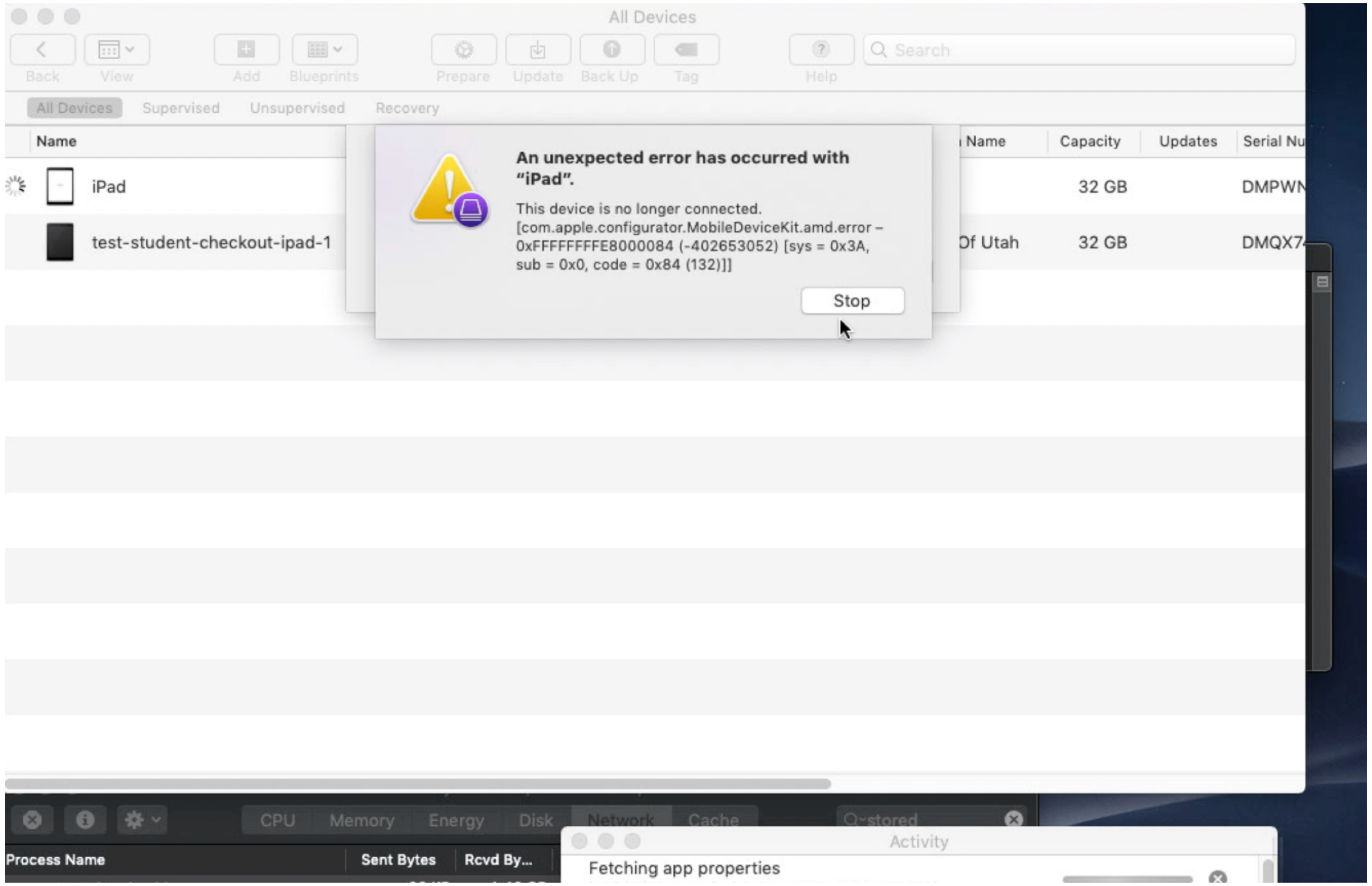
Fixed Issues

- Error Detection
  - Blueprint failed if one app failed on one device
- VPP app installation DoS
  - Invalidated account for 24 hours
- Attach and detach on erase
  - 72 hours of non-stop imaging
- Activation Lock
  - App store sign-in enabled Find my Device by default

Moving Forward

- Solidifying support for macOS 10.13 and 10.14
- Releasing the code for everyone via our GitHub
- Modular:
    - Error handling (sometimes things just act weird)
    - Reporting (allow plugin reporting mechanisms)
    - App-lists (distributed via JAMF)
    - Supervision Identity importing
- More visual feedback
- Blog

Random Errors

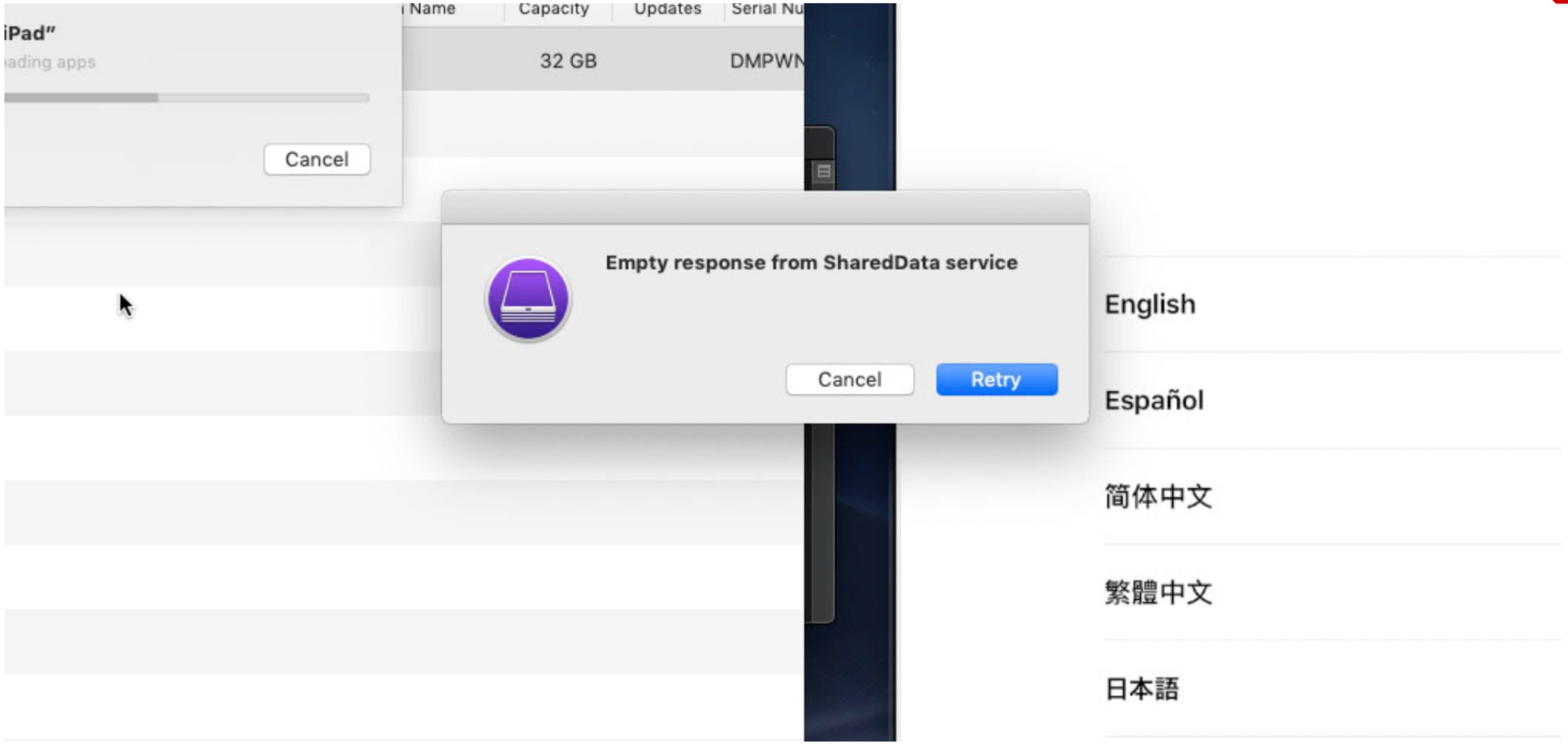


An unexpected error has occurred with "iPad".

This device is no longer connected. [com.apple.configurator.MobileDeviceKit.amd.error – 0xFFFFFFFFE8000084 (-402653052) [sys = 0x3A, sub = 0x0, code = 0x84 (132)]]

Fetching app properties

Random Errors



Empty response from SharedData service

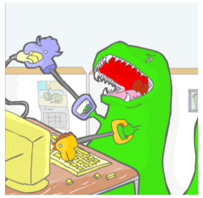
More Research

- Apple School Manager
  - VPP License Transfer
- Apps:
  - Jamf Reset
  - Jamf Setup

Resources – Sal Soghoina

- "De facto iOS Automation Guru" – Me, now
- Automation Product Manger for Apple Inc. (1997 – 2016)
- Code contribution distributed Apple Configurator 2
- Site: https://configautomation.com
- iOS Devices by Sal Soghoina (Mac Managers 2018)
  - http://docs.macsysadmin.se/2018/pdf/Day1Session6.pdf
  - http://docs.macsysadmin.se/2018/video/Day1Session6.mp4

Resources



- Apple:
  - VPP: https://developer.apple.com/programs/volume/
  - DEP: https://support.apple.com/en-us/HT204142
  - iOS Power: https://support.apple.com/en-us/HT204377
  - Shared iPads: https://developer.apple.com/education/shared-ipad/
- MDM:
  - Comparison: http://www.mobiledevicemanagement.io
  - Jamf Pro: https://www.jamf.com/products/jamf-pro/device-management/
- University Enrollment: https://higheredutah.org/data/enrollments/

Questions?

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

ALL U
NEED