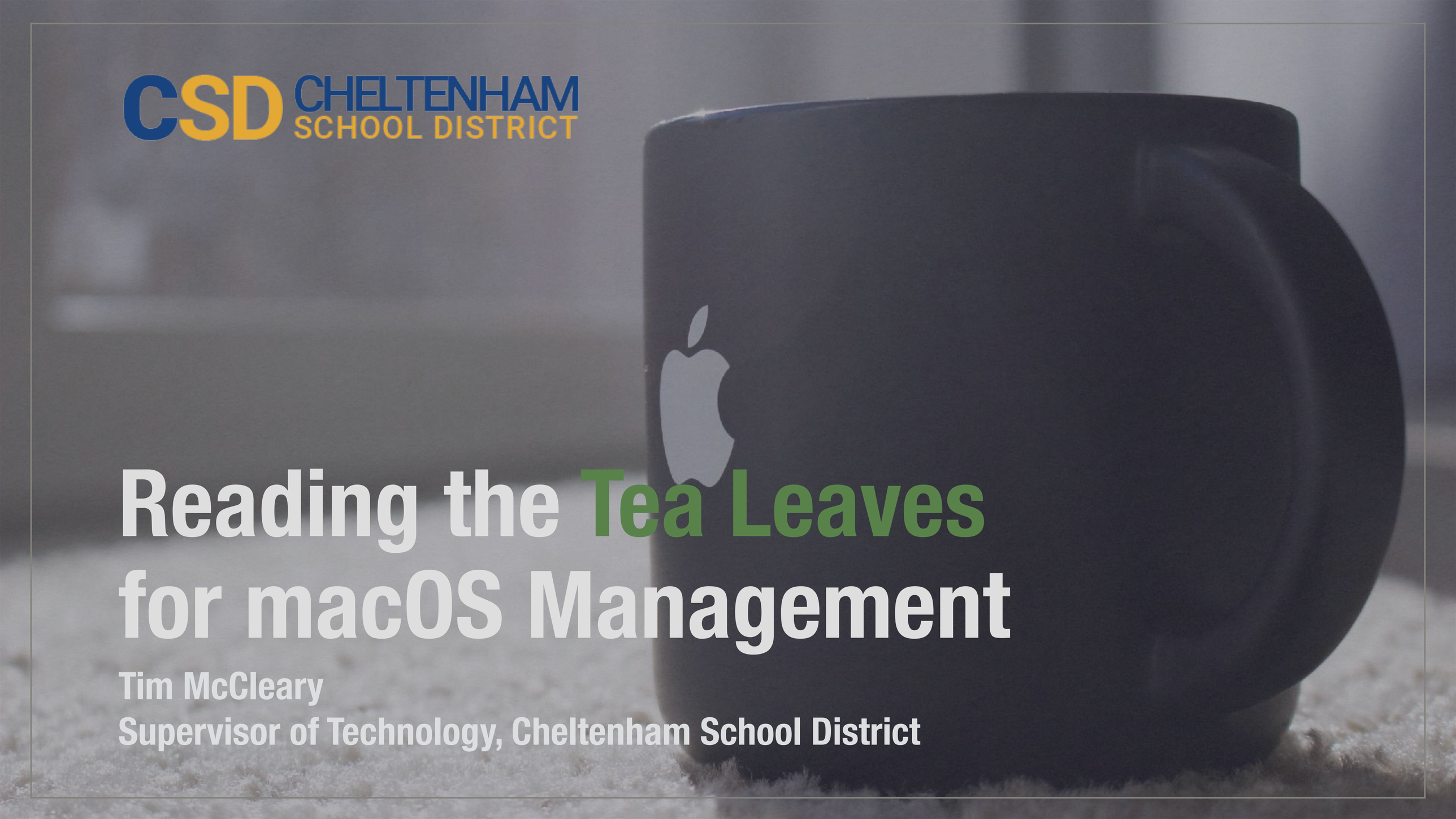


CSD CHELTENHAM SCHOOL DISTRICT

Reading the Tea Leaves for macOS Management

Tim McCleary
Supervisor of Technology, Cheltenham School District

How Do You Deploy Now?

- Building Each Mac Individually
- Monolithic Imaging (Master Image)
- Modular Imaging
- Thin Imaging
- DEP Deployment / “Zero-Touch” Deployment

What Method Do You Use?

- NetBoot/NetInstall solution
- Target Disk Mode
- Booting from External Drive
- Other?

Which MDM Do You Use?

- JAMF Pro (Casper)
- FileWave
- Meraki Systems Manager
- LANRev
- Profile Manager
- MicroMDM
- SimpleMDM
- Munki
- Other?
- What’s an MDM?

Terminology

- **MDM:** Mobile Device Management
- **DEP:** Device Enrollment Program
- **HFS+:** Hierarchical File System or Mac OS Extended; the default file system for the Mac until High Sierra, introduced in January 1998
- **APFS:** Introduced at WWDC as a replacement for HFS+ for macOS, iOS, tvOS, and watchOS; optimized for flash and solid-state storage with a **focus on encryption**

Hints from WWDC 2016

- Credit goes to: http://michaellynn.github.io/2016/10/04/mDMacOS/
- “…Apple File System will be the default file system for all Apple products [in] 2017”
- “…this allows us to unify our **encryption** story across all of our platforms.”
- Translation: We’re going to handle things with macOS similar to how we handle things with iOS, tvOS, and watchOS.
- **Simplified Translation: Get ready to chuck most of what you know about deploying macOS devices out the window!**

Hints from @deploystudio

Hints from High Sierra

- https://support.apple.com/en-us/HT208020
- “Apple doesn't recommend or support monolithic system imaging when upgrading or updating macOS.”
- “If you try to use a monolithic system image, required firmware updates will be missing from the installation. This causes the Mac to operate in an unsupported and unstable state.”

Hints from the iMac Pro

- Secure Boot (https://support.apple.com/en-us/HT208330): “Use Secure Boot to make sure that only a legitimate, trusted operating system loads on your iMac Pro at startup.”
- No NetBoot (https://support.apple.com/en-us/HT202770): “iMac Pro computers don't support starting up from network volumes.”
- https://support.apple.com/en-us/HT201255: For holding “N” during startup — “iMac Pro doesn't support this startup key.”
- https://help.apple.com/configurator/mac/2.6/#/apdebea5be51: Instructions on restoring an iMac Pro with Apple Configurator 2.6.

Hints from macOS Server.app

- https://support.apple.com/en-us/HT208312
- “A number of services will be deprecated, and will be hidden on new installations of an update to macOS Server coming in ~~spring~~ fall 2018.”
- In the list: NetInstall (which also means NetBoot)

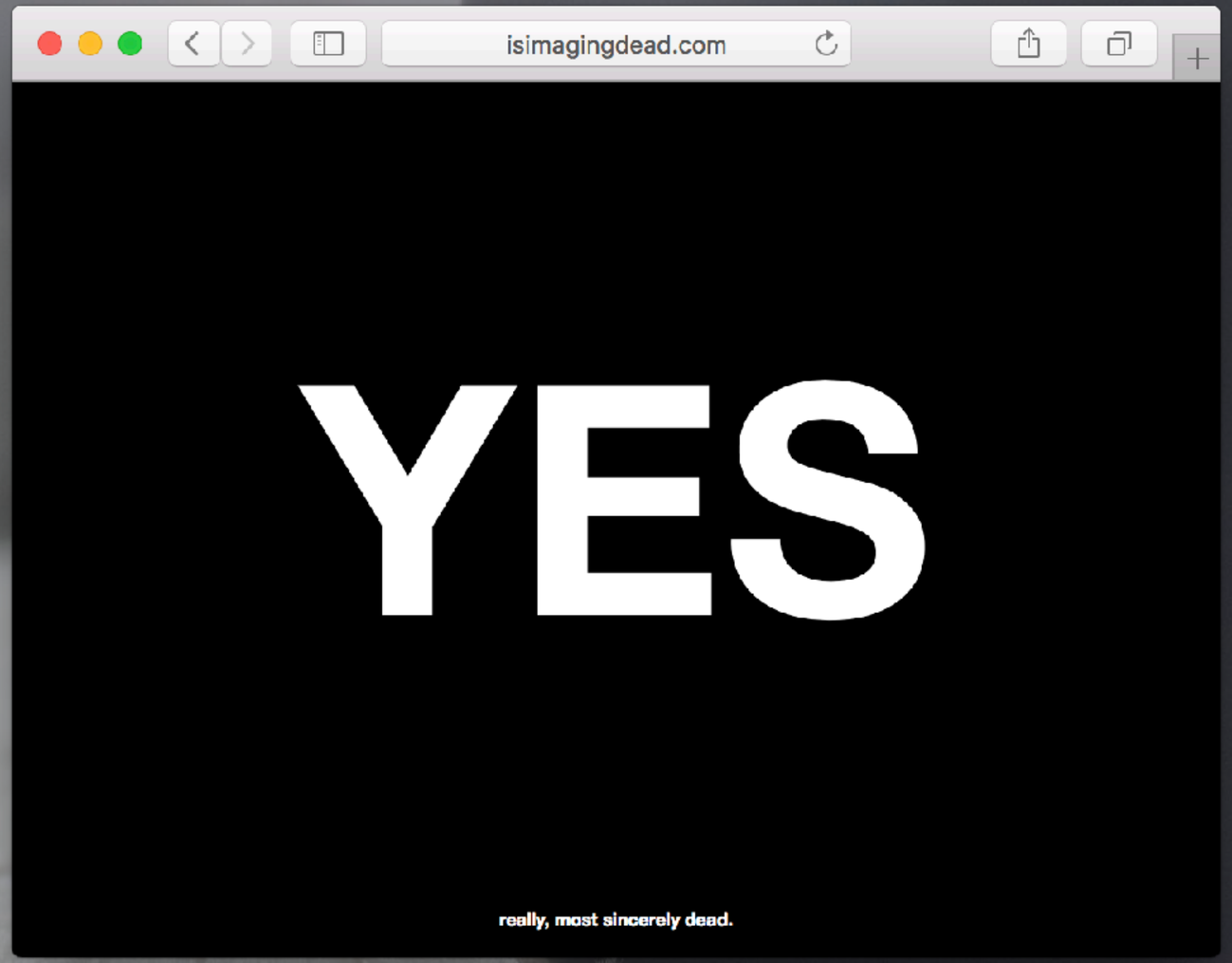
Hints from High Sierra 10.13.4

- https://support.apple.com/en-us/HT208533
- “No longer disables User Approved Kernel Extension Loading on MDM-enrolled devices. For devices with DEP-initiated or User Approved MDM enrollment, administrators can use the Kernel Extension Policy payload.”

Hints from High Sierra 10.13.4

- Just something else to note…
- https://support.apple.com/en-us/HT208436
- “Starting with macOS High Sierra 10.13.4, apps that have not been updated to use 64-bit processes produce a one-time alert when opened. This gives users advance notice that they are running 32-bit software, which will not be compatible with macOS in the future.”

Hints from the InterWebs



Where Do We Go From Here?

Need to Change Our Thinking on Deployment:

~~Imaging~~ ➡ Provisioning

Is Imaging Really Dead? What now?

- Not quite yet, but it’s on life support
- Start experimenting now so you’re ready for the inevitable
- Get connected with the larger Mac community — there’s a lot of really smart people out there that apparently have a lot more time on their hands than probably any of us do.

Where Do I Even Start???

- Three Not-So-Simple Steps
  - Make sure your institution is set up for DEP with Apple
  - Get an MDM that can manage macOS devices
  - Develop and test (and test and test…) a DEP enrollment process with your MDM and/or management system

Two Quick Items to Note…

- **UAMDM — User Approved MDM**
  - If you are not using DEP, you will need to manually approve your MDM starting with 10.13.4
  - This cannot be done remotely, must be done while physically at the device!
  - Approval button cannot be clicked from a remote screen sharing connection (ARD, TeamViewer, etc.)

Two Quick Items to Note…

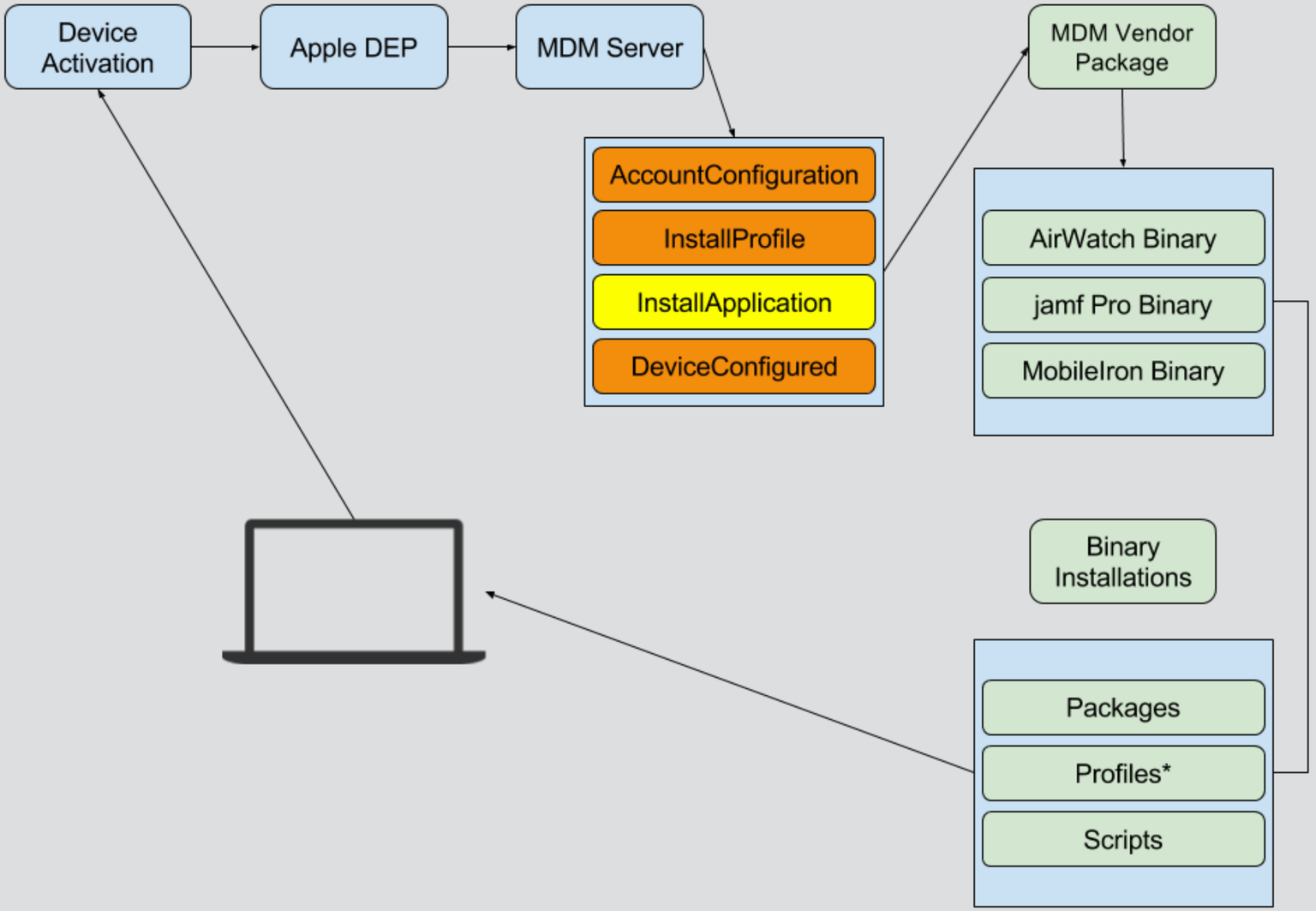
- **UAKEL — User Approved Kernel Extension Loading**
  - https://support.apple.com/en-us/HT208019
  - Requires any Kernel Extensions to be approved before the OS will load them starting with 10.13.4
  - Can be approved via Configuration Profile deployed by your MDM (https://derflounder.wordpress.com/2018/04/12/whitelisting-third-party-kernel-extensions-using-profiles/)
  - Includes SMART drivers, docking station drivers, Google Drive File Stream, etc.

DEP Process Step-By-Step

- Device booted for the first time
- Setup Assistant loads and the user is prompted to connect to a wireless network (if not wired)
- Once connected, the Mac is activated
- If the Mac’s serial number is assigned in DEP to an MDM server, the device registers with the server
- The device will go through the steps: “AccountConfigured”, “InstallProfile”, “InstallApplication”, and finally “DeviceConfigured” (It is possible that the user will be logged into the Mac while this process is happening in the background.)

Visualization of the DEP Enrollment Process

From: http://blog.eriknicolasgomez.com/2017/03/08/Custom-DEP-Part-1-An-Introduction/



InstallApplication is the Key

- This is where your specific customizations and installations happen in the process
- Install Configuration Profiles
- Run scripts to configure defaults
- Prompt user for computer name
- Install packages
- Install software updates

My Process (Still in “Beta”)

- Boot new Mac fresh out of the box
- Connect to WiFi
- Let it enroll with our MDM (Jamf) and create our LocalAdmin account
- Script runs in background and waits for a non-setup user to login
- Log into LocalAdmin account
- Script kicks in after a few seconds and prompts for computer name
- Once computer name is entered, script takes over screen and displays setup and software installation progress
- Ends with checking for any updates and installing them

Live Demo: DEP+MDM+Fingers Crossed

(or “what I’ve figured out so far…”)

Using JAMF Pro and some scripts to make magic happen…

Backup Plan: Pre-Recorded Video
(in case the demo failed horribly)

Using JAMF Pro and some scripts to make magic happen…

Hang on...We are setting up your Mac for the first time

CSD CHELTENHAM SCHOOL DISTRICT

Please wait...calculating pi to a few million digits

Additional Things to Worry About

- UAMDM (User Approved MDM): Requires the user to approve the MDM if computer is enrolled manually. DEP enrollment bypasses this. **Approval cannot not be done via a remote connection!** [10.13.4+]
- UAKEL (User Approved Kernel Extension Loading): Requires an admin user to approve any kernel extensions before they will load. This includes drivers (SMART, docking stations, Google Drive, etc.). **Can be automatically approved with an approved MDM.** [10.13.4+]
- 32-Bit Apps are going away, which affects a lot of older apps, especially in education. [10.15?]

Apple's View

- Hand a Mac to the end user still in the box and they can set it up themselves!
- Give the user the ability to personalize their Mac the way they want it
- You can enforce policies and make software available that they can install themselves

Reality

- You're probably gonna want to still set up each Mac yourself to ensure consistent results
- Let's be honest: DEP works, but there's still things that can go south and screw things up
- You can enforce policies and make software available that they can install themselves

Apple's View

- Need to rebuild an existing Mac?
- Just reinstall from macOS Recovery.
- Hold down Command-R while booting.
- Erase the drive with Disk Utility
- Reinstall macOS
- Spend a lot of time doing this

Reality

- Our existing methods are much faster
- Imaging still works (in some cases), so use it while you can to install a base, never-booted image of macOS
- Don't image a newer version than what's already on it (not supported)
- Boot normally and use DEP+MDM
- Let the MacAdmin community figure out a better way

Recommended Resources

- MacAdmins Slack (https://macadmins.slack.com) — Get invited here: https://macadmins.herokuapp.com/
- Jamf Nation (https://www.jamf.com/jamf-nation/) — Geared towards Jamf products, but also a good source of knowledge
- Managing OS X blog (https://managingosx.wordpress.com/)
- Der Flounder blog (https://derflounder.wordpress.com/)
- ScriptingOSX blog (https://scriptingosx.com/)

Recommended Tools

- Automate checking for and getting the latest app updates:
  AutoPkg / AutoPkgr (https://github.com/lindegroup/autopkgr)
- Build a base image of macOS from a macOS Installer
  AutoDMG (https://github.com/MagerValp/AutoDMG)
- Clone the serial number from a Mac enrolled in DEP, combine it with a base image from AutoDMG and get a VM you can snapshot and easily test your DEP enrollment/provisioning process
  VMware Fusion + vfuse (https://github.com/chilcote/vfuse/releases)

Recommended Tools

- Get an MDM for your Macs if you don’t already have one!
  - Jamf Pro
  - FileWave
  - Meraki Systems Manager
  - LANRev
  - SimpleMDM
  - MicroMDM

Keep in Touch

Tim McCleary
Email: tmccleary@cheltenham.org
MacAdmins Slack: @macpropellerhead

This presentation available here:
https://www.cheltenham.org/2018ttl
https://www.cheltenham.org/2018ttlvideo