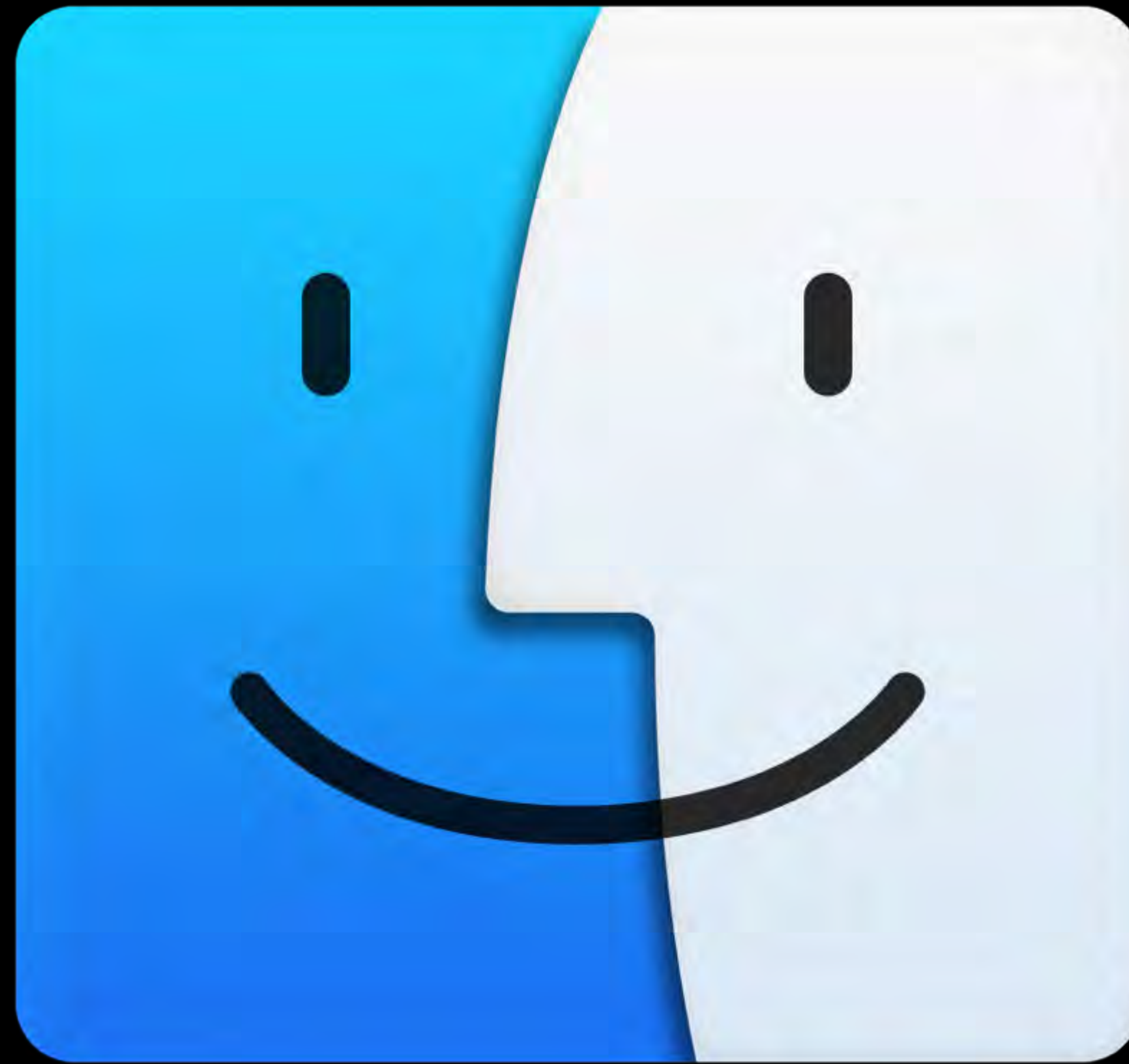


GUUG FRÜHJAHRSFACHGESPRÄCH 2016



APPLE OS X UND IOS MANAGEMENT

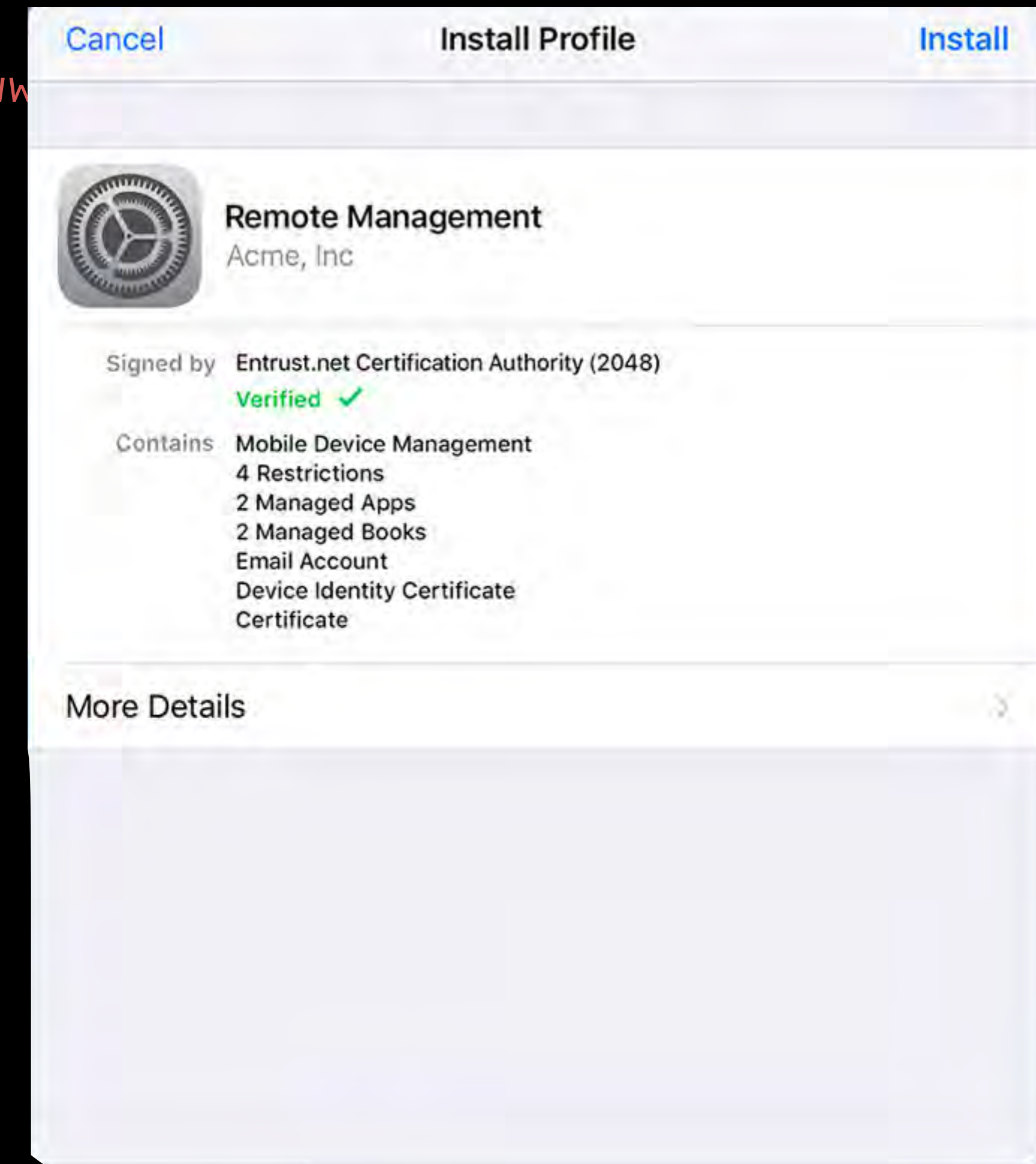


MOBILE DEVICE MANAGEMENT (MDM)

CONFIGURATION PROFILES



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadIdentifier</key>
  <string>com.acme.profile.wifi</string>
  <key>PayloadRemovalDisallowed</key>
  <true/>
  <key>PayloadScope</key>
  <string>System</string>
  <key>PayloadType</key>
  <string>Configuration</string>
  <key>PayloadUUID</key>
  <string>48a39070-1e4c-0131-c321-000c2944c108</string>
  <key>PayloadOrganization</key>
  <string>ACME Inc.</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>PayloadDisplayName</key>
  <string>WiFi</string>
  [...]
```

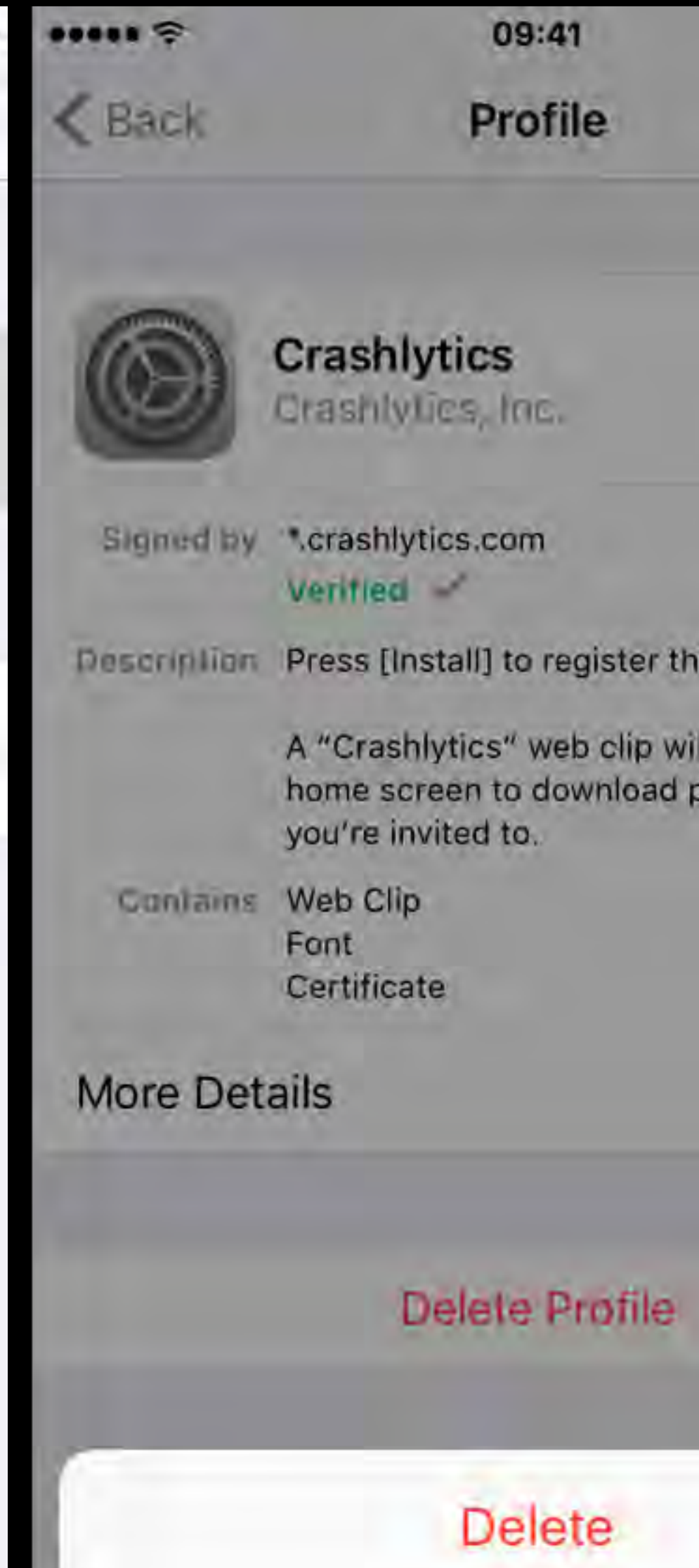
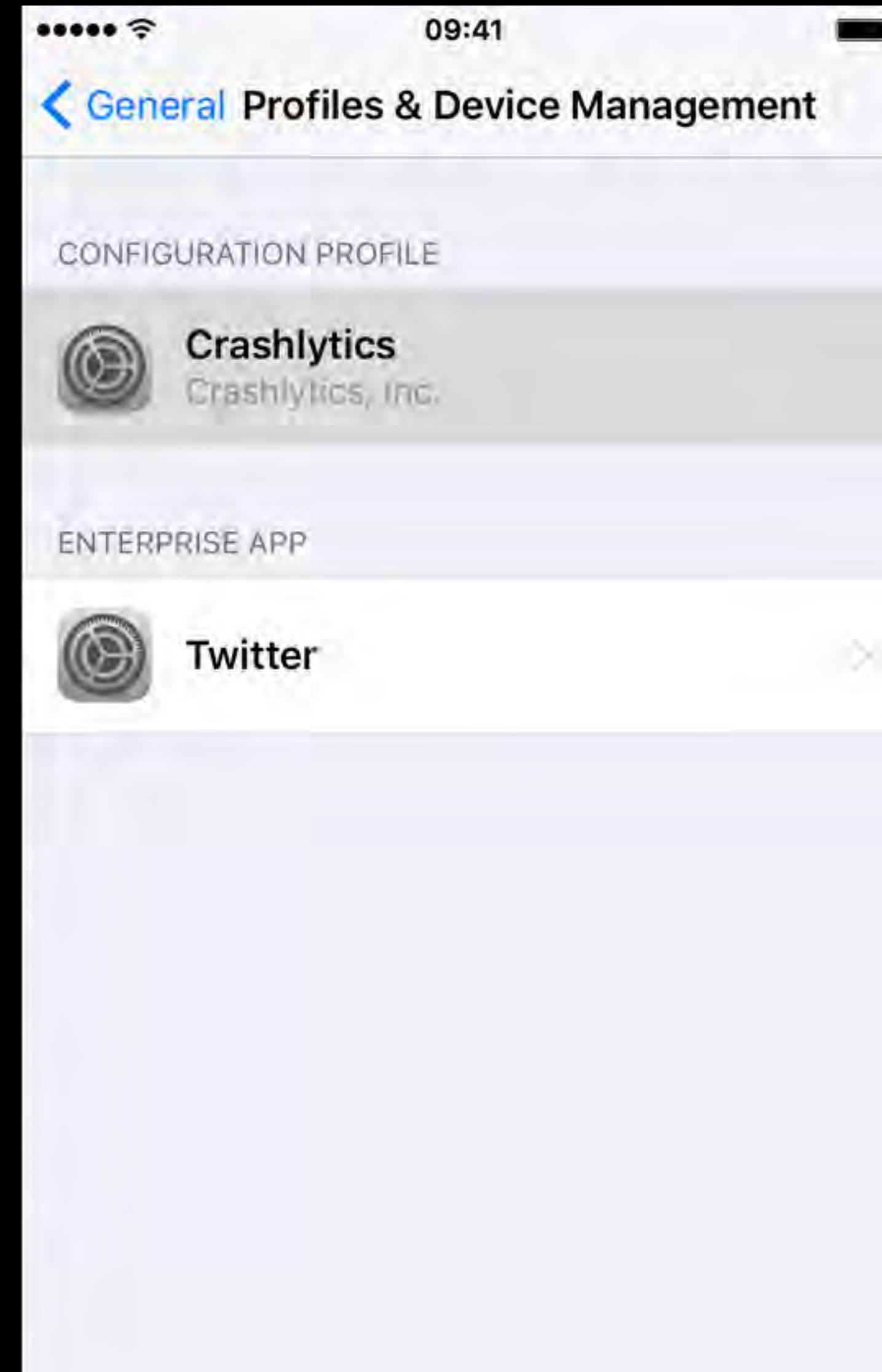


CONFIGURATION PROFILES (CONTINTUED)



UNIVERSITY OF
OXFORD



```
<key>PayloadContent</key>
<array>
<dict>
  <key>PayloadType</key>
  <string>com.apple.wifi.managed</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>PayloadEnabled</key>
  <true/>
  <key>EncryptionType</key>
  <string>WPA</string>
  <key>SSID_STR</key>
  <string>ssid</string>
  <key>Password</key>
  <string>password</string>
  <key>HIDDEN_NETWORK</key>
  <false/>
  <key>AutoJoin</key>
  <true/>
  [...]
</dict>
</array>
</dict></plist>
```

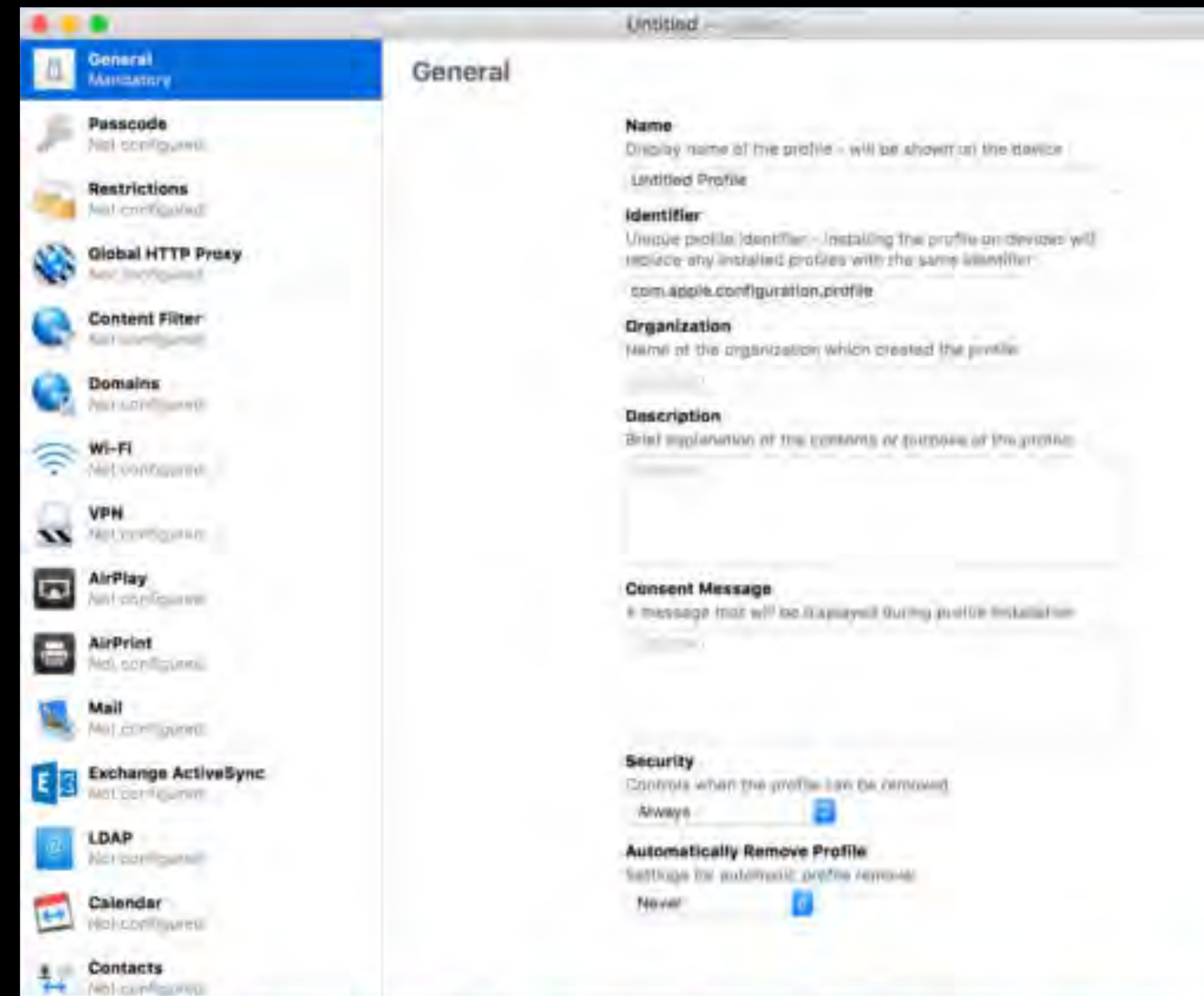


Delete

DEPLOYING CONFIGURATION PROFILES



- Using Apple Configurator (iOS only) 
- In an email message
- On a webpage
- Using over-the air configuration using a Mobile Device Management Server (e.g. Apple Profile Manager) 

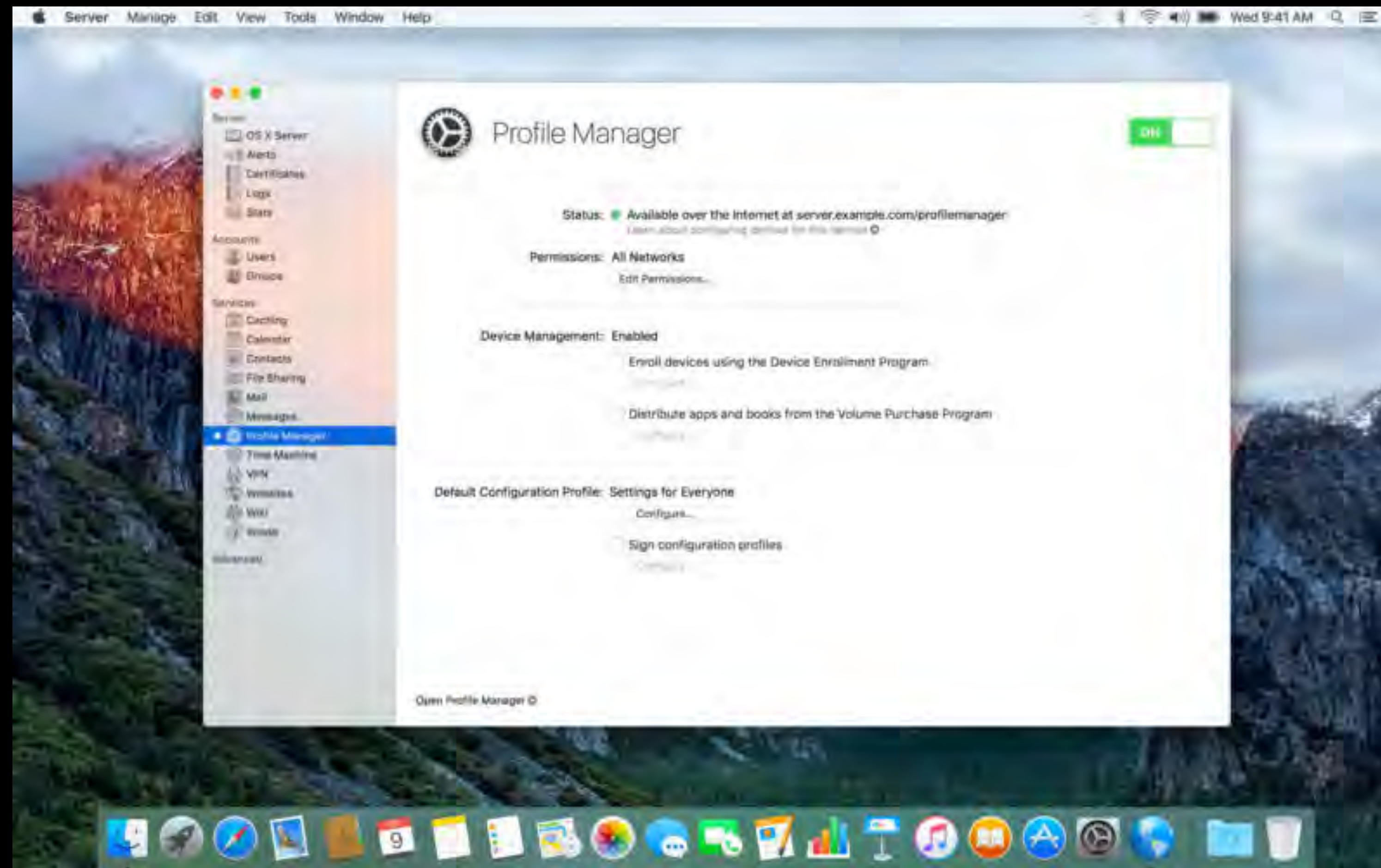


MOBILE DEVICE MANAGEMENT

- Managed apps, books, domains, accounts, extensions, ...
- Policy settings
- Security (e.g. encryption, passcodes, Touch ID, SSO)
- Remote control (e.g. selective remote wipe)
- Asset tracking
- Firmware / OS upgrades
- Comparison of MDM solutions at <http://enterpriseios.com/>



APPLE OS X SERVER



DEVICE ENROLLMENT PROGRAM (DEP)



- Fast, streamlined way to deploy corporate-owned devices
 - Automated enrollment in MDM Server
 - Enables 'zero touch' deployment workflows
- Mac or iOS devices purchased directly from Apple or through participating Apple Authorised Resellers
- Enroll at <http://deploy.apple.com> using a shared Apple ID belong to your organisation



iPad

9:41 AM

100%

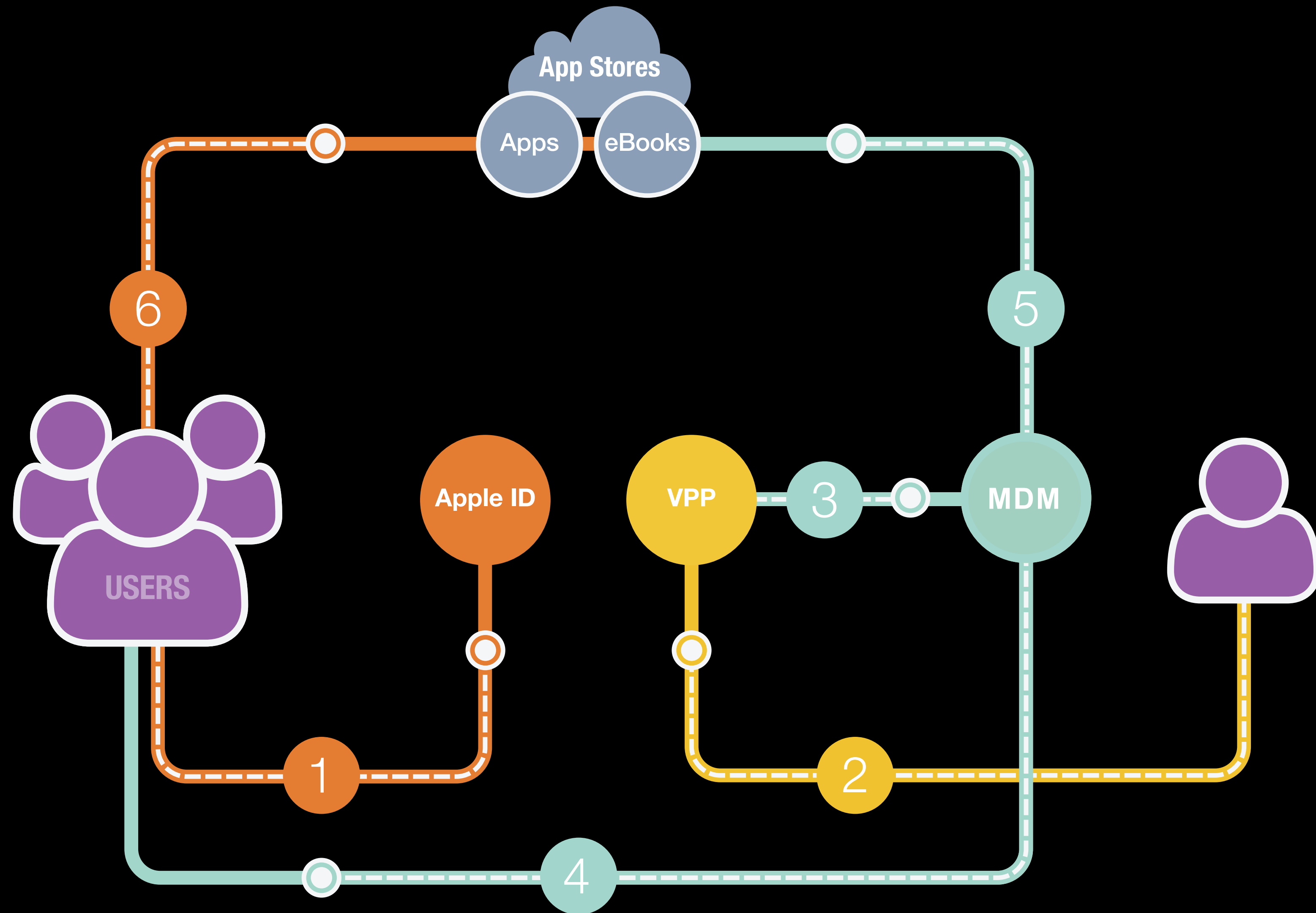
Hello

slide to set up



VOLUME PURCHASE PROGRAM (VPP)

- Bulk purchase of apps and books
- Assign content to users or devices
- Deploy using MDM
- Revoke and re-assign
- Custom B2B apps for iOS





Procure
to DEP enabled account



Ship
directly to user



DEP
automatic MDM enrollment



MDM
Profiles, remote commands



VPP
manage Apps, eBooks

'Zero Touch' Workflow





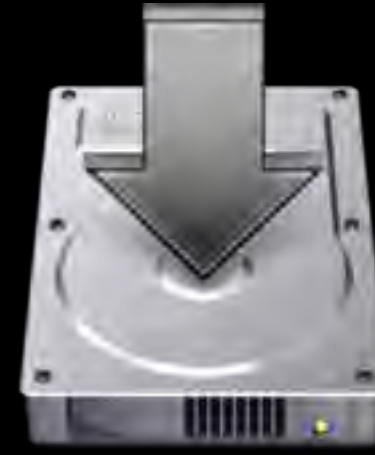
LINUX MANAGEMENT WORKFLOW



PXE Boot



Disk Partitioning



Bootstrapping



Packages



Configuration

OS X MANAGEMENT WORKFLOW

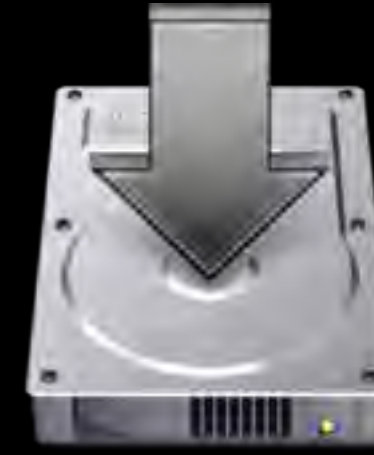


PXE Boot

NetBoot,
NetInstall



Disk Partitioning



Bootstrapping

Imaging



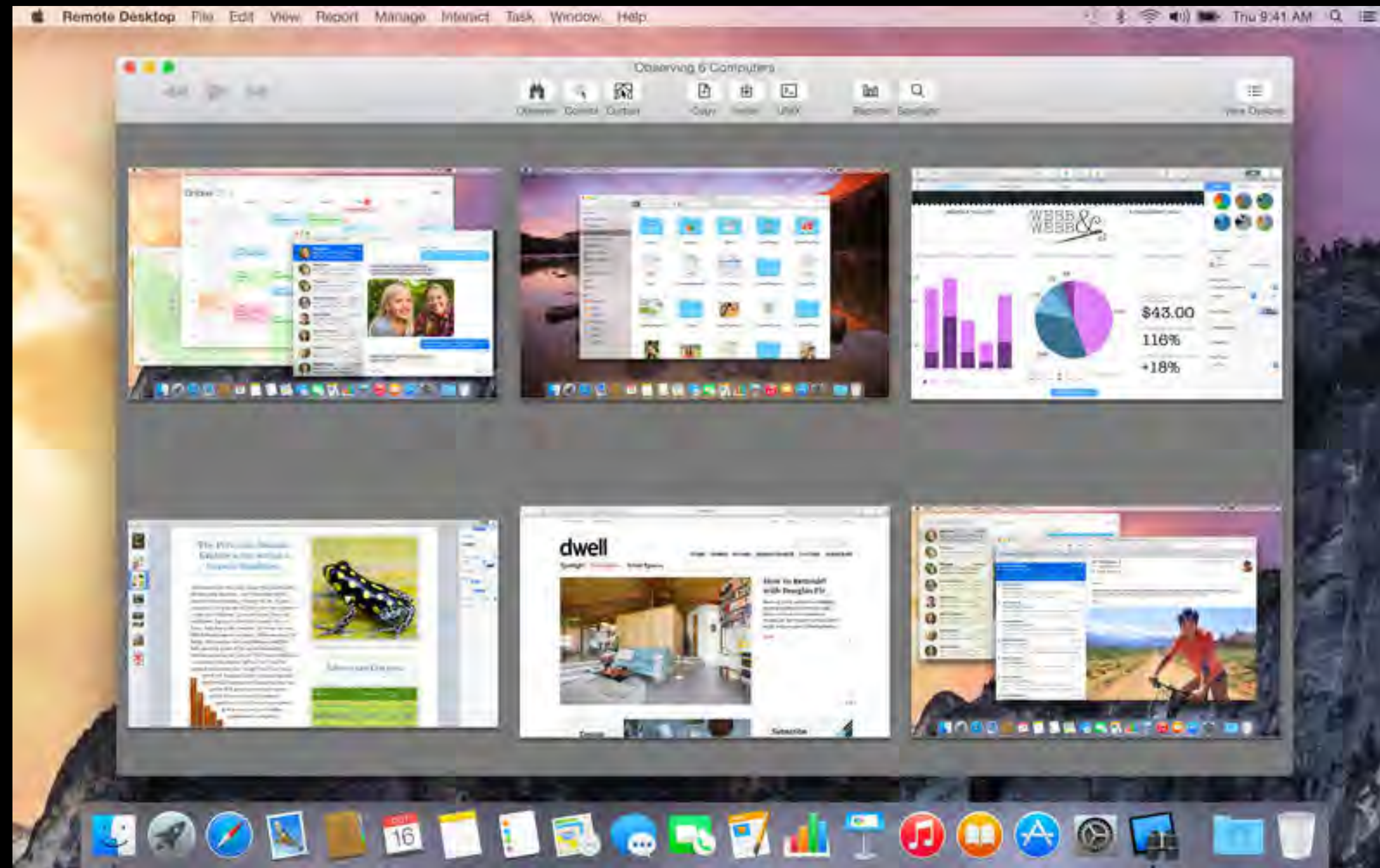
Packages



Configuration

Profiles,
MCX

APPLE REMOTE DESKTOP



BOOTING OVER THE NETWORK



- Apple BSDP – Boot Service Discovery Protocol 

<http://www.opensource.apple.com/source/bootp/bootp-170/Documentation/BSDP.doc>

- BSDP may coexist with any DHCP service
- OS X 10.11 adds security enhancements

`csrutil netboot add <address>` – <https://support.apple.com/en-gb/HT205054>

- BSDP Implementations

- Apple OS X Server NetInstall service 

- BSDPy – Python implementation of BSDP 

<https://bitbucket.org/bruienne/bsdpy>

- ISC DHCPD, TFTP, HTTP-Server (e.g. Apache2, nginx) 

- Justin Elliot: NetBoot Fundamentals and Customizations

<https://youtu.be/yKS2moLySi0>



NETBOOT IMAGE TYPES



- **NetBoot** – Boot a server based OS X image
 - Diskless requires AFP or NFS share to store 'shadow' files
 - Hack the OS X image to use a RAMDisk instead

<https://www.afp548.com/2011/02/01/serving-diskless-netboot-for-your-macs-without-os-x-server/>

- **NetInstall** – Boot an OS X installer
- **NetRestore** – Restore a volume using an `asr` disk image

NETWORK DISK IMAGE CREATION



- Manual

- Apple System Image Utility 

<https://support.apple.com/en-gb/HT202652>

<https://support.apple.com/en-gb/HT202061>

- Casper NetInstall Image Creator

<https://github.com/jamf/CasperNetInstallCreator>

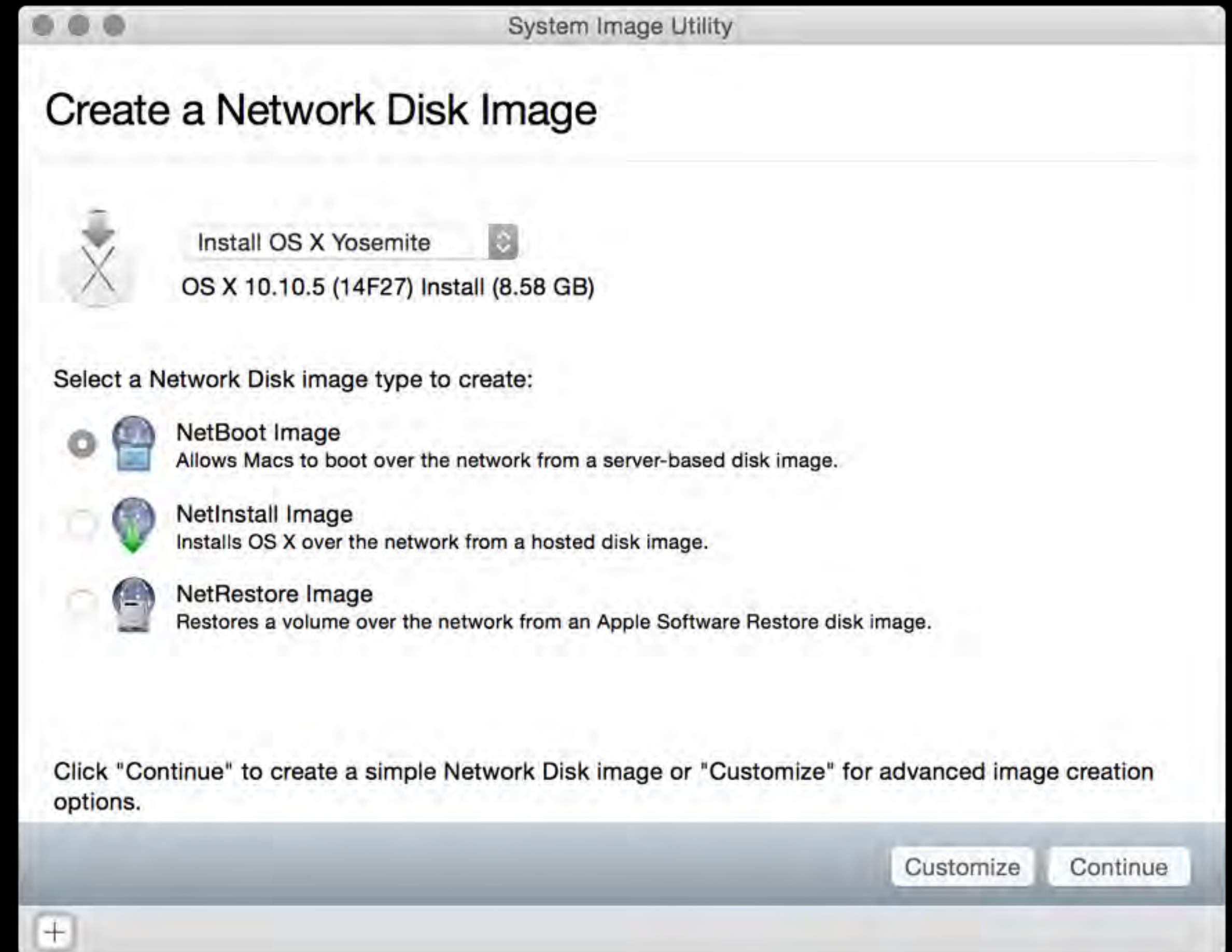
- AutoCasperNBI 

<https://github.com/macmule/AutoCasperNBI/>

- Scripted

- AutoNBI.py 

<https://bitbucket.org/bruienne/autonbi>





IMAGING TECHNIQUES



Thick Image



Hybrid Image



Thin Image



No Image

IMAGING SOFTWARE









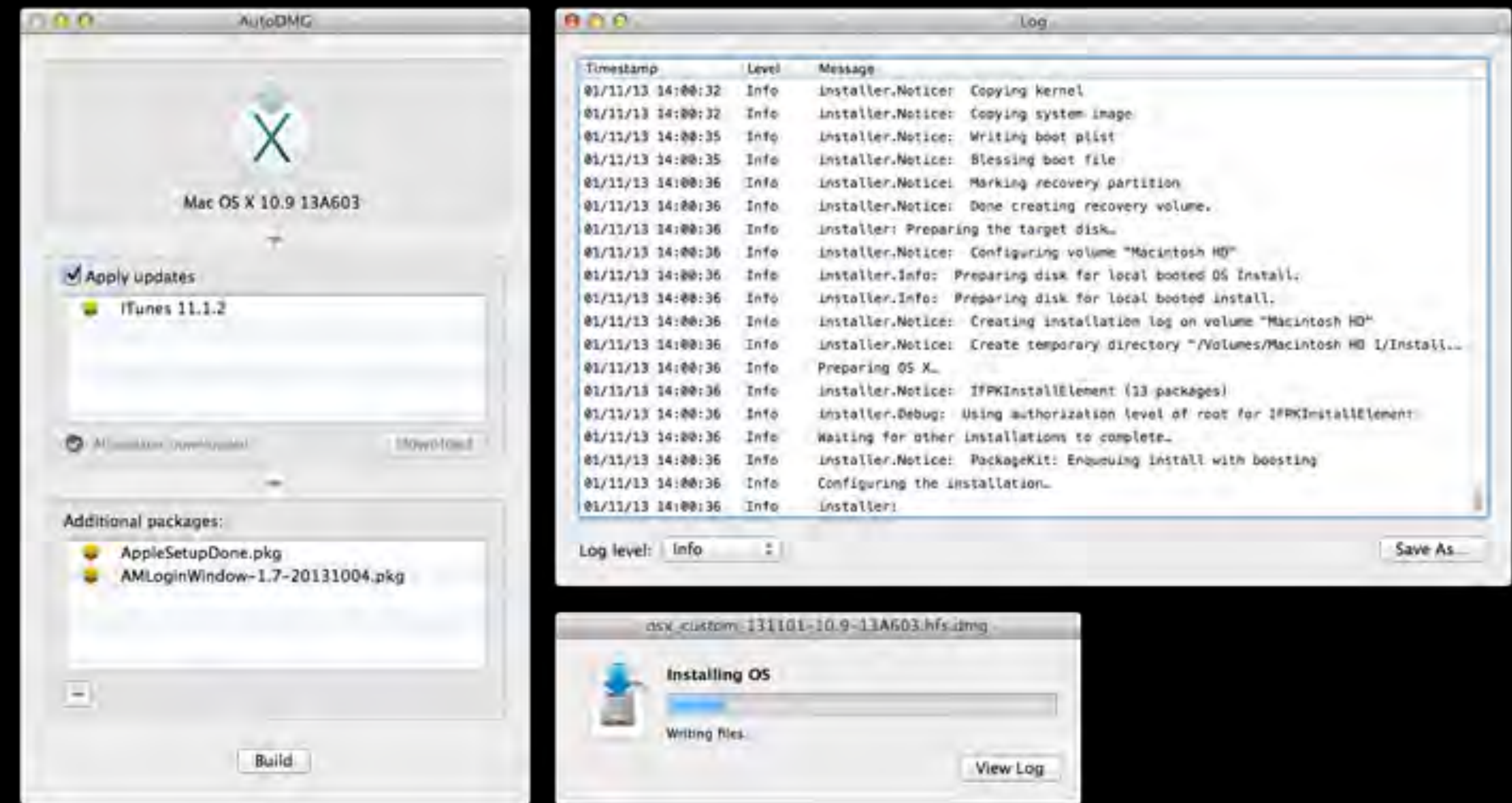
- **Apple asr** (and derived tools) 
- **Casper Imaging** €
www.jamfsoftware.com/products/casper-suite/
- **DeployStudio**
<http://www.deploystudio.com/>
- **Imagr** 
<https://github.com/grahamgilbert/imagr>
- **FileWave Imaging** €
<https://www.filewave.com/products/imaging/>
- **LANrev** (formerly known as Absolute Manage) €
<https://heatsoftware.com/lanrev/>



IMAGE CREATION



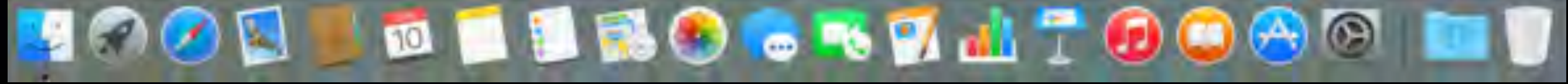
- **Apple Disk Utility** 
<https://support.apple.com/en-gb/HT202841>
- **AutoDMG** 
<https://github.com/MagerValp/AutoDMG>
- **Casper Composer** 
www.jamfsoftware.com/products/casper-suite/
- **FileWave Imaging** 
<https://www.filewave.com/products/imaging/>
- **NBICreator (beta)** 
<https://github.com/NBICreator/NBICreator>




SKYNET

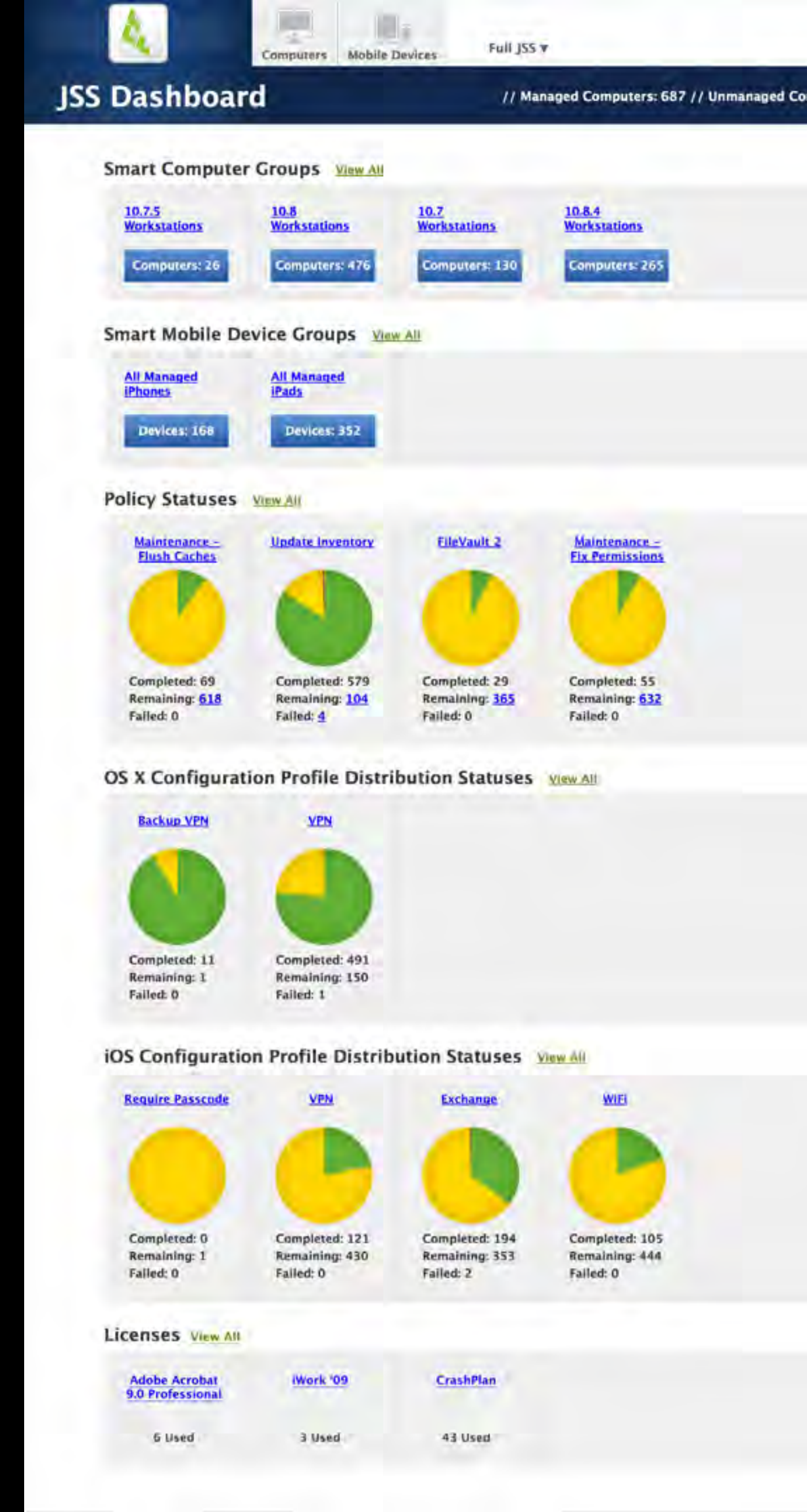


CYBERDYNE
SYSTEMS

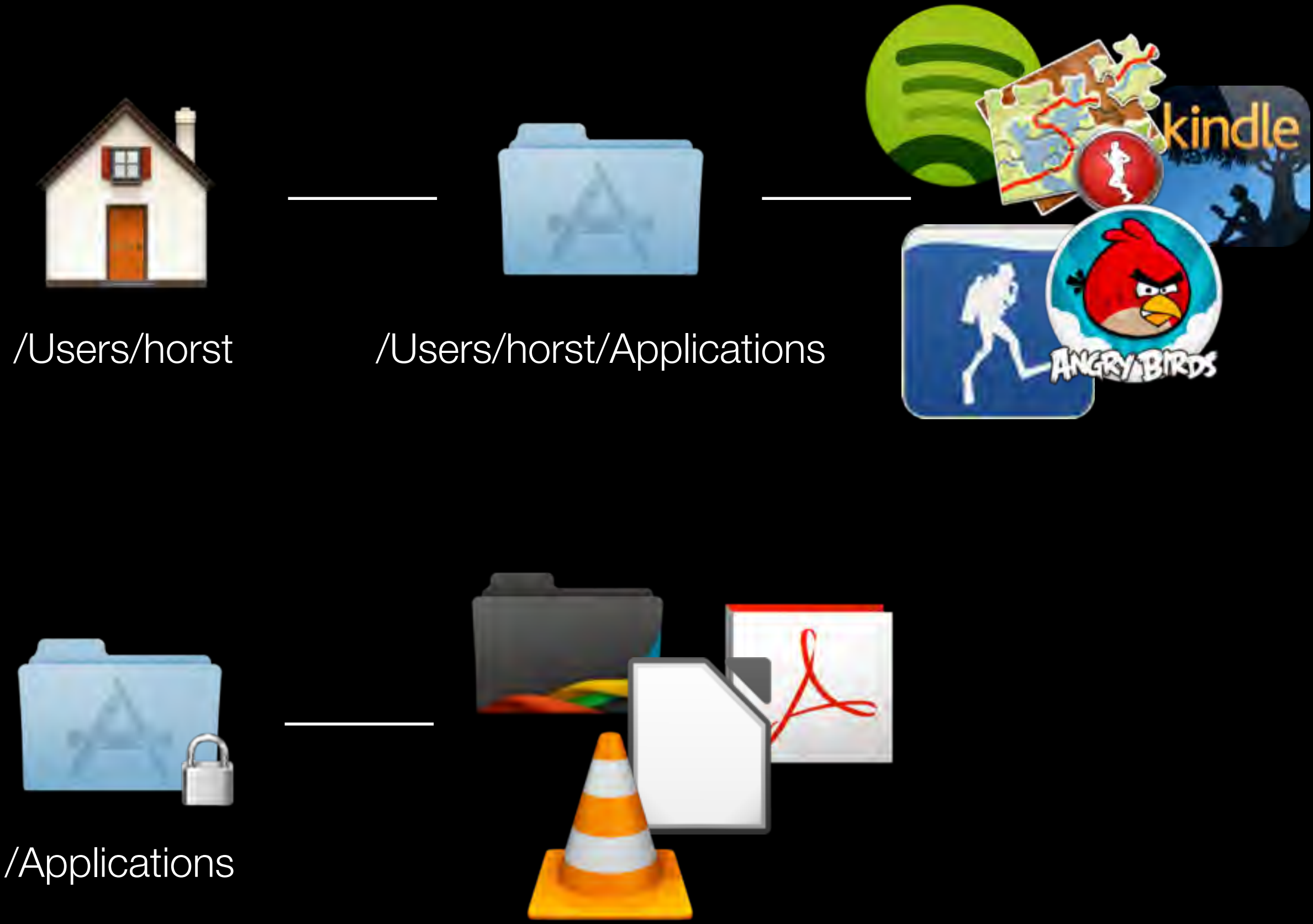


INVENTORY & MANAGEMENT

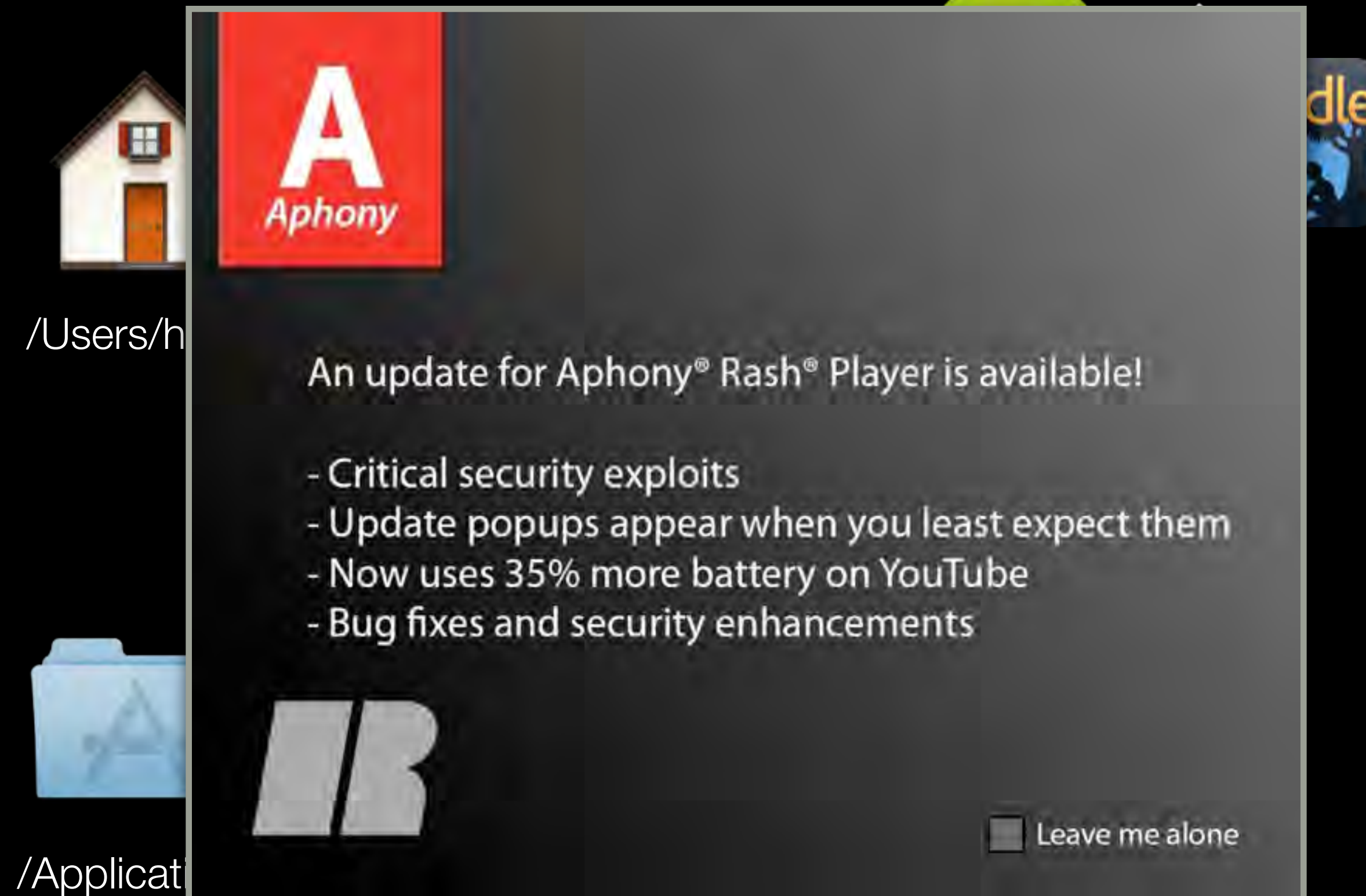
- **Filewave** €
<https://www.filewave.com/>
- **HEAT LANrev** (formerly Absolute Manage) €
<https://heatsoftware.com/lanrev/>
- **JAMF Casper Suite** €
<http://www.jamfsoftware.com/products/casper-suite/>
- **Microsoft System Center Configuration Manager (SCCM)** €
<https://www.microsoft.com/en/server-cloud/products/system-center-configuration-manager/>
- **SAL+** € **SAL** 
<http://salsoftware.com/> <https://github.com/salsoftware/sal>



CHALLENGE: APPLICATIONS



CHALLENGE: APPLICATIONS



The OS X platform lacks a package manager like apt, yum or zypper



- System administrator friendly toolset
 - text based configuration
 - powerful command line tools

- Friendly user interface:
Managed Software Center.app

- Excellent tool ecosystem








- MacSysadmin 2014 – G. Neagle:

WHAT'S NEW WITH MUNKI?

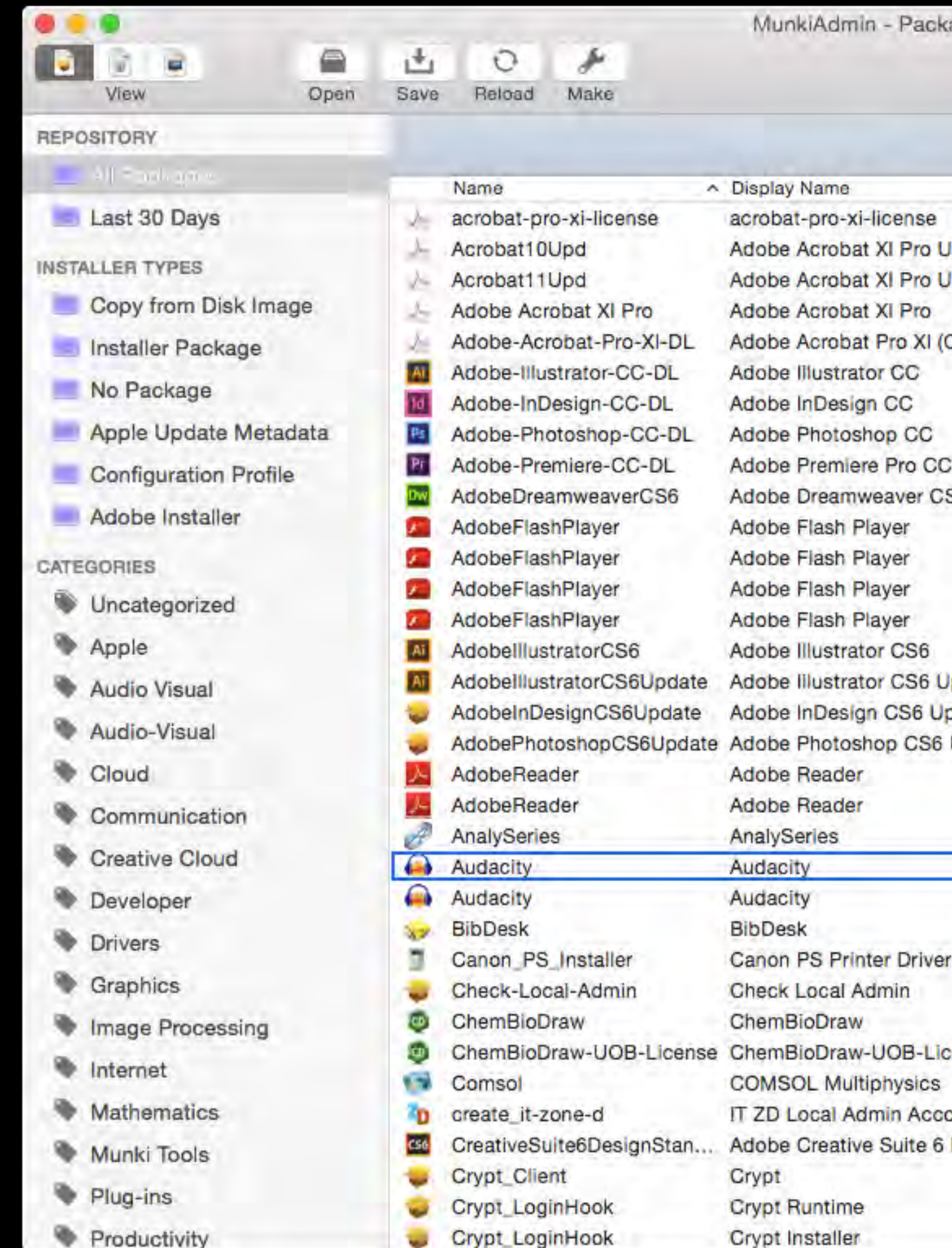
<http://docs.macsysadmin.se/2014/2014doc.html>




MUNKI ECOSYSTEM

- **MunkiAdmin**  <https://github.com/hjuutilainen/munkiadmin>
- **SAL**  <https://github.com/salsoftware/sal>
- **munkireport-php**  <https://github.com/munkireport/munkireport-php>
- **MunkiWebAdmin**  <https://github.com/munki/munkiwebadmin>
- **munki-staging**  <https://github.com/ox-it/munki-staging>
- **Simian**  <https://github.com/google/simian>
- **Manana**  <https://github.com/ox-it/manana>

and many many more <https://github.com/timsutton/python-macadmin-tools#munki>



- Automated preparation of software for managed distribution
- Community maintained recipes (PropertyList XML) to automate complex tasks
 - `Firefox.download.recipe`
 - `Firefox.pkg.recipe`
 - `Firefox.munki.recipe`
- Excellent integration with Munki
- Workflows for other management tools like Absolute Manage, JAMF Casper Suite
- Recipe Robot 
<https://github.com/homebysix/recipe-robot>
- MacSysadmin 2014– G. Neagle, T. Sutton
AUTOPKG: CROWD-SOURCING MAC PACKAGING AND DEPLOYMENT
<http://docs.macsysadmin.se/2014/2014doc.html>

CHALLENGE: OS X RELEASES



CHALLENGE: OS X RELEASES










UNIVERSITY OF
OXFORD

10.10.5	14F1509	
10.10.4	14E46	
10.10.3	14D131	14D136
10.10.2	14C109	14C1510, 14C1514, 14C2043, 14C2513
10.10.1	14B25	
10.10	14A389	



SOLUTION: IN-PLACE UPGRADES



- Minor version updates:
 - Apple Software Update based workflows   
- Software Update Servers:
 - Apple SUS as part of Server
 - Reposado 
<https://github.com/wdas/reposado>
 - Margarita 
<https://github.com/jessepeterson/margarita>
- Major version updates:
 - All commercial management suites provide workflows 
 - createOSXinstallPkg 
<https://github.com/munki/createOSXinstallPkg>



CHALLENGE: CONFIGURATION



- Several configuration methods
 - defaults / plists
 - MCX
 - Profiles
 - **proprietary** (files, databases)
- Configuration caching using `cprefsd` (introduced 10.9)

```
oucs0089 — man cfprefsd — less — 80x17
man

CFPREFSD(8)                BSD System Manager's Manual                CFPREFSD(8)

NAME
    cfprefsd — defaults server

SYNOPSIS
    cfprefsd



DESCRIPTION
    cfprefsd provides preferences services for the CFPreferences and
    NSUserDefaults APIs.

    There are no configuration options to cprefsd manually.

Mac OS X                    October 25th, 2011                    Mac OS X
(END)
```

SOLUTION: CONFIGURATION MANAGEMENT



- Profiles & MDM
- Configuration management tools:
 - **chef** 
<https://www.chef.io/chef/>
 - **puppet** 
<https://puppetlabs.com/puppet/puppet-open-source>
- Use scripts in combination with (payload free) packages
 - idempotency
 - use Apple tools wherever possible
- All commercial management suites provide workflows €





ENCRYPTION: FILEVAULT2

- Require & enforce FileVault2 via Profile
- Recovery key escrow solutions
 - Cauliflower Vest 
<https://github.com/google/cauliflowervest>
 - Crypt 
<https://github.com/grahamgilbert/Crypt>
 - Most commercial management suites €



SECURITY: MORE USEFUL TOOLS



- **osquery** – endpoint visibility 
<https://osquery.io/>
- **Plan B** – remediation for managed Macs 
<https://github.com/google/macops-planb>
- **Santa** – binary whitelisting/blacklisting system 
<https://github.com/google/santa>
- **Zentral** – Elasticsearch based infrastructure event handler 
<https://github.com/zentralopensource/zentral>



OFFICIAL REFERENCES



iOS Deployment Reference



<http://help.apple.com/deployment/ios/>

OS X Deployment Reference



<http://help.apple.com/deployment/osx/>

Apple Developer Program



<http://developer.apple.com>

Orchard – OS X MANAGEMENT



DEP



MDM



Profiles



AD Binding



VPP



Munki



Branding



Non-App Store



Updates



NetBoot & Imaging

KEY LESSONS LEARNED



- Never fight against Apple's tools and workflows
 - Use the Device Enrollment Program
 - Use the App Store (and VPP)
- Trust your users – don't be the evil BOFH
- Automate
- Don't be afraid to ask for help – join the *Mac admin community on Slack*

<http://macadmins.org>



VIELEN DANK!

 <https://github.com/mjung/publications>

MARKO JUNG

GALACTIC VICEROY OF RESEARCH EXCELLENCE

 m@mju.ng

 [@mjung](https://twitter.com/mjung)

 fb.com/markohjung