Ditch Imaging
Modern Mac Deployment Workflows

Nathaniel Strauss

IT Manager

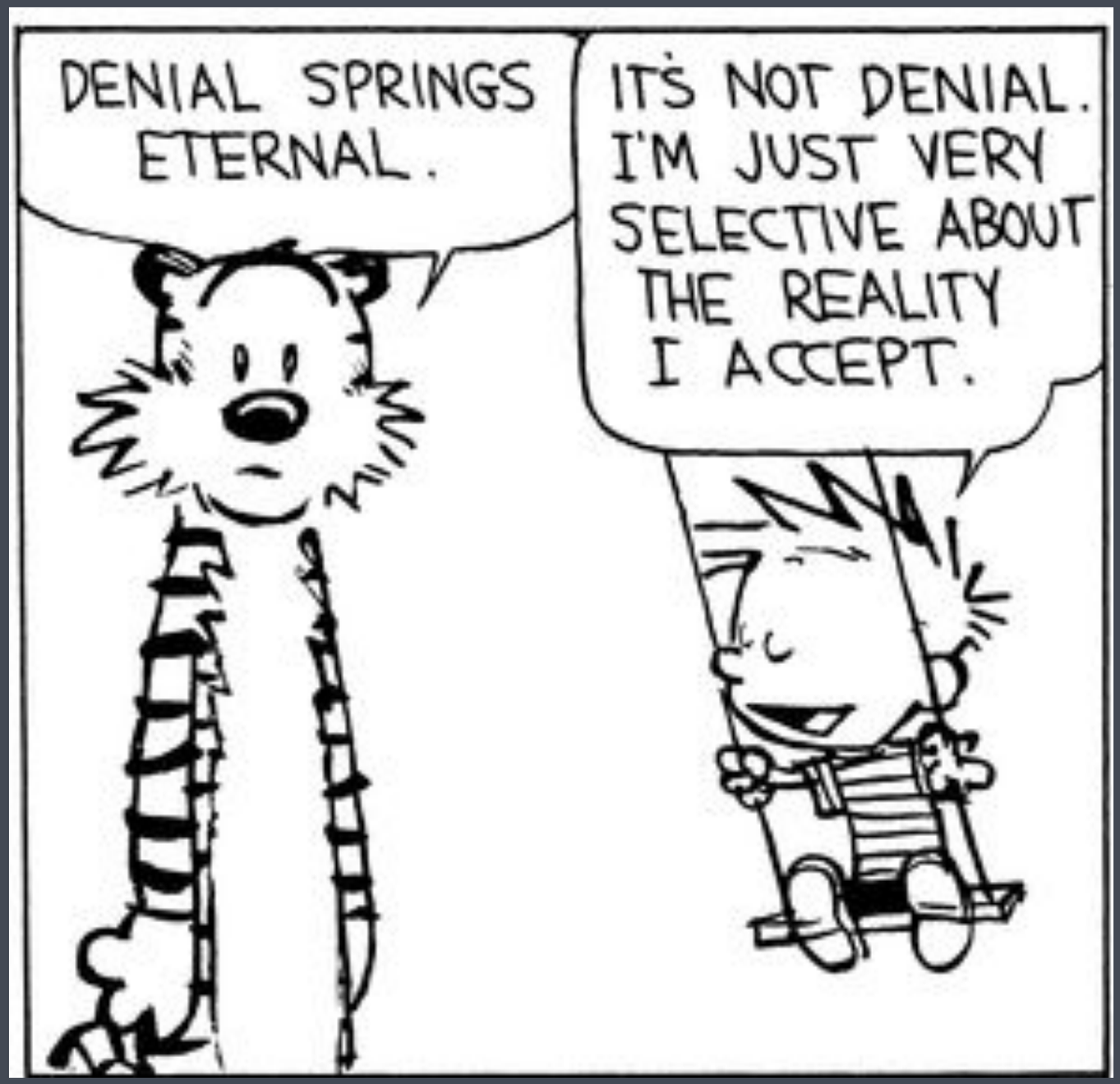
Shakopee Public Schools

- 8,000 students
- 1,200 staff
- 4,500 Macs
- 6,500 iPads

Topics

- Why not imaging?
- MDM
- Local vs. mobile accounts
- New tools
  - installr
  - NoMAD Login
  - NoMAD
- New workflows

#imagingisdead



What is Imaging?

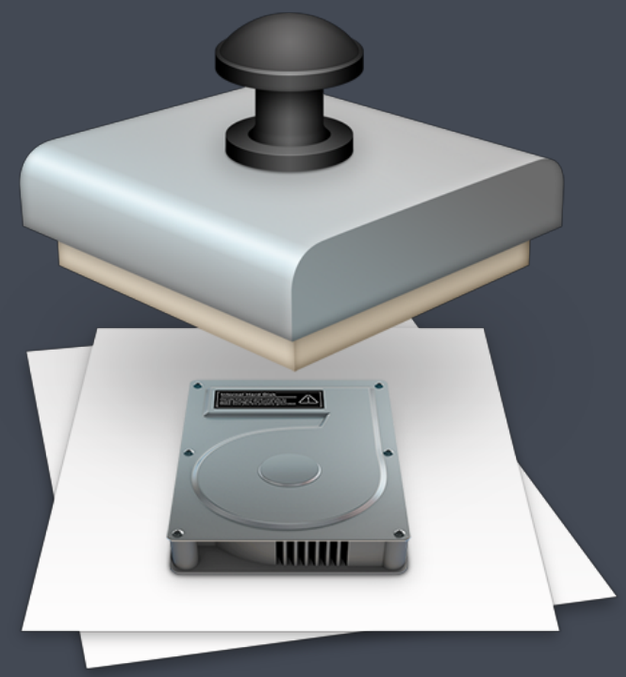
CARBON COPY
CLONER

Jamf **Imaging**

Imaging

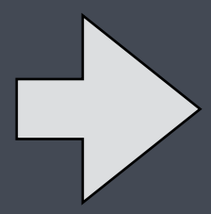
Block copying a preinstalled and or preconfigured OS to a formatted volume.

- Not model aware
- No logic for firmware
- Bad configuration practices



Traditional Imaging Workflow

Format Disk



Copy ASR Image

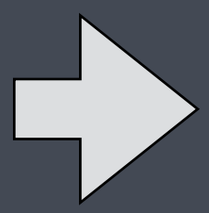
Bind to LDAP

Install Packages

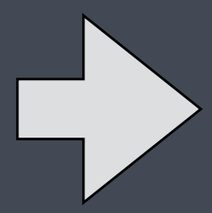
Deployed

Installer + DEP + New Tools = 😀

installr



DEP/MDM



Setup Assistant

NoMAD Login

NoMAD

Deployed

Deployment Workflow Goals

- Standardized and consistent
- Conforms to organization policies and identity
- Reliable
- Efficient

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

Back

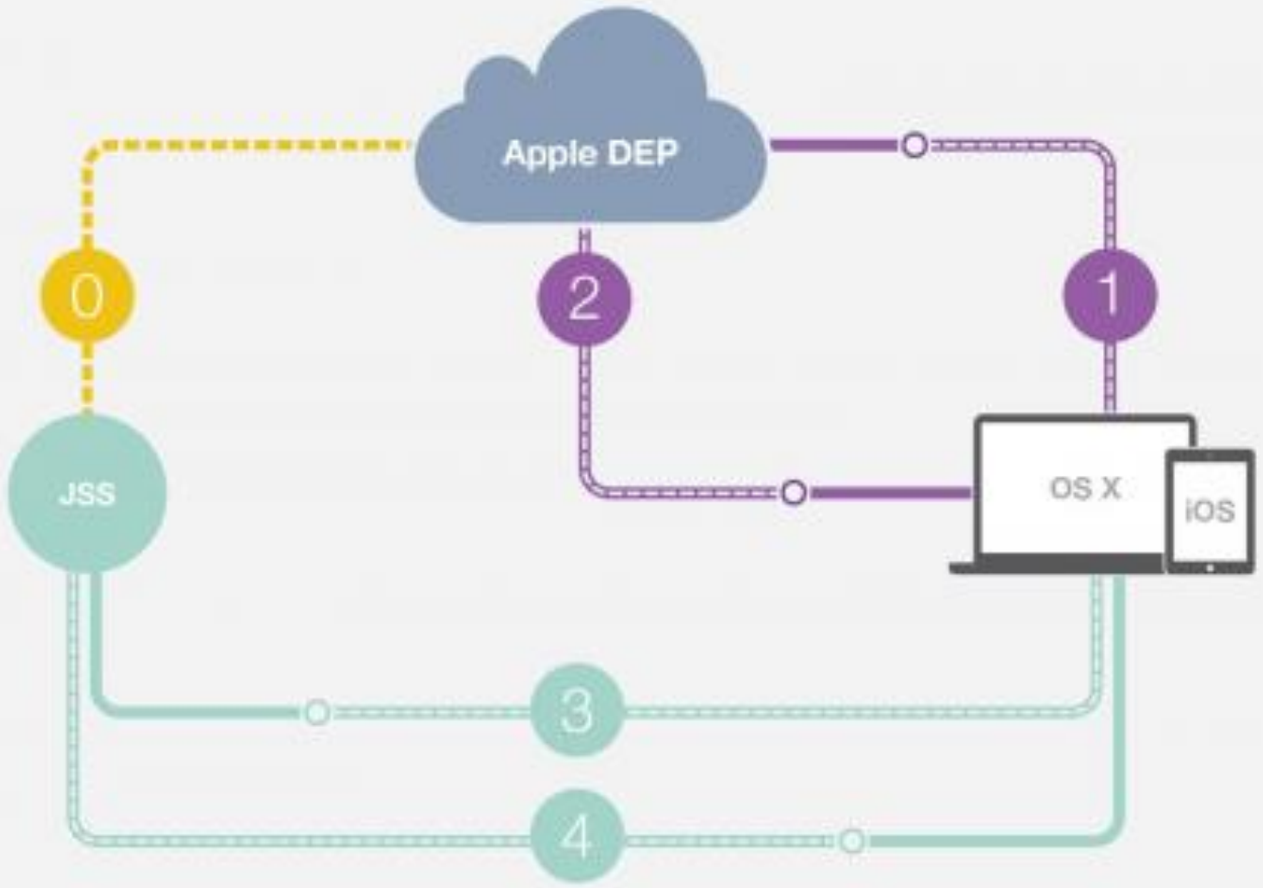
Continue

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.

MDM

- Managing Macs without MDM will not be possible in the future
- UAMDM - User Approved MDM
  - Compare to iOS supervision
- Required to manage kernel extensions and TCC/PPPC
- Paths to UAMDM - DEP enrollment or physical click

DEP



DEP enrollment with the Casper Suite

0 Setup: connect JSS with Apple DEP service

1 During activation, device checks in with Apple DEP service

2 DEP service returns the enrollment details for the Casper Suite server

3 Device enrolls with the Casper Suitet

4 After enrollment, configuration profiles are installed

macOS Installer

- Model and board aware
- Includes firmware
- Converts to APFS
- Provides a known good OS without modification

Using the Installer

- Recovery
- ~30 minutes depending on hardware
- startosinstall

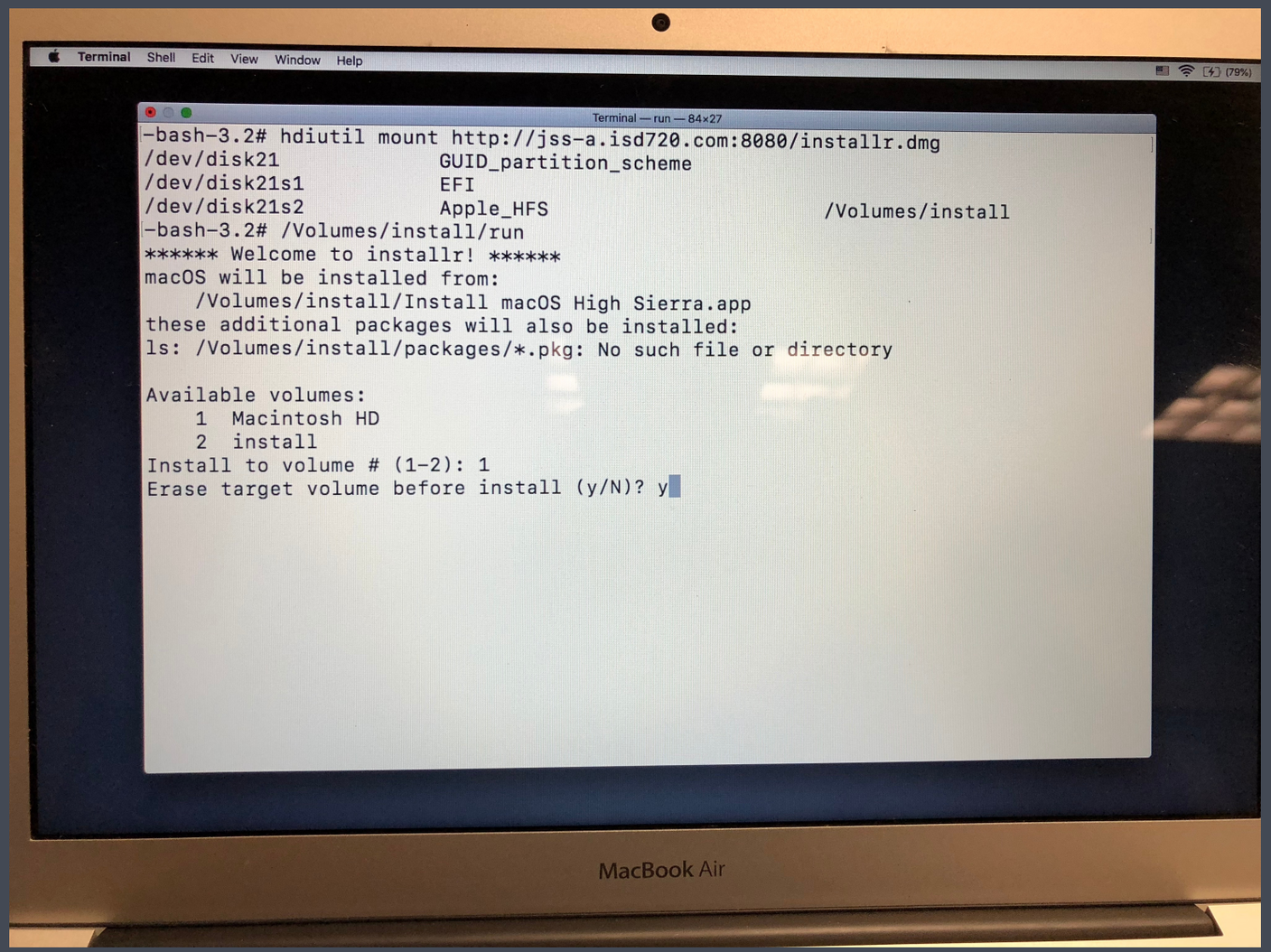
	Action
Command (⌘)-R	Install the latest macOS that was installed on your Mac.
Option-⌘-R	Upgrade to the latest macOS compatible with your Mac.
Shift-Option-⌘-R	Install the macOS that came with your Mac, or the closest version still available.

installr

- Command line tool designed to be run in recovery
- Install from USB or network location
- Can include packages - bootstrap management tools like munki
- Format disk and install a good known OS using startosinstall
- https://github.com/munki/installr

Running installr

```
# Mount installr DMG from network location
$ hdiutil mount http://mydmg.domain.com/installr.dmg

# Run installr
/Volumes/install/run
```



Local Accounts Good, AD Bad

	Local Account	Mobile Account	Network Account
Authority	Local Directory Service	LDAP	LDAP
Account Info	Local	Cached	Network
LDAP Binding	Not Required	Required	Required

Why Local?

- About what authority controls the keys
- Always available
- Avoid AD plugin
- No more keychain issues
- AD functionality without binding

DEP Setup Assistant

Allows authentication to MDM, but…

- Can’t force username
- Can’t force password
- Can’t guarantee either will match existing LDAP or identity management provider

Log in with your district username and password

12345678

password

Cancel | Log In

This Mac will be configured automatically by "Shakopee School District 720"

For further assistance, contact "Shakopee School District 720" at:
(952) 496-5100 — jjacobso@shakopee.k12.mn.us

Administrators may restrict access to apps and features, install and remove apps, remotely erase this Mac, and monitor Internet traffic.

Back Continue

Create a Computer Account

Fill out the following information to create your computer account.

Full name:

Account name:

This will be the name of your home folder.

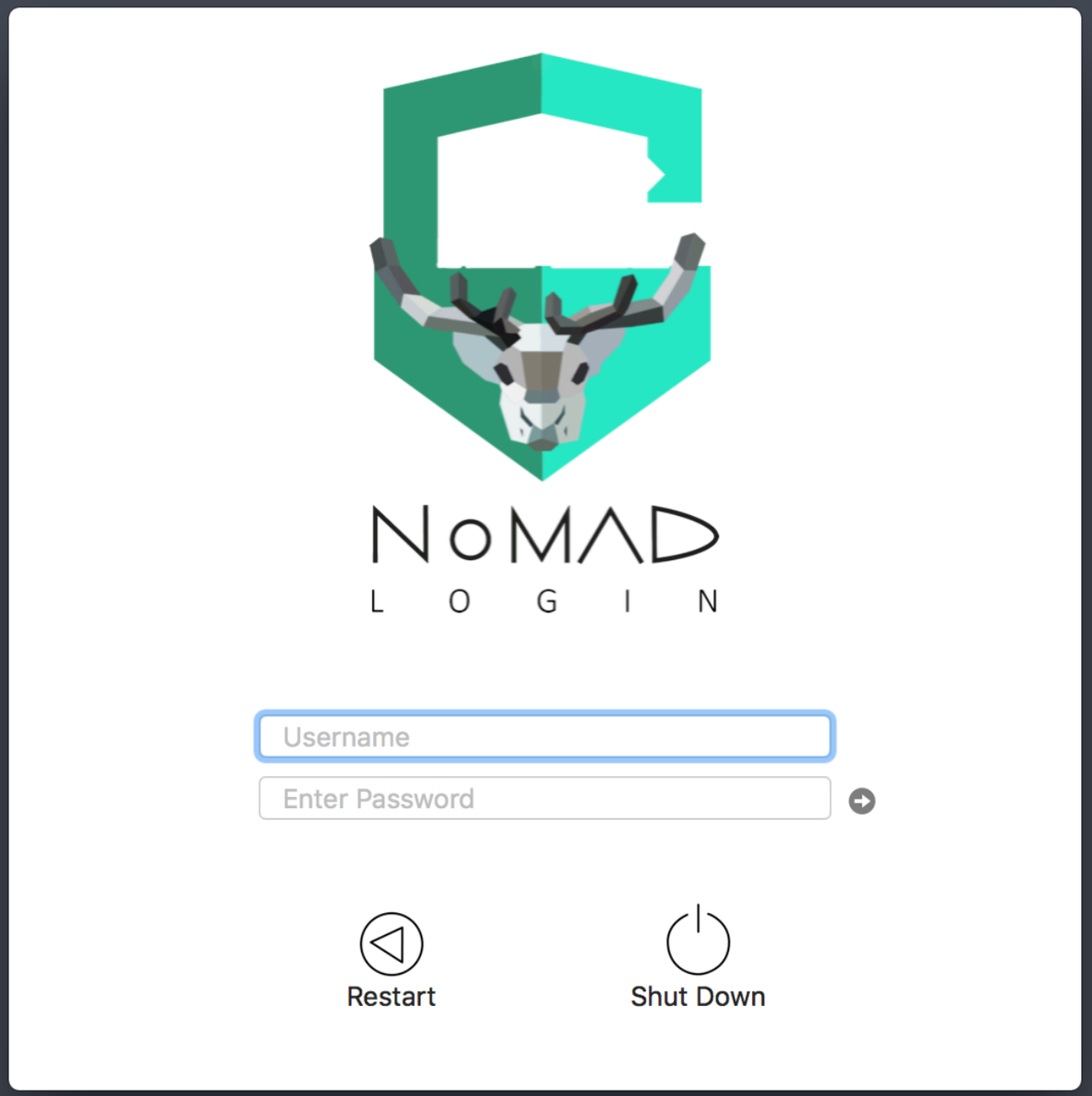
Password: new password verify

Hint: optional

Set time zone based on current location

Back Continue

Enter NoMAD Login

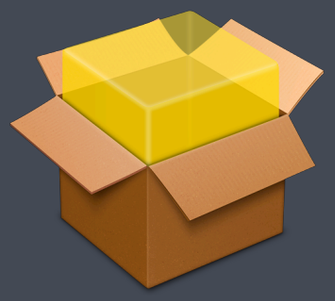


What is NoMAD Login?

Login window authorization plugin

- Creates local accounts based on AD users
- Replaces default login window
- Lives in /Library/Security/SecurityAgentPlugins
- Controlled by authorization mechanisms

Deploying NoMAD Login



Package

Auth Mechs

Preferences

Authorization Mechanisms

An authorization mechanism is code that performs a step in the authorization process.

- Run in order at the login window
- One mechanism defines one function
- References code in NoMADLoginAD.bundle

```
$ security authorizationdb read system.login.console
$ authchanger -print
```

authchanger

- Utility to read and write authorization mechanisms
- Included in all flavors
- Preferred over security commands

authchanger - Default

```
$ authchanger -print  builtin:policy-banner
                      loginwindow:login
                      builtin:login-begin
                      builtin:reset-password,privileged
                      builtin:forward-login,privileged
                      builtin:auto-login,privileged
                      builtin:authenticate,privileged
                      PKINITMechanism:auth,privileged
                      builtin:login-success
                      loginwindow:success
                      loginwindow:FDESupport,privileged
                      HomeDirMechanism:login,privileged
                      HomeDirMechanism:status
                      MCXMechanism:login
                      CryptoTokenKit:login
                      loginwindow:done
```

authchanger - NoMAD Login

```
$ authchanger -AD
```

```
builtin:policy-banner
NoMADLoginAD:CheckAD
NoMADLoginAD:EULA
NoMADLoginAD:PowerControl,privileged
NoMADLoginAD:CreateUser,privileged
NoMADLoginAD:DeMobilize,privileged
builtin:login-begin
builtin:reset-password,privileged
builtin:forward-login,privileged
builtin:auto-login,privileged
builtin:authenticate,privileged
PKINITMechanism:auth,privileged
builtin:login-success
loginwindow:success
loginwindow:FDESupport,privileged
HomeDirMechanism:login,privileged
HomeDirMechanism:status
MCXMechanism:login
CryptoTokenKit:login
loginwindow:done
NoMADLoginAD:EnableFDE,privileged
NoMADLoginAD:SierraFixes,privileged
```

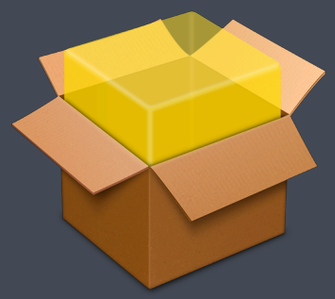
Settings Preferences with Defaults

```
#!/bin/bash

# Variables
domain="mydomain.COM"
background_image="/Library/Desktop Pictures/High Sierra.jpg”
logo="/Library/Application Support/SPS/spslogo.png"

# Write default AD domain
defaults write /Library/Preferences/menu.nomad.login.ad ADDomain $domain

# Set login window logo
defaults write /Library/Preferences/menu.nomad.login.ad LoginLogo $logo

# Set background image
defaults write /Library/Preferences/menu.nomad.login.ad BackgroundImage
$background_image
```

NoMAD

- Menu bar application
- Syncs local password with AD
- File share mounting
- Shortcuts for common tasks
- And more!

Deploying NoMAD



LaunchAgent

Preferences

NoMAD LaunchAgent

```
<?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>KeepAlive</key>
    <true/>
    <key>Label</key>
    <string>com.trusourcelabs.NoMAD</string>
    <key>LimitLoadToSessionType</key>
    <string>Aqua</string>
    <key>Program</key>
    <string>/Applications/Utilities/NoMAD.app/Contents/MacOS/NoMAD</string>
    <key>RunAtLoad</key>
    <true/>
</dict>
</plist>
```

NoMAD Preferences

- https://nomad.menu/help/standard-preferences/
- ADDomain
- RenewTickets
- LocalPasswordSync
- UseKeychain
- UPCAlert

Resources

- http://bit.ly/brainstorm-macdeploy
- MacAdmins Slack!
  - https://macadmins.herokuapp.com/