Replacing NetBoot: T2 chip, MDS, Imagr,

James Reynolds

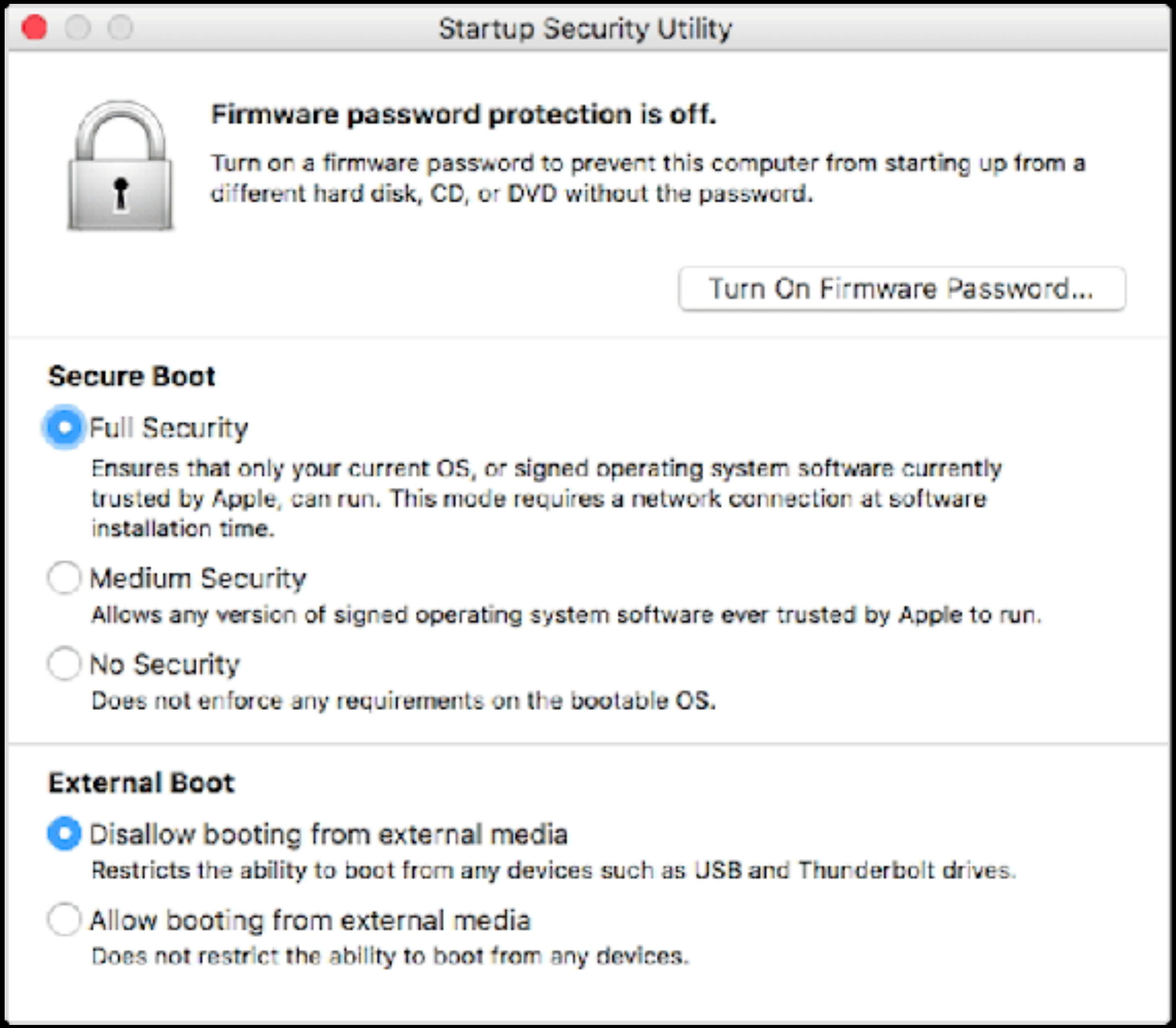
NetBoot

- Mac OS X Server 1.0 Rhapsody
- Macs w/ New World ROM
  - Allows booting to network image (or external drives)
- Client boots, obtains DHCP info, contacts a BSDP server, downloads Mac OS 8, 9, or 10 dmg OS image.
- BSDP - an extension to DHCP (option 43 and 60)
- VERY COOL STUFF

RIP NetBoot (1999-2019?) 10.13+

- T2 chip
  - Oct 2018 Mac Mini (150+ days)
  - Oct 2018 MacBook Air (150+ days)
  - Jul 2018 MacBook Pro (250+ days)
  - Dec 2017 iMac Pro (450+ days)
- No T2 chip
  - Mar 2019 iMac (1 day)
  - Jun 2017 MacBook (650+ days)
  - Dec 2013 Mac Pro (1900+ days)

Secure Boot



Firmware password protection is off.

Turn on a firmware password to prevent this computer from starting up from a different hard disk, CD, or DVD without the password.

Secure Boot

● Full Security
Ensures that only your current OS, or signed operating system software currently trusted by Apple, can run. This mode requires a network connection at software installation time.

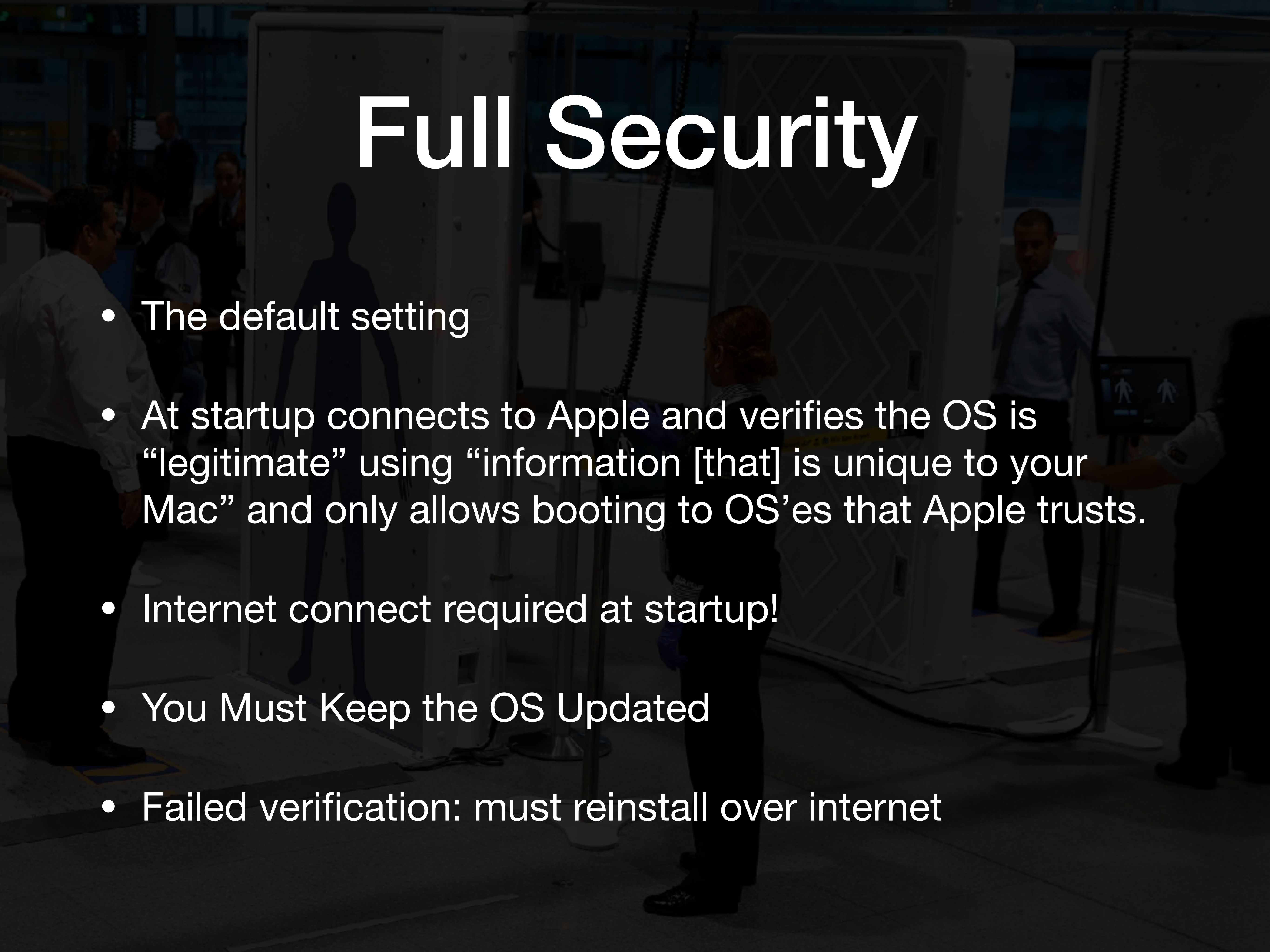
○ Medium Security
Allows any version of signed operating system software ever trusted by Apple to run.

○ No Security
Does not enforce any requirements on the bootable OS.

External Boot

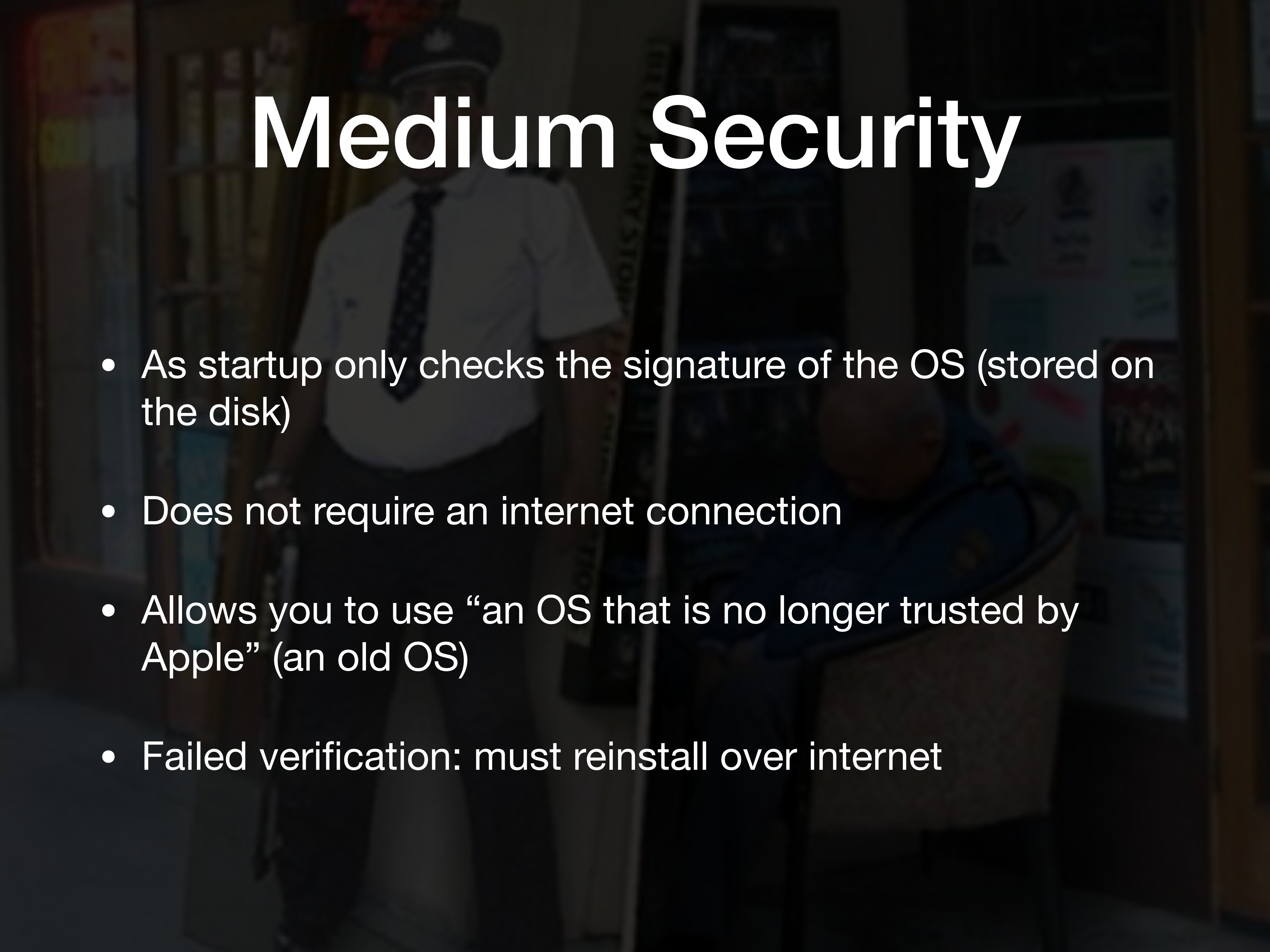
● Disallow booting from external media
Restricts the ability to boot from any devices such as USB and Thunderbolt drives.

○ Allow booting from external media
Does not restrict the ability to boot from any devices.



Full Security

- The default setting
- At startup connects to Apple and verifies the OS is “legitimate” using “information [that] is unique to your Mac” and only allows booting to OS’es that Apple trusts.
- Internet connect required at startup!
- You Must Keep the OS Updated
- Failed verification: must reinstall over internet

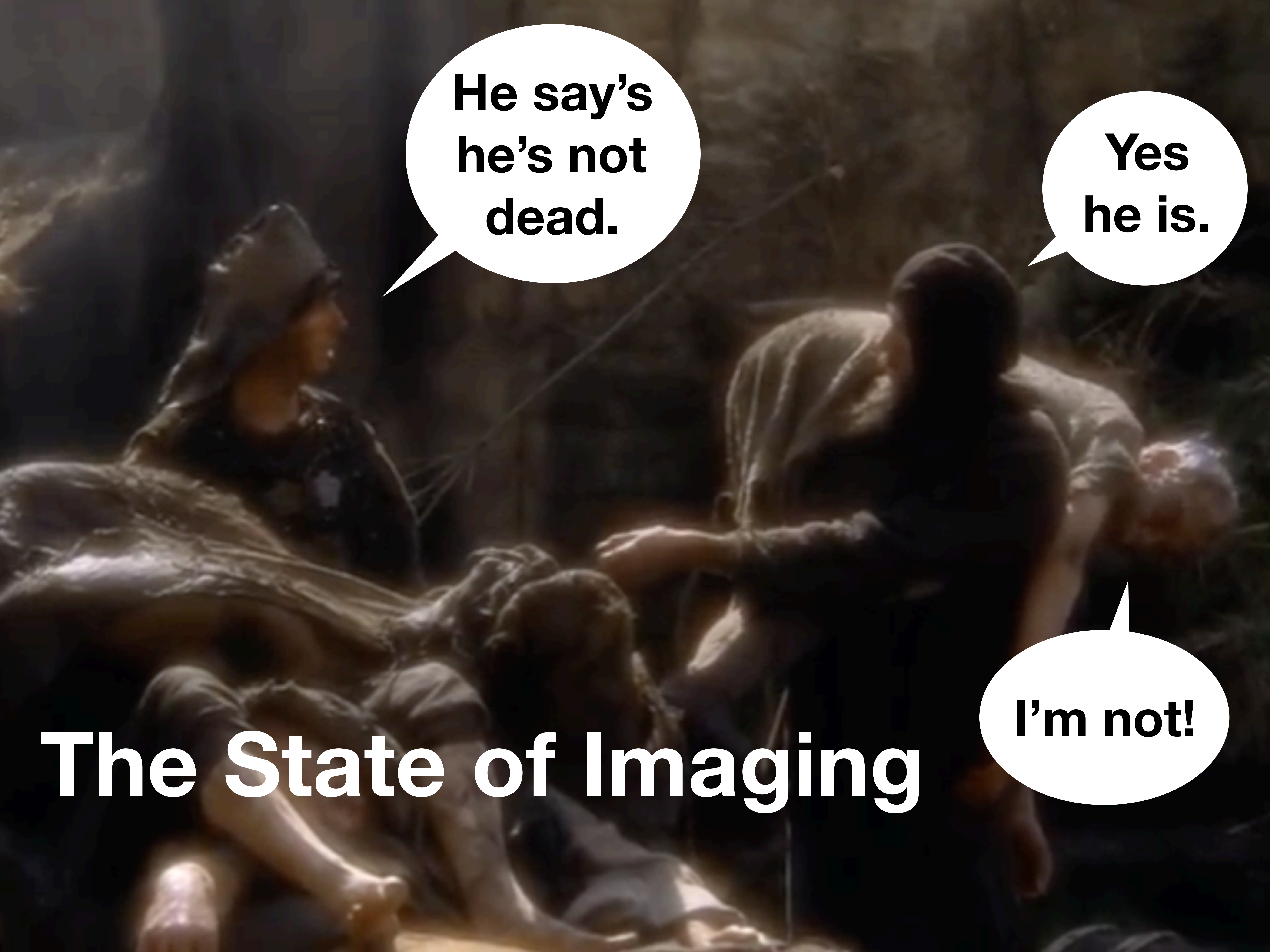


Medium Security

- As startup only checks the signature of the OS (stored on the disk)
- Does not require an internet connection
- Allows you to use “an OS that is no longer trusted by Apple” (an old OS)
- Failed verification: must reinstall over internet

“No Security”

The State of Imaging

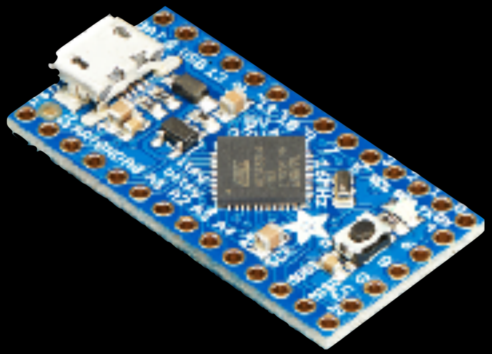


MDS 1.4

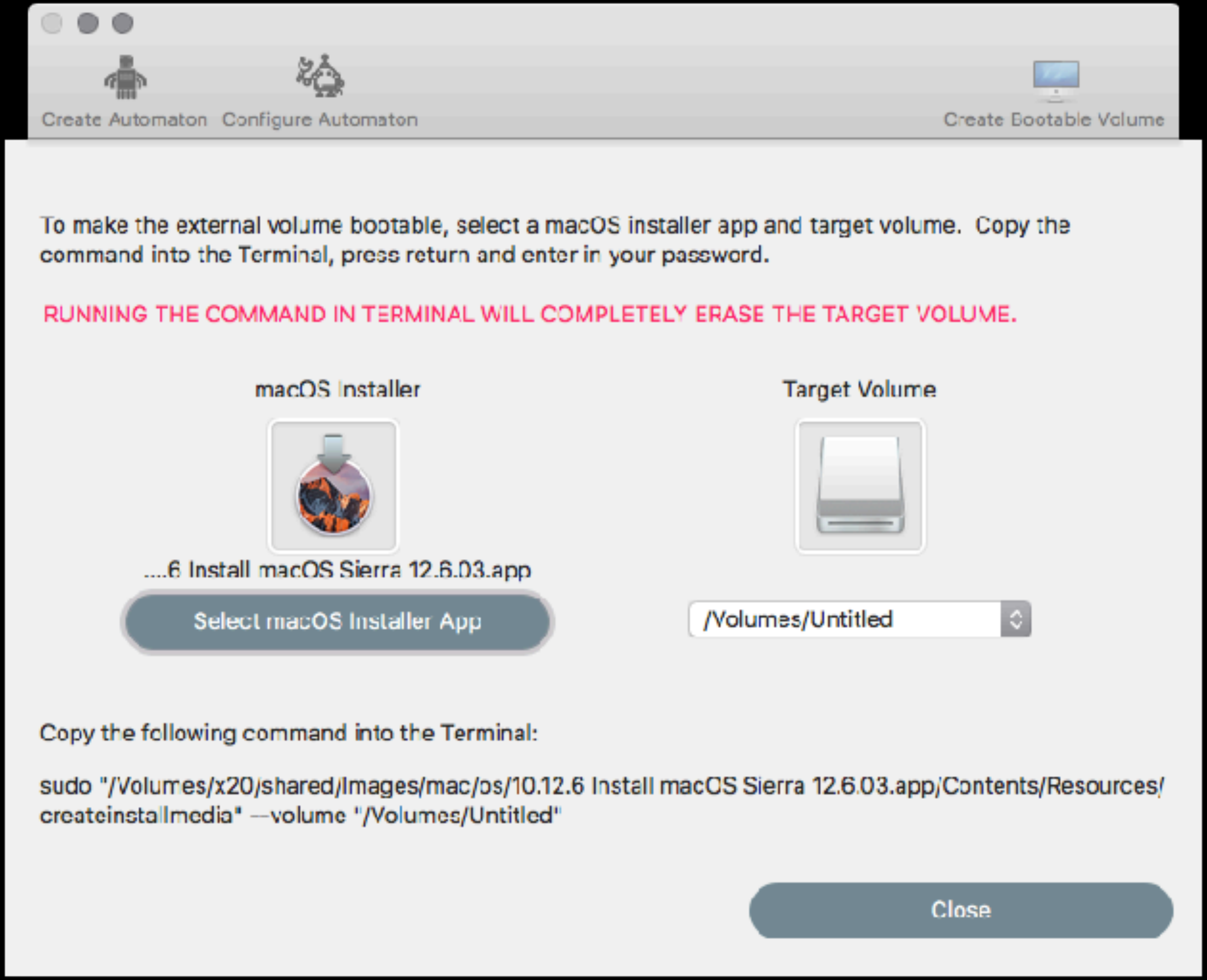
- Mac Deployment Stick (MDS) by Two Canoes
- A tool of tools
- Open Source
- Boot to the Recovery Partition (instead of a NetBoot image) and image from there

MDS.app Tasks

- Create bootable volume
- “Automaton”
  - Arduino Micro
  - Adafruit ItsyBitsy
- “Deploy” stuff on external HD or DMG



Create Bootable Volume



To make the external volume bootable, select a macOS installer app and target volume. Copy the command into the Terminal, press return and enter in your password.

RUNNING THE COMMAND IN TERMINAL WILL COMPLETELY ERASE THE TARGET VOLUME.

macOS Installer: ....6 Install macOS Sierra 12.6.03.app

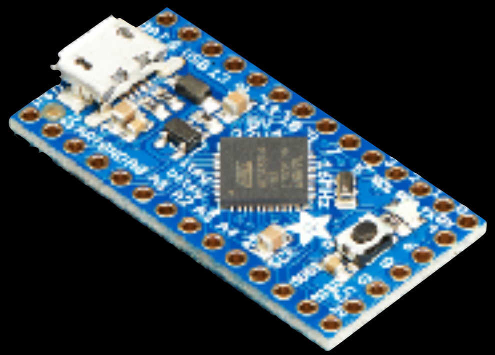
Target Volume: /Volumes/Untitled

Copy the following command into the Terminal:

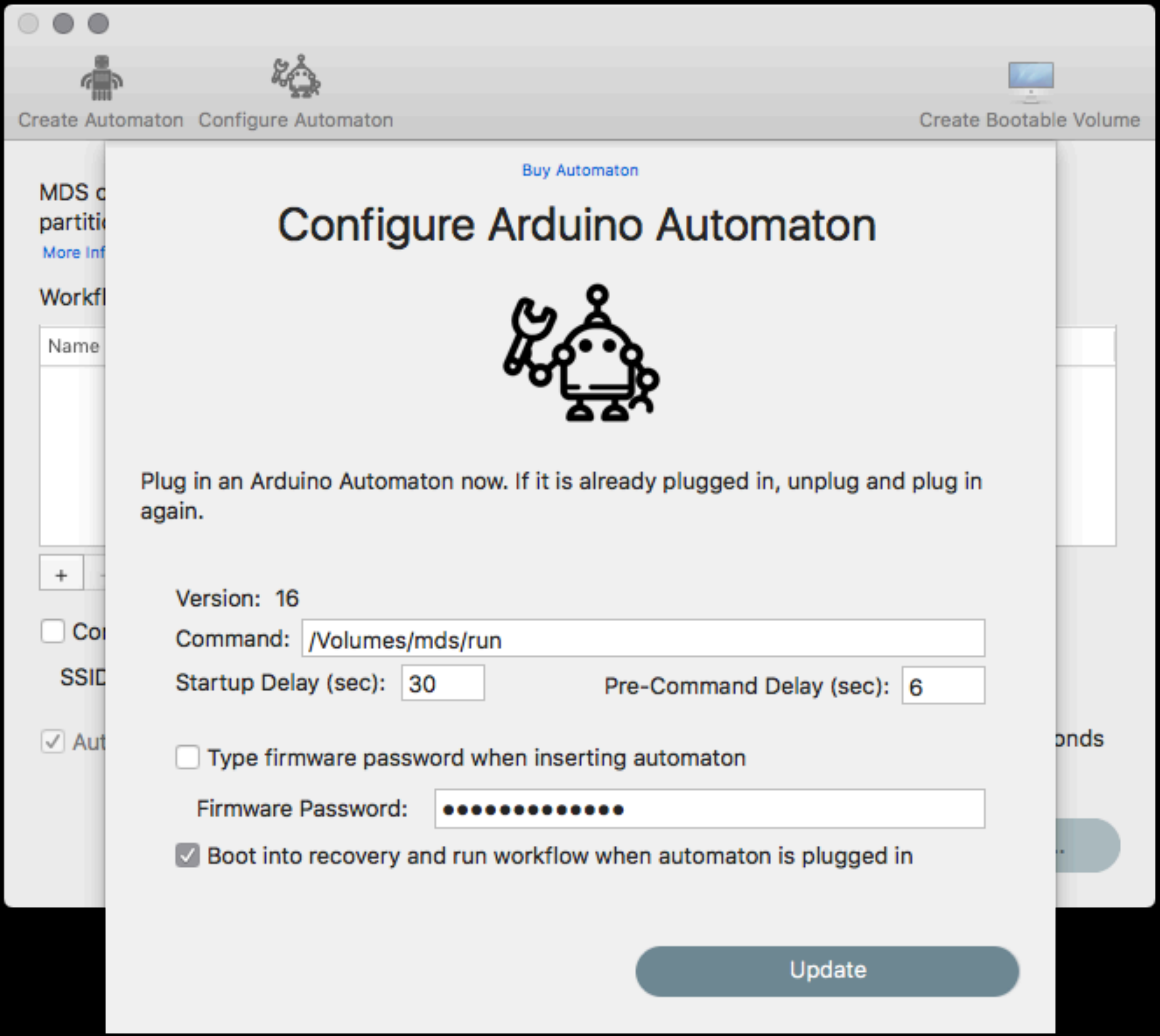
```
sudo "/Volumes/x20/shared/Images/mac/os/10.12.6 Install macOS Sierra 12.6.03.app/Contents/Resources/createinstallmedia" --volume "/Volumes/Untitled"
```

Automaton

- Flashes the firmware
  - avrdude
  - arduino_firmware.hex



- Uploads a script
  - Contents/Resources/sketch.txt
  - Sometimes I couldn’t get it to configure



Configure Arduino Automaton

Plug in an Arduino Automaton now. If it is already plugged in, unplug and plug in again.

Version: 16

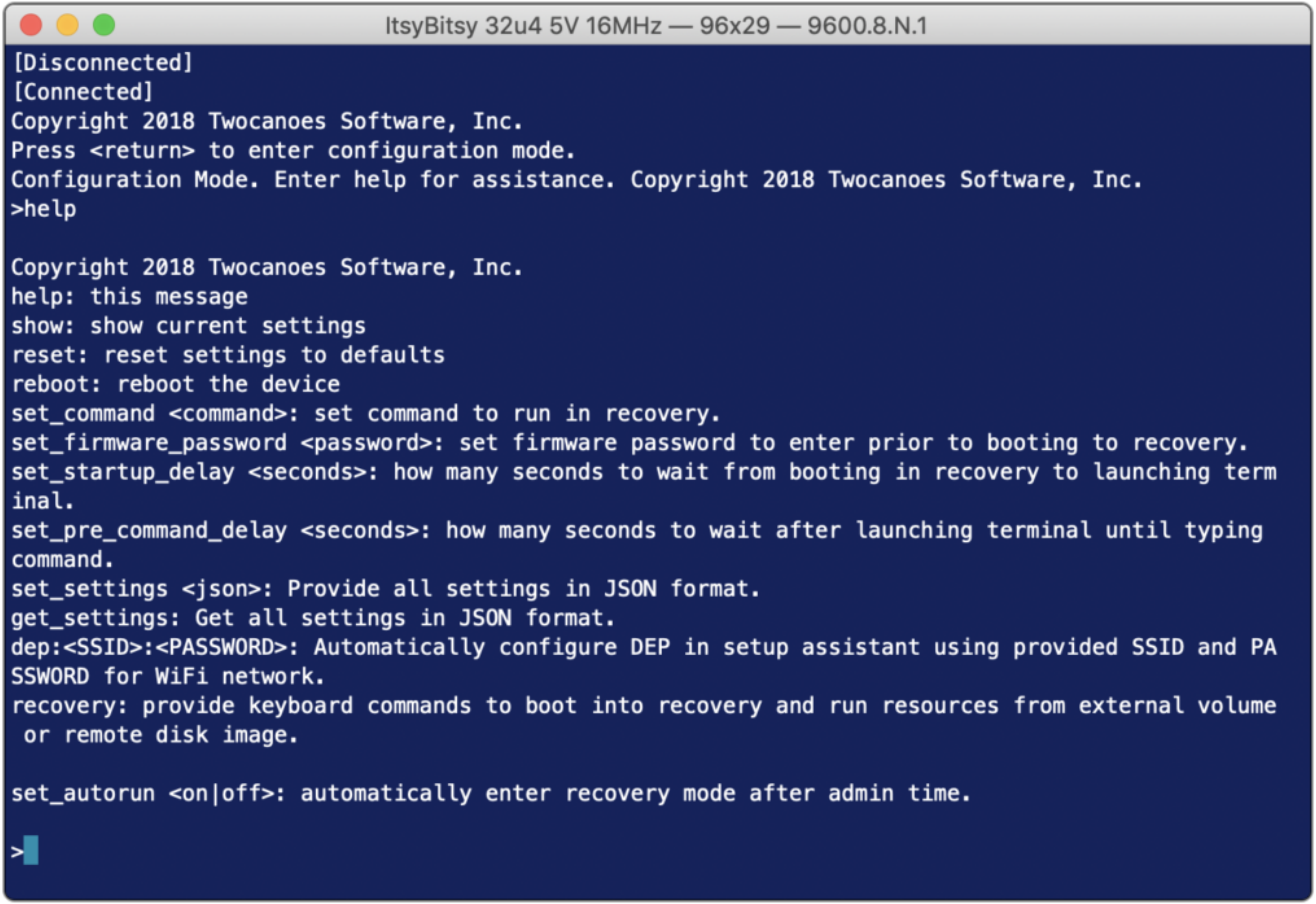
Command: /Volumes/mds/run

Startup Delay (sec): 30   Pre-Command Delay (sec): 6

□ Type firmware password when inserting automaton

Firmware Password: ••••••••••••••

☑ Boot into recovery and run workflow when automaton is plugged in



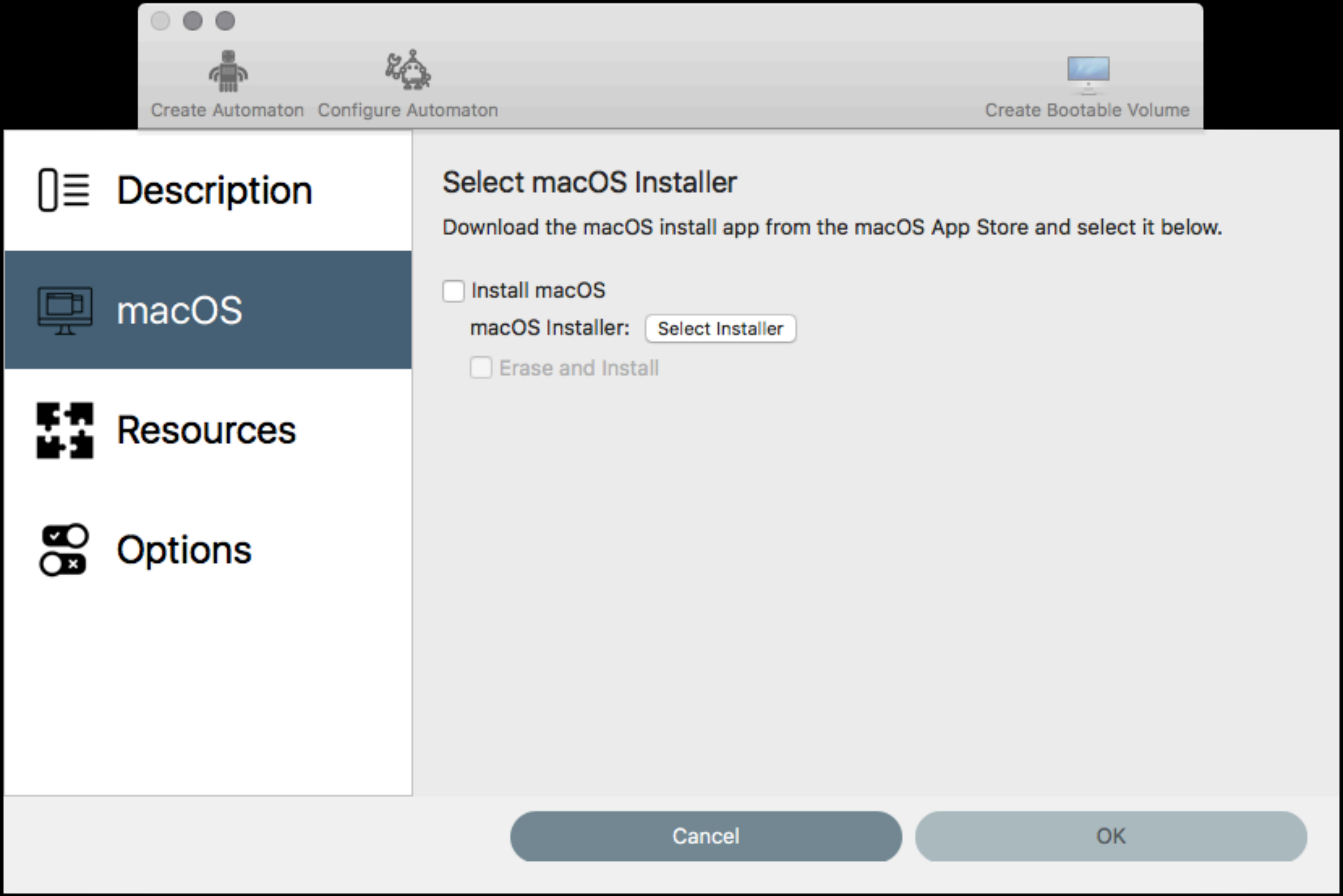
```
[Disconnected]
[Connected]
Copyright 2018 Twocanoes Software, Inc.
Press <return> to enter configuration mode.
Configuration Mode. Enter help for assistance. Copyright 2018 Twocanoes Software, Inc.
>help

Copyright 2018 Twocanoes Software, Inc.
help: this message
show: show current settings
reset: reset settings to defaults
reboot: reboot the device
set_command <command>: set command to run in recovery.
set_firmware_password <password>: set firmware password to enter prior to booting to recovery.
set_startup_delay <seconds>: how many seconds to wait from booting in recovery to launching term
inal.
set_pre_command_delay <seconds>: how many seconds to wait after launching terminal until typing
command.
set_settings <json>: Provide all settings in JSON format.
get_settings: Get all settings in JSON format.
dep:<SSID>:<PASSWORD>: Automatically configure DEP in setup assistant using provided SSID and PA
SSWORD for WiFi network.
recovery: provide keyboard commands to boot into recovery and run resources from external volume
 or remote disk image.

set_autorun <on|off>: automatically enter recovery mode after admin time.

>
```

sketch.txt

- Powers on, waits ~7 seconds
- Optional: types firmware password
- Holds down cmd-r
- Waits X secs, let’s go, waits X secs, presses esc, esc, ctrl-F2, →, →, →, →, ↓, ↓, ↓, ↓, waits 6 seconds, types “/Volumes/mds/run\r”

Deployment Stuff

- Saved to a folder named Deploy
- Or saved to a DMG
  - Place on a web server
  - Run `hdiutil mount http://example.com/mds.dmg` before the `run` script



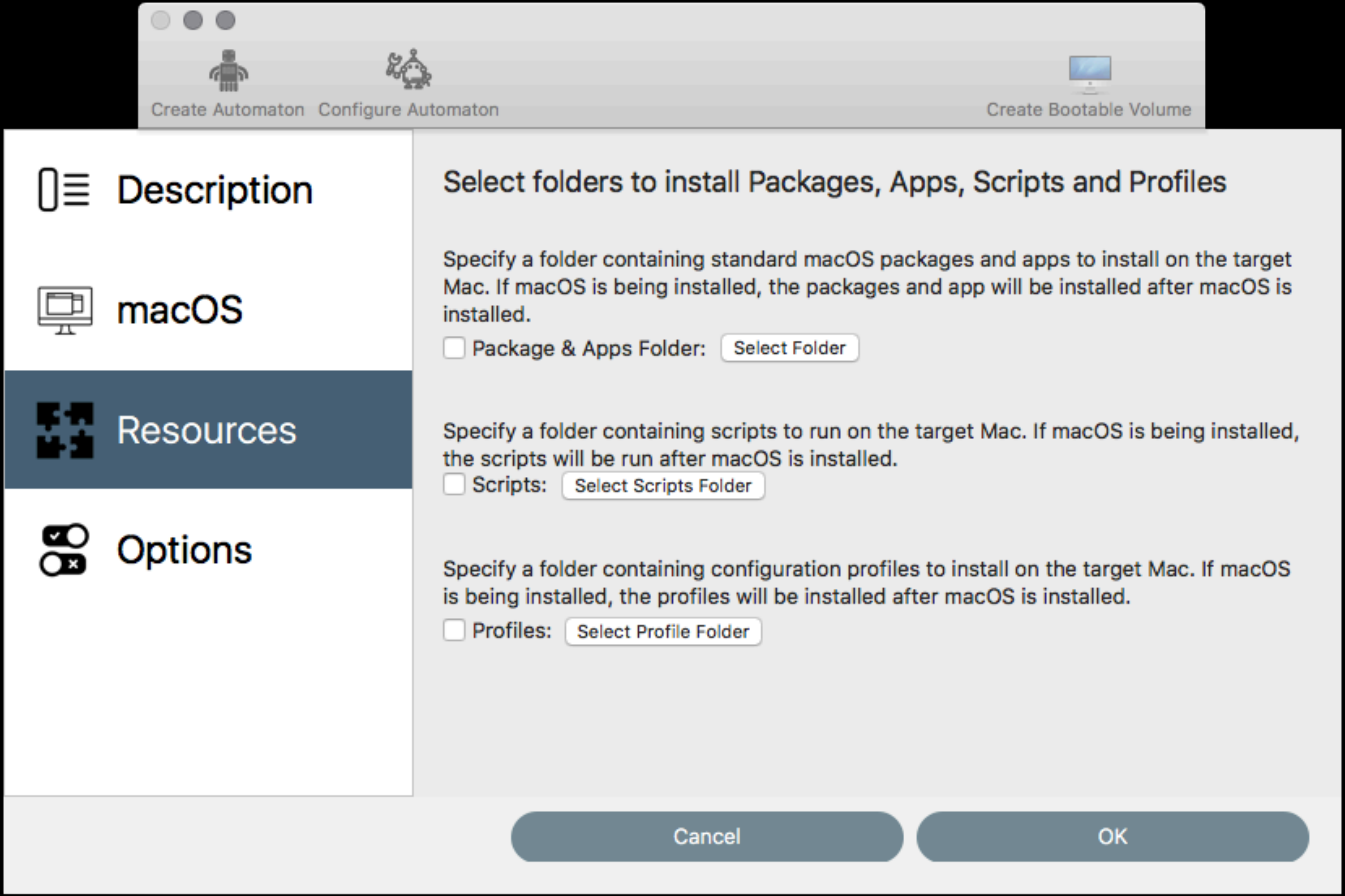
Select macOS Installer

Download the macOS install app from the macOS App Store and select it below.

□ Install macOS

macOS Installer: Select Installer

□ Erase and Install



Select folders to install Packages, Apps, Scripts and Profiles

Specify a folder containing standard macOS packages and apps to install on the target Mac. If macOS is being installed, the packages and app will be installed after macOS is installed.

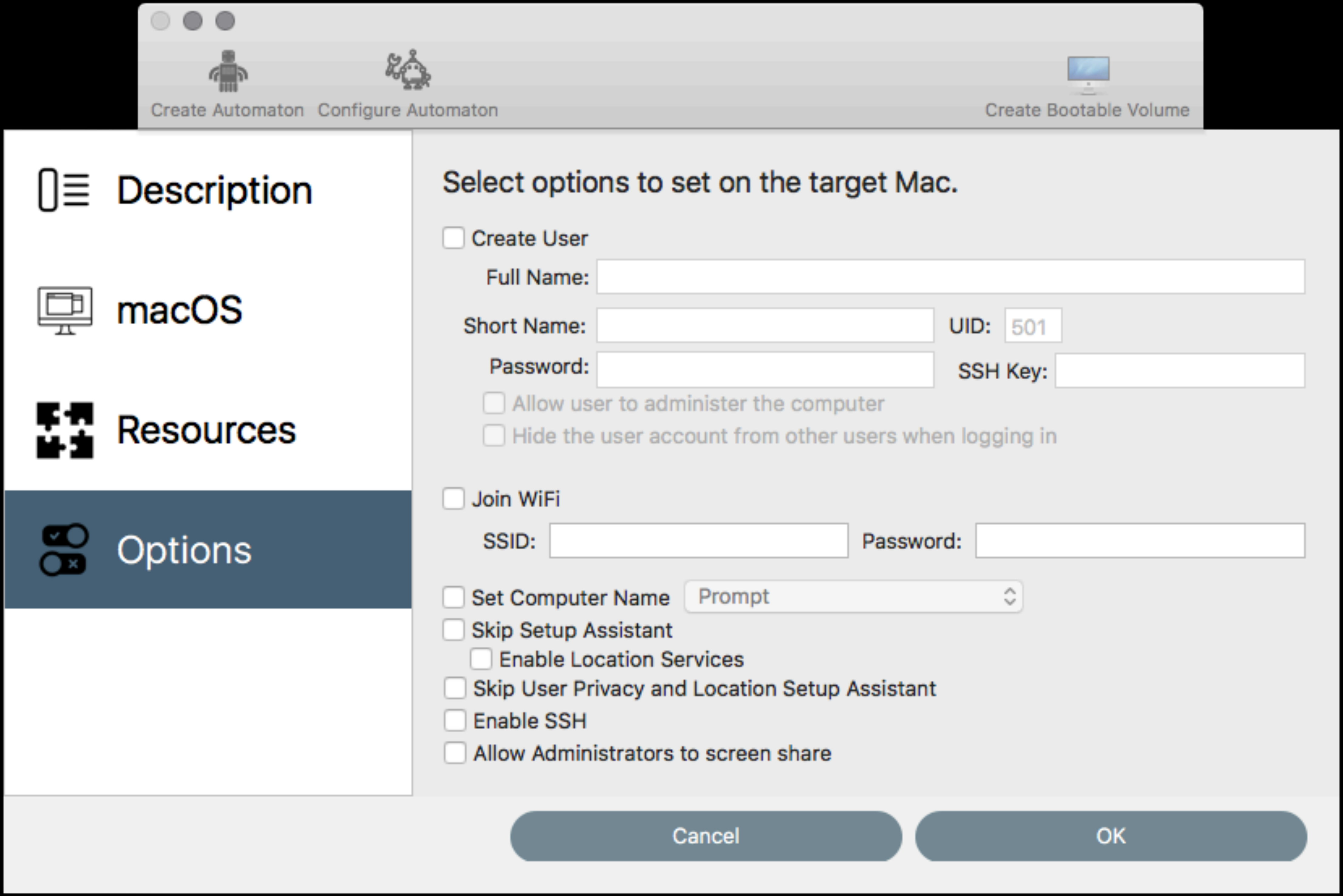
□ Package & Apps Folder: Select Folder

Specify a folder containing scripts to run on the target Mac. If macOS is being installed, the scripts will be run after macOS is installed.

□ Scripts: Select Scripts Folder

Specify a folder containing configuration profiles to install on the target Mac. If macOS is being installed, the profiles will be installed after macOS is installed.

□ Profiles: Select Profile Folder



Select options to set on the target Mac.

□ Create User

Full Name:

Short Name: UID: 501

Password: SSH Key:

□ Allow user to administer the computer

□ Hide the user account from other users when logging in

□ Join WiFi

SSID: Password:

□ Set Computer Name Prompt

□ Skip Setup Assistant

□ Enable Location Services

□ Skip User Privacy and Location Setup Assistant

□ Enable SSH

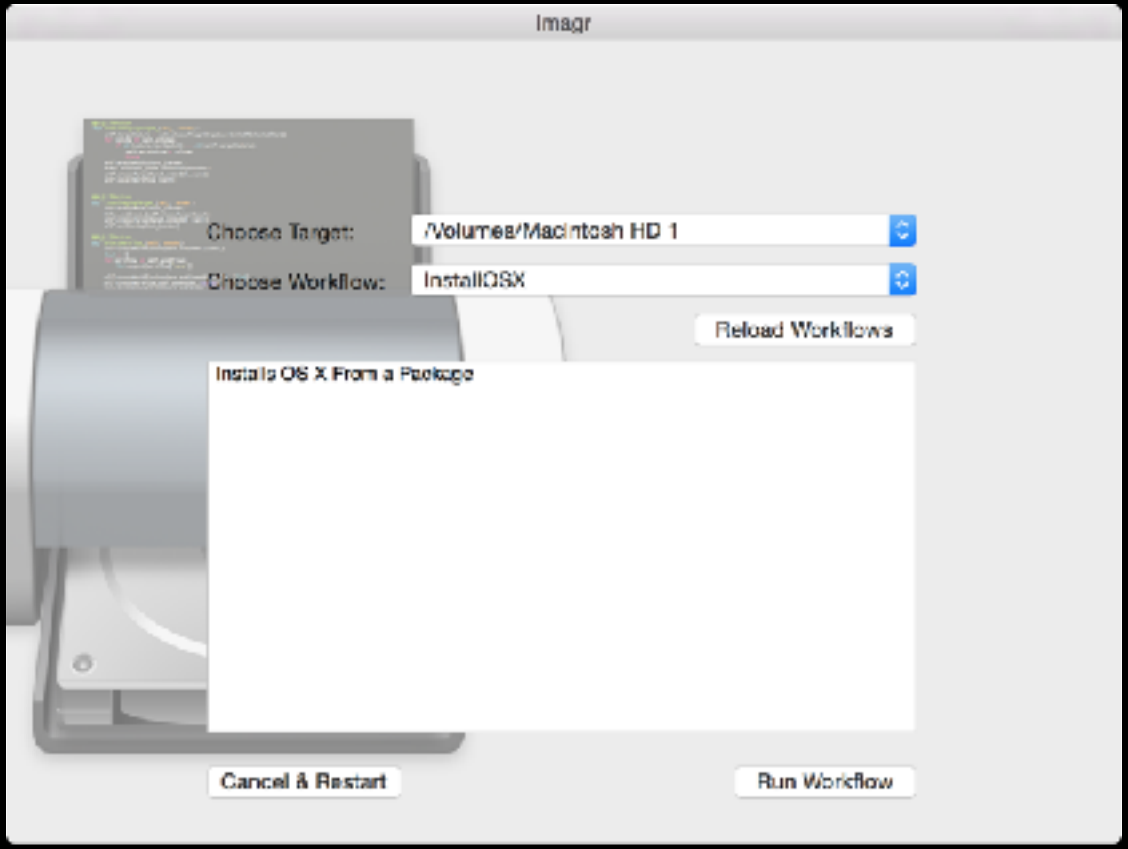
□ Allow Administrators to screen share

Deployment Stuff

- Creates
  - /Volumes/mds/run
  - /Volumes/mds/Deploy
- Creates custom config for Imagr
  - All of the fun stuff is in this config

Imagr

- 10.13+
- Open Source (python app)
- Designed to be run on a NetInstall image (minimal NetBoot image)
- Requires only a web server



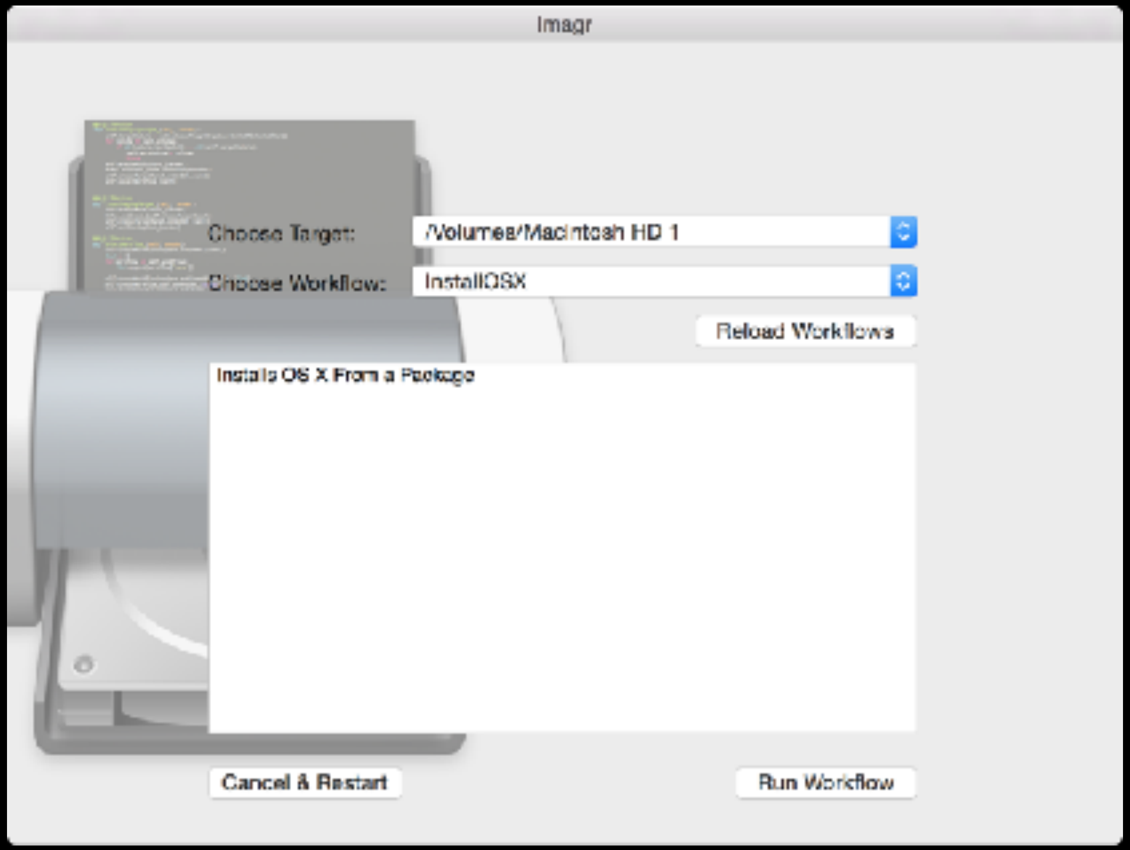
Choose Target: /Volumes/Macintosh HD 1

Choose Workflow: InstallOSX

Installs OS X From a Package

Imagr

- By Graham Gilbert
- ASR image restoration
- Package installation
- Run scripts
- Sets computer name



Choose Target: /Volumes/Macintosh HD 1

Choose Workflow: InstallOSX

Installs OS X From a Package

The Whole Process

- Hold down option while booting
- Plug in automaton
    - I couldn’t get this to work until I realized I was suppose to hold down the option key before plugging it in
        - Also had trouble with the timing, 120 secs worked
- Automaton types stuff and eventually executes /Volumes/mds/run

/Volumes/mds/run

- /Volumes/mds/Deploy/bin/networksetup sets wifi if set
- Checks for internet access (dig), tries 5 times, then waits 30 seconds, then tries 5 more times.
- Runs /Volumes/mds/Deploy/Applications/Imagr.app

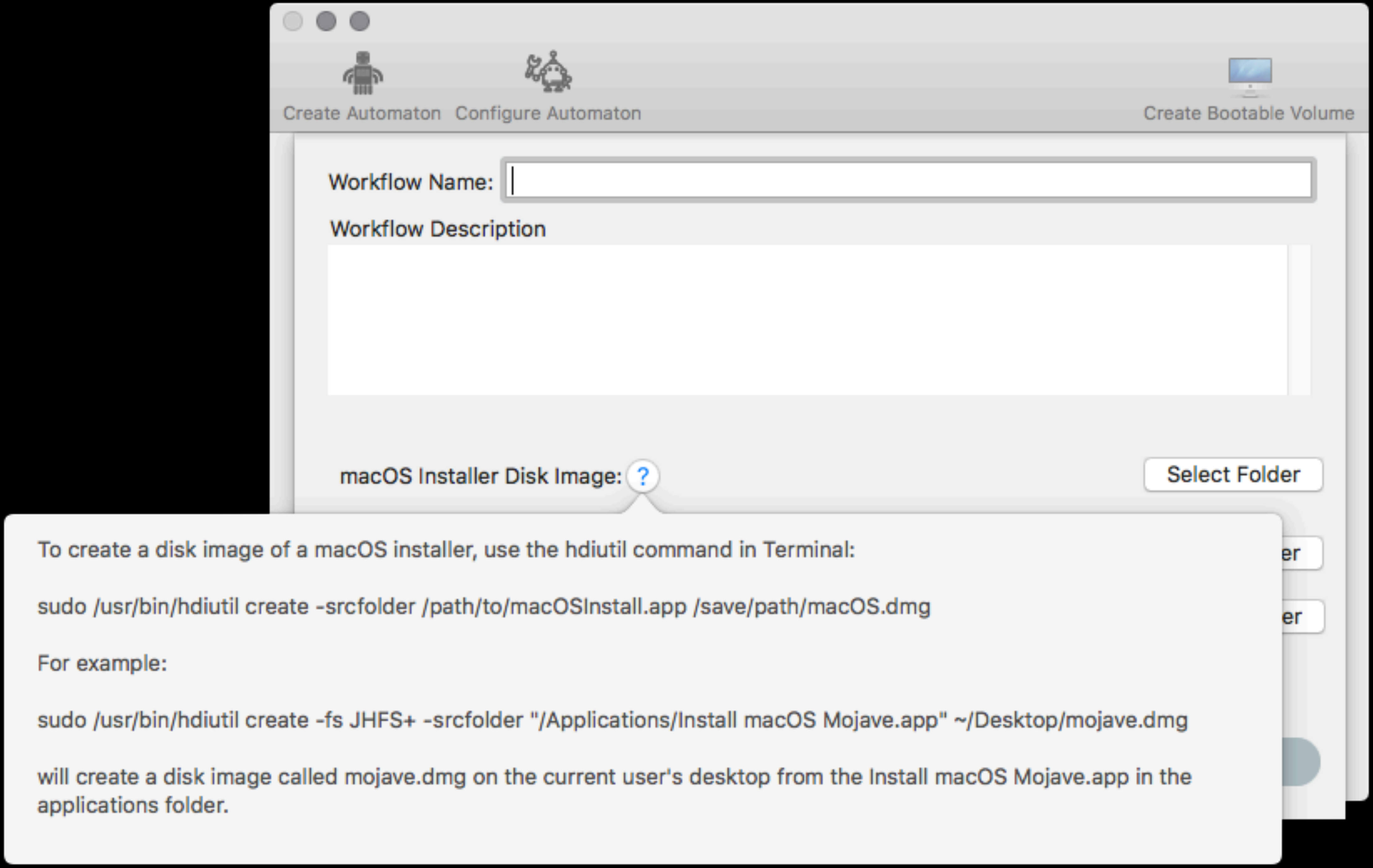
Imagr Steps

- Loads preference file: com.grahamgilbert.Imagr.plist
- Preference file specifies a workflow config
  - serverurl = file:///…/imagr_config.plist
  - serverurl = http://example.com/imagr_config.plist
- 30 second countdown
- Images the computer

So Many Problems

- Difficulty programming the Automaton
- MDS tried to download a version of Imagr from AWS but the permissions were broken (fixed now… or is it?)
- MDS doesn’t remember workflows
- I couldn’t get it to work until this morning…
  - I thought MDS used an image (like from AutoDMG)
  - It wants the installer app, e.g. “Install macOS Mojave”

MDS 1.1



To create a disk image of a macOS installer, use the hdiutil command in Terminal:

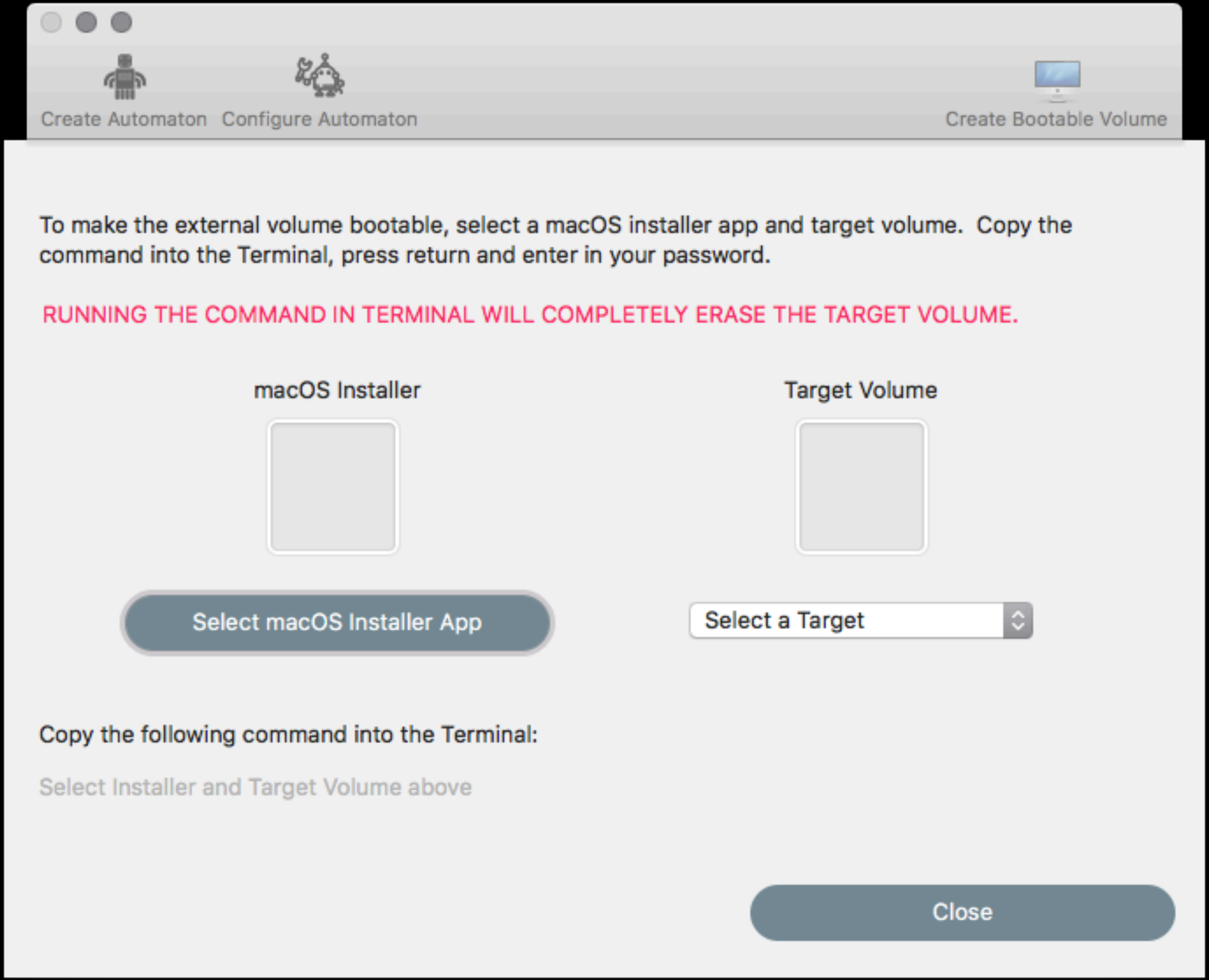
```
sudo /usr/bin/hdiutil create -srcfolder /path/to/macOSInstall.app /save/path/macOS.dmg
```

For example:

```
sudo /usr/bin/hdiutil create -fs JHFS+ -srcfolder "/Applications/Install macOS Mojave.app" ~/Desktop/mojave.dmg
```

will create a disk image called mojave.dmg on the current user's desktop from the Install macOS Mojave.app in the applications folder.

MDS 1.4



To make the external volume bootable, select a macOS installer app and target volume. Copy the command into the Terminal, press return and enter in your password.

RUNNING THE COMMAND IN TERMINAL WILL COMPLETELY ERASE THE TARGET VOLUME.

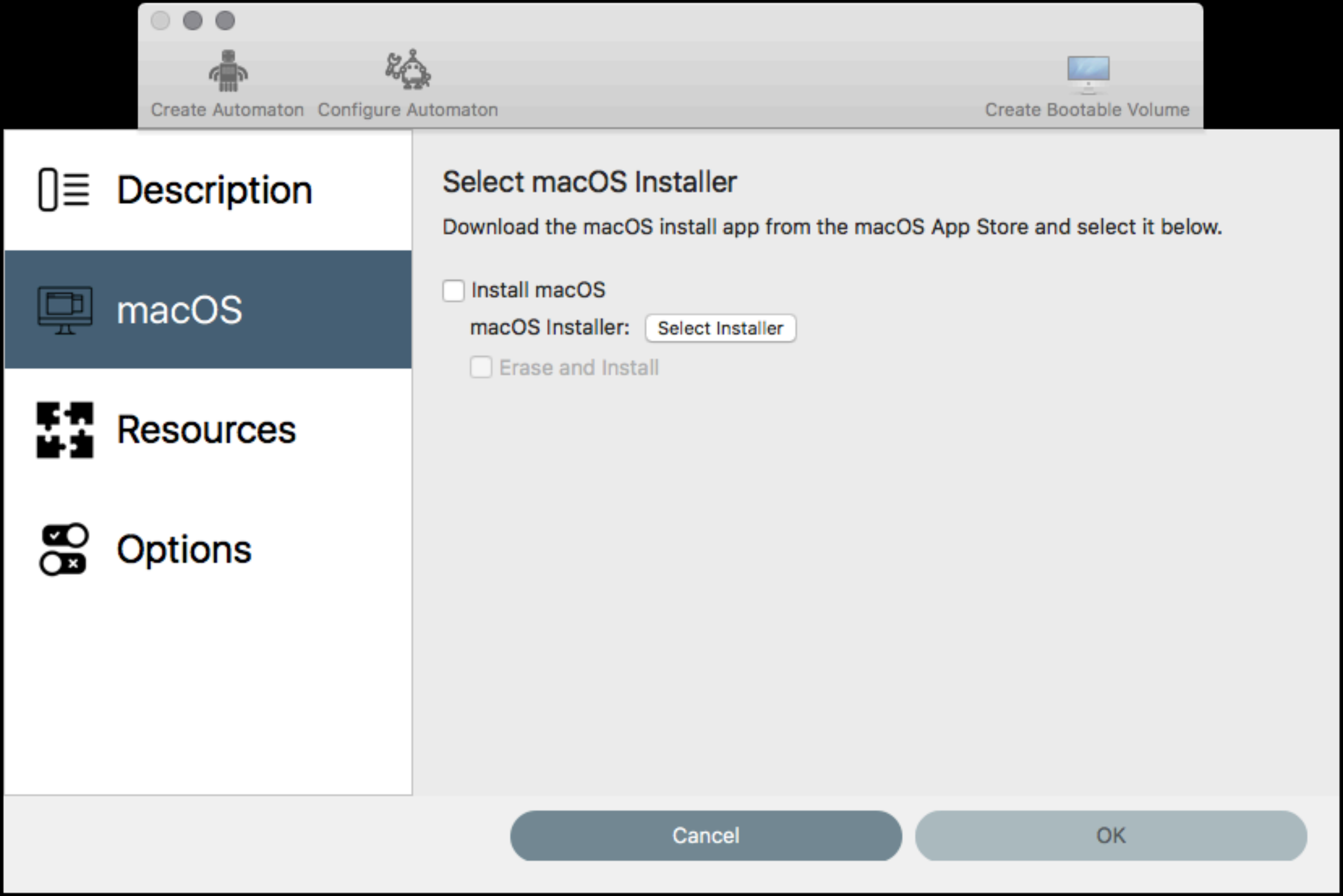
macOS Installer

Target Volume

Copy the following command into the Terminal:

Select Installer and Target Volume above

MDS 1.4



Select macOS Installer

Download the macOS install app from the macOS App Store and select it below.

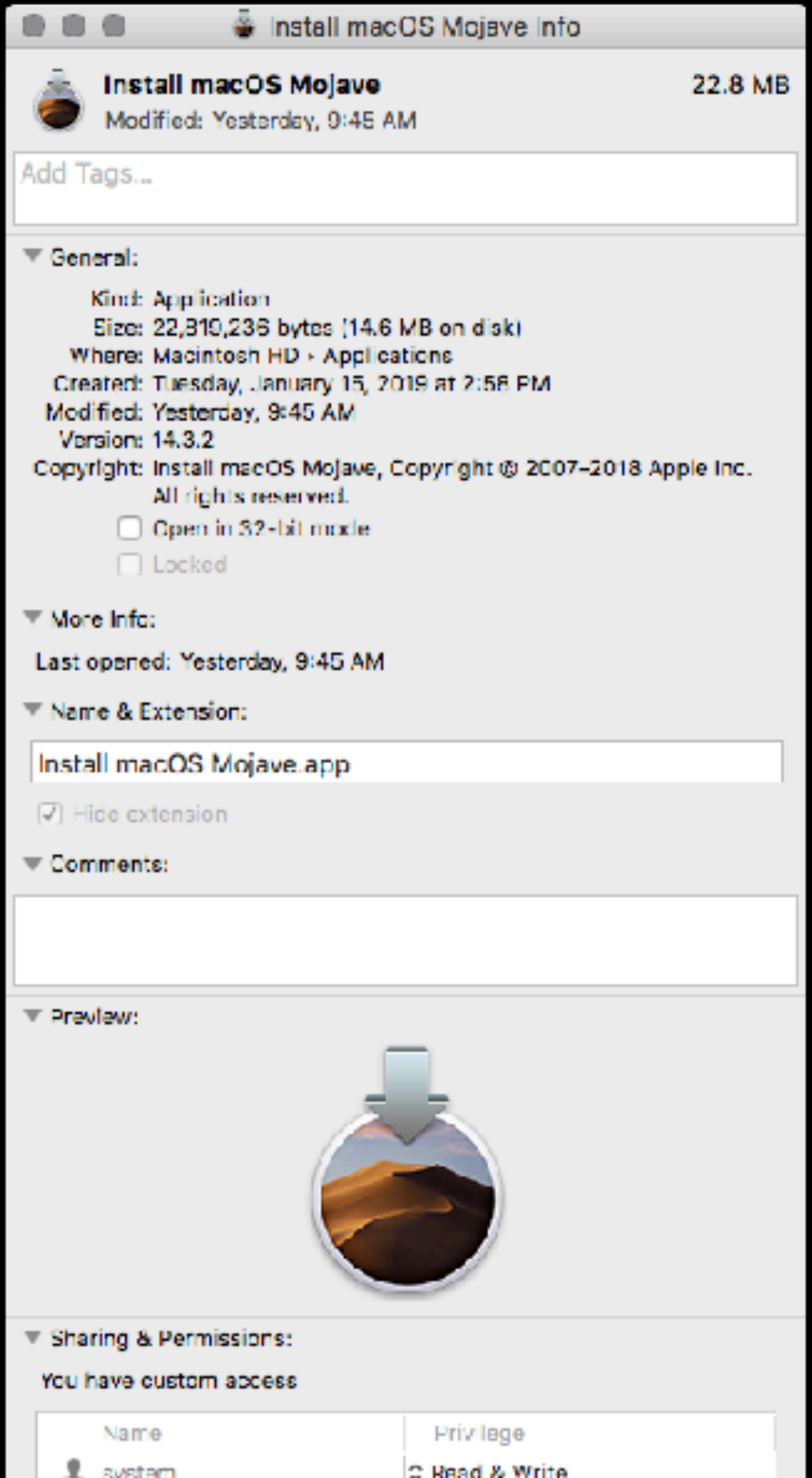
□ Install macOS

macOS Installer: Select Installer

□ Erase and Install

14 MB Installer???

- SharedSupport is missing



Install macOS Mojave Info

Install macOS Mojave 22.8 MB
Modified: Yesterday, 9:45 AM

Add Tags...

▼ General:

Kind: Application
Size: 22,310,236 bytes (14.6 MB on disk)
Where: Macintosh HD ▸ Applications
Created: Tuesday, January 15, 2019 at 2:56 PM
Modified: Yesterday, 9:45 AM
Version: 14.3.2
Copyright: Install macOS Mojave, Copyright © 2007–2018 Apple Inc. All rights reserved.

☐ Open in 32-bit mode
☐ Locked

▼ More Info:

Last opened: Yesterday, 9:45 AM

▼ Name & Extension:

Install macOS Mojave.app

☑ Hide extension

▼ Comments:

▼ Preview:

▼ Sharing & Permissions:

You have custom access

Name	Privilege
system	Read & Write

Other concerns

- Clear text passwords…
  - Wifi - twice, in ~/L/P & the “Deploy” folder
  - Admin account creation - ShadowHash
  - Firmware password - Plug in automaton with a text editor open…
- Restore Partition is missing a lot of stuff
  - Jamf Imaging crashed when launched

Why was I excited?

T2 Imaging from the restore partition

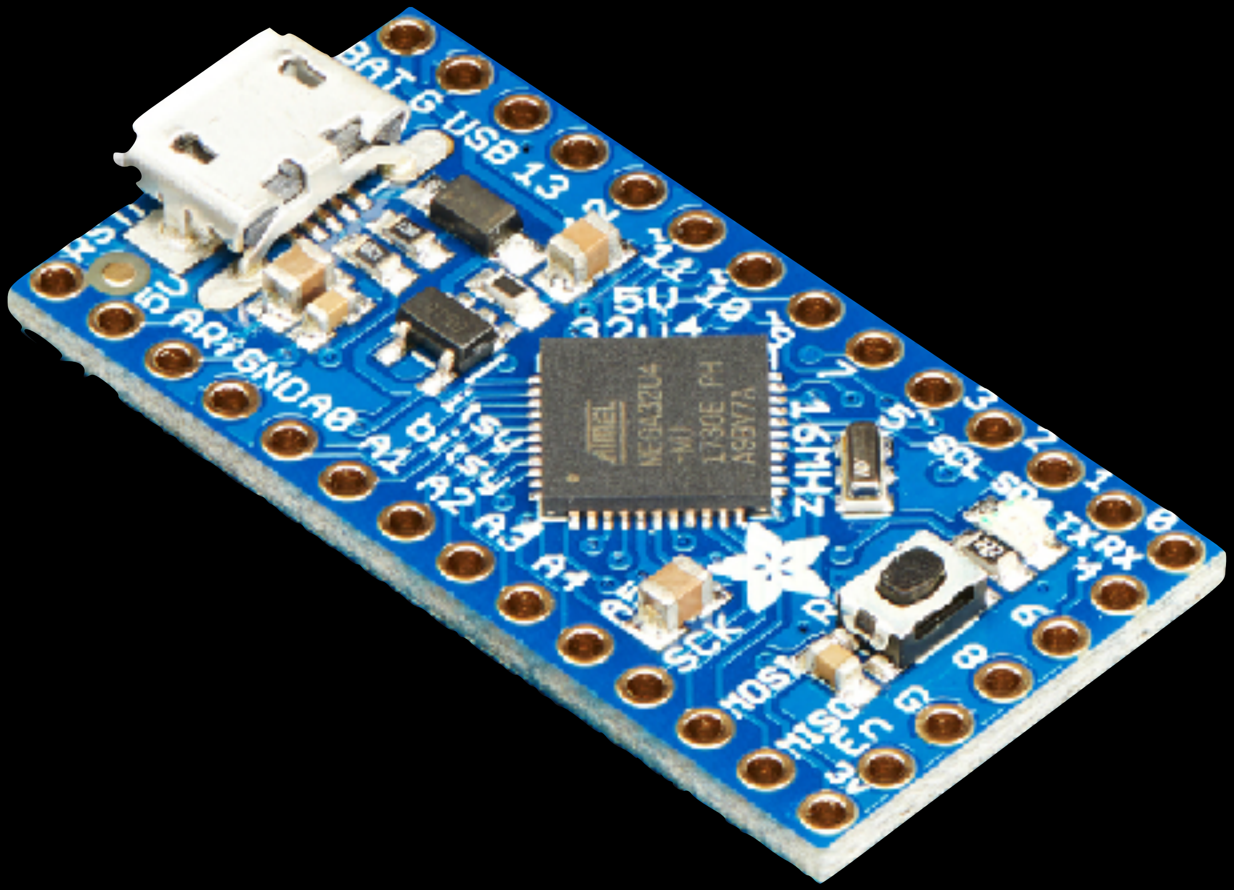
It’s alive!

Why was I excited?

- Locating this on a web server
    - Loads a server-side PHP script?
    - Multiple configs?

Why was I excited?

- It’s a keyboard!
- Add
  - LCD/Screen
  - Switches
    - Multiple configs?
  - Buttons
    - Skip delays
      - Computer Vision?



My Takeaway

- Apple is forcing a lot of unpleasant (IT hostile?) changes
    - I doubt Apple would block this (in the name of security)
- The automaton does speed it up and is very cool
- It’s not “imaging” like before with DMG’s, it’s more like “automated installer.app” w/ added packages and scripts
- I don’t know why I feel the need to erase a drive…
- So much easier than creating a custom restore partition
- MDS is changing quickly