Deploying and Managing Mac's In a Lab Environment

Graham Williams

Who am I?

Graham Williams

Senior Desktop Support Officer
University of Wales Trinity Saint David

Uwch Swyddog Cymorth Cyfrifiaduron Bwrdd Gwaith
Prifysgol Cymru Y Drindod Dewi Sant

- 15 years experience
- Worked up from first line support
- 6 years working in networking and server teams
- Working with Apple products for around 3 years
- Very new Apple admin!

Today's Session

In this session, we'll go through what it takes to create a true zero-touch deployment for a multi-user lab environment. From brand new in box, to user ready. When we're finished, all you'll need to do, is plug it in.

Prerequisites	PreStage & Auto Logon	Preparation & Deployment	User Readiness

Lessons Learned	Q&A

Prerequisites

Prerequisites

Apple School / Business Manager

To make the most of this whole process, we're going to need to have Apple School / Business Manager in place. This will allow us to use the Apple Device Enrolment Program / Automated Device Enrolment services.

Jamf Pro

We'll be using Jamf Pro for this session. To follow along, you're going to need at least:

- Jamf Pro 10.34
- HTTP/S Distribution Point

macOS

And finally, of course, you're going to need macOS Big Sur or later. This is so we can use Auto Advance.

Apple School Manager

Suppliers & Orders

Customer numbers ⑦   Done

Reseller Numbers

● Active
● Active
● Active
● Active

Apple Customer Number   123456789   Add

3 devices · Jamf MDM

Reseller name

Assigned from   Order number

Assigned to   Jamf MDM

Date assigned   21 February 2022 at 15:46

Devices

Device type	Quantity
Mac	3
Total assigned devices	3 ⬇ Download

MDM Servers & Assignments

MDM Servers

Apple Configurator 2
0 devices

Jamf - iPad DEP

Jamf - iPhone DEP

Jamf - Lab DEP

Jamf MDM

Default device assignment   Done

iPad
Jamf - iPad DEP

iPhone
Jamf - iPhone DEP

iPod
Jamf MDM

Mac
Jamf MDM

Apple TV
Jamf MDM

Jamf Pro: Automated Device Enrollment Instances

macOS: Big Sur & Monterey

Auto Advance for Mac

NEW

Power and ethernet required

Requires using Apple Business Manager or Apple School Manager

Auto-advance Setup Assistant

Land at login

Encrypted volumes require passwords

PreStage & Auto Logon

PreStage & Auto Logon

PreStage

Now we have the key pieces in place, we'll create our PreStage and device assignments.

Auto Logon

Using macOS Auto Advance, we can get our devices to land at the logon screen. Then we'll take it a step further.

Jamf Pro: PreStage Setup

General

Display Name   Display name for the PreStage enrollment

Lab Devices - Auto Advance

Automated Device Enrollment Instance
Automated Device Enrollment instance to associate with the PreStage enrollment. Devices associated with the selected Automated Device Enrollment instance can be assigned the PreStage enrollment

Lab - DEP ▾

☑ **Automatically assign new devices**
Automatically assign all new devices to this PreStage enrollment

Enrollment Site   Site that computers will be added to during enrollment

None ▾

☐ Use existing site membership, if applicable

☐ Use existing location information, if applicable

Support Phone Number   Support phone number for the organization

▮▮▮ ▮ ░░ ▮▮

Support Email Address   Support email address for the organization

░░ ▮▮ ░ ▮▮

Department   Department to associate with the PreStage enrollment

▮▮

☐ Require Authentication
Require the user to provide username and password on computers with macOS 10.10 or later

☑ Make MDM Profile Mandatory
Require the user to apply the MDM profile

☐ Allow MDM Profile Removal
Allow the user to remove the MDM profile

☑ Prevent user from enabling Activation Lock

☐ Set Recovery Lock Password
Configure how the Recovery Lock password is set on computers with macOS 11.5 or later

Enrollment Customization Configuration   Configuration to use for customizing the user experience in the Setup Assistant

None ▾

Jamf Pro: PreStage Setup

Setup Assistant

☑ Automatically advance through Setup Assistant (macOS 11 or later only)
Automatically skips all Setup Assistant screens that can be skipped during enrollment.

Language

| English ▾ |

Region

| United Kingdom ▾ |

Setup Assistant Options   Selected items are not displayed in the Setup Assistant during enrollment

[All]

☑ Location Services

☑ Transfer Information

☑ Apple ID

☑ Terms and Conditions

☑ Siri

☑ App Analytics

☑ Touch ID / Face ID

☑ Apple Pay

☑ Registration

☑ Privacy

☐ FileVault

☑ iCloud Diagnostics

☑ All Your Files in iCloud

☑ Choose your Look

☑ True Tone Display [Deprecated]

☑ Screen Time

☑ Accessibility

Jamf Pro: PreStage Setup

Auto Logon: Script

Settings : Computer Management > Scripts

← ◼ ▢ Lab - Onboarding - Set-or-Remove Auto Logon

General | Script | Options | Limitations

Script Contents

Shell ▾ | Dracula `Script` ▾   -T T+   ⌄ Commands

```bash
1  #!/bin/bash
2  : <<-LICENSE_BLOCK
3  setAutoLogin.jamf (20210911) - Copyright (c) 2021 Joel Bruner (https://github.com/brunerd)
4  Licensed under the MIT License
5
6  Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without re
7  The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
8  THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE
9  LICENSE_BLOCK
10
11 #############
12 # VARIABLES #
13 #############
14
15 #JAMF script parameters are shifted +3
16 #provide a username, if blank will disable autologin
17 USERNAME="${4}"
18
19 #this can be blank if that is the password, it will be verified
20 PW="${5}"
21
22 #############
23 # FUNCTIONS #
24 #############
25
26 function jamflog {
27     local logFile="${2:-/var/log/jamf.log}"
28     #if we cannot write to the log or it does not exist, unset and tee simply echoes
29     [ ! -w "${logFile}" ] && unset logFile
30     #this will tee to jamf.log in the jamf log format: <Day> <Month> DD HH:MM:SS <Computer Name> ProcessName[PID]: <Message>
31     echo "$(date +'%a %b %d %H:%M:%S') ${myComputerName:="$(scutil --get ComputerName)"} ${myName:="$(basename "${0}" | sed 's/\..*$//')"}[${myPID:=$$}]: ${1}" | tee -a "${logFile}"
32 }
33
34 #given a string creates data for /etc/kcpassword
35 function kcpasswordEncode {
36
37     #ascii string
38     local thisString="${1}"
39     local i
40
41     #macOS cipher hex ascii representation array
42     local cipherHex_array=( 7D 89 52 23 D2 BC DD EA A3 B9 1F )
43
```

🕑 History   ⬆ Download   ▢ Clone   🗑 Delete   ✏ Edit

Auto Logon: Script

Settings : Computer Management > Scripts

← ▪ ▪ **Lab - Onboarding - Set-or-Remove Auto Logon**

General   Script   Options   Limitations

Priority Priority to use for running the script in relation to other actions during imaging

After

Parameter Labels Labels to use for script parameters. Parameters 1 through 3 are predefined as mount point, computer name, and username

Parameter 4

Username

Parameter 5

Password

Auto Logon: Policy

Auto Logon: Policy

Auto Logon: Policy

Computers : Policies

← 00. ▪▪▪ Lab - Onboarding - Set Auto - Logon

Options   Scope   Self Service   User Interaction

General

Scripts
1 Script

Restart Options
Configured   >

Restart Options

Reboot Method

● **Standard Restart**
Restart the computer using the standard macOS functionality.

○ **MDM Restart with Kernel Cache Rebuild**
Restart the computer using the management command and rebuild the kernel cache. Include specific kernel extensions (kexts) paths to add them to the kernel cache.

Startup Disk   Disk to boot computers to

Current Startup Disk   ▼

No User Logged In Action   Action to take if no user is logged in to the computer

Restart immediately   ▼

User Logged In Action   Action to take if a user is logged in to the computer

Restart immediately   ▼

☐ Perform authenticated restart on computers with FileVault 2 enabled
Restart FileVault 2-encrypted computers without requiring an unlock during the next startup

Auto Logon: Extension Attribute

```
status=`defaults read /Library/Preferences/com.apple.loginwindow autoLoginUser`
if [ "$status" == "labadmin" ]; then
    echo "<result>Auto Logon Enabled</result>"
elif [ "$status" != "labadmin" ]; then
    echo "<result>Auto Logon Disabled</result>"
fi
```

Extension Attributes

Auto Logon Status: Auto Logon Enabled

Auto Logon: Smart Group

Preparation & Application Deployment

Preparation: Inventory Preload

Serial Number	Device Type	Asset Tag	Room	EA Usage Type
12345678	Computer	BLOG01	Room 01	Lab
12345687	Computer	BLOG02	Room 02	Lab
12345876	Computer	BLOG03	Room 03	Lab

Preparation: Inventory Preload

Preparation: DEPNotify Script

Preparation: DEPNotify Script

Settings : Computer Management > Scripts

← NEW_SCRIPT

General   Script   Options   Limitations

Priority Priority to use for running the script in relation to other actions during imaging

After ▾

Parameter Labels Labels to use for script parameters. Parameters 1 through 3 are predefined as mount point, computer name, and username

Parameter 4

DEPN Options

Parameter 5

Main Title: Starting Text (Optional)

Parameter 6

Path to Icon (Optional)

Parameter 7

Window Title (Optional - Invisible)

Preparation: DEPNotify Policy

General

Display Name   Display name for the policy

```
10. Lab - Zero Touch - Onboarding - DEPNotify
```

☑ Enabled

Site   Site to add the policy to

```
None                              ▾
```

Category   Category to add the policy to

```
None                              ▾
```

Trigger   Event(s) to use to initiate the policy

☐ **Startup**
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

☑ **Login**
When a user logs in to a computer. A login event that checks for policies must be configured in Jamf Pro for this to work

☐ **Network State Change**
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

☐ **Enrollment Complete**
Immediately after a computer completes the enrollment process

☑ **Recurring Check-in**
At the recurring check-in frequency configured in Jamf Pro

☑ **Custom**
At a custom event

Custom Event   Custom event to use to initiate the policy. For an iBeacon region change event, use "beaconStateChange"

```
labzt-onboarding-fulldepn
```

Execution Frequency   Frequency at which to run the policy

```
Once per computer                 ▾
```

☑ Automatically re-run policy on failure

Retry Event   Event to use to re-run the policy

```
On next recurring check-in        ▾
```

Retry Attempts

```
3     ▾
```

Preparation: DEPNotify Policy

Packages

Distribution Point   Distribution point to download the package(s) from

Each computer's default distribution point ▼

DEPNotify   ✕   +

Action   Action to take on computers

Install ▼

☐ Update Autorun data
Add or remove the package from each computer's Autorun data

Preparation: DEPNotify Policy

Scripts

Script - Lab - Zero Touch - Onboarding - DEPNotify   ×   +

Priority   Priority to use for running the script in relation to other actions

[After ▼]

Parameter Values   Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username

DEPN Options

[-fullScreen]

Main Title: Starting Text (Optional)

[Configuring Lab Device]

Path to Icon (Optional)

[   ]

Window Title (Optional - Invisible)

[   ]

Preparation: DEPNotify Policy

Preparation: DEPNotify Deployment

```
## EXAMPLE WORKFLOW
##
# ## Machine Configuration
DEPNotify "Command: MainText: Configuring System Settings"
DEPNotify "Status: Setting Computer Name"
jamfCommand labzt-onboarding-setdevicename
DEPNotify "Status: Setting Computer Time Zone to UK"
jamfCommand labzt-onboarding-settimezonentp
#
# ## Browsers
DEPNotify "Status: Installing Microsoft Edge"
DEPNotify "Command: MainText: Starting software deployment.\n\nThis process can take up to 3-4 hours to complete."
jamfCommand labzt-onboarding-edge
#
# ## Office Applications
DEPNotify "Status: Installing Microsoft Office 365"
jamfCommand labzt-onboarding-office365
#
```

Preparation: DEPNotify Deployment

```
# ## Send updated inventory for Smart Groups and check for any remaining scoped policies
DEPNotify "Command: MainText: Installing Room Specific Requirements"
DEPNotify "Status: Update inventory record."
jamfCommand recon
sleep 3
DEPNotify "Status: Installing any Room Specific Software"
jamfCommand policy
sleep 3
/usr/bin/defaults write /Library/Preferences/co.uk.grayw.blog onboardingComplete -string "Complete"
```

User Readiness

User Readiness: Extension Attribute

```
status=`defaults read /Library/Preferences//Library/Preferences/ac.uk.grayw.blog onboardingComplete`
if [ "$status" == "Complete" ]; then
    echo "<result>Onboarding Complete</result>"
elif [ "$status" != "Complete" ]; then
    echo "<result>Onboarding Not Complete</result>"
fi
```

User Readiness: Smart Group

← **Devices - Lab - Onboarding Complete**

Computer Group   Criteria

Display Name   Display name for the smart computer group

Devices - Lab - Onboarding Complete

☐ **Send email notification on membership change**
When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work

Site   Site to add the smart computer group to

None ▾

Computers : Smart Computer Groups

← **Devices - Lab - Onboarding Complete**

Computer Group   Criteria

AND/OR	CRITERIA	OPERATOR	VALUE		
▾	Onboarding Status	is ▾	Onboarding Comple	▾	Delete

+ Add

User Readiness: Final Lines

```
## Prepare for Final Usage
DEPNotify "Status: Install NoMAD & NoMAD Login"
jamfCommand labzt-nomad
DEPNotify "Status: Removing Auto Logon"
jamfCommand labzt-remove-autologon
```
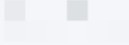
User Ready
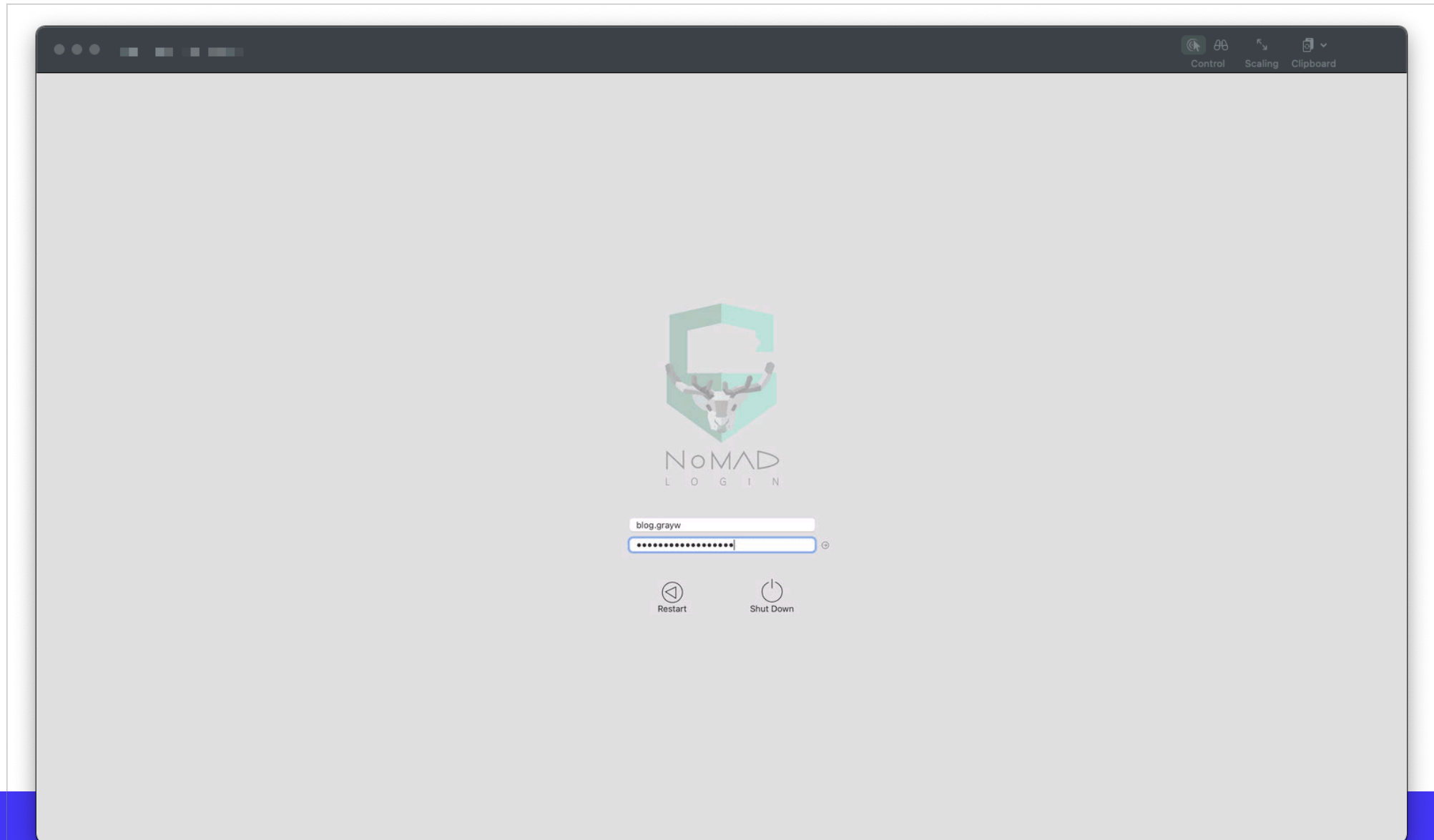
User Ready - Policy Logs

POLICY	USERNAME AT LOGIN/LOGOUT	DATE/TIME ^	DURATION	STATUS	ACTIONS
00. Lab - Zero Touch - Onboarding - Set Auto Logon **①**	_mbsetupuser	01/03/2022 at 09:41	2s	Completed	Details　Flush
LAPS for ▓▓▓▓▓ - Create Local Account - Manual Trigger		01/03/2022 at 09:41	6s	Completed	Details　Flush
LAPS for ▓▓ ▓▓ - Manual Trigger		01/03/2022 at 09:41	5s	Failed	Details　Flush
LAPS - Create Account	_mbsetupuser	01/03/2022 at 09:41	23s	Completed	Details　Flush
Update Inventory **②**	▓▓ ▓▓▓	01/03/2022 at 09:42	1s	Completed	Details　Flush
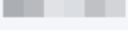
User Ready - Policy Logs

Lab - Onboarding - Set Computer Name to Serial		01/03/2022 at 09:44	1s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - Set UK Time Zone and NTP Server		01/03/2022 at 09:44	0s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - AI - Microsoft Defender ATP		01/03/2022 at 09:45	1m 24s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - Edge		01/03/2022 at 09:47	1m 18s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - AI - Google Chrome		01/03/2022 at 09:48	1m 07s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - AI - Firefox		01/03/2022 at 09:49	58s	Completed	Details	Flush
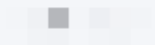
User Ready - Policy Logs

Lab - Zero Touch - Onboarding - AI - Keka		01/03/2022 at 09:50	21s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - AI - VLC		01/03/2022 at 09:52	1m 42s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - AI - Audacity		01/03/2022 at 09:52	39s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - Cache - Adobe SDL 2022 Intel		01/03/2022 at 10:37	33m 44s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - Install - Adobe SDL 2022 Intel		01/03/2022 at 11:14	31m 41s	Completed	Details	Flush

User Ready - Policy Logs

Lab - Zero Touch - Onboarding - Set UK Time Zone and NTP Server **①**		01/03/2022 at 11:20	1s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - Microsoft Office 365 Business Pro		01/03/2022 at 11:26	5m 19s	Completed	Details	Flush
Lab - Zero Touch - Onboarding - Remove Outlook		01/03/2022 at 11:26	10s	Completed	Details	Flush
Lab - Zero Touch - Install - NoMAD		01/03/2022 at 11:48	8s	Completed	Details	Flush
20. Lab - Zero Touch - Onboarding - Remove Auto Logon **②**		01/03/2022 at 11:48	0s	Completed	Details	Flush

User Ready - Policy Logs

Install - Adobe Camera Raw		01/03/2022 at 11:48	25s	Completed	Details	Flush
Install - Blurb Book Wright		01/03/2022 at 11:49	4s	Completed	Details	Flush
Install - Exif Fixer		01/03/2022 at 11:49	3s	Completed	Details	Flush
Install - Insta 360 Studio 2021		01/03/2022 at 11:49	15s	Completed	Details	Flush
Install - RICOH Bundle		01/03/2022 at 11:49	13s	Completed	Details	Flush
Install - Spatial Media Metadata Injector		01/03/2022 at 11:49	4s	Completed	Details	Flush
Printer - Print-Argraffu Universal Queue		01/03/2022 at 11:49	9s	Completed	Details	Flush
10. Lab - Zero Touch - Onboarding - DEPNotify		01/03/2022 at 11:50 ①	2h 06m 49s	Completed (2 attempts)	Details	Flush

```
┌──────────────┐          ┌──────────────────┐
│   Device     │          │ Device Added to  │          ◇ MDM Server            ╭──────────────╮
│   Ordering   │ ───────▶ │ Apple School     │ ───────▶ ◇ Assignment  ╌╌╌╌╌▶     │ Other Server │
│   Process    │          │ Manager by       │          ◇                         ╰──────────────╯
└──────────────┘          │ Supplier         │          ◇
                          └──────────────────┘          │
                                                         │
        ┌────────────────────────────────────────────────┘
        ▼
┌──────────────┐          ┌──────────────────┐          ┌──────────────────┐          ╭──────────────╮
│ Assigned to  │          │ Automatically    │          │ Set up and Power │          │ Wait for     │
│ Lab - DEP    │ ───────▶ │ Scoped to        │ ───────▶ │ on Device        │ ───────▶ │ Device       │
│              │          │ Lab - Auto       │          │                  │          │ Check in     │
└──────────────┘          │ Advance          │          └──────────────────┘          ╰──────────────╯
        ▲                 │ PreStage         │                                                 │
        │                 └──────────────────┘                                                 ▼
┌──────────────┐          ┌──────────────────┐          ╭──────────────╮          ┌──────────────────┐
│ Inventory    │          │ Runs Auto        │          │ Wait for Auto│          │ Checks in        │
│ Preload      │          │ Logon Policy     │ ◀─────── │ Advance to   │ ◀─────── │ with Jamf        │
│ Information  │          │ and Restarts     │          │ Complete     │          │                  │
└──────────────┘          └──────────────────┘          ╰──────────────╯          │ Runs             │
                                   │                                                │ PreStage         │
                                   ▼                                                └──────────────────┘
┌──────────────┐          ┌──────────────────┐          ╭──────────────╮          ┌──────────────────┐          ┌──────────────┐
│ Scoped       │          │ Runs             │          │ Wait for     │          │ Completes        │          │ Smart Group  │
│ Policies     │ ───────▶ │ Onboarding       │ ───────▶ │ Software     │ ───────▶ │ DEPNotify        │ ◀─────── │ Scoped       │
│              │          │ DEPNotify        │          │ Deployment   │          │                  │          │ Policies     │
└──────────────┘          │ Policy           │          ╰──────────────╯          │ Checks for       │          └──────────────┘
                          └──────────────────┘                                    │ other policies   │
                                                                                   │ based on         │
                                                                                   │ Smart Group      │
                                                                                   └──────────────────┘
                                                                                            │
        ┌───────────────────────────────────────────────────────────────────────────────────┘
        ▼
┌──────────────┐          ╭──────────────╮          ╭──────────────╮
│ Device       │          │ Device       │          │ Device at    │
│ Removes      │ ───────▶ │ Restarts     │ ───────▶ │ NoMAD        │
│ Auto Logon,  │          │              │          ╰──────────────╯
│ Installs     │          ╰──────────────╯
│ NoMAD        │
└──────────────┘
```

Q&A