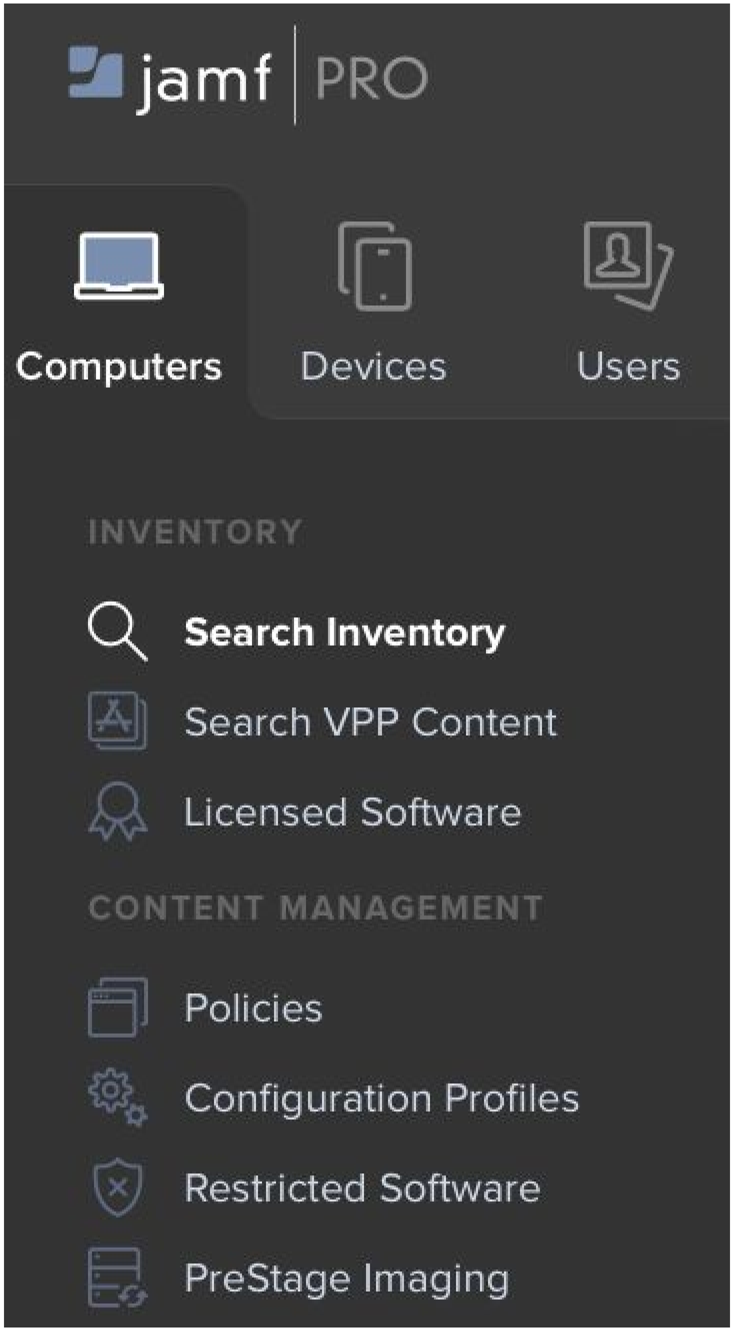
Jamf Pro

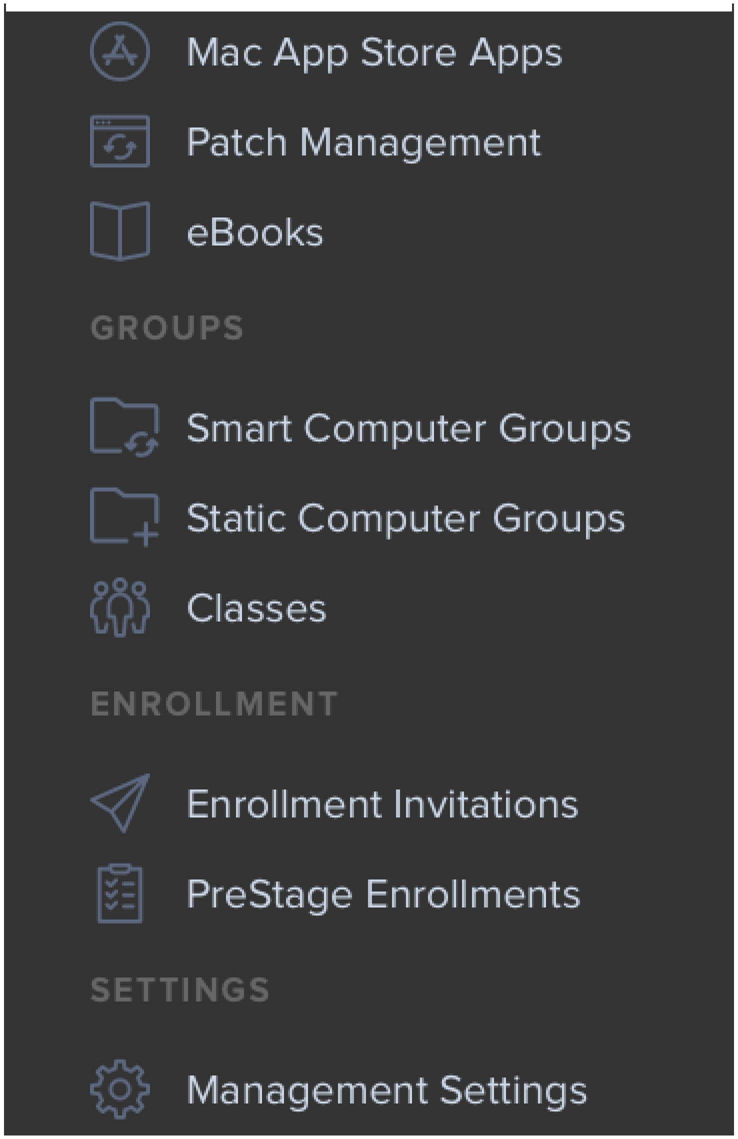
An overview of our Mac management system

jamf

What is Jamf Pro?

- Jamf Pro is a comprehensive management suite for Macintosh computers
- Jamf Pro allows us to push software, manage security settings, manage patching and updates, maintain an inventory, manage our PIV card login process, and much more
- Jamf Pro is a third party software suite that was originally conceived to fill in the gaps in enterprise management, and provide tools that Apple didn’t provide natively.

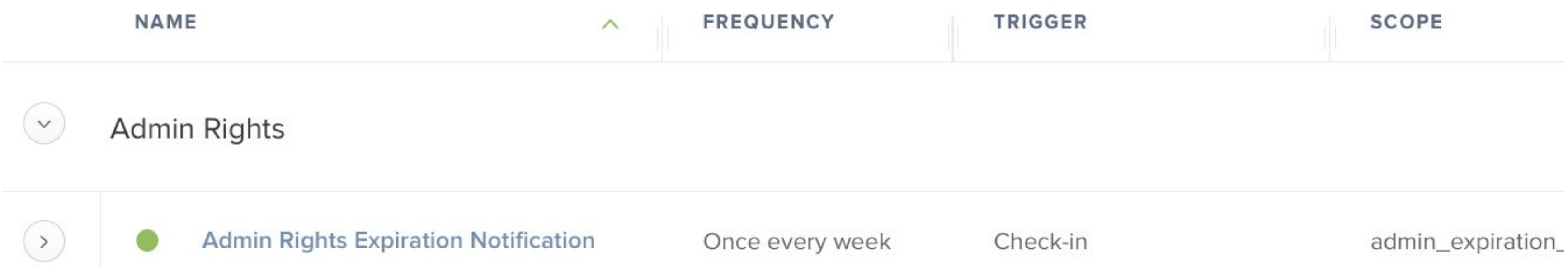

jamf | PRO
Computers
Devices
Users
INVENTORY
Search Inventory
Search VPP Content
Licensed Software
CONTENT MANAGEMENT
Policies
Configuration Profiles
Restricted Software
PreStage Imaging


Mac App Store Apps
Patch Management
eBooks
GROUPS
Smart Computer Groups
Static Computer Groups
Classes
ENROLLMENT
Enrollment Invitations
PreStage Enrollments
SETTINGS
Management Settings

- Jamf Pro’s bread and butter features are Inventory, Policies, Configuration Profiles, Patch Management, Smart Groups, and the scripting framework.

- A Policy is our primary content delivery vehicle, containing software packages or scripts, configurations, accounts, as well as the controls for when it runs, which Macs it runs on, and how it’s triggered. For a successful policy, you need to specify:
    - What - The thing that you are deploying
    - When - The frequency of the deployment
    - How - Via check-in, or self service, or custom
    - Who - Which Macs it is being deployed to

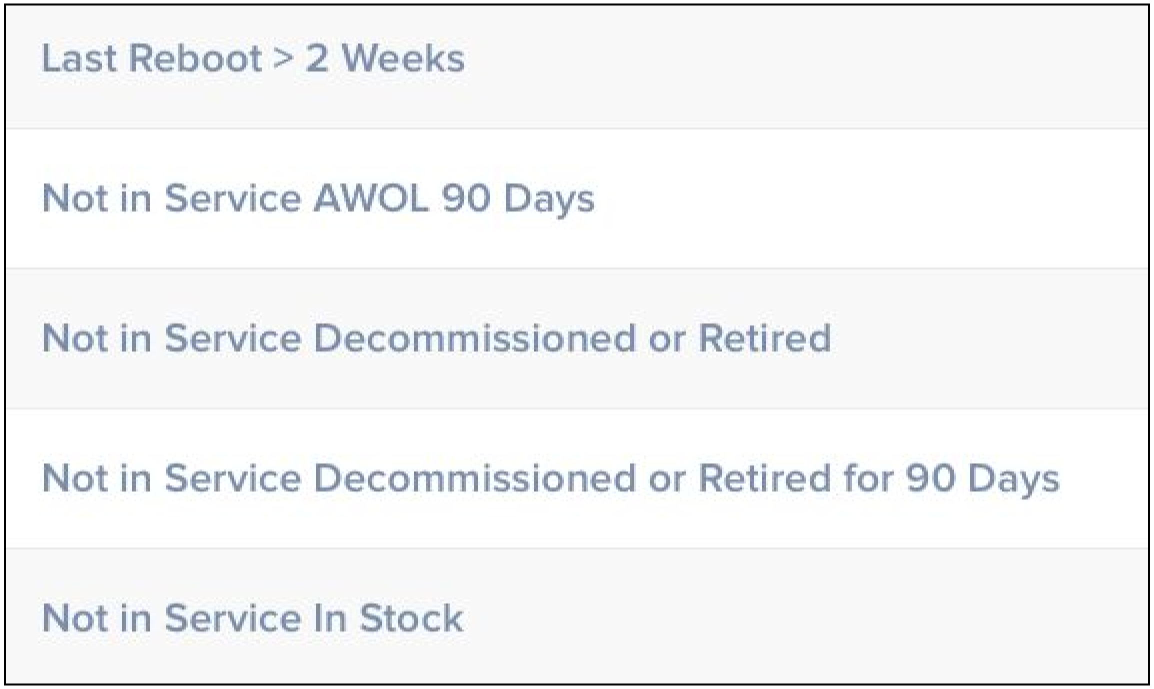
In Jamf Pro, these are called **Name, Frequency, Trigger and Scope.**



NAME	FREQUENCY	TRIGGER	SCOPE
Admin Rights			
● Admin Rights Expiration Notification	Once every week	Check-in	admin_expiration_

- **Name:** The name of the policy you are deploying.
- **Frequency:** The time interval. It can be once, once per user, once per computer, once per day, week, month, or ongoing.

- **Trigger:** The event that triggers the deployment. It can be Startup, Login, Logout, Check-in, Network change, On Enrollment, or you can create a custom trigger that can be called manually.
- **Scope:** The Macs it will be deployed to. This can be a Mac, a user, or a smart or static group. Example:



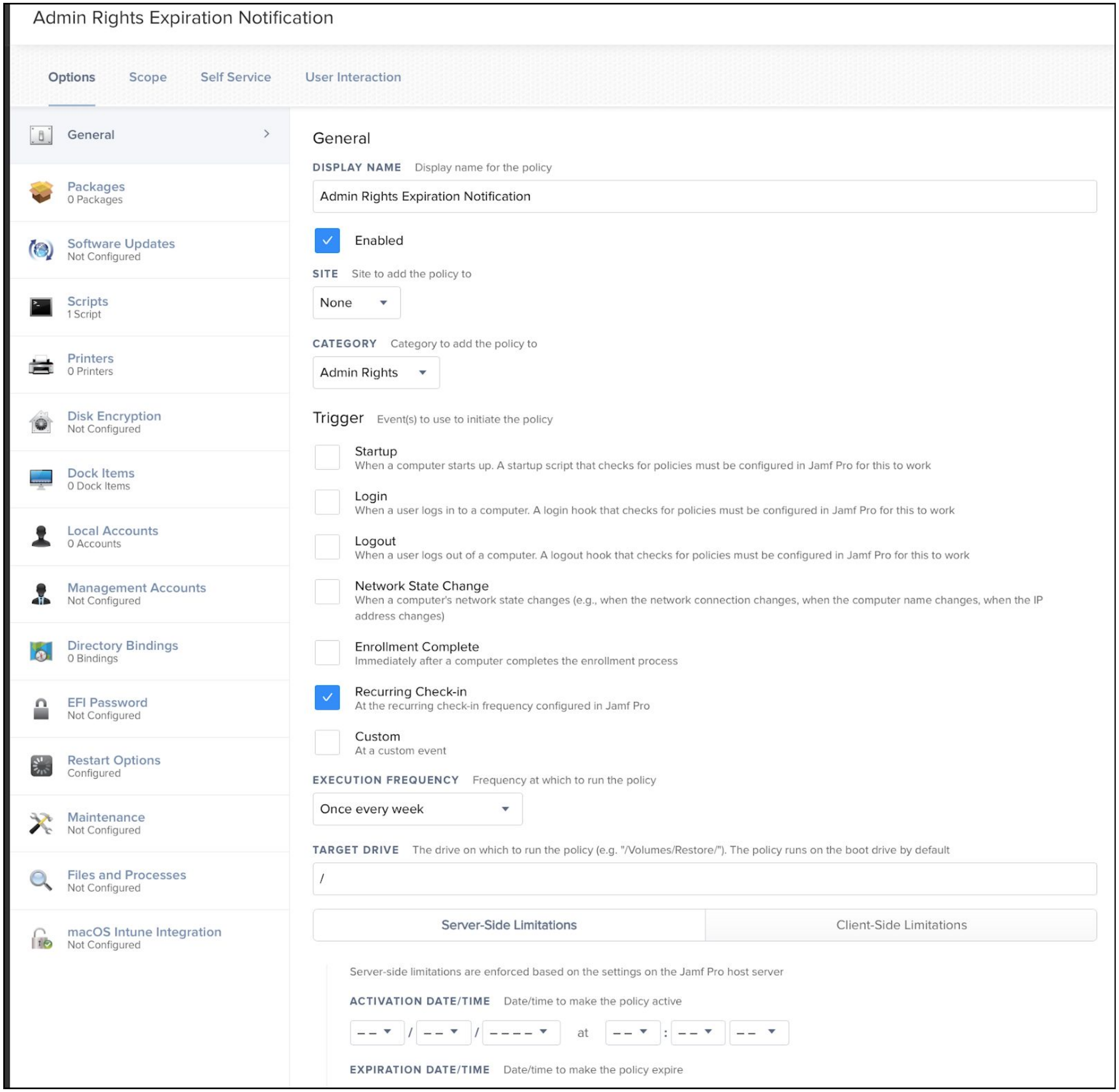
Last Reboot > 2 Weeks

Not in Service AWOL 90 Days

Not in Service Decommissioned or Retired

Not in Service Decommissioned or Retired for 90 Days

Not in Service In Stock



Admin Rights Expiration Notification

- General
- Packages — 0 Packages
- Software Updates — Not Configured
- Scripts — 1 Script
- Printers — 0 Printers
- Disk Encryption — Not Configured
- Dock Items — 0 Dock Items
- Local Accounts — 0 Accounts
- Management Accounts — Not Configured
- Directory Bindings — 0 Bindings
- EFI Password — Not Configured
- Restart Options — Configured
- Maintenance — Not Configured
- Files and Processes — Not Configured
- macOS Intune Integration — Not Configured

General

DISPLAY NAME Display name for the policy

Admin Rights Expiration Notification

☑ Enabled

SITE Site to add the policy to

None

CATEGORY Category to add the policy to

Admin Rights

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 hook that checks for policies must be configured in Jamf Pro for this to work

□ Logout
When a user logs out of a computer. A logout hook 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

EXECUTION FREQUENCY Frequency at which to run the policy

Once every week

TARGET DRIVE The drive on which to run the policy (e.g. "/Volumes/Restore/"). The policy runs on the boot drive by default

/

Server-Side Limitations | Client-Side Limitations

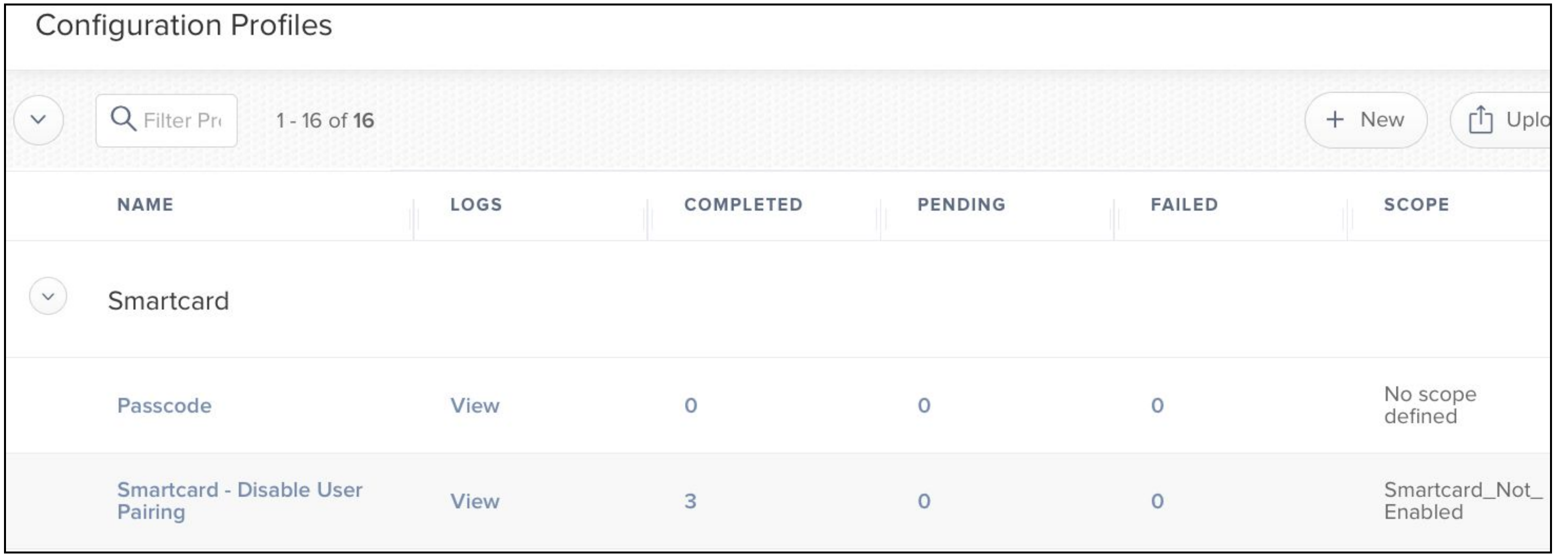
Server-side limitations are enforced based on the settings on the Jamf Pro host server

ACTIVATION DATE/TIME Date/time to make the policy active

– – / – – / – – – – at – – : – – – –

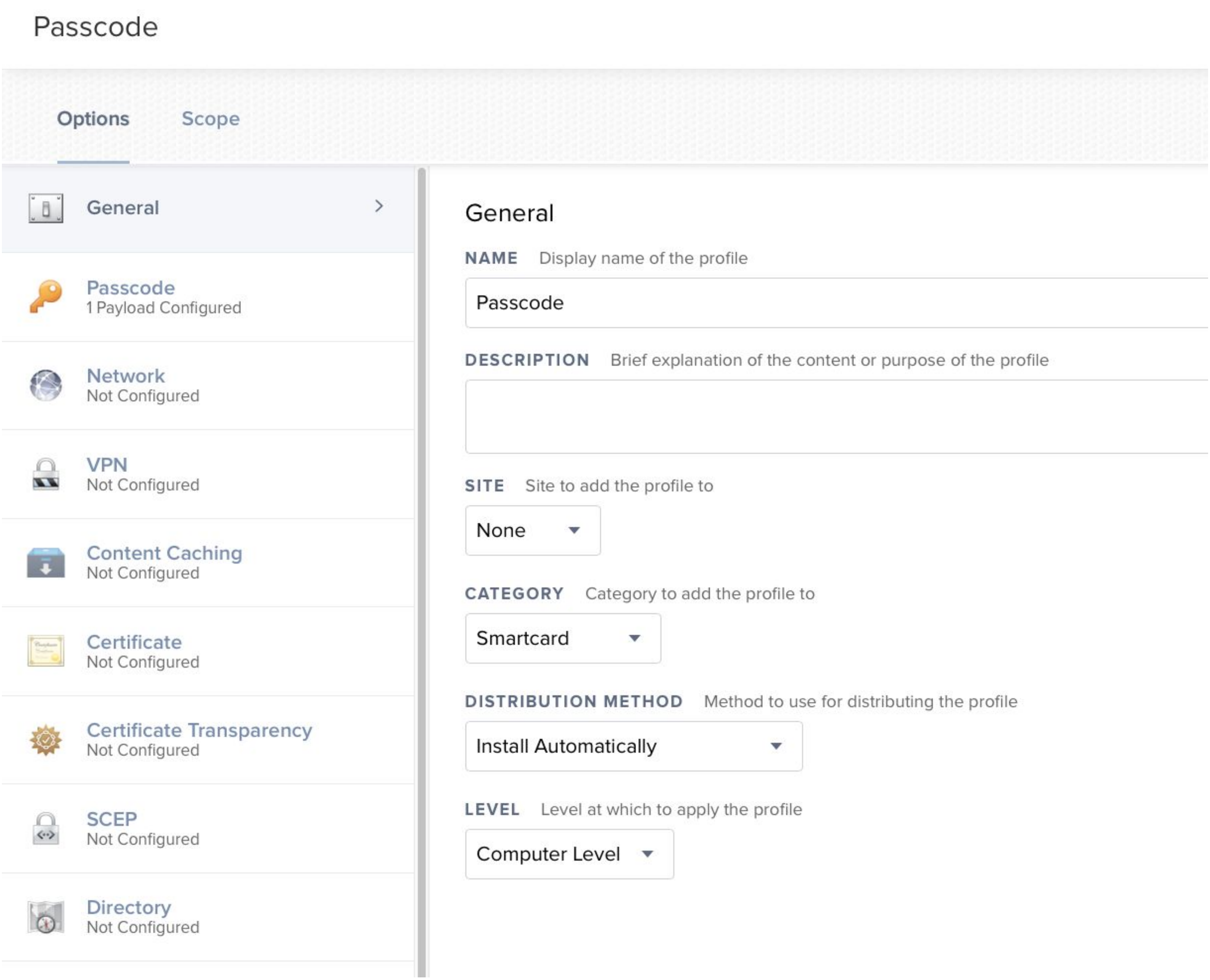
EXPIRATION DATE/TIME Date/time to make the policy expire

- Configuration Profiles are Jamf’s name for MDM profiles. MDM profiles are how we manage security settings on the Macs, whitelist kernel extensions, restrict software, manage and enable PIV logins. MDM commands are pushed instantly to the targeted Mac, and settings enabled by configuration profile are immediately reinforced if they change for any reason.



Configuration Profiles

NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
Smartcard					
Passcode	View	0	0	0	No scope defined
Smartcard - Disable User Pairing	View	3	0	0	Smartcard_Not_ Enabled



General

NAME Display name of the profile

Passcode

DESCRIPTION Brief explanation of the content or purpose of the profile

SITE Site to add the profile to

None

CATEGORY Category to add the profile to

Smartcard

DISTRIBUTION METHOD Method to use for distributing the profile

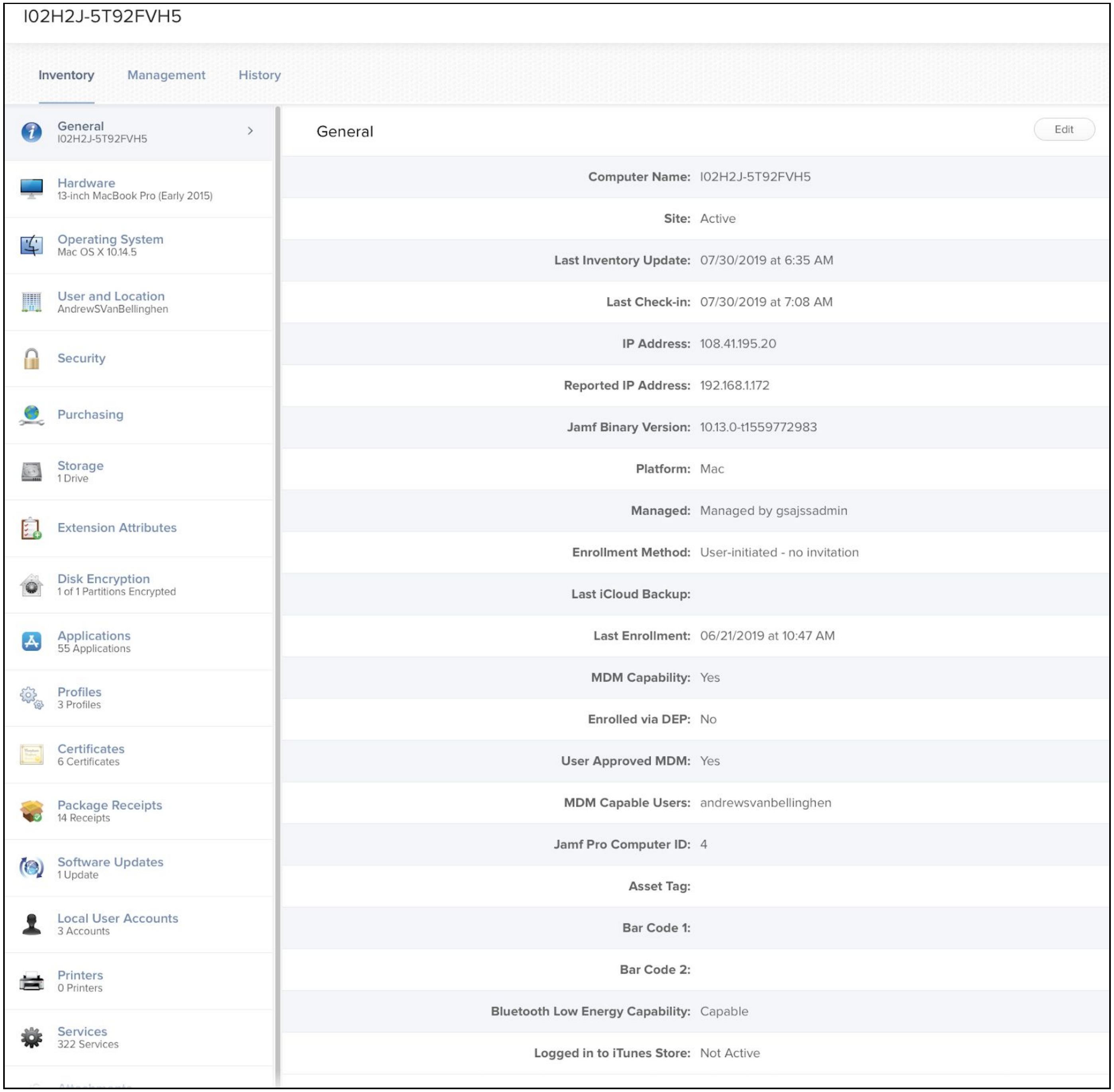
Install Automatically

LEVEL Level at which to apply the profile

Computer Level

- **Inventory:** Jamf pro takes an extensive inventory of every Mac, including info on every piece of hardware inside each Mac, software, settings, users, services, network settings, configuration profiles, disk encryption status, certificates, installed package receipts, usage stats, logs, etc.

- Inventory can be enhanced with **Extension Attributes**, which are customizable, scriptable containers that can be used to pull any info you can script into a format whose results can be used to create a smart group, which can be used to scope a policy.



I02H2J-5T92FVH5

- General
  I02H2J-5T92FVH5
- Hardware
  13-inch MacBook Pro (Early 2015)
- Operating System
  Mac OS X 10.14.5
- User and Location
  AndrewSVanBellinghen
- Security
- Purchasing
- Storage
  1 Drive
- Extension Attributes
- Disk Encryption
  1 of 1 Partitions Encrypted
- Applications
  55 Applications
- Profiles
  3 Profiles
- Certificates
  6 Certificates
- Package Receipts
  14 Receipts
- Software Updates
  1 Update
- Local User Accounts
  3 Accounts
- Printers
  0 Printers
- Services
  322 Services

General

Computer Name: I02H2J-5T92FVH5

Site: Active

Last Inventory Update: 07/30/2019 at 6:35 AM

Last Check-in: 07/30/2019 at 7:08 AM

IP Address: 108.41.195.20

Reported IP Address: 192.168.1.172

Jamf Binary Version: 10.13.0-t1559772983

Platform: Mac

Managed: Managed by gsajssadmin

Enrollment Method: User-initiated - no invitation

Last iCloud Backup:

Last Enrollment: 06/21/2019 at 10:47 AM

MDM Capability: Yes

Enrolled via DEP: No

User Approved MDM: Yes

MDM Capable Users: andrewsvanbellinghen

Jamf Pro Computer ID: 4

Asset Tag:

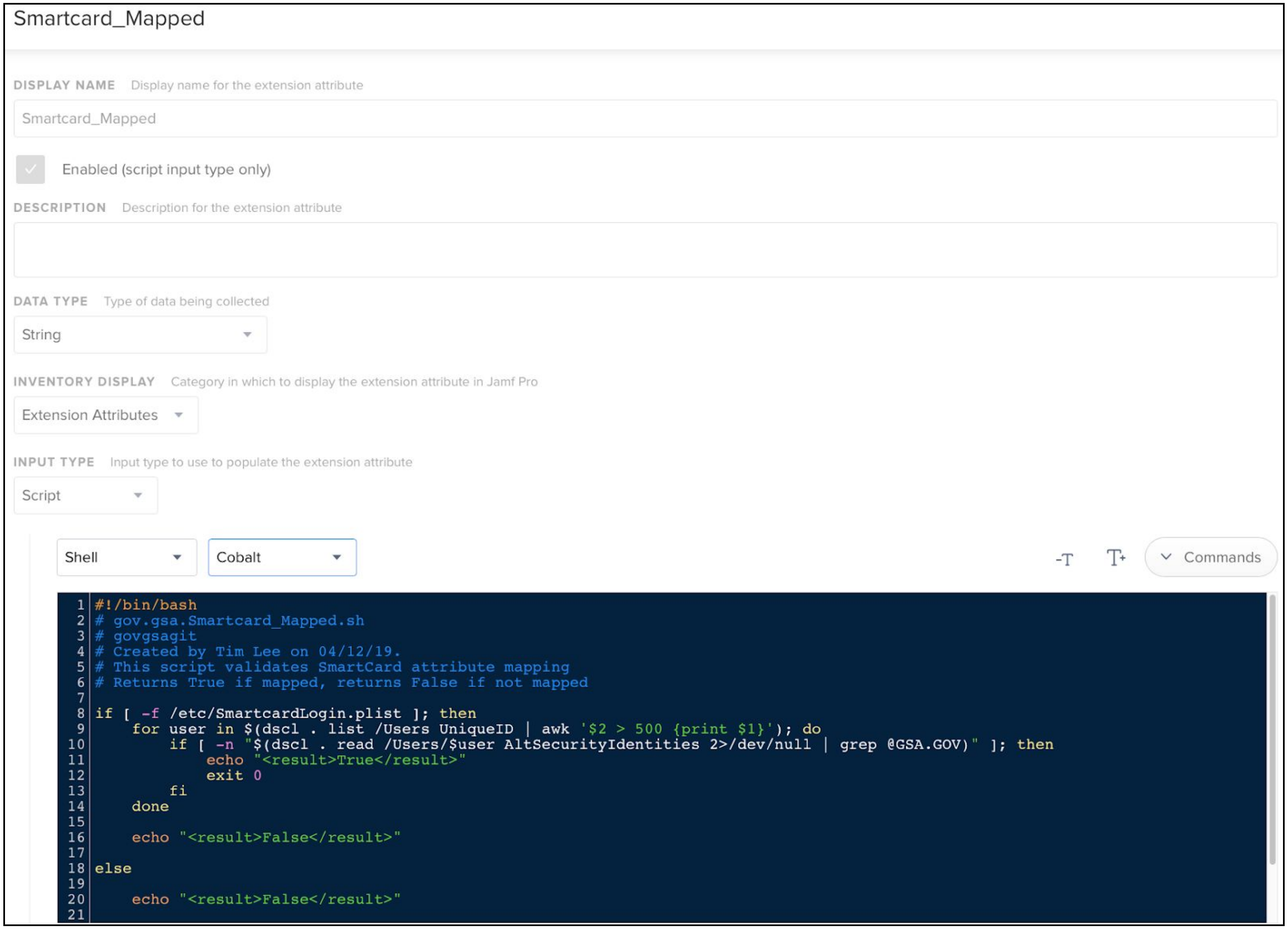
Bar Code 1:

Bar Code 2:

Bluetooth Low Energy Capability: Capable

Logged in to iTunes Store: Not Active

- Extension Attribute:



Smartcard_Mapped

DISPLAY NAME Display name for the extension attribute

Smartcard_Mapped

☑ Enabled (script input type only)

DESCRIPTION Description for the extension attribute

DATA TYPE Type of data being collected

String

INVENTORY DISPLAY Category in which to display the extension attribute in Jamf Pro

Extension Attributes

INPUT TYPE Input type to use to populate the extension attribute

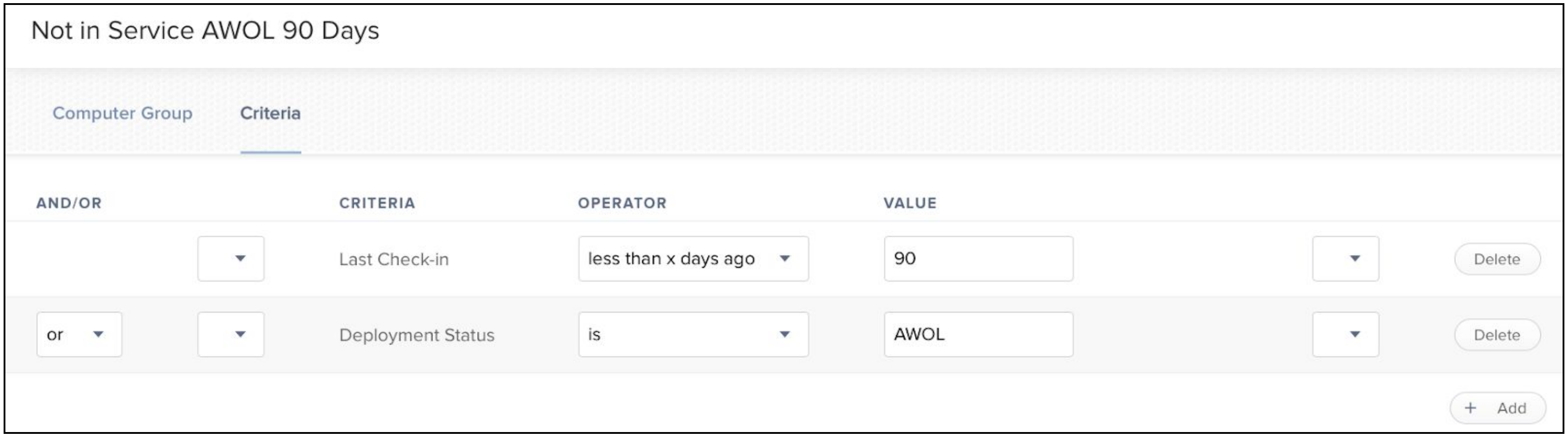
Script

Shell

Cobalt

```
#!/bin/bash
# gov.gsa.Smartcard_Mapped.sh
# govgsagit
# Created by Tim Lee on 04/12/19.
# This script validates SmartCard attribute mapping
# Returns True if mapped, returns False if not mapped

if [ -f /etc/SmartcardLogin.plist ]; then
    for user in $(dscl . list /Users UniqueID | awk '$2 > 500 {print $1}'); do
        if [ -n "$(dscl . read /Users/$user AltSecurityIdentities 2>/dev/null | grep @GSA.GOV)" ]; then
            echo "<result>True</result>"
            exit 0
        fi
    done

    echo "<result>False</result>"

else

    echo "<result>False</result>"

```

- Smart Group:

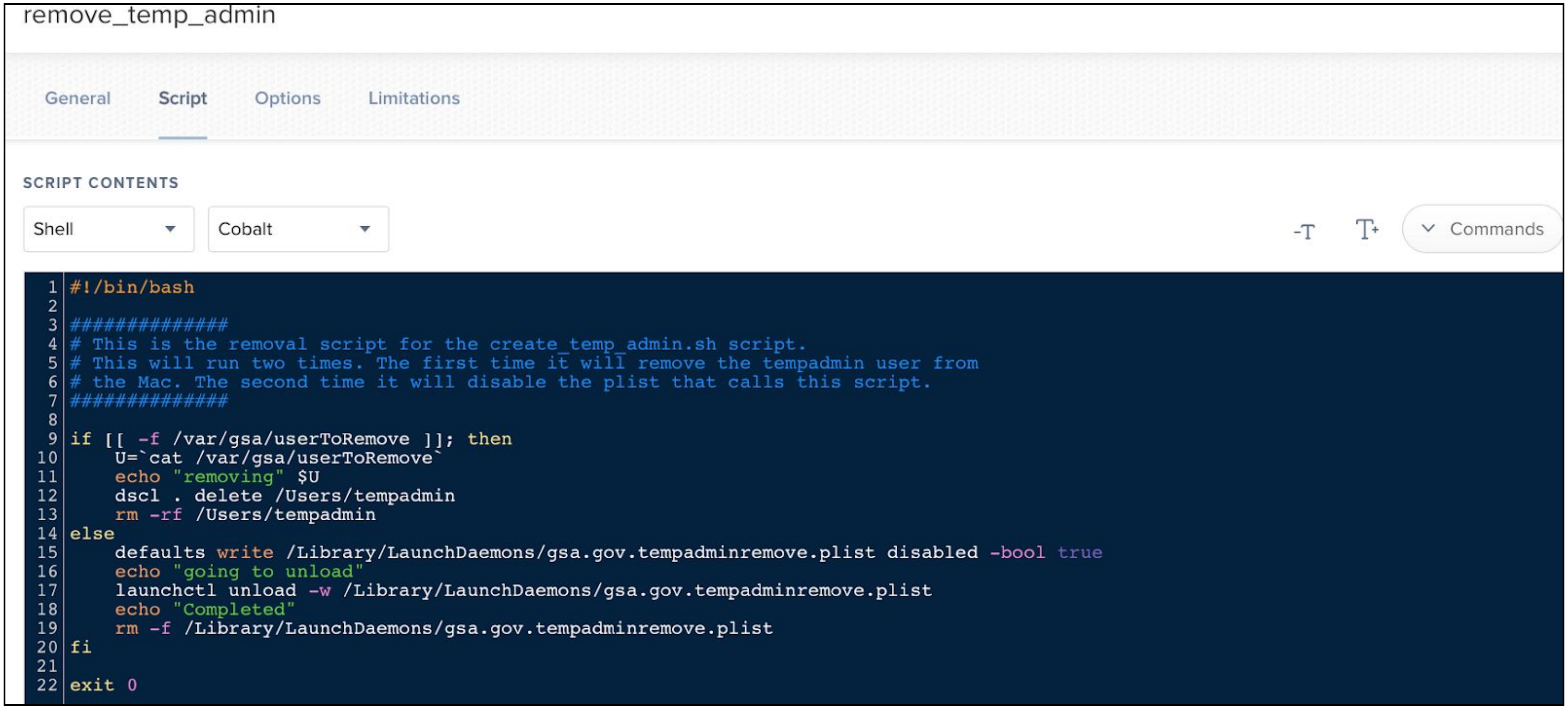


Not in Service AWOL 90 Days

AND/OR		CRITERIA	OPERATOR	VALUE		
		Last Check-in	less than x days ago	90		Delete
or		Deployment Status	is	AWOL		Delete

- Smart groups can use any of the built in criteria to determine membership in the group, or they can use **Extension Attributes** as the criteria. **EAs** can pull any information from the OS that you can script, which is nearly everything because macOS is based on **BSD Unix**.

- **Scripting:** MacOS is largely scriptable, so Jamf Pro has a built-in scripting interface that allows you to create functional shell scripts that can be used to accomplish anything you can script in MacOS.



remove_temp_admin

SCRIPT CONTENTS

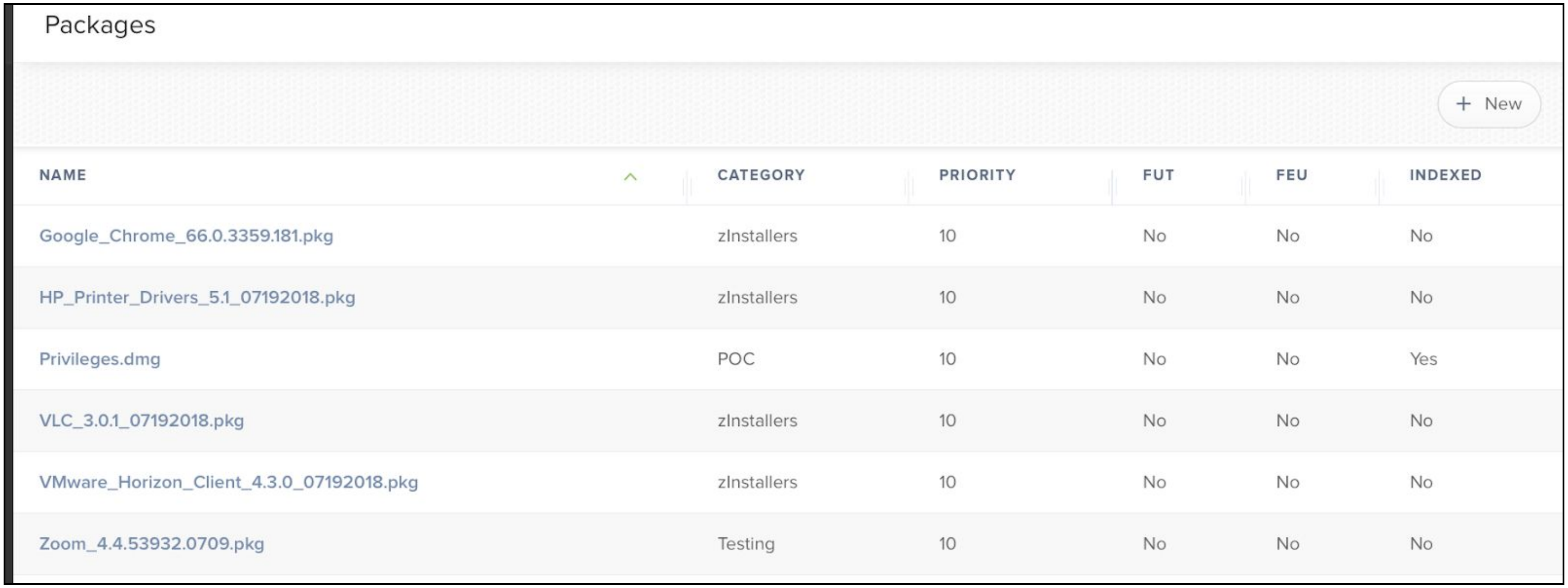
Shell

Cobalt

```
#!/bin/bash

##############
# This is the removal script for the create_temp_admin.sh script.
# This will run two times. The first time it will remove the tempadmin user from
# the Mac. The second time it will disable the plist that calls this script.
##############

if [[ -f /var/gsa/userToRemove ]]; then
    U=`cat /var/gsa/userToRemove`
    echo "removing" $U
    dscl . delete /Users/tempadmin
    rm -rf /Users/tempadmin
else
    defaults write /Library/LaunchDaemons/gsa.gov.tempadminremove.plist disabled -bool true
    echo "going to unload"
    launchctl unload -w /Library/LaunchDaemons/gsa.gov.tempadminremove.plist
    echo "Completed"
    rm -f /Library/LaunchDaemons/gsa.gov.tempadminremove.plist
fi

exit 0
```

- Scripts can be deployed through **policies**, like any other package, with the same controls over who, what, where and when.

- **Packages:** Packages are hosted on the Jamf server, and Jamf recognizes packages from developers like Microsoft, or we can use Jamf Composer to create our own packages.
- Packages are also deployed through **policies**, with the same controls applied.



Packages

NAME	CATEGORY	PRIORITY	FUT	FEU	INDEXED
Google_Chrome_66.0.3359.181.pkg	zInstallers	10	No	No	No
HP_Printer_Drivers_5.1_07192018.pkg	zInstallers	10	No	No	No
Privileges.dmg	POC	10	No	No	Yes
VLC_3.0.1_07192018.pkg	zInstallers	10	No	No	No
VMware_Horizon_Client_4.3.0_07192018.pkg	zInstallers	10	No	No	No
Zoom_4.4.53932.0709.pkg	Testing	10	No	No	No

NEXT: Live Demo!