



Welcome everyone to JAMF Nation User Conference 2014!

This is the first session after the keynote so I'll insert the obvious statement of please mute all your devices. It's not for me, it's for your neighbor. But if I hear it I may just answer the phone for you... who knows. so... lets get started!

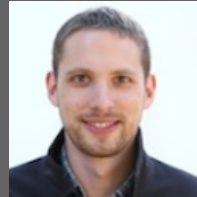
Policies 101: Unleash the Power

Have to cover 50 slides in 30 mins to leave adequate time for Q/A.



Justin Rummel

Director of Operations
Stony River Technologies



Cameron Evjen

Director of Education Services
JAMF Software



I'm Justin, that was Cam.

Policies 101: Unleash the Power

Presentation agenda:

Policies

There is no #2, it's Policies!

Don't make me hurt you

OK, I'll provide some examples

Our agenda is pretty strait forward we're covering Policies!

#3 – Like FightClub “We only talk about Policies”

Policies Manifesto

Policies are comprised of two elements

- What do I want to do?
- To Whom?

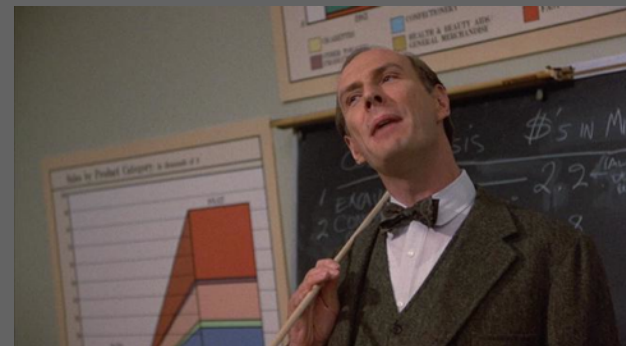
During my JumpStarts I try to break things down to simple goal oriented statements; with Policies...

The What part is very easy as long as you have objects ready to go. Objects being: PKGs, DMGs, Directory (AD) Binding, Dock items, Printers, FileVault settings, etc.

Policies

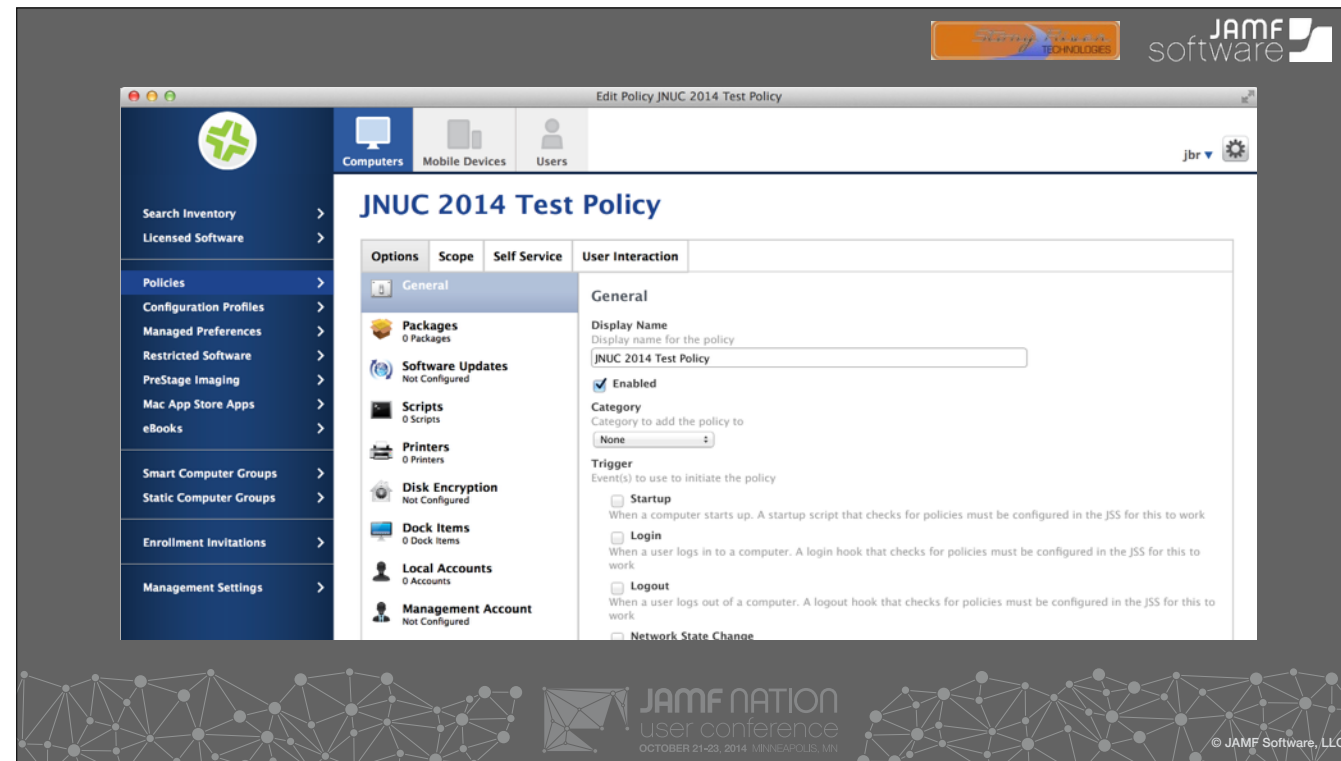
“What do I want to do”

- General
- Packages
- etc...



“I simply have one question; in 27 parts”.

When you create a new policy, there are several items on the left hand column in the main body area of your Browser screen that is focused on the JSS. General is required, but the rest (Packages, Scripts, Printers, etc) are all optional and have customized settings. We’re going to review each item and I’ll add my personal comments to each section.



(take your mental picture for reference)

General

- Display Name
- Enabled
- Category

DN: “pretty name” – for the Admin or for the end user i.e. (Self Service)

Category:

1. These were created by going to the Gear Icon, then to Global Management, finally Categories – in a Policy they are listed alphabetically.
2. Important for Self Service

Triggers

- Startup
- Login
- Logout



JAMF software

JAMF NATION
user conference
OCTOBER 21-23, 2014 MINNEAPOLIS, MN

© JAMF Software, LLC

(after Lord business)

Startup: Enforce Firewall Settings or Network environment checks

Login: File Share Mounts via DNS validation

These Triggers require the Startup and Login scripts to be enabled in Gear Icon -> Computer Management
-> Check-in

```
16 ### Variables
17 DNS_SERVER="10.13.12.122"
18 FILE_SERVER="host.domain.tld"
19 SHARE_NAME="Shared"
20 PROTOCOL="afp"
21
22 WIFI=`networksetup -listnetworkserviceorder | grep "Wi-Fi" | tail -1 | awk -F ":" '{print $NF}' | sed 's/)//g'`
23 ETHERNET=`networksetup -listnetworkserviceorder | grep "Ethernet" | tail -1 | awk -F ":" '{print $NF}' | sed 's/)//g'`
24
25 WIFI_DNS=`ipconfig getpacket "${WIFI}" | awk '/domain_name_server/ {print $NF}' | sed 's/)//g'`
26 ETH_DNS=`ipconfig getpacket "${ETHERNET}" | awk '/domain_name_server/ {print $NF}' | sed 's/)//g'`
27
28 ### Functions
29 net_mount() {
30     open "${PROTOCOL}://${FILE_SERVER}/${SHARE_NAME}/"
31 }
32
33 [[ "${ETH_DNS}" == "${DNS_SERVER}" ]] && { net_mount; exit 0; } || { echo "${ETH_DNS}"; }
34 [[ "${WIFI_DNS}" == "${DNS_SERVER}" ]] && { net_mount; exit 0; } || { echo "${WIFI_DNS}"; }
35
36 echo "Not on the network. I'll stop now."
37 exit 0
```

https://github.com/stonyrivertech/SRT-Public/blob/master/JAMF/FileShare_mount.sh

Triggers

- Network State Change
- Enrollment Complete
- Recurring Check-in
- Custom
 - `sudo jamf policy -event runNumberTwo`

Enroll: Thin Imaging model with “First Run Script” or Core Application install

Recurring: “Client checks in...”

Custom: Testing, but I prefer using Scope, Cascading Policies

Execution Frequency

- Once Per Computer
- Once Per User
- Once a Day
- Once a Week
- Once a Month
- Ongoing

Once per computer means “ONCE”. IF failed, too bad. 525,600 times (rent)
Once per week/month: SUS
Ongoing: next

Execution Frequency

- Once Per Computer
- Once Per User
- Once a Day
- Once a Week
- Once a Month
- Ongoing

Execution Frequency
Frequency at which to run the policy

Make Available Offline
Cache the policy to ensure it runs when the JSS is unavailable

Ongoing “Cache the policy to ensure it runs when the JSS is not available”.

General

- Server-side limitations
- Client-side limitations
 - Do Not Run Between Hours
 - Do Not Run On Particular Days
 - Network Connection (Must be Ethernet)

Server: Activation or Expiration Date/Time

Beta seeds for testing to your test user group

Client: Again, run SUS at night, but only on the Weekends

Ethernet: LARGE packages

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages 1 Package
- Software Updates Configured
- Scripts 0 Scripts
- Printers 0 Printers
- Disk Encryption Not Configured
- Dock Items 0 Dock Items
- Local Accounts 0 Accounts
- Management Account Not Configured

Packages

Bash Update Mavericks

Action
Action to take on computers
Install

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

Distribution Point
Distribution point to download the package(s) from
Each computer's default distribution point

Packages

- Action
 - Install
 - Cache
 - Install from Cache
- Select your Distribution Point

Cache: for large packages (iMovie, FCP, Adobe) for a better End User experience (/Library/Application Support/JAMF/Waiting Room/)

DP: Default, DP, JDS, Cloud (depends on what is configured)

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages 1 Package
- Software Updates Configured
- Scripts 0 Scripts
- Printers 0 Printers
- Disk Encryption Not Configured
- Dock Items 0 Dock Items
- Local Accounts 0 Accounts
- Management Account Not Configured

Software Updates

Install Software Updates From
Software update server to install software updates from
Each computer's default software update server

Software Updates

- Install Software Updates Install
 - Device Default (via Configuration Policy)
 - From Apple



JAMF software

JAMF NATION
user conference
OCTOBER 21-23, 2014 MINNEAPOLIS, MN

© JAMF Software, LLC

Create a policy that could be triggered once a month to automatically install all items found.

Create a policy that could be available in Self Service once a month to install updates

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages 1 Package
- Software Updates Configured
- Scripts 1 Script
- Printers 0 Printers
- Disk Encryption Not Configured
- Dock Items 0 Dock Items
- Local Accounts 0 Accounts
- Management Account Not Configured

Scripts

displayMessage.sh

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

Main Message

Background Message (optional)

Parameter 6

Parameter 7

Parameter 8

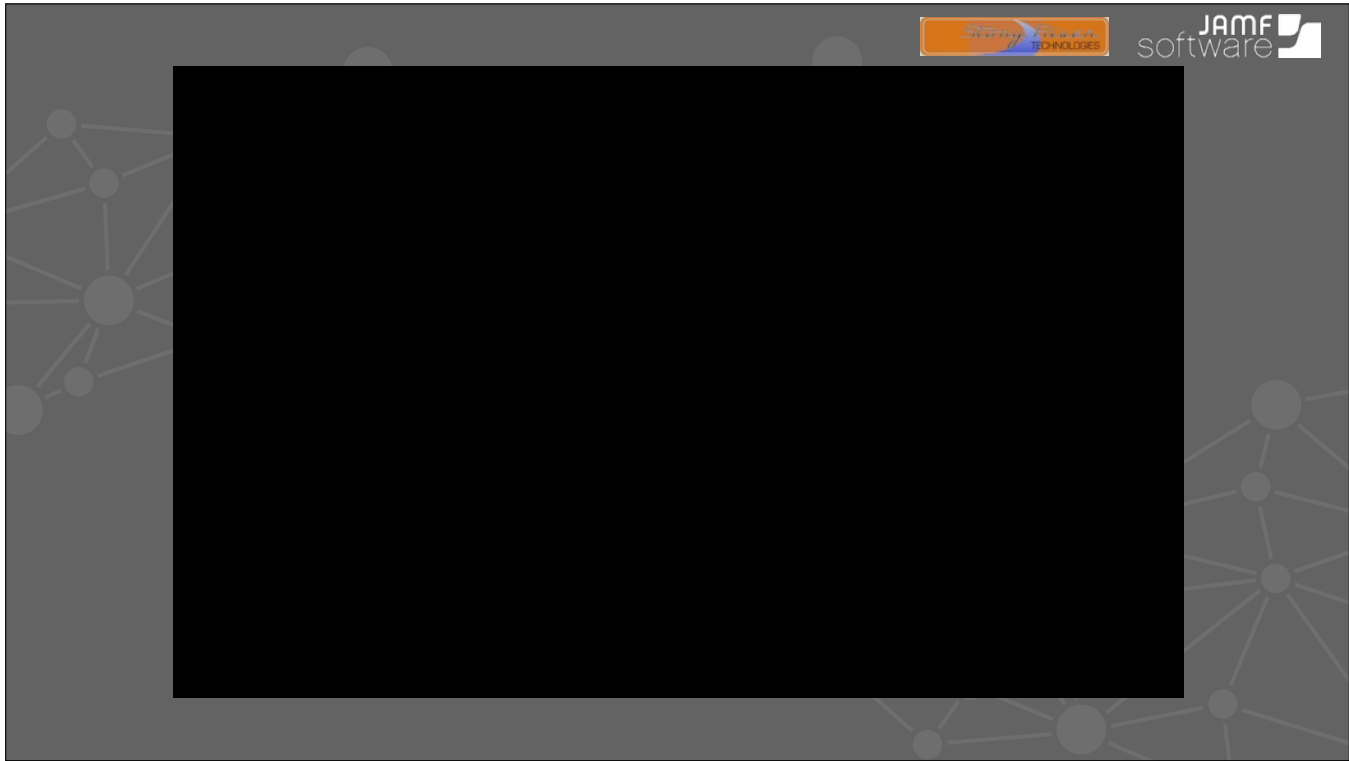
Scripts

- Any script executed through the Casper Suite will automatically receive the first three variables in the following order
 - \$1 = Mount point of the target drive
 - \$2 = Computer name
 - \$3 = Username *

kbase in Resource slide

* Available on a policy at login or via self service

```
1 #!/bin/sh
2
3 # Variables
4 one="${1}"
5 two="${2}"
6 three="${3}"
7 message="VAR #1: ${one}, VAR #2: ${two}, VAR #3: ${three}"
8 background="true"
9
10 [[ "${background}" == "true" ]] && { jamf displayMessage -message "${message}"; logger "${message}"; }
11
12 exit 0
13
```





JAMF software

File Policy JNUC 2014 Test Policy

Computers Mobile Devices Users

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

General

Packages 1 Package

Software Updates 1 Package Configured

Scripts 1 Script

Printers 1 Printer

Disk Encryption Not Configured

Dock Items 1 Dock Item

Local Accounts 1 Account

Management Account Random 0 characters

Directory Bindings Not Configured

EFI Password Not Configured

Restart Options Configured

Maintenance Configured

Dock Items

Self Service

Action Action to take on computers

Add to end of Dock

File Policy JNUC 2014 Test Policy

Computers Mobile Devices Users

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

General

Packages 1 Package

Software Updates 1 Package Configured

Scripts 1 Script

Printers 1 Printer

Disk Encryption Not Configured

Local Accounts 1 Account

Management Account Random 0 characters

Directory Bindings Not Configured

EFI Password Not Configured

Restart Options Configured

Maintenance Configured

Printers

HP 8500A [1]

Action Action to take on computers

Use as Default

Use as the default printer

Printers and Docks

- Printers
 - Add/Remove Printer Configurations, plus set as Default
- Docks
 - Add to left or right, plus Remove

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages (1 Package)
- Software Updates (Configured)
- Scripts (1 Script)
- Printers (0 Printers)
- Disk Encryption (Not Configured)
- Dock Items (0 Dock Items)
- Local Accounts (1 Account)
- Management Account (Not Configured)

Local Accounts

Action: Action to take on computers
Create Account

Username: Username/short name for the account
heman

Full Name: Display name/long username for the account
He Man

Password: Password for the account

Verify Password: ****

Home Directory Location: Full path in which to create the home directory (e.g. "/Users/username/" or "/private/var/username/")

Local Accounts

- Create Local Account
 - Allow as Admin
 - Enable as FileVault
- Reset Password
- Delete Account
- Disable for FileVault



Example: Lab environment for testing, add a “testing” user the night before, and at the end of the day change the password. 14 days later delete the user.

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages (1 Package)
- Software Updates (Configured)
- Scripts (1 Script)
- Printers (0 Printers)
- Disk Encryption (Not Configured)
- Dock Items (0 Dock Items)
- Local Accounts (1 Account)
- Management Account (Configured)

Management Account

Action: Action to take on computers
Specify new password

New Password: New password for the management account
[Required]

Verify Password: [Required]

Management Account

- Change Password
 - Can be random, and why not?
- Enable/Disable for FileVault 2

My Best Practices: Management should be separate from the Admin account used by Helpdesk.

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages (1 Package)
- Software Updates (Configured)
- Scripts (1 Script)
- Printers (0 Printers)
- Disk Encryption (Not Configured)
- Dock Items (0 Dock Items)
- Local Accounts (1 Account)
- Management Account (Configured)

Restart Options

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 if a package or update requires it

User Logged In Action
Action to take if a user is logged in to the computer
Restart if a package or update requires it

Delay
Amount of time to wait before the restart begins
5 Minutes

Restart Options

- Startup Disk
 - Current Disk, NetBoot, Installer, Custom
- Restart Action
 - If a PKG or Update requests, should a restart be performed
 - Delay if someone is logged in?
 - Running apps may interrupt a restart

Test Test Test!!!

What if the you are running a firmware update?

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages (1 Package)
- Software Updates (Configured)
- Scripts (1 Script)
- Printers (0 Printers)
- Disk Encryption (Not Configured)
- Dock Items (0 Dock Items)
- Local Accounts (1 Account)
- Management Account (Configured)

Maintenance

- Update Inventory
Force computers to submit updated inventory information to the JSS
- Reset Computer Names
Change the computer name on computers to match the computer name in the JSS
- Install Cached Packages
Install packages cached by the Casper Suite
- Fix Disk Permissions
- Fix ByHost Files
- Flush System Caches
Flush caches from /Library/Caches/ and /System/Library/Caches/, except for any com.apple.LaunchServices caches
- Flush User Caches
Flush caches from ~/Library/Caches/, ~/jpi_cache/, and ~/Library/Preferences/Microsoft/Office version #/Office Font Cache
- Verify Startup Disk

Maintenance

- Update Inventory!!!
- Reset Name
- Install all Cached items
- “Mac VooDoo”

Update b/c we must know that items have been complete
Reset name does the “scutil” to remove those pesky “(2)” names
Install _all_ Cached items
Voodoo: Fix Permissions, ByHost, Flush System Cache

Edit Policy JNUC 2014 Test Policy

Computers Mobile Devices Users jbr

JNUC 2014 Test Policy

Options Scope Self Service User Interaction

- General
- Packages 1 Package
- Software Updates Configured
- Scripts 1 Script
- Printers 0 Printers
- Disk Encryption Not Configured
- Dock Items 0 Dock Items
- Local Accounts 1 Account
- Management Account Random 8 characters

Files and Processes

Search for File by Path
Full path to the file

 Delete file if found

Search for File by Filename
Name of the file, including the file extension. This field is case-sensitive and returns partial matches

Update "locate" database
Update the "locate" database before searching for the file

Search for File Using Spotlight
File to search for. This field is not case-sensitive and returns partial matches

Search for Process
Name of the process. This field is case-sensitive and returns partial matches

 Kill process if found
This works with exact matches only

Files and Processes

- Find a File or Folder
 - Option to Delete if found
- Process
 - Option to kill if found
- Run Command



Find: full path, “locate” command, Spotlight “mdfind”

Process: pgrep or pkill

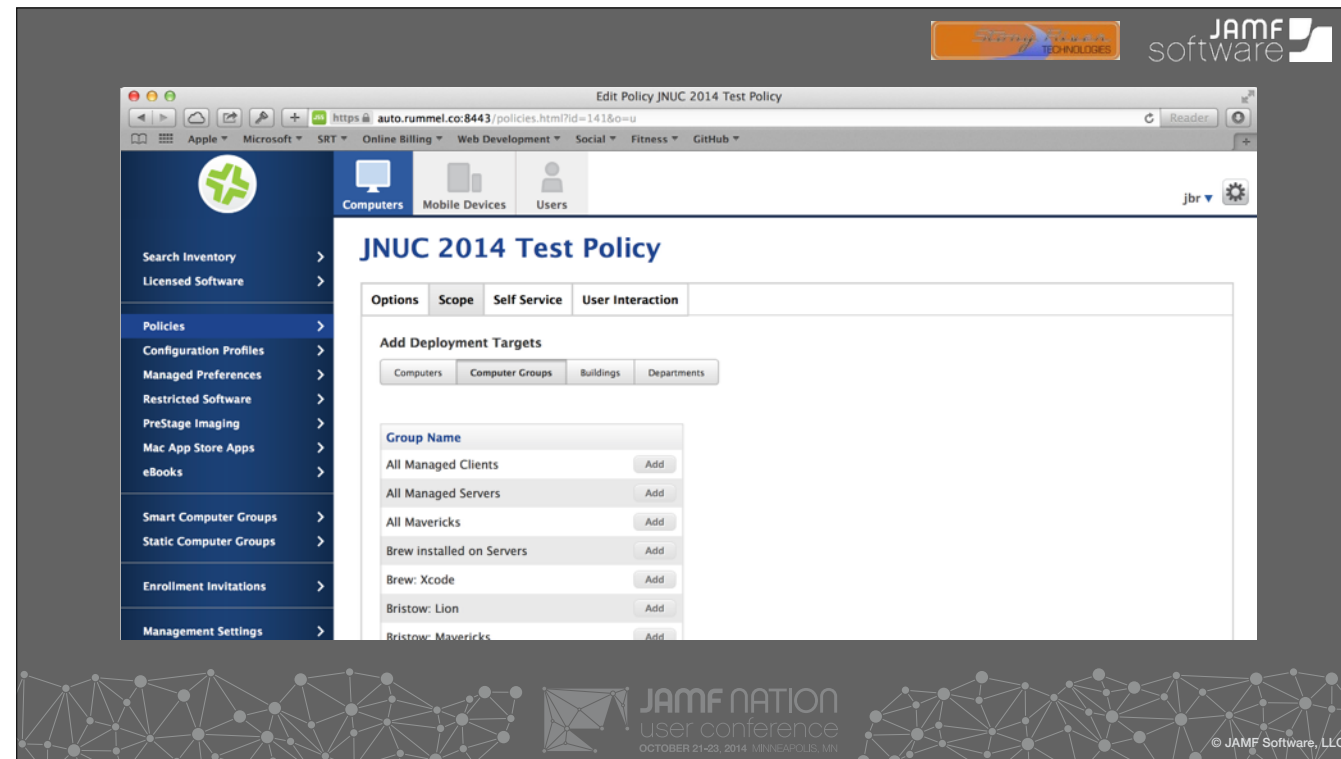
Run: say -v cellos Droid

—— Please be careful on the delete/kill options => next slide

Policies

“To Whom”

- Scope
- Self Service



Computers == individual devices

Groups == Smart or Static

Buildings/Departments made available in Gear => Network Organization AND must be selected on the Devices "User and Location" tab

Scope - Targets

- Bring a Sledge hammer and use ALL!!!
- Specific
 - Computers
 - Groups
 - Departments
 - Buildings

Scope - Limitations

- Of the targets that were previously selected, make sure they are also part of:
 - Network Segment
 - LDAP or Local Account
 - LDAP Group
 - iBeacon

Script example the one line command of “open afp://server/share” with a network segment limitation.
Your network must be unique! no 192.168.0.x or
192.168.1.x!!!

Scope - Exclusions

- Do not run this policy if a device is within one of the following:
 - Computers, Groups, Departments, Buildings, Network Segments, iBeacons

Concepts IT Department, VIPs. ? Does that work for you?

Browser: auto.rummel.co:8443/policies.html?id=1418o=u

Navigation: Computers, Mobile Devices, Users

JNUC 2014 Test Policy

Options | Scope | **Self Service** | User Interaction

- Make the policy available in Self Service
 - Button Name**
Name for the button that users click to initiate the policy
Install
 - Description**
Description to display for the policy in Self Service
YOU MUST READ ME
- Ensure that users view the description
Force users to view the description before the policy runs
- Icon**
Icon to display for the policy. It is recommended that you use a file with the GIF or PNG format. The recommended size is 128x128 pixels
 - Upload Icon
 - Select Existing Icon
- Feature the policy on the main page

Self Service

- One of the key elements for having your users feel that they are empowered to control their machines, even when their account is a Standard User.
- Able to use Icons to customize the look and feel of what is being installed

“This is how you make users with “Standard” user accounts feel like they have Power! (Preview trick)

Browser window: Edit Policy JNUC 2014 Test Policy
URL: https://auto.rummel.co:8443/policies.html?id=141&o=u

Navigation: Computers | Mobile Devices | Users | jbr

JNUC 2014 Test Policy

Options | Scope | Self Service | User Interaction

Start Message
Message to display before the policy runs
Microsoft Office Update will now begin. This update will force you to quit Word, PowerPoint, Excel, Outlook and any web browser (sorry, it will). Save now!

Allow Deferral
Allow users to defer the policy. A deferral limit must be specified for this to work

Deferral Limit
Date/time at which to prohibit further deferral. The policy runs at this date/time if it has not run yet
10 / 24 / 2014 at 3:00 p.m.

Complete Message
Message to display when the policy is complete
Microsoft Office Update is now complete. You may return to using Office and any web browser applications.

Restart Message
Message to display before computers restart
This computer will restart in 5 minutes. Please save anything you are

User Interaction

- Start message
- Defer for
 - 1hr, 2hr, 4hr, 8hr, or absolute deadline
- Complete message



You are doing this for your end users b/c you care.

Examples

- Microsoft Office 2011 14.4.5 Update
- Bash Patch
- Yosemite Update (not Imaging)

Microsoft Office 2011 14.4.5 Update

- What
 - Download 14.4.5 Update from Microsoft
- Whom
 - Smart Group for Devices that have Microsoft Word.app, but NOT version 14.4.5
- Bonus Level - Defer Options

Bash Patch

- What
 - Apple's OS Specific patches (Lion, Mountain Lion, and Mavericks are all different Downloads)
- Whom
 - Smart Group for each patch to their corresponding OS of 10.x.
5

May need to have people run software update to get to each respective “latest and greatest”.

Or scope Yosemite to all users. done!

Yosemite Update (not Imaging)

- What
 - Yosemite Download from MAS (and the proper licenses)
- Whom
 - Cache

Drag Yo.app to Casper Admin
Policy to Cache

Smart group to find computers that have cache (tricky) Policy to make available in Self Service

Resources

- <https://github.com/stonyrivertech/SRT-Public/tree/master/JAMF>
- Script Parameters: <https://jamfnation.jamfsoftware.com/article.html?id=146>

Startup and Login examples

Images

- Thorton (Back to School): movieclips.com
- President Business: hitfix.com forum comment
- Software Update: Apple, Inc.
- He-Man: <http://mugen.wikia.com/wiki/He-Man>
- Coffee: <http://stores.ebay.com/shirtfactory/>
- Care Bears: [ESPN FF Team Icon](#)

Startup and Login examples



JAMF
software

Thank you!