



jamf

|

NATION

User Conference

OCTOBER 24-26

2017



Scott Blake

Endpoint Management Specialist
West Virginia University
[@mscottblake](https://twitter.com/mscottblake)





You've Deployed Your Fleet... Now What?

Presentation agenda:

Desired state management

Increase your efficiency

Give users more freedom





West VI





WVU Facts

**R1: Doctoral Universities - Highest Research
Activity**

Public, land-grant institution, founded in 1867

518 buildings on 15,880 acres

31,287 students





WVU Facts - Morgantown

245 buildings on 1,892 acres

28,488 students

14 colleges and schools

~12 different IT Units





Why does any of that matter?

Efficiency





John Kitzmiller
@JohnKitzmiller

[Follow](#)

"One thing I'm not going to do is tell folks they're using the wrong tool. Unless it's SCCM for Macs. That's the wrong tool." -

[@rtrouton](#)





What is Desired State Management?

Management tool needs to be smart enough
to automatically correct deviations.

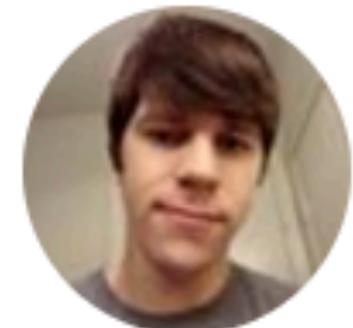




Desired State Management

Allows me the confidence to manage devices
that I know nothing about.





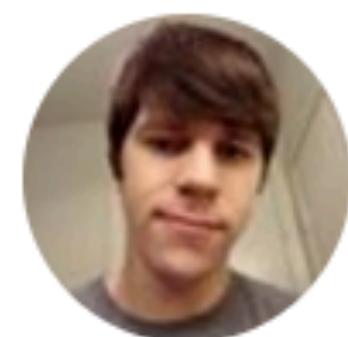
Matthew Turland

@elazar

[Follow](#)

**Q: What's the most common language used
in programming? A: Profanity.**





Matthew Turland

@elazar

[Follow](#)

Q: What's the most common language used in programming? A: Profanity.



Greg Neagle

@gregneagle

[Follow](#)

If you are not comfortable at the command line, your career as an OS X systems administrator will be nasty, brutish, and short.





Desired State Management

Anti-Virus -- What's the goal?

Installed on all devices

Running certain version

Protection is turned on





Desired State Management

Extension Attributes to the rescue!





Kaspersky Patches Applied

Display Name

Display name for the extension attribute

Kaspersky Patches Applied

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 the JSS

Extension Attributes



Input Type

Input type to use to populate the extension attribute

Script





Script

Script to use to collect data on Mac computers

```
1 #!/usr/bin/python
2
3 import xml.etree.ElementTree as ET
4 import os.path
5
6 configPath = "/Library/Application Support/Kaspersky Lab/KAV/Binaries/config.xml"
7
8 if os.path.isfile(configPath):
9     tree = ET.parse(configPath)
10    root = tree.getroot()
11
12    patches = root.findtext("./key[@name='Data']/tSTRING[@name='ProductHotfix']").split('.')
13    patches = ', '.join(sorted(patches))
14
15    print ''.join(["<result>", patches, "</result>"])
16 else:
17    print "<result>Config File Missing</result>"
```





Kaspersky Endpoint Security Protection

Display Name

Display name for the extension attribute

Kaspersky Endpoint Security Protection

Description

Description for the extension attribute

Reports whether protection is 'running', 'malfunctioning', etc.

Data Type

Type of data being collected

String



Inventory Display

Category in which to display the extension attribute in the JSS

Extension Attributes



Input Type

Input type to use to populate the extension attribute

Script





Script

Script to use to collect data on Mac computers

```
1#!/bin/bash
2
3RESULT=$(timeout 2 /usr/local/bin/kav status Protection | awk '/Protection/ {print $2}')
4
5if [ "${RESULT}" = "" ]; then
6    echo "<result>$(timeout 2 /usr/local/bin/kav status)</result>"
7else
8    echo "<result>${RESULT}</result>"
9fi
```





Extension Attribute Sessions

Build Extension Attributes

Wednesday, October 25 @ 4:00 PM

Dan Snelson and Timothy Noffke

Extension Attributes

Thursday, October 26 @ 10:15 AM

Timothy Noffke and Eric Johnson





Desired State Management

Force compliance.





Smart Computer Groups



New

Name

Anti-Virus – Not Installed

Anti-Virus – Not Running

Anti-Virus – Wrong Version





Anti-Virus - Not Installed

And/Or	Criteria	Operator	Value
	Operating System Version	greater than or equal	10.7
and	Application Title	is not	Anti-Virus For Mac.app





Anti-Virus - Not Running

And/Or	Criteria	Operator	Value
	Kaspersky Endpoint Security Protection	is not	running
and	Kaspersky Endpoint Security Protection	is not	
and	Last Check-in	less than x days ago	31





Anti-Virus - Wrong Version

And/Or	Criteria	Operator	Value
	Operating System Version	greater than or equal	10.7
and	Application Title	is	Anti-Virus For Mac.app
and	Kaspersky Patches Applied	not like	d





Anti-Virus Policies

Name	Frequency	Trigger	Scope
- Anti Virus			
- - Install Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup, Check-in	Anti-Virus – Not Installed
Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
Update Inventory			
- - Restart Kaspersky Endpoint Security	Once every day	Check-in	Anti-Virus – Not Running
Run Script restartKasperskyEndpointSecurity.sh			
Update Inventory			
- - Upgrade Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup	Anti-Virus – Wrong Version
Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
Update Inventory			





Anti-Virus Policies

Name	Frequency	Trigger	Scope
- Anti Virus			
- - Install Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup, Check-in	Anti-Virus - Not Installed
- Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
- Update Inventory			
- - Restart Kaspersky Endpoint Security	Once every day	Check-in	Anti-Virus - Not Running
- Run Script restartKasperskyEndpointSecurity.sh			
- Update Inventory			
- - Upgrade Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup	Anti-Virus - Wrong Version
- Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
- Update Inventory			





Anti-Virus Policies

Name	Frequency	Trigger	Scope
- Anti Virus			
- - Install Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup, Check-in	Anti-Virus – Not Installed
Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
Update Inventory			
- - Restart Kaspersky Endpoint Security	Once every day	Check-in	Anti-Virus – Not Running
Run Script restartKasperskyEndpointSecurity.sh			
Update Inventory			
- - Upgrade Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup	Anti-Virus – Wrong Version
Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
Update Inventory			





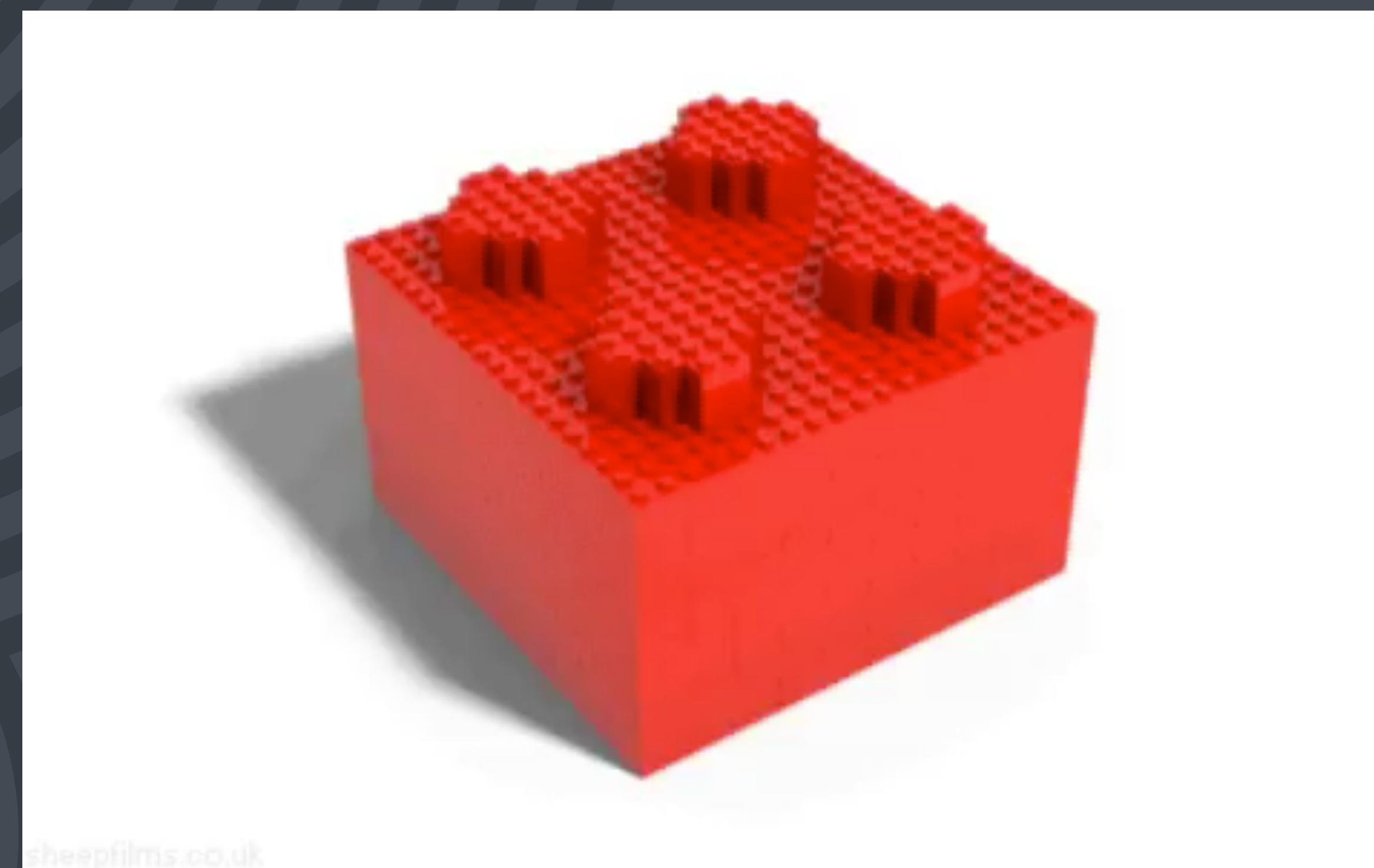
Anti-Virus Policies

Name	Frequency	Trigger	Scope
- Anti Virus			
- - Install Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup, Check-in	Anti-Virus – Not Installed
Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
Update Inventory			
- - Restart Kaspersky Endpoint Security	Once every day	Check-in	Anti-Virus – Not Running
Run Script restartKasperskyEndpointSecurity.sh			
Update Inventory			
- - Upgrade Kaspersky Endpoint Security 10.0.0.327d	Once every day	Login, Startup	Anti-Virus – Wrong Version
Install Kaspersky Endpoint Security-10.0.0.327d.pkg			
Update Inventory			





Smart Group Nesting



Shepphams.co.uk





Smart Group Nesting

AutoUpdate - Google Chrome

SS Avail - Google Chrome

Update Avail - Google Chrome





Smart Group Nesting

AutoUpdate - Google Chrome

SS Avail - Google Chrome

Update Avail - Google Chrome





Smart Group Nesting

Update Avail - Google Chrome

Computer Group	Criteria			
And/Or				
Criteria	Operator	Value		
Application Title	is	Google Chrome.app		
and	Application Version	is not	61.0.3163.100	





Smart Group Nesting

Update Avail – Google Chrome

Computer Group	Criteria								
	<table border="1"><thead><tr><th>And/Or</th><th>Criteria</th><th>Operator</th><th>Value</th></tr></thead><tbody><tr><td>▼</td><td>Patch Reporting: Google Chrome</td><td>less than</td><td>61.0.3163.100</td></tr></tbody></table>	And/Or	Criteria	Operator	Value	▼	Patch Reporting: Google Chrome	less than	61.0.3163.100
And/Or	Criteria	Operator	Value						
▼	Patch Reporting: Google Chrome	less than	61.0.3163.100						





Smart Group Nesting

AutoUpdate - Google Chrome

SS Avail - Google Chrome

Update Avail - Google Chrome





Smart Group Nesting

SS Avail - Google Chrome

Computer Group	Criteria					
And/Or	Criteria	Operator	Value			
<input type="button" value="▼"/>	Application Title	is not	Google Chrome.app	<input type="button" value="▼"/>		
or	<input type="button" value="▼"/>	<input type="button" value="▼"/>	Computer Group	member of	Update Avail - Google	<input type="button" value="▼"/>





Smart Group Nesting

AutoUpdate - Google Chrome

SS Avail - Google Chrome

Update Avail - Google Chrome





Smart Group Nesting

AutoUpdate – Google Chrome

Computer Group	Criteria			
And/Or	Criteria	Operator	Value	
	Computer Group	member of	Update Avail - Google	
and	Jamf Preferences – AutoUpdateSoftware	is	Enabled	





Smart Group Nesting





Change Smart Group Membership

No API needed.





Change Smart Group Membership

AutoUpdate – Google Chrome

Computer Group	Criteria			
And/Or	Criteria	Operator	Value	
	Computer Group	member of	Update Avail - Google	
and	Jamf Preferences – AutoUpdateSoftware	is	Enabled	





Change Smart Group Membership

Script

Script to use to collect data on Mac computers

```
1 #!/bin/bash
2
3 result=$(defaults read /path/to/custom.plist AutoUpdateSoftware)
4
5 if [ $result -eq 0 ]; then
6     echo "<result>Disabled</result>"
7 else
8     echo "<result>Enabled</result>"
9 fi
```





Change Smart Group Membership

config_jamf_preferences.sh

General

Script

Options

Limitations

Script Contents

```
1#!/bin/bash
2
3 defaults write /path/to/custom.plist $4 -$5 $6
```





Change Smart Group Membership

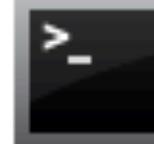
```
#!/bin/bash
```

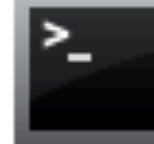
```
defaults write /path/to/custom.plist $4 -$5 $6
```





Change Smart Group Membership

AutoUpdate: Disable	Ongoing	Self Service	All computers
 Run Script config_jamf_preferences.sh			
 Update Inventory			

AutoUpdate: Enable	Ongoing	Self Service	All computers
 Run Script config_jamf_preferences.sh			
 Update Inventory			





Change Smart Group Membership

Parameter Values

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

Setting Name

AutoUpdateSoftware

Type

bool

Value

False

Parameter 7





Change Smart Group Membership

Allow technicians to designate a classroom

Empower users

Presentation mode

Overnight Maintenance

Power Management





Change Smart Group Membership



Questions?





<https://github.com/MScottBlake/Presentations>



Thank you!

