FORESCOUT®

Forescout JAMF Integration

05.23.19 - v1.0

Nick Duda
nduda78@gmail.com
Twitter: @nduda78
LinkedIn: https://www.linkedin.com/in/nickduda/

Summary

Using the Forescout Open Integrations Module (OIM), this document will walk you through integrating Forescout with JAMF (Apple macintosh / MDM management platform). With this integration you will gain the following:

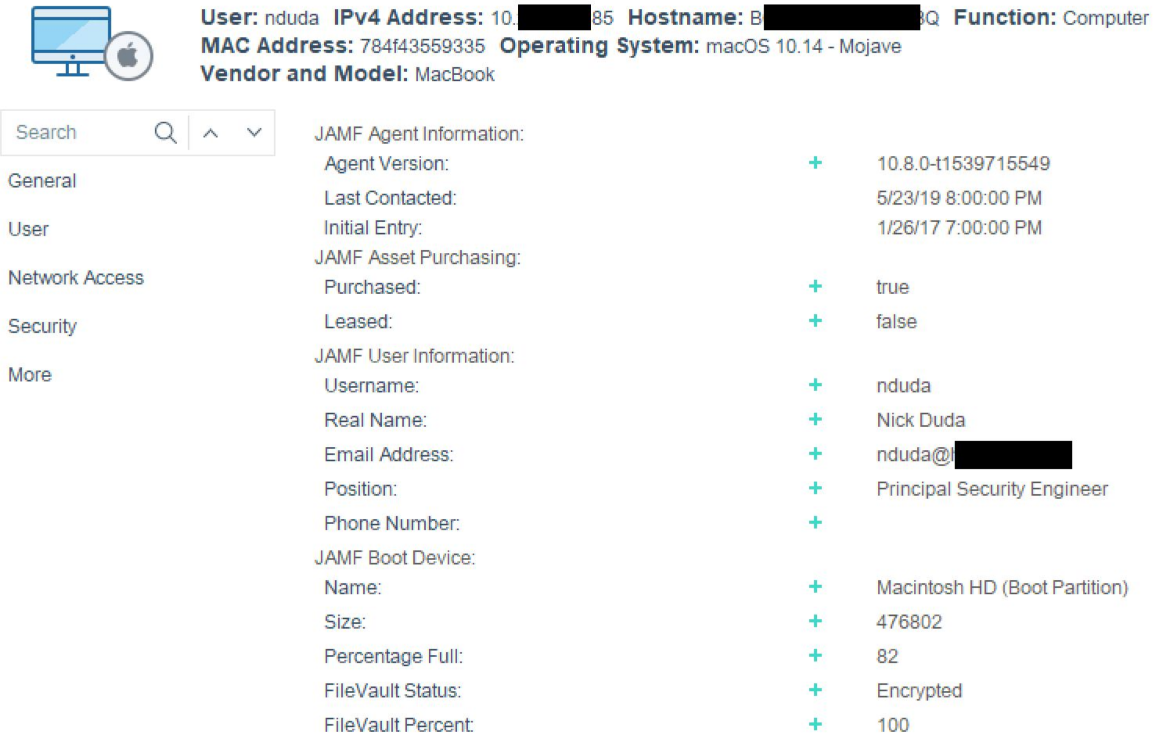
1. JAMF Managed Device
    a. Is the device managed by JAMF, True or False.
2. JAMF Device Name
3. JAMF Device ID
4. JAMF Asset Purchasing
    a. Leased or Owned
5. JAMF User Information
    a. Logged in User
    b. Username
    c. Full Name
    d. Email Address
    e. Position
    f. Phone Number
6. JAMF Device Details
    a. Make
    b. Model
    c. Operating System Name, Version, Build
    d. Processor Type, Architecture, Speed, Total Processors, Total Cores
    e. Memory
    f. Serial Number
    g. Battery Capacity
7. JAMF Partitions (BOOT)
    a. Name
    b. Size

    c. Percentage Used
    d. FileVault status, FileVault percent

8. JAMF Software Installed
9. JAMF Agent Information

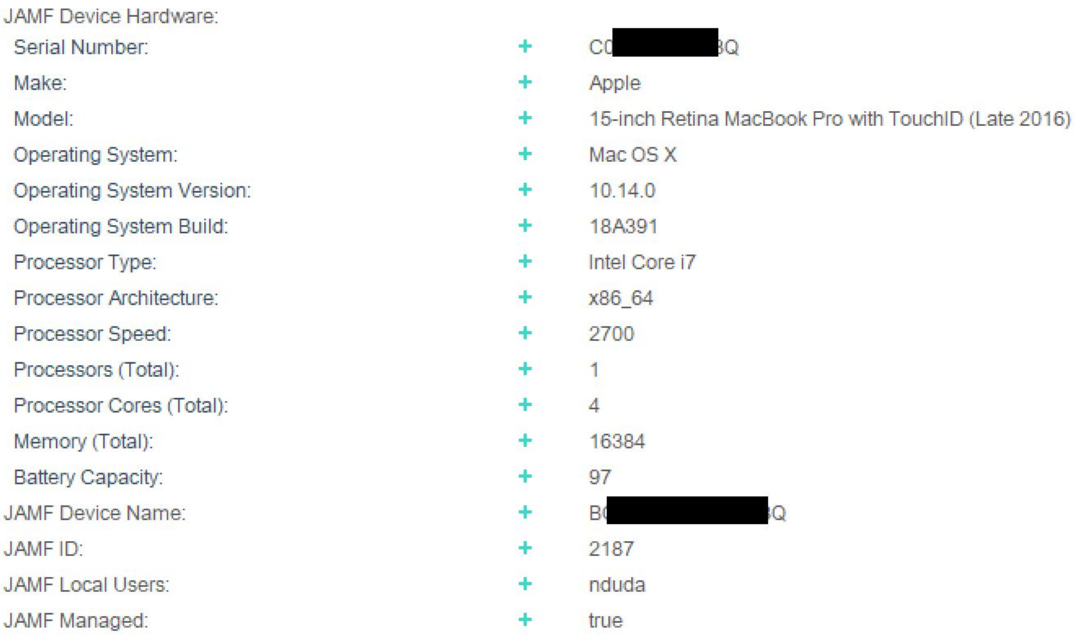
    a. Version
    b. Reported Date, Last Connected Date, Initial Entry Date

With the data from these integrations you will gain deeper visibility into Macintosh devices connected to the network. This information can be used in policies (conditions) as well as {tags}. This integration is recommended to improve your Macintosh manageability policy.

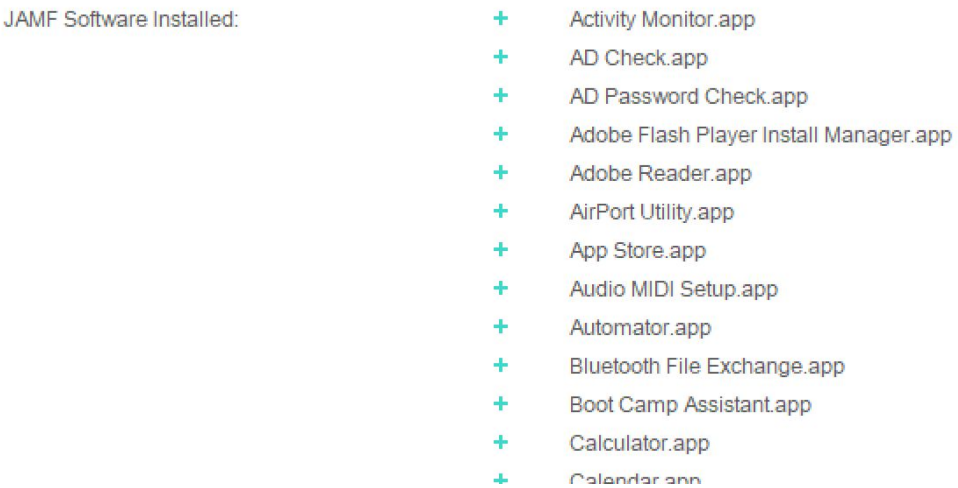


User: nduda **IPv4 Address:** 10.[redacted]85 **Hostname:** B[redacted]Q **Function:** Computer
MAC Address: 784f43559335 **Operating System:** macOS 10.14 - Mojave
Vendor and Model: MacBook

JAMF Agent Information:		
Agent Version:	+	10.8.0-t1539715549
Last Contacted:		5/23/19 8:00:00 PM
Initial Entry:		1/26/17 7:00:00 PM
JAMF Asset Purchasing:		
Purchased:	+	true
Leased:	+	false
JAMF User Information:		
Username:	+	nduda
Real Name:	+	Nick Duda
Email Address:	+	nduda@[redacted]
Position:	+	Principal Security Engineer
Phone Number:	+	
JAMF Boot Device:		
Name:	+	Macintosh HD (Boot Partition)
Size:	+	476802
Percentage Full:	+	82
FileVault Status:	+	Encrypted
FileVault Percent:	+	100



JAMF Device Hardware:		
Serial Number:	+	C[redacted]Q
Make:	+	Apple
Model:	+	15-inch Retina MacBook Pro with TouchID (Late 2016)
Operating System:	+	Mac OS X
Operating System Version:	+	10.14.0
Operating System Build:	+	18A391
Processor Type:	+	Intel Core i7
Processor Architecture:	+	x86_64
Processor Speed:	+	2700
Processors (Total):	+	1
Processor Cores (Total):	+	4
Memory (Total):	+	16384
Battery Capacity:	+	97
JAMF Device Name:	+	B[redacted]Q
JAMF ID:	+	2187
JAMF Local Users:	+	nduda
JAMF Managed:	+	true



JAMF Software Installed:

+ Activity Monitor.app
+ AD Check.app
+ AD Password Check.app
+ Adobe Flash Player Install Manager.app
+ Adobe Reader.app
+ AirPort Utility.app
+ App Store.app
+ Audio MIDI Setup.app
+ Automator.app
+ Bluetooth File Exchange.app
+ Boot Camp Assistant.app
+ Calculator.app
+ Calendar.app

Example of the Profile Tab with JAMF data

Requirements

Forescout Requirements

1. Forescout CounterACT v7.x/8.x
2. Open Integrations Module (OIM - Extended Module)

JAMF Requirements

1. User account with read permissions to the REST API

Configuration

Build (two) Web Service Request

The reason for two is that some of the properties rely on JSON parsing while the others use XML parsing. As of this writing there is a bug with the JAMP JSON response in that if there are multiple disk partitions only the first one can be parse, however the same call using XML will return all partitions. Once resolve by JAMF there will only be the need for one Web Service Request.

JSON Request

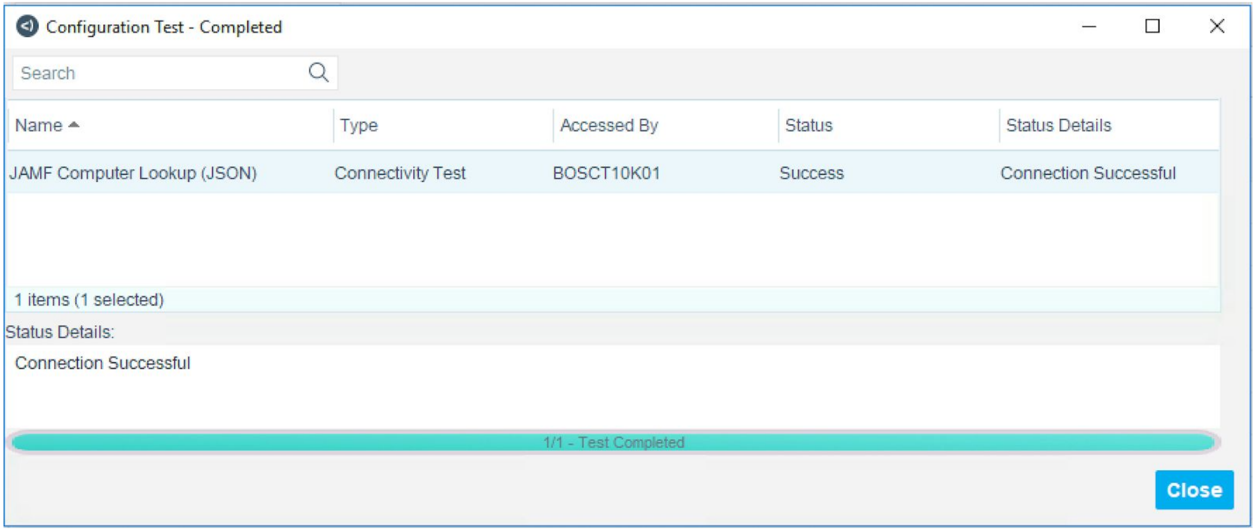
1. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request

2. Add new request
3. General Tab
    a. Request Name: JAMF Computer Lookup (JSON)
    b. Description: This query will lookup the device in JAMF
    c. HTTP Method: Get
    d. URL: https://<jamf url>/JSSResource/computers/macaddress/**{eds_mac_fmt_colon}**
    e. HTTP Message Headers: *Accept: application/json*
4. Authentication Tab
    a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
5. CounterACT Devices Tab
    a. Use Connecting CountetACT Device - Specific a CounterACT appliance that should make these queries.

XML Request

6. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
7. Add new request
8. General Tab
    a. Request Name: JAMF Computer Lookup (XML)
    b. Description: This query will lookup the device in JAMF
    c. HTTP Method: Get
    d. URL: https://<jamf url>/JSSResource/computers/macaddress/**{eds_mac_fmt_colon}**
    e. HTTP Message Headers: *Accept: application/xml*
9. Authentication Tab
    a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
10. CounterACT Devices Tab
    a. Use Connecting CountetACT Device - Specific a CounterACT appliance that should make these queries.

Click OK. After Applying, test the web service calls. Supply the MAC Address colon delimited (i.e. xx:xx:xx:xx:xx:xx) of a device enrolled in JAMF. The query will result a status of Success if the device was found.



Configuration Test - Completed

Search

Name ▲	Type	Accessed By	Status	Status Details
JAMF Computer Lookup (JSON)	Connectivity Test	BOSCT10K01	Success	Connection Successful

1 items (1 selected)

Status Details:

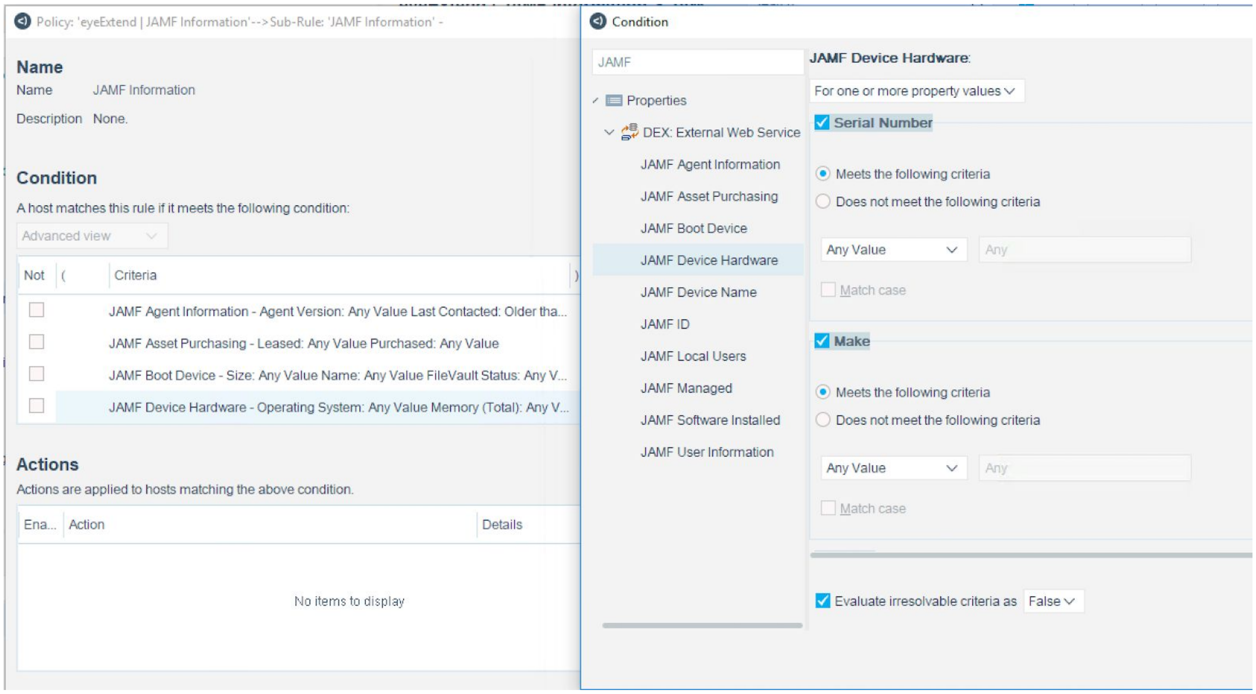
Connection Successful

1/1 - Test Completed

Import JAMF Properties XML

Keeping it simple, just import the follow property XML files. This can be located in the Forescout Community GitHub Repo: https://github.com/fsctcommunity/OIM/tree/master/JAMF%20Integration

That's it! All of these properties can now be used as conditions in policies (as well as {tags}



Policy: 'eyeExtend | JAMF Information'-->Sub-Rule: 'JAMF Information' -

Name

Name JAMF Information

Description None.

Condition

A host matches this rule if it meets the following condition:

Advanced view

Not	(	Criteria
□		JAMF Agent Information - Agent Version: Any Value Last Contacted: Older tha...
□		JAMF Asset Purchasing - Leased: Any Value Purchased: Any Value
□		JAMF Boot Device - Size: Any Value Name: Any Value FileVault Status: Any V...
□		JAMF Device Hardware - Operating System: Any Value Memory (Total): Any V...

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details

No items to display

Condition

JAMF

JAMF Device Hardware:

For one or more property values

☑ Serial Number

● Meets the following criteria
○ Does not meet the following criteria

Any Value | Any

□ Match case

☑ Make

● Meets the following criteria
○ Does not meet the following criteria

Any Value | Any

□ Match case

☑ Evaluate irresolvable criteria as False