FORESCOUT®

Forescout JAMF Integration

12.03.19 - v2.1

—

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

Change Log

12.03.19 - v2.1

- Added steps on how to resolve Error: Received HTTP response reached max content size limit (see Frequently Asked Questions)
- Noted to update port to webservices URL if not using standard TCP/443

08.21.19 - v2.0

- Updated integration to use the JAMF Device Name and Serial Number endpoints in addition to MAC Address.
- Provided an example of how to extract Macintosh Serial Number via script

05.23.19 - v1.0

- Initial Release

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]3Q **Function:** Computer
MAC Address: 784f43559335 **Operating System:** macOS 10.14 - Mojave
Vendor and Model: MacBook

Search

General

User

Network Access

Security

More

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:

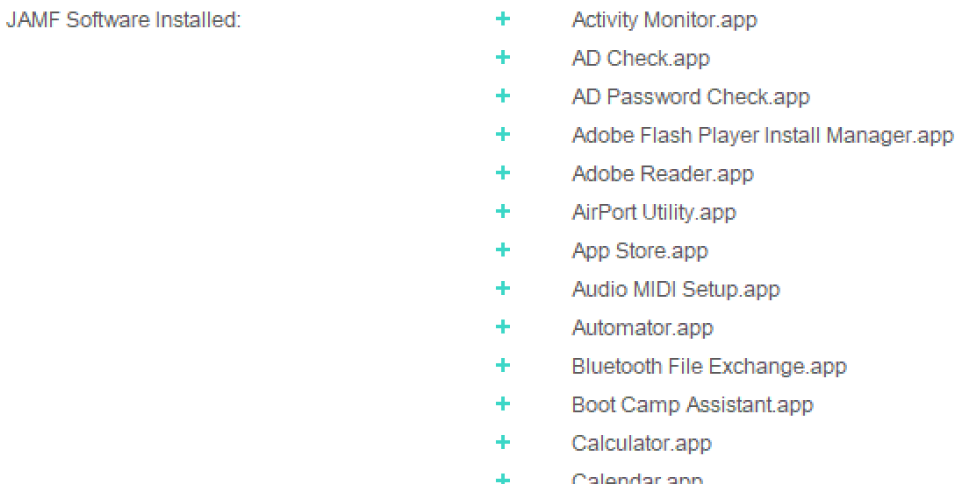
Username:	+	nduda
Real Name:	+	Nick Duda
Email Address:	+	nduda@[redacted]
Position:	+	Principal Security Engineer
Phone Number:	+	

JAMF Boot Device:

Name:	+	Macintosh HD (Boot Partition)
Size:	+	476802
Percentage Full:	+	82
FileVault Status:	+	Encrypted
FileVault Percent:	+	100

JAMF Device Hardware:

Serial Number:	+	C0[redacted]3Q
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]4Q
JAMF ID:	+	2187
JAMF Local Users:	+	nduda
JAMF Managed:	+	true



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 Web Service Request

We need to build two web service requests. 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 JAMF 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 resolved by JAMF there will only be the need for one Web Service Request.

You can query JAMF for assets using numerous endpoints. This whitepaper will cover three of them:

1. **MAC Address** (colon separated).
    a. Summary: This method is the easiest way and most passive from a Forescout perspective. There is however a pretty substantial con to this approach
        i. Pros: The MAC Address is easily learned from Forescout without having to integrate with other solutions.
        ii. Cons: JAMF only records two MAC addresses for an asset. JAMF categorizes them as a primary and secondary MAC address. JAMF considers the 1st network adapter on the Macintosh as the Primary followed by the 2nd network adapter as the Secondary. The problem observed here is that typically the 1st adapter on a Macintosh is the Wireless Adapter. The 2nd is usually the Bluetooth Adapter. Therefore, querying JAMF with the MAC Address of any other adapter will not present any results (e.g. Wired, USB...etc). If your environment is mixed with a lot of movement between Wireless and Wired then this option is not optimal.
2. **Device Name. (Prefered Method)**
    a. Summary: This method, I find, provides the most optimal results for all Macinoths devices (regardless of which network adapter they are connected with). With this method you pass the device name to JAMF.
        i. Pros: As long as the device name in Forescout exists/matches the one in JAMF then you will get results.
        ii. Cons: Obtaining the device name of a device on the Forescout side depends on the method that works best for you. The best results will be in using ***{dhcp_hostname}***, however this requires that Forescout is digesting DHCP information via helpers or SPAN sessions and that the DHCP Classification plugin is operational. Another way to pass the device name is via ***{macintosh_hostname}***, however this method requires the Macintosh device is managed by Forescout as that condition is only obtained from managed systems. You can substitute any {tag} as long as the tag provides the device name of the Macintosh.
3. **Serial Number.**
    a. Summary: This method is more complex but a viable option. It will provide the exact same level of results as passing the Device Name.
        i. Pros: As long as the serial number of the device in Forescout exists/matches the one in JAMF then you will get results.
        ii. Cons: In order to obtain the serial number of the Macintosh it typically needs to be managed. Once managed you can execute a script on the Macintosh to extract the serial number and then pass that {tag} to JAMF. This option was a good option for me (at my current employer

at the time of this writing) since the hostname of the Macintosh systems we deployed was also the serial number. We used {dhcp_hostname}, which was the serial number, and passed that to this endpoint.

Option 1 - Using MAC Address

JSON Request

- Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
- Add new request
- General Tab
    a. Request Name: JAMF Computer Lookup by MAC Address (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}**

    Note: if using a non-standard port other than TCP/443 make sure you update it in the URL

    e. HTTP Message Headers: *Accept: application/json*
- Authentication Tab
    a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
- CounterACT Devices Tab
    a. Use Connecting CountetACT Device - Specific a CounterACT appliance that should make these queries.

XML Request

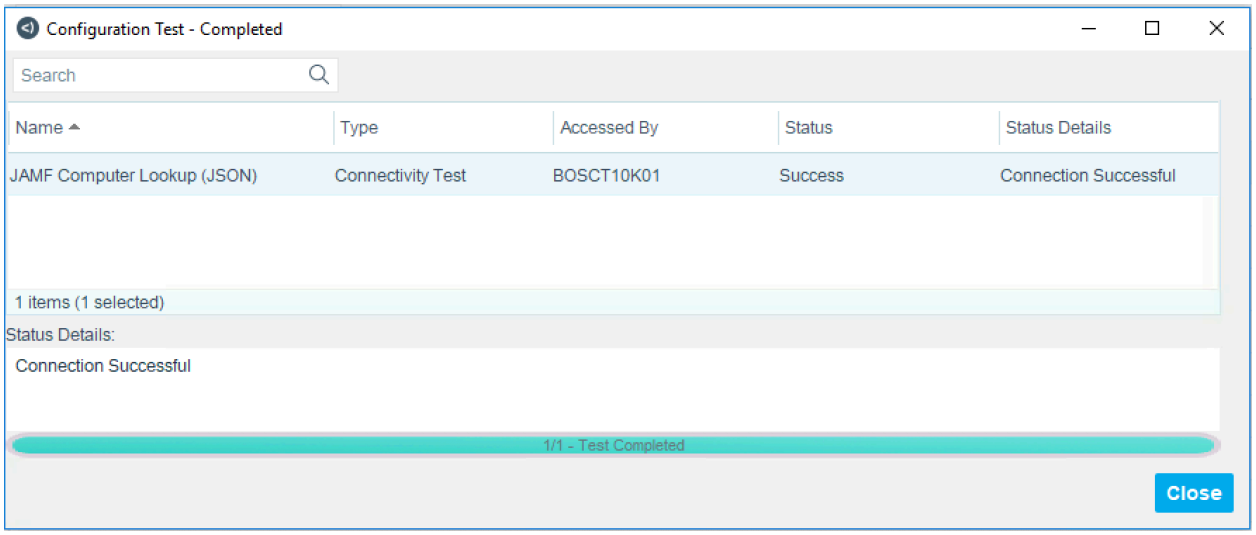
- Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
- Add new request
- General Tab
    a. Request Name: JAMF Computer Lookup by MAC Address (XML)
    b. Description: This query will lookup the device in JAMF
    c. HTTP Method: Get
    d. URL: https://<jamf url>/JSSResource/computers/macaddress/**{eds_mac_fmt_colon}**

Note: if using a non-standard port other than TCP/443 make sure you update it in the URL

e. HTTP Message Headers: *Accept: application/xml*

- Authentication Tab
  a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
- CounterACT Devices Tab
  a. Use Connecting CounterACT 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.



Option 2 - Using Device Name

In the examples below, I'm passing {dhcp_hostname} to the JAMP endpoint. You can substitute this with any {tag} that provides the device name (e.g. {macintosh_hostname}

JSON Request

- Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
- Add new request
- General Tab
  a. Request Name: JAMF Computer Lookup by Device Name (JSON)
  b. Description: This query will lookup the device in JAMF
  c. HTTP Method: Get

    d. URL: https://<jamf url>/JSSResource/computers/name/**{dhcp_hostname}**

       Note: if using a non-standard port other than TCP/443 make sure you update it in the URL

    e. HTTP Message Headers: *Accept: application/json*
- Authentication Tab
    a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
- CounterACT Devices Tab
    a. Use Connecting CountetACT Device - Specific a CounterACT appliance that should make these queries.

XML Request

- Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
- Add new request
- General Tab
    a. Request Name: JAMF Computer Lookup by Device Name (XML)
    b. Description: This query will lookup the device in JAMF
    c. HTTP Method: Get
    d. URL: https://<jamf url>/JSSResource/computers/name/**{dhcp_hostname}**

       Note: if using a non-standard port other than TCP/443 make sure you update it in the URL

    e. HTTP Message Headers: *Accept: application/xml*

- Authentication Tab
    a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
- CounterACT Devices Tab
    a. Use Connecting CounterACT Device - Specific a CounterACT appliance that should make these queries.

<u>Option 3 - Using Serial Number</u>

In the examples below, I'm passing {dhcp_hostname} to the JAMP endpoint. You can substitute this with any {tag} that provides the serial number (e.g. You can run a script on Macintosh to extract the serial number and use the {tag} from those results). See the next section for examples on how to pull serial number via script.

JSON Request

- Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
- Add new request
- General Tab
    a. Request Name: JAMF Computer Lookup by Serial Number (JSON)
    b. Description: This query will lookup the device in JAMF
    c. HTTP Method: Get
    d. URL: https://<jamf url>/JSSResource/computers/serialnumber/**{dhcp_hostname}**

    Note: if using a non-standard port other than TCP/443 make sure you update it in the URL

    e. HTTP Message Headers: *Accept: application/json*
- Authentication Tab
    a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
- CounterACT Devices Tab
    a. Use Connecting CountetACT Device - Specific a CounterACT appliance that should make these queries.

XML Request

- Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
- Add new request
- General Tab
    a. Request Name: JAMF Computer Lookup by Serial Number (XML)
    b. Description: This query will lookup the device in JAMF
    c. HTTP Method: Get
    d. URL: https://<jamf url>/JSSResource/computers/serialnumber/**{dhcp_hostname}**

    Note: if using a non-standard port other than TCP/443 make sure you update it in the URL

    e. HTTP Message Headers: *Accept: application/xml*

- Authentication Tab
    a. Use Basic Authentication Header - Provide username and password created for accessing the JAMF API
- CounterACT Devices Tab
    a. Use Connecting CounterACT Device - Specific a CounterACT appliance that should make these queries.

Obtaining Macintosh Serial Number via script

- Create a new Forescout policy and scope it to Managed Macintosh systems.
- Using *Macintosh Expected Script Result* run the following command on the Macintosh
    - system_profiler SPHardwareDataType | awk '/Seria/ {print $4}'

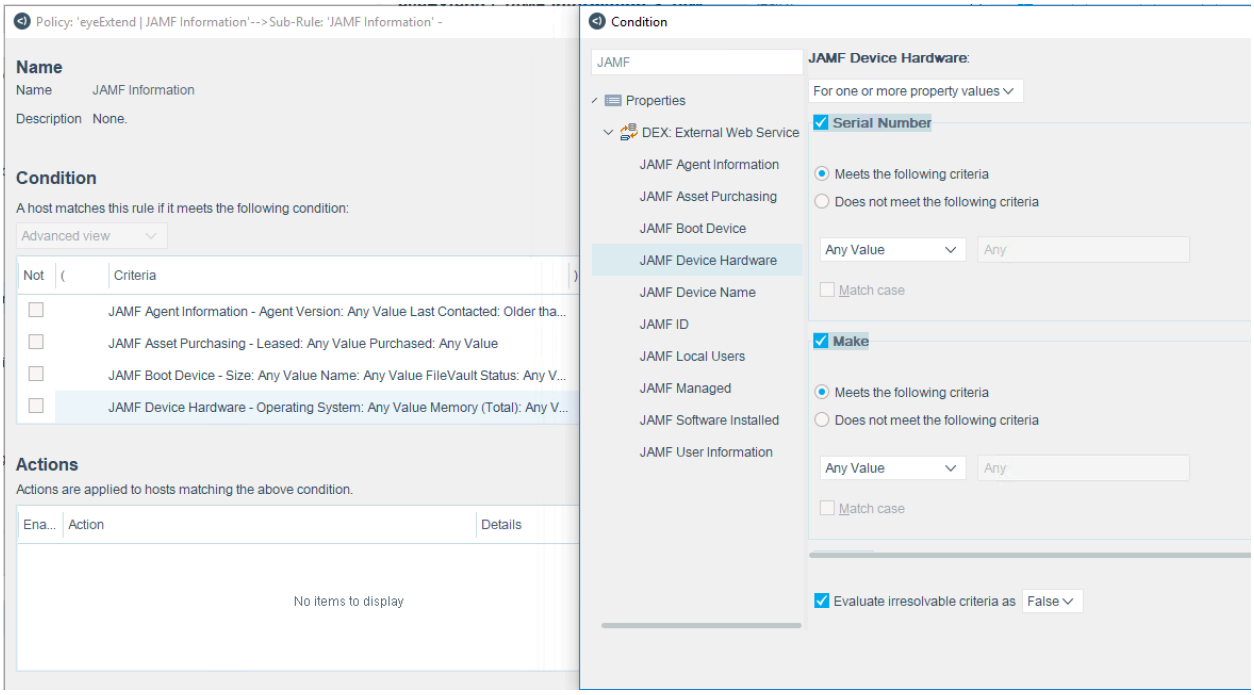
```
[E            J:~          $ system_profiler SPHardwareDataType | awk '/Seria/ {print $4}'
C02YW1J8LVCJ
```

- Based on the policy I wrote for this, the tag I would use to pass the serial number would be: {mac_script_result.9351e58d6ba9c407db4fe8afcc824032}
    - Note, this is not the tag you want to use. Yours will be different.

Import JAMF Properties XML

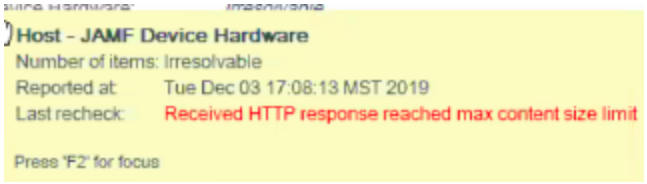
Keeping it simple, just import the following property XML files. This can be located in the Forescout Community GitHub Repo: https://github.com/fsctcommunity/OIM/tree/master/JAMF%20Integration

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



Frequently Asked Questions

I'm getting the following error on some of the JAMF Properties, Received HTTP response reached max content size limit



DEX has a hardcoded limit on how big (bytes) the response of a web service request can be. Some of the JAMF properties, such as Software Installed exceeds this hardcoded limit. You can up this size by editing */usr/local/forescout/plugin/eds/install.properties* and changing the extweb.http.response.content.max value to something higher

```
# Max size of HTTP response content for External Web Service, 100KB
extweb.http.response.content.max = 102400
```

Warning: Editing properties files should be done with caution. Always take a backup of any file you modify.

After importing the Web Service Properties, they didn't map to the Web Service Requests. What gives?

For some of the integrations, they use a unique internal identifier that is different between Forescout environments. You just need to map them manually after importing.

Awesome integration! How can I contribute back?

First off, if you implemented this integration I want to know about it! Shoot me an email with your feedback. Second, I go through a lot of coffee while building these, so feel free to buy me a cup! paypal.me/NickDuda

Can you help me build an integration for <insert technology here>?

Absolutely! Hit me up at nduda78@gmail.com and let's chat.

Where can I go to learn more about all things Forescout?

- Forescout Slack User Community. - I'm a little biased on this one since I created it. This is probably the best place to go if you want realtime chat with Forescout experts (Customers, Partners and even Forescout Employees).
- Official Forescout Forum. - You'll need to be a customer to access it though. There is a good amount of activity going on there and the support team chimes in. This is, of course, the official Forescout method for asking questisons.

- Forescout on Reddit. - Not as active as the Slack Community or Forescout Forum but it's a place to get the attention of some experts.