

# CA Enterprise Management – Deployment Guide

*CA UIM with NFA for Managed Service Providers  
(MSPs)*



## Table of Contents

<b>Executive Summary .....</b>	<b>3</b>
<b>Sample Environment.....</b>	<b>3</b>
<b>Tested Versions.....</b>	<b>4</b>
<b>NFA Sizing: .....</b>	<b>4</b>
<b>Alerting: .....</b>	<b>4</b>
<b>Caveats: .....</b>	<b>5</b>
Overlapping Router IPs .....	5
Custom NFA Interface QOS Enrichment: .....	5
<b>Deployment Process:.....</b>	<b>5</b>
<b>Discovery Steps (ForwardInc MSP): .....</b>	<b>6</b>
Step 1. Deploy discovery_agent to Nordole and VoonAir’s on premise hub. ....	6
Step 2. Configure and Execute a Discovery for both Nordole and VoonAir.....	6
<b>NFA Steps (ForwardInc MSP):.....</b>	<b>7</b>
Step 1. Download NQ_Services 1.20 and NFA_Inventory 1.30 from the Web Archive. ....	7
Step 2. Deploy nq_services probe to the primary hub where trellis is located.....	8
Step 3. Deploy and configure nfa_inventory probe to the NFA Master Console.....	9
<b>SNMPCollector (Customer Nordole):.....</b>	<b>11</b>
Step 1. Configure SNMPCollector .....	11
Step 2. Validate SNMPCollector Data.....	12
<b>QOS Enrichment Steps (ForwardInc MSP): .....</b>	<b>12</b>
Step 1. Create Ruby Script and Enable qos_processor .....	12
Step 2. Validate Origin Enrichment.....	14
Step 3. Validate Origin to NFA Interface Group Mapping.....	14
<b>Create Customer Access (ForwardInc MSP): .....</b>	<b>15</b>
Step 1. Create UIM Accounts for each customer.....	15
Step 2. Provision UIM Customer Account Users to NFA Master Console .....	17
Step 3. Validate UIM to NFA workflow for Customers.....	18
<b>Troubleshooting .....</b>	<b>21</b>
NFA Origin to Interface Group Mapping failing .....	21
Drillout from UIM to NFA Fails with “Unknown Error” .....	22

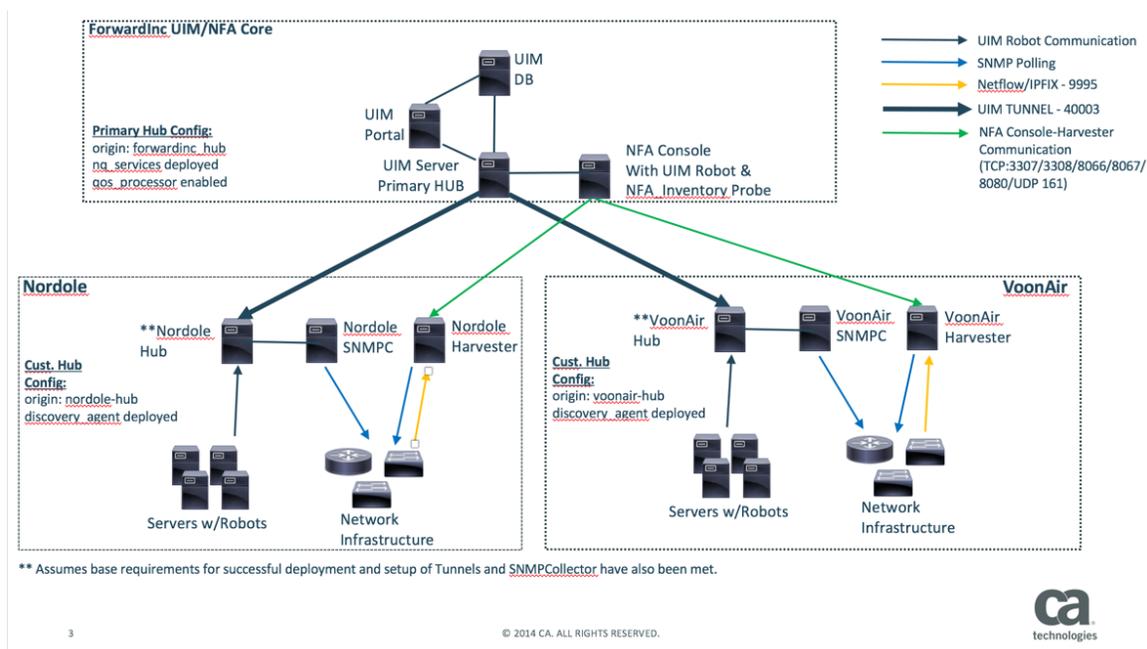
## Executive Summary

CA Network Flow Analysis (NFA) is a network traffic monitoring solution that can help you optimize your network infrastructure for better application performance. With enhanced visibility into your network's applications, hosts, conversations and QoS information, you can proactively manage your network to reduce outages, solve problems faster and ensure efficient and cost-effective operations. When NFA is combined with CA Unified Infrastructure Management (UIM) for Network, the total solution provides complete visibility into Network Health for IT infrastructure.

For MSPs to leverage this solution, a foundational element to success is tenancy. The two components of the solution (UIM/NFA) have different mechanisms for leveraging tenancy and bringing these two products together to offer a holistic multi-tenant solution is not straightforward. With that in mind, the steps below explain the process for deploying CA UIM with CA NFA to offer a complete solution in a multi-tenant configuration.

## Sample Environment

The following diagram depicts a sample architecture for deploying UIM/NFA with Multi-tenancy. The deployment consists of the core UIM/NFA infrastructure deployed at a MSP (ForwardInc), managing two customers (Nordole and VoonAir). Nordole and VoonAir are running UIM Components (Secondary Hub and SNMPCollector) and NFA Components (Harvester) on premise to monitor their network and systems infrastructure.



## Tested Versions

The following versions were used to create this deployment guide:

- Unified Infrastructure Management (UIM) 8.4
- Network Flow Analysis (NFA) 9.3.3
- NFA\_Inventory Probe 1.30
- NQ\_Services Probe 1.20
- SNMPCollector 3.11

To enabled UIM with NFA with Multi-tenancy the minimum supported versions are UIM 8.31, NFA 9.3.2, NFA Inventory Probe 1.10 and NQ\_Services Probe 1.0.

## NFA Sizing:

NFA is sold per device, and scales horizontally by adding additional harvesters to support the devices sending flow data. The rule of thumb is 1000 devices per harvester with ~24 harvesters per NFA console. However, the metric that truly drives performance and scale for NFA is flow rate. Each harvester can handle a max of ~9million flows per minute. The flow rate per harvester can be viewed from the NFA UI – Administration – Flow Statistics page. More information on NFA sizing can be found at

<https://docops.ca.com/display/NFA933/System+Recommendations+and+Requirements>.

## Alerting:

NFA has the capability to send SNMP traps when application traffic exceeds a threshold for an interface or group of interfaces. To support this capability with UIM, you must deploy and configure the snmptd probe to support NFA. The configuration will require uploading the NFA mib file stored on the NFA console at [NFA INSTALL DIRECTORY]\REPORTER\MIB to the snmptd probe.

## Caveats:

### Overlapping Router IPs:

The current GA version of NFA (9.3.3) does not support routers that have overlapping management addresses. Management addresses consist of those addresses that are known to the system. In NFA's case that would be the Export Source, in UIM's case that would be the Polled IP. So given that NFA does not support this capability, neither does the UIM/NFA integration. Again, this does not mean that the hosts/conversations i.e. traffic flows cannot have overlapping IP addressing, just that the router management IPs cannot. This capability is expected to be addressed in a future release of NFA.

### Custom NFA Interface QOS Enrichment:

NFA has interface types that are specific to NFA only. Examples of these are Broadcast/Multicast Interface, Interface Aggregations, and Custom Virtual Interfaces(CVIs). Since these interfaces are specific to only NFA and not able to be monitored via SNMPCollector, QOS enrichment cannot be completed for these interface types. Which also means that you will not see these interfaces show up under the customer views in USM. However, they will be in NFA for the devices that they are associated with.

## Deployment Process:

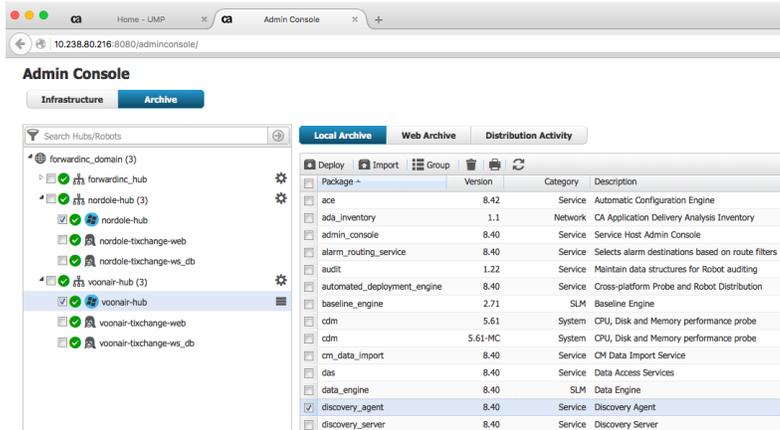
The following pre-requisites should be completed prior to following the deployment process:

- UIM 8.4 base installation has been successfully completed.
- Remote Hubs are installed and successfully communicating over a tunnel back to the primary hub.
- Remote Hubs are configured with the appropriate customer origin.
- SNMPCollector and all dependent probes are installed (but not configured) at each customer location.
- NFA two-tier install with harvesters at each customer location has been completed and Netflow data is successfully being shown in the NFA UI.

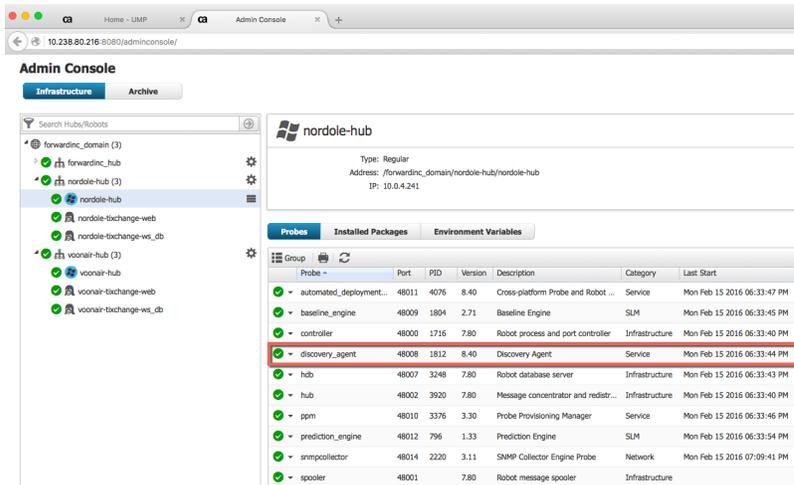
## Discovery Steps (ForwardInc MSP):

### Step 1. Deploy discovery\_agent to Nordole and VoonAir's on premise hub.

- A. Open Admin Console – Select Archive – Select Nordole-Hub & VoonAir-Hub – then select discovery\_agent package and click deploy.



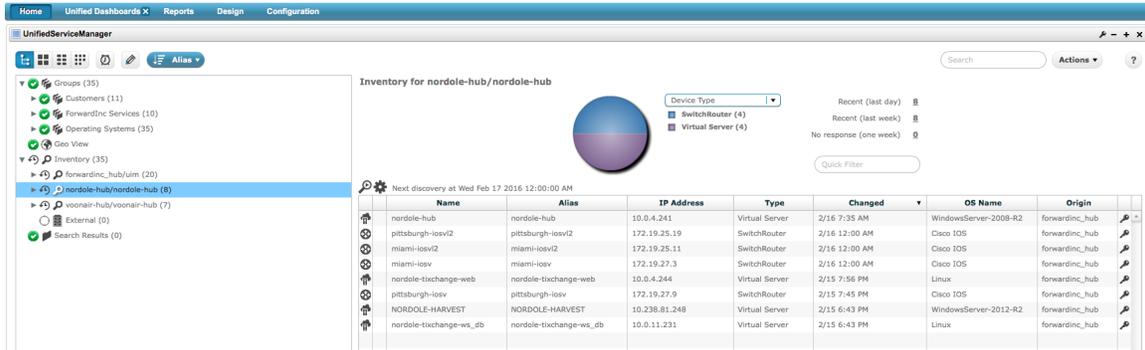
- B. Validate discovery\_agent has successfully started on both Nordole and VoonAir hubs.



### Step 2. Configure and Execute a Discovery for both Nordole and VoonAir.

- A. Login to UMP and Click on the Discovery Wizard for Nordole.  
B. (Minimally) Add SNMP Credentials and Network Range Scope for the desired network devices that will be monitored via SNMPCollector and will be sending flow data.  
C. Run the discovery now, and reschedule discovery to detect changes at the desired interval.

D. Validate devices have successfully been discovered.



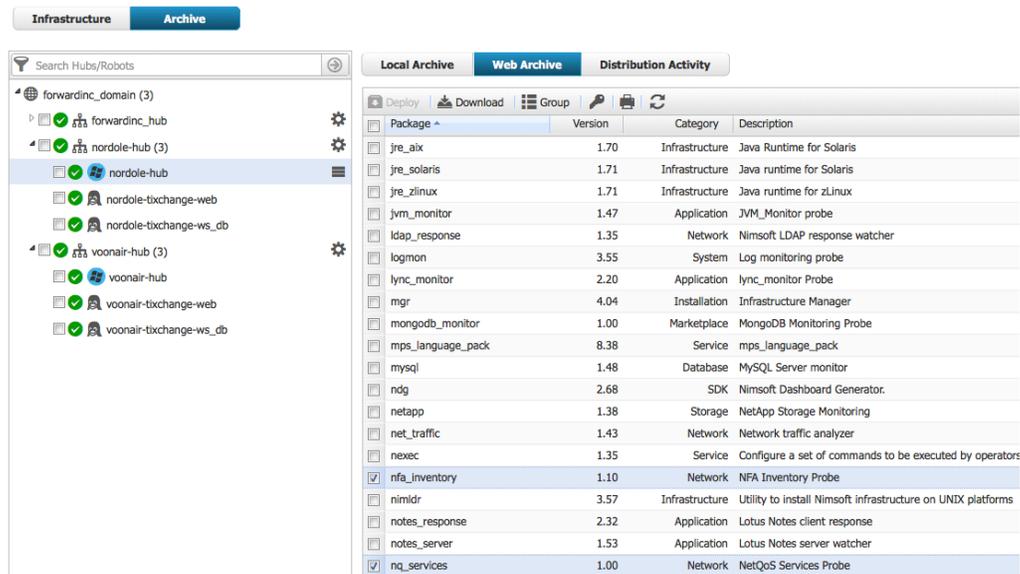
E. Execute same process for VoonAir.

**NFA Steps (ForwardInc MSP):**

**Step 1. Download NQ\_Services 1.20 and NFA\_Inventory 1.30 from the Web Archive.**

- A. Open Admin Console – Click Archive – Web Archive – Select NFA\_Inventory and NQ\_Services and Click Download

**Admin Console**



## Step 2. Deploy nq\_services probe to the primary hub where trellis is located.

- A. Open Admin Console – Select Archive – Select the primary hub – then select nq\_services package and click deploy.

**Admin Console**

Infrastructure Archive

Search Hubs/Robots

forwardinc\_domain (3)

- forwardinc\_hub (5)
  - ada
  - nfa
  - nfa-capc
  - spectrum-mk
  - uim**
- nordole-hub (3)
  - nordole-hub
  - nordole-tixchange-web
  - nordole-tixchange-ws\_db
- voonair-hub (3)
  - voonair-hub
  - voonair-tixchange-web
  - voonair-tixchange-ws\_db

Local Archive Web Archive Distribution Activity

Deploy Import Group

Package	Version	Category	Description
nfas_api_service	8.4.0	Service	NFA API Services
net_connect	3.21	Network	Monitor network connectivity (ICMP / TCP)
nfa_inventory	1.30	Network	Collects NFA inventory of routers and associated interfaces.
nisapi_wasp	8.4.0	Service	NIS Restful API (Wasp Edition)
nis_server	3.51	Infrastructure	NIS Server
<b>nq_services</b>	<b>1.2.0</b>	<b>Service</b>	<b>NetQoS Services</b>
ppm	3.30	Service	Probe Provisioning Manager
pp_defaults	2.12	Service	Probe Provisioning Default Templates
prediction_engine	1.33	SLM	Prediction Engine
qos_processor	8.4.0	SLM	QoS Processor
relationship_services	1.72	Service	Relationship Maintenance and Access Services
robot_aix	7.80	Infrastructure	Native AIX installer
robot_deb	7.80	Infrastructure	Native Ubuntu/Debian installers
robot_exe	7.80	Infrastructure	Native Windows Robot Packages
robot_hpux	7.80	Infrastructure	Native HPLUX installers
robot_rpm	7.80	Infrastructure	Native Linux RPM installers for SLES, SUSE, RHEL, and CentOS
robot_sol	7.80	Infrastructure	Native Solaris Installers

- B. Validate nq\_services probe is active. Open Admin Console – Select Infrastructure – Select the primary hub – Select Trellis Probe – Select Probe Utility – Choose List Services – Click Green Arrow – Look for NQ Origin Service and Active = True.

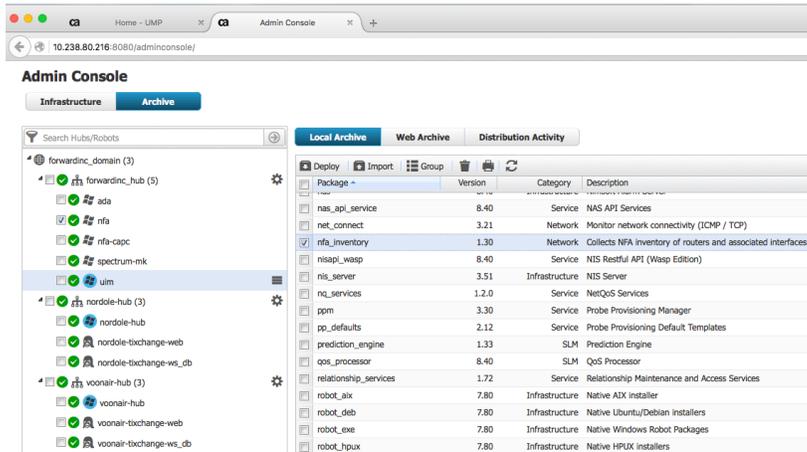
Probe Utility - /forwardinc\_domain/forwardinc\_hub/uim/trellis

list\_services

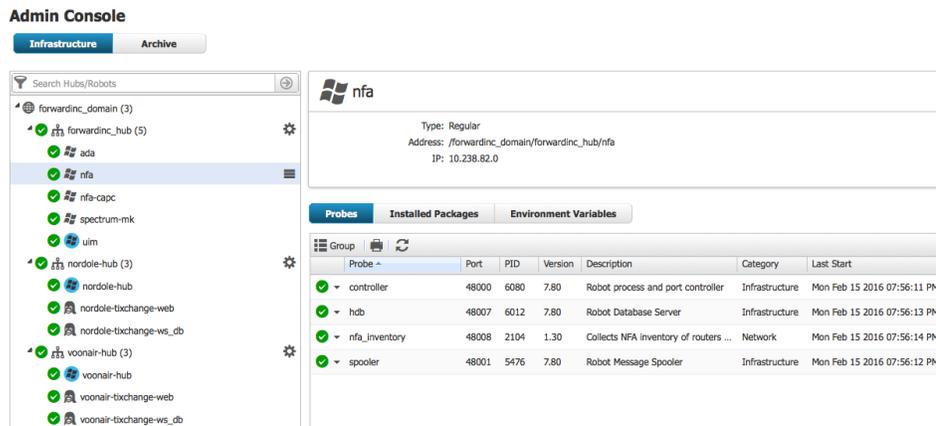
Name	Value
deployments	
0	
active	true
description	Data Access Services
key	das
name	
version	8.4.0
1	
active	true
description	NFA Origin Service
key	nq_services
name	
version	1.2.0
2	
active	true
description	Trellis Container Core Services
key	trellis
name	
version	3.0

### Step 3. Deploy and configure nfa\_inventory probe to the NFA Master Console.

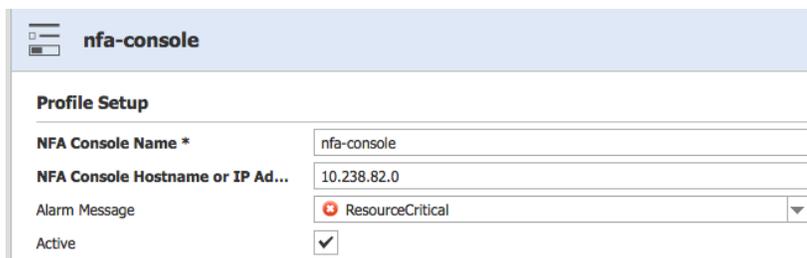
- A. Open Admin Console – Select Archive – Select the NFA Robot – then select nfa\_inventory package and click deploy.



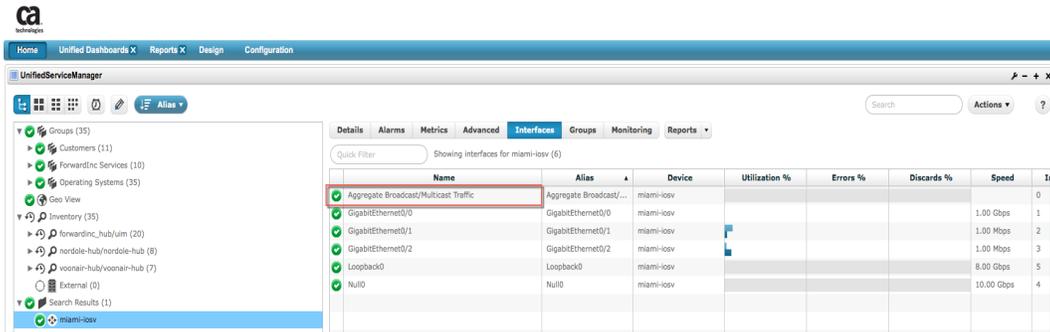
- B. Validate nfa\_inventory probe has successfully started on NFA Console.



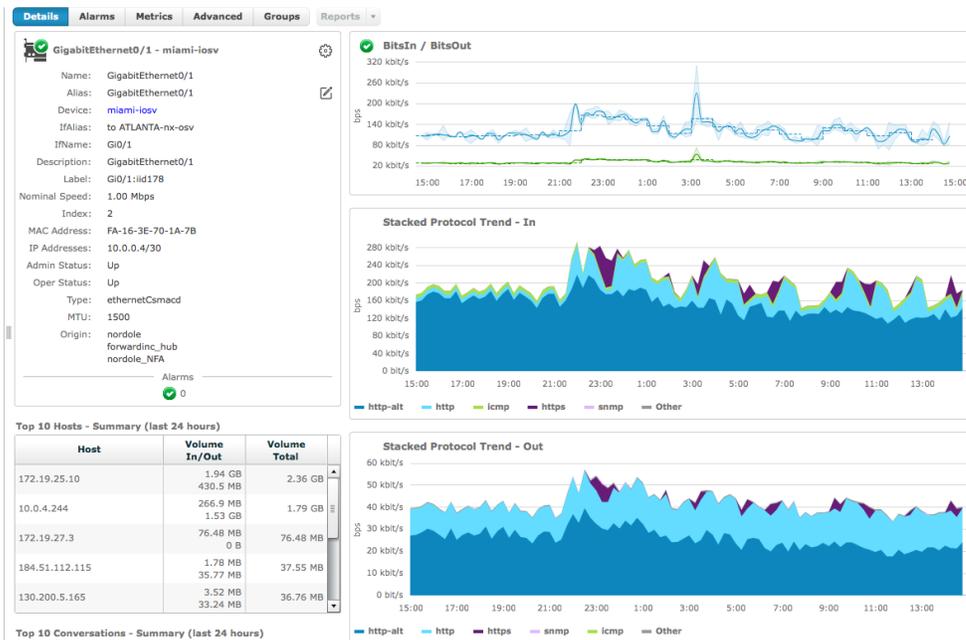
- C. Configure nfa\_inventory probe. Admin Console – Select NFA Robot – Select NFA Inventory – Select Configure – Click Add Console – Add Console Name and IP Address – Click Submit – Click Save



- D. Validate NFA Inventory in UMP – In UMP – Select Router that is in NFA – Click Interface tab – Look for Aggregate Broadcast/Multicast Interface in the list



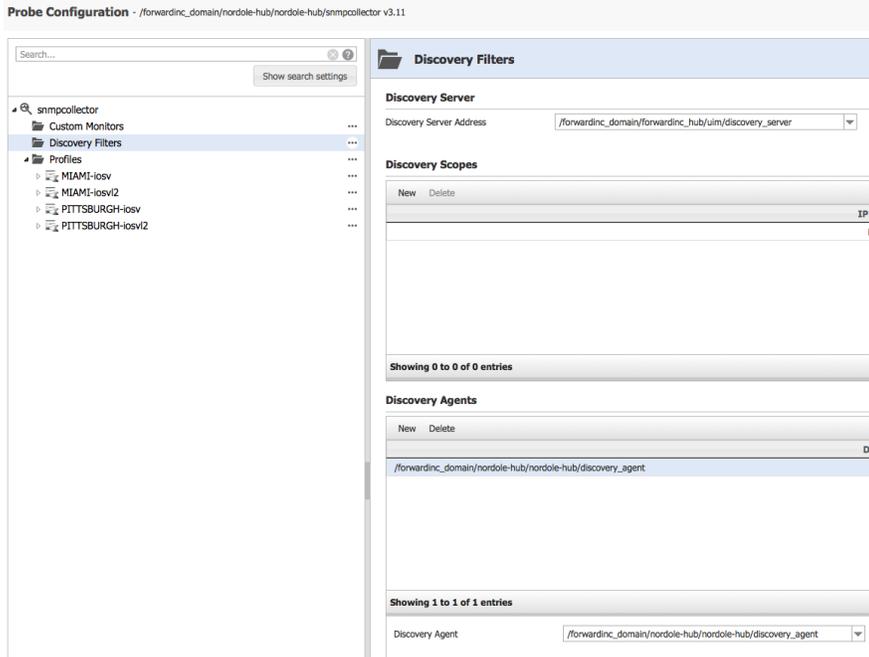
- E. Validate NFA Data in UMP - Select Router that is in NFA – Click Interface tab – Select Interface. The first graph (BitsIn/BitsOut) will not show until SNMP is configured.



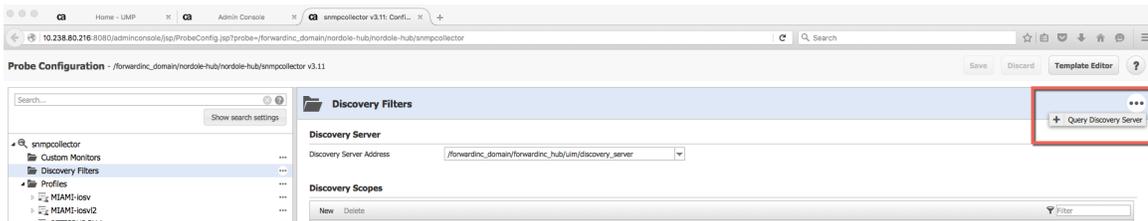
## SNMPCollector (Customer Nordole):

### Step 1. Configure SNMPCollector

- A. Admin Console – Select SNMPCollector Robot – Select SNMPCollector Probe - Configure
- B. Create Discovery Filter for appropriate for Nordole discovery\_agent

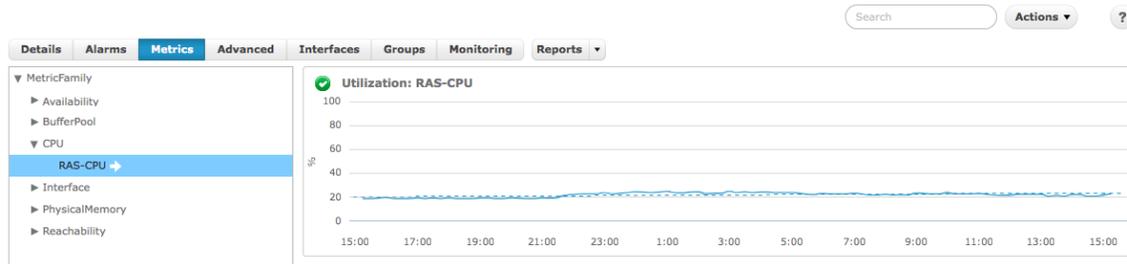


- C. Query Discovery Server for devices to begin discovery and polling of Nordole devices.



## Step 2. Validate SNMPCollector Data

- A. Validate SNMP data for Nordole devices. – Wait 15min after querying the discovery server – In UMP – Select Nordole Network Device – Select Metrics Tab – Expand Metric Family – Select CPU -



- B. Once Nordole SNMP devices have been validated, Repeat Steps for VoonAir.

## QOS Enrichment Steps (ForwardInc MSP):

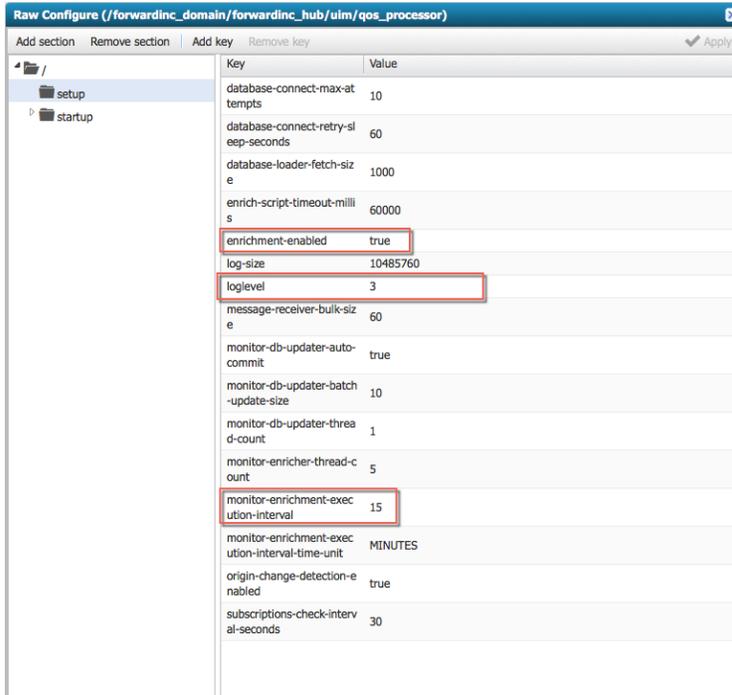
### Step 1. Create Ruby Script and Enable qos\_processor

- A. Create enrichment.rb ruby script to enrich the devices with the appropriate origins.

Example Script:

```
C:\Program Files (x86)\Nimsoft\probes\slm\qos_processor\scripts\enrichment.rb - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
enrichment.rb
1 require 'java'
2
3 $logger.info('Ruby Enricher for qos: ' + $monitor.qos_name + ", source: " + $monitor.source + ", target: " + $monitor.target)
4 $logger.info("Monitor before: origin = " + $monitor.origin + "'")
5
6 if (!$monitor.probe.nil? && $monitor.probe == 'pollagent')
7   if ($monitor.source == 'DALLAS-csr1000v')
8     $monitor.origin = 'voonair'
9   elsif ($monitor.source == 'SAN DIEGO-iosxr')
10    $monitor.origin = 'voonair'
11  elsif ($monitor.source == 'SAN DIEGO-iosv12')
12    $monitor.origin = 'voonair'
13  elsif ($monitor.source == 'PITTSBURGH-iosv')
14    $monitor.origin = 'nordole'
15  elsif ($monitor.source == 'PITTSBURGH-iosv12')
16    $monitor.origin = 'nordole'
17  elsif ($monitor.source == 'MIAMI-iosv')
18    $monitor.origin = 'nordole'
19  elsif ($monitor.source == 'MIAMI-iosv12')
20    $monitor.origin = 'nordole'
21  end
22 end
23
24 $logger.info("Monitor after: origin = " + $monitor.origin + "'")
25 $logger.info('Goodbye, Ruby!')
```

- B. Copy enrichment.rb script to qos\_processor scripts directory. Ex: C:\Program Files (x86)\Nimsoft\probes\slm\qos\_processor\scripts
- C. Configure and Enable qos\_processor – Admin Console – Select Primary Hub – Select Qos\_Processor Probe – Select Raw Configure – Change Log Level to 3, Enrichment-Enabled to true and Monitor-Enrichment-Execution-Interval to 15 minutes.



## Step 2. Validate Origin Enrichment

- A. Log File Method – Admin Console – Select Primary Hub – Select qos\_processor - View Log File – Look for entries such as:

```
#3, qos_processor] Ruby Enricher for qos: QOS_INTERFACE_UTILIZATIONOUT, source: PITTSBURGH-iosv12, target: Gi0/0(GigabitEthernet0/0)
#3, qos_processor] Monitor before: origin = 'forwardinc_hub'
#3, qos_processor] Monitor after: origin = 'nordole'
```

- B. UI Method – In UMP – Select Network Device – Select Interface Tab – Select Interface – Look for modified origin:

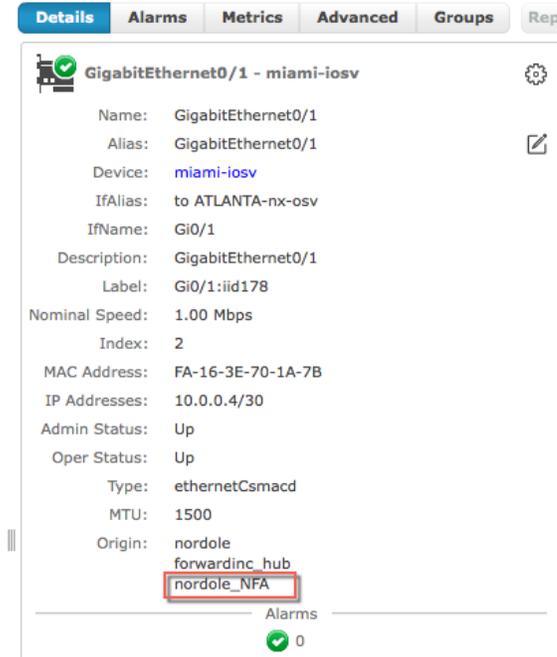
The screenshot shows the configuration page for the network interface GigabitEthernet0/1 on the device miami-iosv. The 'Origin' field is highlighted with a red box and contains the value 'nordole'. Other fields include Name, Alias, Device, IfAlias, IfName, Description, Label, Nominal Speed, Index, MAC Address, IP Addresses, Admin Status, Oper Status, Type, and MTU.

## Step 3. Validate Origin to NFA Interface Group Mapping

- A. Log File Method – Admin Console – Select NFA Robot – Select nfa\_inventory probe - View Log File – Look for entries such as:

```
Feb 15 20:01:21:604 [interfaceToOriginMapping, nfa_inventory] About to map NFA interfaces to UIM origins.
Feb 15 20:01:22:187 [interfaceToOriginMapping, nfa_inventory] Processing interface 175 with 1 origins
Feb 15 20:01:22:187 [interfaceToOriginMapping, nfa_inventory] Found origin nordole for interface 175
Feb 15 20:01:22:187 [interfaceToOriginMapping, nfa_inventory] Found origin voonair for interface 172
Feb 15 20:01:22:187 [interfaceToOriginMapping, nfa_inventory] Processing interface 173 with 1 origins
Feb 15 20:01:22:187 [interfaceToOriginMapping, nfa_inventory] Found origin voonair for interface 173
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Processing interface 201 with 1 origins
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Found origin nordole for interface 201
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Processing interface 179 with 1 origins
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Found origin nordole for interface 179
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Processing interface 178 with 1 origins
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Found origin nordole for interface 178
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Processing interface 176 with 1 origins
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Found origin nordole for interface 176
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Origin: nordole Interfaces: 201, 175, 178, 179, 176,
Feb 15 20:01:22:188 [interfaceToOriginMapping, nfa_inventory] Origin: voonair Interfaces: 173, 172,
```

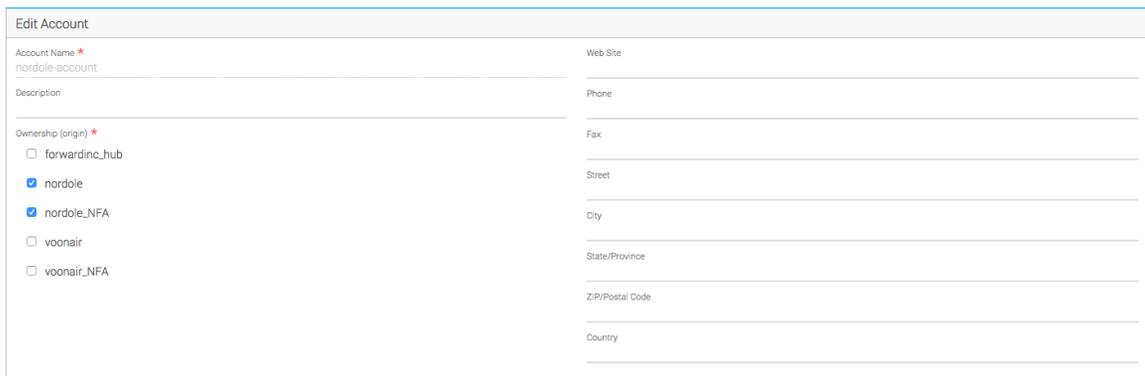
- B. UI Method – In UMP – Select Network Device – Select Interface Tab – Select Interface – Look for modified origin with `_NFA`



### Create Customer Access (ForwardInc MSP):

#### Step 1. Create UIM Accounts for each customer.

- A. In UMP – Click Configuration – Accounts – Click + to add account – enter nordole-account for Account Name – Select nordole and nordole\_nfa for origins and click create.



The screenshot shows the 'Edit Account' form. The 'Account Name' field is filled with 'nordole-account'. The 'Ownership (origin)' section has two radio buttons selected: 'nordole' and 'nordole\_NFA'. The 'Web Site' field is empty. The 'Phone', 'Fax', 'Street', 'City', 'State/Province', 'ZIP/Postal Code', and 'Country' fields are also empty.

- B. In UMP – Click Configuration – Accounts – Click + to add account – enter voonair-account for Account Name – Select voonair and voonair\_nfa for origins and click create.

Edit Account	
Account Name * voonair-account	Web Site
Description	Phone
Ownership (origin) *	Fax
<input type="checkbox"/> forwardinc_hub	Street
<input type="checkbox"/> nordole	City
<input type="checkbox"/> nordole_NFA	State/Province
<input checked="" type="checkbox"/> voonair	ZIP/Postal Code
<input checked="" type="checkbox"/> voonair_NFA	Country

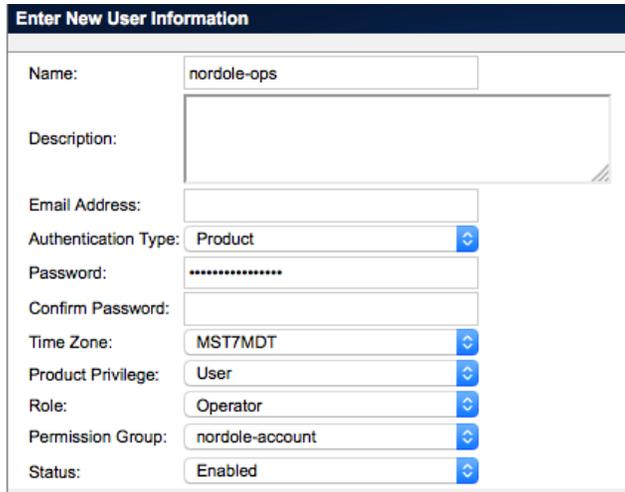
- C. Add User to Account - In UMP – Click Configuration – Accounts – Select nordole-account – click + sign to add user. Enter Login ID, Password, Confirm Password, ACL, Email, First and Last Name and click create. Example Nordole User:

Edit User	
Login ID * nordole-ops	Email * nordole-ops@nordole.com
Password  *****	First Name * Nordole
ACL * Operator	Last Name * Ops
Account * nordole-account	Language English (United States)

- D. Repeat Steps to create a new voonair user mapped to voonair-account.

## Step 2. Provision UIM Customer Account Users to NFA Master Console

- A. In NFA Console – Click Administration – Click Users – Click New – Enter same username and password as used in Step 1 – Item C. All other information can remain default. Note: If username and password are not the same drill-out from UIM will not work. Example NFA User after successful drill out:

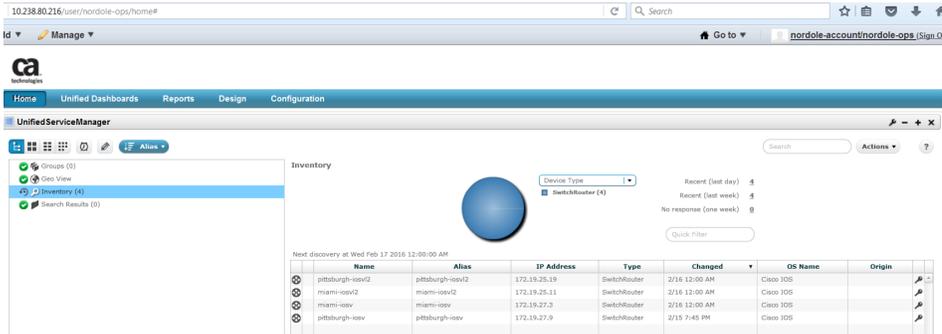


Enter New User Information	
Name:	nordole-ops
Description:	
Email Address:	
Authentication Type:	Product
Password:	*****
Confirm Password:	
Time Zone:	MST7MDT
Product Privilege:	User
Role:	Operator
Permission Group:	nordole-account
Status:	Enabled

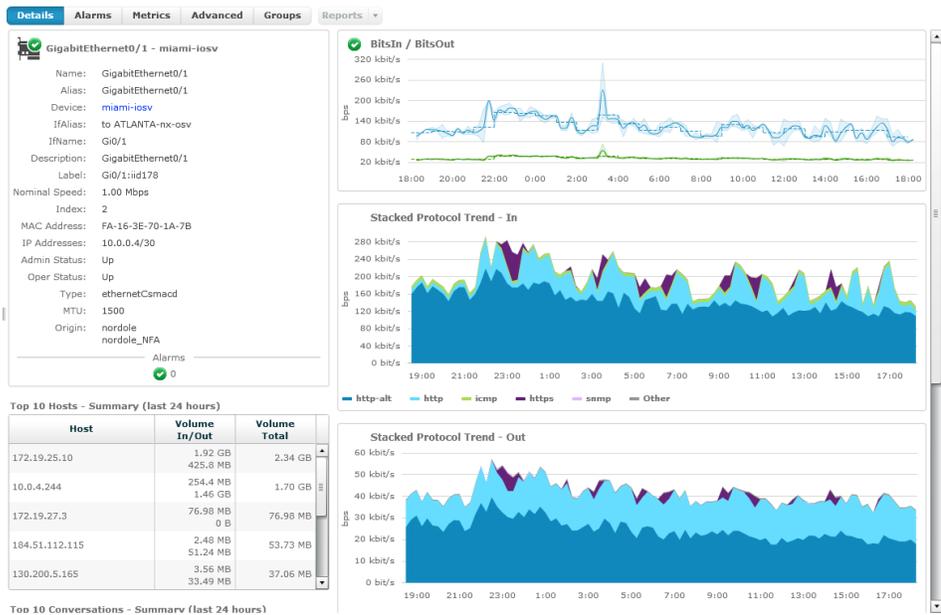
- B. Repeat steps for VoonAir Users:

### Step 3. Validate UIM to NFA workflow for Customers

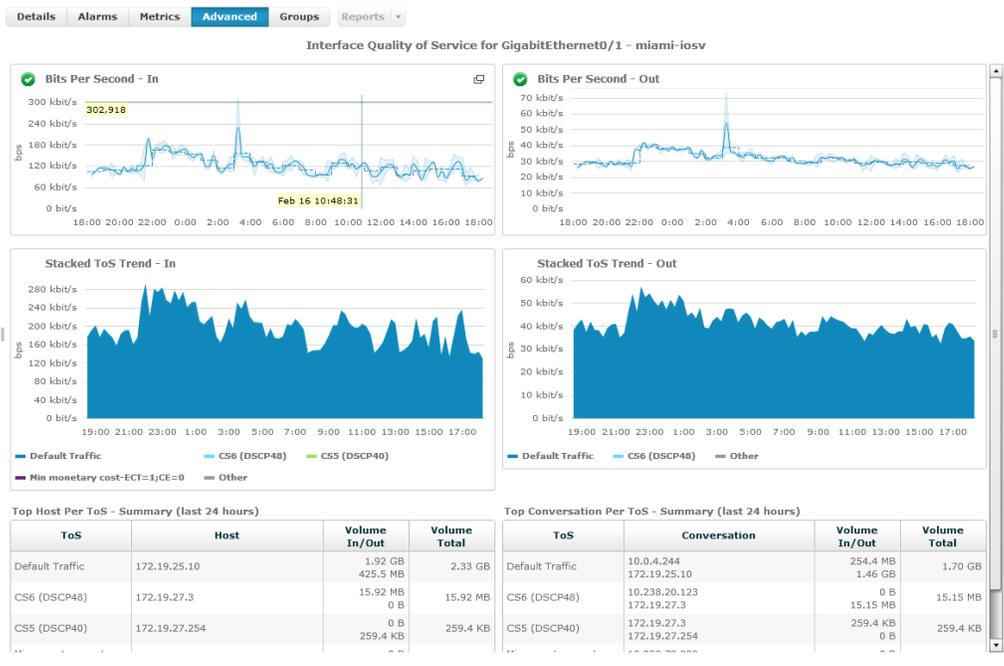
A. In UMP, Login as nordole-ops user and validate inventory only contains devices for the Nordole customer.



B. Validate "Interface Details" (SNMP/Flow data) for an interface on a Nordole device.



C. Validate “Advanced Tab” (SNMP/ToS - Flow data) for an interface on a Nordole device.



D. Validate Drill-out to NFA - Select “Details Tab” – Click on “Launch NFA diagnostics view” from within Stacked Protocol Graph

**Details** | Alarms | Metrics | Advanced | Groups | Reports

**GigabitEthernet0/1 - miami-iosv**

Name: GigabitEthernet0/1  
 Alias: GigabitEthernet0/1  
 Device: miami-iosv  
 IFAlias: to ATLANTA-nx-osv  
 IFName: Gi0/1  
 Description: GigabitEthernet0/1  
 Label: Gi0/1:iid178  
 Nominal Speed: 1.00 Mbps  
 Index: 2  
 MAC Address: FA-16-3E-70-1A-7B  
 IP Addresses: 10.0.0.4/30  
 Admin Status: Up  
 Oper Status: Up  
 Type: ethernetCsmacd  
 MTU: 1500  
 Origin: nordole  
 nordole\_NFA

Alarms: 0

**Top 10 Hosts - Summary (last 24 hours)**

Host	Volume In/Out	Volume Total
172.19.25.10	1.92 GB 425.8 MB	2.34 GB
10.0.4.244	254.4 MB 1.46 GB	1.70 GB
172.19.27.3	76.98 MB 0 B	76.98 MB
184.51.112.115	2.48 MB 51.24 MB	53.73 MB
130.200.5.165	3.56 MB 33.49 MB	37.06 MB

**BitsIn / BitsOut**

**Stacked Protocol Trend - In**

**Stacked Protocol Trend - Out**

**Network Flow Analysis** | Enterprise Overview | Interfaces | Custom Reporting | Flow Forensics | Analysis | Site to Site | Administration

MIAMI-iosv (172.19.27.3)::Gi0/1 - to ATLANTA-nx-osv [change]

1. For this interface, show me: Protocols | **Top N Protocols**

February 15, 2016 6:25:00 PM - February 16, 2016 6:25:00 PM MST

**Flow Forensics**

Stacked Protocol Trend - In  
 February 15, 2016 6:25:00 PM - February 16, 2016 6:25:00 PM MST  
 MIAMI-iosv (172.19.27.3)::Gi0/1 - to ATLANTA-nx-osv

97 samples at 15-minute resolution

Legend: http-alt (\* (p.tcp.8080)), http (\* (p.tcp.80)), icmp (\* (p.1)), https (\* (p.tcp.443)), snmp (\* (p.udp.161)), dns (\* (p.udp.53)), ospf (\* (p.89)), Other

E. Validate NFA Access to only Nordole devices and interfaces – Select Change next to current interface to display list of available interfaces and devices.

**Interface Index** Close X

Router | Interface

Search [Clear Filter](#) Max per Page: 20

MIAMI-iosv (172.19.27.3) 3 Interfaces

Filter By:  All  Active  Inactive Max per page: 10

Interface	Description	Type	In Speed	Out Speed	Active	Last Updated (MST)	Notes
Gi0/0	OoB Management	LAN-ET	1.00 Gbps	1.00 Gbps	No	Never	
Gi0/1	to ATLANTA-nx-osv	LAN-ET	1.00 Mbps	1.00 Mbps	Yes	February 16, 2016 6:30 PM	
Gi0/2	to MIAMI-iosv2	LAN-ET	1.00 Mbps	1.00 Mbps	Yes	February 16, 2016 6:30 PM	

PITTSBURGH-iosv (172.19.27.9) 2 Interfaces

## Troubleshooting

### NFA Origin to Interface Group Mapping failing

A. Run the following query to verify origin enrichment has occurred.

```
select distinct source, origin, nim_origin from s_qos_data order by source;
```

source	origin	nim_origin
1 ada	forwardinc_hub	forwardinc_hub
2 ada-col-sp	forwardinc_hub	forwardinc_hub
3 ADA-COL-SP-TIX	forwardinc_hub	forwardinc_hub
4 ADA-COL-TIX-QA	forwardinc_hub	forwardinc_hub
5 ATLANTA-rx-osv	forwardinc_hub	forwardinc_hub
6 AUSTIN-rx-osv	forwardinc_hub	forwardinc_hub
7 BOSTON-rx-osv	forwardinc_hub	forwardinc_hub
8 DALLAS-csr1000v	voonair	forwardinc_hub
9 DENVER-iosv	forwardinc_hub	forwardinc_hub
10 FORT-COLLINS	forwardinc_hub	forwardinc_hub
11 MIAMI-iosv	nordole	forwardinc_hub
12 MIAMI-iosv2	nordole	forwardinc_hub
13 nordole-txchange-web_nordole.viril.info	forwardinc_hub	forwardinc_hub
14 nordole-txchange-ws_db_nordole.viril.info	forwardinc_hub	forwardinc_hub
15 PITTSBURGH-iosv	nordole	forwardinc_hub
16 PITTSBURGH-iosv2	nordole	forwardinc_hub
17 SANDIEGO-iosv2	voonair	forwardinc_hub
18 SANDIEGO-iosv	voonair	forwardinc_hub
19 um	forwardinc_hub	forwardinc_hub
20 voonair-txchange-web_voonair.viril.info	forwardinc_hub	forwardinc_hub
21 voonair-txchange-ws_db_voonair.viril.info	forwardinc_hub	forwardinc_hub

B. Run the following query to make sure changes are getting through to discovery\_server.

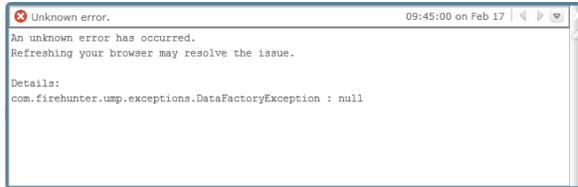
```
select * from cm_computer_system where cs_id in (select cs_id from cm_computer_system_attr where cs_attr_value like '%Nordole');
```

state_time	change_time	alive_time	caption	description	dedicated	state	name	domain	origin	ip	dns_ns
1 116-02-15 18:43:31.287	2016-02-17 00:00:29.210	2016-02-17 00:00:29.210	NULL	Cisco IOS Software, vios_J2 Software (VIOS-J2-ADVENT...	SwitchRouter	0	miami-iosv2	NULL	forwardinc_hub	172.19.25.11	miami-
2 116-02-15 18:43:34.330	2016-02-16 00:00:30.277	2016-02-17 09:11:29.357	NULL	Cisco IOS Software, IOSv Software (VIOS-ADVENTERP...	SwitchRouter	0	miami-iosv	NULL	forwardinc_hub	172.19.27.3	miami-
3 116-02-15 18:43:35.553	2016-02-17 00:00:44.153	2016-02-17 00:00:44.153	NULL	Cisco IOS Software, vios_J2 Software (VIOS-J2-ADVENT...	SwitchRouter	0	pittsburgh-iosv2	NULL	forwardinc_hub	172.19.25.19	pittsbu
4 116-02-15 18:43:43.740	2016-02-15 19:45:17.787	2016-02-17 09:11:29.330	NULL	Cisco IOS Software, IOSv Software (VIOS-ADVENTERP...	SwitchRouter	0	pittsburgh-iosv	NULL	forwardinc_hub	172.19.27.9	pittabu

If the changes are not propagating as expected, go back and validate qos\_processor changes are occurring (requires log level 3), it is also suggested to restart snmpcollector to facilitate qos\_processor changes.

## Drillout from UIM to NFA Fails with “Unknown Error”

When drilling out from UIM to NFA and you receive the following error:



This error will be shown when the UIM user is not provisioned in NFA. Please refer back to page 16 for details on completing this process.