



Configuration Guide for Network Device Monitoring

Table of Contents

| | |
|---|-----------|
| Introduction..... | 2 |
| Scope and Purpose | 2 |
| Architecture Overview | 2 |
| General Procedure..... | 3 |
| Applying NDM License | 4 |
| Defining and Activating Network Devices to be Monitored | 4 |
| Data Collected by Network Device Monitor | 12 |
| Switch or Router Property | 12 |
| Switch / Router Statistics are used to define the ‘Solid’ colors for the ports in NDM user interface | 12 |
| Creating Alert for Network Devices | 13 |
| Device Port Down or Cable Unplugged | 13 |
| Ports in High Utilization Rate, # of Discard Packets, or # of Error Packets | 15 |
| APPENDIX | 17 |
| Confirming Additional Requirements for the target Network Device and connected VMs | 17 |

Introduction

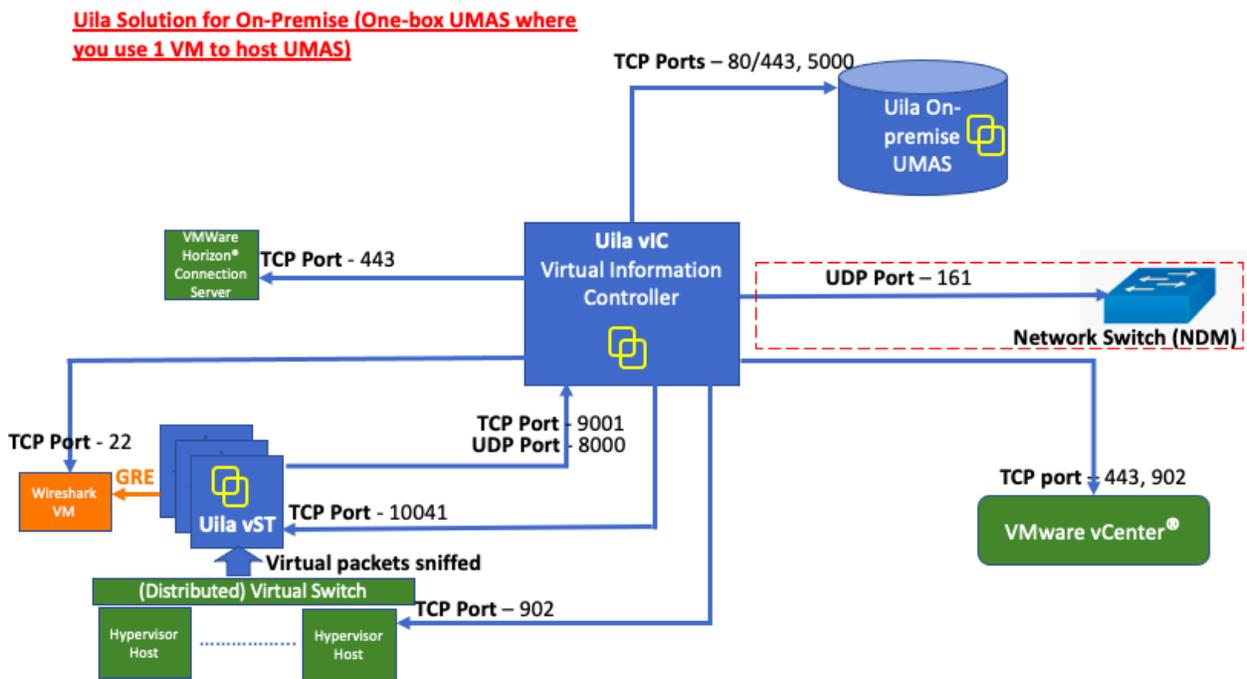
Scope and Purpose

This document describes enabling and configuring Network Device Monitoring (NDM) in order to monitor network switches, routers, load balancers, firewalls, etc.

It is assumed that the reader has already installed VMware and is familiar with the configurations and operations of VMware.

Architecture Overview

The diagram below shows Network Device Monitor related to the Uila Management and Analytics System (UMAS), Virtual Information Controller(vIC) and Uila Virtual Smart Taps(vST).



General Procedure

1. Prerequisites
2. Applying the NDM License
3. Define network devices to monitor
4. Run command in the vic “enablendm”

```
root@vIC>statusall
VIM running [3840832] ...
FlumeAgent Client running [2464466] ...
UpgradeManager Server running [3824940] ...
RabbitMQ running [2462164] ...
ExternalMonitorWorker running [2464551] ...
Monit Server running [1570486] ...
root@vIC>enablendm
Created symlink /etc/systemd/system/multi-user.target.wants/netdisco.service → /etc/systemd/system/netdisco.service.
Created symlink /etc/systemd/system/multi-user.target.wants/uila-network-monitor.service → /etc/systemd/system/uila-network-monitor.service.
Enabled NDM.
root@vIC>statusall
VIM running [3840832] ...
FlumeAgent Client running [2464466] ...
UpgradeManager Server running [3824940] ...
NetDisco ALL Processes running ...
 * Backend running [1570882]
 * Postgres running [1570846]
RabbitMQ running [2462164] ...
NetworkMonitor running [1570956] ...
ExternalMonitorWorker running [2464551] ...
Monit Server running [1571016] ...
root@vIC>
```

Prerequisites:

The following will be required during configuration.

1. Uila NDM License
2. The IP addresses or ranges of the network devices to be monitored
3. SNMP v2 or v3 credentials for your network devices.
 - v2
 - community string
 - v3
 - Authentication Protocol and password: MD5,SHA
 - Privacy Protocol and password: DES,AES128,AES196,AES256

Firewall Ports

vIC is the Uila module that will scan your network to discover and query networking devices. Make sure the inbound and outbound of SNMP port 161 is opened at your firewall between vIC VM and the target networking devices

vIC Resources

More resources are needed on vIC to handle the additional workload introduced by networking device monitoring. Please use the table below as a reference on how to raise the vIC size.

| vIC sizes | vCPU without NDM | vCPU with NDM | Memory without NDM | Memory with NDM | Storage without NDM | Storage with NDM |
|-----------|------------------|---------------|--------------------|-----------------|---------------------|------------------|
| small | 2 cores | 2 cores | 4GB | 8GB | 8GB | 16GB |
| | 4 cores | 4 cores | 24GB | | 24GB | |
| medium | 2 cores | 4 cores | 8GB | 12GB | 8GB | 16GB |
| | 4 cores | 4 cores | 32GB | | 24GB | |
| large | 2 cores | 4 cores | 16GB | 20GB | 8GB | 16GB |
| | 4 cores | 4 cores | 48GB | | 24GB | |

Refer to Appendix to confirm the devices to be monitored support MIB tables.

Applying NDM License

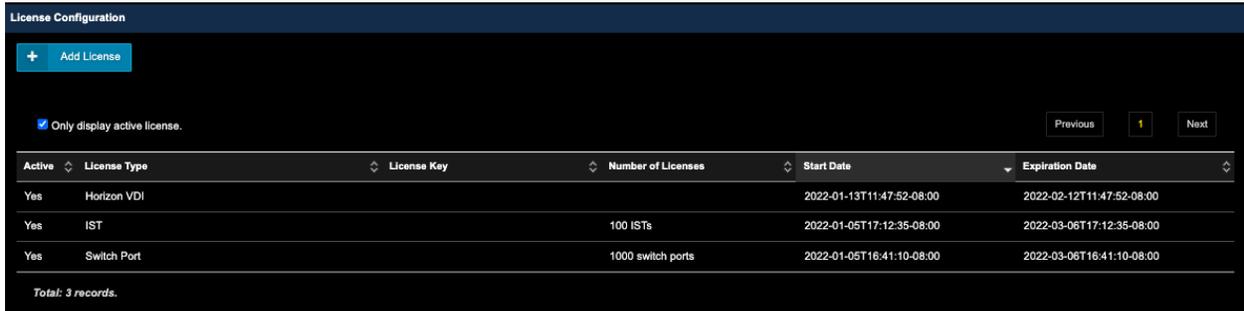
For Uila portal user, the NDM license will be applied and activated by Uila.

For Uila on-prem installations, the NDM license (a TAR file) will be provided by Uila, and follow the instruction below to add the license.

- A) Go to Settings —> Global Configuration
- B) Scroll to licenses
- C) Add the attached license and use the register id below:

Register ID: xxxxxxxx (Register ID is provided by Uila and case-sensitive.)

And verify you have Switch Port license in the Global Configuration -> License Configuration.



The screenshot shows the 'License Configuration' page with a table of active licenses. The table has columns for Active, License Type, License Key, Number of Licenses, Start Date, and Expiration Date. There are three records listed: Horizon VDI, IST, and Switch Port.

| Active | License Type | License Key | Number of Licenses | Start Date | Expiration Date |
|--------|--------------|-------------|--------------------|---------------------------|---------------------------|
| Yes | Horizon VDI | | | 2022-01-13T11:47:52-08:00 | 2022-02-12T11:47:52-08:00 |
| Yes | IST | | 100 ISTs | 2022-01-05T17:12:35-08:00 | 2022-03-06T17:12:35-08:00 |
| Yes | Switch Port | | 1000 switch ports | 2022-01-05T16:41:10-08:00 | 2022-03-06T16:41:10-08:00 |

Total: 3 records.

Defining and Activating Network Devices to be Monitored

Collect your Network Device SNMP setting first

| | | |
|-----------|---|-------------------|
| V2 | Community String | Public or Private |
| V3 | SNMP Group name | |
| | Authentication Protocol | NONE, MD5, SHA |
| | Authentication Protocol Password | |

| | | |
|--|----------------------------------|--------------------------------------|
| | Privacy Protocol | NONE, DES, AES128, AES196 and AES256 |
| | Privacy Protocol Password | |

In network Firewall setting:

Open UDP port 161 from VIC to Network Device

Then Log in to Uila as the primary administrator.

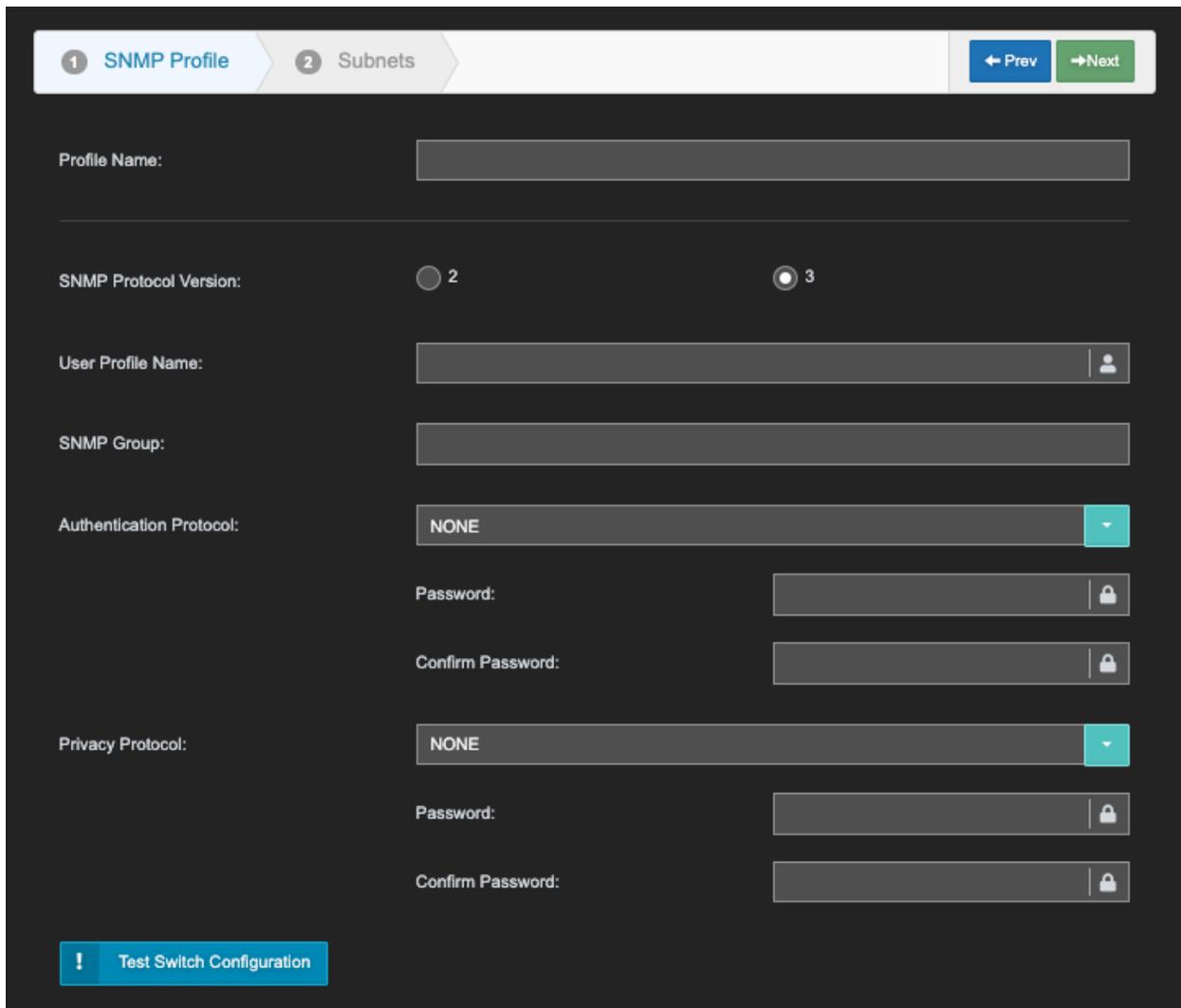
Go to **Settings->Device Monitoring**

Creating an unique SNMP profile for Uila account

In the SNMP Device Discover Profile, click **New**.



The SNMP Device Discover Profile configuration template will appear.



If you use SNMP Protocol Version 2, Select 

Fill in the following:

Profile Name

A unique name for a group of network devices that share the same profile. May also be used to logically group devices by some other characteristic (i.e. location). However, any devices defined in the group must have a common SNMP V2 or V3 profile as listed earlier.

Agent Port, default is 161

Community string. Click the dropdown list for “public” or “private”

SNMP Device Discover Profile ✕

1 SNMP Profile

2 Subnets

← Prev

→ Next

Profile Name:

Agent Port:

SNMP Protocol Version: 2 3

Community:

! Test Switch Configuration

If you use SNMP Protocol Version 3, Select



Fill in the following:

| | |
|---|---|
| User Profile Name | SNMP User name. No duplicated name supported if there is more one (1) profile are created. |
| SNMP Group | Enter the SNMP Group. |
| Authentication Protocol and Password | Select the Authentication protocol and password. The supported protocols: NONE, MD5, SHA |
| Privacy Protocol and Password | Select the Privacy protocol and password. The supported protocols: NONE, DES, AES128, AES196 and AES256 |

SNMP Device Discover Profile

1 **SNMP Profile** 2 Subnets ← Prev → Next

Profile Name:

Agent Port:

SNMP Protocol Version: 2 3

User Profile Name:

SNMP Group:

Authentication Protocol:

Password: *This field is required.*

Confirm Password: *This field is required.*

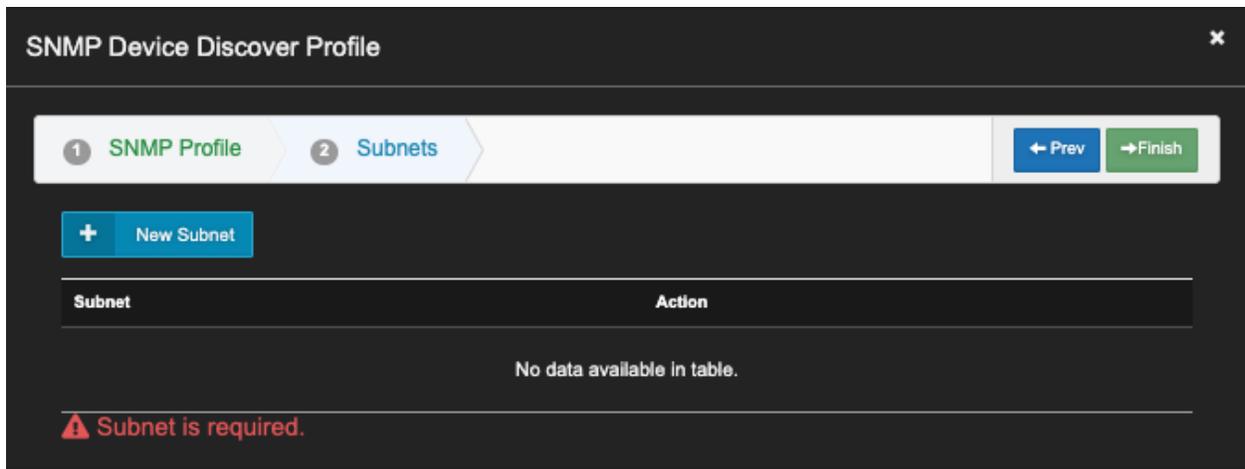
Privacy Protocol:

Password: *This field is required.*

Confirm Password: *This field is required.*

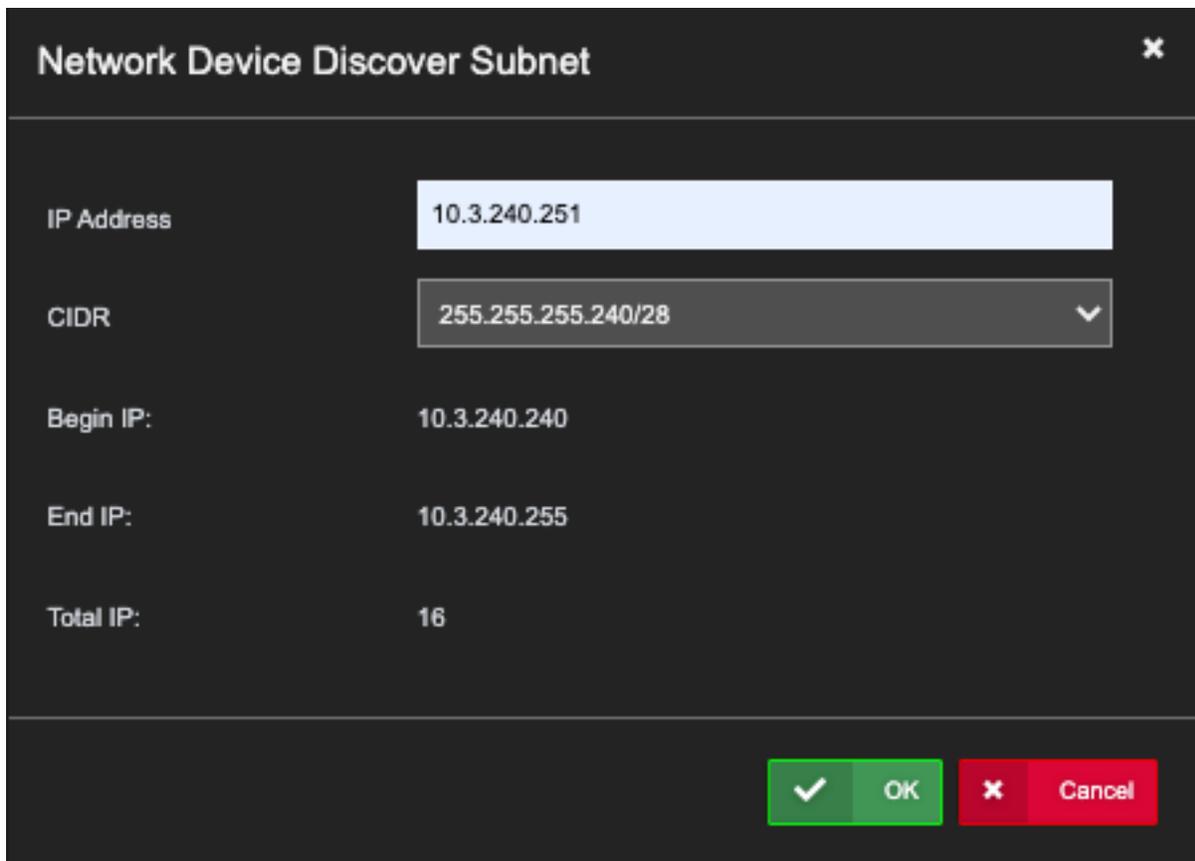
! Test Switch Configuration

Click Next



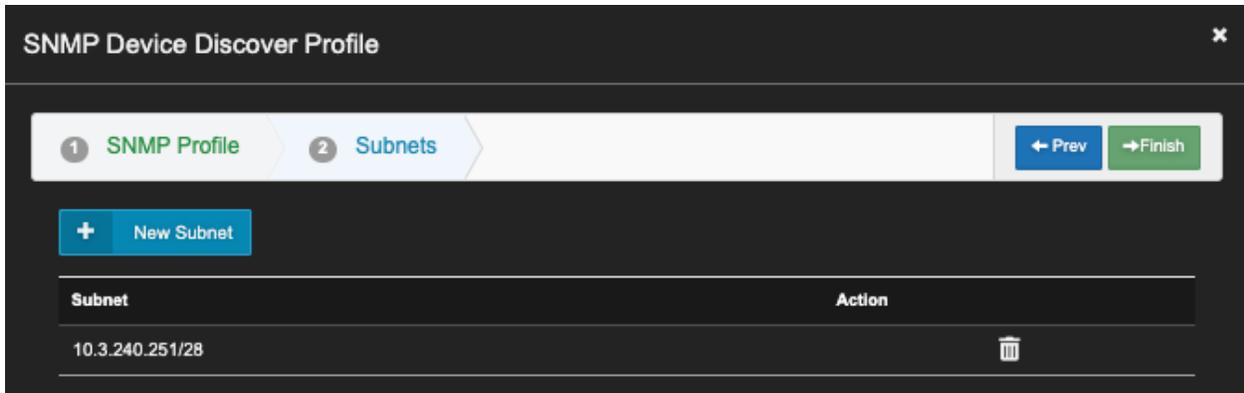
The dialog box titled "SNMP Device Discover Profile" has a close button (X) in the top right corner. It features a progress bar with two steps: "1 SNMP Profile" and "2 Subnets". Below the progress bar is a "New Subnet" button with a plus sign. Underneath is a table with two columns: "Subnet" and "Action". The table is currently empty, with the text "No data available in table." centered below it. At the bottom, there is a red warning icon and the text "Subnet is required." To the right of the progress bar are "Prev" and "Finish" buttons.

Click New Subnet



The dialog box titled "Network Device Discover Subnet" has a close button (X) in the top right corner. It contains several input fields: "IP Address" with the value "10.3.240.251", "CIDR" with a dropdown menu showing "255.255.255.240/28", "Begin IP:" with the value "10.3.240.240", "End IP:" with the value "10.3.240.255", and "Total IP:" with the value "16". At the bottom right, there are two buttons: a green "OK" button with a checkmark and a red "Cancel" button with an X.

Enter IP Address and CIDR, Click OK.



Click Finish to Complete the Setting.

Check The devices listed in the SNMP Device Discover Profile



Next, Go to **Settings->Device Monitoring->Enable Device for Monitoring**, click on **Configuration**.



Check **Enable** the Device(s) to be monitored and click OK.

Enable Device for Monitoring

| | Discovered | Enabled |
|------------------|------------|---------|
| Network Device | 5 | 4 |
| Physical Port(s) | 98 | 94 |
| Active Port(s) | 43 | 40 |

| Device Name | IP Address | Physical Port(s) | Active Port(s) | Enable |
|------------------------------|---------------|------------------|----------------|-------------------------------------|
| Cisco-C3650.mydatacenter.com | 192.168.2.253 | 29 | 12 | <input checked="" type="checkbox"/> |
| cisco-sg300-sw2 | 192.168.0.252 | 10 | 3 | <input checked="" type="checkbox"/> |
| EdgeRouter-4 | 192.168.0.1 | 4 | 3 | <input type="checkbox"/> |
| pfSense.localdomain | 192.168.0.190 | 3 | 3 | <input checked="" type="checkbox"/> |
| switchfc63b9 | 192.168.0.251 | 52 | 22 | <input checked="" type="checkbox"/> |

Wait for 15 to 60 minutes, the newly added network devices will appear with ports populated.

Go to left side of Uila screen, Click Infrastructure->Network Device.

| Device Name | Ports | Network Device Info |
|--|------------------|---------------------|
| pfSense.localdomain (192.168.0.190) | 3 green squares | Info icon |
| switchfc63b9 (192.168.0.251) | 52 green squares | Info icon |
| cisco-sg300-sw2 (192.168.0.252) | 10 green squares | Info icon |
| Cisco-C3650.mydatacenter.com (192.168.2.253) | 29 green squares | Info icon |

Data Collected by Network Device Monitor

Switch or Router Property

Configuration settings including vendor, model, OS versions, uptime, serial number, VTP domain, detailed description, IP/MAC address, etc.

Switch / Router Statistics are used to define the 'Solid' colors for the ports in NDM user interface

- In/Out Utilization
- In/Out Discards
- In/Out Errors

Color of the Port is defined by the Delta mount from the baseline described below.

The Default baselines are as follows:

- Utilization: 80%
- Discards: 999,000,000 pkts/min
- Errors: 999,000,000 pkts/min

Alarm is generated based on the performance metric's delta from the baseline. Alarm is generated every 15 minutes by default.

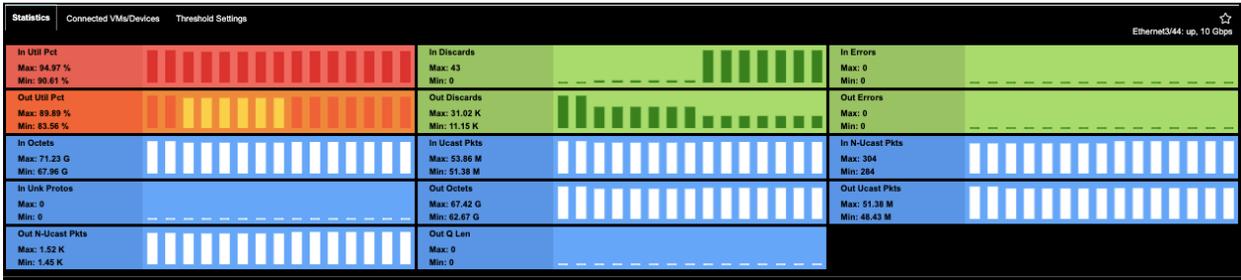
Threshold is defined as the % value that crosses the baseline.

Severity is a user definable indicator to help identify the criticality of the performance metrics monitored to alert user if an entity or entities is (are) about to impact the Application's performance.

| Delta from Baseline | Alarm Severity | Color |
|------------------------------------|---------------------|---------------|
| Less or equal to 5% | Normal | Green |
| Between 5% and 10%, including 10% | Minor (1) | Yellow |
| Between 10% and 20%, including 20% | Major (2) | Orange |
| Above 20% | Critical (3) | Red |

Note: These standard color definitions are applied throughout Uila User Interfaces for consistence and ease of recognition.

Below is an example of the Port Statistics and Color.



You can change the thresholds for the parameters from the “Threshold Settings” tab for individual ports. Go to Settings -> Device Monitoring. Scroll down to Network Device Threshold Setting. Click , to change the threshold values.

| Stat Type | Critical Threshold | Major Threshold | Minor Threshold | Actions |
|-----------------|--------------------|--------------------|--------------------|---------|
| In Utilization | 90 % | 85 % | 80 % | |
| In Discards | 999000000 packets | 998000000 packets | 997000000 packets | |
| In Errors | 999000000 packets | 998000000 packets | 997000000 packets | |
| Out Utilization | 90 % | 85 % | 80 % | |
| Out Discards | 9990000000 packets | 9980000000 packets | 9970000000 packets | |
| Out Errors | 9990000000 packets | 9980000000 packets | 9970000000 packets | |

Device Port Icon Definitions

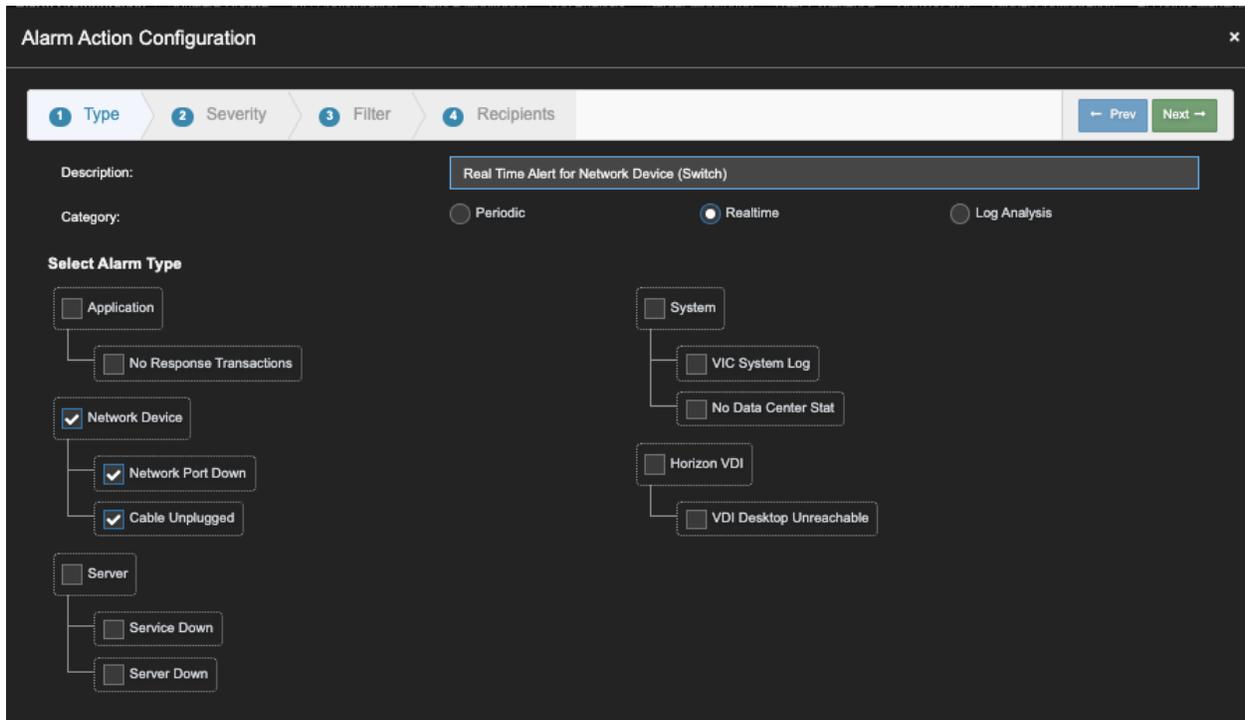
| | |
|---|--|
|  | A server is attached to this port |
|  | Cross link to another network switch or router |
|  | A device is connected |
|  | Open port – no device connected |
|  | Port Statistics are above Normal values |

Creating Alert for Network Devices

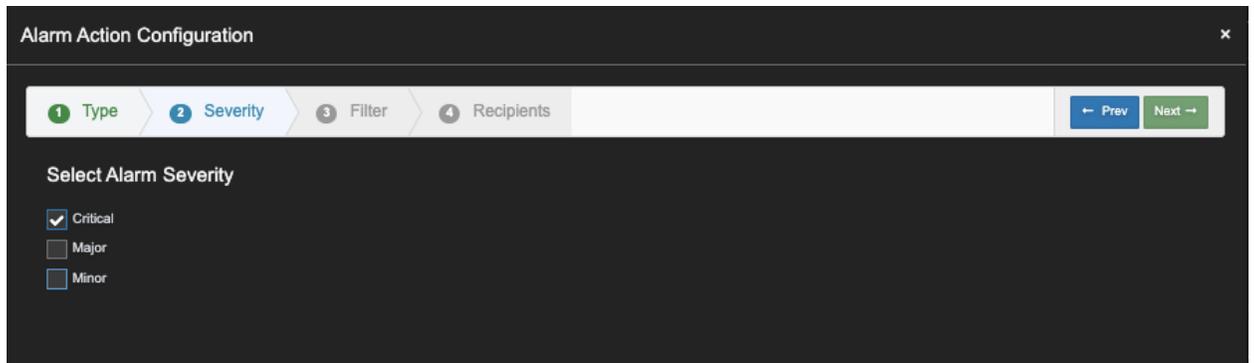
Device Port Down or Cable Unplugged

1. Go to Setting -> Alarm Configuration. Click ‘New Email Action’.

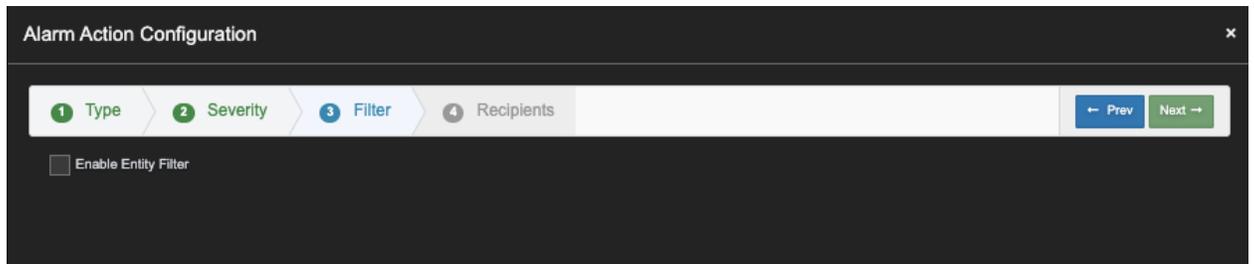
Check ‘Realtime’. Select ‘Network Device’ only. **Note:** Do not Select other Alarm type.



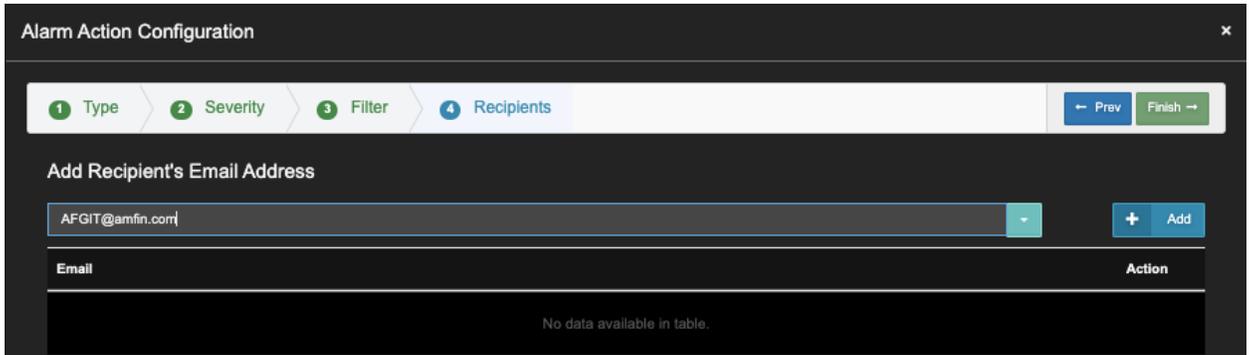
2. Select Alarm Severity to 'Critical', Click 'Next'.



3. Leave Enable Entity Filter Un-checked. (Uila software will use SNMP query to check Network Devices that you have configured in Network Device Setting. Click 'Next'.



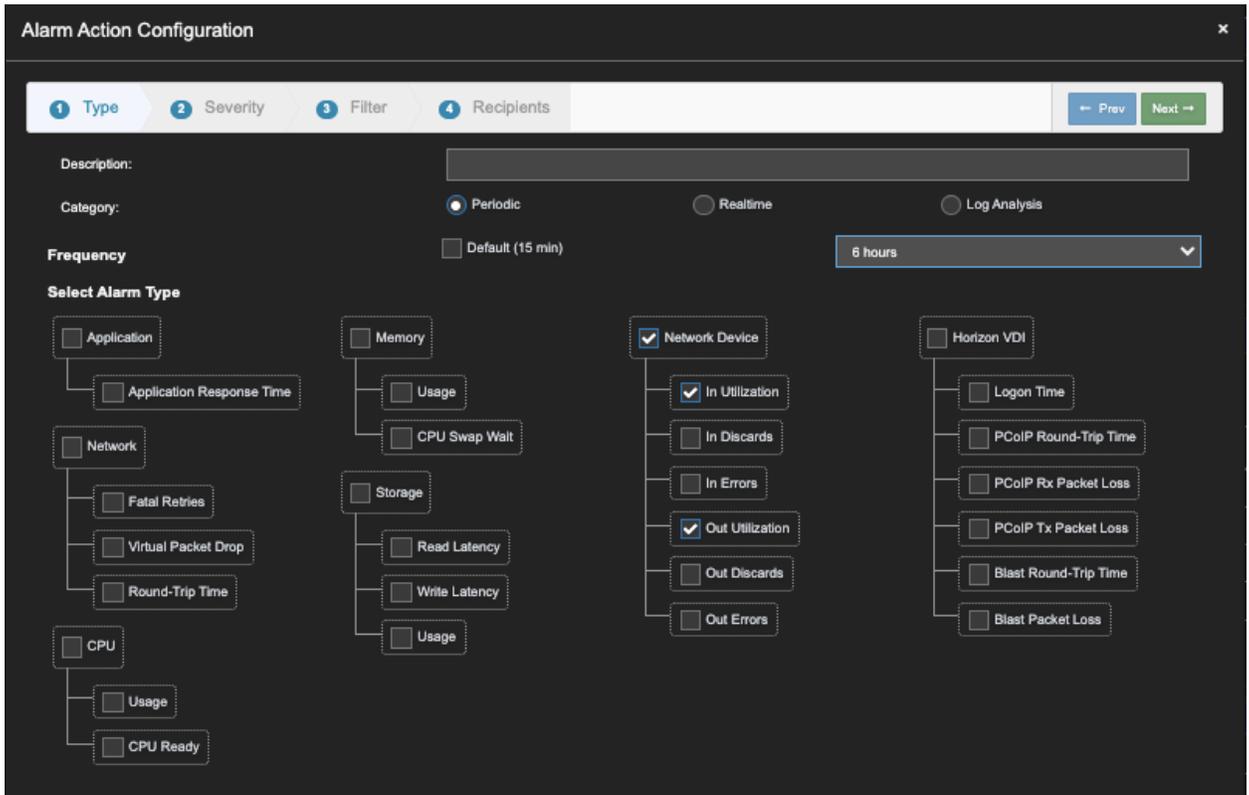
4. Add email address of the alert recipient(s). Click 'Finish'.



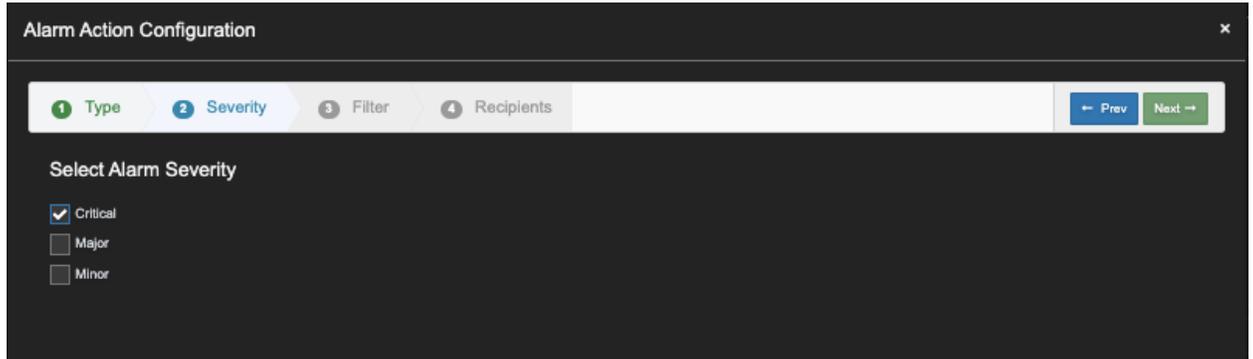
Ports in High Utilization Rate, # of Discard Packets, or # of Error Packets

1. Go to Setting -> Alarm Configuration. Click 'New Email Action'.

Check 'Period'. Select Frequency; 15 min, 1 hour, 3 hours, 6 hours, 12 hours or 24 hours. Select the type of statistics wish to be alerted. Click 'Next'. **Note:** Do not Select other Alarm type.

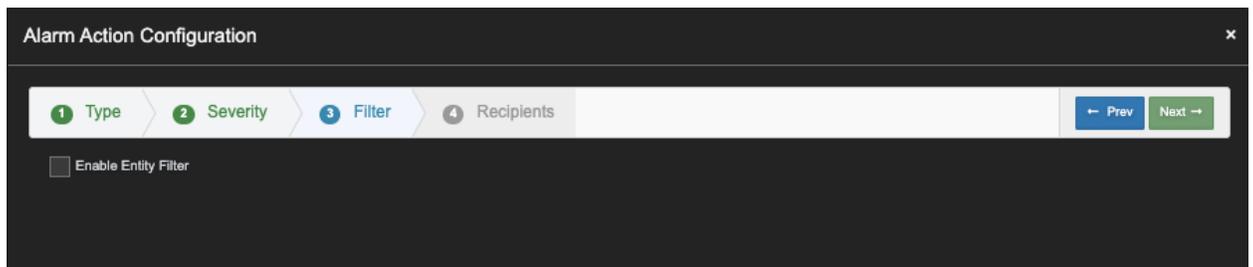


2. Select Alarm Severity, Click 'Next'



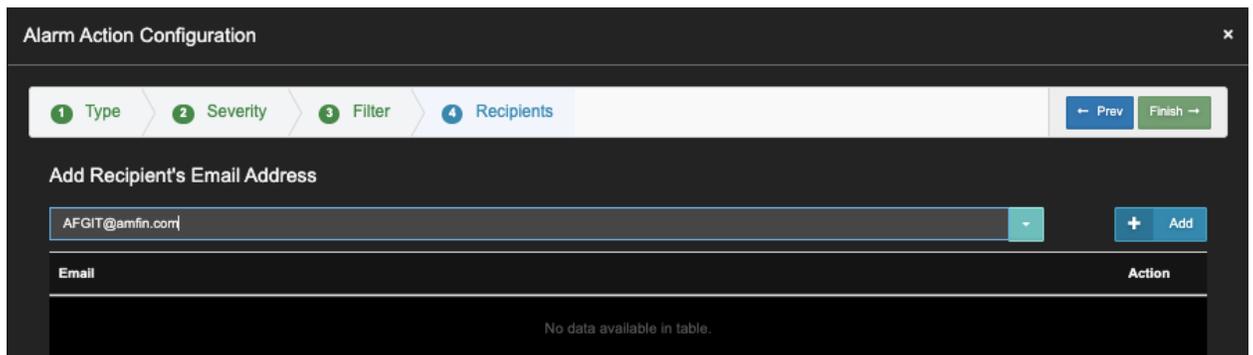
The screenshot shows the 'Alarm Action Configuration' window at step 2, 'Severity'. The progress bar at the top indicates the current step. Below the progress bar, the title 'Select Alarm Severity' is followed by three radio button options: 'Critical' (checked), 'Major', and 'Minor'. Navigation buttons 'Prev' and 'Next' are visible on the right.

3. Leave Enable Entity Filter Un-checked. (Uila software will use SNMP query to check Network Devices that you have configured in Network Device Setting. Click 'Next'.



The screenshot shows the 'Alarm Action Configuration' window at step 3, 'Filter'. The progress bar indicates the current step. Below the progress bar, there is a single checkbox labeled 'Enable Entity Filter' which is currently unchecked. Navigation buttons 'Prev' and 'Next' are visible on the right.

4. Add email address of the alert recipient(s). Click 'Finish'.



The screenshot shows the 'Alarm Action Configuration' window at step 4, 'Recipients'. The progress bar indicates the current step. Below the progress bar, the title 'Add Recipient's Email Address' is followed by a text input field containing 'AFGIT@amfin.com' and an 'Add' button. Below this is a table with columns 'Email' and 'Action'. The table is currently empty, with the message 'No data available in table.' displayed at the bottom.

| Email | Action |
|-----------------------------|--------|
| No data available in table. | |

APPENDIX

To confirm the entries, click on **Test Switch Configuration**. You must have the IP address of the network device to be tested against.

In **Switch IP**, enter the IP address of the network device and click **Test**. A successful test will display a sample query as shown, below.

Test Switch Configuration ✕

Switch IP : ! Test

Test Result :

| ifIndex | ifDescr | ifType | ifMtu | ifSpeed | ifPhysAddress | ifAdminStatus |
|------------|------------------|----------------|-----------|------------|---------------------------|---------------|
| 49 | gigabitethernet1 | ethernetCsmacd | 1500 | 1000000000 | c0:7b:bc:65:22:1d | up |
| up | 0:0:00:37.68 | 334191868 | 195565908 | 134822725 | 0 | 0 |
| 2238220364 | 127972149 | 6418261 | 0 | 0 | ? SNMPv2-SMI::zeroDotZero | |
| 50 | gigabitethernet2 | ethernetCsmacd | 1500 | 1000000000 | c0:7b:bc:65:22:1e | up |
| up | 10:19:04:15.12 | 728064568 | 1141116 | 777 | 0 | 0 |
| 1484061135 | 1149777 | 135594034 | 0 | 0 | ? SNMPv2-SMI::zeroDotZero | |
| 51 | gigabitethernet3 | ethernetCsmacd | 1500 | 1000000000 | c0:7b:bc:65:22:1f | up |
| up | 38:10:50:57.28 | 1671904246 | 123285326 | 500736 | 0 | 0 |
| 3313579855 | 190980747 | 135095535 | 0 | 0 | ? SNMPv2-SMI::zeroDotZero | |

Close the **Test Switch Configuration** by clicking on the X.

Click Next.

Define the Subnet(s) to be discovered by clicking on **New Subnet**.

A single device may be defined by entering its IP Address and setting **CIDR** to 255.255.255.255/32.

For a range of network devices to be discovered, use the appropriate CIDR value.

Click OK.

Click Finish.

Confirming Additional Requirements for the target Network Device and connected VMs

The NDM service must be enabled at the vIC.

To query port statistics, the two MIB tables need to be available on networking devices

IfTable (1.3.6.1.2.1.2.2)

IfXTable(1.3.6.1.2.1.31.1.1): IfXTable provides 64 bits counters, which are needed for port speed of 1G or higher.

User can use the commands below verify if the two MIB tables are available on the networking device.

For SNMP v2:

```
snmptable -v 2c -c public 192.168.0.1 ifTable
snmptable -v 2c -c public 192.168.0.1 ifXTable
```

For SNMP v3:

```
snmptable -v3 -l authPriv -u username -a [SHA|MD5] -A AuthString -x [AES|DES] -
X PrivString 192.168.0.1 ifTable
snmptable -v3 -l authPriv -u username -a [SHA|MD5] -
A AuthString -x [AES|DES] -X PrivString 192.168.0.1 ifXTable
```

To query the connected VMs on a target networking device, at least one of the following two MIB table has to be available.

dot1dTpFdbTable (1.3.6.1.2.1.17.4.3.1)

dot1qFdbTable (1.3.6.1.2.1.17.7.1.2.1)

User can use the commands below verify if the two MIB tables are available on the networking device.

For SNMP v2:

```
snmptable -m +BRIDGE-MIB -v 2c -c public 192.168.0.1
dot1dTpFdbTable
snmptable -m Q-BRIDGE-MIB -v 2c -c public 192.168.0.1
dot1qTpFdbTable
```

For SNMP v3

```
snmptable -v3 -l authPriv -u username -a [SHA|MD5] -
A AuthString -x [AES|DES] -
X PrivString 192.168.0.1 dot1dTpFdbTable
snmptable -v3 -l authPriv -u username -a [SHA|MD5] -
A AuthString -x [AES|DES] -
X PrivString 192.168.0.1 dot1qTpFdbTable
```