Configuration Guide for Network Device Monitoring

Table of Contents

Introduction

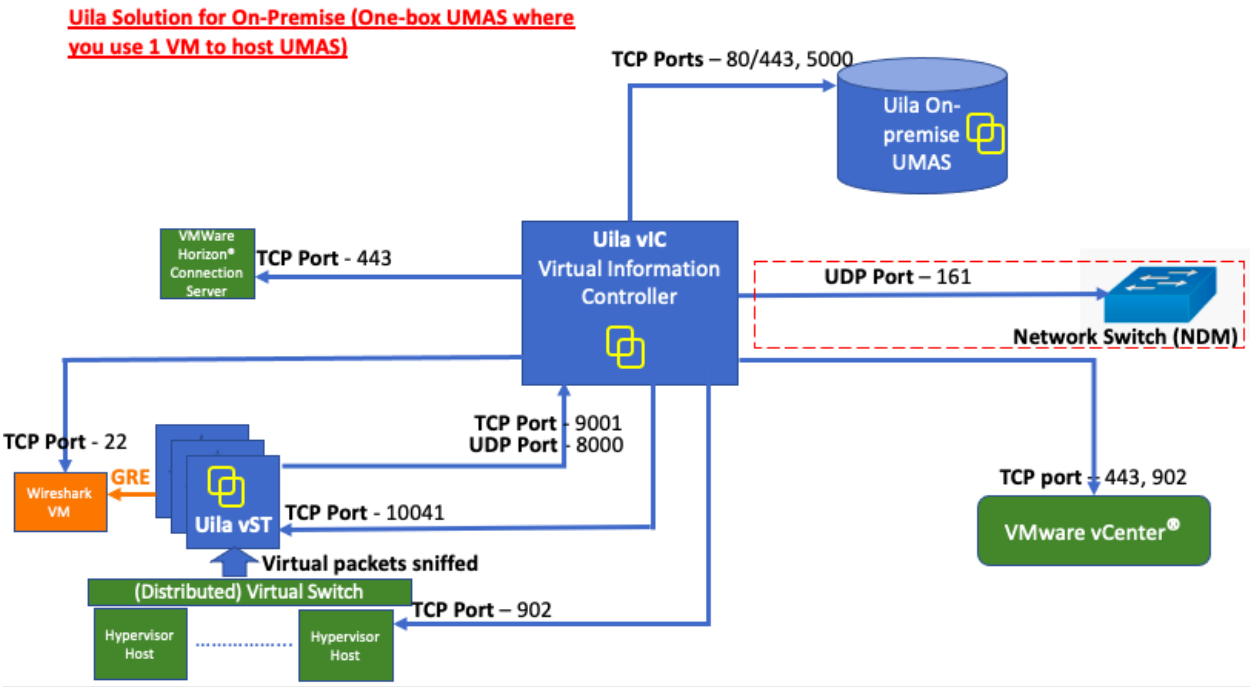
Scope and Purpose

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”

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 4 cores	2 cores 4 cores	4GB 24GB	8GB	8GB 24GB	16GB
medium	2 cores 4 cores	4 cores 4 cores	8GB 32GB	12GB	8GB 24GB	16GB
large	2 cores 4 cores	4 cores 4 cores	16GB 48GB	20GB	8GB 24GB	16GB

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

Applying NDM License

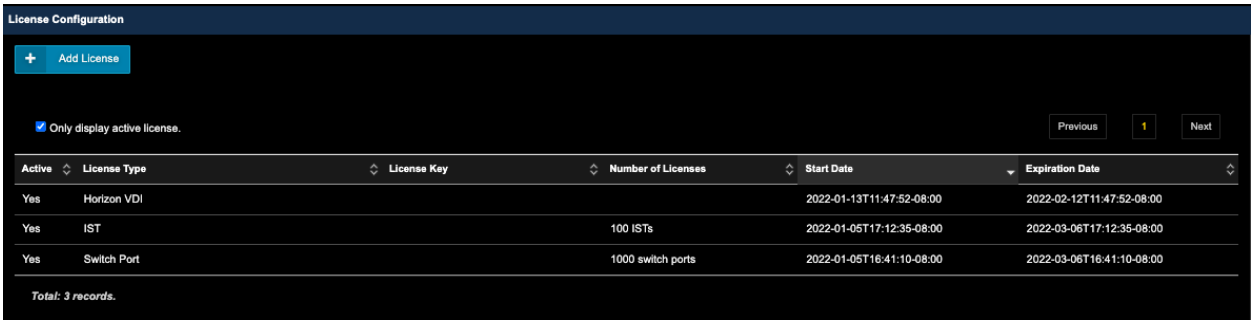
For Uila portal user, the NDM license will be applied and activated by Uila.

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.



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

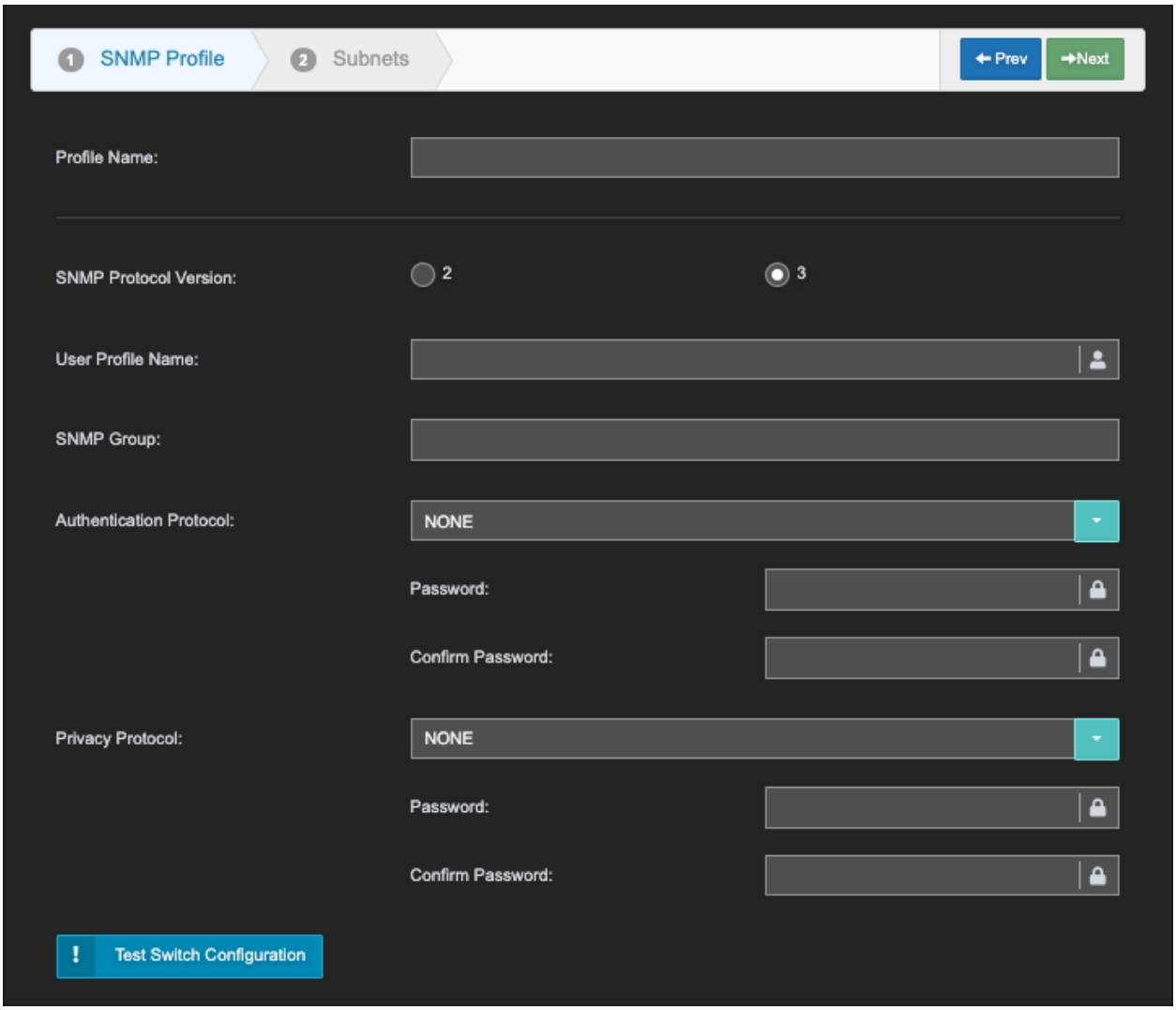
Then Log in to Uila as the primary administrator.

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.



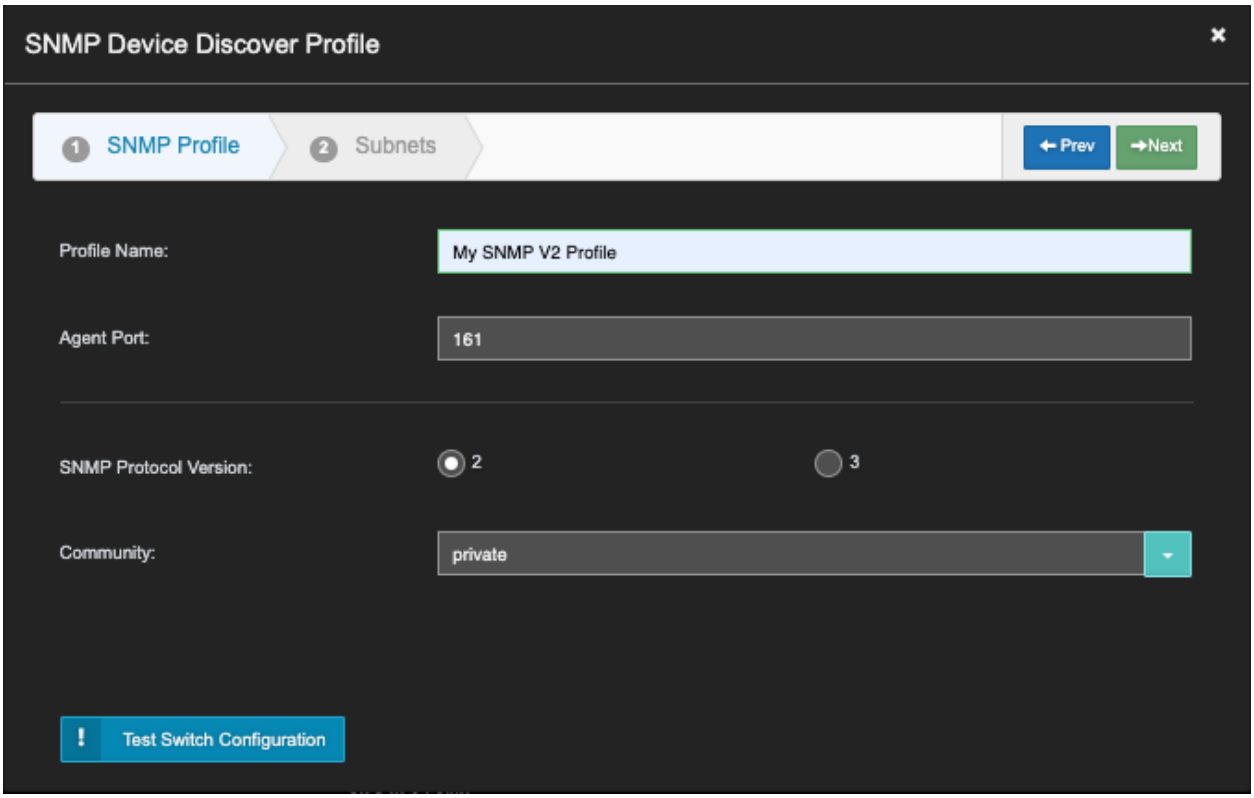
If you use SNMP Protocol Version 2, Select 

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

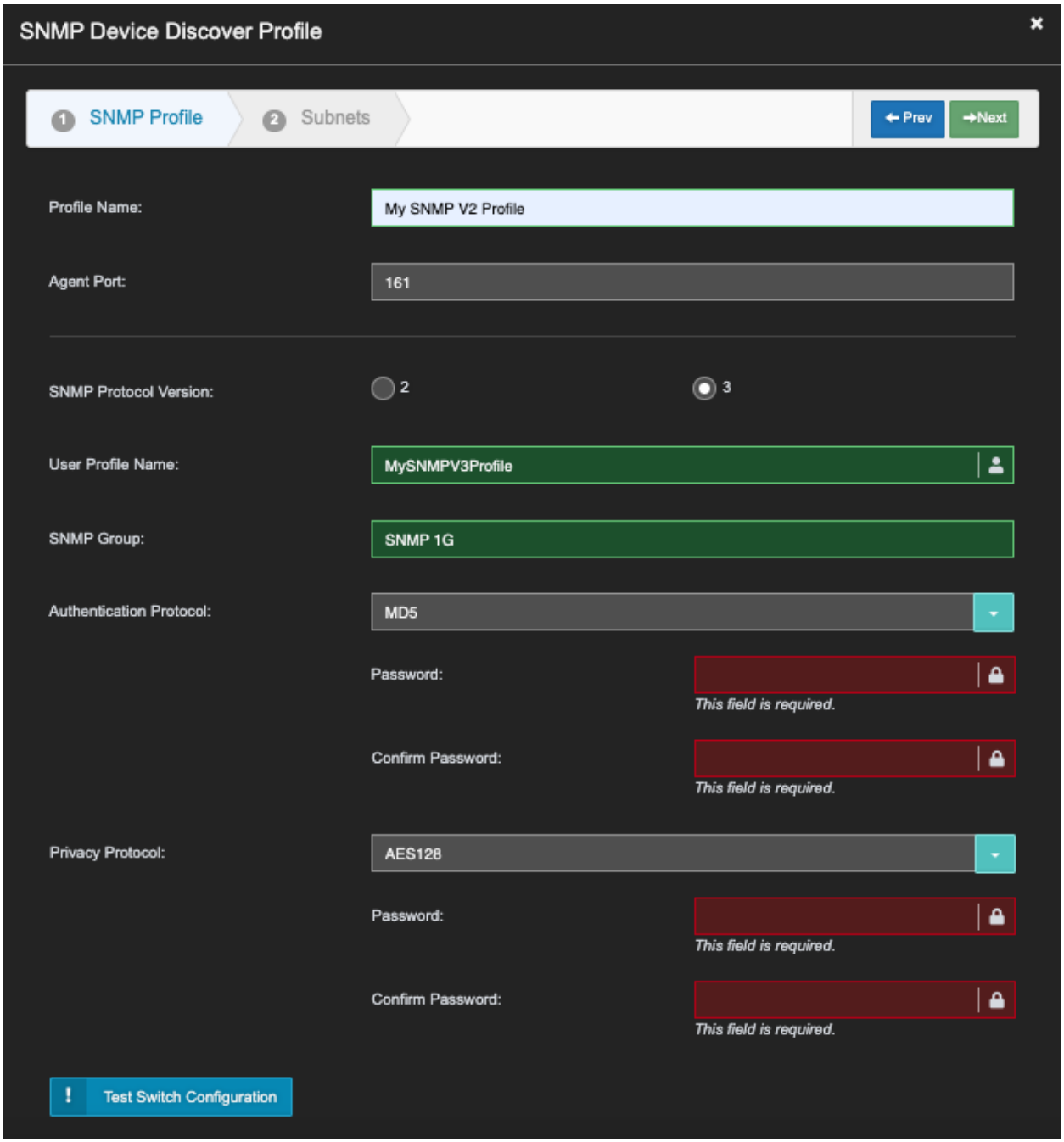
Community string. Click the dropdown list for "public" or "private"



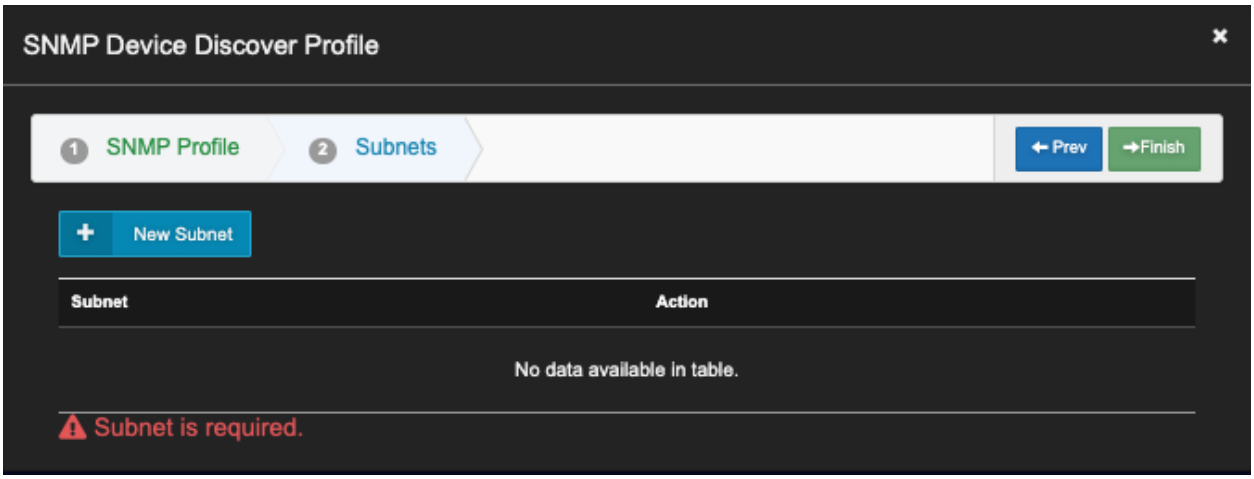
If you use SNMP Protocol Version 3, Select 

Fill in the following:

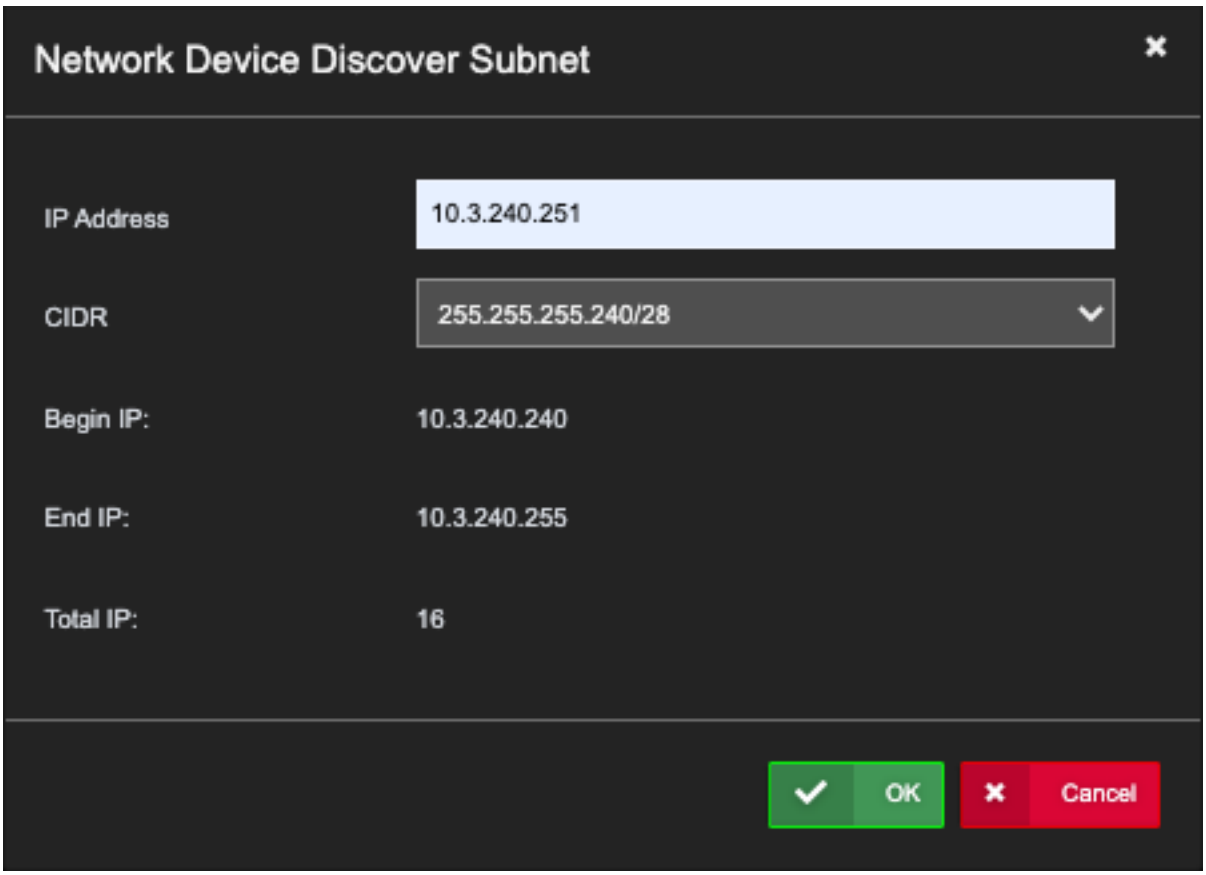
User Profile Name	SNMP User name. No duplicated name supported if there is more one (1) profile are created.
SNMP Group	Enter the SNMP Group.
Authentication Protocol and Password	Select the Authentication protocol and password. The supported protocols: NONE, MD5, SHA
Privacy Protocol and Password	Select 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:
My SNMP V2 Profile
Agent Port:
161
SNMP Protocol Version:
2
3
User Profile Name:
MySNMPV3Profile
SNMP Group:
SNMP 1G
Authentication Protocol:
MD5
Password:
This field is required.
Confirm Password:
This field is required.
Privacy Protocol:
AES128
Password:
This field is required.
Confirm Password:
This field is required.
Test Switch Configuration

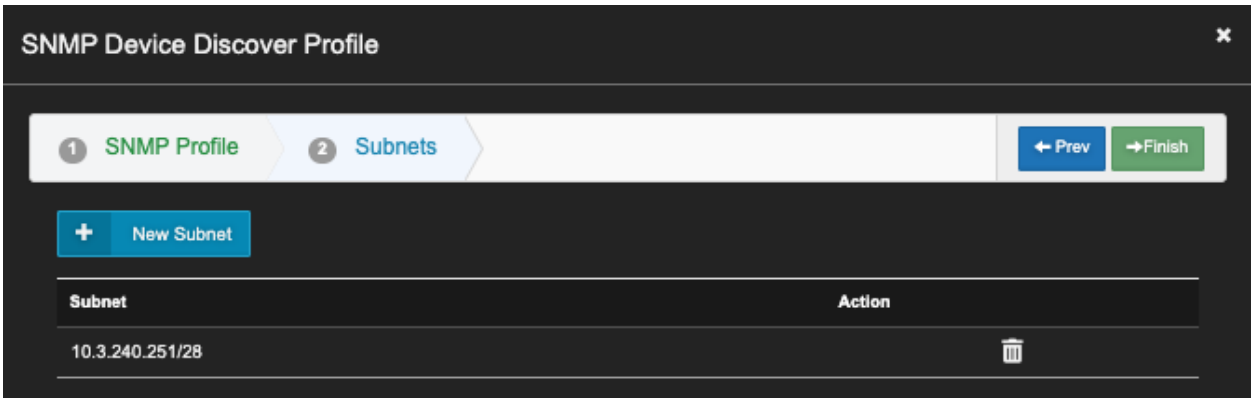
Click Next



Click New Subnet

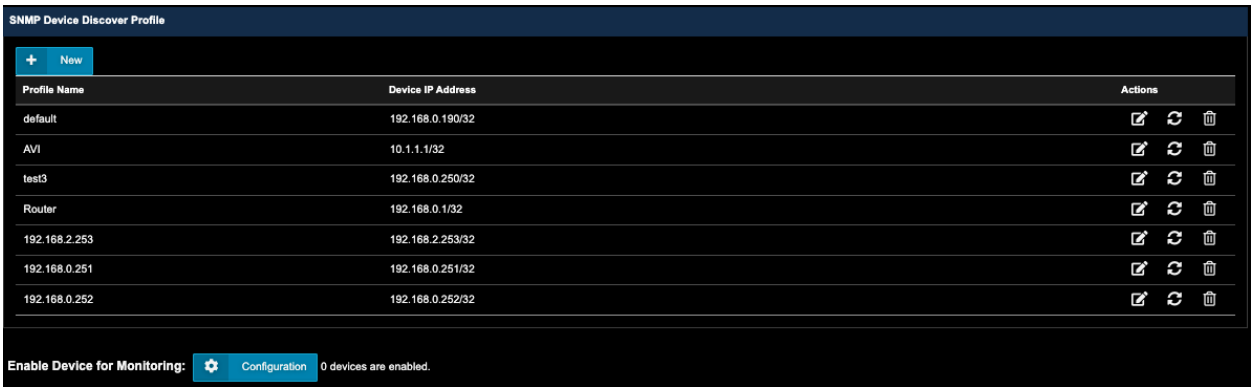


Enter IP Address and CIDR, Click OK.



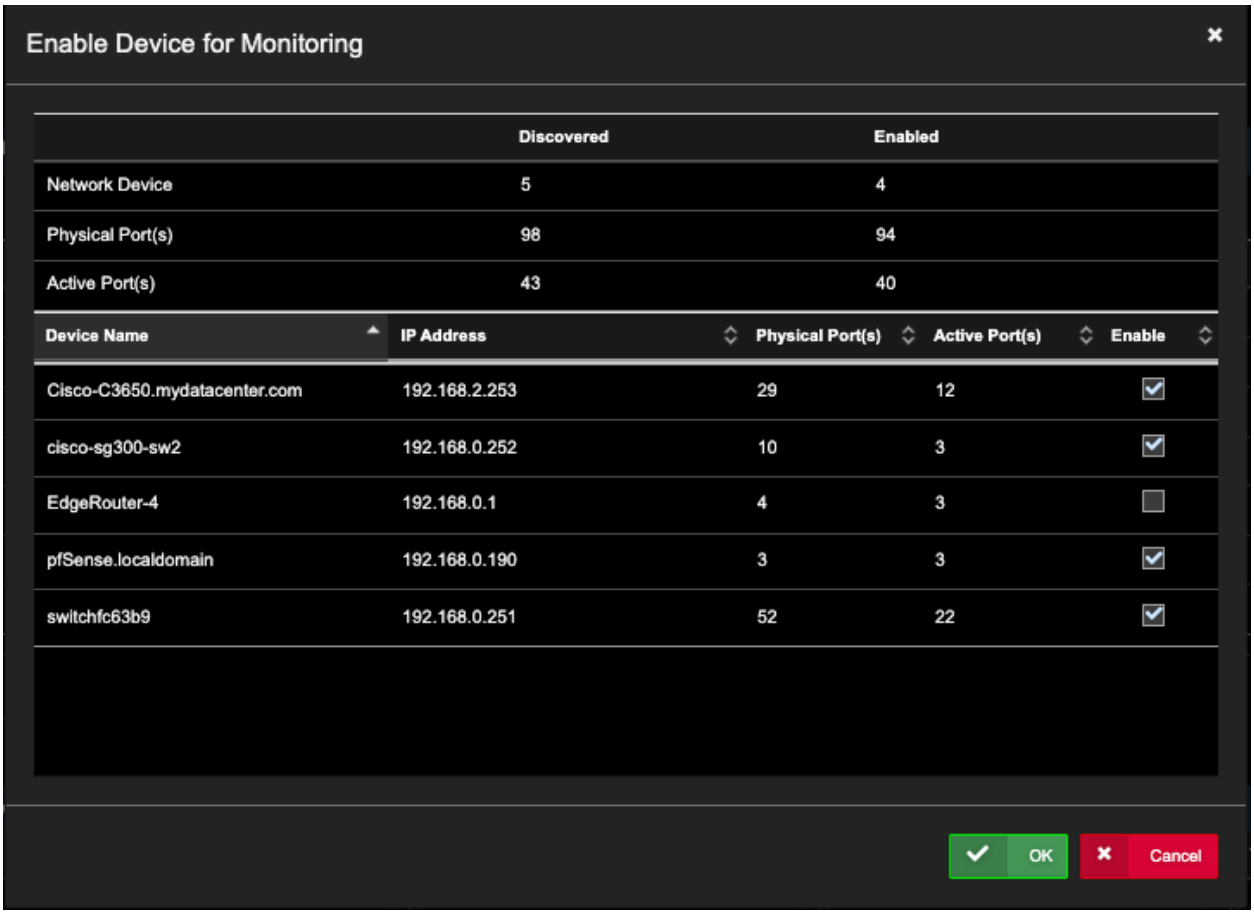
Click Finish to Complete the Setting.

Check The devices listed in the SNMP Device Discover Profile



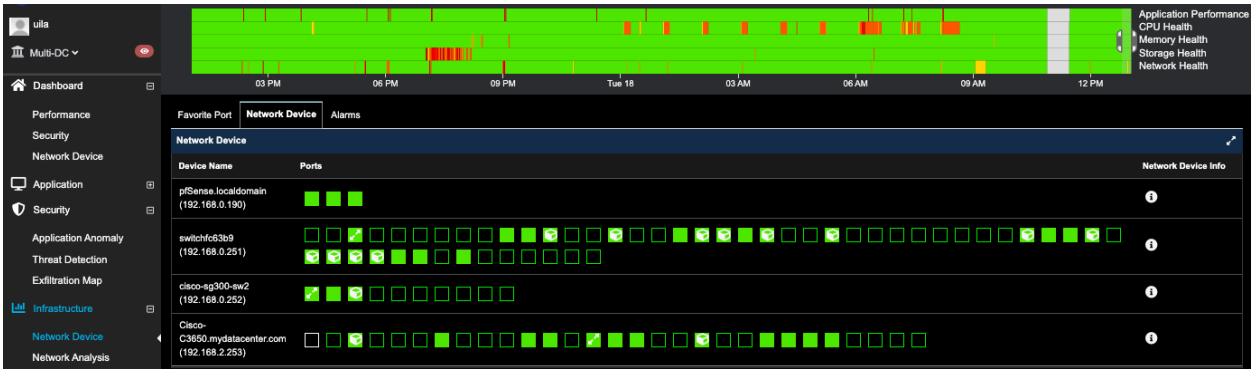
Next, Go to **Settings->Device Monitoring->Enable Device for Monitoring**, click on **Configuration.**

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



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.



uila

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.

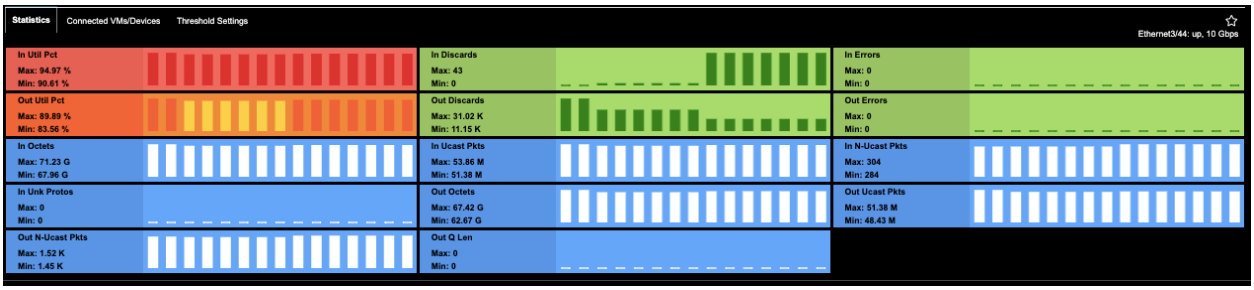
Threshold is defined as the % value that crosses the baseline.

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.

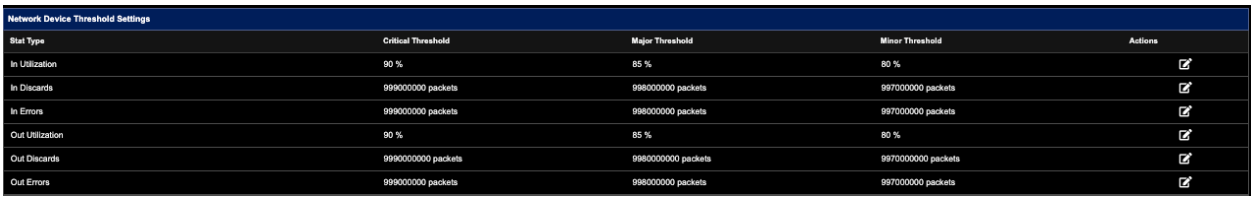
Delta from Baseline	Alarm Severity	Color
Less or equal to 5%	**Normal**	Green
Between 5% and 10%, including 10%	**Minor (1)**	Yellow
Between 10% and 20%, including 20%	**Major (2)**	Orange
Above 20%	**Critical (3)**	Red

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.



Device Port Icon Definitions

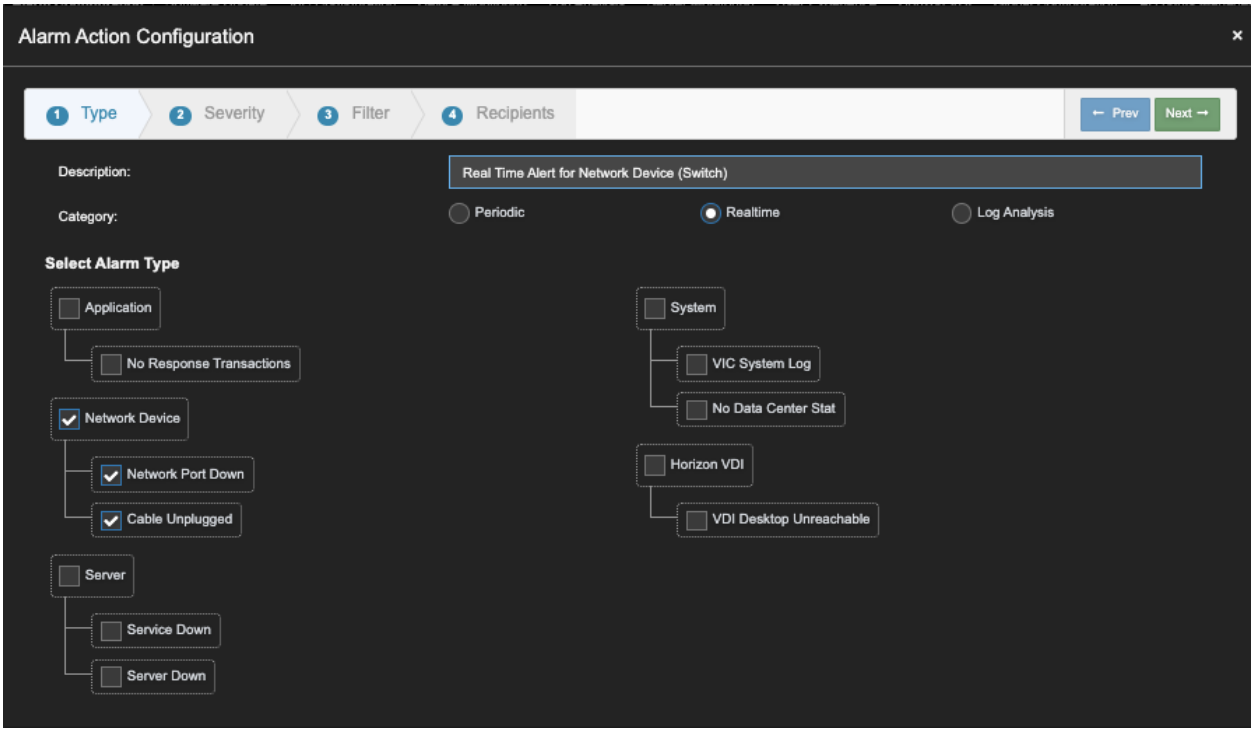
	A server is attached to this port
	Cross link to another network switch or router
	A device is connected
	Open port – no device connected
	Port Statistics are above Normal values

Creating Alert for Network Devices

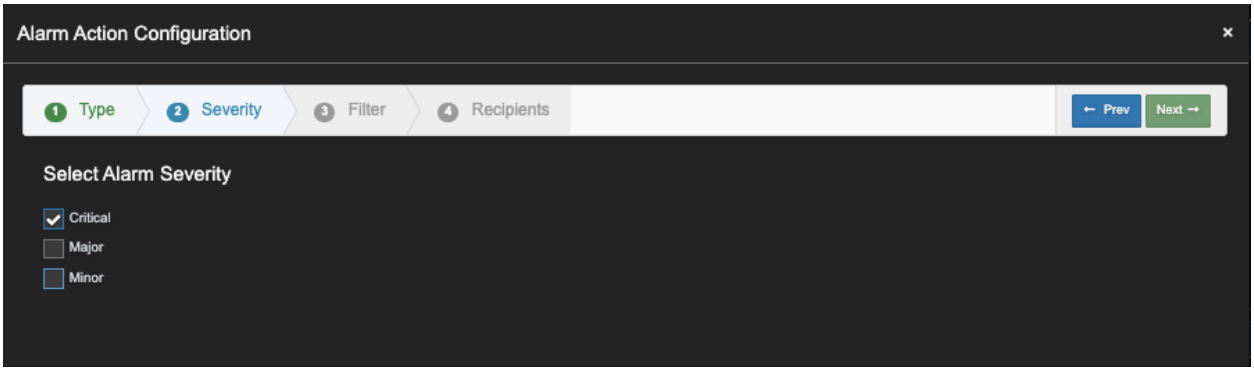
Device Port Down or Cable Unplugged

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

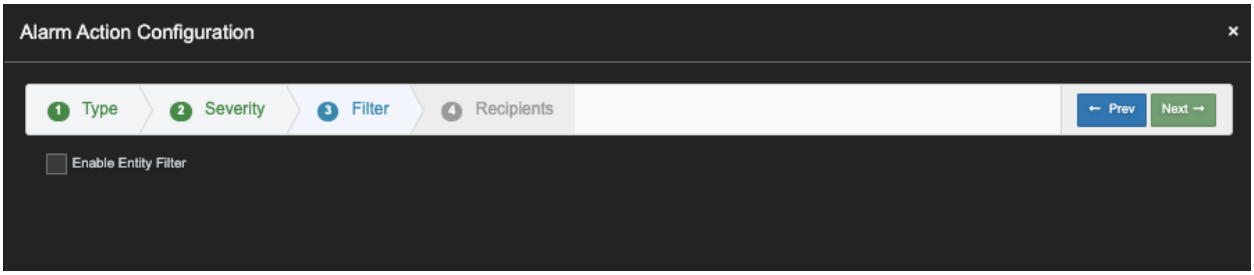
   Check 'Realtime'. Select 'Network Device' only. **Note**: Do not Select other Alarm type.



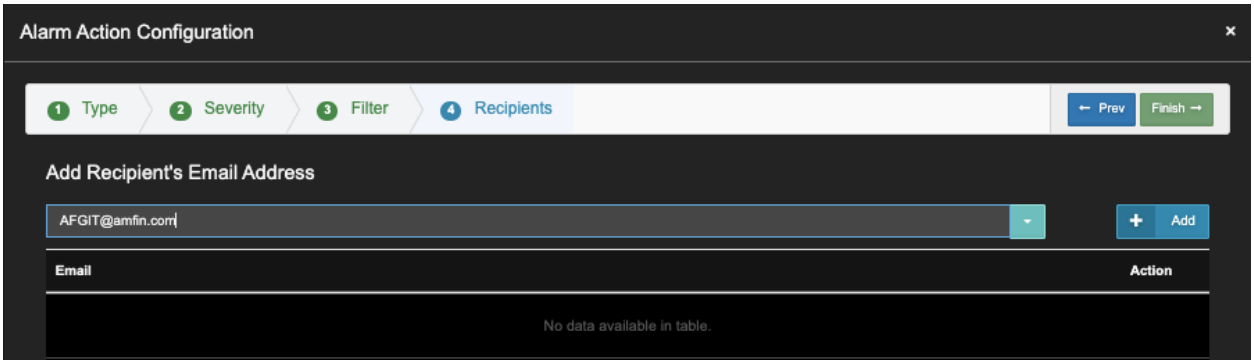
2. Select Alarm Severity to 'Critical', Click 'Next'.



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'.



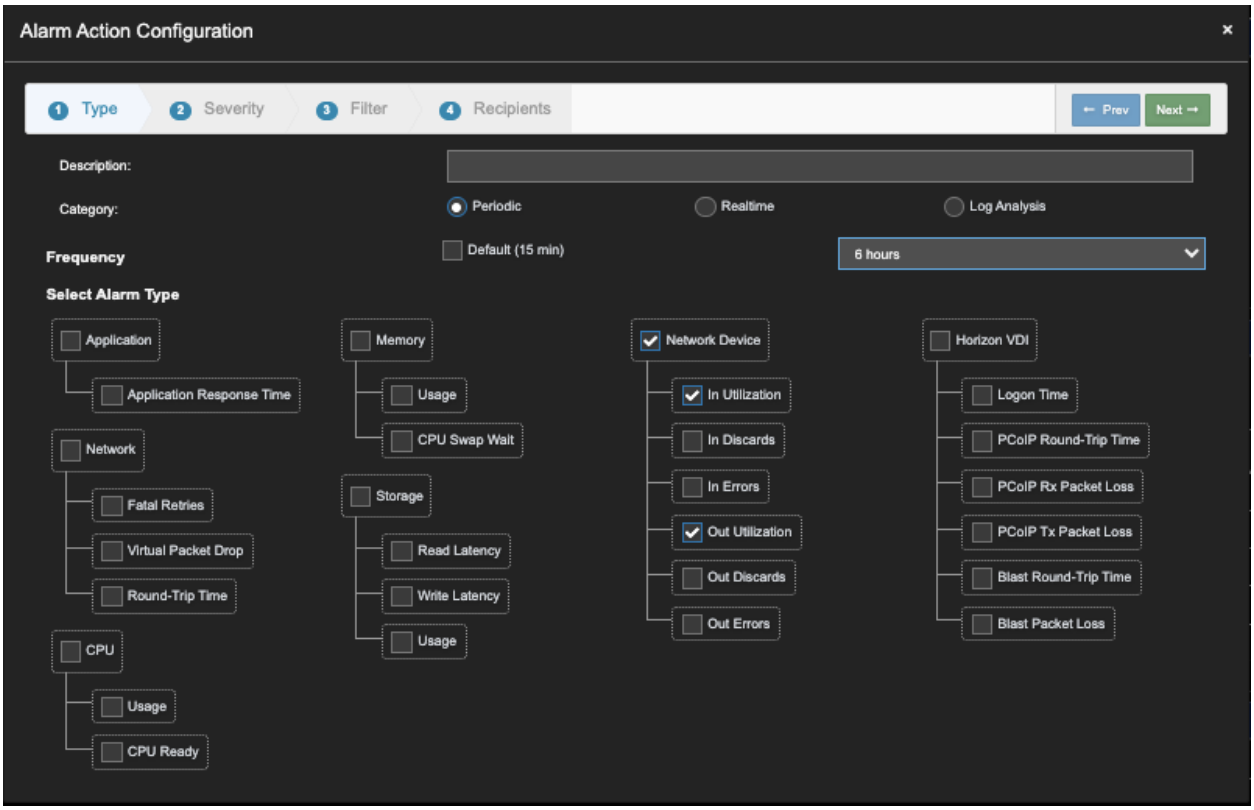
4. Add email address of the alert recipient(s). Click 'Finish'.



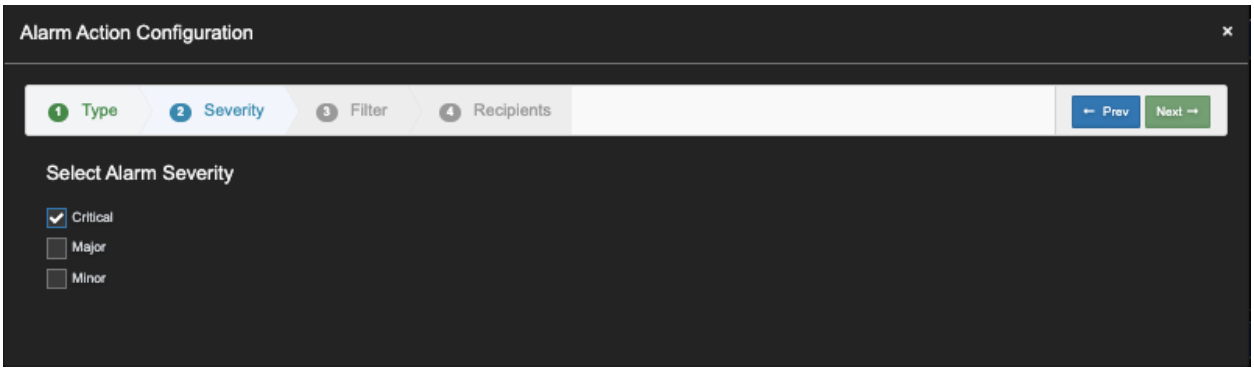
Ports in High Utilization Rate, # of Discard Packets, or # of Error Packets

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

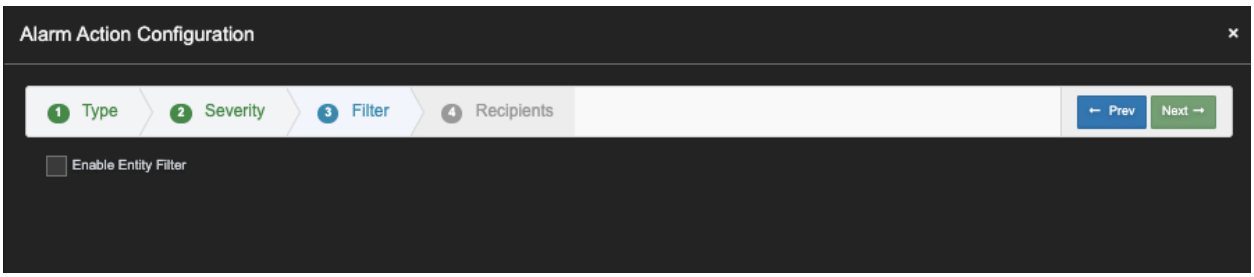
Check 'Period'. Select Frequency; 15 min, 1 hour, 3 hours, 6 hours, 12 hours or 24 hours. Select the type of statistics wish to be alerted. Click 'Next. **Note**: Do not Select other Alarm type.



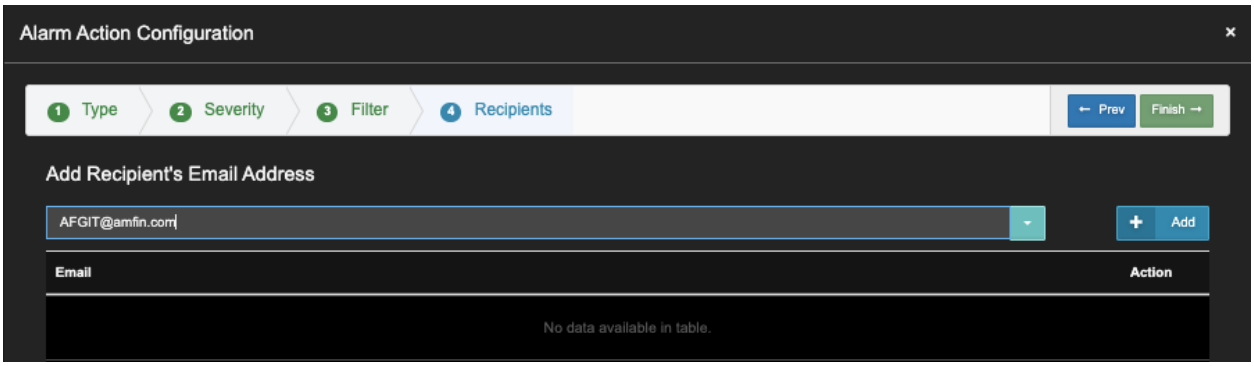
2. Select Alarm Severity, Click ‘Next’



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’.



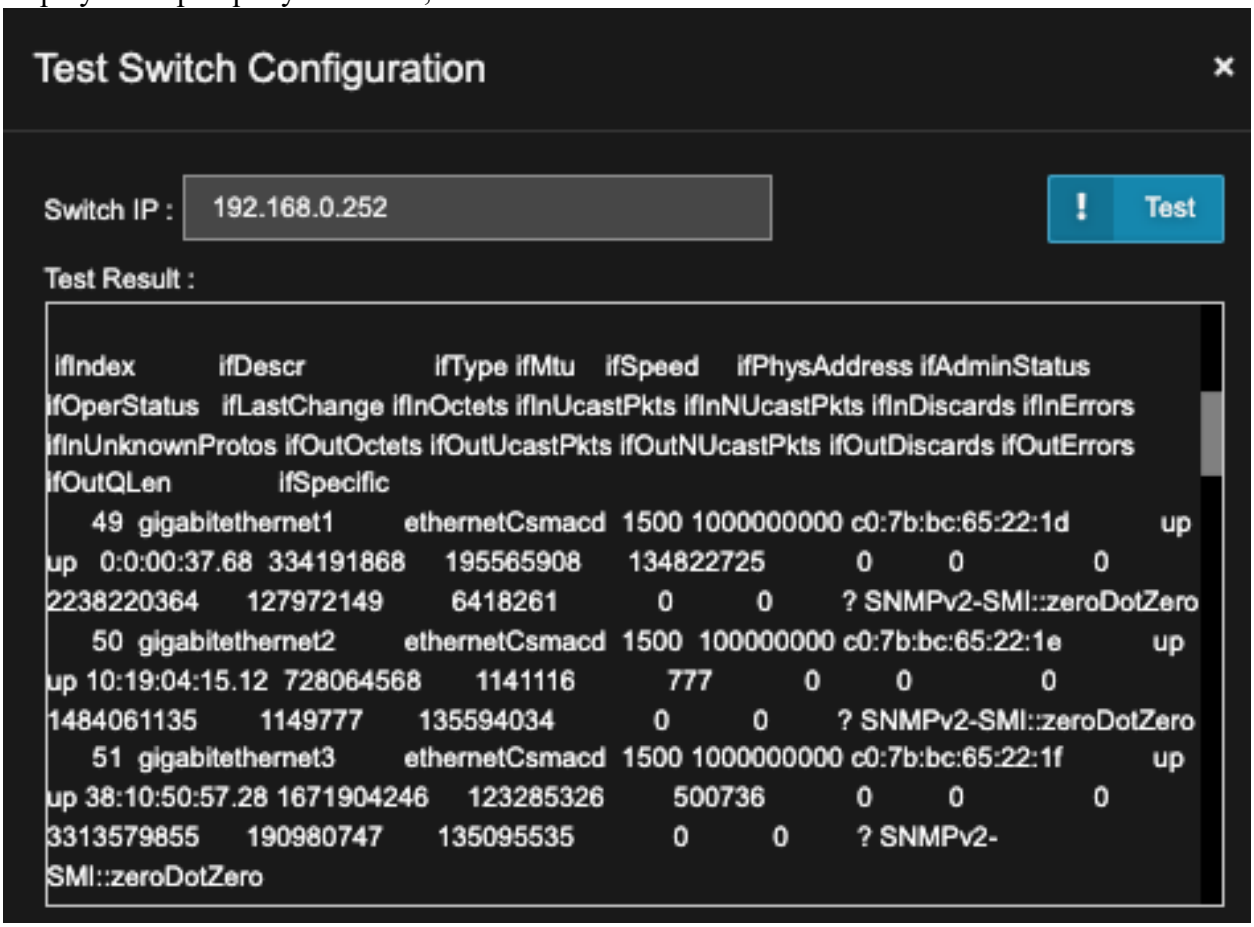
4. Add email address of the alert recipient(s). Click ‘Finish’.



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.



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
```