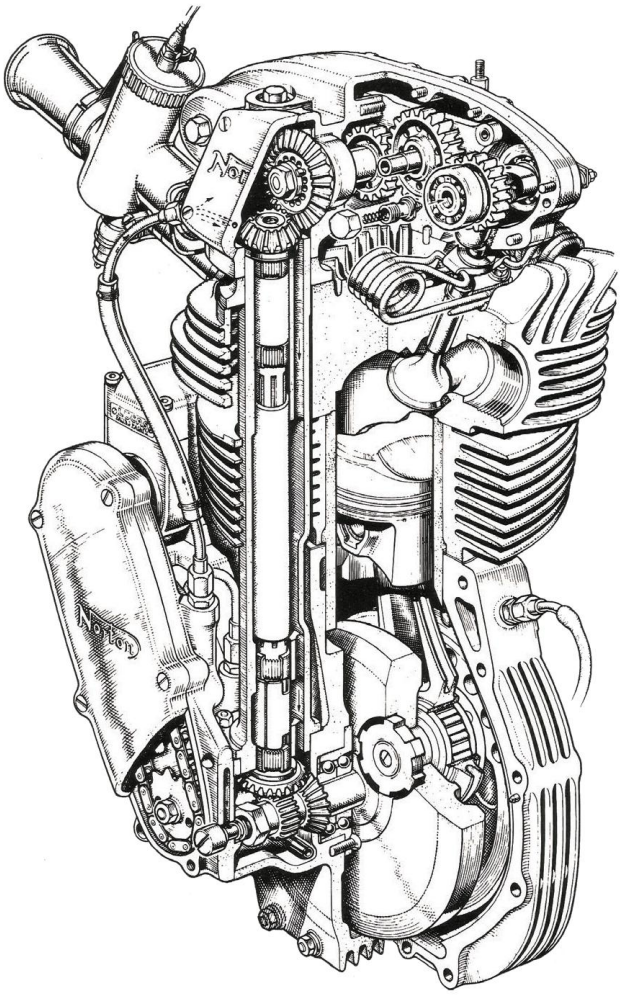
ARGENT®



Argent Omega for SNMP

www.Argent.com

GC33-4001-1

TABLE OF CONTENTS

Introduction

In today's complex network of switches, routers, and servers, managing all these devices is a challenging task – the network sooner or later encounters issues and slows down. It is critical for system administrators to monitor the entire network closely and to see the network as a whole, not just as single devices.

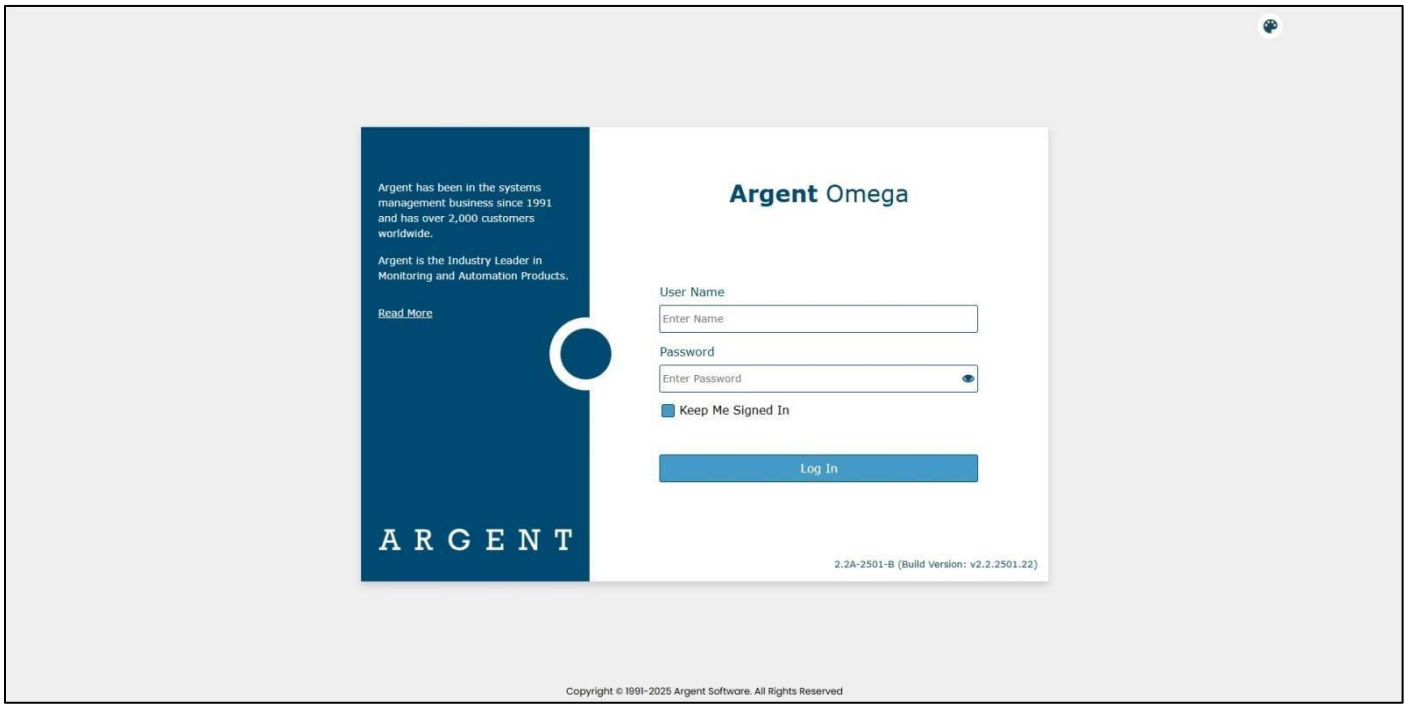
Network devices support the network management protocol, sharing management information. There are various protocols available to support network management, including the popular Simple Network Management Protocol (SNMP) that comes pre-bundled with SNMP agents for most network devices.

SNMP is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).

Argent Omega for SNMP communicates with all devices, allowing network administrators to track network performance, diagnose and manage network faults, and plan network capacity and growth.

Argent Omega for SNMP Tool Sets provide Instant Best Practices for monitoring SNMP-compliant devices. Both sides of SNMP are supported by proactively checking SNMP statistics while also listening for SNMP Traps. All SNMP-enabled devices or applications, such as bridges, hubs, switches, routers, network servers, power supplies, and environmental controls, can be monitored.

Log-On Screen



Argent Omega validates the authenticity of the user through Log-on screen.

Three types of user accounts can be logged into Argent Omega:

- Windows User Accounts
- Argent Demo Accounts
- Argent Internal Accounts

Argent Omega uses Windows authentication to login Windows user accounts. If the Argent server is in Active Directory Domain environment, then users are authenticated by Active Directory. If the machine is Standalone or Workgroup, local Windows user authentication is used. **To use Windows user accounts, a better approach is to create a separate user group for Windows users and assign the required rights.**

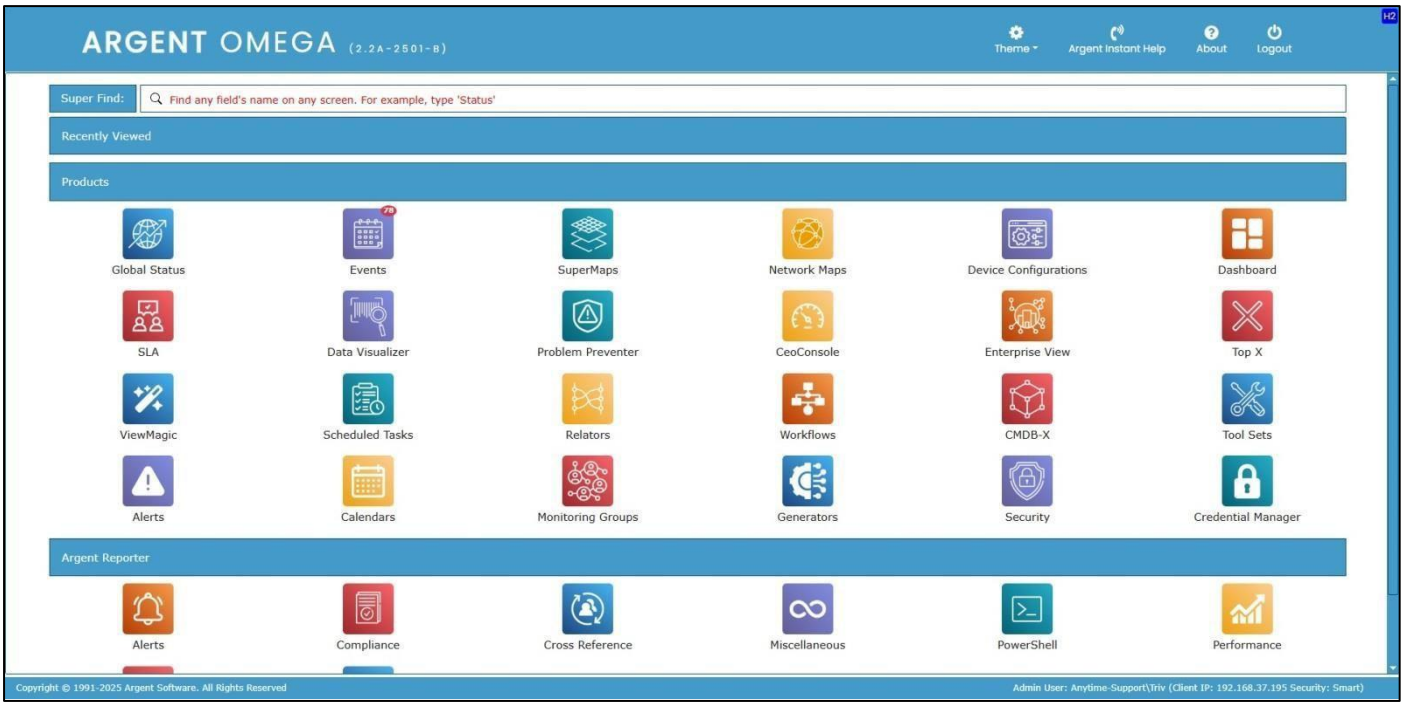
Argent Demo Accounts can be created in the Argent Omega Security section and are used for demonstration purposes. These are read-only accounts and use Argent private authentication to login to Argent Omega. Usually, Argent Demo Accounts are used for a few days or weeks and the access is limited to specific IP addresses.

Argent Internal Accounts also can be created in Argent Omega Security section, and behave like normal Windows accounts. It uses Argent private authentication for login.

Argent Omega username is case **insensitive** and Password is **case sensitive**.

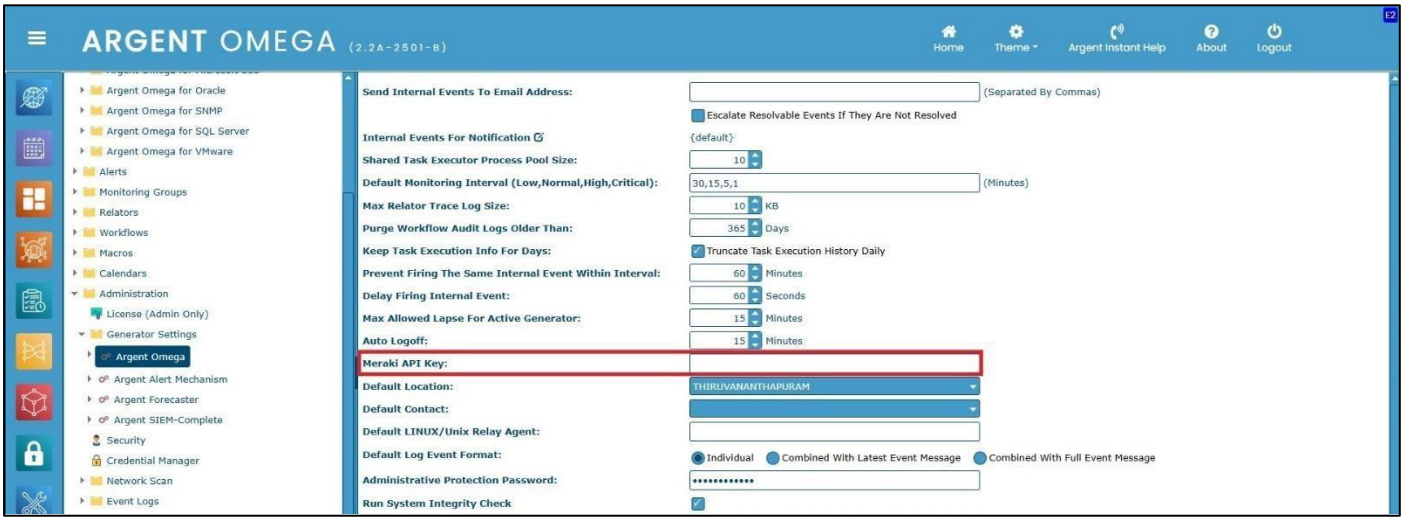
Home Screen

After login, Argent Omega redirects to Home screen, shown below **(note the very useful Super Find):**



Meraki Prerequisites

To use the Meraki feature, the Meraki API key is specified in the Argent Omega settings under **Generator Settings**. Meraki is a cloud-based management protocol for Cisco wireless access points (APs). A common use case is identifying the current wireless clients of a selected Meraki device.



CMDB-X

In the software industry, CMDB stands for Configuration Management DataBase. Argent added the 'X' for eXtensible.

A recent example highlighting the importance of this flexibility is a customer who added a custom field to their CMDB-X to track the license expiry of their firewall. By enabling custom fields, Argent CMDB-X allows customers to utilize it as a comprehensive **IT Asset Management** tool.

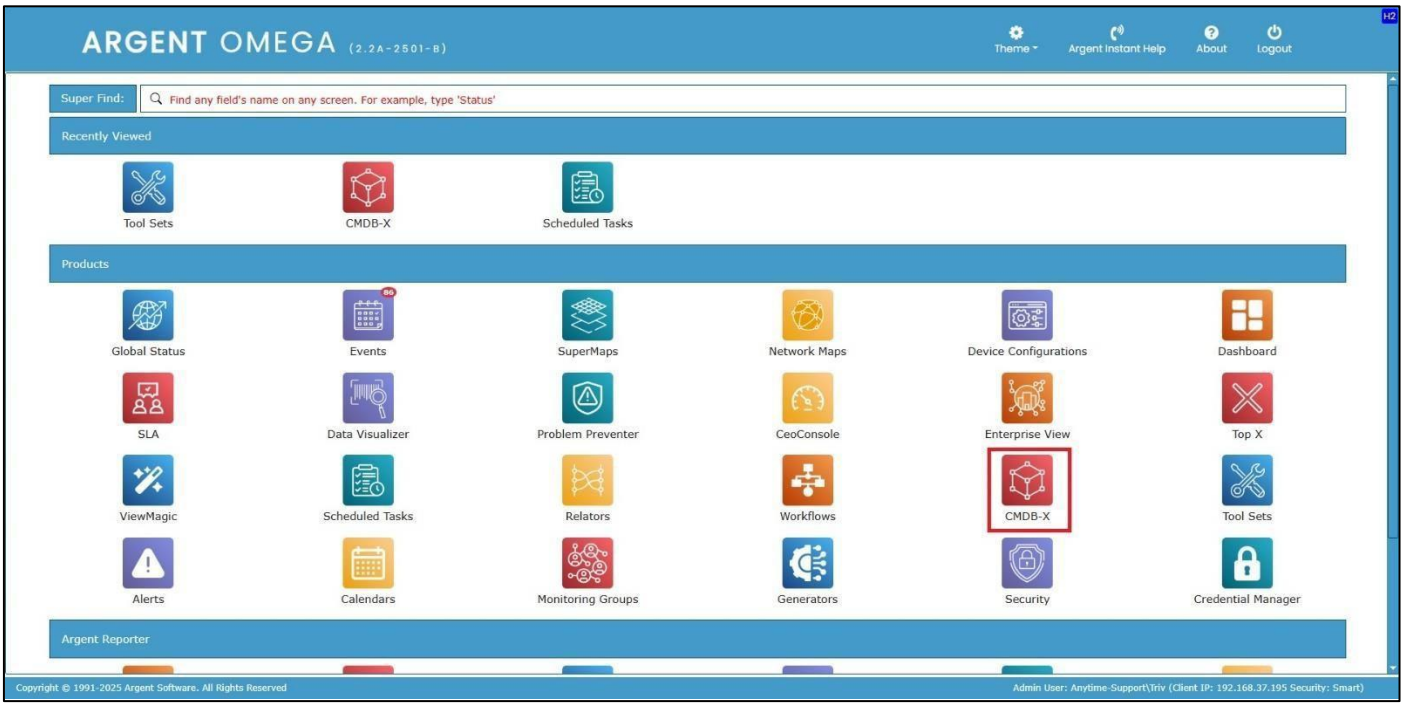
Argent CMDB-X provides an easy and streamlined way to manage all critical servers and devices, as well as all server and device properties and licensing, **all from a single screen.** Argent CMDB-X simplifies the process of adding multiple servers and devices in one batch – 11 or 77,000 -- license them to multiple Argent Omega Products and assign them to existing or new Locations and Network Groups, **all with a single click**.

Argent CMDB-X provides **complete network discovery** of all servers and TCP/IP devices using **Active Directory, Network Browser, ICMP Ping, Windows Cluster, and SNMP Discovery**.

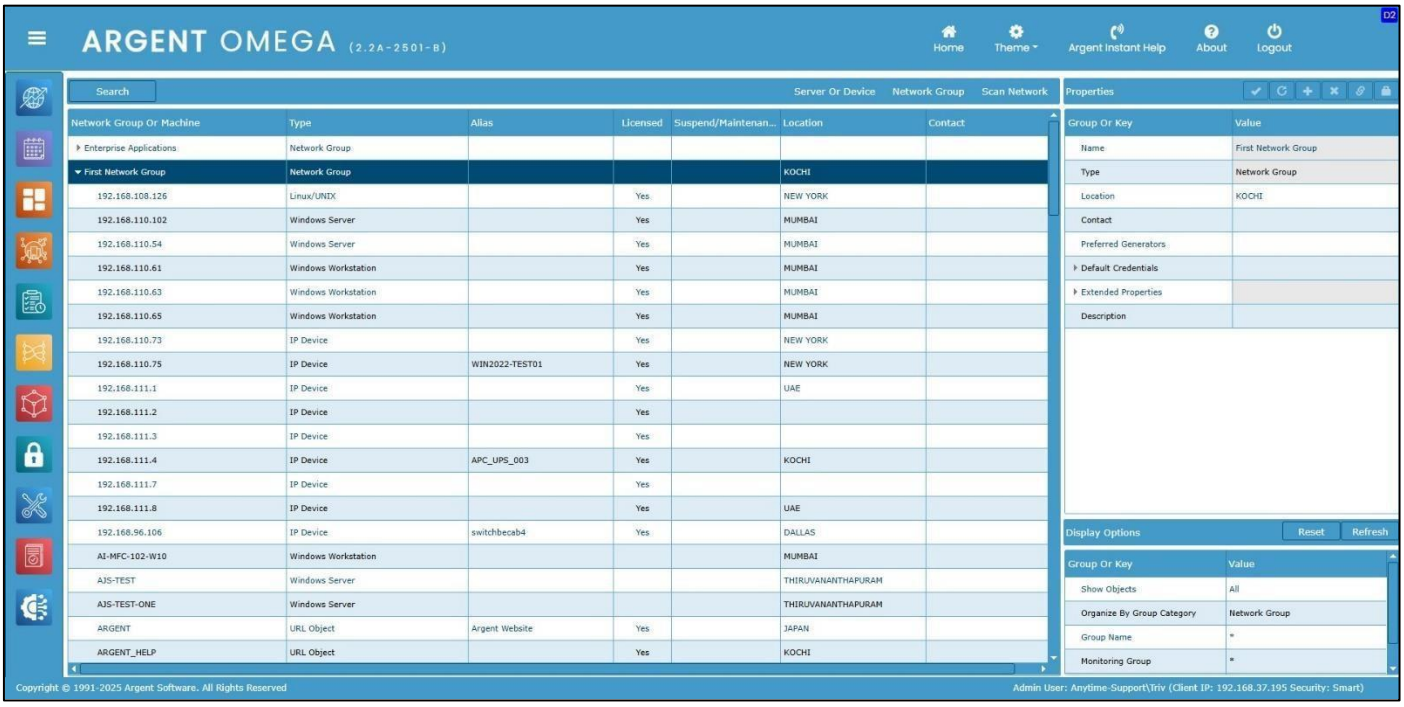
It also supports importing data from Excel files.

Additionally, Argent CMDB-X allows manual addition or removal of servers and devices, bulk licensing, and connectivity testing of monitored assets.

To access CMDB-X, select **'CMDB-X'** from the **Home Screen**:



The CMDB-X screen is shown below:

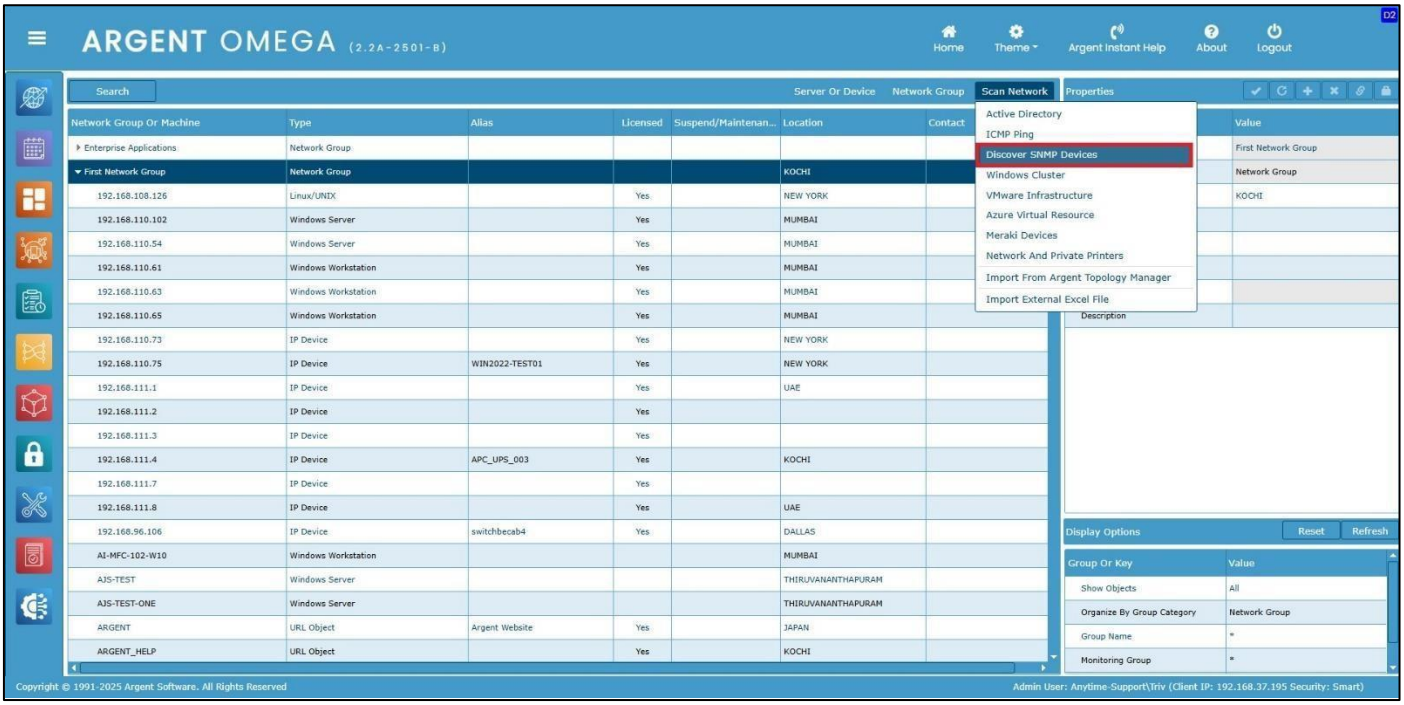


Argent Omega for SNMP supports monitoring the following types of servers and devices:

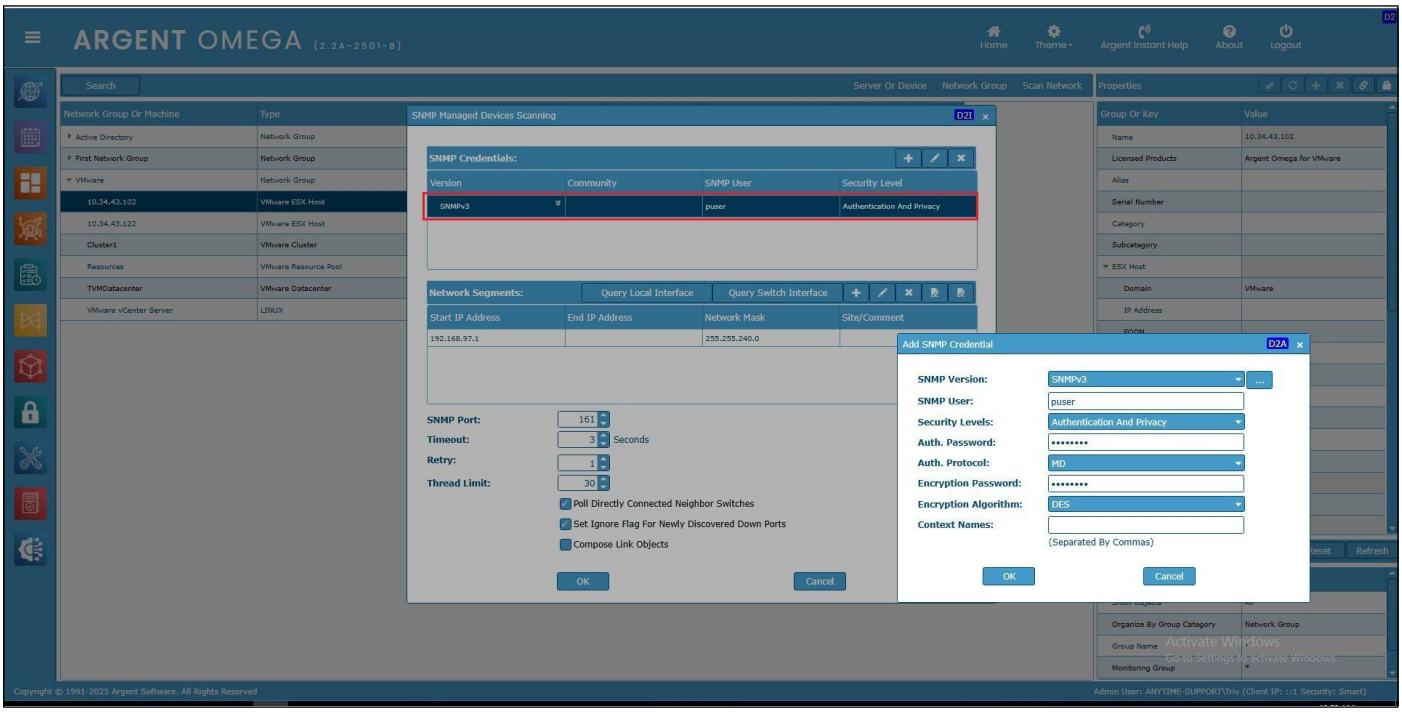
- IP Devices
- Linux
- Windows Server

To add SNMP-compliant devices to Argent CMDB-X, either use network scan option **Discover SNMP Devices**, or use **Manually Add Server/Device** context menu option.

For automatic discovery of SNMP devices, choose **Discover SNMP Devices** from **Scan Network** popup menu:



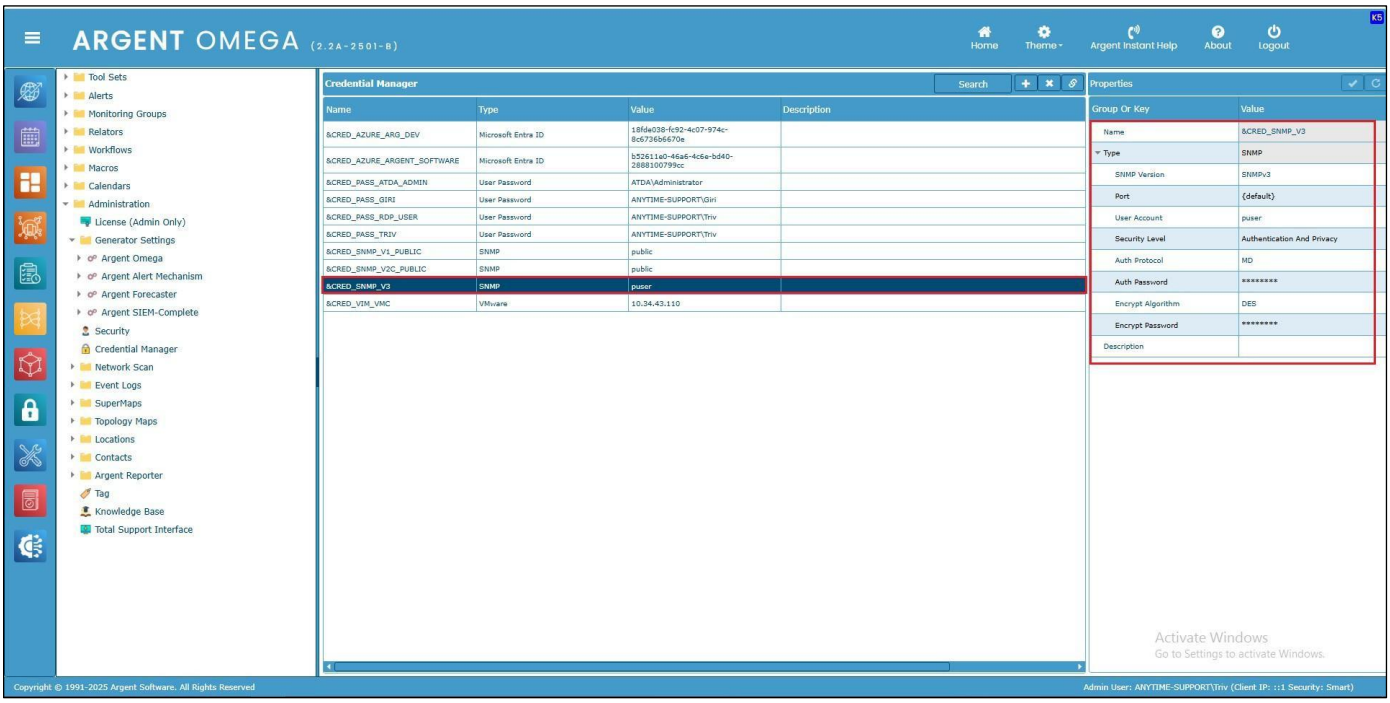
The following dialogs are displayed when asking the SNMP parameters to scan SNMP devices:



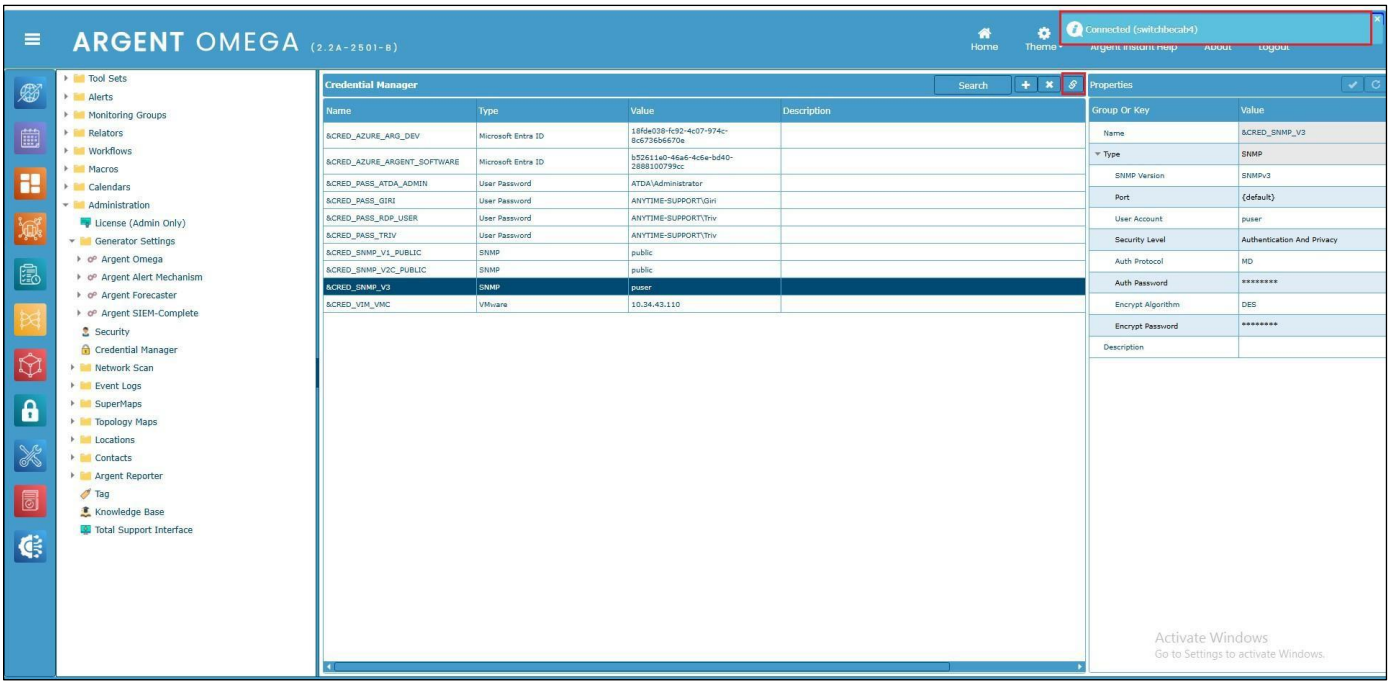
There are two ways to configure SNMP parameters:

- Directly specify the SNMP parameters in the above scan dialog.
- Configure the in the Credential Manager and specify the Credential in the scan dialog.

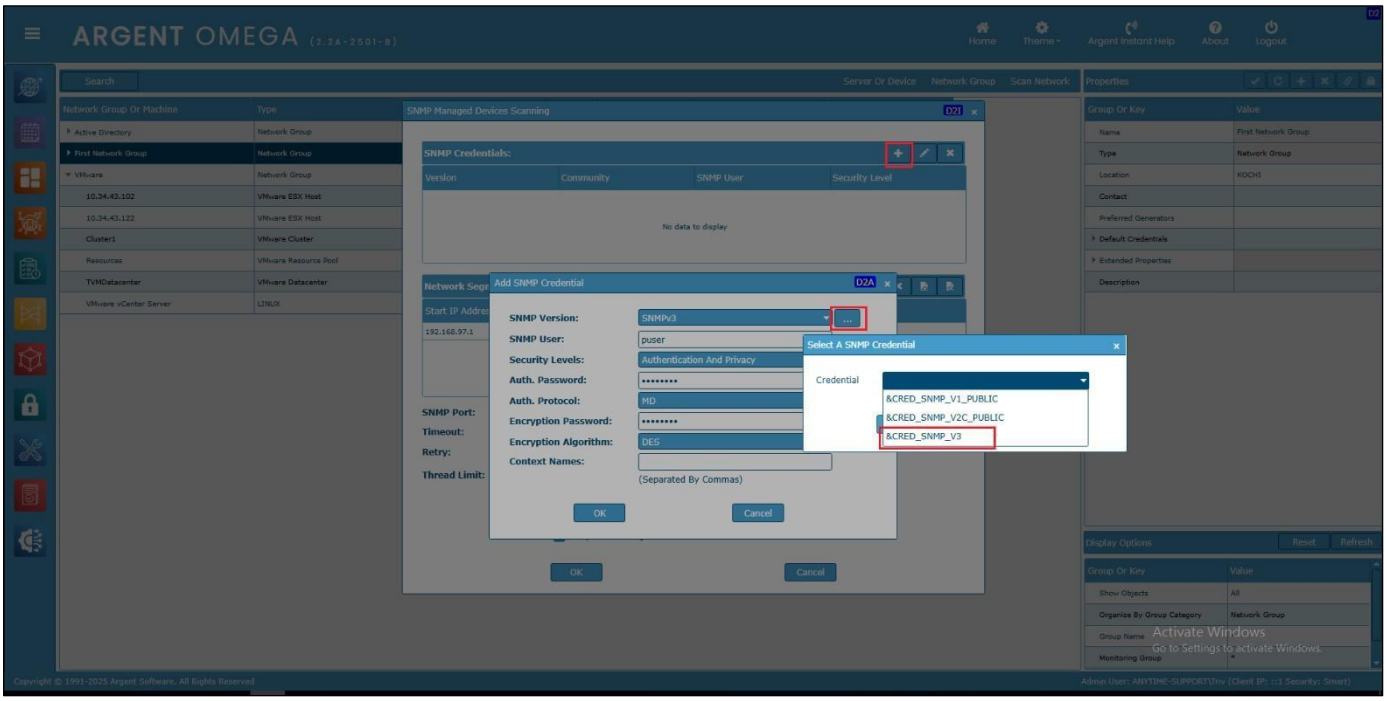
Configure SNMP credentials in Credential Manager:



Do the connectivity test of configured Credential:



Specify the Credential in scan dialog:



The following SNMP parameters should be configured:

SNMP Version:

Default value is SNMPv1. It can be SNMPv1, SNMPv2c or SNMPv3.

Community:

The Community string is like a user ID or password allowing access to a router or other device's statistics. SNMP community strings are used only by devices that support the SNMPv1 and SNMPv2c protocol and the default value is **public**.

SNMPv3 uses username/password authentication, along with an encryption key.

SNMP User (For SNMPv3 Only):

SNMPv3 username

Auth. Password (For SNMPv3 Only):

SNMPv3 authentication password

Auth. Protocol (For SNMPv3 Only):

SNMPv3 authentication protocol. It can be MD, SHA, SHA256, or SHA512

Encryption Password (For SNMPv3 Only):

SNMPv3 encryption password

Encryption Algorithm (For SNMPv3 Only):

SNMPv3 encryption algorithm. It can be DES, AES, 3DES, AES192, or AES256

Start IP Address:

IP address to start the scanning for SNMP devices

End IP Address:

IP address to serve as the end of the IP range to scan for SNMP devices

Network Mask:

Network mask

SNMP Port:

Default value is 161

Timeout:

Timeout in seconds, the range is 3 to 60. The default value is 3.

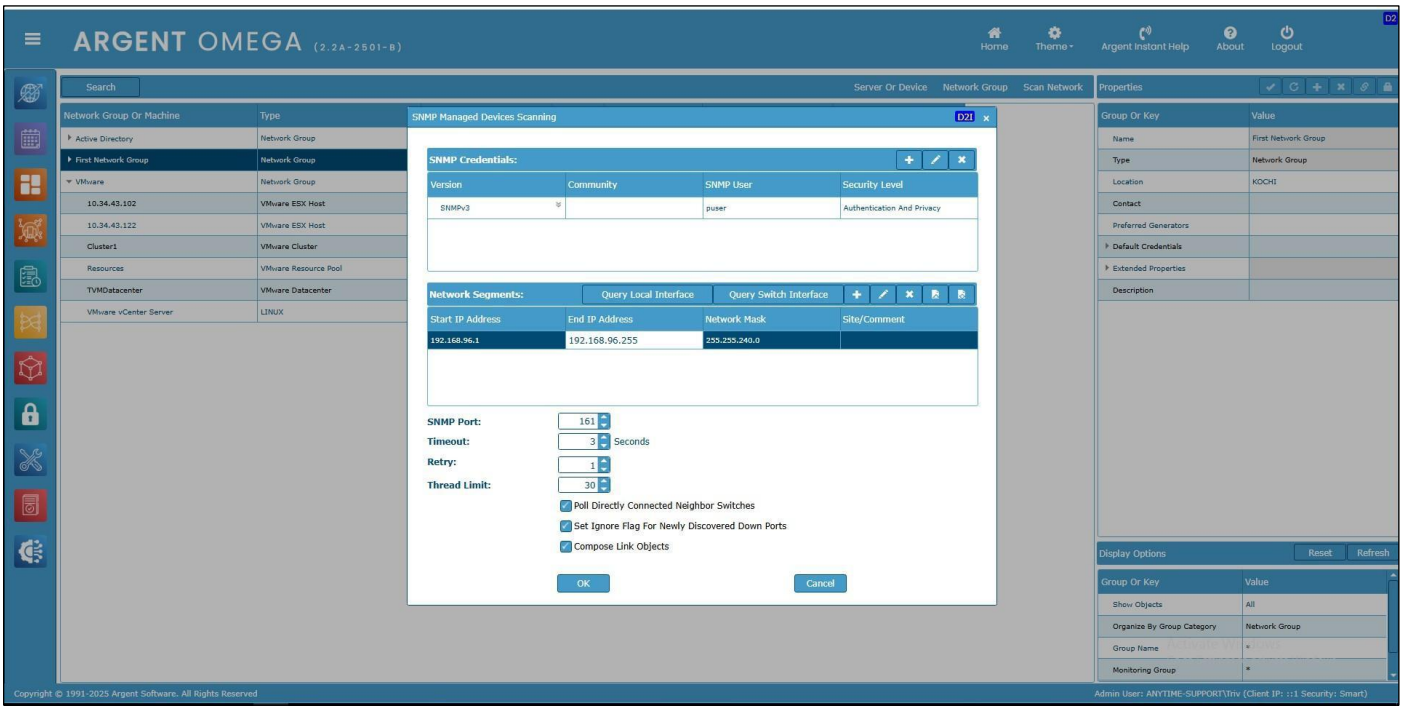
Retry:

The range is 1 to 10. The default value is 1.

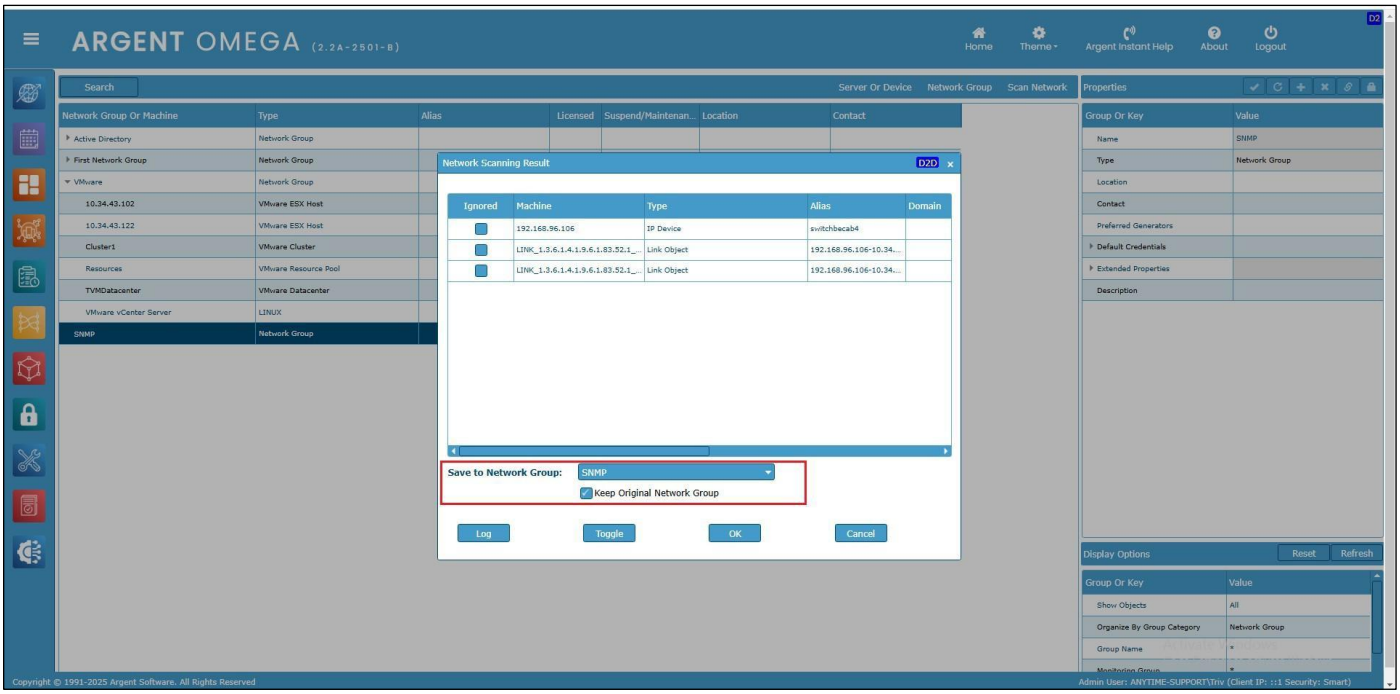
Thread Limit:

This is the thread pool size performing the SNMP scanning. The range is 1 to 100. The default value is 30. Check **Poll Directly Connected Neighbor Switches** option to query neighbor switches connected to the switch.

Press OK button to scan the network for SNMP devices using specified parameters:



The scanning results are shown in a list box as below:



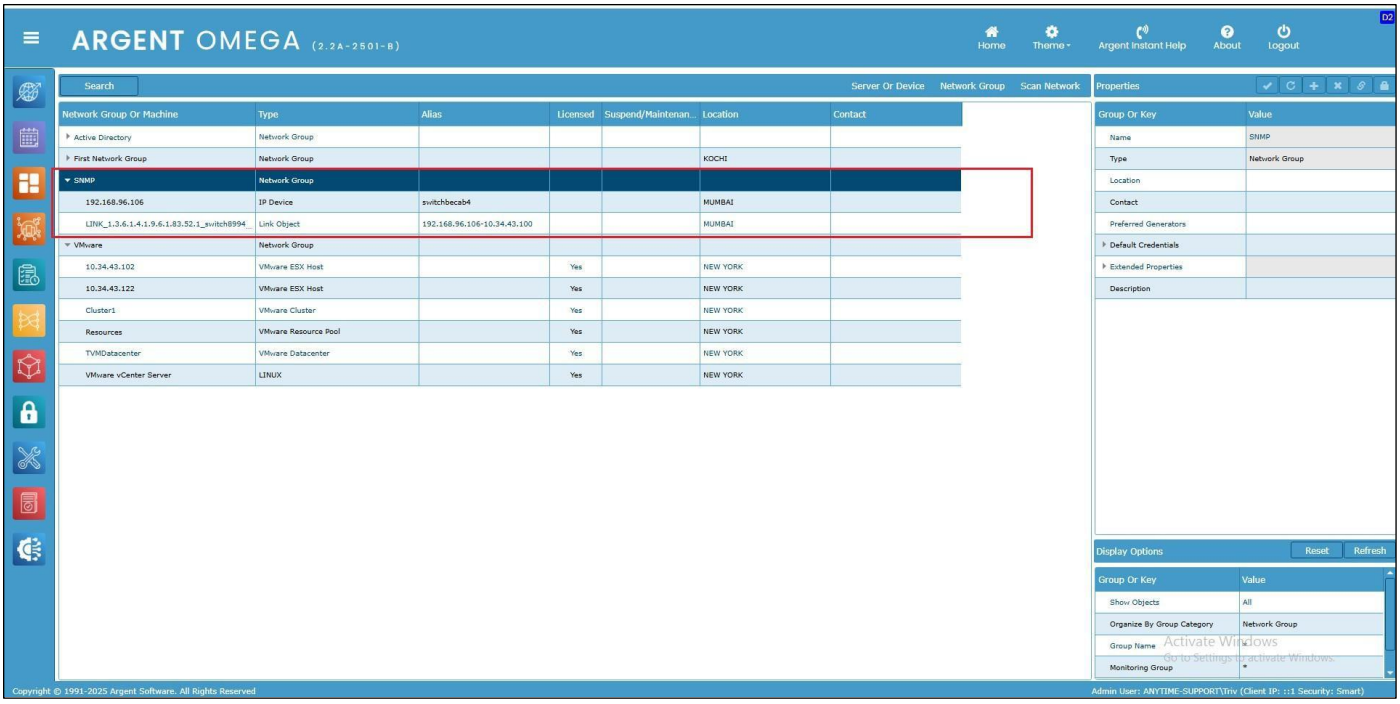
Press OK button to add the scanned devices under specified Network Group in CMDB-X.

Use **Save To Network Group** combo box to select the Network Group.

It is possible to skip the saving of specific devices by checking **Ignored** check box in list.

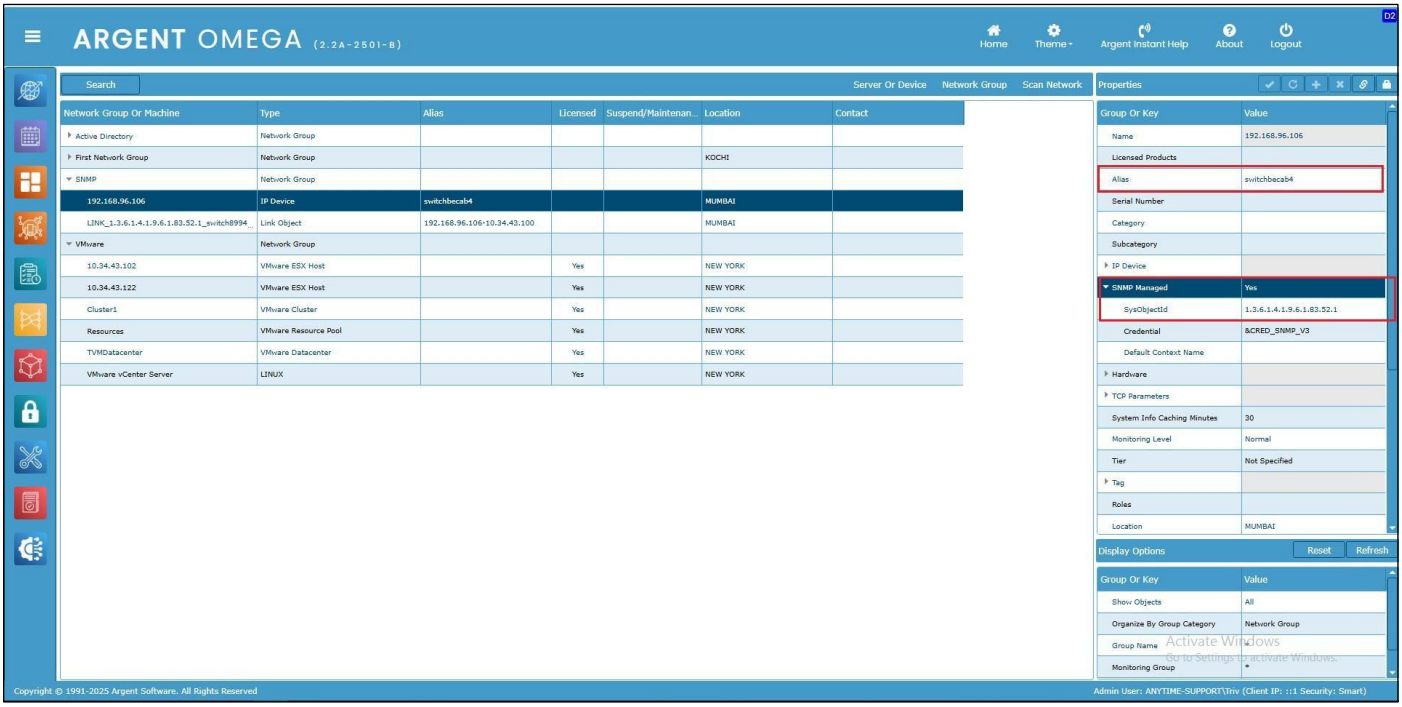
Use Toggle button to switch the selection in **Ignored** check box.

The scanned device will be added to CMDB-X as shown below:

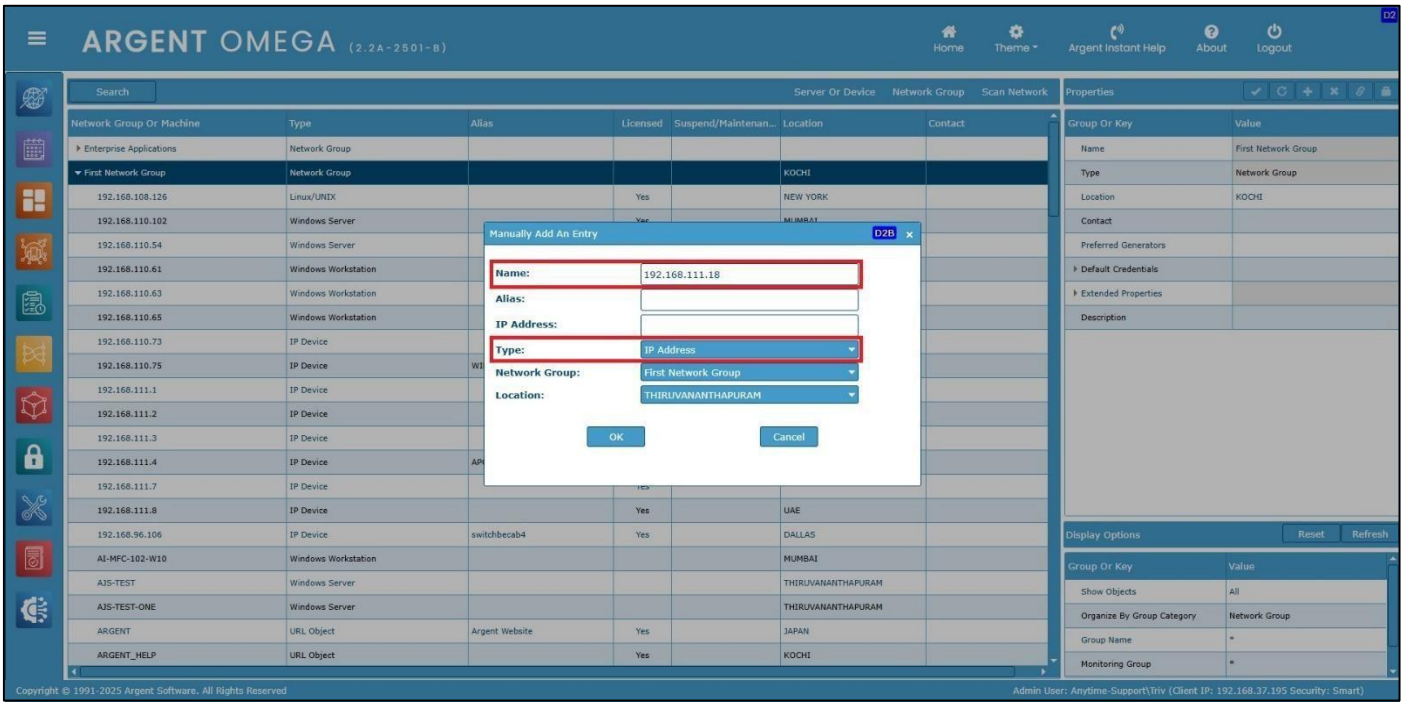


When adding the SNMP device, the CMDB-X property named **SNMP Managed** is set to **Yes** state.

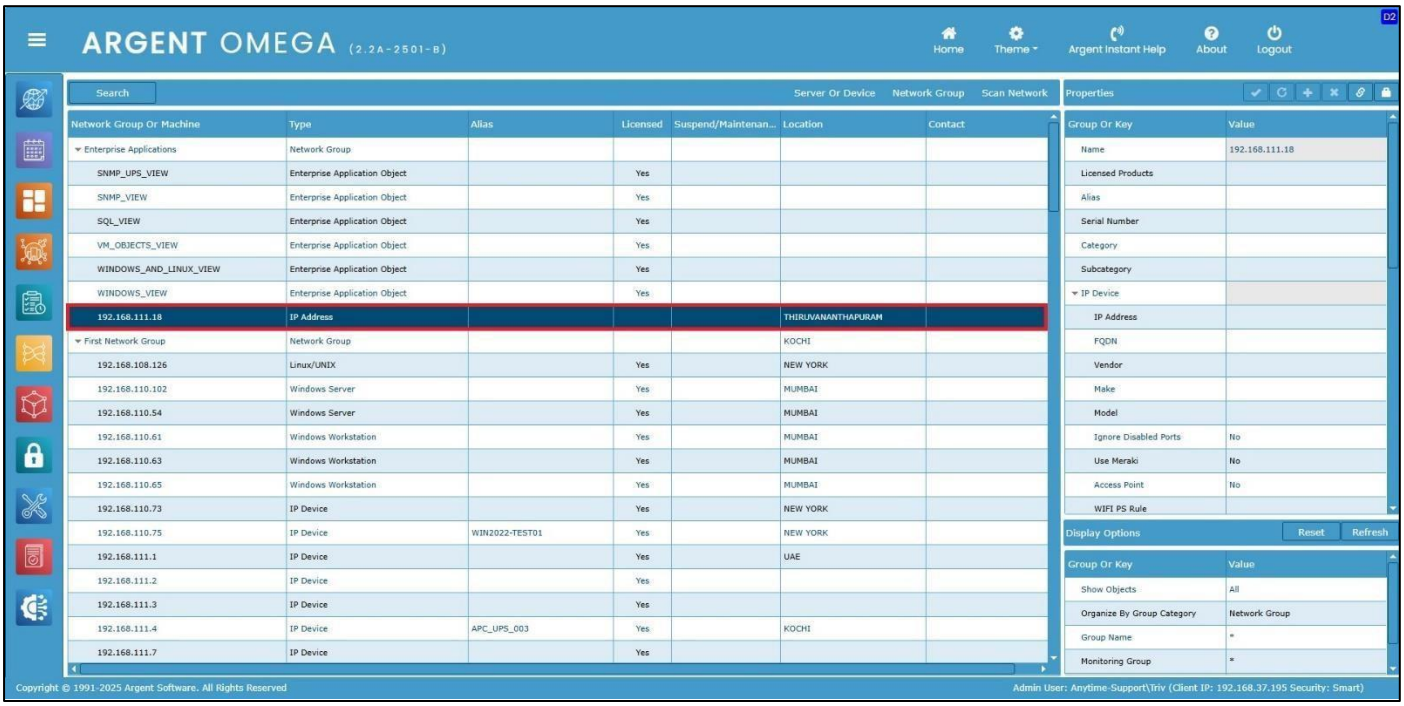
The SysObjectId and device type are automatically retrieved – SysObjectId contains the vendor's identification of an SNMP managed object type:



To manually add an SNMP device to CMDB-X, select **Manually Add Server/Device** from the right click menu. Add the Name/IP of the device and select the **Type**:



The new server is listed in CMDB-X:

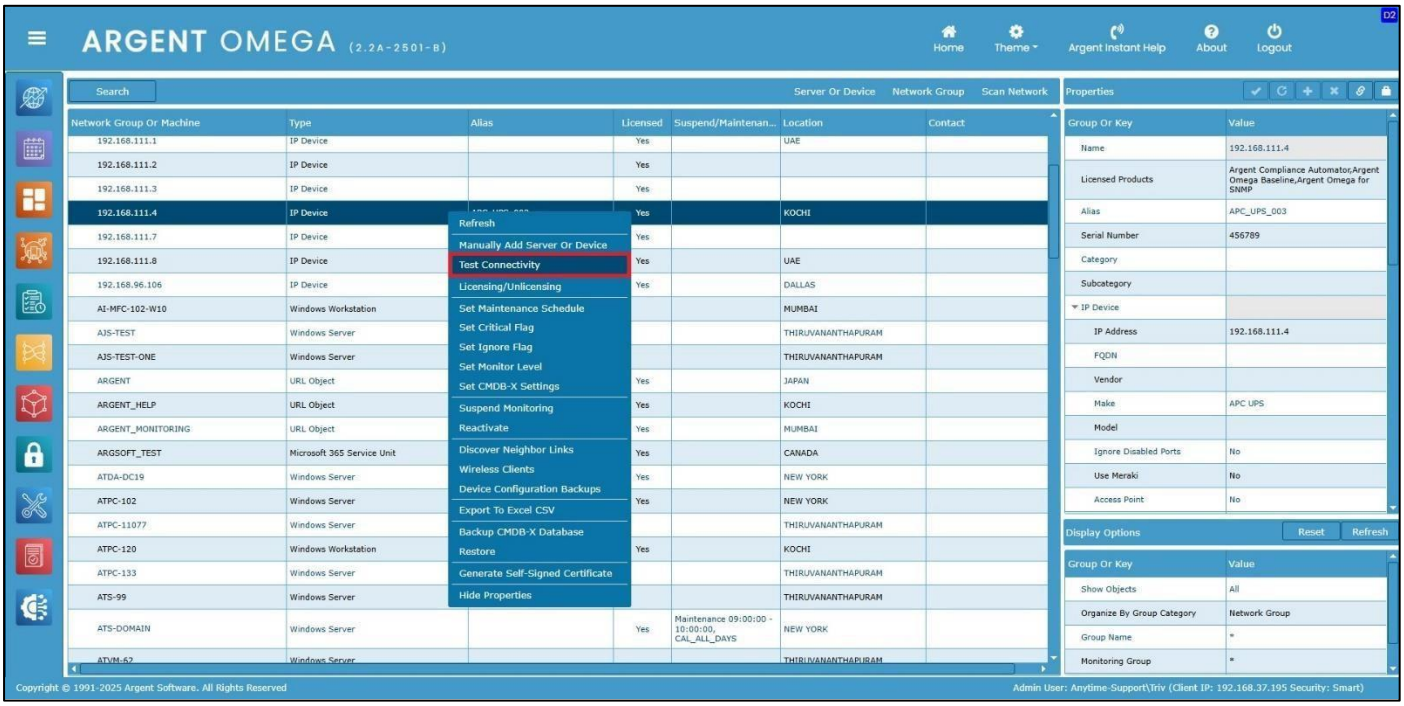


The following SNMP-specific properties need to be configured to monitor the device using Argent Omega for SNMP Tool Sets:

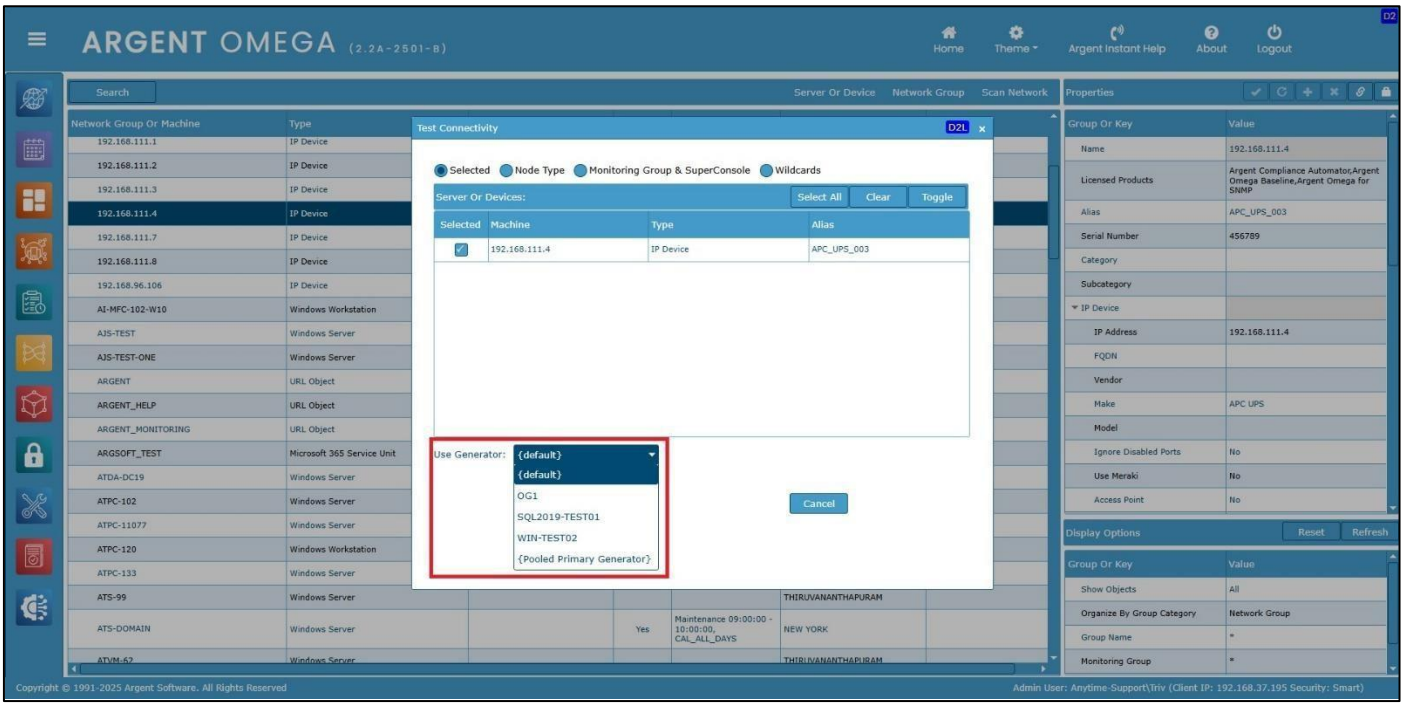
Connect Parameters	Select **Default** to connect using default parameters. Select **Explicit** to define the parameters explicitly. The below parameters need to be defined.
SNMP Version	Can be SNMPv1, SNMPv2c, or SNMPv3. **SNMPv3 requires authentication.** If SNMPv3 is selected, valid authentication credentials need to be specified.
Port	If not specified, default **161** is used.
Community	This is the community string for SNMPv1 and SNMPv2. If not specified, default **public** is used.
User Account	SNMPv3 username
Auth Protocol	SNMPv3 authentication password
Auth Password	SNMPv3 authentication protocol. It can be MD, SHA, SHA256, or SHA512.
Encrypt Algorithm	SNMPv3 encryption algorithm. It can be DES, AES, 3DES, AES192, or AES256.
Encrypt Password	SNMPv3 encryption password

A connectivity test can be run to verify the licensed SNMP device configured in the Argent CMDB-X.

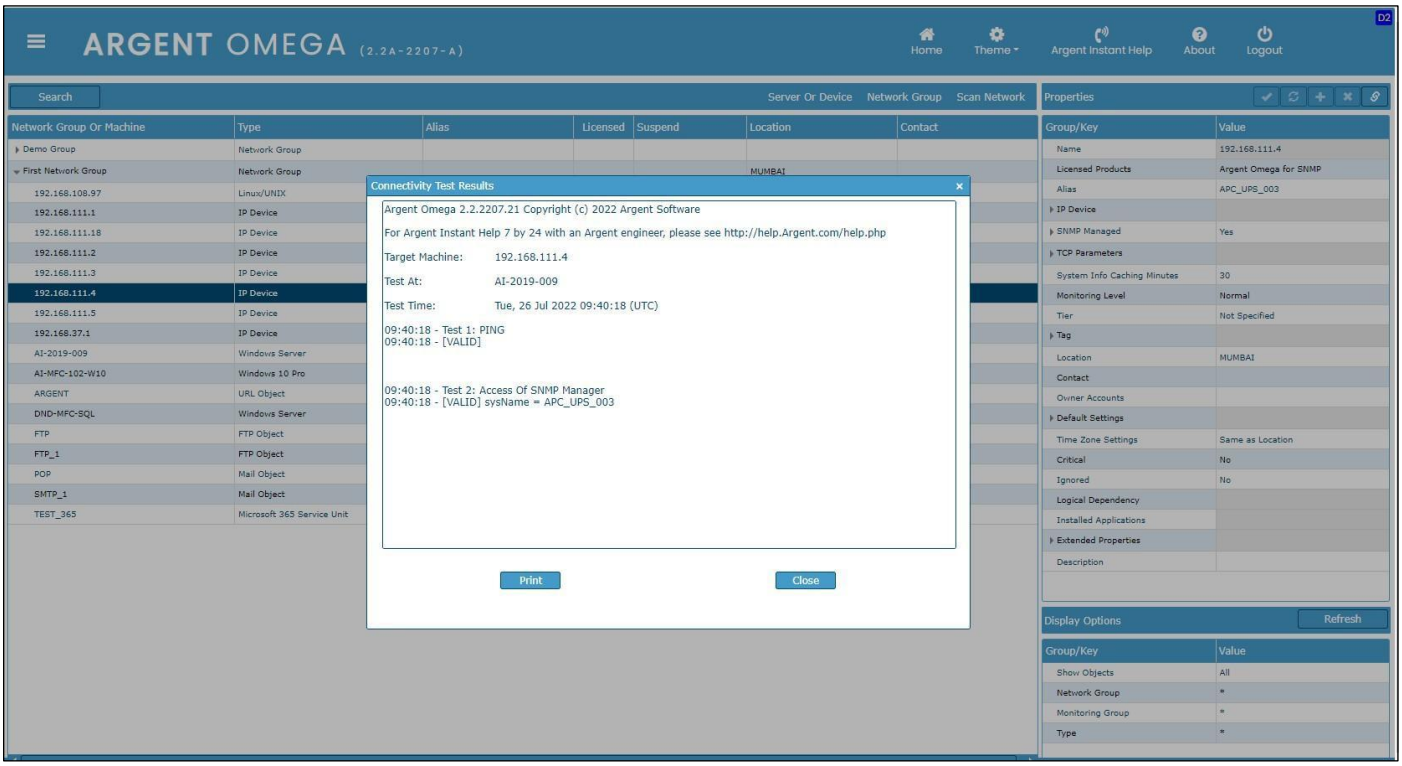
Select **Test Connectivity** from the right click menu or click  from properties to execute the connectivity test:



Select a server or device to execute the connectivity test and click OK:



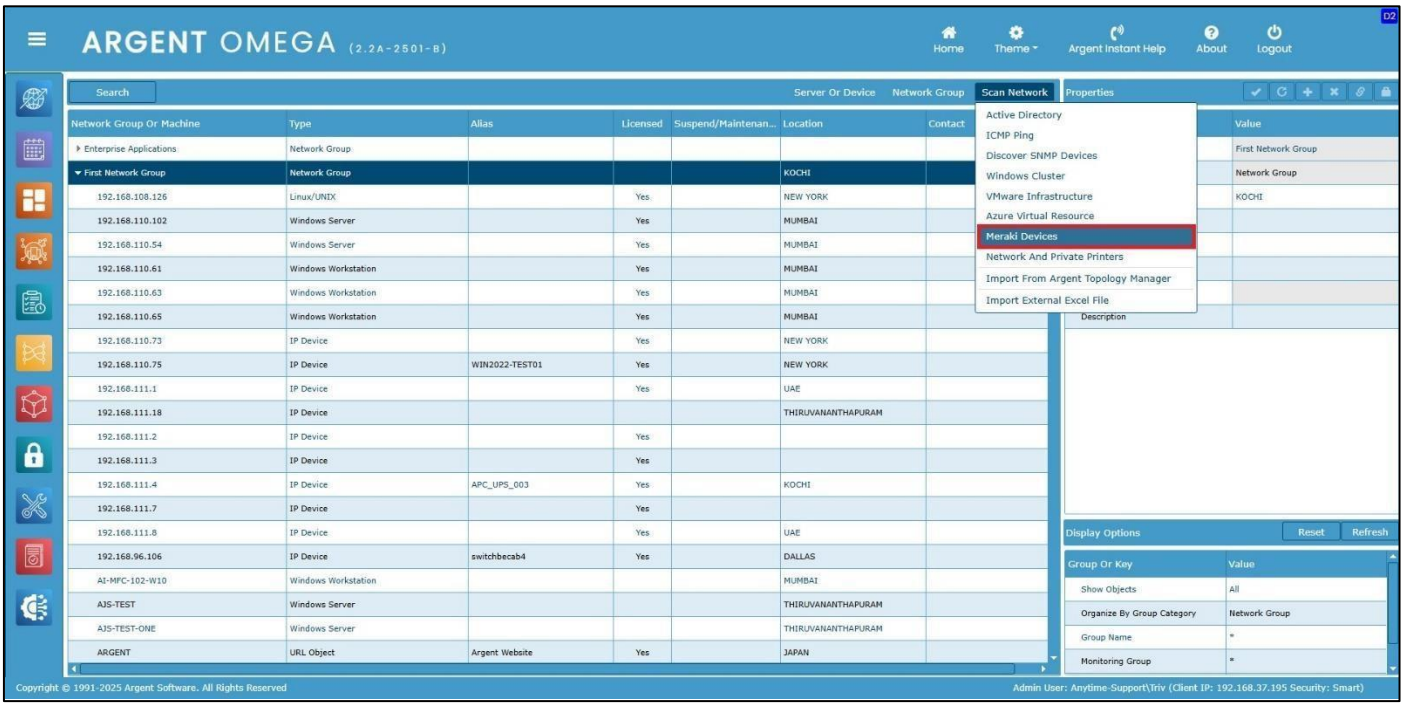
The Results are shown:



Tests can also be run against other servers or device types using the same method.

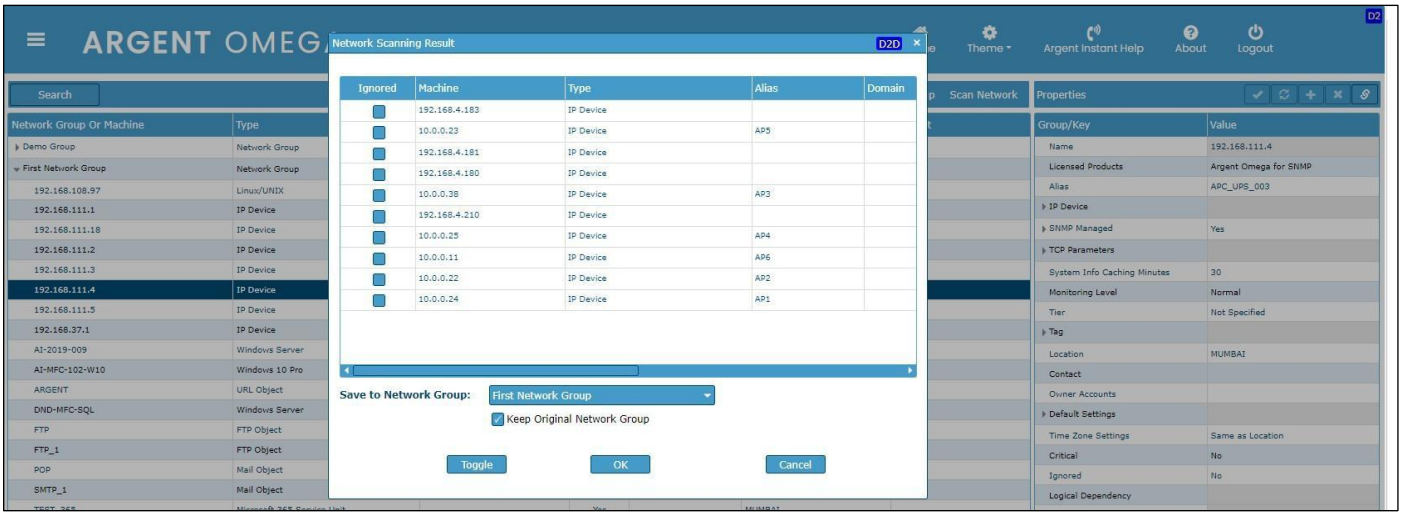
Display Wireless Clients For Meraki Access Point (AP)

Meraki is the cloud-based management protocol for CISCO wireless access points (AP). One common usage is to find current wireless clients of a selected Meraki device. There is a scan option in CMDB-X to scan Meraki devices.



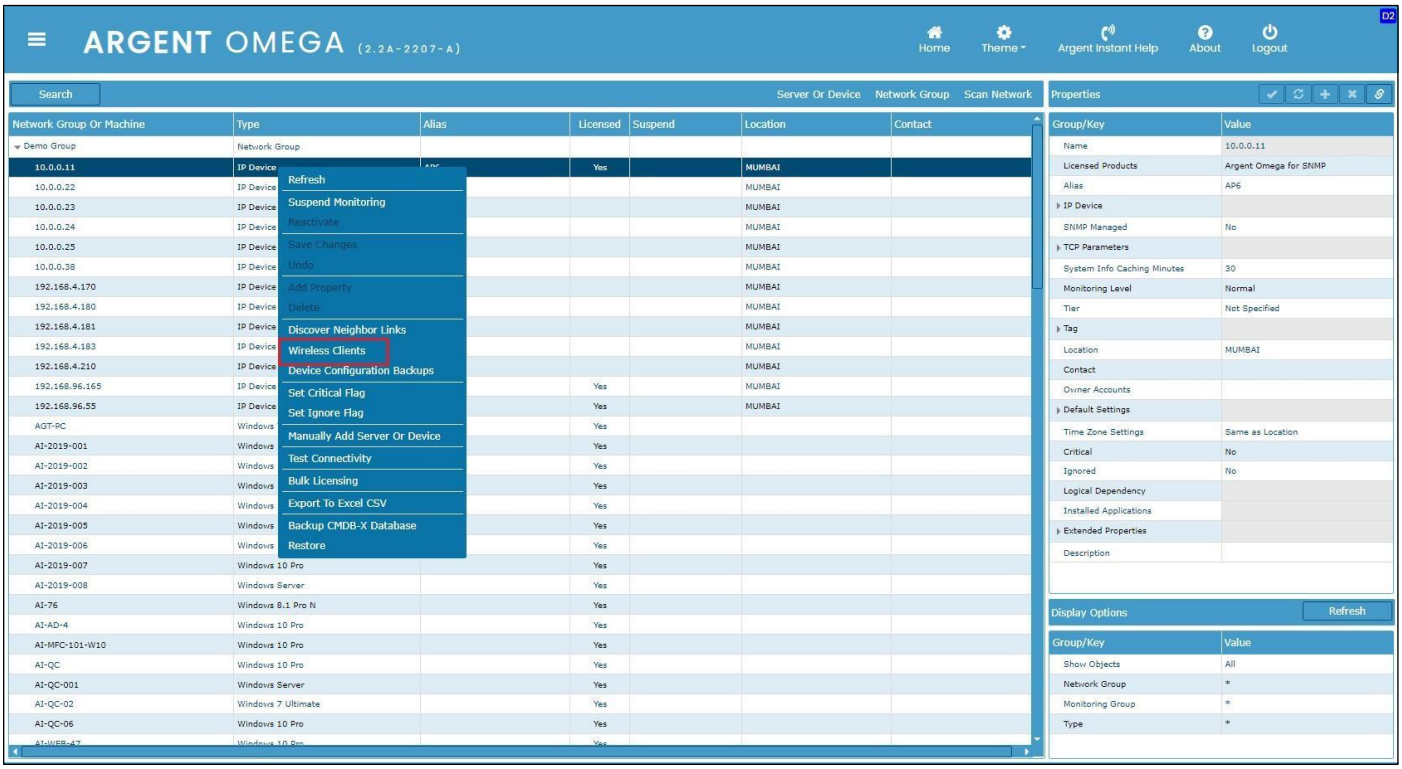
To use this facility, Meraki API key must be specified in **Argent Omega** settings under **Generator Settings.**

Click **Meraki Devices** popup menu option to scan all Meraki devices in the network. The scanning result will be shown in a list box as shown below:

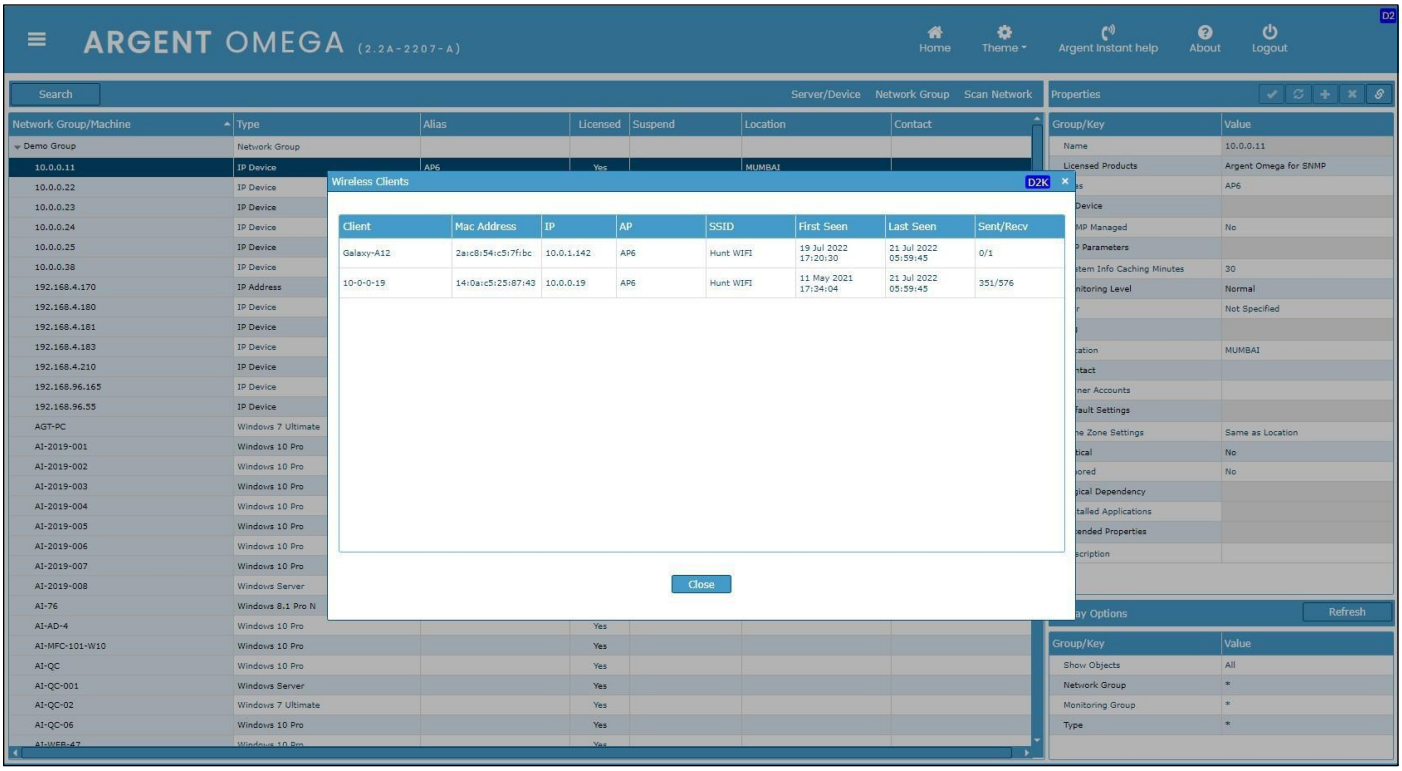


Press **OK** button to add the scanned devices under specified Network Group in CMDB-X.

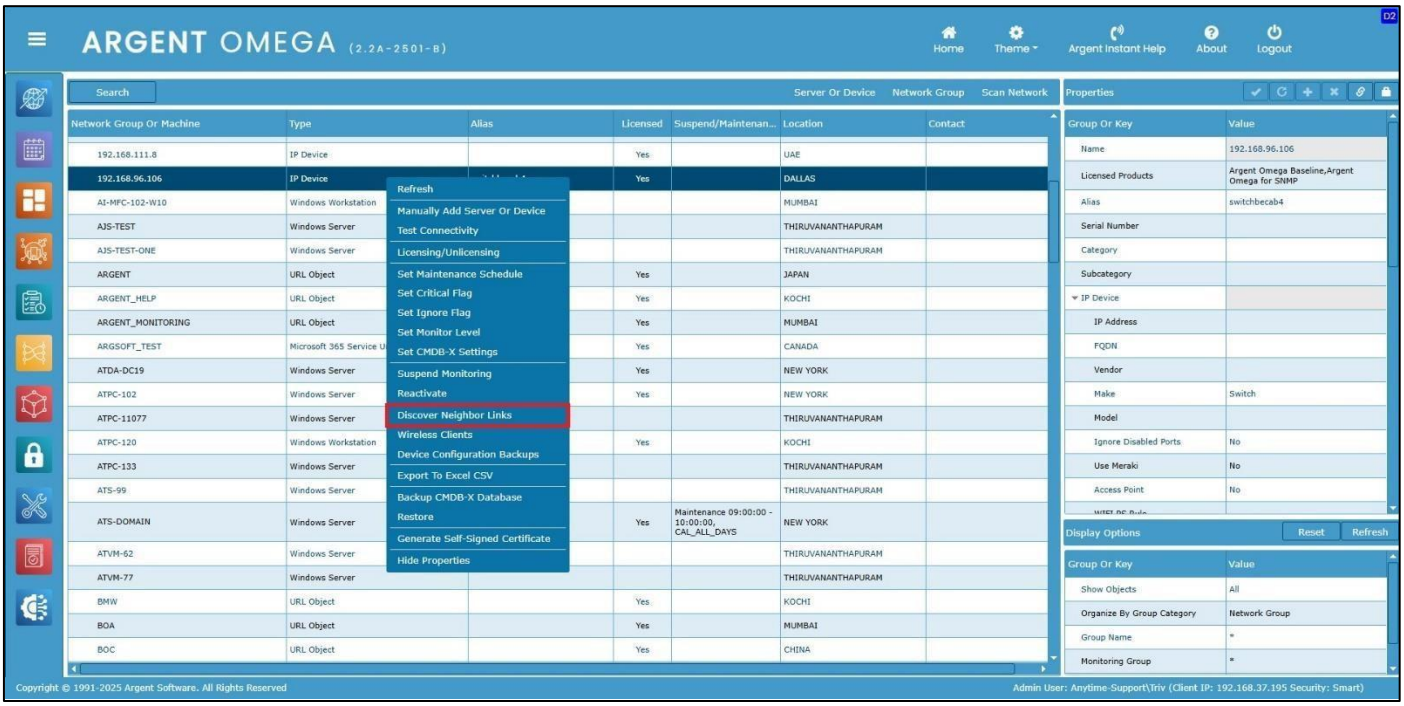
To find out the wireless clients currently connected to a specific Meraki device, select the device and click **Wireless Clients** context menu option.

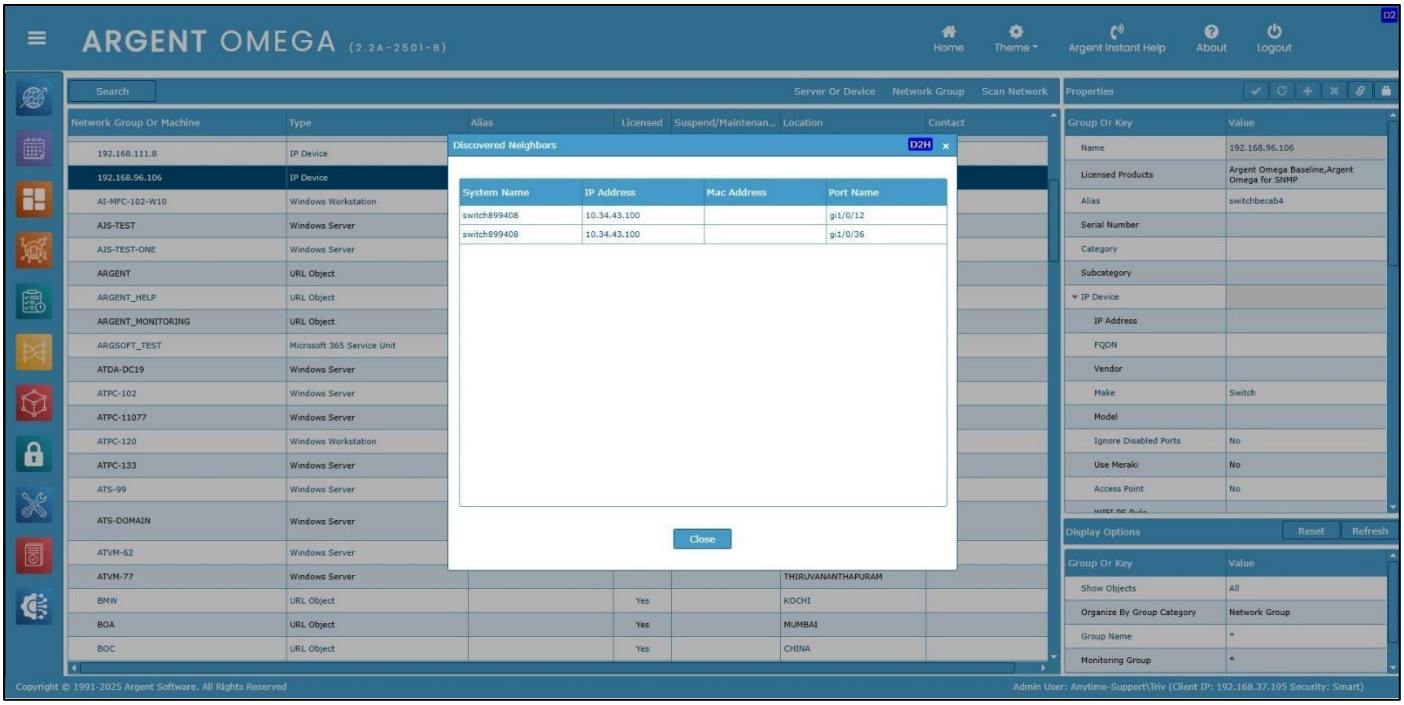


The wireless clients connected to the selected Meraki device will be listed in a popup dialog as shown below:



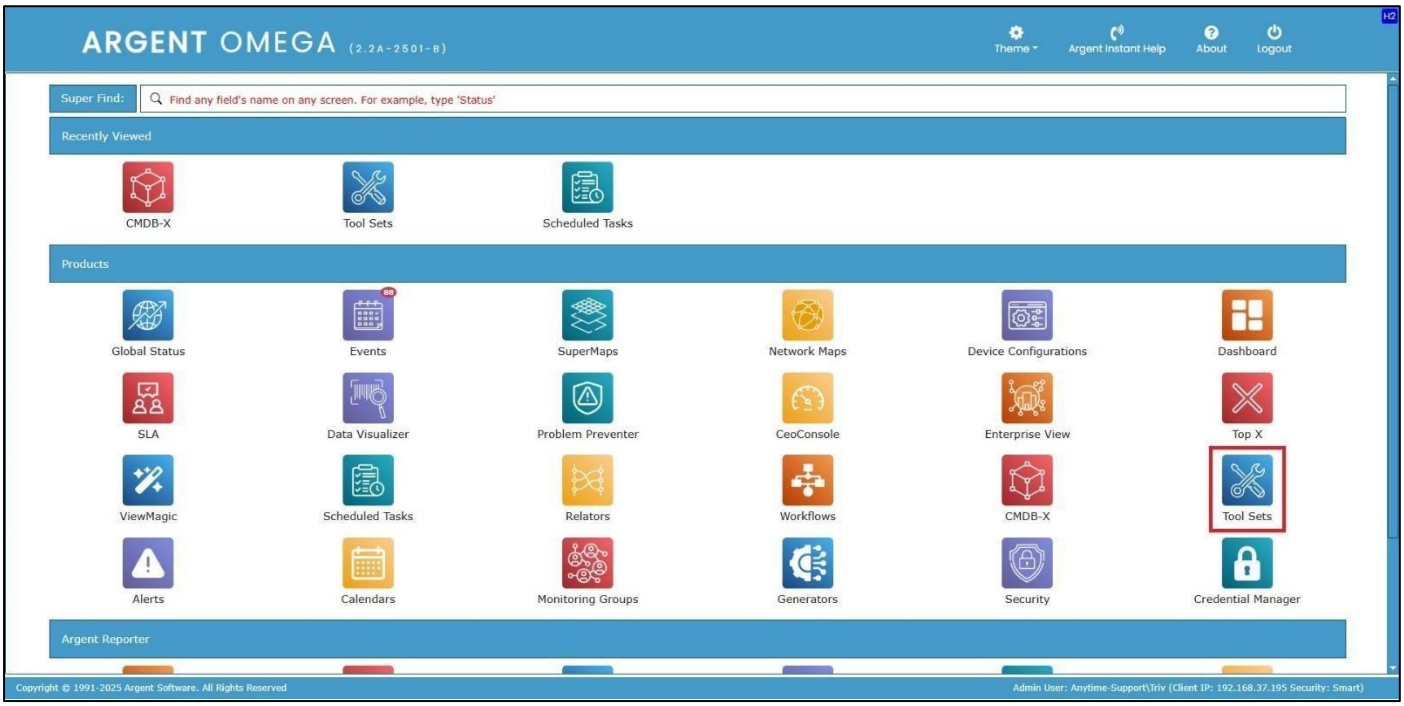
Discover Neighbor Links option finds the neighbor switches connected to the switch device.



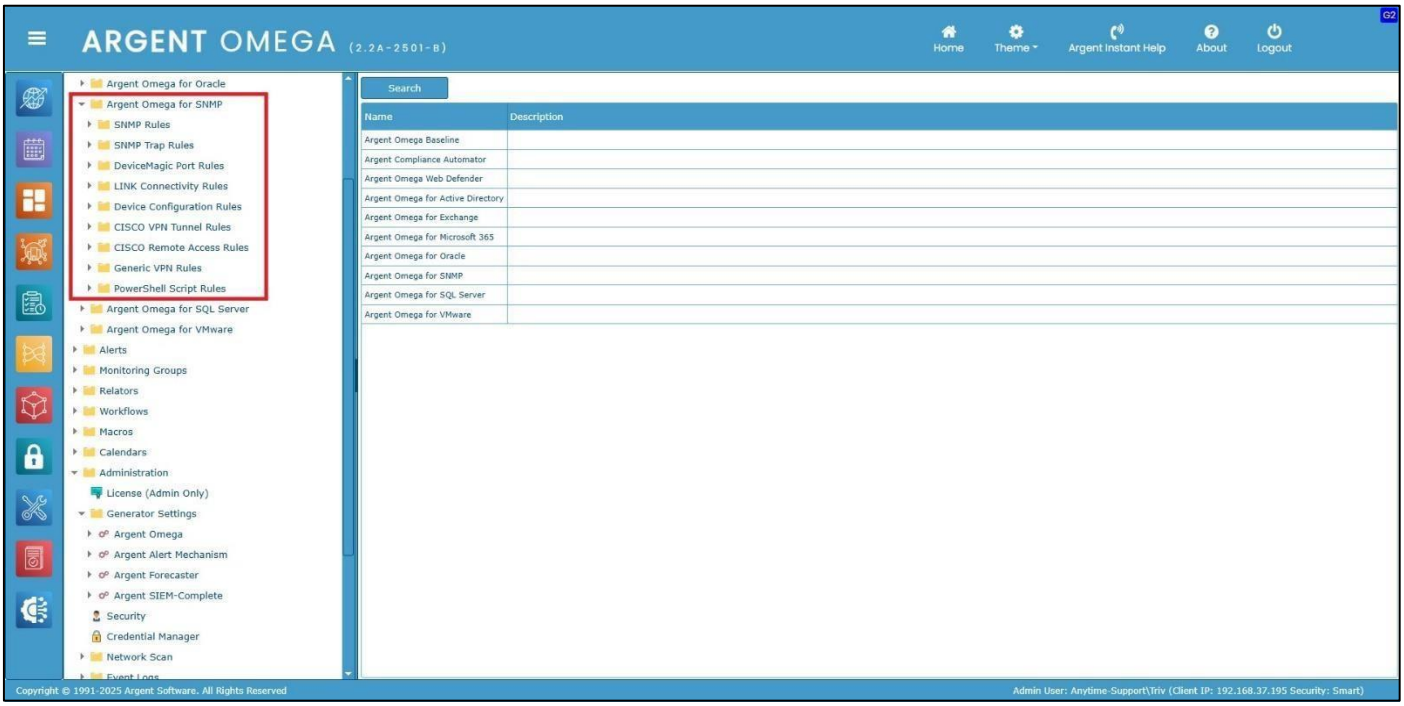


Agent Omega for SNMP Tool Sets

Select **Tool Sets** from the Home Screen **(note the very useful Super Find):**



Under **Tool Sets**, select **Argent Omega for SNMP**. The following Rules are shown.



Argent Omega for SNMP incorporates the following Rules:

- SNMP Rules
- SNMP Trap Rules
- DeviceMagic Port Rules
- Link Connectivity Rules
- Device Configuration Rules
- CISCO VPN Tunnel Rules
- CISCO Remote Access Rules
- Generic VPN Rules
- PowerShell Script Rules

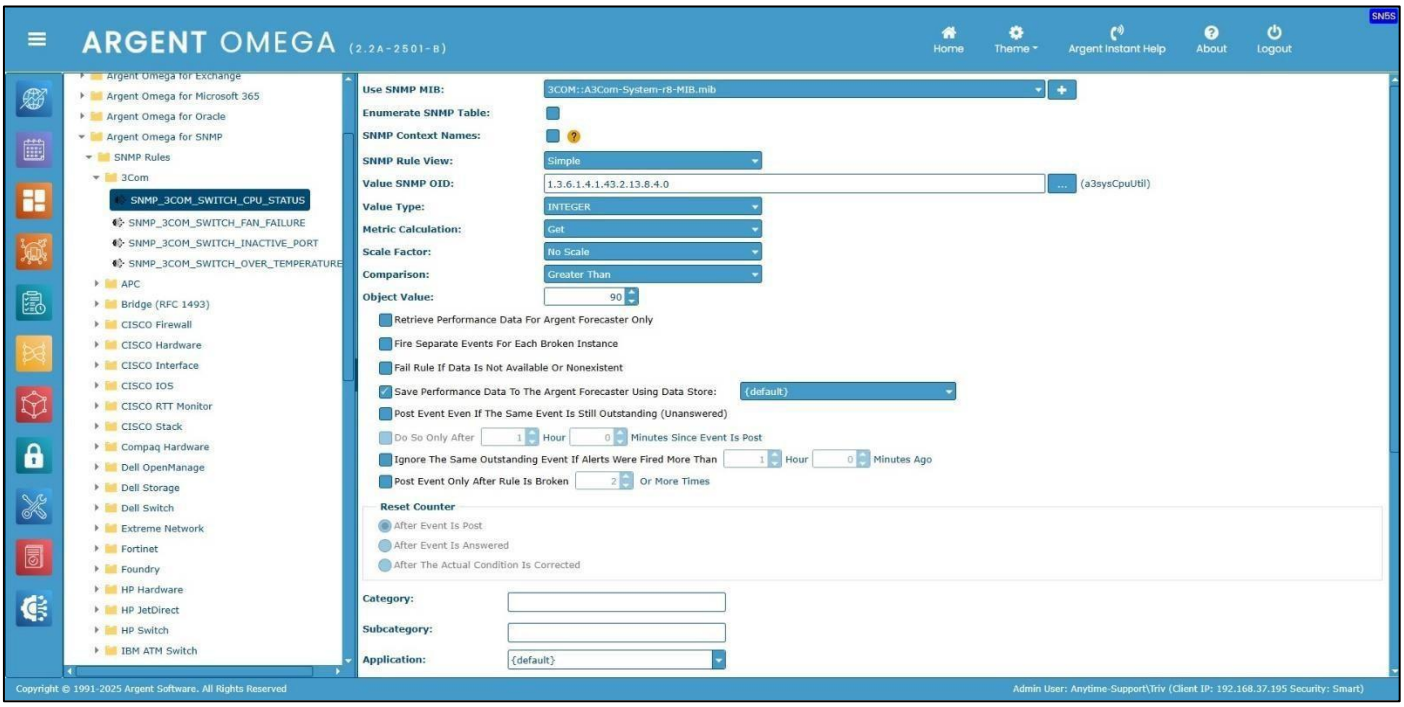
SNMP Rules

Any SNMP-compliant device can be monitored using SNMP Rules. These Rules poll OIDs by either manually specifying the value or using the **Argent OID Browser**. OID values can also be added by using the device specific MIB file. Custom SNMP Rules can be created based on any manufacturer's SNMP information in the MIB file. **Argent engineers can also assist with this process.**

The Tool Sets of Argent Omega for SNMP provide built-in Rules to monitor common SNMP-compliant devices, such as CISCO, 3Com, APC, Dell, Fortinet, HP, Novell, Compaq Server Hardware, IBM Server Hardware, etc.

Because the types of hardware devices vary widely, from Compaq server hardware to air conditioning units and PBXs, SNMP Rules are used to monitor all important aspects of common server hardware, such as the motherboard, power supply, and even the fans.

Following is the SNMP Rule screen:

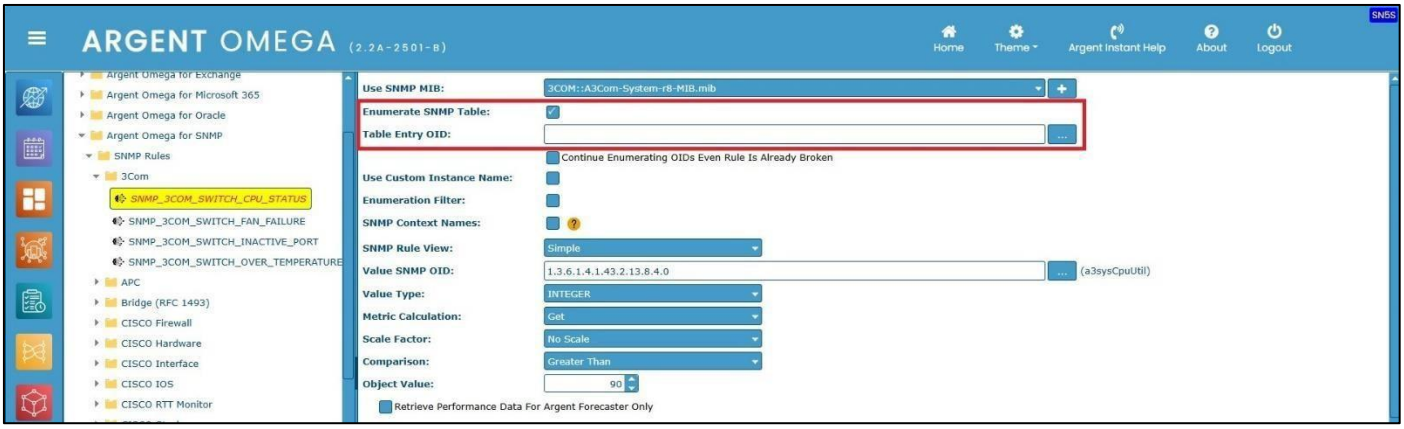


The following selections are necessary to monitor an SNMP-compliant device:

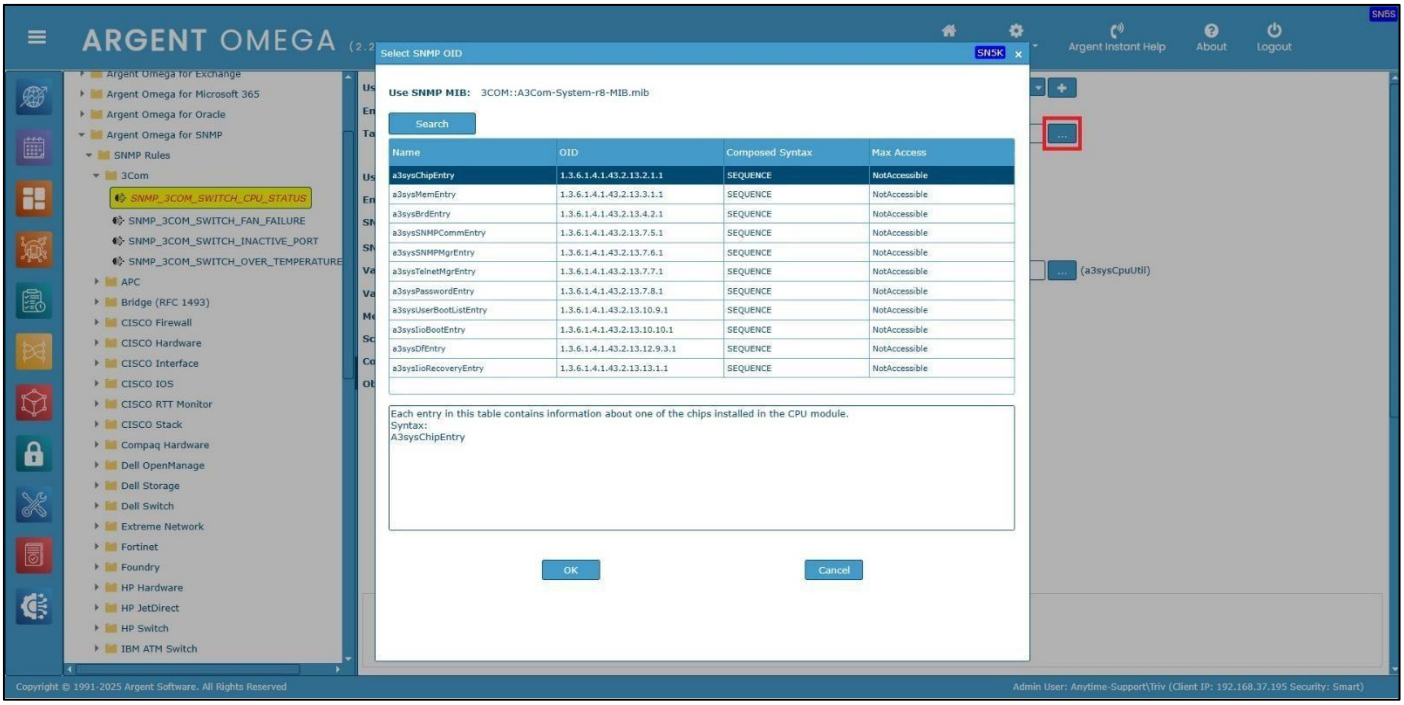
Select the MIB file from **Use SNMP MIB** combo box. **The MIB file is essentially the personality of the device.** The MIBs of all common SNMP devices are already loaded in the combo box. Click **"+"** button to upload a new MIB file to the combo box.

Use the **Enumerate SNMP Table** option if the Rule needs to enumerate SNMP tables defined in the selected MIB file. An **SNMP table** is an ordered collection of objects containing zero or more rows.

The table and each object in the table are identified by using an OID or Object Identifier. The information on a specific network entity will be retrieved from SNMP tables. If **Enumerate SNMP Table** option is checked, SNMP Table OID must be specified in **Table Entry OID** field.

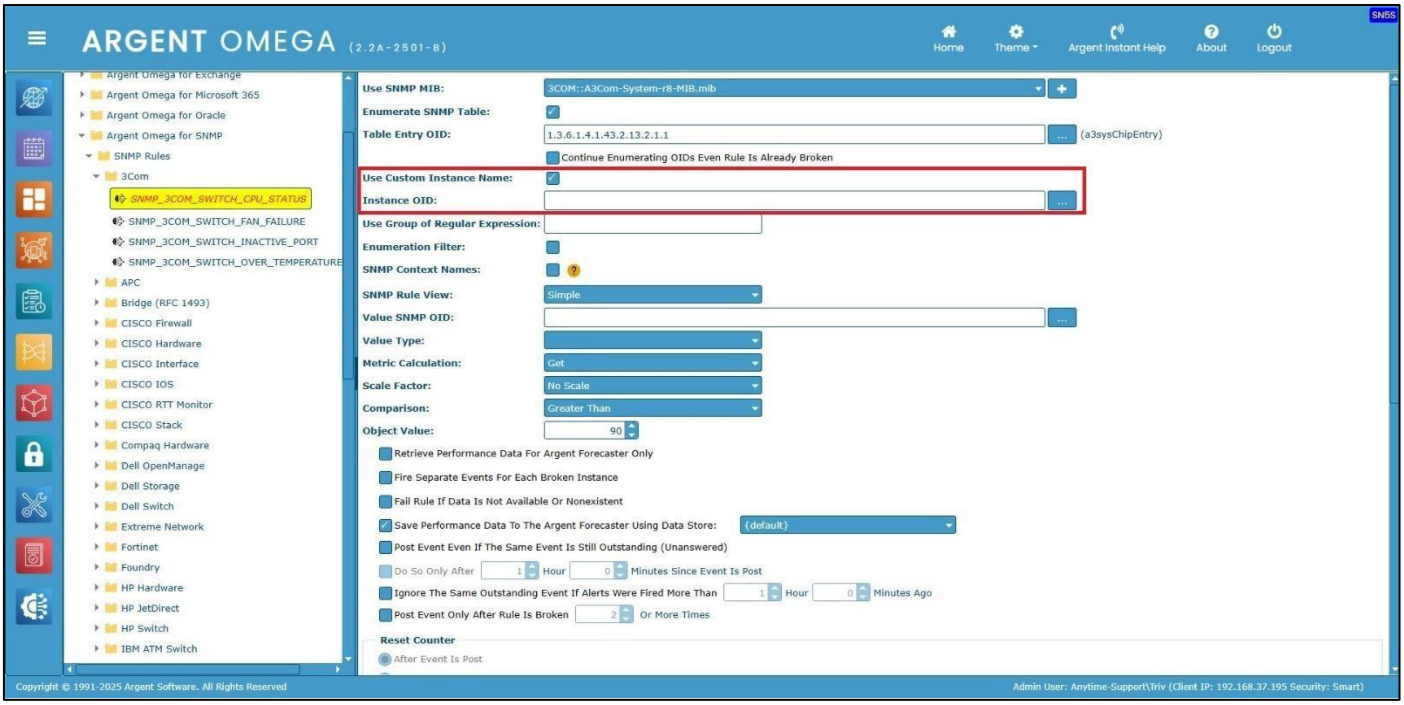


Either manually enter the OID or use the browse button to browse **Table Entry OIDs** of specific MIB file:



Select the **Table Entry OID** and click OK:

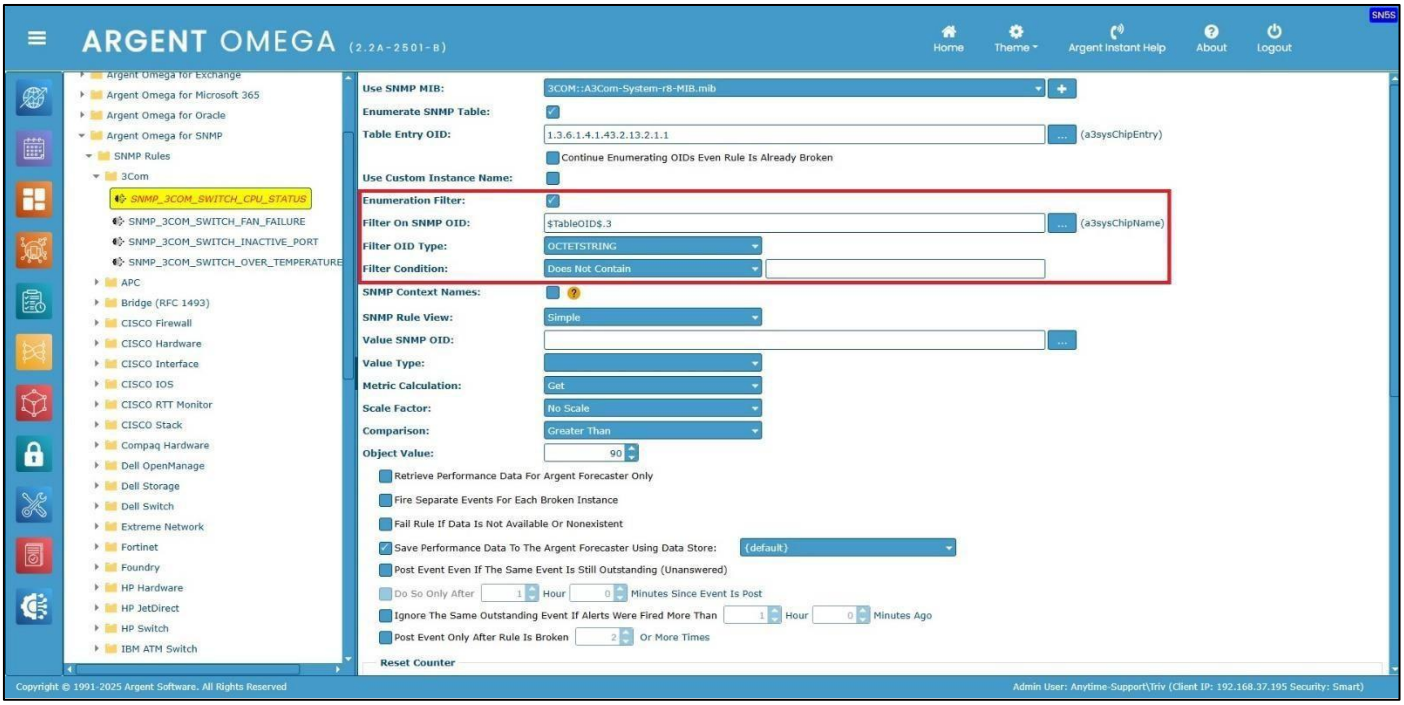
If **Enumerate SNMP Table** is checked, check the option **Use Custom Instance Name** to define custom instance name in Performance Data. Normally, the object name (Example: *upsBatteryStatus*, upsOutputPercentLoad, etc.) is taken as instance name. By checking **Use Custom Instance Name** option, the actual instance (object name) name is appended with value of specified SNMP OID. The SNMP OID can be specified in **Instance OID** field. There is also a provision to browse the Instance OID.



If **Enumerate SNMP Table** is used, check the **Enumeration Filter** option to apply a filter for querying OID values from the SNMP table. The Rule will be validated only if the specified filter condition is satisfied. Filters can be applied to specific SNMP OIDs. The type of OID value and filter condition also needs to be specified. Specify OID in **Filter On SNMP OID** field to which filter is applied.

Select OID value type from **Filter OID Type** combo box.

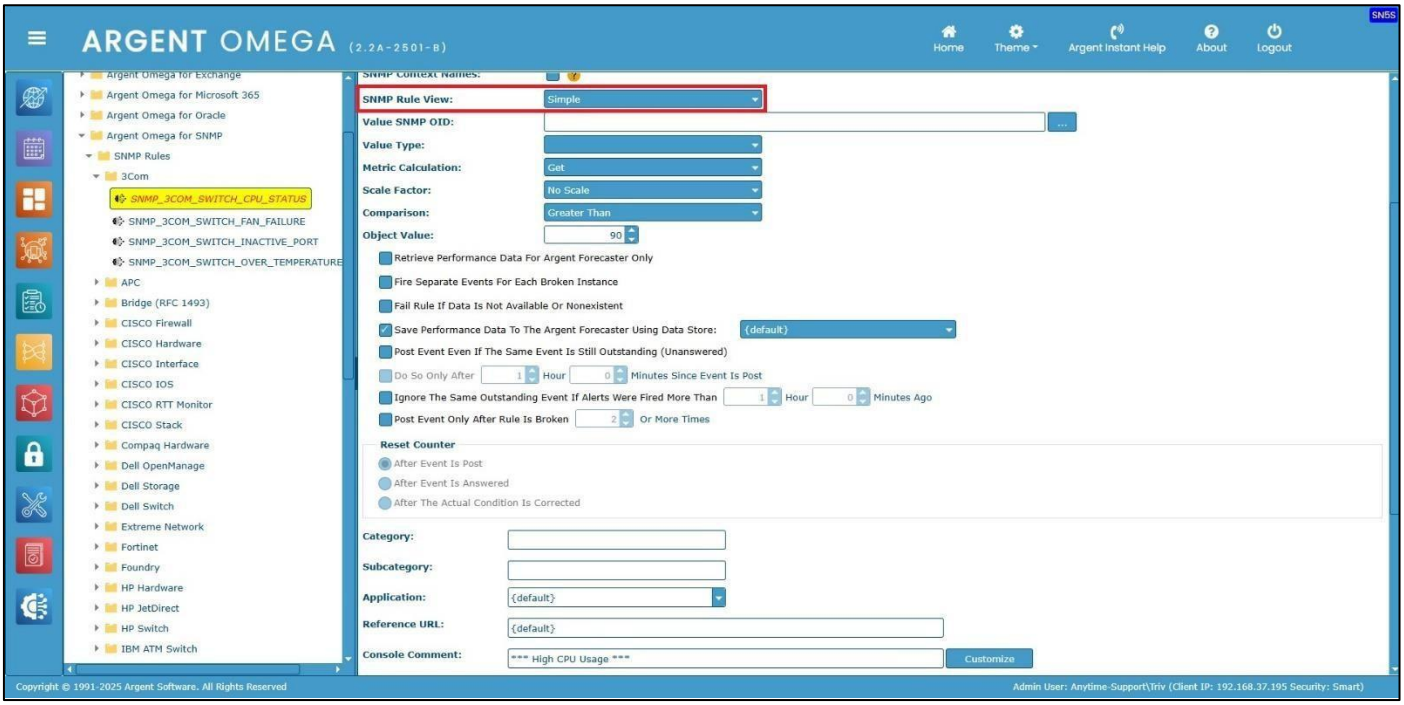
Select filter condition from **Filter Condition** combo box.



SNMP Rule View defines the way in which SNMP parameters are configured in the Rule to retrieve SNMP OID values. There are three types of views, namely: **Simple, Multi-Level** and **Advanced.**

Simple

This is the simplest way to configure SNMP parameters.



Following Parameters need to be configured:

Value SNMP OID: Object ID to query. Either manually enter the OID or browse by clicking browse button.

Value Type: Type of OID value

Metric Calculation: Different SNMP Metric Calculation Methods are available, such as Get, Delta Since Last Poll, Delta Per Second, Delta Per Minute, Delta Per Hour and Delta Wait.

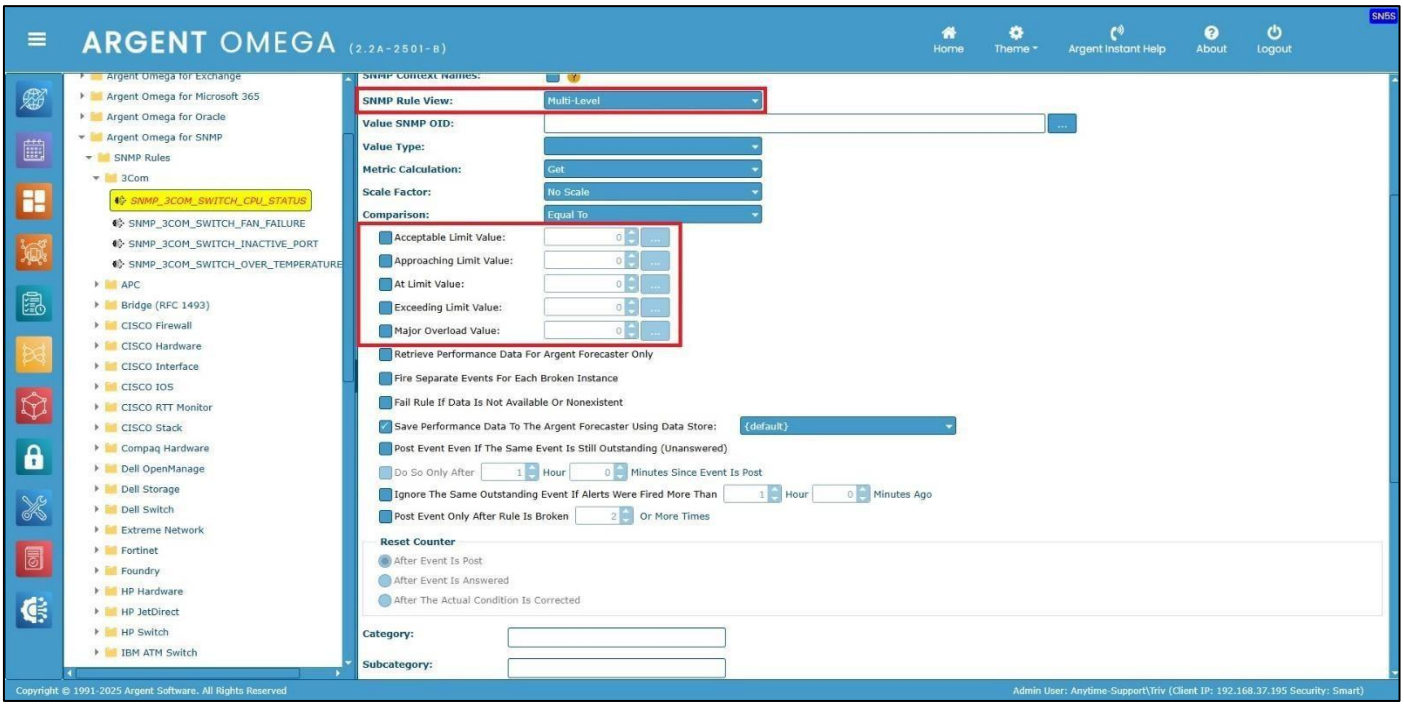
Scale Factor: Scale of measurement of metric value

Comparison: Operator to compare the given threshold against the metric value.

Object Value: Threshold to compare

Multi-Level

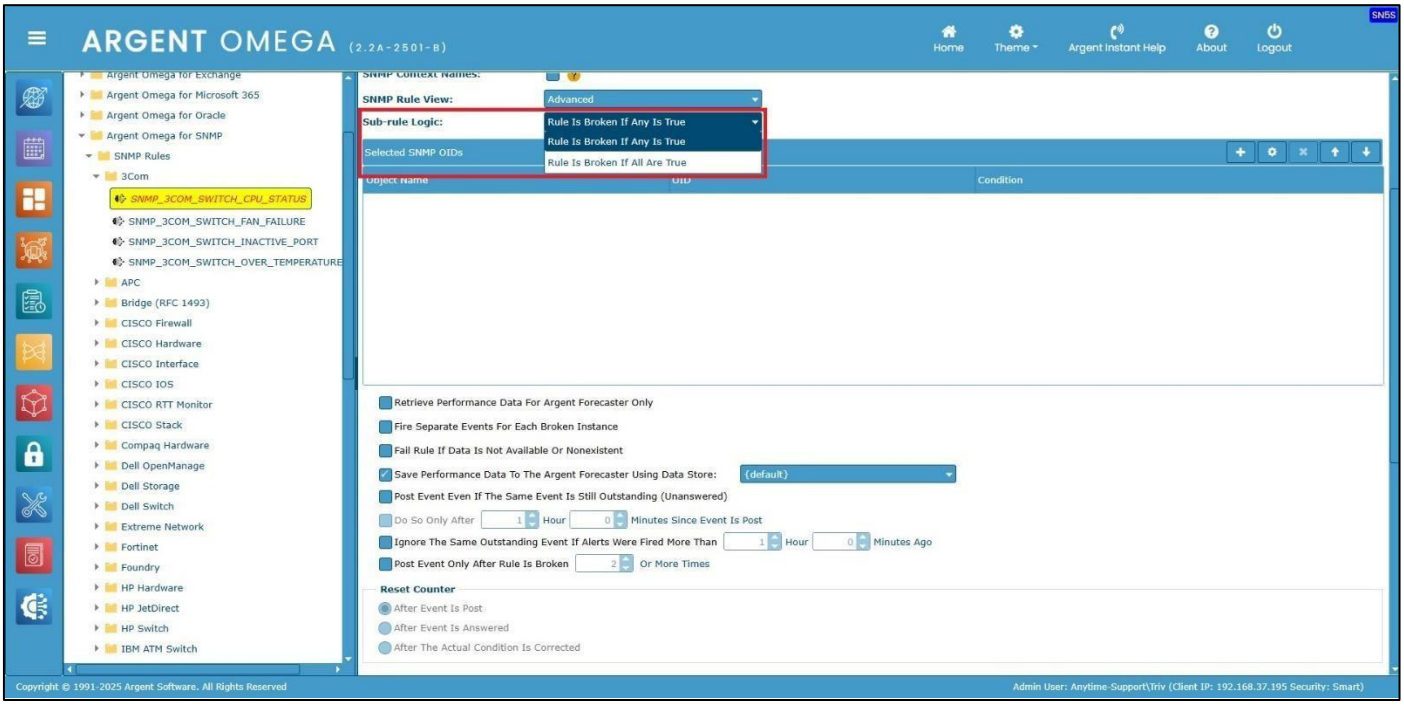
This Rule View option contains additional options for setting the Limit Value.



Advanced

Multiple conditions can be specified in Advanced Rule view. Rule broken logic options are available.

Sub-rule Logic combo box



Rule condition can be added by clicking **“+”** button. A sub-rule definition dialog is displayed where the Rule condition is defined.

There are two Sub-rule Types available in Advanced Rule View, **SNMP OID** and **Formula Expression**. The required details for both are specified in the sub window **SN5A**.

In **SNMP OID** type, Rule condition is defined based on retrieved SNMP OID value.

All parameters described in the **Simple** view (Value SNMP OID, Object Name, Value Type, Metric Calculation, Scale Factor, Comparison and Object Value) are configured here. The extra parameter is Variable Name. Instead of alerting, it is possible to keep the metric value in a user-defined variable by checking **Use As Variable** option – the variable can be used later in **Formula Expression** for metric calculation. Specify the variable name in **Variable Name** field.

Formula Expression offers added flexibility in monitoring SNMP Metrics.

For example, if an environmental monitor returns the temperature of the server room in Celsius, the metric can be converted to Fahrenheit. Alternatively, the uptime of a server or device can be measured by converting TIMETICKS to hours (TIMETICKS are hundredths of a second). Multiple SNMP metrics can also be added together to get a total traffic figure.

Specify a name in **Formula Name** field

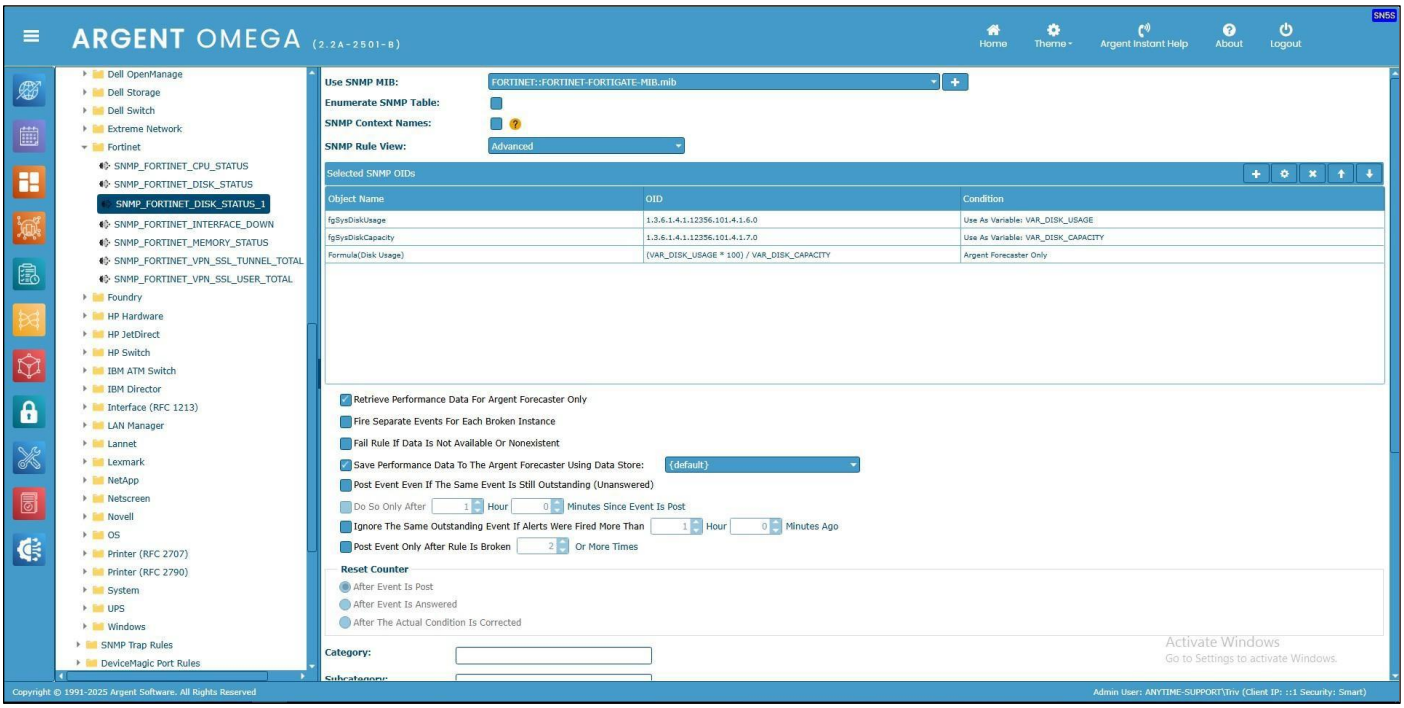
Specify the formula expression in **Formula** field. The formula specified in the screenshot VAR_DISK_USAGE * 100 / VAR_DISK_CAPACITY, where VAR_DISK_USAGE and VAR_DISK_CAPACITY are variables defined using SNMP OID sub-rule type.

Scale Factor defines the scale of measurement of the metric value result.

Comparison defines the operator to compare the given threshold against the metric value result.

Object Value defines the threshold to compare.

Following is a sample Advanced type Rule configured:



Check **Retrieve Performance Data For Argent Forecaster Only** option to only **save** performance metrics to Argent Forecaster, no Alert is fired.

Fire Separate Events For Each Broken Instance option fires separate Alerts for each broken condition.

SNMP Trap Rules

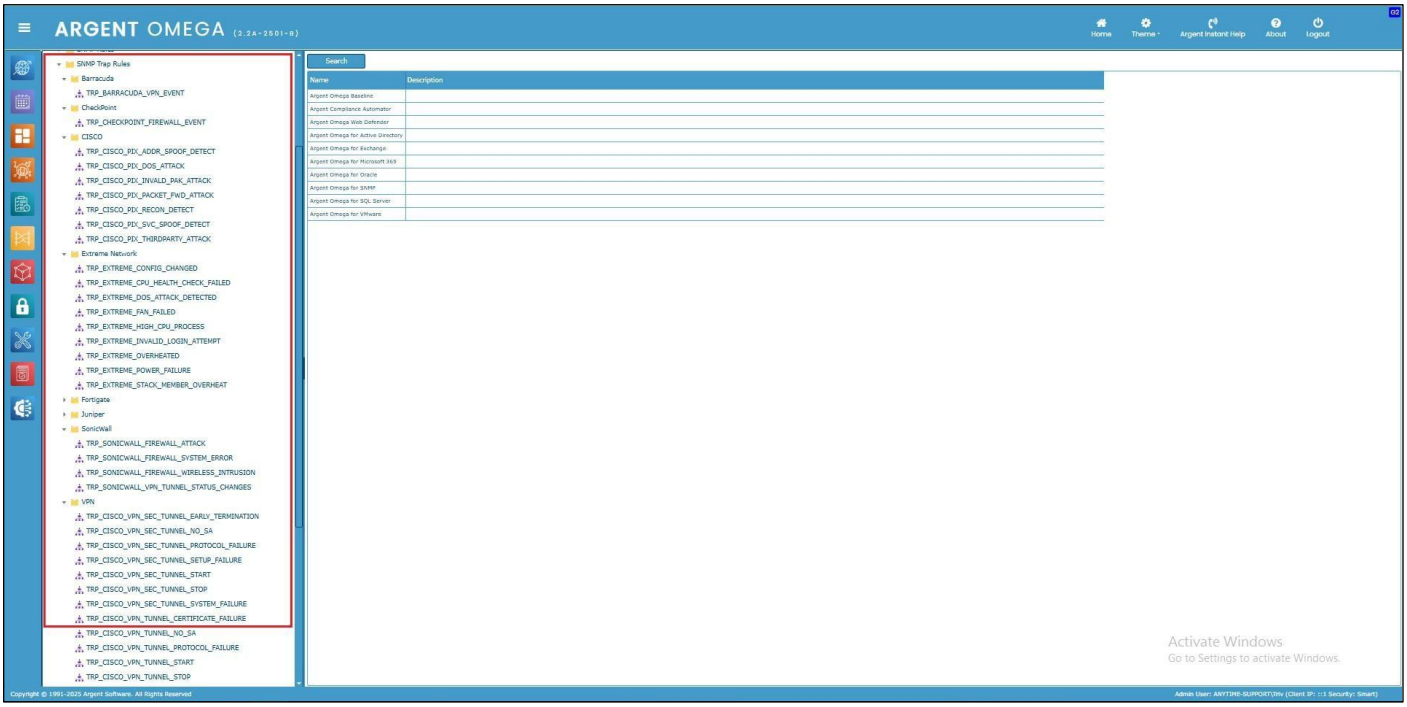
SNMP Traps are unsolicited SNMP information packets sent from any SNMP-compliant device to an SNMP manager, such as Argent Omega.

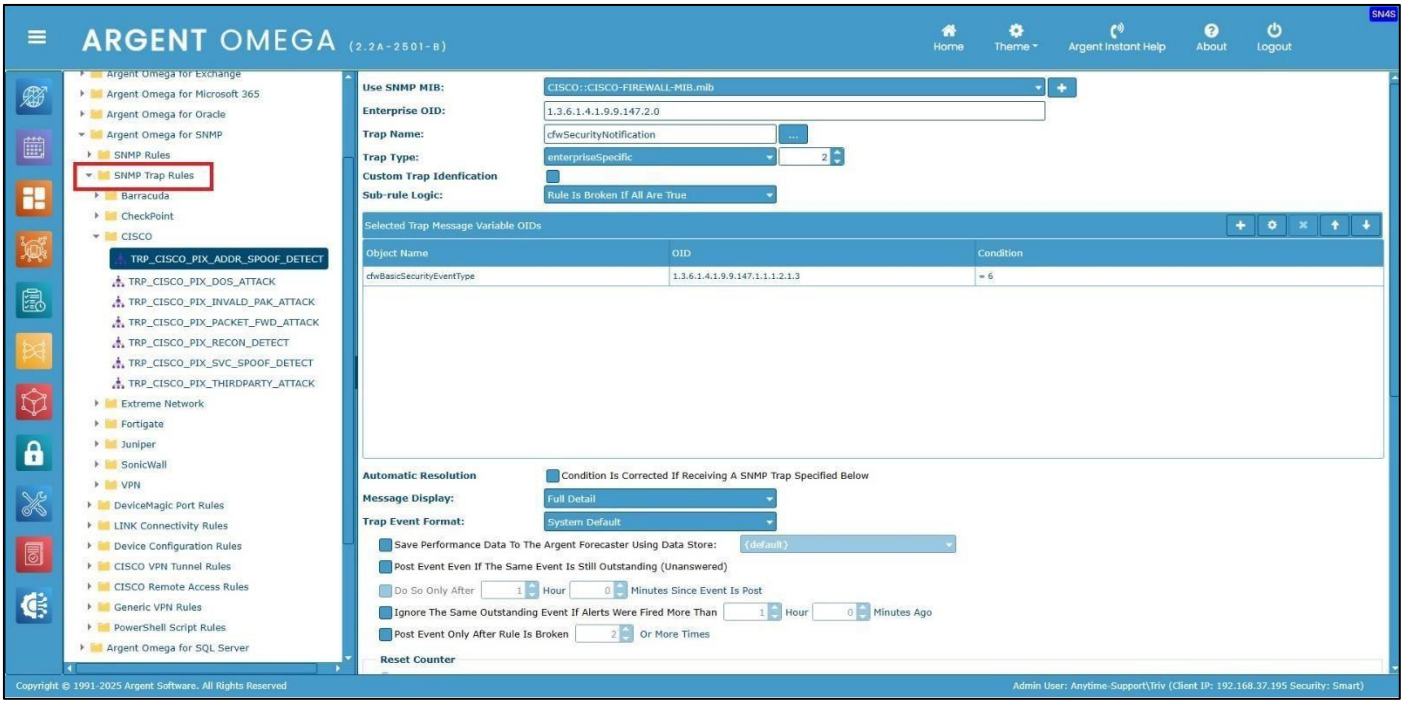
Traps can be sent for many reasons, such as hard drive failures, cooling fans that are not spinning at the right speed (or spinning at all), network interfaces suddenly dropping, or even for simple informational reasons like the SNMP service starting.

SNMP Rules run in Relators at scheduled intervals, so issues like a fan problem that occurs briefly might not be noticed. However, if the device sends an SNMP trap indicating the fan is not running properly, Argent can notify immediately.

SNMP Trap Monitor definitions can be defined to listen for specific traps or specific information within a trap. If a trap matches an SNMP Trap Monitor definition that is in Production Mode, Alerts are fired.

The Argent for SNMP comes equipped with the following highlighted pre-defined SNMP Trap Monitor definitions for a wide variety of devices.




ARGENT OMEGA (2.2A-2501-B)
Home
Theme
Argent Instant Help
About
Logout
Argent Omega for Exchange
Argent Omega for Microsoft 365
Argent Omega for Oracle
Argent Omega for SNMP
SNMP Rules
SNMP Trap Rules
Barracuda
CheckPoint
CISCO
TRP_CISCO_PIX_ADDR_SPOOF_DETECT
TRP_CISCO_PIX_DOS_ATTACK
TRP_CISCO_PIX_INVALD_PAK_ATTACK
TRP_CISCO_PIX_PACKET_FWD_ATTACK
TRP_CISCO_PIX_RECON_DETECT
TRP_CISCO_PIX_SVC_SPOOF_DETECT
TRP_CISCO_PIX_THIRDPARTY_ATTACK
Extreme Network
Fortigate
Juniper
SonicWall
VPN
DeviceMagic Port Rules
LINK Connectivity Rules
Device Configuration Rules
CISCO VPN Tunnel Rules
CISCO Remote Access Rules
Generic VPN Rules
PowerShell Script Rules
Argent Omega for SQL Server
Use SNMP MIB:
CISCO::CISCO-FIREWALL-MIB.mib
Enterprise OID:
1.3.6.1.4.1.9.9.147.2.0
Trap Name:
cfwSecurityNotification
Trap Type:
enterpriseSpecific
2
Custom Trap Idenfication
Sub-rule Logic:
Rule Is Broken If All Are True
Selected Trap Message Variable OIDs
Object Name
OID
Condition
cfwBasicSecurityEventType
1.3.6.1.4.1.9.9.147.1.1.1.2.1.3
= 6
Automatic Resolution
Condition Is Corrected If Receiving A SNMP Trap Specified Below
Message Display:
Full Detail
Trap Event Format:
System Default
Save Performance Data To The Argent Forecaster Using Data Store:
(default)
Post Event Even If The Same Event Is Still Outstanding (Unanswered)
Do So Only After
1
Hour
0
Minutes Since Event Is Post
Ignore The Same Outstanding Event If Alerts Were Fired More Than
1
Hour
0
Minutes Ago
Post Event Only After Rule Is Broken
2
Or More Times
Reset Counter
Copyright © 1991-2025 Argent Software. All Rights Reserved
Admin User: Anytime-Support\Iriv (Client IP: 192.168.37.195 Security: Smart)

The following options are configured to handle SNMP Traps:

Select MIB file from **Use SNMP MIB** combo box. **The MIB file is essentially the personality of the device.** The MIB files govern what is possible to do or see via SNMP for a particular device. The MIBs of all common SNMP devices are already loaded in the combo box. Click **"+"** button to upload a new MIB file to the combo box.

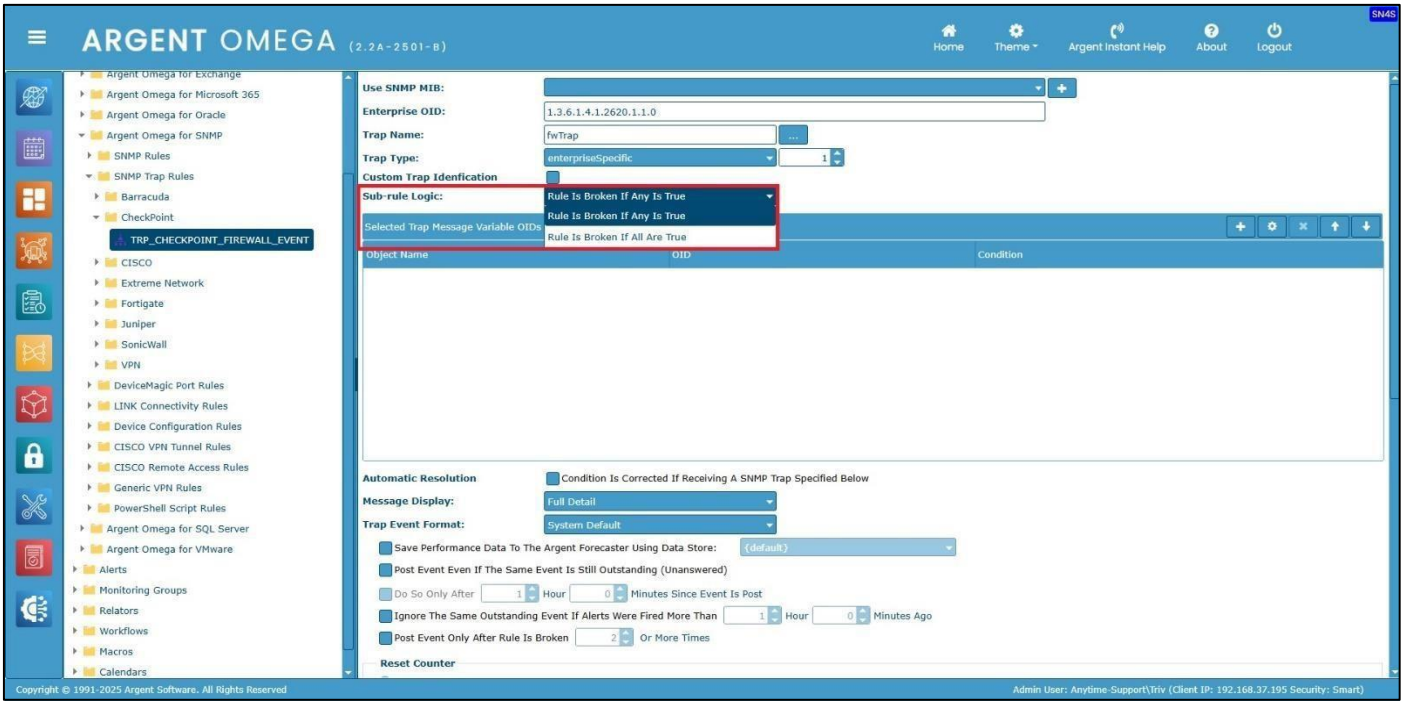
Specify trap Enterprise OID in **Enterprise OID** field.

Whenever an SNMP Trap is sent, it includes an Enterprise OID. This includes the manufacturer ID, and perhaps a particular class or section of traps related to the sending application.

For example, if a server running Dell OpenManage detects a power supply failure, it can send a trap to Argent. The Enterprise OID will start with ".1.3.6.1.4.1.674.10892.1". In this example, "674" is Dell's manufacturer ID, and "10892" is part of OpenManage.

Traps can be filtered by specific trap names and types. Specify **Trap Name** and **Trap Type** to define the Trap filter. This differentiate between trap events – to distinguish between a trap indicating a power supply failure and a trap showing a fan was inserted more specific information is needed. Otherwise, any trap with a specified Enterprise OID would create the same alert. Trap Name can also be browsed and selected from selected MIB file.

Rule broken logic can be selected from **Sub-rule Logic** combo box:

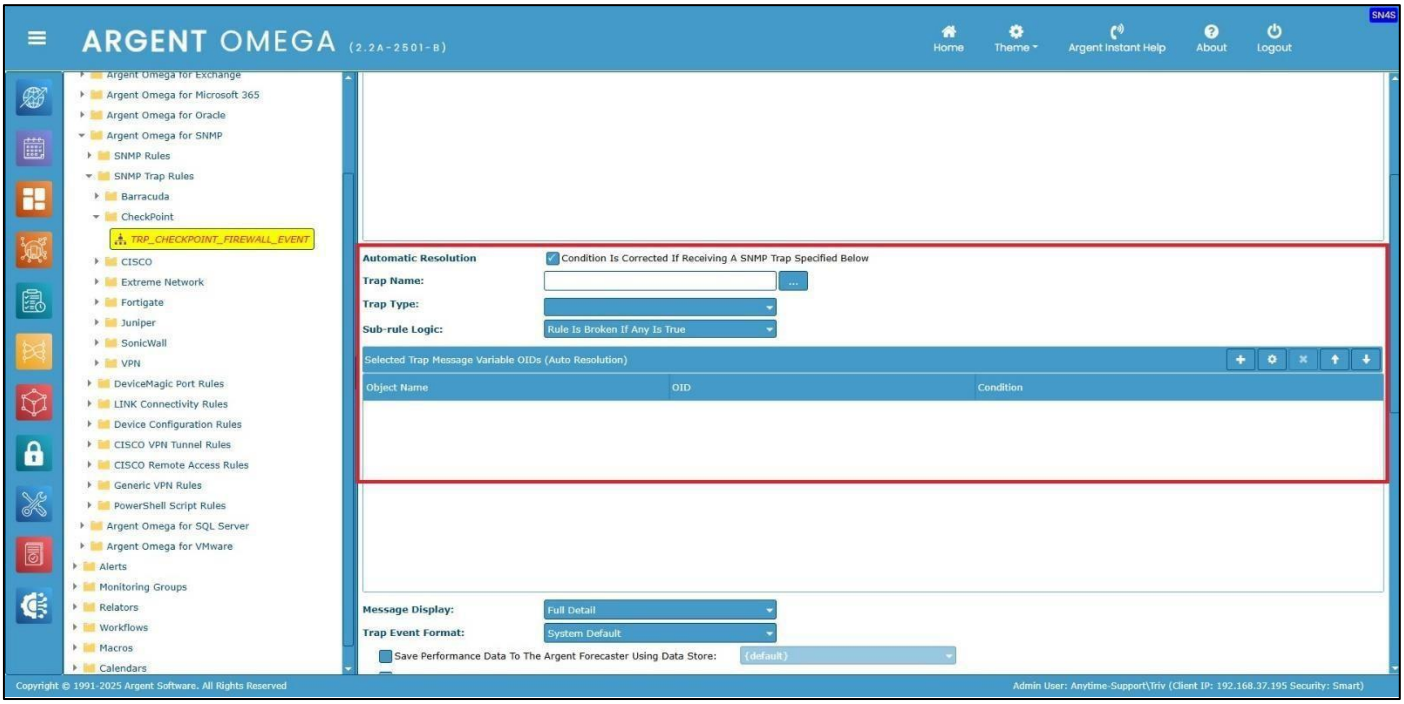


A sub-rule condition can be added by clicking the “**+**” button. A sub-rule definition dialog will pop up, where the rule condition can be defined. Sub-rule conditions should be added in the same way as in SNMP rules.

Condition Is Corrected If Receiving A SNMP Trap Specified Below option can be used to trigger a condition corrected event when receiving a specific SNMP trap.

In many cases, one SNMP Trap is effectively canceled out by another SNMP Trap. For instance, if the power fails trap is sent; then the UPS kicks in and a different trap is sent.

If utility power is restored (hopefully before the battery dies), the UPS could send a trap indicating as such. Argent can be configured to mark the event generated by the "**on battery**" trap when the "**back on normal power**" trap comes through. Check the option **Condition Is Corrected If Receiving A SNMP Trap Specified Below**, then define the Trap Enterprise OID List and Trap SNMP Filter sections in the same way as above, but with the settings for the "**normal power**" trap.

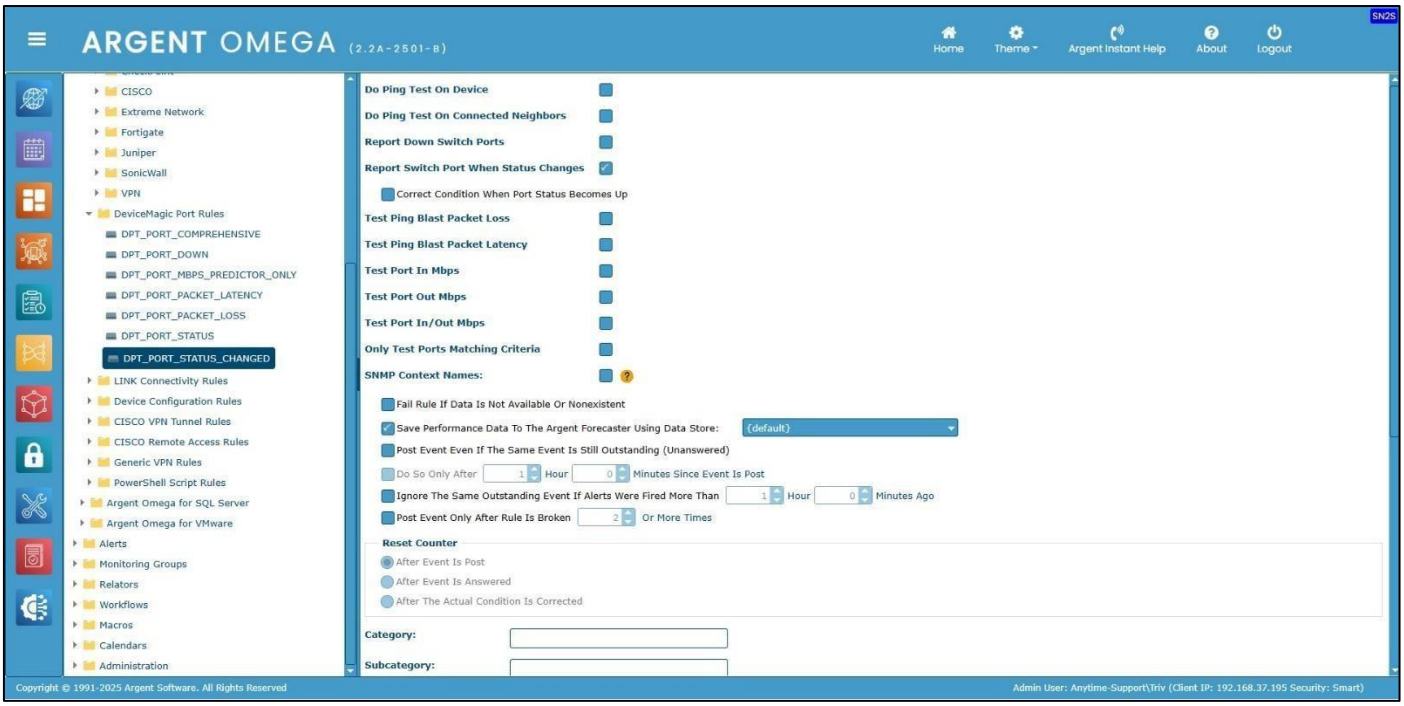


DeviceMagic Port Rules

DeviceMagic Port Rules monitors the switches without dealing with individual, explicit MIBs and OIDs.

DeviceMagic Port Rules monitors the following for switch host as well as individual ports:

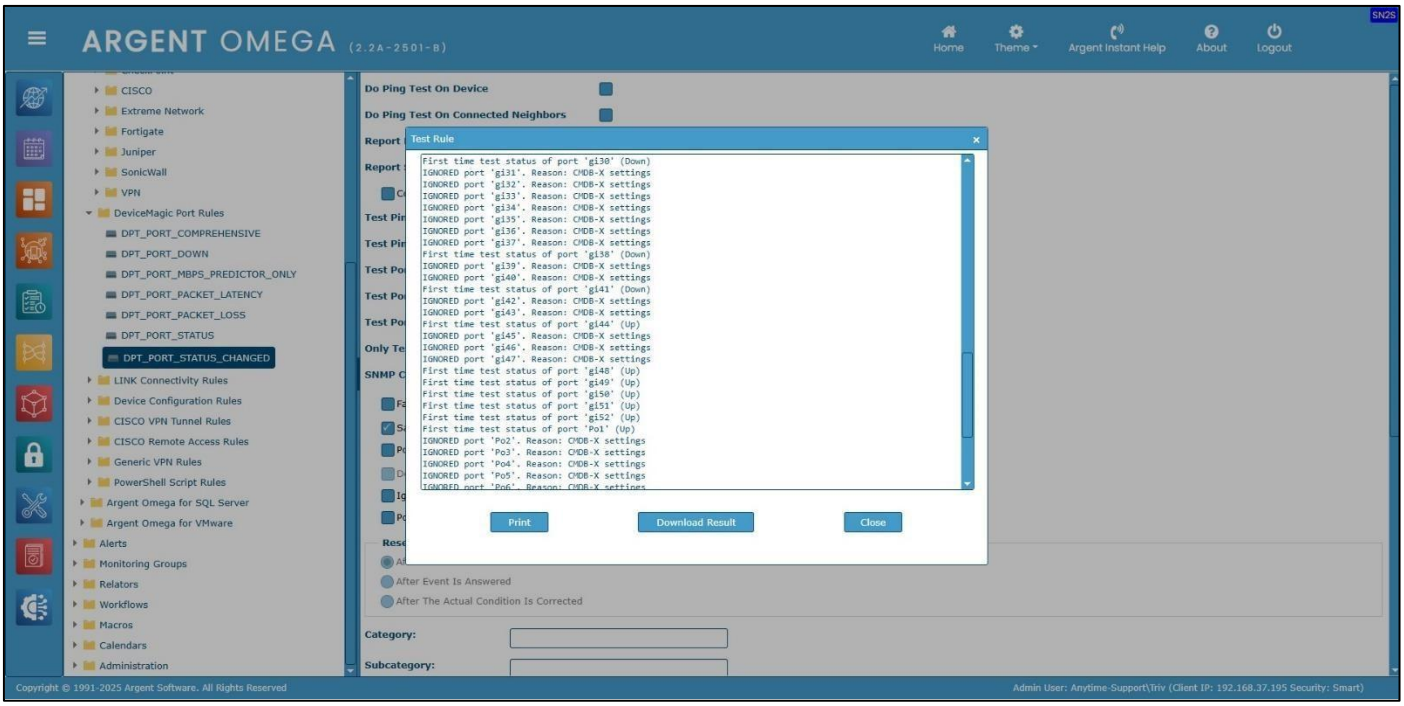
- Up/Down Status
- In/Out Bandwidth Usage (MBPS)
- Packet Latency and Packet Loss



Check the option **Do Ping Test On Device** to check the connectivity of a SNMP device by doing a Ping test.

Check the option **Do Ping Test On Connected Neighbors** to check the connectivity of neighbor switches connected to a switch by doing a Ping test.

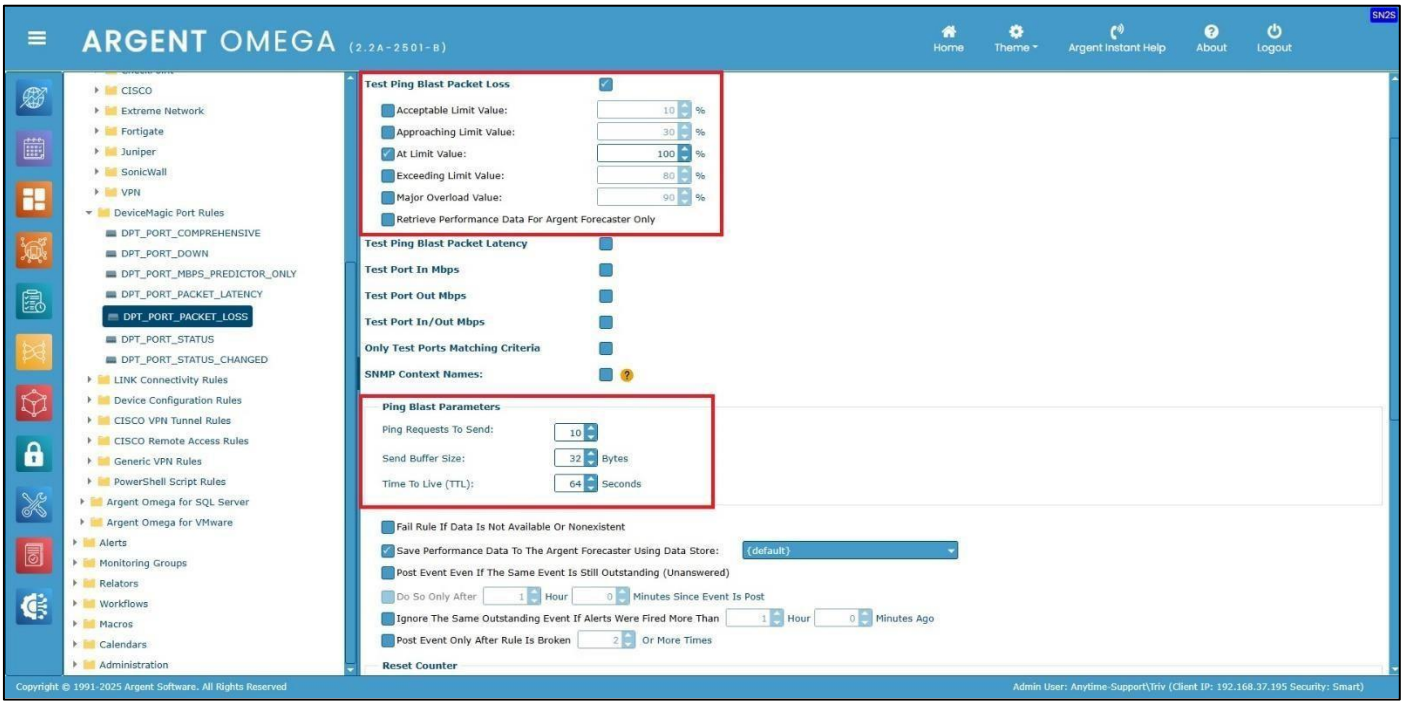
Check the option **Report Down Switch Ports** to Alert when the status of any switch port is down. Sample Rule execution result is below:



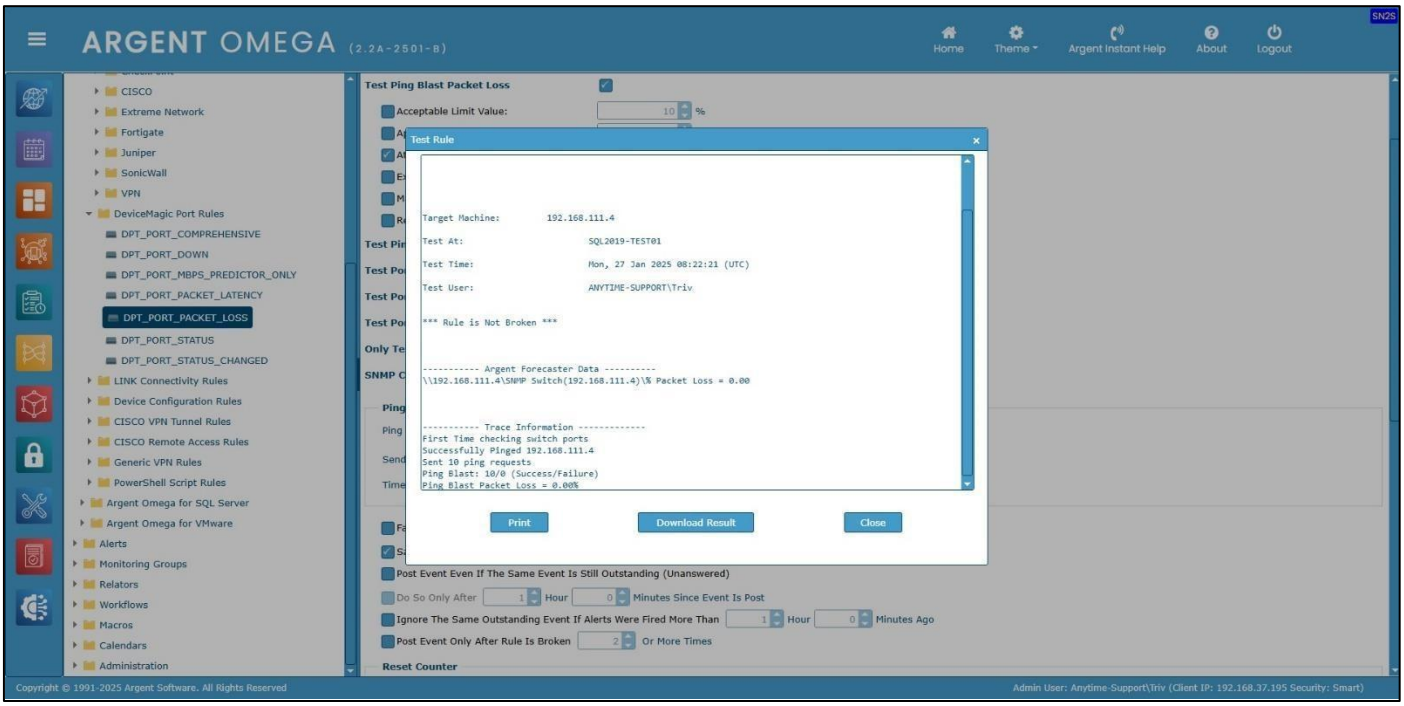
Check the option **Report Switch Port When Status Changes** to Alert when the status (Up or Down) of any switch port is changed.

Check the option **Test Ping Blast Packet Loss** to check packet loss (%) for a device connected to each port of SNMP managed switch. The packet loss % threshold value needs to be configured. Also, the ping blast parameters, such as number of ping requests, packet buffer size and Time To Live (TTL), need to be configured.

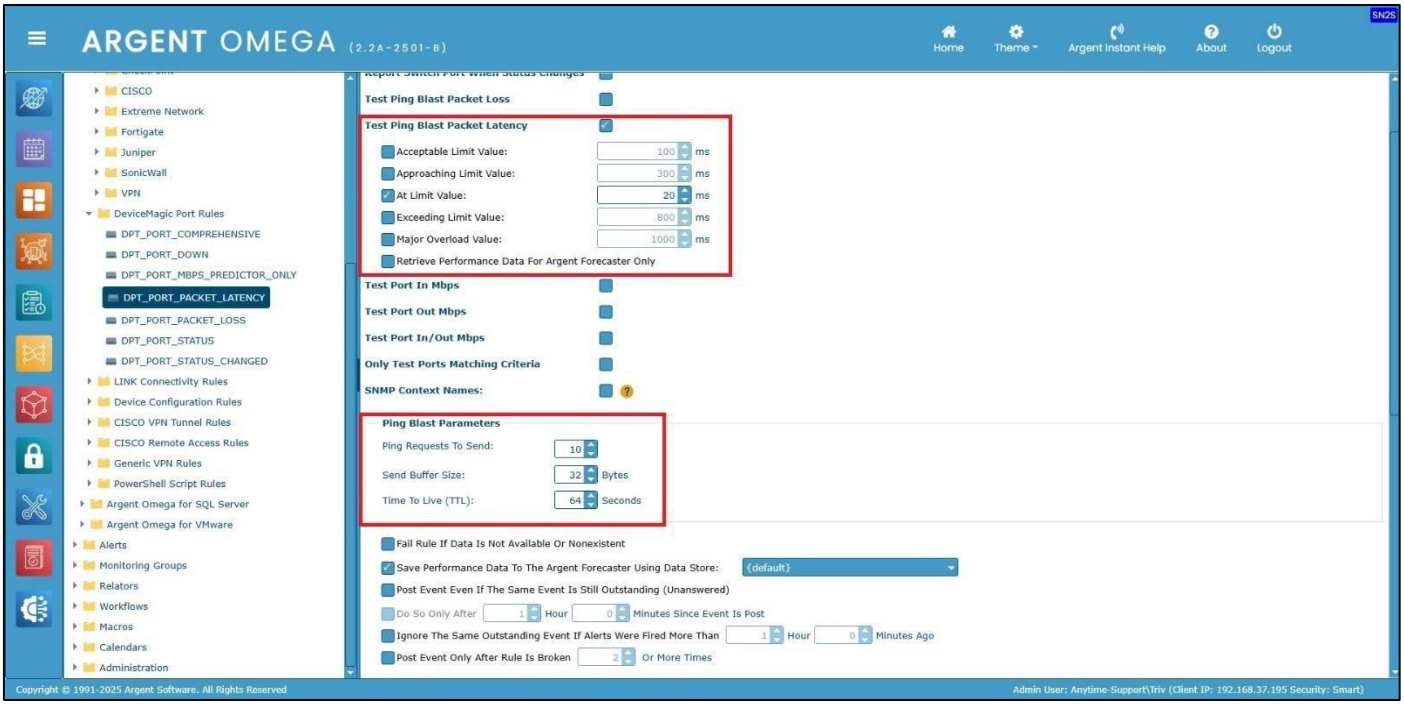
Time To Live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router.



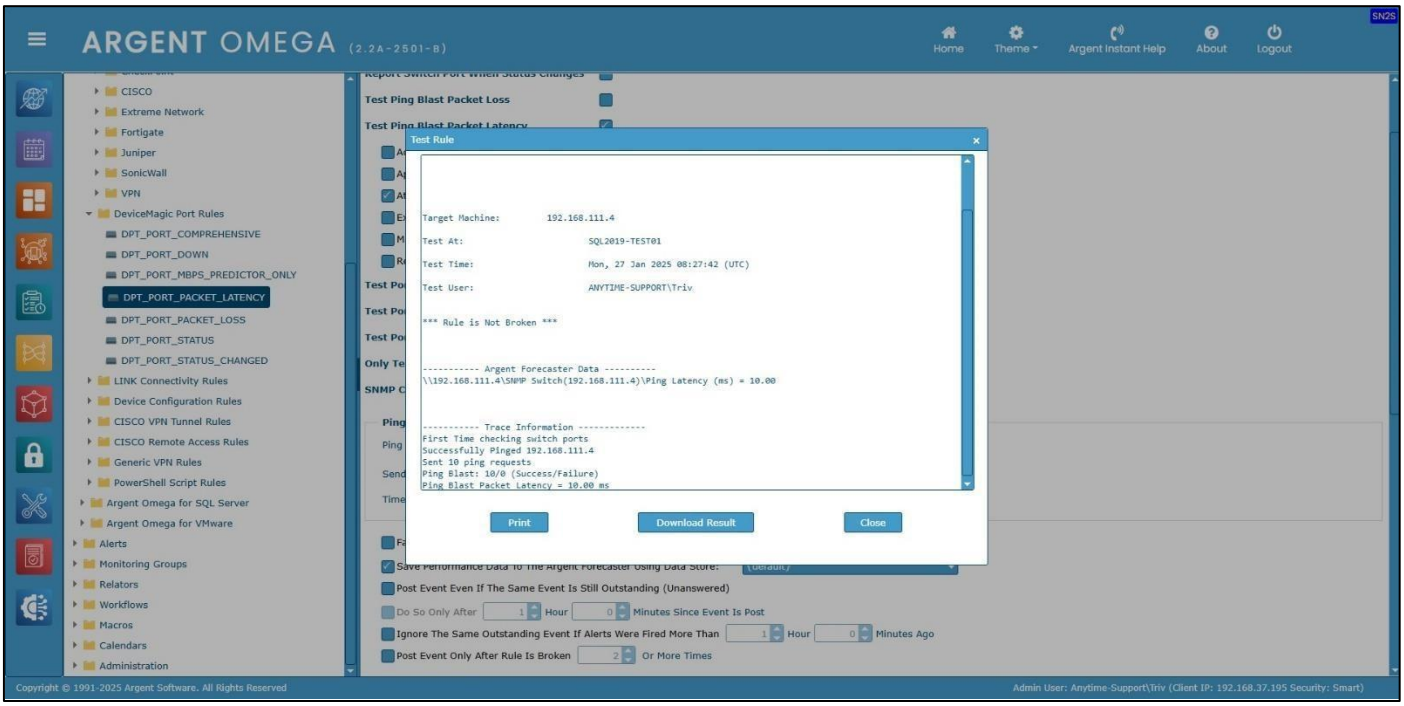
The following is a sample Rule:



Check the **Test Ping Blast Packet Latency** option to check the packet latency in milliseconds for a device connected to the port of SNMP managed switch. The packet latency milliseconds threshold value needs to be configured. Also, the ping blast parameters, such as number of ping requests, packet buffer size and Time To Live (TTL), also need to be configured. Time To Live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router.

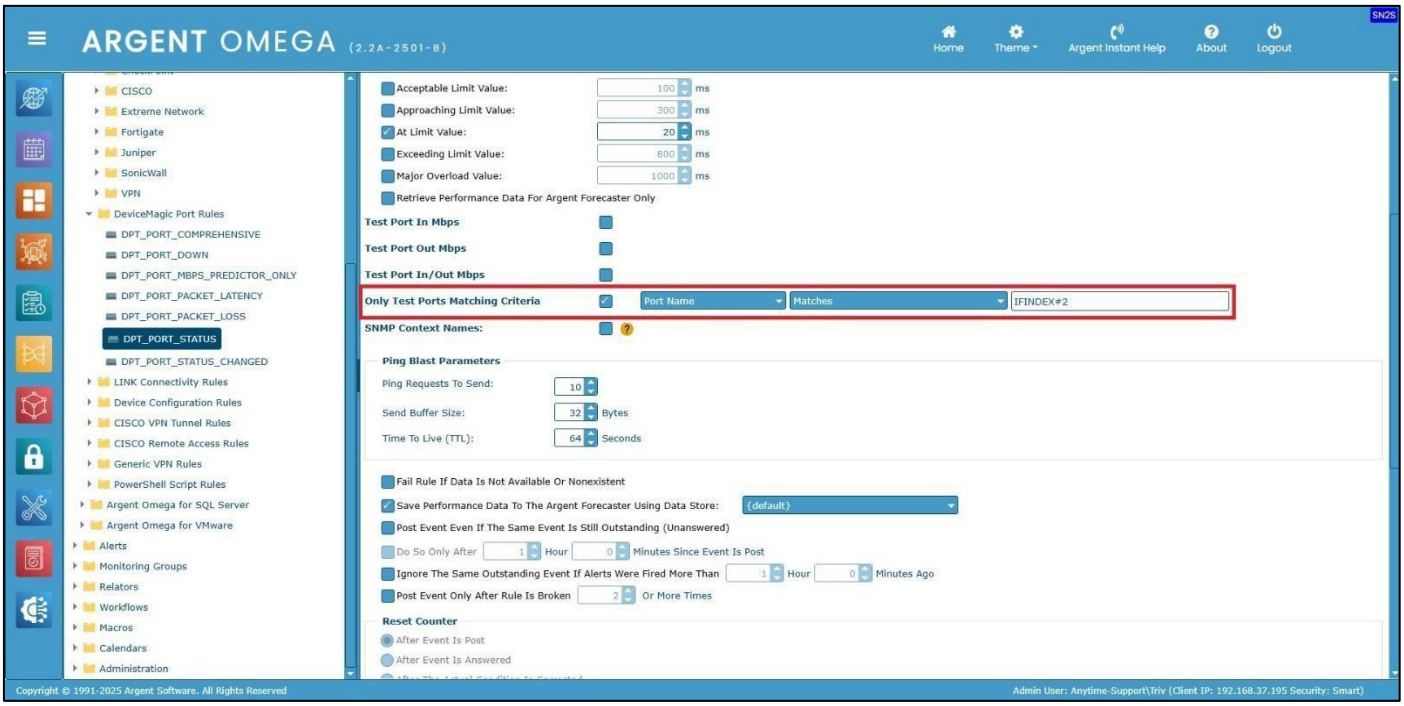


And the Rule result looks like the following:

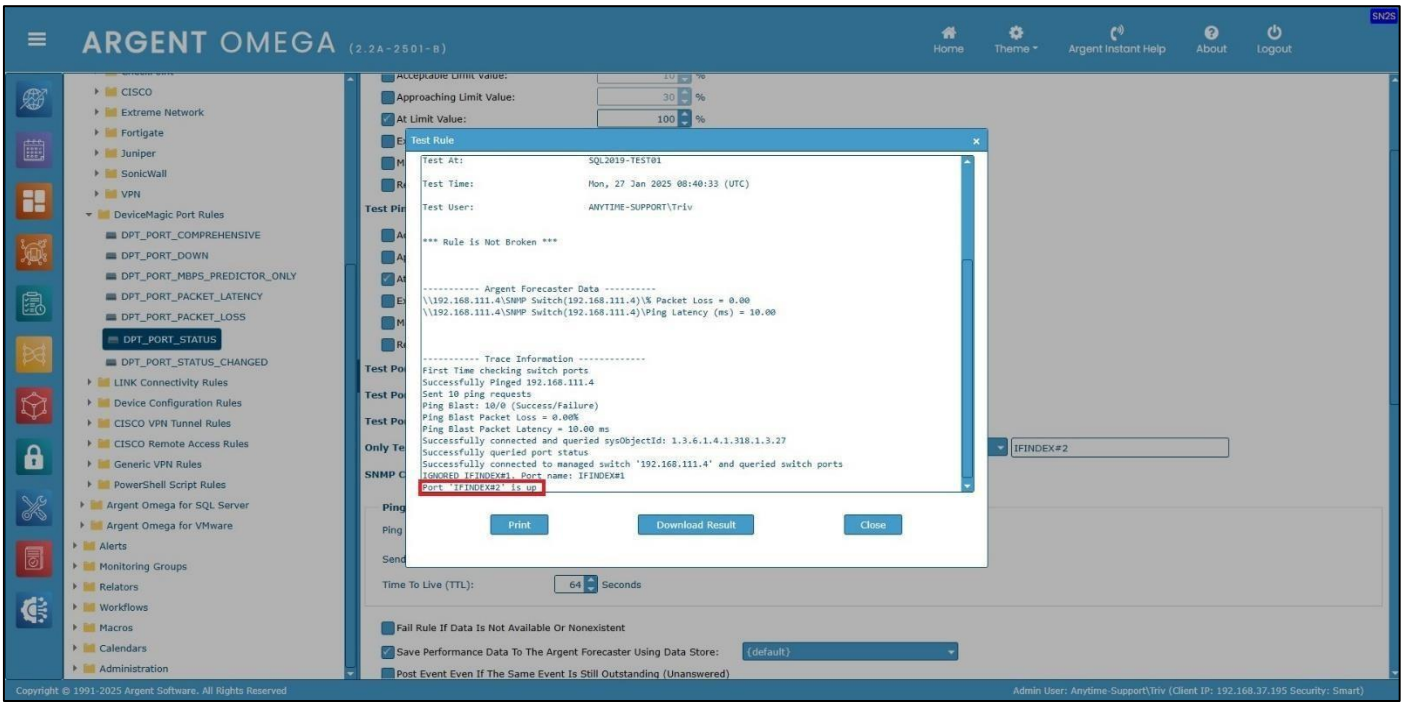


Use options **Test Port In Mbps**, **Test Port Out Mbps** and **Test Port In/Out Mbps** to test a switch port's In and Out bandwidth usage.

Use option **Only Test Ports Matching Criteria** to check the switch ports that match specified criteria.

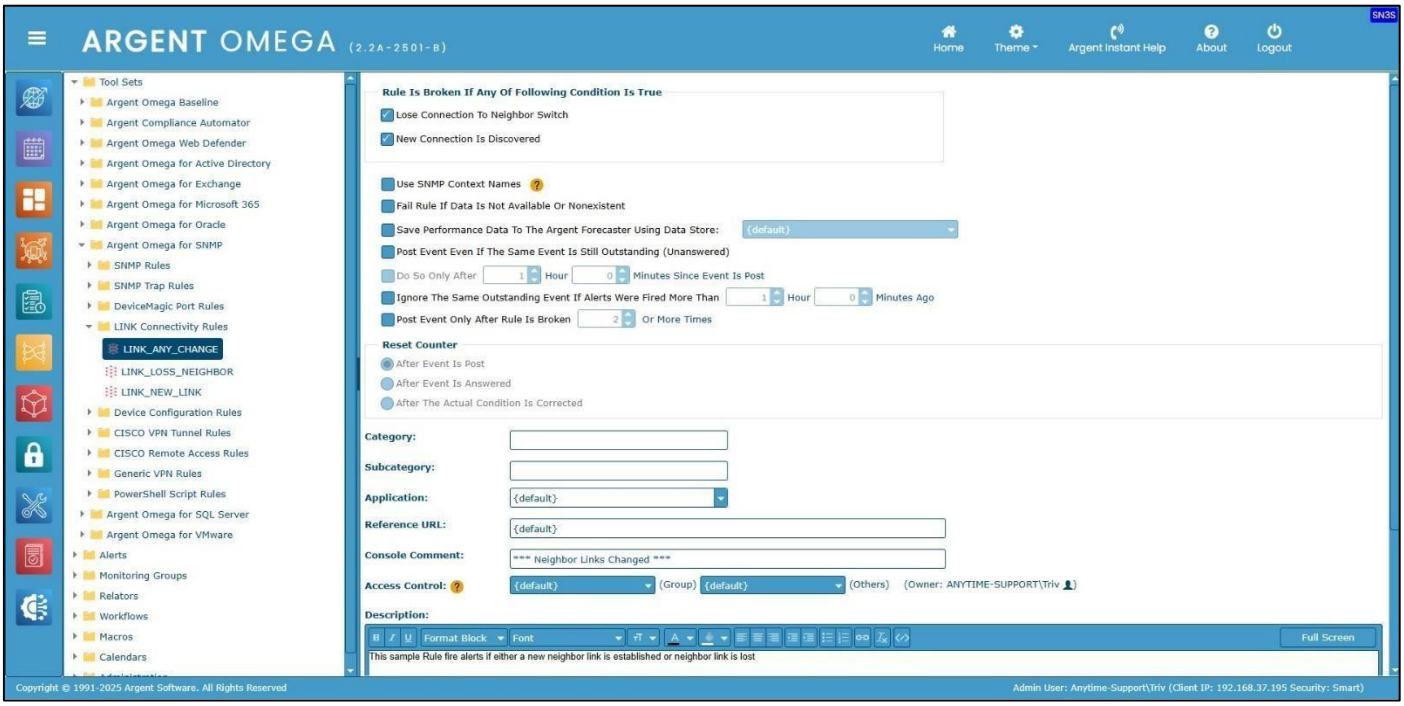


And the Rule result looks like below:



LINK Connectivity Rules

These Rules fire alerts if either a new connection to a neighbor switch is established or an existing neighbor switch connection is lost.



Check the option **Lose Connection To Neighbor Switch** to fire and Alert if the connection to an existing neighbor switch is lost.

Check the option **New Connection Is Discovered** to fire an Alert if a new neighbor switch connection is established.

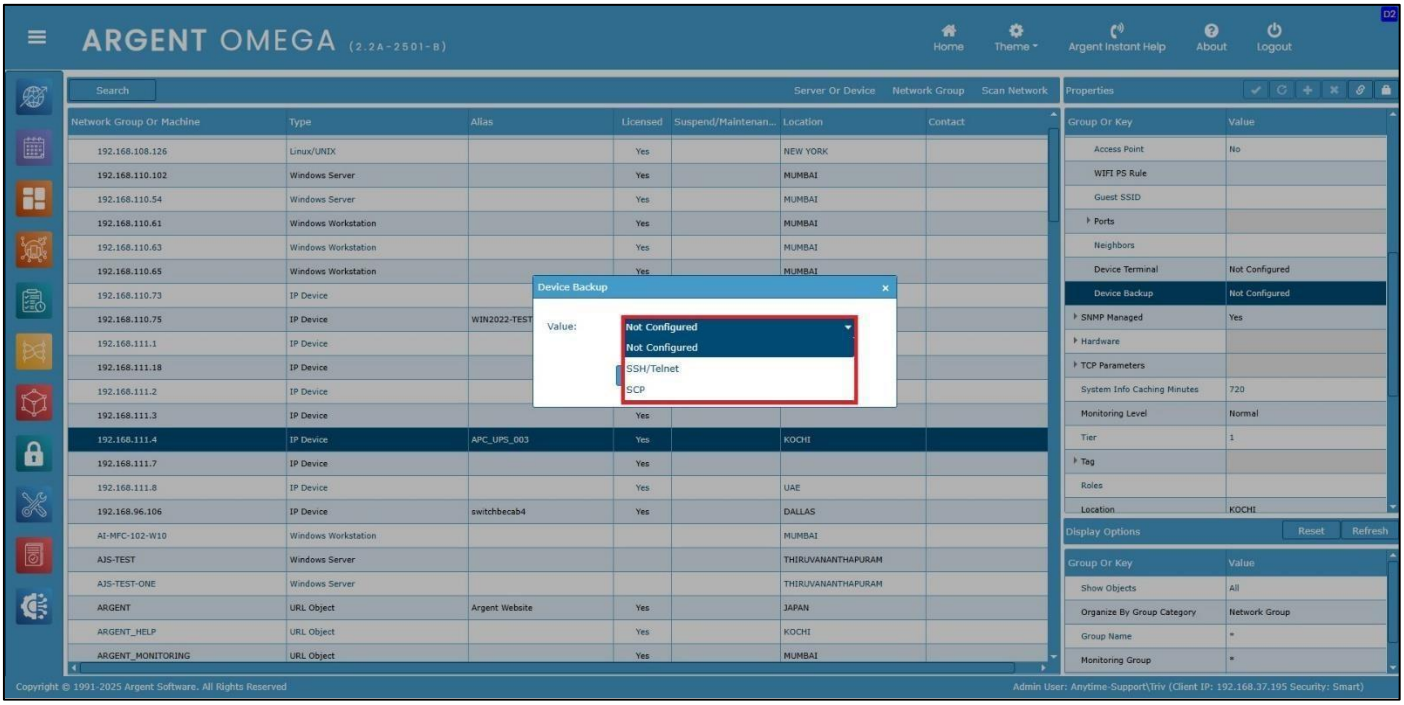
Device Configuration Rules

Cisco and **Cisco-like** devices can be configured to allow the execution of the **show running-config** or **show run** commands. These commands compile the current configuration and dump out to terminal.

This facility uses the same mechanism to back up the device's configuration to the central Argent SQL database. Customers can then view all the versions that have been backed up.

This new facility is a completely automated control and patch management solution for all Cisco and Cisco-like devices.

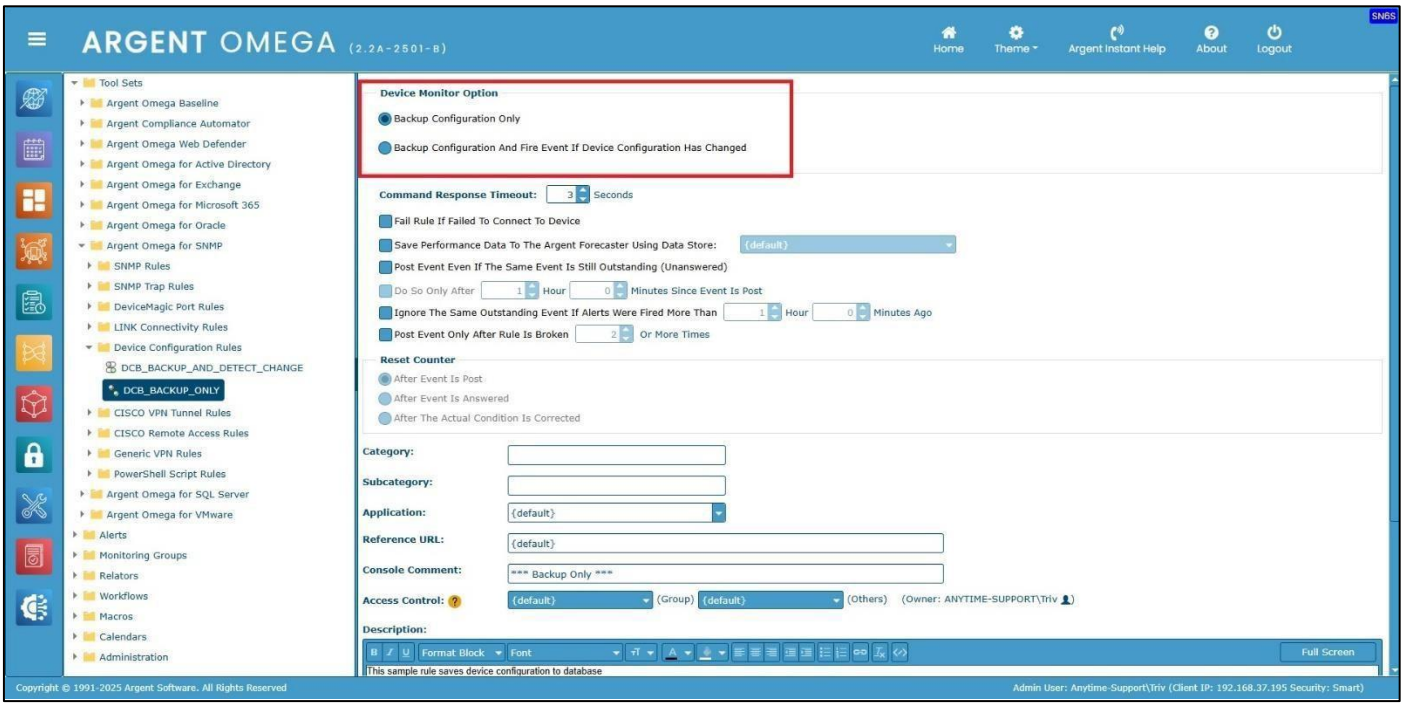
The device backup can be configured in the CMDB-X section.



Select the protocol and click OK. The following highlighted CMDB-X properties need to be configured:

For more details about device backup configuration please refer the Argent KBI
https://help.argent.com/Article/1748

Argent Omega for SNMP Tool Sets contains Device Configuration Rules to backup and monitor the configuration changes.



Choose **Backup Configuration Only** option to back up the device's configuration to the Argent SQL database.

Choose **Backup Configuration And Fire Event If Device Configuration Has Changed** option to backup and fire Alert for configuration changes.

CISCO VPN Tunnel Rules

Merely deploying a Virtual Private Network (VPN) alone does not guarantee smooth IT operations -- constantly monitoring of VPN connections (VPN Tunnel Monitoring) for possible bandwidth constraints and security threats is needed.

Argent Omega can show the full picture of VPN activities, including:

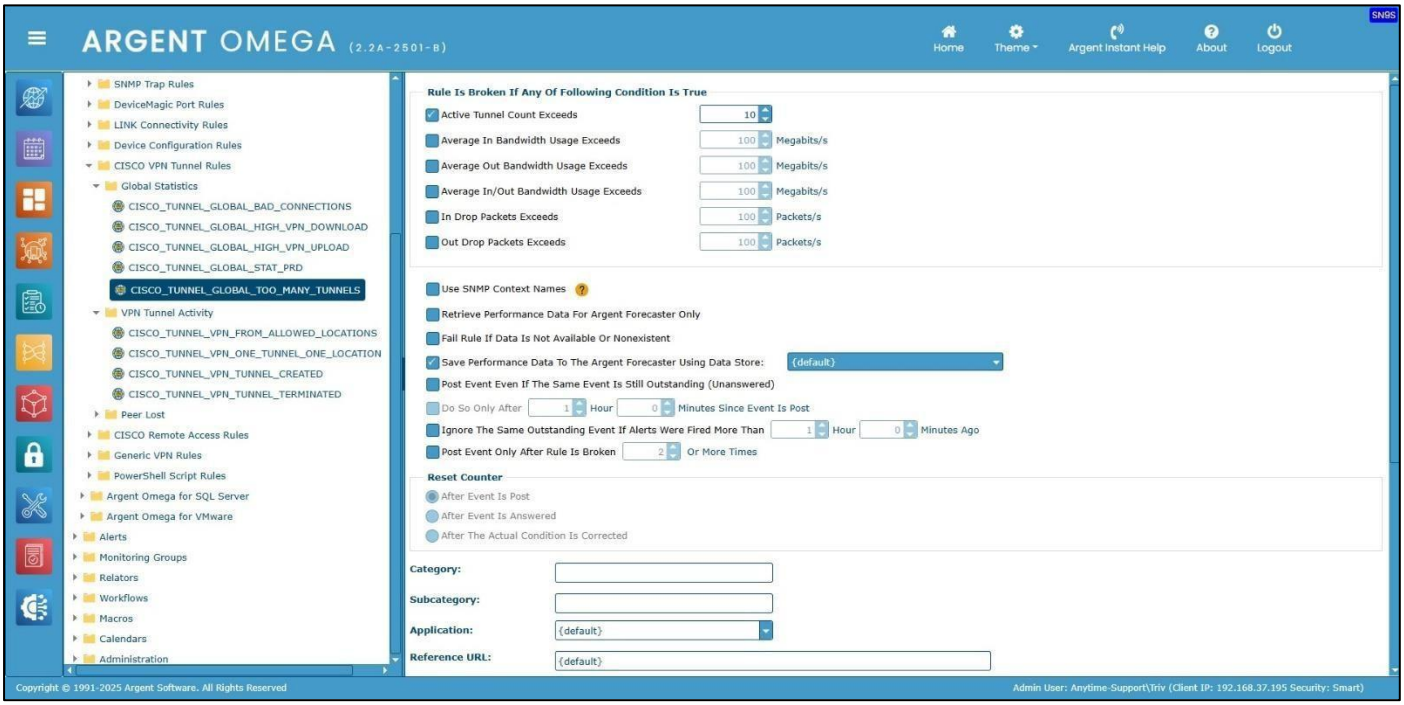
- Who – logon user
- Where – remote IP and geolocation of city, region, and country
- When – start time, end time, and duration of the VPN session
- What – protocol, in/out total bytes, and calculated bandwidth usage

Argent Omega offers the following set of Rules to monitor CISCO VPN Tunnels:

Global Statistics Rules

Configure Global Statistics Rules to monitor the following parameters:

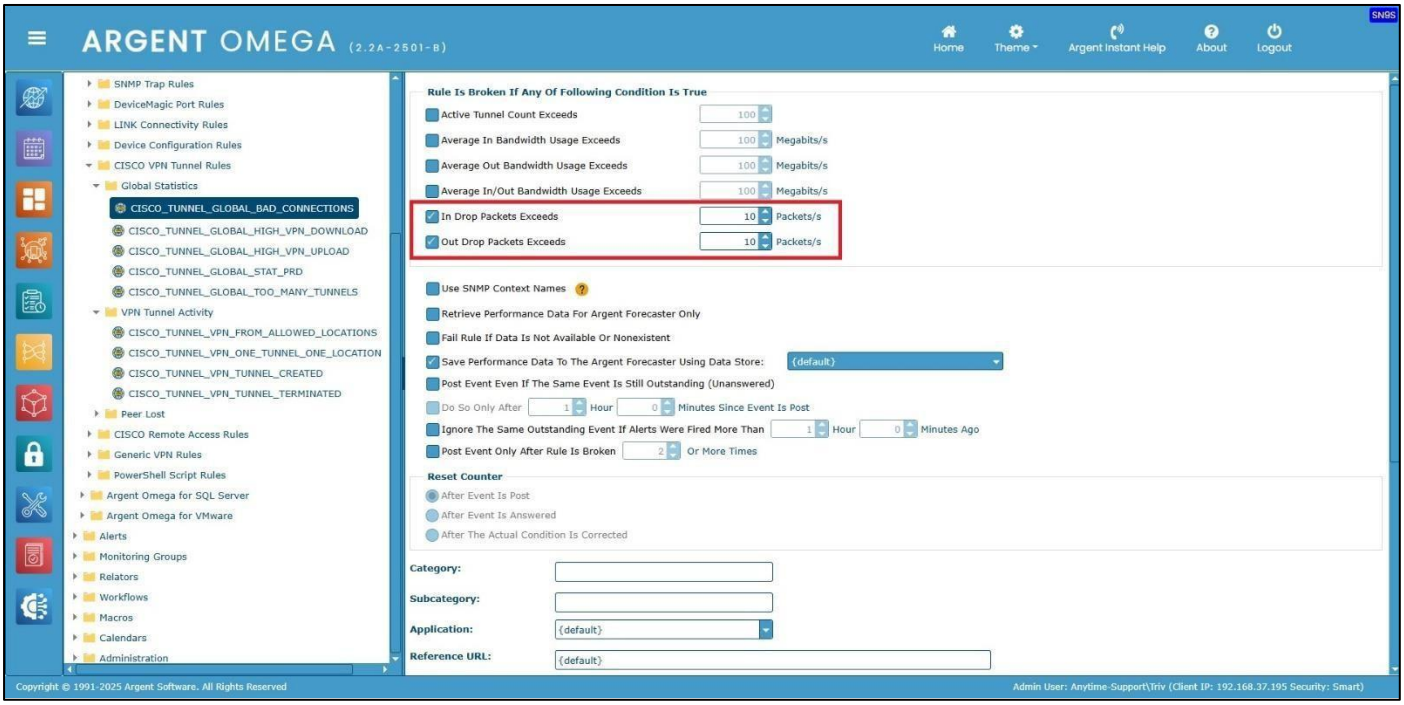
- Site-to-Site VPN tunnel count
- In/Out Bandwidth Usage
- Bad VPN connections and connections that drops too many packets



Check **Active Tunnel Count Exceeds** option to alert if Site-to-Site VPN tunnel count exceeds specified threshold.

Use options **Average In Bandwidth Usage Exceeds**, **Average Out Bandwidth Usage Exceeds** and **Average In/Out Bandwidth Usage Exceeds** to monitor the bandwidth usage.

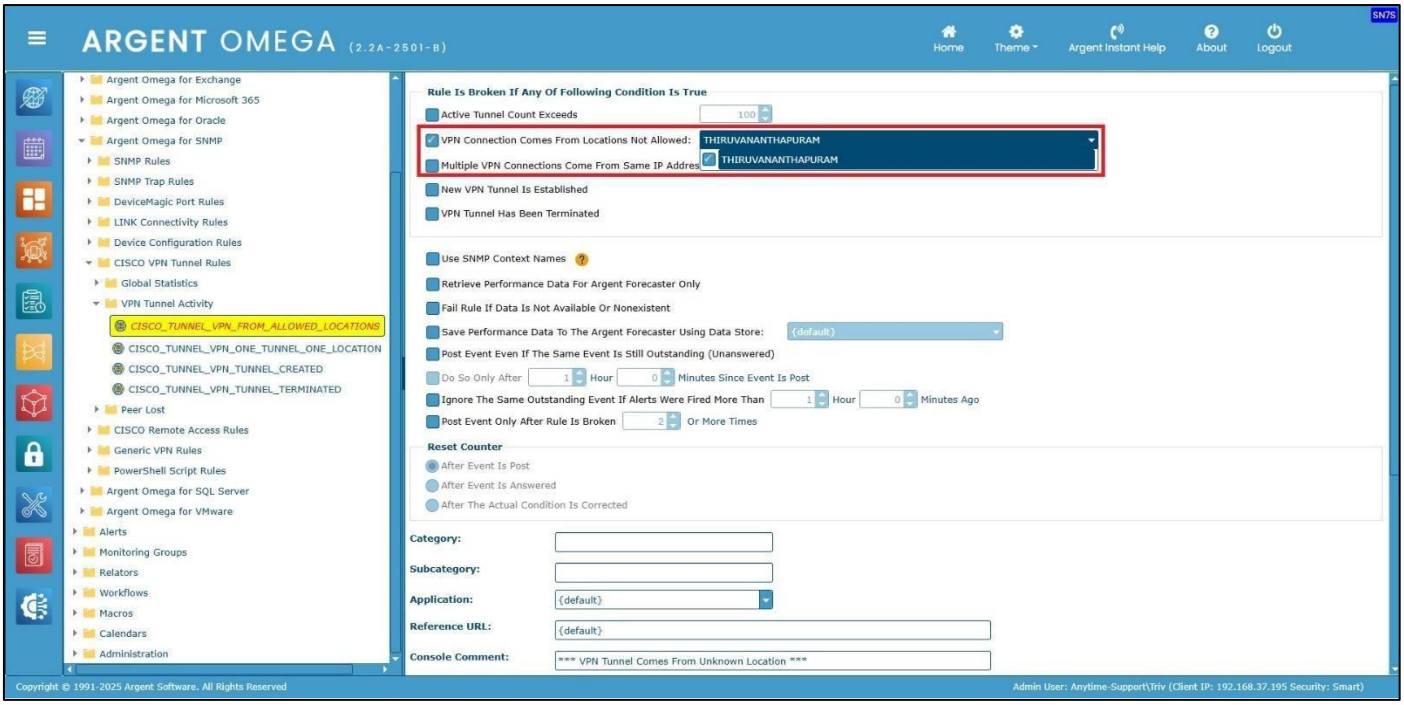
Use options **In Drop Packets Exceeds** and **Out Drop Packets Exceeds** to monitor the VPN connections dropping too many packets.



VPN Tunnel Activity Rules

Configure VPN Tunnel Activity Rules to alert for the following VPN activities:

- New VPN connection created
- Existing VPN connection terminated
- VPN connection coming from location that should have no employees working
- Multiple connections coming from the same remote IP, which is unusual unless both residents work for the same company



Check **VPN Connection Come From Locations Not Allowed** option to alert if VPN connection comes from specific locations. Locations need to be selected from the combo box.

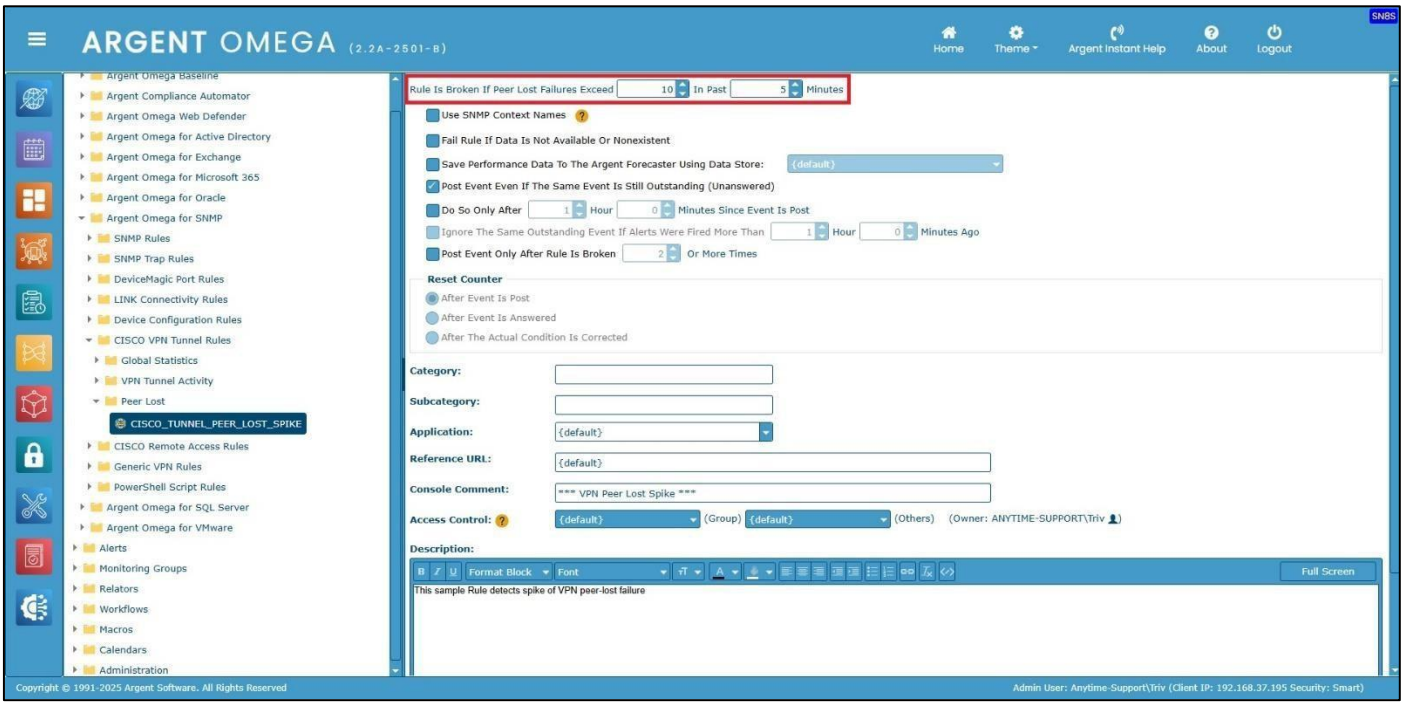
Check **Multiple VPN Connections Come From Same IP Address** option to alert if multiple VPN tunnels come from same IP address.

Check **New VPN Tunnel Is Established** option to alert when a new VPN tunnel is created.

Check **VPN Tunnel Has Been Terminated** option to alert when an existing tunnel is terminated.

Peer Lost Rules

This Rule monitors the connectivity health of Site-to-Site VPN Tunnels. A spike of peer lost errors indicates deteriorating network connections. Configure this to alert if the number of peer lost failures exceeds the threshold within a specific period.



Check the **Rule Is Broken If Peer Lost Failures Exceed** option and specify the threshold.

CISCO Remote Access Rules

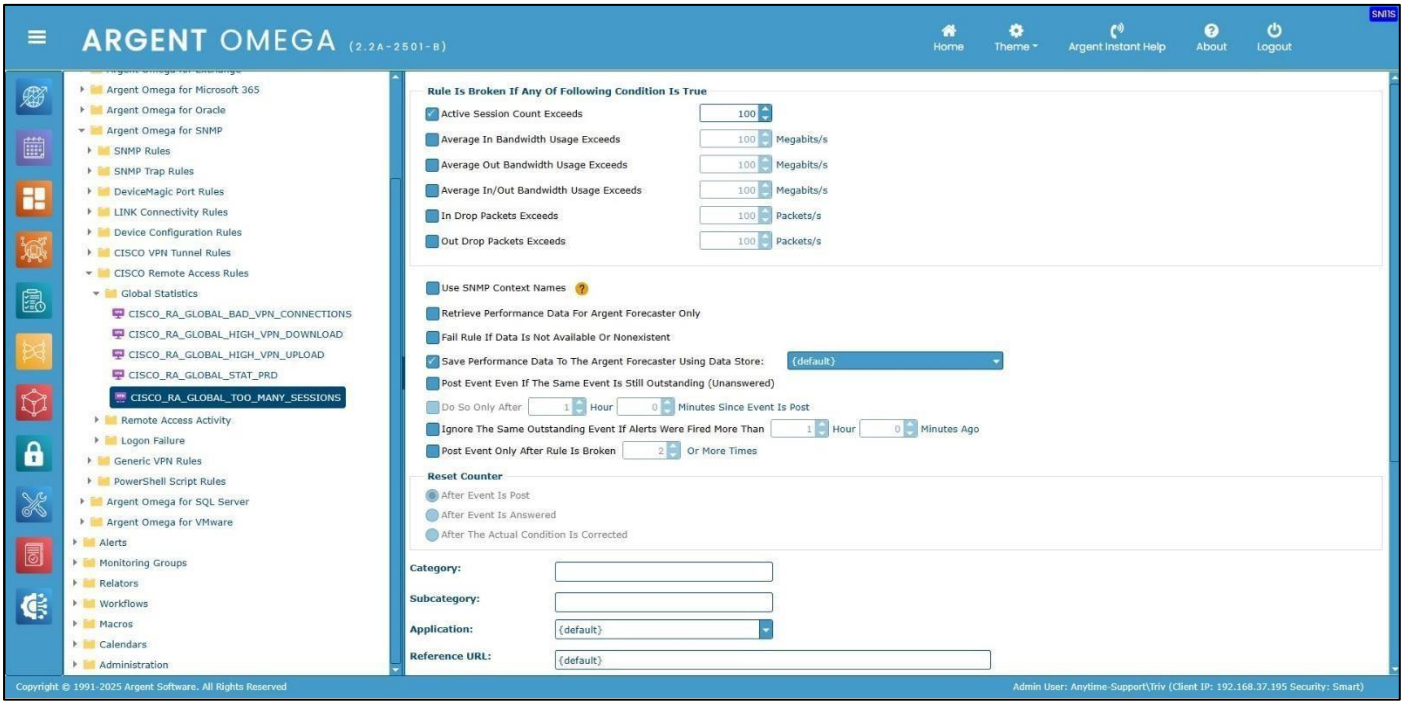
CISCO Remote Access enables tracking of all users connecting remotely to the organization's network, which is an important aspect of monitoring logins, logoffs, bandwidth usage, session duration, etc.

Argent Omega offers the following set of Rules to monitor remote access VPN users:

Global Statistics

Configure Global Statistics Rules to monitor following parameters of remote access VPN:

- Remote access VPN session count
- Bandwidth used by download over VPN
- Bandwidth used by upload over VPN
- Bad VPN connections and connections that drops too many packets



Check **Active Session Count Exceeds** option to alert if Site remote access VPN session count exceeds threshold.

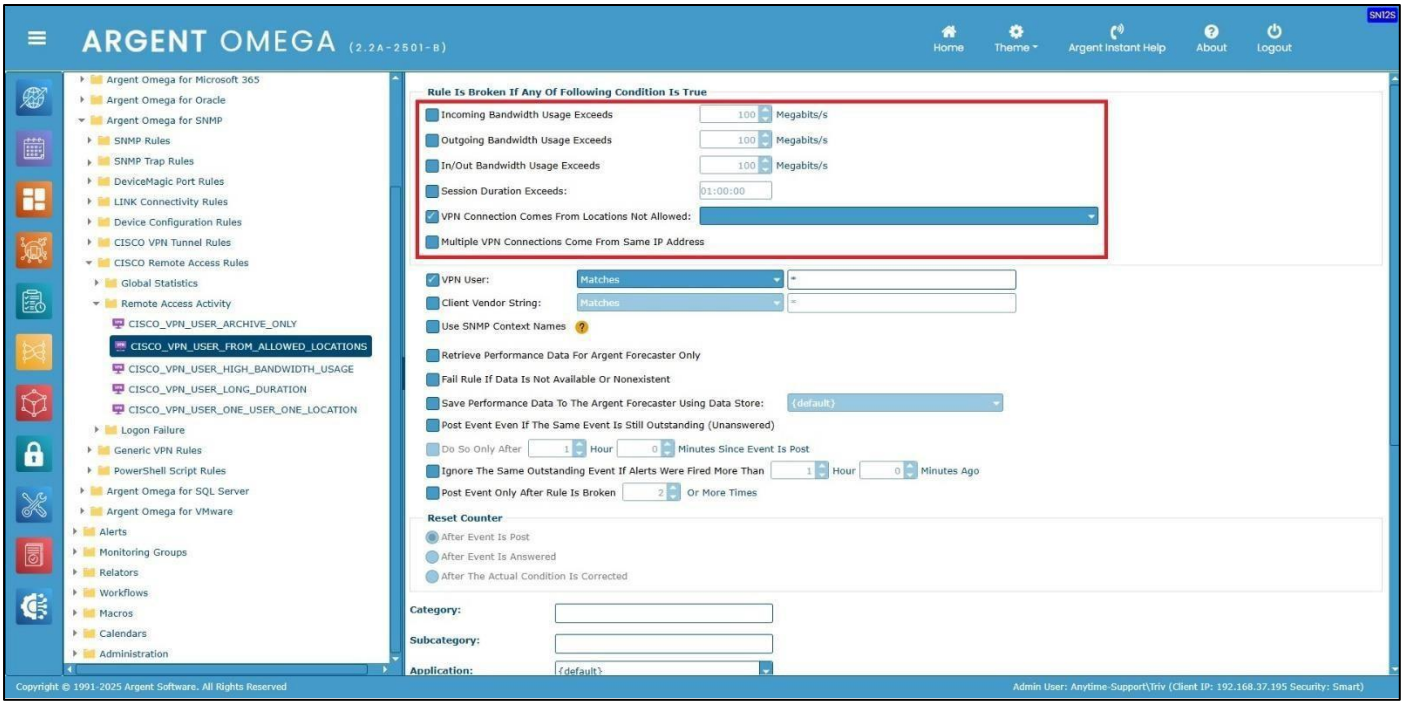
Use options **Average In Bandwidth Usage Exceeds**, **Average Out Bandwidth Usage Exceeds** and **Average In/Out Bandwidth Usage Exceeds to monitor the bandwidth consumptions.**

Use options **In Drop Packets Exceeds** and **Out Drop Packets Exceeds** to monitor the VPN connections that drop too many packets.

Remote Access Activity Rules

Configure Remote Access Activity Rules to Alert for the following VPN activities:

- Extreme bandwidth usage
- Very long duration (forgot to sign off?)
- VPN connection coming from location that should have no employees working
- Multiple connections coming from the same remote IP, which is unusual unless both residents work for the same company



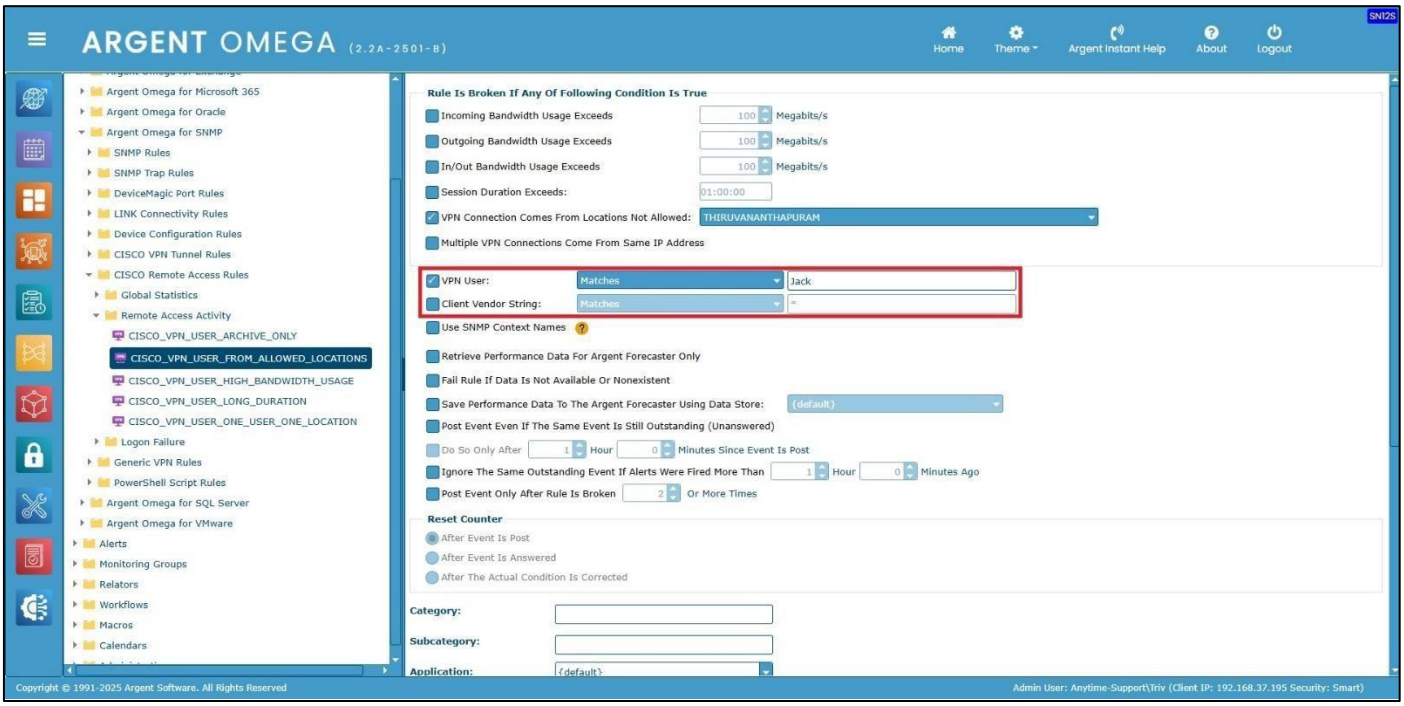
Use options **Incoming Bandwidth Usage Exceeds**, **Outgoing Bandwidth Usage Exceeds** and **In/Out Bandwidth Usage Exceeds** to monitor the extreme bandwidth usage.

Check **Session Duration Exceeds** option to Alert for sessions that exceed specified duration.

Check **VPN Connection Come From Locations Not Allowed** option to alert if VPN connection comes from specific locations. Locations need to be selected from the combo box.

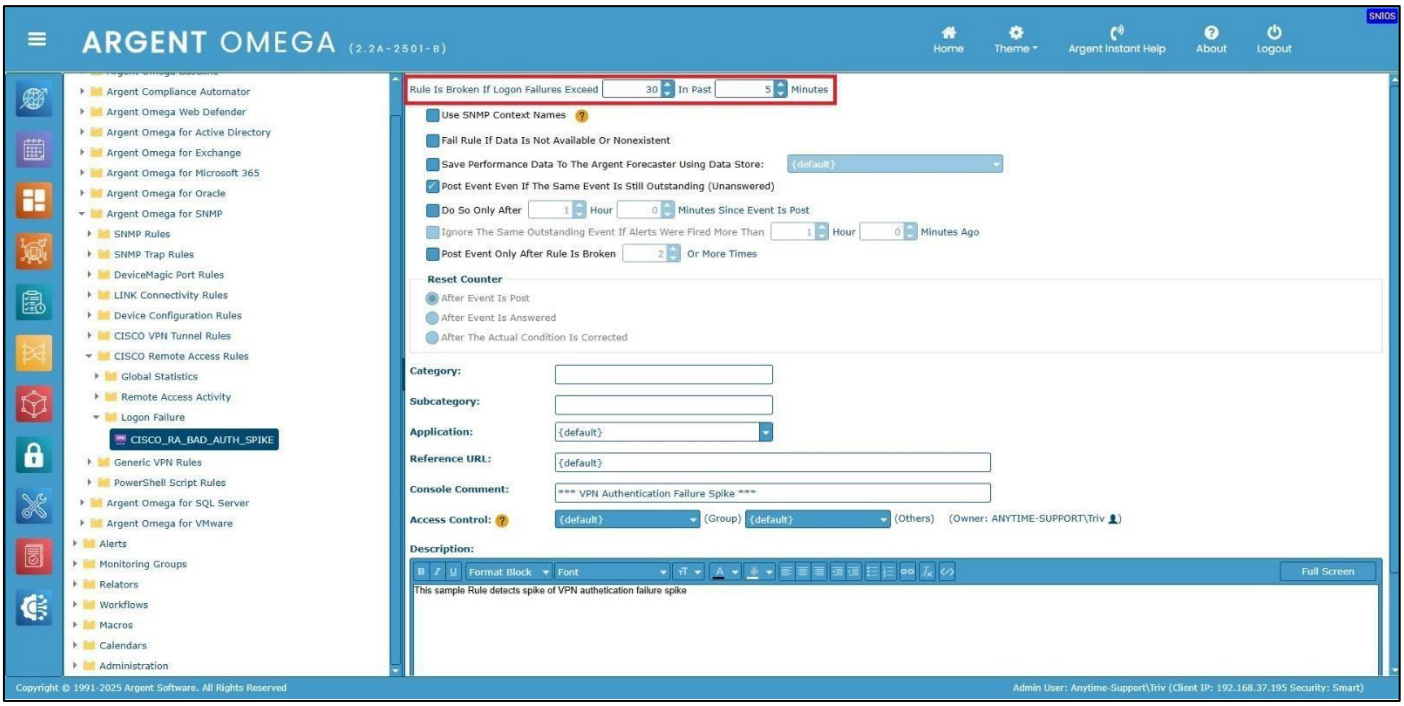
Check **Multiple VPN Connections Come From Same IP Address** option to alert if multiple VPN tunnels come from same IP address.

The Rule provides the options to filter the sessions of specific **VPN User** and **Client Vendor String**.



Logon Failure Rules

This Rule detects spikes of VPN logon failures, which could indicate ongoing hacking activity.



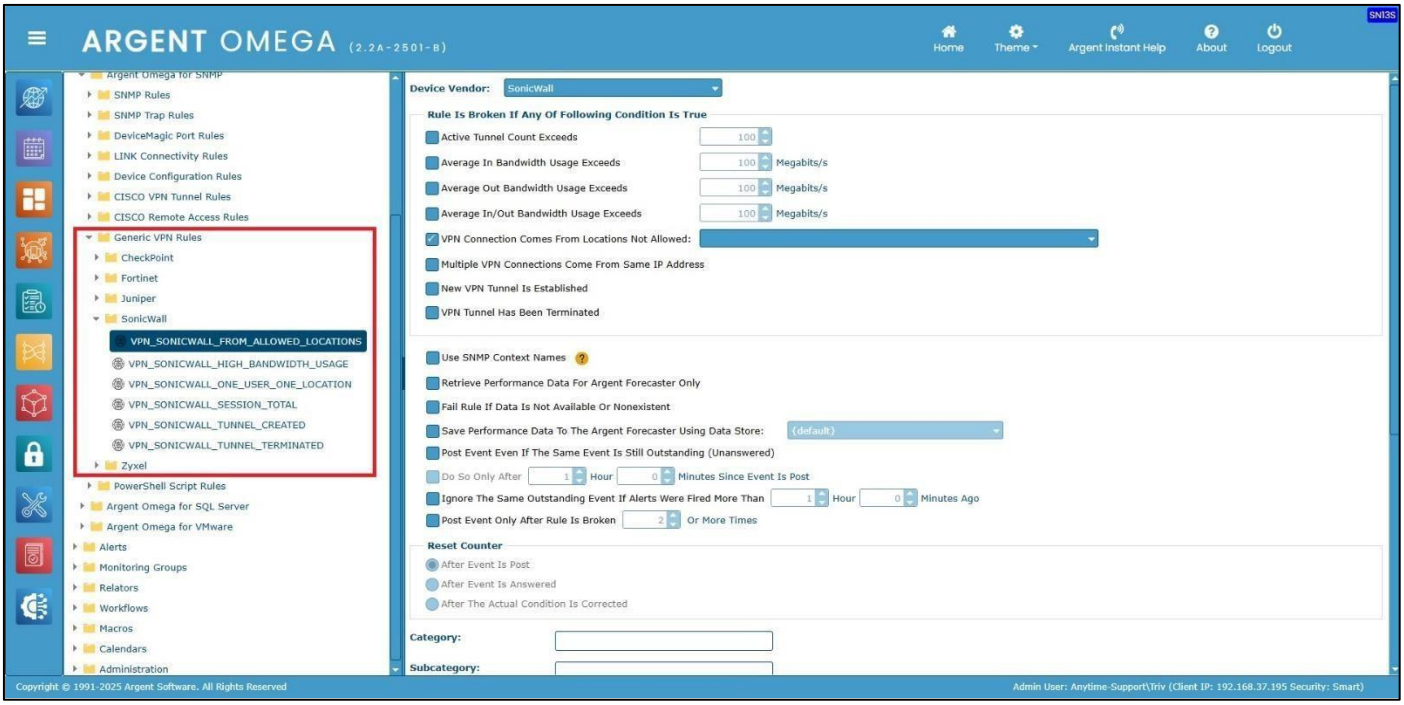
Generic VPN Rules

Argent Omega for SNMP provides a set of Generic VPN Rules that target any non-CISCO VPN devices. The following vendors are supported out of the box:

- Check Point
- Fortinet
- Juniper
- SonicWall
- Zyxel

The Rule gathers common performance metrics, such as total tunnels and in/out bandwidth usage. More importantly, it provides unique security features for real-time alerts for potential hacking:

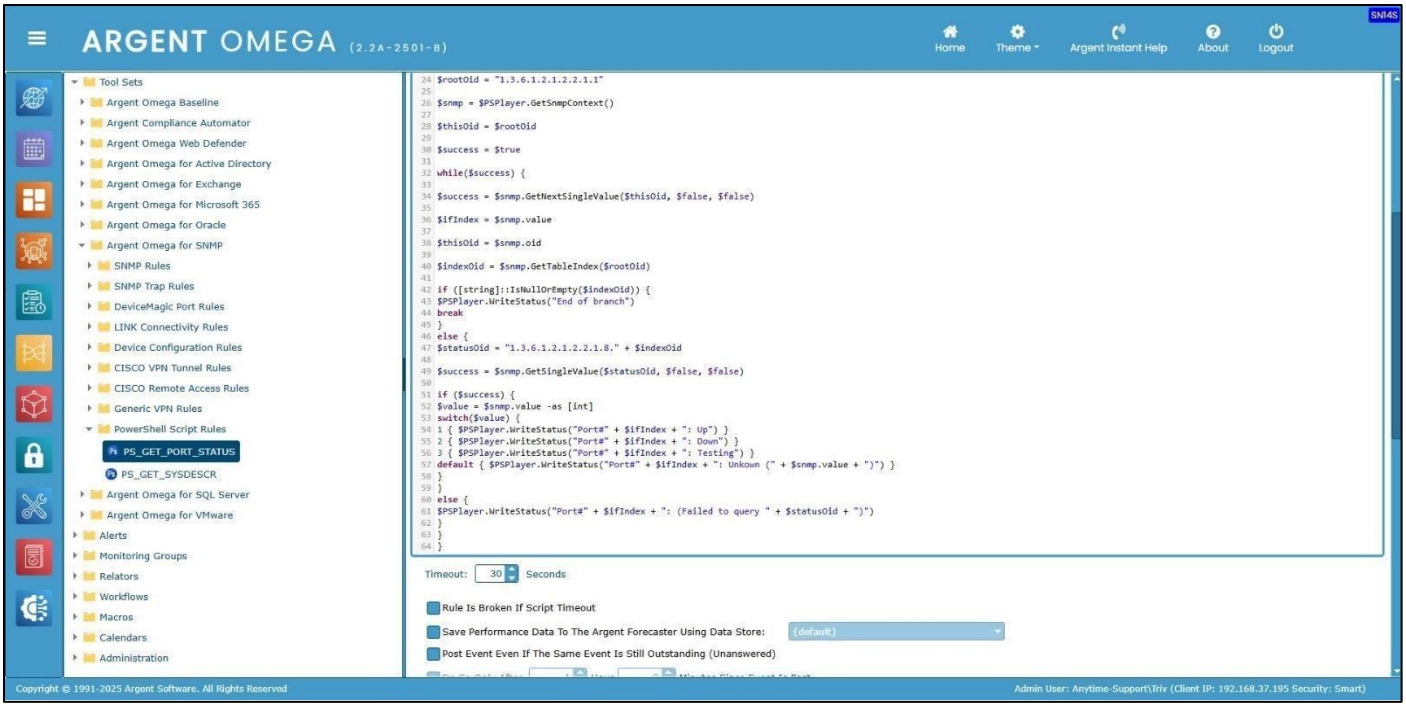
- VPN tunnel creation
- VPN tunnel termination
- VPN connection coming from locations that should have no employees working
- Multiple connections coming from the same remote IP, which is unusual unless both residents work for the same company



PowerShell Script Rules

This Rule allows the creation of custom PowerShell scripts to monitor SNMP-enabled devices. Two built-in Rules are available to demonstrate this:

- How to enumerate SNMP OID table using PowerShell Script



- How to read a single SNMP device metric using PowerShell Script