Argent for SNMP

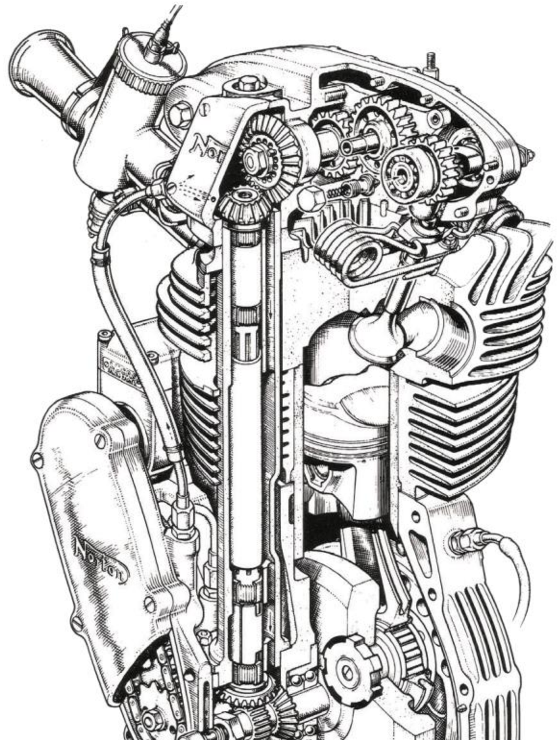


Table Of Contents

Introduction

In today's complex network of switches, routers and servers, managing all these devices can be painful. Eventually, the network begins to have issues and slows down. It is critical for the system administrator to keep an eye on the entire network.

Most of the devices on the network support the network management protocol, allowing network devices to share management information more easily. There are various protocols available to support network management, including the popular Simple Network Management Protocol (SNMP), which comes pre-bundled with SNMP agents for most network devices.

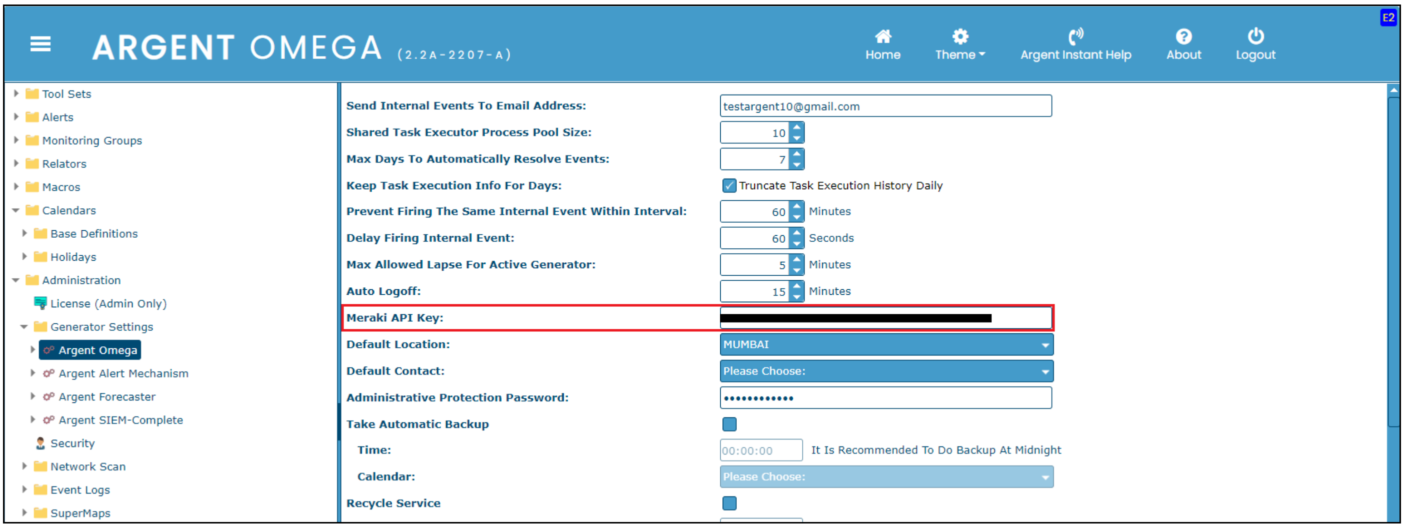
Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).

Argent Omega for SNMP can communicate with network devices, despite having different hardware and software, allowing network administrators to track network performance, diagnose and manage network faults, and plan network capacity and growth.

Argent Omega for SNMP Tool Sets provides 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.

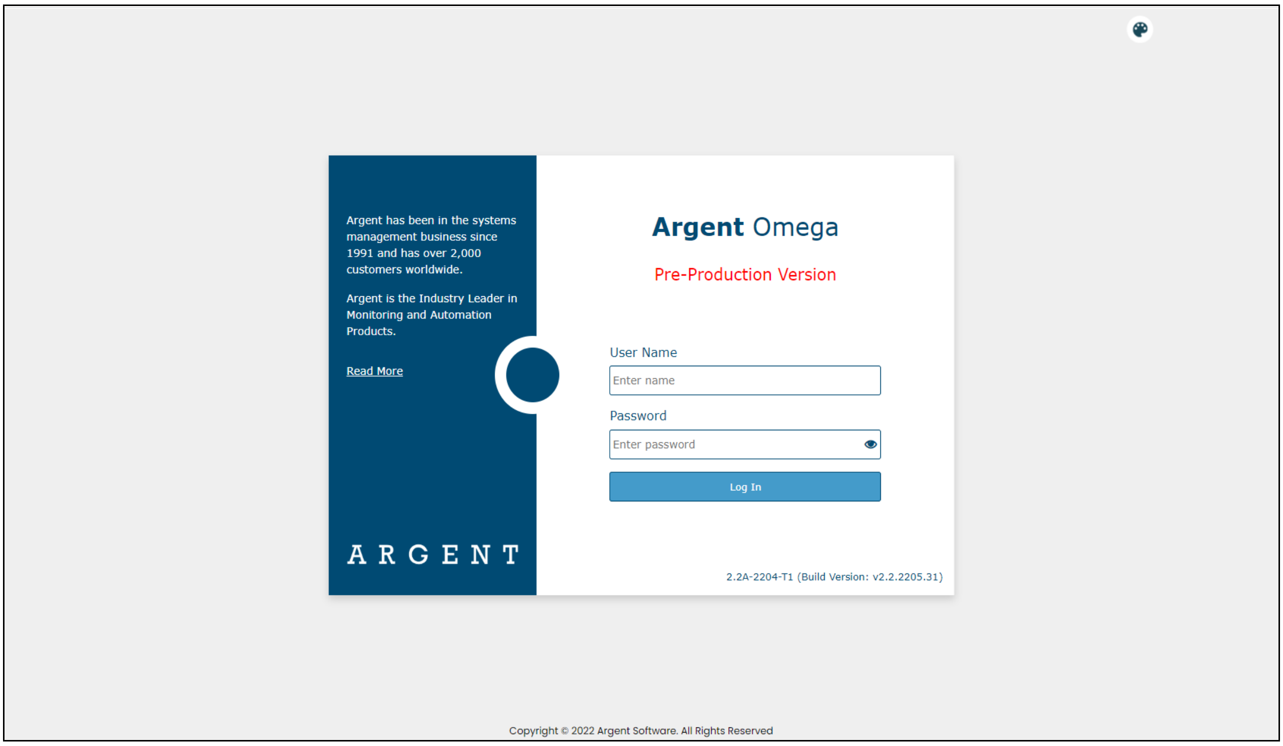
Prerequisites

In order to use Meraki feature, Meraki API key must be specified in **Argent Omega** settings under **Generator Settings.** 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.



Send Internal Events To Email Address:	testargent10@gmail.com
Shared Task Executor Process Pool Size:	10
Max Days To Automatically Resolve Events:	7
Keep Task Execution Info For Days:	☑ Truncate Task Execution History Daily
Prevent Firing The Same Internal Event Within Interval:	60 Minutes
Delay Firing Internal Event:	60 Seconds
Max Allowed Lapse For Active Generator:	5 Minutes
Auto Logoff:	15 Minutes
Meraki API Key:	[redacted]
Default Location:	MUMBAI
Default Contact:	Please Choose:
Administrative Protection Password:	••••••••••••
Take Automatic Backup	□
Time:	00:00:00 It Is Recommended To Do Backup At Midnight
Calendar:	Please Choose:
Recycle Service	□

Log-On Screen



Argent has been in the systems management business since 1991 and has over 2,000 customers worldwide.

Argent is the Industry Leader in Monitoring and Automation Products.

2.2A-2204-T1 (Build Version: v2.2.2205.31)

Copyright © 2022 Argent Software. All Rights Reserved

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

There are three types of user accounts:

- Windows User Accounts
- Demo Accounts
- Internal Accounts

The Argent server is typically in an Active Directory Domain environment and the user is authenticated by Active Directory.

Local Windows user authentication is used instead if the Argent server is standalone or in a Workgroup. With Windows user accounts, the best approach is to create a separate user group for Windows users and assign the required rights.

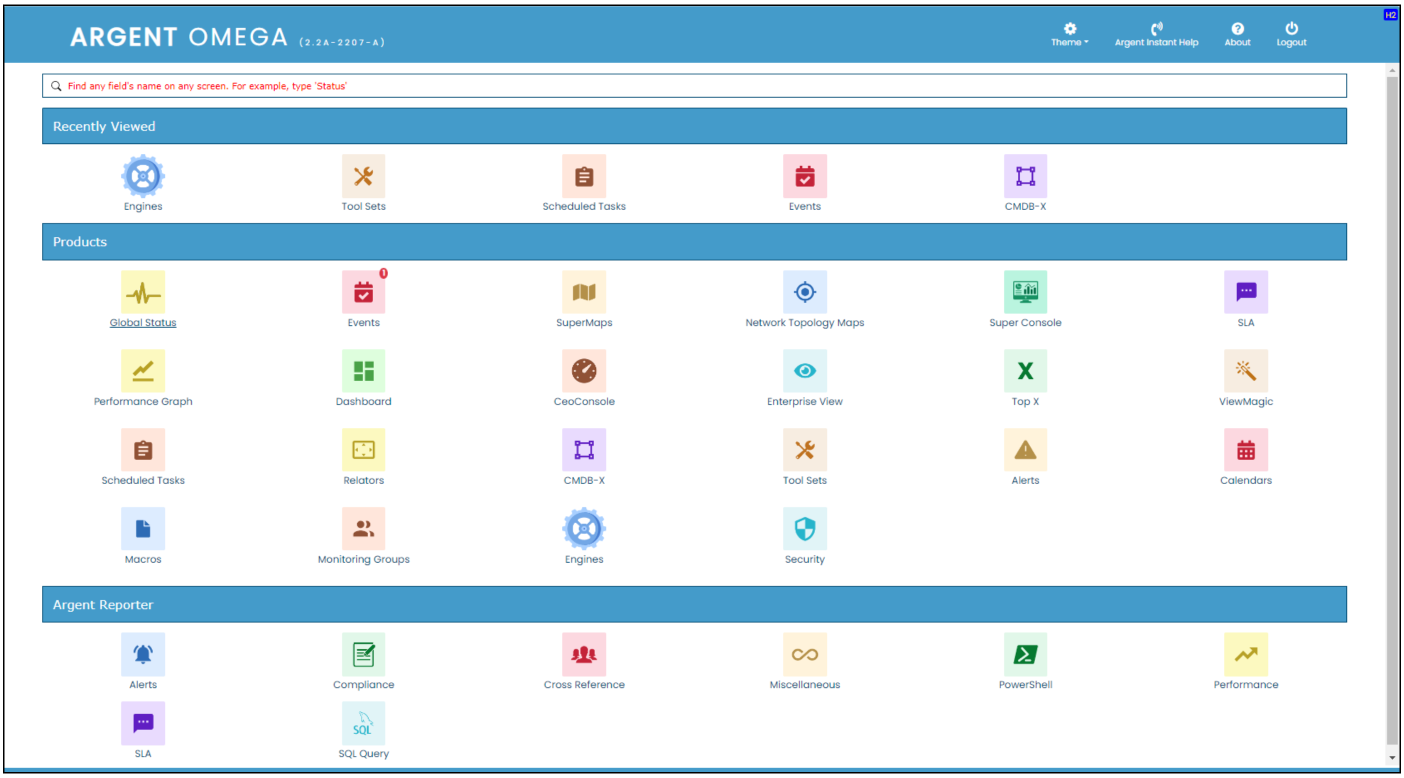
Demo accounts can be created in the **Argent Omega Security** section and are used for demonstration purposes. Demo accounts are read-only accounts and use Argent private authentication to login into Argent Omega. Demo accounts are usually only used temporarily for initial training and are limited to a few specific IP addresses. Argent engineers can create demo training accounts for you at no cost.

Internal accounts also can be created in the **Argent Omega Security** section, and **behave like normal Windows accounts**, using Argent's private authentication for login.

The Argent Omega username is case **insensitive** but the password is case **sensitive**.

Home Screen

The Argent Omega home screen will be displayed after login:



To begin using Argent Omega for SNMP, click on the CMDB-X icon to add monitored servers or devices.

CMDB-X

In the software industry, CMDB stands for Configuration Management DataBase.

Argent added the 'X' for eXtensible.

A recent example of why this feature is so important to you was a customer adding a custom field to their CMDB-X to record **the expiry date of the firewall license**.

The ability to add custom fields in this way allow customers to use the Argent CMDB-X as an IT Asset Management tool.

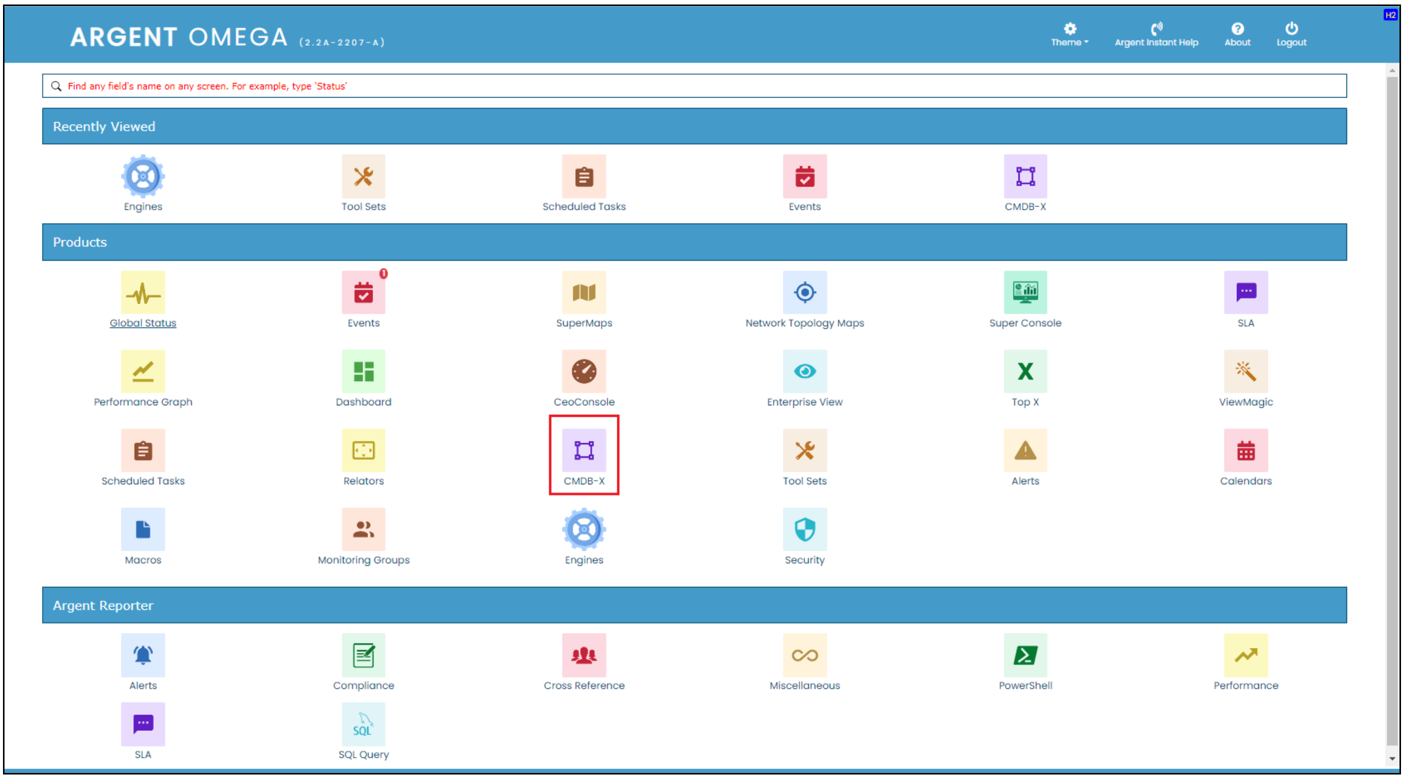
The Argent CMDB-X provides an easy and streamlined way to manage all critical servers and devices, as well as all server and device properties and licensing, **from a single screen.** The Argent CMDB-X makes it easy for you to add multiple servers and devices in one batch – 11 or 77,000 -- license them to multiple Argent Omega products and assign them to existing or new Locations and Network Groups, **all in one single click**.

The 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.

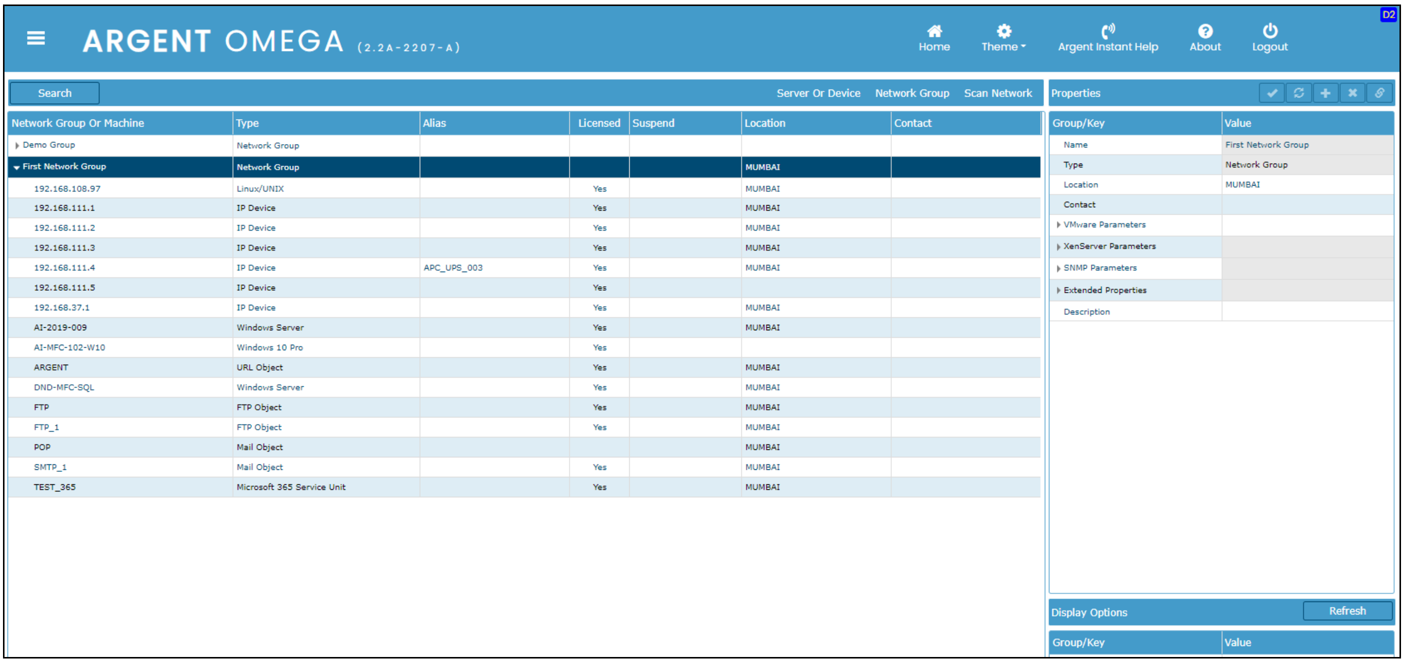
The Argent CMDB-X also has options to import from external Excel files.

The Argent CMDB-X has facilities to manually add or remove servers and devices, license single or multiple servers and devices in bulk groups, test connectivity to the monitored services or devices.

Select '**CMDB-X'** from the Home Screen:



The CMDB-X screen will be displayed as shown below:



Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	

Group/Key	Value
Name	First Network Group
Type	Network Group
Location	MUMBAI
Contact	
VMware Parameters	
XenServer Parameters	
SNMP Parameters	
Extended Properties	
Description	

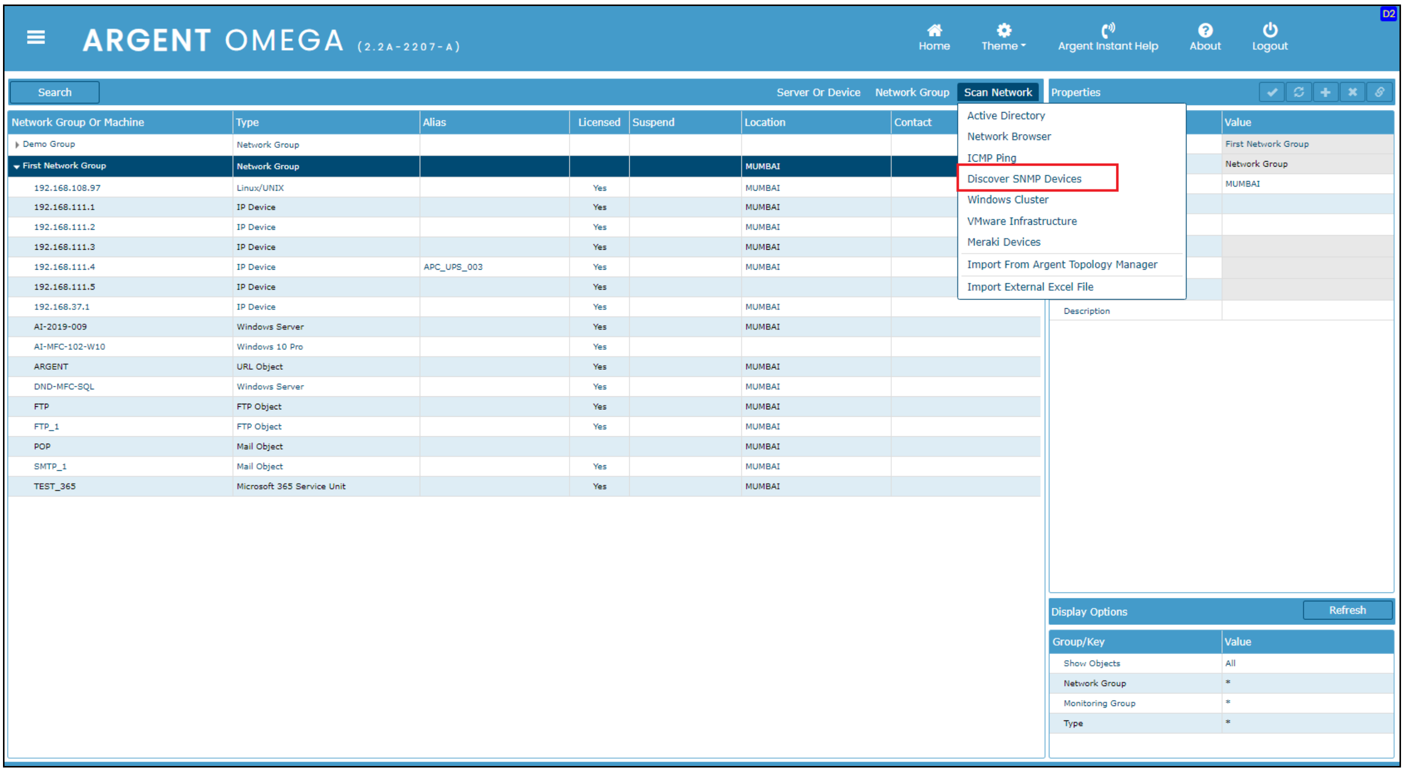
Group/Key	Value

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

- IP Devices
- Linux
- Windows Server

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

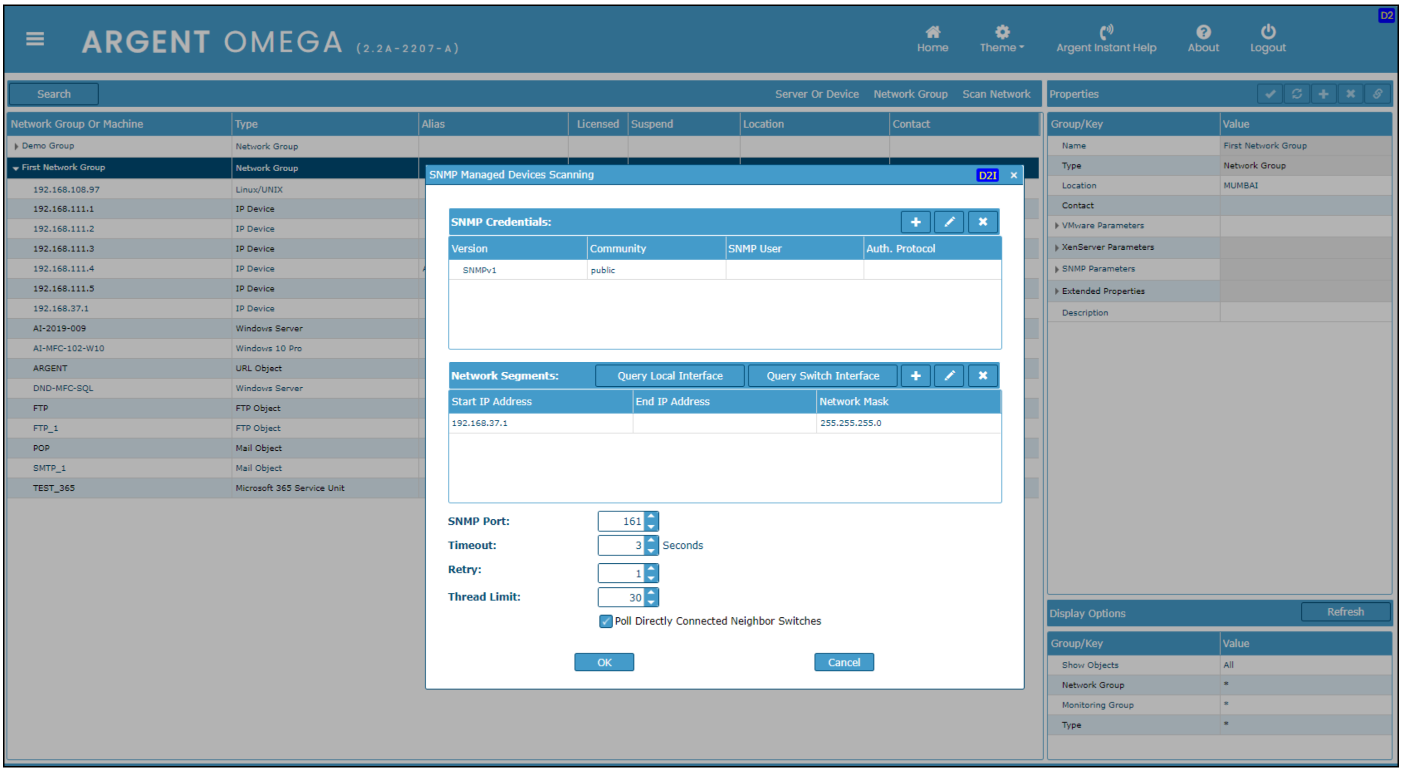
For automatic discovery of SNMP devices, choose **Discover SNMP Devices** from **Scan Network** popup menu:



Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

The following dialog will pop up, asking the SNMP parameters to scan SNMP devices.



SNMP Credentials:

Version	Community	SNMP User	Auth. Protocol
SNMPv1	public		

Network Segments:

Start IP Address	End IP Address	Network Mask
192.168.37.1		255.255.255.0

SNMP Port: 161

Timeout: 3 Seconds

Retry: 1

Thread Limit: 30

☑ Poll Directly Connected Neighbor Switches

Group/Key	Value
Name	First Network Group
Type	Network Group
Location	MUMBAI
Contact	
VMware Parameters	
XenServer Parameters	
SNMP Parameters	
Extended Properties	
Description	

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 that allows access to a router's 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 and 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, 60). The default value is 3.

Retry:

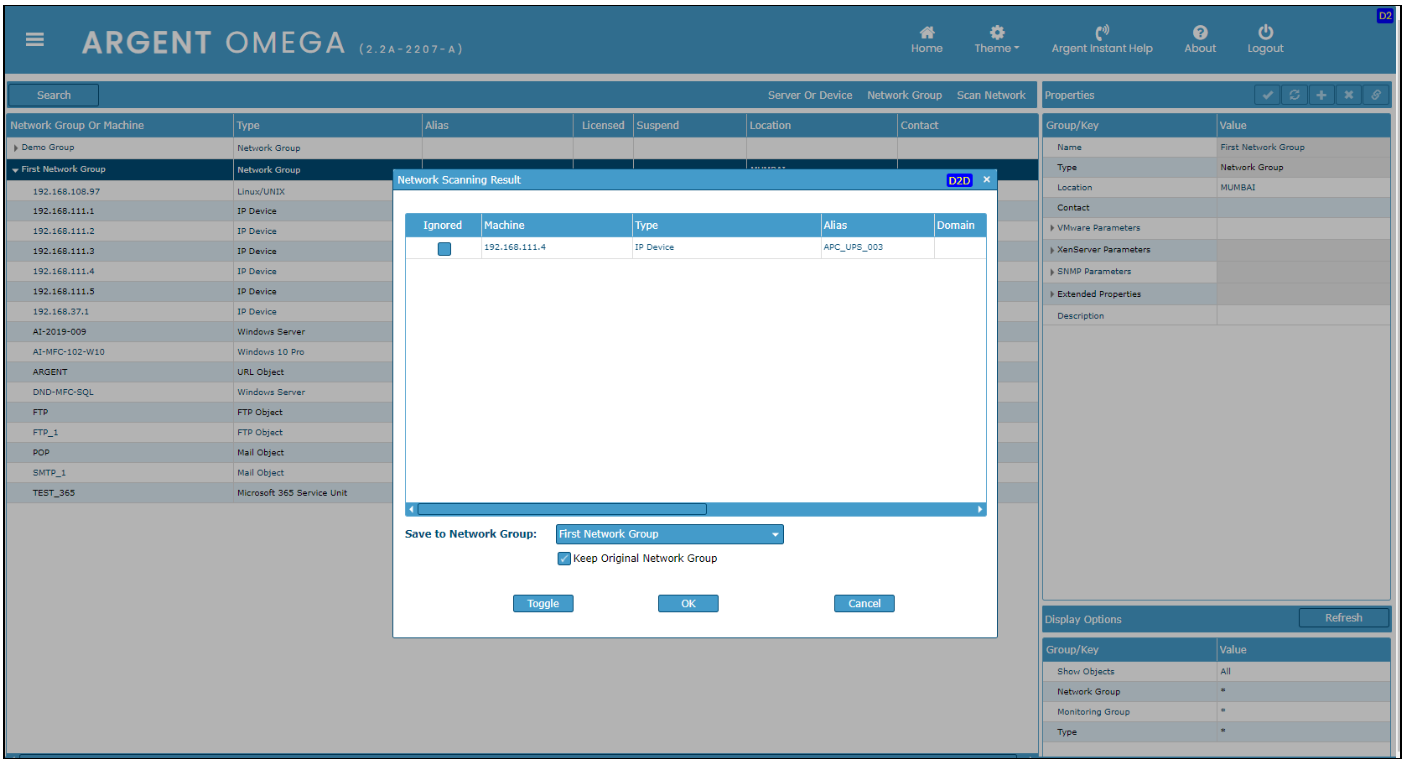
The range is (1, 10). The default value is 1.

Thread Limit:

This is the thread pool size performing the SNMP scanning. The range can be (1, 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 result will be shown in a list box as shown below:



Network Scanning Result

Ignored	Machine	Type	Alias	Domain
☐	192.168.111.4	IP Device	APC_UPS_003	

Save to Network Group: First Network Group

☑ Keep Original Network Group

Group/Key	Value
Name	First Network Group
Type	Network Group
Location	MUMBAI
Contact	
VMware Parameters	
XenServer Parameters	
SNMP Parameters	
Extended Properties	
Description	

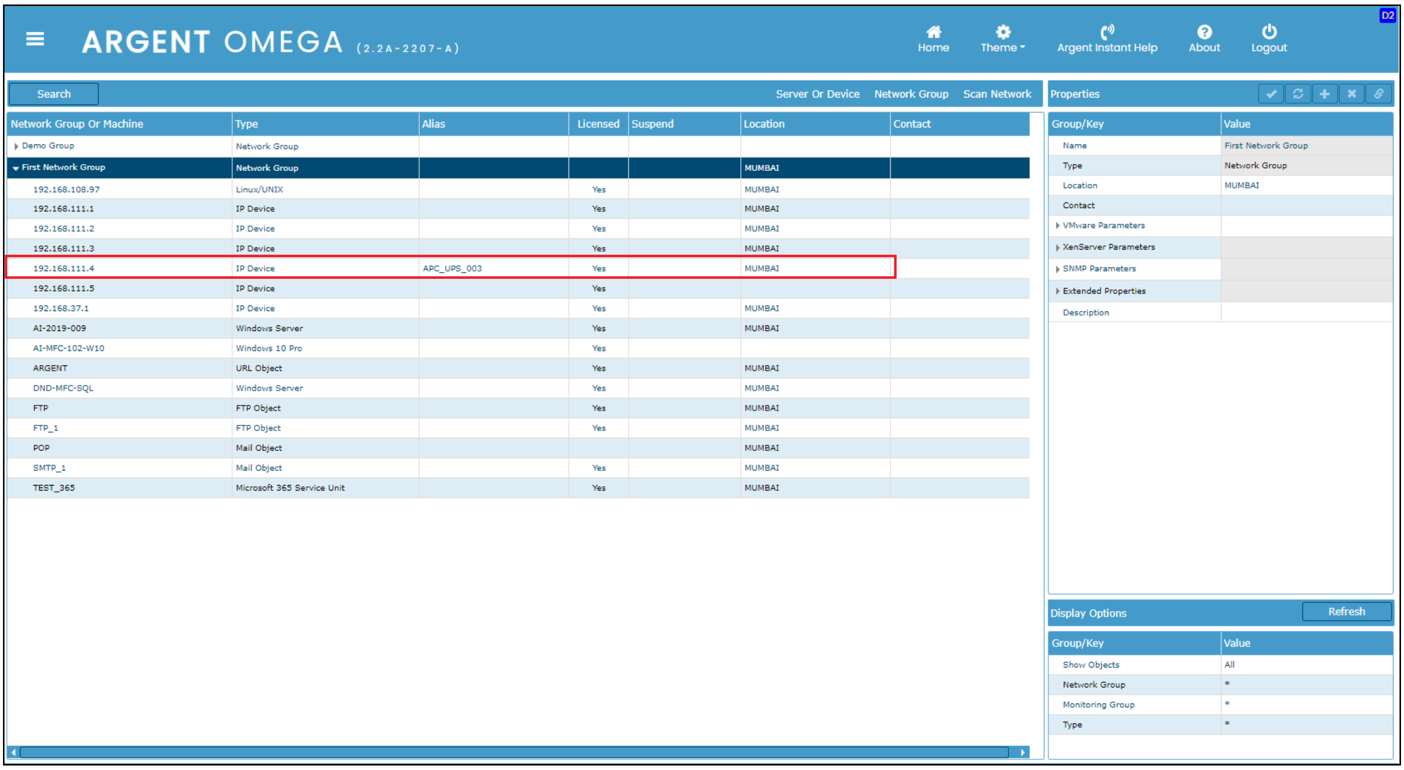
Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

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 saving 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:

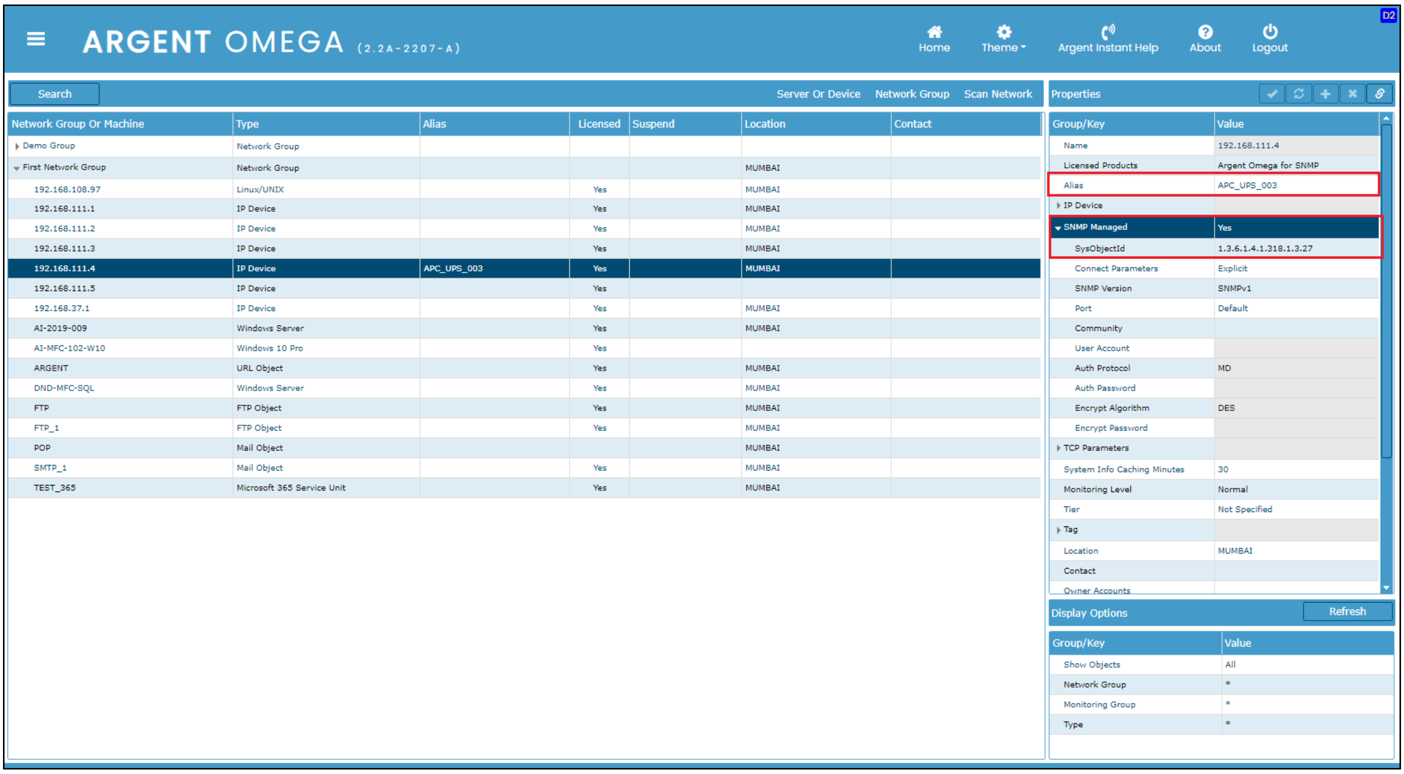


Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	

Group/Key	Value
Name	First Network Group
Type	Network Group
Location	MUMBAI
Contact	
VMware Parameters	
XenServer Parameters	
SNMP Parameters	
Extended Properties	
Description	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

When adding the SNMP device, the CMDB-X property named **SNMP Managed** will automatically be set to **Yes** to show that the device is SNMP managed. The SysObjectId and device type are automatically retrieved. The SysObjectId contains the vendor's identification of an SNMP managed object type.



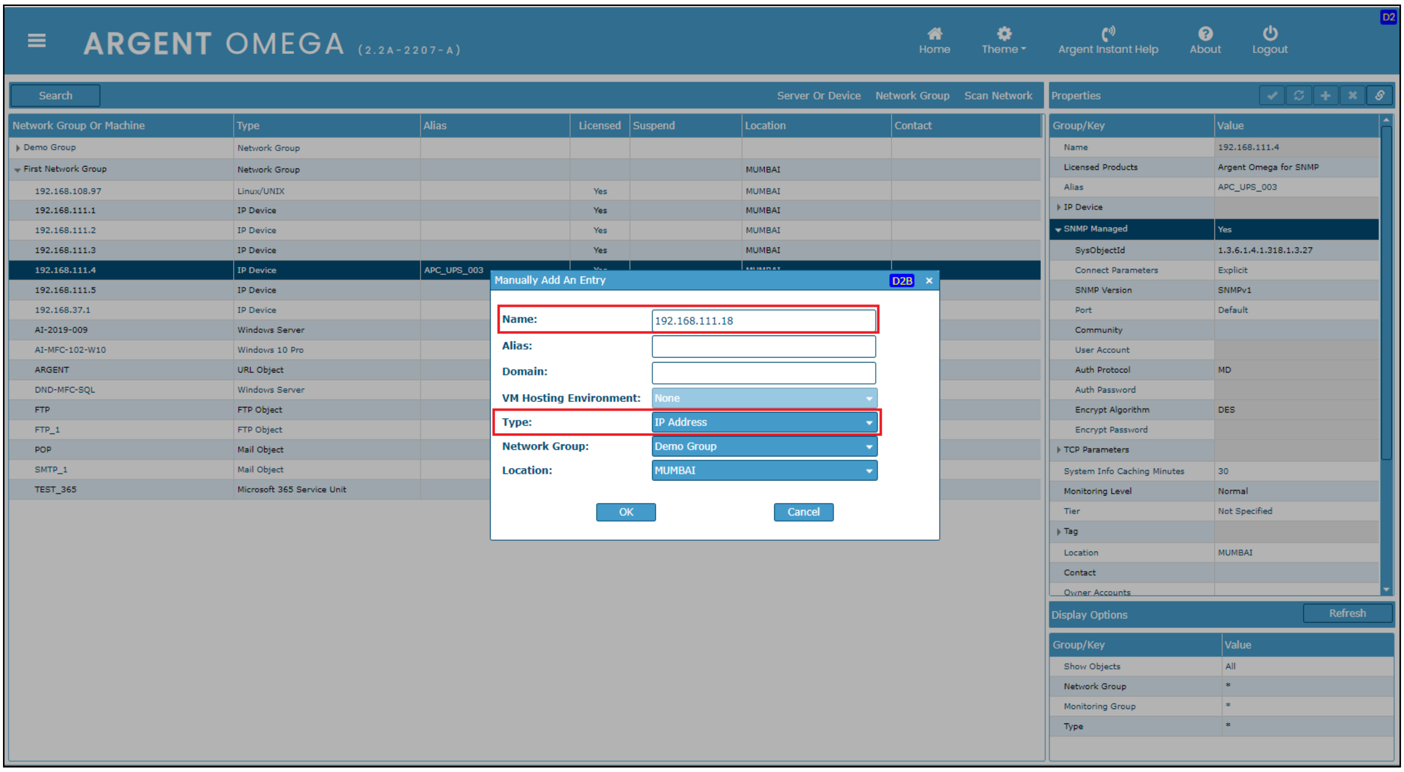
Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	

Group/Key	Value
Name	192.168.111.4
Licensed Products	Argent Omega for SNMP
Alias	APC_UPS_003
IP Device	
SNMP Managed	Yes
SysObjectId	1.3.6.1.4.1.318.1.3.27
Connect Parameters	Explicit
SNMP Version	SNMPv1
Port	Default
Community	
User Account	
Auth Protocol	MD
Auth Password	
Encrypt Algorithm	DES
Encrypt Password	
TCP Parameters	
System Info Caching Minutes	30
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

To manually add a SNMP device to CMDB-X, select **Manually Add Server or Device** from the right click menu:

Add the Name or IP of the device and select the Type:



Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device					
192.168.37.1	IP Device					
AI-2019-009	Windows Server					
AI-MFC-102-W10	Windows 10 Pro					
ARGENT	URL Object					
DND-MFC-SQL	Windows Server					
FTP	FTP Object					
FTP_1	FTP Object					
POP	Mail Object					
SMTP_1	Mail Object					
TEST_365	Microsoft 365 Service Unit					

Manually Add An Entry

Name: 192.168.111.18

Alias:

Domain:

VM Hosting Environment: None

Type: IP Address

Network Group: Demo Group

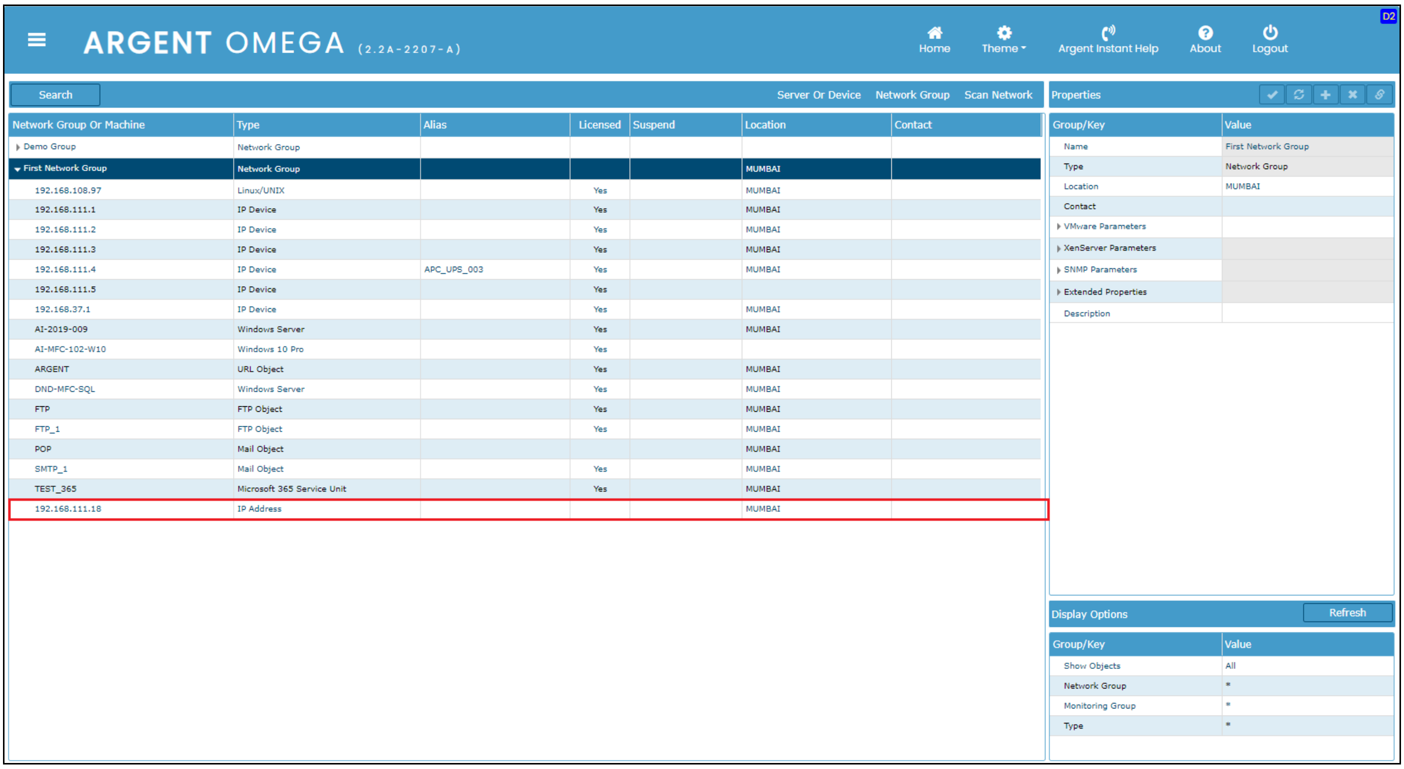
Location: MUMBAI

OK Cancel

Group/Key	Value
Name	192.168.111.4
Licensed Products	Argent Omega for SNMP
Alias	APC_UPS_003
IP Device	
SNMP Managed	Yes
SysObjectId	1.3.6.1.4.1.318.1.3.27
Connect Parameters	Explicit
SNMP Version	SNMPv1
Port	Default
Community	
User Account	
Auth Protocol	MD
Auth Password	
Encrypt Algorithm	DES
Encrypt Password	
TCP Parameters	
System Info Caching Minutes	30
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

The new server will now be listed in the CMDB-X:



Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	
192.168.111.18	IP Address				MUMBAI	

Group/Key	Value
Name	First Network Group
Type	Network Group
Location	MUMBAI
Contact	
VMware Parameters	
XenServer Parameters	
SNMP Parameters	
Extended Properties	
Description	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

The following SNMP specific CMDB-X 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 following parameters need to be defined:

SNMP Version

It can be SNMPv1, SNMPv2c or SNMPv3. SNMPv3 requires authentication. If SNMPv3 is selected, valid authentication credentials should 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 user name.

Auth Protocol

SNMPv3 authentication password.

Auth Password

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

Encrypt Algorithm

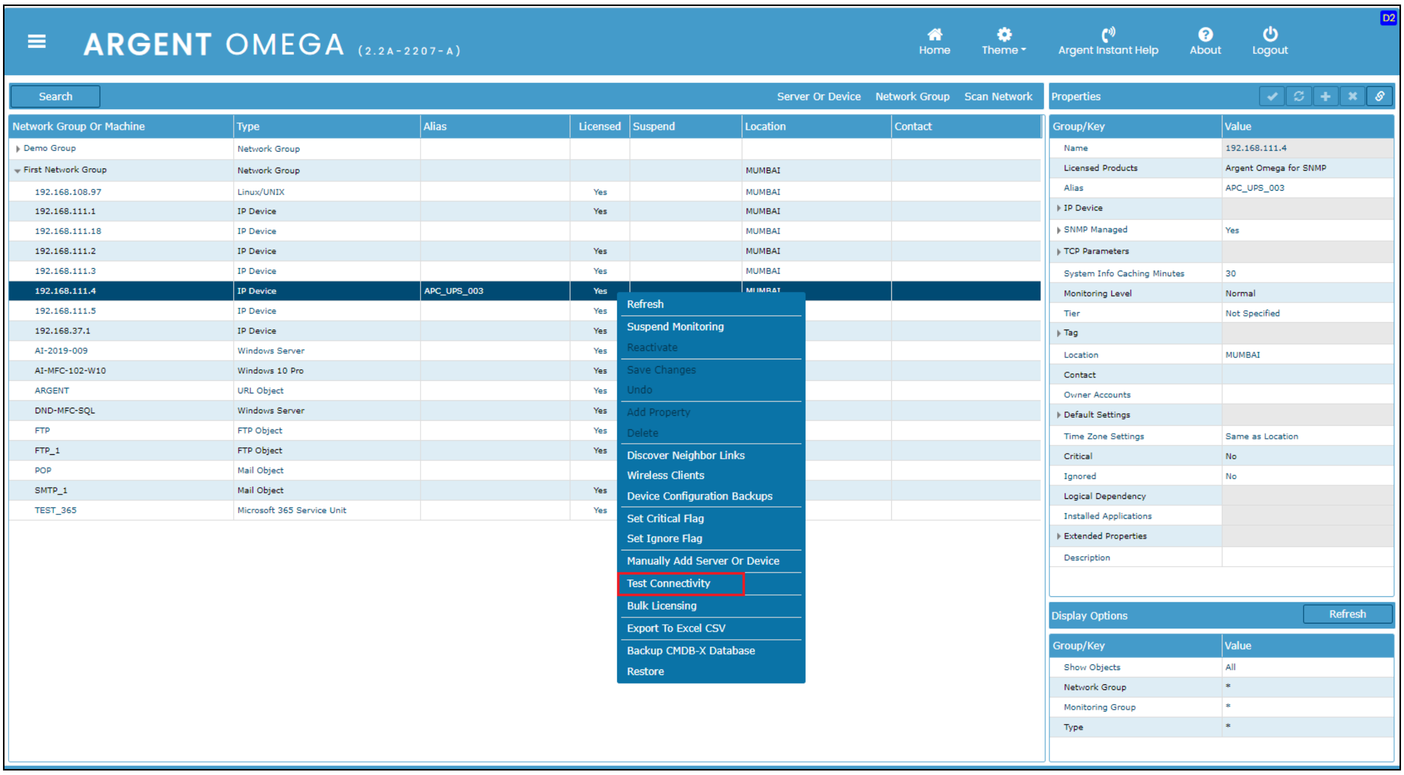
SNMPv3 encryption algorithm. It can be DES, AES, 3DES, AES192 or AES256.

Encrypt Password

SNMPv3 encryption password.

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

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

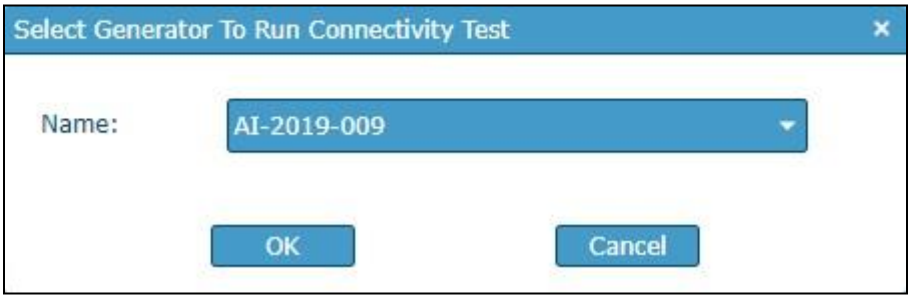


Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes			
AI-2019-009	Windows Server		Yes			
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes			
DND-MFC-SQL	Windows Server		Yes			
FTP	FTP Object		Yes			
FTP_1	FTP Object		Yes			
POP	Mail Object					
SMTP_1	Mail Object		Yes			
TEST_365	Microsoft 365 Service Unit		Yes			

Group/Key	Value
Name	192.168.111.4
Licensed Products	Argent Omega for SNMP
Alias	APC_UPS_003
IP Device	
SNMP Managed	Yes
TCP Parameters	
System Info Caching Minutes	30
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	
Default Settings	
Time Zone Settings	Same as Location
Critical	No
Ignored	No
Logical Dependency	
Installed Applications	
Extended Properties	
Description	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

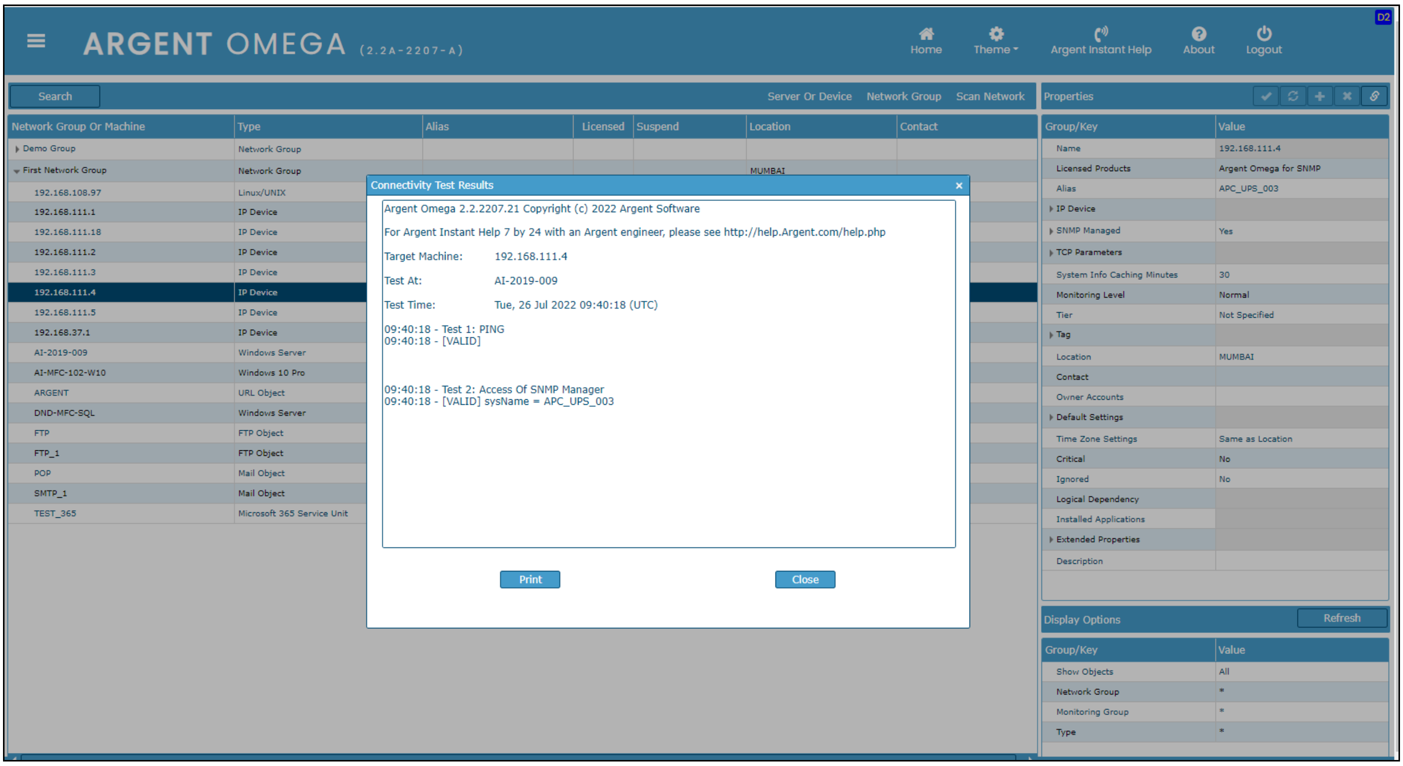
Select a server or device to execute the connectivity test and click OK:



Select Generator To Run Connectivity Test

Name: AI-2019-009

The Results are shown:



Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX					
192.168.111.1	IP Device					
192.168.111.18	IP Device					
192.168.111.2	IP Device					
192.168.111.3	IP Device					
192.168.111.4	IP Device					
192.168.111.5	IP Device					
192.168.37.1	IP Device					
AI-2019-009	Windows Server					
AI-MFC-102-W10	Windows 10 Pro					
ARGENT	URL Object					
DND-MFC-SQL	Windows Server					
FTP	FTP Object					
FTP_1	FTP Object					
POP	Mail Object					
SMTP_1	Mail Object					
TEST_365	Microsoft 365 Service Unit					

Connectivity Test Results

```
Argent Omega 2.2.2207.21 Copyright (c) 2022 Argent Software

For Argent Instant Help 7 by 24 with an Argent engineer, please see http://help.Argent.com/help.php

Target Machine:      192.168.111.4

Test At:             AI-2019-009

Test Time:           Tue, 26 Jul 2022 09:40:18 (UTC)

09:40:18 - Test 1: PING
09:40:18 - [VALID]



09:40:18 - Test 2: Access Of SNMP Manager
09:40:18 - [VALID] sysName = APC_UPS_003
```

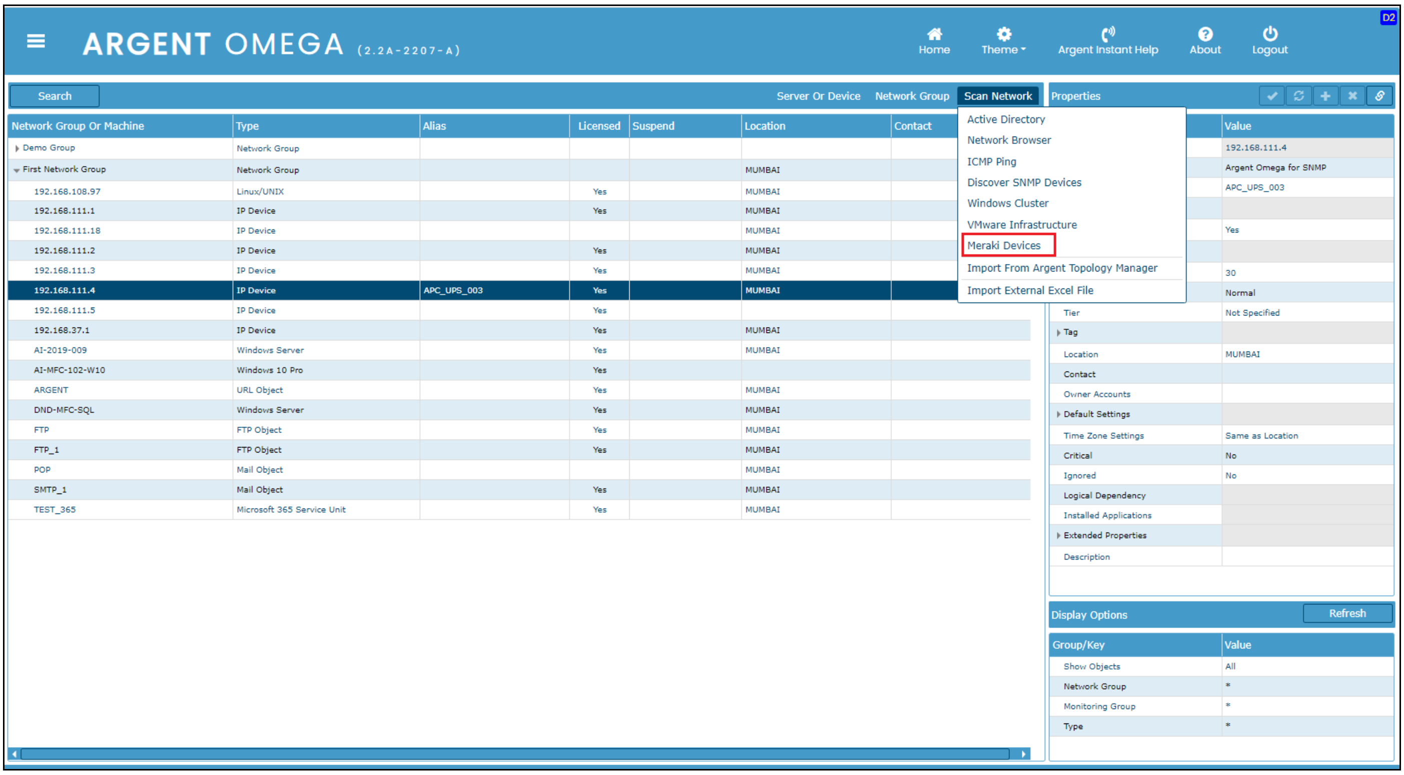
Group/Key	Value
Name	192.168.111.4
Licensed Products	Argent Omega for SNMP
Alias	APC_UPS_003
IP Device	
SNMP Managed	Yes
TCP Parameters	
System Info Caching Minutes	30
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	
Default Settings	
Time Zone Settings	Same as Location
Critical	No
Ignored	No
Logical Dependency	
Installed Applications	
Extended Properties	
Description	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

Tests can also be run against other server 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 out current wireless clients of a selected Meraki device. There is a scan option in CMDB-X to scan Meraki devices.



Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	

	Value
	192.168.111.4
	Argent Omega for SNMP
	APC_UPS_003
	Yes
	30
	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	
Default Settings	
Time Zone Settings	Same as Location
Critical	No
Ignored	No
Logical Dependency	
Installed Applications	
Extended Properties	
Description	

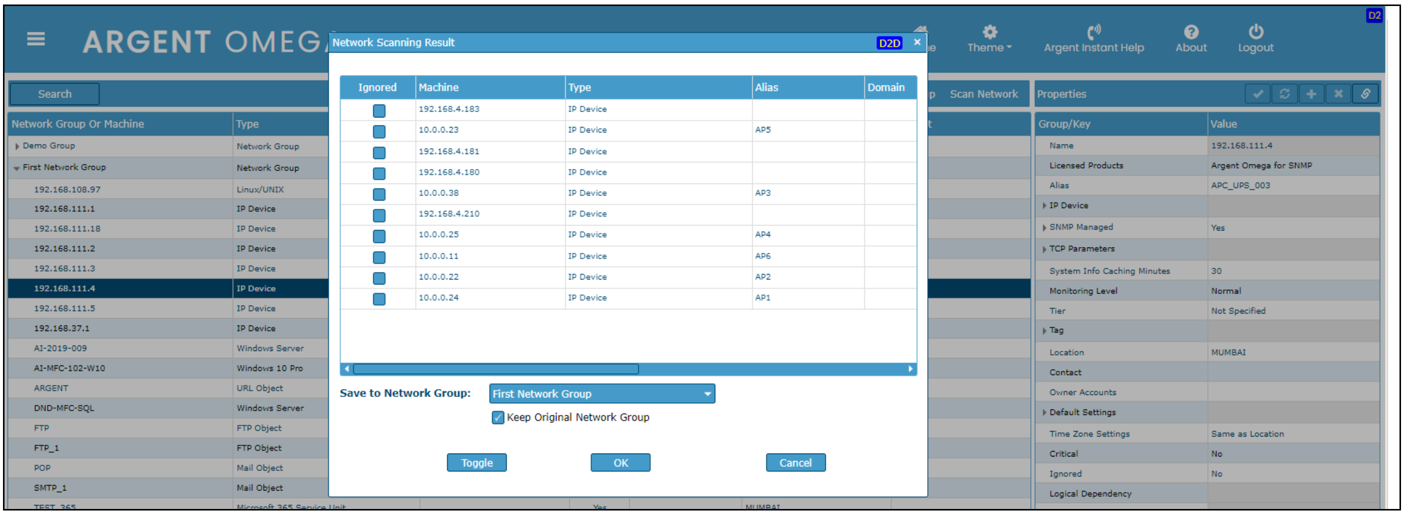
Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

Note:

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:



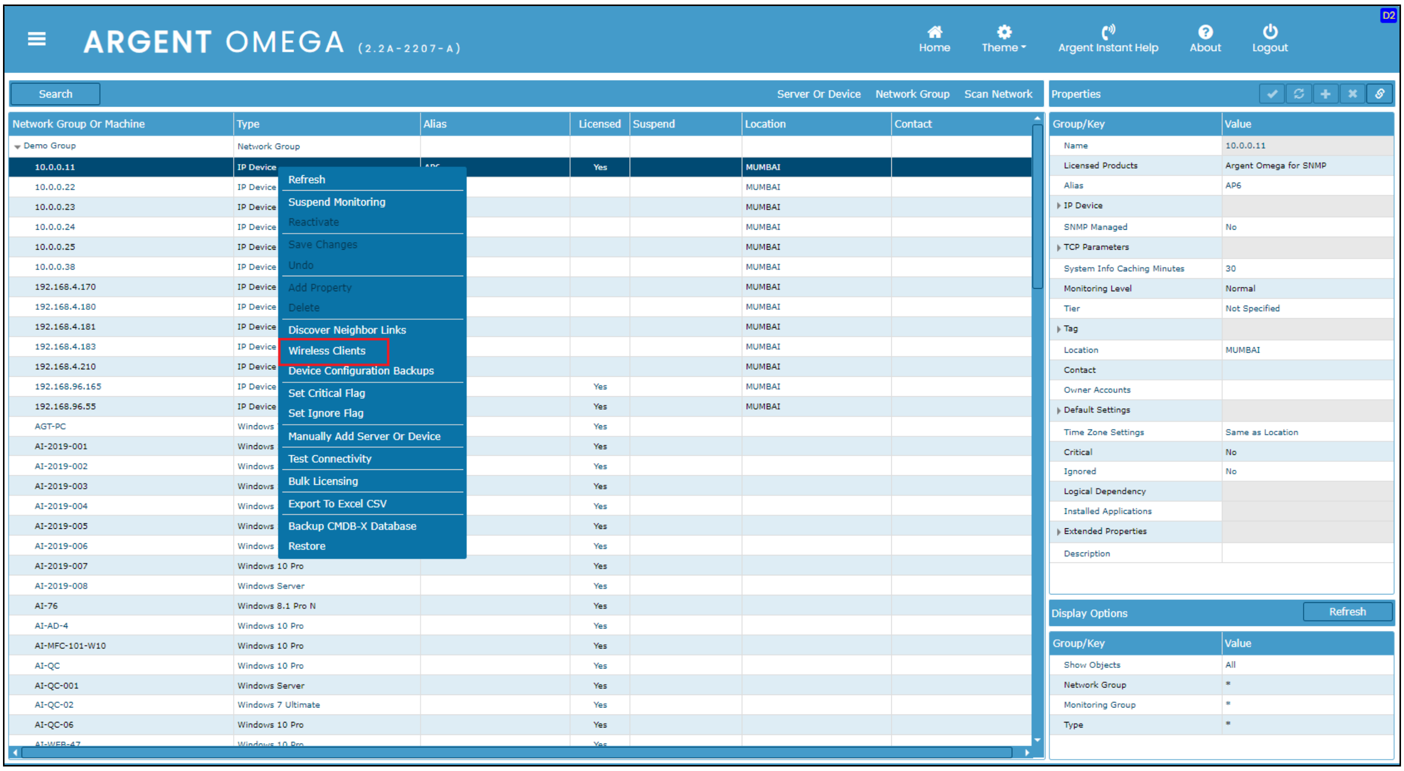
Ignored	Machine	Type	Alias	Domain
□	192.168.4.183	IP Device		
□	10.0.0.23	IP Device	AP5	
□	192.168.4.181	IP Device		
□	192.168.4.180	IP Device		
□	10.0.0.38	IP Device	AP3	
□	192.168.4.210	IP Device		
□	10.0.0.25	IP Device	AP4	
□	10.0.0.11	IP Device	AP6	
□	10.0.0.22	IP Device	AP2	
□	10.0.0.24	IP Device	AP1	

Save to Network Group: First Network Group

☑ Keep Original Network Group

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.

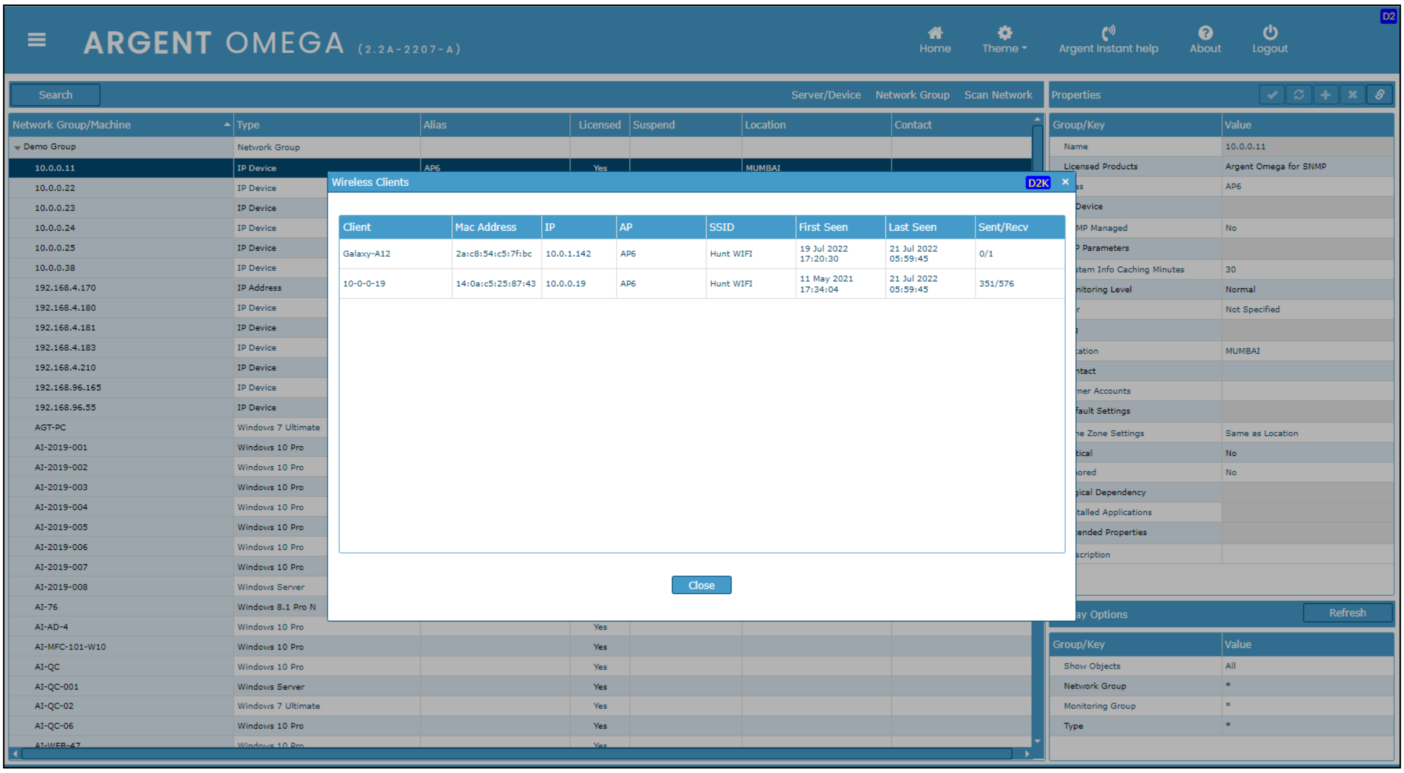


Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
10.0.0.11	IP Device	AP6	Yes		MUMBAI	
10.0.0.22	IP Device				MUMBAI	
10.0.0.23	IP Device				MUMBAI	
10.0.0.24	IP Device				MUMBAI	
10.0.0.25	IP Device				MUMBAI	
10.0.0.38	IP Device				MUMBAI	
192.168.4.170	IP Device				MUMBAI	
192.168.4.180	IP Device				MUMBAI	
192.168.4.181	IP Device				MUMBAI	
192.168.4.183	IP Device				MUMBAI	
192.168.4.210	IP Device				MUMBAI	
192.168.96.165	IP Device		Yes		MUMBAI	
192.168.96.55	IP Device		Yes		MUMBAI	
AGT-PC	Windows		Yes			
AI-2019-001	Windows		Yes			
AI-2019-002	Windows		Yes			
AI-2019-003	Windows		Yes			
AI-2019-004	Windows		Yes			
AI-2019-005	Windows		Yes			
AI-2019-006	Windows		Yes			
AI-2019-007	Windows 10 Pro		Yes			
AI-2019-008	Windows Server		Yes			
AI-76	Windows 8.1 Pro N		Yes			
AI-AD-4	Windows 10 Pro		Yes			
AI-MFC-101-W10	Windows 10 Pro		Yes			
AI-QC	Windows 10 Pro		Yes			
AI-QC-001	Windows Server		Yes			
AI-QC-02	Windows 7 Ultimate		Yes			
AI-QC-06	Windows 10 Pro		Yes			
AI-WEB-47	Windows 10 Pro		Yes			

Group/Key	Value
Name	10.0.0.11
Licensed Products	Argent Omega for SNMP
Alias	AP6
IP Device	
SNMP Managed	No
TCP Parameters	
System Info Caching Minutes	30
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	
Default Settings	
Time Zone Settings	Same as Location
Critical	No
Ignored	No
Logical Dependency	
Installed Applications	
Extended Properties	
Description	

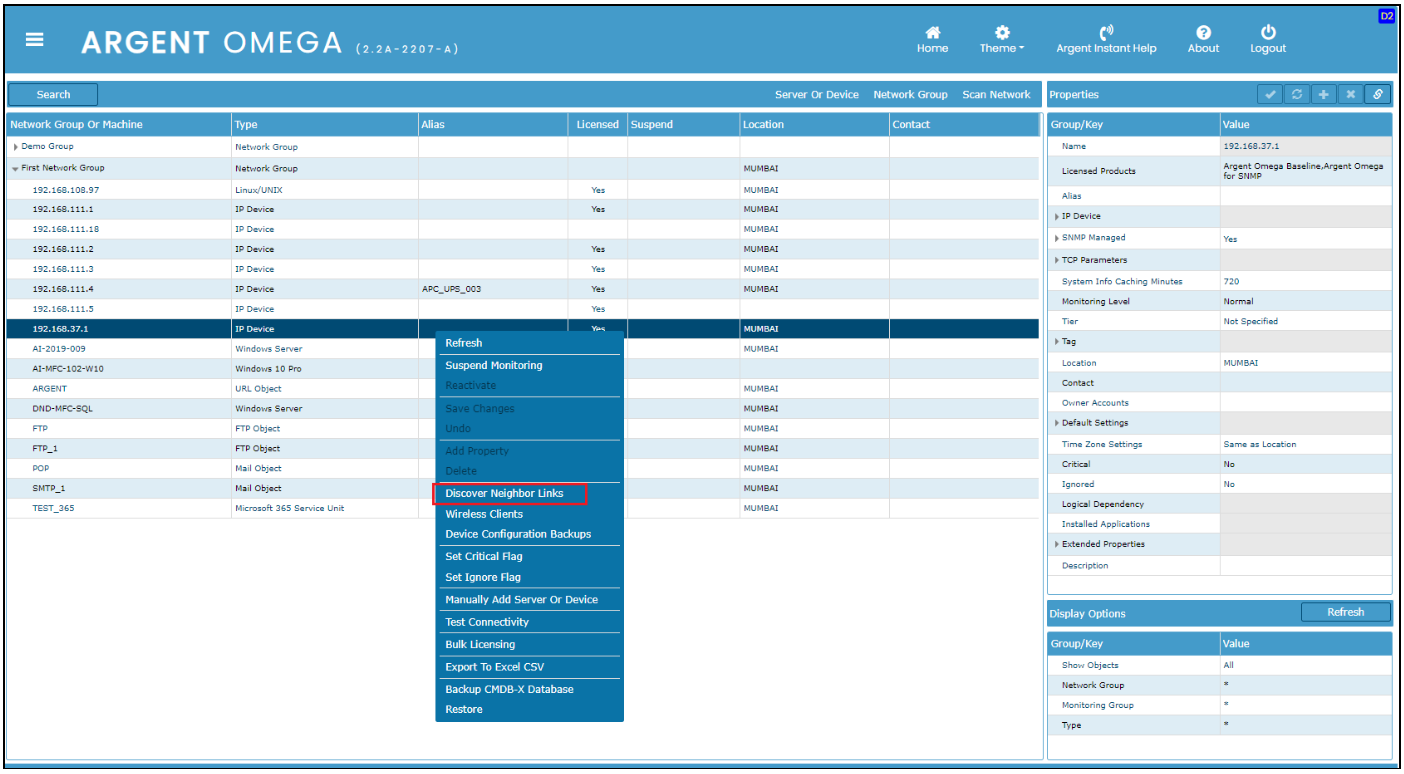
Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

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



Client	Mac Address	IP	AP	SSID	First Seen	Last Seen	Sent/Recv
Galaxy-A12	2a:c8:54:c5:7f:bc	10.0.1.142	AP6	Hunt WIFI	19 Jul 2022 17:20:30	21 Jul 2022 05:59:45	0/1
10-0-0-19	14:0a:c5:25:87:43	10.0.0.19	AP6	Hunt WIFI	11 May 2021 17:34:04	21 Jul 2022 05:59:45	351/576

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



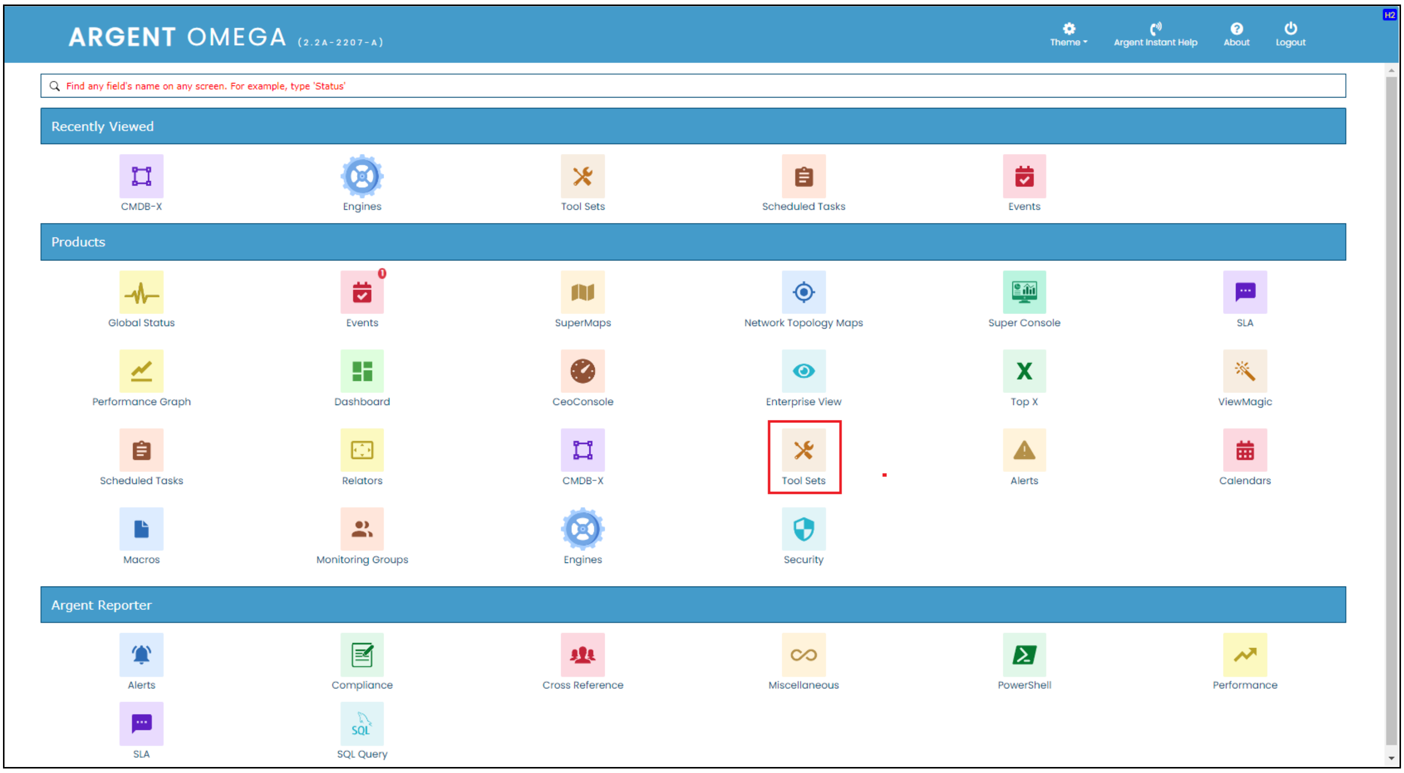
Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server				MUMBAI	
AI-MFC-102-W10	Windows 10 Pro					
ARGENT	URL Object				MUMBAI	
DND-MFC-SQL	Windows Server				MUMBAI	
FTP	FTP Object				MUMBAI	
FTP_1	FTP Object				MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object				MUMBAI	
TEST_365	Microsoft 365 Service Unit				MUMBAI	

Group/Key	Value
Name	192.168.37.1
Licensed Products	Argent Omega Baseline,Argent Omega for SNMP
Alias	
IP Device	
SNMP Managed	Yes
TCP Parameters	
System Info Caching Minutes	720
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	
Default Settings	
Time Zone Settings	Same as Location
Critical	No
Ignored	No
Logical Dependency	
Installed Applications	
Extended Properties	
Description	

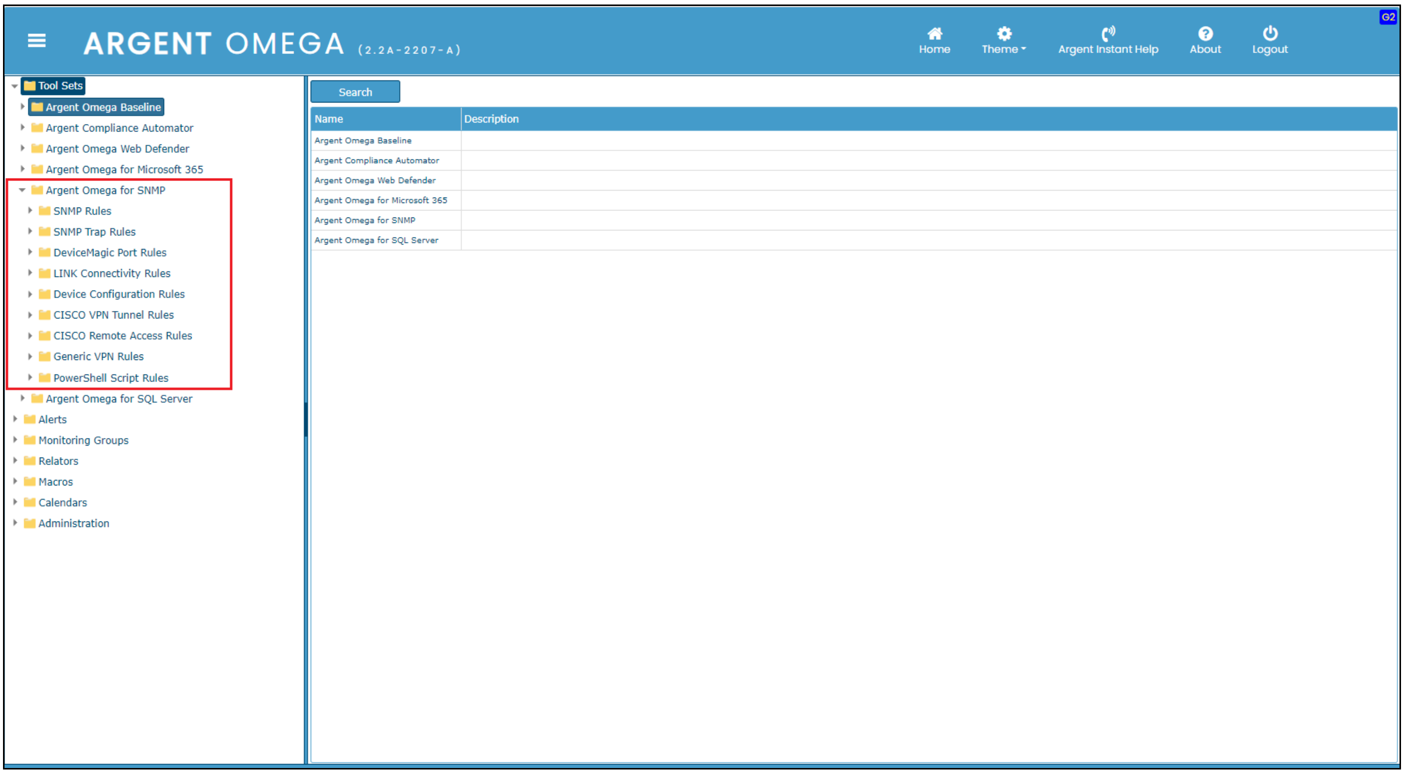
Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

Agent Omega for SNMP Tool Sets

Select **Tool Sets** from the Home Screen:



Under **Tool Sets**, select **Argent Omega for SNMP.** You can find the following Rules there.



Name	Description
Argent Omega Baseline	
Argent Compliance Automator	
Argent Omega Web Defender	
Argent Omega for Microsoft 365	
Argent Omega for SNMP	
Argent Omega for SQL Server	

Argent Omega for SNMP consists of different types of 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

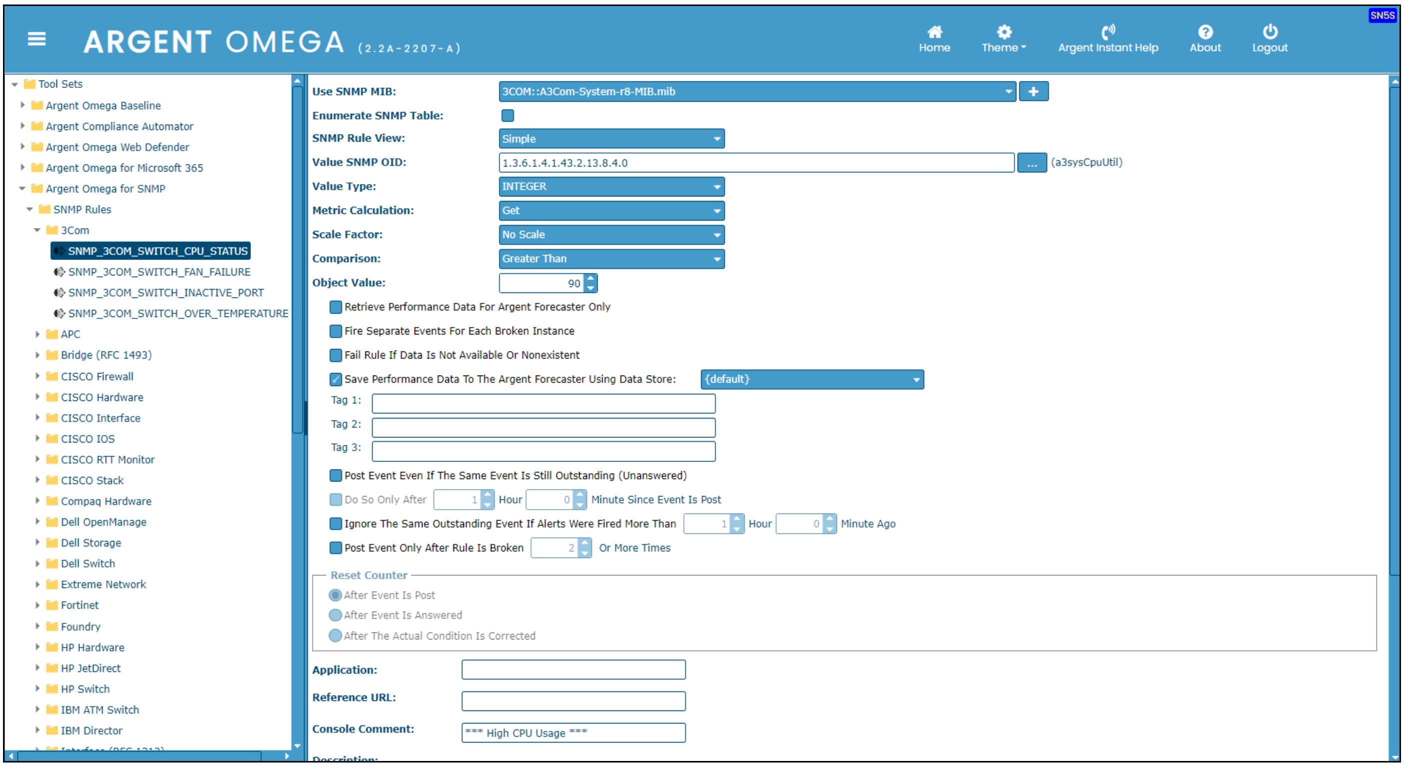
SNMP Rules

Any SNMP-compliant device can be monitored using SNMP Rules. These Rules allow the polling of OID’s 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. You can create your own custom SNMP rules based on any manufacturer's SNMP information (MIB file). You can also have Argent to do this for you.

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

The hardware devices vary widely, from Compaq server hardware to air conditioning units and PBXs. Using SNMP Rules, all common server hardware’s important aspects are monitored, such as the motherboard, the power supply and even the fans in the servers.

Following is the SNMP Rule screen:



Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib +

Enumerate SNMP Table: □

SNMP Rule View: Simple

Value SNMP OID: 1.3.6.1.4.1.43.2.13.8.4.0 ... (a3sysCpuUtil)

Value Type: INTEGER

Metric Calculation: Get

Scale Factor: No Scale

Comparison: Greater Than

Object Value: 90

□ Retrieve Performance Data For Argent Forecaster Only

□ Fire Separate Events For Each Broken Instance

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

Application:

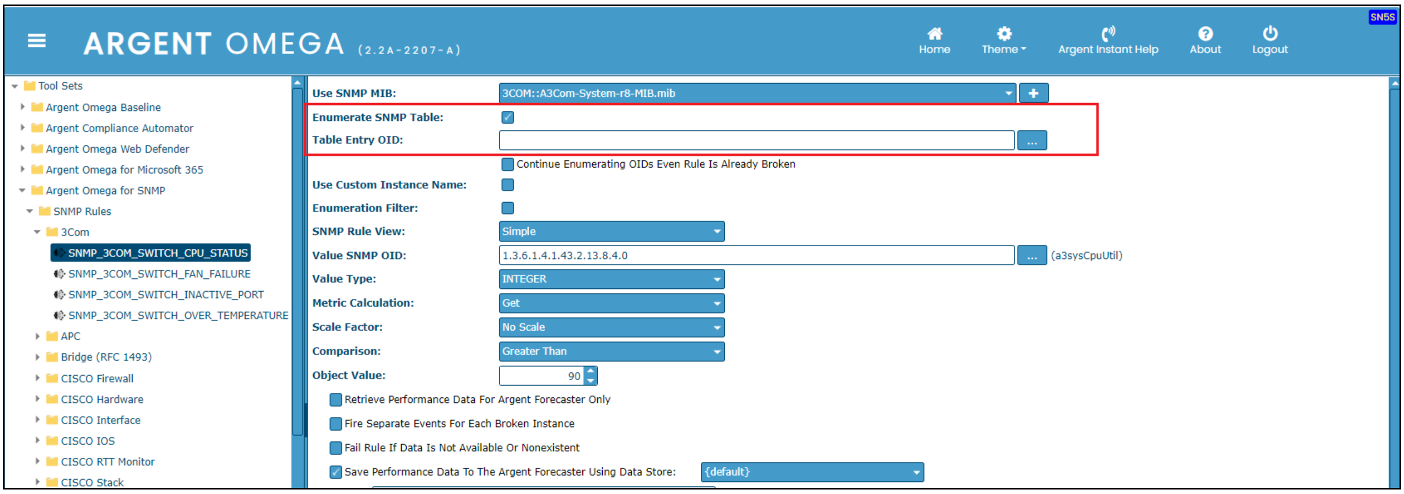
Reference URL:

Console Comment: *** High CPU Usage ***

The following options need to be configured to monitor a SNMP-complaint device:

Select MIB file from **Use SNMP MIB** combo box. 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.

Check **Enumerate SNMP Table** option if the Rule needs to enumerate SMTP tables defined in specified MIB file. SNMP table can be defined as an ordered collection of objects consisting of 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.


ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant Help
About
Logout
SN5S
Tool Sets
Argent Omega Baseline
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
SNMP Rules
3Com
SNMP_3COM_SWITCH_CPU_STATUS
SNMP_3COM_SWITCH_FAN_FAILURE
SNMP_3COM_SWITCH_INACTIVE_PORT
SNMP_3COM_SWITCH_OVER_TEMPERATURE
APC
Bridge (RFC 1493)
CISCO Firewall
CISCO Hardware
CISCO Interface
CISCO IOS
CISCO RTT Monitor
CISCO Stack

Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib +

Enumerate SNMP Table: ☑

Table Entry OID: ...

□ Continue Enumerating OIDs Even Rule Is Already Broken

Use Custom Instance Name: □

Enumeration Filter: □

SNMP Rule View: Simple

Value SNMP OID: 1.3.6.1.4.1.43.2.13.8.4.0 ... (a3sysCpuUtil)

Value Type: INTEGER

Metric Calculation: Get

Scale Factor: No Scale

Comparison: Greater Than

Object Value: 90

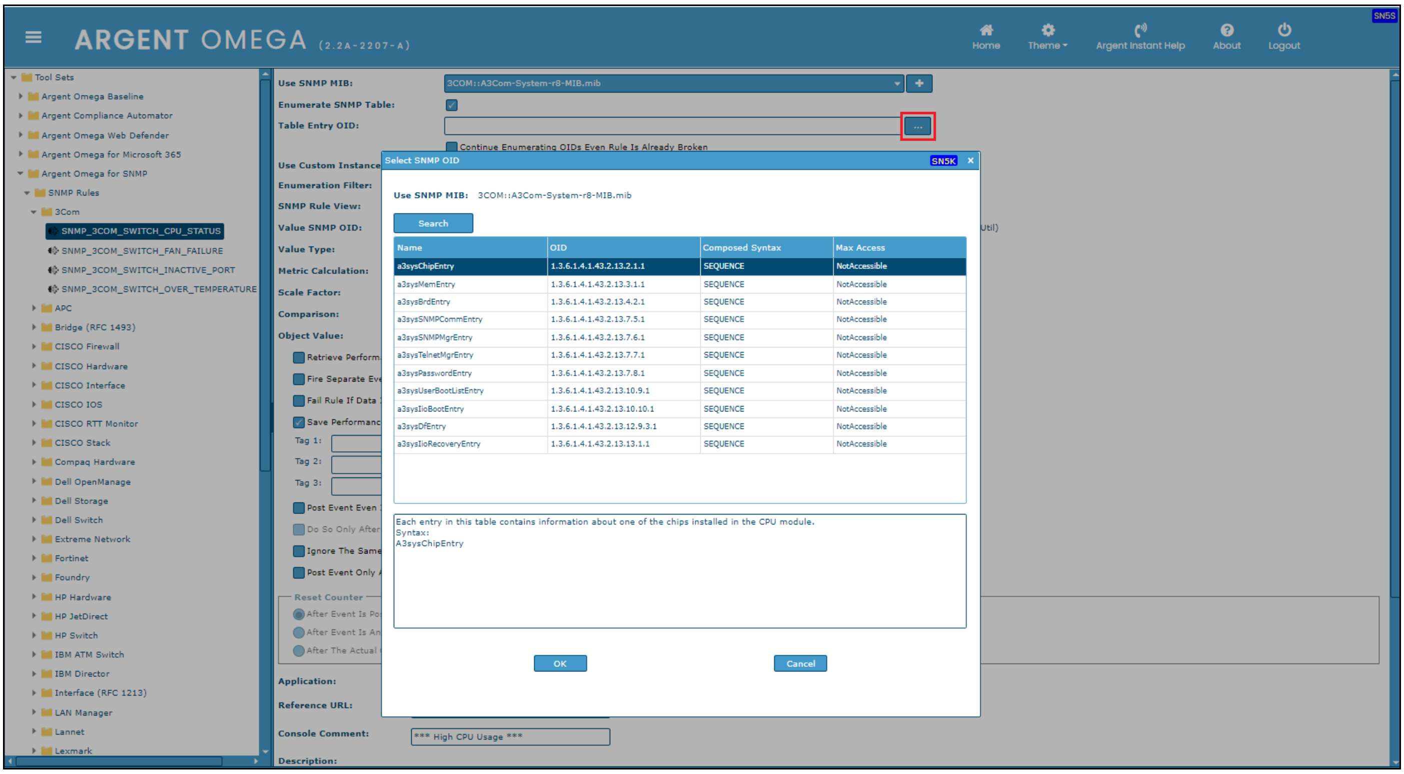
□ Retrieve Performance Data For Argent Forecaster Only

□ Fire Separate Events For Each Broken Instance

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

You can either manually enter the OID or use the browse button to browse Table Entry OIDs of specific MIB file.



Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Enumerate SNMP Table: ☑

Table Entry OID:

□ Continue Enumerating OIDs Even Rule Is Already Broken

Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Name	OID	Composed Syntax	Max Access
a3sysChipEntry	1.3.6.1.4.1.43.2.13.2.1.1	SEQUENCE	NotAccessible
a3sysMemEntry	1.3.6.1.4.1.43.2.13.3.1.1	SEQUENCE	NotAccessible
a3sysBrdEntry	1.3.6.1.4.1.43.2.13.4.2.1	SEQUENCE	NotAccessible
a3sysSNMPCommEntry	1.3.6.1.4.1.43.2.13.7.5.1	SEQUENCE	NotAccessible
a3sysSNMPMgrEntry	1.3.6.1.4.1.43.2.13.7.6.1	SEQUENCE	NotAccessible
a3sysTelnetMgrEntry	1.3.6.1.4.1.43.2.13.7.7.1	SEQUENCE	NotAccessible
a3sysPasswordEntry	1.3.6.1.4.1.43.2.13.7.8.1	SEQUENCE	NotAccessible
a3sysUserBootListEntry	1.3.6.1.4.1.43.2.13.10.9.1	SEQUENCE	NotAccessible
a3sysIioBootEntry	1.3.6.1.4.1.43.2.13.10.10.1	SEQUENCE	NotAccessible
a3sysDfEntry	1.3.6.1.4.1.43.2.13.12.9.3.1	SEQUENCE	NotAccessible
a3sysIioRecoveryEntry	1.3.6.1.4.1.43.2.13.13.1.1	SEQUENCE	NotAccessible

Each entry in this table contains information about one of the chips installed in the CPU module.
Syntax:
A3sysChipEntry

Use Custom Instance
Enumeration Filter:
SNMP Rule View:
Value SNMP OID:
Value Type:
Metric Calculation:
Scale Factor:
Comparison:
Object Value:

□ Retrieve Perform
□ Fire Separate Eve
□ Fail Rule If Data
☑ Save Performanc
Tag 1:
Tag 2:
Tag 3:
□ Post Event Even
□ Do So Only After
□ Ignore The Same
□ Post Event Only

Reset Counter
○ After Event Is Po
○ After Event Is An
○ After The Actual

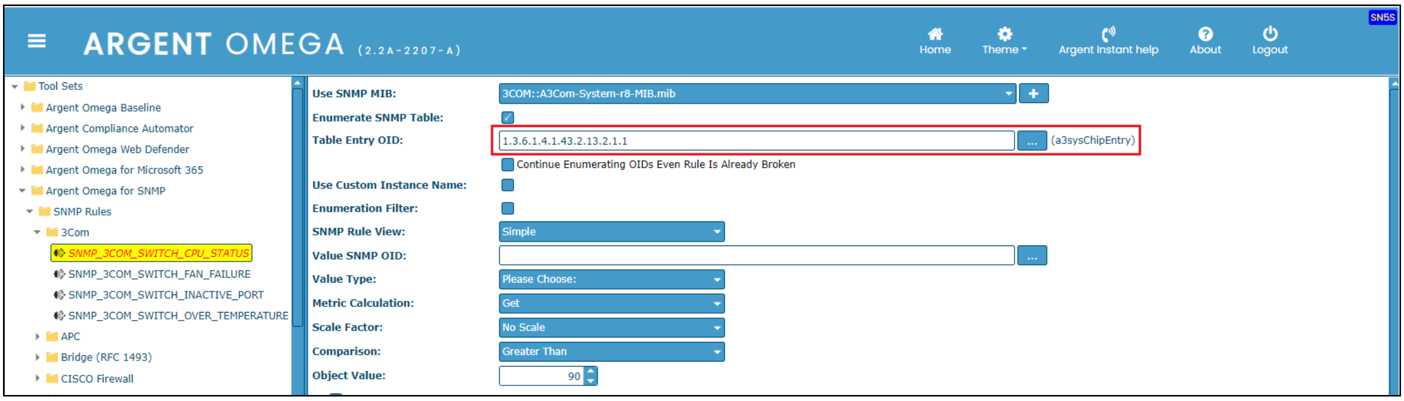
Application:

Reference URL:

Console Comment: *** High CPU Usage ***

Description:

Select the table entry and click OK.


ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant help
About
Logout
SN5S
Tool Sets
Argent Omega Baseline
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
SNMP Rules
3Com
SNMP_3COM_SWITCH_CPU_STATUS
SNMP_3COM_SWITCH_FAN_FAILURE
SNMP_3COM_SWITCH_INACTIVE_PORT
SNMP_3COM_SWITCH_OVER_TEMPERATURE
APC
Bridge (RFC 1493)
CISCO Firewall

Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Enumerate SNMP Table: ☑

Table Entry OID: 1.3.6.1.4.1.43.2.13.2.1.1 (a3sysChipEntry)

□ Continue Enumerating OIDs Even Rule Is Already Broken

Use Custom Instance Name: □

Enumeration Filter: □

SNMP Rule View: Simple

Value SNMP OID:

Value Type: Please Choose:

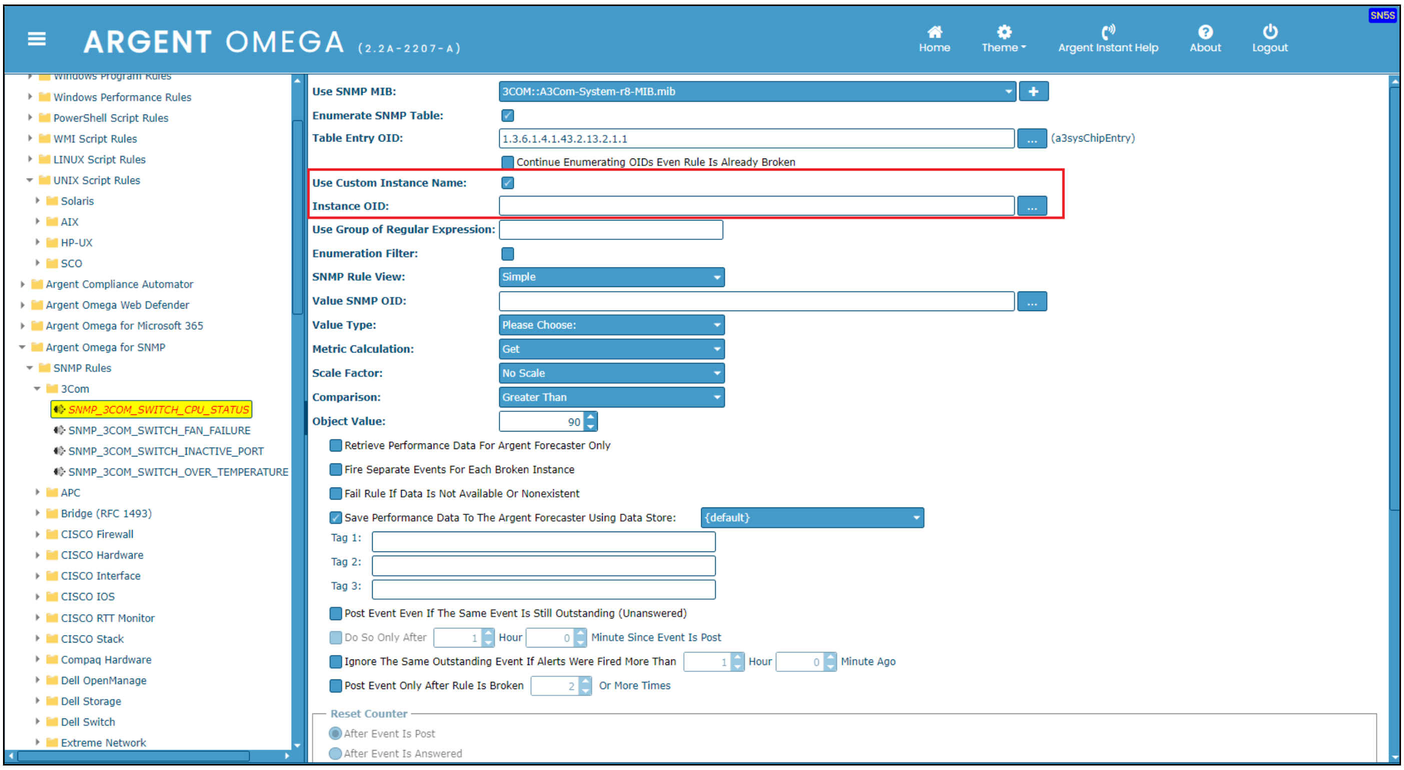
Metric Calculation: Get

Scale Factor: No Scale

Comparison: Greater Than

Object Value: 90

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 will be 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.



Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Enumerate SNMP Table: ☑

Table Entry OID: 1.3.6.1.4.1.43.2.13.2.1.1 (a3sysChipEntry)

☐ Continue Enumerating OIDs Even Rule Is Already Broken

Use Custom Instance Name: ☑

Instance OID:

Use Group of Regular Expression:

Enumeration Filter: ☐

SNMP Rule View: Simple

Value SNMP OID:

Value Type: Please Choose:

Metric Calculation: Get

Scale Factor: No Scale

Comparison: Greater Than

Object Value: 90

☐ Retrieve Performance Data For Argent Forecaster Only

☐ Fire Separate Events For Each Broken Instance

☐ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

☐ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

☐ Do So Only After 1 Hour 0 Minute Since Event Is Post

☐ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

☐ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

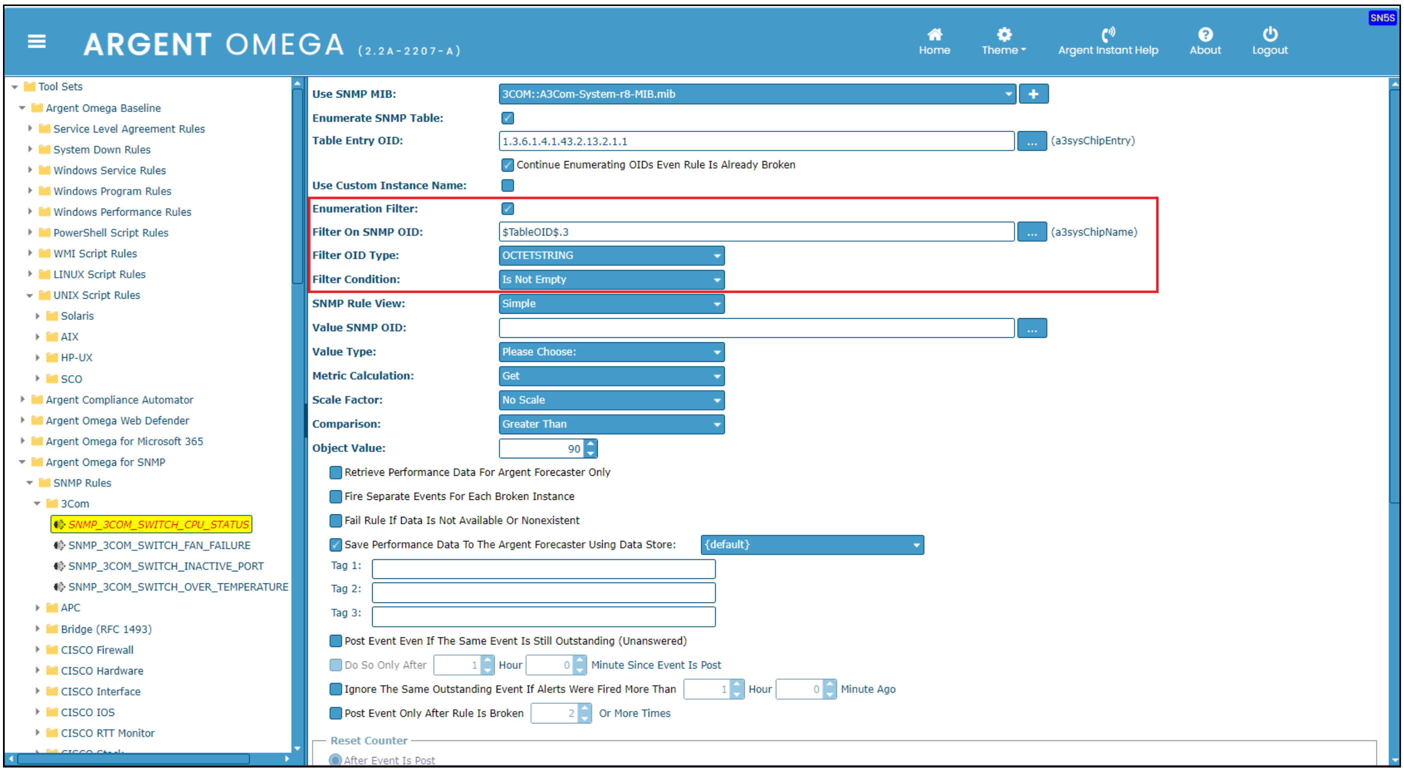
○ After Event Is Post

○ After Event Is Answered

If **Enumerate SNMP Table** is checked, check **Enumeration Filter** option if you want to apply filter for querying OID values from SNMP table. The Rule will be validated only if the specified filter condition is satisfied. You can apply filter on specific SNMP OID. The type of the 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.



Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Enumerate SNMP Table: ☑

Table Entry OID: 1.3.6.1.4.1.43.2.13.2.1.1 (a3sysChipEntry)

☑ Continue Enumerating OIDs Even Rule Is Already Broken

Use Custom Instance Name: ☐

Enumeration Filter: ☑

Filter On SNMP OID: $TableOID$.3 (a3sysChipName)

Filter OID Type: OCTETSTRING

Filter Condition: Is Not Empty

SNMP Rule View: Simple

Value SNMP OID:

Value Type: Please Choose:

Metric Calculation: Get

Scale Factor: No Scale

Comparison: Greater Than

Object Value: 90

☐ Retrieve Performance Data For Argent Forecaster Only

☐ Fire Separate Events For Each Broken Instance

☐ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

☐ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

☐ Do So Only After 1 Hour 0 Minute Since Event Is Post

☐ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

☐ Post Event Only After Rule Is Broken 2 Or More Times

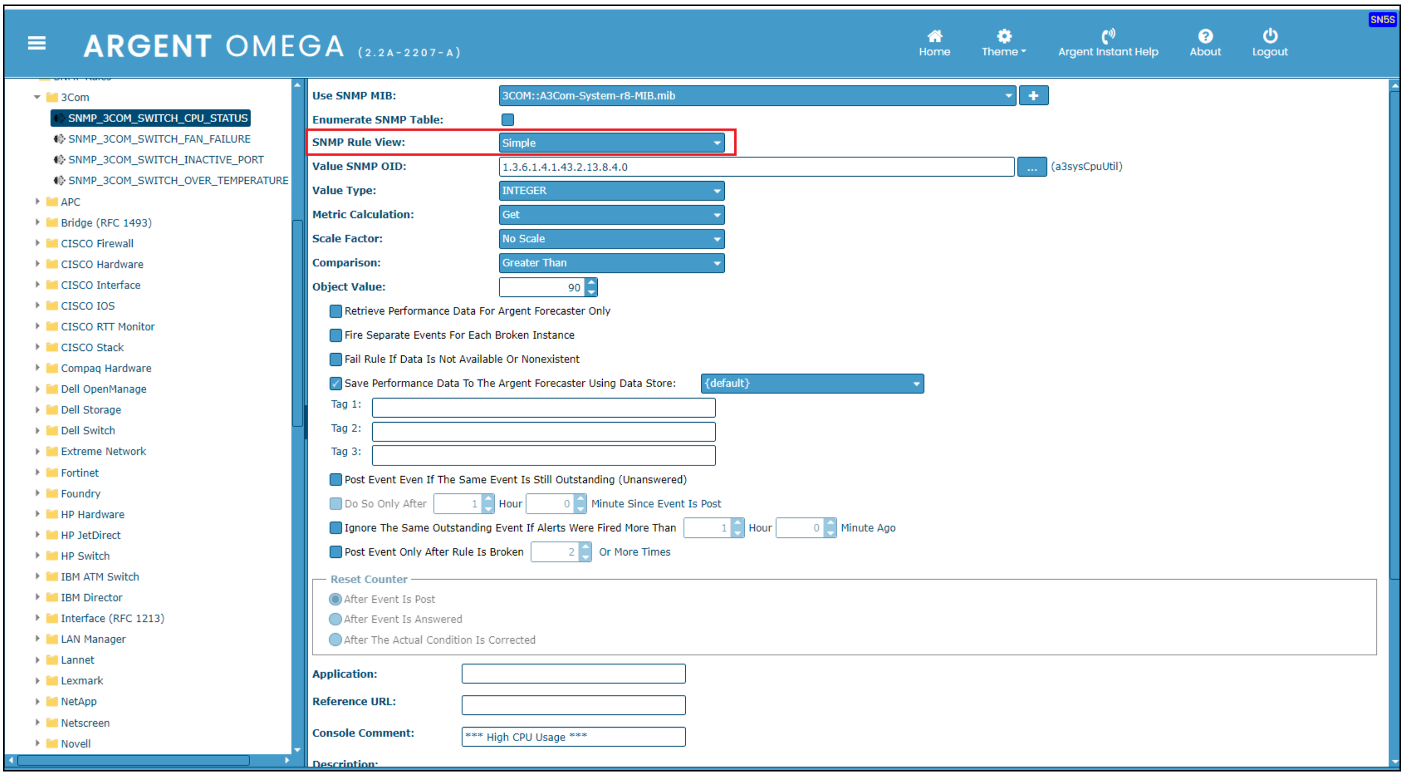
Reset Counter

○ After Event Is Post

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 view to configure SNMP parameters.



Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Enumerate SNMP Table: □

SNMP Rule View: Simple

Value SNMP OID: 1.3.6.1.4.1.43.2.13.8.4.0 ... (a3sysCpuUtil)

Value Type: INTEGER

Metric Calculation: Get

Scale Factor: No Scale

Comparison: Greater Than

Object Value: 90

□ Retrieve Performance Data For Argent Forecaster Only

□ Fire Separate Events For Each Broken Instance

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

Application:

Reference URL:

Console Comment: *** High CPU Usage ***

Description:

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.

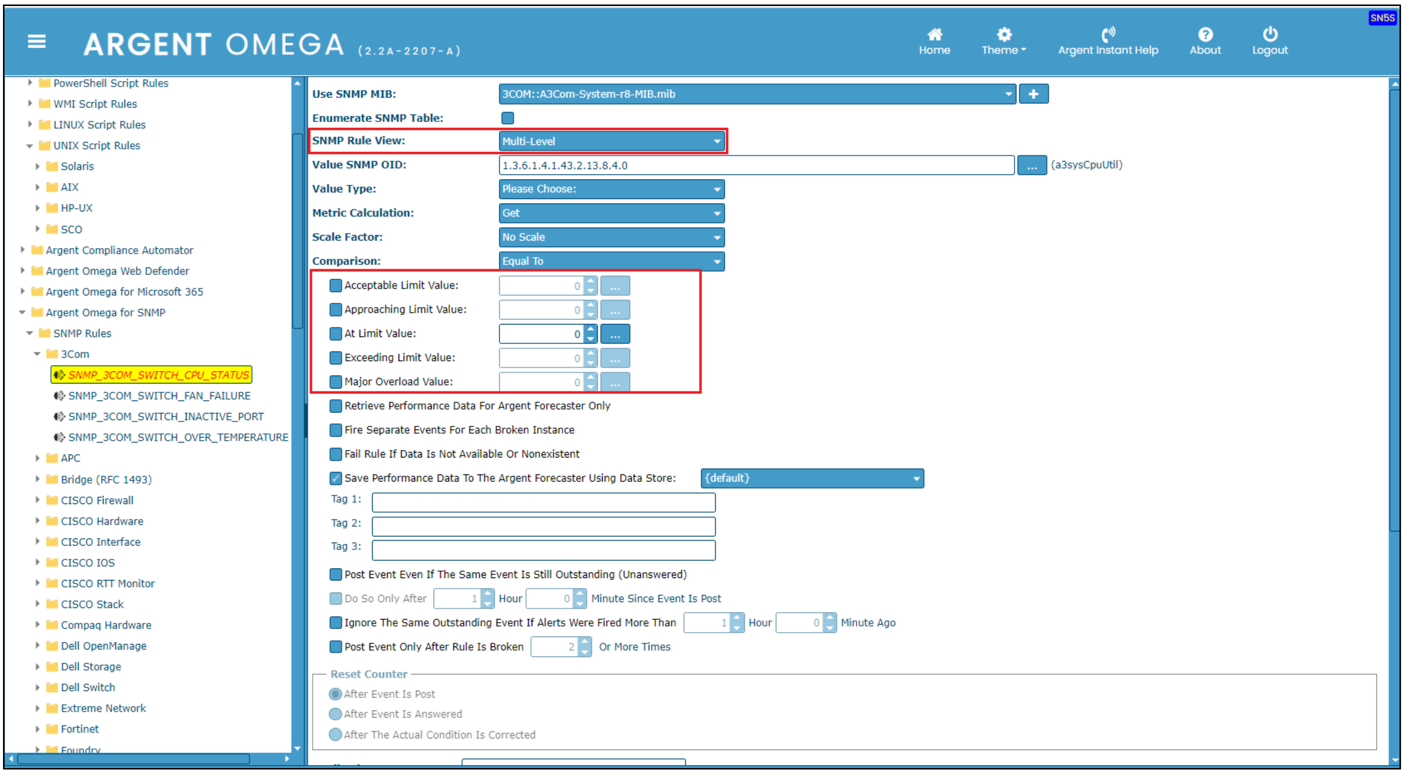
Scale Factor: Scale of measurement of metric value

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

Object Value: Threshold to compare

Multi-Level

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



Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Enumerate SNMP Table: □

SNMP Rule View: Multi-Level

Value SNMP OID: 1.3.6.1.4.1.43.2.13.8.4.0 (a3sysCpuUtil)

Value Type: Please Choose:

Metric Calculation: Get

Scale Factor: No Scale

Comparison: Equal To

□ Acceptable Limit Value: 0

□ Approaching Limit Value: 0

□ At Limit Value: 0

□ Exceeding Limit Value: 0

□ Major Overload Value: 0

□ Retrieve Performance Data For Argent Forecaster Only

□ Fire Separate Events For Each Broken Instance

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

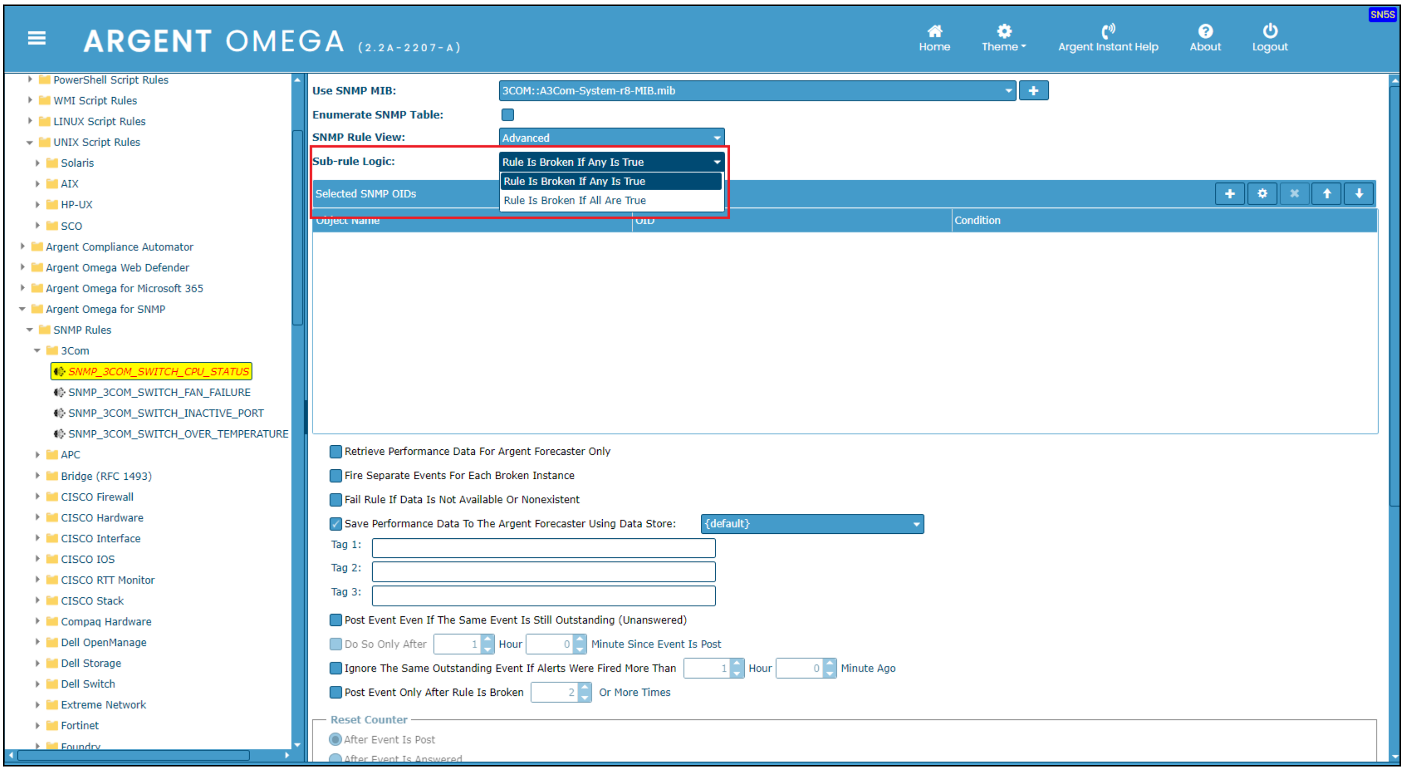
○ After Event Is Answered

○ After The Actual Condition Is Corrected

Advanced

Multiple conditions can be specified in Advanced Rule view. Rule broken logic can be se selected from

Sub-Rule Logic combo box.



Use SNMP MIB: 3COM::A3Com-System-r8-MIB.mib

Enumerate SNMP Table: □

SNMP Rule View: Advanced

Sub-rule Logic: Rule Is Broken If Any Is True

Selected SNMP OIDs

Object Name	OID	Condition

□ Retrieve Performance Data For Argent Forecaster Only

□ Fire Separate Events For Each Broken Instance

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

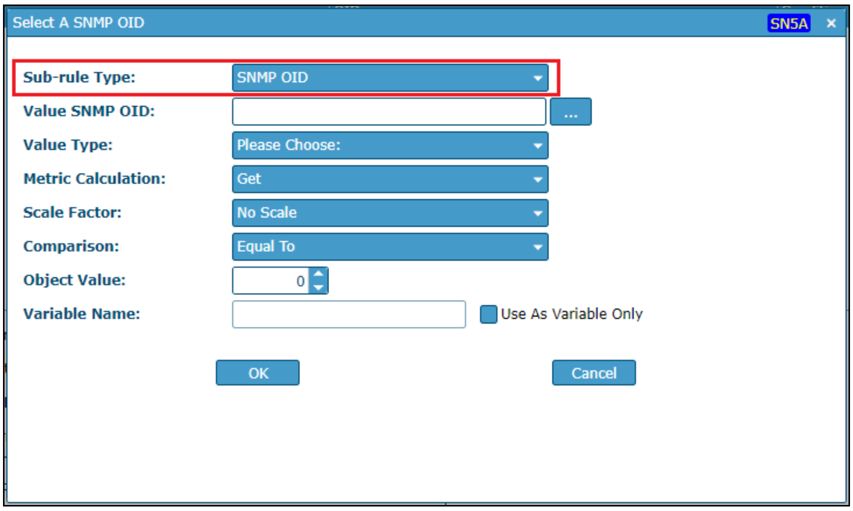
● After Event Is Post

○ After Event Is Answered

Rule conditions can be added by clicking “+” button. A sub-rule definition dialog will be popped up; there you can define the Rule condition.

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

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



Select A SNMP OID

Sub-rule Type: SNMP OID

Value SNMP OID:

Value Type: Please Choose:

Metric Calculation: Get

Scale Factor: No Scale

Comparison: Equal To

Object Value: 0

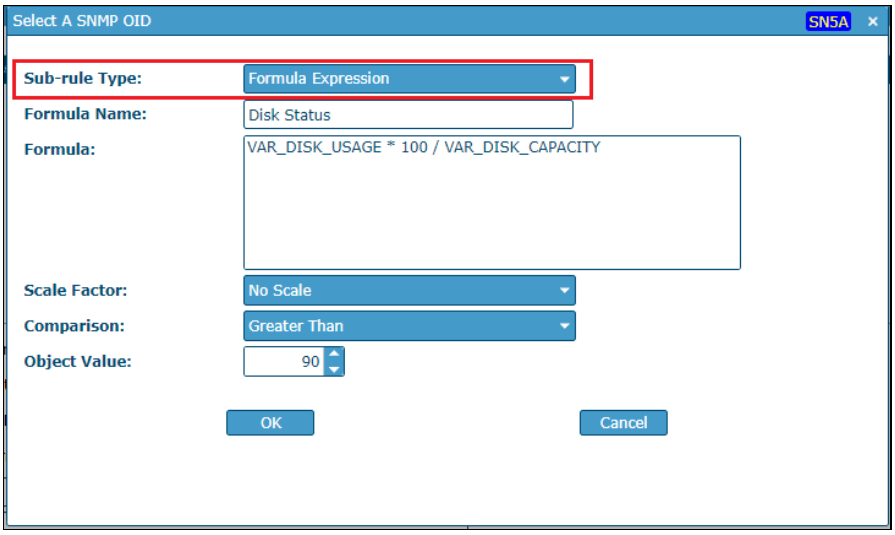
Variable Name:

□ Use As Variable Only

All parameters described in the **Simple** view (Value SNMP OID, Value Type, Metric Calculation, Scale Factor, Comparison, and Object Value) needs to be 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. You can use the variable 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 your environmental monitor returns the temperature of the server room in Celsius, you can convert this metric to Fahrenheit. Or you could measure the uptime of a server or device by converting TIMETICKS to hours. (TIMETICKS are hundredths of a second). Or you could add together several SNMP metrics to get a total traffic figure.



Select A SNMP OID

Sub-rule Type: Formula Expression

Formula Name: Disk Status

Formula: VAR_DISK_USAGE * 100 / VAR_DISK_CAPACITY

Scale Factor: No Scale

Comparison: Greater Than

Object Value: 90

Specify a name in **Formula Name** field.

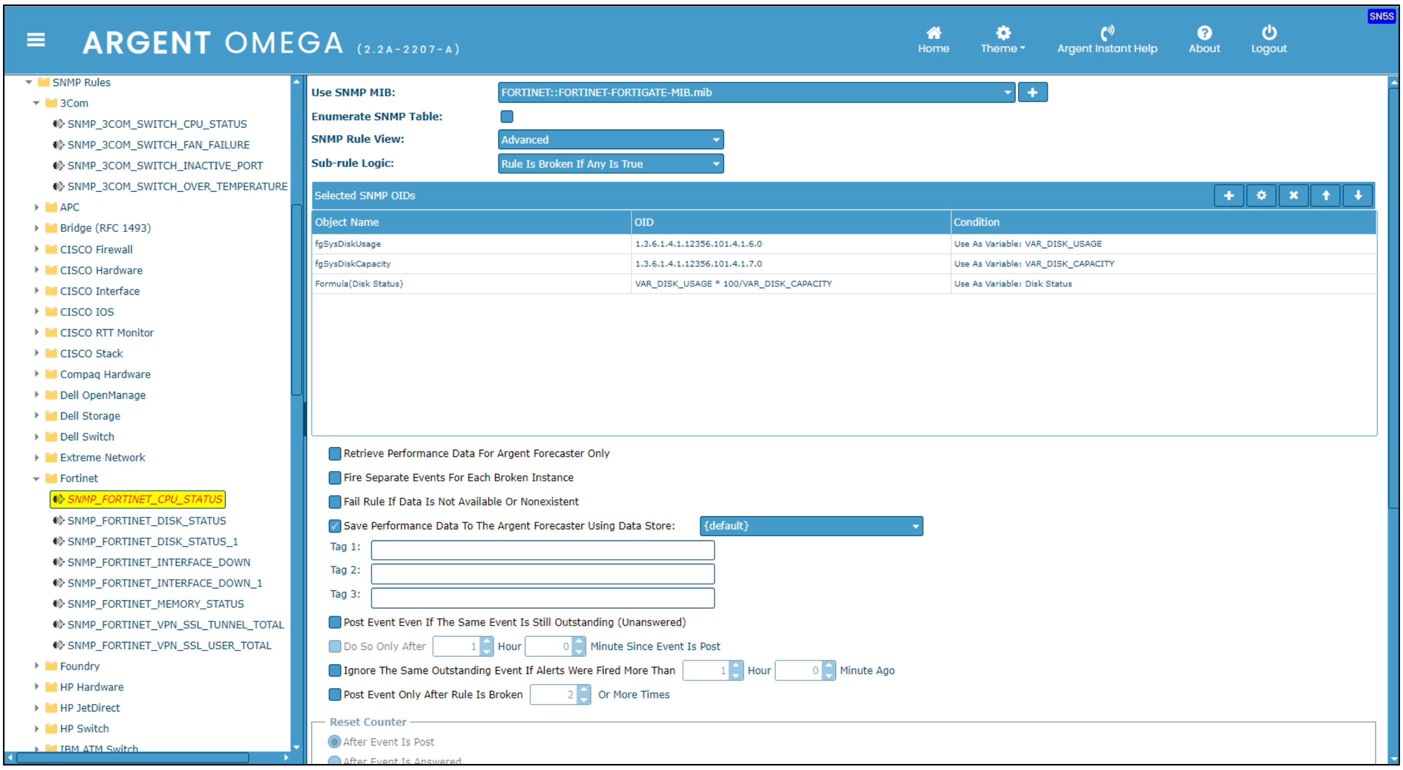
Specify the formula expression in **Formula** field. The formula specified in the screenshot VAR_DISK_USAGE * 100 / VAR_DISK_CAPACITY, where VAR_DISK_USAGE and VAR_DISK_CAPACITY are variables defined using SNMP OID sub-rule type.

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

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

Object Value defines the threshold to compare.

The following is a sample Advanced type Rule configured.


ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant Help
About
Logout
SN5S
SNMP Rules
3Com
SNMP_3COM_SWITCH_CPU_STATUS
SNMP_3COM_SWITCH_FAN_FAILURE
SNMP_3COM_SWITCH_INACTIVE_PORT
SNMP_3COM_SWITCH_OVER_TEMPERATURE
APC
Bridge (RFC 1493)
CISCO Firewall
CISCO Hardware
CISCO Interface
CISCO IOS
CISCO RTT Monitor
CISCO Stack
Compaq Hardware
Dell OpenManage
Dell Storage
Dell Switch
Extreme Network
Fortinet
SNMP_FORTINET_CPU_STATUS
SNMP_FORTINET_DISK_STATUS
SNMP_FORTINET_DISK_STATUS_1
SNMP_FORTINET_INTERFACE_DOWN
SNMP_FORTINET_INTERFACE_DOWN_1
SNMP_FORTINET_MEMORY_STATUS
SNMP_FORTINET_VPN_SSL_TUNNEL_TOTAL
SNMP_FORTINET_VPN_SSL_USER_TOTAL
Foundry
HP Hardware
HP JetDirect
HP Switch
IBM ATM Switch

Use SNMP MIB: FORTINET::FORTINET-FORTIGATE-MIB.mib

Enumerate SNMP Table: □

SNMP Rule View: Advanced

Sub-rule Logic: Rule Is Broken If Any Is True

Selected SNMP OIDs

Object Name	OID	Condition
fgSysDiskUsage	1.3.6.1.4.1.12356.101.4.1.6.0	Use As Variable: VAR_DISK_USAGE
fgSysDiskCapacity	1.3.6.1.4.1.12356.101.4.1.7.0	Use As Variable: VAR_DISK_CAPACITY
Formula(Disk Status)	VAR_DISK_USAGE * 100/VAR_DISK_CAPACITY	Use As Variable: Disk Status

□ Retrieve Performance Data For Argent Forecaster Only

□ Fire Separate Events For Each Broken Instance

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

Retrieve Performance Data For Argent Forecaster Only option only saves performance metrics to Argent Forecaster, does not alert the Rule.

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

SNMP Trap Rules

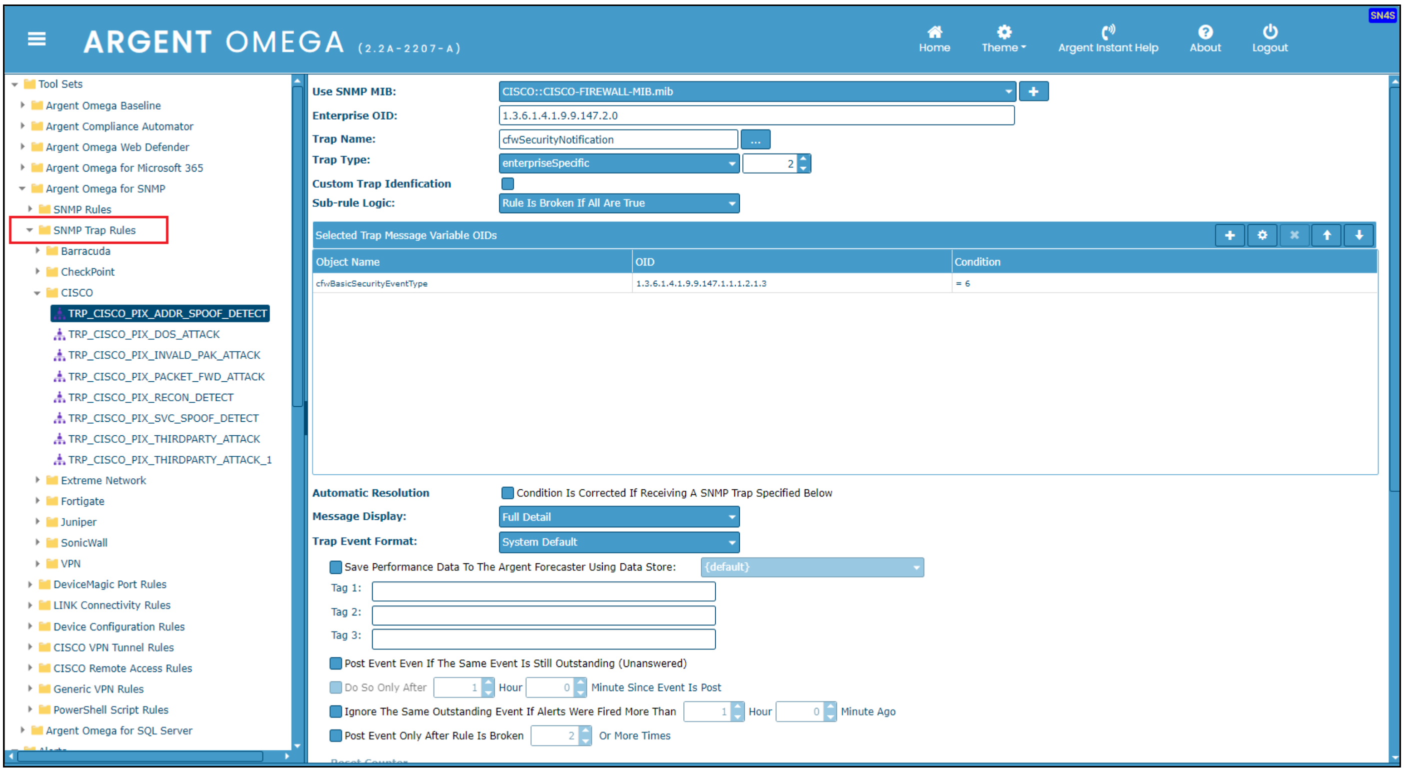
SNMP Traps are unsolicited SNMP information packets sent from any SNMP-compliant device to an SNMP manager, such as Argent Omega.

Traps can be sent for many reasons, such as hard drive failures, cooling fans that aren't 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 something like a fan problem that comes and goes quickly might not be noticed. On the other hand, if the device sends an SNMP Trap that the fan isn't running correctly, Argent can notify you immediately.

You can configure SNMP Trap Monitor definitions to listen for specific traps, even for specific information within a trap, and which alerts to fire if that trap arrives. If a trap that arrives matches an SNMP Trap Monitor definition that's in Production Mode, the selected alerts are fired.

The Argent for SNMP comes equipped with a large number of pre-defined SNMP Trap Monitor definitions for a wide variety of devices.


SN4S
ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant Help
About
Logout
Tool Sets
Argent Omega Baseline
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
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
TRP_CISCO_PIX_THIRDPARTY_ATTACK_1
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}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

The following options needs to be configured to handle SNMP Traps:

Select MIB file from **Use SNMP MIB** combo box. 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.

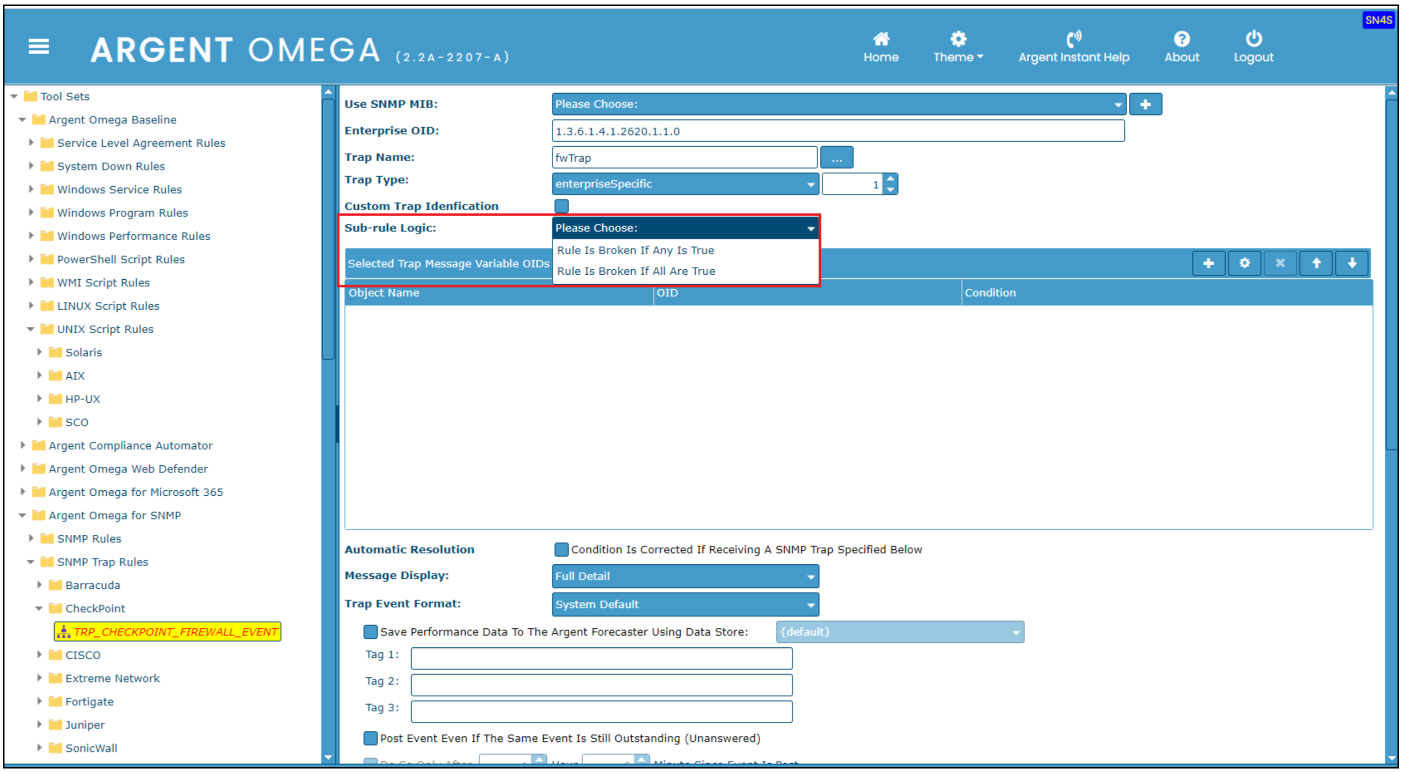
Specify trap Enterprise OID in **Enterprise OID** field.

Whenever an SNMP Trap is sent, it includes an Enterprise OID. This includes the manufacturer ID, and maybe even 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 Trap filter. This is to differentiate between trap events, say, a trap indicating a power supply failure and a trap showing that a fan was inserted, we need to get a little more specific. Otherwise, any trap with a specified Enterprise OID would create the same alert. You can also browse and select Trap Name from selected MIB file.

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



Use SNMP MIB: Please Choose: +

Enterprise OID: 1.3.6.1.4.1.2620.1.1.0

Trap Name: fwTrap ...

Trap Type: enterpriseSpecific 1

Custom Trap Idenfication □

Sub-rule Logic: Please Choose:
- Rule Is Broken If Any Is True
- Rule Is Broken If All Are True

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}

Tag 1:

Tag 2:

Tag 3:

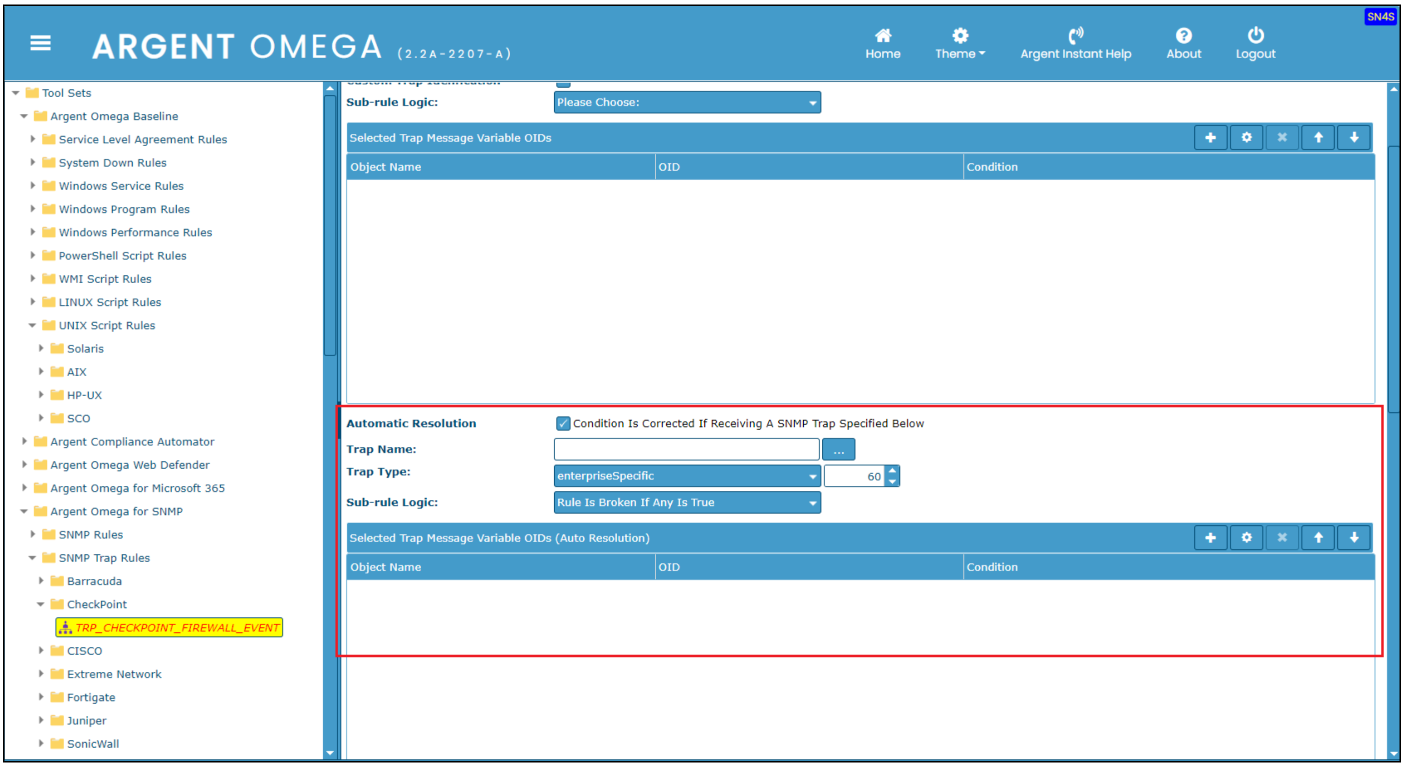
□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

Sub-rule condition can be added by clicking “+” button. A sub-rule definition dialog will pop up; there, you can define the Rule condition. Add sub-rule conditions in the same way we did 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 and your UPS kicks on, it could send a trap indicating it's running on battery power. If this condition were to remain uncorrected too long, of course, the UPS's battery would run out and the computers would simply stop completely.

If utility power is restored (hopefully before the battery dies), the UPS could send a trap indicating as such. You can configure Argent 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 you did above, but with the settings for the "normal power" trap.



Sub-rule Logic: Please Choose:

Selected Trap Message Variable OIDs

Object Name	OID	Condition

Automatic Resolution ☑ Condition Is Corrected If Receiving A SNMP Trap Specified Below

Trap Name:

Trap Type: enterpriseSpecific 60

Sub-rule Logic: Rule Is Broken If Any Is True

Selected Trap Message Variable OIDs (Auto Resolution)

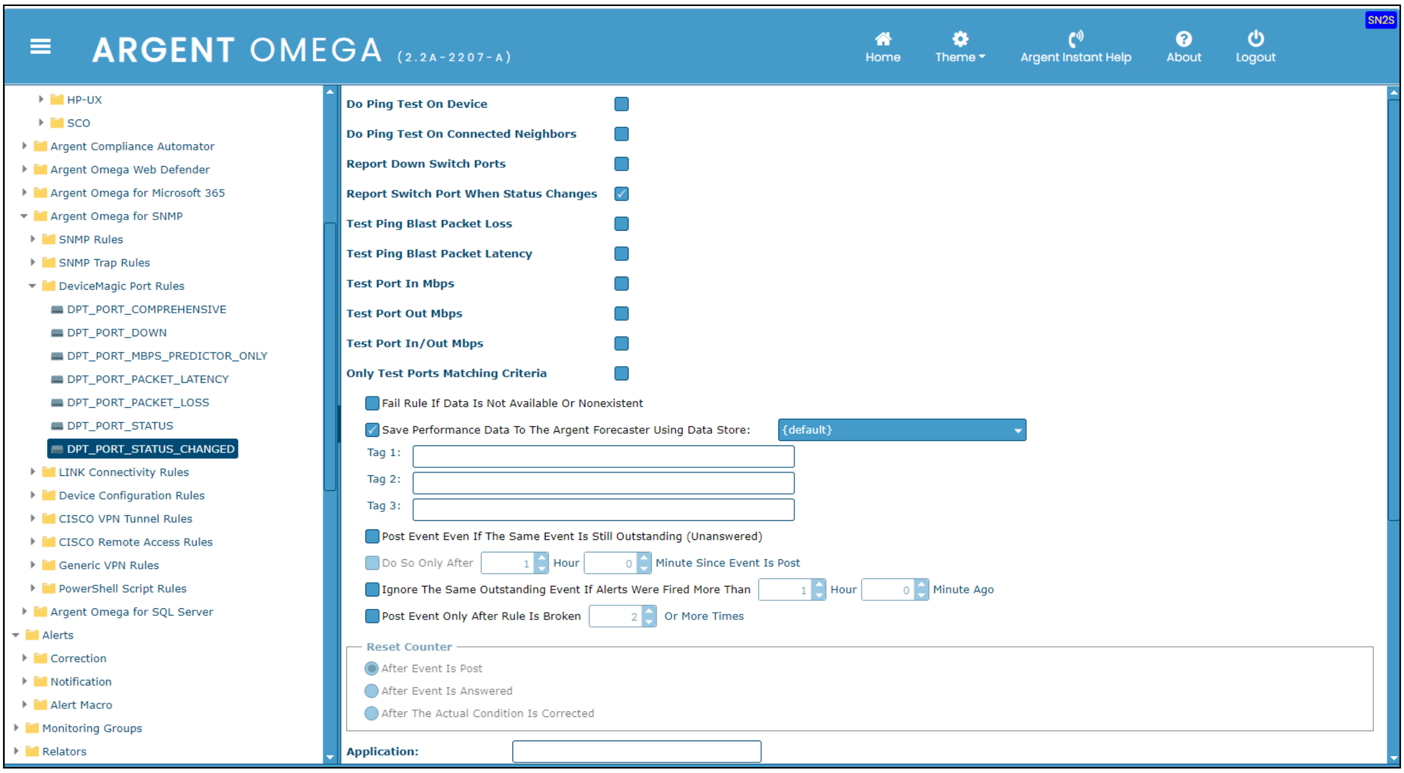
Object Name	OID	Condition

DeviceMagic Port Rules

Device Magic Rules monitor the switches without dealing with individual explicit MIBs and OIDs.

Device Magic monitors the following for switch host as well as individual ports:

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



Do Ping Test On Device □

Do Ping Test On Connected Neighbors □

Report Down Switch Ports □

Report Switch Port When Status Changes ☑

Test Ping Blast Packet Loss □

Test Ping Blast Packet Latency □

Test Port In Mbps □

Test Port Out Mbps □

Test Port In/Out Mbps □

Only Test Ports Matching Criteria □

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

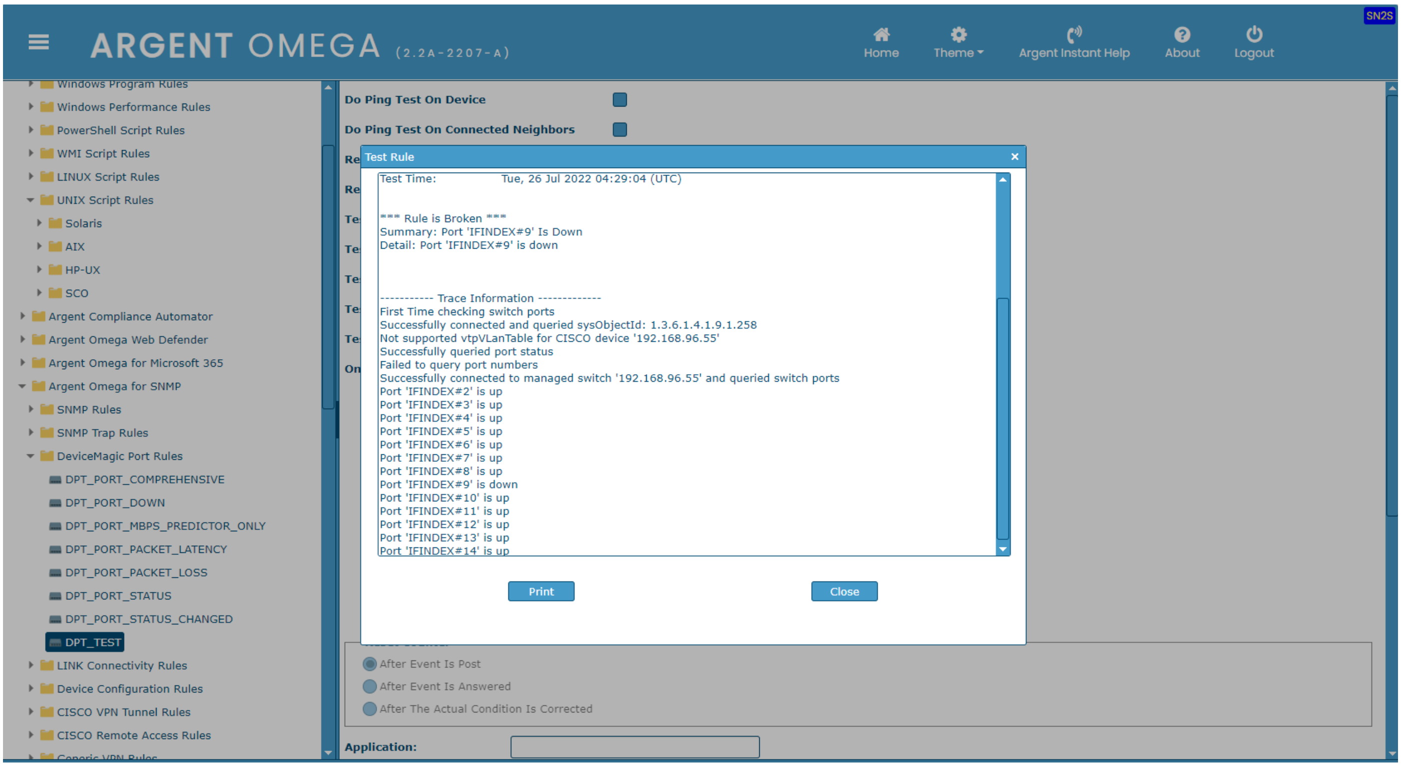
○ After The Actual Condition Is Corrected

Application:

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 ports is down. Sample Rule result is below:



Do Ping Test On Device □

Do Ping Test On Connected Neighbors □

○ After Event Is Post

○ After Event Is Answered

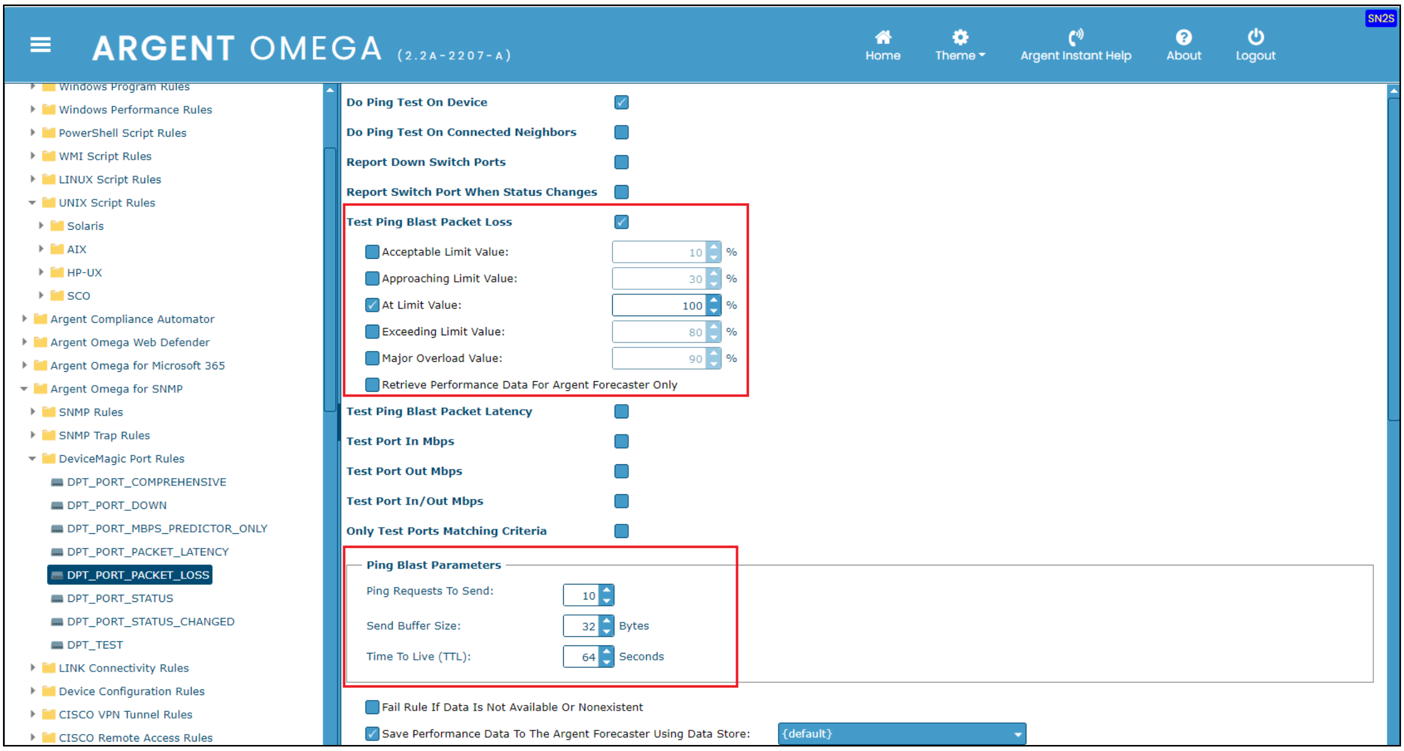
○ After The Actual Condition Is Corrected

Application:

```
Test Time:              Tue, 26 Jul 2022 04:29:04 (UTC)


*** Rule is Broken ***
Summary: Port 'IFINDEX#9' Is Down
Detail: Port 'IFINDEX#9' is down



---------- Trace Information ------------
First Time checking switch ports
Successfully connected and queried sysObjectId: 1.3.6.1.4.1.9.1.258
Not supported vtpVLanTable for CISCO device '192.168.96.55'
Successfully queried port status
Failed to query port numbers
Successfully connected to managed switch '192.168.96.55' and queried switch ports
Port 'IFINDEX#2' is up
Port 'IFINDEX#3' is up
Port 'IFINDEX#4' is up
Port 'IFINDEX#5' is up
Port 'IFINDEX#6' is up
Port 'IFINDEX#7' is up
Port 'IFINDEX#8' is up
Port 'IFINDEX#9' is down
Port 'IFINDEX#10' is up
Port 'IFINDEX#11' is up
Port 'IFINDEX#12' is up
Port 'IFINDEX#13' is up
Port 'IFINDEX#14' is up
```

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 an 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.



Do Ping Test On Device ☑

Do Ping Test On Connected Neighbors □

Report Down Switch Ports □

Report Switch Port When Status Changes □

Test Ping Blast Packet Loss ☑

□ Acceptable Limit Value:	10	%
□ Approaching Limit Value:	30	%
☑ At Limit Value:	100	%
□ Exceeding Limit Value:	80	%
□ Major Overload Value:	90	%

□ Retrieve Performance Data For Argent Forecaster Only

Test Ping Blast Packet Latency □

Test Port In Mbps □

Test Port Out Mbps □

Test Port In/Out Mbps □

Only Test Ports Matching Criteria □

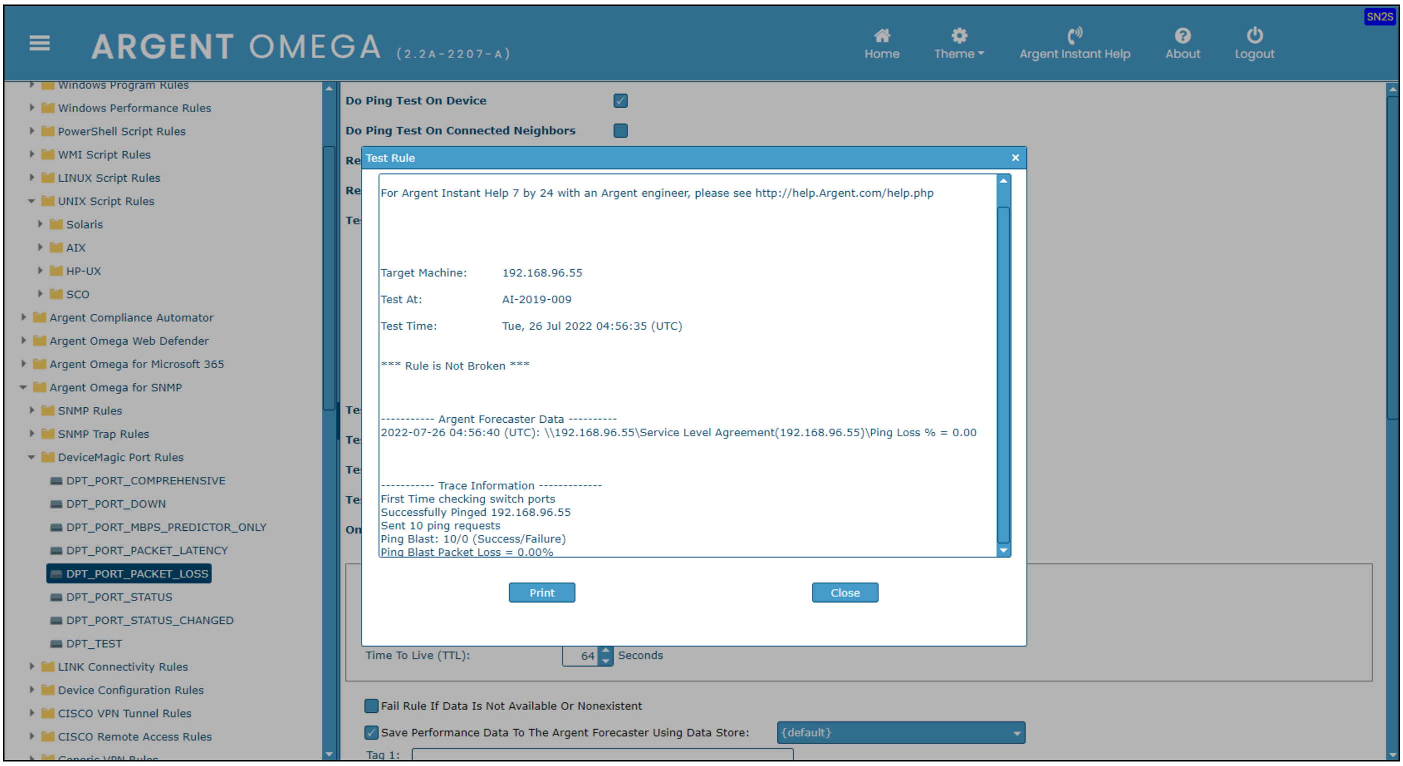
Ping Blast Parameters

Ping Requests To Send:	10	
Send Buffer Size:	32	Bytes
Time To Live (TTL):	64	Seconds

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

The following is an example of the Rule result:



Do Ping Test On Device ☑

Do Ping Test On Connected Neighbors ☐

```
For Argent Instant Help 7 by 24 with an Argent engineer, please see http://help.Argent.com/help.php



Target Machine:       192.168.96.55

Test At:              AI-2019-009

Test Time:            Tue, 26 Jul 2022 04:56:35 (UTC)


*** Rule is Not Broken ***



----------- Argent Forecaster Data ----------
2022-07-26 04:56:40 (UTC): \\192.168.96.55\Service Level Agreement(192.168.96.55)\Ping Loss % = 0.00



----------- Trace Information -------------
First Time checking switch ports
Successfully Pinged 192.168.96.55
Sent 10 ping requests
Ping Blast: 10/0 (Success/Failure)
Ping Blast Packet Loss = 0.00%
```

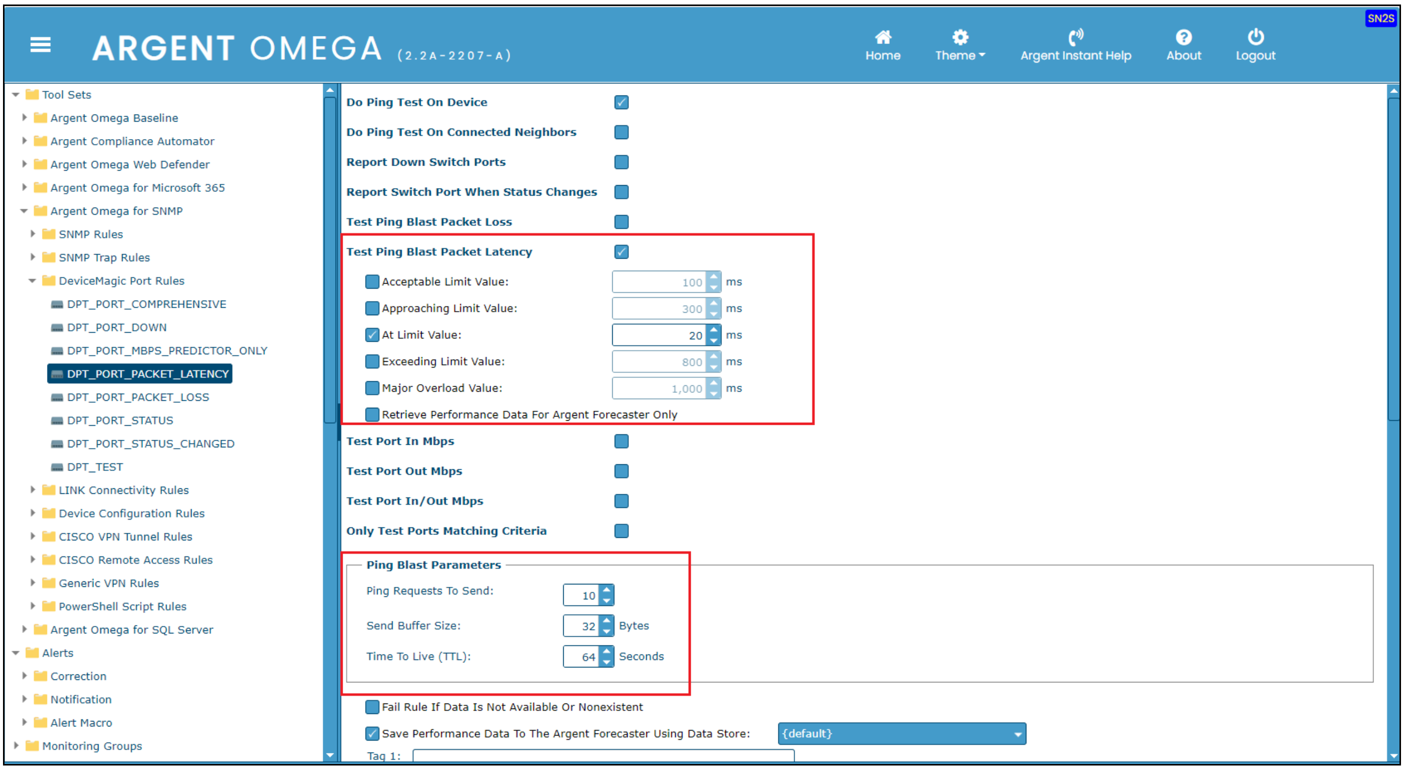
Time To Live (TTL): 64 Seconds

☐ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Check the option **Test Ping Blast Packet Latency** to check the packet latency (ms) for a device connected each port of an 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 needs 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.



Do Ping Test On Device ☑

Do Ping Test On Connected Neighbors ☐

Report Down Switch Ports ☐

Report Switch Port When Status Changes ☐

Test Ping Blast Packet Loss ☐

Test Ping Blast Packet Latency ☑

☐ Acceptable Limit Value: 100 ms

☐ Approaching Limit Value: 300 ms

☑ At Limit Value: 20 ms

☐ Exceeding Limit Value: 800 ms

☐ Major Overload Value: 1,000 ms

☐ Retrieve Performance Data For Argent Forecaster Only

Test Port In Mbps ☐

Test Port Out Mbps ☐

Test Port In/Out Mbps ☐

Only Test Ports Matching Criteria ☐

Ping Blast Parameters

Ping Requests To Send: 10

Send Buffer Size: 32 Bytes

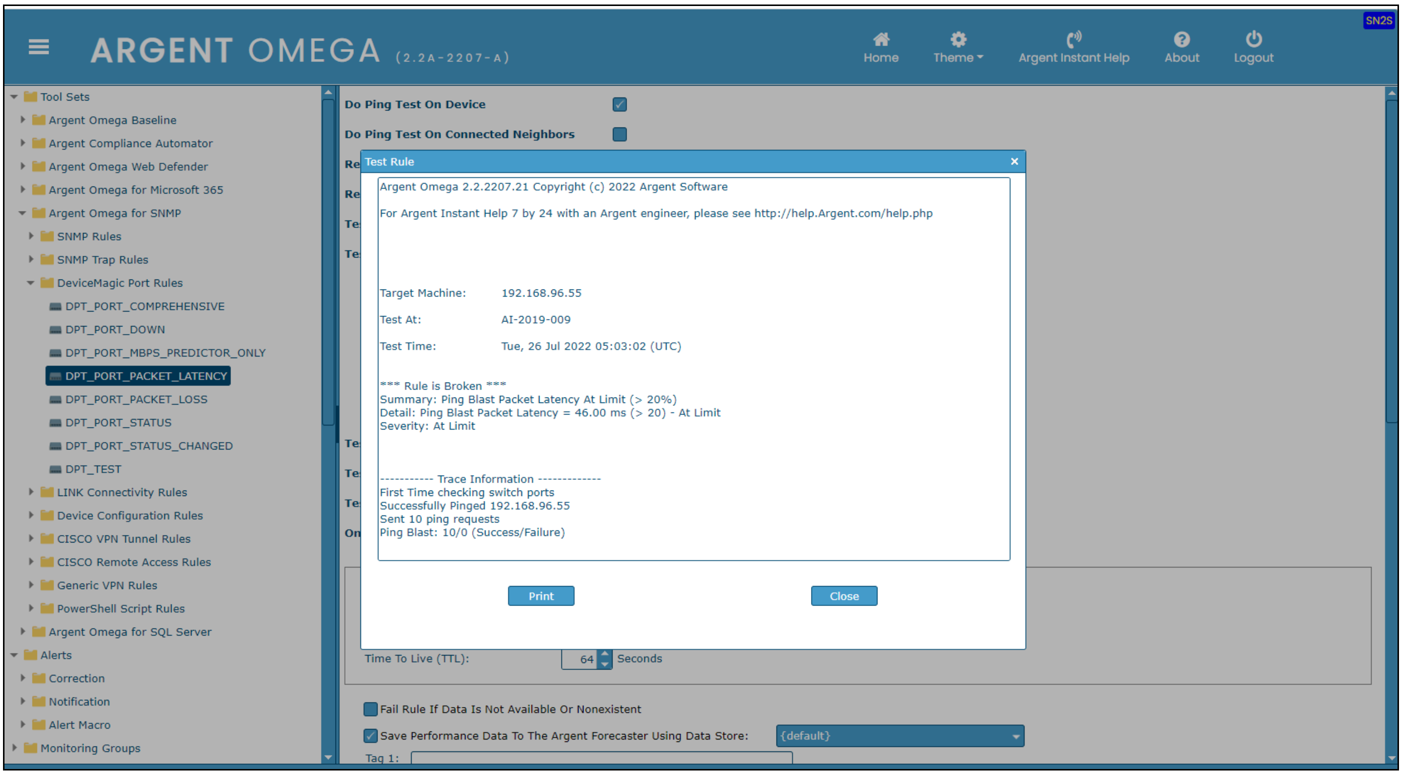
Time To Live (TTL): 64 Seconds

☐ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

The following is an example of the Rule result:



Do Ping Test On Device ☑

Do Ping Test On Connected Neighbors □

```
Argent Omega 2.2.2207.21 Copyright (c) 2022 Argent Software

For Argent Instant Help 7 by 24 with an Argent engineer, please see http://help.Argent.com/help.php



Target Machine:     192.168.96.55

Test At:            AI-2019-009

Test Time:          Tue, 26 Jul 2022 05:03:02 (UTC)


*** Rule is Broken ***
Summary: Ping Blast Packet Latency At Limit (> 20%)
Detail: Ping Blast Packet Latency = 46.00 ms (> 20) - At Limit
Severity: At Limit


---------- Trace Information ------------
First Time checking switch ports
Successfully Pinged 192.168.96.55
Sent 10 ping requests
Ping Blast: 10/0 (Success/Failure)
```

Time To Live (TTL): 64 Seconds

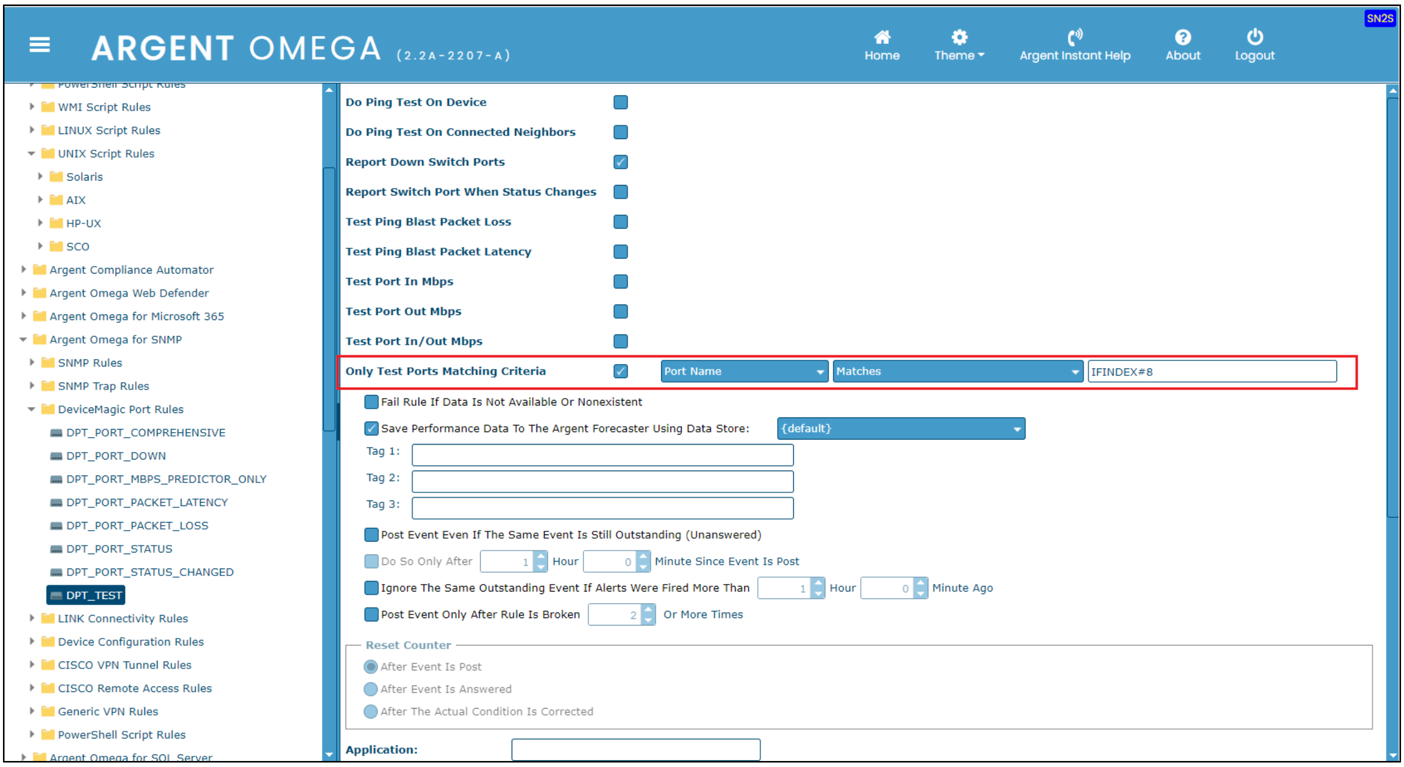
□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

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

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



Do Ping Test On Device □

Do Ping Test On Connected Neighbors □

Report Down Switch Ports ☑

Report Switch Port When Status Changes □

Test Ping Blast Packet Loss □

Test Ping Blast Packet Latency □

Test Port In Mbps □

Test Port Out Mbps □

Test Port In/Out Mbps □

Only Test Ports Matching Criteria ☑ Port Name Matches IFINDEX#8

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

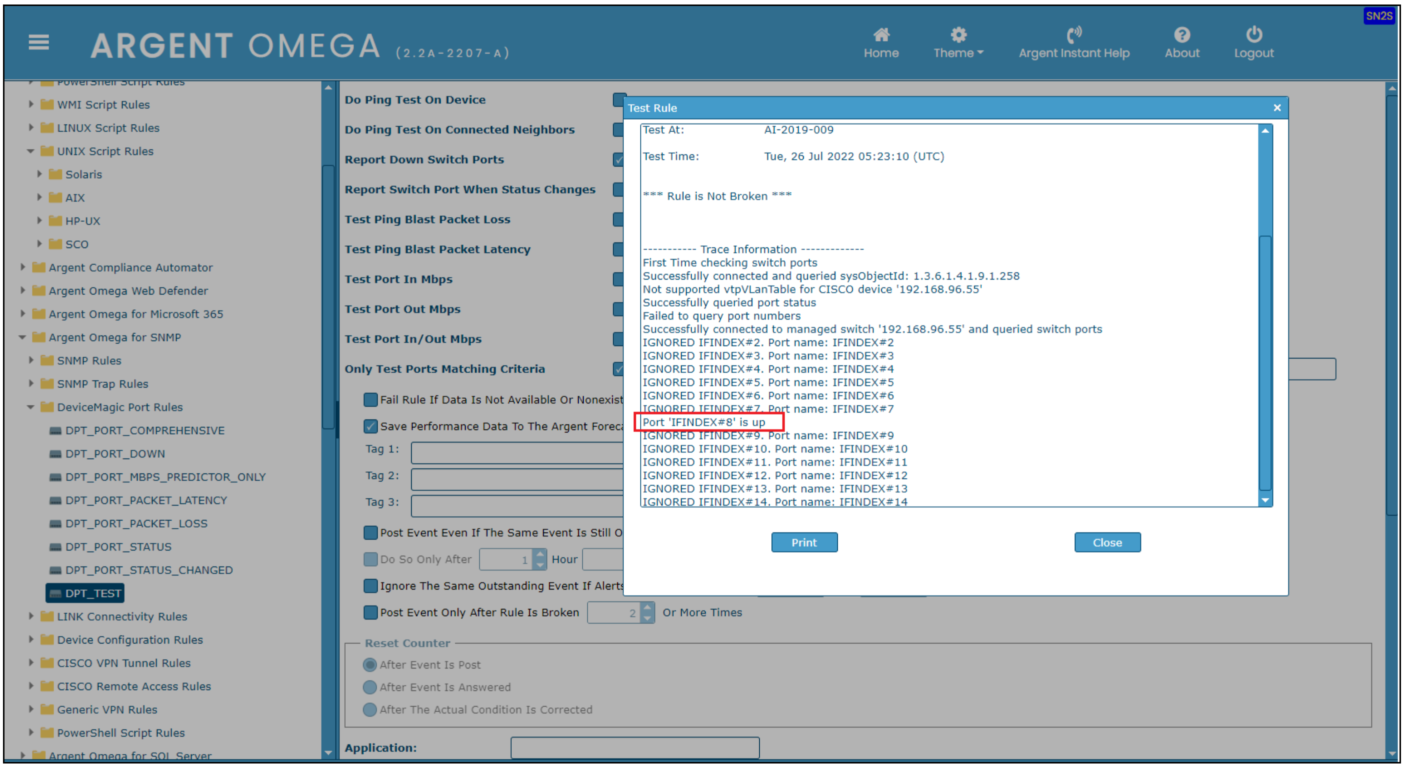
○ After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

Application:

The following is an example of the Rule result:



Do Ping Test On Device
Do Ping Test On Connected Neighbors
Report Down Switch Ports ☑
Report Switch Port When Status Changes
Test Ping Blast Packet Loss
Test Ping Blast Packet Latency
Test Port In Mbps
Test Port Out Mbps
Test Port In/Out Mbps
Only Test Ports Matching Criteria ☑

□ Fail Rule If Data Is Not Available Or Nonexist
☑ Save Performance Data To The Argent Foreca
Tag 1:
Tag 2:
Tag 3:
□ Post Event Even If The Same Event Is Still O
□ Do So Only After 1 Hour
□ Ignore The Same Outstanding Event If Alerts
□ Post Event Only After Rule Is Broken 2 Or More Times

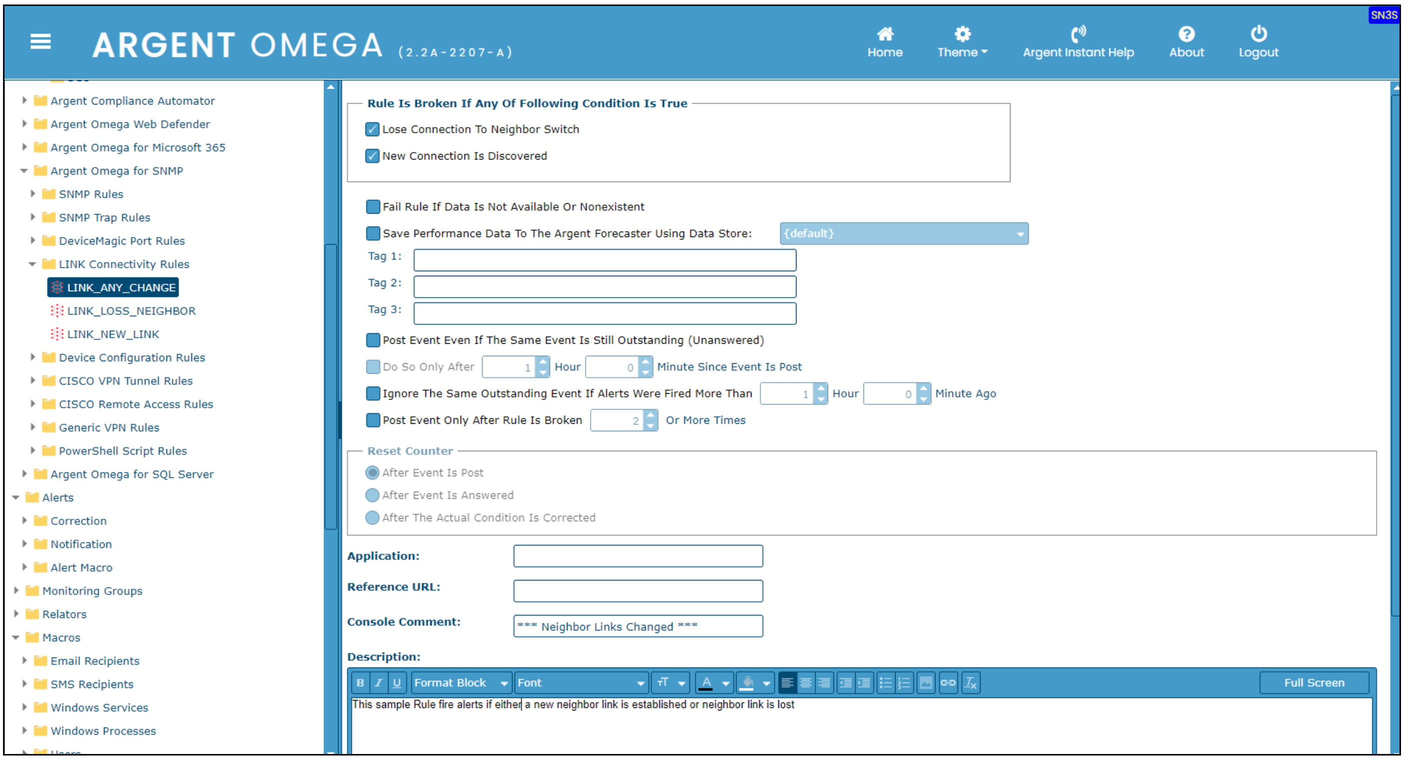
Reset Counter
● After Event Is Post
○ After Event Is Answered
○ After The Actual Condition Is Corrected

Application:

```
Test At:                AI-2019-009

Test Time:              Tue, 26 Jul 2022 05:23:10 (UTC)


*** Rule is Not Broken ***



----------- Trace Information -------------
First Time checking switch ports
Successfully connected and queried sysObjectId: 1.3.6.1.4.1.9.1.258
Not supported vtpVLanTable for CISCO device '192.168.96.55'
Successfully queried port status
Failed to query port numbers
Successfully connected to managed switch '192.168.96.55' and queried switch ports
IGNORED IFINDEX#2. Port name: IFINDEX#2
IGNORED IFINDEX#3. Port name: IFINDEX#3
IGNORED IFINDEX#4. Port name: IFINDEX#4
IGNORED IFINDEX#5. Port name: IFINDEX#5
IGNORED IFINDEX#6. Port name: IFINDEX#6
IGNORED IFINDEX#7. Port name: IFINDEX#7
Port 'IFINDEX#8' is up
IGNORED IFINDEX#9. Port name: IFINDEX#9
IGNORED IFINDEX#10. Port name: IFINDEX#10
IGNORED IFINDEX#11. Port name: IFINDEX#11
IGNORED IFINDEX#12. Port name: IFINDEX#12
IGNORED IFINDEX#13. Port name: IFINDEX#13
IGNORED IFINDEX#14. Port name: IFINDEX#14
```

LINK Connectivity Rules

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



Rule Is Broken If Any Of Following Condition Is True
☑ Lose Connection To Neighbor Switch
☑ New Connection Is Discovered

□ Fail Rule If Data Is Not Available Or Nonexistent
□ Save Performance Data To The Argent Forecaster Using Data Store: {default}
Tag 1:
Tag 2:
Tag 3:
□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)
□ Do So Only After 1 Hour 0 Minute Since Event Is Post
□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter
● After Event Is Post
○ After Event Is Answered
○ After The Actual Condition Is Corrected

Application:
Reference URL:
Console Comment: *** Neighbor Links Changed ***
Description:
This sample Rule fire alerts if either a new neighbor link is established or neighbor link is lost

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

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

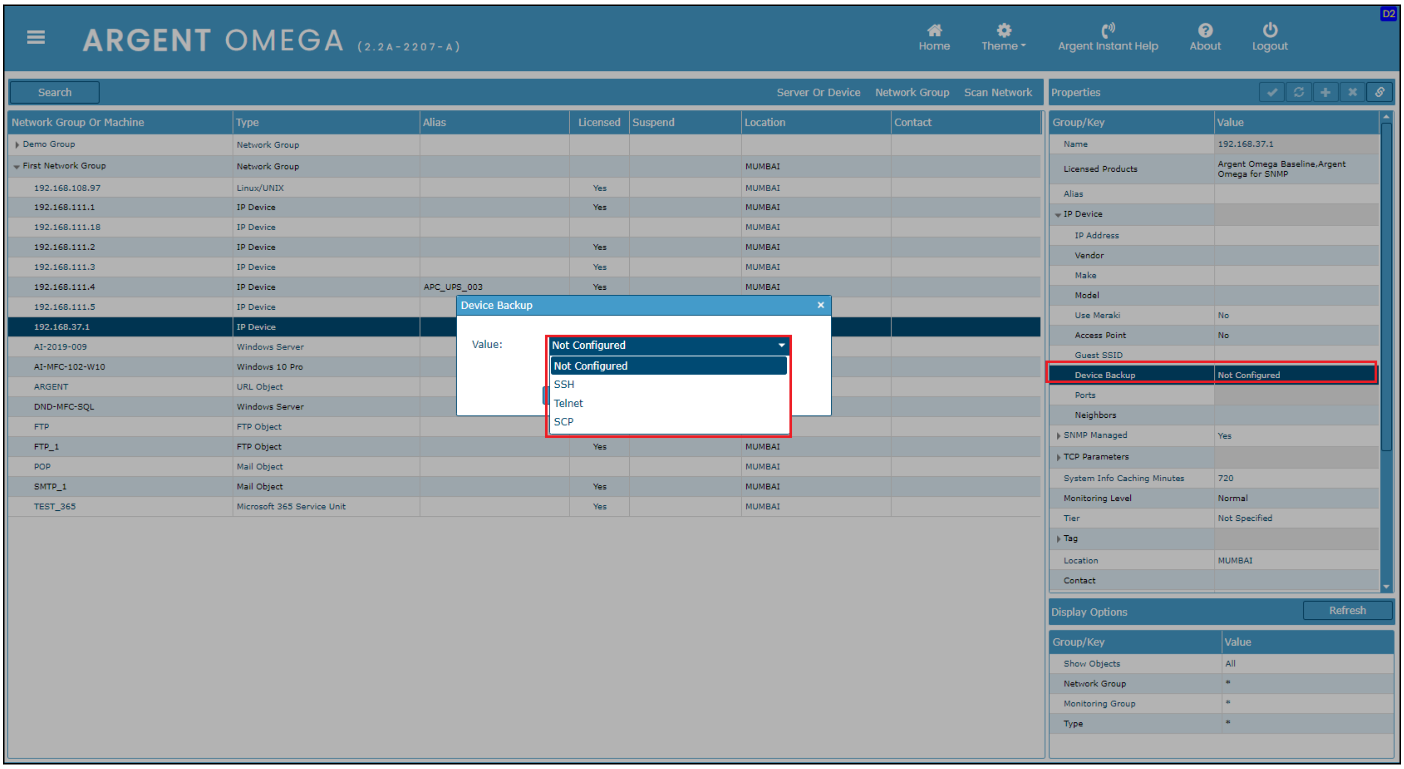
Device Configuration Rules

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

This facility uses the same mechanism to backup 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 CMDB-X section.



Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device					
192.168.37.1	IP Device					
AI-2019-009	Windows Server					
AI-MFC-102-W10	Windows 10 Pro					
ARGENT	URL Object					
DND-MFC-SQL	Windows Server					
FTP	FTP Object					
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	

Device Backup

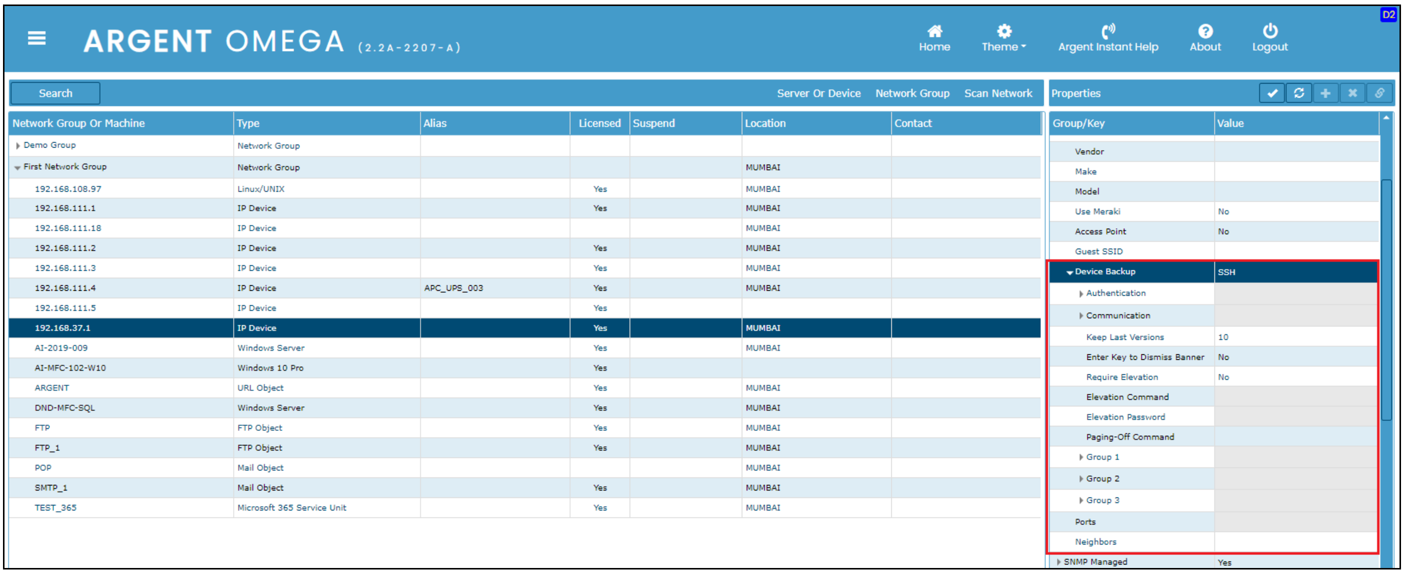
Value: Not Configured

- Not Configured
- SSH
- Telnet
- SCP

Group/Key	Value
Name	192.168.37.1
Licensed Products	Argent Omega Baseline,Argent Omega for SNMP
Alias	
IP Device	
IP Address	
Vendor	
Make	
Model	
Use Meraki	No
Access Point	No
Guest SSID	
Device Backup	Not Configured
Ports	
Neighbors	
SNMP Managed	Yes
TCP Parameters	
System Info Caching Minutes	720
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

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



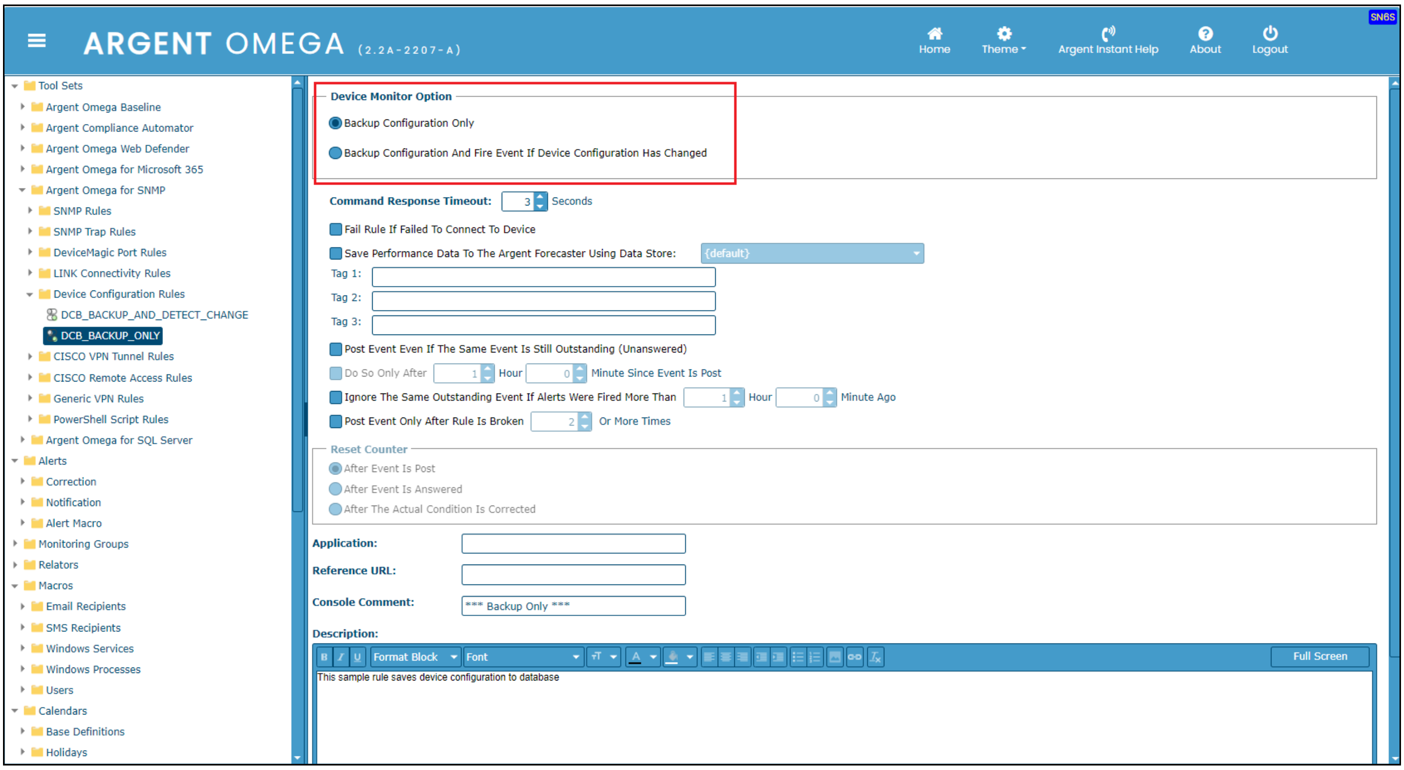
Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	

Group/Key	Value
Vendor	
Make	
Model	
Use Meraki	No
Access Point	No
Guest SSID	
Device Backup	SSH
Authentication	
Communication	
Keep Last Versions	10
Enter Key to Dismiss Banner	No
Require Elevation	No
Elevation Command	
Elevation Password	
Paging-Off Command	
Group 1	
Group 2	
Group 3	
Ports	
Neighbors	
SNMP Managed	Yes

For more details about device backup configuration, please refer to Argent KBI

https://help.argent.com/#KBI_311638

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



Device Monitor Option

● Backup Configuration Only

○ Backup Configuration And Fire Event If Device Configuration Has Changed

Command Response Timeout: 3 Seconds

□ Fail Rule If Failed To Connect To Device

□ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

Application:

Reference URL:

Console Comment: *** Backup Only ***

Description:

This sample rule saves device configuration to database

Choose **Backup Configuration Only** option to backup 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 VPN alone does not guarantee smooth IT operations. You constantly need to monitor VPN connections (VPN Tunnel Monitoring) for possible bandwidth constraints and security threats. Customers can see the full picture of VPN activities including:

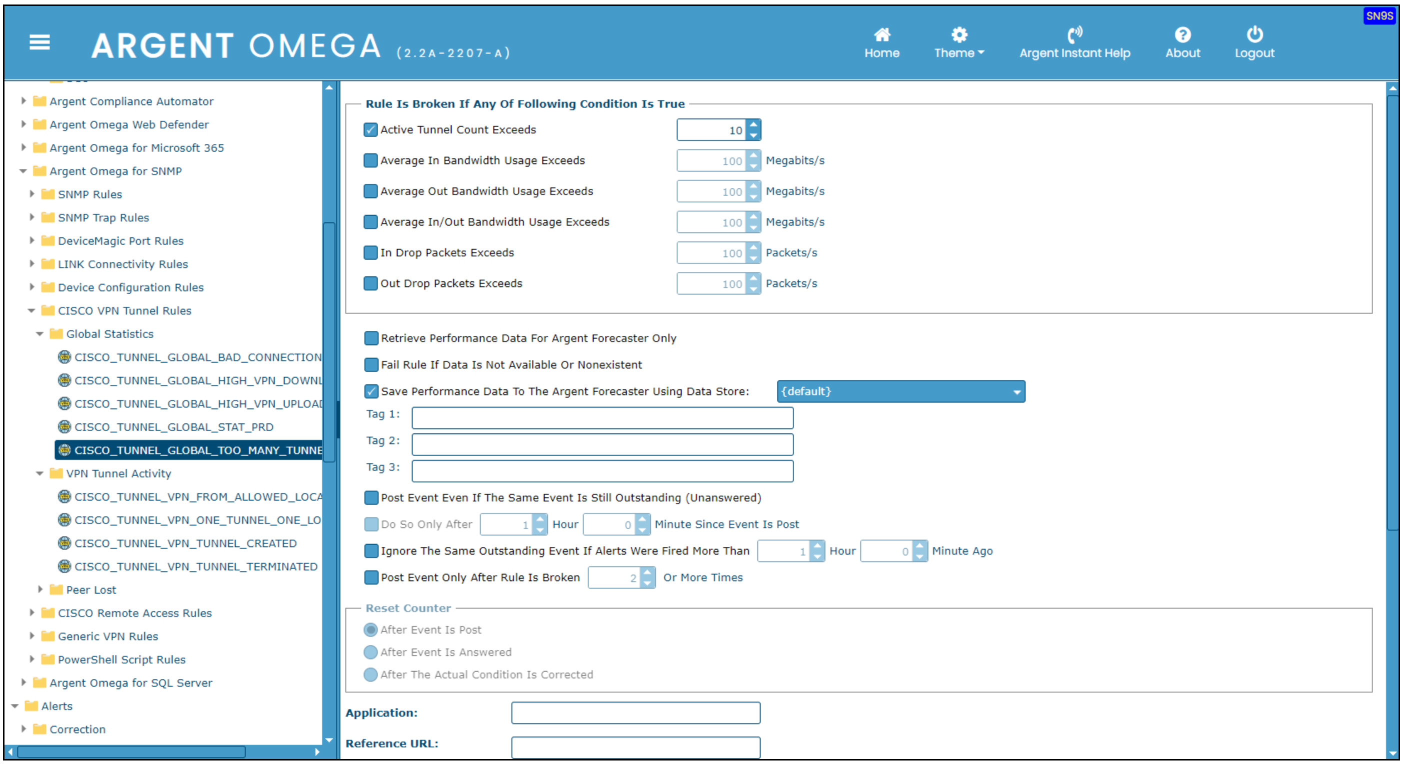
- Who - logon user
- Where - remote IP and geolocation of city, region, and country
- When - start time, end time, and duration of the VPN session
- What - protocol, in/out total bytes, and calculated bandwidth usage

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

Global Statistics Rules

Configure Global Statistics Rules to monitor following parameters

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


ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant Help
About
Logout
SN9S
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
SNMP Rules
SNMP Trap Rules
DeviceMagic Port Rules
LINK Connectivity Rules
Device Configuration Rules
CISCO VPN Tunnel Rules
Global Statistics
CISCO_TUNNEL_GLOBAL_BAD_CONNECTION
CISCO_TUNNEL_GLOBAL_HIGH_VPN_DOWNL
CISCO_TUNNEL_GLOBAL_HIGH_VPN_UPLOAD
CISCO_TUNNEL_GLOBAL_STAT_PRD
CISCO_TUNNEL_GLOBAL_TOO_MANY_TUNNE
VPN Tunnel Activity
CISCO_TUNNEL_VPN_FROM_ALLOWED_LOCA
CISCO_TUNNEL_VPN_ONE_TUNNEL_ONE_LO
CISCO_TUNNEL_VPN_TUNNEL_CREATED
CISCO_TUNNEL_VPN_TUNNEL_TERMINATED
Peer Lost
CISCO Remote Access Rules
Generic VPN Rules
PowerShell Script Rules
Argent Omega for SQL Server
Alerts
Correction

Rule Is Broken If Any Of Following Condition Is True

☑ Active Tunnel Count Exceeds 10

□ Average In Bandwidth Usage Exceeds 100 Megabits/s

□ Average Out Bandwidth Usage Exceeds 100 Megabits/s

□ Average In/Out Bandwidth Usage Exceeds 100 Megabits/s

□ In Drop Packets Exceeds 100 Packets/s

□ Out Drop Packets Exceeds 100 Packets/s

□ Retrieve Performance Data For Argent Forecaster Only

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

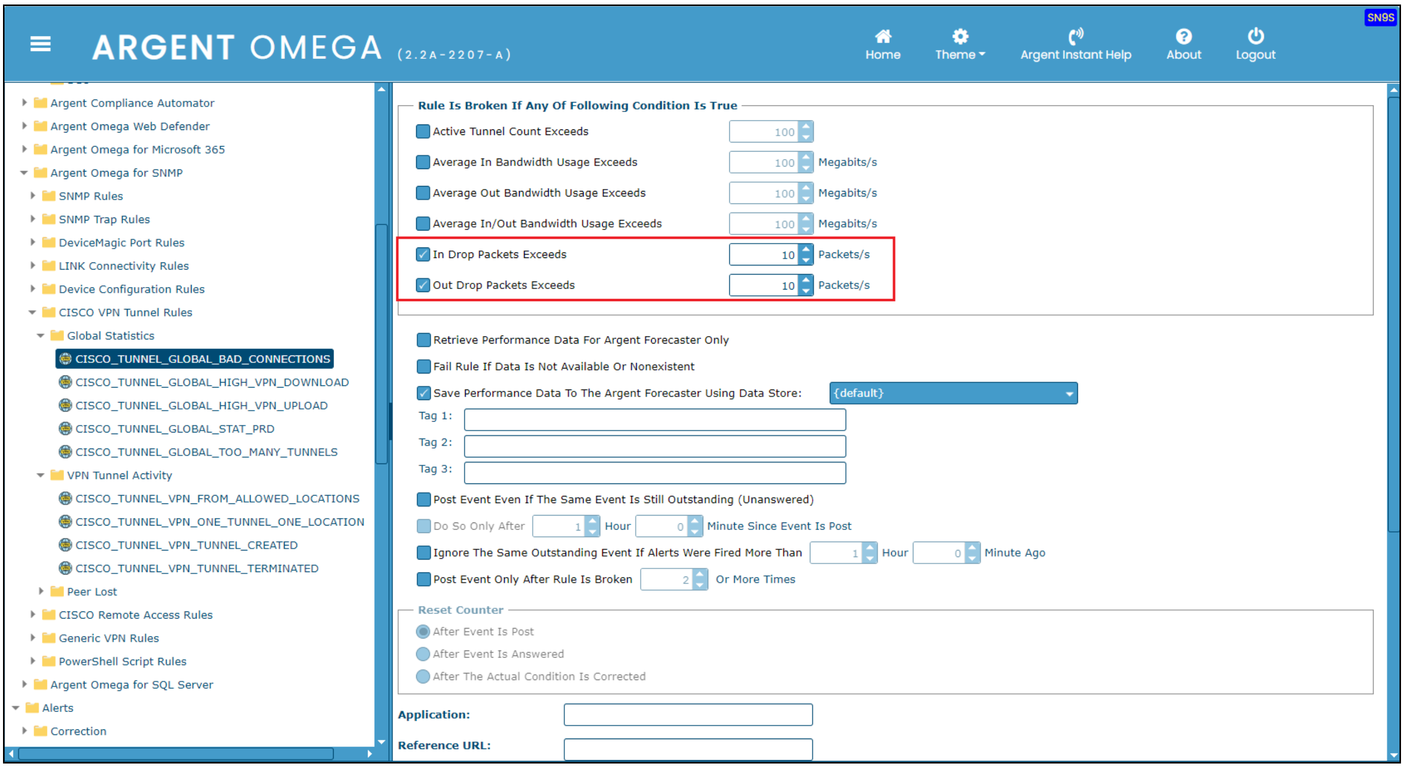
Application:

Reference URL:

Check **Active Tunnel Count Exceeds** option to alert if Site-to-Site VPN tunnel count exceeds threshold. Need to specify the threshold as well.

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.



ARGENT OMEGA (2.2A-2207-A)
SN9S
Home
Theme
Argent Instant Help
About
Logout
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
SNMP Rules
SNMP Trap Rules
DeviceMagic Port Rules
LINK Connectivity Rules
Device Configuration Rules
CISCO VPN Tunnel Rules
Global Statistics
CISCO_TUNNEL_GLOBAL_BAD_CONNECTIONS
CISCO_TUNNEL_GLOBAL_HIGH_VPN_DOWNLOAD
CISCO_TUNNEL_GLOBAL_HIGH_VPN_UPLOAD
CISCO_TUNNEL_GLOBAL_STAT_PRD
CISCO_TUNNEL_GLOBAL_TOO_MANY_TUNNELS
VPN Tunnel Activity
CISCO_TUNNEL_VPN_FROM_ALLOWED_LOCATIONS
CISCO_TUNNEL_VPN_ONE_TUNNEL_ONE_LOCATION
CISCO_TUNNEL_VPN_TUNNEL_CREATED
CISCO_TUNNEL_VPN_TUNNEL_TERMINATED
Peer Lost
CISCO Remote Access Rules
Generic VPN Rules
PowerShell Script Rules
Argent Omega for SQL Server
Alerts
Correction

Rule Is Broken If Any Of Following Condition Is True

☐ Active Tunnel Count Exceeds 100
☐ Average In Bandwidth Usage Exceeds 100 Megabits/s
☐ Average Out Bandwidth Usage Exceeds 100 Megabits/s
☐ Average In/Out Bandwidth Usage Exceeds 100 Megabits/s
☑ In Drop Packets Exceeds 10 Packets/s
☑ Out Drop Packets Exceeds 10 Packets/s

☐ Retrieve Performance Data For Argent Forecaster Only
☐ Fail Rule If Data Is Not Available Or Nonexistent
☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}
Tag 1:
Tag 2:
Tag 3:
☐ Post Event Even If The Same Event Is Still Outstanding (Unanswered)
☐ Do So Only After 1 Hour 0 Minute Since Event Is Post
☐ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
☐ Post Event Only After Rule Is Broken 2 Or More Times

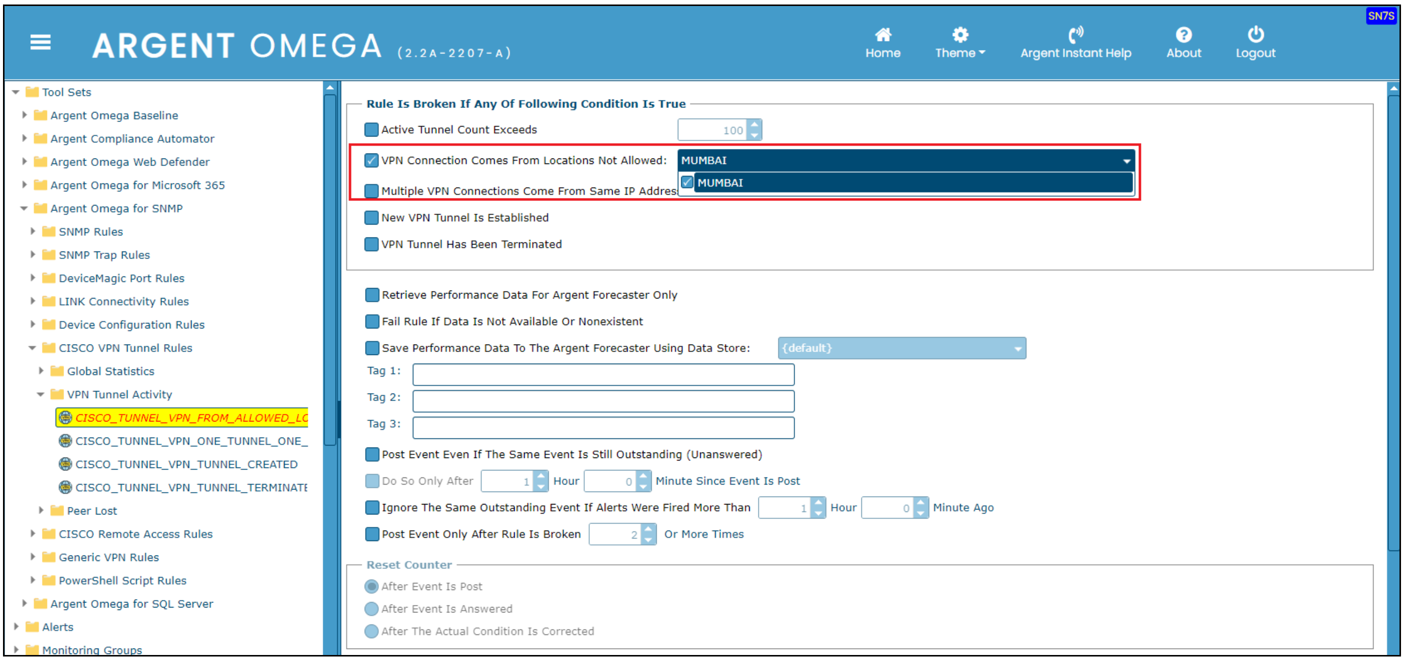
Reset Counter
● After Event Is Post
○ After Event Is Answered
○ After The Actual Condition Is Corrected

Application:
Reference URL:

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



ARGENT OMEGA (2.2A-2207-A)
SN7S
Home
Theme
Argent Instant Help
About
Logout
Tool Sets
Argent Omega Baseline
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
SNMP Rules
SNMP Trap Rules
DeviceMagic Port Rules
LINK Connectivity Rules
Device Configuration Rules
CISCO VPN Tunnel Rules
Global Statistics
VPN Tunnel Activity
CISCO_TUNNEL_VPN_FROM_ALLOWED_LC
CISCO_TUNNEL_VPN_ONE_TUNNEL_ONE_
CISCO_TUNNEL_VPN_TUNNEL_CREATED
CISCO_TUNNEL_VPN_TUNNEL_TERMINATE
Peer Lost
CISCO Remote Access Rules
Generic VPN Rules
PowerShell Script Rules
Argent Omega for SQL Server
Alerts
Monitoring Groups

Rule Is Broken If Any Of Following Condition Is True

☐ Active Tunnel Count Exceeds 100
☑ VPN Connection Comes From Locations Not Allowed: MUMBAI
☑ MUMBAI
☐ Multiple VPN Connections Come From Same IP Addres
☐ New VPN Tunnel Is Established
☐ VPN Tunnel Has Been Terminated

☐ Retrieve Performance Data For Argent Forecaster Only
☐ Fail Rule If Data Is Not Available Or Nonexistent
☐ Save Performance Data To The Argent Forecaster Using Data Store: {default}
Tag 1:
Tag 2:
Tag 3:
☐ Post Event Even If The Same Event Is Still Outstanding (Unanswered)
☐ Do So Only After 1 Hour 0 Minute Since Event Is Post
☐ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
☐ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter
● After Event Is Post
○ After Event Is Answered
○ After The Actual Condition Is Corrected

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

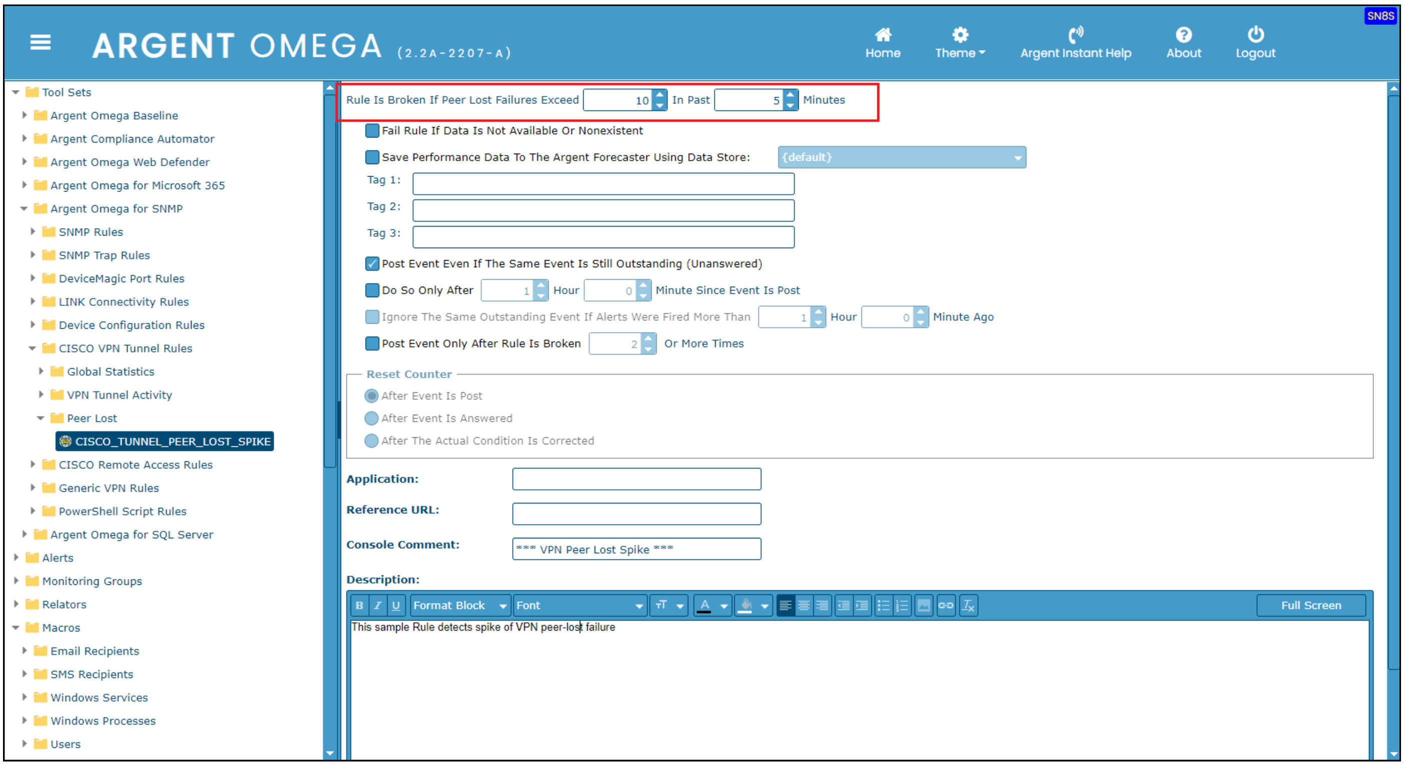
Check **Multiple VPN Connections Come From Same IP Address** option to alert if multiple VPN tunnels come from the same IP address.

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.



Rule Is Broken If Peer Lost Failures Exceed 10 In Past 5 Minutes

□ Fail Rule If Data Is Not Available Or Nonexistent

□ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

☑ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

Application:

Reference URL:

Console Comment: *** VPN Peer Lost Spike ***

Description:

This sample Rule detects spike of VPN peer-lost failure

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

CISCO Remote Access Rules

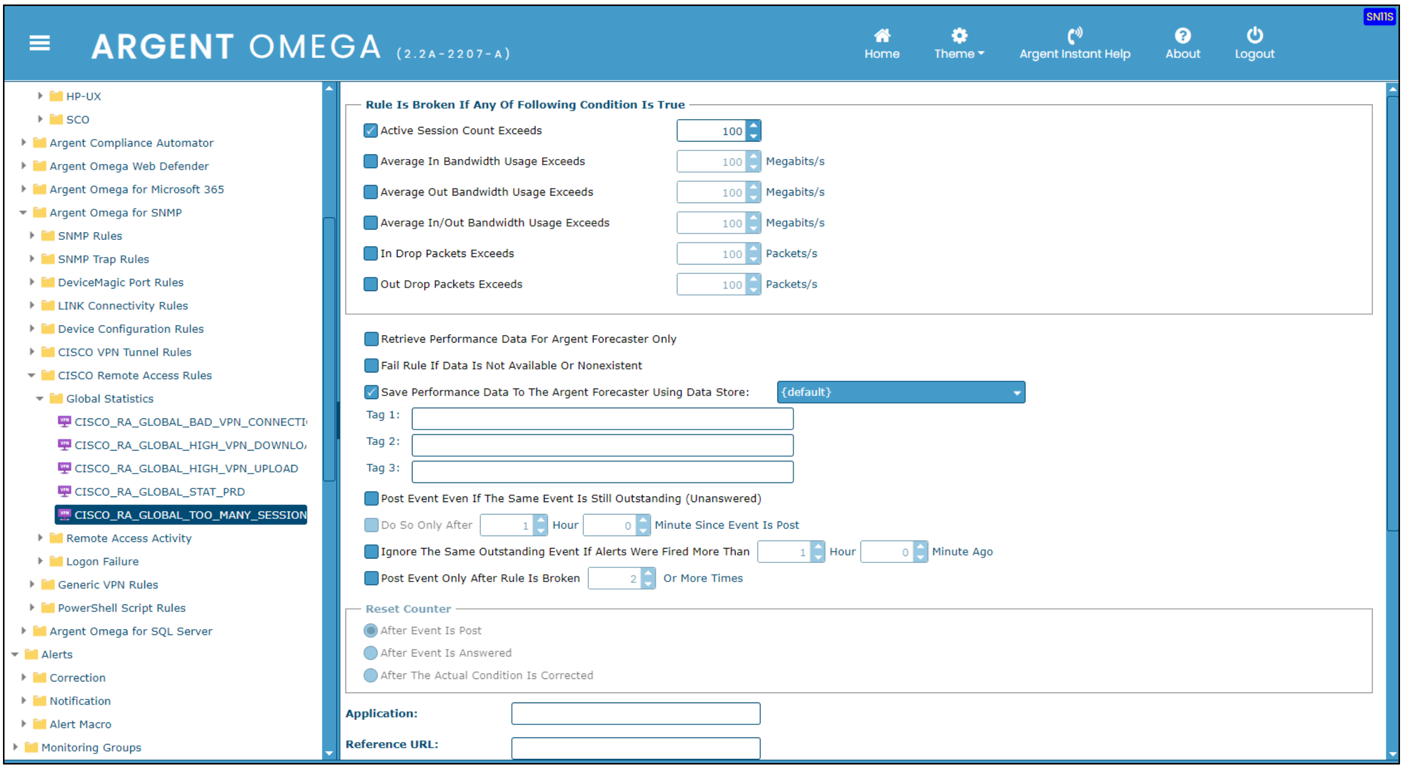
CISCO Remote Access enables you to keep track of all users who connect remotely to your organization's network, which is an important aspect of monitoring logins, logoffs, user's bandwidth usage, user's session duration, etc.

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 drop too many packets



Rule Is Broken If Any Of Following Condition Is True

☑ Active Session Count Exceeds 100

□ Average In Bandwidth Usage Exceeds 100 Megabits/s

□ Average Out Bandwidth Usage Exceeds 100 Megabits/s

□ Average In/Out Bandwidth Usage Exceeds 100 Megabits/s

□ In Drop Packets Exceeds 100 Packets/s

□ Out Drop Packets Exceeds 100 Packets/s

□ Retrieve Performance Data For Argent Forecaster Only

□ Fail Rule If Data Is Not Available Or Nonexistent

☑ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

Application:

Reference URL:

Check **Active Session Count Exceeds** option to alert if Site remote access VPN session count exceeds threshold. Need to specify the threshold as well.

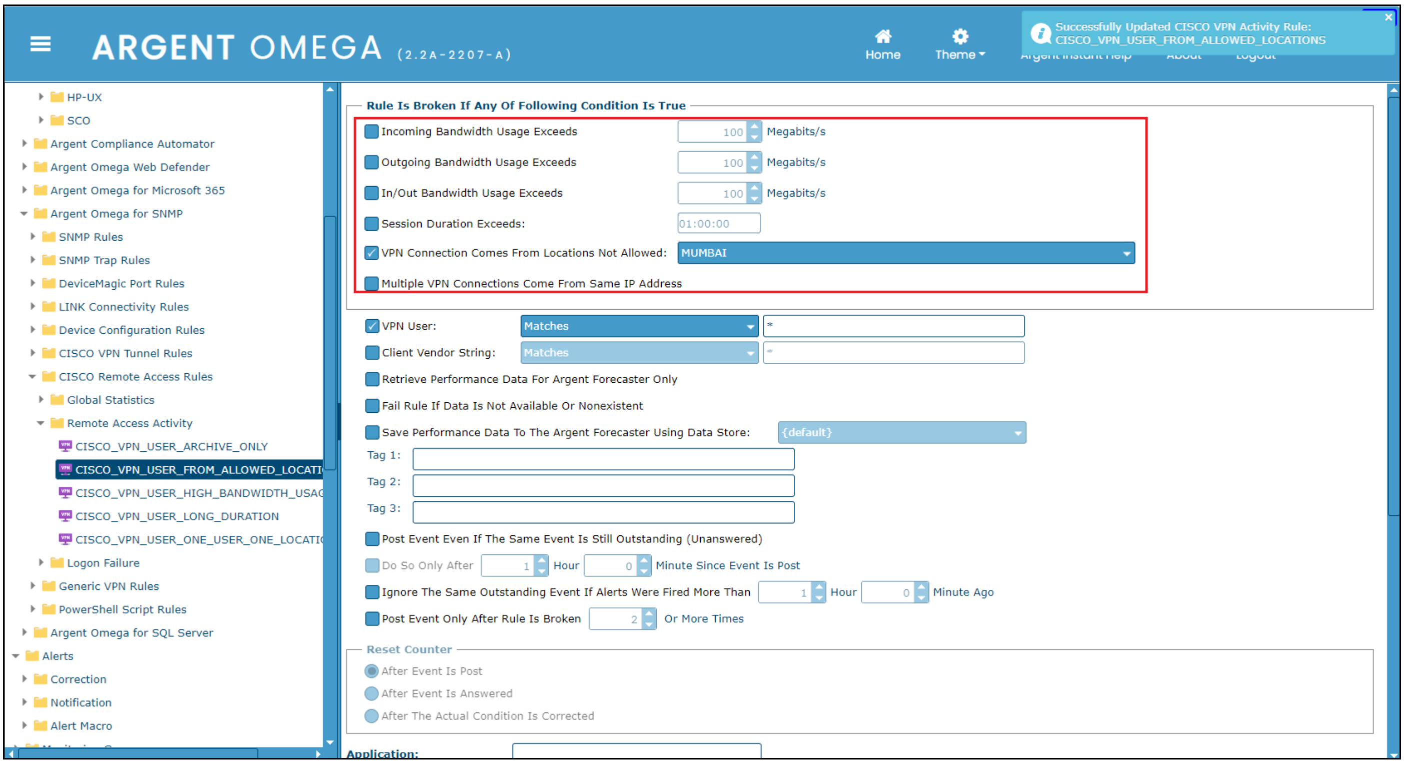
Use options **Average In Bandwidth Usage Exceeds**, **Average Out Bandwidth Usage Exceeds** and **Average In/Out Bandwidth Usage Exceeds** to monitor the bandwidth consumptions.

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


ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant Help
About
Logout
HP-UX
SCO
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
SNMP Rules
SNMP Trap Rules
DeviceMagic Port Rules
LINK Connectivity Rules
Device Configuration Rules
CISCO VPN Tunnel Rules
CISCO Remote Access Rules
Global Statistics
Remote Access Activity
CISCO_VPN_USER_ARCHIVE_ONLY
CISCO_VPN_USER_FROM_ALLOWED_LOCATI
CISCO_VPN_USER_HIGH_BANDWIDTH_USAG
CISCO_VPN_USER_LONG_DURATION
CISCO_VPN_USER_ONE_USER_ONE_LOCATI
Logon Failure
Generic VPN Rules
PowerShell Script Rules
Argent Omega for SQL Server
Alerts
Correction
Notification
Alert Macro

Successfully Updated CISCO VPN Activity Rule: CISCO_VPN_USER_FROM_ALLOWED_LOCATIONS

Rule Is Broken If Any Of Following Condition Is True

☐ Incoming Bandwidth Usage Exceeds 100 Megabits/s
☐ Outgoing Bandwidth Usage Exceeds 100 Megabits/s
☐ In/Out Bandwidth Usage Exceeds 100 Megabits/s
☐ Session Duration Exceeds: 01:00:00
☑ VPN Connection Comes From Locations Not Allowed: MUMBAI
☐ Multiple VPN Connections Come From Same IP Address

☑ VPN User: Matches *
☐ Client Vendor String: Matches *
☐ Retrieve Performance Data For Argent Forecaster Only
☐ Fail Rule If Data Is Not Available Or Nonexistent
☐ Save Performance Data To The Argent Forecaster Using Data Store: {default}
Tag 1:
Tag 2:
Tag 3:
☐ Post Event Even If The Same Event Is Still Outstanding (Unanswered)
☐ Do So Only After 1 Hour 0 Minute Since Event Is Post
☐ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
☐ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post
○ After Event Is Answered
○ After The Actual Condition Is Corrected

Application:

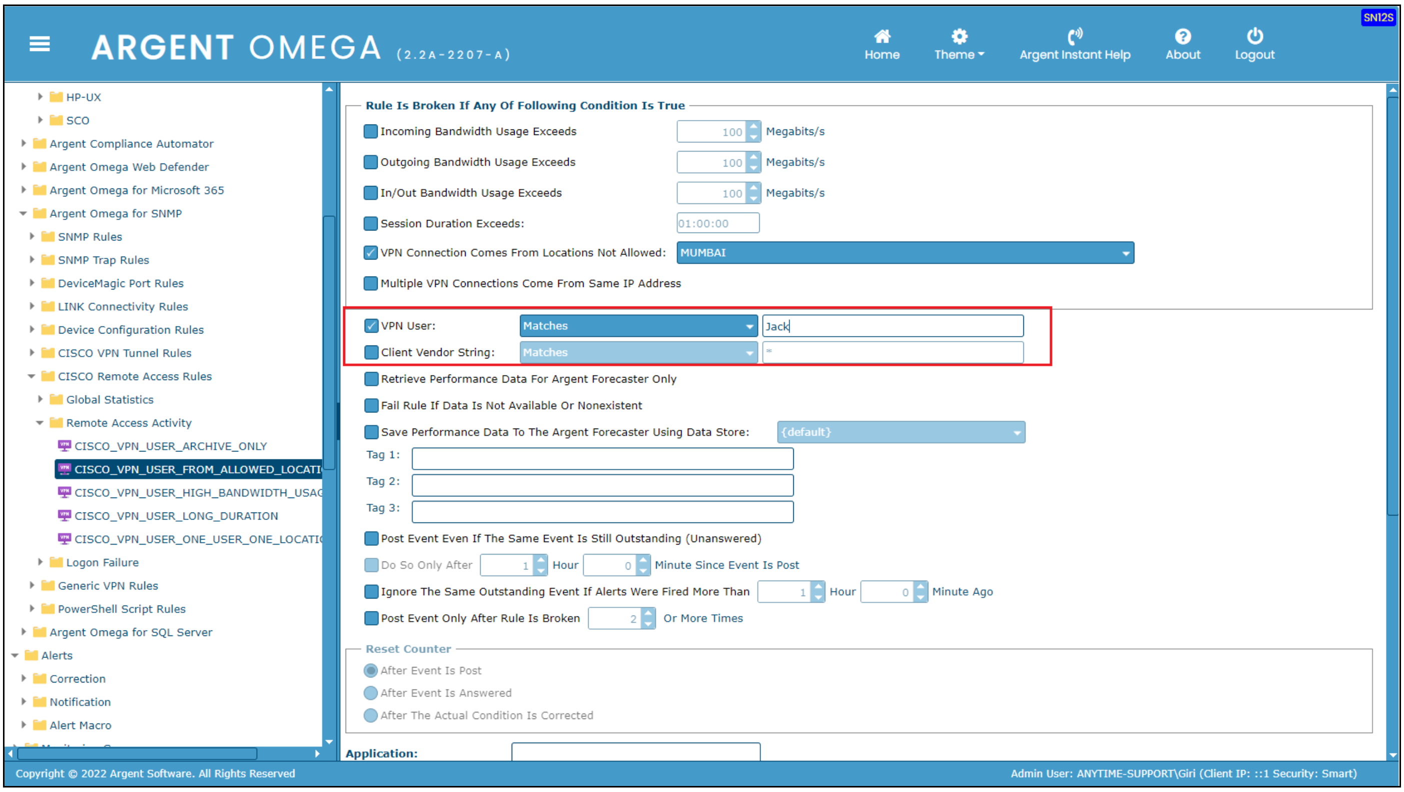
Use options **Incoming Bandwidth Usage Exceeds**, **Outgoing Bandwidth Usage Exceeds** and **In/Out Bandwidth Usage Exceeds** to monitor the extreme bandwidth usage.

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 combo box.

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

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


SN12S
ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant Help
About
Logout
HP-UX
SCO
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
SNMP Rules
SNMP Trap Rules
DeviceMagic Port Rules
LINK Connectivity Rules
Device Configuration Rules
CISCO VPN Tunnel Rules
CISCO Remote Access Rules
Global Statistics
Remote Access Activity
CISCO_VPN_USER_ARCHIVE_ONLY
CISCO_VPN_USER_FROM_ALLOWED_LOCATI
CISCO_VPN_USER_HIGH_BANDWIDTH_USAG
CISCO_VPN_USER_LONG_DURATION
CISCO_VPN_USER_ONE_USER_ONE_LOCATI
Logon Failure
Generic VPN Rules
PowerShell Script Rules
Argent Omega for SQL Server
Alerts
Correction
Notification
Alert Macro

Rule Is Broken If Any Of Following Condition Is True

□ Incoming Bandwidth Usage Exceeds 100 Megabits/s
□ Outgoing Bandwidth Usage Exceeds 100 Megabits/s
□ In/Out Bandwidth Usage Exceeds 100 Megabits/s
□ Session Duration Exceeds: 01:00:00
☑ VPN Connection Comes From Locations Not Allowed: MUMBAI
□ Multiple VPN Connections Come From Same IP Address
☑ VPN User: Matches Jack
□ Client Vendor String: Matches *
□ Retrieve Performance Data For Argent Forecaster Only
□ Fail Rule If Data Is Not Available Or Nonexistent
□ Save Performance Data To The Argent Forecaster Using Data Store: {default}
Tag 1:
Tag 2:
Tag 3:
□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)
□ Do So Only After 1 Hour 0 Minute Since Event Is Post
□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
□ Post Event Only After Rule Is Broken 2 Or More Times

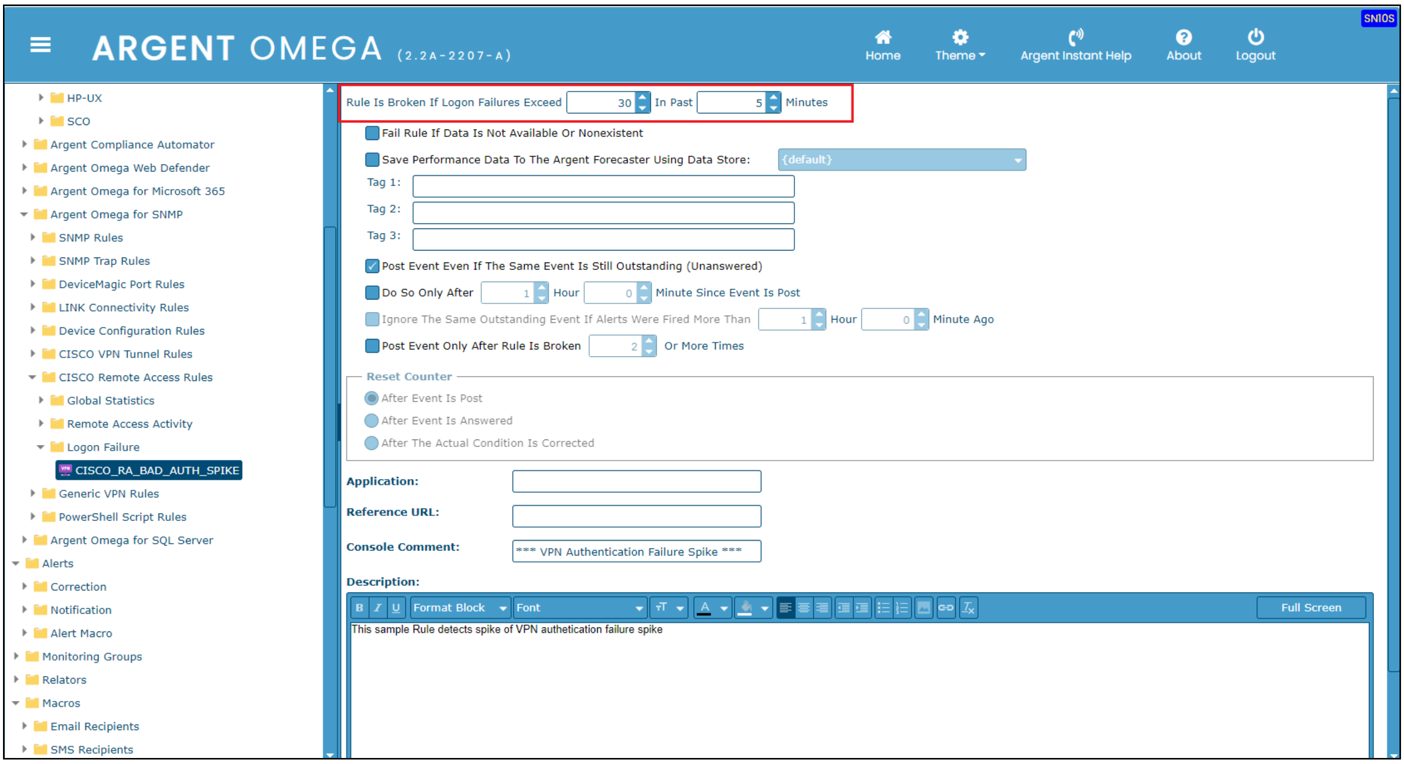
Reset Counter
● After Event Is Post
○ After Event Is Answered
○ After The Actual Condition Is Corrected

Application:

Copyright © 2022 Argent Software. All Rights Reserved
Admin User: ANYTIME-SUPPORT\Giri (Client IP: ::1 Security: Smart)

Logon Failure Rules

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



Rule Is Broken If Logon Failures Exceed 30 In Past 5 Minutes
□ Fail Rule If Data Is Not Available Or Nonexistent
□ Save Performance Data To The Argent Forecaster Using Data Store: {default}
Tag 1:
Tag 2:
Tag 3:
☑ Post Event Even If The Same Event Is Still Outstanding (Unanswered)
□ Do So Only After 1 Hour 0 Minute Since Event Is Post
□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter
● After Event Is Post
○ After Event Is Answered
○ After The Actual Condition Is Corrected

Application:
Reference URL:
Console Comment: *** VPN Authentication Failure Spike ***
Description:
This sample Rule detects spike of VPN authetication failure spike

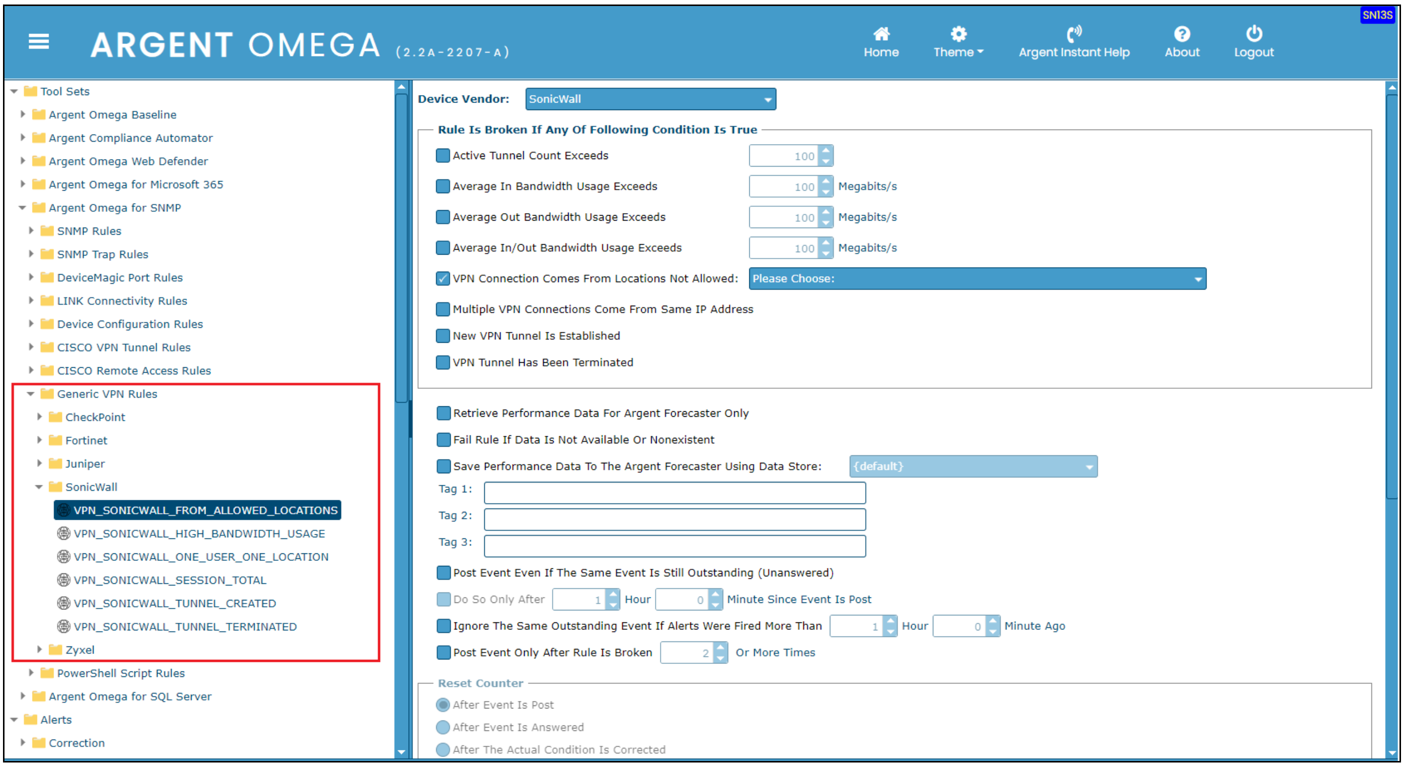
Generic VPN Rules

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 or out bandwidth usage. More importantly, it provides unique security features for real-time alerts for potential hacking, including:

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


SNI3S
ARGENT OMEGA (2.2A-2207-A)
Home
Theme
Argent Instant Help
About
Logout
Tool Sets
Argent Omega Baseline
Argent Compliance Automator
Argent Omega Web Defender
Argent Omega for Microsoft 365
Argent Omega for SNMP
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
CheckPoint
Fortinet
Juniper
SonicWall
VPN_SONICWALL_FROM_ALLOWED_LOCATIONS
VPN_SONICWALL_HIGH_BANDWIDTH_USAGE
VPN_SONICWALL_ONE_USER_ONE_LOCATION
VPN_SONICWALL_SESSION_TOTAL
VPN_SONICWALL_TUNNEL_CREATED
VPN_SONICWALL_TUNNEL_TERMINATED
Zyxel
PowerShell Script Rules
Argent Omega for SQL Server
Alerts
Correction

Device Vendor: SonicWall

Rule Is Broken If Any Of Following Condition Is True

□ Active Tunnel Count Exceeds 100

□ Average In Bandwidth Usage Exceeds 100 Megabits/s

□ Average Out Bandwidth Usage Exceeds 100 Megabits/s

□ Average In/Out Bandwidth Usage Exceeds 100 Megabits/s

☑ VPN Connection Comes From Locations Not Allowed: Please Choose:

□ Multiple VPN Connections Come From Same IP Address

□ New VPN Tunnel Is Established

□ VPN Tunnel Has Been Terminated

□ Retrieve Performance Data For Argent Forecaster Only

□ Fail Rule If Data Is Not Available Or Nonexistent

□ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

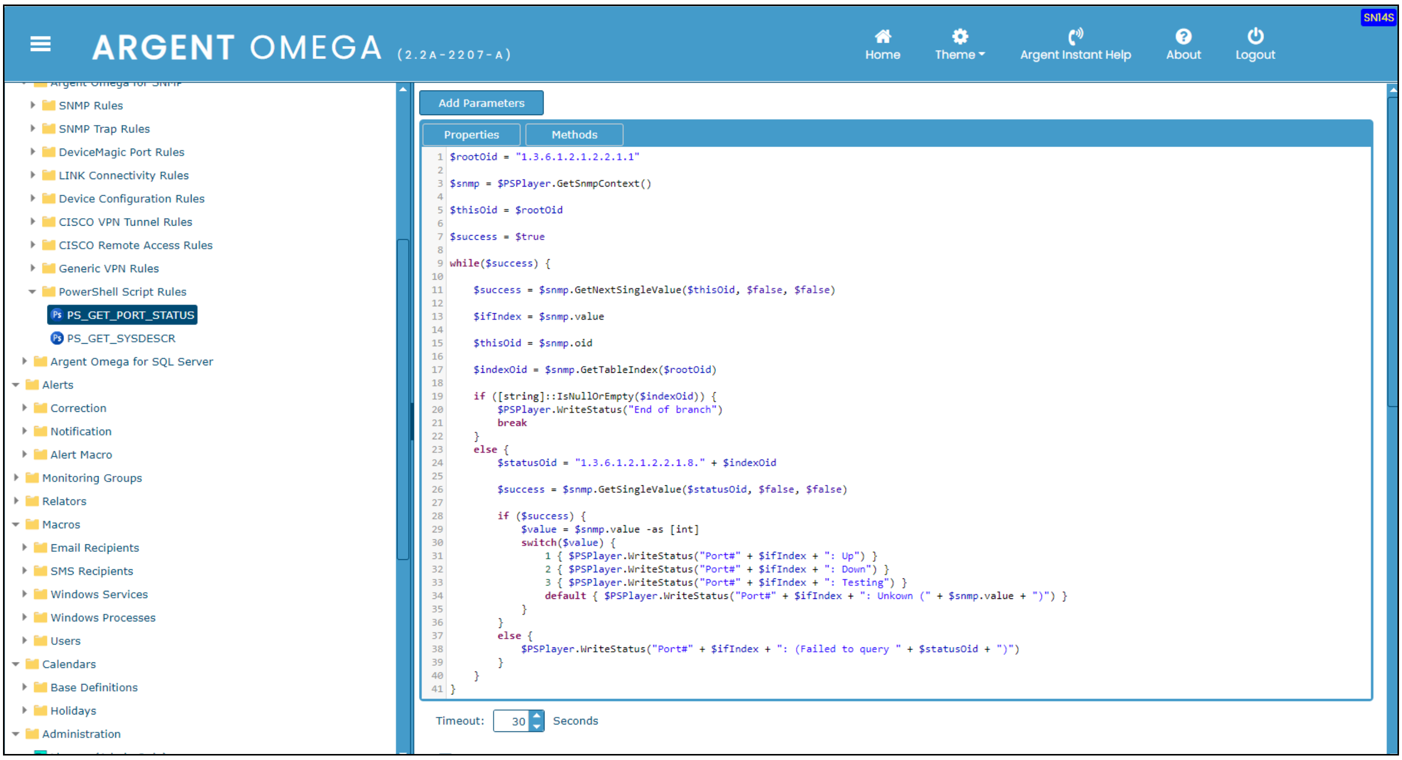
○ After Event Is Answered

○ After The Actual Condition Is Corrected

PowerShell Script Rules

This Rule allows you to create custom PowerShell scripts to monitor SNMP enabled devices. There are two built in Rules that demonstrate this function:

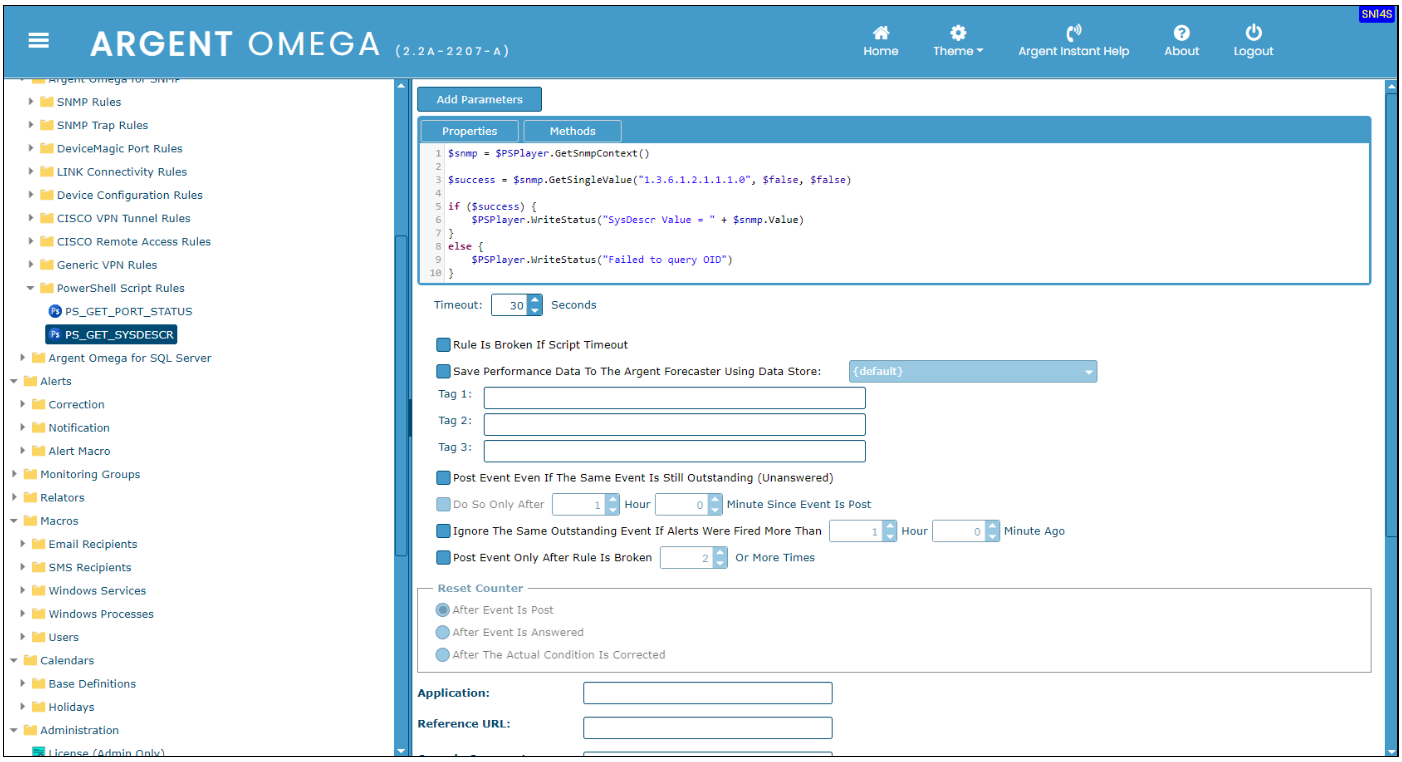
- How to enumerate SNMP OID table using PowerShell Script



```
$rootOid = "1.3.6.1.2.1.2.2.1.1"

$snmp = $PSPlayer.GetSnmpContext()

$thisOid = $rootOid

$success = $true

while($success) {

    $success = $snmp.GetNextSingleValue($thisOid, $false, $false)

    $ifIndex = $snmp.value

    $thisOid = $snmp.oid

    $indexOid = $snmp.GetTableIndex($rootOid)

    if ([string]::IsNullOrEmpty($indexOid)) {
        $PSPlayer.WriteStatus("End of branch")
        break
    }
    else {
        $statusOid = "1.3.6.1.2.1.2.2.1.8." + $indexOid

        $success = $snmp.GetSingleValue($statusOid, $false, $false)

        if ($success) {
            $value = $snmp.value -as [int]
            switch($value) {
                1 { $PSPlayer.WriteStatus("Port#" + $ifIndex + ": Up") }
                2 { $PSPlayer.WriteStatus("Port#" + $ifIndex + ": Down") }
                3 { $PSPlayer.WriteStatus("Port#" + $ifIndex + ": Testing") }
                default { $PSPlayer.WriteStatus("Port#" + $ifIndex + ": Unkown (" + $snmp.value + ")") }
            }
        }
        else {
            $PSPlayer.WriteStatus("Port#" + $ifIndex + ": (Failed to query " + $statusOid + ")")
        }
    }
}
```

Timeout: 30 Seconds

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



```
$snmp = $PSPlayer.GetSnmpContext()

$success = $snmp.GetSingleValue("1.3.6.1.2.1.1.1.0", $false, $false)

if ($success) {
    $PSPlayer.WriteStatus("SysDescr Value = " + $snmp.Value)
}
else {
    $PSPlayer.WriteStatus("Failed to query OID")
}
```

Timeout: 30 Seconds

□ Rule Is Broken If Script Timeout

□ Save Performance Data To The Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

□ Post Event Even If The Same Event Is Still Outstanding (Unanswered)

□ Do So Only After 1 Hour 0 Minute Since Event Is Post

□ Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago

□ Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

● After Event Is Post

○ After Event Is Answered

○ After The Actual Condition Is Corrected

Application:

Reference URL: