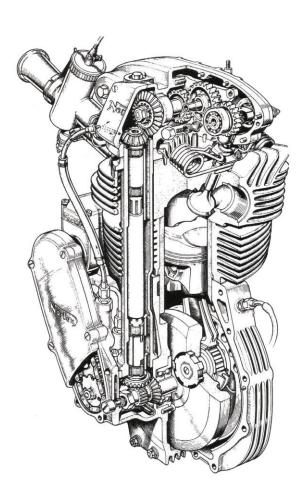
Argent for SNMP



www.Argent.com

Table Of Contents

Introduction	3
Log-On Screen	4
Home Screen	5
CMDB-X	6
Display Wireless Clients For Meraki Access Point (AP)	16
Agent Omega for SNMP Tool Sets	19
SNMP Rules	20
SNMP Trap Rules	28
DeviceMagic Port Rules	31
LINK Connectivity Rules	35
Device Configuration Rules	36
CISCO VPN Tunnel Rules	38
CISCO Remote Access Rules	41
Generic VPN Rules	44
PowerShell Script Rules	45

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.

■ ARGENT OME	GA (2.2A-2207-A)	₩ 후 (한 중 신 Home Theme ▼ Argent Instant Help About Logout	62
▶ 🚰 Tool Sets	Send Internal Events To Email Address:	testargent10@gmail.com	^
Alerts	Shared Task Executor Process Pool Size:		
Monitoring Groups	Max Days To Automatically Resolve Events:		
Relators			
Macros	Keep Task Execution Info For Days:	Truncate Task Execution History Daily	
▼ Mathematical Calendars	Prevent Firing The Same Internal Event Within Interval:	60 🗘 Minutes	
Base Definitions	Delay Firing Internal Event:	60 Seconds	
🕨 🚧 Holidays	Max Allowed Lapse For Active Generator:	5 Minutes	
 Administration 	Auto Logoff:	15 Minutes	
Ticense (Admin Only)	Meraki API Key:		
▼ Generator Settings	· · · ·		
Ø ^o Argent Omega	Default Location:	MUMBAI	
o° Argent Alert Mechanism	Default Contact:	Please Choose:	
• o ^o Argent Forecaster	Administrative Protection Password:	•••••	
oº Argent SIEM-Complete	Take Automatic Backup		L
Security	Time:	00:00:00 It Is Recommended To Do Backup At Midnight	
Network Scan	Calendar:	Please Choose:	
Event Logs			
SuperMaps	Recycle Service		

Log-On Screen

		۲
Argent has been in the systems management business since	Argent Omega	
1991 and has over 2,000 customers worldwide.	Pre-Production Version	
Argent is the Industry Leader in		
Monitoring and Automation Products.		
Read More	User Name Enter name	
	Password	
	Log In	
ARGENT	2.2A-2204-T1 (Build Version: v2.2.2205.31)	
Copyrig	ght © 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.

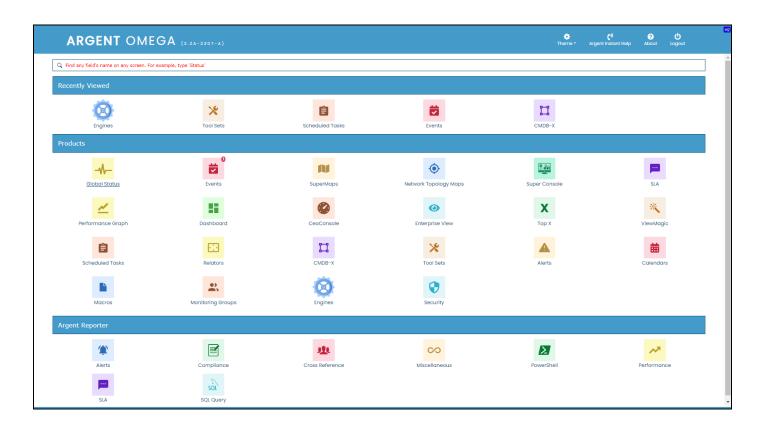
Local Windows user authentication is used instead if the Argent server is standalone or in a Workgroup. With Windows user accounts, the best approach is to create a separate user group for Windows users and assign the required rights.

Demo accounts can be created in the **Argent Omega Security** section and are used for demonstration purposes. Demo accounts are <u>read-only accounts</u> 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.

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 <u>Configuration Management DataBase</u>.

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** <u>single click</u>.

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:

ARGENT OME	GA (2.2A-2207-A)			🔅 Theme - Arge	() () ant Instant Help About Logout
Q Find any field's name on any screen. For	example, type 'Status'				
Recently Viewed					
0	*	Ê		11	
Engines	Tool Sets	Scheduled Tasks	Events	CMDB-X	
Products					
	ĕ		•		
<u>Global Status</u>	Events	SuperMaps	Network Topology Maps	Super Console	SLA
1	55	0	\odot	x	*
Performance Graph	Dashboard	CeoConsole	Enterprise View	Тор Х	ViewMagic
Ê		11	*		曲
Scheduled Tasks	Relators	CMDB-X	Tool Sets	Alerts	Calendars
	•	8			
Macros	Monitoring Groups	Engines	Security		
Argent Reporter					
*		224	00		12
Alerts	Compliance	Cross Reference	Miscellaneous	PowerShell	Performance
P	SQL				
SLA	SQL Query				

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

Search					Server Or Device	Network Group	Scan Network	Properties	✓ 2 + 3
etwork Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact		Group/Key	Value
Demo Group	Network Group	Alids	Licensed	Suspenu	Locadon	Contact		Name	First Network Group
First Network Group	Network Group				мимват			Туре	Network Group
-								Location	MUMBAI
192.168.108.97 192.168.111.1	Linux/UNIX IP Device		Yes		MUMBAI			Contact	
192.168.111.2	IP Device		Yes		MUMBAI			VMware Parameters	
192.168.111.3	IP Device		Yes		MUMBAI			XenServer Parameters	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI			SNMP Parameters	
192.168.111.5	IP Device	AFC_0F5_005	Yes		HUHUHI			Extended Properties	
192.168.37.1	IP Device		Yes		MUMBAI				
AI-2019-009	Windows Server		Yes		MUMBAI			Description	
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				

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:

work Group Or Machine emo Group				Server Or Devi	ice Network Group	Scan Network Properties	✓ S + ×
emo Group	Туре	Alias	Licensed Suspend	Location	Contact	Active Directory	Value
	Network Group					Network Browser	First Network Group
rst Network Group	Network Group			MUMBAI		ICMP Ping	Network Group
192.168.108.97	Linux/UNIX		Yes	MUMBAI		Discover SNMP Devices	MUMBAI
192.168.111.1	IP Device		Yes	MUMBAI		Windows Cluster	
192.168.111.2	IP Device		Yes	MUMBAI		VMware Infrastructure	
192.168.111.3	IP Device		Yes	MUMBAI		Meraki Devices	
192.168.111.4	IP Device	APC_UPS_003	Yes	MUMBAI		Import From Argent Topology Manager	
192.168.111.5	IP Device		Yes			Import External Excel File	
192.168.37.1	IP Device		Yes	MUMBAI		Description	_
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			

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

≡ ARGENT	OMEGA (2.2A-2	207-A)				A Home	🗱 Theme -	ে % বি Argent Instant Help Abc	
Search					Server Or Devi	ce Network Group	Scan Network	Properties	✓ S + × 8
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact		Group/Key	Value
) Demo Group	Network Group							Name	First Network Group
➡ First Network Group	Network Group	SNMP Managed Devices Sca	pping				D21 ×	Туре	Network Group
192.168.108.97	Linux/UNIX	Simp managed Devices Sca	unning					Location	MUMBAI
192.168.111.1	IP Device							Contact	
192.168.111.2	IP Device	SNMP Credentials:				+ /	· ×	VMware Parameters	
192.168.111.3	IP Device	Version	Comm		SNMP User	Auth. Protocol		XenServer Parameters	
192.168.111.4	IP Device	SNMPv1	public					SNMP Parameters	
192.168.111.5	IP Device							Extended Properties	
192.168.37.1	IP Device							Description	
AI-2019-009	Windows Server								
AI-MFC-102-W10	Windows 10 Pro								
ARGENT	URL Object	Network Segments:		uery Local Interface	Query Switch Int	erface 🕂 🖌	× ×		
DND-MFC-SQL	Windows Server								
FTP	FTP Object	Start IP Address		End IP Address		ırk Mask			
FTP_1	FTP Object	192.168.37.1			255.25	5.255.0			
POP	Mail Object								
SMTP_1	Mail Object								
TEST_365	Microsoft 365 Service Unit								
		SNMP Port: Timeout: Retry: Thread Limit:		161 C Seconds					
		Thread Link.		oll Directly Connected	l Neighbor Switches			Display Options	Refresh
				_		_		Group/Key	Value
			ОК		Cano	cel		Show Objects	All
								Network Group	*
								Monitoring Group	*
								Туре	*

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:

	OMEGA (2.2A-2	207-A)			Home Ther			About Logout	D2
Search				Server Or Device Netwo	ork Group Scan Ne	twork	Properties	× ;	3 + x Ø
Network Group Or Machine	Туре	Alias	Licensed Suspend	Location	Contact		Group/Key	Value	
▶ Demo Group	Network Group				Í.		Name	First Network Gro	up
	Network Group						Туре	Network Group	
192.168.108.97	Linux/UNIX	twork Scanning Result			D2D ×		Location	MUMBAI	
192.168.111.1	IP Device						Contact		
192.168.111.2	IP Device	Ignored Machine	Туре	Alias	Domain		VMware Parameters		
192.168.111.3	IP Device	192.168.111.4	IP Device	APC_UPS_003			XenServer Parameters		
192.168.111.4	IP Device						SNMP Parameters		
192.168.111.5	IP Device						Extended Properties		
192.168.37.1	IP Device						Description		
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								
					►.				
	s	ave to Network Group:	rst Network Group	-					
			Keep Original Network Group						
		-							
		Toggle	ОК	Cancel			Display Options		Refresh
							Group/Key	Value	
							Show Objects	All	
							Network Group	*	
							Monitoring Group	*	
							Туре	•	

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:

tetwork Group Or Machine Type b Demo Group Network Group First Network Group Network Group 192:166:108:97 Linco/UNIX 192:166:111:1 IP Device 192:166:111:2 IP Device	Alias	Licensed Suspen	d Location MUMBAI MUMBAI	Contact	Group/Key Name Type	Value First Network Group Network Group
First Helwork Group Helwork Group 192.168.308.97 Linux/UNIX 192.158.311.1 IP Device					Туре	
192.168.108.97 Linux/UNIX 192.168.111.1 IP Device						Network Group
192.168.111.1 IP Device			MUMBAI			
					Location	MUMBAI
192.168.111.2 IP Device		Yes	MUMBAI		Contact	
		Yes	MUMBAI		VMware Parameters	
192.168.111.3 IP Device		Yes	MUMBAI		XenServer Parameters	
192.168.111.4 IP Device	APC_UPS_003	Yes	MUMBAI		SNMP Parameters	
192.168.111.5 IP Device		Yes			Extended Properties	
192.168.37.1 IP Device		Yes	MUMBAI		Description	
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			

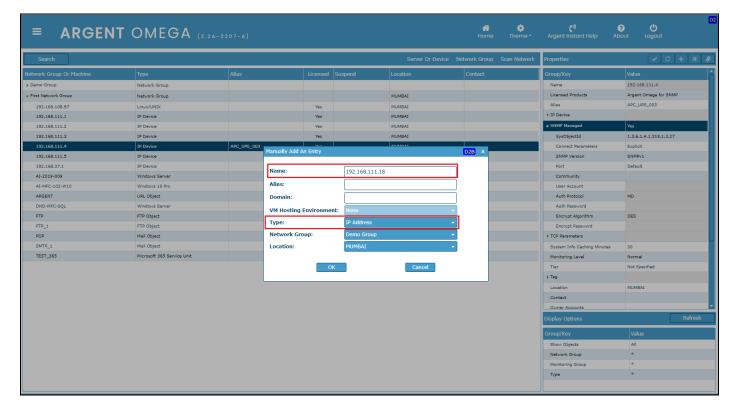
When adding the SNMP device, the CMDB-X property named **SNMP Managed** will automatically be set to **Yes** to show that the device is SNMP managed. The SysObjectId and device type are automatically retrieved. The SysObjectId contains the vendor's identification of an SNMP managed object type.

Search					Server Or Device Ne	etwork Group Scan Network	Properties	✓ 2 ÷ ×
etwork Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact	Group/Key	Value
Demo Group	Network Group						Name	192.168.111.4
First Network Group	Network Group				MUMBAI		Licensed Products	Argent Omega for SNMP
192.168.108.97	Linux/UNIX		Yes		MUMBAI		Alias	APC_UPS_003
192.168.111.1	IP Device		Yes		MUMBAI		▶ IP Device	
192.168.111.2	IP Device		Yes		MUMBAI			Yes
192.168.111.3	IP Device		Yes		MUMBAI		SysObjectId	1.3.6.1.4.1.318.1.3.27
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI		Connect Parameters	Explicit
192.168.111.5	IP Device		Yes				SNMP Version	SNMPv1
192.168.37.1	IP Device		Yes		MUMBAI		Port	Default
AI-2019-009	Windows Server		Yes		MUMBAI		Community	
AI-MFC-102-W10	Windows 10 Pro		Yes				User Account	
ARGENT	URL Object		Yes		MUMBAI		Auth Protocol	MD
DND-MFC-SQL	Windows Server		Yes		MUMBAI		Auth Password	
FTP	FTP Object		Yes		MUMBAI		Encrypt Algorithm	DES
FTP_1	FTP Object		Yes		MUMBAI		Encrypt Password	
POP	Mail Object				MUMBAI		TCP Parameters	
SMTP_1	Mail Object		Yes		MUMBAI		System Info Caching Minutes	30
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI		Monitoring Level	Normal
							Tier	Not Specified
)⊧ Tag	
							Location	MUMBAI
							Contact	
							Owner Accounts	
							Display Options	Refres
							Group/Key	Value
							Show Objects	All
							Network Group	*
							Monitoring Group	*
							Туре	*

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:



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

Search								Argent Instant Help Al	
					Server Or Device Ne	twork Group	Scan Network	Properties	✓ ∅ + ×
etwork Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact		Group/Key	Value
Demo Group	Network Group						1	Name	First Network Group
First Network Group	Network Group				MUMBAI			Туре	Network Group
192.168.108.97 L	Linux/UNIX		Yes		MUMBAI			Location	MUMBAI
192.168.111.1	IP Device		Yes		MUMBAI			Contact	
192.168.111.2	IP Device		Yes		MUMBAI			VMware Parameters	
192.168.111.3	IP Device		Yes		MUMBAI			XenServer Parameters	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI			SNMP Parameters	
192.168.111.5	IP Device		Yes					Extended Properties	
192.168.37.1	IP Device		Yes		MUMBAI			Description	
AI-2019-009	Windows Server		Yes		MUMBAI				
AI-MFC-102-W10	Windows 10 Pro		Yes						
ARGENT	URL Object		Yes		MUMBAI				
DND-MFC-SQL V	Windows Server		Yes		MUMBAI				
FTP F	FTP Object		Yes		MUMBAI				
FTP_1 F	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			1	

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

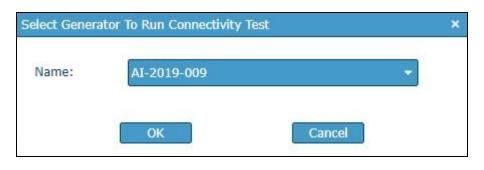
Connect Parameters	Select Default to connect using default parameters. Select Explicit to define
	the parameters explicitly. The following parameters need to be defined:
SNMP Version	It can be SNMPv1, SNMPv2c or SNMPv3. SNMPv3 requires authentication. If
	SNMPv3 is selected, valid authentication credentials 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	public is used. SNMPv3 user name.
User Account Auth Protocol	
	SNMPv3 user name.
Auth Protocol	SNMPv3 user name.

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:

Search					Server Or Device	Network Group	Scan Network	Properties	✓ 3 + ×
letwork Group Or Machine	Туре	Alias	Licensed	Suspend L	ocation	Contact		Group/Key	Value
Demo Group	Network Group							Name	192.168.111.4
First Network Group	Network Group			М	UMBAI			Licensed Products	Argent Omega for SNMP
192.168.108.97	Linux/UNIX		Yes	м	UMBAI			Alias	APC_UPS_003
192.168.111.1	IP Device		Yes	м	UMBAI			▶ IP Device	
192.168.111.18	IP Device			M	UMBAI			SNMP Managed	Yes
192.168.111.2	IP Device		Yes	м	UMBAI			+ TCP Parameters	
192.168.111.3	IP Device		Yes	M	UMBAI			System Info Caching Minutes	30
192.168.111.4	IP Device	APC_UPS_003	Yes					Monitoring Level	Normal
192.168.111.5	IP Device		Yes	Refresh				Tier	Not Specified
192.168.37.1	IP Device		Yes	Suspend Monitoring) Tag	
AI-2019-009	Windows Server		Yes	Reactivate				Location	MUMBAI
AI-MFC-102-W10	Windows 10 Pro		Yes	Save Changes				Contact	
ARGENT	URL Object		Yes					Owner Accounts	
DND-MFC-SQL	Windows Server		Yes					▶ Default Settings	
FTP	FTP Object		Yes					Time Zone Settings	Same as Location
FTP_1	FTP Object		Yes	Discover Neighbor Links				Critical	No
POP	Mail Object			Wireless Clients				Ignored	No
SMTP_1	Mail Object		Yes	Device Configuration Back	tups			Logical Dependency	
TEST_365	Microsoft 365 Service Unit		Ver	Set Critical Flag	-			Installed Applications	
				Set Ignore Flag				Extended Properties	
			-	Manually Add Server Or D				Description	
			_		evice				
				Test Connectivity					
				Bulk Licensing				Display Options	Refresh
			_	Export To Excel CSV					
				Backup CMDB-X Database				Group/Key	Value
				Restore				Show Objects	All
			_					Network Group	*
								Monitoring Group	*

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



The Results are shown:

≡ ARGENT	OMEGA (2.2A-2207-A)				A Home	🔅 Theme -		out Logout	D2
Search					Server Or Device Ne	twork Group	Scan Network	Properties	✓ 3 +	* 8
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact		Group/Key	Value	
Demo Group	Network Group							Name	192.168.111.4	
	Network Group	Connectivity Test Results			MUMBAI			Licensed Products	Argent Omega for SNMP	
192.168.108.97	Linux/UNIX		() 0000 4	10.0				Alias	APC_UPS_003	
192.168.111.1	IP Device	Argent Omega 2.2.2207.21 Copyright		-				▶ IP Device		
192.168.111.18	IP Device	For Argent Instant Help 7 by 24 with	an Argent e	ngineer, please see h	tp://help.Argent.com/help.ph	p		SNMP Managed	Yes	
192.168.111.2	IP Device	Target Machine: 192.168.111.4						TCP Parameters		
192.168.111.3	IP Device	Test At: AI-2019-009						System Info Caching Minutes	30	
192.168.111.4	IP Device	Test Time: Tue, 26 Jul 202	2 09:40:18	(UTC)				Monitoring Level	Normal	
192.168.111.5	IP Device			(0.0)				Tier	Not Specified	
192.168.37.1	IP Device	09:40:18 - Test 1: PING 09:40:18 - [VALID])⊧ Tag		
AI-2019-009	Windows Server							Location	MUMBAI	
AI-MFC-102-W10	Windows 10 Pro							Contact		
ARGENT	URL Object	09:40:18 - Test 2: Access Of SNMP M 09:40:18 - [VALID] sysName = APC_	anager UPS_003					Owner Accounts		
DND-MFC-SQL	Windows Server							▶ Default Settings		
FTP	FTP Object							Time Zone Settings	Same as Location	
FTP_1	FTP Object							Critical	No	
POP	Mail Object							Ignored	No	
SMTP_1	Mail Object							Logical Dependency		
TEST_365	Microsoft 365 Service Unit							Installed Applications		
								Extended Properties		
							-	Description		
		Print			Close					
								Display Options	R	efresh
								Group/Key	Value	
								Show Objects	All	
								Network Group	•	
								Monitoring Group		
								Туре	*	

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.

Search				Server Or D	evice Network Group	Scan Network	Properties	✓ S + ×
Network Group Or Machine	Туре	Alias	Licensed Suspe	nd Location	Contact	Active Directory		Value
Demo Group	Network Group					Network Browse	r	192.168.111.4
First Network Group	Network Group			MUMBAI		ICMP Ping		Argent Omega for SNMP
192.168.108.97	Linux/UNIX		Yes	MUMBAI		Discover SNMP [APC_UPS_003
192.168.111.1	IP Device		Yes	MUMBAI		Windows Cluster		
192.168.111.18	IP Device			MUMBAI		VMware Infrastr	ucture	Yes
192.168.111.2	IP Device		Yes	MUMBAI		Meraki Devices		
192.168.111.3	IP Device		Yes	MUMBAI		Import From Arc	ent Topology Manager	30
192.168.111.4	IP Device	APC_UPS_003	Yes	MUMBAI		Import External	Excel File	Normal
192.168.111.5	IP Device		Yes				Tier	Not Specified
192.168.37.1	IP Device		Yes	MUMBAI) Tag	
AI-2019-009	Windows Server		Yes	MUMBAI			Location	MUMBAI
AI-MFC-102-W10	Windows 10 Pro		Yes				Contact	
ARGENT	URL Object		Yes	MUMBAI			Owner Accounts	
DND-MFC-SQL	Windows Server		Yes	MUMBAI			▶ Default Settings	
FTP	FTP Object		Yes	MUMBAI			Time Zone Settings	Same as Location
FTP_1	FTP Object		Yes	MUMBAI			Critical	No
POP	Mail Object			MUMBAI			Ignored	No
SMTP_1	Mail Object		Yes	MUMBAI			Logical Dependency	
TEST_365	Microsoft 365 Service Unit		Yes	MUMBAI			Installed Applications	
							Extended Properties	
							Description	
							Description	
							Display Options	Refres
							Group/Key	Value
							Show Objects	All
							Network Group	*
							Monitoring Group	*
							Туре	*

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:

= ARGEN	IT OMEG	Network Scann	ing Result			D2D ×	ë Theme -	ر» Argent Instant Help	ල
Search		Ignored	Machine	Туре	Alias	Domain	o Scan Network	Properties	✓ 3 + × 8
Network Group Or Machine	Туре		192.168.4.183	IP Device				Group/Key	Value
			10.0.0.23	IP Device	AP5				
Demo Group	Network Group		192,168,4,181	IP Device				Name	192.168.111.4
First Network Group	Network Group		192.168.4.180	IP Device				Licensed Products	Argent Omega for SNMP
192.168.108.97	Linux/UNIX		10.0.0.38	IP Device	AP3			Alias	APC_UPS_003
192.168.111.1	IP Device		192.168.4.210	IP Device				> IP Device	
192.168.111.18	IP Device		10.0.0.25	IP Device	AP4			SNMP Managed	Yes
192.168.111.2	IP Device		10.0.0.11	IP Device	AP6) TCP Parameters	
192.168.111.3	IP Device		10.0.0.22	IP Device	AP2			System Info Caching Minutes	30
192.168.111.4	IP Device		10.0.0.24	IP Device	AP1			Monitoring Level	Normal
192.168.111.5	IP Device		10.0.0.24	IP Device	AP1			Tier	Not Specified
192.168.37.1	IP Device) Tag	
AI-2019-009	Windows Server							Location	MUMBAI
AI-MFC-102-W10	Windows 10 Pro	•				۱.		Contact	
ARGENT	URL Object	Save to Net	work Group: First Netw	vork Group				Owner Accounts	
DND-MFC-SQL	Windows Server		-					> Default Settings	
FTP	FTP Object		🗹 кеер с	Driginal Network Group				Time Zone Settings	Same as Location
FTP_1	FTP Object							Critical	No
POP	Mail Object		Toggle	ОК	Cancel			Ignored	No
SMTP_1	Mail Object							Logical Dependency	

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.

Search				Server Or De	vice Network Group Scan Network	Properties	✓ 2 + ×
letwork Group Or Machine	Туре	Alias	Licensed Suspend	Location	Contact	Group/Key	Value
Pemo Group	Network Group					Name	10.0.0.11
10.0.0.11	IP Device	407	Yes	MUMBAI		Licensed Products	Argent Omega for SNMP
10.0.0.22	IP Device Refresh			MUMBAI		Alias	AP6
10.0.0.23	IP Device Suspend Monitori	ng		MUMBAI		♦ IP Device	
10.0.0.24	IP Device Reactivate			MUMBAI		SNMP Managed	No
10.0.0.25	IP Device Save Changes			MUMBAI		+ TCP Parameters	
10.0.0.38	IP Device Undo			MUMBAI		System Info Caching Minutes	30
192.168.4.170	IP Device Add Property			MUMBAI		Monitoring Level	Normal
192.168.4.180	IP Device Delete			MUMBAI		Tier	Not Specified
192.168.4.181	IP Device Discover Neighbo	r Links		MUMBAI)⊧ Tag	
192.168.4.183	IP Device Wireless Clients			MUMBAI		Location	MUMBAI
192.168.4.210	IP Device Device Configurat	ion Backups		MUMBAI		Contact	
192.168.96.165	IP Device Set Critical Flag		Yes	MUMBAI		Owner Accounts	
192.168.96.55	IP Device Set Ignore Flag		Yes	MUMBAI		Default Settings	
AGT-PC	Windows Manually Add Ser		Yes			Time Zone Settings	Same as Location
AI-2019-001	Windows		Yes			Critical	No
AI-2019-002	Windows Test Connectivity		Yes			Ignored	No
AI-2019-003	Windows Bulk Licensing		Yes			Logical Dependency	
AI-2019-004	Windows Export To Excel C	sv	Yes			Installed Applications	
AI-2019-005	Windows Backup CMDB-X	Database	Yes			+ Extended Properties	
AI-2019-006	Windows Restore		Yes			Description	
AI-2019-007	Windows 10 Pro		Yes				
AI-2019-008	Windows Server		Yes				
AI-76	Windows 8.1 Pro N		Yes			Display Options	Refrest
AI-AD-4	Windows 10 Pro		Yes				
AI-MFC-101-W10	Windows 10 Pro		Yes			Group/Key	Value
AI-QC	Windows 10 Pro		Yes			Show Objects	All
AI-QC-001	Windows Server		Yes			Network Group	*
AI-QC-02	Windows 7 Ultimate		Yes			Monitoring Group	•
AI-QC-06	Windows 10 Pro		Yes			Туре	•

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

	IT OMEG	A (2.2A-22	07-A)					A Home	🔅 Theme -	ری) Argent Instant help Ab	out Logout
Search							Server/Device	Network Group	Scan Network	Properties	✓ S + ×
letwork Group/Machine	▲ Туре		Alias	Licensed	Suspend	Lo	ation	Contact	ĉ	Group/Key	Value
Demo Group	Network Group									Name	10.0.0.11
10.0.0.11	IP Device		AP6	Yes		MU	MBAI			Licensed Products	Argent Omega for SNMP
10.0.0.22	IP Device	Wireless Clients							D2I	× s	AP6
10.0.0.23	IP Device									Device	
10.0.0.24	IP Device	Client	Mac Address	IP	AP	SSID	First Seen	Last Seen	Sent/Recv	MP Managed	No
10.0.0.25	IP Device	Galaxy-A12	2a:c8:54:c5:7fibc	10.0.1.142	AP6	Hunt WIFI	19 Jul 2022	21 Jul 2022	0/1	P Parameters	
10.0.0.38	IP Device	Calaxy Alz	2010010410017110C	1010111192		ingine wilfi	17:20:30	05:59:45		stem Info Caching Minutes	30
192.168.4.170	IP Address	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	nitoring Level	Normal
192.168.4.180	IP Device									r	Not Specified
192.168.4.181	IP Device										
192.168.4.183	IP Device									ation	MUMBAI
192.168.4.210	IP Device									ntact	
192.168.96.165	IP Device									ner Accounts	
192.168.96.55	IP Device									Fault Settings	
AGT-PC	Windows 7 Ultimate									he Zone Settings	Same as Location
AI-2019-001	Windows 10 Pro									tical	No
AI-2019-002	Windows 10 Pro									ored	No
AI-2019-003	Windows 10 Pro									ical Dependency	
AI-2019-004	Windows 10 Pro									talled Applications	
AI-2019-005	Windows 10 Pro									ended Properties	
AI-2019-006	Windows 10 Pro									scription	
AI-2019-007	Windows 10 Pro									a subjection	
AI-2019-008	Windows Server				Cl	ose					
AI-76	Windows 8.1 Pro N									ay Options	Refres
AI-AD-4	Windows 10 Pro			Yes						ay options	- Keires
AI-MFC-101-W10	Windows 10 Pro			Yes						Group/Key	
AI-QC	Windows 10 Pro			Yes						Show Objects	All
AI-QC-001	Windows Server			Yes						Network Group	*
AI-QC-02	Windows 7 Ultimate			Yes						Monitoring Group	*
AI-QC-06	Windows 10 Pro			Yes						Туре	*
41-WER-47	Windows 10 Pro			Vas					-		

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

Search					Server Or Device N	letwork Group	Scan Network	Properties	✓ C + ×
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact		Group/Key	Value
Demo Group	Network Group							Name	192.168.37.1
First Network Group	Network Group				MUMBAI			Licensed Products	Argent Omega Baseline, Argent Om for SNMP
192.168.108.97	Linux/UNIX		Yes		MUMBAI			Alias	IOI SIMP
192.168.111.1	IP Device		Yes		MUMBAI			> IP Device	
192.168.111.18	IP Device				MUMBAI			SNMP Managed	Yes
192.168.111.2	IP Device		Yes		MUMBAI				Yes
192.168.111.3	IP Device		Yes		MUMBAI			TCP Parameters	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI			System Info Caching Minutes	720
192.168.111.5	IP Device		Yes					Monitoring Level	Normal
192.168.37.1	IP Device		Yes		MUMBAI			Tier	Not Specified
AI-2019-009	Windows Server	Refresh			MUMBAI			▶ Tag	
AI-MFC-102-W10	Windows 10 Pro	Suspend Monitoring						Location	MUMBAI
ARGENT	URL Object	Reactivate			MUMBAI			Contact	
DND-MFC-SQL	Windows Server	Save Changes			MUMBAI			Owner Accounts	
FTP	FTP Object	Undo			MUMBAI			▶ Default Settings	
FTP_1	FTP Object	Add Property			MUMBAI			Time Zone Settings	Same as Location
POP	Mail Object	Delete			MUMBAI			Critical	No
SMTP_1	Mail Object	Discover Neighbor L	nks		MUMBAI			Ignored	No
TEST_365	Microsoft 365 Service Unit	Wireless Clients			MUMBAI			Logical Dependency	
		Device Configuration	Backups					Installed Applications	
		Set Critical Flag						Extended Properties	
		Set Ignore Flag						Description	
			0.0.1.						
		Manually Add Server	Or Device					Display Options	Refresh
		Test Connectivity							
		Bulk Licensing						Group/Key	Value
		Export To Excel CSV						Show Objects	All
		Backup CMDB-X Dat	abase					Network Group	*
		Restore						Monitoring Group	*

Agent Omega for SNMP Tool Sets

Select Tool Sets from the Home Screen:

ARGENT OME	GA (2.2A-2207-A)			🔅 Theme - Arge	ල් 🥱 🖒 nt Instant Help About Logout
Q Find any field's name on any screen. For e	example, type 'Status'				
Recently Viewed					
11	0	*	Ê		
CMDB-X	Engines	Tool Sets	Scheduled Tasks	Events	
Products					
-1		11	()		
Global Status	Events	SuperMaps	Network Topology Maps	Super Console	SLA
1	52		•	X	*
Performance Graph	Dashboard	CeoConsole	Enterprise View	Тор Х	ViewMagic
Ê		11	*	A	曲
Scheduled Tasks	Relators	CMDB-X	Tool Sets	Alerts	Calendars
		0	•		
Macros	Monitoring Groups	Engines	Security		
Argent Reporter					
*		业	\sim		~
Alerts	Compliance	Cross Reference	Miscellaneous	PowerShell	Performance
	SOL				
SLA	SQL SQL Query				

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

= ARGENT ON	MEGA (2.2A-2207-A)			😭 Home	🔅 Theme -	('') Argent Instant Help	? About	U Logout	
Tool Sets	Search								
Argent Omega Baseline	Name	Description							
 Image: Argent Compliance Automator Image: Argent Omega Web Defender 	Argent Omega Baseline								
Argent Omega web Derender Argent Omega for Microsoft 365	Argent Compliance Automator								
	Argent Omega Web Defender								
Argent Omega for SNMP	Argent Omega for Microsoft 365								
SNMP Rules	Argent Omega for SNMP								
SNMP Trap Rules	Argent Omega for SQL Server								
DeviceMagic Port Rules									
IINK Connectivity Rules									
Device Configuration Rules									
CISCO VPN Tunnel Rules									
CISCO Remote Access Rules									
Generic VPN Rules									
PowerShell Script Rules									
Argent Omega for SQL Server	1								
Alerts									
Monitoring Groups									
Relators									
Macros									
Calendars									
Administration									
									_

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:

■ ARGENT OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	(') Argent Instant Help	? About	U Logout	SN5S
▼ 🖬 Tool Sets	Use SNMP MIB:	3COM::A3Com-System-r8-MIB.mib		- +	1			ŕ
🕨 🖬 Argent Omega Baseline	Enumerate SNMP Table:							
Argent Compliance Automator	SNMP Rule View:	Simple						
Argent Omega Web Defender	Value SNMP OID:	1.3.6.1.4.1.43.2.13.8.4.0			(a3sysCpuUtil)			
Argent Omega for Microsoft 365					(absyscpuou)			
Argent Omega for SNMP	Value Type:	INTEGER -						
▼ SNMP Rules	Metric Calculation:	Get 👻						
▼ 🚾 3Com	Scale Factor:	No Scale 👻						
SNMP_3COM_SWITCH_CPU_STATUS	Comparison:	Greater Than 👻						
SNMP_3COM_SWITCH_FAN_FAILURE	Object Value:	90						
SNMP_3COM_SWITCH_INACTIVE_PORT SNMP_3COM_SWITCH_OVER_TEMPERATURE	Retrieve Performance Data Fo	r Argent Forecaster Only						
APC	Fire Separate Events For Each	Broken Instance						
Bridge (RFC 1493)	Fail Rule If Data Is Not Availa	ble Or Nonexistent						
CISCO Firewall	Save Performance Data To Th	e Argent Forecaster Using Data Store: {default}	-					
CISCO Hardware	Tag 1:							
CISCO Interface	Tag 2:							
CISCO IOS								
CISCO RTT Monitor	Tag 3:							
🕨 🛀 CISCO Stack	Post Event Even If The Same	Event Is Still Outstanding (Unanswered)						
🕨 🔛 Compaq Hardware	Do So Only After 1	Hour 0 💭 Minute Since Event Is Post						
🕨 🚧 Dell OpenManage	Ignore The Same Outstanding	Event If Alerts Were Fired More Than						
🕨 🚧 Dell Storage	Post Event Only After Rule Is	Broken 2 Or More Times						
▶ 📶 Dell Switch	- Reset Counter							
Extreme Network	After Event Is Post							
Fortinet	After Event Is Answered							
🕨 🚧 Foundry	After The Actual Condition Is	Corrected						
🕨 🚧 HP Hardware								
HP JetDirect	Application:							
HP Switch	Reference URL:							
IBM ATM Switch								
IBM Director	Console Comment:	High CPU Usage ***						
	Description							-

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 OME	GA (2.2A-2207-A)		😭 Home	🔅 Theme -	رِپُ Argent Instant Help	? About	U Logout	SN5S
👻 🔚 Tool Sets	Use SNMP MIB:	3COM::A3Com-System-r8-MIB.mib		- +]			ŕ
Argent Omega Baseline	Enumerate SNMP Table:							
Argent Compliance Automator Argent Omega Web Defender	Table Entry OID:							
Argent Omega for Microsoft 365		Continue Enumerating OIDs Even Rule Is Already Broken						
 Argent Omega for SNMP 	Use Custom Instance Name:							
✓ III SNMP Rules	Enumeration Filter:							
👻 🔚 3Com	SNMP Rule View:	Simple -						
C SNMP_3COM_SWITCH_CPU_STATUS	Value SNMP OID:	1.3.6.1.4.1.43.2.13.8.4.0			(a3sysCpuUtil)			
SNMP_3COM_SWITCH_FAN_FAILURE	Value Type:	INTEGER 🗸						
SIMP_3COM_SWITCH_INACTIVE_PORT	Metric Calculation:	Get 👻						
Image: Some_scom_switch_over_temperature Image: Some_scom_switch_over_temperature	Scale Factor:	No Scale 👻						
 Bridge (RFC 1493) 	Comparison:	Greater Than 👻						
GISCO Firewall	Object Value:	90						
CISCO Hardware	Retrieve Performance Data For	r Argent Forecaster Only						
CISCO Interface	Fire Separate Events For Each	Broken Instance						
CISCO IOS	Fail Rule If Data Is Not Availab	ole Or Nonexistent						
CISCO RTT Monitor		e Argent Forecaster Using Data Store: {default}	•					
CISCO Stack		(delader)						

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

■ ARGENT OME	GA (2.2A-2207-A)					Home	theme -	(*) Argent Instant Help	() About	Logout	
Tool Sets	Use SNMP MIB:	3COM::A3Com-System	n-r8-MIB.mib		+						
Margent Omega Baseline	Enumerate SNMP Table:										
Argent Compliance Automator	Table Entry OID:										
🕍 Argent Omega Web Defender		Continue Enumerat	ing OIDs Even Rule Is Already I	Broken							
Margent Omega for Microsoft 365	Use Custom Instance Select SN				SN5	3 × 1					
Magent Omega for SNMP	Enumeration Filter:										
V MP Rules		MP MIB: 3COM::A3Com	-System-r8-MIB.mib								
▼ M 3Com		arch									
SNMP_3COM_SWITCH_CPU_STATUS	Value SNMP OID: Name		OID	Composed Syntax	Max Access	Util)					
SNMP_3COM_SWITCH_FAN_FAILURE SNMP_3COM_SWITCH_INACTIVE_PORT	Metric Calculation: a3sysChi	ipEntry	1.3.6.1.4.1.43.2.13.2.1.1	SEQUENCE	NotAccessible						
SNMP_3COM_SWITCH_INACTIVE_PORT SNMP_3COM_SWITCH_OVER_TEMPERATURE	Pietric Calculation:		1.3.6.1.4.1.43.2.13.3.1.1	SEQUENCE	NotAccessible						
<pre>> MAPC</pre>	Scale Factor: a3sysBro	iEntry	1.3.6.1.4.1.43.2.13.4.2.1	SEQUENCE	NotAccessible						
 Bridge (RFC 1493) 	Comparison: a3sysSN	MPCommEntry	1.3.6.1.4.1.43.2.13.7.5.1	SEQUENCE	NotAccessible						
GISCO Firewall	Object Value: a3sysSN	MPMgrEntry	1.3.6.1.4.1.43.2.13.7.6.1	SEQUENCE	NotAccessible						
CISCO Hardware	Retrieve Perform. a3sysTel	netMgrEntry	1.3.6.1.4.1.43.2.13.7.7.1	SEQUENCE	NotAccessible						
CISCO Hardware CISCO Interface	Fire Separate Eve	sswordEntry	1.3.6.1.4.1.43.2.13.7.8.1	SEQUENCE	NotAccessible	_					
CISCO INTERNACE	Fail Rule If Data 1	erBootListEntry	1.3.6.1.4.1.43.2.13.10.9.1	SEQUENCE	NotAccessible						
CISCO RTT Monitor		BootEntry	1.3.6.1.4.1.43.2.13.10.10.1	SEQUENCE	NotAccessible	_					
CISCO Stack	assystem	Entry RecoveryEntry	1.3.6.1.4.1.43.2.13.12.9.3.1 1.3.6.1.4.1.43.2.13.13.1.1	SEQUENCE	NotAccessible NotAccessible	-					
Compag Hardware	Tag 2:	RecoveryEntry	1.3.6.1.4.1.43.2.13.13.1.1	SEQUENCE	NotAccessible	-					
Dell OpenManage											
	Tag 3:										
Dell Storage Dell Switch	Post Event Even 1										
Extreme Network	Do So Only After Syntax:		nformation about one of the chi	ps installed in the CPU module	·						
Extreme Network Fortinet	Ignore The Same	hipEntry									
Foundry	Post Event Only A										
▶ 🖬 HP Hardware	Reset Counter										
HP JetDirect	After Event Is Po:										
HP Switch	After Event Is An					_					
BIM ATM Switch	After The Actual	_			_						
IBM Director			ок	Cance	el la						
Interface (RFC 1213)	Application:										
LAN Manager	Reference URL:										
> M Lannet	Console Comment:										
Idexmark	see conside continent:	High CPU Usage ***									

Select the table entry and click OK.

■ ARGENT OME	GA (2.2A-2207-A)		🐴 Home	🔅 Theme -	(*) Argent Instant help	? About	U Logout	SN5S
 ✓ I Tool Sets ▲ Argent Omega Baseline 	Use SNMP MIB:	3COM::A3Com-System-r8-MIB.mib		• +]			í
Argent Compliance Automator	Enumerate SNMP Table: Table Entry OID:	1.3.6.1.4.1.43.2.13.2.1.1			(a3sysChipEntry)			
 Argent Omega Web Defender Argent Omega for Microsoft 365 	,	Continue Enumerating OIDs Even Rule Is Already Broken						
Argent Omega for SNMP SNMP Rules	Use Custom Instance Name: Enumeration Filter:							
▼ 🖬 3Com	SNMP Rule View:	Simple 🔹						
SNMP_3COM_SWITCH_CPU_STATUS SNMP_3COM_SWITCH_FAN_FAILURE	Value SNMP OID: Value Type:	Please Choose:						
SNMP_3COM_SWITCH_INACTIVE_PORT SNMP_3COM_SWITCH_OVER_TEMPERATURE	Metric Calculation:	Get 👻						
► MAPC	Scale Factor: Comparison:	No Scale Greater Than						
 Bridge (RFC 1493) CISCO Firewall 	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.

■ ARGENT OME	GA (2.2A-2207-A)			ne Theme -	ری Argent Instant Help	? About	U Logout	SN5S
Windows Performance Rules	Use SNMP MIB:	3COM::A3Com-System-r8-MIB.mib		- +	1			ŕ
PowerShell Script Rules	Enumerate SNMP Table:							
WMI Script Rules	Table Entry OID:	1.3.6.1.4.1.43.2.13.2.1.1			(a3sysChipEntry)			
LINUX Script Rules		Continue Enumerating OIDs Even Rule Is Alr	eady Broken		,			
🔻 🖬 UNIX Script Rules	Use Custom Instance Name:							
🕨 🚧 Solaris	Instance OID:							
×IX 🔤	Use Group of Regular Expression:							
HP-UX	Enumeration Filter:							
▶ 🕍 SCO	SNMP Rule View:	Simple						
Grant Compliance Automator	Value SNMP OID:				1			
Argent Omega Web Defender	Value Type:	Please Choose:			I			
Argent Omega for SNMP	Metric Calculation:	Get						
✓ SNMP Rules								
▼ 11 3Com	Scale Factor:	No Scale 🔹						
SNMP_3COM_SWITCH_CPU_STATUS	Comparison:	Greater Than						
SNMP_3COM_SWITCH_FAN_FAILURE	Object Value:	90 🗘						
SNMP_3COM_SWITCH_INACTIVE_PORT	Retrieve Performance Data For	Argent Forecaster Only						
SNMP_3COM_SWITCH_OVER_TEMPERATURE	Fire Separate Events For Each	Broken Instance						
▶ 🛀 APC	Fail Rule If Data Is Not Availabl	e Or Nonexistent						
Bridge (RFC 1493)	Save Performance Data To The	Argent Forecaster Using Data Store: {defau	ult} 👻					
CISCO Firewall	Tag 1:							
CISCO Hardware	Tag 2:							
CISCO Interface	Tag 3:							
	Post Event Even If The Same E	vent Is Still Outstanding (Unanswered)						
GISCO RTT Monitor GISCO Stack		Hour 0 Minute Since Event Is Post						
Compag Hardware			Hour 0 🛋 Minute Ago					
Dell OpenManage	_							
Dell Storage	Post Event Only After Rule Is B	roken 2 Cr More Times						
Dell Switch	Reset Counter							
Extreme Network	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.

■ ARGENT OME	GA (2.2A-2207-A)		👫 Home	🔅 Theme -	(*) Argent Instant Help	? About	ن Logout	SN5S
	Use SNMP MIB: Enumerate SNMP Table: Table Entry OID: Use Custom Instance Name:	3COM: :A3Com-System-r8-MIB.mib I.3.6.1.4.1.43.2.13.2.1.1 Continue Enumerating OIDs Even Rule Is Already Broken		• +	(a3sysChipEntry)			-
Mindows Program Rules Mindows Program Rules Mindows Performance Rules More Rules Mindows Program Rules MMI Script Rules	Enumeration Filter: Filter On SNMP OID: Filter OID Type: Filter Condition:	StableOID\$.3 OCTETSTRING Is Not Empty			(a3sysChipName)			
UNIX Script Rules Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Galaxie Ga	SNMP Rule View: Value SNMP OID: Value Type: Metric Calculation: Scale Factor:	Simple Please Choose: Get No Scale]			
Argent Omega Web Defender Argent Omega for Microsoft 365 Argent Omega for SNMP SNMP Rules GOm	Comparison: Object Value: Retrieve Performance Data Fo Fire Separate Events For Each	Greater Than						
SNMP_3COM_SWITCH_CAL_STATUS SNMP_3COM_SWITCH_CAL_FALURE SNMP_3COM_SWITCH_INACTIVE_PORT SNMP_3COM_SWITCH_OVER_TEMPERATURE MAPC Mark SAC (RFC 1493) Mark Sac (RFC 1493)	Tag 1: Tag 2: Tag 3:	ble Or Nonexistent e Argent Forecaster Using Data Store: default expent fastill Outstanding (Unanswered)	•					
CLSCO Firewall CLSCO Hardware CLSCO Interface CLSCO IOS CLSCO RTT Monitor	Do So Only After 1	Hour O Minute Since Event Is Post 2 Event If Alerts Were Fired More Than 1 Hour 0 Minute Age	0					

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.

■ ARGENT OME	GA (2.2A-2207-A)		de Home	🔅 Theme -	(*) Argent Instant Help	? About	U Logout	SN5S
✓ 11 3Com	Use SNMP MIB:	3COM::A3Com-System-r8-MIB.mib		- +				Ê
SNMP_3COM_SWITCH_CPU_STATUS	Enumerate SNMP Table:				,			
SNMP_3COM_SWITCH_FAN_FAILURE	SNMP Rule View:	Simple -						
\$\$\$ SNMP_3COM_SWITCH_INACTIVE_PORT	Value SNMP OID:	1.3.6.1.4.1.43.2.13.8.4.0			(a3sysCpuUtil)			
SNMP_3COM_SWITCH_OVER_TEMPERATURE	Value Type:	INTEGER						
APC	Metric Calculation:	Get						
Bridge (RFC 1493)	Scale Factor:	No Scale						
CISCO Firewall								
CISCO Hardware	Comparison:	Greater Than						
CISCO Interface	Object Value:	90 😂						
GISCO IOS GISCO RTT Monitor	Retrieve Performance Data Fo	r Argent Forecaster Only						
 CISCO RT Monitor CISCO Stack 	Fire Separate Events For Each	Broken Instance						
Compag Hardware	Fail Rule If Data Is Not Availa	ole Or Nonexistent						
Dell OpenManage	Save Performance Data To Th	e Argent Forecaster Using Data Store: {default}	-					
Dell Storage	Tag 1:							
Dell Switch	Tag 2:							
Extreme Network	Tag 3:							
Fortinet	Deat Sweet Sweet 16 The Course	Sugar to Shill Outstanding (Usersmund)						
🕨 📁 Foundry		Event Is Still Outstanding (Unanswered)						
🕨 🚾 HP Hardware		Hour 0 💭 Minute Since Event Is Post						
🕨 🐸 HP JetDirect	Ignore The Same Outstanding	Event If Alerts Were Fired More Than 1 🗘 Hour 0 🗘 Minute Ago						
🕨 🖬 HP Switch	Post Event Only After Rule Is	Broken 2 🗘 Or More Times						
IBM ATM Switch	Reset Counter							
IBM Director	After Event Is Post							
Interface (RFC 1213)	 After Event Is Answered 							
🕨 🚧 LAN Manager	After The Actual Condition Is	Corrected						
🕨 🚧 Lannet								
▶ 📶 Lexmark	Application:							
▶ 🚾 NetApp	Reference URL:							
Netscreen	Console Comment:	ligh CPU Usage ***						
Novell	• I	nyn cro osaye						
	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.

■ ARGENT OME	GA (2.2A-2207-A)			A Home	🔅 Theme 🕶	ে) Argent Instant Help	? About	U Logout	SN5S
PowerShell Script Rules	Use SNMP MIB:	3COM::A3Com-System-r8-MIB.mib			- +				^
WMI Script Rules	Enumerate SNMP Table:								
IINUX Script Rules	SNMP Rule View:	Multi-Level	-						
Image: UNIX Script Rules Image: Solaris	Value SNMP OID:	1.3.6.1.4.1.43.2.13.8.4.0				(a3sysCpuUtil)			
						(assyschuou)			
HP-UX	Value Type:	Please Choose:							
▶ SCO	Metric Calculation:	Get	<u> </u>						
Argent Compliance Automator	Scale Factor:	No Scale	-						
Argent Omega Web Defender	Comparison:	Equal To	-						
Argent Omega for Microsoft 365	Acceptable Limit Value:	0 🗘							
 Argent Omega for SNMP 	Approaching Limit Value:	0 🗘							
▼ 🐸 SNMP Rules	At Limit Value:	0 🗘							
🔻 🖬 3Com	Exceeding Limit Value:	0 🗘							
SNMP_3COM_SWITCH_CPU_STATUS	Major Overload Value:								
SNMP_3COM_SWITCH_FAN_FAILURE	Retrieve Performance Data Fo		1						
SNMP_3COM_SWITCH_INACTIVE_PORT	_								
SNMP_3COM_SWITCH_OVER_TEMPERATURE	Fire Separate Events For Each								
APC	Fail Rule If Data Is Not Availab	ole Or Nonexistent							
Bridge (RFC 1493)	Save Performance Data To The	e Argent Forecaster Using Data Store:	{default}	-					
CISCO Firewall	Tag 1:								
CISCO Hardware	Tag 2:								
CISCO Interface	Tag 3:		=						
CISCO IOS	Post Event Even If The Same I	Event Is Still Outstanding (Unanswered)							
CISCO RTT Monitor			P1						
CISCO Stack									
Compaq Hardware		Event If Alerts Were Fired More Than	1 🗘 Hour 🛛 🗘 Minute Ago						
Dell OpenManage	Post Event Only After Rule Is I	Broken 2 🚺 Or More Times							
Dell Storage	Reset Counter								
Dell Switch	After Event Is Post								
Extreme Network	After Event Is Answered								
Fortinet	After The Actual Condition Is (Corrected							
Foundry									

Advanced

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

Sub-Rule Logic combo box.

■ ARGENT OME	GA (2.2A-2207-A)		Hor	Ne Theme -	ری Argent Instant Help	? About	U Logout	SN5S
MowerShell Script Rules MVII Script Rules MII Script Rules	Use SNMP MIB: Enumerate SNMP Table:	3COM::A3Com-System-r8-MIB.mib		* +]			í
INVX Script Rules	SNMP Rule View:	Advanced						
Solaris	Sub-rule Logic:	Rule Is Broken If Any Is True						
▶ MIX		Rule Is Broken If Any Is True						
► HP-UX	Selected SNMP OIDs	Rule Is Broken If All Are True				+	🗢 × 1	
> 🖬 SCO	object warne	UIU		Condition				
Argent Compliance Automator								
🕨 🐸 Argent Omega Web Defender								
Argent Omega for Microsoft 365								
✓ Interpret 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	Retrieve Performance Data	For Argent Forecaster Only						
🕨 🔤 Bridge (RFC 1493)	Fire Separate Events For Ea	ach Broken Instance						
CISCO Firewall	Fail Rule If Data Is Not Ava	ilable Or Nonexistent						
CISCO Hardware	Save Performance Data To	The Argent Forecaster Using Data Store: {def	ault}					
CISCO Interface	Tag 1:							
CISCO IOS	Tag 2:							
CISCO RTT Monitor	Tag 3:							
CISCO Stack								
🕨 🔚 Compaq Hardware	_	ne Event Is Still Outstanding (Unanswered)						
🕨 🕍 Dell OpenManage	Do So Only After 1	Hour 0 C Minute Since Event Is Post						
🕨 📔 Dell Storage	Ignore The Same Outstand	ing Event If Alerts Were Fired More Than 1	Hour 0 C Minute Ago					
Dell Switch	Post Event Only After Rule	Is Broken 2 Or More Times						
Extreme Network	Reset Counter							
Fortinet	After Event Is Post							
Foundry	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.

Select A SNMP OID		SN5A	×
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		
	OK		

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

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		SN5A ×
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 🗘	
	OK	

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 OME	GA (2.2A-2207-A)			🐴 Home Th	🔅 heme -	ڑی) Argent Instant Help	? About	U Logout	SN5:
SNMP Rules SNMP Rules SNMP_SCOM_SWITCH_CPU_STATUS SNMP_3COM_SWITCH_FAN_FAILURE	Use SNMP MIB: Enumerate SNMP Table: SNMP Rule View:	FORTINET::FORTINET-FOR Advanced	RTIGATE-MIB.mib		• +				
SNMP_3COM_SWITCH_INACTIVE_PORT	Sub-rule Logic:	Rule Is Broken If Any Is T	rue 🔻						
SNMP_3COM_SWITCH_OVER_TEMPERATURE	Selected SNMP OIDs						+	* ×	↑
 iii APC iiii Bridge (RFC 1493) 	Object Name		OID	Conditio	on				
CISCO Firewall	fgSysDiskUsage		1.3.6.1.4.1.12356.101.4.1.6.0	Use As V	Variable: VAR_	DISK_USAGE			
CISCO Hardware	fgSysDiskCapacity		1.3.6.1.4.1.12356.101.4.1.7.0	Use As V	Variable: VAR_	DISK_CAPACITY			
CISCO Interface	Formula(Disk Status)		VAR_DISK_USAGE * 100/VAR_DISK_CAPACITY	Use As V	Variable: Disk	Status			
CISCO IOS									
CISCO RTT Monitor									
CISCO Stack									
🕨 🖬 Compaq Hardware									
🕨 🖬 Dell OpenManage									
🕨 📶 Dell Storage	4								
Dell Switch									
Extreme Network	Retrieve Performance Data Fo								
✓ I Fortinet	Fire Separate Events For Each								
SNMP_FORTINET_CPU_STATUS	Fail Rule If Data Is Not Availa	ble Or Nonexistent							
SNMP_FORTINET_DISK_STATUS	Save Performance Data To Th	e Argent Forecaster Using Da	ata Store: {default}	-					
SNMP_FORTINET_DISK_STATUS_1	Tag 1:								
SNMP_FORTINET_INTERFACE_DOWN	Tag 2:								
SNMP_FORTINET_INTERFACE_DOWN_1	Tag 3:								
SNMP_FORTINET_MEMORY_STATUS SNMP_FORTINET_VPN_SSL_TUNNEL_TOTAL	Post Event Even If The Same	Event Is Still Outstanding (U	Inanswered)						
<pre>w snmp_fortinet_vpn_ssl_user_total</pre>			Since Event Is Post						
Foundry									
HP Hardware	Ignore The Same Outstanding								
HP JetDirect	Post Event Only After Rule Is	Broken 2 🗘 Or Mo	re Times						
HP Switch	Reset Counter								
IBM ATM Switch	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.

■ ARGENT OME	GA (2.2A-2207-A)		📸 🔅 Home Theme - Argent I	sN4: (۱) المعالم (۱۹۹۵) Instant Help About Logout
▼ 📶 Tool Sets	Use SNMP MIB:	CISCO::CISCO-FIREWALL-MIB.mib	- +	
🕨 🕍 Argent Omega Baseline	Enterprise OID:	1.3.6.1.4.1.9.9.147.2.0		
Argent Compliance Automator	Trap Name:			
Argent Omega Web Defender				
Argent Omega for Microsoft 365	Trap Type:	enterpriseSpecific 👻 2		
🔻 📁 Argent Omega for SNMP	Custom Trap Idenfication			
SNMP Rules	Sub-rule Logic:	Rule Is Broken If All Are True		
🔻 🕍 SNMP Trap Rules	Selected Trap Message Variable (OIDs		+
Barracuda	Object Name	qip	Condition	
CheckPoint	cfwBasicSecurityEventType	13614199147111213	= 6	
👻 🚾 CISCO	crwBasicSecurityEventType	1.3.6.1.4.1.9.9.147.1.1.1.2.1.3	= 6	
TRP_CISCO_PIX_ADDR_SPOOF_DETECT				
A TRP_CISCO_PIX_DOS_ATTACK				
A TRP_CISCO_PIX_INVALD_PAK_ATTACK				
ATTACK				
A TRP_CISCO_PIX_RECON_DETECT				
A TRP_CISCO_PIX_SVC_SPOOF_DETECT				
A TRP_CISCO_PIX_THIRDPARTY_ATTACK				
ATRP_CISCO_PIX_THIRDPARTY_ATTACK_1				
Extreme Network				
Fortigate	Automatic Resolution	Condition Is Corrected If Receiving A SNMP Trap Specified Below		
🕨 🚧 Juniper	Message Display:	Full Detail		
SonicWall	Trap Event Format:	System Default 🗸		
VPN	Save Performance Data To	The Argent Forecaster Using Data Store: {default}	~	
DeviceMagic Port Rules	Tag 1:			
LINK Connectivity Rules	Tag 2:			
Device Configuration Rules	Tag 3:			
CISCO VPN Tunnel Rules				
CISCO Remote Access Rules	Post Event Even If The San	ne Event Is Still Outstanding (Unanswered)		
Generic VPN Rules	Do So Only After 1	Hour 0 C Minute Since Event Is Post		
PowerShell Script Rules	Ignore The Same Outstand	ding Event If Alerts Were Fired More Than 1 🗍 Hour 0 🖨 Minute Age		
Argent Omega for SQL Server	Post Event Only After Rule	Is Broken 2 0 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.

= ARGENT OME	GA (2.2A-2207-A)		effective Home	🔅 Theme -	ری Argent Instant Help	? About	U Logout
▼ 🔚 Tool Sets	Use SNMP MIB:	Please Choose:			- +		-
🔻 🔚 Argent Omega Baseline	Enterprise OID:	1.3.6.1.4.1.2620.1.1.0					
Service Level Agreement Rules	Trap Name:	fwTrap					
System Down Rules	Trap Type:	enterpriseSpecific	- 1 (
Windows Service Rules	Custom Trap Idenfication						
🕨 📔 Windows Program Rules	Sub-rule Logic:	Please Choose:	-				
Windows Performance Rules	Sub Tule Logici	Rule Is Broken If Any Is True					
PowerShell Script Rules	Selected Trap Message Variable (Rule Is Broken If All Are True					
WMI Script Rules	Object Name	OID		Condition			
LINUX Script Rules							
UNIX Script Rules							
Solaris	_						
AIX 📔							
▶ 🚧 HP-UX							
▶ 🕍 SCO							
Argent Compliance Automator							
🕨 🛀 Argent Omega Web Defender							
Argent Omega for Microsoft 365							
▼ Magent Omega for SNMP							
SNMP Rules	Automatic Resolution	Condition Is Corrected If Receiving A 1	SNMP Tran Specified Below				
🔻 🔚 SNMP Trap Rules	Message Display:	Full Detail	Shirin hup Speemed Delow				
🕨 🚧 Barracuda	message Display:	Full Detail	-				
	Trap Event Format:	System Default	-				
trp_checkpoint_firewall_event	Save Performance Data To	The Argent Forecaster Using Data Store:			•		
▶ 🖬 CISCO	Tag 1:						
Extreme Network	Tag 2:		f i				
Fortigate	Tag 3:		4				
🕨 🚧 Juniper							
🕨 🖬 SonicWall		he 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.

■ ARGENT OME	GA (2.2A-2207-A)		😚 Home	🔅 Theme -	(") Argent Instant Help	? About	ن Logout	SN4S
▼ 📶 Tool Sets	Sub-rule Logic:	Please Choose:	-					ľ
🔻 🕍 Argent Omega Baseline	Sub rule Logie.							
Service Level Agreement Rules	Selected Trap Message Variable					+		↑ ↓
System Down Rules	Object Name	OID		Condit	ion			
Windows Service Rules								
🕨 🔚 Windows Program Rules								
Windows Performance Rules								
PowerShell Script Rules								
WMI Script Rules								
LINUX Script Rules								
🔻 🔚 UNIX Script Rules								
🕨 🚞 Solaris								
N 🖬 AIX								
🕨 🚞 HP-UX								
▶ 🖬 sco	Automatic Resolution	Condition Is Corrected If Receiving A SNMF	Trap Specified Belov	v				L
Argent Compliance Automator	Trap Name:	_						
🕨 🚧 Argent Omega Web Defender	Trap Type:	enterpriseSpecific	60					
Argent Omega for Microsoft 365	Sub-rule Logic:							
▼ Interpret Argent Omega for SNMP	Sub-rule Logic:	Rule Is Broken If Any Is True	~					
SNMP Rules	Selected Trap Message Variable	e OIDs (Auto Resolution)				+		† +
👻 🚧 SNMP Trap Rules	Object Name	OID		Condit	ion			
🕨 🚾 Barracuda								
▼ CheckPoint								
trp_checkpoint_firewall_event								
▶ 🖬 CISCO								
🕨 🚞 Extreme Network								
🕨 🚞 Fortigate								
🕨 🚧 Juniper								
🕨 🛀 SonicWall								

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

■ ARGENT OME	GA (2.2A-2207-A)
▶ 🛀 HP-UX	Do Ping Test On Device
▶ 🚧 sco	Do Ping Test On Connected Neighbors
Argent Compliance Automator	
🕨 🕍 Argent Omega Web Defender	Report Down Switch Ports
Argent Omega for Microsoft 365	Report Switch Port When Status Changes 🛛
▼ I Argent Omega for SNMP	Test Ping Blast Packet Loss
SNMP Rules	Test Ping Blast Packet Latency
SNMP Trap Rules	
🔻 🔚 DeviceMagic Port Rules	Test Port In Mbps
DPT_PORT_COMPREHENSIVE	Test Port Out Mbps
DPT_PORT_DOWN	Test Port In/Out Mbps
DPT_PORT_MBPS_PREDICTOR_ONLY	
DPT_PORT_PACKET_LATENCY	Only Test Ports Matching Criteria
DPT_PORT_PACKET_LOSS	Fail Rule If Data Is Not Available Or Nonexistent
DPT_PORT_STATUS	Save Performance Data To The Argent Forecaster Using Data Store: {default}
DPT_PORT_STATUS_CHANGED	Tag 1:
🕨 🚞 LINK Connectivity Rules	Tag 2:
🕨 📁 Device Configuration Rules	Tag 3
CISCO VPN Tunnel Rules	
CISCO Remote Access Rules	Post Event Even If The Same Event Is Still Outstanding (Unanswered)
🕨 🚞 Generic VPN Rules	Do So Only After 1 C Hour 0 Minute Since Event Is Post
🕨 🚞 PowerShell Script Rules	🔲 Ignore The Same Outstanding Event If Alerts Were Fired More Than 🔢 🛟 Hour 💿 🛟 Minute Ago
Argent Omega for SQL Server	Post Event Only After Rule Is Broken 2 🗘 Or More Times
▼ 🖬 Alerts	- Reset Counter
Correction	Assc Counce Assc Coun
Motification	After Event 1s Answerd
🕨 🚧 Alert Macro	After Territ A studied of the studie
Monitoring Groups	
🕨 🚞 Relators 🗸 🗸	Application:

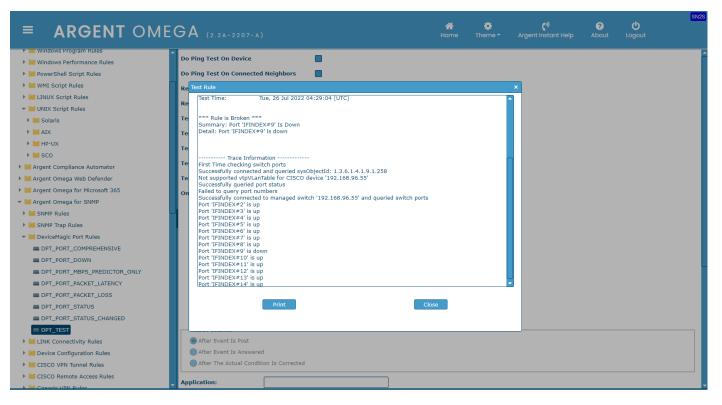
Check the option **Do Ping Test On Device** to check the connectivity of a SNMP device by doing a Ping

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:



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.

■ ARGENT OME	GA (2.2A-2207-A) GA (2.2A-2207-A) Home Theme Argent Instant Help About Logout
Windows Program Rules	Do Ping Test On Device
Windows Performance Rules	
PowerShell Script Rules	Do Ping Test On Connected Neighbors
WMI Script Rules	Report Down Switch Ports
LINUX Script Rules	Report Switch Port When Status Changes
 UNIX Script Rules 	
🕨 🚾 Solaris	
AIX	Acceptable Limit Value: 10 🗘 %
▶ 🚧 HP-UX	Approaching Limit Value: 30 🗘 %
▶ 🚾 SCO	🖉 At Limit Value: 100 🗘 %
Argent Compliance Automator	Exceeding Limit Value: 80 9%
🕨 🚧 Argent Omega Web Defender	Major Overload Value: 90 🖉 %
Argent Omega for Microsoft 365	
🔻 🔚 Argent Omega for SNMP	Retrieve Performance Data For Argent Forecaster Only
SNMP Rules	Test Ping Blast Packet Latency
SNMP Trap Rules	Test Port In Mbps
👻 🔛 DeviceMagic Port Rules	Test Port Out Mbps
DPT_PORT_COMPREHENSIVE	
DPT_PORT_DOWN	Test Port In/Out Mbps
DPT_PORT_MBPS_PREDICTOR_ONLY	Only Test Ports Matching Criteria
DPT_PORT_PACKET_LATENCY	- Ping Blast Parameters
DPT_PORT_PACKET_LOSS	
DPT_PORT_STATUS	Ping Requests To Send: 10
DPT_PORT_STATUS_CHANGED	Send Buffer Size: 32 🗘 Bytes
DPT_TEST	Time To Live (TTL): 64 Seconds
LINK Connectivity Rules	Time to Live (TL): 64 → Seconds
Device Configuration Rules	
🕨 📁 CISCO VPN Tunnel Rules	Fail Rule If Data Is Not Available Or Nonexistent
CISCO Remote Access Rules	Save Performance Data To The Argent Forecaster Using Data Store: (default)

Argent Software Proprietary Information – All Rights Reserved The following is an example of the Rule result:

■ ARGENT OMEG		N2S
Windows Program Rules	Do Ping Test On Device	F
Windows Performance Rules	be pring resc on Device	
PowerShell Script Rules	Do Ping Test On Connected Neighbors	
🕨 🕍 WMI Script Rules	Re Test Rule ×	
LINUX Script Rules	Re For Argent Instant Help 7 by 24 with an Argent engineer, please see http://bein.Argent.com/bein.php	
 UNIX Script Rules 		
🕨 🖬 Solaris	Te la	
▶ 🖬 AIX		
▶ 🖬 HP-UX	Target Machine: 192.168.96.55	
> 🖬 sco	Test At: AI-2019-009	
Argent Compliance Automator	Test Time: Tue, 26 Jul 2022 04:56:35 (UTC)	
🕨 🔚 Argent Omega Web Defender		
🕨 🔚 Argent Omega for Microsoft 365	Rule is Not Broken	
👻 🕍 Argent Omega for SNMP		
🕨 🔚 SNMP Rules	Te Argent Forecaster Data	
🕨 🔚 SNMP Trap Rules	2022-07-26 04:55:40 (UTC): \\192.168.96.55\Service Level Agreement(192.168.96.55)\Ping Loss % = 0.00	
🔻 🔚 DeviceMagic Port Rules		
DPT_PORT_COMPREHENSIVE	Te	
DPT_PORT_DOWN	Te First Time checking switch ports Successfully Pinged 192.168.96.55	
DPT_PORT_MBPS_PREDICTOR_ONLY	On Sent 10 ping requests	
DPT_PORT_PACKET_LATENCY	Ping Blast: 10/0 (Success/Failure) Ping Blast: 10/0 (Success/Failure)	
DPT_PORT_PACKET_LOSS		
DPT_PORT_STATUS	Print Close	
DPT_PORT_STATUS_CHANGED		
DPT_TEST		
🕨 🕍 LINK Connectivity Rules	Time To Live (TTL): 64 Seconds	
Device Configuration Rules		
CISCO VPN Tunnel Rules	Fail Rule If Data Is Not Available Or Nonexistent	
CISCO Remote Access Rules	Save Performance Data To The Argent Forecaster Using Data Store: (default)	
N See Canadia VIDN Bulan	Tao 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.

■ ARGENT OME	GA (2.2A-2207-A) GA (2.2A-2207-A) Home Theme Argent Instant Help About Logout
▼ 🐸 Tool Sets	Do Ping Test On Device
🕨 🚧 Argent Omega Baseline	
Argent Compliance Automator	Do Ping Test On Connected Neighbors
🕨 🕍 Argent Omega Web Defender	Report Down Switch Ports
🕨 🚞 Argent Omega for Microsoft 365	Report Switch Port When Status Changes
🔻 🔚 Argent Omega for SNMP	Test Ping Blast Packet Loss
SNMP Rules	
SNMP Trap Rules	Test Ping Blast Packet Latency
▼ Image: Port Rules	Acceptable Limit Value: 100 C ms
DPT_PORT_COMPREHENSIVE	Approaching Limit Value: 300 🗧 ms
DPT_PORT_DOWN	A Limit Value: 20 ms
DPT_PORT_MBPS_PREDICTOR_ONLY	Exceeding Limit Value: 800 ms
DPT_PORT_PACKET_LATENCY	
DPT_PORT_PACKET_LOSS	Major Overload Value: 1,000 🗘 ms
DPT_PORT_STATUS	Retrieve Performance Data For Argent Forecaster Only
DPT_PORT_STATUS_CHANGED	Test Port In Mbps
DPT_TEST	Test Port Out Mbps
LINK Connectivity Rules	Test Port In/Out Mbps
Device Configuration Rules	
CISCO VPN Tunnel Rules	Only Test Ports Matching Criteria
CISCO Remote Access Rules	Ping Blast Parameters
🕨 🔚 Generic VPN Rules	Ping Requests To Send:
PowerShell Script Rules	
Argent Omega for SQL Server	Send Buffer Size: 32 Bytes
✓ Interval Alerts	Time To Live (TTL): 64 👶 Seconds
Correction	
Motification	Fail Rule If Data Is Not Available Or Nonexistent
🕨 🚞 Alert Macro	Save Performance Data To The Argent Forecaster Using Data Store: {default}
Monitoring Groups	Tag 1:

The following is an example of the Rule result:

■ ARGENT OMEG	A (2.2A-2207-A) C [®] O Home Theme → Argent Instant Help About Lo	SN2S ogout
▼ 🕍 Tool Sets 📥	Do Ping Test On Device	
🕨 🕍 Argent Omega Baseline		
Argent Compliance Automator	Do Ping Test On Connected Neighbors	
🕨 🕍 Argent Omega Web Defender	Re Test Rule X	
🕨 🕍 Argent Omega for Microsoft 365	Re Argent Omega 2.2.2207.21 Copyright (c) 2022 Argent Software	
👻 🔚 Argent Omega for SNMP	For Argent Instant Help 7 by 24 with an Argent engineer, please see http://help.Argent.com/help.php	
SNMP Rules		
🕨 📶 SNMP Trap Rules	Te	
🔻 📶 DeviceMagic Port Rules	Target Machine: 192.168.96.55	
DPT_PORT_COMPREHENSIVE		
DPT_PORT_DOWN	Test At: AI-2019-009	
DPT_PORT_MBPS_PREDICTOR_ONLY	Test Time: Tue, 26 Jul 2022 05:03:02 (UTC)	
DPT_PORT_PACKET_LATENCY	*** Rule is Broken ***	
DPT_PORT_PACKET_LOSS	Summary: Ping Blast Packet Latency At Limit (> 20%)	
DPT_PORT_STATUS	Detail: Ping Blast Packet Latency = 46.00 ms (> 20) - At Limit Severity: At Limit	
DPT_PORT_STATUS_CHANGED	Te	
DPT_TEST	Te Trace Information	
🕨 🔚 LINK Connectivity Rules	First Time checking switch ports	
Device Configuration Rules	Te Successfully Pinged 192.168.96.55 Sent 10 ping requests	
Fill CISCO VPN Tunnel Rules	On Ping Blast: 10/0 (Success/Failure)	
🕨 🔚 CISCO Remote Access Rules		
🕨 🕍 Generic VPN Rules	Print Close	
🕨 🕍 PowerShell Script Rules	PINK	
🕨 🔚 Argent Omega for SQL Server		
🕶 🕍 Alerts	Time To Live (TTL): 64 🗯 Seconds	
> 🔚 Correction		
Notification	Fail Rule If Data Is Not Available Or Nonexistent	
▶ 🔛 Alert Macro	Save Performance Data To The Argent Forecaster Using Data Store:	
Monitoring Groups	Taq 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.

■ ARGENT OME	GA (2.2A-2207-A)		🔅 🕻 🆓 eme - Argent Instan	? t Help About	U Logout	SN2S
WMI Script Rules	Do Ping Test On Device					
LINUX Script Rules	Do Ping Test On Connected Neighbors					
👻 🔛 UNIX Script Rules	Report Down Switch Ports					
🕨 🚾 Solaris						
AIX	Report Switch Port When Status Changes					
▶ 🔚 HP-UX	Test Ping Blast Packet Loss					
▶ 🖬 sco	Test Ping Blast Packet Latency					
Argent Compliance Automator	Test Port In Mbps					
🕨 🚧 Argent Omega Web Defender						
Argent Omega for Microsoft 365	Test Port Out Mbps					
Argent Omega for SNMP	Test Port In/Out Mbps					
SNMP Rules	Only Test Ports Matching Criteria 🛛 Port Name	✓ Matches	~ Ⅰ	FINDEX#8		
SNMP Trap Rules	Fail Rule If Data Is Not Available Or Nonexistent		A			
▼ MoviceMagic Port Rules	Save Performance Data To The Argent Forecaster Using Data Store:	ult)	_			
DPT_PORT_COMPREHENSIVE	Tag 1:	uicy	· · · ·			
DPT_PORT_DOWN	Taq 2:					
DPT_PORT_MBPS_PREDICTOR_ONLY						
DPT_PORT_PACKET_LATENCY DPT_PORT_PACKET_LOSS	Tag 3:					
DPT_PORT_STATUS	Post Event Even If The Same Event Is Still Outstanding (Unanswered)					
DPT_PORT_STATUS_CHANGED	Do So Only After 1 Hour 0 Minute Since Event Is Post					
	Ignore The Same Outstanding Event If Alerts Were Fired More Than	🗧 Hour 🛛 🗯 Mini	ute Ago			
LINK Connectivity Rules	Post Event Only After Rule Is Broken 2 Cr More Times					
🕨 🚞 Device Configuration Rules	Reset Counter					
🕨 🛀 CISCO VPN Tunnel Rules	After Event Is Post					
CISCO Remote Access Rules	After Event Is Answered					
🕨 🚞 Generic VPN Rules	After The Actual Condition Is Corrected					
PowerShell Script Rules						
Argent Omega for SOL Server	Application:					

The following is an example of the Rule result:

= ARGENT OME	∧ * * ° 0 0
- ARGENT OWE	UA (2.2A-2207-A) Home Theme + Argent Instant Help About Logout
WMI Script Rules	Do Ping Test On Device Test Rule X
ILINUX Script Rules	Do Ping Test On Connected Neighbors Fest At: 2019-009
✓ III UNIX Script Rules	
Solaris	Report Down Switch Ports Lest Time: Tue, 26 Jul 2022 05:23:10 (UTC)
▶ 🖬 AIX	Report Switch Port When Status Changes 🗧 *** Rule is Not Broken ***
🕨 🕍 HP-UX	Test Ping Blast Packet Loss
▶ 🕍 SCO	Test Ping Blast Packet Latency Trace Information
Argent Compliance Automator	First Time checking switch ports
🕨 🔚 Argent Omega Web Defender	Not supported vtpVLanTable for CISCO device '192.168.96.55'
Argent Omega for Microsoft 365	Test Port Out Mbps Successfully queried port status Failed to query port numbers
▼ 📶 Argent Omega for SNMP	Test Port In/Out Mbps Successfully connected to managed switch '192.168.96.55' and queried switch ports INORED IFINOEX#2. Port name: IFINOEX#2
SNMP Rules	IGNORED IFINDEX#3. Port name: IFINDEX#3 Only Test Ports Matching Criteria IGNORED IFINDEX#4. Port name: IFINDEX#4
SNMP Trap Rules	IGNORED IFINDEX#5. Port name: IFINDEX#5
▼ 📁 DeviceMagic Port Rules	IGNORED IFINDEX#7
DPT_PORT_COMPREHENSIVE	Save Performance Data To The Argent Force
DPT_PORT_DOWN	Tag 1: IGNORED IFINDEX#10. Port name: IFINDEX#10 IGNORED IFINDEX#11. Port name: IFINDEX#11
DPT_PORT_MBPS_PREDICTOR_ONLY	Tag 2: IGNORED IFINDEX=12. Port name: IFINDEX=13 IGNORED IFINDEX=13. Port name: IFINDEX=13
DPT_PORT_PACKET_LATENCY	Tag 3: IGNORED IFINDEX=14, 9 or name: IFINDEX=14
DPT_PORT_PACKET_LOSS	Post Event Event Is Still O
DPT_PORT_STATUS	Do So Only After 1 Hour
DPT_PORT_STATUS_CHANGED	Ignore The Same Outstanding Event If Alerts
E DPT_TEST	
LINK Connectivity Rules	Post Event Only After Rule Is Broken 2 C Or More Times
Device Configuration Rules	Reset Counter
CISCO VPN Tunnel Rules	After Event Is Post
CISCO Remote Access Rules	After Event Is Answered
Generic VPN Rules	After The Actual Condition Is Corrected
PowerShell Script Rules	Application:
Argent Omega for SOL Server	- Appreciation

LINK Connectivity Rules

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

■ ARGENT OME	GA (2.2A-2207-A) 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 Rules DeviceMagic Port Rules LINK_Connectivity Rules LINK_COSS_NEGENBOR LINK_LOSS_NEGENBOR LINK_NEW_LINK Device Configuration Rules CLSCO VPN Tunnel Rules	Rule Is Broken If Any Of Following Condition Is True Issee 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: Itag 1: Tag 1: Tag 2: Tag 3: Post Event Even If The Same Event Is Still Outstanding (Unanswered) Do So Only After Itag Inter Since Event Is Post Ignore The Same Outstanding Event If Alerts Were Fired More Than Itag Orier The Same Outstanding Event If Alerts Were Fired More Than
CISCO Remote Access Rules CISCO Remote Access Rules CISCO Remote Access Rules PowerShell Script Rules CISCO RULES CI	Post Event Only After Rule Is Broken 2 Or More Times Reset Counter After Event Is Post After Event Is Answered
Correction Motification Marco Monitoring Groups	After The Actual Condition Is Corrected Application: Reference URL:
 Relators Relators Email Recipients S SR Recipients Windows Services Windows Processes 	Console Comment: *** Neighbor Links Changed *** Description: Image: Console Block I Font Image: Console Block Font Full Screen 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.

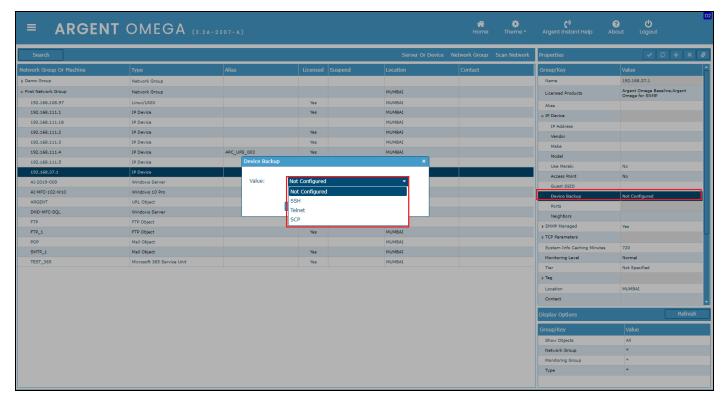
This facility uses the same mechanism to backup the device's configuration to the central Argent SQL

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.



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

≡ ARGEN					et Home	🔅 Theme -	ে) Argent Instant Help Abo		
Search				Ser	ver Or Device Network Group	Scan Network	Properties	✓ 3 +	×
etwork Group Or Machine	Туре	Alias	Licensed	Suspend Location	Contact		Group/Key	Value	
Demo Group	Network Group						Vendor		
First Network Group	Network Group			MUMBAI			Make		
192.168.108.97	Linux/UNIX		Yes	MUMBAI			Model		
192.168.111.1	IP Device		Yes	MUMBAI			Use Meraki	No	
192.168.111.18	IP Device			MUMBAI			Access Point	No	
192.168.111.2	IP Device		Yes	MUMBAI			Guest SSID		
192.168.111.3	IP Device		Yes	MUMBAI			✓ Device Backup	SSH	
192.168.111.4	IP Device	APC_UPS_003	Yes	MUMBAI			Authentication		
192.168.111.5	IP Device		Yes				Communication		
192.168.37.1	IP Device		Yes	MUMBAI			Keep Last Versions	10	
AI-2019-009	Windows Server		Yes	MUMBAI			Enter Key to Dismiss Banner		
AI-MFC-102-W10	Windows 10 Pro		Yes				Require Elevation	No	
ARGENT	URL Object		Yes	MUMBAI			Elevation Command		
DND-MFC-SQL	Windows Server		Yes	MUMBAI			Elevation Password		
FTP	FTP Object		Yes	MUMBAI			Paging-Off Command		
FTP_1	FTP Object		Yes	MUMBAI			Group 1		
POP	Mail Object			MUMBAI			▶ Group 2		
SMTP_1	Mail Object		Yes	MUMBAI			Group 3		
TEST_365	Microsoft 365 Service Unit		Yes	MUMBAI			Ports		
							Neighbors		
							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.

■ ARGENT OME	GA (2.2A-2207-			🚮 Home	🔅 Theme -	ে) Argent Instant Help	? About	ن Logout	SN6S
▼ Mol Sets	- Device Monitor Optio		1						
🕨 🖬 Argent Omega Baseline	- Device Monitor Optio	n							
Argent Compliance Automator	Backup Configuration	Only							
🕨 🕍 Argent Omega Web Defender	Backup Configuration	And Fire Event If Device Configuration Has Changed							
Argent Omega for Microsoft 365	_								
▼ I Argent Omega for SNMP	Command Response	Timeout: 3 Seconds	-						
SNMP Rules									
SNMP Trap Rules	Fail Rule If Failed To	Connect To Device		_					
DeviceMagic Port Rules	Save Performance D	ata To The Argent Forecaster Using Data Store: {defa							
LINK Connectivity Rules	Tag 1:								
	Tag 2:								
BCB_BACKUP_AND_DETECT_CHANGE	Tag 3:								
CB_BACKUP_ONLY	Best Event Even If T	ne Same Event Is Still Outstanding (Unanswered)							
CISCO VPN Tunnel Rules	_								
CISCO Remote Access Rules	Do So Only After								
Generic VPN Rules			🗧 Hour 🛛 0 🗘 Minute Ago						
PowerShell Script Rules	Post Event Only Afte	r Rule Is Broken 2 Cr More Times							
Argent Omega for SQL Server	Reset Counter								
✓ Intervention of the second seco	After Event Is Post								
Correction	After Event Is Answe	red							
Notification	After The Actual Con	dition Is Corrected							
Alert Macro									
Monitoring Groups	Application:								
Relators	Reference URL:								
▼ Macros	Console Comment:								
Email Recipients	console comment.	*** Backup Only ***							
SMS Recipients	Description:								
Windows Services Windows Processes	B Z U Format Block	▼ Font ▼ 17 ▼ A ▼ A ▼ E =	: = := := := = - • <i>I</i> _×						en
Windows Processes	This sample rule saves device	configuration to database							
Calendars									
Galendars Base Definitions									
Holidays									
r monuays									

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 OME	GA (2.2A-2207-A)	A 🔅 Home Theme	ে % e → Argent Instant Help	? ් About Logout	SN99
	Rule Is Broken If Any Of Following Condition Is True Active Tunnel Count Exceeds 10 Average In Bandwidth Usage Exceeds 100 Average Out Bandwidth Usage Exceeds 100 Average In Dandwidth Usage Exceeds 100 Average In Dandwidth Usage Exceeds 100 In Drop Packets Exceeds 100 In Drop Packets Exceeds 100 Packets/s 100				
 Envice Configuration Rules CISCO VPN Tunnel Rules 	Out Drop Packets Exceeds				
Clobal Statistics CISCO_TUNNEL_GLOBAL_BAD_CONNECTION GISCO_TUNNEL_GLOBAL_HIGH_VPN_DOWNL CISCO_TUNNEL_GLOBAL_HIGH_VPN_UPLOAL CISCO_TUNNEL_GLOBAL_TAT_PRD CISCO_TUNNEL_GLOBAL_TAT_PRD CISCO_TUNNEL_VPN_FROM_ALLOWED_LOCA GISCO_TUNNEL_VPN_FROM_ALLOWED_LOCA GISCO_TUNNEL_VPN_FROM_ALLOWED_LOCA GISCO_TUNNEL_VPN_ONE_TUNNEL_ONE_LO GISCO_TUNNEL_VPN_TUNNEL_CREATED GISCO_TUNNEL_VPN_TUNNEL_TERMINATED Peer Lost	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: Tag 1: Tag 2: Tag 3: Post Event Even If The Same Event Is Still Outstanding (Unanswered) Do So Only After Ignore The Same Outstanding Event If Alerts Were Fired More Than Ignore The Same Outstanding Event If Alerts Were Fired More Than Post Event Only After Rule Is Broken Q Or More Times	r 0 🗘 Minute	Ago		
CLSCO Remote Access Rules CLSCO Remote Access Rules Construction Rules PowerShell Script Rules Argent Omega for SQL Server	Reset Counter After Event Is Post After Event Is Answered After The Actual Condition Is Corrected				
✓ Alerts Main Correction	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	*	•	(°)	?		SN9S
■ ARGENT OMEGA		Theme - A	rgent Instant Help	About	Logout	
▶ 🖬 Argent Compliance Automator	Rule Is Broken If Any Of Following Condition Is True					
🕨 🕍 Argent Omega Web Defender	Active Tunnel Count Exceeds					
Argent Omega for Microsoft 365						
🔻 🔚 Argent Omega for SNMP	Average In Bandwidth Usage Exceeds					
SNMP Rules	Average Out Bandwidth Usage Exceeds 100 🗘 Megabits/s					
SNMP Trap Rules	Average In/Out Bandwidth Usage Exceeds 100 🔵 Megabits/s					
DeviceMagic Port Rules	In Drop Packets Exceeds					
LINK Connectivity Rules						
Device Configuration Rules	Out Drop Packets Exceeds 10 CPackets/s					
▼ 🖬 CISCO VPN Tunnel Rules						
👻 🔚 Global Statistics	Retrieve Performance Data For Argent Forecaster Only					
<pre>@ CISCO_TUNNEL_GLOBAL_BAD_CONNECTIONS</pre>	Fail Rule If Data Is Not Available Or Nonexistent					
CISCO_TUNNEL_GLOBAL_HIGH_VPN_DOWNLOAD	Save Performance Data To The Argent Forecaster Using Data Store: {default}		_			
CISCO_TUNNEL_GLOBAL_HIGH_VPN_UPLOAD	Taq 1:		· ·			
CISCO_TUNNEL_GLOBAL_STAT_PRD						
CISCO_TUNNEL_GLOBAL_TOO_MANY_TUNNELS	Tag 2:					
👻 🛀 VPN Tunnel Activity	Tag 3:					
CISCO_TUNNEL_VPN_FROM_ALLOWED_LOCATIONS	Post Event Even If The Same Event Is Still Outstanding (Unanswered)					
<pre> @ CISCO_TUNNEL_VPN_ONE_TUNNEL_ONE_LOCATION </pre>	Do So Only After 1 Hour 0 Minute Since Event Is Post					
<pre> @ CISCO_TUNNEL_VPN_TUNNEL_CREATED</pre>	Iqnore The Same Outstanding Event If Alerts Were Fired More Than	0 📄 Minute A	100			
CISCO_TUNNEL_VPN_TUNNEL_TERMINATED			-go			
🕨 🔛 Peer Lost	Post Event Only After Rule Is Broken 2 Or More Times					
CISCO Remote Access Rules	Reset Counter					
🕨 🚞 Generic VPN Rules	After Event Is Post					
🕨 🚞 PowerShell Script Rules	After Event Is Answered					
Argent Omega for SQL Server	After The Actual Condition Is Corrected					
👻 📶 Alerts	Application:					
Correction						
<	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 OME	GA (2.2A-2207-A)	Home	🔅 Theme -	्र्" Argent Instant Help	? About	ڻ Logout	517
	Rule Is Broken If Any Of Following Condition Is True Active Tunnel Count Exceeds VPN Connection Comes From Locations Not Allowed: 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						
CISCO_TOWNEL_VEN_TOWNEL_TEXHINATE Market CISCO Remote Access Rules Generic VPN Rules Generic VPN Rules Argent Omega for SQL Server Argent Access Rules	Ignore The Same Outstanding Event If Alerts Were Fired More Than Post Event Only After Rule Is Broken Reset Counter After Event Is Post After Event Is Answered After The Actual Condition Is Corrected	ır (Minute Ago				
Monitoring Groups							

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.

■ ARGENT OME	GA (2.2A-2207-A) About Logout
🔻 🔚 Tool Sets	Rule Is Broken If Peer Lost Failures Exceed 10 🔵 In Past 5 🍃 Minutes
🕨 🔚 Argent Omega Baseline	
Argent Compliance Automator	Fail Rule If Data Is Not Available Or Nonexistent
🕨 🔚 Argent Omega Web Defender	Save Performance Data To The Argent Forecaster Using Data Store: (default)
🕨 🚧 Argent Omega for Microsoft 365	Tag 1:
🔻 🔚 Argent Omega for SNMP	Tag 2:
SNMP Rules	Tag 3:
SNMP Trap Rules	Post Event Even If The Same Event Is Still Outstanding (Unanswered)
DeviceMagic Port Rules	Do So Only After 1 Hour 0 Minute Since Event Is Post
LINK Connectivity Rules	
Device Configuration Rules	Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
👻 🔚 CISCO VPN Tunnel Rules	Post Event Only After Rule Is Broken 2 🗘 Or More Times
Global Statistics	Reset Counter
VPN Tunnel Activity	● After Event Is Post
👻 🚧 Peer Lost	After Event Is Answered
<pre>(@) CISCO_TUNNEL_PEER_LOST_SPIKE</pre>	After The Actual Condition Is Corrected
CISCO Remote Access Rules	
Generic VPN Rules	Application:
PowerShell Script Rules	Reference URL:
Argent Omega for SQL Server	Console Comment:
Alerts	Console Comment: === VPN Peer Lost Spike ===
Monitoring Groups	Description:
Relators	B Z U Format Block ▼ Font ▼ T ▼ ▲ ▼ S ▼ S = E I I I I I I I I I I I I I I I I I I
▼ 📶 Macros	This sample Rule detects spike of VPN peer-lost failure
🕨 🖬 Email Recipients	
SMS Recipients	
Windows Services	
Windows Processes	
▶ 🚰 Users	

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

■ ARGENT OME	GA (2.2A-2207-A) GA (2.2A-2207-A) Home Theme - Argent Instant Help About Logout
▶ 📶 HP-UX	
▶ FI SCO	Rule Is Broken If Any Of Following Condition Is True
Argent Compliance Automator	CActive Session Count Exceeds 100 🗣
Argent Omega Web Defender	Average In Bandwidth Usage Exceeds 100 C Megabits/s
Argent Omega for Microsoft 365	Average Out Bandwidth Usage Exceeds 100 Regabits/s
SNMP Rules	Average In/Out Bandwidth Usage Exceeds 100 🗧 Megabits/s
SNMP Trap Rules	In Drop Packets Exceeds 100 C Packets/s
🕨 🚞 DeviceMagic Port Rules	Out Drop Packets Exceeds 100 P Packets/s
🕨 🚞 LINK Connectivity Rules	
🕨 🚞 Device Configuration Rules	Retrieve Performance Data For Argent Forecaster Only
File CISCO VPN Tunnel Rules	
✓	Fail Rule If Data Is Not Available Or Nonexistent
👻 🔚 Global Statistics	Save Performance Data To The Argent Forecaster Using Data Store: {default}
PCISCO_RA_GLOBAL_BAD_VPN_CONNECTI	Tag 1:
PCISCO_RA_GLOBAL_HIGH_VPN_DOWNLO	Tag 2:
PCISCO_RA_GLOBAL_HIGH_VPN_UPLOAD	Tag 3:
P CISCO_RA_GLOBAL_STAT_PRD	Post Event Even If The Same Event Is Still Outstanding (Unanswered)
	Do So Only After 1 Hour 0 Minute Since Event Is Post
Remote Access Activity	
🕨 📶 Logon Failure	Ignore The Same Outstanding Event If Alerts Were Fired More Than
Fiel Generic VPN Rules	Post Event Only After Rule Is Broken 2 🕒 Or More Times
PowerShell Script Rules	Reset Counter
Argent Omega for SQL Server	After Event Is Post
▼ 📶 Alerts	After Event Is Answered
Correction	After The Actual Condition Is Corrected
Motification	
▶ 🗀 Alert Macro	Application:
🕨 📶 Monitoring Groups 🗸 🗸	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 OME	GA (2.2A-2207-A) Successfully Updated CISCO VPN Activity Rule: Home Theme* August Instant Traps August Instant Traps August Instant Traps August Instant Traps August
HP-UX Marcology Gradient Compliance Automator Argent Omega Web Defender Margent Omega for Microsoft 365 Margent Omega for SNMP	Rule Is Broken If Any Of Following Condition Is True Incoming Bandwidth Usage Exceeds 100 C Megabits/s In/Out Bandwidth Usage Exceeds 100 C Megabits/s In/Out Bandwidth Usage Exceeds 100 C Megabits/s
Argenic Unlegg for SNMP Argenic Unlegg for SNMP SNMP Rules SNMP Trap Rules DeviceMagic Port Rules SNL LINK Connectivity Rules	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: •
CISCO_VPN_USER_HIGH_BANDWIDTH_USAC CISCO_VPN_USER_LONG_DURATION CISCO_VPN_USER_ONE_USER_ONE_LOCATIO CISCO_VPN_USER_ONE_USER_ONE_LOCATIO CIGCO_VPN_USER_ONE_USE CIGCO_VPN_USES CIGCO_VPN_USES CIGCO_VPN_USES CIGCO_VPN_USES CIGCO_V	Tag 2: Tag 3: Post Event Even If The Same Event Is Still Outstanding (Unanswered) Do So Only After 1 C Hour 0 C Minute Same Outstanding Event If Alerts Were Fired More Than 1 C Post Event Only After Rule Is Broken 2 C Or More Times
Argent Omega for SQL Server Alerts Correction Notification Alert Macro Alert Macro	Reset Counter

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.

= ARGENT OME	GA (2.2A-2207-A) Home Theme Argent Instant Help About Logout
▶ 🔛 HP-UX	- Rule Is Broken If Any Of Following Condition Is True
▶ 🖬 sco	Incoming Bandwidth Usage Exceeds 100 Megabits/s
Argent Compliance Automator	
🕨 🚧 Argent Omega Web Defender	Outgoing Bandwidth Usage Exceeds 100 🖗 Megabits/s
Argent Omega for Microsoft 365	In/Out Bandwidth Usage Exceeds
👻 🚧 Argent Omega for SNMP	Session Duration Exceeds: 01:00:00
SNMP Rules	VPN Connection Comes From Locations Not Allowed: MUMBAI
SNMP Trap Rules	
DeviceMagic Port Rules	Multiple VPN Connections Come From Same IP Address
LINK Connectivity Rules	VPN User: Matches
Device Configuration Rules	
CISCO VPN Tunnel Rules	Client Vendor String: Matches -
CISCO Remote Access Rules	Retrieve Performance Data For Argent Forecaster Only
Global Statistics	Fail Rule If Data Is Not Available Or Nonexistent
Remote Access Activity	Save Performance Data To The Argent Forecaster Using Data Store: {default}
CISCO_VPN_USER_ARCHIVE_ONLY	Tag 1:
<pre>CISCO_VPN_USER_FROM_ALLOWED_LOCATI </pre>	Tag 2:
<pre>EXAMPLE CISCO_VPN_USER_HIGH_BANDWIDTH_USAG</pre>	Tag 3:
CISCO_VPN_USER_LONG_DURATION	
CISCO_VPN_USER_ONE_USER_ONE_LOCATION	Post Event Even If The Same Event Is Still Outstanding (Unanswered)
Generic VPN Rules	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
PowerShell Script Rules Margent Omega for SQL Server	Post Event Only After Rule Is Broken 2 🗘 Or More Times
Algent Onlega for SQL Server	- Reset Counter -
Alerts Correction	After Event Is Post
Notification	After Event Is Answered
Alert Macro	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.

■ ARGENT ON	EGA (2.2A-2207-A)
🕨 🖬 HP-UX	🔓 Rule Is Broken If Logon Failures Exceed 30 💭 In Past 5 💭 Minutes
🕨 🚾 SCO	Fail Rule If Data Is Not Available Or Nonexistent
Argent Compliance Automator	
🕨 🚞 Argent Omega Web Defender	Save Performance Data To The Argent Forecaster Using Data Store: (default)
🕨 🚧 Argent Omega for Microsoft 365	Tag 1:
🔻 🚧 Argent Omega for SNMP	Tag 2:
SNMP Rules	Tag 3:
🕨 📒 SNMP Trap Rules	Post Event Even If The Same Event Is Still Outstanding (Unanswered)
🕨 🔚 DeviceMagic Port Rules	Do So Only After 1 Hour 0 Minute Since Event Is Post
LINK Connectivity Rules	I gnore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago
Device Configuration Rules	
CISCO VPN Tunnel Rules	Post Event Only After Rule Is Broken 2 🗘 Or More Times
👻 🔚 CISCO Remote Access Rules	Reset Counter
Global Statistics	After Event Is Post
Remote Access Activity	After Event Is Answered
👻 🔚 Logon Failure	After The Actual Condition Is Corrected
CISCO_RA_BAD_AUTH_SPIKE	Application:
Control of the target PowerShell Script Rules	Reference URL:
Argent Omega for SQL Server	
Algent official of SQL Server	Console Comment: VPN Authentication Failure Spike
Correction	Description:
Notification	BZU Format Block ▼ Font ▼
Alert Macro	This sample Rule detects spike of VPN authetication failure spike
Monitoring Groups	
Relators	
▼ 📶 Macros	
Email Recipients	
SMS Recipients	

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

	2.2A-2207-A) Annu Annu Annu Annu Annu Annu Annu An
▼ 🔚 Tool Sets	Device Vendor: SonicWall
🕨 🚞 Argent Omega Baseline	Rule Is Broken If Any Of Following Condition Is True
Argent Compliance Automator	
🕨 🚧 Argent Omega Web Defender	Active Tunnel Count Exceeds 100 💭
Argent Omega for Microsoft 365	Average In Bandwidth Usage Exceeds 100 🗘 Megabits/s
🔻 🔚 Argent Omega for SNMP	Average Out Bandwidth Usage Exceeds 100 🚔 Megabits/s
SNMP Rules	
SNMP Trap Rules	Average In/Out Bandwidth Usage Exceeds 100 Megabits/s
DeviceMagic Port Rules	VPN Connection Comes From Locations Not Allowed: Please Choose:
LINK Connectivity Rules	Multiple VPN Connections Come From Same IP Address
Device Configuration Rules	New VPN Tunnel Is Established
CISCO VPN Tunnel Rules	_
Fill CISCO Remote Access Rules	VPN Tunnel Has Been Terminated
🔻 🚞 Generic VPN Rules	
CheckPoint	Retrieve Performance Data For Argent Forecaster Only
🕨 🖬 Fortinet	Fail Rule If Data Is Not Available Or Nonexistent
🕨 🖬 Juniper	Save Performance Data To The Argent Forecaster Using Data Store: (default)
🔻 📶 SonicWall	Tag 1:
VPN_SONICWALL_FROM_ALLOWED_LOCATIONS	Tag 2:
VPN_SONICWALL_HIGH_BANDWIDTH_USAGE	Taq 3:
VPN_SONICWALL_ONE_USER_ONE_LOCATION	
VPN_SONICWALL_SESSION_TOTAL	Post Event Even If The Same Event Is Still Outstanding (Unanswered)
VPN_SONICWALL_TUNNEL_CREATED	Do So Only After 1 🕞 Hour 0 💭 Minute Since Event Is Post
VPN_SONICWALL_TUNNEL_TERMINATED	Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 🗘 Hour 0 🗘 Minute Ago
🕨 🖬 Zyxel	Post Event Only After Rule Is Broken 2 🗘 Or More Times
PowerShell Script Rules	- Reset Counter -
Argent Omega for SQL Server	Asset Control
👻 🔚 Alerts	After Event Is Answered
Correction	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

■ ARGENT OMEGA	SMI ش کې (۴) کې کې ال (2.2.4 - 22.0.7 - ۸) Home Theme - Argent Instant Help About Logout
 Argent Omega for Shift SNMP Rules SNMP Trap Rules DeviceMagic Port Rules Device Configuration Rules CLISCO VPN Tunnel Rules CLISCO VPN Tunnel Rules CLISCO VPN Rules CLISCO Commot Access Rules CLISCO COMPUTATION Rules CLISCO COMPUTATION Rules CLISCO COMPUTATION Rules PowerShell Script Rules PS_GET_SYSDESCR Argent Omega for SQL Server Alerts Correction Notification Alert Macro Relators Macros SMS Recipients SMS Recipients Windows Processes Windows Processes Clendars Base Definitions 	Add Parameters Properties Methods 1 \$protolid = "1.3.6.1.2.1.2.2.1.1" 2 \$prop = \$psplayer.detSompContext() 3 \$thisdid = \$protolid 9 \$protolid = "1.3.6.1.2.1.2.2.1.1" 1 \$protolid = "1.3.6.1.2.1.2.2.1.1" 2 \$protolid = "1.3.6.1.2.1.2.2.1.1" 3 \$protolid = "1.3.6.1.2.1.2.2.1.1" 1 \$protolid = "1.3.6.1.2.1.2.2.1.1" 2 \$protolid = "1.3.6.1.2.1.2.2.1.1" 1 \$protolid = "1.3.6.1.2.1.2.1.2.1.1.1" 1 \$protolid = "1.3.6.1.2.1.2.2.1.1.1" 1 \$protolid = \$protolid 1 \$protolid = \$protolid 2 \$protolid = \$protolid 3 \$protolid = \$protolid \$protolid 3 \$protolid = \$protolid \$protolid \$protolid 3 \$protolid = \$protolid \$protolid \$protolid 3 \$protolid = \$protolid \$protolid \$protolid \$protolid 3 \$protolid = \$protolid \$pro
Holidays Administration	Timeout: 30 Seconds

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

■ ARGENT OMEGA	2.2A-2207-A) Home Theme Argent Instant Help About Logout
Argen Conego to Shift Argen Conego to Shift SIMP Tap Rules Solution DeviceMagic Port Rules Device Configuration Rules CISCO VPN Tunnel Rules CISCO VPN Tunnel Rules CISCO VPN Rules CISCO Remote Access Rules CISCO PowerShell Script Rules PowerShell Script Rules Pos_GET_SYSDESCR Argent Omega for SQL Server Alerts Monitoring Groups Relators Monitoring Groups Relators Macros Macros Macros More Services	Add Parameters Properties Methods 1 \$snmp = \$F\$Player.detSmpContext() 2 \$succes + \$snmp.detSingleValue("1.3.6.1.2.1.1.1.0", \$false, \$false) 4 if (\$succes) { 5 \$ff[\$succes) { 6 \$F\$Player.MriteStatus("SysDescr Value = " + \$snmp.Value) 7 } 8 \$ff[\$succes) { 9 \$F\$Player.MriteStatus("Failed to query OID") 10 } \$seconds Rule Is Broken If Script Timeout \$save Performance Data To The Argent Forecaster Using Data Store: 7 ag 1:
 Windows Processes Users Calendars Base Definitions Holidays Administration License (Admin Only) 	After Event Is Post After Event Is Answered After The Actual Condition Is Corrected Application: Reference URL:

Argent_Omega_for_SNMP.doc