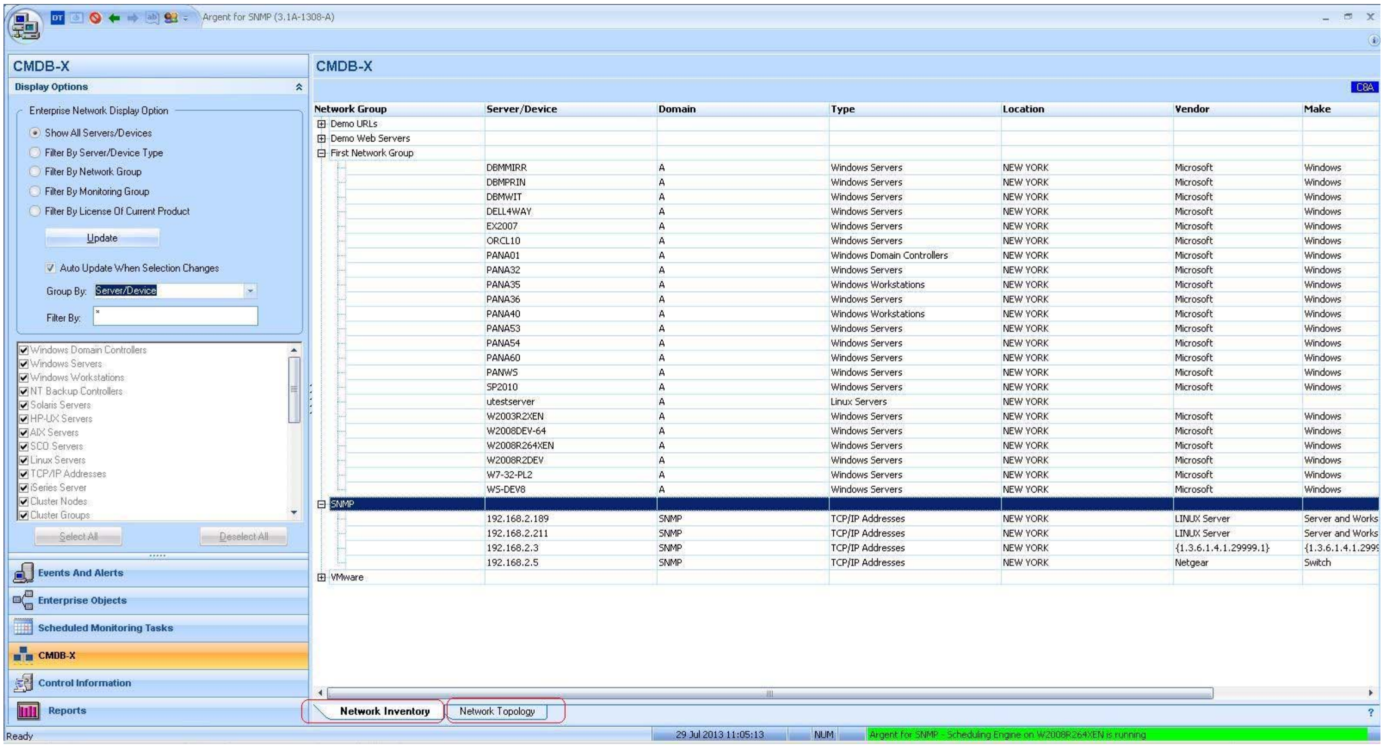
ARGENT

Argent Atlas Secrets

Argent Atlas is Argent's open CMDB-X database that is not only a network inventory but also the modeling product for both network topology and infrastructure dependency.

The network inventory stores nodal information that can be shared among all Argent AT products, as well as third-party products.

The network topology is useful for root cause analysis.



Argent for SNMP (3.1A-1308-A)

Enterprise Network Display Option

● Show All Servers/Devices

○ Filter By Server/Device Type

○ Filter By Network Group

○ Filter By Monitoring Group

○ Filter By License Of Current Product

☑ Auto Update When Selection Changes

Group By: Server/Device

Filter By: *

☑ Windows Domain Controllers
☑ Windows Servers
☑ Windows Workstations
☑ NT Backup Controllers
☑ Solaris Servers
☑ HP-UX Servers
☑ AIX Servers
☑ SCO Servers
☑ Linux Servers
☑ TCP/IP Addresses
☑ iSeries Server
☑ Cluster Nodes
☑ Cluster Groups

Network Group	Server/Device	Domain	Type	Location	Vendor	Make
⊞ Demo URLs						
⊞ Demo Web Servers						
⊟ First Network Group						
	DBMMIRR	A	Windows Servers	NEW YORK	Microsoft	Windows
	DBMPRIN	A	Windows Servers	NEW YORK	Microsoft	Windows
	DBMWIT	A	Windows Servers	NEW YORK	Microsoft	Windows
	DELL4WAY	A	Windows Servers	NEW YORK	Microsoft	Windows
	EX2007	A	Windows Servers	NEW YORK	Microsoft	Windows
	ORCL10	A	Windows Servers	NEW YORK	Microsoft	Windows
	PANA01	A	Windows Domain Controllers	NEW YORK	Microsoft	Windows
	PANA32	A	Windows Servers	NEW YORK	Microsoft	Windows
	PANA35	A	Windows Workstations	NEW YORK	Microsoft	Windows
	PANA36	A	Windows Servers	NEW YORK	Microsoft	Windows
	PANA40	A	Windows Workstations	NEW YORK	Microsoft	Windows
	PANA53	A	Windows Servers	NEW YORK	Microsoft	Windows
	PANA54	A	Windows Servers	NEW YORK	Microsoft	Windows
	PANA60	A	Windows Servers	NEW YORK	Microsoft	Windows
	PANWS	A	Windows Servers	NEW YORK	Microsoft	Windows
	SP2010	A	Windows Servers	NEW YORK	Microsoft	Windows
	utestserver	A	Linux Servers	NEW YORK		
	W2003R2XEN	A	Windows Servers	NEW YORK	Microsoft	Windows
	W2008DEV-64	A	Windows Servers	NEW YORK	Microsoft	Windows
	W2008R264XEN	A	Windows Servers	NEW YORK	Microsoft	Windows
	W2008R2DEV	A	Windows Servers	NEW YORK	Microsoft	Windows
	W7-32-PL2	A	Windows Servers	NEW YORK	Microsoft	Windows
	WS-DEV8	A	Windows Servers	NEW YORK	Microsoft	Windows
⊟ SNMP						
	192.168.2.189	SNMP	TCP/IP Addresses	NEW YORK	LINUX Server	Server and Works
	192.168.2.211	SNMP	TCP/IP Addresses	NEW YORK	LINUX Server	Server and Works
	192.168.2.3	SNMP	TCP/IP Addresses	NEW YORK	{1.3.6.1.4.1.29999.1}	{1.3.6.1.4.1.2999
	192.168.2.5	SNMP	TCP/IP Addresses	NEW YORK	Netgear	Switch
⊞ VMware						

29 Jul 2013 11:05:13

Argent for SNMP - Scheduling Engine on W2008R264XEN is running

Here are some common chores that Argent Atlas can automate:

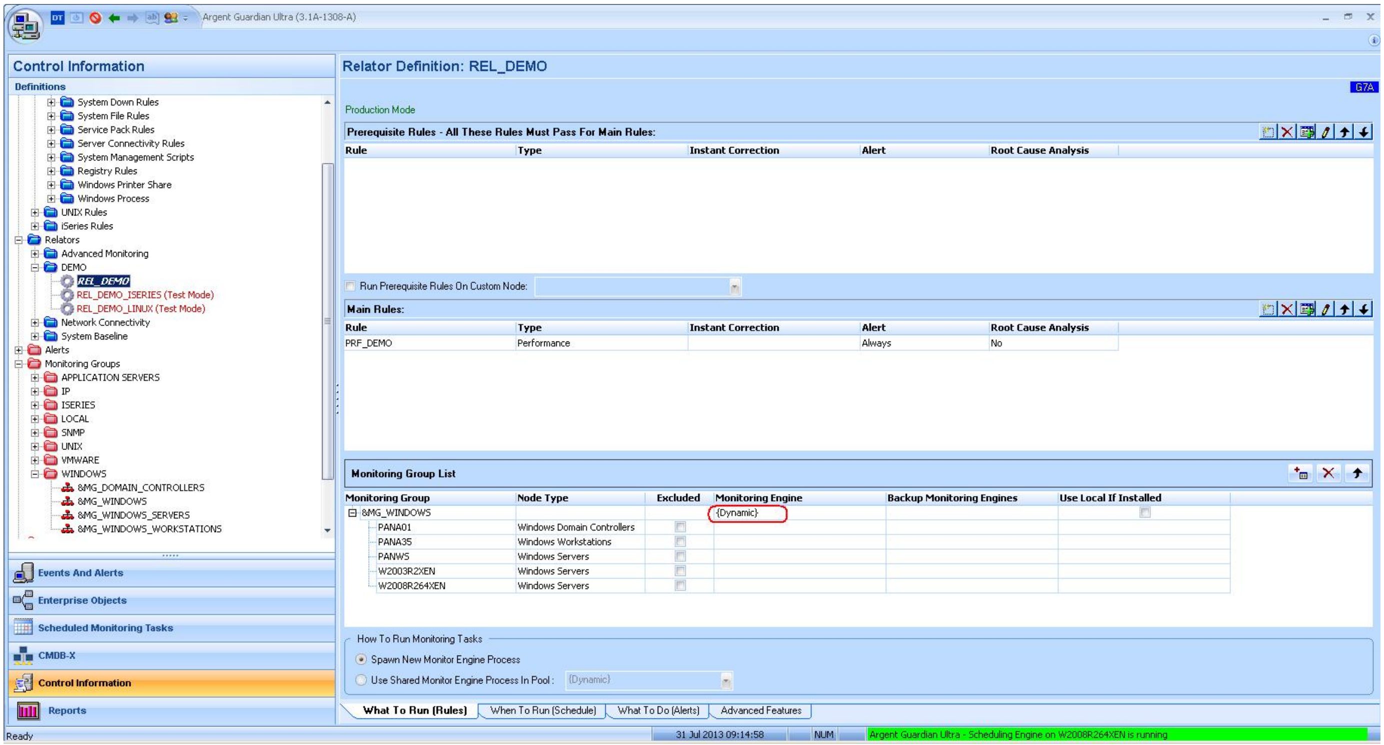
- Automated application monitoring using CLI and Argent AT maintenance scripts
- Detect newly installed SQL Servers
- Notify the changes of Exchange infrastructure
- Alert on installation of rogue SMTP services
- Maintain a master network inventory of Linux/Unix servers
- Bulk import IP addresses for the entire network
- Use third-party data source as data feed for Argent Atlas
- Implement third-party GUI and Web Interface to manage Argent Atlas
- Pass network inventory information between separate network locations
- Determine how servers and devices are connected
- Discover SNMP devices and information of vendor, make, model, etc
- Find MAC addresses of connected wireless devices
- Manage Monitoring Groups used by Argent AT
- Manage license to all Argent AT products
- Manage all Argent AT services

How Do I Assign A Node To A Daughter Engine For Monitoring When {Dynamic} Monitoring Engine Is Used?

The Argent AT Engine determines which Supervising Engine to use to schedule a monitored task for a node by inspecting the associated Monitoring Engine in the Relator.

The controlling Supervising Engine for the Monitoring Engine will be responsible for monitoring the node.

By default, {Dynamic} monitoring engine is used.



Relator Definition: REL_DEMO

Production Mode

Prerequisite Rules - All These Rules Must Pass For Main Rules:

Rule	Type	Instant Correction	Alert	Root Cause Analysis

□ Run Prerequisite Rules On Custom Node:

Main Rules:

Rule	Type	Instant Correction	Alert	Root Cause Analysis
PRF_DEMO	Performance		Always	No

Monitoring Group List

Monitoring Group	Node Type	Excluded	Monitoring Engine	Backup Monitoring Engines	Use Local If Installed
⊟ &MG_WINDOWS			{Dynamic}		□
PANA01	Windows Domain Controllers	□			
PANA35	Windows Workstations	□			
PANWS	Windows Servers	□			
W2003R2XEN	Windows Servers	□			
W2008R264XEN	Windows Servers	□			

How To Run Monitoring Tasks

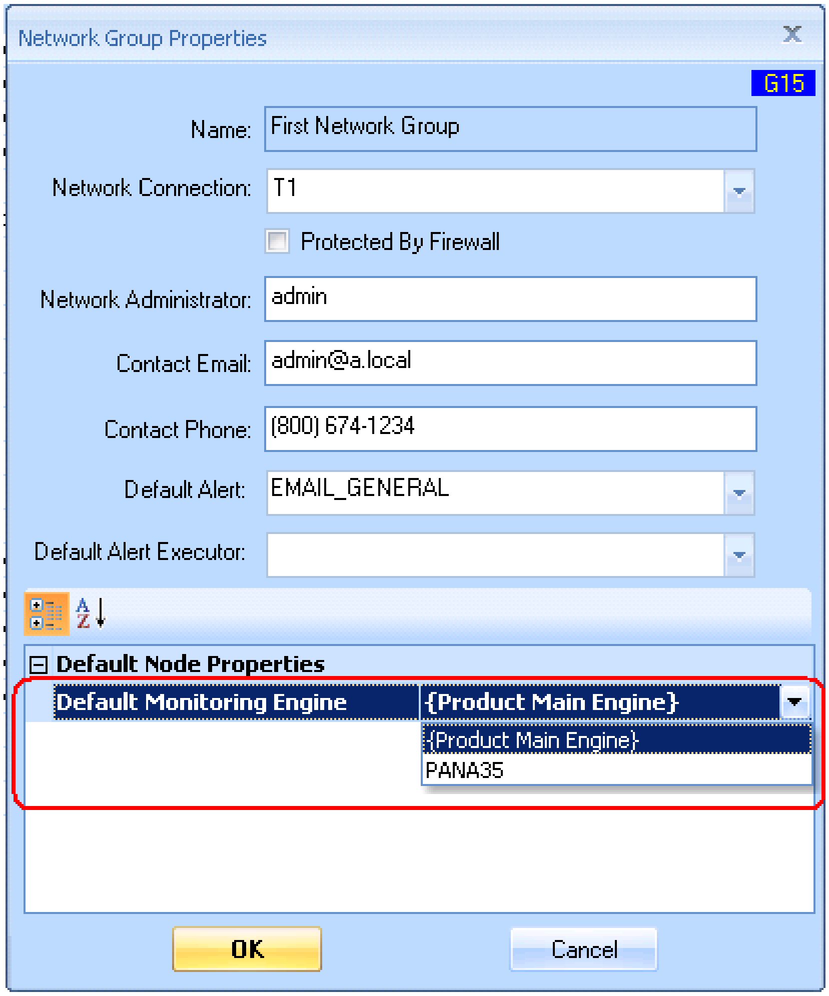
● Spawn New Monitor Engine Process

○ Use Shared Monitor Engine Process In Pool : {Dynamic}

Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

The Argent AT engine uses the following algorithm to determine which Supervising Engine to use:

- Find the Network Group a node belongs under
- Get the 'Default Monitoring Engine' for the Network Group
- Determine which Supervising Engine controls the Monitoring Engine, and the Supervising Engine is the one that schedules tasks for the node



Network Group Properties

G15

Name: First Network Group

Network Connection: T1

□ Protected By Firewall

Network Administrator: admin

Contact Email: admin@a.local

Contact Phone: (800) 674-1234

Default Alert: EMAIL_GENERAL

Default Alert Executor:

Default Node Properties

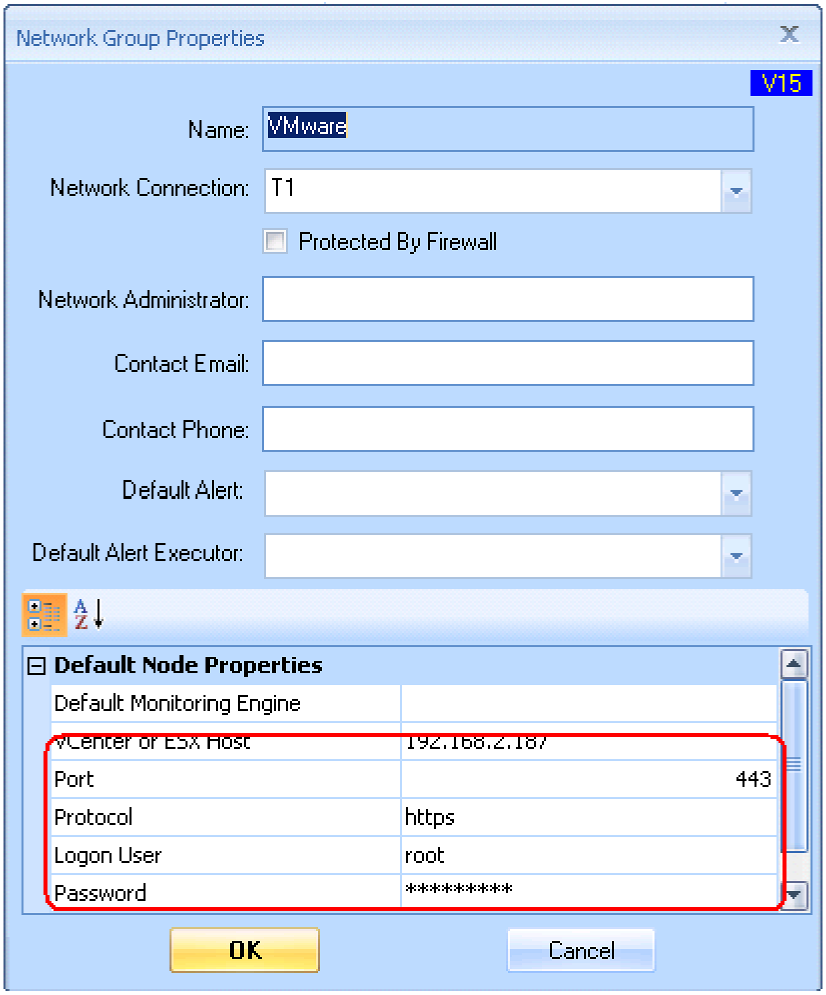
Default Monitoring Engine: {Product Main Engine}

{Product Main Engine}
PANA35

Which Logon Credential Does Argent for VMware Use To Monitor VMware Objects?

To determine the logon credential for a VMware object, Argent for VMware uses the following logic:

- First check if the VMware object has explicitly set a user/password at the licensed node level
- If default, check the logon credential specified in the Network Group that the node belongs to
- If set, use it
- If not set, use the logon credential at the system level specified in the Supervising Engine setting



Name: VMware

Network Connection: T1

☐ Protected By Firewall

Network Administrator:

Contact Email:

Contact Phone:

Default Alert:

Default Alert Executor:

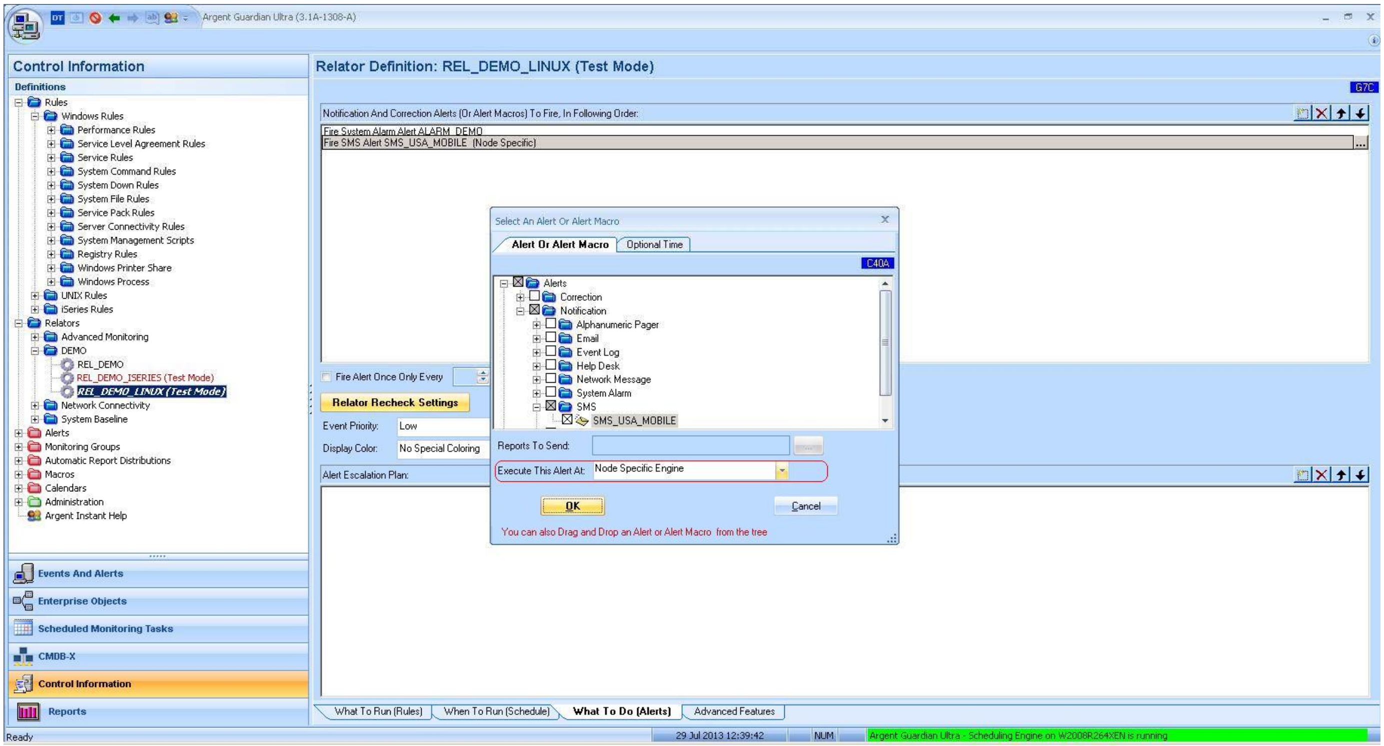
⊟ **Default Node Properties**

Default Monitoring Engine	
vCenter or ESX Host	192.168.2.187
Port	443
Protocol	https
Logon User	root
Password	**********

How Do I Fire An Alert Through A Node-Specific Argent Alert Executor?

The Argent Alert Executor allows Argent AT to fire alerts from a different machine other than the Argent Console main engine.

Customers can specify to use the Argent Alert Executor when defining Alerts in a Relator.



Relator Definition: REL_DEMO_LINUX (Test Mode)

Notification And Correction Alerts (Or Alert Macros) To Fire, In Following Order:

Fire System Alarm Alert ALARM_DEMO
Fire SMS Alert SMS_USA_MOBILE (Node Specific)

□ Fire Alert Once Only Every

Event Priority: Low

Display Color: No Special Coloring

Alert Escalation Plan:

Select An Alert Or Alert Macro

Reports To Send:

Execute This Alert At: Node Specific Engine

You can also Drag and Drop an Alert or Alert Macro from the tree

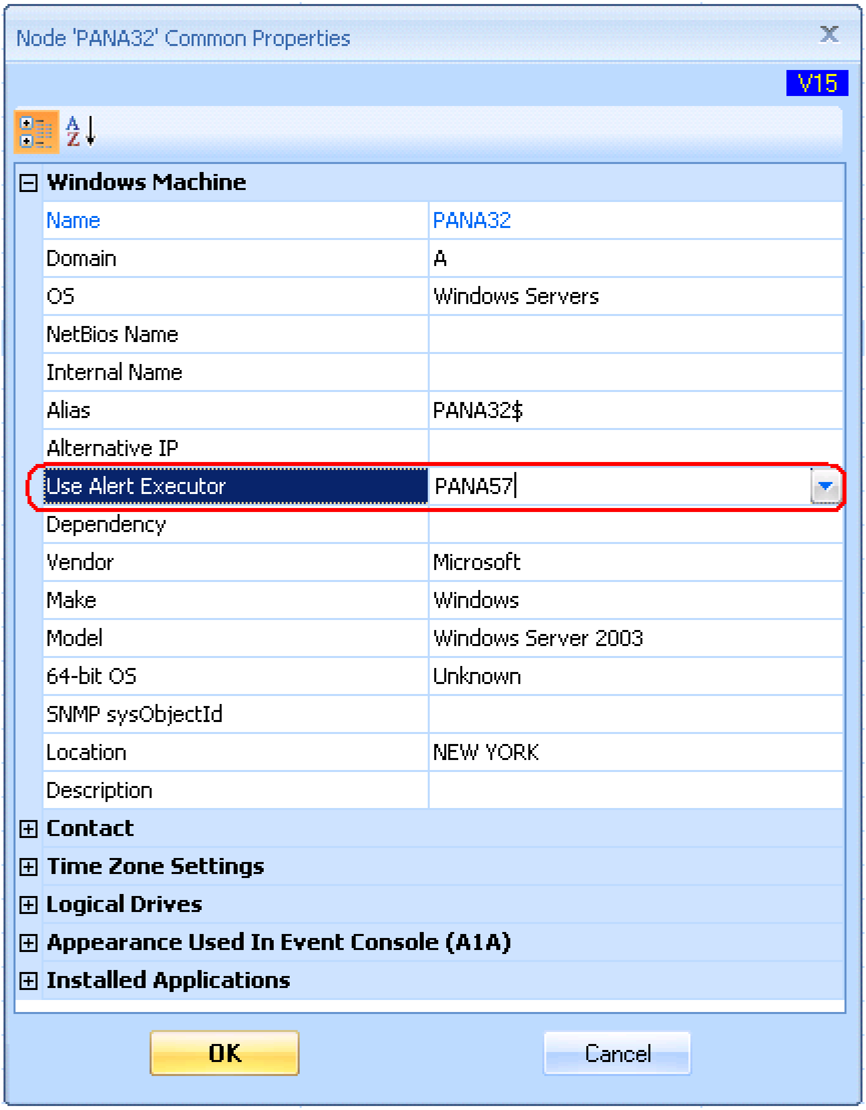
29 Jul 2013 12:39:42

Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

The Alert Executor can be either explicit or node specific.

When it is node specific, the Argent Console engine use the following algorithm to determine which Alert Executor should be used:

- If the node has an Alert Executor specified, use it

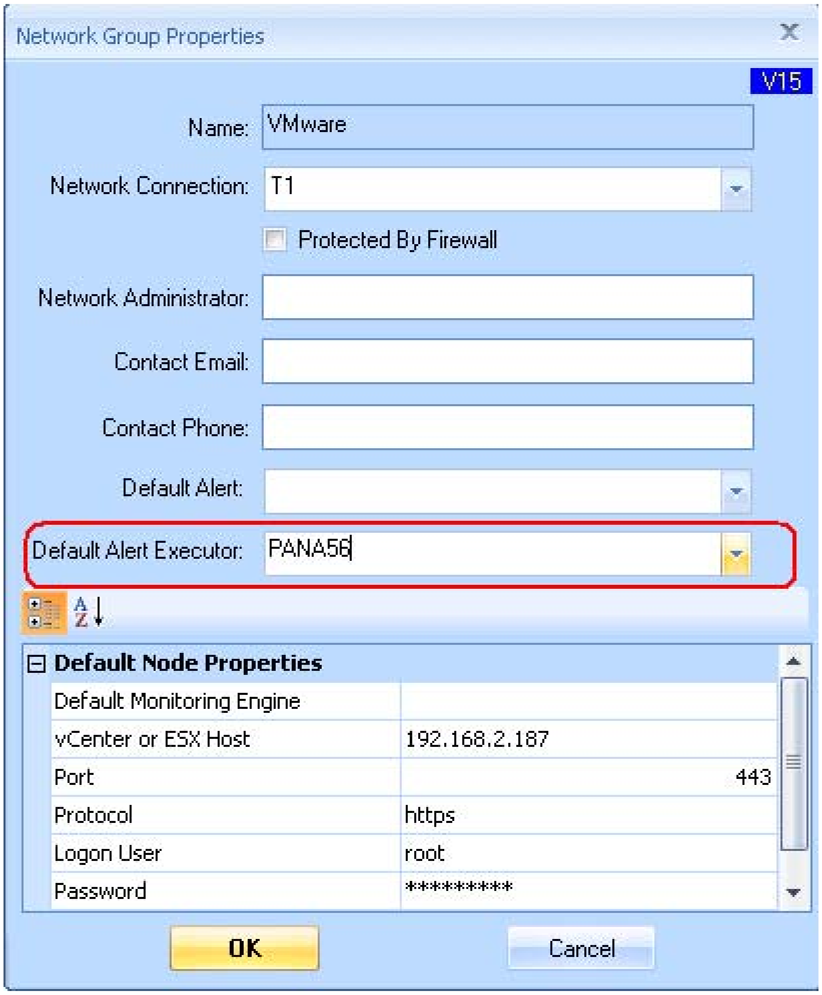


Node 'PANA32' Common Properties

V15

Windows Machine	
Name	PANA32
Domain	A
OS	Windows Servers
NetBios Name	
Internal Name	
Alias	PANA32$
Alternative IP	
Use Alert Executor	PANA57
Dependency	
Vendor	Microsoft
Make	Windows
Model	Windows Server 2003
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	
Contact	
Time Zone Settings	
Logical Drives	
Appearance Used In Event Console (A1A)	
Installed Applications	

- If the Network Group that node belongs to has an Alert Executor specified, use it



Network Group Properties

V15

Name:	VMware
Network Connection:	T1
	□ Protected By Firewall
Network Administrator:	
Contact Email:	
Contact Phone:	
Default Alert:	
Default Alert Executor:	PANA56

⊟ **Default Node Properties**

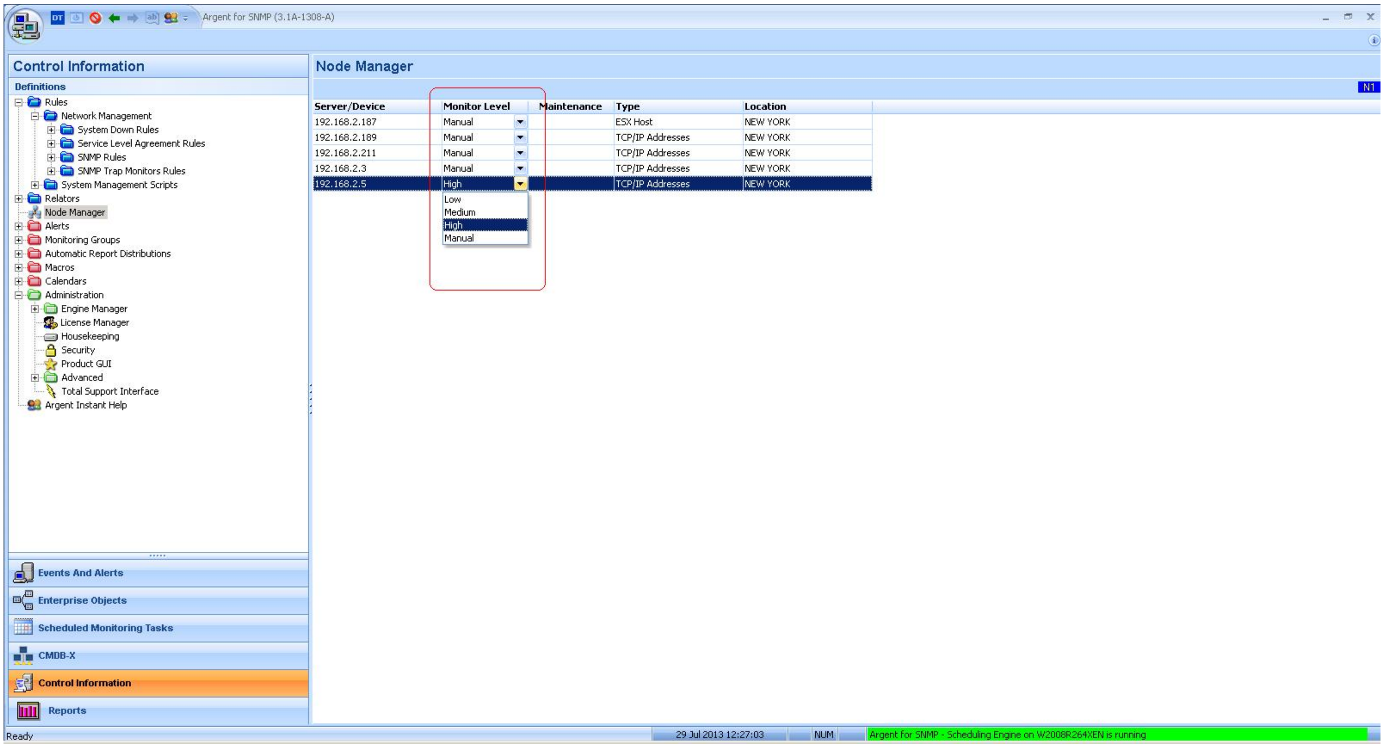
Default Monitoring Engine	
vCenter or ESX Host	192.168.2.187
Port	443
Protocol	https
Logon User	root
Password	*********

- Otherwise, use the Argent Console Main Engine to fire the Alert

How Do I Specify What Alert To Fire When Doing Automated Monitoring In Argent for SNMP?

Argent for SNMP provides a powerful heuristic self-learning facility. This is explained in more detail in the document “Argent for SNMP Self-Learning Facility”.

Customers can select a monitoring level at the Node Manager, and the Argent for VMware engine synthetically generates internal Relators to monitor.



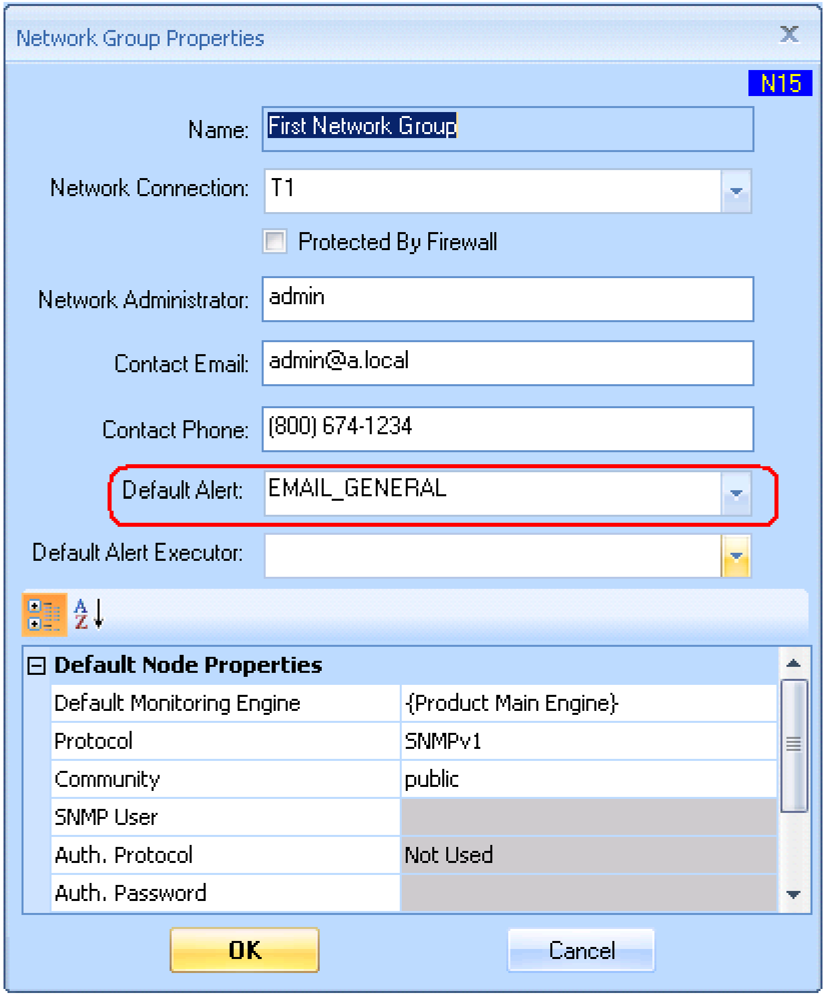
Server/Device	Monitor Level	Maintenance	Type	Location
192.168.2.187	Manual		ESX Host	NEW YORK
192.168.2.189	Manual		TCP/IP Addresses	NEW YORK
192.168.2.211	Manual		TCP/IP Addresses	NEW YORK
192.168.2.3	Manual		TCP/IP Addresses	NEW YORK
192.168.2.5	High		TCP/IP Addresses	NEW YORK

29 Jul 2013 12:27:03

Argent for SNMP - Scheduling Engine on W2008R264XEN is running

Because the synthetically generated internal Relator does not exist physically, the engine needs to know what Alert to fire if the Rule is broken.

The Alert is defined as the Default Alert in the Network Group the node belongs to.



Network Group Properties

N15

Name: First Network Group

Network Connection: T1

□ Protected By Firewall

Network Administrator: admin

Contact Email: admin@a.local

Contact Phone: (800) 674-1234

Default Alert: EMAIL_GENERAL

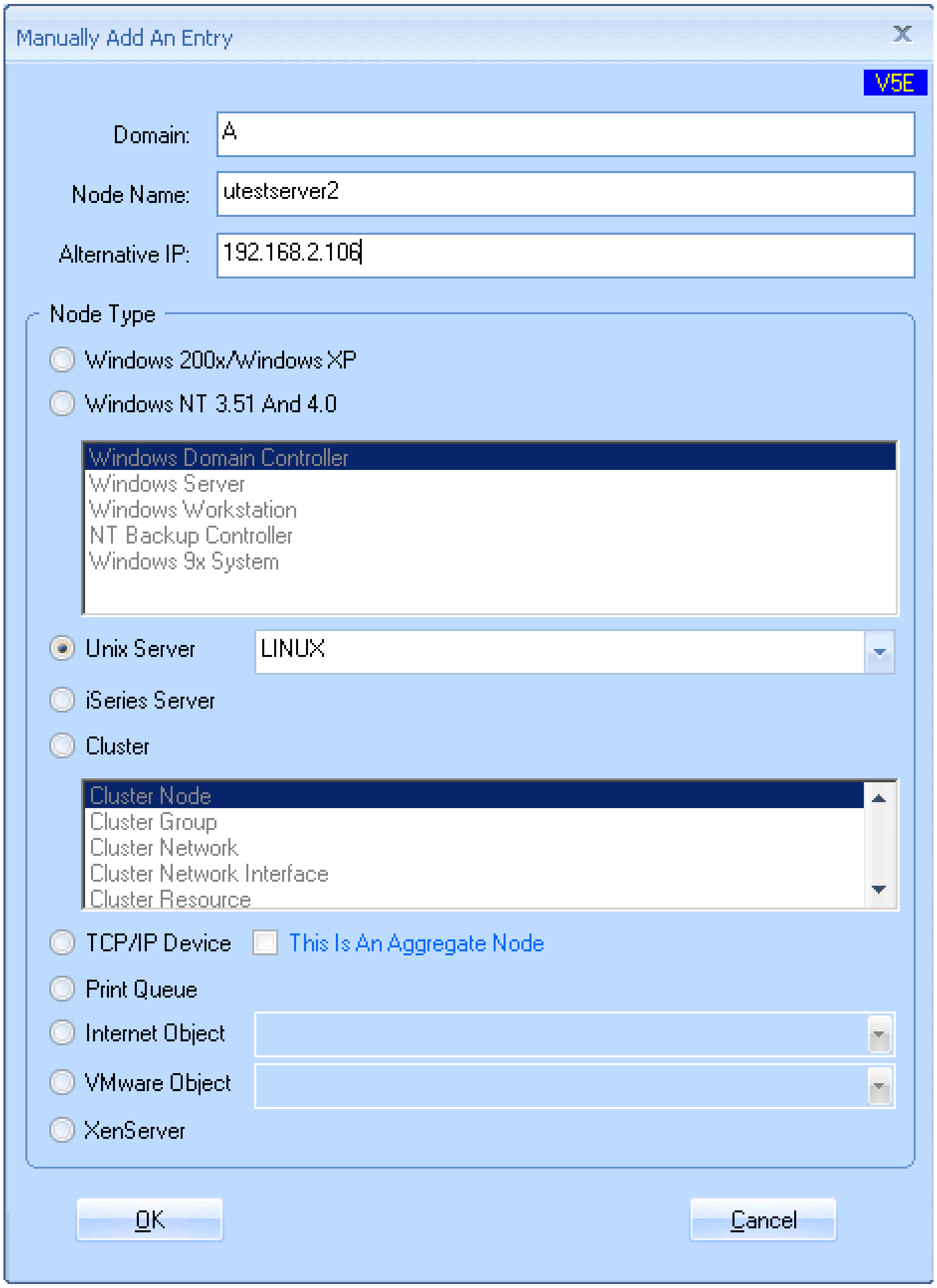
Default Alert Executor:

Default Node Properties

Default Monitoring Engine	{Product Main Engine}
Protocol	SNMPv1
Community	public
SNMP User	
Auth. Protocol	Not Used
Auth. Password	

How Do I Add Linux/Unix Servers To Argent Atlas?

To add a few Linux/Unix servers, add them manually by right-clicking and ‘**Add Server Or Device**’ on CMDB-X screen.


Manually Add An Entry

Domain: A

Node Name: utestserver2

Alternative IP: 192.168.2.106

Node Type

● Unix Server LINUX

If a large number of servers are to be added, use the Argent AT command-line facility.

```
ARGENT_CMDB_CLI -n node [-o “property:value”]  [-g group] -a
```

- Argument '-n' specifies the node name
- Argument '-g' specifies the network group that the node will be added to; it is optional; if not specified, the default 'First Network Group' is assumed
- Argument '-o' specifies relevant pairs of property and value

To add a Linux server, specify the OS as 'Linux Servers'. Example:

```
ARGENT_CMDB_CLI -n TestNode1 -o "Domain:A" -o "OS:Linux Servers" -o "Alternative
IP:192.168.2.106" -a
```

For details see Argent AT command-line facilities

Customers can read the Linux/Unix servers from another data source, and repeatedly call the command line to add all the servers.

How Do I Programmatically Remove Server/Devices From Argent Atlas?

Customers can use the Argent AT command-line facility to accomplish it.

```
ARGENT_CMDB_CLI -n node -r
```

Argument '-n' specifies the node name.

For example, the following command removes node ‘W2008R264XEN’ from Argent Atlas.

```
ARGENT_CMDB_CLI -n W2008R264XEN -r
```

Note: The operation will fail if the server/device is licensed in any Argent AT product.

In that case, customers should first call the following to unlicense the node from the Argent AT products.

```
ARGENT_LICENSE_CLI -n node -p product –r
```

For example, the following command unlicenses the node ‘W2008R264XEN’ from Argent Guardian Ultra.

```
ARGENT_LICENSE_CLI -n W2008R264XEN -p “Argent Guardian Ultra” -r
```

How Do I Add Servers In An Active Directory Environment To Argent Atlas?

Scanning Windows network using Active Directory is the most reliable way to accomplish this.

For details, see section ‘Scan Windows Network Using Active Directory’ in Appendix B.

How Do I Add Servers In A Workgroup Environment To Argent Atlas?

Scanning Windows network using Network Browser is the easiest way, but the Microsoft Network Browser must be treated with caution, as it is sometimes unreliable.

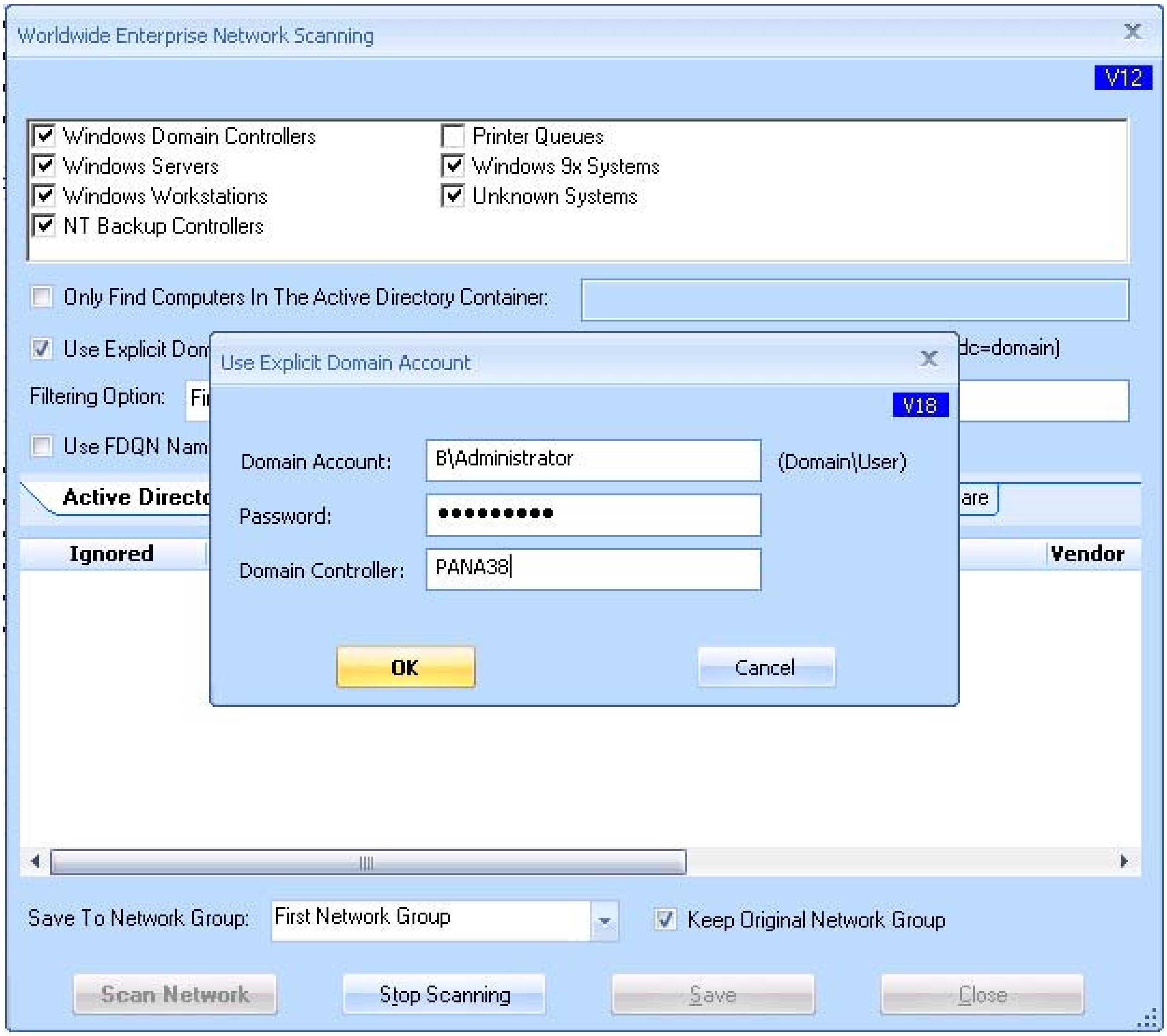
For small amounts of servers, customers can opt to add manually.

For details, see section 'Scan Windows Network Using Network Browser' in Appendix B.

How Do I Add Servers In A Different Domain To Argent Atlas?

Use the option **'Use Explicit Domain Account'** when doing Active Directory scanning.

Customers are prompted to enter the logon credentials and domain controllers before the actual scanning.



Worldwide Enterprise Network Scanning

☑ Windows Domain Controllers
☑ Windows Servers
☑ Windows Workstations
☑ NT Backup Controllers
□ Printer Queues
☑ Windows 9x Systems
☑ Unknown Systems

□ Only Find Computers In The Active Directory Container:

☑ Use Explicit Dom

□ Use FDQN Nam

Use Explicit Domain Account

Domain Account: B\Administrator (Domain\User)

Password: ●●●●●●●●●●

Domain Controller: PANA38

Save To Network Group: First Network Group

☑ Keep Original Network Group

How Do I Scan A Large TCP/IP Network Quickly?

IANA-reserved private IPv4 network ranges

	Start	End	No. Of addresses
24-bit block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16777216
20-bit block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1048576
16-bit block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65536

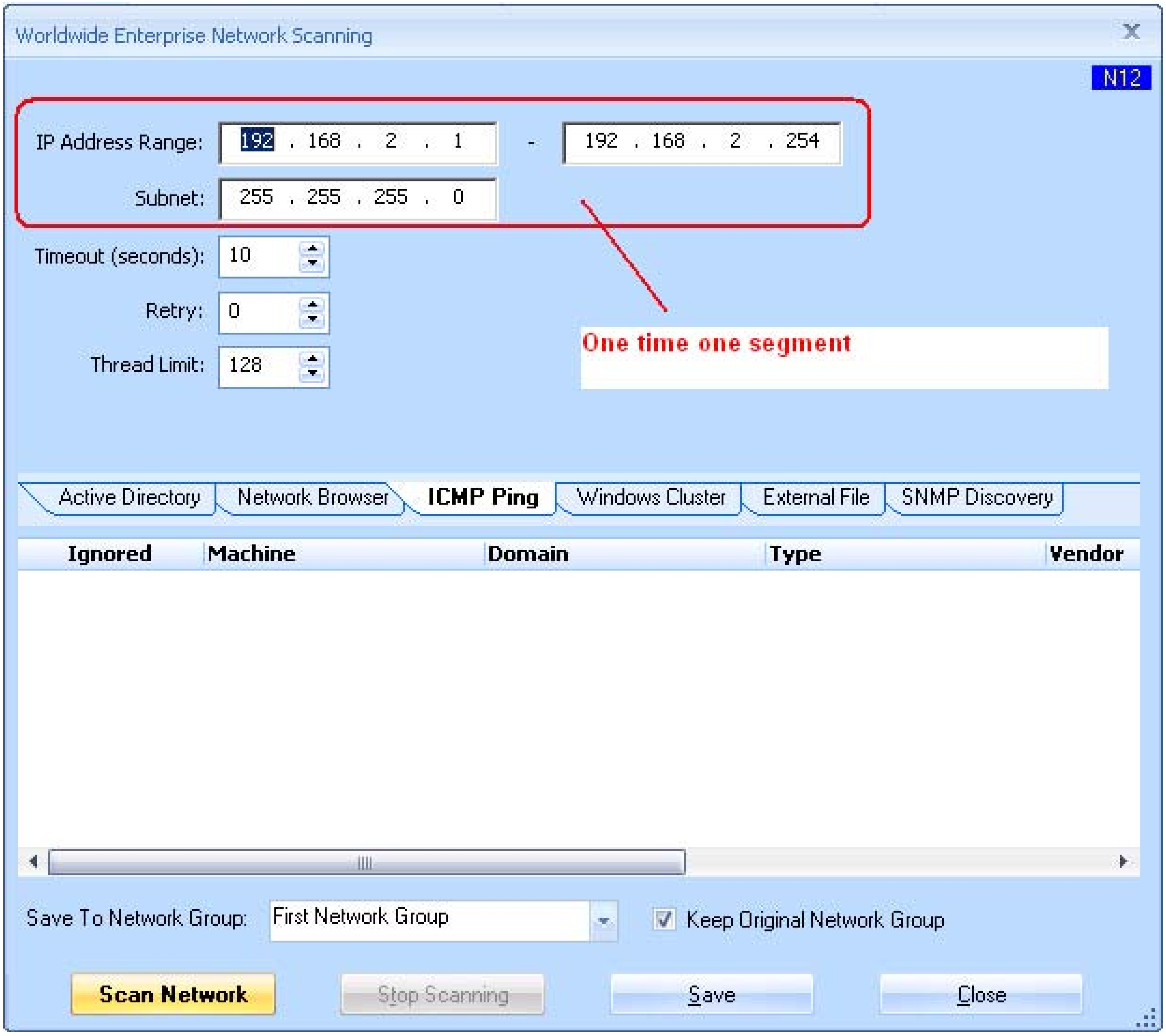
Theoretically customers can pick any of the above as a whole for the network.

For example, a large network may have a range of 10.0.0.0 – 10.255.255.255, while SOHO can use 192.168.1.0 – 192.168.1.255.

If more than 256 IP addresses are needed, then 192.168.0.0 can be selected with a network mask 255.255.0.0.

In most cases, customers will pick multiple network segments such as 192.168.0.x, 192.168.1.x, 192.168.2.x etc.

To scan such a network, it is a lot faster to do it by scanning each segment of 256 addresses instead of scanning the whole range of 65,536 addresses.



IP Address Range: 192 . 168 . 2 . 1 - 192 . 168 . 2 . 254

Subnet: 255 . 255 . 255 . 0

Timeout (seconds): 10

Retry: 0

Thread Limit: 128

One time one segment

Ignored	Machine	Domain	Type	Vendor

Save To Network Group: First Network Group

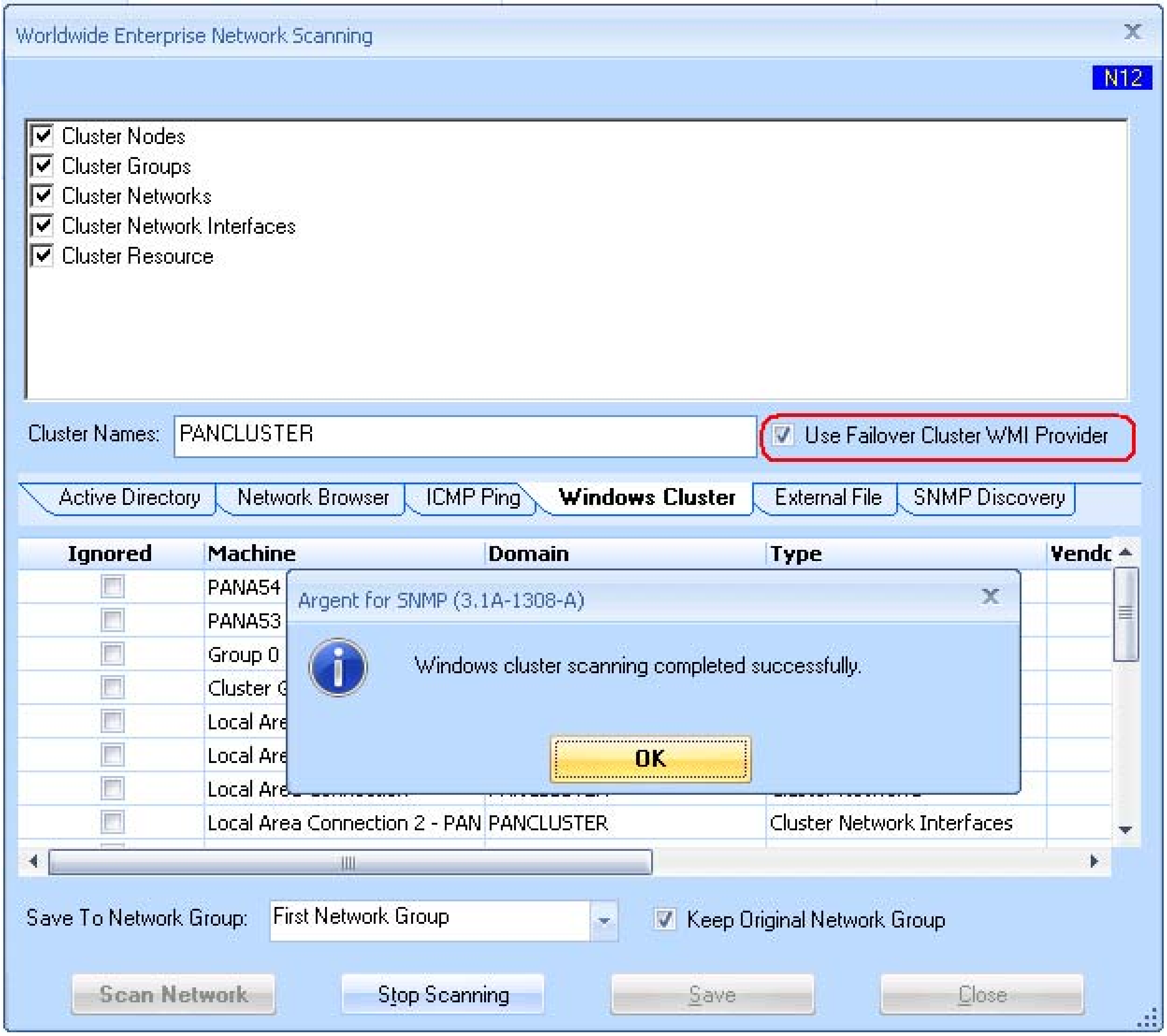
☑ Keep Original Network Group

How Do I Scan A Mixed Cluster Environment?

Microsoft Clusters for W2003 and W2008 do not talk to each other.

As a result, native cluster WIN32 API does not work on W2003 querying a remote W2008 cluster, and vice versa.

To handle a mixed cluster environment, the option **'Failover Cluster WMI Provider'** should be used.



Worldwide Enterprise Network Scanning

N12

☑ Cluster Nodes
☑ Cluster Groups
☑ Cluster Networks
☑ Cluster Network Interfaces
☑ Cluster Resource

Cluster Names: PANCLUSTER

☑ Use Failover Cluster WMI Provider

Ignored	Machine	Domain	Type	Vendc
□	PANA54			
□	PANA53			
□	Group 0			
□	Cluster G			
□	Local Are			
□	Local Are			
□	Local Are			
□	Local Area Connection 2 - PAN	PANCLUSTER	Cluster Network Interfaces	

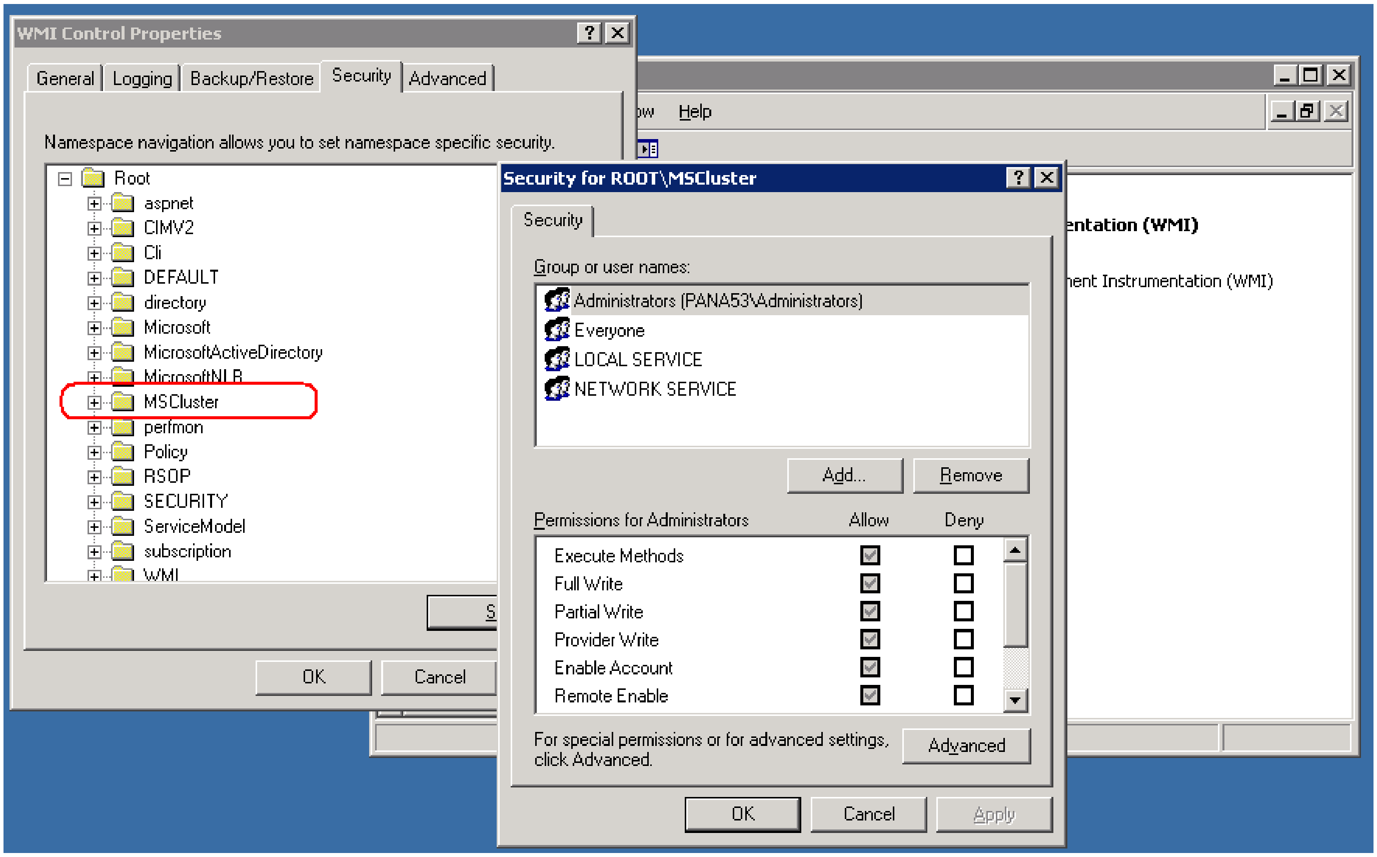
Argent for SNMP (3.1A-1308-A)

Windows cluster scanning completed successfully.

Save To Network Group: First Network Group

☑ Keep Original Network Group

Because it relies on WMI, the security on the cluster must be adjusted to allow the Argent AT engine access to the WMI name space ‘root\mscluster’.



Namespace navigation allows you to set namespace specific security.

Group or user names:

- Administrators (PANA53\Administrators)
- Everyone
- LOCAL SERVICE
- NETWORK SERVICE

Permissions for Administrators	Allow	Deny
Execute Methods	☑	□
Full Write	☑	□
Partial Write	☑	□
Provider Write	☑	□
Enable Account	☑	□
Remote Enable	☑	□

For special permissions or for advanced settings, click Advanced.

Why Are Some SNMP Device Not Discovered?

Scanning SNMP devices is similar to ICMP Ping by enumerating all the possible IP addresses in the range. As a result, the recommendation of using small network segments in How To Scan A Large TCP/IP Network Quickly also applies here.

Customers may find some or all SNMP devices are not found during network scanning. The possible causes include the following:

1. Each SNMP device has a built-in configuration of allowed management workstations. In other words, it only handles requests from certain IP addresses. Contact the Network Administrator, ensure the machine where the scanning is done (e.g. Argent Main Engine) is listed as a management workstation in the SNMP devices.

2. Check supported SNMP version. Version 1 and 2c are most common, and version 3 is the most complicated. Scan the network using the appropriate SNMP version setting.

3. If it is v1 or v2c, ensure the community string is correct. The string is the password in the SNMP world.

4. If it is v3, double check the password and protocol for authentication and encryption. If any of them mismatches, the scanning won't work.

5. If the network segment for scanning is outside of the local network segment, ensure the option 'Active Poll Each IP Address' is checked. Most routers won't forward SNMP broadcast packets out of a local segment.

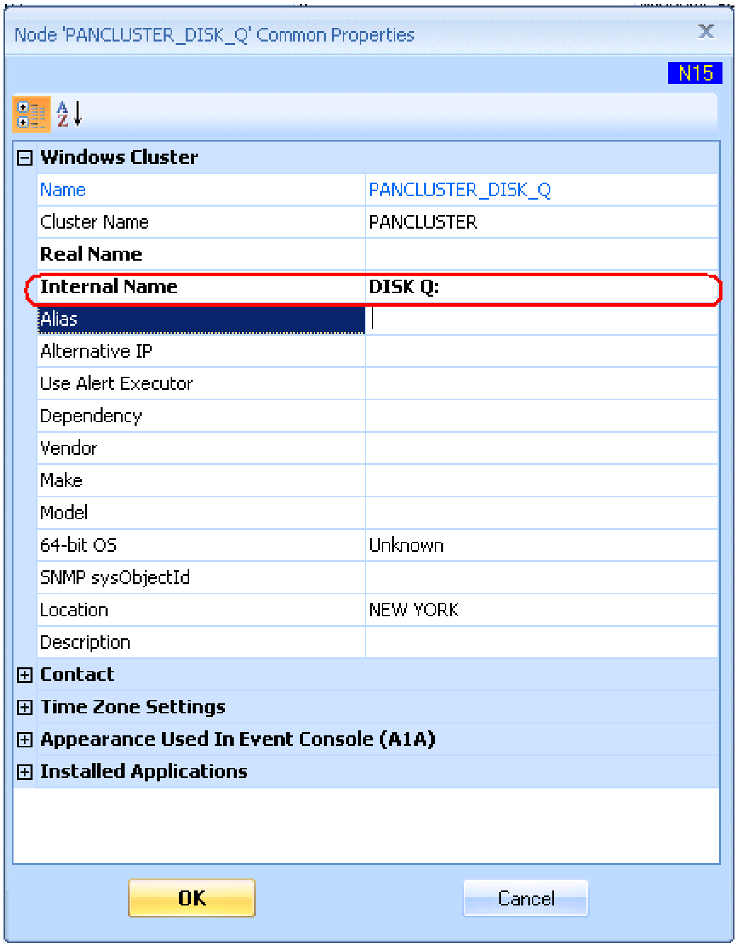
What Do I Do When Two Cluster Objects Have The Same Name But Are From Different Clusters?

Give each Cluster Object distinct node names while using the ‘Internal Name’ field to hold the real object name.

When monitoring multiple Windows Clusters there may be naming conflicts.

For example, two SQL Clusters have resource ‘Disk Q:’. Clearly both cannot use ‘Disk Q:’ for the cluster object name.

Instead, use DISK_Q_OF_CLUSTER_A and DISK_Q_OF_CLUSTER_B for the two objects, and specify ‘Disk Q:’. Because the Cluster is determined by the property **‘Cluster Name’**, the two objects are fully defined without conflict.



Windows Cluster

Name	PANCLUSTER_DISK_Q
Cluster Name	PANCLUSTER
Real Name	
Internal Name	**DISK Q:**
Alias	
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	
Make	
Model	
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	

Contact

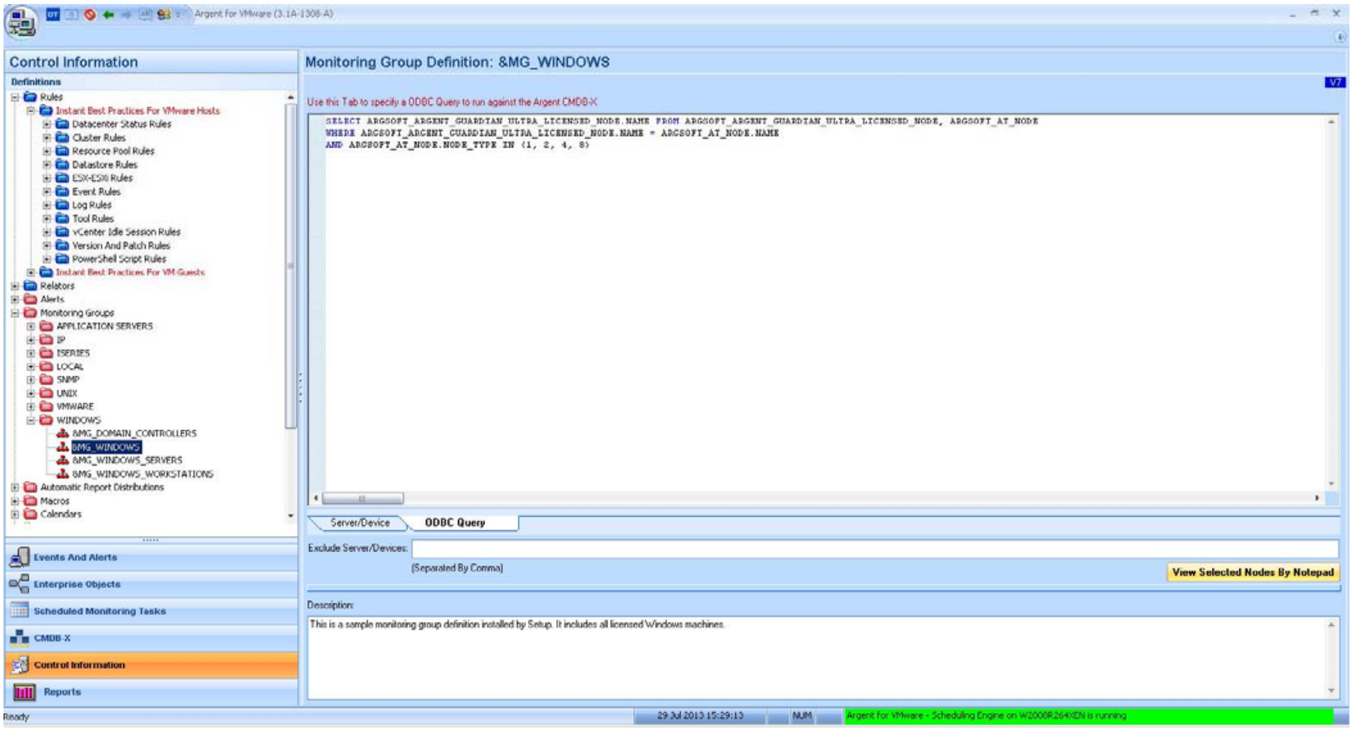
Time Zone Settings

Appearance Used In Event Console (A1A)

Installed Applications

How Do I Define Monitoring Groups Based On Node Type?

This is can be done by using an ODBC query-based Monitoring Group.



Monitoring Group Definition: &MG_WINDOWS

Use this Tab to specify a ODBC Query to run against the Argent CMDB-X

```
SELECT ARGSOFT_ARGENT_GUARDIAN_ULTRA_LICENSED_NODE.NAME FROM ARGSOFT_ARGENT_GUARDIAN_ULTRA_LICENSED_NODE, ARGSOFT_AT_NODE
WHERE ARGSOFT_ARGENT_GUARDIAN_ULTRA_LICENSED_NODE.NAME = ARGSOFT_AT_NODE.NAME
AND ARGSOFT_AT_NODE.NODE_TYPE IN (1, 2, 4, 8)
```

Exclude Server/Devices:

(Separated By Comma)

Description:

This is a sample monitoring group definition installed by Setup. It includes all licensed Windows machines.

The query uses the column 'NODE_TYPE' to specify Windows OS. The possible values are as follows:

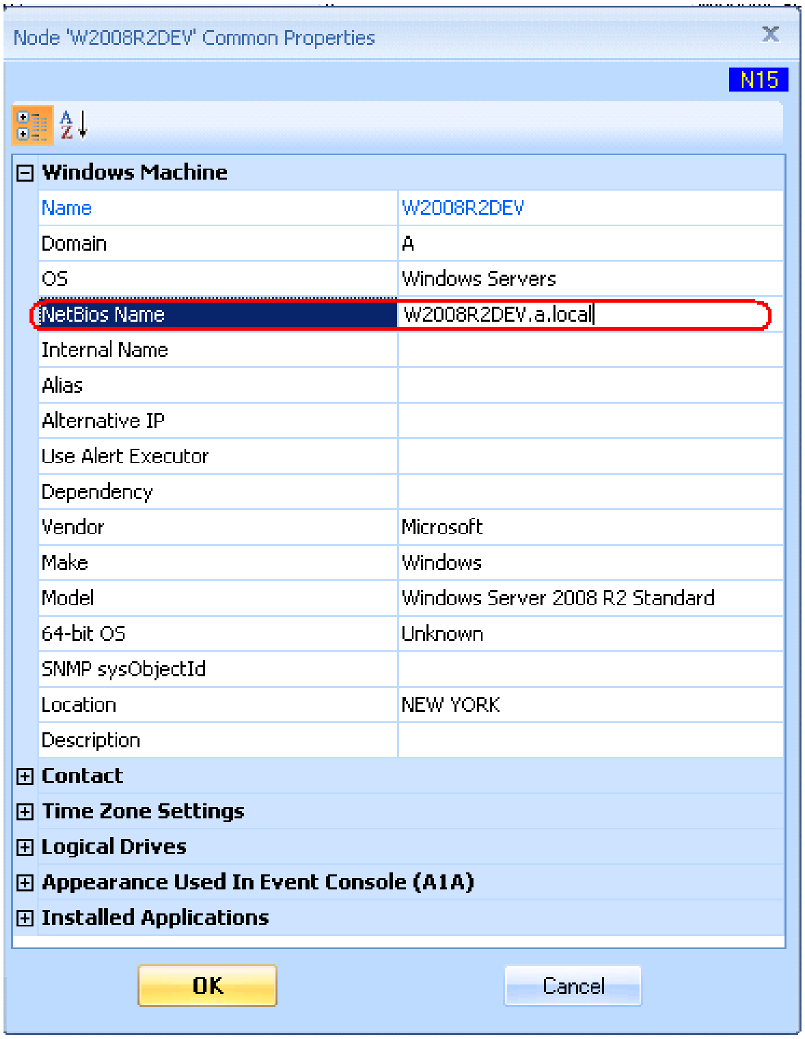
0x1 (1)	– Windows Domain Controller
0x2 (2)	– Windows Backup Domain Controller
0x4 (4)	– Windows Server
0x8 (8)	– Windows Workstation
0x10 (16)	– Sun Solaris
0x20 (32)	– HP-UX
0x40 (64)	– AIX
0x80 (128)	– SCO UNIX
0x100 (256)	– Linux
0x200 (512)	– IP Address
0x400 (1,024)	– iSeries Server
0x800 (2,048)	– Cluster Node
0x1000 (4,096)	– Cluster Group

0x2000 (8,192)	– Cluster Network
0x4000 (16,384)	– Cluster Network Interface
0x8000 (32,768)	– Cluster Resource
0x10000 (65,536)	– Printer Queue
0x20000 (131,072)	– Windows 9x (obsolete)
0x40000 (262,144)	– Novell Server (obsolete)
0x80000 (524,288)	– Unknown
0x100000 (1,048,576)	– URL Object
0x200000 (2,097,152)	– Mail Object
0x400000 (4,194,304)	– FTP Object

How Do I Add Two Machines With The Same Machine Name But In Separated Unrelated Networks?

ISP customers can run into such a situation. Two accounts may have machines of the same name. It happens when the machine is either cloned or installed with default settings of a Microsoft small business suite. Because each account has its own network, there is no conflict until the ISP needs to monitor both of them.

To address the issue, customers can add two machines using arbitrary names, but specify the NetBIOS property with the real machine name. As long as two machines are monitored by separate Daughter Engines, it will work as expected.



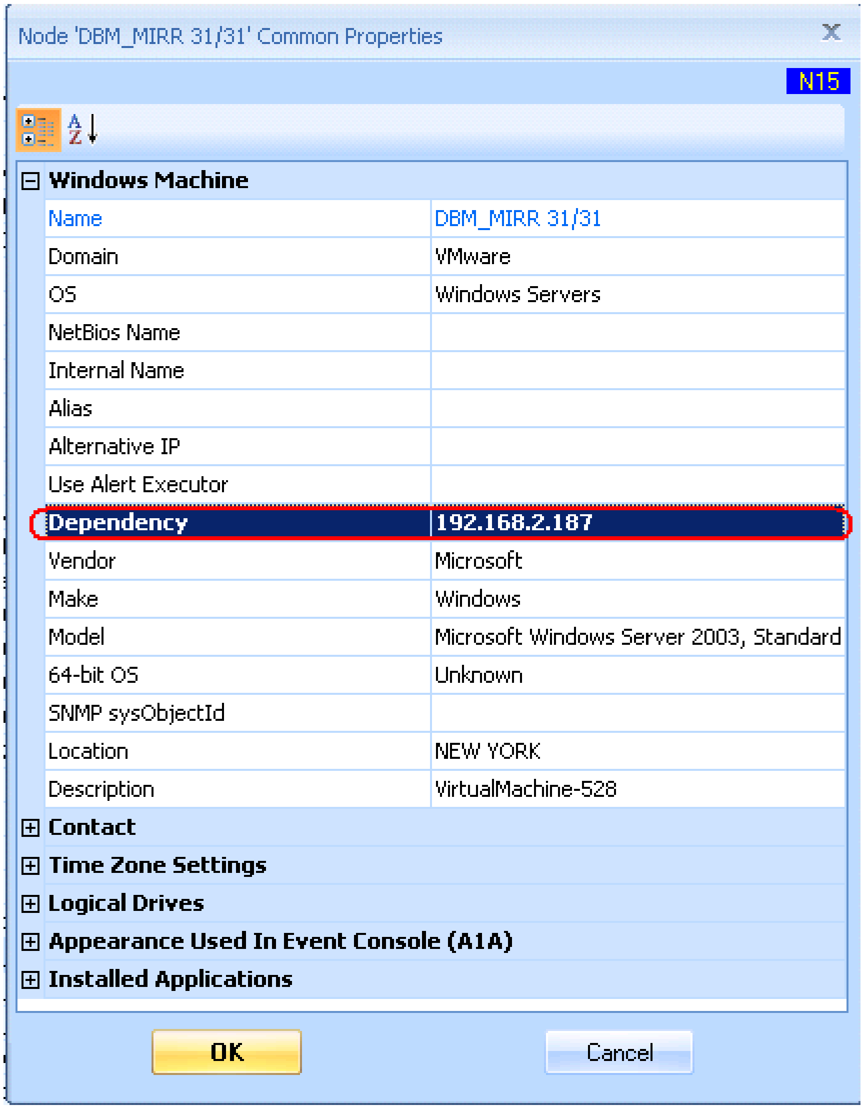
Windows Machine

Name	W2008R2DEV
Domain	A
OS	Windows Servers
NetBios Name	W2008R2DEV.a.local
Internal Name	
Alias	
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	Microsoft
Make	Windows
Model	Windows Server 2008 R2 Standard
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	

⊞ Contact
⊞ Time Zone Settings
⊞ Logical Drives
⊞ Appearance Used In Event Console (A1A)
⊞ Installed Applications

When An ESX Host Is Offline, A Flood Of Alerts Are Sent About Offline VMs. How Do I Receive Just One Alert Telling The Root Cause?

Specify the ESX host as a Logical Dependency for the VMs and enable Root Cause Analysis in the Relator definition.



Node 'DBM_MIRR 31/31' Common Properties

N15

⊟ Windows Machine

Name	DBM_MIRR 31/31
Domain	VMware
OS	Windows Servers
NetBios Name	
Internal Name	
Alias	
Alternative IP	
Use Alert Executor	
Dependency	192.168.2.187
Vendor	Microsoft
Make	Windows
Model	Microsoft Windows Server 2003, Standard
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	VirtualMachine-528

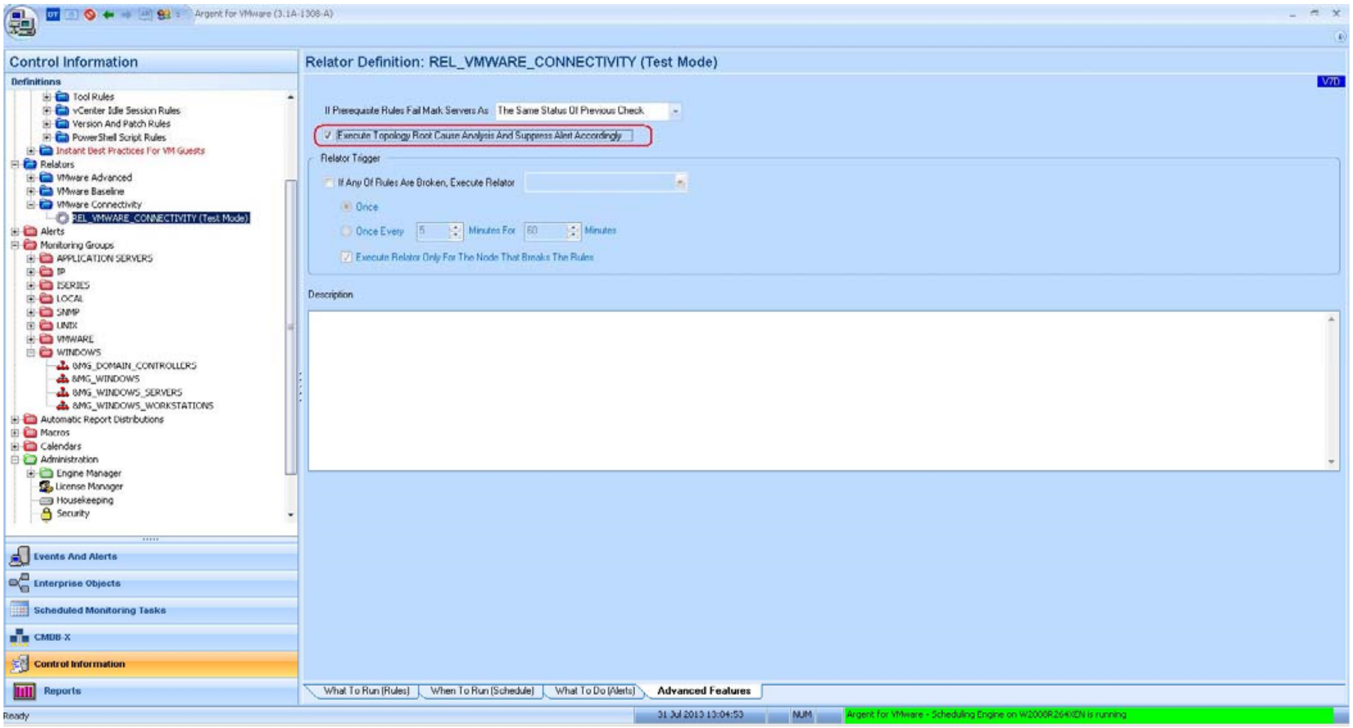
⊞ Contact

⊞ Time Zone Settings

⊞ Logical Drives

⊞ Appearance Used In Event Console (A1A)

⊞ Installed Applications



Relator Definition: REL_VMWARE_CONNECTIVITY (Test Mode)

If Prerequisite Rules Fail Mark Servers As: The Same Status Of Previous Check

☑ Execute Topology Root Cause Analysis And Suppress Alert Accordingly

Relator Trigger

□ If Any Of Rules Are Broken, Execute Relator

● Once

○ Once Every 5 Minutes For 60 Minutes

☑ Execute Relator Only For The Node That Breaks The Rules

Description

31 Jul 2013 13:04:53

Argent for VMware - Scheduling Engine on W2008R264XEN is running

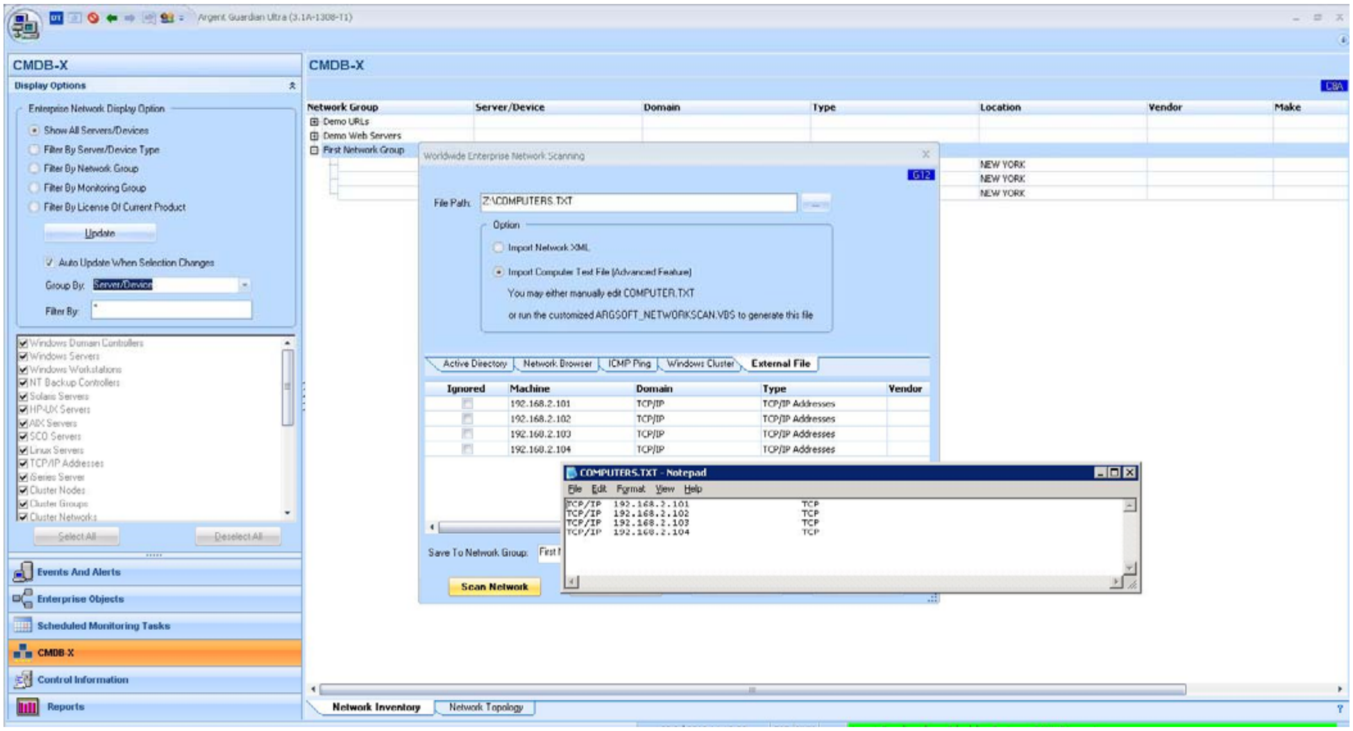
When the Argent AT engine cannot access the VM, it will check the accessibility of its logical dependency. In this case, it is the ESX host. If the ESX host is offline, the event will be raised about the dependency instead of the offline VM.

How Can IP Addresses In An Excel File Be Imported To Argent Atlas?

Compose COMPUTERS.TXT then import into CMDB-X. Do the following:

1. Copy out the IP address column in the Excel into notepad.
2. Put ‘TCP/IP<TAB>’ in front of each line.
3. Put ‘<TAB><TAB><TAB>TCP’ in end of each line.
4. Save file as COMPUTERS.TXT
5. Import into CMDB-X (See Import And Export CMDB-X Data)

Note the count of one <TAB> and then three <TAB> is essential.



File Path: Z:\COMPUTERS.TXT

Option
○ Import Network XML
● Import Computer Text File (Advanced Feature)
You may either manually edit COMPUTER.TXT
or run the customized ARGSOFT_NETWORKSCAN.VBS to generate this file

Ignored	Machine	Domain	Type	Vendor
□	192.168.2.101	TCP/IP	TCP/IP Addresses	
□	192.168.2.102	TCP/IP	TCP/IP Addresses	
□	192.168.2.103	TCP/IP	TCP/IP Addresses	
□	192.168.2.104	TCP/IP	TCP/IP Addresses	

Save To Network Group: First N

```
TCP/IP   192.168.2.101                    TCP
TCP/IP   192.168.2.102                    TCP
TCP/IP   192.168.2.103                    TCP
TCP/IP   192.168.2.104                    TCP
```

There are Many Devices in the DMZ; They Cannot Be Scanned By The Argent AT Engine; There Are Too Many To Add Manually.

How Can The Devices Be Added To Argent Atlas?

Customers can do a quick install of Argent Guardian Ultra using SQL Server Compact on a machine of DMZ, then do the following:

1. Do a network scan using from the Argent GUI
2. Export the result as an XML file
3. Copy the XML file to the Main Engine
4. Import the XML file
5. Uninstall Argent AT from the machine in the DMZ

How Do I Determine All The Known SQL Servers In Argent Atlas?

Run the following SQL query using ‘osql’:

```
SELECT ARGSOFT_AT_NODE.NAME FROM ARGSOFT_AT_NODE, ARGSOFT_AT_NODE_APPLICATION
WHERE ARGSOFT_AT_NODE.UUID = ARGSOFT_AT_NODE_APPLICATION.NODE_UUID
AND ARGSOFT_AT_NODE_APPLICATION.NAME = 'MSSQL'
```

The key is to query with the qualified application name ‘MSSQL’.

The same technique can be used to find Exchange servers, Oracle servers etc.

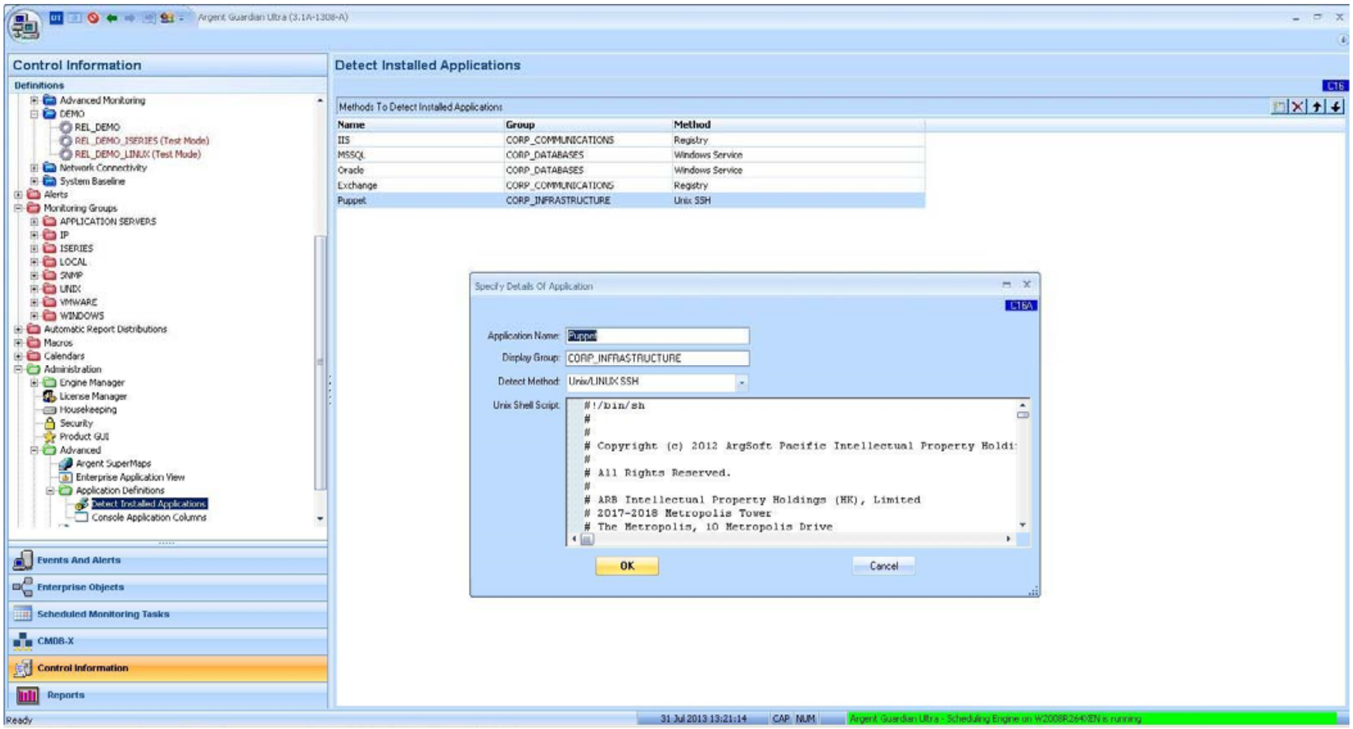
For the command syntax of ‘osql’, see:
http://msdn.microsoft.com/en-us/library/aa213087(v=sql.80).aspx

How To Detect Whether Puppet Is Installed On A Linux Server?

The Puppet product has two components: Puppet master and Puppet client.

The easiest way to detect Puppet master is to use the method ‘TCP service’ to check if the Linux server is listening on port 8140. This generally is sufficient but be careful -- some rogue program may use the same port.

The most reliable way is to define an application using SSH methods to detect if the daemon ‘puppetmaster’ or ‘puppet’ is running.



Detect Installed Applications

Methods To Detect Installed Applications

Name	Group	Method
IIS	CORP_COMMUNICATIONS	Registry
MSSQL	CORP_DATABASES	Windows Service
Oracle	CORP_DATABASES	Windows Service
Exchange	CORP_COMMUNICATIONS	Registry
Puppet	CORP_INFRASTRUCTURE	Unix SSH

Specify Details Of Application

Application Name: Puppet

Display Group: CORP_INFRASTRUCTURE

Detect Method: Unix/LINUX SSH

Unix Shell Script:

```
#!/bin/sh
#
#
# Copyright (c) 2012 ArgSoft Pacific Intellectual Property Holdi
#
# All Rights Reserved.
#
# ARB Intellectual Property Holdings (HK), Limited
# 2017-2018 Metropolis Tower
# The Metropolis, 10 Metropolis Drive
```

Sample code is shown as follows:

```
#!/bin/sh
#
#
# Copyright (c) 2013 ArgSoft Pacific Intellectual Property Holdings (HK), Limited
#
# All Rights Reserved.
#
# ARB Intellectual Property Holdings (HK), Limited
# 2017-2018 Metropolis Tower
# The Metropolis, 10 Metropolis Drive
# Hong Kong
#
#
#
# This is PROPRIETARY SOURCE CODE of ARB Intellectual Property Holdings (HK), Limited.
#
# The contents of this file may not be disclosed to third parties, copied or
# duplicated in any form, in whole or in part, without the prior written
# permission of ArgSoft Pacific Intellectual Property Holdings (HK), Limited.
#
# RESTRICTED RIGHTS LEGEND:
# Use, duplication or disclosure by the Government is subject to restrictions
# as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data
# and Computer Software clause at DFARS 252.227-7013, and/or in similar or
# successor clauses in the FAR, DOD or NASA FAR Supplement.
#
# Unpublished - rights reserved under the Copyright Laws of the United States
# and other countries.
#
#
#
#
# This rule checks the status of the Puppet daemon.
#
# The rule fails if puppet is not running.
#
# For more information: email Unix@Argent.com.


STATUS=NOVAL

SUMMARY=NOVAL

COMMENT=NOVAL

#
# xmlOut() - prints an entire XML output for a command script.
```

```
#
#  Used for The Argent Guardian rules that return a PASS/FAIL
#
#  status and summary and comment descriptions.
#

xmlOut()
{
xmlBegin

xmlStatus

xmlEnd
}



#
# xmlBegin() - Prints out the definition of the XML format used to
#
#  send status data to The Argent Guardian.
#

xmlBegin()
{
cat <<!
<?xml version="1.0"?>
<!DOCTYPE TAGResult
[
<!ELEMENT TAGResult  (QEResult+)>
<!ELEMENT QEResult (status, summary, comment)>
<!ELEMENT status   (#PCDATA)> <!-- (PASS | FAIL) -->
<!ELEMENT summary  (#PCDATA) >
<!ELEMENT comment  (#PCDATA) >
]>

<TAGResult>
!

} # End of xmlBegin()



#
# xmlStatus() - Send a status block to The Argent Guardian.
#
# The status should be 'PASS' or 'FAIL'.
#
# The summary explains the result and the comment is a generic description of the Unix rule.
#
```

```
xmlStatus()
{
cat <<!
<QEResult>
<status>$STATUS</status>
<summary>$SUMMARY</summary>
<comment>$COMMENT</comment>
</QEResult>
!

} # End of xmlStatus()



#
# xmlEnd() - Completes the XML data block.
#

xmlEnd()
{
cat <<!
</TAGResult>
!

} # End of xmlEnd()



############################# Main portion of script ##########################

DAEMON=puppet

COMMENT="Using ps and grep to determine if $DAEMON is running."

#
# Using the 'ps -ae' command, search for the process and extract the
#
# process ID.
#

DAEMON_PID=`ps -ae | grep $DAEMON | grep -v daemon | awk '{ print $1 }'`

#
# Generate status based on whether the process is running or not.
#
if [ -z "$DAEMON_PID" ]; then

STATUS=FAIL
```

```
SUMMARY="The $DAEMON daemon is not running."

EXIT_CODE=1

else

STATUS=PASS

SUMMARY="The $DAEMON daemon is running. PID: $DAEMON_PID"

EXIT_CODE=0

fi

#
# Report the findings back to The Argent Guardian
#

xmlOut

exit $EXIT_CODE
```

Servers Are Assigned To Different Administrators. When A Rule Is Broken, The Assigned Administrator Should Be Notified In One Relator.

How Is This Done?

Assume within one Relator, there is one Email Alert. The actual 'To' field in the Email Alert cannot be fixed when sending emails to a range of different recipients. Otherwise, an Alert for *any* node in the Relator will be sent to the fixed and static 'To' email address. Instead, the 'To' field must be a node-specific variable

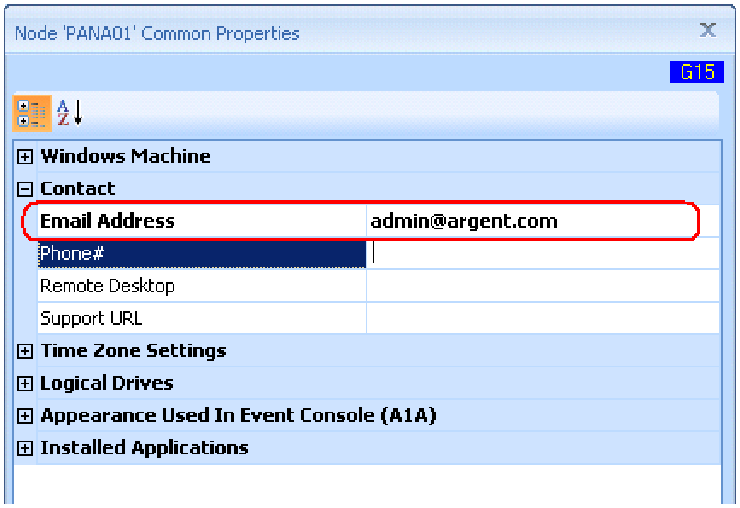
Therefore the variable '%DefaultNode%+a@a.com' does just that. Before the Argent Console engine fires the Alert, it sees %DefaultNode% in the To/CC field.
It then looks up the CMDB-X to find out the contact email address for the node that breaks the rule. If the engine finds it, it use it as the To/CC email address. If the engine does not find it, it uses 'a@a.com' as fallback.

Do the following:

1. Assign the email address in the CMDB-X property **'Contact\Email Address'** of the servers/devices

2. Define email alert using '%DefaultNode%+some_backup_email_address' in the To/CC field

3. Use the Email Alert in the Relator that monitors all server/devices



Node 'PANA01' Common Properties

G15

⊞ **Windows Machine**
⊟ **Contact**

Email Address	**admin@argent.com**
Phone#	
Remote Desktop	
Support URL	

⊞ **Time Zone Settings**
⊞ **Logical Drives**
⊞ **Appearance Used In Event Console (A1A)**
⊞ **Installed Applications**

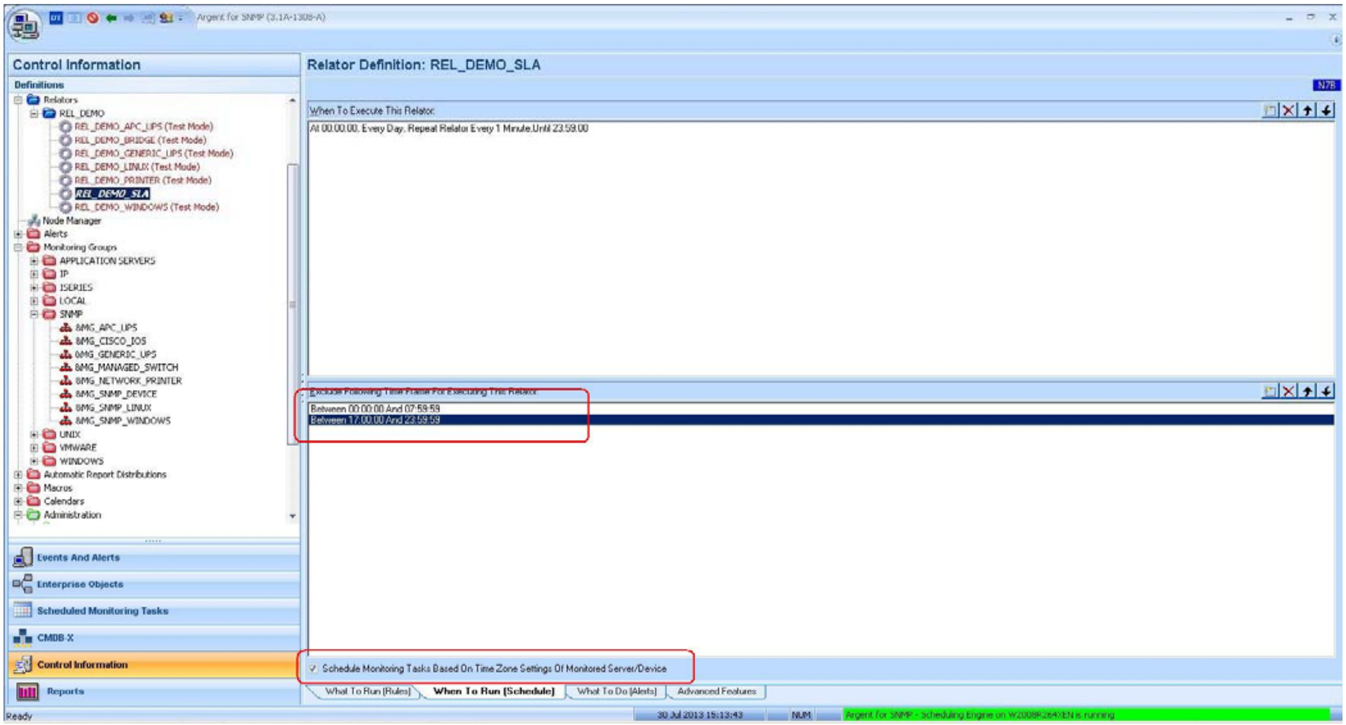
How Do I Monitor Server/Devices During Local Work Hours Only?

Do the following:

1. Configure the time zone settings for each relevant node first

2. In the Relator schedule, use **'Schedule Monitoring Task Based On Time Zone Settings Of Monitored Server/Device'** in the Relator

3. Define time exclusions, such as 00:00-07:59 and 17:00-23:59.



Relator Definition: REL_DEMO_SLA

When To Execute This Relator:

At 00.00.00, Every Day, Repeat Relator Every 1 Minute,Until 23.59.00

Exclude Following Time Frame For Executing This Relator:

Between 00:00:00 And 07:59:59
Between 17:00:00 And 23:59:59

☑ Schedule Monitoring Tasks Based On Time Zone Settings Of Monitored Server/Device

30 Jul 2013 15:13:43

Argent for SNMP - Scheduling Engine on W2008R264XEN is running

How Do I Detect Whether Application ‘XXX’ Is Installed?

Most Windows applications always leave some footprint in registry.

Server programs are generally installed as Windows services.

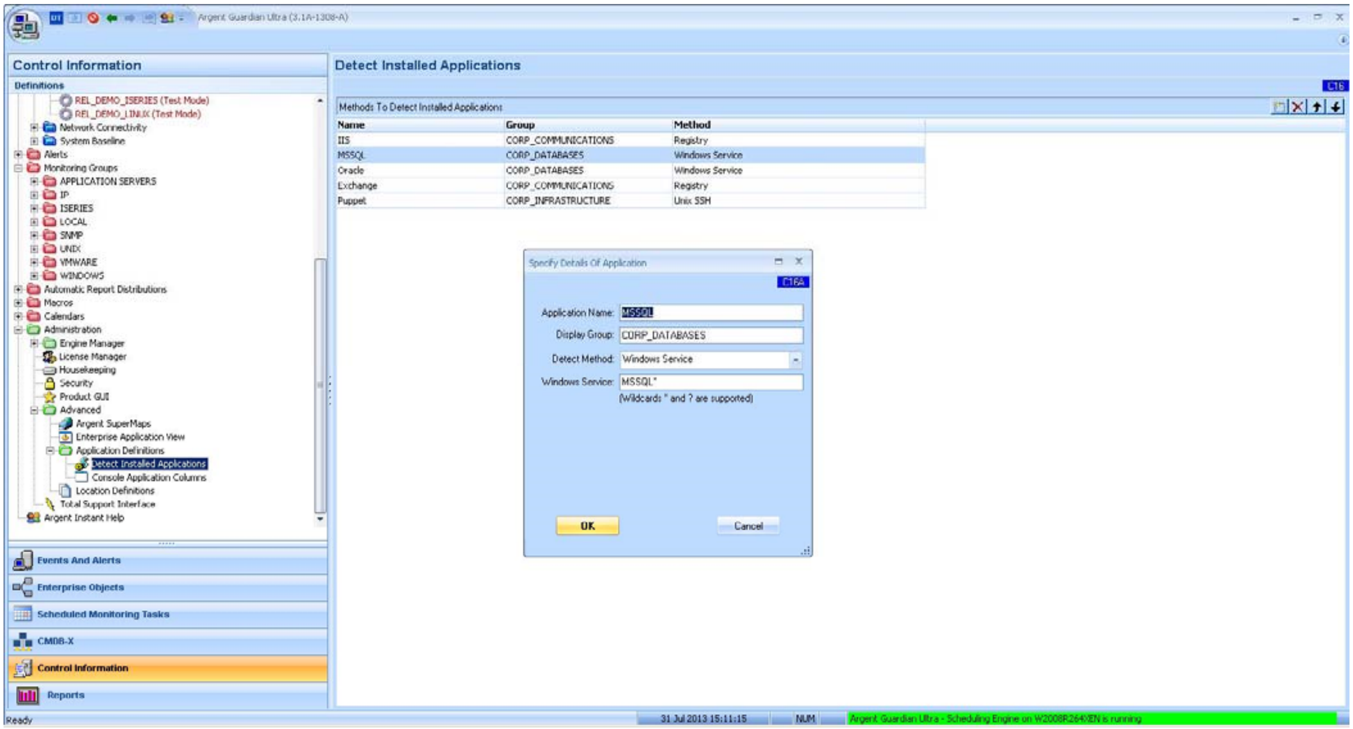
Application detection can be defined either by using the Windows Registry or Windows Service method.

For rare exceptions, use the VBScript method to implement any kind of custom logic.

For Linux/Unix application, the easiest way is to use the TCP Service method.

Using port scanning and simple chat, it is straightforward to pick up well known TCP services such SSH, Telnet, SMTP, POP3, IMAP, HTTP/HTTPS etc.

For applications not exposed to a TCP port, SSH or Telnet method can be used to physically logon to the box to check the existence of running processes.



Detect Installed Applications

Methods To Detect Installed Applications

Name	Group	Method
IIS	CORP_COMMUNICATIONS	Registry
MSSQL	CORP_DATABASES	Windows Service
Oracle	CORP_DATABASES	Windows Service
Exchange	CORP_COMMUNICATIONS	Registry
Puppet	CORP_INFRASTRUCTURE	Unix SSH

Specify Details Of Application

Application Name: MSSQL

Display Group: CORP_DATABASES

Detect Method: Windows Service

Windows Service: MSSQL*

(Wildcards * and ? are supported)

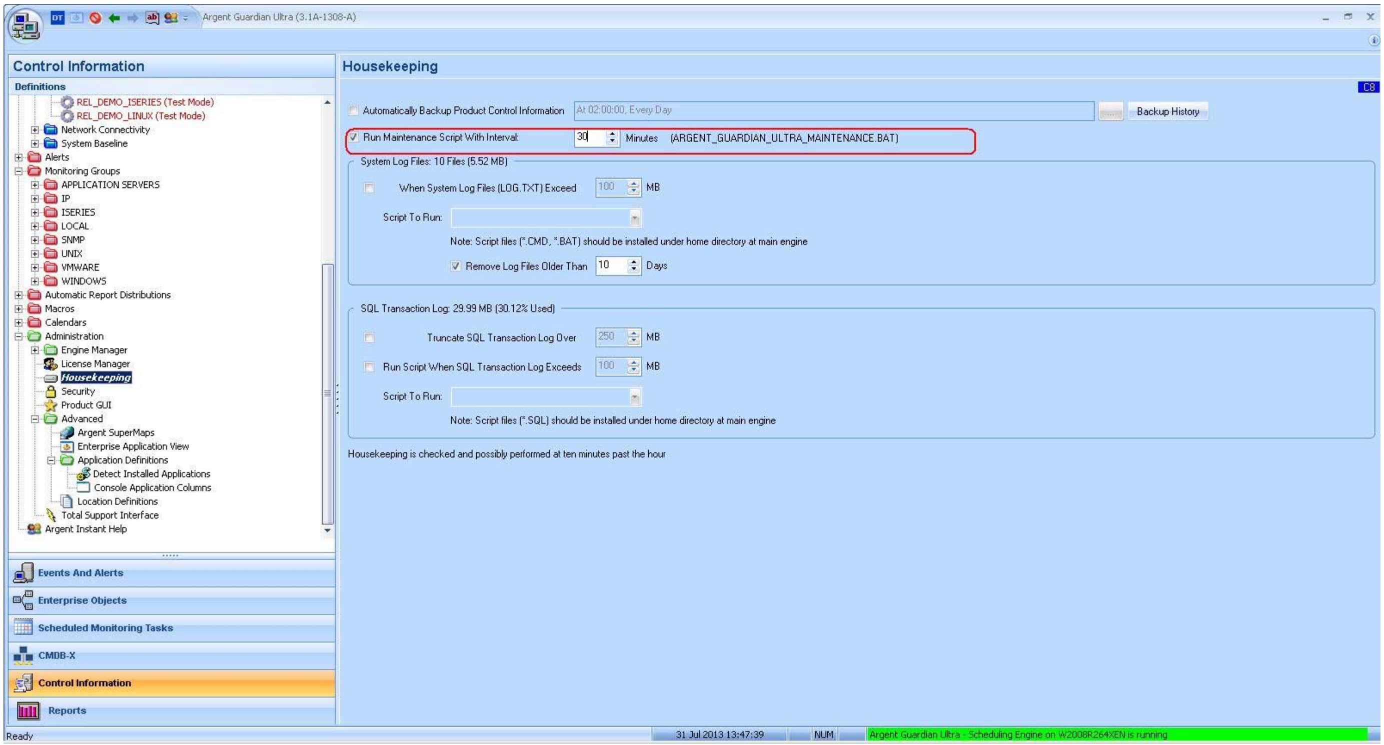
How Do I Automate Application Detection?

The Argent AT Command Line can run application detection at the command line.

For example, the following command line can pick up applications including Linux/Unix servers and SNMP devices.

```
ARGENT_DETECTAPP_CLI    -all -user user -pswd pswd -snmp v1 -comm public
```

Put the command line in a product maintenance script, and configure it to run once every x minutes.



Housekeeping

□ Automatically Backup Product Control Information: At 02:00:00, Every Day

☑ Run Maintenance Script With Interval: 30 Minutes (ARGENT_GUARDIAN_ULTRA_MAINTENANCE.BAT)

System Log Files: 10 Files (5.52 MB)

□ When System Log Files (LOG.TXT) Exceed 100 MB

Script To Run:

Note: Script files (*.CMD, *.BAT) should be installed under home directory at main engine

☑ Remove Log Files Older Than 10 Days

SQL Transaction Log: 29.99 MB (30.12% Used)

□ Truncate SQL Transaction Log Over 250 MB

□ Run Script When SQL Transaction Log Exceeds 100 MB

Script To Run:

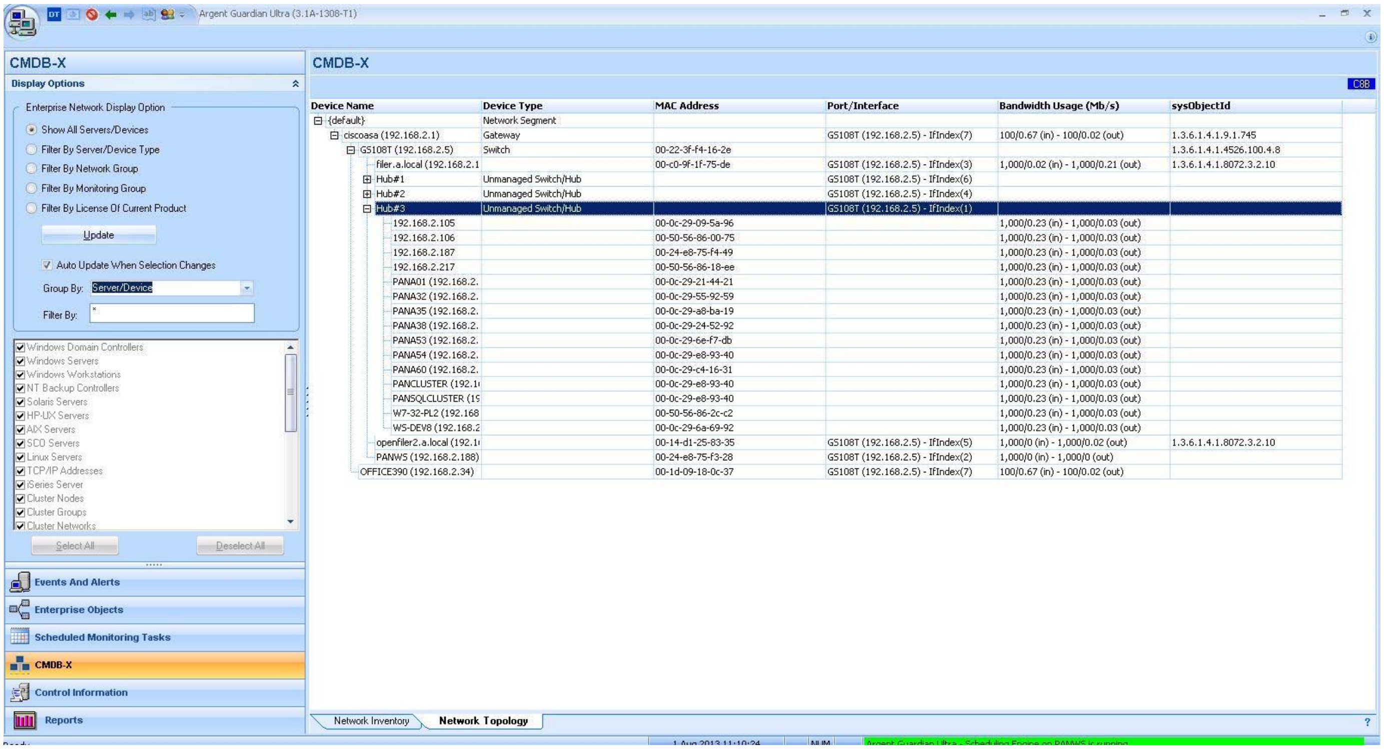
Note: Script files (*.SQL) should be installed under home directory at main engine

Housekeeping is checked and possibly performed at ten minutes past the hour

How Do I Determine My Network Topology?

Argent Atlas supports network topology generation.

There is an option to scan network topology by polling SNMP managed switches, as well as to maintain topology manually.



Enterprise Network Display Option

- ● Show All Servers/Devices
- ○ Filter By Server/Device Type
- ○ Filter By Network Group
- ○ Filter By Monitoring Group
- ○ Filter By License Of Current Product

☑ Auto Update When Selection Changes

Group By: Server/Device

Filter By: *

- ☑ Windows Domain Controllers
- ☑ Windows Servers
- ☑ Windows Workstations
- ☑ NT Backup Controllers
- ☑ Solaris Servers
- ☑ HP-UX Servers
- ☑ AIX Servers
- ☑ SCO Servers
- ☑ Linux Servers
- ☑ TCP/IP Addresses
- ☑ iSeries Server
- ☑ Cluster Nodes
- ☑ Cluster Groups
- ☑ Cluster Networks

Device Name	Device Type	MAC Address	Port/Interface	Bandwidth Usage (Mb/s)	sysObjectId
⊟ {default}	Network Segment				
⊟ ciscoasa (192.168.2.1)	Gateway		GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	1.3.6.1.4.1.9.1.745
⊟ GS108T (192.168.2.5)	Switch	00-22-3f-f4-16-2e			1.3.6.1.4.1.4526.100.4.8
filer.a.local (192.168.2.1		00-c0-9f-1f-75-de	GS108T (192.168.2.5) - IfIndex(3)	1,000/0.02 (in) - 1,000/0.21 (out)	1.3.6.1.4.1.8072.3.2.10
⊞ Hub#1	Unmanaged Switch/Hub		GS108T (192.168.2.5) - IfIndex(6)		
⊞ Hub#2	Unmanaged Switch/Hub		GS108T (192.168.2.5) - IfIndex(4)		
⊟ Hub#3	Unmanaged Switch/Hub		GS108T (192.168.2.5) - IfIndex(1)		
192.168.2.105		00-0c-29-09-5a-96		1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.106		00-50-56-86-00-75		1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.187		00-24-e8-75-f4-49		1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.217		00-50-56-86-18-ee		1,000/0.23 (in) - 1,000/0.03 (out)	
PANA01 (192.168.2.		00-0c-29-21-44-21		1,000/0.23 (in) - 1,000/0.03 (out)	
PANA32 (192.168.2.		00-0c-29-55-92-59		1,000/0.23 (in) - 1,000/0.03 (out)	
PANA35 (192.168.2.		00-0c-29-a8-ba-19		1,000/0.23 (in) - 1,000/0.03 (out)	
PANA38 (192.168.2.		00-0c-29-24-52-92		1,000/0.23 (in) - 1,000/0.03 (out)	
PANA53 (192.168.2.		00-0c-29-6e-f7-db		1,000/0.23 (in) - 1,000/0.03 (out)	
PANA54 (192.168.2.		00-0c-29-e8-93-40		1,000/0.23 (in) - 1,000/0.03 (out)	
PANA60 (192.168.2.		00-0c-29-c4-16-31		1,000/0.23 (in) - 1,000/0.03 (out)	
PANCLUSTER (192.1		00-0c-29-e8-93-40		1,000/0.23 (in) - 1,000/0.03 (out)	
PANSQLCLUSTER (19		00-0c-29-e8-93-40		1,000/0.23 (in) - 1,000/0.03 (out)	
W7-32-PL2 (192.168		00-50-56-86-2c-c2		1,000/0.23 (in) - 1,000/0.03 (out)	
WS-DEV8 (192.168.2		00-0c-29-6a-69-92		1,000/0.23 (in) - 1,000/0.03 (out)	
openfiler2.a.local (192.1		00-14-d1-25-83-35	GS108T (192.168.2.5) - IfIndex(5)	1,000/0 (in) - 1,000/0.02 (out)	1.3.6.1.4.1.8072.3.2.10
PANWS (192.168.2.188)		00-24-e8-75-f3-28	GS108T (192.168.2.5) - IfIndex(2)	1,000/0 (in) - 1,000/0 (out)	
OFFICE390 (192.168.2.34)		00-1d-09-18-0c-37	GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	

How Can The MAC Address Of A Switch Be Determined?

The Argent Atlas Network Topology shows the MAC address in the column “MAC Address”.

How Can A DMZ Topology Be Added To Argent Atlas?

If the DMZ topology cannot be directly added by the Argent AT engine due to router settings, do the following:

1: Copy ARGSOFT_SNMP_TOPOLOGY.EXE to any machine in the DMZ

2: Run ARGSOFT_SNMP_TOPOLOGY.EXE generating found_snmp_topology.xml

3: Import found_snmp_topology.xml into Network Topology

This topic is about discovering network topology.

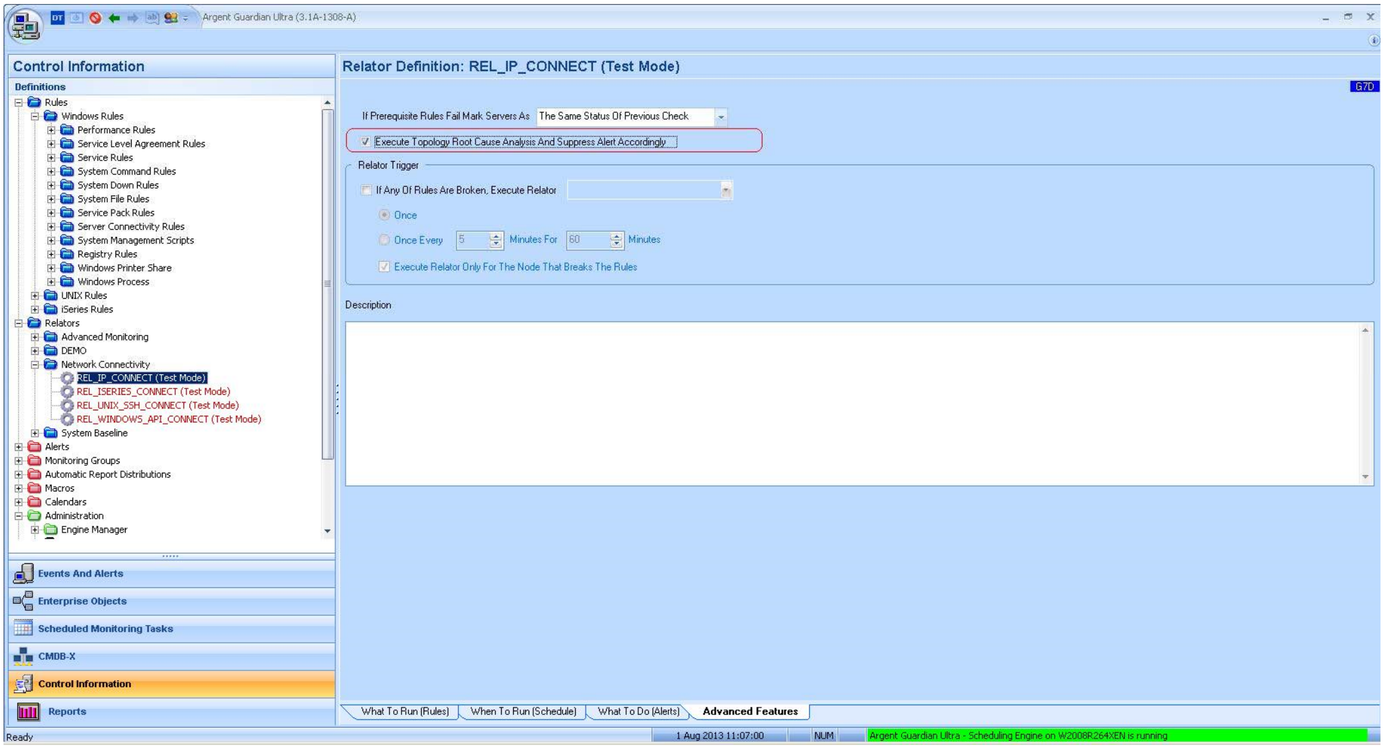
Also see “There are Many Devices in the DMZ; They Cannot Be Scanned By The Argent AT Engine; There Are Too Many To Add Manually.”, which is about discovering all active IP devices.

How Can All the SNMP Devices In The Network Be Determined Without Installing Argent For SNMP?

See topic, “How Can A DMZ Topology Be Added To Argent Atlas” and use the same approach of importing the generated found_snmp_topology.xml file.

I Have Been Alerted With A Flood Of Alerts When A Switch Went Bad. How Can Argent AT Just Tell Me That Switch Is Bad?

Turn on the option Execute Topology Root Cause Analysis And Suppress Alert Accordingly in the Relator.



Relator Definition: REL_IP_CONNECT (Test Mode)

If Prerequisite Rules Fail Mark Servers As: The Same Status Of Previous Check

☑ Execute Topology Root Cause Analysis And Suppress Alert Accordingly

Relator Trigger

☐ If Any Of Rules Are Broken, Execute Relator

● Once

○ Once Every 5 Minutes For 60 Minutes

☑ Execute Relator Only For The Node That Breaks The Rules

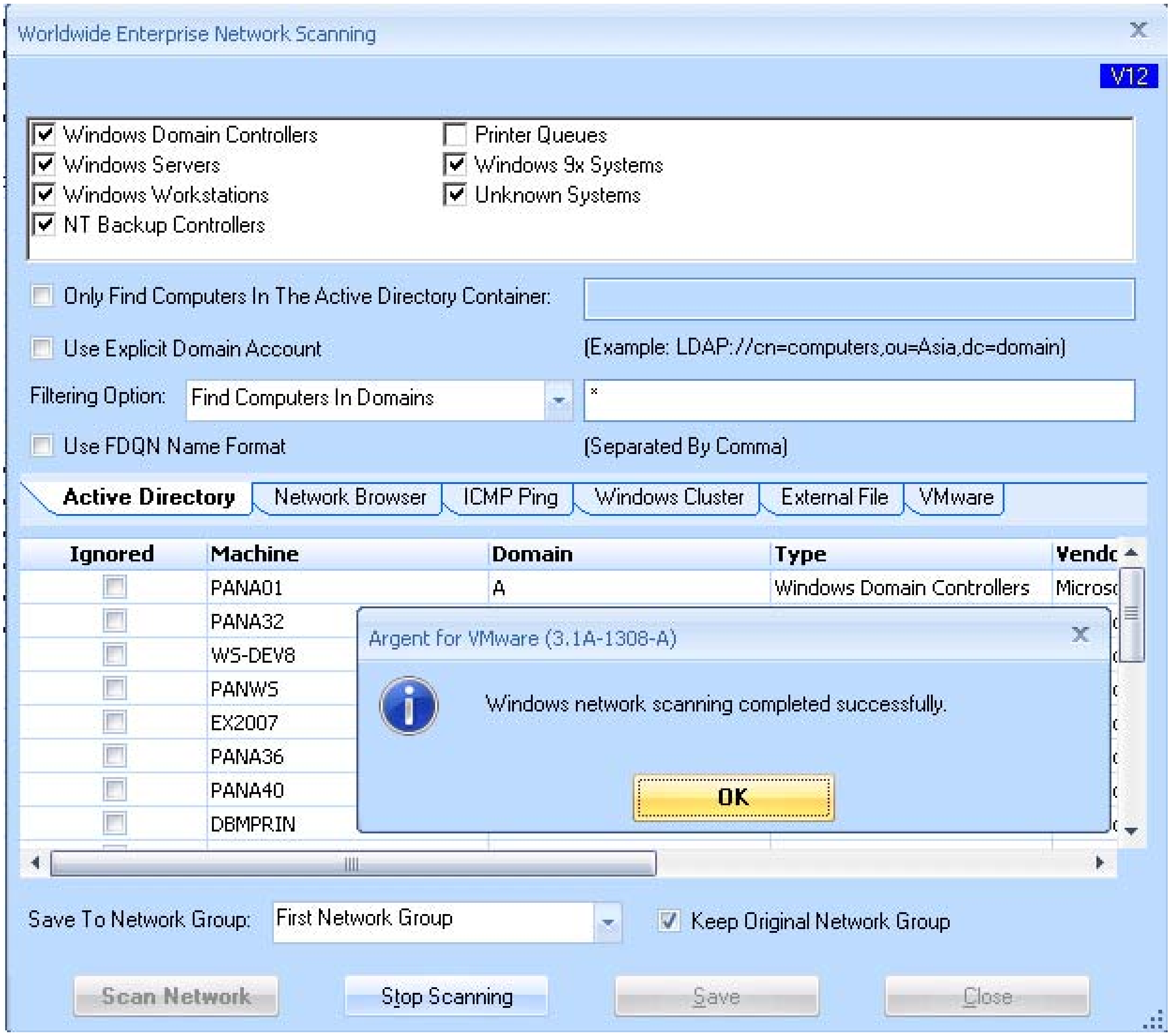
Description

Root cause analysis relies on the topology dependency being accurate. Therefore it is essential to maintain the accuracy of the network topology by using Argent's automatic scanning facilities. Discuss with an Argent engineer to learn more about these facilities.

Appendix A – Networking Scanning

Scan Windows Network Using Active Directory

The most convenient way to add a bulk of server/devices into Argent Atlas is to scan the network.



Worldwide Enterprise Network Scanning

V12

- ☑ Windows Domain Controllers
- ☑ Windows Servers
- ☑ Windows Workstations
- ☑ NT Backup Controllers
- □ Printer Queues
- ☑ Windows 9x Systems
- ☑ Unknown Systems

□ Only Find Computers In The Active Directory Container:

□ Use Explicit Domain Account

(Example: LDAP://cn=computers,ou=Asia,dc=domain)

Filtering Option: Find Computers In Domains

*

□ Use FDQN Name Format

(Separated By Comma)

Ignored	Machine	Domain	Type	Vendo
□	PANA01	A	Windows Domain Controllers	Microso
□	PANA32			
□	WS-DEV8			
□	PANWS			
□	EX2007			
□	PANA36			
□	PANA40			
□	DBMPRIN			

Argent for VMware (3.1A-1308-A)

Windows network scanning completed successfully.

Save To Network Group: First Network Group

☑ Keep Original Network Group

Scanning Options

Save To Network Group

Specifies the Network Group that the scanning result will be save to.

Keep Original Network Group

If a found server/device is already in the CMDB-X, it will be moved to a new Network Group specified in **'Save To Network Group'** with this option unchecked. The default is checked.

Only Find Computers In The Active Directory Container

This option can be useful for a very big Active Directory network, where a specific container can be targeted

Filter Option

Customers can specify whether to find computers for specific domains.

Use FDQN Name Format

Some networks require FDQN name due to DNS configuration. For example, if the option is checked, machine 'PANA01' is saved as 'pana01.a.local'.

Use Explicit Domain Account

This option is useful when the Argent AT engine is in a workgroup, or customers try to scan computers at another domain. Customers need to enter the logon credentials and domain controller before the actual scanning.

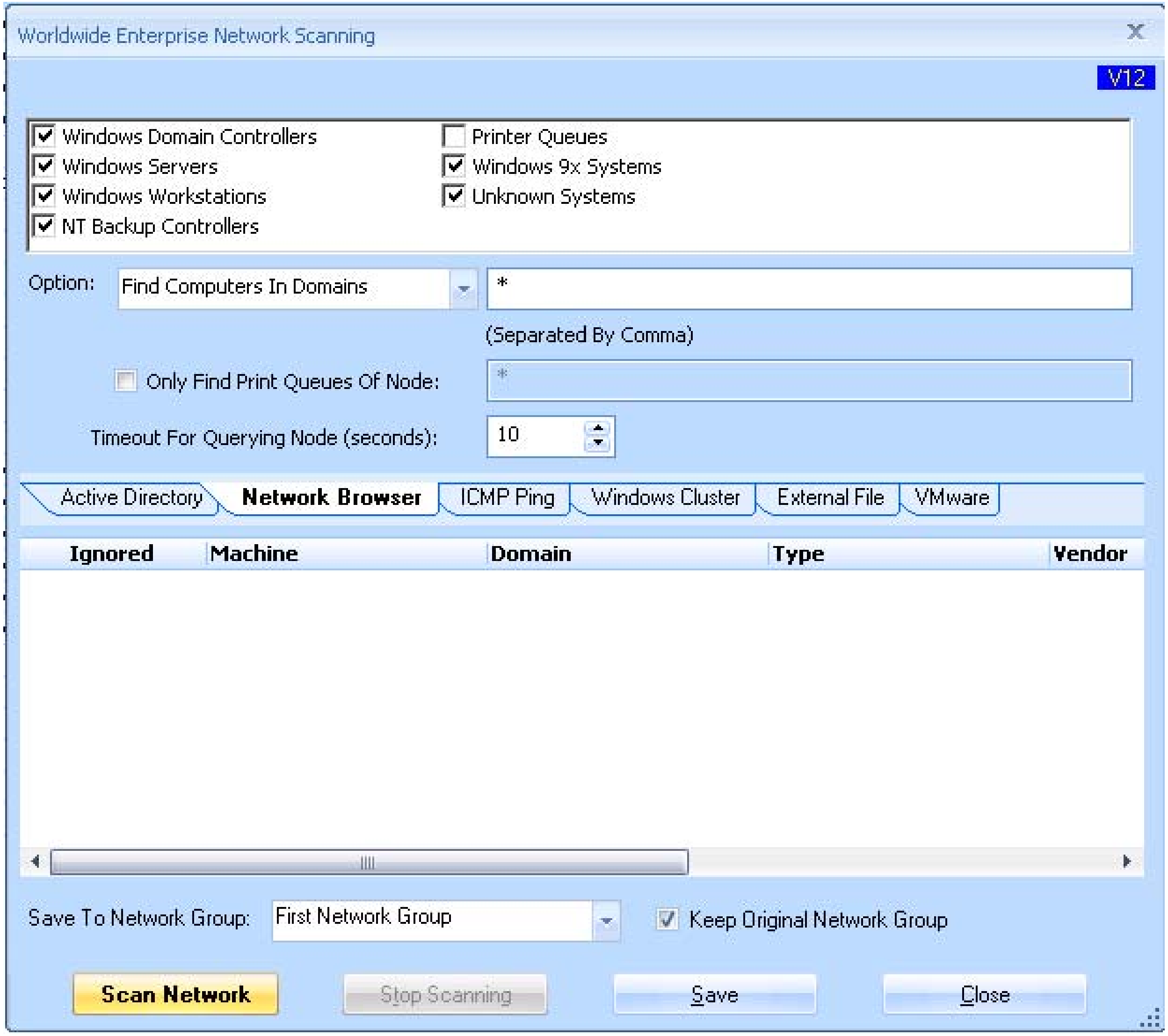
Scan Windows Network Using Network Browser

Using Network Browser is another method to scan Windows network.

It is useful for workgroup environments.

It is not recommended for Domain environments, as it is less reliable than the Active Directory method.

All scanning options on screen are self-explanatory.



Worldwide Enterprise Network Scanning

V12

☑ Windows Domain Controllers
☑ Windows Servers
☑ Windows Workstations
☑ NT Backup Controllers
☐ Printer Queues
☑ Windows 9x Systems
☑ Unknown Systems

Option: Find Computers In Domains | *

(Separated By Comma)

☐ Only Find Print Queues Of Node: *

Timeout For Querying Node (seconds): 10

Ignored	Machine	Domain	Type	Vendor

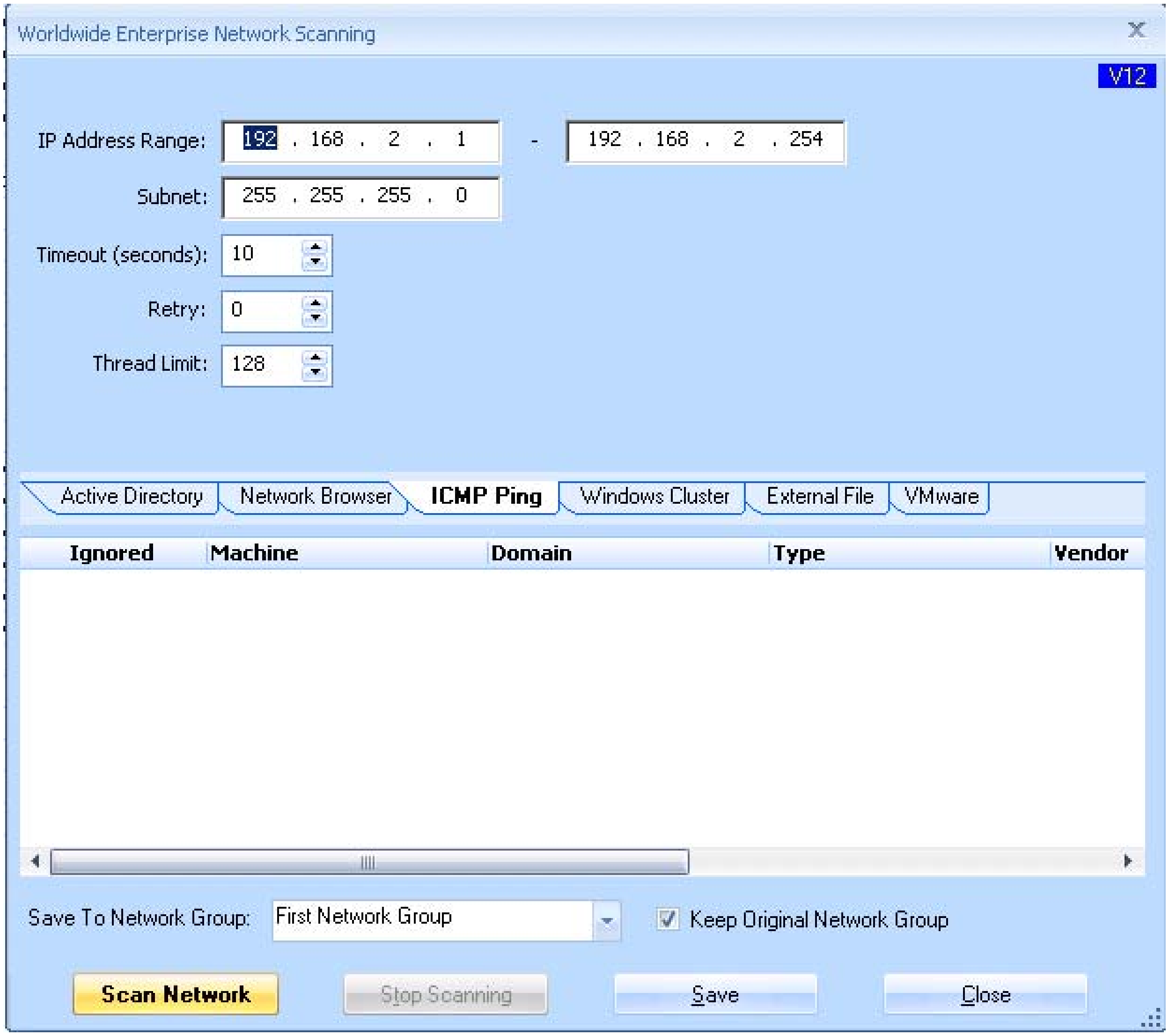
Save To Network Group: First Network Group

☑ Keep Original Network Group

Scan TCP/IP Network Using ICMP Ping

This method scans the whole TCP/IP network segment by pinging each possible IP address in the segment.

All scanning options on screen are self-explanatory.



IP Address Range: 192 . 168 . 2 . 1 - 192 . 168 . 2 . 254

Subnet: 255 . 255 . 255 . 0

Timeout (seconds): 10

Retry: 0

Thread Limit: 128

Save To Network Group: First Network Group

☑ Keep Original Network Group

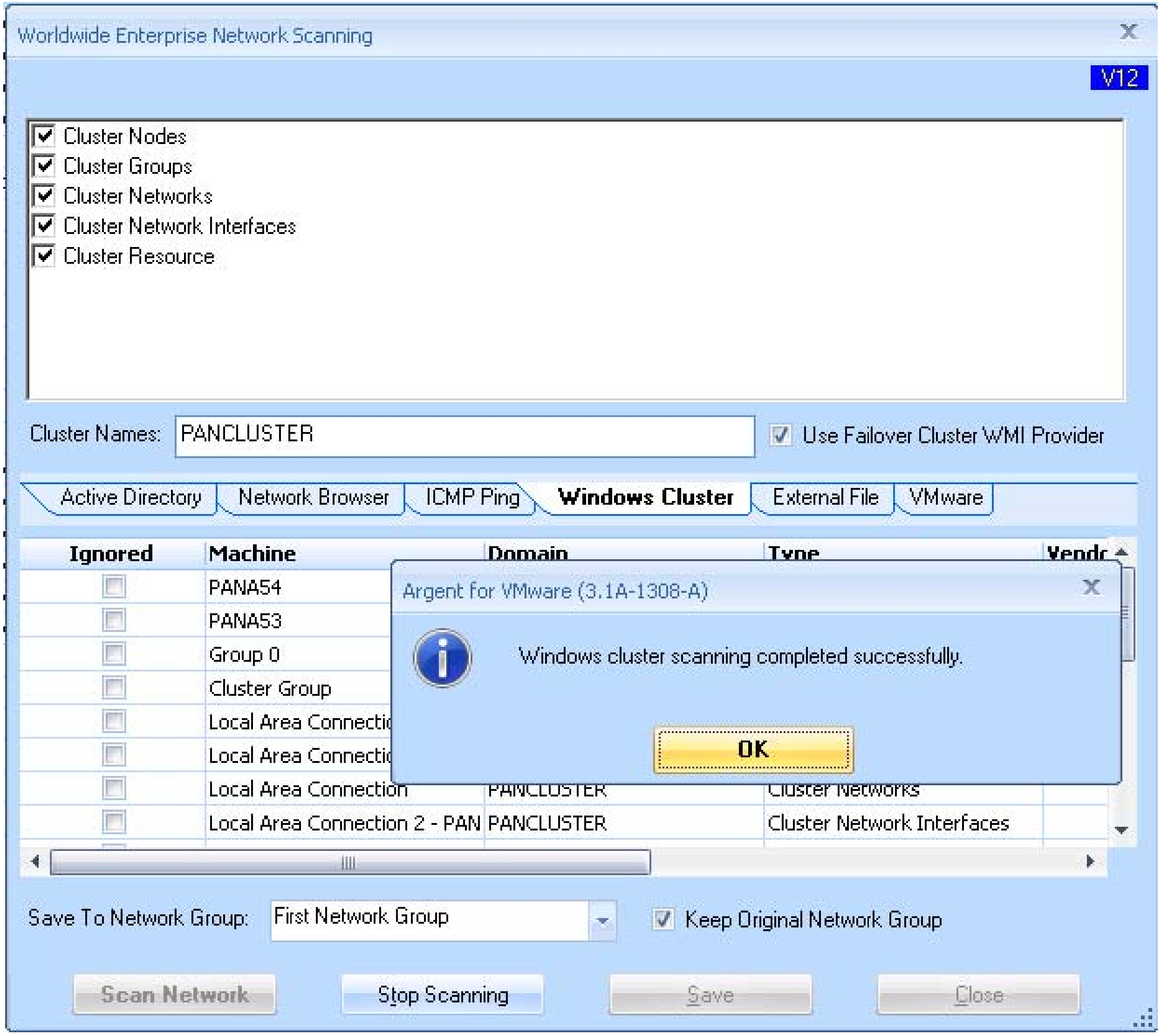
Scan Windows Cluster Objects

Argent AT scans Windows Cluster Objects using either native WIN32 API or Failover Cluster WMI Provider.

Native WIN32 API is faster but requires both Argent AT engine and Windows Cluster run the same Windows operating system -- Cluster API on W2003 works only for W2003 cluster. Cluster API on W2008 works only for W2008 cluster. If customer has mixed cluster versions, or AT on W2008 and cluster is W2003, native API won't work.

"Failover Cluster WMI Provider" works for all Windows versions. But it requires the Windows Cluster to allow the Argent AT service account access to its WMI name space 'root\mscluster'.

It is recommended to use '**Failover Cluster WMI Provider'** in a mixed W2003 and W2008 environment.



Worldwide Enterprise Network Scanning

V12

☑ Cluster Nodes
☑ Cluster Groups
☑ Cluster Networks
☑ Cluster Network Interfaces
☑ Cluster Resource

Cluster Names: PANCLUSTER

☑ Use Failover Cluster WMI Provider

Ignored	Machine	Domain	Type	Vendc
□	PANA54			
□	PANA53			
□	Group 0			
□	Cluster Group			
□	Local Area Connectic			
□	Local Area Connectic			
□	Local Area Connection	PANCLUSTER	Cluster Networks	
□	Local Area Connection 2 - PAN	PANCLUSTER	Cluster Network Interfaces	

Argent for VMware (3.1A-1308-A)

Windows cluster scanning completed successfully.

Save To Network Group: First Network Group

☑ Keep Original Network Group

Scan Network Using SNMP Discovery

Argent for SNMP discovers SNMP devices by querying well-known OIDs for each possible IP address in the specified network segment.

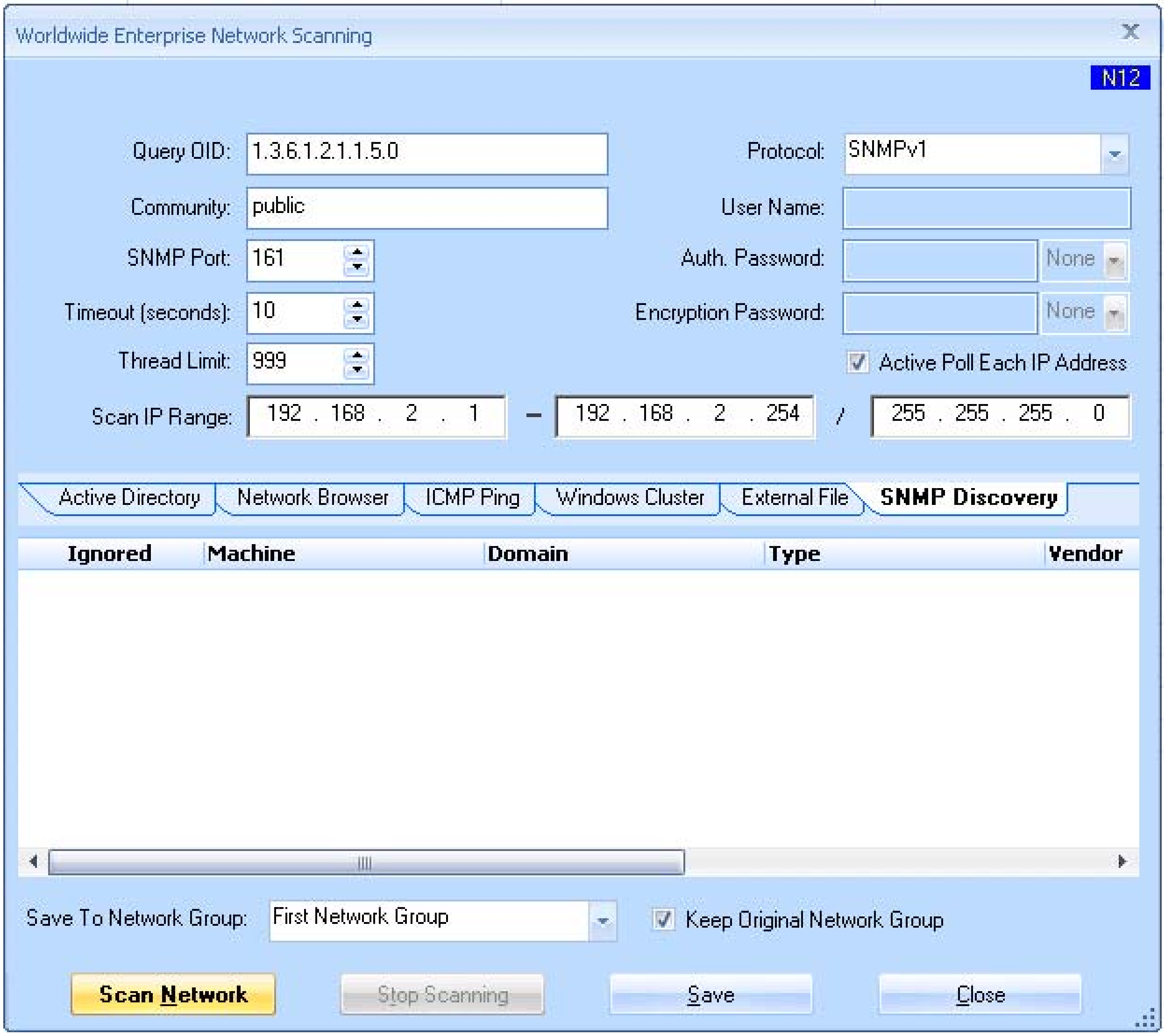
If it discovers nothing, customers should go through the following checklist:

1. Is the current machine a management workstation for SNMP devices? This has to be configured on each SNMP device. Contact the Network Administrator.

2. Is it the right SNMP protocol? v1, v2c or v3.

3. If it is SNMP v1 or v2c, is the community string specified correctly? Community string is like the password for SNMPv1 and v2c.

4. If it is SNMPv3, there are more passwords, authentication and encryption protocols to specify.



Worldwide Enterprise Network Scanning

N12

Query OID: 1.3.6.1.2.1.1.5.0

Protocol: SNMPv1

Community: public

User Name:

SNMP Port: 161

Auth. Password: None

Timeout (seconds): 10

Encryption Password: None

Thread Limit: 999

☑ Active Poll Each IP Address

Scan IP Range: 192 . 168 . 2 . 1 – 192 . 168 . 2 . 254 / 255 . 255 . 255 . 0

Ignored	Machine	Domain	Type	Vendor

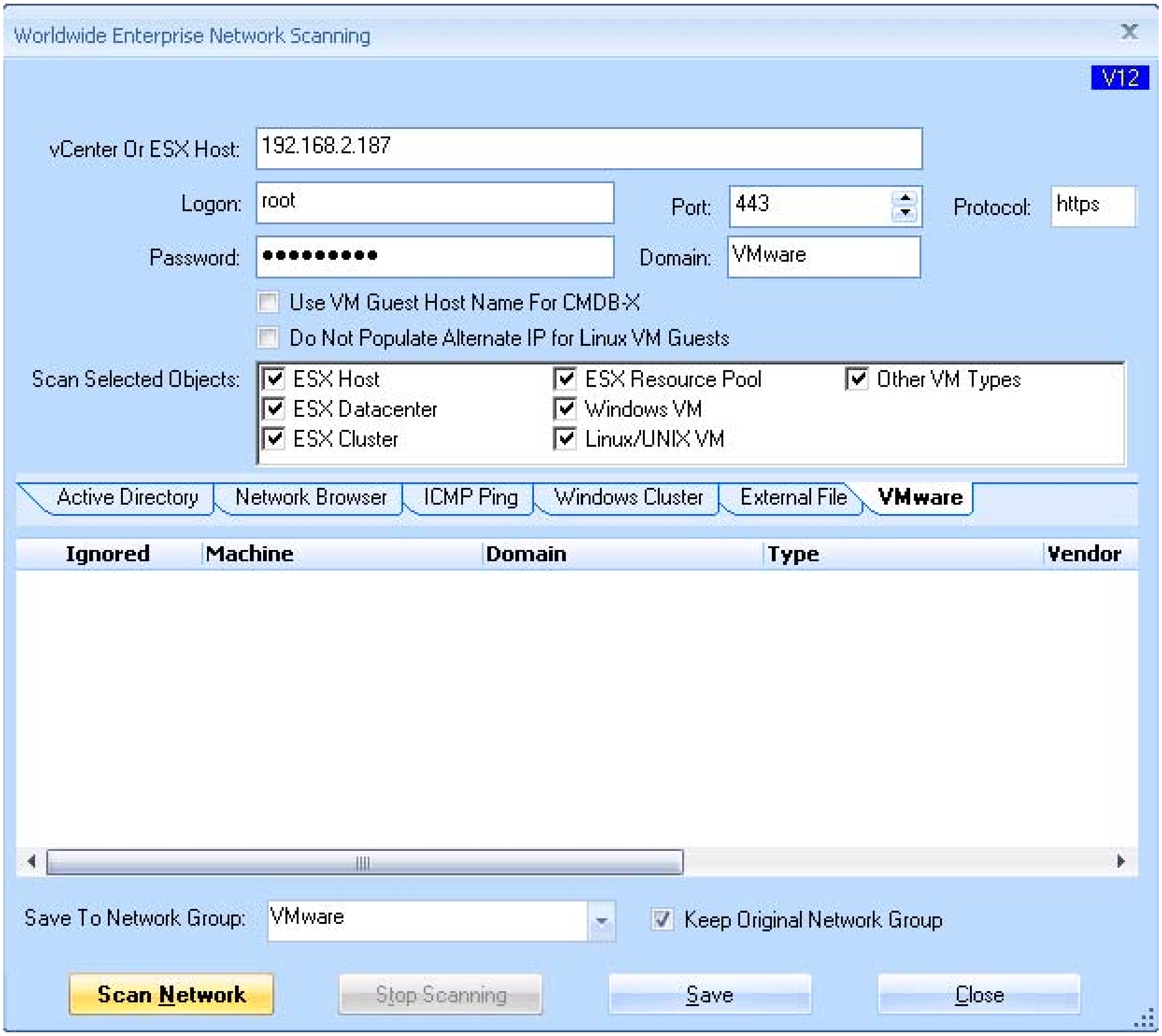
Save To Network Group: First Network Group

☑ Keep Original Network Group

Scan VMware Objects

Argent AT scans VMware objects through VMware PowerCLI.

It is easier to scan vCenter than individual ESX hosts, as it returns all objects on all included ESX hosts.



Worldwide Enterprise Network Scanning

vCenter Or ESX Host: 192.168.2.187

Logon: root

Port: 443

Protocol: https

Password: ●●●●●●●●●●

Domain: VMware

☐ Use VM Guest Host Name For CMDB-X

☐ Do Not Populate Alternate IP for Linux VM Guests

Scan Selected Objects:

- ☑ ESX Host
- ☑ ESX Datacenter
- ☑ ESX Cluster
- ☑ ESX Resource Pool
- ☑ Windows VM
- ☑ Linux/UNIX VM
- ☑ Other VM Types

Ignored	Machine	Domain	Type	Vendor

Save To Network Group: VMware

☑ Keep Original Network Group

Scanning Options

vCenter or ESX Host

This option determines where the result will be read from.

Logon/Password

Logon credential for PowerCLI session.

Port

TCP/IP port used by PowerCLI session. The default value is 443.

Protocol

The web service protocol. It is either ‘https’ or ‘http’.

Domain

It specifies the domain of found VMware object. The default value is ‘VMware’.

Use VM Guest Host Name For CMDB-X

VM name can be different from the VM guest host name.

For example, a VM machine named ‘W2008R2DEV 212/212’ has the host name ‘W2008R2DEV’.

The VM machine name is defined in VMware Sphere, while host name is specified when the OS is installed.

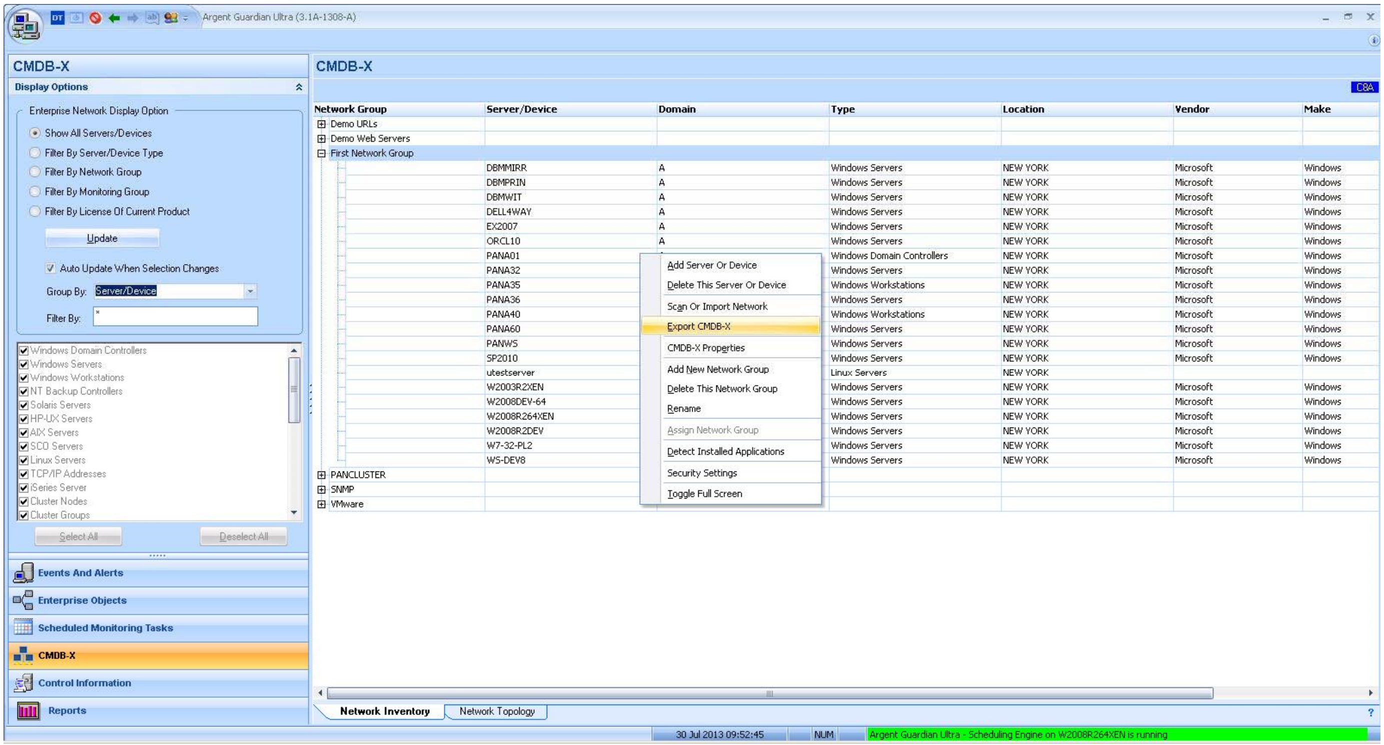
Do Not Populate Alternative IP for Linux Guest VM

Alternative IP field is not filled for Linux VM if this option is checked. It is useful when the VM has multiple NIC cards, and the customer does not want to use the main IP address.

Import And Export CMDB-X Data

Export CMDB-X Data

For backup purposes or exchanging data between installations, customers can export CMDB-X data to an XML file.



Argent Guardian Ultra (3.1A-1308-A)

CMDB-X

Display Options

Enterprise Network Display Option

● Show All Servers/Devices
○ Filter By Server/Device Type
○ Filter By Network Group
○ Filter By Monitoring Group
○ Filter By License Of Current Product

☑ Auto Update When Selection Changes

Group By: Server/Device

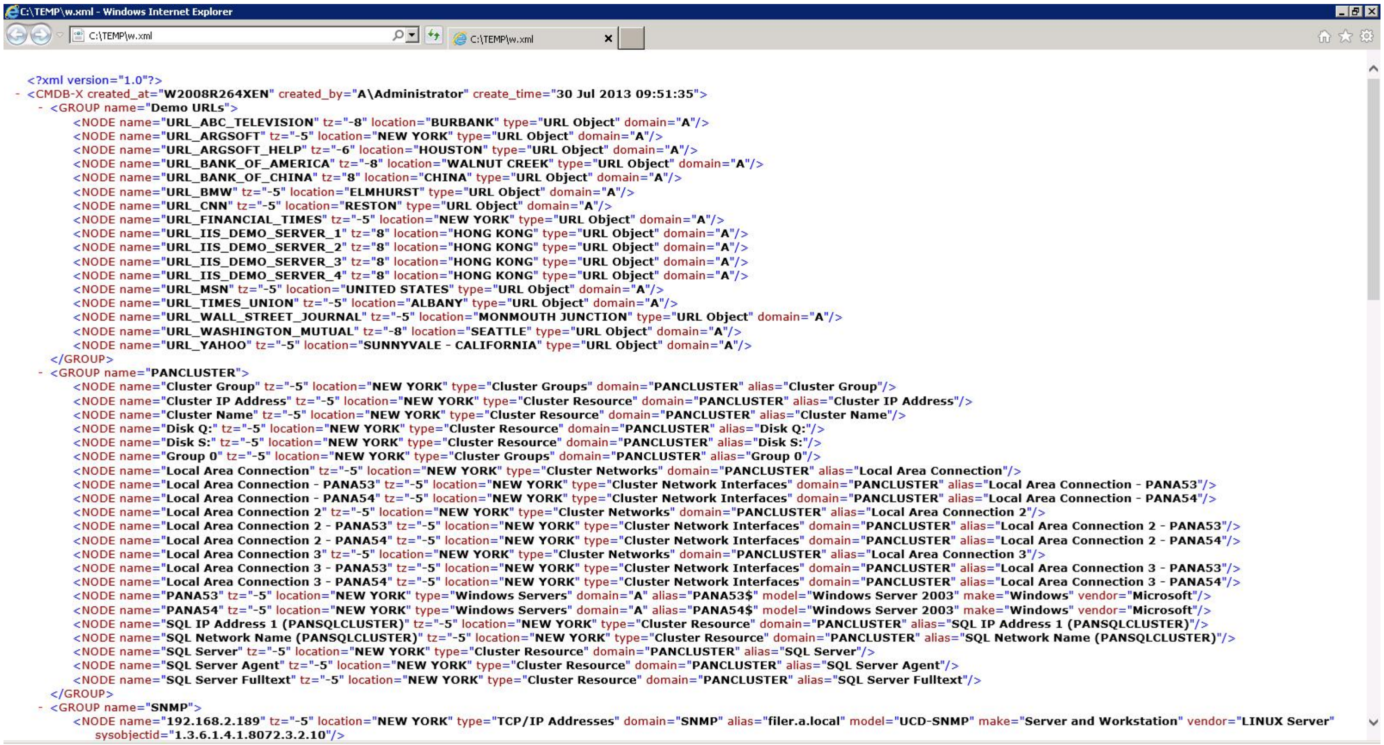
Filter By: *

☑ Windows Domain Controllers
☑ Windows Servers
☑ Windows Workstations
☑ NT Backup Controllers
☑ Solaris Servers
☑ HP-UX Servers
☑ AIX Servers
☑ SCO Servers
☑ Linux Servers
☑ TCP/IP Addresses
☑ iSeries Server
☑ Cluster Nodes
☑ Cluster Groups

Network Group	Server/Device	Domain	Type	Location	Vendor	Make
⊞ Demo URLs						
⊞ Demo Web Servers						
⊟ First Network Group						
	DBMMIRR	A	Windows Servers	NEW YORK	Microsoft	Windows
	DBMPRIN	A	Windows Servers	NEW YORK	Microsoft	Windows
	DBMWIT	A	Windows Servers	NEW YORK	Microsoft	Windows
	DELL4WAY	A	Windows Servers	NEW YORK	Microsoft	Windows
	EX2007	A	Windows Servers	NEW YORK	Microsoft	Windows
	ORCL10	A	Windows Servers	NEW YORK	Microsoft	Windows
	PANA01		Windows Domain Controllers	NEW YORK	Microsoft	Windows
	PANA32		Windows Servers	NEW YORK	Microsoft	Windows
	PANA35		Windows Workstations	NEW YORK	Microsoft	Windows
	PANA36		Windows Servers	NEW YORK	Microsoft	Windows
	PANA40		Windows Workstations	NEW YORK	Microsoft	Windows
	PANA60		Windows Servers	NEW YORK	Microsoft	Windows
	PANWS		Windows Servers	NEW YORK	Microsoft	Windows
	SP2010		Windows Servers	NEW YORK	Microsoft	Windows
	utestserver		Linux Servers	NEW YORK		
	W2003R2XEN		Windows Servers	NEW YORK	Microsoft	Windows
	W2008DEV-64		Windows Servers	NEW YORK	Microsoft	Windows
	W2008R264XEN		Windows Servers	NEW YORK	Microsoft	Windows
	W2008R2DEV		Windows Servers	NEW YORK	Microsoft	Windows
	W7-32-PL2		Windows Servers	NEW YORK	Microsoft	Windows
	WS-DEV8		Windows Servers	NEW YORK	Microsoft	Windows
⊞ PANCLUSTER						
⊞ SNMP						
⊞ VMware						

30 Jul 2013 09:52:45 | NUM | Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

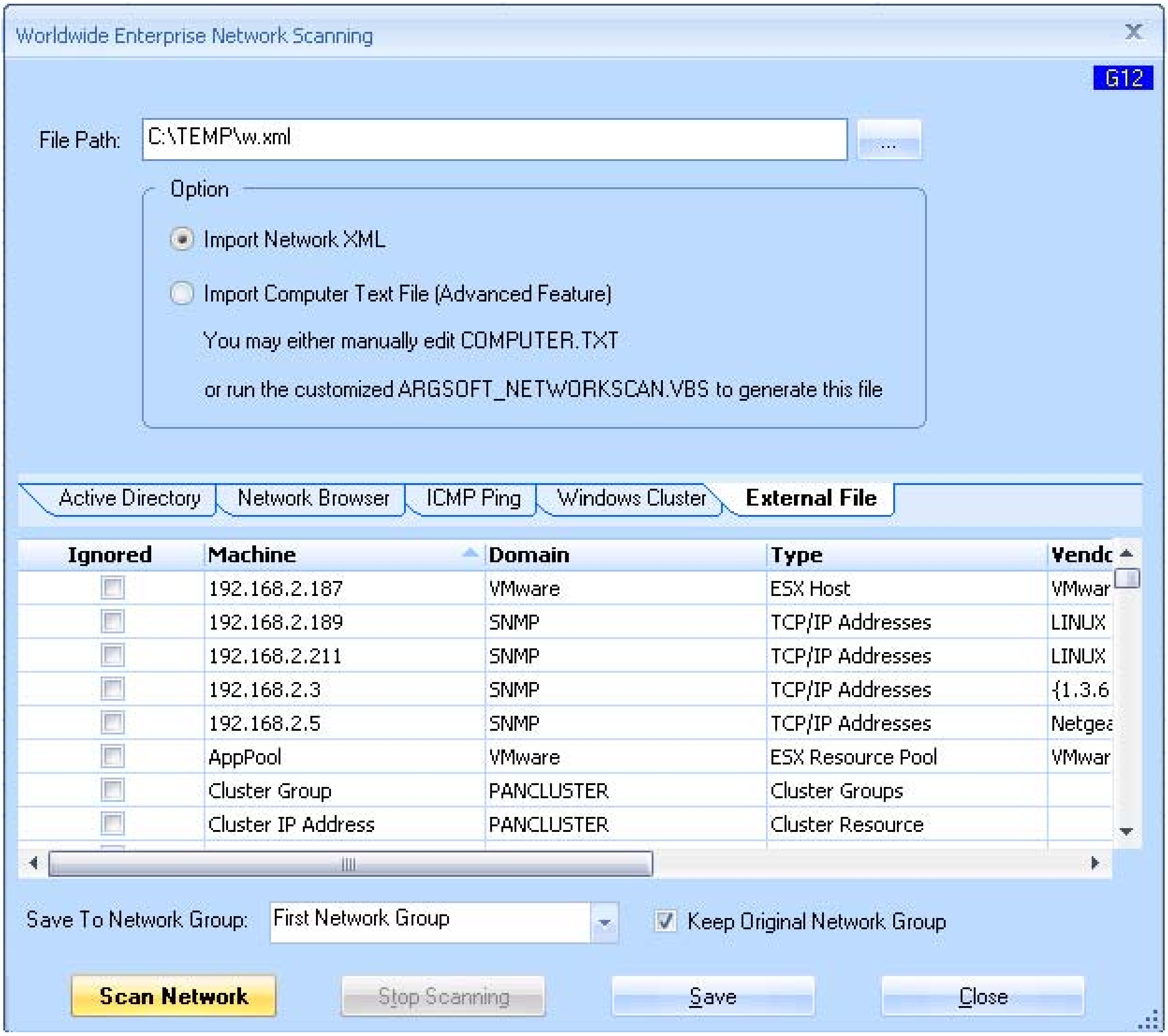
The exported CMDB-X data is stored in XML format. A sample XML is shown as follows:



```
  <?xml version="1.0"?>
- <CMDB-X created_at="W2008R264XEN" created_by="A\Administrator" create_time="30 Jul 2013 09:51:35">
  - <GROUP name="Demo URLs">
      <NODE name="URL_ABC_TELEVISION" tz="-8" location="BURBANK" type="URL Object" domain="A"/>
      <NODE name="URL_ARGSOFT" tz="-5" location="NEW YORK" type="URL Object" domain="A"/>
      <NODE name="URL_ARGSOFT_HELP" tz="-6" location="HOUSTON" type="URL Object" domain="A"/>
      <NODE name="URL_BANK_OF_AMERICA" tz="-8" location="WALNUT CREEK" type="URL Object" domain="A"/>
      <NODE name="URL_BANK_OF_CHINA" tz="8" location="CHINA" type="URL Object" domain="A"/>
      <NODE name="URL_BMW" tz="-5" location="ELMHURST" type="URL Object" domain="A"/>
      <NODE name="URL_CNN" tz="-5" location="RESTON" type="URL Object" domain="A"/>
      <NODE name="URL_FINANCIAL_TIMES" tz="-5" location="NEW YORK" type="URL Object" domain="A"/>
      <NODE name="URL_IIS_DEMO_SERVER_1" tz="8" location="HONG KONG" type="URL Object" domain="A"/>
      <NODE name="URL_IIS_DEMO_SERVER_2" tz="8" location="HONG KONG" type="URL Object" domain="A"/>
      <NODE name="URL_IIS_DEMO_SERVER_3" tz="8" location="HONG KONG" type="URL Object" domain="A"/>
      <NODE name="URL_IIS_DEMO_SERVER_4" tz="8" location="HONG KONG" type="URL Object" domain="A"/>
      <NODE name="URL_MSN" tz="-5" location="UNITED STATES" type="URL Object" domain="A"/>
      <NODE name="URL_TIMES_UNION" tz="-5" location="ALBANY" type="URL Object" domain="A"/>
      <NODE name="URL_WALL_STREET_JOURNAL" tz="-5" location="MONMOUTH JUNCTION" type="URL Object" domain="A"/>
      <NODE name="URL_WASHINGTON_MUTUAL" tz="-8" location="SEATTLE" type="URL Object" domain="A"/>
      <NODE name="URL_YAHOO" tz="-5" location="SUNNYVALE - CALIFORNIA" type="URL Object" domain="A"/>
    </GROUP>
  - <GROUP name="PANCLUSTER">
      <NODE name="Cluster Group" tz="-5" location="NEW YORK" type="Cluster Groups" domain="PANCLUSTER" alias="Cluster Group"/>
      <NODE name="Cluster IP Address" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="Cluster IP Address"/>
      <NODE name="Cluster Name" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="Cluster Name"/>
      <NODE name="Disk Q:" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="Disk Q:"/>
      <NODE name="Disk S:" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="Disk S:"/>
      <NODE name="Group 0" tz="-5" location="NEW YORK" type="Cluster Groups" domain="PANCLUSTER" alias="Group 0"/>
      <NODE name="Local Area Connection" tz="-5" location="NEW YORK" type="Cluster Networks" domain="PANCLUSTER" alias="Local Area Connection"/>
      <NODE name="Local Area Connection - PANA53" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection - PANA53"/>
      <NODE name="Local Area Connection - PANA54" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection - PANA54"/>
      <NODE name="Local Area Connection 2" tz="-5" location="NEW YORK" type="Cluster Networks" domain="PANCLUSTER" alias="Local Area Connection 2"/>
      <NODE name="Local Area Connection 2 - PANA53" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 2 - PANA53"/>
      <NODE name="Local Area Connection 2 - PANA54" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 2 - PANA54"/>
      <NODE name="Local Area Connection 3" tz="-5" location="NEW YORK" type="Cluster Networks" domain="PANCLUSTER" alias="Local Area Connection 3"/>
      <NODE name="Local Area Connection 3 - PANA53" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 3 - PANA53"/>
      <NODE name="Local Area Connection 3 - PANA54" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 3 - PANA54"/>
      <NODE name="PANA53" tz="-5" location="NEW YORK" type="Windows Servers" domain="A" alias="PANA53$" model="Windows Server 2003" make="Windows" vendor="Microsoft"/>
      <NODE name="PANA54" tz="-5" location="NEW YORK" type="Windows Servers" domain="A" alias="PANA54$" model="Windows Server 2003" make="Windows" vendor="Microsoft"/>
      <NODE name="SQL IP Address 1 (PANSQLCLUSTER)" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="SQL IP Address 1 (PANSQLCLUSTER)"/>
      <NODE name="SQL Network Name (PANSQLCLUSTER)" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="SQL Network Name (PANSQLCLUSTER)"/>
      <NODE name="SQL Server" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="SQL Server"/>
      <NODE name="SQL Server Agent" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="SQL Server Agent"/>
      <NODE name="SQL Server Fulltext" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="SQL Server Fulltext"/>
    </GROUP>
  - <GROUP name="SNMP">
      <NODE name="192.168.2.189" tz="-5" location="NEW YORK" type="TCP/IP Addresses" domain="SNMP" alias="filer.a.local" model="UCD-SNMP" make="Server and Workstation" vendor="LINUX Server"
         sysobjectid="1.3.6.1.4.1.8072.3.2.10"/>
```

Import CMDB-X Data

Use **'Scan Or Import Network'** to bring up network scanning dialog box, then select the tab **'External File'**.



Worldwide Enterprise Network Scanning

G12

File Path: C:\TEMP\w.xml

Option

● Import Network XML

○ Import Computer Text File (Advanced Feature)

You may either manually edit COMPUTER.TXT

or run the customized ARGSOFT_NETWORKSCAN.VBS to generate this file

Ignored	Machine	Domain	Type	Vendc
□	192.168.2.187	VMware	ESX Host	VMwar
□	192.168.2.189	SNMP	TCP/IP Addresses	LINUX
□	192.168.2.211	SNMP	TCP/IP Addresses	LINUX
□	192.168.2.3	SNMP	TCP/IP Addresses	{1.3.6
□	192.168.2.5	SNMP	TCP/IP Addresses	Netgea
□	AppPool	VMware	ESX Resource Pool	VMwar
□	Cluster Group	PANCLUSTER	Cluster Groups	
□	Cluster IP Address	PANCLUSTER	Cluster Resource	

Save To Network Group: First Network Group

☑ Keep Original Network Group

Use the option **'Import Network XML'** if the XML file is an exported XML file from Argent AT or Argent XT.

Argent AT can also import the nodes from a text file, which is very useful for importing from external sources such as SQL queries, Excel files, etc.

COMPUTERS.TXT Format

Each line consists of 5 fields separated by a TAB.

Field 1: Domain

Field 2: Server/Device Name

Field 3: Make

Field 4: Model

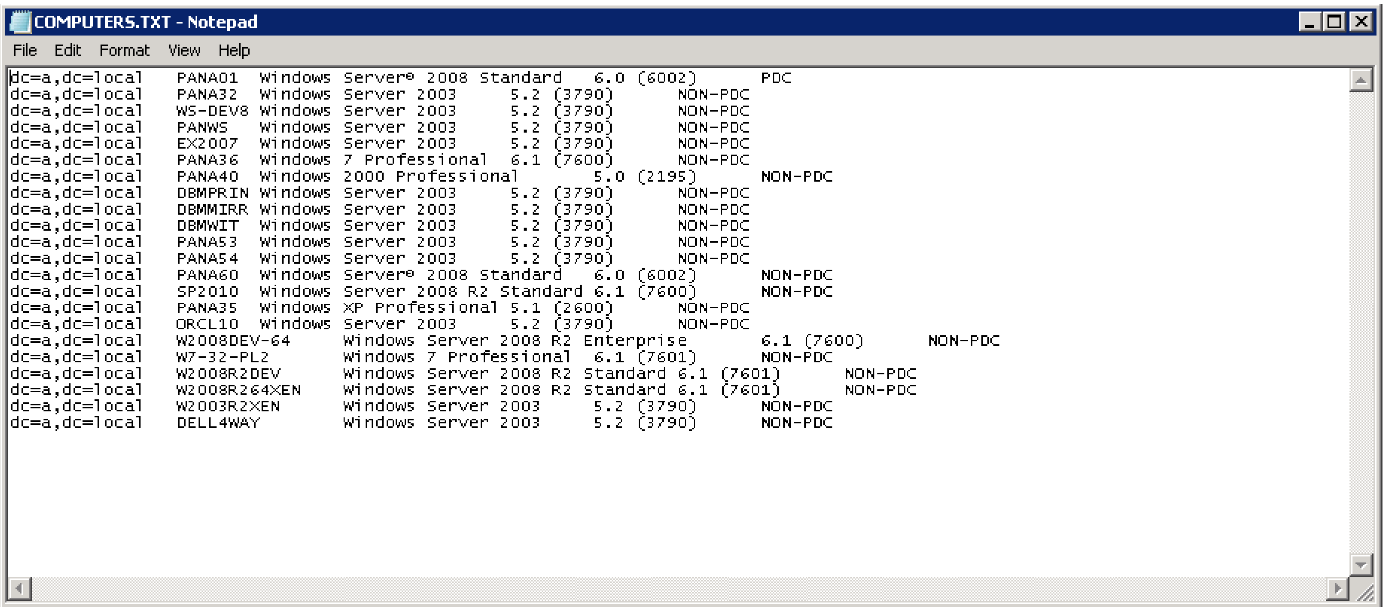
Field 5: Node Type.

It can be any of following:

- TCP or TCP/IP – IP Address
- SUNOS or SOLARIS – Sun Solaris OS
- HP-UX or HPUX – HP-UX OS
- AIX – AIX OS
- SCO – SCO Unix
- LINUX – Linux
- PDC – Windows Domain Controller

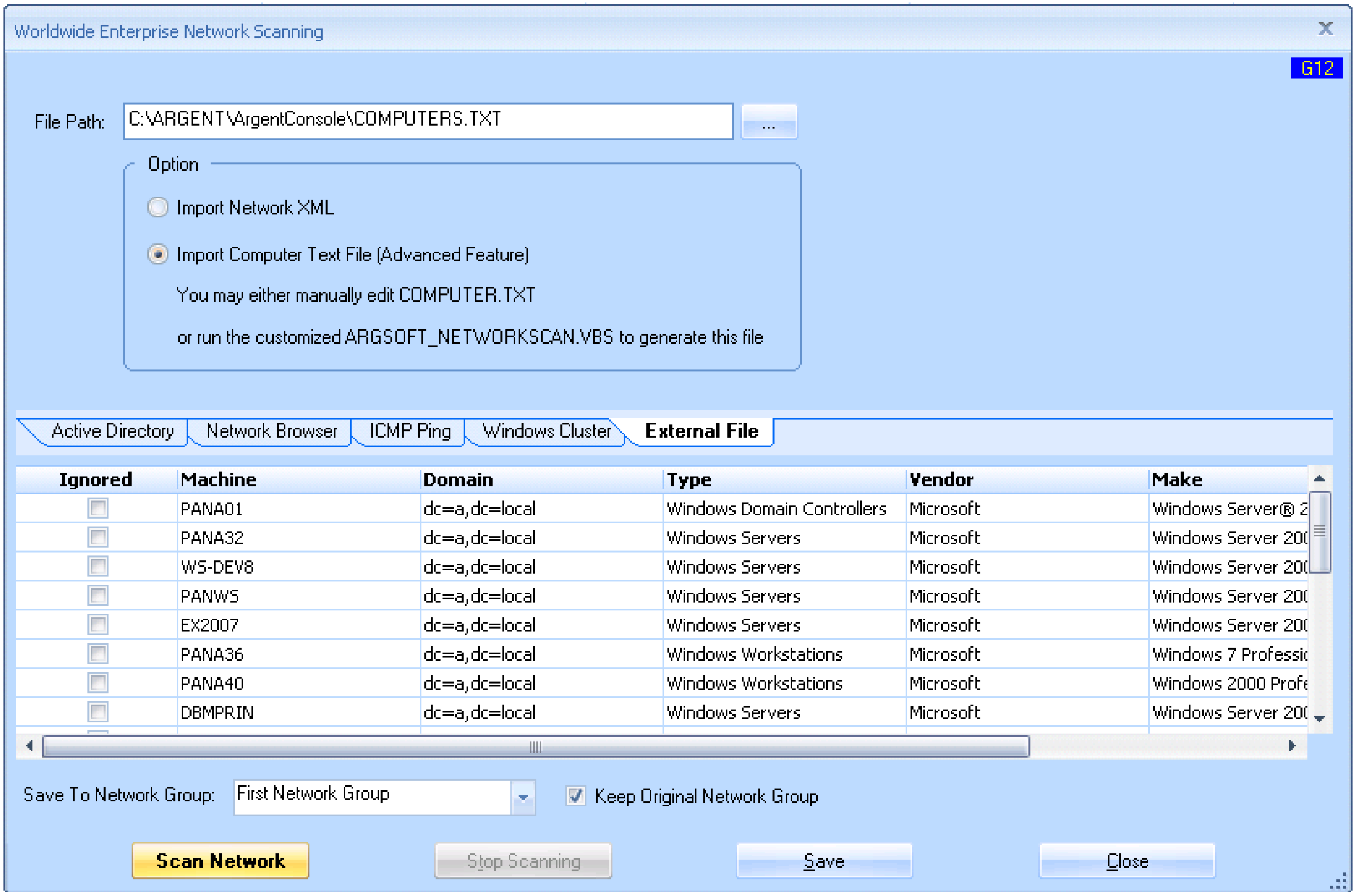
Note: if the string contains ‘Professional’ or ‘XP’, it is deemed as Windows Workstation, otherwise, Windows Server.

A sample COMPUTERS.TXT is shown as follows:



```
dc=a,dc=local   PANA01  Windows Server® 2008 Standard   6.0 (6002)      PDC
dc=a,dc=local   PANA32  Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   WS-DEV8 Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   PANWS   Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   EX2007  Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   PANA36  Windows 7 Professional  6.1 (7600)      NON-PDC
dc=a,dc=local   PANA40  Windows 2000 Professional       5.0 (2195)      NON-PDC
dc=a,dc=local   DBMPRIN Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   DBMMIRR Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   DBMWIT  Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   PANA53  Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   PANA54  Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   PANA60  Windows Server® 2008 Standard   6.0 (6002)      NON-PDC
dc=a,dc=local   SP2010  Windows Server 2008 R2 Standard 6.1 (7600)      NON-PDC
dc=a,dc=local   PANA35  Windows XP Professional 5.1 (2600)      NON-PDC
dc=a,dc=local   ORCL10  Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   W2008DEV-64     Windows Server 2008 R2 Enterprise       6.1 (7600)      NON-PDC
dc=a,dc=local   W7-32-PL2       Windows 7 Professional  6.1 (7601)      NON-PDC
dc=a,dc=local   W2008R2DEV      Windows Server 2008 R2 Standard 6.1 (7601)      NON-PDC
dc=a,dc=local   W2008R264XEN    Windows Server 2008 R2 Standard 6.1 (7601)      NON-PDC
dc=a,dc=local   W2003R2XEN      Windows Server 2003     5.2 (3790)      NON-PDC
dc=a,dc=local   DELL4WAY        Windows Server 2003     5.2 (3790)      NON-PDC
```

It can be imported into the CMDB-X similar to the Network XML file.



File Path: C:\ARGENT\ArgentConsole\COMPUTERS.TXT

○ Import Network XML

● Import Computer Text File (Advanced Feature)

You may either manually edit COMPUTER.TXT

or run the customized ARGSOFT_NETWORKSCAN.VBS to generate this file

Ignored	Machine	Domain	Type	Vendor	Make
□	PANA01	dc=a,dc=local	Windows Domain Controllers	Microsoft	Windows Server® 2
□	PANA32	dc=a,dc=local	Windows Servers	Microsoft	Windows Server 200
□	WS-DEV8	dc=a,dc=local	Windows Servers	Microsoft	Windows Server 200
□	PANWS	dc=a,dc=local	Windows Servers	Microsoft	Windows Server 200
□	EX2007	dc=a,dc=local	Windows Servers	Microsoft	Windows Server 200
□	PANA36	dc=a,dc=local	Windows Workstations	Microsoft	Windows 7 Professio
□	PANA40	dc=a,dc=local	Windows Workstations	Microsoft	Windows 2000 Profe
□	DBMPRIN	dc=a,dc=local	Windows Servers	Microsoft	Windows Server 200

Save To Network Group: First Network Group

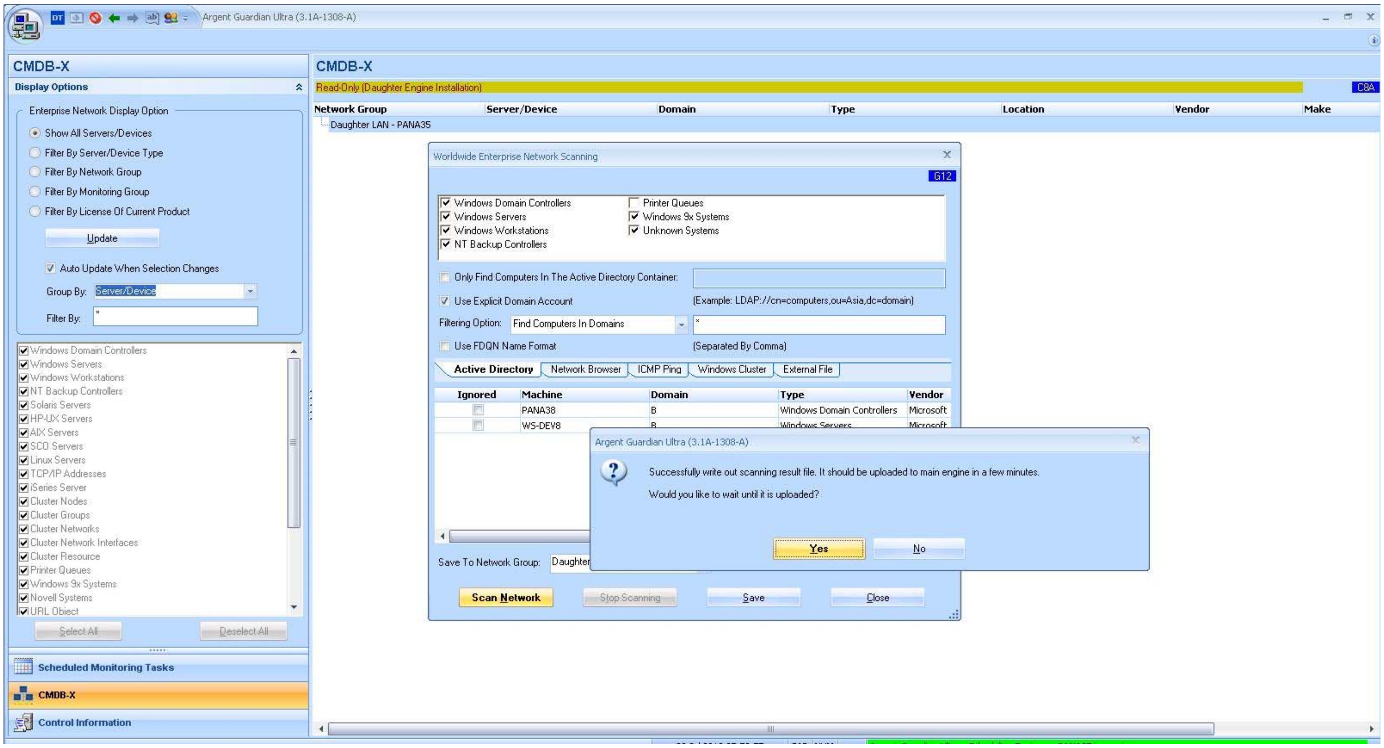
☑ Keep Original Network Group

Upload Remote Network Information From Daughter Engine

Most of the time it is not feasible to directly scan the remote network from the Argent AT Main Engine.

That is the main reason that customers install the Daughter Engine in the first place.

To include the remote network in the central CMDB-X, customers should scan the network at the Daughter site and upload the network information directly from the GUI.



Argent Guardian Ultra (3.1A-1308-A)

CMDB-X

Display Options

Enterprise Network Display Option

- ● Show All Servers/Devices
- ○ Filter By Server/Device Type
- ○ Filter By Network Group
- ○ Filter By Monitoring Group
- ○ Filter By License Of Current Product

☑ Auto Update When Selection Changes

Group By: Server/Device

Filter By: *

- ☑ Windows Domain Controllers
- ☑ Windows Servers
- ☑ Windows Workstations
- ☑ NT Backup Controllers
- ☑ Solaris Servers
- ☑ HP-UX Servers
- ☑ AIX Servers
- ☑ SCO Servers
- ☑ Linux Servers
- ☑ TCP/IP Addresses
- ☑ iSeries Server
- ☑ Cluster Nodes
- ☑ Cluster Groups
- ☑ Cluster Networks
- ☑ Cluster Network Interfaces
- ☑ Cluster Resource
- ☑ Printer Queues
- ☑ Windows 9x Systems
- ☑ Novell Systems
- ☑ URL Object

CMDB-X

Read-Only (Daughter Engine Installation)

Network Group	Server/Device	Domain	Type	Location	Vendor	Make
Daughter LAN - PANA35						

Worldwide Enterprise Network Scanning

- ☑ Windows Domain Controllers
- ☑ Windows Servers
- ☑ Windows Workstations
- ☑ NT Backup Controllers
- □ Printer Queues
- ☑ Windows 9x Systems
- ☑ Unknown Systems

□ Only Find Computers In The Active Directory Container:

☑ Use Explicit Domain Account

(Example: LDAP://cn=computers,ou=Asia,dc=domain)

Filtering Option: Find Computers In Domains *

□ Use FDQN Name Format

(Separated By Comma)

Ignored	Machine	Domain	Type	Vendor
□	PANA38	B	Windows Domain Controllers	Microsoft
□	WS-DEV8	B	Windows Servers	Microsoft

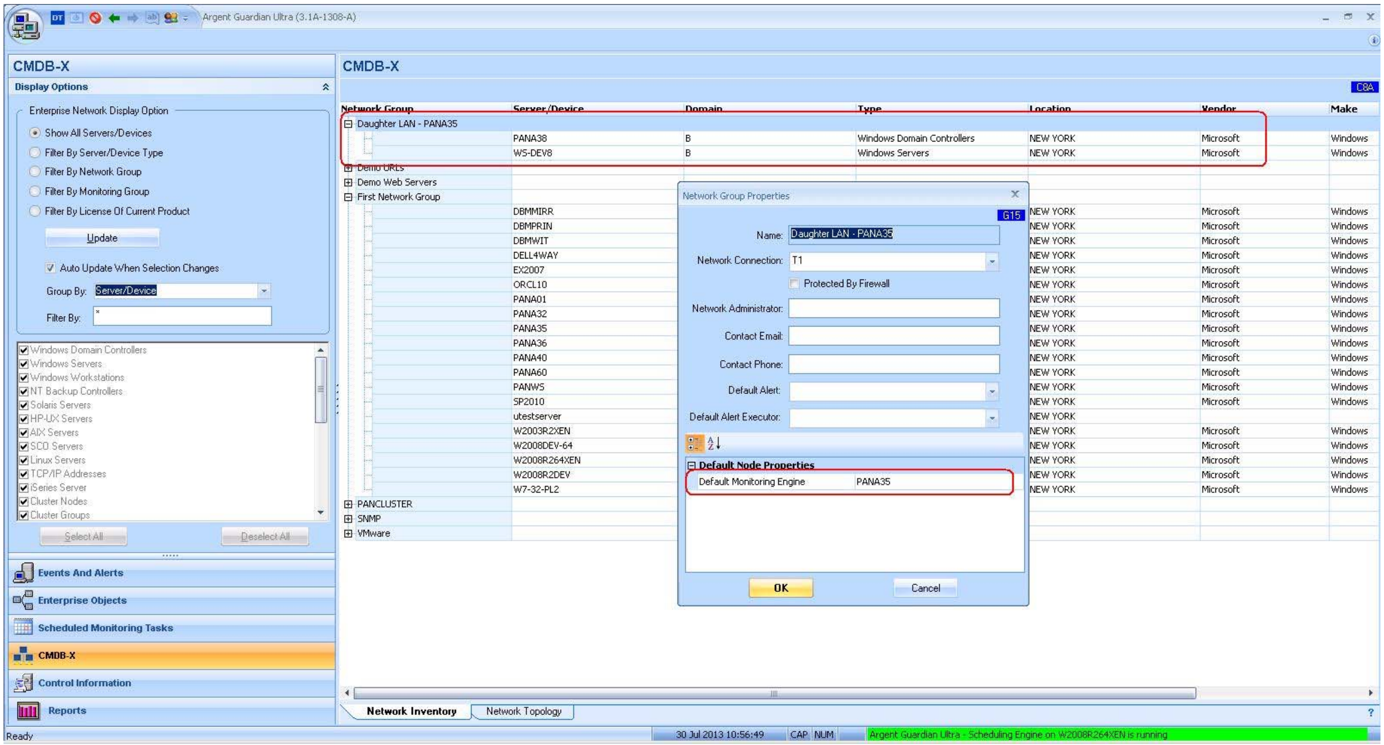
Save To Network Group: Daughter

Argent Guardian Ultra (3.1A-1308-A)

Successfully write out scanning result file. It should be uploaded to main engine in a few minutes.

Would you like to wait until it is uploaded?

After successful uploading the information, the remote network information shows up in the central CMDB-X.



Enterprise Network Display Option

● Show All Servers/Devices
○ Filter By Server/Device Type
○ Filter By Network Group
○ Filter By Monitoring Group
○ Filter By License Of Current Product

☑ Auto Update When Selection Changes

Group By: Server/Device

Filter By: *

☑ Windows Domain Controllers
☑ Windows Servers
☑ Windows Workstations
☑ NT Backup Controllers
☑ Solaris Servers
☑ HP-UX Servers
☑ AIX Servers
☑ SCO Servers
☑ Linux Servers
☑ TCP/IP Addresses
☑ iSeries Server
☑ Cluster Nodes
☑ Cluster Groups

Network Group	Server/Device	Domain	Type	Location	Vendor	Make
Daughter LAN - PANA35						
	PANA38	B	Windows Domain Controllers	NEW YORK	Microsoft	Windows
	WS-DEV8	B	Windows Servers	NEW YORK	Microsoft	Windows
Demo URLs						
Demo Web Servers						
First Network Group						
	DBMMIRR			NEW YORK	Microsoft	Windows
	DBMPRIN			NEW YORK	Microsoft	Windows
	DBMWIT			NEW YORK	Microsoft	Windows
	DELL4WAY			NEW YORK	Microsoft	Windows
	EX2007			NEW YORK	Microsoft	Windows
	ORCL10			NEW YORK	Microsoft	Windows
	PANA01			NEW YORK	Microsoft	Windows
	PANA32			NEW YORK	Microsoft	Windows
	PANA35			NEW YORK	Microsoft	Windows
	PANA36			NEW YORK	Microsoft	Windows
	PANA40			NEW YORK	Microsoft	Windows
	PANA60			NEW YORK	Microsoft	Windows
	PANWS			NEW YORK	Microsoft	Windows
	SP2010			NEW YORK	Microsoft	Windows
	utestserver			NEW YORK		
	W2003R2XEN			NEW YORK	Microsoft	Windows
	W2008DEV-64			NEW YORK	Microsoft	Windows
	W2008R264XEN			NEW YORK	Microsoft	Windows
	W2008R2DEV			NEW YORK	Microsoft	Windows
	W7-32-PL2			NEW YORK	Microsoft	Windows
PANCLUSTER						
SNMP						
VMware						

Network Group Properties

Name: Daughter LAN - PANA35

Network Connection: T1

□ Protected By Firewall

Network Administrator:

Contact Email:

Contact Phone:

Default Alert:

Default Alert Executor:

Default Node Properties

Default Monitoring Engine	PANA35

Ready | 30 Jul 2013 10:56:49 | CAP | NUM | Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

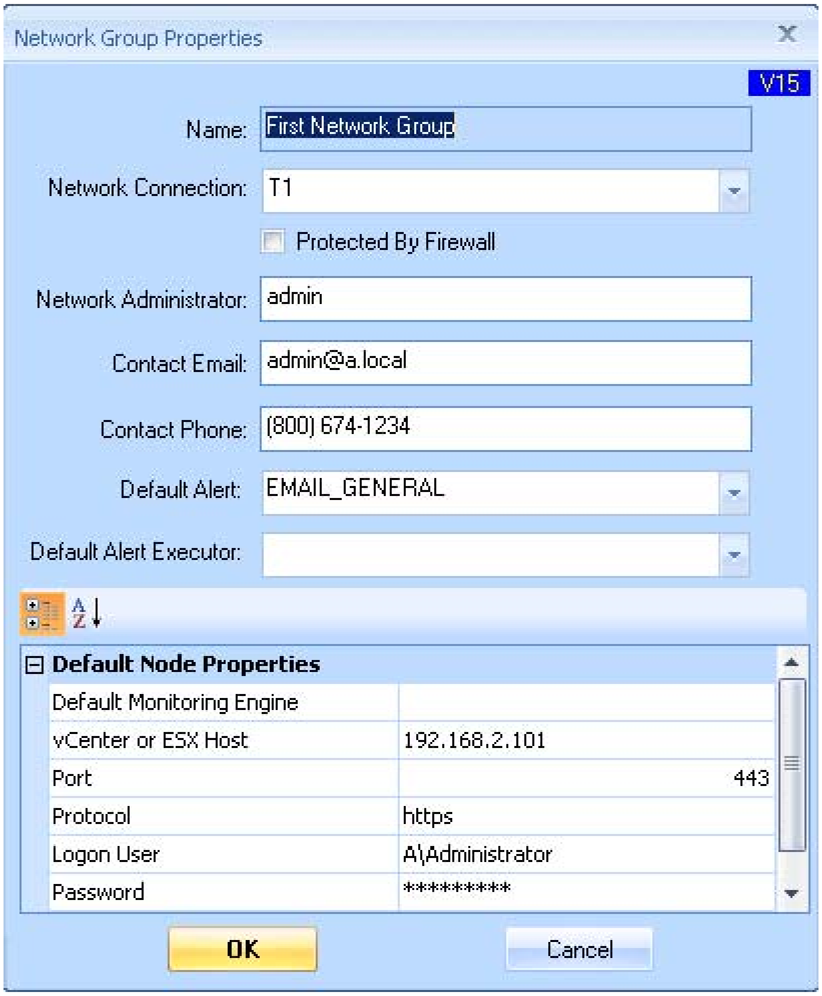
Appendix B - Network Group

A Network Group is a logical group to organize server/devices within the same network. Network Groups can be modeled using whatever logic that customers sees fit.

Typical examples include:

- Server/device locations such as main office and remote offices.
- Related services such as Exchange, SQL Server, Oracle, Web etc.
- Management teams such as Enterprise, Linux, Sales department etc.

Use context menu **'Properties'** to view or update Network Group properties.



Name: First Network Group

Network Connection: T1

□ Protected By Firewall

Network Administrator: admin

Contact Email: admin@a.local

Contact Phone: (800) 674-1234

Default Alert: EMAIL_GENERAL

Default Alert Executor:

⊟ **Default Node Properties**

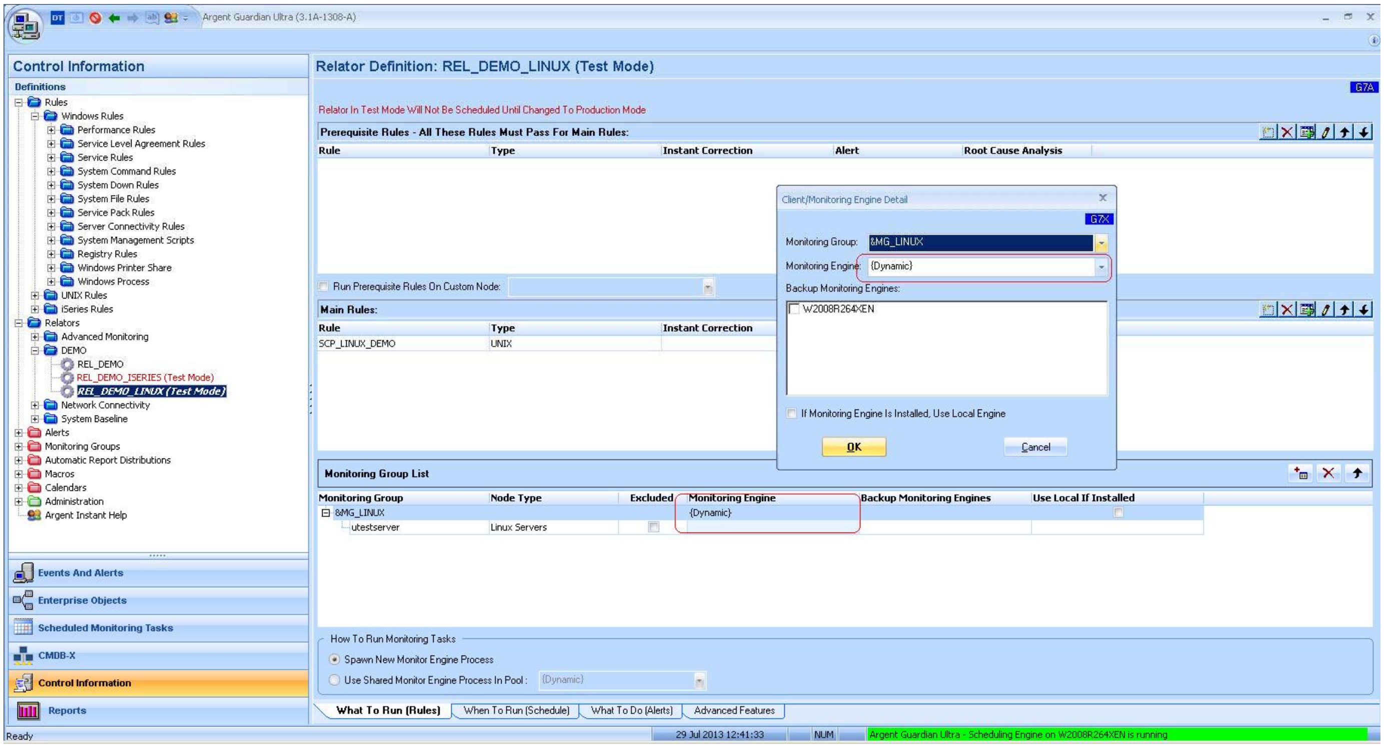
Default Monitoring Engine	
vCenter or ESX Host	192.168.2.101
Port	443
Protocol	https
Logon User	A\Administrator
Password	*********

Default Monitoring Engine

This is the most important setting in Mother/Daughter architecture.

When customers uses '{Dynamic}' as the Monitoring Engine in a Relator, Argent AT needs this information to determine which engine should monitor the node in a Relator.

If the Default Monitoring Engine belongs to a Mother Engine, the Mother Engine will schedule the task; if it belongs to Daughter Engine, the Daughter Engine will schedule the task.



Relator Definition: REL_DEMO_LINUX (Test Mode)

Relator In Test Mode Will Not Be Scheduled Until Changed To Production Mode

Prerequisite Rules - All These Rules Must Pass For Main Rules:

Rule	Type	Instant Correction	Alert	Root Cause Analysis

□ Run Prerequisite Rules On Custom Node:

Main Rules:

Rule	Type	Instant Correction
SCP_LINUX_DEMO	UNIX	

Client/Monitoring Engine Detail

Monitoring Group: &MG_LINUX

Monitoring Engine: {Dynamic}

Backup Monitoring Engines:

□ W2008R264XEN

□ If Monitoring Engine Is Installed, Use Local Engine

Monitoring Group List

Monitoring Group	Node Type	Excluded	Monitoring Engine	Backup Monitoring Engines	Use Local If Installed
⊟ &MG_LINUX			{Dynamic}		□
utestserver	Linux Servers	□			

How To Run Monitoring Tasks

● Spawn New Monitor Engine Process

○ Use Shared Monitor Engine Process In Pool : {Dynamic}

Ready | 29 Jul 2013 12:41:33 | NUM | Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

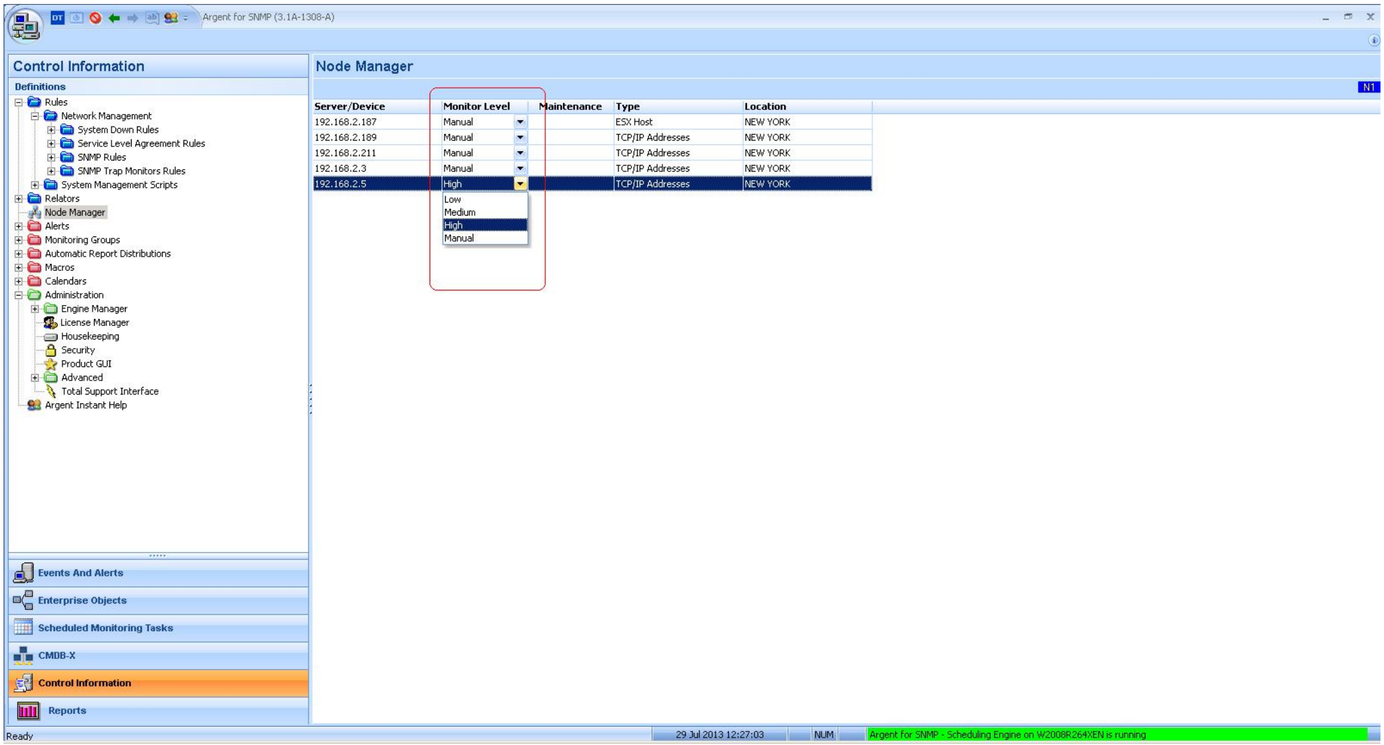
Default Alert

For Argent for SNMP, some monitoring tasks can be automatically generated.

As SNMP covers a wide universe of devices, Argent can automatically generate Alerts – see the topic "How To Specify What Alert To Fire When Doing Automated Monitoring In Argent for SNMP" for details.

Customers can select a monitoring level at the Node Manager, and the Argent for SNMP engine can use the synthetically generated Relator to perform the monitoring. Because the synthetically generated internal Relator does not exist physically, the engine needs to know what alert to fire if the Rule is broken. The Default Alert is used here.

Note: There is also an option to define the Default Alert at the node level. The one in the Network Group level is used only if it is not defined at the node level.



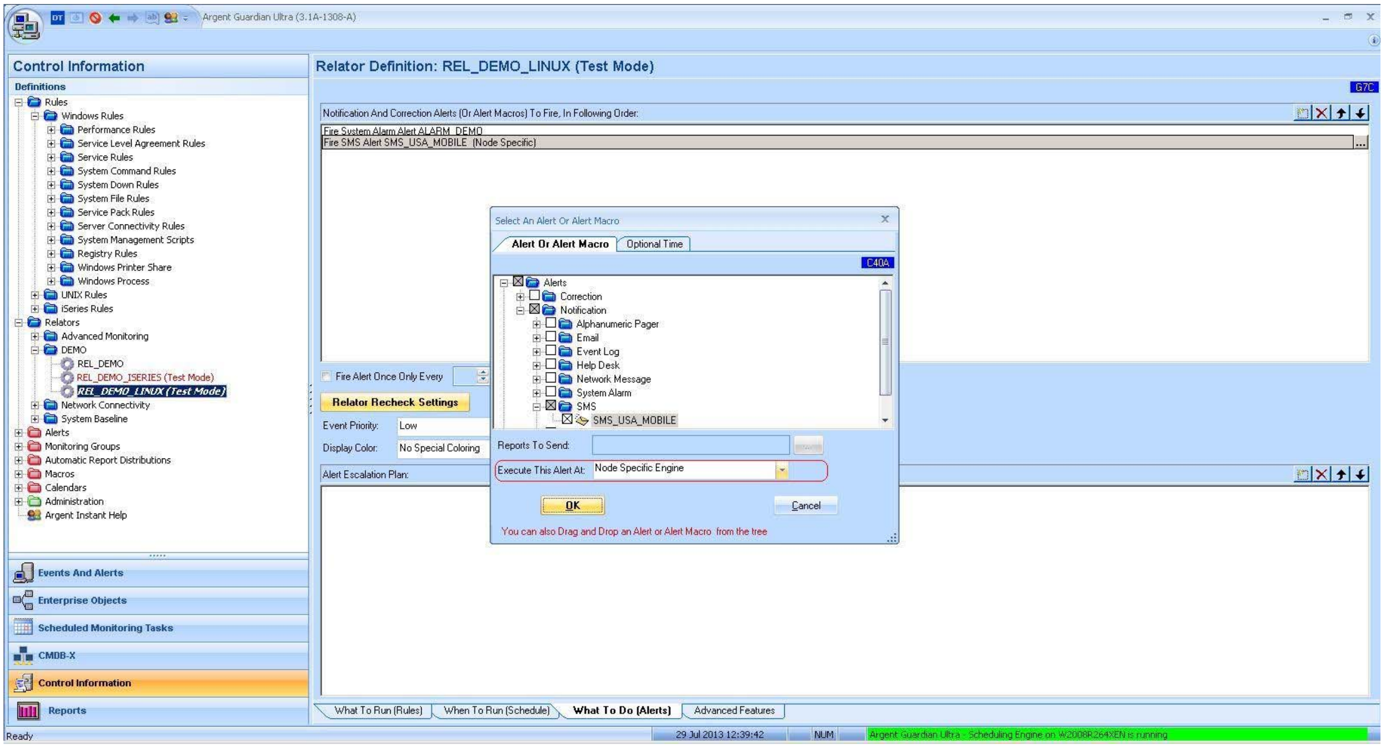
Server/Device	Monitor Level	Maintenance	Type	Location
192.168.2.187	Manual		ESX Host	NEW YORK
192.168.2.189	Manual		TCP/IP Addresses	NEW YORK
192.168.2.211	Manual		TCP/IP Addresses	NEW YORK
192.168.2.3	Manual		TCP/IP Addresses	NEW YORK
192.168.2.5	High		TCP/IP Addresses	NEW YORK

Ready 29 Jul 2013 12:27:03 NUM Argent for SNMP - Scheduling Engine on W2008R264XEN is running

Default Alert Executor

When customers use Argent Alert Executors to fire and Alert without explicitly specifying the Executor, the Argent Console engine uses **Default Alert Executor** to determine which Alert Executor to use.

Note: **Default Alert Executor** is also defined in the node level. The node takes precedence – if specified at the node level and at the Network Group level, then the node level is used only if it is not defined at the node level.



Relator Definition: REL_DEMO_LINUX (Test Mode)

Notification And Correction Alerts (Or Alert Macros) To Fire, In Following Order:

Fire System Alarm Alert ALARM_DEMO
Fire SMS Alert SMS_USA_MOBILE (Node Specific)

☐ Fire Alert Once Only Every

Relator Recheck Settings

Event Priority: Low

Display Color: No Special Coloring

Alert Escalation Plan:

Select An Alert Or Alert Macro

- ☒ Alerts
  - ☐ Correction
  - ☒ Notification
    - ☐ Alphanumeric Pager
    - ☐ Email
    - ☐ Event Log
    - ☐ Help Desk
    - ☐ Network Message
    - ☐ System Alarm
    - ☒ SMS
      - ☒ SMS_USA_MOBILE

Reports To Send:

Execute This Alert At: Node Specific Engine

You can also Drag and Drop an Alert or Alert Macro from the tree

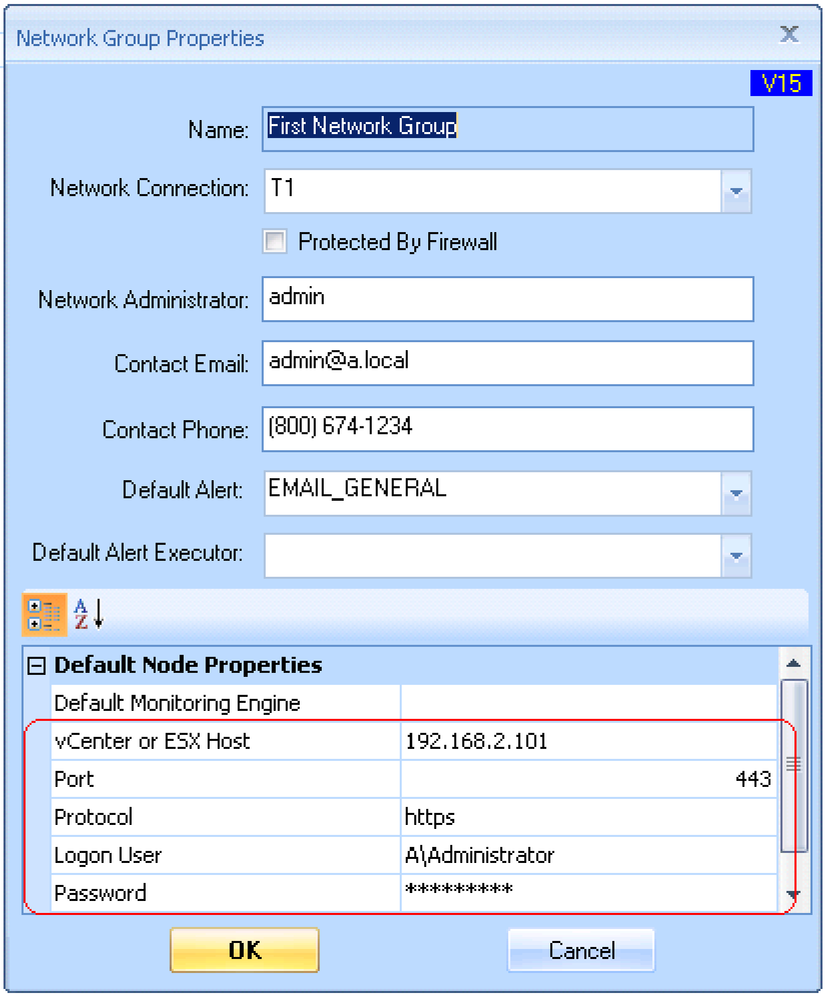
29 Jul 2013 12:39:42

Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

Product Specific Properties

There may be additional product-specific properties in the list of Default Node Properties. For example, Argent for SNMP has SNMP version, community string etc, Argent for VMware has VMware logon credentials.

The properties are used when the same information is not explicitly specified at the node level.



Network Group Properties

V15

Name: First Network Group

Network Connection: T1

□ Protected By Firewall

Network Administrator: admin

Contact Email: admin@a.local

Contact Phone: (800) 674-1234

Default Alert: EMAIL_GENERAL

Default Alert Executor:

Default Node Properties

Default Monitoring Engine	
vCenter or ESX Host	192.168.2.101
Port	443
Protocol	https
Logon User	A\Administrator
Password	**********

Display-Only Properties

The following fields can be used for customers' own purposes:

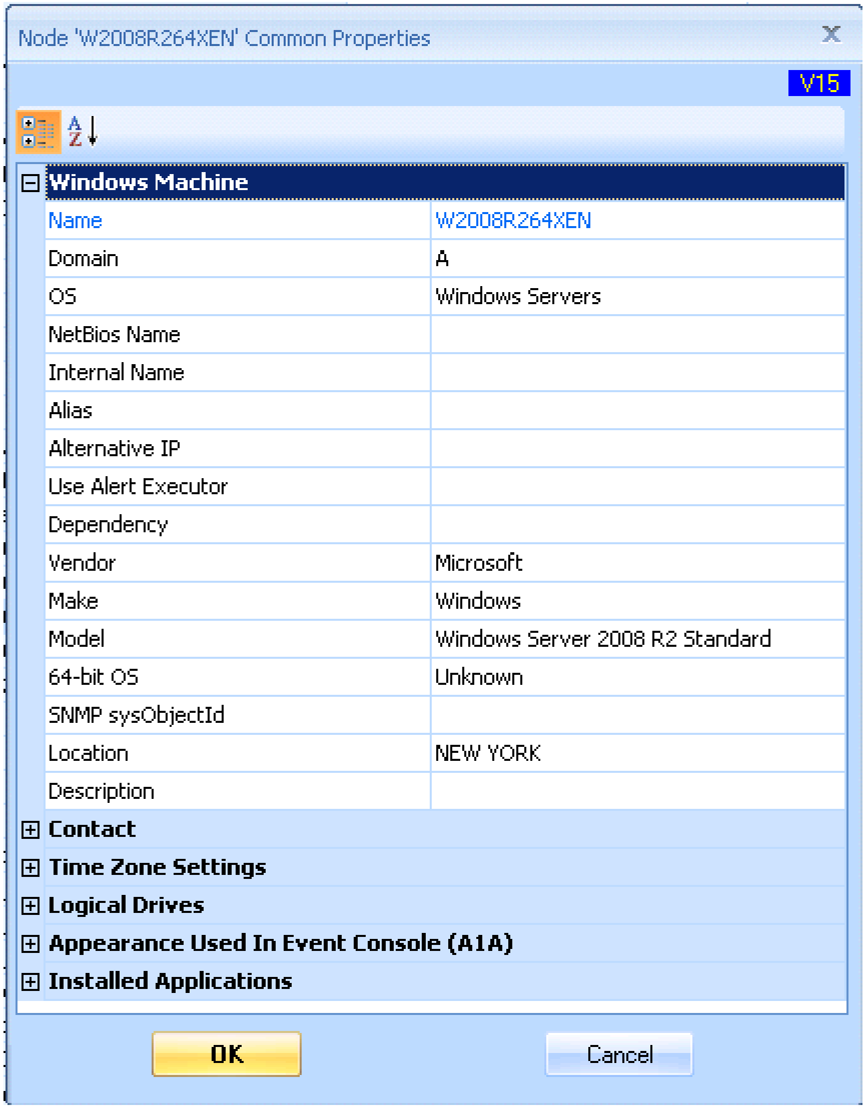
- Network Connection
- Protected By Firewall
- Network Administrator
- Contact Email
- Contact Phone

Appendix C - CMDB-X Node Properties

Node properties defined in CMDB-X are shared among Argent AT products.

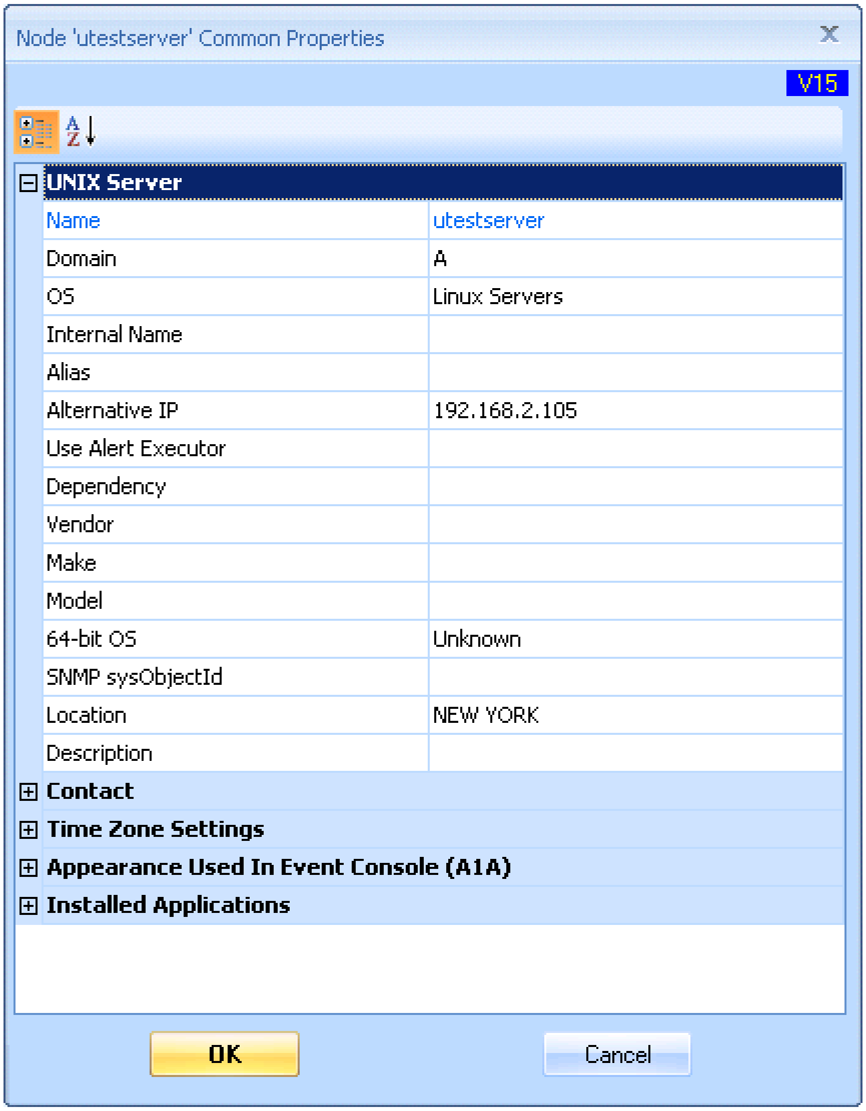
The properties vary based on the type of node.

Windows Machine



Windows Machine	
Name	W2008R264XEN
Domain	A
OS	Windows Servers
NetBios Name	
Internal Name	
Alias	
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	Microsoft
Make	Windows
Model	Windows Server 2008 R2 Standard
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	

Linux/Unix



UNIX Server

Name	utestserver
Domain	A
OS	Linux Servers
Internal Name	
Alias	
Alternative IP	192.168.2.105
Use Alert Executor	
Dependency	
Vendor	
Make	
Model	
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	

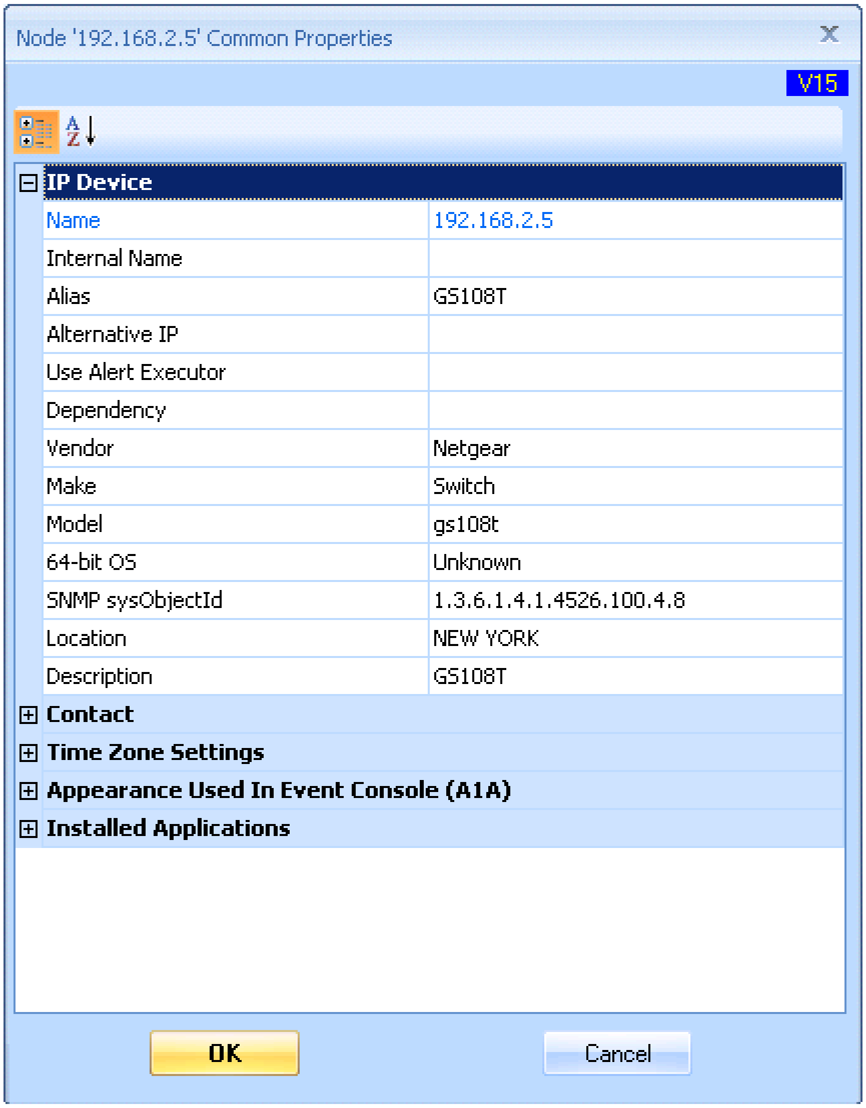
⊞ **Contact**

⊞ **Time Zone Settings**

⊞ **Appearance Used In Event Console (A1A)**

⊞ **Installed Applications**

IP Address

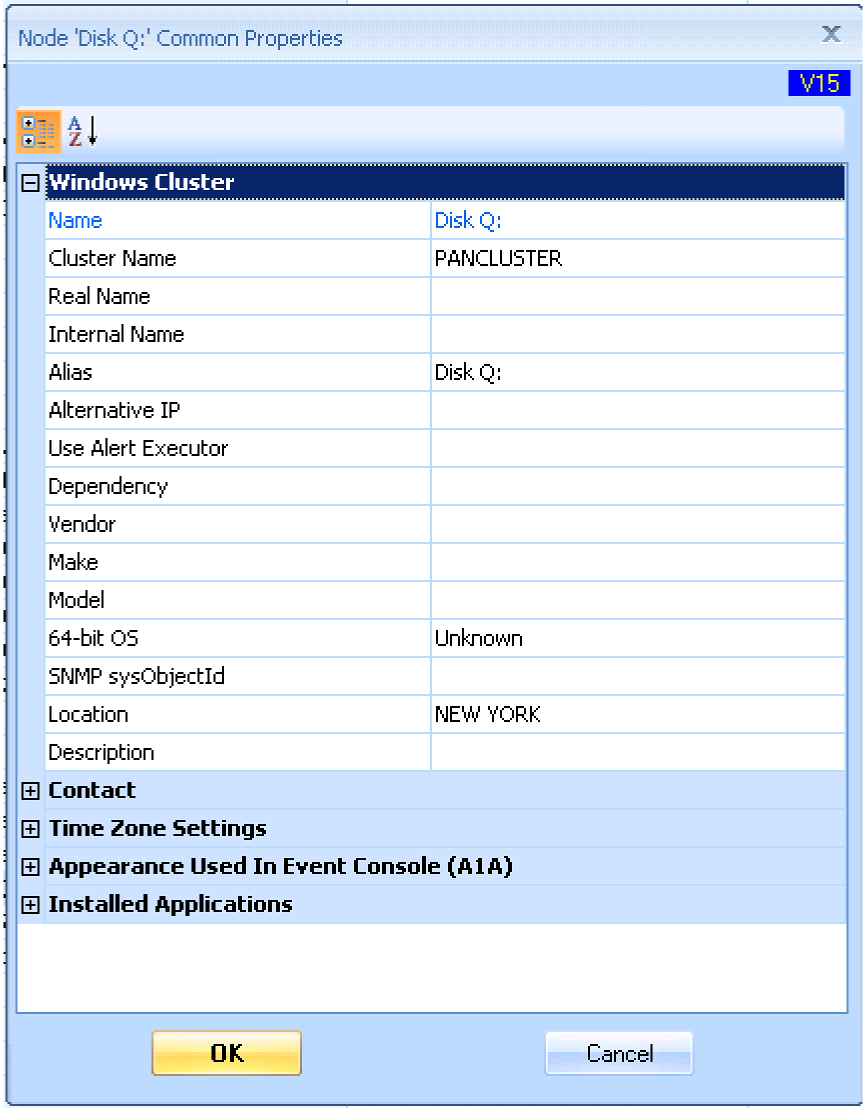


Node '192.168.2.5' Common Properties

IP Device

Name	192.168.2.5
Internal Name	
Alias	GS108T
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	Netgear
Make	Switch
Model	gs108t
64-bit OS	Unknown
SNMP sysObjectId	1.3.6.1.4.1.4526.100.4.8
Location	NEW YORK
Description	GS108T

Windows Cluster Object

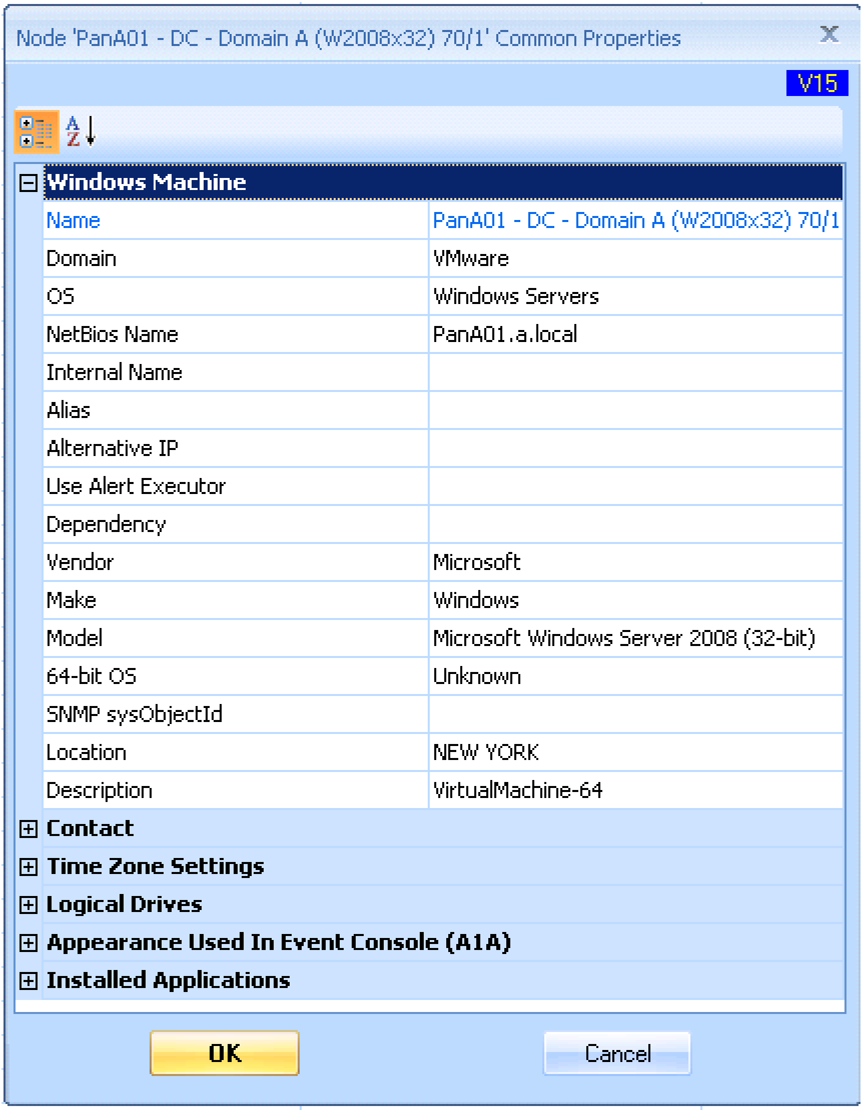


⊟ **Windows Cluster**

Name	Disk Q:
Cluster Name	PANCLUSTER
Real Name	
Internal Name	
Alias	Disk Q:
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	
Make	
Model	
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	

⊞ **Contact**
⊞ **Time Zone Settings**
⊞ **Appearance Used In Event Console (A1A)**
⊞ **Installed Applications**

VMware Object



Node 'PanA01 - DC - Domain A (W2008x32) 70/1' Common Properties
V15

⊟ **Windows Machine**

Name	PanA01 - DC - Domain A (W2008x32) 70/1
Domain	VMware
OS	Windows Servers
NetBios Name	PanA01.a.local
Internal Name	
Alias	
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	Microsoft
Make	Windows
Model	Microsoft Windows Server 2008 (32-bit)
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	VirtualMachine-64

⊞ **Contact**

⊞ **Time Zone Settings**

⊞ **Logical Drives**

⊞ **Appearance Used In Event Console (A1A)**

⊞ **Installed Applications**

Domain

The Domain property is only used for the cluster objects.

It is useful for grouping and display.

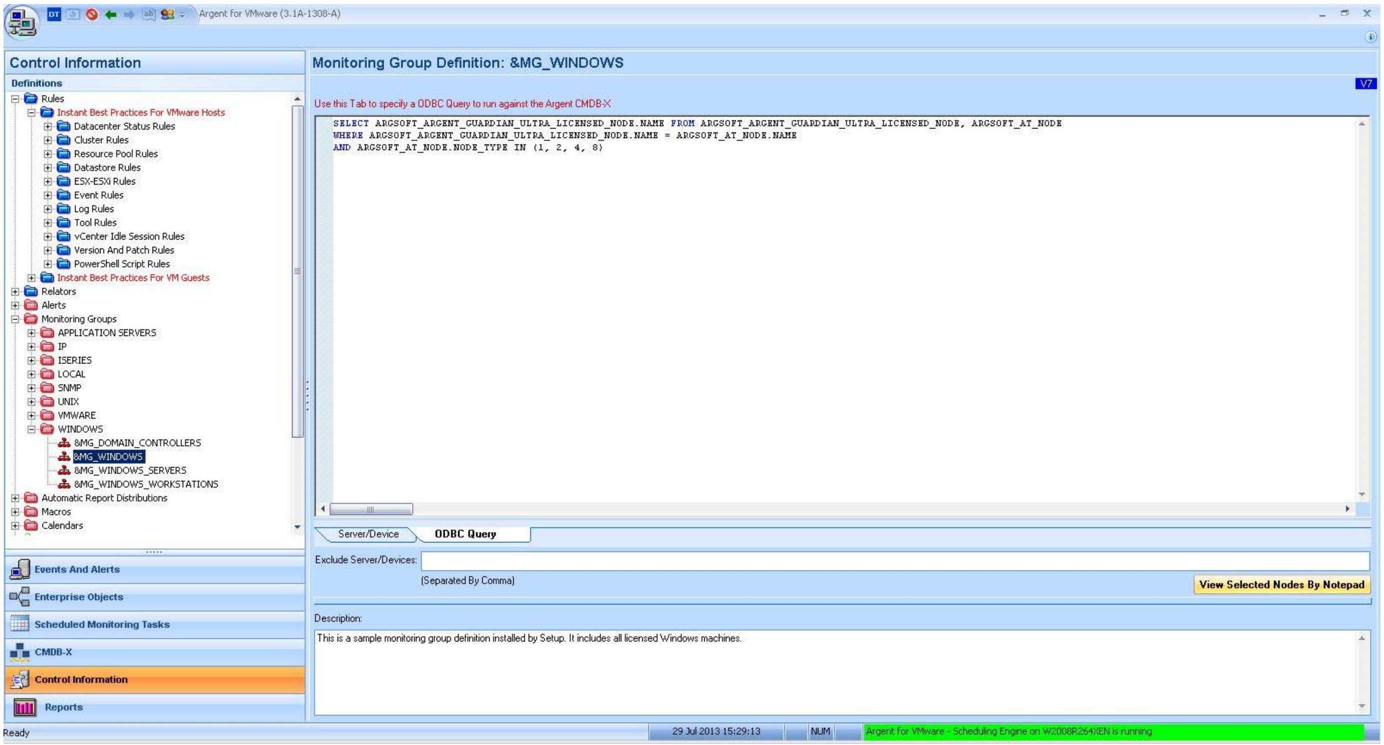
The filtering based on domain is available on both CMDB-X and License Manager.

In the case of Windows Cluster, this field is actually the Cluster Name. It is required by the Cluster APIs.

OS

Monitoring Groups can be defined based on node OS type.

The pre-defined ‘&MG_WINDOWS’ provided by Argent Guardian Ultra is a good example.



Monitoring Group Definition: &MG_WINDOWS

Use this Tab to specify a ODBC Query to run against the Argent CMDB-X

```
SELECT ARGSOFT_ARGENT_GUARDIAN_ULTRA_LICENSED_NODE.NAME FROM ARGSOFT_ARGENT_GUARDIAN_ULTRA_LICENSED_NODE, ARGSOFT_AT_NODE
WHERE ARGSOFT_ARGENT_GUARDIAN_ULTRA_LICENSED_NODE.NAME = ARGSOFT_AT_NODE.NAME
AND ARGSOFT_AT_NODE.NODE_TYPE IN (1, 2, 4, 8)
```

Exclude Server/Devices:

(Separated By Comma)

Description:

This is a sample monitoring group definition installed by Setup. It includes all licensed Windows machines.

Argent for VMware - Scheduling Engine on W2008R264XEN is running

The SQL query uses the column ‘NODE_TYPE’ to specify Windows OS.

The possible values are as follows:

0x1 (1)	– Windows Domain Controller
0x2 (2)	– Windows Backup Domain Controller
0x4 (4)	– Windows Server
0x8 (8)	– Windows Workstation
0x10 (16)	– Sun Solaris
0x20 (32)	– HP-UX
0x40 (64)	– AIX
0x80 (128)	– SCO UNIX
0x100 (256)	– Linux
0x200 (512)	– IP Address
0x400 (1,024)	– iSeries Server
0x800 (2,048)	– Cluster Node
0x1000 (4,096)	– Cluster Group
0x2000 (8,192)	– Cluster Network
0x4000 (16,384)	– Cluster Network Interface
0x8000 (32,768)	– Cluster Resource
0x10000 (65,536)	– Printer Queue
0x20000 (131,072)	– Windows 9x (obsolete)
0x40000 (262,144)	– Novell Server (obsolete)
0x80000 (524,288)	– Unknown
0x100000 (1,048,576)	– URL Object
0x200000 (2,097,152)	– Mail Object
0x400000 (4,194,304)	– FTP Object

NetBIOS Name (Windows)

This is the real Windows machine name for the entity. There are occasions that monitored machines have the same name. This happens a lot in ISP environments when customers clone machines, and because the machines reside in separate networks monitored by Daughter Engines. There is no network conflict until customers need to differentiate them in Argent Atlas.

To handle such a situation, customers can manually add the machines with distinguishable names, and use property 'NetBIOS Name' to point to the real machine name.

When the Argent AT engine monitors a Windows machine, if it is specified, the NetBIOS name is used instead of the node name for API calls.

Internal Name (Windows Cluster Object)

Similar to NetBIOS name for Windows machine, Internal Name is the real cluster object name that is used in Windows Cluster API.

Alias

Property **'Alias'** is useful for IP address.

Alternative IP

Alternative IP can specify the actual IP address for Linux/Unix and iSeries server. If it is not specified, Argent AT engine will attempt to resolve the IP address from the node name.

Use Alert Executor

This defines the node-specific Alert Executor. When a Relator defines alerts using node-specific Alert Executors, the Argent Console engine uses this property to determine which Argent Alert Executor should be used.

Dependency

This defines the logical dependency for the node. There are two types of dependency supported in Argent AT. One is topology dependency; the other is logical dependency. A typical example is that the ESX host is the logical dependency for a VM running on the ESX host. If the ESX host is offline, all the VM guests running on it will be offline.

The information is used for Root Cause Analysis. Say a customer defines esx1.a.local as the dependency for VM pana01.a.local. When the Argent AT engine detects pana01.a.local is offline, instead of reporting VM outage right away, it checks the VM's dependency. If esx1.a.local is also offline, the Argent AT engine will report a single event of the real root cause instead of flooding the user with VM offline events.

Vendor/Make/Model

These properties are mostly for display except for Argent for SNMP, which uses the information plus sysObjectId, combined with Argent's internal knowledge base to generate synthetic Relators for automated monitoring. See Default Alert in Network Group for details.

64-bit OS

This information can have an important performance impact on situations that require such information. For example, when Argent for Compliance engine reads Windows event log using traditional Event Log API, it must determine whether the target machine is 32-bit or 64-bit. If the property is not specified, the engine needs to run an additional routine to determine it. It can be costly.

As a result, if customers know exactly what the OS type is, the property should be specified to give Argent AT a little boost.

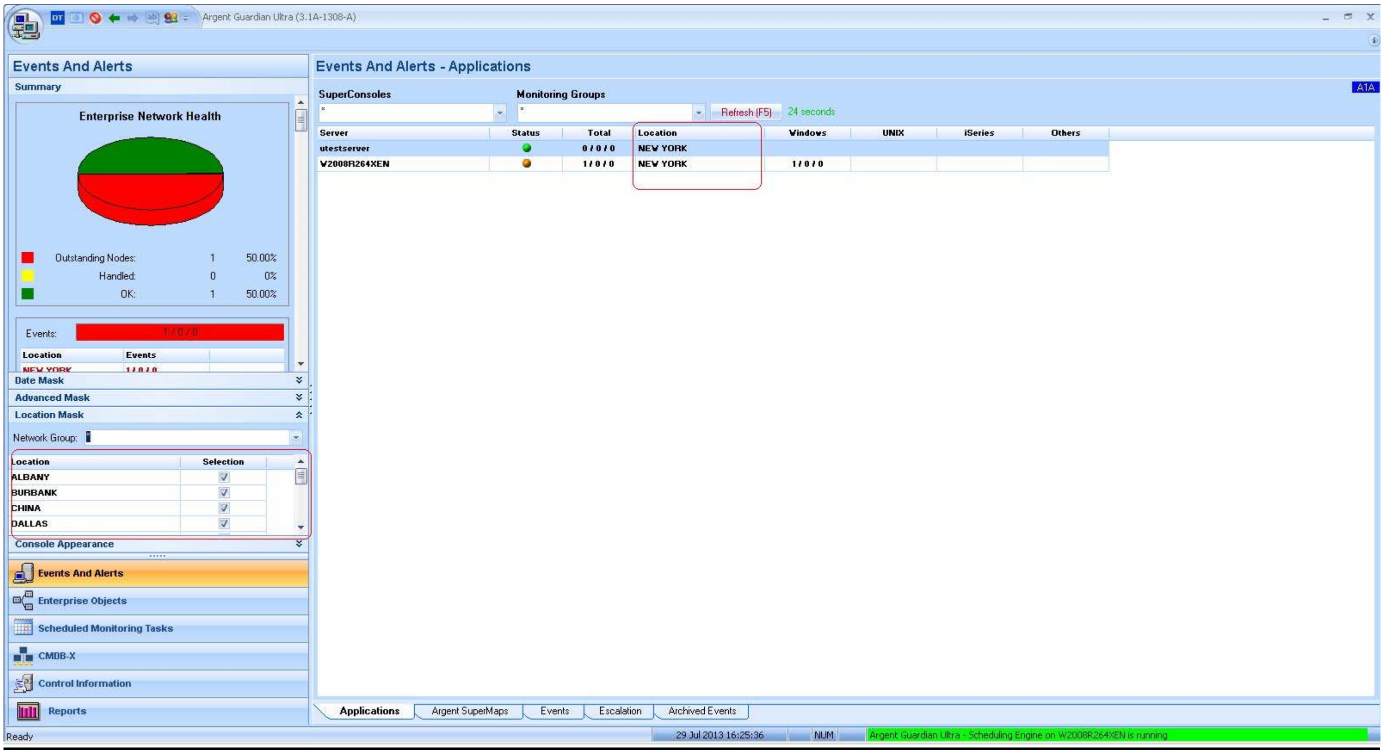
SNMP sysObjectId

This property is used by SNMP objects. It is another property used in automated monitoring.

See Vendor/Make/Model.

Location

The node location is used for filtering in Argent Console A1x screens, and the Argent SuperMaps



🟥 Outstanding Nodes:	1	50.00%
🟨 Handled:	0	0%
🟩 OK:	1	50.00%

Events: 1 / 0 / 0

Location	Events
NEW YORK	1 / 0 / 0

Network Group: *

Location	Selection
ALBANY	☑
BURBANK	☑
CHINA	☑
DALLAS	☑

SuperConsoles: *

Monitoring Groups: *

24 seconds

Server	Status	Total	Location	Windows	UNIX	iSeries	Others
utestserver	●	0 / 0 / 0	NEW YORK				
W2008R264XEN	●	1 / 0 / 0	NEW YORK	1 / 0 / 0			

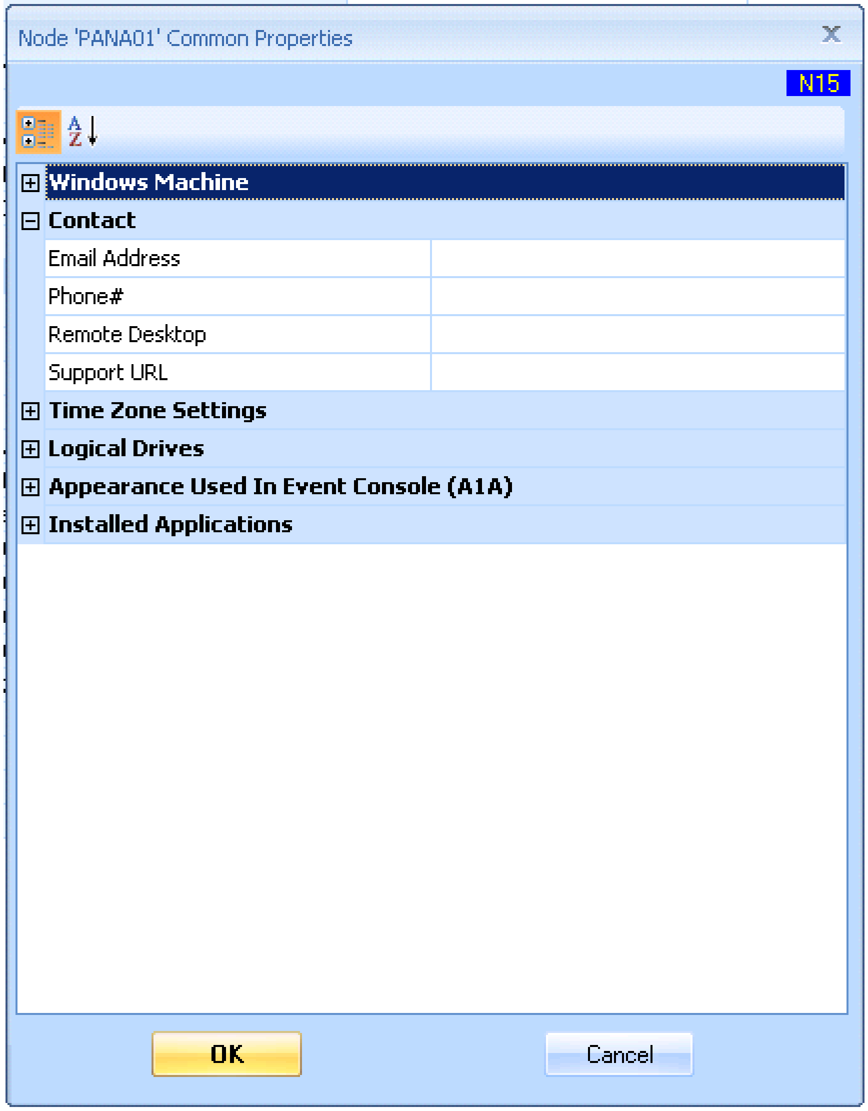
29 Jul 2013 16:25:36

Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

Description

Customers can enter any information here about this particular node.

Contact



Node 'PANA01' Common Properties

N15

⊞ Windows Machine	
⊟ Contact	
Email Address	
Phone#	
Remote Desktop	
Support URL	
⊞ Time Zone Settings	
⊞ Logical Drives	
⊞ Appearance Used In Event Console (A1A)	
⊞ Installed Applications	

Email Address

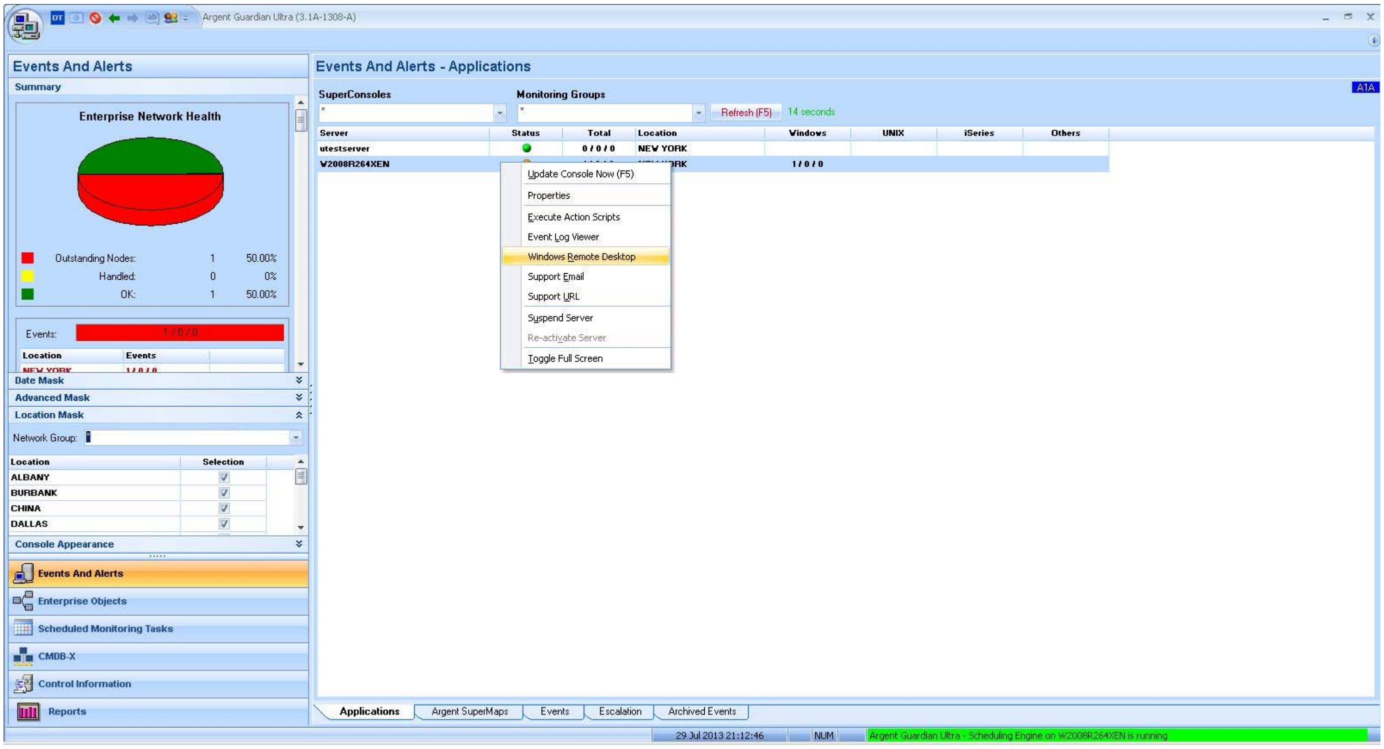
This is the email address of contact for this node. This property is not just for display. It can be used as replacement for the %DefaultNode%. See 'KBI 310392 New Feature: Node-Specific Email In Email Alert' for details.

Phone#

It is the phone# of contact for this node. This property is for display only.

Remote Desktop

It is the custom command line to start up remote desktop session for the node from A1A. For example, 'mstsc /v:%AGNodeName%' will connect to the target machine using remote desktop.



Server	Status	Total	Location	Windows	UNIX	iSeries	Others
utestserver	●	0 / 0 / 0	NEW YORK				
W2008R264XEN				1 / 0 / 0			

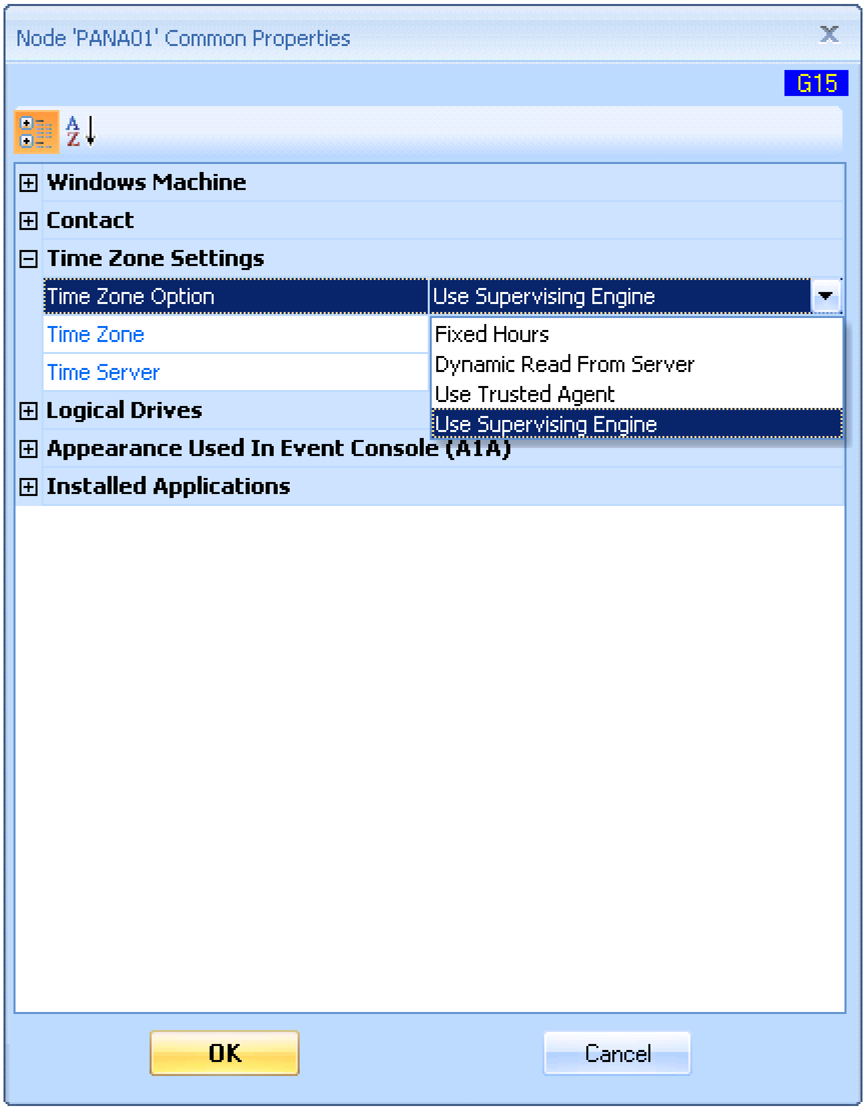
Location	Selection
ALBANY	☑
BURBANK	☑
CHINA	☑
DALLAS	☑

Support URL

It is the support URL for the node. Customers can invoke the URL using the context menu on A1A.

Time Zone Settings

This set of properties defines the time zone of the node. The information can be used for scheduling monitoring tasks or putting the node into maintenance mode.



Node 'PANA01' Common Properties

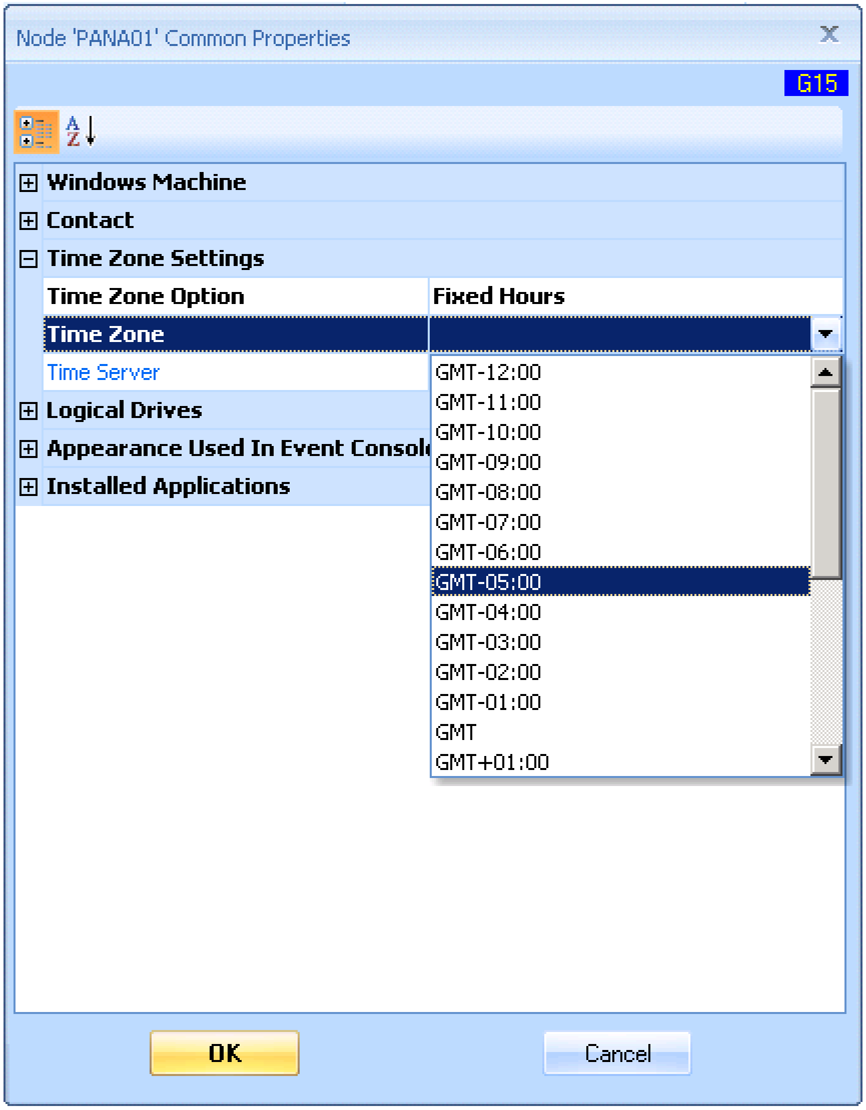
Time Zone Option: Use Supervising Engine

Time Zone Option

The available options include following:

- Fixed Hours

  It is easy to use and causes little overhead. It assumes the node has the same daylight savings time setting bias as the Supervising Engine. For example, the scheme works well if all servers/devices are in USA and in the same time zone.



Node 'PANA01' Common Properties

G15

⊞ Windows Machine

⊞ Contact

⊟ Time Zone Settings

Time Zone Option	Fixed Hours
Time Zone	
Time Server	

⊞ Logical Drives

⊞ Appearance Used In Event Consol

⊞ Installed Applications

- Dynamic Read From Server

  If the Time Server is not specified, the same node is assumed. The Time Server must be a Windows machine.

Querying time zone information causes some overhead. Because the Argent AT engine caches time zone information, it would make sense to use one or a few common machines as the Time Server for all other machines in the same time zone.

- Use Trusted Agent

  Queries time zone information from the specified Argent AT Trusted Agent.

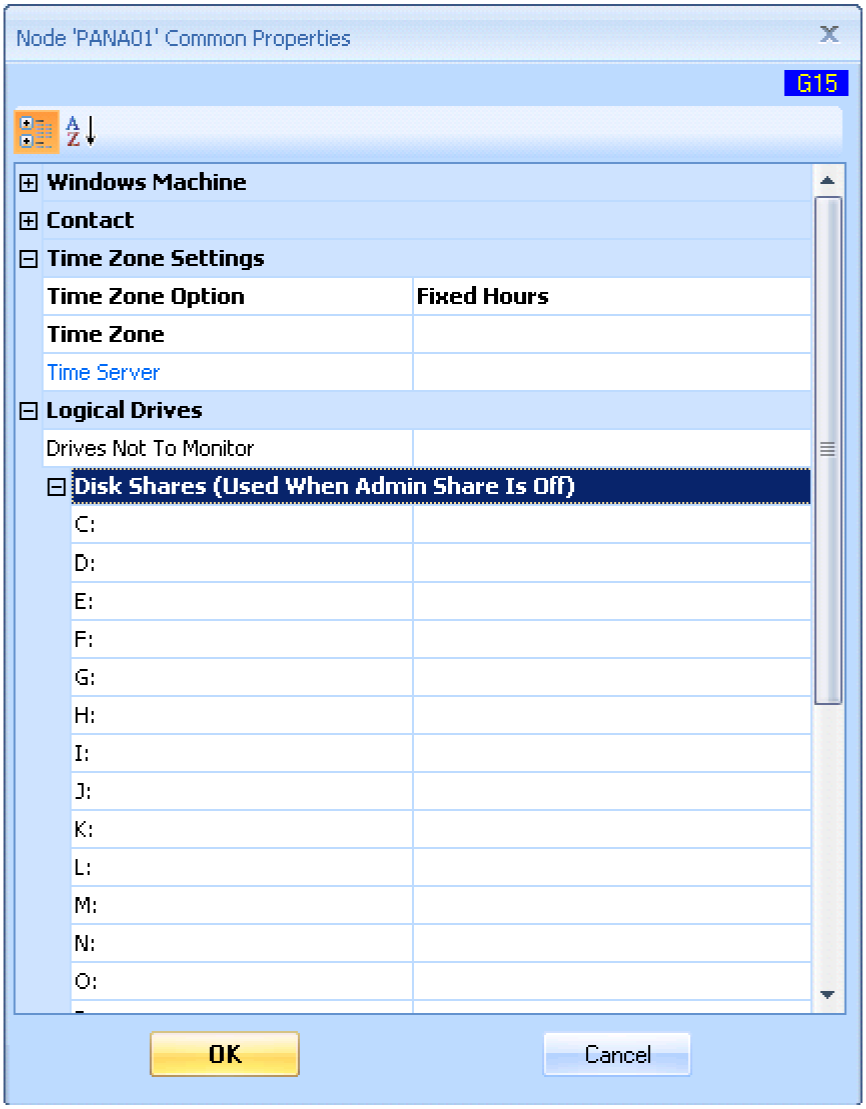
- Use Supervising Engine

  Assume the node has the same time zone setting as the Supervising Engine that is scheduling the monitoring task. This is the default time zone setting for the node.

Note: the Supervising Engine can be a Mother Engine or a Daughter Engine. The Daughter Engine may not necessarily be in the same time zone as the Mother Engine. As a result, all the nodes monitored by the Daughter Engine are scheduled based on the time zone of Daughter Engine. This makes senses for most situations.

Logical Drives

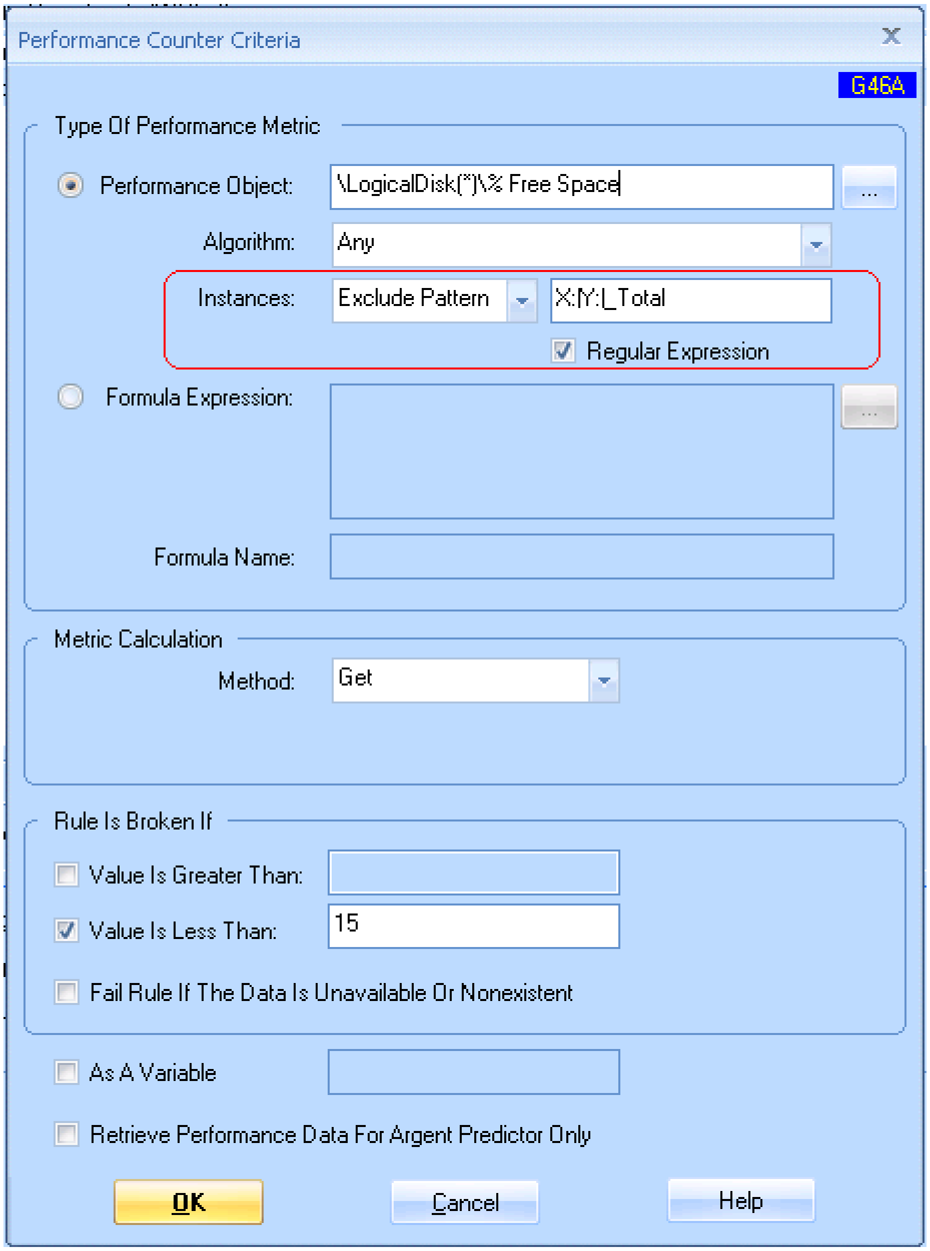
Logical Drives are used to explicitly ignore some logical drives when checking logical drive related performance data. It can be used to get free disk space when the remote registry service is not running.



⊞ Windows Machine	
⊞ Contact	
⊟ Time Zone Settings	
Time Zone Option	Fixed Hours
Time Zone	
Time Server	
⊟ Logical Drives	
Drives Not To Monitor	
⊟ Disk Shares (Used When Admin Share Is Off)	
C:	
D:	
E:	
F:	
G:	
H:	
I:	
J:	
K:	
L:	
M:	
N:	
O:	

Drives Not To Monitor

If one or multiple drives should be excluded for all monitored servers, it is easier to exclude drives in the Performance Rule.



Performance Counter Criteria

G46A

Type Of Performance Metric

● Performance Object: \LogicalDisk(*)\% Free Space

Algorithm: Any

Instances: Exclude Pattern X:|Y:|_Total

☑ Regular Expression

○ Formula Expression:

Formula Name:

Metric Calculation

Method: Get

Rule Is Broken If

□ Value Is Greater Than:

☑ Value Is Less Than: 15

□ Fail Rule If The Data Is Unavailable Or Nonexistent

□ As A Variable

□ Retrieve Performance Data For Argent Predictor Only

If one or multiple drives are only excluded for some servers, or the excluded drives are different for each server, it is better to define the Performance Rule excluding no drives, and use this property to exclude the specific drives for the server.

Disk Shares (Used When Admin Share Is Off)

The remote performance data may not be available due to security settings or the remote registry service is turned off on the remote machine. This is quite common for locked down machines in the DMZ.

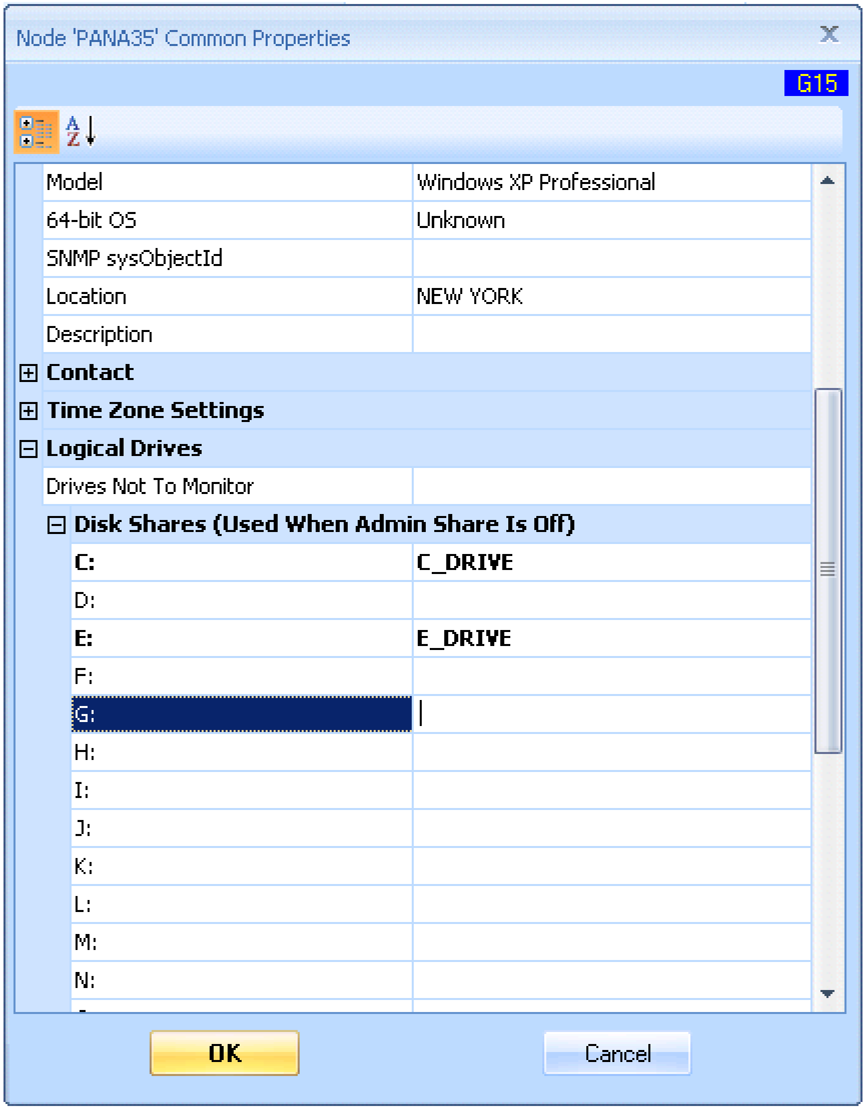
Even though customers may still need to get disk information such as free disk space. Fortunately the disk information can be retrieved through WIN32 API 'GetDiskFreeSpaceEx'.

In order to use the API, customers need to specify what drives to check. Customers can do so by assigning drive shares for the used drives. For example, C$ for C:, D$ for D: etc.

Sometimes the admin shares (C$, D$ etc) are turned off too. If there is any defined share on the drive, not necessarily the admin share, customers can specify the share for the drive. The API works using the share too.

In the following example, machine 'PANA35' has two logical drives 'C:' and 'E:'. Because admin share is turned off, customers define two shares C_DRIVE and E_DRIVE for accessing the drives.

Also see KBI 310607 New Feature: Checking Disk Space When Performance Data Unavailable.



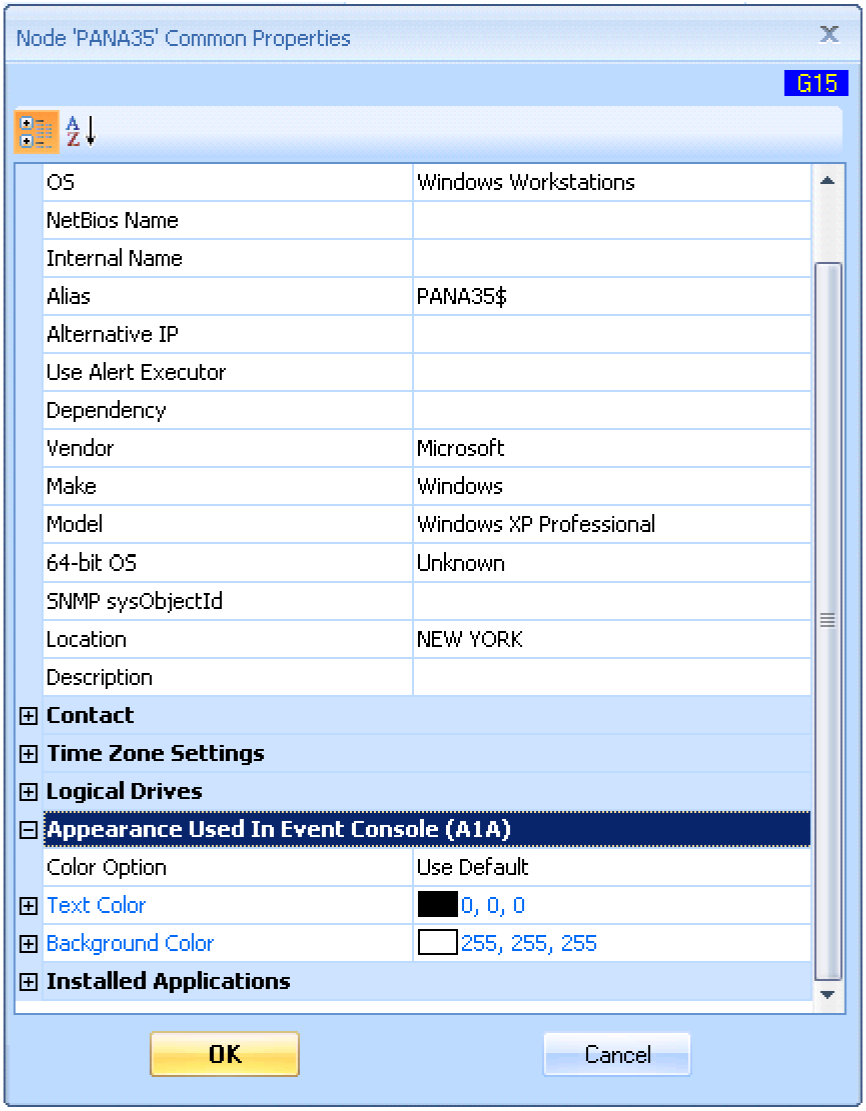
Node 'PANA35' Common Properties

G15

Model	Windows XP Professional
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	
⊞ **Contact**	
⊞ **Time Zone Settings**	
⊟ **Logical Drives**	
Drives Not To Monitor	
⊟ **Disk Shares (Used When Admin Share Is Off)**	
C:	**C_DRIVE**
D:	
E:	**E_DRIVE**
F:	
G:	
H:	
I:	
J:	
K:	
L:	
M:	
N:	

Appearance Used In Event Console (A1A)

These properties control the text and background color for the specific nodes in Event Console. Customers can customize the colors to make some nodes stand out on the screen.

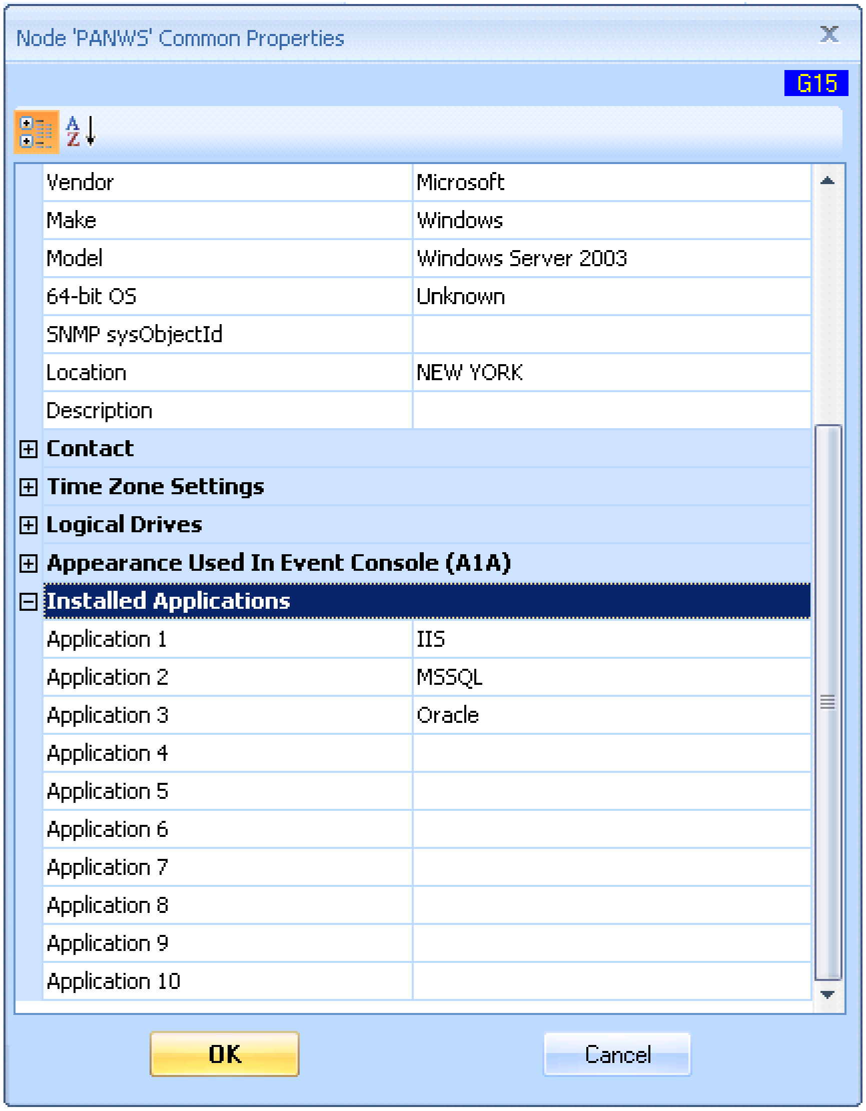


OS	Windows Workstations
NetBios Name	
Internal Name	
Alias	PANA35$
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	Microsoft
Make	Windows
Model	Windows XP Professional
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	
⊞ **Contact**	
⊞ **Time Zone Settings**	
⊞ **Logical Drives**	
⊟ **Appearance Used In Event Console (A1A)**	
Color Option	Use Default
⊞ Text Color	■ 0, 0, 0
⊞ Background Color	□ 255, 255, 255
⊞ **Installed Applications**	

Installed Applications

These properties simply list out all the known applications installed on the node.

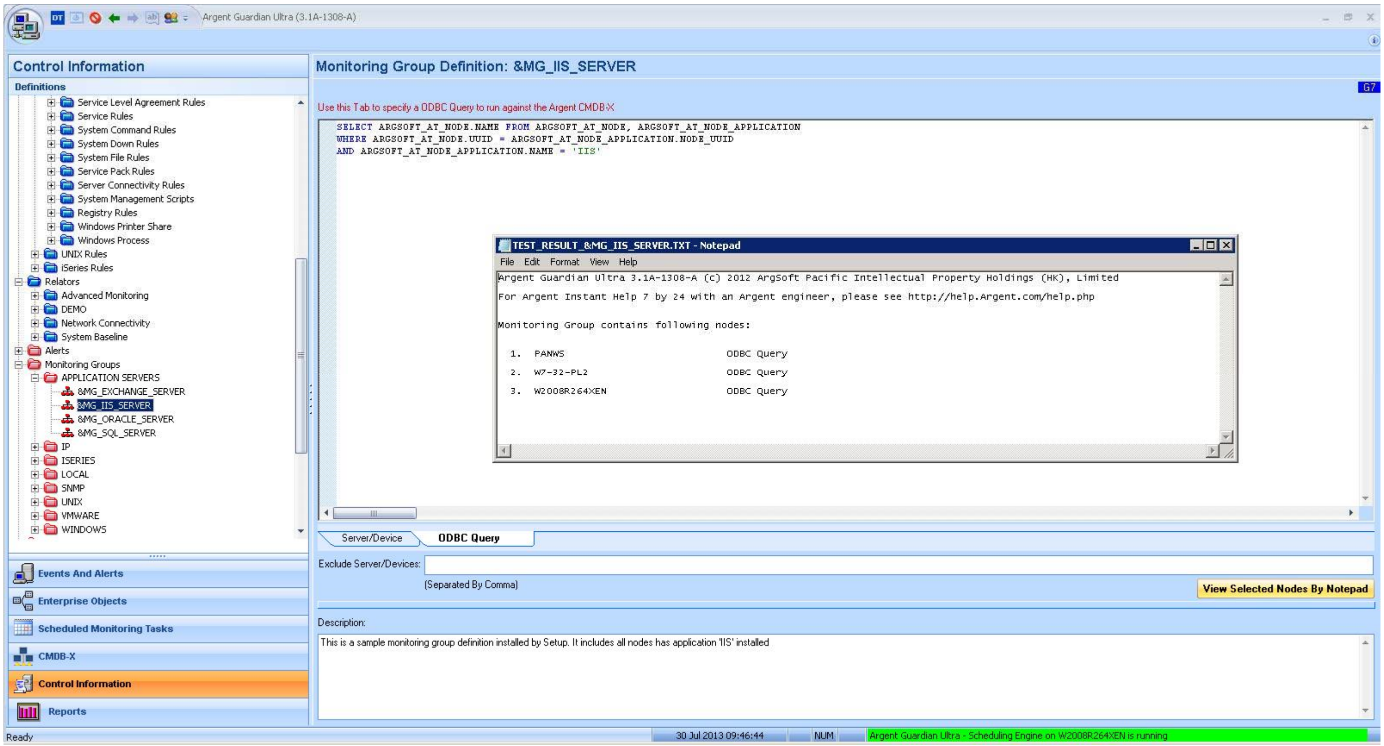
The applications can be entered directly, or discovered by a program (See Detect Installed Applications)



Vendor	Microsoft
Make	Windows
Model	Windows Server 2003
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	
⊞ **Contact**	
⊞ **Time Zone Settings**	
⊞ **Logical Drives**	
⊞ **Appearance Used In Event Console (A1A)**	
⊟ **Installed Applications**	
Application 1	IIS
Application 2	MSSQL
Application 3	Oracle
Application 4	
Application 5	
Application 6	
Application 7	
Application 8	
Application 9	
Application 10	

Customers can define Monitoring Groups based on the installed applications.

Argent AT provides a few pre-defined sample Monitoring Groups to demonstrate this.



Monitoring Group Definition: &MG_IIS_SERVER

Use this Tab to specify a ODBC Query to run against the Argent CMDB-X

```
SELECT ARGSOFT_AT_NODE.NAME FROM ARGSOFT_AT_NODE, ARGSOFT_AT_NODE_APPLICATION
WHERE ARGSOFT_AT_NODE.UUID = ARGSOFT_AT_NODE_APPLICATION.NODE_UUID
AND ARGSOFT_AT_NODE_APPLICATION.NAME = 'IIS'
```

TEST_RESULT_&MG_IIS_SERVER.TXT - Notepad

```
Argent Guardian Ultra 3.1A-1308-A (c) 2012 ArgSoft Pacific Intellectual Property Holdings (HK), Limited

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


Monitoring Group contains following nodes:


  1.   PANWS                            ODBC Query

  2.   W7-32-PL2                        ODBC Query

  3.   W2008R264XEN                     ODBC Query
```

Exclude Server/Devices:

(Separated By Comma)

Description:

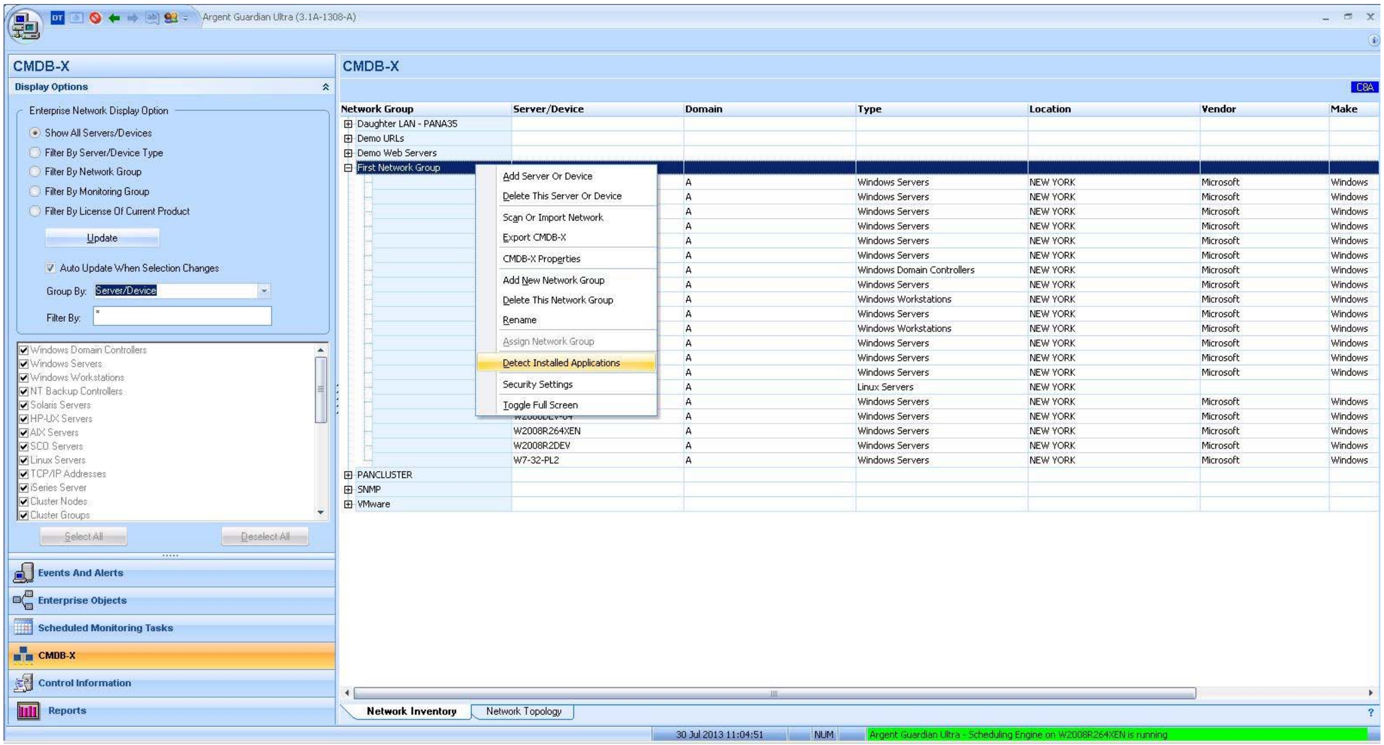
This is a sample monitoring group definition installed by Setup. It includes all nodes has application 'IIS' installed

Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

Customers can use these Monitoring Groups in the Relators. Combined with automatic application discovery by using Argent AT Command Line Tools, automatic monitoring of an application can be accomplished.

Appendix D – Detect Installed Applications

By right-clicking and showing the context menu, customers can use pre-defined mechanisms to scan the selected nodes for installed applications.



Enterprise Network Display Option

- ● Show All Servers/Devices
- ○ Filter By Server/Device Type
- ○ Filter By Network Group
- ○ Filter By Monitoring Group
- ○ Filter By License Of Current Product

☑ Auto Update When Selection Changes

Group By: Server/Device

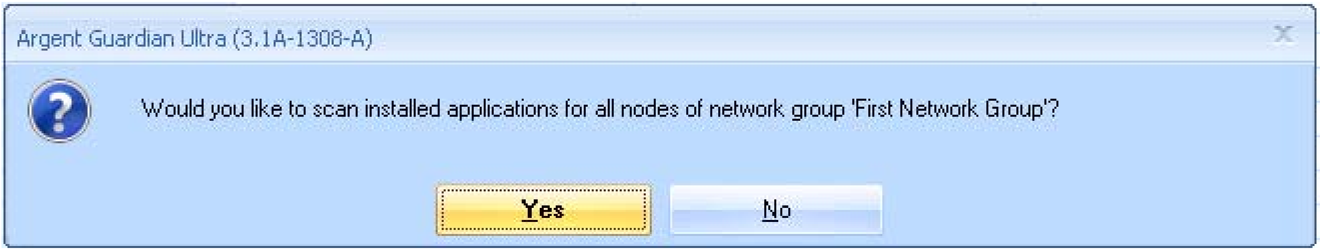
Filter By: *

- ☑ Windows Domain Controllers
- ☑ Windows Servers
- ☑ Windows Workstations
- ☑ NT Backup Controllers
- ☑ Solaris Servers
- ☑ HP-UX Servers
- ☑ AIX Servers
- ☑ SCO Servers
- ☑ Linux Servers
- ☑ TCP/IP Addresses
- ☑ iSeries Server
- ☑ Cluster Nodes
- ☑ Cluster Groups

Network Group	Server/Device	Domain	Type	Location	Vendor	Make
⊞ Daughter LAN - PANA35						
⊞ Demo URLs						
⊞ Demo Web Servers						
⊟ First Network Group						
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Domain Controllers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Workstations	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Workstations	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Windows Servers	NEW YORK	Microsoft	Windows
		A	Linux Servers	NEW YORK		
		A	Windows Servers	NEW YORK	Microsoft	Windows
	W2008DEV-04	A	Windows Servers	NEW YORK	Microsoft	Windows
	W2008R264XEN	A	Windows Servers	NEW YORK	Microsoft	Windows
	W2008R2DEV	A	Windows Servers	NEW YORK	Microsoft	Windows
	W7-32-PL2	A	Windows Servers	NEW YORK	Microsoft	Windows
⊞ PANCLUSTER						
⊞ SNMP						
⊞ VMware						

30 Jul 2013 11:04:51 | NUM | Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

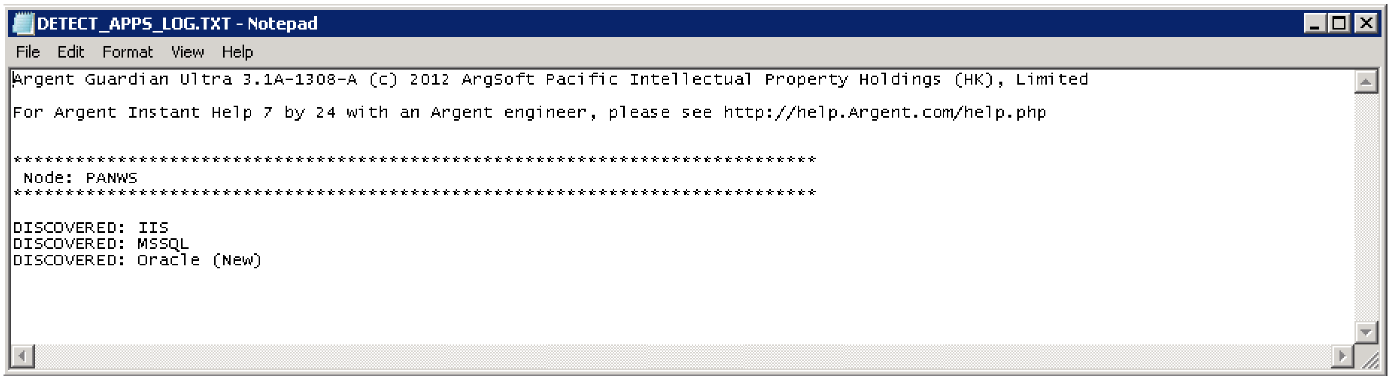
If the current selection is a Network Group, the following prompt is shown:



Argent Guardian Ultra (3.1A-1308-A)

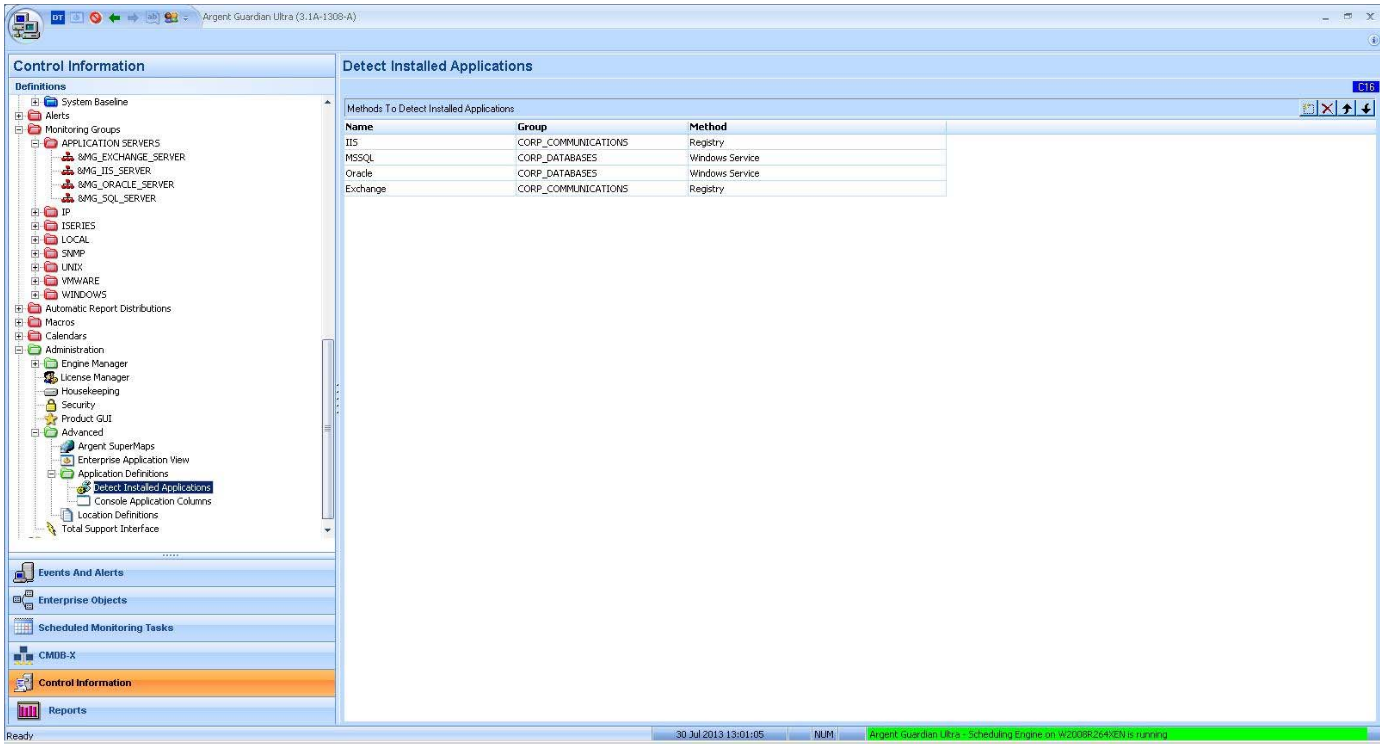
Would you like to scan installed applications for all nodes of network group 'First Network Group'?

At the end of detection, the CMDB-X database is updated and the log is shown in notepad.



```
Argent Guardian Ultra 3.1A-1308-A (c) 2012 ArgSoft Pacific Intellectual Property Holdings (HK), Limited

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


*****************************************************************************
 Node: PANWS
*****************************************************************************

DISCOVERED: IIS
DISCOVERED: MSSQL
DISCOVERED: Oracle (New)
```

The detection of installed applications relies on the pre-defined application discovery mechanism.



Detect Installed Applications

Methods To Detect Installed Applications

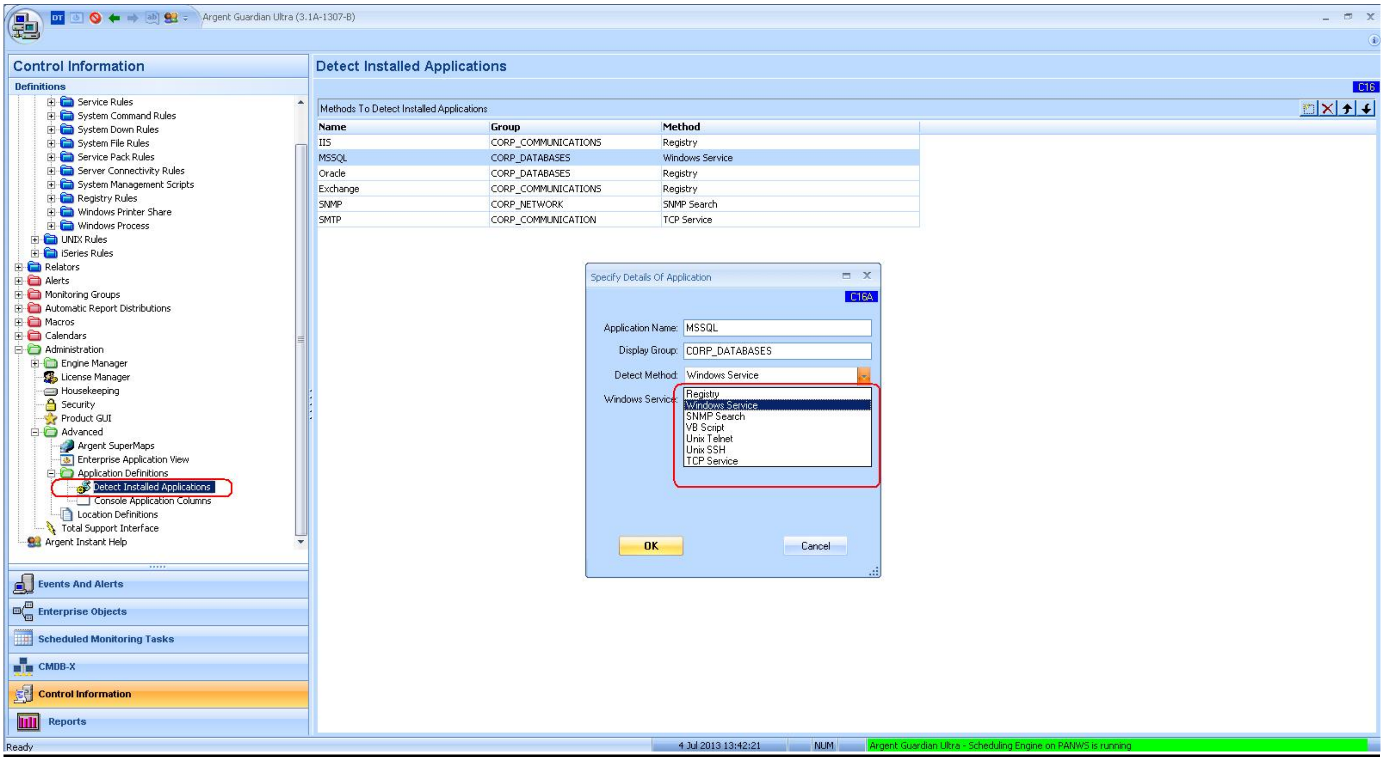
Name	Group	Method
IIS	CORP_COMMUNICATIONS	Registry
MSSQL	CORP_DATABASES	Windows Service
Oracle	CORP_DATABASES	Windows Service
Exchange	CORP_COMMUNICATIONS	Registry

30 Jul 2013 13:01:05

Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

The supported mechanisms include the following:

1. Windows registry
2. Windows service
3. SNMP OID
4. VBScript
5. Unix Telnet
6. Unix SSH
7. TCP service



Name	Group	Method
IIS	CORP_COMMUNICATIONS	Registry
MSSQL	CORP_DATABASES	Windows Service
Oracle	CORP_DATABASES	Registry
Exchange	CORP_COMMUNICATIONS	Registry
SNMP	CORP_NETWORK	SNMP Search
SMTP	CORP_COMMUNICATION	TCP Service

Application Name: MSSQL

Display Group: CORP_DATABASES

Detect Method: Windows Service

Windows Service:

Ready | 4 Jul 2013 13:42:21 | NUM | Argent Guardian Ultra - Scheduling Engine on PANWS is running

As the majority of Windows applications have Windows services as background processes, or use specific registry hives, the methods of ‘Windows Registry’ and ‘Windows Service’ are most commonly used.

For Linux/Unix applications, the method ‘TCP Service’ is recommended, as it is the easiest and least intrusive.

Argent AT provides command line utilities to accomplish the same functions of detecting installed application as the GUI. It can be very useful to implement automated monitoring by running application detection periodically in a background maintenance script.

Define Applications

(Windows Registry)

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m registry -reg reghive [-val value]

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m registry' specifies the method of Windows registry.
- Argument '-reg' specifies the registry key path
- Argument '-val' specifies the optional value for the registry key.

(Windows Service)

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m service -serv svcname

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m service' specifies the method of Windows service.
- Argument '-serv' specifies the Windows service name.

ARGENT_DETECTAPP_CLI [-add | *-update] -p application -g group -m snmp -oid oid*

- Argument ‘-add’ adds a new application.
- Argument ‘-update’ updates an existing application
- Argument ‘-p’ specifies the application name.
- Argument ‘-g’ specifies the group for the application.
- Argument ‘-m snmp’ specifies the method of SNMP.
- Argument ‘-oid’ specifies the signature OID for the application.

ARGENT_DETECTAPP_CLI [-add | *-update] -p application -g group -m vbscript -file script*

- Argument ‘-add’ adds a new application.
- Argument ‘-update’ updates an existing application
- Argument ‘-p’ specifies the application name.
- Argument ‘-g’ specifies the group for the application.
- Argument ‘-m vbscript’ specifies the method of VBScript.
- Argument ‘-file’ specifies the script file path.

ARGENT_DETECTAPP_CLI [-add | *-update] -p application -g group -m ssh -file script*

- Argument ‘-add’ adds a new application.
- Argument ‘-update’ updates an existing application
- Argument ‘-p’ specifies the application name.
- Argument ‘-g’ specifies the group for the application.
- Argument ‘-m ssh’ specifies the method of SSH.
- Argument ‘-file’ specifies the script file path.

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m telnet -file script

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m telnet' specifies the method of Telnet.
- Argument '-file' specifies the script file path.

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m tcp -port port_number [-file script]

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m tcp' specifies the method of TCP service.
- Argument '-p' specifies the TCP port to detect.
- Argument '-file' specifies the script file path.

<u>Delete A Defined Application</u>

ARGENT_DETECTAPP_CLI -delete -p application

- Argument '-delete' deletes an existing application
- Argument '-p' specifies the application name.

Detect Installed Applications

ARGENT_DETECTAPP_CLI -s server [-p application] [-user user] [-pswd pswd] [-snmp v1|v2c] [-comm community]

ARGENT_DETECTAPP_CLI -n group [-p application] [-user user] [-pswd pswd] [-snmp v1|v2c] [-comm community]

ARGENT_DETECTAPP_CLI -all [-p application] [-user user] [-pswd pswd] [-snmp v1|v2c] [-comm community]

- Argument '-s' specifies the single server/device to detect.
- Argument '-n' specifies the network group. All server/devices of the network group should be scanned.
- Argument '-all' means that all server/devices should be scanned.
- Argument '-p' specifies the single application to detect. If not specified, all defined applications should be scanned.
- Argument '-user' specifies the logon user for LINUX/UNIX server. It is used only when the application uses SSH or telnet method.
- Argument '-pswd' specifies the logon password for LINUX/UNIX server.
- Argument '-snmp' specifies the SNMP version. SNMP version 1 and 2c are supported. It is used only when the application uses SNMP method.
- Argument '-comm' specifies the SNMP community.

Appendix E – Extended VBScript Syntax For Detecting Installed Application

Customers can use VBScript to implement very complicated logic for determining whether an application is installed. Besides ordinary VBScript syntax, Argent Advanced Technology introduces the following keywords to communicate information back and forth:

TargetServer (Read-Only)
Argent AT assigns the real server name to this property.

ApplicationName (Read-Only)
Argent AT assigns the application name to this property.

ApplicationFound (Write-Only)
Customers should assign True to this property if the application is determined as being installed; otherwise, assign False.

ScriptHasError (Write-Only)
Customers can assign True to this property if encountering some unrecoverable error within script logic.

WriteStatus (Method)
Write a line to the log.

Appendix F – UNIX Script Output Syntax For Detecting Installed Application

The UNIX script syntax uses the same format as UNIX script rules.

If the output contains status ‘PASS’, it means the application is found; if the output contains status ‘FAIL’, it means the application is not found.

A ‘PASS’ sample output should look like:

```
<TAGResult>
 <QEResult>
      <STATUS>PASS</STATUS>
 </QEResult>
</TAGResult>
```

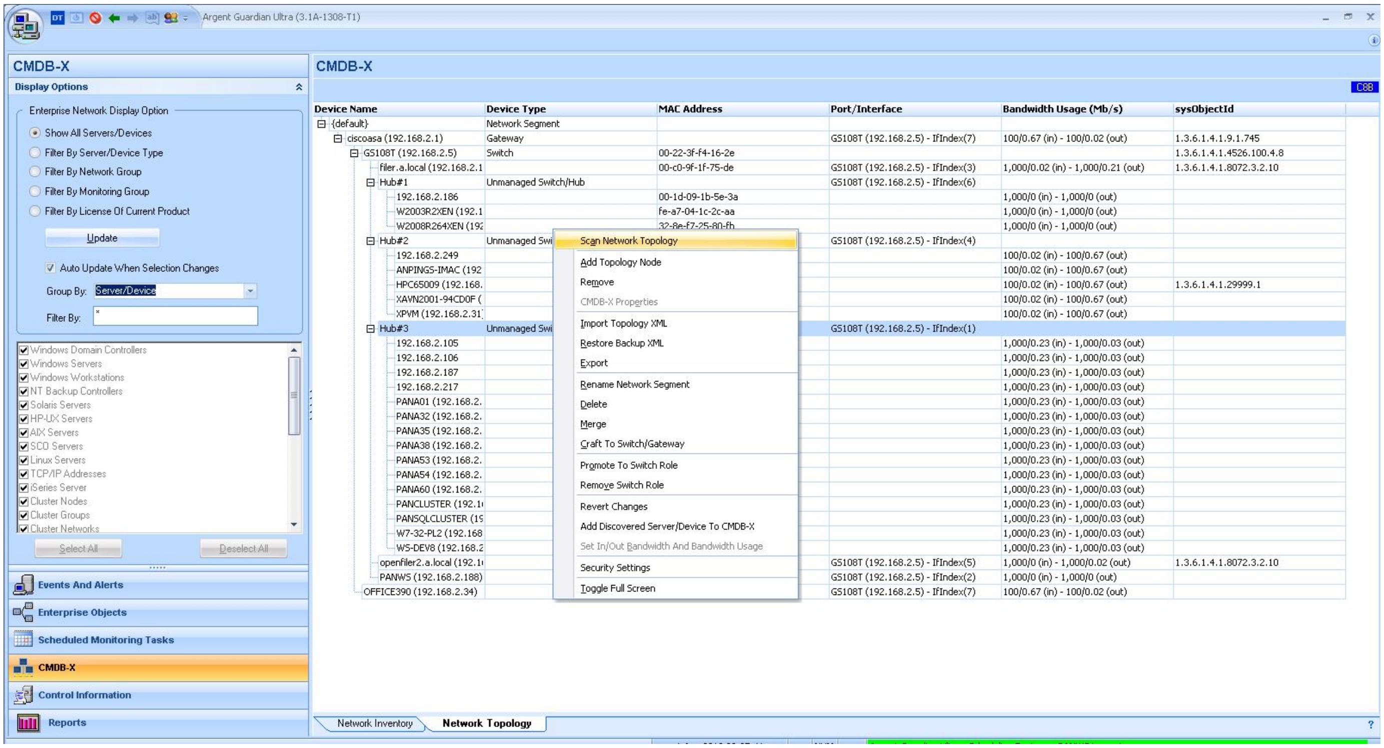
A ‘FAIL’ sample output should look like:

```
<TAGResult>
 <QEResult>
      <STATUS>FAIL</STATUS>
 </QEResult>
</TAGResult>
```

Appendix G – Network Topology

Argent AT can scan the network topology by querying SNMP managed switches. It relies on the support of BRIDGE-MIB to gather the information of port and connections.

To scan the network topology, use the context menu ‘Scan Network Topology’.

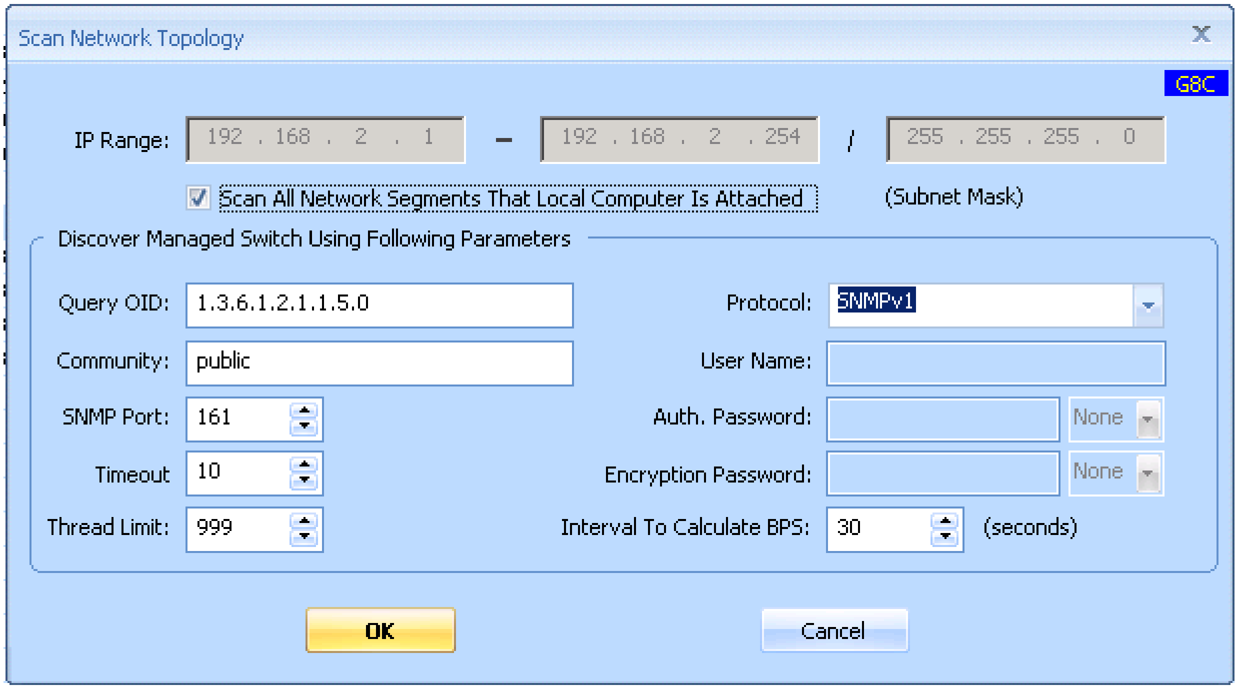


Group By: Server/Device

Filter By: *

Device Name	Device Type	MAC Address	Port/Interface	Bandwidth Usage (Mb/s)	sysObjectId
⊟ {default}	Network Segment				
⊟ ciscoasa (192.168.2.1)	Gateway		GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	1.3.6.1.4.1.9.1.745
⊟ GS108T (192.168.2.5)	Switch	00-22-3f-f4-16-2e			1.3.6.1.4.1.4526.100.4.8
filer.a.local (192.168.2.1		00-c0-9f-1f-75-de	GS108T (192.168.2.5) - IfIndex(3)	1,000/0.02 (in) - 1,000/0.21 (out)	1.3.6.1.4.1.8072.3.2.10
⊟ Hub#1	Unmanaged Switch/Hub		GS108T (192.168.2.5) - IfIndex(6)		
192.168.2.186		00-1d-09-1b-5e-3a		1,000/0 (in) - 1,000/0 (out)	
W2003R2XEN (192.1		fe-a7-04-1c-2c-aa		1,000/0 (in) - 1,000/0 (out)	
W2008R264XEN (192		32-8e-f7-25-80-fb		1,000/0 (in) - 1,000/0 (out)	
⊟ Hub#2	Unmanaged Swi		GS108T (192.168.2.5) - IfIndex(4)		
192.168.2.249				100/0.02 (in) - 100/0.67 (out)	
ANPINGS-IMAC (192				100/0.02 (in) - 100/0.67 (out)	
HPC65009 (192.168.				100/0.02 (in) - 100/0.67 (out)	1.3.6.1.4.1.29999.1
XAVN2001-94CD0F (				100/0.02 (in) - 100/0.67 (out)	
XPVM (192.168.2.31				100/0.02 (in) - 100/0.67 (out)	
⊟ Hub#3	Unmanaged Swi		GS108T (192.168.2.5) - IfIndex(1)		
192.168.2.105				1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.106				1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.187				1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.217				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA01 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA32 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA35 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA38 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA53 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA54 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA60 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANCLUSTER (192.1				1,000/0.23 (in) - 1,000/0.03 (out)	
PANSQLCLUSTER (19				1,000/0.23 (in) - 1,000/0.03 (out)	
W7-32-PL2 (192.168				1,000/0.23 (in) - 1,000/0.03 (out)	
WS-DEV8 (192.168.2				1,000/0.23 (in) - 1,000/0.03 (out)	
openfiler2.a.local (192.1			GS108T (192.168.2.5) - IfIndex(5)	1,000/0 (in) - 1,000/0.02 (out)	1.3.6.1.4.1.8072.3.2.10
PANWS (192.168.2.188)			GS108T (192.168.2.5) - IfIndex(2)	1,000/0 (in) - 1,000/0 (out)	
OFFICE390 (192.168.2.34)			GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	

A dialog box of options is shown before the actual network topology scanning.



IP Range: 192 . 168 . 2 . 1 – 192 . 168 . 2 . 254 / 255 . 255 . 255 . 0 (Subnet Mask)

☑ Scan All Network Segments That Local Computer Is Attached

Discover Managed Switch Using Following Parameters

Query OID: 1.3.6.1.2.1.1.5.0

Community: public

SNMP Port: 161

Timeout 10

Thread Limit: 999

Protocol: SNMPv1

User Name:

Auth. Password: None

Encryption Password: None

Interval To Calculate BPS: 30 (seconds)

If the local machine has multiple network interfaces, customers can opt to scan all or just one using the option 'Scan All Network Segments That Local Computer Is Attached'.

After scanning is done, the network topology screen is populated with the discovered topology.

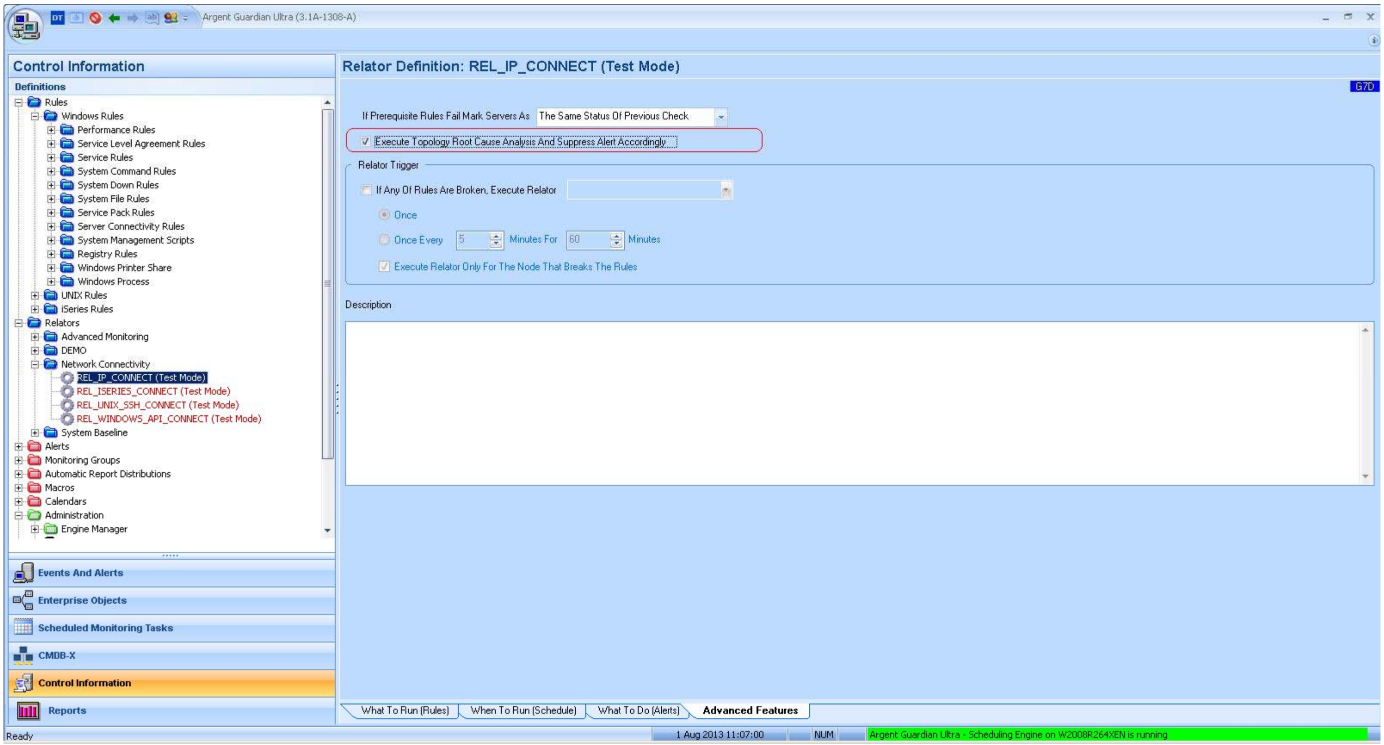
Network Topology And Root Cause Analysis

Network Topology allows administrators to see the network layout easily. Argent AT engine also uses this information to do root cause analysis.

One common complaint about other networking products by the Network Administrator is that he is blasted with a flood of alerts of down servers when a switch or router fails.

In contrast, with Argent -- if network topology is maintained and used properly – the Network Administrator is alerted with a single event of the down switch.

To use network topology for root cause analysis, customers need to turn on this option in the Relator.



Relator Definition: REL_IP_CONNECT (Test Mode)

If Prerequisite Rules Fail Mark Servers As: The Same Status Of Previous Check

☑ Execute Topology Root Cause Analysis And Suppress Alert Accordingly

Relator Trigger

☐ If Any Of Rules Are Broken, Execute Relator

● Once

○ Once Every 5 Minutes For 60 Minutes

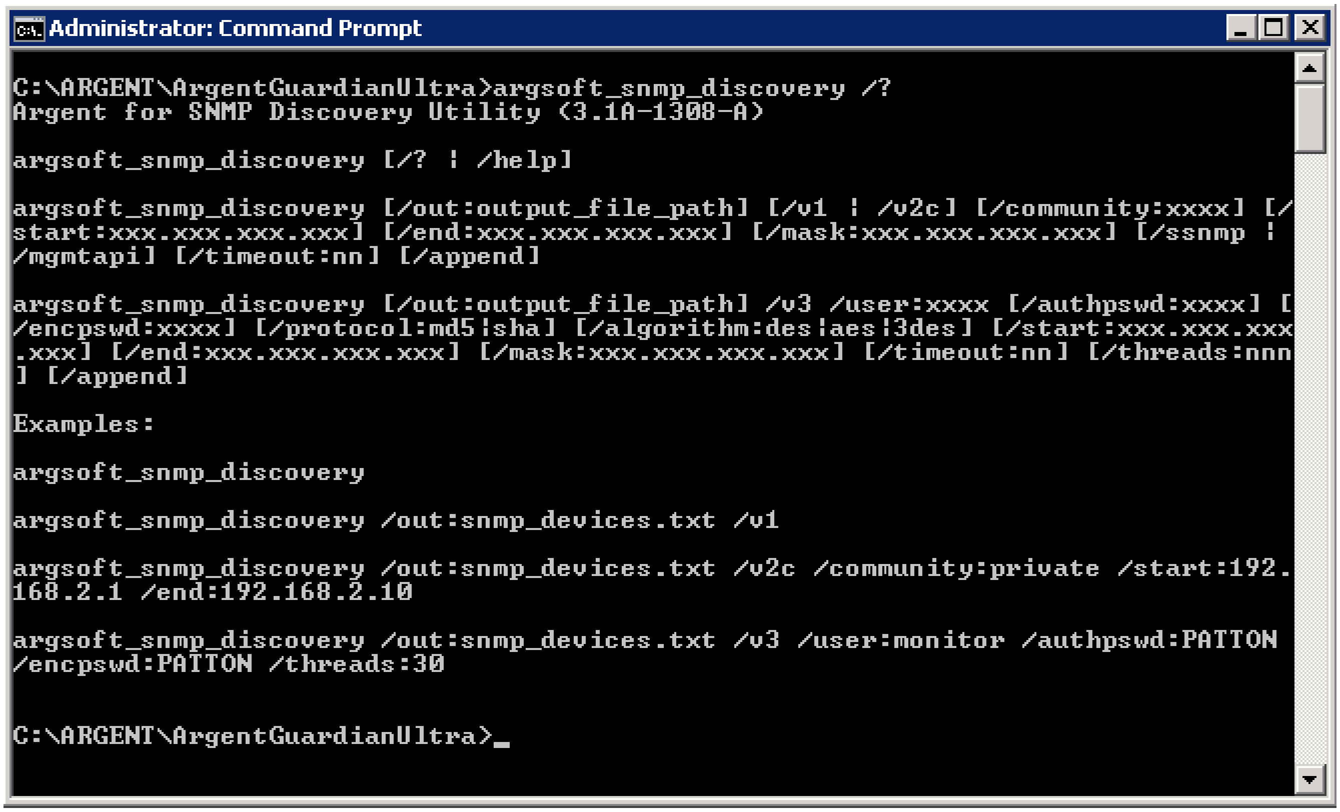
☑ Execute Relator Only For The Node That Breaks The Rules

Description

Command Line Tool - Discover SNMP Devices

Argent AT provides a command line tool to discover SNMP devices in the network.

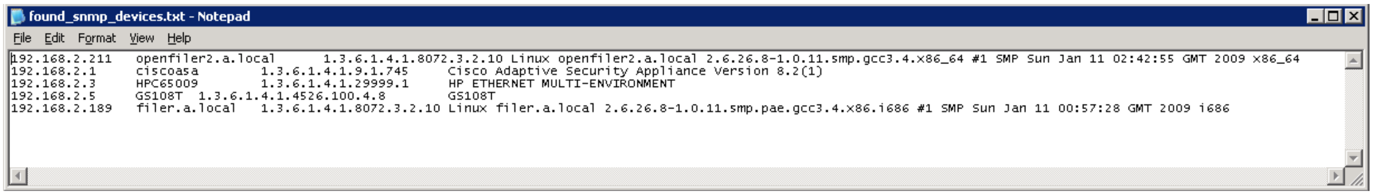
The executable has no dependency so it can be copied and run from any SNMP management workstation.



```
C:\ARGENT\ArgentGuardianUltra>argsoft_snmp_discovery /?
Argent for SNMP Discovery Utility (3.1A-1308-A)

argsoft_snmp_discovery [/? | /help]

argsoft_snmp_discovery [/out:output_file_path] [/v1 | /v2c] [/community:xxxx] [/
start:xxx.xxx.xxx.xxx] [/end:xxx.xxx.xxx.xxx] [/mask:xxx.xxx.xxx.xxx] [/ssnmp |
/mgmtapi] [/timeout:nn] [/append]

argsoft_snmp_discovery [/out:output_file_path] /v3 /user:xxxx [/authpswd:xxxx] [
/encpswd:xxxx] [/protocol:md5|sha] [/algorithm:des|aes|3des] [/start:xxx.xxx.xxx
.xxx] [/end:xxx.xxx.xxx.xxx] [/mask:xxx.xxx.xxx.xxx] [/timeout:nn] [/threads:nnn
] [/append]

Examples:

argsoft_snmp_discovery

argsoft_snmp_discovery /out:snmp_devices.txt /v1

argsoft_snmp_discovery /out:snmp_devices.txt /v2c /community:private /start:192.
168.2.1 /end:192.168.2.10

argsoft_snmp_discovery /out:snmp_devices.txt /v3 /user:monitor /authpswd:PATTON
/encpswd:PATTON /threads:30


C:\ARGENT\ArgentGuardianUltra>_
```

The default output file is ‘found_snmp_devices.txt’ in the same directory as the executable.

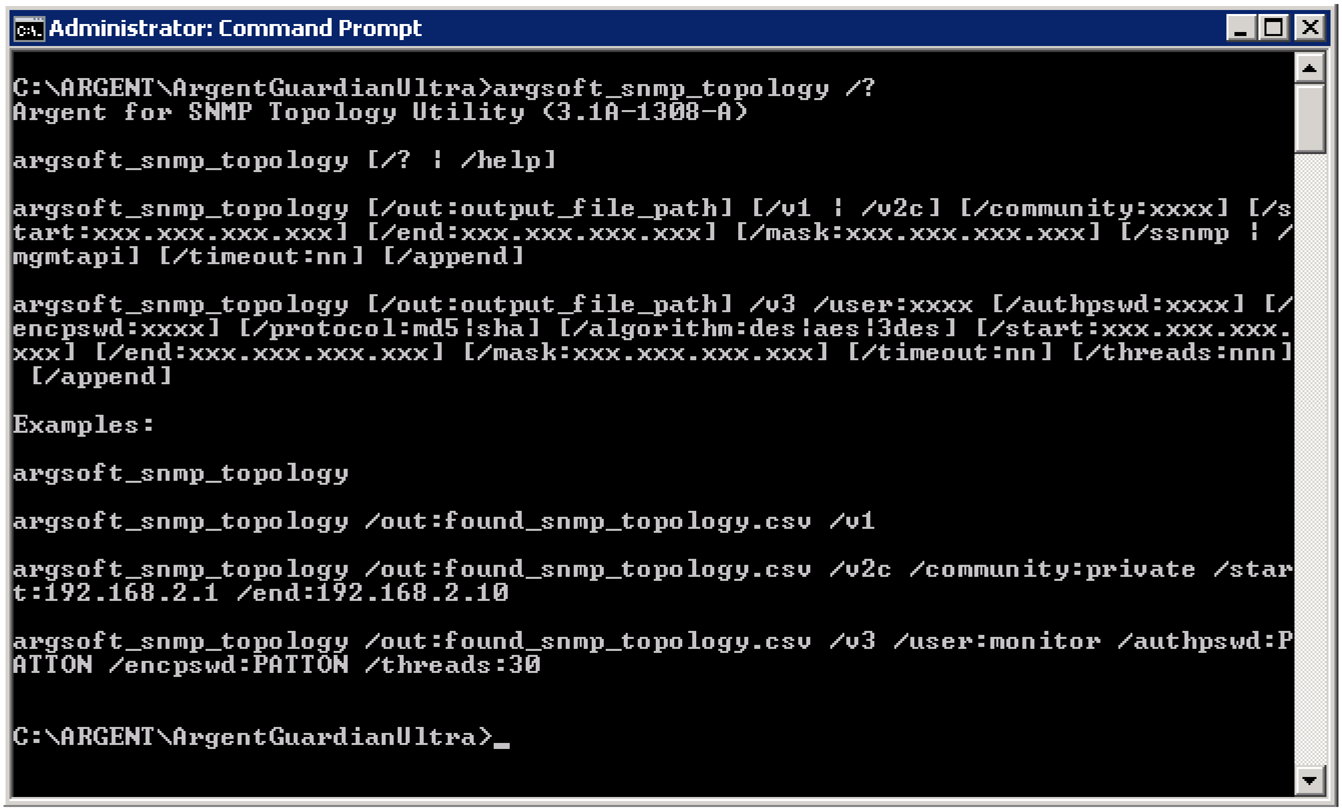
A sample result is shown as follows:



```
192.168.2.211    openfiler2.a.local      1.3.6.1.4.1.8072.3.2.10 Linux openfiler2.a.local 2.6.26.8-1.0.11.smp.gcc3.4.x86_64 #1 SMP Sun Jan 11 02:42:55 GMT 2009 x86_64
192.168.2.1      ciscoasa        1.3.6.1.4.1.9.1.745     Cisco Adaptive Security Appliance Version 8.2(1)
192.168.2.3      HPC65009        1.3.6.1.4.1.29999.1     HP ETHERNET MULTI-ENVIRONMENT
192.168.2.5      GS108T  1.3.6.1.4.1.4526.100.4.8        GS108T
192.168.2.189    filer.a.local   1.3.6.1.4.1.8072.3.2.10 Linux filer.a.local 2.6.26.8-1.0.11.smp.pae.gcc3.4.x86.i686 #1 SMP Sun Jan 11 00:57:28 GMT 2009 i686
```

Command Line Tool - Discover Network Topology

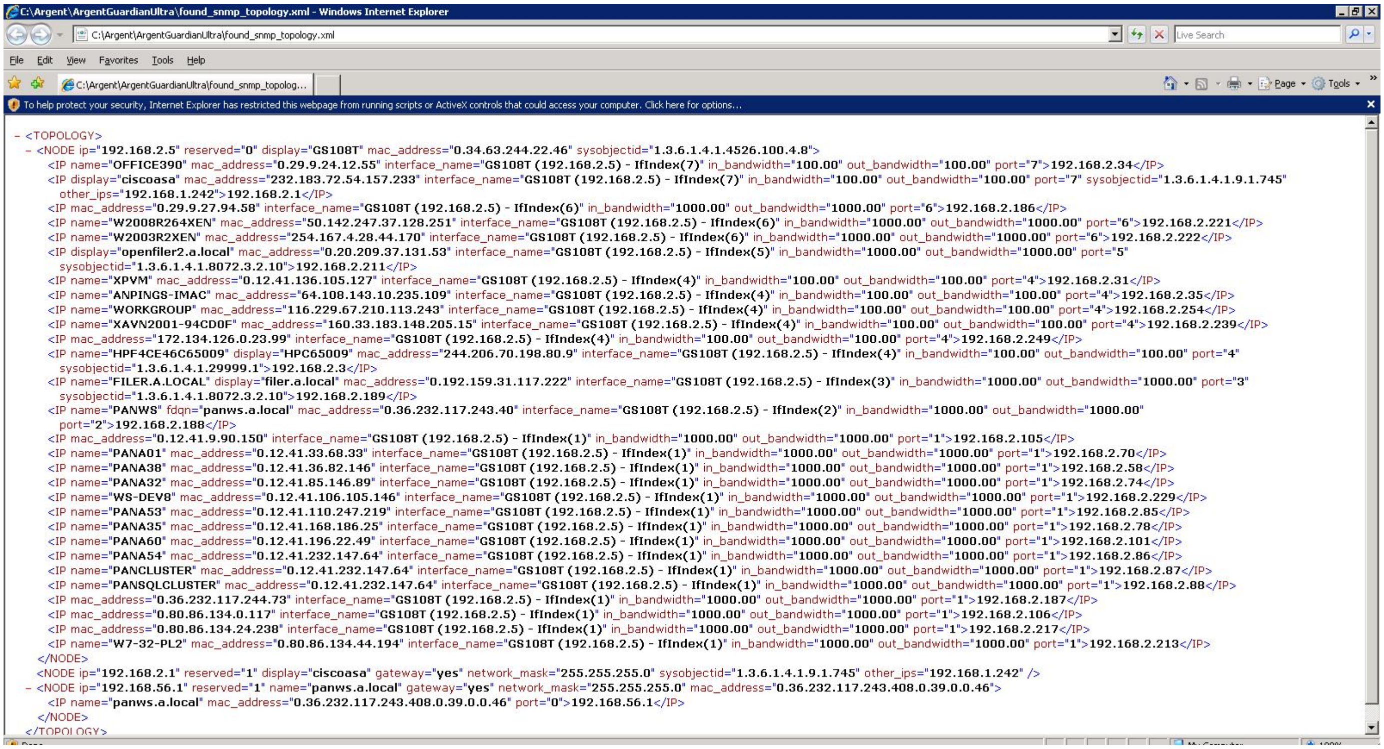
Argent AT provides a command line tool to scan network topology. The executable has no dependency so it can be copied and run from any SNMP management workstation.



```
C:\ARGENT\ArgentGuardianUltra>argsoft_snmp_topology /?
Argent for SNMP Topology Utility (3.1A-1308-A)

argsoft_snmp_topology [/? | /help]

argsoft_snmp_topology [/out:output_file_path] [/v1 | /v2c] [/community:xxxx] [/s
tart:xxx.xxx.xxx.xxx] [/end:xxx.xxx.xxx.xxx] [/mask:xxx.xxx.xxx.xxx] [/ssnmp | /
mgmtapi] [/timeout:nn] [/append]

argsoft_snmp_topology [/out:output_file_path] /v3 /user:xxxx [/authpswd:xxxx] [/
encpswd:xxxx] [/protocol:md5|sha] [/algorithm:des|aes|3des] [/start:xxx.xxx.xxx.
xxx] [/end:xxx.xxx.xxx.xxx] [/mask:xxx.xxx.xxx.xxx] [/timeout:nn] [/threads:nnn]
 [/append]

Examples:

argsoft_snmp_topology

argsoft_snmp_topology /out:found_snmp_topology.csv /v1

argsoft_snmp_topology /out:found_snmp_topology.csv /v2c /community:private /star
t:192.168.2.1 /end:192.168.2.10

argsoft_snmp_topology /out:found_snmp_topology.csv /v3 /user:monitor /authpswd:P
ATTON /encpswd:PATTON /threads:30


C:\ARGENT\ArgentGuardianUltra>_
```

Customers can specify the output file as either XML or CSV format. The default output file is **‘found_snmp_topology.xml’** in the same directory as the executable.

A sample result is shown as follows:

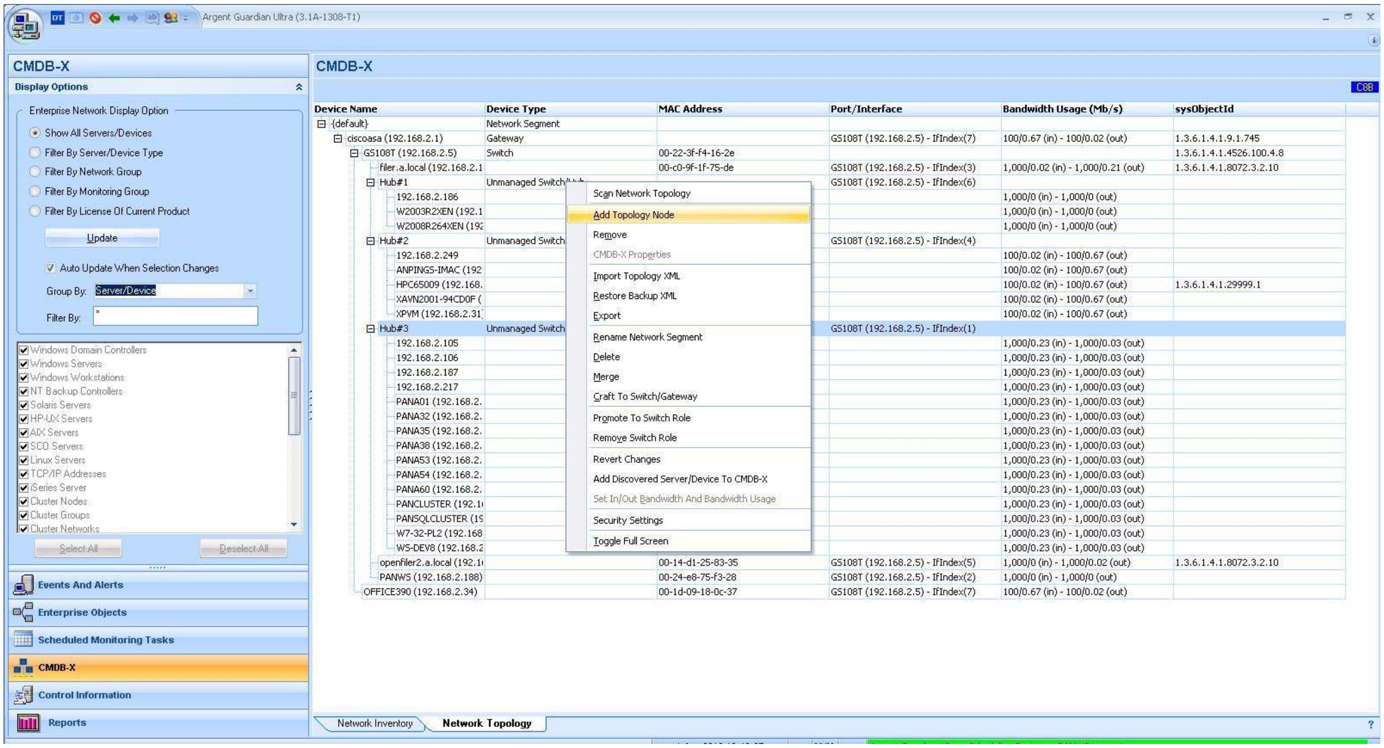

C:\Argent\ArgentGuardianUltra\found_snmp_topology.xml - Windows Internet Explorer
C:\Argent\ArgentGuardianUltra\found_snmp_topology.xml
Live Search
File
Edit
View
Favorites
Tools
Help
C:\Argent\ArgentGuardianUltra\found_snmp_topolog...
Page
Tools
To help protect your security, Internet Explorer has restricted this webpage from running scripts or ActiveX controls that could access your computer. Click here for options...

```
- <TOPOLOGY>
 - <NODE ip="192.168.2.5" reserved="0" display="GS108T" mac_address="0.34.63.244.22.46" sysobjectid="1.3.6.1.4.1.4526.100.4.8">
     <IP name="OFFICE390" mac_address="0.29.9.24.12.55" interface_name="GS108T (192.168.2.5) - IfIndex(7)" in_bandwidth="100.00" out_bandwidth="100.00" port="7">192.168.2.34</IP>
     <IP display="ciscoasa" mac_address="232.183.72.54.157.233" interface_name="GS108T (192.168.2.5) - IfIndex(7)" in_bandwidth="100.00" out_bandwidth="100.00" port="7" sysobjectid="1.3.6.1.4.1.9.1.745"
       other_ips="192.168.1.242">192.168.2.1</IP>
     <IP mac_address="0.29.9.27.94.58" interface_name="GS108T (192.168.2.5) - IfIndex(6)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="6">192.168.2.186</IP>
     <IP name="W2008R264XEN" mac_address="50.142.247.37.128.251" interface_name="GS108T (192.168.2.5) - IfIndex(6)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="6">192.168.2.221</IP>
     <IP name="W2003R2XEN" mac_address="254.167.4.28.44.170" interface_name="GS108T (192.168.2.5) - IfIndex(6)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="6">192.168.2.222</IP>
     <IP display="openfiler2.a.local" mac_address="0.20.209.37.131.53" interface_name="GS108T (192.168.2.5) - IfIndex(5)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="5"
       sysobjectid="1.3.6.1.4.1.8072.3.2.10">192.168.2.211</IP>
     <IP name="XPVM" mac_address="0.12.41.136.105.127" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_bandwidth="100.00" port="4">192.168.2.31</IP>
     <IP name="ANPINGS-IMAC" mac_address="64.108.143.10.235.109" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_bandwidth="100.00" port="4">192.168.2.35</IP>
     <IP name="WORKGROUP" mac_address="116.229.67.210.113.243" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_bandwidth="100.00" port="4">192.168.2.254</IP>
     <IP name="XAVN2001-94CD0F" mac_address="160.33.183.148.205.15" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_bandwidth="100.00" port="4">192.168.2.239</IP>
     <IP mac_address="172.134.126.0.23.99" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_bandwidth="100.00" port="4">192.168.2.249</IP>
     <IP name="HPF4CE46C65009" display="HPC65009" mac_address="244.206.70.198.80.9" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_bandwidth="100.00" port="4"
       sysobjectid="1.3.6.1.4.1.29999.1">192.168.2.3</IP>
     <IP name="FILER.A.LOCAL" display="filer.a.local" mac_address="0.192.159.31.117.222" interface_name="GS108T (192.168.2.5) - IfIndex(3)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="3"
       sysobjectid="1.3.6.1.4.1.8072.3.2.10">192.168.2.189</IP>
     <IP name="PANWS" fdqn="panws.a.local" mac_address="0.36.232.117.243.40" interface_name="GS108T (192.168.2.5) - IfIndex(2)" in_bandwidth="1000.00" out_bandwidth="1000.00"
       port="2">192.168.2.188</IP>
     <IP mac_address="0.12.41.9.90.150" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.105</IP>
     <IP name="PANA01" mac_address="0.12.41.33.68.33" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.70</IP>
     <IP name="PANA38" mac_address="0.12.41.36.82.146" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.58</IP>
     <IP name="PANA32" mac_address="0.12.41.85.146.89" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.74</IP>
     <IP name="WS-DEV8" mac_address="0.12.41.106.105.146" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.229</IP>
     <IP name="PANA53" mac_address="0.12.41.110.247.219" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.85</IP>
     <IP name="PANA35" mac_address="0.12.41.168.186.25" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.78</IP>
     <IP name="PANA60" mac_address="0.12.41.196.22.49" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.101</IP>
     <IP name="PANA54" mac_address="0.12.41.232.147.64" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.86</IP>
     <IP name="PANCLUSTER" mac_address="0.12.41.232.147.64" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.87</IP>
     <IP name="PANSQLCLUSTER" mac_address="0.12.41.232.147.64" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.88</IP>
     <IP mac_address="0.36.232.117.244.73" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.187</IP>
     <IP mac_address="0.80.86.134.0.117" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.106</IP>
     <IP mac_address="0.80.86.134.24.238" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.217</IP>
     <IP name="W7-32-PL2" mac_address="0.80.86.134.44.194" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.00" port="1">192.168.2.213</IP>
   </NODE>
   <NODE ip="192.168.2.1" reserved="1" display="ciscoasa" gateway="yes" network_mask="255.255.255.0" sysobjectid="1.3.6.1.4.1.9.1.745" other_ips="192.168.1.242" />
 - <NODE ip="192.168.56.1" reserved="1" name="panws.a.local" gateway="yes" network_mask="255.255.255.0" mac_address="0.36.232.117.243.408.0.39.0.0.46">
     <IP name="panws.a.local" mac_address="0.36.232.117.243.408.0.39.0.0.46" port="0">192.168.56.1</IP>
   </NODE>
 </TOPOLOGY>
```

Maintain Network Topology Manually

Argent AT relies on SNMP managed switches, which must support BRIDGE-MIB, to gather the port and connection information. Not all switches have SNMP feature, let alone BRIDGE-MIB support. As a result, network topology may not always be successful or complete.

Argent AT fully supports manual editing of network topology.



CMDB-X

Display Options

Enterprise Network Display Option

● Show All Servers/Devices
○ Filter By Server/Device Type
○ Filter By Network Group
○ Filter By Monitoring Group
○ Filter By License Of Current Product

Update

☑ Auto Update When Selection Changes

Group By: Server/Device

Filter By: *

☑ Windows Domain Controllers
☑ Windows Servers
☑ Windows Workstations
☑ NT Backup Controllers
☑ Solaris Servers
☑ HP-UX Servers
☑ AIX Servers
☑ SCO Servers
☑ Linux Servers
☑ TCP/IP Addresses
☑ iSeries Server
☑ Cluster Nodes
☑ Cluster Groups
☑ Cluster Networks

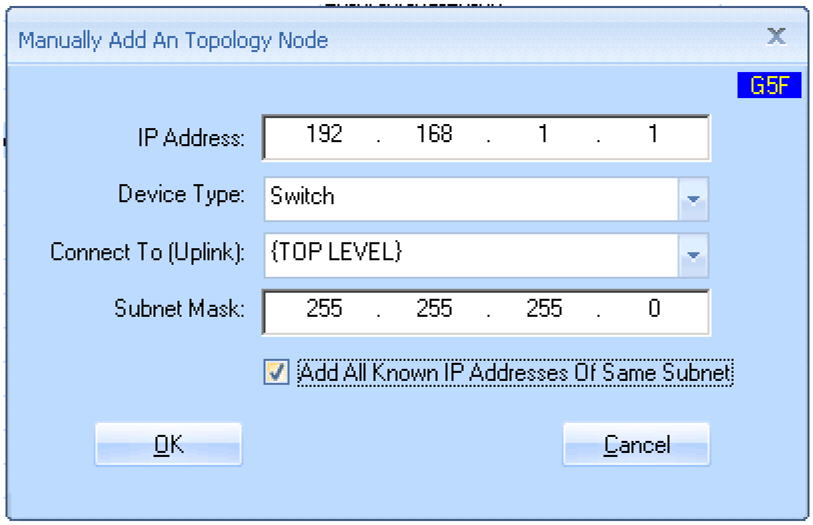
Select All Deselect All

CMDB-X

Device Name	Device Type	MAC Address	Port/Interface	Bandwidth Usage (Mb/s)	sysObjectId
{default}	Network Segment				
ciscoasa (192.168.2.1)	Gateway		GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	1.3.6.1.4.1.9.1.745
GS108T (192.168.2.5)	Switch	00-22-3f-f4-16-2e			1.3.6.1.4.1.4526.100.4.8
filer.a.local (192.168.2.1		00-c0-9f-1f-75-de	GS108T (192.168.2.5) - IfIndex(3)	1,000/0.02 (in) - 1,000/0.21 (out)	1.3.6.1.4.1.8072.3.2.10
Hub#1	Unmanaged Switch/		GS108T (192.168.2.5) - IfIndex(6)		
192.168.2.186				1,000/0 (in) - 1,000/0 (out)	
W2003R2XEN (192.1				1,000/0 (in) - 1,000/0 (out)	
W2008R264XEN (192				1,000/0 (in) - 1,000/0 (out)	
Hub#2	Unmanaged Switch		GS108T (192.168.2.5) - IfIndex(4)		
192.168.2.249				100/0.02 (in) - 100/0.67 (out)	
ANPINGS-IMAC (192				100/0.02 (in) - 100/0.67 (out)	
HPC65009 (192.168.				100/0.02 (in) - 100/0.67 (out)	1.3.6.1.4.1.29999.1
XAVN2001-94CD0F (				100/0.02 (in) - 100/0.67 (out)	
XPVM (192.168.2.31				100/0.02 (in) - 100/0.67 (out)	
Hub#3	Unmanaged Switch		GS108T (192.168.2.5) - IfIndex(1)		
192.168.2.105				1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.106				1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.187				1,000/0.23 (in) - 1,000/0.03 (out)	
192.168.2.217				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA01 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA32 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA35 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA38 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA53 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA54 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANA60 (192.168.2.				1,000/0.23 (in) - 1,000/0.03 (out)	
PANCLUSTER (192.1				1,000/0.23 (in) - 1,000/0.03 (out)	
PANSQLCLUSTER (1				1,000/0.23 (in) - 1,000/0.03 (out)	
W7-32-PL2 (192.168				1,000/0.23 (in) - 1,000/0.03 (out)	
WS-DEV8 (192.168.2				1,000/0.23 (in) - 1,000/0.03 (out)	
openfiler2.a.local (192.1		00-14-d1-25-83-35	GS108T (192.168.2.5) - IfIndex(5)	1,000/0 (in) - 1,000/0.02 (out)	1.3.6.1.4.1.8072.3.2.10
PANWS (192.168.2.188)		00-24-e8-75-f3-28	GS108T (192.168.2.5) - IfIndex(2)	1,000/0 (in) - 1,000/0 (out)	
OFFICE390 (192.168.2.34)		00-1d-09-18-0c-37	GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	

Add Topology Node

When customers add a top-level gateway or router, it is handy to use the option ‘Add All Known IP Addresses Of Same Subnet’. Of course, customers have to do ICMP Ping scanning of the network segment first to crop all the known IP addresses in the segment.



Manually Add An Topology Node

G5F

IP Address: 192 . 168 . 1 . 1

Device Type: Switch

Connect To (Uplink): {TOP LEVEL}

Subnet Mask: 255 . 255 . 255 . 0

☑ Add All Known IP Addresses Of Same Subnet

Remove Topology Node

If a switch is removed, all the child nodes can be removed as well.

Import Topology XML

Typically the XML is the result file of command line utility ARGSOFT_SNMP_TOPOLOGY.EXE.

It will add the nodes in the XML into the current topology.

Restore Backup XML

It replaces the current topology with information in the backup XML.

Export

It generates a backup XML that can be used for later restoration.

Rename Network Segment

Rename the network segment name in the topology. It is the folder in the topology, generally representing a gateway, router, switch or hub.

Delete Network Segment

Delete a whole network segment. This is a destructive operation. Argent recommends customersto backup the topology using ‘Export’ first.

Merge

Merge selected network segments with another network segment.

Craft To Switch Or Gateway

Craft selected network segment under a switch or gateway.

Merge

Merge selected network segment with another network segment.

Promote To Switch Role

Promote a node to a switch role so that child nodes can be added under.

Remove Switch Role

Remove the switch role from a node.

Revert Changes

Undo the change. The undo information is cached in memory. If customers exit the program, all undo information is lost.

Add Discovered Server/Devices To CMDB-X

Add any nodes in topology that is not in CMDB-X yet to CMDB-X database.

Appendix H – CMDB-X SQL Tables

In contrast to most vendors, Argent provides a full and complete schema of the database tables used in the Argent Atlas CMDB-X.

ARGSOFT_AT_LAN

This table stores the information of network segments in the enterprise:

Field	Type	Description
UUID	varchar(36)	Unique Identifier
CREATE_TIME	datetime	Record creation time
MODIFY_TIME	datetime	Last modified time
NAME	nvarchar(256)	Network segment name
DESCRIPTION	nvarchar(1024)	Description
NETWORK	int	Network type 1 – T1 2 – DSL 3 – Cable Modem 4 – ISDN 5 – Frame Relay 6 – VPN or Dial-up (inbound) 7 – VPN or Dial-up (outbound)
FIREWALL	int	Firewall (Boolean) 0 – Not enabled 1 – Enabled
CONTACT_ADMIN	nvarchar(256)	Administrative contact name
CONTACT_EMAIL	nvarchar(256)	Administrative contact email
CONTACT_PHONE	nvarchar(256)	Administrative contact phone
DEFAULT_ALERT	nvarchar(256)	Default alert
DEFAULT_EXECUTOR	nvarchar(256)	Default Argent Alert Executor

OTHERS	ntext	Container field that holds product specific settings.
OWNER	nvarchar(256)	Owner
CRC_LOW	int	CRC low
CRC_HIGH	int	CRC high

ARGSOFT_AT_NODE

This table stores the information of known servers and devices in the enterprise

Relationship: ARGSOFT_AT_NODE.LAN = ARGSOFT_AT_LAN.UUID

Field	Type	Description
UUID	varchar(36)	Unique Identifier
CREATE_TIME	datetime	Record creation time
MODIFY_TIME	datetime	Last modified time
NAME	nvarchar(256)	Node name
INTERNAL_NAME	nvarchar(256)	Internal name for the node
DESCRIPTION	nvarchar(1024)	Description
NODE_DOMAIN	nvarchar(256)	Domain name
NODE_TYPE	int	Node type. 0x1 (1) – Windows Domain Controller 0x2 (2) – Windows Backup Domain Controller 0x4 (4) – Windows Server 0x8 (8) – Windows Workstation 0x10 (16) – Sun Solaris 0x20 (32) – HP-UX 0x40 (64) – AIX 0x80 (128) – SCO Unix 0x100 (256) – Linux 0x200 (512) – IP Address 0x400 (1,024) – iSeries Server 0x800 (2,048) – Cluster Node 0x1000 (4,096) – Cluster Group 0x2000 (8,192) – Cluster Network 0x4000 (16,384) – Cluster Network Interface 0x8000 (32,768) – Cluster Resource 0x10000 (65,536) – Printer Queue 0x20000 (131,072) – Windows 9x (obsolete) 0x40000 (262,144) – Novell Server (obsolete) 0x80000 (524,288) – Unknown 0x100000 (1,048,576) – URL Object 0x200000 (2,097,152) – Mail Object 0x400000 (4,194,304) – FTP Object

NETBIOS_NAME	nvarchar(256)	NETBIOS name
ALTERNATIVE_IP	nvarchar(128)	Alternative IP address
ALIAS	nvarchar(256)	Alias
DEFAULT_ALERT_EXECUTOR	nvarchar(256)	Default Argent Alert Executor
VENDOR	nvarchar(256)	Server/Device vendor
MAKE	nvarchar(256)	Server/Device make
MODEL	nvarchar(256)	Server/Device model
SYSOBJECTID	nvarchar(256)	SNMP sysObjectId for the device
LAN	varchar(36)	UUID of Network segment
LOCATION	nvarchar(256)	Location
SUSPEND	int	Boolean value. 0 – Node is active 1 – Node is suspended 2 – (XT Backup Compatible Mode) Node is monitored continuously in the background. The Argent Predictor data is saved but event is fired.
NODE_COLOR	int	Boolean value True – Use explicit color option False – Use default setting
NODE_TX_COLOR	int	Text color when using explicit color option
NODE_BG_COLOR	int	Background color when using explicit color option
TZ_OPTION	int	0 - Fixed Hours 1 - Dynamic Read From Server 2 - Use Trusted Agent 3 - Use Supervising Engine
TZ_HOUR_DIFF	int	Hour difference with GMT
TZ_SERVER	nvarchar(256)	Time server
CONTACT_EMAIL	nvarchar(128)	Contact email address

CONTACT_PHONE	nvarchar(128)	Contact phone number
REMOTE_DESKTOP	nvarchar(256)	Command line for remote desktop session
SUPPORT_URL	nvarchar(256)	Support URL
DISK_SHARES	ntext	Disk shares
LOGIC_DEPENDENCY	nvarchar(256)	Logic dependency
AGGR_DATA_TYPE	int	1 = IP Address And/Or IP Range 2 = Text File 3 = SQL Query
AGGR_DATA_SOURCE	ntext	Data source for the aggregate node
AGGR_QUERY_INTERVAL	int	Query interval for the aggregate node
OWNER	nvarchar(256)	Owner
CRC_LOW	int	CRC low
CRC_HIGH	int	CRC high

ARGSOFT_AT_NODE_APPLICATION

This table stores the names of all installed applications for a particular node.

Relationship: ARGSOFT_AT_NODE_APPLICATION.NODE_UUID = ARSOFT_AT_NODE.UUID

Field	Type	Description
UUID	varchar(36)	Unique Identifier
CREATE_TIME	datetime	Record creation time
MODIFY_TIME	datetime	Last modified time
NODE_UUID	varchar(36)	UUID of node
NAME	nvarchar(256)	Application name
OWNER	nvarchar(256)	Owner
CRC_LOW	int	CRC low
CRC_HIGH	int	CRC high