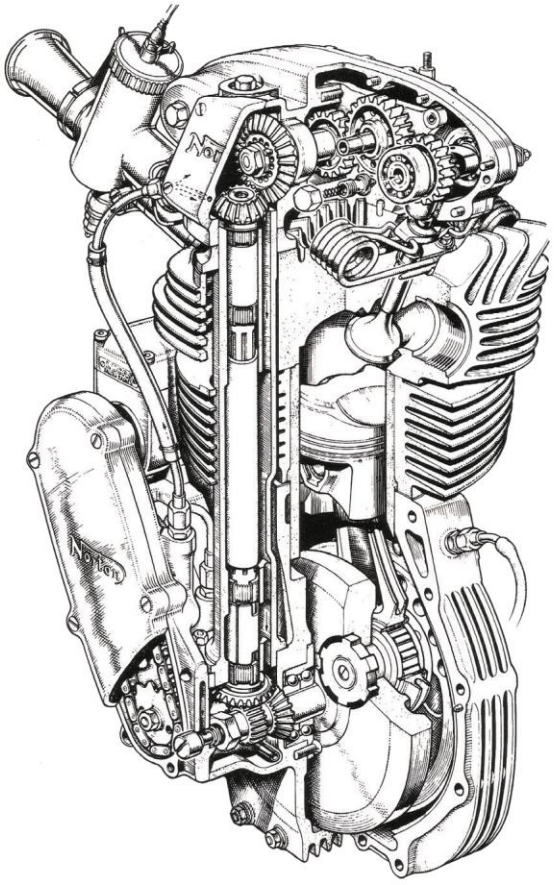
Argent Baseline



www.Argent.com

Table Of Contents

Introduction To Argent Omega 3

Log-On Screen 4

Home Screen 5

Argent Omega Four Building Blocks 15

Tool Sets – Set Of Pre-defined Rules For A Product 16

Relators 17

Workflows 23

Monitoring Groups 69

Generator Settings 75

Generator Configuration: 75

Argent Alert Mechanism Configuration 78

Configure SMS Generator 79

Configure Email Generator 80

Argent SIEM-Complete Configuration 88

Manage Archive Repository 89

License 91

Network Scan 92

Event Logs 97

Adding Devices To Google Maps 101

Adding Devices To Static Map 101

Set Device Location 102

Locations 107

Argent Omega Baseline 113

Service Level Agreement Rules 113

Windows Service Rules 119

Windows Program Rules 121

Windows Performance Rules 122

PowerShell Script Rules 129

WMI Script Rules 131

Proprietary Information – All Rights Reserved

Introduction To Argent Omega

The Argent Omega is the next-generation Argent automation product, combining easy-to-use components with a scalable and reliable architecture.

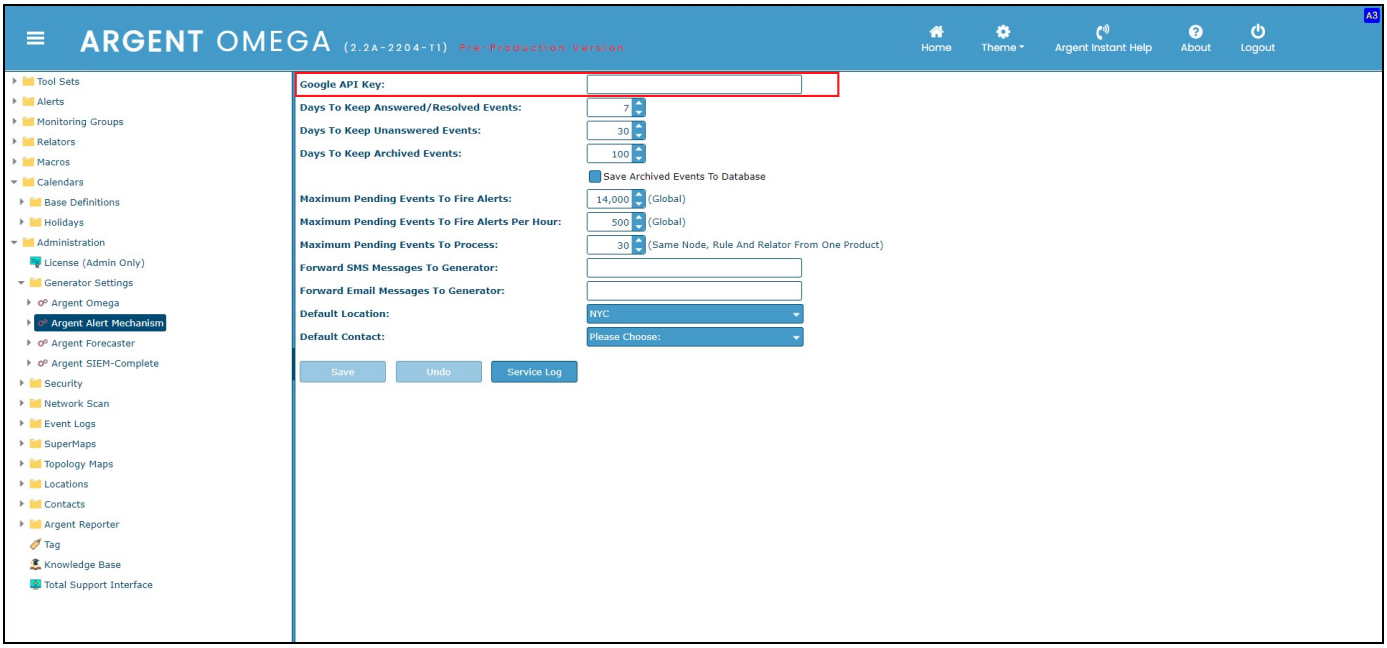
Argent Omega provides a User Interface, which is a single pane of glass where you can see all the building blocks of Argent Monitoring products, even from a tablet while you are sitting in Starbucks.

The Argent Alert Mechanism in Argent Omega consolidates events from Primary, Secondary, and Trusted Generators.

Secondary Generators are the same as Daughter Engines in Argent Advanced Technology products. Trusted Generators are the same as Trusted Engines in Argent Advanced Technology products.

Prerequisites

If you choose to use the Google Maps option, then a Google API key is required to access Google Maps in Location, Argent SuperMaps and Argent Topology Maps; apply the API key either in **Argent Omega Setup** or Argent Alert Mechanism settings under **Generator Settings**



Proprietary Information – All Rights Reserved

Log-On Screen

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

There are three types of user accounts:

- Windows User Accounts
- Demo Accounts
- Internal Accounts

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

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

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

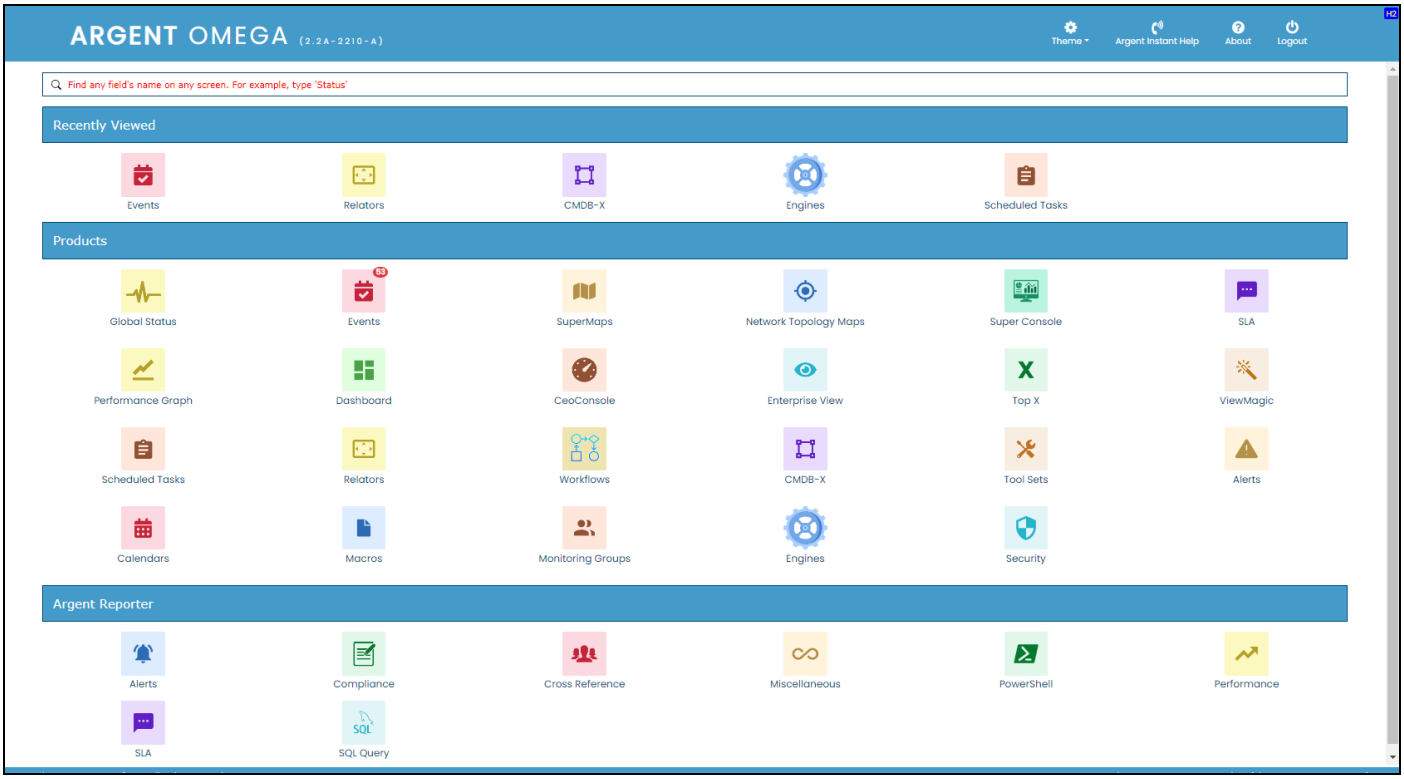
Internal accounts also can be created in the **Argent Omega Security** section, and **behave like normal Windows accounts**, using Argent's private authentication for login.

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

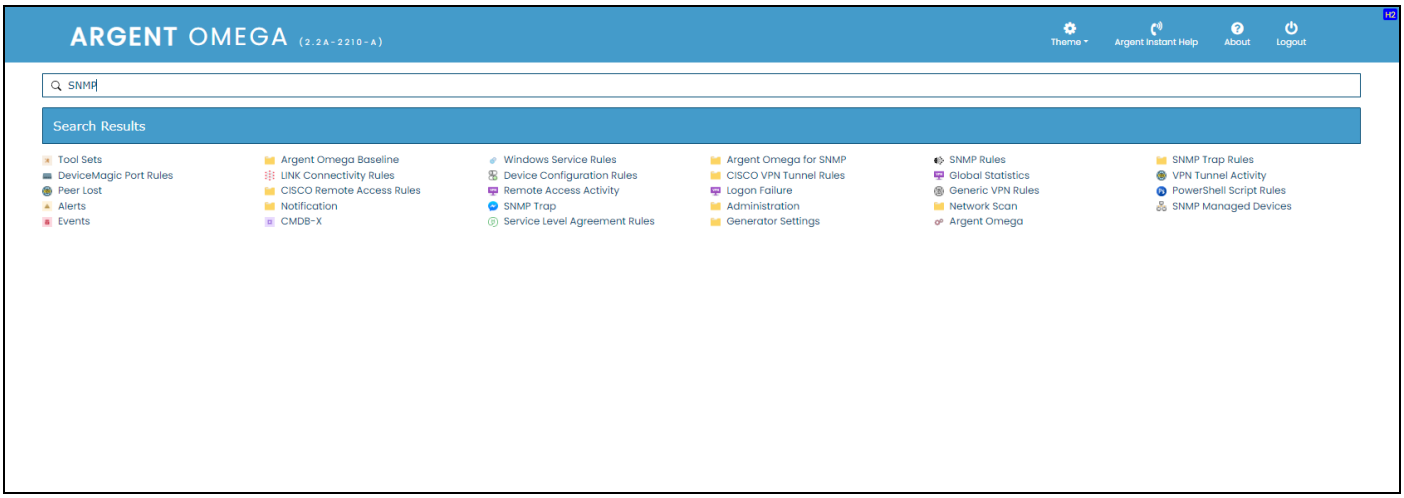
Proprietary Information – All Rights Reserved

Home Screen

After successful login, Argent Omega will redirect to home screen.

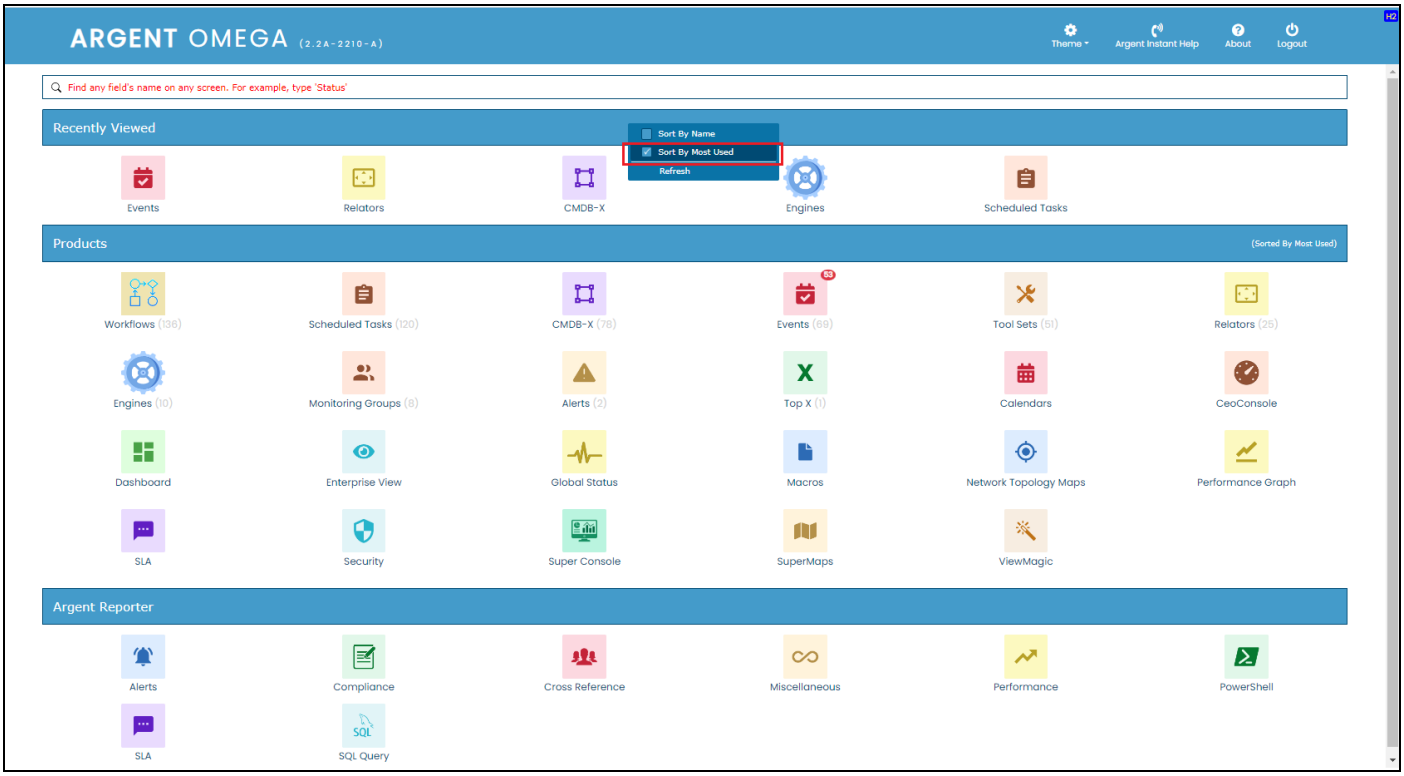


Argent Omega is a powerful search facility. It is possible to search any component or screen in Argent Omega by **screen tag**, label text, list's column name, etc.



Proprietary Information – All Rights Reserved

You can sort items on the Home Screen based on its usage:



CMDB-X

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

Argent added the 'X' for eXtensible.

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

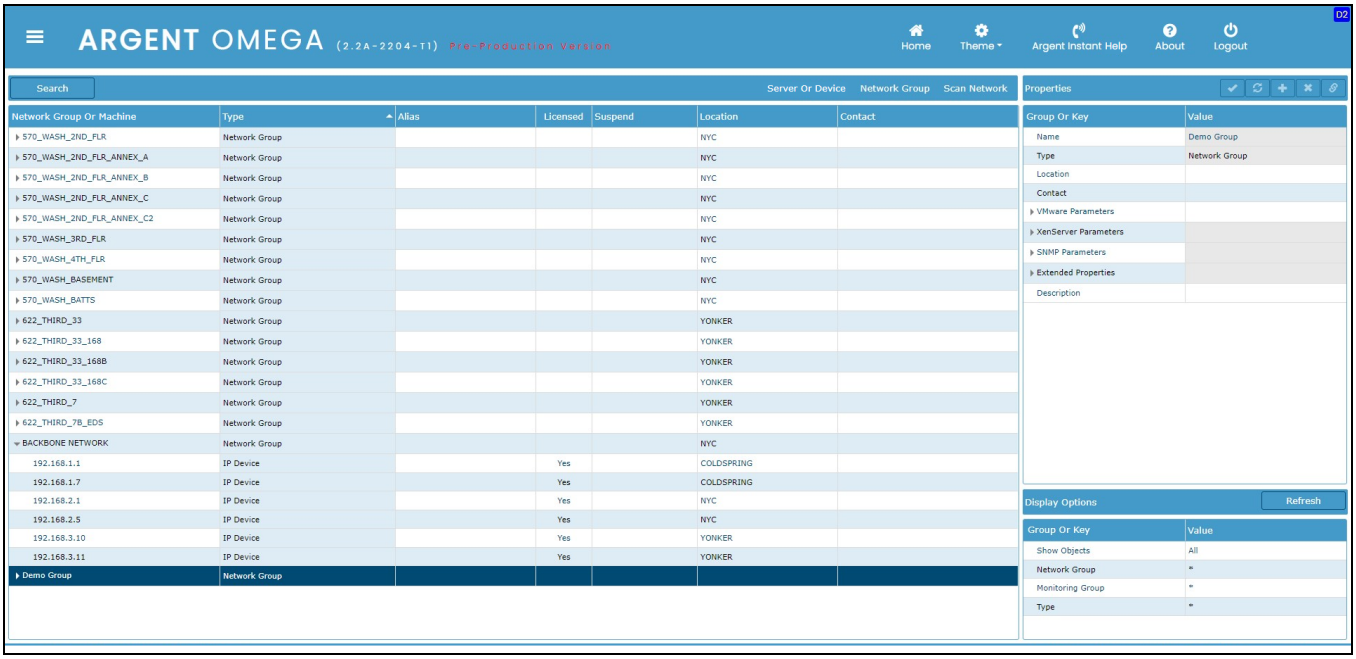
Providing the ability to add custom fields allows customers to use the Argent CMDB-X as an IT Asset Management tool.

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

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

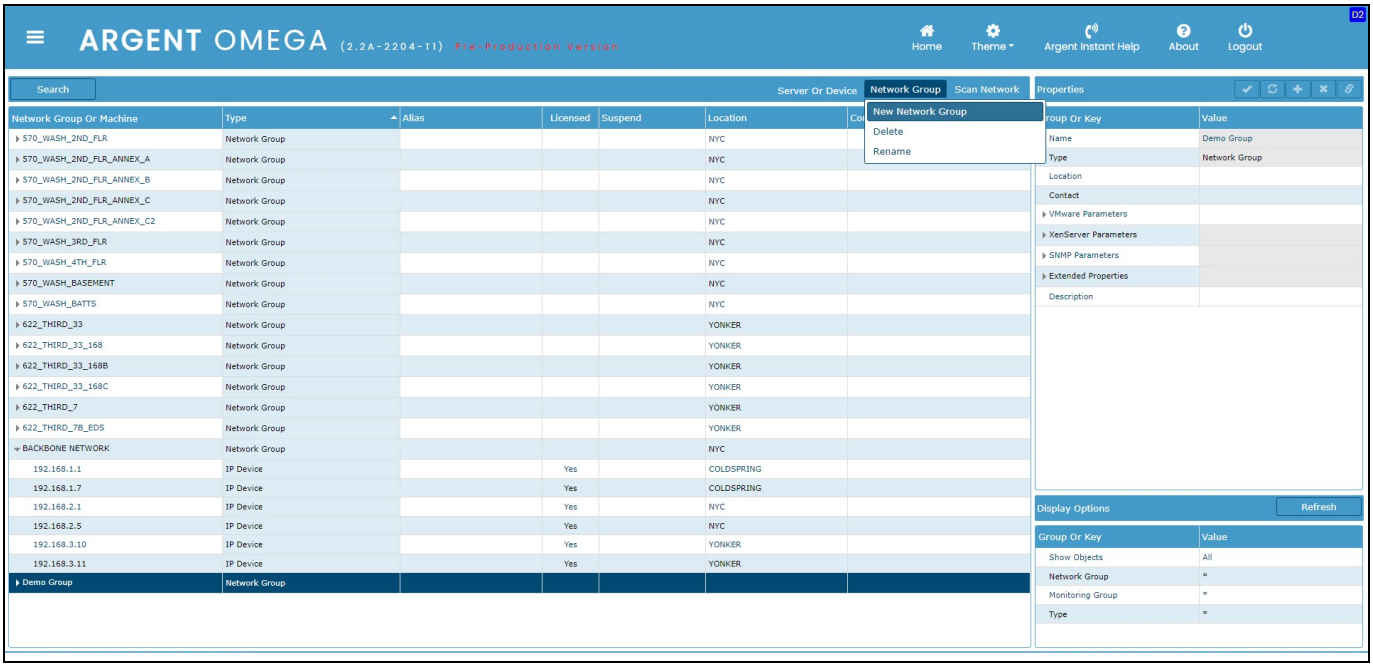
The Argent CMDB-X also has options to import from external Excel files.

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

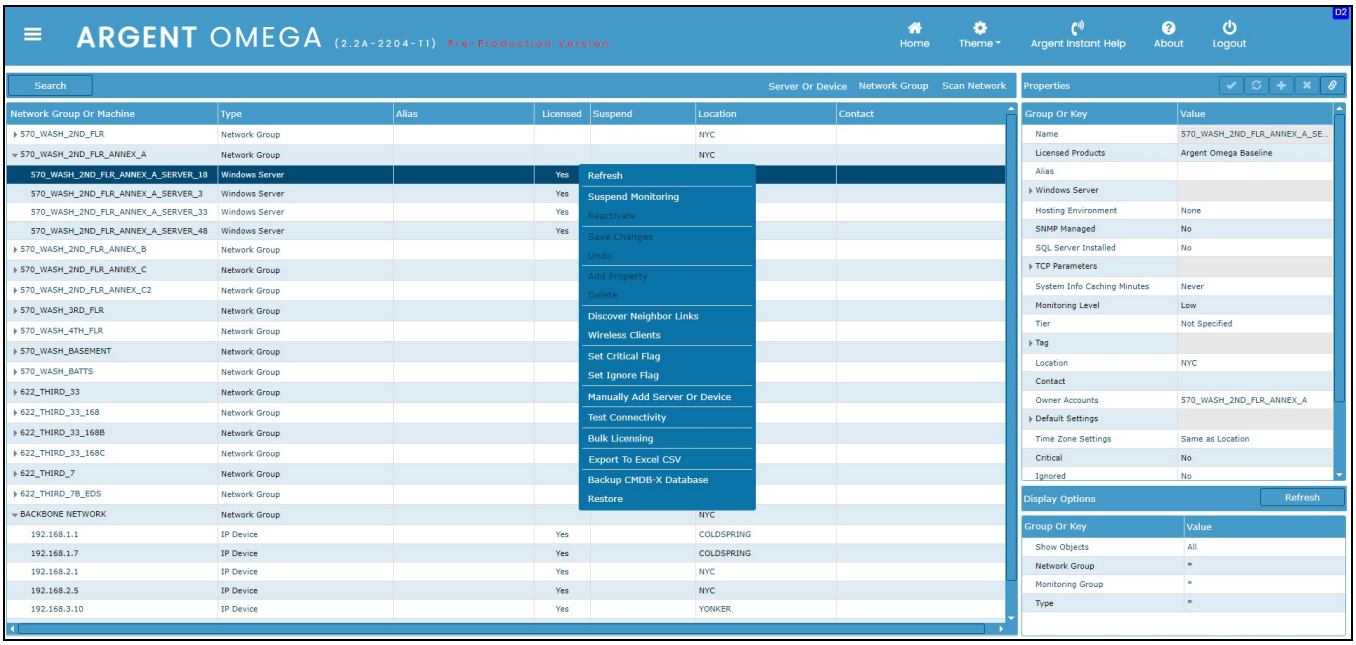


Proprietary Information – All Rights Reserved

The Argent Omega CMDB-X offers Network Group facility to group servers and devices. The Network Group popup menu provides the options to add, delete, or rename Network Groups.



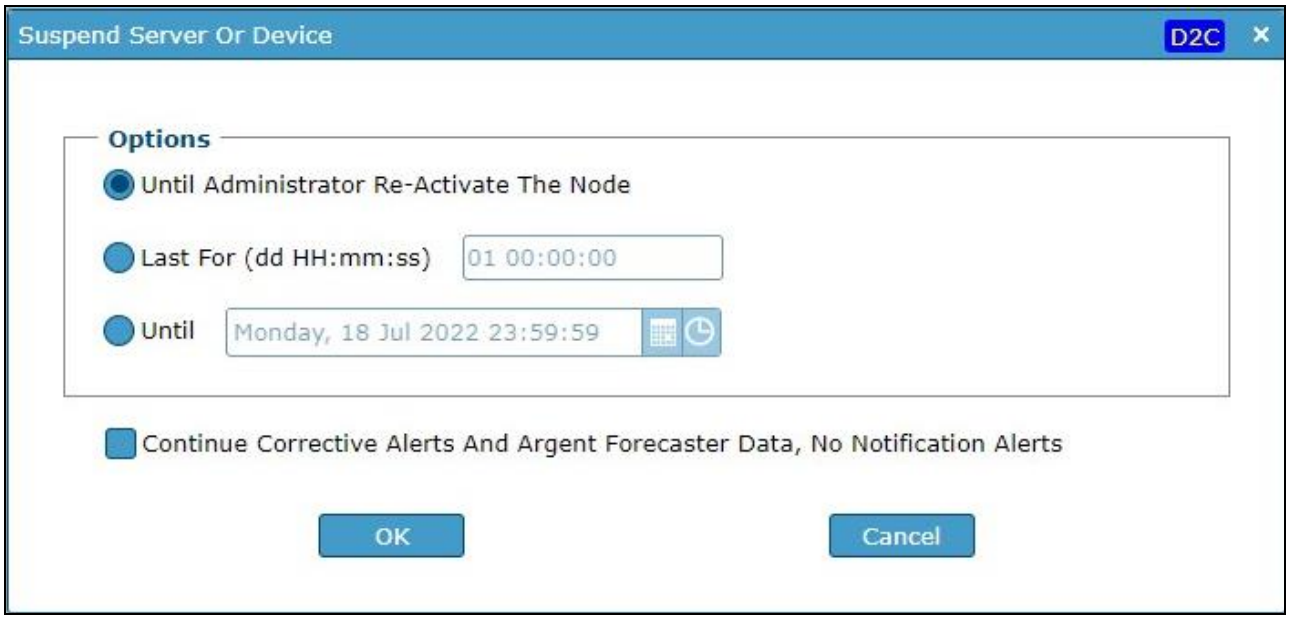
The context menu options available for various functionalities:



The **Suspend Monitoring** option suspends the selected servers from monitoring. This will skip the normal execution of Relators for the suspended servers or devices. For example, if you have maintenance on specific servers or devices, you can configure Argent Omega to stop monitoring those servers or devices during specific time period or until they are manually re-activated by the Administrator.

Proprietary Information – All Rights Reserved

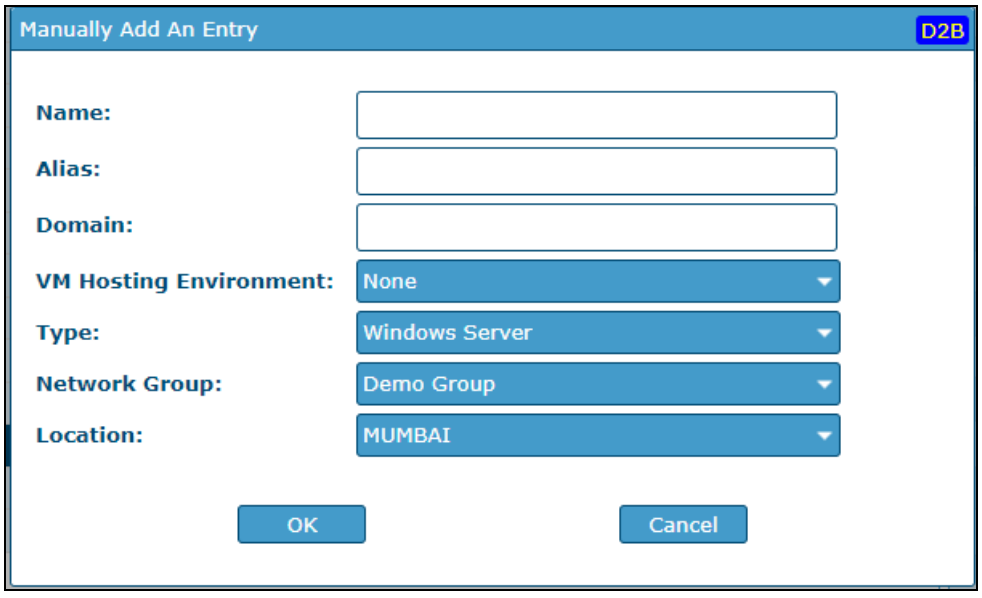
A configuration dialog will pop up when clicking this option and you can select the suspension options:



Reactivate option re-activates the suspended devices.

The **Manually Add Server Or Device** option allows you to manually add a server or device into CMDB-X.

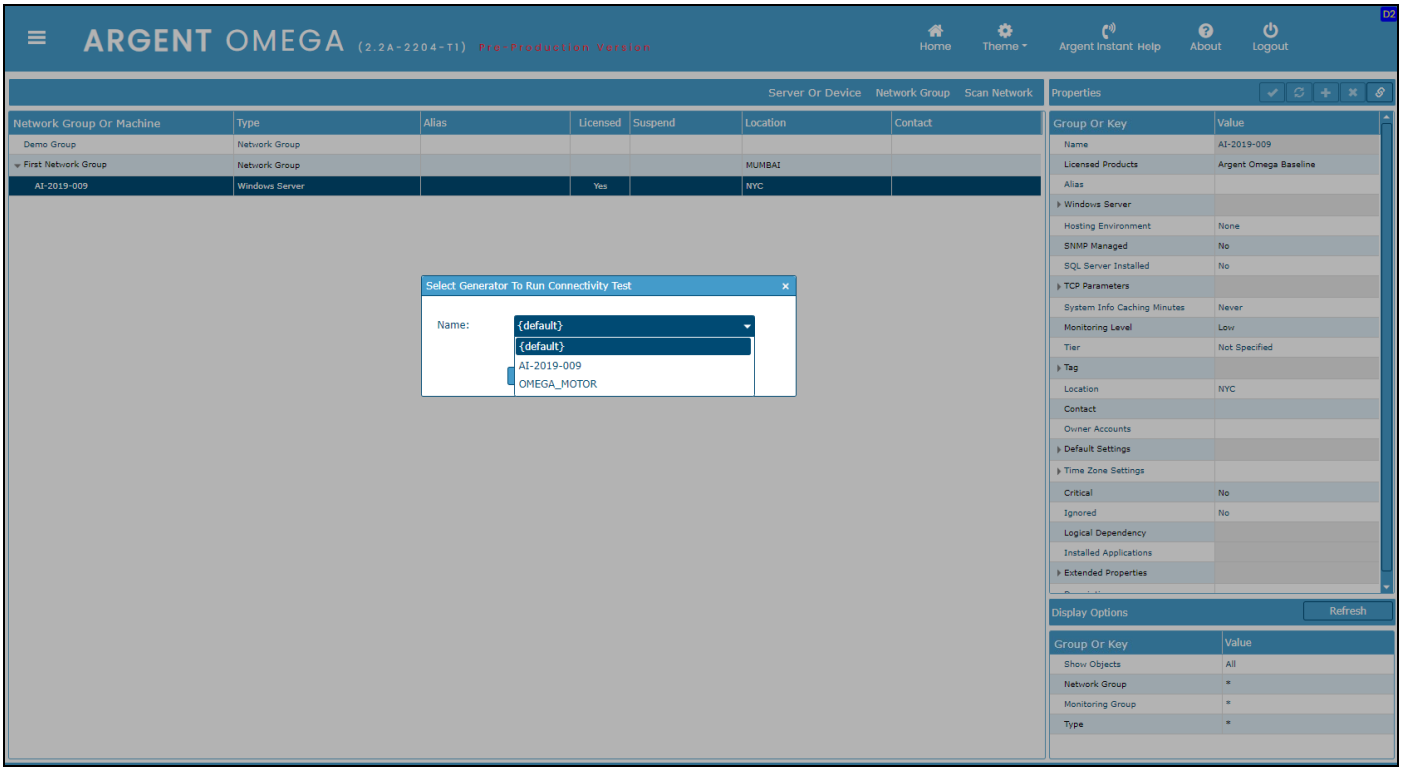
A configuration dialog will pop up when clicking this option, asking the Name, Type, Domain, Network Group, Location, etc.



Proprietary Information – All Rights Reserved

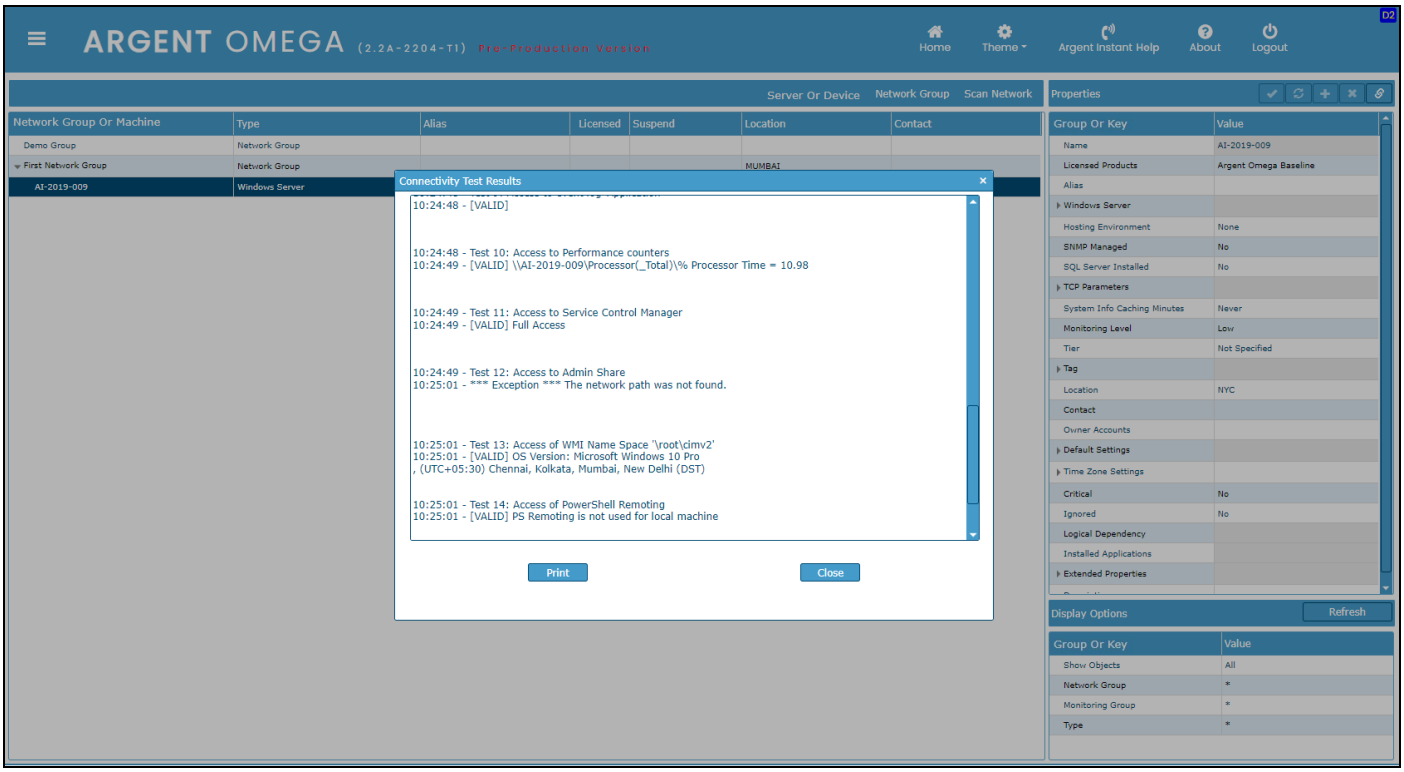
Test Connectivity option checks connectivity to the selected server or device.

This option uses the selected server or device's CMDB-X properties configured in the right pane for connectivity testing. When clicking **Test Connectivity** context menu option, a Generator selection dialog will pop up asking to select the Generator to run the connectivity test.



Leave it as "{default}" if you want to use the current Primary Generator to run the connectivity test. Click OK to run the connectivity test. The test results will be displayed in a pop up window, as shown below:

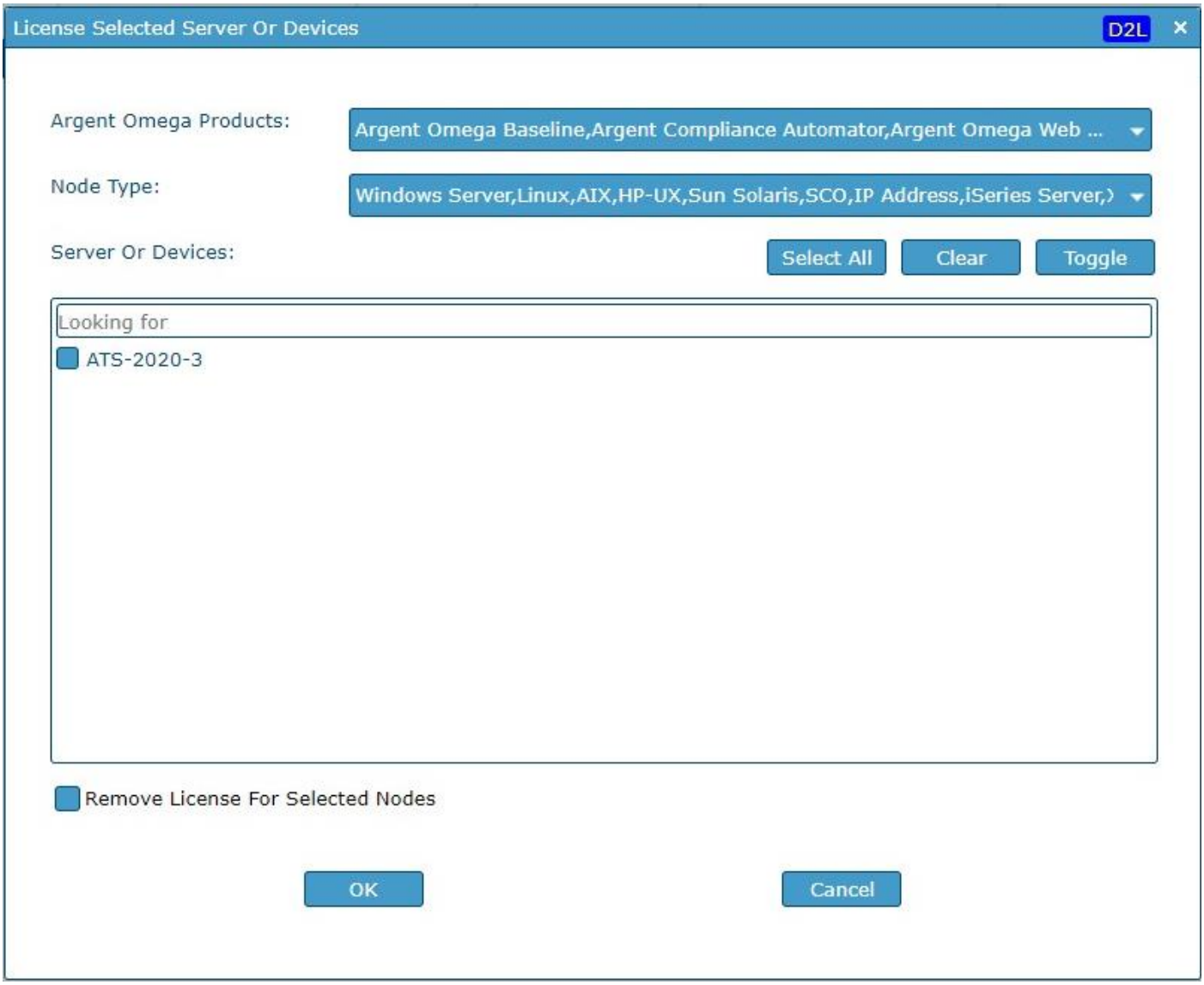
Proprietary Information – All Rights Reserved



This option uses the selected server or device's CMDB-X properties configured in the right pane for connectivity testing. A Generator selection dialog will pop up when clicking this option, asking to select the Generator to run the connectivity test.

Proprietary Information – All Rights Reserved

Bulk Licensing option is to license a group of servers in the CMDB-X. A configuration dialog will pop up when clicking this option, asking to select the servers to license, products to be licensed for selected servers, etc.



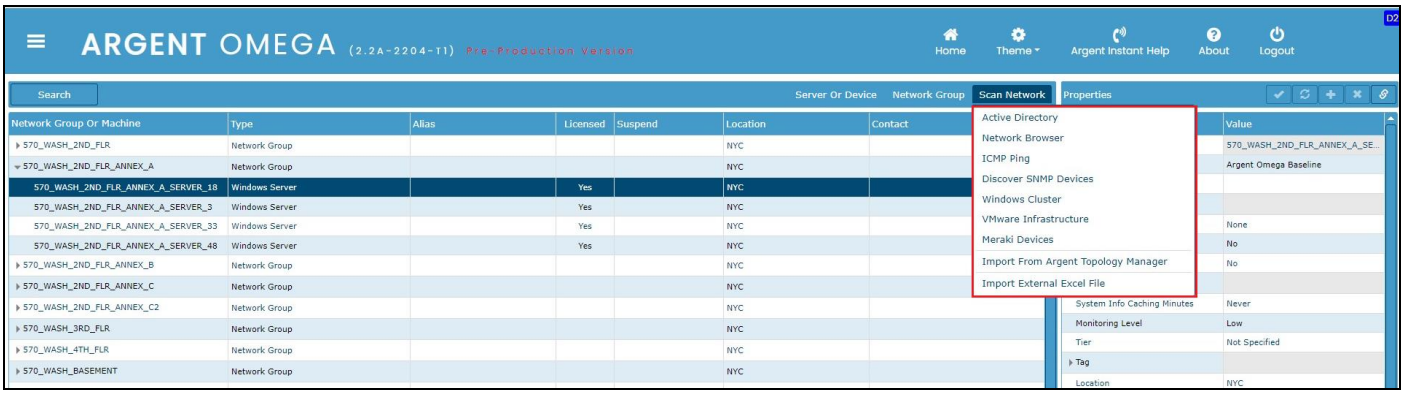
Export to Excel CSV option exports all servers and devices in CMDB-X to a CSV file.

Backup CMDB-X Database option backs up CMDB-X to a file that you can restore later.

Restore option restores CMDB-X from a backup file.

The Scan Network popup menu option offers the following network scanning mechanisms:

Proprietary Information – All Rights Reserved



Active Directory

Argent Omega polls the Active Directory to provide a list of all registered devices.

Network Browser

The network browser uses the Computer Browser service to perform network discovery.

ICMP Ping

This method does an IP scan across an entire IP range, and comes back with a list of IP addresses that responded to it.

Windows Cluster

This method finds all machines in a named cluster.

Discover SNMP Devices

This method walks through your entire network, looking for SNMP devices that respond to a specific Query OID.

VMware Infrastructure

This method finds all machines in specified VMware Infrastructure.

Meraki Device

This method finds all Cisco Meraki devices in the network. Meraki API needs to be configured in Argent Omega configuration screen in Administration section.

Proprietary Information – All Rights Reserved

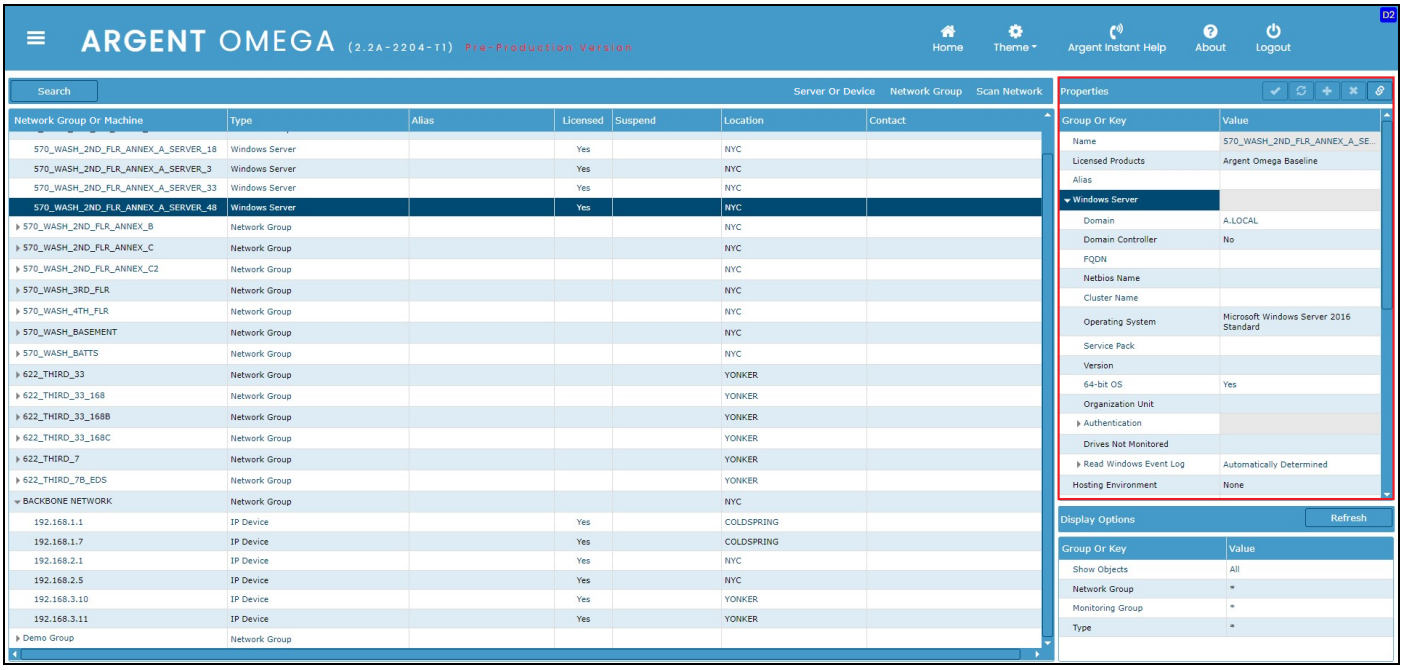
Import From Argent Topology Manager

This method retrieves the SNMP devices detected by Argent Topology Manager.

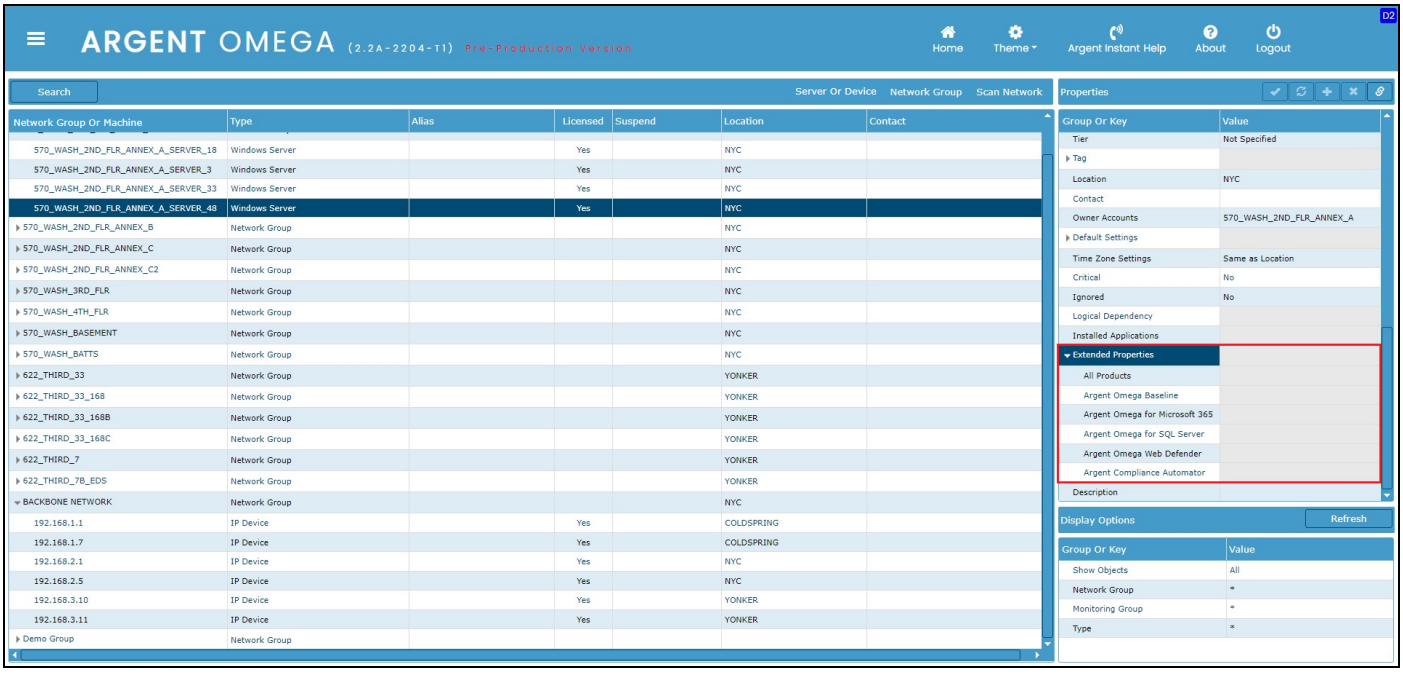
Import From External Excel File

This method imports devices from an Excel or CSV file.

After adding devices manually or via the scan, you can specify the device properties in the **Properties** section in the right pane. Common properties can be configured by selecting multiple servers and devices from the list.



Custom properties can be defined in the **Extended Properties** section in the Properties window.



Proprietary Information – All Rights Reserved

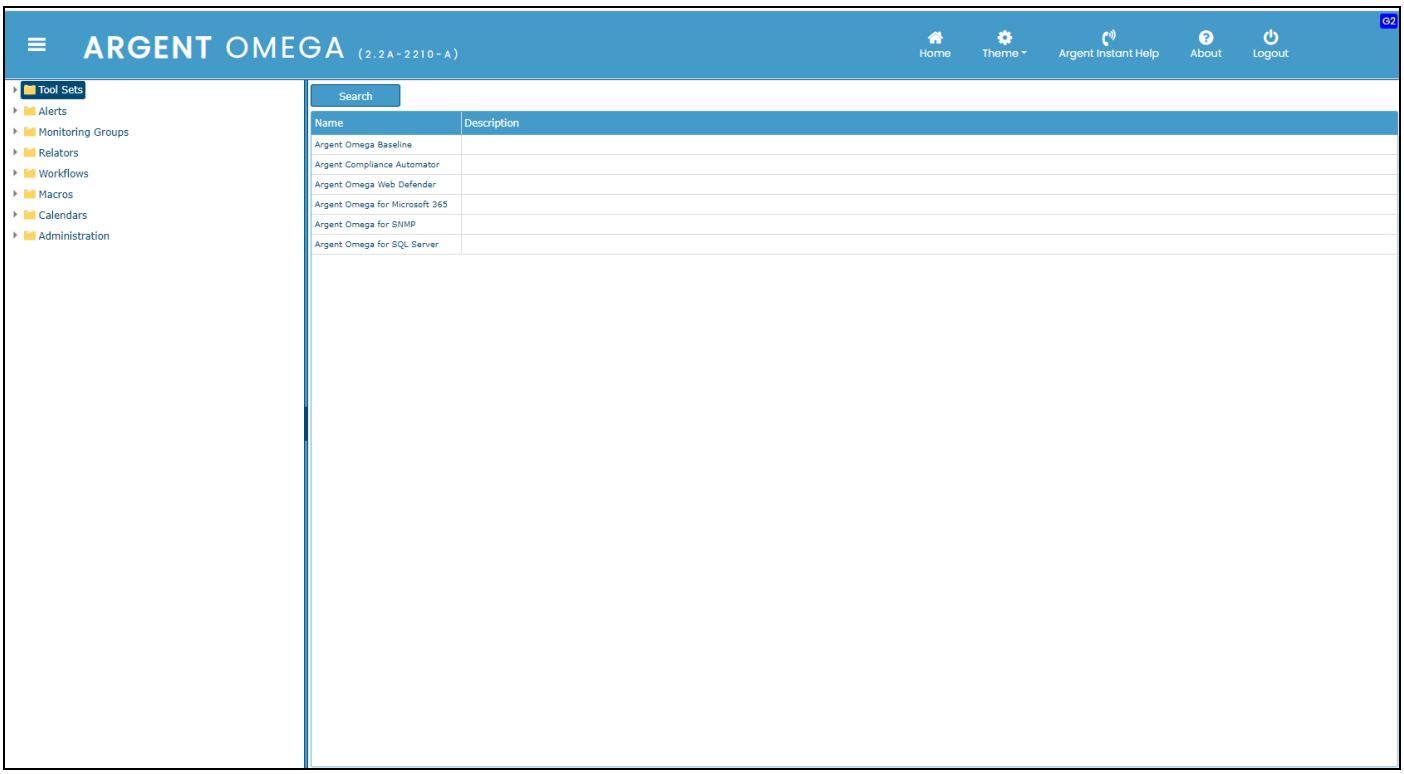
Argent Omega Four Building Blocks

In Argent Omega, all monitoring products are engineered around five building blocks, namely:

- Tool Sets
- Alerts
- Monitoring Groups
- Relators
- Workflows

In addition, there are:

- Macros
- Calendars



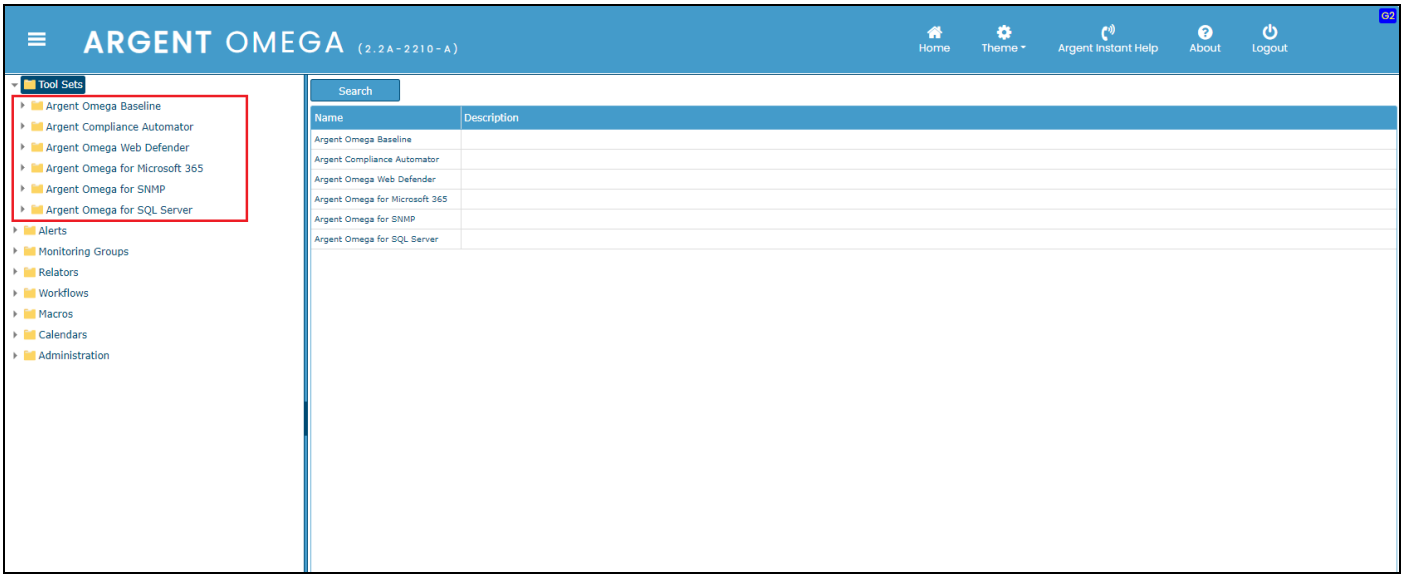
Proprietary Information – All Rights Reserved

Tool Sets – Set Of Pre-defined Rules For A Product

Each Tool Set in Argent Omega contains a set of Rules to monitor specific servers or devices.

Currently, Argent Omega provides Tool Sets for the following:

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



Rules are tests for conditions.

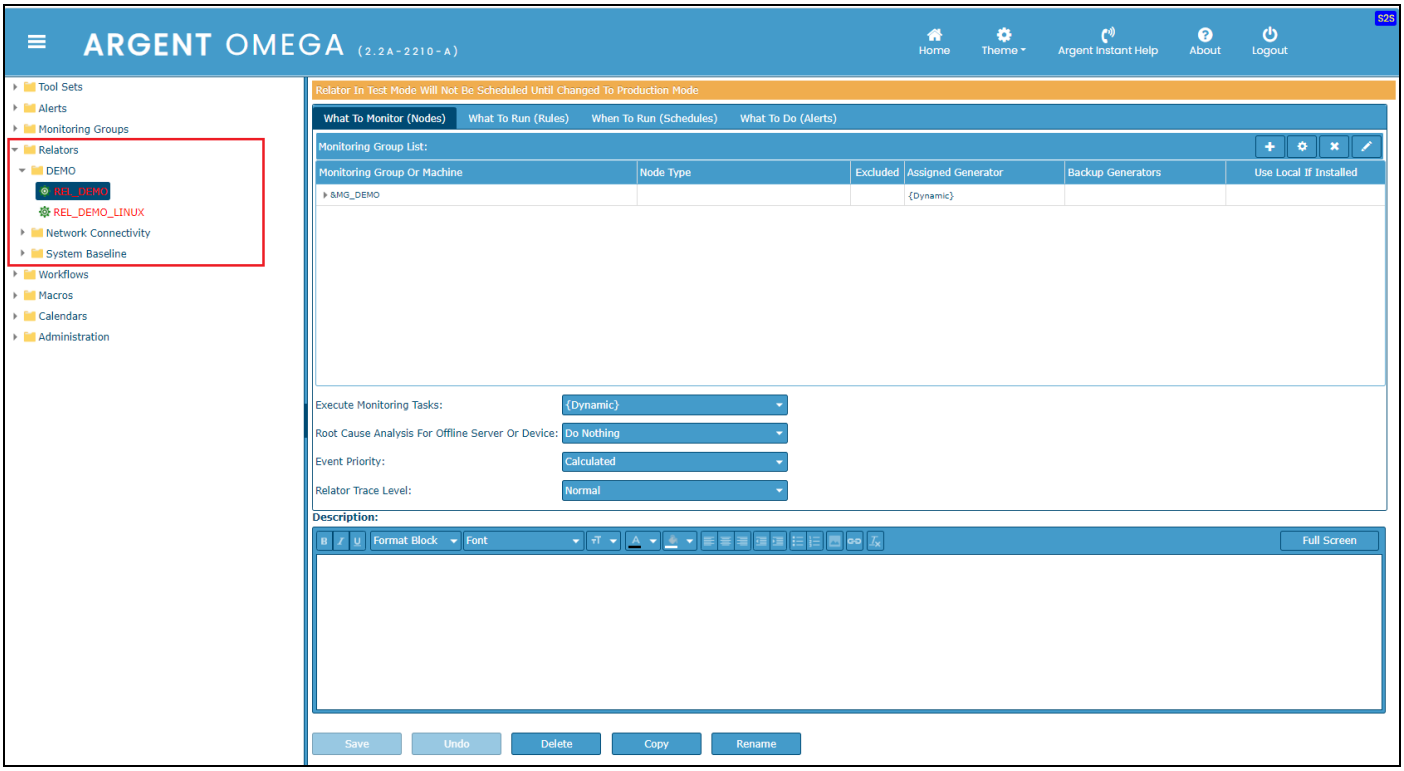
A Rule is broken if the threshold is exceeded. Notification Alerts simply provide different avenues if the specified condition is not satisfied. The Rules are an accumulated base of knowledge from thousands of Customers worldwide. Whenever new Rules are created by Argent for a single customer, these Rules are added to the next release of the product to enable all Argent customers to share in the expanded base of knowledge.

These pre-defined Rules monitor almost all of what customers need to monitor. We can add an unlimited number of new Rules and can copy and edit the pre-defined Rules because Rules **do not specify** the server or device in the actual Rule; you can use the same Rule to monitor many different servers and devices.

Proprietary Information – All Rights Reserved

Relators

Relators tie together or relate the other building blocks, namely **Rules, Alerts,** and **Monitoring Groups**. In a Relator, the Rule to be executed against the servers and devices in the Monitoring Groups is specified. In addition, the Relator specifies the **Alerts** that will be fired when an issue is detected.

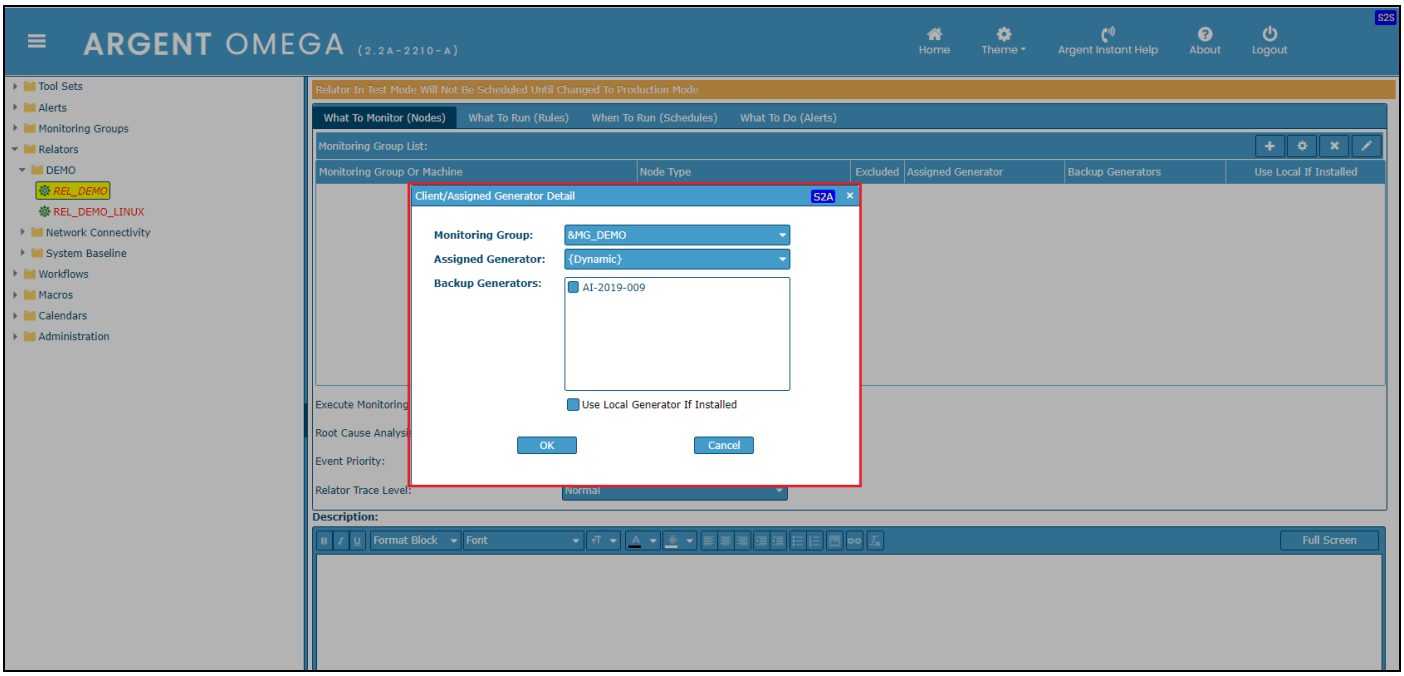


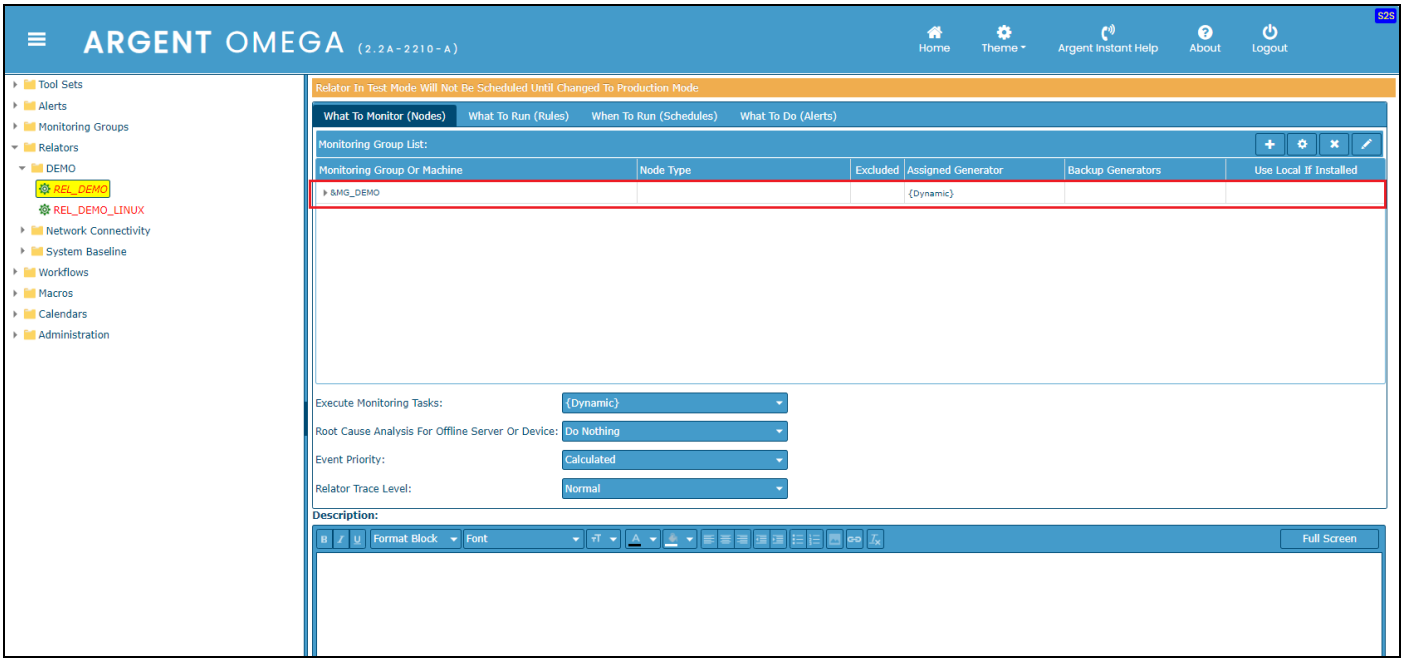
The **benefit** of a Relator is Rules, Alerts, and Monitoring Groups are all shared. Each Relator has its own monitoring rate -- the frequency in minutes or seconds. The Relator executes to check the servers and devices in the Monitoring Group. Each server and device is checked independently of the others -- the results of checking one server or device in the Monitoring Group in no way affects the results of checking other servers or devices.

Relators can also ***optionally*** use Calendars. Calendars are used to provide maximum flexibility when scheduling events, such as Relators, Alerts, and Automatic Report Distributions. Any complex Calendar can be created easily.

Proprietary Information – All Rights Reserved

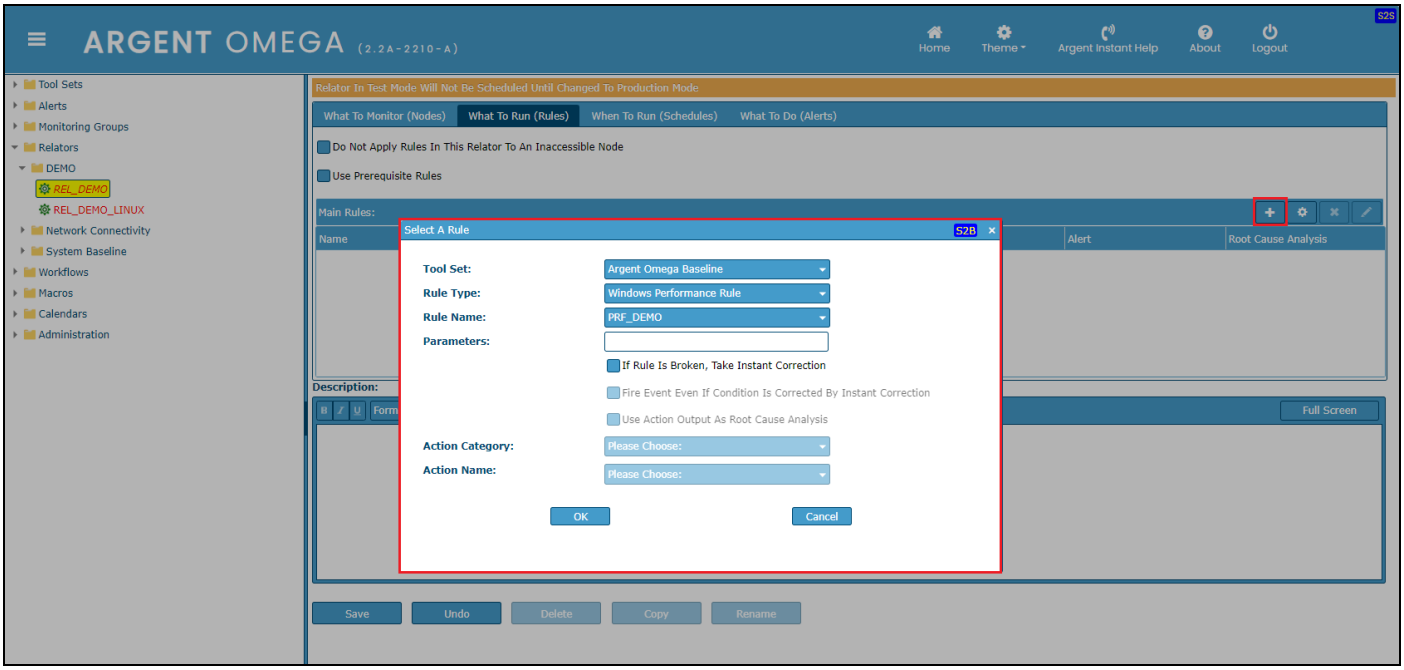
Select any Relator. Select **What To Monitor (Nodes)** tab and click "**+**" to add Monitoring Group.

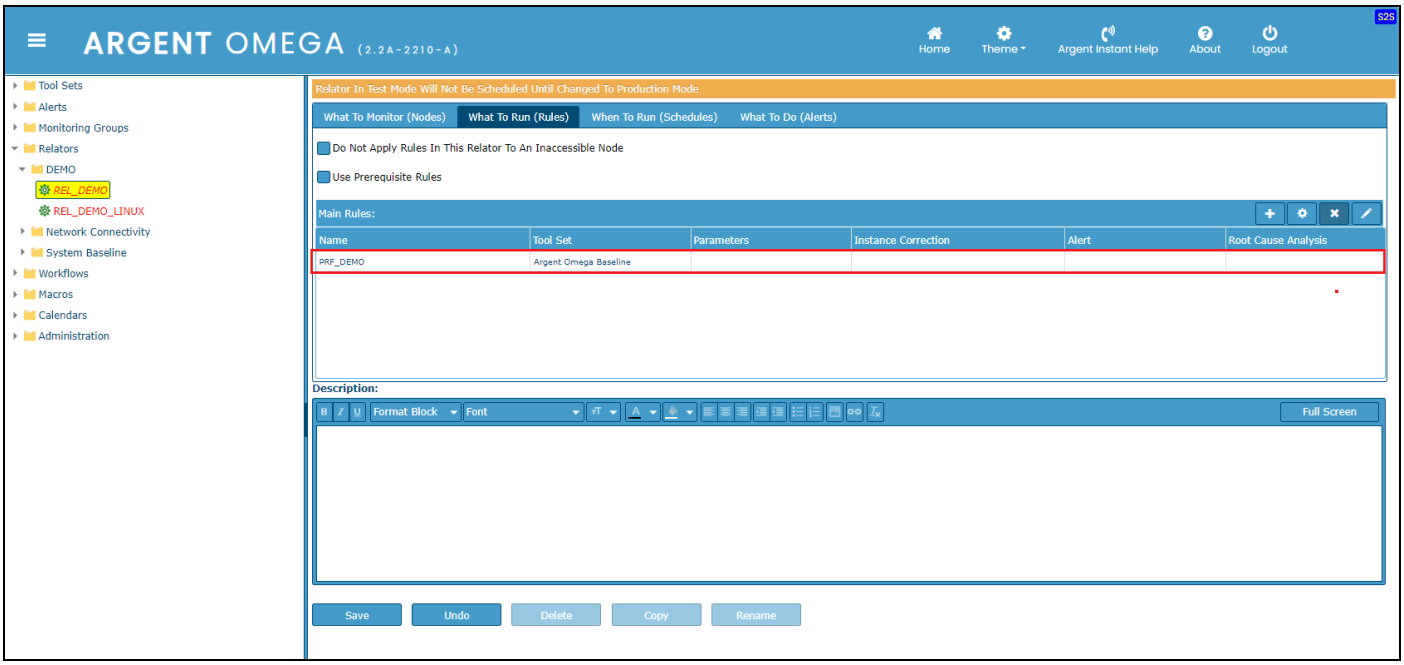




Proprietary Information – All Rights Reserved

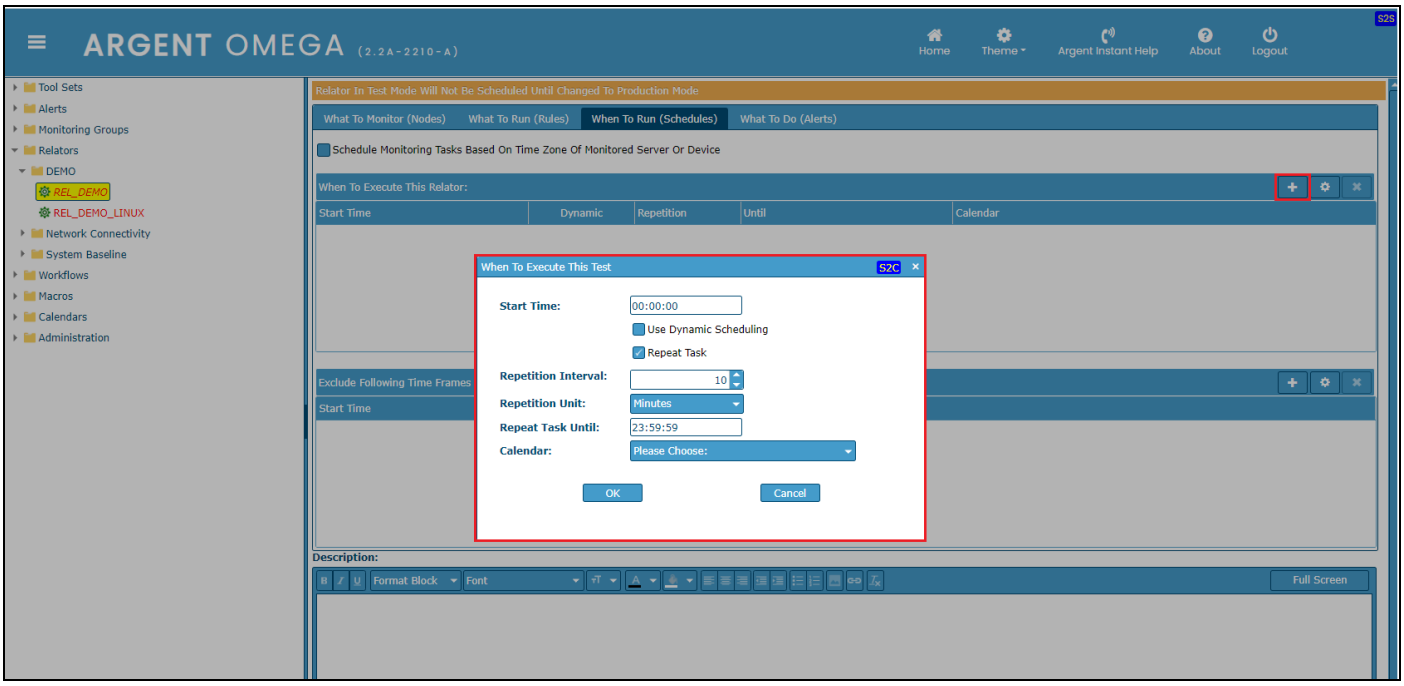
Select **What To Run (Rules)** tab and click "**+**" to add Rule.

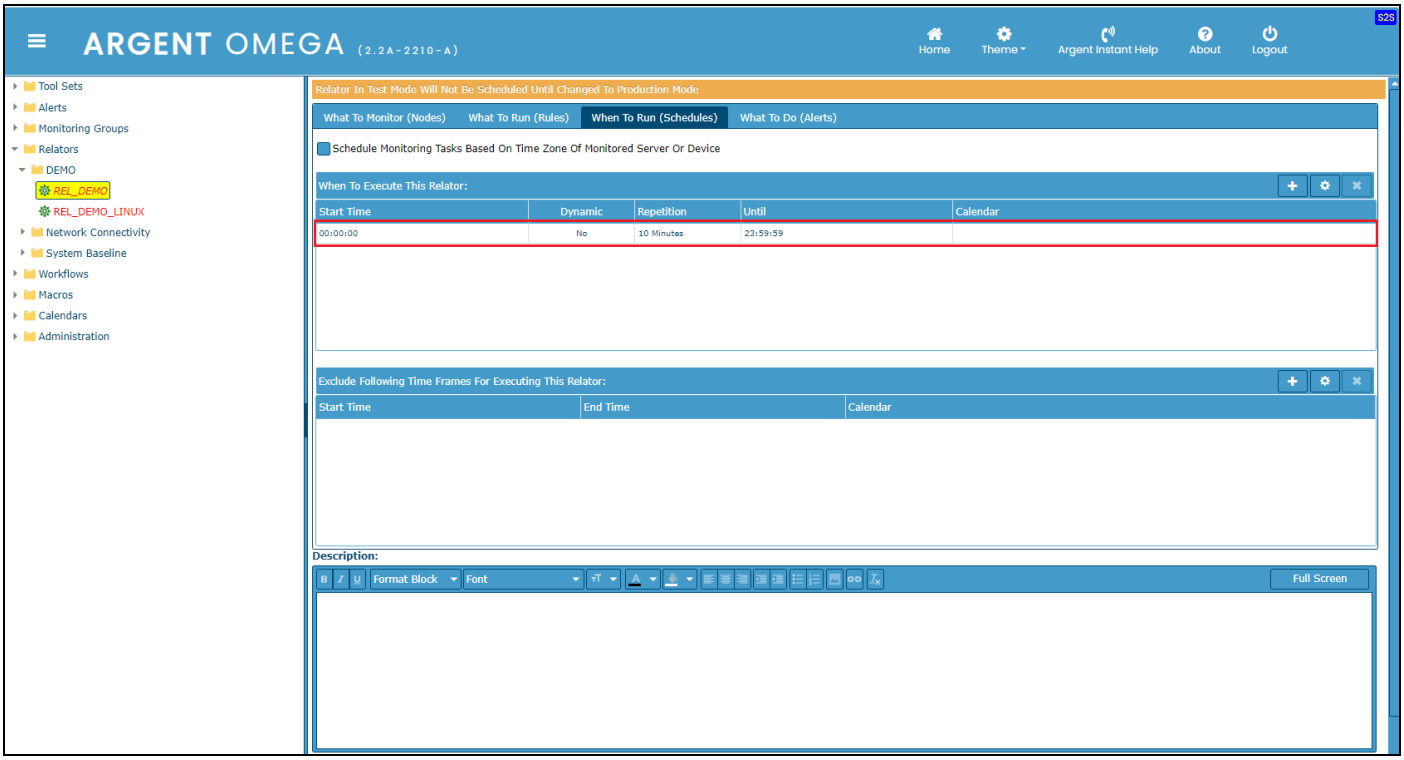




Proprietary Information – All Rights Reserved

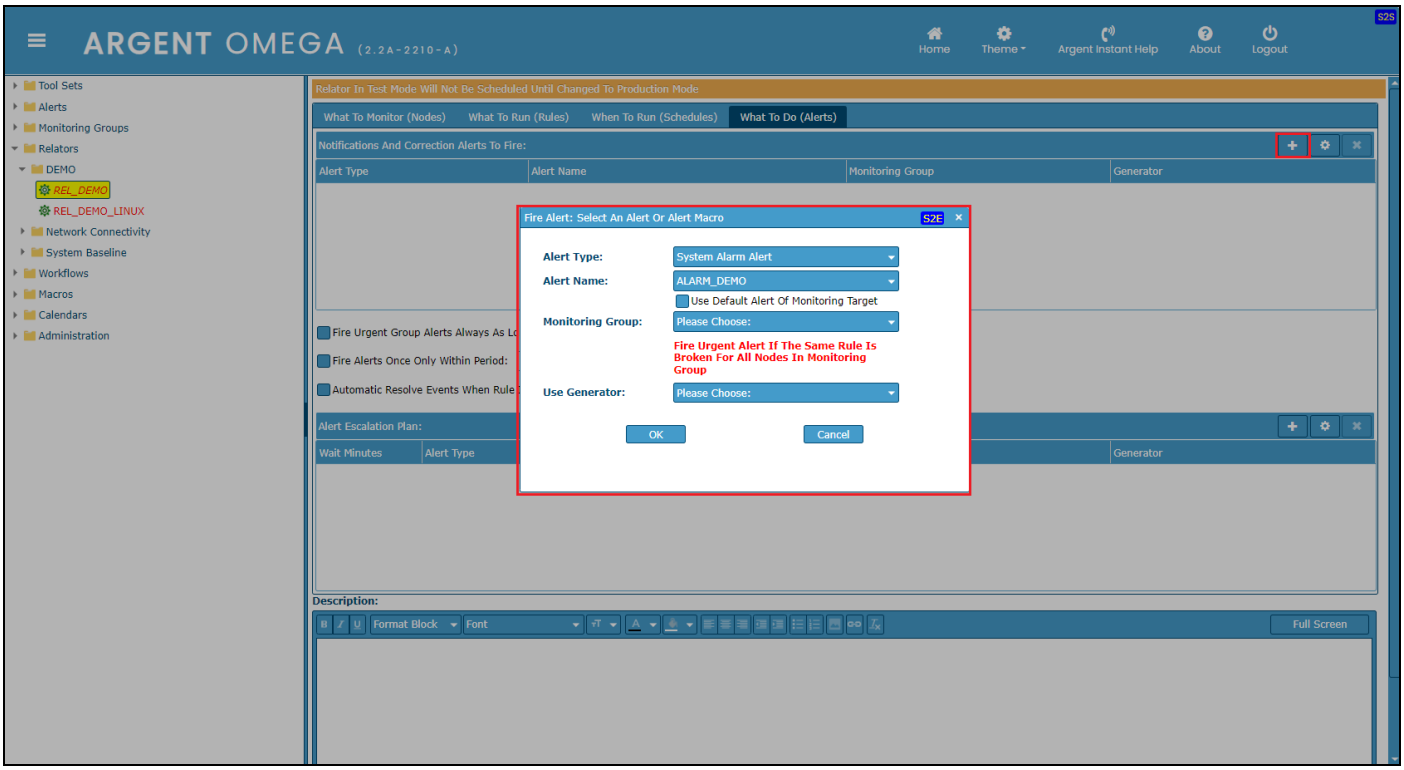
Select **When To Run (Schedules)** tab and click "**+**" to add schedule to run.

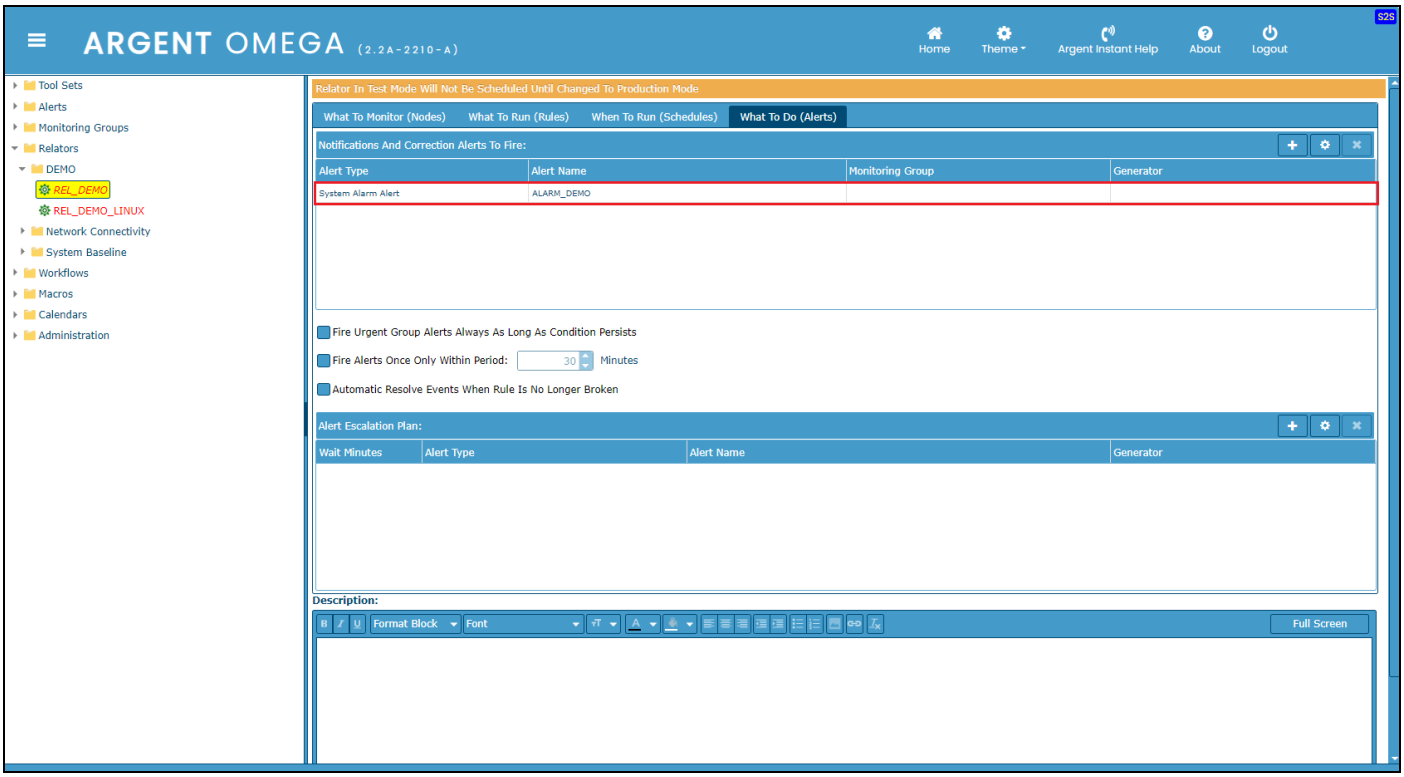




Proprietary Information – All Rights Reserved

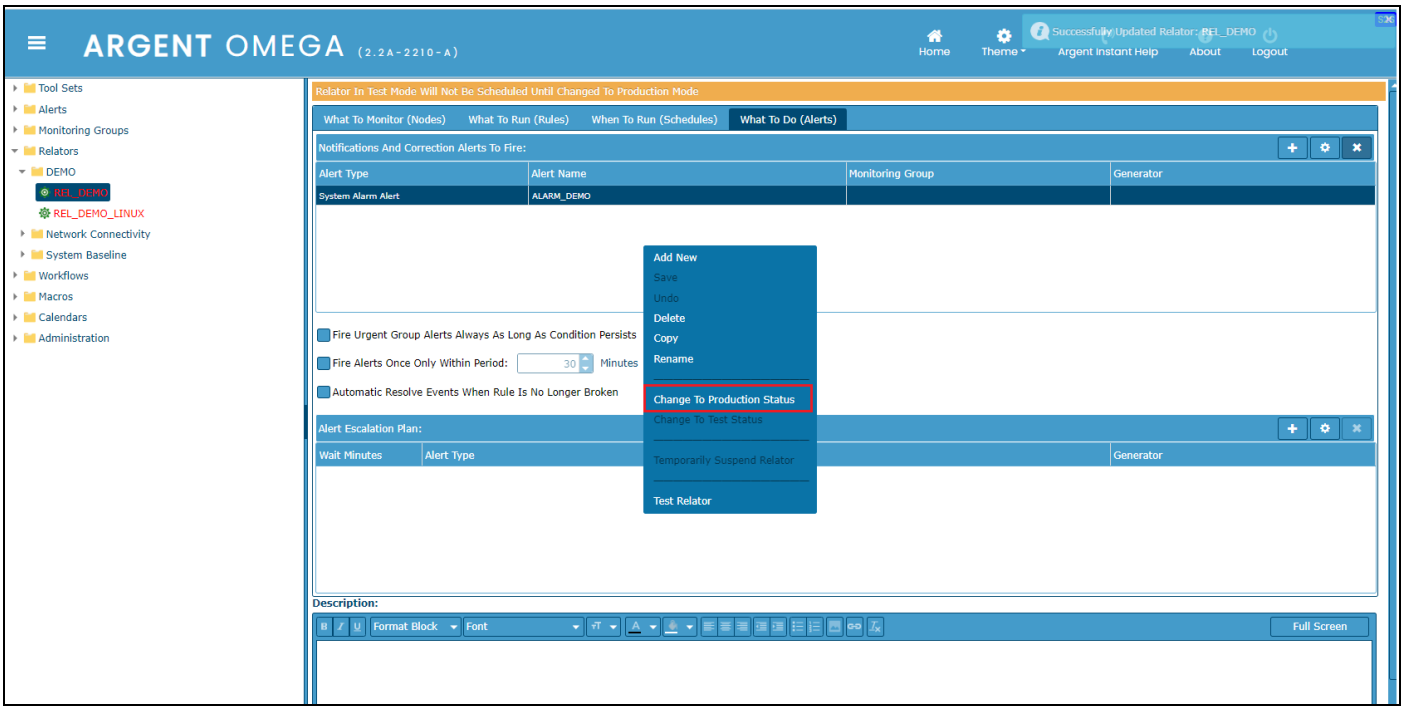
Select **What To Do (Alerts)** tab and click "**+**" to add Alert.

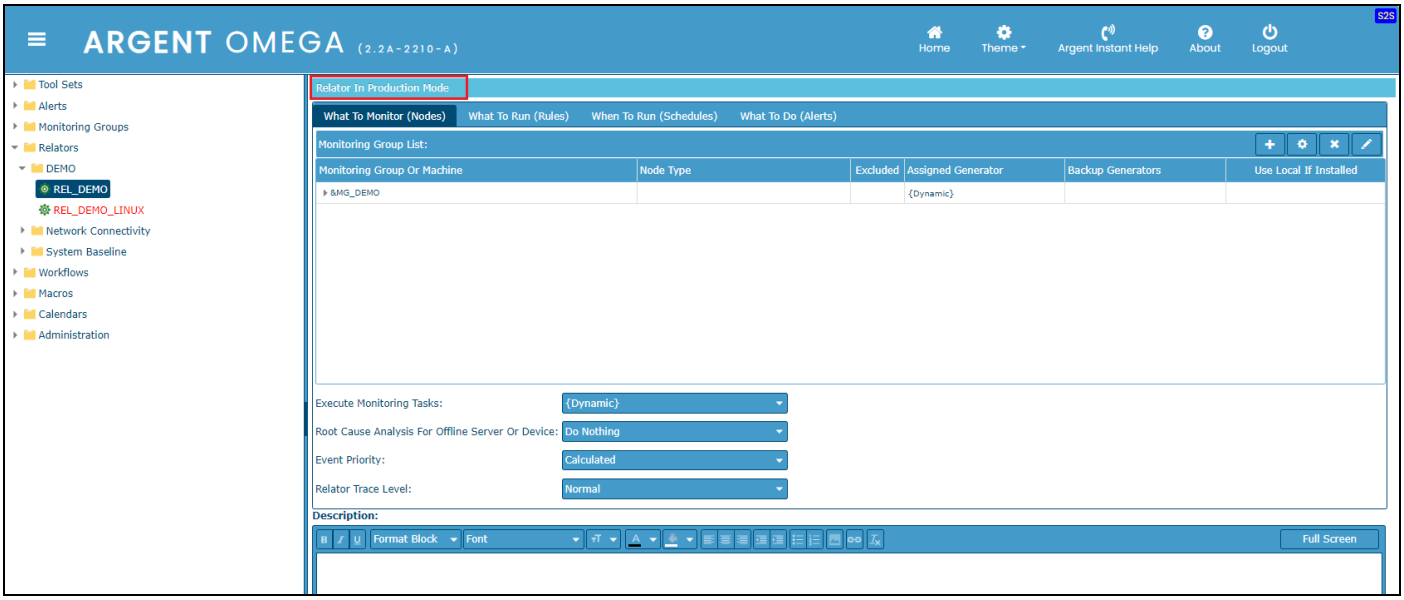




Proprietary Information – All Rights Reserved

Select **Change To Production Status** from context menu to put the Relator in Production and the Relator runs as per the Schedule.





Proprietary Information – All Rights Reserved

Workflows

Workflow is a superset of Relator. Workflow is designed to fulfill some special requirements that cannot be achieved by using Relator. Workflow has all the functionalities of Relator, and it has following additional features:

1. Facility to run Workflow tasks on multiple licensed servers. Example: Install Windows updates in licensed server.
   Each task in a Workflow is called a **Step**.
2. Some Steps execute in parallel, and some are sequential.
3. Facility to configure conditional branches in Workflow definition.
4. Facility to configure task looping and it can be controlled properly.
5. Run and control long running tasks.

The above features do not fit well into Relator model, which is simple, linear, independent, and generally for short running tasks.

Workflow = Steps + Success Alert + Failure Alert + Escalation + Schedule.

Step = Step# + Independent Licensed Server or Monitoring Group + Condition + True Operation + False Operation + Repetition + Failure Handling + Next.

Step# – Step number. Workflow executes in order of Step number.

Independent Licensed Server or Monitoring Group – Step logic is applied to the selected licensed server or all machines in selected Monitoring Group. They are executed in parallel.

Condition – It can be a Rule or built-in condition such as ‘Apply Windows Updates’ or “Create VM Snapshot”. Built-in ones will grow over time.

True-Operation – It is executed when condition is true. It can be an Action Alert or built-in operation such as ‘Apply Windows Updates’. Built-in ones will grow over time.

False-Operation – It is executed when condition is false.

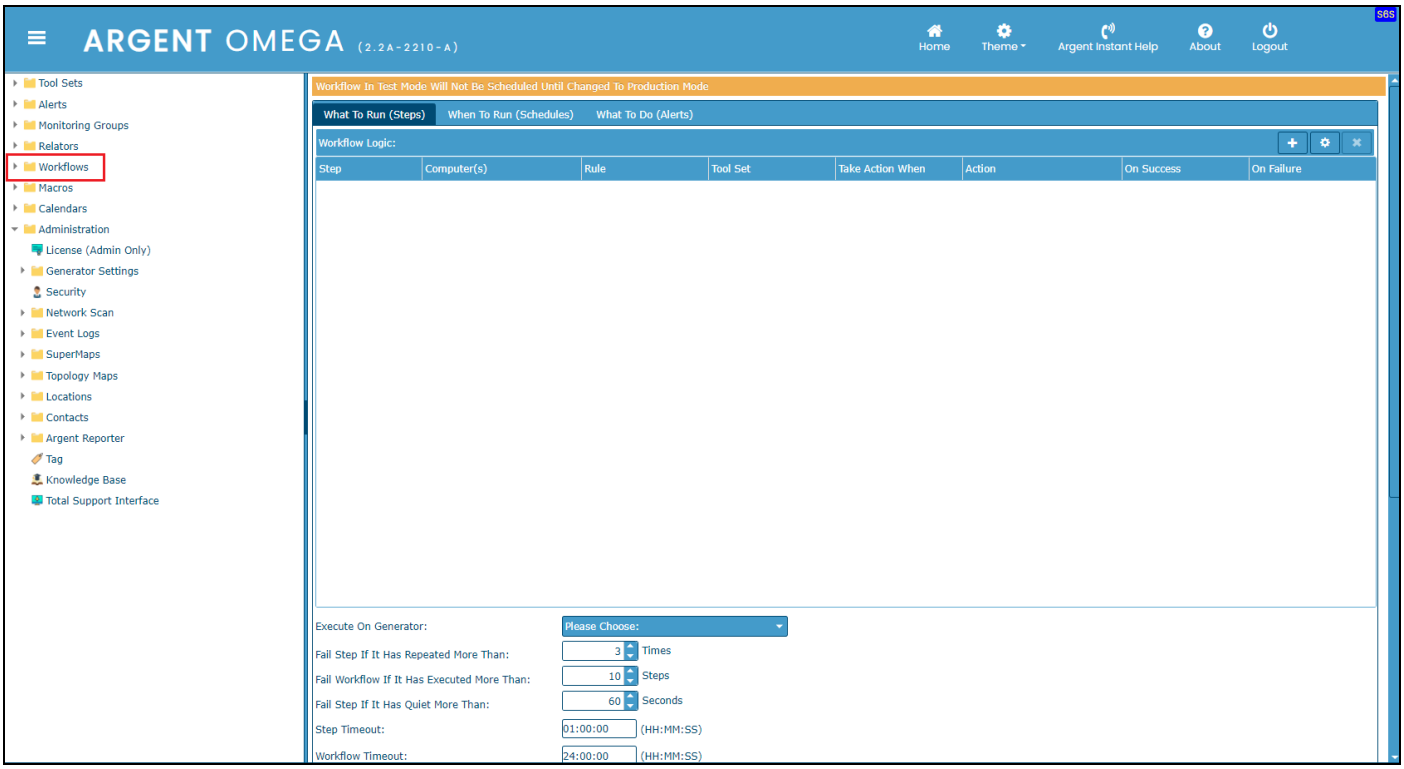
Repetition – If true, after operation is done, recheck condition, repeat until condition becomes false.

Failure Handling – It can be Ignore or Bail Out or Go to Step.

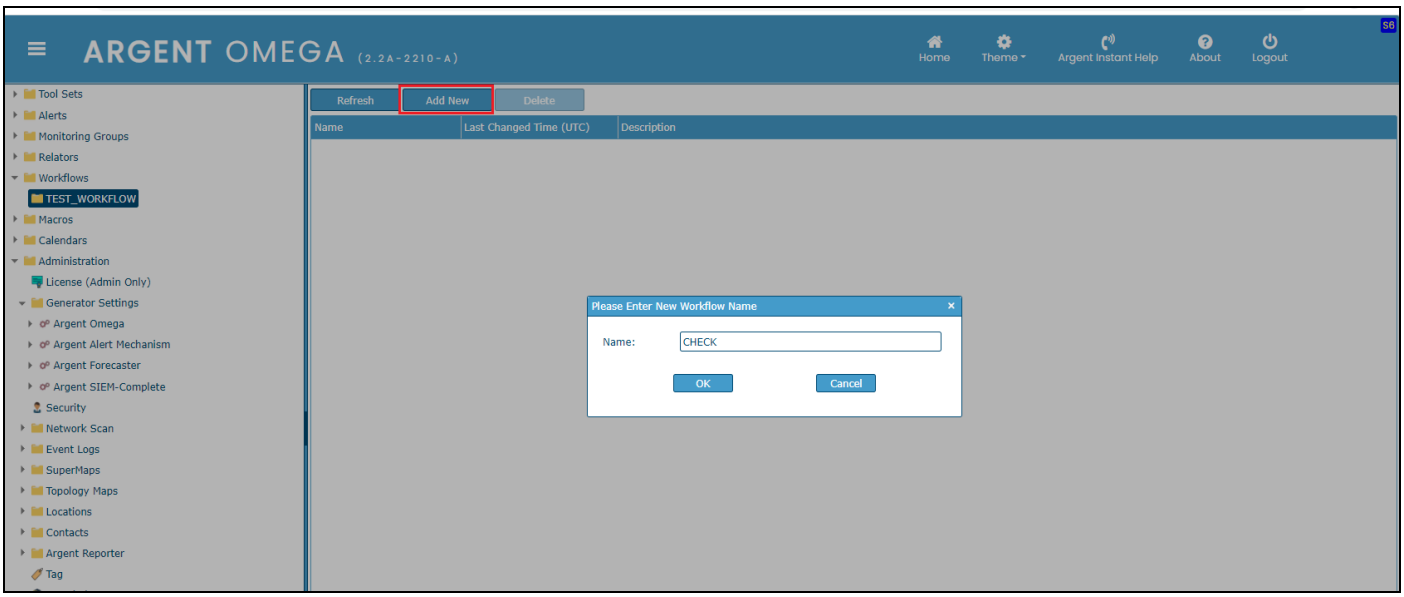
Next – It can be End Workflow or Next Step or Go To Step or Repeat Step.

Proprietary Information – All Rights Reserved

Workflow is a separate node right after Relators in **Control Information** tree as shown below:



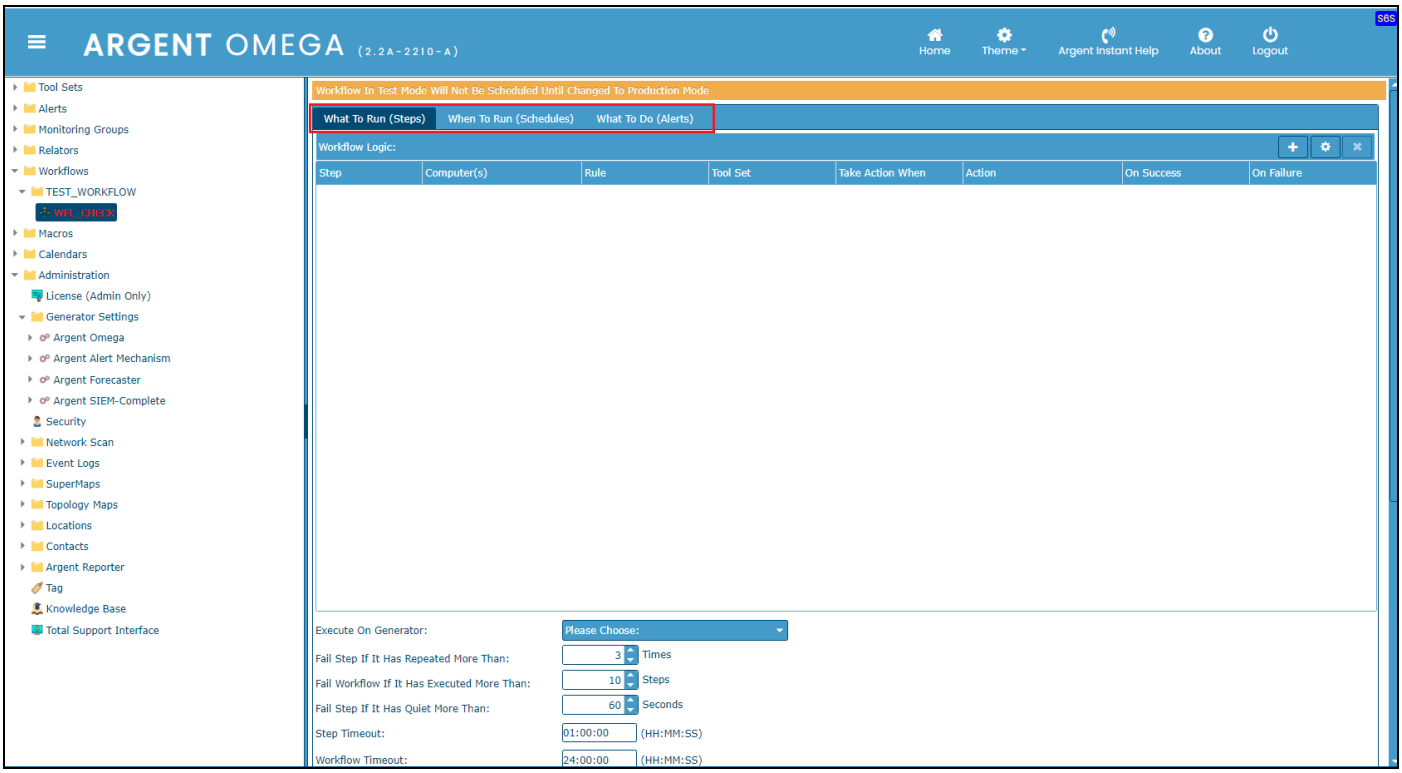
To define a new Workflow, click **Add New** and specify a name:



Need to define the following sections to complete the definition of a Workflow:

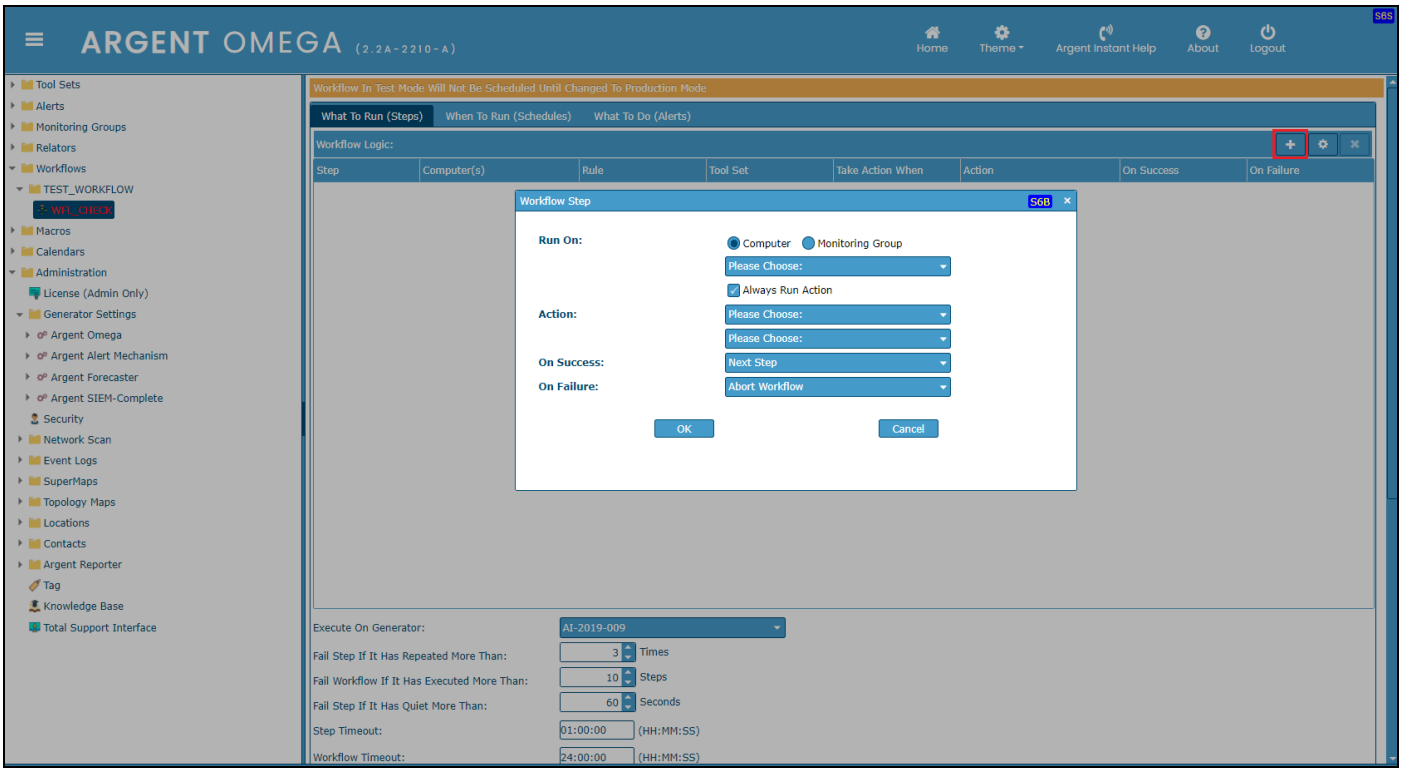
- Configure Steps in **What To Run (Steps)** tab.
- Configure execution schedules in **When To Run (Schedules)** tab.
- Configure Alerts in **What To Do (Alerts)** tab.

Proprietary Information – All Rights Reserved



A Workflow can have one or more Step definition. Each Step is identified by its unique Step number. Workflow executes in order of Step number. Steps in a Workflow are executed in sequential manner.

To define a Workflow Step, click “+” in **What To Run (Steps)** tab. Workflow definition dialog will be popped up:

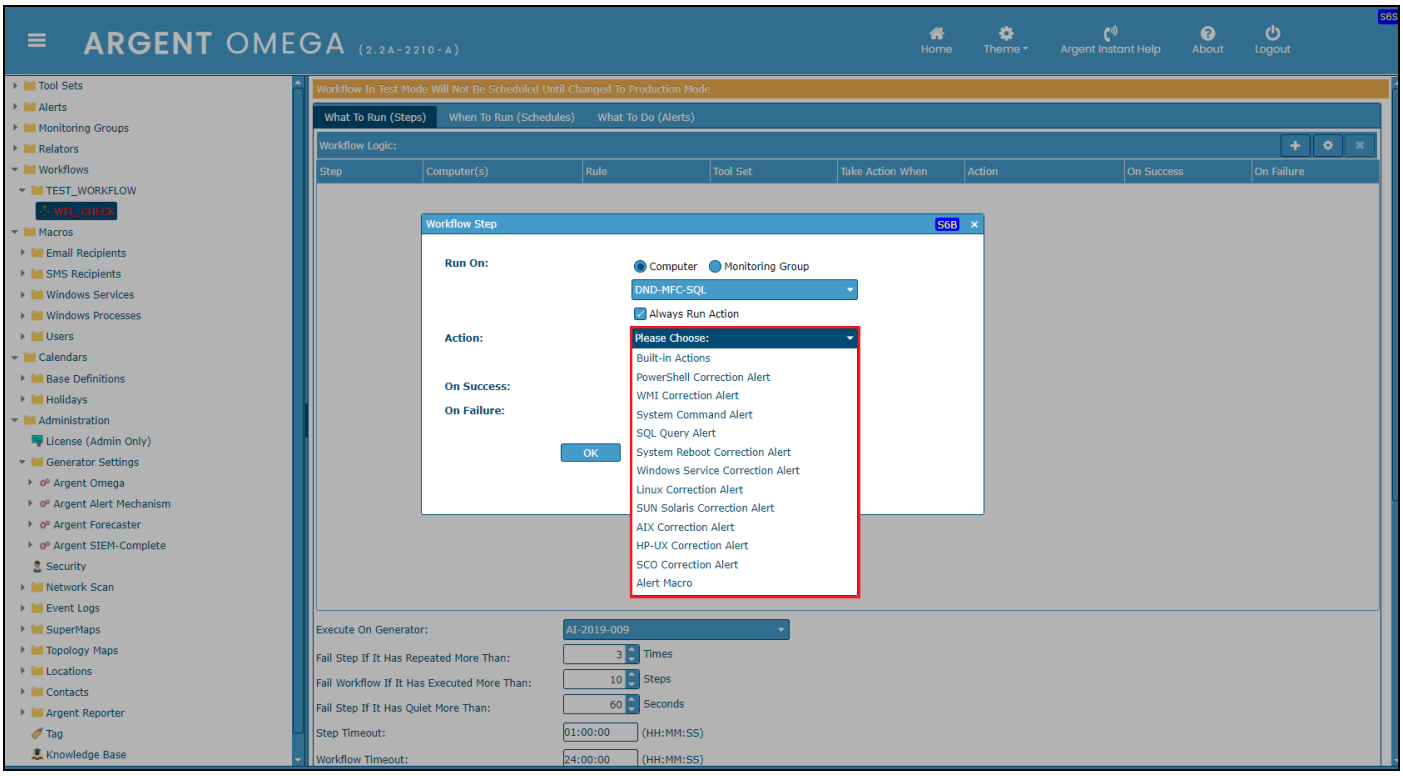


Proprietary Information – All Rights Reserved

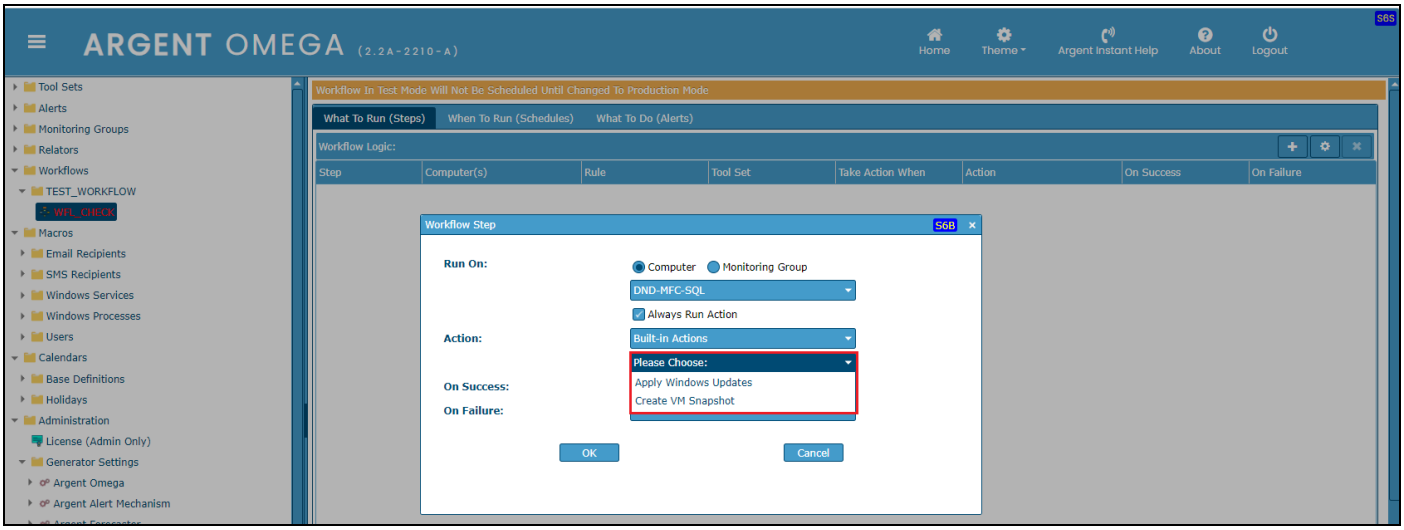
Select the Computer or Monitoring Group in **Run On** section. The Step logic will be applied to the selected Computer or all machines in the selected Monitoring Group.

Check **Always Run Action** check box to execute a built-in action or action Alert.

Select action type from **Action** combo box. Example: Built-in Actions:

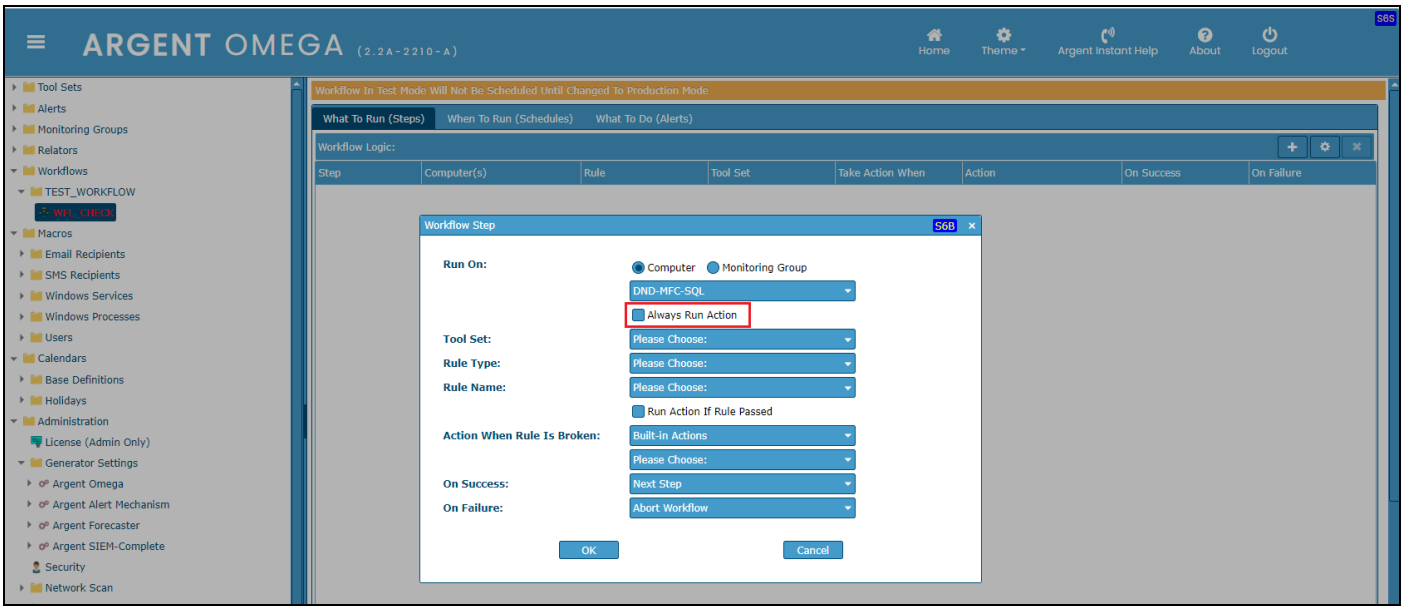


Select the Action from combo box. Example: Apply Windows Updates:

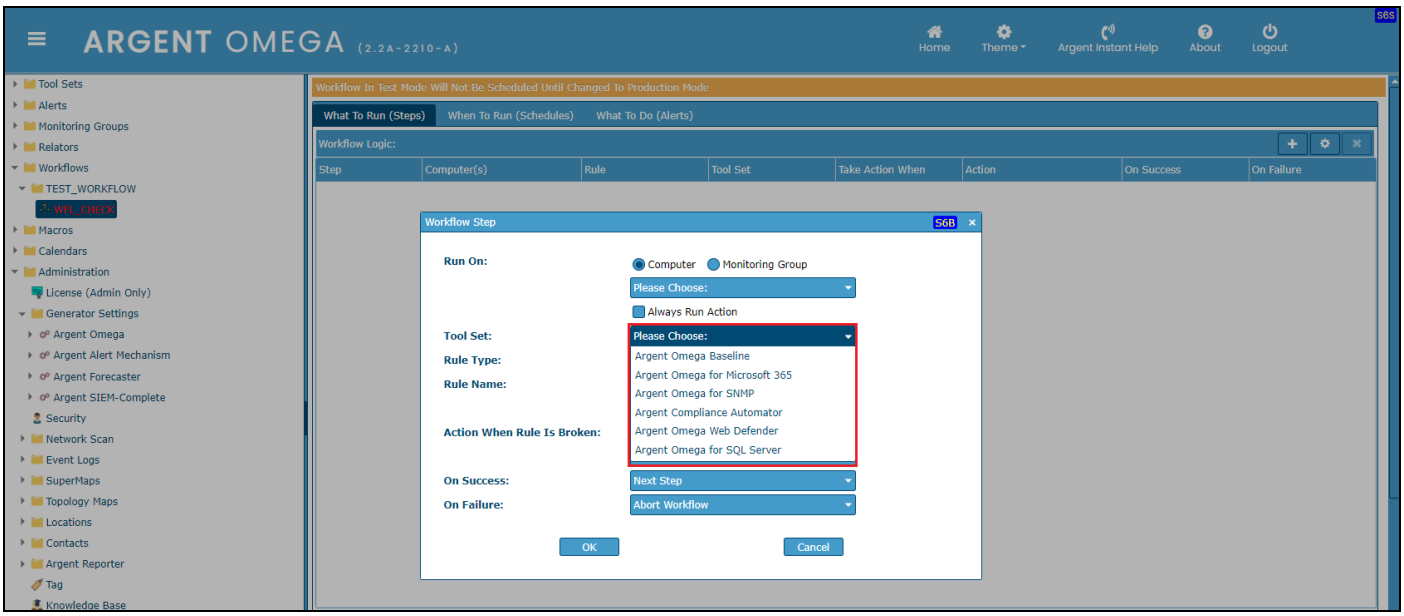


If you want to execute any Tool Set Rule instead of action, uncheck **Always Run Action** option. This will show all available Tool Sets and Rules as shown below:

Proprietary Information – All Rights Reserved



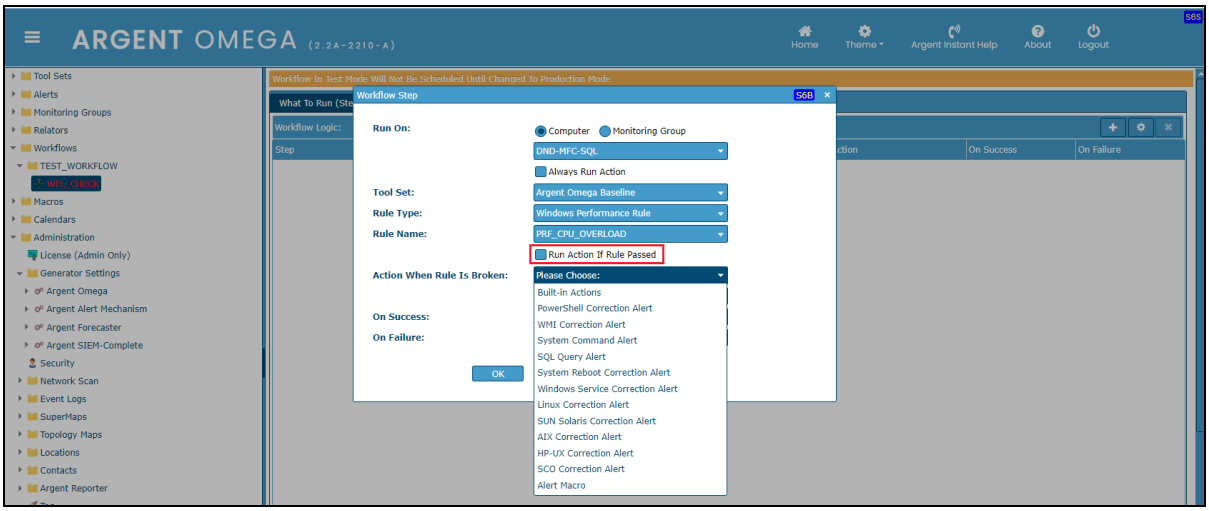
Select the **Tool Set** from combo box. It lists all available Tool Sets:



After the selection of Tool Set, all the available Rule types and Rule names will be populated in respective combo boxes. Choose the **Rule Type** and **Rule Name**.

Proprietary Information – All Rights Reserved

Choose the action required to execute from **Action When Rule Is Broken** combo box if the selected Rule is broken:

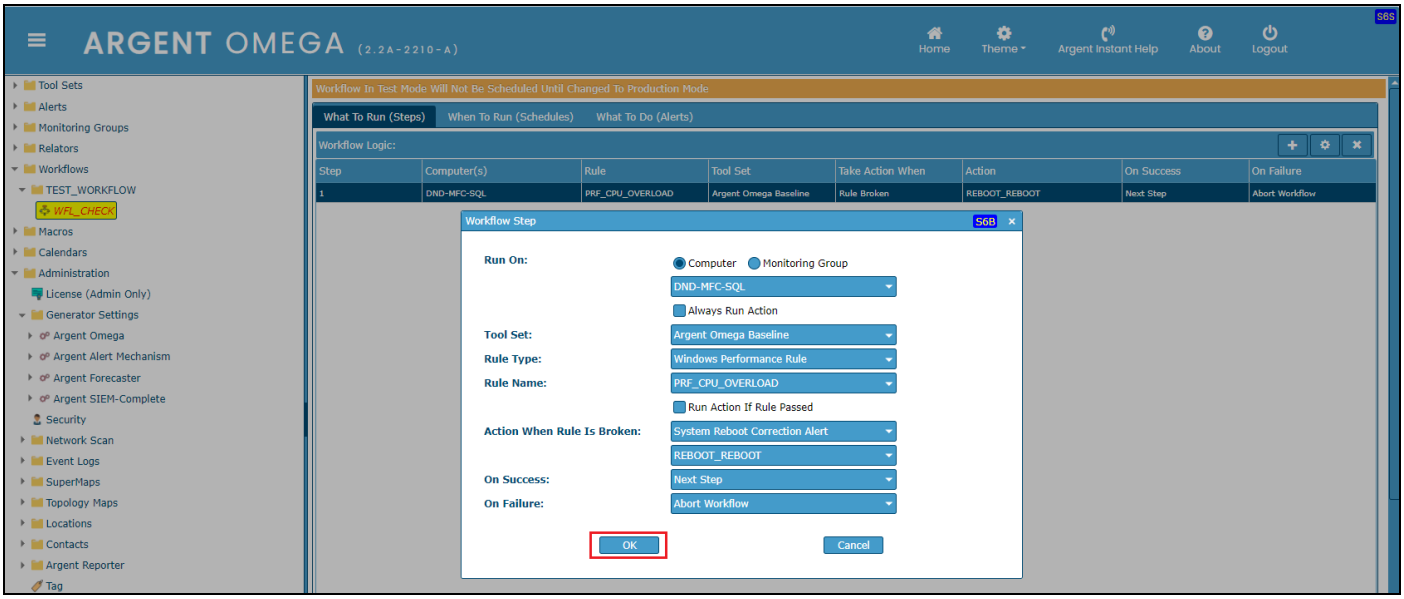


Check **Run Action If Rule Passed** option if you want to execute action if the Rule is NOT broken.

Select the action on successful Step execution from **On Success** combo box. The available actions are **Next Step**, **Go to Step**, **End Workflow** and **Repeat Step**.

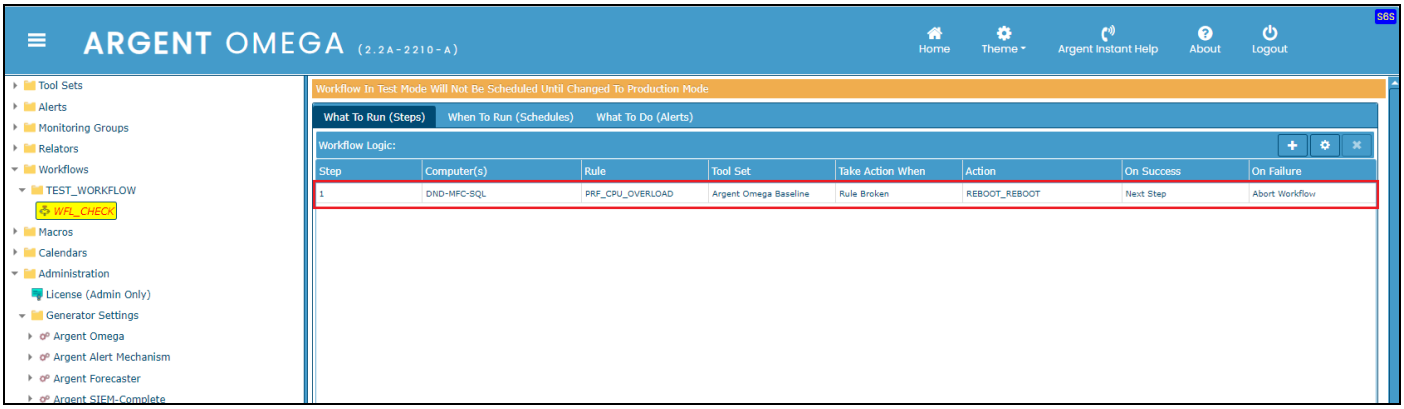
Select the action on failed Step execution from **On Failure** combo box. The available actions are **Next Step**, **Go to Step**, **End Workflow** and **Abort Workflow**.

Click OK button to complete the Step definition:



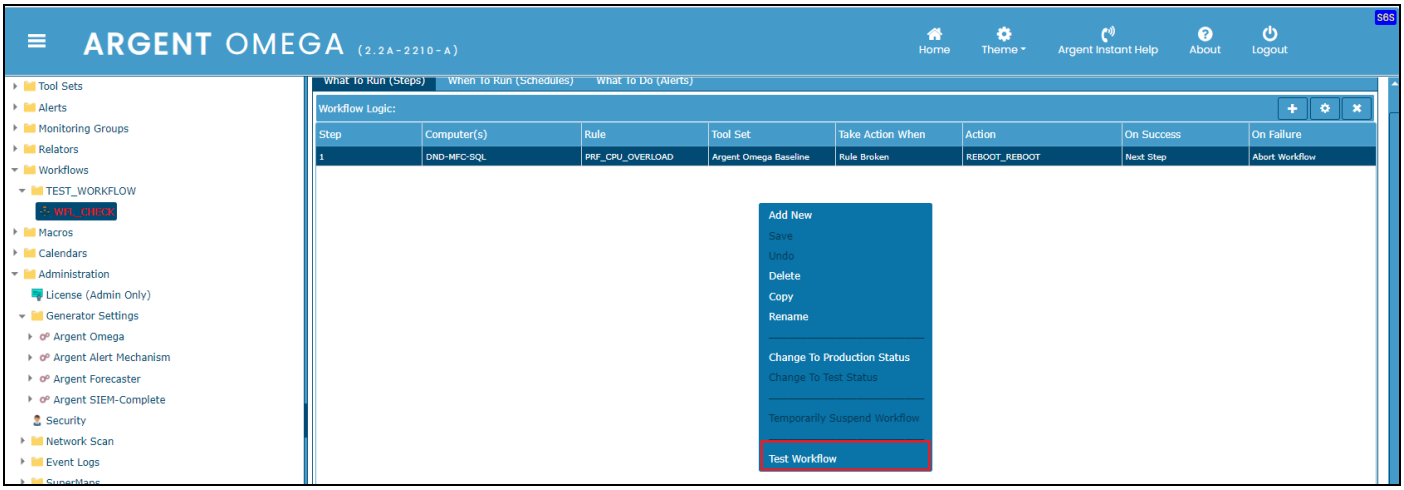
Proprietary Information – All Rights Reserved

The Step will be added to **Workflow Logic** list as shown below:

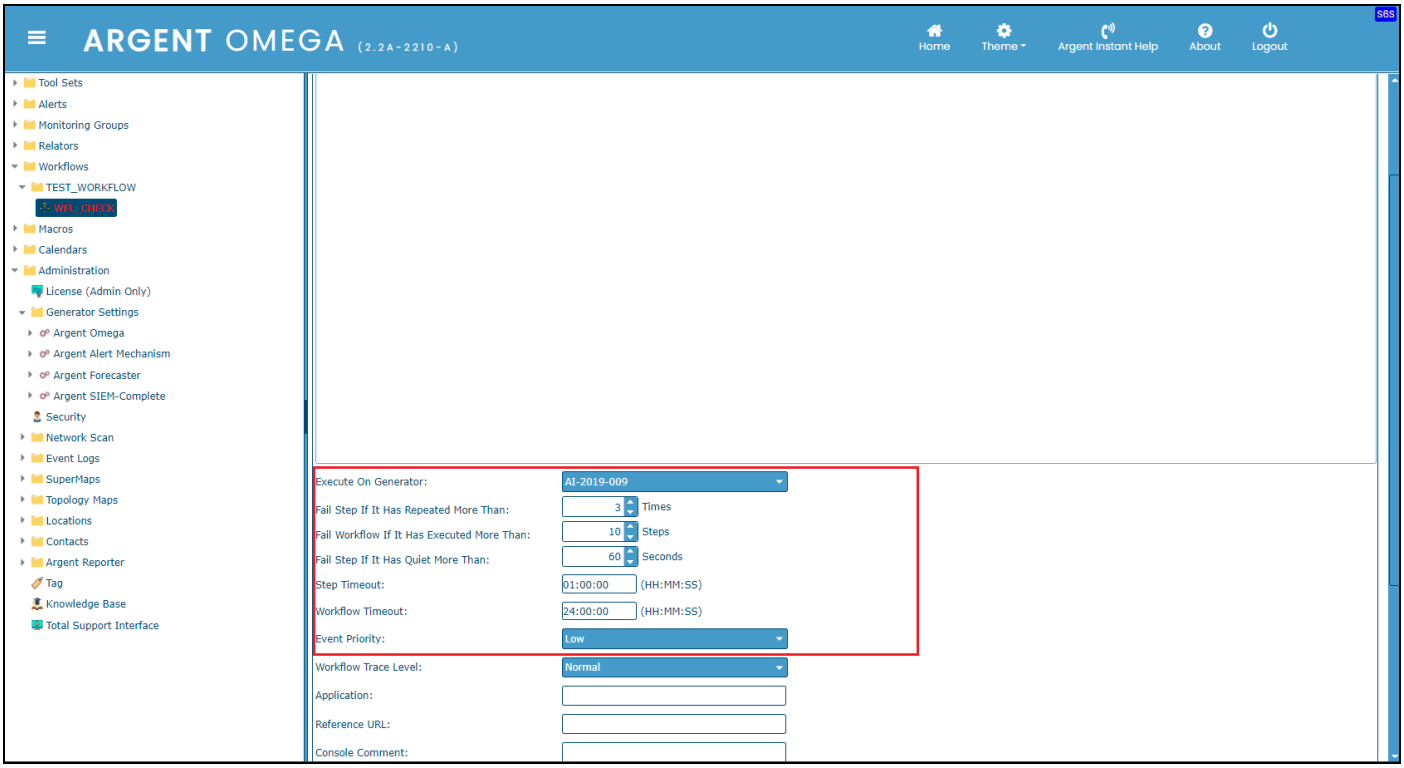


This way you can add any number of Steps.

To test the execution of Workflow, click **Test Workflow** context menu option:



Before testing ensure that the following Workflow options are configured:



Execute On Generator: Select the Generator in which Workflow needs to be executed. Workflow only executes on Primary Generator for this version.

Fail Step If It Has Repeated More Than: Specify the limit. Step execution will be considered as failed if a same Step execution will be repeated more than specified number of times.

Fail Workflow If It Has Executed More Than: Specify the limit. Workflow execution will be considered as failed if the number of Step executions exceeds the limit specified.

Fail Step If It Has Quiet More Than: Specify the time limit seconds. Step execution will be considered as failed if the execution not responding or no communication between the Omega Engine and target server since the time limit configured.

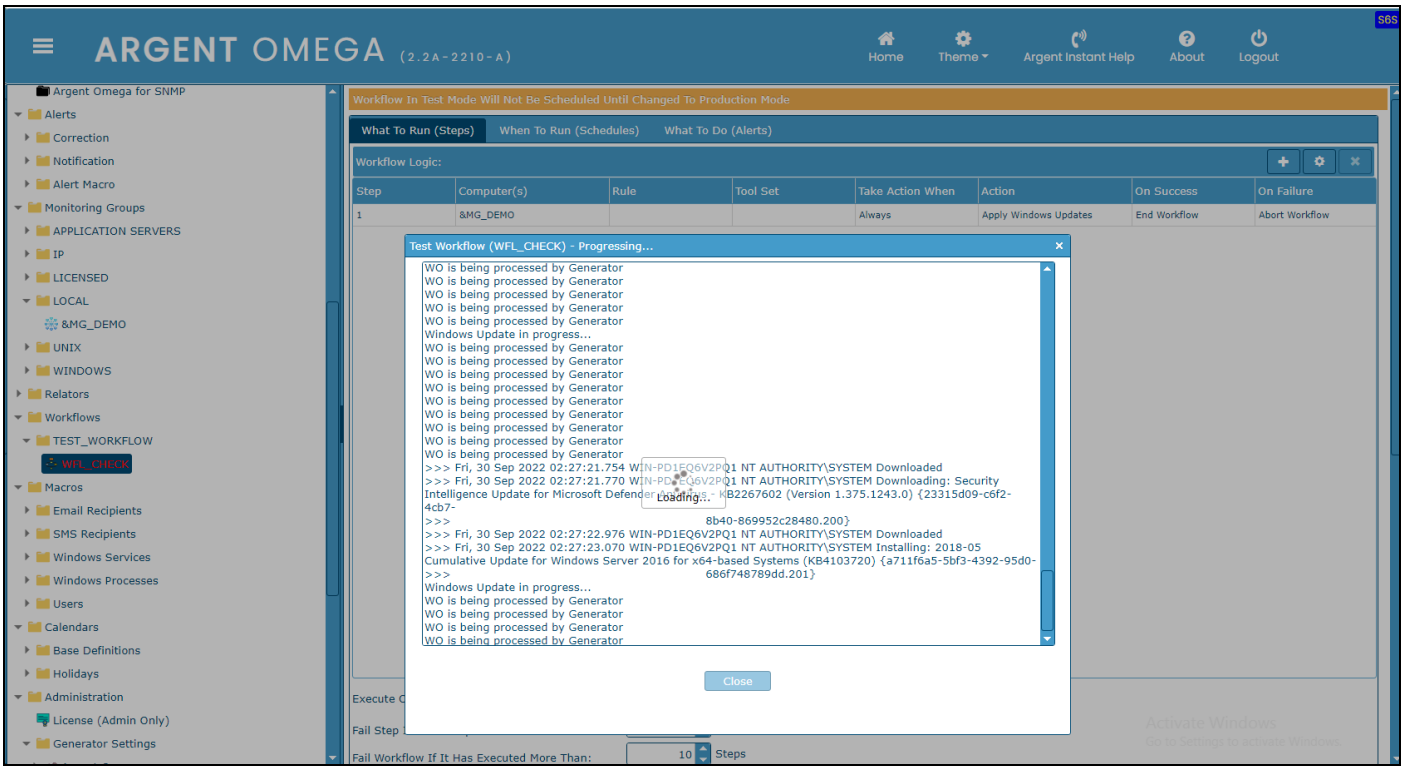
Step Timeout: Specify the time limit in HH:MM:SS format. Step execution will be considered as failed if the Step execution duration exceeds the limit specified.

Workflow Timeout: Specify the time limit in HH:MM:SS format. Workflow execution will be considered as failed if its execution duration exceeds the limit specified.

Event Priority: Configure this to fire event with specified priority.

Click **Save** context menu option to save the Workflow definition.

Click **Test Workflow** to test the Workflow definition. You can see the execution progress in result dialog:

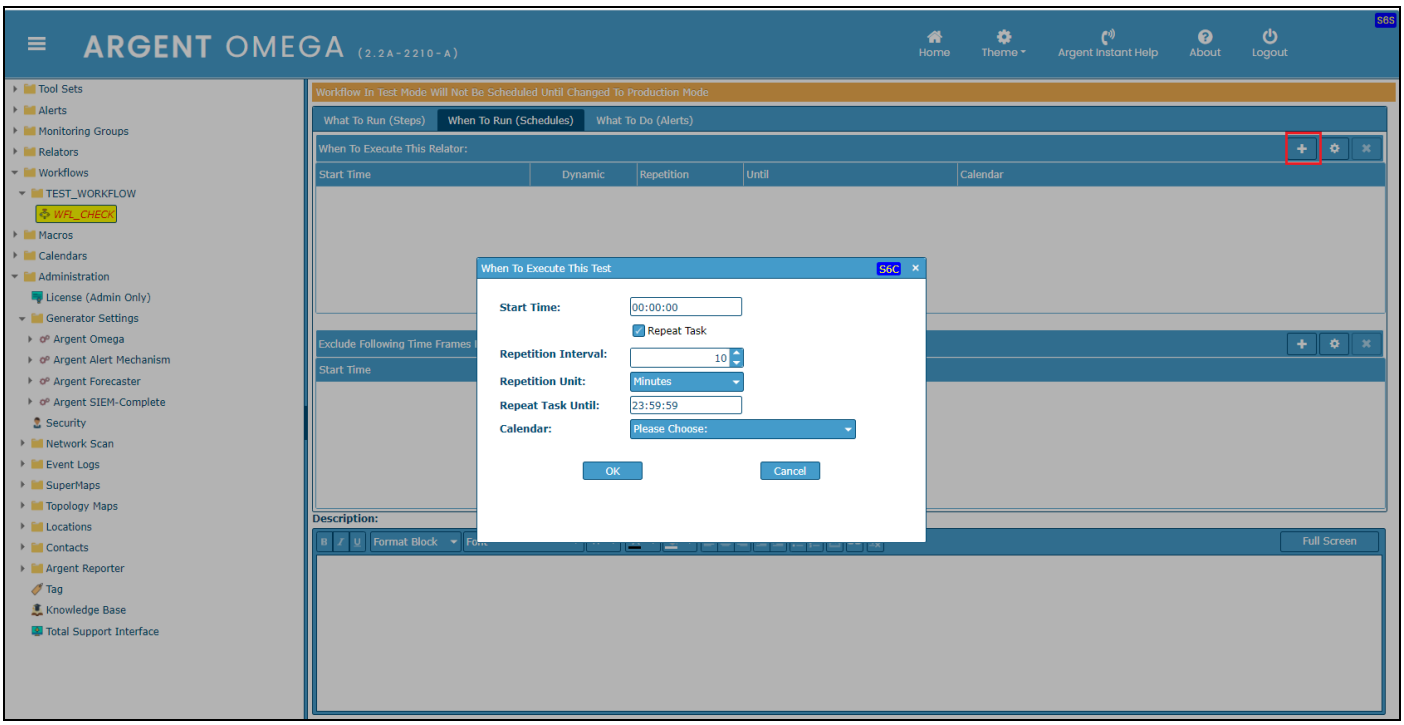


Proprietary Information – All Rights Reserved

Workflow log file will be created in **OMEGA_INSTALLATION_FOLDER\LOGS\WORKFLOW** folder.

To execute the Workflow in Production mode, Schedules and Alerts needs to be configured. Configure Schedules in **When To Run (Schedules)** tab.

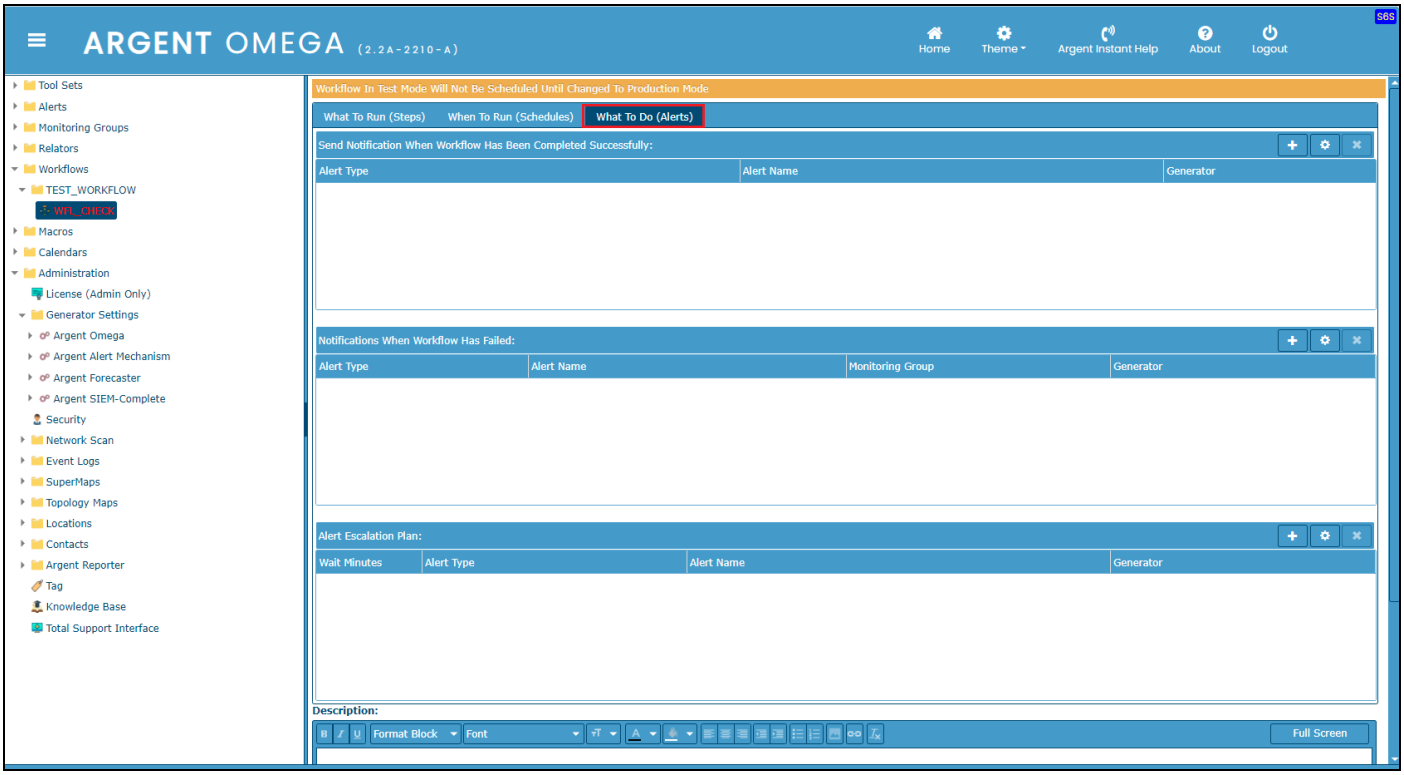
Select **When To Run (Schedules)** tab and click "**+**" to configure the schedule to execute:



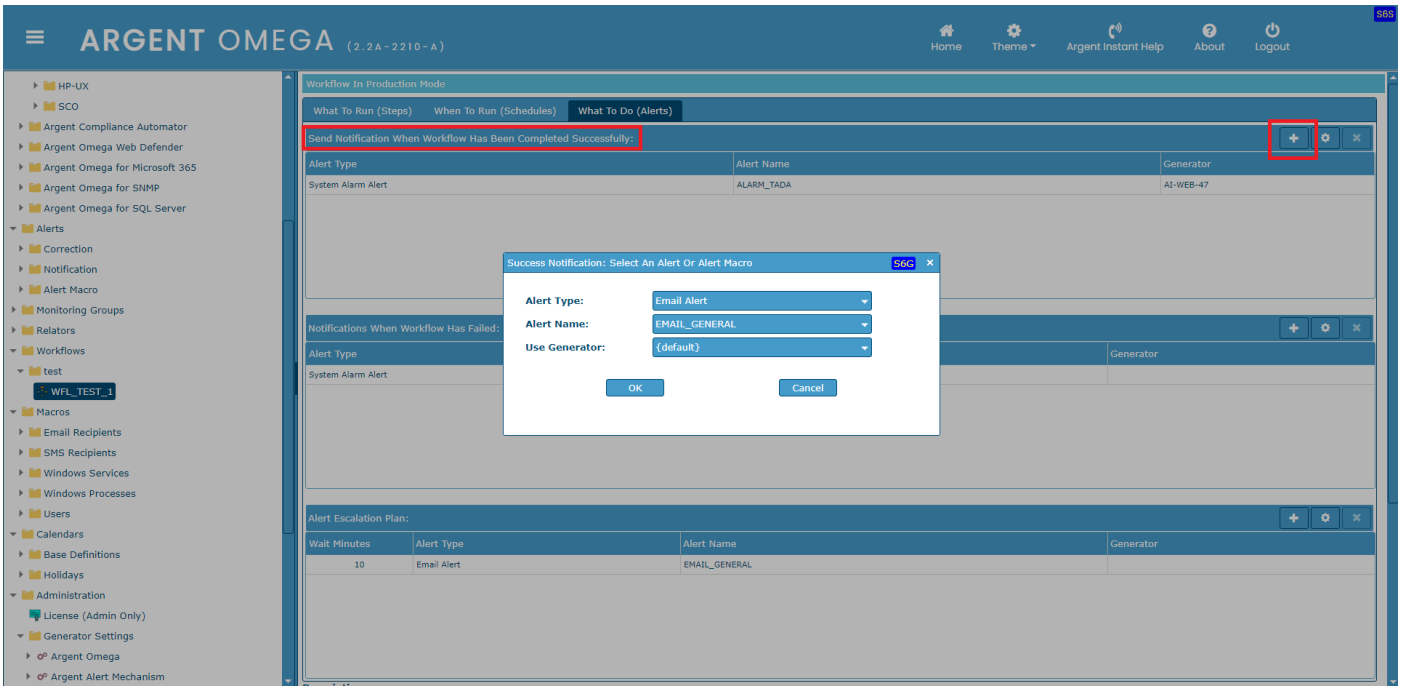
Workflows can also ***optionally*** use Calendars.

Specify Alerts in **What To Do (Alerts)** tab. Workflow has facility to fire Alerts in following situations:

- Fire Alert when Workflow has been completed successfully.
- Fire Alert when Workflow has failed.
- Fire Escalation Alert after configured time.



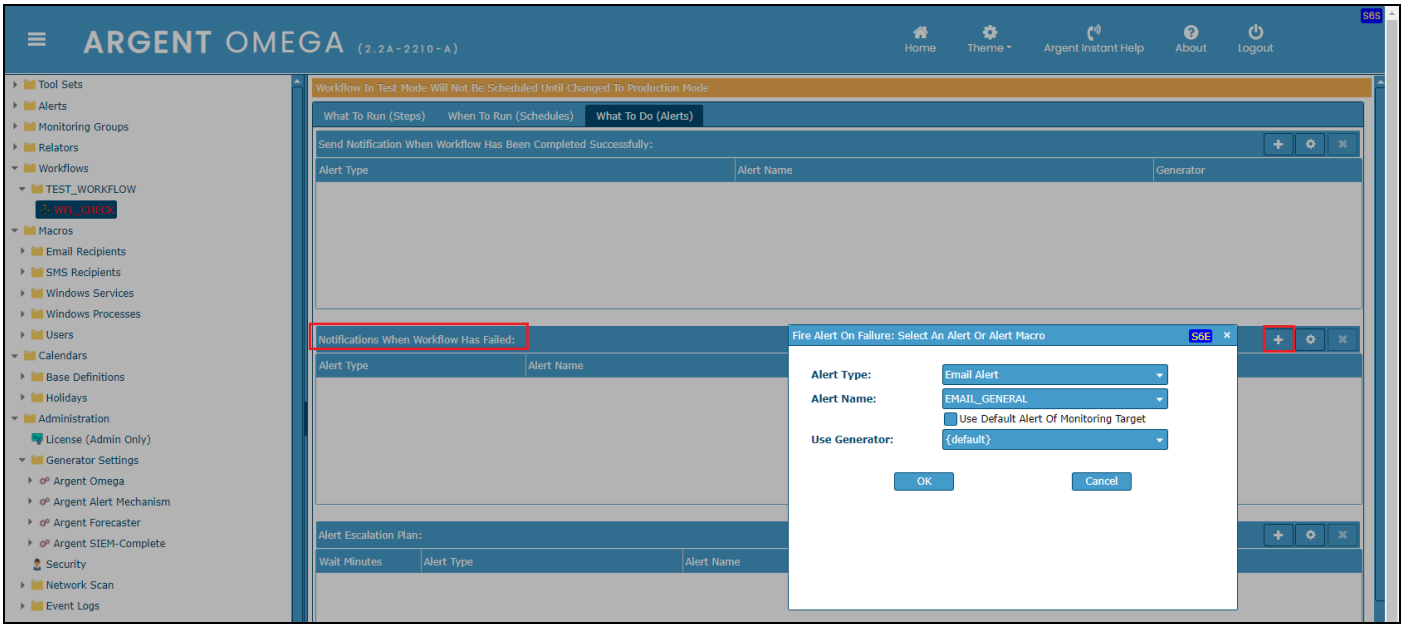
To fire Alert on successful execution of Workflow, configure Alerts in **Send Notification When Workflow Has Been Completed Successfully** section:



Note: If Workflow succeeded, Alert will be fired without raising Event in console.

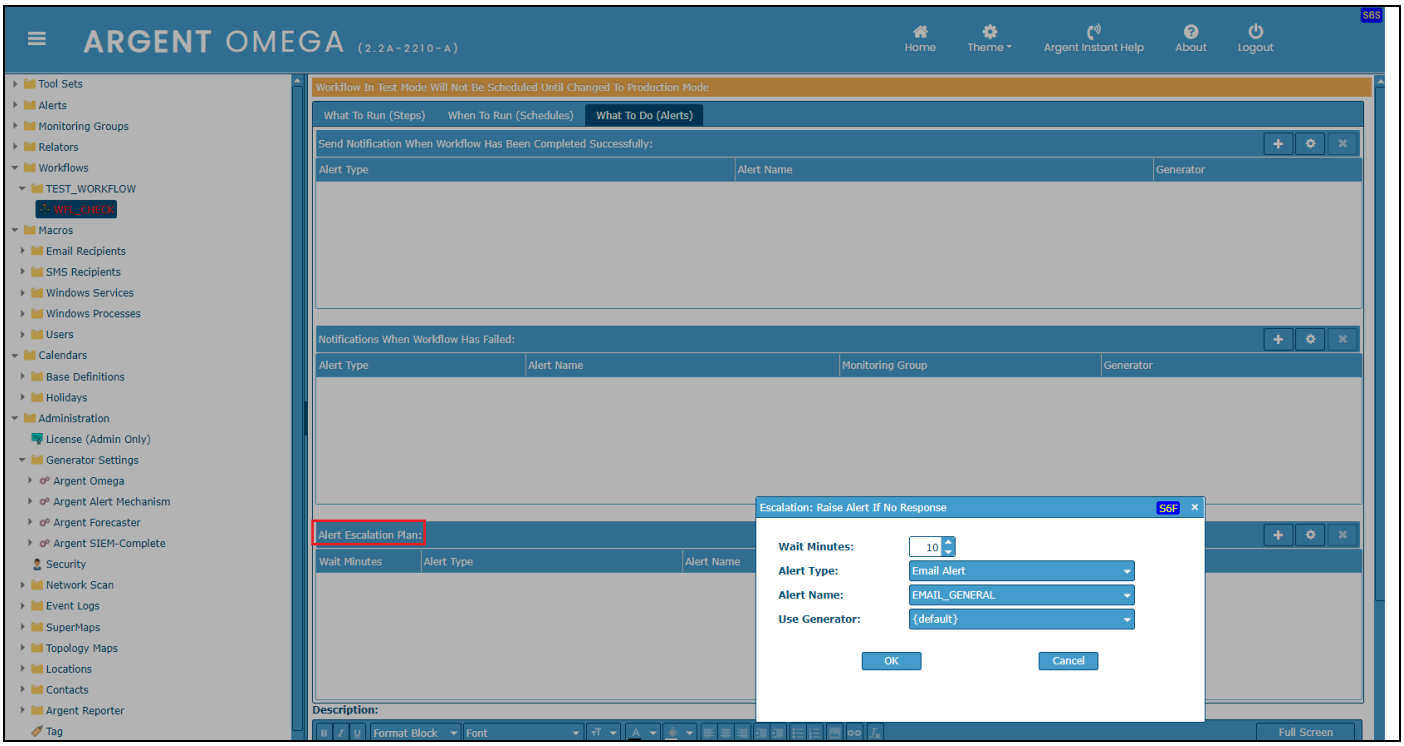
Example: Email will be sent with details.

To fire Alert when Workflow execution failed, configure Alerts in **Notifications When Workflow Has Failed** section:

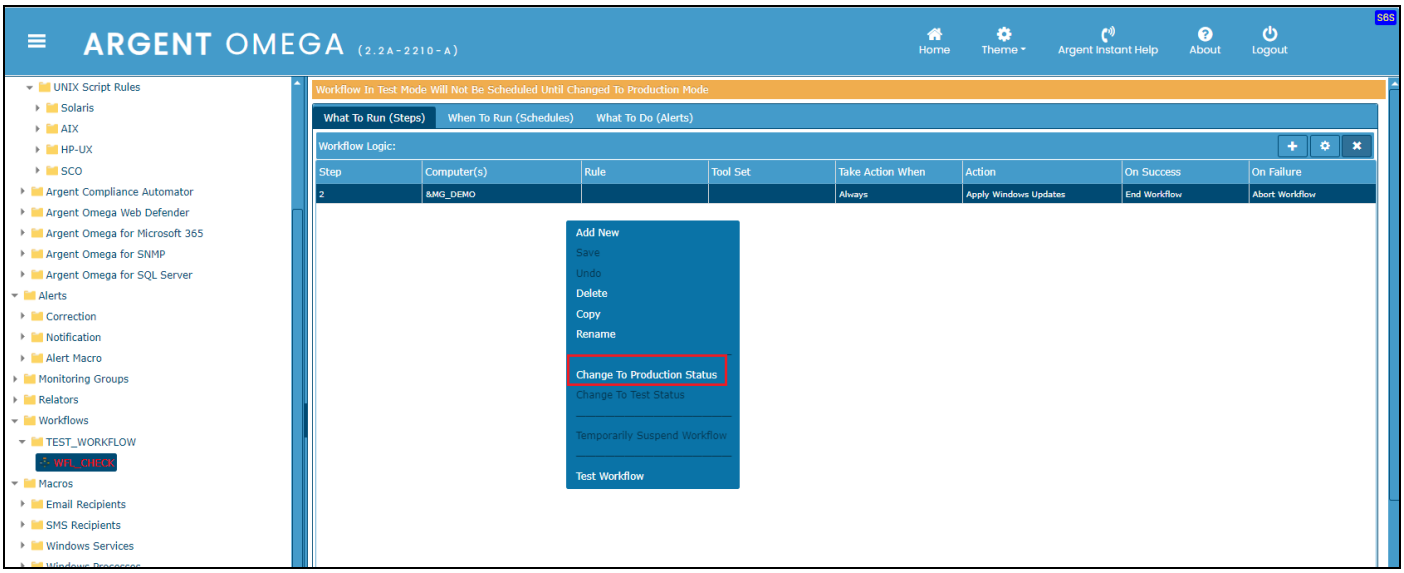


To fire Escalation Alert, configure Alerts in **Alert Escalation Plan** section. Need to specify **Wait Minutes**. Escalation Alert will be fired after the specified time if there is no response:

Proprietary Information – All Rights Reserved

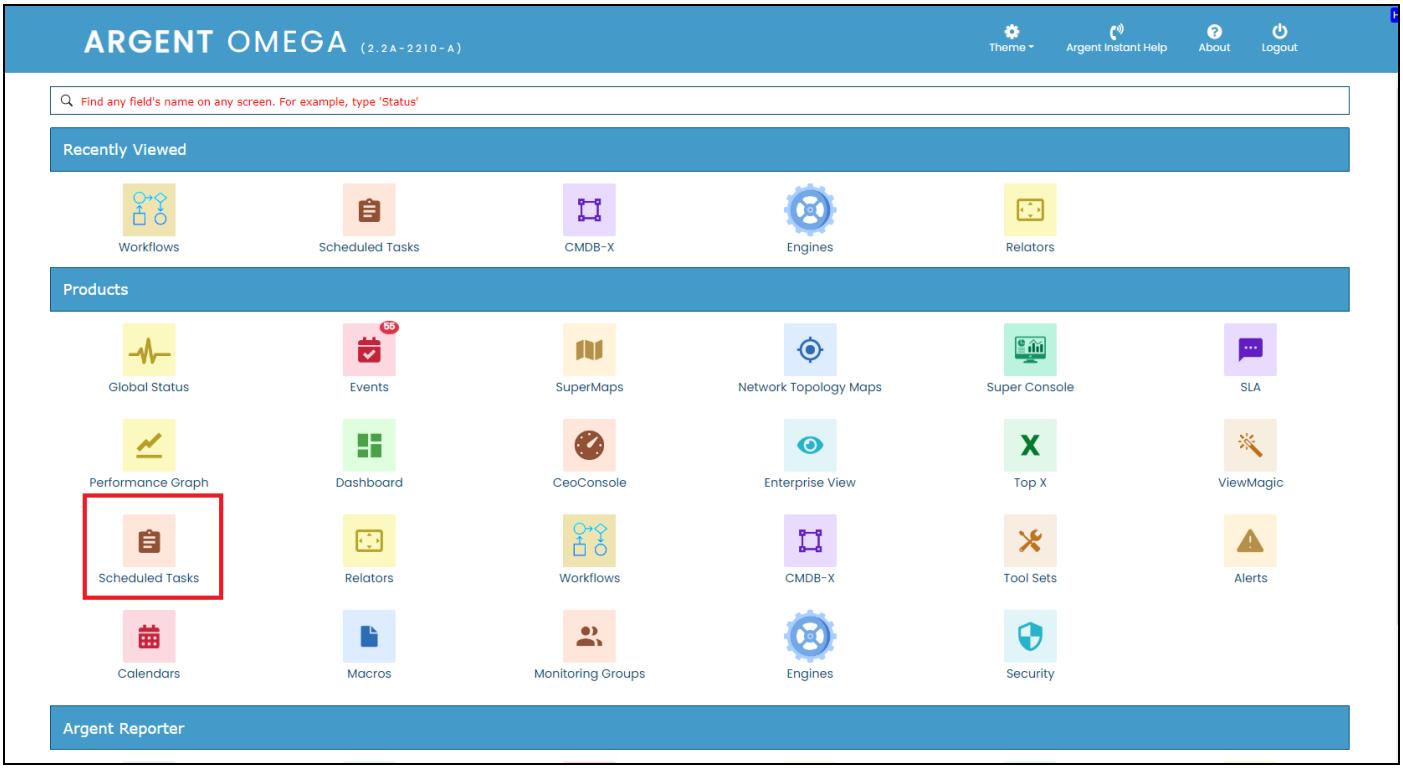


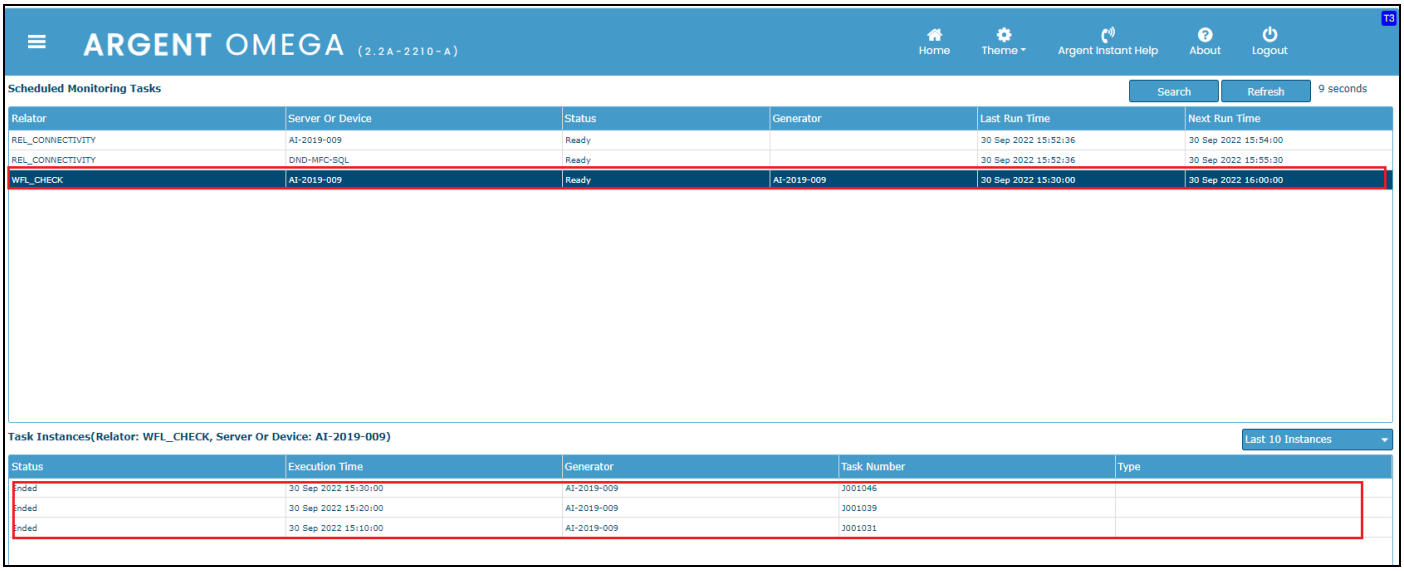
Click **Change To Production Status** context menu option to run Workflow in Production Mode:



Proprietary Information – All Rights Reserved

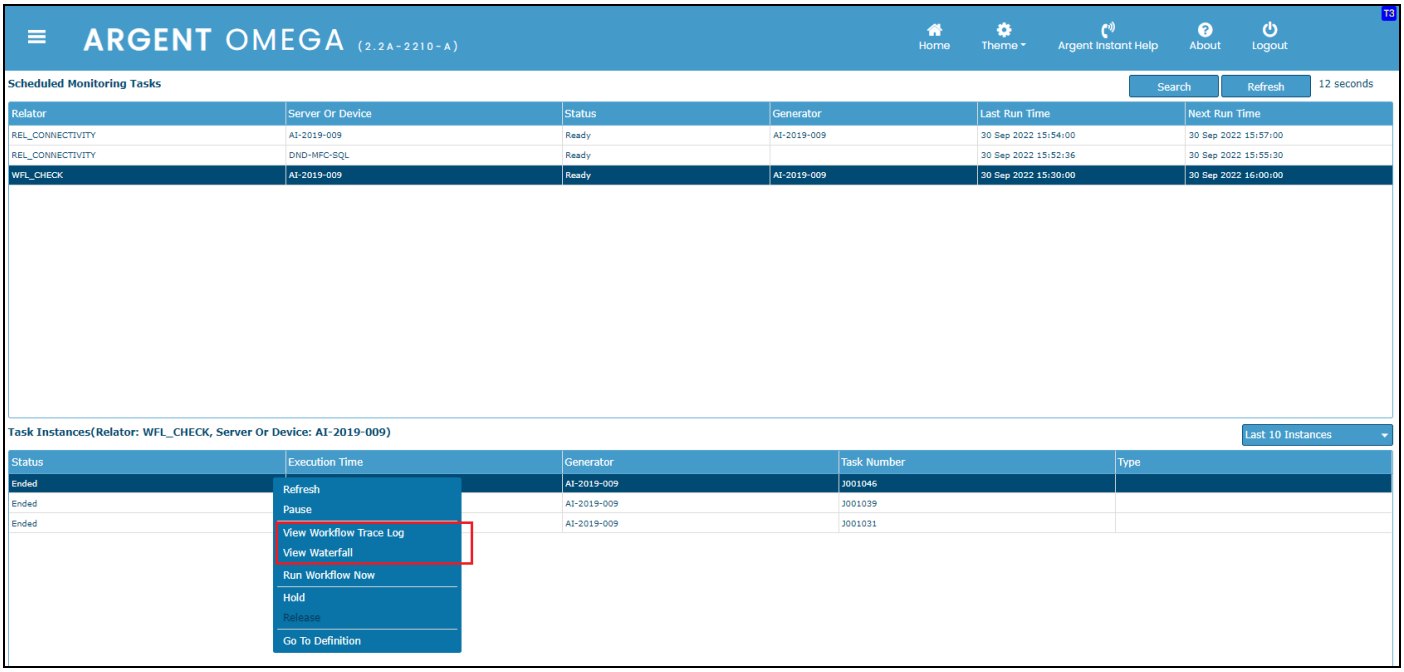
Click **Scheduled Tasks** menu item in Home screen to see the Workflow task instances:



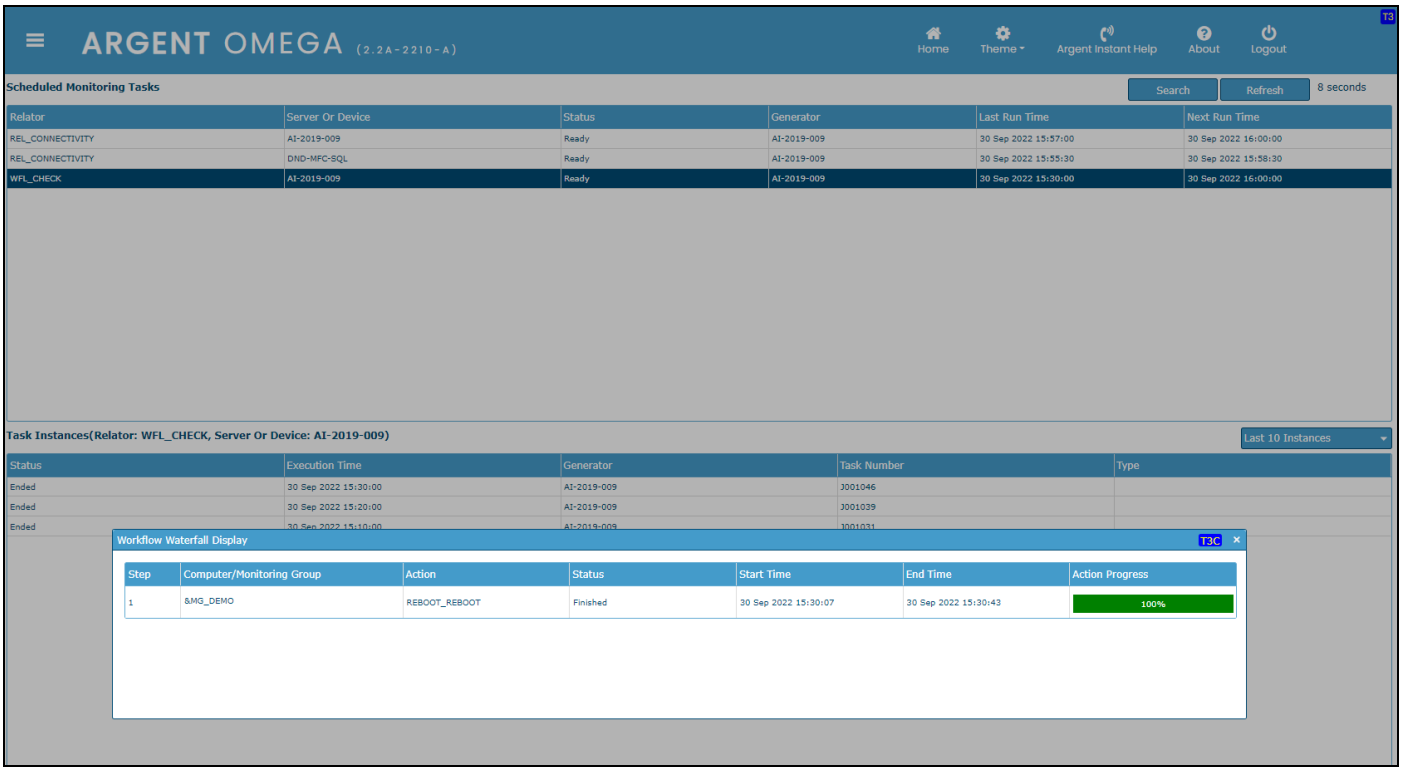


Proprietary Information – All Rights Reserved

Click **View Workflow Trace Log** to see execution trace log of selected Workflow instance:



Click **View Waterfall** to see Workflow waterfall display:

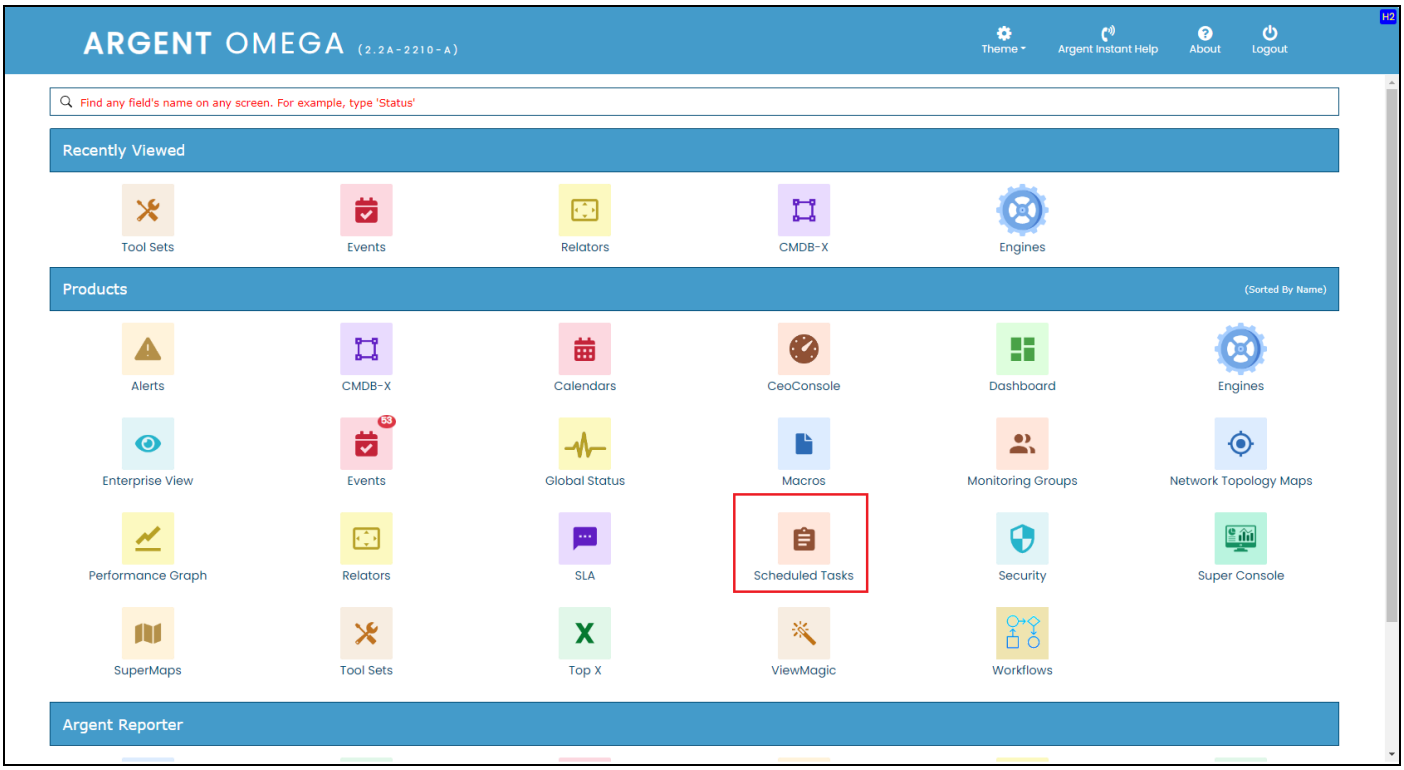


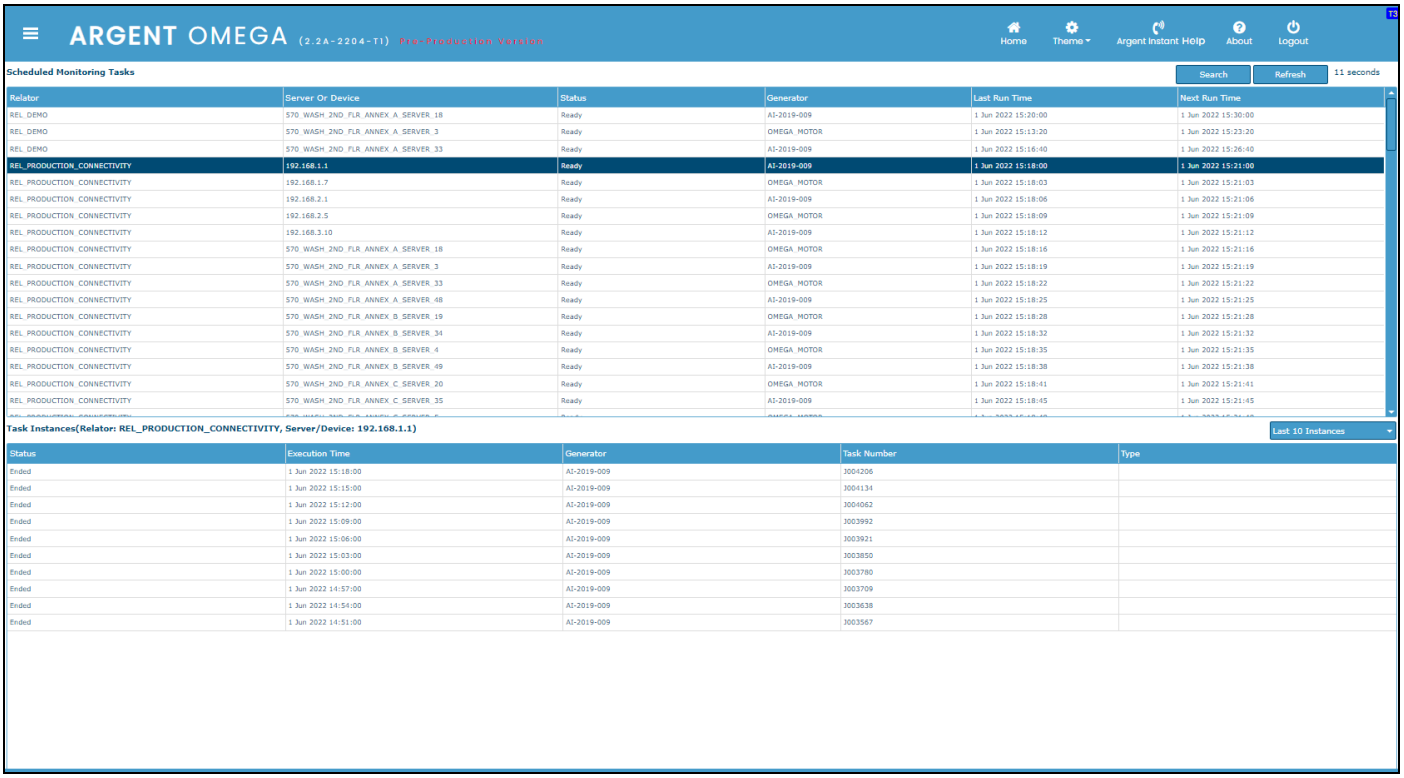
Proprietary Information – All Rights Reserved

Scheduled Tasks

The **Scheduled Tasks** section is a useful method of viewing the schedules for upcoming Relators or Workflows, as well as Relators or Workflows that have completed execution. Each task has an individual log that can be viewed by right-clicking on the task.

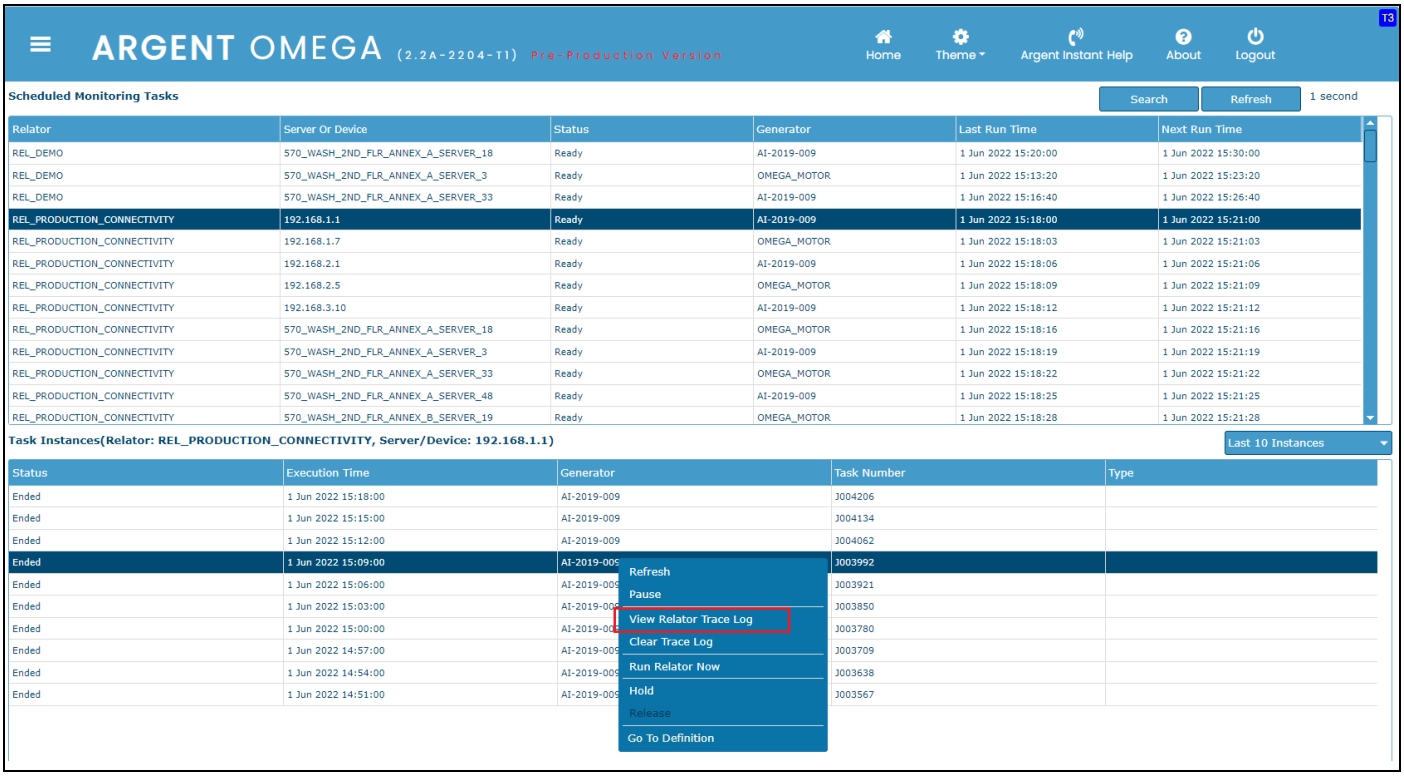
Select **Scheduled Tasks** from the Home Screen.

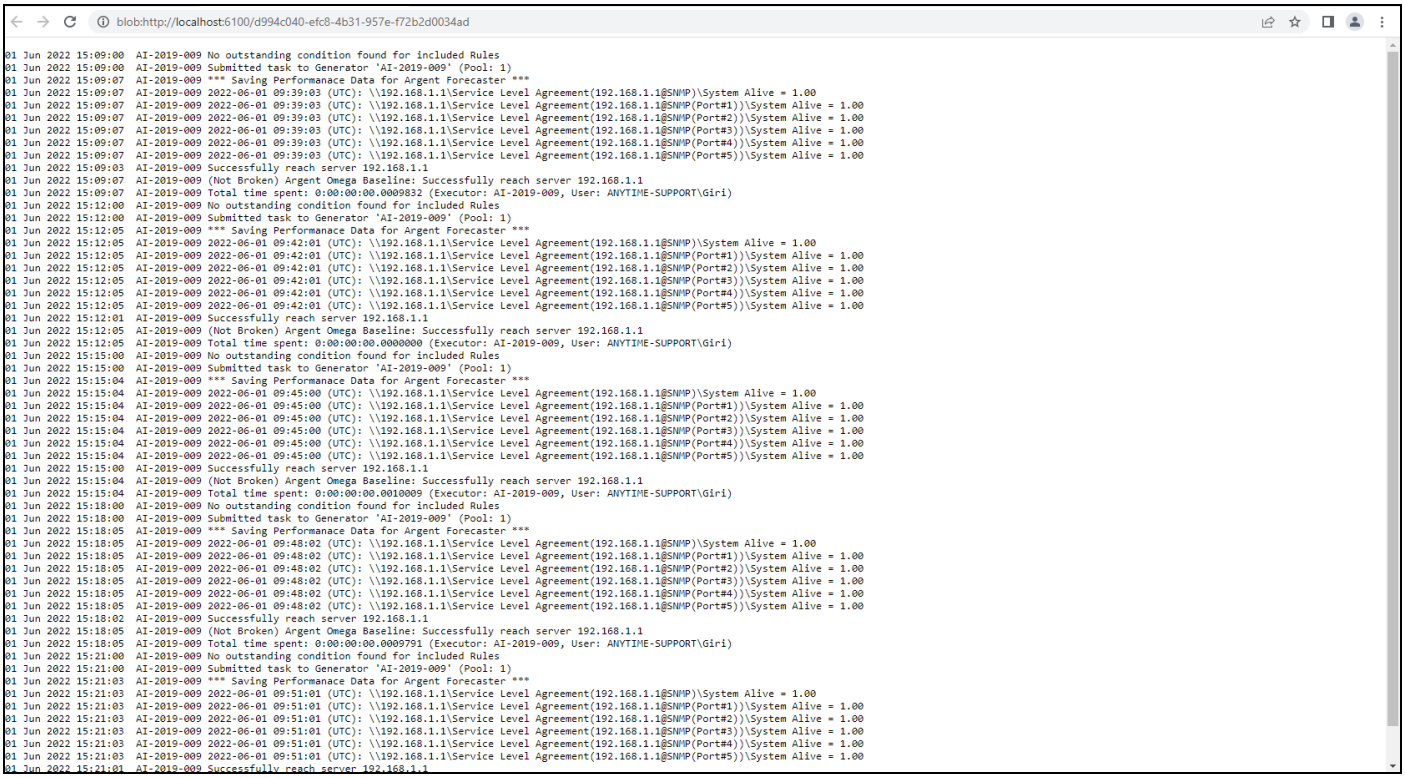




Proprietary Information – All Rights Reserved

Select any Relator and click **View Relator Trace Log** from context menu.



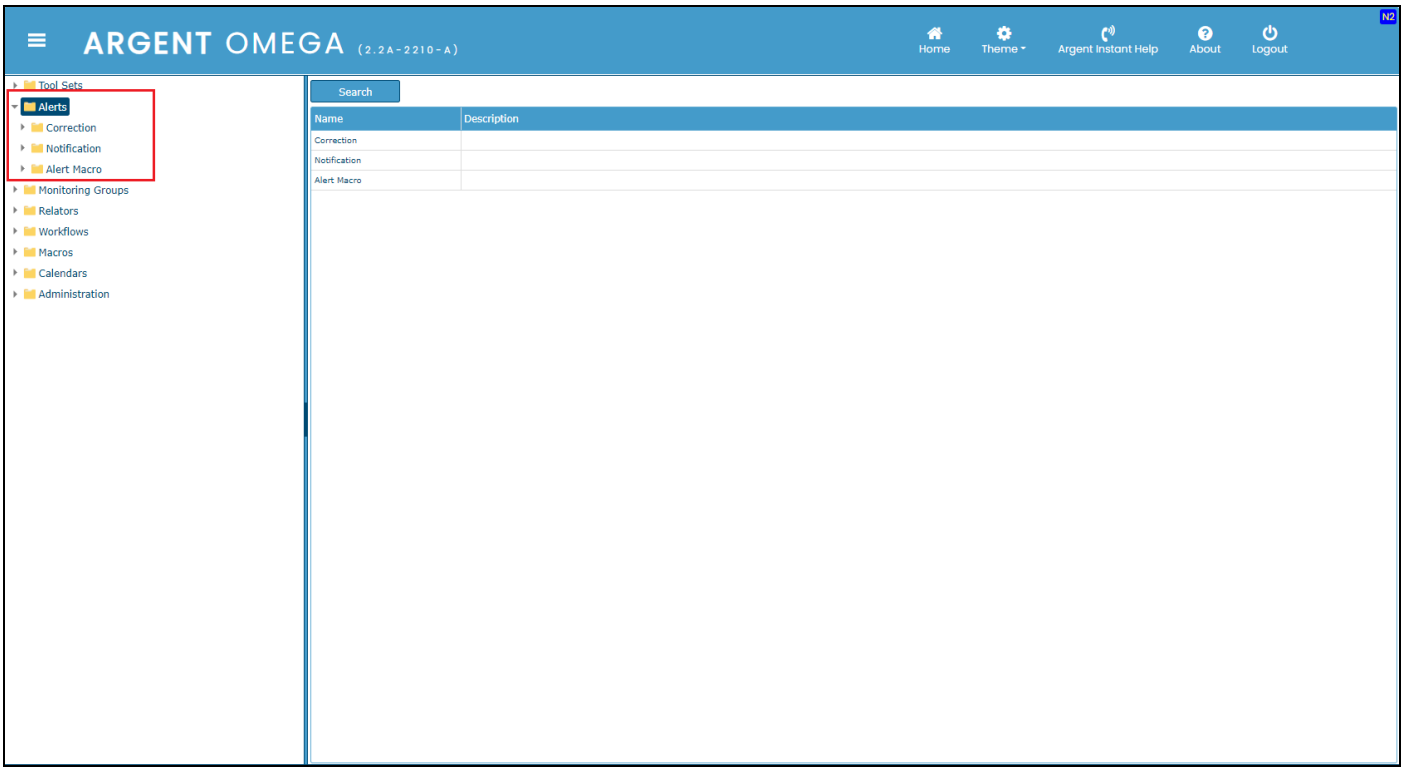


Proprietary Information – All Rights Reserved

Alerts

Argent Omega separates Alerts into three categories:

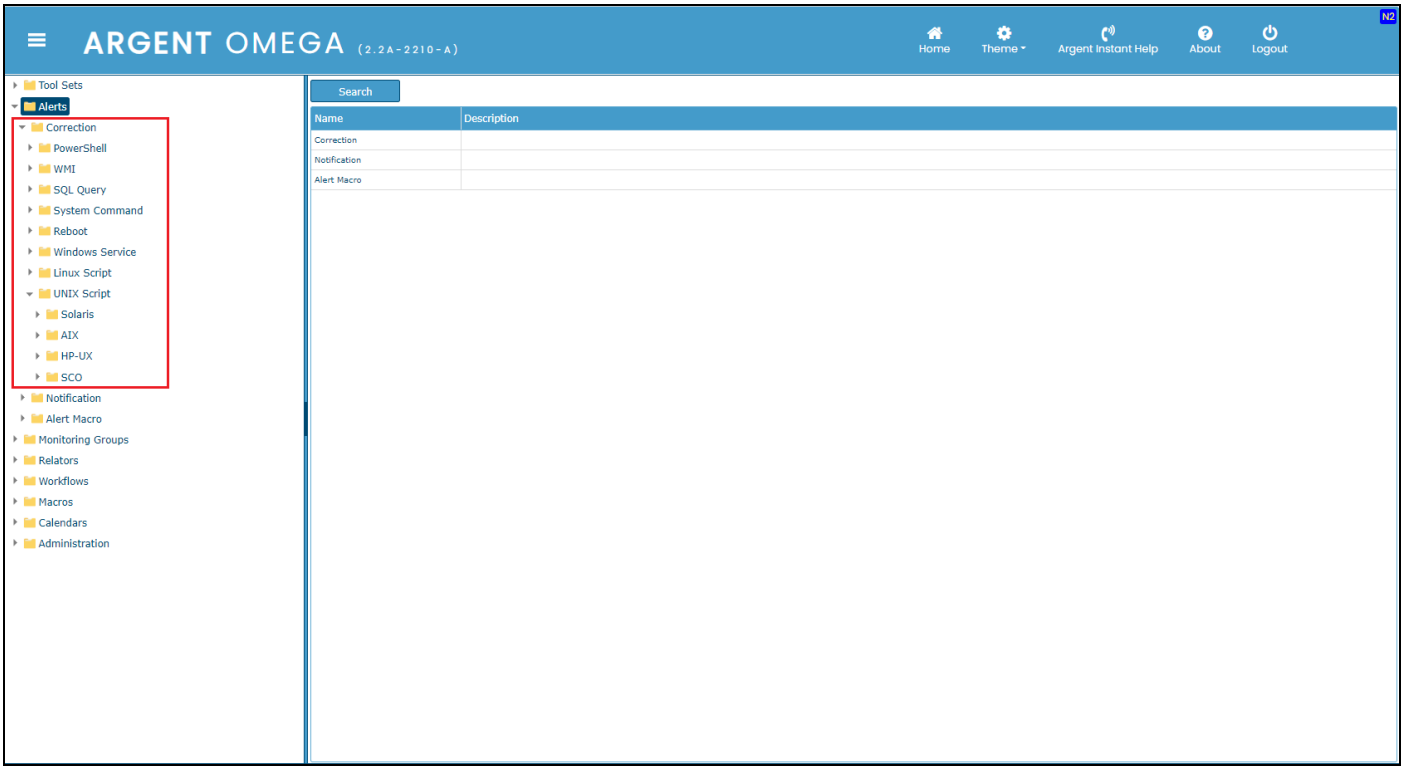
- Correction
- Notification
- Alert Macros



Proprietary Information – All Rights Reserved

Correction Alerts

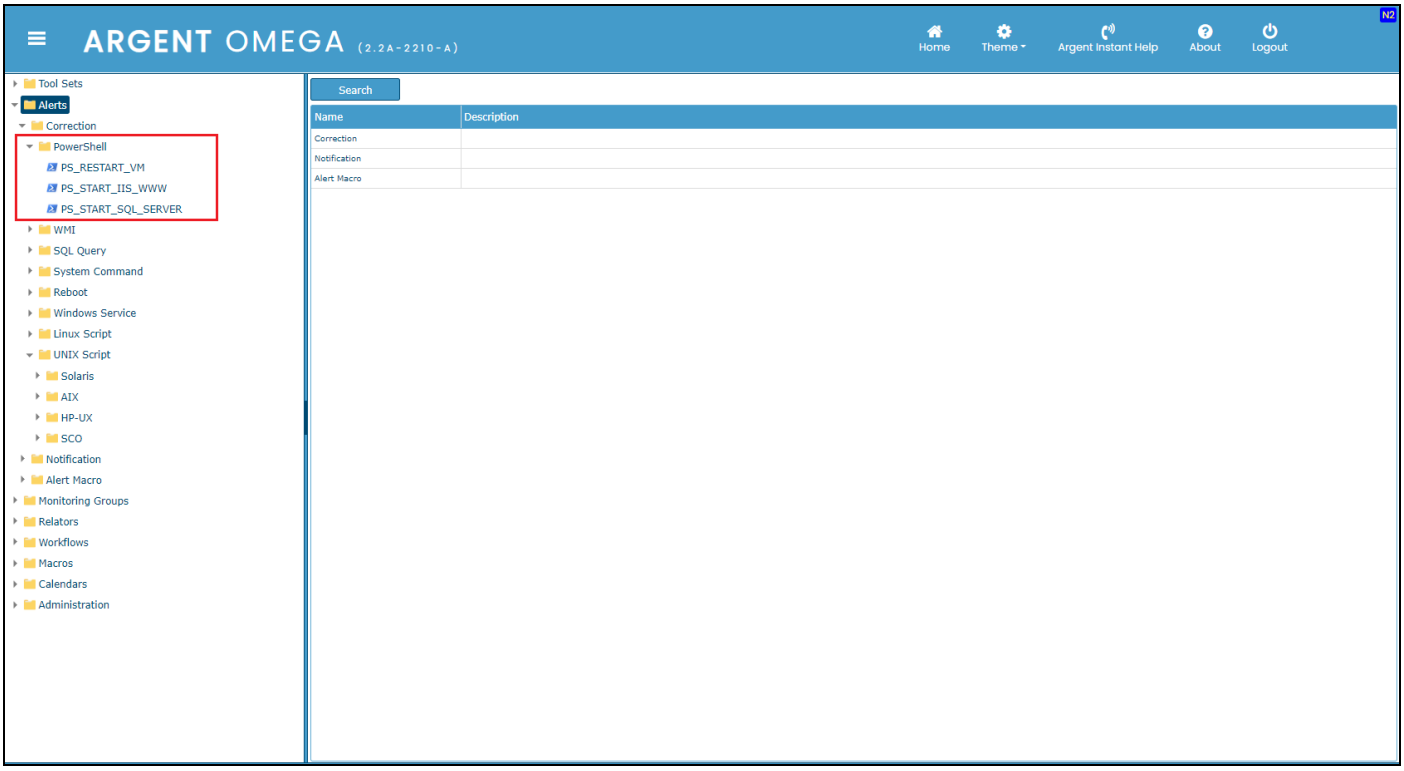
Argent Omega comes with a set of Correction Alerts to proactively correct issues.



- PowerShell

  These Alerts allow you to execute any PowerShell script.

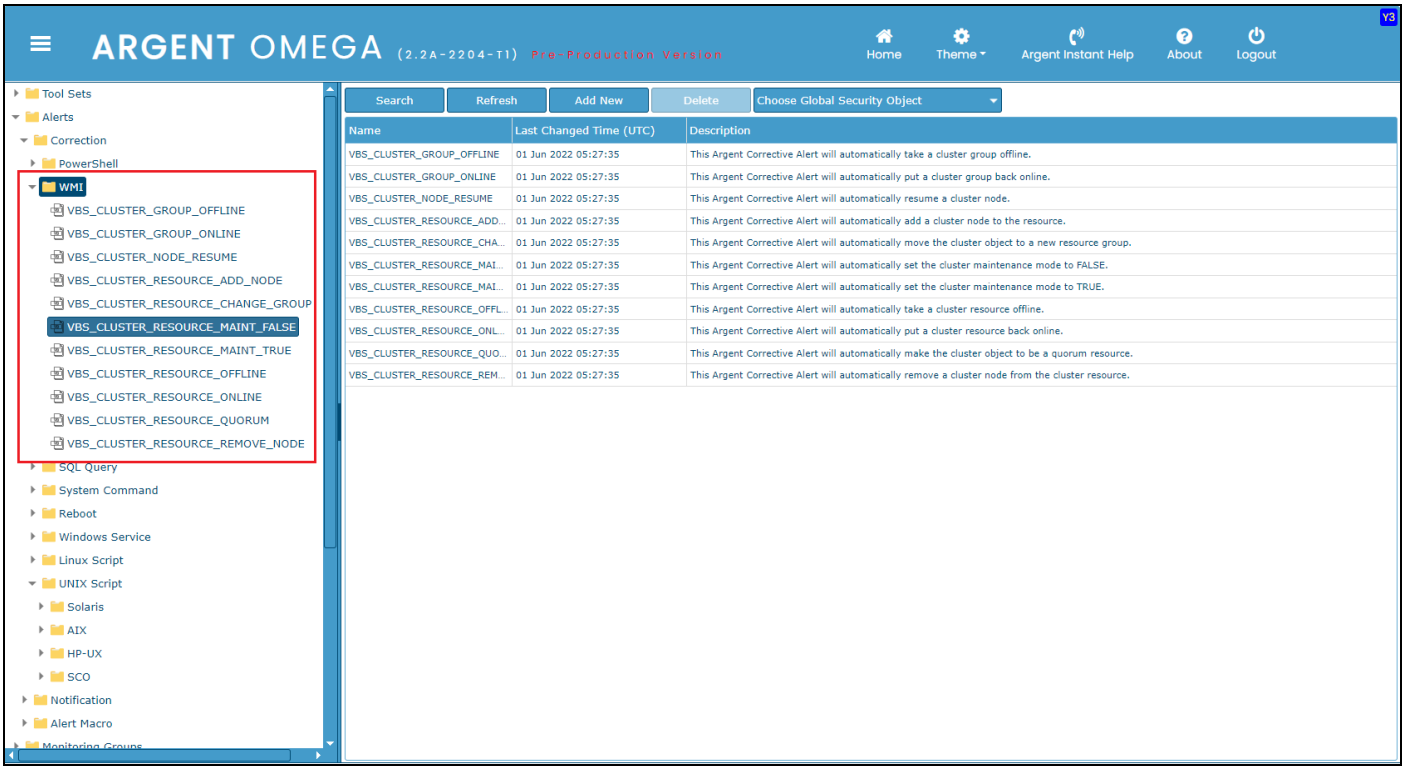
  Remember to specify the PowerShell credentials before executing the Alert.



Proprietary Information – All Rights Reserved

- **WMI**

  These Alerts allow you to execute any WMI script.

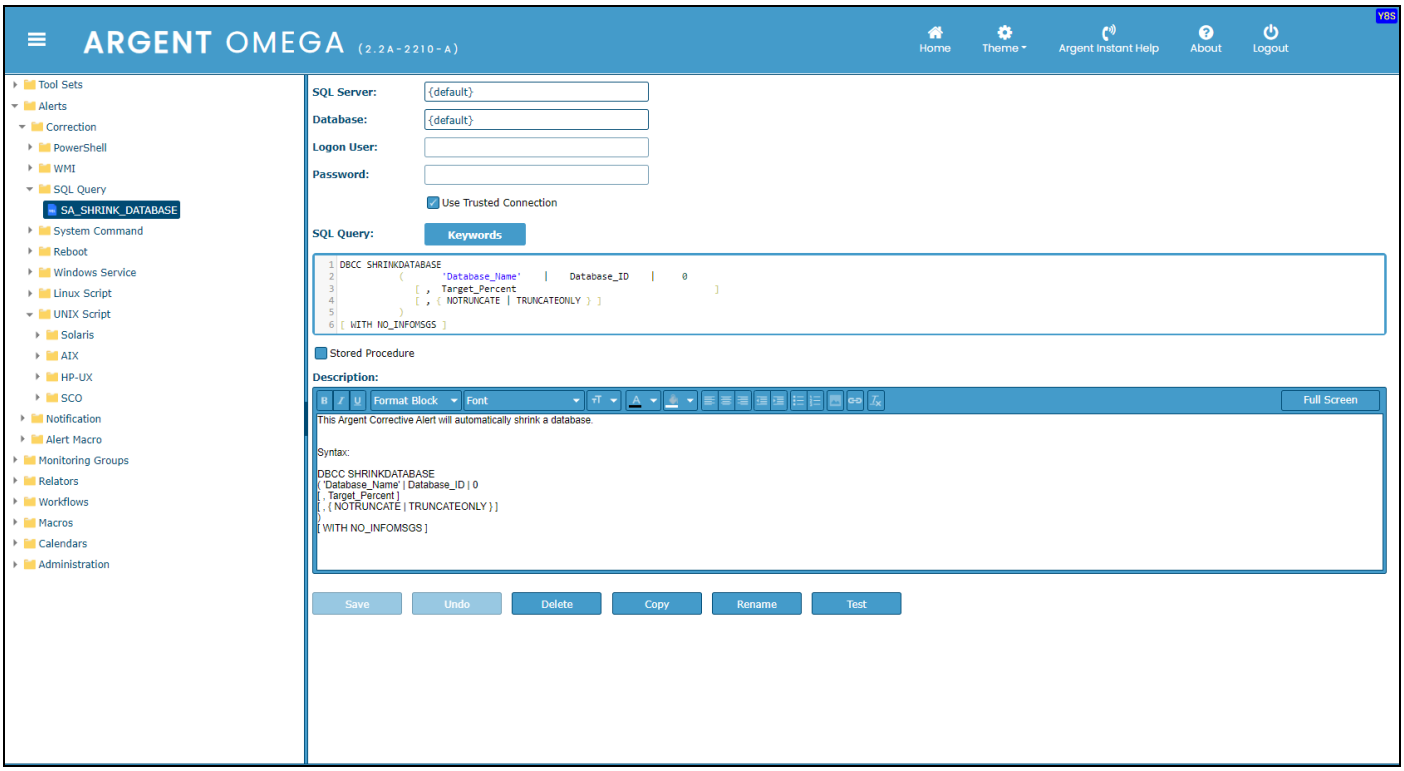


Proprietary Information – All Rights Reserved

- **SQL Query**

  These Alerts allow you to execute any SQL Query.

  Remember to specify the SQL Server credentials before executing the Alert.

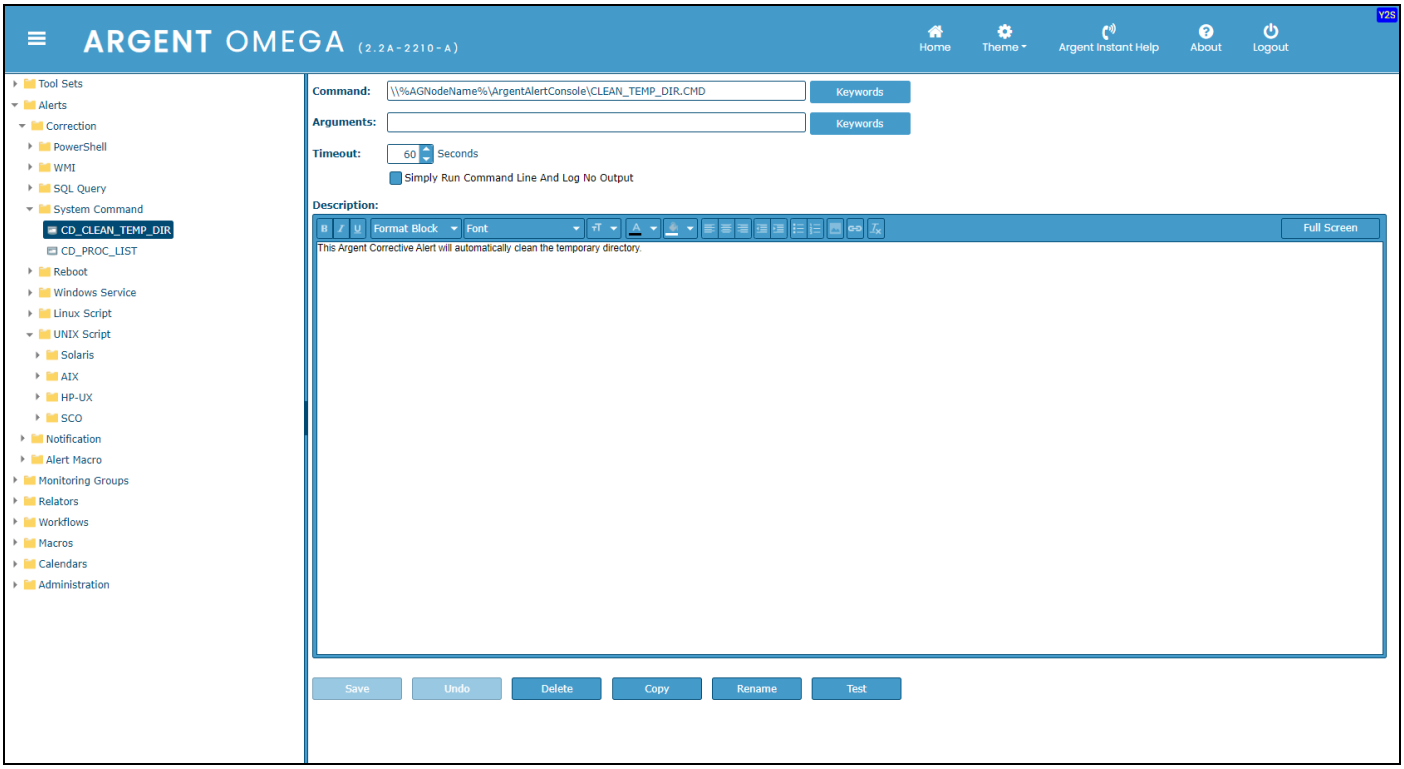


Proprietary Information – All Rights Reserved

- **System Command**

  These Alerts allow you to execute any batch file, command file or executable on any machine.

  Remember to specify the Windows credentials before executing the Alert on a remote machine.

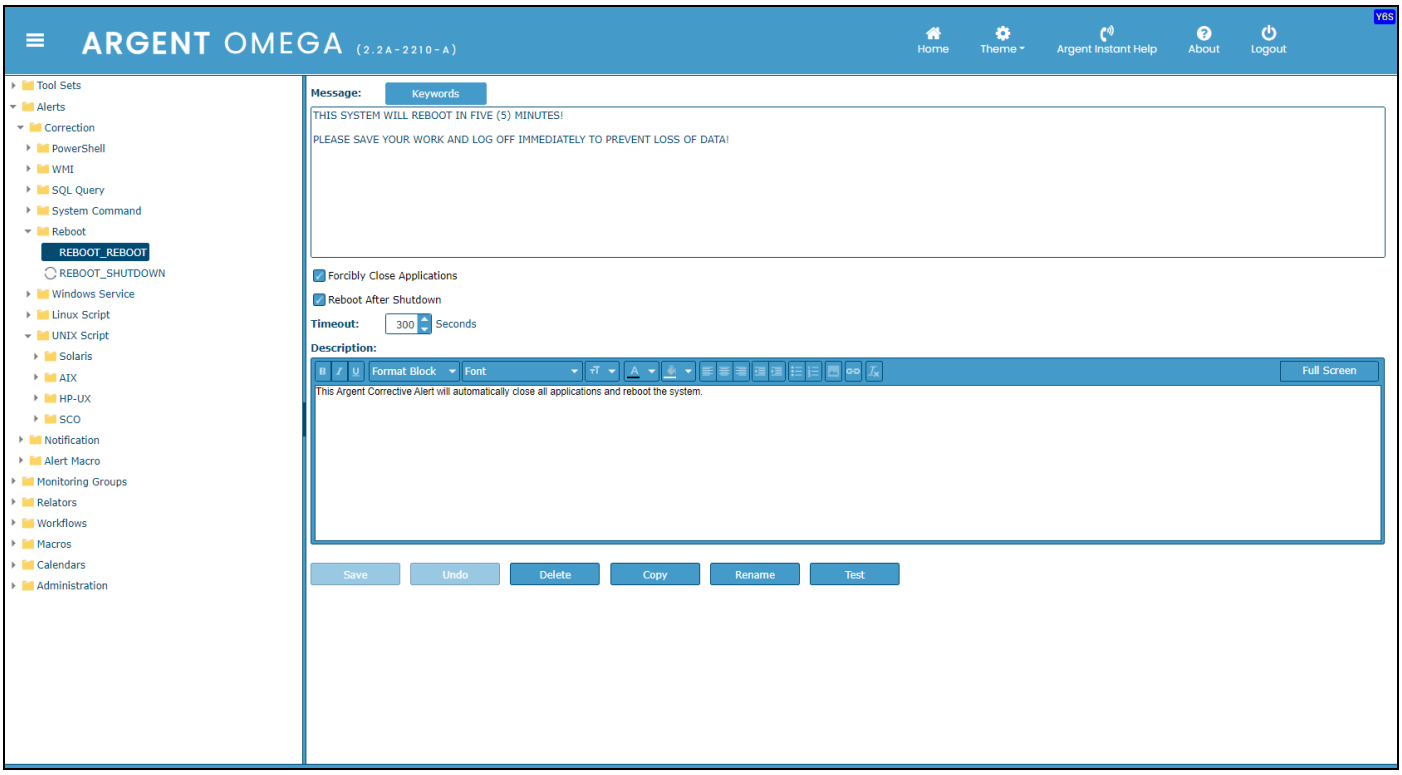


Proprietary Information – All Rights Reserved

- **Reboot**

  These Alerts allow you to perform a **system reboot or shutdown**. Argent Omega will automatically close all applications and perform the specified action.

  This Alert is restricted only to Administrator users.

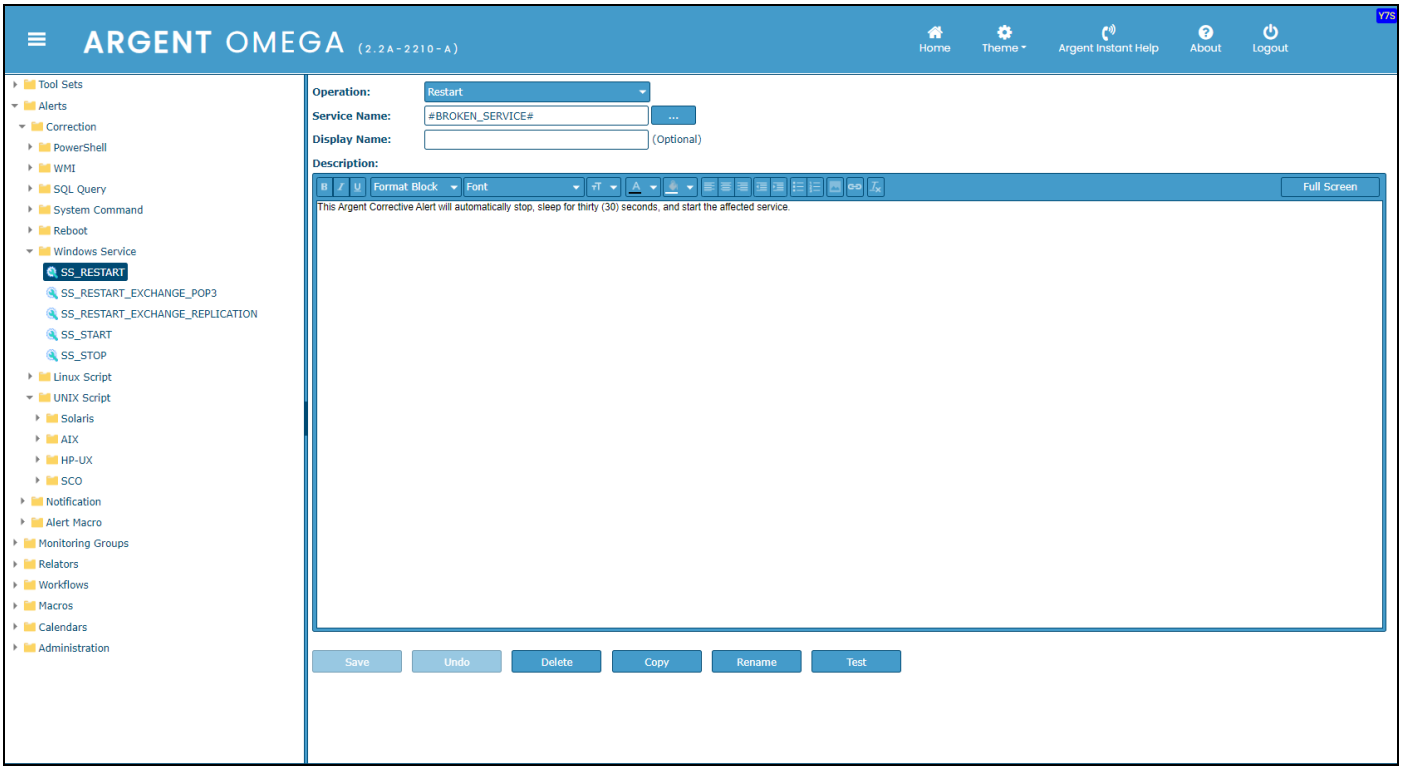


Proprietary Information – All Rights Reserved

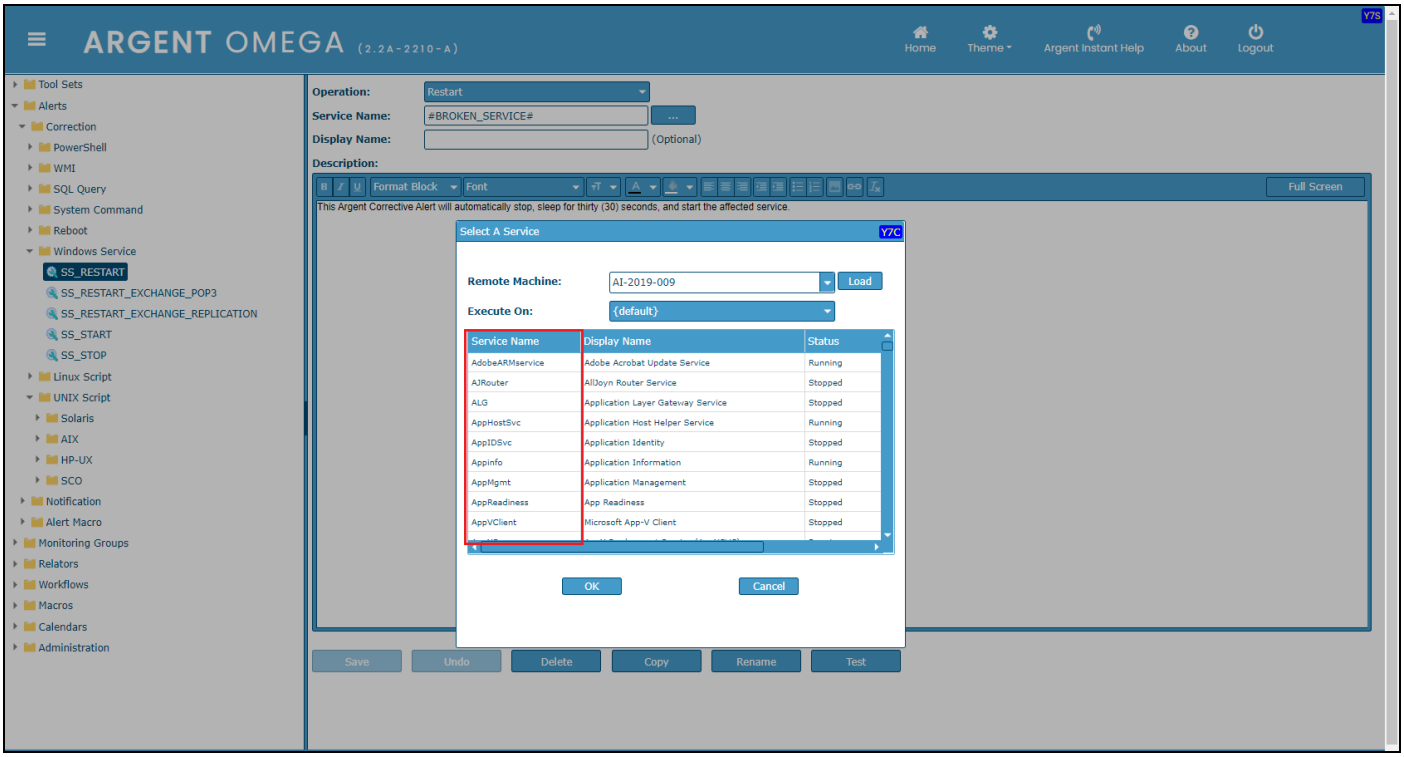
- **Windows Service**

  These Alerts allow you to Stop, Start, or Restart a stalled or stopped service.

  Argent is unique in its ability to detect and correct a stalled service – one that says "Running" on the SCM screen; see Argent KBI Https://Help.Argent.com/#KBI_310212



Select any service name and choose the type of operation for broken service.



Proprietary Information – All Rights Reserved

- **Linux Script**

  These Alerts allow you to execute any Linux shell script.

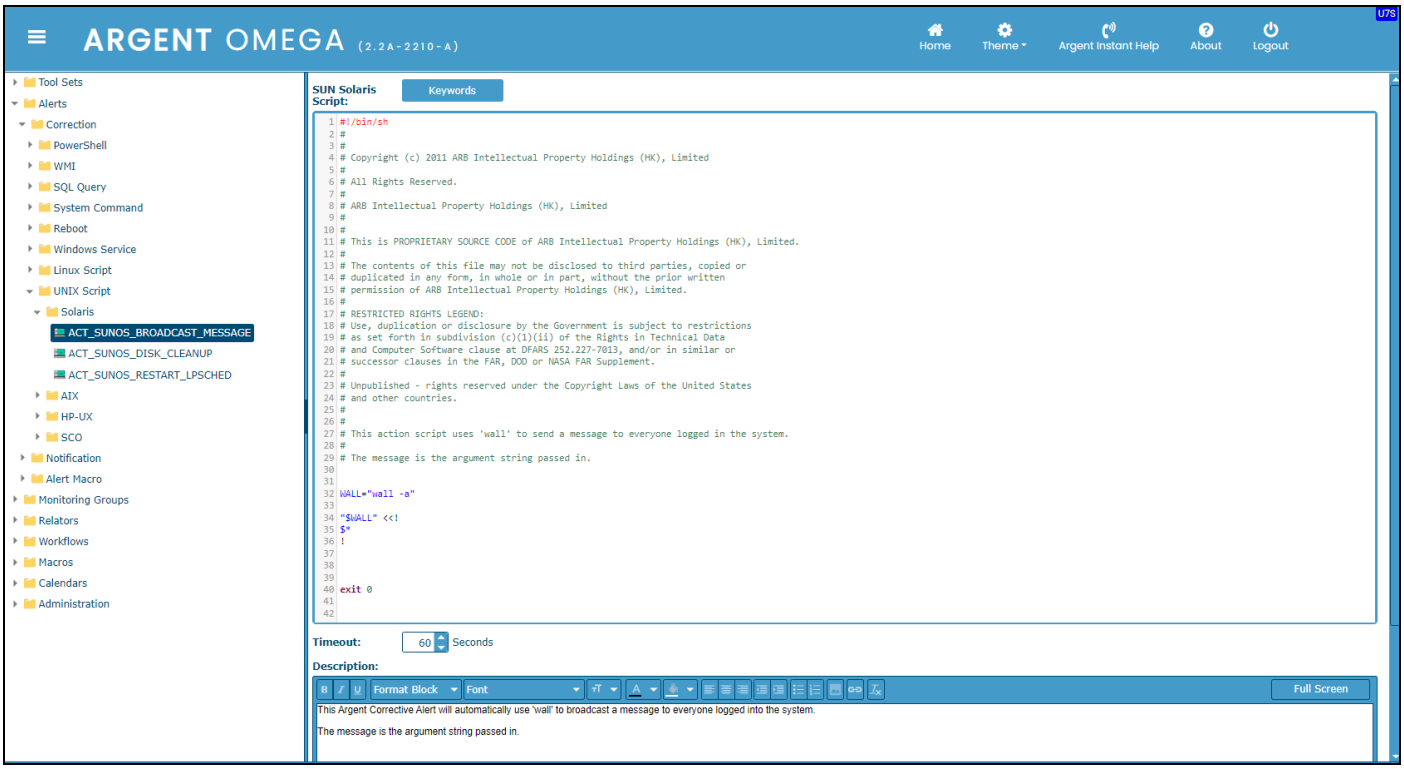
  Remember to specify the Linux credentials before executing the Alert.

Applications hosted off a UNIX environment that are causing issues in your environment can easily be corrected by running shell scripts to restart daemons, kill processes, cleanup disk space, etc.

Proprietary Information – All Rights Reserved

- **UNIX Script**

  These Alerts allow you to execute a UNIX shell script.



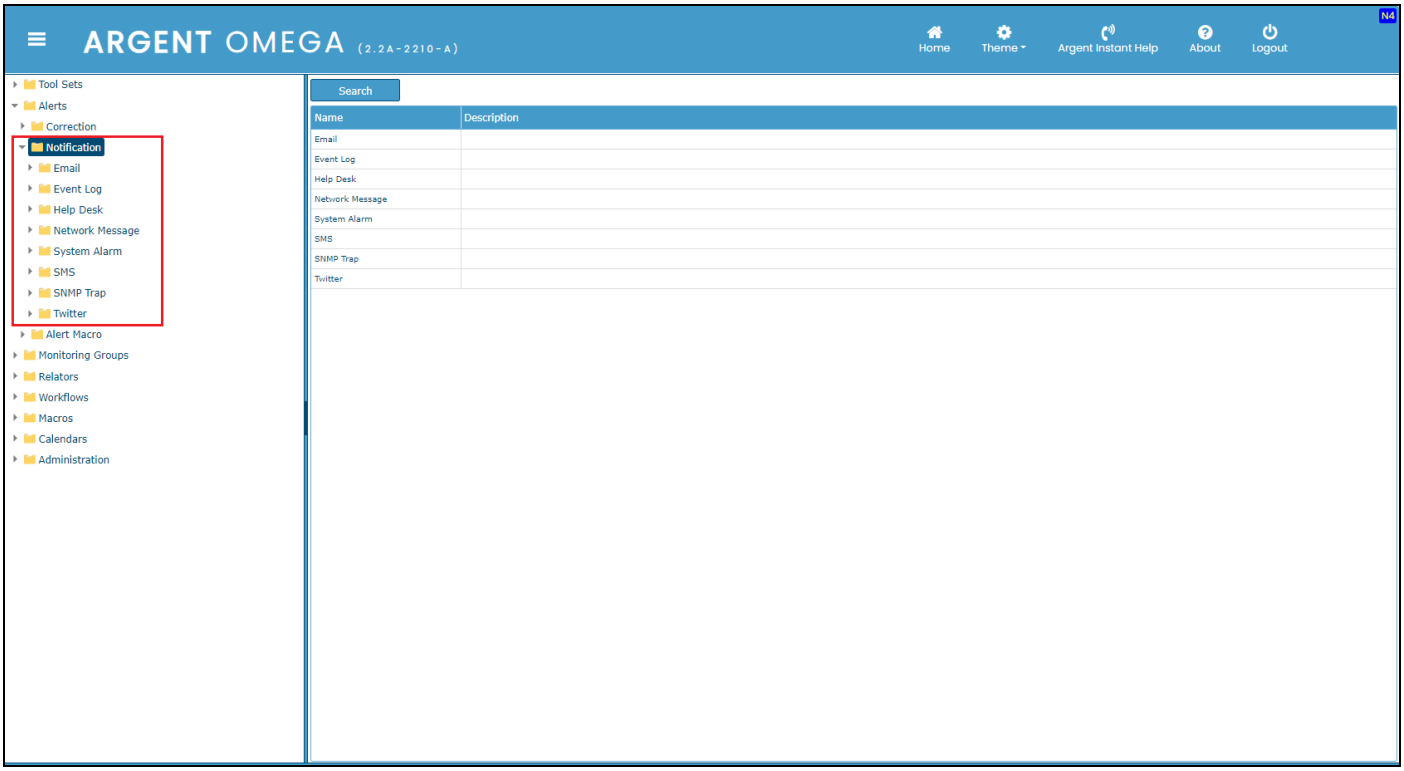
Applications hosted off a UNIX environment that are causing issues in your environment can easily be corrected by running shell scripts to restart daemons, kill processes, cleanup disk space, etc.

Proprietary Information – All Rights Reserved

Notification Alerts

Notification Alerts provide several ways to alert Administrators and support staff.

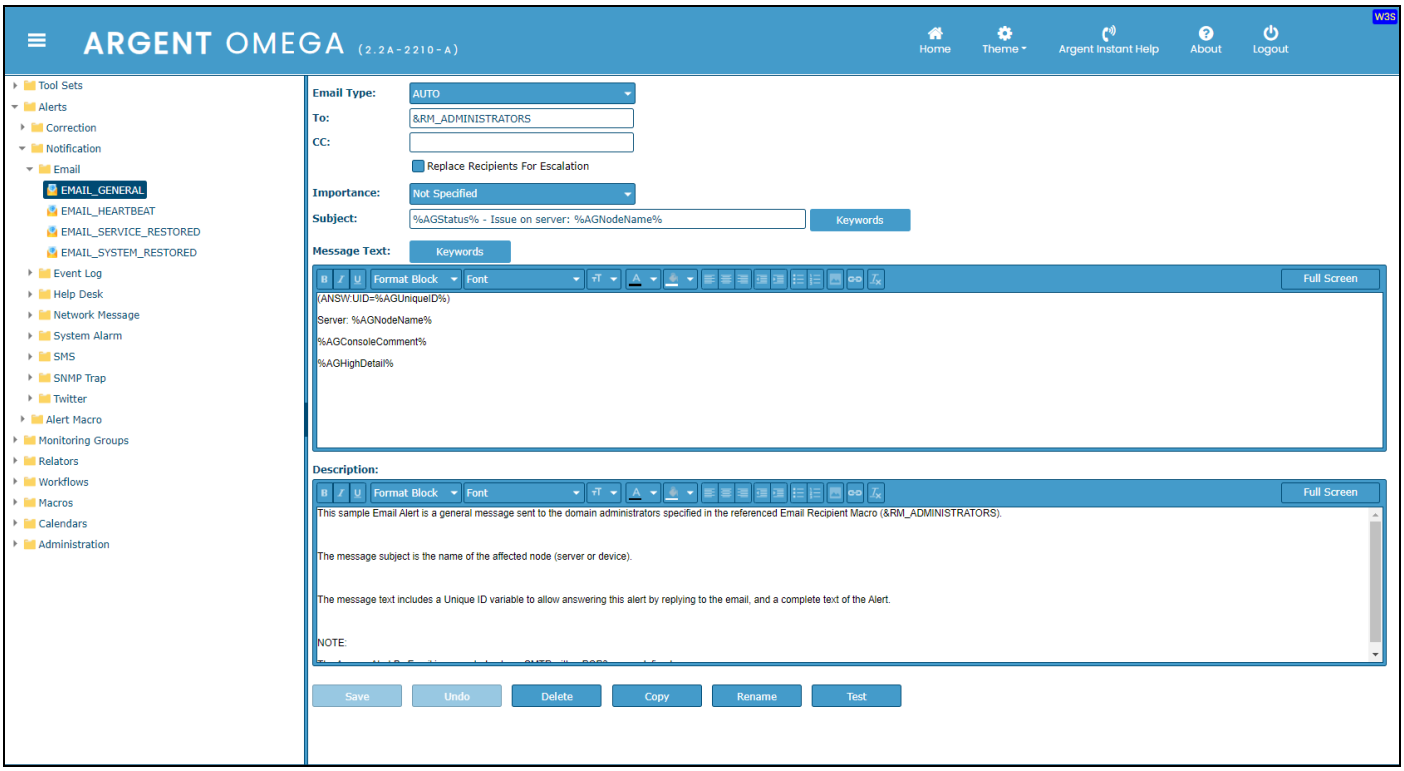
Argent Omega comes with a rich set of Notification Alerts.



Proprietary Information – All Rights Reserved

- **Email**

  This Alert allows you to send an email containing the details of the Alert to any recipient.



The SMTP server or MAPI profile is configured in the Administration area of Argent Omega.

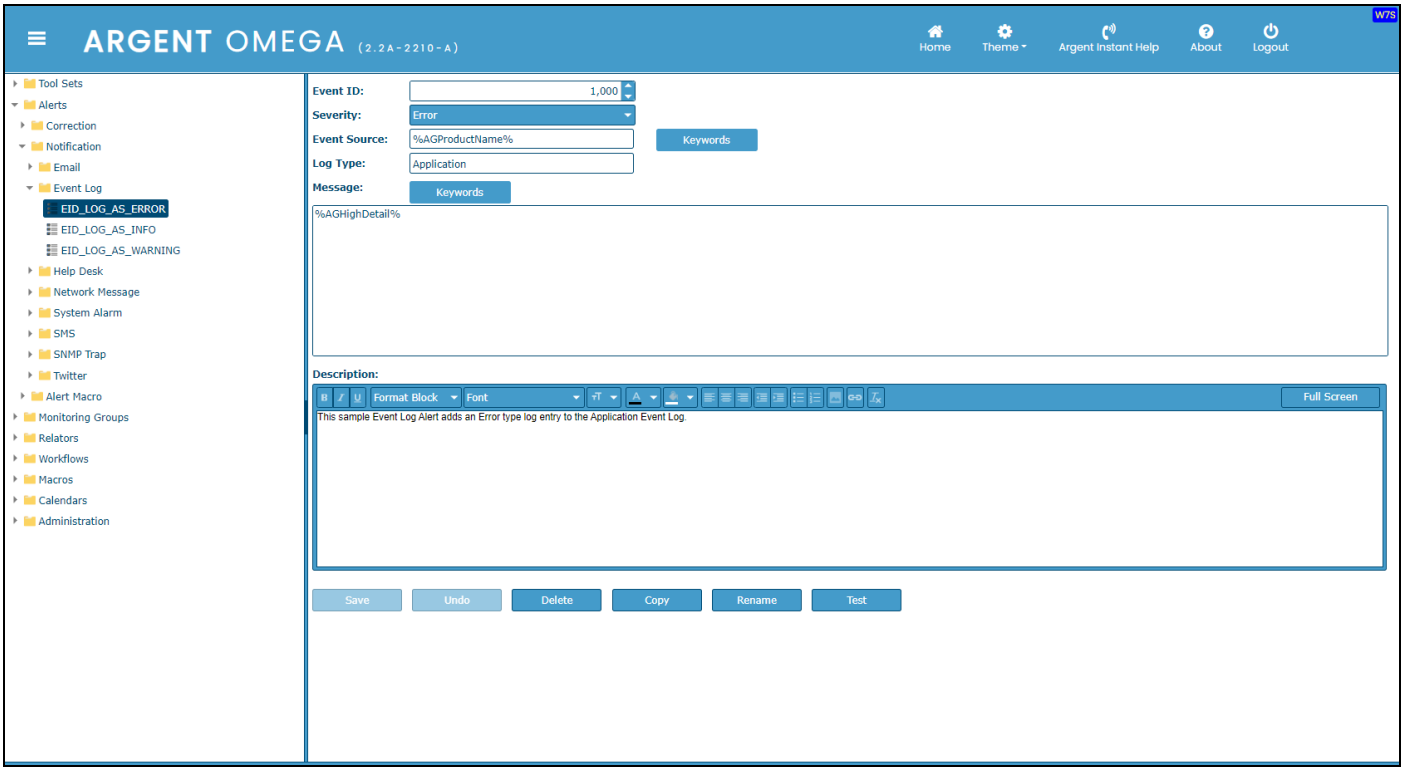
Built-in "**Keywords**" can also be used in any of the fields to customize your Alert – see Argent KBI

Https://Help.Argent.com/#KBI_312002

Proprietary Information – All Rights Reserved

- **Event Log**

  This Alert allows you to create a custom Event Log with the specified type and source.

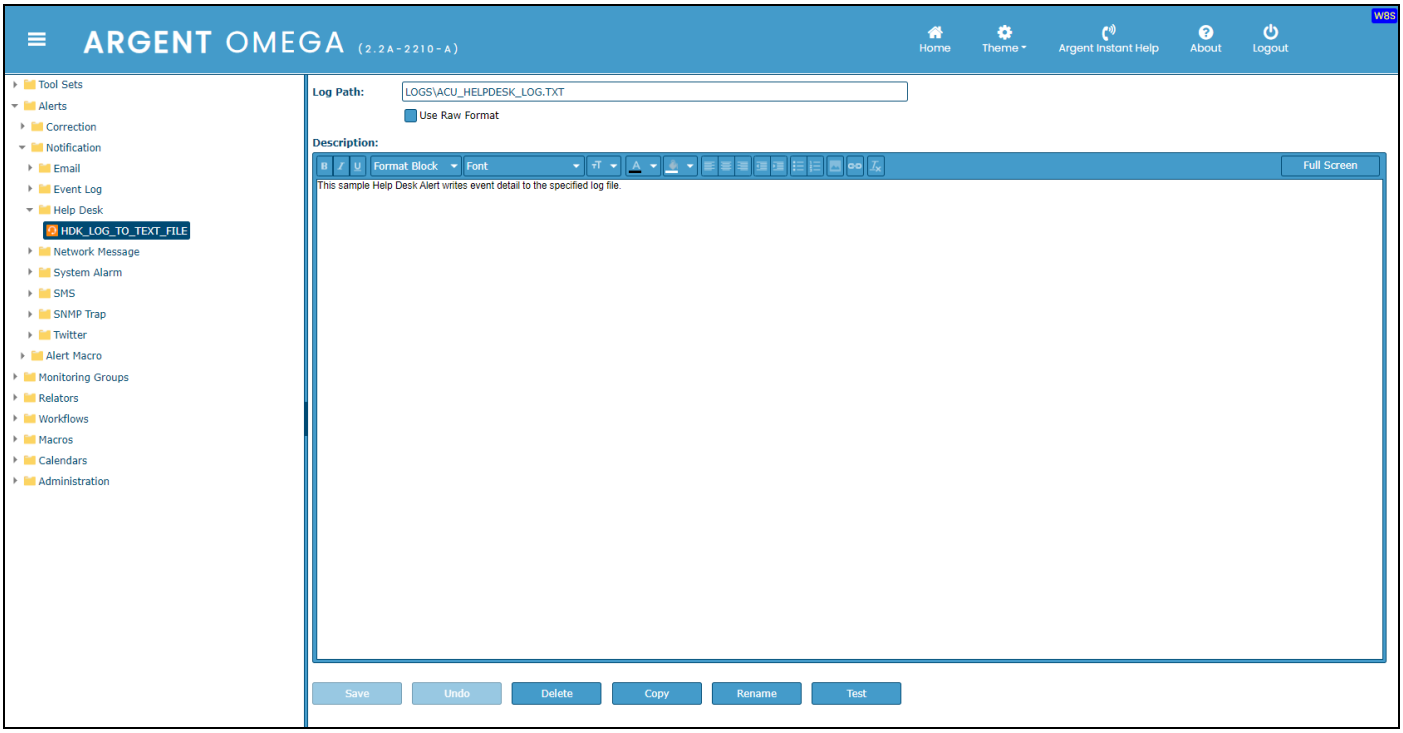


Built-in “**Keywords”** can also be used in any of the fields to customize your Alert, see Argent KBI

Https://Help.Argent.com/#KBI_312002

- **Help Desk**

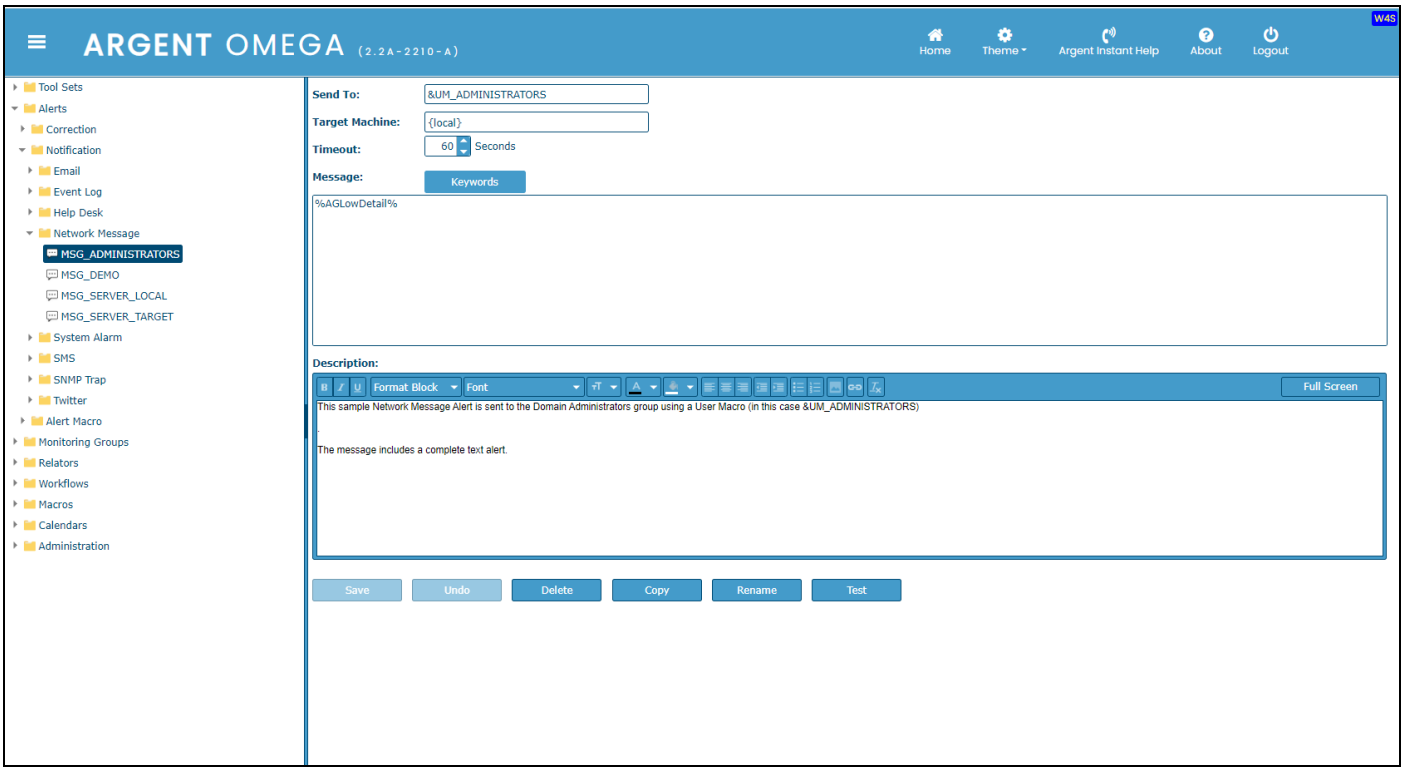
  This Alert allows you to forward Alerts to any third-party help desk facility.



Proprietary Information – All Rights Reserved

- **Network Message**

  This Alert allows you to send a network message (using the Messenger service) to a specific account, account group, or an entire domain.



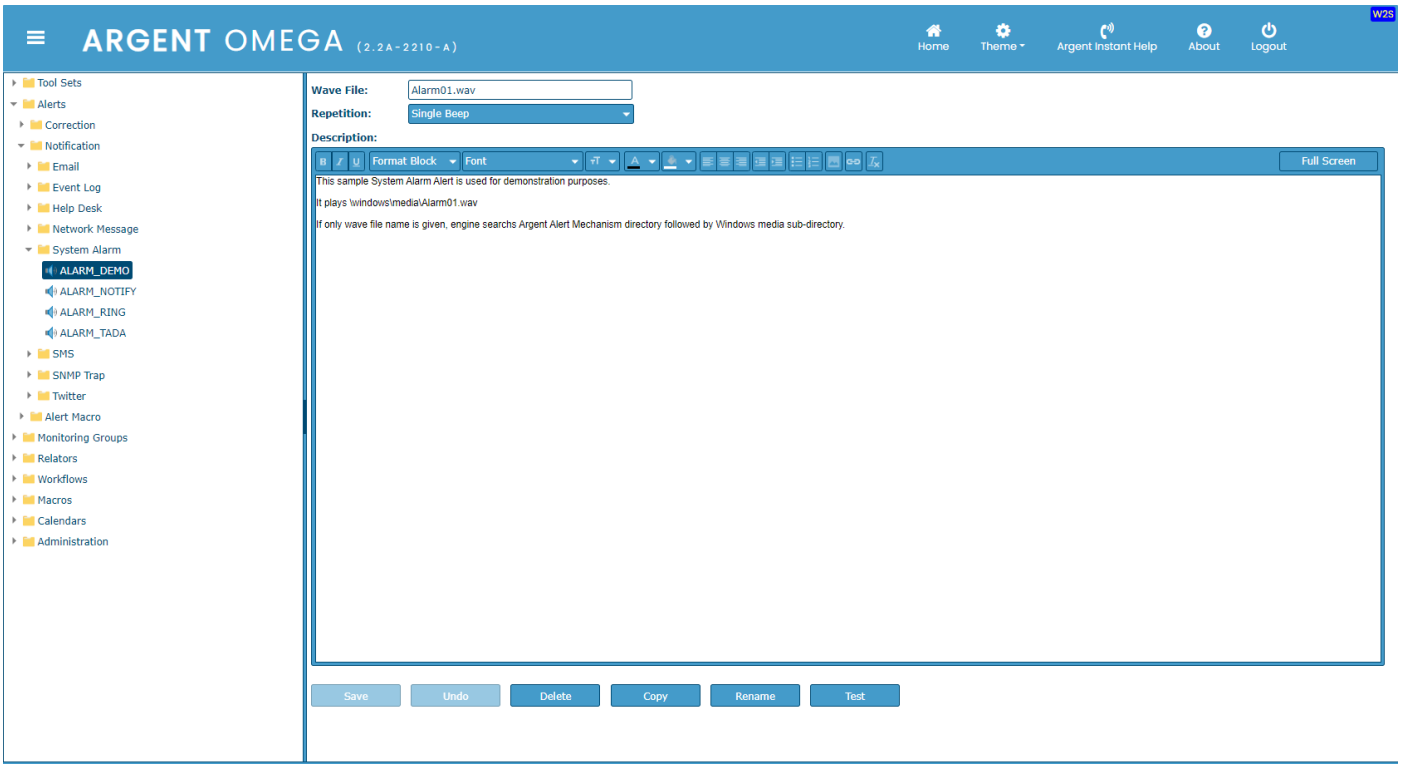
Built-in "**Keywords"** can also be used in any of the fields to customize your Alert, see Argent KBI

Https://Help.Argent.com/#KBI_312002

Proprietary Information – All Rights Reserved

- **System Alarm**

  This Alert causes the Argent Omega server to emit a customized alarm (beep) originating from the machine's speaker.

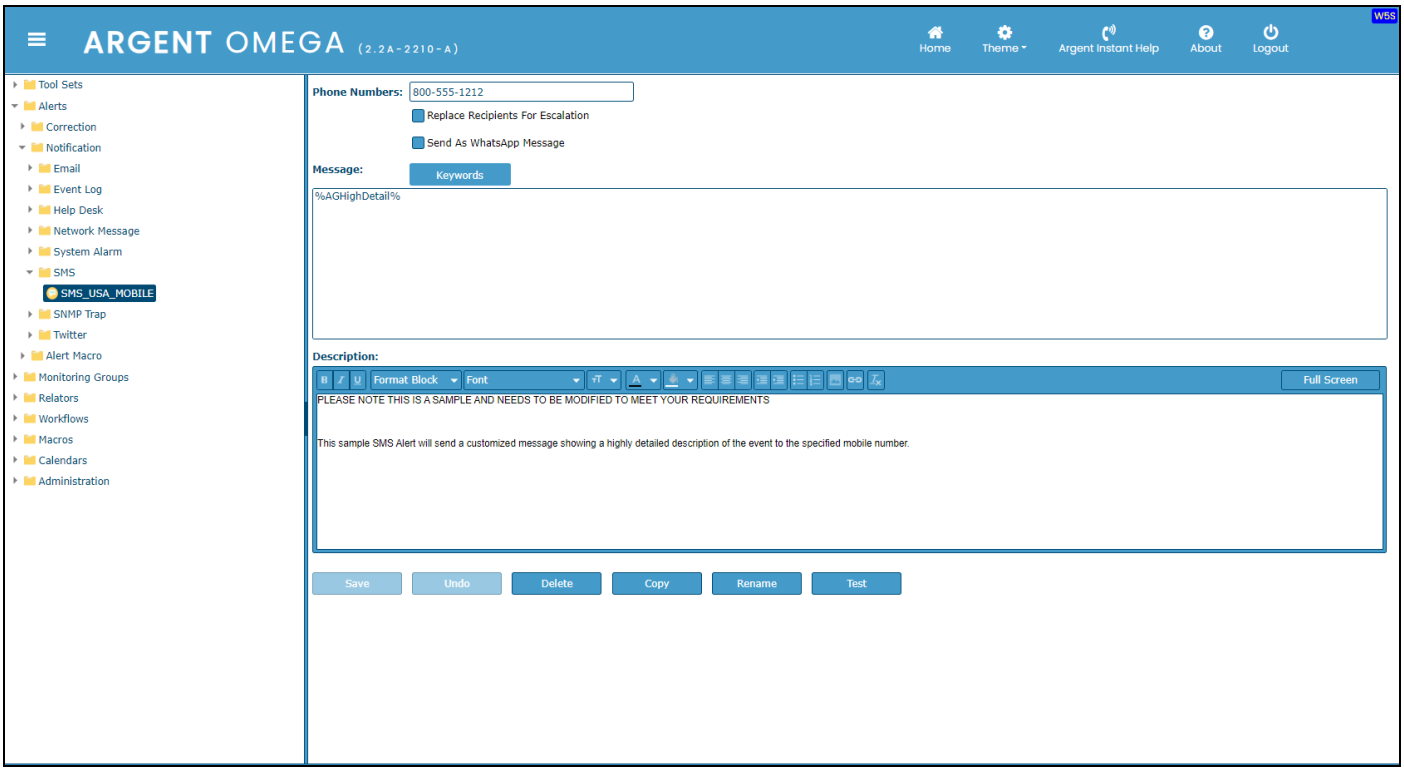


This Alert is typically used for local testing, and in most cases, is not a good choice for production use.

Proprietary Information – All Rights Reserved

- **SMS**

  This Alert allows you to send an SMS message to a specified cell phone number.

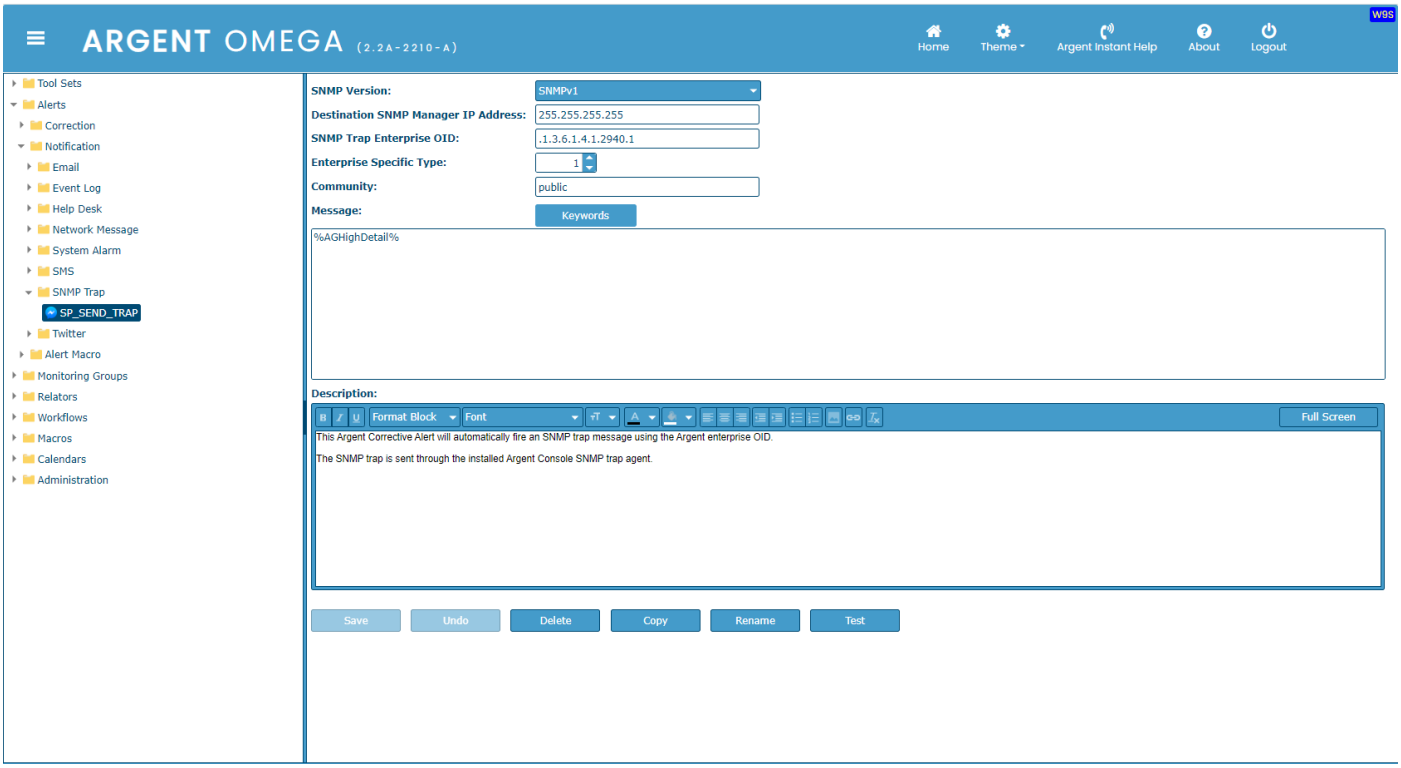


An SMS modem and service provider is required to send the SMS message. The configuration for the SMS modem is set in the Administration area.

Proprietary Information – All Rights Reserved

- **SNMP Trap**

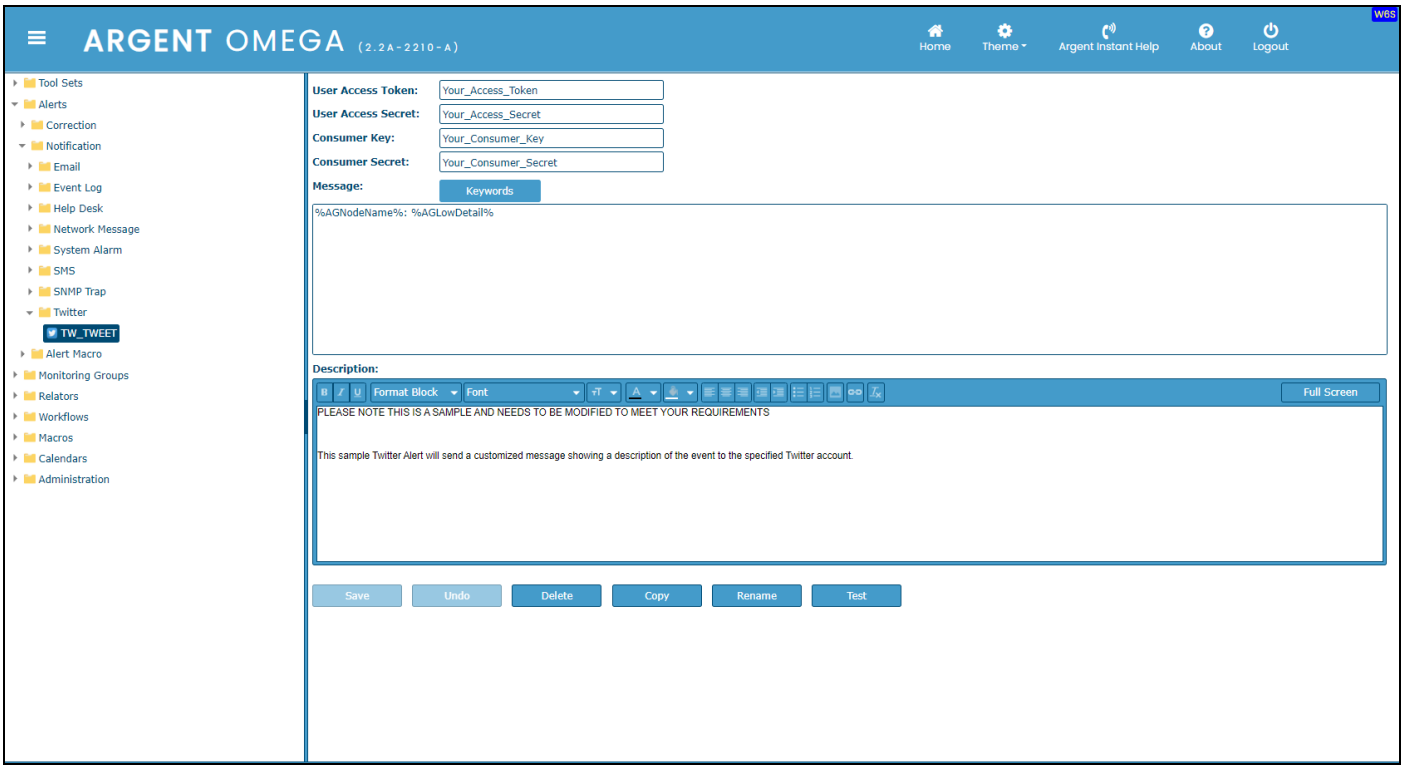
  This Argent Corrective Alert will automatically fire an SNMP trap message using the Argent Enterprise OID. The SNMP trap is sent through the installed Argent Console SNMP trap agent.



Proprietary Information – All Rights Reserved

- **Twitter**

  This Twitter Alert will send a customized message showing a description of the Event to the specified Twitter account.



Proprietary Information – All Rights Reserved

Calendars

Calendars provide maximum flexibility and customization while creating a schedule. The schedules can be defined to run the **Rule** on any desired day. For example, the last working day of a quarter.

The Calendar consists of two parts:

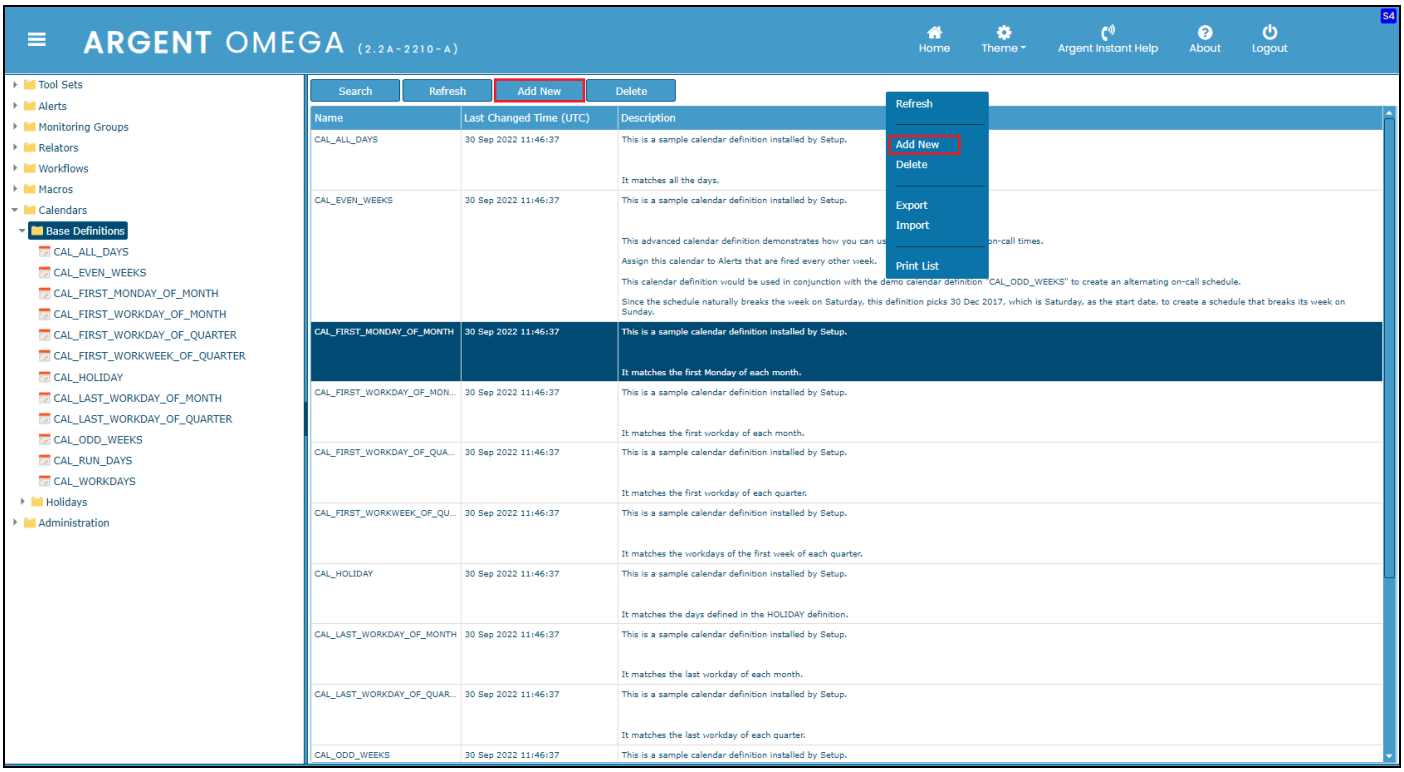
- **Base Definitions**
- **Holidays**

The known **Holidays** of a year can be defined in advance and the Base definition can be configured to consider the Holidays so that the schedule does not fall on a holiday.

The **Base Definition** has 12 predefined Calendar definitions to ease the creation of schedules. All these definitions can be customized further, or new ones created.

Add New available as a button on top of the list screen of the Base Definitions and as a right-click menu item can be used to create new Calendar definitions.

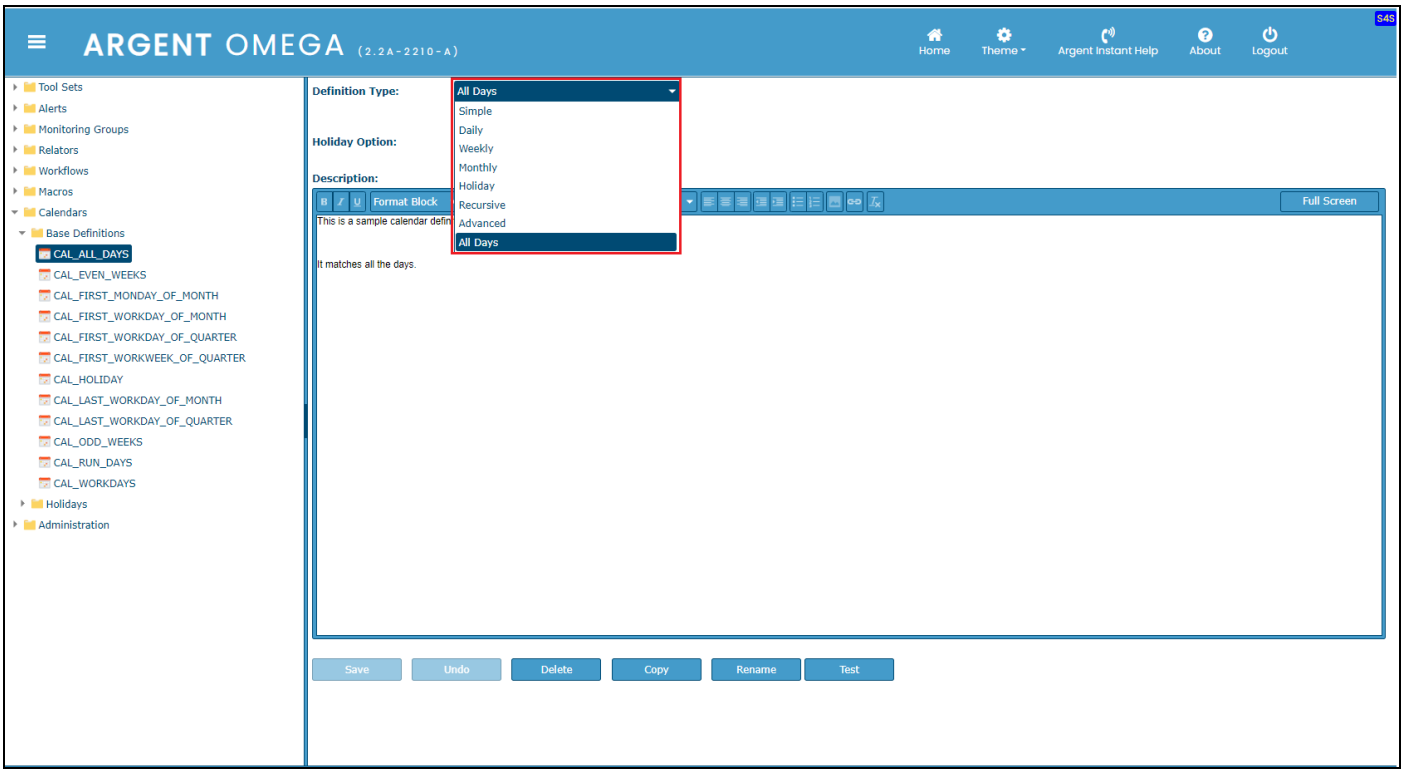
The name of the new Calendar definition can be specified in the pop-up sub-window:



Proprietary Information – All Rights Reserved

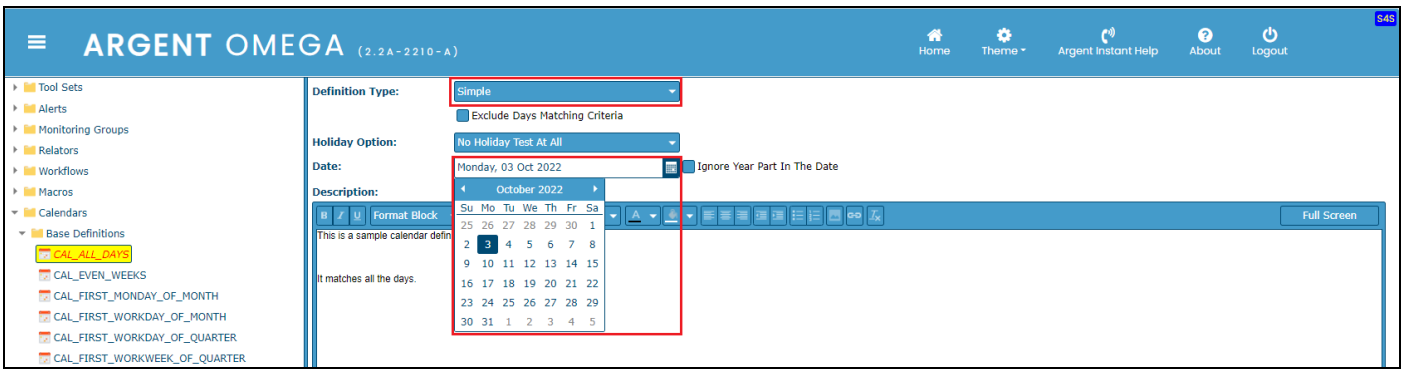
For ease of creating the Calendars and increasing flexibility, eight different types of calendar definition are available in the Base Definitions. They are:

- Simple
- Daily
- Weekly
- Monthly
- Holiday
- Recursive
- Advanced
- All Days



Simple

A Simple definition type can be used to create a schedule for any particular date of a year.

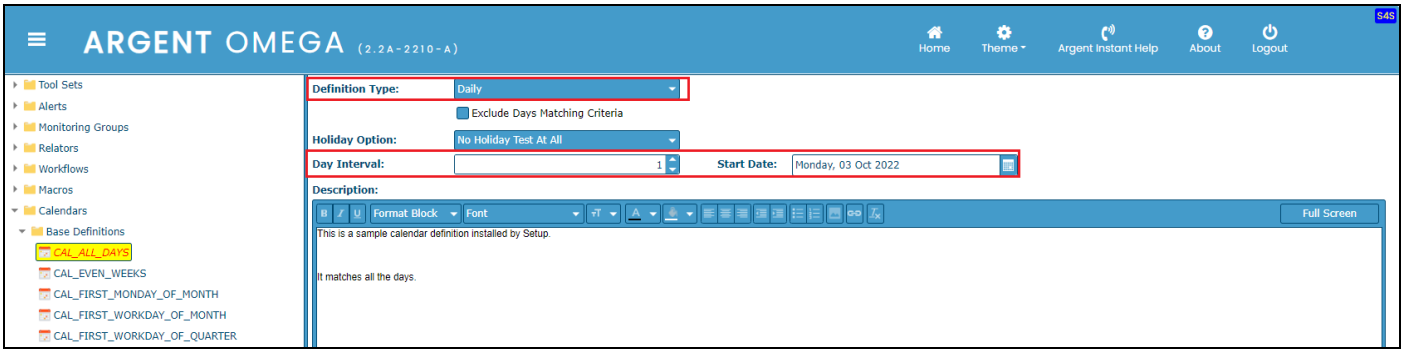


Proprietary Information – All Rights Reserved

The **“Ignore Year Part in the Date”** option, when checked, will ensure the schedule is valid across all future years.

Daily

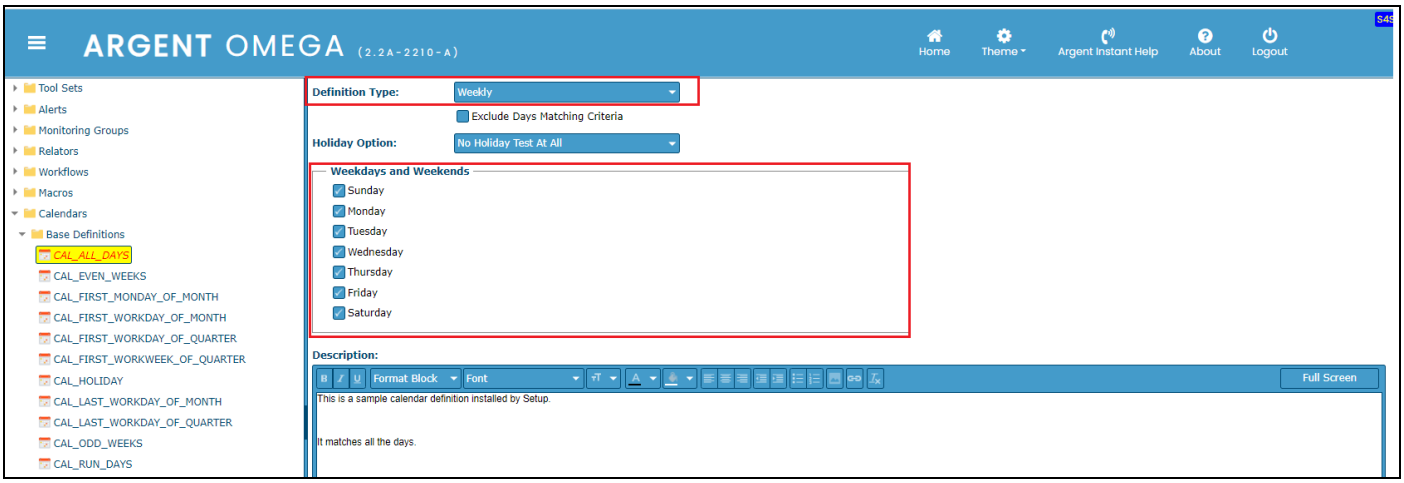
The Daily definition type can be used to create a schedule for repetitive tasks that should occur in an interval of days. The start date and the frequency in days can be specified.



In the above definition, the schedule starts on Wednesday, 01 June 2022 and occurs every day thereafter.

Weekly

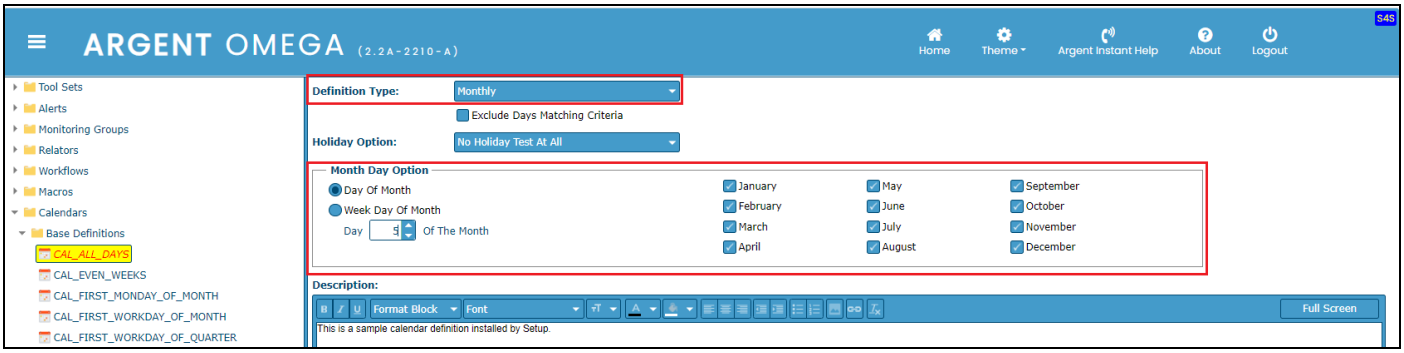
The Weekly definition type can be used to create a schedule for tasks that should occur on a particular day of a week.



In the above screenshot, scheduled task is configured to occur on all days of a week.

Monthly

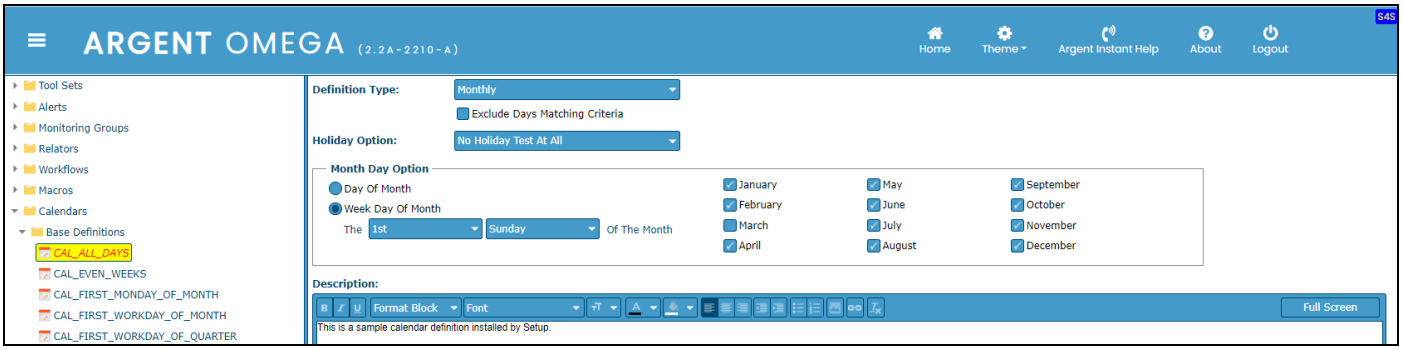
The Monthly definition type can be used to create a schedule for tasks that should occur on a particular day of a month or on a particular week of a month.



Proprietary Information – All Rights Reserved

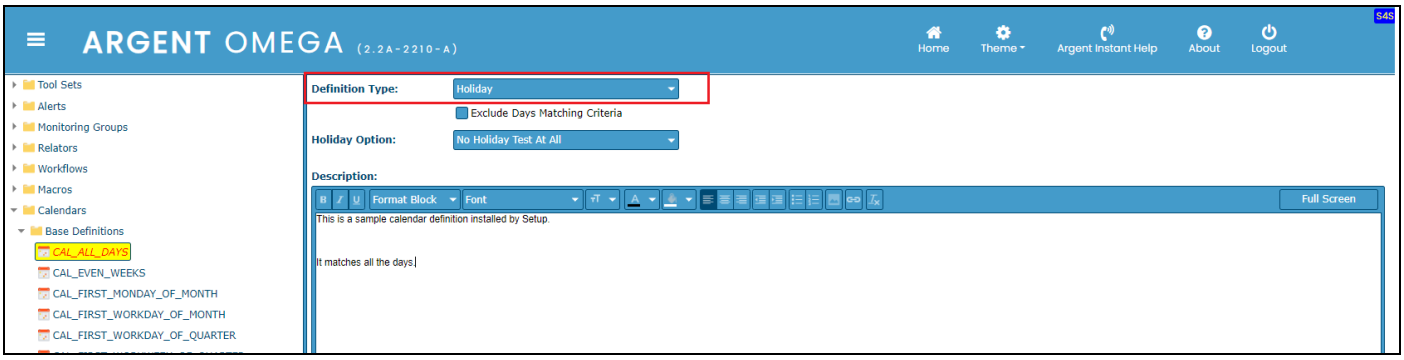
In the above screenshot, the schedule is set for 5th of every month.

In the below screenshot, the schedule is configured for the first Sunday of every month, excluding March.



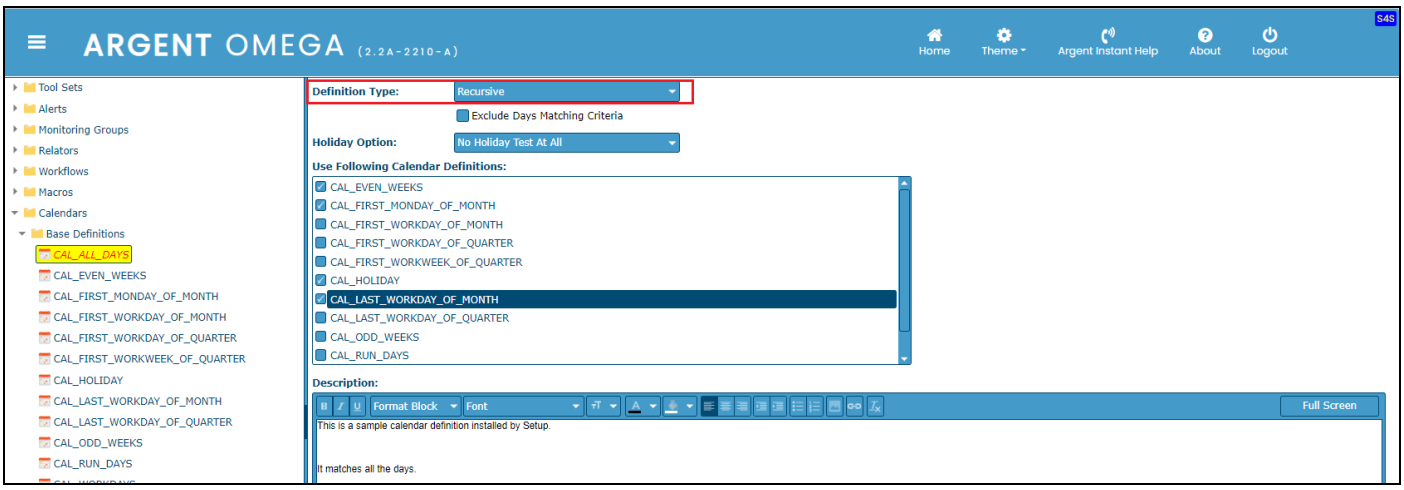
Holiday

The Holiday type definition can be used to create a schedule for a task to occur on defined Holidays.



Recursive

The Recursive type definition can be used to create a schedule that includes one or more of the previously defined schedules, with a depth limit of 10.

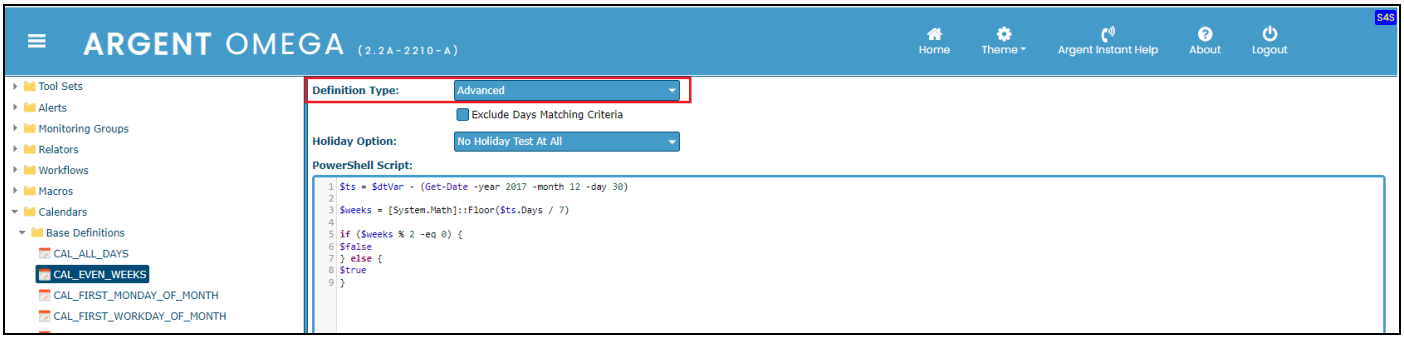


In the above screenshot, the schedule makes use of four other Calendar definitions defined earlier.

Proprietary Information – All Rights Reserved

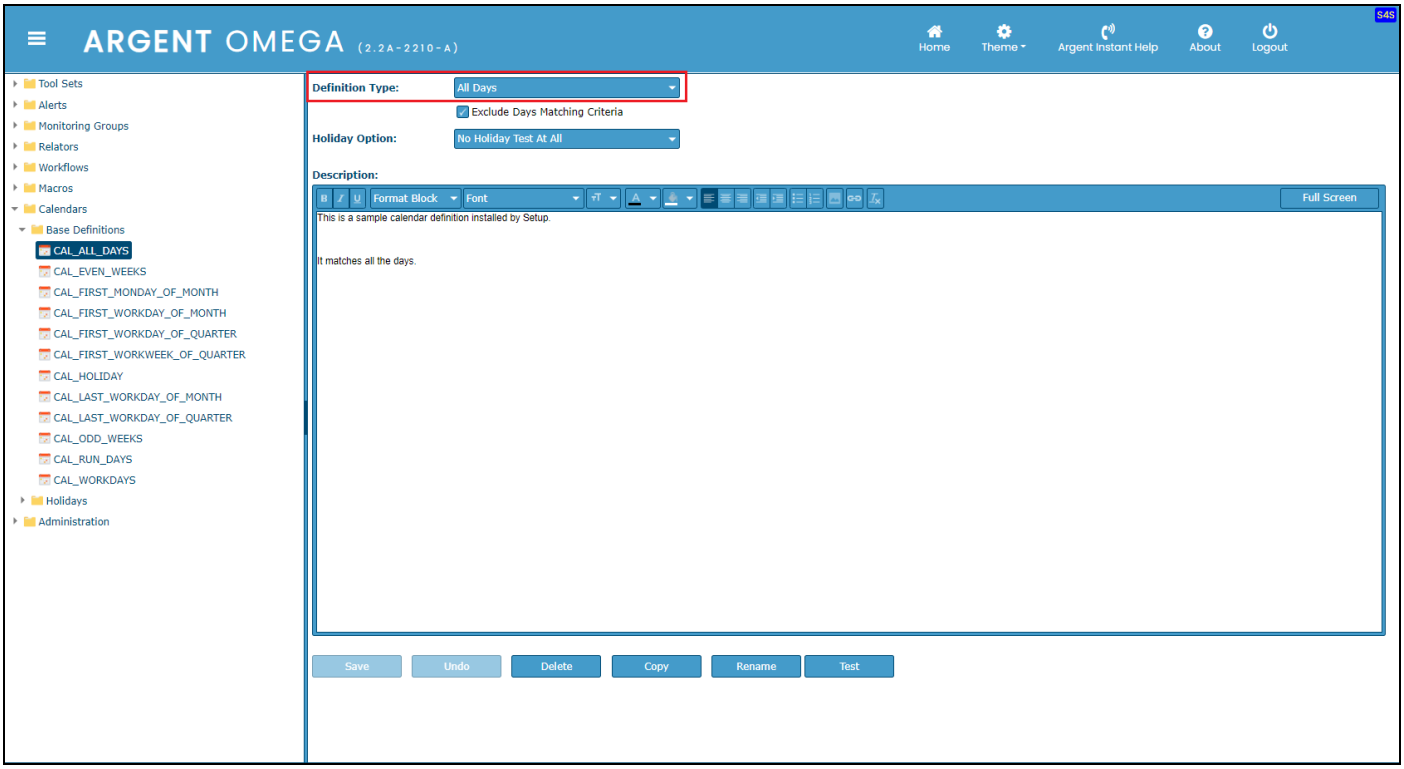
Advanced

The Advanced type definition can be used to create a schedule using PowerShell script.



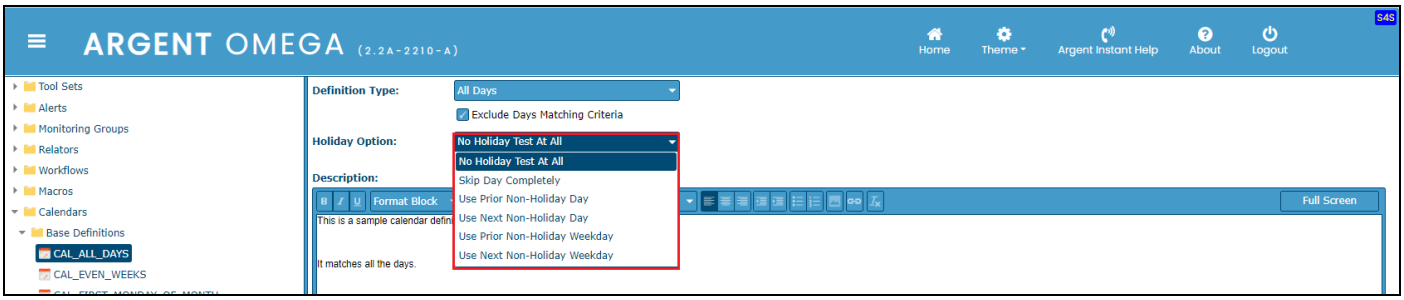
All Days

This type of definition can be used to create a schedule for all days.



Holiday Option

The Calendar definitions can automatically handle holiday definitions using the **“Holiday Option”** available in all types of definitions.

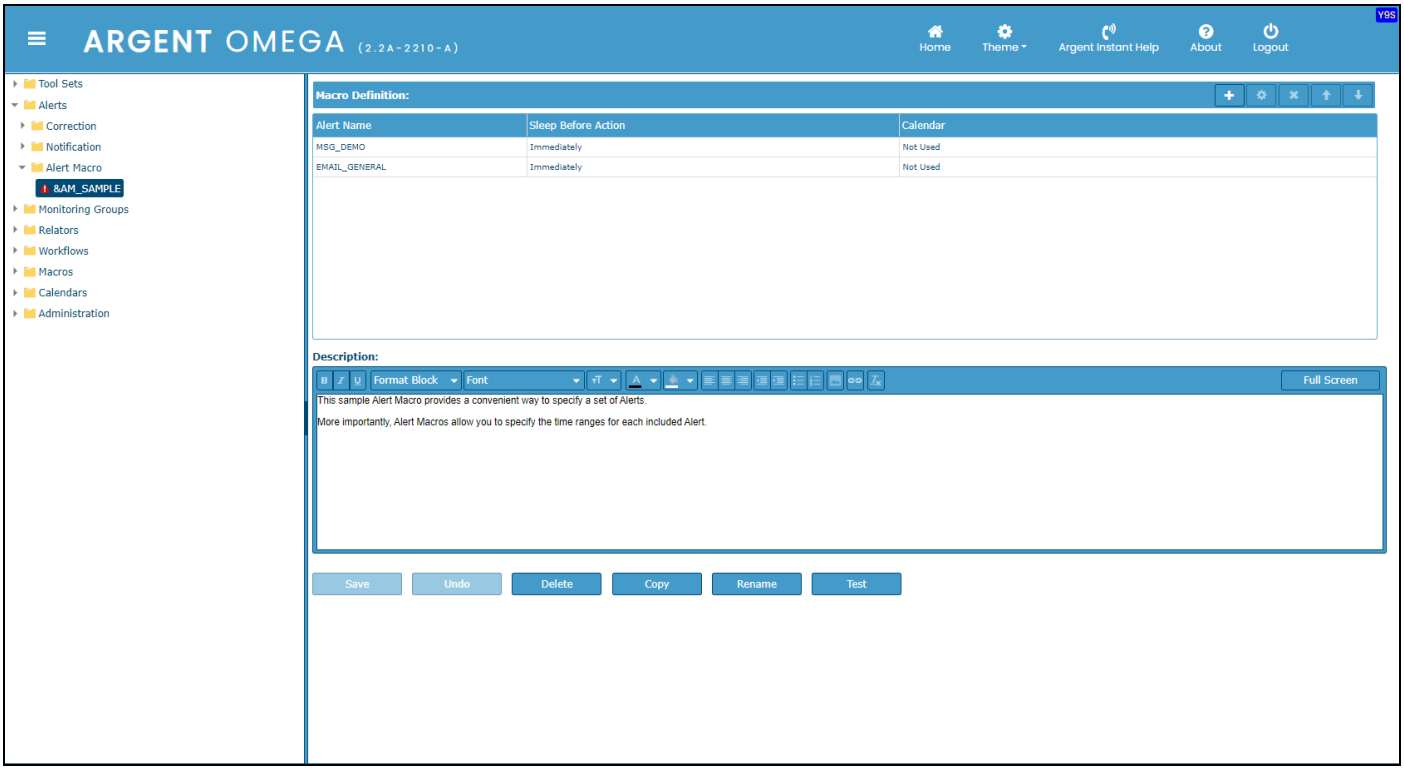


Macros

Macros are a collection of a particular item, such as email addresses (Email Macros) or login names (User Macros).

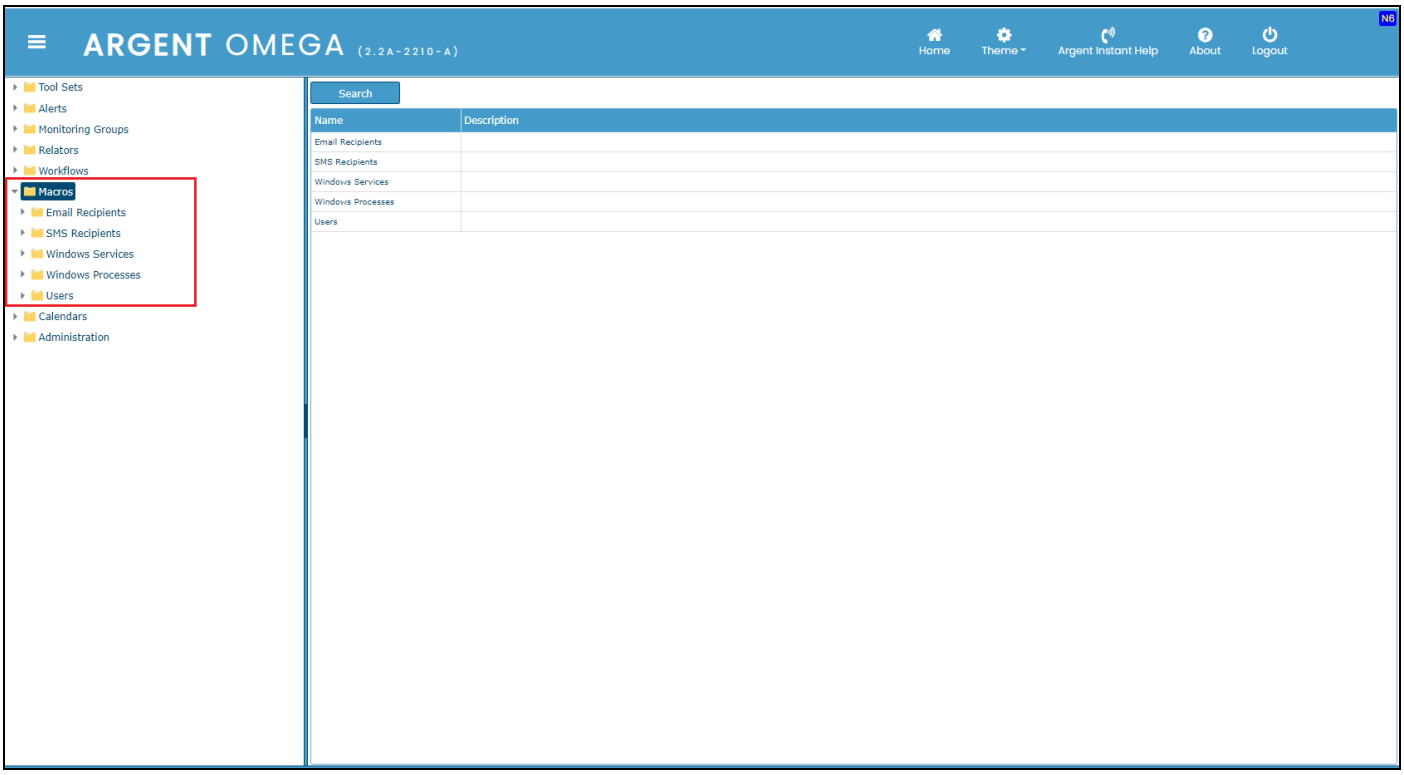
A macro enables you to define once, in one location, common information that can then be used on dozens or hundreds of other building blocks.

For example, a single email macro can be created that lists all the email addresses of people in the support team. Then, this Email Macro can be specified in dozens or hundreds of Relators; when a new person is added to the support team, then only a single change needs to be made to this single Email Macro.



Proprietary Information – All Rights Reserved

If a typical Alert procedure involves an SMS to the help desk team, a page to a group of engineers, and an email to the CIO, you can create a single Alert Macro and use this Alert process at multiple times.



Macros can be used in areas of the product that apply. For instance, you can use a single Email Macro containing 10 email addresses in any Email Alert. So, rather than defining 10 email addresses in the Email Alert definition, you define it once in an Email Macro under a convenient alias. The added benefit is it can be re-used for other Email Alert definitions as needed.

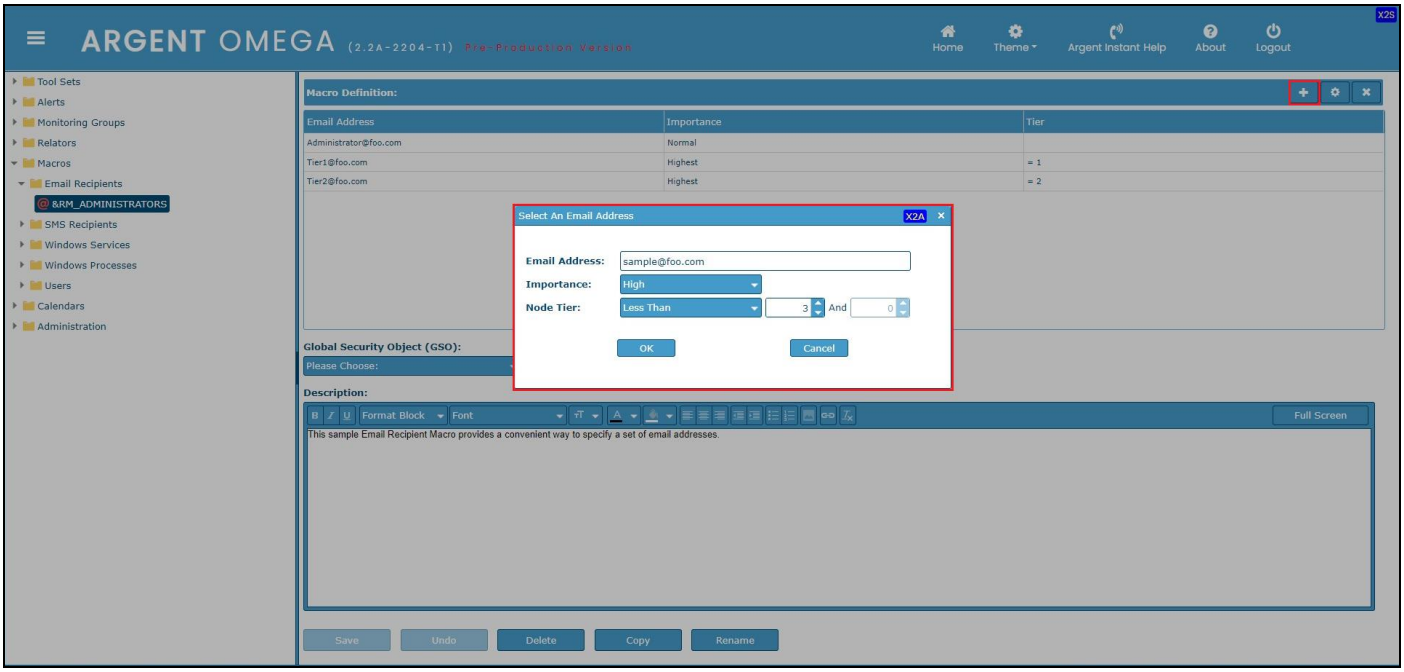
Proprietary Information – All Rights Reserved

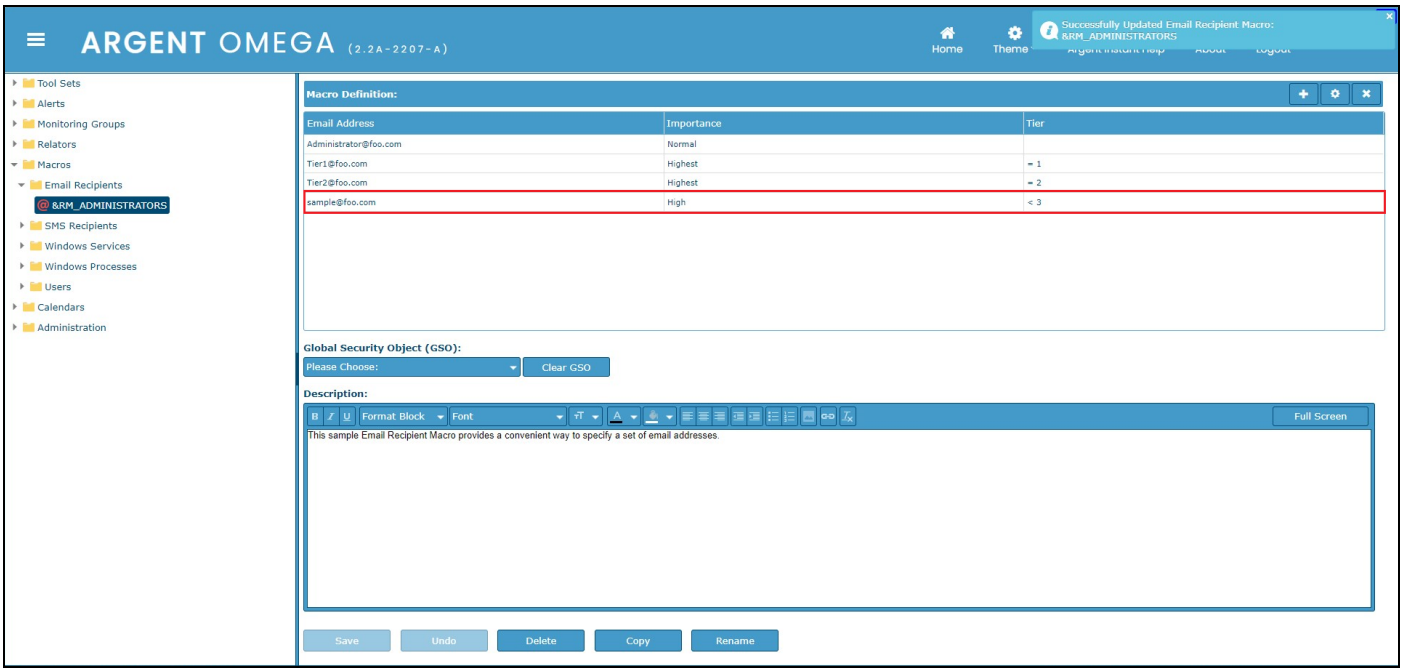
Email Recipient

This Macro provides a convenient way to specify a set of email addresses.

The specifications include the **Email Address**, **Importance,** and **Node Tier.**

The **Node Tier** property can used in Email Recipient Macros and SMS Recipient Macros to control which email addresses or mobile numbers should be used when an alert is fired for the specific node.





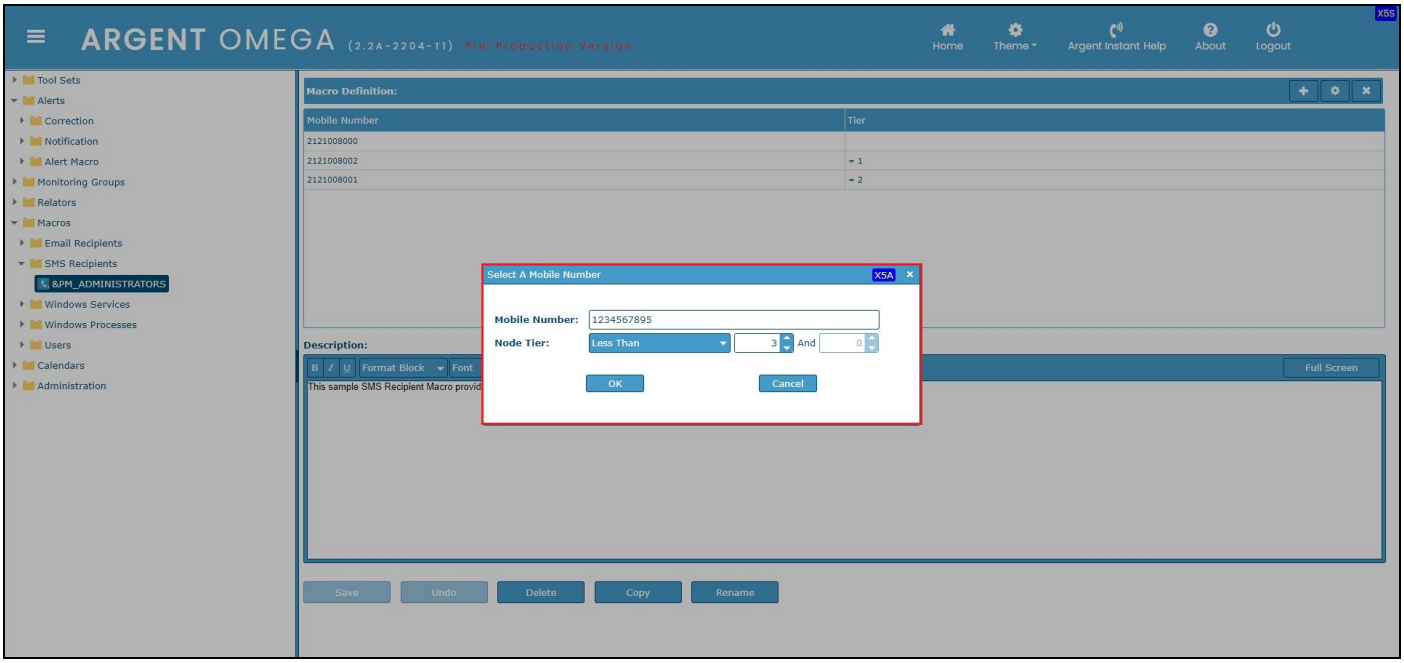
SMS Recipient

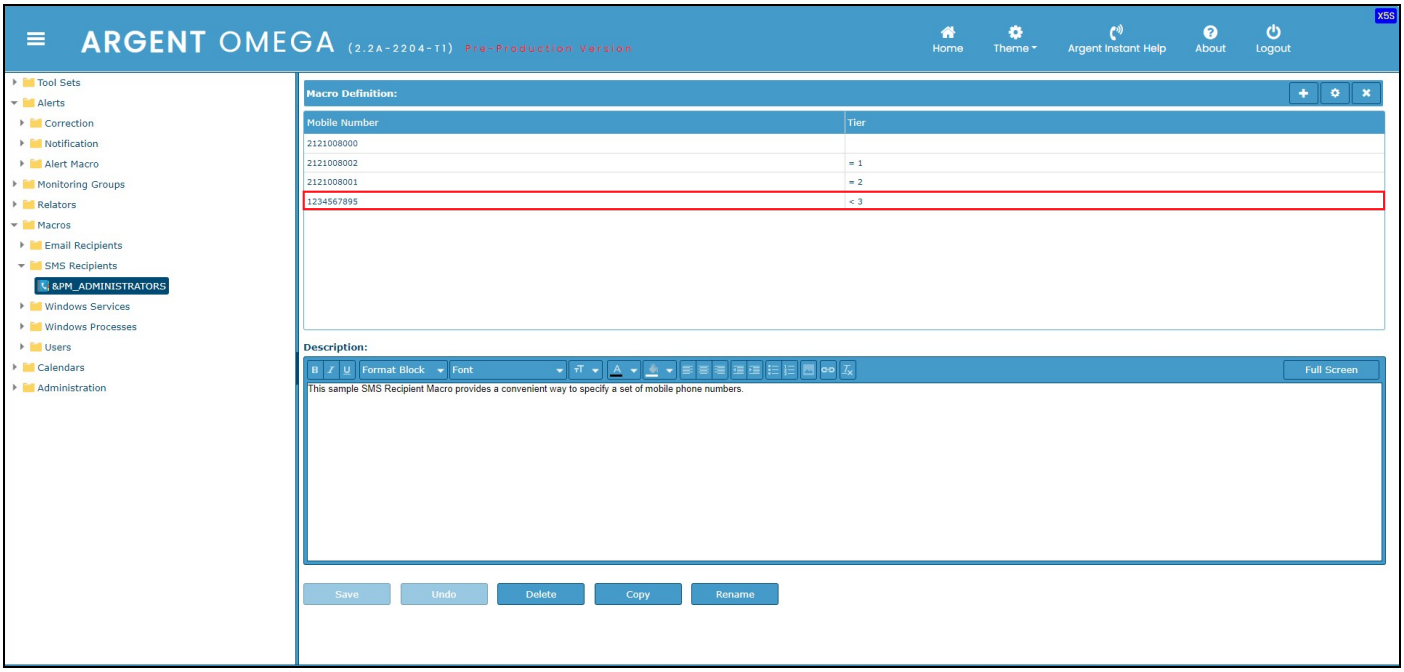
This sample SMS Recipient Macro provides a convenient way to specify a set of mobile phone numbers.

The user will enter the **Mobile Number** and **Node Tier.**

Proprietary Information – All Rights Reserved

The **Node Tier** property can be used in Email Recipient Macros and SMS Recipient Macros to control which email addresses or mobile numbers should be used when an alert is fired for the specific node.

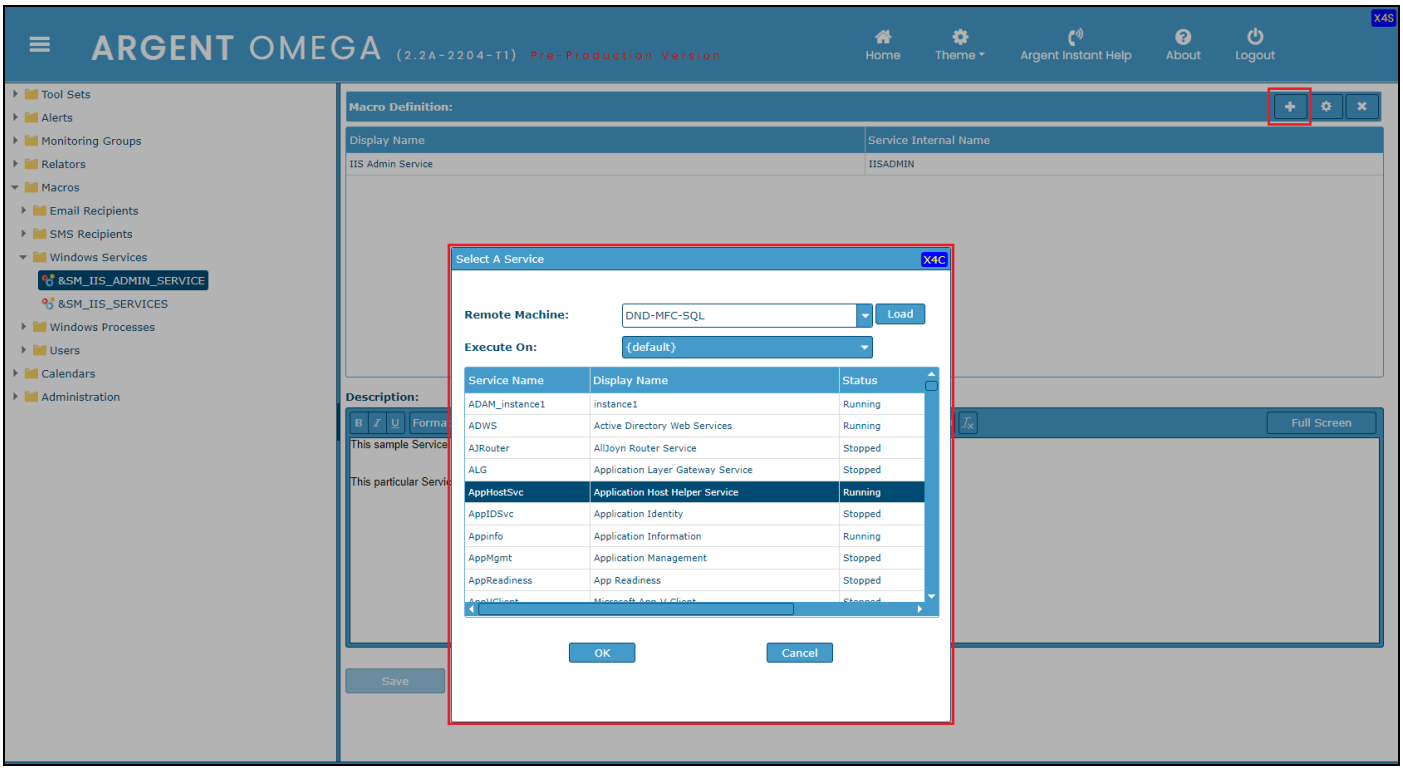


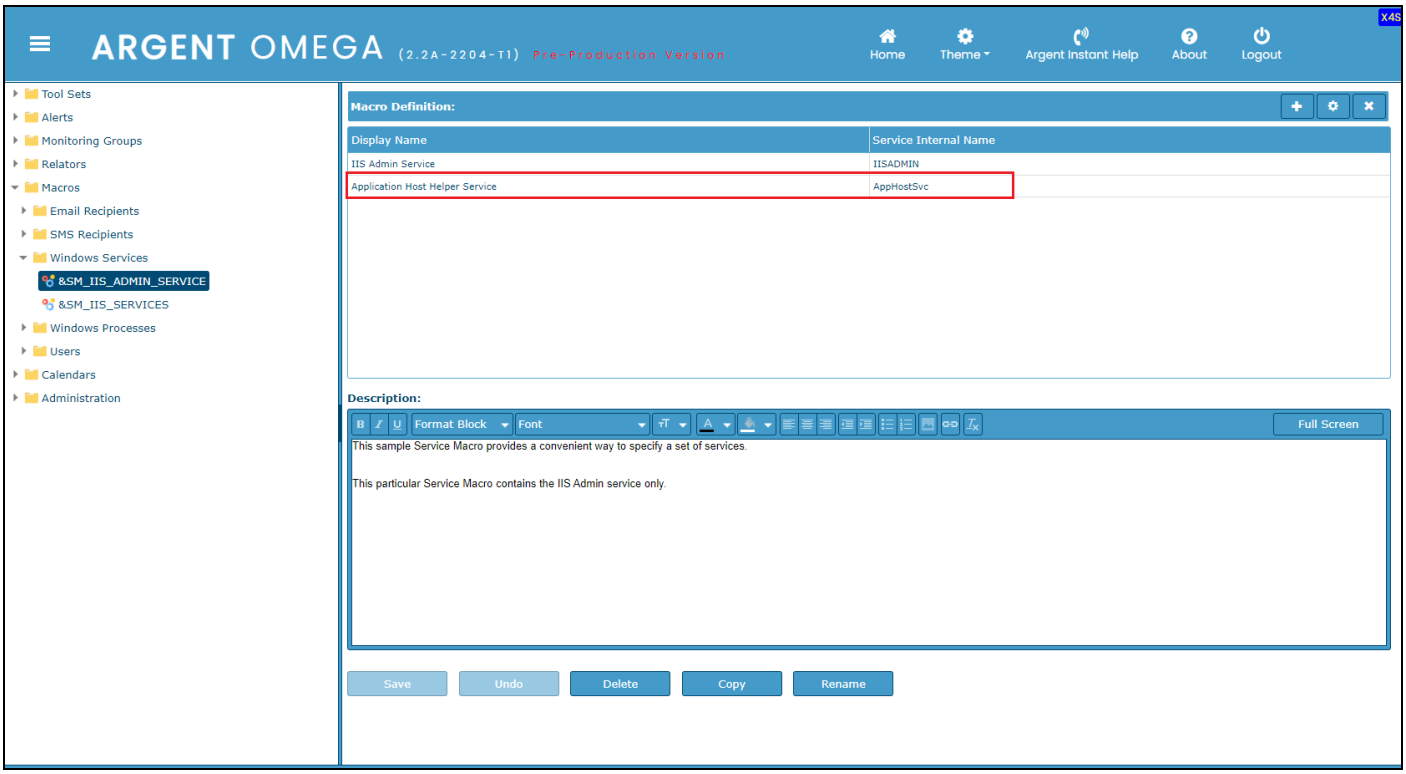


Proprietary Information – All Rights Reserved

Windows Services

This Macro provides a convenient way to specify a set of Windows services.

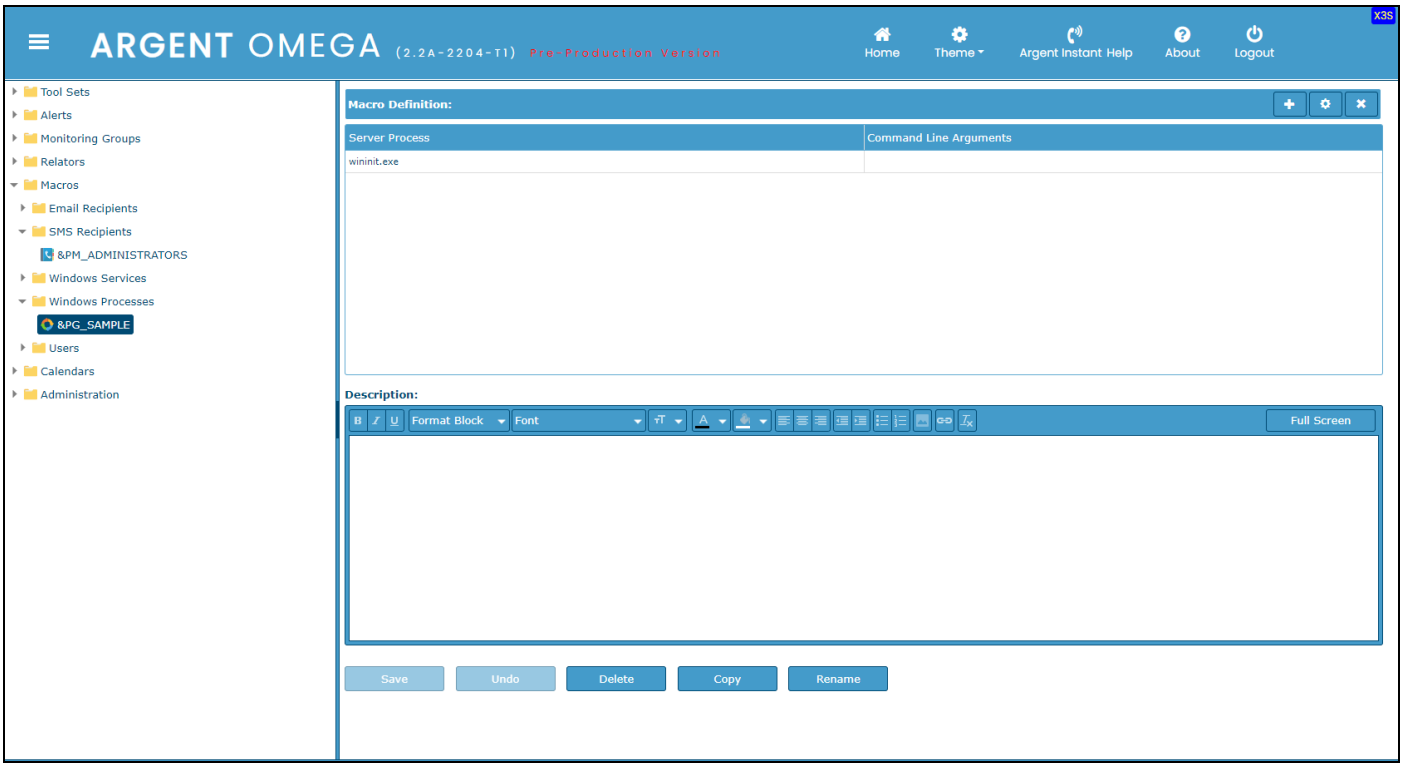




Proprietary Information – All Rights Reserved

Windows Processes

This Macro provides a convenient way to specify a set of Windows processes.



Proprietary Information – All Rights Reserved

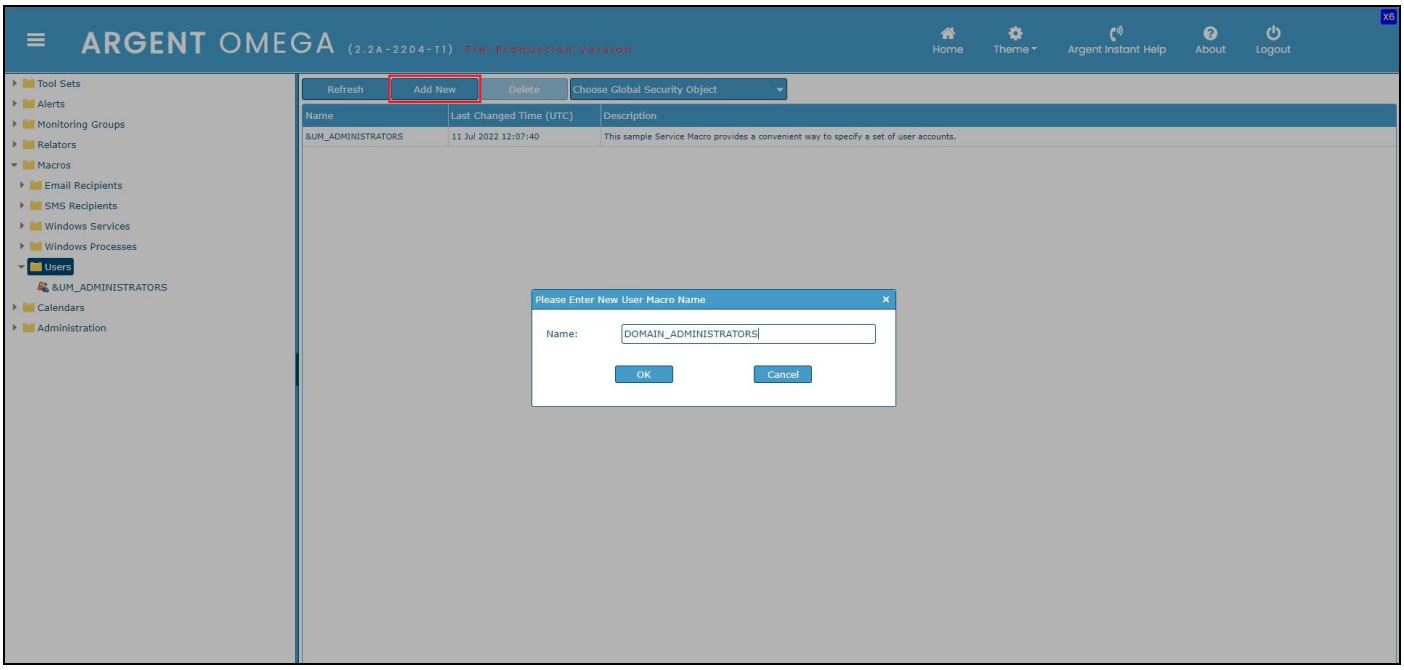
Users

User Macros are a collection of user accounts.

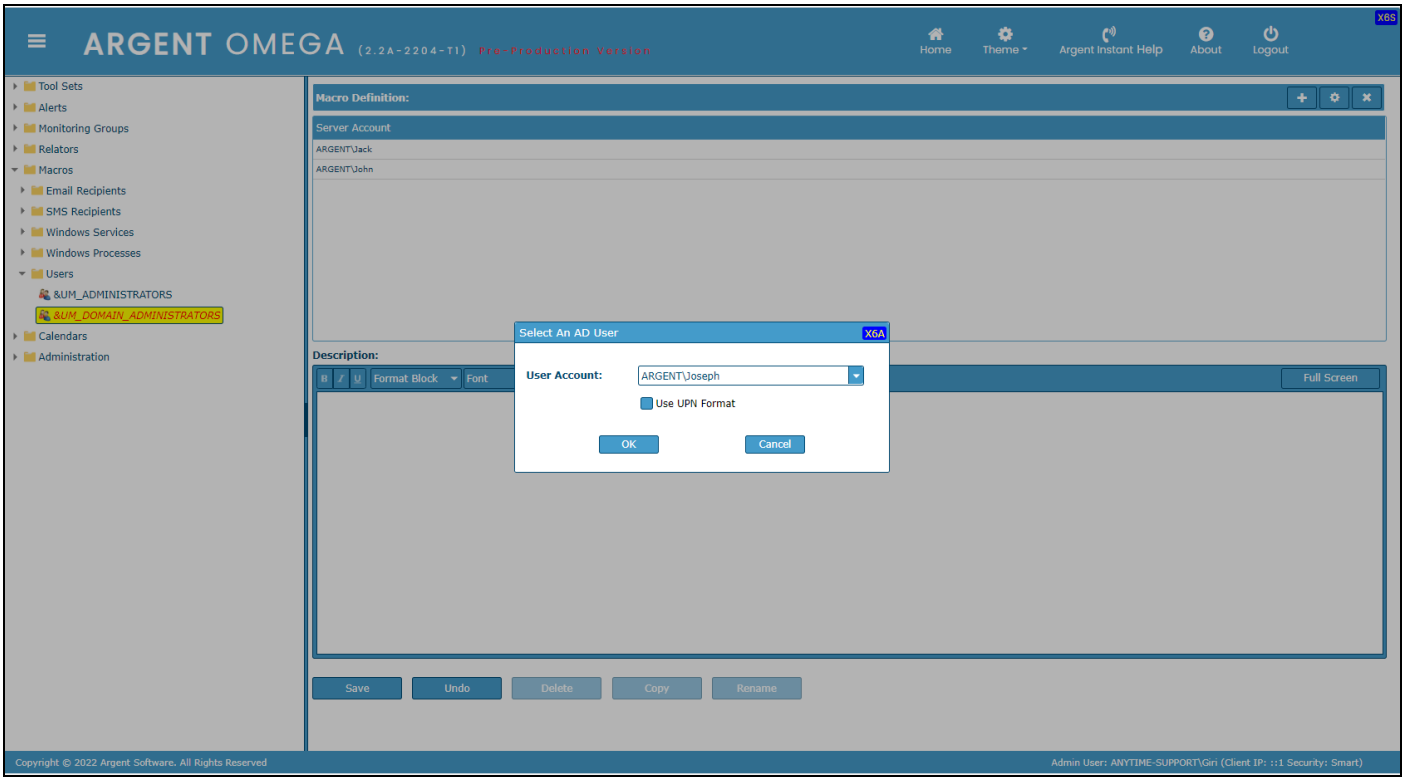
For example, you can use a single User Macro containing 10 user accounts in any Network Message Alert.

So rather than defining 10 user accounts in the Network Message Alert definition, you define it once in a User Macro under a convenient alias. The added benefit is it can be re-used for other Alert definitions as needed.

To define a User Macro, navigate to **Macros or Users** and click **Add New.**

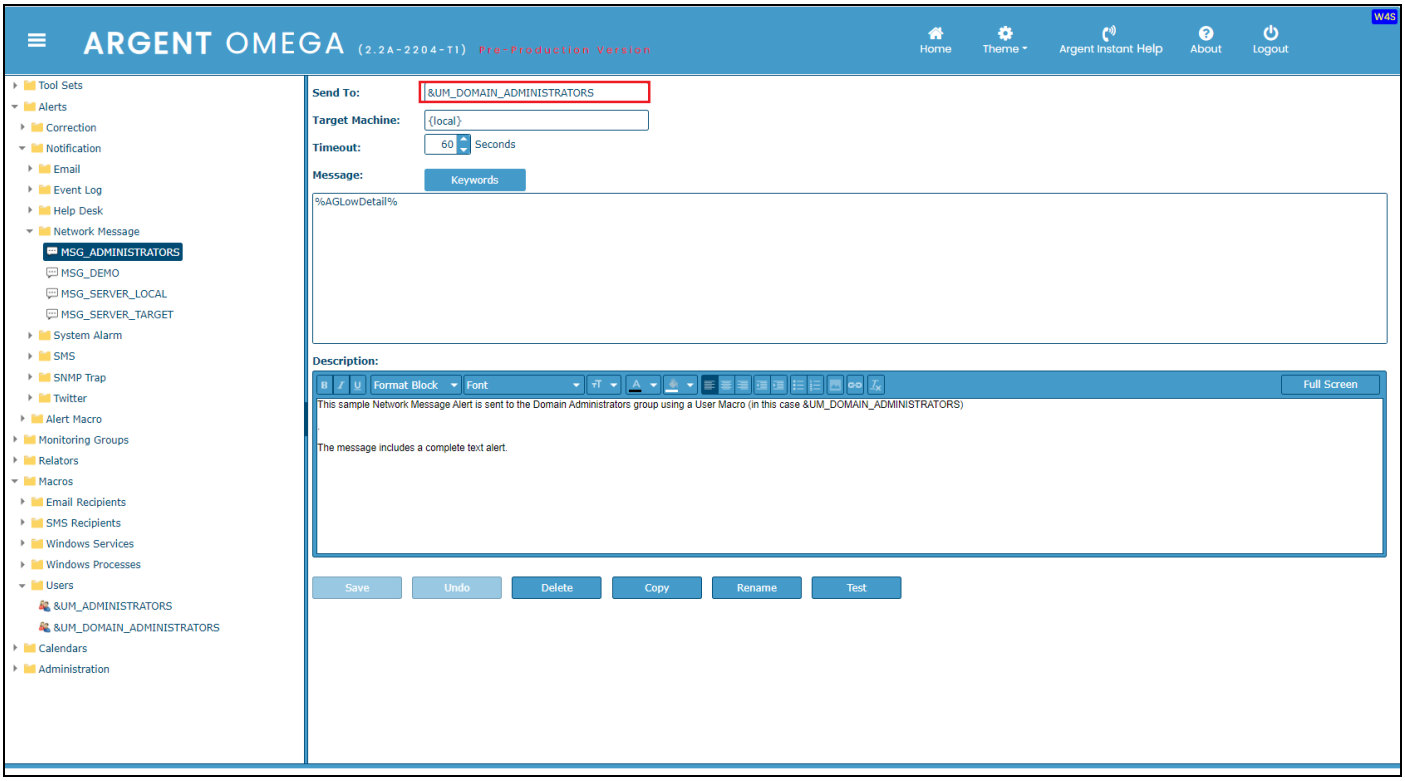


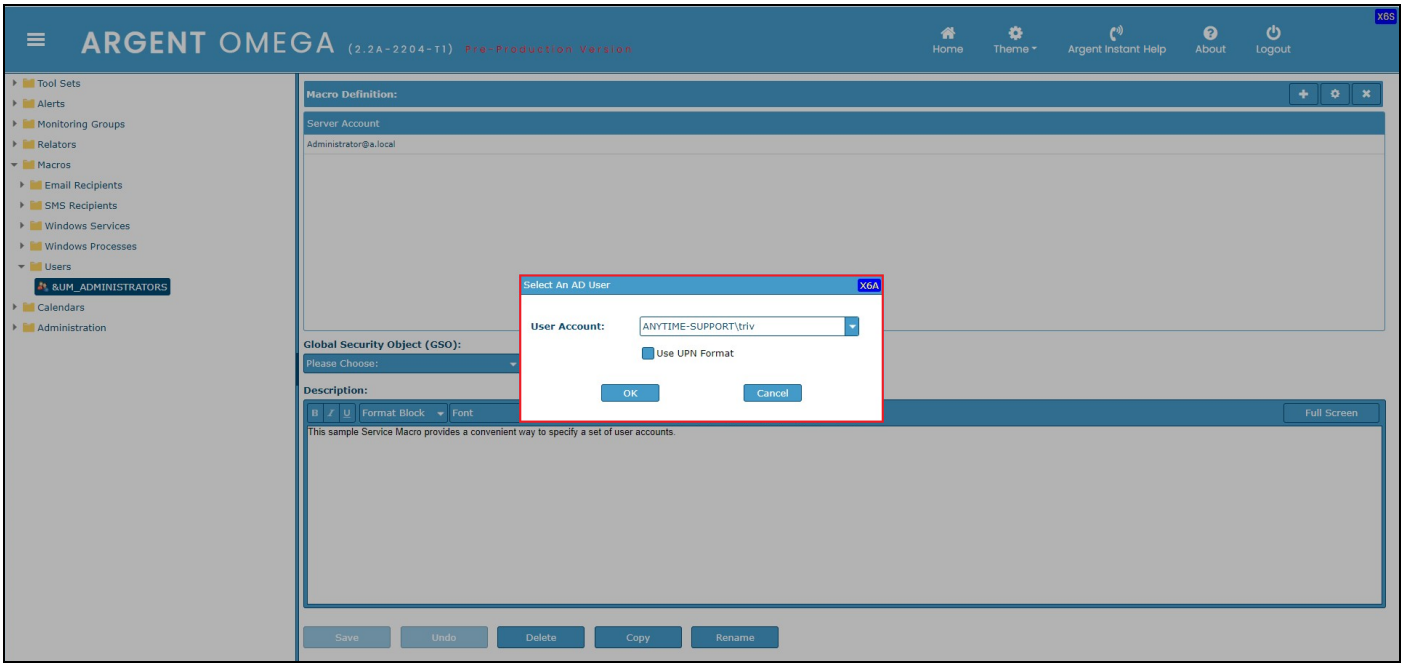
Then define user accounts in the new User Macro.



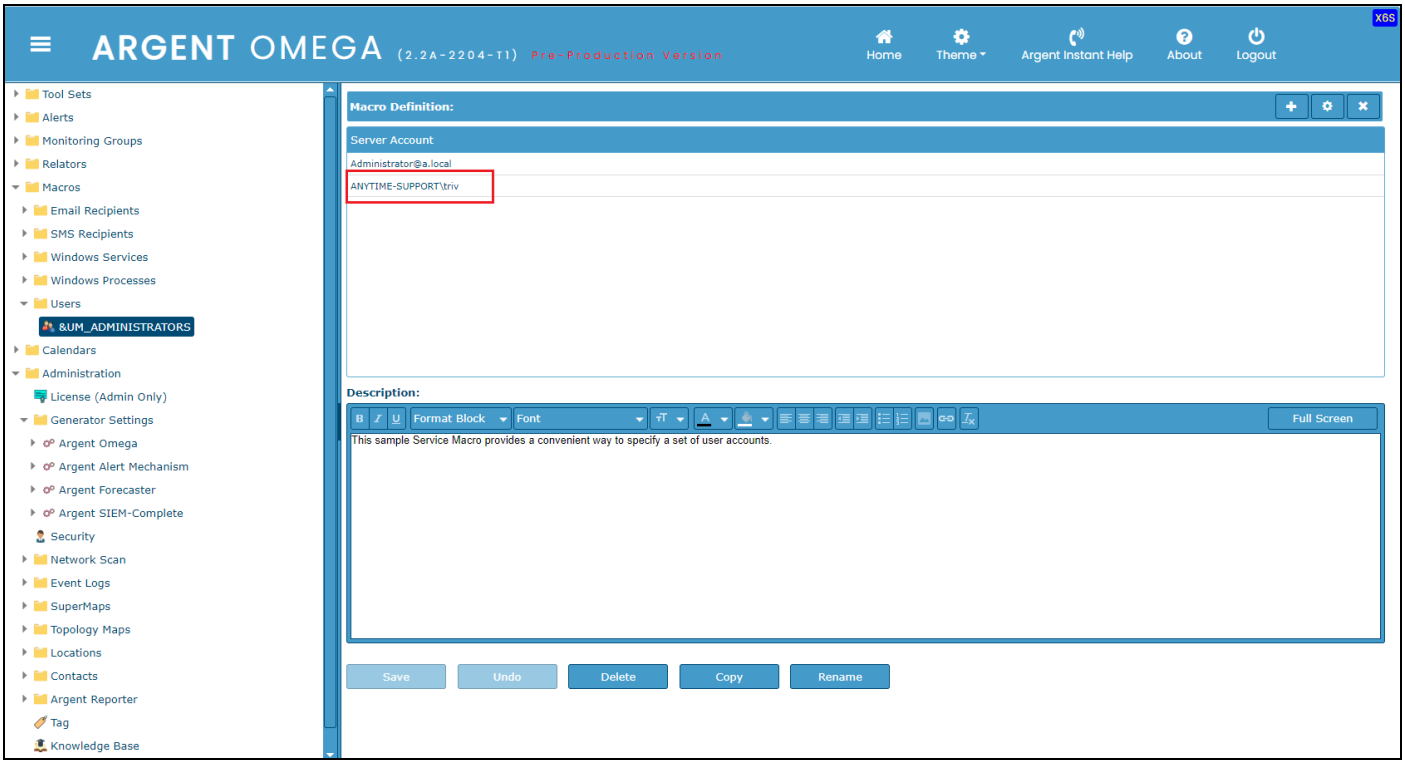
Then configure the User Macro in required Alerts. For example, to configure User Macro in Network Message Alert, navigate to Alerts\Notification\Network Message\MSG_ADMINISTRATORS as shown below.

The specified message will be sent to the Domain Administrators accounts defined in User Macro UM_ DOMAIN_ADMINISTRATORS.





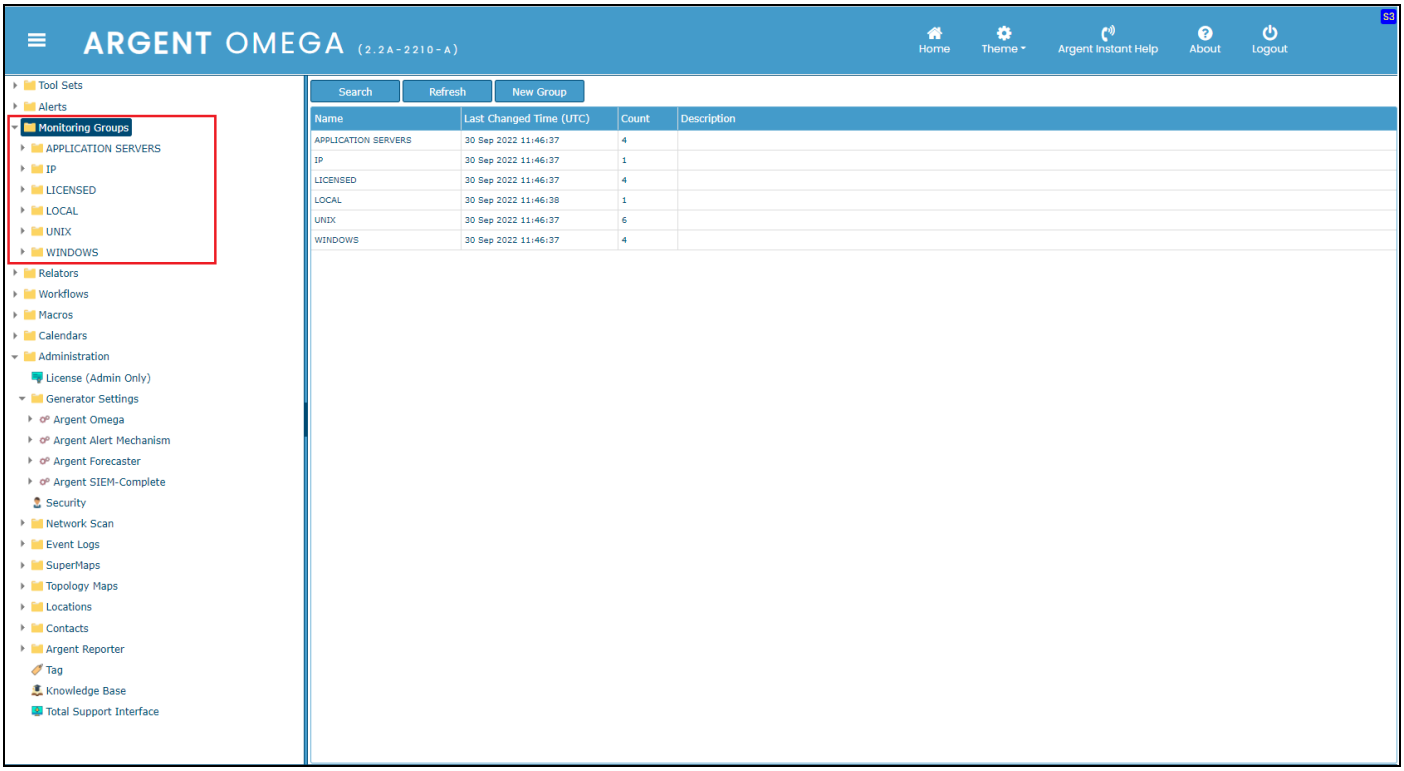
Proprietary Information – All Rights Reserved



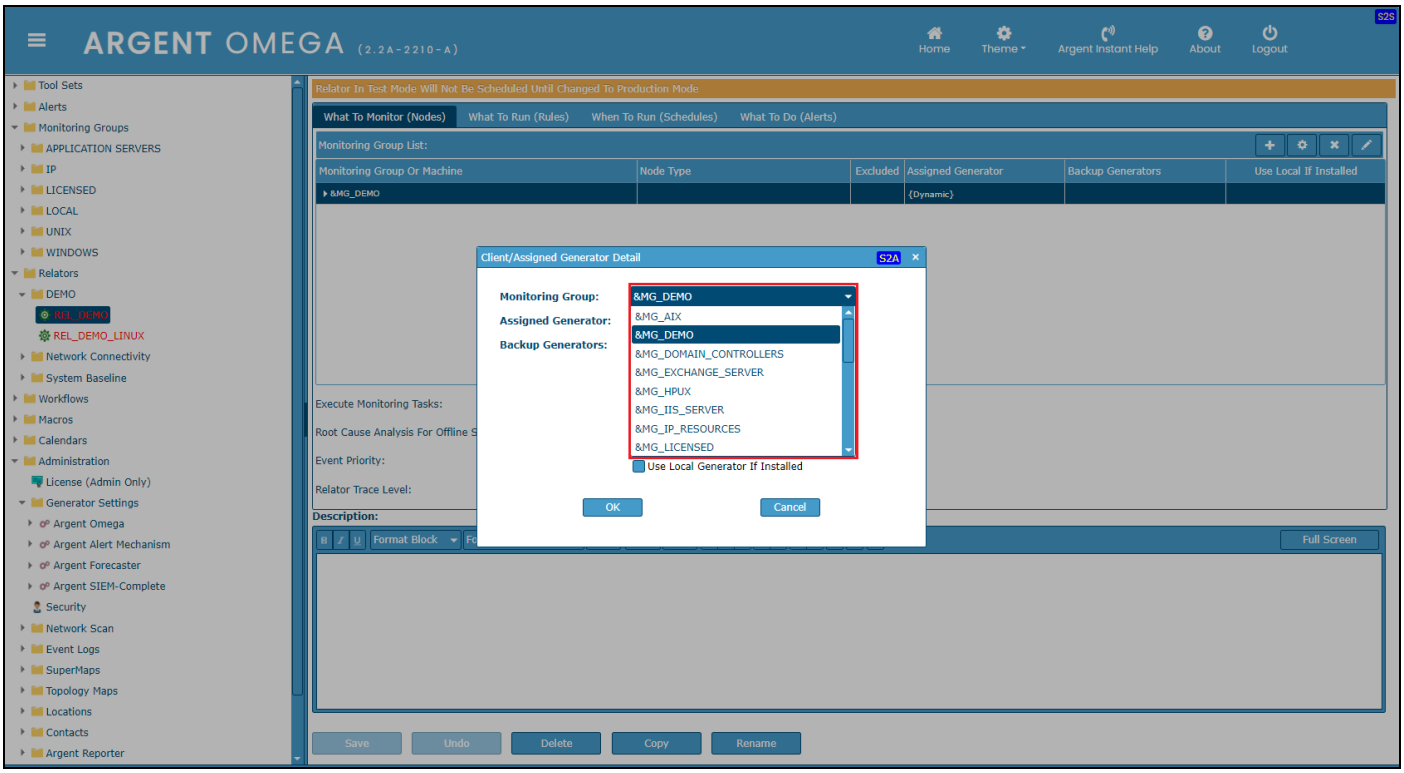
Proprietary Information – All Rights Reserved

Monitoring Groups

A Monitoring Group is a list of one or more servers or IP addresses.



In Argent Omega, Monitoring Groups define the servers and devices to be processed; Monitoring Groups are shared by all Argent Omega Tool Sets. The same Monitoring Group can be used by any number of Relators in Agent Omega.



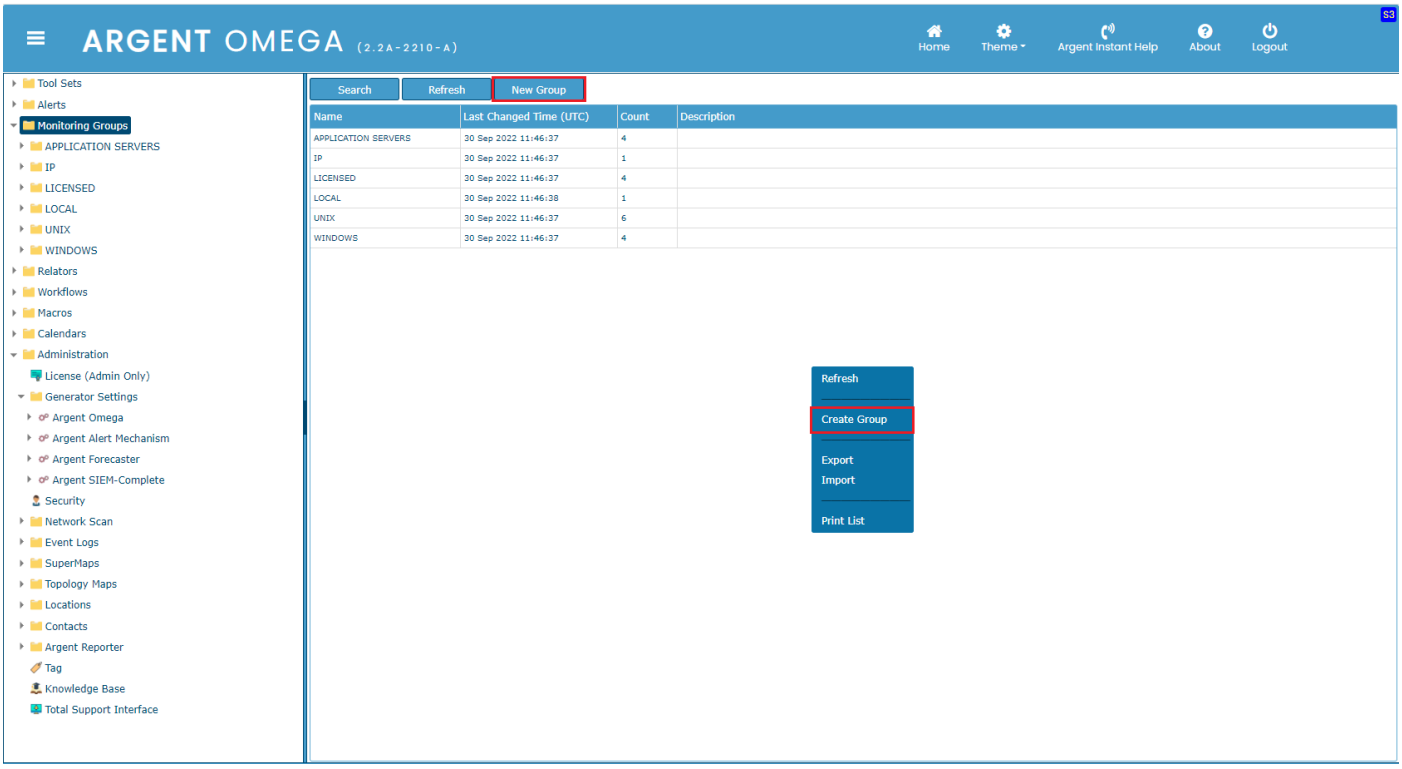
Proprietary Information – All Rights Reserved

By not having to specify servers and devices in the actual Relators, and by sharing Monitoring Groups, only the Monitoring Groups need change when a new production server comes online (or an existing server is replaced), rather than having to change hundreds of occurrences of the same server name or device address.

There is no limit to the ways Monitoring Groups can be created -- you can have one Monitoring Group consisting of the servers and devices in the Accounting Department, and another Monitoring Group of those in the Engineering Department.

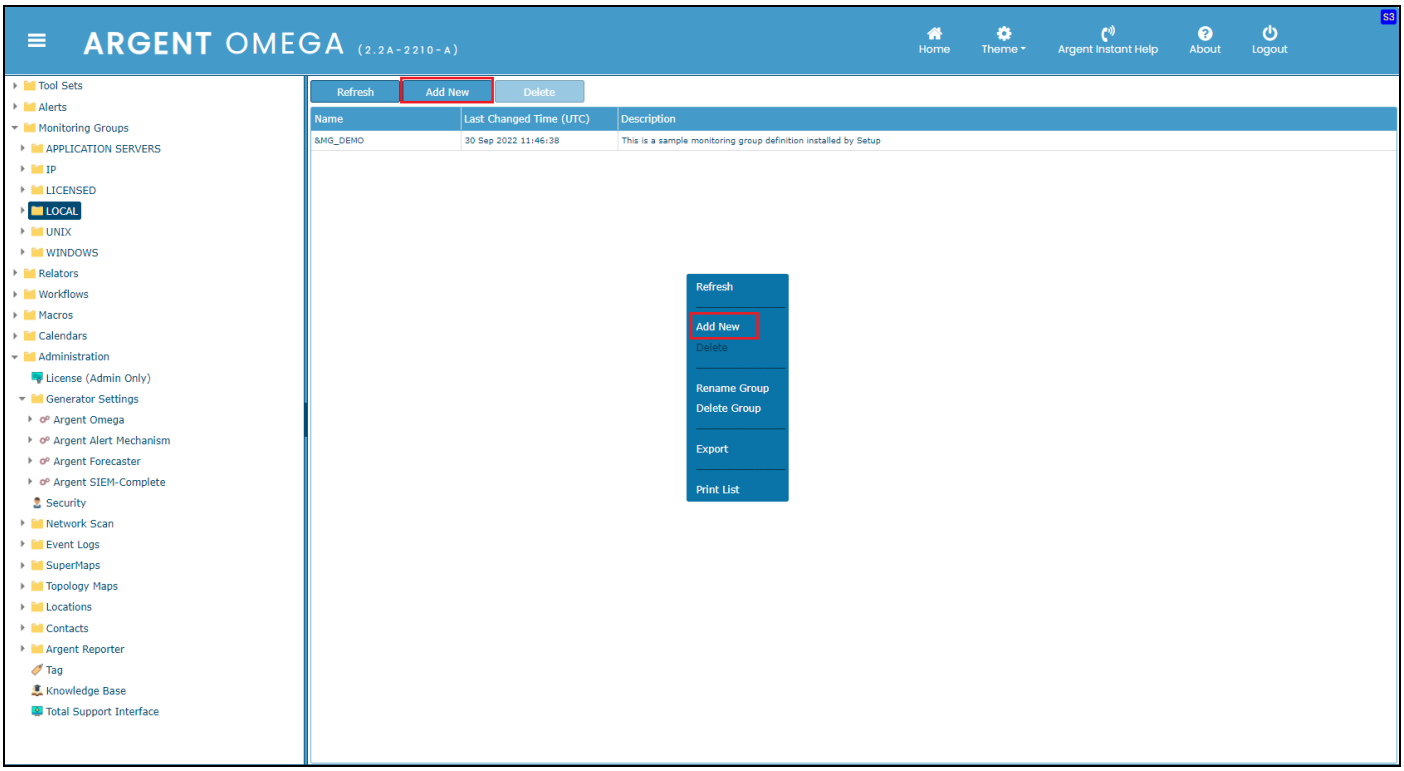
These same servers and devices can be in different Monitoring Groups may list servers by application - all production Exchange servers in one Monitoring Group, all production Oracle servers in another Monitoring Group, all test Linux machines in another Monitoring Group, and all network printers in another Monitoring Group.

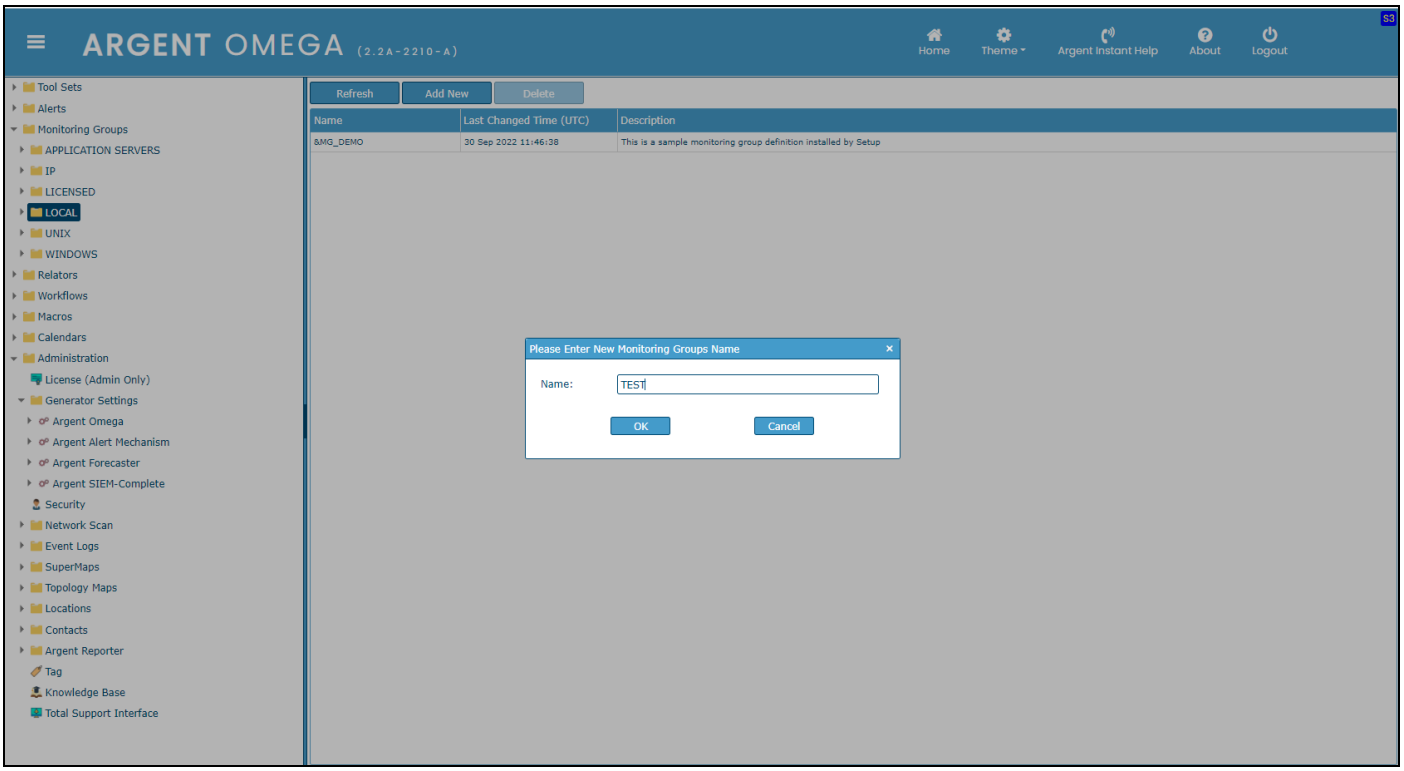
A new group is created using the **'New Group'** button or '**Create Group**' on the right-click menu option.



Proprietary Information – All Rights Reserved

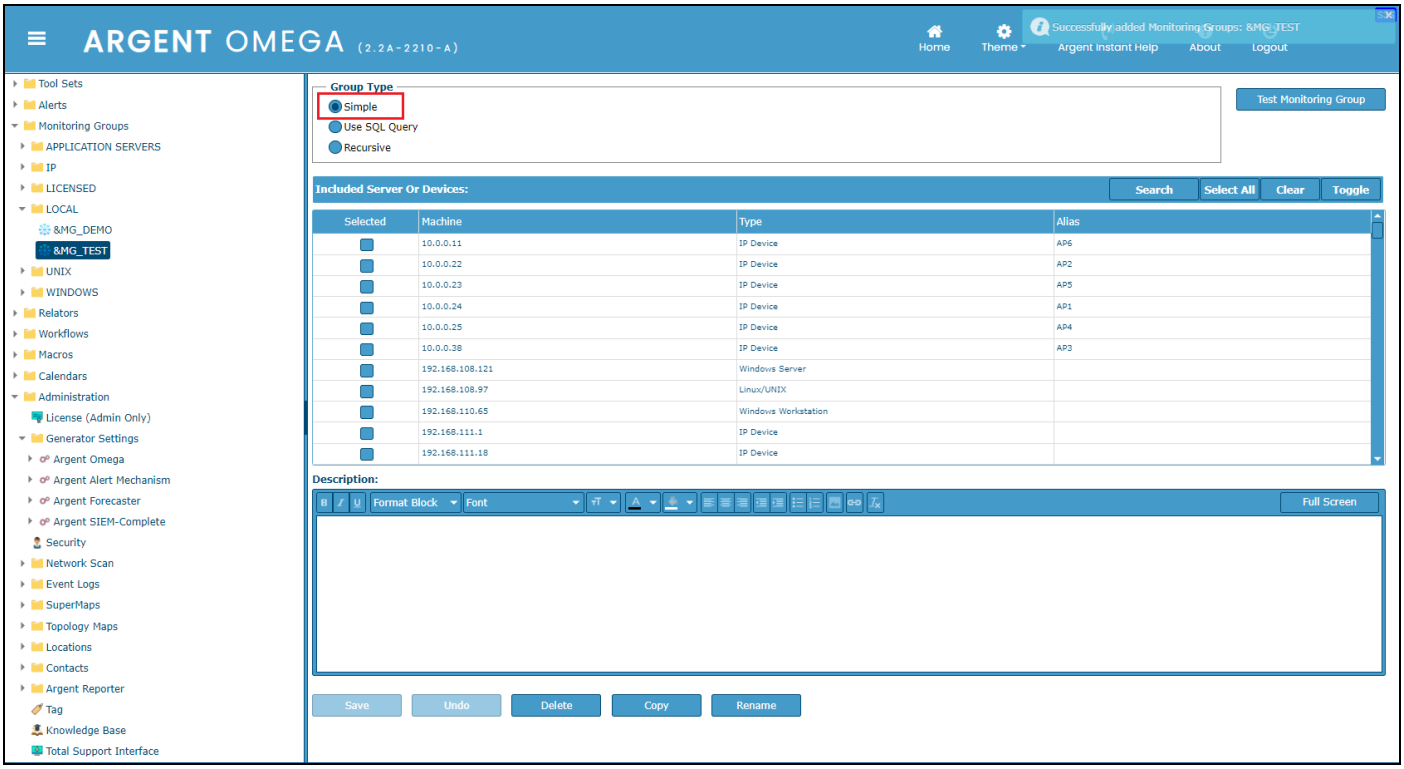
Select any group and a new monitoring group is created using **Add New** button or right-click menu option.



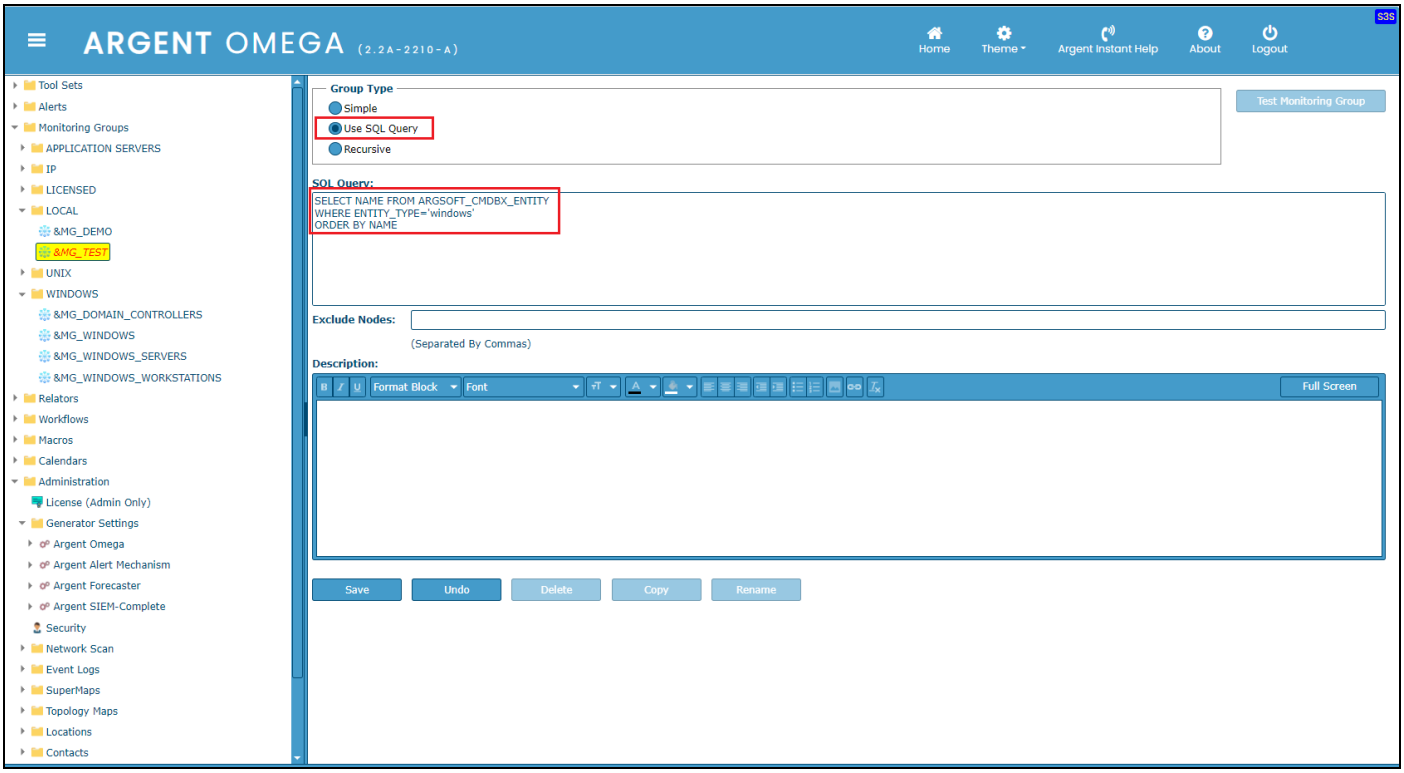


Select group type as Simple or Use SQL Query or Recursive.

In **Simple** mode, you need to select the server or device from the list by checking the box of the corresponding server.

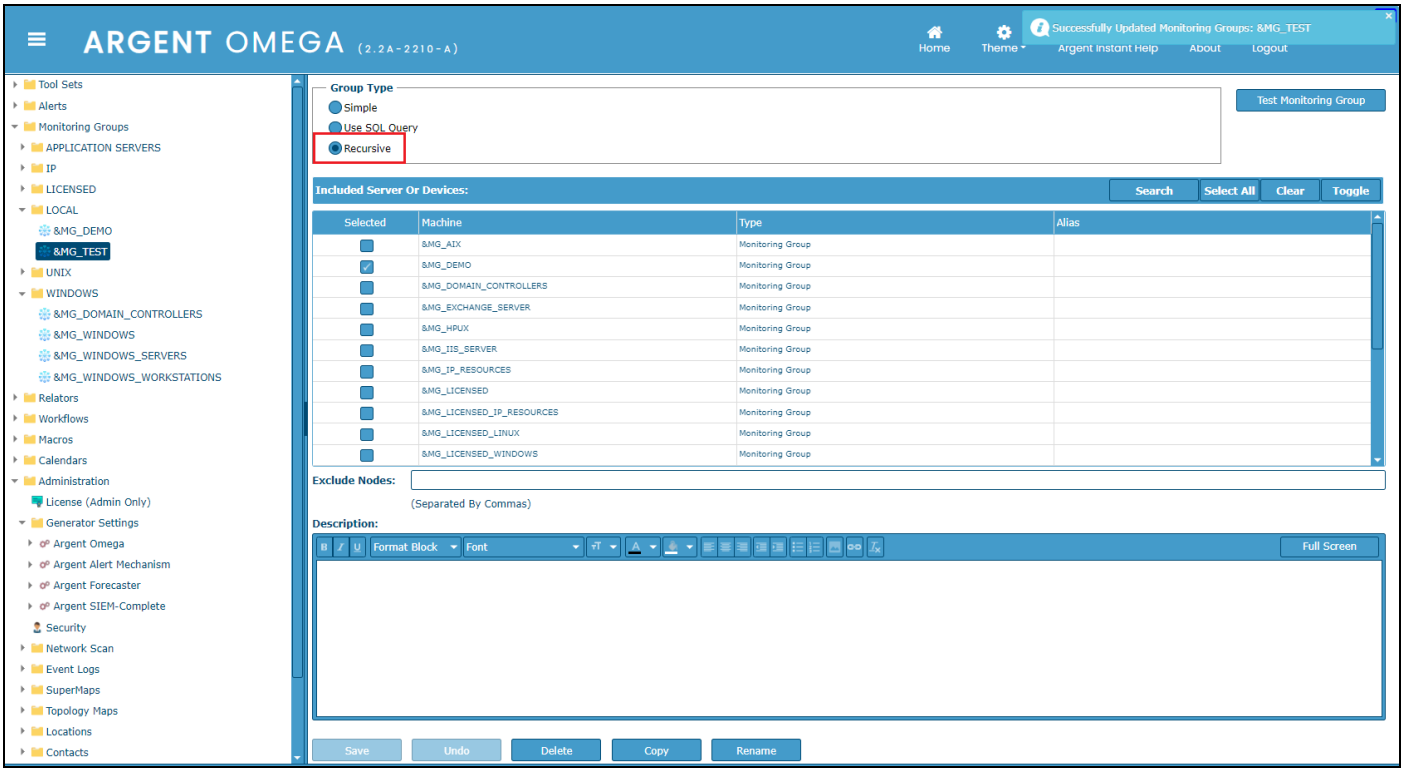


In **Use SQL Query** mode, you can select the servers and devices by specifying a SQL Query.



Proprietary Information – All Rights Reserved

Recursive mode allows you to select and use other Monitoring Groups recursively.

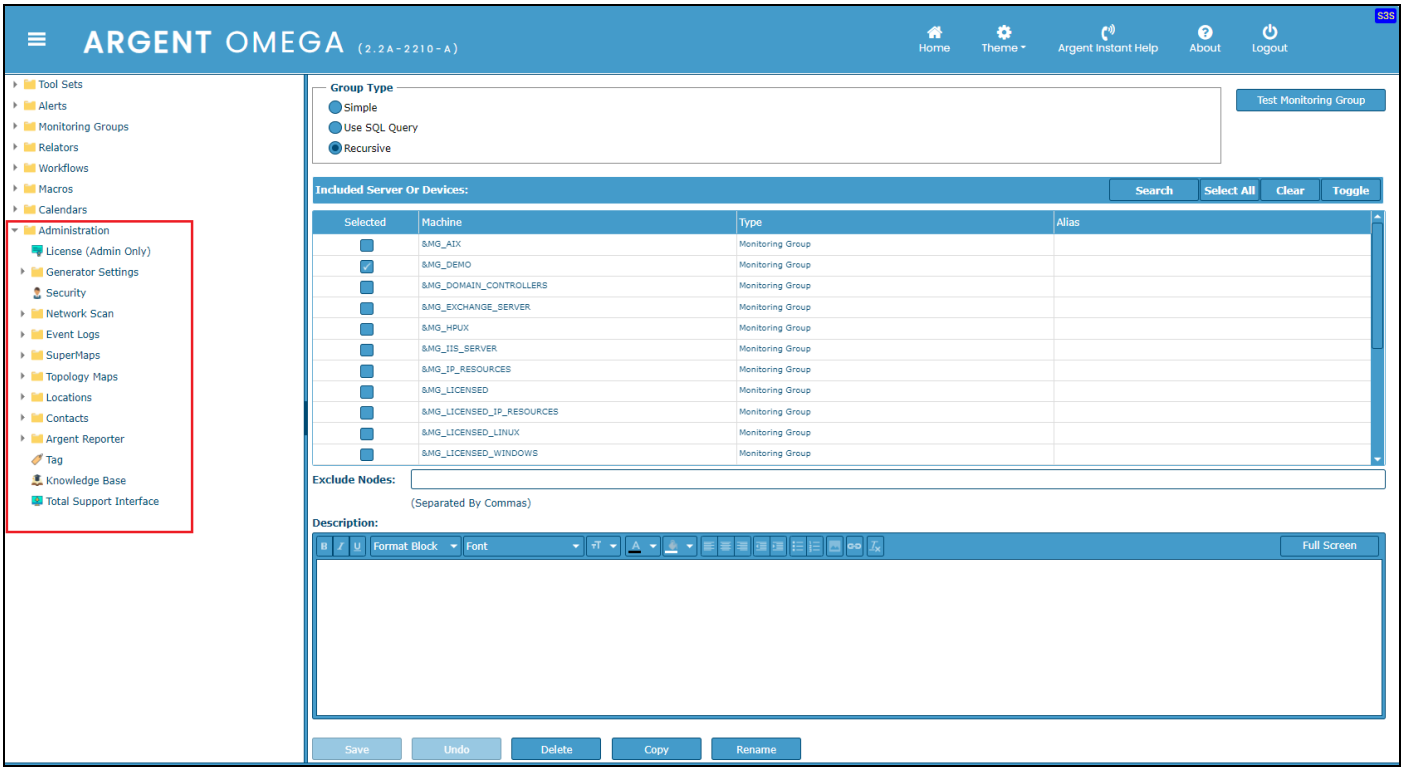


Proprietary Information – All Rights Reserved

Administration

The Administration section is where authorized Administrators can centrally configure many of the one-time, critical aspects of Argent Omega.

This includes configuring Primary or Secondary or Offload Generators, licensing, configuring Argent Alert Mechanism, configuring security components, etc. The administration section configures the following components:



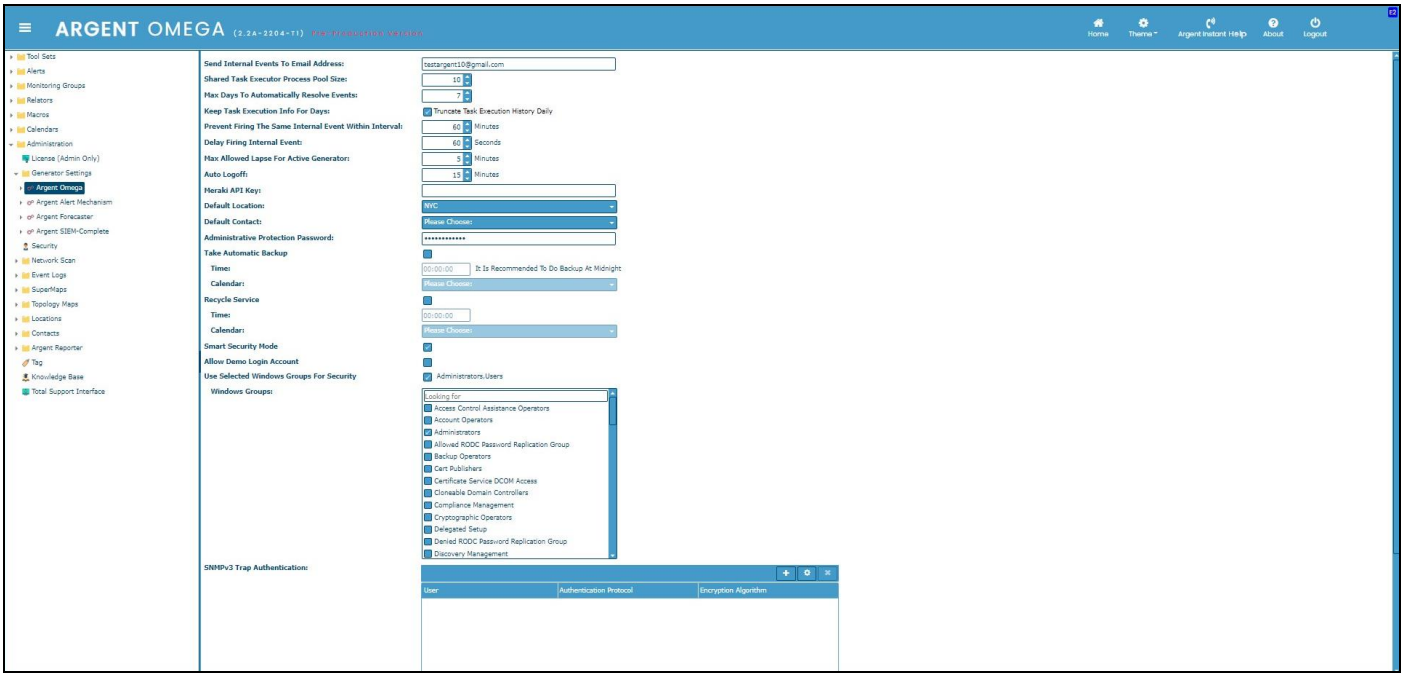
Proprietary Information – All Rights Reserved

Generator Settings

The Generator Settings screen selects the configuration settings of the **Argent Omega Primary or Secondary or Offload Generator, Argent Alert Mechanism, Argent Forecaster, Argent SIEM-Complete** and **License**.

(To learn more about Argent Omega terms please see Argent KBI Https://Help.Argent.com/#KBI_312003)

Generator Configuration:



- **Send Internal Events to Email Address**
  Specify the email address for receiving alerts on internal events of Argent Omega, Argent Alert Mechanism, Argent Forecaster, and Argent SIEM generator.

- **Shared Task Executor Process Pool Size**
  Set the pool size to execute the shared task.

- **Max Days to Automatically Resolve Events**
  Specify the maximum number of days to resolve events automatically.

- **Keep Task Execution Info For Days**
  Number of days to keep the executed task information. There is an option to truncate task execution daily.

Proprietary Information – All Rights Reserved

- **Delay Firing Internal Event**
  Specify the interval for firing internal events.

- **Prevent Firing the Same Internal Event Within Interval**
  Specify the number of minutes to prevent firing the same internal event within the interval specified in Delay Firing Internal Event.

- **Max Allowed Lapse For Active Generator**
  Specify the maximum allowed time lapse minutes to consider the Generator as Active.

- **Auto Logoff Minutes**
  Specify the number of inactive minutes to auto logoff Argent Omega.

- **Miraki API Key**
  API key to monitor Cisco Meraki devices.

- **Default Location**
  Specify the default location for Argent Omega.

- **Default Contact**
  Specify the default contact for Argent Omega.

- **Administrative Protection Password**
  Protection password for Administrator level operations. Default password is “Argent Omega.”

- **Action Alert Test Password**
  Specify the password for alert testing.

- **Take Automatic Backup**
  Check this option and specify time and calendar to backup Argent Omega automatically.

- **Recycle Service**
  Check this option and specify time and calendar to recycle Argent Omega service.

- **Smart Security Mode**
  This option is checked by default as Argent Omega uses Smart Security Mode by default. Uncheck this option to use Advanced Mode security.

Proprietary Information – All Rights Reserved

- **Use Selected Windows Groups For Security**

  Check this option to use selected Windows Groups in Argent Omega Security. Select groups from “Windows Groups” combo box. If this option is unchecked, all predefined Windows Groups are used in Argent Omega Security.

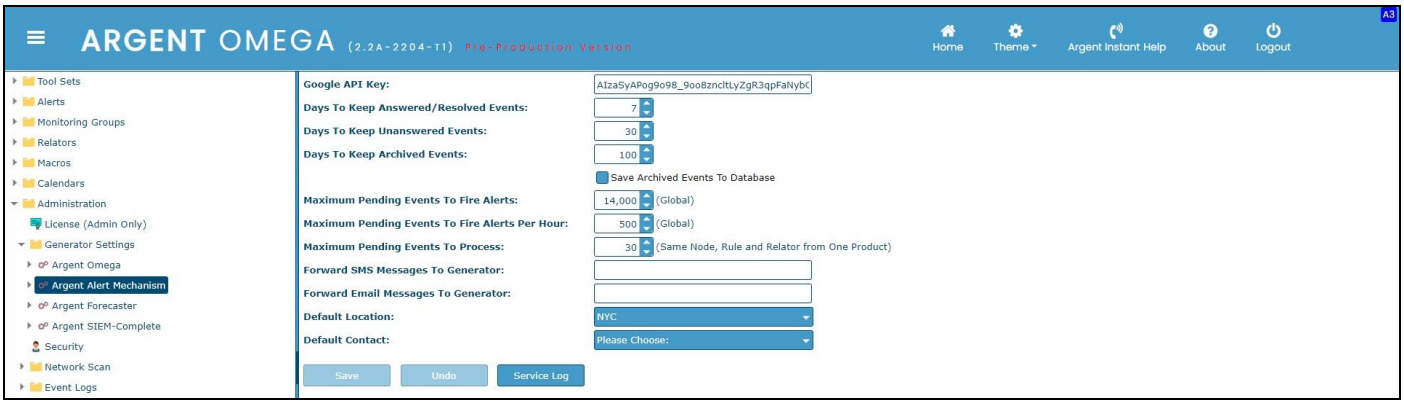
- **Windows Groups**

  If “Use Selected Windows Groups For Security” option is checked, select the groups from Windows Groups combo box.

Proprietary Information – All Rights Reserved

Argent Alert Mechanism Configuration

This is where the Argent Alert Mechanism is configured. This section also provides the facility to configure Email and SMS Generators to fire Email and SMS alerts respectively.



- **Google API Key**

  Google API key required for using the **optional** Google Maps.

- **Days to Keep Answered Or Resolved Events**

  Specify number of days to keep answered or resolved events.

- **Days to Keep Unanswered Events**

  Specify number of days to keep unanswered events.

- **Days to Keep Archived Events**

  Specify number of days to keep archived events. There is an option to save events to database.

- **Maximum Pending Events To Fire Alerts**

  Specify the maximum number of pending events to fire alerts.

- **Maximum Pending Events To Fire Alerts Per Hour**

  Specify the maximum number of pending events to fire alerts per hour.

- **Maximum Pending Events To Process**

  Specify the maximum number of pending events to process for the same Node, Rule, and Relator from One Product.

- **Forward SMS Messages To Generator**

  Generator name to forward SMS Messages.

Proprietary Information – All Rights Reserved

- **Forward Email Messages To Generator**

  Generator Name to forward Email Messages.

- **Default Location**

  Specify the default location for Argent Alert Mechanism.

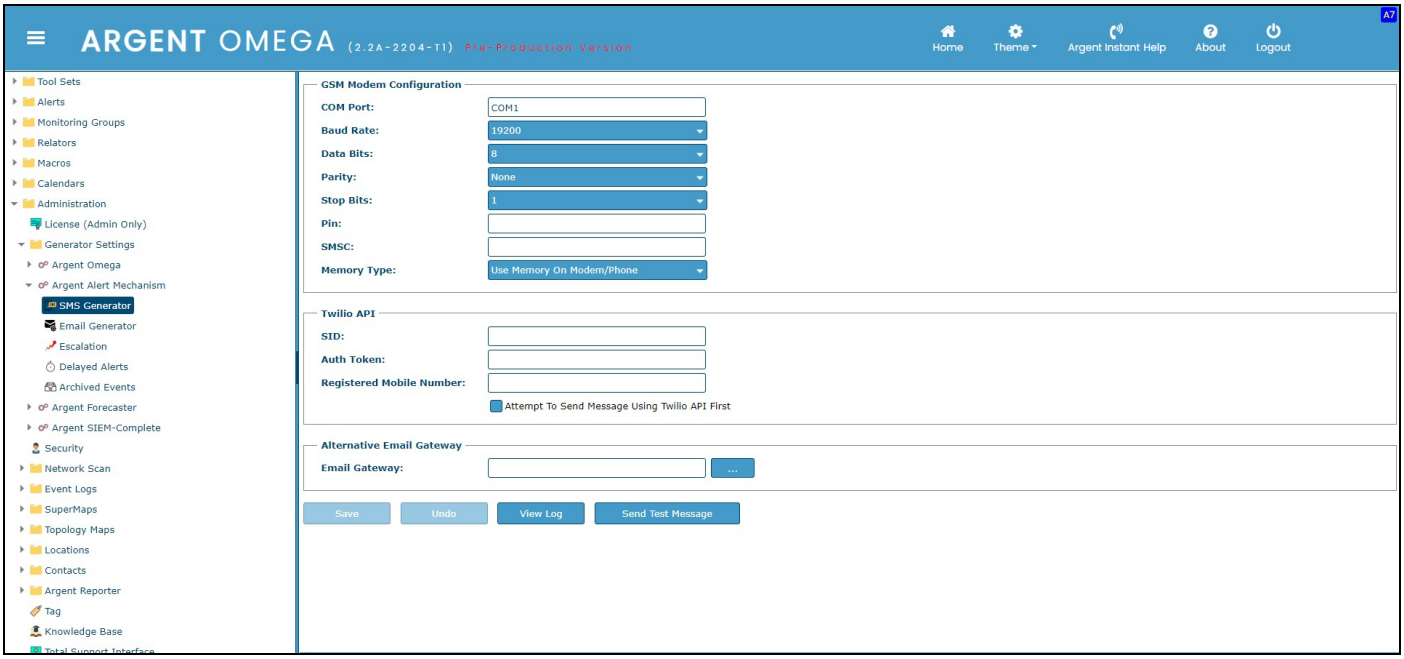
- **Default Contact**

  Specify the default contact for Argent Alert Mechanism.

Configure SMS Generator

SMS Generator sends SMS Alerts. SMS Generator uses any of the following communication method to send SMS Alerts:

1. Using GSM Modem
2. Using Twilio API
3. Using SMS gateway of cell service provider



Proprietary Information – All Rights Reserved

GSM Modem Configuration Settings

COM Port: Serial port or the virtual serial port of the computer to which the GSM Modem is connected.

Baud Rate: Maximum port speed of modem.

Data Bits: Communication Data Bits size between GSM Modem and the computer.

Parity: Type of parity check for communication between GSM Modem and the computer.

Stop Bit: Communication Stop Bits size between GSM Modem and the computer.

Pin: Specifies the **PIN** (Personal Identity Number) for activating the services in the GSM Modem

SMSC: SMSC address of SIM card.

Memory Type: Specify the message storage area.

Twilio API Settings

SID: Security Identifier provided by Twilio.

Auth Token: Authentication Token provided by Twilio.

Registered Mobile Number: Mobile number registered in Twilio.

Email Gateway Settings

Email Gateway: Specify the SMS gateway or you can select the SMS gateway of a specific cell service provider.

Configure Email Generator

The following three services or protocols can be configured in Email Generator to send email Alerts in Argent Omega:

- Exchange Web Service
- MAPI Protocol
- SMTP Protocol

The following services can be configured to check incoming emails:

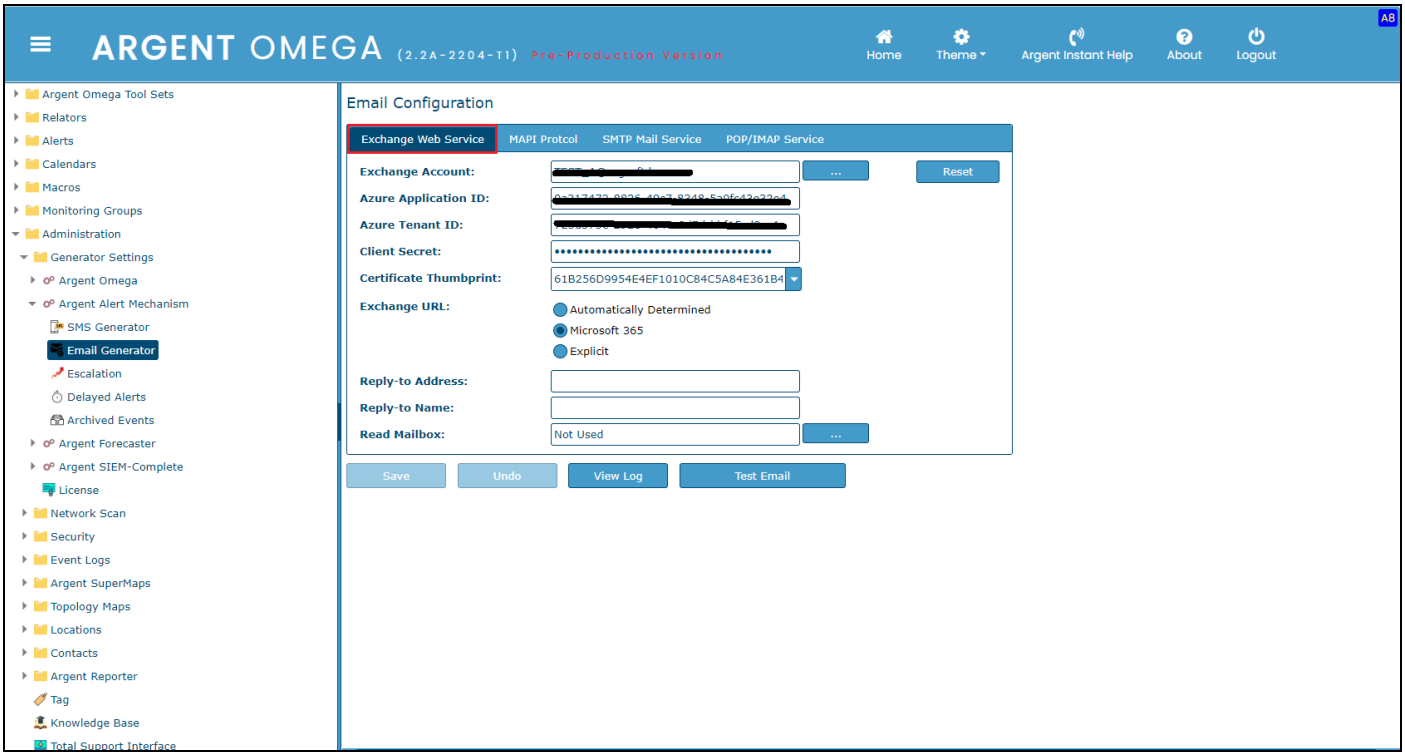
- POP
- IMAP

Proprietary Information – All Rights Reserved

Email incoming services are required to check email server for auto-answering messages in particular intervals.

Exchange Web services (EWS) uses Microsoft Exchange Web Services Managed API to send Alert email messages. Specify the following properties to send emails using EWS:

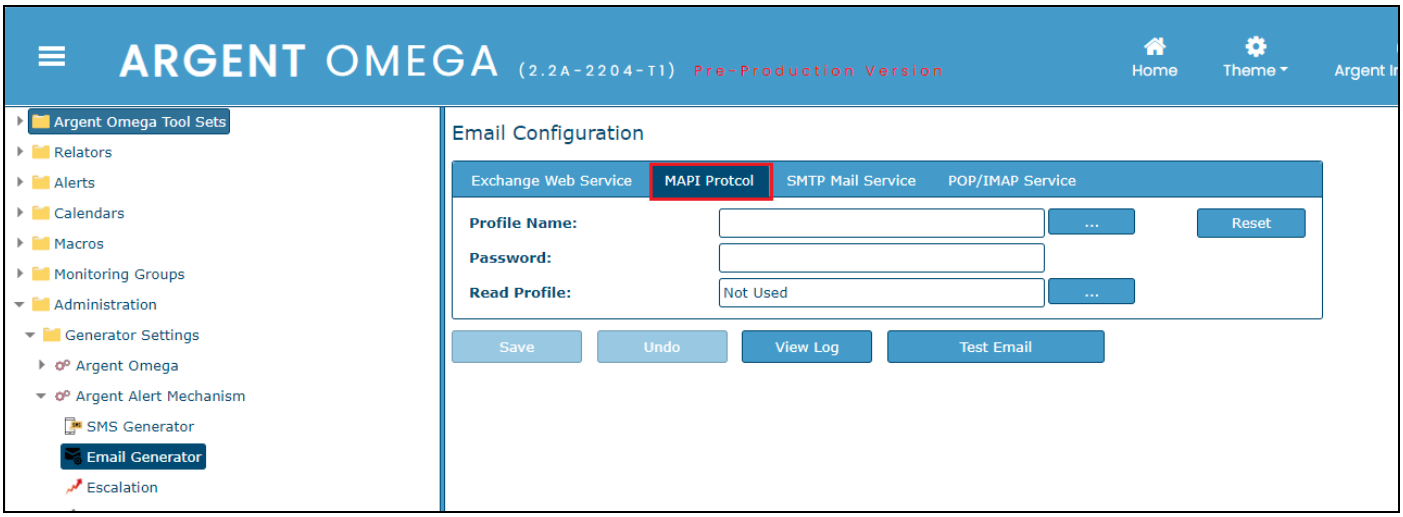
- Exchange Account
- Azure Application ID
- Azure Tenant ID
- Client Secret
- Certificate Thumbprint
- Exchange URL



Specify the following properties to send emails using MAPI:

- Profile Name
- Password

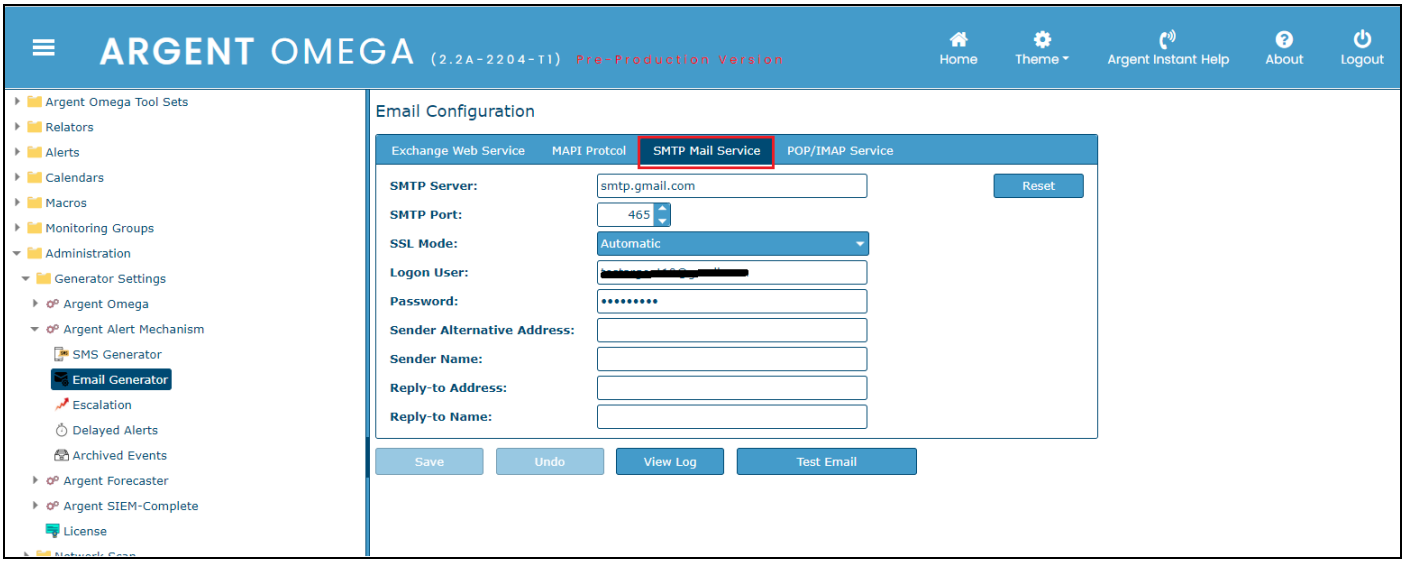
Proprietary Information – All Rights Reserved



Proprietary Information – All Rights Reserved

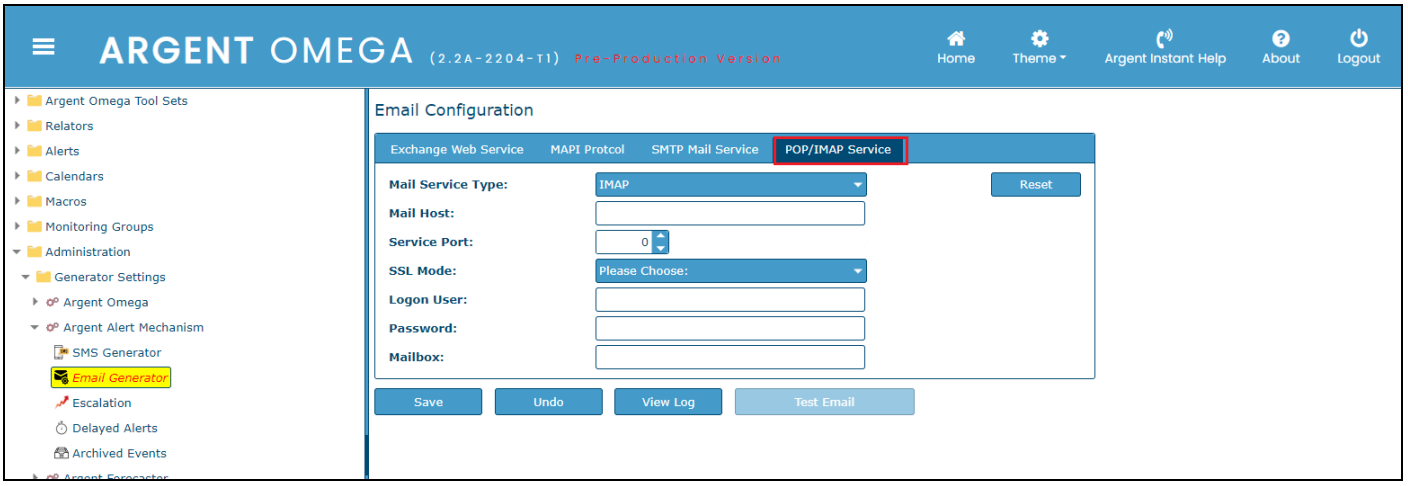
Specify the following properties to send emails using SMTP service:

- SMTP Server
- SMTP Port
- SSL Mode
- Logon User
- Password

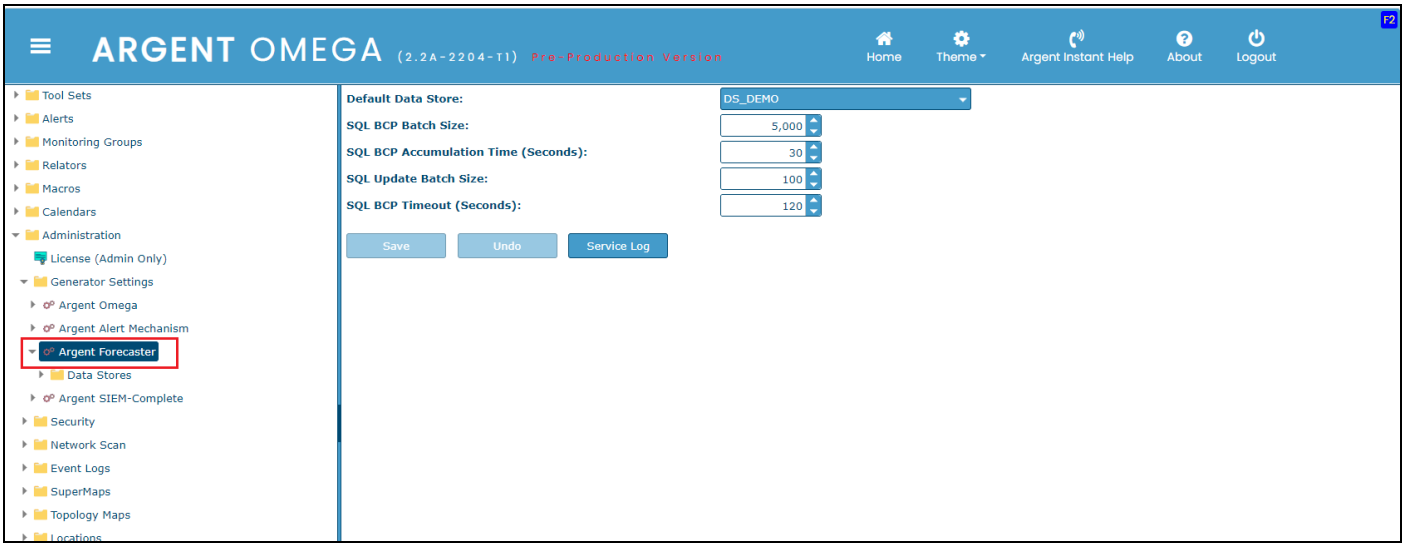


Specify the following properties to send emails using POP/IMAP service:

- Mail Host
- Service Port
- SSL Mode
- Logon User
- Password



Argent Forecaster Configuration:



- **Default Data Store**

  Specify the default data store for Argent Forecaster to store Performance data.

- **SQL BCP Batch Size**

  Specify the SQL bulk copy batch size.

- **SQL BCP Accumulation Time (Seconds)**

  Specify the SQL bulk copy accumulation time in seconds.

- **SQL Update Batch Size**

  Specify the SQL update batch size.

- **SQL BCP Timeout (Seconds)**

  Specify the SQL bulk copy timeout.

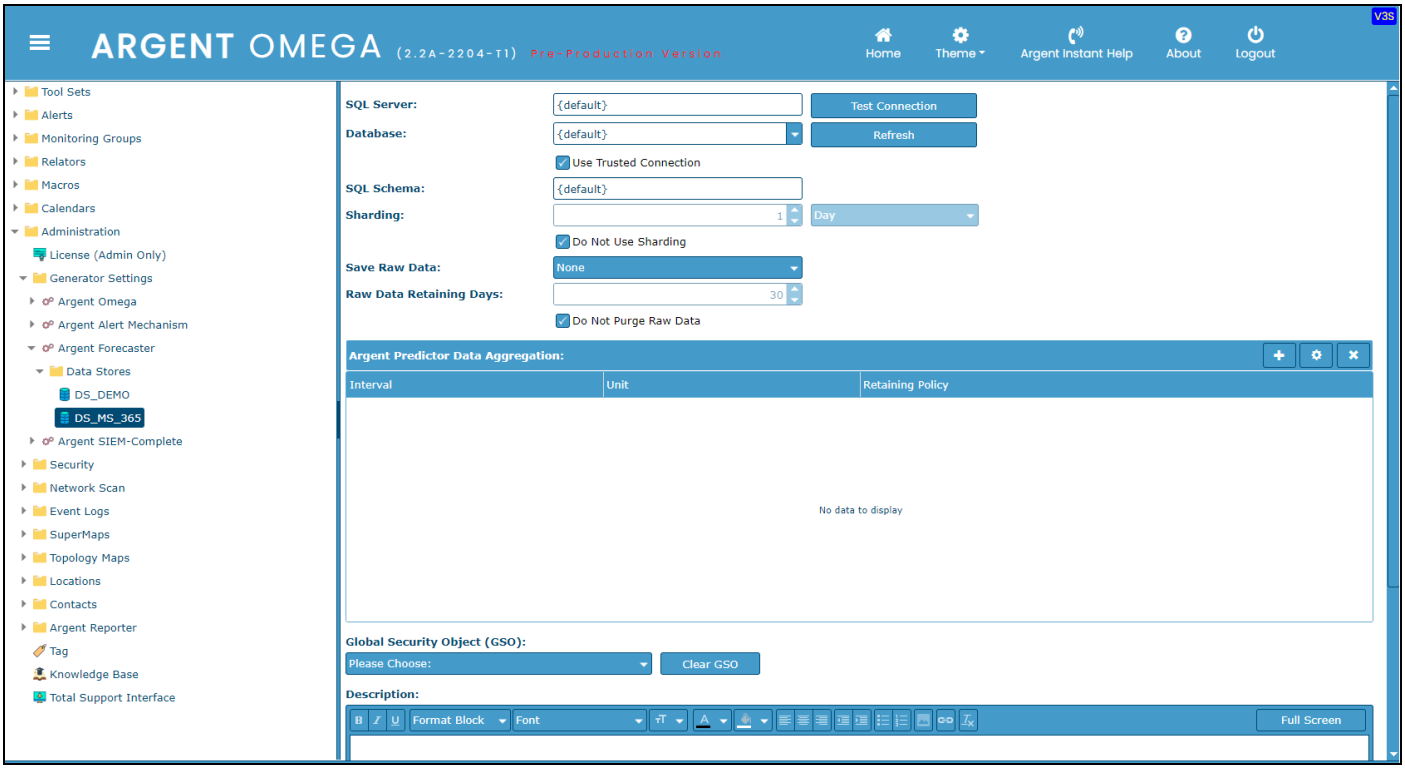
Proprietary Information – All Rights Reserved

Manage Data Stores

Data Stores defines the SQL Server database details to store Performance metrics retrieved by Argent Omega Rules. Users can create and manage Data Stores in Argent Forecaster section.

Proprietary Information – All Rights Reserved

To create a Data Store, click **Add New** context menu option or **Add New** button and specify a name for the new Data Store.



Specify the **SQL Server** and **Database**. The Performance data will be stored in the specified SQL database when you configure this Data Store in Tool Sets.

Specify **Logon** and **Password** if trusted connection is not used.

Use **Test Connection** button to test the SQL Server connectivity using the specified credentials.

Specify **SQL Schema** to override the default Schema.

Uncheck **Do Not Use Sharding** option to use database sharding. Sharding improves performance. Specify sharding criteria in **Sharding** field. Each shard is a separate table in Argent Omega database.

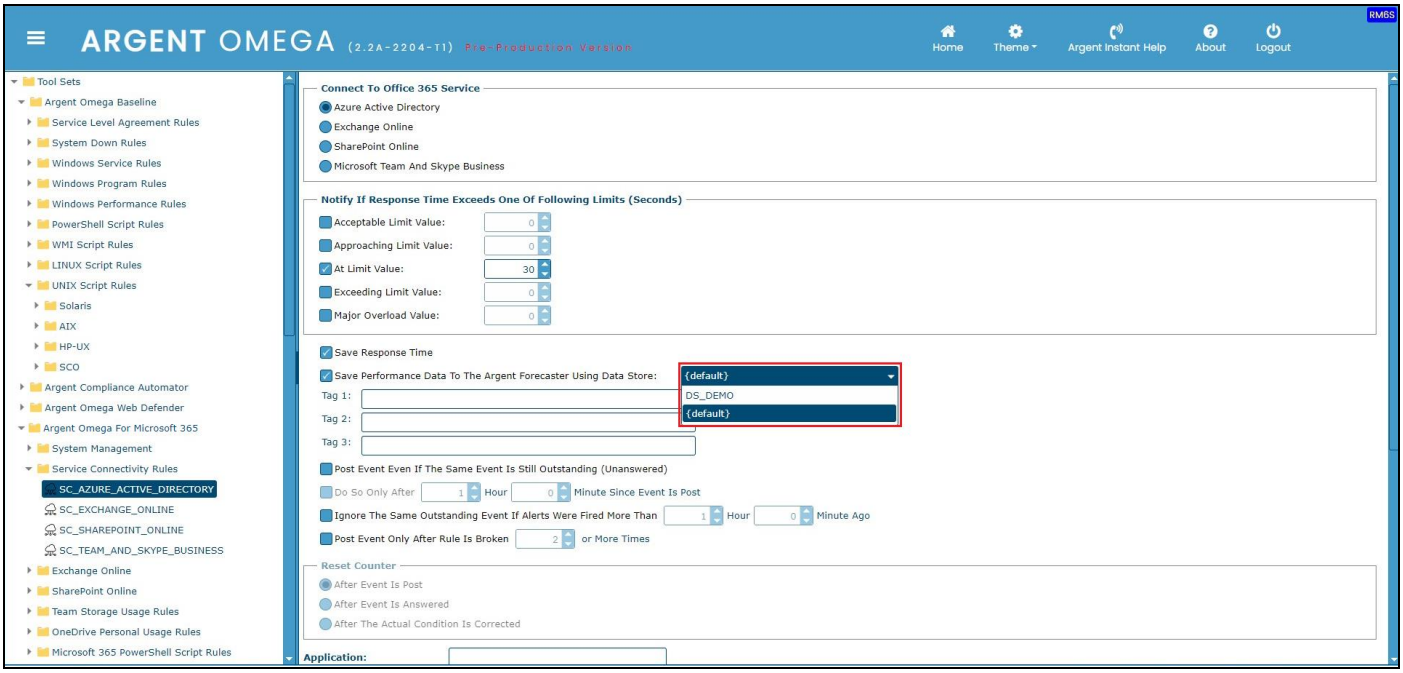
Select the method of keeping raw data from **Save Raw Data** combo box. It can be “None” for not keeping raw data or it can be either “SQL Database” or “File System” to store the raw data in database table or file system respectively.

Uncheck **Do Not Purge Raw Data** option to purge raw data after the days specified in **Raw Data Retaining Days** field.

Proprietary Information – All Rights Reserved

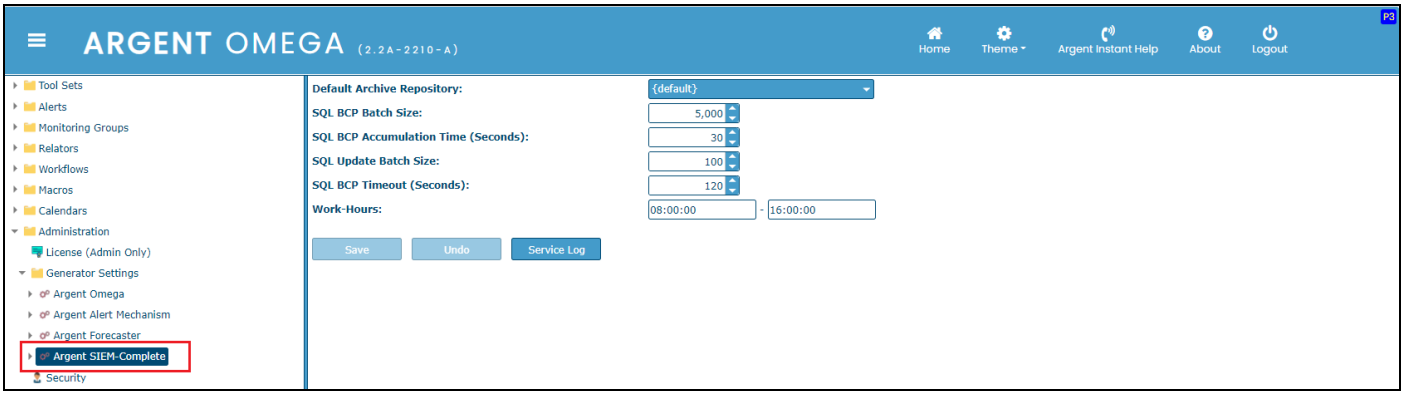
Define **Argent Predictor Data Aggregation.** Data Store Allow aggregates Predictor Data by minute, hour and day. It is possible to define multiple aggregation definitions. Users specify the interval and aggregated data retaining days in each definition. Aggregated result data of each definition will be stored in a separate database table. Uncheck **Do Not Purge Shardings** option to delete older aggregated data.

You can configure the newly created Data Store in Argent Omega Rules as shown below. The Performance Data retrieved by the Rule will be stored in configured Data Store.



Proprietary Information – All Rights Reserved

Argent SIEM-Complete Configuration



- **Default Archive Repository**

  Specify default Archive Repository for Argent SIEM.

- **SQL BCP Batch Size**

  Specify the SQL bulk copy batch size.

- **SQL BCP Accumulation Time (Seconds)**

  Specify the SQL bulk copy accumulation time in seconds.

- **SQL Update Batch Size**

  Specify the SQL update batch size.

- **SQL BCP Timeout (Seconds)**

  Specify the SQL bulk copy timeout.

- **Work-Hours**

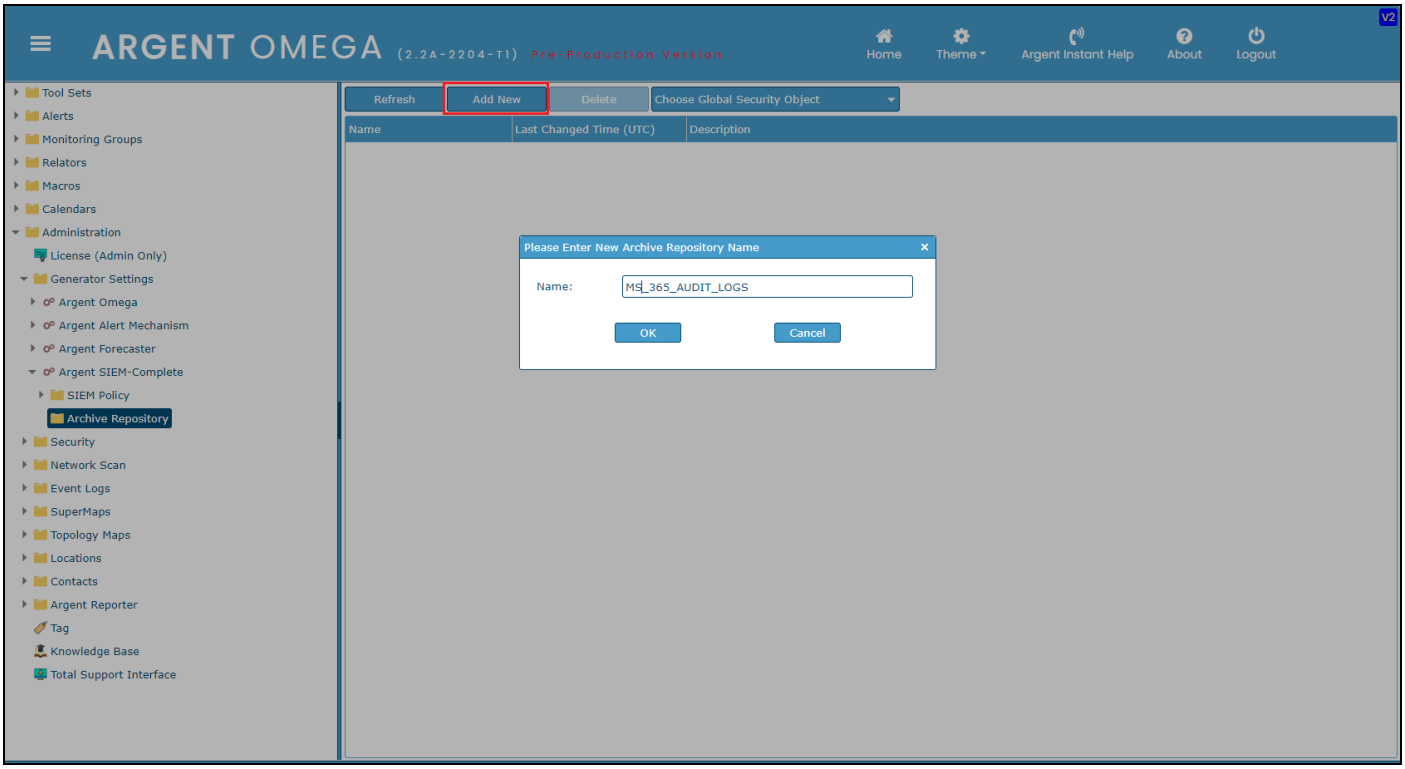
  Specify the working hours to operate Argent SIEM.

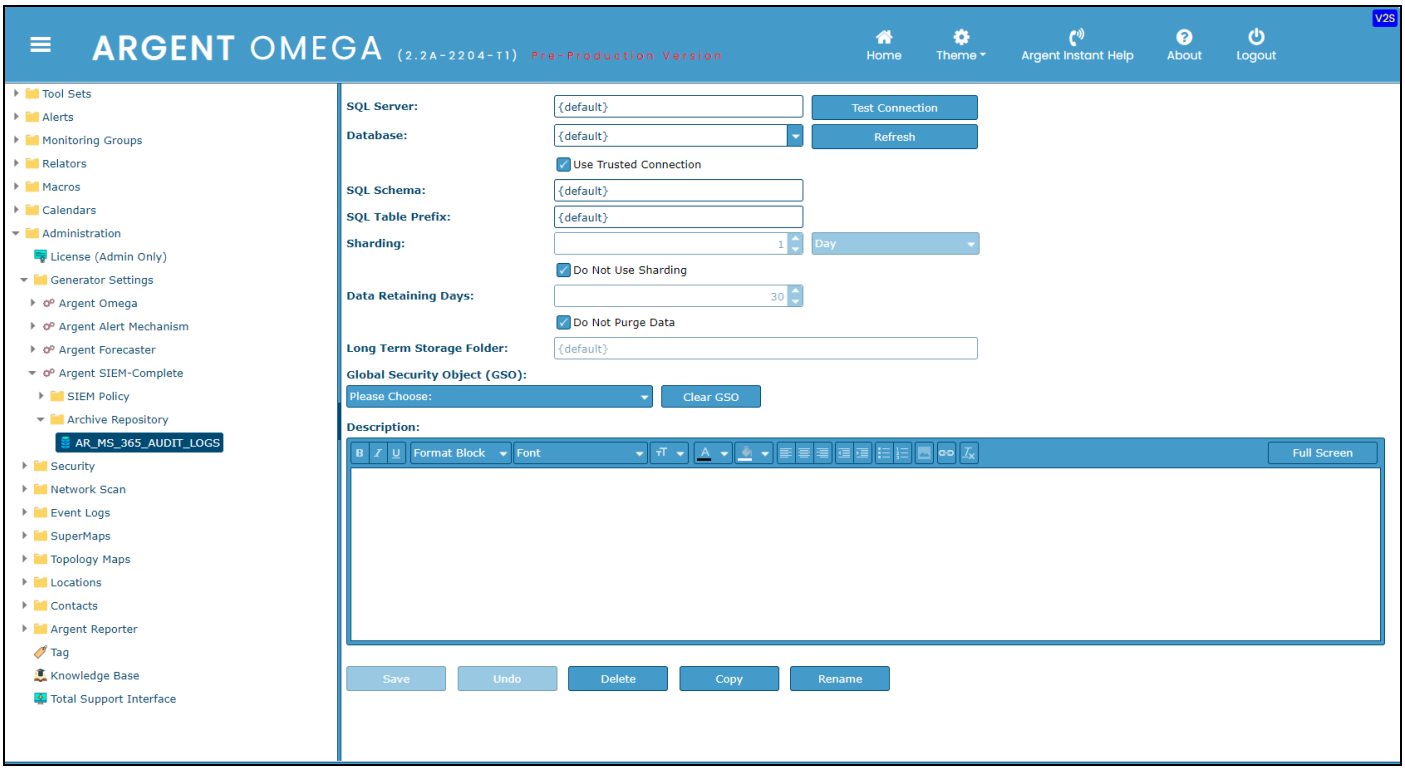
Proprietary Information – All Rights Reserved

Manage Archive Repository

Archive Repository defines the SQL Server database details to archive compliance data retrieved by Argent Compliance Automator. It is possible to create and manages Archive Repositories in Argent SIEM-Complete section.

To create an Archive Repository click **Add New** context menu option or **Add New** button and specify a name for new Archive Repository.





Specify the **SQL Server** and **Database**. The compliance data will be stored in the configured SQL database when using this Archive Repository in Argent Compliance Automator Rules and SIEM policies.

Proprietary Information – All Rights Reserved

Specify **Logon** and **Password** if trusted connection is not used.

Use **Test Connection** button to test the SQL Server connectivity using the specified credentials.

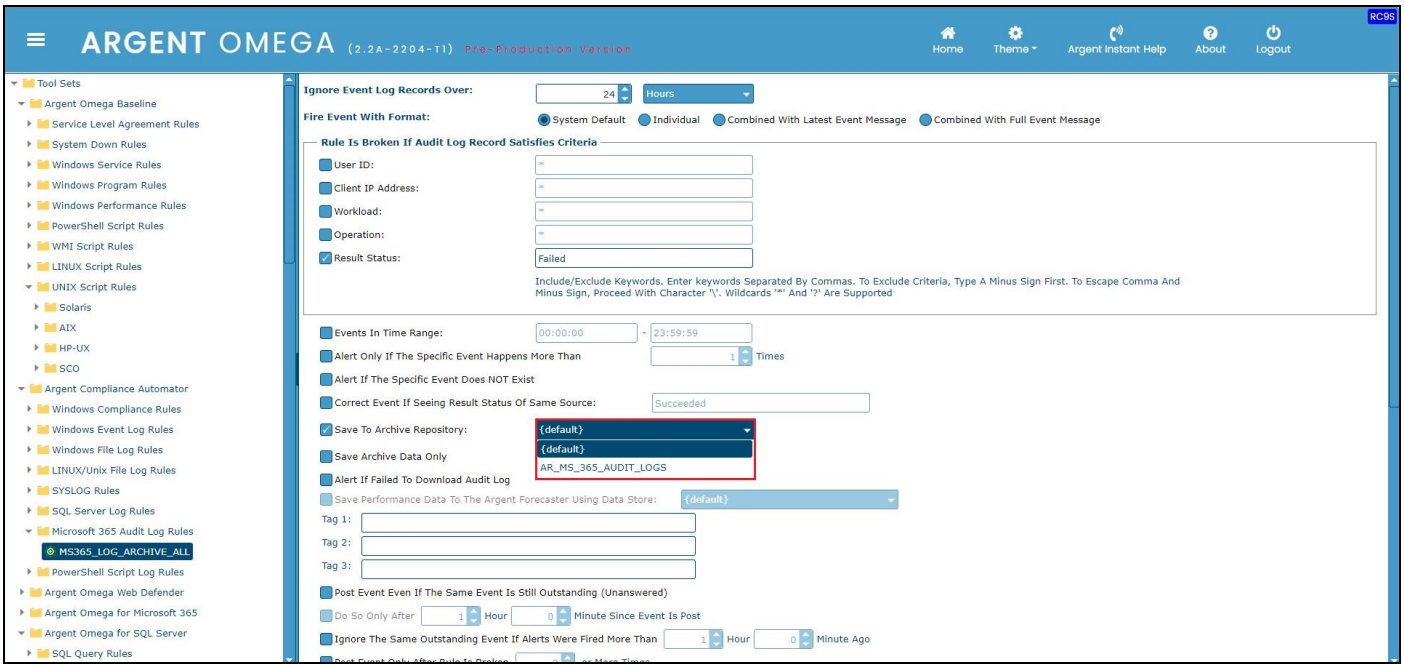
Specify **SQL Schema** to override the default Schema.

Specify **SQL Table Prefix** to use custom table prefixes for tables that stores compliance audit data.

Uncheck **Do Not Use Sharding** option to use database sharding. Sharding improves performance. Specify sharding criteria in **Sharding** field. Each shard is a separate table in Argent Omega database.

Uncheck **Do Not Purge Data** option to purge the archived data after the days specified in **Data Retaining Days** field**.**

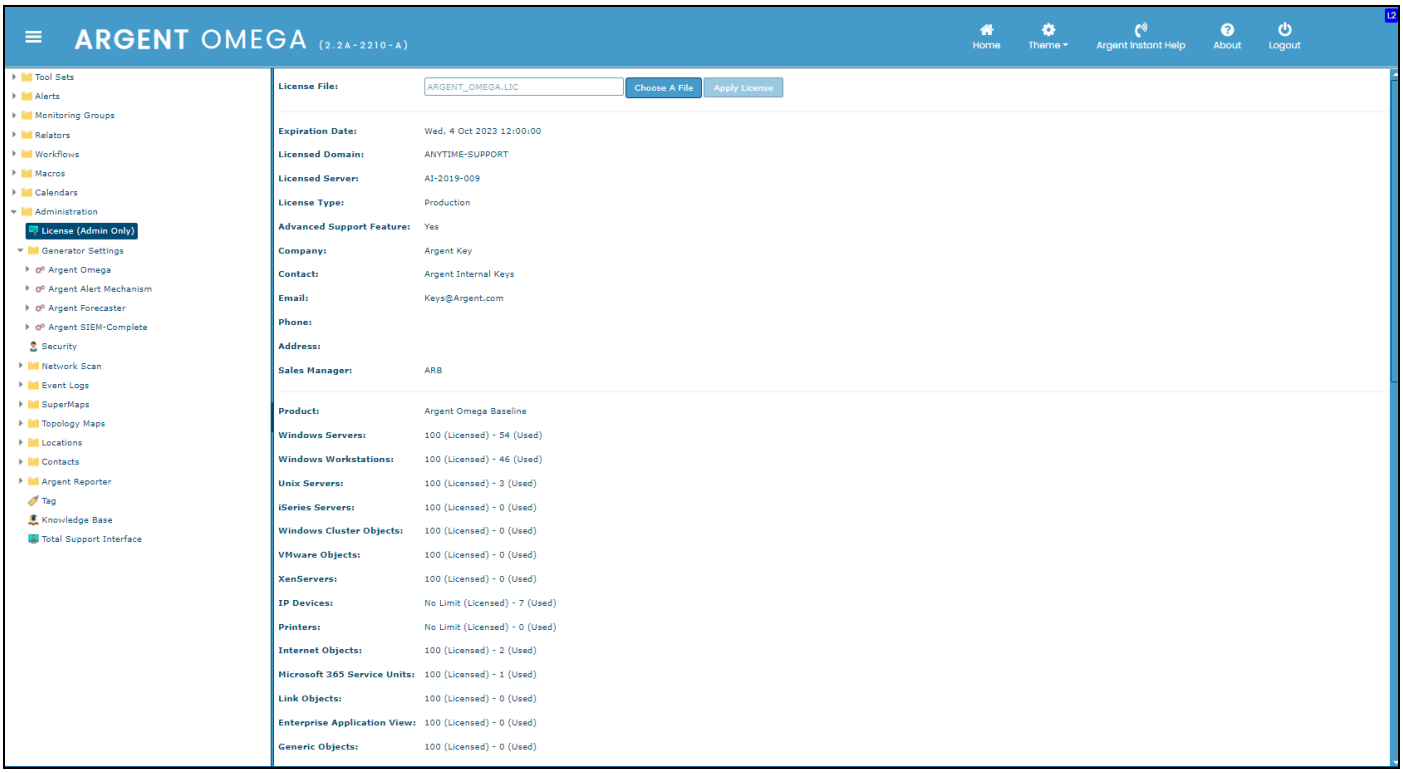
You can configure the newly created Archive Repository in Argent Compliance Automator Rules. The event data retrieved by the Rule will be stored in configured Archive Repository.



Proprietary Information – All Rights Reserved

License

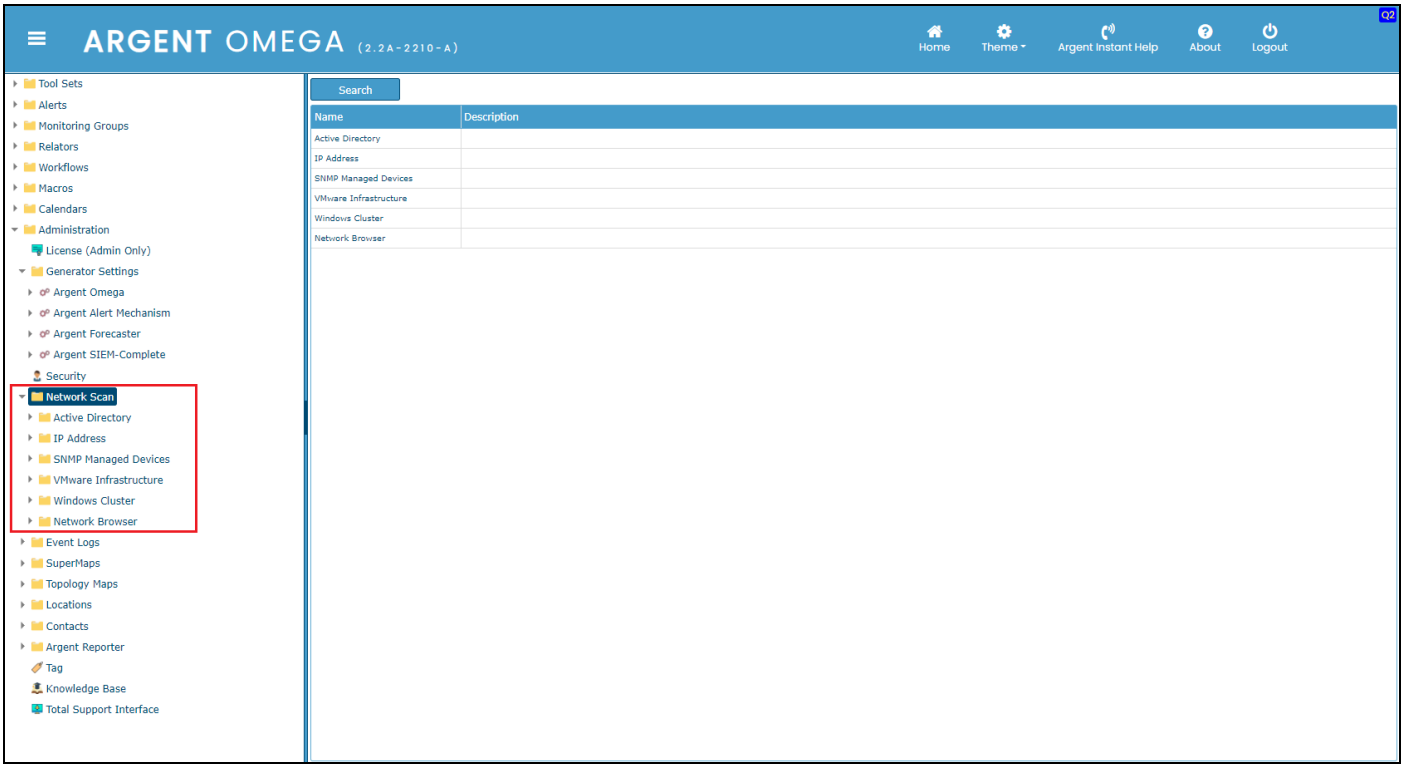
New license file can be browsed and applied from the License screen. The information regarding the applied license is displayed in the screen.



Proprietary Information – All Rights Reserved

Network Scan

Network Scan is used to scan servers or devices in the network.



Argent Omega provides the facility to scan servers or devices in the following environments:

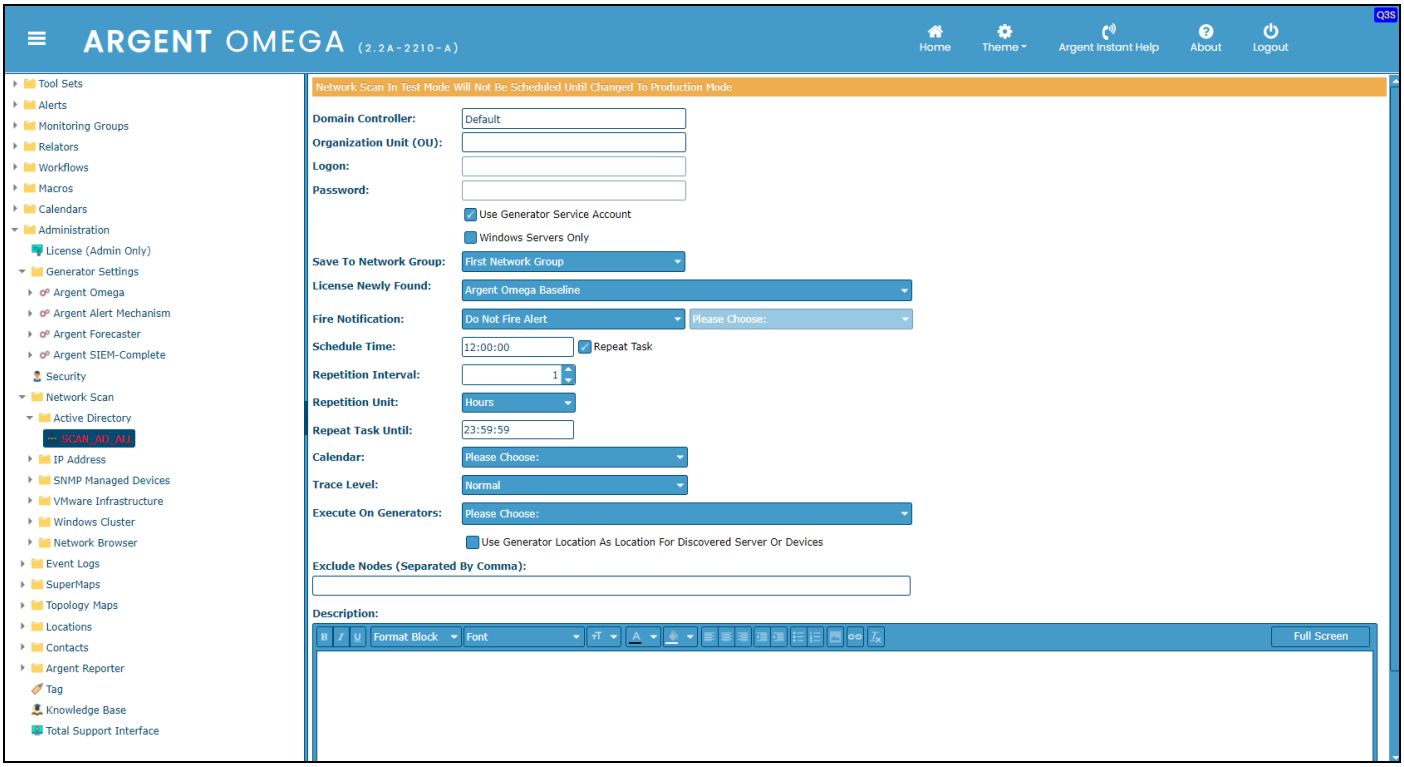
- Active Directory
- IP Address
- SNMP Managed Devices
- VMware Infrastructure
- Windows Cluster
- Network Browser

Proprietary Information – All Rights Reserved

Active Directory

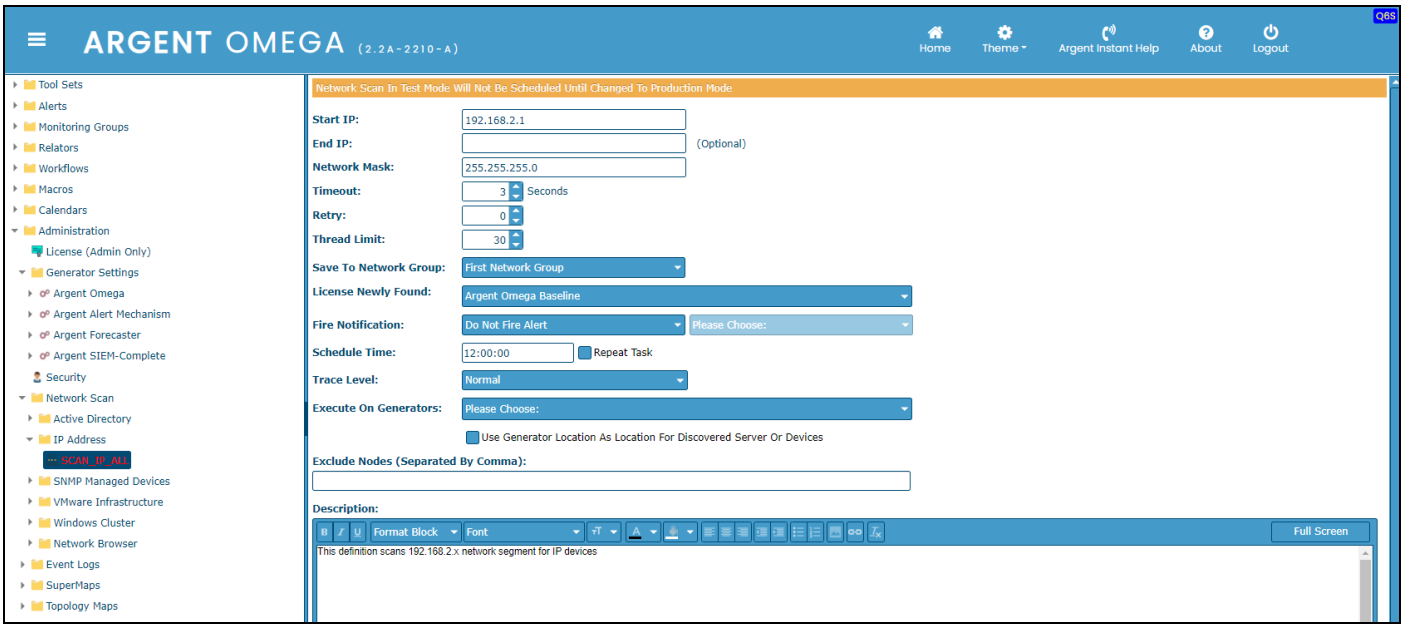
Define this scan to search devices in Active Directory.

Argent Omega provides for repeating the scan at specific intervals by defining a schedule.



IP Address

Define this scan to search devices in a specified IP address range.

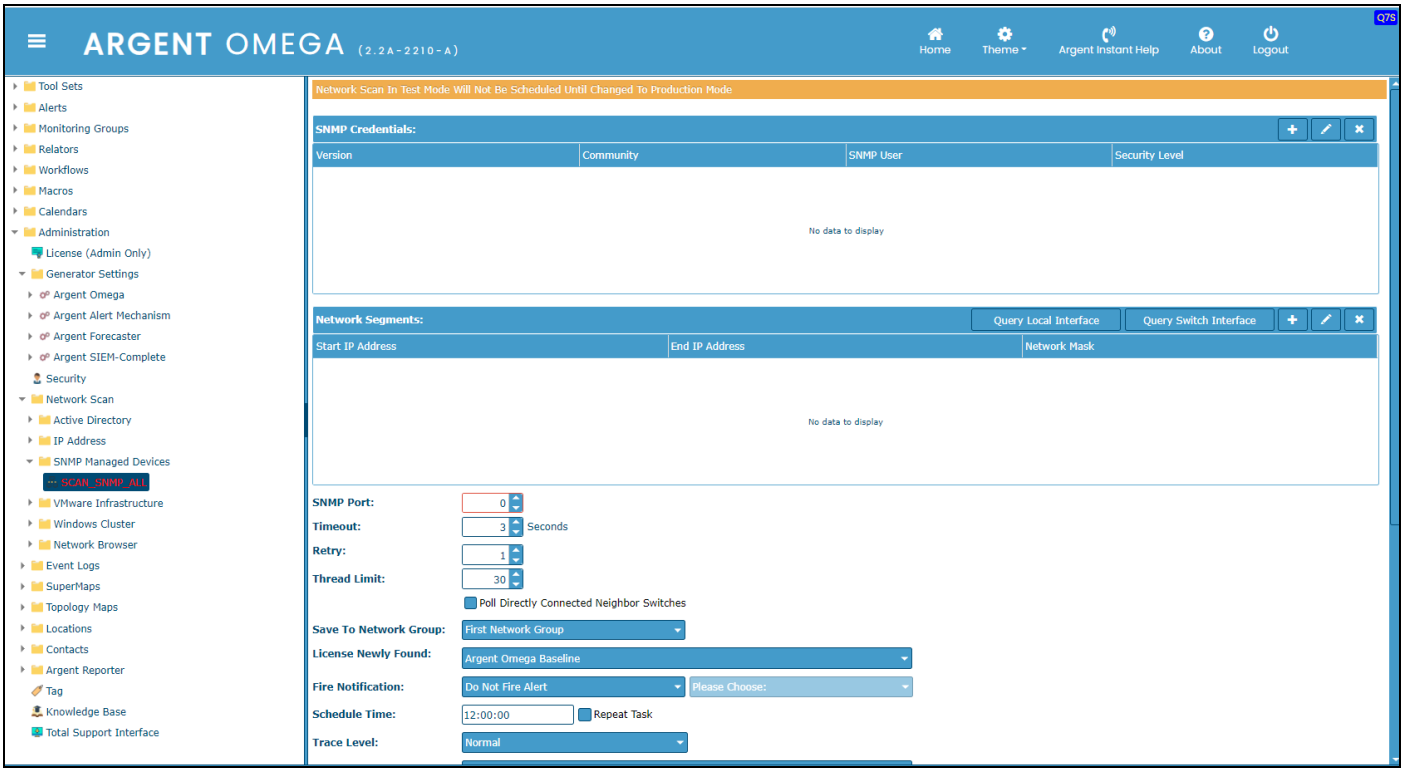


Proprietary Information – All Rights Reserved

SNMP Managed Device

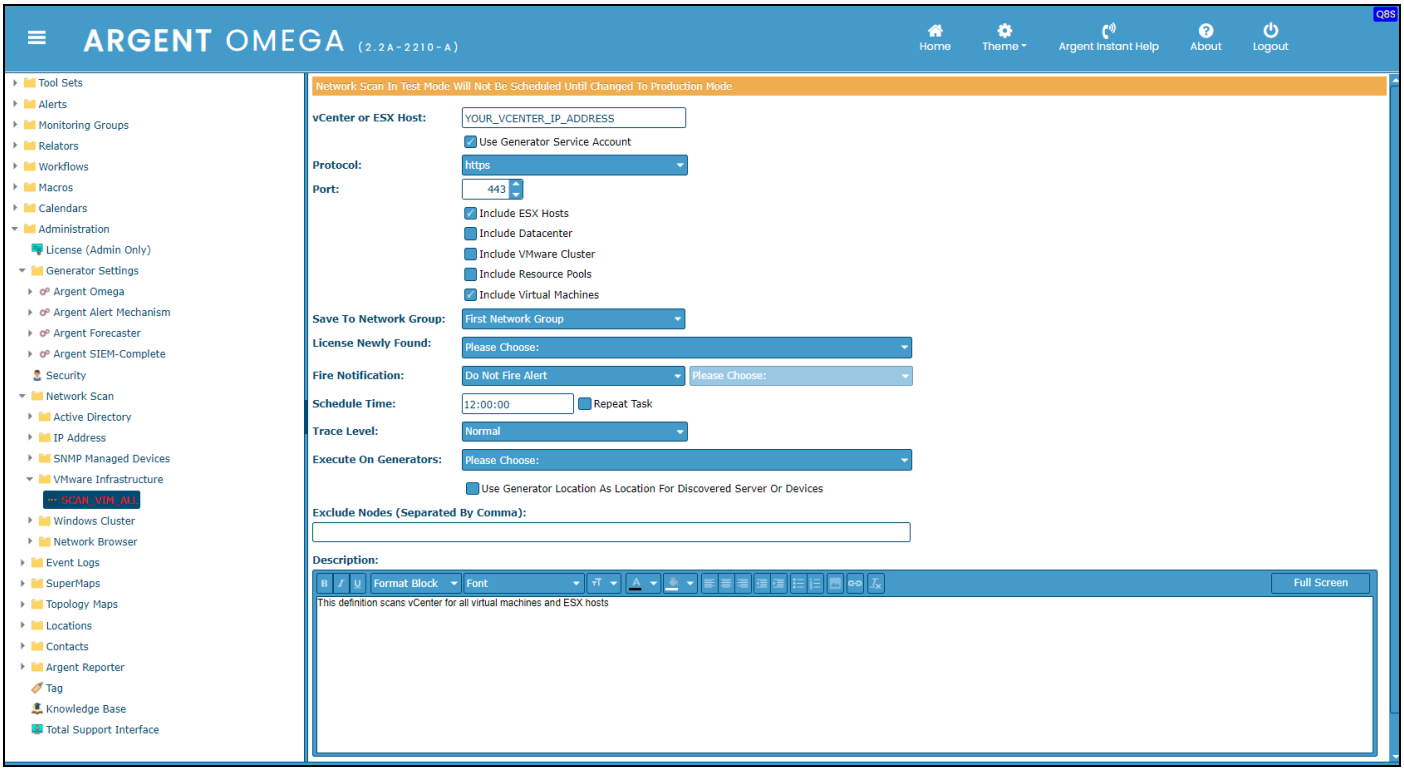
Define this scan to search SNMP-enabled devices in a network.

Users have the option to specify an IP address range to search for SNMP-enabled devices in a specific IP address range.



VMware Infrastructure

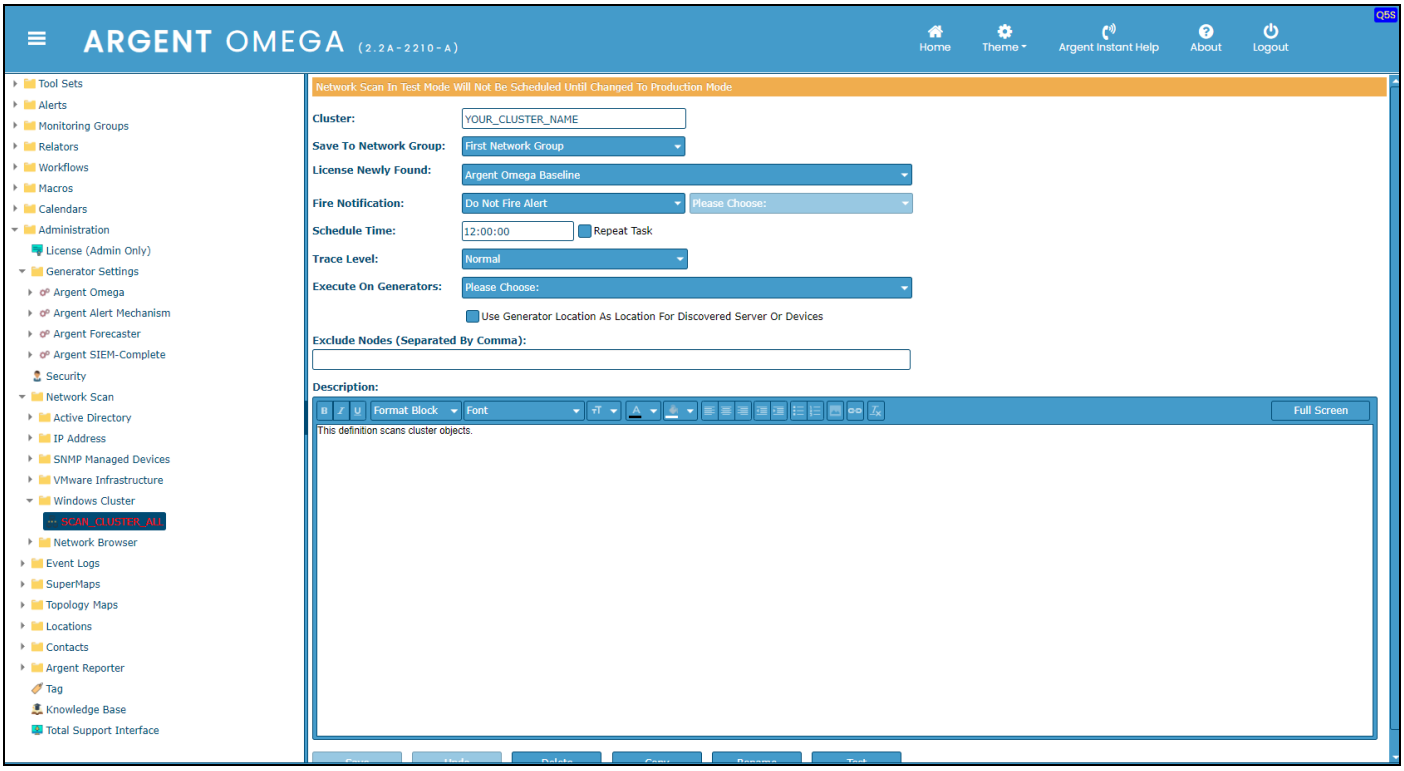
This definition scans vCenter for all Virtual Machines and ESX hosts.



Proprietary Information – All Rights Reserved

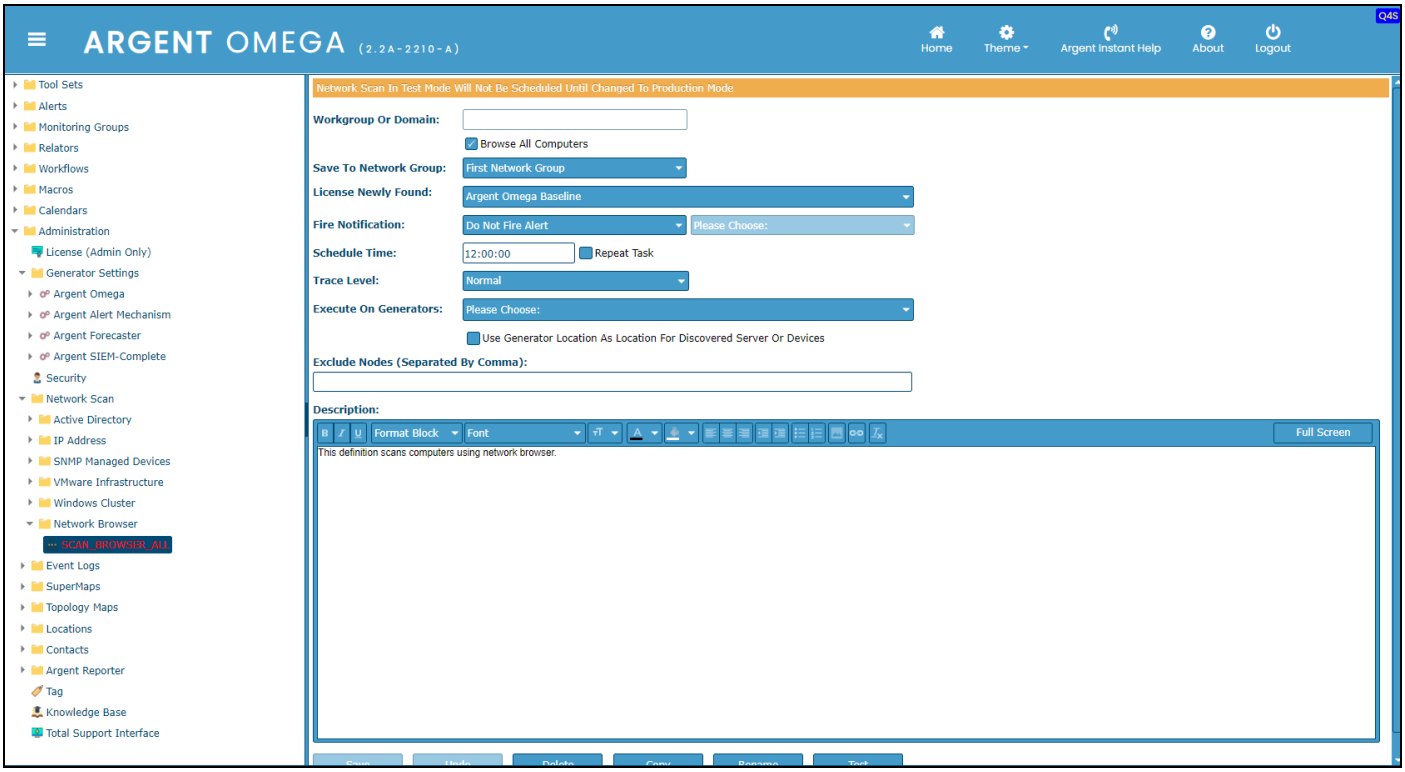
Windows Cluster

This definition scans servers or devices in a Windows Cluster environment.



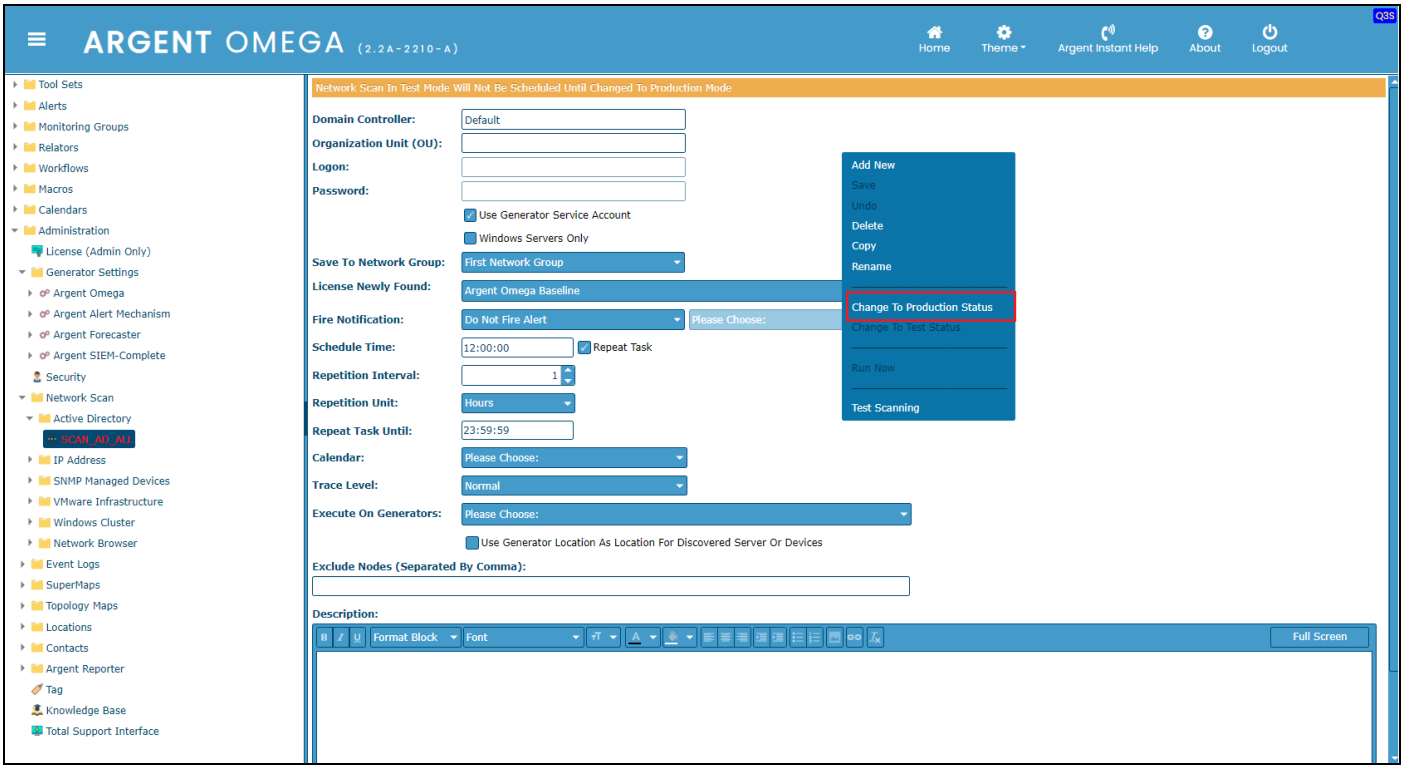
Network Browser

This definition scans computers using network browser.



Proprietary Information – All Rights Reserved

Change the scan definition to Production Mode to execute the scanning as per the schedule.



Proprietary Information – All Rights Reserved

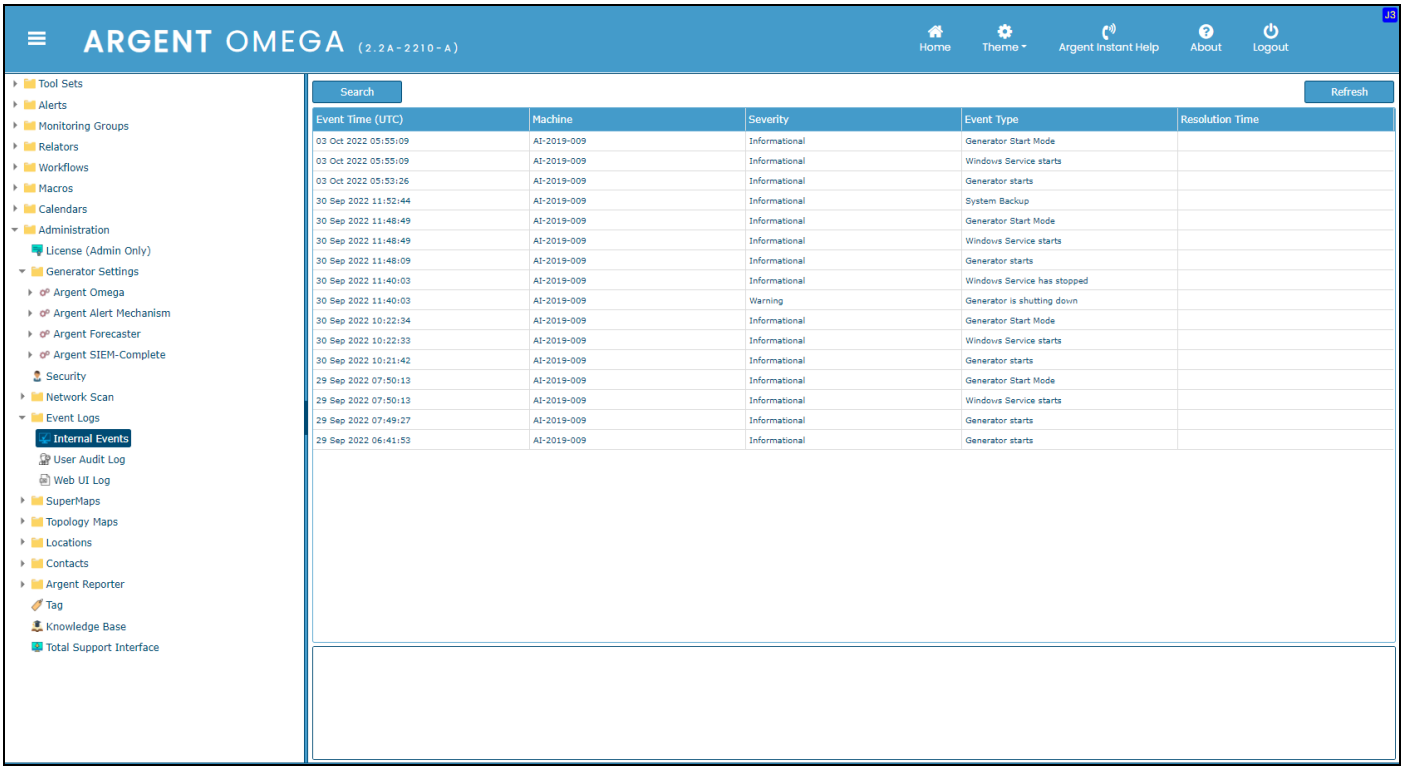
Event Logs

The Event Logs screen provides details on the following:

- Internal Events
- User Audit Log
- Web UI Log

Internal Events

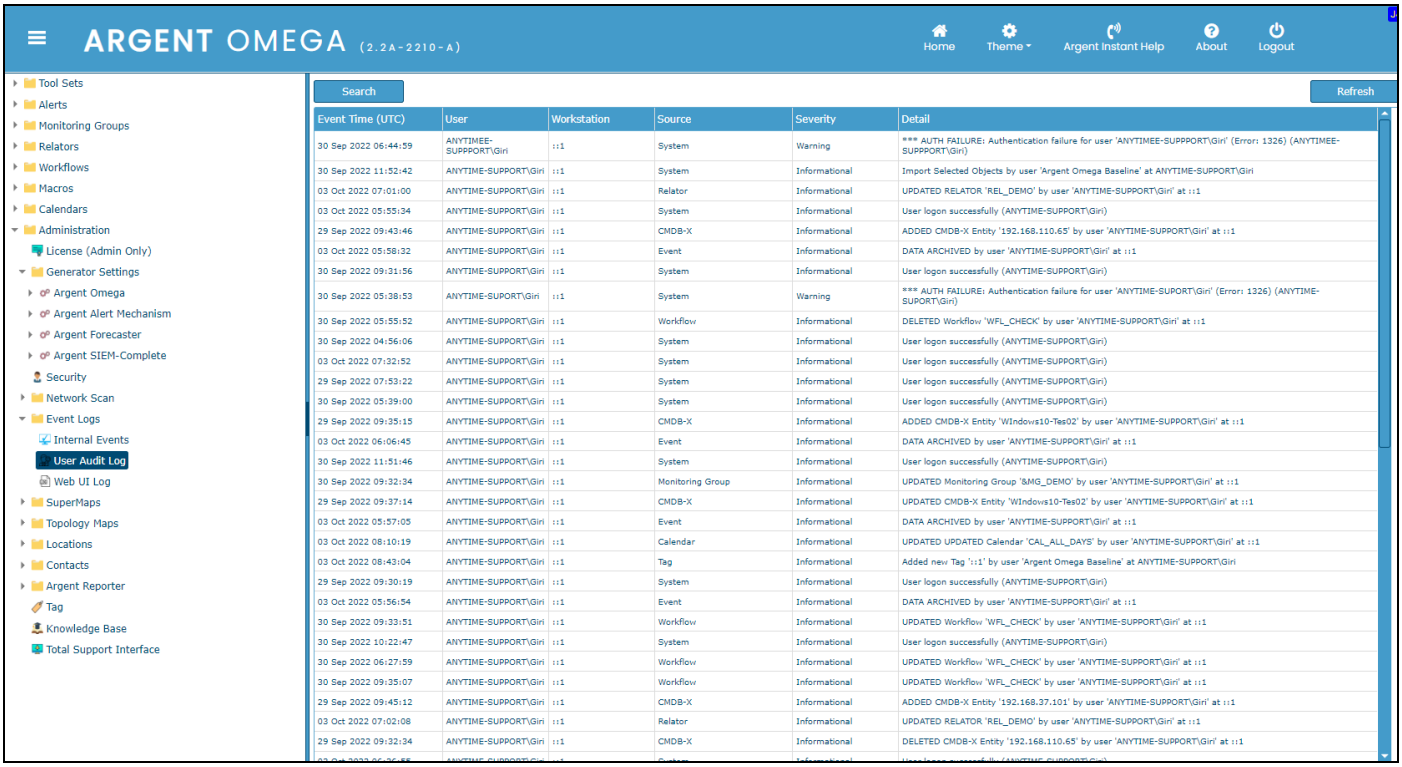
The Internal Events screen lists the internal events that occurred in the Argent Omega environment. Filtering options are provided to search the list by Machine, Severity and Event Type.



Proprietary Information – All Rights Reserved

User Audit Log

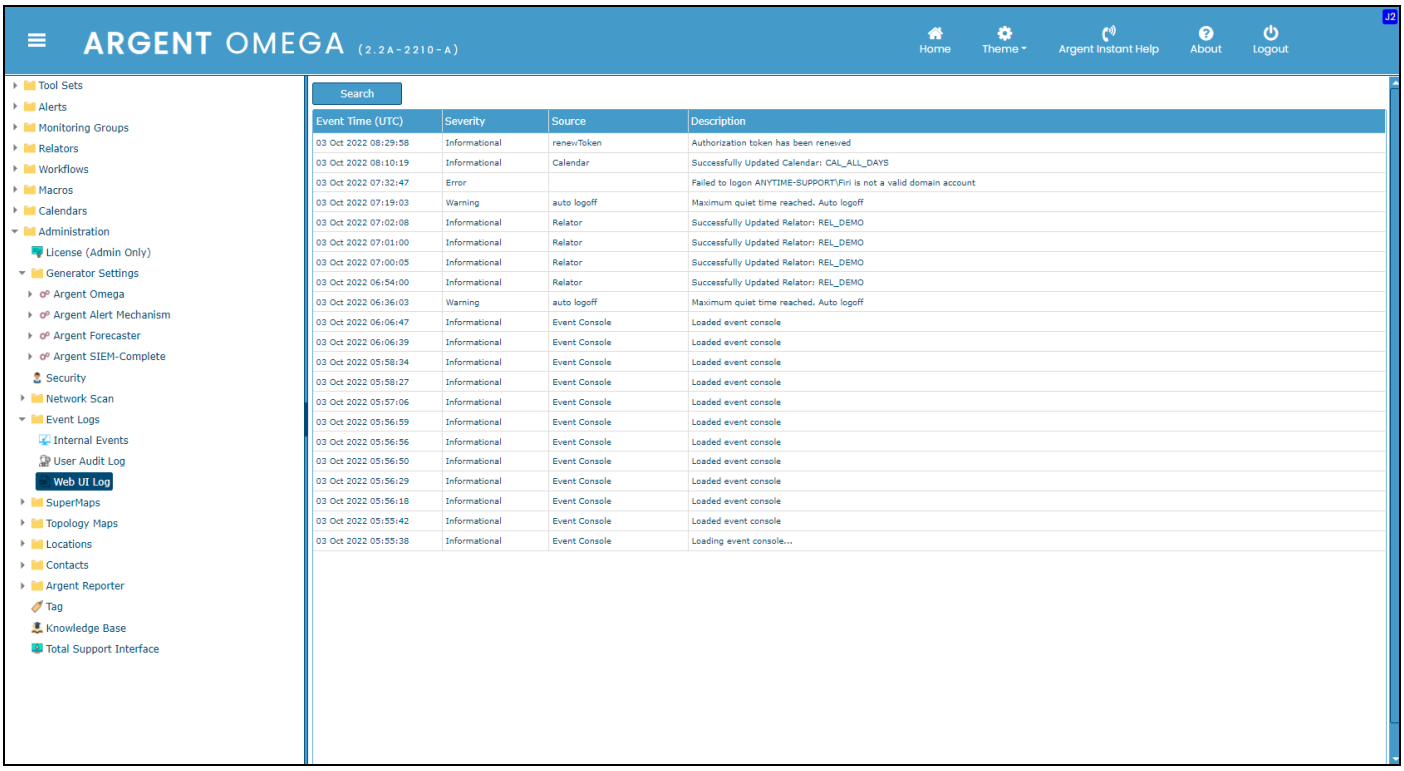
The User Audit Log screen lists the Argent Omega user events. Filtering options are provided to search the list by User, Workstation, Source and Severity type.



Web UI Log

The Web UI Log screen lists the Argent Omega WUI events.

Filtering options are provided to search the list by Severity, Source and Description.



Proprietary Information – All Rights Reserved

Argent SuperMaps Or Topology Maps

These Maps are network diagrams that show the selected devices; there are of three types:

- **Optional Google Maps**

  When using Google Maps, Argent Omega automatically marks the selected devices in Google Maps, provided the locations are defined and correctly assigned to the device. A Google license is required.

- **Static Map**

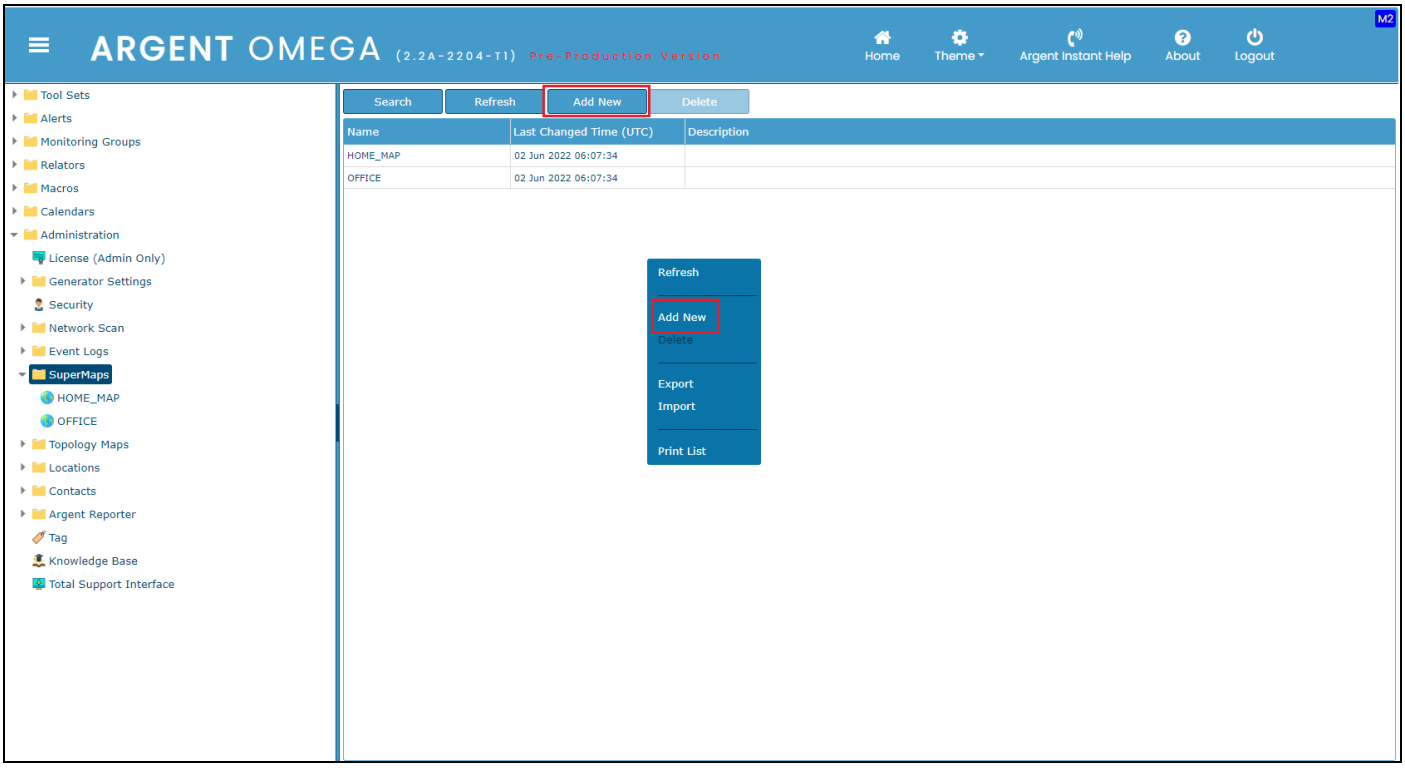
  Using a static map, an image available in the server can be used to specify the location of the devices manually

  Empty Map

  When using an empty map, no background appears for the map. The size of the map can be selected from the available sizes in the drop-down combo

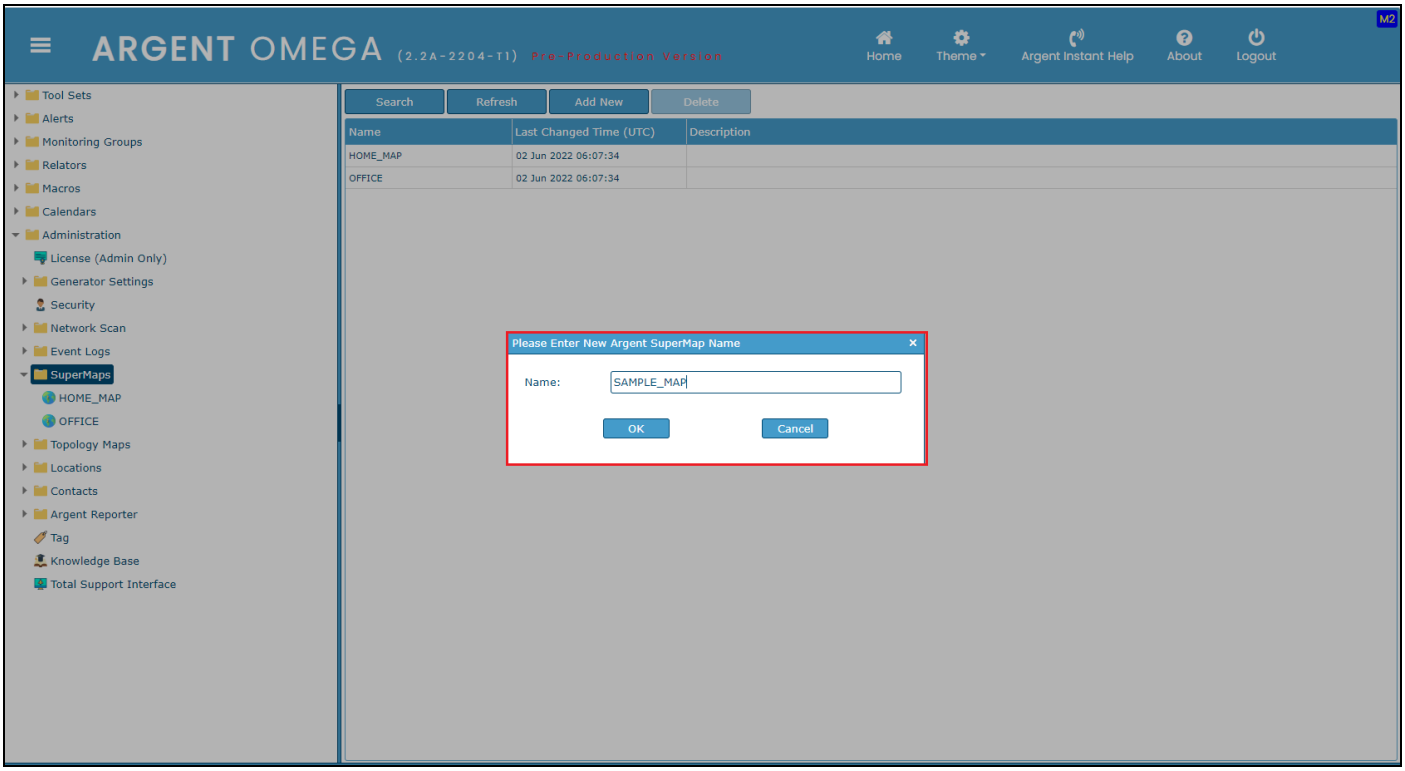
Add New Map

A new map can be created using **"Add New"** in the right-click menu item or the button on top of the **"Group folder's"** list screen.



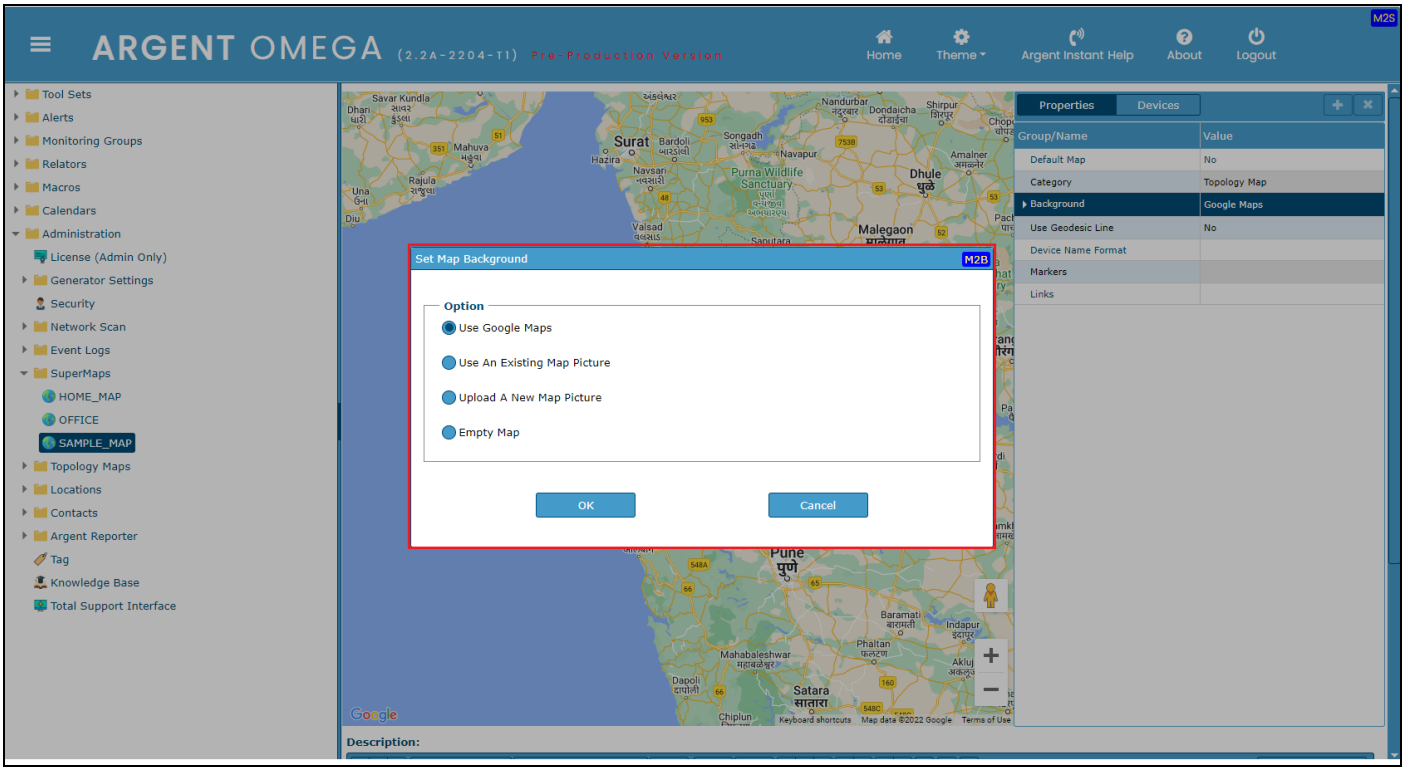
Proprietary Information – All Rights Reserved

The Map name can be specified in the sub-window that pops up.



Set Map Background

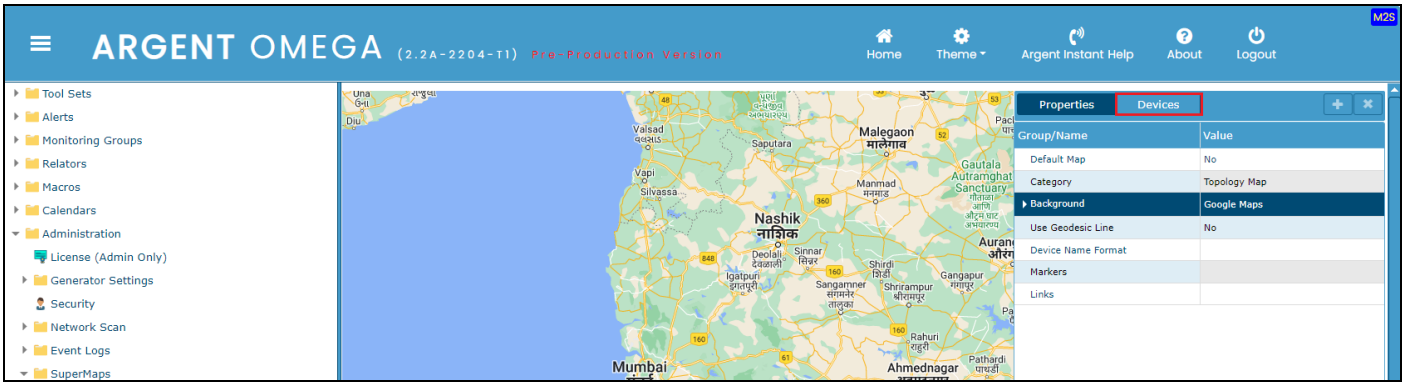
Double clicking the **"Background"** field in the Properties window, pops up the sub-window "**Set Map Background**." This option can edit an existing Map or define a new Map. The sub-window contains options to choose Google Map, Static Map, or an Empty Map. If the choice is for a static Map, either an existing Map can be selected, or a new one can be uploaded. If the choice is for an empty Map, the size of the map can be selected from the drop-down combo.



Adding Devices To Google Maps

The optional Google Maps can only be used when the Locations are properly defined for the Network devices.

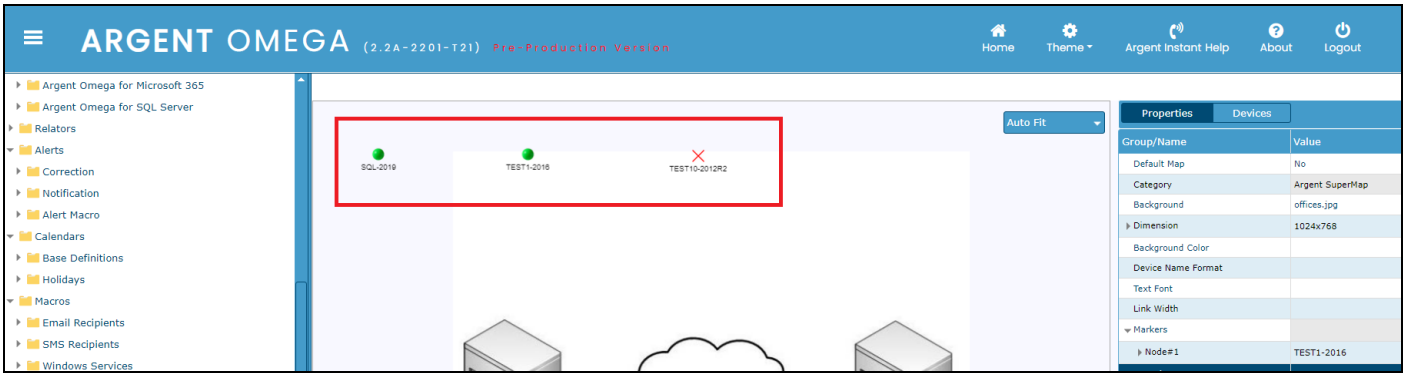
To add a device to the map, select the device list, pick the device from list, then click on **"+"** button.
If it is a Google Map, the device's location property determines the device dot on the map.



The application also supports the selection of multiple devices and adding them to the Map in one click.
A combination of (Shift or Ctrl + left mouse click) can be used for multiple selections.

Adding Devices To Static Map

Listed devices can be added to a Static Map similarly to the way they are added to a Google Map. The difference is that the location of the device should be manually positioned. This can be done using drag and drop of the **"X"** mark or by specifying the X and Y coordinates in the Properties window.

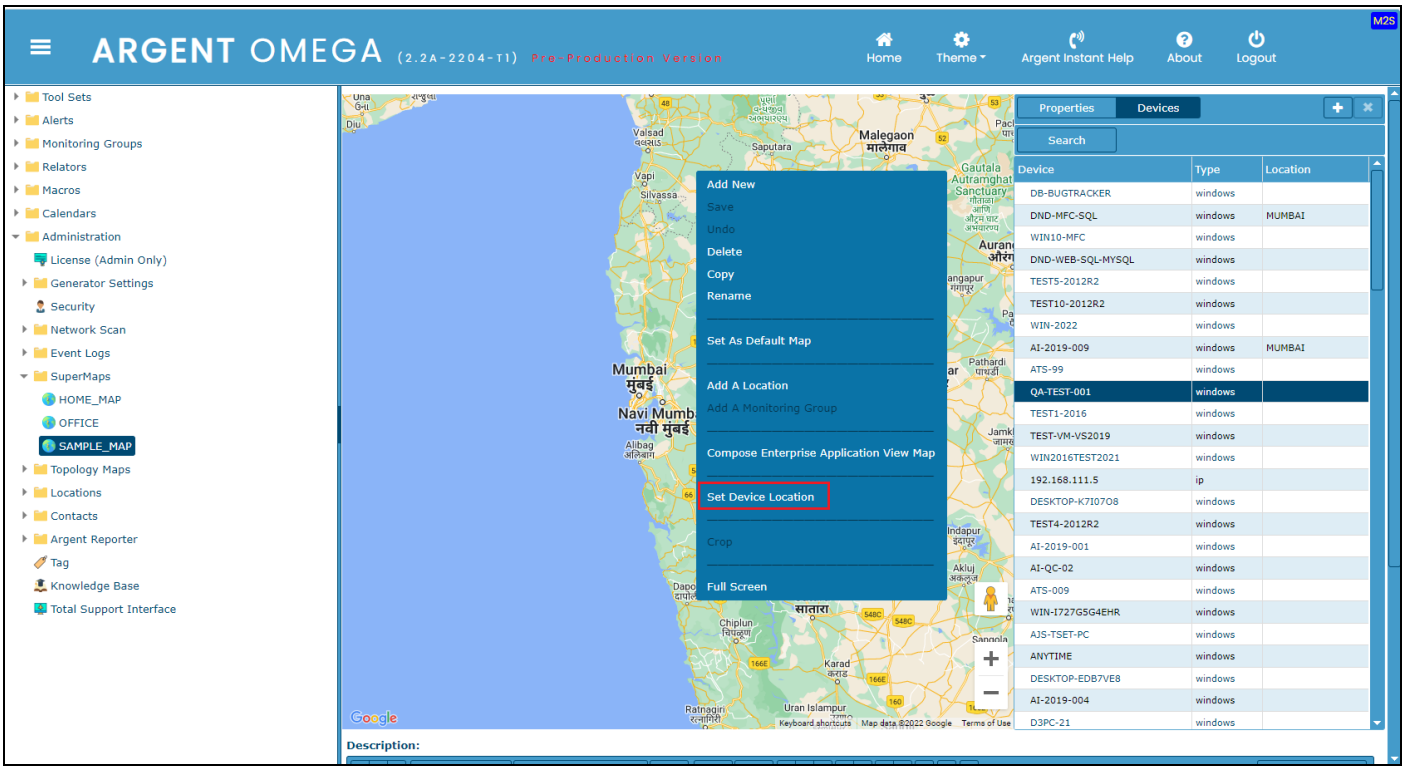


Multiple devices can be added to the Static Map through multiple selection. Even when multiple devices are added to the Map, their position of each device is set individually.

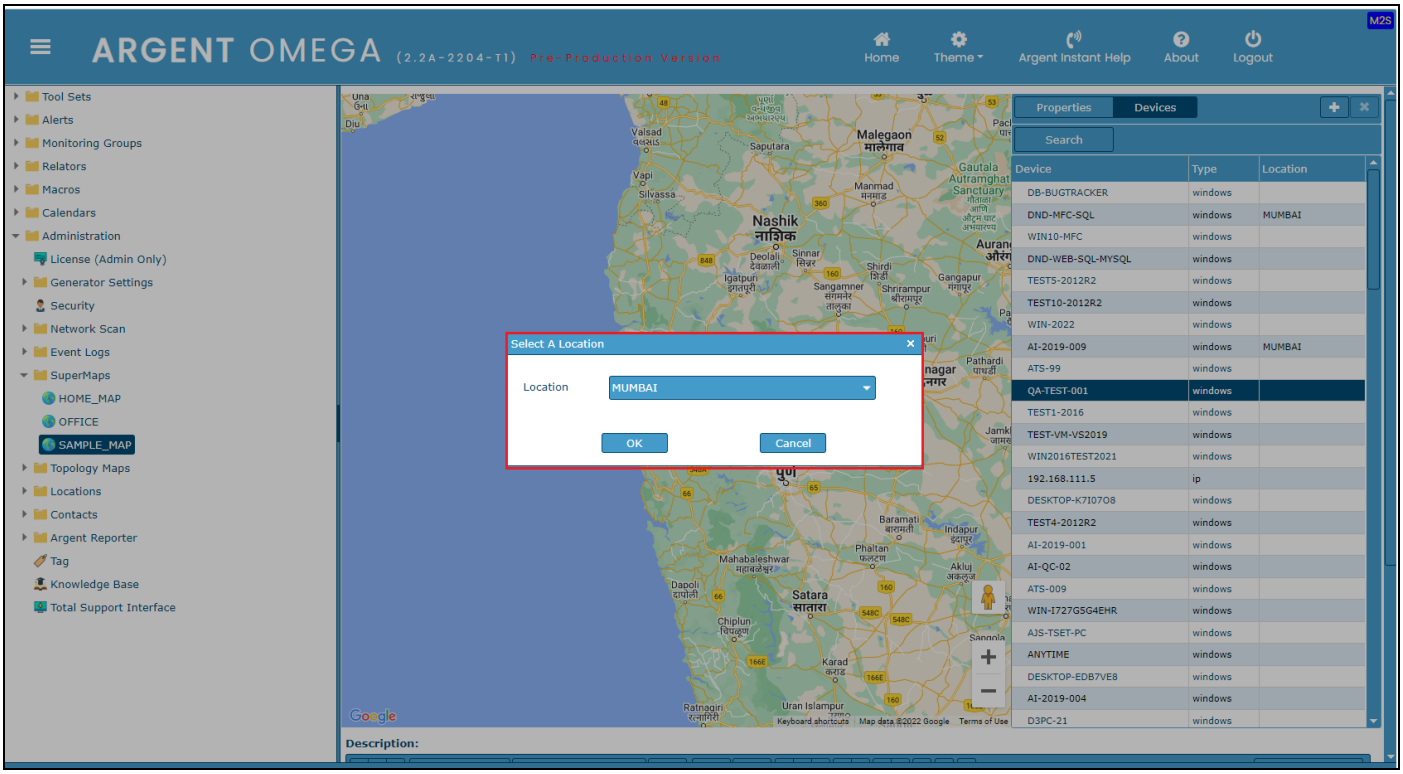
Proprietary Information – All Rights Reserved

Set Device Location

To set the location of the device, select the device from the list under the **“Devices”** tab and either use the right-click menu item “**Select Device Location”** or double click the selected device.



A sub-window pops up to enter or edit the device location.

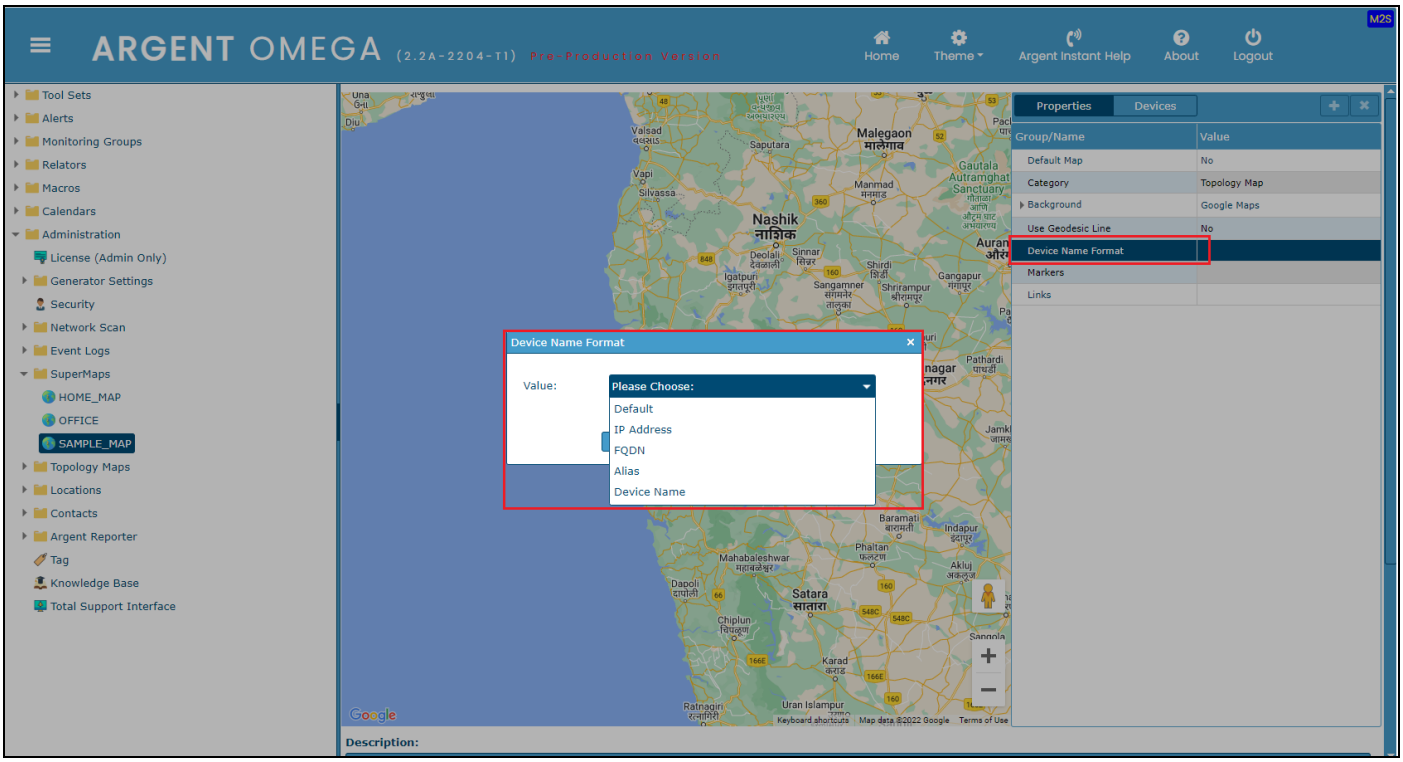


Device Name Format

The Properties tab of the Map definition has a field “**Device Name Format**.” This field allows setting the name format by which the device should be displayed in the Argent SuperMaps or Topology Maps home screen.

The Available options are:

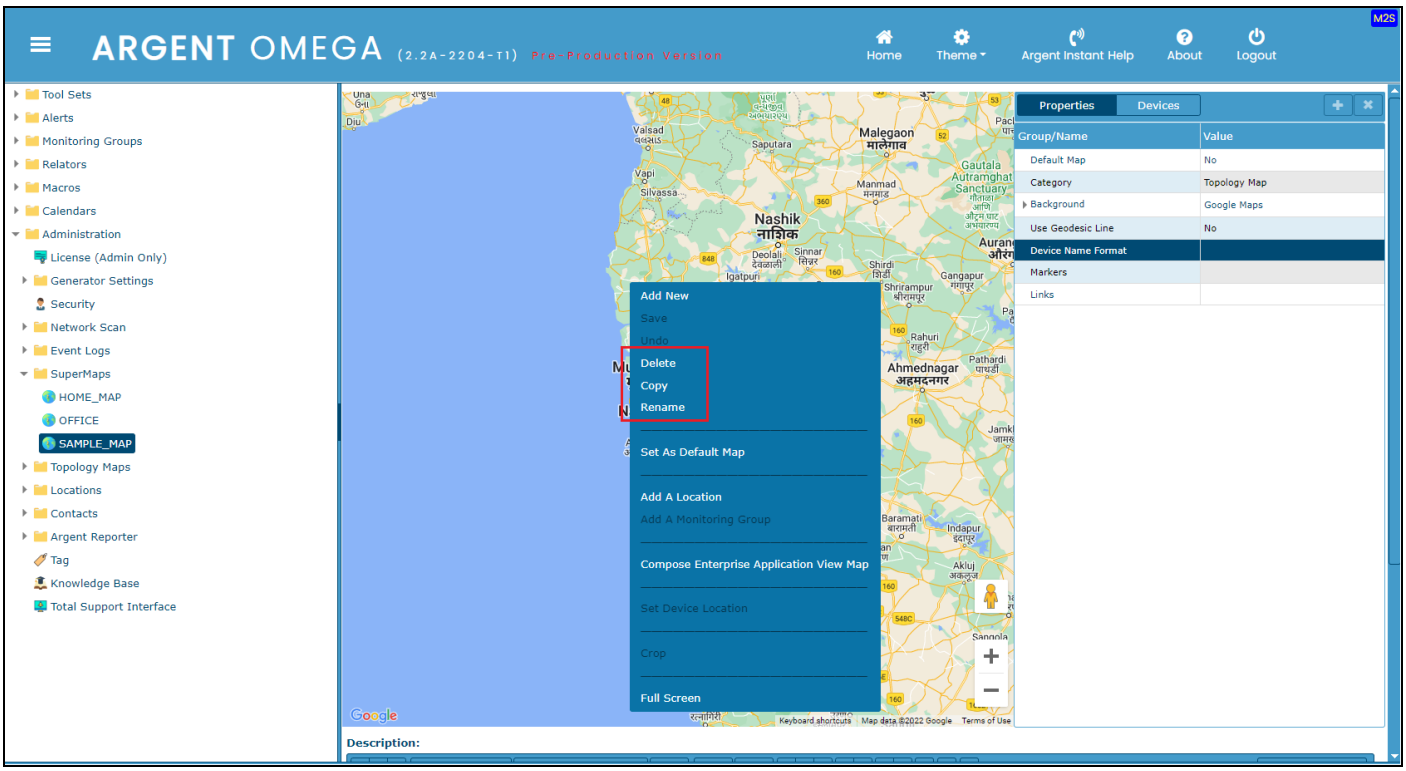
- Default
- IP Address
- Full Qualified Domain Name (FQDN)
- Alias



Delete, Copy Or Rename

The option to delete, copy or rename the Map definition is available in the right-click menu.

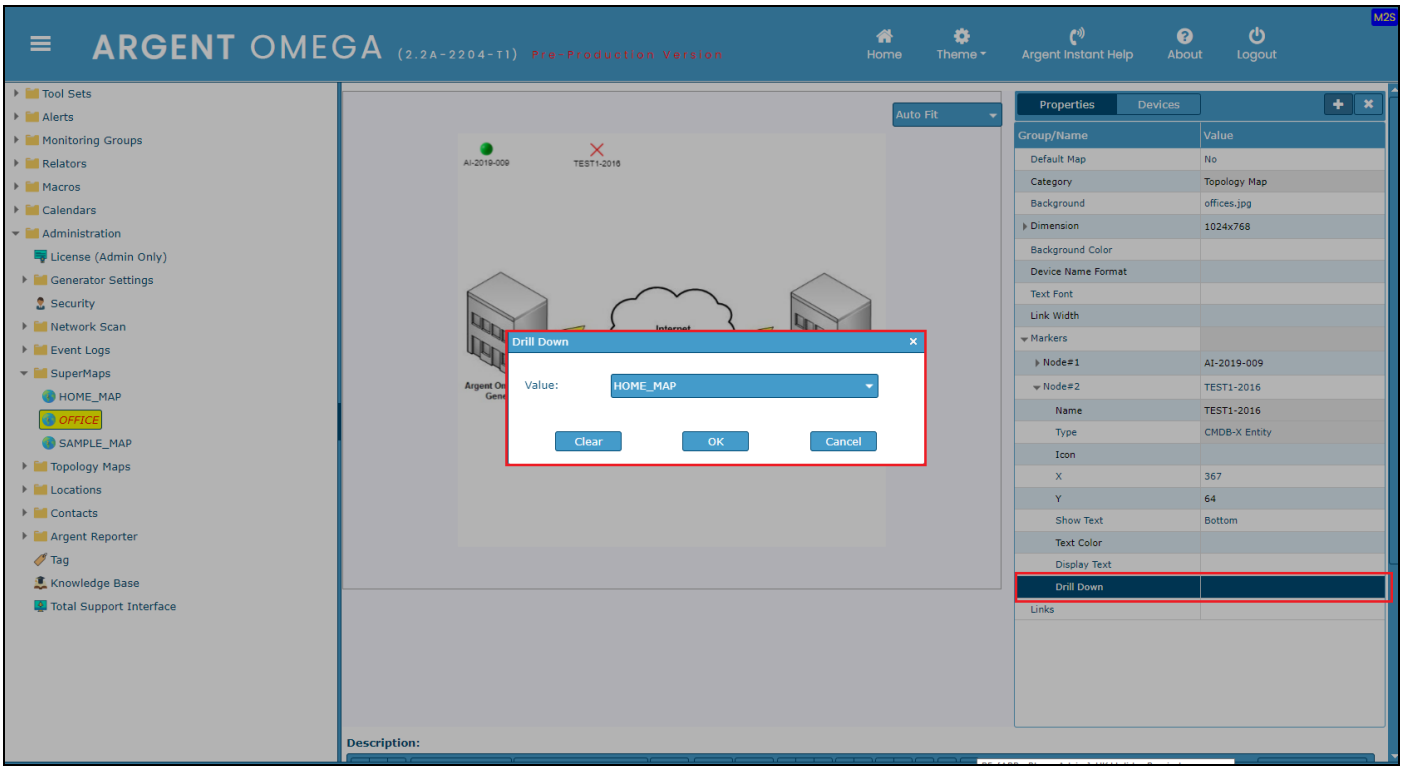
Proprietary Information – All Rights Reserved



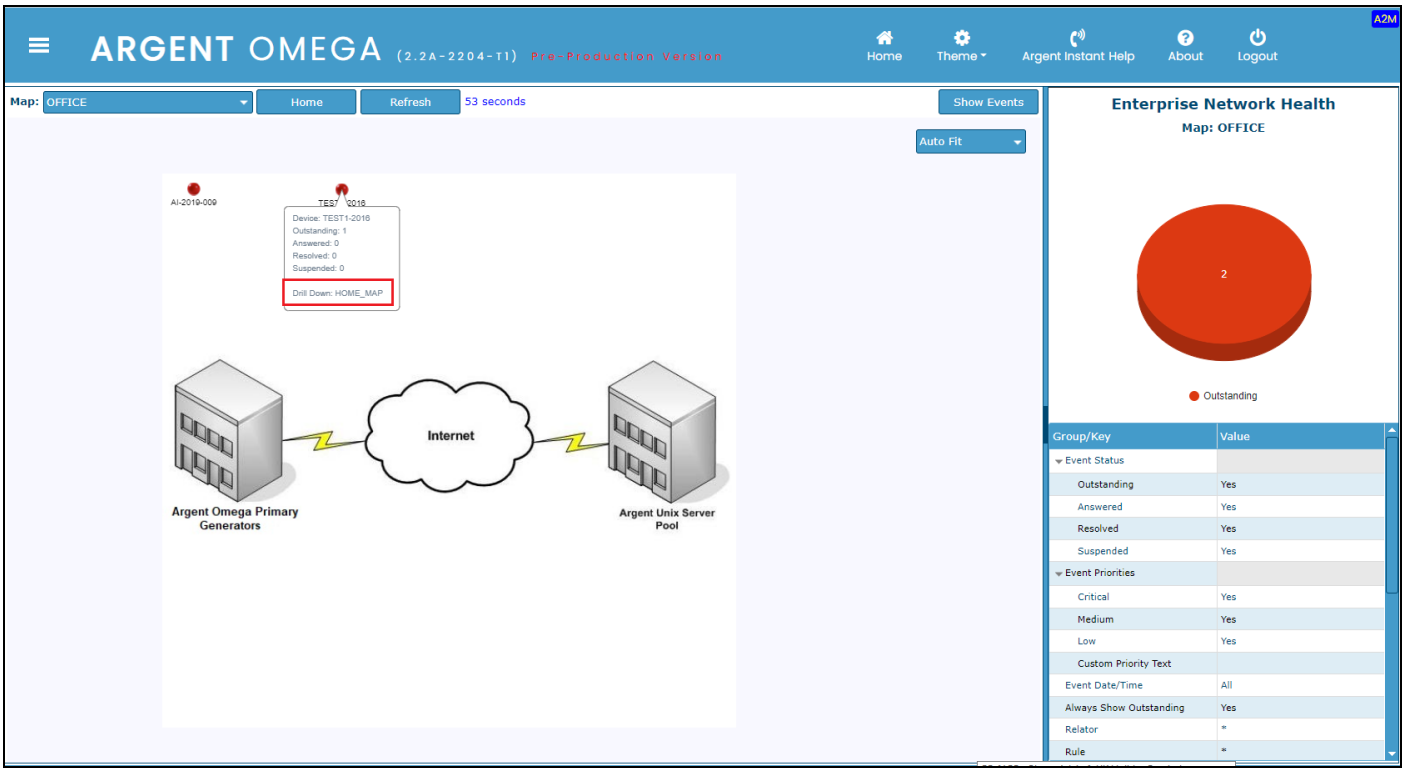
Proprietary Information – All Rights Reserved

Drill Down

Map definitions provide a drill down option. The “**Drill Down” option** in Properties allows specifying another Map. Double clicking the property pops up a sub-window from which any defined Map can be selected.



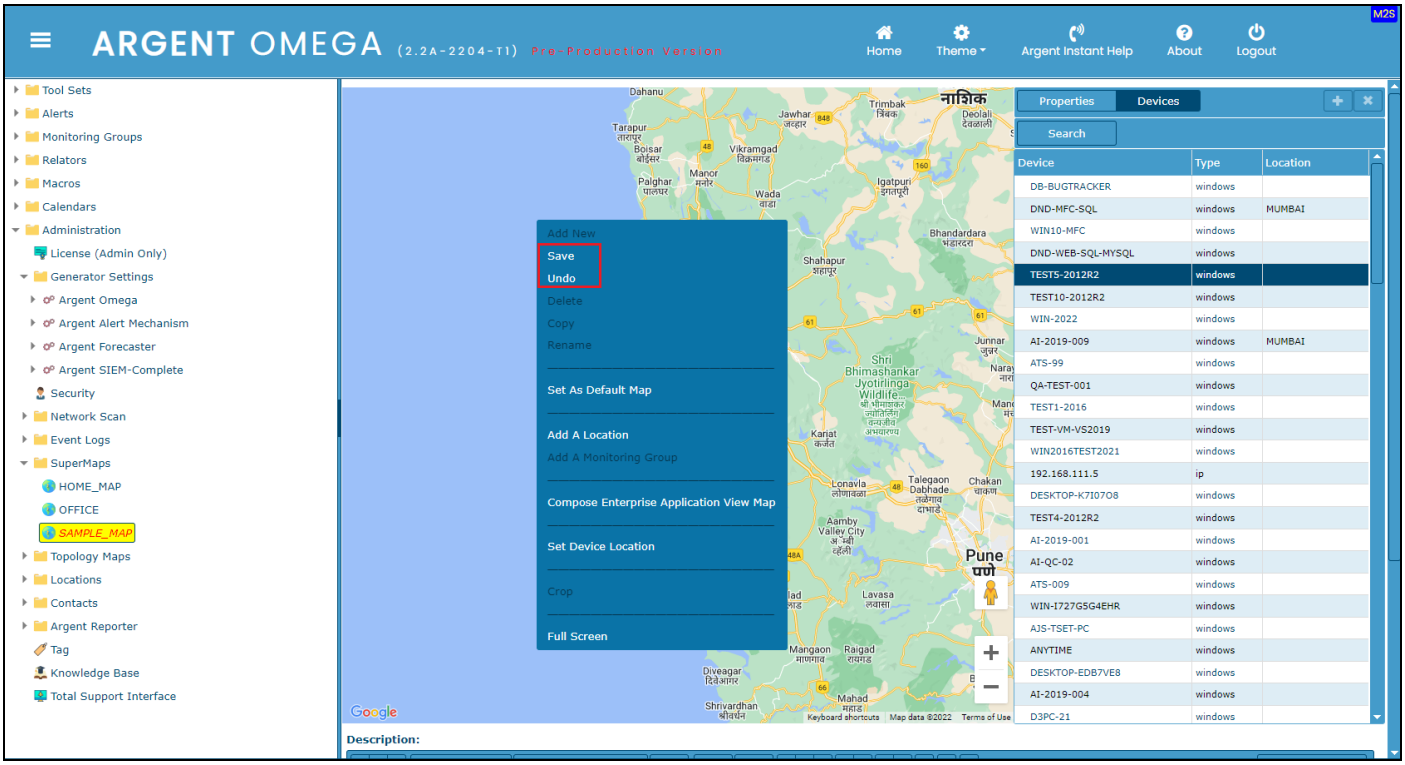
If any Drill Down item is defined for a device, the popup info window in the Home screen will contain a hyperlink. Click on the hyper link to get directed to the configured Map.



Proprietary Information – All Rights Reserved

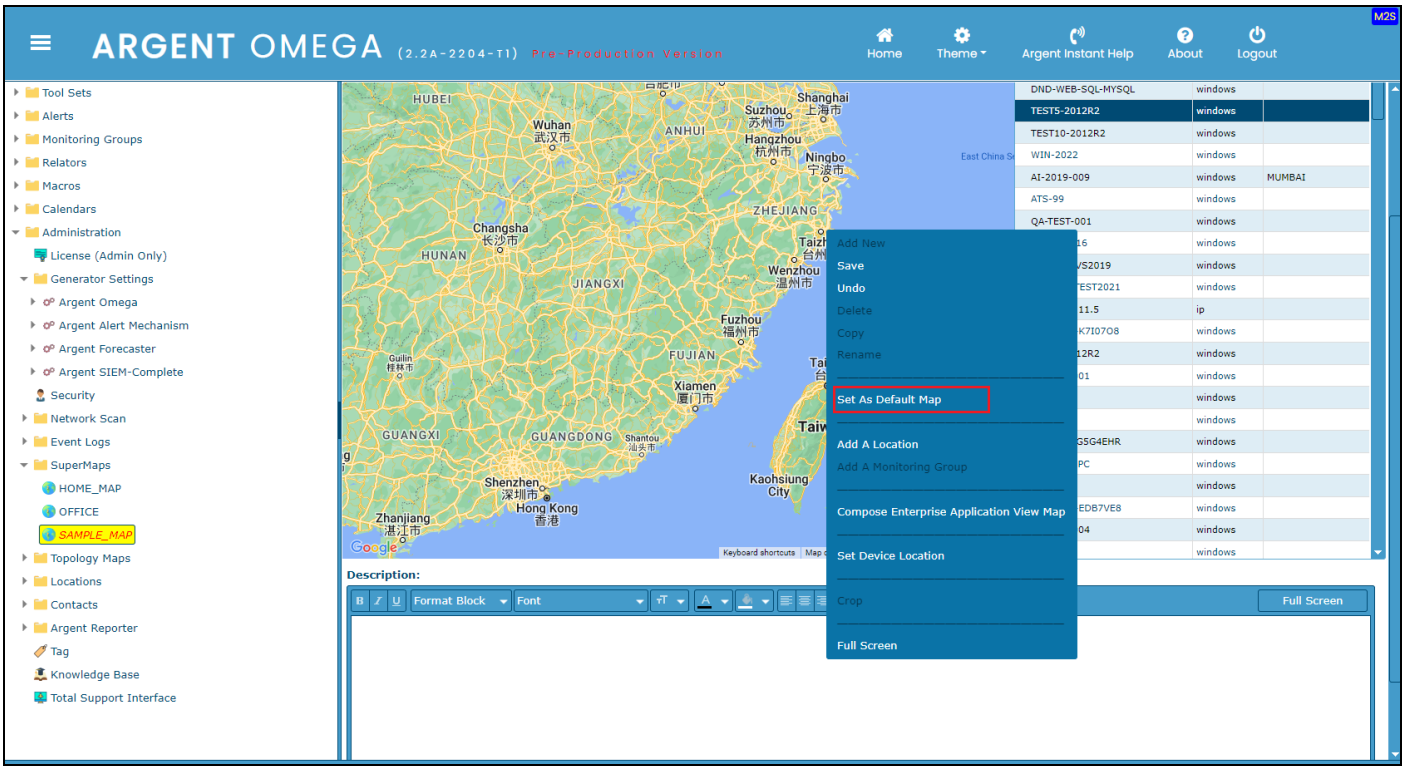
Save And Undo

The changes made in the Map definition should be saved or undone before one can traverse to another screen. The right-click menu items **“Save”** and “**Undo”** are useful in practice.



Set As Default Map

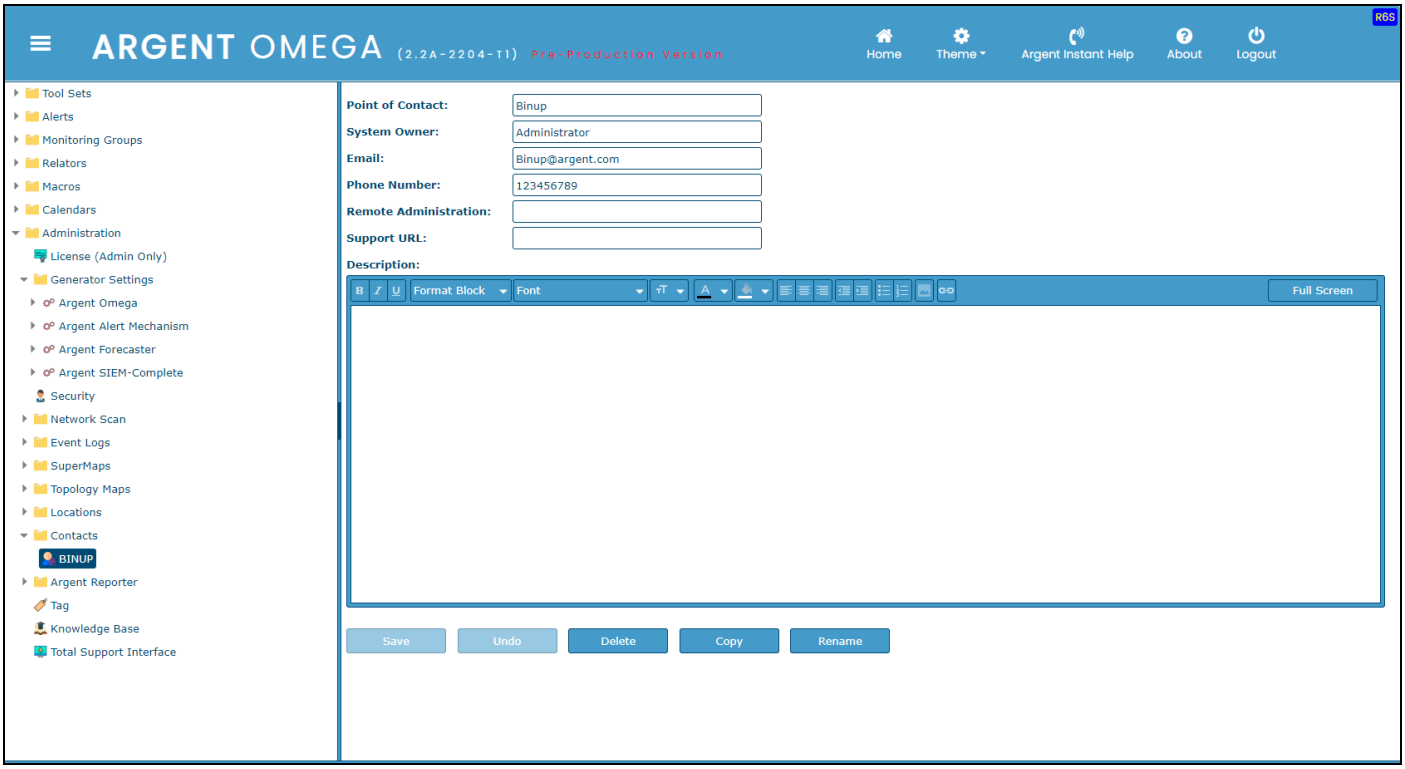
Set the Map as the default Map on the Home screen by using the right-click menu item **“Set As Default Map.”**



Proprietary Information – All Rights Reserved

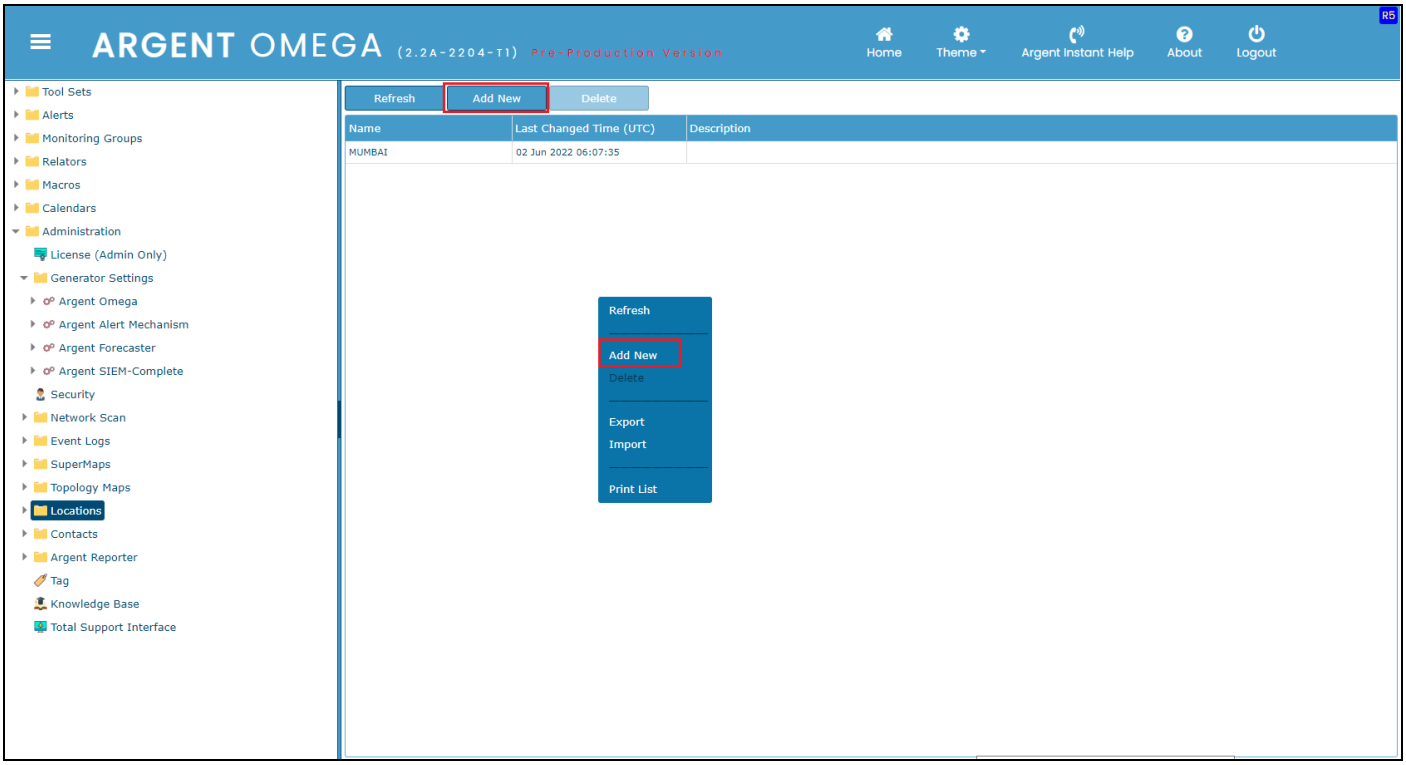
Contacts

Add contact information in Contacts.



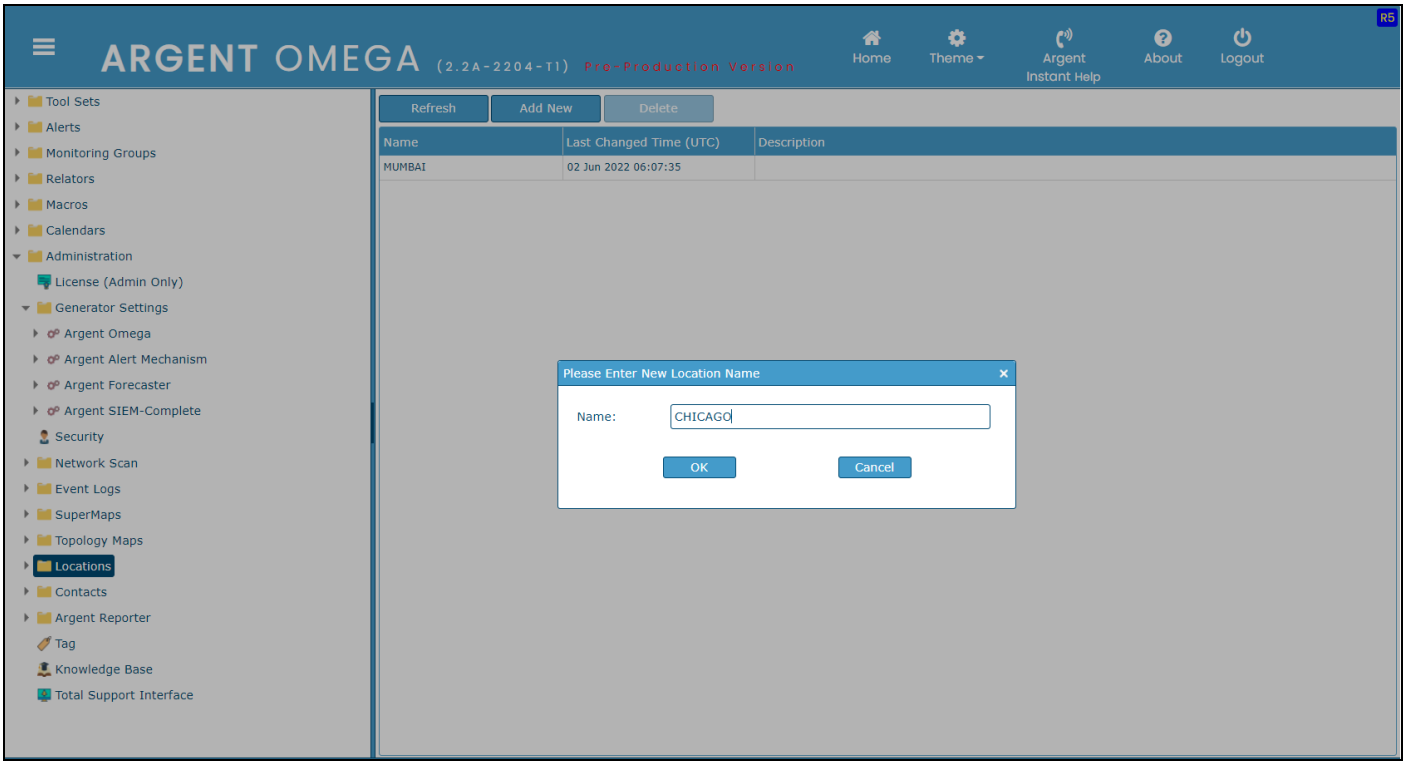
Locations

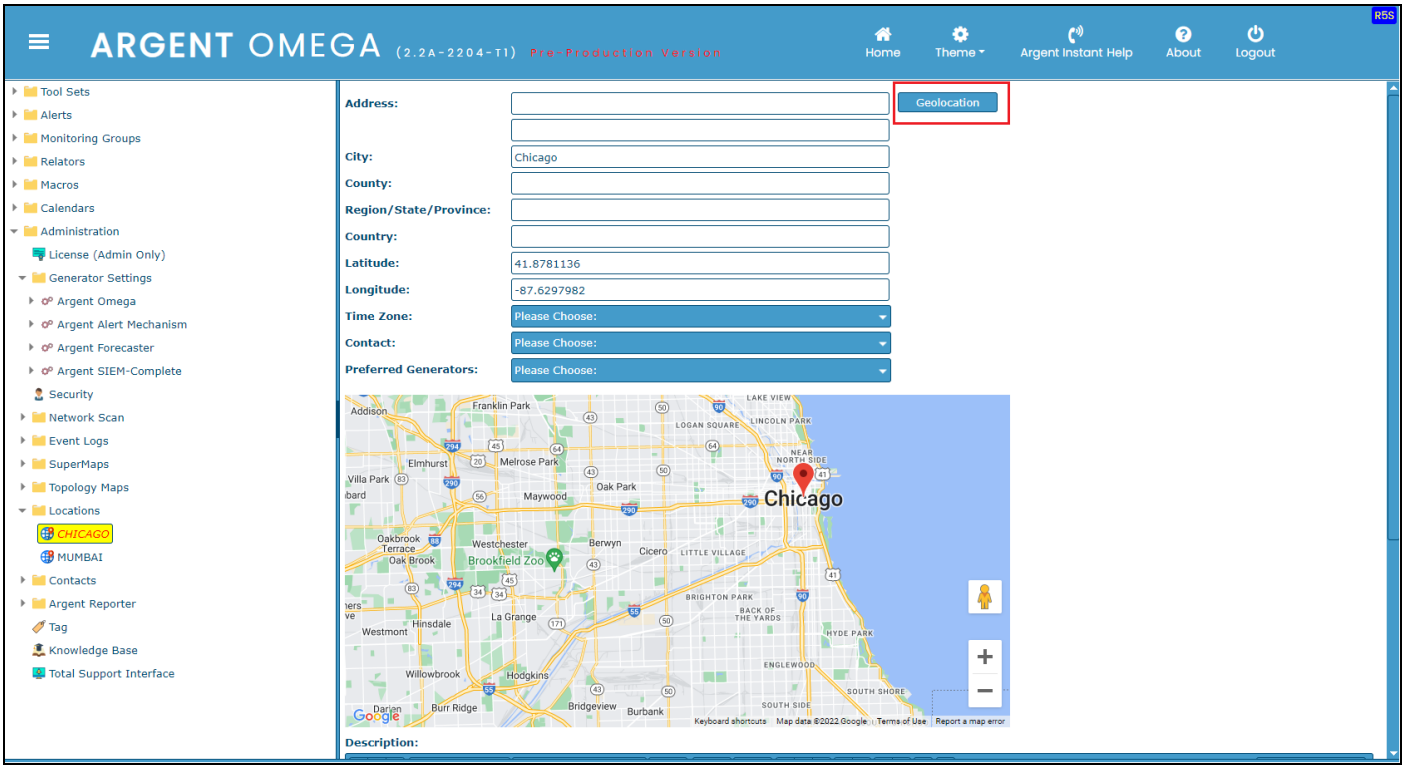
A new location can be created using “**Add New”** in the right-click menu item or the button on top.



Proprietary Information – All Rights Reserved

Enter name of the new location:





It shows geo-locations that can be used for the Location property.

Clicking the "**Geo-Location"** button after specifying the city name yields the **latitude and longitude details.**

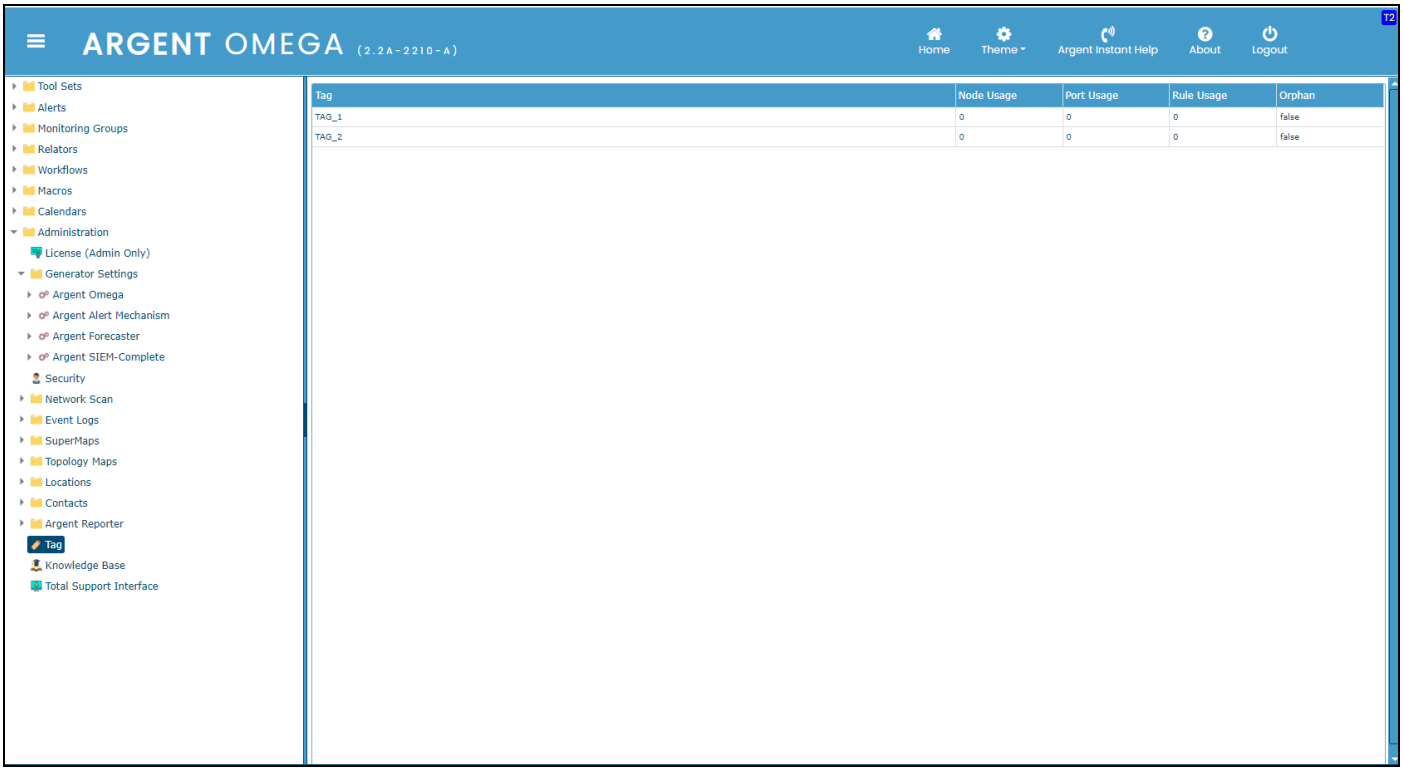
Location definitions are critical when Google Maps is used. A managed device has a **location property**. When it is placed on Google Maps, its longitude and latitude are retrieved from its location.

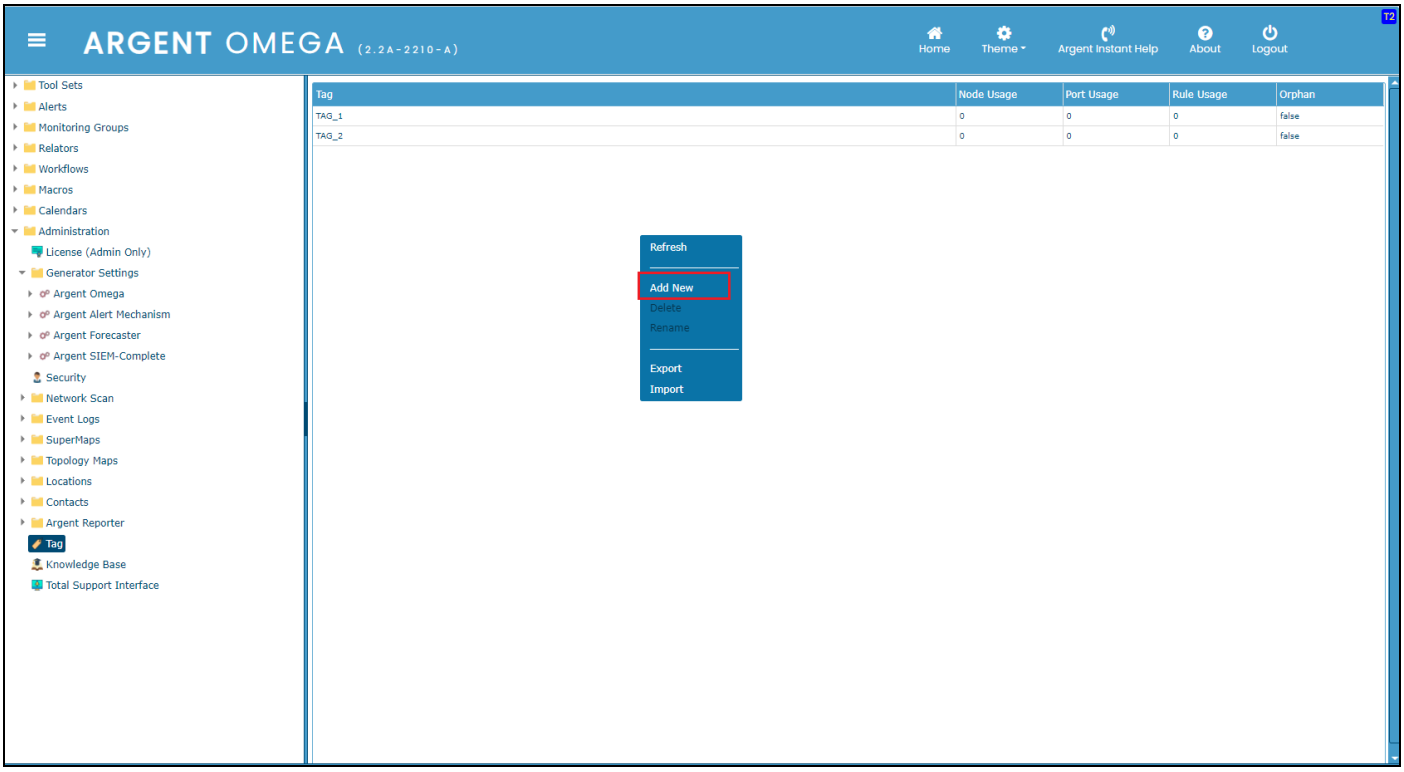
Proprietary Information – All Rights Reserved

Tag

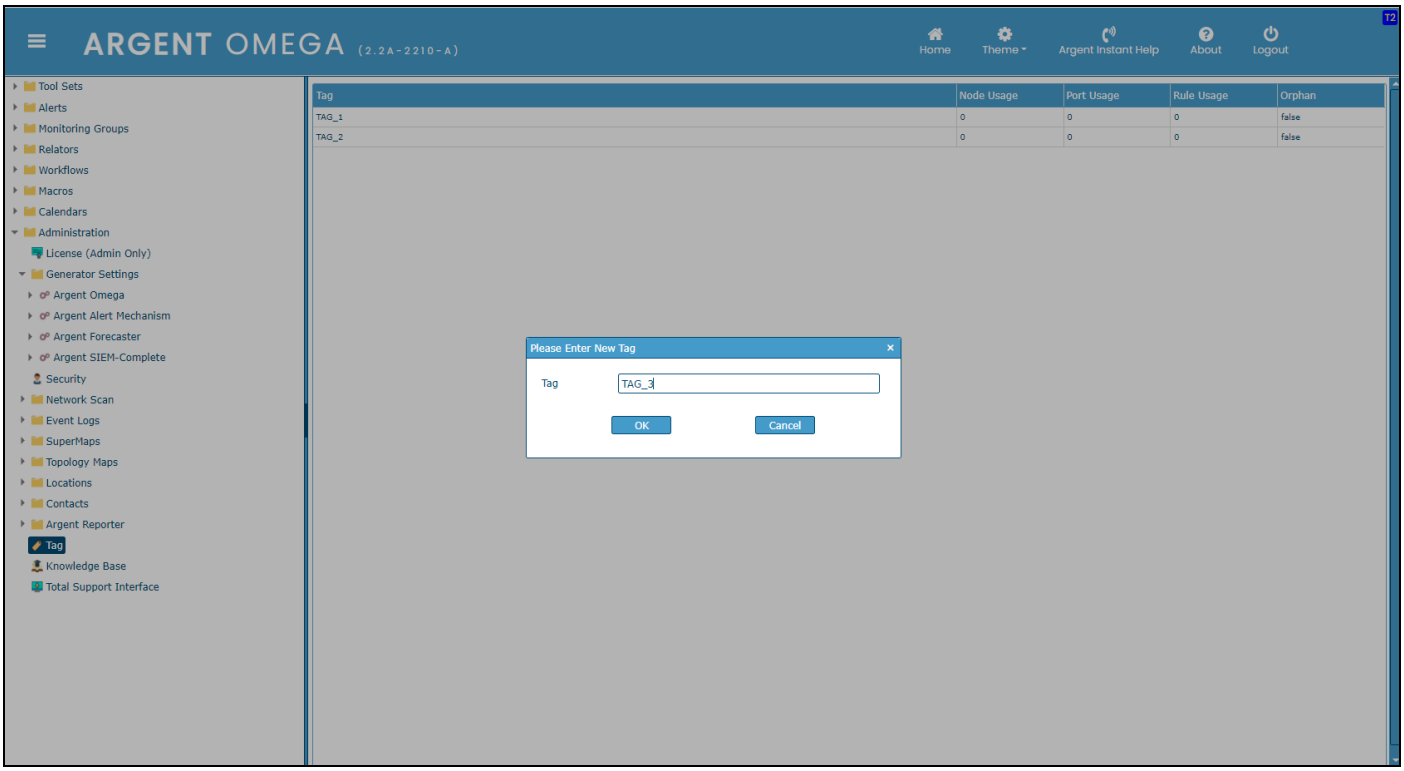
A new Tag for Server or device can be created in Tag screen.

(See Argent KBI Https://Help.Argent.com/#KBI_312001 for more details.)

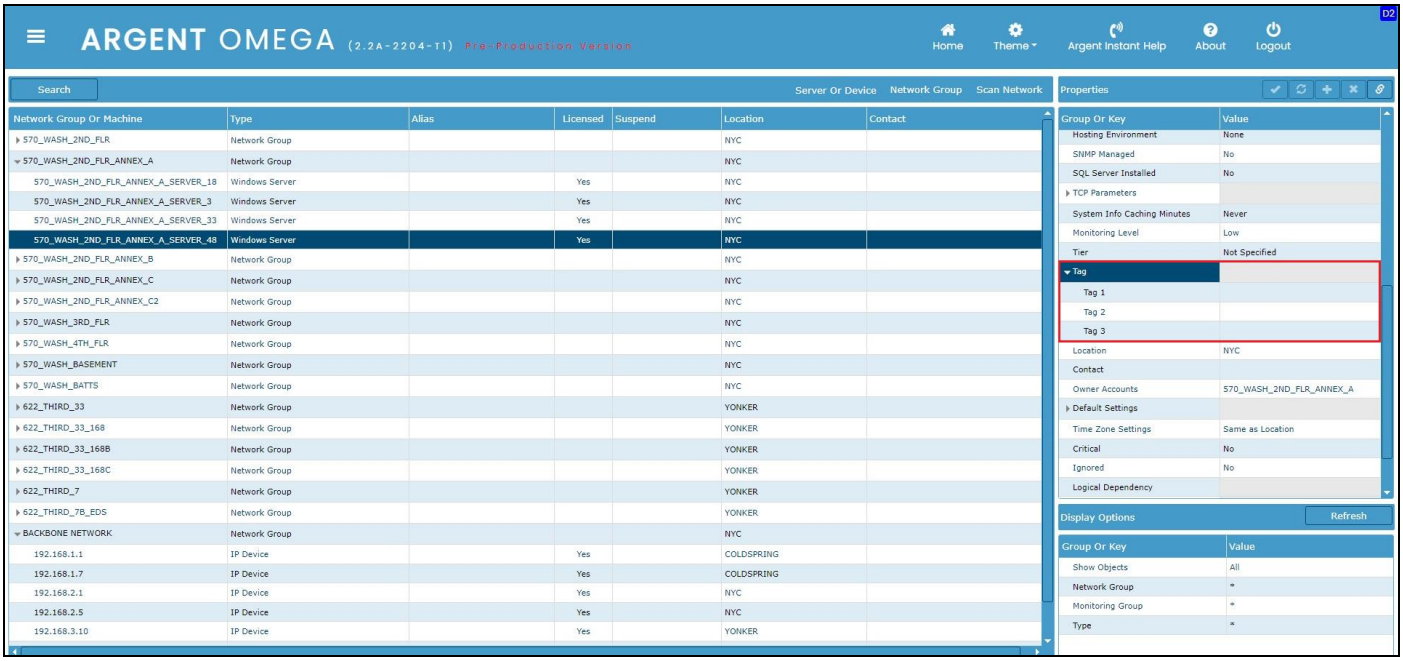




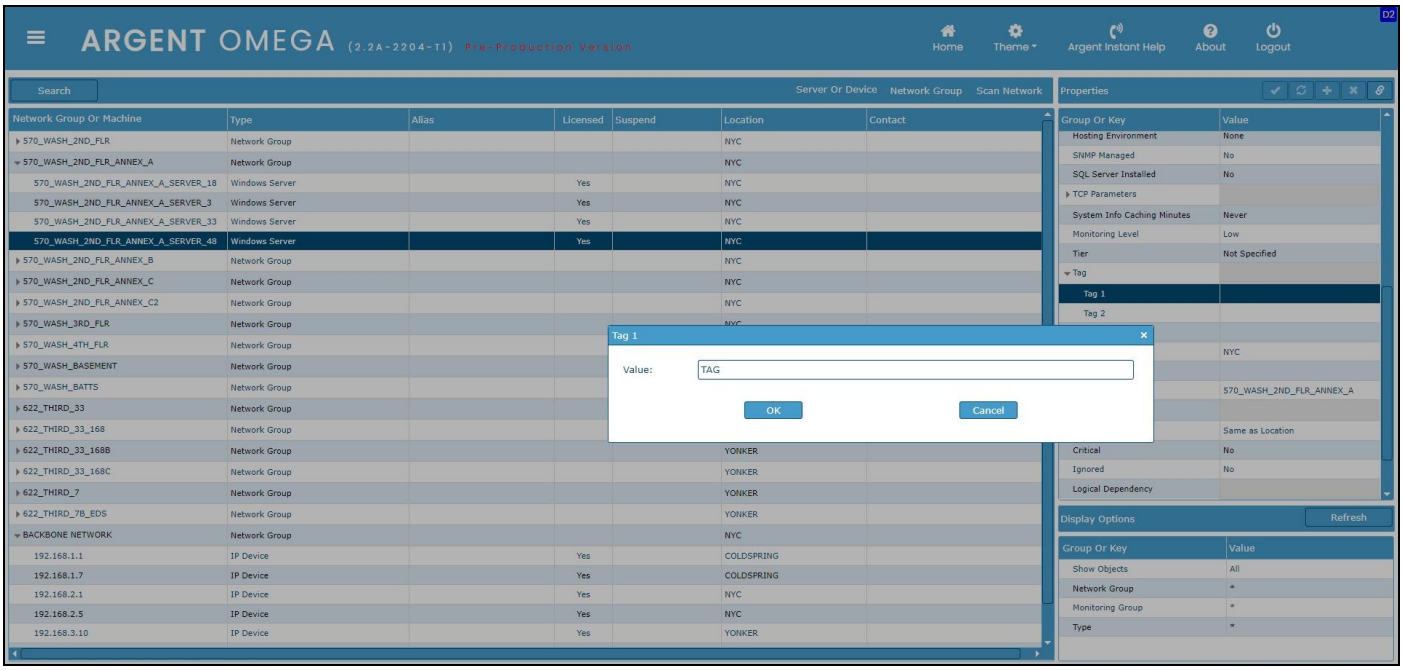
Proprietary Information – All Rights Reserved



The newly created Tags will be listed under CMDB-X properties. Double-click on Tag property and select create Tags.



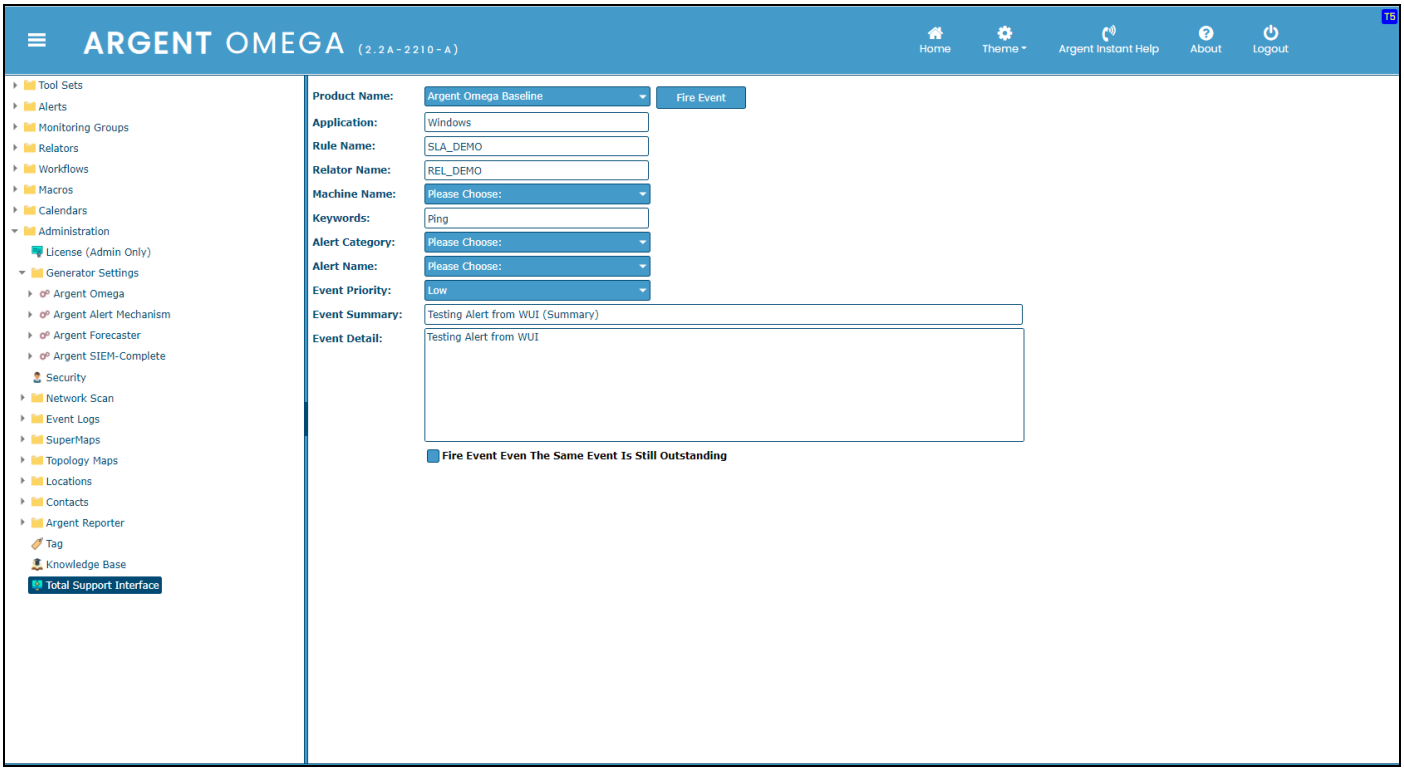
Proprietary Information – All Rights Reserved



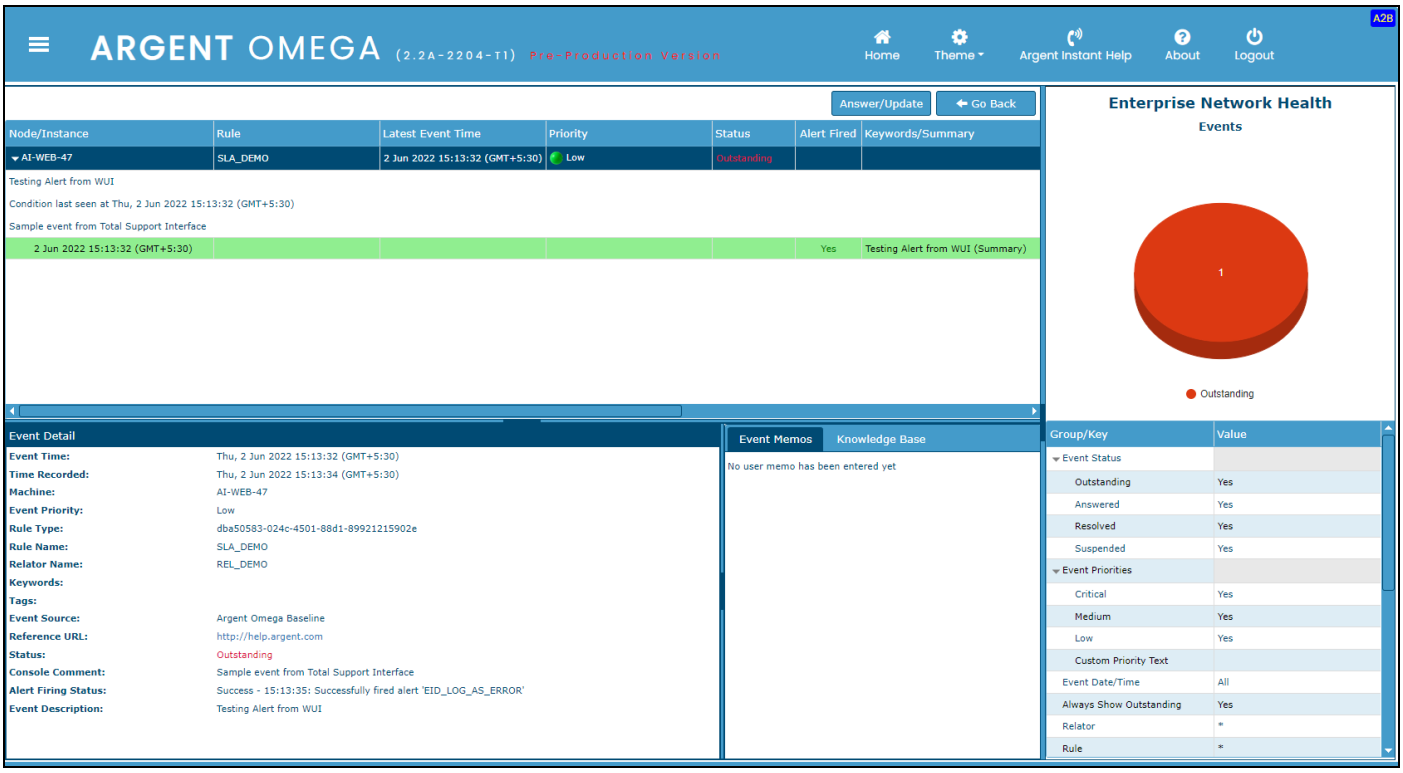
Proprietary Information – All Rights Reserved

Total Support Interface

The Total Support Interface allows you or third-party products and vendors to send Events directly to the central Argent Console.



Click the **Fire Event** button so that the event will be added to the console.



Proprietary Information – All Rights Reserved

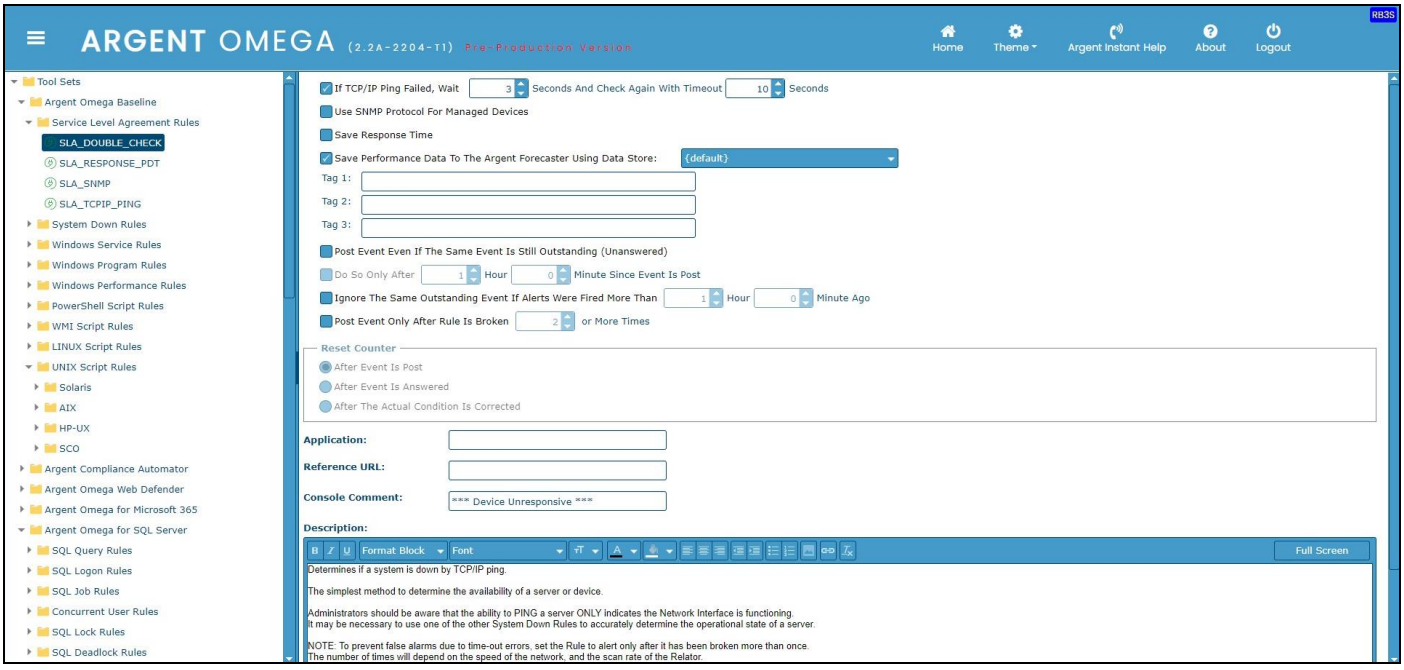
Argent Omega Baseline

Argent Omega Baseline is a **Tool Set** within Argent Omega. There are different types of Rules used in Argent Omega Baseline, namely:

- Service Level Agreement Rules
- System Down Rules
- Windows Service Rules
- Windows Program Rules
- Windows Performance Rules
- PowerShell Script Rules
- WMI Script Rules
- LINUX Script Rules
- UNIX Script Rules

Service Level Agreement Rules

Service Level Agreement Rules check if a system is down via TCP/IP ping. This is the simplest method to determine the availability of a server or device.
Administrators should be aware that the ability to PING a server ONLY indicates the Network Interface is functioning.
You need to use a complete System Down Rule to accurately determine the operational state of a server.

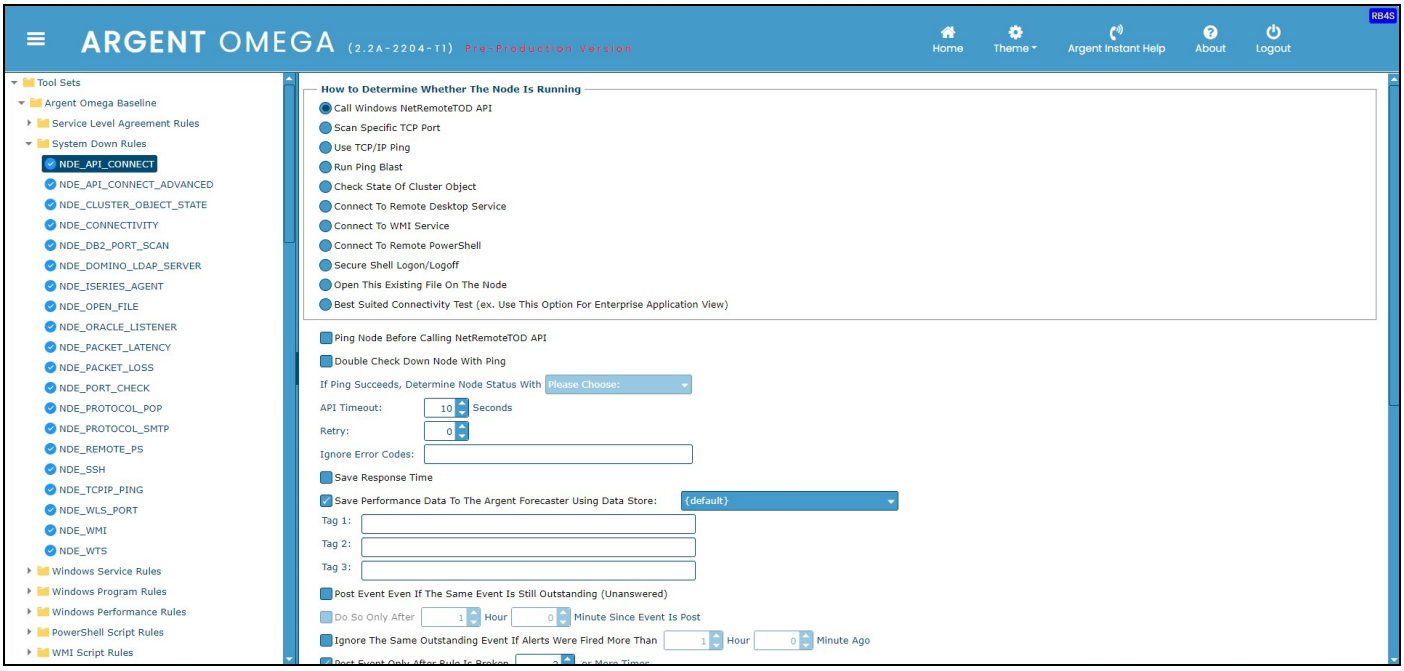


NOTE: To prevent false alarms due to time-out errors, set the rule to alert only after it has been broken more than once. The number of times will depend on the speed of the network and the scan rate of the Relator. (For more details, see Argent KBI https://Help.Argent.com/#KBI_312000)

Proprietary Information – All Rights Reserved

System Down Rules

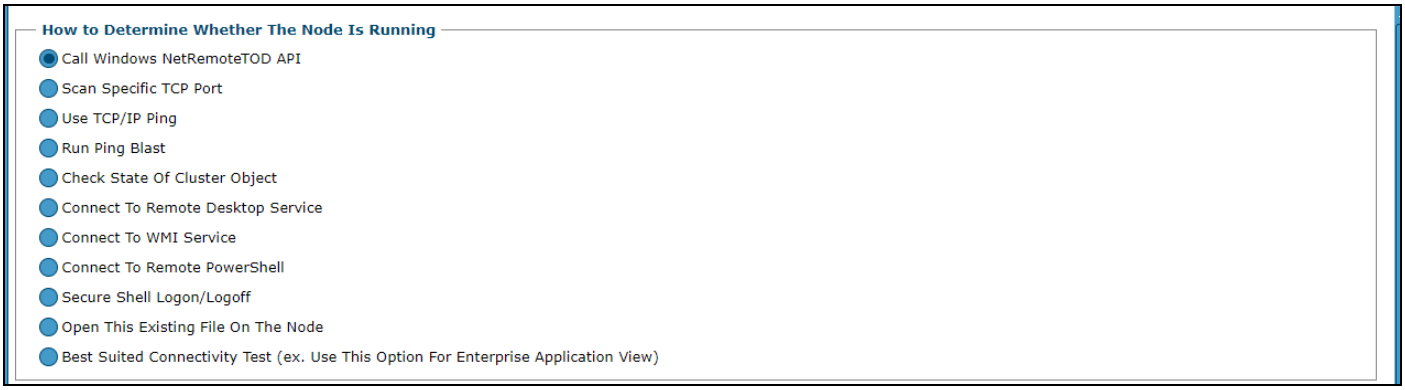
System Down Rules provide various methods to determine if a particular server is alive or not.



Argent Omega provides a bundle of built-in Rules to check the status of various servers and devices. System Down Rules provides the following methods to monitor a server or device:

NetRemoteTOD Win32 API

This method is more reliable than using a simple TCP/IP ping, which simply checks the network card, and does not go into the actual operating system itself; this method does have a concomitant increase in overhead.



By using the API call, this Rule checks that the operating system on the monitored server is actually running.

Testing by Argent shows that the NetRemoteTOD API call has the lowest overhead of any API call. Any API could be used to exercise the operating system on the remote machine; NetRemoteTOD was used because of its light weight.

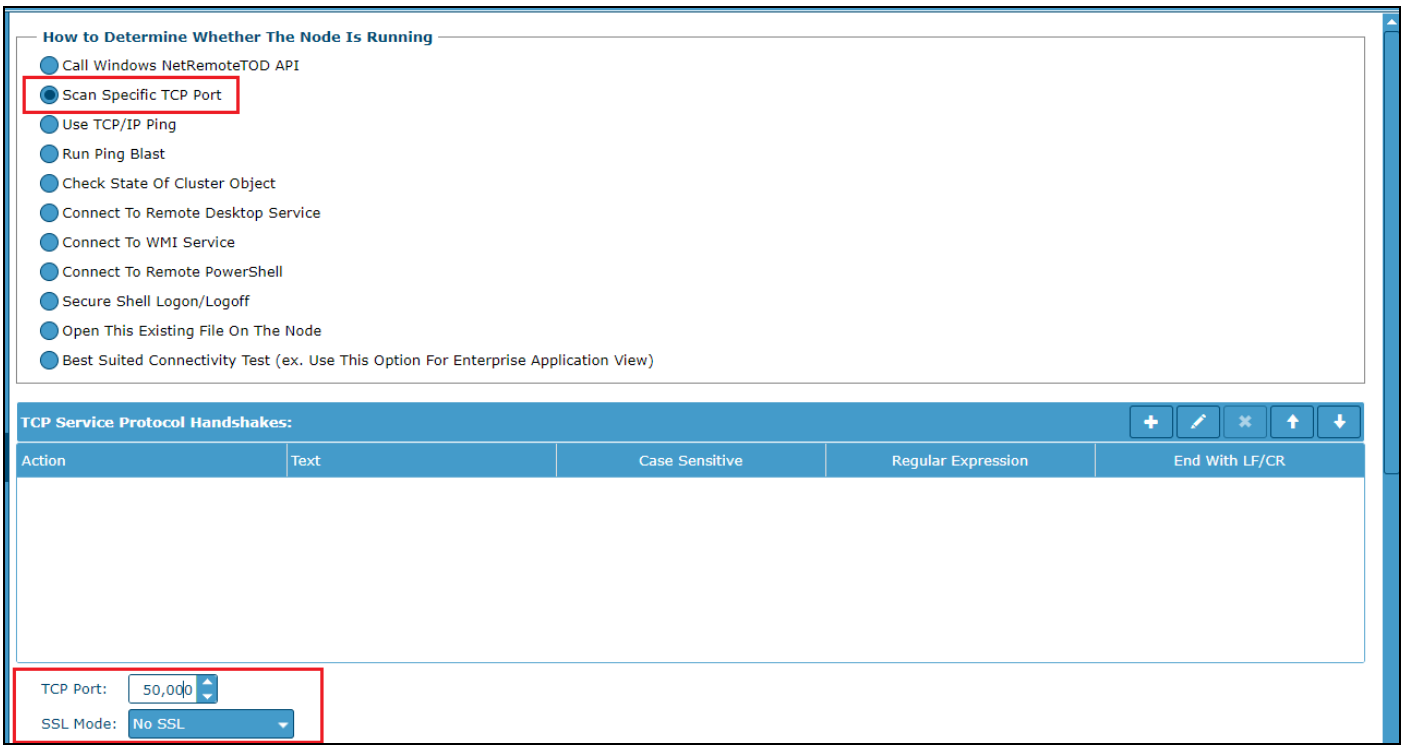
Proprietary Information – All Rights Reserved

Scan Specific TCP/IP Port

It is possible to scan a specific TCP/IP port.

By default, it is a simple port scanning, connecting a TCP port then disconnecting.

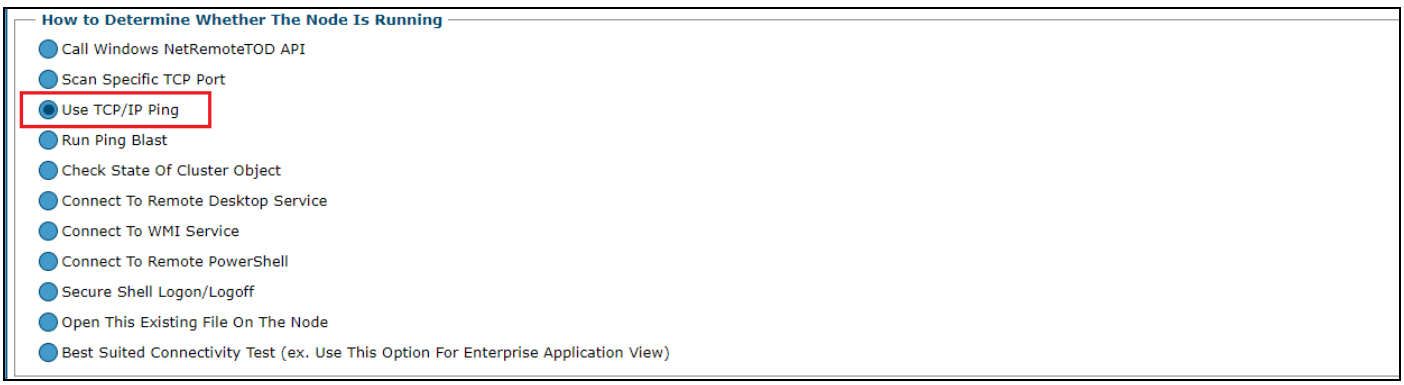
Also there is an option to scan SSL ports.



Use TCP/IP Ping

Determines if a system is down by TCP/IP ping.

The simplest method to determine the availability of a server or device.

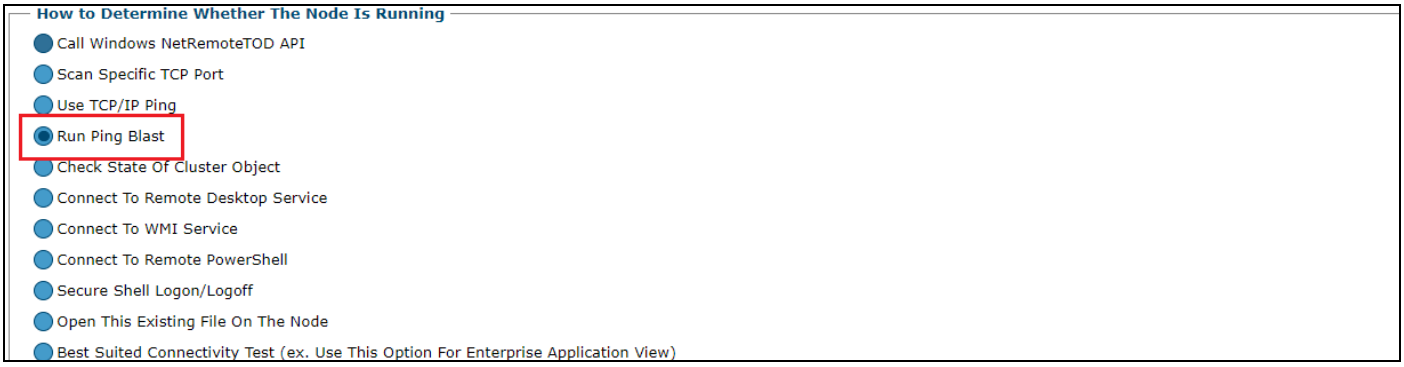


Proprietary Information – All Rights Reserved

Use Ping Blast

Determines if a system is unreliable with high packet loss by TCP/IP ping blast.

It can be useful to test an unreliable slow link.

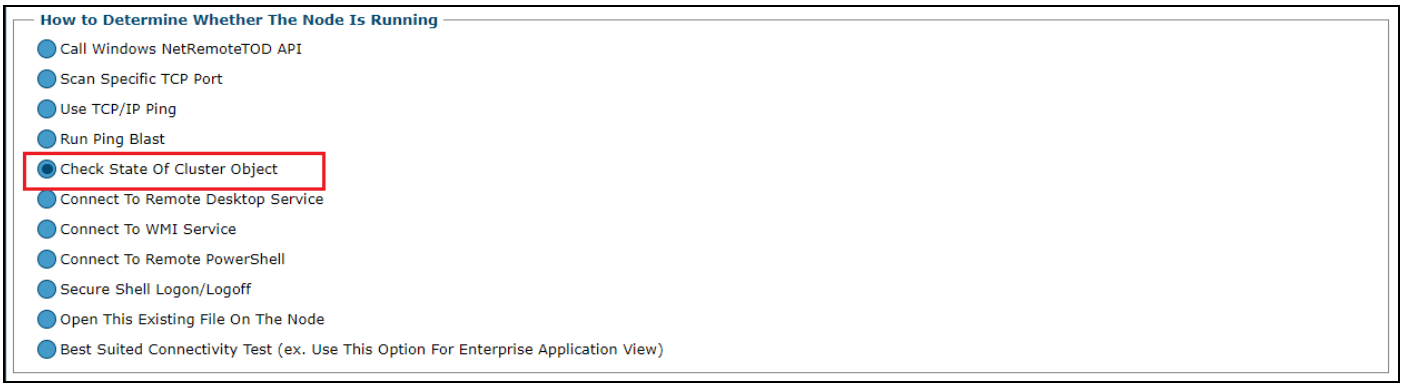


Check State Of Cluster Object

Uses Failover Cluster WMI Provider to query state of cluster object.

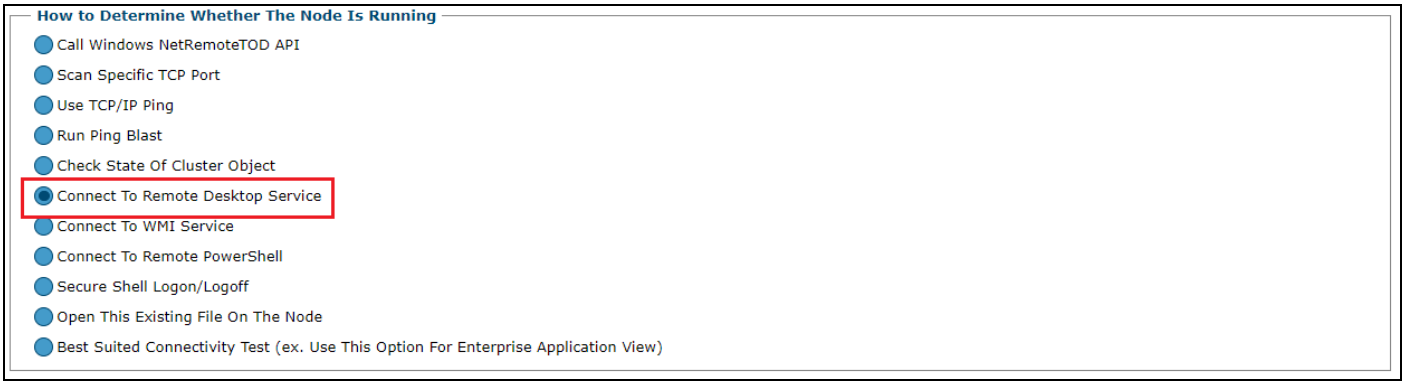
WMI method is required if Argent Omega Engine runs on OS platform different from Cluster OS platform.

For example, Argent Omega Engine of Windows 2008 R2 monitoring a Windows 2016 Cluster.



Use Remote Desktop Service

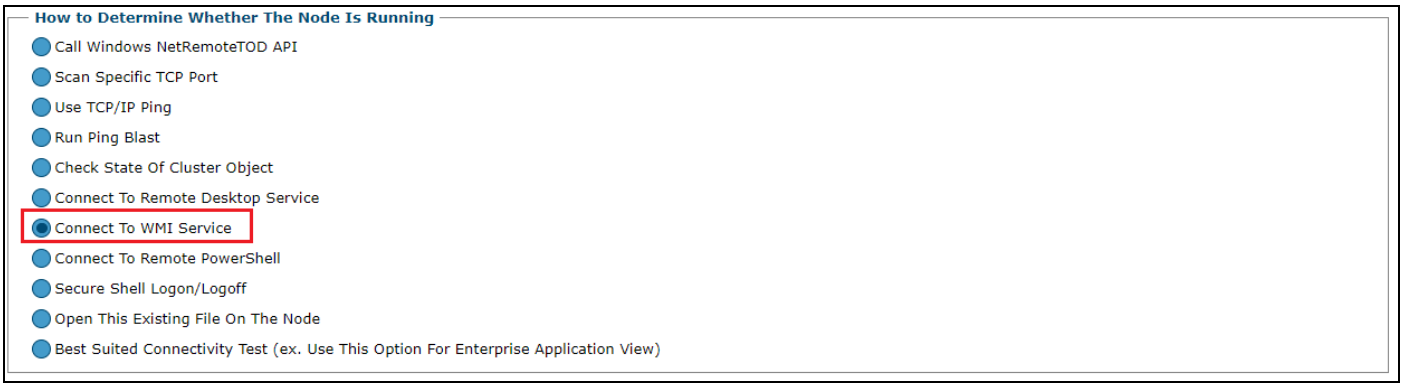
This Rule connects to RDP service to determine if a machine is actually functioning.



Proprietary Information – All Rights Reserved

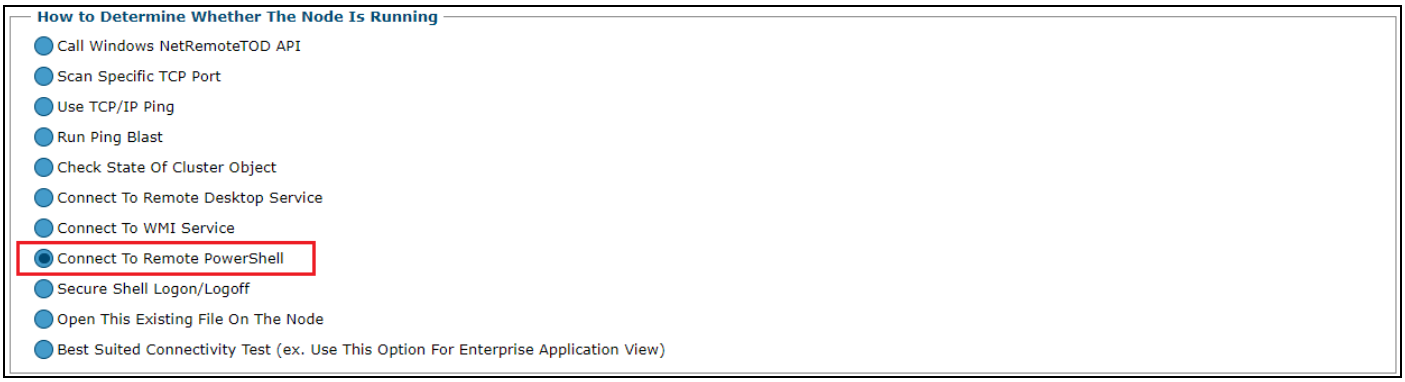
Use WMI Service

This Rule connects to WMI namespace 'root\cimv2' to determine if a machine is actually functioning.



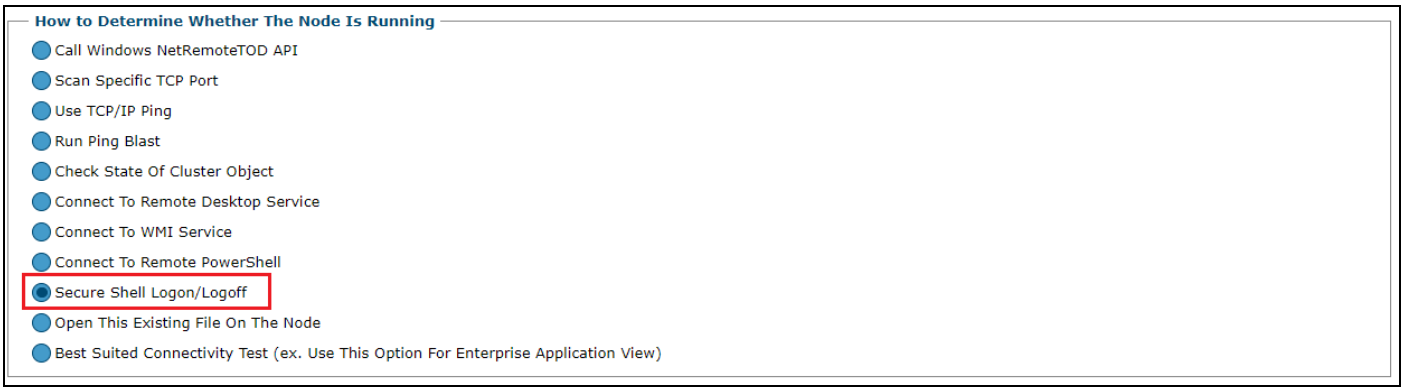
Use Remote PowerShell

This Rule connects to remote PowerShell service to determine if a machine is actually functioning.



Use Secure Shell Logon or Logoff

Determines if a UNIX server is down by explicitly logging on through Secure SSH.



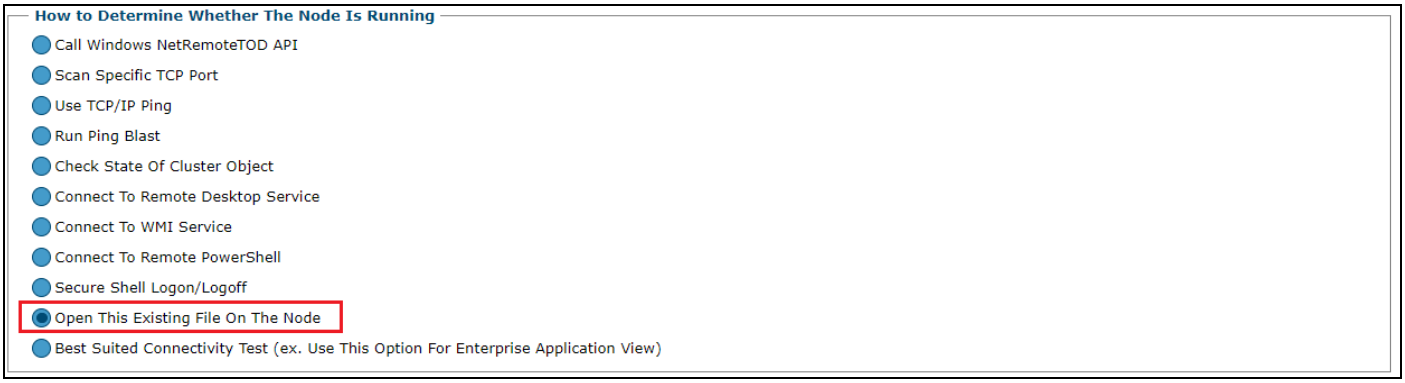
Proprietary Information – All Rights Reserved

Open Existing File On Specific Node

Determines if a system is down by checking for the existence of a file on the system.

This is a useful method to check the availability of a machine that is not running the Microsoft Windows operating system.

The Administrator can take the appropriate action to resolve the system-down when this Rule breaks.

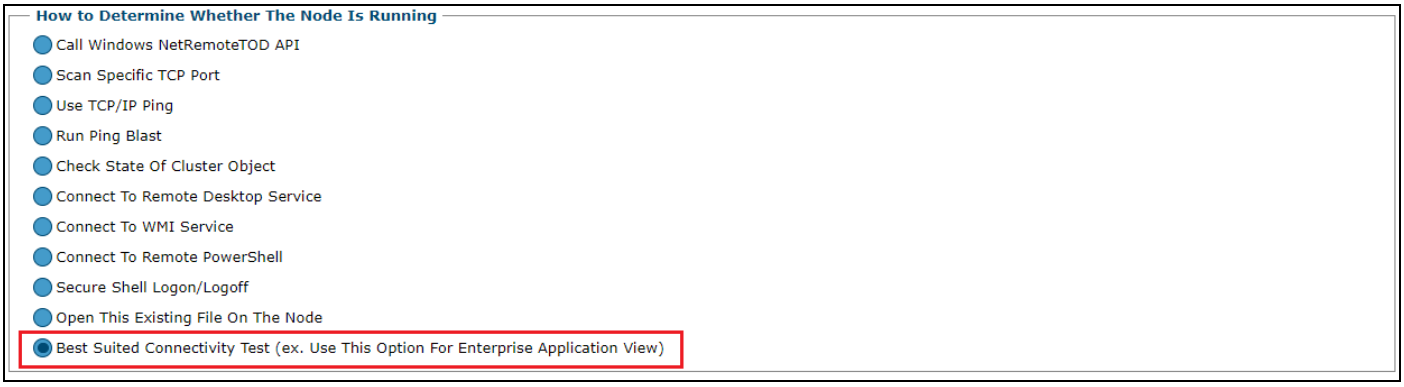


Best Suited Connectivity Test

This Rule uses the most appropriate method based on target node type to test target connectivity.

For example, use the NetRemoteTOD Win32 API for Windows machines, SNMP for managed switches, green, red, yellow or gray status for VMware objects etc.

Note: Link Object and Enterprise Application View should use this option to determine the object state.



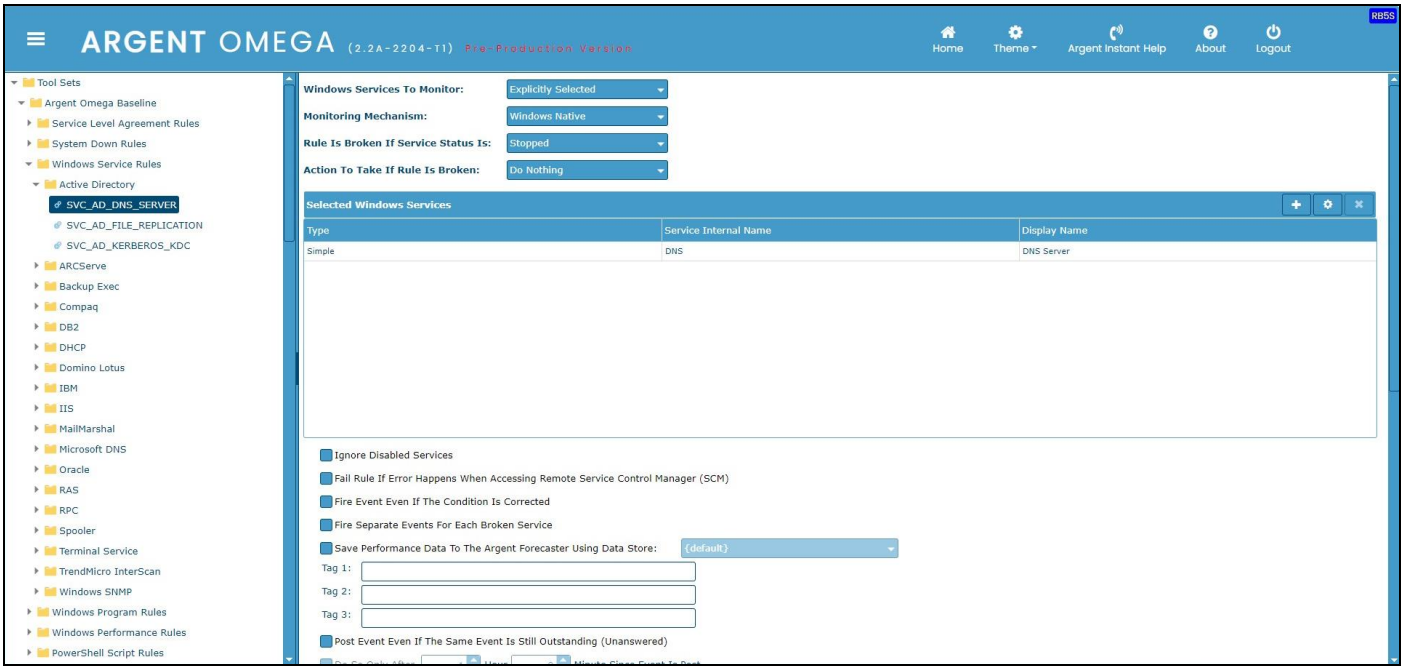
Proprietary Information – All Rights Reserved

Windows Service Rules

W200x Service Rules allow you to check if specific services are:

- “Running”*
- Stopped
- Paused
- Start Pending
- Stop Pending
- Pause Pending
- Continue Pending
- Stalled
- Installed
- Not Installed

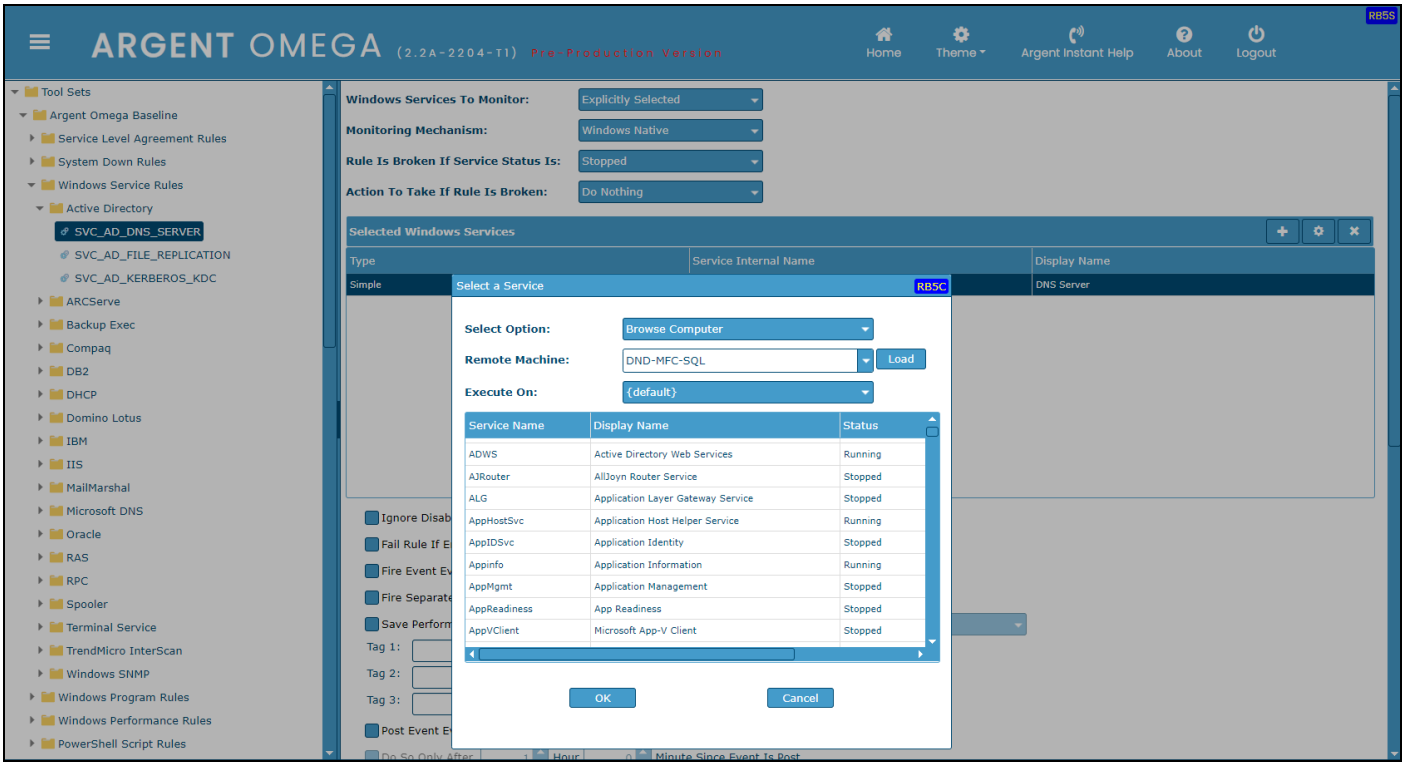
* See Argent KBI Https://Help.Argent.com/#KBI_310212



Windows Service Rules can also be used to take appropriate action if the Rule is Broken.

Proprietary Information – All Rights Reserved

You can customize your Services Rules by loading the service lists from any machine.

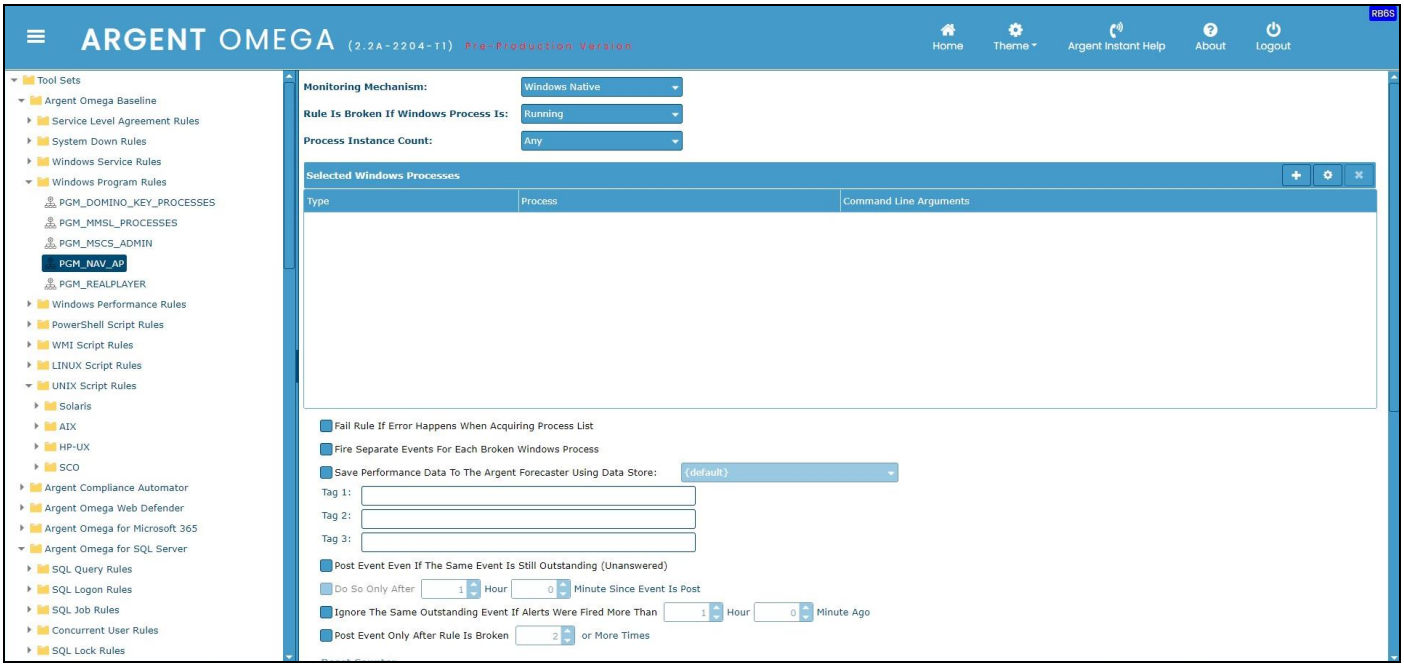


Proprietary Information – All Rights Reserved

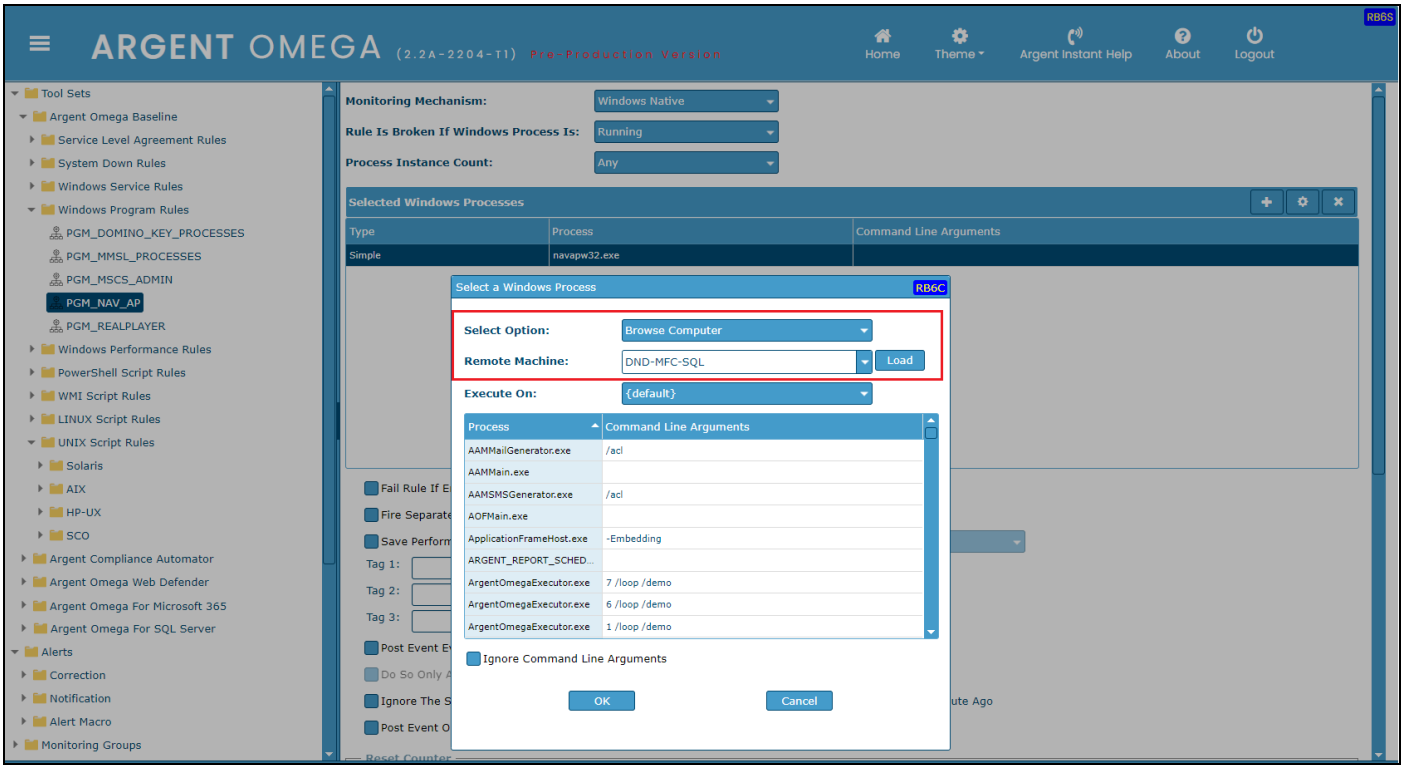
Windows Program Rules

Windows Program Rules monitors Windows Processes.

The Administrator can take the appropriate action to ensure the process is restarted or killed, depending upon the Rule configuration.



You can customize your Program Rules by loading the processes lists from any machine.



Proprietary Information – All Rights Reserved

Windows Performance Rules

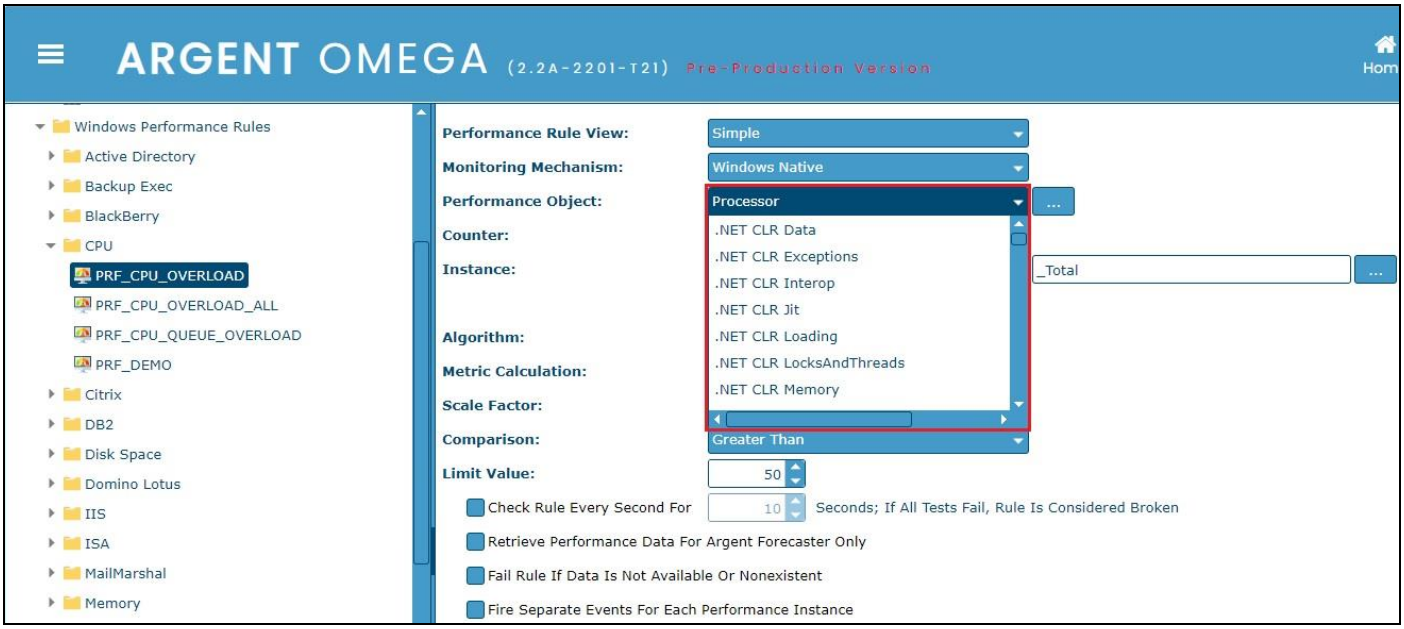
Windows Performance Rules are used to retrieve valuable performance data and snapshots for a particular server.

Monitoring Mechanism

Two types of monitoring mechanisms, Windows Native and PowerShell Remoting, are available in Windows Performance Rule.

Performance Object

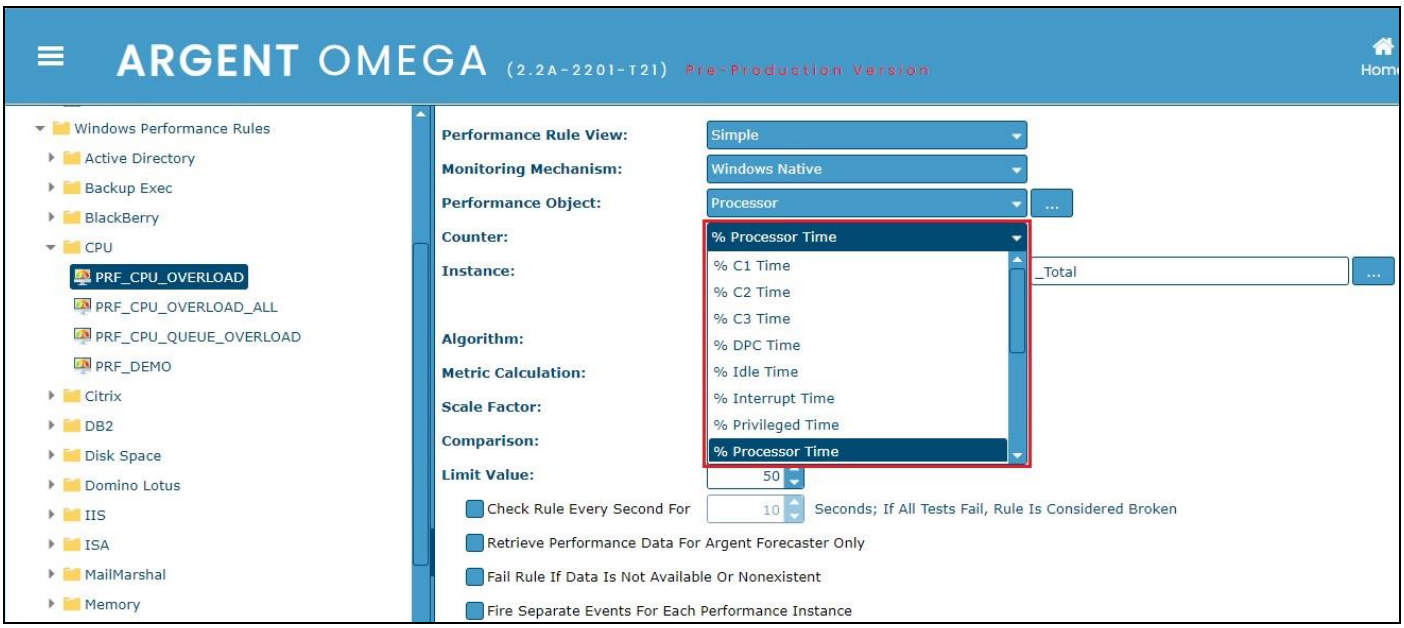
After specifying the server to monitor, the performance object field drop down will show the available performance objects of the server and the Administrator can select the required object form the drop down.



Proprietary Information – All Rights Reserved

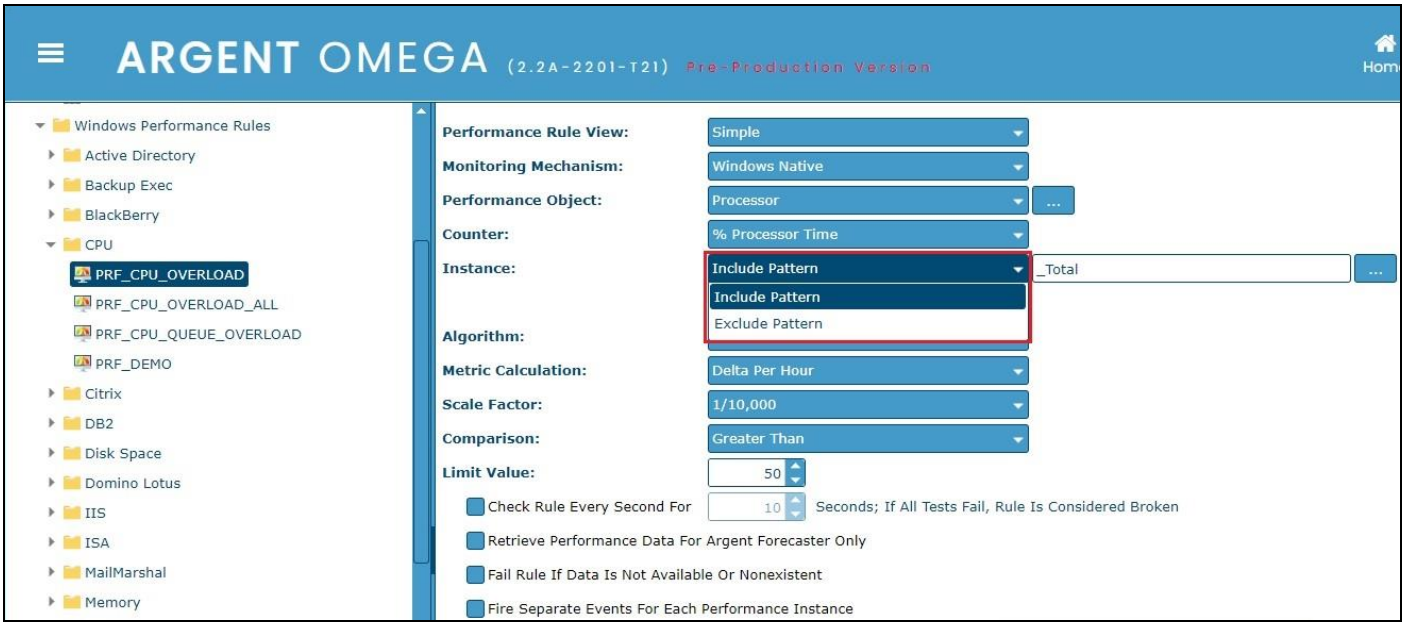
Counter

On choosing the Performance Object, the Counter field drop down will list the available counters with respect to that Object.



Instance

Pattern to include or exclude can be specified.



Proprietary Information – All Rights Reserved

Algorithm

Choose the required algorithm for the performance.

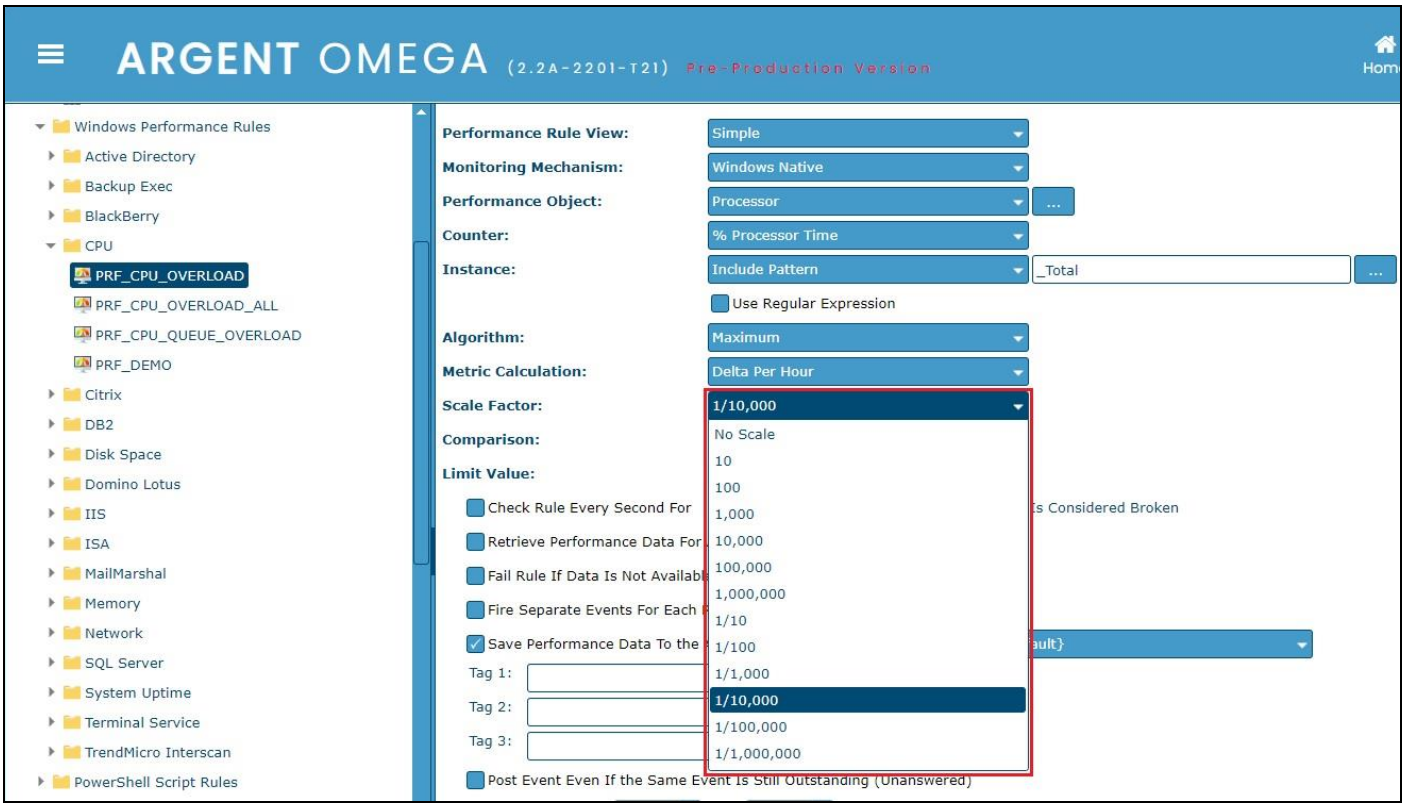
Metric Calculation

The Administrator can select the appropriate metric calculation from the drop-down list.

Proprietary Information – All Rights Reserved

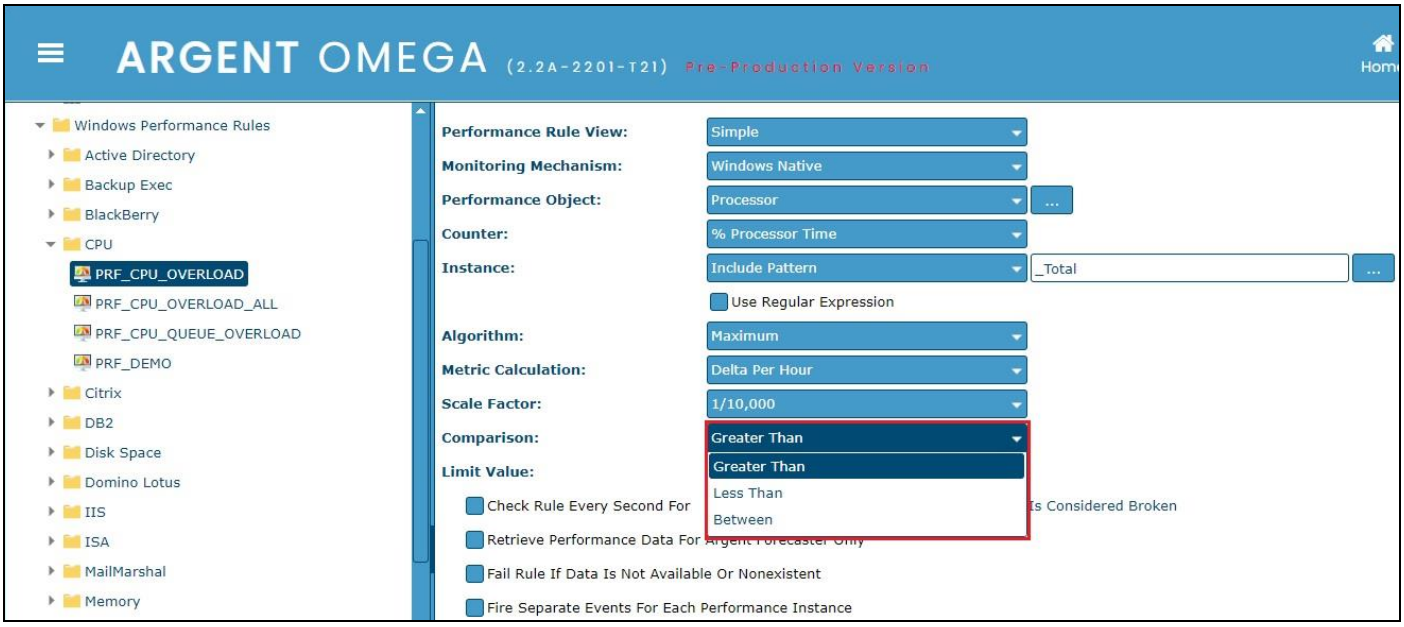
Scale Factor

Specify the scale factor for the performance calculation.



Comparison

The Administrator can select Greater Than, Less Than or Between, for comparing.



Limit Value

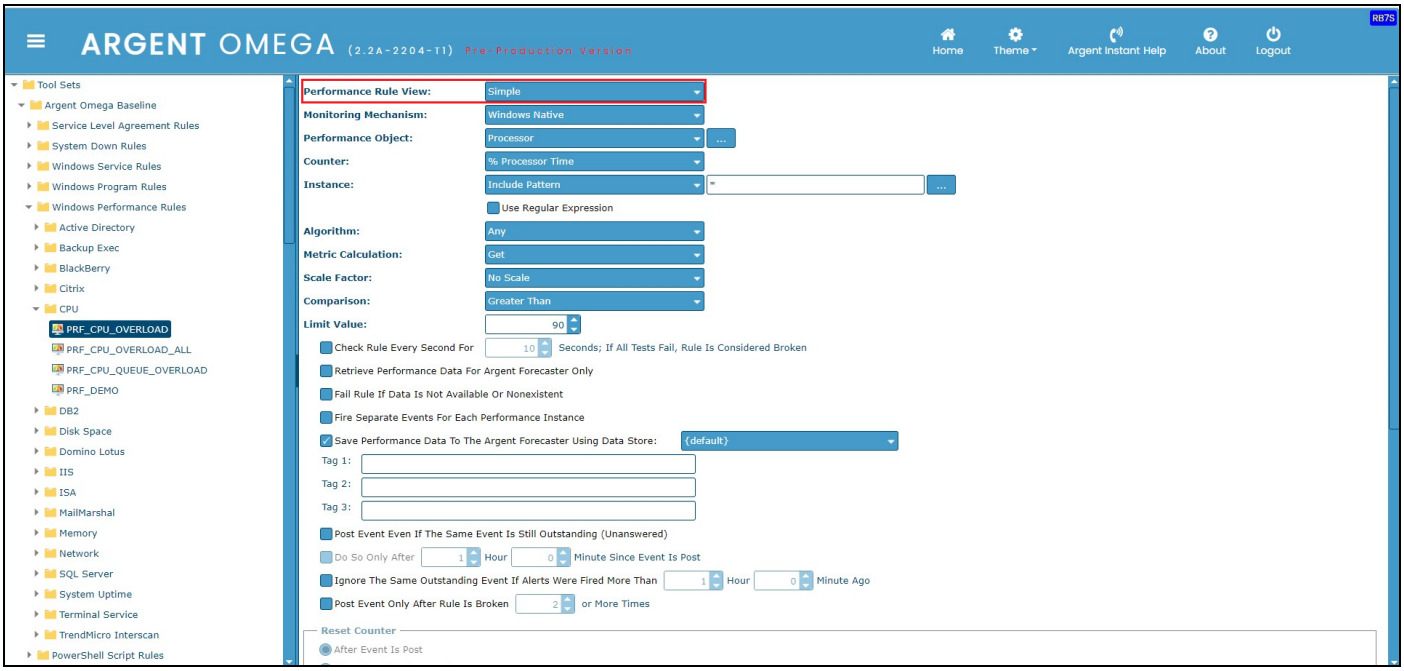
Limit value for can be specified for the comparison and operation**.**

Performance Rule View

There are three types of views: **Simple, Multi-Level,** and **Advanced**

- **Simple**

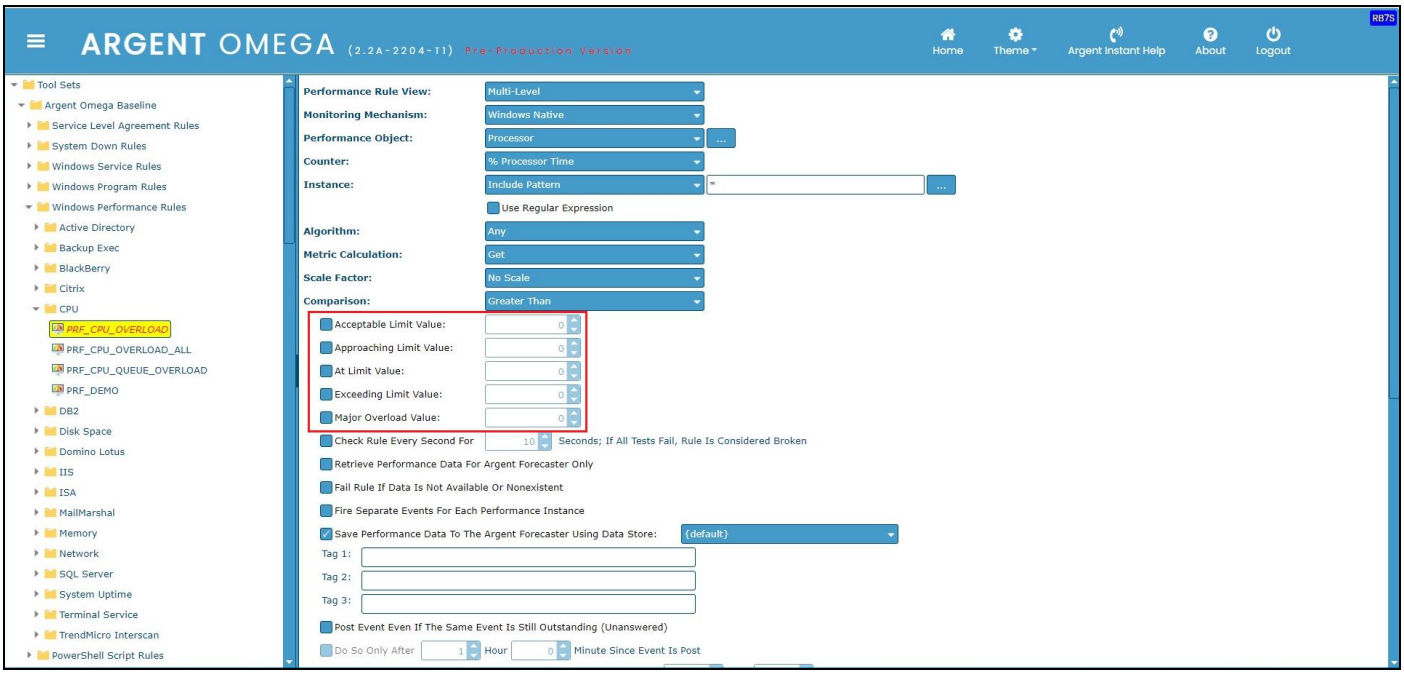
  This is the simplest view of performance monitoring.



Proprietary Information – All Rights Reserved

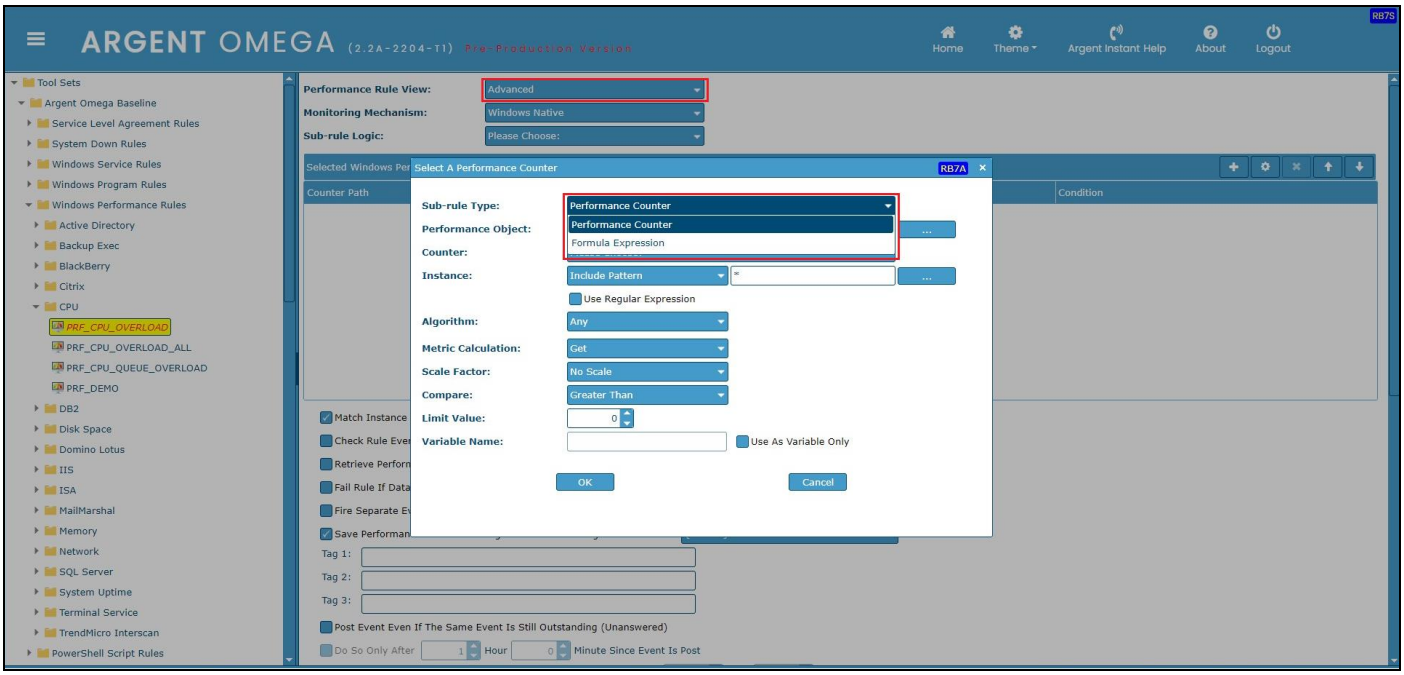
- **Multi-Level**

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



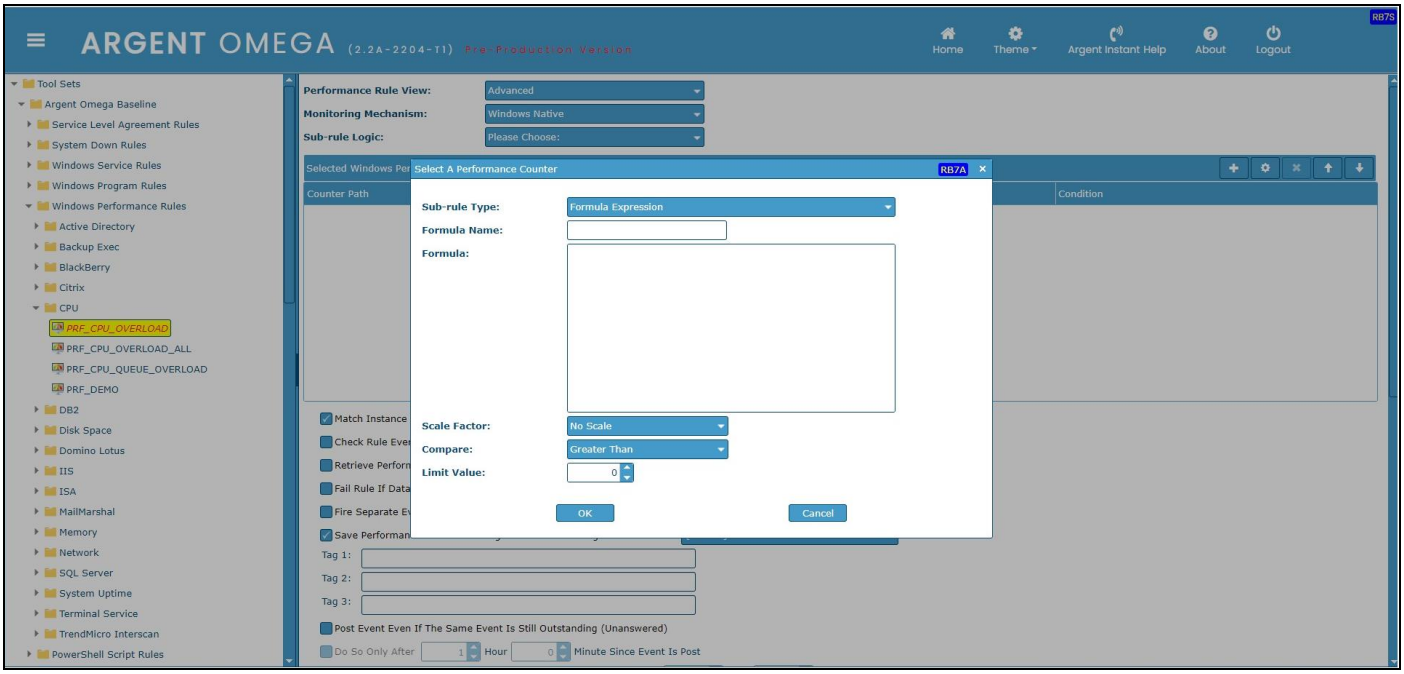
- **Advanced**

  For the Advanced Performance Rule View option there are two Sub-rule Types available: Performance. Counter and Formula Expression. All the required details for both can be specified in sub window B5A.



Proprietary Information – All Rights Reserved

Specify the required formula if choosing the Sub-rule Type “Formula Expression.”



Proprietary Information – All Rights Reserved

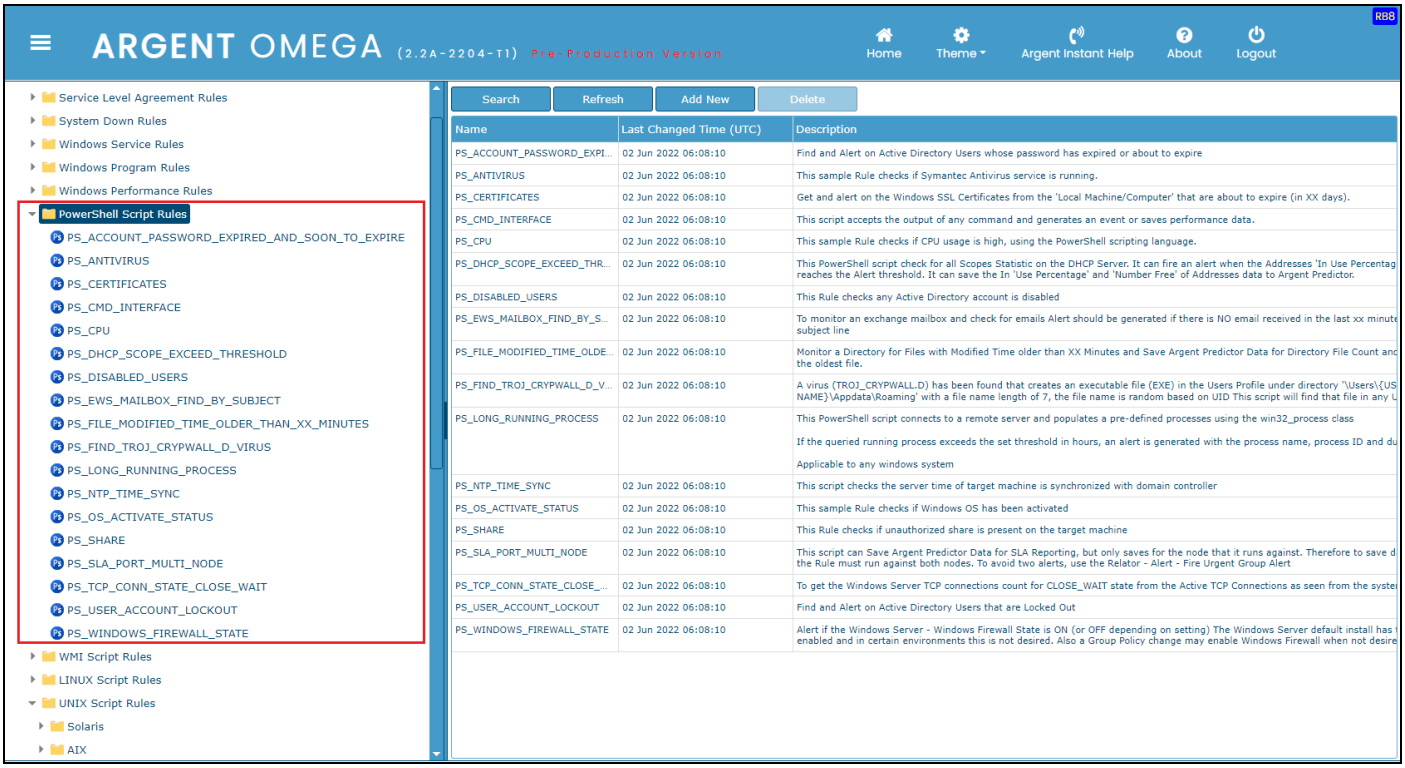
PowerShell Script Rules

With the appropriate credentials, PowerShell Script Rules allow you to create your own custom PowerShell scripts to monitor a specific server or device.

It is also possible to save Performance Data to Argent Forecaster in PowerShell Script Rules.

Windows PowerShell (3.0 or higher) is required -- PowerShell is free of charge and executes as a standalone application (no services required)

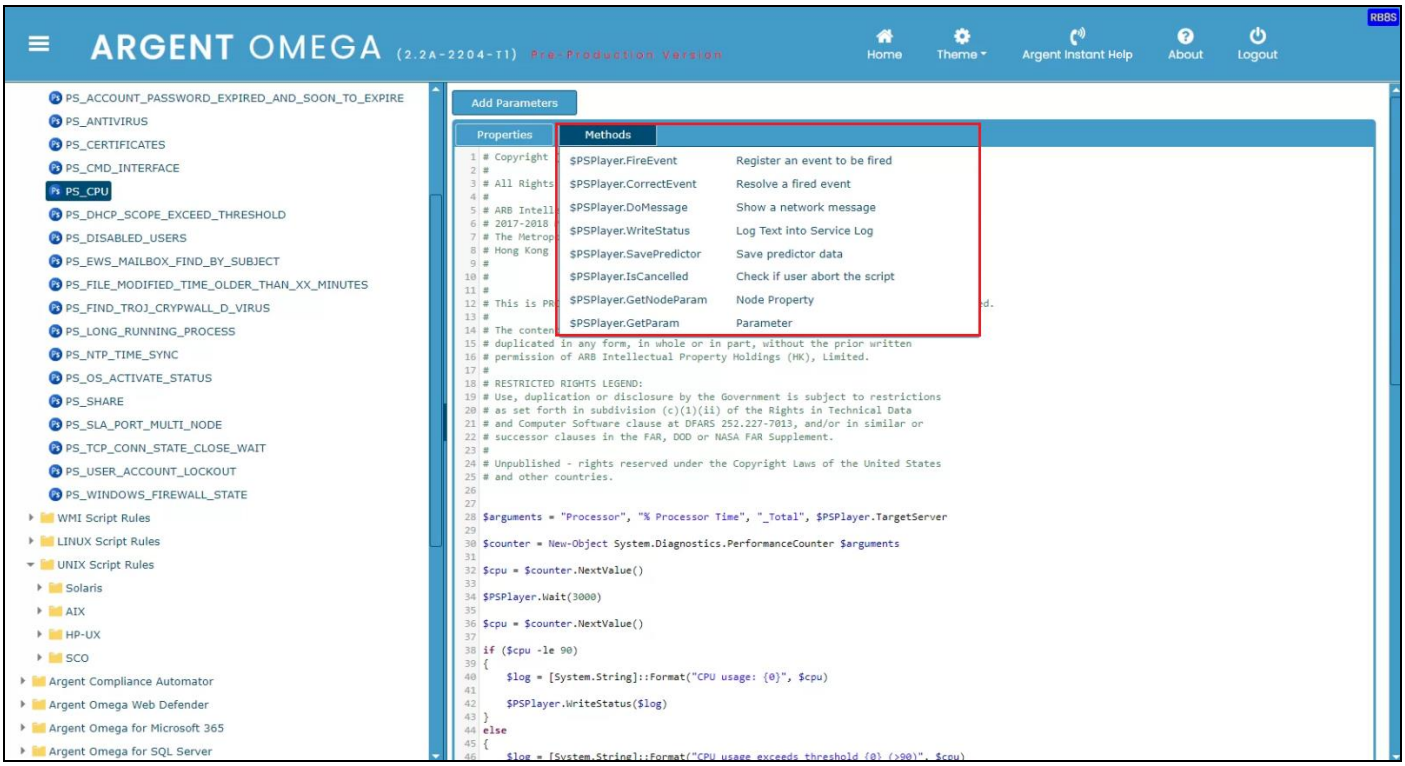
Argent Omega provides a useful collection of built-in PowerShell Script Rules:



Proprietary Information – All Rights Reserved

To tightly integrate with PowerShell technology, Argent provides a set of Properties and Methods that extend the PowerShell script naming space.

They are conveniently available through the drop down menu by clicking the specific buttons.



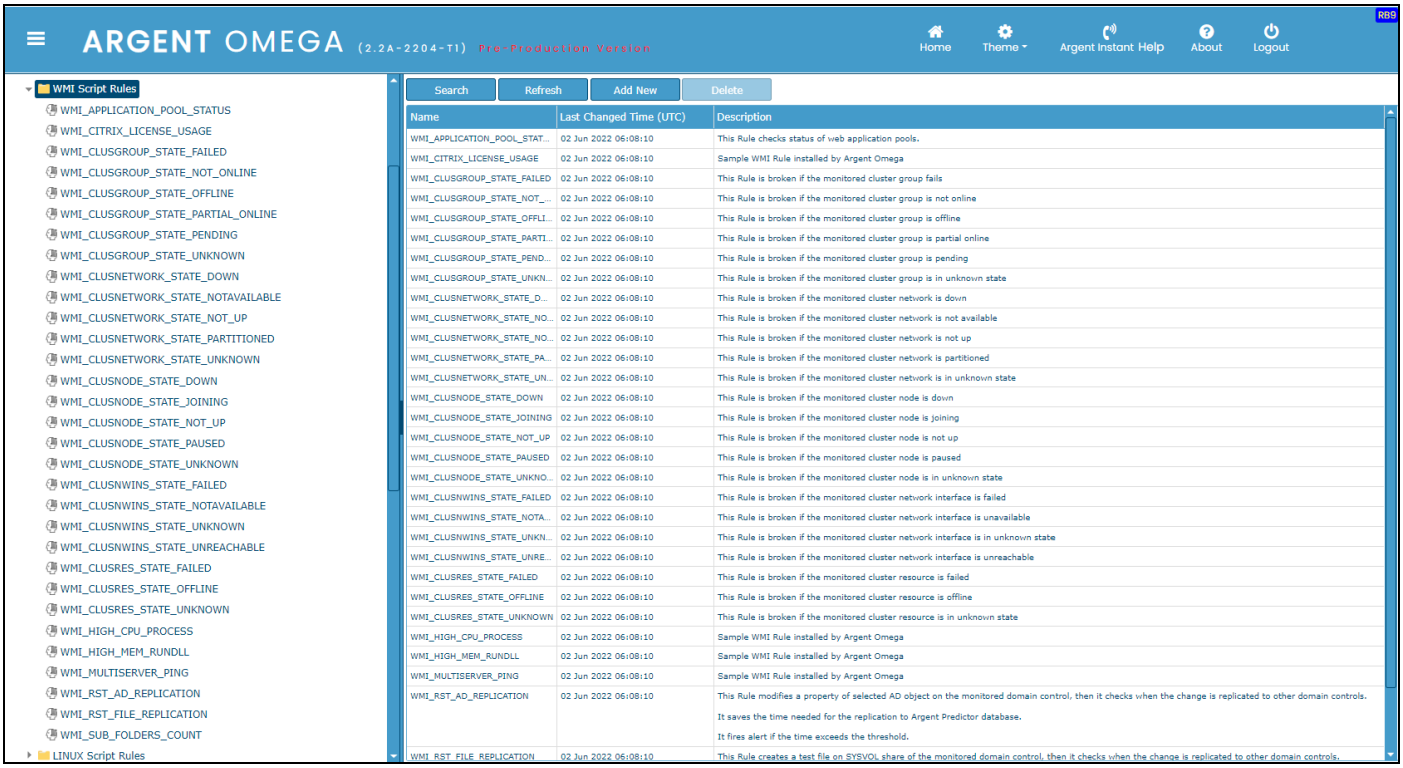
Proprietary Information – All Rights Reserved

WMI Script Rules

WMI Script Rules allow you to create your own custom WMI scripts to monitor a specific server or device.

It is also possible to save Performance Data to Argent Forecaster in WMI Script Rules.

Argent Omega provides bundle of built-in WMI Script Rules:



Proprietary Information – All Rights Reserved

WMI Script Rules permit extremely flexible monitoring because the monitoring is accomplished through a custom VBScript.

What makes WMI Rules so powerful and useful is their ability to run any WMI script.

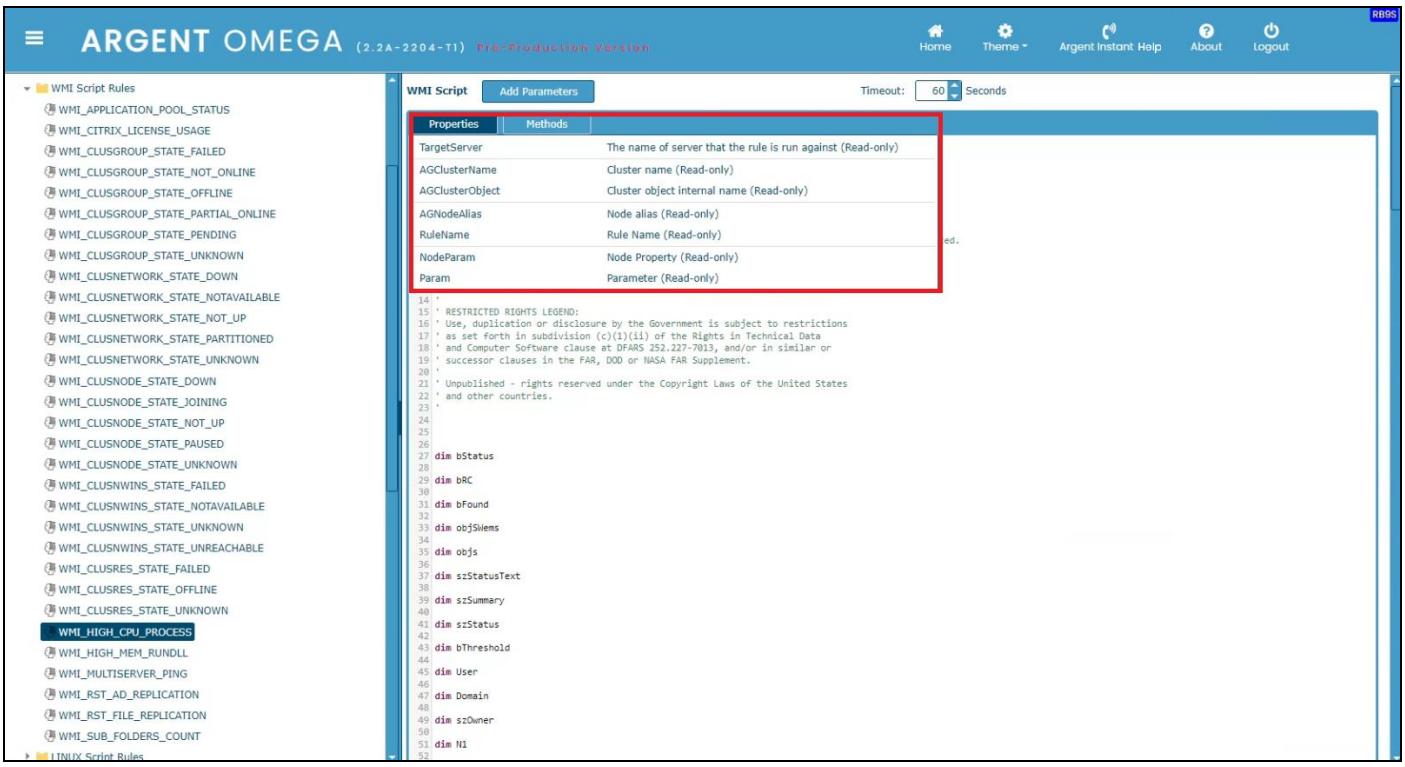
WMI Rules can be used in the following situations:

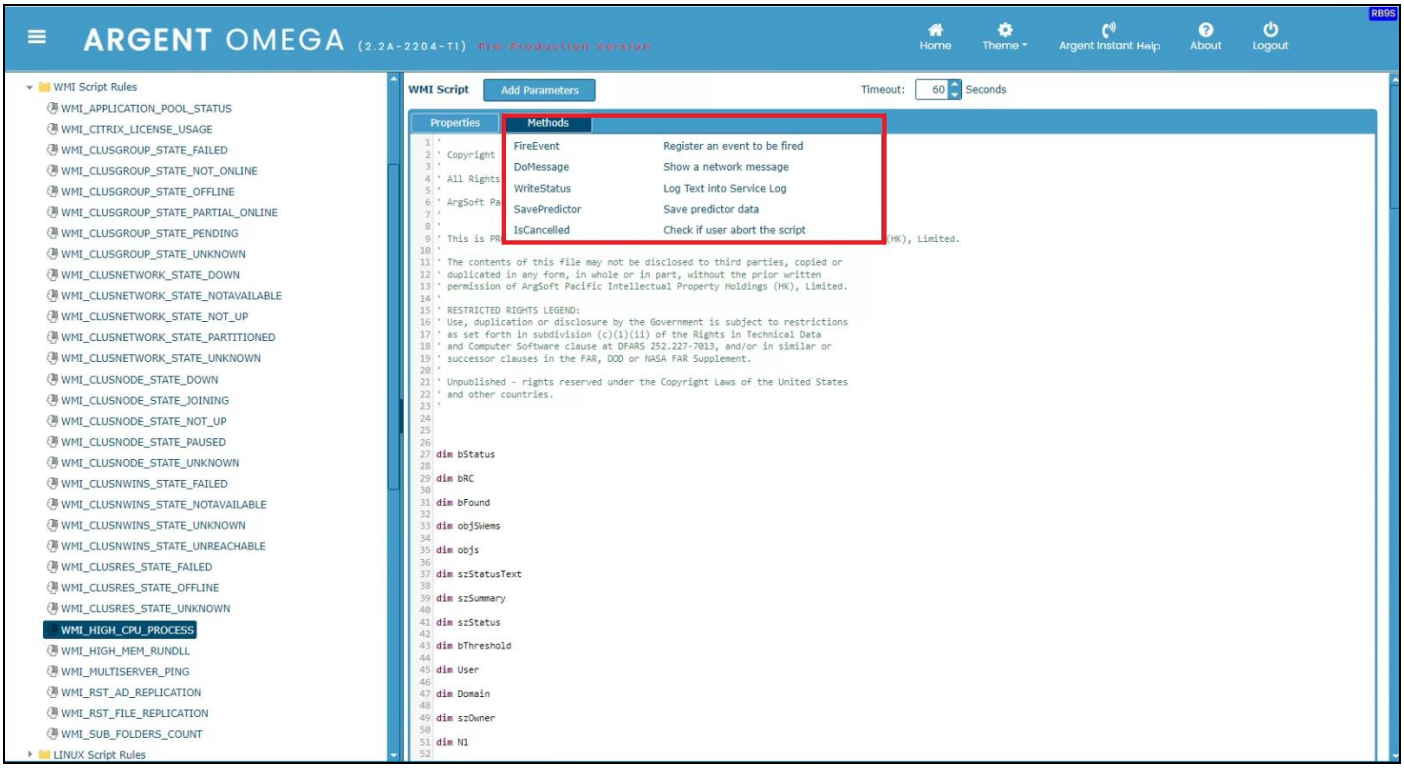
- The monitored object is only exposed through a WMI interface. This is becoming more common as Microsoft pushes WMI technology.
- The monitoring logic needed is very complicated, making use of existing Rule-types difficult.
- A third-party product exposes its programming interface through ActiveX objects.

Proprietary Information – All Rights Reserved

To tightly integrate with WMI technology, Argent Omega provides a set of Properties and Methods that extend the VBScript naming space.

They are conveniently available through the drop-down menu by clicking the specific buttons.





Proprietary Information – All Rights Reserved

UNIX Script Rules

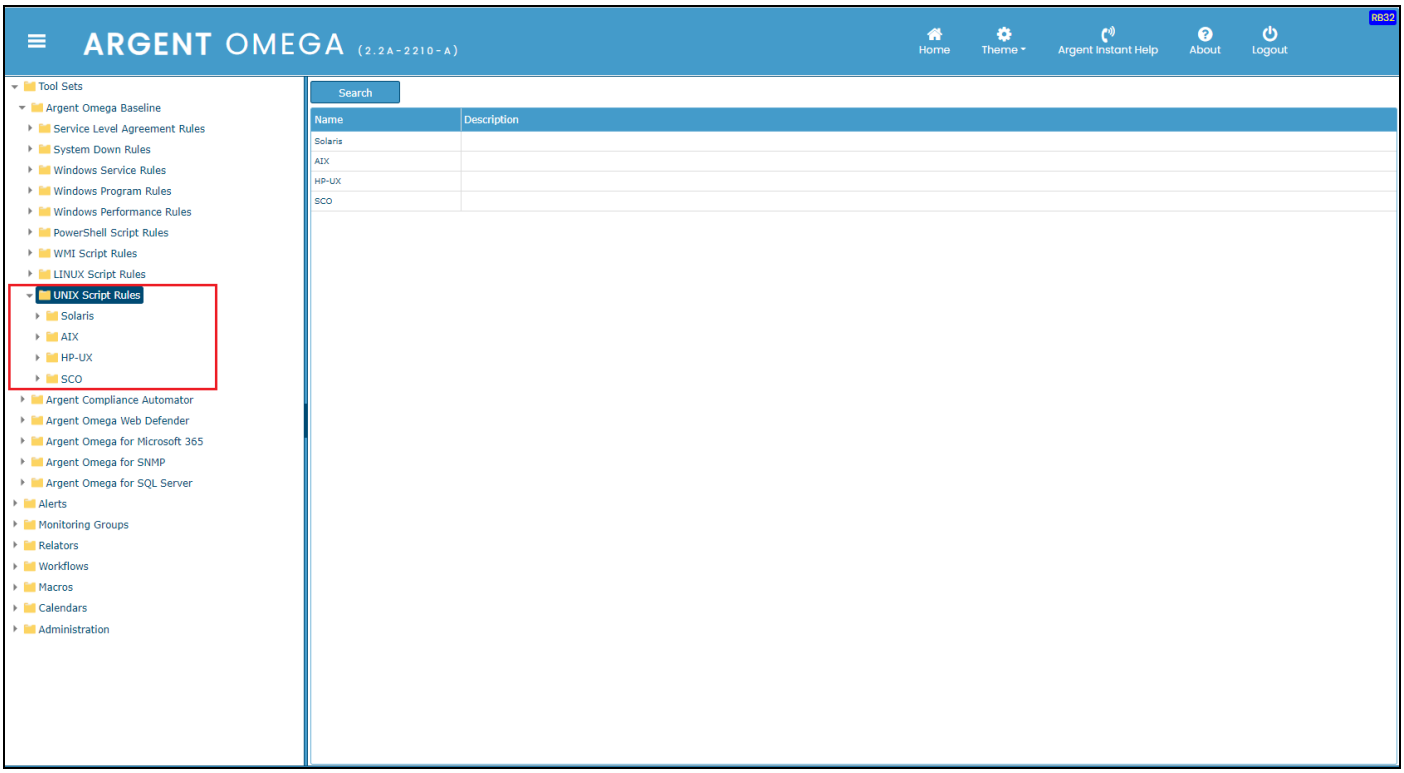
Unix servers often run your most critical applications. Why? Because of the stability that Unix offers. But, let's be honest. Unix is complicated. The stability Unix provides exists because the underlying operating system is far more complex.

Thankfully, Argent automates even the most complicated application monitoring routines.

Applications running on Unix servers are monitored using a script-based system that is both flexible and popular with Unix administrators.

Unix Rules exist for all the popular platforms, including:

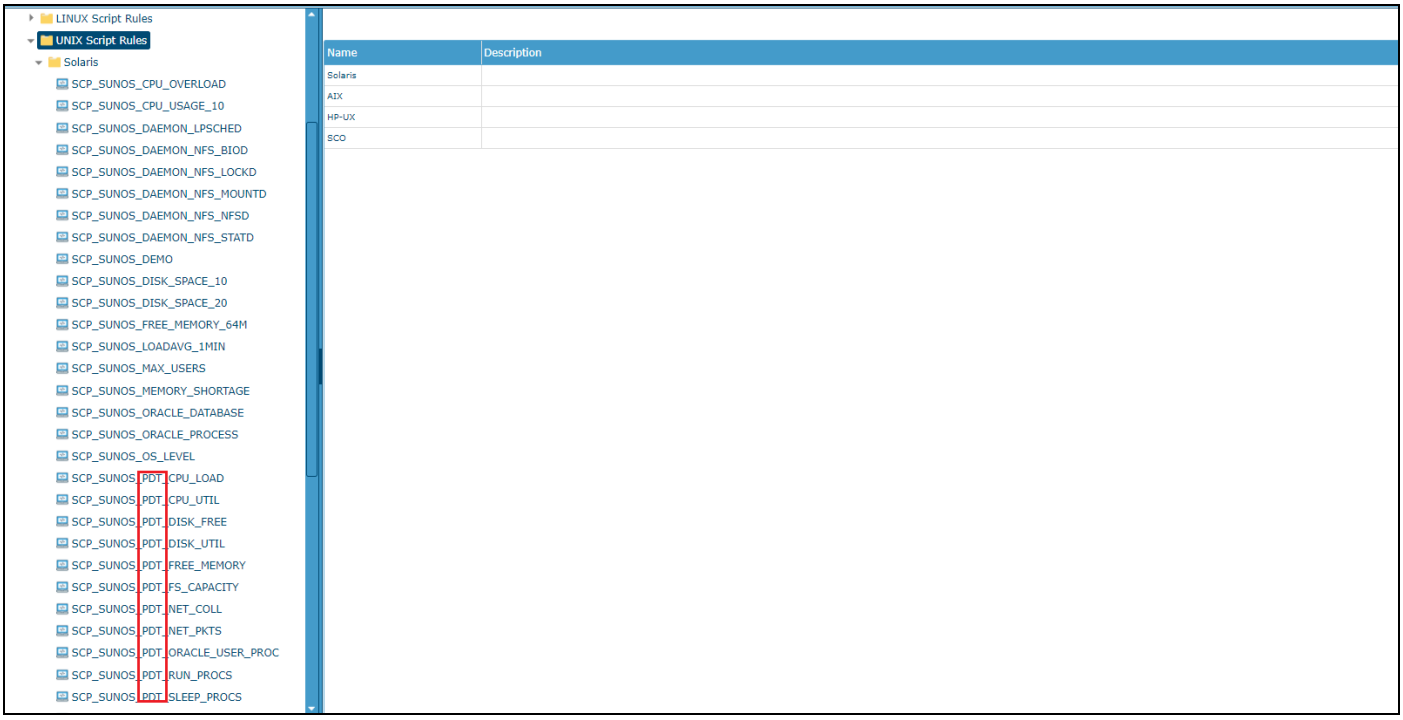
- RedHat
- Solaris
- HP-UX
- AIX
- SCO



Proprietary Information – All Rights Reserved

There are two types of monitoring scripts:

- Threshold Based, Alerting Rules.
- Argent Predictor Based, Trend Analysis Rules, identified by the 'PDT' in the name.



Argent Software
Proprietary Information – All Rights Reserved