

Argent Compliance Automator

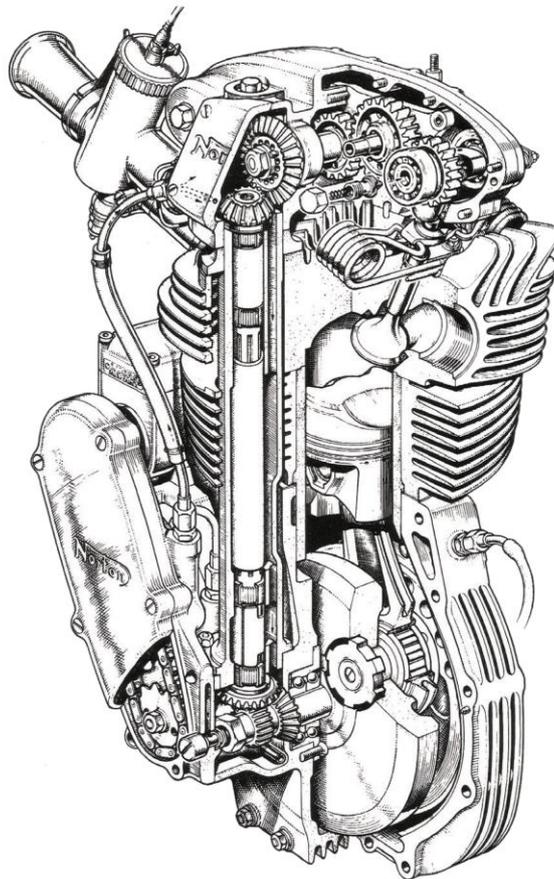


Table Of Contents

Introduction.....	3
Log-On Screen	5
Home Screen	6
CMDB-X	7
CMDB-X Properties	16
Microsoft 365 Service Unit Credentials	18
Manage The Archive Repository.....	21
Argent Compliance Automator	24
Windows Compliance Rules	25
Windows File Log Rules	40
Linux Or Unix File Log Rules	51
SYSLOG Rules	61
SQL Server Log Rules.....	65
Microsoft 365 Audit Log Rules	70
PowerShell Script Log Rules	75

Introduction

One Product Does It All

Argent customers range in size from 11 servers to 77,000 servers.

These customers have many different types of logs on varying classes of computers and devices that need to be scanned and archived.

Typical log types that customers scan and archive include Windows Event Logs, Windows File Logs, Linux\Unix File Logs, Network Device SYSLOGS, Microsoft 365 Audit Logs and many more.

Piecemeal solutions – one per platform – create as many problems as they solve.

In contrast, the Argent Compliance Automator addresses all of these needs in one centrally-managed product.

All of these logs are stored centrally in one secure SQL Server (or ODBC) database.

Argent Compliance Automator can easily detect and stop hacking from any platform – Windows, Linux, Unix; **if the application has a log, the Argent Compliance Automator can monitor it.**

The Argent Compliance Automator utilizes fifteen different types of Notification and Corrective Action Alerts combined with robust customization.

Real-world Examples

Here are some real-world examples of how customers use Argent today:

An international company in northern New Jersey had an issue with their open-source web server suddenly crashing and leaving users hanging and unable to log back in. Argent now scans the log for imminent failure and then -- in a controlled manner -- restarts the web server in under five seconds. Automatically.

A large arts gallery in Australia has five restaurants with over 40 Point Of Sales (POS) devices. But the third-party software was quite buggy and would often crash all 40 POS devices. Argent now scans the third-party software's logs and restarts the application in under five seconds. Automatically.

Long-Term Data Archiving

The Argent Compliance Automator is extremely efficient by first compressing and then encrypting archived data. The Argent Compliance Automator can archive data for up to 10 years – **this is especially important for banks and other regulated financial institutions**. (In contrast to Microsoft's 30-day limit, the Argent Compliance Automator can store Azure logs for up to 10 years.)

The Argent Compliance Automator uses advanced Artificial Intelligence to automatically filter noise and transient aberrations; this is critical to reliably archiving security logs from heavily-used Domain Controllers and all types of file servers, and this is just one example.

Data bloat is eliminated by using highly efficient compression algorithms.

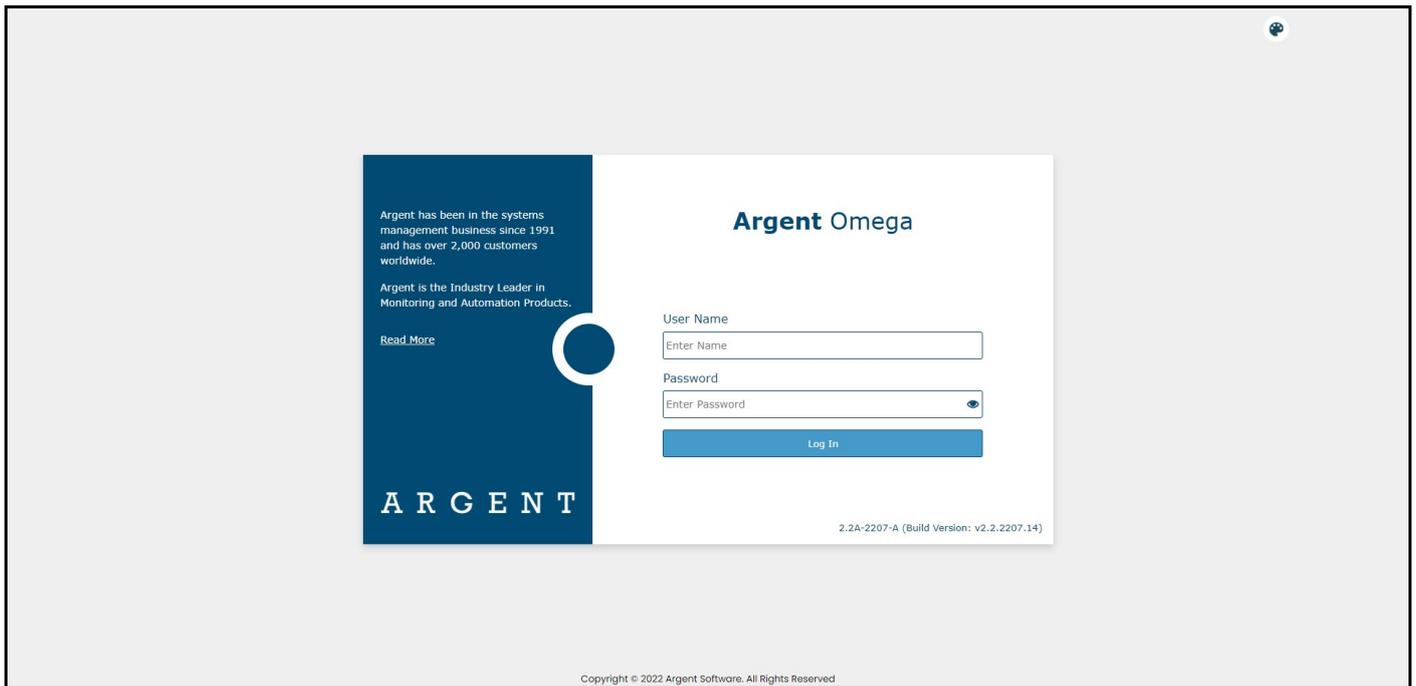
Automated Reporting For All Compliance Needs

When the always-grumpy external auditors arrive, Argent Compliance Automator and the Argent Reporter do all the heavy lifting for you.

Reports can be generated in under 60 seconds and automatically emailed or uploaded to a customer secure web site.

These reports provide administrators with full visibility on who, what, and where changes occurred on all platforms.

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.

For Windows user accounts, the best approach is to create a separate user group for Windows users and assign the required rights.

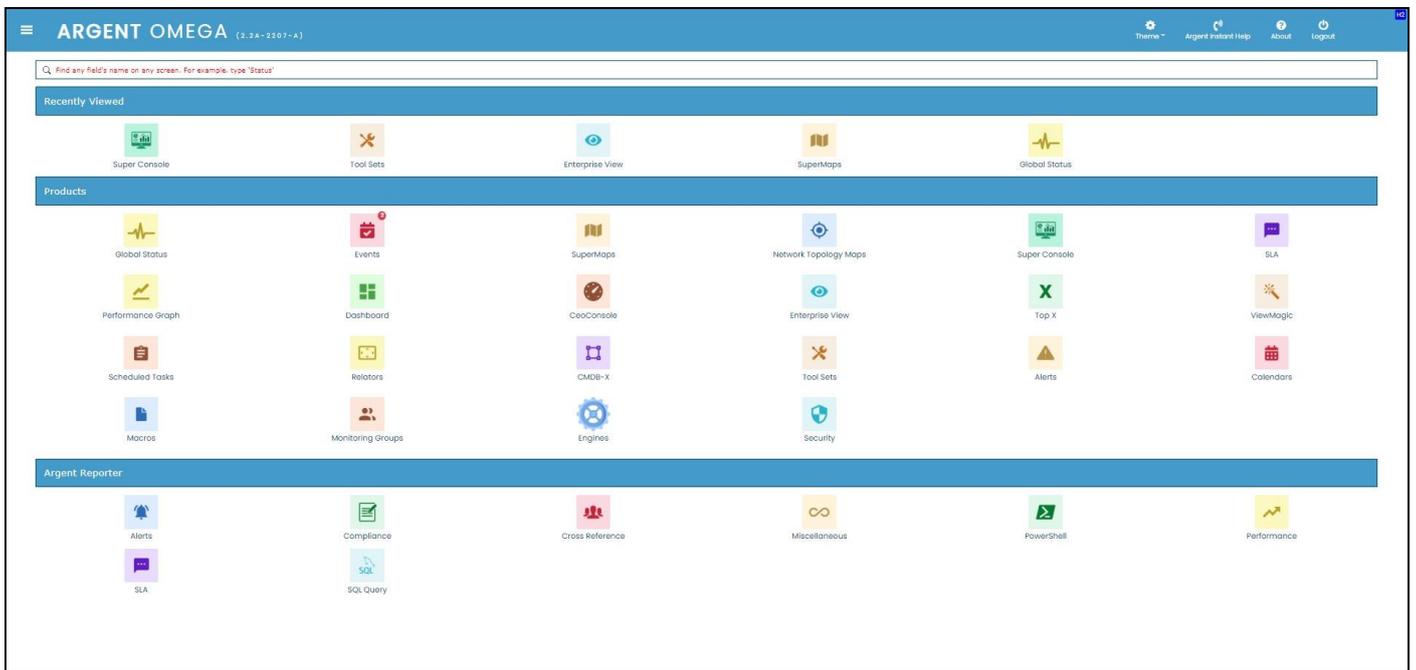
Demo accounts can be created in the **Argent Omega Security** section and are used for demonstration purposes. Demo accounts are read-only accounts and use Argent private authentication to login into Argent Omega. Demo accounts are usually only used temporarily for initial training and are limited to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

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

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

Home Screen

The Argent Omega home screen will be displayed after login:



To begin using Argent Compliance Automator, click on the CMDB-X icon to add monitored servers or devices.

CMDB-X

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

Argent added the 'X' for eXtensible.

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

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

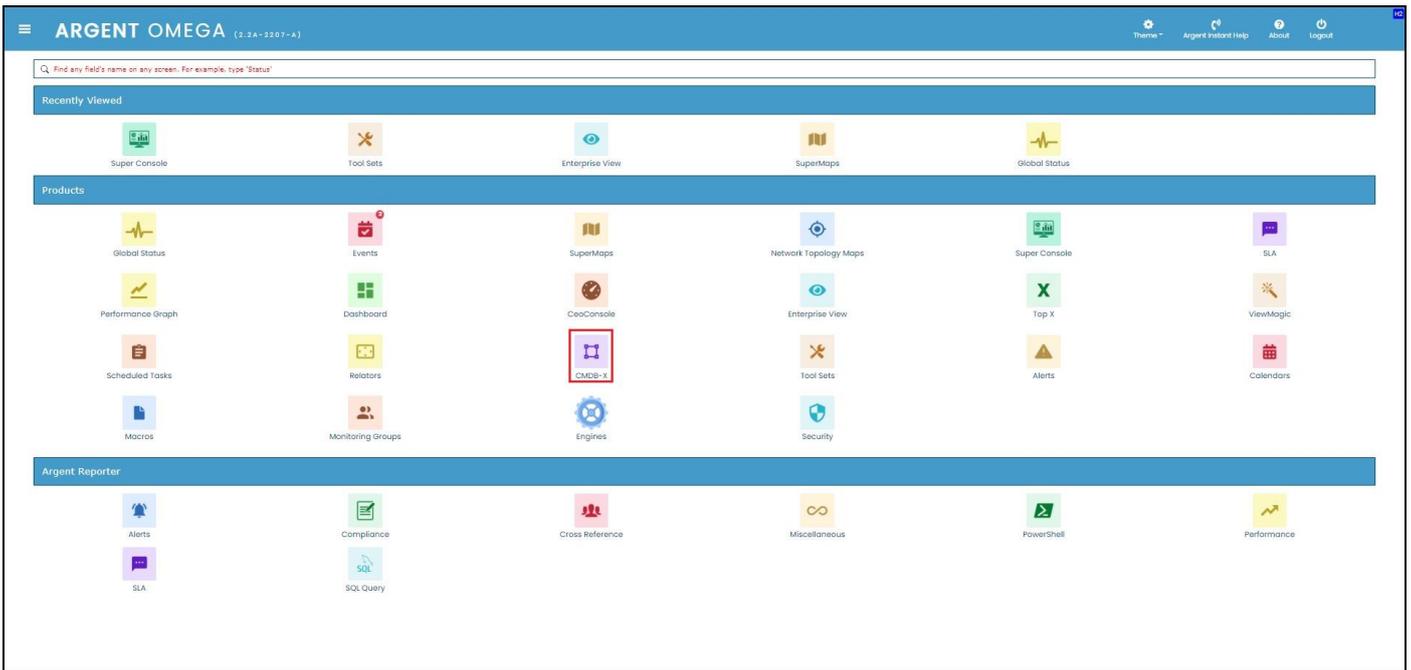
The Argent CMDB-X provides an easy and streamlined way to manage all critical servers and devices, as well as all server and device properties and licensing **from a single screen**. The Argent CMDB-X makes it easy for you to add multiple servers and devices in one batch – 11 or 77,000 -- license them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

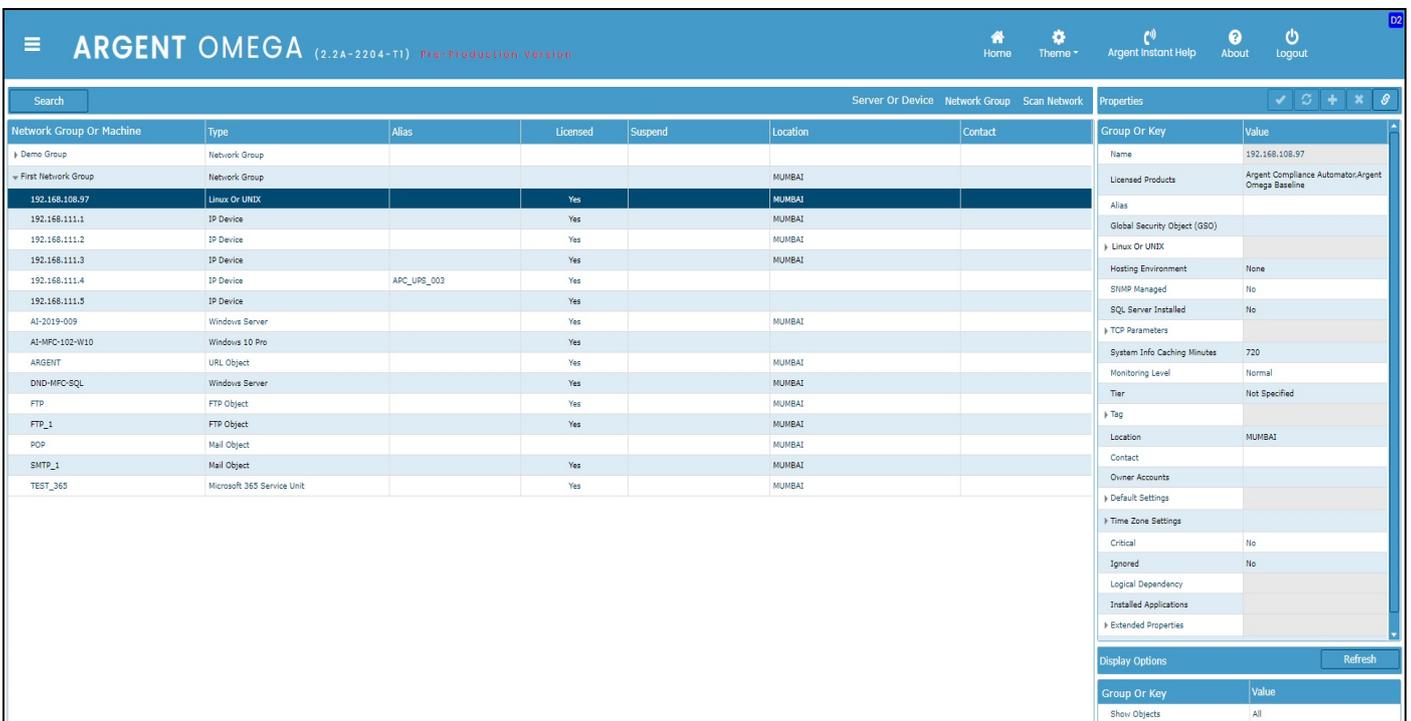
The Argent CMDB-X also has options to import from external Excel files.

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

Select 'CMDB-X' from the Home Screen:



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



Argent Compliance Automator supports monitoring the following types of servers and devices:

- Windows Server
- Linux
- Microsoft 365 Service Unit

- IP Devices

In the CMDB-X, select **Manually Add Server Or Device** from the right click menu:

The screenshot shows the ARGENT OMEGA (2.2A-2204-T1) Pre-Production Version interface. The main table lists network groups and machines. A context menu is open over the table, with the option 'Manually Add Server Or Device' highlighted in red. The table columns include Network Group Or Machine, Type, Alias, Licensed, Suspend, Location, and Contact. The right sidebar shows properties for the selected item, including Name, Type, Location, Contact, and various parameters like VMware, XenServer, and SNMP.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
365_SERVICE_UNIT_1	Microsoft 365 Service Unit				MUMBAI	
AGT-PC	Windows 7 Ultimate		Yes			
AI-2019-001	Windows 10 Pro		Yes			
AI-2019-002	Windows 10 Pro					
AI-2019-003	Windows 10 Pro					
AI-2019-004	Windows 10 Pro					
AI-2019-005	Windows 10 Pro					
AI-2019-006	Windows 10 Pro					
AI-2019-007	Windows 10 Pro					
AI-2019-008	Windows Server					
AI-76	Windows 8.1 Pro N					
AI-AD-4	Windows 10 Pro					
AI-MFC-101-W10	Windows 10 Pro					
AI-QC	Windows 10 Pro					
AI-QC-001	Windows Server					
AI-QC-01	Windows 7 Ultimate					
AI-QC-06	Windows 10 Pro					
AI-WEB-47	Windows 10 Pro					
AI-WEB-NEW	Windows 10 Pro					
AI-WIN67	Windows Server					
AILAP01	Windows 10 Pro				MUMBAI	
AIWEB	Windows 10 Pro					
AIS-TEST	Windows Storage Server 2016 Standard		Yes			
AIS-TEST-ONE	Windows Storage Server 2016 Standard		Yes			
AIS-TSET-PC	Windows 7 Ultimate		Yes			
ANYTIME	Windows 10 Pro		Yes			
ANYTIME-SLHMF7B	Windows XP Professional		Yes			
ANYTIME-SUPPORT	Windows Server		Yes			
ATS-009	Windows 10 Pro		Yes			

Add the name of the server and select **Windows Server** as the Type:

The screenshot shows the 'Manually Add An Entry' dialog box in ARGENT OMEGA. The dialog has a blue header with the title 'Manually Add An Entry' and a 'D2B' button in the top right corner. The form contains the following fields:

- Name:** AI-WIN-67
- Alias:** (empty)
- Domain:** (empty)
- VM Hosting Environment:** None
- Type:** Windows Server (highlighted in red)
- Network Group:** Demo Group
- Location:** THIRUVANANTHAPURAM

At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

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

The screenshot shows the ARGENT OMEGA (2.2A-2204-T1) interface. The main window displays a table of servers with columns for Network Group Or Machine, Type, Alias, Licensed, Suspend, Location, and Contact. The server 'AI-WIN-67' is highlighted in red. To the right, the 'Properties' panel for 'AI-WIN-67' is visible, showing details such as Name, Licensed Products, Global Security Object (SSO), Windows Server, Hosting Environment, SNMP Managed, SQL Server Installed, TCP Parameters, System Info Caching Minutes, Monitoring Level, Tier, Tag, Location, Contact, Owner Accounts, Time Zone Settings, Critical, Ignored, Logical Dependency, Installed Applications, and Extended Properties.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
ES11-2016	Windows Storage Server 2016 Standard		Yes			
TEST10-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST3-2016	Windows Storage Server 2016 Standard		Yes			
TEST4-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST5-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST6-2012R2	Windows Server 2012 R2 Standard		Yes			
TESTNODE_1SAMPLE_1_2SAMPLE_1_3EAMP...	Windows Server 2008 R2 Standard		Yes			
TRIV-NAS-001	Windows Server		Yes			
TRV-102-0049	Windows 7 Ultimate		Yes			
VS2005	Windows Server 2008 R2 Standard		Yes			
WEB-2012	Windows Server 2012 Standard		Yes			
WIN-2019-2021	Windows Server 2019 Standard		Yes			
WIN-2019-0FF-365	Windows Server 2019 Standard		Yes			
WIN-2020-1IS-OL	Windows Server 2022 Standard Evaluation		Yes			
WIN-2022	Windows Server 2022 Standard Evaluation		Yes			
WIN-17270504EHR	Windows Server 2012 R2 Standard		Yes			
WIN-MPC-TEST	Windows Server 2012 R2 Standard		Yes			
WIN-OL2016	Windows Server 2019 Standard		Yes			
WIN10-MFC	Windows 10 Pro		Yes			
WIN2000	Windows 2000 Professional		Yes			
WIN2000SERVER	Windows 2000 Server		Yes			
WIN2008-TEST1	Windows Server 2008 R2 Standard		Yes			
WIN2008-TEST2	Windows Server 2008 R2 Standard		Yes			
WIN2008-TEST3	Windows Server 2008 R2 Standard		Yes			
WIN2012R2-TEST-	Windows Server		Yes			
WIN2012R2-TEST-MFC	Windows Server 2012 R2 Standard		Yes			
WIN2016-TEST	Windows Storage Server 2016 Standard		Yes			
WIN2016-TEST2	Windows Storage Server 2016 Standard		Yes			
WIN2016-TEST3	Windows Storage Server 2016 Standard		Yes			
WIN2016TEST2021	Windows Server 2016 Standard		Yes			
WINXP	Windows XP Professional		Yes			
AI-WIN-67	Windows Server				THIRUVANANTHAPURAM	

Linux Devices, Microsoft 365 Service Units and IP Devices can be added using the same method:

The screenshot shows the 'Manually Add An Entry' dialog box. The fields are as follows:

- Name:** AI-LIN-23
- Alias:** (empty)
- Domain:** (empty)
- VM Hosting Environment:** None
- Type:** Linux (highlighted with a red box)
- Network Group:** Demo Group
- Location:** THIRUVANANTHAPURAM

Buttons for 'OK' and 'Cancel' are at the bottom.

Manually Add An Entry D2B

Name:

Alias:

Domain:

VM Hosting Environment:

Type:

Network Group:

Location:

ARGENT OMEGA (2.2A-2204-T1) First Production Version D2

Home Theme Argent Instant Help About Logout

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
TEST	Windows Storage Server 2016 Standard		Yes			
TEST-2012R2-MFC	Windows Server 2012 R2 Standard		Yes			
TEST-DATACENTER-2016	Windows Server 2016 Datacenter Evaluation		Yes			
TEST-Q42	Windows Server 2008 R2 Standard		Yes			
TEST-VM-152019	Windows 10 Pro		Yes			
TEST1-2016	Windows Storage Server 2016 Standard		Yes			
TEST10-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST3-2016	Windows Storage Server 2016 Standard		Yes			
TEST4-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST5-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST6-2012R2	Windows Server 2012 R2 Standard		Yes			
TESTNODE_1SAMPLE_1_2SAMPLE_1_3SAMP...	Windows Server 2008 R2 Standard		Yes			
TRV-NAS-001	Windows Server		Yes			
TRV-102-0049	Windows 7 Ultimate		Yes			
VS2005	Windows Server 2008 R2 Standard		Yes			
WEB-2012	Windows Server 2012 Standard		Yes			
WIN-2019-2021	Windows Server 2019 Standard		Yes			
WIN-2019-09F-365	Windows Server 2019 Standard		Yes			
WIN-20200-118-OL	Windows Server 2022 Standard Evaluation		Yes			
WIN-2022	Windows Server 2022 Standard Evaluation		Yes			
WIN-17270504EHR	Windows Server 2012 R2 Standard		Yes			
WIN-MFC-TEST	Windows Server 2012 R2 Standard		Yes			
WIN-OL2016	Windows Server 2019 Standard		Yes			
WIN10-MFC	Windows 10 Pro		Yes			
WIN2012R2-TEST-	Windows Server		Yes			
WIN2012R2-TEST-MFC	Windows Server 2012 R2 Standard		Yes			
WIN2016-TEST	Windows Storage Server 2016 Standard		Yes			
WIN2016TEST2021	Windows Server 2016 Standard		Yes			
AI-WIN-67	Windows Server				THIRUVANANTHAPURAM	
AI-LIN-23	Linux				THIRUVANANTHAPURAM	
AI-M365	Microsoft 365 Service Unit				THIRUVANANTHAPURAM	
First Network Group	Network Group				MUMBAI	

Properties

Group Or Key | Value

Contact

Description

Extended Properties

Location

Name | Demo Group

SNMP Parameters

Type | Network Group

VMware Parameters

XenServer Parameters

Display Options

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

Manually Add An Entry D2B

Name:

Alias:

Domain:

VM Hosting Environment:

Type:

Network Group:

Location:

ARGENT OMEGA (2.2A-2204-T1) Home Theme Argent Instant Help About Logout

Search Server Or Device Network Group Scan Network Properties

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
TEST	Windows Storage Server 2016 Standard		Yes			
TEST-2012R2-MFC	Windows Server 2012 R2 Standard		Yes			
TEST-DATACENTER-2016	Windows Server 2016 Datacenter Evaluation		Yes			
TEST-QA-2	Windows Server 2008 R2 Standard		Yes			
TEST-VN-VS2019	Windows 10 Pro		Yes			
TEST1-2016	Windows Storage Server 2016 Standard		Yes			
TEST10-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST3-2016	Windows Storage Server 2016 Standard		Yes			
TEST4-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST5-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST6-2012R2	Windows Server 2012 R2 Standard		Yes			
TESTNODE_18AMPLE_1_28AMPLE_1_38AMP...	Windows Server 2008 R2 Standard		Yes			
TRV-NAS-001	Windows Server		Yes			
TRV-102-0049	Windows 7 Ultimate		Yes			
VS2005	Windows Server 2008 R2 Standard		Yes			
WEB-2012	Windows Server 2012 Standard		Yes			
WIN-2019-2021	Windows Server 2019 Standard		Yes			
WIN-2019-OPP-365	Windows Server 2019 Standard		Yes			
WIN-2020-119-OL	Windows Server 2022 Standard Evaluation		Yes			
WIN-2022	Windows Server 2022 Standard Evaluation		Yes			
WIN-1727G5G4EHR	Windows Server 2012 R2 Standard		Yes			
WIN-MFC-TEST	Windows Server 2012 R2 Standard		Yes			
WIN-OL2016	Windows Server 2019 Standard		Yes			
WIN10-MFC	Windows 10 Pro		Yes			
WIN2012R2-TEST-	Windows Server		Yes			
WIN2012R2-TEST-MFC	Windows Server 2012 R2 Standard		Yes			
WIN2016-TEST	Windows Storage Server 2016 Standard		Yes			
WIN2016TEST2021	Windows Server 2016 Standard		Yes			
AZ-WIN-67	Windows Server				THIRUVANANTHAPURAM	
AZ-LIN-22	Linux				THIRUVANANTHAPURAM	
AZ-M365	Microsoft 365 Service Unit				THIRUVANANTHAPURAM	
First Network Group	Network Group				MUMBAI	

Properties

Group Or Key	Value
Contact	
Description	
Extended Properties	
Location	
Name	Demo Group
SNMP Parameters	
Type	Network Group
VMware Parameters	
XenServer Parameters	

Display Options

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

Bulk Licensing

Licensing 11 servers is not such a chore, but licensing 77,000 servers is a major undertaking with most vendors.

Not so with Argent.

Instead of individually licensing each server or device in the CMDB-X, Argent Omega provides a **Bulk Licensing** feature to license multiple servers or devices at a time.

After adding a server or device, select **Bulk Licensing** from the right click menu:

The screenshot displays the Argent Omega web interface. At the top, the header includes the logo 'ARGENT OMEGA (2.2A-2204-T1) Pre-Production Version' and navigation links for Home, Theme, Argent Instant Help, About, and Logout. Below the header is a search bar and a table of server entries. The table has columns for Network Group Or Machine, Type, Alias, Licensed, Suspend, Location, and Contact. A context menu is open over the row for 'WIN-2022', with 'Bulk Licensing' highlighted in red. The context menu options include Refresh, Suspend Monitoring, Production, Save Changes, Info, Add Property, Delete, Discover Neighbor Links, Wireless Clients, Set Critical Flag, Set Ignore Flag, Manually Add Server Or Device, Test Connectivity, Bulk Licensing, Export To Excel CSV, Backup CMDB-X Database, and Restore. On the right side, there is a 'Properties' panel for the selected server, showing various attributes like Alias, Contact, Critical, Description, and Monitoring Level.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
TEST-2012R2-MFC	Windows Server 2012 R2 Standard		Yes			
TEST-DATACENTER-2016	Windows Server 2016 Datacenter Evaluation		Yes			
TEST-QA-2	Windows Server 2008 R2 Standard		Yes			
TEST-VN-VS2019	Windows 10 Pro		Yes			
TEST1-2016	Windows Storage Server 2016 Standard					
TEST10-2012R2	Windows Server 2012 R2 Standard					
TEST3-2016	Windows Storage Server 2016 Standard					
TEST4-2012R2	Windows Server 2012 R2 Standard					
TEST5-2012R2	Windows Server 2012 R2 Standard					
TEST6-2012R2	Windows Server 2012 R2 Standard					
TESTNODE_1SAMPLE_1_2SAMPLE_1_3SAMP...	Windows Server 2008 R2 Standard					
TRV-NAS-001	Windows Server					
TRV-102-0049	Windows 7 Ultimate					
VS2005	Windows Server 2008 R2 Standard					
WEB-2012	Windows Server 2012 Standard					
WIN-2019-2021	Windows Server 2019 Standard					
WIN-2019-0FF-265	Windows Server 2019 Standard					
WIN-2020-129-CL	Windows Server 2022 Standard Evaluation					
WIN-2022	Windows Server 2022 Standard Evaluation					
WIN-17270504HR	Windows Server 2012 R2 Standard					
WIN-MFC-TEST	Windows Server 2019 R2 Standard					
WIN-OL2016	Windows Server 2019 Standard					
WIN10-MFC	Windows 10 Pro		Yes			
WIN2012R2-TEST-	Windows Server		Yes			
WIN2012R2-TEST-MFC	Windows Server 2012 R2 Standard		Yes			
WIN2016-TEST	Windows Storage Server 2016 Standard		Yes			
WIN2016TEST2021	Windows Server 2016 Standard		Yes			
A1-WIN-47	Windows Server				THIRUVANANTHAPURAM	
A1-LIN-23	Linux				THIRUVANANTHAPURAM	

Select Argent Compliance Automator in the 'Argent Omega Products' drop-down selection.

Select the Node Types in the 'Node Type' drop-down selection for the new servers and devices to be added:

License Selected Server Or Devices D2L

Argent Omega Products: Argent Compliance Automator

Node Type: Windows Server, Linux, Microsoft 365 Service Unit

Server Or Devices: Select All Clear Toggle

AI

- AI-WIN-67
- AI-LIN-23
- AI-M365

Remove License For Selected Nodes

OK Cancel

Bulk Licensing Results

```
06 Jun 2022 12:06:28 Licensed AI-M365
06 Jun 2022 12:06:28 Licensed AI-WIN-67
06 Jun 2022 12:06:28 Licensed AI-LIN-23
06 Jun 2022 12:06:28 ****
06 Jun 2022 12:06:28 Total of 3 nodes licensed (Skipped: 0, Failed: 0)
```

Print Close

CMDB-X Properties

Name	Name of the server
Licensed Products	Licensed products of a server or device
Alias	Alias name of the server or device
Type	Type of server or device – example: Windows Server, Linux or Other
Hosting Environment	Hosting Environment regarding the server or device
SNMP Managed	SNMP managed on server or device or not.
SQL Server Installed	Option to specify SQL Server details to monitor the server using Argent Omega for SQL Server
TCP Parameters	Options for setting TCP parameters for the server or device. The options are as follows: <ul style="list-style-type: none">• Timeout• Retry
Tier	1 to 9 (can be used for customer's internal hierarchy or priority, etc.)
Tag	String variable used as an identifier
Location	Location of the server or device (This information is used to determine the device location on Google Maps.)
Contact	Person or people responsible for the device
Preferred Generators	Setting Generator for server or device
Time Zone Settings	Option to set Time Zone Settings
Critical	Option to set a server or device as critical
Ignored	Option to set a server or device as ignored
Logical Dependency	Shows Logical Dependency of a server or device
Installed Applications	Shows Installed Applications of a server or device
Extended Properties	Option to specify custom properties

Select a server or device to set any of its properties.

Selection of multiple devices are supported to set common properties like Location, Contact, Alert Email, Tier, Tag, Maintenance Start and End dates and Ignore Flag.

A combination of (Shift/Ctrl + left mouse click) can be used for multiple selections:

The screenshot shows the ARGENT OMEGA web interface. The main table lists various servers and devices with columns for Network Group, Type, Alias, Licensed, Suspend, Location, and Contact. The right-hand panel displays the 'Properties' for a selected device, with a red box highlighting the 'Group Or Key' and 'Value' fields. The 'Group Or Key' field is set to 'Critical' and the 'Value' field is set to 'No'. Other properties include Global Security Object (GSO), Hosting Environment, Ignored, Installed Applications, Licensed Products, Location, Logical Dependency, Monitoring Level, Name, Preferred Generators, System Info Caching Minutes, Tag, TCP Parameters, Retry, Timeout, Tier, Time Zone Settings, Windows Server, 64-bit OS, Authentication, Cluster Name, and Domain.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
D3PC-14	Windows 10 Pro		Yes			
D3PC-21	Windows 10 Pro		Yes			
DC-001	Windows 10 Pro		Yes			
DESKTOP-AD-HR	Windows 10 Pro		Yes			
DND-SUPPORT	Windows Server 2008 R2 Standard		Yes			
MOBOX	URL Object		Yes		MUMBAI	
WIN2000	Windows 2000 Professional		Yes			
WIN2000SERVER	Windows 2000 Server		Yes			
WIN2008-TEST1	Windows Server 2008 R2 Standard		Yes			
WIN2008-TEST2	Windows Server 2008 R2 Standard		Yes			
WIN2008-TEST3	Windows Server 2008 R2 Standard		Yes			
WIN2016-TEST2	Windows Storage Server 2016 Standard		Yes			
WIN2016-TEST3	Windows Storage Server 2016 Standard		Yes			
W200P	Windows XP Professional		Yes			
AGT-PC	Windows 7 Ultimate		Yes			
AI-2019-001	Windows 10 Pro		Yes			
AI-2019-002	Windows 10 Pro		Yes			
AI-2019-003	Windows 10 Pro		Yes			
AI-2019-004	Windows 10 Pro		Yes			
AI-2019-005	Windows 10 Pro		Yes			
AI-2019-007	Windows 10 Pro		Yes			
AI-2019-008	Windows Server		Yes			
AI-76	Windows 8.1 Pro N		Yes			
AI-AD-4	Windows 10 Pro		Yes			
AI-MFC-101-W10	Windows 10 Pro		Yes			
AI-QC	Windows 10 Pro		Yes			
AI-QC-001	Windows Server		Yes			
AI-QC-02	Windows 7 Ultimate		Yes			
AI-QC-06	Windows 10 Pro		Yes			

Microsoft 365 Service Unit Credentials

Credentials for monitoring Microsoft 365 Units are added in the CMDB-X screen:

The screenshot shows the ARGENT OMEGA (2.2A-2204-T1) Production Version interface. The main table lists various network devices and their properties. A specific entry, 'TEST_365', is highlighted as a Microsoft 365 Service Unit. The properties panel on the right shows the configuration for this unit, including the administrator email 'test_a@argsoftdev.com', application ID, certificate thumbprint, directory or tenant ID, organization, and SharePoint URL. The monitoring level is set to 'Normal' and the system info caching is set to 720 minutes.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
ARGENT	URL Object		Yes		MUMBAI	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object		Yes		MUMBAI	
SMT2_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes			
192.168.111.5	IP Device		Yes			
AI-2019-009	Windows Server		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			

Group Or Key	Value
Ignore Security Objects Group	
Ignored	No
Installed Applications	
Licensed Products	Argent Compliance Automator/Argent Omega for Microsoft 365
Location	MUMBAI
Logical Dependency	
Microsoft 365 Service Unit	
Administrator	test_a@argsoftdev.com
Application Id	[REDACTED]
Certificate Thumbprint	[REDACTED]
Directory Or Tenant Id	[REDACTED]
Licensed Units	
Organization	[REDACTED]
SharePoint Url	[REDACTED]
SKU	
Monitoring Level	Normal
Name	TEST_365
Owner Accounts	
System Info Caching Minutes	720
Tag	
TCP Parameters	
Tier	6
Time Zone Settings	Same as Location

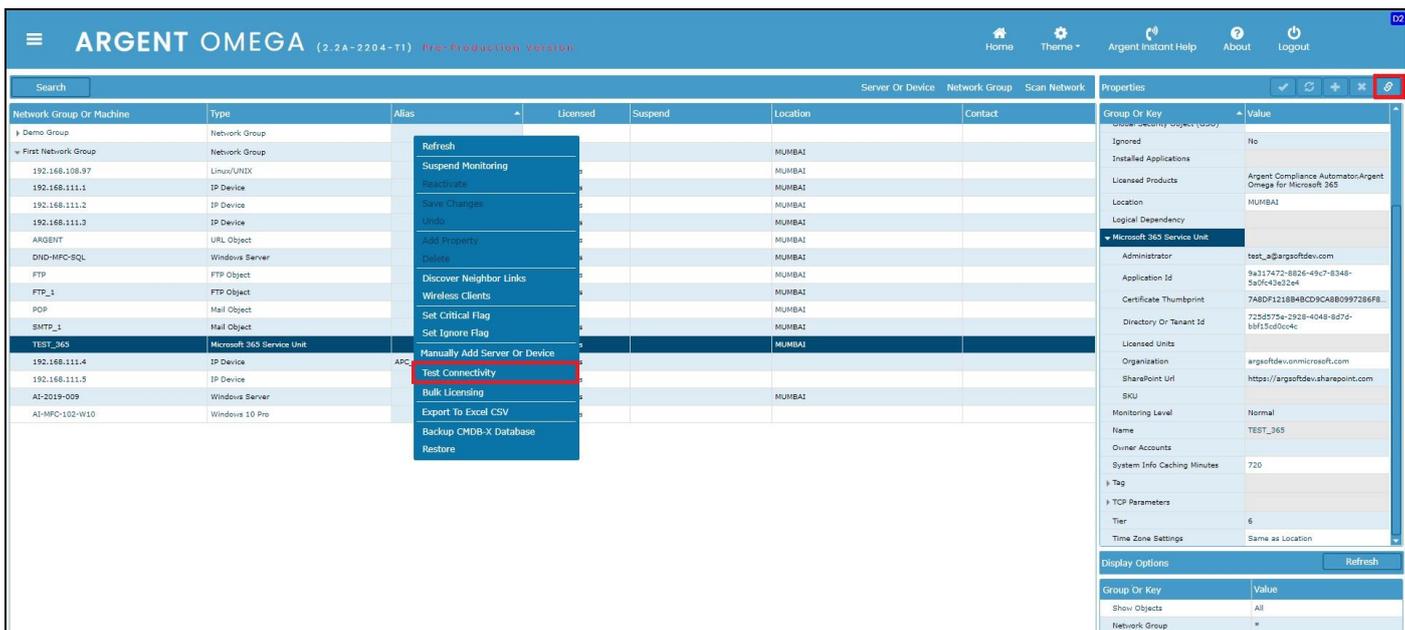
Test Connectivity

A connectivity test can be run to verify the Microsoft 365 Service Unit credentials configured in the CMDB-X.

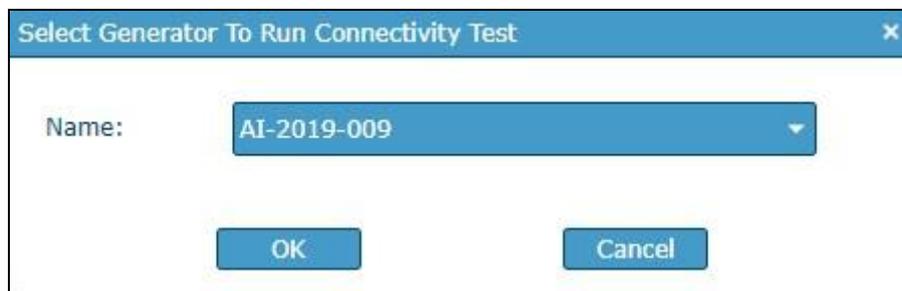
It connects to the following Microsoft 365 components using the configured credentials:

- Azure Active Directory
- Exchange Online
- SharePoint Online
- Microsoft Teams

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



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



The Results are shown:

The screenshot shows a window titled "Connectivity Test Results" with a close button in the top right corner. The window contains the following text:

Argent Omega 2.2.2205.31 Copyright (c) 2022 Argent Software

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

Target Machine: TEST_365

Test At: AI-2019-009

Test Time: Mon, 06 Jun 2022 06:50:20 (UTC)

06:50:20 - Test 1: Access of Azure Active Directory
06:50:20 - PowerShell Module 'AzureAD' (Version: 2.0.2.140)
06:50:24 - [VALID] Registered App has roles: Global Administrator,Application Administrator,Directory Readers,Exchange Administrator
06:50:24 - Found Azure Domains: argsoftdev.com,argsoftdev.onmicrosoft.com
06:50:25 - *** WARNING *** Failed to determined Microsoft 365 License information

06:50:25 - Test 2: Access of Exchange Online
06:50:25 - PowerShell Module: ExchangeOnlineManagement (2.0.5)
06:50:41 - [VALID] Matched SharePoint URL: <https://argsoftdev.sharepoint.com>

06:50:41 - Test 3: Access of SharePoint Online
06:50:41 - PowerShell Module: SharePointPnPPowerShellOnline (3.29.2101.0)
06:50:43 - [VALID]

At the bottom of the window, there are two buttons: "Print" and "Close".

Connectivity tests can also be run against other server or device types using the same method.

Manage The Archive Repository

The Archive Repository defines the SQL Server database to archive compliance data retrieved by the Argent Compliance Automator.

The Archive Repository also defines how long to retain the archived data.

The Argent SIEM-Complete product scans the Archive Repository to generate various statistics and metrics for display in the real-time dashboard.

These statistics can be saved to Argent Forecaster for trend analysis.

The Argent SIEM-Complete product uses built-in Security Intelligence Rules to detect suspicious activities and fire events using the Argent Alert Mechanism.

Benefits Of Archive Repository And Argent SIEM-Complete:

Data Compliance

The Argent Reporter can generate compliance reports for external auditors.

User Activity Monitoring

Suspicious user activities can be easily detected by analyzing logon sessions and file operations.

Insider Threat Detection

Phishing attacks can be stopped and malware found and removed by analyzing firewall, switch, and router logs.

Requests from black-listed IPs and URLs can be prevented by monitoring web server logs.

Zero-day Threats Detection

Malware, such as ransomware, can be detected.

File Integrity Monitoring

Both Windows and Linux have extensive file audit logs.

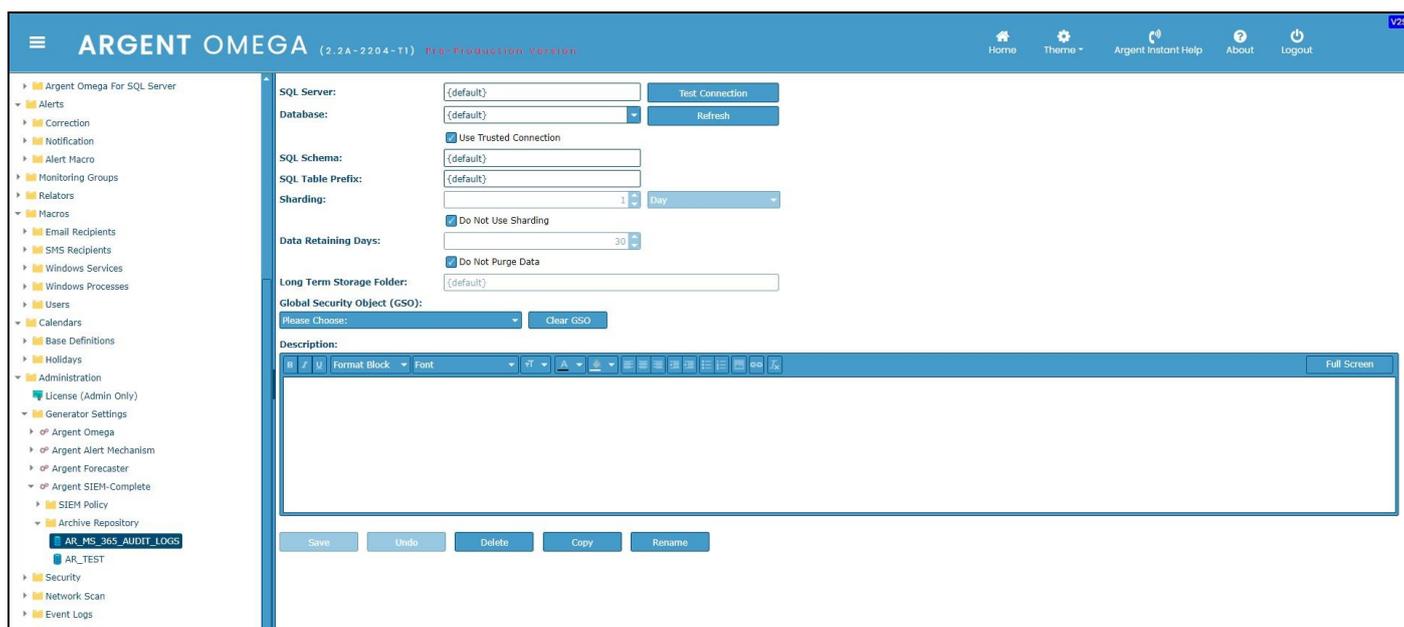
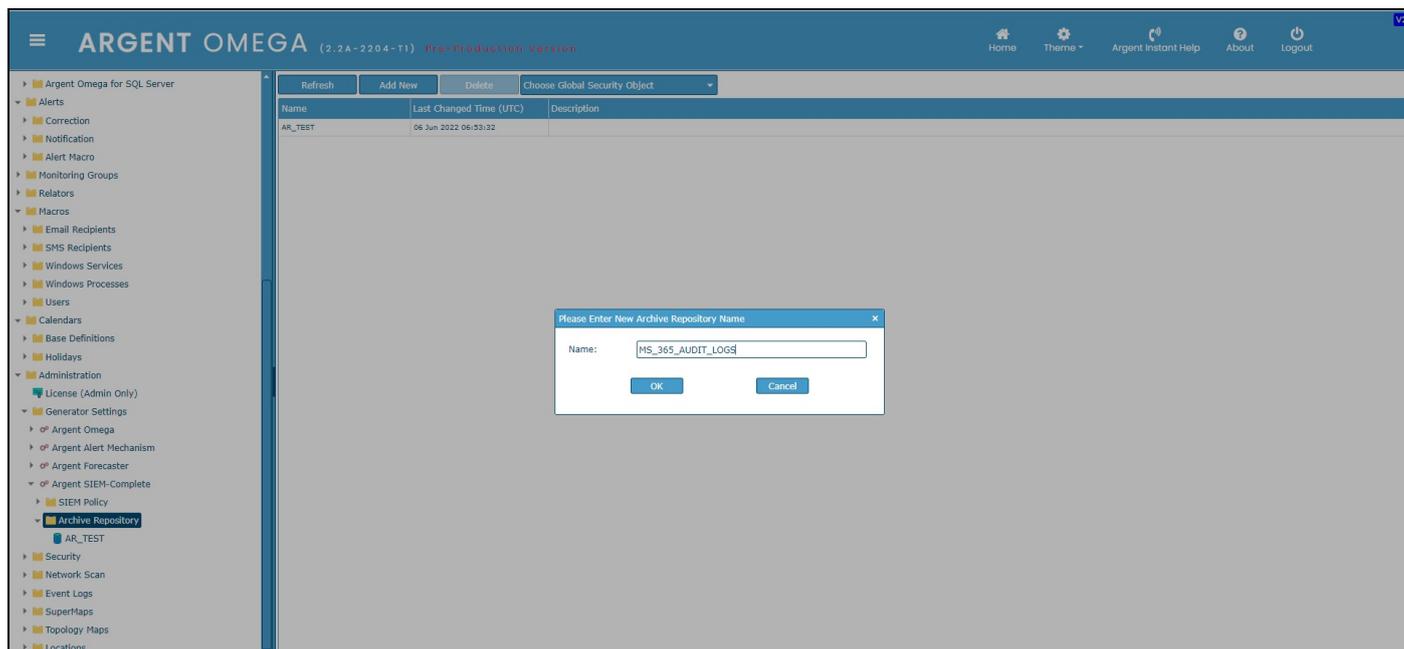
These logs can be very useful for security personnel.

For example, a disgruntled former employee trying to delete thousands of files, can be detected.

Forensic Analysis

Various reports can be generated by the Argent Reporter, as well as online displays of SQL queries.

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



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

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

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

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

Specify the **SQL Table Prefix** to use custom table prefixes for tables that stores compliance audit data. Uncheck the **Do Not Use Sharding** option to use database sharding.

Sharding is a relatively new development whereby a large data base is broken into a number of free-standing databases that can be accessed concurrently. So rather than one long query running against a single massive database, dozens – or hundreds -- of small queries can concurrently run against these small databases; “shard” means "a small part of a whole.”

The Sharding criteria is specified in the **Sharding** field.

Each shard is a separate table in Argent Omega database.

An example would be a customer that wants to retain 12 months of archived log data.

Setting the Sharding field to a value of 1 month would automatically separate the archived data moving forward into separate database tables for each month’s worth of data.

This allows the queries for generating reports and purging old data to run much faster since they are running against smaller databases instead of a single large database.

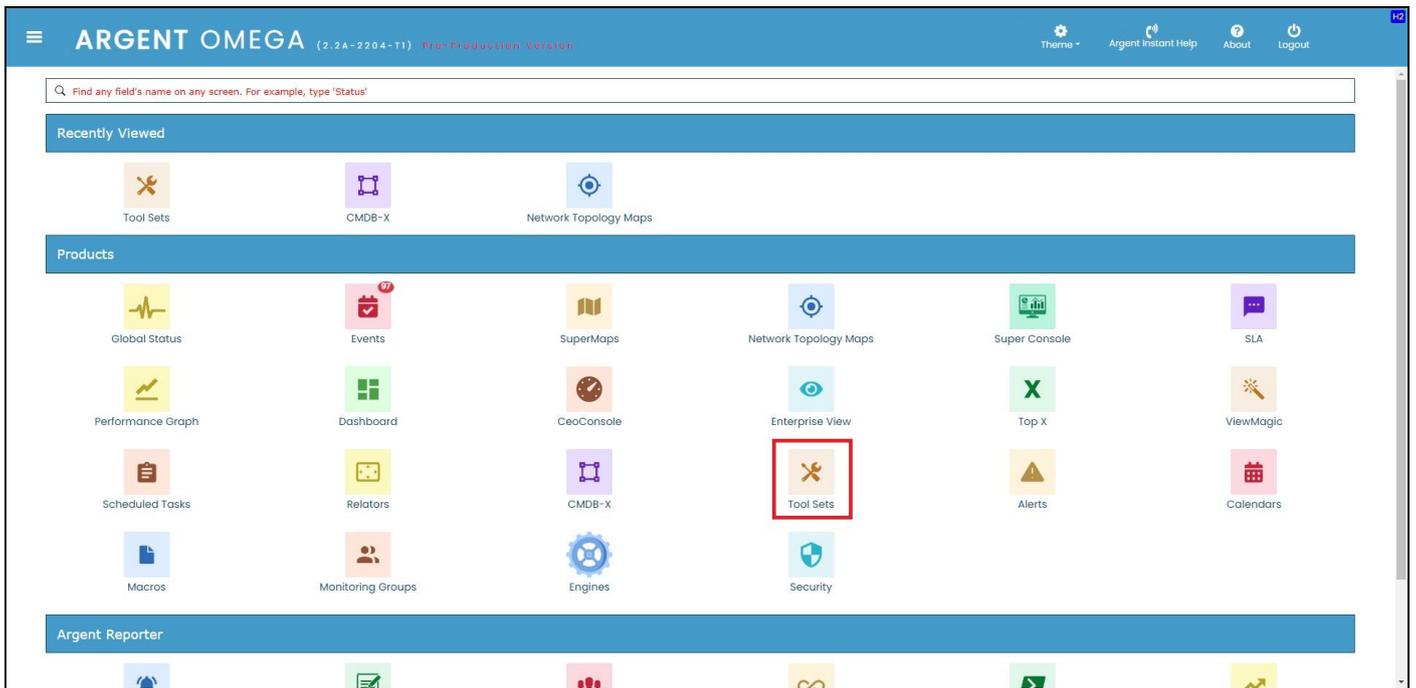
Uncheck the **Do Not Purge Data** option to purge the data after the days specified in **Data Retaining Days** field.

You can configure the newly created Archive Repository in the Argent Compliance Automator Rules.

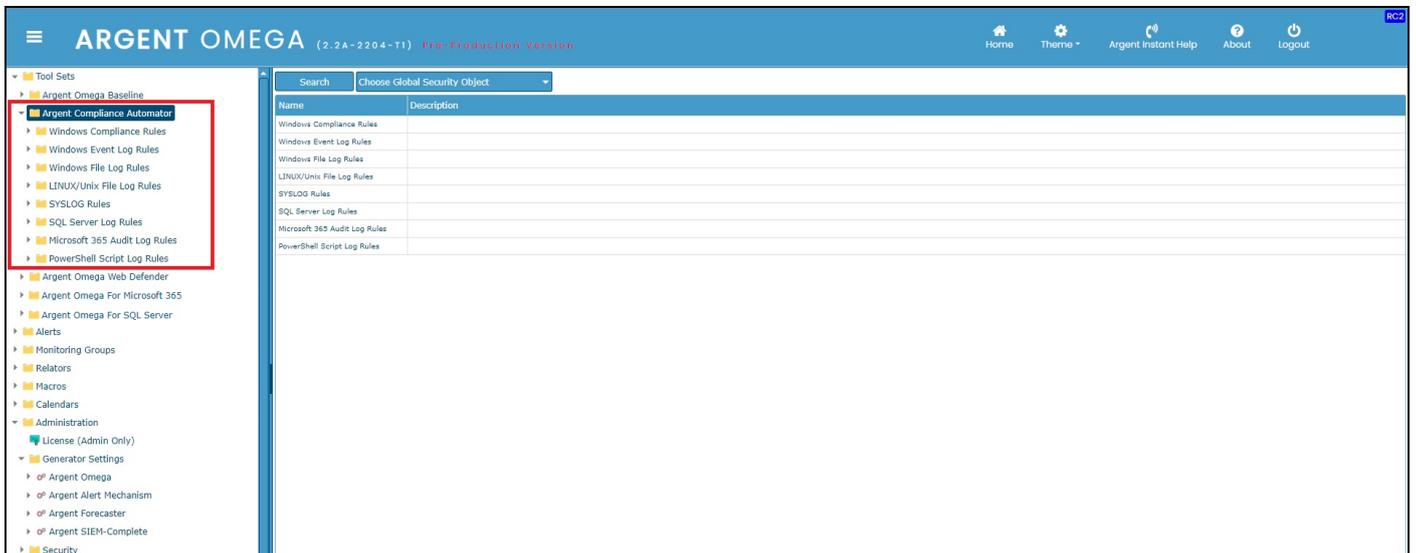
The event data retrieved by the Rule will be archived in the configured Archive Repository.

Argent Compliance Automator

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



Under **Tool Sets**, select **Argent Compliance Automator**:



Argent Compliance Automator consists of different types of Rules:

- * Windows Compliance Rules
- * Windows Event Log Rules
- * Windows File Log Rules
- * Linux or Unix File Log Rules
- * SYSLOG Rules
- * SQL Server Log Rules
- * Microsoft 365 Audit Log Rules

Windows Compliance Rules

This Super Rule performs all critical archiving for Windows Security Logs for current compliance laws, such as Sarbanes-Oxley, HIPAA, GLBA, PCI, etc.

To save disk space, Argent Compliance Automator uses patented technology to archive and compress only the essential data elements.

By using this single Super Rule, all required data from Windows Security Logs are stored in the central Argent database.

From this database, any of the 75 pre-defined audit reports in Argent can be executed, as well as custom reports created by customers (or Argent engineers, at no cost):

The screenshot displays the Argent Omega web interface for configuring a rule. The left sidebar shows a navigation menu with categories like Tool Sets, Alerts, Relators, and Administration. The main content area is titled 'Read Windows Security Log With Method: Automatically Determined'. It includes fields for 'Archive Repository: {default}', 'Skip Security Log Records Over: 24 Hours', and a section for 'In Addition To Compliance Audit Log, Archive Windows Security Log Matching Following Criteria'. This section contains checkboxes for 'Event ID:', 'Event User:', 'Event Category:', and 'Event Source:', each with a corresponding input field. There are also checkboxes for 'Match Case', 'Match Whole Word', and 'Match Regular Expression'. Other options include 'Include Audit Failure Events', 'Read User Data From Custom XPath', 'Alert On Potential Data Loss', 'Alert If Failed To Open Windows Event Log', and 'Save Performance Data To The Argent Forecaster Using Data Store: {default}'. At the bottom, there are 'Tag 1:', 'Tag 2:', and 'Tag 3:' fields, and a 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)' section with time-based filters. The 'Reset Counter' section has radio buttons for 'After Event Is Post' and 'After Event Is Answered'.

The following Rule screen options can be configured to archive Windows Security Events.

The **Read Windows Security Log With Method** option is used to configure the Event Log read method.

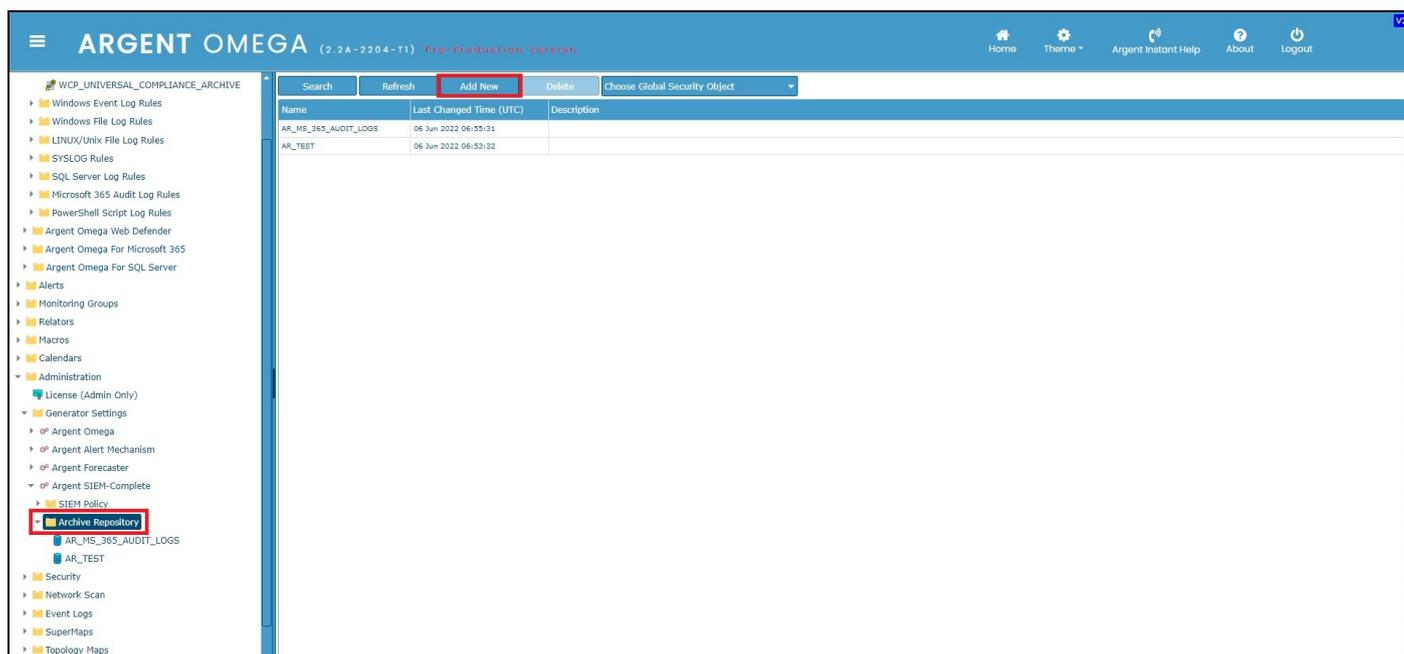
Argent Omega uses the following Event read methods:

- Windows Event Log API
- Legacy Event Logging API
- WMI
- PowerShell Remoting
- Automatically Determined (Default)

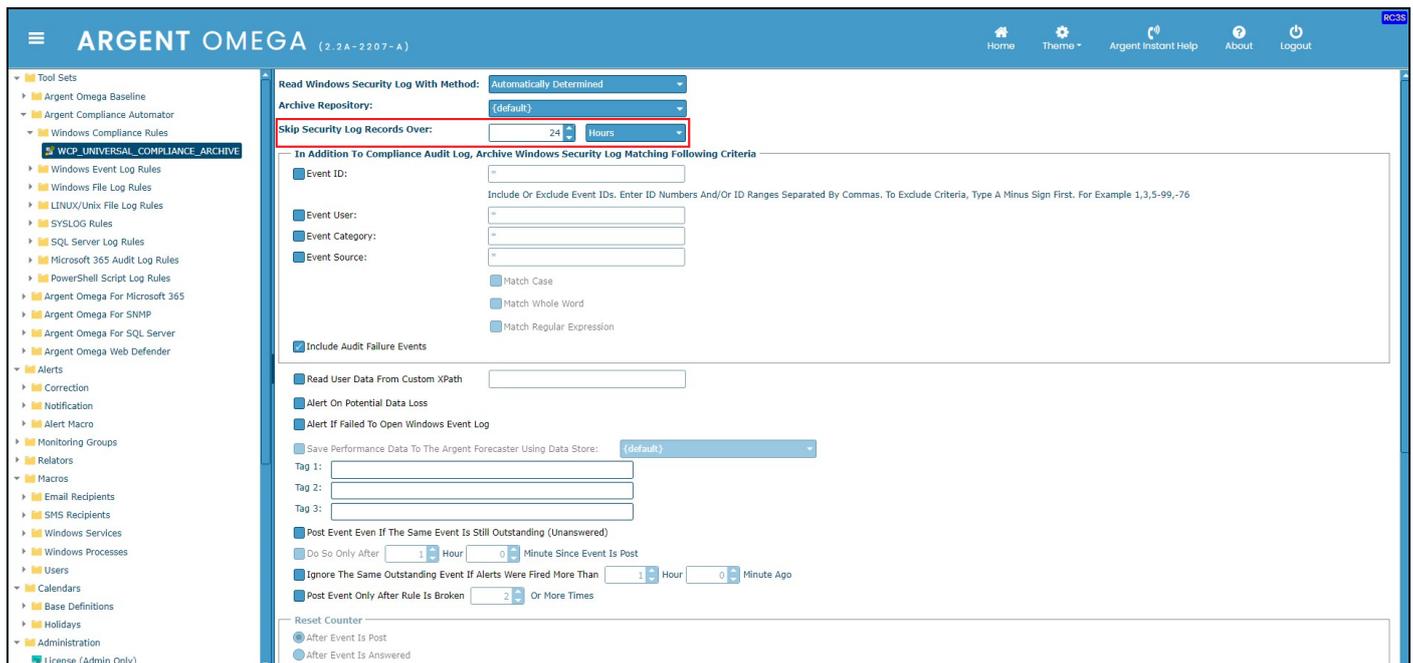
Archive Repository specifies the database in which Event logs to be archived.

Default value **{default}** means Event logs will be archived into the database in which Argent Omega is installed.

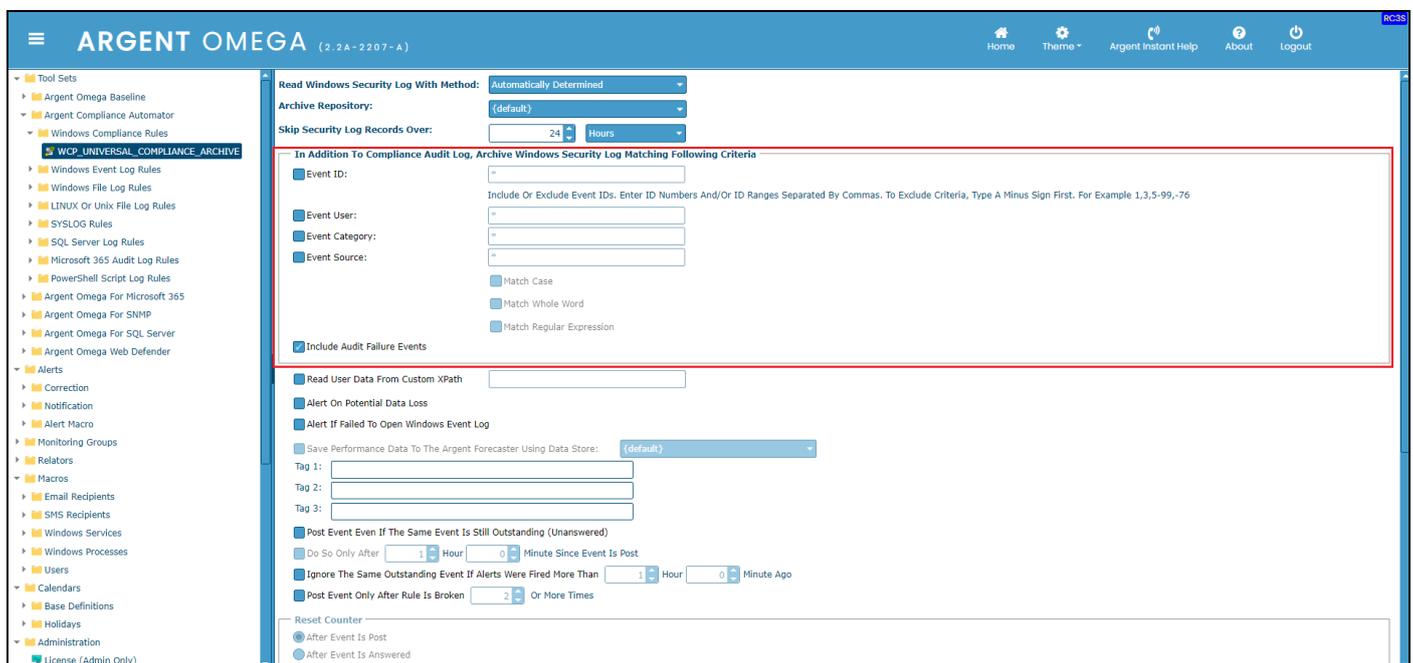
It is possible to create new Archive Repositories in the Administration section:



Use the **Skip Security Log Records Over** field to skip monitoring Security Event Log records that are older than the specified time:



The “**In Addition To Compliance Audit Log...**” section can be used to filter the Event log records to be archived:



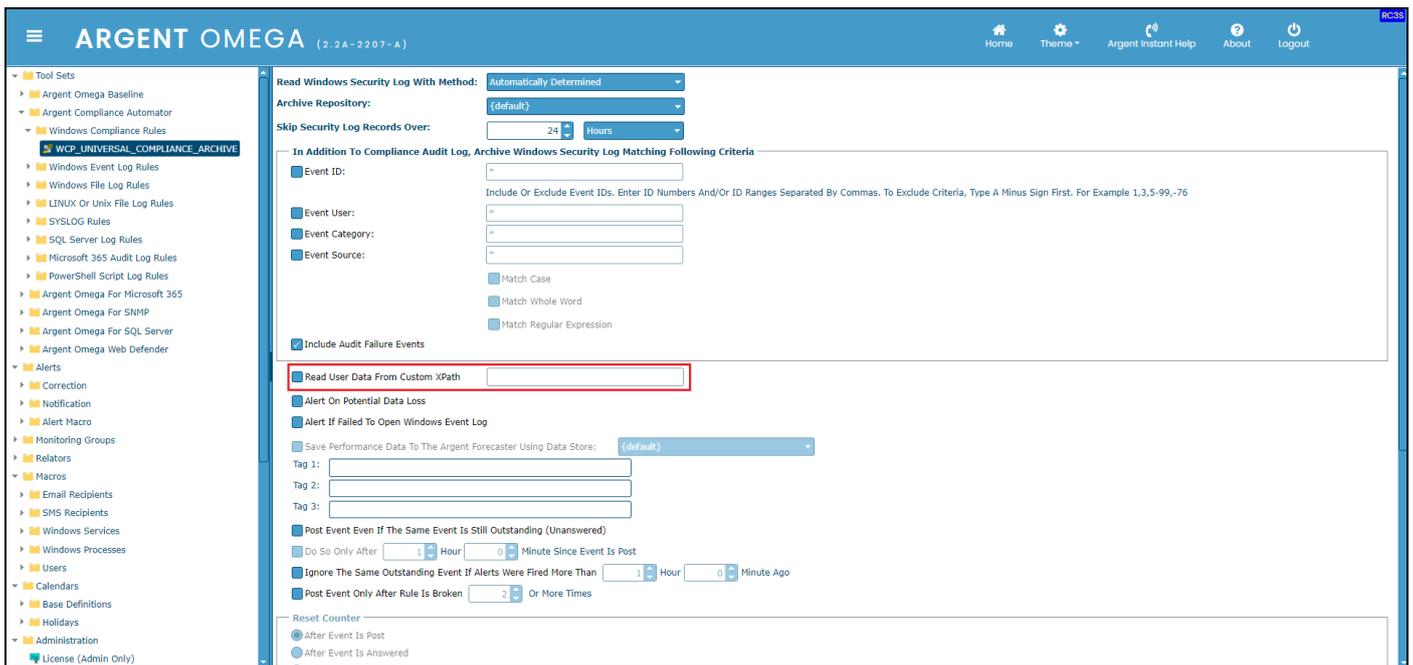
The **Read User Data From Custom XPath** option is used to specify additional filtering criteria for monitored events.

Windows NT6 (Vista or Server 2008) events are saved in XML format.

XPath is a method for selecting specific XML nodes from an XML document.

An example would be filtering on specific fields in the monitored event message body, such as 'Account

Name', 'Logon Type', 'Process Name', etc.



The **Alert If Failed to Open Windows Event Log** option can be used to trigger an alert if the Windows Compliance Rule fails to open the Windows Event Logs on the monitored server.

This can happen if the monitored server is down or if there is a permissions issue connecting to the server.

Windows Event Log Rules

Windows Event Log Rules allow customers to choose and filter on specific Windows Event Log criteria for monitoring or archiving or both.

Windows Event Log Rules can monitor and archive critical security logs across all windows servers and workstations in your network.

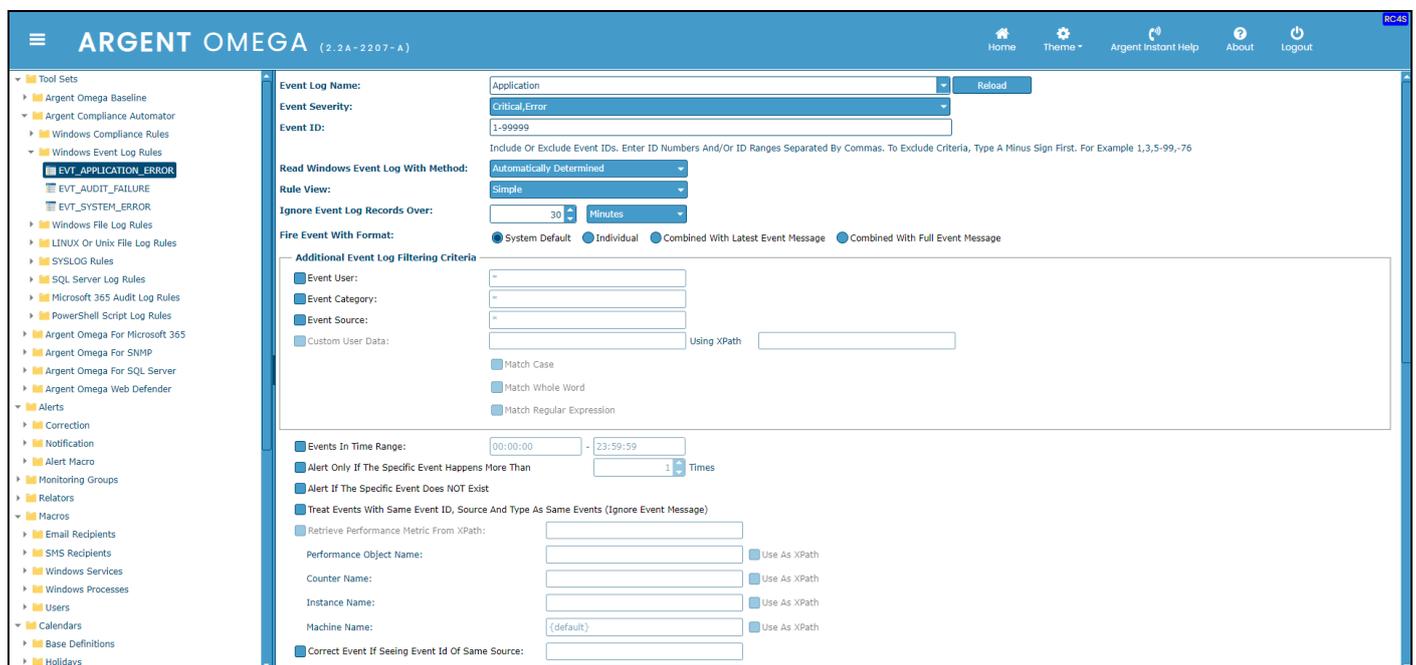
You can easily detect events such as failed logons, bad passwords, account lockouts, failed attempts to access secure files, **security log tampering**, etc.

You can also create any number of Rules to enforce the security policies adopted by your company; this is like an Active Directory policy on steroids.

In addition to Security logs, Windows Event Log Rules can monitor or archive Application, System, Directory Services, DNS Server, File Replication and other event logs.

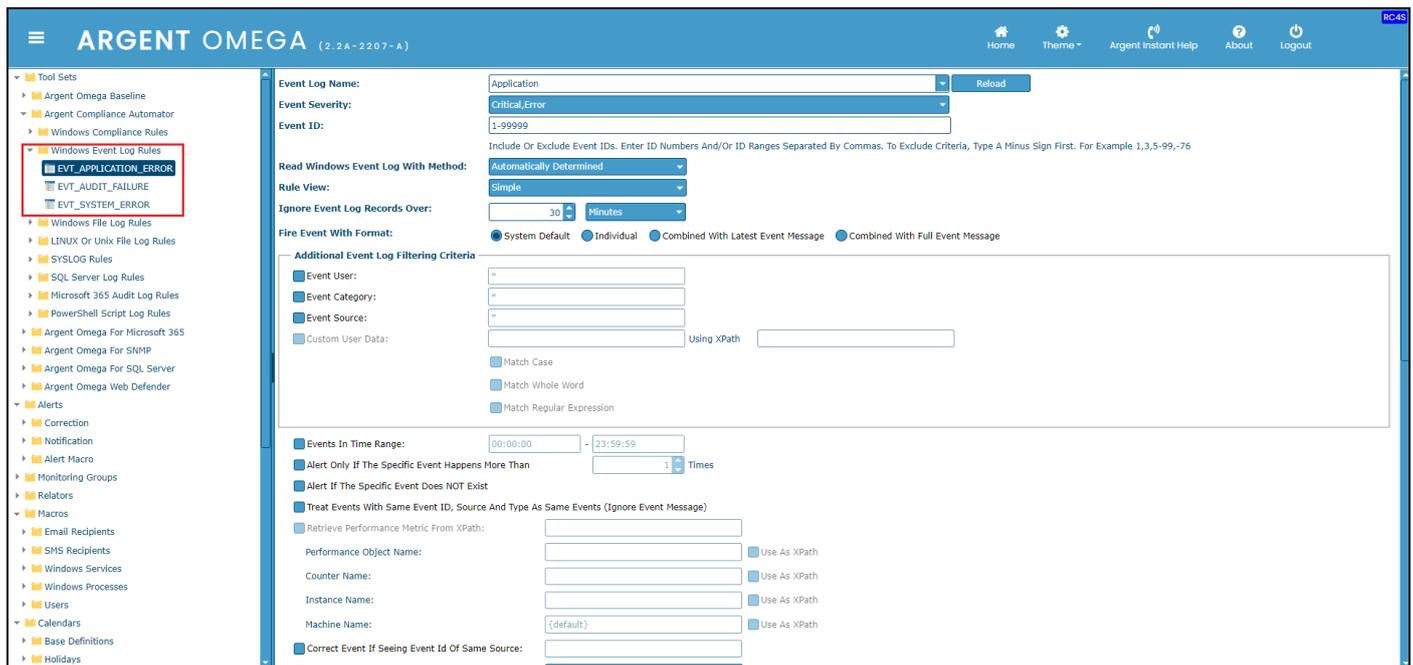
Rules can be configured to monitor events generated by any application, including mission-critical applications like Exchange, IIS, MS-SQL and ISA servers.

Event Log Rule Screen:



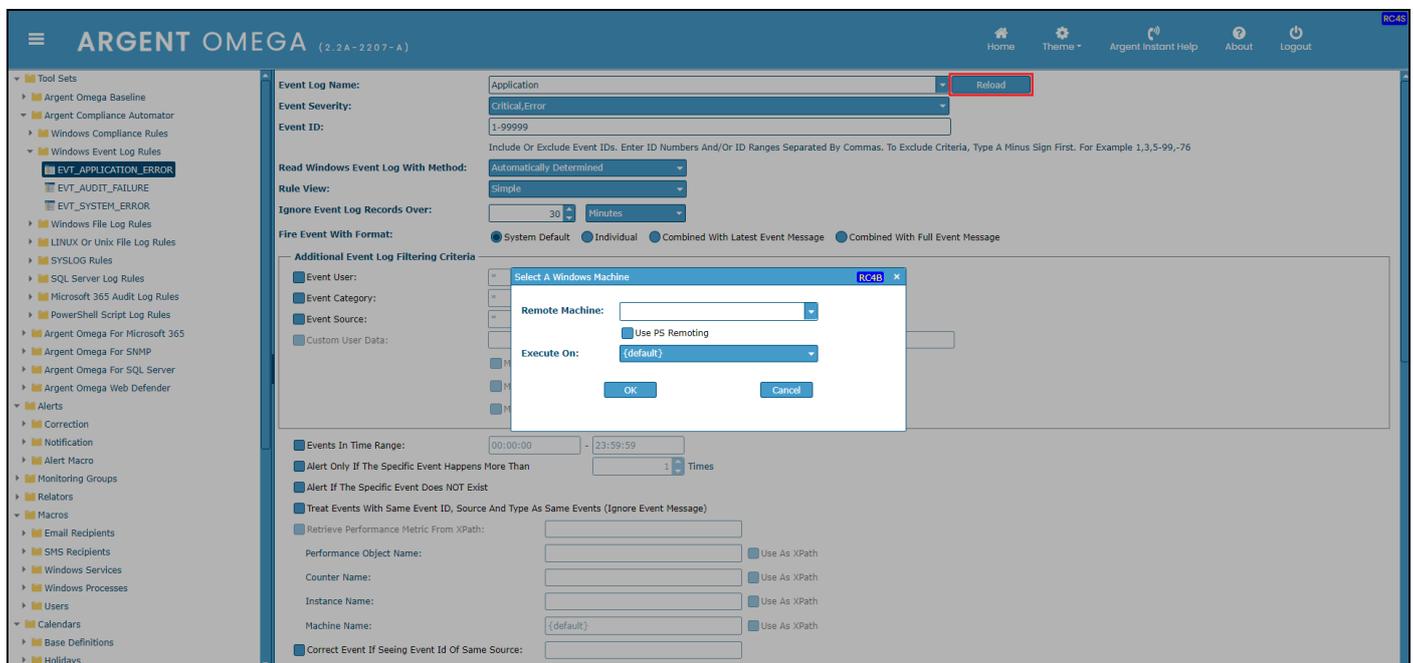
Select any Rule and use the 'Add New' right-click option to create a new Rule in the **Windows Event Log**

Rules:



Event Log Names can be loaded from Licensed Remote or Local Windows machines by clicking on the

Reload button:

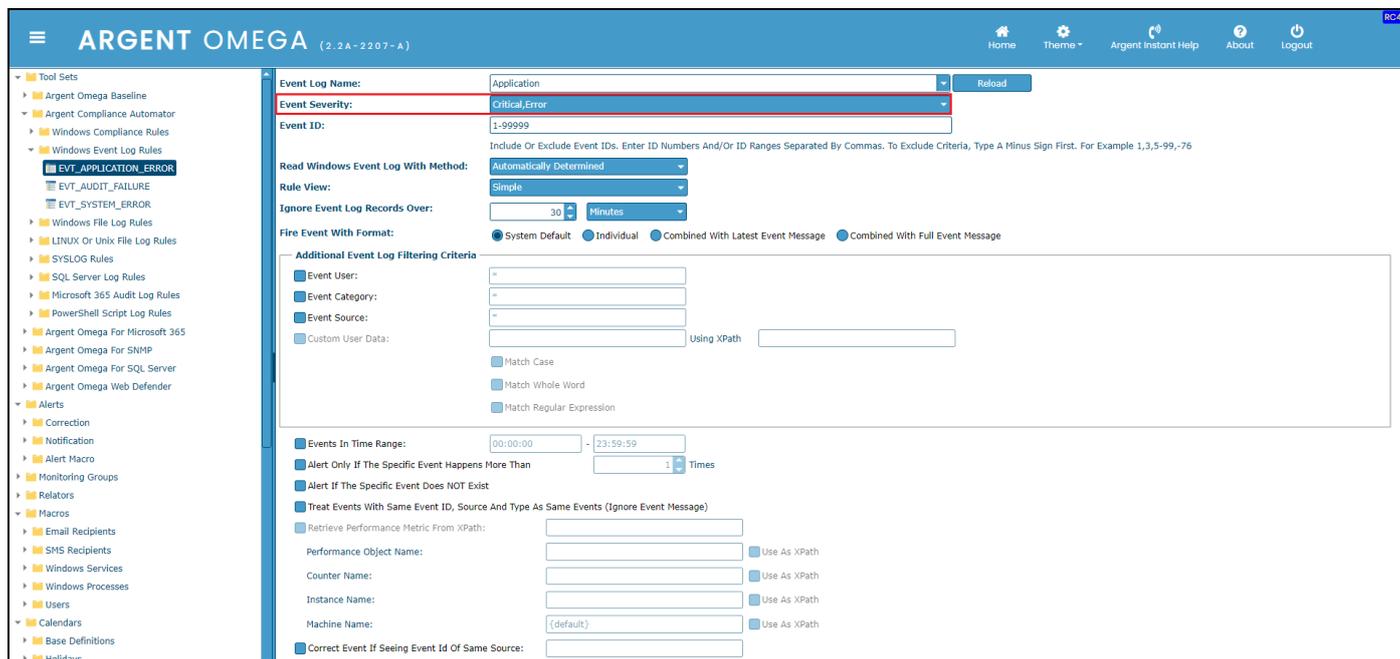


Monitored machines can be selected from the **Remote Machine** combo box.

Check the **Use PowerShell Remoting** option if you want to use the PowerShell Remoting method to retrieve Event logs from the Remote machine.

Select a Generator from the **Execute On** combo box. The selected Generator retrieves Event log names from the specified machine.

Use the **Event Severity** field to filter events by the specified severity level.

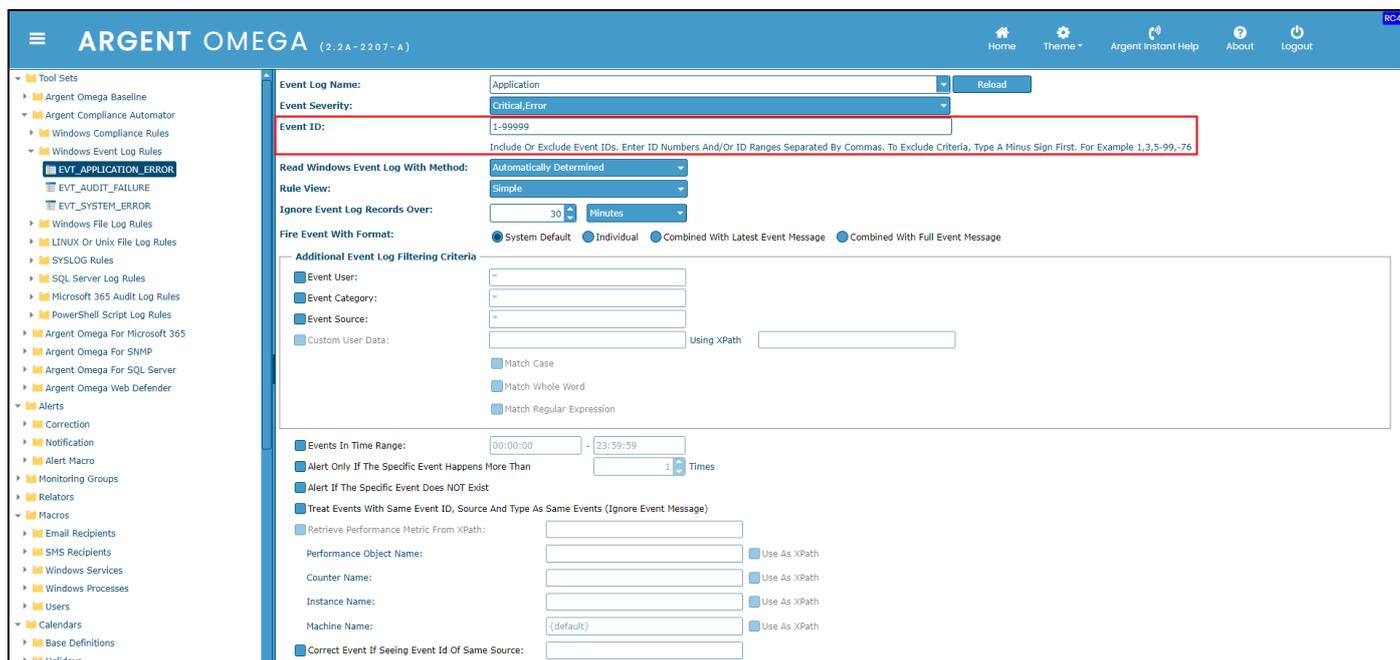


Use the **Event ID** field to specify which Event IDs you'd like the Rule to look for when archiving or triggering events.

Event ID numbers can be added as individual numbers or as ranges separated by commas.

A **minus sign** can be used to exclude monitoring a specific Event ID from the listed Event ID Range.

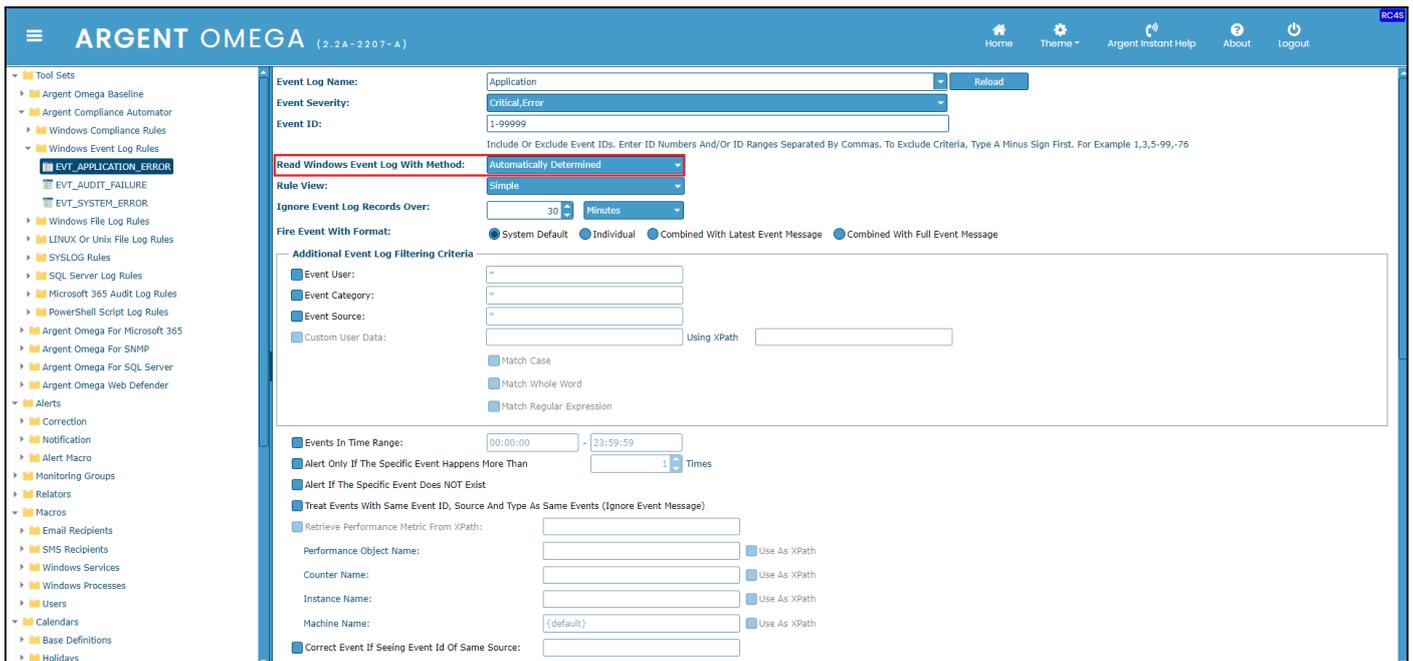
For example: '1,3,5-99, -76'



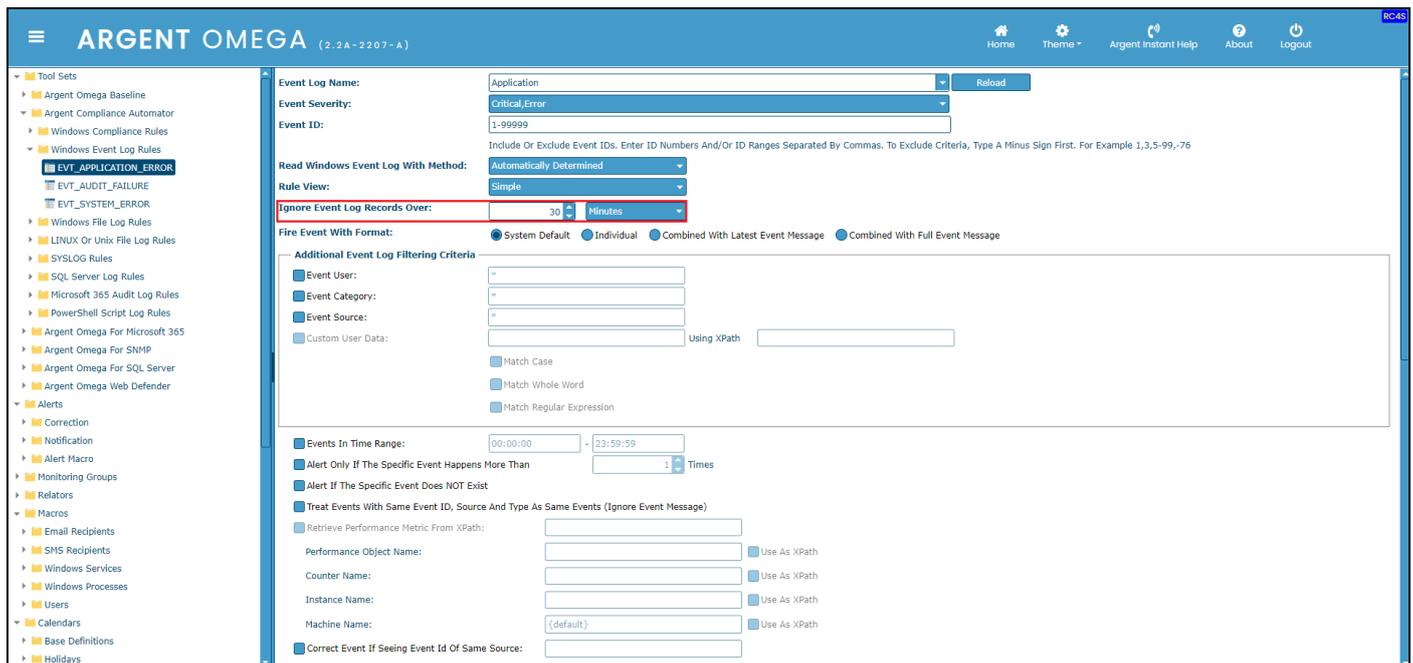
The **Read Windows Security Log With Method** option is used to configure the Event Log Read method.

Argent Omega uses the following Event read methods:

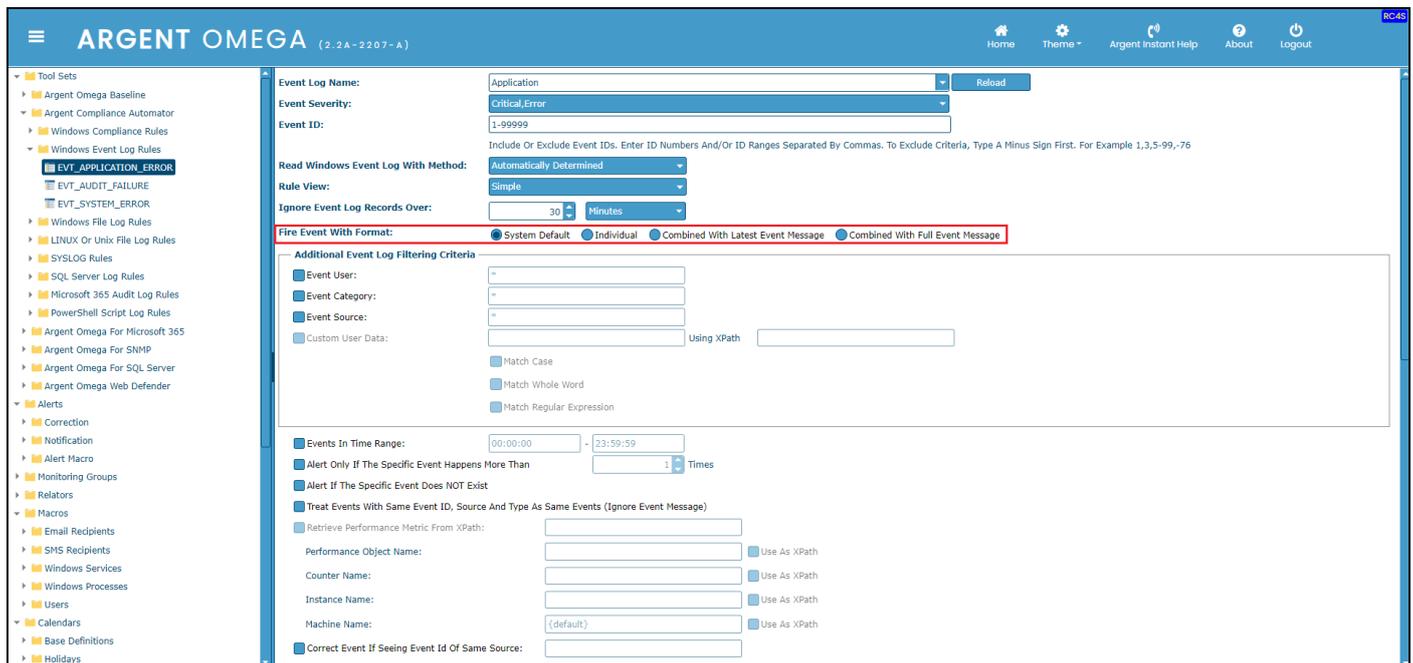
- Windows Event Log API
- Legacy Event Logging API
- WMI
- PowerShell Remoting
- Automatically Determined (Default)



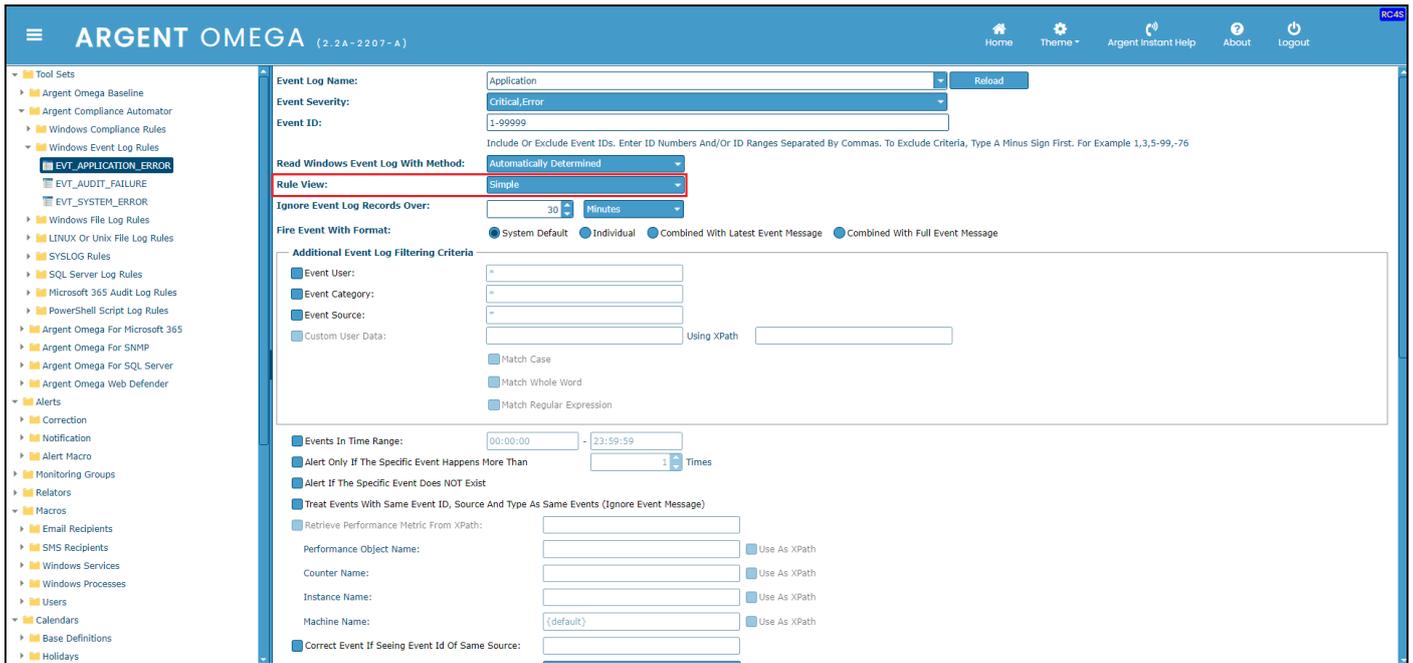
Specify a time period in the **Ignore Event Log Records Over** field to skip monitoring Security Event Log records that are older than the specified time:



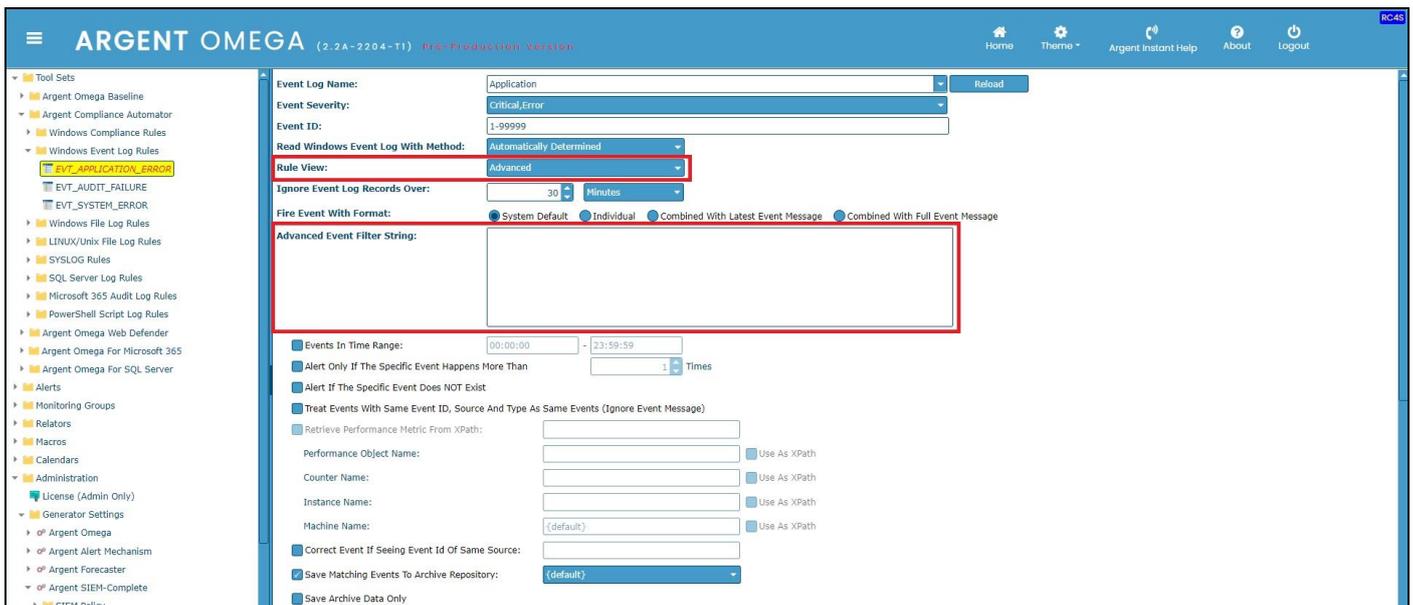
Select the Alert message format in the **Fire Event With Format** section:



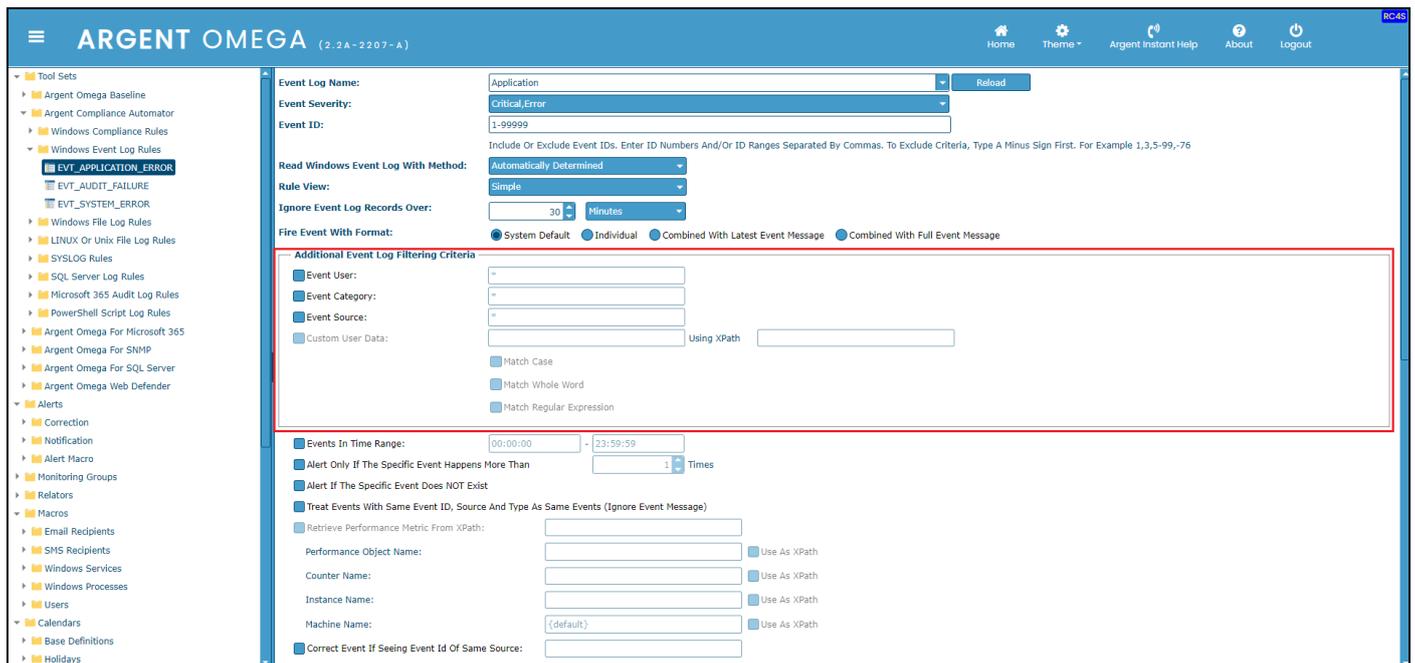
The Rule View can be defined as **Simple** or **Advanced**:



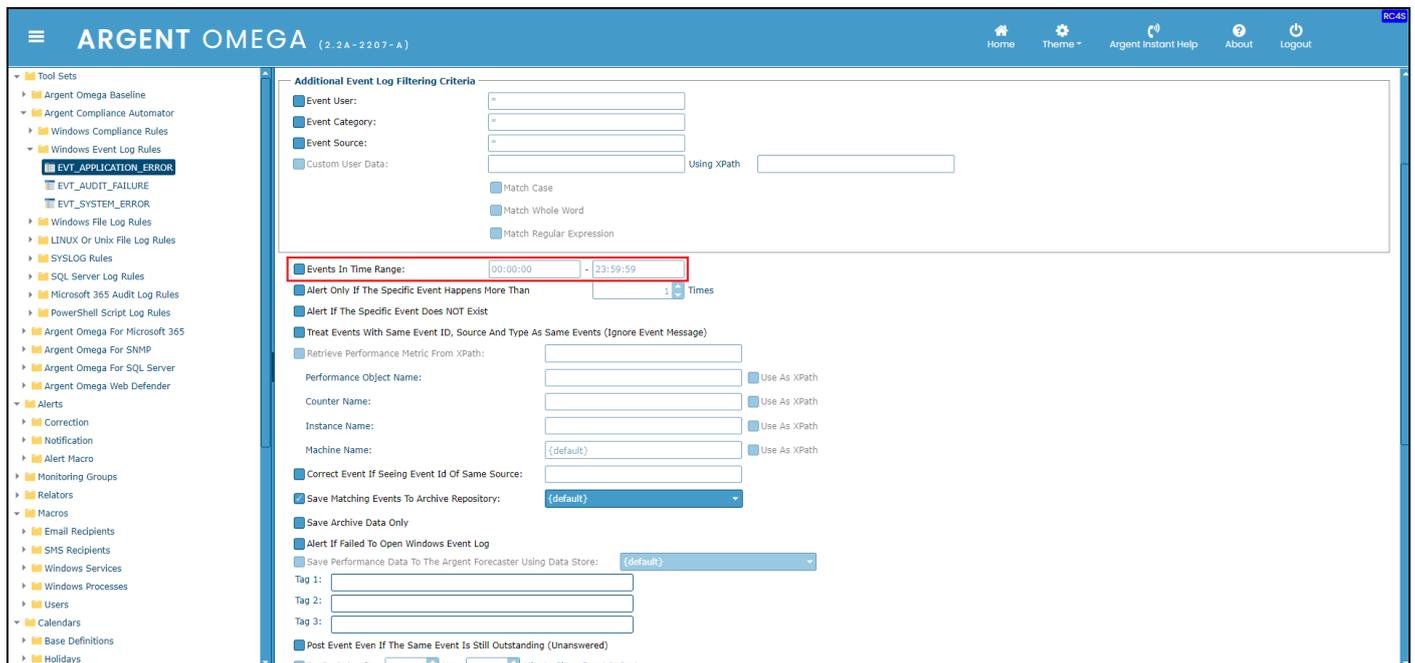
When using the **Advanced Rule View**, it is possible to use the Advanced Event Filter String option using XPath or PowerShell:



In the **Simple Rule View**, there is an **Additional Event Log Filtering Criteria** block where you can specify **Event User, Category, Source and Custom User Data**:

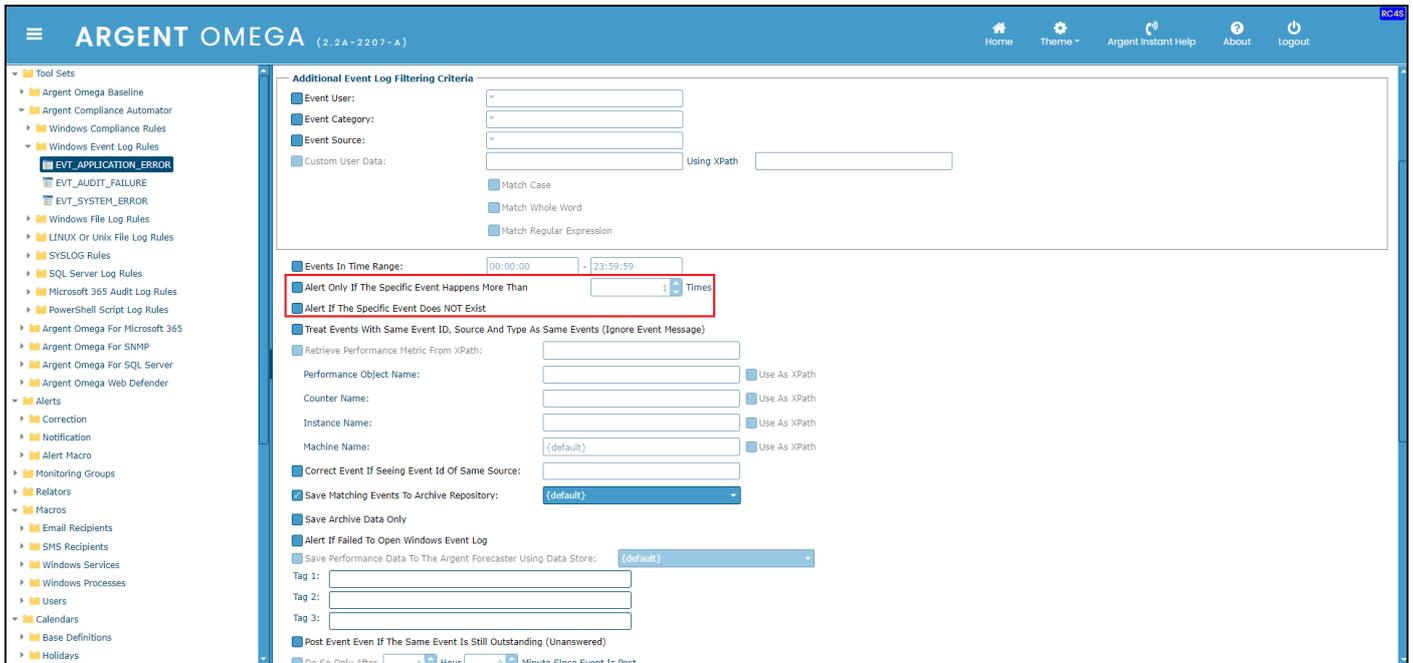


The **Events In Time Range** filtering option is used to retrieve events in the specified Time Range:



The **Alert Only If The Specific Event Happens More Than** option is used to fire an Alert only if the filtered events happens more than the specified number of times.

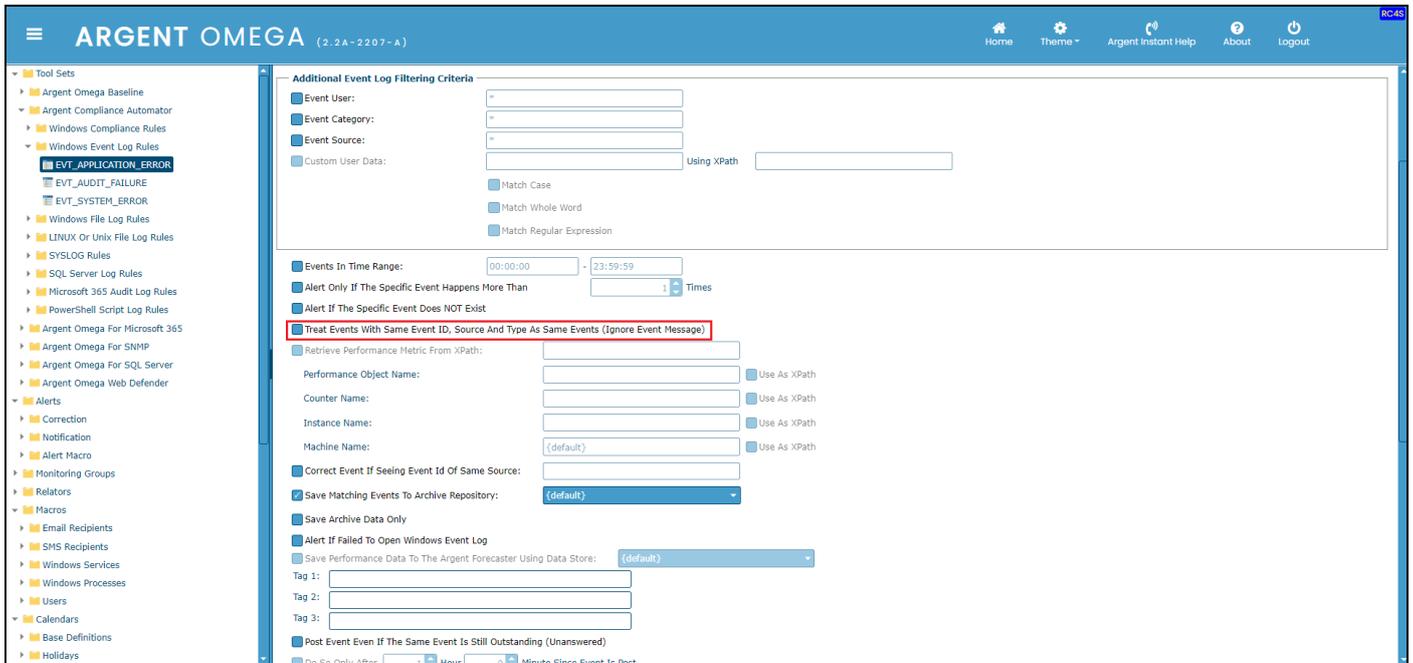
There is an option to **Alert if the Specific Event does not exist**:



The **Treat Events with Same Event ID, Source And Type As Same Events (Ignore Event Message)**

option can be used to ignore the content of the Event Message description field when determining if multiple monitored event instances should be considered as the same event.

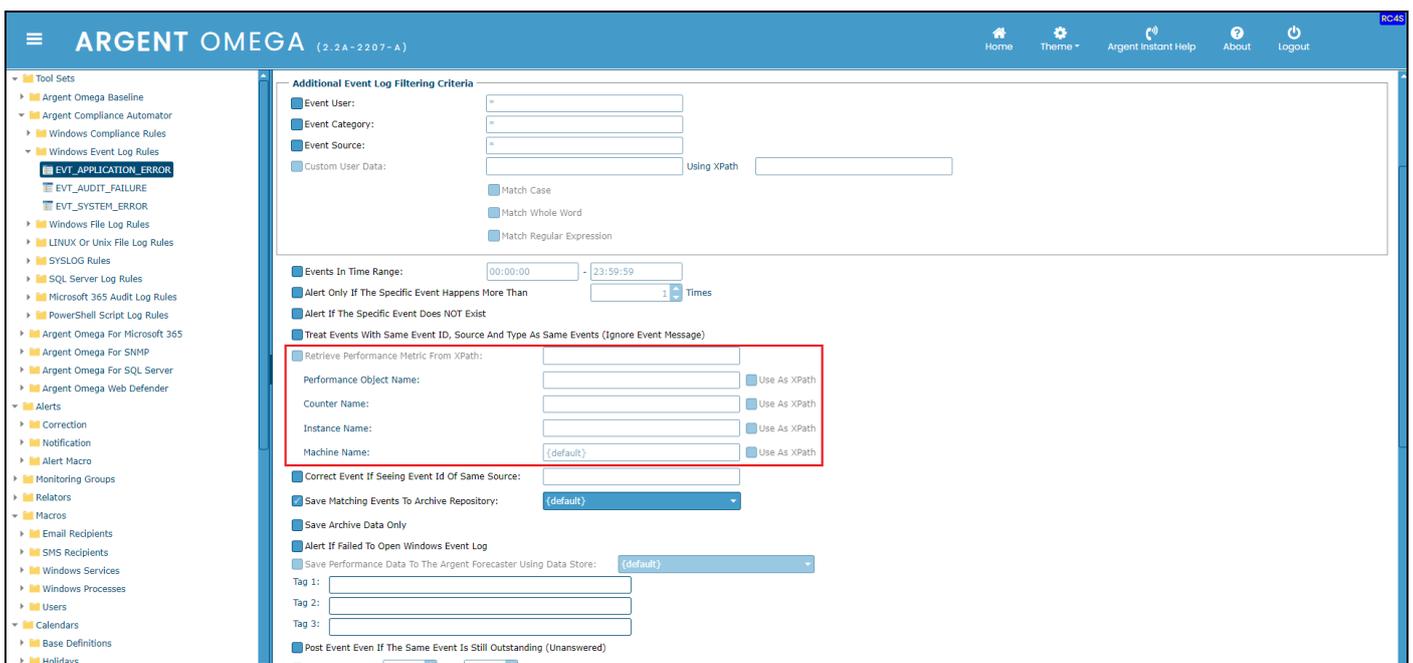
This is used in conjunction with the options for **Alert Only If The Specific Event Happens More Than X Times** and **Post Event Even If The Same Event Is Still Outstanding (Unanswered)**.



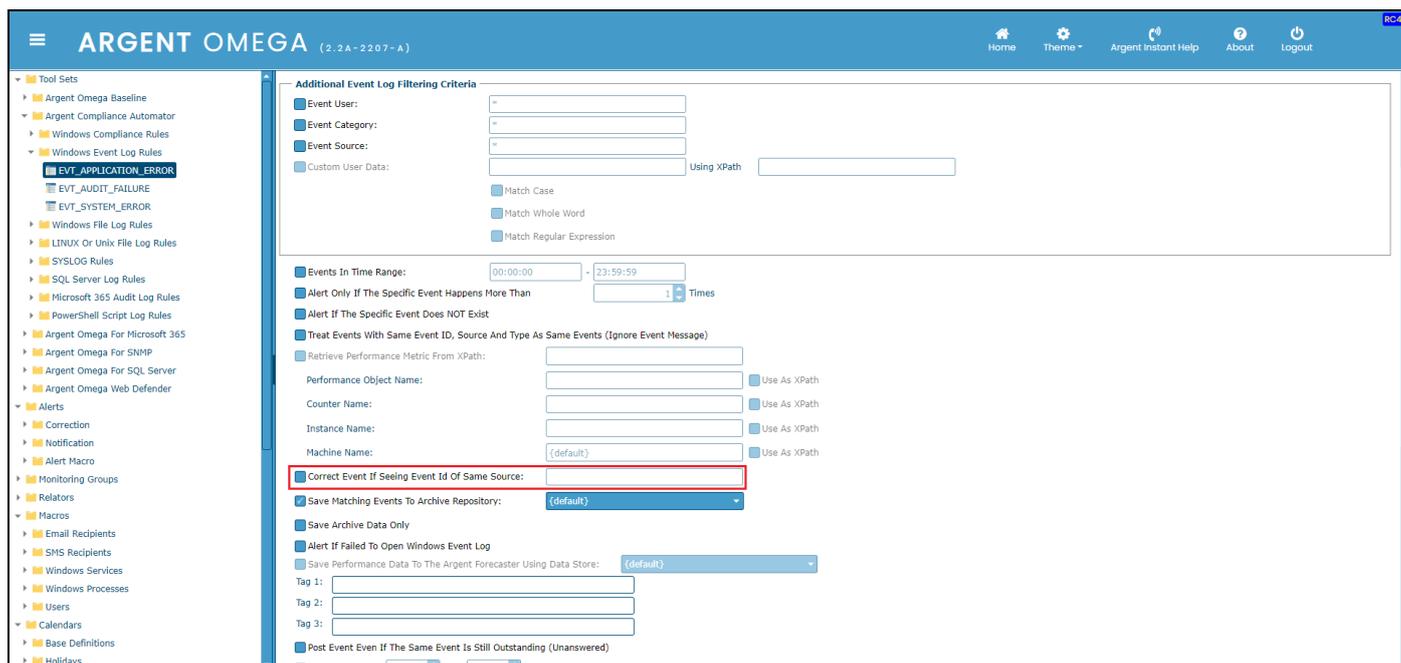
The **Performance Metric from XPath** option provides the ability to save specified fields from monitored events as Performance Object metrics.

Specific fields in the monitored logs can be saved and labeled in the database as **Performance Object Name, Counter Name, Instance Name and Machine Name**.

This is useful if the monitored log events contain metrics that a customer would like to view in a historical graph report in the same way that Windows Performance Object metrics are often viewed.

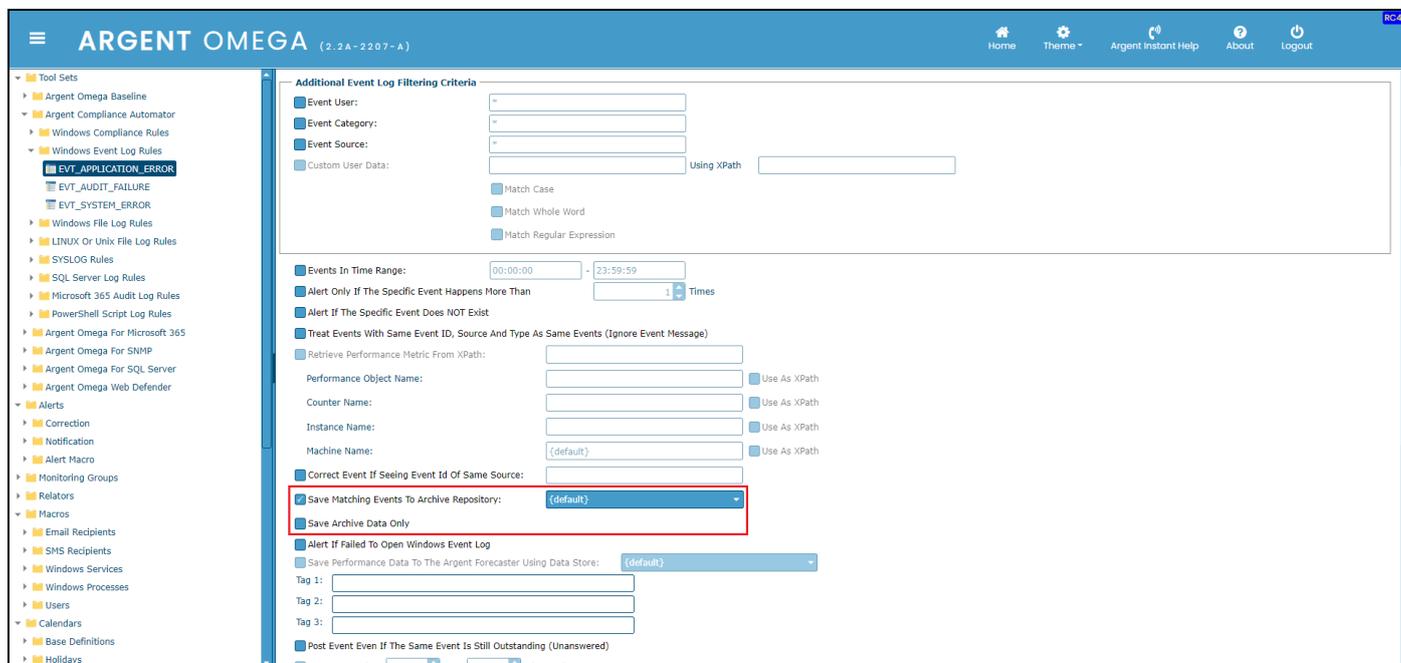


The **Correct Event If Seeing Event ID of Same Source** option can be used to trigger a condition corrected event if the specified Event ID is seen from the same Event source:



The **Save Matching Events To Archive Repository** option is used to specify the Archive Repository where events are saved.

The **Save Archive Data Only** option can be used to save archived data without triggering Alerts:



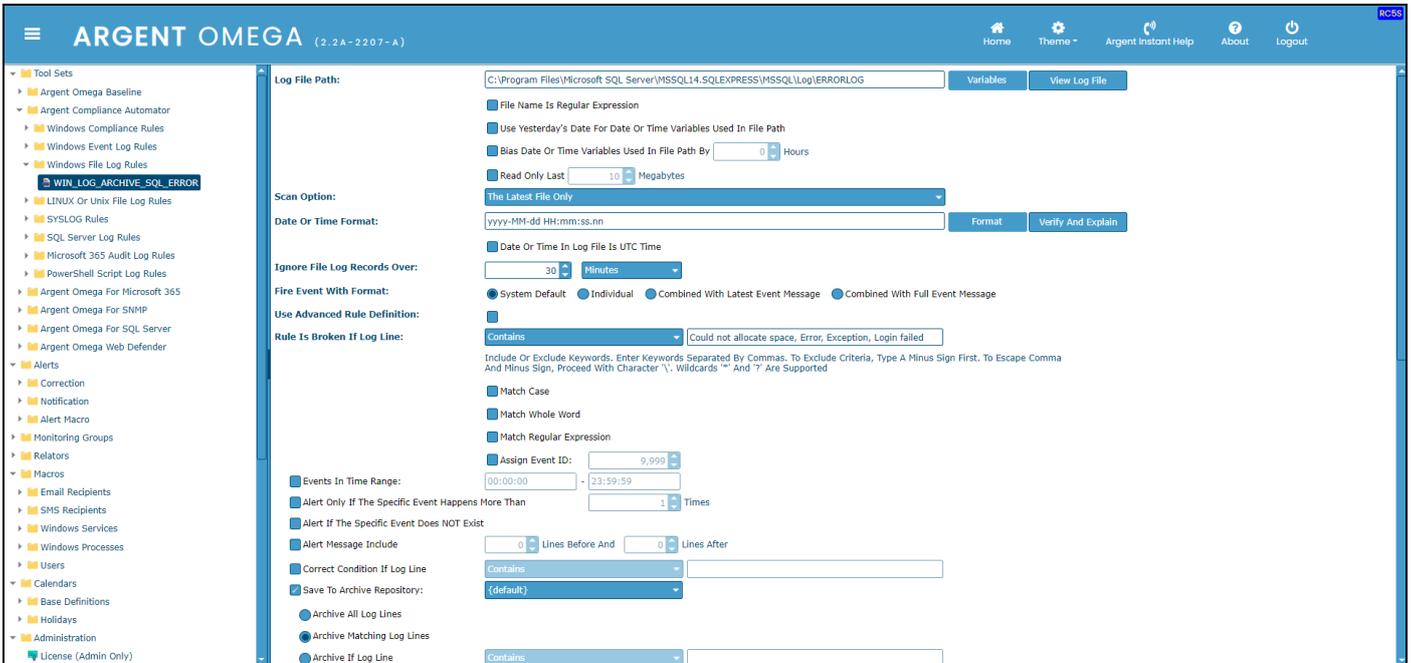
The **Alert If Failed to Open Windows Event Log** option can be used to trigger an alert if the Windows Compliance Rules failed to open the Windows Event Log on the monitored server.

The screenshot displays the ARGENT OMEGA configuration interface. On the left is a navigation tree with categories like 'Tool Sets', 'Alerts', and 'Macros'. The 'Alerts' section is expanded, and 'Alert If Failed to Open Windows Event Log' is highlighted with a red box. The main panel shows the configuration for this alert, including filtering criteria (Event User, Category, Source, Custom User Data), time range (00:00:00 to 23:59:59), and various alerting options such as 'Alert Only If The Specific Event Happens More Than 1 Times', 'Alert If The Specific Event Does NOT Exist', and 'Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)'. Other options include 'Retrieve Performance Metric From XPath', 'Performance Object Name', 'Counter Name', 'Instance Name', 'Machine Name', 'Correct Event If Seeing Event Id Of Same Source', 'Save Matching Events To Archive Repository', 'Save Archive Data Only', 'Save Performance Data To The Argent Forecaster Using Data Store', and 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)'. The interface also includes a top navigation bar with 'Home', 'Theme', 'Argent Instant Help', 'About', and 'Logout' buttons, and a version number '(2.2A-2207-A)'.

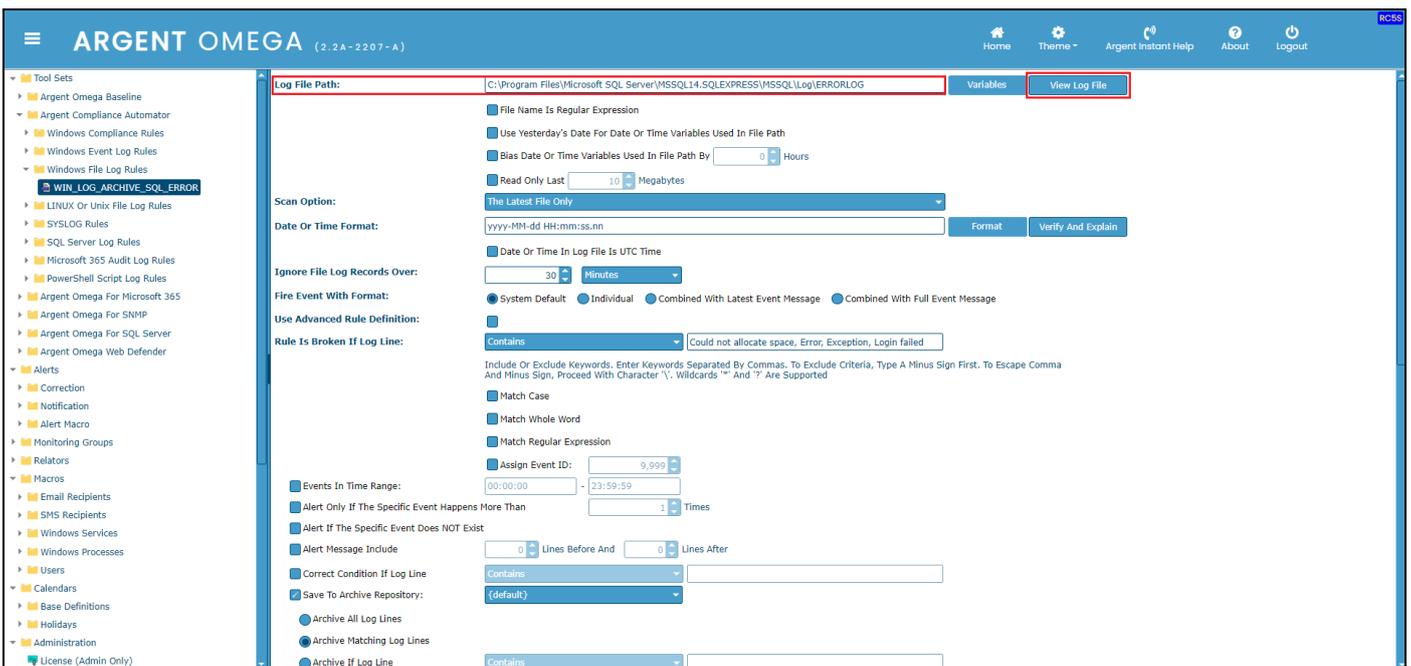
Windows File Log Rules

Applications often write logging debug information to text files for software developers and system engineers to resolve application issues when they occur.

The Argent Windows File Log Rules automates looking for key text phrases within any log file for both monitoring and archiving:



Use the **Log File Path** text box to specify the path to the monitored file. The current file can be viewed by clicking the **View Log File** button:



```

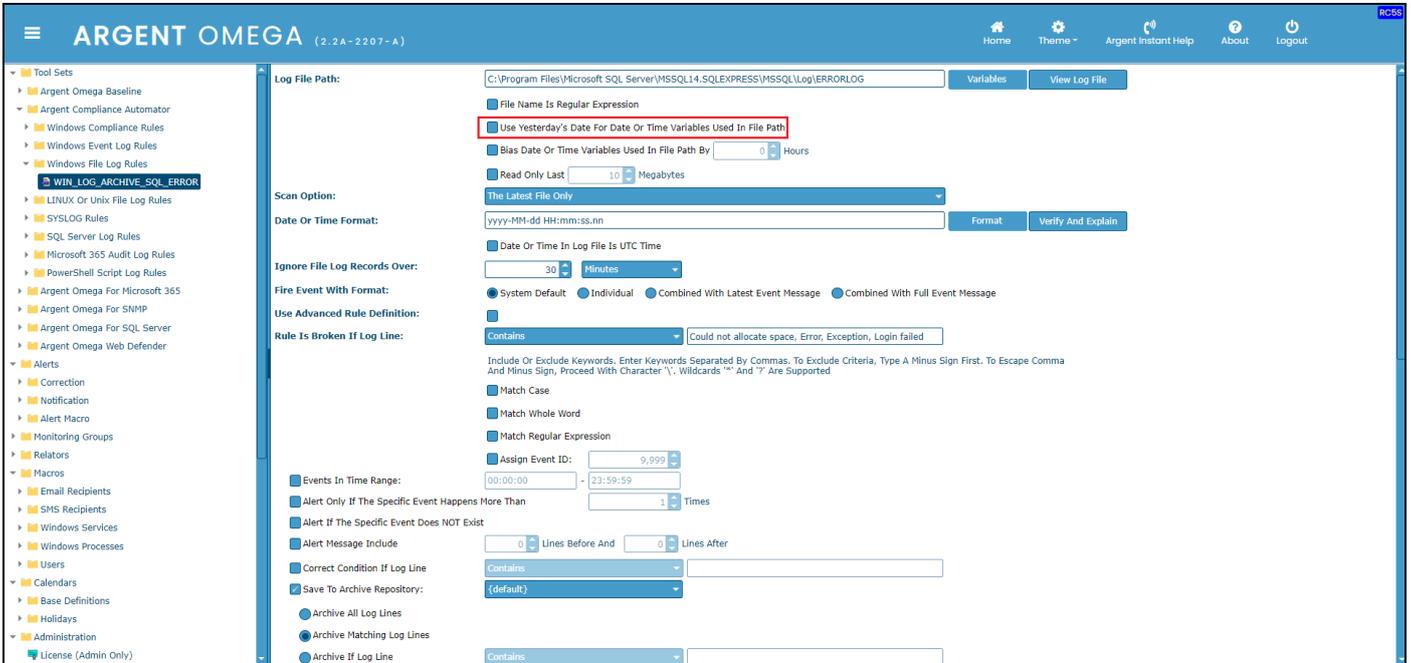
localhost6100/app/OmegaSystemInfo/DownloadTestLog?log=C%3A%5CProgram%20Files%5CMicrosoft%20SQL%20Server%5C MSSQL13.MSSQLSERVER%5C MSSQL%5C Log%5C ERRORLOG&machine=AI-WEB-47&use_regex=false
2022-03-09 10:53:01.66 Server Microsoft SQL Server 2016 (RTM) - 13.0.1601.5 (X64)
Apr 29 2016 23:23:58
Copyright (c) Microsoft Corporation
Express Edition (64-bit) on Windows 10 Pro 6.3 <X64> (Build 19044.) (Hypervisor)
2022-03-09 10:53:01.67 Server UTC adjustment: 5:30
(c) Microsoft Corporation.
All rights reserved.
Server process ID is 6052.
System Manufacturer: 'LENOVO', System Model: '10132'.
Authentication mode is MIXED.
Logging SQL Server messages in file 'C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Log\ERRORLOG'.
The service account is 'NT SERVICE\MSSQLSERVER'. This is an informational message; no user action is required.
Registry startup parameters:
-d C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\master.mdf
-e C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Log\ERRORLOG
-l C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\mastlog.ldf
Command Line Startup Parameters:
-s "MSSQLSERVER"
SQL Server detected 1 sockets with 4 cores per socket and 4 logical processors per socket, 4 total logical processors; using 4 logical processors based on SQL Server licensing. This is an informational message; no user action is required.
2022-03-09 10:53:01.71 Server SQL Server is starting at normal priority base (+7). This is an informational message; no user action is required.
Detected 8106 MB of RAM. This is an informational message; no user action is required.
Using conventional memory in the memory manager.
Default collation: SQL_Latin1_General_CP1_CI_AS (us_english 1033)
Buffer pool extension is already disabled. No action is necessary.
InitializeExternalUserGroupSid failed. Implied authentication will be disabled.
Implied authentication manager initialization failed. Implied authentication will be disabled.
The maximum number of dedicated administrator connections for this instance is '1'.
This instance of SQL Server last reported using a process ID of 5380 at 3/9/2022 10:52:25 AM (UTC). This is an informational message only; no user action is required.
Node configuration: node 0: CPU mask: 0x0000000000000000 Active CPU mask: 0x0000000000000000. This message provides a description of the NUMA configuration for this computer. This is an informational message only. No user action is required.
Using dynamic lock allocation. Initial allocation of 2500 lock blocks and 5000 Lock Owner blocks per node. This is an informational message only. No user action is required.
Database Instant File Initialization: disabled. For security and performance considerations see the topic 'Database Instant File Initialization' in SQL Server Books Online. This is an informational message only. No user action is required.
2022-03-09 10:53:04.07 Server Query Store settings initialized with enabled = 1.
Software Usage Metrics is disabled.
2022-03-09 10:53:04.12 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [1] 'master'. XTP Engine version is 0.0.
Starting up database 'master'.
2022-03-09 10:53:04.22 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [1] 'master'. XTP Engine version is 0.0.
CLR version v4.0.30319 loaded.
2022-03-09 10:53:04.61 Server SQL Server Audit is starting the audits. This is an informational message. No user action is required.
SQL Server Audit has started the audits. This is an informational message. No user action is required.
Server name is 'AI-WEB-47'. This is an informational message only. No user action is required.
Common Language Runtime (CLR) functionality initialized using CLR version v4.0.30319 from C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
SQL Trace ID 1 was started by login 'sa'.
2022-03-09 10:53:05.10 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [32767] 'msdtsystemresource'. XTP Engine version is 0.0.
Starting up database 'msdtsystemresource'.
2022-03-09 10:53:05.22 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [17] 'ARGENT_OMEGA'. XTP Engine version is 0.0.
The resource database build version is 13.00.1601. This is an informational message only. No user action is required.
2022-03-09 10:53:05.34 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [32767] 'msdtsystemresource'. XTP Engine version is 0.0.
2022-03-09 10:53:05.43 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [4] 'msdb'. XTP Engine version is 0.0.
2022-03-09 10:53:05.51 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [17] 'ARGENT_OMEGA'. XTP Engine version is 0.0.
2022-03-09 10:53:05.58 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [32767] 'msdtsystemresource'. XTP Engine version is 0.0.
2022-03-09 10:53:05.64 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [4] 'msdb'. XTP Engine version is 0.0.
2022-03-09 10:53:05.69 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [3] 'model'. XTP Engine version is 0.0.
Starting up database 'model'.
2022-03-09 10:53:06.00 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [17] 'ARGENT_OMEGA'. XTP Engine version is 0.0.
2022-03-09 10:53:06.01 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [3] 'model'. XTP Engine version is 0.0.
2022-03-09 10:53:06.02 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [3] 'model'. XTP Engine version is 0.0.

```

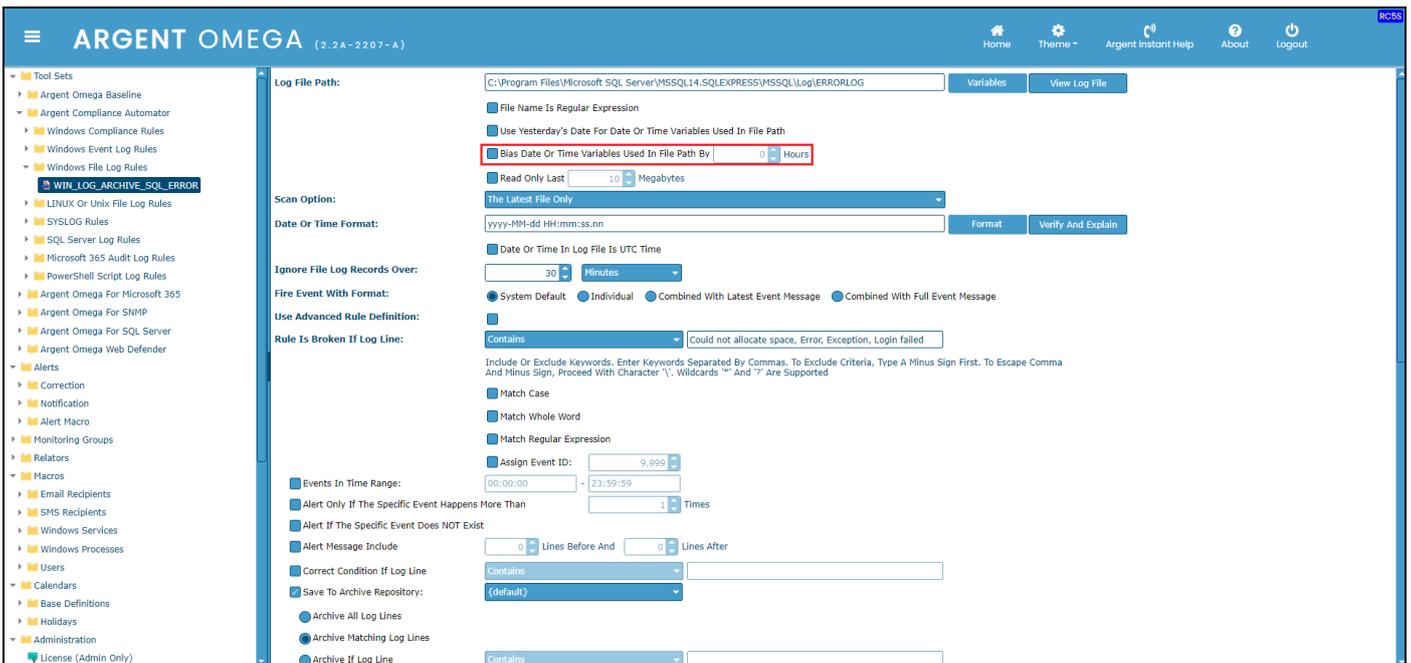
The **File Name Is Regular Expression** option can be used to specify portions of a file name in order to scan multiple files.

The **Variables** drop down menu can be used to specify Date or Time variables in the file name.

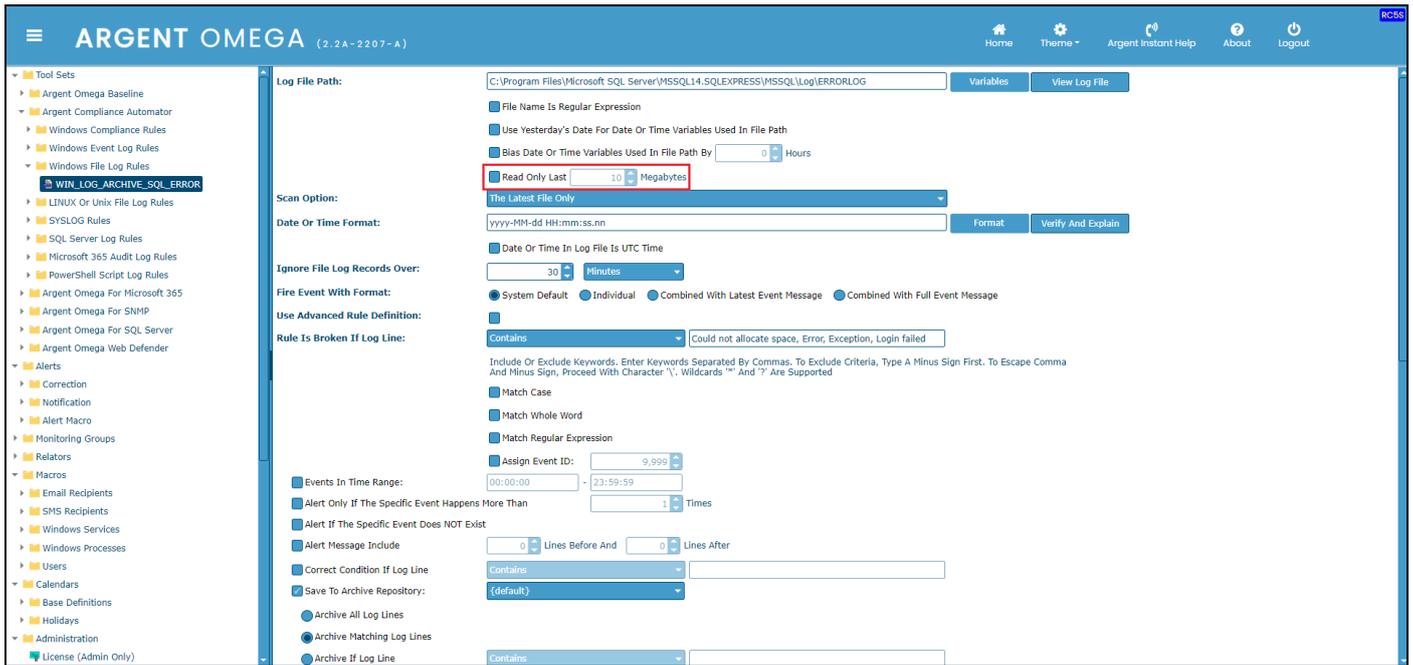
When the Date or Time variables are used in the file name, the **'Use Yesterday's Date For Date or Time Variables Used In File Path'** option can be used to look for files with yesterday's date in the name instead of the current day:



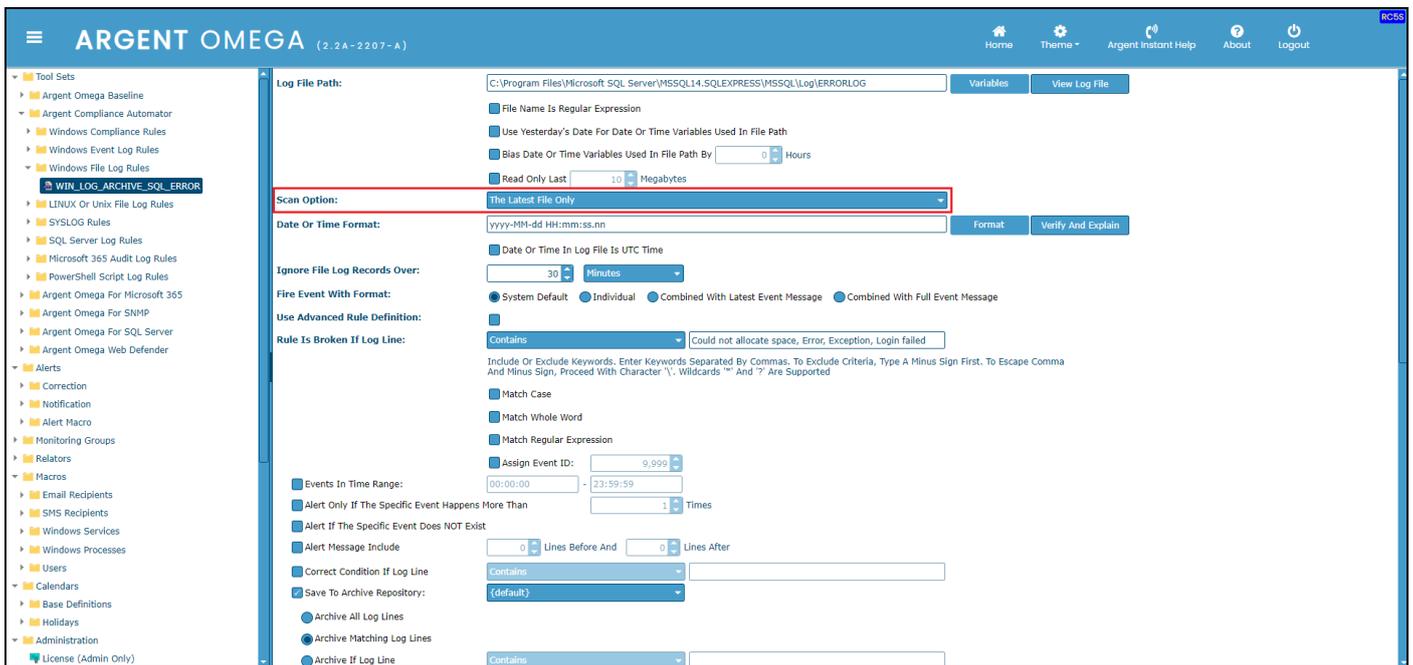
When the Date or Time variables are used in the file name, the **Bias Date or Time Variables Used In File Path** option can be used to increment or decrement the time by x Hours:



The **Read Only Last** option can be used to specify only scanning the last x Megabytes of data from the specified log file:

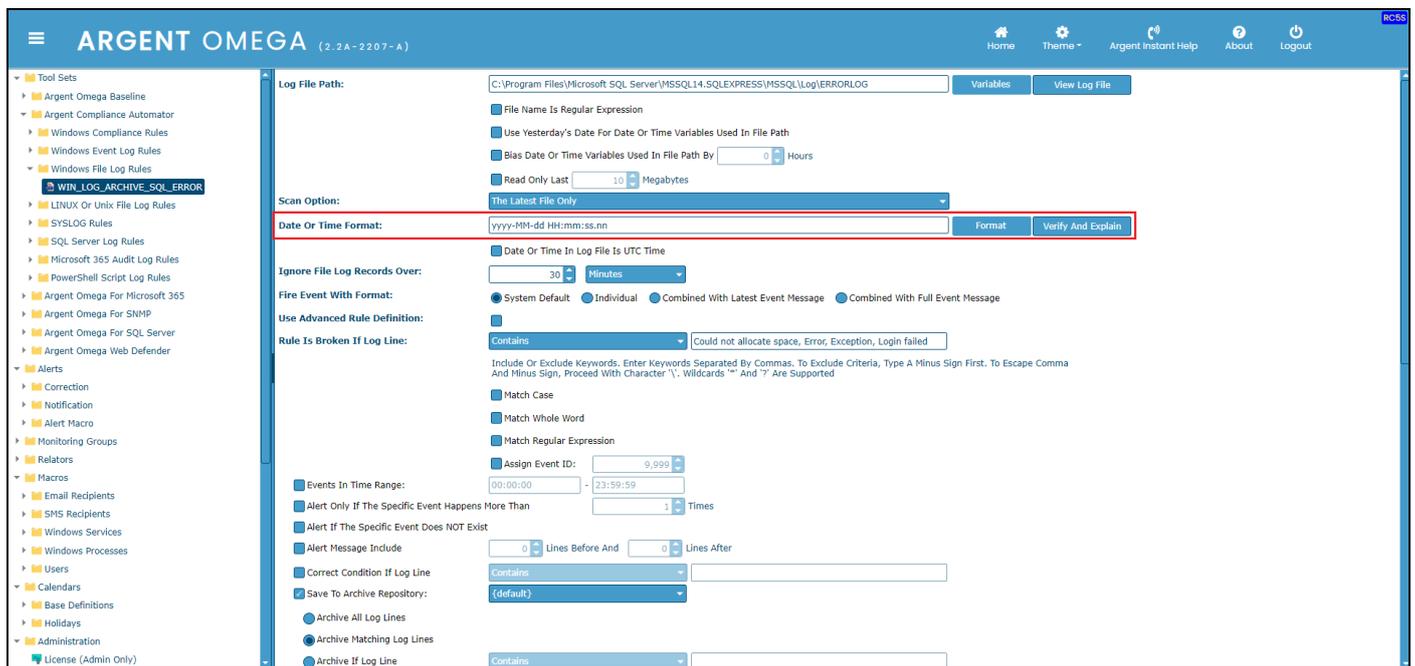


The **Scan Option** combo box is used to specify the required scanning method, such as “The Latest File Only,” etc.

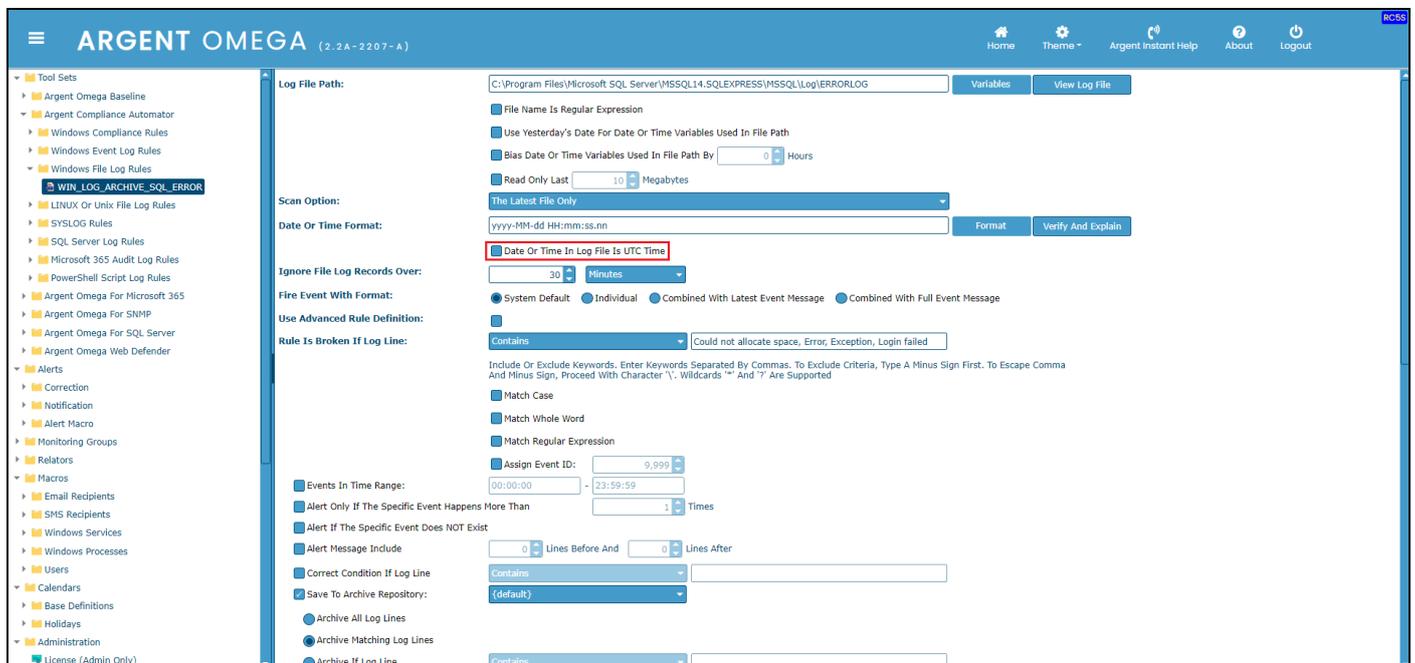


The **Date or Time Format** field is used to specify the Date or Time format used in the monitored log.

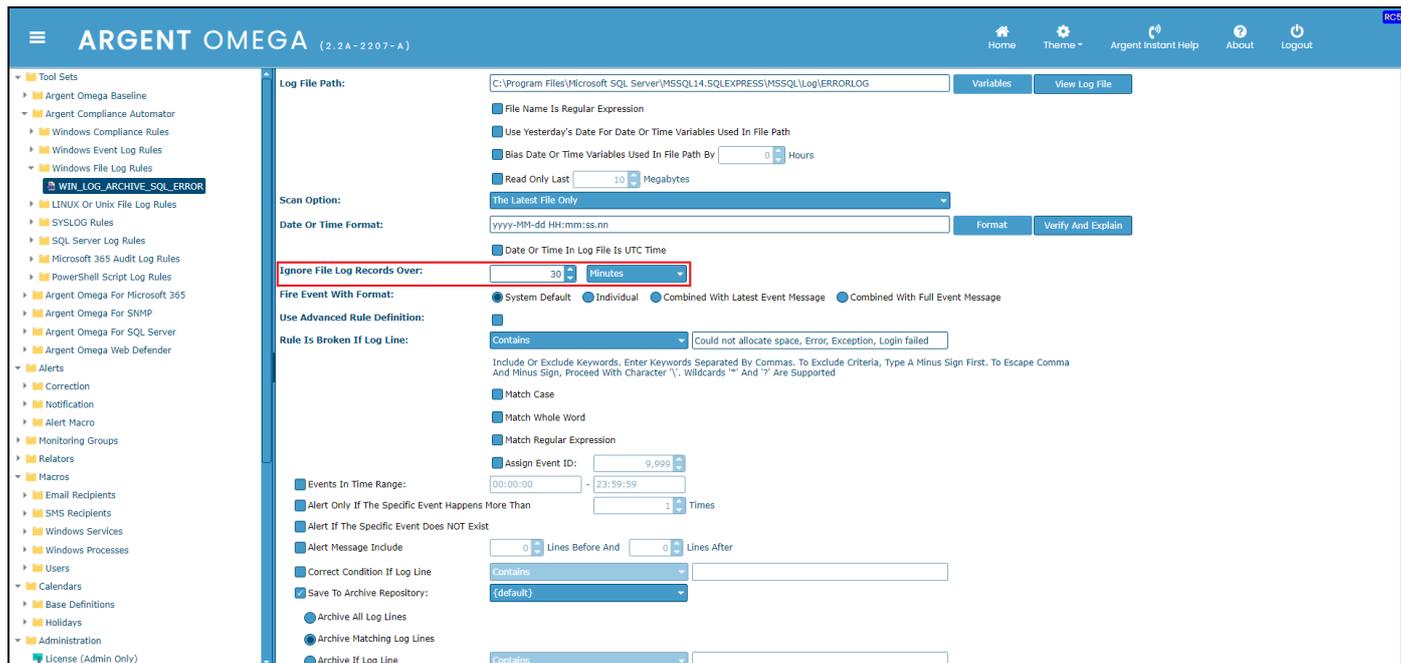
The **Verify And Explain** button is used to explain the Date or Time format specification string used and the number of matching lines with the specified Date or Time format that are currently present in the log file:



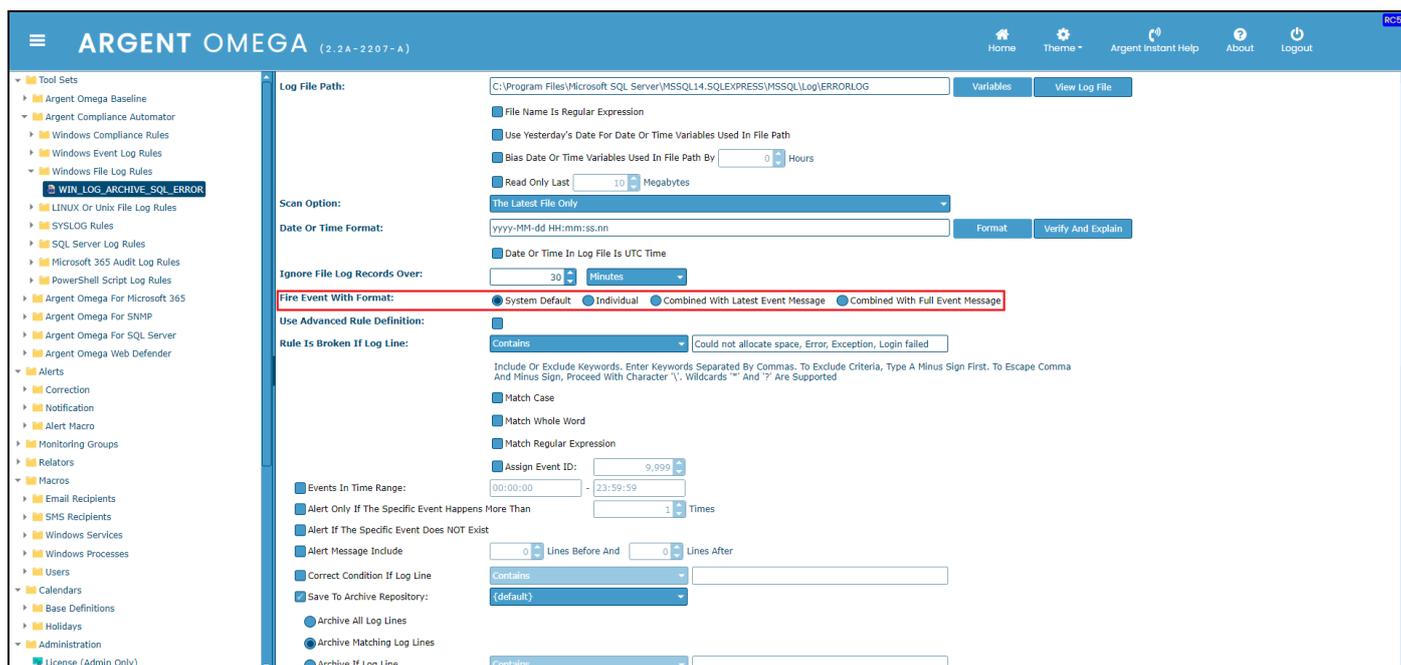
The **Date or Time In Log File Is UTC Time** option should be used when the monitored log file is using UTC time for its Date or Time field.



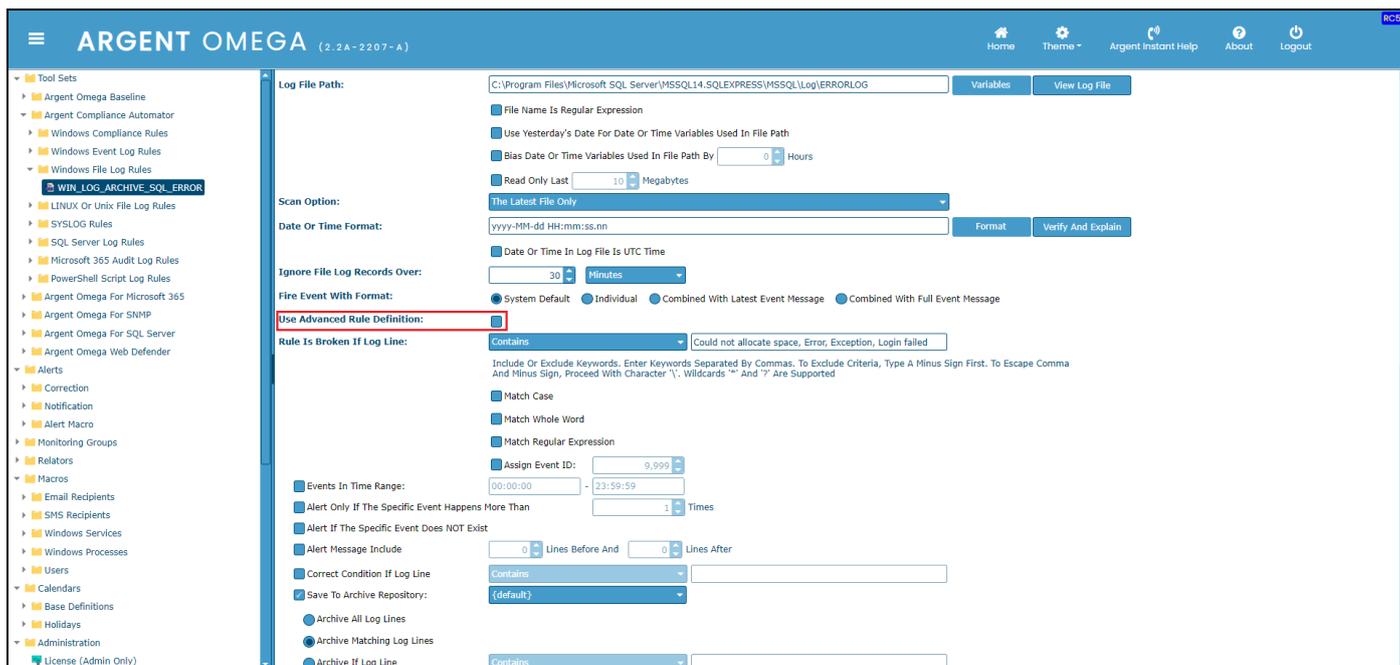
Use the **Ignore File Log Records Over** field to skip monitoring File Log records that are older than the specified time:



Use the **Fire Event With Format** section to select the Alert message format:



The **Use Advanced Rule Definition** option uses advanced PowerShell script logic to filter the log records:

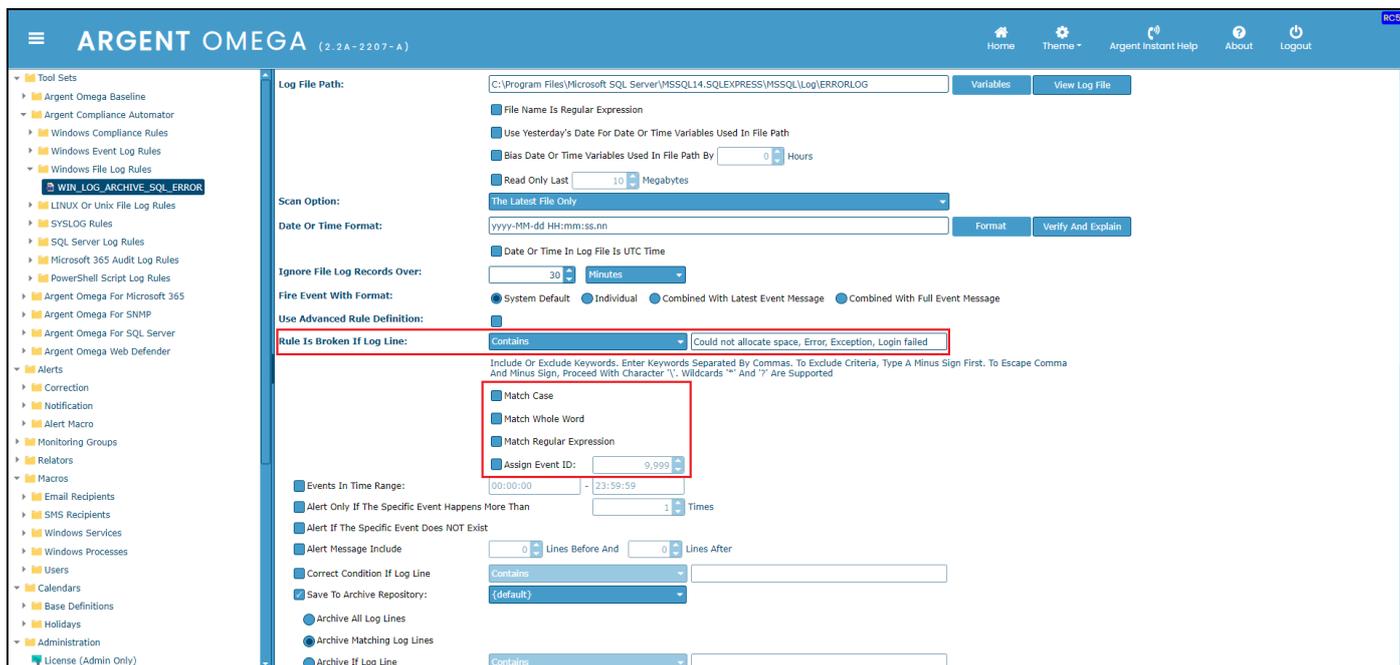


The **Rule Is Broken If Log Line** section is used to specify the keyword string criteria to look for in the monitored log when archiving or triggering alerts.

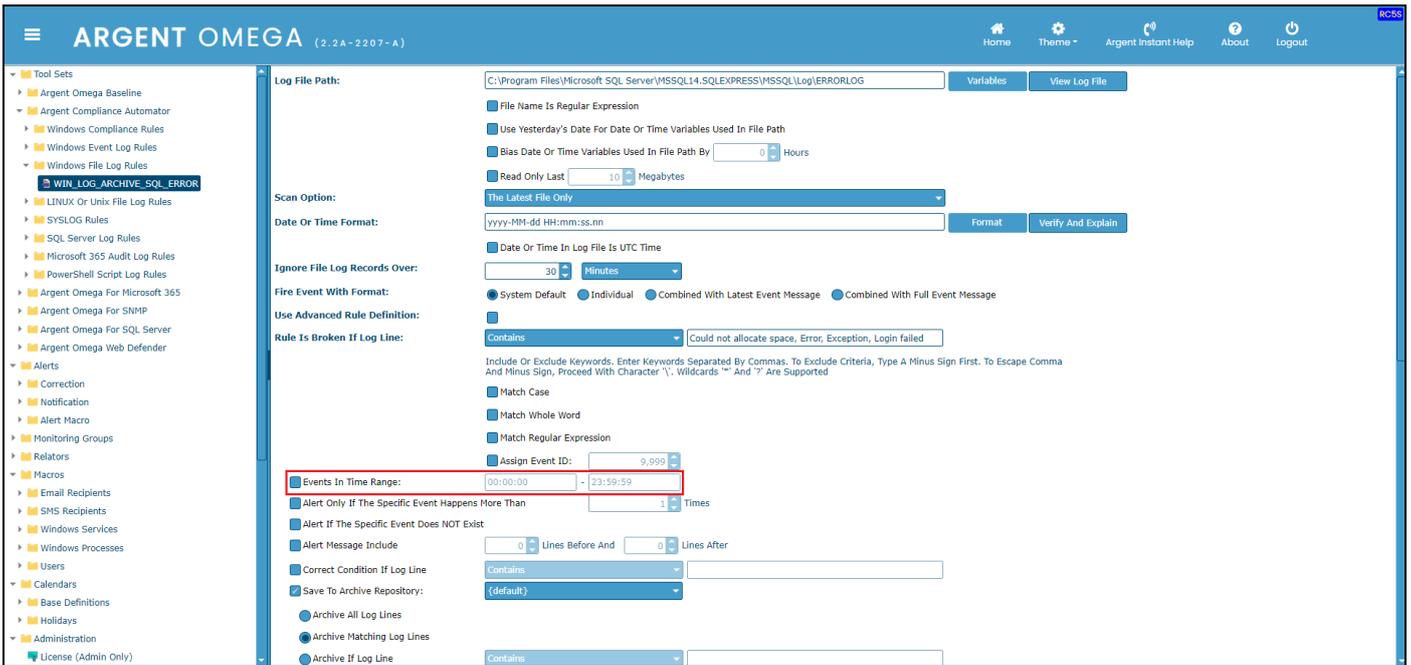
It is possible to specify multiple keywords separated by commas. **To exclude criteria, type a minus sign first.** To escape comma and minus sign, proceed with character '\'. Wildcards '*' and '?' are supported.

There are also options, such as **Match Case**, **Match Whole Word** and **Match Regular Expression**, for more accurate filtering.

An Event ID can be specified in the **Assign Event ID** field to save a custom Event ID in the EVENT_ID_INT field while archiving data in the database table:

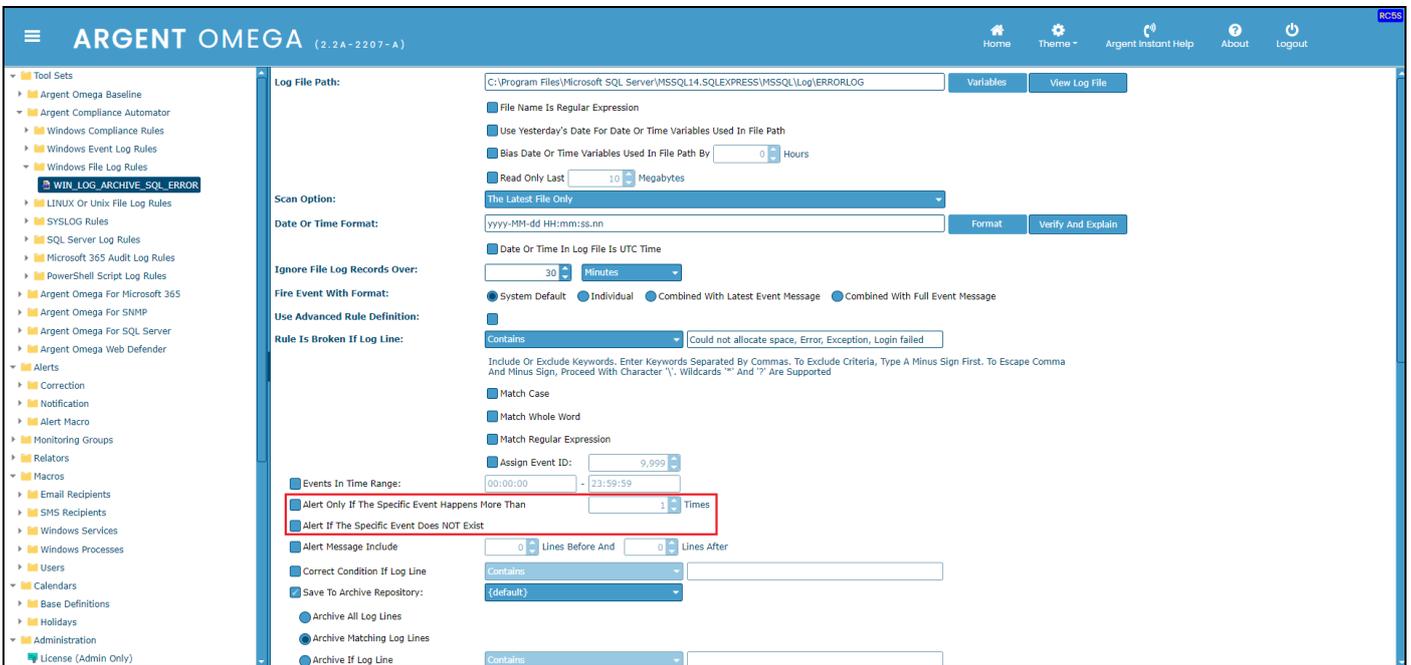


Use the **Events In Time Range** option to filter event records within a specific time range:



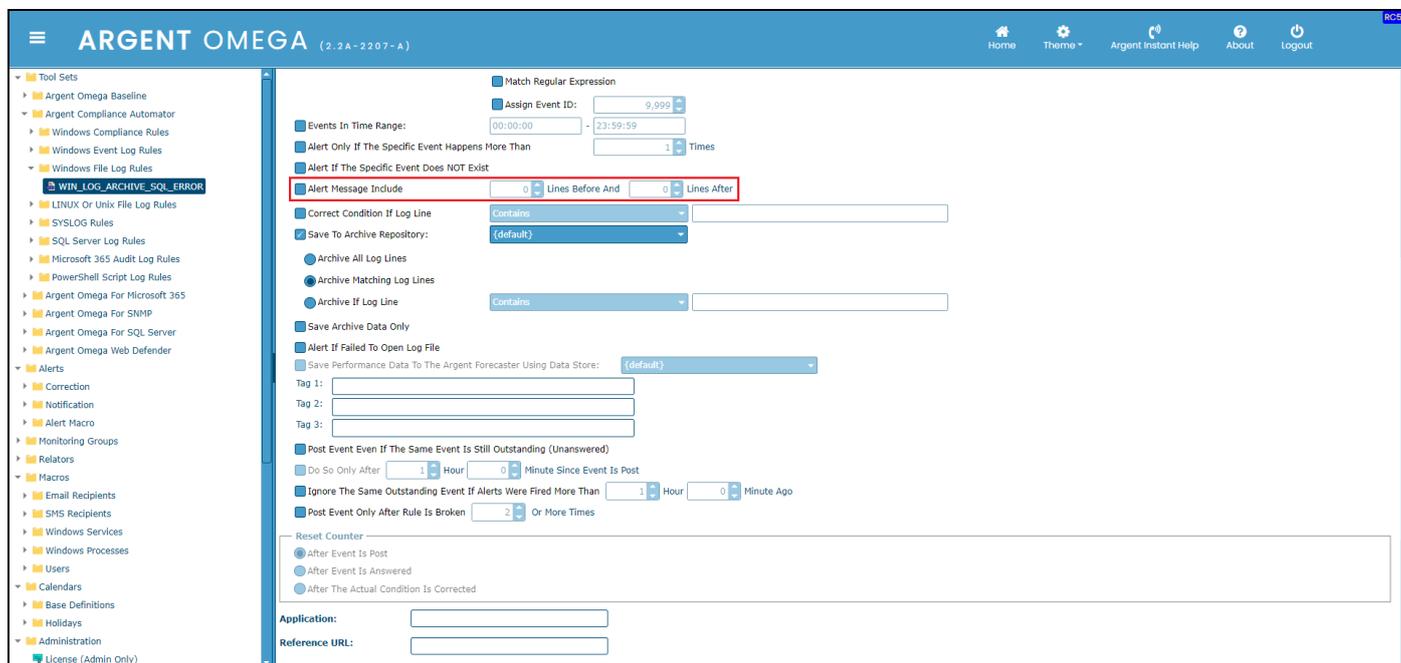
Use the **Alert Only If The Specific Event Happens More Than** option to trigger alerts only after the specified event has occurred a given number of times.

There is an option to **Alert if the Specific Event Does NOT Exist**:



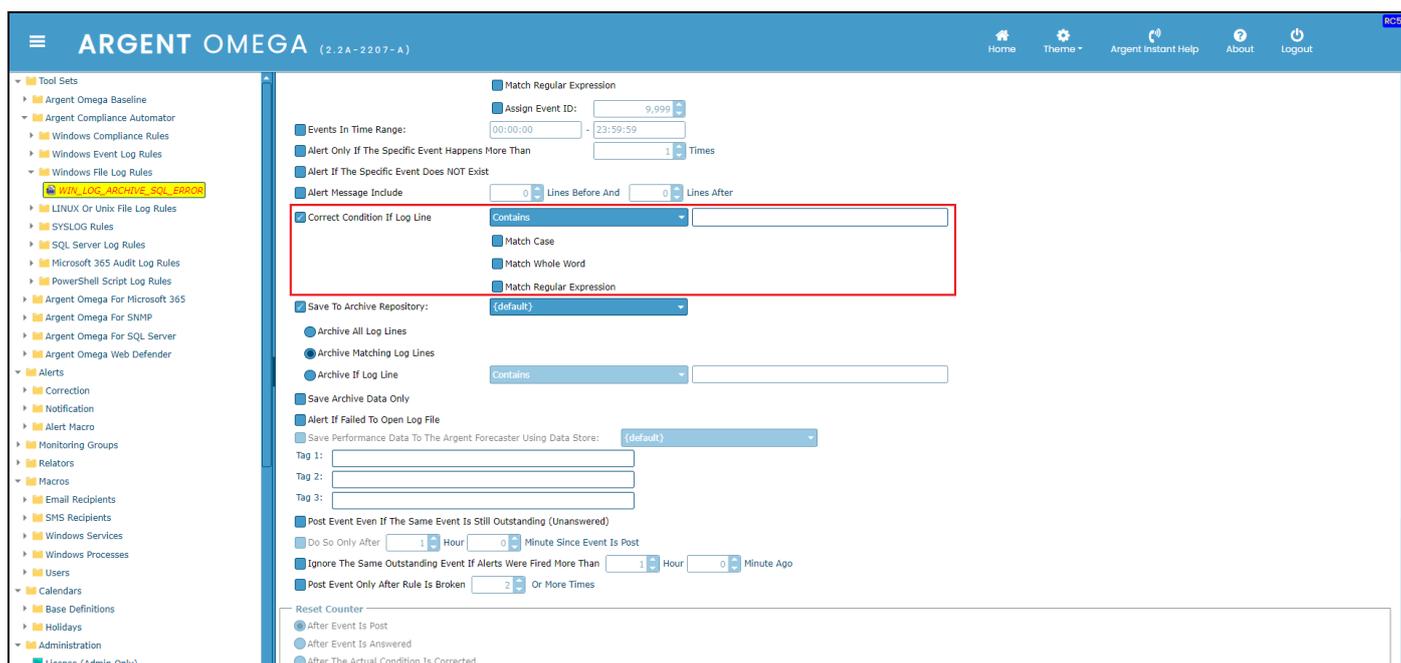
A very useful feature is to add a few lines before and after the event to make it clear to the reader the perspective of the event.

The **Alert Message Include** option can be used to have the alert details include a given number of log lines from before and after the log event line that triggers the alert:



The **Correct Condition If Log Line** option can be used to look for a message string in the monitored log that will trigger a condition corrected alert during a future log poll.

There are also options, such as **Match Case**, **Match Whole Word** and **Match Regular Expression**, for more accurate filtering:

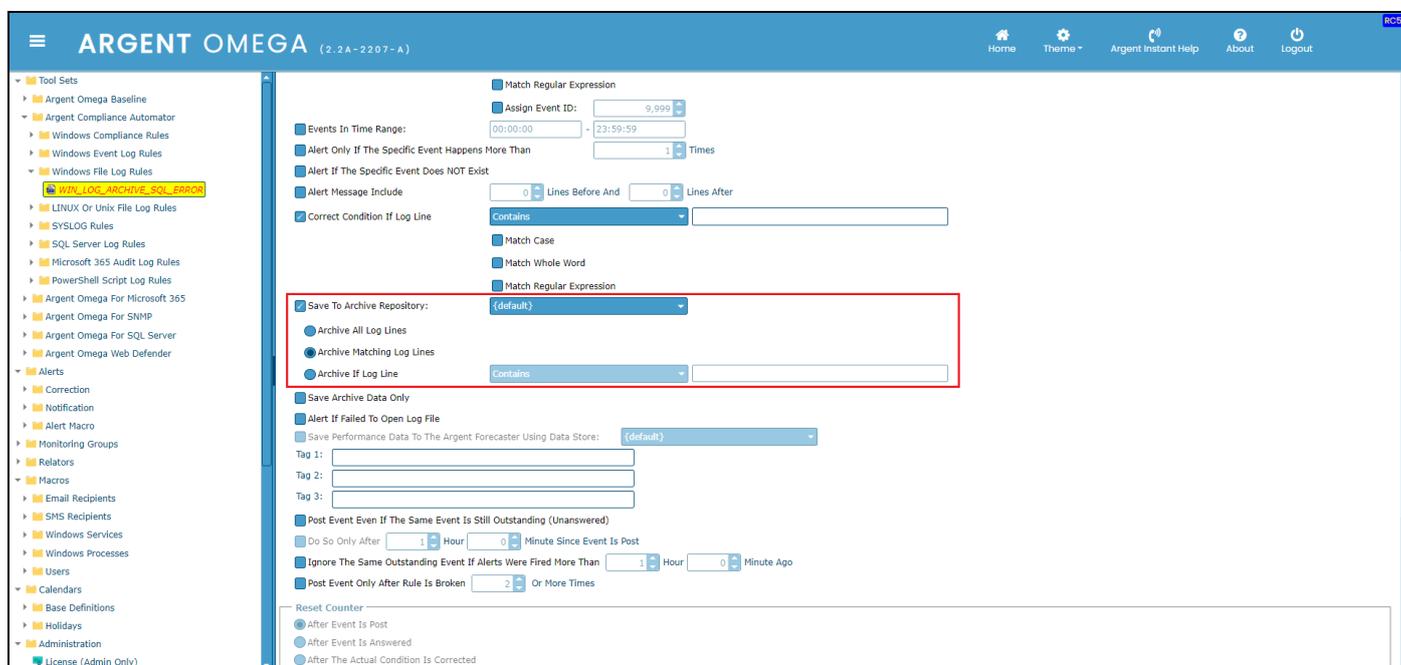


The **Save To Archive Repository** option provides different criteria for saving the event records to the Archive Repository.

The **Archive All Log Lines** option is used to save all log line entries from the monitored log to the database tables. Each line in the monitored log file will be saved as a separate record in the database table.

The **Archive Matching Log Lines** option is used to save only the log line entries that match the condition specified in the **Rule Is Broken If Log Line** section. Each matching line in the log file will be saved as a separate record in the database table.

The **Archive If Log Line Contains** option is used to save only the log lines that contain the specified strings.



The **Save Archive Data Only** option can be used to save archived data without triggering Alerts.

The **Alert If Failed to Open Windows Event Log** option can be used to trigger an alert if the Windows Compliance Rules fails to open the Windows Event Log on the monitored server.

ARGENT OMEGA (2.2A-2207-A) Home Theme Argent Instant Help About Logout

- Tool Sets
 - Argent Omega Baseline
 - Argent Compliance Automator
 - Windows Compliance Rules
 - Windows Event Log Rules
 - Windows File Log Rules
 - WPN_LOG_ARCHIVE_SQL_ERROR**
 - LINUX Or Unix File Log Rules
 - SYSLOG Rules
 - SQL Server Log Rules
 - Microsoft 365 Audit Log Rules
 - PowerShell Script Log Rules
 - Argent Omega For Microsoft 365
 - Argent Omega For SNMP
 - Argent Omega For SQL Server
 - Argent Omega Web Defender
- Alerts
 - Correction
 - Notification
 - Alert Macro
 - Monitoring Groups
 - Relators
 - Macros
 - Email Recipients
 - SMS Recipients
 - Windows Services
 - Windows Processes
 - Users
 - Calendars
 - Base Definitions
 - Holidays
 - Administration
 - License (Admin Only)

Match Regular Expression

Assign Event ID:

Events In Time Range: -

Alert Only If The Specific Event Happens More Than Times

Alert If The Specific Event Does NOT Exist

Alert Message Include Lines Before And Lines After

Correct Condition If Log Line

Match Case

Match Whole Word

Match Regular Expression

Save To Archive Repository:

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line

Save Archive Data Only

Alert If Failed To Open Log File

Save Performance Data To The Argent Forecaster Using Data Store:

Tag 1:

Tag 2:

Tag 3:

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

Do So Only After Hour Minute Since Event Is Post

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

Post Event Only After Rule Is Broken Or More Times

Reset Counter

After Event Is Post

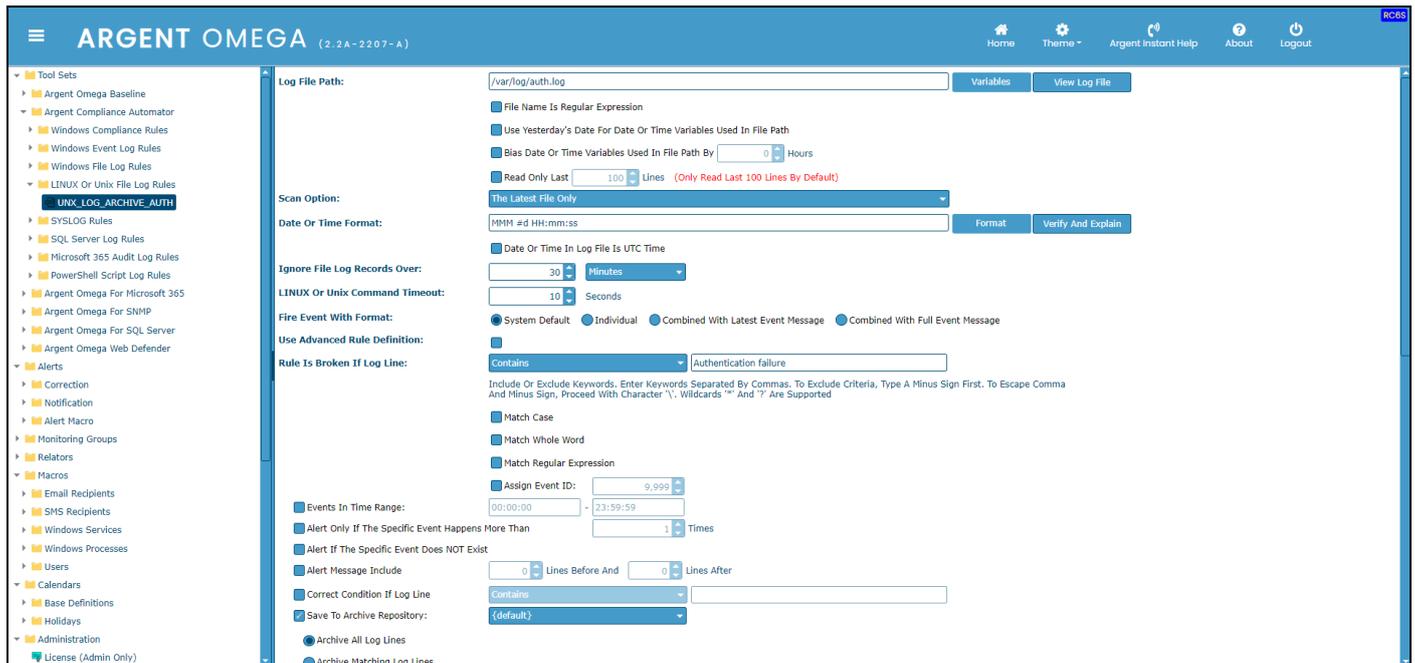
After Event Is Answered

After The Actual Condition Is Corrected

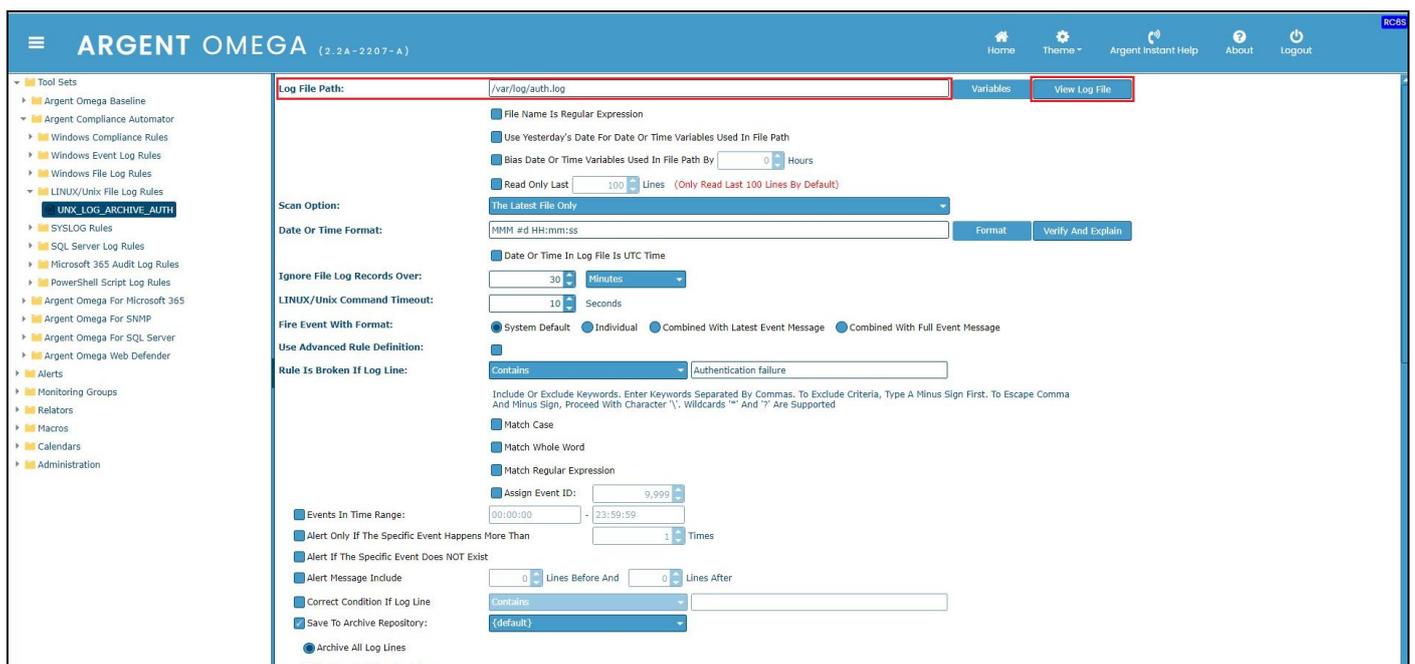
Linux Or Unix File Log Rules

Applications often write logging debug information to text files for software developers and system engineers to resolve application issues when they occur.

The Linux or Unix File Log Rules automate looking for key text phrases within any log file for both monitoring and archiving:

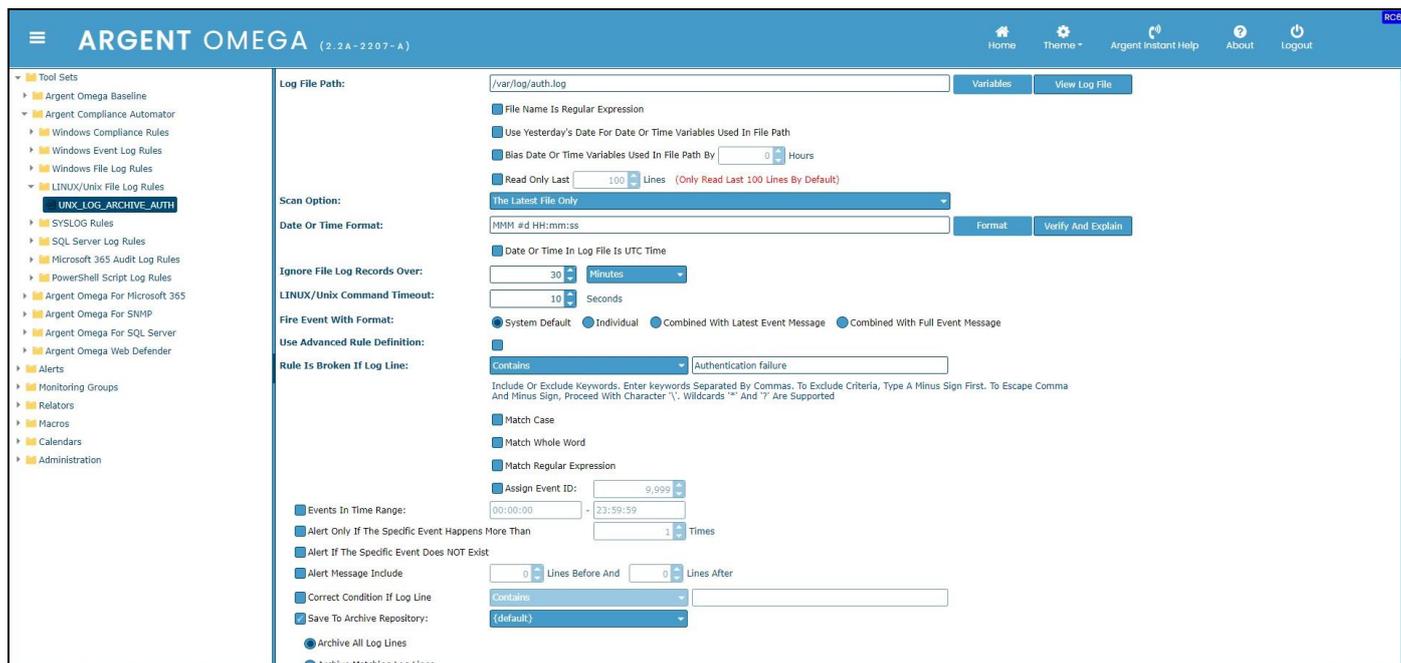


Use the **Log File Path** text box to specify the path to the monitored file. The current file can be viewed by clicking the **View Log File** button:

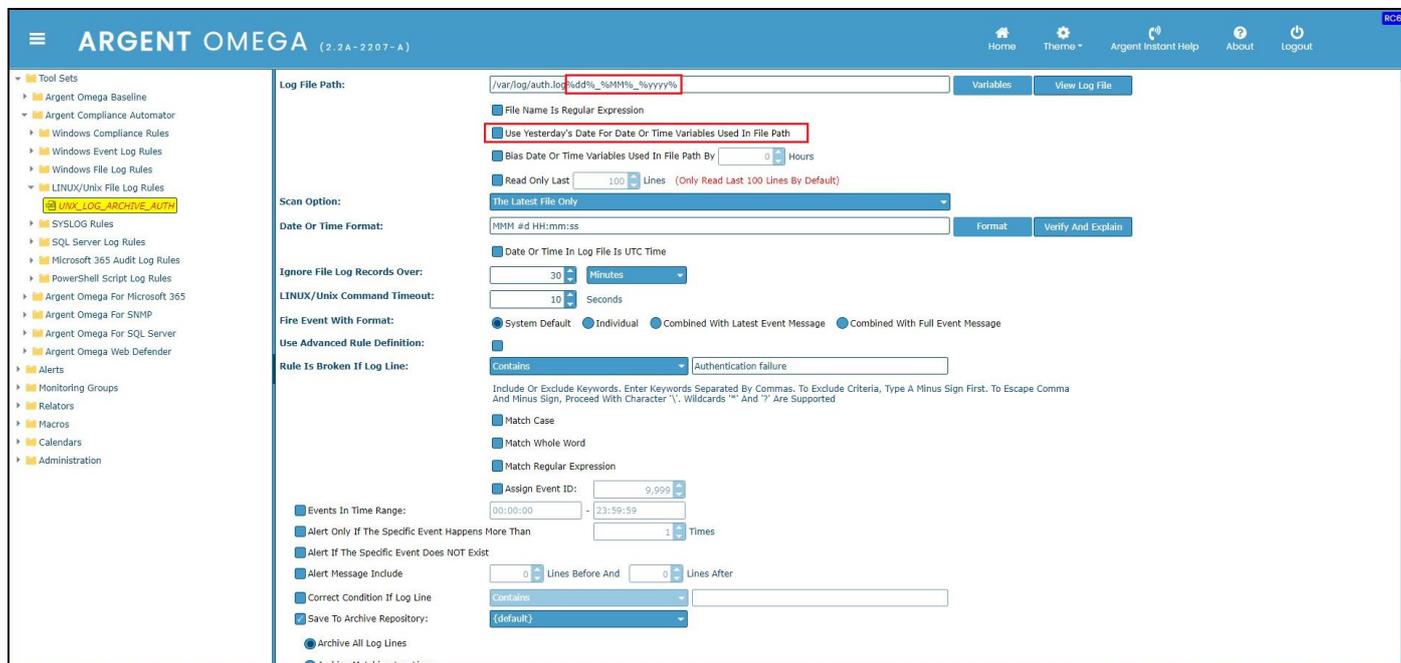


The **File Name Is Regular Expression** option can be used to specify portions of a file name in order to scan multiple files.

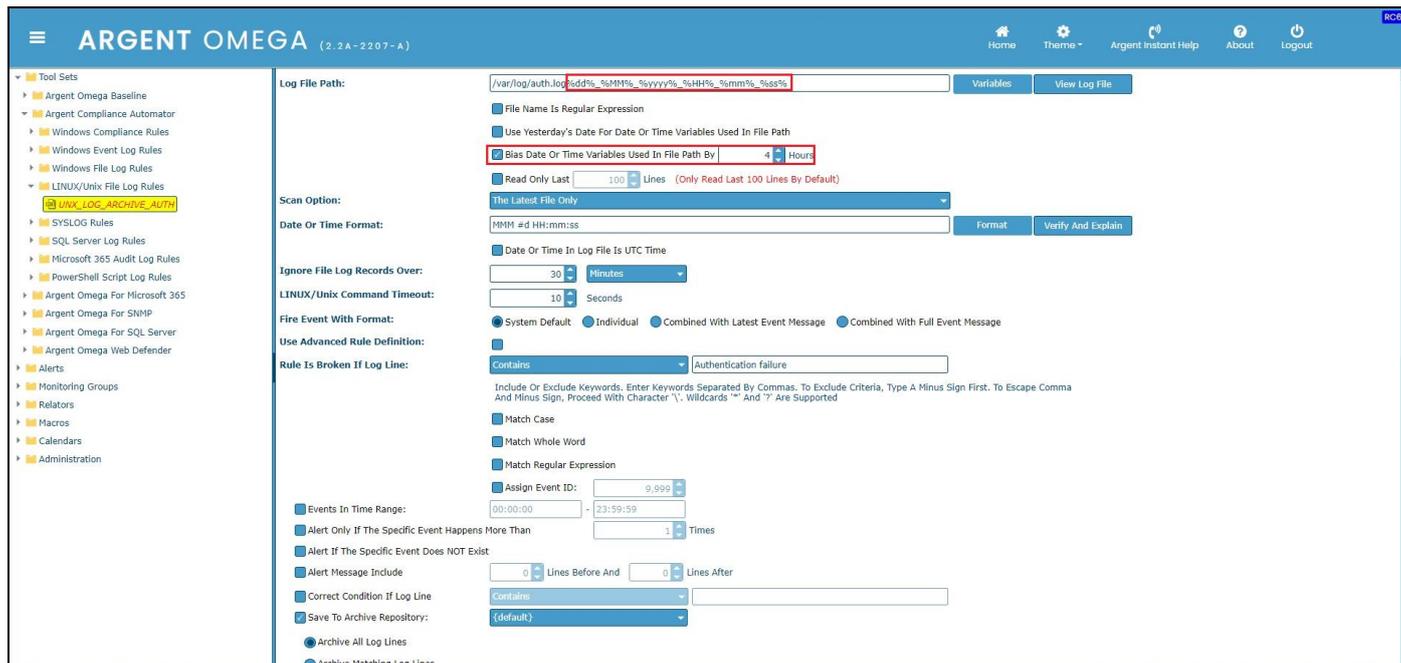
The **Variables** drop down menu can be used to specify Date or Time variables in the file name.



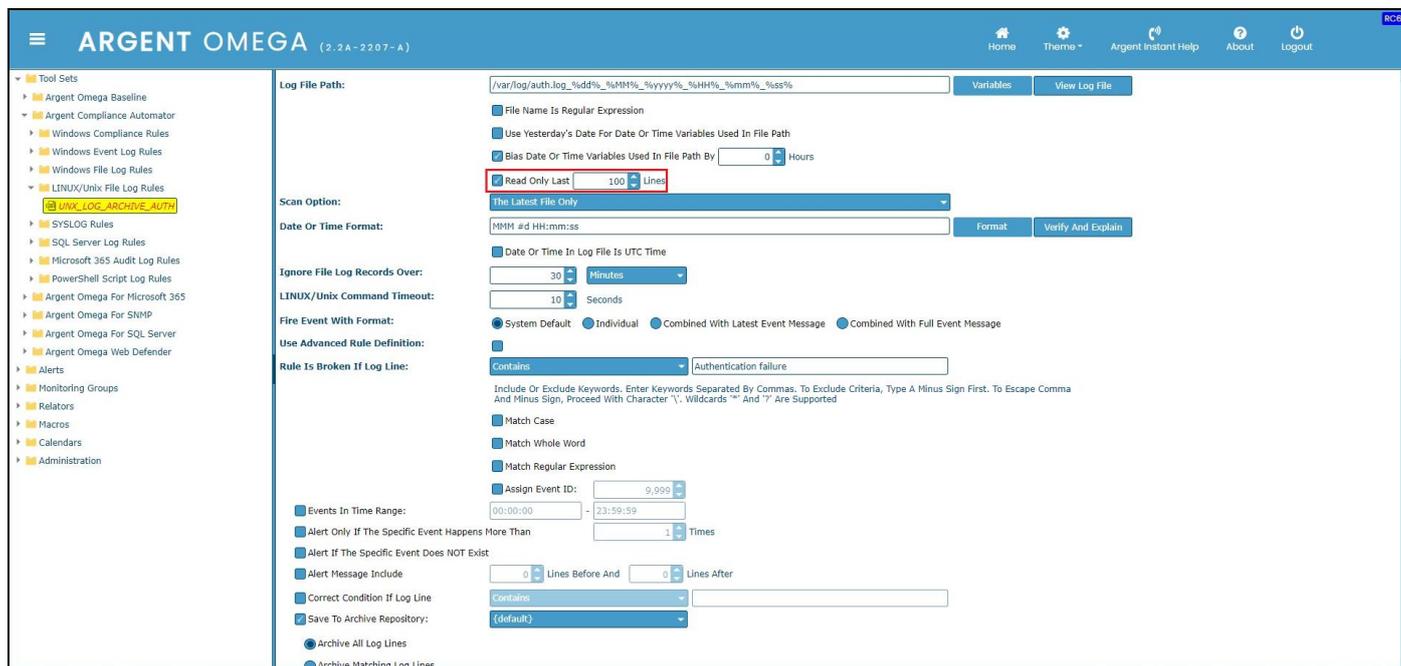
When the Date or Time variables are used in the file name, the **Use Yesterday's Date For Date Or Time Variables Used In File Path** option can be used to look for files with yesterday's date in the name instead of the current day:



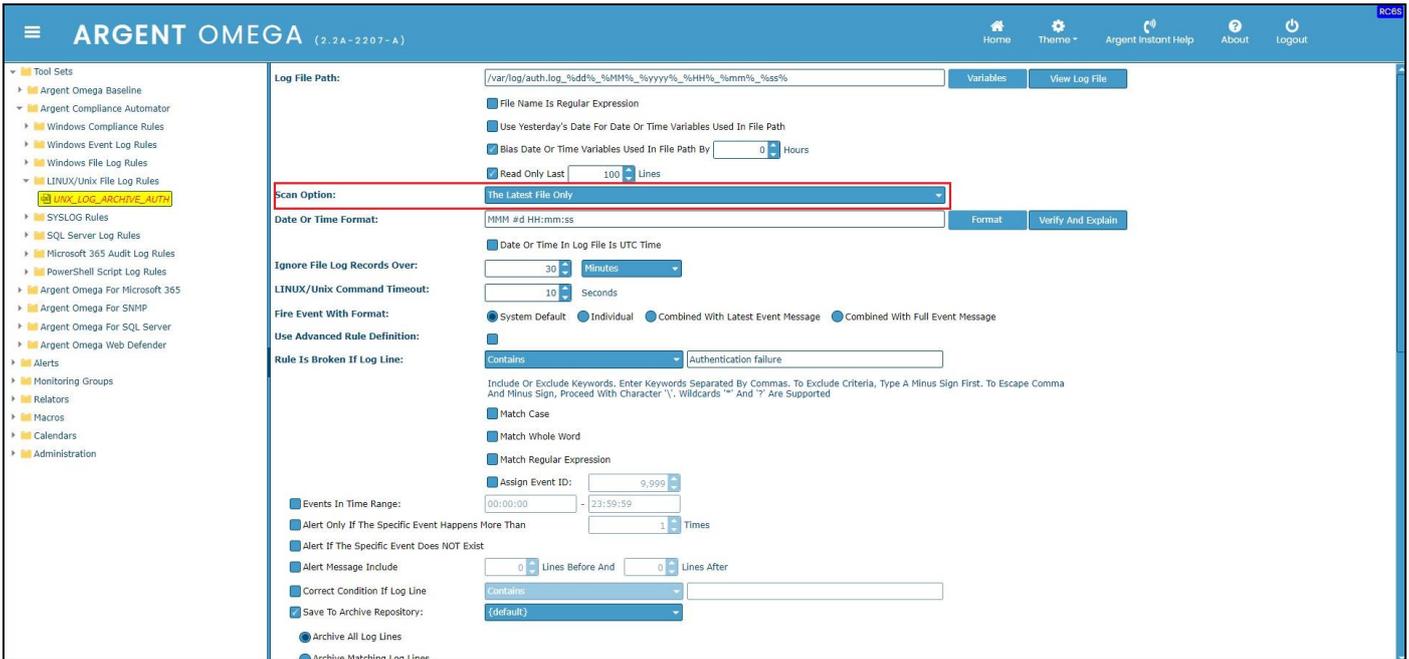
When the Date or Time variables are used in the file name, the **Bias Date or Time Variables Used In File Path** option can be used to increment or decrement the time by x Hours:



The **Read Only Last** option can be used to specify only scanning the last x number of lines from the monitored log file:

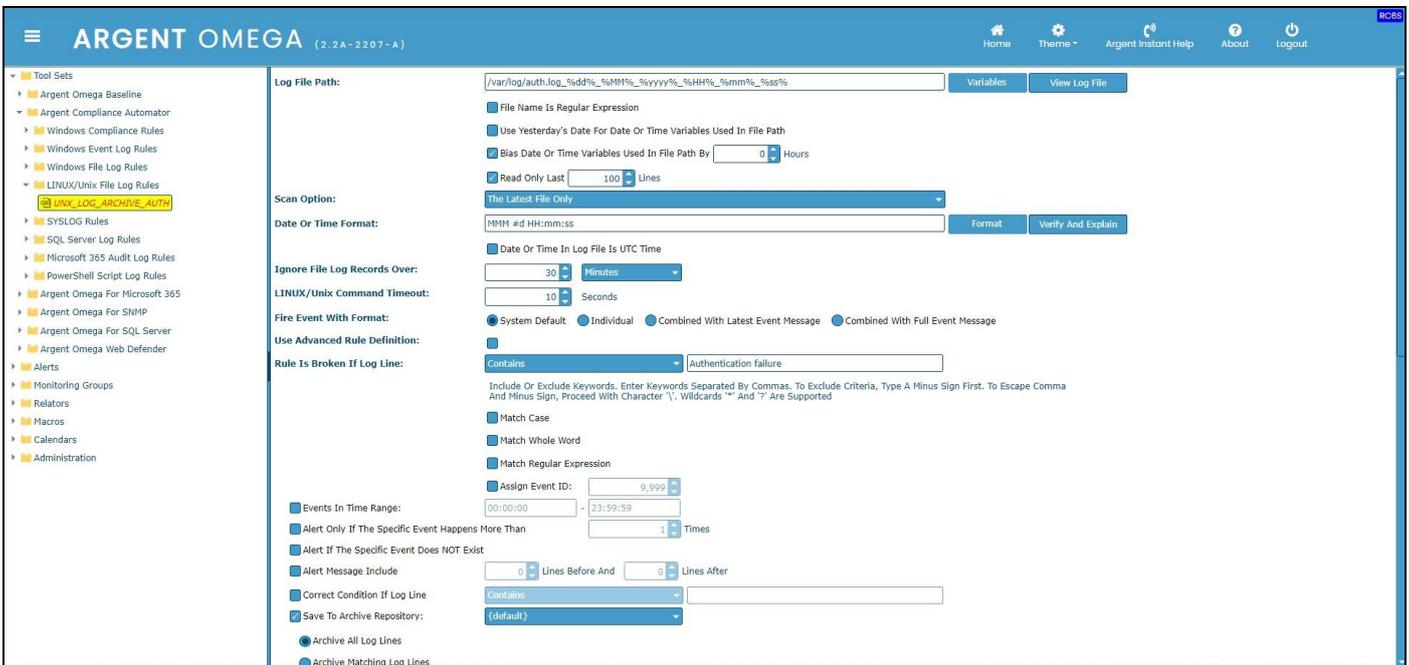


The **Scan Option** combo box is used to specify the required scanning method, such as 'The Latest File Only', etc.

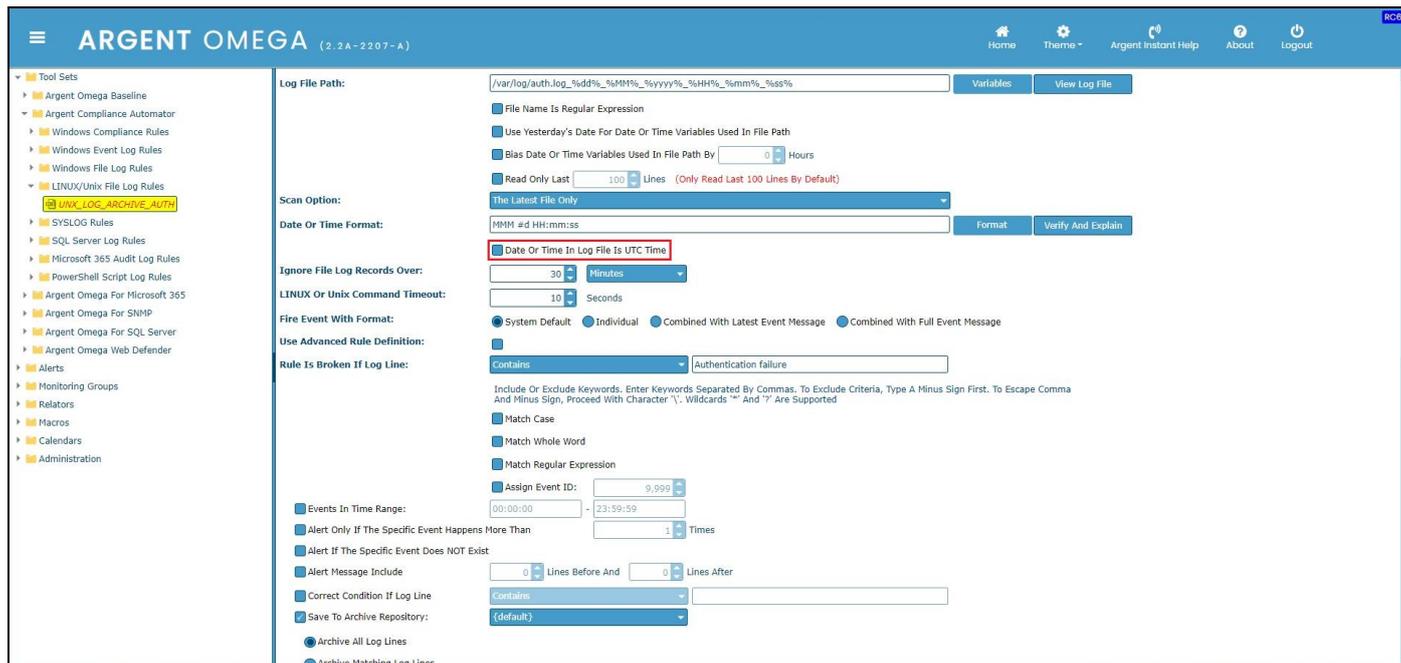


The **Date or Time Format** field is used to specify the Date or Time format used in the monitored log.

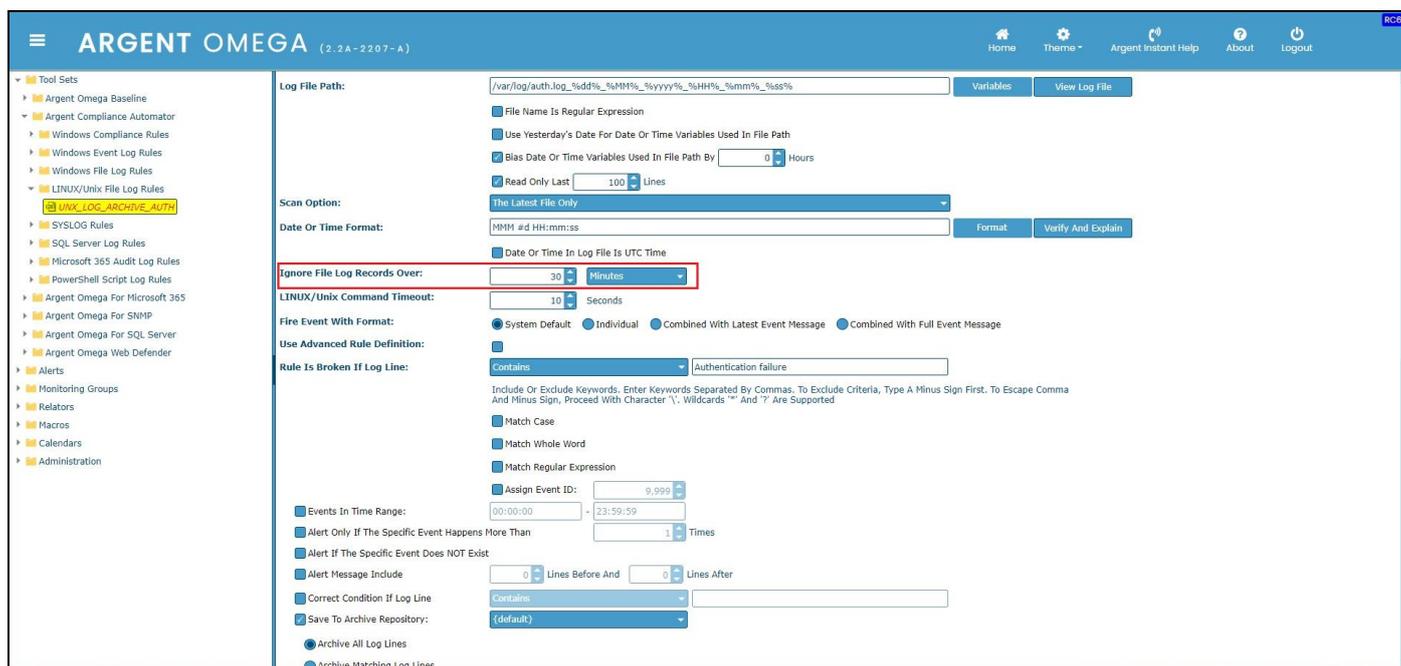
The **Verify And Explain** button is used to explain the Date or Time format specification string used and the number of matching lines with the specified Date or Time format that are currently present in the log file:



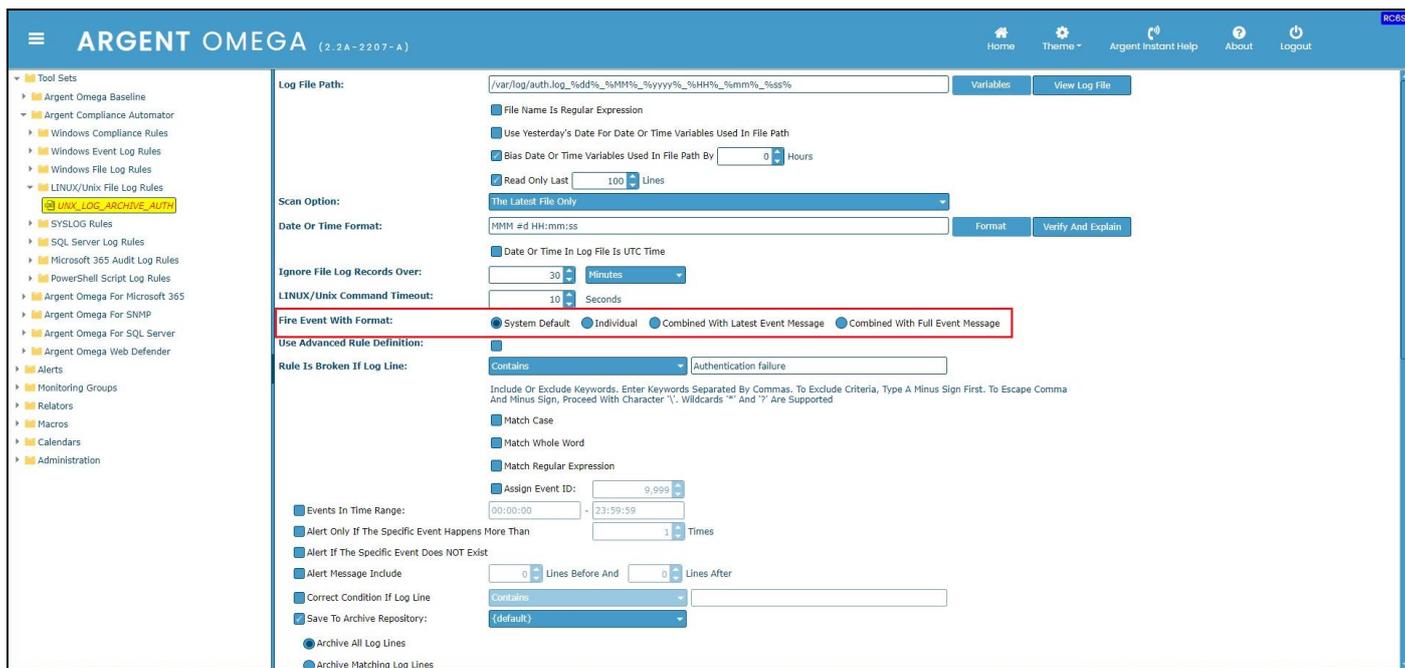
The **Date or Time In Log File Is UTC Time** option should be used when the monitored log file is using UTC time for its Date or Time field:



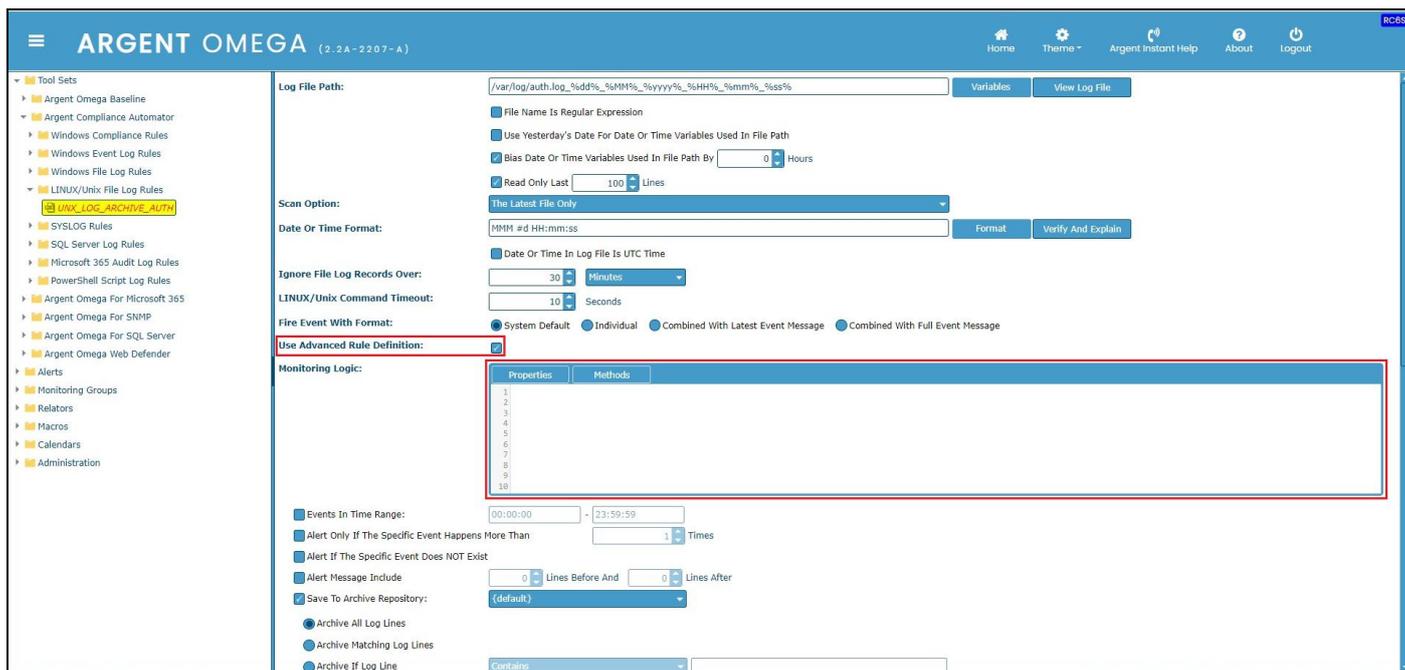
Use the **Ignore File Log Records Over** field to skip monitoring File Log records that are older than the specified time:



Select the Alert message format in the **Fire Event With Format** section:



The **Use Advanced Rule Definition** option can be used to add advanced PowerShell script logic to filter the log records:



The **Rule Is Broken If Log Line** section is used to specify the keyword string criteria to search for in the logs. It is possible to specify multiple keywords separated by commas. **To exclude criteria, type a minus sign first.** To escape comma and minus sign, proceed with character '\'. Wildcards '*' and '?' are supported.

There are also options, such as **Match Case**, **Match Whole Word** and **Match Regular Expression**, for more accurate filtering.

An Event ID can be specified in the Assign Event ID field to save a custom Event ID in the EVENT_ID_INT field while archiving data in the database table.

The screenshot shows the ARGENT OMEGA configuration interface. The left sidebar lists various tool sets and rules. The main configuration area is divided into several sections:

- Log File Path:** /var/log/auth.log_%d%_MM%_%yyyy%_%HH%_%mm%_%ss%
- Scan Option:** The Latest File Only
- Ignore File Log Records Over:** 30 Minutes
- LINUX/Unix Command Timeout:** 10 Seconds
- Fire Event With Format:** System Default
- Use Advanced Rule Definition:**
 - Rule Is Broken If Log Line:** Contains Authentication failure
 - Events In Time Range:** 00:00:00 - 23:59:59
 - Alert Only If The Specific Event Happens More Than:** 1 Times
 - Alert If The Specific Event Does NOT Exist:** (unchecked)
 - Alert Message Include:** 0 Lines Before And 0 Lines After
 - Correct Condition If Log Line:** Contains
 - Save To Archive Repository:** (default)
 - Archive All Log Lines:** (checked)
 - Archive Matching Log Lines:** (checked)

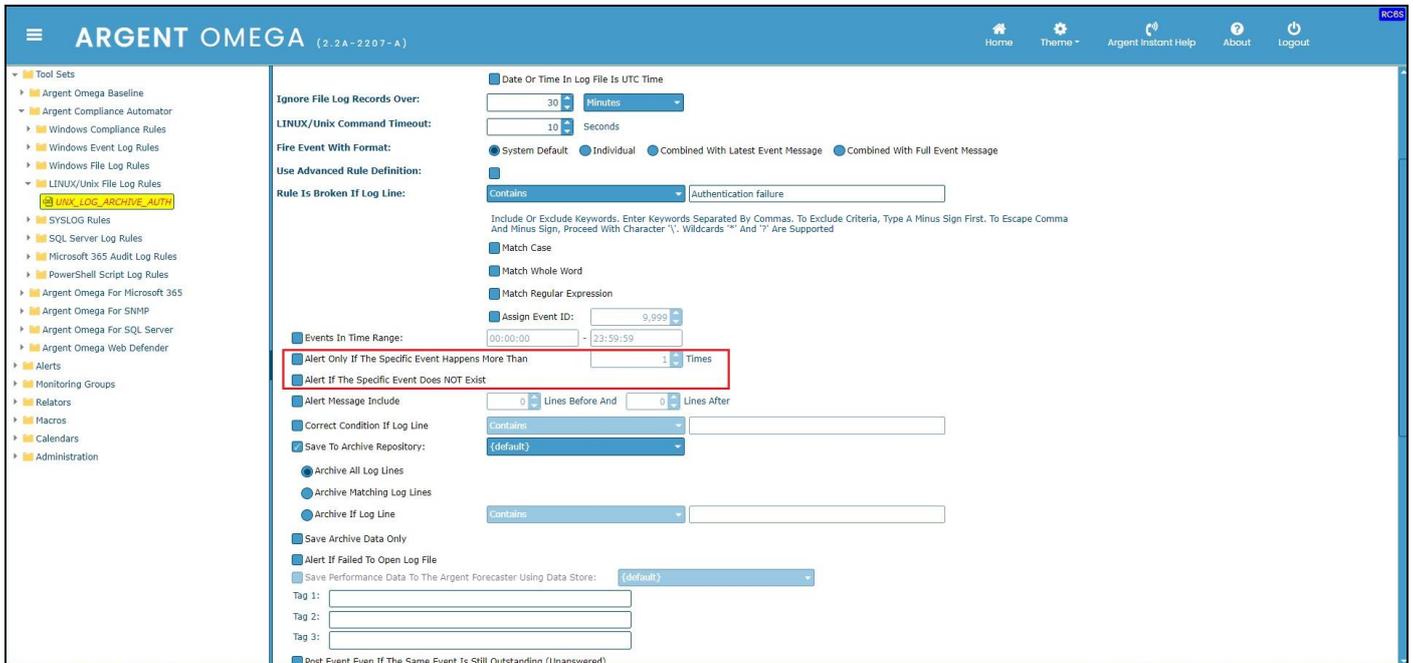
The **Events In Time Range** option can be used to filter event records in a specific time range:

The screenshot shows the ARGENT OMEGA configuration interface. The left sidebar lists various tool sets and rules. The main configuration area is divided into several sections:

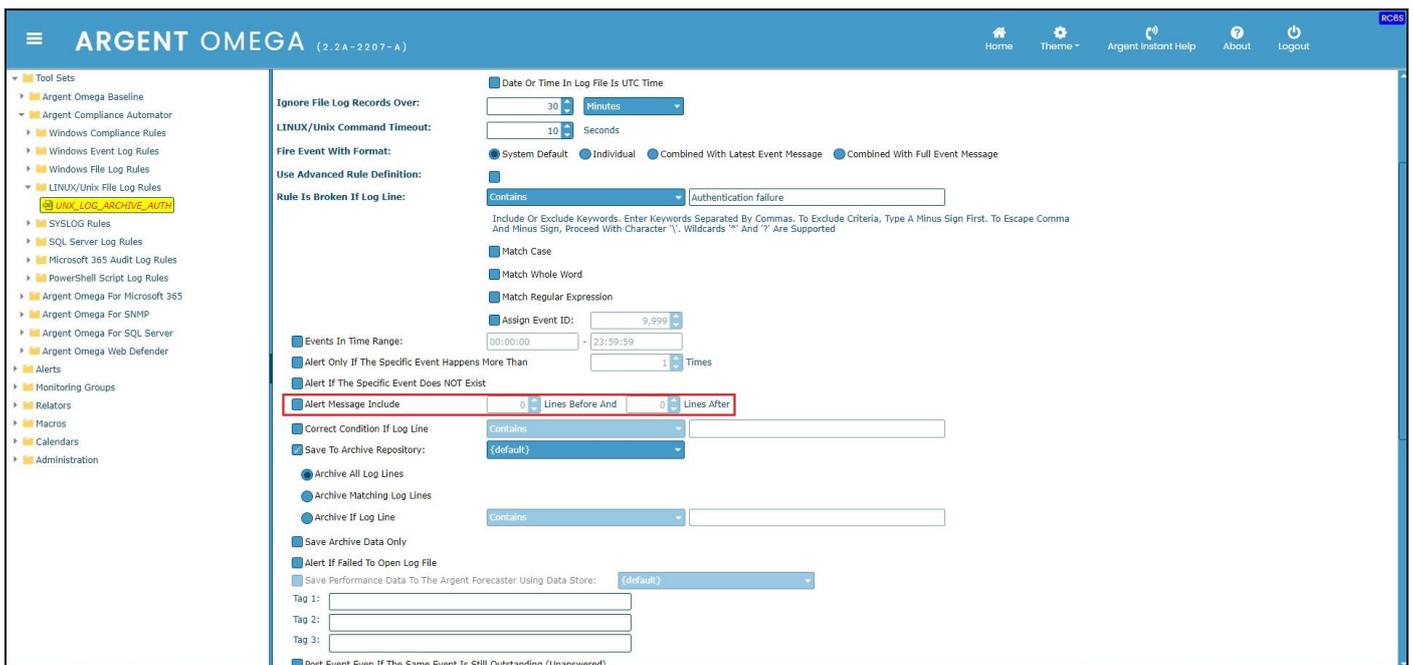
- Ignore File Log Records Over:** 30 Minutes
- LINUX/Unix Command Timeout:** 10 Seconds
- Fire Event With Format:** System Default
- Use Advanced Rule Definition:**
 - Rule Is Broken If Log Line:** Contains Authentication failure
 - Events In Time Range:** 00:00:00 - 23:59:59
 - Alert Only If The Specific Event Happens More Than:** 1 Times
 - Alert If The Specific Event Does NOT Exist:** (checked)
 - Alert Message Include:** 0 Lines Before And 0 Lines After
 - Correct Condition If Log Line:** Contains
 - Save To Archive Repository:** (default)
 - Archive All Log Lines:** (checked)
 - Archive Matching Log Lines:** (checked)
 - Archive If Log Line:** Contains
 - Save Archive Data Only:** (checked)
 - Alert If Failed To Open Log File:** (unchecked)
 - Save Performance Data To The Argent Forecaster Using Data Store:** (default)
 - Tag 1:** (empty)
 - Tag 2:** (empty)
 - Tag 3:** (empty)
 - Post Event Even If The Same Event Is Still Outstanding (Unanswered):** (checked)

Use the **Alert Only If The Specific Event Happens More Than x Times** option to trigger alerts only after the specified event has occurred a given number of times.

There is an option to Alert if the **Specific Event does not exist**:

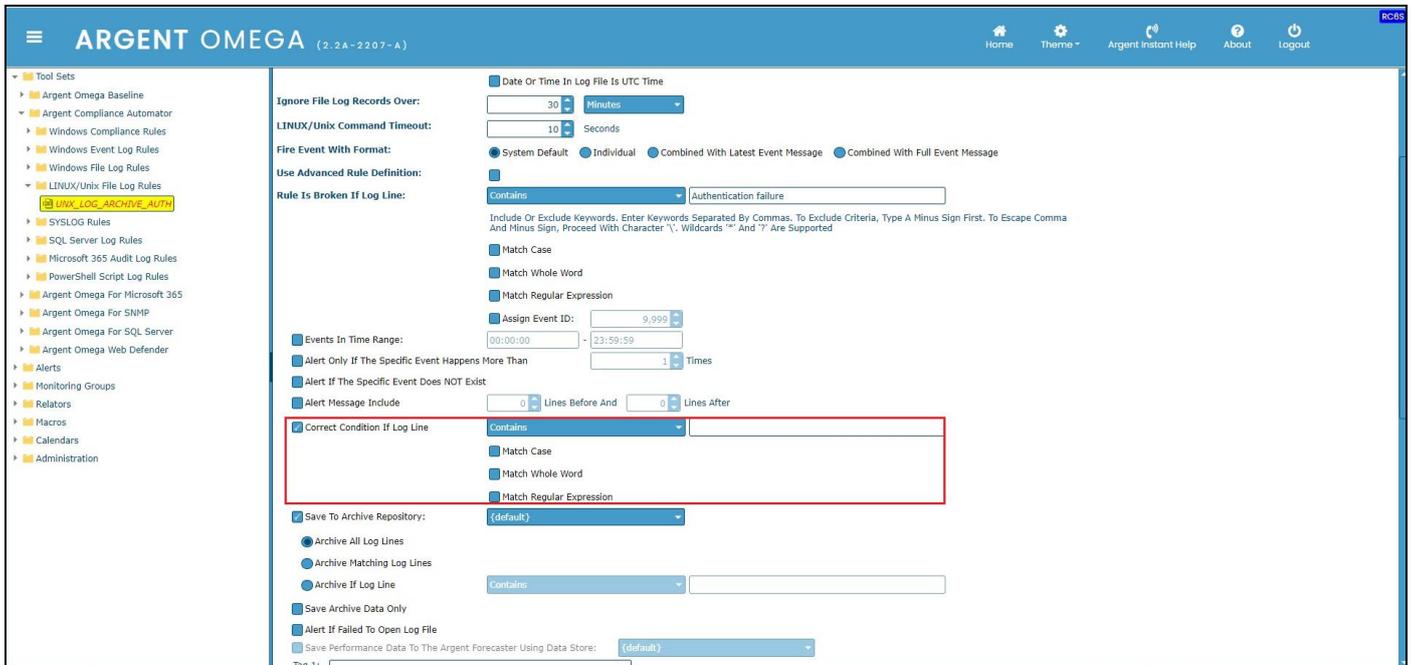


The **Alert Message Include** option can be used to have the alert details include a given number of log lines from before and after the log event line that triggers the alert::



The **Correct Condition If Log Line** option can be used to look for a message string in the monitored log that will trigger a condition corrected alert during a future log poll.

There are also options such as **Match Case**, **Match Whole Word** and **Match Regular Expression** for accurate filtering:

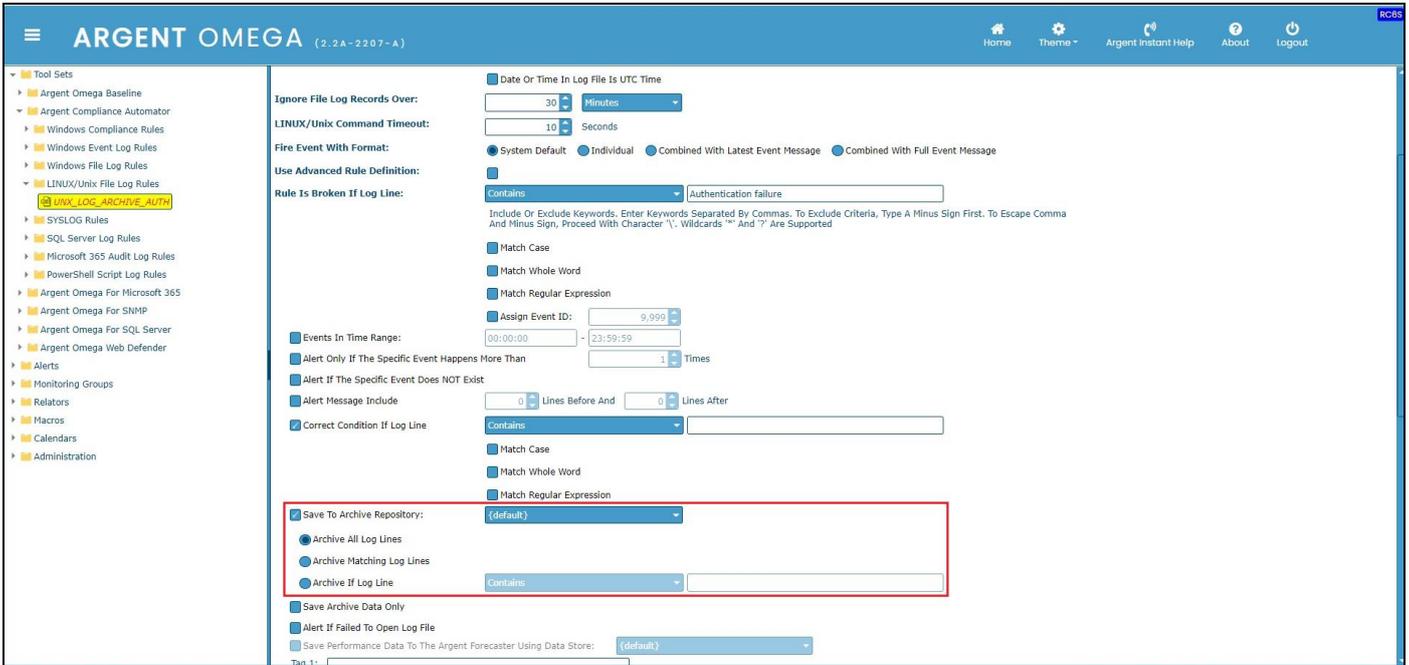


The **Save To Archive Repository** option provides different criteria for saving the event records to the Archive Repository.

The **Archive All Log Lines** option is used to save all log line entries from the monitored log to the database tables. Each line in the monitored log file will be saved as a separate record in the database table.

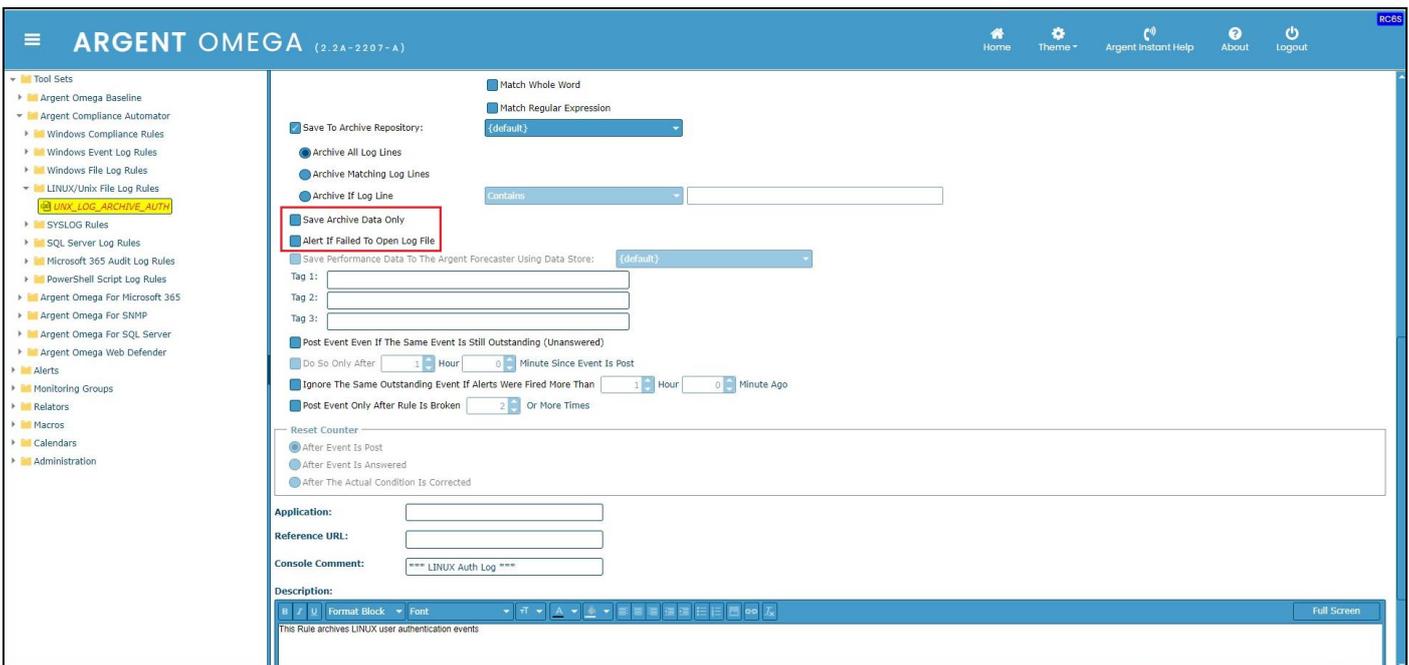
The **Archive Matching Log Lines** option is used to save only the log line entries that match the condition specified in the **Rule Is Broken If Log Line** section. Each matching line in the log file will be saved as a separate record in the database table.

The **Archive If Log Line Contains** option is used to save only the log lines that contain the specified strings.



The **Save Archive Data Only** option can be used to save archived data without triggering Alerts.

The **Alert If Failed to Open Log File** option can be used to trigger an alert if the Rule fails to open the logs on the monitored server.

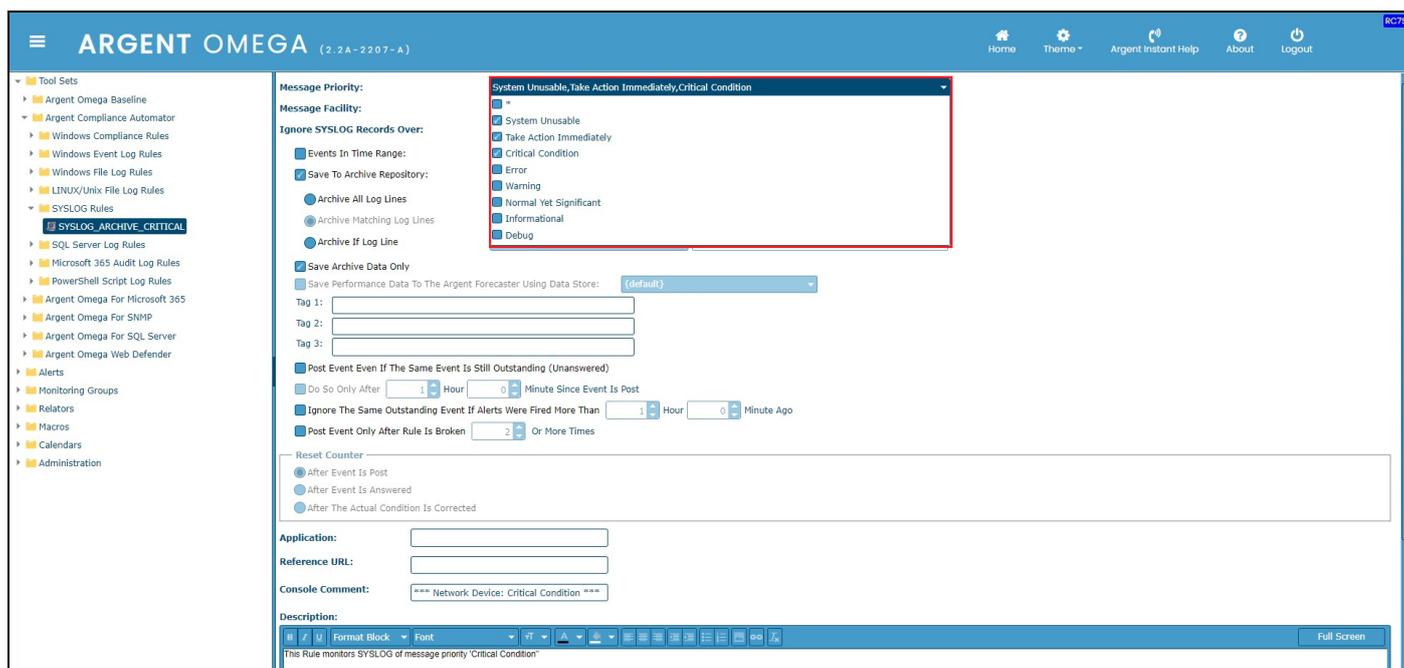


SYSLOG Rules

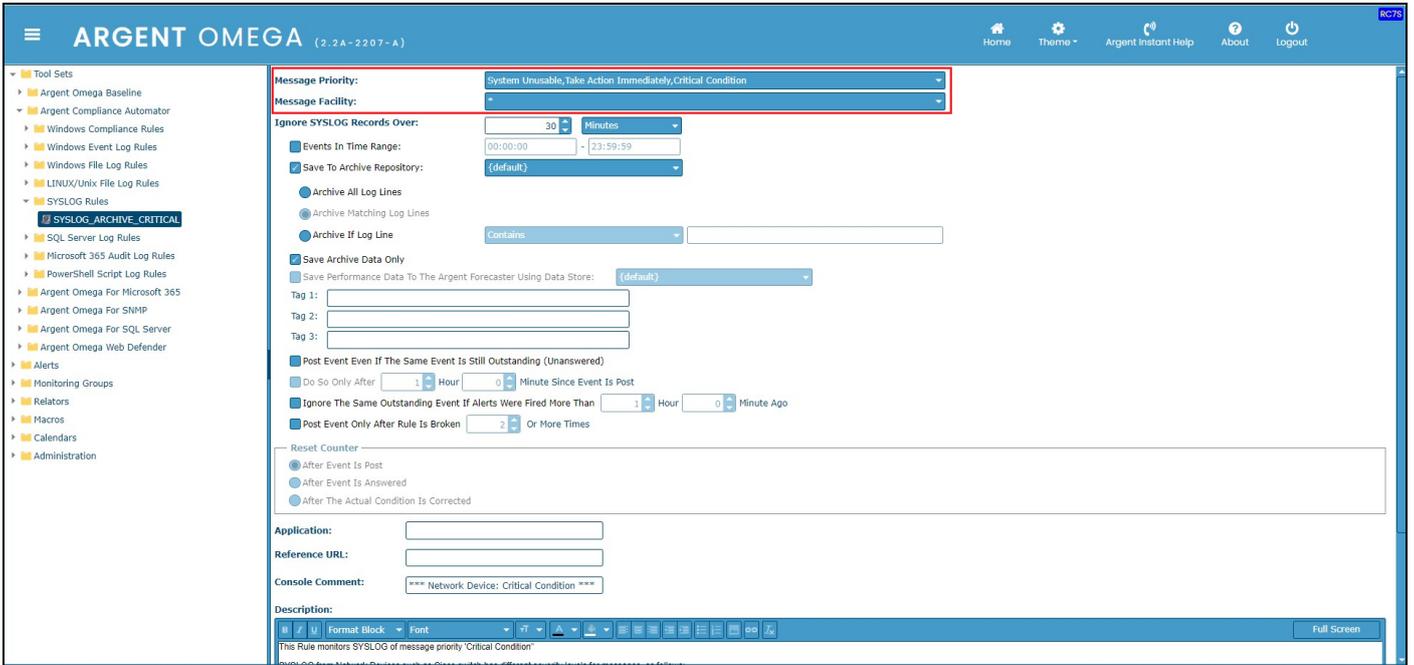
SYSLOG Rules are used to monitor and archive SYSLOG events from any type of network device.

The SYSLOG Rules include the option to filter by the different SYSLOG message severity levels:

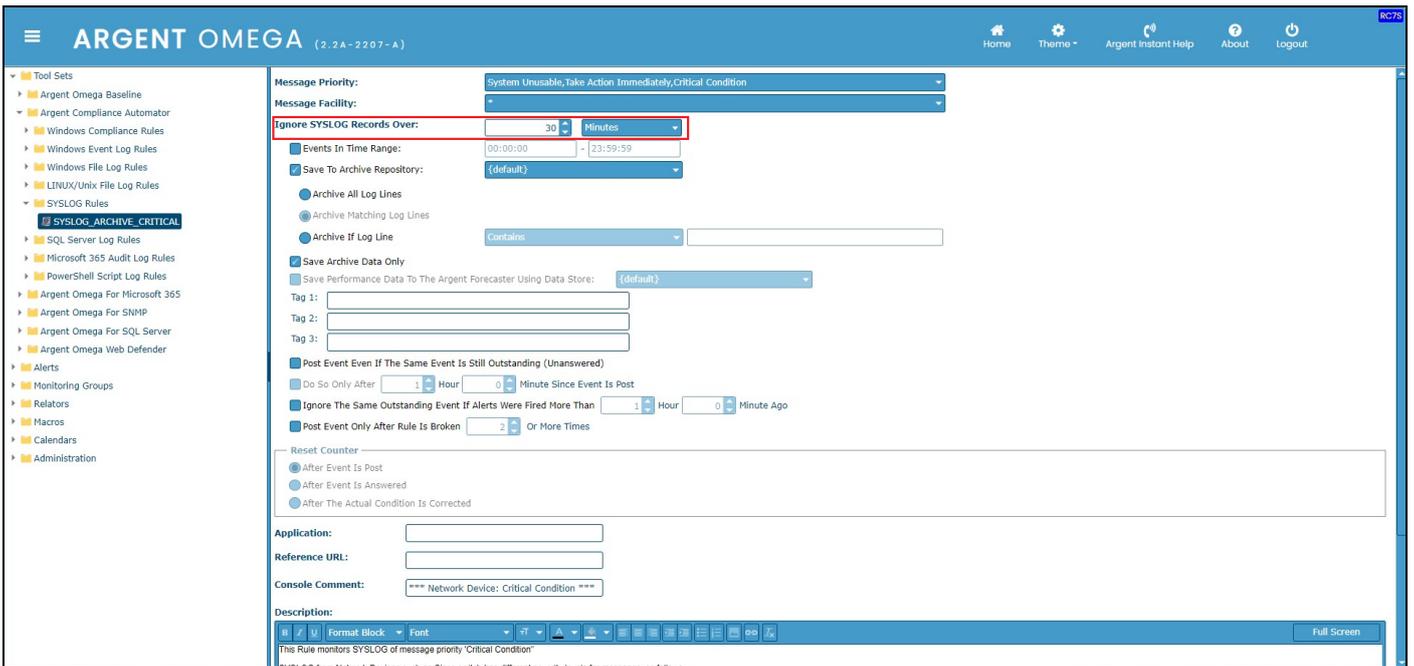
- System Unusable
- Take Action Immediately
- Critical Condition
- Error
- Warning
- Normal, But Significant
- Informational
- Debug Information



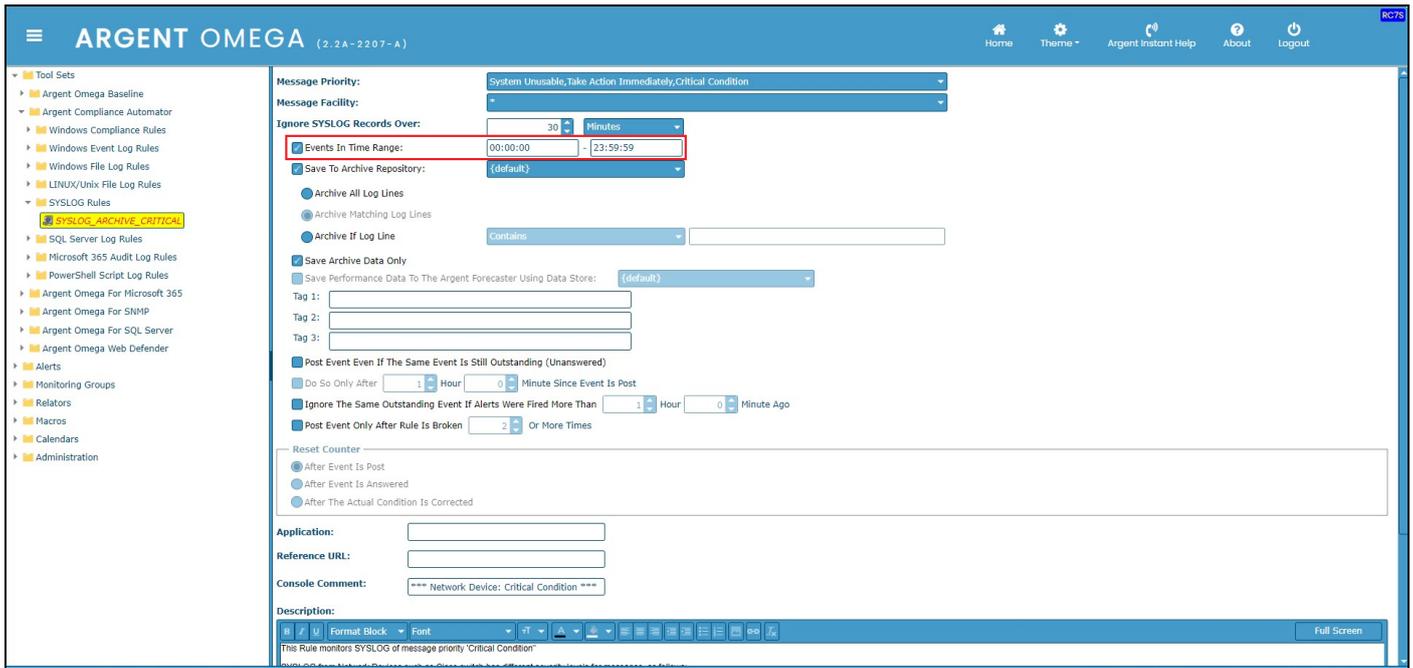
These filters are specified using the **Message Priority** and **Message Facility** drop-down selections:



Use the **Ignore File Log Records Over** field to skip monitoring SYSLOG records that are older than the specified time:



The **Events in Time Range** option can be used to filter event records in a specific time range:



The **Save To Archive Repository** option provides different criteria for saving the event records to the Archive Repository.

The **Archive All Log Lines** option is used to save all log line entries from the monitored log to the database tables. Each line in the monitored log file will be saved as a separate record in the database table.

The **Archive Matching Log Lines** option is used to save only the log line entries that match the condition specified in the **Rule Is Broken If Log Line** section. Each matching line in the log file will be saved as a separate record in the database table.

The **Archive If Log Line Contains** option is used to save only the log lines that contain the specified strings.

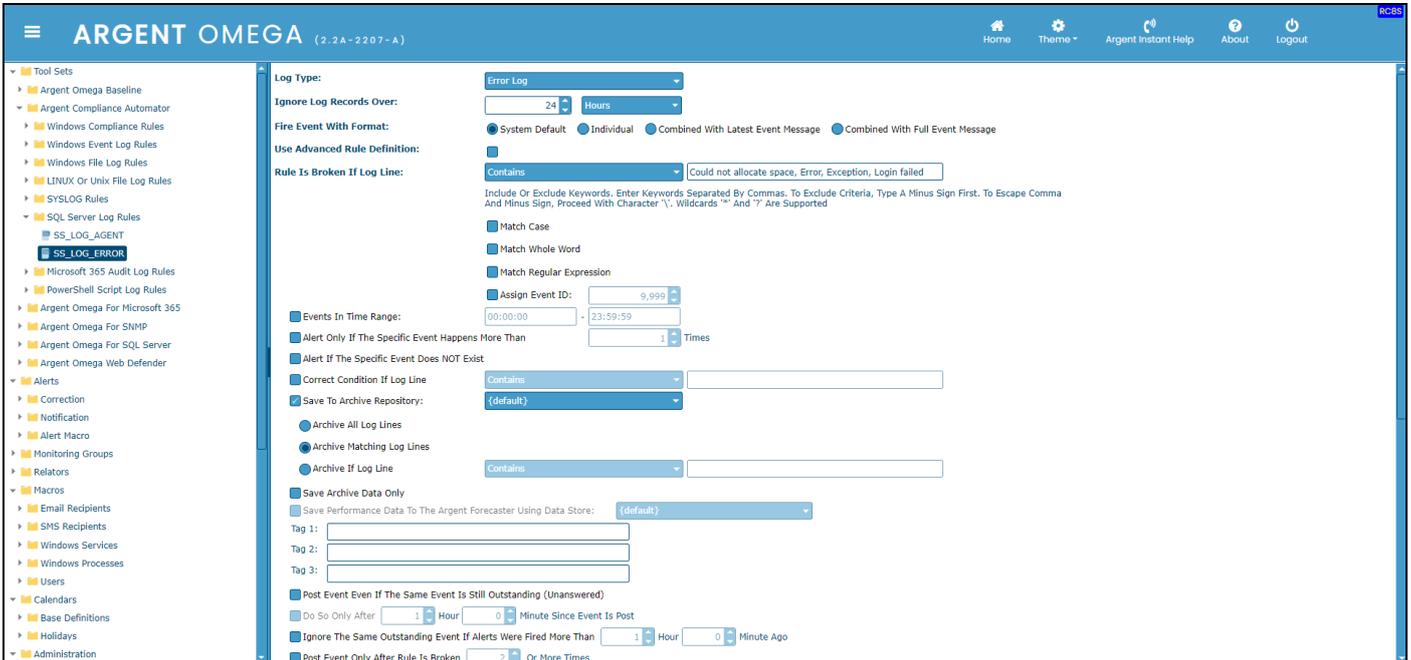
The **Save Archive Data Only** option can be used to save archived data without triggering Alerts:

The screenshot displays the ARGENT OMEGA configuration interface. The left sidebar shows a tree view of tool sets, with 'SYSLOG ARCHIVE CRITICAL' highlighted. The main configuration area is for a rule with the following settings:

- Message Priority:** System Unusable, Take Action Immediately, Critical Condition
- Message Facility:** (empty)
- Ignore SYSLOG Records Over:** 20 Minutes
- Events In Time Range:** 00:00:00 - 23:59:59
- Save To Archive Repository:** (default)
- Archive Options:**
 - Archive All Log Lines
 - Archive Matching Log Lines
 - Archive If Log Line Contains (empty)
- Save Archive Data Only:** (highlighted in a red box)
- Save Performance Data To The Argent Forecaster Using Data Store:** (default)
- Tag 1:** (empty)
- Tag 2:** (empty)
- Tag 3:** (empty)
- Post Event Even If The Same Event Is Still Outstanding (Unanswered):**
- Do So Only After:** 1 Hour 0 Minute Since Event Is Post
- Ignore The Same Outstanding Event If Alerts Were Fired More Than:** 1 Hour 0 Minute Ago
- Post Event Only After Rule Is Broken:** 2 Or More Times
- Reset Counter:**
 - After Event Is Post
 - After Event Is Answered
 - After The Actual Condition Is Corrected
- Application:** (empty)
- Reference URL:** (empty)
- Console Comment:** *** Network Device: Critical Condition ***
- Description:** This Rule monitors SYSLOG of message priority 'Critical Condition'

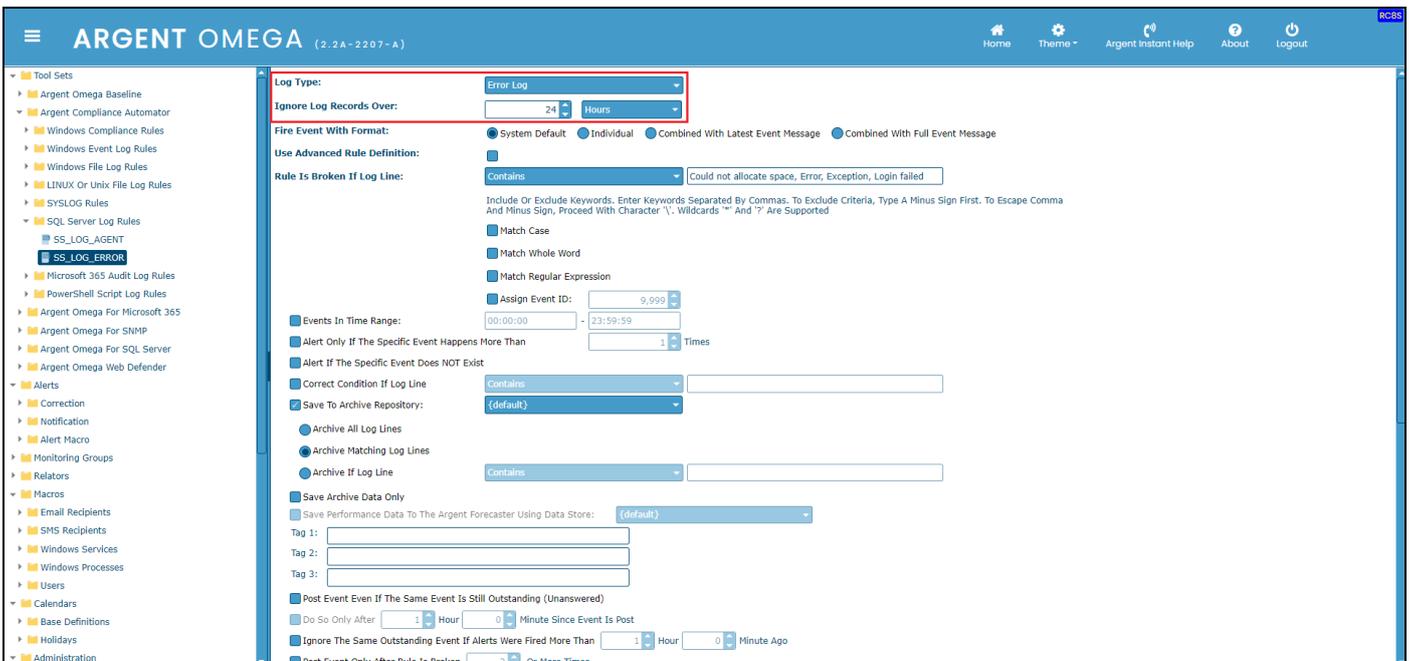
SQL Server Log Rules

The SQL Server Log Rules are used to monitor or archive SQL Server and SQL Server Agent log files to identify significant errors:

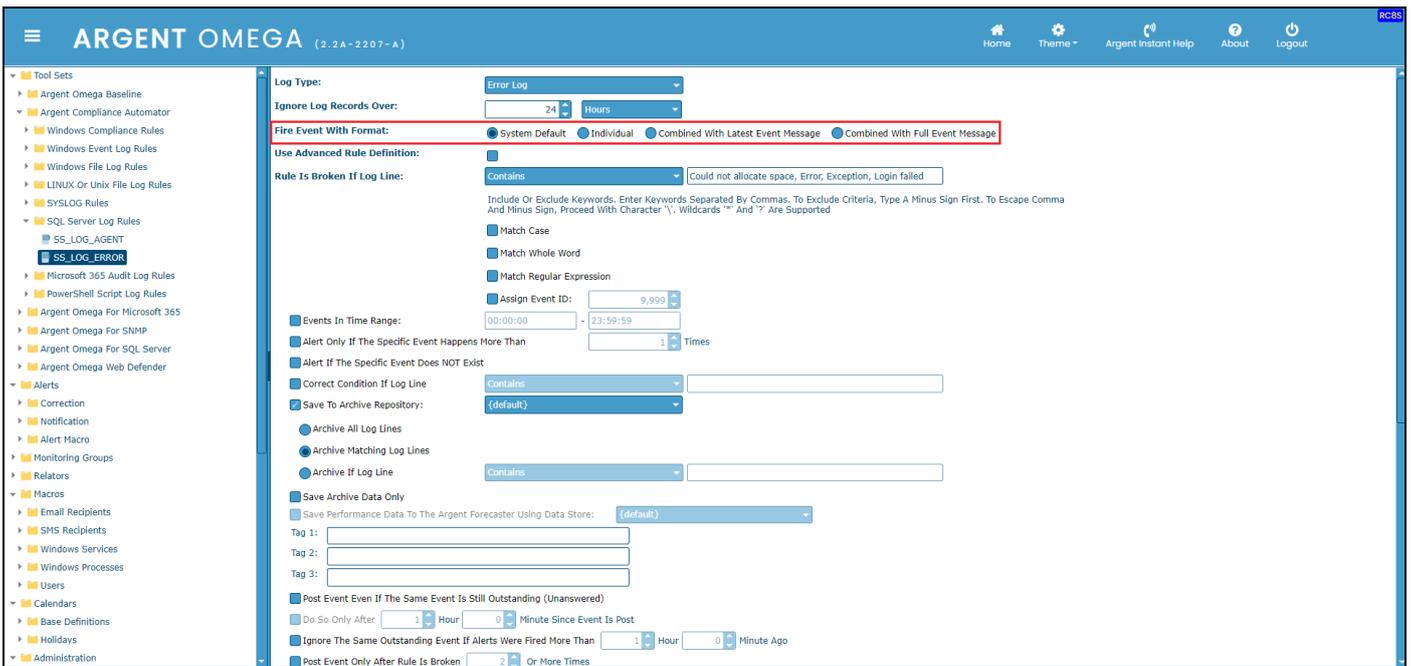


The **Log Type** option can be configured to specify monitoring the Agent Log or the Error Log.

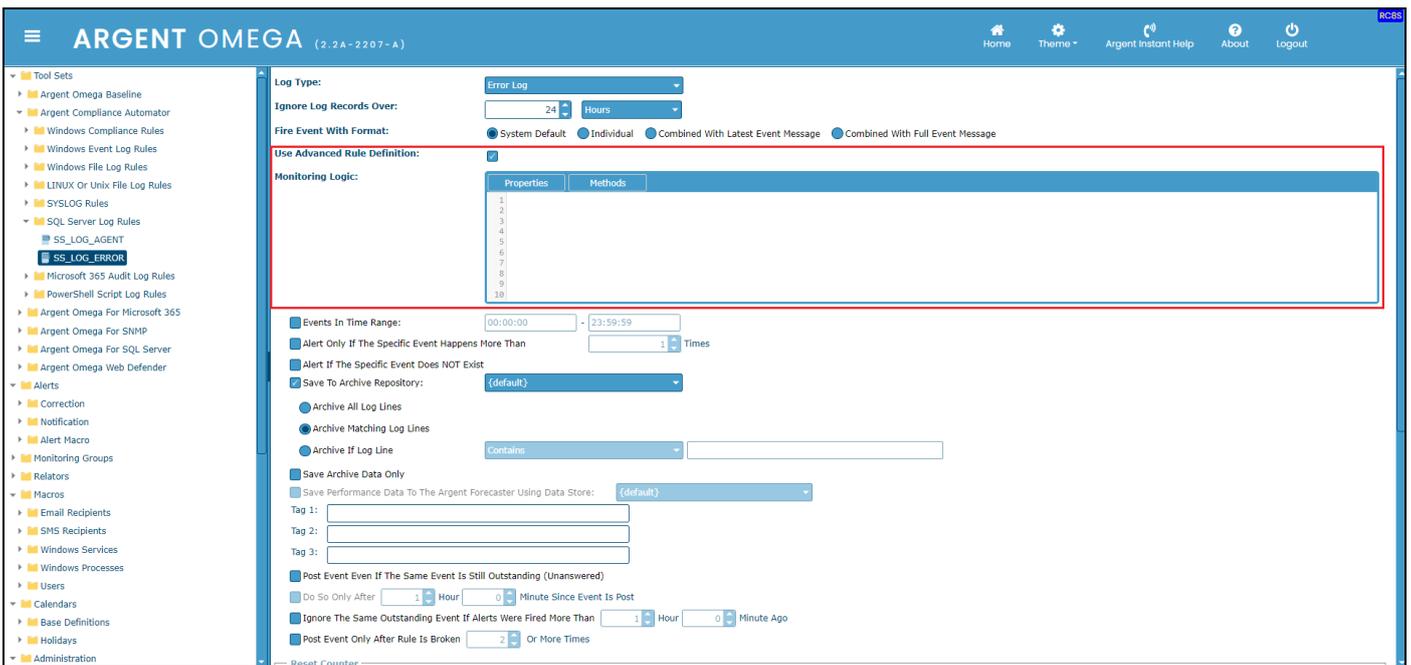
Use the **Ignore File Log Records Over** field to skip monitoring Log records that are older than the specified time:



The **Fire Event With Format** option is used to select the Alert message format:



The **Use Advanced Rule Definition** option adds advanced PowerShell script logic to filter the log records:



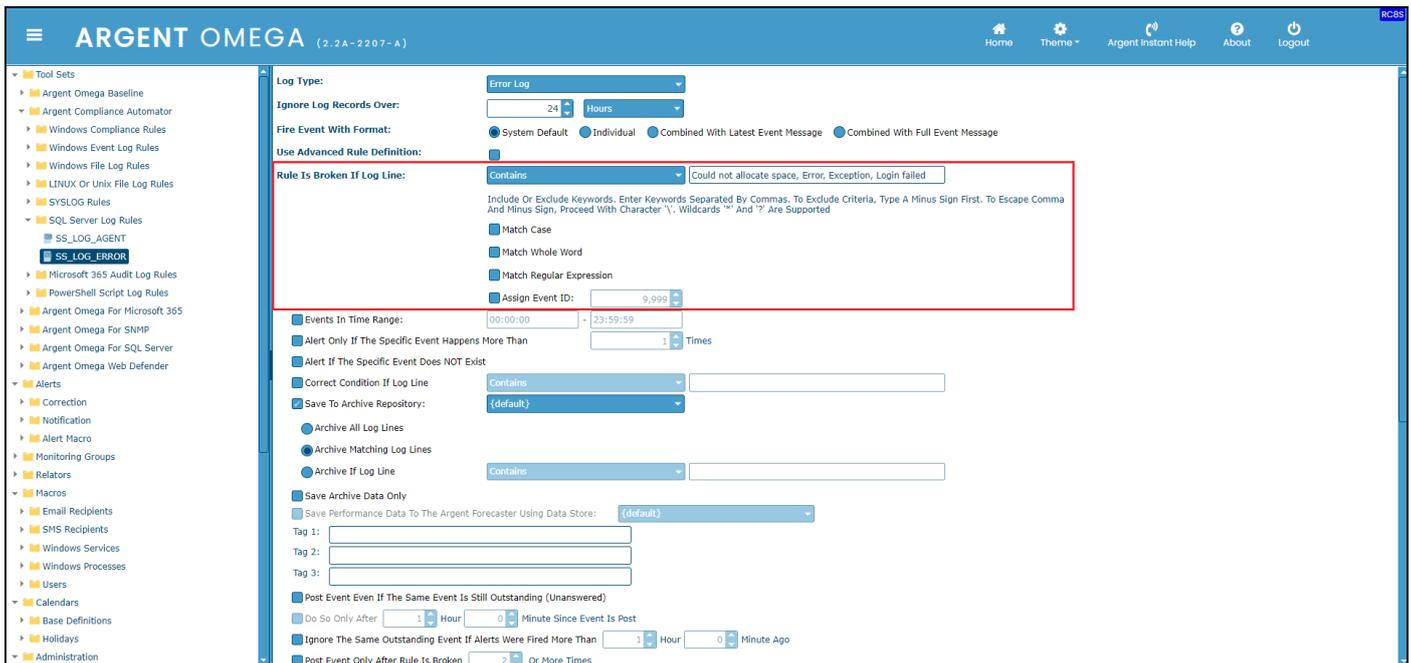
The **Rule Is Broken If Log Line** section is used to specify the keyword string criteria to search for in the logs.

Multiple keywords, separated by commas, can be specified.

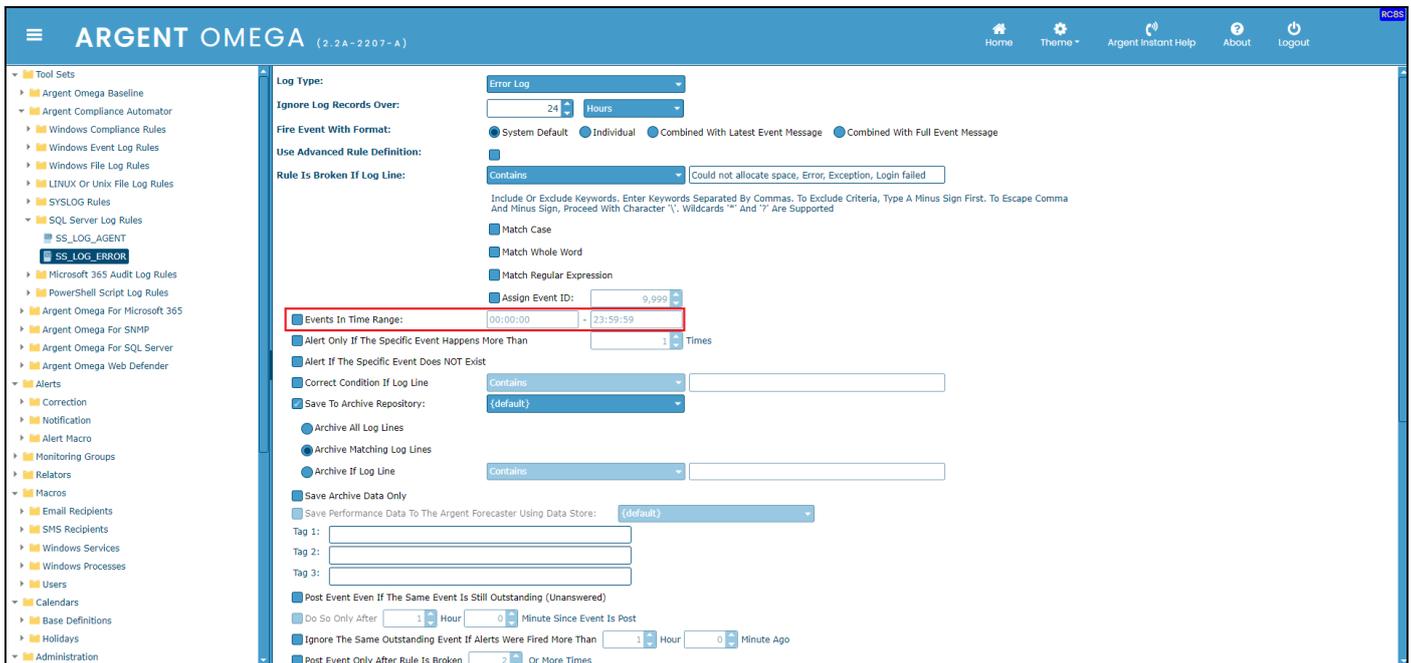
To exclude criteria, type a minus sign first. To escape comma and minus sign, proceed with character '\'. Wildcards '*' and '?' are supported.

There are also options, such as **Match Case**, **Match Whole Word** and **Match Regular Expression**, for more accurate filtering.

An Event ID can be specified in the Assign Event ID field to save a custom Event ID in the EVENT_ID_INT field while archiving data in the database table:

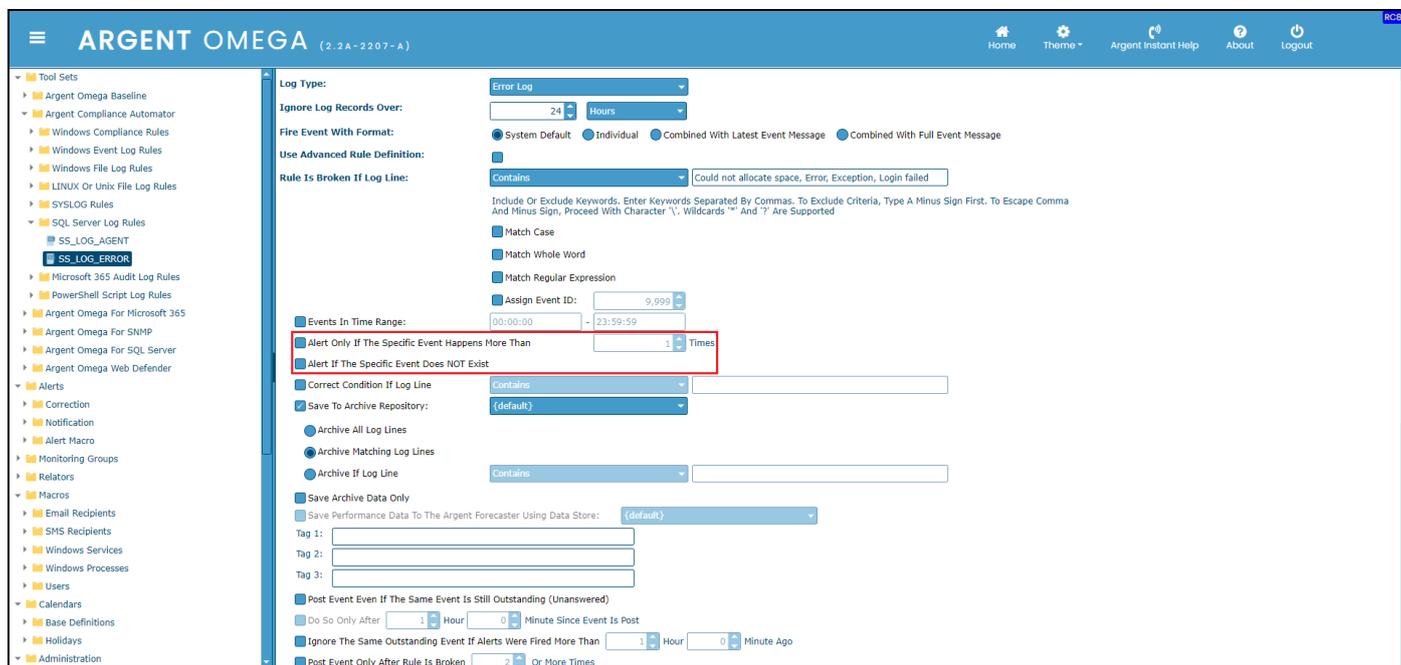


The **Events In Time Range** option can be used to filter Event log records in a specific time range:



Use the **Alert Only If The Specific Event Happens More Than** option to trigger alerts only after the specified event has occurred a given number of times..

There is an option to Alert if the **Specific Event does not exist**:



There is an option to save the Event records to the Archive Repository.

There are different options for **Save To Archive Repository**.

The **Archive All Log Lines** option is used to save all log line entries from the monitored log to the database tables. Each line in the monitored log file will be saved as a separate record in the database table.

The **Archive Matching Log Lines** option is used to save only the log line entries that match the condition specified in the **Rule Is Broken If Log Line** section. Each matching line in the log file will be saved as a separate record in the database table.

The **Archive If Log Line Contains** option is used to save only the log lines that contain the specified strings.

The **Save Archive Data Only** option can be used to save archived data without triggering Alerts:

The screenshot displays the ARGENT OMEGA configuration interface. The left sidebar shows a tree view of tool sets, with 'SS_LOG_ERROR' selected under 'SQL Server Log Rules'. The main configuration area is for an 'Error Log' rule. The 'Save Archive Data Only' checkbox is checked and highlighted with a red box. Below it, the 'Save Performance Data To The Argent Forecaster Using Data Store:' checkbox is also checked. The 'Archive If Log Line' radio button is selected, and the condition is set to 'Contains'. Other settings include 'Log Type: Error Log', 'Ignore Log Records Over: 24 Hours', and 'Fire Event With Format: System Default'.

Microsoft 365 Audit Log Rules

The Microsoft 365 Audit Log Rules are used to monitor or archive Microsoft 365 Audit Log events.

This Rule uses the PowerShell cmdlet "Search_UnifiedAuditLog."

The following should be configured prior to using these Rules:

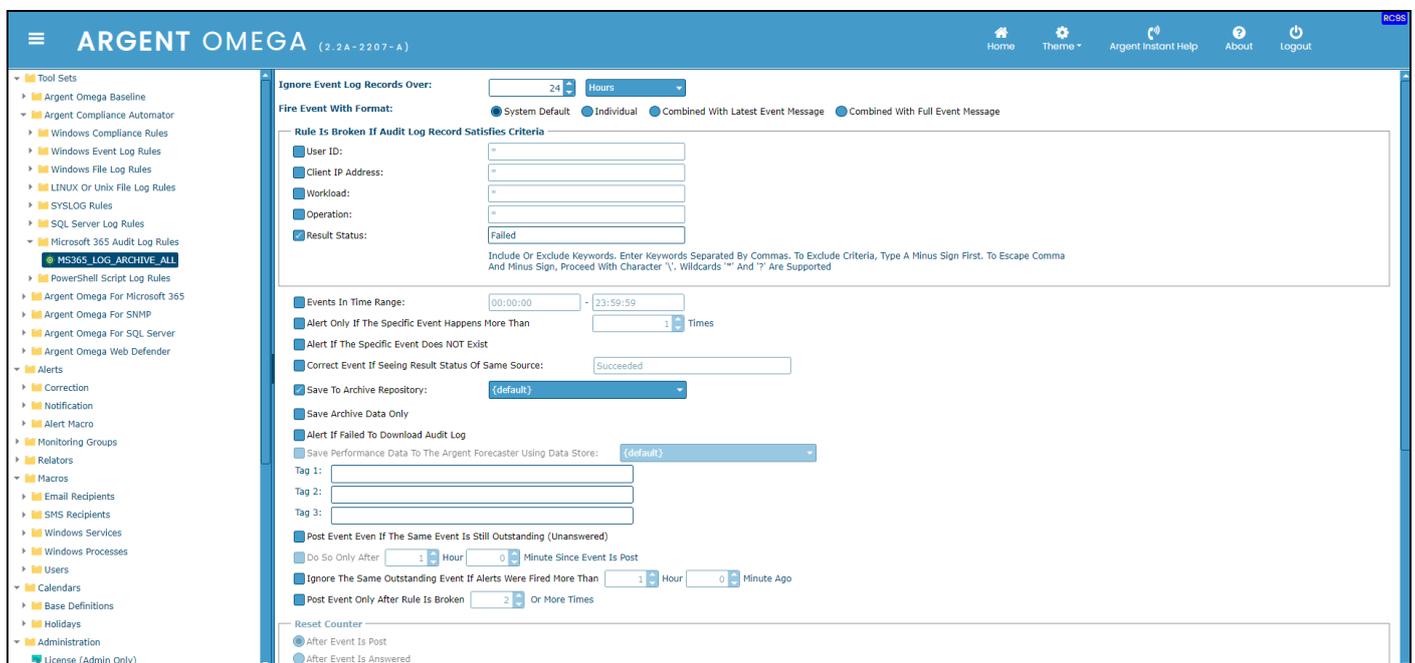
Install PowerShell module "ExchangeOnlineManagement"

Register Application has to be assigned the Audit Logs role in Exchange Online to turn auditing on or off in your Microsoft 365 organization. By default, this role is assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center. Global admins in Microsoft 365 are members of the Organization Management role group in Exchange Online.

Turn auditing on by running "Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled \$true"

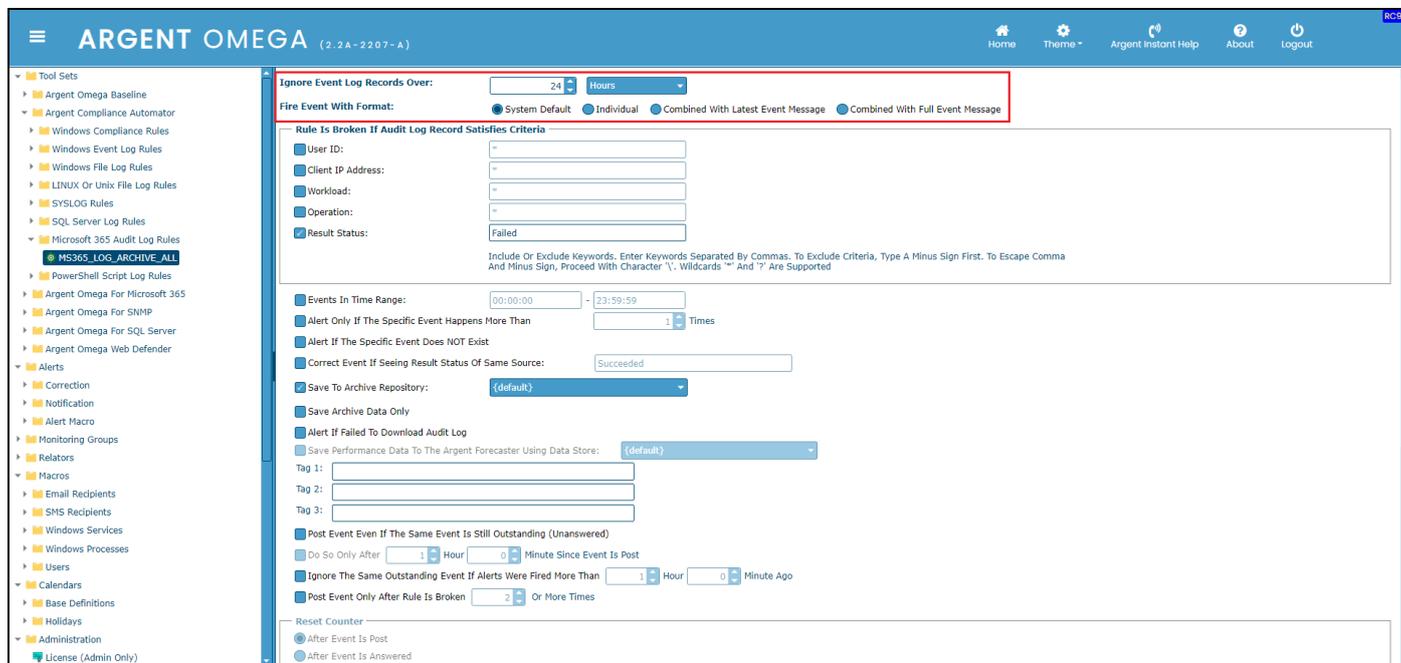
Run the following command to confirm that auditing is turned:

```
'Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled'
```



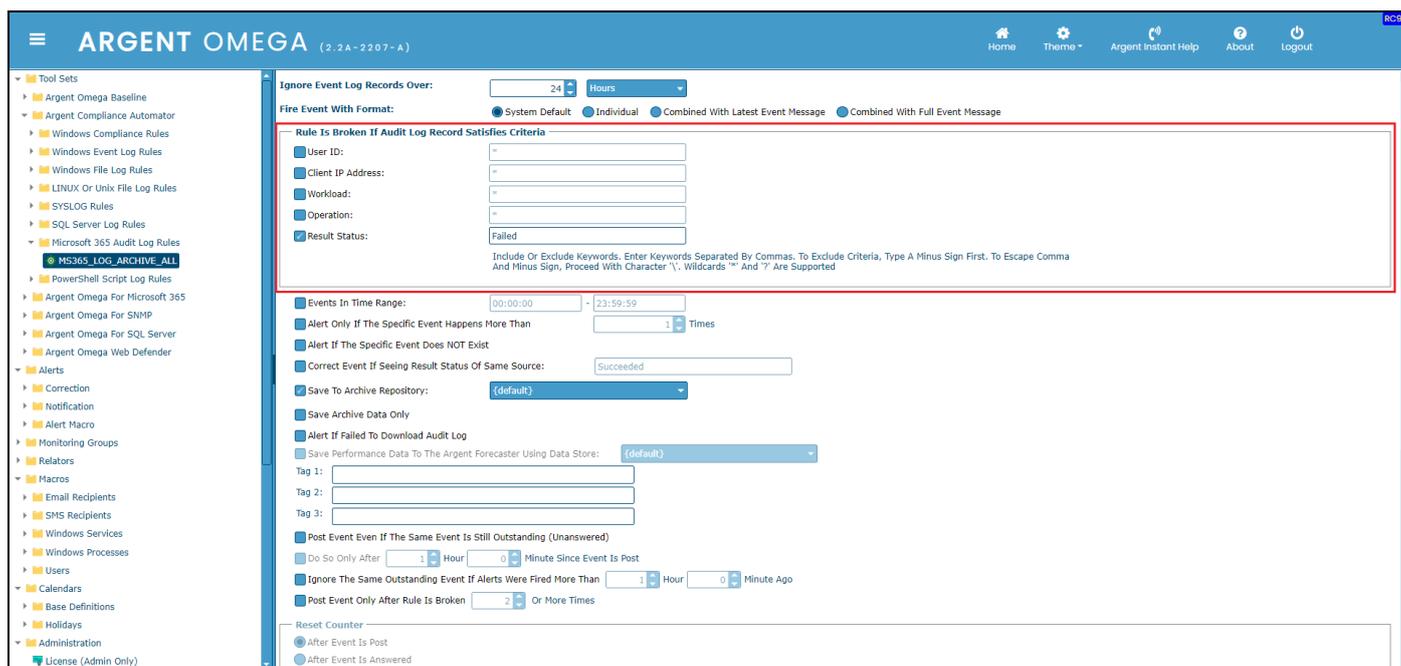
Use the **Ignore File Log Records Over** field to skip monitoring Log records that are older than the specified time.

The **Fire Event With Format** option is used to select the Alert message format:

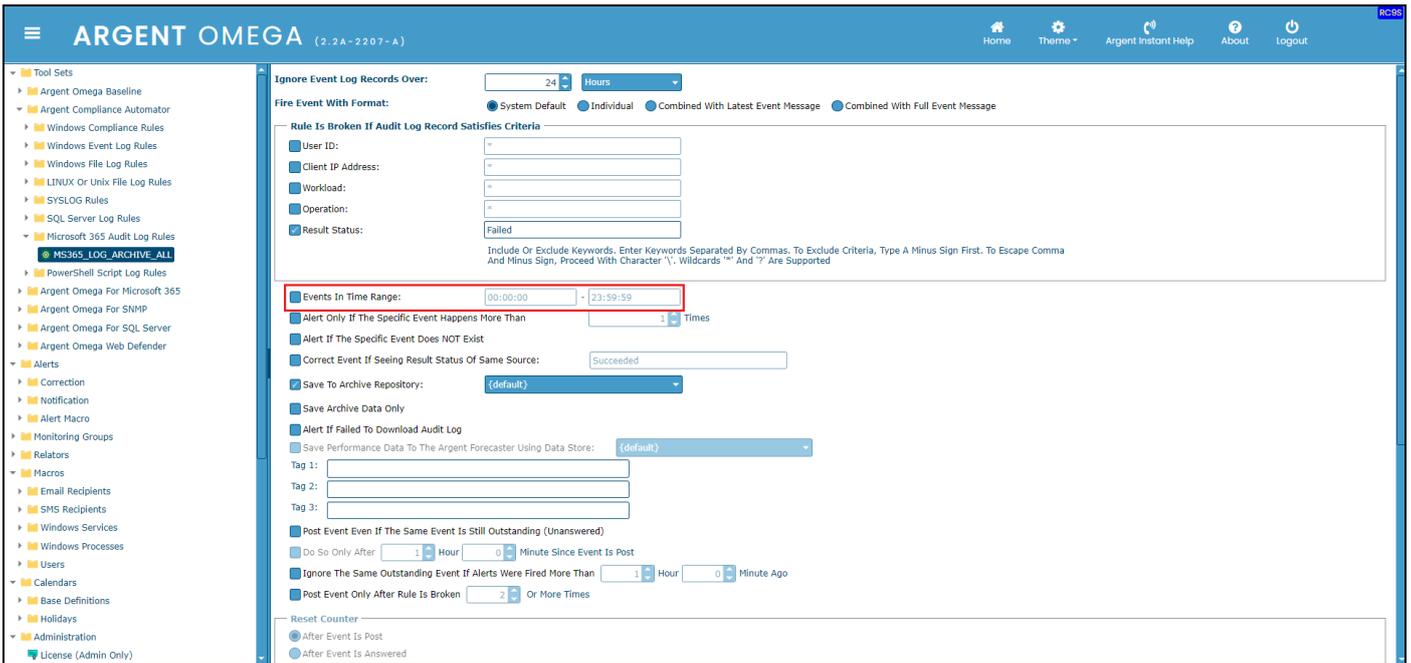


The **Rule Is Broken If Audit Log Record Satisfies Criteria** section provides various fields for filtering events.

Events can be filtered by User ID, Client IP Address, Workload, Operation or Result Status:

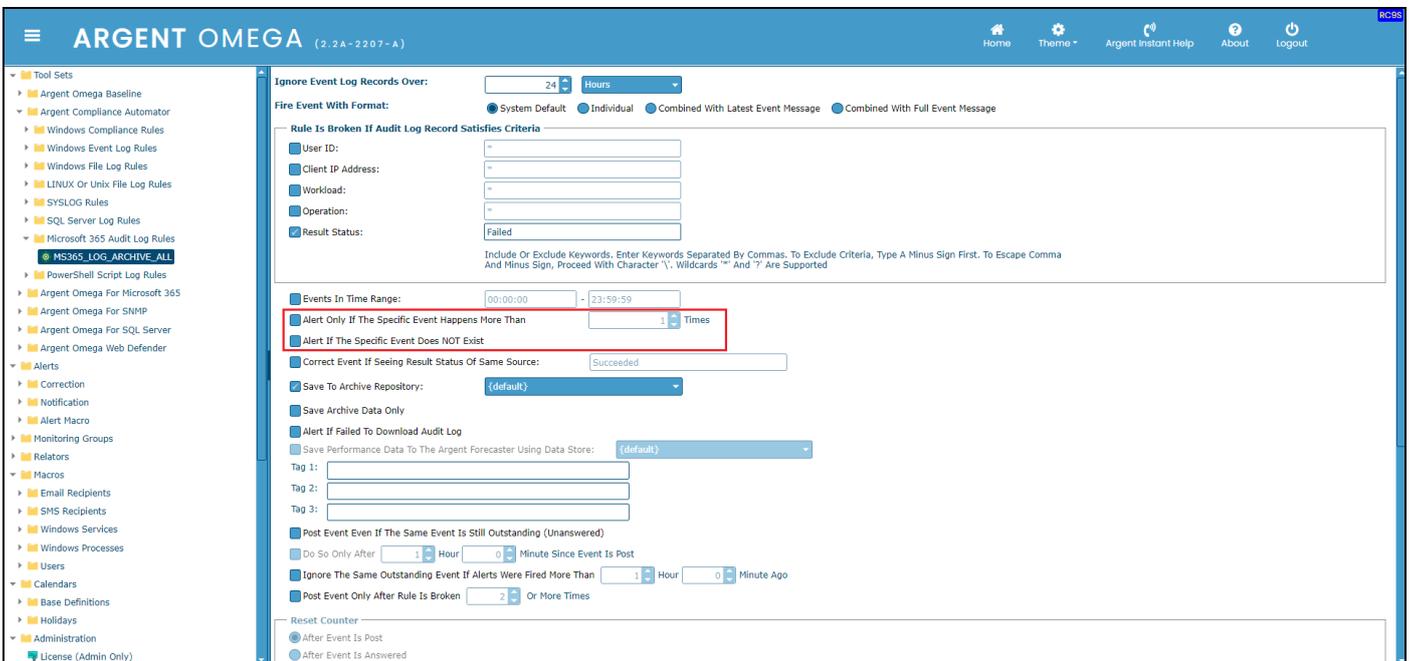


The **Events in Time Range** option can be used to filter event records in a specific time range:

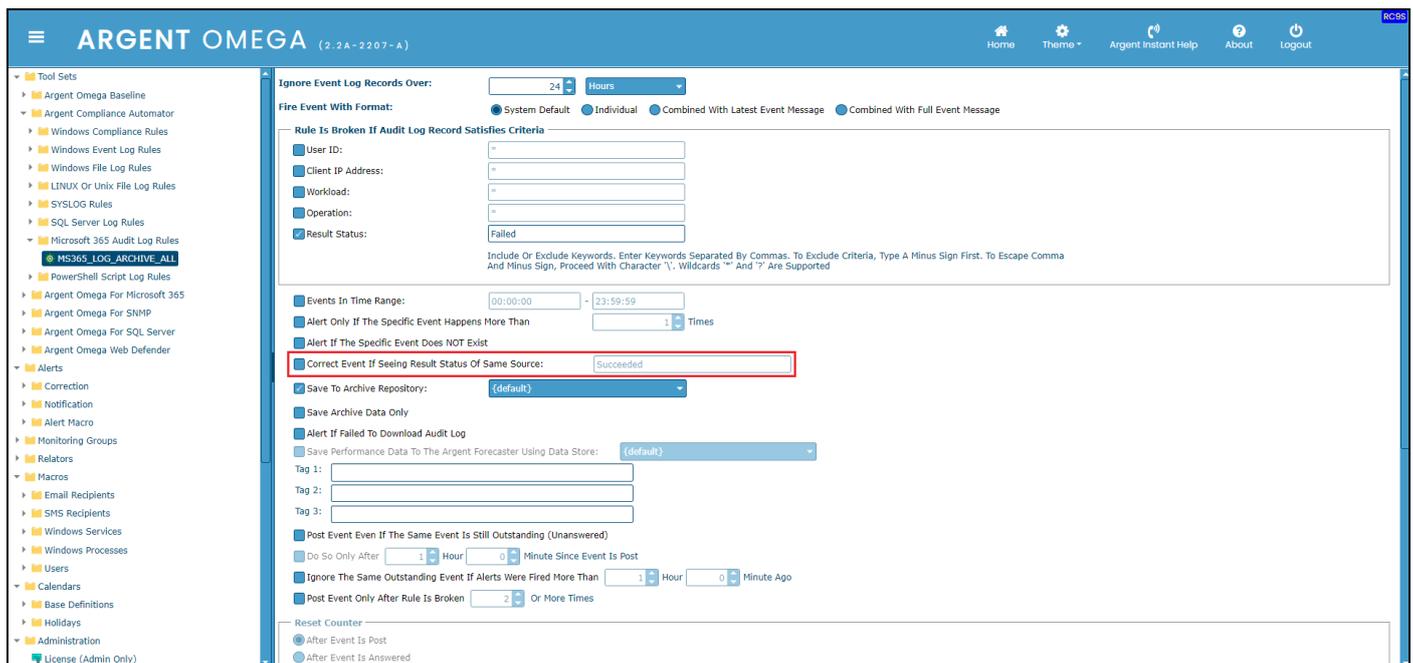


Use the **Alert Only If The Specific Event Happens More Than x Times** option to trigger alerts only after the specified event has occurred a given number of times.

There is an option to alert if the **Specific Event does not exist**:



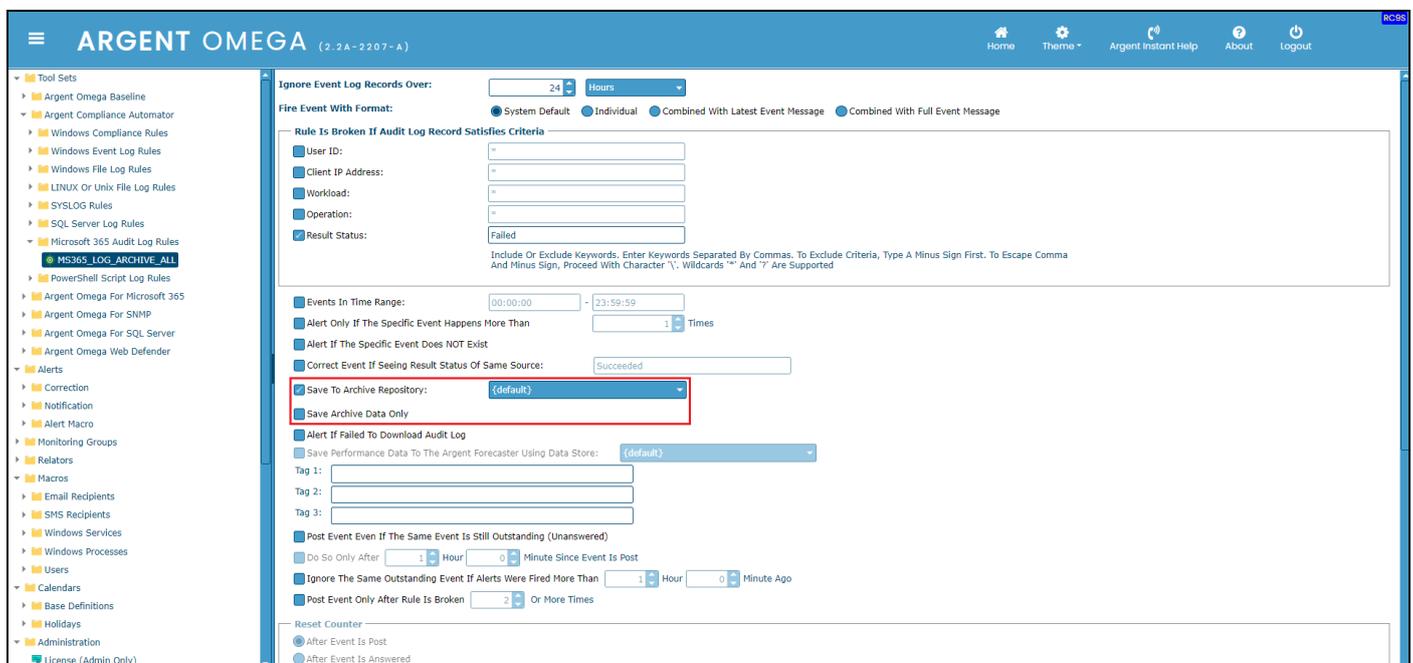
Use the **Correct Event If Seeing Result Status Of Same Source** option to specify the criteria to trigger a condition corrected alert:



The Rule can be saved to a specified Archive Repository.

The Audit Records should be archived to the database table name **ARGSOFT_COMPLIANCE_LOG_ARCHIVE**.

The **Save Archive Data Only** option can be used to save archived data without triggering Alerts:



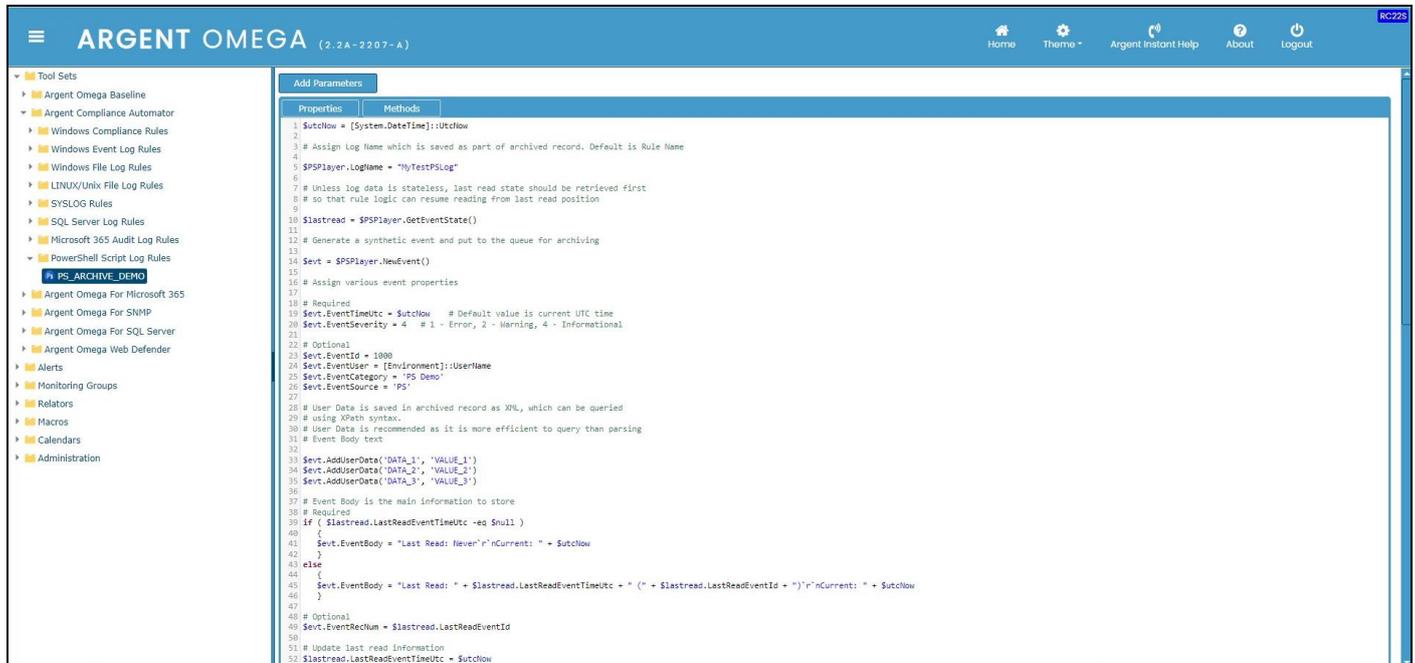
The **Alert If Failed to Download Audit Log** option can be used to trigger an Alert if the Rule failed to retrieve the Microsoft 365 Event Log records:

The screenshot displays the ARGENT OMEGA configuration interface. The top navigation bar includes 'Home', 'Theme', 'Argent Instant Help', 'About', and 'Logout'. The left sidebar lists various tool sets, with 'MS365_LOG_ARCHIVE_ALL' selected. The main configuration area is titled 'Ignore Event Log Records Over: 24 Hours'. Below this, the 'Fire Event With Format' section has radio buttons for 'System Default', 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'. The 'Rule Is Broken If Audit Log Record Satisfies Criteria' section contains several criteria: 'User ID', 'Client IP Address', 'Workload', 'Operation', and 'Result Status' (set to 'Failed'). A note below these criteria reads: 'Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Proceed With Character \'. Wildcards * and ? Are Supported'. The 'Events In Time Range' is set to '00:00:00 - 23:59:59'. Other options include 'Alert Only If The Specific Event Happens More Than 1 Times', 'Alert If The Specific Event Does NOT Exist', 'Correct Event If Seeing Result Status Of Same Source: Succeeded', 'Save To Archive Repository: (default)', 'Save Archive Data Only', and the highlighted 'Alert If Failed To Download Audit Log' option. Below this is 'Save Performance Data To The Argent Forecaster Using Data Store: (default)'. There are three 'Tag' input fields. The 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)' section includes 'Do So Only After 1 Hour 0 Minute Since Event Is Post', 'Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 Hour 0 Minute Ago', and 'Post Event Only After Rule is Broken 2 Or More Times'. The 'Reset Counter' section has radio buttons for 'After Event Is Post' and 'After Event Is Answered'.

PowerShell Script Log Rules

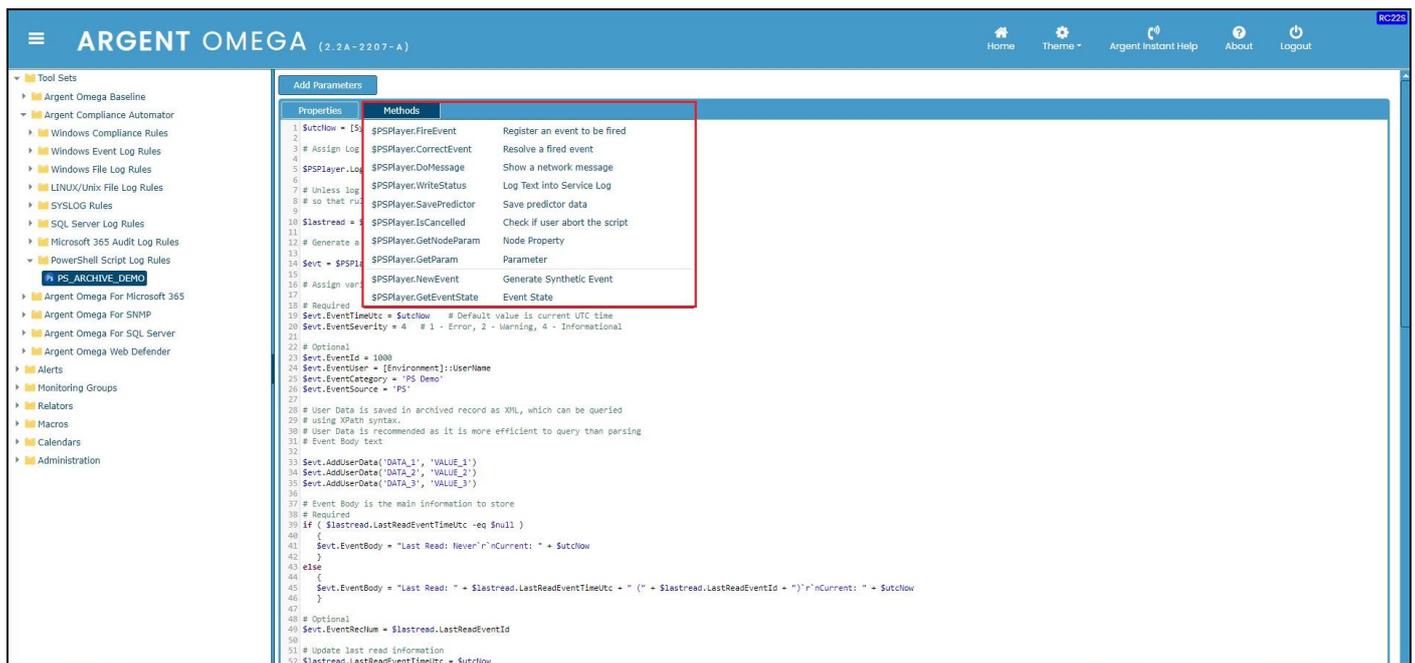
This Rule allows you to create custom PowerShell scripts to monitor Windows Event logs.

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



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

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



There is an option to define parameters for a PowerShell script:

Name	Type	Value
P1	Numeric	100

```
1 $UtcNow = [System.DateTime]:$UtcNow
2
3 # Assign Log Name which is saved as part of archived record. Default is Rule Name
4 $SPSPPlayer.LogName = "PS TestPSLog"
5
6 # Unless log data is stateless, last read state should be retrieved first
7 # so that rule logic can resume reading from last read position
8
9
10 $Lastread = $SPSPPlayer.GetEventState()
11
12 # Generate a synthetic event and put to the queue for archiving
13
14 $Evt = $SPSPPlayer.NewEvent()
15
16 # Assign various event properties
17
18 # Required
19 $Evt.EventTimeUtc = $UtcNow # Default value is current UTC time
20 $Evt.EventSeverity = 4 # 1 - Error, 2 - Warning, 4 - Informational
21
22 # Optional
23 $Evt.EventID = 1000
24 $Evt.EventUser = [Environment]:$UserName
25 $Evt.EventCategory = "PS Demo"
26 $Evt.EventSource = "PS"
27
28 # User Data is saved in archived record as XML, which can be queried
29 # using XPath syntax.
30 # User Data is recommended as it is more efficient to query than parsing
31 # Event Body text
32
```

The PowerShell script can use the defined parameters using the built-in method **GetParam**.

The **Rule Is Broken If Script Timeout** option can be used to trigger an alert if the script runs longer than the value defined in the **Timeout x Seconds** field.

The **Show PowerShell Script** option can be used to hide the script from view:

Timeout: 30 Seconds

Show PowerShell Script

Rule Is Broken If Script Timeout

Save Performance Data To The Argent Forecaster Using Data Store: (default)

Tag 1:

Tag 2:

Tag 3:

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

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

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

Post Event Only After Rule Is Broken 2 Or More Times

Reset Counter

After Event Is Post

After Event Is Answered

After The Actual Condition Is Corrected

Application:

Reference URL:

Console Comment:

Description: