

Argent Compliance Automator

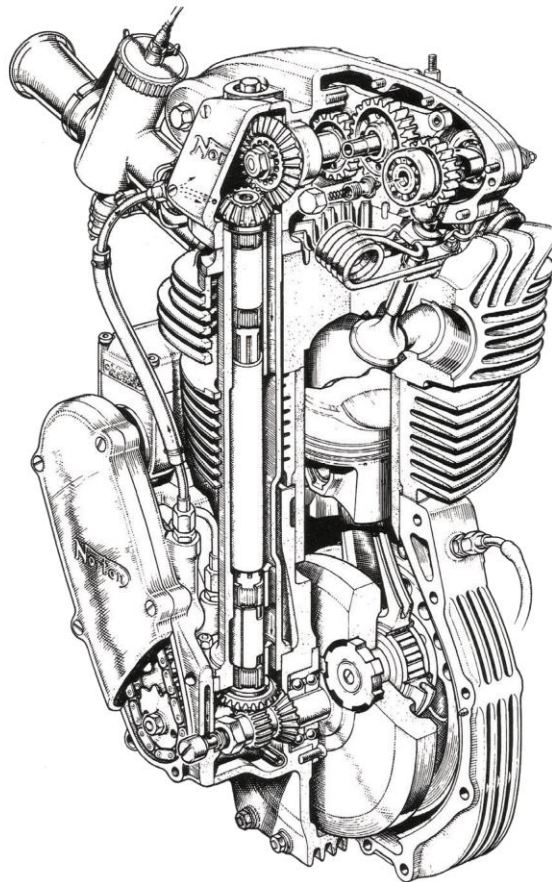


Table Of Contents

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.

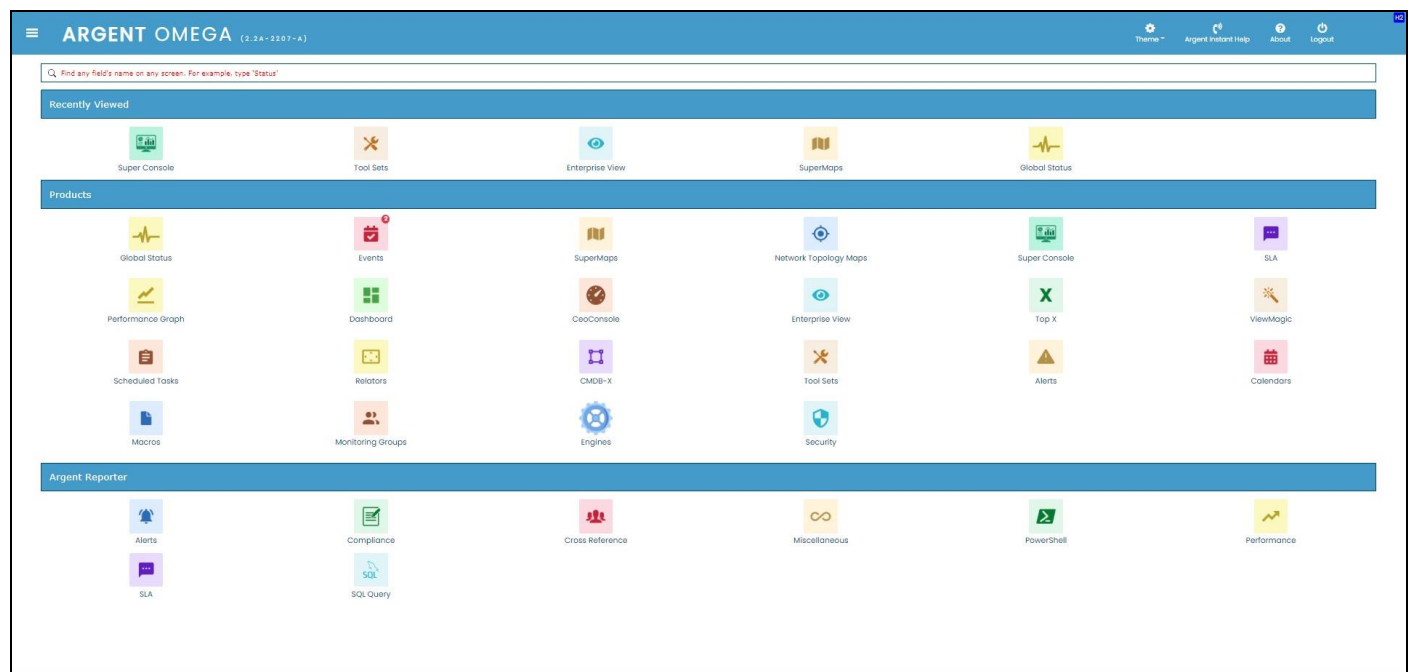
Demo accounts can be created in the **Argent Omega Security** section and are used for demonstration purposes. Demo accounts are read-only accounts and use Argent private authentication to login into Argent Omega. Demo accounts are usually only used temporarily for initial training and are limited to 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.

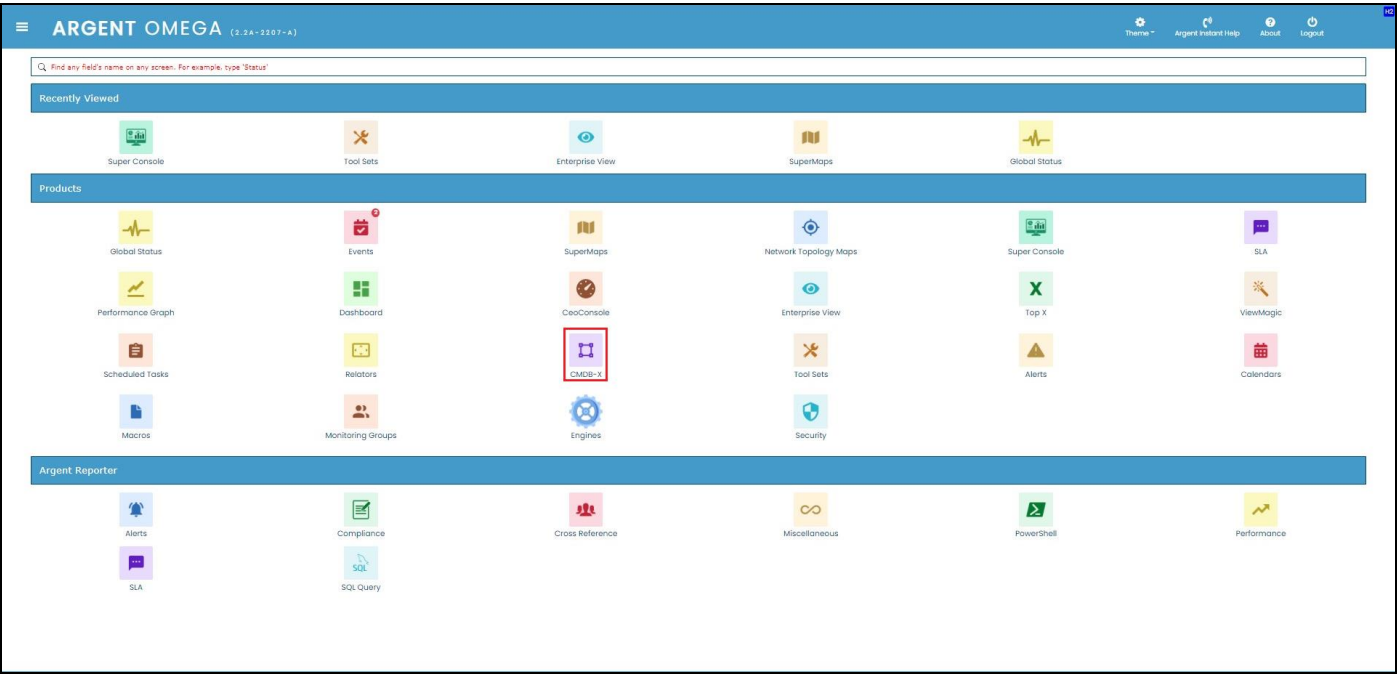
The Argent CMDB-X provides an easy and streamlined way to manage all critical servers and devices, as well as all server and device properties and licensing **from a single screen**. The Argent CMDB-X makes it easy for you to add multiple servers and devices in one batch – 11 or 77,000 -- license them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

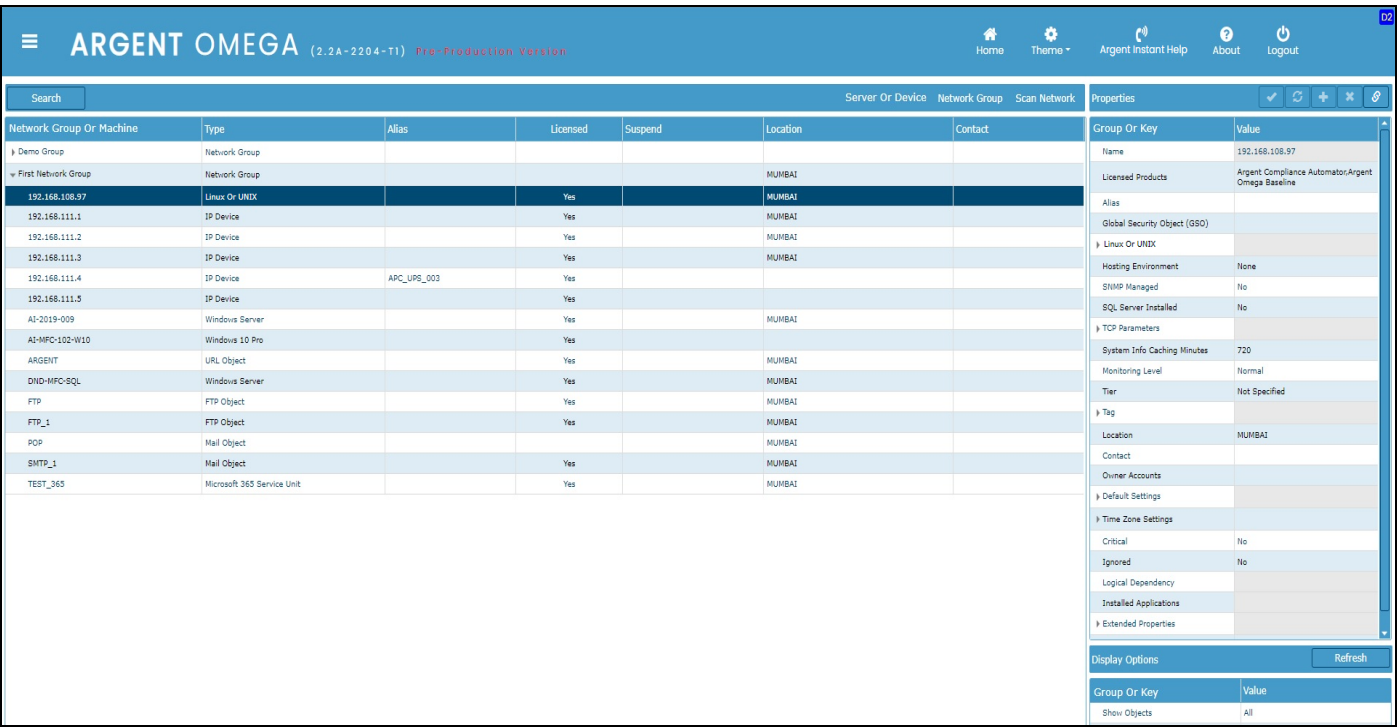
The Argent CMDB-X also has options to import from external Excel files.

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) interface. The main table lists network groups and machines. A right-click context menu is open over the 'AI-2019-003' row, showing options like 'Refresh', 'Suspend Monitoring', 'Reactivate', 'Save Changes', 'Undo', 'Add Property', 'Delete', 'Discover Neighbor Links', 'Wireless Clients', 'Set Critical Flag', 'Set Ignore Flag', 'Manually Add Server Or Device' (highlighted in red), 'Test Connectivity', 'Bulk Licensing', 'Export To Excel CSV', 'Backup CMDB-X Database', and 'Restore'.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
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-MPC-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					
AI-LAP01	Windows 10 Pro				MUMBAI	
AI-WEB	Windows 10 Pro					
AI3-TEST	Windows Storage Server 2016 Standard		Yes			
AI3-TEST-ONE	Windows Storage Server 2016 Standard		Yes			
AI3-TEST-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 'Manually Add An Entry' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

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

≡

ARGENT OMEGA

(2.2A-2204-T1) Not Production Version

Home

Theme

Argent Instant Help

About

Logout

Search

Server Or Device

Network Group

Scan Network

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
TEST10-2012R2	Windows Storage Server 2016 Standard		Yes			
TEST10-2012R2	Windows Server 2012 R2 Standard		Yes			
TEST10-2016	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_3SAMPLE...	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-OFF-365	Windows Server 2019 Standard		Yes			
WIN-2020-118-OL	Windows Server 2022 Standard Evaluation		Yes			
WIN-2022	Windows Server 2022 Standard Evaluation		Yes			
WIN-172705G4EHK	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			
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	

Properties

Group Or Key

Value

Name

AI-WIN-67

Licensed Products

Alias

Global Security Object (GSO)

Windows Server

Hosting Environment

None

SNMP Managed

No

SQL Server Installed

No

TCP Parameters

System Info Caching Minutes

720

Monitoring Level

Normal

Tier

Not Specified

Tag

Location

THIRUVANANTHAPURAM

Contact

Owner Accounts

Default Settings

Time Zone Settings

Same as Location

Critical

No

Ignored

No

Logical Dependency

Installed Applications

Extended Properties

Description

Display Options

Refresh

Group Or Key

Value

Show Objects

All

Network Group

*

Monitoring Group

*

Type

*

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

Manually Add An Entry

D2B

Name:

AI-LIN-23

Alias:

Domain:

VM Hosting Environment:

None

Type:

Linux

Network Group:

Demo Group

Location:

THIRUVANANTHAPURAM

OK

Cancel

Manually Add An Entry

D2B

Name:

AI-M365

Alias:

Domain:

VM Hosting Environment:

None

Type:

Microsoft 365 Service Unit

Network Group:

Demo Group

Location:

THIRUVANANTHAPURAM

OK

Cancel

≡

ARGENT OMEGA

(2.2A-2204-T1) - PRE-PRODUCTION VERSION

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-Q4-2	Windows Server 2008 R2 Standard		Yes			
TEST-VM-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_1SAMPLE_1_2SAMPLE_1_3SAMP...	Windows Server 2008 R2 Standard		Yes			
TRIV-NAS-001	Windows Server		Yes			
TRIV-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-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	

Group Or Key

Value

Contact

Description

Extended Properties

Location

Name

SHMP Parameters

Type

VMware Parameters

XenServer Parameters

Display Options

Refresh

Group Or Key

Value

Show Objects

Network Group

Monitoring Group

Type

All

*

*

*

Manually Add An Entry

D2B

Name:

192.168.108.92

Alias:

Domain:

VM Hosting Environment:

None

Type:

IP Address

Network Group:

Demo Group

Location:

THIRUVANANTHAPURAM

OK

Cancel

≡

ARGENT OMEGA (2.2A-2204-T1) Pre-Production Version

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-VM-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_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-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-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			
AZ-WIN-67	Windows Server				THIRUVANANTHAPURAM	
AZ-LIN-23	Linux				THIRUVANANTHAPURAM	
AZ-M365	Microsoft 365 Service Unit				THIRUVANANTHAPURAM	
First Network Group	Network Group				MUMBAI	

Group Or Key

Value

Contact

Description

Extended Properties

Location

Name

SNMP Parameters

Type

VMware Parameters

XenServer Parameters

Display Options

Refresh

Group Or Key

Value

Show Objects

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 shows 'ARGENT OMEGA (2.2A-2204-T1) Pre-Production Version' along with navigation links for Home, Theme, Argent Instant Help, About, and Logout. Below the header is a search bar and a table of servers. The table has columns for Network Group Or Machine, Type, Alias, Licensed, Suspend, Location, and Contact. A right-click context menu is open over the row with Alias 'WIN-2022', showing options like Refresh, Suspend Monitoring, Reconnect, Save Changes, Undo, Add Property, Delete, Discover Neighbor Links, Wireless Clients, Set Critical Flag, Set Ignore Flag, Manually Add Server Or Device, Test Connectivity, **Bulk Licensing** (highlighted with a red box), Export To Excel CSV, Backup CMDB-X Database, and Restore. To the right of the table is a 'Properties' panel for the selected 'WIN-2022' server, showing various configuration details like Group Or Key, Value, Description, and Location. At the bottom of the Properties panel is a 'Display Options' section with a 'Refresh' button.

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-VM-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-OL	Windows Server 2022 Standard Evaluation					
WIN-2022	Windows Server 2022 Standard Evaluation					
WIN-1727G504EHR	Windows Server 2012 R2 Standard					
WIN-MFC-TEST	Windows Server 2012 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			
A2-WIN-47	Windows Server				THORUVANANTHAPURAM	
A2-LIN-23	Linux				THORUVANANTHAPURAM	
A2-MFC	Windows Server 2012 R2 Standard				THORUVANANTHAPURAM	

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

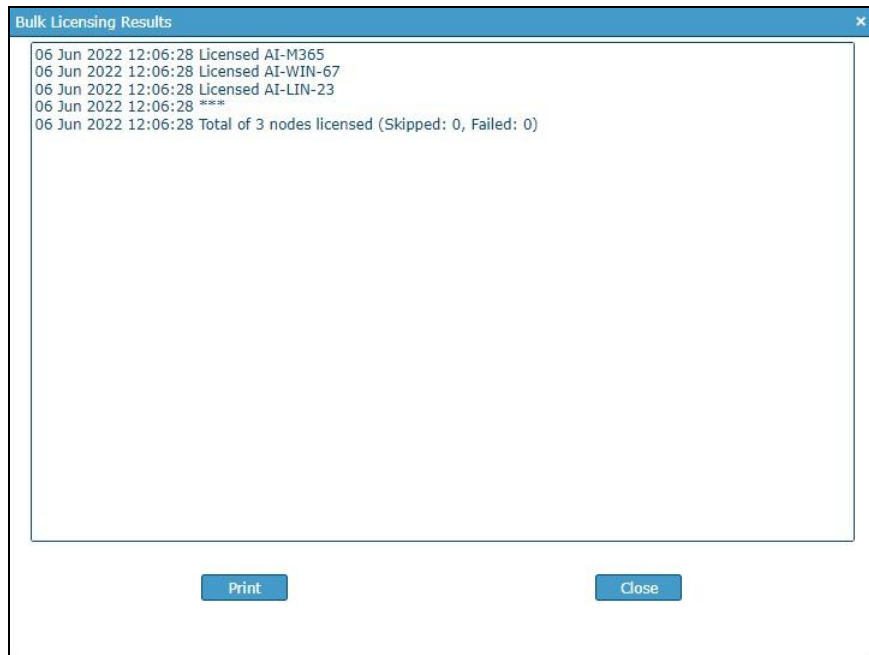
☒ AI-LIN-23

☒ AI-M365

☐ Remove License For Selected Nodes

OK

Cancel



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	<p>Options for setting TCP parameters for the server or device.</p> <p>The options are as follows:</p> <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	<p>Location of the server or device</p> <p>(This information is used to determine the device location on Google Maps.)</p>
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:

ARGENT OMEGA (2.2A-2204-T1) - PRE-PRODUCTION VERSION

HomeThemeArgent Instant HelpAboutLogout

SearchServer Or DeviceNetwork GroupScan NetworkProperties

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			

Group Or KeyValue

Critical

No

Global Security Object (GSO)

Hosting Environment

None

Ignored

No

Installed Applications

Licensed Products

Argent Omega Baseline

Location

Logical Dependency

Monitoring Level

Low

Name

WIN2008-TEST1, WIN2008-TEST2, WIN2008-TEST3, WIN2016-TEST2, WIN2016-TEST3

Preferred Generators

System Info Caching Minutes

Never

Tag

TCP Parameters

Retry

0

Timeout

Default

Tier

Not Specified

Time Zone Settings

Same as Location

Windows Server

64-bit OS

Yes

Authentication

Cluster Name

Domain

Display Options

Refresh

Group Or KeyValue

Show ObjectsAll

Network Group*

Microsoft 365 Service Unit Credentials

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

The screenshot displays the ARGENT OMEGA (2.2A-2204-T1) interface. The main table lists various network devices and their properties. A specific entry, 'TEST_365', is highlighted as a 'Microsoft 365 Service Unit'. To the right, the 'Properties' panel for this unit is expanded, showing configuration details for the 'Microsoft 365 Service Unit'.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group					
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-MPC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes			
192.168.111.5	IP Device		Yes			
AS-2019-009	Windows Server		Yes		MUMBAI	
AI-MPC-102-W10	Windows 10 Pro		Yes			

Properties Panel for Microsoft 365 Service Unit:


- Group Or Key: Microsoft 365 Service Unit
- Administrator: test_a@argsoftdev.com
- Application Id: [Redacted]
- Certificate Thumbprint: [Redacted]
- Directory Or Tenant Id: [Redacted]
- Licensed Units: [Redacted]
- Organization: [Redacted]
- SharePoint Url: [Redacted]
- SKU: [Redacted]
- Monitoring Level: Normal
- Name: TEST_365
- Owner Accounts: [Redacted]
- System Info Caching Minutes: 720
- Tag: [Redacted]
- Tier: 6
- Time Zone Settings: Same as Location

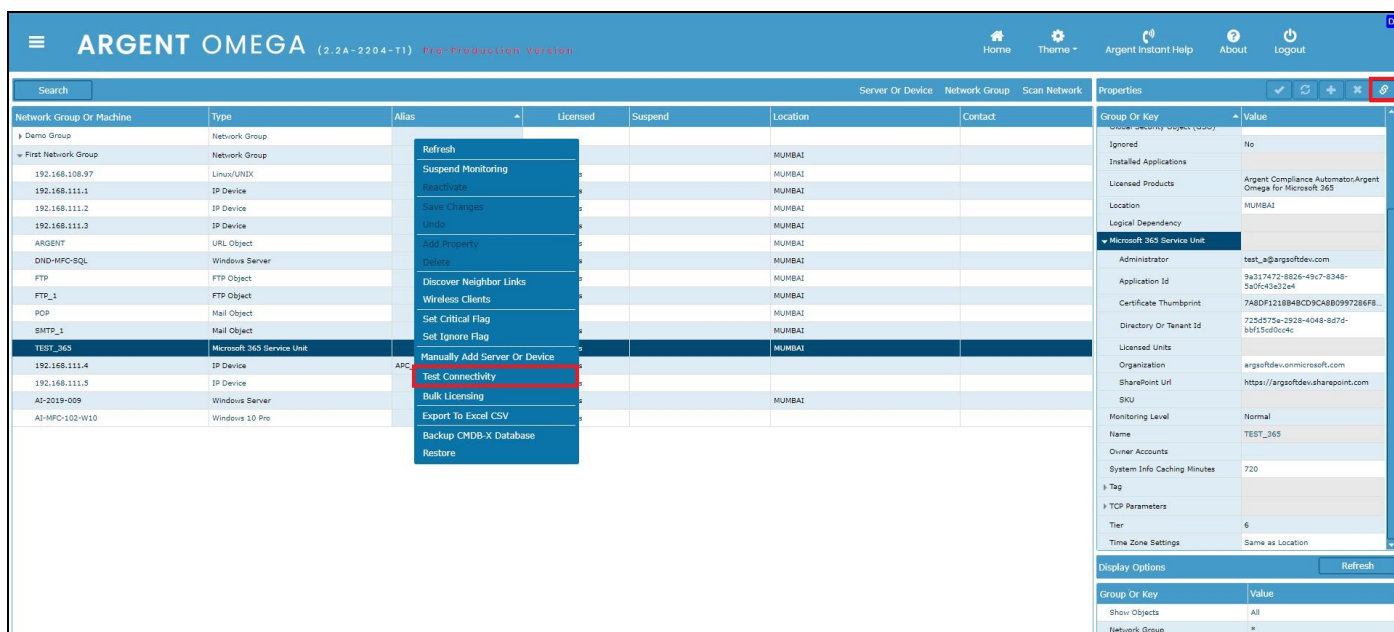
Test Connectivity

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:



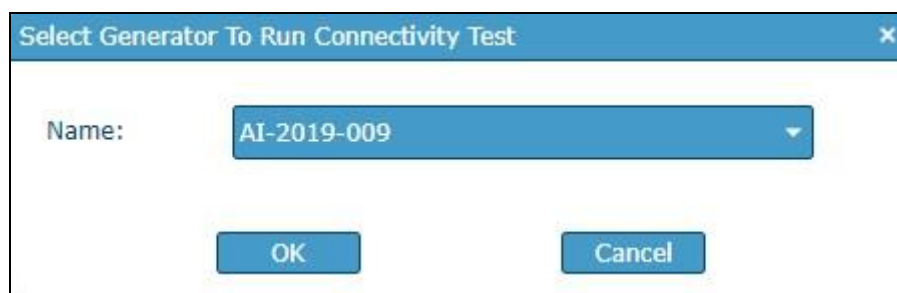
The screenshot shows the ARGENT OMEGA application interface. The main table lists various network groups and machines. A right-click context menu is open over the 'TEST_365' entry, with 'Test Connectivity' highlighted in red. The 'Properties' panel on the right shows details for the selected 'Microsoft 365 Service Unit'.

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

Properties Panel (Microsoft 365 Service Unit):

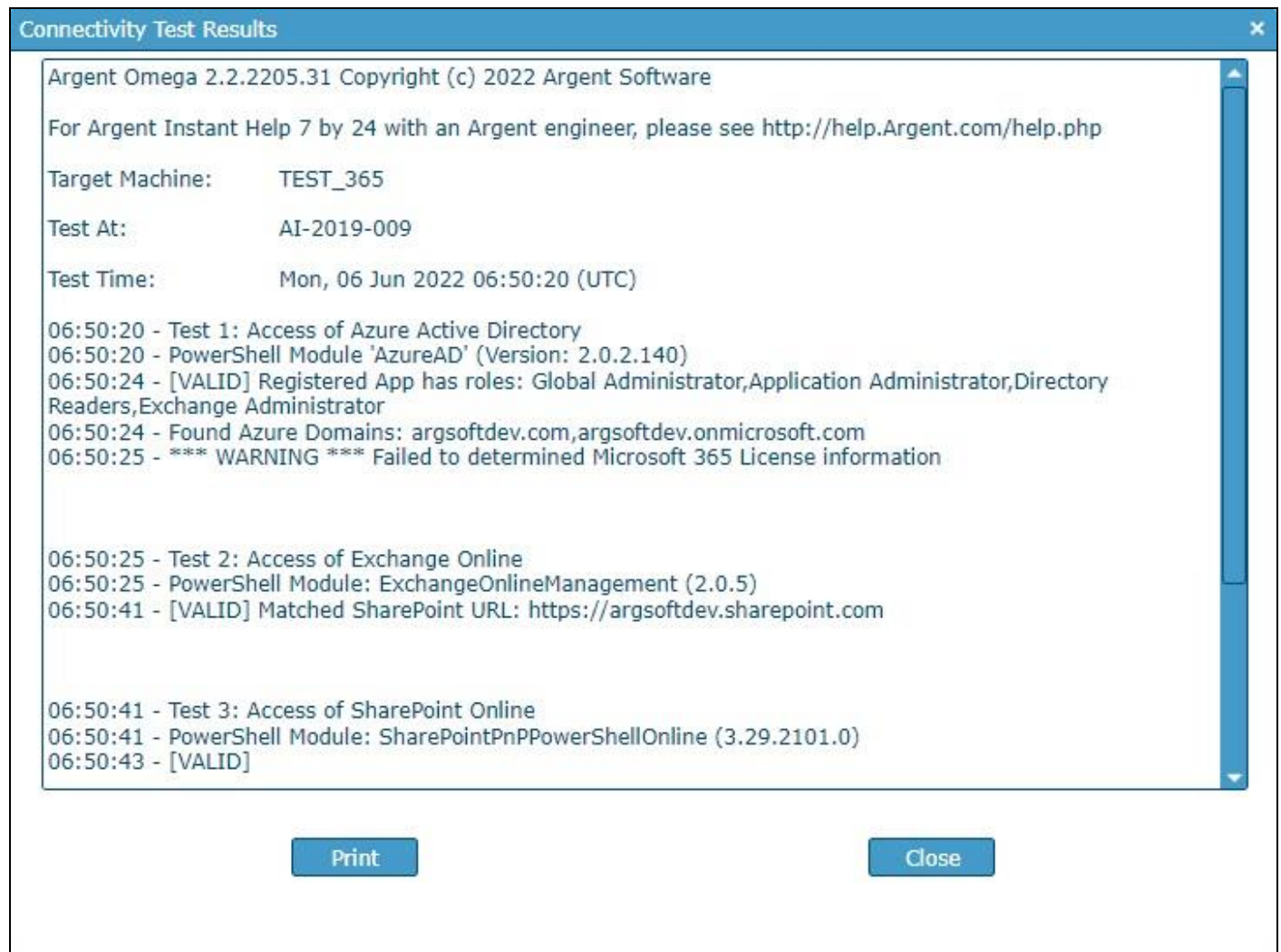
- Group Or Key: Microsoft 365 Service Unit
- Administrator: test_a@argsoftdev.com
- Application Id: 9a317472-8826-49c7-8348-5a0fc43e32e4
- Certificate Thumbprint: 748DF1218B4BCD9CA8B0997286F8
- Directory Or Tenant Id: 7252575e-2928-4048-8d7d-bbf15a00c4c0
- Licensed Units: argsoftdev.onmicrosoft.com
- Organization: argsoftdev.onmicrosoft.com
- SharePoint Url: https://argsoftdev.sharepoint.com
- 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

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



The dialog box is titled 'Select Generator To Run Connectivity Test'. It contains a 'Name:' label followed by a dropdown menu showing 'AI-2019-009'. At the bottom, there are 'OK' and 'Cancel' buttons.

The Results are shown:



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.

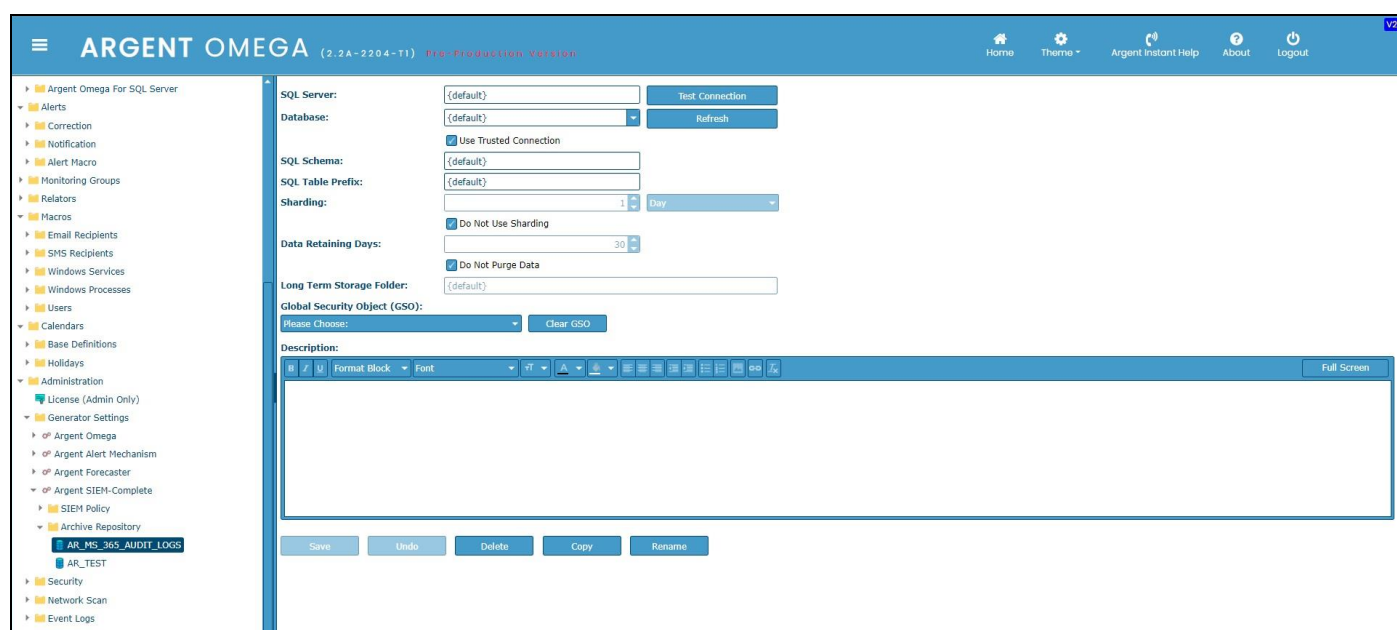
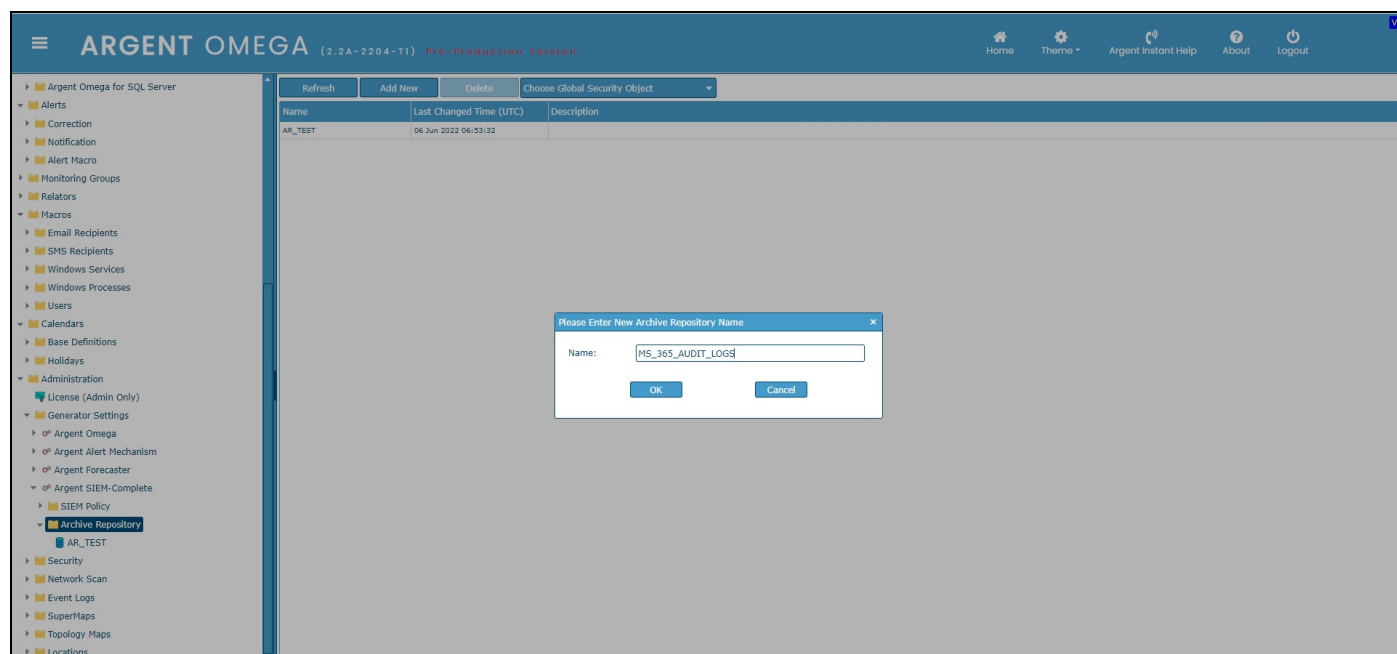
These logs can be very useful for security personnel.

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.

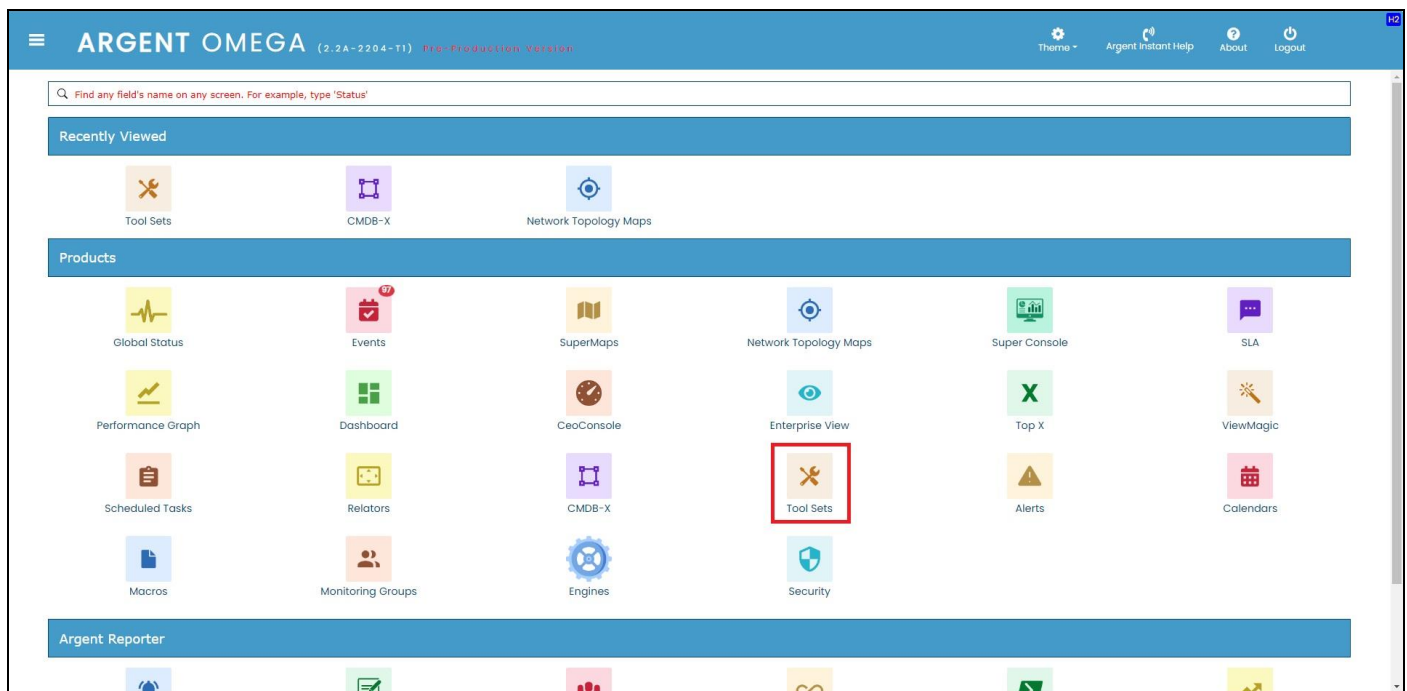
Uncheck the **Do Not Purge Data** option to purge the data after the days specified in **Data Retaining Days** field.

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

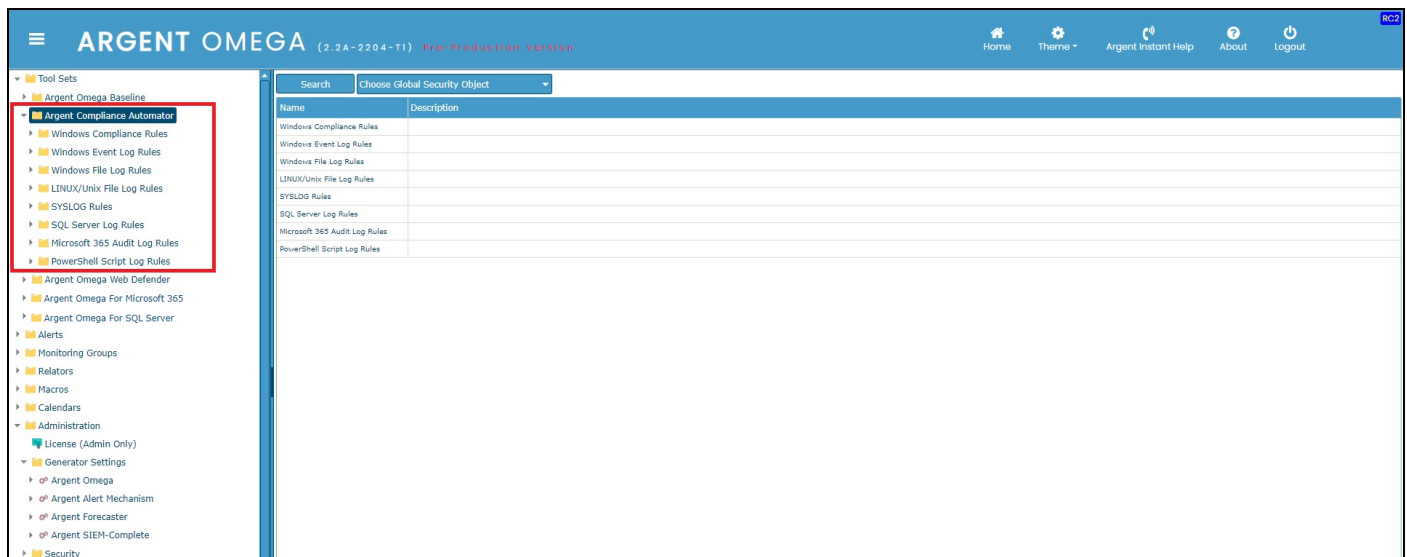
The event data retrieved by the Rule will be archived in the configured Archive Repository.

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 (2.2A-2207-A) configuration interface. The sidebar on the left shows a tree view of tool sets and alerts, with 'WCP_UNIVERSAL_COMPLIANCE_ARCHIVE' selected. The main configuration area for this rule includes the following settings:

- Read Windows Security Log With Method:** Automatically Determined
- Archive Repository:** {default}
- Skip Security Log Records Over:** 24 Hours
- In Addition To Compliance Audit Log, Archive Windows Security Log Matching Following Criteria:**
 - ☐ Event ID: * (Include Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Criteria, Type A Minus Sign First. For Example 1,3,5-99,-76)
 - ☐ Event User: *
 - ☐ Event Category: *
 - ☐ Event Source: *
 - ☐ Match Case
 - ☐ Match Whole Word
 - ☐ Match Regular Expression
- ☒ Include Audit Failure Events
- ☐ Read User Data From Custom XPath: *
- ☐ Alert On Potential Data Loss
- ☐ Alert If Failed To Open Windows Event Log
- ☐ 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

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.

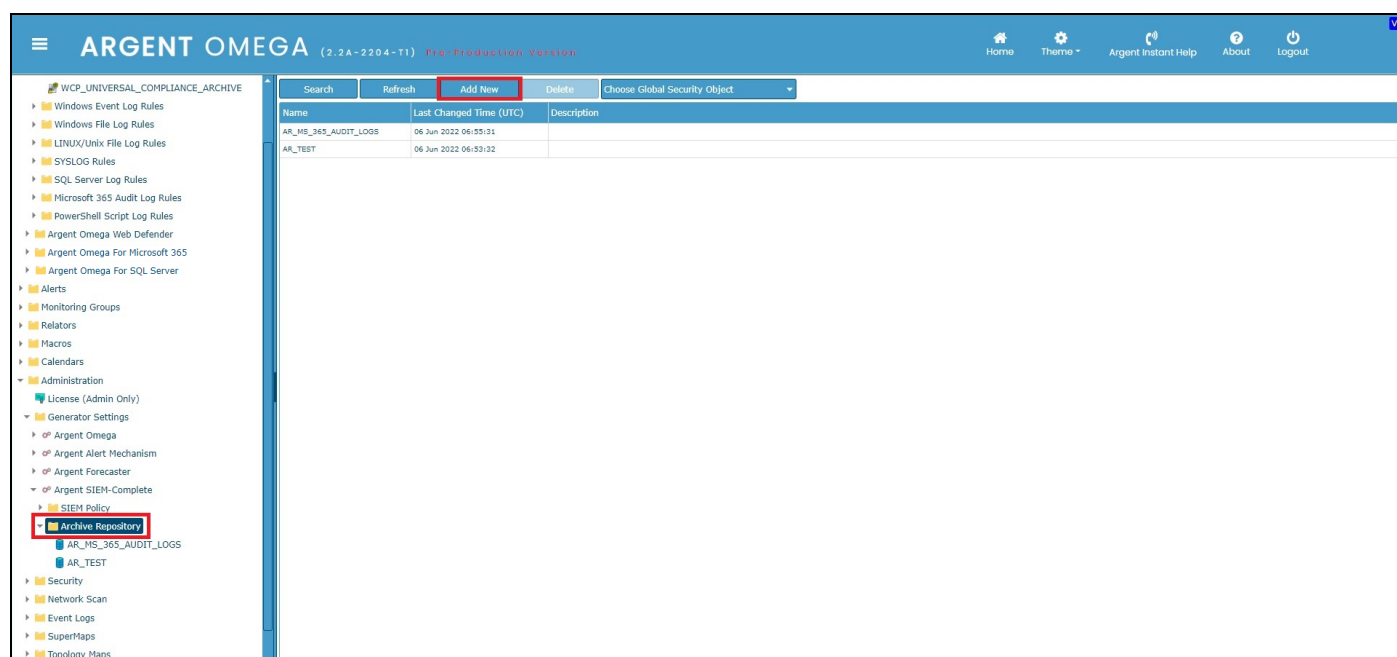
Argent Omega uses the following Event read methods:

- 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 screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. On the left is a sidebar with a tree view of tool sets, including 'WCP_UNIVERSAL_COMPLIANCE_ARCHIVE'. The main panel is titled 'Read Windows Security Log With Method: Automatically Determined'. It contains several configuration fields: 'Archive Repository' is set to '{default}'; 'Skip Security Log Records Over' is set to '24' hours; 'In Addition To Compliance Audit Log, Archive Windows Security Log Matching Following Criteria' includes checkboxes for 'Event ID', 'Event User', 'Event Category', and 'Event Source', each with a corresponding input field. Below these are checkboxes for 'Match Case', 'Match Whole Word', and 'Match Regular Expression'. There are also checkboxes for 'Include Audit Failure Events', 'Read User Data From Custom XPath', 'Alert On Potential Data Loss', and 'Alert If Failed To Open Windows Event Log'. At the bottom, there are fields for 'Tag 1', 'Tag 2', and 'Tag 3', and a 'Reset Counter' section with radio buttons for 'After Event Is Post' and 'After Event Is Answered'.

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

This screenshot is similar to the one above, but the 'In Addition To Compliance Audit Log, Archive Windows Security Log Matching Following Criteria' section is highlighted with a red box. This section contains checkboxes for 'Event ID', 'Event User', 'Event Category', and 'Event Source', each with a corresponding input field. Below these are checkboxes for 'Match Case', 'Match Whole Word', and 'Match Regular Expression'. There are also checkboxes for 'Include Audit Failure Events', 'Read User Data From Custom XPath', 'Alert On Potential Data Loss', and 'Alert If Failed To Open Windows Event Log'. At the bottom, there are fields for 'Tag 1', 'Tag 2', and 'Tag 3', and a 'Reset Counter' section with radio buttons for 'After Event Is Post' and 'After Event Is Answered'.

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.

ARGENT OMEGA (2.2A-2207-A)

Home Theme Argent Instant Help About Logout

Tool Sets

- Argent Omega Baseline
- Argent Compliance Automator
- Windows Compliance Rules
 - WCP_UNIVERSAL_COMPLIANCE_ARCHIVE**
 - 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
 - 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)

Read Windows Security Log With Method: Automatically Determined

Archive Repository: (default)

Skip Security Log Records Over: 24 Hours

In Addition To Compliance Audit Log, Archive Windows Security Log Matching Following Criteria

☐ Event ID: *

☐ Event User: *

☐ Event Category: *

☐ Event Source: *

☐ Match Case

☐ Match Whole Word

☐ Match Regular Expression

☒ Include Audit Failure Events

☒ Read User Data From Custom XPath *

☐ Alert On Potential Data Loss

☐ Alert If Failed To Open Windows Event Log

☐ 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

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:

The screenshot displays the ARGENT OMEGA (2.2A-2207-A) interface for configuring an Event Log Rule. The left sidebar shows a tree view of tool sets, with 'EVT_APPLICATION_ERROR' selected under 'Windows Event Log Rules'. The main configuration area includes the following sections:

- Event Log Name:** Application (with a Reload button)
- Event Severity:** Critical/Error
- Event ID:** 1-99999
- Read Windows Event Log With Method:** Automatically Determined
- Rule View:** Simple
- Ignore Event Log Records Over:** 30 Minutes
- Fire Event With Format:** System Default (selected), Individual, Combined With Latest Event Message, Combined With Full Event Message
- Additional Event Log Filtering Criteria:**
 - Event User: *
 - Event Category: *
 - Event Source: *
 - Custom User Data: Using XPath (checkbox), Match Case (checkbox), Match Whole Word (checkbox), Match Regular Expression (checkbox)
- 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** (checkbox)
- Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)** (checkbox)
- Retrieve Performance Metric From XPath:**
 - Performance Object Name: (input field) Use As XPath (checkbox)
 - Counter Name: (input field) Use As XPath (checkbox)
 - Instance Name: (input field) Use As XPath (checkbox)
 - Machine Name: {default} Use As XPath (checkbox)
- Correct Event If Seeing Event Id Of Same Source:** (checkbox)

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

Rules:

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**
 - EVT_APPLICATION_ERROR**
 - EVT_AUDIT_FAILURE
 - EVT_SYSTEM_ERROR
- Windows File Log Rules
- 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

Event Log Name: Application [Reload]

Event Severity: Critical/Error

Event ID: 1-99999

Include Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Criteria, Type A Minus Sign First. For Example 1,3,5-99,-76

Read Windows Event Log With Method: Automatically Determined

Rule View: Simple

Ignore Event Log Records Over: 30 Minutes

Fire Event With Format: ☒ System Default ☐ Individual ☐ Combined With Latest Event Message ☐ Combined With Full Event Message

Additional Event Log Filtering Criteria

☐ Event User: *

☐ Event Category: *

☐ Event Source: *

☐ Custom User Data: Using XPath

☐ Match Case

☐ Match Whole Word

☐ Match Regular Expression

☐ 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

☐ Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)

☐ Retrieve Performance Metric From XPath:

Performance Object Name: Use As XPath

Counter Name: Use As XPath

Instance Name: Use As XPath

Machine Name: {default} Use As XPath

☐ Correct Event If Seeing Event Id Of Same Source:

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

Reload button:

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**
 - EVT_APPLICATION_ERROR**
 - EVT_AUDIT_FAILURE
 - EVT_SYSTEM_ERROR
- Windows File Log Rules
- 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

Event Log Name: Application [Reload]

Event Severity: Critical/Error

Event ID: 1-99999

Include Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Criteria, Type A Minus Sign First. For Example 1,3,5-99,-76

Read Windows Event Log With Method: Automatically Determined

Rule View: Simple

Ignore Event Log Records Over: 30 Minutes

Fire Event With Format: ☒ System Default ☐ Individual ☐ Combined With Latest Event Message ☐ Combined With Full Event Message

Additional Event Log Filtering Criteria

☐ Event User: *

☐ Event Category: *

☐ Event Source: *

☐ Custom User Data: Using XPath

☐ Match Case

☐ Match Whole Word

☐ Match Regular Expression

☐ 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

☐ Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)

☐ Retrieve Performance Metric From XPath:

Performance Object Name: Use As XPath

Counter Name: Use As XPath

Instance Name: Use As XPath

Machine Name: {default} Use As XPath

☐ Correct Event If Seeing Event Id Of Same Source:

Select A Windows Machine

Remote Machine: [Dropdown]

☒ Use PS Remoting

Execute On: {default}

OK Cancel

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.

ARGENT OMEGA (2.2A-2207-A)

Event Log Name: Application

Event Severity: Critical/Error

Event ID: 1-99999

Read Windows Event Log With Method: Automatically Determined

Rule View: Simple

Ignore Event Log Records Over: 30 Minutes

Fire Event With Format: System Default

Additional Event Log Filtering Criteria

Event User: *

Event Category: *

Event Source: *

Custom User Data: Using XPath

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

Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)

Retrieve Performance Metric From XPath:

Performance Object Name: Use As XPath

Counter Name: Use As XPath

Instance Name: Use As XPath

Machine Name: {default} Use As XPath

Correct Event If Seeing Event Id Of Same Source:

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'

ARGENT OMEGA (2.2A-2207-A)

Event Log Name: Application

Event Severity: Critical/Error

Event ID: 1-99999

Read Windows Event Log With Method: Automatically Determined

Rule View: Simple

Ignore Event Log Records Over: 30 Minutes

Fire Event With Format: System Default

Additional Event Log Filtering Criteria

Event User: *

Event Category: *

Event Source: *

Custom User Data: Using XPath

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

Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)

Retrieve Performance Metric From XPath:

Performance Object Name: Use As XPath

Counter Name: Use As XPath

Instance Name: Use As XPath

Machine Name: {default} Use As XPath

Correct Event If Seeing Event Id Of Same Source:

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)

The screenshot displays the Argent Omega web interface (version 2.2 A - 2207 - A) with a sidebar menu on the left and a main configuration panel on the right. The sidebar menu includes categories like Tool Sets, Alerts, Macros, and Calendars. The main panel is titled "Read Windows Event Log With Method" and contains several configuration options:

- Event Log Name:** Application (dropdown)
- Event Severity:** Critical, Error (dropdown)
- Event ID:** 1-99999 (text input)
- Read Windows Event Log With Method:** Automatically Determined (dropdown, highlighted with a red box)
- Rule View:** Simple (dropdown)
- Ignore Event Log Records Over:** 30 Minutes (text input)
- Fire Event With Format:** System Default (radio button selected), Individual, Combined With Latest Event Message, Combined With Full Event Message
- Additional Event Log Filtering Criteria:**
 - ☐ Event User: *
 - ☐ Event Category: *
 - ☐ Event Source: *
 - ☐ Custom User Data: Using XPath
 - ☐ Match Case
 - ☐ Match Whole Word
 - ☐ Match Regular Expression
- 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
- ☐ Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)
- ☐ Retrieve Performance Metric From XPath:
 - Performance Object Name: Use As XPath
 - Counter Name: Use As XPath
 - Instance Name: Use As XPath
 - Machine Name: {default} Use As XPath
- ☐ Correct Event If Seeing Event Id Of Same Source:

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:

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) configuration interface. The left sidebar contains a tree view of tool sets, including 'Tool Sets', 'Argent Omega Baseline', 'Argent Compliance Automator', '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', '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', and 'Holidays'. The main configuration area is titled 'Event Log Name: Application' and 'Event Severity: Critical/Error'. The 'Event ID' is set to '1-99999'. The 'Read Windows Event Log With Method' is 'Automatically Determined'. The 'Rule View' is 'Simple'. The 'Ignore Event Log Records Over' field is highlighted with a red box and set to '30 Minutes'. The 'Fire Event With Format' section is also highlighted with a red box, showing four radio button options: 'System Default' (selected), 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'. Below this is the 'Additional Event Log Filtering Criteria' section, which includes fields for 'Event User', 'Event Category', 'Event Source', and 'Custom User Data'. There are also checkboxes for 'Match Case', 'Match Whole Word', and 'Match Regular Expression'. At the bottom, there are fields for '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', 'Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)', 'Retrieve Performance Metric From XPath', 'Performance Object Name', 'Counter Name', 'Instance Name', 'Machine Name', and 'Correct Event If Seeing Event Id Of Same Source'.

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

This screenshot is identical to the one above, showing the ARGENT OMEGA (2.2A-2207-A) configuration interface. The 'Fire Event With Format' section is highlighted with a red box, showing four radio button options: 'System Default' (selected), 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'. The 'Ignore Event Log Records Over' field is also highlighted with a red box and set to '30 Minutes'. The rest of the interface, including the sidebar and other configuration fields, is the same as in the previous screenshot.

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

The screenshot displays the ARGENT OMEGA (2.2A-2207-A) web interface. On the left is a navigation tree with categories like Tool Sets, Windows Event Log Rules, and Alerts. The main panel is titled 'Event Log Name: Application' and 'Event Severity: Critical_Error'. The 'Rule View' is set to 'Simple' and is highlighted with a red box. Other settings include 'Event ID: 1-99999', 'Read Windows Event Log With Method: Automatically Determined', 'Ignore Event Log Records Over: 30 Minutes', and 'Fire Event With Format: System Default'. Below these are sections for 'Additional Event Log Filtering Criteria' (Event User, Event Category, Event Source, Custom User Data) and 'Events In Time Range' (00:00:00 - 23:59:59). The interface also includes a 'Reload' button and a top navigation bar with links for Home, Theme, Argent Instant Help, About, and Logout.

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

The screenshot displays the ARGENT OMEGA (2.2A-2204-T1) web interface. The 'Rule View' is set to 'Advanced' and is highlighted with a red box. The 'Advanced Event Filter String' section is also highlighted with a red box, showing a large text area for entering XPath or PowerShell expressions. The 'Event Log Name' is 'Application' and 'Event Severity' is 'Critical_Error'. The 'Event ID' is '1-99999'. The 'Read Windows Event Log With Method' is 'Automatically Determined'. The 'Ignore Event Log Records Over' is '30 Minutes'. The 'Fire Event With Format' is 'System Default'. The 'Advanced Event Filter String' section includes a text area for the filter string. Below this are sections for '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', 'Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)', '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', and 'Save Archive Data Only'. The interface also includes a 'Reload' button and a top navigation bar with links for Home, Theme, Argent Instant Help, About, and Logout.

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 screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The left sidebar lists various tool sets, including 'Event Application Error'. The main configuration area is titled 'Additional Event Log Filtering Criteria'. It includes the following fields and options:

- Event Log Name:** Application
- Event Severity:** Critical, Error
- Event ID:** 1-99999
- Read Windows Event Log With Method:** Automatically Determined
- Rule View:** Simple
- Ignore Event Log Records Over:** 30 Minutes
- Fire Event With Format:** System Default, Individual, Combined With Latest Event Message, Combined With Full Event Message
- Additional Event Log Filtering Criteria:**
 - ☐ Event User: *
 - ☐ Event Category: *
 - ☐ Event Source: *
 - ☐ Custom User Data: Using XPath
 - ☐ Match Case
 - ☐ Match Whole Word
 - ☐ Match Regular Expression
- 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
- ☐ Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)
- ☐ Retrieve Performance Metric From XPath: Performance Object Name: Use As XPath
- ☐ Counter Name: Use As XPath
- ☐ Instance Name: Use As XPath
- ☐ Machine Name: (default) Use As XPath
- ☐ Correct Event If Seeing Event Id Of Same Source:

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

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The left sidebar lists various tool sets, including 'Event Application Error'. The main configuration area is titled 'Additional Event Log Filtering Criteria'. It includes the following fields and options:

- Event User:** *
- Event Category:** *
- Event Source:** *
- Custom User Data:** Using XPath
- ☐ Match Case
- ☐ Match Whole Word
- ☐ Match Regular Expression
- 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
- ☐ Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)
- ☐ Retrieve Performance Metric From XPath: Performance Object Name: Use As XPath
- ☐ Counter Name: Use As XPath
- ☐ Instance Name: Use As XPath
- ☐ Machine Name: (default) Use As XPath
- ☐ Correct Event If Seeing Event Id Of Same Source:
- ☐ Save Matching Events To Archive Repository: (default)
- ☐ Save Archive Data Only
- ☐ Alert If Failed To Open Windows Event Log
- ☐ 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)

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 screenshot shows the ARGENT OMEGA configuration interface. On the left is a sidebar with a tree view of tool sets and alerts. The main panel is titled 'Additional Event Log Filtering Criteria'. It contains several sections:

- Event Filtering:** Fields for Event User, Event Category, Event Source, and Custom User Data with checkboxes for Match Case, Match Whole Word, and Match Regular Expression.
- Time Range:** A time range selector set to 00:00:00 - 23:59:59.
- Alerting:** Checkboxes for '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)'.
- Performance Metrics:** Fields for Performance Object Name, Counter Name, Instance Name, and Machine Name, each with a 'Use As XPath' checkbox.
- Event ID Matching:** A checkbox 'Correct Event If Seeing Event ID of Same Source' is checked and highlighted with a red box.
- Archiving:** A dropdown 'Save Matching Events To Archive Repository' is set to '(default)'.
- Alerts:** A checkbox 'Save Archive Data Only' is present.
- Other Options:** Checkboxes for 'Alert If Failed To Open Windows Event Log', 'Save Performance Data To The Argent Forecaster Using Data Store: (default)', and 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)'.

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:

This screenshot is similar to the previous one, showing the same ARGENT OMEGA configuration interface. In this view, the 'Save Matching Events To Archive Repository' dropdown is highlighted with a red box, and the 'Save Archive Data Only' checkbox is also checked and highlighted with a red box. The other configuration options remain the same as in the previous screenshot.

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.

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
 - EVT_APPLICATION_ERROR**
 - EVT_AUDIT_FAILURE
 - EVT_SYSTEM_ERROR
 - Windows File Log Rules
 - 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

Additional Event Log Filtering Criteria

☐ Event User: *

☐ Event Category: *

☐ Event Source: *

☐ Custom User Data: Using XPath

☐ Match Case

☐ Match Whole Word

☐ Match Regular Expression

☐ 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

☐ Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)

☐ Retrieve Performance Metric From XPath:

Performance Object Name: Use As XPath

Counter Name: Use As XPath

Instance Name: Use As XPath

Machine Name: {default} Use As XPath

☐ Correct Event If Seeing Event Id Of Same Source:

☒ Save Matching Events To Archive Repository: {default}

☐ Save Archive Data Only

☒ **Alert If Failed To Open Windows Event Log**

☐ 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)

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:

ARGENT OMEGA (2.2A-2207-A)

Log File Path: C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG

File Name Is Regular Expression

Use Yesterday's Date For Date Or Time Variables Used In File Path

Bias Date Or Time Variables Used In File Path By: 0 Hours

Read Only Last: 10 Megabytes

Scan Option: The Latest File Only

Date Or Time Format: yyyy-MM-dd HH:mm:ss.nn

Ignore File Log Records Over: 30 Minutes

Fire Event With Format: System Default

Use Advanced Rule Definition: Contains

Rule Is Broken If Log Line: Contains

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: Alert Message Include

Correct Condition If Log Line: Contains

Save To Archive Repository: Archive All Log Lines

Archive If Log Line: Contains

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:

ARGENT OMEGA (2.2A-2207-A)

Log File Path: C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG

View Log File

File Name Is Regular Expression

Use Yesterday's Date For Date Or Time Variables Used In File Path

Bias Date Or Time Variables Used In File Path By: 0 Hours

Read Only Last: 10 Megabytes

Scan Option: The Latest File Only

Date Or Time Format: yyyy-MM-dd HH:mm:ss.nn

Ignore File Log Records Over: 30 Minutes

Fire Event With Format: System Default

Use Advanced Rule Definition: Contains

Rule Is Broken If Log Line: Contains

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: Alert Message Include

Correct Condition If Log Line: Contains

Save To Archive Repository: Archive All Log Lines

Archive If Log Line: Contains

```
localhost:6100/app/OmegaSystemInfo/DownloadTestLog?log=C:\34%\SCProgram%\20Files%\SCMicrosoft%\20SQL%\20Server%\SCMSSQL13.MSSQLSERVER%\SCMSSQL%\SQLlog%\SCERRORLOG&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
2022-03-09 10:53:01.67 Server (c) Microsoft Corporation.
2022-03-09 10:53:01.67 Server All rights reserved.
2022-03-09 10:53:01.67 Server Server process ID is 6052.
2022-03-09 10:53:01.67 Server System Manufacturer: 'LENOVO', System Model: '10132'.
2022-03-09 10:53:01.67 Server Authentication mode is MIXED.
2022-03-09 10:53:01.67 Server Logging SQL Server messages in file 'c:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Log\ERRORLOG'.
2022-03-09 10:53:01.68 Server The service account is 'NT Service\MSSQLSERVER'. This is an informational message; no user action is required.
2022-03-09 10:53:01.68 Server 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
2022-03-09 10:53:01.68 Server Command Line Startup Parameters:
-r "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 only. No user action is required.
2022-03-09 10:53:01.71 Server Detected 8106 MB of RAM. This is an informational message; no user action is required.
2022-03-09 10:53:01.71 Server Using conventional memory in the memory manager.
2022-03-09 10:53:02.24 Server Default collation: SQL_Latin1_General_CP1_CI_AS (us_english 1033)
2022-03-09 10:53:03.22 Server Buffer pool extension is already disabled. No action is necessary.
2022-03-09 10:53:03.44 Server InitializeExternalUserGroupSid failed. Implied authentication will be disabled.
2022-03-09 10:53:04.44 Server Implied authentication manager initialization failed. Implied authentication will be disabled.
2022-03-09 10:53:05.91 Server The maximum number of dedicated administrator connections for this instance is '1'.
2022-03-09 10:53:05.95 Server This instance of SQL Server last reported using a process ID of 5380 at 3/9/2022 10:52:25 AM (local). This is an informational message only; no user action is required.
2022-03-09 10:53:05.98 Server Node configuration: node 0: CPU mask: 0x000000000000000f:0 Active CPU mask: 0x000000000000000f:0. This message provides a description of the NUMA configuration for this computer. This is an informational message only. No user action is required.
2022-03-09 10:53:04.00 Server 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.
2022-03-09 10:53:04.03 Server 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.
2022-03-09 10:53:04.08 Server 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.
2022-03-09 10:53:04.22 spid5s Starting up database 'master'.
2022-03-09 10:53:04.43 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [1] 'master'. XTP Engine version is 0.0.
2022-03-09 10:53:04.61 Server CLR version v4.0.30319 loaded.
2022-03-09 10:53:05.22 spid5s SQL Server Audit is starting the audits. This is an informational message. No user action is required.
2022-03-09 10:53:05.22 spid5s SQL Server Audit has started the audits. This is an informational message. No user action is required.
2022-03-09 10:53:05.34 Server Common Language runtime (CLR) functionality initialized using CLR version v4.0.30319 from c:\Windows\Microsoft.NET\Framework64\v4.0.30319\
2022-03-09 10:53:05.82 spid5s SQL Trace ID 1 was started by login 'sa'.
2022-03-09 10:53:05.82 spid5s Server name is 'AI-WEB-47'. This is an informational message only. No user action is required.
2022-03-09 10:53:05.85 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [32767] 'msgsysresource'. XTP Engine version is 0.0.
2022-03-09 10:53:05.85 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [4] 'msdb'. XTP Engine version is 0.0.
2022-03-09 10:53:05.85 spid5s Starting up database 'msdb'.
2022-03-09 10:53:05.85 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [17] 'ARGENT_OMEGA'. XTP Engine version is 0.0.
2022-03-09 10:53:05.85 spid5s Starting up database 'ARGENT_OMEGA'.
2022-03-09 10:53:05.87 spid5s The resource database build version is 13.00.1601. This is an informational message only. No user action is required.
2022-03-09 10:53:05.87 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [32767] 'msgsysresource'. XTP Engine version is 0.0.
2022-03-09 10:53:05.89 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [4] 'msdb'. XTP Engine version is 0.0.
2022-03-09 10:53:05.89 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [17] 'ARGENT_OMEGA'. XTP Engine version is 0.0.
2022-03-09 10:53:05.91 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [32767] 'msgsysresource'. XTP Engine version is 0.0.
2022-03-09 10:53:05.94 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [4] 'msdb'. XTP Engine version is 0.0.
2022-03-09 10:53:06.00 spid5s [INFO] HkHostDBCtx::Initialize(): Database ID: [3] 'model'. XTP Engine version is 0.0.
2022-03-09 10:53:06.00 spid5s 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.

ARGENT OMEGA (2.2A-2207-A)

HomeTheme*Argent Instant HelpAboutLogout

Tools

Argent Omega Baseline

Argent Compliance Automator

Windows Compliance Rules

Windows Event Log Rules

Windows File Log Rules

WIN_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)

Log File Path:

C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG

VariablesView Log File

File Name Is Regular Expression

Use Yesterday's Date For Date Or Time Variables Used In File Path

Bias Date Or Time Variables Used In File Path By0Hours

Read Only Last10Megabytes

Scan Option:

The Latest File Only

Date Or Time Format:

yyyy-MM-dd HH:mm:ss.nnn

FormatVerify And Explain

Date Or Time In Log File Is UTC Time

Ignore File Log Records Over:

30Minutes

Fire Event With Format:

System DefaultIndividualCombined With Latest Event MessageCombined With Full Event Message

Use Advanced Rule Definition:

Rule Is Broken If Log Line:

ContainsCould not allocate space, Error, Exception, Login failed

Include Or Exclude Keywords: Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Precede With Character \. Wildcards * And ? Are Supported

Match Case

Match Whole Word

Match Regular Expression

Assign Event ID:

0,000

Events In Time Range:

00:00:00-23:59:59

Alert Only If The Specific Event Happens More Than1Times

Alert If The Specific Event Does NOT Exist

Alert Message Include

0Lines Before And0Lines After

Correct Condition If Log Line

Contains

Save To Archive Repository:

(default)

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line

Contains

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:

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. On the left is a sidebar with a tree view of tool sets and rules. The main panel is titled 'Log File Path' and contains several configuration sections:

- Log File Path:** A text field with the value 'C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG'. Below it are three radio buttons: 'File Name Is Regular Expression' (selected), 'Use Yesterday's Date For Date or Time Variables Used In File Path' (highlighted with a red box), and 'Bias Date or Time Variables Used In File Path By'. The 'Read Only Last' field is set to 10 Megabytes.
- Scan Option:** A dropdown menu set to 'The Latest File Only'.
- Date Or Time Format:** A text field with the value 'yyyy-MM-dd HH:mm:ss.nn'. Buttons for 'Format' and 'Verify And Explain' are next to it.
- Ignore File Log Records Over:** A dropdown menu set to 30 Minutes.
- Fire Event With Format:** Radio buttons for 'System Default', 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'.
- Use Advanced Rule Definition:** A dropdown menu set to 'Contains'.
- Rule Is Broken If Log Line:** A text field with the value 'Could not allocate space, Error, Exception, Login failed'.
- Events In Time Range:** A text field with the value '00:00:00 - 23:59:59'.
- Alert Only If The Specific Event Happens More Than:** A text field with the value '1 Times'.
- Alert If The Specific Event Does NOT Exist:** A text field with the value '0 Lines Before And 0 Lines After'.
- Correct Condition If Log Line:** A dropdown menu set to 'Contains'.
- Save To Archive Repository:** A dropdown menu set to '{default}'.
- Archive All Log Lines:** A radio button.
- Archive Matching Log Lines:** A radio button.
- Archive If Log Line:** A radio button.

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 screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. On the left is a sidebar with a tree view of tool sets and rules. The main panel is titled 'Log File Path' and contains several configuration sections:

- Log File Path:** A text field with the value 'C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG'. Below it are three radio buttons: 'File Name Is Regular Expression', 'Use Yesterday's Date For Date or Time Variables Used In File Path', and 'Bias Date or Time Variables Used In File Path By' (highlighted with a red box). The 'Read Only Last' field is set to 10 Megabytes.
- Scan Option:** A dropdown menu set to 'The Latest File Only'.
- Date Or Time Format:** A text field with the value 'yyyy-MM-dd HH:mm:ss.nn'. Buttons for 'Format' and 'Verify And Explain' are next to it.
- Ignore File Log Records Over:** A dropdown menu set to 30 Minutes.
- Fire Event With Format:** Radio buttons for 'System Default', 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'.
- Use Advanced Rule Definition:** A dropdown menu set to 'Contains'.
- Rule Is Broken If Log Line:** A text field with the value 'Could not allocate space, Error, Exception, Login failed'.
- Events In Time Range:** A text field with the value '00:00:00 - 23:59:59'.
- Alert Only If The Specific Event Happens More Than:** A text field with the value '1 Times'.
- Alert If The Specific Event Does NOT Exist:** A text field with the value '0 Lines Before And 0 Lines After'.
- Correct Condition If Log Line:** A dropdown menu set to 'Contains'.
- Save To Archive Repository:** A dropdown menu set to '{default}'.
- Archive All Log Lines:** A radio button.
- Archive Matching Log Lines:** A radio button.
- Archive If Log Line:** A radio button.

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

ARGENT OMEGA (2.2A-2207-A)

Log File Path: C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG

File Name Is Regular Expression

Use Yesterday's Date For Date Or Time Variables Used In File Path

Bias Date Or Time Variables Used In File Path By 0 Hours

Read Only Last 10 Megabytes

Scan Option: The Latest File Only

Date Or Time Format: yyyy-MM-dd HH:mm:ss.nn

Ignore File Log Records Over: 30 Minutes

Fire Event With Format: System Default

Use Advanced Rule Definition: [unchecked]

Rule Is Broken If Log Line: Contains

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

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

Archive Matching Log Lines

Archive If Log Line: Contains

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

ARGENT OMEGA (2.2A-2207-A)

Log File Path: C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG

File Name Is Regular Expression

Use Yesterday's Date For Date Or Time Variables Used In File Path

Bias Date Or Time Variables Used In File Path By 0 Hours

Read Only Last 10 Megabytes

Scan Option: The Latest File Only

Date Or Time Format: yyyy-MM-dd HH:mm:ss.nn

Ignore File Log Records Over: 30 Minutes

Fire Event With Format: System Default

Use Advanced Rule Definition: [unchecked]

Rule Is Broken If Log Line: Contains

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

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

Archive Matching Log Lines

Archive If Log Line: Contains

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:

ARGENT OMEGA (2.2A-2207-A)

Log File Path: C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG

Scan Option: The Latest File Only

Date Or Time Format: yyyy-MM-dd HH:mm:ss.nn

Verify And Explain

Ignore File Log Records Over: 30 Minutes

Fire Event With Format: System Default

Use Advanced Rule Definition: Contains

Rule Is Broken If Log Line: Could not allocate space, Error, Exception, Login failed

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: Alert Message Include

Correct Condition If Log Line: Contains

Save To Archive Repository: {default}

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line

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.

ARGENT OMEGA (2.2A-2207-A)

Log File Path: C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG

Scan Option: The Latest File Only

Date Or Time Format: yyyy-MM-dd HH:mm:ss.nn

Date Or Time In Log File Is UTC Time

Verify And Explain

Ignore File Log Records Over: 30 Minutes

Fire Event With Format: System Default

Use Advanced Rule Definition: Contains

Rule Is Broken If Log Line: Could not allocate space, Error, Exception, Login failed

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: Alert Message Include

Correct Condition If Log Line: Contains

Save To Archive Repository: {default}

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line

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

The screenshot shows the ARGENT OMEGA configuration interface. The left sidebar contains a tree view of tool sets, with 'WIN_LOG_ARCHIVE_SQL_ERROR' selected. The main panel displays the configuration for a log file path. The 'Log File Path' is set to 'C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG'. The 'Scan Option' is 'The Latest File Only'. The 'Date Or Time Format' is 'yyyy-MM-dd HH:mm:ss.nn'. The 'Ignore File Log Records Over' field is highlighted with a red box, showing a value of '30' minutes. The 'Fire Event With Format' section is also visible, with options for 'System Default', 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'.

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

The screenshot shows the ARGENT OMEGA configuration interface, similar to the previous one. The 'Fire Event With Format' section is highlighted with a red box, showing the 'Combined With Full Event Message' option selected. The 'Ignore File Log Records Over' field is also visible, showing a value of '30' minutes. The 'Fire Event With Format' section is also visible, with options for 'System Default', 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'.

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

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The left sidebar contains a tree view of tool sets, including 'Tool Sets', 'Alerts', 'Macros', 'Monitoring Groups', 'Relators', 'Calendars', 'Base Definitions', 'Holidays', and 'Administration'. The main panel displays the configuration for a log rule. The 'Log File Path' is set to 'C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG'. The 'Scan Option' is 'The Latest File Only'. The 'Date Or Time Format' is 'yyyy-MM-dd HH:mm:ss.nn'. The 'Ignore File Log Records Over' is '30 Minutes'. The 'Fire Event With Format' is 'System Default'. The 'Use Advanced Rule Definition' checkbox is checked. The 'Rule Is Broken If Log Line' dropdown is set to 'Contains' with the value 'Could not allocate space, Error, Exception, Login failed'. The 'Events In Time Range' is '00:00:00 - 23:59:59'. The 'Alert Only If The Specific Event Happens More Than' is '1 Times'. The 'Alert If The Specific Event Does NOT Exist' is checked. The 'Alert Message Include' is '0 Lines Before And 0 Lines After'. The 'Correct Condition If Log Line' is 'Contains'. The 'Save To Archive Repository' is '(default)'. The 'Archive All Log Lines' checkbox is checked. The 'Archive Matching Log Lines' checkbox is checked. The 'Archive If Log Line' checkbox is checked.

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:

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The left sidebar contains a tree view of tool sets, including 'Tool Sets', 'Alerts', 'Macros', 'Monitoring Groups', 'Relators', 'Calendars', 'Base Definitions', 'Holidays', and 'Administration'. The main panel displays the configuration for a log rule. The 'Log File Path' is set to 'C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG'. The 'Scan Option' is 'The Latest File Only'. The 'Date Or Time Format' is 'yyyy-MM-dd HH:mm:ss.nn'. The 'Ignore File Log Records Over' is '30 Minutes'. The 'Fire Event With Format' is 'System Default'. The 'Use Advanced Rule Definition' checkbox is checked. The 'Rule Is Broken If Log Line' dropdown is set to 'Contains' with the value 'Could not allocate space, Error, Exception, Login failed'. The 'Events In Time Range' is '00:00:00 - 23:59:59'. The 'Alert Only If The Specific Event Happens More Than' is '1 Times'. The 'Alert If The Specific Event Does NOT Exist' is checked. The 'Alert Message Include' is '0 Lines Before And 0 Lines After'. The 'Correct Condition If Log Line' is 'Contains'. The 'Save To Archive Repository' is '(default)'. The 'Archive All Log Lines' checkbox is checked. The 'Archive Matching Log Lines' checkbox is checked. The 'Archive If Log Line' checkbox is checked. The 'Match Case', 'Match Whole Word', and 'Match Regular Expression' checkboxes are checked. The 'Assign Event ID' field is set to '9,999'.

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

The screenshot shows the ARGENT OMEGA configuration interface. On the left is a sidebar with a tree view of tool sets and alerts. The main panel is titled 'Log File Path:' and contains various configuration options. The 'Events In Time Range' option is selected and highlighted with a red box. The time range is set from 00:00:00 to 23:59:59. Other options include 'Scan Option' (The Latest File Only), 'Date Or Time Format' (yyyy-MM-dd HH:mm:ss.nn), 'Ignore File Log Records Over' (30 Minutes), 'Fire Event With Format' (System Default), 'Use Advanced Rule Definition' (Contains), and 'Rule Is Broken If Log Line' (Contains).

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**:

The screenshot shows the ARGENT OMEGA configuration interface. On the left is a sidebar with a tree view of tool sets and alerts. The main panel is titled 'Log File Path:' and contains various configuration options. The 'Alert Only If The Specific Event Happens More Than' and 'Alert If The Specific Event Does NOT Exist' options are selected and highlighted with a red box. The time range is set from 00:00:00 to 23:59:59. Other options include 'Scan Option' (The Latest File Only), 'Date Or Time Format' (yyyy-MM-dd HH:mm:ss.nn), 'Ignore File Log Records Over' (30 Minutes), 'Fire Event With Format' (System Default), 'Use Advanced Rule Definition' (Contains), and 'Rule Is Broken If Log Line' (Contains).

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:

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
- WIN_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: 9,999

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

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

Archive Matching Log Lines

Archive If Log Line Contains

Save Archive Data Only

Alert If Failed To Open Log File

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:

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:

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
- WIN_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: 9,999

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

Alert Message Include 0 Lines Before And 0 Lines After

Correct Condition If Log Line Contains

Match Case

Match Whole Word

Match Regular Expression

Save To Archive Repository: (default)

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line Contains

Save Archive Data Only

Alert If Failed To Open Log File

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

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 screenshot displays the ARGENT OMEGA (2.2 A - 2207 - A) configuration interface. The left sidebar shows a tree view of tool sets, with 'WPN_LOG_ARCHIVE_SQL_ERROR' highlighted. The main panel shows configuration options for this rule. A red box highlights the 'Save To Archive Repository' section, which includes three radio buttons: 'Archive All Log Lines', 'Archive Matching Log Lines', and 'Archive If Log Line'. The 'Archive If Log Line' option is selected, and its dropdown menu is open, showing 'Contains' as the selected condition. Other visible options include 'Match Regular Expression', 'Assign Event ID', 'Events In Time Range', 'Alert Only If The Specific Event Happens More Than', 'Alert If The Specific Event Does NOT Exist', 'Alert Message Include', 'Correct Condition If Log Line', 'Match Case', 'Match Whole Word', 'Match Regular Expression', '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', and 'Reset Counter'.

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.

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:

ARGENT OMEGA (2.2A-2207-A)

Log File Path: Variables View Log File

☐ File Name Is Regular Expression

☐ Use Yesterday's Date For Date Or Time Variables Used In File Path

☐ Bias Date Or Time Variables Used In File Path By Hours

☐ Read Only Last Lines (Only Read Last 100 Lines By Default)

Scan Option:

Date Or Time Format: Format Verify And Explain

☐ Date Or Time In Log File Is UTC Time

Ignore File Log Records Over: Minutes

LINUX Or Unix Command Timeout: Seconds

Fire Event With Format: ☒ System Default ☐ Individual ☐ Combined With Latest Event Message ☐ Combined With Full Event Message

Use Advanced Rule Definition: ☒

Rule Is Broken If Log Line:

Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Precede With Character \. Wildcards * and ? Are Supported

☐ Match Case

☐ Match Whole Word

☐ 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

☒ Save To Archive Repository:

☒ Archive All Log Lines

☒ Archive Matching Log Lines

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:

ARGENT OMEGA (2.2A-2207-A)

Log File Path: Variables View Log File

☐ File Name Is Regular Expression

☐ Use Yesterday's Date For Date Or Time Variables Used In File Path

☐ Bias Date Or Time Variables Used In File Path By Hours

☐ Read Only Last Lines (Only Read Last 100 Lines By Default)

Scan Option:

Date Or Time Format: Format Verify And Explain

☐ Date Or Time In Log File Is UTC Time

Ignore File Log Records Over: Minutes

LINUX Or Unix Command Timeout: Seconds

Fire Event With Format: ☒ System Default ☐ Individual ☐ Combined With Latest Event Message ☐ Combined With Full Event Message

Use Advanced Rule Definition: ☒

Rule Is Broken If Log Line:

Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Precede With Character \. Wildcards * and ? Are Supported

☐ Match Case

☐ Match Whole Word

☐ 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

☒ Save To Archive Repository:

☒ Archive All Log Lines

☒ Archive Matching Log Lines

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.

The screenshot shows the ARGENT OMEGA configuration interface. The 'Log File Path' is set to '/var/log/auth.log'. The 'Scan Option' is set to 'The Latest File Only'. The 'Date Or Time Format' is set to 'MM/DD/YYYY'. The 'Ignore File Log Records Over' is set to '30 Minutes'. The 'Linux/Unix Command Timeout' is set to '10 Seconds'. The 'Fire Event With Format' is set to 'System Default'. The 'Use Advanced Rule Definition' is set to 'Contains'. The 'Rule Is Broken If Log Line' is set to 'Authentication failure'. The 'Events In Time Range' is set to '00:00:00 - 23:59:59'. The 'Alert Only If The Specific Event Happens More Than' is set to '1 Times'. The 'Alert If The Specific Event Does NOT Exist' is set to '0 Lines Before And 0 Lines After'. The 'Correct Condition If Log Line' is set to 'Contains'. The 'Save To Archive Repository' is set to '{default}'. The 'Archive All Log Lines' and 'Archive Matching Log Lines' options are both selected.

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:

The screenshot shows the ARGENT OMEGA configuration interface. The 'Log File Path' is set to '/var/log/auth.log'. The 'Scan Option' is set to 'The Latest File Only'. The 'Date Or Time Format' is set to 'MM/DD/YYYY'. The 'Ignore File Log Records Over' is set to '30 Minutes'. The 'Linux/Unix Command Timeout' is set to '10 Seconds'. The 'Fire Event With Format' is set to 'System Default'. The 'Use Advanced Rule Definition' is set to 'Contains'. The 'Rule Is Broken If Log Line' is set to 'Authentication failure'. The 'Events In Time Range' is set to '00:00:00 - 23:59:59'. The 'Alert Only If The Specific Event Happens More Than' is set to '1 Times'. The 'Alert If The Specific Event Does NOT Exist' is set to '0 Lines Before And 0 Lines After'. The 'Correct Condition If Log Line' is set to 'Contains'. The 'Save To Archive Repository' is set to '{default}'. The 'Archive All Log Lines' and 'Archive Matching Log Lines' options are both selected. The 'Use Yesterday's Date For Date Or Time Variables Used In File Path' option is highlighted with a red box.

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 screenshot shows the ARGENT OMEGA configuration interface. The left sidebar contains a tree view of tool sets, with 'UNIX_LOG_ARCHIVE_AUTH' highlighted. The main configuration area is divided into several sections:

- Log File Path:** A text field containing a file path, with 'Variables' and 'View Log File' buttons.
- Scan Option:** A dropdown menu currently set to 'The Latest File Only', which is highlighted with a red box.
- Date Or Time Format:** A text field containing a date/time format, with 'Format' and 'Verify And Explain' buttons.
- Ignore File Log Records Over:** A section with a dropdown set to '30 Minutes'.
- LINUX/Unix Command Timeout:** A section with a dropdown set to '10 Seconds'.
- Fire Event With Format:** A section with radio buttons for 'System Default', 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'.
- Use Advanced Rule Definition:** A section with a checkbox and a text field for 'Rule Is Broken If Log Line'.
- Events In Time Range:** A section with a range selector from '00:00:00' to '23:59:59'.
- Alert Only If The Specific Event Happens More Than:** A section with a dropdown set to '1 Times'.
- Alert If The Specific Event Does NOT Exist:** A section with a dropdown set to '0 Lines Before And 0 Lines After'.
- Alert Message Include:** A section with a dropdown set to 'Contains'.
- Correct Condition If Log Line:** A section with a dropdown set to 'Contains'.
- Save To Archive Repository:** A section with a dropdown set to '{default}'.
- Archive All Log Lines:** A section with a radio button.
- Archive Matching Log Lines:** A section with a radio button.

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:

This screenshot is identical to the one above, showing the ARGENT OMEGA configuration interface. The 'Verify And Explain' button, located next to the 'Date Or Time Format' field, is highlighted with a red box.

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:

The screenshot shows the ARGENT OMEGA configuration interface. The left sidebar lists various tool sets, with 'UNIX_LOG_ARCHIVE_AUTH' highlighted. The main configuration area is titled 'Log File Path:' and contains several sections: 'Scan Option:', 'Date Or Time Format:', 'Ignore File Log Records Over:', 'LINUX/Unix Command Timeout:', 'Fire Event With Format:', 'Use Advanced Rule Definition:', and 'Rule Is Broken If Log Line:'. The 'Date Or Time In Log File Is UTC Time' option is highlighted with a red box. Other options include 'File Name Is Regular Expression', 'Use Yesterday's Date For Date Or Time Variables Used In File Path', 'Bias Date Or Time Variables Used In File Path By', 'Read Only Last', 'The Latest File Only', 'MM HH:mm:ss', '30 Minutes', '10 Seconds', 'System Default', 'Individual', 'Combined With Latest Event Message', 'Combined With Full Event Message', 'Contains', 'Authentication failure', 'Match Case', 'Match Whole Word', 'Match Regular Expression', 'Assign Event ID', 'Events In Time Range', 'Alert Only If The Specific Event Happens More Than', 'Alert If The Specific Event Does NOT Exist', 'Alert Message Include', 'Correct Condition If Log Line', 'Save To Archive Repository', 'Archive All Log Lines', and 'Archive Matching Log Lines'.

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

The screenshot shows the ARGENT OMEGA configuration interface. The left sidebar lists various tool sets, with 'UNIX_LOG_ARCHIVE_AUTH' highlighted. The main configuration area is titled 'Log File Path:' and contains several sections: 'Scan Option:', 'Date Or Time Format:', 'Ignore File Log Records Over:', 'LINUX/Unix Command Timeout:', 'Fire Event With Format:', 'Use Advanced Rule Definition:', and 'Rule Is Broken If Log Line:'. The 'Ignore File Log Records Over:' field is highlighted with a red box. Other options include 'File Name Is Regular Expression', 'Use Yesterday's Date For Date Or Time Variables Used In File Path', 'Bias Date Or Time Variables Used In File Path By', 'Read Only Last', 'The Latest File Only', 'MM HH:mm:ss', '30 Minutes', '10 Seconds', 'System Default', 'Individual', 'Combined With Latest Event Message', 'Combined With Full Event Message', 'Contains', 'Authentication failure', 'Match Case', 'Match Whole Word', 'Match Regular Expression', 'Assign Event ID', 'Events In Time Range', 'Alert Only If The Specific Event Happens More Than', 'Alert If The Specific Event Does NOT Exist', 'Alert Message Include', 'Correct Condition If Log Line', 'Save To Archive Repository', 'Archive All Log Lines', and 'Archive Matching Log Lines'.

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

The screenshot shows the ARGENT OMEGA configuration interface. The left sidebar lists various tool sets, with 'UNIX_LOG_ARCHIVE_AUTH' highlighted. The main panel displays configuration options for log file paths, scan options, and alert formats. The 'Fire Event With Format' section is highlighted with a red box, showing four radio button options: 'System Default', 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'. Below this, the 'Use Advanced Rule Definition' checkbox is also highlighted with a red box.

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

This screenshot shows the same ARGENT OMEGA configuration interface, but with the 'Use Advanced Rule Definition' checkbox selected. The 'Monitoring Logic' section is highlighted with a red box, showing a table with columns for 'Properties' and 'Methods'. The table is currently empty, with row numbers 1 through 9 visible in the 'Properties' column.

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 **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**:

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.

ARGENT OMEGA (2.2A-2207-A)

Tool Sets

- Argent Omega Baseline
- Argent Compliance Automator
- Windows Compliance Rules
- Windows Event Log Rules
- Windows File Log Rules
- LINUX/Unix File Log Rules
 - UNIX_LOG_ARCHIVE_AUTH**
 - 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
- Monitoring Groups
- Relators
- Macros
- Calendars
- Administration

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

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

Match Case []

Match Whole Word []

Match Regular Expression []

Assign Event ID: 9,999

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 []

Alert Message Include 0 Lines Before And 0 Lines After

Correct Condition If Log Line: Contains

Match Case []

Match Whole Word []

Match Regular Expression []

Save To Archive Repository: (default)

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: (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: *** LINUX Auth Log ***

Description: []

Full Screen

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.

ARGENT OMEGA (2.2A-2207-A)

Tool Sets

- Argent Omega Baseline
- Argent Compliance Automator
- Windows Compliance Rules
- Windows Event Log Rules
- Windows File Log Rules
- LINUX/Unix File Log Rules
 - UNIX_LOG_ARCHIVE_AUTH**
 - 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
- Monitoring Groups
- Relators
- Macros
- Calendars
- Administration

Match Whole Word []

Match Regular Expression []

Save To Archive Repository: (default)

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: (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: *** LINUX Auth Log ***

Description: []

Full Screen

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:

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

The screenshot displays the ARGENT OMEGA configuration interface. On the left is a sidebar menu with categories like Tool Sets, Alerts, Monitoring Groups, Relators, Macros, Calendars, and Administration. The main panel is titled 'Message Priority: System Unusable, Take Action Immediately, Critical Condition'. It contains several configuration sections: 'Message Facility' (set to ' '), 'Ignore SYSLOG Records Over' (30 Minutes), 'Events in Time Range' (00:00:00 - 23:59:59, highlighted with a red box), 'Save To Archive Repository' (set to '{default}'), 'Archive All Log Lines' (selected), 'Archive Matching Log Lines', 'Archive If Log Line Contains' (empty), 'Save Archive Data Only' (checked), 'Save Performance Data To The Argent Forecaster Using Data Store' (set to '{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' (empty), 'Reference URL' (empty), 'Console Comment' (*** Network Device: Critical Condition ***), and 'Description' (This Rule monitors SYSLOG of message priority 'Critical Condition'). A 'Full Screen' button is located at the bottom right of the main panel.

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. On the left is a sidebar menu with categories like Tool Sets, Alerts, Monitoring Groups, Relators, Macros, Calendars, and Administration. The main area shows the configuration for a rule named 'SYSLOG_ARCHIVE_CRITICAL'. The configuration includes fields for Message Priority, Message Facility, Ignore SYSLOG Records Over, Events In Time Range, Save To Archive Repository, and Save Archive Data Only. The 'Save Archive Data Only' option is highlighted with a red box. Below this are fields for Tag 1, Tag 2, and Tag 3, and a section for Post Event Even If The Same Event Is Still Outstanding (Unanswered). The bottom of the interface shows a description field and a Full Screen button.

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
 - Linux/Unix File Log Rules
- SYSLOG Rules**
 - SYSLOG_ARCHIVE_CRITICAL**
 - 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
 - Monitoring Groups
 - Relators
 - Macros
 - Calendars
 - Administration

Message Priority: System Unusable, Take Action Immediately, Critical Condition

Message Facility:

Ignore SYSLOG Records Over: 30 Minutes

☒ **Events In Time Range:** 00:00:00 - 23:59:59

☒ **Save To Archive Repository:** (default)

- ☒ Archive All Log Lines
- ☐ Archive Matching Log Lines
- ☐ Archive If Log Line Contains

☒ **Save Archive Data Only**

☐ 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: *** Network Device: Critical Condition ***

Description:

This Rule monitors SYSLOG of message priority 'Critical Condition'

Full Screen

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:

ARGENT OMEGA (2.2A-2207-A)

Log Type: Error Log

Ignore Log Records Over: 24 Hours

Fire Event With Format: System Default

Use Advanced Rule Definition: [X]

Rule Is Broken If Log Line: Contains

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: [X]

Correct Condition If Log Line: Contains

Save To Archive Repository: [X]

Archive All Log Lines: [X]

Archive Matching Log Lines: [X]

Archive If Log Line: Contains

Save Archive Data Only: [X]

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

Tag 1: Error Log

Tag 2: Error Log

Tag 3: Error Log

Post Event Even If The Same Event Is Still Outstanding (Unanswered): [X]

Do So Only After: 1 Hour

Minute Since Event Is Post: 0

Ignore The Same Outstanding Event If Alerts Were Fired More Than: 1 Hour

Minute Ago: 0

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

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:

ARGENT OMEGA (2.2A-2207-A)

Log Type: Error Log

Ignore Log Records Over: 24 Hours

Fire Event With Format: System Default

Use Advanced Rule Definition: [X]

Rule Is Broken If Log Line: Contains

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: [X]

Correct Condition If Log Line: Contains

Save To Archive Repository: [X]

Archive All Log Lines: [X]

Archive Matching Log Lines: [X]

Archive If Log Line: Contains

Save Archive Data Only: [X]

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

Tag 1: Error Log

Tag 2: Error Log

Tag 3: Error Log

Post Event Even If The Same Event Is Still Outstanding (Unanswered): [X]

Do So Only After: 1 Hour

Minute Since Event Is Post: 0

Ignore The Same Outstanding Event If Alerts Were Fired More Than: 1 Hour

Minute Ago: 0

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

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

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. On the left is a navigation tree with categories like Tool Sets, Alerts, Relators, Macros, and Administration. The main panel is titled 'Log Type: Error Log'. Under 'Ignore Log Records Over:', there's a dropdown for '24' and 'Hours'. The 'Fire Event With Format:' section is highlighted with a red box and contains four radio buttons: 'System Default' (selected), 'Individual', 'Combined With Latest Event Message', and 'Combined With Full Event Message'. Below this, 'Use Advanced Rule Definition:' is unchecked. The 'Rule Is Broken If Log Line:' section has a dropdown set to 'Contains' and a text input field containing 'Could not allocate space, Error, Exception, Login failed'. Further down, there are checkboxes for 'Events In Time Range:', 'Alert Only If The Specific Event Happens More Than' (set to 1), 'Alert If The Specific Event Does NOT Exist', 'Correct Condition If Log Line' (set to Contains), 'Save To Archive Repository:' (set to default), and 'Archive All Log Lines'. There are also fields for 'Tag 1:', 'Tag 2:', and 'Tag 3:'. At the bottom, there are checkboxes for 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)', 'Do So Only After' (1 Hour, 0 Minute), 'Ignore The Same Outstanding Event If Alerts Were Fired More Than' (1 Hour, 0 Minute), and 'Post Event Only After Rule Is Broken' (2 Or More Times).

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

This screenshot shows the same ARGENT OMEGA interface, but with 'Use Advanced Rule Definition:' checked. The 'Monitoring Logic:' section is now active and highlighted with a red box. It contains a table with two columns: 'Properties' and 'Methods'. The table is currently empty, showing only a list of numbers 1 through 10 in the first column. The other configuration options, such as 'Fire Event With Format' (still 'System Default') and 'Rule Is Broken If Log Line' (still 'Contains'), remain the same as in the previous screenshot.

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:

ARGENT OMEGA (2.2A-2207-A)

Log Type: Error Log

Ignore Log Records Over: 24 Hours

Fire Event With Format: System Default

Use Advanced Rule Definition:

Rule Is Broken If Log Line: Contains Could not allocate space, Error, Exception, Login failed

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

Match Case

Match Whole Word

Match Regular Expression

Assign Event ID: 9,999

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

Correct Condition If Log Line: Contains

Save To Archive Repository: (default)

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line: Contains

Save Archive Data Only

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

Tag 1:

Tag 2:

Tag 3:

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

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

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

Post Event Only After Rule Is Broken 2 Or More Times

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

ARGENT OMEGA (2.2A-2207-A)

Log Type: Error Log

Ignore Log Records Over: 24 Hours

Fire Event With Format: System Default

Use Advanced Rule Definition:

Rule Is Broken If Log Line: Contains Could not allocate space, Error, Exception, Login failed

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

Match Case

Match Whole Word

Match Regular Expression

Assign Event ID: 9,999

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

Correct Condition If Log Line: Contains

Save To Archive Repository: (default)

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line: Contains

Save Archive Data Only

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

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**:

The screenshot displays the ARGENT OMEGA (2.2A-2207-A) configuration interface. The left sidebar shows a tree view of tool sets, with 'SS_LOG_ERROR' selected under 'SQL Server Log Rules'. The main panel shows configuration for 'Log Type: Error Log'. Under 'Fire Event With Format', 'Alert Only If The Specific Event Happens More Than' is selected and highlighted with a red box, set to '1' times. Other options include 'Alert If The Specific Event Does NOT Exist', 'Save To Archive Repository' (set to '(default)'), and 'Archive All Log Lines'. The bottom section includes options for 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)' and 'Ignore The Same Outstanding Event If Alerts Were Fired More Than'.

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

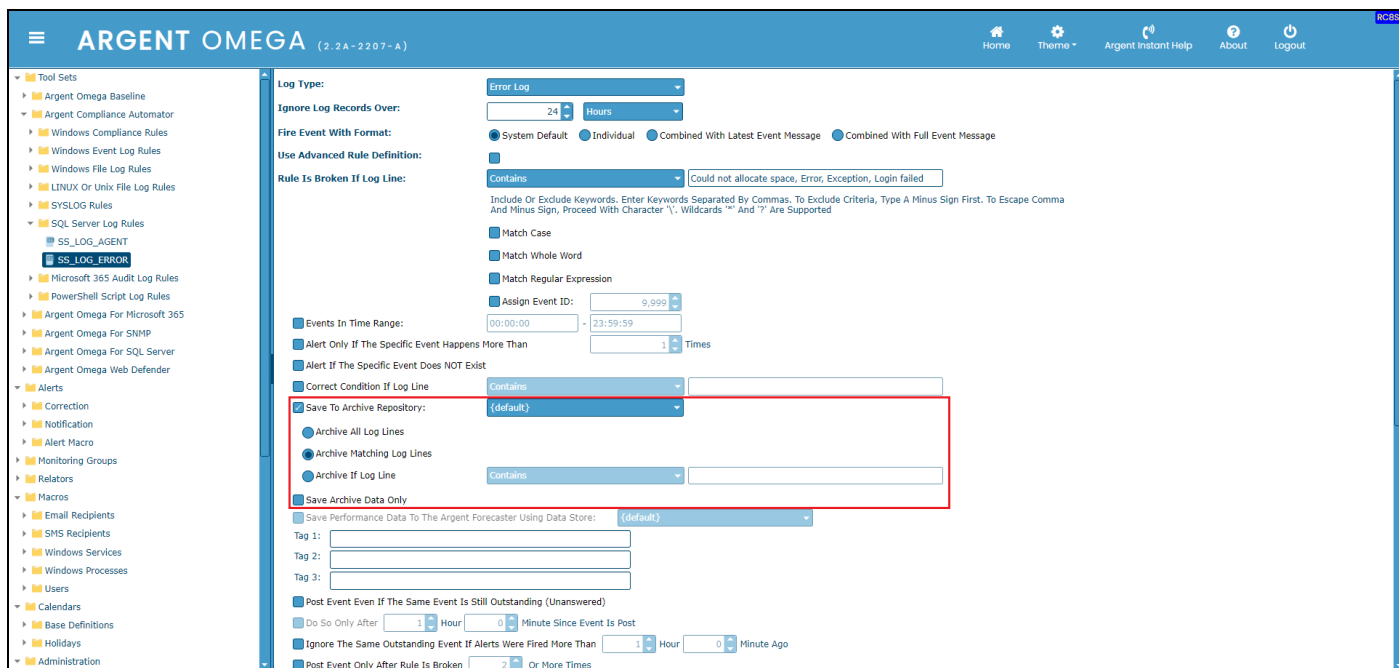
There are different options for **Save To Archive Repository**.

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:



ARGENT OMEGA (2.0A-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
- LINUX Or Unix File Log Rules
- SYSLOG Rules
- SQL Server Log Rules
- SS_LOG_AGENT
- SS_LOG_ERROR
- 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

Log Type: Error Log

Ignore Log Records Over: 24 Hours

Fire Event With Format: System Default Individual Combined With Latest Event Message Combined With Full Event Message

Use Advanced Rule Definition:

Rule Is Broken If Log Line: Contains Could not allocate space, Error, Exception, Login failed

Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Precede With Character \. Wildcards * and ? Are Supported

Match Case

Match Whole Word

Match Regular Expression

Assign Event ID: 9,999

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

Correct Condition If Log Line: Contains

Save To Archive Repository: (default)

Archive All Log Lines

Archive Matching Log Lines

Archive If Log Line: Contains

Save Archive Data Only

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

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'
```

The screenshot displays the ARGENT OMEGA (2.2A-2207-A) web interface. On the left is a sidebar with a tree view of tool sets, including 'Microsoft 365 Audit Log Rules' and 'MS365_LOG_ARCHIVE_ALL'. The main area shows the configuration for the 'MS365_LOG_ARCHIVE_ALL' rule. The 'Ignore Event Log Records Over' section is set to 24 hours. The 'Fire Event With Format' section has 'System Default' selected. The 'Rule Is Broken If Audit Log Record Satisfies Criteria' section includes checkboxes for 'User ID', 'Client IP Address', 'Workload', 'Operation', and 'Result Status', with a text input for keywords. The 'Events In Time Range' section includes checkboxes for 'Events In Time Range', 'Alert Only If The Specific Event Happens More Than', 'Alert If The Specific Event Does NOT Exist', 'Correct Event If Seeing Result Status Of Same Source', 'Save To Archive Repository', 'Save Archive Data Only', 'Alert If Failed To Download Audit Log', and 'Save Performance Data To The Argent Forecaster Using Data Store'. The 'Tag 1', 'Tag 2', and 'Tag 3' fields are empty. The 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)' section includes checkboxes for 'Do So Only After', 'Ignore The Same Outstanding Event If Alerts Were Fired More Than', and 'Post Event Only After Rule Is Broken'. The 'Reset Counter' section has 'After Event Is Post' selected.

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:

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
- LINUX Or Unix File Log Rules
- SYSLOG Rules
- SQL Server Log Rules
- Microsoft 365 Audit Log Rules
- MS365_LOG_ARCHIVE_ALL**
- 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)

Ignore Event Log Records Over: 24 Hours

Fire Event With Format: ☒ System Default ☐ Individual ☐ Combined With Latest Event Message ☐ Combined With Full Event Message

Rule Is Broken If Audit Log Record Satisfies Criteria

☐ User ID: *

☐ Client IP Address: *

☐ Workload: *

☐ Operation: *

☒ Result Status: Failed

Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Precede With Character \. Wildcards * and ? Are Supported

☐ 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

☐ Correct Event If Seeing Result Status Of Same Source: Succeeded

☒ Save To Archive Repository: (default)

☐ Save Archive Data Only

☐ Alert If Failed To Download Audit Log

☐ 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

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:

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
- LINUX Or Unix File Log Rules
- SYSLOG Rules
- SQL Server Log Rules
- Microsoft 365 Audit Log Rules
- MS365_LOG_ARCHIVE_ALL**
- 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)

Ignore Event Log Records Over: 24 Hours

Fire Event With Format: ☒ System Default ☐ Individual ☐ Combined With Latest Event Message ☐ Combined With Full Event Message

Rule Is Broken If Audit Log Record Satisfies Criteria

☐ User ID: *

☐ Client IP Address: *

☐ Workload: *

☐ Operation: *

☒ Result Status: Failed

Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Precede With Character \. Wildcards * and ? Are Supported

☐ 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

☐ Correct Event If Seeing Result Status Of Same Source: Succeeded

☒ Save To Archive Repository: (default)

☐ Save Archive Data Only

☐ Alert If Failed To Download Audit Log

☐ 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

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

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
- LINUX Or Unix File Log Rules
- SYSLOG Rules
- SQL Server Log Rules
- Microsoft 365 Audit Log Rules
- MS365_LOG_ARCHIVE_ALL**
- 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)

Ignore Event Log Records Over: 24 Hours

Fire Event With Format: System Default Individual Combined With Latest Event Message Combined With Full Event Message

Rule Is Broken If Audit Log Record Satisfies Criteria

User ID: *

Client IP Address: *

Workload: *

Operation: *

Result Status: Failed

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

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

Correct Event If Seeing Result Status Of Same Source: Succeeded

Save To Archive Repository: (default)

Save Archive Data Only

Alert If Failed To Download Audit Log

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

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**:

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
- LINUX Or Unix File Log Rules
- SYSLOG Rules
- SQL Server Log Rules
- Microsoft 365 Audit Log Rules
- MS365_LOG_ARCHIVE_ALL**
- 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)

Ignore Event Log Records Over: 24 Hours

Fire Event With Format: System Default Individual Combined With Latest Event Message Combined With Full Event Message

Rule Is Broken If Audit Log Record Satisfies Criteria

User ID: *

Client IP Address: *

Workload: *

Operation: *

Result Status: Failed

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

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

Correct Event If Seeing Result Status Of Same Source: Succeeded

Save To Archive Repository: (default)

Save Archive Data Only

Alert If Failed To Download Audit Log

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

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

ARGENT OMEGA (2.2A-2207-A)

Ignore Event Log Records Over: 24 Hours

Fire Event With Format: System Default Individual Combined With Latest Event Message Combined With Full Event Message

Rule Is Broken If Audit Log Record Satisfies Criteria

User ID: * Client IP Address: * Workload: * Operation: * Result Status: Failed

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

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

Correct Event If Seeing Result Status Of Same Source: Succeeded

Save To Archive Repository: (default)

Save Archive Data Only

Alert If Failed To Download Audit Log

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

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:

ARGENT OMEGA (2.2A-2207-A)

Ignore Event Log Records Over: 24 Hours

Fire Event With Format: System Default Individual Combined With Latest Event Message Combined With Full Event Message

Rule Is Broken If Audit Log Record Satisfies Criteria

User ID: * Client IP Address: * Workload: * Operation: * Result Status: Failed

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

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

Correct Event If Seeing Result Status Of Same Source: Succeeded

Save To Archive Repository: (default)

Save Archive Data Only

Alert If Failed To Download Audit Log

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

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:

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
- LINUX Or Unix File Log Rules
- SYSLOG Rules
- SQL Server Log Rules
- Microsoft 365 Audit Log Rules
 - MS365_LOG_ARCHIVE_ALL**
 - 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)

Ignore Event Log Records Over: 24 Hours

Fire Event With Format: System Default Individual Combined With Latest Event Message Combined With Full Event Message

Rule Is Broken If Audit Log Record Satisfies Criteria

User ID: *

Client IP Address: *

Workload: *

Operation: *

Result Status: Failed

Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sign, Precede With Character \. Wildcards * and ? Are Supported

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

Correct Event If Seeing Result Status Of Same Source: Succeeded

Save To Archive Repository: (default)

Save Archive Data Only

Alert If Failed To Download Audit Log

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

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):

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. On the left, a sidebar lists various tool sets, including 'PowerShell Script Log Rules' and 'PS_ARCHIVE_DEMO'. The main area displays the 'Add Parameters' dialog for a PowerShell script. The 'Properties' tab is active, showing a list of parameters and their values. The 'Methods' tab is also visible, showing a list of methods and their descriptions. The 'Properties' tab includes fields for 'LogName', 'EventId', 'EventSource', 'EventCategory', 'EventSeverity', 'EventTimeUtc', 'EventBody', 'EventReclum', and 'EventSource'. The 'Methods' tab includes a list of methods such as 'Register an event to be fired', 'Resolve a fired event', 'Show a network message', 'Log Text into Service Log', 'Save predictor data', 'Check if user abort the script', 'Node Property', 'Parameter', 'Generate Synthetic Event', and 'Event State'.

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:

This screenshot is similar to the previous one, but it highlights a dropdown menu in the 'Methods' tab. The dropdown menu is open, showing a list of methods and their descriptions. The methods listed are: 'Register an event to be fired', 'Resolve a fired event', 'Show a network message', 'Log Text into Service Log', 'Save predictor data', 'Check if user abort the script', 'Node Property', 'Parameter', 'Generate Synthetic Event', and 'Event State'. The 'Event State' method is currently selected.

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

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. On the left is a navigation tree with categories like Tool Sets, Alerts, Monitoring Groups, Relators, Macros, Calendars, and Administration. The 'PowerShell Script Log Rules' section is expanded, showing a rule named 'PS_ARCHIVE_DEMO'. The main panel displays the rule configuration for 'Rule Is Broken If Performance Metrics Is Over Threshold'. It includes a table with one parameter:

Name	Type	Value
P1	Numeric	100

Below the table is a 'Properties' tab showing the PowerShell script code. The script starts with a 'Set-Content' command to write the rule name to a file, followed by a 'Get-Content' command to read the file. The script then uses the 'Get-Param' method to retrieve the value of the 'P1' parameter and compares it to the current performance metrics.

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:

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The 'PowerShell Script Log Rules' section is expanded, showing the 'PS_ARCHIVE_DEMO' rule. The main panel displays the rule configuration for 'Rule Is Broken If Script Timeout'. The 'Timeout' field is set to 30 seconds. The 'Show PowerShell Script' checkbox is checked. The 'Rule Is Broken If Script Timeout' checkbox is also checked. The 'Save Performance Data To The Argent Forecaster Using Data Store' dropdown is set to '{default}'. The 'Tag 1', 'Tag 2', and 'Tag 3' fields are empty. The 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)' checkbox is checked. The 'Do So Only After' field is set to 1 hour and 0 minutes. The 'Ignore The Same Outstanding Event If Alerts Were Fired More Than' field is set to 1 hour and 0 minutes. The 'Post Event Only After Rule Is Broken' field is set to 2 or more times. The 'Reset Counter' section has three options: 'After Event Is Post', 'After Event Is Answered', and 'After The Actual Condition Is Corrected'. The 'Application' field is empty. The 'Reference URL' field is empty. The 'Console Comment' field contains '*** DEMO ***'. The 'Description' field is empty. The 'Full Screen' button is visible in the bottom right corner.

Argent_Compliance_Automator.doc