Argent Compliance Automator



www.Argent.com

Table Of Contents

Introduction
Log-On Screen
Home Screen6
CMDB-X7
CMDB-X Properties
Microsoft 365 Service Unit Credentials
Manage The Archive Repository21
Argent Compliance Automator24
Windows Compliance Rules
Windows File Log Rules40
Linux Or Unix File Log Rules
SYSLOG Rules
SQL Server Log Rules
Microsoft 365 Audit Log Rules70
PowerShell Script Log Rules75

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 <u>centrally-managed</u> 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 <u>any</u> platform – Windows, Linux, Unix; <u>if the application has a log, the Argent Compliance Automator can monitor it</u>.

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 has been in the systems management business since 1991 and has over 2,000 customers worldwide.	Argent Omega	
Argent is the Industry Leader in Monitoring and Automation Products.	Liner Name	
Read More	Enter Name	
	Password	
	Enter Password	
	Log In	
ARGENT		
	2.2A-2207-A (Build Version: v2.2.2207.14)	
Copyright	© 2022 Argent Software. All Rights Reserved	

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

There are three types of user accounts:

- Windows User Accounts
- Demo Accounts
- Internal Accounts

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

Local Windows user authentication is used instead if the Argent server is standalone or in a Workgroup.

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 <u>read-only accounts</u> and use Argent private authentication to login into Argent Omega. Demo accounts are usually only used temporarily for initial training and are limited to a few specific IP addresses. Argent engineers can create demo training accounts for you at no cost.

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

The Argent Omega username is case **insensitive** but the <u>password is case **sensitive**</u>. Argent Software Proprietary Information – All Rights Reserved

Home Screen

The Argent Omega home screen will be displayed after login:

ARGENT OMEGA (2.2				f The	🗘 🕻 🧐 🕑 me - Argent Instant Help About Logout
Find any field's name on any screen. For example, type 'S	Status'				
ecently Viewed					
. fiit	*	Θ	N	-1-	
Super Console	Tool Sets	Enterprise View	SuperMaps	Global Status	
roducts					
-1-	t i i i i i i i i i i i i i i i i i i i	RI	۲	2 (1)	—
Global Status	Events	SuperMaps	Network Topology Maps	Super Console	SLA
11	12	Ø	0	X	**
Performance Graph	Dashboard	CeoConsole	Enterprise View	тор Х	ViewMagic
Ê		11	*		曲
Scheduled Tasks	Relators	CMDB-X	Tool Sets	Alerts	Calendars
		0	•		
Macros	Monitoring Groups	Engines	Security		
rgent Reporter					
*		284	0	E	FN
Alerts	Compliance	Cross Reference	Miscellaneous	PowerShell	Performance
-					
SIA	SQL SQL Query				

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 <u>C</u>onfiguration <u>M</u>anagement <u>D</u>ata<u>B</u>ase.

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

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:

= ARGENT OMEGA (2.2A	-2207-A)			The	රී C ⁰ ලි ඒ me − Argent Instant Help About Logout
Q. Find any field's name on any screen. For example, type 'Stat	us'				
Recently Viewed					
2 m	*	•	RU		
Super Console	Tool Sets	Enterprise View	SuperMaps	Global Status	
Products					
	te "	I M	۲		5
Gobal status	Events	supermups	Hatwork ropology mops	super console	DLA.
~	55		•	x	**
Performance Graph	Dashboard	CeoConsole	Enterprise View	Top X	ViewMagic
E Scheduled Tasks	E. Belators				Colendare
_					
	•••	0	•		
Macros	Monitoring Groups	Engines	Security		
Argent Reporter					
*		<u>121</u>	~		13
Alerts	Compliance	Cross Reference	Miscellaneous	PowerShell	Performance
	squ				
SLA	SQL Query				

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

= ARGEN	OMEGA (2.2A					🔺 🌼 Home Theme -	(1) Argent Instant Help At	ට2 ? ර vout Logout
Search					Server Or Device N	letwork Group Scan Network	Properties	✓ 2 + × 8
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact	Group Or Key	Value
) Demo Group	Network Group						Name	192.168.108.97
+ First Network Group	Network Group				MUMBAI		Licensed Products	Argent Compliance Automator, Argent
192.168.108.97	Linux Or UNIX		Yes		MUMBAI		Alias	Onlega baseine
192.168.111.1	IP Device		Yes		MUMBAI		Global Security Object (GSO)	
192.168.111.2	IP Device		Yes		MUMBAI		Linux Or UNIX	
192.168.111.3	IP Device		Yes		MUMBAI		Hosting Environment	None
192.168.111.4	IP Device	APC_UPS_003	Yes				SNMP Managed	No
192.168.111.5	IP Device		Yes				SQL Server Installed	No
AI-2019-009	Windows Server		Yes		MUMBAI		+ TCP Parameters	
AI-MFC-102-W10	Windows 10 Pro		Yes				System Info Caching Minutes	720
ARGENT	URL Object		Yes		MUMBAI		Monitoring Level	Normal
DND+MFC-SQL	Windows Server		Yes		MUMBAI		Tier	Not Specified
FTP	FTP Object		Yes		MUMBAI) Tag	
FTP_1	FTP Object		Yes		MUMBAI		Location	MUMBAI
PUP	Mail Object				MUMBAL		Contact	
SMIP_1	Mail Object		Tes		MUMBAL		Owner Accounts	
1651_363	Microsoft 363 Service Unit		Tes		NUMBAL		Default Settings	
							> Time Zone Settings	
							Critical	No
							Ignored	No
							Logical Dependency	
							Installed Applications	
							Extended Properties	
							Display Options	Refresh
							Group Or Key	Value
							Show Objects	All

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:

≡ ARGENT	OMEGA (2.2A-220)	4-TI) Pro-Production	Version			🚔 🔅 Horne Therne -	ල්) Argent Instant Help	ි ඒ About Logout
Search					Server	Or Device Network Group Scan Network	Properties	🗸 🖸 🕂 🗶 Ø
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact	Group Or Key	Value
→ Demo Group	Network Group						Name	Demo Group
365_SERVICE_UNIT_1	Microsoft 365 Service Unit				MUMBAI		Туре	Network Group
AGT-PC	Windows 7 Ultimate		Yes				Location	
AI-2019-001	Windows 10 Pro		Yes				Contact	
AI-2019-002	Windows 10 Pro	Refresh					VMware Parameters	
AI-2019-003	Windows 10 Pro	Suspend Monitoring					XenServer Parameters	
AI-2019-004	Windows 10 Pro	Reactivate					SNMP Parameters	
AI-2019-005	Windows 10 Pro	Save Channes					Extended Properties	
AI-2019-006	Windows 10 Pro	Lindo					Description	
AI-2019-007	Windows 10 Pro	Lidd Decest						
AI-2019-008	Windows Server	Add Property						
AI-76	Windows 8.1 Pro N	Derete						
AI-AD-4	Windows 10 Pro	Discover Neighbor L	inks					
AI-MFC-101-W10	Windows 10 Pro	Wireless Clients						
AI-QC	Windows 10 Pro	Set Critical Flag						
AI-QC-001	Windows Server	Set Ignore Flag						
AI-QC-02	Windows 7 Ultimate	Manually Add Server	Or Device					
AI-QC-06	Windows 10 Pro	Test Connectivity						
AI-WEB-47	Windows 10 Pro	Bulk Licensing						
AI-WEB-NEW	Windows 10 Pro	Export To Excel CSV						
AI-WIN67	Windows Server	Dealars CMDD X Dat			MUMBAI			
AILAP01	Windows 10 Pro	Backup ChiDb-X Dat	abase					
AIWEB	Windows 10 Pro	Restore	1					
AJS-TEST	Windows Storage Server 2016 Standard		Yes					
AJS-TEST-ONE	Windows Storage Server 2016 Standard		Yes				and the second second	Defeed
AJS-TSET-PC	Windows 7 Ultimate		Yes				Display Options	Kerresh
ANYTIME	Windows 10 Pro		Yes				Group Or Key	Value
ANYTIME-ILHKF7B	Windows XP Professional		Yes				Show Objects	All
ANYTIME-SUPPORT	Windows Server		Yes				Network Group	
ATS-009	Windows 10 Pro		Yes				Monitoring Group	*

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

Manually Add An Entry		D2B
Name:	AI-WIN-67	
Alias: Domain:		
VM Hosting Environment:	None 🗸	
Туре:	Windows Server 🗸	
Network Group:	Demo Group 🗸 🗸	
Location:	THIRUVANANTHAPURAM	
ОК	Cancel	

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

Stearch Type Network, Group, Or, Machine Type TEST1-0015 Windows Server 2) TEST3-0016 Windows Server 2) TEST3-00172 Windows Server 2) TEST3-00182 Windows Server 2) TEST3-00182 Windows Server 2) TEST5-00182 Windows Server 2) TEST5-00182 Windows Server 2) TEST5-00182 Windows Server 2) TEST6-00182 Windows Server 2) TEST6-00182 Windows Server 2) WID-0019 Windows Server 2) WID-00213 Windows Server 2) WID-2019-0F7-865 Windows Server 2) WID-2019-0F7-865 Windows Server 2) WID-2019-0F7-865 Windows Server 2) WID-1017-72030-EIS-0L Windows Server 2) WID-1017-72030-EIS-1 Windows Server 2) WID-10215 Windows Server 2) WID-10216 Windows Server 2) WID-10205 Windows Server 2)	Allas Sarver 2016 Standard 012 A2 Standard	Licensed Vea Vea Vea Vea Vea Vea Vea Vea	Suspend	Server Or Location	Device Network Group Scan Networ	k Properties Croup Or Key Name Licensed Products Alias Global Security Object (050)	Image: Signal and Sig
Network Group Or Machine Type 123 17 2015 Windows Broke 2 125 17 20152 Windows Broke 2 TEST 20153 Windows Broke 2 TEST 20154 Windows Broke 2 VID 2015-021 Windows Store 2 With 2015-02 Windows Store 2	Alias Sarver 2015 Standard Sarver 2016 Standard Sarver 2016 Standard D12 R2 Standard D12 R2 Standard D12 R2 Standard D12 R2 Standard Alias A	Licensed Vea Vea Vea Vea Vea Vea Vea Vea Vea	Suspend	Location	Contact	Group Or Key Name Licensed Products Alias Global Security Object (GSO)	Value AL-WIN-67
Its11-2015 Widen: Strapp TIS110-20172 Widen: Strapp TIS110-20172 Widen: Strapp TIS174-20182 Widen: Strapp VID005 Widen: Strapp WID012-2018 Widen: Strapp WID012-2012 Widen: Strapp WID1-2019-2021 Widen: Strapp WID1-2019-2021 Widen: Strapp WID1-2019-2024 Widen: Strapp WID1-2019-2025 Widen: Strapp WID1-2019-2026 Widen: Strapp WID1-2019-2021 Widen: Strapp WID1-2019-2024 Widen: Strapp WID1-2019-2	Sarvar 2012 Standard Sarvar 2016 Standard Oliz A 2 Standard Oliz A 2 Standard Oliz A 2 Standard Oliz A 2 Standard Olio A 2 Standard At	Yes Yes Yes Yes Yes Yes Yes Yes				Name Licensed Products Alias Global Security Object (GSO)	AI-WIN-67
TEST-001242 Wildon Storeg 2 TEST-2012R2 Wildon Storeg 2 TRAV-1045-001 Wildon Storeg 2 Wildon Storeg 2 Wildon Storeg 2 Wildon Storeg 2 Wildon Storeg 2 Wildon Storeg 2 Wildon Storeg 2 Will-0029-0515-0L Wildon Storeg 2 Will-00290-115-0L Wildon Storeg 2 Will-00290-115-0L Wildon Storeg 2 Will-00290-115-0L Wildon Storeg 2 Will-00290-115-0L Wildon Storeg 2 Will-00200-115-0L Wildon Storeg 2 Will-00200-115-0L Wildon Storeg 2 Will-00200-115-0L Wildon Storeg 2 Will-004-TEST Wildon Storeg 2 Will-004-TEST Wildon Storeg 2 Will-004-Will Wildon Storeg 2 Will-004-WE	UIL AL Sandard UIL AL Standard UIL AL Standard UIL AL Standard UIL AL Standard UIL AL Standard UIL AL Standard UIL AL Standard Eta	Tes Yes Yes Yes Yes Yes Yes				Licensed Products Alias Global Security Object (GSO)	
TBST-2013F2 Window Server 2 Window Server 2 Window Server 2 WIN-2015 Window Server 2 WIN-2015-2011 Window Server 2 WIN-2016 Window Server 2	Sarvar 2015 Standard 012 R2 Standard 012 R2 Standard 012 R2 Standard 008 R2 Standard	Yes Yes Yes Yes Yes Yes				Alias Global Security Object (GSO)	
TB1F-4012H2 Window Server 2 TESTS-2012P2 Window Server 2 TTA1/-MAS-011	012 K2 Standard 012 R2 Standard 0108 R2 Standard 008 R2 Standard te	Yes Yes Yes Yes Yes				Global Security Object (GSO)	
TEST-2012/12 Window Server 2 TEST-2012/2 Window Server 2 TEST-2012/2 Window Server 2 TEST-2012/2 Window Server 2 TEST-2012 Window Server 2 Window Server 2 Window Server 2 Wind	1012 K2 Standard 1012 R2 Standard 1008 R2 Standard te	Yes Yes Yes Yes					
TEBTROE_LSARME_L_SAMPLE_LSAMP.E Winden Server 2 TETTROE_LSAMPLE_LSAMPLE_LSAMP.E Winden Server 2 TR1-VA8-001 Winden Server 2 TR1-VA8-001 Winden Server 2 VEX005 Winden Server 2 VEX005 Winden Server 2 WIN-2012 Winden Server 2 WIN-2013 Winden Server 2 WIN-2015-001 Winden Server 2 WIN-2020-115-0L Winden Server 2 WIN-2020-115-0L Winden Server 2 WIN-2020-115-0L Winden Server 2 WIN-12720504HR Winden Server 2 WIN-12016 Winden Server 2 WIN-0205 Winden Server 2 WIN-0205 Winden Server 2	012 R2 Standard 1008 R2 Standard te	Yes Yes Yes				Windows Server	
TteSTHODEISANDL_IISANDL_I Window Server TRU/-MG-00 Window Server TRU/-102-0049 Window Server TRU-102-0049 Window Server WBB-0012 Window Server WRI-0019-02014 Window Server WRI-0019-02014 Window Server WRI-0019-02014 Window Server WRI-0020-015-001 Window Server WRI-0200-015-001 Window Server WRI-0200-015-001 Window Server WRI-02015 Window Server WRI-02016 Window Server WRI-02016 Window Server WRI-02016 Window Server WRI-02016 Window Server	1008 R2 Standard	Yes				Hosting Environment	None
TTA1-VAR-001 Windens Server TTA1-VAR-002 Windens Server 2) VIS2005 Windens Server 2) VIS1-001-2011 Windens Server 2) WIN-0019-0071-805 Windens Server 2) WIN-0019-0071-805 Windens Server 2) WIN-0019-0071-804 Windens Server 2) WIN-0019-0071-804 Windens Server 2) WIN-0019-0071-804 Windens Server 2) WIN-0019-0071-804 Windens Server 2) WIN-0016 Windens Server 2) WIN-0016 Windens Server 2)	te	Yes				SNMP Managed	No
TW-1022-0049 Window 7 Umms V12005 Windows Server 2 WEB-2012 Windows Server 2 WIN-0318-7021 Windows Server 2 WIN-0318-7021 Windows Server 2 WIN-0318-7021 Windows Server 2 WIN-0302-015-0L Windows Server 2 WIN-0302 Windows Server 2 WIN-0302 Windows Server 2 WIN-0302 Windows Server 2 WIN-0302 Windows Server 2 WIN-0404 Windows Server 2	te					SQL Server Installed	No
VI2005 Winden Server 2 WEB-002 Winden Server 2 WIN-0019-007-065 Winden Server 2 WIN-0019-077-065 Winden Server 2 WIN-0020 Winden Server 2 WIN-0020-18F-0L Winden Server 2 WIN-0020-18F-0L Winden Server 2 WIN-0220 Winden Server 2 WIN-0216 Winden Server 2 WIN-0216 Winden Server 2 WIN-02016 Winden 2000 fm WINDOD Winden 2000 fm		Yes				TCP Parameters	
WBE-0012 Window Server 2 WIhr 0019-02011 Window Server 2 WIhr 0019-0201-030 Window Server 2 WIhr 0019-0201-030 Window Server 2 WIhr 0010-0200 Window Server 2 WIhr 0020 Window Server 2 WIhr 00216 Window Server 2 WIhr 00206 Window Server 2 Winth-0407C Window Server 2	2008 R2 Standard	Yes				System Info Caching Minutes	720
WIT-0319-2021 Windows Server 2 WIT-0319-0FF-365 Windows Server 2 WIT-0202-0FF-365 Windows Server 2 WIT-0202 Windows Server 2 WIT-02016 Windows Server 2 WIT-02016 Windows Server 2 WIT-040-WE Windows Server 2	012 Standard	Yes				Monitoring Level	Normal
WIN-2020-015-02 Winden Server 2 WIN-2020-015-0L Winden Server 2 WIN-2022 Winden Server 2 WIN-7272053EHR Winden Server 2 WIN-VET Winden Server 2	1019 Standard	Yes				Tier	Not Specified
WIN-0200-15-0L Windows Server 2 WIN-0202 Windows Server 2 WIN-0202 Windows Server 2 WIN-02030545HR Windows Server 2 WIN-02016 Windows Server 2 WIN-02016 Windows Server 2 WIN-02016 Windows Server 2 WIN-02010 Windows Server 2	019 Standard	Yes				h Tao	
WIN-0202 Windows Server 2 WIN-1727/0304BHR Windows Server 2 WIN-MCFEBT Windows Server 2 WIN-02.016 Windows Server 2 WIN-04-WC Windows Server 2 WIN-04-WC Windows Server 2	022 Standard Evaluation	Yes				1	TUTTUNANANTUATUATU
WIN-1727GSG4EHR Windows Server 2 WIN-MFC-TEST Windows Server 2 WIN-012016 Windows Server 2 WIN-01-MFC Windows 10 Pro WIN2000 Windows 2000 Pro	022 Standard Evaluation	Yes				Contract	THEROVARANT HAPONAN
WIN-MPC-TEST Windows Server 2 WIN-0L2016 Windows Server 2 WIN-0L9016 Windows 10 Pro WIN2000 Windows 2000 Pro	1012 R2 Standard	Yes				Contact	
WIN-OL2016 Windows Server 2- WIN10-MFC Windows 10 Pro WIN2000 Windows 2000 Pro	012 R2 Standard	Yes				Owner Accounts	
WIN10-MFC Windows 10 Pro WIN2000 Windows 2000 Pro	019 Standard	Yes				Default Settings	
WIN2000 Windows 2000 Pro		Yes				Time Zone Settings	Same as Location
	ofessional	Yes				Critical	No
WIN2000SERVER Windows 2000 Ser	rver	Yes				Ignored	No
WIN2008-TEST1 Windows Server 2	1008 R2 Standard	Yes				Logical Dependency	
WIN2008-TEST2 Windows Server 2	1008 R2 Standard	Yes				Installed Applications	
WIN2008-TEST3 Windows Server 2	1008 R2 Standard	Yes				Extended Properties	
WIN2012R2-TEST- Windows Server		Yes				Description	
WIN2012R2-TEST-MFC Windows Server 2	012 R2 Standard	Yes				Display Options	Refresh
WIN2016-TEST Windows Storage /	Server 2016 Standard	Yes					
WIN2016-TEST2 Windows Storage '	Server 2016 Standard	Yes				Group Or Key	Value
WIN2016-TEST3 Windows Storage *	Server 2016 Standard	Yes				Show Objects	All
WIN2016TEST2021 Windows Server 2	016 Standard	Yes				Network Group	*
WINXP Windows XP Profe		Yes				Monitoring Group	•
AI-WIN-67 Windows Server	ssional			THIRUVANANTHAPURAM		Туре	*

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

Name:	AI-LIN-23	
Alias:		
Domain:		
VM Hosting Environment:	None	-
Туре:	Linux	~
Network Group:	Demo Group	-
Location:	THIRUVANANTHAPURAM	-

Name:	AI-M365	
lias:		
omain:		
/M Hosting Environment:	None	
уре:	Microsoft 365 Service Unit	
etwork Group:	Demo Group	-
ocation:	THIRUVANANTHAPURAM	-

≡ ARGENT	OMEGA (2.2A-220)	4-T1) Pro-Production v	ersion			👫 🔅 Home Theme •	ڑی) Argent Instant Help	?
Search					Server Or D	evice Network Group Scan Network	Properties	✓ (3 + [×]
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact	Group Or Key	▲ Value
TEST	Windows Storage Server 2016 Standard		Yes				Contact	
TEST-2012R2-MFC	Windows Server 2012 R2 Standard		Yes				Description	
TEST-DATACENTER-2016	Windows Server 2016 Datacenter Evaluation		Yes				+ Extended Properties	
TEST-QA+2	Windows Server 2008 R2 Standard		Yes				Location	
TEST-VM-VS2019	Windows 10 Pro		Yes				Name	Demo Group
TEST1-2016	Windows Storage Server 2016 Standard		Yes				SNMP Parameters	
TEST10-2012R2	Windows Server 2012 R2 Standard		Yes				Type	Network Group
TEST3-2016	Windows Storage Server 2016 Standard		Yes				VMware Parameters	
TEST4-2012R2	Windows Server 2012 R2 Standard		Yes				h Yan Canada Damanda	
TEST5-2012R2	Windows Server 2012 R2 Standard		Yes				Xenserver Parameters	
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					
TRV-102-0049	Windows 7 Ultimate		Yes					
V\$2005	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-20200-IIS-OL	Windows Server 2022 Standard Evaluation		Yes					
WIN-2022	Windows Server 2022 Standard Evaluation		Yes					
WIN-1727G5G4EHR	Windows Server 2012 R2 Standard		Yes					
WIN-MFC-TEST	Windows Server 2012 R2 Standard		Yes					
WIN-OL2016	Windows Server 2019 Standard		Yes					
WIN10-MFC	Windows 10 Pro		Yes					
WIN2012R2-TEST-	Windows Server		Yes					
WIN2012R2-TEST-MFC	Windows Server 2012 R2 Standard		Yes				Display Options	Refresh
WIN2016-TEST	Windows Storage Server 2016 Standard		Yes				Common News	Malue
WIN2016TEST2021	Windows Server 2016 Standard		Yes				Group Of Key	value
AI-WIN-67	Windows Server				THIRUVANANTHAPURAM		Show Objects	All
AI-LIN-23	Linux				THIRUVANANTHAPURAM		Network Group	
AI-M365	Microsoft 365 Service Unit				THIRUVANANTHAPURAM		Monitoring Group	*
First Network Group	Network Group				MUMBAT		Туре	

lame:	192.168.108.92	
ias:		
omain:		
I Hosting Environment:	None	-
pe:	IP Address	~
twork Group:	Demo Group	-
cation:	THIRUVANANTHAPURAM	

= ARGENT	OMEGA (2.2A-220)	4-T1) Pro-Production	Version			者 🔅 Home Theme -	(1) ? Argent Instant Help Abou	් t Logout
Search					Server Or Device N	etwork Group Scan Network	Properties	✓ S + × Ø
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact	Group Or Key	Value
TEST	Windows Storage Server 2016 Standard		Yes				Contact	
TEST-2012R2-MFC	Windows Server 2012 R2 Standard		Yes				Description	
TEST-DATACENTER-2016	Windows Server 2016 Datacenter Evaluation		Yes				Extended Properties	
TEST-QA-2	Windows Server 2008 R2 Standard		Yes				Location	
TEST-VM-VS2019	Windows 10 Pro		Yes				Name	Demo Group
TEST1-2016	Windows Storage Server 2016 Standard		Yes				SNMP Parameters	
TEST10-2012R2	Windows Server 2012 R2 Standard		Yes				Type	Network Group
TEST3-2016	Windows Storage Server 2016 Standard		Yes				k VMware Parameters	
TEST4-2012R2	Windows Server 2012 R2 Standard		Yes					
TEST5+2012R2	Windows Server 2012 R2 Standard		Yes				F AenDerver Parameters	
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					
TRV-102-0049	Windows 7 Ultimate		Yes					
V52005	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-20200-IIS-OL	Windows Server 2022 Standard Evaluation		Yes					
WIN-2022	Windows Server 2022 Standard Evaluation		Yes					
WIN-1727G5G4EHR	Windows Server 2012 R2 Standard		Yes					
WIN-MFC-TEST	Windows Server 2012 R2 Standard		Yes				4	
WIN-OL2016	Windows Server 2019 Standard		Yes					
WIN10-MFC	Windows 10 Pro		Yes				4	
WIN2012R2-TEST-	Windows Server		Yes					
WIN2012R2-TEST-MFC	Windows Server 2012 R2 Standard		Yes				Display Options	Refresh
WIN2016-TEST	Windows Storage Server 2016 Standard		Yes				Common Kan	lister.
WIN2016TEST2021	Windows Server 2016 Standard		Yes				Charles Charles	All
AI-WIN-67	Windows Server				THIRUVANANTHAPURAM		bnow Ubjects	All
AI-LIN-23	Linux				THIRUVANANTHAPURAM		Network Group	
AI-M365	Microsoft 365 Service Unit				THIRUVANANTHAPURAM		Monitoring Group	
First Network Group	Network Group				MUMBAI		ivpe	
<								

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:

= ARGENT	OMEGA (2.2A-2204	-T1) Bri	8-Production	version			Home Th	erne - Argent Instant Help	ල උ About Logout	C
Search						Server Or Devi	ce Network Group Scan	Network Properties	 ✓ S + 	* 8
Network Group Or Machine	Туре	Alias	•	Licensed	Suspend	Location	Contact	Group Or Key	▲ Value	1
TEST-2012R2-MFC	Windows Server 2012 R2 Standard			Yes				Alias		
TEST-DATACENTER-2016	Windows Server 2016 Datacenter Evaluation			Yes				Contact		
TEST-QA-2	Windows Server 2008 R2 Standard			Yes				Critical	No	
TEST-VM-VS2019	Windows 10 Pro		Construction of the	Yac				► Default Settings		
TEST1-2016	Windows Storage Server 2016 Standard		Refresh					Description		
TEST10-2012R2	Windows Server 2012 R2 Standard		Suspend Monito	ring				Extended Properties		
TEST3-2016	Windows Storage Server 2016 Standard		Reactivate					Global Security Object (GSO)		
TEST4-2012R2	Windows Server 2012 R2 Standard		Save Changes					Hosting Environment	None	
TEST5-2012R2	Windows Server 2012 R2 Standard		Undo					Ignored	No	
TEST6-2012R2	Windows Server 2012 R2 Standard		Add Property					Installed Applications		
TESTNODE_1SAMPLE_1_2SAMPLE_1_3SAMP	Windows Server 2008 R2 Standard		Delete					Licensed Products	Argent Omega Baseline	
TRIV-NAS-001	Windows Server		Discover Neight	oor Links				Location		
TRV-102-0049	Windows 7 Ultimate		Wireless Clients					Logical Dependency		
VS2005	Windows Server 2008 R2 Standard		Set Critical Flag					Monitoring Level	Low	
WEB-2012	Windows Server 2012 Standard		Set Janore Flag					Name	WIN-2022	
WIN-2019-2021	Windows Server 2019 Standard		See Ignore Hug					Owner Accounts		
WIN-2019-OFF-365	Windows Server 2019 Standard		Manually Add Se	erver Or Device				SNMP Managed	No	
WIN-20200-IIS-OL	Windows Server 2022 Standard Evaluation		Test Connectivit	Υ.				SQL Server Installed	No	
WIN-2022	Windows Server 2022 Standard Evaluation		Bulk Licensing					System Info Caching Minutes	Never	
WIN-1727G5G4EHR	Windows Server 2012 R2 Standard		Export To Excel	CSV				+ Teo		
WIN-MFC-TEST	Windows Server 2012 R2 Standard		Backup CMDB-X	(Database				 TCR Parameters 		
WIN-OL2016	Windows Server 2019 Standard		Restore					The second	Net Courterd	
WIN10-MFC	Windows 10 Pro			Yes				Ter Ter Collins	Not opeched	_
WIN2012R2-TEST-	Windows Server			Yes				Window Create	Jame as Location	
WIN2012R2-TEST-MFC	Windows Server 2012 R2 Standard			Yes				p windows server		
WIN2016-TEST	Windows Storage Server 2016 Standard			Yes				Display Options		Refresh
WIN2016TEST2021	Windows Server 2016 Standard			Yes				Group Or Key	Value	
AI-WIN-67	Windows Server					THIRUVANANTHAPURAM		Charle Objects	All	
AI-LIN-23	Linux					THIRUVANANTHAPURAM		Network Group	All S	
								retwork Group		

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:

nse Selected Server Or Devi	Ces	D
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		
Remove License For Sele	OK Cancel	

Bulk Licensing Results	¢
06 Jun 2022 12:06:28 Licensed AI-M365 06 Jun 2022 12:06:28 Licensed AI-UIN-67 06 Jun 2022 12:06:28 Excensed AI-LIN-23 06 Jun 2022 12:06:28 *** 06 Jun 2022 12:06:28 Total of 3 nodes licensed (Skipped: 0, Failed: 0)	
Print Close	

CMDB-X Properties

Name	Name of the server
Licensed Products	Licensed products of a server or device
Alias	Alias name of the server or device
Туре	Type of server or device – example: Windows Server, Linux or Other
Hosting Environment	Hosting Environment regarding the server or device
SNMP Managed	SNMP managed on server or device or not.
SQL Server Installed	Option to specify SQL Server details to monitor the server using Argent
	Omega for SQL Server
TCP Parameters	Options for setting TCP parameters for the server or device.
	The options are as follows:
	Timeout
	• Retry
Tier	1 to 9 (can be used for customer's internal hierarchy or priority, etc.)
Тад	String variable used as an identifier
Location	Location of the server or device
	(This information is used to determine the device location on Google Maps.)
Contact	Person or people responsible for the device
Preferred Generators	Setting Generator for server or device
Time Zone Settings	Option to set Time Zone Settings
Critical	Option to set a server or device as critical
Ignored	Option to set a server or device as ignored
Logical Dependency	Shows Logical Dependency of a server or device
Installed Applications	Shows Installed Applications of a server or device
Extended Properties	Option to specify custom properties

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

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

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

≡ ARGENT	OMEGA (2.2A-2204	I-TI) Pro-Production	Version			🔏 🔅 Home Theme -	(1) Argent Instant Help Ab	وی out Logout
Search					Server Or Device N	etwork Group Scan Network	Properties	✓ S + × Ø
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact	Group Or Key	▲ Value
D3PC-14	Windows 10 Pro		Yes				Critical	No
D3PC-21	Windows 10 Pro		Yes				Global Security Object (GSO)	
DC-001	Windows 10 Pro		Yes				Hosting Environment	None
DESKTOP-AD-HR	Windows 10 Pro		Yes				Ignored	No
DND-SUPPORT	Windows Server 2008 R2 Standard		Yes				Installed Applications	
MOBOX	URL Object		Yes		MUMBAI		Licensed Products	Argent Omega Baseline
WIN2000	Windows 2000 Professional		Yes				Location	
WIN2000SERVER	Windows 2000 Server		Yes				Logical Dependency	
WIN2008-TEST1	Windows Server 2008 R2 Standard		Yes				Monitoring Level	Low
WIN2008-TEST2	Windows Server 2008 R2 Standard		Yes				liama	WIN2008-TEST1, WIN2008-TEST2, WIN2008-TEST2 WIN2016-TEST2
WIN2008-TEST3	Windows Server 2008 R2 Standard		Yes				iname.	WIN2016-TEST3
WIN2016-TEST2	Windows Storage Server 2016 Standard		Yes				Preferred Generators	
WIN2016-TEST3	Windows Storage Server 2016 Standard		Yes				System Info Caching Minutes	Never
WINXP	Windows XP Professional		Yes) Tag	
AGT-PC	Windows 7 Ultimate		Yes				+ TCP Parameters	
AI-2019-001	Windows 10 Pro		Yes				Retry	0
AI-2019-002	Windows 10 Pro		Yes				Timeout	Default
AI-2019-003	Windows 10 Pro		Yes				Tier	Not Specified
AI-2019-004	Windows 10 Pro		Yes				Time Zone Settings	Same as Location
AI-2019-005	Windows 10 Pro		Yes				windows Server	
AI-2019-007	Windows 10 Pro		Yes				64-bit OS	Yes
AI-2019-008	Windows Server		Yes				Authentication	
AI-76	Windows 8.1 Pro N		Yes				Cluster Name	
AI-AD-4	Windows 10 Pro		Yes				Domain	
AI-MFC-101-W10	Windows 10 Pro		Yes					¥
AI-QC	Windows 10 Pro		Yes				Display Options	Refresh
AI-QC-001	Windows Server		Yes				Group Or Vov	Value
AI-QC-02	Windows 7 Ultimate		Yes				Charles Objects	All
AI-QC-06	Windows 10 Pro		Yes				Note and Group	*
							methors aroup	

Microsoft 365 Service Unit Credentials

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

≡ ARGEN	IT OMEGA (2.2A	-2204-TI) Pre-Productio	n Version			🚔 🌞 Horne Therne •	ر) Argent Instant Help	ී ඒ About Logout
Search					Server O	r Device Network Group Scan Network	Properties	🖌 S 🕂 🗶 Ø
Network Group Or Machine	Туре	Alias	 Licensed 	Suspend	Location	Contact	Group Or Key	▲ Value
) Demo Group	Network Group				ĺ.		· · · · · · · · · · · · · · · · · · ·	
w First Network Group	Network Group				MUMBAI		Ignored	NO
192.168.108.97	Linux/UNIX		Yes		MUMBAI		Installed Applications	Arrest Complete A transfer Arrest
192.168.111.1	IP Device		Yes		MUMBAI		Licensed Products	Omega for Microsoft 365
192.168.111.2	IP Device		Yes		MUMBAI		Location	MUMBAI
192.168.111.3	IP Device		Yes		MUMBAI		Logical Dependency	
ARGENT	URL Object		Yes		MUMBAI		w Microsoft 365 Service Unit	
DND-MFC-SQL	Windows Server		Yes		MUMBAI		Administrator	test_a@argsoftdev.com
FTP	FTP Object		Yes		MUMBAI		Application Id	
FTP_1	FTP Object		Yes		MUMBAI		Contribute Thromborist	
POP	Mail Object				MUMBAI		Certificate multiplinit	
SMTP_1	Mail Object		Yes		MUMBAI		Directory Or Tenant Id	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI		Licensed Units	
192.168.111.4	IP Device	APC_UPS_003	Yes				Organization	
192.168.111.5	IP Device		Yes				SharePoint Url	
AI-2019-009	Windows Server		Yes		MUMBAI		SKU	
AI-MFC-102-W10	Windows 10 Pro		Yes				Monitoring Level	Normal
							Name	TEST_365
							Owner Accounts	
							System Info Caching Minutes	720
) Tag	
							+ TCP Parameters	
							Tier	6
							Time Zone Settings	Same as Location
							Display Options	Refresh
							Group Or Key	Value
							Show Objects	All

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:

= ARGEN	IT OMEGA (2.2	A-2204-T1)	Pro-Production Vetsion			📸 🔅 Home Theme *	(්) Argent Instant Help	ල උ About Logout
Search					Serve	er Or Device Network Group Scan Network	Properties	S + * Ø</th
Network Group Or Machine	Туре	Alias	Licensed	Suspend	Location	Contact	Group Or Key	▲ Value
) Demo Group	Network Group						Innored	No
v First Network Group	Network Group		Refresh		MUMBAI		Installed Applications	
192.168.108.97	Linux/UNIX		Suspend Monitoring		MUMBAI			Argent Compliance Automator Argent
192.168.111.1	IP Device		Reactivate		MUMBAI		Licensed Products	Omega for Microsoft 365
192.168.111.2	IP Device		Save Changes a		MUMBAI		Location	MUMBAI
192.168.111.3	IP Device		Undo		MUMBAI		Logical Dependency	
ARGENT	URL Object		Add Property a		MUMBAI		✓ Microsoft 365 Service Unit	
DND-MFC-SQL	Windows Server		Delete		MUMBAI		Administrator	test_a@argsoftdev.com
FTP	FTP Object		Discover Neighbor Links		MUMBAI		Application Id	9a317472-8826-49c7-8348-
FTP_1	FTP Object		Wireless Clients		MUMBAI		Certificate Thumborint	7A8DF1218B4BCD9CA8B0997286F8
POP	Mail Object		Set Critical Flag		MUMBAI			725d575e-2928-4048-8d7d-
SMTP_1	Mail Object		Set Ignore Flag		MUMBAI		Directory Or Tenant Id	bbf15cd0cc4c
TEST_365	Microsoft 365 Service Unit		Manually Add Server Or Device		MUMBAI		Licensed Units	
192.168.111.4	IP Device	APC_	Test Connectivity				Organization	argsoftdev.onmicrosoft.com
192.168.111.5	IP Device		Test connectivity				SharePoint Url	https://argsoftdev.sharepoint.com
AI-2019-009	Windows Server		Bulk Licensing		MUMBAI		SKU	
AI-MFC-102-W10	Windows 10 Pro		Export To Excel CSV				Monitoring Level	Normal
			Backup CMDB-X Database				Name	TEST_365
			Restore				Owner Accounts	
							System Info Caching Minutes	720
)⊧ Tag	
							+ TCP Parameters	
							Tier	6
							Time Zone Settings	Same as Location
							Display Options	Refresh
							Group Or Key	Value
							Show Objects	All
							Network Group	*

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

Select Genera	tor To Run Connectivity Test	×
Name:	AI-2019-009	-
	ОК	Cancel

The Results are shown:

nnectivity test kest	ilts	
Argent Omega 2.2.	2205.31 Copyright (c) 2022 Argent Software	<u>_</u>
For Argent Instant	Help 7 by 24 with an Argent engineer, please see http://help.Argent.com/help.php	
Target Machine:	TEST_365	
Test At:	AI-2019-009	
Test Time:	Mon, 06 Jun 2022 06:50:20 (UTC)	
06:50:20 - Test 1: 06:50:20 - PowerS 06:50:24 - [VALID] Readers,Exchange 06:50:24 - Found A 06:50:25 - *** WA	Access of Azure Active Directory hell Module 'AzureAD' (Version: 2.0.2.140) Registered App has roles: Global Administrator,Application Administrator,Directory Administrator Azure Domains: argsoftdev.com,argsoftdev.onmicrosoft.com RNING *** Failed to determined Microsoft 365 License information	
06:50:25 - Test 2: 06:50:25 - PowerS 06:50:41 - [VALID]	Access of Exchange Online hell Module: ExchangeOnlineManagement (2.0.5) Matched SharePoint URL: https://argsoftdev.sharepoint.com	2007.
06:50:41 - Test 3: 06:50:41 - PowerS	Access of SharePoint Online hell Module: SharePointPnPPowerShellOnline (3.29.2101.0)]	

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:

						_
Ver Refresh Add New	Delete Choose Global Security Object	•				
Name	st Changed Time (UTC) Description					
AR_TEST 06	Jun 2022 06:53:32					
	Please Enter New Arch	ive Repository Name	×			
		,				
	Name: MS_	365_AUDIT_LOGS				
	c	Cancel				
			_			
			#	¢ Thomas		() About
T OMEGA (2.2A-2204-TI)	Rta-Praduction Variation		A Home	theme -	(1) Argent instant Help	? About
OMEGA (2.2A-2204-TI) SQL Server:	The Production Vateran (default)	Test Connection	# Home	theme -	දී Argent Instant Help	? About
MEGA (2.2A-2204-TI) SQL Server: Database:	Tre-Production Variation [defailt]	Test Connection	# Home	Theme -	Ç Ø Argent instant Help	? About
NEGA (2.2A-2204-TI) SQL Server: Database:	fite: Fload up transition (default) (default) (default)	Test Connection Refresh	Home	therne -	رہ Argent Instant Help	? About
MEGA (2.2A-2204-TI) SQL Server: Database:	Ite: Production {default} (default) @ Use Trusted Connection	Test Connection Refresh	Home	therne -	C ⁰ Argent Instant Help	? About
DMEGA (2.2A-2204-11) SQL Server: Database: SQL Schema:	Idefault) (default) (default) @ Use Trusted Connection (default)	Test Connection Refresh	# Home	Theme -	Ç ^ð Argent Instant Help	3 About
SQL Server: Database: SQL Schema: SQL Table Prefix:	file File [default] • [default] • [default] • [default] • [default] •	Test Connection Refresh	# Home	Theme •	Ç ⁰ Argent İnstant Help	? About
MEGA (2.2A-2204-TI) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding:	Itel Fload up (intervention) (default) Image: Im	Test Connection Refresh	Home	theme *	Ç Ø Argent Instant Help	? About
SQL Server: Database: SQL Schema: SQL Schema: SQL Table Prefix: Sharding:	Idefault) (default) Use Trusted Connection (default) (default) (default) (default) (default) (default)	Test Connection Refresh	Home	Theme -	Ç Ø Argent Instant Help	? About
SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days:	files Files Files [default)	Test Connection Refresh	# Home	theme -	CO Argent instant Help	? About
SQL Server: Database: SQL Schema: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days:		Test Connection Refresh	Home	Differing -	Ç Ø Argent Instant Help	? About
SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days:	Idefault) (default)	Test Connection Refresh	Home	therme -	C⁰ Argent Instant Help	? About
SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder:	Image: Provide of the connection (default) [default] @ Use Trusted Connection (default) [default] [default] [default] [default] [] <td>Test Connection Refresh</td> <td># Home</td> <td>r Thome -</td> <td>CO Argent instant Help</td> <td>About</td>	Test Connection Refresh	# Home	r Thome -	CO Argent instant Help	About
SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO):	Image: Constraint of the second se	Test Connection Refresh	Home	thome -	Ç Ø Argent Instant Help	R About
MEGA (2.2A-2204-71) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Hease Choose:	Idefault) (default) (default) (default) (default) (default) (default) 0 Not Due Sharding 0 Not Purge Data (default) (default)	Test Connection Refresh	Home	Theme -	C o Argent Instant Help	2 About
SQL Server: Database: SQL Schema: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Plescription:	files Files (default) • (default) • @ Use Trusted Connection (default) (default) • (default) • @ Do Not Use Sharding 30 • @ Do Not Use Sharding 30 • @ Do Not Use Sharding 30 • @ Do Not Purge Data (default)	Test Connection Refresh	# Home	theme -	CO Argent instant Help	About
SQL Server: Database: SQL Schema: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Mease Choose: Description:	Tree-Production Variation [default] default] (default] (default] (default] (default] 0 bo Not Dise Sharding 0 bo Not Purge Data (default] 0 bo Not Purge Data (default) 0 bo Not Purge Data (default) 0 bo Not Purge Data	Test Connection Refresh	Homo	theme -	Ç® Argent Instant Help	? About
AEGA (2.2A-2204-11) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Mase Choose: Description: III V Format Block r fo	The Production Variation (default)	Test Connection Refresh	A Home	thorno -	C Argent instant Help	About
SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Pascription: It / U Format Block ~ Fo	Area - Fronduction Variation (default) • • • • • • • • • • • • • • •	Test Connection Refresh	Нопое	theme -	CO Argent instant Help	About
MEGA (2.2A-2204-71) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Clobal Security Object (CSO): Flease Choose: Description: I I I I Format Block To	Ing - Production Variation [(default) (default) (default) (default) (default) (default) 0 Not Durge Data (default) 0 Not Purge Data (default) 0 Not Purge Data (default) 0 Not Purge Data	Test Connection Refresh	Home	there -	C [®] Argent Instant Help	About
MEGA (2.2A-2204-TI) SQL Server: Database: SQL Schema: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Socurity Object (GSO): Ffease Choose: Description: I Z U Format Block Fo	The Production Valence (default) (default	Test Connection Refresh	Ното	theme -	C ⁹ Argent instant Help	Q About
OMEGA (2.2A-2204-11) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Flease Choose: Description: If I I Format Block • Fo	The Fruduction Variation (default) (defau	Test Connection Refresh	Home	theme -	C [®] Argent instant Help	Q About
SQL Server: Database: SQL Schema: SQL Sche	Ing - Production Variation [default] [default] [default] [default] [default] [] Do Not Durge Data [[default] [] De Not Purge Data [[default] [] De Not Purge Data [[default]	Test Connection Refresh	Homo	theme -	C ⁰ Argent Instant Help	e About
OMEGA (2.2A-2204-11) SQL Server: Database: SQL Schema: SQL Schema: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Clobal Socurity Object (GSO): Please Choose: Description: I V Format Block Fo	Arep-Providuation Variation (default) (default) (default) (default) (default) (default) 0 Not Use Sharding 30 0 0 Not Duse Sharding 30 0 1 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0	Test Connection Refresh	Ното	thome -	C ⁹ Argent instant Help	Q About
OMEGA (2.2A-2204-TI) SQL Server: Database: SQL Schema: SQL Schema:	Pre-Fruduction Variation (default) (defaul	Test Connection Refresh	Нопре	theme -	C [®] Argent instant Help	About
DMEGA (2.2A-2204-11) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Waare Choose: Description: Description: Description:	Idefault) (default) (default) (default) (default) (default) 0 Do Not Use Sharding 30 0 0 Do Not Purge Data (default) (default) 0 Do Not Purge Data (default) 1	Test Connection Rofresh	Homo	Thomo -	C ⁰ Argent Instant Help	About
SQL Server: Database: SQL Schema: SQL Table Preffx: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Mease Choose: Description:	Arep-Providuo tiener Viertener (default) (default) (default) (default) (default) 0 Not Use Sharding 30 0 0 Not Durge Data (default) 0 Not Ourge Data (default) 0 Not Ourge Data (default) 0 Not Ourge Data (default) 0 Not Ourge Data	Test Connection Refresh	Ното	thome -	C ⁹ Argent Instant Help	About
MEGA (2.2A-2204-TI) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Flease Choose: Description: I V format Block • Fo	Area - Frond up that Valuation (default)	Test Connection Refresh	Нопо	theme -	C ⁰ Argent instant Help	About
MEGA (2.2A-2204-TI) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Clobal Security Object (GSO): Mease Choose: Description: Description: Description: Superior Storage Telder of the security of th	Idefault [default] @ Use Trusted Connection [default] @ Oo Not Use Sharding @ Oo Not Purge Data [default] @ Oo Not Purge Data [default] @ On Not Purge Data [default] @ On Not Purge Data [default] @ Dete	Test Connection Refresh	Homo	Thomo -	C ⁹ Argent linstont Help	About
SQL Server: Database: SQL Schema: SQL Table Preffx: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Please Choose Description:	Image: Provolucion Variation (default)	Test Connection Refresh	Home	thome -	C ⁰ Argent Instant Help	About
OMEGA (2.2A-2204-TI) SQL Server: Database: SQL Schema: SQL Table Prefix: Sharding: Data Retaining Days: Long Term Storage Folder: Global Security Object (GSO): Flease Choose: Description: I V Format Block row Save Undo	Idefault: Image: Copy	Test Connection Refresh	Homo	theme -	C [®] Argent instant Help	2 Abou

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:

■ ARGENT OME	GA (2.2A-2204-TI) Pro-Pro-			Theme - Argent	(* ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
Q Find any field's name on any screen. For	example, type 'Status'				
Recently Viewed					
Tool Sets	CMDB-X	Network Topology Maps			
Products					
Global Status	Events	SuperMaps	Network Topology Maps	Super Console	SLA
Performance Graph	Dashboard	CeoConsole	Contempose View	X Top X	ViewMagic
Scheduled Tasks	Relators	СМДВ-Х	X Tool Sets	Alerts	Calendars
Macros	American Ameri American American Americ American American Americ American American A	Engines	Security		
Argent Reporter					
			60	51	R 1

Under Tool Sets, select Argent Compliance Automator:

ARGENT OMEGA (2.2A-2204-TI) #78-#roduction Version				合 Home	🔅 Theme -	heme - Argent Instant Help		ن Logout	
ool Sets Argent Omega Baseline	Search Choose	Slobal Security Object	-						
Argent Compliance Automator	Name	Description							
Windows Compliance Rules	Windows Compliance Rules								
ndows Event Log Rules	Windows Event Log Rules								
dows File Log Rules	Windows File Log Rules								
IUX/Unix File Log Rules	LINUX/Unix File Log Rules								
SLOG Rules	SYSLOG Rules								
Server Log Rules	SQL Server Log Rules								
rosoft 365 Audit Log Rules	Microsoft 365 Audit Log Rules								
verShell Script Log Rules	PowerShell Script Log Rules								
gent Omega For Microsoft 365 gent Omega For SQL Server ts tioring Groups tors TOS									
lars istration									
nse (Admin Only)									
erator Settings									
gent Omega									
gent Alert Mechanism									
gent Forecaster									
gent SIEM-Complete									
urity									

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):

= ARGENT OME	GA (2.2A-2207-A)	イオー 交 (*) ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・		
▼ 🐸 Tool Sets	Read Windows Security Log With Method:	Automatically Determined 👻		
Argent Omega Baseline	Archive Repository:	(default)		
 Argent Compliance Automator 	Skip Socurity Log Records Query			
✓ Windows Compliance Rules	Skip Security Log Records Over:	Hours		
WCP_UNIVERSAL_COMPLIANCE_ARCHIVE	In Addition To Compliance Audit Log, A	Archive Windows Security Log Matching Following Criteria		
Windows Event Log Rules	Event ID:	-		
Windows File Log Rules		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		
EINOX/ONIX File Log Rules	Event User:			
STSLOG Rules	Event Category:	×		
Microsoft 365 Audit Log Rules	Event Source:	-		
PowerShell Script Log Rules		Match Care		
Argent Omega For Microsoft 365		Produit Case		
Argent Omega For SNMP		Match Whole Word		
Argent Omega For SQL Server		Match Regular Expression		
Argent Omega Web Defender	Include Audit Failure Events			
▼ 🐸 Alerts				
Correction	Read User Data From Custom XPath			
Notification	Alert On Potential Data Loss			
Alert Macro	Alert If Failed To Open Windows Event Lo	00		
Monitoring Groups	Save Performance Data To The Argent Fo	orecaster Using Data Store: (default)		
Relators	Tag 1:			
🔻 🔚 Macros	Tag 2:			
Email Recipients	Tag 3:			
SMS Recipients				
Windows Services	Post Event Event If The Same Event Is Still Outstanding (Unanswered)			
Windows Processes	Do So Only After 1 Beur 0 Minute Since Event is Post			
v users	Ignore The Same Outstanding Event If A	Alerts Were Fired More Than 1 🔁 Hour 0 🔁 Minute Ago		
Calendars	Post Event Only After Rule Is Broken 2 Or More Times			
 Base Deminuons Holidave 	reset Counter			
Administration	After Event Is Post			
License (Admin Only)	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:

= ARGENT OME	GA (2.2A-)						Home	theme -	را) Argent Instant Help	? About	U Logout	√2
& WCP_UNIVERSAL_COMPLIANCE_ARCHIVE	Search	Refresh	Add New	Delete	Choose Global Security Object	-						
Windows Event Log Rules	Name	Las	t Changed Time (UTC)	Descripti	on							
Windows File Log Rules	AR_MS_365_AUDIT_L	LOGS 06 J	lun 2022 06:55:31									
LINUX/Unix File Log Rules	AR_TEST	06.3	lun 2022 06:53:32									
SYSLOG Rules												
SQL Server Log Rules												
Microsoft 365 Audit Log Rules												
Powershell Script Log Rules												
Argent Omega web Derender												
Argent Omega For SQL Server												
Alerts												
Monitoring Groups												
Relators												
Macros												
Calendars												
🕶 🔚 Administration												
Ticense (Admin Only)												
🔻 🔚 Generator Settings												
▶ o ^p Argent Omega												
 o^o Argent Alert Mechanism 												
 o^o Argent Forecaster 												
✓ 0 ^o Argent SIEM-Complete												
SIEM Policy Archive Repository Ar_MS_365_AUDIT_LOGS												
AR_TEST												
Security												
Network Scan												
Event Logs												
SuperMaps	1											
Topology Maps												

Use the Skip Security Log Records Over field to skip monitoring Security Event Log records that are

older than the specified time:

■ ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme -	(') Argent Instant Help	? About	U Logout	RC39
	 Read Windows Security Log With Method: Archive Repository: Skip Security Log Records Over: In Addition To Compliance Audit Log, A Event D: Event User: Event Category: Event Source: 	Automatically Determined (default) (default) 24 () Itours - Include Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude (Hatch Case Hatch Whole Word Match Case Hatch Regular Expression	Criteria, Type A Minu:	s Sign First. For	Example 1,3,5-99,-76			
Argent Omega For SQL Server Alerts Correction Aution Autification Include Audit Failure Events Read User Data From Custom XPath Adet On Potential Data Loss Jart If Failed To Open Windows Event Lt Save Performance Data To The Argent For To 1: Tag 2: Tag 3: Do So Only After 1 Do So Only After 1 Do So Only After 1 Do So Conly After Save Custanding Event If A								
 Homdays Administration License (Admin Only) 	After Event Is Post After Event Is Answered							

The "In Addition To Compliance Audit Log..." section can be used to filter the Event log records to be

archived:

■ ARGENT OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	ර ්) Argent Instant Help	? About	ம் Logout	RC3S
View Tool Sets Argent Omega Baseline Argent Omega Baseline Windows Compliance Automator Windows Compliance Rules Windows Event Log Rules Windows Event Log Rules Windows Event Log Rules SYSLOG Rules SYSLOG Rules SYSLOG Rules Microsoft 365 Audit Log Rules Microsoft 365 Microsoft 365 Microsoft 365	Read Windows Security Log With Method: Archive Repository: Skip Security Log Records Over: In Addition To Compliance Audit Log, Al Event ID: Event User: Event Source:	Automatically Determined (default) 24 Visuus Inductor Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separa Inductor Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separa Automatically Determined Natch Case Natch	ted By Commas. To Exclude Criteria, Type A Minu	s Sign First. For	Example 1,3,5-99,-76			
 Argent Omega For SQL Server Argent Omega Veb Defender Alerts Correction Notification Alert Macro Monitoring Groups Kelators Bacros Bacros Enail Recipients Windows Services Windows Services Windows Services Users Calendars Calendars Alext Processes Holidays 	Include Audit Failure Events Read User Data From Custom XPath Alert On Potential Data Loss Alert 1f Failed To Open Windows Event Lo Save Performance Data To The Argent Fo Tag 1: Tag 2: Tag 3: Post Event Even If The Same Event Is St Do So Only After Igent For Same Over I and Post Event Only After Rule Is Broken Reset Counter Reset Data Broken	g g ill Outstanding (Unanswered) g @ Minute Since Event Is Post lefts Ware Find Mere Than 1 @ Hour g @ Or More Times						
 Administration License (Admin Only) 	After Event Is Post 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 OME	GA (2.2A-2207-A) C O C Home Theme Argent Instant Help About Log	ით. gout		
	Read Windows Security Log With Method Automatically Determined Archive Repository: (default) Skip Security Log Records Over: 24 In Addition To Compliance Audit Log, Archive Windows Security Log Matching Following Criteria Event ID: - Include Or Exclude Event IDs. Enter ID Humbers And/Or ID Ranges Separated By Commas. To Exclude Criteria, Type A Minus Sign First. For Example 1,3,5-99,-76 Event User: -			
SQL Server Log Rules Microsoft 365 Audit Log Rules Microsoft 365 Audit Log Rules Microsoft 365 Microsoft 365 Microsoft 365 Microsoft 365 Microsoft 365 Microsoft 365 Microsoft Omaga For SQL Server Microsoft Omaga Veb Defender				
Alerts Correction Motification Motification Motification Motification Motification Groups Motificators Motificators Motificators Email Recipients Motifications	Read User Data From Cuttom XPath Alert On Potential Data Loss Alert If Failed To Open Windows Event Log Save Performance Data To The Argent Forecaster Using Data Store: Tap 1: Tag 2: Tag 3:			
Windows Services Windows Processes Users Calendars Base Definitions Holidays Madministration Ecses (Admin Only)	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:

■ ARGENT OME	GA (2.2A-2207-A)	et Home	RC4s ک کاری Theme - Argent Instant Help About Logout
▼ M Tool Sets	Event Log Name:	Application Reload	
Argent Omega Baseline	Event Severity:	Critical,Error 🗸	
Argent compliance Automator	Event ID:	1-99999	
Windows Event Log Bules		nclude Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Criteria, Type A Minus Si	ign First. For Example 1,3,5-99,-76
EVT APPLICATION ERROR	Read Windows Event Log With Method:	Automatically Determined 🗾 👻	
EVT_AUDIT_FAILURE	Rule View:	Simple	
EVT_SYSTEM_ERROR	Ignore Event Log Records Over:	20 A Minutee	
Windows File Log Rules	C. C. Huffle C	30 V Minuces	
LINUX Or Unix File Log Rules	Fire Event with Format:	🖲 System Default 🛛 Individual 💭 Combined With Latest Event Message 🔵 Combined With Full Event Message	
SYSLOG Rules	Additional Event Log Filtering Criteria —		
SQL Server Log Rules	Event User:		
Microsoft 365 Audit Log Rules	Event Category:		
PowerShell Script Log Rules	Event Source:	6	
Argent Omega For Microsoft 365	Custom User Data:	Using XPath	
Argent Omega For SNMP	1	Match Case	
Argent Omega For SQL Server	1	Matels Wheele Wood	
Argent Omega web Derender		Platen whole word	
Alerts		Match Regular Expression	
Notification			
Alert Macro	Events in time kange.		
Monitoring Groups	Alert Only If The Specific Event Happens N	ore Ihan 1 Imes	
Relators	Alert If The Specific Event Does NOT Exist		
👻 🖬 Macros	Treat Events With Same Event ID, Source	Ind Type As Same Events (Ignore Event Message)	
Email Recipients	Retrieve Performance Metric From XPath:		
SMS Recipients	Performance Object Name:	Use As XPath	
Windows Services	Counter Name:	Ilse As XPath	
Windows Processes			
Users	Instance Name:	Use As XPath	
▼ Mathematical Calendars	Machine Name:	{default}	
Base Definitions	Correct Event If Seeing Event Id Of Same	Source:	
Holidays			

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

Rules:

■ ARGENT OME	GA (2.2A-2207-A)		👫 Home	🔅 Theme -	(1) Argent Instant Help	? About	U Logout	RC45
	Event Log Name:	Application	Reload	1				
Argent Omega Baseline	Event Severity:	Critical,Error		, 				
 Image: Argent Compliance Automator 	Event ID:	1-99999						
Windows Compliance Rules		Include Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Crite	eria. Type A Minus	s Sian First, For	Example 1.3.5-9976			
Windows Event Log Roles	Read Windows Event Log With Method:	Automatically Determined						
	Rule View:	Simple *						
EVT SYSTEM ERROR	Teners Fuent Les Reserts Quer							
Windows File Log Rules	Ignore Event Log Records Over.	30 💭 Minutes 👻						
LINUX Or Unix File Log Rules	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Even	nt Message					
SYSLOG Rules	Additional Event Log Filtering Criteria							
SQL Server Log Rules	Event User:	8						
Microsoft 365 Audit Log Rules	Event Category:	*						
PowerShell Script Log Rules	Event Source:	*						
Argent Omega For Microsoft 365	Custom User Data:	Using XPath						
Argent Omega For SNMP	1	Match Case						
Argent Omega For SQL Server		Makele Whate Ward						
Argent Omega Web Defender		Match whole word						
Alerts		Match Regular Expression						
Notification	Currente des Times Desserve	00.00.00						
▶ Malert Macro	events in time range:	0:0:00						
Monitoring Groups	Alert Only If The Specific Event Happens	More Inan 1 Imes						
Relators	Alert If The Specific Event Does NOT Exit	st						
👻 🕍 Macros	Treat Events With Same Event ID, Source	e And Type As Same Events (Ignore Event Message)						
Email Recipients	Retrieve Performance Metric From XPath	:						
SMS Recipients	Performance Object Name:	Use As XPath						
Windows Services	Counter Name:	Use As XPath						
Windows Processes	Instance Name:							
▶ 🔤 Users	instance warne.	Use as Apath						
✓ III Calendars	Machine Name:	{default} Use As XPath						
Base Definitions	Correct Event If Seeing Event Id Of Sam	e Source:						
Holidays	_							

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

Reload button:

			4			٩		RC4S
= ARGENT OME	GA (2.2A-2207-A)		Home	Theme -		About	Logout	
Argent Omplane Rules More Complane Rules Windows Event Log Rules Windows Event Log Rules Windows Event Log Rules EVT_ARRENT FALLOR RULE EVT_AUDIT_FALLURE EVT_SYSTEM_RRANR Windows File Log Rules Structor Unix File Log Rules Structor Log Rules Structor Log Rules Structor Log Rules Microsoft 365 Audit Log Rules Microsoft 365 Audit Log Rules Microsoft 365 Audit Log Rules Microsoft 365 Margent Omega For SNP Margent Omega For SQL Server	Event Log Name: Event Severity: Event ID: Read Windows Event Log With Method: Rule View: Ignore Event Log Records Over: Fire Event Uog Records Over: Fire Event With Format: Additional Event Log Filtering Criteria – Event Ser: Event Gaegory: Event Source: Custom User Data:	Application Critical, Error L-0999 Include Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Criter Atomatically Determined Single 30 Plinutes Solicit A Windows Machine Remote Machine Remote Machine Remote Machine Goody # Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Remote Machine Coody # Remote Machine Coody # Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Remote Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Message Combined With Full Event Solicit A Windows Machine Coody # Combined With Combined With Latest Event Solicit A Windows Combined With Combined With Combined With Full Solicit A Windows Combined With Combined Coody # Combined With Combined Combined With Combined Combined With Full Solicit A Windows Combined With Combined	Home Reload	Sign First. For	Argent Instant Help	About	Logout	
Margent Omega web Defender Margent S		OK Cancel						
Correction Motification Motification Mater Macro Motification Groups Motificators	Events In Time Range: Alert Only If The Specific Event Happens Alert If The Specific Event Does NOT Exis	00:00:00 - [23:59:59 More Than 1 Times t						
Macros Macros Maros Marol Recipients MS Recipients	Treat Events With Same Event ID, Source Retrieve Performance Metric From XPath: Performance Object Name:	And Type As Same Events (Ignore Event Message)						
Windows Services Windows Processes Users	Counter Name: Instance Name:	Use As XPath						
 ✓ Marcalendars ▶ Marcale Definitions ▶ Marcale Holidays 	Machine Name:	{default}						

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 OME	GA (2.2A-2207-A)	····································
	Event Log Name:	Application V Reload
Argent Omega Baseline	Event Severity:	Critical,Error
Argent Compliance Automator	Event ID:	1-9999
Windows Compliance Rules		Include OF 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
Windows Event Log Roles	Read Windows Event Log With Method:	Automatically Determined
EVT AUDIT FAILURE	Rule View:	Simple
EVT_SYSTEM_ERROR	Tanora Event Log Records Over:	
Windows File Log Rules	Ignore Event Log Records over.	30 Vinutes Vinutes
LINUX Or Unix File Log Rules	Fire Event With Format:	🗑 System Default 🔵 Individual 🛛 Combined With Latest Event Message 🔍 Combined With Full Event Message
SYSLOG Rules	Additional Event Log Filtering Criteria —	
SQL Server Log Rules	Event User:	*
Microsoft 365 Audit Log Rules	Event Category:	-
PowerShell Script Log Rules	Event Source:	•
Argent Omega For Microsoft 365	Custom User Data:	Using XPath
Argent Omega For SNMP		Match Case
Argent Omega For SQL Server		ratu tese
Image:		Match Whole Word
✓ Alerts		Match Regular Expression
Correction		
Find Alert Macro	Events In Time Range:	00:00:00 - 23:59:59
Manitoring Groups	Alert Only If The Specific Event Happens I	lore Than 1 Times
Belators	Alert If The Specific Event Does NOT Exist	
✓ Macros	Treat Events With Same Event ID, Source	And Type As Same Events (Ignore Event Message)
Email Recipients	Retrieve Performance Metric From XPath:	
SMS Recipients	Performance Object Name:	Use As XPath
Windows Services	Counter Name:	
Windows Processes	counter nume.	
Users	Instance Name:	Use As XPath
	Machine Name:	(default) Use As XPath
Base Definitions	Correct Event If Seeing Event Id Of Same	Source:
Holidays		

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 OME	GA (2.2A-2207-A)	میں اور کی ک Home Theme - Argent Instant Help About Logout
	Event Log Name:	Application Reload
Argent Omega Baseline	Event Severity:	Critical Error
Argent Compliance Automator	Event ID:	1-9999
Windows Compliance Rules		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 -
EVT_AUDIT_FAILURE	Rule View:	Simple •
EVT_SYSTEM_ERROR	Ignore Event Log Records Over:	
Windows File Log Rules	Fire Event With Format:	30 Timoxo
LINUX Or Unix File Log Rules		System Default Undividual Combined With Latest Event Message Combined With Full Event Message
SYSLOG Rules	— Additional Event Log Filtering Criteria —	
SQL Server Log Rules	Event User:	*
Microsoft 365 Audit Log Rules	Event Category:	·
PowerSneil Script Log Rules	Event Source:	•
Argent Omega For SNMP	Custom User Data:	Using XPath
Argent Omega For SQL Server		Match Case
Argent Omega Web Defender		Match Whole Word
▼ 🖬 Alerts		Match Recular Expression
Correction		
Notification	Events In Time Range:	00:000 - 23:59:59
Alert Macro	Alert Only If The Specific Event Happens	ore Than 1 Times
Monitoring Groups	Alert If The Specific Event Does NOT Exist	
Relators	Treat Events With Same Event ID. Source	And Tune As Same Events (Innore Event Messare)
✓ Macros	Ratriava Derformance Metric From VDath:	
Email Recipients		
 SMS Recipients Mindews Caprices 	Performance Object Name:	Use As XPath
Windows Processes	Counter Name:	Use As XPath
▶ III Users	Instance Name:	Use As XPath
🔻 🖬 Calendars	Machine Name:	{default}
Base Definitions	Correct Event If Seeing Event 14 of Com-	
+ 🖬 Holidays 🗸 🗸	Correct Event in Seeing Event to Or Same	

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)

= ARGENT OM	IEGA (2.2A-2207-A)	تې ۲۵ کې ۲۵ کې ۲۵ کې Home Theme - Argent listant Help About Logout
	Event Log Name:	Application v Reload
Argent Omega Baseline	Event Severity:	Critical,Error 🔹
Argent Compliance Automator	Event ID:	1-99999
Windows Event Log Rules		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
EVT_APPLICATION_ERROR	Read Windows Event Log With Method:	Automatically Determined 🔹
EVT_AUDIT_FAILURE	Rule View:	Simple 👻
EVT_SYSTEM_ERROR	Ignore Event Log Records Over:	30 Minutes V
Windows File Log Rules	Fire Event With Format	
LINUX Or Unix File Log Rules	Addisional Front Lee Filterine Criteria	System Default Sindividual Combined with Latest Event Message Combined with Full Event Message
SYSLOG Rules	Additional Event Log Filtering Criteria –	
SQL Server Log Rules	Event Oser:	
Plicrosoft 365 Audit Log Rules	Event Category:	
Argent Omena For Microsoft 355	Event Source:	
Argent Omega For SNMP	Custom User Data:	Using XPath
Image: Argent Omega For SQL Server		Match Case
Argent Omega Web Defender		Match Whole Word
Merts		Match Regular Expression
Correction		
Notification	Events In Time Range:	00:00:00 - 23:59:59
Alert Macro	Alert Only If The Specific Event Happens	More Than 1 🗘 Times
Monitoring Groups	Alert If The Specific Event Does NOT Exis	
Relators	Treat Events With Same Event ID, Source	And Type As Same Events (Ignore Event Message)
Macros	Retrieve Performance Metric From XPath:	
SMS Recipients	Borformanco Object Name:	
Windows Services	Performance object Name.	
Windows Processes	Counter Name:	Use As XPath
🕨 🔤 Users	Instance Name:	Use As XPath
Calendars	Machine Name:	{default}
Base Definitions	Correct Event If Seeing Event Id Of Same	source:
Holidays		

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:

= ARGENT OME	GA (2.2A-2207-A)	ec: بیش فری وی Home Theme* Argent Instant Help About Logout
	Event Log Name:	Application Reload
Argent Omega Baseline	Event Severity:	Critical, Error •
 In Argent Compliance Automator 	Event ID:	1-9999
Windows Compliance Rules		Include OF Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Criteria, Type A Minus Sian First. For Example 1.3.5-9976
Windows Event Log Rules	Read Windows Event Log With Method:	Automatically Determined
EVT_AUDIT_FAILURE	Rule View:	Simule
EVT_SYSTEM_ERROR	Ignore Event Log Records Over:	
Windows File Log Rules		30 Minutes
LINUX Or Unix File Log Rules	Fire Event With Format:	🗑 System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔷 Combined With Full Event Message
SYSLOG Rules	Additional Event Log Filtering Criteria -	
SQL Server Log Rules	Event User:	-
Microsoft 365 Audit Log Rules	Event Category:	
PowerShell Script Log Rules	Event Source:	
Image: Argent Omega For Microsoft 365	Custom User Data:	Using XPath
Argent Omega For SNMP		Match Case
Argent Omega For SQL Server		Match Whole Wood
Algent Onlega web berenden		
> Correction		atch Regular Expression
Interview Notification	Events In Time Bange:	00-00-00 + 22-50-50
Alert Macro	Alert Only If The Specific Event Happens	
Monitoring Groups	Alert Only I The Specific Event Rappens	
Relators	Alert If The Specific Event Does NOT Exis	
👻 🚧 Macros	Treat Events With Same Event ID, Source	And Type As Same Events (Ignore Event Message)
Email Recipients	Retrieve Performance Metric From XPath:	
SMS Recipients	Performance Object Name:	Use As XPath
Windows Services	Counter Name:	Use As XPath
Windows Processes	Instance Name:	Use As XPath
 Users Colondara 		
Calculats	machine Name:	(Geraut) use as xPath
 Base Deminuons Holidays 	Correct Event If Seeing Event Id Of Same	e Source:
Holidays		

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

= ARGENT OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	('') Argent Instant Help	? About	ပု Logout	Re4s
👻 📔 Tool Sets	Event Log Name:	Application	Reload					i i i i i i i i i i i i i i i i i i i
Argent Omega Baseline	Event Severity:	Critical,Error 🗸						
Argent Compliance Automator	Event ID:	1-99999						
Windows Compliance Rules		Include Or Exclude Event IDs. Enter ID Numbers And/Or ID Ranges Separated By Commas. To Exclude Criter	ria, Type A Minus	Sian First. For	Example 1.3.5-9976			
Windows Event Log Kales	Read Windows Event Log With Method:	Automatically Determined						
EVT_AUDIT_FAILURE	Rule View:	Simple						
EVT SYSTEM ERROR	Ignore Event Log Records Over:							
Windows File Log Rules	Ignore Event Log Records Over.	30 T Minutes T						
LINUX Or Unix File Log Rules	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Even	nt Message					
SYSLOG Rules	- Additional Event Log Filtering Criteria -							
SQL Server Log Rules	Event User:	*						
Microsoft 365 Audit Log Rules	Event Category:	*						
PowerShell Script Log Rules	Event Source:	×						
Argent Omega For Microsoft 365	Custom User Data:	Using XPath						
Argent Omega For SNMP		Match Case						
Argent Omega For SQL Server		Plateir case						
Argent Omega Web Defender		Match Whole Word						
✓ I Alerts		Match Regular Expression						
Correction	L							
Notification	Events In Time Range:	00:00:00 - 23:59:59						
Alert Macro	Alert Only If The Specific Event Happens	s More Than 1 🗘 Times						
Monitoring Groups	Alert If The Specific Event Does NOT Exis	st						
	Treat Events With Same Event ID, Source	e And Type As Same Events (Ignore Event Message)						
Email Recipients	Retrieve Performance Metric From XPath:	N						
SMS Recipients	Performance Object Name:	Use As XPath						
Windows Services	Country Name							
Windows Processes	counter Name:	USE AS APALIT						
Users	Instance Name:	Use As XPath						
👻 🖬 Calendars	Machine Name:	{default}						
Base Definitions	Correct Event If Seeing Event Id Of Same	ne Source:						
Holidays	Seeing Event to or Same							

The Rule View can be defined as Simple or Advanced:

■ ARGENT OMEGA (2.2A-2207-A)	RC4 合一 で で ひ Home Theme * Argent Instant Help About Logout
▼ 🐸 Tool Sets 🗧 Event Log Name:	Application V Reload
Argent Omega Baseline Event Severity:	Critical, Error
Argent Compliance Automator Event ID:	1-00000
Windows Compliance Rules	Le Include Or Evolutio Event The Enter TD Numbers And/Or TD Bannes Senarated By Commas: To Evolutio Orbitalia Tune A Minus Sinn Eirst: Enr Evanuela 1 3 5-09 -75
Windows Event Log Rules	and the characteristic processed
EVT_APPLICATION_ERROR Read windows Event Log with Me	loo: Automatically betermined
EVT_AUDIT_FAILURE Rule View:	Simple •
EVI_SYSTEM_ERROR 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 C	riteria
SOL Server Log Rules	-
Microsoft 365 Audit Log Bules Event Category:	
PowerShell Script Log Rules	
Argent Omega For Microsoft 365	
Custom User Data:	Using XPath
Index of the second secon	Match Case
▶ 🖬 Argent Omega Web Defender	Match Whole Word
▼ 🖬 Alerts	Match Regular Expression
Correction	
Notification Events In Time Range:	00:00:00 - 23:59:59
Alert Macro Alert Only If The Specific Event	Hannens More Than
Monitoring Groups	
Relators	
✓ Macros), source and type as same events (ignore event message)
Email Recipients	n XPath:
SMS Recipients Performance Object Name:	Use As XPath
Windows Services Counter Name:	Use As XPath
Windows Processes	
Users Instance wante:	
▼ Calendars Machine Name:	(default) Use As XPath
Base Definitions Correct Event If Seeing Event Is	Of Same Source:

When using the Advanced Rule View, it is possible to use the Advanced Event Filter String option using

XPath or PowerShell:

= ARGENT OME	GA (2.2A-2204-T1) Pro-Produ					Home	theme -	(1) Argent Instant Help	? About	ن Logout	RC4S
✓	Event Log Name:	Application			-	Reload					
Argent Omega Baseline	Event Severity:	Critical,Error									
 Argent Compliance Automator 	Event ID:	1-99999									
Windows Compliance Rules	Read Windows Event Log With Method	Automatically Del	ermined 👻	1							
Windows Event Log Rules	Pulo View:	Advanced	-	1							
	Rule view:	Advanced									
	Ignore Event Log Records Over:	30	🗘 Minutes 👻								
Windows File Lon Rules	Fire Event With Format:	System Defaul	t 🔵 Individual 🔵 Comb	ined With Latest Event Message	Combined With Full Eve	nt Message					
LINUX/Unix File Log Rules	Advanced Event Filter String:										
SYSLOG Rules											
SQL Server Log Rules											
Microsoft 365 Audit Log Rules											
PowerShell Script Log Rules											
Argent Omega Web Defender						4					
Argent Omega For Microsoft 365	Events In Time Range:	00:00:00	- 23:59:59								
Argent Omega For SQL Server	Alert Only If The Specific Event Happens	More Than	1	Times							
Alerts	Alert If The Specific Event Does NOT Exis	t									
Monitoring Groups	Treat Events With Same Event ID, Source	And Type As Same	e Events (Ignore Event Mes	age)							
Relators	Retrieve Performance Metric From XPath:										
Macros	Performance Object Name			Use As XPath							
Calendars	Performance object Name.			Ose As Aradi							
 Administration 	Counter Name:			Use As XPath							
Ticense (Admin Only)	Instance Name:			Use As XPath							
Generator Settings	Machine Name:	-{def	ault}	Use As XPath							
Argent Onega	Correct Event If Seeing Event Id Of Same	Source:									
Argent Argent Forecaster			0.3426								
d ^o Argent SIEM-Complete	Save Matching Events To Archive Reposite	ory: (def	ault}	×							
SIEM Policy	Save Archive Data Only										

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:

= ARGENT OME	GA (2.2A-2207-A)	۲۵۵۵ ۲۵۵۹ CO CO Home Theme ★ Argent Instant Help About Logout
👻 🔚 Tool Sets	Event Log Name:	Application relation
Argent Omega Baseline	Event Severity:	Critical, Error •
 Image: Argent Compliance Automator 	Event ID:	1-99999
Windows Compliance Rules		Include OF Exclude Event IDs. Enter ID Numbers And/Or ID Rances Senarated By Commas. To Exclude Criteria. Type A Minus Sian First. For Example 1.3.5-99-76
Windows Event Log Rules	Read Windows Event Log With Method:	Automatically Determined
	Rule View:	Simple
EVT SYSTEM ERROR	Impore Event Log Records Overs	
Windows File Log Rules	Ignore Event Log Records Over:	30 T Minutes
LINUX Or Unix File Log Rules	Fire Event With Format:	🗑 System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔹 Combined With Full Event Message
SYSLOG Rules	- Additional Event Log Filtering Criteria -	
SQL Server Log Rules	Event User:	
Microsoft 365 Audit Log Rules	Event Category:	
PowerShell Script Log Rules	Event Source:	
Argent Omega For Microsoft 365	Custom User Data:	Using XPath
Argent Omega For SNMP		
Argent Omega For SQL Server		
Argent Omega Web Defender		Match Whole Word
✓ Alerts		Match Regular Expression
Correction		
Notification	Events In Time Range:	00:00:00 - 22:59:59
Alert Macro	Alert Only If The Specific Event Happens	More Than 1 Times
Belators	Alert If The Specific Event Does NOT Exis	t
✓ Macros	Treat Events With Same Event ID, Source	And Type As Same Events (Ignore Event Message)
Image:	Retrieve Performance Metric From XPath:	
SMS Recipients	Performance Object Name:	Use As XPath
Windows Services	Counter Namo	
Windows Processes	counter Name.	USE PS Areus
Users	Instance Name:	Use As XPath
✓ III Calendars	Machine Name:	(default) Use As XPath
Base Definitions	Correct Event If Seeing Event Id Of Same	≥ Source:
Holidays		

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

■ ARGENT OME	GA (2.2A-2207-A)			de Home	🔅 Theme -	ر ش Argent Instant Help	? About	U Logout	Re4s
👻 🔚 Tool Sets	- Additional Event Log Filtering Criteria								
🕨 🔤 Argent Omega Baseline	Event User:	e							
 Argent Compliance Automator 	Event Category:								
Windows Compliance Rules									
▼ Windows Event Log Rules	Event Source:								
EVT_APPLICATION_ERROR	Custom User Data:		Using XPath						
EVT_AUDIT_FAILURE		Match Case							
EVT_SYSTEM_ERROR		Match Whole Word							
Windows File Log Rules		Match Regular Expression							
LINUX Or Unix File Log Rules		Match Regular Expression							
SYSLOG Rules	Events In Time Panger	22:50:50							
SQL Server Log Rules	Events in time kange:								
Microsoft 365 Audit Log Rules	Alert Only If The Specific Event Happens Mo	bre Than 1	Times						
PowerShell Script Log Rules	Alert If The Specific Event Does NOT Exist								
Argent Omega For Microsoft 365	Treat Events With Same Event ID, Source A	nd Type As Same Events (Ignore Event M	tessage)						
Argent Omega For SNMP	Retrieve Performance Metric From XPath:								
Argent Omega For SQL Server	Performance Object Name		Line As Visth						
🕨 🖬 Argent Omega Web Defender	Performance object Name.		Use As APadi						
🔻 🐸 Alerts	Counter Name:		Use As XPath						
Correction	Instance Name:		Use As XPath						
Notification	Marking Marya	C 1 - C - 103							
Alert Macro	Hachine Name:	{derault}	Use As APadri						
Monitoring Groups	Correct Event If Seeing Event Id Of Same S	iource:							
Relators	Save Matching Events To Archive Repository	{default}	•						
✓ Macros									
Email Recipients	Save Archive Data Only								
SMS Recipients	Alert If Failed To Open Windows Event Log								
Windows Services	Save Performance Data To The Argent Forec	caster Using Data Store: {default}	~						
Windows Processes	Tag 1:								
Users	Tag 2:								
💌 🐸 Calendars	Tag 3:								
Base Definitions	Post Event Even If The Same Event Is Still (Outstanding (Unanswered)							
🕨 🖬 Holidays		Aliante Cines Front In Deat							

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:**

= ARGENT OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	ر ٹ) Argent Instant Help	? About	U Logout	RC4S
								1
🕨 🐸 Argent Omega Baseline								
✓ III Argent Compliance Automator								
Windows Compliance Rules	Event Category:							
✓	Event Source:							
EVT_APPLICATION_ERROR	Custom User Data:	Using XPath						
EVT_AUDIT_FAILURE	Match	Case						
EVT_SYSTEM_ERROR	Match	Whole Word						
Windows File Log Rules		Reserved as a second as						
LINUX Or Unix File Log Rules	Match	Regular Expression						
SYSLOG Rules								
SQL Server Log Rules	Events in time kange: 00:00:00	- 23:59:59						
Microsoft 365 Audit Log Rules	Alert Only If The Specific Event Happens More Than	1 🔁 Times						
PowerShell Script Log Rules	Alert If The Specific Event Does NOT Exist							
Argent Omega For Microsoft 365	Treat Events With Same Event ID, Source And Type	As Same Events (Ignore Event Message)						
Argent Omega For SNMP	Retrieve Performance Metric From XPath:							
Argent Omega For SQL Server	Performance Object Name	Lice As YPath						
Argent Omega Web Defender	r chomanee object namer							
✓ Merts	Counter Name:	Use As XPath						
Correction	Instance Name:	Use As XPath						
Notification	Machine Name:	(default)						L
Alert Macro								
Monitoring Groups	Correct Event If Seeing Event Id Of Same Source:							
Relators	Save Matching Events To Archive Repository:	{default}						
✓ Macros	Save Archive Data Only							
Email Recipients	Alert If Failed To Open Windows Event Log							
SMS Recipients	Save Performance Data To The Argent Forecaster II	ino Data Store: {default}						
Windows Services	Tag 1:	ang bata starat						
Windows Processes	Top 2:							
Users								
✓ Calendars	Tag 3:							
Base Definitions	Post Event Even If The Same Event Is Still Outstand	ing (Unanswered)						
Holidays	Do So Only After 1 Hour 0 📥 N	inute Since Event To Doct						

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).
= ARGENT OME	GA (2.2A-2207-A)			😭 Home	🛟 Theme -	ে) Argent Instant Help	? About	ل Logout	RC4S
👻 🔚 Tool Sets	- Additional Event Log Filtering Criteria								
🕨 🕍 Argent Omega Baseline	Event User:								
Argent Compliance Automator	Event Category:								
Windows Compliance Rules	Event Courses								
▼ Windows Event Log Rules	Event Source:								
EVT_APPLICATION_ERROR	Custom User Data:	Using XPath							
EVT_AUDIT_FAILURE	Match	Case							
EVT_SYSTEM_ERROR	Match	Whole Word							
Windows File Log Rules	Match	Regular Expression							
LINUX Or Unix File Log Rules		regular Expression							
SYSLOG Rules	Events In Time Range: 00:00:00	- 23:59:59							
SQL Server Log Rules	Alert Only If The Specific Event Hannens More Than	1 Times							
Microsoft 365 Audit Log Rules	Alast If The Coordia Duant Date NOT Fuist								
Powershell Script Log Rules	Wert if the specific Event boes not Exist								
Argent Omega For Microsoft 365	Ireat Events With Same Event ID, Source And Type	As Same Events (Ignore Event Message)							
Argent Omega For SOL Server	Retrieve Performance Metric From XPath:								
Argent Omega Web Defender	Performance Object Name:		Use As XPath						
 Algente onnega web berenden 	Counter Name:		Use As XPath						
> Correction	Tesheese Manual								
Notification	Instance Name:		Use as XPath						
Alert Macro	Machine Name:	{default}	Use As XPath						
Monitoring Groups	Correct Event If Seeing Event Id Of Same Source:]						
Relators	Save Matching Events To Archive Repository:	{default}							
👻 🕍 Macros		1	•						
Email Recipients	Save Archive Data Only								
SMS Recipients	Alert If Failed To Open Windows Event Log								
Windows Services	Save Performance Data To The Argent Forecaster Us	ing Data Store: {default}	*						
Windows Processes	Tag 1:								
Users	Tag 2:								
✓ III Calendars	Tag 3:								
Base Definitions	Post Event Even If The Same Event Is Still Outstandi	ng (Unanswered)							
Holidays	Do So Only After 1 Hour 0 Mi	nute Since Event Ic Doct							

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.

= ARGENT OME	GA (2.2A-2207-A)	Home	theme -	(1) Argent Instant Help	? About	U Logout	RC45
	Additional Event Log Filtering Criteria						
🕨 🔚 Argent Omega Baseline							
👻 🔚 Argent Compliance Automator							
Windows Compliance Rules	event Category:						
▼	Event Source:						
EVT_APPLICATION_ERROR	Custom User Data: Using XPath						
EVT_AUDIT_FAILURE	Match Case						
EVT_SYSTEM_ERROR	Match Whole Word						
Windows File Log Rules	Match Regular Expression						
LINUX Or Unix File Log Rules							
SYSLOG Rules	Events In Time Range: 00:00:00 - 23:59:59						
SQL Server Log Rules	Alert Only If The Sperific Event Hannens More Than						
Microsoft 365 Audit Log Rules							
PowerShell Script Log Rules	Alert in the specific event boes NOT Exist						
Argent Omega For Microsoft 365	Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)						
Argent Omega For SNMP	Retrieve Performance Metric From XPath:						
Argent Omega For SQL Server	Performance Object Name:						
Argent Omega web berender	Counter Name:						
Alerts Alerts							
Notification	Instance Name:						
Alert Macro	Machine Name: {default} Use As XPath						
Monitoring Groups	Correct Event If Seeing Event Id Of Same Source:						
Relators	Save Matching Events To Archive Repository:						
→ Macros	Sare naculing Events to A cline repository. (deadure)						
Email Recipients	Save Archive Data Only						
SMS Recipients	Alert If Failed To Open Windows Event Log						
Windows Services	Save Performance Data To The Argent Forecaster Using Data Store: (default)						
Windows Processes	Tag 1:						
Users	Tag 2:						
👻 🔚 Calendars	Tag 3:						
Base Definitions	Post Event Even If The Same Event Is Still Outstanding (Unanswered)						
Holidays	Do So Oply After Alexandre Concerning Concerning Street						

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:

■ ARGENT OMEGA (2.24	-2207-A)			et al anti-	e Theme -	८ ७) Argent instant Help	? About	U Logout	RC49
✓	event Log Filtering Criteria								
Argent Omega Baseline	r: *		7						
Argent Compliance Automator Event Cate	egory:								
Windows Compliance Rules									
▼ Windows Event Log Rules									
EVT_APPLICATION_ERROR	Jer Data:		Using XPath						
EVT_AUDIT_FAILURE	Match (Case							
EVT_SYSTEM_ERROR	Match '	Whole Word							
Windows File Log Rules	Match	Regular Expression							
LINUX OF UNIX File Log Rules									
Events In	Time Range: 00:00:00	- 23:59:59	7						
Alert Only	If The Specific Event Happens More Than	1	Times						
PowerShell Script Log Rules	e Specific Event Does NOT Exist		-						
Argent Omega For Microsoft 365	nts With Same Event ID. Source and Type	As Same Events (Innore Event Me	(906326						
Argent Omega For SNMP Retrieve D	Performance Matric From VBath								
Argent Omega For SQL Server	enomance rieute nom Aradi.								
Performan	ce Object Name:		Use As XPath						
✓ Merts	ame:		Use As XPath						
Correction Instance N	lame:		Use As XPath						
Notification	lamo	(4-6-34)	Use As VPath						
▶ Macro	anne.	(deradic)	Use As Apaul						
Monitoring Groups	ent If Seeing Event Id Of Same Source:								
▶ 🔤 Relators 🖉 Save Mato	hing Events To Archive Repository:	{default}	*						
✓ Macros Save Arch	ive Data Only								
Email Recipients	iled To Onen Windows Event Log								
SMS Recipients Save Perf	ormance Data To The Argent Forecaster Us	ing Data Store: {default}	*						
Windows Services Tag 1:	Annance beta to the Argent forecaster oa	(denoid)							
Windows Processes									
Vers 1 ag 2.									
Calendars Iag 3:									
Post Event	t Even If The Same Event Is Still Outstandi	ing (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:

■ ARGENT OME	GA (2.2A-2207-A)	A C C C C C C C C C C C C C C C C C C C
👻 🖬 Tool Sets	- Additional Event Log Filtering Criteria	
🕨 🔚 Argent Omega Baseline	Event liser:	
🔻 🔚 Argent Compliance Automator	Fuent Category	
Windows Compliance Rules		
✓ Windows Event Log Rules	Event Source:	
EVT_APPLICATION_ERROR	Custom User Data:	
EVT_AUDIT_FAILURE	Match Case	
EVT_SYSTEM_ERROR	Match Whole Word	
Windows File Log Rules	Match Regular Evencerian	
LINUX Or Unix File Log Rules	Hatur Kegular Expression	
SYSLOG Rules	Events In Time Range: 00:00:00 - 23:59:59	
SQL Server Log Rules	Alast Only If The Constitutioners Mare Then	
Microsoft 365 Audit Log Rules		
PowerShell Script Log Rules	Alert If The Specific Event Does NOT Exist	
Argent Omega For Microsoft 365	Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)	
Argent Omega For SNMP	Retrieve Performance Metric From XPath:	
Argent Omega For SQL Server	Performance Object Name:	
Argent Omega Web Derender	Counter Name:	
Alerts		
Correction	Instance Name:	
Notification	Machine Name: [default] Use As XPath	
Alert Macro	Correct Event If Seeing Event Id Of Same Source:	
Pointoring Groups		
× Macros	Save Matching Events to Archive Repository:	
Email Recipients	Save Archive Data Only	
SMS Recipients	Alert If Failed To Open Windows Event Log	
Windows Services	Save Performance Data To The Argent Forecaster Using Data Store: {default}	
Windows Processes	Tag 1:	
Users	Tag 2:	
✓ I Calendars	Tag 3:	
Base Definitions	Dost Even If The Same Event Is Still Outstanding (Unanswered)	
Holidays		

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.

		<u>~</u>	~	ச ர்)	0	ф	RC4S
= ARGENT OME	GA (2.2A-2207-A)	Home	Theme -	Argent Instant Help	About	Logout	
Tool Sets							
Argent Omega Baseline	Additional Event Log Filtering Criteria						
Argent Compliance Automator	Event User:						
Windows Compliance Rules	Event Category:						
Vindows Event Log Rules	Event Source:						
EVT APPLICATION ERROR	Custom User Data: Using XPath						
EVT_AUDIT_FAILURE	Match Case						
EVT_SYSTEM_ERROR	Natab Weed						
Windows File Log Rules	Platch whole word						
LINUX Or Unix File Log Rules	Match Regular Expression						
SYSLOG Rules							
SQL Server Log Rules	Events In Time Range: 00:00:00 - 23:59:59						
Microsoft 365 Audit Log Rules	Alert Only If The Specific Event Happens More Than 1 💭 Times						
PowerShell Script Log Rules	Alert If The Specific Event Does NOT Exist						
Argent Omega For Microsoft 365	Treat Events With Same Event ID, Source And Type As Same Events (Ignore Event Message)						
Argent Omega For SNMP	Retrieve Performance Metric From XPath:						
Argent Omega For SQL Server	Defense of the Manage						
🕨 🔤 Argent Omega Web Defender	Performance Object Name.						
✓ III Alerts	Counter Name: Use As XPath						
Correction	Instance Name: Use As XPath						
Notification	Machine Name:						L
Alert Macro	Tacline Name.						
Monitoring Groups	Correct Event If Seeing Event Id Of Same Source:						
Relators	Save Matching Events To Archive Repository: (default)						
👻 🚧 Macros	Save Archive Data Only						
Email Recipients							
SMS Recipients	Alert Ir hailed to Open Windows Event Log						
Windows Services	Save Performance Data to The Argent Forecaster Using Data Store: (default)						
Windows Processes	lag 1:						
Users	Tag 2:						
✓ III Calendars	Tag 3:						
Base Definitions	Post Event If The Same Event Is Still Outstanding (Unanswered)						
🕨 🖬 Holidays 🗸 🗸	Do So Oply After Super A Minute Since Super to Dect						

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 OME	GA (2.2A-2207-A)		😭 Home	🔅 Theme -	ڑ¢) Argent Instant Help	? About	U Logout	RC5S
✓	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log F	ile			ŕ
Argent Omega Baseline		Sile Name In Regular Everancian		-				
 Argent Compliance Automator 								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By 0						
WINDOWS FILE LOG RULES		Read Only Last 10 C Megabytes						
IIII LOS ACCINE SQL ENCON	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	vyyy-MM-dd HH:mm:ss.nn	Format	Verify And Ex	plain			
SQL Server Log Rules								
Microsoft 365 Audit Log Rules		Date Or Time In Log File Is UTC Time						
PowerShell Script Log Rules	Ignore File Log Records Over:	30 🗘 Minutes 👻						
Argent Omega For Microsoft 365	Fire Event With Format:	🔵 System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔵 Combined With Full Event I	Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains						
Argent Omega Web Defender		Include Or Exclude Keywords, Enter Keywords Separated By Commas, To Exclude Criteria, Type A Minus Sign I	First. To Escape	Comma				
✓ Alerts		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Correction		Match Case						
 Notification Individual Macro 		Match Whole Word						
Monitoring Groups		Match Regular Expression						
▶ M Relators								
✓		asign event 10: 9,999						
Email Recipients	Events In Time Range:	000000 - 5323020						
SMS Recipients	Alert Only If The Specific Event Happen:	More Than 1 Times						
Windows Services	Alert If The Specific Event Does NOT Ex	st						
Windows Processes	Alert Message Include	0 🗘 Lines Before And 🛛 0 🗘 Lines After						
Users	Correct Condition If Log Line	Contains 👻						
▼ Mathematical Calendars	Save To Archive Repository:	(default)						
Base Definitions	Archive All Log Lines							
Holidays	Anakira Matakira Las Lines							
Administration	Archive Matching Log Lines							
Ticense (Admin Only)	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 OME	GA (2.2A-2207-A)		Home	theme -	्र ्ण Argent Instant Help	? About	U Logout	RC5S
▼ 📶 Tool Sets	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log File	e			ŕ
Argent Omega Baseline		File Name Is Regular Expression		-				
Windows Compliance Rules		Ise Yesterday's Date for Date Or Time Variables Used In File Path						
Windows Event Log Rules		Dias Data Os Time Veriables Hand In Cile Data Dr.						
▼								
MUN_LOG_ARCHIVE_SQL_ERROR		Read Only Last 10 C Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Expl	lain			
SQL Server Log Rules		Date Or Time In Log File Is UTC Time		_				
Microsoft 365 Audit Log Rules	Ignore File Log Records Over:	20 Minutes						
PowerShell Script Log Rules	Eiro Event With Formati							
Argent Omega For Pilcrosoft 305	File Event with Format.	System Default Individual Combined With Latest Event Message Combined With Full Event	nt Message					
Argent Omega For SQL Server	Use Advanced Rule Definition:							
Argent Omega Web Defender	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
✓ III Alerts		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sig And Minus Sign Proceed With Character 'V' Wildcarde '8' And '2' Are Supported	in First. To Escap	e Comma				L
Correction		Match Care						
Motification								
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
▶ Mathematics		Assign Event ID: 9,999						
Macros	Events In Time Range:	00:00:00 - 23:59:59						
SMS Recipients	Alert Only If The Specific Event Happer	is More Than 1 🗘 Times						
Windows Services	Alert If The Specific Event Does NOT E	dist						
Windows Processes	Alert Message Include	0 🗘 Lines Before And 0 💭 Lines After						
Users	Correct Condition If Log Line	Contains						
✓	Save To Archive Repository:	/dafault3						
Base Definitions		(annu)						
🕨 🚾 Holidays	Archive All Log Lines							
 Administration 	Archive Matching Log Lines							
Ticense (Admin Only)	Archive If Log Line	Contains 👻						

$\leftrightarrow \rightarrow \mathbf{C}$ (i) localhost:6100/ap	//Omegatysteminlo/DownloadTextLog7log=C%34%5CProgram%20File%55CMicrosoft%205QL%20Sever%SCMSSQL13MSSQLSERVER%5CMSSQL%2CLog%SCERRORLOG&machine=A1-WEB-47&use_regex=false 🖻 🖈 😰 🚦
2022-03-09 10:53:01.66 Server Apr 29 2016 23:23:58 Copyright (c) Microsoft Co	Microsoft SQL Server 2016 (RTM) - 13.0.1601.5 (X64) rporation
Express Edition (64-bit) o	n Windows 10 Pro 6.3 <x64> (Build 19044:) (Hypervisor)</x64>
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 10 15 0052.
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\Micro	SOTE SQL Server VISQULS. ISSQLSERVER VISQULVA A NIBSTET. INF
-1 C:\Program Files\Micro	Soft SD Server VISSOL3 XISSOLSEVER VISSOLVATA Mastlag. 1df
2022-03-09 10:53:01.68 Server	Command Line Startup Parameters:
2022-03-09 10:53:01.71 Server	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
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	surrer pool extension is already disabled. No action is necessary.
2022-03-09 10:53:03.44 Server	Includent control of the second
2022-03-09 10:53:03.91 Server	The maximum number of dedicated administrator connections for this instance is '1'
2022-03-09 10:53:03.95 Server	This instance of SQL Server last reported using a process ID of 5380 at 3/9/2022 10:52:25 AM (local) 3/9/2022 5:22:25 AM (UTC). This is an informational message only; no user action is required.
2022-03-09 10:53:03.98 Server	Node configuration: node 0: CPU mask: 0x00000000000000000000 Active CPU mask: 0x00000000000000000000000000000000000
action is required.	When descriptions and a state of and the black and the black are black and the description and the state of a second and
2022-03-09 10:53:04.00 Server	Using upmail lock allocation: initial allocation or 2000 lock Ducks and 2000 lock under Ducks per mole. Inis is an informational message only. No user action is required. Ducks and informational message only. No user action is Ducksber Instant is allocation. This is an informational message only. No user action is
required.	Annu Share estimate a statistical with enabled a 1
2022-03-09 10:55:04.07 Server	Query store sectings initialized mith employ - 1,
2022-03-09 10:53:04.12 spid5s	[INFO] HMOSOBOCKT::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 10:53:04.35 spid5s	[INFO] HkHostDbCtxt::Initialize(): Database ID: [1] 'master'. XTP Engine version is 0.0.
2022-03-09 10:53:04.43 spid5s	[INFO] HkHostDDCtxt:Initialize(): Database ID: [1] 'master'. XTP Engine version is 0.0.
2022-03-09 10:53:04.61 Server	LLK Version V4.6.3619 108060.
2022-03-09 10:53:05.22 spid5s	SQL Server Addit is started the addits. 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 10:53:05.81 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 spid6s	[INFO] HKHOSTUDECtxt::Initialize(): Database ID: [32/87] 'mssqlsystemresource'. XIP Engine version 15 0.0.
2022-03-09 10:53:05.85 spidios	[INFO] MKHOSTUDITKT:IIITIAIIZE(): UATABASE 10: [4] MSGD . XIP Engine Version 15 0.0.
2022-03-09 10:53:05.85 spid16s	Starting up database "moduly."
2022-03-09 10:53:05.85 spid17s	[INF0] MkHostDbCtxt::Initialize(): Database ID: [17] 'ARGENT_OMEGA'. XTP Engine version is 0.0.
2022-03-09 10:53:05.85 spid17s	Starting up database 'ARGENT_OMEGA'.
2022-03-09 10:53:05.87 spid6s	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 spid6s	Larry mrnusuuutkiiinitaliselyi uutuuutkiiinitalee uu jazong mässaisystemmesuuree . Xiv engine version 15 0.0. INNEN Melaesinthyttyi-toitaijaa) in tahaasa Thi tah "sedia Version is 0.0.
2022-03-09 10:53:05.89 spid10s	[INFO] HkHostDbCtxt::Initialize(): Database ID: [1] AdGKIO (MGGA'. XTP Engine version is 0.0.
2022-03-09 10:53:05.91 spid6s	[INFO] MkHostDbCtxt::Initialize(): Database ID: [32767] 'mssqlsystemresource'. XTP Engine version is 0.0.
2022-03-09 10:53:05.94 spid16s	[INFO] HkHostObCtxt::Initialize(): Database ID: [4] 'msdb'. XTP Engine version is 0.0.
2022-03-09 10:53:06.00 spid6s	[INFO] HkHostDbCtxt::Initialize(): Database ID: [3] 'model'. XTP Engine version is 0.0.
2022-03-09 10:53:06.00 spid6s	Starting up database 'model'.
2022-03-09 10:53:06.01 snid6e	Lamon inside concentration (), because to: [17] model, and concentration to e.e.
2022-03-09 10:53:06.02 spid6s	INFO HkHostDhCtxt: Initialize(): Database ID: [3] 'model', XTD 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 OME	GA (2.2A-2207-A)		de Horne	theme - Ar	(1) gent Instant Help	? About	ن Logout	RC5S
▼ 🐸 Tool Sets	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	/ariables	View Log File				ŕ
🕨 🔚 Argent Omega Baseline		Cile Name Is Desular Conversion						
 Argent Compliance Automator 		File Name Is Regular Expression						
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By 0 🏮 Hours						
 Windows File Log Rules 		Read Only Last 10 Megabytes						
WIN_LOG_ARCHIVE_SQL_ERROR	Scan Option:	The Latest File Only						
EINUX OF UNIX FILE LOG RULES								
SI Server Log Rules	Date Or Time Format:	yyyy-MM-aa HH:mm:ss.nn	Format	Verify And Explain	1			
Microsoft 365 Audit Log Rules		Date Or Time In Log File Is UTC Time						
PowerShell Script Log Rules	Ignore File Log Records Over:	30 💭 Minutes 👻						
Argent Omega For Microsoft 365	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event Mes	ancone					
Argent Omega For SNMP	Use Advanced Bule Definition:		Suge					
Argent Omega For SQL Server	ose Advanced Kule Demittion.							
🕨 🔚 Argent Omega Web Defender	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
👻 🔚 Alerts		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign Firs And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported	rst. To Escape	Comma				_
Correction		Match Care						
Notification		- Match Case						
▶ I Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators	-	Assign Event ID: 0,999 🗘						
👻 🚾 Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happen	More Than 1 Times						
SMS Recipients	Alert If The Specific Event Does NOT Ex	st						
Windows Services	Alert Message Technic Does NOT Ex	A lines Defers And						
Windows Processes	Alerc Plessage Include							
Users	Correct Condition If Log Line	Contains						
Carenuars	Save To Archive Repository:	(default)						
Base Demittors	Archive All Log Lines							
Administration	Archive Matching Log Lines							
License (Admin Only)	Archive If Log Line	Contains						
E exercise (Remmi curk)	Archive tribug time	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:

■ ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme -	ری) Argent Instant Help	? About	U Logout	RC5S
	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log Fil	e			
Argent Omega Baseline		File Name Is Regular Expression						
Argent Compliance Automator		I have been been been for the for the best for the best for the best						
Windows Event Lon Rules		ose resteriday's Date for Date of Hinte variables Osed in File Path						
Vindows File Log Rules		Bias Date Or Time Variables Used In File Path By						
MUN_LOG_ARCHIVE_SQL_ERROR		Read Only Last 10 C Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only -						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Exp	lain			
SQL Server Log Rules		Date Or Time In Log File Is UTC Time						
Microsoft 365 Audit Log Rules	Japore File Log Records Over:							
PowerShell Script Log Rules	Fire Front With Format	30 V Printices						
Argent Omega For Microsoft 365	Fire Event with Format:	System Default OIndividual OCombined With Latest Event Message OCombined With Full Even	nt Message					
Argent Omega For SQL Server	Use Advanced Rule Definition:							
Argent Omega Web Defender	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
✓ III Alerts		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sig	n First. To Escap	e Comma				
Correction		And Minus Sign, Proceed with Character \. Wildcards ~ And 7 Are Supported						
Notification		match case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators		Assign Event ID: 9,999						
 Macros 	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happens	s More Than 1 🗘 Times						
Windows Services	Alert If The Specific Event Does NOT Exi	st						
Windows Processes	Alert Message Include	0 🗘 Lines Before And 0 🔵 Lines After						
▶ 🚾 Users	Correct Condition If Log Line	Contains						
✓	Save To Archive Repository:	(default)						
Base Definitions	Bute to Alenite Repository.	[unuur]						
🕨 🚾 Holidays	Archive All Log Lines							
 Administration 	Archive Matching Log Lines							
Ticense (Admin Only)	Archive If Log Line	Contains 👻						

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:

■ ARGENT OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	ر ش Argent Instant Help	? About	U Logout	RC5S
👻 🔚 Tool Sets	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log File	2			ŕ
Argent Omega Baseline		Cile Name In Regular Expression						
Argent Compliance Automator								
Windows Compliance Rules		Use Yesterday's Date For Date or Time variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By 0 📮 Hours						
MINING ARCHIVE SOL ERROR		Read Only Last 10 💭 Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Expl	lain			
SQL Server Log Rules		Date Or Time In Les File Is UTC Time						
Microsoft 365 Audit Log Rules	Terrora File Los Desente Over							
PowerShell Script Log Rules	Ignore the Log Records Over.	30 Vinutes V						
Image: Argent Omega For Microsoft 365	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	t Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
Argent Omega web Derender		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sigr	n First. To Escape	e Comma				L
 Alerts Correction 		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Notification		Match Case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators	-	Assign Event ID: 9,999						
✓ Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Hannens	More Than 1 Times						
SMS Recipients	Alert If The Specific Event Does NOT Evi	st						
Windows Services	Alert Message Include	Ines Refore And						
Windows Processes	- Helder							
Calendare	Correct Condition If Log Line	Contains •						
Base Definitions	Save To Archive Repository:	{default}						
Holidays	 Archive All Log Lines 							
▼ Mainistration	Archive Matching Log Lines							
License (Admin Only)	Archive If Log Line	Contains 👻						

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



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

■ ARGENT OME	GA (2.2A-2207-A)		🚰 Home	theme -	(1) Argent Instant Help	? About	U Logout	RC55
	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log File				
In Argent Omega Baseline		File Name Is Regular Expression						
Argent Compliance Automator		I have been a start of the Date for Date for Time Veriables Hand to file Date						
Windows Event Log Rules								
Windows File Log Rules		Bias Date Or Time Variables Used In File Path By 0 Hours						
MIN_LOG_ARCHIVE_SQL_ERROR		Read Only Last 10 C Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Expla	ain			
SQL Server Log Rules		Date Or Time In Log File Is UTC Time						
Microsoft 365 Audit Log Rules	Japore File Log Records Over							
PowerShell Script Log Rules								
Argent Omega For Microsoft 365	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	nt Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
✓ Alerts		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sig	in First. To Escap	e Comma				l
Correction		And Philos Sign, Proceed With Character 1, Wildcards - And 7 Are Supported						
Motification		Match Case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators	_	Assign Event ID: 9,999 🗘						
👻 🚾 Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happens	s More Than 1 🗍 Times						
SMS Recipients	Alert If The Specific Event Does NOT Ex	st						
Windows Services	Alert Messane Include	Ines Before And						
windows Processes								
✓ III Calendars	Correct Condition If Log Line	Contains						
Base Definitions	Save To Archive Repository:	{default}						
Holidays	Archive All Log Lines							
👻 🔚 Administration	Archive Matching Log Lines							
📮 License (Admin Only)	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 OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	(') Argent Instant Help	? About	U Logout	RC55
✓	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log Fil	le			
Argent Omega Baseline		File Name Is Regular Expression						
Argent Compliance Automator		I lee Vesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules								
▼ 🐸 Windows File Log Rules		Bias Date Or Time Variables Used In File Path By 0 Hours						
MIN_LOG_ARCHIVE_SQL_ERROR		Read Only Last 10 C Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Exp	olain			
SQL Server Log Rules		Date Or Time In Log File Is UTC Time						
Microsoft 365 Audit Log Rules	Janore File Log Records Over:	an A Minuter						
PowerShell Script Log Rules	Cine Frank With Common							
Argent Omega For Pilcrosoft 365	Fire Event with Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	t Message					
Argent Omega For SQL Server	Use Advanced Rule Definition:							
Argent Omega Veb Defender	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 Sig And Minus Sign, Proceed With Character 'V. Wildcards '*' And '7' Are Supported	in First. To Escape	e Comma				L
Correction		Match Cace						
Notification								
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators	1	Assign Event ID: 9,999						
 Macros 	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients SMS Parinients	Alert Only If The Specific Event Happens	More Than 1 🗘 Times						
Windows Services	Alert If The Specific Event Does NOT Exit	t						
Windows Processes	Alert Message Include	0 💭 Lines Before And 0 🔵 Lines After						
▶ 🔤 Users	Correct Condition If Log Line	Contains						
✓ III Calendars	Save To Archive Renository:	(default)						
Base Definitions	Save to stative Repository.	[acanal]						
🕨 🕍 Holidays	Archive All Log Lines							
 Administration 	Archive Matching Log Lines							
Ticense (Admin Only)	Archive If Log Line	Contains 👻						

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 OME	GA (2.2A-2207-A)		👫 Home	🔅 Theme -	(1) Argent Instant Help	? About	U Logout	RC5S
👻 🔚 Tool Sets	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log Fi	ile			Ê
Argent Omega Baseline		Elle Name Is Regular Expression						
Argent Compliance Automator								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows File Log Rules		Bias Date Or Time Variables Used In File Path By						
M WIN LOG ARCHIVE SOL ERROR		Read Only Last 10 💭 Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Ex	plain			
SQL Server Log Rules		Date Or Time In Lon File Is LITC Time						
Microsoft 365 Audit Log Rules	Ignoro Eilo Log Records Over							
PowerShell Script Log Rules	Ignore File Log Records Over:	30 C Minutes V						
Argent Omega For Microsoft 365	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	t Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
Argent Omega web Derender		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign	n First. To Escape	e Comma				L
 Alerts Correction 		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Notification		Match Case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
▶ 1 Relators	_	Assign Event ID: 9,999						
✓ Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happen	s More Than 1 Times						
SMS Recipients	Alert If The Specific Event Does NOT Ex							
Windows Services	Alert Mercane Technologia	I lines Before And						
Windows Processes	Alert Message Include							
 Users Colordore 	Correct Condition If Log Line	Contains						
Base Definitions	Save To Archive Repository:	{default}						
Holidays	Archive All Log Lines							
✓	Archive Matching Log Lines							
👎 License (Admin Only)	Archive If Log Line	Contains 👻						

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



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

■ ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme - Arg	(® gent Instant Help	? About	ပံ Logout	RC5S
	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log File				i
Argent Omega Baseline		File Name Ic Regular Evoression						
Argent Compliance Automator								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Elle Log Rules		Bias Date Or Time Variables Used In File Path By						
WIN LOG ARCHIVE SOL ERROR		Read Only Last 10 💭 Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Explain				
SQL Server Log Rules		Date Or Time In Log File Is LITC Time						
Microsoft 365 Audit Log Rules	Ignoro Eilo Log Records Over							
PowerShell Script Log Rules	Ignore File Log Records Over:	30 📮 Minutes 👻						
Argent Omega For Microsoft 365	Fire Event With Format:	System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔵 Combined With Full Event Me	essage					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
Argent Omega web Derender		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign Fin	irst. To Escape	Comma				L.
Correction		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Notification		Match Case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators		Assign Event ID: 9,999						
🔻 🔚 Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happen	More Than 1 Times						
SMS Recipients	Alert If The Specific Event Does NOT Ex	et						
Windows Services	Alart Massana Jackuda	A lines Refers And A lines After						
Windows Processes	Alert Hessage Include							
 Colordare 	Correct Condition If Log Line	Contains						
Galerious Base Definitions	Save To Archive Repository:	{default}						
Holidays	Archive All Log Lines							
 Administration 	Archive Matching Log Lines							
Ticense (Admin Only)	Archive If Log Line	Contains 👻						

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

■ ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme -	ڑ) Argent Instant Help	? About	U Logout	RC5S
✓	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log Fi	ile			ŕ
Argent Omega Baseline		Gile Name In Regular Expression		-				
 Argent Compliance Automator 								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By						
MINING ARCHIVE SOL ERROR		Read Only Last 10 🗘 Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only 🔹						
SYSLOG Rules	Date Or Time Format:	vvvv-MM-dd HH:mm:ss.nn	Format	Verify And Exc	plain			
SQL Server Log Rules		Date On Time In Las Sile In 1970 Time						
Microsoft 365 Audit Log Rules		Date of time in Log File is of C time						
PowerShell Script Log Rules	Ignore File Log Records Over:	30 C Minutes						
Argent Omega For Microsoft 365	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	t Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
Argent Omega Web Defender	'	Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sig	n First. To Escap	e Comma				
Alerts		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Notification		Match Case						
Ident Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators		Assign Event ID:						
👻 🕍 Macros	Events In Time Range:	00:00:00						
Email Recipients	Alert Only If The Specific Event Hannens	Mara Than						
SMS Recipients	Alert only if the specific event happens							
Windows Services	Alert If The Specific Event Does NOT Exit							
Windows Processes	Alert Message Include	0 Unes Before And 0 Unes After						
Users	Correct Condition If Log Line	Contains 🔹						
 Calendars Interpretations 	Save To Archive Repository:	{default}						
 Base Deminuons Holidays 	Archive All Log Lines							
Administration	Archive Matching Log Lines							
License (Admin Only)	Archive If Log Line	Contains						
E montre (Hammenn)/	Archive in Log Lille	Contains •						

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:

■ ARGENT OME	GA (2.2A-2207-A)		A Home	theme -	(ग) Argent Instant Help	? About	U Logout	RC55
👻 🕍 Tool Sets	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log File				
🕨 🔚 Argent Omega Baseline		Ella Nama la Regular Expression						
 Argent Compliance Automator 								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By 0 🗧 Hours						
WINDOWS FILE LOG KURES		Read Only Last 10 C Megabytes						
IINUX Or Unix File Log Rules	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Expl	ain			
🕨 📔 SQL Server Log Rules		Date On Time In Las File In 100 Time						
Microsoft 365 Audit Log Rules		Date of lime in Log file is of C lime						
PowerShell Script Log Rules	Ignore File Log Records Over:	30 C Minutes						
Argent Omega For Microsoft 365	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event Message	nt Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
Argent Omega Web Defender		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Si	gn First. To Escap	e Comma				l
Correction		And Minus Sign, Proceed with Character (, Wildcards * And 7 Are Supported						
Notification		Match Case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators	-	Assign Event ID: 9,999						
▼ Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happen	s More Than 1 Times						
SMS Recipients	Alert If The Specific Event Does NOT Ex	st						
Windows Services	Alert Message Include	0 1 Lines Before And 0 1 Lines After						
Windows Processes	Here Hessige Include							
 Galendars 	Correct Condition If Log Line	Contains						
Base Definitions	Save To Archive Repository:	{default}						
▶ 🖬 Holidays	Archive All Log Lines							
👻 🖬 Administration	Archive Matching Log Lines							
👎 License (Admin Only)	Archive If Log Line	Contains 👻						

Argent Software Proprietary Information – All Rights Reserved

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

■ ARGENT OME	GA (2.2A-2207-A)		🛟 Home	Theme -	(णे Argent Instant Help	? About	U Logout	RC5S
✓	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log File	•			ŕ
Argent Omega Baseline		File Name Is Regular Expression						
Argent Compliance Automator		I ha Vastardav's Date Fas Date Or Time Variables Lload In Elle Dath						
Windows Event Lon Rules		ose resterday's bate for bate of nime variables used in file path						
Windows File Log Rules		Bias Date Or Time Variables Used In File Path By 0 Hours						
B WIN_LOG_ARCHIVE_SQL_ERROR		Read Only Last 10 C Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only -						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Expl	ain			
SQL Server Log Rules		Date Or Time In Lon File Is LITC Time						
Microsoft 365 Audit Log Rules	Japore File Log Records Over:							
PowerShell Script Log Rules		30 V Minutes V						
Argent Omega For Microsoft 365	Fire Event with Format:	System Default Individual Combined With Latest Event Message Combined With Full Even	nt Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega For SQL Server	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
✓ Alerts		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sig	n First. To Escap	e Comma				L
Image: Correction		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Notification		Match Case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators	-	Assign Event ID: 9,999 🗘						
✓ Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happens	More Than 1 🗘 Times						
SMS Recipients	Alert If The Specific Event Does NOT Exi	st						
Windows Services	Alert Message Include	Lines Before And						
Windows Processes								
✓ Calendars	Correct Condition if Log Line							
Base Definitions	Save to Archive Repository:	(detaint)						
🕨 🖬 Holidays	Archive All Log Lines							
 Administration 	Archive Matching Log Lines							
Ticense (Admin Only)	Archive 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:**

■ ARGENT OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	ڑی Argent Instant Help	? About	U Logout	RC5S
▼ 🐸 Tool Sets	Log File Path:	C:\Program Files\Microsoft SQL Server\MSSQL14.SQLEXPRESS\MSSQL\Log\ERRORLOG	Variables	View Log Fi	ile			ŕ
Argent Omega Baseline		Ella Nama la Regular Everaccion						
 Image: Argent Compliance Automator 								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By						
MUNICIPAL ARCHIVE SOL ERROR		Read Only Last 10 🗘 Megabytes						
LINUX Or Unix File Log Rules	Scan Option:	The Latest File Only 🔹						
SYSLOG Rules	Date Or Time Format:	yyyy-MM-dd HH:mm:ss.nn	Format	Verify And Ex	plain			
SQL Server Log Rules		Date Or Time In Log File Is LITC Time						
Microsoft 365 Audit Log Rules	Japore File Log Records Over							
PowerShell Script Log Rules	Ignore The Log Records over.	30 Vinutes V						
Argent Omega For Microsoft 365	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event Message	ent Message					
Argent Omega For SNMP	Use Advanced Rule Definition:							
Argent Omega Web Defender	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
✓ III Alerts		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus S And Minus Sian. Proceed With Character '\' Wildcards '*' And '2' Are Supported	ign First. To Escap	pe Comma				_
Correction		Makela Case						
Notification		match case						
Alert Macro		Match Whole Word						
Monitoring Groups		Match Regular Expression						
Relators	-	Assign Event ID: 9,999						
✓ Macros	Events In Time Range:	00:00:00 - 23:59:59						
Email Recipients	Alert Only If The Specific Event Happen	s More Than 1 🗘 Times						
Shis Recipients Windows Services	Alert If The Specific Event Does NOT Ex	ist						
Windows Processes	Alert Message Include	0 C Lines Before And 0 C Lines After						
Users	Correct Condition If Log Line	Contains •						
👻 🔚 Calendars	Save To Archive Repository:	(default)						
Base Definitions		(annul)						
Holidays	Archive All Log Lines							
👻 🔚 Administration	Archive Matching Log Lines							
- License (Admin Only)	 Archive 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 OME	GA (2.2A-2207-A)	🚰 Home	🔅 Theme 🕶	(*) Argent Instant Help	? About	U Logout	RC59
	Match Regular Expression						
🕨 🚧 Argent Omega Baseline	Assian Event ID:						
 Argent Compliance Automator 	Events In Time Paper						
Windows Compliance Rules	Alert Only If The Energies Event Hanness Mars Than						
Windows Event Log Rules							
	Alert in the specific Event Does NOT Exist						
LINUX or Univ Ele Lon Bules	Alert Message Include						
SYSLOG Rules	Correct Condition If Log Line						
SQL Server Log Rules	Save To Archive Repository: (default)						
Microsoft 365 Audit Log Rules	Archive All Log Lines						
PowerShell Script Log Rules	Archive Matching Log Lines						
Argent Omega For Microsoft 365	Archive If Log Line						
Argent Omega For SNMP							
Argent Omega For SQL Server	Save Archive Data Only						
Argent Omega Web Defender	Alert If Failed To Open Log File						
✓ III Alerts	Save Performance Data Io Ine Argent Forecaster Using Data Store: (default)						
Correction	lag 1:						
Notification	Tag 2:						
Alert Macro	Tag 3:						
Monitoring Groups	Post Event Even If The Same Event Is Still Outstanding (Unanswered)						
Relators	Do So Only After 1 C Hour 0 C Minute Since Event Is Post						
Inderios Inderios	Ignore The Same Outstanding Event If Alerts Were Fired More Than 1 📄 Hour 0 🚔 Minute Ago						
SMS Recipients	Post Event Only After Rule Is Broken 2 Or More Times						
In Windows Services	Basel Counter						
Windows Processes	Reset Control						
Users	After Event is Answered						
	After The Actual Condition Is Corrected						
Base Definitions							
Holidays	Application:						
🔻 🖬 Administration	Reference URL:						
Ticense (Admin Only)							

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 OME	GA (2.2A-2207-A)	A Home	🛟 Theme -	ර ^{ා)} Argent Instant Help	? About	U Logout	RC5S
👻 🔚 Tool Sets	Match Regular Expression						
🕨 🔚 Argent Omega Baseline	Andrea Fuerk ID:						
👻 🕍 Argent Compliance Automator	a sayar vent LD. a sayar a						
Windows Compliance Rules	Events in time Range: 00:00:00 - 23:59:59						
Windows Event Log Rules	Alert Only If The Specific Event Happens More Than 1 Times						
✓	Alert If The Specific Event Does NOT Exist						
WIN_LOG_ARCHIVE_SQL_ERROR	Alert Message Include 0 🖨 Lines Before And 0 🚔 Lines After						
LINUX Or Unix File Log Rules	Correct Condition If Log Line Contains						
SYSLOG Rules							
SQL Server Log Rules	inatch Case						
Microsoft 365 Audit Log Rules	Match Whole Word						
PowerShell Script Log Rules	Match Regular Expression						
Argent Omega For Microsoft 365	Save To Archive Repository: (default)						
Argent Omega For SNHP Argent Omega For SOL Server	Archive All Log Lines						
Argent Omega Web Defender	Archive Matching Log Lines						
✓ III Alerts	Archive If Log Line Contains						
Correction	Caue Archive Data Calu						
Interpretation	are Active Data only						
Alert Macro	Alert If Hailed to Open Log File						
Monitoring Groups	Save Performance Data to the Argent Porecaster Using Data Store: (default)						
Relators							
✓ Macros	lag 2:						
Email Recipients	Tag 3:						
SMS Recipients	Post Event Even If The Same Event Is Still Outstanding (Unanswered)						
Windows Services	Do So Only After 1 C Hour 0 Minute Since Event Is Post						
Windows Processes	Ignore The Same Outstanding Event If Alerts Were Fired More Than						
Users	Post Event Only After Rule Is Broken 2 Cr More Times						
 Calendars 							
Base Definitions	Reset Counter						
Holidays	W Arter Event Is Post						
Administration	After Event Is Answered						

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 OME	GA (2.2A-2207-A)		A Home	🔅 Theme •	(ग) Argent Instant Help	? About	U Logout	RC5S
		Match Regular Expression						F
Argent Omega Baseline								
👻 🔚 Argent Compliance Automator		Assign Event ID: 9,999						
Windows Compliance Rules	Events In Time Range:	00:00:00 - 23:59:59						
Windows Event Log Rules	Alert Only If The Specific Event Happe	ns More Than 1 🗘 Times						
👻 🚧 Windows File Log Rules	Alert If The Specific Event Does NOT E	xist						
WIN_LOG_ARCHIVE_SQL_ERROR	Alert Message Include	0 🗘 Lines Before And 0 💭 Lines After						
III LINUX Or Unix File Log Rules	Correct Condition If Log Line	Contains 👻						
SQL Server Log Rules		Match Case						
Microsoft 365 Audit Log Rules		Match Whole Word						
PowerShell Script Log Rules		Match Bagular Evoracsion						
Argent Omega For Microsoft 365	Save To Archive Repository:							
Argent Omega For SNMP	Save to Archive Repository.	(uclauk)						
Argent Omega For SQL Server	Archive All Log Lines							
🕨 🔚 Argent Omega Web Defender	Archive Matching Log Lines							
✓ III Alerts	Archive If Log Line	Contains 👻						
Correction	Save Archive Data Only							
Notification	Alert If Failed To Open Log File							
Alert Macro	Save Performance Data To The Argent	Forecaster Using Data Store: (default)						
Monitoring Groups	Tag 1:							
Relators	Tag 2:							
✓ Macros								
Email Recipients	lag 3:							
SMS Recipients	Post Event Even If The Same Event Is	Still Outstanding (Unanswered)						
Windows Services	Do So Only After 1 Hour	0 C Minute Since Event Is Post						
Windows Processes	Ignore The Same Outstanding Event I	f Alerts Were Fired More Than 1 🗘 Hour 0 🗘 Minute Ago						
Users	Post Event Only After Rule Is Broken	2 Or More Times						
Calendars								
Base Definitions	Reset Counter							
Holidays	After Event Is Post							
 Administration 	After Event Is Answered							
Ticense (Admin Only)	After The Actual Condition Is Correcte							

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 OME	GA (2.2A-2207-A)		de Home	Theme - A	(ग) rgent Instant Help	? About	U Logout	RC6S
▼ 🐸 Tool Sets	Log File Path:	/var/log/auth.log	Variables	View Log File				^
🕨 🔚 Argent Omega Baseline		Cile Name Te Denvies Function						
 Argent Compliance Automator 		The Name is Regular Expression						
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By 0 🟮 Hours						
Windows File Log Rules		Read Only Last 100 🗧 Lines (Only Read Last 100 Lines By Default)						
	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	MMM #d HH:mm:ss	Format	Verify And Explain				
SQL Server Log Rules								
🕨 📔 Microsoft 365 Audit Log Rules		Date Or Time In Log File Is UTC Time						
PowerShell Script Log Rules	Ignore File Log Records Over:	30 C Minutes V						
Argent Omega For Microsoft 365	LINUX Or Unix Command Timeout:	10 Seconds						
Argent Omega For SNMP	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	t Message					
Argent Omega For SQL Server	Use Advanced Rule Definition:							
🕨 🔚 Argent Omega Web Defender								
✓ Merts	Rule 1s Broken If Log Line:	Contains Authentication failure						
Correction		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported	n First. To Escape	e Comma				
Notification		Match Case						
Alert Macro								
Monitoring Groups		Match Whole Word						
 Relators Macros 	1	Match Regular Expression						
Email Recipients		Assign Event ID: 9,999						
SMS Recipients	Events In Time Range:	00:00:00 - 23:59:59						
Windows Services	Alert Only If The Specific Event Happens	More Than 1 🗘 Times						
Windows Processes	Alert If The Specific Event Does NOT Exi	st						
🕨 🔚 Users	Alert Message Include	0 🚔 Lines Before And 🛛 0 🚔 Lines After						
👻 🚾 Calendars	Correct Condition If Los Line	Containe						
Base Definitions	Contect contaition in Edg Ente	Concaris V						
Holidays	Save to Archive Repository:	{derault}						
👻 🔚 Administration	Archive All Log Lines							
Ticense (Admin Only)	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 OM	1EGA (2.2A-2207-A)		den Home	Theme - Ar	(') rgent Instant Help	? About	U Logout	RC6S
	Log File Path:	/var/log/auth.log	Variables	View Log File				
Argent Omega Baseline Argent Compliance Automator		File Name Is Regular Expression						
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By 0 Hours						
Windows File Log Rules		Bead Only Last 100 Lines (Only Read Last 100 Lines By Default)						
LINUX/Unix File Log Rules	Scan Ontion:	The Latest File Only	1					
UNX_EOG_ARCHIVE_AUTH	Data Or Time Cormati	MMM and Ultramouse	Format	Verific and Freedor				
SQL Server Log Rules	Date of Time Pormat.		ronnac	verny And Explan	1			
Microsoft 365 Audit Log Rules	Second State State Second	Date Or Time In Log File Is UTC Time						
PowerShell Script Log Rules	Ignore File Log Records Over:	30 🗘 Minutes 👻						
Argent Omega For Microsoft 365	LINUX/Unix Command Timeout:	10 Seconds						
Argent Omega For SNMP	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	ent Message					
Argent Omega For SQL Server	Use Advanced Rule Definition:							
Alerts	Rule Is Broken If Log Line:	Contains Authentication failure						
 Monitoring Groups 		Include Or Exclude Keywords, Enter Keywords Senarated By Commas, To Exclude Criteria, Type & Minus S	ion First. To Escar	ne Comma				
Relators		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Macros		Match Case						
Calendars		Match Whole Word						
Administration		Match Regular Expression						
		Assign Event ID: 9,999 🖨						
	Events In Time Range:	00:00:00 - 23:59:59						
	Alert Only If The Specific Event Happe	ens 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							

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.

■ ARGENT OME	GA (2.2A-2207-A)		Home	theme -	(1) Argent Instant Help	? About	U Logout	RC6S
Tool Sets Argent Omega Baseline	Log File Path:	/var/log/auth.log	Variables	View Log F	-ile			i
 Argent Compliance Automator 		File Name Is Regular Expression						
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		Bias Date Or Time Variables Used In File Path By						
Windows File Log Rules		Read Only Last 100 Dines. (Only Read Last 100 Lines By Default)						
LINUX/Unix File Log Rules	Scan Ontion:	The Latert File Only						
UNX_LOG_ARCHIVE_AUTH	Scall Option.			-				
 SYSLOG Rules SOL Server Lee Pulse 	Date Or Time Format:	MMM #d HH:mm:ss	Format	Verify And Ex	(plain			
Microsoft 365 Audit Log Rules		Date Or Time In Log File Is UTC Time						
PowerShell Script Log Rules	Ignore File Log Records Over:	30 🗘 Minutes 👻						
🕨 🔚 Argent Omega For Microsoft 365	LINUX/Unix Command Timeout:	10 Seconds						
Argent Omega For SNMP	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Even	of Message					
Argent Omega For SQL Server	Use Advanced Rule Definition:	System beraut Strawload Sconomed with Latest Event Hessage Sconomed with har Even	ur message					
🕨 🔤 Argent Omega Web Defender	Puls To Pasher T6 Los Lines	Contraction - Antheorem - Anth						
Alerts	Rule is broken if Log Line:	Authentication failure						
Monitoring Groups		And Minus Sign, Proceed With Character "\'. Wildcards '*' And '?' Are Supported	gn First. 10 Escap	e comma				
Macros		Match Case						
Calendars		Match Whole Word						
Administration		Match Regular Expression						
		Assign Event ID: 0 000						
	Events In Time Range:	00:00:00 - 23:59:59						
	Alert Only If The Specific Event Happen	s More Than 1 🗧 Times						
	Alert If The Specific Event Does NOT Ex	ist						
	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							

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:

■ ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme -	្រាំ Argent Instant Help	? About	U Logout	RC6S
▼ 🐸 Tool Sets	Log File Path:	/var/log/auth.log%dd%_%MM%_%yyy%	Variables	View Log Fi	le			-
Argent Omega Baseline		File Name Ts Regular Expression						
Argent Compliance Automator								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Ele Log Rules		Blas Date Or Time Variables Used In File Path By						
LINUX/Unix File Log Rules		Read Only Last 100 💭 Lines (Only Read Last 100 Lines By Default)						
MUNX_LOG_ARCHIVE_AUTH	Scan Option:	The Latest File Only 👻						
SYSLOG Rules	Date Or Time Format:	MMM #d HH:mm:ss	Format	Verify And Exp	əlain			
SQL Server Log Rules		Date Or Time In Log File Is UTC Time						
Microsoft 365 Audit Log Rules	Japore File Log Records Over:							
PowerShell Script Log Rules	1 Thurs / Unio Command Timesuk	30 Minutes						
Argent Omega For Microsoft 365	LINUX/UNIX Command Timeout:	10 Seconds						
Argent Omega For SQL Server	Fire Event With Format:	🖲 System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔵 Combined With Full Even	nt Message					
Argent Omega Web Defender	Use Advanced Rule Definition:							
Alerts	Rule Is Broken If Log Line:	Contains Authentication failure						
Monitoring Groups		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Si	gn First. To Escap	e Comma				
Relators		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Macros		Match Case						
Calendars		Match Whole Word						
Administration		Match Regular Expression						
		Assign Event ID: 9,999						
	Events In Time Range:	00:00:00 - 23:59:59						
	Alert Only If The Specific Event Happer	ns More Than 1 🗧 Times						
	Alert If The Specific Event Does NOT E	xist						
	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							

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



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

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



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

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

= ARGENT OME	GA (2.2A-2207-A)		And Home	theme -	(® Argent Instant Help	? About	U Logout	RC6S
Argent Omega Baseline Argent Omega Baseline Argent Omega Baseline Argent Compliance Automator Windows Compliance Rules Windows Flex to g Rules Unoux Stream Log Rules Unoux Code ancorange Automator Systach Stele to g Rules Statistics Argent Omega For Statistics Argent Omega For Microsoft 365 Argent Omega For Statistics Argen	GA (2.2A-2207-A) Log File Path: Scan Option: Date Or Time Format: Ignore File Log Records Over: LINUX/Unix Command Timeout: Fire Event With Format: Use Advanced Rule Definition: Rule Is Broken If Log Line:	[/var/log/auth.log_%dd%s_%MMM%_%byryt%s_%MM%s_%omm%s_%ops% [File Name Is Regular Expression Use Vesterday's Date For Date Or Time Variables Used In File Path @ isas Date Or Time Variables Used In File Path @ isas Date Or Time Variables Used In File Path @ isas Date Or Time Variables Used In File Path @ isas Date Or Time Variables Used In File Path @ isas Date Or Time Variables Used In File Path @ isas Date Or Time Variables Used In File Path @ isas Date Or Time Variables Used In File Path @ isas Date Or Time In Log File Is UTC Time @ isseconds @ isseconds @ seconds @ of Visite Visite Include Or Exclude Keywords. Enter Keyword Separated for Commas. To Exclude Criteria, Type A Minus Sign And Y Are Supported Match Case Whatch Regular Expression Assign Event ID: 0,900 is	Kormat Variables Format t Message gn First. To Escap	Yiew Log File	¢ ∮ Argent Instant Help	O About	U Logout	(1008
	Events In Time Range:	00:00:00 - 23:59:59						
	Alert If The Specific Event Does NOT Exis	st						
	Alert Message Include	0 C Lines Before And						
	Correct Condition If Log Line	Contains (default)						
	Archive All Log Lines Archive Matching Log Lines							

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 OME	GA (2.2A-2207-A)		And Home	🌞 Theme -	(ٹ) Argent Instant Help	? About	U Logout	RC6S
Argent Compa Baseline Social Compa Baseline Social Compa Baseline Argent Compa Baseline Social Compa Baseline Argent Compa Baseline Argent Compa Baseline Argent Compa For Microsoft 365 Argent Compa For SQL Server Argent Compa For	GA (2.2A-2207-A) Log File Path: Scan Option: Date Or Time Format: Ignore File Log Records Over: LINUX Or Unix Command Timeout: Fire Event With Format: USe Advanced Rule Definition: Rule Is Broken If Log Line: Events In Time Range: Alert Only If The Specific Event Happers Alert If The Specific Event Happers Alert HT The Specific Event Happers Alert HT The Specific Event Happers Alert Masage Indude Correct Constitut If too Line	[var/log/auth.log_%idd%_%iehtM%_%ieyyy%%%%iehtM%_%ient%%%ie%iehtM%_%ies%iehtM%_%ies%iehtM%_%ies%iehtM%_%ies%iehtM%_%ies%iehtM%_%ies%iehtM%_%ies%iehtM%_%ield%iehtM%ieht	Homo Variables Format nt Message	View Log f	Argent instant Help	About	U Logout	
	Save To Archive Repository: Archive All Log Lines Archive Matching Log Lines	(default) -						

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

= ARGENT OME	GA (2.2A-2207-A)		Home	theme -	(्) Argent Instant Help	? About	U Logout	RC6S
Tool Sets Argent Omega Baseline	Log File Path:	/var/log/auth.log_%dd%_%MM%%_%yyyy%_%HH%_%mm%_%ss%	Variables	View Log File	8			ŕ
Argent Compliance Automator Windows Compliance Rules Windows Event Log Rules Windows File Log Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
IINUX/Unix File Log Rules IINUX/LOG_ARCHIVE_AUTH ISYSLOG Rules	Scan Option: Date Or Time Format:	Read Only Last 100 Unes The Latest File Only MNH #d HH:mm:ss	▼ Format	Verify And Expl	lain			
SQL Server Log Rules Microsoft 365 Audit Log Rules Microsoft 365 Audit Log Rules	Ignore File Log Records Over:	Date Or Time In Log File Is UTC Time						
Argent Omega For Microsoft 365 Argent Omega For SNMP Argent Omega For SQL Server Argent Omega For SQL Server	LINUX/Unix Command Timeout: Fire Event With Format: Use Advanced Rule Definition:	10 Seconds System Default Individual Combined With Latest Event Message Combined With Fi	ull Event Message					
Alerts Monitoring Groups Relators	Rule Is Broken If Log Line:	Contains Authentication failure Include OF Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Mi And Minus Sign, Proceed With Character '\. Wildcards '*' And '?' Are Supported	inus Sign First. To Escar	pe Comma				
Macros Calendars dministration		Match Case Match Whole Word Match Regular Expression						
	 Events In Time Range: Alert Only If The Specific Event Happens 	Assign Event ID: 9,999 00:00:00 - 23:59:59 - SMore Than 1						
	Alert If The Specific Event Does NOT Exi	ist						
	Correct Condition If Log Line	Contains (default)						
	Archive All Log Lines Archive Matching Log Lines							

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

= ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme - 🛛 A	(') rgent Instant Help	? About	U Logout	RC6S
	Log File Path:	/var/log/auth.log_%dd%_%MM%_%yyyy%_%HH%_%mm%_%ss%	Variables	View Log File				
Argent Omega Baseline		Ella Nama la Regular Expression			_			
 Argent Compliance Automator 								
Windows Compliance Rules		Use Yesterday's Date For Date Or Time Variables Used In File Path						
Windows Event Log Rules		🖉 Bias Date Or Time Variables Used In File Path By 🛛 0 🏮 Hours						
TINIIX/Unix File Log Rules		Read Only Last 100 🖨 Lines						
UNX_LOG_ARCHIVE_AUTH	Scan Option:	The Latest File Only						
SYSLOG Rules	Date Or Time Format:	MMM #d HH:mm:ss	Format	Verify And Explai	n			
SQL Server Log Rules		Date Or Time In Los Sile Ir LITC Time						
Microsoft 365 Audit Log Rules	Japara Fila Log Records Over							
PowerShell Script Log Rules	Ignore File Log Records Over.	30 Vinutes V						
Argent Omega For Microsoft 365	LINUX/Unix Command Timeout:	10 Seconds						
Argent Omega For SNMP	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With Full Event	nt Message					
Argent Omega For SQL Server	Use Advanced Rule Definition:	0						
Algent onlega web belenden	Rule Is Broken If Log Line:	Contains Authentication failure						
Monitoring Groups		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sig	on First. To Escape	Comma				
Relators		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
Macros		Match Case						
Calendars		Match Whole Word						
Administration		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	s More Than 1 💭 Times						
	Alert If The Specific Event Does NOT Exit	ist						
	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							

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

the log records:

In Tool Sets Log File Argent Compliance Automator Windows Compliance Rules Windows Event Log Rules Windows File Log Rules Windows File Rules Windows File Rules	Path:	/var/log/auth.log_%dd%_%MM%_%yyy%_%HH%_%mm%_%ss%	Allowed and design				
		Ela Nama Is Regular Expression	variables	View Log File			ŕ
		Use Visterday's Date For Date or Time Variables Used In File Path Use Visterday's Date For Date or Time Variables Used In File Path By 0 Hours Read Only Last 100 Lines					
Image: Market Marke	otion: • Time Format:	The Latest File Only v	Format	Verify And Expla	ain		
SQL Server Log Rules SQL Server Log Rules Microsoft 355 Audit Log Rules PowerShell Script Log Rules Argent Omega For SNIP Argent Omega For SNIP Argent Omega For SQL Server Tites Adv	File Log Records Over: Unix Command Timeout: ant With Format: canced Rule Definition:	Date Or Time In Log File Is UTC Time 30 Virtutes 10 Seconds System Default Ordinidual Combined With Latest Event Message Combined With Full Event	: Message				
Alerts Adents	ing Logic:	Properties Hethods 1 2 3 6 5 6 7 8 30 30					
	vents In Time Range: ert Only If The Specific Event Happens I ert If The Specific Event Does NOT Exist ert Message Include are To Archive Repository: Archive All Log Lines Archive Matching Log Lines	00:00:00 - 23:59:59 More Than 1 1 1 1 1 0 Unes Before And 0 (default) •					

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.

- In Taol Seld - Unit	= ARGENT OME	GA (2.2A-2207-A)		😭 Home	🄅 Theme -	(1) Argent Instant Help	? About	U Logout	RC6S
Honkforing Groups Honkforing Groups Indude OF Exclude Keywords. Enter Keywords. Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And And Minus Sign First. To Escape Comma And And Minus Sign First. To Escape Comma And And And Minus Sign First. To Escape Comma And		Log File Path: Scan Option: Date Or Time Format: Ignore File Log Records Over: LLINUX/Unix Command Timeout: Fire Event With Format: USe Advanced Rule Definition: Rule Is Broken IT Log Line:	[/var/log/auth.log_%idf%_%iMM%s_%iMM%s_%iMM%s_%imm%s_%iss% File Name Is Regular Expression Use Yesterday's Date For Date Or Time Variables Used In File Path Bias Date for Time Variables Used In File Path By @ Read Only Last 100 * Unes The Lattest File Only VMM #d HH::mm:ss 00 * Mentes 10 * Seconds \$ystem Default Onditions Authentication failure	Variables Format	View Log F	ile pluin			
Correct Condition If Log Line Contains	Address Honitoring Groups Exelators Honitoring Aroups Galandars Administration	Events In Time Range: Alert Only If The Specific Event Happens Alert If The Specific Event Happens Alert If The Specific Event Does NOT Exi Alert Message Include Correct Condition If Log Line Save To Archive Repository: Archive All Log Lines	Include OF Exclude Keywords, Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sin, Proceed With Character V. Wildcards ⁵⁵ And ¹⁷ Are Supported Match Acase Match Regular Expression Station Viole Word Extern Viole Word Station Second Station Sta	Sign First. To Escaj	pe Comma				

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

= ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme -	(*) Argent Instant Help	? About	Logout	RC6S
	Ignore File Log Records Over: LINUX/Unix Command Timeout: Fire Event With Format: Use Advanced Rule Definition: Rule Is Broken If Log Line:	Date Or Time In Log File Is UTC Time 30	sage t. To Escape	e Comma				
enverthells Cript Log rules in Argent Omega For Kirosoft 365 in Argent Omega For SiNAP argent Omega For SiNAP Argent Omega Web Defender Alerts Maintoring Groups Relators Calendars Administration	Events In Time Range: Alert Only If The Specific Event Happen Alert If The Specific Event Does NOT Ex Alert Message Include Correct Condition If Log Line Save To Archive Raposlory: Archive All Log Lines 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 I Tag 1: Tag 2: Post Event Even If The Same Event Lis S							

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 OME	GA (2.2A-2207-A)		A Home	🔅 Theme -	(*) Argent Instant Help	? About	U Logout	RC6S
Argent Compa Baseline Argent Compa Baseline Argent Company Automator Windows Compliance Rules Windows Field to pitules Windows Field to pitules Windows Field to pitules Windows Field to pitules Systed Carlow Compliance Rules Systed Carlow Compliance Rules Systed Carlow Compliance Rules Systed Carlow Compliance Rules More Rules Systed Carlow Compliance Rules More Rules Argent Compa For System Argent Argent Compa For System Argent Argent Argent	CA (2.2A-2207-A) Ignore File Log Records Over: LINUX/Unix Command Timeout: Fire Event With Format: Use Advanced Rule Definition: Rule Is Broken If Log Line: Events In Time Range: Alert Only If The Spedific Event Dees NOT E Alert Message Include Correct Condition If Log Line Save To Archive Repository: Archive Al Log Lines Archive If Log Lines Archive If Log Line Save Archive Data Only	Date Or Time In Log File Is UTC Time 30 Vinutes Seconds System Default Ordiarie Luthentication failure Include Or Exclude Keywords, Enter Keywords Separated By Commas, To Exclude Orteria, Type A Minus Sign, Froceed With Character Y., Widcards ¹⁰ And ¹⁰ Are Supported Match Case Match Mole Word Match Regular Expression Sign Event ID: 9,099 000000 123:59:59 15 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 13 Times Match Regular Expression 14 Times Match Regular Expression 15 Times Ma	Home ent Message Sign First. To Escap	theme •	Argent instant Help	About	Logout	
	Tag 1: Tag 2: Tag 3: Doct Event Even If The Same Event Fe	Forecaster Using Data Store: (default) Still Curctanding (Unanswered)						

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 OME	GA (2.2A-2207-A)		Home	theme -	(1) Argent Instant Help	? About	U Logout	RC6S
GOI Sets Gol Sets Grapent Compliance Automator Windows Compliance Automator Windows Event Log Rules Windows File Log Rules Glaver, LOG_ARCRYC_AUTH SYSLOG Rules SQL Server Log Rules Microsoft 365 Audit Log Rules PowerShell Script Log Rules	Ignore File Log Records Over: LINUX/Unix Command Timeout: Fire Event With Format: Use Advanced Rule Definition: Rule Is Broken If Log Line:	Date Or Time In Log File Is UTC Time	ent Message Sign First. To Escaj	e Comma				
Argent Omega For SNUP Argent Omega For SQL Server Argent Omega For SQL Server Arts Monitoring Groups Relators Calendars Administration	Events In Time Range: Alert Only If The Specific Event Happen Alert If The Specific Event Does NOT E Alert Message Include Correct Condition If Log Line Correct Condition If Log Line Archive All Log Lines Archive Matching Log Lines Archive Matching Log Lines Archive Matching Log Lines Archive Matching Log Lines Archive Data Only Alert If Field To Open Log File Save Performance Data To The Argent Tag 1: Tag 2: Dost Event Even If The Same Event Is							

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:

• Market Protect Compliance Juncander Protect Up Juncander Protect	■ ARGENT OMEG	A (2.2A-2207-A)		A Home	🔅 Theme -	(*) Argent Instant Help	? About	() Logout	RC8S
	Tool Sets Argent Compa Baseline Argent Compliance Automator Windows Compliance Automator Windows Compliance Automator Windows File Log Rules Windows File Log Rules Use SYSLOG Rules SYSLOG Rules SYSLOG Rules Argent Compa For SNP Argent Compa For SN	gnore File Log Records Over: INUX/Unix Command Timeout: ire Event With Format: ISE Advanced Rule Definition: tule Is Broken If Log Line: Alert Only If The Specific Event Happens Alert If The Specific Event Happens Alert If The Specific Event Happens Alert If The Specific Event Does NOT Exis Alert Message Include Correct Condition If Log Line Save To Archive Repository: Archive MI Log Lines Archive MI Log Lines Archive MI Log Lines Archive MI Log Lines Archive Matching Log Lines Save Archive Bit Log Line Save Archive Data Only Alert If Failed To Open Log File	Date Or Time In Log File Is UTC Time 00 Winutes 10 Seconds System Default Individual Combined With Latest Event Message Combined With Full Event Message Totalians contains Authentication failure Individual Corescued Reproved Separated By Commas, To Exclude Citeria, Type A Minus Sign File and Minus Sign Proved With Character '\', Wildcards '*' And '7' Are Supported Match Regular Expression Assign Event D: 0,999 0 0 0 Unes After Match Case I Match Case I Match Case I Unes Before And I Unes After (ontains I Match Case I Match Case I Unes Before And I Unes After (ontains I Match Case I Match Case (Indefault) I which Bedore And I Unes After (ontains I when Winde Word I when Whole W	iessage irst. To Escap	e Comma				

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 OME	GA (2.2A-2207-A)		ran ar an	🔅 Theme -	(*) Argent Instant Help	? About	U Logout	RCBS
🕶 🔚 Tool Sets		Date Or Time In Log File Is UTC Time						-
Argent Omega Baseline Argent Compliance Automator Mindows Compliance Rules	Ignore File Log Records Over: LINUX/Unix Command Timeout:	30 Minutes Minutes Seconds						
 Windows File Log Rules Windows File Log Rules LINUX/Unix File Log Rules SYSLOG Rules SYSLOG Rules SQL Server Log Rules Microsoft 355 Audit Log Rules Microsoft 355 Audit Log Rules Argent Omega For SNP Argent Omega For SQL Server Argent Argent /li>	Fire Event With Format: Use Advanced Rule Definition: Rule 1s Broken If Log Line: Events In Time Range: Alert Only If The Specific Event Happen Alert If The Specific Event Does NOT Ex Alert Hessage Include Correct Condition If Log Line Save To Archive Repository: Archive All Log Lines Archive All Log Lines Archive Matching Log Lines	System Default Individual Combined With Latest Event Message Combined With Full Event Message System Default Individual Combined With Latest Event Message Combined With Full Event Message Contine Indived OF Exclude Keywords, Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign And Minus Sign, Proceed With Character 1. Wildcards And 17 Are Supported Match Regular Expression Assign Event ID: 9,099 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Yessage First. To Escap	e Comma				
	Save Archive Data Only Alert If Failed To Open Log File Save Performance Data To The Argent F	orecaster Using Data Store: (default)						

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)		ome 🔐	🔅 Theme -	C ⁰⁾ Argent Instant Help	? About	ڻ Logout	RC6
Tool Sets Introd Sets Introd Sets Introduction of the compliance Rules Windows Compliance Rules Windows Compliance Rules Windows File Lop Rules Introduction of Rules Struct Comparison Rules Struct Comparison Rules Microsoft 355 Aulit Lop Rules Struct Comparison Rules Microsoft 355 Aulit Lop Rules Argent Omega For Microsoft 365 Argent Omega For Struct Log Rules Argent Omega For Struct Server Argent Omega For Server<	Hatch Whole Word Hatch Regular Expression (default) Contains Cont					Fulls	Streen

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

= ARGENT OME	GA (2.2A-2207-A)		de Home	🔅 Theme -	ে) Argent Instant Help	? About	ပု Logout	RC75
	Message Priority: Message Facility: Ignore SYSLOG Record Over: Events In Time Range: Save To Archive Repository: Archive All Log Lines Archive Matching Log Lines Tag 1: Tag 2: Tag 3: Post Event Even If The Same Event Is Dos So Only After Ignore The Same Outstanding Event I Post Event Only After Rule Is Broken	System Unusable, Take Action Immediately, Critical Condition System Unusable System Unusable System Unusable Condition Condit						
Administration	Reset Counter @ After Event Is Post @ After Event Is Post @ After Event Is Answered @ After The Actual Condition Is Correcte Application: Reference URL: Console Comment:	d Device: Critical Condition ****					Full	Screen

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

= ARGENT OME	GA (2.2A-2207-A)		🐣 Home	🔅 Theme •	ে) Argent Instant Help	? About	ن Logout	RC7S
	Message Priority:	System Unusable, Take Action Immediately, Critical Condition						ŕ
🕨 🛀 Argent Omega Baseline	Message Facility:	•						
 Argent Compliance Automator 	Ignore SYSLOG Records Over							
Windows Compliance Rules		30 V Minutes V						
Windows Event Log Rules	Events In Time Range:	00:00:00 - 23:59:59						
Windows File Log Rules	Save To Archive Repository:	{default} •						
LINUX/Unix File Log Rules	Archive All Log Lines							
SYSLOG RUIES	Archive Matching Log Lines							
SOL Server Log Rules	Archive If Log Line	Contains						
Set Server Edg Rules Microsoft 365 Audit Log Rules Server Shell Script Log Rules	Save Archive Data Only	precaster Using Data Store: [default]						
🕨 🔚 Argent Omega For Microsoft 365	Tag 1:							
Argent Omega For SNMP	Tag 2:							
Argent Omega For SQL Server	Tag 2:							
Argent Omega Web Defender	lag 5.							
Alerts	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)						
Monitoring Groups	Do So Only After 1 C Hour	0 💭 Minute Since Event Is Post						
Relators	Ignore The Same Outstanding Event If	vlerts Were Fired More Than 1 🗘 Hour 0 🗘 Minute Ago						
Macros	Post Event Only After Rule Is Broken	2 🗘 Or More Times						
Calendars	Reset Counter							
Administration	After Event Is Post							
	After Event Is Answered							
	After The Actual Condition Is Corrected							
	Application:							
	Reference IIRI -							
	Console Comment: *** Network D	evice: Critical Condition ***						
	Description:							
	B Z U Format Block 👻 Font	• # • A • • = = = = = = = = = = = = = = = =					Full Scr	reen
	This Rule monitors SYSLOG of message priority 'Cr	tical Condition"						
		h han dillerant an aich. Ia aile das annan an della an						

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

ARGENT OF	MEGA (2.2A-2207-A)		Home	theme -	(1) Argent Instant Help	? About	ப் Logout
l Sets rgent Omega Baseline	Message Priority: Message Facility:	System Unusable, Take Action Immediately, Critical Condition	* *				
Windows Compliance Rules	Ignore SYSLOG Records Over:	30 🗘 Minutes 🗸					
Windows Event Log Rules	Events In Time Range:	00:00:00 - 23:59:59					
Windows File Log Rules	Save To Archive Repository:	{default}					
LINUX/Unix File Log Rules	Archive All Log Lines						
SLOG Rules	Archive Matching Log Lines						
Server Log Rules	Archive If Log Line	Contains					
rosoft 365 Audit Log Rules	Save Archive Data Only						
verShell Script Log Rules	Save Performance Data To The Argen	t Forecaster Using Data Store: {default}					
nt Omega For Microsoft 365	Tag 1:						
nt Omega For SNMP	Tag 2:						
nt Omega For SQL Server	Tag 3:						
t Omega Web Defender	Post Event Even If The Same Event I	Still Outstanding (Unanswered)					
ing Croups		A Minute Since Event Is Post					
ig Groups	Innore The Same Outstanding Event	If Alerte Ware Fired More Than 1 Hour 0 A Minute Ann					
	Doct Event Only After Pule Is Broken						
rs	Post Event Only Arter Kule is broken	2 Or Pole Times					
ration	Reset Counter						
	After Event Is Answered						
	After The Actual Condition Is Correct	id					
	Application:						
	Reference URL:						
	Console Comment: *** Network	Device: Critical Condition ***					
	Description:						
	B Z U Format Block - Font						Full Scre
	This Rule monitors SYSLOG of message priority	"Critical Condition"					

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

■ ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme -	ری Argent Instant Help	? About	() Logout	RC75
	Message Priority:	System Unusable, Take Action Immediately, Critical Condition						
Argent Omega Baseline	Message Facility:	•						
 Argent Compliance Automator 	Japore SYSLOC Records Over							
Windows Compliance Rules		30 V Minutes V						
Windows Event Log Rules	Vents In Time Range:	00:00:00 - 23:59:59						
Windows File Log Rules	Save To Archive Repository:	{default} 👻						
LINUX/Unix File Log Rules	Archive All Log Lines							
✓ SYSLOG Rules	Archive Matching Log Lines							
SYSLOG_ARCHIVE_CRITICAL	Arabia 16 Lee Lies	Cashin						
SQL Server Log Rules	Archive II Log Line	Concains						
Microsoft 365 Audit Log Rules	Save Archive Data Only							
PowerShell Script Log Rules	Save Performance Data To The Argent	Forecaster Using Data Store: {default}						
Argent Omega For Microsoft 365	Tag 1:							
Argent Omega For SNMP	Tag 2:							
Argent Omega For SQL Server	Tag 3:							
Argent Omega Web Defender	Rost Event Even If The Same Event Is	Still Outstanding (Unanswered)						
Alerts								
Monitoring Groups	Do So Univ Arter	0 Minute Since Event Is Post						
Relators	Ignore The Same Outstanding Event If	Alerts Were Fired More Than 1 Hour 0 Minute Ago						
Macros	Post Event Only After Rule Is Broken	2 🗘 Or More Times						
Calendars	Reset Counter							
Administration	After Event Is Post							
	After Event Is Answered							
	After The Actual Condition Is Corrected							
	Application:							
	Reference URL:							
	Console Comment: *** Network I	Device: Critical Condition ***						
	Description:							
	B Z U Format Block - Font						Full 9	Screen
	This Rule monitors SYSLOG of message priority '	Critical Condition"						
	I Invol on the Network Devices and as Oleve and	And have different and the set of the second set of the second second second second second second second second						

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:

■ ARGENT OME	EGA (2.2A-2207-A)		Ame Home	🛟 Theme -	(ग) Argent Instant Help	? About	U Logout	RC7
In Tool Sets Argent Omega Baseline Argent Compliance Automator Windows Event Log Rules Windows File Log Rules Windows File Log Rules Introver File Log Rules SYSLOG Rules SYSLOG Rules SYSLOG Rules Microsoft 355 Audit Log Rules Microsoft 355 Audit Log Rules Argent Omega For SNHP Argent Omega For SNHP	Message Priority: Message Facility: Ignore SYSLOC Records Over: © Events In Time Range: © Save To Archive Repository: Archive All Log Lines Archive Hatching Log Lines Archive Hatching Log Lines Archive Data Only © Save Archive Data Only © Save Archive Data Only Tag 1: Tag 2: Tag 3: © Sos Only Arter © Sos Only Arter © Sos Only Arter © Sone The Same Outstanding Event I © Post Event Only After Fulle Is Broken	System Unusable, Take Action Immediately, Critical Condition						
Administration	After Event Is Post After Event Is Answerd After The Actual Condition Is Correcte Application: Reference URL: Console Comment: Description: I 2 2 1 Format Block Font The Rule montors SYSLOG of message priorly	d Device: 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 OME	GA (2.2A-2207-A)	슈 수 (이 연 선 Home Theme * Argent listant Help About Logout	RC8S
▼ Mool Sets	Log Type:	Error Log 🔹	Ê
Argent Omega Baseline	Ignore Log Records Over:		
Argent Compliance Automator	Fire Event With Format		
Windows Event Log Rules		System Default Undividual Combined With Latest Event Message Combined With Full Event Message	
Windows File Log Rules	Use Advanced Rule Definition:		
LINUX Or Unix File Log Rules	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed	
SYSLOG Rules		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign First. To Escape Comma And Minus Sion. Proceed With Character '' Wildrards ''' and '' Are Sunonted.	
✓ SQL Server Log Rules			
SS_LOG_AGENT		matth ase	
SS_LOG_ERROR		Match Whole Word	
Microsoft 365 Audit Log Rules		Match Regular Expression	
PowerShell Script Log Rules		Assign Event ID: 9,999	
Argent Omega For Microsoft 365	Events In Time Range:	00:00:00 - 23:59:59	
Image: Argent Omega For SNMP	Alert Only If The Specific Event Happen	Shore Than 1 Times	
Argent Omega For SQL Server	Alert If The Specific Event Does NOT Ex	ist	
Argent Omega web Defender	Correct Condition If Log Line	Containe	
Arer to Are to	Connect contaition in Edg Ente		
Interview of the second sec	Save to Archive Repository:	foeaut.	
Ident Macro	Archive All Log Lines		
Monitoring Groups	Archive Matching Log Lines		
Relators	Archive If Log Line	Contains	
👻 🖬 Macros	Save Archive Data Only		
Email Recipients	Save Performance Data To The Argent F	orecaster Using Data Store: {default}	
SMS Recipients	Tag 1:		
Windows Services	Tag 2:		
Windows Processes	Tag 3:		
Users	Best Event Even If The Same Event Is 5	NII Outstanding (Tipageward)	
✓ Image: Calendars	Post event even if the same event is s		
Base Definitions	Hour 1 Hour	U minute since Event is vost	
Holidays	Ignore The Same Outstanding Event If	Alerts Were Fired More Than 1 Hour 0 Minute Ago	
Administration	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:

					- 2			RC8S
= ARGENT OME	GA (2.24-2207-A)		Home	Theme -	لاتی Argent Instant Help	? About	Logout	
					· ·			
	Log Type:	Error Log						i i i i i i i i i i i i i i i i i i i
🕨 🕍 Argent Omega Baseline	Japore Log Records Over:							
 Argent Compliance Automator 	Ignore Log Records over	24 Hours Y						
Windows Compliance Rules	Fire Event With Format:	System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔵 Combined With Full Event M	lessage					
Windows Event Log Rules	Use Advanced Rule Definition:							
Windows File Log Rules	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
ELINDX OF UNIX File Log Rules		Include Or Exclude Keywords, Enter Keywords Separated By Commas, To Exclude Criteria, Type A Minus Sign F	irst. To Escape	Comma				
 STSLOG Kules SOL Server Log Pules 		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
SS LOG AGENT		Match Case						
SS LOG ERROR		Match Whole Word						
Microsoft 365 Audit Log Rules		Match Regular Expression						
PowerShell Script Log Rules		Assign Event ID:						
Argent Omega For Microsoft 365								
🕨 🔚 Argent Omega For SNMP	Events In Time Range:	00:00:00 - 23:59:59						
Argent Omega For SQL Server	Alert Only If The Specific Event Happen	s More Than 1 💭 Times						
Argent Omega Web Defender	Alert If The Specific Event Does NOT Ex	ist						
👻 🔚 Alerts	Correct Condition If Log Line	Contains 👻						
Correction	Save To Archive Repository:	{default} 👻						
Notification	Archive All Log Lines							L
Alert Macro	Archive Matching Log Lines							
Monitoring Groups	Archive Hatching Log Lines							
Relators	Archive If Log Line	Contains						
👻 🕍 Macros	Save Archive Data Only							
Email Recipients	Save Performance Data To The Argent F	Forecaster Using Data Store: {default}						
SMS Recipients	Tag 1:							
Windows Services	Tag 2:							
Windows Processes	Tag 3:							
 Users 	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)						
Calendars	Do So Only After 1 Hour	Minute Since Event Is Post						
 Base Deminuons Melidava 		Alaste Mass Find Mass Than 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1						
 Administration 	Ignore the same Outstanding Event If							
- Aurimati duon	Post Event Only After Rule Is Broken	2 Cr More Times						

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

			*		C)	?	Ċ,	RC8S
	2.2A-2207-A)		ноте	Ineme *	Argent Instant Help		Logout	
✓		Frront Lon						
Argent Omega Baseline	a Records Over							
Argent Compliance Automator	g Records Over.	24 Hours						
Windows Compliance Rules Fire Event	With Format:	System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔵 Combined With Full Event	: Message					
Windows Event Log Rules Use Advant	nced Rule Definition:							
Windows File Log Rules Rule Is Br	oken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
LINUX Or Unix File Log Rules SYSLOG Rules		Include Or Exclude Keywords, Enter Keywords Separated By Commas, To Exclude Criteria, Type A Minus Sign	n First. To Escap	e Comma				
✓		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
SS_LOG_AGENT		Match Case						
SS_LOG_ERROR		Match Whole Word						
Microsoft 365 Audit Log Rules		Match Regular Expression						
PowerShell Script Log Rules		Assian Event ID: 0 000						
→ Margent Omega For Microsoft 365	to In Time Panger	00:00:00						
Argent Omega For SNMP	e l fret e 10 e							
Argent Omega For SQL Server	CONIV IF The Specific Event Happens	More Inan 1 Times						
Alert Argent Omega Web Defender	t If The Specific Event Does NOT Exis	st						
✓ Merts	ect Condition If Log Line	Contains 👻						
Correction	e To Archive Repository:	{default}						
Notification	chive All Log Lines							
Alert Macro	chive Matching Log Lines							
Monitoring Groups	whive If Log Line	Contains						
Ar Ar	crive ir Log Line	contains •						
Save	e Archive Data Only							
Email Recipients	e Performance Data To The Argent Fo	recaster Using Data Store: {default}						
Tag 1:								
Tag 2:								
Tag 3:								
Post	Event Even If The Same Event Is St	ill Outstanding (Unanswered)						
Base Definitions	So Only After 1 Hour	0 🚔 Minute Since Event Is Post						
Holidays	re The Same Outstanding Event If A	lerts Were Fired More Than 1 Hour 0 Minute Ano						
✓ Machinistration	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:

■ ARGENT OME	GA (2.2A-2207-A)		den Home	🔅 Theme -	(') Argent Instant Help	? About	ပ္ Logout	
	Log Type: Ignore Log Records Over: Fire Event With Format: Use Advanced Rule Definition: Monitoring Logic:	Error Log 24 Hours 25 Combined With Latest Event Message Combined With Fu 7 Properties 4 4 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7	ull Event Message					
MoverShell Script Log Rules Argent Omega For NMP Argent Omega For SNMP Argent Omega For SQL Server Margent Omega Web Defender Argent Omega Veb Defender Argent Omega Veb Defender Modification Modification Alert Macro	Events In Time Range: Alert Only If The Specific Event Happen Alert If The Specific Event Does NOT Ex 2 Save To Archive Repository: Archive All Log Lines Archive All Log Lines Archive It Log Line	10 00:00:00 • [23:59:59 s Hore Than 1 (default) • Contains						
	Save Archive Data Only Save Performance Data To The Argent F Tag 1: Tag 2: Do Stevent Even If The Same Event Is S Do So Only After Ignore The Same Oustanding Event If Post Event Only After Rule Is Broken	Sorecaster Using Data Store: (default) Still Outstanding (Unanswered) Still Outstanding (Unanswered) Still Since Event Is Post Alerts Were Fired More Than Cool Minute Ago Cool Or More Times						

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 OME	GA (2.2A-2207-A)		∰ Home	🔅 Theme -	ڑٹ) Argent Instant Help	? About	U Logout	RC8S
	Log Type:	Error Log						
Argent Omega Baseline	Ignore Log Records Over:							
Argent Compliance Automator	Fire Event With Format:							
Windows Event Log Rules		System Default Individual Combined With Latest Event Message Combined With Full Event —	Message					
Windows File Log Rules	Use Advanced Rule Definition:							
LINUX Or Unix File Log Rules	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
SYSLOG Rules		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign	First. To Escape	Comma				
✓ III SQL Server Log Rules		Mite minus Sign, Proceed With Character 1, Wildcards 1, Allo 7 Ale Supported						
SS_LOG_AGENT								
SS_LOG_ERROR		Match Whole Word						
Microsoft 365 Audit Log Rules		Match Regular Expression						
PowerShell Script Log Rules		Assign Event ID: 9,999 🗧						
Argent Omega For Microsoft 365	Events In Time Range:	00:00:00 - 23:59:59						
Argent Omega For SNMP	Alert Only If The Specific Event Happens	s More Than 1 🗘 Times						
Argent Omega Veb Defender	Alert If The Specific Event Does NOT Exi	ist						
▼ III Alerts	Correct Condition If Log Line	Contains 👻						
Correction	Save To Archive Repository:	{default}						
Motification	Authine All Lon Lines							
Alert Macro	Archive Air Log Lines							
Monitoring Groups	Archive Matching Log Lines							
Relators	Archive If Log Line	Contains 👻						
👻 🕍 Macros	Save Archive Data Only							
Email Recipients	Save Performance Data To The Argent F	orecaster Using Data Store: {default}						
SMS Recipients	Tag 1:							
Windows Services	Tag 2:							
Windows Processes	Tag 3:							
 Users Colondars 	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)						
Garcinuars	Do So Only After 1 Hour	0 Minute Since Event Is Post						
Holidays	Ignore The Same Outstanding Event If J	Alerts Were Fired More Than 1 Hour 0 Minute Ago						
✓ In Administration	Post Event Only After Pule Is Broken							
	Post Event Only After Rule Is Broken	2 joint Or More Times						

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

■ ARGENT OME	A (2.2A-2207-A) A (2.2A-2207-A)
	og Type: gnore Log Records Over: ire Event With Format: ise Advanced Rule Definition: ule Is Broken If Log Line: Include Or Exclude Keywords, Enter Keywords Separated By Commas, To Exception, Login failed Include Or Exclude Keywords, Enter Keywords Separated By Commas, To Exclude Citeria, Type A Minus Sign First. To Escape Comma And Minus Sign, Proceed With Character '\. Wildcards ** And '7 Are Supported Match Case Hatch Whole Word
	Match Regular Expression Assign Event ID: 0,999 Events In Time Range: 00:00:00 - 22:59:59 Alert Only If The Specific Event Happens More Than 1 Times Alert If The Specific Event Logs NOT Exist - Correct Condition If Log Lines - Archive All Log Lines - Archive All Log Lines -
Adelators Melators Email Recipients Macros Macros Move Services Mindows Processes Windows Processes Move Services Move Services	Archive Is Log Line Save Archive Data Only Save Archive Data To The Argent Forecaster Using Data Store: Tag 1: Tag 2: Tag 3: Post Event Event If The Same Event Is Still Outstanding (Uranswered) Do So Only After Image: Im

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:

■ ARGENT OME	GA (2.2A-2207-A)		😭 Home	🔅 Theme -	(' ') Argent Instant Help	? About	ပံ Logout	RC8S
	Log Type:	Frror Log						ŕ
🕨 🔤 Argent Omega Baseline	Japore Log Records Over							
Argent Compliance Automator		24 Hours						
Windows Compliance Rules	Fire Event With Format:	System Default 🔵 Individual 🔵 Combined With Latest Event Message 🔵 Combined With Full Event 1	Message					
Windows Event Log Rules	Use Advanced Rule Definition:							
Windows File Log Rules	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
SYSLOG Pules		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign	First. To Escap	e Comma				
SOL Server Log Rules		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported						
SS LOG AGENT		Match Case						
SS_LOG_ERROR		Match Whole Word						
Microsoft 365 Audit Log Rules		Match Regular Expression						
PowerShell Script Log Rules		Assian Event ID:						
Argent Omega For Microsoft 365	Events In Time Panger	00:00:00						
Argent Omega For SNMP	Alert Only 16 The Coordin Sweet Upper	- Mare Then						
Argent Omega For SQL Server	Alert Only If The Specific Event Happens	imes						
🕨 🐸 Argent Omega Web Defender	Alert If The Specific Event Does NOT Exi	st						
✓ Merts	Correct Condition If Log Line	Contains 💌						
Correction	Save To Archive Repository:	{default}						
Notification	Archive All Log Lines							
Alert Macro	Archive Matching Log Lines							
Monitoring Groups	Archive If Log Line	Contains -						
Relators		Contains						
Macros Email Paciniante	Save Archive Data Only	Contraction and Contraction						
SMS Recipients	Save Performance Data to The Argent F	orecaster Using Data Store: {derault}						
Windows Services	Tag 1:							
Windows Processes	lag 2:							
Users	Tag 3:							
✓ Image: Calendars ✓ Image: Cale	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)						
Base Definitions	Do So Only After 1 📄 Hour	0 Dimute Since Event Is Post						
🕨 🔚 Holidays	Ignore The Same Outstanding Event If A	Alerts Were Fired More Than 1 🗘 Hour 0 💭 Minute Ago						
✓	Post Event Only After Rule Is Broken	2 Or More Times						

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 OME	GA (2.2A-2207-A)		😭 Home	🔅 Theme -	(') Argent Instant Help	? About	U Logout	RC8S
	Log Type:	Error Log						ŕ
In Argent Omega Baseline	Ignore Log Records Over:	24 A Hours						
Argent Compliance Automator Windows Compliance Rules	Fire Event With Format:	Contraction of the Contraction of Web Lateral Device Manager and Web Diff. Contraction						
Windows Event Log Rules	Use Advanced Pule Definition	System Default Individual Combined with Latest Event Message Combined with Full Event M	lessage					
Windows File Log Rules	ose Advanced Kule Demittion.							
LINUX Or Unix File Log Rules	Rule Is Broken If Log Line:	Contains Could not allocate space, Error, Exception, Login failed						
SYSLOG Rules		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign F And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported	First. To Escap	e Comma				
✓ SQL Server Log Rules		Match Case						
SS_LOG_AGENT		Makeh Whole Wood						
SS_LOG_ERROR								
Microsoft 365 Audit Log Rules		Match Regular Expression						
Argent Omena For Microsoft 365		Assign Event ID: 9,999						
Argent Omega For SNMP	Events In Time Range:	00:00:00 - 23:59:59						
Argent Omega For SQL Server	Alert Only If The Specific Event Happen	s More Than 1 🗘 Times						
Argent Omega Web Defender	Alert If The Specific Event Does NOT E	ist						
👻 🔚 Alerts	Correct Condition If Log Line	Contains 👻						
Correction	Save To Archive Repository:	{default} 👻						
Notification	Archive All Log Lines							_
Alert Macro	Archive Matching Log Lines							
Monitoring Groups	Archive If Log Line	Contains +						
Relators		Contains						
Final Recipients	Save Archive Data Only	accesses Lising Data Classes (Jafoult)						
SMS Recipients	Tag 1:	Vietaster Osing Data Store. Luerauity						
Windows Services	Tag 2:							
Windows Processes	The 2							
🕨 🔚 Users	Tag 3:							
👻 🔚 Calendars	Post Event Even If The Same Event Is S	Still Outstanding (Unanswered)						
Base Definitions	Do So Only After 1 💭 Hour	0 Minute Since Event Is Post						
Holidays	Ignore The Same Outstanding Event If	Alerts Were Fired More Than 1 Hour 0 C Minute Ago						
 Administration 	Post Event Only After Rule Is Broken	2 Cr 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'

= ARGENT OME	GA (2.2A-2207-A)		🔏 🔅 Home Theme •	්) Argent Instant Help	? About L	egout
	f Ignore Event Log Records Over:	24 🛔 Hours				
Argent Omega Baseline	Fire Event With Format:	System Default Individual Combined With Latert Event Mercage Combined With E	Full Event Mercage			
Argent Compliance Automator		ticfice Cultoria	run Evenc Hessage			
Windows Compliance Rules	Rule 15 Broken 11 Addit Log Record Sa	asites Criteria				
Windows Event Log Rules	User ID:					
Windows File Log Rules	Client IP Address:	*				
ELINOX OF ONLY FILE LOG Rules	Workload:	*				
 STSLOG Rules M GOL Graves Les Pulses 	Operation:	*				
 SQL Server Log Rules Microsoft 265 Audit Los Pulsa 	Result Status:	Failed				
Microsoft 365 Addit Edg Kules		Include Or Exclude Keywords, Enter Keywords Separated By Commas, To Exclude Criteria, Type A Mi	inus Sign First. To Escape Comma			
h BawarChall Script Log Pulos		And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported				
PowerShell Script Log Rules						
Argent Omega For SNMP	Events In Time Range:	00:00:00 - 23:59:59				
Argent Omega For SOL Server	Alert Only If The Specific Event Happen	s More Than 1 🗘 Times				
Argent Omega Web Defender	Alert If The Specific Event Does NOT Ex	ist				
 Allerts 	Correct Event If Seeing Result Status O	f Same Source: Succeeded				
Correction	Save Te Archive Reportance	Edofault).				
Notification		(uerauity -				
Alert Macro	Save Archive Data Only					
Monitoring Groups	Alert If Failed To Download Audit Log					
Relators	Save Performance Data To The Argent F	orecaster Using Data Store: {default}				
👻 🚾 Macros	Tag 1:					
Email Recipients	Tag 2:					
SMS Recipients	Tag 3:					
Windows Services	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)				
Windows Processes	Do So Only After 1 Hour	Minute Since Event In Pact				
▶ 🔤 Users		0 Printite Since Event IS Post				
✓	Ignore The Same Outstanding Event If	Alerts Were Fired More Than 1 Hour 0 Minute Ago				
Base Definitions	Post Event Only After Rule Is Broken	2 🚺 Or More Times				
Holidays	Reset Counter					
✓	After Event Is Post					
Ticense (Admin Only)	After Event Is Answered					

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 OME	GA (2.2A-2207-A)		rian de la comencia d	🔅 Theme -	(*) Argent Instant Help	? About	U Logout	RC9
✓ Interview of the second	Ignore Event Log Records Over:	24 C Hours						
Argent Omega Baseline Argent Compliance Automator	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With F	Full Event Message					
Windows Compliance Rules	Rule Is Broken If Audit Log Record Sat	isfies Criteria						
Windows Event Log Rules	User ID:	*						
Windows File Log Rules	Client IP Address:	*						
LINUX Or Unix File Log Rules	Workload:	*						
SYSLOG Rules	Operation	*						
SQL Server Log Rules	Desult Chabura							
▼ Microsoft 365 Audit Log Rules	Result Status:	Falled						
MS365_LOG_ARCHIVE_ALL		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Mir And Minus Sign, Proceed With Character '\'. Wildcards '*' And '?' Are Supported	inus Sign First. To Escape	Comma				
PowerShell Script Log Rules								
Argent Omega For Microsoft 365	Events In Time Range:	00:00:00 - 23:59:59						
Argent Omega For SNMP	Alert Only If The Specific Event Happens	More Than 1 C Times						
Argent Omega For SQL Server	Alert If The Specific Event Does NOT Exi	st						
 Algent Onlega web berenden Alerts 	Correct Event If Seeing Result Status Of	Same Source: Succeeded						
> Correction	Save To Archive Repository:	/default)						
Notification		(denois)						
▶ 🖬 Alert Macro	Save Archive Data Only							
Monitoring Groups	Alert If Failed To Download Audit Log							
Relators	Save Performance Data To The Argent F	orecaster Using Data Store: {default}						
🕶 🔚 Macros	lag 1:							
Email Recipients	Tag 2:							
SMS Recipients	Tag 3:							
Windows Services	Post Event Even If The Same Event Is S	ill Outstanding (Unanswered)						
Windows Processes	Do So Only After 1 📮 Hour	0 💭 Minute Since Event Is Post						
Users	Ignore The Same Outstanding Event If A	lerts Were Fired More Than 1 Hour 0 Minute Ago						
Calendars	Post Event Only After Rule Is Broken	2 Or More Times						
Base Definitions	- De Erene only Piter hare 28 broken							
Holidays	Reset Counter							
 Administration 	After Event Is Post							

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 OME	GA (2.2A-2207-A)						de Home	🔅 Theme -	(') Argent Instant Help	? About	U Logout	RC9S
▼ 🖬 Tool Sets	Ignore Event Log Records Over:	24 A Hou		1								-
🕨 🔤 Argent Omega Baseline	Circ Current Middle Community	24	uis .									
 Argent Compliance Automator 	Fire Event with Format:	System Default In	ndividual 🔵 Con	bined With Latest Event	Message 🔵 Combine	ed With Full Event Mes	ssage					
Windows Compliance Rules	Rule Is Broken If Audit Log Record Sa	atisfies Criteria		7								
Windows Event Log Rules	User ID:	*										
Windows File Log Rules	Client IP Address:	*										
LINUX Or Unix File Log Rules	Workload:	*]								
SYSLOG Rules	Operation:	*]								
SQL Server Log Rules	Result Status:	Failed		Ī								
MS365_LOG_ARCHIVE_ALL MS365_LOG_ARCHIVE_ALL		Include Or Exclude Keywo And Minus Sign, Proceed V	ords. Enter Keywor With Character '\'.	ds Separated By Comma Wildcards '*' And '?' Are	s. To Exclude Criteria, Supported	Type A Minus Sign Fire	st. To Escape	Comma				
Argent Omega For Microsoft 365	Events In Time Range:	00:00:00 - 23	3:59:59	1								
Argent Omega For SNMP	Alert Only If The Specific Event Wannen	uns More Than	1	Times								
Argent Omega For SQL Server	Alert Only If the Specific Event Happen		1	Times								
🕨 🖬 Argent Omega Web Defender	Alert If The Specific Event Does NOT ES	=xist			-							
✓ Merts	Correct Event If Seeing Result Status C	Of Same Source:	Succeeded		J							
Correction	Save To Archive Repository:	{default}		-								
Notification	Save Archive Data Only											
Alert Macro	Alert If Failed To Download Audit Log											
Monitoring Groups	Save Performance Data To The Argent I	Forecaster Using Data Store:	{default}		•							L
Relators	Tag 1:											
Macros	Tag 2:		_									
Email Recipients	Tag 3:		_									
 SHS Recipients Mindows Convision 												
Windows Services	Post Event Even If The Same Event Is S	Still Outstanding (Unanswered	d)									
 Willows Processes Illeare 	Do So Only After 1 C Hour	0 📋 Minute Since Event	t Is Post									
- Colondarr	Ignore The Same Outstanding Event If	f Alerts Were Fired More Than	1 🗘 Hou	r 💦 👔 Minute Ag	D							
Galeridans	Post Event Only After Rule Is Broken	2 💭 Or More Times										
Holidays	- Reset Counter											
Administration	After Event Is Post											
License (Admin Only)	After Event Is Answered											

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

■ ARGENT OME	GA (2.2A-2207-A)		Home	🔅 Theme -	ڑ¢) Argent Instant Help	? About	U Logout	RCBS
	Ignore Event Log Records Over:	24 Hours						
🕨 🕍 Argent Omega Baseline	Fire Event With Format:							
 Argent Compliance Automator 		System Default Individual Combined with Latest Event Message Combined with Full Event M	lessage					
Windows Compliance Rules	Rule Is Broken If Audit Log Record Sat	Listies Criteria						
Windows Event Log Rules	User ID:	*						
Windows File Log Rules	Client IP Address:	8						
ELINUX OF UNIX File Log Rules	Workload:	8						
SYSLOG Rules	Operation:	8						
SQL Server Log Rules Microcoft 265 Audit Log Pulor	Result Status:	Failed						
MR365_LOG_ARCHIVE_ALL MS365_LOG_ARCHIVE_ALL		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign F And Minus Sign, Proceed With Character '\'. Wildcards ' ^{ser} And '?' Are Supported	irst. To Escape	e Comma				
Argent Omega For Microsoft 365	Events In Time Bange:	00:00:00 - 23:50:50						
Argent Omega For SNMP	Alact Only If The Specific Event Hannen	s More Then						
Argent Omega For SQL Server	Alert Only If the Specific Event Happens	s more man						
Argent Omega Web Defender	Alert If The Specific Event Does NOT Exi	ist						
✓ III Alerts	Correct Event If Seeing Result Status Of	Same Source: Succeeded						
Correction	Save To Archive Repository:	{default}						
Notification	Save Archive Data Only							
Alert Macro	Alert If Failed To Download Audit Log							
Monitoring Groups	Save Performance Data To The Argent F	orecaster Using Data Store: {default}						l
Relators	Tag 1:							
👻 🚾 Macros	Tag 2:							
Email Recipients	The 2:							
SMS Recipients	Tay 3:							
Windows Services	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)						
Windows Processes	Do So Only After 1 🚺 Hour	0 💭 Minute Since Event Is Post						
Visers	Ignore The Same Outstanding Event If A	Alerts Were Fired More Than 1 🗧 Hour 0 🗧 Minute Ago						
Carenuars	Post Event Only After Rule Is Broken	2 Or More Times						
Base Demittoris	- Reset Counter							
 Administration 	After Event Is Post							
Flicense (Admin Only)	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 OME	GA (2.2A-2207-A)					Home	theme •	្រ ាំ) Argent Instant Help	? About	ပ် Logout	
Tool Sets Argent Omega Baseline Magent Compliance Automator	Ignore Event Log Records Over: Fire Event With Format:	24 Hours	al Ocombined With Li	atest Event Message 🔵	Combined With Full Event Mes	ssage					
Windows Compliance Rules	Rule Is Broken If Audit Log Record Sat	isfies Criteria									
Windows Event Log Rules	User ID:	*									
🕨 🐸 Windows File Log Rules	Client IP Address:	*									
LINUX Or Unix File Log Rules	Workload:	*									
SYSLOG Rules	Operation:	*									
SQL Server Log Rules	Recult Status:	Failed									
 Microsoft 365 Audit Log Rules 	Result Status.	raieu					_				
MS365_LOG_ARCHIVE_ALL	A	Include Or Exclude Keywords. Er And Minus Sign, Proceed With C	ter Keywords Separated haracter '\'. Wildcards '*'	By Commas. To Exclude Ci And '?' Are Supported	riteria, Type A Minus Sign Firs	st. To Escape	Comma				
PowerShell Script Log Rules											
Argent Omega For Microsoft 365	Events In Time Range:	00:00:00 - 23:59:5	i9								
Argent Omega For SNMP	Alert Only If The Specific Event Happen	s More Than	1 🗘 Times								
Argent Omega For SQL Server	Alert If The Specific Event Does NOT Ex	ist									
Argent Omega web Derender	Correct Event If Seeing Result Status Of	Same Source: Succee	ded								
Alerts	Construction Descriptions	61.6.10									
Notification	Save to Archive Repository:	{derault}	· · ·								
Alert Macro	Save Archive Data Only										
Manitoring Groups	Alert If Failed To Download Audit Log										
Relators	Save Performance Data To The Argent F	orecaster Using Data Store: 🛛 👔		-							
Macros	Tag 1:]								
Image:	Tag 2:		Ĵ								
Image: SMS Recipients	Tag 3:		ĩ								
Windows Services	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)									
Windows Processes	Do So Doly After 1 Dury	Minute Cince Fuent Is D									
Users			ist								
👻 🖬 Calendars	Ignore The Same Outstanding Event If J	lerts Were Fired More Than	1 Hour 0	Minute Ago							
Base Definitions	Post Event Only After Rule Is Broken	2 📋 Or More Times									
Holidays	Reset Counter										
 Administration 	After Event Is Post										
Ticense (Admin Only)	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 OM	IEGA (2.2A-2207-A) (* O O Home Theme- Argent Instant Help About Logout	RC
▼ 📁 Tool Sets	Grant Log Records Over: 24 Heurs	
Argent Omega Baseline	Fire Event With Format:	
 Argent Compliance Automator 	System Default Compared With Latest EVent Plessage Compared With Event Plessage	
Windows Compliance Rules	Rule Is Broken IT Audit Log Record Satisfies Criteria	
Windows Event Log Rules	User ID:	
Windows File Log Rules	Client IP Address:	
LINUX Or Unix File Log Rules	Workload:	
SYSLOG Rules	Operation:	
SQL Server Log Rules	Result Status: Falled	
 Microsoft 365 Audit Log Rules 		
MS365_LOG_ARCHIVE_ALL	Include Or Exclude KeyWords. Enter KeyWords Separated by Commas. Io exclude Unterlar, type a minus sign rinst. Io escape Comma And Minus Sign, Proceed With Character (*), VillGrands ** And **, And **, Are Supported	
PowerShell Script Log Rules		
Argent Omega For Microsoft 365	Events In Time Range: 00:00:00 - 23:59:59	
Argent Omega For SNMP	Alert. Only If The Specific Event Happens More Than	
Argent Omega For SQL Server	A late if The Sharing Event Does NTT Evid	
Argent Omega Web Defender		
▼ Merts	Correct Event If Seeing Result Status Of Same Source: Succeeded	
Correction	Save To Archive Repository: (default)	
Notification	Save Archive Data Only	
Alert Macro		
Monitoring Groups		
Relators	Save Performance Data to the Argent Forecaster Using Data Store: (default)	
🔻 🐸 Macros	lag 1:	
Email Recipients	Tag 2:	
SMS Recipients	Tag 3:	
Windows Services	Post Event Even If The Same Event Is Still Outstanding (Unanswered)	
Windows Processes		
Users	Do so Only Alter 1 Hour 0 Plintue since Event is Post	
✓ III Calendars	Ignore The Same Outstanding Event If Alerts Were Fired More Than	
Base Definitions	Post Event Only After Rule Is Broken 2 🕞 Or More Times	
Holidays	r Reset Counter	
Administration	After Event Is Post	
License (Admin Only)	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 OME	GA (2.2A-2207-A)		den Home	🔅 Theme -	ू ण) Argent Instant Help	? About	ل Logout	RC9
	Ignore Event Log Records Over:	24 A Hours						
🕨 🚧 Argent Omega Baseline	Fire French With French							
Argent Compliance Automator	Fire Event with Format:	System Default Individual Combined With Latest Event Message Combined With Full Event N	Message					
Windows Compliance Rules	Rule Is Broken If Audit Log Record Sat	isfies Criteria						
Windows Event Log Rules	User ID:	*						
Windows File Log Rules	Client IP Address:	9						
LINUX Or Unix File Log Rules	Workload:	8						
SYSLOG Rules	Operation:	*						
SQL Server Log Rules	Result Status:	Failed						
Pricrosoft 365 Audit Log Rules		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A Minus Sign I	First. To Escap	e Comma				
PowerShell Script Log Pules		And Minus Sign, Proceed With Character "\'. Wildcards '*' And '?' Are Supported						
Argent Omega For Microsoft 365								
Argent Omega For SNMP	Events In Time Range:	00:00:00 - 23:59:59						
Argent Omega For SQL Server	Alert Only If The Specific Event Happens	s More Than 1 💭 Times						
Argent Omega Web Defender	Alert If The Specific Event Does NOT Exi	st						
✓ III Alerts	Correct Event If Seeing Result Status Of	Same Source: Succeeded						
Correction	Save To Archive Repository:	{default}						
Notification		Conners -						
Alert Macro	Save Archive Data Only							
Monitoring Groups	Alert If Failed To Download Audit Log							
Relators	Save Performance Data To The Argent F	orecaster Using Data Store: {default}						
🔻 🕍 Macros	lag 1:							
Email Recipients	Tag 2:							
SMS Recipients	Tag 3:							
Windows Services	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)						
Windows Processes	Do So Only After 1 Hour	0 C Minute Since Event Is Post						
Users	Ignore The Same Outstanding Event If 4	Slerts Were Fired More Than 1 Hour 0 Minute Ano						
	Dest Super Only After Bule Is Broken							
Base Definitions	Post Event Only After Rule Is Broken							
Holidays	Reset Counter							
Administration	After Event Is Post							
Ficense (Admin Only)	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 OME	GA (2.2A-2207-A)		A Home	🛟 Theme -	(' ') Argent Instant Help	? About	U Logout	RC95
	Ignore Event Log Records Over:	24 🔶 Hours						
Argent Omega Baseline	Fire Event With Format:	System Default Individual Combined With Latest Event Message Combined With E	Full Event Message					
Argent Compliance Automator		ticfies Criteria	an evene nessage					
Windows Event Log Rules		×						
Windows File Log Rules	Client ID Address:	*						
LINUX Or Unix File Log Rules	Client IF Address.	·						
SYSLOG Rules	workload:							
SQL Server Log Rules	Operation:	2						
👻 🔚 Microsoft 365 Audit Log Rules	Result Status:	Failed						
MS365_LOG_ARCHIVE_ALL		Include Or Exclude Keywords. Enter Keywords Separated By Commas. To Exclude Criteria, Type A M And Minus Sign, Proceed With Character 'V', Wildcards '*' And 'Z' Are Supported	linus Sign First. To Escape	Comma				
PowerShell Script Log Rules								
Argent Omega For Microsoft 365	Events In Time Range:	00:00:00 - 23:59:59						
Argent Omega For SNMP	Alert Only If The Specific Event Happens	s More Than 1 Times						
Argent Omega For SQL Server	Alert If The Specific Event Does NOT Evi	ist .						
Argent Omega Web Defender	Correct Event If Seeing Result Status Of	Came Source:						
✓ Alerts		Same Source.						
Correction	Save To Archive Repository:	{default}						
Notification	Save Archive Data Only							
Alert Macro	Alert If Failed To Download Audit Log							
Relators	Save Performance Data To The Argent F	orecaster Using Data Store: {default}						L
✓ Macros	Tag 1:							
Imail Recipients	Tag 2:							
SMS Recipients	Tag 3:							
Windows Services	Post Event Even If The Same Event Is S	till Outstanding (Unanswered)						
Windows Processes	Do So Only After 1 Hour	Minute Since Event Is Post						
Users								
✓ I Calendars	Ignore the same outstanding Event If A							
Base Definitions	Post Event Only After Rule Is Broken	2 Vr More Times						
Holidays	Reset Counter							
 Administration 	After Event Is Post							
Ticense (Admin Only)	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):

= ARGENT ON	MEGA (2.2A-2207-A)	A Home	🔅 Theme -	(®) Argent Instant Help	? About	ပု Logout	RC22
👻 🐸 Tool Sets	Add Parameters						1
🕨 🔤 Argent Omega Baseline		_	_		_	_	
👻 🔚 Argent Compliance Automator	Properties Methods						
Windows Compliance Rules	1 SutcNow = [System.DateTime]::UtcNow						
Windows Event Log Rules	3 # Assign Log Name which is saved as part of archived record. Default is Rule Name						
Windows File Log Rules	5 \$P\$Player.LogName + "HyTestPSLog"						/
LINUX/Unix File Log Rules	6 7 # Unless log data is stateless, last read state should be retrieved first						- L'
SYSLOG Rules	8 # so that rule logic can resume reading from last read position						- I /
SQL Server Log Rules	<pre>10 Slastread = SPSPlayer.GetEventState()</pre>						
🕨 📒 Microsoft 365 Audit Log Rules	$\frac{11}{12}$ # Generate a synthetic event and put to the queue for archiving						/
👻 🔚 PowerShell Script Log Rules	13 14 Sevt = SPSPlayer.NeuGvent()						/
PS_ARCHIVE_DEMO	15 16 # Assign various event properties						
▶ Margent Omega For Microsoft 365	17 17 Assay to Los cells projetices						
Argent Omega For SNMP	18 # Required 19 Sevt.EventTimeUtc = SutcNow # Default value is current UTC time						
Argent Omega For SQL Server	20 Sevt.EventSeverity = 4 # 1 - Error, 2 - Warning, 4 - Informational 21						
Argent Omega Web Defender	22 # Optional						
🕨 🚾 Alerts	2-3 Sevt.EventUd = 1000 24 Sevt.EventUder = [Environment]::UserName						
Monitoring Groups	25 Sevt.EventCategory = 'P5 Demo' 26 Sevt.EventSource = 'P5'						
Relators	27 28 Bit Ker Data is saved in archived record as XVL, which can be overied						
Macros	29 # using XPath syntax.						
Calendars	30;# User Data is recommended as it is more efficient to query than persing 31;# Event Body text						
Administration	32, Sert.AddUserOata('MATA_1', 'MALUE_1') 34 Sert.AddUserOata('MATA_2', 'MALUE_2') 35 Sert.AddUserOata('MATA_3', 'MALUE_3') 36 37 F Event Body is the main information to store						
1	38 # Required						
i l	39 IT (SLASTFAGLASTRAGUEVENTIALAULT) 400 {						
	[41] Sevt.EventBody = "Last Read: Never'r'nCurrent: " + Sutchlow 42 }						
	<pre>43 cise 44 cise 4</pre>						
	50 51 # Update last read information 52 \$lastread.lastReadEventTimeUtc = SutcHow						

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:

■ ARGENT OME	GA (2.2A-2207-A)	Home Theme - Argent Instant Help About Logout	RC225
	Add Parameters		<u>^</u>
Argent Complance Automator Argent Complance Automator Windows Event Log Rules Windows File Log Rules Windows File Log Rules Windows File Log Rules Style Start Log Rules PowerShell Script Log Rules PowerShell Script Log Rules Argent Omega For Style Ar	CA (2.42207-A) Advances Properties Advances Properties Properties Properties br>Properties Pro	Home Theme- Argent Instant Help About Logout	
	<pre>32 F Breet Body is the main information to store 33 # Browind 39 # Browind 30 # Browind 30 # Browind 40 { 41 Sevt.EventBody = "Last Read: Hever'n"nCurrent: " + Sutclow 42 } 43 { 44 { 43 { 43 { 44 { 43 { 43 { 43 {</pre>)'r'nCurrent: " + Sutclinu	
	46 47 48 Dotional 49 Seri: ForeRechum - Slastread.LastReadEventId 50 Seri: ForeRechum - Slastread.information 51 E Update last read information 52 Slastread.LastReadEventTimeUtc - SutClow		

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

= ARGENT OME	GA (2.2A-2207-A)		effective Home	🔅 Theme -	(®) Argent Instant Help	? About	U Logout	RG225
▼ 🐸 Tool Sets		and and a						
🕨 🚧 Argent Omega Baseline	Rule 15 Broken II Performance Metrics 15 Over Thr	reshold						• •
✓ Magent Compliance Automator	Name	Туре	Va	ue				
Windows Compliance Rules	P1	Numeric	10	0				
Windows Event Log Rules								
Windows File Log Rules								
LINUX/Unix File Log Rules								
SYSLOG Rules								
SQL Server Log Rules								
Microsoft 365 Audit Log Rules								
✓ MoverShell Script Log Rules								
PS_ARCHIVE_DEMO								
Argent Omega For Microsoft 365	L							
Argent Omega For SNMP	Properties Methods							
Argent Omega For SQL Server	1 SutcNow = [System.DateTime]::UtcNow							
Argent Omega Web Defender	2 3 # Assign Log Name which is saved as part of arc	chived record. Default is Rule Name						
Alerts	4 5 \$P\$01aven Loniane = "W/TertP\$Lon"							
Monitoring Groups	6							
Relators	7 # Unless log data is stateless, last read state 8 # so that rule logic can resume reading from la	e should be retrieved first ast read position						
Macros	9 10 \$lastread = \$P\$Player.GetEventState()							
Calendars		no for eachider						
Administration	12 + denerate a synthetic event and put to the que	eve for archiving						
	14 Sevt = SPSPlayer.NewEvent() 15							
	16 # Assign various event properties							
	18 # Required							
	19 Sevt.EventTimeUtc = SutcNow # Default value 20 Sevt.EventSeverity = 4 # 1 - Error, 2 - Warni	is current UTC time ing. 4 - Informational						
	21 22 # Ontional							
	23 Sevt.EventId = 1000							
	25 Sevt.EventCategory = 'PS Demo'							
	26 Sevt.EventSource = 'PS' 27							
	28 # User Data is saved in archived record as XML,	, which can be queried						
	30 # User Data is recommended as it is more effici	ient to query than parsing						
	31 # Event Body text 32							

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

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

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

■ ARGENT OM	EGA (2.2A-2207-A)	ome 🔐	theme -	(1) Argent Instant Help	? About	U Logout	RG22s
Tool Sets Tool Sets Tool Sets Argrent Compalance Automator Windows Compliance Rules Windows Compliance Rules Windows Event Log Rules Windows Flexe Log Rules SYSLOG Rules SSYSLOG Rules SSYSLOG Rules SSYSLOG Rules Microsoft 355 Audit Log Rules SSYSLOG Rules Microsoft 355 Audit Log Rules SSYSLOG Rules Argrent Omega For Microsoft 355 Argrent Omega For Microsoft 355 Argrent Omega For SNIPP Argrent Omega For SSNIP Argrent O	Signal Signal					Fidl Sc	reed

Argent_Compliance_Automator.doc