

Argent Web Defender

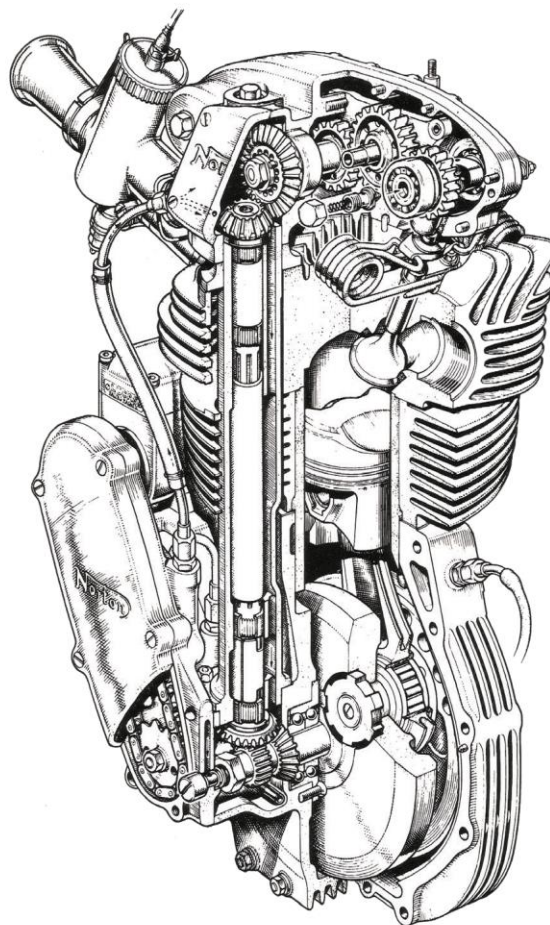


Table Of Contents

Introduction	3
Prerequisites To Run Web Session Rules	5
Log-On Screen.....	6
Home Screen	7
Configure Internet Objects In CMDB-X	8
Web Session Rules	15
Website Availability Rules	28
Website Response Time Rules	29
Website Reliability Rules	30
Email Performance Rules	31
FTP Site Rules	32
Windows Performance Rules	33

Introduction

What is website performance monitoring?

This is the process of measuring and testing how a website, web server, web application or other web-based service responds during end user interactions.

Using website performance data, administrators can more easily perform website speed optimization, reduce bounce rates, and increase ease of use and satisfaction for end users. The end goal is ensuring each service functions as expected.

Argent Omega Web Defender provides Toolsets for comprehensive monitoring of websites, so that network administrators can collect data related to internet latency, network hop issues, and other metrics to help build a snapshot of the website or web server's performance. These performance data are then translated into report, graph, or chart form, allowing for quick, at-a-glance comprehension of the overall state of the website.

The Toolsets provided by Argent Omega Web Defender not only monitors website performance but also it does the performance monitoring of web applications, remote email servers, and FTP sites, etc.

Below are the most important features and benefits of Argent Omega Web Defender Toolsets:

Simple Website Monitoring To Prevent Downtime:

- Monitor your website at regular intervals.
- Get notified instantly when the website goes down or if the page loading time increases.
- Utilize downtime analysis reports to resolve website performance issues or downtime.

End-To-End Web Monitoring:

- Handles all known HTTP error codes.
- Check for one or more known error codes for each URL.
- The Toolset provides preconfigured error cases. It has a list of all known HTTP errors.

Root Cause Analysis And Correction:

- Run WMI and Linux or UNIX scripts if a web server is offline or slow.
- Preconfigured scripts for checking system resources like CPU, memory, NIC traffic, etc.
- Screenshot capturing.

It is possible to identify and correct the root cause of an issue without manual intervention.

Robotic Web Testing:

- Mimics user interactions.
- Supports manual operations such as mouse clicks and keyboard input.

It is possible to automatically run laborious, pain staking web testing which normally requires human interaction.

1. Web Data Scraping:

- Retrieves data from web pages and makes it available as variables in script.

Example: Go to finance.yahoo.com, retrieve Apple's stock price, and alert if it crosses a threshold or store the stock price in Argent Forecaster for Analytics.

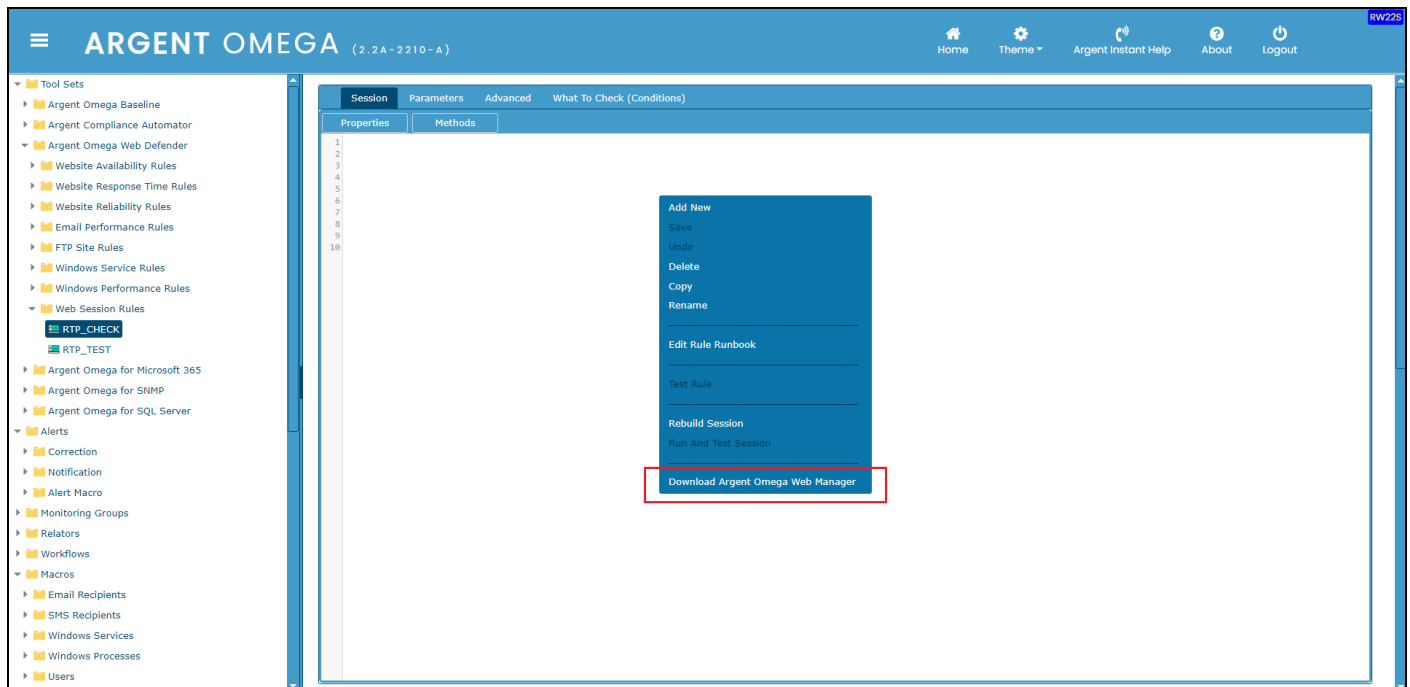
It is possible to configure notification alerts based on data updated in websites. Also use Argent Forecaster and Argent Reporter for web-scraped data.

2. Email Performance Monitoring:

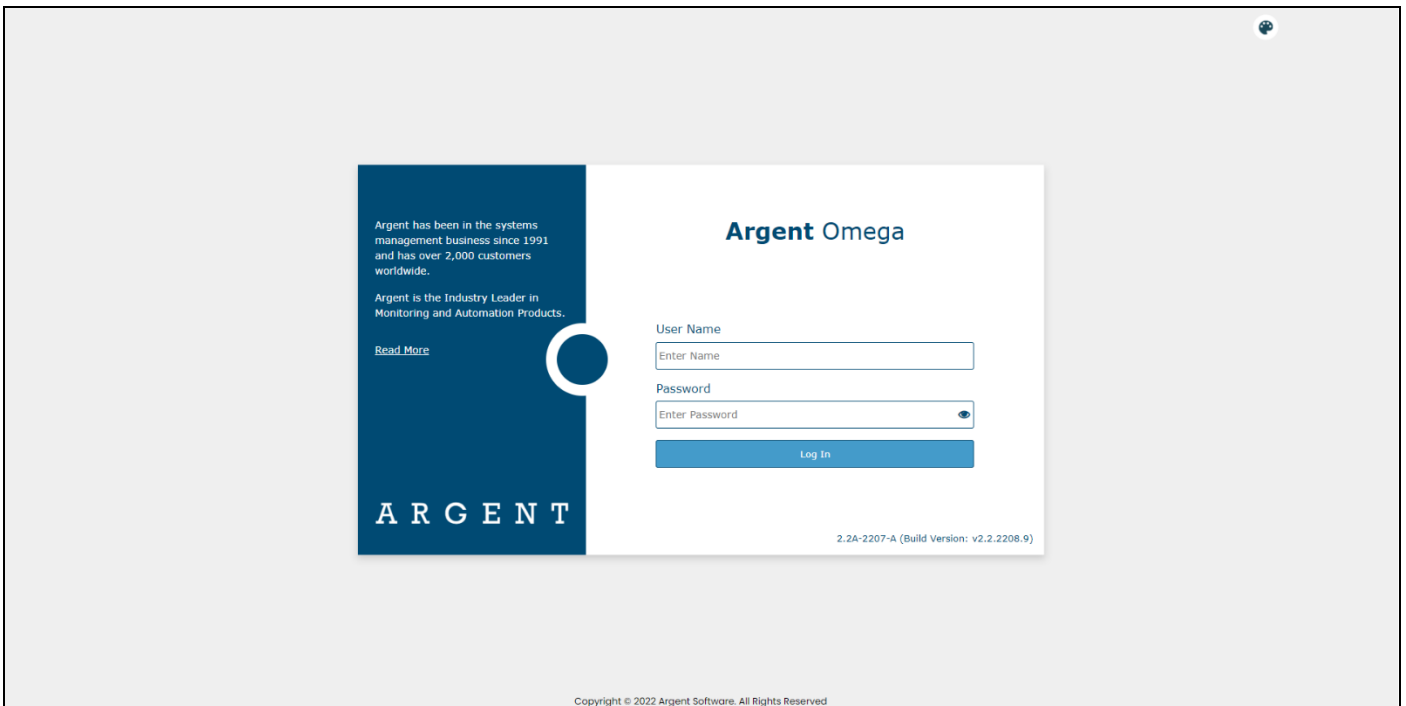
- Monitor the email sending and receiving capabilities of a SMTP, POP and IMAP servers and test round-trip email performance.
- Performance data is saved for trend analysis using the Argent Forecaster.

Prerequisites To Run Web Session Rules

Argent Omega Web Manager should be installed in the machine to record Web Sessions in Web Session Rules. To download Argent Omega Web Manager, go to any Web Session Rule and select **Download Argent Omega Web Manager** option from context menu. This will download Setup.msi package into the machine. After downloading, install the downloaded **Setup.msi** package.



Log-On Screen



The Argent Omega validates the authenticity of the user through log-on screen.

Three types of user accounts can logon to Argent Omega:

- Windows User Accounts
- Demo Accounts
- Internal Accounts

Argent Omega uses Windows authentication to login Windows user accounts into Argent Omega. If the Argent server is in an Active Directory Domain environment, then the user will be authenticated by Active Directory. If the server is Standalone or in a Workgroup, local Windows user authentication is used. For Windows user accounts, the recommended approach is to create a separate user group for Windows users and assign the required rights.

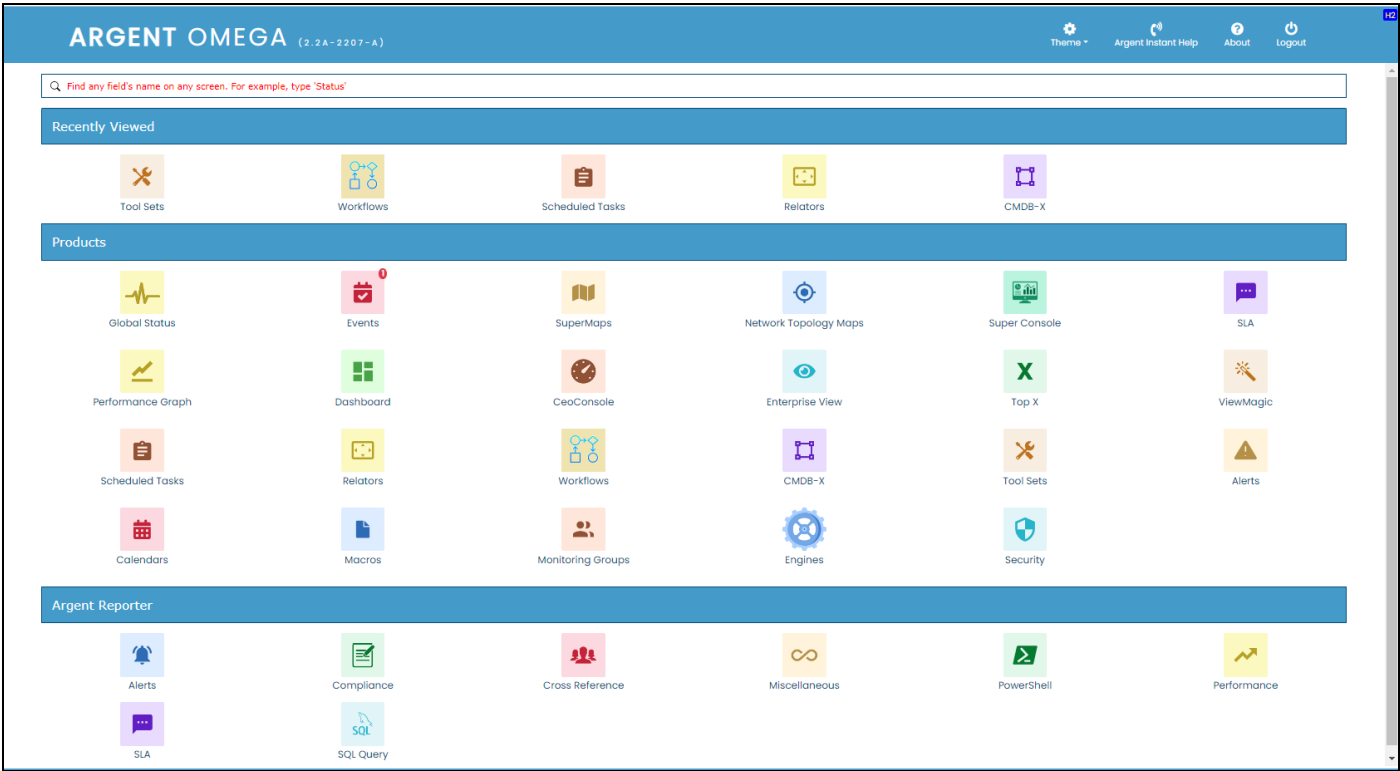
Demo Accounts can be created in Argent Omega Security section and are used for demonstration purposes. Demo accounts are read-only accounts and it uses Argent private authentication to login into Argent Omega. Usually Demo Accounts has short validity time, and the access is limited to specific IP addresses only.

Internal Accounts also can be created in Argent Omega Security section, and will behaves like normal Windows account. Use Argent private authentication for login.

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

Home Screen

After logging in, Argent Omega will redirect to Home screen.



Configure Internet Objects In CMDB-X

It is possible to license following four types of objects in Argent Omega Web Defender:

- URL Object
- Mail Object
- FTP Object
- Windows Servers

Configure URL Object In CMDB-X

Argent Omega contains Web Session Rules for Automated Website Monitoring. It also contains the Rules to monitor the Availability and Response Time of websites. Specify **Type** as **URL Object** while adding to the CMDB-X as shown below:

The screenshot displays the Argent Omega web interface. A modal dialog titled "Manually Add An Entry" is open, allowing the user to add a new entry to the CMDB-X. The dialog contains the following fields:

- Name:** ARGENT
- Alias:** (empty)
- Domain:** (empty)
- VM Hosting Environment:** None
- Type:** URL Object (highlighted with a red box)
- Network Group:** Demo Group
- Location:** MUMBAI

The background shows a table of network groups with columns: Network Group Or Machine, Type, Alias, Licensed, Suspend, Location, and Contact. The table lists various IP devices and Windows servers. On the right, there is a sidebar with "Properties" and "Display Options" sections.

Then specify the following CMDB-X properties:

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The main table lists network groups and machines. The 'ARGENT' URL object is highlighted. The properties panel on the right shows the configuration for the 'ARGENT' URL object, including the URL Path, Authentication settings, and Proxy settings.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
Demo Group	Network Group					
First Network Group	Network Group				MUMBAI	
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
192.168.96.106	IP Device	switchbecab4	Yes		NEW YORK	
192.168.96.57	IP Device		Yes		MUMBAI	
2222	Linux/UNIX		Yes		NEW YORK	
A1-2019-009	Windows Machine		Yes		MUMBAI	
A1-MFC-102-W10	Windows 10 Pro		Yes			
ADK-1	Linux/UNIX		Yes		NEW YORK	
ARG-365	Microsoft 365 Service Unit				MUMBAI	
ARGENT	URL Object		Yes		MUMBAI	
AUBNECTX02	Windows Machine	Citrix Server 2	Yes		Brisbane	
AUWINCF501	IP Device	Winnellie FS			Brisbane	

Group Or Key	Value
Name	ARGENT
Licensed Products	Argent Omega Baseline, Argent Omega Web Defender
Alias	
URL Object	
URL Path	https://www.argent.com/
Authentication	
Logon User	
Password	
Auth Mode	Basic
Service Port	(default)
Proxy	
Proxy Server	
Proxy Server Port	
Proxy User	
Proxy Password	
Vital URLs To Check	
URL #1	https://www.argent.com/products/p...
TCP Parameters	
System Info Caching Minutes	720

URL Path: The path for the URL.

Authentication: The authentication scheme to use when server authorization is required. Any of the following type of Authentication Mode can be set:

- Basic
- Digest
- NTLM
- Negotiate

If Logon User and Password properties are empty, no authentication will be performed. By default, it uses Basic authentication if Logon User and Password properties are set. Otherwise, the selected authentication will be attempted.

Service Port: The port for the URL.

Proxy: Specify proxy settings if there is a proxy server. This section contains properties describing the proxy settings through which the Argent Omega Web Defender will attempt to connect to the specified website. There are options to configure proxy server name, port, proxy username and password.

Vital URLs To Check: Specify critical URLs. The Rule will check the availability of specified vital URLs.

Configure Mail Object In CMDB-X

Argent Omega Web Defender contains the Rules to monitor the performance of email protocols such as SMTP, POP and IMAP. Specify **Type** as **Mail Object** while adding the service to the CMDB-X as shown below:

The screenshot displays the ARGENT OMEGA (2.2A-2207-A) interface. A modal dialog titled "Manually Add An Entry" is open, allowing the user to configure a new entry. The dialog fields are as follows:

- Name: SMTP_1
- Alias: (empty)
- Domain: (empty)
- VM Hosting Environment: None
- Type: Mail Object
- Network Group: First Network Group
- Location: MUMBAI

The background interface shows a table of network devices with columns: Network Group Or Machine, Type, Alias, Licensed, Suspend, Location, and Contact. The right-hand side features a "Properties" panel with various configuration options for the selected device.

Then configure the following Mail Service CMDb-X properties:

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The main table lists various network devices and their properties. The 'Properties' panel on the right is configured for the 'SMTP_1' mail service.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
192.168.96.106	IP Device	switchbecab4	Yes		NEW YORK	
192.168.96.57	IP Device		Yes		MUMBAI	
2222	Linux/UNIX		Yes		NEW YORK	
AI-2019-009	Windows Machine		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ADK-1	Linux/UNIX		Yes		NEW YORK	
ARG-365	Microsoft 365 Service Unit				MUMBAI	
ARGENT	URL Object		Yes		MUMBAI	
AUBNECTX02	Windows Machine	Citrix Server 2	Yes		Brisbane	
AUWINCF501	IP Device	Winnellie P5			Brisbane	
CNN	URL Object	https://edition.cnn.com/	Yes		NEW YORK	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
INTRANET	URL Object	https://intranettest.cardno.com			Brisbane	
PERPRN01P	IP Device	Perth Print Server	Yes		Brisbane	
POP	Mail Object				MUMBAI	
SMTP_1	Mail Object		Yes		MUMBAI	
TEST_365	Microsoft 365 Service Unit		Yes		MUMBAI	
TEST_EMAIL	Mail Object	testargent10@gmail.com	Yes		NEW YORK	

Group Or Key	Value
Name	SMTP_1
Licensed Products	Argent Omega Web Defender
Alias	
Mail Service	
IP Address	smtp.gmail.com
Authentication	
Logon User	testargent10@gmail.com
Password	*****
Auth Mode	User Password
Service Port	465
SSL Start Mode	Automatic
Type	SMTP
Destination Email Address	testargent11@gmail.com
Associated Object	POP
TCP Parameters	
System Info Caching Minutes	720
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	
Default Settings	

IP Address: The name or address of a mail server (mail relay).

Authentication: The Authentication Mechanism property to be used when connecting to the mail server.

Any of the following type of Authentication Mode can be set:

- User Password
- NTLM
- Kerberos

By default, it uses **User Password** authentication mode if Logon User and Password properties are set.

Otherwise, the selected authentication will be attempted.

Service Port: The server port for Mail service.

SSL Start Mode: Determines how the SSL negotiation to be started. It can be any one of the following:

- None: No SSL negotiation, no SSL security. All communication will be in plaintext mode.
- Automatic: If the remote port is set to the standard plaintext port of the protocol, the component will behave the same as if SSL Start Mode is set to Explicit. In all other cases, SSL negotiation will be Implicit.
- Implicit: The SSL negotiation will start immediately after the connection is established.

- Explicit: The component will first connect in plaintext, and then explicitly start SSL negotiation through a protocol command.

Type: Select the type of Mail service. It can be any one of the following:

- SMTP
- POP3
- IMAP

Destination Email Address: The address to which test emails to be sent to check the email performance.

Associated Object: It is possible to configure multiple email protocols in a Mail object. It is useful when doing email round-trip performance test, it requires to use both SMTP and POP or IMAP objects. You can select the configured Mail service from the list as an Associated Object.

Configure FTP Object In CMDB-X

File Transfer Protocol (FTP) is used to transfer files between a server and client in a TCP or IP network. Users, who have been granted access, can receive and transfer files in the File Transfer Protocol server. Secure version of the FTP protocol is SFTP. SFTP encrypts the transmitted commands and data using SSH (Secure Shell Protocol). Argent Omega Web Defender provides the Rules for FTP monitoring that helps enterprises and other organizations to ensure smooth delivery of FTP or SFTP facilities. Specify

Type as **FTP Object** while adding the object to the CMDB-X as shown below:

The screenshot shows the Argent Omega CMDB-X interface. A modal dialog titled "Manually Add An Entry" is open. The dialog contains the following fields:

- Name:
- Alias:
- Domain:
- VM Hosting Environment:
- Type: - Network Group:
- Location:

Buttons for "OK" and "Cancel" are at the bottom of the dialog. The background shows a table of network devices and a properties panel on the right.

Then specify the following FTP service CMDB-X properties:

The screenshot shows the ARGENT OMEGA (2.2A-2207-A) interface. The main table lists various network devices and their properties. The 'FTP_1' service is highlighted, and its properties are shown in a sidebar on the right.

Network Group Or Machine	Type	Alias	Licensed	Suspend	Location	Contact
192.168.108.97	Linux/UNIX		Yes		MUMBAI	
192.168.111.1	IP Device		Yes		MUMBAI	
192.168.111.18	IP Device				MUMBAI	
192.168.111.2	IP Device		Yes		MUMBAI	
192.168.111.3	IP Device		Yes		MUMBAI	
192.168.111.4	IP Device	APC_UPS_003	Yes		MUMBAI	
192.168.111.5	IP Device		Yes			
192.168.37.1	IP Device		Yes		MUMBAI	
192.168.96.106	IP Device	switchbecab4	Yes		NEW YORK	
192.168.96.57	IP Device		Yes		MUMBAI	
2222	Linux/UNIX		Yes		NEW YORK	
AI-2019-009	Windows Machine		Yes		MUMBAI	
AI-MFC-102-W10	Windows 10 Pro		Yes			
ADK-1	Linux/UNIX		Yes		NEW YORK	
ARG-365	Microsoft 365 Service Unit				MUMBAI	
ARGENT	URL Object		Yes		MUMBAI	
AUBNECTX02	Windows Machine	Citrix Server 2	Yes		Brisbane	
AUWINCF501	IP Device	Winnellie PS			Brisbane	
CNN	URL Object	https://edition.cnn.com/	Yes		NEW YORK	
DND-MFC-SQL	Windows Server		Yes		MUMBAI	
FTP	FTP Object		Yes		MUMBAI	
FTP_1	FTP Object		Yes		MUMBAI	
INTRANET	URL Object	https://intranettest.cardno.com			Brisbane	
PERPRN01P	IP Device	Perth Print Server	Yes		Brisbane	
POP	Mail Object				MUMBAI	

Group Or Key	Value
Name	FTP_1
Licensed Products	Argent Omega Web Defender
Alias	
FTP Service	
IP Address	test.rebex.net
Authentication	
Logon User	demo
Password	*****
Auth Mode	Basic
Service Port	{default}
SSL Start Mode	
Type	FTP
System Info Caching Minutes	720
Monitoring Level	Normal
Tier	Not Specified
Tag	
Location	MUMBAI
Contact	
Owner Accounts	
Default Settings	
Time Zone Settings	Same as Location
Critical	No

IP Address: The domain name or IP address of the FTP server.

Authentication: For SFTP sites, Authentication Mode can be any of the following:

- Password
- Keyboard Interactive

FTP sites only use basic Authentication.

Service Port: The port for the FTP service.

SSL Start Mode: Determines how the SSL negotiation to be started. It can be any one of the following:

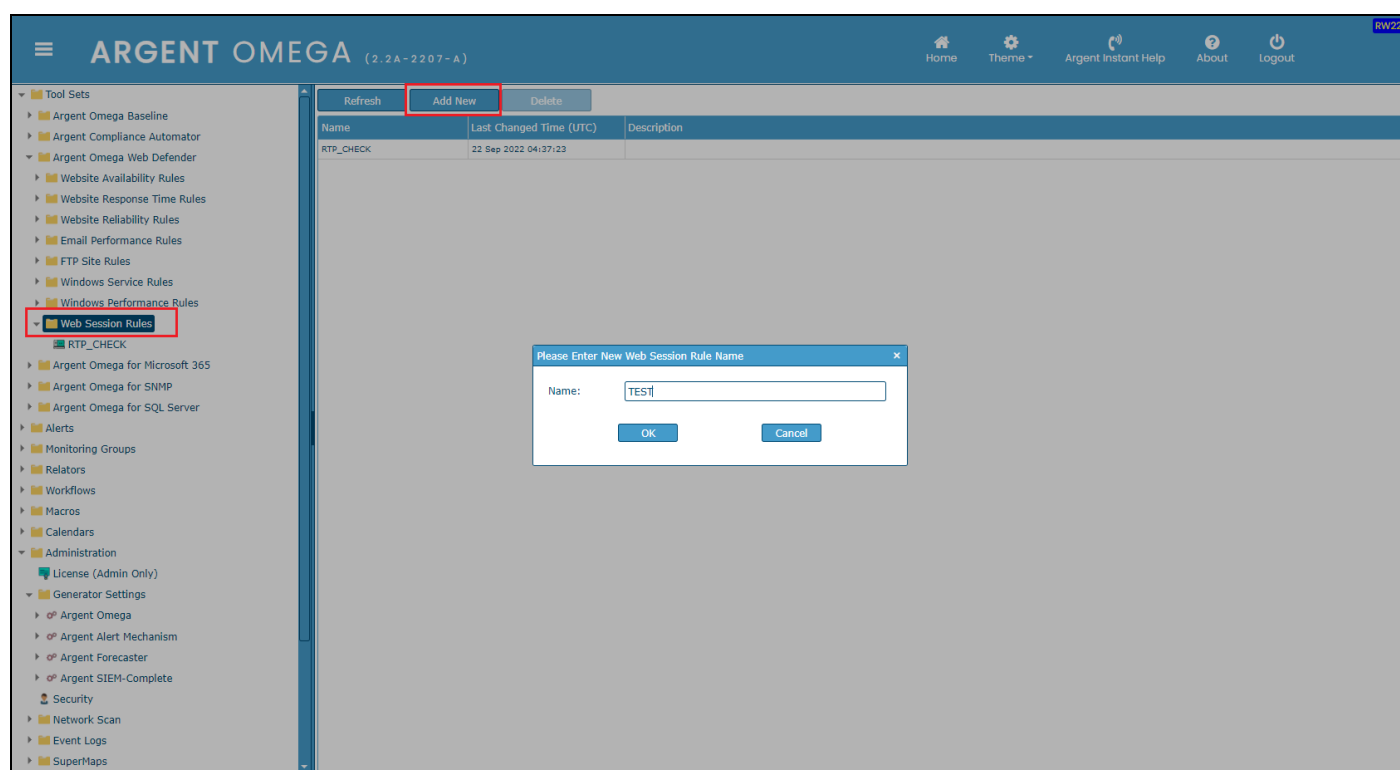
- None: No SSL negotiation, no SSL security. All communication will be in plaintext mode.
- Automatic: If the remote port is set to the standard plaintext port of the protocol, the component will behave the same as if SSL Start Mode is set to Explicit. In all other cases, SSL negotiation will be Implicit.
- Implicit: The SSL negotiation will start immediately after the connection is established.
- Explicit: The component will first connect in plaintext, and then explicitly start SSL negotiation through a protocol commands.

Type: Select the service type. It can be either FTP or SFTP.

Web Session Rules

Argent Omega Web Session Rules built-in with Chromium based browser to deliver automated website monitoring. Web Session Rules records specific user activities in a website and plays back the recorded sequence in Chromium browser to mimic user activities and collect performance metrics. You can record the user activities of any licensed URL object. The recorded activity of a URL object is called Web Session. Web Session Script is generated against each Web Session. Any number of Web Sessions can be created against a licensed URL object.

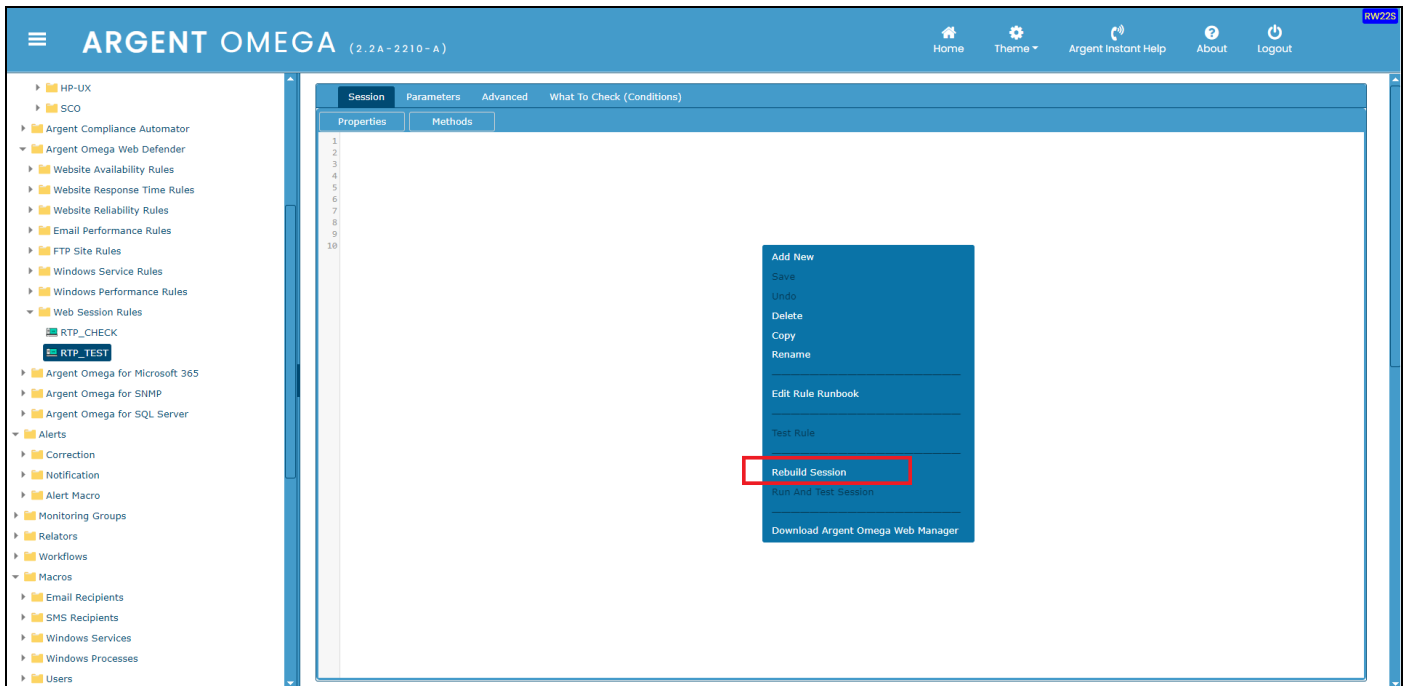
To create a new Web Session, go to Web Session Rules and click **Add New**. Then give a name for the Web Session:



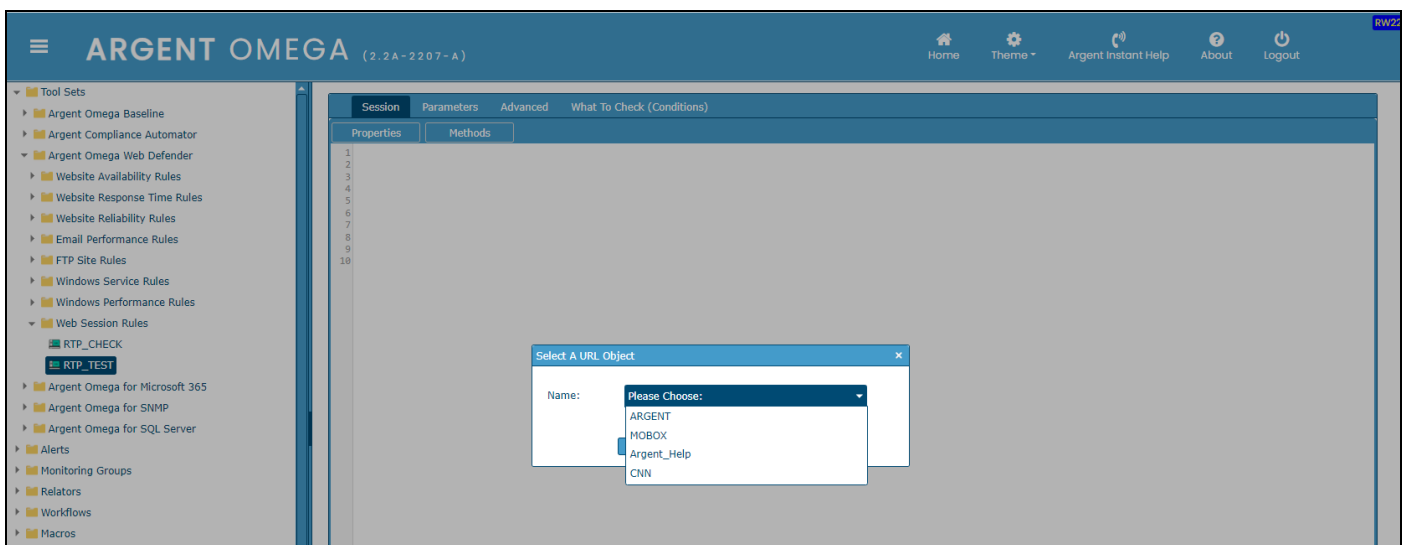
To record a new Web Session, select Rebuild Session from context menu.

Note:

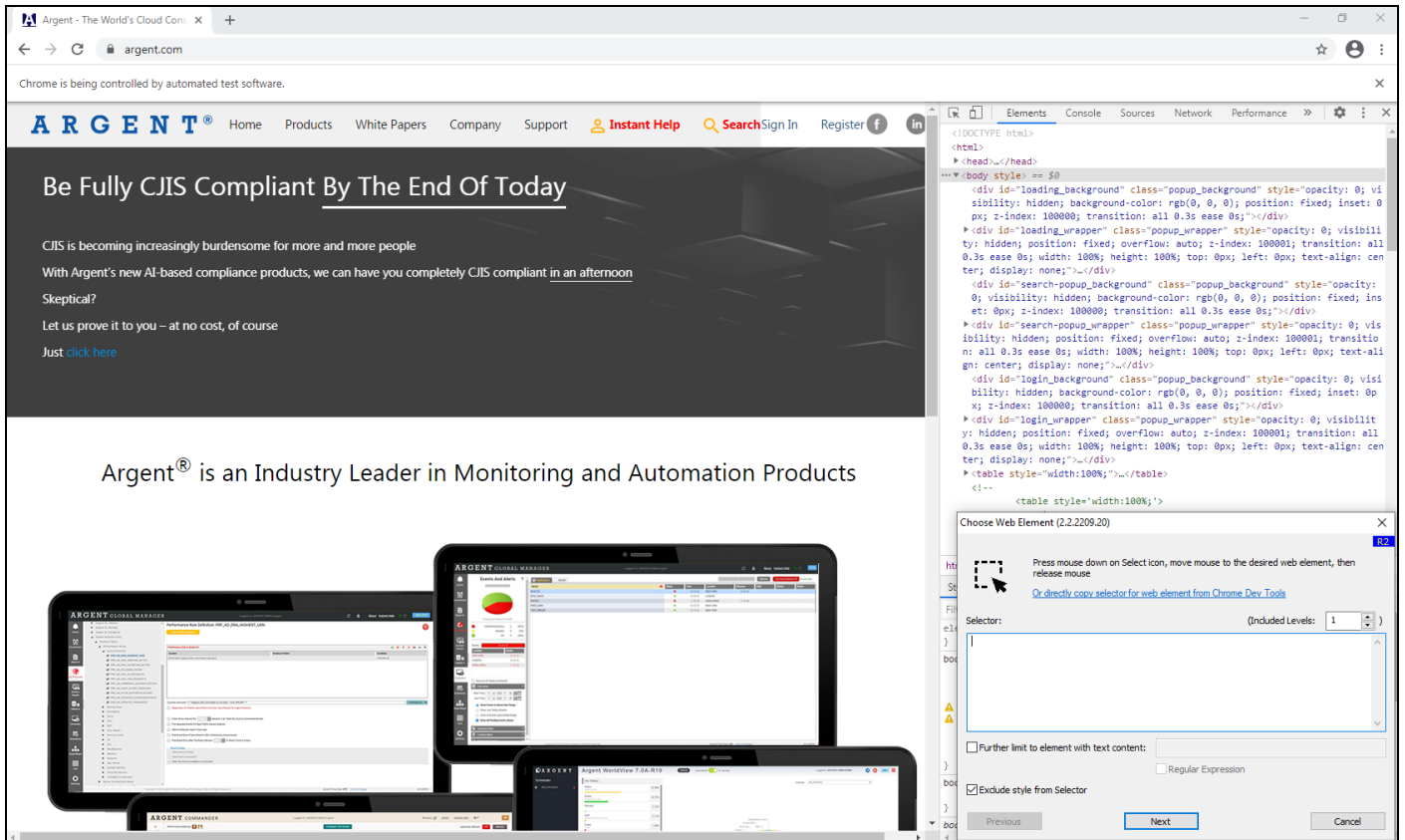
Make sure that Argent Omega Web Manager is installed in the machine on which Web Session is recording. Other than the Primary Generator, it is possible to record Web Session from any machine that can access Argent Omega WUI URL:



Select the licensed URL object from list and click OK:



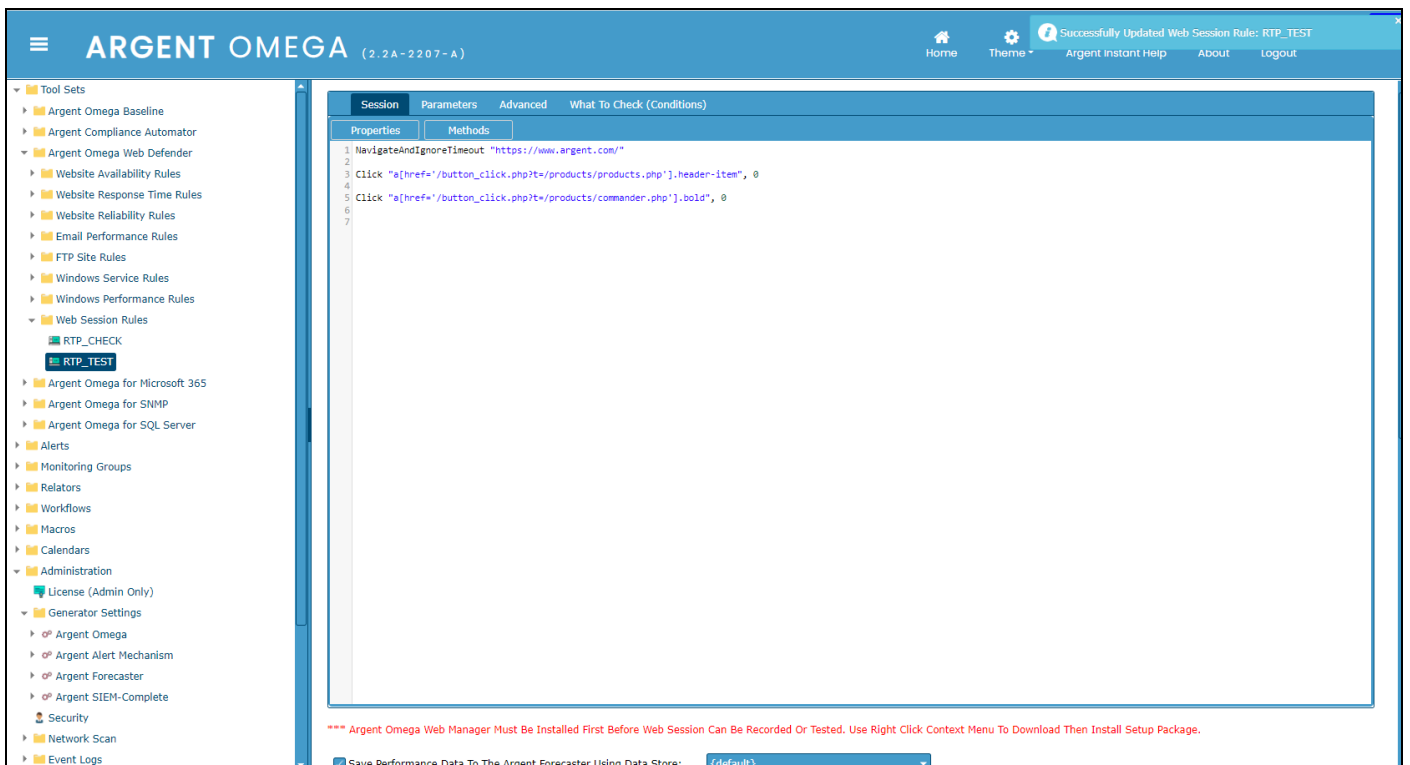
This will load the website specified in the URL object in Chromium browser and show the Argent Omega Web Element Selector tool on the bottom corner of the screen as shown below:



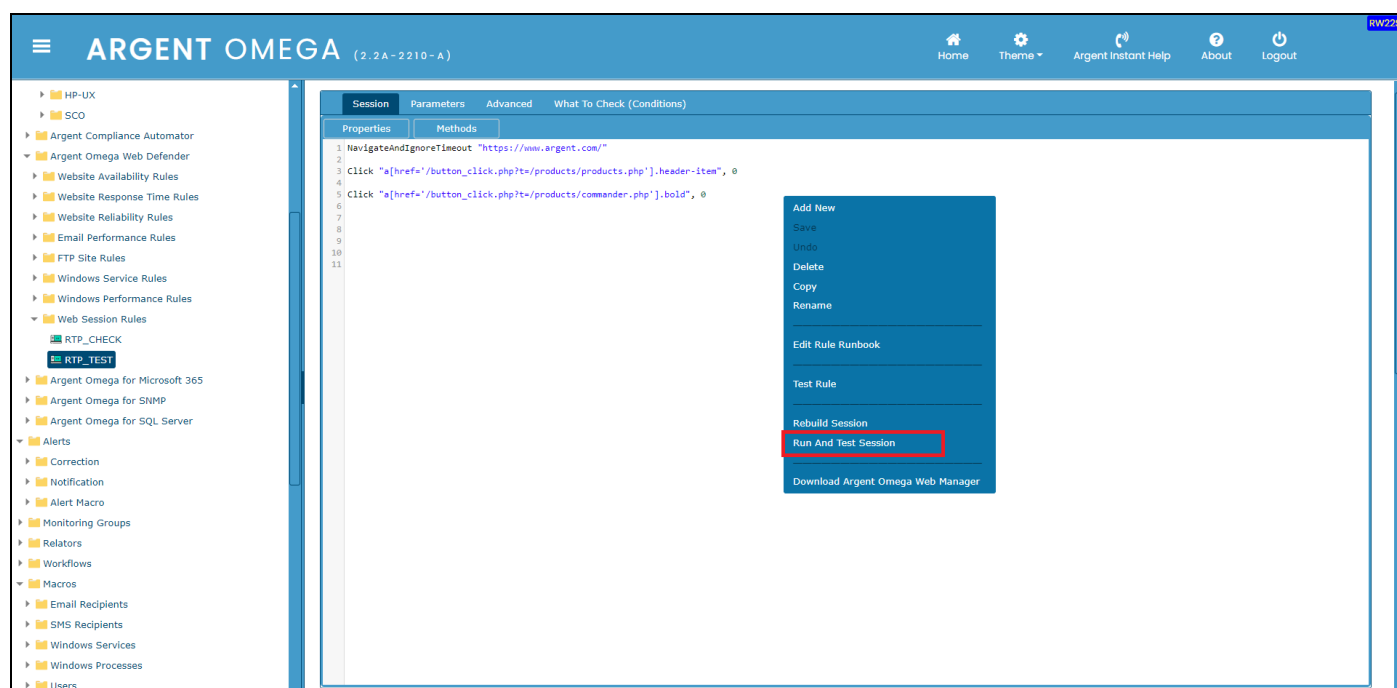
To record a user activity using Element Selector, refer the following Argent KBI article:

https://help.argent.com/#argent_sentinel_selector_new

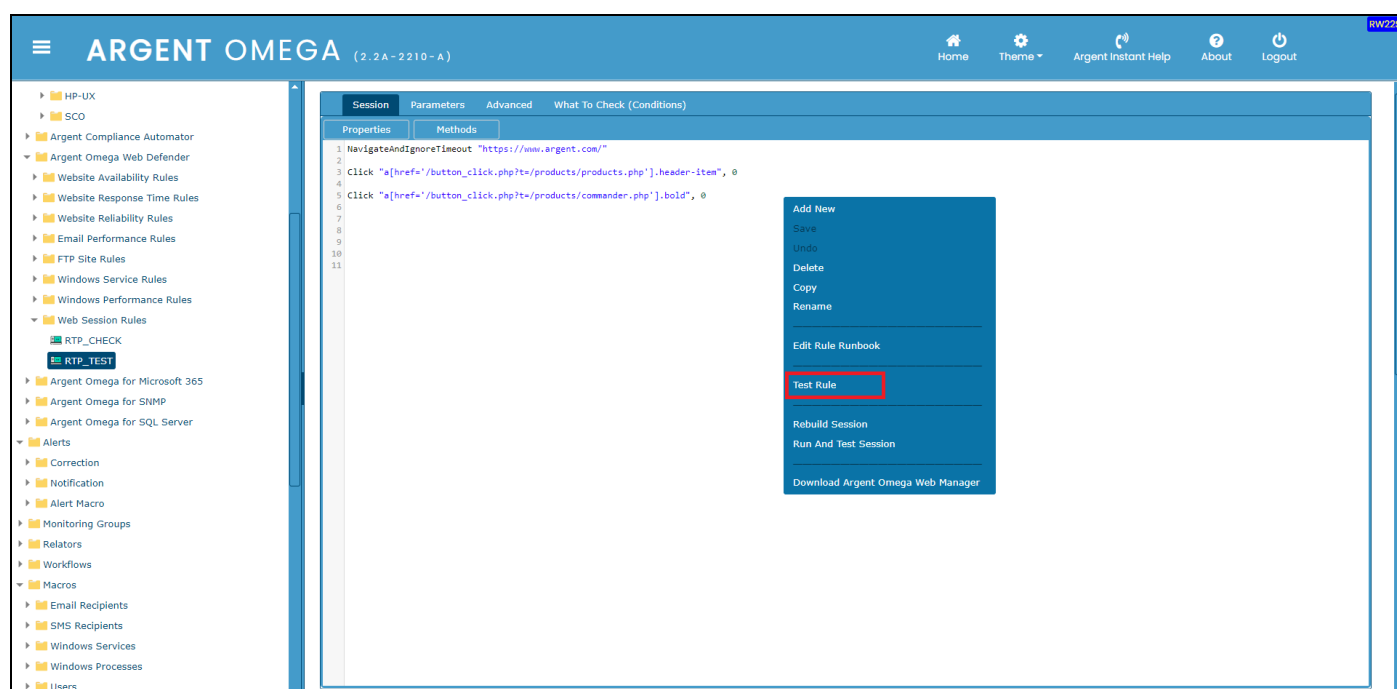
After session recording is completed, you can see the session script in Session tab as shown below:



To replay the recorded session in Chromium browser, click **Run and Test Session** context menu option:



To test the Web Session Rule, click **Test Rule** context menu option:



It is possible to customize the generated Web Session script. Argent Omega Web Defender provides predefined Methods and Properties to allow the user to define required monitoring logic.

Predefined Properties:

The screenshot shows the ARGENT OMEGA (2.2 A - 2207 - A) interface. The left sidebar contains a tree view of tool sets, including 'RTP_TEST'. The main panel displays a table with two tabs: 'Properties' and 'Methods'. The 'Properties' tab is active, showing a list of predefined properties and their methods.

Properties	Methods
Home URL	Home Address of URL Object (Read-only)
DisableNewWindow	Allow/Disallow New Window Popup (Write-Only)
SaveWaterfall	Start/Stop Waterfall Capturing (Write-Only)
OnErrorResume	VBScript Error Handling (Write-Only)
UserAgent	Set Custom User Agent Value (Write-Only)
FindElementInSeconds	Set Maximum Wait Time (Write-Only)
ScreenShotPath	Set Folder To Save Screen Shot (Write-Only)
EmailScreenShot	Email Or Not Email Screen Shot If Error Happens (Write-Only)
ParamDefined	Test If A Indexed Parameter Is Defined (Read-Only)
Param	Get Value Of A Indexed Parameter (Read-Only)
MatchedParam	Get Matching Value Of A Indexed Parameter (Read-Only)
PageUrl	Get Current Page Address (Read-Only)
PageLoadTime	Get Loading Time of Current Page In Seconds (Read-Only)

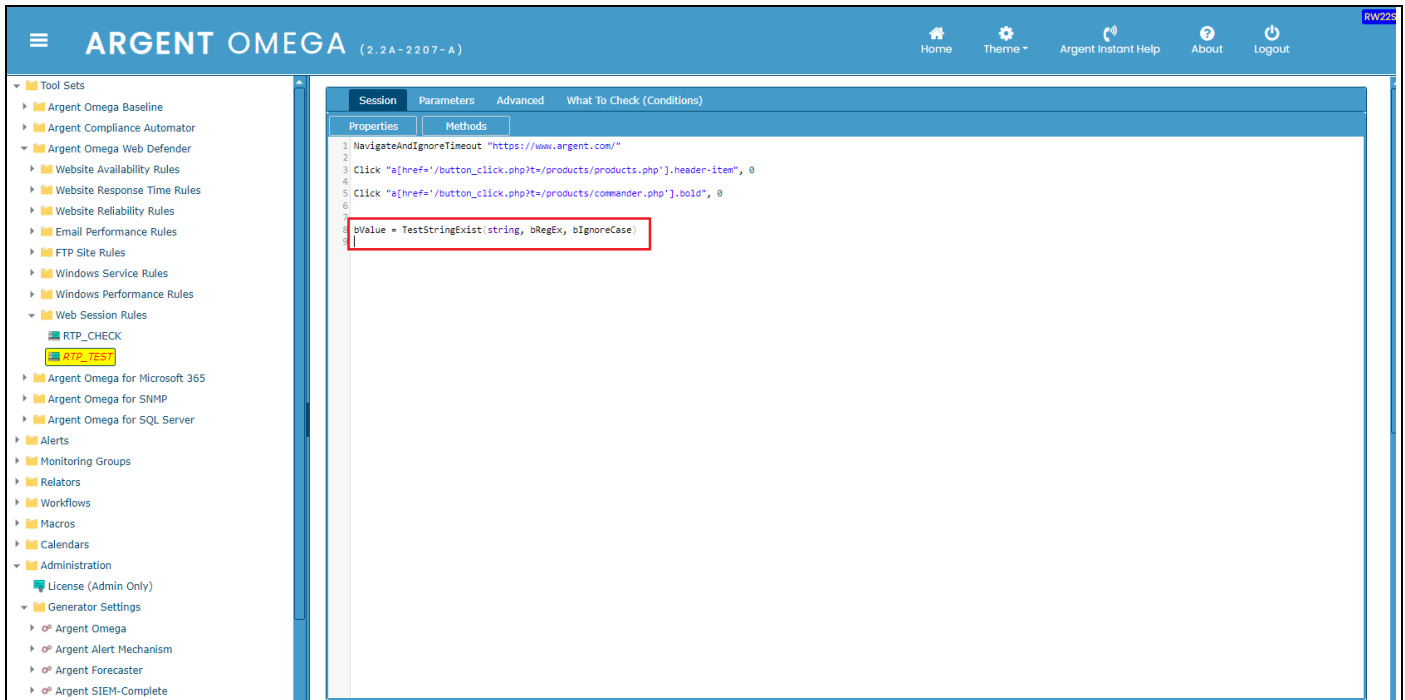
Predefined Methods:

The screenshot shows the ARGENT OMEGA (2.2 A - 2207 - A) interface. The left sidebar contains a tree view of tool sets, including 'RTP_TEST'. The main panel displays a table with two tabs: 'Properties' and 'Methods'. The 'Methods' tab is active, showing a list of predefined methods and their descriptions.

Properties	Methods
1 NavigateAndIs	Display
2	Write Message to Task Log
3 Click "e[href	FireEvent
4	Register an Event to Be Fired through Argent Alert Mechanism
5 Click "e[href	SavePredictor
6	Save Performance Data to Argent Forecaster
7	SaveScreenShot
	Screen Shot Current Page and Save to Local File
	SendEmail
	Send Email Message
	TestStringExist
	Test If Current Page Contains Specified String
	Navigate
	Navigate to A URL Address
	NavigateAndIgnoreTimeout
	Navigate to A URL Address And Ignore Timeout Error If Any
	Navigate2
	Navigate to A URL Address with Advanced Options
	StartPerfLog
	Begin A Block Of Script To Record Performance Metrics
	EndPerfLog
	Close A Block Of Script To Record Performance Metrics
	WaitNewPage
	Wait Until New Page Is Loaded
	WaitTimeout
	Pause For Specified Seconds
	CloseNewWindow
	Close Current Popup Window
	AcceptDialog
	Enter Text String to Input Dialog Box
	DismissDialog
	Dismiss Current Dialog Box
	AllowExternalUrl
	Allow Specific External URL
	IsElementDisabled
	Test If A Element Is Disabled
	GetElementAttributeValue
	Get Element Attribute Value
	GetDownloadedFile
	Get Downloaded File Path
	MoveFileToFolder
	Move A File to Specified Folder
	RaiseError
	Raise Error And Terminate Script Execution
	ResetErrorState
	Reset Current Error State If Any
	GetErrorState
	Return Current Error State

To use a method or property in Web Session script, select it from the dropdown list. The selected method or property will be displayed in script box with the usage syntax.

For example, on clicking **TestStringExist** method, it displays in the script box like below:




Define Script Parameters

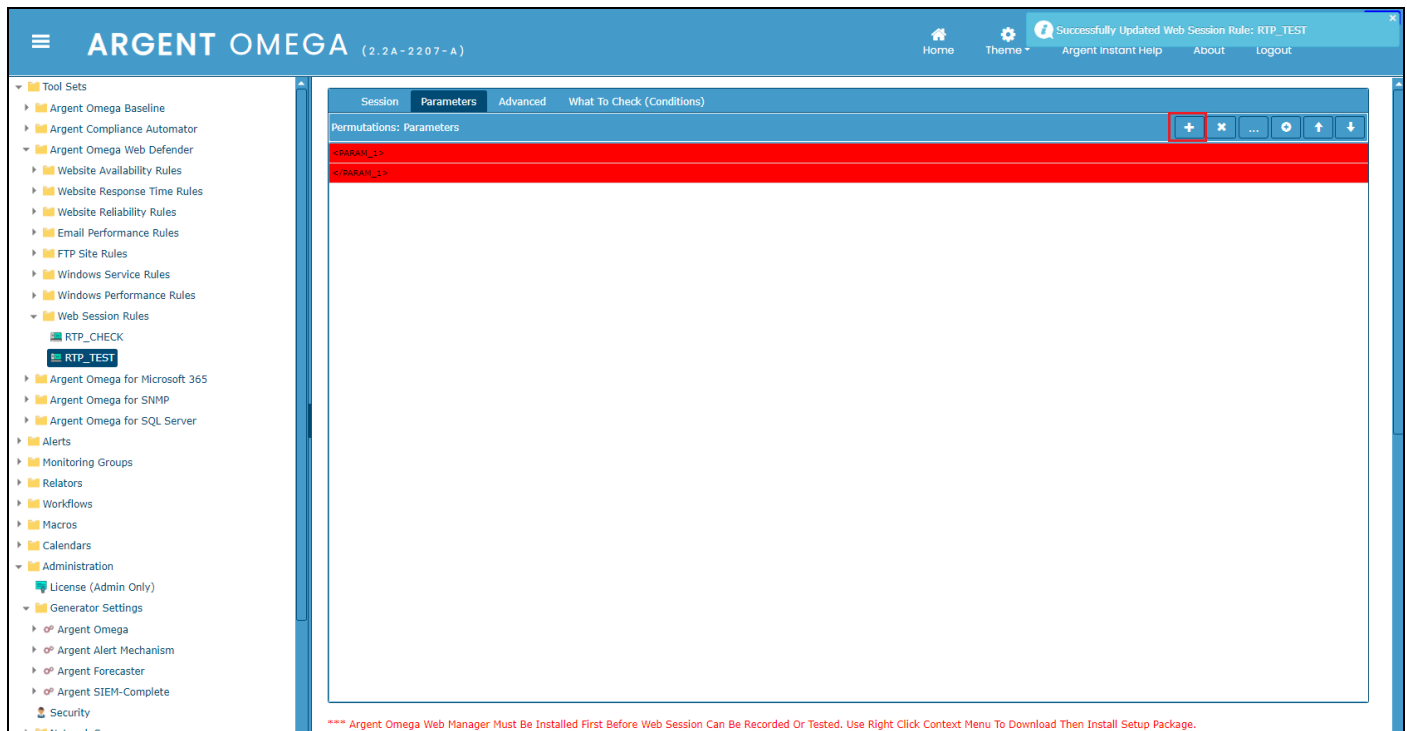
You can define Script Parameters in Parameters tab. The defined Parameters can be used in the Web Session Script to enhance the monitoring. A set of predefined Properties are available to use the Parameters in Session script. That will be described later in this document.

A set of Parameter values are enclosed with <PARAM_{Index}> and </PARAM_{index}>.

Example:

```
<PARAM_1>
Apple
Banana
Kiwi
Grape
Orange
Watermelon
</PARAM_1>
```

Parameter index starts from 1. Any number of Parameters sets can be defined. It is possible to define explicit parameters and from different sources such as external text file, external CSV file and ODBC sources. To define an explicit parameter, click on  button in Parameters tab. This will add an empty Parameter block as shown below:

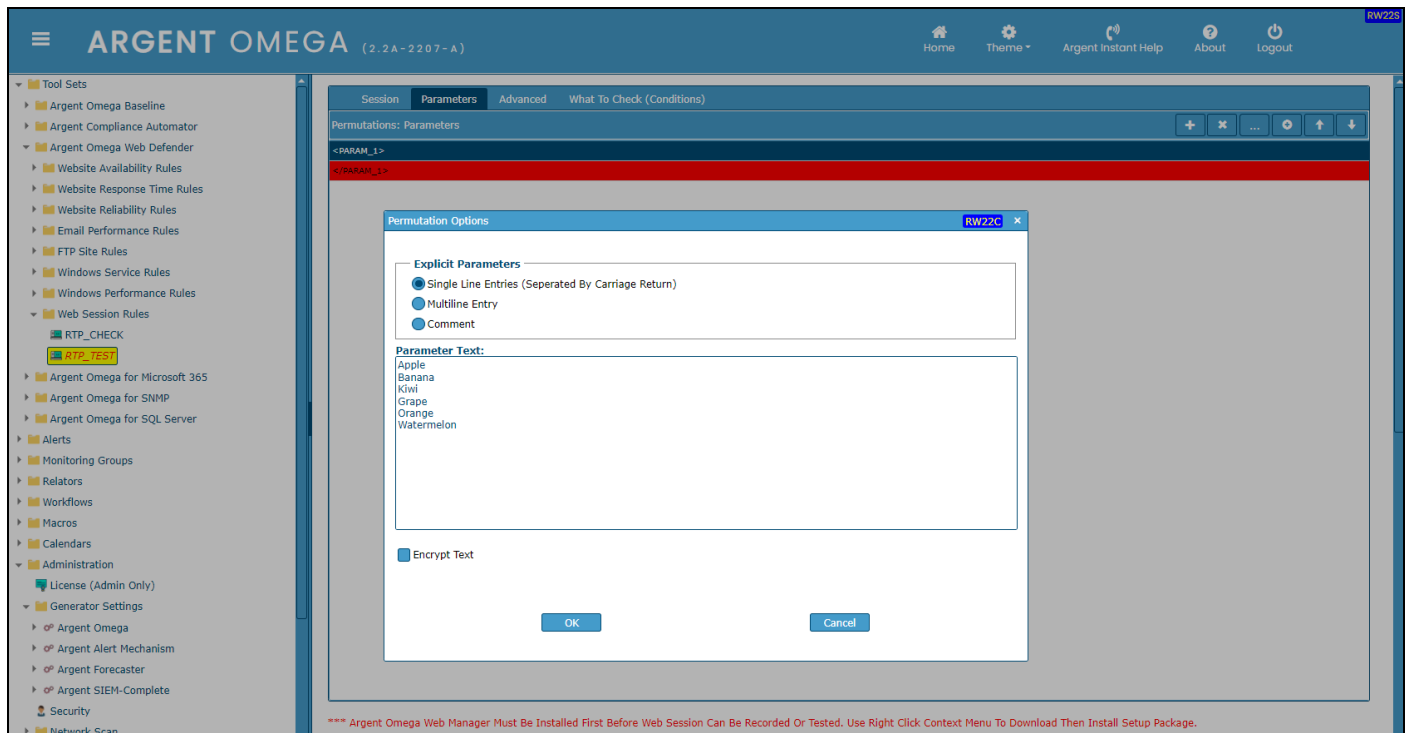


When you double click on an empty parameter block, "Permutation Options" dialog will be popped up.

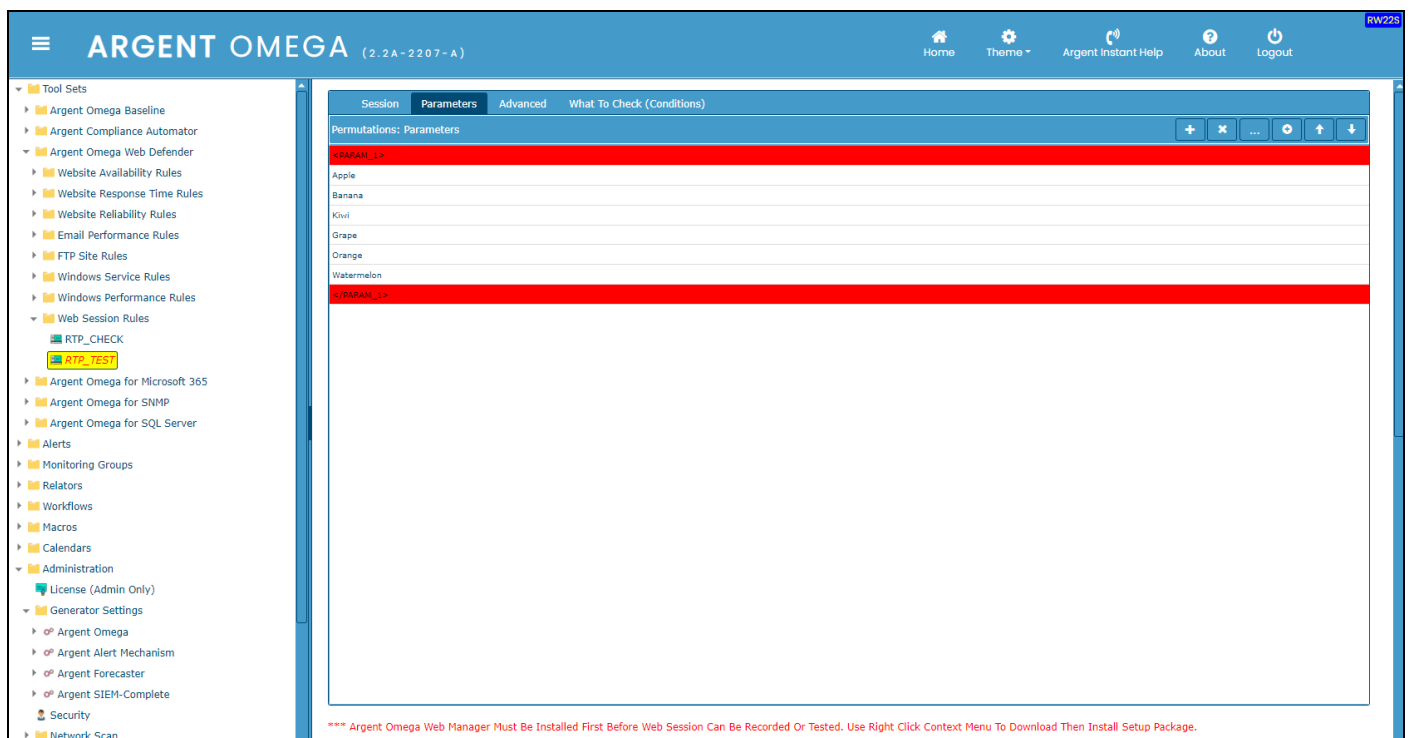
There you can specify the Parameter values. It is possible to define following types of Explicit Parameters:


- Single Line Entries
- Multiline Entry
- Comment – Commenting specific entries

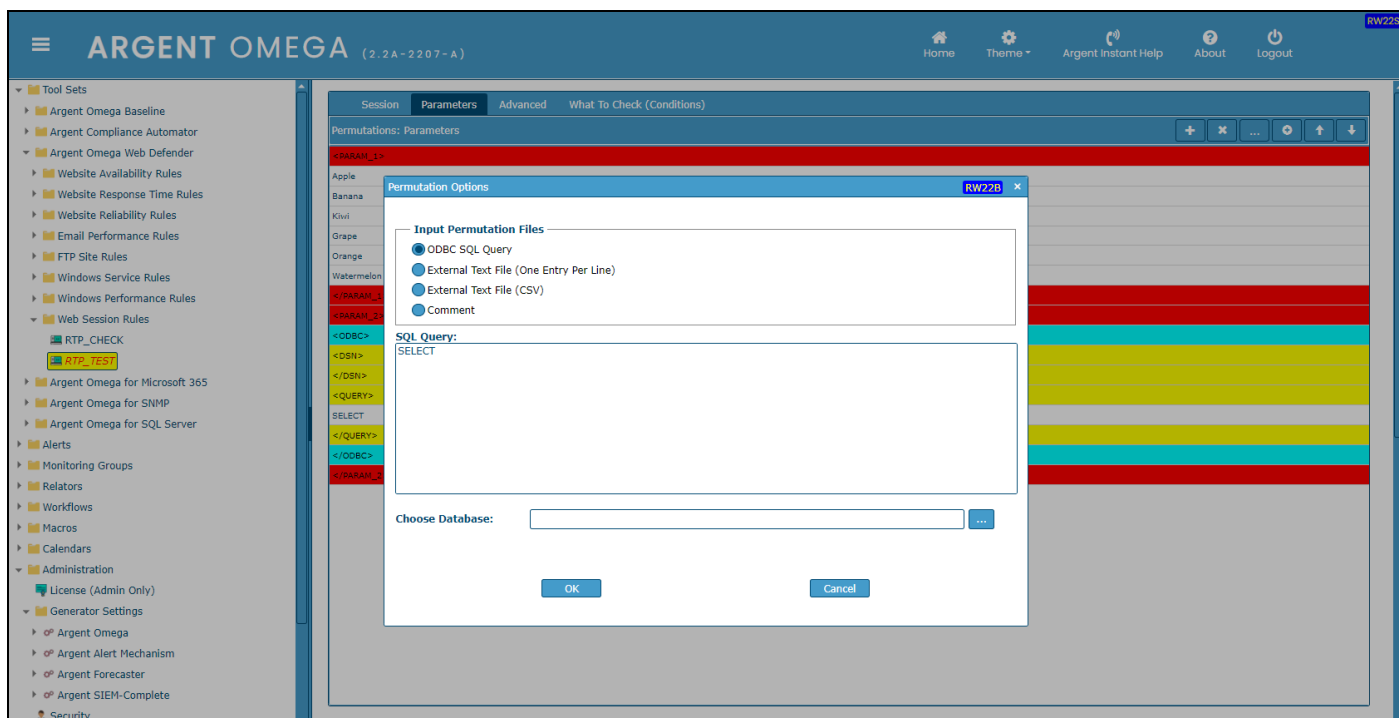
Following screenshot defines single line Parameter values:



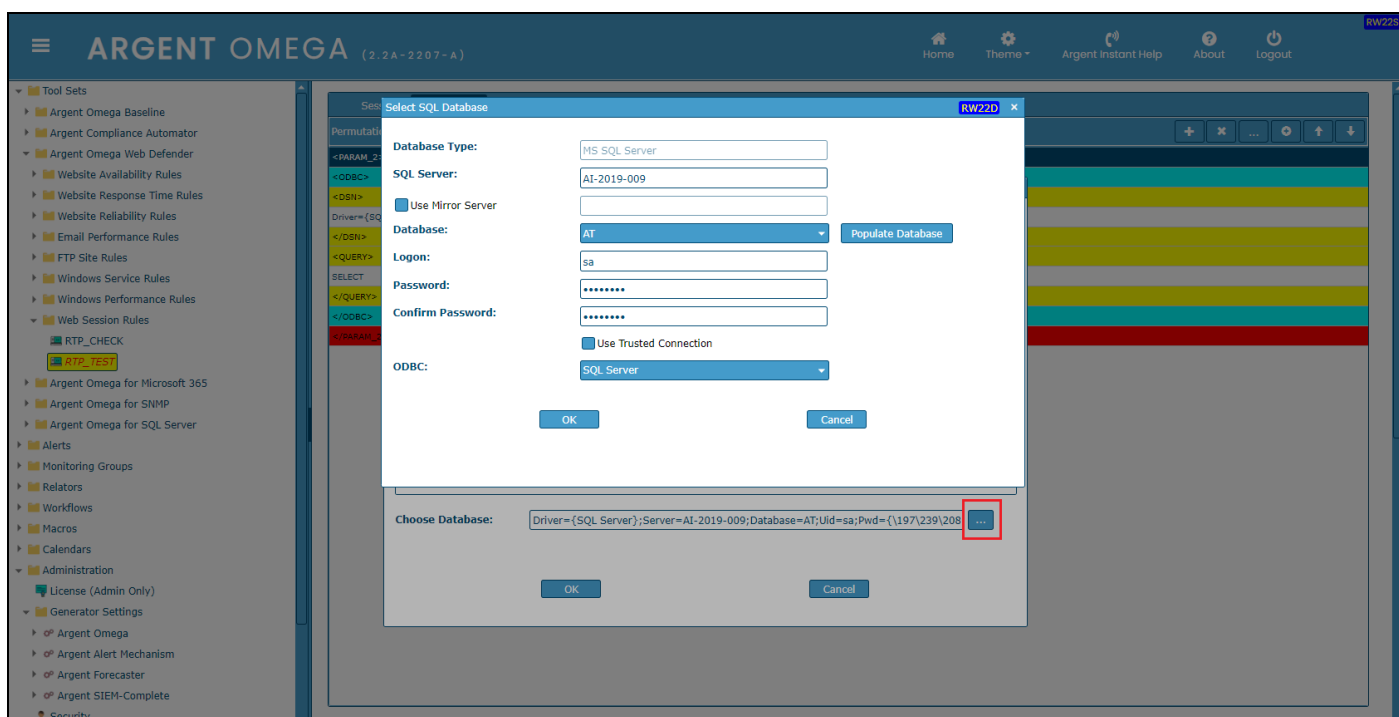
The **Encrypt Text** option encrypts the Parameter values, so it is not possible to see it in plain text. After specifying the Parameter Values, click OK. The Parameter values will be added in the list:



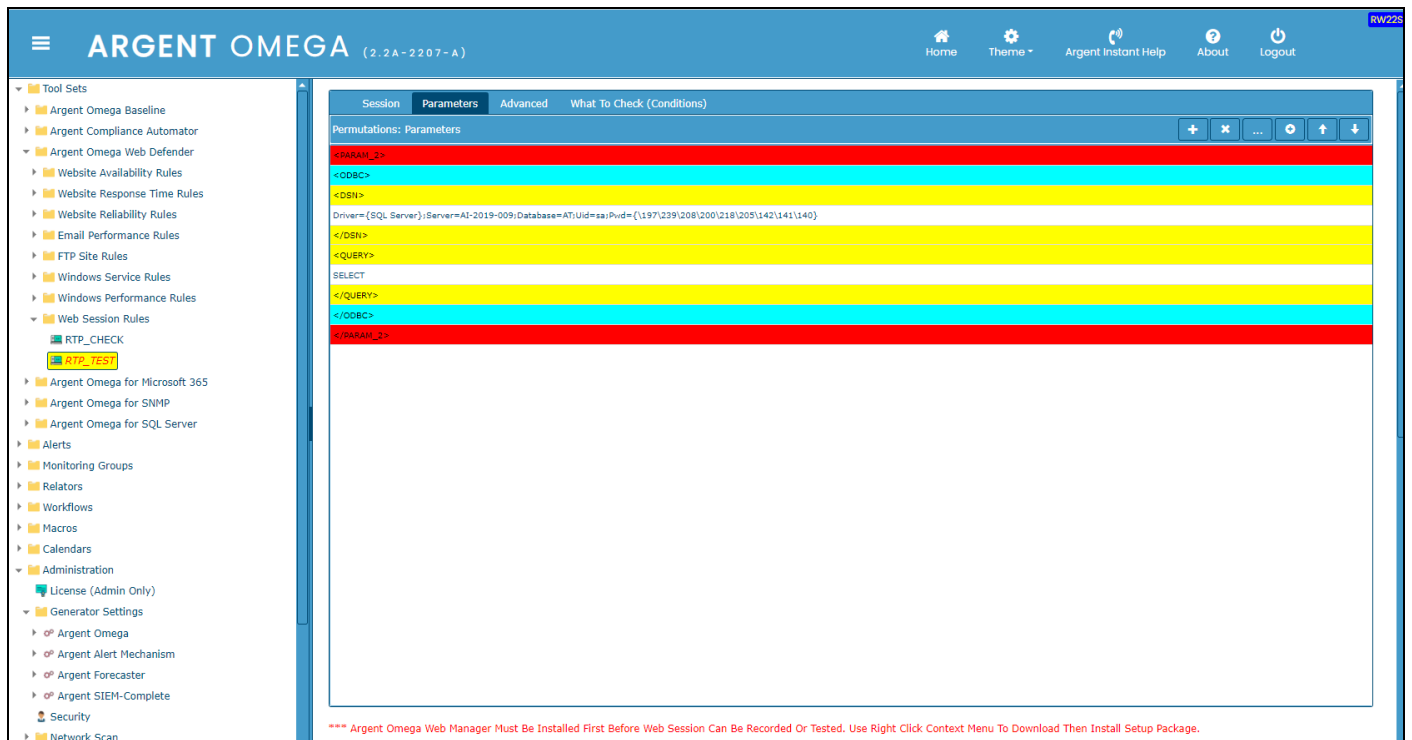
To define Parameter values from external file or ODBC source, click  button. This will popup “Permutation Options” dialog as shown below:



For **ODBC SQL Query** option, need to specify the SQL Server machine and database details, SQL query, etc. Use **Choose Database** option to specify SQL Server machine and database details:



An ODBC SQL Query parameter looks like below:



Use **External Text File** option to retrieve Parameter values from text or CSV file.

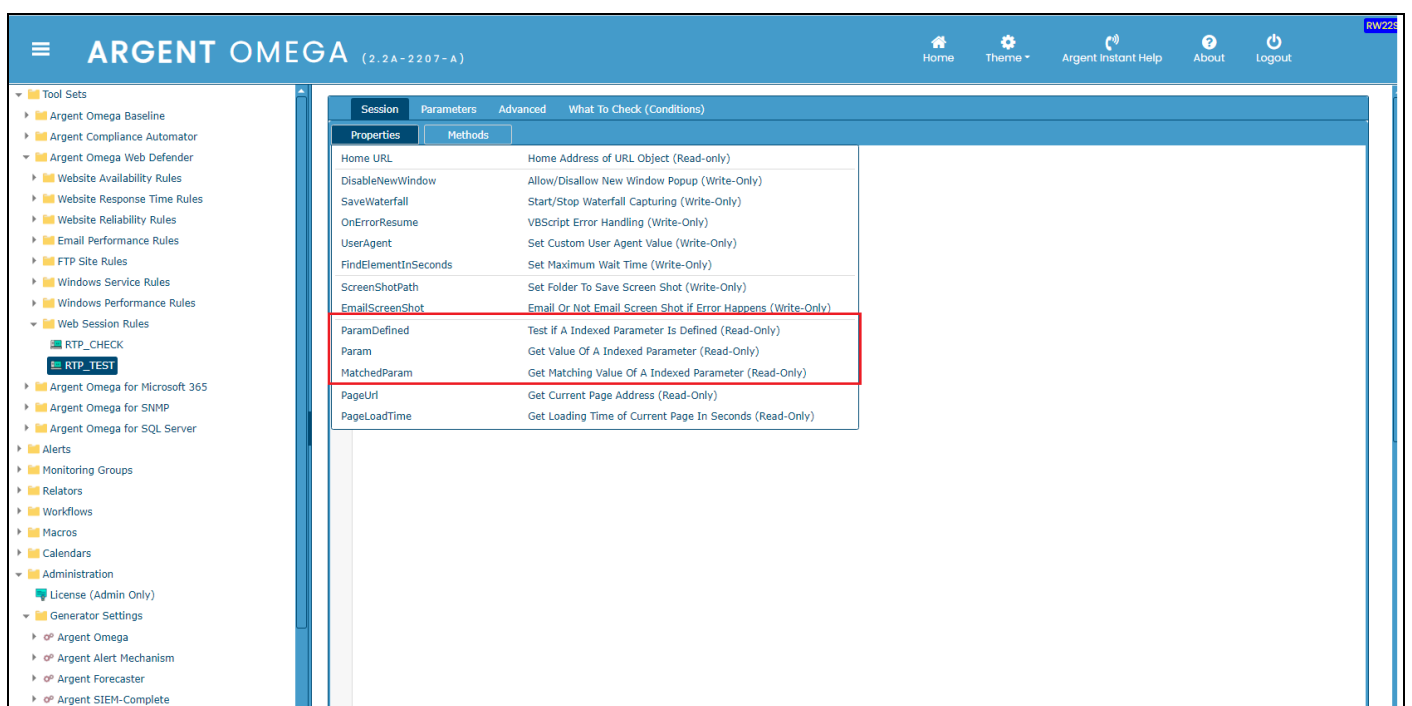
While Web Session Rule execution, the Parameters will be filled with the values read from specified Text, CSV or ODBC sources.

To use the Parameters in Web Session Script, following predefined Properties can be used:

ParameterDefined: Test if a Parameter with specified index is defined or not.

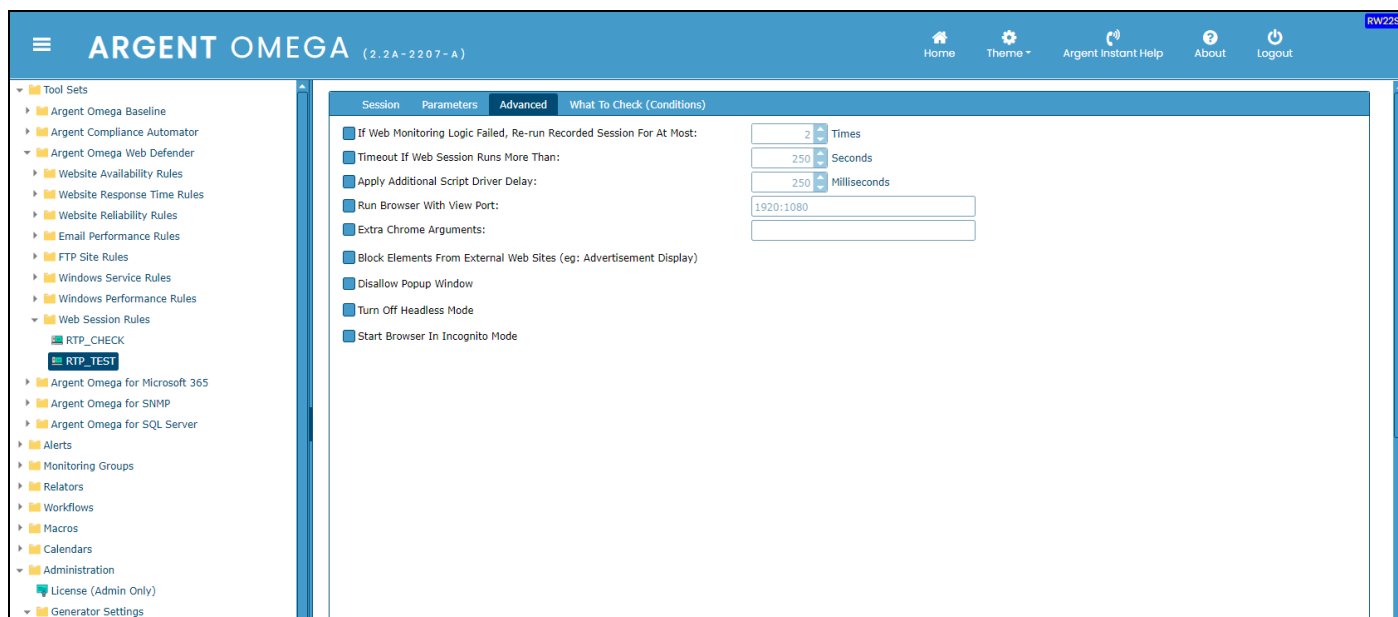
Param: Get the random Parameter value from a Parameter with specified index.

MatchedParam: Get the matching value from an indexed Parameter:



Advanced Options In Web Session Rule

Advanced tab contains the options to configure Chromium browser for session recording and replay:



Configure **If Web Monitoring Logic Failed, Re-run Recorded Session For At Most** option to retry the script execution in specified number of times if the script execution failed.

Configure **Timeout If Web Session Runs More Than** option to break the Web Session Rule with timeout exception if the script execution takes more than the specified seconds.

Configure **Apply Additional Script Driver Delay** option to slow down the script execution by the specified number of milliseconds.

Configure **Run Browser With View Port** option to set the screen size of Chromium browser.

Specify additional script driver argument in **Extra Chrome Arguments** input box.

Check **Block Elements From External Web Sites** option to block external website popup while session recording.

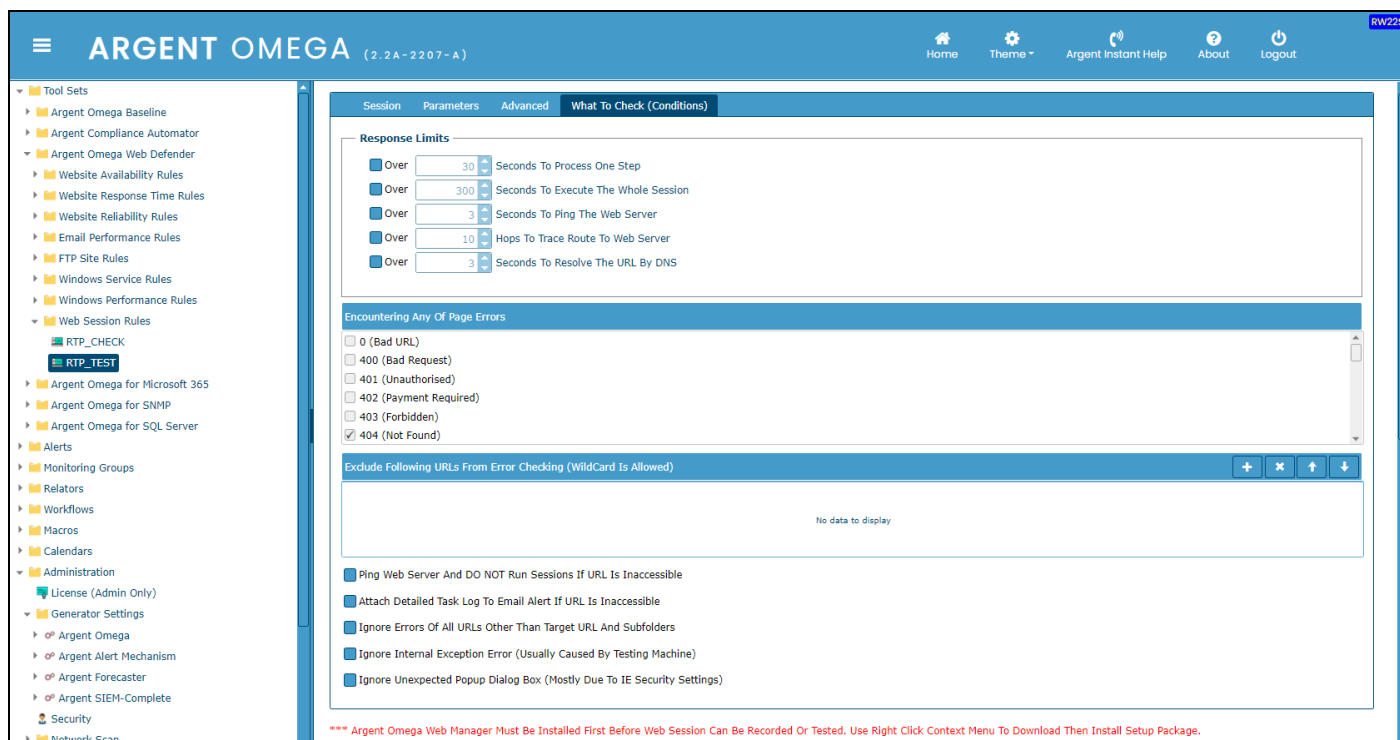
Check **Disallow Popup Window** to block popup window while session recording.

Check **Turn Off Headless Mode** option to run the Chromium browser in non-headless mode.

Check **Start Browser In Incognito Mode** option to run the Chromium browser in Incognito mode.

What To Check (Conditions) In Web Session Rules

Configure Web Session Rules breaking conditions in **What To Check** tab:



Configure the following Response Limit Thresholds in **Response Limits** section:

Configure **Over N Seconds To Process One Step** option to alert Web Session Rules if execution time of recorded single script statement exceeds the threshold.

Configure **Over N Seconds To Execute The Whole Session** option to alert Web Session Rules if execution time of whole recorded script exceeds the threshold.

Configure **Over N Seconds To Ping The Web Server** option to alert Web Session Rules if the time taken to ping to the website's web server exceeds the threshold.

Configure **Over N Hops To Trace Route To Web Server** option to alert Web Session Rules if the number of hops to Trace Route website's web server exceeds the threshold.

Configure **Over N Seconds To Resolve The URL By DNS** option to alert Web Session Rules if time taken to resolve the URL by DNS exceeds the threshold.

Select HTTP response status codes in **Encountering Any Of Page Errors** section, so that the Web Session Rules will break if any recorded script statement return any of the selected status codes. There is an option to exclude URLs from status code checking. Configure the URLs to be excluded in **Exclude Following URLs From Error Checking** section.

By checking the option **Ping Web Server And DO NOT Run Sessions If URL Is Inaccessible**, the Rule will not execute the session script if the ping to the website's web server is failed.

By checking the option **Attach Detailed Task Log To Email Alert If URL Is Inaccessible**, the Rule will attach the task log to email alert if the website URL is inaccessible.

By checking the option **Ignore Errors Of All URLs Other Than Target URL And Subfolders**, the Rule will ignore errors of URLs other than main website URL and it's sub URLs.

Website Availability Rules

The Website Availability Rules in Argent Omega Web Defender checks the availability of website specified in URL object. It also checks the availability of URLs configured in **Vital URLs To Check** CMDB-X property.

There is an option to save the predictor data (1 = site is UP, 0 = site is DOWN) to the Argent Forecaster:

The screenshot displays the Argent Omega Web Defender configuration page for the 'Rule Is Broken If Website Is Not Available'. The interface includes a sidebar with a navigation menu, a top navigation bar, and a main configuration area.

Top Navigation Bar: ARGENT OMEGA (2.2A-2207-A) | Home | Theme | Argent Instant Help | About | Logout | RW33

Sidebar Navigation:

- Tool Sets
 - Argent Omega Baseline
 - Argent Compliance Automator
 - Argent Omega Web Defender
 - Website Availability Rules
 - WA_CHECK**
 - Website Response Time Rules
 - Website Reliability Rules
 - Email Performance Rules
 - FTP Site Rules
 - Windows Service Rules
 - Windows Performance Rules
 - Web Session Rules
 - Argent Omega for Microsoft 365
 - Argent Omega for SNMP
 - Argent Omega for SQL Server
 - Alerts
 - Monitoring Groups
 - Relators
 - Workflows
 - Macros
 - Calendars
 - Administration
 - License (Admin Only)
 - Generator Settings
 - Argent Omega
 - Argent Alert Mechanism
 - Argent Forecaster
 - Argent SIEM-Complete
 - Security

Main Configuration Area:

Rule Is Broken If Website Is Not Available

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

Tag 1:
Tag 2:
Tag 3:

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

☐ Do So Only After Hour Minutes Since Event Is Post

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

☐ Post Event Only After Rule Is Broken Or More Times

Reset Counter

☒ After Event Is Post
☐ After Event Is Answered
☐ After The Actual Condition Is Corrected

Application:

Reference URL:

Console Comment:

Description:

Full Screen

Website Response Time Rules

The Argent Web Site Response Time Rules ensure a website is fully loaded within a given number of seconds. This Rule can be configured to alert if the website loading (response) time exceeds the configured threshold.

The **Save Predictor Data Only** option ensures that no alerts will be fired, it only saves the response time value to Argent Forecaster:

The screenshot shows the Argent Omega configuration interface. The left sidebar contains a tree view of tool sets, including 'Website Response Time Rules' and 'WRT_OFFLINE_SERVER'. The main panel is titled 'Rule Is Broken If Response Time In Seconds Is Greater Than Threshold'. It features three threshold settings: 'Threshold 1 (Critical): 30', 'Threshold 2 (Medium Priority): 0', and 'Threshold 3 (Low Priority): 0'. Each threshold has a 'Not Used' checkbox. Below the thresholds is a section for 'Check Following Lower-Level URLs Below Base URL' with a table for adding URLs. The 'Rule Is Broken If The Following Conditions Are True' section contains a table for adding conditions. At the bottom, there are checkboxes for 'Break Rule When Any Error Occurred', 'Save Performance Data To The Argent Forecaster Using Data Store: {default}', and 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)'. There are also input fields for 'Tag 1', 'Tag 2', and 'Tag 3'.

Configure the response time threshold in **Rule Is Broken If Response Time In Seconds Is Greater Than Threshold** section.

The **Ignore Base URL** option is for checking ONLY the lower-level URLs listed. Specify the lower-level URLs in **Check Following Lower-Level URLs Below Base URL** section.

This Rule also checks for a given string within the embedded content of a web site. Configure this in **Rule Is Broken If The Following Conditions Are True** section.

Website Reliability Rules

The Argent Website Reliability Rules check EVERY hyperlink within a website. This feature goes through a website checking for broken links, missing images, etc. You can adjust the depth of the scan by setting the control variable **Maximum Number Of Pages To Process**. Set here the maximum number of pages to monitor. Use 9,999 if there is no limit to the number of pages to monitor.

Check **Cancel Downloading If Broken Link Is Found** option to cancel downloading if a broken link is found.

Configure URLs in **Exclude Following URLs From Checking** section to skip it from checking:

The screenshot displays the Argent Omega web interface. On the left is a navigation menu with categories like Tool Sets, Alerts, Workflows, and Administration. The 'Website Reliability Rules' section is expanded, showing 'WR_CHECK_HOME_PAGE' as the selected rule. The main panel on the right is titled 'Rule Is Broken When Any Bad Or Missing Links Are Detected'. It contains several configuration options: 'Maximum Number Of Pages To Process' is set to 1; 'Cancel Downloading If Broken Link Is Found' is checked; the 'Exclude Following URLs From Checking' section is empty; 'Rule Is Broken If Any Error Occurred' is checked; 'Save Performance Data To The Argent Forecaster Using Data Store' is set to '{default}'; 'Tag 1', 'Tag 2', and 'Tag 3' are empty text boxes; 'Post Event Even If The Same Event Is Still Outstanding (Unanswered)' is checked; 'Do So Only After' is set to 1 hour and 0 minutes; 'Ignore The Same Outstanding Event If Alerts Were Fired More Than' is set to 1 hour and 0 minutes; 'Post Event Only After Rule Is Broken' is set to 2 or more times; the 'Reset Counter' section has three radio buttons, with 'After Event Is Post' selected; 'Application' is an empty text box; 'Reference URL' is an empty text box; 'Console Comment' contains '*** Found Broken Links In Home Page ***'; and 'Description' is an empty text box.

Email Performance Rules

Note:

Please read **Configure Mail Object in CMDB-X** section to configure Mail object in CMDB-X.

The Argent Email Performance Rules monitor the email sending and receiving capabilities of a SMTP, POP3 and IMAP objects and test round-trip email performance. The performance data is saved for trend analysis using the Argent Forecaster. A round-trip email is a synthetic email message generated by Argent. Then Argent sends the email to the **Destination Email Address** configured in CMDB-X and calculates the time consumption of the entire process:

Subject, **Attachment** and **Message** are the three common fields used to simulate any type of email message.

Configure **Checking For New Incoming Mail Every X Seconds** to specify the number of seconds to wait before checking for incoming email.

Broken If Total Round Trip Time Exceeds X Seconds specify the limit in seconds for an email to be sent and re-read back. If this number of seconds is exceeded, the Rule is broken, and an alert will be fired by the Argent Alert Mechanism.

Check **Retain Email Message In User's Mailbox** option to retain email messages in the user's mailbox -- typically used for troubleshooting purposes, or to retain a record of each test.

FTP Site Rules

Note:

Please read **Configure FTP Object in CMDB-X** section to configure FTP objects in CMDB-X.

The Argent FTP Site Rules test the existence of a file by downloading files from an FTP server. The Rule is broken if one of the specified files doesn't exist, or optionally does exist, depending on the Rule settings:

ARGENT OMEGA (2.2 A - 2207 - A)

Files At FTP Site To Download For This Test (Wildcards Allowed)

/pub/SOME_VITAL_FILE

Toggle "Rule Is Broken If File Exists"

☐ Check Only Files With File Size Value Is Greater Than 0 Bytes

☐ Check Only Files With Last Write Time Older Than 0 Days 0 Hours 0 Minutes

☒ Do Not Traverse Subdirectories

☒ Check File Existence Only

☒ Rule Is Broken When Any Error Occurred

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

Tag 1:

Tag 2:

Tag 3:

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

☐ Do So Only After 1 Hour 0 Minutes Since Event Is Post

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

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

Reset Counter

☒ After Event Is Post

☐ After Event Is Answered

☐ After The Actual Condition Is Corrected

Application:

Reference URL:

Console Comment: *** Vital File Not Found In FTP Server ***

Specify files to be downloaded from the FTP site in **Files At FTP Site To Download For This Test (Wildcards Allowed)** section.

Check the option **Do Not Traverse Subdirectories** to prevent checking the files in subfolders.

Check the option **Check File Existence Only** to verify only the existence of the file. No download occurs with this option selected.

Windows Performance Rules

Argent Omega Web Defender contains set of predefined Rules to monitor the following critical performance metrics of IIS Web Server:

- Active Requests
- Active Threads Count
- Number of Current Files Cached
- Number of Current Metadata Cached
- Number of Current URIs Cached
- Rate of File Cache Hits per Second
- Current File Cache Memory Usage
- Rate of Metadata Cache Misses per Second
- Number of Metadata Cache Flushes
- Number of Metadata Cache Hits
- Rate of Metadata Cache Hits per Second
- Number of Metadata Cache Misses
- Number of Requests per Second
- Rate of URI Cache Hits per Second
- Bytes Received per Second
- Bytes Sent per Second
- Connection Attempts per Second
- Current Anonymous User Connections
- Current Non-Anonymous User Connections
- Active User Connections
- GET Requests per Second
- POST Requests per Second

ABG859_User_Guide_for_Argent_Omega_Web_Defender.doc