NetWitness® Platform

Universal Rest API Event Source Log Configuration Guide

NETWITNESS
Platform

Universal Rest API Plugin

Event Source Product Information:

Versions: v1.0

NetWitness Product Information:

Supported On: NetWitness Platform 12.2 and later

Note: Universal Rest API Plugin is supported from NetWitness Platform 12.2 . However, NetWitness recommends you to update NetWitness Platform to the latest version.

Event Source Log Parser: o365_trace, proofpoint, sailpointiiq

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November 2024

Contents

Introduction **5**
Set-up Office 365 Message Trace API Permission for your Application **6**
Examples Collection Configuration **7**
Setup the Universal Rest API Plugin in NetWitness Platform **10**
Deploy the Universal Rest API V1 Files from Live 10
Configure Universal Rest API Plugin in NetWitness Platform 10
Universal Rest API Collection Configuration Parameters 12
Basic Parameters 12
Getting Help with NetWitness Platform **15**
Self-Help Resources 15
Contact NetWitness Support 15
Feedback on Product Documentation 16

Introduction

This Universal Rest API Plugin is used to collect logs from any event source that exposes REST API for log collection, provided that the API satisfies the below conditions.

1. The Authentication method used is HTTP Basic Auth. To collect Office365 message trace logs, the customer should use the application id/secret authentication method.

2. The API provides option to query using StartTime and EndTime as query parameters.

3. The format expected for StartTime and EndTime is YYYY-MM-DDTHH:MM:SSZ (2023-05-01T12:00:00Z).

4. The response of the API call is in JSON format.

Note: This Plugin has been tested against the O365 Message Trace API and Proofpoint SIEM API. If your Event Source satisfies the above conditions but prevents you from using the plugin, raise a customer support ticket.

Set-up Office 365 Message Trace API Permission for your Application

1. Sign in to https://portal.office.com/adminportal/home#/homepage.
2. In the left navigation pane, click **Azure Active Directory** > **App registrations**.
3. Search and select your application under the app registrations.
4. Go to the **API Permissions** > **Add a permission** > **APIs my organization uses**.
5. Search for **Office 365 Exchange Online** and select.
6. Select **Application permission** and type ***ReportingWebService*** into the search field.
7. Select the check box for the required permissions and click **Add permissions**.
8. Provide the Global reader permission to the application. Go to **Azure Active Directory** > **Roles and administrators** > **Global reader** > **Add assignment**.

Examples Collection Configuration

The below Collection Configuration Parameters are examples with detailed descriptions of each field.

Office 365 Message Trace API

For more information on Office 365 Message trace API, see MessageTrace report.

Parameters	Description
Event Source Name	o365_trace ←The parser to which the collected logs are routed to depends on the "Event Source Name". In this case the logs are parsed using o365_trace json parser.
URL	https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace?$filter=StartDate eq datetime'{starttime}' and EndDate eq datetime'{endtime}' ← {starttime} and {endtime} will be replaced with the start and end time being used for bookmarking.
User Name	Your application id
Password	Enter application secret
Tenant Domain	Go to **Active Directory** and click on the directory. In the Active Directory list, click the directory that you are using with your Office 365 tenant. The tenant ID for your Office 365 tenant is displayed as part of the URL. NetWitness recommends you to use a Tenant Domain, rather than an Tenant ID. Example Tenant Domain is netwitnesstest.onmicrosoft.com
Path to Events Array	The jmespath to the list of events in the response
Next Token Path	odata.nextLink ← jmespath to the next token field if the API supports pagination
Start From(In Hours)	N← Log Collection will start from N hours prior to current time

Proofpoint SIEM API

For more information on Proofpoint SIEM API, refer SIEM API.

Parameters	Description
Event Source Name	proofpoint ← The parser to which the collected logs are routed to depends on the "Event Source Name". In this case the logs are parsed using **proofpoint** json parser.

Parameters	Description
URL	https://tap-api-v2.proofpoint.com/v2/siem/messages/delivered?format=json&interval={starttime}/{endtime} ← {starttime} and {endtime} will be replaced with the start and end time being used for bookmarking.
User Name	Your username
Password	Enter your password
Tenant Domain	Tenant Domain is set to **default**, leave as it is.
Path to Events Array	MessagesDelivered ← The jmespath to the list of events in the response
Next Token Path	← jmespath to the next token field if the API supports pagination. Empty in this case.
Start From(In Hours)	N← Log Collection will start from N hours prior to current time

Sailpoint IdentityIQ

For more information on Proofpoint SIEM API, refer IDENTITYIQ.

Parameters	Description
Event Source Name	sailpointiiq ← The parser to which the collected logs are routed to depends on the "Event Source Name". In this case the logs are parsed using **sailpointiiq** json parser.
URL	http://<hosted_ serverName>/identityiq/plugin/rest/SIEMPlugin/audit-events?startTime={starttime}&endTime={endtime} {starttime} and {endtime} will be replaced with the start and end time being used for bookmarking by the plugin code. **Note:** Replace <hosted_serverName> with the your sailpoint Idenitity IQ server value before you paste the URL in the plugin config in your logcollector. If you hosted the API inside your local system, please put **localhost:<portNumber of localhost>** in the place of hosted_serverName.
User Name	Your username.
Password	Enter your password.
Tenant Domain	Tenant Domain is set to **default**, leave as it is.

Parameters	Description
Path to Events Array	auditEvents ← Enter this string for sailpointiiq audit logs.
Next Token Path	← jmespath to the next token field if the API supports pagination. Empty in this case.
Start From(In Hours)	N← Log Collection will start from N hours prior to current time.

Setup the Universal Rest API Plugin in NetWitness Platform

In NetWitness Platform, perform the following tasks.

- Deploy the Universal Rest API V1 Files from Live.
- Configure Universal Rest API Plugin in NetWitness Platform.

Deploy the Universal Rest API V1 Files from Live

Universal Rest API plugin requires resources available in Live in order to collect logs.

To deploy the universal rest API content from Live:

1. In the NetWitness Platform menu, select **Configure** > **Live Content**. Browse **Live Content** for Universal Rest API plugin by typing ***universal_rest_api_v1*** into the Keywords text box and click **Search**.
2. Select the item returned from the Search.
3. Click **Deploy** to deploy the Universal Rest API Plugin to the appropriate Log Collectors using the Deployment Wizard.
4. Log Parsers **proofpoint, o365_trace,** and **sailpointiiq** have been added as required resources of universal_rest_api_v1 plugin in NetWitness Live. Deploy these parsers to appropriate Log Decoders when you deploy plugin log collection file. The **o365_trace** is enabled automatically on deployment but, **proofpoint** and **sailpointiiq** parser should be enabled manually.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the Live Resource Guide on NetWitness Link.

Configure Universal Rest API Plugin in NetWitness Platform

1. In NetWitness Platform menu, select **Admin** > **Services**.

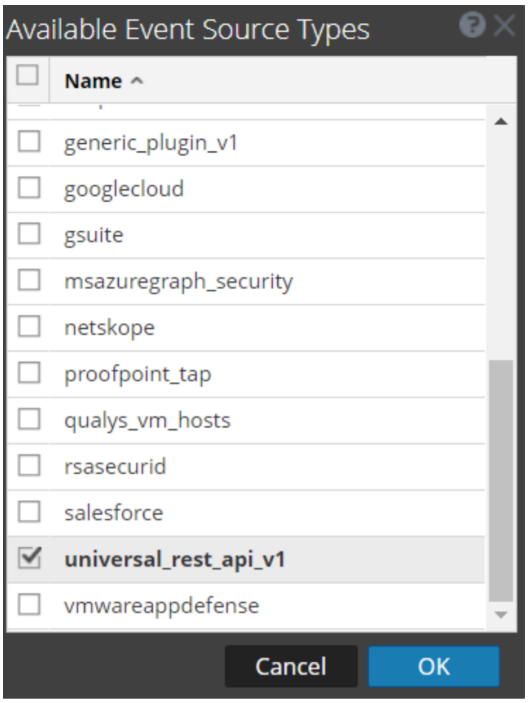
2. In the Services grid, select a Log Collector service, and from the **Actions (** **)** menu, choose **View** > **Config** > **Event Sources**.

3. In the **Event Sources** tab, select plugins from the dropdown menu.

The **Event Categories** panel displays the File event sources that are configured, if any.

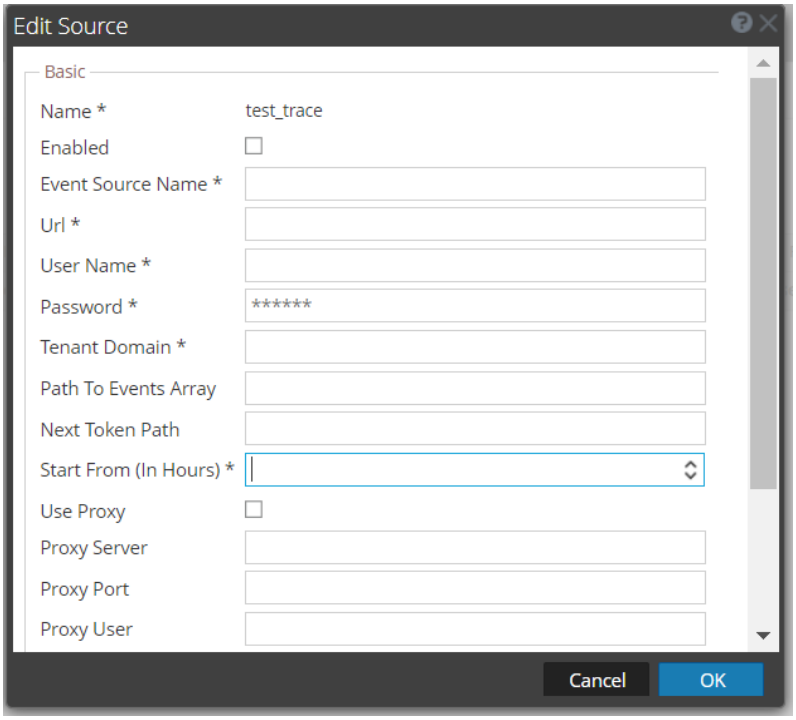
4. In the **Event Categories** panel tool bar, click +.

The **Available Event Source Types** dialog is displayed.



5. Select **universal_rest_api** from the list and click **OK**. The newly added event source type is displayed in the **Event Categories** panel.

6. Select the new type in the **Event Categories** panel and click +, in the **Source** panel tool bar, the **Add Source** dialog is displayed.



7. Define parameter values as described in Universal Rest API Collection Configuration Parameters.

8. Click **Test Connection**.

The result of the test is displayed in the dialog box. If the test is not successful, edit the device or service information based on message shown and retry.

Note: The log collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform displays a Request Timed Out Error.

Note: Once the test connection is successful and the instance is saved, if the instance is re-opened in the edit panel, the test connection will fail. This is a known bug which is fixed .To do test connection for instance(s) after saving them, select the required instance(s) and click on the test connection tab without opening the edit window.

9. If the test is successful, click **OK**. The new event source is displayed in the **Sources** panel.

10. Repeat steps **4–9** to add another instance of Universal Rest API plugin type.

Universal Rest API Collection Configuration Parameters

This section describes the Universal Rest API plugin configuration parameters.

Note: Items that are followed by an asterisk (*) are required.

Basic Parameters

Name	Description
Name*	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Event Source Name*	This value is used to route the logs collected to the correct parser. Example: o365_trace, proofpoint, or sailpointiiq.
Url*	The complete URL to be used to query for the logs. The URL is expected to have query parameters for starttime and endtime which will be used for bookmarking. The plugin looks for “{starttime}” and “{endtime}” strings to replace them with startTime and endTime bookmarked timestamps. The format used is YYYY-MM-DDTHH:MM:SSZ (2023-05-01T12:00:00Z). Example: https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace?$filter=StartDate eq datetime'{starttime}' and EndDate eq datetime'{endtime}' https://tap-api-v2.proofpoint.com/v2/siem/messages/delivered?format=json&interval={starttime}/{endtime}
User Name*	Username to be used for HTTP Basic Auth
Password*	Password to be used for HTTP Basic Auth

Name	Description
Tenant Domain*	Go to **Active Directory** and click on the directory. In the Active Directory list, click the directory that you are using with your Office 365 tenant. The tenant ID for your Office 365 tenant is displayed as part of the URL. NetWitness recommends you to use a Tenant Domain, rather than an Tenant ID. Example Tenant Domain is netwitnesstest.onmicrosoft.com
Event Source Path	JMESPath to the list of events within the response.
Next Token Path	In case the API uses pagination. This is the JMESPath to the next token key within the response.
Start From (In Hours)	N number of hours to backtrack and pull data from.
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address	A custom IP chosen for the Event Source in the customer environment, such as 10.1.2.3. The value of this parameter is captured by the device.ip meta key. This is useful for grouping/querying all events collected by a single instance of the plugin and has no bearing on the collection.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Click **Advanced** to view and edit the advanced parameters, if necessary.

Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 180. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.

Name	Description
Max Duration Poll	The maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600. We recommend setting this value to 1800 to reduce the no of API calls.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	The maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Caution: Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: **Off** = (default) disabled **On** = enabled **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enable	Uncheck to disable certificate verification
Trail By (In Minutes)	Customers might end up missing some events if they query the server too close to the current time as API servers usually take some time to aggregate the logs at their end. This field can be used to set the time in minutes to fall behind current time.
Retention Period (In Minutes)	This field is used to specify the period for which logs are stored at the Server. This parameter is used to make sure that we do not query the server for events beyond the retention period. Ex: Proofpoint SIEM API has a log retention period of 12 hours.
HTTPS Proxy	If Proxy server is configured, enable or disable based on the proxy traffic allowed. By default HTTPS Protocol is enabled for the Proxy connection. If the only HTTP traffic allowed via proxy, then uncheck this parameter.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.