NetWitness® Platform XDR

OPSWAT MetaAccess Cloud Event Source Log Configuration Guide

NETWITNESS
Platform XDR

OPSWAT MetaAccess Cloud

Event Source Product Information:

Vendor: OPSWAT

Event Source: opswat

Versions: API v3.2

NetWitness Product Information:

Supported On: NetWitness Platform 12.2 or later

Note: OPSWAT MetaAccess Cloud is supported from NetWitness Platform XDR 12.2 . However, NetWitness recommends you to update NetWitness Platform XDR to the latest version.

Event Source Log Parser: opswat

Note: The opswat parser parses this event source as **device.type=opswat**.

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/.

February, 2024

Contents

Collecting OPSWAT Events in NetWitness Platform

Security teams face challenges with increasing work-from-home scenarios and lack visibility and control over devices accessing their network. Adding to the complexity is the myriad point products generally needed to gain this visibility and control. OPSWAT Meta Access is one solution that gives secure network access and deep endpoint compliance to your organization. With this one-platform approach, you can greatly simplify ongoing management, reducing time, effort, and most importantly, risk. For more details, see the official OPSWAT web page: https://www.opswat.com/products/metaaccess.

In NetWitness Platform XDR, we collect logs from OPSWAT using the REST API provided by OPSWAT and collect events like admin, device, webhook, device_report into the platform. NetWitness helps you to do the security investigation by fine parsing these collected events.

The following sections describe OPSWAT configuration as an event source in Netwitness:

- Configure the OPSWAT Event Source
- Set Up the OPSWAT Event Source in NetWitness Platform
- OPSWAT Collection Configuration Parameters.

Configure the OPSWAT Event Source

You can forward the OPSWAT MetaAccess logs to either OPSWAT MetaAccess API or AWS S3 bucket storage. Netwitness XDR supports both of these methods. If you want to collects logs from AWS S3 bucket, follow the instructions provided in S3 Universal Connector Event Source Log Configuration Guide and skip using this document.

Perform the following tasks to event source in your OPSWAT account to receive events through their REST API:

1. Create OPSWAT account and install OPSWAT clients in your networks, see https://gears.opswat.com/console/.
2. Register your applications in OPSWAT to retrieve events through API,

   https://docs.opswat.com/macloud-sdp/developer-guide/how-to-work-with-metaaccess-apis

   https://gears.opswat.com/o/app/register.

   Note: When you register application, please use http://127.0.0.1/opswat as both website URL and Callback URL if URL information is not specified in the OPSWAT official document. We at least need a "read" permission to retrieve events through the REST API.

We use client credentials type of authentication in API. For more information, refer OPSWAT documentation, https://docs.opswat.com/macloud-sdp/developer-guide/authentication#client-credentials-grant-type---no-log-in-required-from-a-user. You will receive the client key (or client id) and client secret when you register application by following Register your applications in OPSWAT to retrieve events through API,. Please keep client key (or client id) and client secret securely. They are required when you configure OPSWAT eventsource plugin in NetWitness Platform XDR.

We use OPSWAT API version 3.2 from at NetWitness. For more information on the OPSWAT REST API that we use for collecting events, please refer https://docs.opswat.com/macloud-sdp/developer-guide/get-logs.

Note: Please make sure that below URLs are allowed to open in your network firewalls/proxies as we use them for event collection.
- https://gears.opswat.com/o/oauth/token
- https://gears.opswat.com/o/api/v3.2/logs?access_token=

Set Up the OPSWAT Event Source in NetWitness Platform

In NetWitness Platform XDR, perform the following tasks:

i. Deploy the OPSWAT Files from NetWitness Live

ii. Configure the Event Source

Deploy the OPSWAT Files from NetWitness Live

OPSWAT eventsource requires resources available in NetWitness Live to collect logs. OPSWAT uses the opswat json parser.

To deploy the OPSWAT content from Live:

1. In the NetWitness Platform menu, select  **(Configure)** .
2. Browse Live for the **opswat** parser using RSA Log Device as the Resource Type.
   Select **opswat** parser from the list.
3. Click **Deploy** to deploy the opswat parser to the appropriate Log Decoders using the Deployment Wizard.
4. You should also deploy the OPSWAT log collection package. Browse Live for OPSWAT content by typing

   opswat_metaaccess in the search text box and click **Search**.
5. Select the item returned from the search and click **Deploy** to deploy to the appropriate Log Collectors.

   Note: On a hybrid installation, you should deploy the package on both the Virtual Log Collector (VLC) and the Log Collector (LC). If you deploy the package on the LC, you should restart the log decoder and log collector services, otherwise logs will not be collected.
6. Restart the `nwlogcollector` service.

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

Configure the Event Source

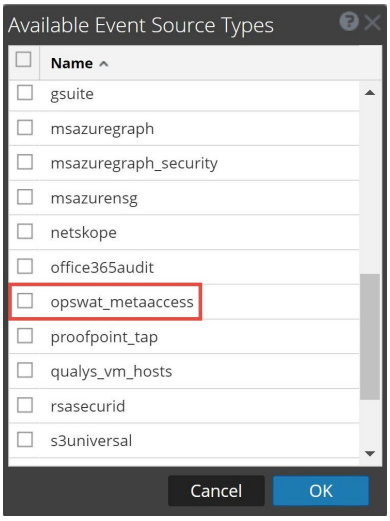
This section contains details on setting up the event source in NetWitness Platform. In addition to the procedure, the OPSWAT Collection Configuration Parameters are described.

To configure the OPSWAT Event Source:

1. In the NetWitness Platform menu, select **Administration > Services**.
2. In the **Services grid**, select a Log Collector service, and from the **Actions** menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The **Event Categories** panel displays the File event sources that are configured, if any.
4. In the **Event Categories** panel toolbar, click +.

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

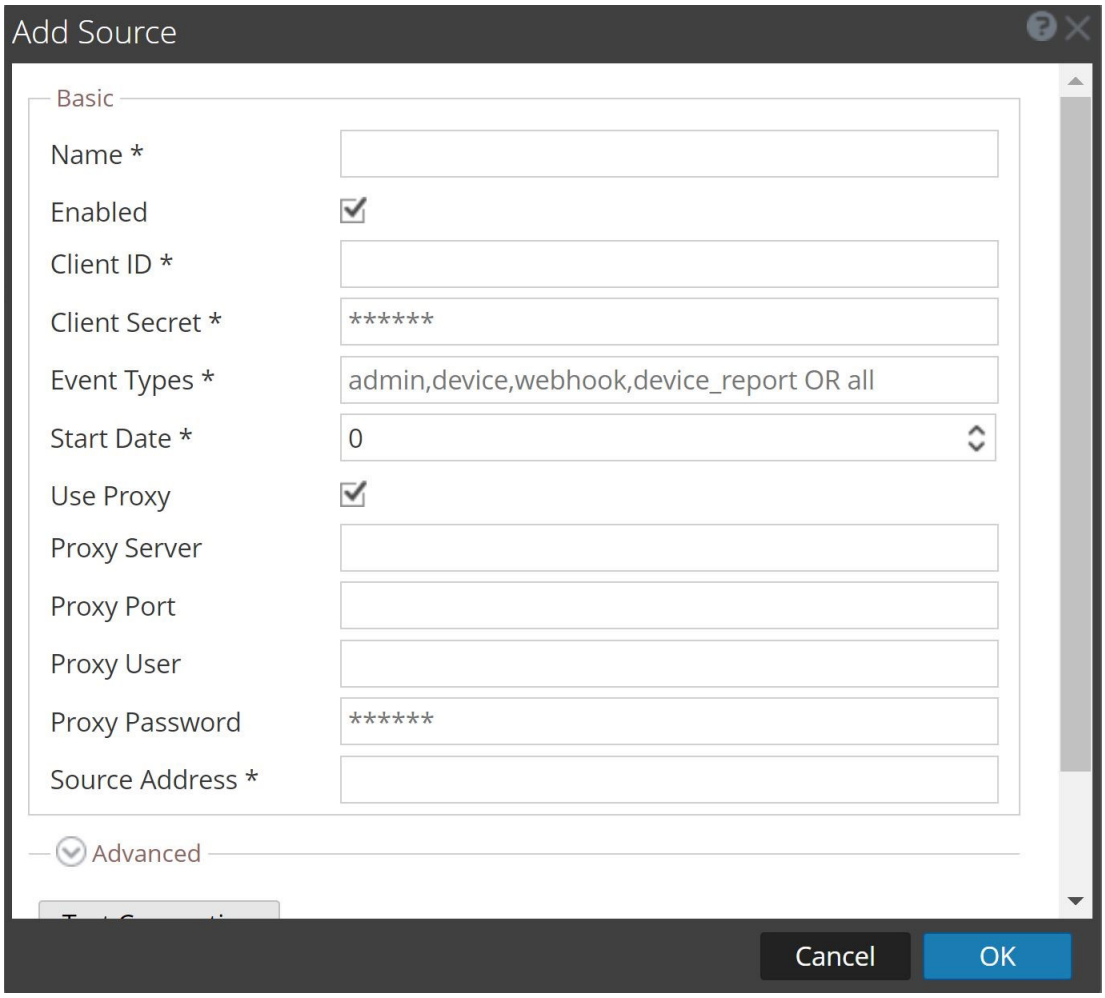


5. Select **opswat_metaaccess** from the list, and click **OK**.

   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 **Sources** panel toolbar.

   The **Add Source** dialog is displayed.



7. Define parameter values, as described in OPSWAT Collection Configuration Parameters.
8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information 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 an error message.

9. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

OPSWAT Collection Configuration Parameters

The following table describes the configuration parameter for the OPSWAT integration with NetWitness Platform. Fields marked with an asterisk (*) are required.

Note: When run from behind an SSL proxy, if certificate verification needs to be disabled, uncheck the **SSL Enable** checkbox in the **Advanced** section.

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 box to enable the event source configuration to start collection. The box is selected by default.
Client ID *	The Client ID (or client key) is found in the OPSWAT application registration page. Please refer step 2 in Configure the OPSWAT Event Source.
Client Secret *	The Client Secret is found in the OPSWAT application registration page. Please refer step 2 in Configure the OPSWAT Event Source.
Event Types *	Accepted values are `admin`, `device`, `webhook`, `device_report`, or `all`. In a single configuration, you can either pass single value or multiple values separated by comma. If you require all 4 event types to be collected with the same config, please put value as **all.**
Start Date *	Choose the date from which to start collecting. This parameter defaults to the current date, i.e, 0 and logs will be collected from last 60 mins. The Maximum value is 30.
Use Proxy	Uncheck to disable proxy configuration. This is enabled by default.
Proxy Server	If you are using a proxy in your environment, 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).

Name	Description
Source Address	A custom value chosen to represent the hostname for the OPSWAT Event Source in the customer environment and the value should be in IPV4 format. The value of this parameter is captured by the **device.ip** meta key.

Advanced Parameters

Click **Advanced** to view and edit the advanced parameters.

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.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	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	**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. 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. This is enabled by default.

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.