NetWitness® Platform

Symantec Zero Trust Network Access (ZTNA) Plugin Event Source Log Configuration Guide

NETWITNESS
Platform

Symantec Zero Trust Network Access (ZTNA) Plugin

Event Source Product Information:

Vendor: Broadcom

Event Source: Symantec Zero Trust Network Access (ZTNA)

Versions: v2

NetWitness Product Information:

Supported On: NetWitness Platform 12.1 and later

Event Source Log Parser: symantecztna

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

Introduction

The zero-trust security model is based on "never trust, always verify". Users and devices should be verified every time, even on trusted or approved networks. The zero-trust approach requires mutual authentication, which checks both users and devices regardless of where they access applications and services. This way, it prevents network threats by trusting user and device identity only after authentication. The zero trust principles can be used for data access and management in networks that include cloud, mobile or remote environments across different zones and locations.

Symantec Zero Trust Network Access (ZTNA) is a SaaS solution that allows secure access to any corporate resource in the cloud or on-premises. It connects at the application level, hiding all resources from the end-user devices and the Internet. For more information refer

https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/ztna/1-0/about-secure-access-cloud.html

Netwitness Platform integrates with Symantec ZTNA via luminate-api (https://api.lumiate.io/#section/Introduction) and collects Audit Logs and Forensics logs.

- Audit logs (collects from last 30 days):
  - API reference : https://api.luminate.io/#tag/Audit-Logs
  - Documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/ztna/1-0/log-concept/logs-audit.html
- Forensics logs (collects from last 7 days):
  - API reference : https://api.luminate.io/#tag/Forensics-Logs
  - Documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/ztna/1-0/log-concept/logs-forensics.html

Symantec ZTNA configuration for integrating with Netwitness Platform

- **To create Client credentials**:

  https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/ztna/1-0/navigate-app-portal/api-client-session- lifetime.html

  Refer https://api.luminate.io/#section/Authentication more information.

- Copy and Save the Client ID and Client Secret from the above configuration.
- Get the tenant name configured in https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/cloud-management-portal/all/configure-and-provision-your-cloud-services/configure-cloud-services.html

Setup the Symantec ZTNA plugin in Netwitness Suite

In RSA NetWitness Suite, perform the following tasks.

- Deploy the symantec_ztna package from Live
- Configure the symantec_ztna plugin in NetWitness Suite UI

Deploy symantec_ztna files from Live:

Symantec ZTNA plugin requires resources available in Live in order to collect logs.

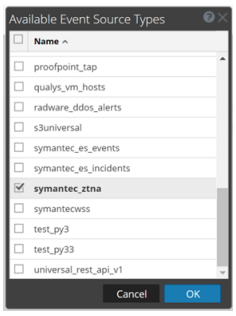
To deploy the symantec_ztna content from live:

1. In the RSA NetWitness Suite menu, select Live. Browse Live for Symantec ZTNA plugin by typing symantec_ztna 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 Parser **Symantecztna** has been added as required resources of **Symantec_ztna** Plugin in RSA Live. Deploy the parser to appropriate Log Decoders when you deploy plugin log collection file.

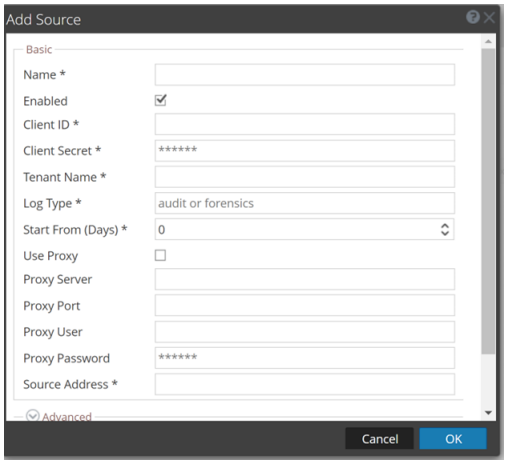
For more details, see the Add or Update Supported Event Source Log Parsers topic, or the Live Resource Guide on RSA Link.

Configure symantec_ztna plugin in NetWitness Suite UI

1. In RSA NetWitness Suite menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Collector service, and choose Config option from the system menu.
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 symantec_ztna 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  , the Source panel tool bar, the Add Source dialog is displayed.



7. Define parameter values, as described in Symantec_ztna Collection Configuration.



8. Click **Test Connection**, the result of the test will display in the dialog box. If the test is not successful, edit the device or service information based on the 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 RSA NetWitness Suite displays a Request Timed Out Error. It is recommended to start the plugin even if the testconnection times out and then check the log for errors

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 Symantec_ztna plugin type.

Symantec_ztna Collection Configuration Parameters

This section describes the Symantec_ztna plugin configuration parameters.

Note: Items that are followed by an asterisk (*) 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.
Client ID*	Client ID to be used to connect to ZTNA luminate API.
Client Secret*	Client Secret to be used to connect to ZTNA luminate API.
Tenant Name*	Name of the tenant configured for Symantec ZTNA.
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 Passwor	Password for the proxy (leave empty if using anonymous proxy).
Source Address	IP address that is to be given to Symantec Endpoint Security plugin instance. (Logs from this event source will be collected with this device IP)
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. **Note:** Set this value to 600 seconds for the symantec_ztna plugin.
Max Duration Poll	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	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

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.