

NetWitness[®] Platform

Symantec Web Security Services Plugin Event Source Log Configuration Guide

Symantec Web Security Services Plugin

Last Modified: Thursday, July 18, 2024

Event Source Product Information:

Vendor: [BROADCOM](#)

Event Source: [Symantec Web Security Service](#)

Versions: v1.0

RSA Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: symantec_wss

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 and 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/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

February, 2024

Contents

- Introduction 5**
- Setup the Symantec WSS plugin in the NetWitness Platform 6**
 - Deploy symantecwss files from Live 6
 - Configure the symantecwss plugin in the NetWitness Platform UI 6
 - Symantec WSS Collection Configuration Parameters 9
 - Basic Parameters 9
 - Advanced Parameters 9
- Getting Help with NetWitness Platform 11**
 - Self-Help Resources 11
 - Contact NetWitness Support 11
 - Feedback on Product Documentation 12

Introduction

Increasing web use, rapid cloud adoption, and more significant numbers of mobile and remote users are exposing your network to additional risk. Symantec Web Security Service (WSS) is an indispensable line of defense against modern day cyber threats. It provides secure web services, enables enterprises to control access, protects users from threats, and secures their sensitive data.

The Web Security Service offers two APIs (Download and Sync) for obtaining access log data from the cloud. The Download API restricts a client from receiving partial hour data, thus obtaining log data from the current hour is not possible with this API. The Sync API is an enhancement to the Download API. It allows a web client to obtain recently hardened log data from the cloud by downloading the current hour in smaller up-to-the-minute segments.

This plugin uses the sync API to capture real-time access log data.

Setup the Symantec WSS plugin in the NetWitness Platform

In the RSA NetWitness Platform, perform the following tasks:

- Deploy the symantecwss package from Live
- Configure the symantecwss plugin in the NetWitness Platform UI

Deploy symantecwss files from Live

Symantec WSS plugin requires resources available in Live to collect logs.

To deploy the symantecwss content from live:

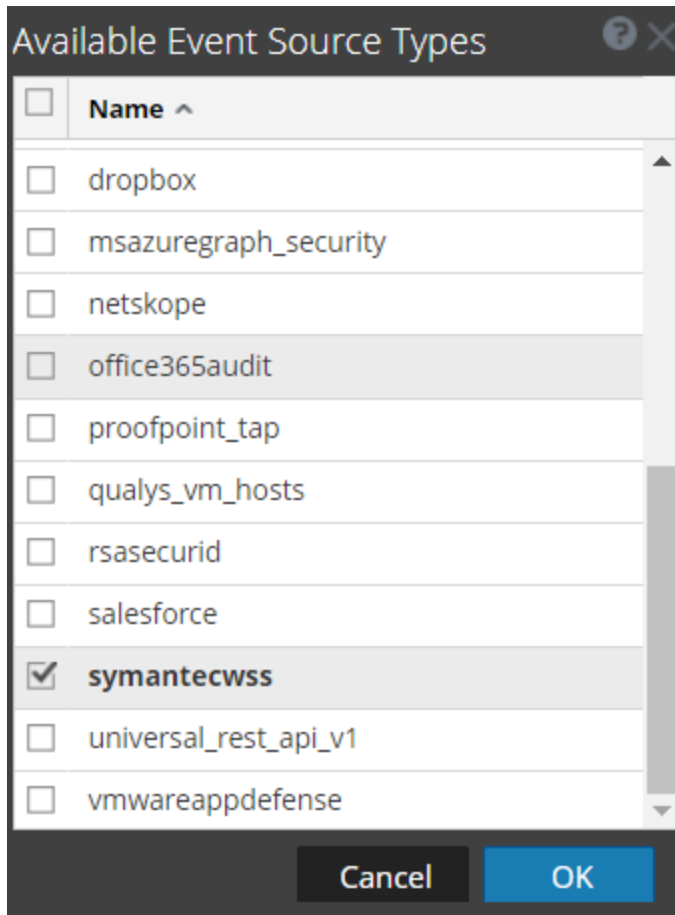
1. In the RSA NetWitness Platform menu, select **Live**. Browse Live for Universal Rest API plugin by typing **symantecwss** into the Keywords text box and click **Search**.
2. Select the result returned from the Search.
3. Click **Deploy** to deploy the Universal Rest API Plugin to the appropriate Log Collectors, using the Deployment Wizard.
4. Log Parser **Symantec_wss** has been added as required resources of symantecwss Plugin in RSA Live. Deploy the parser to appropriate Log Decoders when you deploy the plugin log collection file.

For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic, or the *Live Services Management Guide* on RSA Link.

Configure the symantecwss plugin in the NetWitness Platform UI

Perform the following steps to configure the symantecwss plugin in the NetWitness Platform UI

1. In the RSA NetWitness Platform 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 drop-down menu.
The **Event Categories** panel displays the File event sources that are configured, if any.
4. In the **Event Categories** panel, click +.
The **Available Event Source Types** dialog is displayed.



5. Select **symantecwss** 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. The **Add Source** dialog is displayed.

The screenshot shows the 'Add Source' dialog box with the following fields and values:

- Name * (empty)
- Enabled
- User Name * (empty)
- Password * (masked with asterisks)
- Start Date (In Hours) * (0)
- Use Proxy
- Proxy Server (empty)
- Proxy Port (empty)
- Proxy User (empty)
- Proxy Password (masked with asterisks)
- Source Address * (empty)

Buttons: Test Connection, Cancel, OK

7. Define parameter values, as described in [Symantec WSS 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 the message displayed 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 the RSA NetWitness Platform displays a **Request Timed Out** Error. This API sends a zip of the aggregated logs for the current hour and thus, there is a delay in the initial response time due to which test connection may time out. It is recommended to start the plugin even if the test connection 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 Universal Rest API plugin type.

Symantec WSS Collection Configuration Parameters

This section describes the Universal Rest API plugin configuration parameters.

Note: Fields 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.
User Name*	Username to be used for the sync API.
Password*	Password to be used for the sync API.
Start From (In Hours)*	Number of hours to backtrack and pull data from.
Use Proxy	Select the checkbox 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 an anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using an anonymous proxy).
Source Address*	The IP address that is to be given to the Universal Rest API 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	<p>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.</p> <div data-bbox="597 520 1421 573" style="border: 1px solid green; padding: 5px;"> <p>Note: Set this value to 600 seconds for the symantecwss plugin.</p> </div>
Max Duration Poll	<p>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.</p>
Max Events Poll	<p>The maximum number of events per polling cycle (how many events collected per polling cycle).</p>
Max Idle Time Poll	<p>The maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.</p>
Command Args	<p>Optional arguments to be added to the script invocation.</p>
Debug	<div data-bbox="597 951 1421 1066" style="border: 1px solid yellow; padding: 5px;"> <p>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.</p> </div> <div data-bbox="597 1087 1421 1171" style="border: 1px solid yellow; padding: 5px;"> <p>Caution: Enabling debugging will adversely affect the performance of the Log Collector.</p> </div> <p>Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"> • Off = (default) disabled • On = enabled • Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>This parameter is designed for debugging and monitoring 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.</p>
SSL Enable	<p>Uncheck to disable certificate verification.</p>

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.