

# NetWitness<sup>®</sup> Platform XDR

## Symantec Endpoint Security Incidents Plugin Event Source Log Configuration Guide

# Symantec Endpoint Security Incidents Plugin

## Event Source Product Information:

**Vendor:** [BROADCOM](#)

**Event Source:** [Symantec Endpoint Security](#)

**Versions:** 14.3.x

## NetWitness Product Information:

**Supported On:** NetWitness Platform XDR 11.5.0 and later

**Event Source Log Parser:** symantec\_endpointsecurity

**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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2022

## Contents

---

<b>Introduction</b> .....	<b>5</b>
<b>Integrate Symantec Endpoint Security with the NetWitness Platform XDR</b> .....	<b>6</b>
<b>Setup the Symantec Endpoint Security Incidents Plugin in the NetWitness Platform XDR</b> .....	<b>7</b>
Deploy symantec_es_incidents Files from Live .....	7
Configure the symantec_es_incidents Plugin in the NetWitness Platform XDR .....	7
Symantec Endpoint Security Incidents Collection Configuration Parameters .....	10
Basic Parameters .....	10
Advanced Parameters .....	10
<b>Getting Help with NetWitness Platform XDR</b> .....	<b>12</b>
Self-Help Resources .....	12
Contact NetWitness Support .....	12
Feedback on Product Documentation .....	13

## Introduction

---

Endpoint security plays a major role in securing endpoints of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors or intruders. The endpoint security space has evolved over the last several years away from limited antivirus software into a more advanced, comprehensive defense.

Symantec Endpoint Security, a cloud-managed software, delivers multilayer protection to stop threats, regardless of how they attack your endpoints. Symantec Endpoint Security provides security on Windows, Mac, and Linux. For more information, see <https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Getting-Started/what-is-v129161010-d4161e112.html>.

Symantec Endpoint Security escalates the malicious events to incidents. An incident is a collection of one or more events that represent a significant risk or potential threat to the organization. The NetWitness Symantec Endpoint Security Incidents plugin collects these incidents generated on the Symantec Endpoint Detection and Response (EDR).

## Integrate Symantec Endpoint Security with the NetWitness Platform XDR

---

To configure and integrate Symantec Endpoint Security with the NetWitness Platform XDR:

1. Login to the Symantec Endpoint Security console.
2. Go to **Integration > Client Applications**.
3. Click **Add Client Application**.
4. Enter the name of the application and click the **Add** button.  
The client application details view is displayed.
5. Select the privileges for the client application. Click **Save**.
6. Click the ellipsis and select **Client Secret**.  
Make sure the credentials have the permission to run commands remotely.
7. Click the **copy** icon and copy the credentials.

For more information, see [https://apidocs.securitycloud.symantec.com/#/doc?id=ses\\_auth](https://apidocs.securitycloud.symantec.com/#/doc?id=ses_auth).

## Setup the Symantec Endpoint Security Incidents Plugin in the NetWitness Platform XDR

---

In the NetWitness Platform XDR, perform the following tasks:

- [Deploy symantec\\_es\\_incidents Files from Live](#)
- [Configure the symantec\\_es\\_incidents Plugin in the NetWitness Platform XDR.](#)

### Deploy symantec\_es\_incidents Files from Live

Symantec Endpoint Security Incidents plugin requires resources available in Live to collect logs.


**To deploy the symantec\_es\_incidents content from live:**

1. In the NetWitness Platform XDR menu, select **Configure > Live Content**. Browse Live for Symantec Endpoint Security Incidents plugin by typing **symantec\_es\_incidents** 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\_endpointsecurity** has been added as required resources of **Symantec\_es\_incidents** Plugin in NetWitness Live. Deploy the parser to appropriate Log Decoders when you deploy the plugin log collection file.

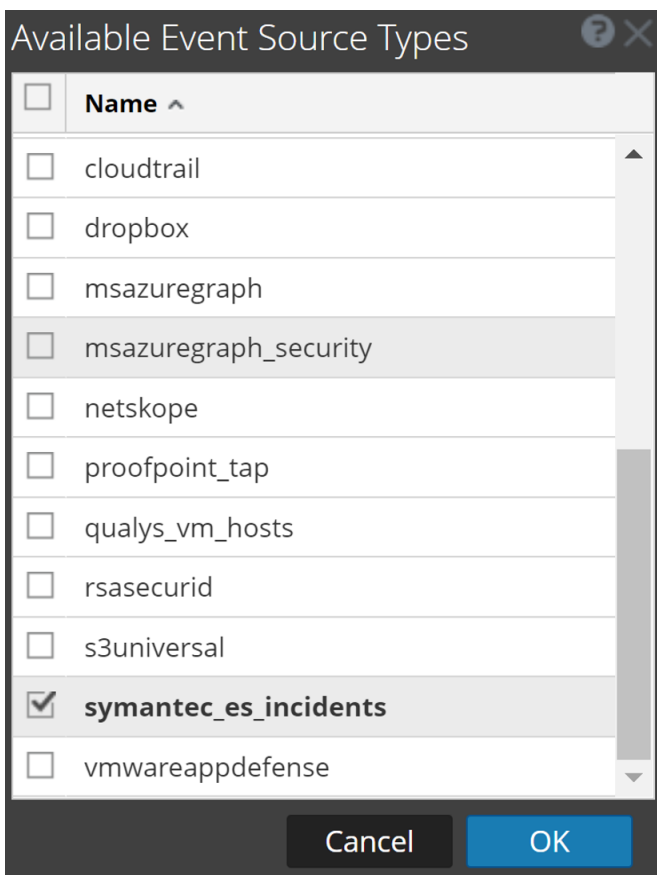
For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic, or the *Live Services Management Guide* on NetWitness Link.

### Configure the symantec\_es\_incidents Plugin in the NetWitness Platform XDR

Perform the following steps to configure the symantec\_es\_incidents plugin in the NetWitness Platform XDR:

1. In the NetWitness Platform XDR 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 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 **symantec\_es\_incidents** 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 \*
- Enabled
- Client ID \*
- Client Secret \* (masked with asterisks)
- Start From (Days) \* (0)
- Use Proxy
- Proxy Server
- Proxy Port
- Proxy User
- Proxy Password (masked with asterisks)
- Source Address \*

Buttons: Test Connection, Cancel, OK

7. Define parameter values, as described in [Symantec Endpoint Security Incidents 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 NetWitness Platform XDR 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 Symantec\_es\_incidents plugin type.

## Symantec Endpoint Security Incidents Collection Configuration Parameters

This section describes the Symantec\_es\_incidents 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.
Client ID *	Client ID used to connect to event export stream API.
Client Secret *	Client Secret used to connect to event export stream API.
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 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	<p>Interval (amount of time in seconds) between each poll. The default value is <b>180</b>. 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 1417 604" style="border: 1px solid green; padding: 5px;"> <p><b>Note:</b> Set this value to <b>600</b> seconds for the <b>symantec_es_incidents</b> 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 <b>600</b>. We recommend setting this value to <b>1800</b> 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="597 982 1417 1100" style="border: 1px solid yellow; padding: 5px;"> <p><b>Caution:</b> Only enable debugging (set this parameter to <b>On</b> or <b>Verbose</b>) if you have a problem with an event source and you need to investigate this problem.</p> </div> <div data-bbox="597 1121 1417 1205" style="border: 1px solid yellow; padding: 5px;"> <p><b>Caution:</b> 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"> <li>• <b>Off</b> = (default) disabled</li> <li>• <b>On</b> = enabled</li> <li>• <b>Verbose</b> = enabled in verbose mode - adds thread information and source context information to the messages.</li> </ul> <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>
Incidents Limit	<p>The number of records fetched in each request. Event export stream API supports maximum of <b>2000</b> Incidents per request.</p>

## Getting Help with NetWitness Platform XDR

### 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 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 XDR 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	<a href="https://community.netwitness.com">https://community.netwitness.com</a> In the main menu, click <b>Support &gt; Case Portal &gt; View My Cases</b> .
International Contacts (How to Contact NetWitness Support)	<a href="https://community.netwitness.com/t5/support/ct-p/support">https://community.netwitness.com/t5/support/ct-p/support</a>
Community	<a href="https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions">https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions</a>

## Feedback on Product Documentation

You can send an email to [nwdocsfeedback@netwitness.com](mailto:nwdocsfeedback@netwitness.com) to provide feedback on NetWitness Platform documentation.