

RSA NetWitness Platform

Event Source Log Configuration Guide



Forcepoint Websense Web Security

Last Modified: Wednesday, February 27, 2019

Event Source Product Information:

Vendor: [Forcepoint](#)

Event Source: Websense Web Security

Versions: 5.5, 6.3, 7.0, 7.1, 7.5, 7.6, 7.7, 7.8.1, 7.8.4, 8.x

Note: RSA supports the legacy Websense format, as well as the new log format which is part of the Forcepoint rebranding. RSA continues to support all minor versions of Forcepoint Websense Web security. Use of older parser versions may lead to unknown messages.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: websense

Collection Method: SNMP, ODBC (7.5, 7.6, and 7.7), and Syslog (7.7 and later)

Event Source Class.Subclass: Host.Web Logs

To receive all logs from Websense Web Security version 7.5 or later, you must configure RSA NetWitness Platform to use the SNMP collection method. You must also configure either ODBC or syslog as a second collection method. RSA NetWitness Platform collects system alerts and usage alerts via SNMP, and uses ODBC or syslog to collect Internet activity logs and the associated web filtering actions from the Websense Web Security event source.

Note: RSA recommends using syslog collection instead of ODBC for version 7.7 and later.

For earlier versions of Websense Web Security, you only need to configure RSA NetWitness Platform to use the SNMP collection method.

Depending on your Websense version, see one of the following sections:

- [Configure Websense Web Security 7.7 and later](#)
- [Configure Websense Web Security 7.1, 7.5, and 7.6](#)
- [Configure Websense Web Security Suite 6.3 or Web Security 7.0](#)
- [Configure Websense Web Security Suite 5.5](#)

To enable ODBC collection for versions 7.5, 7.6 and 7.7, see [Configure NetWitness Platform for ODBC Collection](#):

Syslog collection is only supported for version 7.7 and later of this event source. For instructions, see [Configure Syslog Collection for Websense Web Security 7.7 or later](#).

Note: To receive all logs from the Websense Web Security event source, you must configure SNMP collection. For version 7.5 or later, you must also configure ODBC or syslog collection. RSA recommends using syslog as the collection method.

Configure Websense Web Security 7.7 and later

To enable SNMP:

1. Log on to Triton Unified Security Center.
2. On the **Settings** tab, expand **Alerts**, and click **Enable Alerts**.
3. In the Enable Alerts window, in the **SNMP Alerts** section, select **Enable SNMP alerts**.
4. Complete the fields as follows.

Field	Value
Community name	public
Server IP or name	The IP address of the RSA NetWitness Log Collector
Port	162

5. Click **OK**.
6. Click **Save and Deploy**.

To configure SNMP:

1. On the **Settings** tab, expand **Alerts**, and click **System**.
2. In the Settings window, follow these steps:
 - a. In the **SNMP** column, select the events on which you want to receive alerts.
 - b. Click **OK**.
 - c. Click **Save and Deploy**.
3. On the **Settings** tab, in the **Alerts** section, click **Category Usage**.
4. In the Category Usage window, follow these steps:
 - a. Click a category name on which you want to receive alerts.
 - b. In the Edit Category window, select **SNMP**, and select the **Threshold** value.
 - c. Repeat steps a and b for all categories on which you want to receive alerts.

- d. Click **OK**.
- e. Click **Save and Deploy**.
5. On the **Settings** tab, in the **Alerts** section, click **Protocol Usage**.
6. In the Protocol Usage window, follow these steps:
 - a. Click a protocol name on which you want to receive alerts.
 - b. In the Edit Category window, select **SNMP**, and select the **Threshold** value.
 - c. Repeat steps a and b for all protocols on which you want to receive alerts.
 - d. Click **OK**.
 - e. Click **Save and Deploy**.

Configure Websense Web Security 7.1, 7.5, and 7.6

To enable SNMP:

1. Log on to Websense Manager.
2. On the **Settings** tab, expand **Alerts and Notifications**, and click **Alerts**.
3. In the Alerts and Notifications window, in the **SNMP Alerts** section, select **Enable SNMP alerts**.
4. Complete the fields as follows.

Field	Value
Community name	public
Server IP or name	The IP address of the RSA NetWitness Log Collector
Port	162

5. Click **OK**.
6. Click **Save All**.

To configure SNMP:

1. On the **Settings** tab, expand **Alerts and Notifications**, and click **System**.
2. In the Settings window, follow these steps:
 - a. In the **SNMP** column, select the events on which you want to receive alerts.
 - b. Click **OK**.
 - c. Click **Save All**.
3. On the **Settings** tab, in the **Alerts and Notifications** section, click **Category Usage**.
4. In the Category Usage window, follow these steps:
 - a. Click a category name on which you want to receive alerts.
 - b. In the Edit Category window, select **SNMP**, and, from the **Threshold** drop-down list, select a value.

- c. Repeat steps a and b for all categories on which you want to receive alerts.
 - d. Click **OK**.
 - e. Click **Save All**.
5. On the **Settings** tab, in the **Alerts and Notifications** section, click **Protocol Usage**.
6. In the Protocol Usage window, follow these steps:
 - a. Click a protocol name on which you want to receive alerts.
 - b. In the Edit Category window, select **SNMP**, and from the **Threshold** drop-down list, select a value.
 - c. Repeat steps a and b for all protocols on which you want to receive alerts.
 - d. Click **OK**.
 - e. Click **Save All**.

Configure Websense Web Security Suite 6.3 or Web Security 7.0

To enable SNMP:

1. Log on to Websense Manager.
2. Click **Server > Settings**.
3. In the Settings dialog box, click **Alerts and Notifications**.
4. Select SNMP Alerts and complete the fields as follows.

Field	Value
Community name	public
Server IP or name	The IP address of the RSA NetWitness Log Collector
Port	162

To configure SNMP:

1. Expand **Alerts and Notifications**, and select **System**, **Category Usage**, or **Protocol Usage**.
2. Select the SNMP alerts that you want to enable, and click **OK**.
3. Repeat steps 1 and 2 until you have configured all of the categories.
4. Click **OK** to close the Settings dialog box.

Configure Websense Web Security Suite 5.5

RSA NetWitness Platform uses SNMP traps to collect from this event source. You must complete the following tasks to configure Websense to send SNMP traps:

- I. On the Websense event source:
 - i. Configure the SNMP traps.
 - ii. Configure the filter definitions.
 - iii. Verify that the Websense Log Reporter and associated databases are running.
- II. In RSA NetWitness Platform, perform the following steps:
 - i. Add the SNMP Event Source Type
 - ii. Configure SNMP Users

Configure the SNMP Traps

To configure the SNMP Traps:

1. On the Websense host, start Websense Enterprise Manager.
2. On the **Network** tab, click **Server > Settings**.
3. Click **Logging/Events**.
4. Select **Event Publisher enabled**.
5. Under **Publisher Service for IBM**, complete the fields as follows.

Publisher Service	IP address of Websense host
Publisher Port	55813
SNMP Trap Destination – IP Address	The IP address of the RSA NetWitness Log Collector (for a multiple appliance site, the IP address of the LC or RC collecting the SNMP traps).
SNMP Trap Destination – Community Name	Public

Publisher Service	IP address of Websense host
SNMP Destination - Port	162

Configure the Filter Definitions

To configure the filter definitions:

1. In the main window in the Websense Enterprise Manager, select **Filter Definitions**.
2. Select **Event Publisher**.
3. Select **Categories for Event Alerts**.
4. Select the categories for which you want traps sent.


Verify that Websense Log Reporter and Associated Databases are Running

The Websense Log Reporter and associated databases must be running for SNMP traps to be generated. For information, see the Websense documentation.

Add the SNMP Event Source Type

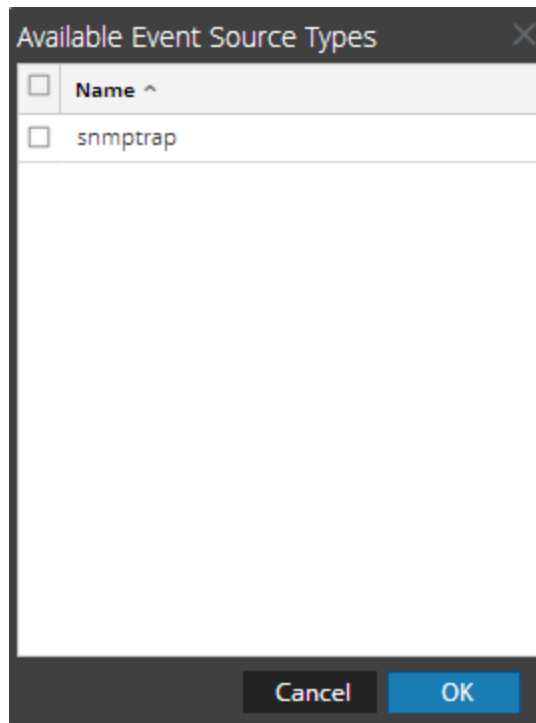
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

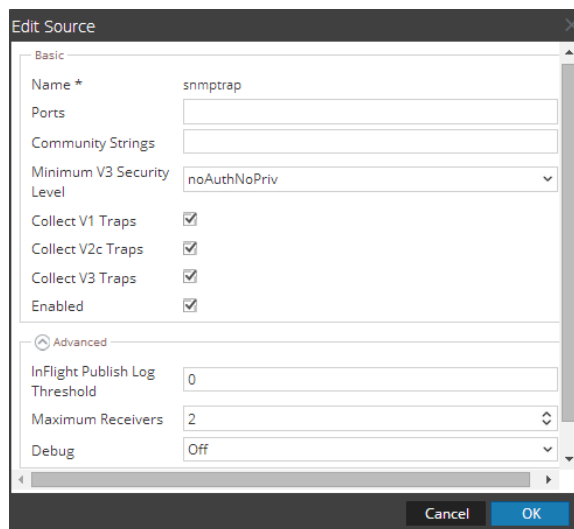
1. In the **RSA NetWitness Platform** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

The Sources panel is displayed with the existing sources, if any.

5. Click **+** to open the **Available Event Source Types** dialog.



6. Select **snmptrap** from the Available Event Source Types dialog and click **OK**.
7. Select **snmptrap** in the Event Categories panel.
8. Select **snmptrap** in the Sources panel and then click the Edit icon to edit the parameters.




9. Update any of the parameters that you need to change.

(Optional) Configure SNMP Users

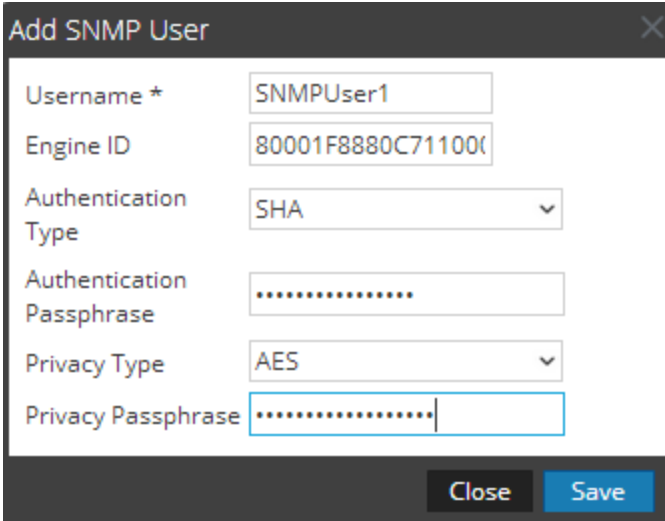
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

Configure SNMP v3 Users

1. In the **RSA NetWitness Platform** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/SNMP v3 User Manager** from the drop-down menu.

The SNMP v3 User panel is displayed with the existing users, if any.

5. Click **+** to open the **Add SNMP User** dialog.



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

Field	Value
Username *	SNMPUser1
Engine ID	80001F8880C71100
Authentication Type	SHA
Authentication Passphrase
Privacy Type	AES
Privacy Passphrase

6. Fill in the dialog with the necessary parameters. The available parameters are described below.

SNMP User Parameters

The following table describes the parameters that you need to enter when you create an SNMP v3 user.

Parameter	Description
Username *	<p>User name (or more accurately in SNMP terminology, security name). RSA NetWitness Platform uses this parameter and the Engine ID parameter to create a user entry in the SNMP engine of the collection service.</p> <p>The Username and Engine ID combination must be unique (for example, logcollector).</p>
Engine ID	<p>(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source.</p> <p>For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.</p>
Authentication Type	<p>(Optional) Authentication protocol. Valid values are as follows:</p> <ul style="list-style-type: none"> • None (default) - only security level of noAuthNoPriv can be used for traps sent to this service • SHA - Secure Hash Algorithm • MD5 - Message Digest Algorithm
Authentication Passphrase	<p>Optional if you do not have the Authentication Type set. Authentication passphrase.</p>
Privacy Type	<p>(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows:</p> <ul style="list-style-type: none"> • None (default) • AES - Advanced Encryption Standard • DES - Data Encryption Standard
Privacy Passphrase	<p>Optional if you do not have the Privacy Type set. Privacy passphrase.</p>
Close	<p>Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.</p>
Save	<p>Adds the SNMP v3 user parameters or saves modifications to the parameters.</p>

Configure NetWitness Platform for ODBC Collection

To configure Websense Web Security for ODBC collection, perform the following tasks in RSA NetWitness Platform:

- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Add the Event Source Type

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it from RSA NetWitness Platform Live.


Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions** menu, choose **View > Config**.
3. In the **Service Parsers Configuration** panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **websense**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
5. The **DSNs** panel is displayed with the existing **DSNs**, if any.

- Click **+** to open the **Add DSN** dialog.


Note: If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).

- Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
- Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by Websense
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Websense
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqs27.so For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqs26.so

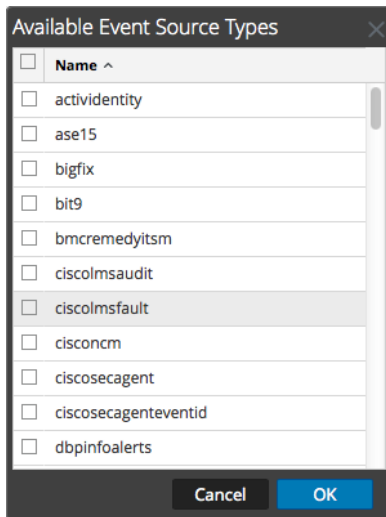
Add the ODBC Event Source Type

Add the ODBC Event Source Type:

- In the **NetWitness** menu, select **ADMIN > Services**.
- In the **Services** grid, select a **Log Collector** service.
- Click  under **Actions** and select **View > Config**.
- In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.

The Event Categories panel is displayed with the existing sources, if any.

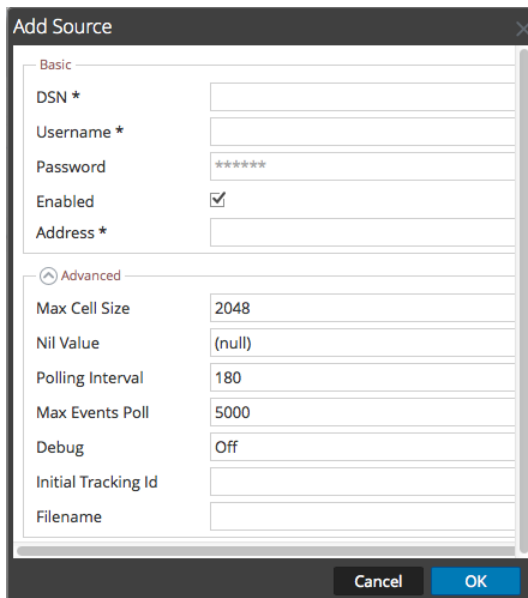
- Click **+** to open the **Available Event Source Types** dialog.



- Choose the log collector configuration type for your event source type and click **OK**.

Choose **websense** from the **Available Event Source Types** dialog box.

- In the **Event Categories** panel, select the event source type that you just added.
- In the **Sources** panel, click **+** to open the **Add Source** dialog.



- Enter the DSN you configured during the **Configure a DSN** procedure.

10. For the other parameters, see the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Configure Syslog Collection for Websense Web Security 7.7 or later

To configure Syslog collection for the Websense Web Security you must:

- I. Configure Syslog Output on Websense Web Security
- II. In RSA NetWitness Platform, Ensure the Required Parser is Enabled
- III. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Websense Web Security

To configure syslog collection for Websense Web Security 7.7 or later:

1. Select **Settings > General > SIEM Integration**.
2. Select **Enable SIEM integration for this Policy Server**, and complete the following fields:

Field	Action
IP address or hostname	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Transport protocol	Select UDP .
SIEM format	Select syslog/key-value pairs .

3. To cache your changes, click **OK**. To save changes, click **Save and Deploy**.

In RSA NetWitness Platform, Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.



Note: The required parser is **websense**.

Configure RSA NetWitness Platform for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:
 - If you see  **Start Capture**, click the icon to start capturing Syslog.
 - If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

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

The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.