

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## Symantec Endpoint Protection

Last Modified: Friday, September 27, 2019

### Event Source Product Information:

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

**Event Source:** Endpoint Protection, AntiVirus Corporate Edition

**Versions:** 9.0, 10.x, 11, 11.0.5, 11.0.6, 12.x, 14, 15 (Syslog only)

### RSA Product Information:

**Supported On:** NetWitness Platform 10.0 and later

**Event Source Log Parser:** symantecav

**Collection Method:** SNMP, Syslog, ODBC

**Event Source Class.Subclass:** Security.Antivirus

This document describes how to configure the Symantec event source to communicate with the RSA NetWitness Platform. This document contains the following sections:

- [Symantec Collection Methods](#)
- [Configure Syslog](#)
- [Configure ODBC](#)
- [Configure AntiVirus SNMP Traps](#)

## Symantec Collection Methods

---

To integrate Symantec Endpoint Protection with RSA NetWitness Platform, you can choose among several collection methods, depending on your environment and the types of messages that you want to collect.

### Collect via SNMP

If you set up SNMP collection, you can collect antivirus messages.

### Collect via Syslog

If you set up Syslog collection, you can collect the following logs:

- Management Server Logs
  - System Administrative log
  - System Client-Server Activity log
  - Audit log
  - System Server Activity log
- Client Logs
  - Activity log
  - Security log
  - Traffic log
  - Packet log
  - Control log
  - Scan log
  - Risk Log
  - Proactive Threat Protection log

## Collect via ODBC

If you set up ODBC collection, you can collect different logs, depending on your Symantec version.

### **Symantec Endpoint Protection version 12**

If you set up ODBC collection, you can collect the following logs for Symantec Endpoint Protection version 12:

- System Server activity logs
- Scan logs
- Client Activity log
- Client Behavior logs
- Client Security log
- Client Traffic log

### **Symantec Endpoint Protection version 11**

If you set up ODBC collection, you can collect the following logs for Symantec Endpoint Protection version 11:

- System Server activity logs
- Scan logs

## Configure Syslog

---

To configure Syslog, perform the following tasks:

- Configure Symantec Endpoint Protection for Syslog
- Configure RSA NetWitness Platform for Syslog Collection

### Configure Symantec Endpoint Protection for Syslog

Perform the following procedure to configure Symantec Endpoint Protection to collect Syslog.

#### To configure Symantec Endpoint Protection for Syslog:

1. Log on to the **Symantec Endpoint Protection Manager Console** with administrative credentials.
2. Click the **Admin** icon.
3. Click **Servers**.
4. Click the local or remote site from which you want to export log data.
5. Click **Configure External Logging**.
6. On the **General** tab, select **Enable Transmission of Logs to a Syslog Server**, and the parameters as follows.

| Field                | Value  |
|----------------------|--|
| Syslog Server        | the IP address of the RSA NetWitness Log Decoder or Remote Log Collector |
| UDP Destination Port | <b>514</b>   |
| Log Facility         | <b>6</b>   |

7. On the **Log Filter** tab, select the logs that you want to monitor. Select any of the following logs:

- Management Server Logs
  - System Administrative Log
  - System Client-Server Activity Log
  - Audit Log
  - System Server Activity Log
- Client Logs
  - Client Activity Log
  - Security Log
  - Traffic Log
  - Packet Log
  - Control Log
  - Scan Log
  - Risk Log
  - Proactive Threat Protection Log

8. Click **OK**.



## 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 **ADMIN > 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 **ADMIN > 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.

After 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.

## Configure ODBC Collection

---

To configure the Internet Scanner or RealSecure 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 **symantecav**.

### 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.
6. 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](#).

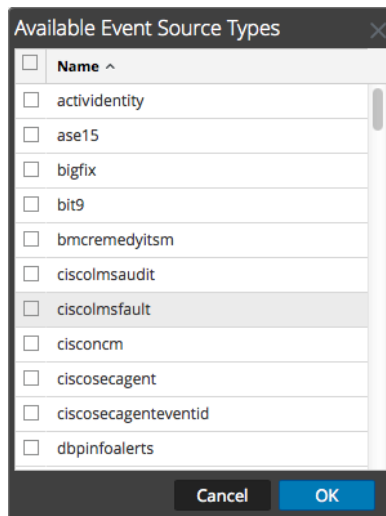
7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

| Field                     | Description  |
|---------------------------|--|
| DSN Template              | Choose the correct template from the available choices.  |
| DSN Name                  | Enter a descriptive name for the DSN   |
| <b>Parameters section</b> |  |
| Database                  | Specify the database used by Symantec Endpoint Protection  |
| PortNumber                | Specify the Port Number. The default port number is <b>1433</b>  |
| HostName                  | Specify the hostname or IP Address of Symantec Endpoint Protection   |
| Driver                    | Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> <li>• For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so</li> <li>• For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so</li> </ul> |

## Add the ODBC Event Source Type

### Add the ODBC Event Source Type:

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/Config** from the drop-down menu.  
The Event Categories panel is displayed with the existing sources, if any.
5. Click **+** to open the **Available Event Source Types** dialog.



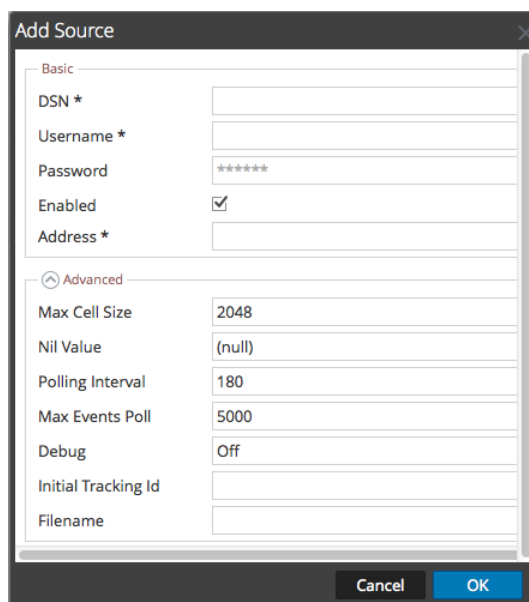
6. Choose the log collector configuration type for your event source type and click **OK**.

From the **Available Event Source Types** dialog, select the appropriate value for your version:

- For version 11 and earlier, select **symantecep**
- For version 12 and later, select **symantecepv12**

7. In the **Event Categories** panel, select the event source type that you just added.

8. In the **Sources** panel, click **+** to open the **Add Source** dialog.



9. 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 SNMP Traps

---

To configure SNMP Traps, perform the following tasks:

- Configure Symantec Endpoint Protection for SNMP
- In RSA NetWitness Platform, Add the SNMP Event Source Type
- In RSA NetWitness Platform, Configure SNMP Users

## Configure Symantec Endpoint Protection for SNMP

You must configure Symantec Antivirus to send SNMP traps to the RSA NetWitness Platform Log Decoder or Remote Log Collector designated as the collector of Symantec events.

**Note:** The administrator performing this task must be familiar with the Symantec System Console.

**Warning:** Configure each physical device running Symantec Antivirus to send traps, in addition to the master server running the Symantec System Center.

### To configure Symantec AntiVirus for SNMP:

1. On your Symantec Antivirus Corporate server, set up and configure the Symantec Antivirus and the Symantec Asset Management Suite (AMS) server according to the vendor's instructions.
2. On your Symantec Antivirus Corporate server, configure the NetWitness Platform Log Decoder or Remote Log Collector as the destination address of the SNMP Service. Follow these steps:
  - a. Click **START > All Programs > Administrative Tools > Services**.
  - b. Right-click **SNMP Service**, and select **Properties**.
  - c. Click the **Traps** tab.
  - d. In the **Community Name** field, type NetWitness Platform, and click **Add to list**.
  - e. Click **Add**.
  - f. Enter the IP address of the NetWitness Platform Log Decoder or Remote Log Collector, and click **Add**.

- g. Click **Apply**.
      - h. Click **OK**.
    3. Ensure that the SNMP Service is **Running** and is set to **Automatic**.
    4. To configure the AMS Admin Utility to send SNMP traps to RSA NetWitness Platform, follow these steps:
      - a. Start the AMS Admin Utility.
      - b. Click **Configure AMS**.
      - c. Expand **Symantec Antivirus Corporate Edition**, and select **Virus Found**.
      - d. Click **Configure**.
      - e. Select **Send SNMP Trap** and click **Next**.
      - f. Select the Symantec Antivirus Server, and click **Next**.
      - g. Clear the Alert Message Box field, and add the following message to the field:

```
<Actual Action>
<Alert Name>
<Computer Name>
<Date>
<File Path>
<Logger>
<Requested Action>
<Severity>
<Source>
<Time>
<User>
<Virus Name>
```
      - h. Set **Action Name** to NetWitness Platform, and click **Finish**.

## 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:

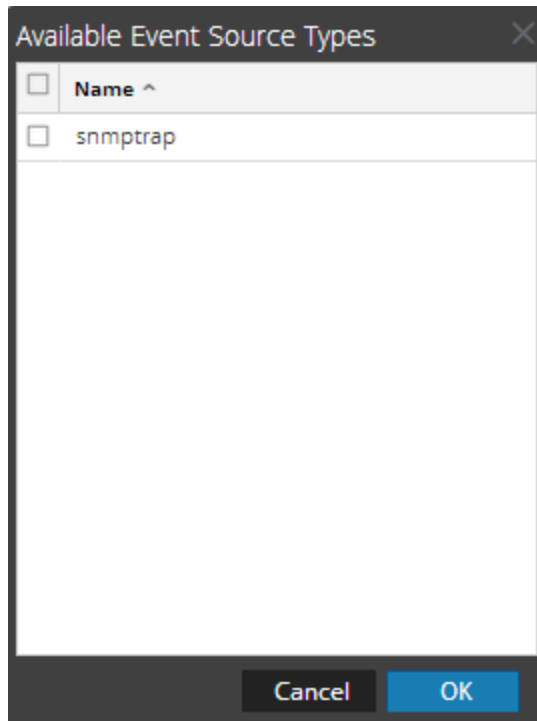
1. In the **RSA NetWitness Platform** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click

 under **Actions** and select **View > Config**.

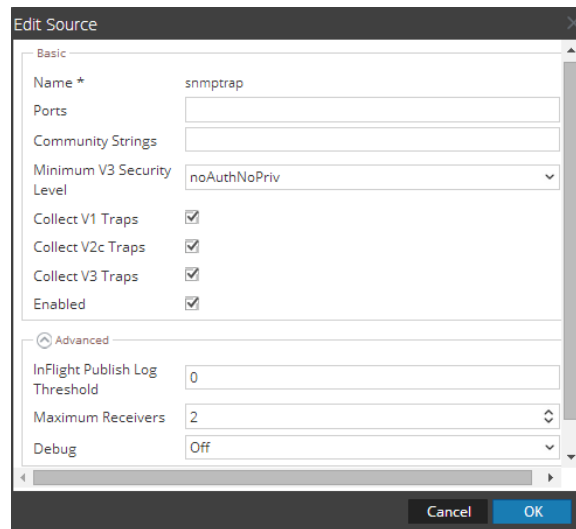
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

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.

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  |
|----------------------------|--|
| <b>Username *</b>          | <p>User name (or more accurately in SNMP terminology, security name). RSA NetWitness Platform uses this parameter and the <b>Engine ID</b> parameter to create a user entry in the SNMP engine of the collection service.</p> <p>The <b>Username</b> and <b>Engine ID</b> combination must be unique (for example, <b>logcollector</b>).</p> |
| <b>Engine ID</b>           | <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>                                    |
| <b>Authentication Type</b> | <p>(Optional) Authentication protocol. Valid values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default) - only security level of <b>noAuthNoPriv</b> can be used for traps sent to this service</li> <li>• <b>SHA</b> - Secure Hash Algorithm</li> </ul>  |



| Parameter                        | Description  |
|----------------------------------|--|
|                                  | <ul style="list-style-type: none"><li>• <b>MD5</b> - Message Digest Algorithm</li></ul>  |
| <b>Authentication Passphrase</b> | Optional if you do not have the <b>Authentication Type</b> set. Authentication passphrase.   |
| <b>Privacy Type</b>              | (Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows: <ul style="list-style-type: none"><li>• <b>None</b> (default)</li><li>• <b>AES</b> - Advanced Encryption Standard</li><li>• <b>DES</b> - Data Encryption Standard</li></ul> |
| <b>Privacy Passphrase</b>        | Optional if you do not have the <b>Privacy Type</b> set. Privacy passphrase.   |
| <b>Close</b>                     | Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.   |
| <b>Save</b>                      | Adds the SNMP v3 user parameters or saves modifications to the parameters.   |

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](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).