

RSA NetWitness Platform

Event Source Log Configuration Guide



Sophos Enterprise Console

Last Modified: Friday, May 31, 2019

Event Source Product Information:

Vendor: [Sophos](#)

Event Source: Enterprise Console, Endpoint Security

Versions: 3.0, 4.5, 4.7, 5.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: sophos

Collection Method: SNMP, ODBC

Event Source Class.Subclass: Security.Antivirus

Depending on your version of Sophos Enterprise Console, do one of the following:

- [Configure Collection for Sophos Enterprise Console 4 and 5](#)
- [Configure Collection for Sophos Enterprise Console 3.0](#)

Configure Collection for Sophos Enterprise Console 4 and 5

RSA NetWitness Platform collects log information from Sophos Enterprise Console 4 and 5 using ODBC Collection.

To configure Sophos Enterprise Console 4 and 5 to work with RSA NetWitness Platform, you must complete these tasks:

- I. Create a SQL Server User SQL Server Management Studio
- II. Configure RSA NetWitness Platform for ODBC Collection

Create a SQL Server User in SQL Server Management Studio

You must create a SQL Server user. You use these credentials when you Configure RSA NetWitness Platform for ODBC Collection, later in this configuration.

To create a SQL Server logon:

1. Open the SQL Server Management Studio with administrative credentials, and access the Database Engine.
2. To create a new login, follow these steps:
 - a. From the **Object Explorer** navigation menu, expand your database server, which is the top item in the navigation pane.
 - b. Expand **Security**.
 - c. Right-click **Logins** and select **New Login**.
 - d. From the **Select a page** navigation menu, select **General**.
 - e. From the **Login name** field, type **audit_reader**.
 - f. Select **SQL Server authentication**.
 - g. Create and confirm a password.
 - h. Ensure that **Enforce Password Expiration** is not selected.
 - i. Click **OK**.

- j. Click **Security > Login**, and right-click **audit_reader**.
 - k. Select **Properties**, and from the **Select a page** navigation menu, select **User Mapping**.
 - l. Ensure that **Map** is selected for the **master** database.

Note: If using version 5.2.1 and later, ensure that 'Map' is selected for the 'master' database as well as the database name that reflects the version of the Sophos Console in use. (for example, SOPHOS521 for Sophos Enterprise Console version 5.2.1 R2).
 - m. Select the Database name reflecting the version of the Sophos Console (for example, SOPHOS521 for Sophos Console v 5.2.1.x), and under 'Database role membership', check **db_accessadmin** and **db_datareader**.
 - n. Click **OK**.
3. To set the login account permission, follow these steps:
 - a. From the **Object Explorer** navigation menu, right-click your database server, and select **Properties**.
 - b. From the **Select a page** navigation menu, select **Permissions**.
 - c. From the **Login or roles** section, select **audit_reader**.
 - d. From the **Explicit permissions** section, select the Grant column for **Alter trace** and **Connect SQL**.
 - e. Click **OK**.
 4. To set the database access permission, follow these steps:
 - a. From the **Object Explorer** navigation menu, expand your database server.
 - b. Expand **Databases > System Databases**.
 - c. Right-click **master** and select **Properties**.
 - d. From the **Select a page** navigation menu, select **Permissions**.
 - e. From the **Login or roles** section, select **audit_reader**.
 - f. From the **Explicit permissions** section, select the Grant column for **Connect** and **Execute**.
 - g. Click **OK**.

Configure RSA NetWitness Platform for ODBC Collection

Perform the following procedures:

- Ensure the required parser is enabled
- Configure a DSN
- 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 **sophos**.

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](#).

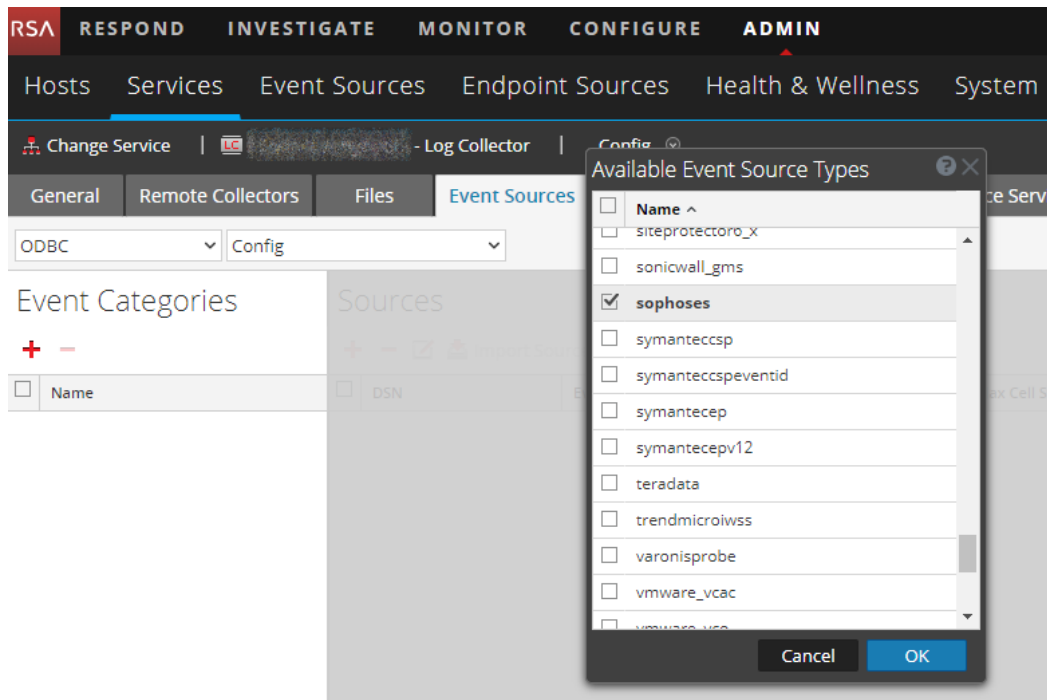
7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by Sophos Enterprise Console, for example 'SOPHOS521' should be entered for Sophos Enterprise Console version 5.2.1 R2.
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Sophos Enterprise Console
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/R3sqls27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so

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 **sophoses** for the log collector configuration type and click **OK**.



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*.

You can collect other Sophos log events:

- To collect Sophos Exploit Prevention Events:
 - Repeats steps 1–5 of the above procedure.
 - In step 6 above, choose **sophosestvm** from the available Event Source Types dialog box, then click OK.
- To collect Sophos Reporting Interface events:
 - Repeats steps 1–5 of the above procedure.
 - In step 6 above, choose **sophoses5_x** from the available Event Source Types dialog box, then click OK.

Configure Collection for Sophos Enterprise Console 3.0

RSA NetWitness Platform collects log information from Sophos Enterprise Console 3.0 using SNMP Collection.

To configure Sophos Enterprise Console 3.0 to work with RSA NetWitness Platform, you must complete these tasks:

- I. Set Up SNMP Traps on Sophos Enterprise Console 3.0
- II. Configure RSA NetWitness Platform for SNMP Collection
 - i. Add the SNMP Event Source Type
 - ii. Configure SNMP Users

Set Up SNMP Traps on Sophos Enterprise Console 3.0

To configure Sophos Enterprise Console 3.0:

1. Log on to the Sophos Enterprise Console with administrative credentials.
2. In the **Policies** section, right-click the appropriate Anti-virus and HIPS policy, and select **View/Edit Policy**.
3. Click **Messaging**, and select the **SNMP Messaging** tab.
4. Select the following:
 - **Virus/spyware detection and cleanup**
 - **Suspicious behavior detection**
 - **Suspicious file detection**
 - **Adware/PUA detection and cleanup**
 - **Scanning errors**
 - **Other errors**
5. Complete the fields as follows.


Field	Value
SNMP trap destination	Enter the IP address of your RSA NetWitness Platform Log Decoder or Remote Log Collector.
SNMP community name	Type public .

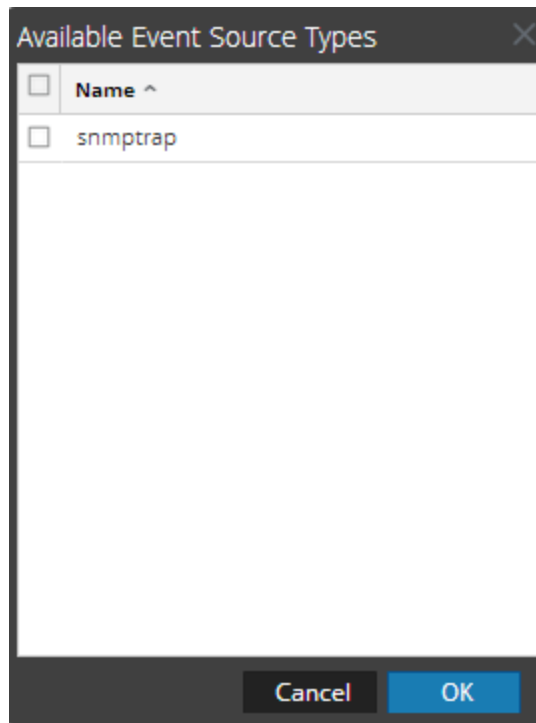
- Click **OK**.
- In the **Policies** section, right-click the appropriate Application control policy, and select **View/Edit policy**.
- Click the **SNMP Messaging** tab, and select **Enable SNMP mess.**

Add the SNMP Event Source Type

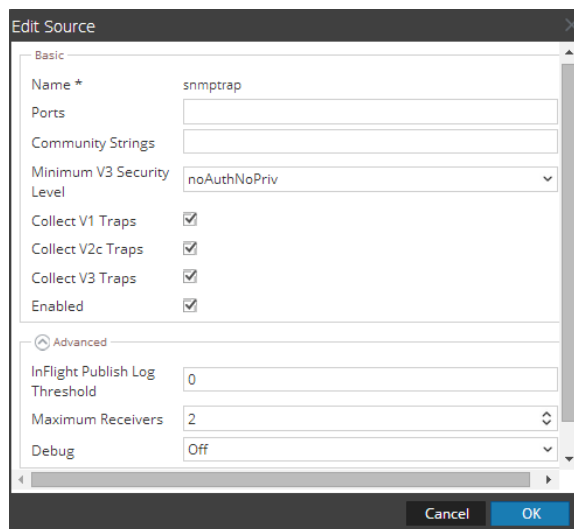
Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

Add the SNMP Event Source Type:

- In the **RSA NetWitness Platform** menu, select **Administration > 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 **SNMP/Config** from the drop-down menu.
The Sources panel is displayed with the existing sources, if any.
- 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

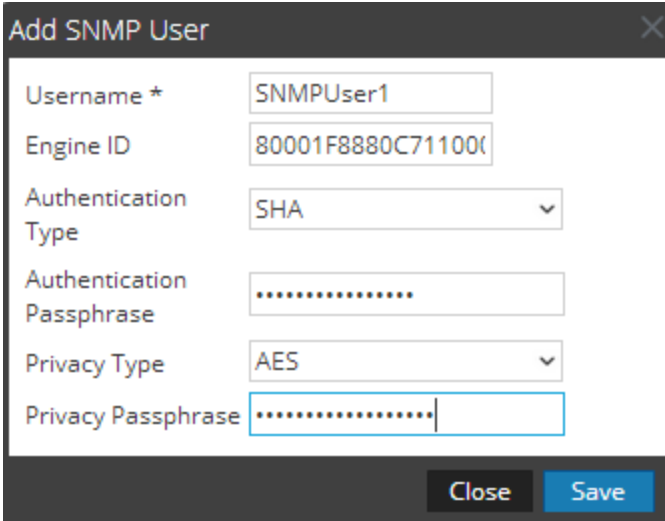
If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

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>

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.