

RSA NetWitness Logs

Event Source Log Configuration Guide



McAfee Host Intrusion Prevention System

Last Modified: Tuesday, March 07, 2017

Event Source Product Information:

Vendor: [McAfee](#)

Event Source: Host Intrusion Prevention System (also branded as Entercept)

Versions:

- 6.0.1 on McAfee ePolicy Orchestrator 3.6.0, 3.6.1
- 7.0 and 8.0 on McAfee ePolicy Orchestrator 4.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: entercept

Collection Method: ODBC

Event Source Class.Subclass: Security.IDS

Configure McAfee HIPS

Note: The ODBC connection for HIPS6X queries **ENT_IPSEvent** and **ENT_BlockedAppEvent** tables. If these tables contain no data on initial setup, the collection will fail. Make sure each of these tables contains at least one entry (row). If collection fails, add rows to the tables, and restart the ODBC service on RSA NetWitness Suite.

To configure ODBC collection in RSA NetWitness Suite, perform the following procedures:

- 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 in RSA NetWitness Suite Live.


Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration > 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 **entercept**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** 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 **ODBC/DSNs** from the drop-down menu.

- 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 [Configure DSNs](#) in the NetWitness User Guide.

- 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	
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> For 10.6.2 and newer, use <code>/opt/netwitness/odbc/lib/R3sqls27.so</code> For 10.6.1 and older, use <code>/opt/netwitness/odbc/lib/R3sqls26.so</code>
Database	Specify the database used by McAfee HIPS
PortNumber	The default port number is 1521
HostName	Specify the hostname or IP Address of the McAfee database.

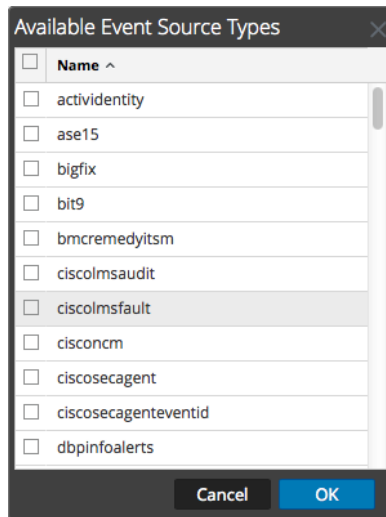
Add the Event Source Type

Add the ODBC Event Source Type:

- In the **NetWitness** 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 **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**.

To collect HIPS events, choose the entry that corresponds to your version of HIPS:

- For HIPS 6.0, select **hips6x**.
- For HIPS 7.0, select **hips7x**.
- For HIPS 8.0, select **hips8x**.

To collect ePolicy system log events, choose the entry that corresponds to your version:

- For version 3.5, select **ePolicy**.
- For versions 3.6.0 or 3.6.1, select **ePolicy36X**.
- For version 4.0, select **ePolicy4_x**.
- For version 4.5, select **ePolicy4_5**.
- For version 4.6, select **ePolicy4_5**.
- (Optional) If you want to use AutoID as the tracking column, select **ePolicy4_5AutoId**.

To collect ePolicy virus log events, choose the entry from the **Available Event Source Types** dialog box that corresponds to your version:

- For versions 3.5, 3.6.0, or 3.6.1, select **ePolicyvirus** .
- For version 4.0, select **ePolicyvirus4_x**.
- For version 4.5, select **ePolicyvirus4_5**.
- For version 4.6, select **ePolicyvirus4_5**.
- (Optional) If you want to use AutoID as the tracking column, select **ePolicyvirus4_5AutoId**.

To collect more than one type of event, you must add event source types for each. That is, run through this procedure two or three times, and add event source types for HIPS, epolicy system logs, and epolicy virus logs.

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.

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

Section	Field	Value
Basic	DSN *	
	Username *	
	Password	*****
	Enabled	<input checked="" type="checkbox"/>
	Address *	
Advanced	Max Cell Size	2048
	Nil Value	(null)
	Polling Interval	180
	Max Events Poll	5000
	Debug	Off
	Initial Tracking Id	
	Filename	

9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see [ODBC Event Source Configuration Parameters](#) in the NetWitness Suite Log Collection Guide.

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.