

RSA NetWitness Logs

Event Source Log Configuration Guide



McAfee VirusScan Enterprise

Last Modified: Monday, September 18, 2017

Event Source Product Information:

Vendor: [McAfee](#)

Event Source: VirusScan Enterprise

Versions: 8.x

Note: RSA has tested major versions of this product; all minor versions are expected to work based on the configuration and log format of this event source. Any deviation from this format, **or use of an older parser version**, may lead to unknown messages.

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: mcafeevirusscan

Collection Method: ODBC

Event Source Class.Subclass: Security.Antivirus

McAfee VirusScan Enterprise uses McAfee ePolicy Orchestrator as a management console. To configure the event source to work with RSA NetWitness Suite, perform the following steps:

- I. Set Up Event Filtering in ePolicy Orchestrator
- II. Configure NetWitness Suite for ODBC Collection

Set Up Event Filtering in ePolicy Orchestrator

To configure McAfee VirusScan, you must set up event filtering in McAfee ePolicy Orchestrator.

Note: All events in ePolicy Orchestrator are supported by RSA NetWitness Suite.

1. Log on to the ePolicy Orchestrator web console.
2. Click **Menu > Configuration > Server Settings**.
3. Under Setting Categories, click **Event Filtering**.
4. Click **Edit**.
5. In the Edit Events Filtering window, select one of the following:
 - All events to the server
 - Only selected events to the server

Note: This option requires that you select the events you want.

6. Click **Save**.

Configure NetWitness Suite for ODBC Collection

To configure McAfee VirusScan Enterprise for ODBC collection, perform the following tasks in RSA NetWitness Suite:

- 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 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 **mcafeevirusscan**.

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.
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 [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	
Database	Specify the database used by McAfee VirusScan
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of McAfee VirusScan
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

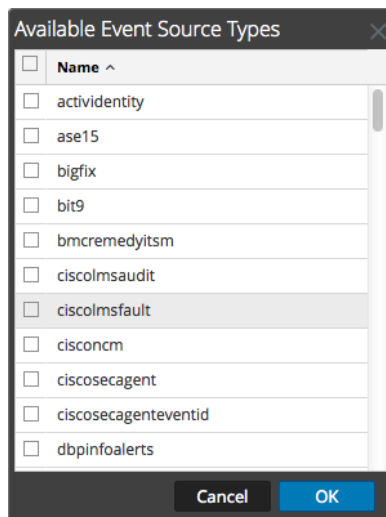
Add the ODBC Event Source Type

Add the ODBC Event Source Type:

- 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.

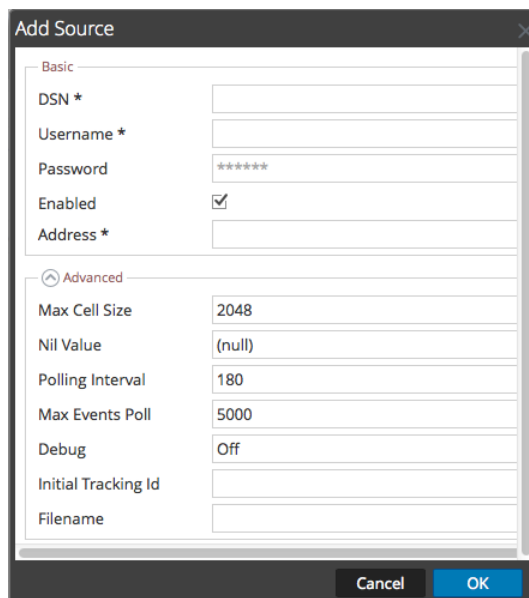
- Click **+** to open the **Available Event Source Types** dialog.



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

Select **mcafeevse** from the **Available Event Source Types** dialog.

- 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 [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.