NetWitness® Platform

McAfee Endpoint Security Event Source Log Configuration Guide

NETWITNESS
Platform

McAfee Endpoint Security

Event Source Product Information:

Vendor: McAfee

Event Source: Endpoint Security

Versions: 10.x

NetWitness Product Information:

Supported On: NetWitness Platform 11.7 and later

Note: McAfee Endpoint Security is supported from NetWitness Platform 11.5. However, NetWitness recommends you to update NetWitness Platform to the latest version.

Event Source Log Parser: epolicy

Collection Method: ODBC

Event Source Class.Subclass: Security.Antivirus

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

October, 2023

Configure McAfee Endpoint Security

To configure ODBC collection in NetWitness Platform, 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

Ensure that the parser for your event source is available:

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 **epolicy**. If you do not see the **epolicy** parser in the list while performing this procedure, you need to download it fromNetWitness Platform > Configure > Live Content.

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 and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
4. The DSNs panel is displayed with the existing DSNs, if any.
5. Click + to open the **Add DSN** dialog.

   Note: To add a DSN template, see the **Configure a DSN** topic in the *Log Collection Configuration Guide*, available in NetWitness Community.
6. Choose a **DSN Template** from the drop down menu and enter a name for the DSN. (Use this name when you set up the ODBC event source type.)
7. Fill in the parameters and click **Save**.

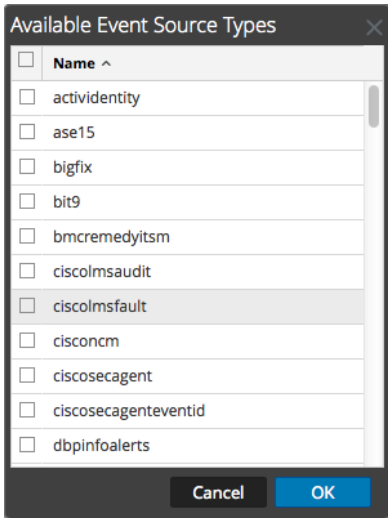
Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
	Parameters section
Database	Specify the database used by McAfee Endpoint Security
PortNumber	Specify the Port Number. The default port number is **1433**
HostName	Specify the hostname or IP Address of McAfee Endpoint Security
Driver	Depending on your NetWitness Log Collector version: • 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 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, and from the **Actions** ( ) menu, choose **View** > **Config**.
3. 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.
4. Click + to open the **Available Event Source Types** dialog.

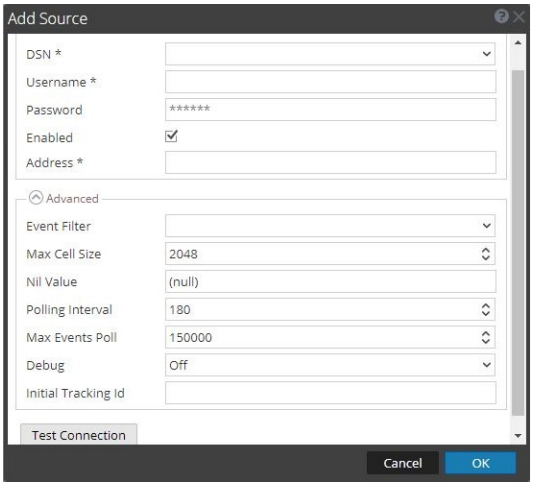


5. Choose the log collector configuration type for your event source type and click **OK**.

From the Available Event Source Types dialog box, select one of the following values:

- To collect McAfee ENS 10.x logs, select **epolicyens10_5autoid**.
- To collect McAfee ENS logs with extended events, select **epolicyens5_9_x**.
- To collect Trellix ENS 10.7.x logs with Epolicy Orchestrator events, select **epolicyens10_7_x**.

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 details on the other parameters, see the "ODBC Event Source Configuration Parameters" topic in the *Log Collection Configuration Guide*, available in NetWitness Community.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.