

RSA NetWitness Logs

Event Source Log Configuration Guide



Lumension Endpoint Management and Security Suite

Last Modified: Friday, March 10, 2017

Event Source Product Information:

Vendor: [Lumension](#)

Event Source: Endpoint Management and Security Suite

Versions: 7.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: lumensionemss

Collection Method: ODBC

Event Source Class.Subclass: Network.Configuration Management

Configure NetWitness Suite for ODBC Collection

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 from RSA NetWitness Suite Live Services.

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 **lumensionemss**.

Configure a DSN

For IBM Tivoli Identity Manager, you can use Oracle or SQL Server:

In both cases, you can follow the procedure below. The procedure differs only for step 8, where you choose the appropriate DSN template.

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.
6. Click **+** to open the **Add DSN** dialog.


Note: If you need to add a DSN template, see [Configure DSNs](#) in the NetWitness User Guide.

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 Lumension Endpoint Management and Security Suite
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Lumension Endpoint Management and Security Suite
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 Event Source Type

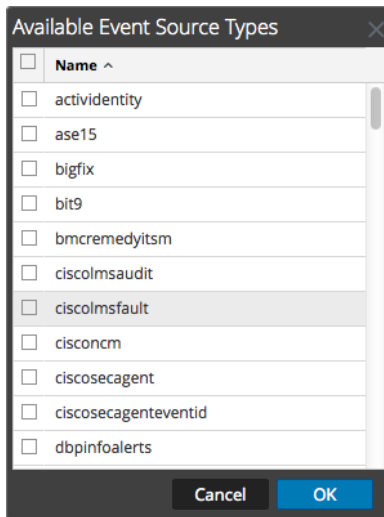
Add the ODBC Event Source Type:

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/Config** from the drop-down menu.

The Event Categories panel is displayed with the existing sources, if any.

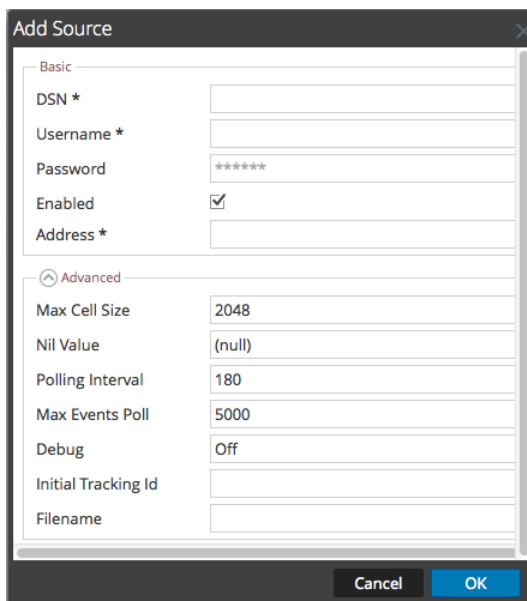
5. Click **+** to open the **Available Event Source Types** dialog.



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

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

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 [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.