

RSA NetWitness Platform

Event Source Log Configuration Guide



CiscoWorks LAN Management Solution

Last Modified: Wednesday, June 19, 2019

Event Source Product Information:

Vendor: [Cisco](#)

Event Source: LAN Management Solution

Versions: 3.2, 4.0

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: ciscolms

Collection Method: ODBC

Event Source Class.Subclass: Network.Configuration Management

Configure CiscoWorks LAN Management Solution

Enable Access to the Database

To enable access to the database, you must complete one of the following tasks:

- Run the **dbaccess.pl** utility on Windows systems, or
- Run the **dbaccess.pl** utility on Solaris systems

Windows Systems

To enable access to the application database from a Windows system, run the following command:

```
NMSROOT\bin\perl NMSROOT\bin\dbaccess.pl {install|clean} [debug]
```

where:

- *NMSROOT* is the default CiscoWorks installation directory,
- **install** is the command line parameter that cleans the existing views, creates new views, and provides access to databases,
- **clean** is the command line parameter that cleans the existing views,
- **debug** prints the debug and warning messages on the screen.

Solaris Systems

To enable access to the application database from a Unix/Linux system, run the following command:

```
NMSROOT/bin/perl NMSROOT/bin/dbaccess.pl {install|clean} [debug]
```

where:

- *NMSROOT* is the default CiscoWorks installation directory,
- **install** is the command line parameter that cleans the existing views, creates new views, and provides access to databases,
- **clean** is the command line parameter that cleans the existing views,
- **debug** prints the debug and warning messages on the screen.

Copy CiscoWorks Files to RSA NetWitness Platform

Before you access the database views from RSA NetWitness Platform, you must copy the following CiscoWorks files to a directory in RSA NetWitness Platform:

- *NMSROOT*\lib\classpath\jconn2.jar
- *NMSROOT*\lib\classpath\jodbc.jar
- *NMSROOT*\objects\db\win32\dbodbc10.dll
- *NMSROOT*\objects\db\win32\dblgen10.dll
- *NMSROOT*\objects\db\win32\dbccon10.dll

where *NMSROOT* is the installation directory for Cisco LMS.

Configure NetWitness Platform for ODBC Collection

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

- I. Ensure the required parser is enabled
- II. Create and Configure a DSN
- III. Add the Event Source Type

For table reference, see [Reference Tables](#) below.

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 **ciscolms**.

Create and Configure a DSN

CiscoWorks LMS uses an embedded database, and in RSA NetWitness Platform, you need to add and configure a DSN for this embedded database.

Create a DSN template:

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  **Manage Templates**.
The **Manage DSN Templates** dialog is displayed.
7. Click **+** to activate the right panel, where you enter the name and parameters for the DSN template.
8. Specify a template name and click **+** on the right panel to add parameters.
 - a. For the Template Name, specify **CiscoWorks Embedded Database**.
 - b. Add the following parameters and values (if no value is listed, leave it blank):

Name	Value
Type	CiscoLMS
Server Name	
Start Line	dbsrv10
Host IP	
DOBROADCAST	NO
ServerPort	43445
Interval	Use Interval
Use Interval	10

9. After you have specified all of the parameters, click **Save** to save your template.
10. Click **Close** to close **Manage DSN Templates** dialog box.

Next, you configure two DSNs using the template you just created.

Configure DSNs (Data Source Names):

1. Click **+** to open the **Add DSN** dialog, and fill in the parameter values as shown below.

Field	Description
DSN Template	Select the Cisco Embedded Database template.
DSN Name	Enter dfmFh
Parameters section	
Type	Enter CiscoLMSFault .
Server Name	Enter dfmFhEng
Start Line	Accept the default value, dbsrv10
Host IP	Enter the IP address of the Cisco LMS event source.
DOBROADCAST	Accept the default value, NO
ServerPort	Accept the default value, 43445
Interval	Accept the default value, Use Interval
Use Interval	The default value is 10 (seconds)

2. Click Save to save this DSN.
3. Click **+** to open another **Add DSN** dialog, and fill in with the following values.

Field	Description
DSN Template	Select the Cisco Embedded Database template.
DSN Name	Enter rmeng
Parameters section	
Type	Enter CISCOLMSAUDIT .
Server Name	Enter rmengEng
Start Line	Accept the default value, dbsrv10
Host IP	Enter the IP address of the Cisco LMS event source.
DOBROADCAST	Accept the default value, NO
ServerPort	Accept the default value, 43445
Interval	Accept the default value, Use Interval


Field	Description
Use Interval	The default value is 10 (seconds)

4. Click Save to save this DSN.

Add the Event Source Type

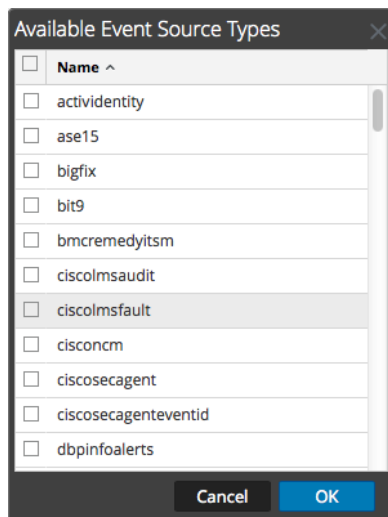
Just as you created two DSNs, you also need to add two event source types. You need to perform the following procedure twice.

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

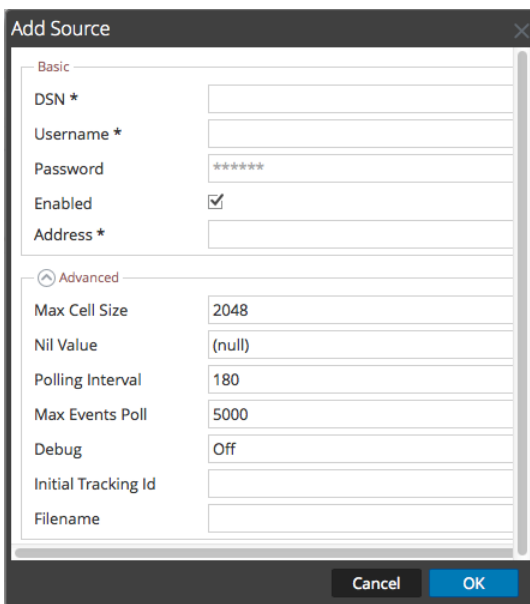
From the **Available Event Source Types** dialog, select one of the following:

- **ciscolmsaudit**: if you select this event source type, select the **rmeng** DSN you created, or
- **ciscolmsfault**: if you select this event source type, select the **dfmFh** DSN you created

The second time through the procedure, select the other event source type and DSN.

Note: The default user name for the embedded Cisco LMS database is **lmsdatafeed**.

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*.

Reference Tables

This event source collects data from the following tables, using the indicated typespec files.

- The **CHANGE_AUDIT_HISTORY** table uses the **ciscolmsaudit.xml** typespec file.
- The following tables use the **ciscolmsfault.xml** typespec file:
 - **FAULT_EVENT_HISTORY**
 - **Fault_Event_Details**

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.