

RSA NetWitness Platform

Event Source Log Configuration Guide



EMC Ionix Unified Infrastructure Manager

Last Modified: Tuesday, August 6, 2019

Event Source Product Information:

Vendor: [EMC](#)

Event Source: EMC Ionix Unified Infrastructure Manager (UIM)

Versions: 1.0, 2.1, 3.0, 3.1

Note: Risk Reporting is only supported for 3.1 Patch 1 and later versions.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: emc-ionix-uim

Collection Method: Syslog, File Risk Reporting only), ODBC

Event Source Class.Subclass: Network.Configuration Management

To configure syslog and ODBC collection in EMC Ionix Unified Infrastructure Manager, complete these tasks:

- For Syslog, [Configure EMC Ionix to send logs to RSA NetWitness Platform](#)
- For ODBC: [Configure ODBC Collection](#)

Note: You must configure both syslog and ODBC collection to collect all types of logs.

To configure Risk Reporting in EMC Ionix Unified Infrastructure Manager, complete one of these tasks:

- [Configure Risk Reporting via Syslog](#), or
- [Configure Risk Reporting via File Collection](#)

Configure EMC Ionix to send logs to RSA NetWitness Platform

If you use EMC Ionix UIM 2.1 or 3.0, you must set up both provisioning and operations features. This section includes steps to configure these two features:

- [Configure EMC Ionix Provisioning](#)
- [Configure EMC Ionix Operations](#)

Configure EMC Ionix Provisioning

To configure EMC Ionix UIM Provisioning:

1. Access the EMC Ionix Unified Infrastructure Manager through a Secure Shell (SSH) connection, and authenticate with the user credentials of Red Hat Enterprise Linux.
2. To modify the firewall to accept a TCP connection on the PostgreSQL port 5435, you must modify the **iptables** file. Depending on your environment, perform exactly one of the following procedures:
 - If you can modify the **iptables** file directly, open `/etc/sysconfig/iptables` for editing, and add the following line:

```
A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5435 -j ACCEPT
```
 - If **iptables** is installed on your server as a command line utility, run the following command:

```
iptables -I INPUT 1 -m state --state NEW -m tcp -p tcp --dport 5435 -j ACCEPT
```
3. To enable client authentication, follow these steps:

a. Locate the **pg_hba.conf** file.

b. Under # IPv4 local connections, type the following line:

```
host all all RSA-IP Net_Mask trust
```

where:

- **RSA-IP** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
- **Net_Mask** is the value of your netmask.

4. To enable a TCP/IP socket between the PostgreSQL database and RSA NetWitness Platform, follow these steps:

a. Locate the **postgresql.conf** file.

b. Replace `listen_addresses='localhost'` with `listen_addresses='*'`

5. To restart the PostgreSQL server, restart RSA NetWitness Platform or open a command prompt and enter the following command:

```
# /etc/init.d/postgresql restart
```

Note: This command varies depending on the location of the **postgresql** file.

6. To create a user account that allows RSA NetWitness Platform to access the PostgreSQL database, follow these steps:

a. Access the PostgreSQL database through a SSH connection.

b. In the command prompt, type:

```
su - pgdba
```

c. In the command prompt, type:

```
psql voyencedb voyence
```

d. In the command prompt, type:

```
CREATE USER username WITH PASSWORD password CREATEUSER;
```

where:

- *username* is the user name of your RSA NetWitness Platform.
- *password* is the password of your RSA NetWitness Platform.

Configure EMC Ionix Operations

To configure EMC Ionix UIM 2.1 and EMC Ionix UIM 3.0 Operations:

1. Log on to the EMC Ionix UIM Operations Web console with administrative credentials.
2. Click the **Administration** tab.
3. Click **Manage Alert Forwarding**.
4. In the Manage Alert Forwarding page, click **Create**.
5. In the Create Configuration window, follow these steps:
 - a. From the **Type** drop-down list, select **Syslog Forwarder**.
 - b. Ensure that **Enable this configuration** is selected.
 - c. In the **Name** field, type a descriptive name for the configuration.
 - d. In the **Hostname** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
 - e. In the **Port** field, type **514**.
 - f. From the **Facility** drop-down list, select **local0**.
 - g. From the **Severity** drop-down list, select **Warning**.
 - h. Ensure that **Forward existing alerts in addition to new alerts** is selected.

-
- i. In the **Heartbeat Interval (minutes)** field, type **5**.
 - j. Click **OK**.

Configure ODBC Collection

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

- I. Ensure the required parser is enabled
- II. 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 **emcionixuim**.

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.
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 the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).

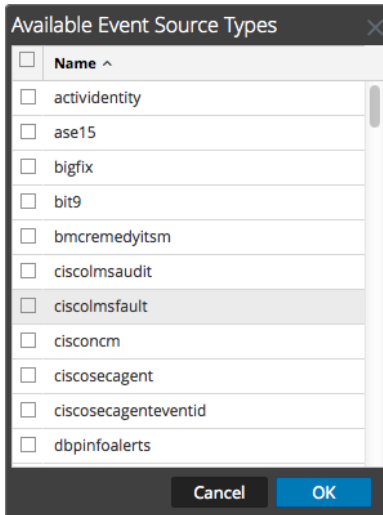
7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

| Field | Description |
|---------------------------|---|
| DSN Template | Choose a PostgreSQL template from the available choices. |
| DSN Name | Enter a descriptive name for the DSN |
| Parameters section | |
| Database | Enter voyencedb for the name of your PostgreSQL database used by the EMC Ionix event source. |
| PortNumber | Enter 5435 for the port number. |
| HostName | Enter the EMC Ionix UIM Provisioning Module IP address. |

Add the Event Source Type

Add the ODBC Event Source Type:

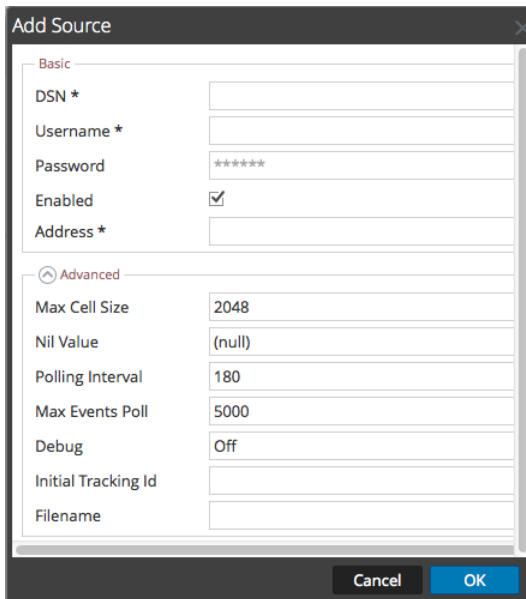
1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.
The Event Categories panel 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 **emcionixuim** 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 the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Configure Risk Reporting via Syslog

To configure syslog for risk reporting:

1. Access the EMC Ionix Unified Infrastructure Manager through a Secure Shell (SSH) connection, and authenticate with administrator credentials.
2. Modify the **Syslog-ng.conf** file located at **/etc/syslog-ng** so that it points to the syslog domain, with port 514, to the RSA NetWitness Log Decoder or Remote Log Collector. For example:

```
destination logserver {udp("RSA_IP_address" port(514)); };  
log { source(src); destination(logserver); };
```

where ***RSA_IP_address*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

3. Restart the syslog services by running the following command:

```
service syslog restart
```

4. Open a command prompt, and run the following as a background command:

```
tail -F /var/log/tomcat6/flex-rest-proxy/flex-rest-proxy-audit.log  
/var/log/tomcat6/cas-server/cas-serveraudit.log | logger &
```

Configure Risk Reporting via File Collection

Set up the SFTP agent, and then configure the RSA NetWitness Log Collector for File collection.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see [Install and Update SFTP Agent](#)
- To set up the SFTP agent on Linux, see [Configure SFTP Shell Script File Transfer](#)

Configure the Log Collector for File Collection

Perform the following steps to configure the Log Collector for File collection.

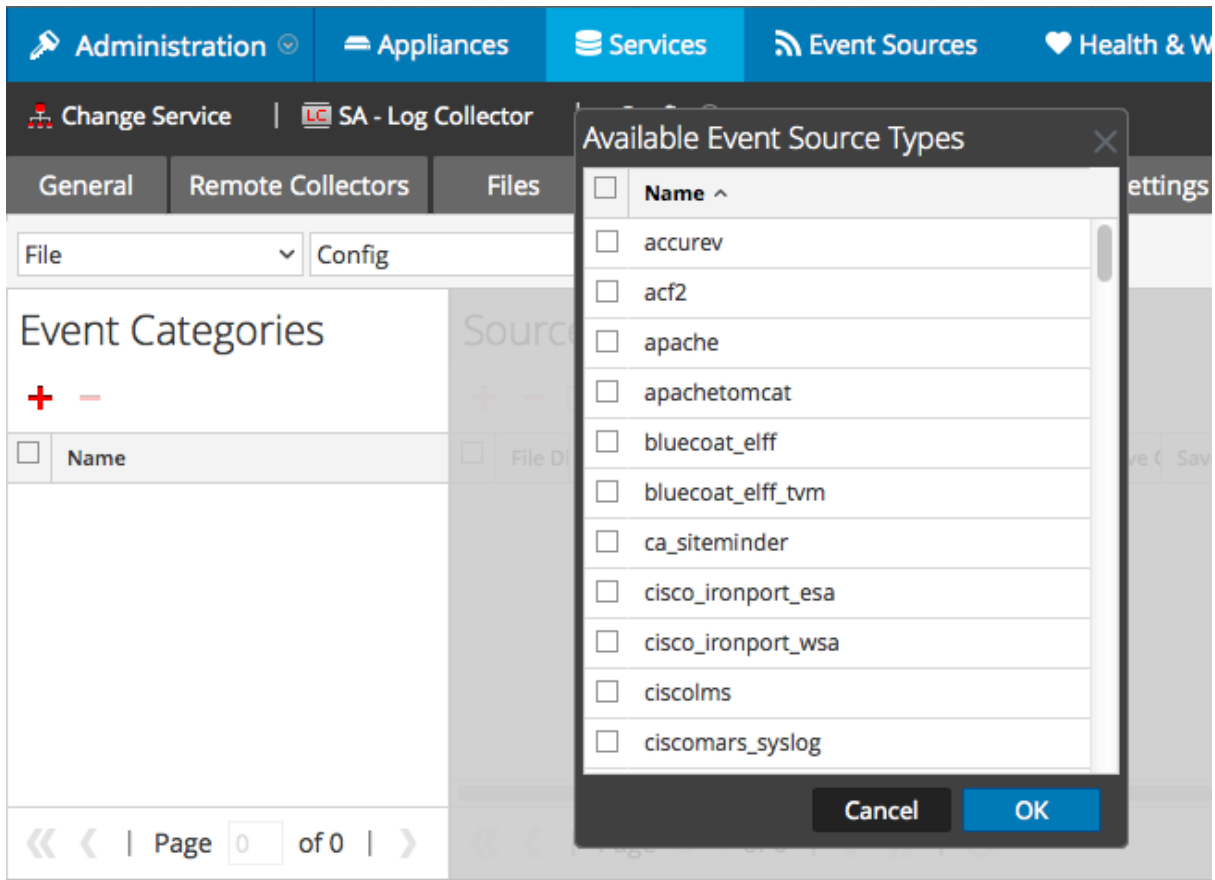
To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **File/Config** from the drop-down menu.

The Event Categories panel displays the File event sources that are configured, if any.

4. In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

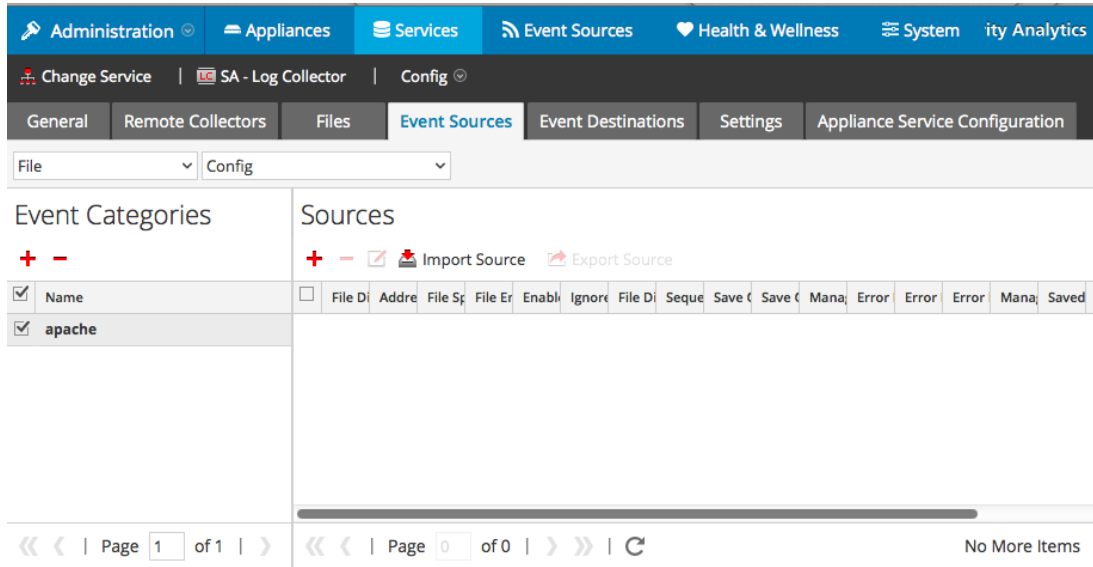


5. Select the correct type from the list, and click **OK**.

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

The newly added event source type is displayed in the Event Categories panel.

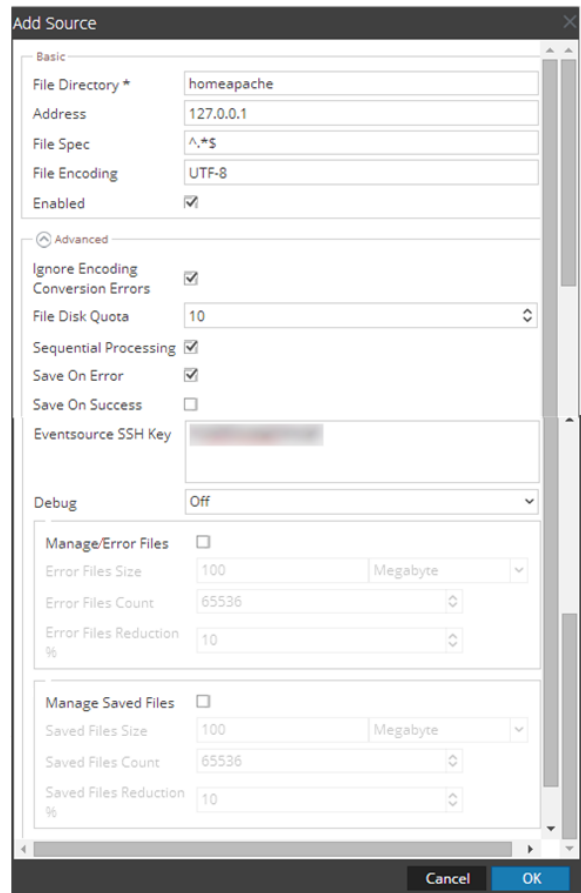
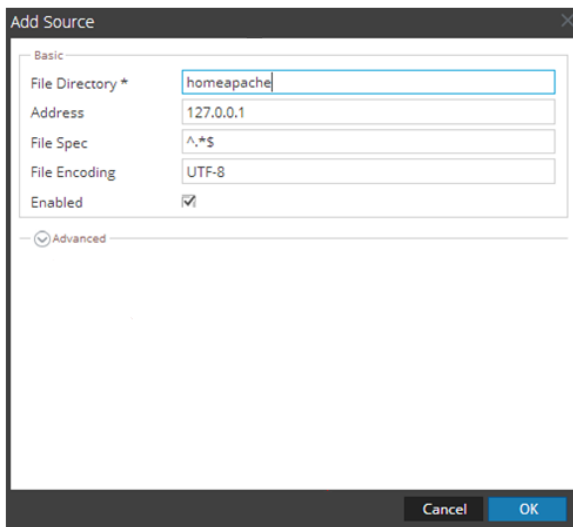
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Reference Tables

This event source collects data from the **voyence.cm_cel_audit_record** table, using the **emcionixuim.xml** typespec file.

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.