

RSA NetWitness Platform

Event Source Log Configuration Guide



Bit9 Security Platform

Last Modified: Tuesday, June 18, 2019

Event Source Product Information:

Vendor: [Bit9](#)

Event Source: Bit9 Security Platform

Versions: 6.0.2, 7.0, 7.2

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: bit9

Collection Method: Syslog, ODBC

Event Source Class.Subclass: Security.Application Firewall

Configure the Bit9 Event Source

To integrate the Bit9 Security Platform with RSA NetWitness Platform, you can choose between Syslog and ODBC collection methods. The ODBC collection method collects logs from the internal database used by the Bit9 Security Platform event source.

Note: The same set of events are collected for Syslog and ODBC. RSA recommends that you configure one or the other collection method, but not both.

To use Syslog collection:

- Configure RSA NetWitness Platform for Syslog Collection
- Configure Bit9 to send Syslog to RSA NetWitness Platform



Or, to use ODBC collection, configure RSA NetWitness Platform for ODBC Collection

Configure RSA NetWitness Platform for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:
 - If you see  **Start Capture**, click the icon to start capturing Syslog.
 - If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

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

The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Configure Bit9 to send Syslog to RSA NetWitness Platform

The following procedure describes how to set up the Syslog collection method for the Bit9 Security Platform event source.

To configure Bit9 Security Platform to send Syslog formatted messages to NetWitness Platform:

1. Log onto the Bit9 Management Console
2. From the left-hand navigation menu, select **System Configuration**.
3. In **Config Options**, select **Server Status**, and click **Edit**.
4. Configure the Syslog Settings below and then select **Save**.

Field	Action
Enable Syslog	Select
Syslog Address	Enter the IP address of the RSA NetWitness Platform Log Decoder or Remote Log Collector.

Field	Action
Syslog Port	Enter 514
Syslog format	Select CEF(Archsight)

Configure RSA NetWitness Platform for ODBC Collection

To configure Bit9 for ODBC Collection on RSA NetWitness Platform, perform the following tasks:

- 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 in RSA NetWitness 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 **bit9**.

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 the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by Bit9
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Bit9
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

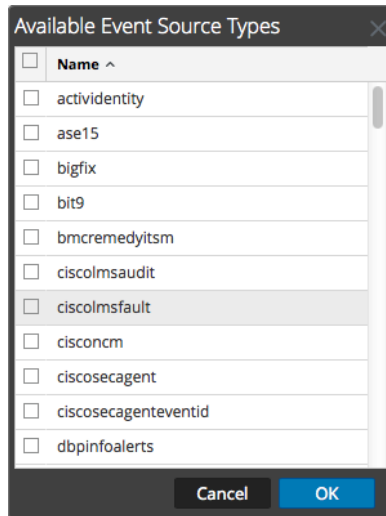
Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **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 box, select one of the following:

- Select **bit9v72** for version 7.2
- Select **bit9** for versions prior to 7.2

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.

The screenshot shows a dialog box titled "Add Source" with a close button (X) in the top right corner. It is divided into two sections: "Basic" and "Advanced".

Basic Section:

- DSN *: [Empty text box]
- Username *: [Empty text box]
- Password: [Text box containing asterisks]
- Enabled:
- Address *: [Empty text box]

Advanced Section:

- Max Cell Size: [Text box containing 2048]
- Nil Value: [Text box containing (null)]
- Polling Interval: [Text box containing 180]
- Max Events Poll: [Text box containing 5000]
- Debug: [Text box containing Off]
- Initial Tracking Id: [Empty text box]
- Filename: [Empty text box]

At the bottom of the dialog are two buttons: "Cancel" and "OK".

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:

- The **ExEvents** table, using the **bit9.xml** typespec file (for Bit9 versions earlier than 7.2)
- The **bit9_public.ExEvents** table, using the **bit9v72.xml** typespec file (for Bit9 versions 7.2 and later)

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.