

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## Enforcive Enterprise Security

Last Modified: Thursday, September 19, 2019

### Event Source Product Information:

**Vendor:** [Synsort](#)

**Event Source:** Enforcive Enterprise Security

**Versions:** 7.x

**Note:** RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

### RSA Product Information:

**Supported On:** NetWitness Platform 10.0 and later

**Event Source Log Parser:** cef

**Collection Method:** Syslog

**Event Source Class.Subclass:** Security.Access Control

To configure the Enforcive event source, you must:

- I. Configure Syslog Output on Enforcive
- II. Configure RSA NetWitness Platform for Syslog Collection

## Configure Syslog Output on Enforcive

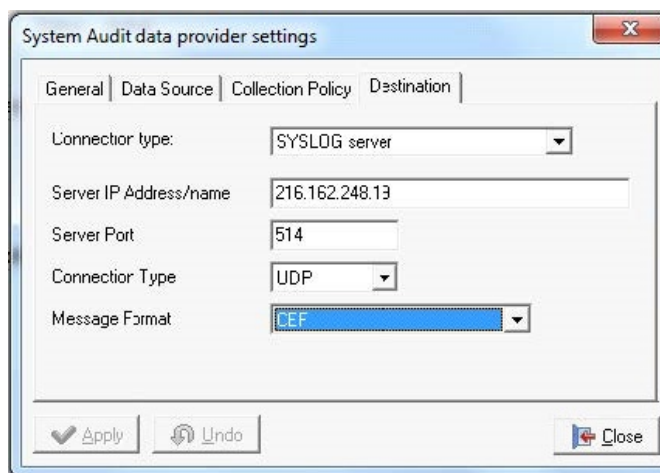
---

Syncsort's Enforcive Enterprise Security Suite is a security and compliance solution for IBM i (an operating system that runs on IBM Power Systems and IBM PureSystems). It contains over 20 integrated, GUI-controlled modules. Enforcive enables system administrators and security officers to manage security and compliance tasks efficiently, as they can use Enforcive to manage multiple systems at once.

- I. Set up Syslog on your system:
  - For IBM i (AS/400) data providers, or
  - For IBM z (Mainframe) Remote Collection Service
- II. Add Multi-system Alerts

**For IBM i (AS/400) data providers, perform the following steps:**

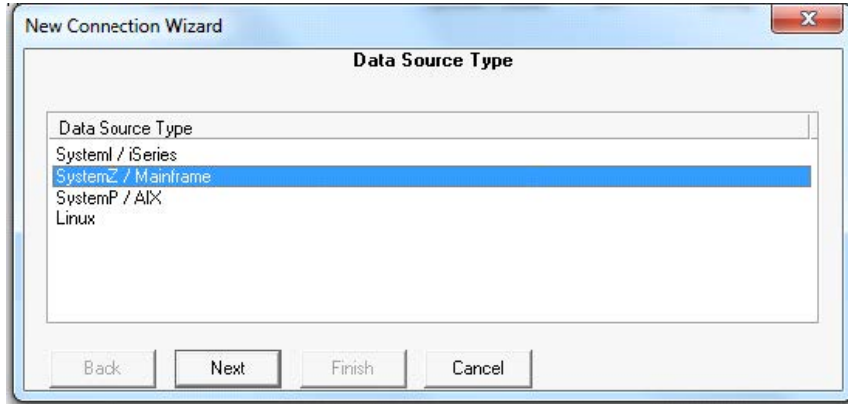
1. Log onto Enforcive Enterprise Security Manager on the IBM i system, then enter the IBM i system Data Providers module.
2. Choose a data provider type and click **Change Settings**.
3. In the **Destination** tab, define the required Syslog server details.



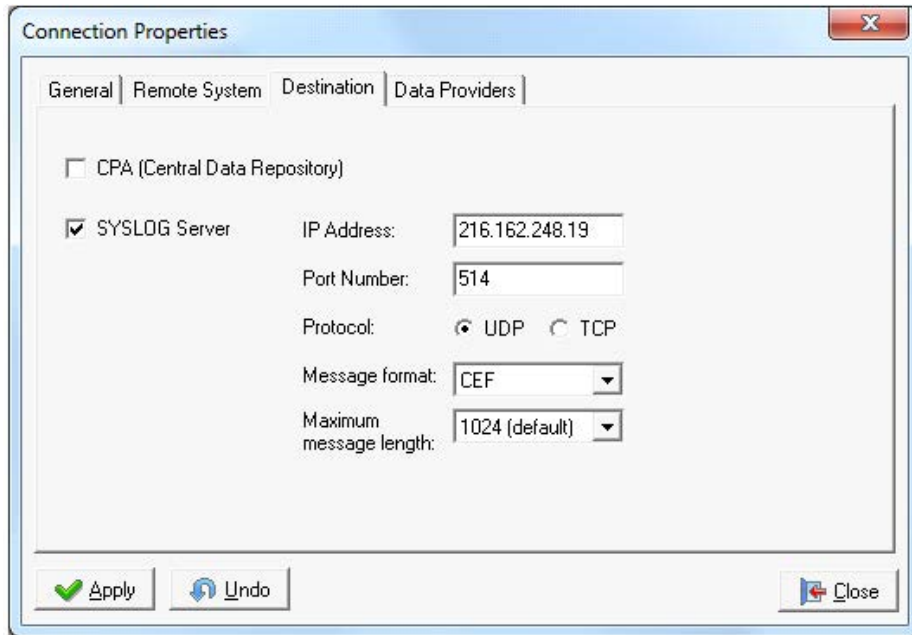
**For IBM z (Mainframe) Remote Collection Service, perform the following steps:**

1. Log onto the Central Management System, then select the **Cross Platform Audit** module.
2. Choose **Remote Collection Service**, then click **Add Connection**.

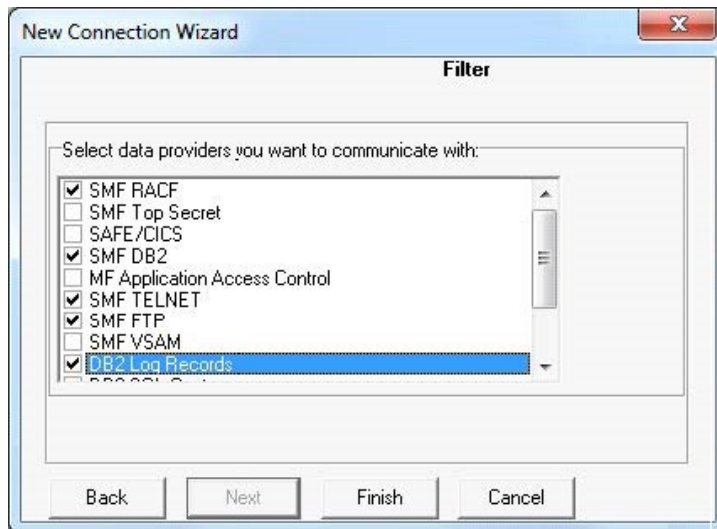
- From the Data Source Type list, choose **SystemZ / Mainframe**, then click **Next** to continue the wizard.



- Choose a specific remote system, then continue the wizard until you get to the **Destination** screen.
- Select the **SYSLOG Server** option, enter the required information, then click **Next**.



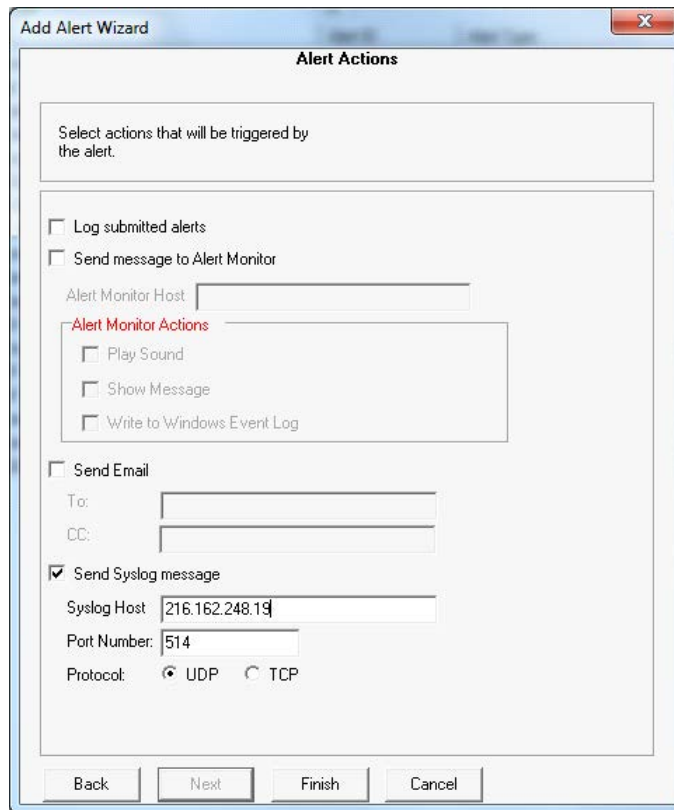
- On the Filter screen, choose one or more of the applications to be sent to your Syslog server.



7. Click **Finish**.

**To add Multi-system Alerts, perform the following steps:**

1. Log onto the Central Management System, then select the **Cross Platform Audit** module.
2. Choose **CPA Alerts** and click **Add Alert**.
3. Choose an alert type and click **Next** to continue the wizard.
4. Choose **Send Syslog message** and fill in the details, as in the example shown below.



5. Click **Finish** to complete the procedure.

## Configure RSA NetWitness Platform

---

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

### 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 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 **cef**.

## Configure 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 **ADMIN > 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 **ADMIN > 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.

After 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.

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](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).