

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## Juniper Networks JUNOS

Last Modified: Thursday, June 20, 2019

### Event Source Product Information:

**Vendor:** [Juniper Networks](#)

**Event Source:** JUNOS Router, Juniper SRX Series

**Versions:** 6.1, JUNOS 9.4, 9.6, 10.0, 10.3, 10.4, 11.1, 11.2, 11.4, 12.x, 17.x

### RSA Product Information:

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

**Event Source Log Parser:** junosrouter

**Collection Method:** Syslog

**Event Source Class.Subclass:** Network.Router

To configure the Juniper JUNOS event source, you must:

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

## Configure Syslog Output on Juniper JUNOS

---

The following procedure describes how to configure Syslog output on your device.

You must perform the following tasks:

- [Configure JUNOS Router](#)
- [Configure Juniper SRX Series \(JUNOS\)](#)

### Configure Juniper JUNOS Router

**To configure Juniper JUNOS Router to send logs to RSA NetWitness Platform:**

To direct system log messages to RSA NetWitness Platform, include the host statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
host (NetWitness Platform hostname/ip address) {
    facility level;
    facility-override facility;
    log-prefix string;
}

source-address source-address;
```

Where *NetWitness Platform hostname/ip address* is the IP address or fully qualified hostname of the RSA NetWitness Platform Log Decoder or Remote Log Collector.

Note the following:

- Each system log message directed to the RSA NetWitness Platform includes the hostname of the local Routing Engine after the timestamp to indicate that it is the source for the message.
- When directing messages to remote machines, you can use the source-address statement to specify the source address to use.

## Configure Juniper SRX Series (JUNOS)

This section describes how to configure Juniper SRX Series for event mode and stream mode.

### Configure Juniper SRX for Event Mode

#### To configure Juniper SRX Series (JUNOS) to send logs to the RSA NetWitness Platform via event mode:

Open a new command line shell, and type:

```
user@host> configure
[edit]
user@host> set system syslog user * any emergency
[edit system]
user@host> set system syslog host NetWitness Platform-IP any any
      Where NetWitness Platform-IP is the IP address of your RSA
      NetWitness Platform.
[edit system]
user@host> set system syslog host NetWitness Platform-IP change-
log none
[edit system]
user@host> set system syslog host NetWitness Platform-IP
interactive-commands none
[edit system]
user@host> commit
```

### Configure Juniper SRX for Stream Mode

#### To configure Juniper SRX Series (JUNOS) to send logs to the RSA NetWitness Platform via stream mode:

Open a new command line shell, and type:

```
user@host> configure
[edit]
user@host> set security log mode stream
[edit]
user@host> set security log format syslog-type
```

Where *syslog-type* is the structure of the logging messages (either **syslog** or **sd-syslog**). For Stream Mode, the Logtype is expected to be **sd-syslog** as the Logs are received from the Data Plane.

[edit]

```
user@host> set security log source-address source-address
```

Where *source-address* is the IP address of the Juniper SRX event source that sends the logs to RSA NetWitness Platform.

[edit]

```
user@host> set security log stream stream-name category logging-category
```

Where:

*stream-name* is the name of the syslog stream.

*logging-category* is the logging category (**content-security**).

[edit]

```
user@host> set security log stream stream-name host NetWitness Platform-IP
```

Where *NetWitness Platform-IP* is the IP address of your RSA NetWitness Platform.

```
user@host> set security log stream stream-name host port 514
```

[edit]

```
user@host> commit
```

## 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 **junosrouter**.



### 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.

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.

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).