

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Check Point IPSO

Last Modified: Tuesday, May 09, 2017

### Event Source Product Information:

**Vendor:** [Check Point](#)

**Event Source:** IPSO (formerly Nokia IPSO)

**Versions:** 3.6, 3.7, 3.8, 3.9, and 6.2

### RSA Product Information:

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

**Event Source Log Parser:** nokiaipso

**Collection Method:** Syslog

**Event Source Class.Subclass:** Host.Unix

To configure Check Point IPSO to communicate with RSA NetWitness Suite, perform the following tasks.

- I. Configure Check Point IPSO
- II. Configure NetWitness Suite for Syslog Collection

## Configure Check Point IPSO

---

Depending on your version of IPSO, complete one of the following tasks:

- Configure Check Point IPSO 6.2, or
- Configure Check Point IPSO 3.8, or
- Configure Check Point IPSO 3.6

### Configure Check Point IPSO 6.2

**To configure Check Point IPSO 6.2 to send logs to RSA NetWitness Suite:**

1. Log on to Network Voyager with your administrator credentials.
2. On the **System** tab, click **System > Configuration > System Configuration > System Logging**.
3. In the System Logging Configuration window, do the following:
  - a. In the **Add a New Remote Log Server** section, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
  - b. In the **System Configuration Audit Log** section, select **Logging of transient and permanent changes**.
  - c. Ensure that **Textual format** and **Voyager Audit Log** are selected.
4. Click **Apply**, and then click **Save**.
5. In the **Remote System Logging** section, in the row containing the IP address of the RSA NetWitness Log Decoder or Remote Log Collector, from the **Log at Severity Level or above** menu, select **Debug**.
6. Click **Apply**, and then click **Save**.

### Configure Nokia IPSO 3.8

**To configure Nokia IPSO 3.8 to work with RSA NetWitness Suite:**

1. Log on to the Nokia Network Voyager via a web browser.
2. Go to **System Configuration > System Logging**.

3. In the **Accept syslog messages from remote machines** field, select either **Yes** or **No**.
4. In the **Add new remote IP address to log to** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
5. Click **Apply**, and click **Save**.

The system displays the IP address you typed in step 4 in the table above the **Add new remote IP address to log to** field.
6. Complete the following procedures to complete the setup for the IP address.
  - a. Verify that the **On** option for the RSA NetWitness Suite IP address is selected.
  - b. Verify that the option **Log at or above severity** for the IP address is set to **Yes**.
  - c. To add or remove severities:
    - To add severities, select an option from the drop-down menu. Click **Apply**, and then click **Save**.
    - To remove severities select **No** next to the severity you want to remove. Click **Apply**, and then click **Save**.
  - d. Under **System Configuration Auditlog**, select **Logging of transient and permanent changes**.
  - e. Under **Voyager AuditLog**, select **Enabled**.
7. Click **Apply**, and then click **Save**.

**Note:** RSA NetWitness Suite supports the logging of all severities.

## Configure Nokia IPSO 3.6

### To configure Nokia IPSO 3.6 to work with RSA NetWitness Suite:

1. Log on to the Nokia Network Voyager via a web browser.
2. Go to **System Configuration > System Logging**.
3. In the **Accept syslog messages from remote machines** field, select either **Yes** or **No**.
4. In the **Add new remote IP address to log to** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

5. Click **Apply**, and click **Save**.

The system displays the IP address you typed in step 4 in the table above the **Add new remote IP address to log to** field.

6. Complete the following procedures to complete the setup for the IP address:
  - a. Verify that the **On** option for the IP address of the RSA NetWitness Log Decoder or Remote Log Collector is selected.
  - b. Verify that the option **Log at or above severity** for the IP address is set to **Yes**.
  - c. Select a severity option from the drop-down menu. Click **Apply**, and then click **Save**.
  - d. To remove a severity, select **No** next to the severity you want to remove. Click **Apply**, and then click **Save**.

**Note:** RSA NetWitness Suite supports the logging of all severities.



- e. Under **System Configuration Auditlog**, select **Logging of transient and permanent changes**.
7. Click **Apply**, and then click **Save**.

## Configure NetWitness Suite 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.

Copyright © 2017 EMC Corporation. All Rights Reserved.

### Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.