

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Imperva SecureSphere

Last Modified: Monday, May 22, 2017

### Event Source Product Information:

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

**Event Source:** SecureSphere

**Versions:** Versions 6, 7, 8, 8.5, 9, 9.5, 10

**Additional Downloads:** Impervawaf.txt

### RSA Product Information:

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

**Event Source Log Parser:** impervawaf

**Collection Method:** Syslog

**Event Source Class.Subclass:** Security.Application Firewall

# Configure Imperva SecureSphere

---

To configure Syslog collection for Imperva SecureSphere you must:

- Configure NetWitness Suite for Syslog Collection
- Configure Syslog Output on Imperva SecureSphere



## 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.


## Configure Syslog Output on Imperva SecureSphere

These instructions describe how to configure Imperva SecureSphere to communicate with the RSA NetWitness Suite.

### To configure Imperva SecureSphere:

1. Connect to the SecureSphere web interface.
2. Select the **Policies > Action Sets** tab.
3. To set up Alerts monitoring, follow these steps:

- a. Select **Create New** .

**Note:** In version 10.0, select **Create New** .

- b. In the **Name** field, type `Security Platform Alerts`.
- c. From the **Apply to event type** drop-down list, select **Any Event Type**.
- d. Click **Create**.
- e. Select the action set, **Security Platform Alerts**.
- f. Move the **Server System Log > Log to System Log (syslog)** action from **Available Action Interfaces** to **Selected Actions** by clicking the green arrow next to the action.
- g. Expand **Selected Actions**, and complete the fields as follows.

Field	Action
Name	Type: <code>Security Platform Alerts</code> .
Syslog Host	Enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
Syslog Host Level	Type: <code>Info</code> .


Field	Action
Message	Copy and paste text from the impervawaf.txt file. Use the line below <b>Security Alerts</b> . This file is available on SCOL as an Additional Download.
Facility	Type: Syslog.


- h. Select **Run on Every Event**.
  - i. Click **Save**.
4. To set up Events, follow these steps:
- a. Select **Create New** .

**Note:** In version 10.0, select **Create New** .

- b. In the **Name** field, type: Security Platform Events.
- c. From the **Apply to event type** drop-down list, select **System Events**.
- d. Click **Create**.
- e. Select the action set, **Security Platform Events**.
- f. Move the **Server System Log > Log to System Log (syslog)** action from **Available Action Interfaces to Selected Actions** by clicking the green arrow next to the action.
- g. Expand **Selected Actions**, and complete the fields as follows.

Field	Value
Name	Type: Security Platform Events.
Syslog Host	Enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
Syslog Host Level	Type: Info.
Message	Copy and paste text from the imperva.txt file. Use the line below <b>Security Events</b> .
Facility	Type: Syslog.

- h. Select **Run on Event Event**.
  - i. Click **Save**.
5. To set up Database Activity Monitoring, follow these steps:
- a. Select **Create New** .

**Note:** In version 10.0, select **Create New** .

- b. In the **Name** field, type: `Security Database Activity Monitoring`
- c. From the **Apply to event type** drop-down list, select **Audit**.
- d. Click **Create**.
- e. Select the action set, **Security Database Activity Monitoring**.
- f. Move the **Gateway Syslog > Log audit events to System Log (Gateway syslog)** action from the **Available Action Interfaces** to the **Selected Actions** by clicking the green arrow next to the action.
- g. Expand **Gateway Syslog > Log audit events to System Log (Gateway syslog)**, and complete the fields as follows.

Field	Value
Name	Type: Security Database Activity Monitoring
Primary Host	Enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
Primary Port	Type: 514
Syslog Host Level	Type: Info
Message	Copy and paste text from the <code>imperva.txt</code> file. Use the line below <b>Security Database Activity Monitoring</b> .
Facility	Type: Syslog

- h. Click **Save**.
6. Click the **Policies > Audit** tab.
7. Select the **External Logger** tab for a particular policy that you want to apply the new action set.

8. Select the name of your newly created action set, **Security Database Activity Monitoring**, and click **Save**.

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.