RSA NetWitness Platform

Event Source Log Configuration Guide

Trend Micro TippingPoint

Last Modified: Monday, August 13, 2018

Event Source Product Information:

Vendor: Trend Micro
Event Source: Security Management System (SMS)
Versions: 2.x, 3.x, 4.x, 5.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: tippingpoint
Collection Method: Syslog
Event Source Class.Subclass: Security.IDS

Configure Trend Micro TippingPoint

To configure Syslog collection for the TippingPoint event source you must:

I. Configure NetWitness Platform for Syslog Collection

II. Configure Syslog Output on TippingPoint

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 **Administration** > **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 **tippingpoint**.

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 **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 Trend Micro TippingPoint

Depending on your version of TippingPoint SMS, configure one of the following versions of Trend Micro TippingPoint Security Management System:

- TippingPoint Security Management System 2.1
- TippingPoint Security Management System 2.5 – 3.1
- TippingPoint Security Management System 3.2 and higher

Configure TippingPoint SMS 2.1

Note: The syslog must come from Trend Micro TippingPoint SMS.

To configure TippingPoint SMS 2.1:

1. Open the **Server Properties – Management** page.
2. In the **System Information** section, do the following:
   a. In the **Name** field, enter the fully qualified host name of the SMS server.
   b. In the **Contact** field, enter the name or e-mail address of the system administrator.
   c. In the **Location** field, enter the location of the server or administrator.
3. In the **Services** section, to disable all services, clear the check boxes.
4. In the **Remote Syslog for Events** section, do the following:
   a. In the **IP Address** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   b. In the **Port** field, type **514**.
   c. Select a **Facility** option.
   d. From the list of delimiters, select **TAB**.
5. Click **Save**.
6. Click **Apply**.

Configure TippingPoint SMS 2.5 – 3.1

Note: The syslog must come from Trend Micro TippingPoint SMS.

To configure TippingPoint SMS 2.5, 2.6, 2.7, 3.0, 3.1:

1. Log on to the TippingPoint SMS Client with administrator credentials.
2. Click **Admin**> **Server Properties**.
3. On the **Management** tab, click **Add**.
4. In the Edit Syslog Notification Setting dialog box, complete the fields as follows.

Field	Action
Syslog Server	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Type **514**.
Log Type	Select **SMS 2.5 Syslog Format**.
Facility	Select **Security/Authorization**.
Severity	Select **Severity in Event**.
Delimiter	Select **SEMI-COLON**.
Include Timestamp in Header	Select **Use original event timestamp**.
Include SMS Hostname in Header	Select **Include SMS Hostname in Header**.
Enable	Ensure that **Enable** is selected.

5. Click **OK**.
6. Click **Apply**.

Configure TippingPoint SMS 3.2 and higher

There are two ways to configure Trend Micro TippingPoint 3.2 and higher:

- Configure TippingPoint SMS to send SMS logs to RSA NetWitness Platform
- Configure the IPS to send logs directly to RSA NetWitness Platform (in addition to the device logs sent by SMS)

Configure TippingPoint SMS 3.2 and higher to send SMS logs

To configure TippingPoint SMS 3.2 and higher:

> **Note:** In addition to adding an entry for SMS 2.5 Syslog Format, you must add entries for SMS Audit, SMS System, Device Audit, and Device System.

1. Log on to the TippingPoint SMS Client with administrator credentials.
2. Click **Admin**> **Server Properties**.
3. Depending on your TippingPoint version, do one of the following:
   - For version 3.2, on the **Management** tab, click **Add**.
   - For version 3.5 and higher, on the **Syslog** tab, click **New**.
4. In the Edit Syslog Notification Setting dialog box, complete the fields as follows.

Field	Action
Syslog Server	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Type **514**.
Log Type	Select **SMS 2.5 Syslog Format**.
Facility	Select **Security/Authorization**.
Event Query	Select **All Events**.
Severity	Select **Severity in Event**.
Delimiter	Select **SEMI-COLON**.

Field	Action
Include Timestamp in Header	Select **Use original event timestamp**.
Include SMS Hostname in Header	Select **Include SMS Hostname in Header**.
Enable	Ensure that **Enable** is selected.

5. Click **OK**.
6. Click **Apply**.
7. Repeat steps 2 through 6 for SMS Audit, SMS System, Device Audit, and Device System logs with the following changes.

Field	Action
Log Type	Select **SMS Audit**, **SMS System**, **Device Audit**, or **Device System**.
Facility	Select **Local Use 0**.

Configure the IPS to send logs directly to RSA NetWitness Platform

Configure the IPS to send logs directly to RSA NetWitness Platform for TippingPoint SMS 3.2:

1. Log on to the TippingPoint SMS Client with administrator credentials.
2. In the **Device** tab, select the IPS device to send logs to RSA NetWitness Platform.
3. Select **Device Configuration**, and click **Edit**.
4. Ensure that **System Log** and **Audit Log** are checked.
5. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector, and click **OK**.
6. From the **Admin** tab, click **Apply** to apply changes and restart the server.

Note: Repeat steps 2 through 6 for each IPS device that you want to log in RSA NetWitness Platform.

Configure the IPS to send logs directly to RSA NetWitness Platform for TippingPoint SMS 3.5 and higher:

1. Log on to the TippingPoint SMS Client with administrator credentials.
2. In the **Device** tab, select the IPS device to send logs to RSA NetWitness Platform.
3. Select **Device Configuration**, and click **Remote Syslog**.
4. Ensure that **System Log** and **Audit Log** are checked.
5. Click **New**.
6. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector, and click **OK**.
7. Select **Semicolon** as the Delimiter and click **OK**.
8. In the Device Configuration window, click **OK** to apply changes.

Note: Repeat steps 2 through 5 for each IPS device that you want to log in that you want to log in RSA NetWitness Platform.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.