RSA NetWitness Platform

Event Source Log Configuration Guide

Trend Micro Deep Security

Last Modified: Monday, May 16, 2022

Event Source Product Information:

Vendor: Trend Micro
Event Source: Deep Security
Versions: 7.0, 7.5, 8.0, 9.x, 10.x, 11.x, 12.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 11.0 and later
Event Source Log Parser: CEF, trendmicrods

Note: The **trendmicrods** parser will be deprecated soon.

Collection Method: Syslog
Event Source Class.Subclass: Security.Application Firewall

To configure the Trend Micro Deep Security event source, you must:

I. Configure Syslog Output on Trend Micro Deep Security

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Trend Micro Deep Security

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

To configure Trend Micro Deep Security:

1. Open a browser and log on to the Trend Micro Deep Security console.
2. In the **Dashboard** menu, click **System** > **System Settings**.

   Note: For version 9.x, 10.x, 11.x, and 12.x in the **Administration** Tab, click **System Settings**.
3. Click the **Notifications** tab.

   Note: For version 9.x, 10.x, 11.x, and 12.x click the **SIEM** tab.
4. In the **System Event Notification (From The Manager)** section, follow these steps:
   a. Ensure that **Forward System Events to a remote computer (via Syslog)** is selected.
   b. Enter the IP address to which events should be sent.
   c. Enter the UDP port to which events should be sent. The default value is **514**.
   d. In the **Syslog Facility** drop-down list, select a syslog facility. The default value is **Local 0**.
   e. In the **Syslog Format** drop-down list, select **Common Event Format**.
   f. Click **Save**.

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**.

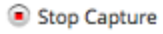
Configure Syslog Collection

Note: Syslog collection must be configured only for the first time when you set up an event source which uses Syslog to send its output to NetWitness.

For Syslog, configure either the Log Decoder or the Remote Log Collector. You do not need to configure both.

Log Decoder Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the **Services** grid, choose 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  , click the icon to start capturing Syslog.
- If you see  , you do not need to do anything; this Log Decoder is already capturing Syslog.

Remote Log Collector Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, go to **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 will appear.
5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Choose the **New Type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog will appear.
7. Enter **514** for the port, and choose **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.

November 2020

Trademarks