

RSA NetWitness Platform

Event Source Log Configuration Guide



Trend Micro Deep Security Agent

Last Modified: Wednesday, July 25, 2018

Event Source Product Information:

Vendor: [Trend Micro](#)

Event Source: Deep Security Agent

Versions: 7.0, 7.5, 9.x, 10.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: trendmicrodsa

Collection Method: Syslog

Event Source Class.Subclass: Security.Application Firewall

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

- I. Configure Syslog Output on Trend Micro Deep Security Agent
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Trend Micro Deep Security Agent

The following procedures describe how to configure Syslog output on your device. Choose the procedure for your version of Trend Micro Deep Security Agent:

- [Configure Trend Micro DSA Version 9.x or 10.x](#)
- [Configure Trend Micro DSA Version 7.0 or 7.5](#)

Configure Trend Micro DSA Version 9.x or 10.x

1. Open a browser and log on to the Trend Micro Deep Security Agent console.
2. In the **Dashboard** menu, click **Computers**.
3. Double-click on the Agent computer to which you want to send logs.
4. In the Agent Computer window, select **Settings** on the left menu.
5. Select the **SIEM** tab.
6. To configure each security module to forward events to RSA NetWitness Platform via syslog see the following modules. For each of the modules, edit the fields as follow:
 - a. Ensure that **Forward Events To:** is selected.
 - b. Ensure that one of the following options is selected:
 - **Relay via the Manager:** If you select this option, the manager forwards all logs to RSA NetWitness Platform.
 - **Direct forward:** If you select this option, all agents will send logs to RSA NetWitness Platform separately.
 - c. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector to which events should be sent.
 - d. Enter the UDP port to which events should be sent. The default value is **514**.

- e. In the **Syslog Facility** drop-down list, select a syslog facility. The default value is **Local 0**.
 - f. In the **Syslog Format** drop-down list, select **Common Event Format**.
 - g. Click **Save**.
7. Follow steps 3,4,5 & 6 for every agent computer that need to forward logs to RSA NetWitness Platform.

Configure Trend Micro DSA Version 7.0 or 7.5

1. Open a browser and log on to the Trend Micro Deep Security Agent console.
2. In the **Dashboard** menu, click **System > System Settings**.
3. Click the **Notifications** tab.
4. You can configure each security module to forward events to the RSA NetWitness Platform via syslog. For each of the modules, edit the fields as follow:
 - a. Ensure that **Forward System Events to a remote computer (via Syslog)** is selected.
 - b. Ensure that one of the following options is selected:
 - **Relay via the Manager:** If you select this option, the manager forwards all logs to RSA NetWitness Platform.
 - **Direct forward:** If you select this option, all agents will send logs to the RSA NetWitness Platform separately.
 - c. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector to which events should be sent.
 - d. Enter the UDP port to which events should be sent. The default value is **514**.
 - e. In the **Syslog Facility** drop-down list, select a syslog facility. The default value is **Local 0**.
 - f. In the **Syslog Format** drop-down list, select **Common Event Format**.
 - g. 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 **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 **trendmicrodsa**.



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.

Copyright © 2018 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.