

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## Trend Micro Deep Discovery Analyzer

Last Modified: Monday, December 21, 2020

### Event Source Product Information:

**Vendor:** [Trend Micro](#)

**Event Source:** Deep Discovery Analyzer Agent

**Versions:** 6.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:** cef

**Collection Method:** Syslog

**Event Source Class.Subclass:** Advanced Threat Detection

# Introduction

---

Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. It can be used to augment or centralize the sandbox analysis of other products. The custom sandboxing environments that can be created within Deep Discovery Analyzer precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives.

The following Deep Discovery Analyzer system logs can be forwarded to syslog servers:

- Virtual Analyzer analysis logs
- Integrated product detection logs
- System events
- Alert events

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

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

## Configure Syslog Output on Trend Micro Deep Discovery Analyzer

---

The below steps will help you configure syslog settings for Trend Micro Deep Analyzer

1. Navigate to Administration > Integrated Products or Services > Syslog.
2. In the System Settings screen click **Add** to add a syslog server.
3. On the screen that appears next, specify the **Status** for the profile.
4. Enter the Profile name and IP address or hostname of the RSA NetWitness Log Decoder or Remote Log Collector.
5. Enter the port number. Default values recommended by Trend Micro are UDP: 514, TCP:601, SSL: 443
6. Select the protocol used for data transport, either UDP or TCP.
7. Select **CEF** as the format in which the logs will be sent to RSA NetWitness
8. Select the scope of logs to send to the syslog server
9. Click **Save**

**Note:** A maximum of 3 syslog servers can be configured to forward logs. Only logs saved after performing and enabling the above settings are forwarded

### Additional Resources and Troubleshooting

For more information refer [Trend Micro-Deep Discovery Analyzer-Syslog Content Mapping Guide for V6.9](#)

**Warning:** The above link is subjected to change

## Configure Syslog Collection on NetWitness Platform

---


Perform the following steps in RSA NetWitness Platform

- Ensure required parser is enabled
- Configure Syslog Collection

### Ensure the Required Parser is Enabled

**Note:** 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:** 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**.

- 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:

- In the NetWitness menu, select **Administration > Services**.
- In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
- Select **Syslog/Config** from the drop-down menu.

The Event Categories panel displays the Syslog event sources that are configured, if any.
- In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.
- Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
- Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.
- 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.

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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November 2020

## Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.