

RSA NetWitness Platform

Event Source Log Configuration Guide



Forcepoint Email Security

Last Modified: Friday, September 27, 2019

Event Source Product Information:

Vendor: [Forcepoint](#)

Event Source: Forcepoint Email Security

Version: 8.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: Security.Antivirus

To configure the Forcepoint Email Security event source, you must:

- I. Configure Syslog Output on Forcepoint Email Security
- II. Configure RSA NetWitness Platform for Syslog Collection

Forcepoint Email Security

Forcepoint Email Security provides protection for email systems to prevent malicious threats from entering an organization's network. This email solution provides on-premises email security hosted on a Forcepoint appliance.

The following email protection system logs can send data to a SIEM server:

- Connection
- Message
- Policy
- Delivery
- Hybrid

Configure Forcepoint Email Security

To configure Forcepoint Email Security to send Syslog:

1. Navigate to **Settings > General > SIEM Integration** in the Forcepoint Security Manager Email Security module.
2. Select **Enable SIEM integration** to activate SIEM integration functions.
3. Enter the IP address or hostname of the RSA NetWitness Log Decoder or Remote Log Collector in the IP address or hostname entry field.
4. Enter the port number for the **SIEM integration server** in the **Port** field. Default is 514.
5. Select the protocol used for data transport: either UDP or TCP.

For more details and troubleshooting information, see https://www.websense.com/content/support/library/email/v84/email_siem/siem_log_map.pdf. Note that this link is subject to change.

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: 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 **ADMIN > 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 **ADMIN > 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.

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.

Copyright © 2019 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.