RSA NetWitness Platform

Event Source Log Configuration Guide

FireEye Web MPS

Last Modified: Tuesday, June 4, 2019

Event Source Product Information:

Vendor: FireEye
Event Source: Web Malware Protection System (MPS)
Versions: 6.x, 7.x, 8.x

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: fireeyewebmps
Collection Method: Syslog
Event Source Class.Subclass: Antivirus.Malware

To configure the FireEye Web MPS event source, you must:

I. Configure Syslog Output on FireEye Web MPS

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on FireEye Web MPS

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

To configure the FireEye Web MPS to send LEEF formatted syslog messages to RSA NetWitness:

1. Log on to the FireEye Web console.
2. On the main navigation bar, click **Settings > Notifications**.
3. Ensure that the **rsyslog** box is checked for the **Event Type** row to enable collection of all five event types.
4. Click the **rsyslog** link at the head of the table. In the Settings window, complete the following fields:

Field	Action
Default format	Select **LEEF**.
Default delivery	Select **Per Event**.
Default send as	Select **Critical**.

5. Click **Apply Settings**.
6. Navigate to the **Rsyslog Server Listing** section below the Settings table.
   a. Enter a name for the device.
   b. Click **Add Rsyslog Server**.
7. Ensure that the following information is entered alongside the RSA NetWitness Platform:

Field	Action
Enabled	Select the box to enable RSA NetWitness Platform
IP Address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Delivery	Select **Default** .

Field	Action
Notification	Select **All Events**.
Format	Select **Default**.
Send As	Select **Default**.
Protocol	Select **UDP**.

8. Click **Update**.

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.

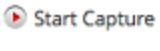
Note: The required parser is **fireeyewebmps**.

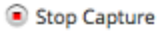
Configure RSA NetWitness Platform for Syslog Collection

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 

, click the icon to start capturing Syslog.
   - If you see 

, 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.

Trademarks

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