NetWitness® Platform XDR

FireEye Web Malware Protection System Event Source Log Configuration Guide

NETWITNESS
Platform XDR

FireEye Web MPS

Event Source Product Information:

Vendor: FireEye

Event Source: Web Malware Protection System (MPS)

Versions: 6.x, 7.x, 8.x, 9.x

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.5 and higher

Event Source Log Parser: fireeyewebmps

Collection Method: Syslog

Event Source Class.Subclass: Antivirus.Malware

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

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.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

November, 2022

Contents

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

1. Configure Syslog Output on FireEye Web MPS.

2. Configure NetWitness Platform XDR 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 NetWitness Platform XDR:

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 NetWitness Platform XDR:

Field	Action
Enabled	Select the box to enable [[[Undefined variable SAVariables.ProductSuiteName]]]
IP Address	Enter the IP address of the [[[Undefined variable SAVariables.ProductName]]] Log Decoder or Remote Log Collector.
Delivery	Select **Default** .
Notification	Select **All Events**.
Format	Select **Default**.
Send As	Select **Default**.
Protocol	Select **UDP**.

8. Click **Update**.

Configure NetWitness Platform XDR

Perform the following steps in NetWitness Platform XDR:

- 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 NetWitness Platform XDR Live.

Ensure that the parser for your event source is available:

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 NetWitness Platform XDR for 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 ⊙ 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.

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.

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here:
  https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.

- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.

- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.

- See Troubleshooting section in the guides.

- See also NetWitness® Platform Blog Posts.

- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.

- Logs information, even source version, and collection method.

- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.