NetWitness® Platform

Fortinet Forticlient Endpoint Security Event Source Configuration Guide

Fortinet Forticlient Endpoint Security

Last Modified: Wednesday, March 25, 2026

Event Source Product Information:

Vendor: Fortinet

Event Source: Forticlient Endpoint Security

Versions: 4.x, 7.x

RSA Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Log Parser: forticlientendpoint

Collection Method: Syslog

Event Source Class.Subclass: Security.Firewall

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

License Agreement

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

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

Miscellaneous

January, 2026

Contents

Configure Syslog Output on Fortinet Forticlient **6**
Configure NetWitness Platform **7**
Ensure the Required Parser is Enabled 7
Configure Syslog Collection 7

To configure the Fortinet Forticlient event source, you must:

I. Configure Syslog Output on Fortinet Forticlient

II. Configure NetWitness Platform for Syslog Collection

Configure Syslog Output on Fortinet Forticlient

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

To configure Fortinet Forticlient Endpoint Security to send Syslog messages to NetWitness Platform:

1. Open the Fortinet Forticlient Endpoint Security console.
2. Click **General > Log Settings**.
3. In the **Event Log Settings** section, from the drop-down list select **Warning**.
4. In the **What to log** section, select **All events**.
5. In the **Remote Logging** section, ensure that **Server** is selected, and enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
6. From the **Facilities** drop-down list, select **log audit**.
7. Ensure that **Syslog** is selected.
8. From the **Syslog** level drop-down list, select **Warning**.
9. Click **Apply**.

Configure NetWitness Platform

Perform the following steps in 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 NetWitness Platform 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 **forticlientendpoint**.

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 only need to configure either the Log Decoder or the Remote Log Collector for Syslog, not both.

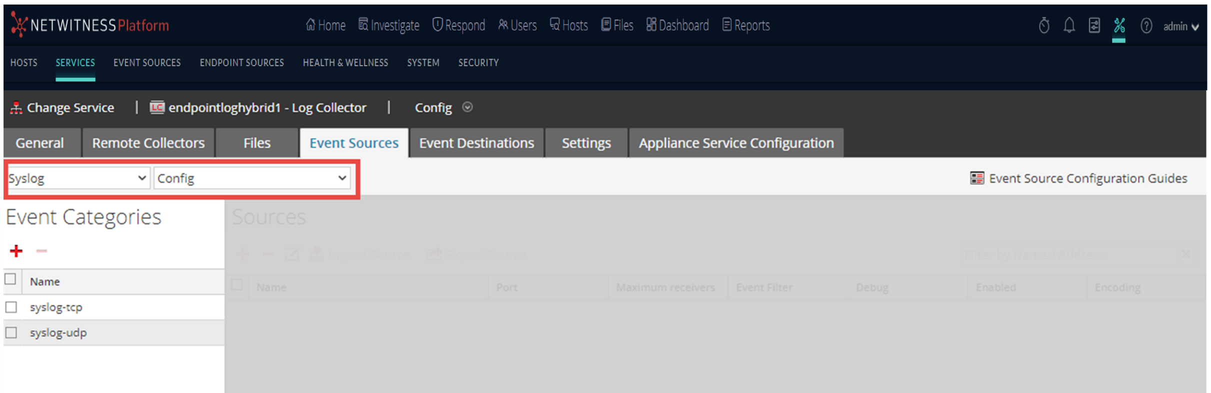
To configure Log Decoder for Syslog Collection

1. In the NetWitness Platform menu, select (Admin) > **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.

To configure Remote Log Collector for Syslog Collection

1. In the NetWitness Platform menu, go to (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.

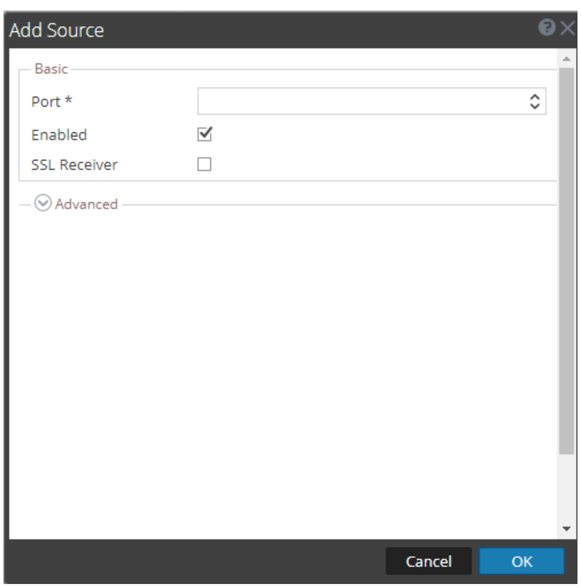
   The **Event Categories** panel displays the Syslog event sources that are configured, if any.



4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog 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. You can continue to add Syslog event sources to your system without a need to do any further configuration in NetWitness Platform.