Tripwire Enterprise

Last Modified: Monday, November 10, 2025

Event Source Product Information:

Vendor: Tripwire

Event Source: Tripwire Enterprise

Versions: 5.4, 5.5, 7.x, 8.x

Note: NetWitness supports the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case in the NetWitness Community Portal for support.

Supported Platforms: Microsoft Windows and Linux

Additional Downloads: sftpagent.conf.tripwire

RSA Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Log Parser: tripwire, cef

Collection Method: File, Syslog

Note: Syslog collection only supported on version 8.x.

Event Source Class.Subclass: Network.Configuration Management

NetWitness Platform supports Tripwire Enterprise running on Microsoft Windows or Linux platforms. Additionally, RSA enVision supports collection via File Collection and Syslog (versions 8.0 and later).

- To collect audit messages, NetWitness recommends that you set up Syslog collection.
- Configure File Collection to collect configuration-change related messages.

There are several tasks to set up Tripwire Enterprise:

I. Configure Tripwire

II. Set Up File Collection

III. Configure Syslog Collection (version 8.x only)

Configure Tripwire

To log detailed data from Tripwire you must configure an execute action and enable the action on each rule. This action creates a copy of the XML output from a scan to be picked up and processed by the File Service in NetWitness Platform.

To configure Tripwire Enterprise to work with NetWitness Platform:

1. In Tripwire Enterprise, configure a new Tripwire action as follows:

   a. Use the web interface to select **Actions > New Action > Execute Action**.

   b. Complete the fields as follows:

Field	Value
Name	NetWitness
Description	Use to archive for NetWitness

Command line (on Windows platforms)	**%SystemRoot%\system32\cmd.exe /c copy "%f" "%f.nic"**
	Replace SystemRoot with the system root for your Tripwire server. For example:
	`C:\WINDOWS\system32\cmd.exe /c copy "%f" "%f.nic"`
	Note: If the above command does not work, enter the last part of the command only:
	`copy "%f" "%f.nic"`

Command line (on Linux platforms)	`cp "%f" "%f.nic"`

   c. Click **Finish**.

2. In Tripwire Enterprise, click on the Rules tab to access the Rules groups. Modify each rule to enable the NetWitness Platform action you created in step **1.**

3. Set up File Collection

Set up File Collection

Perform the following steps to configure File Collection:

- Configure the Log Collector for File Collection
- Set up the SFTP Agent

Configure the Log Collector for File Collection

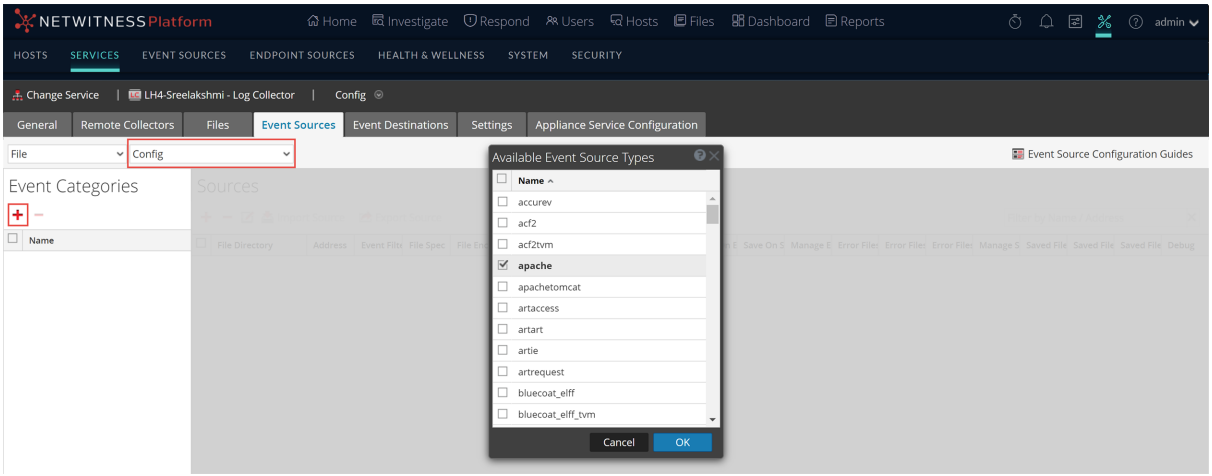
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select (Admin) > **Services**.
2. In the **Services** grid, select a Log Collector, and from the **Actions** ( ) menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

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

   The **Available Event Source Types** dialog is displayed.

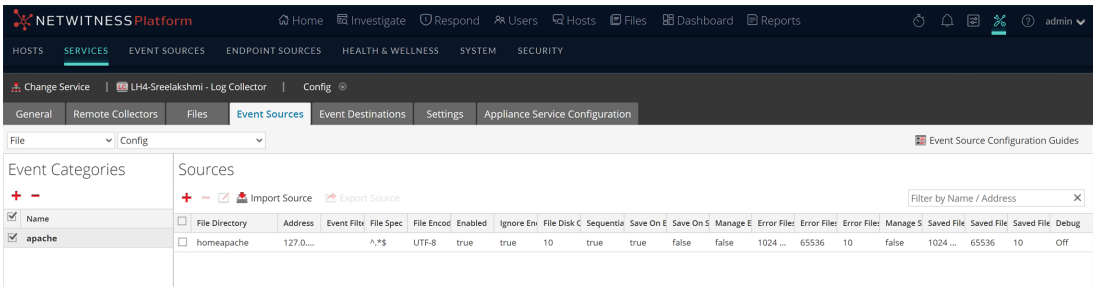


5. Select the correct type from the list and click **OK**.

   Select **tripwire** from the **Available Event Source Types** dialog.

   The newly added event source type is displayed in the Event Categories panel.

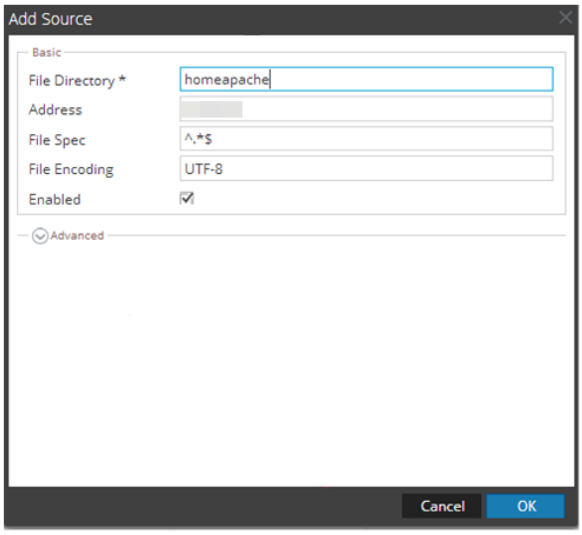
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

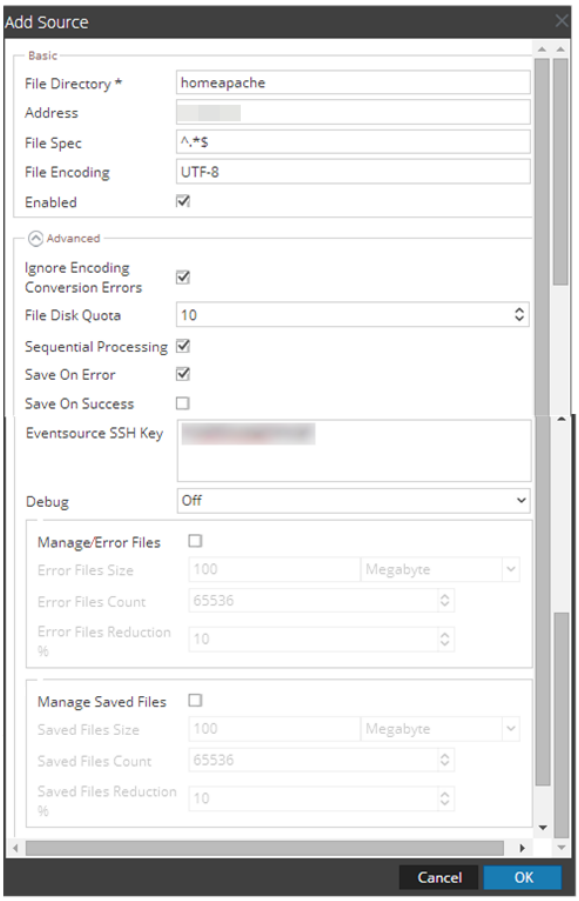


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The **Add Source** dialog is displayed.

> **Note:** Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.





7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from NetWitness Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SFTP Shell Script File Transfer

To set up the SFTP Agent for NetWitness Platform, follow these instructions:

Configure Syslog Collection (version 8.x only)

To set up Syslog collection:

I. Configure the Tripwire Enterprise Syslog Collection Service

II. Ensure the Required Parser is Enabled in NetWitness Platform

III. Configure NetWitness Platform for Syslog Collection

Configure the Tripwire Enterprise Syslog Collection Service

For Tripwire version 8.x, you can collect audit messages through Syslog. To collect configuration-change related messages please configure File Collection.

To configure the Syslog Collection Service:

1. In Tripwire Enterprise, click **Settings** from the top navigation bar.
2. From the left-hand menu, expand **System** > **Log Management**.
3. Check the **Forward TE log messages** to syslog box.
4. For **TCP Host**, enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
5. For **TCP Port**, enter **514**.
6. Click **Apply**.

Ensure the Required Parser is Enabled in NetWitness Platform

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 **tripwire**. If incoming log type is configured for CEF format, enable cef parser.

Configure NetWitness Platform for Syslog Collection

If you are configuring the Remote Log Collector for syslog, select **syslog-tcp** in step 5 below. The Tripwire event source sends Syslog over TCP only.

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.

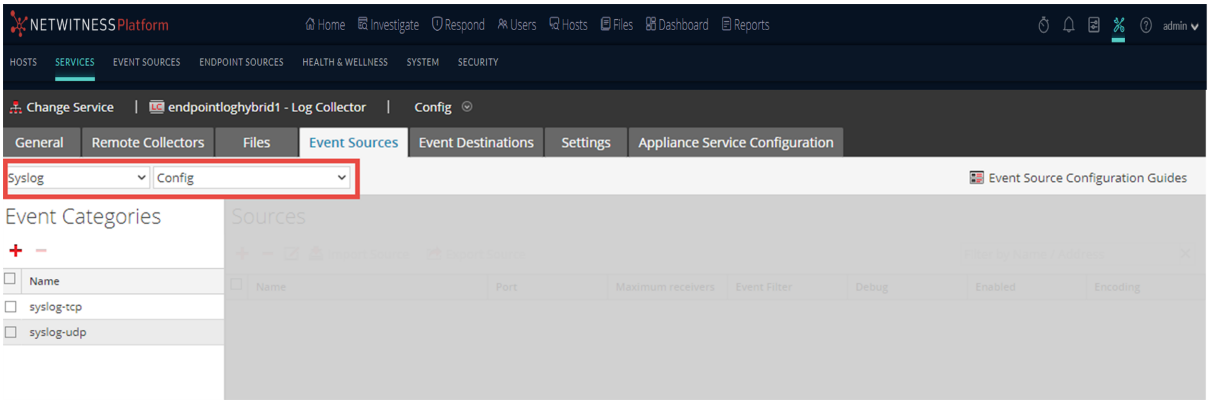
To configure Log Decoder for Syslog Collection

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.

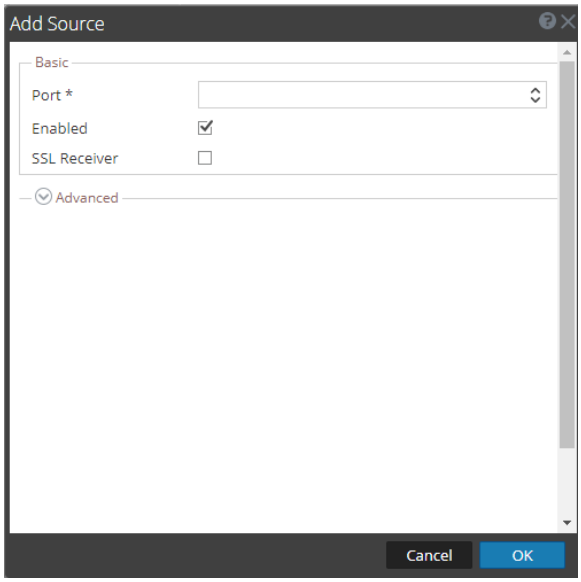


4. In the **Event Categories** panel toolbar, click +.

   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.

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.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November 2024