

NetWitness[®] Platform XDR

Fortinet Manager / FortiAnalyzer Event Source Log Configuration Guide

Fortinet Manager / FortiAnalyzer

Event Source Product Information:

Vendor: [Fortinet](#)

Event Source: Fortinet Manager and Fortinet FortiAnalyzer

Versions: 5.x, 6.x, 7.x

Note: NetWitness 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.

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.5 or later

Note: Fortinet Manager and Fortinet FortiAnalyzer are supported from NetWitness Platform XDR 11.5. However, NetWitness recommends you to update NetWitness Platform XDR to the latest version.

Event Source Log Parser: fortinetmgr

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

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 and 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/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

September, 2022

Contents

Configure Syslog Output on Fortinet Manager or FortiAnalyzer	6
Configure NetWitness Platform XDR for Syslog Collection	8
Ensure the Required Parser is Enabled	8
Configure Syslog Collection	8
Getting Help with NetWitness Platform XDR	11
Self-Help Resources	11
Contact NetWitness Support	11
Feedback on Product Documentation	12

To configure the Fortinet Manager or FortiAnalyzer event source, you must:

- [Configure Syslog Output on Fortinet Manager or FortiAnalyzer](#)
- [Configure NetWitness Platform XDR for Syslog Collection](#)

Configure Syslog Output on Fortinet Manager or FortiAnalyzer

To configure Fortinet Manager or FortiAnalyzer 5.x or 6.x to send logs to NetWitness Platform XDR:

1. Open the command line interface and enter the Fortinet Manager credentials.
2. Enter the following string:

```
config system locallog syslogd setting
```
3. Set server to the IP address of the NetWitness Log Decoder or Remote Log Collector:

```
set server "LD/RLC IP address"
```

where **LD/RLC IP address** is the IP address of the NetWitness Log Decoder or Remote Log Collector.
4. Set severity to either **warning** or **information**:

```
set severity warning  
set severity information
```

Note: Set the severity to **warning** to receive warning messages. Informational messages are also supported.

5. Set status to **enable**:

```
set status enable
```
6. End the command line process:

```
end
```

To configure Fortinet Manager or FortiAnalyzer 7.x to send logs to NetWitness Platform XDR:

1. Open the command line interface and enter the Fortinet Manager credentials.
2. Enter the following string:

```
config system syslog
```
3. Provide syslog server name.

```
edit "name" where name is syslog server name.
```
4. Set the the IP address of the NetWitness Log Decoder or Remote Log Collector.

```
set ip "LD/RLC IP address" where LD/RLC IP address is the IP address of the NetWitness Log Decoder or Remote Log Collector.
```
5. Set the syslog server port (default is 514).

```
set port 514
```
6. End the command line process.

```
end
```

7. Enter the following string.

```
config system locallog syslogd setting
```

8. Set syslog server name.

```
set syslog-name "name" where name is syslog server name that you have set at step 3, To configure Fortinet Manager or FortiAnalyzer 7.x to send logs to NetWitness Platform XDR:.
```

9. Set severity to either **warning** or **information**:

```
set severity warning  
set severity information
```

Note: Set the severity to **warning** to receive warning messages. Informational messages are also supported.

10. Set status to **enable**:

```
set status enable
```

11. End the command line process:

```
end
```

Configure NetWitness Platform XDR for Syslog Collection



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 **fortinetmgr**.



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 Log Decoder for Syslog Collection

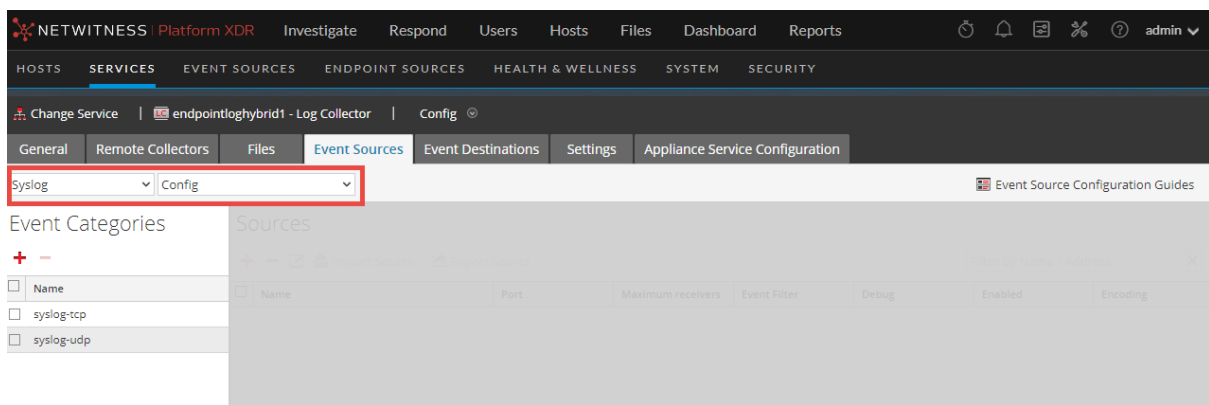
1. In the NetWitness Platform XDR menu, select  (Admin) > **Services**.
2. In the **Services** grid, choose a Log Decoder and from the **Actions** () menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:

- 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

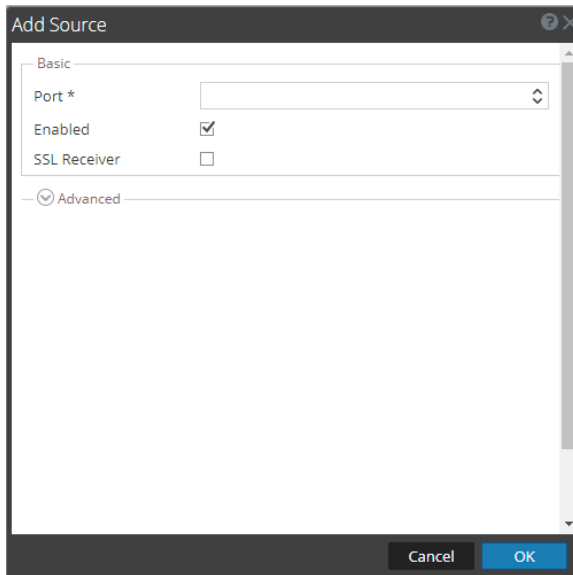
1. In the NetWitness Platform XDR menu, go to  (Admin) > **Services**.
2. In the **Services** grid, select a Remote Log Collector and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog** / **Config** from the drop-down menu.

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 XDR.

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 the documentation for Logstash JDBC input plugin here: <https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- 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.