

# NetWitness<sup>®</sup> Platform

## Cyber Ark Event Source Log Configuration Guide

## 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/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

November 2024

# Cyber-Ark

Last Modified: Tuesday, September 9, 2025

## Event Source Product Information:

**Vendor:** [Cyber-Ark](#)

### Event Source:

- Privileged Identity Management Suite: versions 7.x, 9.x, 10.x, 12.1
- Privileged Account Security Solution: versions 8.x and 9.x

**Versions:** 7.x, 8.x, 9.x, 10.x, 12.1

**Additional Downloads:** [SecurityAnalytics.xsl](#), [RFC5424Changes.xsl](#)

## RSA Product Information:

**Supported On:** NetWitness Platform 12.3 and later

**Event Source Log Parser:** cyberark

**Collection Method:** Syslog

**Event Source Class.Subclass:** Security.Access Control

To configure Syslog collection for the Cyber-Ark event source, you must:

- I. Configure Syslog Output on Cyber-Ark
- II. Configure RSA NetWitness Platform for Syslog Collection

## Configure Syslog Output on Cyber-Ark

### To configure Cyber-Ark:

1. Navigate to the Cyber-Ark Suite additional downloads space on the NetWitness Community: <https://community.netwitness.com/s/article/Cyber-ArkPrivilegedAccountSecuritySolutionandPrivilegedIdentityManagementSuite-RSANetWitnessParserSourcePackage>.
2. Download the **CyberArk.zip** archive, and extract **SecurityAnalytics.xml** and **RFC5424Changes.xml**.
3. Save the files to the Cyber-Ark installation folder: `/Server/Syslog`.

**Note:** The contents of **RFC5424Changes.xml** get imported into **SecurityAnalytics.xml**.

4. Log on to the Cyber-Ark appliance with administrator credentials.
5. Open the Cyber-Ark installation folder.
6. In the **dbparm.ini** file, ensure that the following parameters are set:

| Field                   | Action   |
|-------------------------|--|
| SyslogServerIP          | Enter the IP address of the NetWitness Log Decoder or Remote Log Collector.  |
| Server Port             | Type <b>514</b> .  |
| SyslogMessageCodeFilter | This field designates the messages that are sent from the Vault to NetWitness Platform through the Syslog protocol. You can accept the default (all message codes are sent for users and secure activities), or select individual IDs.<br><br>To specify individual IPs, use commas to separate individual messages or ranges of messages. For example,<br><code>SyslogMessageCodeFilter=1,2,5-10</code> . |
| SyslogTranslatorFile    | Enter <code>Syslog\SecurityAnalytics.xml</code><br><br>This is the location of the translator file used to generate logs in syslog format and send to NetWitness Platform.   |
| UseLegacySyslogFormat   | Enter <b>No</b> .  |
| SyslogServerProtocol    | Select <b>UDP</b> or <b>TCP</b> .  |

7. Restart the Cyber-Ark service:
  - a. From the desktop of the Vault Server, click the PrivateArk Server icon.  
The Server Central Administrator launches
  - b. Click **Stop/Start** to restart the Cyber-Ark service.

**Note:** On selecting TCP, if you are unable to receive the logs properly, update the **SecurityAnalytics.xsl** file with `<xsl:text>&#xa;</xsl:text>` in between `</xsl:foreach>` and `</xsl:template>`. For more information, see <https://cyberark-customers.force.com/s/article/00004289>.

## Configure NetWitness Platform for Syslog Collection



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 RSA 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 **cyberark**.



### 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.

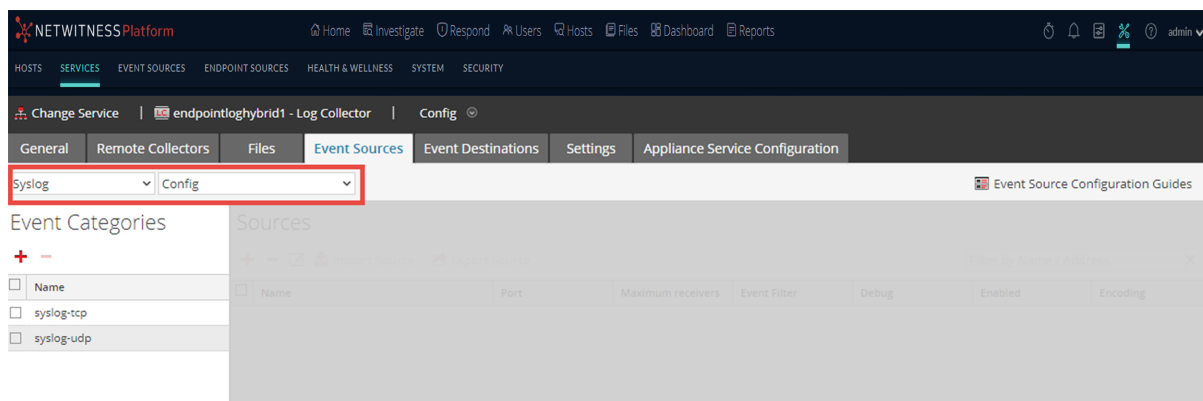
**To configure Log Decoder for Syslog Collection**

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

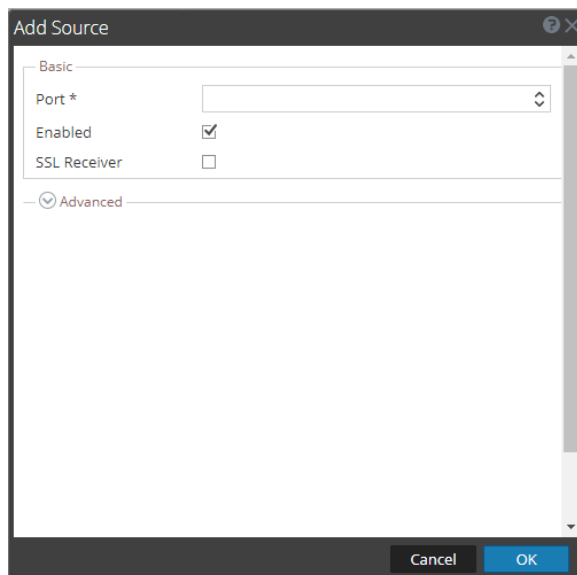
1. In the NetWitness Platform menu, go to  (Admin) > **Services**.
2. In the **Services** grid, select a Remote Log Collector and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog / Config** from the drop-down menu.

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.