# NetWitness® Platform

## Palo Alto Prisma Access Event Source Log Configuration Guide

NETWITNESS

Platform

# Palo Alto Prisma Access

**Event Source Product Information:**

**Vendor**: Palo Alto
**Event Source**: Prisma Access
**Versions**: Prisma Access 2.1 Schema Logs

**NetWitness Product Information:**

**Supported On**: NetWitness Platform 12.2 and higher
**Event Source Log Parser**: paloaltonetworks
**Collection Method**: Syslog
**Event Source Class.Subclass**: Cloud

## 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, 2023

# Contents

# Introduction to Prisma Access

Prisma Access helps you deliver consistent security to your remote networks and mobile users. All your users—at headquarters, office branches, and on the road—connect to Prisma Access to safely use the internet and cloud and data center applications. You get protection at scale with global coverage, so you don't have to worry about things like sizing and deploying firewalls at your branches, or building out and managing appliances in collocation facilities.

With Prisma Access, Palo Alto Networks deploys and manages the security infrastructure globally to secure your remote networks and mobile users. Prisma Access logs directly to Cortex Data Lake. All Prisma Access logs are stored in the Cortex Data Lake, providing centralized analysis, reporting, and forensics across all users, applications, and locations.

Palo Alto Networks Cortex Data Lake provides cloud-based, centralized log storage and aggregation for your on-premise, virtual (private cloud and public cloud) firewalls and for Prisma Access.

Cortex Data Lake is secure, resilient, and fault-tolerant, and it ensures your logging data is up-to-date and available when you need it.

To meet your long-term storage, reporting and monitoring, or legal and compliance needs, you can configure Cortex Data Lake to forward all logs or a subset of logs to our Netwitness syslog receiver.

## Supported Log Types

We support the collection of various log types from the Cortex Datalake, such as Traffic, Authentication, System, Config, GlobalProtect, HIP Match, File, etc.

# Forward Logs from Cortex Data Lake to a Syslog Server

Configure the Cortex Data Lake to forward logs to syslog receiver at Newitness, see Forward Logs from Cortex Data Lake to a Syslog Server.

> **Note:** For any inquiries regarding the configuration process on Cortex Data Lake, please contact Palo Alto Networks support.

During the configuration of your Cortex Data Lake instance, it is essential to ensure that below parameter details are entered accurately.

- Syslog Server - Enter the IP address or hostname of the NetWitness Log Decoder or Remote Log Collector.
- Log Format - LEEF (Tab delimiter).
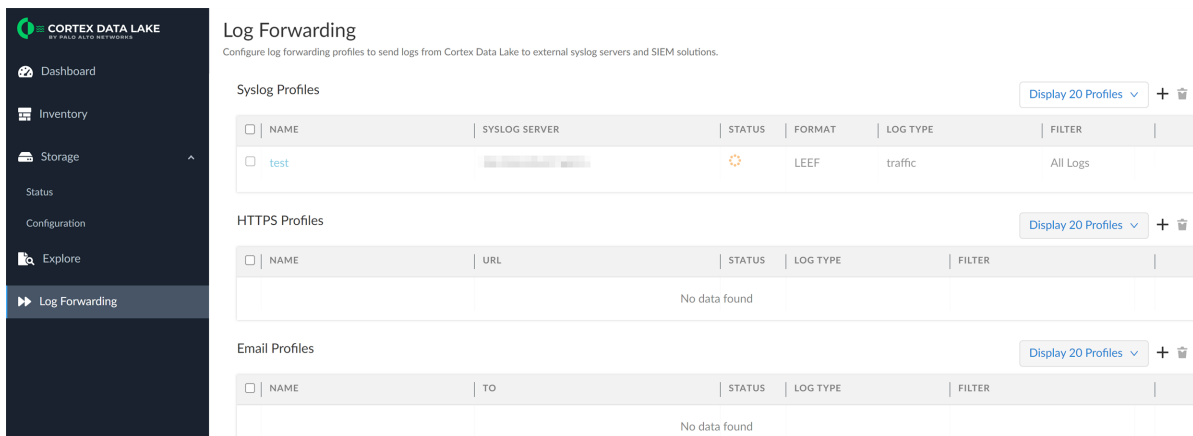
# Configure Syslog Event Sources on the NetWitness Platform

This section provides instructions for configuring the Palo Alto Prisma Access with NetWitness Log Collector. It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products to install the required components.

Perform the below steps on the NetWitness Platform to configure Syslog Event Source:

- Enable the Required Parser.

- Configure NetWitness Platform for Syslog Collection.

## Enable the Required Parser

If you do not see your parser in the list while performing this procedure, you need to download it in NetWitness Platform Live.

**To enable the required parser:**

1. In the **NetWitness** Platform 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, **paloaltonetworks** and ensure that the **Config Value** field for your event source is selected.

   The new device is listed under the Log Decoder(s) General Tab within the **Service Parsers Configuration**.

   > **Note:** The required parser is *paloaltonetworks*.

## Configure NetWitness Platform for 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.
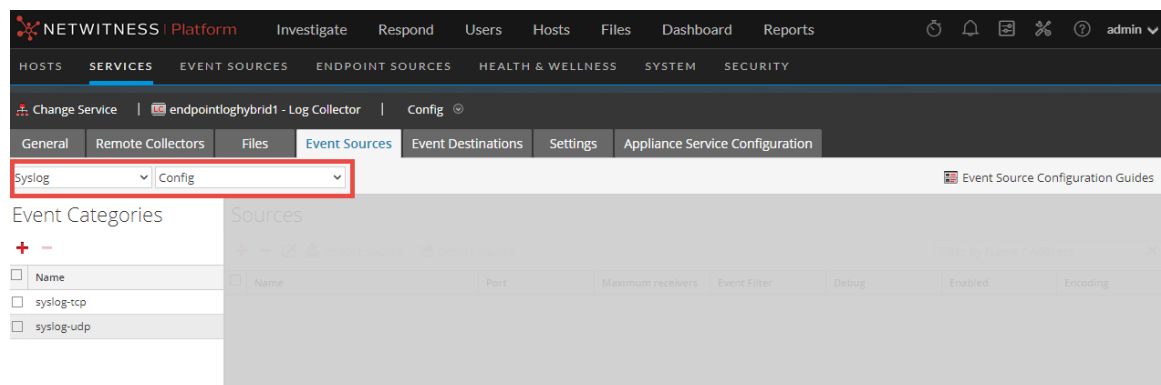


4. In the **Event Categories** panel toolbar, click **+**.

   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.
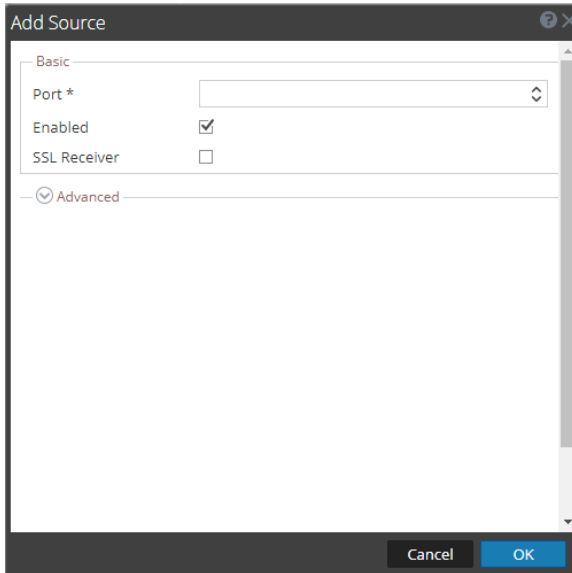


7. Enter **514** for the port and choose **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   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.

# Getting Help with NetWitness Platform

## 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 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 <br><br> 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 feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.