How to-Configure Zscaler ZPA to forward logs to EventTracker

EventTracker v9.2 and above

Publication Date: July 8, 2020

Abstract

This guide helps you in configuring **Zscaler ZPA** with EventTracker to receive **Zscaler ZPA** events. In this guide, you will find the detailed procedures required for monitoring **Zscaler ZPA.**

Scope

The configuration details in this guide are consistent with EventTracker version v9.2 or above and **Zscaler ZPA.**

Audience

Administrators, who are assigned the task to monitor and manage **Zscaler ZPA** events using **EventTracker.**

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

1. Overview

This guide helps you in configuring **Zscaler ZPA** with EventTracker to receive **Zscaler ZPA** events. In this guide, you will find the detailed procedures required for monitoring **Zscaler ZPA.**

EventTracker helps to monitor events from **Zscaler ZPA**. Its dashboard, alerts and reports help to detect authentication failure and other suspicious activities.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Prerequisites

- **EventTracker v9.2** or **above** should be installed.
- **Zscaler ZPA** should be configured.
- **Port 514** should be open.

3. Integration of Zscaler ZPA with EventTracker

A. Configure a connector.

To configure a new Connector: https://help.zscaler.com/zpa/configuring-connectors.

B. Configure the log receiver.

To add a log receiver.

1. Go to **Administration** > **Log Receivers**.
2. Click **Add Log Receiver**.

The **Add Log Receiver** window appears.

In the **Add Log Receiver** window, configure the following tabs.

a. In the **Log Receiver** tab:
   - **Name**: Enter a name for the log receiver. The name cannot contain special characters, except for periods (.), hyphens (-), and underscores (_).

- **Description**: (Optional)Enter a description.
- **Domain or IP Address**: Enter the fully qualified domain name (FQDN) or IP address of EventTracker Manager.

If the FQDN or IP address of the log receiver overlaps with or is as same as the wildcard domain or IP subnet defined in an application segment, the Bypass setting configured for the application segment takes precedence. As a result, if the FQDN or IP address is bypassed for a user on a trusted network, the user's device will not be able to communicate with the log receiver.

- **TCP Port**: Enter the TCP port number used by the EventTracker Manager.
- **Connector Groups**: Choose the Connector groups that can forward logs to the receiver and click **Done**. You can search for a specific group, click **Select All** to apply all groups, or click **Clear Selection** to remove all selections.

If you have a use case where the user's device needs to send logs to the log receiver using ZPA, configure an application segment with the log receiver domain or IP address and the port that the log receiver is listening on.

b. Click **Next**.

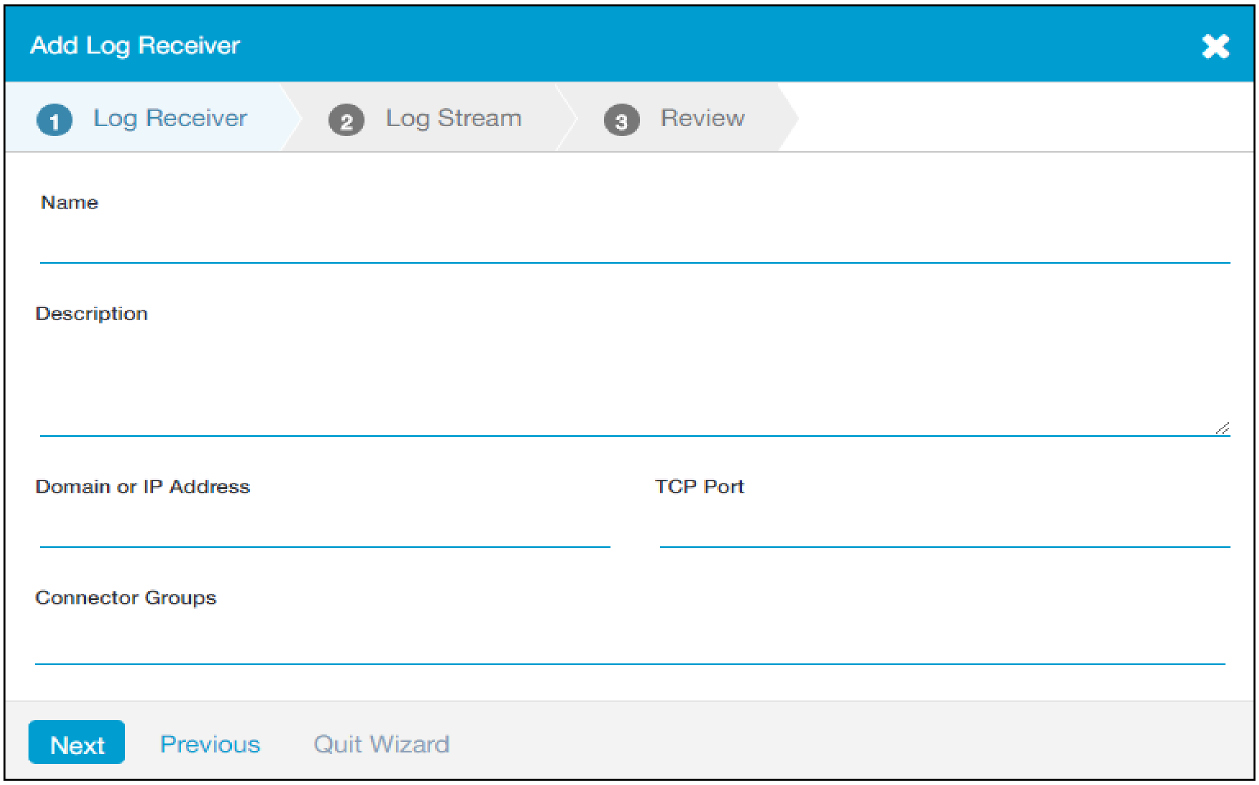

Figure 1

C. Configure Log stream

In the **Log Stream** tab, select a **Log Type** from the drop-down menu:

- **User Activity**: Information on end user requests to applications.
- **User Status**: Information related to an end user's availability and connection to ZPA.
- **Connector Status**: Information related to a Connector's availability and connection to ZPA.
- **Browser Access**: HTTP log information related to browser access.

Select **Log Template** from the drop-down menu as **Json**.

Click **Next**

Note: For any query regarding configuring log receiver and log stream, click on following link.
https://help.zscaler.com/zpa/configuring-log-receiver#Step1