sumo logic

Deployment Guide

Zscaler Internet Access

Zscaler Private Access

Nov 2021

For the latest documentation and information, refer to the integrations page at https://help.sumologic.com/07Sumo-Logic-Apps/22Security_and_Threat_Detection/Zscaler_Internet_Access

sumo logic

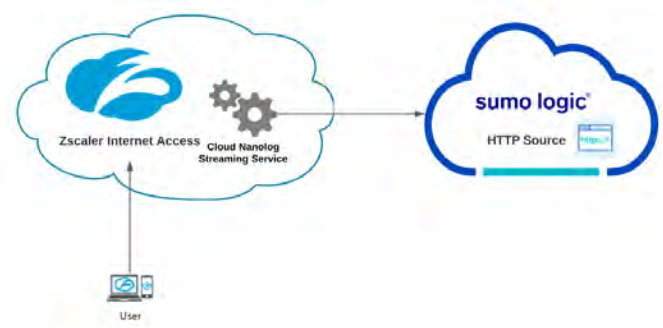
Collect Logs for the Zscaler Internet Access App

Learn how to Collect Logs for Zscaler Internet Access App

Zscaler uses Cloud Nanolog Streaming Service (NSS), which allows direct cloud-to-cloud log streaming for all types of ZIA logs into Sumo Logic.

To collect logs for Zscaler, perform these steps, detailed in the following sections:

1. Configure Sumo Logic Hosted Collector and an HTTP Source.
2. Configure Zscaler Cloud NSS feeds.



Configure Sumo Logic Hosted Collector and an HTTP Source

To collect logs for Zscaler Web Security, do the following in Sumo Logic:

1. Configure an Hosted Collector.
2. Configure an Http Source.
    1. For Source Category, enter any string to tag the output collected from this Source, such as **ZIA**.
    2. Click **Save** and make note of the HTTP address for the Source. You will need it when you configure the Zscaler Cloud NSS in the next section.

Configure Zscaler Cloud NSS

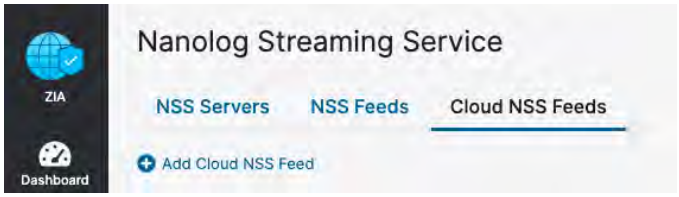
Zscaler uses Cloud Nanolog Streaming Service (NSS), which allows direct cloud-to-cloud log streaming for all types of ZIA logs into Sumo Logic.

To send logs to Sumo Logic using Cloud NSS, add a feed in ZIA using the following steps.

1. Log into your Zscaler Internet Access system.

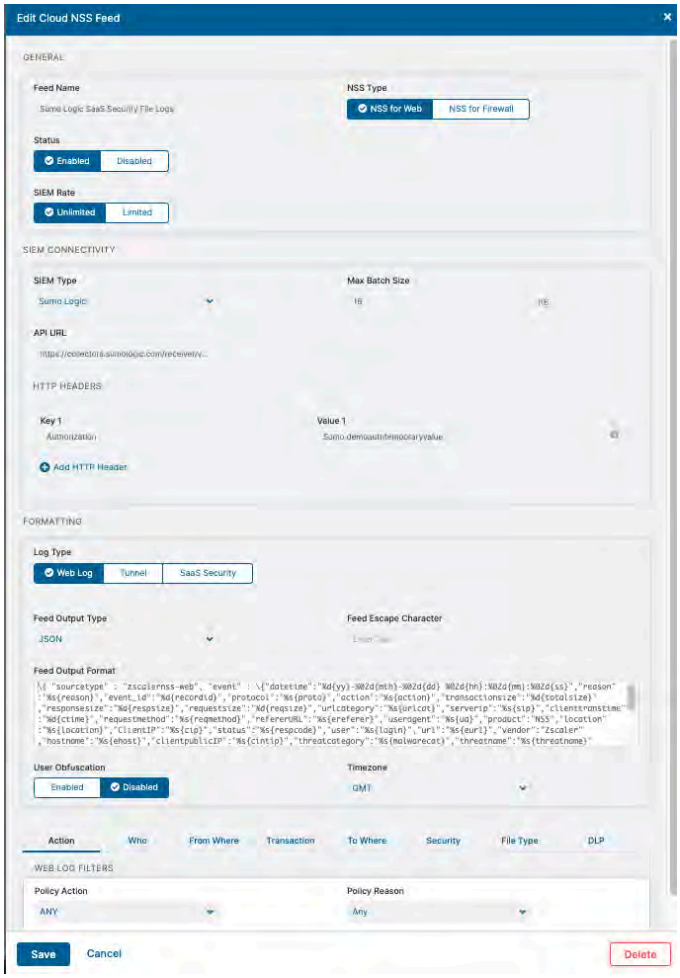
2. Go to **Administration -> Nanolog Streaming Service -> Cloud NSS Feeds**.

Cloud NSS is not enabled by default in ZIA. If you do not see Cloud NSS Feeds option in your ZIA environment, create a support request with Zscaler support.

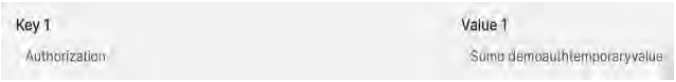


3. From the **Cloud NSS Feeds** tab, click **Add Cloud NSS Feed**.

4. In the **Add NSS Feed** dialog:



1. **Feed Name.** Enter a name for your NSS feed.
2. **NSS Server.** Select NSS for Web.
3. **Status. Enabled.**
4. **SIEM Type.**Select **Sumo Logic**.
5. **API URL.** Paste the HTTP address for the Source generated in the previous section.
6. **HTTP Headers. No Headers are required for Sumo Logic. If it requires at least one Header, add a dummy Header:**



7. **Log Type.** Select Web Log.
8. **Feed Output Type.** Select JSON.
9. **Feed Escape Character.** Leave this field blank.
10. **Feed Output Format.** The JSON format is displayed.
11. **User Obfuscation.** Select Disabled.
12. **Timezone.** Set to GMT by default.
13. **Web Log Filters**. Choose filters you would like to have.

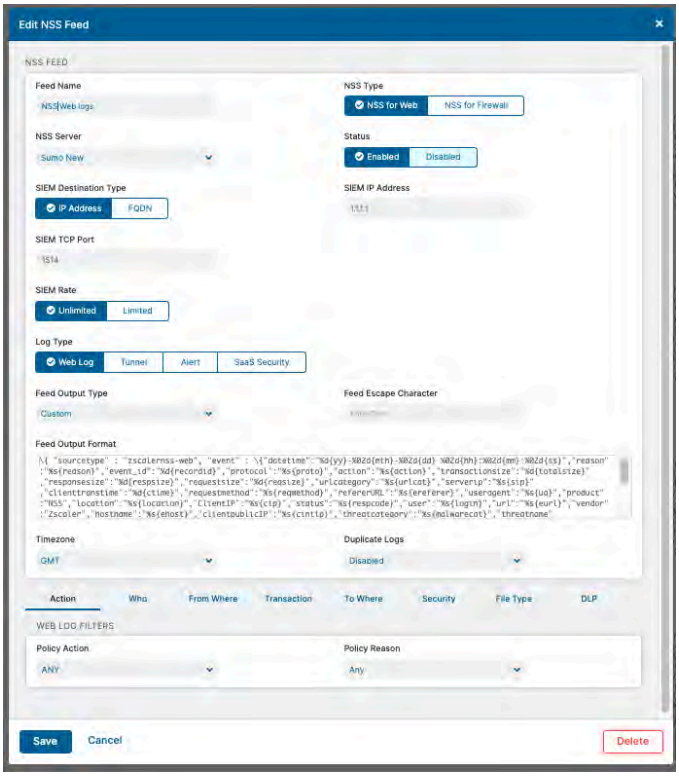
5. Click **Save**.
6. Repeat above steps for:
    1. NSS Type: NSS for Web and Log Type: Tunnel.
    2. NSS Type: NSS for Web and Log Type: SaaS Security.
    3. NSS Type: NSS for FireWall and Log Type: Firewall Logs.
    4. NSS Type: NSS for FireWall and Log Type: DNS Logs.

Note: Sumo Logic Dashboards utilize Web, Tunnel, DNS Logs.

(Optional) Configure the Zscaler NSS Feeds

If you are not able to use Zscaler Cloud NSS, you can collect logs for the ZIA App using NSS Servers. For DNS, Firewall, and Tunnel logs you can select JSON as the output format for the feed in the Add NSS Feeds dialog. For Web logs you will need to configure the feed as follows:

1. Log into your Zscaler NSS system.
2. Go to **Administration > Settings > Nanolog Streaming Service**.
3. From the **NSS Feeds** tab, click **Add**.
4. In the **Add NSS Feed** dialog:



1. **Feed Name.** Enter a name for your NSS feed.
2. **NSS Server.** Select the NSS Server.
3. **SIEM IP Address.** Enter the Sumo Logic Installed Collector IP address.
4. **Log Type.** Select Web Log.
5. **Feed Output Type.** Custom.
6. **NSS Type.** NSS for Web is the default.

7. **Status.** Select Enabled.

8. **SIEM TCP Port.** Enter the Sumo Logic Syslog Source TCP port number.

9. **Feed Escape Character.** Leave this field blank.

10. **Feed Output Format.** Select Custom and paste the following:
    REFER TO ONLINE DOCUMENTATION FOR FORMAT STRING

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd}
%02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_
id":"%d{recordid}","protocol":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize":"%d{respsize}"
```

11. **Duplicate Logs.** Disabled by default.

12. **Timezone.** Set to GMT by default.

5. Click **Save**.

Sample Log Message

Web Log Sample:


```
{
  "sourcetype": "zscalernss-web",
  "event": {
    "datetime": "2021-06-17 14:53:16",
    "reason": "Allowed",
    "event_id": "6974776045860487177",
    "protocol": "HTTP_PROXY",
    "action": "Allowed",
    "transactionsize": "639",
    "responsesize": "65",
    "requestsize": "574",
    "urlcategory": "Corporate Marketing",
    "serverip": "104.21.31.16",
    "clienttranstime": "0",
    "requestmethod": "CONNECT",
    "refererURL": "None",
    "useragent": "Windows Microsoft Windows 10 Pro ZTunnel/1.0",
    "product": "NSS",
    "location": "Road Warrior",
    "ClientIP": "40.83.138.250",
    "status": "200",
    "user": "testuser2@bd-dev.com",
    "url": "hamsan.yektanet.com:443",
    "vendor": "Zscaler",
    "hostname": "hamsan.yektanet.com",
    "clientpublicIP": "40.83.138.250",
    "threatcategory": "None",
    "threatname": "None",
```

```
    "filetype": "None",
    "appname": "General Browsing",
    "pagerisk": "0",
    "department": "Service Admin",
    "urlsupercategory": "Business and Economy",
    "appclass": "General Browsing",
    "dlpengine": "None",
    "urlclass": "Business Use",
    "threatclass": "None",
    "dlpdictionaries": "None",
    "fileclass": "None",
    "bwthrottle": "NO",
    "servertranstime": "0",
    "contenttype": "Other",
    "unscannabletype": "None",
    "odeviceowner": "5864177",
    "odevicehostname": "4051327232"
  }
}
```


Query Sample

Top 10 Blocked Base URLs

```
_sourceCategory=ZIA
| json field=_raw "event.clientpublicIP", "event.user", "event.url", "event.action" as src_ip, src_user, url, action
| where action != "Allowed"
| parse regex field=url "(?<baseurl>.+?)[:/]" nodrop
| count by baseurl
| sort _count
| top 10 baseurl by _count
```

sumo logic

Install the Zscaler Internet Access App and view the Dashboards

This page provides instructions on how to install the Zscaler Internet Access App, and provides examples of each of the dashboards.

This page provides instructions on how to install the Zscaler Internet Access App, and provides examples of each of the dashboards. The App preconfigured searches and Dashboards provide easy-to-access visual insights into your data.

Install the Sumo Logic App

To install the app, do the following:

Locate and install the app you need from the **App Catalog**. If you want to see a preview of the dashboards included with the app before installing, click **Preview Dashboards**.

1. From the **App Catalog**, search for and select the app**.**
2. Select the version of the service you're using and click **Add to Library**.

Version selection is applicable only to a few apps currently. For more information, see the Install the Apps from the Library.

3. To install the app, complete the following fields.
    a. **App Name.** You can retain the existing name, or enter a name of your choice for the app.
    b. **Data Source.** Select either of these options for the data source.
        - Choose **Source Category**, and select a source category from the list.
        - Choose **Enter a Custom Data Filter**, and enter a custom source category beginning with an underscore. Example: (_sourceCategory=MyCategory).
    c. **Advanced**. Select the **Location in Library** (the default is the Personal folder in the library), or click **New Folder** to add a new folder.
4. Click **Add to Library**.

Once an app is installed, it will appear in your **Personal** folder, or other folder that you specified. From here, you can share it with your organization.

Panels will start to fill automatically. It's important to note that each panel slowly fills with data matching the time range query and received since the panel was created. Results won't immediately be available, but with a bit of time, you'll see full graphs and maps.

Dashboards

Zscaler- Overview

The **Zscaler - Overview** Dashboard provides general information of the Zscaler Web Gateway logs, including Panels that drill-down into the other Zscaler Dashboards. The Overview Dashboard gives a good starting point for detecting anomalies in blocked traffic and geographic hotspots for allowed and blocked traffic.

Zscaler- Behavior

The **Zscaler - Behavior** Dashboard focuses on allowed traffic behaviors, showing trends and deviations by users, content types accessed, content categories, super categories, and bandwidth trends.

Zscaler- Blocked Traffic

The **Zscaler - Blocked** Traffic Dashboard illustrates outliers in both blocked traffic peaks and multi-dimensional outliers

for blocked activity specific to user.

Zscaler- File Classification Activity

The **Zscaler - File Classification Activity** Dashboard focuses on file-based threats by users, threat name, file types, and subtypes for a overarching view of blocked files across the Zscaler environment.

ZIA - DNS

The **ZIA - DNS** Dashboard focuses on DNS activity specifically around denied requests and responses, server locations across the Zscaler environment.

Use this dashboard to:

- Gain insights into DNS health and performance.
- Determine if rules need tweaking based on volume of denied/allowed requests and responses.

ZIA - Logs

The **ZIA - Logs** Dashboard gives insights into different logs being produced in the Zscaler environment.

Use this dashboard to:

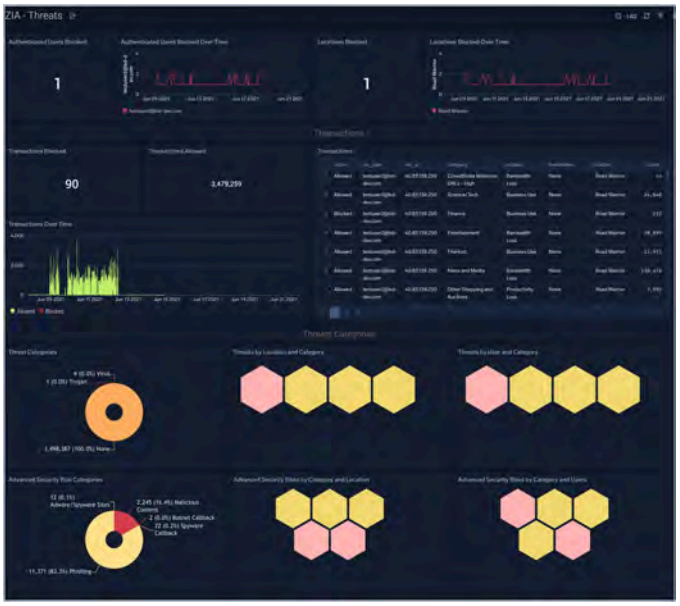
- Get quick insights into logs volume by source.
- View logs filtered by type and users and determine any potential issues.

ZIA - Threats

The **ZIA - Threats** Dashboard focuses on threats in your Zscaler environment.

Use this dashboard to:

- Detect anomalies in blocked traffic and geographic hotspots for allowed and blocked traffic.
- Gain insights into threats by categories and transactions.
- Identify locations and users being blocked as a sign of potential suspicious or malicious activity.



sumo logic

Collect Logs for the Zscaler Private Access (ZPA) App

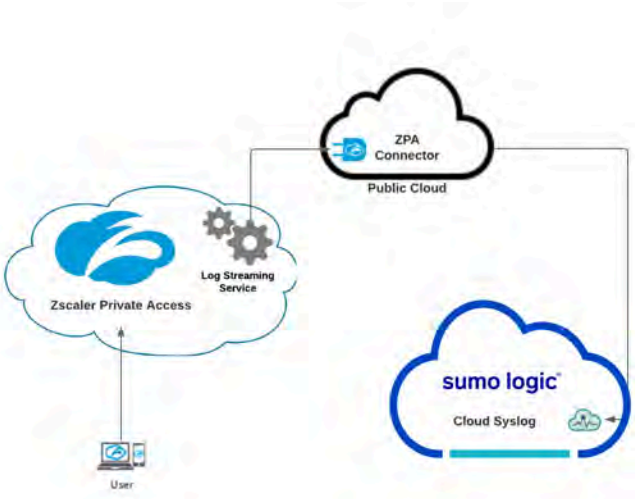
This page provides instructions for configuring log and metric collection for the Sumo Logic App for ZPA.

Zscaler Private Access uses the Log Streaming Service (LSS), to stream logs from the Zscaler service and deliver them to the Sumo Logic Hosted collector via Syslog.

LSS is deployed using two components, a log receiver and a ZPA App Connector. LSS resides in ZPA and initiates a log stream through a ZPA Public Service Edge (formerly Zscaler Enforcement Node or ZEN). The App Connector resides in your company's enterprise environment. It receives the log stream and then forwards it to Sumo Logic Cloud Syslog.

To collect logs for Zscaler Private Access, perform these steps, detailed in the following sections:

1. Configure Sumo Logic Hosted Collector and a Cloud Syslog Source
2. Configure App Connector in ZPA
3. Deploy an App Connector on a Supported Platform
4. Configure Log Receivers in ZPA to send logs to Sumo Logic



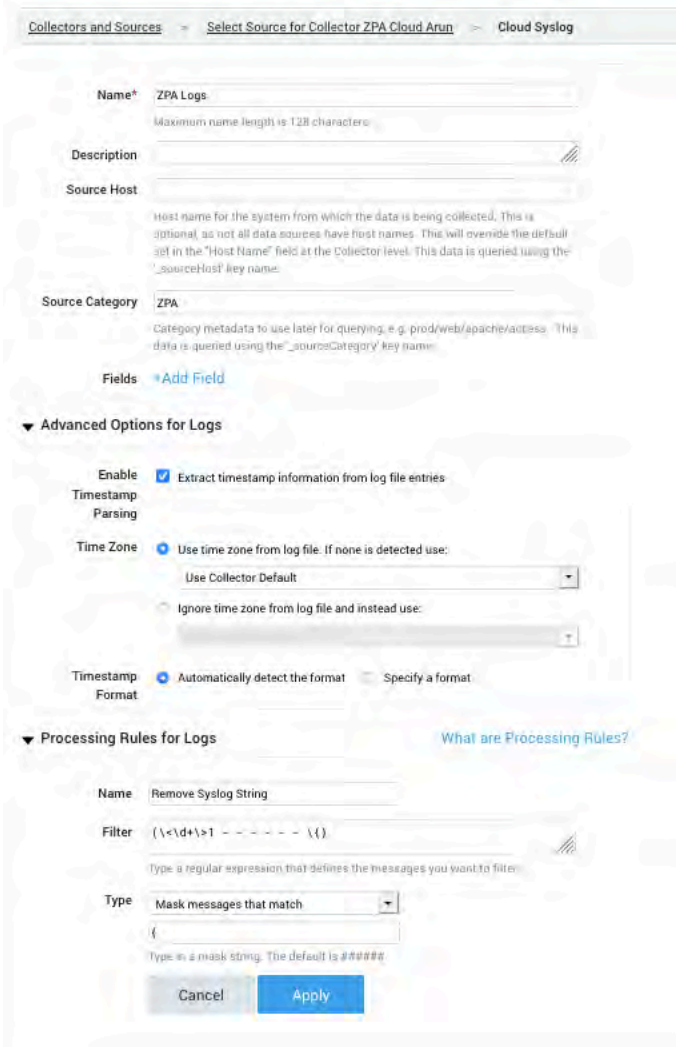
Configure Sumo Logic Hosted Collector and a Cloud Syslog Source

To collect logs for ZPA, do the following in Sumo Logic:

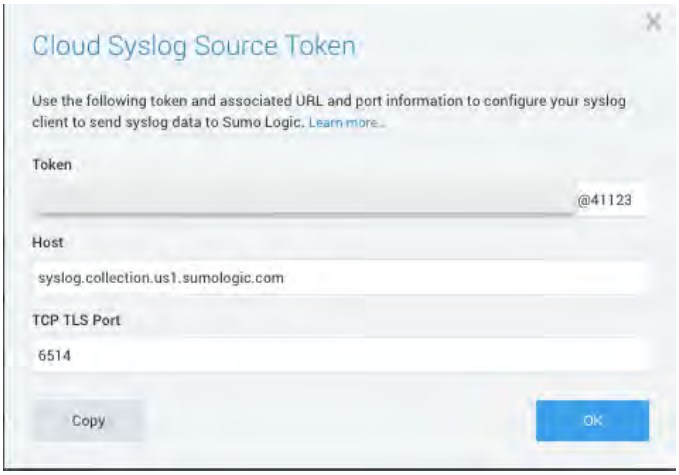
1. Configure a Hosted Collector.
2. Perform the steps in Configure a Cloud Syslog Source. and configure the following Source fields:

- **Name**. (Required) A name is required. Description is optional.
- **Source Category**. (Required) [Provide a realistic Source Category example for this data type.] The Source Category metadata field is a fundamental building block to organize and label Sources.
  For details see Best Practices.

3. In the Advanced section, specify the following configurations:
   - **Enable Timestamp Parsing**. True
   - **Time Zone**. Use time zone from log file. If none is detected use: Use Collector Default.
   - **Timestamp Format**. Auto Detect
4. In the Processing Rules for Logs section, add a Processing Rule:
   - **Name:** Remove Syslog String
   - **Filter**: (\<\d+\>1 - - - - - - \{)
   - **Type**: Mask messages that match
   - **Mask String**: {



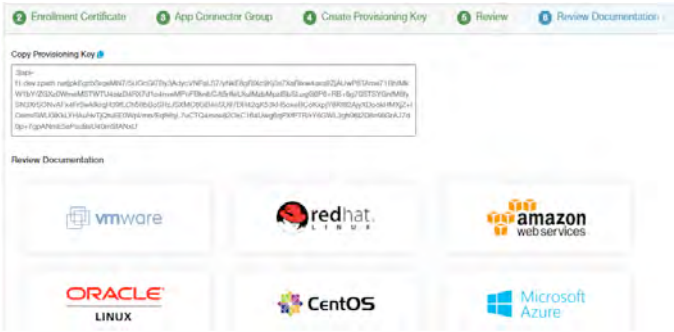
5. Click **Save**.



Copy and paste the **Token, Host and Port** in a secure location. You will need these when you configure ZPA LSS.

Configure App Connector in ZPA

Configure a new App Connector in ZPA. Copy the provisioning key created/selected during App Connector configuration.



Deploy an App Connector on a Supported Platform

After you add an App Connector, you must deploy it. Deployment consists of installing the App Connector and also enrolling the App Connector, which allows the App Connector to obtain a TLS client certificate that it must use to authenticate itself to the ZPA cloud. After deployment, the App Connector is ready to send logs to Sumo Logic.

Before you begin a deployment, read App Connector Deployment Prerequisites which provides detailed information on VM image sizing and scalability, supported platform requirements, deployment best practices, and other essential guidelines.

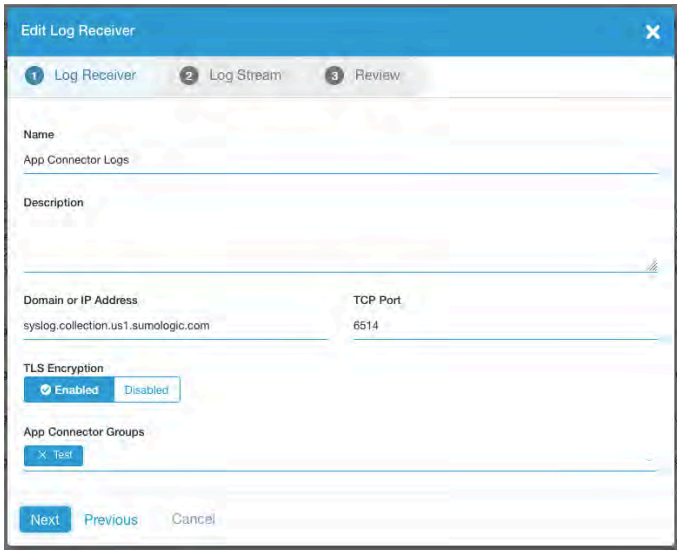
The deployment process differs depending on the platform used for the App Connector. Zscaler recommends that App Connectors be deployed in pairs, to ensure continuous availability during software upgrades.

To deploy the App Connector, see the Deployment Guide for your platform.

Configure Log Receivers in ZPA to send logs to Sumo Logic

Once you have deployed the App Connector, configure log receivers to send logs to the Sumo Logic cloud syslog endpoint using the following steps:

1. Log into your ZPA system.
2. Go to **Administration** > **Log Receivers**.
3. Click **Add Log Receiver**.
4. In the **Add Log Receiver** window, configure the following tabs:
    1. Log Receiver



1. **Name**: Enter a name for the log receiver. The name cannot contain special characters, with the exception of periods (.), hyphens (-), and underscores (_).
2. **Description**: (Optional) Enter a description.
3. **Domain or IP Address**: Enter the Domain name from the Sumo Logic Cloud Syslog Source.
4. **TCP Port**: Enter the TCP port number from the Sumo Logic Cloud Syslog Source. Default: 6514
5. **TLS Encryption**: Select Enabled.
6. **Connector Groups**: Choose the App 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.
7. Click **Next**.

2. Log Stream

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

        1. **User Activity**: Information on end user requests to applications. To learn more, see User Activity Log Fields.
        2. **User Status**: Information related to an end user's availability and connection to ZPA. To learn more, see User Status Log Fields.
        3. **Connector Status**: Information related to an App Connector's availability and connection to ZPA. To learn more, see App Connector Status Log Fields.
        4. **Browser Access**: HTTP log information related to Browser Access. To learn more, see Browser

Access Log Fields and About Browser Access.

5. **Audit Logs**: Session information for all admins accessing the ZPA Admin Portal. To learn more, see About Audit Log Fields and About Audit Logs.

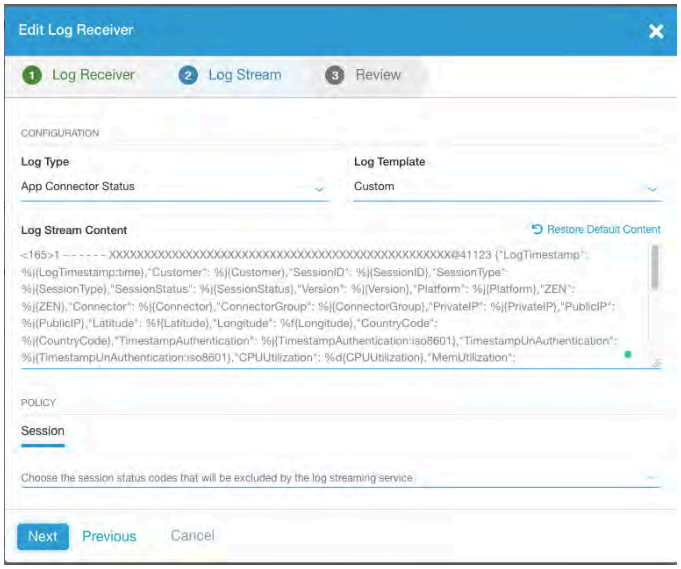
2. In the **Log Template** field, select **JSON.**
3. The default **Log Stream Content** that is displayed will change based on the **Log Type** and **Log Template** you selected in previous steps.

   You can also edit the log stream content within the text field in order to capture specific fields and create a **Custom** log template. To learn more, see Understanding the Log Stream Content Format.

   Edit the the log stream content, paste the following text in the beginning of the template:

> <165>1 - - - - - - <Syslog Token>

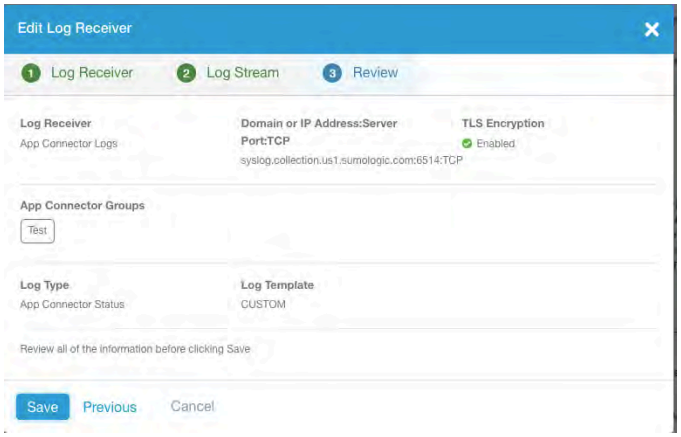
For **Syslog Token,** enter the token from the Sumo Logic Cloud Syslog Source. The token should end with **@41123**. This number is the Sumo Logic Private Enterprise Number (PEN).



4. You can define a streaming **Policy** for the log receiver. For example, you can create a policy where the receiver will only capture logs for a specified segment group or a specific set of session status error codes. The criteria you can use is dependent upon the **Log Type** you selected. For various options to define a streaming policy, see ZPA help.
5. Click **Next**.

3. Review

1. In the **Review** tab, review your log receiver configuration, and click **Save**.



5. Repeat the previous steps for all the **Log Types**:

    1. **User Activity**: Information on end user requests to applications. To learn more, see User Activity Log Fields.

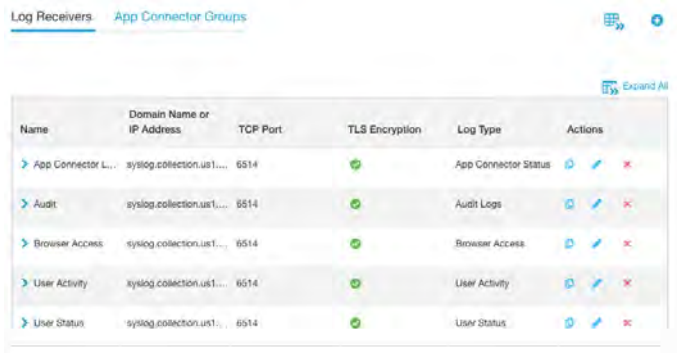
    2. **User Status**: Information related to an end user's availability and connection to ZPA. To learn more, see User Status Log Fields.

    3. **Connector Status**: Information related to an App Connector's availability and connection to ZPA. To learn more, see App Connector Status Log Fields.

    4. **Browser Access**: HTTP log information related to Browser Access. To learn more, see Browser Access Log Fields and About Browser Access.

    5. **Audit Logs**: Session information for all admins accessing the ZPA Admin Portal. To learn more, see About Audit Log Fields and About Audit Logs.

6. The end result should look like below:



7. At this point, ZPA should start sending logs to Sumo Logic.

sumo logic

Install the Zscaler Private Access App and View the Dashboards

This page has instructions for installing the Sumo App for Zscaler Private Access, and descriptions of each of the app dashboards.

This page has instructions for installing the Sumo App for Zscaler Private Access and descriptions of each of the app dashboards.

Install the App

Now that you have set up collection for HAProxy, you can install the HAProxy App to use the pre-configured searches and dashboard that provide insight into your data.

To install the App, do the following:

Locate and install the app you need from the **App Catalog**. If you want to see a preview of the dashboards included with the app before installing, click **Preview Dashboards**.

1. From the **App Catalog**, search for and select the app**.**
2. Select the version of the service you're using and click **Add to Library**.

Version selection is applicable only to a few apps currently. For more information, see the Install the Apps from the Library.

3. To install the app, complete the following fields.
    a. **App Name.** You can retain the existing name, or enter a name of your choice for the app.
    b. **Data Source.** Select either of these options for the data source.
        - Choose **Source Category**, and select a source category from the list.
        - Choose **Enter a Custom Data Filter**, and enter a custom source category beginning with an underscore. Example: (_sourceCategory=MyCategory).
    c. **Advanced**. Select the **Location in Library** (the default is the Personal folder in the library), or click **New Folder** to add a new folder.
4. Click **Add to Library**.

Once an app is installed, it will appear in your **Personal** folder, or other folder that you specified. From here, you can share it with your organization.

Panels will start to fill automatically. It's important to note that each panel slowly fills with data matching the time range query and received since the panel was created. Results won't immediately be available, but with a bit of time, you'll see full graphs and maps.

Filter with template variables

Template variables provide dynamic dashboards that can re-scope data on the fly. As you apply variables to troubleshoot through your dashboard, you view dynamic changes to the data for a quicker resolution to the root cause. For more information, see the Filter with template variables help page. You can use template variables to drill down and examine the data on a granular level.

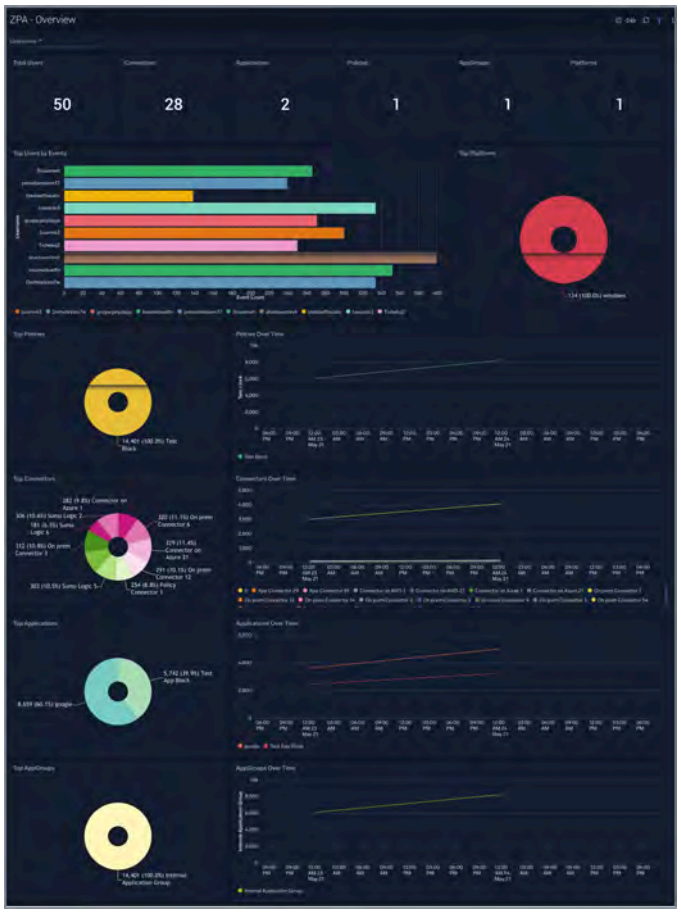
Dashboards

ZPA - Overview

The **ZPA - Overview** Dashboard focuses on the overall health of the ZPA system.

Use this dashboard to:

- Gain insights into ZPA health.
- Manage ZPA connector health.



ZPA - Audit

The **ZPA - Audit** Dashboard focuses the changes in the ZPA admin UI. It allows easy tracking and change management.

Use this dashboard to:

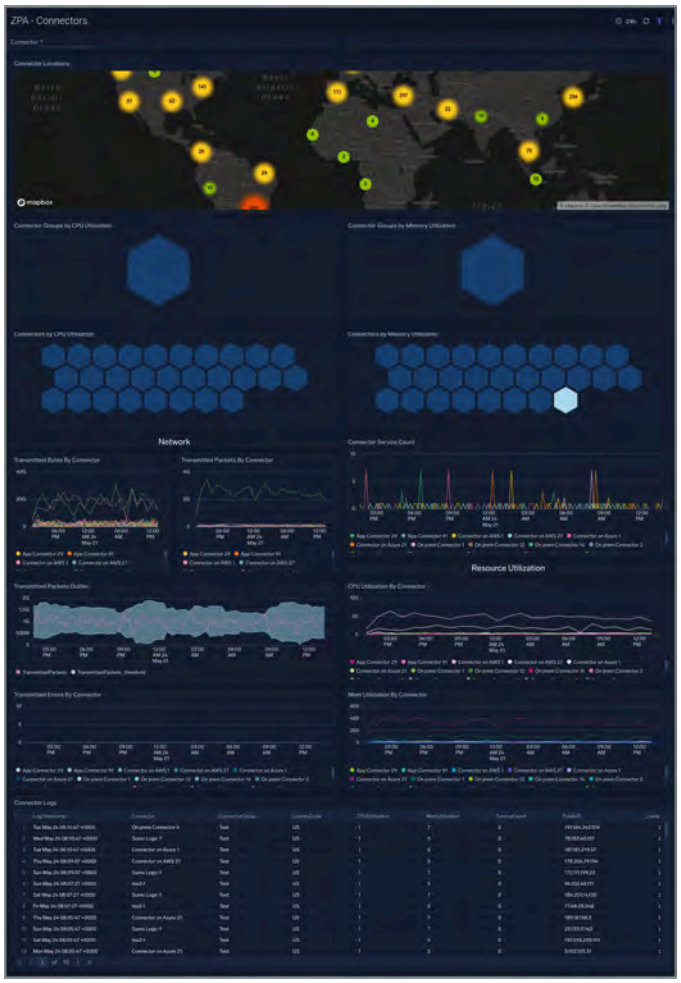
- Gain insights into ZPA configuration changes.
- Easily identify the mis-configurations for erratic behavior.

ZPA - Connectors

The **ZPA - Connectors** Dashboard focuses on connector health and resource utilization.

Use this dashboard to:

- Gain insights into ZPA connector health.
- Identify and manage connectors erroring out or having resource constraints.



ZPA - Performance

The **ZPA - Performance** Dashboard focuses on the performance of the connectors and the ZPA system.

Use this dashboard to:

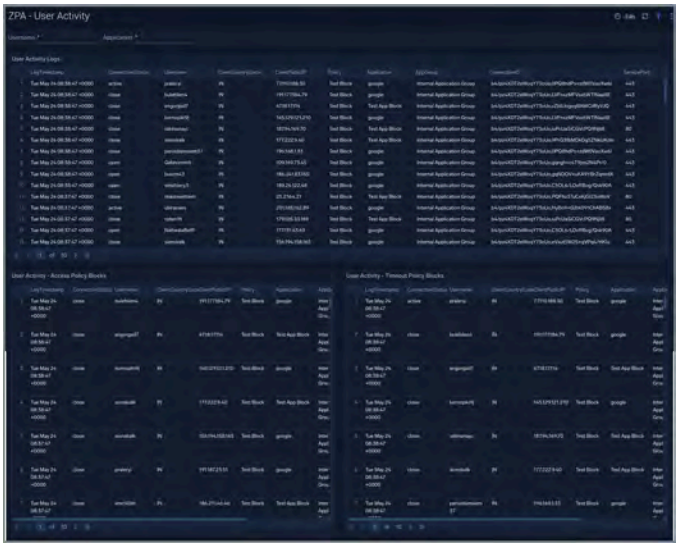
- Gain insights into ZPA Performance.
- Manage ZPA connector setup times to determine potential issues.

ZPA - User Activity

The **ZPA - User Activity** Dashboard focuses on the users activity.

Use this dashboard to:

- Gain insights into User activity.



ZPA - Users

The **ZPA - Users** Dashboard focuses on the user details.

Use this dashboard to:

- Gain insights into User connections and Access.
- Manage Policy and Timeout blocks.