ZSCALER AND GURUCUL DEPLOYMENT GUIDE

DECEMBER 2023, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
NSS	Nanolog Streaming Service
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
UEBA	User and Entity Behavior Analytics
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website or follow Zscaler on Twitter @zscaler.

Gurucul Overview

Gurucul is a global cyber security company that is changing the way organizations protect their most valuable assets, data and information from insider and external threats both on-premises and in the cloud. Gurucul's real-time Cloud-Native Security Analytics and Operations Platform provides customers with a Next-Generation SIEM, UEBA, Open XDR, and Identity & Access Analytics. It combines machine learning behavior profiling with predictive risk-scoring algorithms to predict, prevent, and detect breaches. Gurucul technology is used by Global 1000 companies and government agencies to fight cybercrimes, IP theft, insider threat and account compromise as well as for log aggregation, compliance and risk-based security orchestration and automation for real-time extended detection and response. To learn more, refer to Gurucul's website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- Gurucul Resources

Software Versions

This document was authored using the latest version of Zscaler software.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Gurucul Introduction

Overviews of the Zscaler and Gurucul applications are described in this section.

⚠ If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, please contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Gurucul Next-Gen SIEM Overview

Gurucul Next-Gen SIEM is focused on unburdening security teams from floods of alerts and false positives, leveraging automation to drastically reduce mean-time-to-detect (MTTD), and prioritizing investigations and response actions to lower mean-time-to-respond (MTTR). In addition, Gurucul Next-Gen SIEM provides the necessary capabilities to achieve or exceed compliance requirements and strongly maps to the MITRE Att&ck Framework. Gurucul also works natively within any cloud environment and is the only vendor that supports cross-cloud analytics for poly-cloud threat detection and response.

Gurucul Next-Gen SIEM improves data collection and infrastructure visibility, while automating and consolidating manual tasks related to correlation, analysis, investigation, and response actions. It is also one of the only solutions that automatically includes out-of-the-box threat content powered by threat intelligence and open-source machine learning (ML) models. This delivers immediate automated threat detection upon deployment.

Gurucul UEBA Overview

Gurucul User and Entity Behavior Analytics (UEBA) detects and responds quickly to threats based on an understanding of normal activity that continuously learns and adjusts to characterize suspicious and anomalous activity. Combined with our out-of-the-box threat content and other analytical capabilities, Gurucul UEBA can help security teams quickly distinguish malicious activity from false positives.

Gurucul Resources

The following table contains links to Gurucul support resources.

Name	Definition
Support Portal	Gurucul customer support portal.
Product Technical Training	Gurucul product technical training.

Introduction

This guide helps users to integrate Gurucul Risk Analytics (GRA) with Zscaler NSS Feeds and APIs. It also provides instructions for Configuring GRA with Zscaler. This document is not intended to suggest optimum configurations. It is assumed the reader has working knowledge of both suites of products involved and possesses the ability to perform the tasks outlined in the following sections. Administrators should have access to the product documentation for all products in order to install and configure the required components.

This document describes how to integrate Gurucul Next-Gen SIEM and UEBA products with ZIA. Gurucul integrates with ZIA using three different mechanisms:

1. NSS: NSS forwards ZIA logs over secure Syslog connection to Gurucul's log collection endpoint, which requires the deployment of a Zscaler NSS Virtual Machine (VM). ZIA logs do not support TLS encryption.
2. Cloud NSS: Gurucul integrates with ZIA through Cloud NSS using the following mechanisms:
   a. AWS S3 Integration: ZIA can forward logs to a Gurucul-owned AWS S3 bucket.
   b. HTTP Endpoint: ZIA can send logs to Gurucul HTTP endpoint using HTTP/HTTPS POST.
3. Log Streaming Service: ZPA can send logs to Gurucul using the Syslog endpoint.

Prerequisites

- Zscaler Cloud NSS Service enabled or a Zscaler NSS VM is deployed.
- Zscaler Cloud API enabled and Zscaler user with Service Admin Group access.
- ZPA Log Streaming Service.
- Gurucul HTTP Endpoint and/or S3 Bucket for your Gurucul tenant.

Integration Architecture

The following diagram shows the ZIA and Gurucul integration.

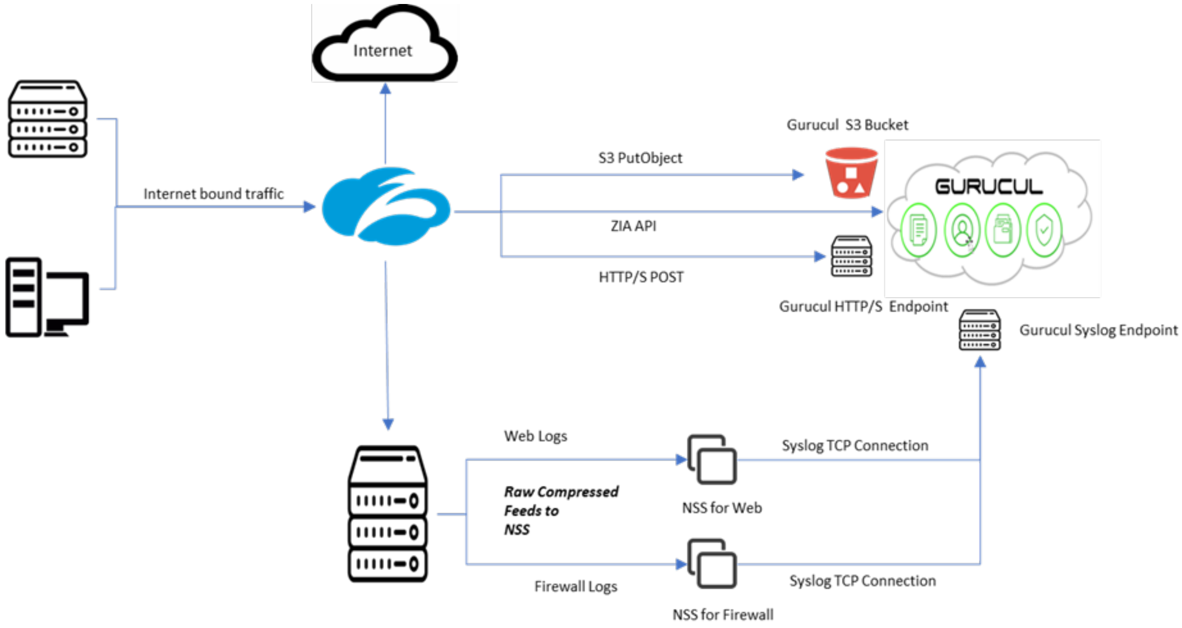


Figure 1. ZIA and Gurucul architecture

Logs Ingested

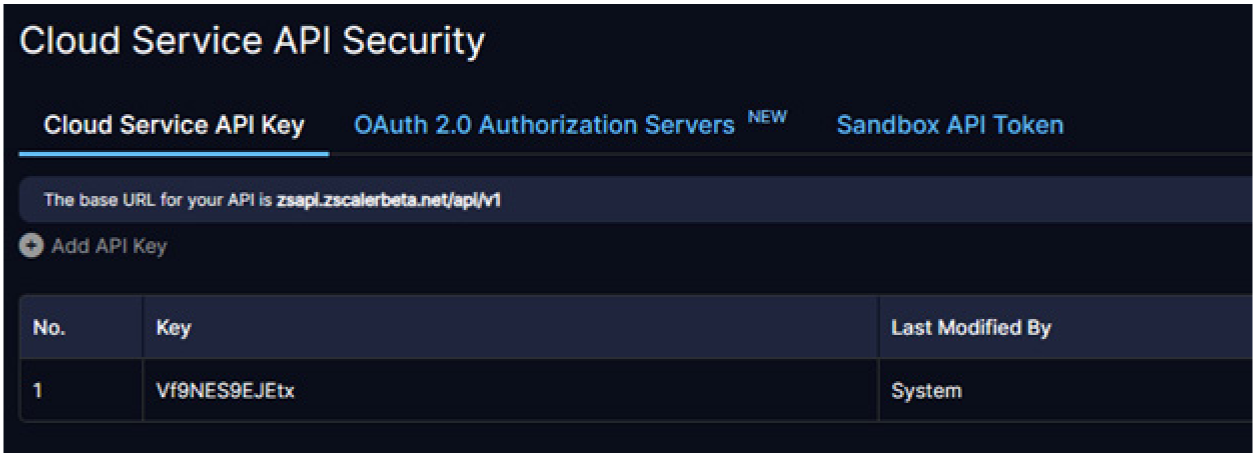
The following logs are ingested into Gurucul from ZIA.

Integration Mechanism	Logs Ingested
NSS Server / VM	Web Logs Firewall Logs
Cloud NSS (ZIA)Admin	Audit Logs Tunnel Logs Web Logs Firewall Logs DNS Logs DLP/CASB Logs
Log Streaming Service (ZPA)	User Activity and Status Browser Access Audit Logs Private Service Edge App Connector Status and Metrics
Zscaler API	Admin Audit Logs Event Logs User and Group Information

Zscaler Prerequisites

To use the Cloud Service API:

1. File a ticket with Zscaler Support to enable the API for your account and create a user with Service Admin Rights.
2. After the API is enabled, log in to the ZIA Admin Portal and go to **Administration** > **Authentication** > **Cloud Service API Security** > **Cloud Service API Key** to retrieve your API key or regenerate the API Key.



Cloud Service API Security

The base URL for your API is **zsapi.zscalerbeta.net/api/v1**

No.	Key	Last Modified By
1	Vf9NES9EJEtx	System

Figure 2. Cloud Service API Key

Gurucul Configuration

The following sections details a list of endpoints and S3 buckets that are available to a Gurucul tenant after signup.

Gurucul S3 Bucket

The Gurucul S3 bucket used to send logs to and from ZIA is provisioned when the Gurucul Tenant signs up for either one or more of Gurucul's product suite. The name of the S3 bucket is available to be viewed in the console and is also sent with the welcome email during the signup process.

In this document, the bucket will be called GURUCUL-TENANT-S3-BUCKET.

Gurucul HTTP/HTTPS Endpoint

The Gurucul HTTP/HTTPS endpoint used to send logs to from ZIA is provisioned when the Gurucul Tenant signs up for either one or more of Gurucul's product suite. The URL of the HTTP/HTTPS endpoint is available to be viewed in the console and is also sent with the welcome email during the signup process.

In this document, the endpoint will be called GURUCUL-TENANT-HTTP-ENDPT.

Gurucul Syslog Endpoint

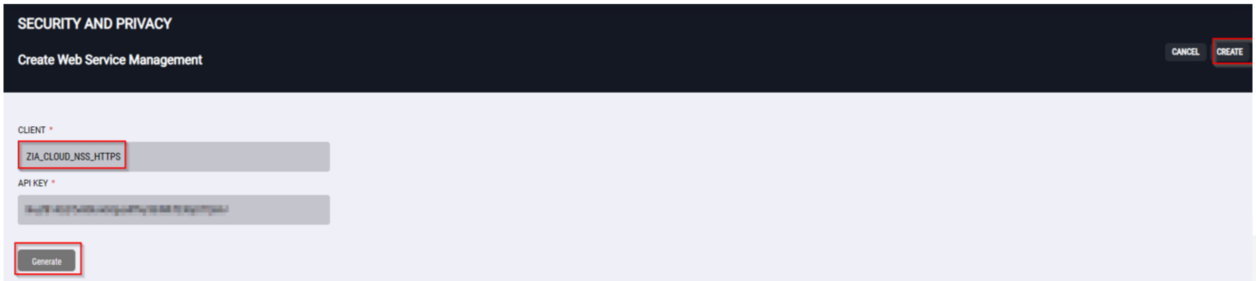
The Gurucul Syslog endpoint used to receive streaming logs from ZIA/ZPA is provisioned when the Gurucul Tenant signs up for either one or more of Gurucul's product suite. The URL of the Syslog endpoint is available to be viewed in the console and is also sent with the welcome email during the signup process. ZIA logs do not support TLS encryption.

In this document, the endpoint will be called GURUCUL-TENANT-SYSLOG-ENDPT.

API Token Creation

To use the Gurucul HTTP/HTTPS endpoint for ZIA logs, the tenant must create an authentication token that is later configured in ZIA Cloud NSS configurations. Perform the following steps:

1. Log in to the Gurucul console with Admin or System Admin rights.
2. Go to **Configure** > **Security and Access** > **Web Service Management**.
3. Click **Add** to create a new API token.
4. Fill in the name for the token as desired and click **Generate**.
5. Click **Create** to create and save the token.



SECURITY AND PRIVACY

Create Web Service Management

CLIENT * ZIA_CLOUD_NSS_HTTPS

API KEY * [redacted]

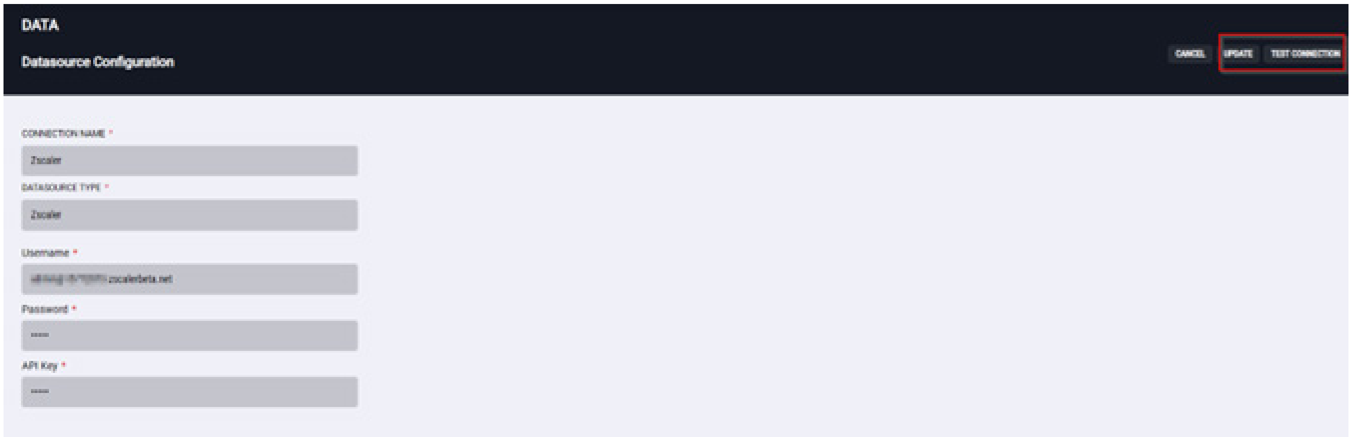
Figure 3. API Token

You can use the token in the ZIA Cloud NSS HTTP/HTTPS configurations.

API Data Source

To collect Admin Audit and Event Logs along with ZIA User and Group Information, set up the ZIA API connection:

1. Log in to the Gurucul console with Admin or System Admin rights.
2. Go to **Configure** > **Data** > **Setup**.
3. Click **Add** to create a new ZIA data source.
4. Fill in the following fields:
    a. **Connection Name**: Enter the connection name to identify the data source.
    b. **Username**: Enter the Zscaler username with API rights.
    c. **Password**: Enter the password for the Zscaler User.
    d. **API Key**: Enter the Zscaler Cloud Security Service API token associated with the user.
5. Click **Test Connection** to test the API connection.
6. Click **Save** or **Update** to save the connection details.



CONNECTION NAME *
Zscaler

DATASOURCE TYPE *
Zscaler

Username *
[redacted]zscalerbeta.net

Password *
•••••

API Key *
•••••

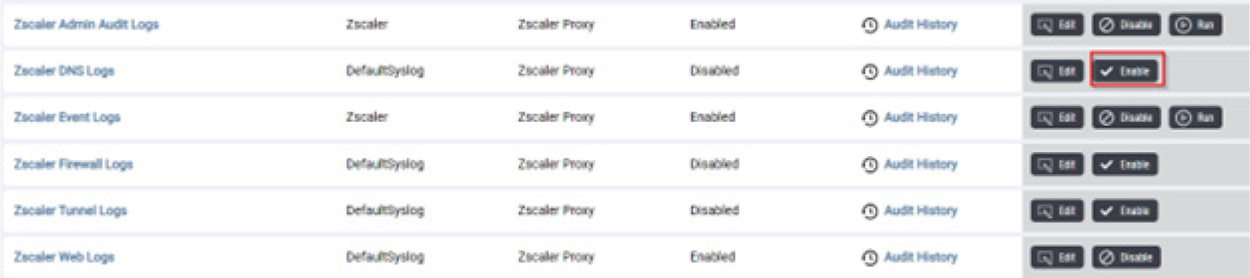
Figure 4. API Data Source

Enable Zscaler Pipelines

Your Gurucul product is pre-packaged with all the required Zscaler pipelines.

Zscaler Cloud NSS pipelines are shared when using either S3 or HTTP endpoint URLs along with Syslog using Zscaler NSS servers. You can enable pipelines by performing the following steps:

1. Log in to the Gurucul console with Admin or System Admin rights.
2. Go to **Pipelines** > **Activity**.
3. Search for Zscaler pipelines by entering `zscaler` in the search bar.
4. For each pipeline you want to enable, click **Enable** in the **Action** column that corresponds to the pipeline.

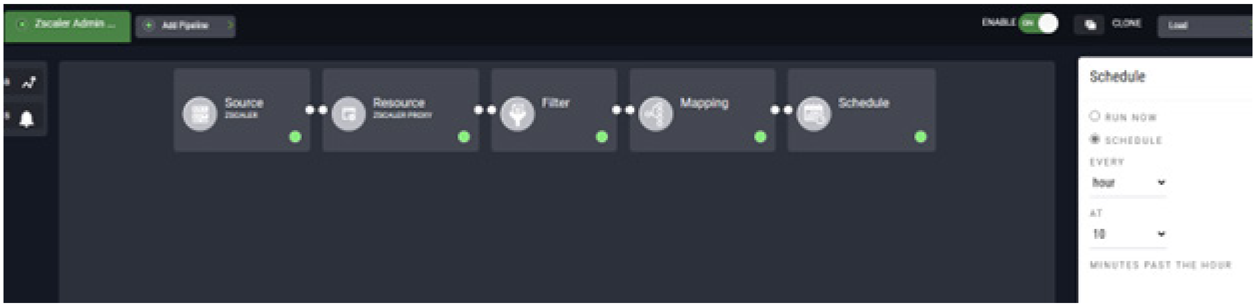


Zscaler Admin Audit Logs	Zscaler	Zscaler Proxy	Enabled	Audit History	Edit Disable Run
Zscaler DNS Logs	DefaultSyslog	Zscaler Proxy	Disabled	Audit History	Edit Enable
Zscaler Event Logs	Zscaler	Zscaler Proxy	Enabled	Audit History	Edit Disable Run
Zscaler Firewall Logs	DefaultSyslog	Zscaler Proxy	Disabled	Audit History	Edit Enable
Zscaler Tunnel Logs	DefaultSyslog	Zscaler Proxy	Disabled	Audit History	Edit Enable
Zscaler Web Logs	DefaultSyslog	Zscaler Proxy	Enabled	Audit History	Edit Disable

Figure 5. Pipelines

For Admin and Event logs, you can schedule the pipelines to run at the desired intervals. To schedule the pipeline:

1. Click **Edit**. This opens the **Schedule** tab.
2. Select the appropriate schedule and click **Start**.



Schedule

○ RUN NOW

● SCHEDULE

EVERY

hour

AT

10

MINUTES PAST THE HOUR

Figure 6. Pipeline schedules

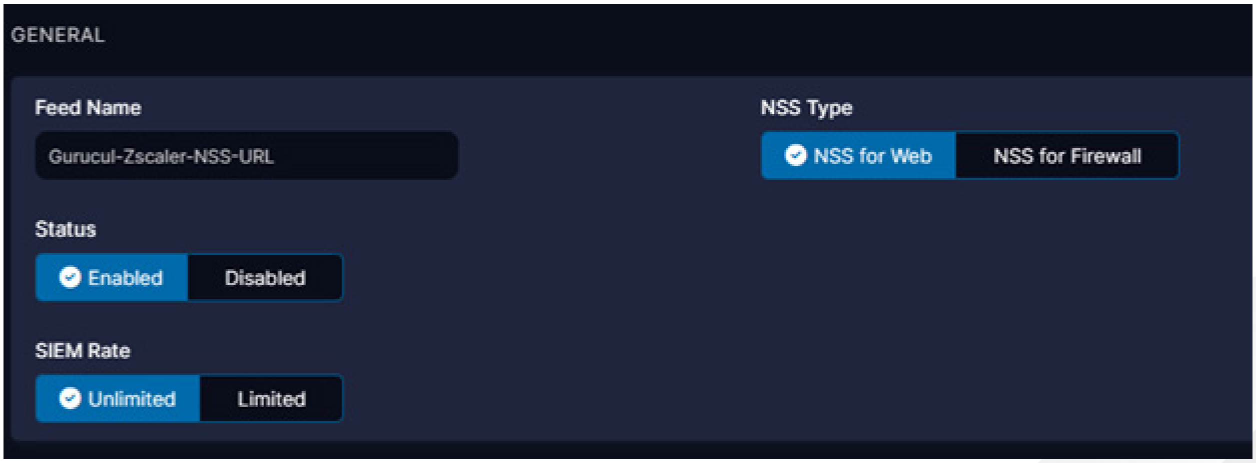
ZIA Configuration

The following sections describe how to configure ZIA.

Zscaler Cloud NSS Configuration

To set up the Cloud NSS feeds:

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **Nanolog Streaming Service** > **Cloud NSS Feeds**.
3. Click **Add Cloud NSS Feed**.
4. In the **Add Cloud NSS Feed** window, fill in the following information:
   a. For **HTTP/HTTPS Endpoint**:
      i. **Feed Name**: Desired Feed Name
      ii. **NSS Type**: NSS for Web or NSS for Firewall
      iii. **SIEM Rate**: Unlimited
      iv. **SIEM Type**: Other
      v. **OAuth 2.0 Authentication**: Off
      vi. **Max Batch Size**: 16 KB
      vii. **API URL**: Enter `GURUCUL-TENANT-HTTP-ENDPT`
      viii. **HTTP Headers**:
         - **Content-Type**: `application/x-www-form-urlencoded`
         - **Content-Encoding**: `gzip`
         - **apikey**: `<API Key from Gurucul console>`
      ix. **Log Type**:
         - For Web Logs, select **Web Log**, Tunnel, or **Admin Audit**.
         - For Firewall Logs, select **DNS Logs** or **Firewall Logs**.
      x. **Feed Output Type**: JSON
      xi. **Feed Escape Character**: Keep blank
      xii. **Timezone**: GMT



GENERAL

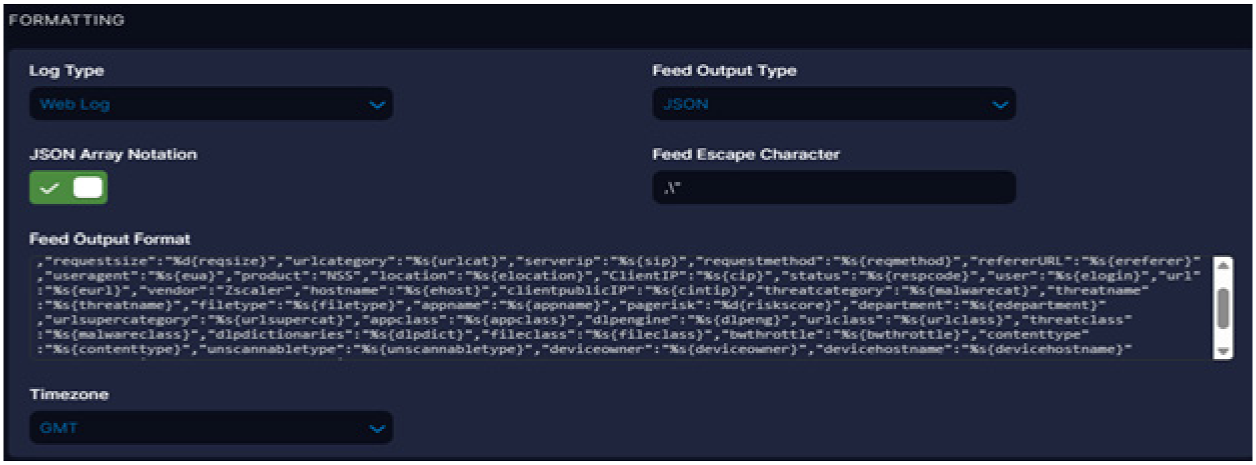
Feed Name: Gurucul-Zscaler-NSS-URL

NSS Type: ● NSS for Web | NSS for Firewall

Status: ● Enabled | Disabled

SIEM Rate: ● Unlimited | Limited

Figure 7. HTTP/HTTPS Endpoint General



FORMATTING

Log Type: Web Log

Feed Output Type: JSON

JSON Array Notation: ✓

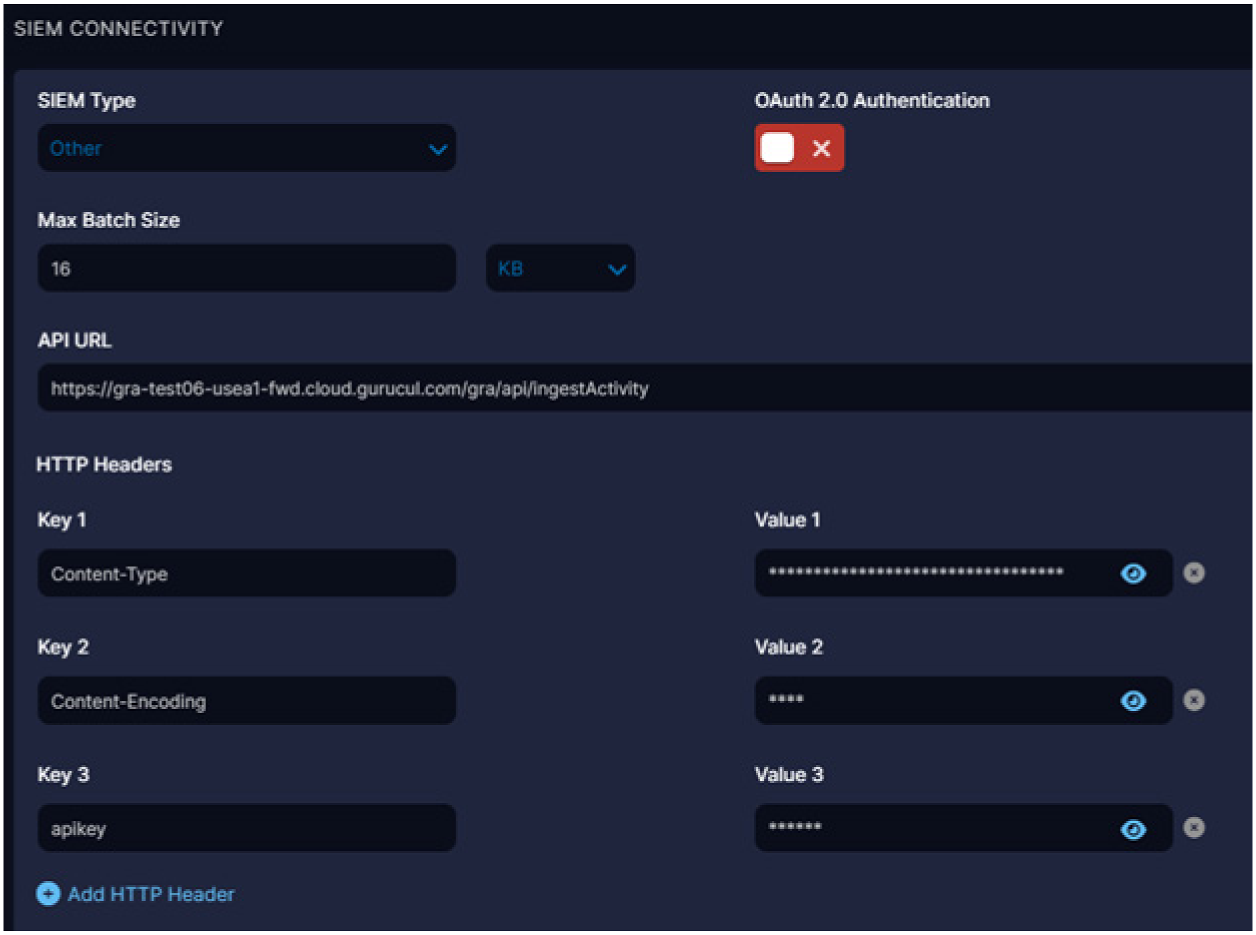
Feed Escape Character: ,\"

Feed Output Format

```
,"requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip":"%s{sip}","requestmethod":"%s{reqmethod}","refererURL":"%s{ereferer}"
,"useragent":"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP":"%s{cip}","status":"%s{respcode}","user":"%s{elogin}","url"
:"%s{eurl}","vendor":"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}","threatcategory":"%s{malwarecat}","threatname"
:"%s{threatname}","filetype":"%s{filetype}","appname":"%s{appname}","pagerisk":"%d{riskscore}","department":"%s{edepartment}"
,"urlsupercategory":"%s{urlsupercat}","appclass":"%s{appclass}","dlpengine":"%s{dlpeng}","urlclass":"%s{urlclass}","threatclass"
:"%s{malwareclass}","dlpdictionaries":"%s{dlpdict}","fileclass":"%s{fileclass}","bwthrottle":"%s{bwthrottle}","contenttype"
:"%s{contenttype}","unscannabletype":"%s{unscannabletype}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"
```

Timezone: GMT

Figure 8. HTTP/HTTPS Endpoint Formatting



SIEM CONNECTIVITY

SIEM Type: Other

OAuth 2.0 Authentication: ✗

Max Batch Size: 16 KB

API URL: https://gra-test06-usea1-fwd.cloud.gurucul.com/gra/api/ingestActivity

HTTP Headers

Key 1: Content-Type | Value 1: ************************************

Key 2: Content-Encoding | Value 2: ****

Key 3: apikey | Value 3: ******

Figure 9. HTTP/HTTPS Endpoint SIEM Connectivity

b. For S3 Bucket:

i. **Feed Name**: Desired Feed Name

ii. **NSS Type**: NSS for Web or NSS for Firewall

iii. **SIEM Rate**: Unlimited

iv. **SIEM Type**. S3

v. **AWS Access Id**: Enter the AWS Access Key for the Bucket

vi. **AWS Secret Key**: Enter the AWS Secret Key for the Bucket

vii. **Max Batch Size**: 128 KB

viii. **API URL**: `https://GURUCUL-TENANT-S3-BUCKET.s3.region-code.amazonaws.com/zscaler-cloud-nss-logs/{optional/{NSSType}/{optionalLogType}`

ix. **HTTP Headers**: `apikey: <API Key from Gurucul console>`

x. **JSON Array Notation**: False

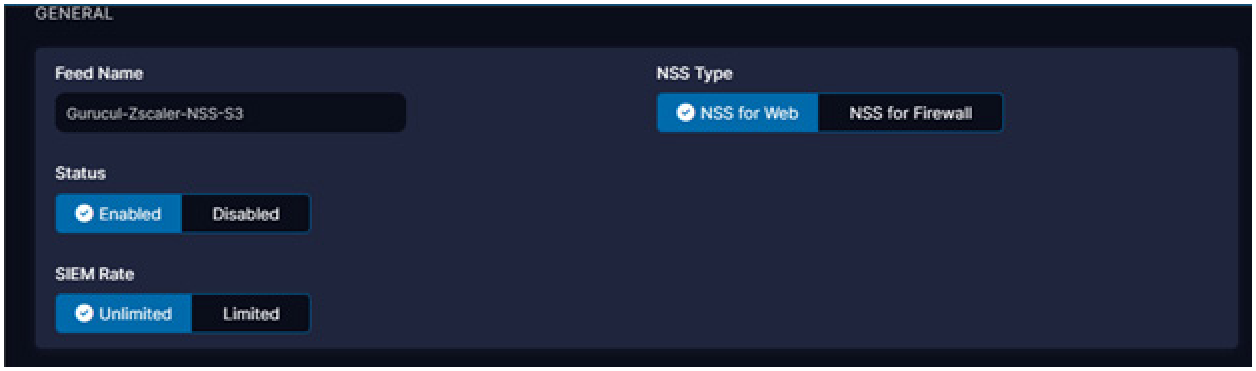
xi. **Log Type**:

- For Web Logs, select **Web Log**, **Tunnel**, or **Admin Audit**.
- For Firewall Logs, select **DNS Logs** and **Firewall Logs**.

xii. **Feed Output Type**: JSON

xiii. **Feed Escape Character**: **,** \”

xiv. **Timezone**: GMT



GENERAL

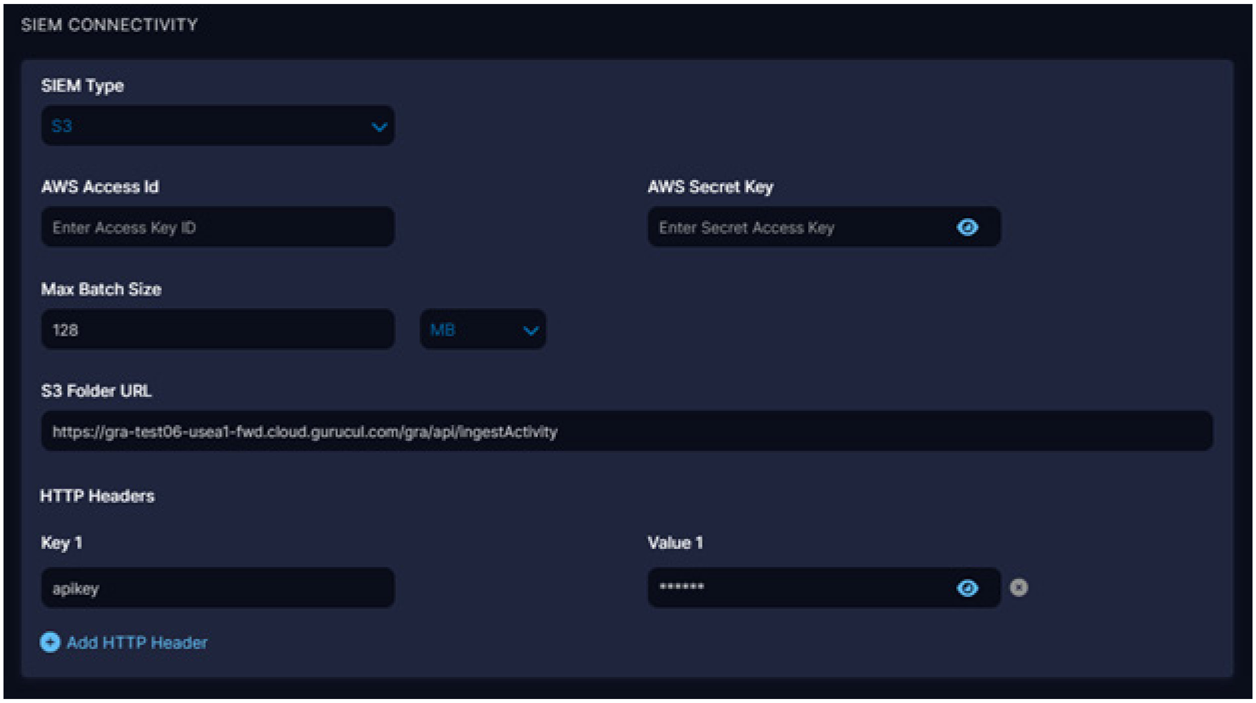
Feed Name: Gurucul-Zscaler-NSS-S3

NSS Type: ✓ NSS for Web | NSS for Firewall

Status: ✓ Enabled | Disabled

SIEM Rate: ✓ Unlimited | Limited

Figure 10. S3 Bucket General



SIEM CONNECTIVITY

SIEM Type: S3

AWS Access Id: Enter Access Key ID

AWS Secret Key: Enter Secret Access Key

Max Batch Size: 128 MB

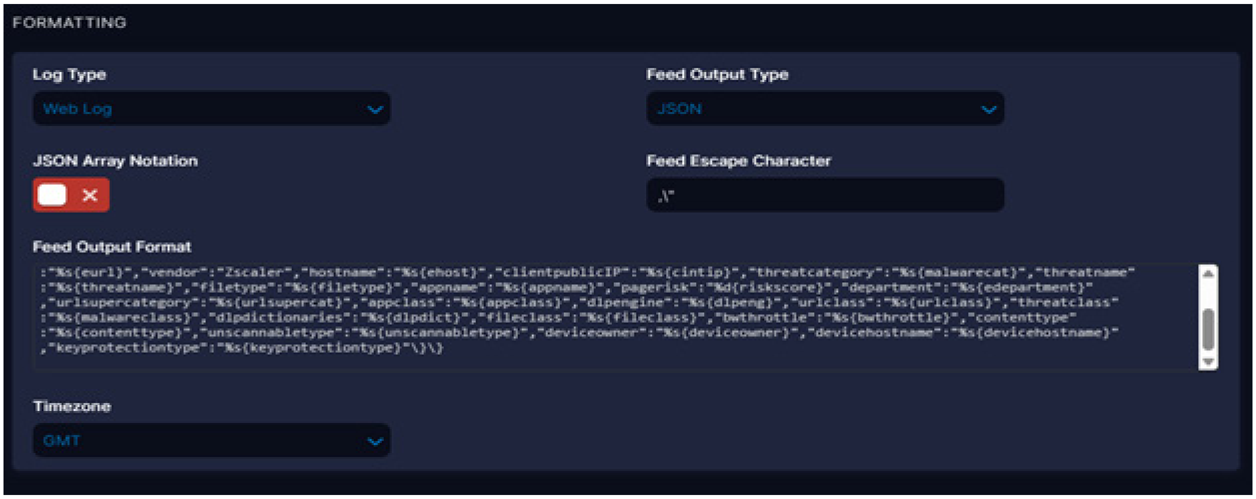
S3 Folder URL: https://gra-test06-usea1-fwd.cloud.gurucul.com/gra/api/ingestActivity

HTTP Headers

Key 1: apikey

Value 1: ******

Figure 11. S3 Bucket SIEM Connectivity



FORMATTING

Log Type: Web Log

Feed Output Type: JSON

JSON Array Notation: ☒

Feed Escape Character: .\"

Feed Output Format

```
:"%s{eurl}","vendor":"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}","threatcategory":"%s{malwarecat}","threatname"
:"%s{threatname}","filetype":"%s{filetype}","appname":"%s{appname}","pagerisk":"%d{riskscore}","department":"%s{edepartment}"
,"urlsupercategory":"%s{urlsupercat}","appclass":"%s{appclass}","dlpengine":"%s{dlpeng}","urlclass":"%s{urlclass}","threatclass"
:"%s{malwareclass}","dlpdictionaries":"%s{dlpdict}","fileclass":"%s{fileclass}","bwthrottle":"%s{bwthrottle}","contenttype"
:"%s{contenttype}","unscannabletype":"%s{unscannabletype}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"
,"keyprotectiontype":"%s{keyprotectiontype}"\}\}
```

Timezone: GMT

Figure 12. S3 Bucket Formatting

5. After the firewall or web log feed has been configured, activate the changes as needed and test the feed by going to **Administration** > **Nanolog Streaming Service** > **Cloud NSS Feeds**.
6. Click the **Cloud** icon to send a test message or file and validate the connection. Wait for the success message `Test Connectivity Successful: OK-Success (200).`

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

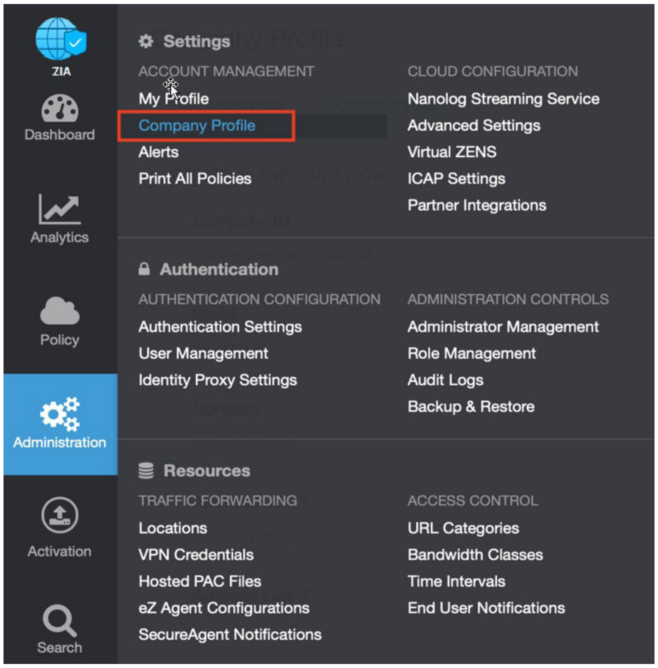
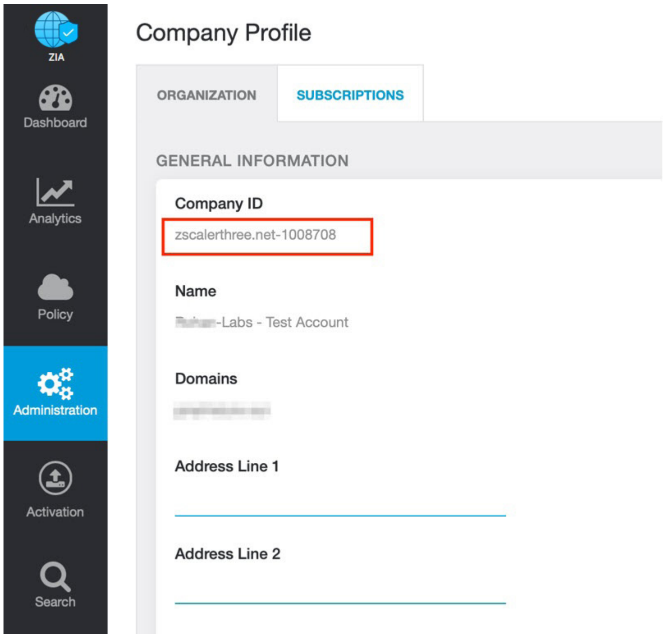


Figure 13. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 14. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

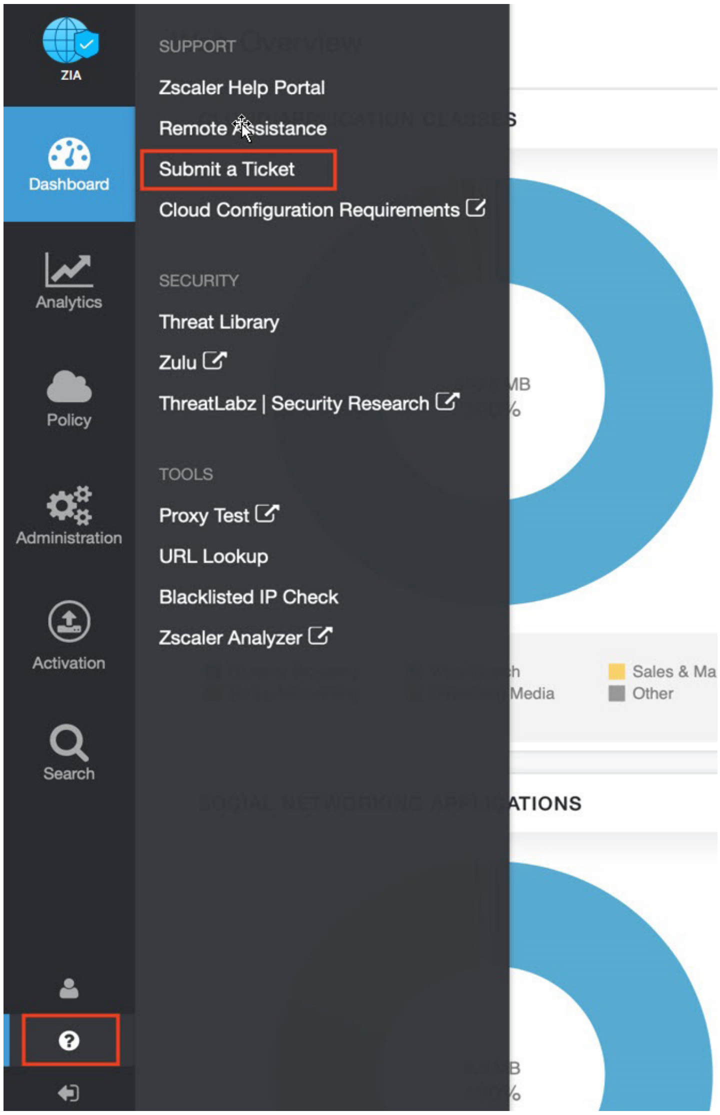


Figure 15. Submit a ticket