ZSCALER AND PANTHER DEPLOYMENT GUIDE

NOVEMBER 2024, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms 4

About This Document 6

Zscaler Overview 6

Panther Overview 6

Audience 6

Software Versions 6

Request for Comments 6

Zscaler and Panther Introduction 7

ZIA Overview 7

ZPA Overview 7

Panther Platform Overview 8

Panther Resources 8

Introduction 9

Ingesting ZIA Logs via Cloud NSS 9

Step 1: Set Up the ZIA Source in Panther 9

Step 2: Set Up an S3 Bucket 10

Step 3: Configure a Cloud NSS Feed in the ZIA Admin Portal 10

Supported Log Types 11

Zscaler.ZIA.AdminAuditLog 11

Ingesting ZPA logs 14

Step 1: Set Up a ZPA Source in Panther 14

Step 2: Create and Deploy an App Connector in ZPA 16

Step 3: Configure One or More Log Receivers 16

Supported Log Types 18

Zscaler.ZPA.AuditLog 18

Zscaler.ZPA.UserActivity 20

Zscaler.ZPA.UserStatus 28

Zscaler.ZPA.AppConnectorStatus 32

Zscaler.ZPA.AppConnectorMetrics 37

Appendix A: Requesting Zscaler Support 41

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
DDoS	Distributed Denial of Service
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)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SIEM	Security Information and Event Management
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

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.

Panther Overview

Panther is a leading provider of next-generation SIEM solutions, designed to detect and respond to security threats in real time. Leveraging a modern architecture, Panther offers speed, scale, and accuracy in threat detection, helping organizations stay ahead of cyber threats. To learn more, refer to Panther'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:

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

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 Panther Introduction

Overviews of the Zscaler and Panther 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, 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 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.

Panther Platform Overview

Panther is a cloud-native threat detection platform that helps organizations detect and respond to security threats:

- Threat detection: Panther analyzes logs in real time to detect threats as soon as they are ingested. It uses detection-as-code (DaC) to write and manage detections using software engineering best practices.
- Incident response: Panther provides enriched alerts for context to help teams quickly identify and mitigate security incidents.
- Data lake: Panther stores critical security logs in a scalable data lake that provides fast search performance on large data sets.
- Scalability: Panther’s serverless architecture autoscales with your team as it grows.
- Integration: Panther integrates with critical log sources like AWS S3, AWS CloudTrail, and AWS VPC Flow Logs.
- Ease of use: Panther’s interface centralizes and expands security and compliance operations.

Panther Resources

The following table contains links to Panther support resources.

Name	Definition
Panther Knowledge Base	Help articles on Panther.
Zscaler Integration Guide	Integration Guide for Zscaler and Panther.
S3 Integration Guide	Onboarding AWS S3 as a Data Transport log source in the Panther Console.

Introduction

Cloud NSS is an optional service managed by Zscaler and uses HTTP/HTTPS to send logs. With Cloud NSS, there is no need to deploy a VM.

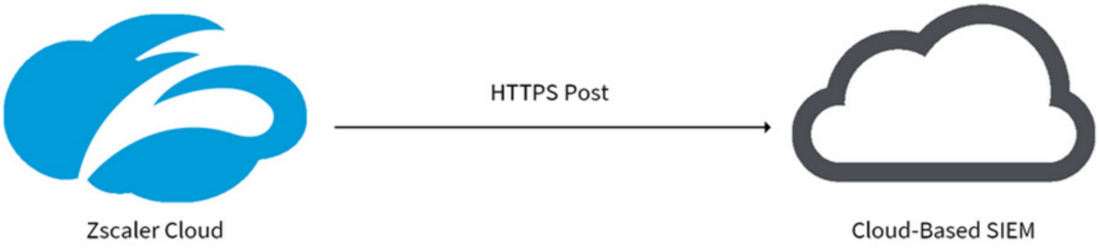


Figure 1. Zscaler Cloud NSS architecture

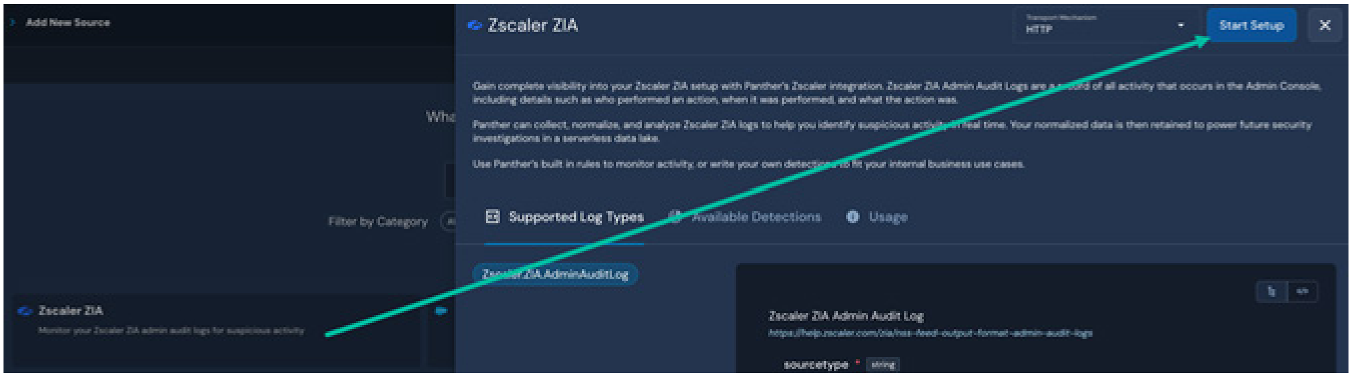
Ingesting ZIA Logs via Cloud NSS

Panther supports ingesting Zscaler Internet Access (ZIA) Admin Audit logs by using either an HTTP source or an AWS S3 bucket. To onboard the Zscaler ZIA log in Panther, you first create a Zscaler ZIA source in Panther, then configure an NSS Cloud Feed in Zscaler.

Step 1: Set Up the ZIA Source in Panther

To set up the ZIA source in Panther:

1. In the left-side pane of the Panther Console, select **Configure** > **Log Sources**.
2. In the top right, click **Create New**.
3. Search for `Zscaler ZIA`, then click that tile. You can configure Zscaler to either stream ZIA logs directly to a Panther HTTP endpoint, or to an S3 bucket in your environment, from which Panther then pulls.
4. In the Transport Mechanism drop-down menu, select the Data Transport method you want to use for this integration: **HTTP** or **AWS S3 Bucket**.
5. Click **Start Setup**.



Gain complete visibility into your Zscaler ZIA setup with Panther's Zscaler integration. Zscaler ZIA Admin Audit Logs are a record of all activity that occurs in the Admin Console, including details such as who performed an action, when it was performed, and what the action was.

Panther can collect, normalize, and analyze Zscaler ZIA logs to help you identify suspicious activity in real time. Your normalized data is then retained to power future security investigations in a serverless data lake.

Use Panther's built in rules to monitor activity, or write your own detections to fit your internal business use cases.

Zscaler ZIA Admin Audit Log

https://help.zscaler.com/zia/nss-feed-output-format-admin-audit-logs

sourcetype * string

Figure 2. Start Setup

6. Follow Panther's instructions for configuring the [Data Transport]() method you chose:
   a. **HTTP**: Follow Panther's [instructions for configuring an HTTP Source]().
      - During setup, on the security configuration page, you are required to use [shared secret authentication]().
      - Payloads sent to this source are subject to the [payload requirements for all HTTP sources]().
      - Do not proceed to the next step until the creation of your HTTP endpoint has completed.
   b. **S3**: Follow Panther's [instructions for configuring an S3 Source]().
      - Follow the [instructions on setting up an S3 source in Panther]().

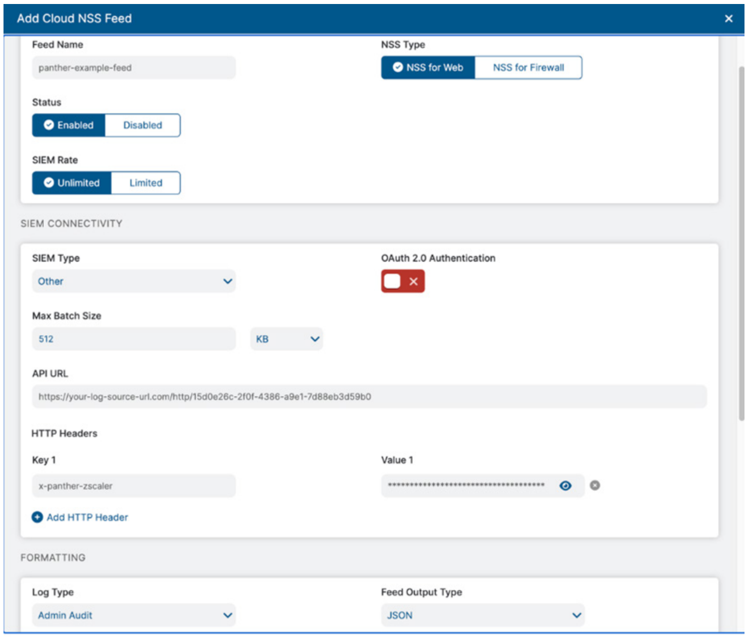
Step 2: Set Up an S3 Bucket

For AWS S3 ingest only. In the [Zscaler SaaS Security and Amazon S3 Deployment Guide](), follow the instructions in the *Integrating Zscaler Cloud NSS with Amazon S3* section. Stop when you reach the *Add a Cloud NSS Feed in the ZIA Admin Portal* section, and go to Step 3: Configure a Cloud NSS Feed in the ZIA Admin Portal.

Step 3: Configure a Cloud NSS Feed in the ZIA Admin Portal

To configure a Cloud NSS feed:

1. For an HTTP source, if you are using HTTP as your Data Transport, follow the instructions in [Adding Cloud NSS Feeds for Admin Audit Logs]() (government agencies, see [Adding Cloud NSS Feeds for Admin Audit Logs]()).
   a. **SIEM Rate**: Leave as **Unlimited**.
   b. **SIEM Type**: Select **Other**.
   c. **OAuth 2.0 Authentication**: Make sure this setting is disabled.
   d. **Max Batch Size**: Leave as-is.
   e. **API URL**: Enter the HTTP Source URL you generated in the Panther Console.
   f. **HTTP Headers**: In the **Key** field, enter `x-panther-zscaler`. In the **Value** field, enter the Shared Secret value you generated or entered in Panther.
   g. **Log Type**: Select **Admin Audit** and leave the rest of the fields as they are.



Add Cloud NSS Feed

Feed Name: panther-example-feed

NSS Type: ● NSS for Web | NSS for Firewall

Status: ● Enabled | Disabled

SIEM Rate: ● Unlimited | Limited

SIEM CONNECTIVITY

SIEM Type: Other

OAuth 2.0 Authentication: ☒

Max Batch Size: 512 KB

API URL: https://your-log-source-url.com/http/15d0e26c-2f0f-4386-a9e1-7d88eb3d59b0

HTTP Headers

Key 1: x-panther-zscaler

Value 1: ************************************

Add HTTP Header

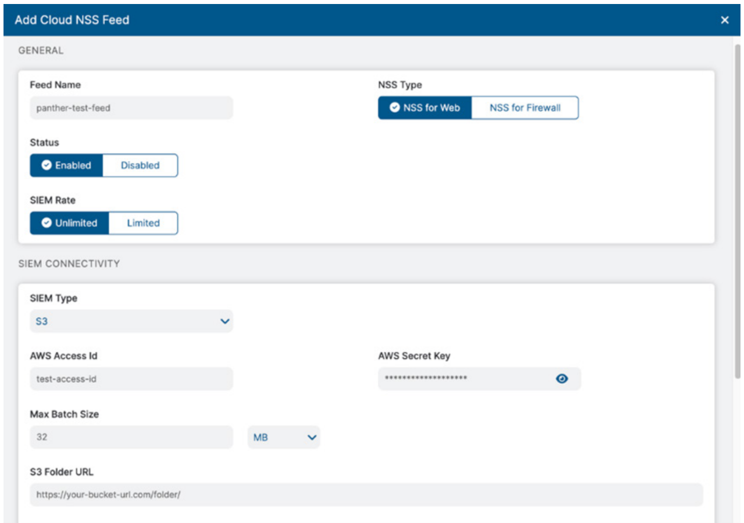
FORMATTING

Log Type: Admin Audit

Feed Output Type: JSON

Figure 3. Add Cloud NSS Feed

2. For an S3 bucket, If you are using S3 as your Data Transport, follow the *Add a Cloud NSS Feed in the ZIA Admin Portal* instructions in the **Zscaler SaaS Security and Amazon S3 Deployment Guide** (government agencies, see **Zscaler SaaS Security API and Amazon S3 Deployment Guide**):



Add Cloud NSS Feed

GENERAL

Feed Name: panther-test-feed

NSS Type: ● NSS for Web | NSS for Firewall

Status: ● Enabled | Disabled

SIEM Rate: ● Unlimited | Limited

SIEM CONNECTIVITY

SIEM Type: S3

AWS Access Id: test-access-id

AWS Secret Key: *******************

Max Batch Size: 32 MB

S3 Folder URL: https://your-bucket-url.com/folder/

Figure 4. Add Cloud NSS Feed

Supported Log Types

The following log types are supported.

Zscaler.ZIA.AdminAuditLog

The Admin Audit log records key events in the ZIA Admin Portal, such as logins, logouts, and resource actions (like create and update). The Admin Audit log is primarily used to investigate potentially suspicious activity or diagnose and troubleshoot errors.

```
schema: Zscaler.ZIA.AdminAuditLog

description: Zscaler ZIA Admin Audit Log

referenceURL: https://help.zscaler.com/zia/nss-feed-output-format-admin-audit-logs

fields:

  - name: sourcetype

    required: true

    description: The type of source generating the log event.

    type: string

  - name: event

    required: true

    description: The audit log event.

    type: object

    fields:
```

```
- name: time
  required: true
  description: The timestamp of the audit log.
  type: timestamp
  timeFormats:
    - '%a %b %e %H:%M:%S %Y'
  isEventTime: true
- name: recordid
  required: true
  description: The unique identifier for the log.
  type: string
- name: action
  required: true
  description: The action performed.
  type: string
- name: category
  description: The location in the portal where the action was performed.
  type: string
- name: subcategory
  description: The sub-location in the portal where the action was performed.
  type: string
- name: resource
  description: The specific location within a sub-category.
  type: string
- name: interface
  description: The means by which the user performed their actions.
  type: string
- name: adminid
  description: The login id of the admin who performed the action.
  type: string
  indicators:
    - email
    - actor_id
- name: clientip
  description: The source IP address for the admin.
  type: string
  indicators:
    - ip
- name: result
  description: The outcome of an action.
  type: string
- name: errorcode
  description: The error code if the action failed.
  type: string
- name: auditlogtype
  description: The Admin Audit log type.
  type: string
- name: preaction
  description: Data before any policy or configuration changes.
  type: json
- name: postaction
  description: Data after any policy or configuration changes.
  type: json
```

Ingesting ZPA logs

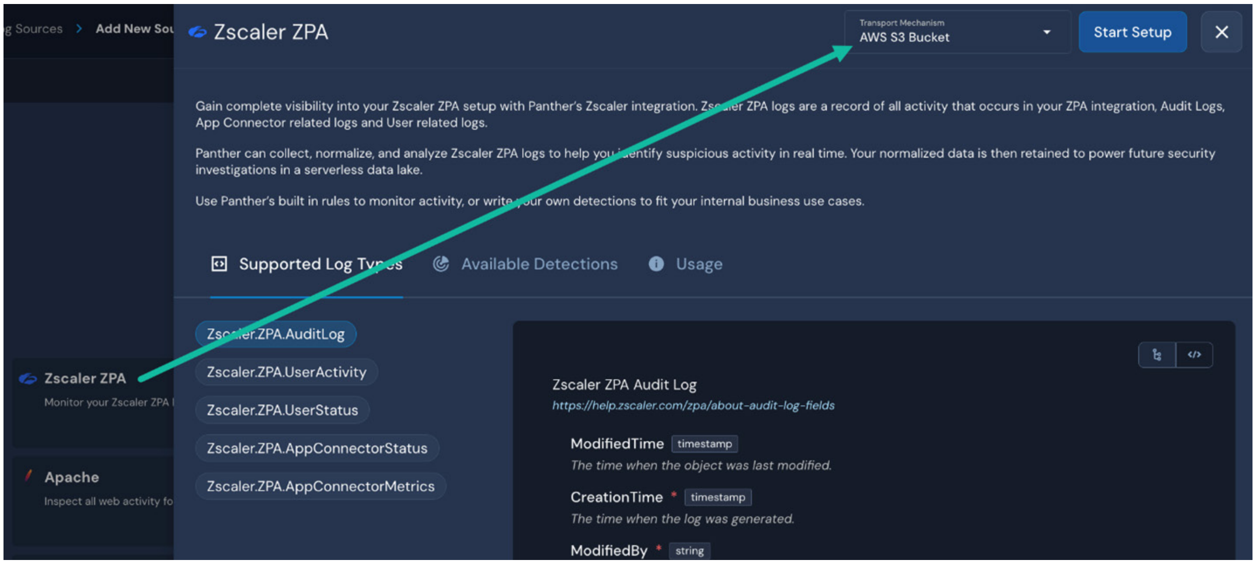
Panther supports ingesting ZPA logs by using either an HTTP or AWS S3 Data Transport source. The following ZPA log types are supported:

- Audit Log (government agencies, see Audit Log)
- User Activity (government agencies, see User Activity)
- User Status (government agencies, see User Status)
- App Connector Status (government agencies, see App Connector Status)
- App Connector Metrics (government agencies, see App Connector Metrics)

Step 1: Set Up a ZPA Source in Panther

To configure a ZPA source:

1. In the left-side navigation bar of your Panther Console, click **Configure** > **Log Sources**.
2. In the top right, click **Create New**.
3. Search for `Zscaler ZPA`, then click its tile.
4. In the **Transport Mechanism** drop-down menu of the drawer, select the Data Transport method you'd like to use for this integration: **AWS S3 Bucket** or **HTTP**. This selection depends on how you'd like to configure your Log Receiver to forward logs—either to a Panther HTTP endpoint, or to an S3 bucket in your environment, from which Panther pulls.
5. Click **Start Setup**.



Gain complete visibility into your Zscaler ZPA setup with Panther's Zscaler integration. Zscaler ZPA logs are a record of all activity that occurs in your ZPA integration, Audit Logs, App Connector related logs and User related logs.

Panther can collect, normalize, and analyze Zscaler ZPA logs to help you identify suspicious activity in real time. Your normalized data is then retained to power future security investigations in a serverless data lake.

Use Panther's built in rules to monitor activity, or write your own detections to fit your internal business use cases.

Zscaler ZPA Audit Log
https://help.zscaler.com/zpa/about-audit-log-fields

ModifiedTime timestamp
The time when the object was last modified.

CreationTime * timestamp
The time when the log was generated.

ModifiedBy * string

Figure 5. Zscaler ZPA

6. Follow Panther's instructions for configuring the Data Transport method you chose:
   a. **HTTP**: Follow Panther's instructions for configuring an HTTP Source.
      - During setup, on the security configuration page, Shared Secret is recommended for its simplicity.
      - Payloads sent to this source are subject to the payload requirements for all HTTP sources.
      - Do not proceed to the next step until the creation of your HTTP endpoint has completed.

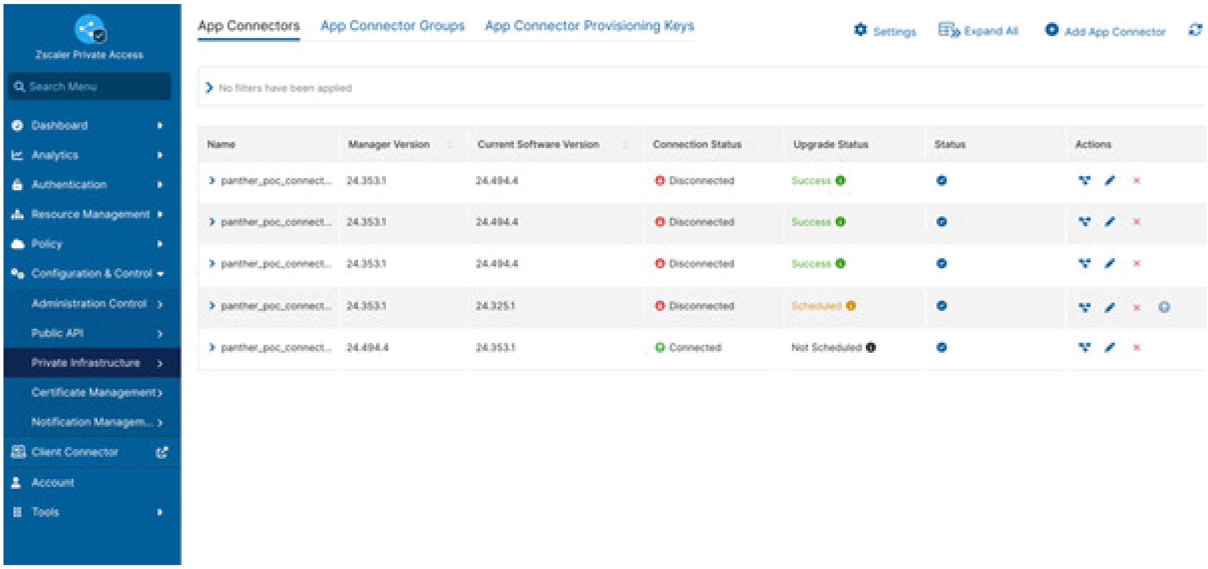
   b. **S3**: Follow Panther's instructions for configuring an S3 Source.
      - Follow the instructions on setting up an S3 source in Panther.

Step 2: Create and Deploy an App Connector in ZPA

If you already have App Connectors deployed as part of your existing Zscaler infrastructure, you can also use them for forwarding logs to Panther. In that case, you can skip this step.

To create and deploy an App Connector (government agencies, see App Connector).

1. Add an App Connector to the ZPA Admin Portal by following the instructions in Configuring App Connectors (government agencies, see Configuring App Connectors).
2. Deploy the App Connector on the supported platform (government agencies, see supported platform) of your choice by following the relevant guide within App Connector Deployment Guides for Supported Platforms (government agencies, see App Connector Deployment Guides for Supported Platforms)
    - To learn more about deployment, see About Deploying App Connectors (government agencies, see About Deploying App Connectors).
3. Monitor the status of your App Connector instances in your ZPA Admin Portal by going to **Configuration & Control** > **Private Infrastructure** > **App Connectors**.



Name	Manager Version	Current Software Version	Connection Status	Upgrade Status	Status	Actions
panther_poc_connect...	24.353.1	24.494.4	Disconnected	Success		
panther_poc_connect...	24.353.1	24.494.4	Disconnected	Success		
panther_poc_connect...	24.353.1	24.494.4	Disconnected	Success		
panther_poc_connect...	24.353.1	24.325.1	Disconnected	Scheduled		
panther_poc_connect...	24.494.4	24.353.1	Connected	Not Scheduled		

Figure 6. App Connectors

Step 3: Configure One or More Log Receivers

A Log Receiver is any storage location that can receive TCP traffic with ZPA logs from your App Connectors, then forward them to your HTTP or S3 log source in Panther.

Zscaler recommends using Fluent Bit as your Log Receiver, but you can use a different Log Receiver depending on your needs. The following instruction set assumes you are using Fluent Bit.

Deploy a Fluent Bit Service

For an S3 Bucket, if you are using S3 as your Data Transport, follow the Panther documentation. Use the TCP to Amazon S3 example on Fluent Bit Configuration Examples as a reference.

You can optionally enable TLS between your TCP input by adding the following entries to the [INPUT] variables:

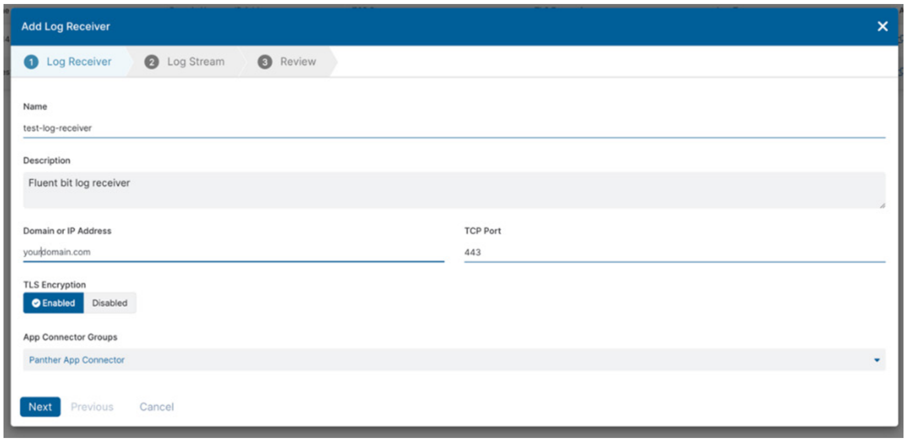
- `tls: on`
- `tls.verify: on`
- `tls.key_file: {tls_key_path}`
- `tls.cert_file: {certificate_path}`

Configure One or More Log Receivers in ZPA

You must create a separate Log Receiver for each log type you'd like to forward to Panther. For all of these log types, you can use the same Fluent Bit instance and log source (HTTP endpoint or S3 bucket) in Panther.

For each log type you'd like to ingest in Panther, add a log receiver by following the instructions in Configuring a Log Receiver (government agencies, see Configuring a Log Receiver). Take note of the following input guidelines:

- On the **Log Receiver** tab:
  - **Domain or IP Address**: Enter the domain or IP of your Fluent Bit service.
  - **TCP Port**: Enter the port where the Fluent Bit service is running.
  - **TLS Encryption**: Select **Enabled** if you require TLS encryption for the data sent to your Fluent Bit input, and you have enabled it in the Fluent Bit configuration file.



Name: test-log-receiver

Description: Fluent bit log receiver

Domain or IP Address: yourdomain.com

TCP Port: 443

TLS Encryption: ● Enabled Disabled

App Connector Groups: Panther App Connector

Figure 7. Add Log Receiver

- On the **Log Stream** tab:
  - **Log Type**: Select one of the log types supported by Panther.
  - **Log Template**: Select **JSON**.

Supported Log Types

The following log types are supported.

Zscaler.ZPA.AuditLog

The Audit log records key events in the ZPA Admin Portal, such as logins, logouts, and resource actions (like create and update). The Audit log is primarily used to investigate potentially suspicious activity or diagnose and troubleshoot errors.

```
schema: Zscaler.ZPA.AuditLog
description: Zscaler ZPA Audit Log
referenceURL: https://help.zscaler.com/zpa/about-audit-log-fields
fields:
  - name: ModifiedTime
    description: The time when the object was last modified.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: CreationTime
    required: true
    description: The time when the log was generated.
    type: timestamp
    timeFormats:
      - rfc3339
    isEventTime: true
  - name: ModifiedBy
    required: true
    description: The ID of the user who modified the object.
    type: string
  - name: RequestID
    description: The unique ID associated with the request.
    type: string
  - name: SessionID
    description: The ID of the user session.
    type: string
  - name: AuditOldValue
    description: The previous value before the change.
    type: json
  - name: AuditNewValue
    description: The new value after the change.
    type: json
  - name: AuditOperationType
    required: true
    description: The action performed.
    type: string
  - name: ObjectType
    description: The location within the ZPA Admin Portal where the Action was
performed.
    type: string
  - name: ObjectName
    description: The name of the object being affected.
    type: string
  - name: ObjectID
    description: The ID of the affected object.
    type: string
  - name: CustomerID
    description: The ZPA tenant ID of the customer.
    type: string
  - name: User
    description: The username of the admin associated with the audit action.
    type: string
    indicators:
      - email
      - username
      - actor_id
  - name: ClientAuditUpdate
```

```
    description: Indicates whether the client audit was updated. Value is either 0 or 1.

    type: bigint
```

Zscaler.ZPA.UserActivity

The User Activity log captures and records various activities performed by users when they access internal applications via the ZPA service. You can use the User Activity log to investigate unauthorized access attempts, perform compliance monitoring, and identify unusual application access patterns.

```
schema: Zscaler.ZPA.UserActivity

description: Zscaler ZPA User Activity log

referenceURL: https://help.zscaler.com/zpa/about-user-activity-log-fields

fields:

  - name: LogTimestamp

    required: true

    description: Timestamp when the log was generated.

    type: timestamp

    timeFormats:

      - ‘%a %b %e %H:%M:%S %Y’

    isEventTime: true

  - name: Customer

    required: true

    description: The name of the customer.

    type: string

  - name: SessionID

    description: The TLS session ID.

    type: string

  - name: ConnectionID

    description: The application connection ID.

    type: string

  - name: InternalReason

    required: true

    description: The internal reason for the status of the transaction.

    type: string
  - name: ConnectionStatus
    description: ‘The status of the connection. The expected values for this field are:
Open, Close, Active.’
    type: string
  - name: IPProtocol
    description: The IP protocol number.
    type: bigint
  - name: DoubleEncryption
    description: The double encryption status.
    type: bigint
  - name: Username
    required: true
    description: The user name as entered into the Zscaler Client Connector.
    type: string
    indicators:
      - username
  - name: ServicePort
    description: The service port associated with the application request.
    type: bigint
  - name: ClientPublicIP
    description: The public IP address of the Zscaler Client Connector.
    type: string
    indicators:
      - ip
  - name: ClientPrivateIP
    description: The private IP address of the Zscaler Client Connector.
    type: string
    indicators:
      - ip
  - name: ClientLatitude
    description: The latitude coordinate of the Zscaler Client Connector location.
    type: float
  - name: ClientLongitude
    description: The longitude coordinate of the Zscaler Client Connector location.
    type: float
  - name: ClientCountryCode
    description: The country code of the Zscaler Client Connector location.
    type: string
  - name: ClientZEN
    description: The ZPA Public Service Edge that received the request from the Zscaler Client Connector.
    type: string
  - name: Policy
    description: The access policy rule name.
    type: bigint
  - name: Connector
    description: The App Connector name.
    type: string
  - name: ConnectorZEN
    description: The ZPA Public Service Edge that sent the request from the App Connector.
    type: string
  - name: ConnectorIP
    description: The source IP address of the App Connector.
    type: string
    indicators:
      - ip
  - name: ConnectorPort
    description: The port number used by the connector.
    type: bigint
  - name: Host
    description: The host domain or IP address.
    type: string

    indicators:

      - hostname

  - name: Application

    description: The application name.

    type: string

  - name: AppGroup

    description: The application group name.

    type: string

  - name: Server

    description: The server ID name. The server ID will be set to zero if dynamic server discovery is enabled.

    type: string

  - name: ServerIP

    description: The destination IP address of the server.

    type: string

    indicators:

      - ip

  - name: ServerPort

    description: The destination port of the server.

    type: bigint

  - name: PolicyProcessingTime

    description: Time in microseconds taken for processing the access policy associated with the application.

    type: bigint

  - name: ServerSetupTime

    description: Time in microseconds taken for setting up connection at server.

    type: bigint

  - name: TimestampConnectionStart

    description: Timestamp when the ZPA Public Service Edge or ZPA Private Service Edge received the initial request from Zscaler Client Connector to start the connection.

    type: timestamp
```

```
    timeFormats:
      - rfc3339
  - name: TimestampConnectionEnd
    description: Timestamp when the ZPA Public Service Edge or ZPA Private Service Edge terminated the connection.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampCATx
    description: Timestamp when the central authority sent request to ZPA Public Service Edge or ZPA Private Service Edge.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampCARx
    description: Timestamp when the central authority received request from ZPA Public Service Edge or ZPA Private Service Edge.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampAppLearnStart
    description: Timestamp when ZPA services start the process to learn about an application.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampZENFirstRxClient
    description: Timestamp when the ZPA Public Service Edge received the first byte from the Zscaler Client Connector.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampZENFirstTxClient
```

```
    description: Timestamp when the ZPA Public Service Edge sent the first byte to the Zscaler Client Connector.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampZENLastRxClient
    description: Timestamp when the ZPA Public Service Edge received the last byte from the Zscaler Client Connector.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampZENLastTxClient
    description: Timestamp when the ZPA Public Service Edge sent the last byte to the Zscaler Client Connector.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampConnectorZENSetupComplete
    description: Timestamp when the ZPA Public Service Edge received request from App Connector to set up data connection.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampZENFirstRxConnector
    description: Timestamp when the ZPA Public Service Edge received the first byte from the App Connector.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampZENFirstTxConnector
    description: Timestamp when the ZPA Public Service Edge sent the first byte to the App Connector.
    type: timestamp
  timeFormats:
   - rfc3339
 - name: TimestampZENLastRxConnector
  description: The timestamp of the last received packet from the connector.
  type: timestamp
  timeFormats:
   - rfc3339
 - name: TimestampZENLastTxConnector
  description: Timestamp when the ZPA Public Service Edge sent the last byte to the
App Connector.
  type: timestamp
  timeFormats:
   - rfc3339
 - name: ZENTotalBytesRxClient
  description: The total bytes received from the Zscaler Client Connector by the ZPA
Public Service Edge.
  type: bigint
 - name: ZENBytesRxClient
  description: Bytes received from the client during the session.
  type: bigint
 - name: ZENTotalBytesTxClient
  description: The total bytes transmitted to the Zscaler Client Connector from the
ZPA Public Service Edge.
  type: bigint
 - name: ZENBytesTxClient
  description: The additional bytes transmitted to the Zscaler Client Connector since
the last transaction log.
  type: bigint
 - name: ZENTotalBytesRxConnector
  description: Total bytes received from the connector.
  type: bigint
 - name: ZENBytesRxConnector
```

```
    description: The total bytes received from the App Connector by the ZPA Public Service Edge.
    type: bigint
  - name: ZENTotalBytesTxConnector
    description: The total bytes transmitted to the App Connector from the ZPA Public Service Edge.
    type: bigint
  - name: ZENBytesTxConnector
    description: The additional bytes transmitted by the App Connector since the last transaction log.
    type: bigint
  - name: Idp
    description: The name of the identity provider (IdP) as configured in the ZPA Admin Portal.
    type: string
  - name: ClientToClient
    description: The status of the client-to-client connection.
    type: string
  - name: ClientCity
    description: The city of the client.
    type: string
  - name: MicroTenantID
    description: The Microtenant ID of the user accessing the application.
    type: string
  - name: AppMicroTenantID
    description: The Microtenant ID of the application.
    type: string
```

Zscaler.ZPA.UserStatus

The User Status log provides detailed information about the connection and status of users within the ZPA environment. It helps with monitoring users' real-time access behavior, diagnosing connectivity issues, and tracking overall system health from a user perspective.

```
schema: Zscaler.ZPA.UserStatus
description: Zscaler ZPA User Status log
referenceURL: https://help.zscaler.com/zpa/about-user-status-log-fields
fields:
  - name: LogTimestamp
    required: true
    description: Timestamp when the log was generated.
    type: timestamp
    timeFormats:
      - ‘%a %b %e %H:%M:%S %Y’
    isEventTime: true
  - name: Customer
    required: true
    description: The name of the customer.
    type: string
  - name: Username
    required: true
    description: The user name.
    type: string
    indicators:
      - username
  - name: SessionID
    description: The TLS session ID.
    type: string
  - name: SessionStatus
    description: The status of the session.
    type: string
```

```
- name: Version
  description: The Zscaler Client Connector version.
  type: string
- name: ZEN
  description: The ZPA Public Service Edge that was selected for the connection.
  type: string
- name: CertificateCN
  description: The certificate common name.
  type: string
- name: PrivateIP
  description: The private IP address of the Zscaler Client Connector.
  type: string
  indicators:
    - ip
- name: PublicIP
  required: true
  description: The public IP address of the Zscaler Client Connector.
  type: string
  indicators:
    - ip
- name: Latitude
  description: The latitude coordinate of the Zscaler Client Connector location.
  type: float
- name: Longitude
  description: The longitude coordinate of the Zscaler Client Connector location.
  type: float
- name: CountryCode
  description: The country code of the Zscaler Client Connector location.
  type: string
- name: TimestampAuthentication
```

```
    description: Timestamp when the Zscaler Client Connector was authenticated.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TimestampUnAuthentication
    description: Timestamp when the Zscaler Client Connector was unauthenticated.
    type: timestamp
    timeFormats:
      - rfc3339
  - name: TotalBytesRx
    description: The total bytes received.
    type: bigint
  - name: TotalBytesTx
    description: The total bytes transmitted.
    type: bigint
  - name: Idp
    description: The name of the identity provider (IdP) as configured in the ZPA Admin Portal.
    type: string
  - name: Hostname
    description: The name of the device as reported by the Zscaler Client Connector.
    type: string
    indicators:
      - hostname
  - name: Platform
    description: The platform on the device as reported by the Zscaler Client Connector.
    type: string
  - name: ClientType
    description: The client type for the request.
    type: string
  - name: TrustedNetworks
    description: The unique IDs for the trusted networks that the Zscaler Client Connector has determined for this device.
    type: array
    element:
      type: string
  - name: TrustedNetworksNames
    description: The names for the trusted networks that the Zscaler Client Connector has determined for this device.
    type: array
    element:
      type: string
  - name: SAMLAttributes
    description: The list of SAML attributes reported by the IdP.
    type: string
  - name: PosturesHit
    description: The posture profiles that the Zscaler Client Connector verified for this device.
    type: array
    element:
      type: string
  - name: PosturesMiss
    description: The posture profiles that the Zscaler Client Connector failed to verified for this device.
    type: array
    element:
      type: string
  - name: ZENLatitude
    description: The latitude coordinates for the ZPA Public Service Edge.
    type: float
  - name: ZENLongitude
    description: The longitude coordinates for the ZPA Public Service Edge.
    type: float

  - name: ZENCountryCode

    description: The country code for the ZPA Public Service Edge.

    type: string

  - name: FQDNRegistered

    description: The status of the hostname for the client-to-client connection.

    type: string

  - name: FQDNRegisteredError

    description: The status of the registered hostname.

    type: string

  - name: City

    description: The city of the client.

    type: string

  - name: MicroTenantID

    description: The Microtenant ID of the user accessing the application.

    type: string
```

Zscaler.ZPA.AppConnectorStatus

The App Connector Status log provides detailed information about the health, status, and operational behavior of App Connectors. Monitoring these logs helps administrators ensure that App Connectors are operating efficiently. These longs can help troubleshoot issues, maintain service reliability, and detect potential security incidents, such as attacks or misuse of applications.

```
schema: Zscaler.ZPA.AppConnectorStatus

description: Zscaler ZPA App Connector Status log

referenceURL: https://help.zscaler.com/zpa/about-connector-status-log-fields

fields:

  - name: LogTimestamp

    required: true

    description: Timestamp when the log was generated.

    type: timestamp

    timeFormats:

      - ‘%a %b %e %H:%M:%S %Y’

    isEventTime: true
```

```
- name: Customer
  required: true
  description: The name of the customer.
  type: string
- name: SessionID
  description: The TLS session ID.
  type: string
- name: SessionType
  description: The type of session.
  type: string
- name: SessionStatus
  description: The status of the session.
  type: string
- name: Version
  description: The App Connector package version.
  type: string
- name: Platform
  description: The host platform.
  type: string
- name: ZEN
  description: The ZPA Public Service Edge that was selected for the connection.
  type: string
- name: Connector
  required: true
  description: The App Connector name.
  type: string
- name: ConnectorGroup
  required: true
  description: The App Connector group name.
  type: string
```

```
- name: PrivateIP
  description: The private IP address of the App Connector.
  type: string
  indicators:
    - ip
- name: PublicIP
  description: The public IP address of the App Connector.
  type: string
  indicators:
    - ip
- name: Latitude
  description: The latitude coordinate of the App Connector location.
  type: float
- name: Longitude
  description: The longitude coordinate of the App Connector location.
  type: float
- name: CountryCode
  description: The country code.
  type: string
- name: TimestampAuthentication
  description: Timestamp when the App Connector was authenticated.
  type: timestamp
  timeFormats:
    - rfc3339
- name: TimestampUnAuthentication
  description: Timestamp when the App Connector was unauthenticated.
  type: timestamp
  timeFormats:
    - rfc3339
- name: CPUUtilization
```

```
  description: The CPU utilization in %.

  type: bigint

- name: MemUtilization

  description: The memory utilization in %.

  type: bigint

- name: ServiceCount

  description: The number of services being monitored by the App Connector.

  type: bigint

- name: InterfaceDefRoute

  description: The name of the interface to default route.

  type: string

- name: DefRouteGW

  description: The IP address of the gateway to default route.

  type: string

  indicators:

    - ip

- name: PrimaryDNSResolver

  description: The IP address of the primary DNS resolver.

  type: string

  indicators:

    - ip

- name: HostStartTime

  description: Time in seconds at which host was started.

  type: bigint

- name: ConnectorStartTime

  description: Time in seconds at which the App Connector was started.

  type: bigint

- name: NumOfInterfaces

  description: The number of interfaces on the App Connector host.

  type: bigint
```

```
- name: BytesRxInterface
  description: The bytes received on the interface.
  type: bigint
- name: PacketsRxInterface
  description: The packets received on the interface.
  type: bigint
- name: ErrorsRxInterface
  description: The errors received on the interface.
  type: bigint
- name: DiscardsRxInterface
  description: The discards received on the interface.
  type: bigint
- name: BytesTxInterface
  description: The bytes transmitted on the interface.
  type: bigint
- name: PacketsTxInterface
  description: The packets transmitted on the interface.
  type: bigint
- name: ErrorsTxInterface
  description: The errors transmitted on the interface.
  type: bigint
- name: DiscardsTxInterface
  description: The discards transmitted on the interface.
  type: bigint
- name: TotalBytesRx
  description: The total bytes received.
  type: bigint
- name: TotalBytesTx
  description: The total bytes transmitted.
  type: bigint
- name: MicroTenantID
  description: The Microtenant ID of the user accessing the application.
  type: string
```

Zscaler.ZPA.AppConnectorMetrics

The App Connector Metrics log provides detailed information about the operational status and performance of an App Connector. Monitoring these logs can help administrators diagnose key security cases such as resource exhaustion (e.g., DDoS attacks), unauthorized access, data exfiltration attempts, and compromised connectors.

```
schema: Zscaler.ZPA.AppConnectorMetrics
description: Zscaler ZPA App Connector Metrics log
referenceURL: https://help.zscaler.com/zpa/about-app-connector-metrics-log-fields
fields:
  - name: LogTimestamp
    required: true
    description: Timestamp when the log was generated.
    type: timestamp
    timeFormats:
      - ‘%a %b %e %H:%M:%S %Y’
    isEventTime: true
  - name: Connector
    required: true
    description: The App Connector name.
    type: string
  - name: CPUUtilization
    description: The maximum CPU usage in the past 5 minutes.
    type: bigint
  - name: SystemMemoryUtilization
    description: The memory utilization of the entire VM.
    type: bigint
  - name: ProcessMemoryUtilization
    description: The memory utilization of the App Connector process.
    type: bigint
  - name: AppCount
    required: true
    description: The number of Applications configured for access via this App
Connector.
    type: bigint
  - name: ServiceCount
    description: The number of services configured for access via this App Connector.
    type: bigint
  - name: TargetCount
    description: The number of targets configured for access via this App Connector.
    type: bigint
  - name: AliveTargetCount
    description: The number of targets alive for access via this App Connector.
    type: bigint
  - name: ActiveConnectionsToPublicSE
    description: The number of active Microtunnel (M-tunnel) connections to the ZPA
Public Service Edge.
    type: bigint
  - name: DisconnectedConnectionsToPublicSE
    description: The number of disconnected Microtunnel (M-tunnel) connections to the
ZPA Public Service Edge.
    type: bigint
  - name: ActiveConnectionsToPrivateSE
    description: The number of active Microtunnel (M-tunnel) connections to the ZPA
Private Service Edge.
    type: bigint
  - name: DisconnectedConnectionsToPrivateSE
    description: The number of disconnected Microtunnel (M-tunnel) connections to the
ZPA Private Service Edge.
    type: bigint
  - name: TransmittedBytesToPublicSE
    description: The number of bytes transmitted by the App Connector to the ZPA Public
Service Edge.
```

```
    type: bigint
  - name: ReceivedBytesFromPublicSE
    description: The number of bytes received by the App Connector from the ZPA Public
Service Edge.
    type: bigint
  - name: TransmittedBytesToPrivateSE
    description: The number of bytes transmitted by the App Connector to the ZPA
Private Service Edge.
    type: bigint
  - name: ReceivedBytesFromPrivateSE
    description: The number of bytes received by the App Connector from the ZPA Private
Service Edge.
    type: bigint
  - name: AppConnectionsCreated
    description: The number of created application Microtunnel (MTunnel) connections.
    type: bigint
  - name: AppConnectionsCleared
    description: The number of cleared application Microtunnel (MTunnel) connections.
    type: bigint
  - name: AppConnectionsActive
    description: The number of active application Microtunnel (MTunnel) connections.
    type: bigint
  - name: UsedTCPPortsIPv4
    description: The number of used TCP ports for an IPv4 connection.
    type: bigint
  - name: UsedUDPPortsIPv4
    description: The number used UDP ports for an IPv4 connection.
    type: bigint
  - name: UsedTCPPortsIPv6
    description: The number of used TCP ports for an IPv6 connection.
    type: bigint
  - name: UsedUDPPortsIPv6
    description: The number of used UDP ports for an IPv6 connection.
    type: bigint
  - name: AvailablePorts
    description: The number of usable ports.
    type: bigint
  - name: SystemMaximumFileDescriptors
    description: The number of total App Connector system file descriptors.
    type: bigint
  - name: SystemUsedFileDescriptors
    description: The number of used App Connector system file descriptors.
    type: bigint
  - name: ProcessMaximumFileDescriptors
    description: The number of total App Connector process file descriptors.
    type: bigint
  - name: ProcessUsedFileDescriptors
    description: The number of used App Connector process file descriptors.
    type: bigint
  - name: AvailableDiskBytes
    description: The number of free bytes available for an App Connector.
    type: bigint
  - name: MicroTenantID
    description: The Microtenant ID of the App Connector.
    type: string
```

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**.

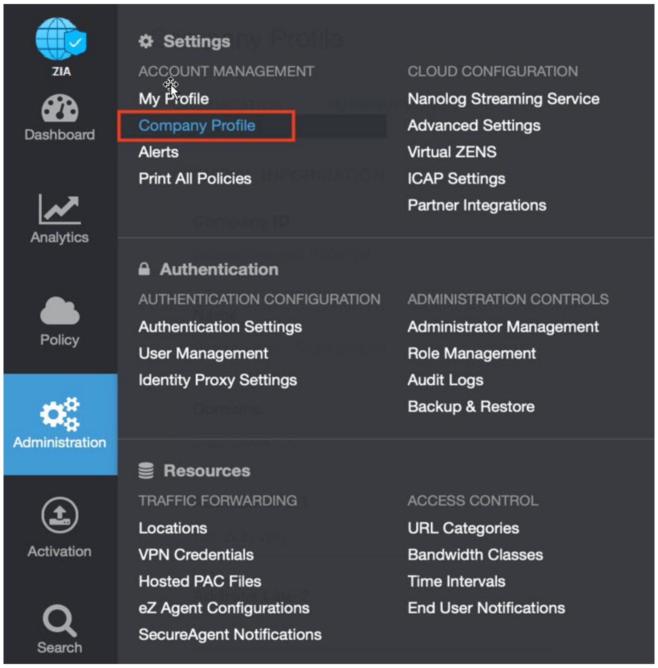
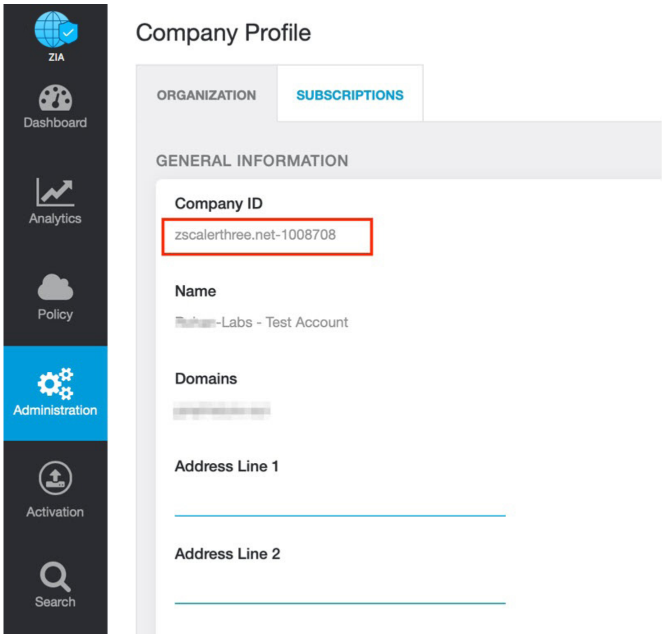


Figure 8. Collecting details to open support case with Zscaler TAC

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 9. Company ID

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

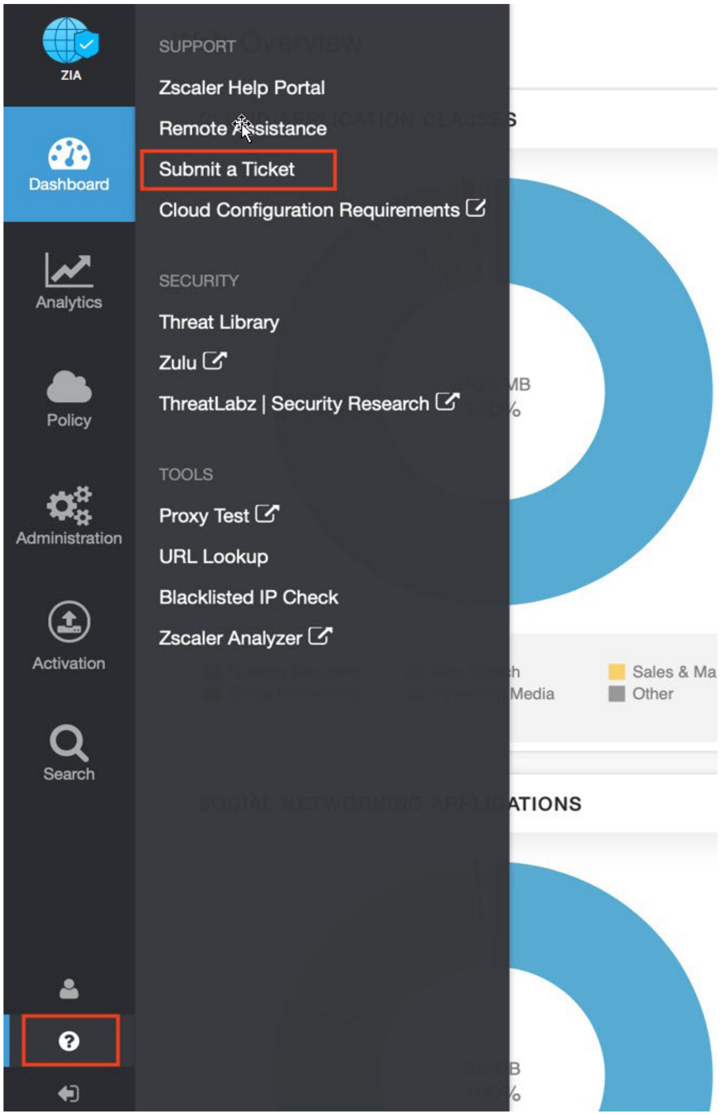


Figure 10. Submit a ticket