ZSCALER AND SEKOIA DEPLOYMENT GUIDE

OCTOBER 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)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
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.

Sekoia Overview

Sekoia is a European cybersecurity SaaS company, whose mission is to develop the best protection capabilities against cyberattacks. The company, created in France, provides modern technologies, proven in the field to enable its major account customers and cybersecurity service providers to neutralize cyber threats before they have consequences. To learn more, refer to Sekoia'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
- Sekoia 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 Sekoia Introduction

Overviews of the Zscaler and Sekoia 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.

Zscaler Resources

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
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.
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.

Sekoia XDR Overview

Sekoia.io XDR leverages Cyber Threat Intelligence to combine anticipation with automated incident response. It allows you to integrate and analyze the events and alerts produced by your applications, endpoints, cloud and SaaS perimeters in real time, and it is designed with the sole purpose of protecting your assets from potential cyber threats.

Sekoia Resources

The following table contains links to Sekoia support resources.

Name	Definition
Sekoia.io XDR Help Portal	Help articles and documentation on Sekoia.io XDR.
Zscaler ZIA Integration Guide	Integration guide.

Introduction

This document describes how to integrate Sekoia XDR with ZIA. ZIA sends logs out via two different mechanisms: NSS and Cloud NSS. NSS uses Syslog over TCP, which requires the deployment of a Zscaler NSS VM.

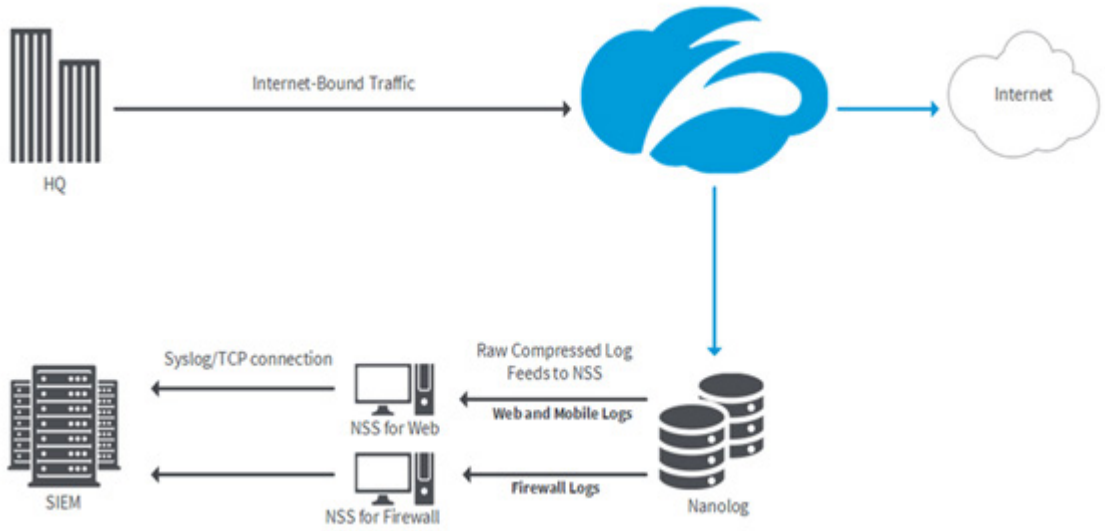

Figure 1. Zscaler NSS architecture

Deploy your collector on the same subnet as the NSS VM since NSS VM doesn't encrypt data outbound towards your collector.

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

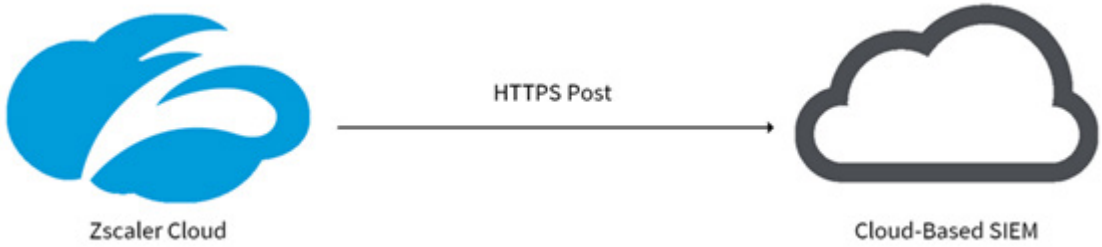

Figure 2. Cloud NSS (no VM)

Sekoia XDR Setup

To configure Sekoia XDR:

1. Log in to your instance of Sekoia XDR.

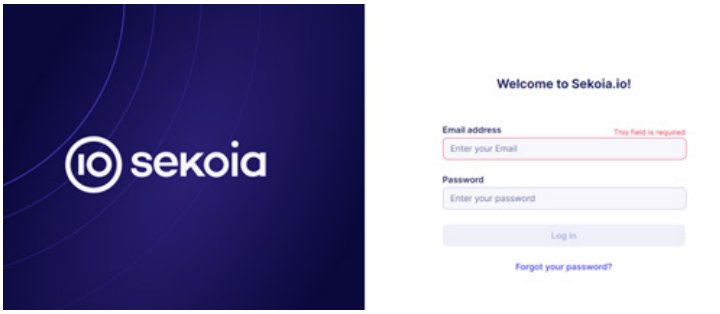

Figure 3. Log in to Sekoia

2. Go to **Intakes** > **New Intake** (at top right corner).

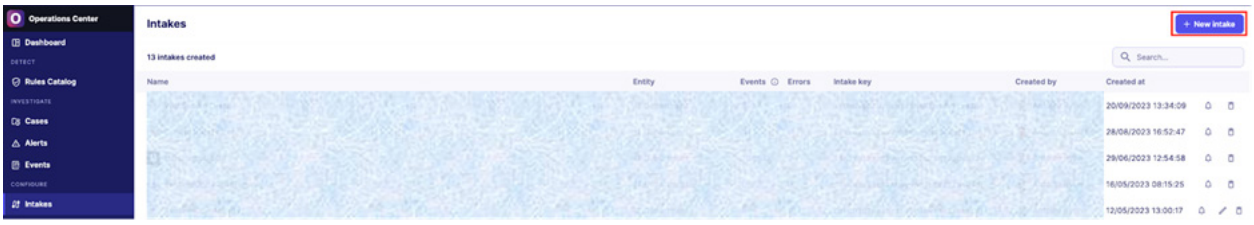

Figure 4. New Intakes

3. Select the **Zscaler Internet Access** format.

Figure 5. Zscaler Internet Access format

4. Define a name for the Intake and associated entity and click **Create**.

Intake is now created and associated Intake Key is available. This integration ingests the following Zscaler ZIA logs:

- Admin Audit
- DNS logs
- Firewall Logs
- SaaS Security
- SaaS Security Activity
- Tunnel
- Web Log

Zscaler NSS Setup

This section explains how to forward Zscaler ZIA events to Sekoia XDR.

Option 1: Forward Events with NSS Servers

You must have an internal log concentrator to forward events with NSS servers.

To configure forwarding:

1. From the ZIA Admin Portal, go to **Administration** > **Cloud Configuration** > **Nanolog Streaming Service**.

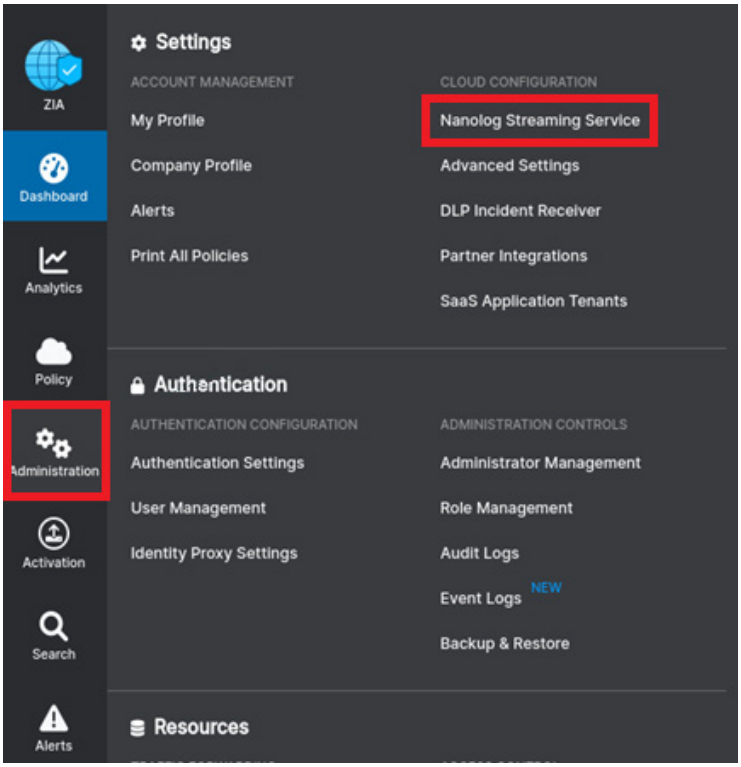

Figure 6. Nanolog Streaming Service

2. According to your tenant configuration, select the **NSS Feeds** tab.
3. Click **Add NSS Feed** for each type of log type you want forwarded.

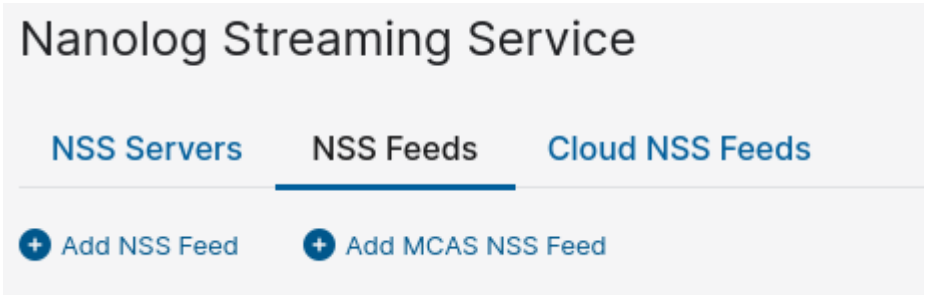

Figure 7. NSS Feeds

4. Type a **Name** for the feed.
5. Select the **NSS Server**.
6. Set the **Status** to **Enabled**.
7. Enter the **SIEM IP Address** and the **SIEM TCP Port** as the IP address and port of the log concentrator.

8. Select the **Log Type**.
9. Select **Custom** as the **Feed Output Type**. When possible, enter **,\"** (comma, backslash, quote) as the **Feed Escape Character**.
10. For **Feed Output Format**, paste the following format according to the **Log Type**:

    Weblogs:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss \{ "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}","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}","keyprotectiontype":"%s{keyprotectiontype}"\}\}
```

    SaaS Security:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss \{ "sourcetype" : "zscalernss-casb", "event" :\{"datetime":"%s{time}","recordid":"%d{recordid}","company":"%s{company}","tenant":"%s{tenant}","login":"%s{user}","dept":"%s{department}","applicationname":"%s{applicationname}","filename":"%s{filename}","filesource":"%s{filesource}","filemd5":"%s{filemd5}","threatname":"%s{threatname}","policy":"%s{policy}","dlpdictnames":"%s{dlpdictnames}","dlpdictcount":"%s{dlpdictcount}","dlpenginenames":"%s{dlpenginenames}","fullurl":"%s{fullurl}","lastmodtime":"%s{lastmodtime}","filescantimems":"%d{filescantimems}","filedownloadtimems":"%d{filedownloadtimems}"\}\}
```

    SaaS Security Activity:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss \{ "sourcetype" : "zs-calernss-casb", "event" :\{"login":"%s{username}","tenant":"%s{tenant}","object_type":"%d{objtype1}","applicationname":"%s{appname}","object_name_1":"%s{objnames1}","object_name_2":"%s{objnames2}"\}\}
```

    Tunnel IKE Phase 1:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss \{ "sourcetype" : "zscalernss-tunnel", "event" : \{"datetime":"%s{datetime}","Recordtype":"%s{tunnelactionname}","tunneltype":"IPSEC IKEV %d{ikeversion}","user":"%s{vpncredentialname}","location":"%s{elocationname}","sourceip":"%s{sourceip}","destinationip":"%s{destvip}","sourceport":"%d{srcport}","destinationport":"%d{dstport}","lifetime":"%d{lifetime}","ikeversion":"%d{ikeversion}","spi_in":"%lu{spi_in}","spi_out":"%lu{spi_out}","algo":"%s{algo}","authentication":"%s{authentication}","authtype":"%s{authtype}","recordid":"%d{recordid}"\}\}
```


Tunnel IKE Phase 2:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss \{ "sourcetype" : "zscalernss-tunnel", "event" : \{"datetime":"%s{datetime}","Recordtype":"%s{tunnelactionname}","tunneltype":"IPSEC IKEV %d{ikeversion}","user":"%s{vpncredentialname}","location":"%s{elocationname}","sourceip":"%s{sourceip}","destinationip":"%s{destvip}","sourceport":"%d{srcport}","sourceportstart":"%d{srcportstart}","destinationportstart":"%d{destportstart}","srcipstart":"%s{srcipstart}","srcipend":"%s{srcipend}","destinationipstart":"%s{destipstart}","destinationipend":"%s{destipend}","lifetime":"%d{lifetime}","ikeversion":"%d{ikeversion}","lifebytes":"%d{lifebytes}","spi":"%d{spi}","algo":"%s{algo}","authentication":"%s{authentication}","authtype":"%s{authtype}","protocol":"%s{protocol}","tunnelprotocol":"%s{tunnelprotocol}","policydirection":"%s{policydirection}","recordid":"%d{recordid}"\}\}
```

Tunnel:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss \{ "sourcetype" : "zscalernss-tunnel", "event" : \{"datetime":"%s{datetime}","Recordtype":"%s{tunnelactionname}","tunneltype":"%s{tunneltype}","user":"%s{vpncredentialname}","location":"%s{elocationname}","sourceip":"%s{sourceip}","destinationip":"%s{destvip}","sourceport":"%d{srcport}","event":"%s{event}","eventreason":"%s{eventreason}","recordid":"%d{recordid}"\}\}
```

Admin Audit:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss \{ "sourcetype" : "zscalernss-audit", "event" :\{"time":"%s{time}","recordid":"%d{recordid}","action":"%s{action}","category":"%s{category}","subcategory":"%s{subcategory}","resource":"%s{resource}","interface":"%s{interface}","adminid":"%s{adminid}","clientip":"%s{clientip}","result":"%s{result}","errorcode":"%s{errorcode}","auditlogtype":"%s{auditlogtype}","preaction":"%s{epreaction}","postaction":"%s{epostaction}"\}\}
```

11. Click **Save**.

Option 2: Forward events with Cloud NSS Feed

From the ZIA Admin Portal:

1. Go to **Administration** > **Cloud Configuration** > **Nanolog Streaming Service**.

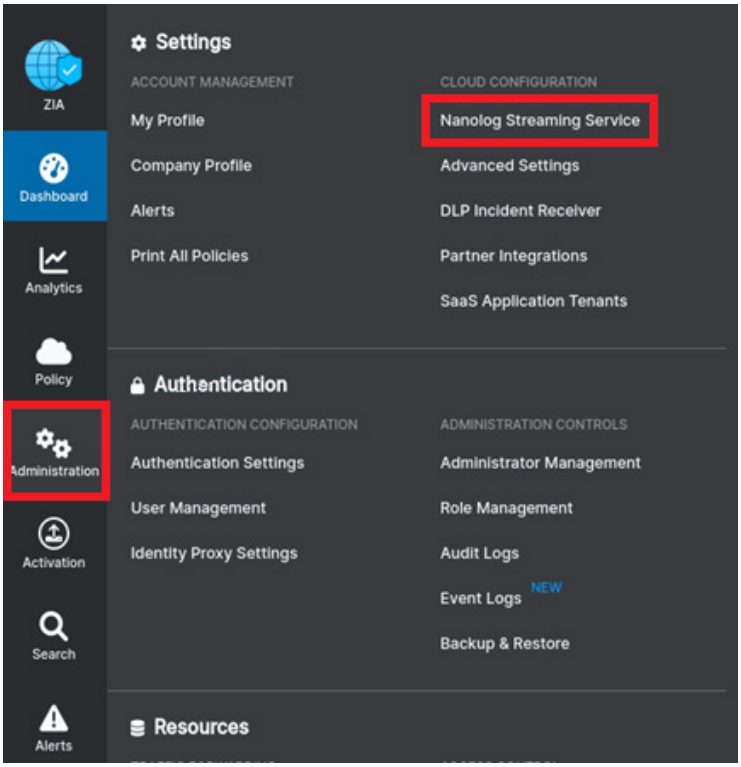

Figure 8. Nanolog Streaming Service

2. According to your tenant configuration, select the **Cloud NSS Feeds** tab.
3. Click **Add Clous NSS Feed** for each type of log type you want to forward.

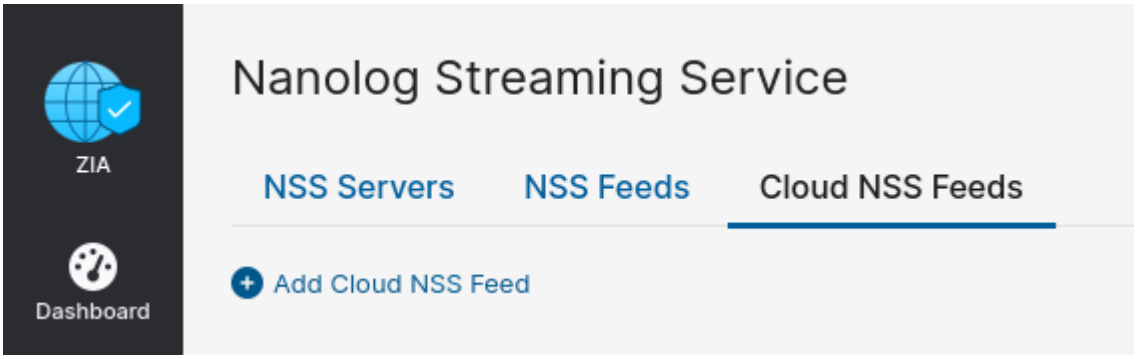

Figure 9. Cloud NSS Feeds

4. In the **General** section, enter a **Feed Name** and set the **Status** to **Enabled**. According to the log type you want to forward, select the **NSS Type**:
   a. For **Admin Audit**, **SaaS Security**, **SaaS Security Activity**, and **Web Log**, select **NSS for Web**.

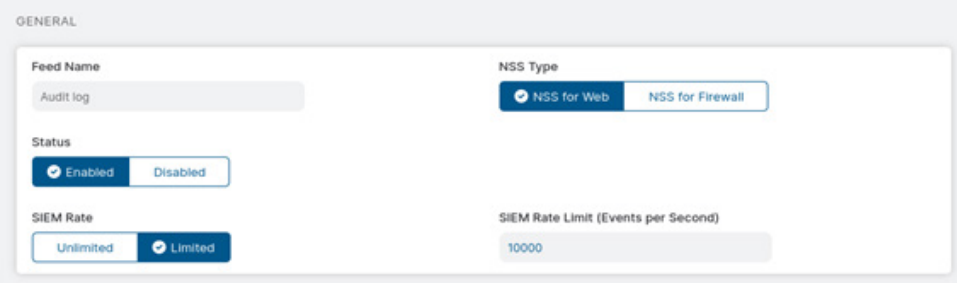

Figure 10. NSS for Web

   b. For **Firewall Logs** or **DNS Logs**, select **NSS for Firewall**.

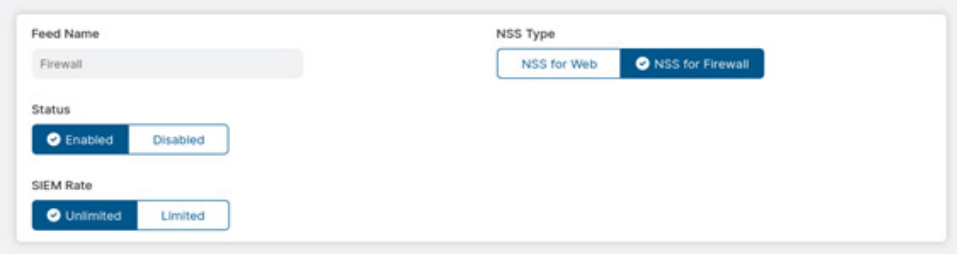

Figure 11. NSS for Firewall

5. In the SIEM Connectivity section:
   a. Select **Other** as the **SIEM Type**.
   b. Deselect **OAUTH2.0 Authentication**.
   c. Enter `512` for the **Max Batch Size**.
   d. For the **API URL**, enter `https://intake.sekoia.io/plain/batch?status_code=200`.
   e. Click **Add HTTP Header** and add the HTTP header `X-SEKOIAIO-INTAKE-KEY` with the intake key as the value (available after intake creation in Sekoia.io).

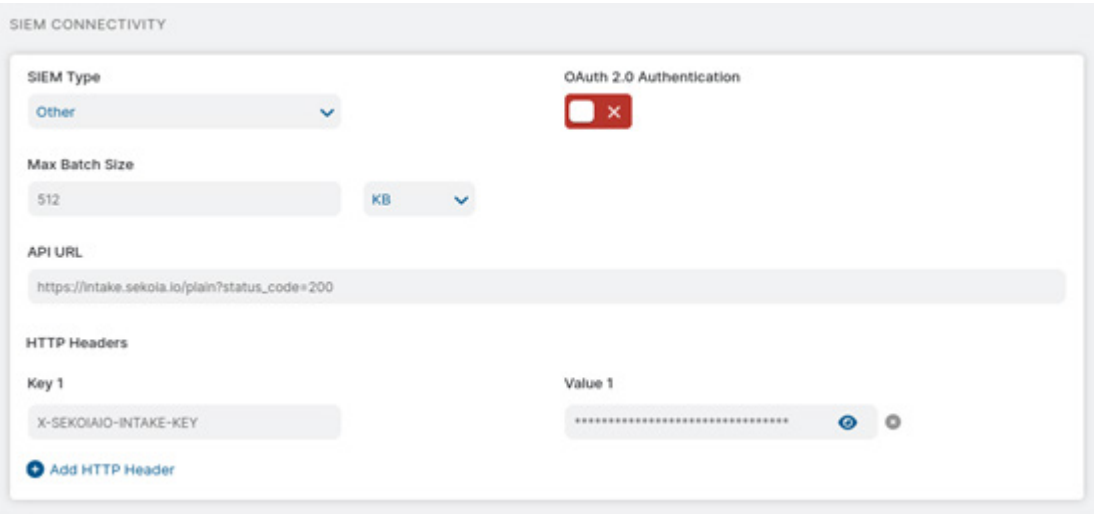

Figure 12. SIEM Connectivity

6. In the **Formatting** section:
   a. Select the **Log Type**.
   b. Select **JSON** as the **Feed Output Type**.
   c. Deselect **JSON Array Notation**.
   d. Enter **,** \" (comma, backslash, quote) for the **Feed Escape Character**.
   e. Keep the **Feed Output Format** unchanged.
   f. Set **Timezone** to **GMT**.

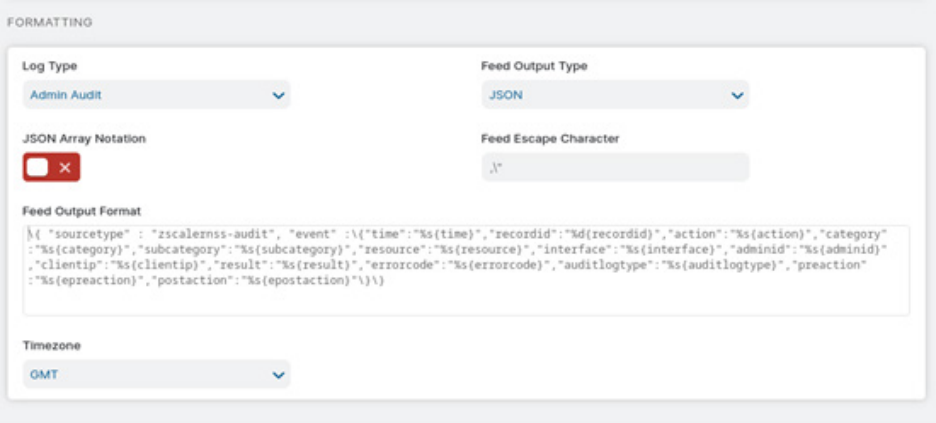

Figure 13. Formatting

7. Click **Save**.
8. **Activate** changes.

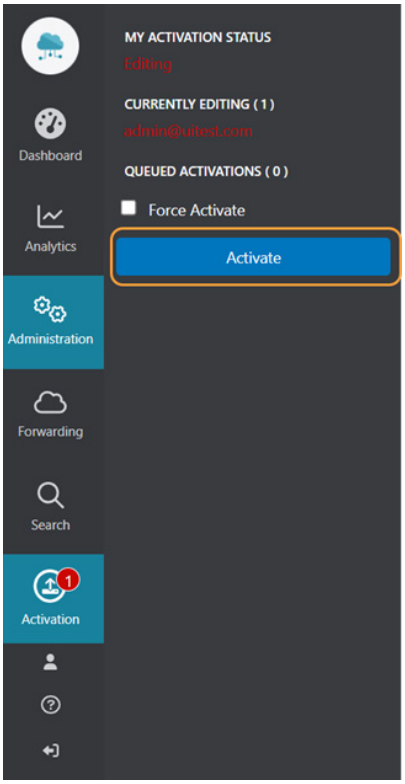

Figure 14. Activate changes

9. Click the **Cloud** icon to test connectivity.

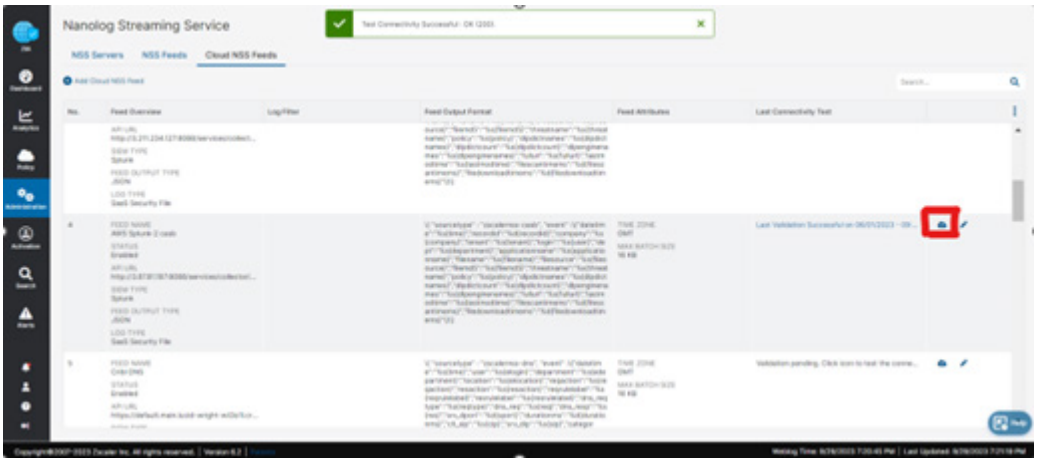

Figure 15. Check connectivity

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**.

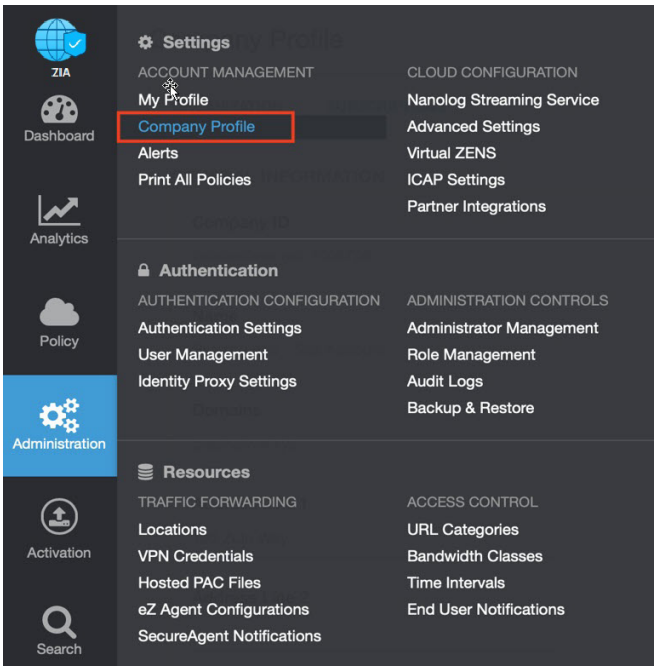

Figure 16. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

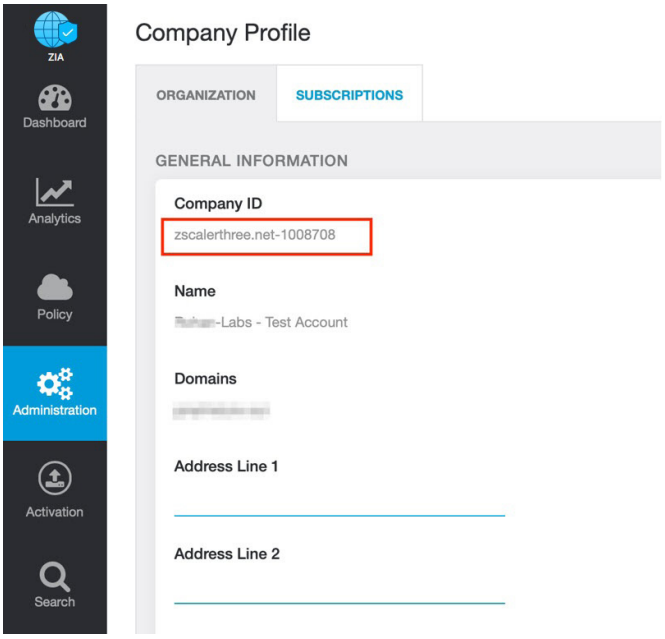

Figure 17. Company ID

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

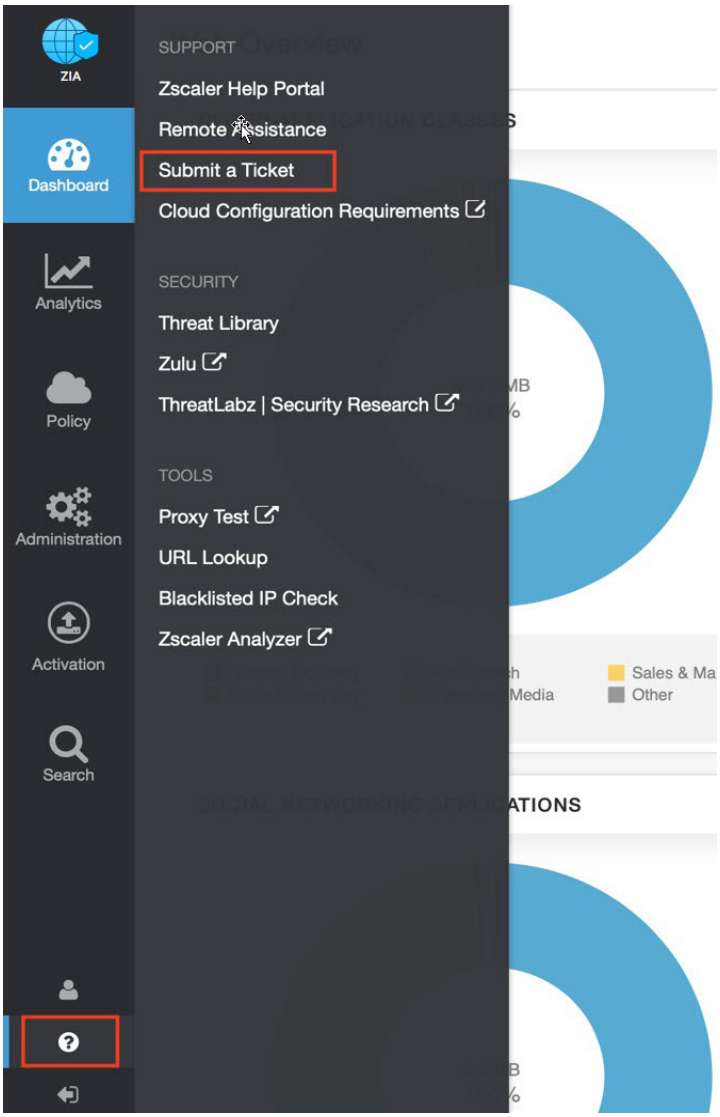

Figure 18. Submit a ticket

