ZSCALER AND LIVING SECURITY DEPLOYMENT GUIDE

AUGUST 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.

Living Security Overview

Living Security is a global leader in human risk management. Living Security transforms human risk into proactive defense by quantifying human risk to engage the human with relevant content and communications to truly change human behavior. Living Security solves the challenges of human risk through risk identification, awareness, training, and risk reduction all through an integrated platform. Living Security is trusted by security-minded organizations like MasterCard, Verizon, Biogen, AmerisourceBergen, Hewlett Packard, and more.

To learn more, refer to the Living Security 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
- Living Security 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 Living Security Introduction

Overviews of the Zscaler and Living Security 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 representative.

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.

Living Security Human Risk Management Platform Overview

The Human Risk Management Platform uses your organization's data from existing technology platforms to deliver unique, actionable insights to prioritize resources, focus efforts, and proactively decrease human risk. As you minimize human risk exposure, you reduce overall risk to your organization.

By understanding the context and risk level of individuals or teams, you can deploy training only to those who actually need it. Positive reinforcement and healthy competition help you cultivate and reinforce a vigilant security culture. By engaging the workforce with risk mitigation targeted to an individual's behaviors, scorecards, and risk, they more clearly understand the impact of their actions in the moment and make lasting behavior changes.

Living Security Resources

The following table contains links to Living Security support resources.

Name	Definition
Living Security Tech Support	Online tech support for Living Security solutions.
Living Security Online Community	Online community for Living Security users.

Living Security Unify Data and Zscaler ZIA Cloud NSS Integration

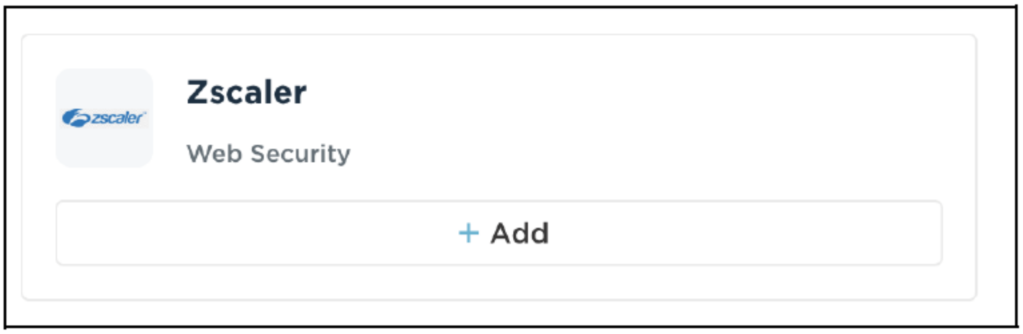
The following instructions detail how to integrate Zscaler ZIA with Living Security Unify.

Configure the Zscaler Integration in Living Security Unify

The first step is setting up a Zscaler integration in Unify so that a Zscaler Cloud NSS feed has the details needed to push data to Unify.

As an authorized Unify Admin:

1. Log in to Unify.
2. Go to **Integrations**.
3. Locate **Zscaler** in the list of available integrations, and click **Add**.

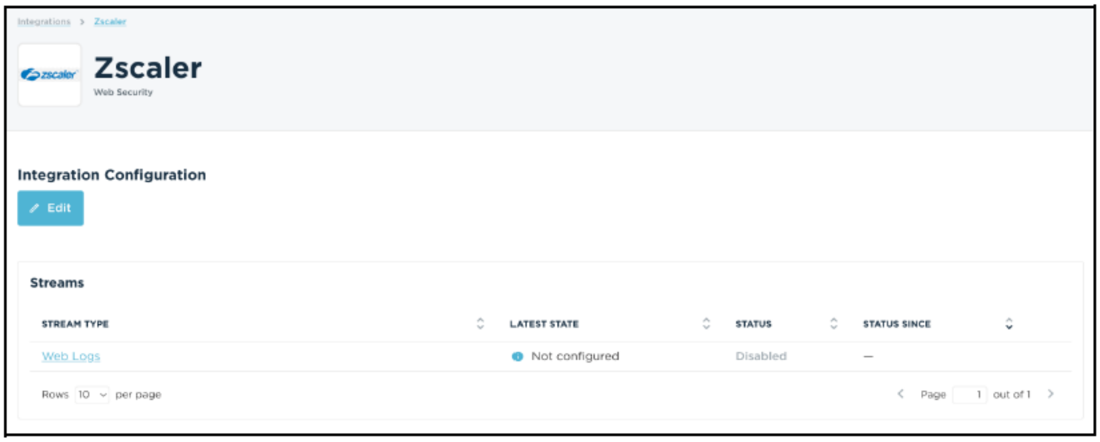


Zscaler

Web Security

Figure 1. Add Zscaler integration

4. Click the Web Logs stream from the list of available streams.



Zscaler

Web Security

Integration Configuration

Streams

STREAM TYPE	LATEST STATE	STATUS	STATUS SINCE
Web Logs	● Not configured	Disabled	—

Rows 10 per page

Page 1 out of 1

Figure 2. Available Streams

5. Click **Enable Stream**.

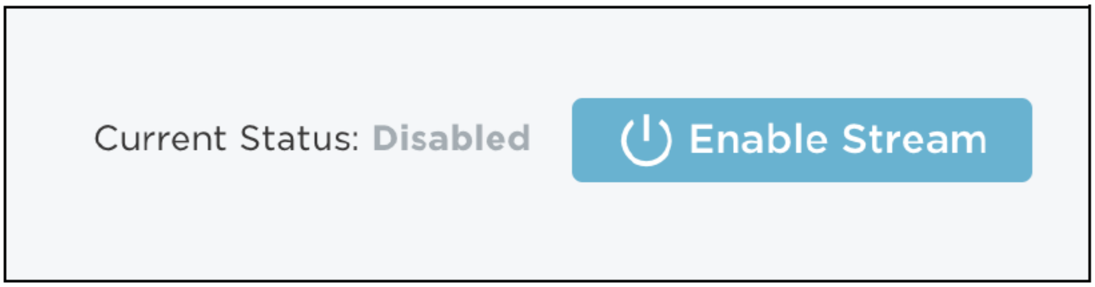
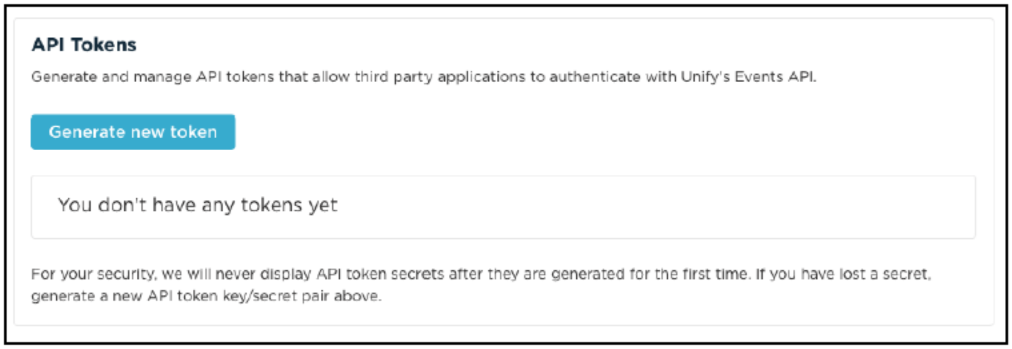


Figure 3. Enable Stream

6. Your Unify Zscaler integration is now ready to receive Web Logs from Zscaler Cloud NSS, but you must first also create an API Token. Go to **Settings**.
7. Select the **API Tokens** tab.
8. Click **Generate new token**.



API Tokens

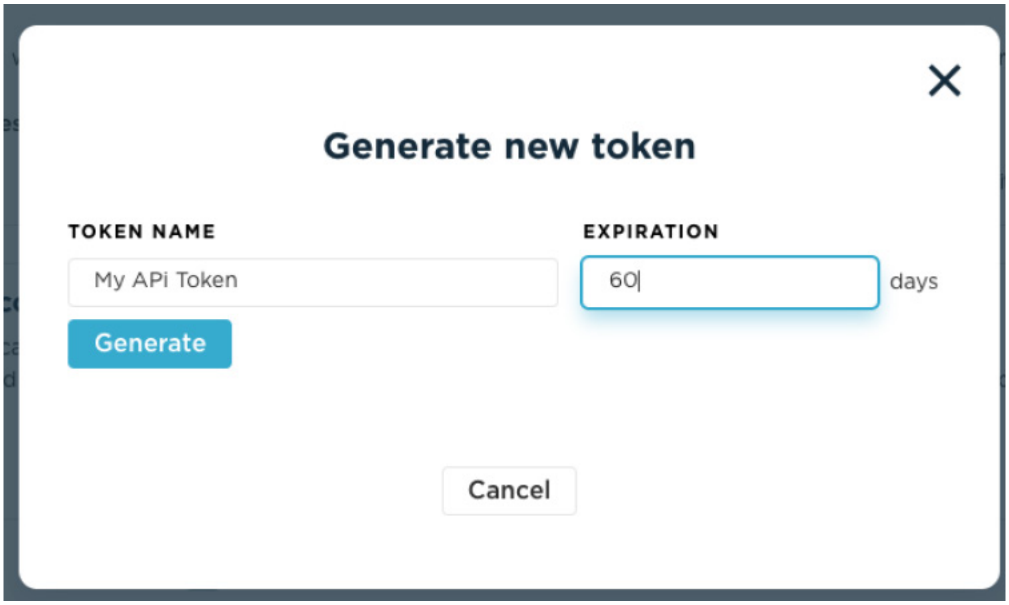
Generate and manage API tokens that allow third party applications to authenticate with Unify's Events API.

You don't have any tokens yet

For your security, we will never display API token secrets after they are generated for the first time. If you have lost a secret, generate a new API token key/secret pair above.

Figure 4. Generate new token

9. Provide a short and unique **Token Name** and set an **Expiration** for your token (in days). The expiration is required to generate a token, and must be a positive integer from 1 to 365.



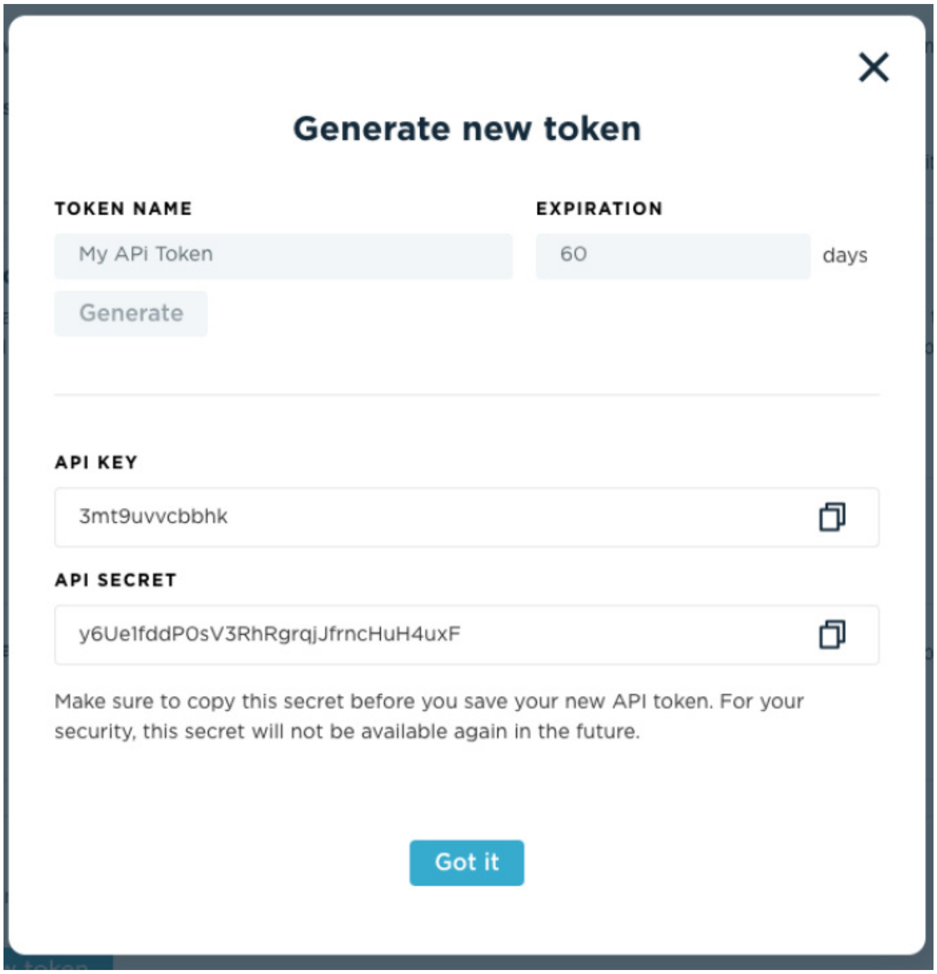
Generate new token

TOKEN NAME: My APi Token

EXPIRATION: 60 days

Figure 5. Configure new token

10. Click **Generate**.
11. An API Token is generated. Copy the **API Key** and the **API Secret** and save it in a password manager or other secure password storage. Both the API Key and API Secret are necessary for Cloud NSS to authenticate, though only the API Secret is considered sensitive.



Generate new token

TOKEN NAME: My APi Token

EXPIRATION: 60 days

API KEY: 3mt9uvvcbbhk

API SECRET: y6Ue1fddP0sV3RhRgrqjJfrncHuH4uxF

Make sure to copy this secret before you save your new API token. For your security, this secret will not be available again in the future.

Figure 6. Token API Key and API Secret

12. Click **Got it**. You cannot see your API Secret anywhere in the Unify platform.

Configure a Cloud NSS Feed to Send Data to Unify

The following section describes configuring the Zscaler Cloud NSS feed.

Before you begin this process, ensure that you have a Zscaler ZIA Cloud NSS License.

Granting Access

Without a license, you cannot establish a connection. If you need to establish an on-premises NSS Feed connection, reach out to help@livingsecurity.com for support in establishing a setup. There are strict infrastructure requirements you must meet to push logs to Unify via this feed.

To learn more, see Adding Cloud NSS Feeds for Web Logs.

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

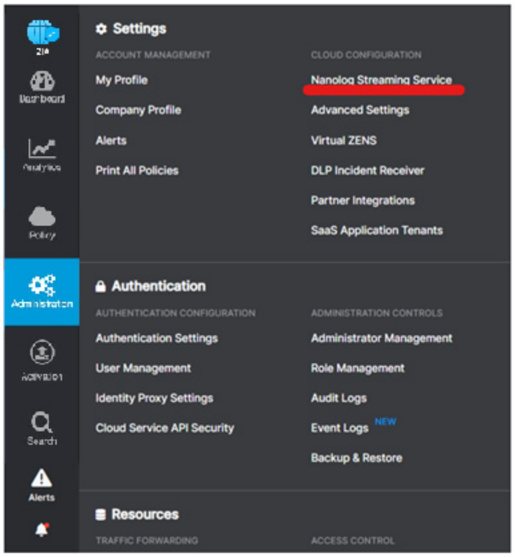


Figure 7. Zscaler Nanolog Streaming Service

2. In the **Cloud NSS Feeds** tab, click **Add Cloud NSS Feed**. The **Add Cloud NSS Feed** window appears.

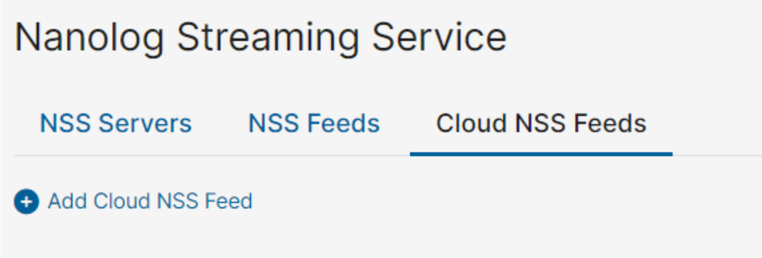


Figure 8. Add Cloud NSS Feed

3. In the **Add Cloud NSS Feed** window:
   a. **Feed Name**: Enter or edit the name of the feed.
   b. **NSS Type**: **NSS for Web** is selected by default.
   c. **Status**: The NSS feed is **Enabled** by default. Choose **Disabled** if you want to activate it at a later time.

d. **SIEM Rate**: Set this value to **Limited**.

e. **SIEM Rate Limit (Events per Second)**: Set this to `100` to ensure you don't reach the rate limits.

f. **SIEM Type**: Set to **Other**.

g. **OAuth 2.0 Authentication**: This setting is enabled by default if it is applicable to the SIEM type.

h. **Max Batch Size**: Set this to `20` KB.

i. **API URL**: Living Security provides you with your API URL.

j. Under HTTP Headers:

- **Key 1**: Set this to `x-api-key`.
- **Value 1**: Add the `<api key>.<api secret>` format based on the Unify API article.
- **Add HTTP Header**: Click to add more HTTP headers (keys and values).
- **Key 2**: Enter content-type.
- **Value 2**: Enter application/json.

Refer to Living Security's article on how to create a Unify API Token.

k. **Log Type**: Choose **Web Log**.

l. **Feed Output Type**: The output is **JSON** by default.

m. **JSON Array Notation**: Make sure that this setting is **ENABLED**, as this ensures the data is sent in the required JSON array structure.

n. **Feed Escape Character**: Leave this field empty.

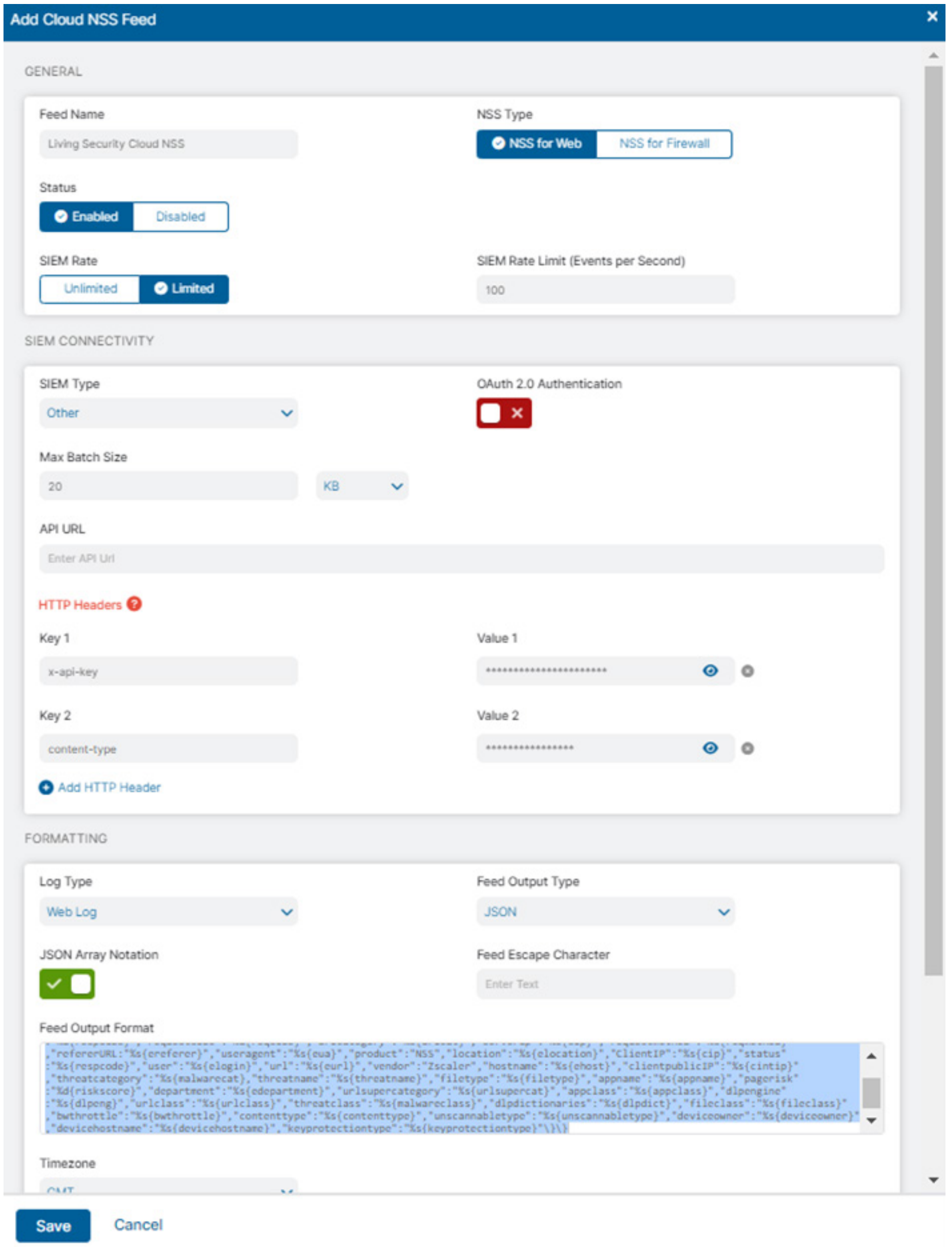
o. **Feed Output Format**: Use the following format for the **Feed Output**.

```
\{ "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":"%scontenttype}","unscannabletype":
"%s{unscannabletype}","deviceowner":"%s{deviceowner}","devicehostname":
"%s{devicehostname}","keyprotectiontype":"%s{keyprotectiontype}"\}\}
```

PDF files add line breaks to preserve the source text formatting. When copying code from a PDF into the Feed Output Format, you must remove any line breaks from the text.

Copy the code text and paste it into this tool (or one similar) to remove the line breaks. When cleaned, copy the code from the tool and paste it into the Feed Output Format.

p. **Timezone**: By default, this is set to the organization’s time zone. The time zone you set applies to the time field in the output file. The time zone automatically adjusts to changes in daylight savings in the specific time zone. The configured time zone is output to the logs as a separate field. The list of time zones is derived from the IANA Time Zone database. You can also specify direct GMT offsets.



Add Cloud NSS Feed

GENERAL

Feed Name: Living Security Cloud NSS

NSS Type: [✓ NSS for Web] NSS for Firewall

Status: [✓ Enabled] Disabled

SIEM Rate: Unlimited [✓ Limited]

SIEM Rate Limit (Events per Second): 100

SIEM CONNECTIVITY

SIEM Type: Other

OAuth 2.0 Authentication: ☒

Max Batch Size: 20 KB

API URL: Enter API Url

HTTP Headers

Key 1: x-api-key

Value 1: ••••••••••••••••••••••

Key 2: content-type

Value 2: ••••••••••••••••

Add HTTP Header

FORMATTING

Log Type: Web Log

Feed Output Type: JSON

JSON Array Notation: ✓

Feed Escape Character: Enter Text

Feed Output Format:

```
,"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}"\}\}
```

Timezone: GMT

Figure 9. Configure Cloud NSS Feed

Defining Filters

Filters restrict the logs from your Zscaler ZIA instance from overloading the Unify API. Zscaler recommends you implement the following filters to ensure Unify Insights expressly sees only logs within these Policy Reasons.

Only enable for events for which you have established policies within Zscaler, to ensure your NSS Feed is secure, unless you plan on implementing policies for these events so Unify can have these insights.

Policy Reason Filter

- Blocked Mobile App exhibiting malicious behavior
- Blocked Mobile App leaking user credentials insecurely
- Blocked Mobile App with known security vulnerability
- Custom Reputation block outbound request: malicious URL
- File attachment not allowed
- IPS block inbound response: malicious content
- IPS block inbound response: phishing content
- IPS block inbound response: page contains known browser exploits
- Malware Block: Malicious File
- Not allowed because URL is placed on denylist
- Not allowed because this file contains known vulnerabilities
- Not allowed to access this file type
- Not allowed to upload/download encrypted or password-protected archive files
- Not allowed to upload/download files of size greater than configured limit
- Not allowed to upload/download files of this type
- PageRisk block inbound response: page is unsafe
- Reputation block outbound request: malicious URL
- Reputation block outbound request: phishing site
- Secure Browsing blocked an outdated/disallowed component
- Secure Browsing warned about an outdated/disallowed component

After you have defined these filters, click Save.

Managing Your Stream

After the Cloud NSS Feed is enabled, you can click into the Web Logs stream in the Zscaler Integrations card of your Unify Integrations Page to administer the stream itself, view how the stream is performing, and enable/disable that stream.

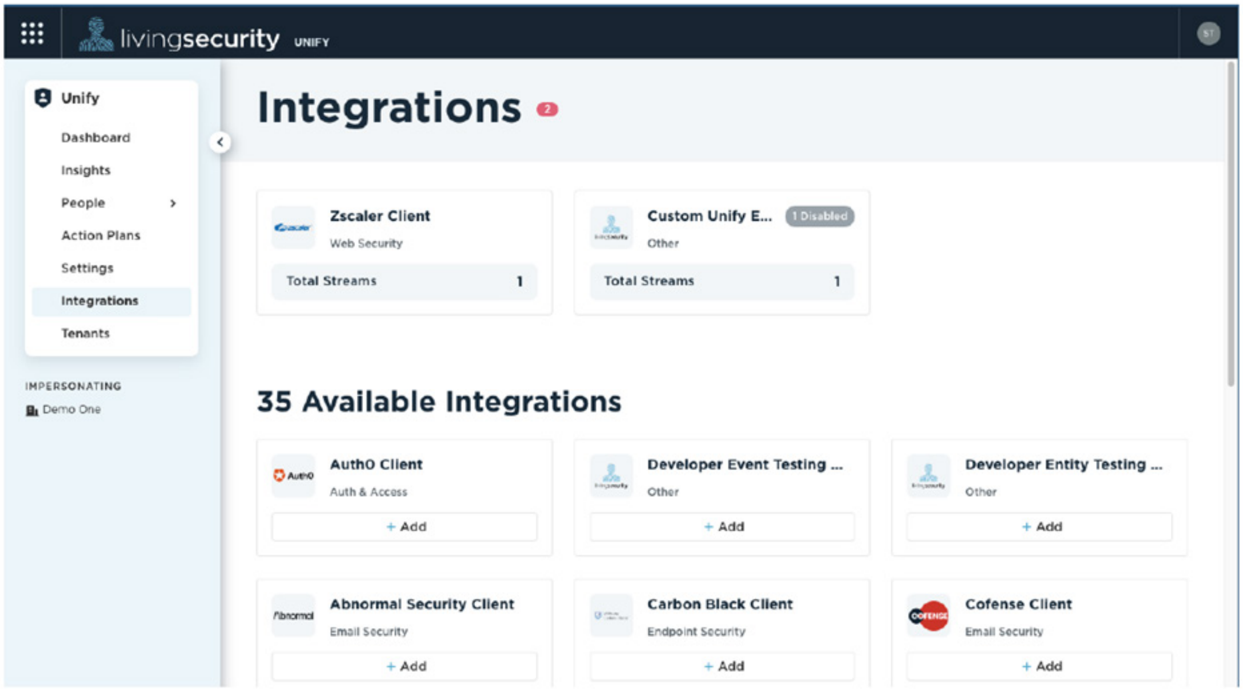


Figure 10. Managing Integrations

In order to enable or disable a stream, select the Enable Stream at the top right of the page, which is available when the stream is in a Disabled state. Disable Stream is available for streams in an Active state.

If your organization intends to stop the stream to prevent data from coming into the Unify Insights tool, Zscaler recommends that the Zscaler Admin disable the Cloud NSS Feed in Zscaler to ensure absolute control of your data.

The Stream Result history shows requests that were made by your Unify instance to the specific endpoint for the integration. If there is an issue, you can view it here.

If there are repeated failures from a stream, there is likely an error with the authentication or the service stream. Zscaler recommends you reach out to help@livingsecurity.com for help with troubleshooting your integration.

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**.

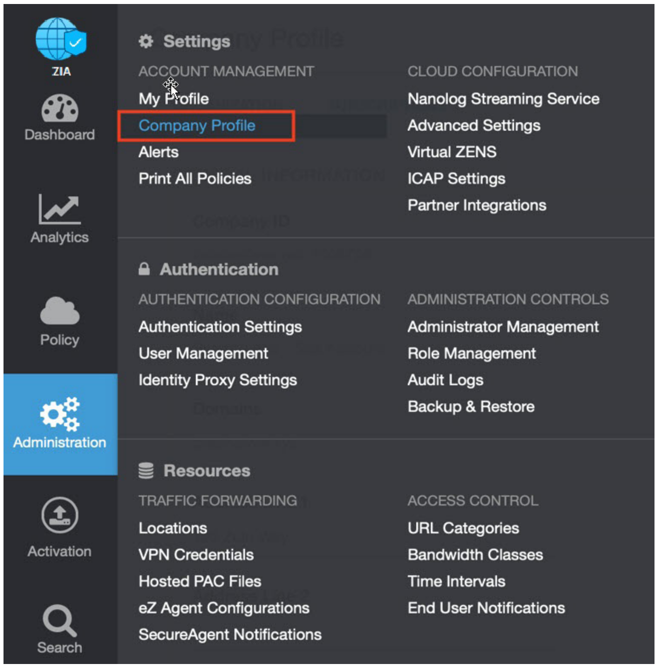
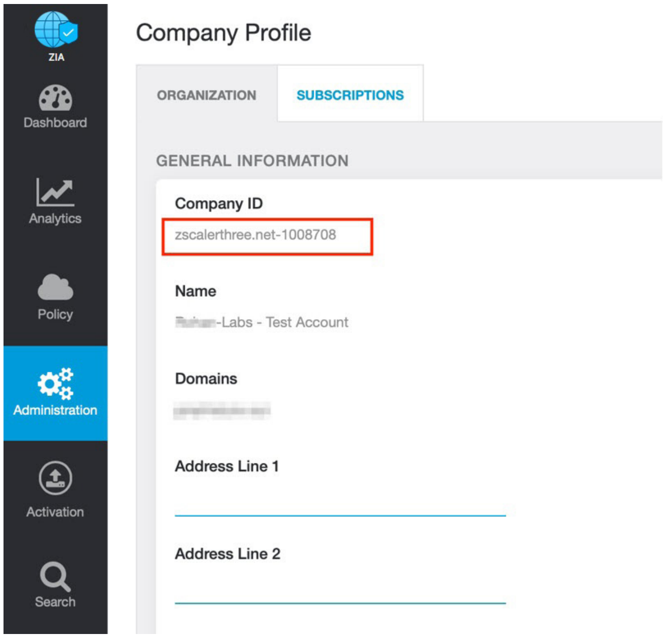


Figure 11. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 12. Company ID

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

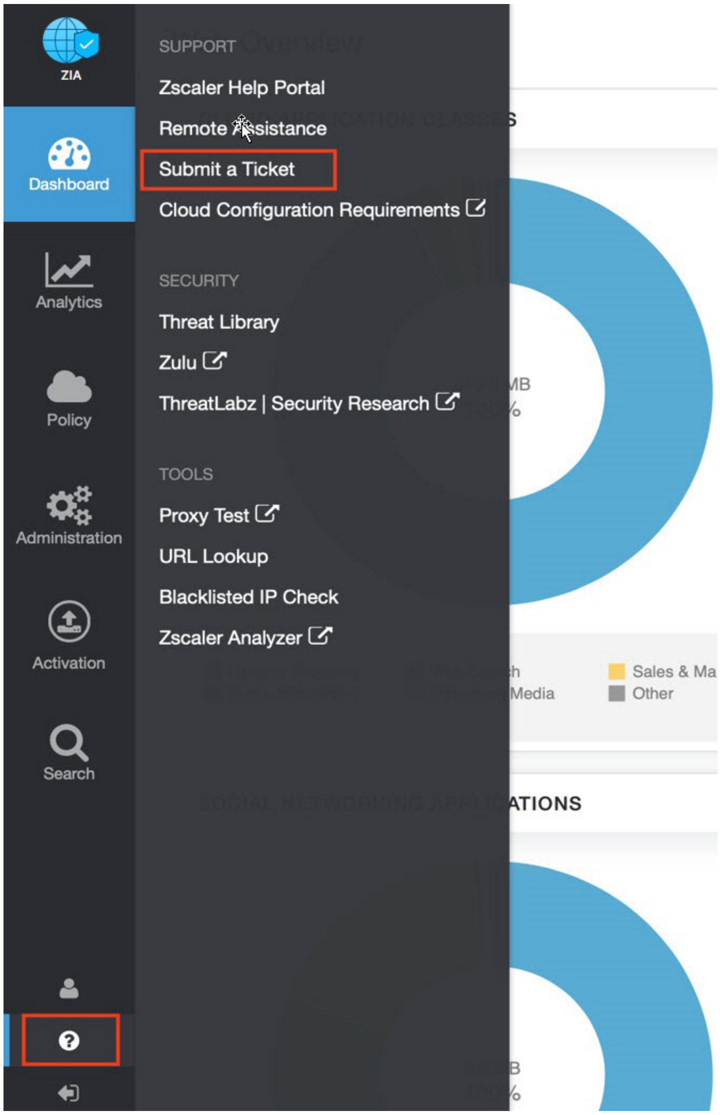


Figure 13. Submit a ticket