ZSCALER AND ELEVATE SECURITY DEPLOYMENT GUIDE

NOVEMBER 2022, 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
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.

Elevate Security Overview

Elevate Security solves the age-old problem of worker risk. Their platform proactively safeguards an organization's riskiest users by integrating into the current technology stack to identify behaviors, attack patterns, and other characteristics that affect an individual's risk levels. Security teams apply Elevate's risk scoring, risk-aware interventions to predict, personalize controls, and help prevent the next incident before it happens. To learn more, see Elevate Security'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
- Elevate 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 us at 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 Elevate Security Introduction

Overviews of the Zscaler and Elevate 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 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 virtual desktop interface (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, intrusion prevention system (IPS), Sandboxing, data loss prevention (DLP), and Browser Isolation, allowing you 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.
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.

Elevate Security Platform Overview

All of the information you need to understand and identify your riskiest users already exists in your enterprise. The Elevate Security Platform integrates and ingests this valuable employee security data from all your current cybersecurity tools and systems.

The Elevate Security Platform makes it easy to analyze and defend your organization against insider risk. Use benchmark visibility, targeted security controls, and personalized feedback to focus on risky employees and strengthen your cyber defenses.

The Elevate Security Platform provides:

- Depth. Access security controls, decision support, and dashboards with deep insights.
- Breadth. Leverage security data and insights from your existing tools--with results in minutes.
- Visibility. Quickly identify which users and contractors are most likely to cause a breach.
- Control. Use risk scores, context, and automated policy changes to eliminate workforce risk.

Elevate Security Resources

The following table contains links to Elevate Security support resources.

Name	Definition
Elevate Security Documentation	Online documentation for the Elevate Security Platform.
Elevate Security Resources	Resources center for the Elevate Security Platform.

Integration with Zscaler

The integration between Zscaler and Elevate Security leverages Zscaler's logs using Cloud Nanolog Streaming Service (NSS) to get activity pushed into the Elevate Security Platform.

To set up the integration, you need:

- A Zscaler Cloud NSS subscription
- An authentication token from Elevate Security

Elevate Security Configuration

The following steps are based on procedures documented on the Elevate Security website. To configure Elevate Security:

1. Navigate to the **Data and Integrations** page in the Elevate Platform.
2. Click **Add Integrations** near the top of the page.
3. Find and select the **Zscaler** tile.
4. Select **Secure Browsing**, **Push Data**, and **Elevate data push API**.
5. Click **Start Integration**.

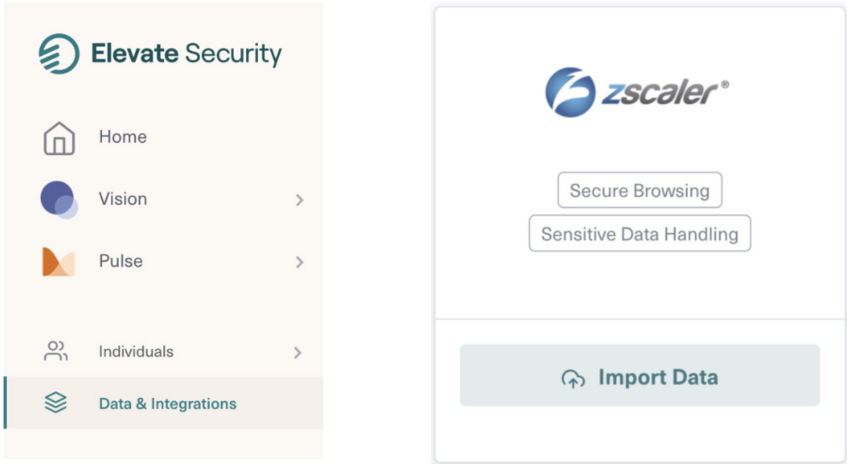
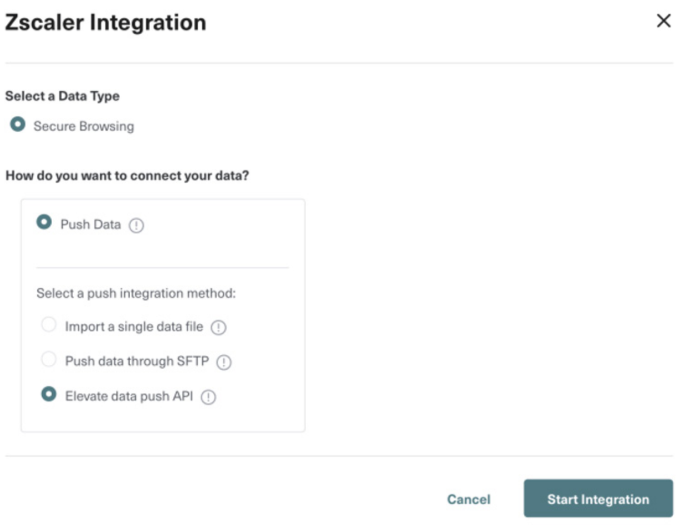


Figure 1. Configure Elevate Security



Zscaler Integration ×

Select a Data Type

● Secure Browsing

How do you want to connect your data?

● Push Data ⓘ

Select a push integration method:

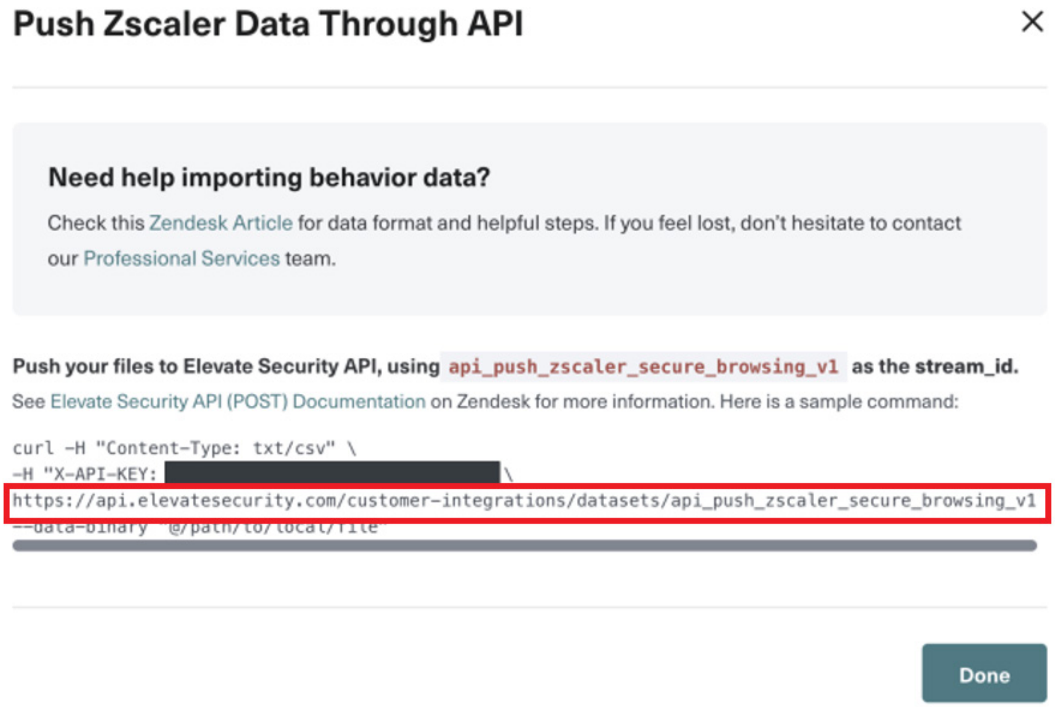
○ Import a single data file ⓘ

○ Push data through SFTP ⓘ

● Elevate data push API ⓘ

Figure 2. Zscaler Integration

6. You have created the endpoint for Zscaler to push data to the Elevate Security Platform. You are given an API key and a URL. Make a note of these as they are needed when configuring Zscaler Cloud NSS. In the following example, the **API URL** is https://api.elevatesecurity.com/customer-integrations/datasets/api_push_zscaler_secure_browsing_v1.



Push Zscaler Data Through API

Need help importing behavior data?

Check this Zendesk Article for data format and helpful steps. If you feel lost, don't hesitate to contact our Professional Services team.

Push your files to Elevate Security API, using `api_push_zscaler_secure_browsing_v1` **as the stream_id.**

See Elevate Security API (POST) Documentation on Zendesk for more information. Here is a sample command:

```
curl -H "Content-Type: txt/csv" \
-H "X-API-KEY: [redacted]\
https://api.elevatesecurity.com/customer-integrations/datasets/api_push_zscaler_secure_browsing_v1
--data-binary "@/path/to/local/file"
```

Figure 3. Push Zscaler Data Through API

Zscaler Cloud NSS Configuration

To configure Zscaler Cloud NSS in the ZIA Admin Portal:

1. Open the **Nanolog Streaming Service** page by clicking **Administration** > **Nanolog Streaming Service** in the left navigation pane.

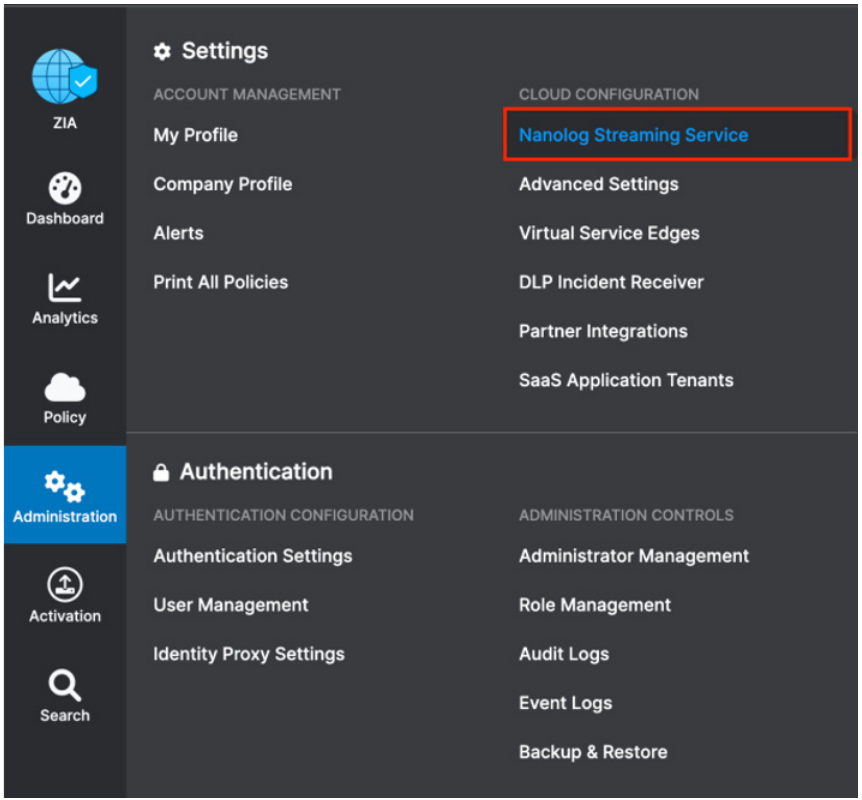


Figure 4. Nanolog Streaming Service

2. On the **Cloud NSS Feeds** tab, and click **Add Cloud NSS Feed**. If you do not see a **Cloud NSS Feeds** tab, contact your Zscaler Account team about adding this feature.

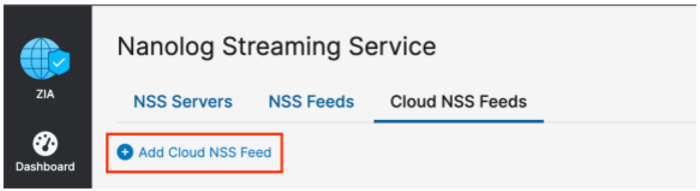


Figure 5. New Cloud NSS Feed

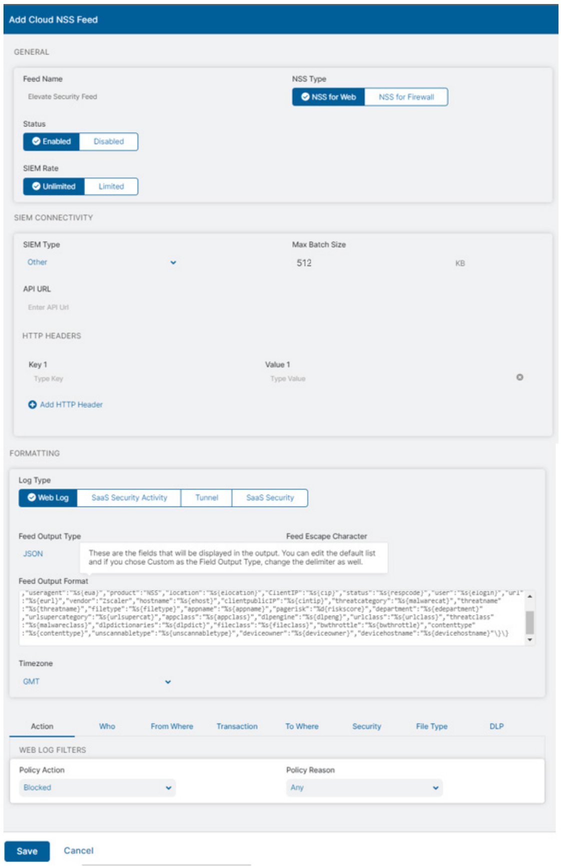
3. Fill the form with the following values (leave fields not listed as-is):
    a. Set **Feed Name** to **Any value**.
    b. Set **NSS Type** to **NSS for Web**.
    c. Set **Status** to **Enabled**.
    d. Set the **SIEM Rate** to **Unlimited**.
    e. Set the **SIEM Type** to **Other**.
    f. Set the **Max Batch Size** to `512 KB`.
    g. Set the **API URL** to the URL obtained from Elevate Security.
    h. Enter the API key created in Elevate Security as **Key 1**.
    i. Select **Add HTTP Header**, then set **Key 2** as **Content Type Value 2: application/json**.
    j. Set the **Log Type** to **Web Log**.
    k. Set the **Feed Output Type** to **JSON**.
    l. Leave the **Feed Escape Character** as-is.
    m. Set the **Time Zone** to **GMT**.
    n. Set the **Policy Action** to **Web log filters > Blocked**.

o. Enter the following into the **Feed Output Format**:

```
{"action":"%s{action}","appclass":"%s{appclass}","appname":"%s{appname}","apprulelabel"
:"%s{apprulelabel}","bamd5":"%s{bamd5}","bwclassname":"%s{bwclassname}","bwrulename":"%
s{bwrulename}","bwthrottle":"%s{bwthrottle}","cintip":"%s{cintip}","cip":"%s{cip}","cl
ientsslcipher":"%s{clientsslcipher}","clientsslsessreuse":"%s{clientsslsessreuse}","cl
ienttlsversion":"%s{clienttlsversion}","cltipv6":"%s{cltipv6}","contenttype":"%s{conte
nttype}","ctime":"%d{ctime}","datacenter":"%s{datacenter}","datacentercity":"%s{datace
ntercity}","datacentercountry":"%s{datacentercountry}","datetime":"%d{yyyy}-%02d{mth}-
%02d{dd}%02d{hh}:%02d{mm}:%02d{ss}","day":"%s{day}","day_of_month":"%02d{dd}","dept":"%
s{dept}","deviceappversion":"%s{deviceappversion}","devicehostname":"%s{devicehostname}
","devicemodel":"%s{devicemodel}","devicename":"%s{devicename}","deviceostype":"%s{devi
ceostype}","deviceosversion":"%s{deviceosversion}","deviceowner":"%s{deviceowner}","df_
hosthead":"%s{df_hosthead}","df_hostname":"%s{df_hostname}","dlpdict":"%s{dlpdict}","dl
pdicthitcount":"%s{dlpdicthitcount}","dlpeng":"%s{dlpeng}","dlpidentifiers":"%d{dlpident
ifier}","dlpmd5":"%s{dlpmd5}","edepartment":"%s{edepartment}","eedone":"%s{eedone}","efil
ename":"%s{efilename}","ehost":"%s{ehost}","elocation":"%s{elocation}","elogin":"%s{elog
in}","emobappname":"%s{emobappname}","epochtime":"%d{epochtime}","ereferer":"%s{erefere
r}","erefererhost":"%s{erefererhost}","ereferertpath":"%s{ereferertpath}","erulelabel":"%
s{erulelabel}","eua":"%s{eua}","eurl":"%s{eurl}","eurlpath":"%s{eurlpath}","externalspr
":"%s{externalspr}","fileclass":"%s{fileclass}","filename":"%s{filename}","filesubtype":"%s{
filesubtype}","filetype":"%s{filetype}","login":"%s{login}","malwarecat":"%s{malwarecat}"-
,"malwareclass":"%s{malwareclass}","minutes":"%02d{mm}","mobappcat":"%s{mobappcat}","mo
bappname":"%s{mobappname}","mobdevtype":"%s{mobdevtype}","module":"%s{module}","month":
"%s{mon}","month_of_year":"%02d{mth}","nsssvcip":"%s{nsssvcip}","odevicehostname":"%s{o
devicehostname}","odevicename":"%s{odevicename}","odeviceowner":"%s{odeviceowner}","olo
gin":"%s{ologin}","productversion":"%s{productversion}","proto":"%s{proto}","reason":"%
s{reason}","recordid":"%d{recordid}","referer":"%s{referer}","refererhost":"%s{refererh
ost}","reqdatasize":"%d{reqdatasize}","reqhdrsize":"%d{reqhdrsize}","reqmethod":"%s{req
method}","reqsize":"%d{reqsize}","reqversion":"%s{reqversion}","respcode":"%s{respcode}
","respdatasize":"%d{respdatasize}","resphdrsize":"%d{resphdrsize}","respsize":"%d{resp
size}","respversion":"%s{respversion}","riskscore":"%d{riskscore}","rulelabel":"%s{rule
label}","ruletype":"%s{ruletype}","seconds":"%02d{ss}","serversslsessreuse":"%s{servers
slsessreuse}","sip":"%s{sip}","srvcertchainvalpass":"%s{srvcertchainvalpass}","srvcertv
alidationtype":"%s{srvcertvalidationtype}","srvcertvalidityperiod":"%s{srvcertvalidityp
eriod}","srvocspresult":"%s{srvocspresult}","srvsslcipher":"%s{srvsslcipher}","srvtlsve
rsion":"%s{srvtlsversion}","srvwildcardcert":"%s{srvwildcardcert}","ssldecrypted":"%s{s
sldecrypted}","stime":"%d{stime}","threatname":"%s{threatname}","throttlereqsize":"%d{t
hrottlereqsize}","throttlerespsize":"%d{throttlerespsize}","timezone":"%s{tz}","totalsi
ze":"%d{totalsize}","trafficredirectmethod":"%s{trafficredirectmethod}","ua":"%s{ua}","ua_
token":"%s{ua_token}","uaclass":"%s{uaclass}","unscannable":"%s{unscannable}","url":"%s
{url}","urlcat":"%s{urlcat}","urlclass":"%s{urlclass}","urlfilterrulelabel":"%s{urlfilter
rulelabel}","urlsupercat":"%s{urlsupercat}","year":"%d{yyyy}","ztunnelversion":"%s{ztun
nelversion}"}
```

PDF files adds 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. Once cleaned, copy the code from the tool and paste it into the Feed Output Format.



Add Cloud NSS Feed

GENERAL

Feed Name: Elevate Security Feed

NSS Type: ✓ NSS for Web | NSS for Firewall

Status: ✓ Enabled | Disabled

SIEM Rate: ✓ Unlimited | Limited

SIEM CONNECTIVITY

SIEM Type: Other

Max Batch Size: 512 KB

API URL: Enter API Url

HTTP HEADERS

Key 1: Type Key

Value 1: Type Value

FORMATTING

Log Type: ✓ Web Log | SaaS Security Activity | Tunnel | SaaS Security

Feed Output Type: JSON

Feed Escape Character

These are the fields that will be displayed in the output. You can edit the default list and if you chose Custom as the Field Output Type, change the delimiter as well.

Feed Output Format

```
,"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

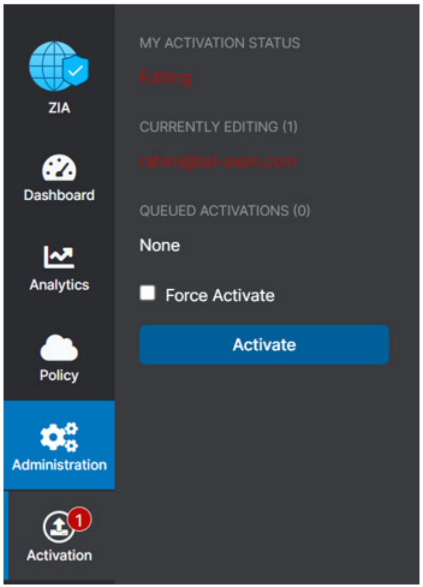
WEB LOG FILTERS

Policy Action: Blocked

Policy Reason: Any

Figure 6. Add Cloud NSS Feed

4. Click **Save** and **Activate** the configuration.



MY ACTIVATION STATUS

Editing

CURRENTLY EDITING (1)

rahim@bd-siem.com

QUEUED ACTIVATIONS (0)

None

□ Force Activate

Figure 7. Activate the configuration

Appendix A: Requesting Zscaler Support

You might need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

To contact Zscaler Support:

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

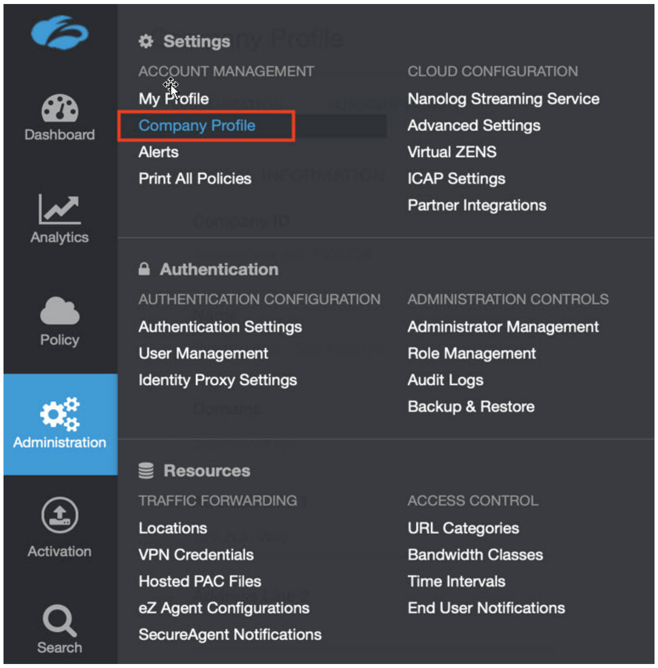
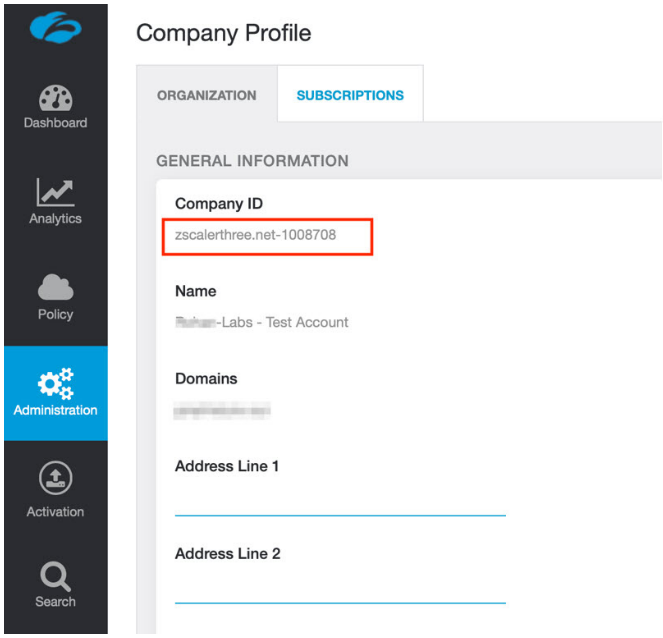


Figure 8. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company 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. Navigate to **Dashboard** > **Support** > **Submit a Ticket**.

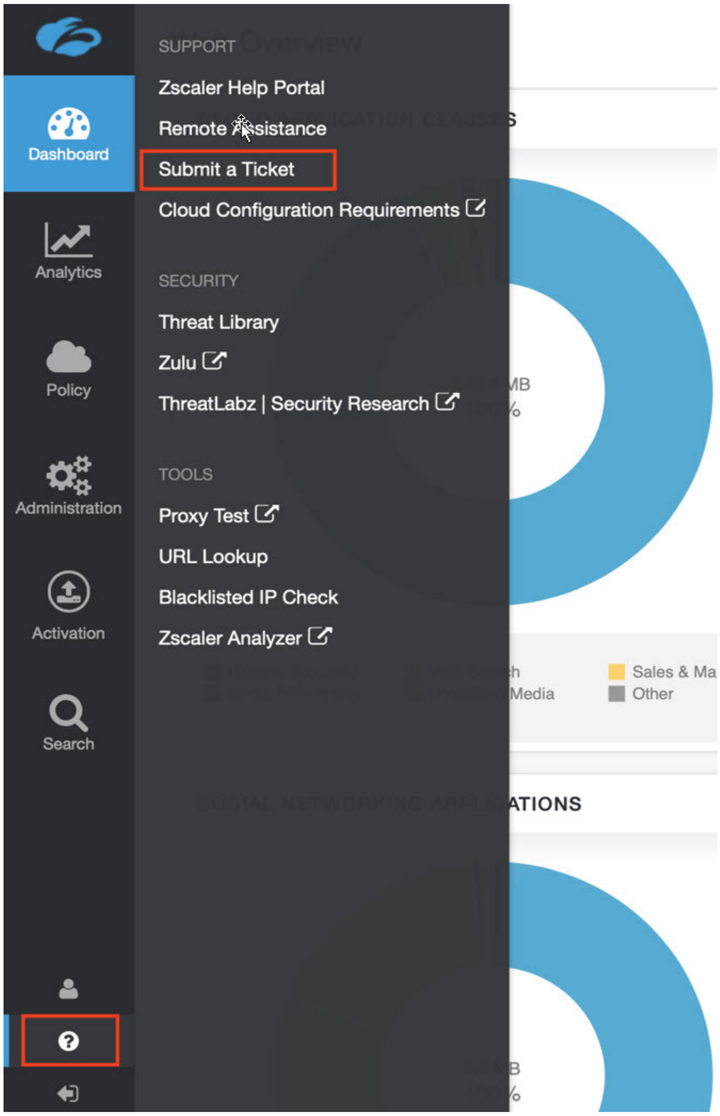


Figure 10. Submit a Ticket