zscaler™ | Secureworks®

ZSCALER AND SECUREWORKS DEPLOYMENT GUIDE

OCTOBER 2025, VERSION 1.1

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
SIEM	Security Information and Event Management
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)

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.

Secureworks Overview

Secureworks is a leader in cybersecurity providing best-in-class cybersecurity solutions and threat intelligence that reduces risk, optimizes IT and security investments, and fills security team talent gaps. Secureworks Taegis is the cybersecurity analytics cloud platform built on real-world threat intelligence and research. Taegis detects the most advanced threats, streamlines collaboration between your team and ours, and automatically spotlights the most important actions first. To learn more, refer to Secureworks 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
- Secureworks 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 Secureworks Introduction

Overviews of the Zscaler and Secureworks 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.

Secureworks Taegis XDR Overview

Secureworks Taegis XDR enables you to detect advanced threats, trust your alerts, streamline and collaborate on investigations, and automate the correct action.

Secureworks Resources

The following table contains links to Secureworks support resources.

Name	Definition
Taegis XDR Help Portal	Help articles and documentation on Taegis XDR.
Zscaler Integration Guide	Zscaler and Secureworks Integration Guide.

Introduction

You must configure Zscaler to send logs via the Nanolog Streaming Service (NSS) to a Taegis XDR Data Collector. The following diagram provides the necessary actions and steps to configure log forwarding on Zscaler NSS.

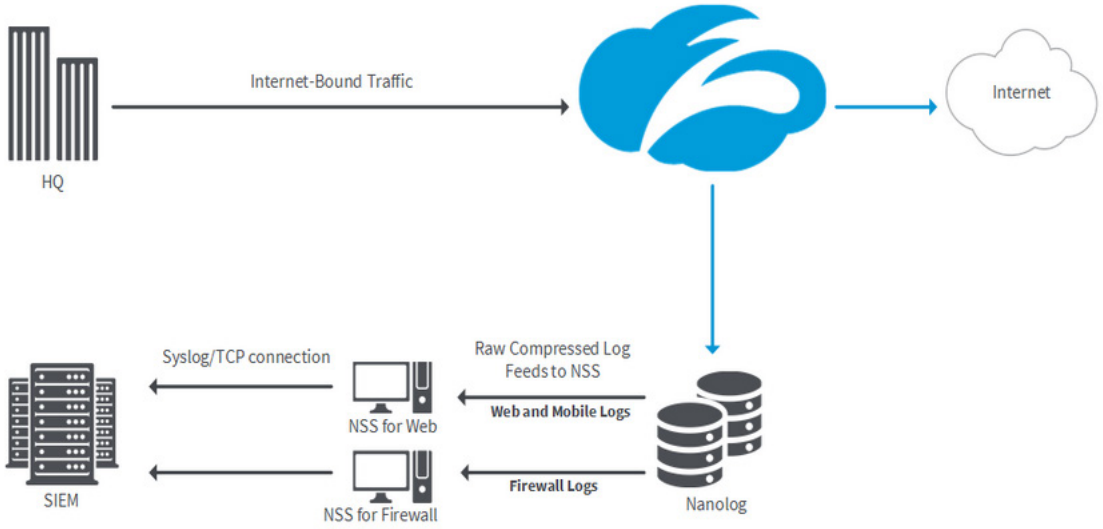

Figure 1. Zscaler NSS architecture

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

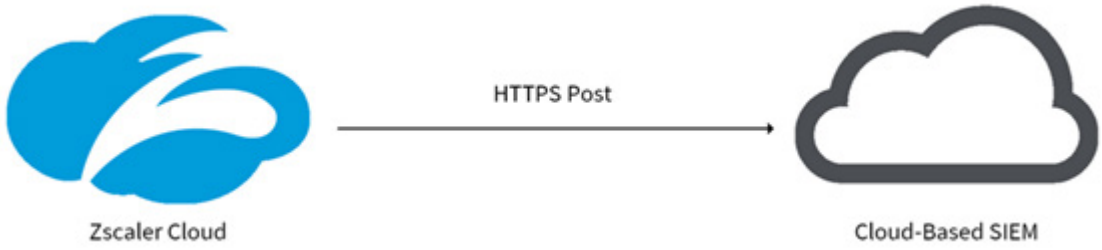

Figure 2. Zscaler Cloud NSS architecture

Secureworks Taegis XDR Setup

The following steps set up Taegis XDR:

1. Log in to your instance of Taegis XDR.
2. Go to **Integrations** > **Data Collectors**.

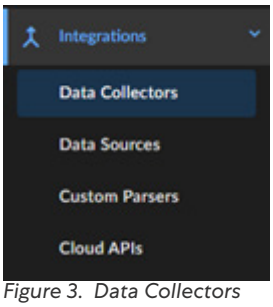

Figure 3. Data Collectors

3. Locate the IP address of the XDR Data Collector to which Zscaler logs are sent.

Configuring Taegis Collector

This step is only necessary if you have not already deployed an XDR Data Collector, or must configure a new XDR Data Collector specifically for Zscaler.

Secureworks provides the following guides to configure a new XDR Data Collector:

- On-Premises Data Collector (secureworks.com)
- AWS Data Collector (secureworks.com)
- Azure Data Collector (secureworks.com)
- Google Cloud Platform (GCP) Data Collector (secureworks.com)

Zscaler NSS Setup

The following sections explain how to set up Zscaler NSS.

Web Logs

1. Log in to your ZIA Admin Portal and go to **Administration** > **Nanolog Streaming Service**.
2. Click **Add NSS Feed**.

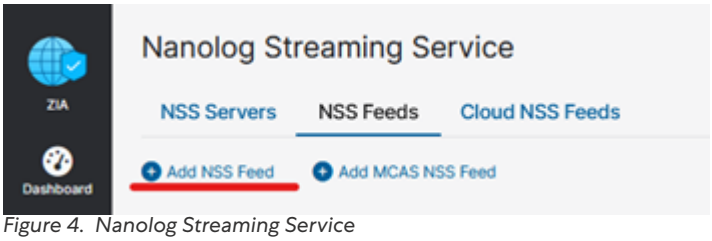

Figure 4. Nanolog Streaming Service

3. On the **Add NSS Feed** page, edit the fields listed in the following steps.
   a. **NSS Type**: Select **NSS for Web**.
   b. **SIEM IP Address**: Enter the IP address of the Taegis XDR Data Collector.
   c. **SIEM TCP Port**: Enter `601`.
   d. **Feed Output Type**: Select **Custom**.
   e. **Feed Output Format**: Copy and paste the following into the **Feed Output Format**.

```
NSS_Web_v1 %s{mon} %d{dd} %d{hh}:%d{mm}:%d{ss} %d{yyyy} recordId=%d{recordid}
login=%s{login} dname=%s{host} dip=%s{sip} sip=%s{cip} natPublicIp=%s{cintip}
url=%s{url} ua=%s{ua} module=%s{module} proto=%s{proto} action=%s{action} rea-
son=%s{reason} appName=%s{appname} appClass=%s{appclass} fileType=%s{filetype} req-
Size=%d{reqsize} responseSize=%d{respsize} totalSize=%d{totalsize} sTime=%d{ctime}
cTime=%d{ctime} malwareCat=%s{malwarecat} malwareClass=%s{malwareclass} threatNam-
e=%s{threatname} riskScore=%d{riskscore} DLPEng=%s{dlpeng} DLPDict=%s{dlpdict} lo-
cation=%s{location} dept=%s{dept} reqMethod=%s{reqmethod} respCode=%s{respcode}
respVersion=%s{respversion} urlClass=%s{urlclass} urlSuperCat=%s{urlsupercat} url-
Cat=%s{urlcat} referer=%s{referer}
```


f. **Timezone**: Select **GMT** from the drop-down menu.

g. **Duplicate Logs**: Select **Disabled** from the drop-down menu.

h. **Policy Action**: Select **Blocked** from the drop-down menu.

i. **Policy Reason**: Select **Any** from the drop-down menu.

j. Click **Save**.

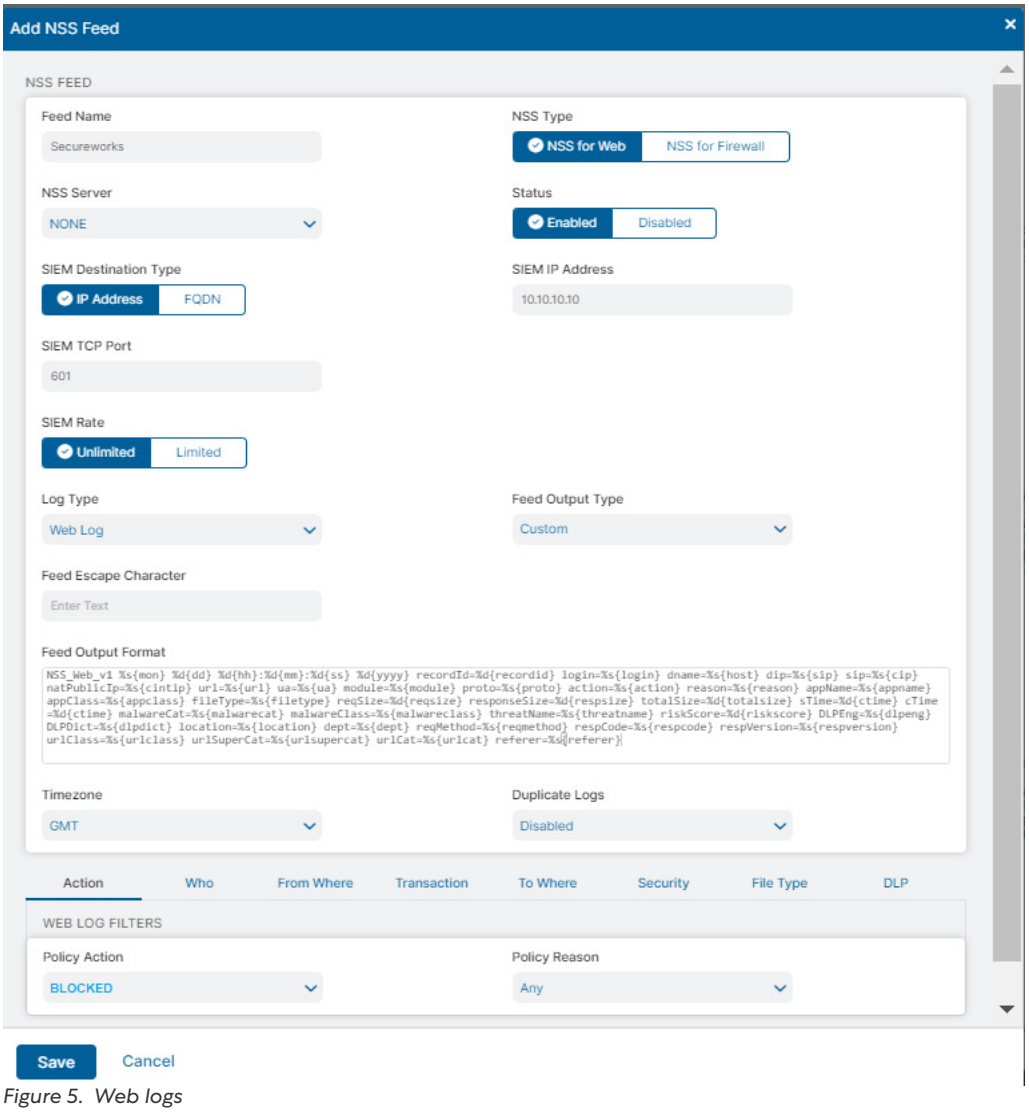

Figure 5. Web logs

Firewall Logs

1. Log in to your ZIA Admin Portal and go to **Administration** > **Nanolog Streaming Service**.
2. Add a new **NSS Feed**.

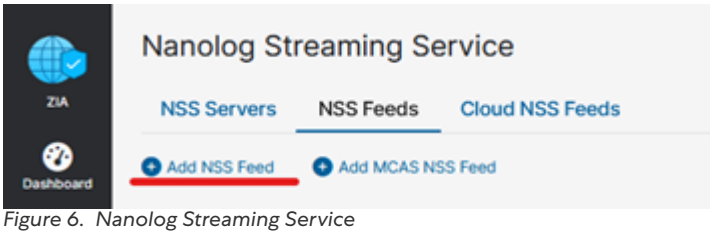

Figure 6. Nanolog Streaming Service

3. On the **Add NSS Feed** page, edit the fields listed in the following steps.
   a. **NSS Type**: Select **NSS for Firewall**.
   b. **SIEM IP Address**: Enter the IP address of the Taegis XDR Collector.
   c. **SIEM TCP Port**: Enter `601`.
   d. **SIEM Rate**: Select **Unlimited**.
   e. **Log Type**: Select **Firewall**.
   f. **Feed Output Type**: Select **Custom**.
   g. **Feed Output Format**: Copy and paste the following into the **Feed Output Format**.

```
time="%s{time}" login="%s{login}" dept="%s{dept}" location="%s{location}" cd-
port="%d{cdport}" csport="%d{csport}" sdport="%d{sdport}" ssport="%d{ssport}"
csip="%s{csip}" cdip="%s{cdip}" ssip="%s{ssip}" sdip="%s{sdip}" tsip="%s{tsip}"
tsport="%d{tsport}" ttype="%s{ttype}" action="%s{action}" dnat="%s{dnat}" state-
ful="%s{stateful}" aggregate="%s{aggregate}" nwsvc="%s{nwsvc}" nwapp="%s{n-
wapp}" ipproto="%s{ipproto}" ipcat="%s{ipcat}" destcountry="%s{destcountry}" avg-
duration="%d{avgduration}" rulelabel="%s{rulelabel}" inbytes="%ld{inbytes}"
outbytes="%ld{outbytes}" duration="%d{duration}" durationms="%d{durationms}"
numsessions="%d{numsessions}"
```


h. **Timezone**: Select **GMT** from the drop-down menu.

i. **Duplicate Logs**: Select **Disabled** from the drop-down menu.

j. **Policy Action**: Select **Blocked** from the drop-down menu.

k. **Policy Reason**: Select **Any** from the drop-down menu.

l. Click **Save**.

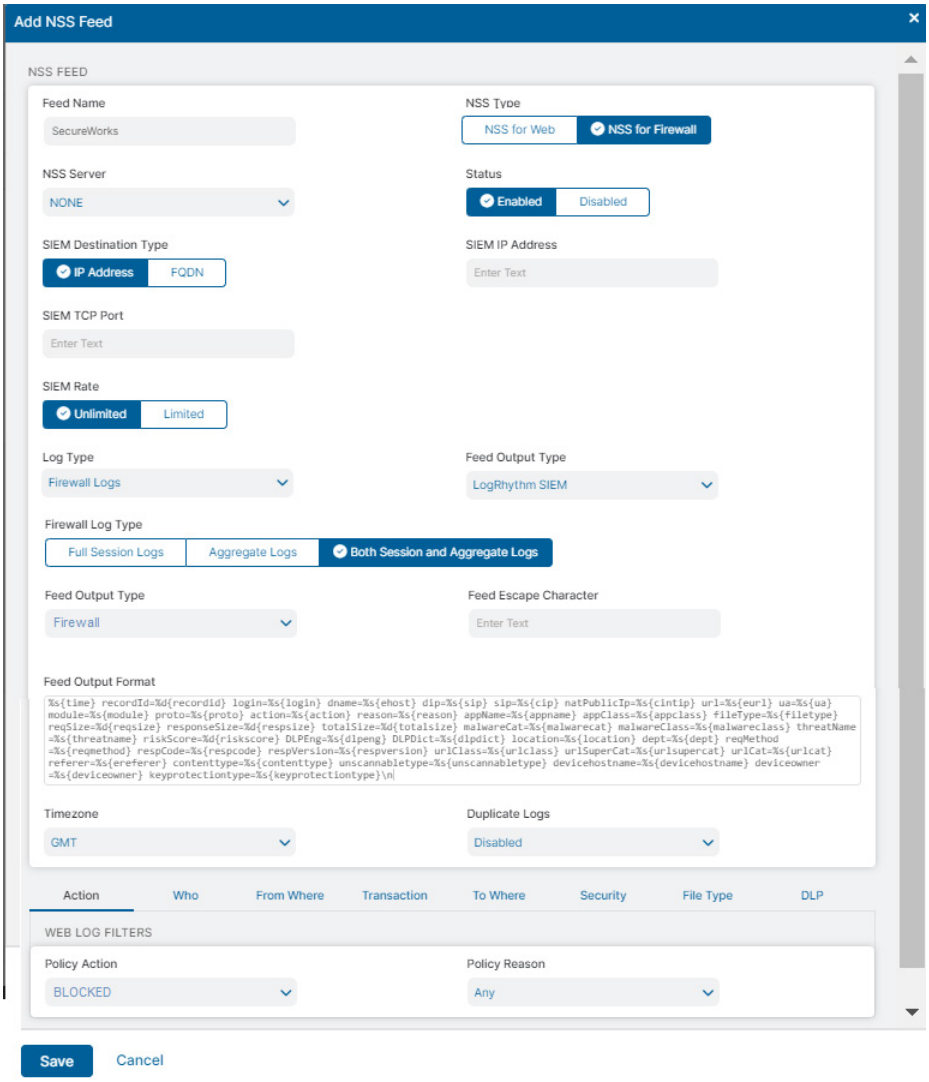

Figure 7. Firewall logs

DNS Logs

1. Log in to your ZIA Admin Portal and go to **Administration** > **Nanolog Streaming Service**.
2. Click **Add NSS Feed**.

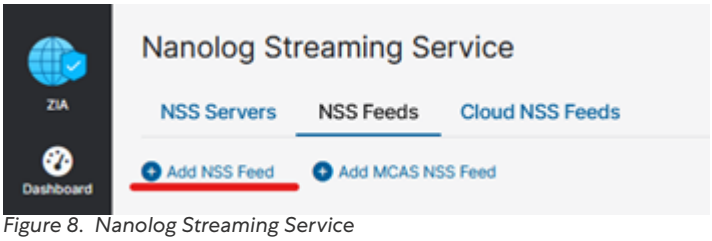

Figure 8. Nanolog Streaming Service

3. On the **Add NSS Feed** page, edit the fields listed in the following steps.
   a. **NSS Type**: Select **NSS for Firewall**.
   b. **SIEM IP Address**: Enter the IP address of the Taegis XDR Collector.
   c. **SIEM TCP Port**: Enter `601`.
   d. **SIEM Rate**: Select **Unlimited**.
   e. **Log Type**: Select **DNS Logs**.
   f. **Feed Output Type**: Select **Custom**.
   g. **Feed Output Format:** Copy and paste the following into the **Feed Output Format**.

```
time="%s{time}" login="%s{login}" dept="%s{dept}" location="%s{location}" cd-
port="%d{cdport}" csport="%d{csport}" sdport="%d{sdport}" ssport="%d{ssport}"
csip="%s{csip}" cdip="%s{cdip}" ssip="%s{ssip}" sdip="%s{sdip}" tsip="%s{tsip}"
tsport="%d{tsport}" ttype="%s{ttype}" action="%s{action}" dnat="%s{dnat}" state-
ful="%s{stateful}" aggregate="%s{aggregate}" nwsvc="%s{nwsvc}" nwapp="%s{n-
wapp}" ipproto="%s{ipproto}" ipcat="%s{ipcat}" destcountry="%s{destcountry}" avg-
duration="%d{avgduration}" rulelabel="%s{rulelabel}" inbytes="%ld{inbytes}"
outbytes="%ld{outbytes}" duration="%d{duration}" durationms="%d{durationms}"
numsessions="%d{numsessions}"
```


h. **Timezone**: Select **GMT** from the drop-down menu.

i. **Duplicate Logs**: Select **Disabled** from the drop-down menu.

j. **Policy Action**: Select **Blocked** from the drop-down menu.

k. **Policy Reason**: Select **Any** from the drop-down menu.

l. Click **Save**.

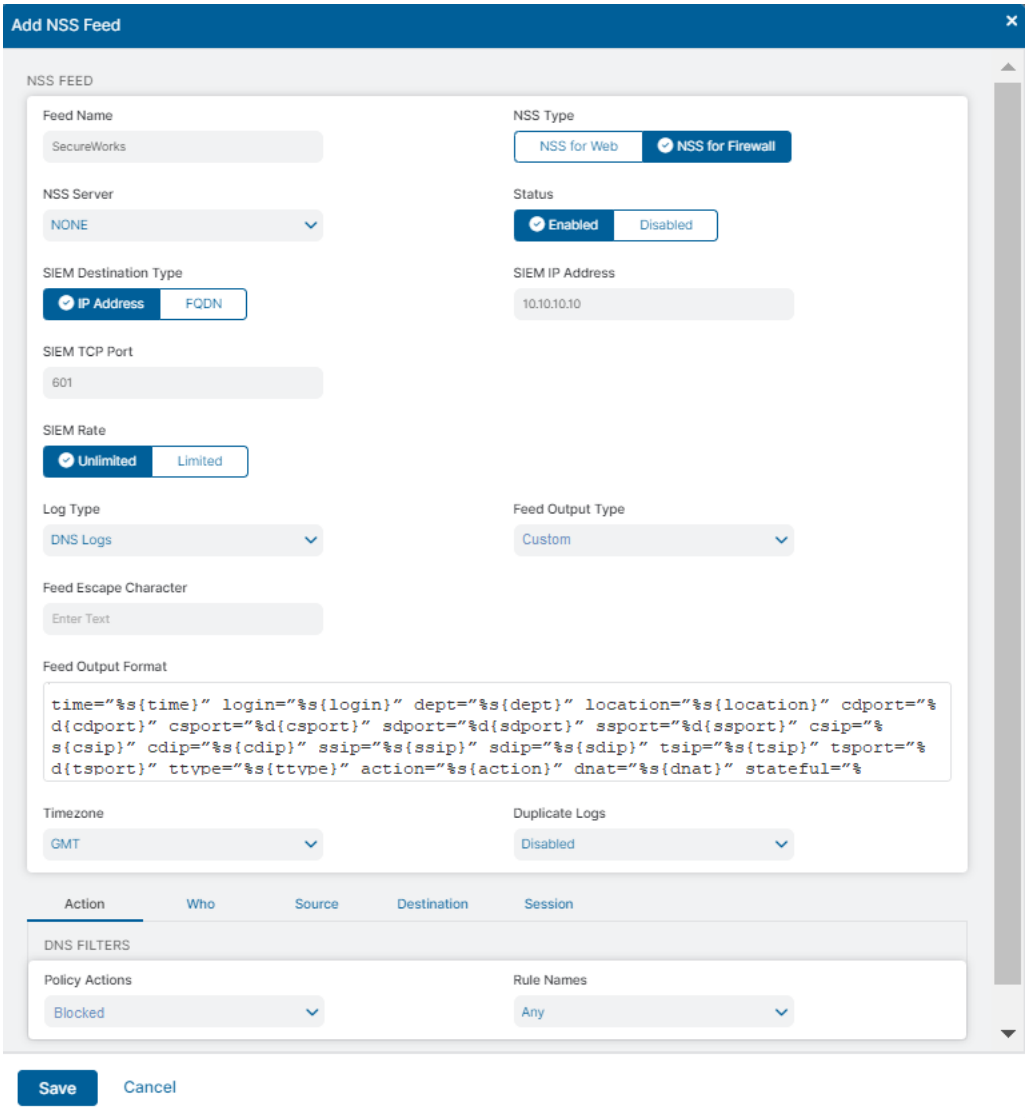

Figure 9. DNS logs

Zscaler Cloud NSS Setup

The following sections describe how to configure Zscaler Cloud NSS.

1. Use the Splunk option for Cloud NSS. You'll make three NSS configurations: Web, Firewall, and DNS. From your ZIA Admin Portal, go to **Administration** > **Nanolog Streaming Service**.

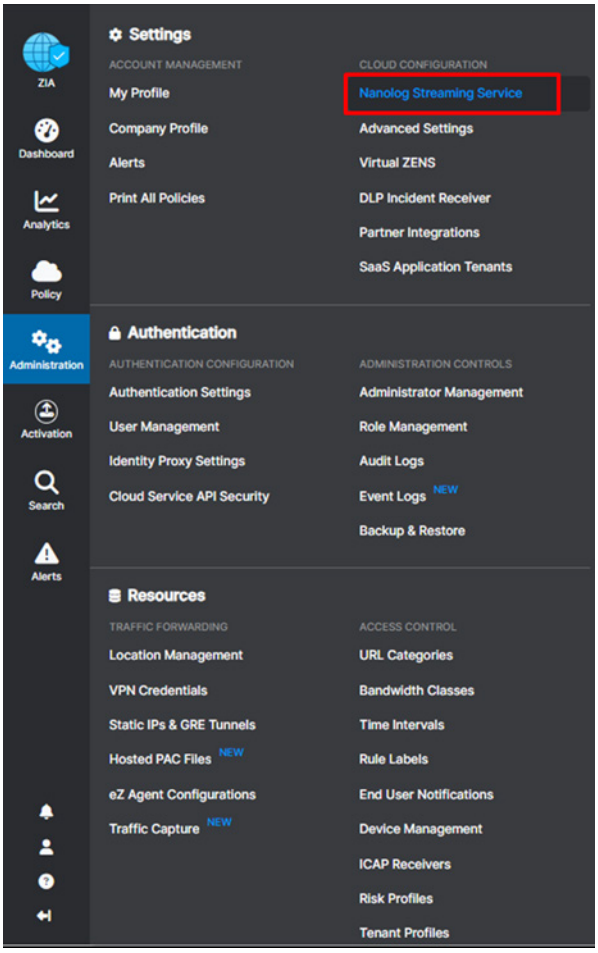

Figure 10. Nanolog Streaming Service

2. Select the **Cloud NSS Feeds** tab, then **Add Cloud NSS Feed**.

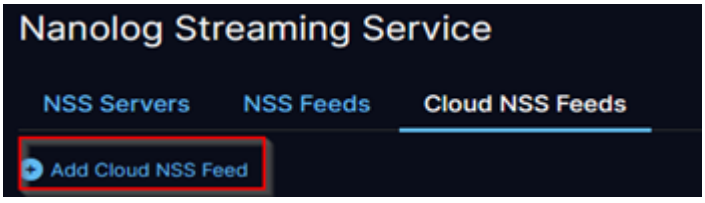

Figure 11. Add Cloud NSS Feed

3. Configure the **Cloud NSS** feed as needed in the **Edit Cloud NSS Feed** window.

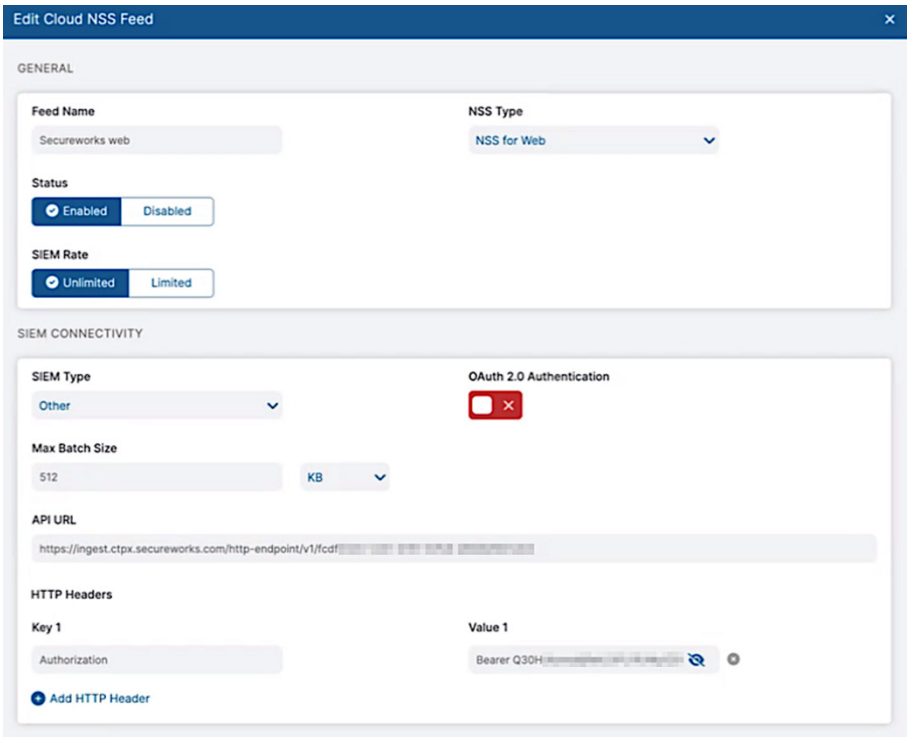

Figure 12. Edit Cloud NSS Feed

4. Create a new **HTTP integration** in Taegis and copy the **URL** and **Integration Key** into the Cloud NSS parameters.
5. The **Integration Key** must go in a request header field called **Authorization** and be passed in as Bearer <INTEGRATION_KEY> (e.g., `Bearer idfj9318ufs9dfuh019fh9f234r2rqfh`).
6. If the header is not allowed, pass the Taegis **Integration Key** as the token for the Splunk config. It is passed in the same header.
7. Set the **Max Batch Size in Cloud NSS** to `512` KB.
8. Use the UTC time zone.
9. Test the connection. A successful connection indicates a 200 response from the server.
10. Save the Cloud NSS config.

Check the Taegis HTTP integration configuration page after 30 minutes to verify that data is coming.

Log Formats

The following sections show what to add to the Log Feed Output Format.

Weblog Format

NSS_Web_v1 %s{mon} %d{dd} %d{hh}:%d{mm}:%d{ss} %d{yyyy} recordId=%d{recordid} login=%s{login} dname=%s{host} dip=%s{sip} sip=%s{cip} natPublicIp=%s{cintip} url=%s{url} ua=%s{ua} module=%s{module} proto=%s{proto} action=%s{action} reason=%s{reason} appName=%s{appname} appClass=%s{appclass} fileType=%s{filetype} reqSize=%d{reqsize} responseSize=%d{respsize} totalSize=%d{totalsize} sTime=%d{ctime} cTime=%d{ctime} malwareCat=%s{malwarecat} malwareClass=%s{malwareclass} threatName=%s{threatname} riskScore=%d{riskscore} DLPEng=%s{dlpeng} DLPDict=%s{dlpdict} location=%s{location} dept=%s{dept} reqMethod=%s{reqmethod} respCode=%s{respcode} respVersion=%s{respversion} urlClass=%s{urlclass} urlSuperCat=%s{urlsupercat} urlCat=%s{urlcat} referer=%s{referer}

Firewall Log Format

time="%s{time}" login="%s{login}" dept="%s{dept}" location="%s{location}" cdport="%d{cdport}" csport="%d{csport}" sdport="%d{sdport}" ssport="%d{ssport}" csip="%s{csip}" cdip="%s{cdip}" ssip="%s{ssip}" sdip="%s{sdip}" tsip="%s{tsip}" tsport="%d{tsport}" ttype="%s{ttype}" action="%s{action}" dnat="%s{dnat}" stateful="%s{stateful}" aggregate="%s{aggregate}" nwsvc="%s{nwsvc}" nwapp="%s{nwapp}" ipproto="%s{ipproto}" ipcat="%s{ipcat}" destcountry="%s{destcountry}" avgduration="%d{avgduration}" rulelabel="%s{rulelabel}" inbytes="%ld{inbytes}" outbytes="%ld{outbytes}" duration="%d{duration}" durationms="%d{durationms}" numsessions="%d{numsessions}"

DNS Log Format

time="%s{time}" login="%s{login}" dept="%s{dept}" location="%s{location}" reqaction="%s{reqaction}" reqrulelabel="%s{resrulelabel}" reqtype="%s{reqtype}" req="%s{req}" cip="%s{cip}" sport="%d{sport}" durationms="%d{durationms}" sip="%s{sip}" domcat="%s{domcat}"

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support:

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

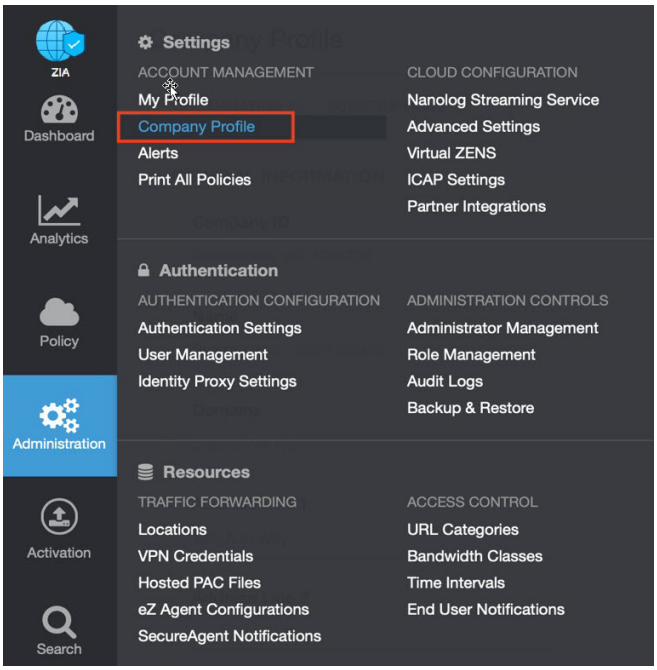

Figure 13. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

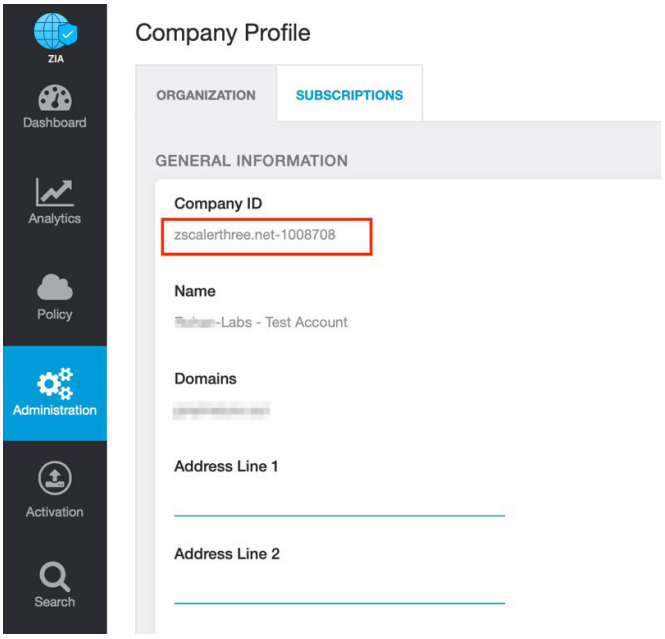

Figure 14. Company ID

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

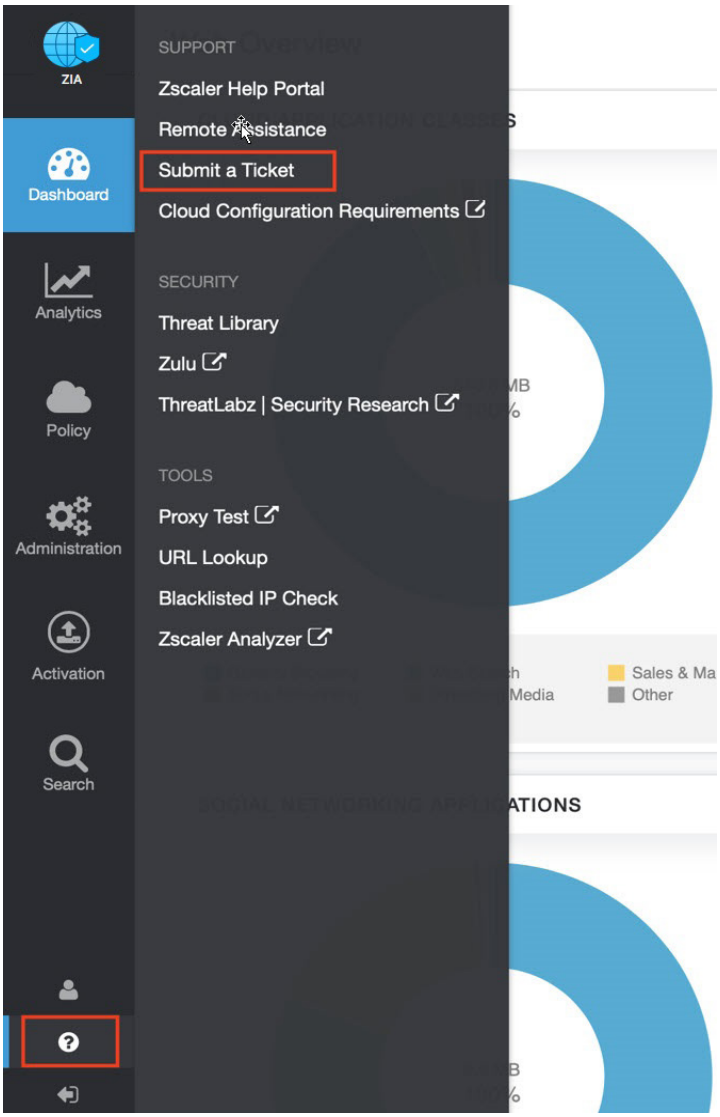

Figure 15. Submit a ticket

