ZSCALER AND NETWITNESS DEPLOYMENT GUIDE

JANUARY 2024, 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)
JDBC	Java Database Connectivity
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)
ZPC	Zscaler Posture Control (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.

NetWitness Overview

For organizations all over the globe, NetWitness delivers comprehensive and highly scalable threat detection and response capabilities—fueled by their unique unified data architecture. To learn more, refer to NetWitness' 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
- NetWitness 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 NetWitness Introduction

Overviews of the Zscaler and NetWitness 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.
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.

NetWitness Platform XDR Overview

The NetWitness Platform XDR delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect threats, prioritize activities, investigate, and automate response. All this empowers security analysts with better, faster efficiency to keep security operations well ahead of business-impacting threats.

NetWitness Resources

The following table contains links to NetWitness support resources.

Name	Definition
NetWitness Platform Demo	Platform demo.
NetWitness Documentation	Platform documentation.
NetWitness Community	NetWitness discussion forums.
NetWitness Knowledge Base	NetWitness Knowledge Base.
Logstash JDBC	Documentation for the Logstash JDBC input plugin.
Blog Posts	NetWitness Community Blog.

Introduction

You must configure Zscaler to send logs via the Nanolog Streaming Service (NSS) to a NetWitness Platform XDR Data Collector. This guide provides the necessary actions and steps to configure log forwarding on Zscaler NSS.

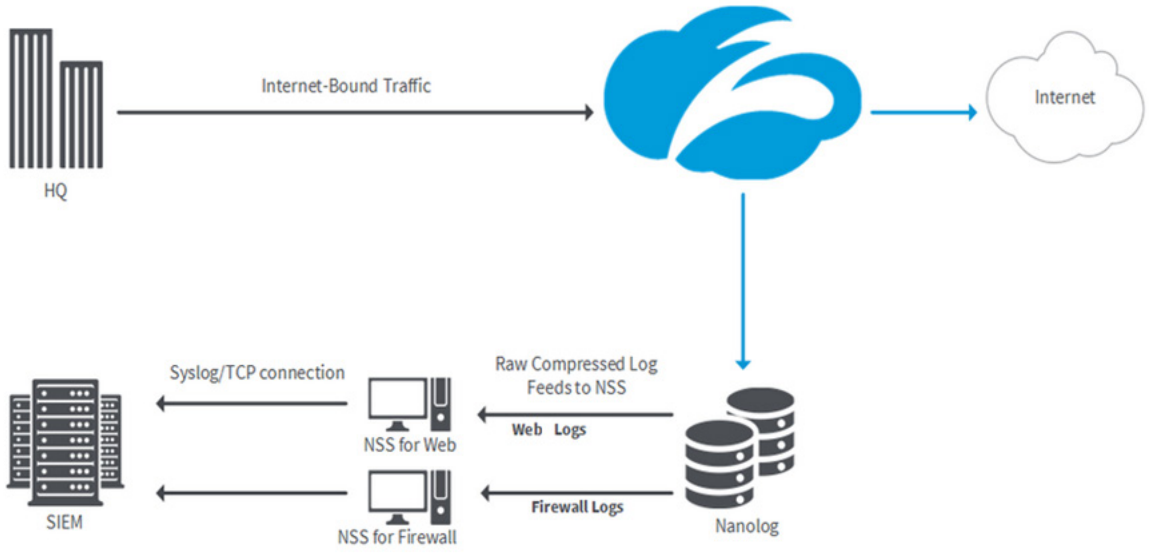


Figure 1. ZIA and NetWitness integration architecture

Customers should deploy their collector on the same subnet as the NSS VM since NSS VM doesn't encrypt data outbound towards the SIEM.

Configure NetWitness Platform for Syslog Collection

Only configure the Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

Configure either the Log Decoder or the Remote Log Collector for Syslog, not both.

To configure Log Decoder for Syslog Collection:

1. In the **NetWitness Platform** menu, select **Admin** > **Services**.
2. In the **Services** grid, choose a **Log Decoder**.
3. From the **Actions** menu, choose **View** > **System**.
4. Depending on the icon you see, do one of the following:
   - If you see **Start Capture**, click the icon to start capturing Syslog.
   - If you see **Stop Capture**, don't do anything. The Log Decoder is already capturing Syslog.

To configure Remote Log Collector for Syslog Collection:

1. In the **NetWitness Platform** menu, go to **Admin** > **Services**.
2. In the **Services** grid, select a Remote Log Collector.
3. From the **Actions** menu, choose **View** > **Config** > **Event Sources**.
4. Select **Syslog / Config** from the drop-down menu. The **Event Categories** panel displays the Syslog event sources that are configured, if any.

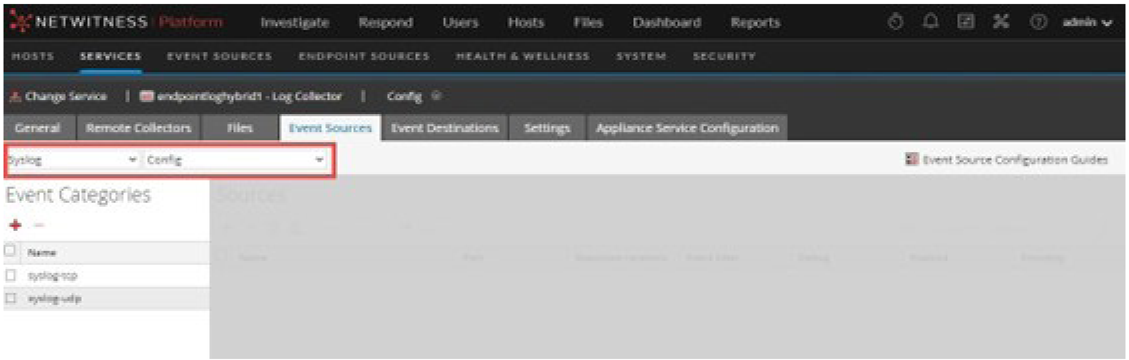
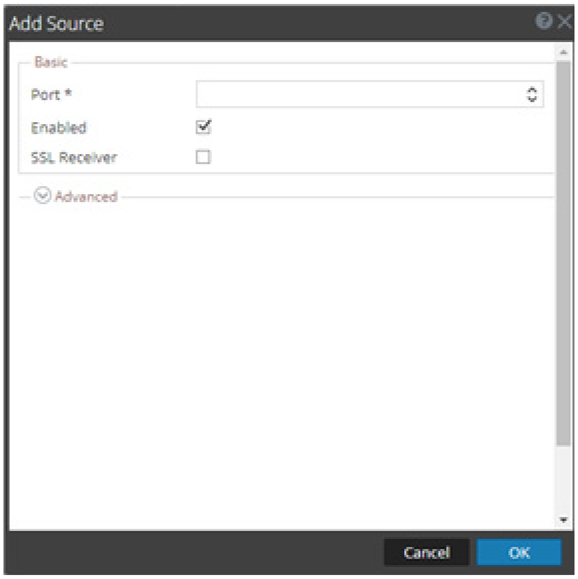


Figure 2. Event Categories panel

5. In the **Event Categories** panel toolbar, click the **Add** (**+**) icon. The **Available Event Source Types** dialog is displayed.
6. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
7. Choose **New Type** in the **Event Categories** panel and click the **Add** (**+**) in the **Sources** panel toolbar. The **Add Source** dialog is displayed.



Port *

Enabled ☑

SSL Receiver □

Figure 3. Add Source dialog

8. (Optional) Enter `514` for the port and choose **Enabled**.
9. Configure any of the **Advanced** parameters as necessary.
10. Click **OK**.

After you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. You can continue to add Syslog event sources to your system without a need to do any further configuration in the NetWitness Platform.

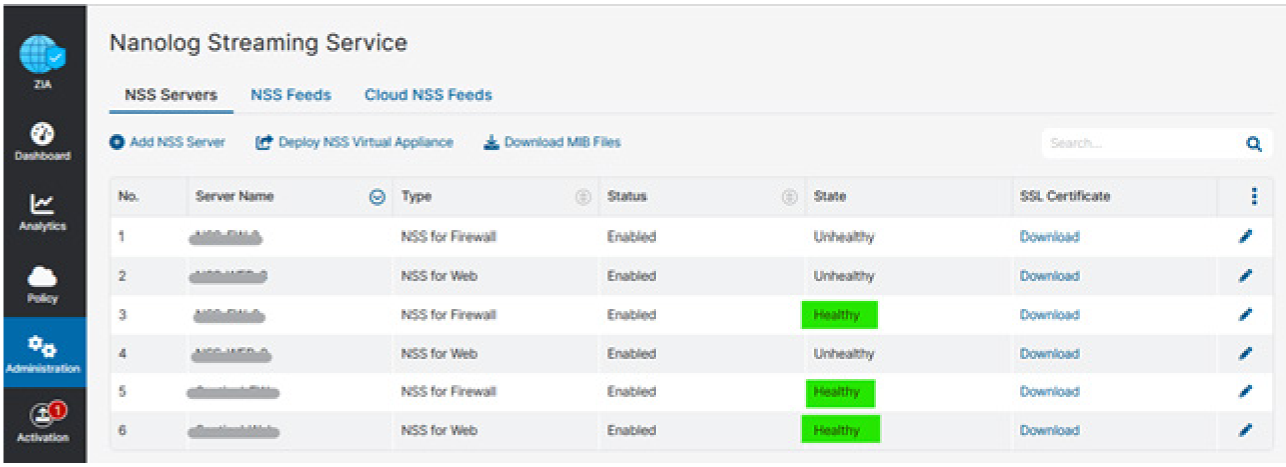
Configure Syslog Output on ZIA

Configure at least one feed that defines the logs that the ZIA sends to the NetWitness Platform.

Configure ZIA to Send WebLog Logs to the NetWitness Platform

To configure ZIA to send weblogs to the NetWitness Platform:

1. Log in to the ZIA Admin Portal with your admin account credentials.
2. Go to **Administration** > **Nanolog Streaming Service** > **NSS Servers** tab.
3. Click **Add NSS Server**. See Adding NSS Servers (government agencies, see Adding NSS Servers) to add an NSS Server.



Nanolog Streaming Service

No.	Server Name	Type	Status	State	SSL Certificate
1	[redacted]	NSS for Firewall	Enabled	Unhealthy	Download
2	[redacted]	NSS for Web	Enabled	Unhealthy	Download
3	[redacted]	NSS for Firewall	Enabled	Healthy	Download
4	[redacted]	NSS for Web	Enabled	Unhealthy	Download
5	[redacted]	NSS for Firewall	Enabled	Healthy	Download
6	[redacted]	NSS for Web	Enabled	Healthy	Download

Figure 4. NSS Server

Ensure that the NSS server State is Healthy.

4. Click **Add NSS Feed** and input the following information:
   a. **Feed Name**: Enter or edit the name of the feed. Each feed is a connection between NSS and your NetWitness Platform.
   b. **NSS Type**: Select **NSS for Web**.
   c. **NSS Server**: Select the NSS Server that you created from the list.
   d. **Status**: The NSS feed is **Enabled** by default. Choose **Disabled** if you want to activate it later.
   e. **SIEM Destination Type**: This is set to **IP Address** by default.
   f. **SIEM IP Address**: Enter the IP address of the NetWitness Log Decoder or Remote Log Collector to which the logs are streamed.
   g. **SIEM TCP Port**: Enter `514` for NetWitness Log Decoder or Remote Log Collector.
   h. **SIEM Rate**: Leave as **Unlimited**, unless you need to throttle the output stream due to licensing or other constraints.
   i. **Log Type**: Select **Web Log**.
   j. **Feed Output Type**: Choose **RSA Security Analytics**.
   k. **Feed Output Format**: Enter the following log format in the text box.

```
<134>1 ZSCALERNSS: time=%s{time}^^timezone=%s{tz}^^action=%s{action}^^reason=%s{reason
}^^hostname=%s{ehost}^^protocol=%s{proto}^^serverip=%s{sip}^^url=%s{eurl}^^urlcategor
y=%s{urlcat}^^urlclass=%s{urlclass}^^dlpdictionaries=%s{dlpdict}^^dlpengine=%s{dlpeng
}^^filetype=%s{filetype}^^threatcategory=%s{malwarecat}^^threatclass=%s{malwareclass}^^
pagerisk=%d{riskscore}^^threatname=%s{threatname}^^clientpublicIP=%s{cintip}^^ClientI
P=%s{cip}^^location=%s{location}^^refererURL=%s{ereferer}^^useragent=%s{ua}^^departme
nt=%s{dept}^^user=%s{login}^^event_id=%d{recordid}^^requestmethod=%s{reqmethod}^^requ
estsize=%d{reqsize}^^requestversion=%s{reqversion}^^status=%s{respcode}^^responsesize
=%d{respsize}^^responseversion=%s{respversion}^^transactionsize=%d{totalsize}^^conten
ttype=%s{contenttype}^^unscannabletype=%s{unscannabletype}^^deviceowner=%s{deviceowne
r}^^devicehostname=%s{devicehostname}^^keyprotectiontype=%s{keyprotectiontype}^^login
=%s{login}^^filename=%s{filename}^^filesubtype=%s{filesubtype}^^upload_filetype=%s{upload_
filetype}^^upload_filename=%s{upload_filename}^^upload_filesubtype=%s{upload_filesub
type}^^host=%s{host}^^uaclass=%s{uaclass}^^mobappname=%s{mobappname}^^mobdevtyp
e=%s{mobdevtype}^^clt_sport=%d{clt_sport}^^cltipv6=%s{cltipv6}^^dfhosthead=%s{
df_hosthead}^^dfhostname=%s{df_hostname}^^deviceostype=%s{deviceostype}\n
```

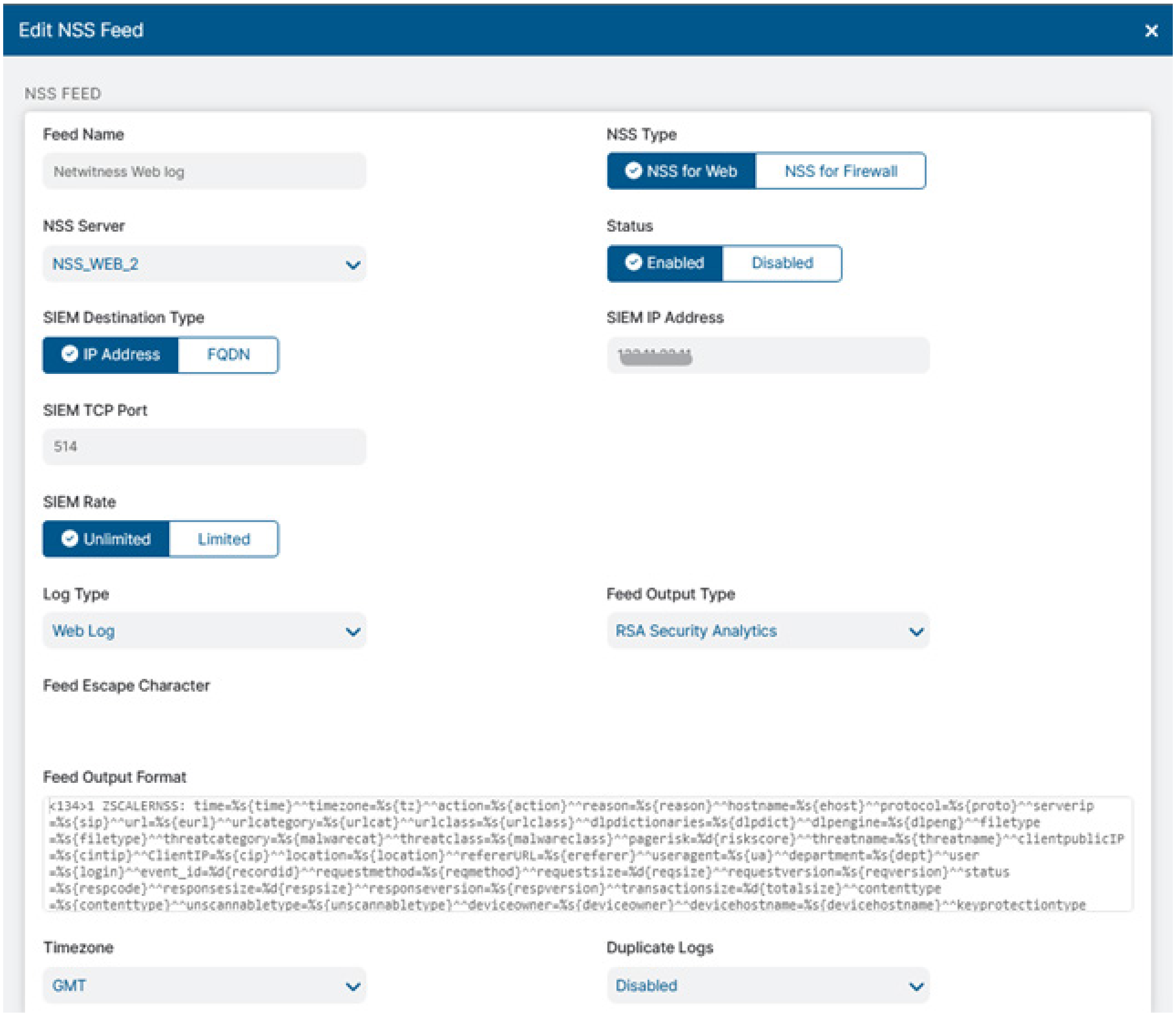
If you want to capture additional fields, add them as new values separated by ^^ in the above format. You must create a custom parser to parse the newly added field.

l. **Timezone of the date and time in log output**: 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. You can output the configured time zone 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.

m. **Duplicate Logs**: To ensure that no logs are skipped during any down time, specify the number of minutes that NSS sends duplicate logs. To learn more, see Understanding Nanolog Streaming Service (NSS) (government agencies, see Understanding Nanolog Streaming Service (NSS)).

n. **(Optional) Web Log Filters**: Define filters to limit which logs are sent to the SIEM.

5. Click **Save**.



Edit NSS Feed

NSS FEED

Feed Name: Netwitness Web log

NSS Type: ● NSS for Web | NSS for Firewall

NSS Server: NSS_WEB_2

Status: ● Enabled | Disabled

SIEM Destination Type: ● IP Address | FQDN

SIEM IP Address: [redacted]

SIEM TCP Port: 514

SIEM Rate: ● Unlimited | Limited

Log Type: Web Log

Feed Output Type: RSA Security Analytics

Feed Escape Character

Feed Output Format

```
<134>1 ZSCALERNSS: time=%s{time}^^timezone=%s{tz}^^action=%s{action}^^reason=%s{reason}^^hostname=%s{ehost}^^protocol=%s{proto}^^serverip
=%s{sip}^^url=%s{eurl}^^urlcategory=%s{urlcat}^^urlclass=%s{urlclass}^^dlpdictionaries=%s{dlpdict}^^dlpengine=%s{dlpeng}^^filetype
=%s{filetype}^^threatcategory=%s{malwarecat}^^threatclass=%s{malwareclass}^^pagerisk=%d{riskscore}^^threatname=%s{threatname}^^clientpublicIP
=%s{cintip}^^ClientIP=%s{cip}^^location=%s{location}^^refererURL=%s{ereferer}^^useragent=%s{ua}^^department=%s{dept}^^user
=%s{login}^^event_id=%d{recordid}^^requestmethod=%s{reqmethod}^^requestsize=%d{reqsize}^^requestversion=%s{reqversion}^^status
=%s{respcode}^^responsesize=%d{respsize}^^responseversion=%s{respversion}^^transactionsize=%d{totalsize}^^contenttype
=%s{contenttype}^^unscannabletype=%s{unscannabletype}^^deviceowner=%s{deviceowner}^^devicehostname=%s{devicehostname}^^keyprotectiontype
```

Timezone: GMT

Duplicate Logs: Disabled

Figure 5. Edit Web NSS Feed

Configure ZIA to Send Other Logs to the NetWitness Platform

To configure ZIA to send other logs to the NetWitness Platform:

1. Log in to the ZIA Admin Portal with your admin account credentials.
2. Go to **Administration** > **Nanolog Streaming Service** > **NSS Servers**.
3. Click **Add NSS Server**. To learn more, see Adding NSS Servers (government agencies, see Adding NSS Servers).
4. Click **Add NSS Feed** and input the following information:
   a. Web logs are sent via the NSS for Web VM.
   b. Firewall and DNS logs are sent via the NSS for Firewall VM.

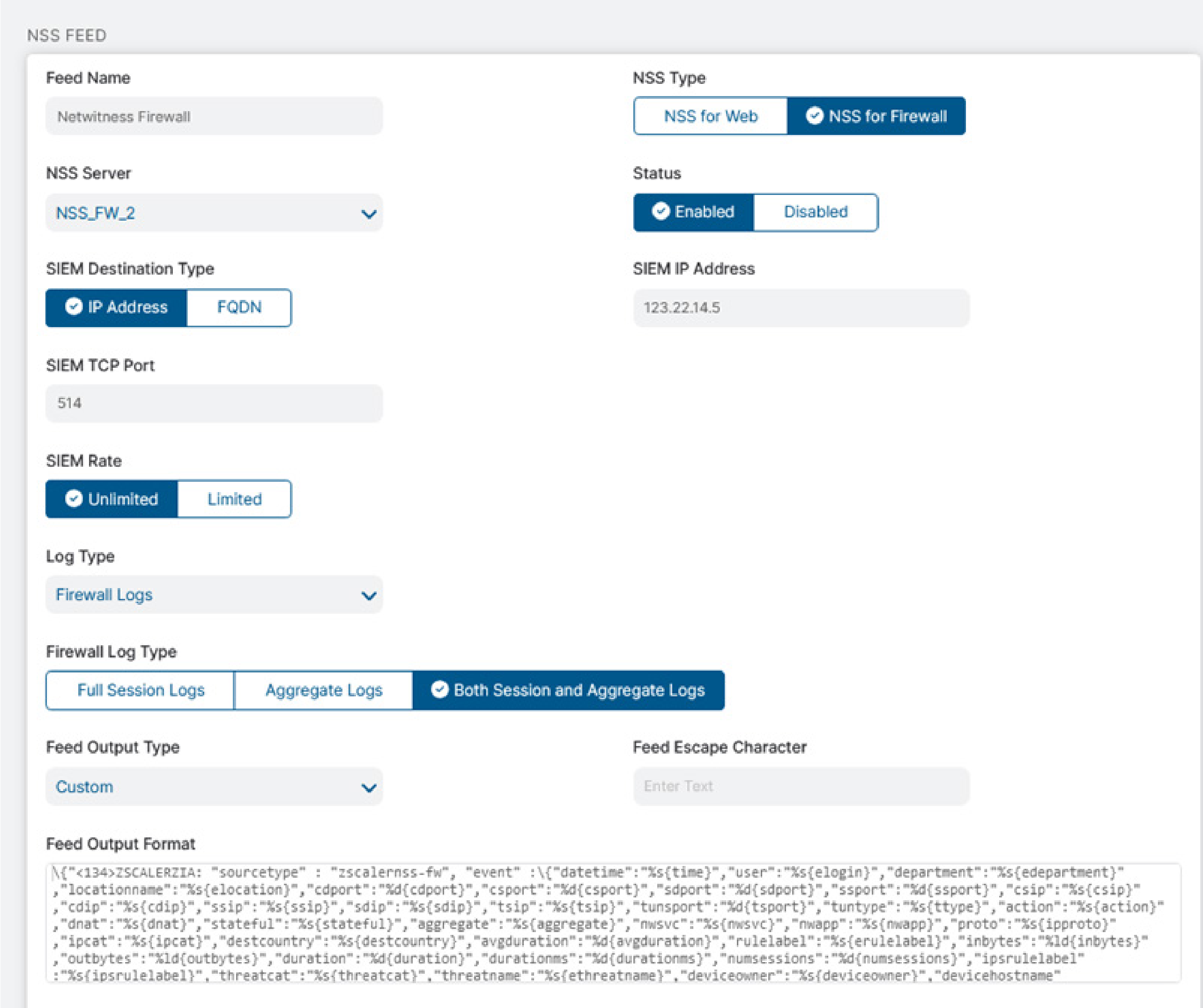
> Ensure that the NSS server State is Healthy.

   c. **Feed Name**: Enter or edit the name of the feed. Each feed is a connection between NSS and your NetWitness Platform.
   d. **NSS Type**: Choose **NSS for Web** or **NSS for Firewall**.
   e. **NSS Server**: Choose the NSS Server that you created from the list.
   f. **Status**: The NSS feed is **Enabled** by default. Choose **Disabled** if you want to activate it later.
   g. **SIEM Destination Type**: The SIEM Destination Type is set to **IP Address** by default.
   h. **SIEM IP Address**: Enter the IP address of the NetWitness Log Decoder or Remote Log Collector to which the logs are streamed.
   i. **SIEM TCP Port**: Enter `514` for NetWitness Log Decoder or Remote Log Collector.
   j. **SIEM Rate**: Leave as **Unlimited**, unless you need to throttle the output stream due to licensing or other constraints.
   k. **Log Type**: Choose any one Log Type (**Tunnel**, **Firewall**, **DNS**, **SaaS Security**, or **SaaS Security Activity**). If you want configure ZIA to send WebLogs to NetWitness, see Configure ZIA to Send WebLog Logs to the NetWitness Platform.
   l. **Feed Output Type**: Choose **JSON**.
   m. **Feed Output Format**: Add `<134>ZSCALERZIA: ` in the beginning of the Feed output format.

> When you add `<134>ZSCALERZIA: ` , the Log Template field is changed to **Custom**. Do not change it back to JSON. NetWitness recommends you copy and paste `<134>ZSCALERZIA: ` , including the space after the colon.

   n. **Timezone of the date and time in log output**: 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. You can output the configured time zone 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.
   o. **Duplicate Logs**: To ensure that no logs are skipped during any down time, specify the number of minutes that NSS sends duplicate logs. To learn more, see General Guidelines for NSS Feeds and Feed Formats (government agencies, see General Guidelines for NSS Feeds and Feed Formats).
   p. **(Optional) Select which logs are sent to the SIEM...**: Define filters to limit which logs are sent to the SIEM.
5. Click **Save**.

Firewall Logs Feed Output Format



NSS FEED

Feed Name: Netwitness Firewall

NSS Type: ○ NSS for Web ● NSS for Firewall

NSS Server: NSS_FW_2

Status: ● Enabled ○ Disabled

SIEM Destination Type: ● IP Address ○ FQDN

SIEM IP Address: 123.22.14.5

SIEM TCP Port: 514

SIEM Rate: ● Unlimited ○ Limited

Log Type: Firewall Logs

Firewall Log Type: ○ Full Session Logs ○ Aggregate Logs ● Both Session and Aggregate Logs

Feed Output Type: Custom

Feed Escape Character: Enter Text

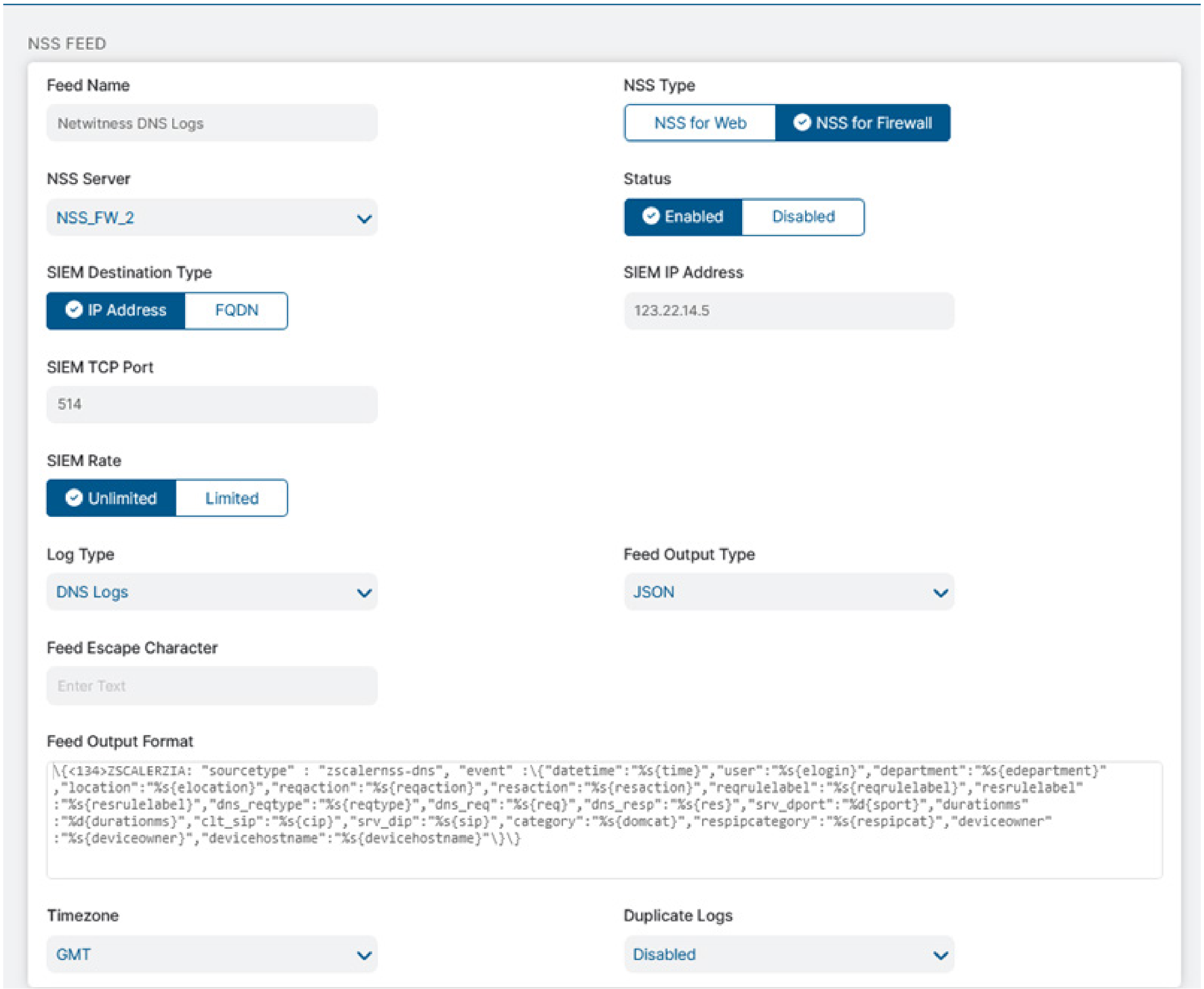
Feed Output Format:

```
\{"<134>ZSCALERZIA: "sourcetype" : "zscalernss-fw", "event" :\{"datetime":"%s{time}","user":"%s{elogin}","department":"%s{edepartment}"
,"locationname":"%s{elocation}","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}","tunsport":"%d{tsport}","tuntype":"%s{ttype}","action":"%s{action}"
,"dnat":"%s{dnat}","stateful":"%s{stateful}","aggregate":"%s{aggregate}","nwsvc":"%s{nwsvc}","nwapp":"%s{nwapp}","proto":"%s{ipproto}"
,"ipcat":"%s{ipcat}","destcountry":"%s{destcountry}","avgduration":"%d{avgduration}","rulelabel":"%s{erulelabel}","inbytes":"%ld{inbytes}"
,"outbytes":"%ld{outbytes}","duration":"%d{duration}","durationms":"%d{durationms}","numsessions":"%d{numsessions}","ipsrulelabel"
:"%s{ipsrulelabel}","threatcat":"%s{threatcat}","threatname":"%s{ethreatname}","deviceowner":"%s{deviceowner}","devicehostname"
```

Figure 6. Firewall Logs Feed Output Format

```
\{"<134>ZSCALERZIA: "sourcetype" : "zscalernss-fw", "event" :\{"datetime":"%s{time}","u
ser":"%s{elogin}","department":"%s{edepartment}","locationname":"%s{elocation}","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}","tu
nsport":"%d{tsport}","tuntype":"%s{ttype}","action":"%s{action}","dnat":"%s{dnat}","sta
teful":"%s{stateful}","aggregate":"%s{aggregate}","nwsvc":"%s{nwsvc}","nwapp":"%s{nwapp
}","proto":"%s{ipproto}","ipcat":"%s{ipcat}","destcountry":"%s{destcountry}","avgdurati
on":"%d{avgduration}","rulelabel":"%s{erulelabel}","inbytes":"%ld{inbytes}","outbytes":
"%ld{outbytes}","duration":"%d{duration}","durationms":"%d{durationms}","numsessions":"
%d{numsessions}","ipsrulelabel":"%s{ipsrulelabel}","threatcat":"%s{threatcat}","threat
name":"%s{ethreatname}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehos
tname}"\}\}
```

DNS Logs Feed Output Format



NSS FEED

Feed Name: Netwitness DNS Logs

NSS Type: ○ NSS for Web ● NSS for Firewall

NSS Server: NSS_FW_2

Status: ● Enabled ○ Disabled

SIEM Destination Type: ● IP Address ○ FQDN

SIEM IP Address: 123.22.14.5

SIEM TCP Port: 514

SIEM Rate: ● Unlimited ○ Limited

Log Type: DNS Logs

Feed Output Type: JSON

Feed Escape Character: Enter Text

Feed Output Format:

```
\{<134>ZSCALERZIA: "sourcetype" : "zscalernss-dns", "event" :\{"datetime":"%s{time}","user":"%s{elogin}","department":"%s{edepartment}"
,"location":"%s{elocation}","reqaction":"%s{reqaction}","resaction":"%s{resaction}","reqrulelabel":"%s{reqrulelabel}","resrulelabel"
:"%s{resrulelabel}","dns_reqtype":"%s{reqtype}","dns_req":"%s{req}","dns_resp":"%s{res}","srv_dport":"%d{sport}","durationms"
:"%d{durationms}","clt_sip":"%s{cip}","srv_dip":"%s{sip}","category":"%s{domcat}","respipcategory":"%s{respipcat}","deviceowner"
:"%s{deviceowner}","devicehostname":"%s{devicehostname}"\}\}
```

Timezone: GMT

Duplicate Logs: Disabled

Figure 7. DNS Logs Feed Output Format

```
\{<134>ZSCALERZIA: "sourcetype" : "zscalernss-dns", "event" :\{"datetime":"%s{time}",
"user":"%s{elogin}","department":"%s{edepartment}","location":"%s{elocation}","reqact
ion":"%s{reqaction}","resaction":"%s{resaction}","reqrulelabel":"%s{reqrulelabel}","r
esrulelabel":"%s{resrulelabel}","dns_reqtype":"%s{reqtype}","dns_req":"%s{req}","dns_
resp":"%s{res}","srv_dport":"%d{sport}","durationms":"%d{durationms}","clt_
sip":"%s{cip}","srv_dip":"%s{sip}","category":"%s{domcat}","respipcategory":"%s{respipc
at}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"\}\
```

Configure Syslog Output on ZPA

Configure at least one feed that defines the logs that the ZPA sends to NetWitness.

To configure ZPA to send logs to the NetWitness Platform:

1. Log in to the ZPA Admin Portal with your admin account credentials.
2. Create App Connector:
   a. Go to **Configuration & Control** > **Private Infrastucture** > **App Connectors** under the **App Connector Management** group.
   b. Follow the instructions given in the [About App Connectors]() (government agencies, see [About App Connectors]()) to create an App Connector.

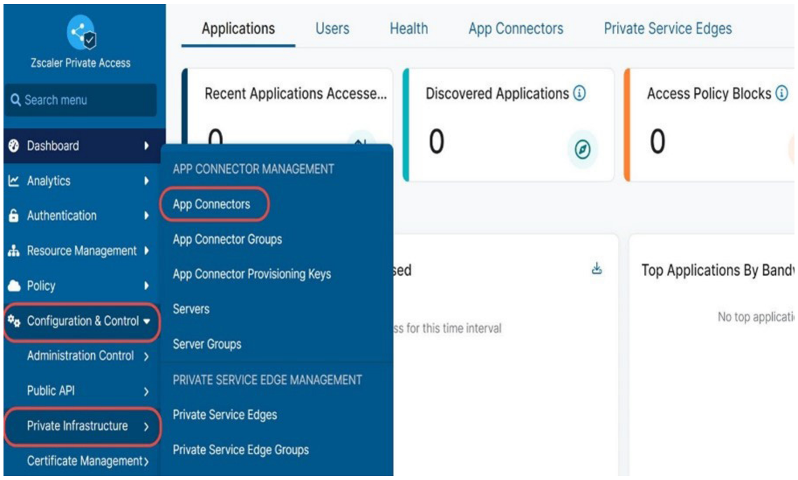
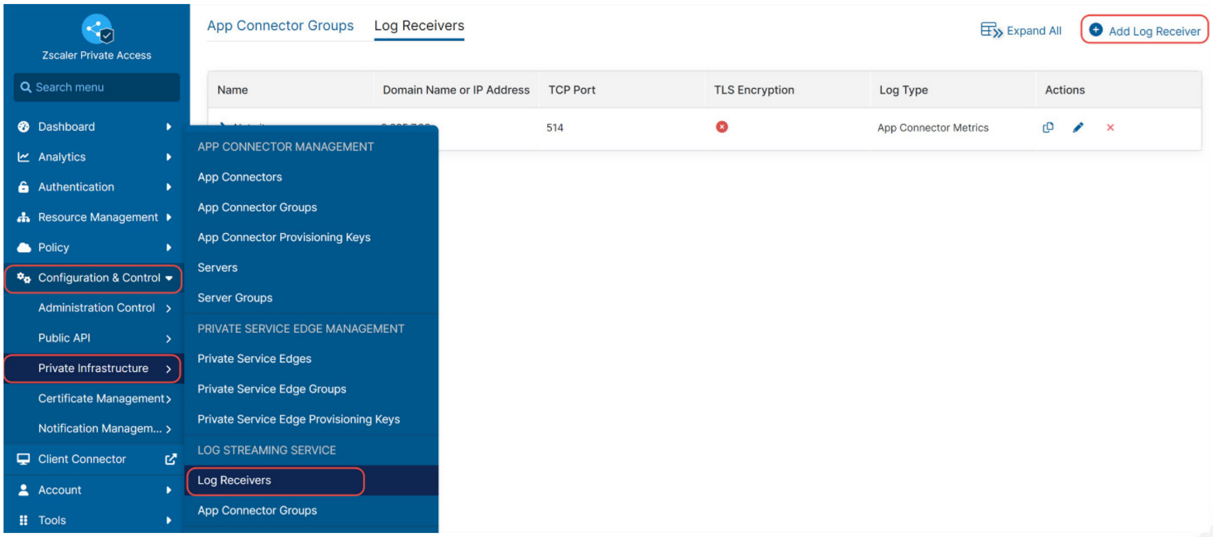


Figure 8. App Connector

3. After successfully creating an App Connector, go to **Configuration & Control** > **Private Infrastucture** > **Log Receivers** under the **Log Streaming Service** group.



Name	Domain Name or IP Address	TCP Port	TLS Encryption	Log Type	Actions
[illegible]	[illegible]	514	✕	App Connector Metrics	

Figure 9. Log stream content

4. Click **Log Stream Content** and input the following information:
    a. **Name**: Enter a name for the log receiver. The name cannot contain special characters with the exception of periods (.), hyphens (-), and underscores (_).
    b. **(Optional) Description**: Enter a description.
    c. **Domain or IP Address**: Enter the IP address and TCP Port of the NetWitness Log Decoder or Remote Log Collector to which the logs are streamed.
    d. **TCP Port**: Enter the TCP port number used by the log receiver.
    e. **TLS Encryption**: Choose **Enabled** to enable TLS encryption on traffic between the log streaming service components. It is **Disabled** by default.
    f. **App Connector Groups**: Choose an app connector group that can forward logs to the receiver and click **Next**. You can search for a specific group by clicking **Select All** to apply all groups, or click **Clear Selection** to remove all selections.

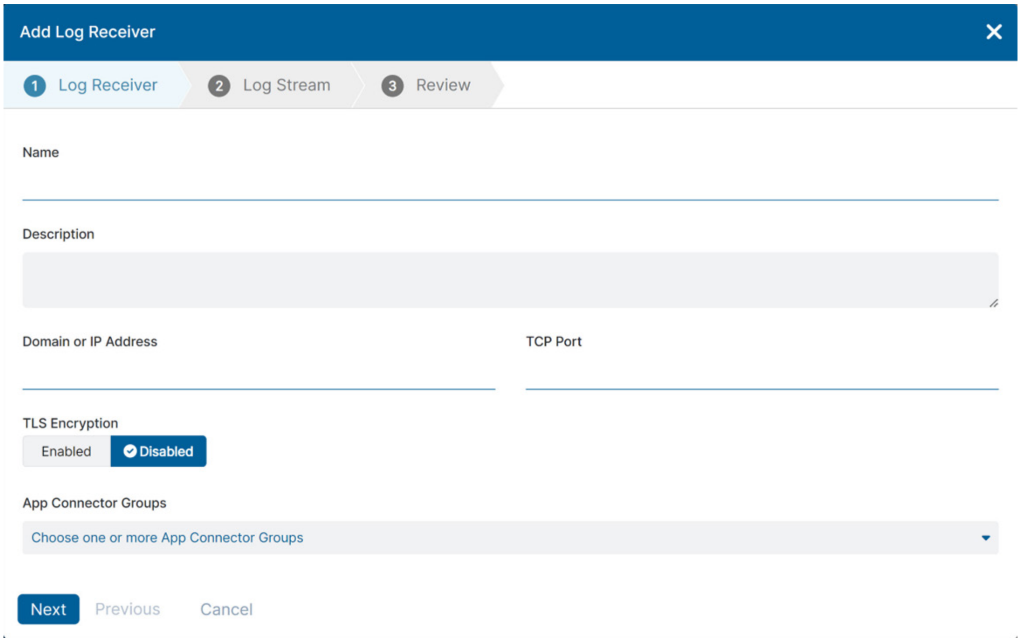
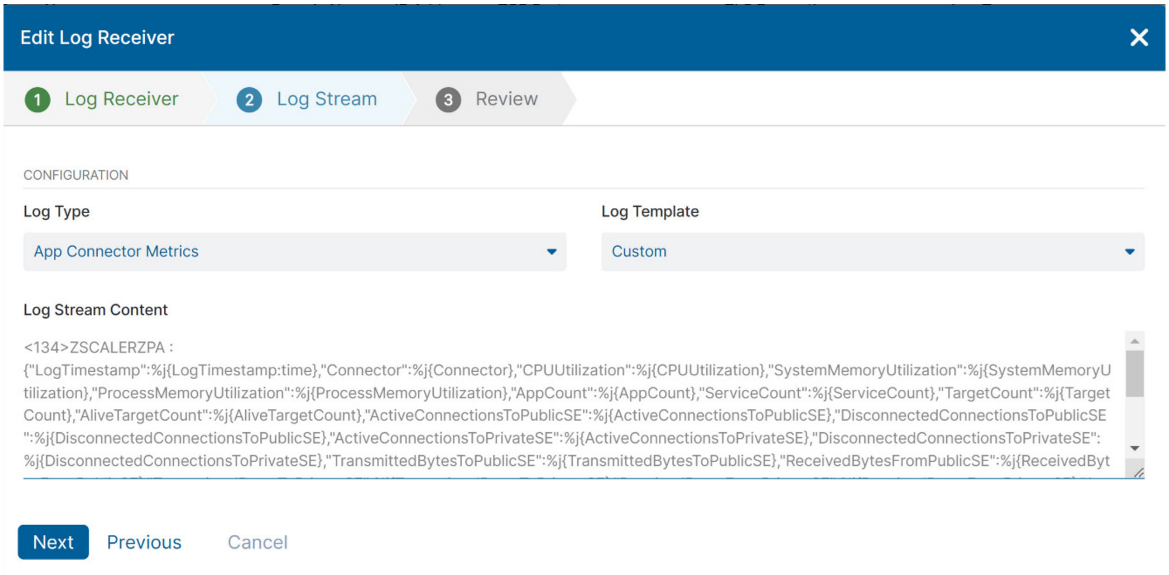


Figure 10. App Connector Groups

g. On the **Log Stream** tab, select a **Log Type** from the drop-down menu. Choose any one of the Log Types (**User Activity**, **User Status**, **App Connector Status**, **Private Service Edge Status**, **Browser Access**, **Audit Logs**, **App Connector Metrics**, or **Private Service Edge Metrics**).

h. **Log Template**: Select **JSON**.

i. **Log Stream Content**: Add `<134>ZSCALERZPA:` in the beginning of the Log Stream Content.



CONFIGURATION

Log Type: App Connector Metrics

Log Template: Custom

Log Stream Content

```
<134>ZSCALERZPA :
{"LogTimestamp":%j{LogTimestamp:time},"Connector":%j{Connector},"CPUUtilization":%j{CPUUtilization},"SystemMemoryUtilization":%j{SystemMemoryU
tilization},"ProcessMemoryUtilization":%j{ProcessMemoryUtilization},"AppCount":%j{AppCount},"ServiceCount":%j{ServiceCount},"TargetCount":%j{Target
Count},"AliveTargetCount":%j{AliveTargetCount},"ActiveConnectionsToPublicSE":%j{ActiveConnectionsToPublicSE},"DisconnectedConnectionsToPublicSE
":%j{DisconnectedConnectionsToPublicSE},"ActiveConnectionsToPrivateSE":%j{ActiveConnectionsToPrivateSE},"DisconnectedConnectionsToPrivateSE":
%j{DisconnectedConnectionsToPrivateSE},"TransmittedBytesToPublicSE":%j{TransmittedBytesToPublicSE},"ReceivedBytesFromPublicSE":%j{ReceivedByt
```

Figure 11. Log Stream Content

When you add `<134>ZSCALERZPA:` , the Log Template is changed to **Custom**. Do not change it back to JSON. NetWitness recommends you copy and paste `<134>ZSCALERZPA:` , including the space after the colon.

5. Click **Next** and review all the provided information.
6. Click **Save**.

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**.

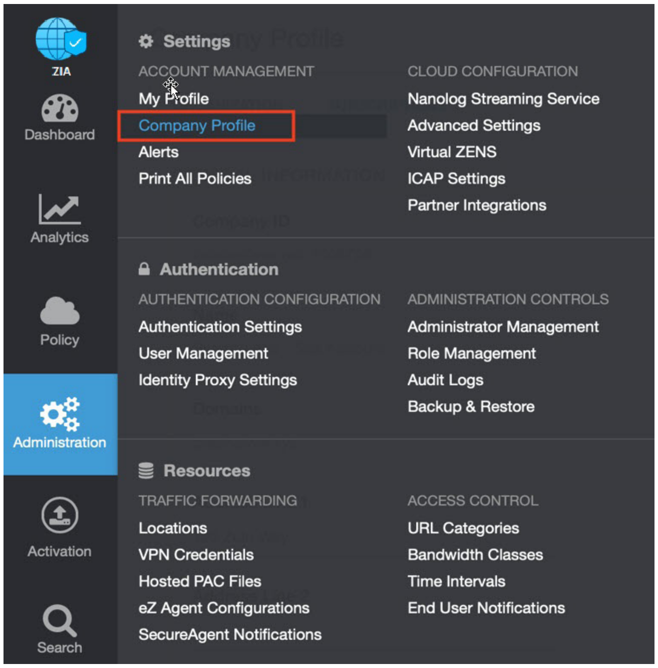
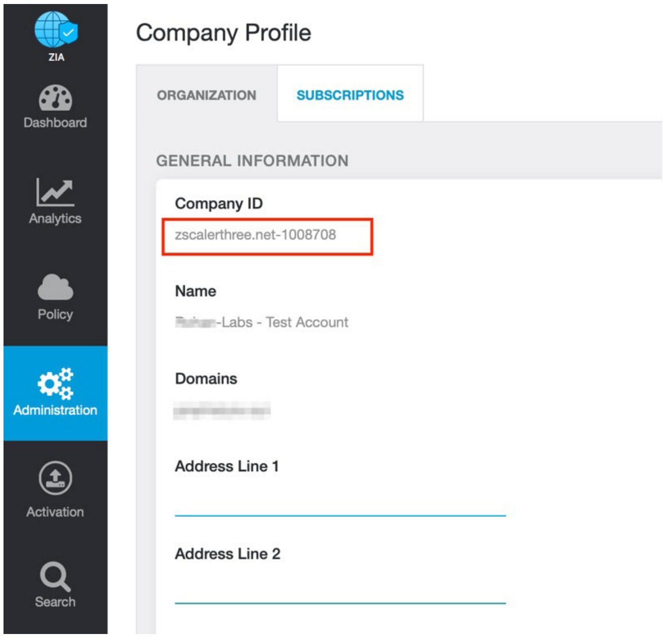


Figure 12. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.



Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 13. Company ID

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

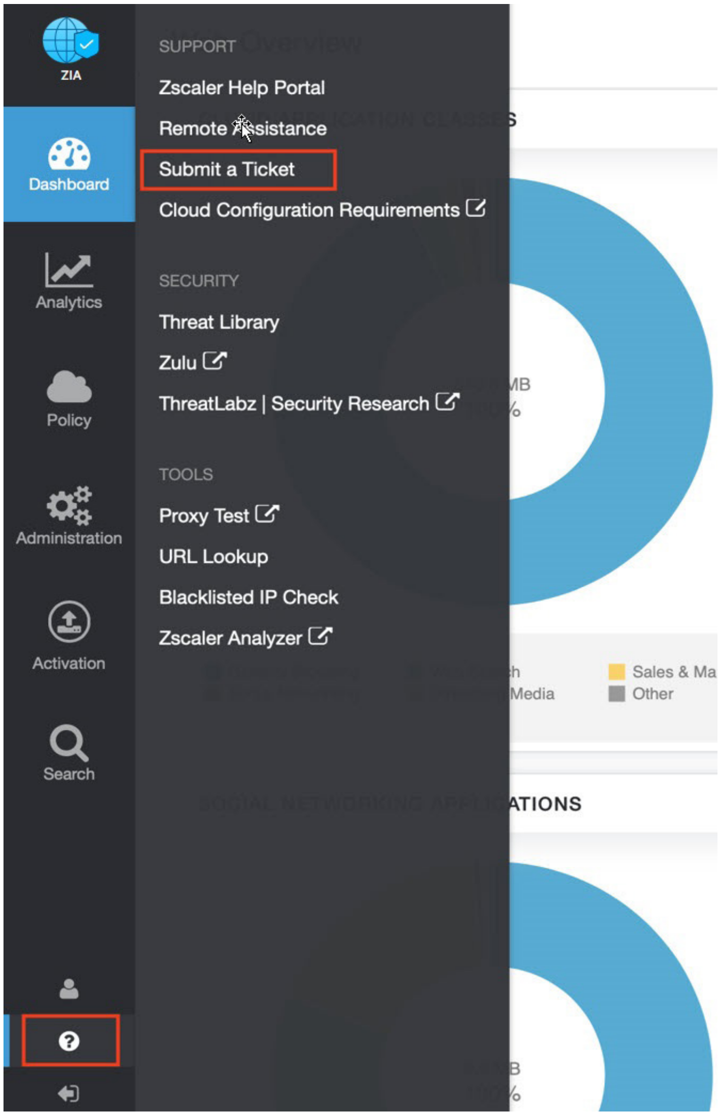


Figure 14. Submit a ticket