ZSCALER AND TEHTRIS DEPLOYMENT GUIDE

APRIL 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.

TEHTRIS Overview

TEHTRIS is the software editor of the TEHTRIS XDR Platform, the world leader in automatic, real-time, non-human neutralization of cyberattacks. The TEHTRIS solution provides cybersecurity specialists with a holistic view of their infrastructure, while guaranteeing the confidentiality of their data. The TEHTRIS XDR Platform is interoperable with existing security solutions through its APIs and integrated orchestrator. The company is positioned as a European trusted third party. Together with its international partners, TEHTRIS XDR Platform monitors, analyzes, detects, and neutralizes threats worldwide for the benefit of major players in industry, transportation, engineering, services, and administrations. TEHTRIS is constantly on the lookout for cybercrime and listens to its customers to reduce the risks as much as possible and to face the unpredictable. To learn more, refer to the TEHTRIS 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
- **TEHTRIS 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 TEHTRIS Introduction

Overviews of the Zscaler and TEHTRIS 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 Browser 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 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.
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.

TEHTRIS SIEM Overview

TEHTRIS Security Information and Event Management (SIEM) provides an effective alerting tool to monitor the security of your systems and applications through reports and event dashboards powered by a correlation engine fed by threat intelligence from the extensive TEHTRIS XDR Platform.

The resulting analysis allows you to keep an eye on the security health of your systems while your assets are under control through real-time data aggregation. This keeps track of abnormal behavior and also provides data retention for further forensic analysis that allows you to hunt down threats at a higher level for better compliance with common standards.

Integrated with the TEHTRIS XDR Platform, TEHTRIS SIEM enables real-time incident detection and response, and automation of Security Operations Center (SOC) services to provide insights and smart alerts, making the job of your SOC response team easier.

The key features of TEHTRIS SIEM are:

- Simplified deployment of your SIEM infrastructure.
- Solution operated by TEHTRIS which maintains it in operational condition at all times.
- Flexible integration on-premises or in the cloud, or both in Hybrid mode.
- Cloud sources are taken into account (e.g., Azure Active Directory / Office 365, Salesforce, etc.).
- Possibility to build source-based offerings for unlimited number of Endpoint Protection Platform (EPP) agent-based and agentless log collection.
- Monitoring of all your IT and OT equipment.
- Compatible with all operating systems (Unix, Windows, etc.).
- Compatible with all the components of your infrastructure (routers, firewalls, proxies, switches, bastion hosts, etc.).
- Compatible with all your applications to be monitored (antiviruses, databases, SAP, etc.).
- Provision of hundreds of correlation rules covering all the attacks recognized by TEHTRIS and collected by default on your SIEM to be operational from day one.
- All formats are accepted: LEEF, CEF, JSON, CSV, etc.
- All standard protocols are accepted: Syslog TCP, Syslog UDP, etc.
- Extra correlation rules may be added to cover business aspects and internal applications (business rules).
- Ultra-secure solution running on appliances containing a hardened kernel (anti-zero-day) with a fully encrypted hard drive.
- Simplified and scalable integration of TEHTRIS SIEM appliances in your VMware ESXi environments. The hardware can be scaled over time to keep up with the evolution of your SIEM solution (more CPU, RAM, or disk).

TEHTRIS Resources

The following table contains links to TEHTRIS support resources.

Name	Definition
TEHTRIS Services & Support	Description of the TEHTRIS Security solution.

TEHTRIS SIEM Architecture

Security Information and Event Management (SIEM) allows you to collect and filter billions of logs from all kinds of network sources (operating system, cloud, firewalls, proxies, database, antivirus, etc.). Thanks to multiples alert rules, TEHTRIS SIEM raises security alerts on specific events logged. From the TEHTRIS XDR Platform, TEHTRIS SIEM also allows searching more precise details directly in collected and parsed logs.

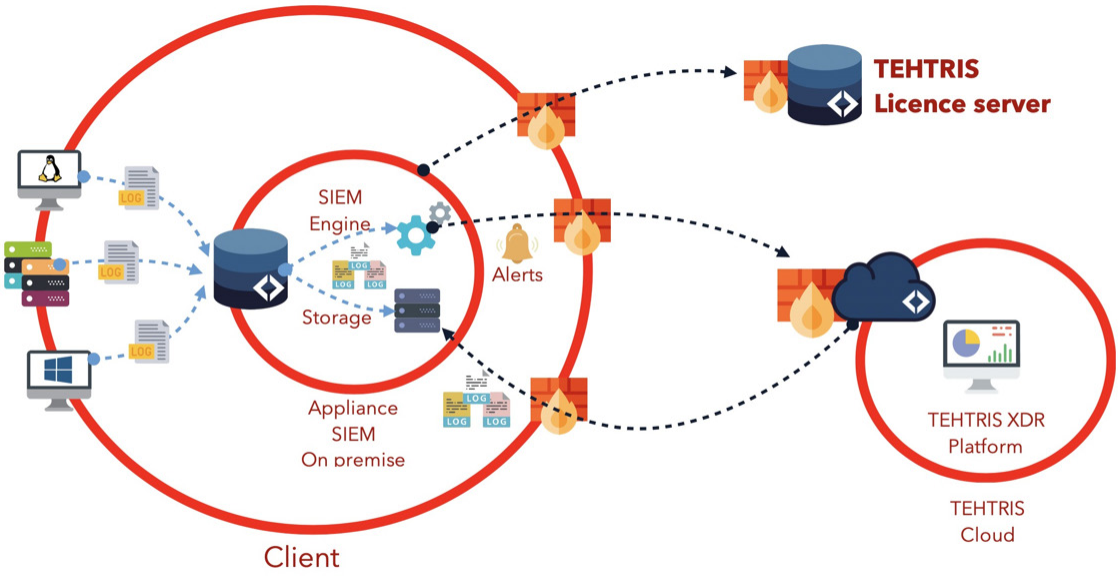

Figure 1. TEHTRIS architecture

Zscaler Configuration

This documentation provides the steps required to configure Nanolog Streaming Service (NSS) and Log Streaming Service (LSS) in order to send Zscaler raw logs to your TEHTRIS SIEM appliance.

The main focus is on ZIA and ZPA solutions.

ZIA Setup

This section presents how to set up ZIA Nanolog Streaming Service (NSS) to send logs to a TEHTRIS SIEM appliance.

An NSS feed specifies data from the logs that the NSS sends to the SIEM. One NSS feed can process only one type of log.

An NSS server is a representation of the NSS VM in the ZIA Admin Portal. NSS feeds retrieve logs from Zscaler, then applies the format from the NSS feed and sends logs to the SIEM.

For more information related to the setup, see the ZIA Help Portal (government agencies, see ZIA Help Portal).

NSS Server Setup

For each NSS feed addition, you must create a NSS server.

In order to create a NSS server:

1. Navigate to **Administration** > **Nanolog Streaming Service**.

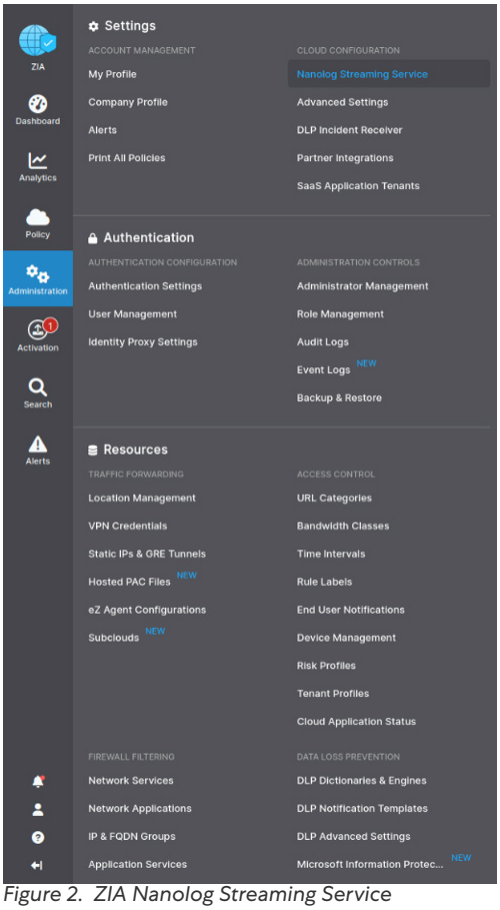

Figure 2. ZIA Nanolog Streaming Service

2. In the **NSS** tab, click **Add NSS Server.**

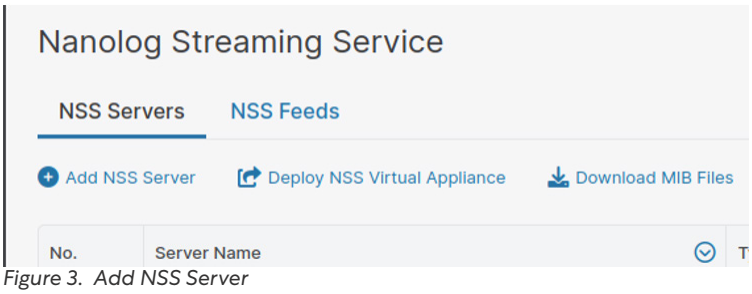

Figure 3. Add NSS Server

3. Define a name for the NSS server, then, choose between **NSS for Web** or **NSS for Firewall**.
4. Click **Save**.

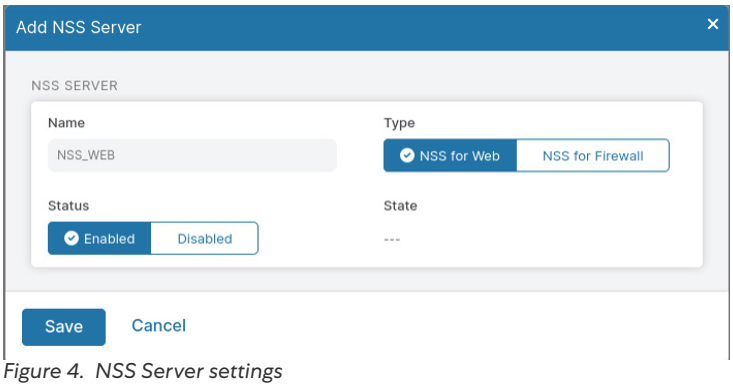

Figure 4. NSS Server settings

Zscaler administrator's rights are needed to make the whole deployment on an appliance.

The NSS server must be deployed to send logs on a SIEM. Each NSS server can have only one NSS feed.

Create NSS Feeds

To create an NSS Feed:

1. Navigate to **Administration** > **Nanolog Streaming Service**.
2. In the **NSS Feed** tab, click **Add NSS Feed**.

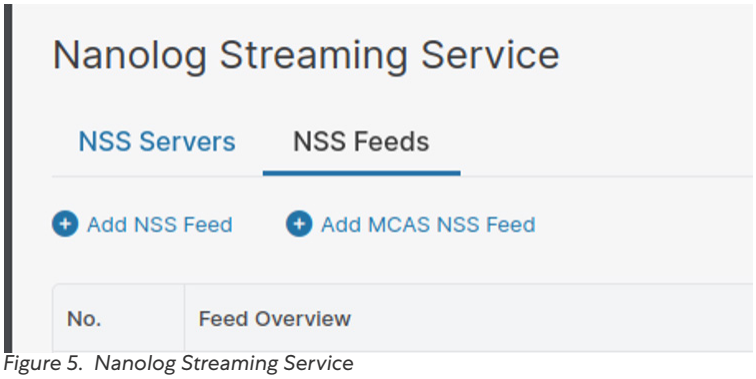

Figure 5. Nanolog Streaming Service

3. Configure the following settings for each NSS feed (in order to send logs to the TEHTRIS SIEM, you must configure this specific settings for every log type):

Name Field	Value
Status	Enabled
SIEM IP Address	TEHTRIS SIEM IP
SIEM TCP Port	514
SIEM Rate	Unlimited
SIEM Destination Type	IP Address
Feed Output Type	Tab-Separated
Duplicate Logs	Disabled
Timezone	GMT

4. Replace **TEHTRIS SIEM IP** with the IP address of your TEHTRIS SIEM appliance, as provided by TEHTRIS Support.

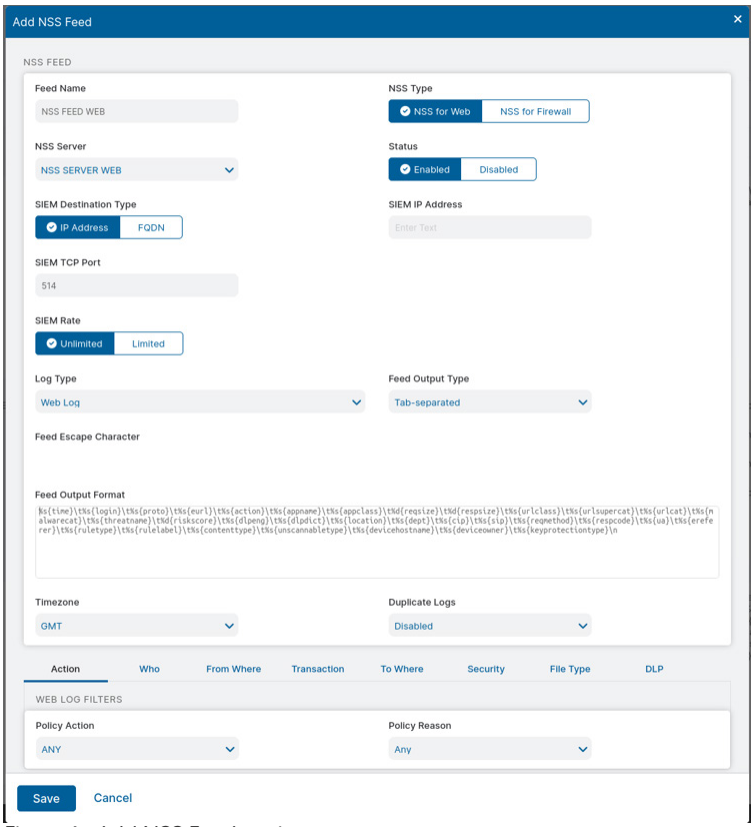

Figure 6. Add NSS Feed settings

The feed name must be different on each NSS feed. Don't modify any parameters not mentioned in this documentation.

NSS Web

NSS Web contains different log types:

- Web logs
- Tunnel logs
- SaaS Security logs
- Admin Audit logs

For each NSS Web log type, select NSS for Web within your NSS Server.

Web Logs

- Log Type: Web Log (government agencies, see Web Log).
-
- Feed Output Format:

```
%s{time}\t%s{login}\t%s{host}\t%s{proto}\t%s{eurl}\t%s{action}\t%s{appname}\
t%s{appclass}\t%d{reqsize}\t%d{respsize}\t%d{stime}\t%d{ctime}\t%s{urlclass}\
t%s{urlsupercat}\t%s{urlcat}

\t%s{malwarecat}\t%s{threatname}\t%d{riskscore}\t%s{location}\t%s{dept}\t%s{cip}\
t%s{sip}\t%s{reqmethod}\t%s{respcode}\t%s{ua}\t%s{ereferer}\t%s{devicemodel}\
t%s{devicename}

\t%s{srvcertchainvalpass}\t%s{datacentercountry}\t%s{datacentercity}\t%s{datacenter}\
t%s{fileclass}\t%s{malwareclass}\t%s{filetype}\t%s{cintip}\t%s{respcode}\t%s{reason}\
t%d{recordid}

\t%d{totalsize}\t%s{trafficredirectmethod}\t%s{devicehostname}\tweb
```

- Log Sample :

```
{"MessageSourceAddress": "54.00.00.10", "EventReceivedTime": "2023-01-
26T12:44:07.081009+00:00", "SourceModuleName": "i_tcp_zia", "SourceModuleType":
"im_tcp", "eGImport": "import", "RawLogSizeByte": 573, "eGDirectory": "SEC_
Zscaler_ZIA/54.220.65.10", "TehtrisLogId": "1ac89038-f32a-1005-807d-6f312e703234",
"EventTime": "2023-01-26T12:44:05.000000+00:00", "user": "test@dev-tehtris.com",
"hostname": "cdn.lamp.avct.cloud", "protocol": "HTTP_PROXY", "url": "cdn.lamp.avct.
cloud:443", "action": "Allowed", "appname": "General Browsing", "appclass": "General
Browsing", "requestsize": "572", "responsesize": "65", "servertranstime": "0",
"clienttranstime": "0", "urlclass": "Business Use", "urlsupercategory": "Business
and Economy", "urlcategory": "Professional Services", "threatcategory": "None",
"threatname": "None", "pagerisk": "0", "location": "Road Warrior", "department":
"test", "ClientIP": "185.00.00.39", "serverip": "13.00.00.48", "requestmethod":
"CONNECT", "status": "200", "useragent": "Linux Ubuntu 20.04.3 LTS ZTunnel/1.0",
"refererURL": "None", "zccdevmodel": "VMware Virtual Platform", "zccdevname":

"M2VmYjc5NjQzYmFiNThlMzJjM2NjNmE4YzhmMDY1YjI5Mj
UzNzY5YTAyNWVjNzEzMWI4ZDM4MTAwYTg2NzY3OQ==:
```


nG6xExtCAq0Zl2VGU5Gpn2SYAJw=", "srvcertchainvalpass": "UNKNOWN", "datacentercountry": "DE", "datacentercity": "Fr", "datacenter": "FRA4", "fileclass": "None", "threatclass": "None", "filetype": "None", "clientpublicIP": "185.00.00.39", "reason": "Allowed", "event_id": "7192940838106234882", "transactionsize": "637", "trafficredirectmethod": "ZscalerClientConnector", "port": "443", "uri_path": null, "uri_query": null, "log_channel": "web", "GuessedPlatform": "zscaler", "LogType": "Zscaler Internet Access (ZIA) via NSS"}

Tunnel Logs

- Log Type : Tunnel Log (government agencies, see Tunnel Log).

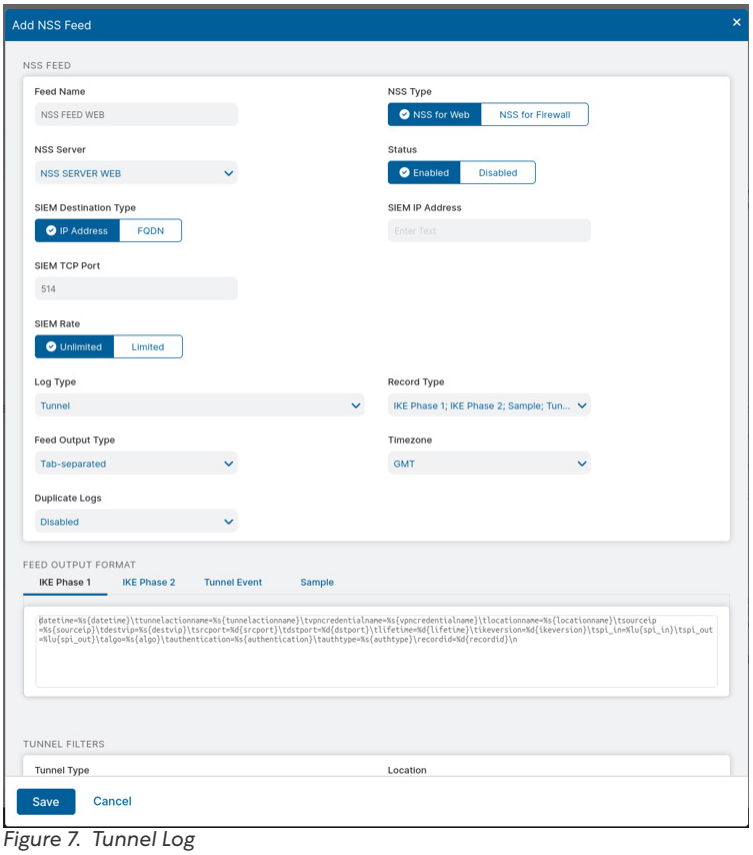

Figure 7. Tunnel Log

IKE Phase 1

- Feed Output Format:

```
%s{datetime}\t%s{tunnelactionname}\t%s{vpncredentialname}\t%s{locationname}\
t%s{sourceip}\t%s{destvip}\t%d{srcportstart}\t%d{destportstart}\t%s{srcipstart}\
t%s{srcipend}\t%s{destipstart}

\t%s{destipend}\t%d{lifetime}\t%d{ikeversion}\t%d{lifebytes}\t%d{spi}\t%s{algo}\
t%s{authentication}\t%s{authtype}\t%s{protocol}\t%s{tunnelprotocol}\t%-
s{policydirection}\t%d{recordid}

\ttunnel_ike2\n
```


- Log Sample:

{“MessageSourceAddress”: “127.00.00.1”, “EventReceivedTime”: “2022-10-25T08:13:02.849845+00:00”, “SourceModuleName”: “i_test_zscaler_ike1”, “SourceModuleType”: “im_tcp”, “datetime”: “2022-10-25T08:06:35.000000+00:00”, “tunnelactionname”: “IPSec Phase2”, “vpncredentialname”: “3.00.00.47”, “locationname”: “aws-dublin”, “sourceip”: “3.00.00.47”, “destvip”: “165.00.00.39”, “srcportstart”: “0”, “destportstart”: “0”, “srcipstart”: “0.00.00.0”, “srcipend”: “0.00.00.0”, “destipstart”: “10.00.00.0”, “destipend”: “10.00.00.255”, “lifetime”:

“86400”, “ikeversion”: “2”, “lifebytes”: “0”, “spi”: “3352167295”, “algo”: “AES-CBS”, “authentication”: “HMAC-SHA2-256-128”, “authtype”: “None”, “protocol”: “Any”, “tunnelprotocol”: “ESP”, “policydirection”: “Outbound SA Policy”, “recordid”: “7158358405684133892”, “log_channel”: “tunnel_ike2”, “eGDirectory”: “SEC_Zscaler_ZIA/127.0.0.1”, “GuessedPlatform”: “zscaler”, “LogType”: “Zscaler Internet Access (ZIA) via NSS”, “EventTime”: “2022-10-25T08:13:02.849845+00:00”}

IKE Phase 2

- Feed Output Format:

```
%s{datetime}\t%s{tunnelactionname}\t%s{vpncredentialname}\t%s{locationname}\
t%s{sourceip}\t%s{destvip}\t%d{srcportstart}\t%d{destportstart}\t%s{srcipstart}\
t%s{srcipend}\t%s{destipstart}

\t%s{destipend}\t%d{lifetime}\t%d{ikeversion}\t%d{lifebytes}\t%d{spi}\t%s{algo}\
t%s{authentication}\t%s{authtype}\t%s{protocol}\t%s{tunnelprotocol}\t%-
s{policydirection}\t%d{recordid}

\ttunnel_ike2\n
```

- Log Sample:

{“MessageSourceAddress”: “127.00.00.1”, “EventReceivedTime”: “2022-10-25T08:13:02.849845+00:00”, “SourceModuleName”: “i_test_zscaler_ike1”, “SourceModuleType”: “im_tcp”, “datetime”: “2022-10-25T08:06:35.000000+00:00”, “tunnelactionname”: “IPSec Phase2”, “vpncredentialname”: “3.00.00.47”, “locationname”: “aws-dublin”, “sourceip”: “3.00.00.47”, “destvip”: “165.00.00.39”, “srcportstart”: “0”, “destportstart”: “0”, “srcipstart”: “0.00.00.0”, “srcipend”: “0.00.00.0”, “destipstart”: “10.00.00.0”, “destipend”: “10.00.00.255”, “lifetime”:

“86400”, “ikeversion”: “2”, “lifebytes”: “0”, “spi”: “3352167295”, “algo”: “AES-CBS”, “authentication”: “HMAC-SHA2-256-128”, “authtype”: “None”, “protocol”: “Any”, “tunnelprotocol”: “ESP”, “policydirection”: “Outbound SA Policy”, “recordid”: “7158358405684133892”, “log_channel”: “tunnel_ike2”, “eGDirectory”: “SEC_Zscaler_ZIA/127.0.0.1”, “GuessedPlatform”: “zscaler”, “LogType”: “Zscaler Internet Access (ZIA) via NSS”, “EventTime”: “2022-10-25T08:13:02.849845+00:00”}

Tunnel Events

- Feed Output Format:

```
%s{datetime}\t%s{tunnelactionname}\t%s{tunneltype}\t%s{vpncredentialname}\
t%s{locationname}\t%s{sourceip}\t%s{destvip}\t%d{srcport}\t%s{event}\t%s{eventreason}\
t%d{recordid}\ttunnel_event\n
```

- Log Sample:

{“MessageSourceAddress”: “127.00.00.1”, “EventReceivedTime”: “2022-10-24T13:59:01.229924+00:00”, “SourceModuleName”: “i_test_zscaler”, “SourceModuleType”: “im_tcp”, “datetime”: “2022-10-24T12:48:09.000000+00:00”, “tunnelactionname”: “Tunnel Event”, “tunneltype”: “IPSec IKEv2”, “vpncredentialname”: “3.00.00.47”, “locationname”: “aws-dublin”, “sourceip”:

“3.00.00.47”, “destvip”: “165.00.00.39”, “srcport”: “4500”, “event”: “IPsec tunnel is up”, “eventreason”: “None”, “recordid”: “7158059879687258118”, “log_channel”: “tunnel_event”, “eGDirectory”: “SEC_Zscaler_ZIA/127.0.0.1”, “GuessedPlatform”: “zscaler”, “LogType”: “Zscaler Internet Access (ZIA) via NSS”, “EventTime”: “2022-10-24T13:59:01.229924+00:00”}

Tunnel Samples

- Feed Output Format:

```
%s{datetime}\t%s{tunnelactionname}\t%s{tunneltype}\t%s{vpncredentialname}\
t%s{locationname}\t%s{sourceip}\t%s{destvip}\t%d{srcport}\t%lu{txbytes}\t%lu{rxbytes}\
t%d{dpdrec}\t%d{recordid}

\ttunnel_sample\n
```

- Log Sample:

{“MessageSourceAddress”: “63.00.00.2”, “EventReceivedTime”: “2022-10-24T12:06:02.169770+00:00”, “SourceModuleName”: “i_test_zscaler”, “SourceModuleType”: “im_tcp”, “datetime”: “2022-10-24T12:06:00.000000+00:00”, “tunnelactionname”: “Tunnel Samples”, “tunneltype”: “IPSec IKEv2”, “vpncredentialname”: “3.00.00.47”, “locationname”: “aws-dublin”, “sourceip”: “3.00.00.47”, “destvip”: “165.00.00.39”, “srcport”: “4500”, “txbytes”: “0”, “rxbytes”: “384”, “dpdrec”: “0”, “recordid”: “7158049017714966529”, “log_channel”: “tunnel_event”, “eGDirectory”: “SEC_Zscaler_ZIA/63.34.200.2”, “GuessedPlatform”: “zscaler”, “LogType”: “Zscaler Internet Access (ZIA) via NSS”, “EventTime”: “2022-10-24T12:06:02.169770+00:00”}

SaaS Security Logs

- Log Type: SaaS Security (government agencies, see SaaS Security).
- Add one NSS feed for each SaaS security log type. Zscaler provides you with a list of available applications for each SaaS Security subtypes of logs. Without one of these applications, you can’t collect the logs.

As an example, if you have GitHub, Slack, and Dropbox as application on Zscaler, you must create three NSS Feeds: SaaS Security Collaboration, SaaS Security ITSM, and SaaS Security File.

Consult available applications on your Zscaler tenant by navigating to Administration > SaaS Application Tenants.

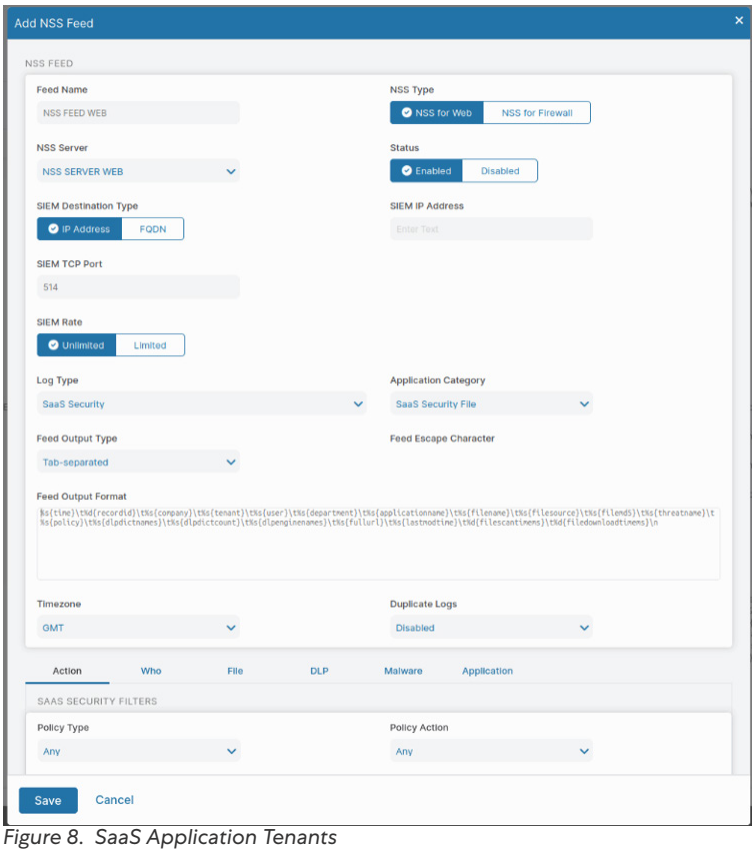

Figure 8. SaaS Application Tenants

Public Cloud Storage

- Application Category: Public Cloud Storage
- Compatible application: Amazon S3
- Feed Output Format:

```
%s{time}\t%d{recordid}\t%s{company}\t%s{tenant}\t%s{owner}\t%s{department}\
t%s{applicationname}\t%s{filename}\t%s{filesource}\t%s{filemd5}\t%s{threatname}\
t%s{policy}\t%s{dlpdictnames}

\t%s{dlpdictcount}\t%s{dlpenginenames}\t%s{fullurl}\t%s{lastmodtime}\t%s{bucketname}\
tcloud
```


Security Collaboration

- Application Category: SaaS Security Collaboration
- Compatible applications: Slack, Microsoft Teams
- Feed Output Format:

```
%s{tenant}\t%s{applicationname}\t%s{time}\t%s{owner}\t%s{filename}\t%s{filetypename}\
t%d{filesize}\t%s{filemd5}\t%s{extownername}\t%s{policy}\t%s{rulelabel}\t%s{ruletype}\
t%s{malware}

\t%s{threatname}\t%s{malwareclass}\t%s{dlpdictnames}\t%s{dlpenginenames}\
t%d{dlpidentifier}\t%s{severity}\t%s{dlpdictcount}\t%s{internal_recptnames}\
t%s{external_recptnames}

\t%s{ointernal_recptnames}\t%s{oexternal_recptnames}\t%s{sharedchannel_hostname}\
t%s{osharedchannel_hostname}\t%s{sender}\t%s{osender}\t%s{esender}\t%s{channel_name}\
t%s{ochannel_name}

\t%s{company}\t%s{department}\tcollaboration
```

- Log Sample:

```
{"MessageSourceAddress": "127.00.00.1", "EventReceivedTime": "2022-10-
18T08:44:35.074587+00:00", "SourceModuleName": "i_test_zscaler", "SourceModuleType":
"im_tcp", "time":

"2022-10-12T12:52:52.000000+00:00", "tenant": "QA-Box", "applicationname": "Box",
"owner": "jsmith", "filename": "test.pdf", "filetypename": "pdf", "filesize": "6721",
"filemd5": "196a3d797bfee07fe4596b69f4ce1141", "extownername": "jane@yahoo.com",
"policy": "Revoke", "rulelabel": "no tehtris", "ruletype": "File Type Control",
"malware": "Virus", "threatname": "None", "malwareclass": "Win32.Ransom.WannaCry",
"dlpdictnames": "Credit Cards&#124", "dlpenginenames": "HIPAA&#124", "dlpidentifier":
"6646484838839025669", "severity": "High Severity", "dlpdictcount": "4&#124",
"internal_recptnames": "john@yahoo.com&#124;doe@gmail.com", "external_recptnames":
"jane@yahoo.com&#124;roe@gmail.com", "ointernal_recptnames": "243561&#124;779116",
"oexternal_recptnames": "753148&#124;091212", "sharedchannel_hostname": "channel",
"osharedchannel_hostname": "63897110953", "sender": "johndoe@slack.com", "osender":
"9854901", "esender": "6A6F6E646F6540736C61636B2E636F6D", "channel_name": "demo-ops",
"ochannel_name": "9769110", "company": "Zscaler", "department": "test", "log_channel":
"saas_collaboration", "eGDirectory": "SEC_Zscaler_ZIA/127.0.0.1", "GuessedPlatform":
"zscaler", "LogType": "Zscaler Internet Access (ZIA) via NSS", "EventTime":

"2022-10-18T08:44:35.074587+00:00"}
```


Security CRM

- Application Category: CRM
- Compatible application: Salesforce
- Feed Output Format:

```
%s{tenant}\t%s{applicationname}\t%s{time}\t%s{owner}\t%s{filename}\t%s{filetypename}\
t%d{filesize}\t%s{filemd5}\t%s{extownername}\t%s{policy}\t%s{rulelabel}\t%s{ruletype}\
t%s{malware}

\t%s{threatname}\t%s{malwareclass}\t%s{dlpdictnames}\t%s{dlpenginenames}\
t%d{dlpidentifier}\t%s{severity}\t%s{dlpdictcount}\t%s{objectname}\t%s{objecttype}\
t%s{filetypecategory}

\t%s{hostname}\t%s{internal_collabnames}?\t%s{external_collabnames}?\t%s{filepath}\
t%s{component}\t%s{sha}\t%s{company}\t%s{department}\CRM
```

- Log Sample:

```
{"MessageSourceAddress": "63.00.00.2", "EventReceivedTime": "2022-11-
14T10:58:41.434234+00:00", "SourceModuleName": "i_zscaler", "SourceModuleType":
"im_tcp", "eGImport": "import", "log_channel": "saas_crm", "time": "2022-11-
14T10:57:52.000000+00:00", "tenant": "salesforce test", "applicationname":
"SALESFORCE", "owner": "unknown_saas_user$@11242169.zscalerbeta.net", "filename":
"chatter-message", "filetypename": "txt", "filesize": "352", "filemd5": "None",
"extownername": "tyqubannudd-3415@yopmail.com", "policy": "None", "rulelabel":
"None", "ruletype": "None", "malware": "None", "threatname": "None", "malwareclass":
"None", "dlpdictnames": "None", "dlpenginenames": "None", "dlpidentifier": "0",
"severity": "None", "dlpdictcount": "None", "objectname": "None", "objecttype":
"None", "filetypecategory": "Text File", "hostname": "Unknown Host", "internal_
collabnames": "None", "external_collabnames": "None", "filepath": "None", "component":
"Message", "sha": "None", "company": "Tehtris", "department": "Default Department",
"eGDirectory": "SEC_Zscaler_ZIA/63.34.200.2", "GuessedPlatform": "zscaler",
"LogType": "Zscaler Internet Access (ZIA) via NSS", "EventTime": "2022-11-
14T10:58:41.434234+00:00"}
```

Security Repository

- Application Category: Repository
- Compatible application: ServiceNow
- Feed Output Format:

```
%s{time}\t%s{tenant}\t%s{applicationname}\t%s{owner}\t%s{filename}\t%s{filetypename}\
t%d{filesize}\t%s{filemd5}?\t%s{extownername}\t%s{policy}\t%s{rulelabel}\t%s{ruletype}\
t%s{malware}

\t%s{threatname}\t%s{malwareclass}\t%s{dlpdictnames}\t%s{dlpenginenames}\
t%d{dlpidentifier}\t%s{severity}\t%s{dlpdictcount}\t%s{objectname}\t%s{objecttype}\
t%s{filetypecategory}

\t%s{hostname}\t%s{internal_collabnames}?\t%s{external_collabnames}?\t%d{filesize}\
t%s{filepath}\t%s{component}\t%s{sha}?\t%s{collabscope}?\t%s{filemd5}?\t%s{filename}\
t%s{company}

\t%s{department}\trepository
```


Security ITSM

- Application Category: ITSM
- Compatible application: GitHub
- Feed Output Format:

```
%s{time}\t%s{tenant}\t%s{applicationname}\t%s{owner}\t%s{filename}\t%s{filetypename}\
t%d{filesize}\t%s{filemd5}\t%s{extownername}\t%s{policy}\t%s{rulelabel}\t%s{ruletype}\
t%s{malware}

\t%s{threatname}\t%s{malwareclass}\t%s{dlpdictnames}\t%s{dlpenginenames}\
t%d{dlpidentifier}\t%s{severity}\t%s{dlpdictcount}\t%s{objectname}\t%s{objecttype}\
t%s{filetypecategory}

\t%s{hostname}\t%s{internal_collabnames}?\t%s{external_collabnames}?\t%d{filesize}\
t%s{filepath}\t%s{component}\t%s{sha}?\t%s{collabscope}?\t%s{filemd5}?\t%s{filename}\
t%s{company}

\t%s{department}\titsm
```

Security Email

- Application Category: SaaS Security Email
- Compatible applications: Gmail, Microsoft Exchange
- Feed Output Format:

```
%s{time}\t%d{recordid}\t%s{company}\t%s{tenant}\t%s{owner}\t%s{department}\
t%s{applicationname}\t%s{threatname}\t%s{malware}\t%s{malwareclass}\t%s{policy}\
t%s{messageid}\t%s{dlpdictnames}

\t%s{dlpdictcount}\t%s{dlpenginenames}\t%d{dlpidentifier}\t%s{severity}t%s{any_
incident}\t%s{rtime}\t%s{attchcomponentmd5s}\t%s{attchcomponentfilenames}\
t%s{attchcomponentfilesizes}

\t%s{attchcomponentfiletypes}\temail
```

- Log Sample:

```
{"MessageSourceAddress": "127.00.00.1", "EventReceivedTime": "2022-10-
18T09:27:27.999874+00:00", "SourceModuleName": "i_test_zscaler", "SourceModuleType":
"im_tcp", "time":

"2020-11-27T06:13:01.000000+00:00", "recordid": "1515155", "company": "Zscaler",
"tenant": "QA-Box", "owner": "jsmith", "department": "test", "applicationname":
"OneDrive", "threatname": "menace", "malware": "Spyware", "malwareclass": "WannaCry",
"policy": "Make sharing read only", "messageid": "196a3d797bfee07fe4596b69f4ce1141",
"dlpdictnames": "Gambling&#124", "dlpdictcount": "1&#124", "dlpenginenames":
"PCI&#124", "dlpidentifier": "6646497338839025669", "severityt": "Info Severity",
"any_incident": "No", "rtime": "Wed Nov 27 06:13:01 2019", "attchcomponentmd5s":
"196a3d797bfee07fe4596b69f4ce1141", "attchcomponentfilenames": "test.pdf",
"attchcomponentfilesizes": "attchcomponentfilesizes", "attchcomponentfiletypes":
"executable", "log_channel": "saas_email", "eGDirectory": "SEC_Zscaler_ZIA/127.0.0.1",
"GuessedPlatform": "zscaler", "LogType": "Zscaler Internet Access (ZIA) via NSS",
"EventTime": "2022-10-18T09:27:27.999874+00:00"}
```


Security File

- Application Category: SaaS Security File
- Compatible applications: Box, Citrix ShareFile, Dropbox, Google Drive, Microsoft OneDrive, Microsoft SharePoint
- Feed Output Format:

```
%s{time}\t%d{recordid}\t%s{company}\t%s{tenant}\t%s{user}\t%s{department}\
t%s{extownername}\t%s{applicationname}\t%s{filename}\t%s{filetypename}\t%d{filesize}\
t%s{filesource}

\t%s{filemd5}\t%s{threatname}\t%s{policy}\t%s{dlpdictnames}\t%s{dlpdictcount}\
t%s{dlpenginenames}\t%d{dlpidentifier}\t%s{fullurl}\t%s{lastmodtime}\t%d{filescantimems}

\t%d{filedownloadtimems}\t%s{malware}\t%s{malwareclass}\t%s{severity}\tfile
```

- Log Sample:

```
{"MessageSourceAddress":"127.0.0.1","EventReceivedTime":"2022-10-18T09:43:06.155488+
00:00","SourceModuleName":"i_test_zscaler","SourceModuleType":"im_tcp","time":"2020-
11-27T06:13:01.000000+00 Box","user":"john.smith@example.com","department":"test","ex
townername":"jane@yahoo.com","applicationname":"Microsoft","filename":"mon_fichier.pdf"
,"filetypename":"pdf","filesize":"164511","fi  All Files/10.65.1.220_2/compressed/test",
"filemd5":"196a3d157bfee07fe4596b69f4ce1141&#124","threatname":"phising_toto","policy"
:"None","dlpdictnames":"MRN Numbers","dlpdictcount":"1&#124","dlpenginenames":"Social
Security Numbers","dlpidentifier":"6646848838839025623","fullurl":"zscaler2.box.com/v/1
23456789010","lastmodtime":"Wed Nov 27

06:13:01

2019","filescantimems":"1555555","filedownloadtimems":"199999","malware":"Virus"
,"malwareclass":"Win32.Ransom.WannaCry","severity":"None","log_channel":"saas_
file","eGDirectory":"SEC_Zscaler_Z 127.0.0.1","GuessedPlatform":"zscaler","LogType":"Zs
caler Internet Access (ZIA) via NSS","EventTime":"2022-10-18T09:43:06.155488+00:00"}
```

Security Activity Logs

- Log Type: SaaS Security Activity (government agencies, see SaaS Security Activity).
- Feed Output Format:

```
%s{username}\t%s{tenant}\t%d{objtype1}\t%s{appname}\t%s{objnames1}\t%s{objnames2}\
t%d{act_cnt}\t%s{act_type_name}\t%s{eventtime}\t%s{extownername}\t%s{src_ip}\tactivity
```

- Log Sample:

```
{"MessageSourceAddress": "63.00.00.2", "EventReceivedTime": "2022-11-
15T10:35:37.304520+00:00", "SourceModuleName": "i_zscaler", "SourceModuleType": "im_
tcp", "eGImport": "import", "log_channel": "saas_activity", "username": "unknown_
saas_user$@11242169.zscalerbeta.net", "tenant": "salesforce test", "objtype1": "0",
"appname": "SALESFORCE", "objnames1": "None", "objnames2": "None", "act_cnt": "1",
"act_type_name": "Login Fail", "eventtime": "2022-11-15T00:59:42.000000+00:00",
"extownername": "0054x000004qcgx", "src_ip": "147.00.00.102", "eGDirectory": "SEC_
Zscaler_ZIA/63.34.200.2", "GuessedPlatform": "zscaler", "LogType": "Zscaler Internet
Access (ZIA) via NSS"}
```


Admin Audit Log

- Log Type: Admin Audit (government agencies, see Admin Audit).
- Feed Output Format:

```
%s{time}\t%d{recordid}\t%s{action}\t%s{category}\t%s{subcategory}\t%s{resource}\
t%s{interface}\t%s{adminid}\t%s{clientip}\t%s{result}\t%s{errorcode}\
t%s{auditlogtype}\t%s{preaction}

\t%s{postaction}\tadmin_audit\n
```

Alert

- Log Type: Alert
- Output Format: Syslog. The Syslog format for Alert log type cannot be edited.
- Log Sample:

```
<114>Oct 10 09:10:32 [5.00.00.141] ZscalerNSS: SIEM Feed connection "test tunnel" to
5.00.00.141:514 lost and unavailable for the past 71.93 minutes
```

NSS Firewall

NSS Firewall contains different log types:

- Firewall logs
- DNS logs

For each NSS Firewall log type, select **NSS for Firewall** within your NSS Server.

Firewall Logs

- Log Type: Firewall Log (government agencies, see Firewall Log).
- Firewall Log Type: Both Session and Aggregate Logs
- Feed Output Format:

```
%s{time}\t%s{login}\t%s{dept}\t%s{location}\t%d{cdport}\t%d{csport}\t%d{sdport}\
t%d{ssport}\t%s{csip}\t%s{cdip}\t%s{ssip}\t%s{sdip}\t%s{tsip}\t%d{tsport}\t%s{ttype}\
t%s{action}\t%s{dnat}

\t%s{stateful}\t%s{aggregate}\t%s{nwsvc}\t%s{nwapp}\t%s{ipproto}\t%s{ipcat}\
t%s{destcountry}\t%d{avgduration}\t%s{rulelabel}\t%ld{inbytes}\t%ld{outbytes}\
t%d{duration}\t%d{durationms}

\t%d{numsessions}\t%s{ipsrulelabel}\t%s{threatcat}\t%s{threatname}\t%s{deviceowner}\
t%s{devicehostname}\tfw
```

- Log Sample:

```
{"MessageSourceAddress": "99.00.00.37", "EventReceivedTime": "2022-11-
08T15:44:08.270209+00:00", "SourceModuleName": "i_zscaler", "SourceModuleType":
"im_tcp", "eGImport": "import", "log_channel": "fw", "EventTime": "2022-11-
08T15:43:59.000000+00:00", "user": "sd@dev-tehtris.com", "department": "test",
"locationname": "Road Warrior", "cdport": "443", "csport": "27505", "sdport":
"80", "ssport": "38463", "csip": "37.00.00.234", "cdip": "165.00.00.38", "ssip":
"165.00.00.151", "sdip": "35.00.00.17", "tsip": "0.00.00.0", "tunsport": "0",
"tuntype":

"ZscalerClientConnector", "action": "Allow", "dnat": "No", "stateful": "Yes",
```


"aggregate": "Yes", "nwsvc": "HTTP", "nwapp": "http", "proto": "TCP", "ipcat": "Internet Services", "destcountry": "United States", "avgduration": "281", "rulelabel": "Recommended Firewall Rule", "inbytes": "533", "outbytes": "1055", "duration": "0", "durationms": "281", "numsessions": "1", "ipsrulelabel": "None", "threatcat": "None", "threatname": "None", "deviceowner": "siem", "eGDirectory": "SEC_Zscaler_ZIA/99.80.19.37", "GuessedPlatform": "zscaler", "LogType": "Zscaler Internet Access (ZIA) via NSS"}

DNS Logs

- Log Type: DNS Log (government agencies, see DNS Log).
- Feed Output Format:

```
%s{time}\t%s{login}\t%s{dept}\t%s{cip}\t%d{durationms}\t%s{sip}\t%d{recordid}\
t%s{location}\t%s{req}\t%s{res}\t%s{domcat}\t%s{respipcat}\t%s{reqtype}\t%s{restype}\
t%d{sport}\t%s{error}

\t%s{reqrulelabel}\t%s{reqaction}\t%s{resrulelabel}\t%s{resaction}\t%s{datacenter}\
t%s{datacentercity}\t%s{datacentercountry}\t%s{deviceowner}\t%s{devicehostname}
```

Final Step

When you are ready to enable your NSS setup, go to the **Activation** tab and click **Activate**.

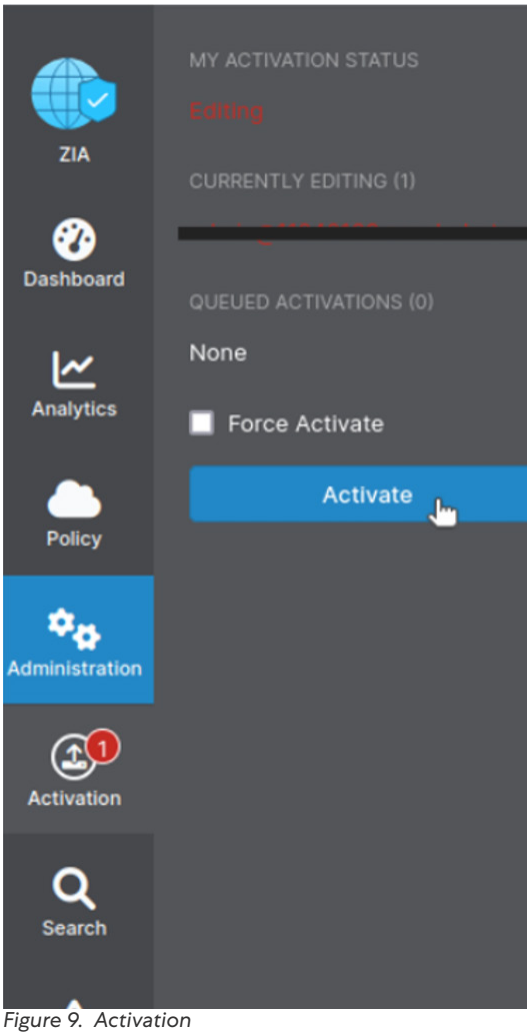

Figure 9. Activation

ZPA

This section presents how to set up ZPA Log Streaming Service (LSS) to send logs to the TEHTRIS SIEM appliance. An App Connector provides a secure authenticated interface between a customer's servers and ZPA cloud.

A Log Receiver specifies data from the logs that the App Connector sends to the SIEM. One Log Receiver Feed can only manipulate one type of log.

For more information about the setup, see the ZPA Help Portal (government agencies, see ZPA Help Portal).

Setup LSS Server

To create App Connectors:

1. Navigate to the **Administration** > **App Connector**.
2. Click **Add App Connectors**.

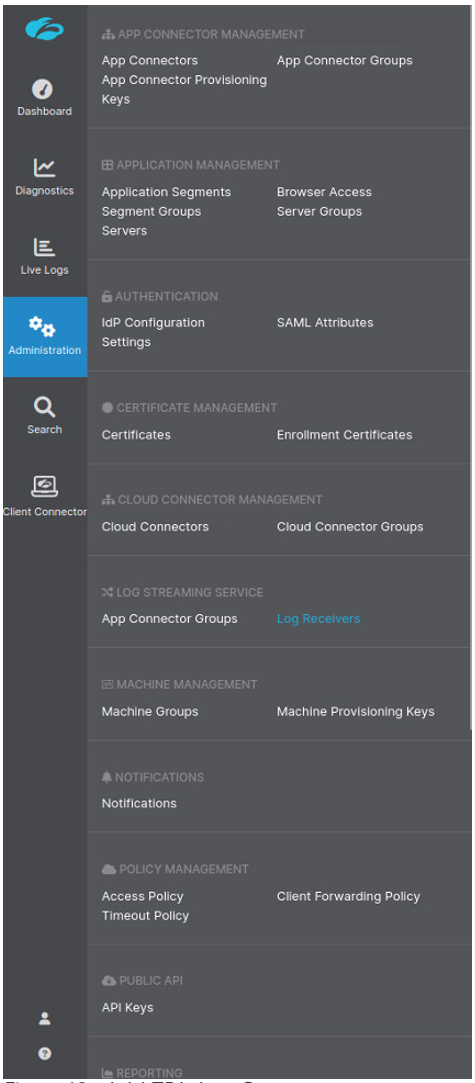

Figure 10. Add ZPA App Connector

Zscaler administrator rights are needed to make the whole deployment on an appliance.
The App Connector must be deployed in order to send logs to a SIEM. (government agencies, see send logs to a SIEM).

Create Log Receiver

To create a Log Receiver:

1. Navigate to **Administration** > **Log Receivers**.
2. Click **Add Log Receiver**.

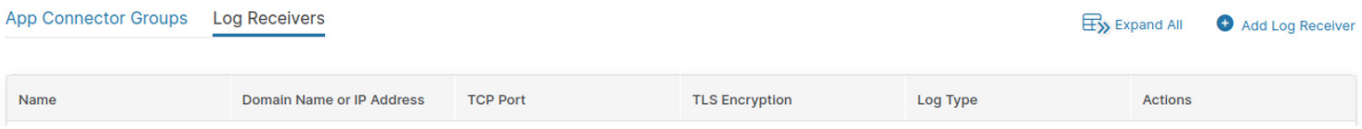

Figure 11. Add Log Receiver

3. Configure the following Log Receiver settings (in order to send logs to the TEHTRIS SIEM, you must configure this specific settings for every log type):

Name Field	Value
Status	Enabled
SIEM IP Address	TEHTRIS SIEM IP
Name	Name of the Log Receiver
Description	Description of the Log Receiver
Domain or IP Address	TEHTRIS SIEM IP
TCP Port	514
TLS Encryption	Disabled
APP Connector Groups	Our APP Connector

4. Replace T**EHTRIS SIEM IP** with the TEHTRIS SIEM appliance IP address provided by TEHTRIS Support.

The name must be different on every Log Receiver. Don't modify any parameters not mentioned in this documentation.

You can set up all of your Log Receivers on the same App Connector, or split your Log Receivers on several App Connectors.

5. Click **Next**.

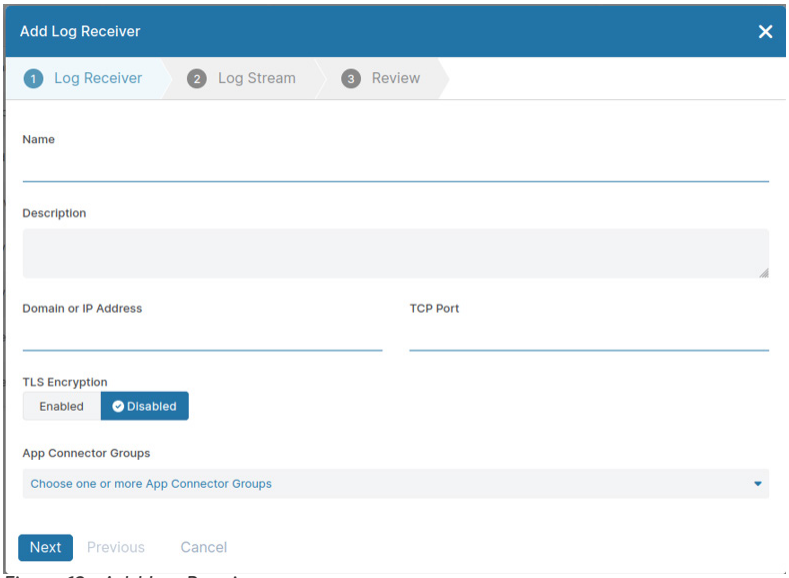

Figure 12. Add Log Receiver

Log Stream

For each log type, fill in the Log Template value with JSON format. The output log format designation for ZPA is called Log Stream Content.

User Activity

- Log Type: User Activity (government agencies, see User Activity).
- Log Stream Content:

```
 {"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"SessionID":
%j{SessionID},"ConnectionID": %j{ConnectionID},"InternalReason": %j{InternalReason},"C
onnectionStatus":

%j{ConnectionStatus},"IPProtocol": %d{IPProtocol},"DoubleEncryption": %d{DoubleEncrypt
ion},"Username": %j{Username},"ServicePort": %d{ServicePort},"ClientPublicIP":

%j{ClientPublicIP},"ClientPrivateIP": %j{ClientPrivateIP},"ClientLatitude": %f{ClientL
atitude},"ClientLongitude": %f{ClientLongitude},"ClientCountryCode":

%j{ClientCountryCode},"ClientZEN": %j{ClientZEN},"Policy": %j{Policy},"Connector":
%j{Connector},"ConnectorZEN": %j{ConnectorZEN},"ConnectorIP": %j{ConnectorIP},"Connect
orPort":

%d{ConnectorPort},"Host": %j{Host},"Application": %j{Application},"AppGroup":
%j{AppGroup},"Server": %j{Server},"ServerIP": %j{ServerIP},"ServerPort":

%d{ServerPort},"PolicyProcessingTime": %d{PolicyProcessingTime},"ServerSetupTime": %d{
ServerSetupTime},"TimestampConnectionStart":

%j{TimestampConnectionStart:iso8601},"TimestampConnectionEnd": %j{TimestampConnectionE
nd:iso8601},"TimestampCATx": %j{TimestampCATx:iso8601},"TimestampCARx":

%j{TimestampCARx:iso8601},"TimestampAppLearnStart": %j{TimestampAppLearnStart:iso8601}
,"TimestampZENFirstRxClient": %j{TimestampZENFirstRxClient:iso8601},"TimestampZENFirst
TxClient":

%j{TimestampZENFirstTxClient:iso8601},"TimestampZENLastRxClient": %j{TimestampZENLastR
xClient:iso8601},"TimestampZENLastTxClient":

%j{TimestampZENLastTxClient:iso8601},"TimestampConnectorZENSetupComplete":
%j{TimestampConnectorZENSetupComplete:iso8601},"TimestampZENFirstRxConnector":

%j{TimestampZENFirstRxConnector:iso8601},"TimestampZENFirstTxConnector":
%j{TimestampZENFirstTxConnector:iso8601},"TimestampZENLastRxConnector":

%j{TimestampZENLastRxConnector:iso8601},"TimestampZENLastTxConnector": %j{TimestampZEN
LastTxConnector:iso8601},"ZENTotalBytesRxClient": %d{ZENTotalBytesRxClient},"ZENBytesR
xClient":

%d{ZENBytesRxClient},"ZENTotalBytesTxClient": %d{ZENTotalBytesTxClient},"ZENBytesTxCli
ent": %d{ZENBytesTxClient},"ZENTotalBytesRxConnector":

%d{ZENTotalBytesRxConnector},"ZENBytesRxConnector": %d{ZENBytesRxConnector},"Z
ENTotalBytesTxConnector": %d{ZENTotalBytesTxConnector},"ZENBytesTxConnector":
%d{ZENBytesTxConnector},"Idp":
```



```
%j{Idp},"ClientToClient": %j{c2c}}
```

User Status

- Log Type: User Status (government agencies, see User Status).
- Log Stream Content:

```
{"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"Username":
%j{Username},"SessionID": %j{SessionID},"SessionStatus": %j{SessionStatus},"Version":
%j{Version},"ZEN":

%j{ZEN},"CertificateCN": %j{CertificateCN},"PrivateIP": %j{PrivateIP},"PublicIP":
%j{PublicIP},"Latitude": %f{Latitude},"Longitude": %f{Longitude},"CountryCode":

%j{CountryCode},"TimestampAuthentication": %j{TimestampAuthentication:iso8601},"Timest
ampUnAuthentication": %j{TimestampUnAuthentication:iso8601},"TotalBytesRx":

%d{TotalBytesRx},"TotalBytesTx": %d{TotalBytesTx},"Idp": %j{Idp},"Hostname":
%j{Hostname},"Platform": %j{Platform},"ClientType": %j{ClientType},"TrustedNetworks":
[%j(,)

{TrustedNetworks}],"TrustedNetworksNames": [%j(,){TrustedNetworksNames}],"SAMLAttribut
es": %j{SAMLAttributes},"PosturesHit": [%j(,){PosturesHit}],"PosturesMiss": [%j(,)

{PosturesMiss}],"ZENLatitude": %f{ZENLatitude},"ZENLongitude": %f{ZENLongitude},"ZENCo
untryCode": %j{ZENCountryCode},"FQDNRegistered": %j{fqdn_registered},"FQDNRegisteredEr
ror":

%j{fqdn_register_error}}
```

App Connector Status

- Log Type: App Connector Status (government agencies, see App Connector Status).
- Log Stream Content:

```
 {"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"SessionID":
%j{SessionID},"SessionType": %j{SessionType},"SessionStatus":
%j{SessionStatus},"Version":

%j{Version},"Platform": %j{Platform},"ZEN": %j{ZEN},"Connector":
%j{Connector},"ConnectorGroup": %j{ConnectorGroup},"PrivateIP":
%j{PrivateIP},"PublicIP": %j{PublicIP},"Latitude":

%f{Latitude},"Longitude": %f{Longitude},"CountryCode": %j{CountryCode},"TimestampAuthe
ntication": %j{TimestampAuthentication:iso8601},"TimestampUnAuthentication":

%j{TimestampUnAuthentication:iso8601},"CPUUtilization": %d{CPUUtilization},"MemUtiliza
tion": %d{MemUtilization},"ServiceCount": %d{ServiceCount},"InterfaceDefRoute":

%j{InterfaceDefRoute},"DefRouteGW": %j{DefRouteGW},"PrimaryDNSResolver": %j{PrimaryDNS
Resolver},"HostUpTime": %j{HostUpTime},"ConnectorUpTime": %j{ConnectorUpTime},"NumOfIn
terfaces":

%d{NumOfInterfaces},"BytesRxInterface": %d{BytesRxInterface},"PacketsRxInterface": %d{
PacketsRxInterface},"ErrorsRxInterface": %d{ErrorsRxInterface},"DiscardsRxInterface":

%d{DiscardsRxInterface},"BytesTxInterface": %d{BytesTxInterface},"PacketsTxInterface":
%d{PacketsTxInterface},"ErrorsTxInterface": %d{ErrorsTxInterface},"DiscardsTxInterfa
```



```
ce":

%d{DiscardsTxInterface},"TotalBytesRx": %d{TotalBytesRx},"TotalBytesTx":
%d{TotalBytesTx}}
```

- Log Sample:

```
{"LogTimestamp": "Thu Dec 8 15:54:35 2022", "Customer": "Tehtris", "SessionID":
"", "SessionType": "ZPN_ASSISTANT_BROKER_LOG", "SessionStatus": "ZPN_STATUS_
AUTHENTICATED", "Version": "", "Platform": "", "ZEN": "BETA-US-7987",
"Connector": "Test key-1670426847401", "ConnectorGroup": "0", "PrivateIP": "",
"PublicIP": "3.00.00.75", "Latitude": 0.0, "Longitude": 0.0, "CountryCode": "",
"TimestampAuthentication": "2022-12-08T15:54:35.054Z", "TimestampUnAuthentication":
"", "CPUUtilization": 0, "MemUtilization": 0, "ServiceCount": 0, "InterfaceDefRoute":
"", "DefRouteGW": "", "PrimaryDNSResolver": "", "HostUpTime": "0", "ConnectorUpTime":
"0", "NumOfInterfaces": 0, "BytesRxInterface": 0, "PacketsRxInterface": 0,
"ErrorsRxInterface": 0,

"DiscardsRxInterface": 0, "BytesTxInterface": 0, "PacketsTxInterface": 0,
"ErrorsTxInterface": 0, "DiscardsTxInterface": 0, "TotalBytesRx": 7032678,
"TotalBytesTx": 2069157, "logChannel": "AppConnecteurStatus"}
```

App Connector Metrics

- Log Type: App Connector Metrics (government agencies, see App Connector Metrics).
- Log Stream Content:

```
{"LogTimestamp":%j{LogTimestamp:time},"Connector":%j{Connector},"CPUUtiliza
tion":%j{CPUUtilization},"SystemMemoryUtilization":%j{SystemMemoryUtilizati-
on},"ProcessMemoryUtilization":

%j{ProcessMemoryUtilization},"AppCount":%j{AppCount},"ServiceCount":%j{ServiceCount},"
TargetCount":%j{TargetCount},"AliveTargetCount":%j{AliveTargetCount},"ActiveConnection
sToPublicSE":

%j{ActiveConnectionsToPublicSE},"DisconnectedConnectionsToPublicSE":
%j{DisconnectedConnectionsToPublicSE},"ActiveConnectionsToPrivateSE":

%j{ActiveConnectionsToPrivateSE},"DisconnectedConnectionsToPrivateSE":
%j{DisconnectedConnectionsToPrivateSE},"TransmittedBytesToPublicSE":

%j{TransmittedBytesToPublicSE},"ReceivedBytesFromPublicSE":%j{ReceivedBytes
FromPublicSE},"TransmittedBytesToPrivateSE":%j{TransmittedBytesToPrivateSE}-
,"ReceivedBytesFromPrivateSE":

%j{ReceivedBytesFromPrivateSE},"AppConnectionsCreated":%j{AppConnectionsCreated},"AppC
onnectionsCleared":%j{AppConnectionsCleared},"AppConnectionsActive":

%j{AppConnectionsActive},"UsedTCPPortsIPv4":%j{UsedTCPPortsIPv4},"UsedUDPPortsIPv4":%j
{UsedUDPPortsIPv4},"UsedTCPPortsIPv6":%j{UsedTCPPortsIPv6},"UsedUDPPortsIPv6":

%j{UsedUDPPortsIPv6},"AvailablePorts":%j{AvailablePorts},"SystemMaximumFileDescriptors
":%j{SystemMaximumFileDescriptors},"SystemUsedFileDescriptors":

%j{SystemUsedFileDescriptors},"ProcessMaximumFileDescriptors":%j{ProcessMax
imumFileDescriptors},"ProcessUsedFileDescriptors":%j{ProcessUsedFileDescrip-
tors},"AvailableDiskBytes":
```



```
%j{AvailableDiskBytes}}
```

- Log Sample:

```
{"LogTimestamp": "Thu Dec 8 15:54:59 2022", "Connector": "Test key-1670426847401",
"CPUUtilization": "1", "SystemMemoryUtilization": "6", "ProcessMemoryUtilization":
"1", "AppCount": "8",

"ServiceCount": "1", "TargetCount": "1", "AliveTargetCount": "1",
"ActiveConnectionsToPublicSE": "2", "DisconnectedConnectionsToPublicSE": "0",
"ActiveConnectionsToPrivateSE": "0",

"DisconnectedConnectionsToPrivateSE": "0", "TransmittedBytesToPublicSE": "0",
"ReceivedBytesFromPublicSE": "10185580", "TransmittedBytesToPrivateSE": "0",
"ReceivedBytesFromPrivateSE":

"0", "AppConnectionsCreated": "117", "AppConnectionsCleared": "97",
"AppConnectionsActive": "20", "UsedTCPPortsIPv4": "31", "UsedUDPPortsIPv4": "5",
"UsedTCPPortsIPv6": "2",

"UsedUDPPortsIPv6": "2", "AvailablePorts": "28232", "SystemMaximumFileDescriptors":
"370349", "SystemUsedFileDescriptors": "1120", "ProcessMaximumFileDescriptors":
"512000",

"ProcessUsedFileDescriptors": "201", "AvailableDiskBytes": "52048216064",
"logChannel": "AppConnecteurMetrics"}
```

Private Service Edge Status

- Log Type: Private Edge Service Status (government agencies, see Private Edge Service Status).
- Log Stream Content:

```
{"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"SessionID":
%j{SessionID},"SessionType": %j{SessionType},"SessionStatus":
%j{SessionStatus},"Version":

%j{Version},"PackageVersion": %j{PackageVersion},"Platform": %j{Platform},"ZEN":
%j{ZEN},"ServiceEdge": %j{ServiceEdge},"ServiceEdgeGroup": %j{ServiceEdgeGroup},"Priva
teIP":

%j{PrivateIP},"PublicIP": %j{PublicIP},"Latitude": %f{Latitude},"Longitude":
%f{Longitude},"CountryCode": %j{CountryCode},"TimestampAuthentication":

%j{TimestampAuthentication:iso8601},"TimestampUnAuthentication": %j{TimestampUnAuthent
ication:iso8601},"CPUUtilization": %d{CPUUtilization},"MemUtilization":

%d{MemUtilization},"InterfaceDefRoute": %j{InterfaceDefRoute},"DefRouteGW": %j{DefRout
eGW},"PrimaryDNSResolver": %j{PrimaryDNSResolver},"HostUpTime": %j{HostUpTime},"Servic
eEdgeStartTime":

%j{ServiceEdgeStartTime},"NumOfInterfaces": %d{NumOfInterfaces},"BytesRxInterface":
%d{BytesRxInterface},"PacketsRxInterface": %d{PacketsRxInterface},"ErrorsRxInterface":

%d{ErrorsRxInterface},"DiscardsRxInterface": %d{DiscardsRxInterface},"BytesTxInterfa
ce": %d{BytesTxInterface},"PacketsTxInterface": %d{PacketsTxInterface},"ErrorsTxInterf
ace":

%d{ErrorsTxInterface},"DiscardsTxInterface": %d{DiscardsTxInterface},"TotalBytesRx":
```



```
%d{TotalBytesRx},"TotalBytesTx": %d{TotalBytesTx}}
```

Private Service Edge Metrics

- Log Type: Private Service Edge Metrics (government agencies, see Private Service Edge Metrics).
- Log Stream Content:

```
{"LogTimestamp":%j{LogTimestamp:time},"PrivateSE":%j{PrivateSE},"CPUUtiliza
tion":%j{CPUUtilization},"SystemMemoryUtilization":%j{SystemMemoryUtilizati-
on},"ProcessMemoryUtilization":

%j{ProcessMemoryUtilization},"UsedTCPPortsIPv4":%j{UsedTCPPortsIPv4},"UsedUDPPortsIPv4
":%j{UsedUDPPortsIPv4},"UsedTCPPortsIPv6":%j{UsedTCPPortsIPv6},"UsedUDPPortsIPv6":

%j{UsedUDPPortsIPv6},"AvailablePorts":%j{AvailablePorts},"SystemMaximumFileDescriptors
":%j{SystemMaximumFileDescriptors},"SystemUsedFileDescriptors":%j{SystemUsedFileDescri
ptors},"ProcessMaximumFileDescriptors":%j{ProcessMaximumFileDescriptors},"ProcessUsedF
ileDescriptors":%j{ProcessUsedFileDescriptors},"AvailableDiskBytes":

%j{AvailableDiskBytes}}
```

Browser Access

- Log Type: Browser Access (government agencies, see Browser Access).
-
- Log Stream Content:

```
{"LogTimestamp":%j{LogTimestamp:time},"ConnectionID":%j{ConnectionID},"Exporter":%j{Ex
porter},"TimestampRequestReceiveStart":

%j{TimestampRequestReceiveStart:iso8601},"TimestampRequestReceiveHeaderFinish":%j
{TimestampRequestReceiveHeaderFinish:iso8601},"TimestampRequestReceiveFinish":

%j{TimestampRequestReceiveFinish:iso8601},"TimestampRequestTransmitStart":%j
{TimestampRequestTransmitStart:iso8601},"TimestampRequestTransmitFinish":

%j{TimestampRequestTransmitFinish:iso8601},"TimestampResponseReceiveStart":%j
{TimestampResponseReceiveStart:iso8601},"TimestampResponseReceiveFinish":

%j{TimestampResponseReceiveFinish:iso8601},"TimestampResponseTransmitStart":%j
{TimestampResponseTransmitStart:iso8601},"TimestampResponseTransmitFinish":

%j{TimestampResponseTransmitFinish:iso8601},"TotalTimeRequestReceive":%d{To
talTimeRequestReceive},"TotalTimeRequestTransmit":%d{TotalTimeRequestTransm-
it},"TotalTimeResponseReceive":

%d{TotalTimeResponseReceive},"TotalTimeResponseTransmit":%d{TotalTimeResponseTransmit}
,"TotalTimeConnectionSetup":%d{TotalTimeConnectionSetup},"TotalTimeServerResponse":

%d{TotalTimeServerResponse},"Method":%j{Method},"Protocol":%j{Protocol},"Ho
st":%j{Host},"URL":%j{URL},"UserAgent":%j{UserAgent},"XFF":%j{XFF},"NameID"-
:%j{NameID},"StatusCode":

%d{StatusCode},"RequestSize":%d{RequestSize},"ResponseSize":%d{ResponseSize},"Applicat
ionPort":%d{ApplicationPort},"ClientPublicIp":%j{ClientPublicIp},"ClientPublicPort":
```



```
%d{ClientPublicPort},"ClientPrivateIp":%j{ClientPrivateIp},"Customer":%j{Customer},"Co
nnectionStatus":%j{ConnectionStatus},"ConnectionReason":%j{ConnectionReason},"Origin":

%j{Origin},"CorsToken":%j{CorsToken}}
```

Audit Logs

- Log Type: Audit Logs (government agencies, see Audit Logs).
- Log Stream Content:

```
{"ModifiedTime":%j{modifiedTime:iso8601},"CreationTime":%j{creationTime:iso
8601},"ModifiedBy":%d{modifiedBy},"RequestID":%j{requestId},"SessionID":%j{-
sessionId},"AuditOldValue":

%j{auditOldValue},"AuditNewValue":%j{auditNewValue},"AuditOperationType":%j{auditOpera
tionType},"ObjectType":%j{objectType},"ObjectName":%j{objectName},"ObjectID":

%d{objectId},"CustomerID":%d{customerId},"User":%j{modifiedByUser},"ClientAuditUpdate":
%d{isClientAudit}}
```

- Log Sample:

```
{"ModifiedTime": "2022-12-08T10:18:13.000Z", "CreationTime":
"2022-12-08T10:18:13.000Z", "ModifiedBy": 72058679590912001, "RequestID":
"e11acce1-0b7d-41d2-be6a-b3eff06099bf", "SessionID": "j4k11w5000nr0epv2gnuh45ie",
"AuditOldValue": "{\"id\":\"1141\", \"name\":\"petimey991@cosaxu.com\"}",
"AuditNewValue": "", "AuditOperationType": "Delete", "ObjectType": "Executive Insights
User", "ObjectName": "petimey991@cosaxu.com", "ObjectID": 1141, "CustomerID":
72050000590912000, "User": "zpaadmin@72000679500000000.zpa-customer.com",
"ClientAuditUpdate": 0, "logChannel": "audit"}
```

Final Step

When you are ready to enable your LSS setup, click **Save**. Your logs are then forwarded to the TEHTRIS SIEM appliance from your App Connector.

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**.

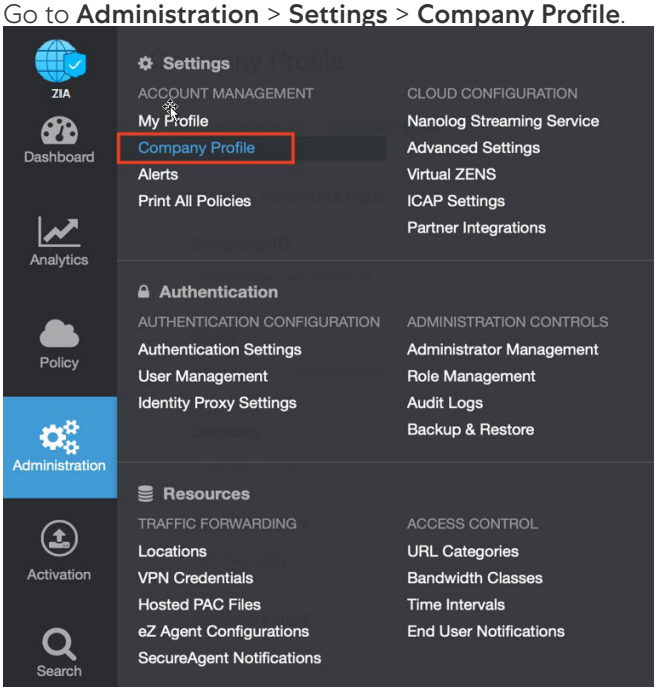

Figure 13. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

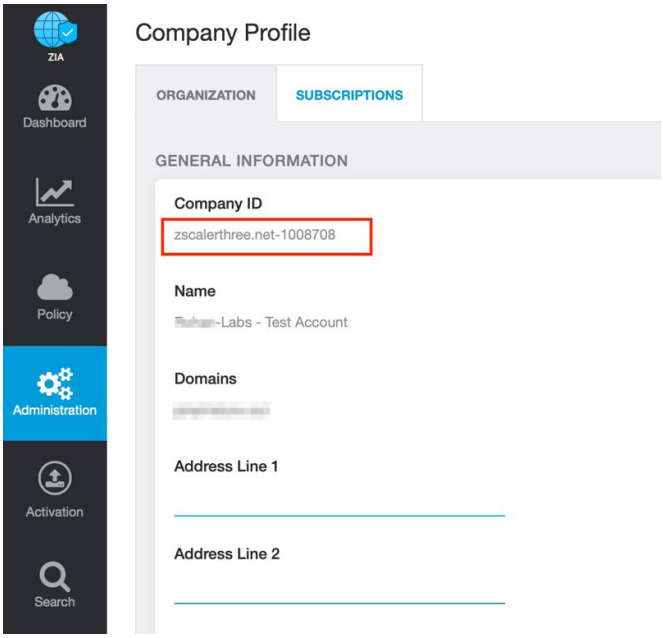

Figure 14. Company ID

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

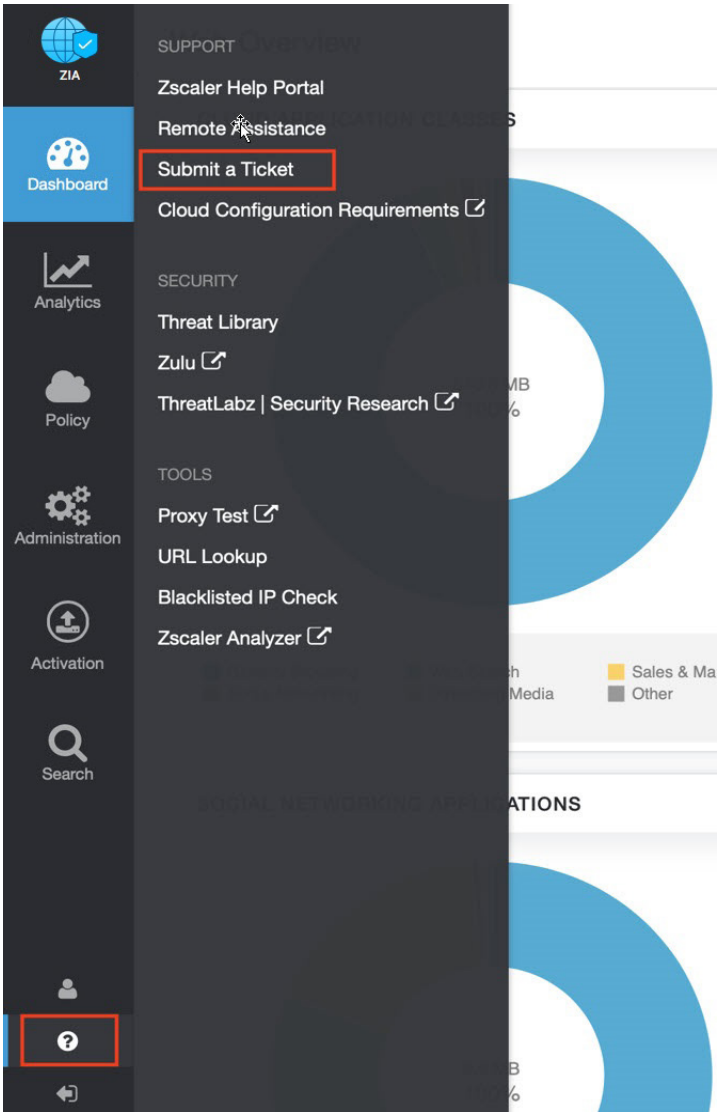

Figure 15. Submit a Ticket

