



elastic

ZSCALER AND ELASTIC DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	5
Zscaler Overview	5
Elastic Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and Elastic Introduction	6
ZIA Overview	6
ZPA Overview	6
Zscaler Resources	6
Elastic Security Overview	7
Elastic Resources	7
Using Elastic Security with ZIA	8
NSS Syslog Setup Steps	8
Install an Elastic Agent	8
Setup ZIA NSS Server	8
Configuring the ZIA NSS Feed	9
Cloud NSS Integration Setup Steps	10

ZIA Feed Formats	11
Web Log Formats	11
Firewall Log Format	11
DNS Log Format	12
Alert Log Format	12
Tunnel Log Format	12
IKE Phase 1 Format	12
IKE Phase 2 Format	13
Enable the Integration in Kibana	13
View the ZIA Dashboards in Kibana	15
Using Elastic with ZPA	17
Setup Steps	17
ZPA Log Receiver Setup	17
ZPA Log Formats	18
User Activity Log Format	18
User Status Log Format	19
App Connector Status Log Format	19
Audit Log Format	19
Browser Access Log Format	20
Enabling ZPA Integration in Kibana	21
Viewing ZPA Dashboards in Kibana	23
Zscaler ZPA Datastreams	24
Appendix A: Requesting Zscaler Support	25

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
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
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 and information event management
SSL	Secure Socket Layer (RFC6101)
XFF	X-Forwarded-For (RFC7239)
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](#).

Elastic Overview

Elastic (Trading Index: [ESTC](#)) is a search company built on a free and open heritage. Anyone can use Elastic products and solutions to get started quickly and frictionlessly. Elastic offers three solutions for [enterprise search](#), [observability](#), and [security](#), built on one technology stack that can be deployed anywhere. From finding documents to monitoring infrastructure to hunting for threats, Elastic makes data usable in real time and at scale. Founded in 2012, Elastic is a distributed company with Elasticians around the globe. To learn more, refer to [Elastic's website](#).

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- [Zscaler Resources](#)
- [Elastic Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

This document was authored using the latest versions of ZIA and ZPA.

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 Elastic Introduction

Overviews of the Zscaler and Elevate Security applications are described in this section.



If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a 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, SaaS Security, 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, 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.

Elastic Security Overview

Elastic Security combines SIEM threat detection features with endpoint prevention and response capabilities in one solution. These analytical and protection capabilities, leveraged by the speed and extensibility of Elasticsearch, enable analysts to defend their organization from threats before damage and loss occur.

Elastic Security provides the following security benefits and capabilities:

- A detection engine to identify attacks and system misconfigurations.
- A workspace for event triage and investigations.
- Interactive visualizations to investigate process relationships.
- Inbuilt case management with automated actions.
- Detection of signatureless attacks with prebuilt machine learning anomaly jobs and detection rules.

Elastic Resources

The following table contains links to Elastic support resources.

Name	Definition
Elastic Security overview	Description of the Elastic Security solution.
Elastic Security help	Online help for Elastic Security.
Elastic ZIA module help	Online help for integrating ZIA and Elastic Security.
Elastic ZPA module help	Online help for integrating ZPA and Elastic Security.

Using Elastic Security with ZIA

This section provides examples for configuring ZIA and Elastic Security. It explains setting up your production network or for proof of concept (PoC) topologies and demos when evaluating interoperability and integration.

ZIA can send logs to Elastic via NSS or Cloud NSS. NSS sends data using syslog over TCP and requires the deployment of NSS virtual machines (VMs), one for web logs and another for firewall. For more information about NSS, see [Understanding Nanolog Streaming Service](#) (government agencies, see [Understanding Nanolog Streaming Service](#)).

Cloud NSS is an optional service provided by Zscaler. Logs are sent over HTTPS to an endpoint. With Cloud NSS, there are no VMs to deploy and manage. Zscaler manages, monitors, and scales the logging pipeline as needed. To leverage Cloud NSS, the HTTP endpoint input collector must be enabled on the Elastic side.

NSS Syslog Setup Steps

1. Install an [Elastic Agent](#).
2. Set up ZIA NSS Server.
3. Configure the ZIA NSS feed.
4. Enable the integration in Kibana.
5. View dashboards in Kibana.

Install an Elastic Agent

Elastic Agent is a single, unified agent (deployed to hosts or containers) that collects data and sends it to Elastic. Follow the steps outlined [here](#) to install an agent.

Setup ZIA NSS Server

1. Log in to the ZIA Admin Portal using your admin account. If you're unable to log in, contact [Zscaler Support](#) (government agencies, contact [Zscaler Support](#)).
2. Add an NSS server. See [Adding NSS Servers](#) (government agencies, see [Adding NSS Servers](#)) in the Zscaler Help Portal to set up an NSS server for web or firewall.
3. Verify NSS state. Verify that the state of the NSS server is healthy.
 - a. In the ZIA Admin Portal, go to **Administration > Nanolog Streaming Service > NSS Servers**.
 - b. In the **State** column, confirm that the state of the NSS server is **Healthy**.

No.	Server Name	Type	Status	State
1	NSS-FW-3	NSS for Firewall	Enabled	Unhealthy
2	NSS-WEB-3	NSS for Web	Enabled	Unhealthy
3	NSS_FW_2	NSS for Firewall	Enabled	Unhealthy
4	NSS_WEB_2	NSS for Web	Enabled	Healthy

Figure 1. NSS server health

Configuring the ZIA NSS Feed

- See [Adding NSS Feeds](#) (government agencies, see [Adding NSS Feeds](#)) and select the type of feed you want to configure. The following fields require specific inputs:
 - **SIEM IP Address:** Enter the IP address of the Elastic agent to which the Zscaler integration is assigned.
 - **SIEM TCP Port:** Enter the port number, depending on the logs associated with the NSS feed. You must create an NSS feed for each log type.
 - **Alerts:** 9006
 - **DNS:** 9007
 - **Firewall:** 9008
 - **Tunnel:** 9009
 - **Web:** 9010
 - **Feed Output Type:** Select **Custom** and paste the appropriate response format (see [ZIA Feed Formats](#)):

Add NSS Feed

NSS FEED

Feed Name
Elastic

NSS Server
NSS_WEB_2

SIEM Destination Type
☒ IP Address ☐ FQDN

SIEM TCP Port
9010

SIEM Rate
☒ Unlimited ☐ Limited

Log Type
☒ Web Log ☐ SaaS Security Activity ☐ Tunnel ☐ Alert ☐ SaaS Security

Feed Output Type
Custom

Feed Escape Character
Enter Text

Feed Output Format

```
[{"sourcetype": "zscaler-nss-web", "event": {"time": "%s(time)", "login": "%s(login)", "proto": "%s(proto)", "eurl": "%s(eurl)", "action": "%s(action)", "appname": "%s(appname)", "appclass": "%s(appclass)", "reqsize": "%d(reqsize)", "respsize": "%d(respsize)", "stime": "%d(stime)", "ctime": "%d(ctime)", "urlclass": "%s(urlclass)", "urlsupercat": "%s(urlsupercat)", "urlcat": "%s(urlcat)", "malwarecat": "%s(malwarecat)", "threatname": "%s(threatname)", "riskscore": "%d(riskscore)", "dlpeng": "%s(dlpeng)", "dlpdic": "%s(dlpdic)", "location": "%s(location)", "dept": "%s(dept)", "cip": "%s(cip)", "sip": "%s(sip)", "reqmethod": "%s(reqmethod)", "respcode": "%s(respcode)", "ua": "%s(ua)", "referer": "%s(referer)", "ruletype": "%s(ruletype)", "rulelabel": "%s(rulelabel)", "contenttype": "%s(contenttype)", "unscannabletype": "%s(unscannabletype)", "deviceowner": "%s(deviceowner)", "devicehostname": "%s(devicehostname)"}]}
```

Timezone
GMT

Duplicate Logs
Disabled

Action **Who** **From Where** **Transaction** **To Where** **Security** **File Type** **DLP**

WEB LOG FILTERS

Policy Action
ANY

Policy Reason
Any

Save **Cancel**

Figure 2. Add NSS Feed dialog

Cloud NSS Integration Setup Steps

1. On the Elastic side, ensure that the HTTP Endpoint Agent is enabled.
2. Configure the Zscaler Cloud NSS Feed to send logs to the Elastic Agent that is running this integration. Provide the API URL to send logs to the Elastic Agent. Perform the following steps to configure Zscaler Cloud NSS Feeds:
 - In the ZIA Admin Portal, add a Cloud NSS Feed.
 - Log in to the ZIA Admin Portal using your admin account.
 - Add a Cloud NSS Feed. See [Add Cloud NSS Feed](#) (government agencies, see [Add Cloud NSS Feed](#))
 - In the ZIA Admin Portal, go to **Administration > Nanolog Streaming Service > Cloud NSS Feeds**.
 - Assign a **Feed Name**, ensure the status is changed to **Enabled**.
 - Select **NSS Type**.
 - Change **SIEM Type** to **Other**.
 - Add an **API URL**.
 - Default ports:
 - DNS: 9556
 - Firewall: 9557
 - Tunnel: 9558
 - Web: 9559
 - Select **JSON** as the **Feed Output Type**.
 - Remember to add the identical **HTTP Header** along with its value to both ZIA and Elastic Security for additional security.

The screenshot displays the 'SIEM CONNECTIVITY' configuration page. It includes a dropdown for 'SIEM Type' currently set to 'Other', a 'Max Batch Size' of '16 KB', an 'API URL' field with a placeholder 'Add your API URL here', and an 'HTTP HEADERS' section. Under 'HTTP HEADERS', there is a table with 'Key 1' as 'Content-Type' and 'Value 1' as 'application/ndjson'. A '+ Add HTTP Header' button is located at the bottom left of the headers section.

Figure 3. SIEM Connectivity

ZIA Feed Formats

The following are the log formats you can copy and paste into the **Feed Output Format** section of the **Add NSS Feed** dialog (depending on the type of feed created).



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

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

Web Log Formats

Web Log Format

Add in \" as the Feed Escape characters.

Feed Escape Character:

\"

Ports

• Default port (NSS Feed): 9014

• Default port (Cloud NSS Feed): 9559

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"time":"%s{time}", "login":"%s{login}", "proto":"%s{proto}", "eurl":"%s{eurl}", "action":"%s{action}", "appname":"%s{appname}", "appclass":"%s{appclass}", "reqsize":"%d{reqsize}", "respsize":"%d{respsize}", "stime":"%d{stime}", "ctime":"%d{ctime}", "urlclass":"%s{urlclass}", "urlsupercat":"%s{urlsupercat}", "urlcat":"%s{urlcat}", "malwarecat":"%s{malwarecat}", "threatname":"%s{threatname}", "riskscore":"%d{riskscore}", "dlpeng":"%s{dlpeng}", "dlpdicthit":"%s{dlpdicthit}", "location":"%s{location}", "dept":"%s{dept}", "cip":"%s{cip}", "sip":"%s{sip}", "reqmethod":"%s{reqmethod}", "respcode":"%s{respcode}", "ua":"%s{ua}", "ereferer":"%s{ereferer}", "ruletype":"%s{ruletype}", "rulelabel":"%s{rulelabel}", "contenttype":"%s{contenttype}", "unscannabletype":"%s{unscannabletype}", "deviceowner":"%s{deviceowner}", "devicehostname":"%s{devicehostname}"\}\}
```

Firewall Log Format

Firewall Log Format

Ports

• Default port (NSS Feed): 9012

• Default port (Cloud NSS Feed): 9557

```
\{ "sourcetype" : "zscalernss-fw", "event" : \{"datetime":"%s{time}", "user":"%s{ellogin}", "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}", "tunstype":"%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":"%s{devicehostname}"\}\}
```

DNS Log Format

DNS Log Format

Ports

- Default port (NSS Feed): 9011
- Default port (Cloud NSS Feed): 9556

```
\{ "sourcetype" : "zscalernss-dns", "event" : \{"datetime":"%s{time}", "user":"%s{e
login}", "department":"%s{edepartment}", "location":"%s{elocation}", "reqaction":"%s
{reqaction}", "resaction":"%s{resaction}", "regrulelabel":"%s{regrulelabel}", "resru
lelabel":"%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}", "deviceowner":"%s{deviceown
er}", "devicehostname":"%s{devicehostname}"\}\}
```

Alert Log Format

Alert Format

Ports

- Default port (NSS Feed): 9010
- Not available in Cloud NSS

```
<%d{syslogid}>%s{Monthname} %2d{Dayofmonth} %02d{Hour}:%02d{Minutes}:%02d{Seconds}
[%s{Deviceip}] ZscalerNSS: %s{Eventinfo}\n
```

Tunnel Log Format

Tunnel Event Format

Ports

- Default port (NSS Feed): 9012
- Default port (Cloud NSS Feed): 9557

```
\{ "sourcetype" : "zscalernss-tunnel", "event" : \{"datetime":"%s{datetime}", "Recordty
pe":"%s{tunnelactionname}", "tunneltype":"%s{tunneltype}", "user":"%s{vpncredentialname}
", "location":"%s{elocationname}", "sourceip":"%s{sourceip}", "destinationip":"%s{destvip
}", "sourceport":"%d{srcport}", "event":"%s{event}", "eventreason":"%s{eventreason}", "re
cordid":"%d{recordid}"\}\}
```

IKE Phase 1 Format

IKE Phase 1 Format

```
\{ "sourcetype" : "zscalernss-tunnel", "event" : \{"datetime":"%s{datetime}", "Recordty
pe":"%s{tunnelactionname}", "tunneltype":"IPSEC IKEV %d{ikeversion}", "user":"%s{vpncred
entialname}", "location":"%s{elocationname}", "sourceip":"%s{sourceip}", "destinationip":
"%s{destvip}", "sourceport":"%d{srcport}", "destinationport":"%d{dstport}", "lifetime":
"%d{lifetime}", "ikeversion":"%d{ikeversion}", "spi_in":"%lu{spi_in}", "spi_out":"%lu{spi_
out}", "algo":"%s{algo}", "authentication":"%s{authentication}", "authtype":"%s{authtype}
", "recordid":"%d{recordid}"\}\}
```

IKE Phase 2 Format

IKE Phase 2 Format

```
\{ "sourcetype" : "zscalernss-tunnel", "event" : \{"datetime":"%s{datetime}","Recordtype":"%s{tunnelactionname}","tunneltype":"IPSEC IKEV %d{ikeversion}","user":"%s{vpncredentialsname}","location":"%s{elocationname}","sourceip":"%s{sourceip}","destinationip":"%s{destvip}","sourceport":"%d{srcport}","sourceportstart":"%d{srcportstart}","destinationportstart":"%d{destportstart}","srcipstart":"%s{srcipstart}","srcipend":"%s{srcipend}","destinationipstart":"%s{destipstart}","destinationipend":"%s{destipend}","lifetime":"%d{lifetime}","ikeversion":"%d{ikeversion}","lifebytes":"%d{lifebytes}","spi":"%d{spi}","algo":"%s{algo}","authentication":"%s{authentication}","authtype":"%s{authtype}","protocol":"%s{protocol}","tunnelprotocol":"%s{tunnelprotocol}","policydirection":"%s{policydirection}","recordid":"%d{recordid}"\}\}
```

Enable the Integration in Kibana

The following steps describe how to enable the integration in Kibana:

1. Log into Kibana.
2. From the **Management** drop-down menu, select **Integrations**.

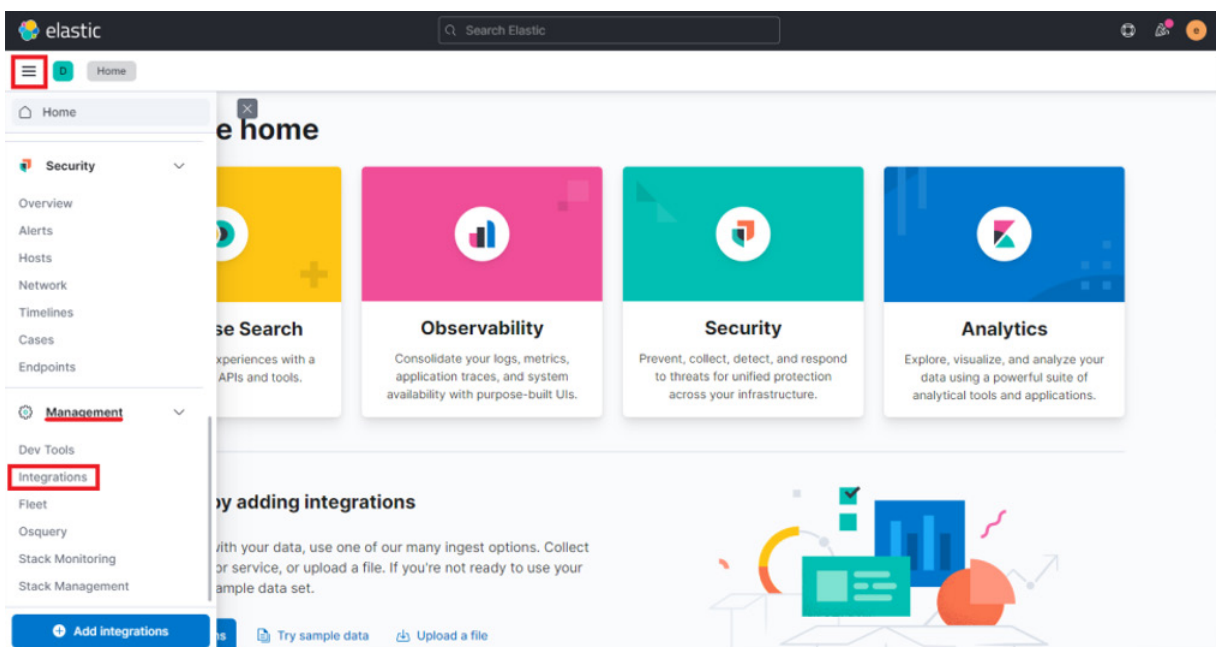


Figure 4. Elastic Integrations tab in Kibana

3. Search for `zscaler zia`, then select the **Zscaler Internet Access** tile.

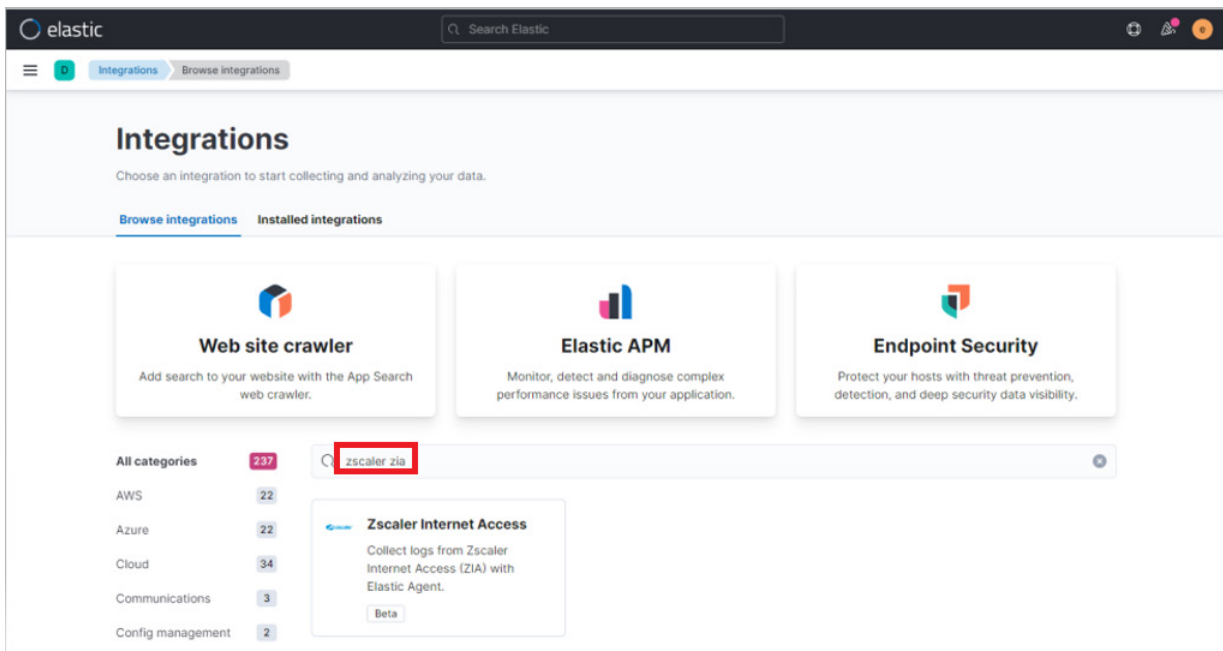


Figure 5. Elastic Integrations tab

4. Enable the appropriate NSS feeds (e.g., **Alerts**, **DNS**, **Firewall**, etc.).

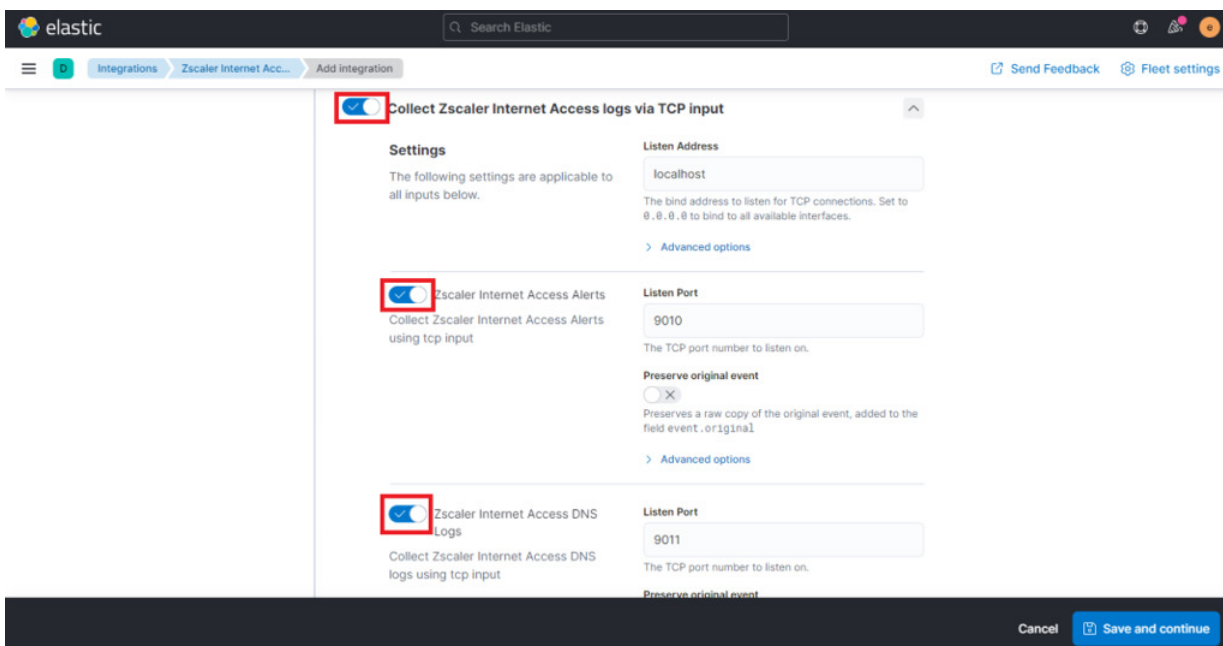


Figure 6. Elastic Add Integration dialog

5. Apply the integration to an **Agent policy**, and ensure the agent you used when adding the NSS feed in the ZIA portal is assigned to that policy.

elastic Search Elastic

Integrations Zscaler Internet Acc... Add Integration

Send Feedback Fleet settings

☒ Zscaler Internet Access Web Logs
Collect Zscaler Internet Access Web Logs using tcp input

2 Apply to agent policy

Agent policy
Agent policies are used to manage a group of integrations across a set of agents

Agent policy Create agent policy
Default policy
1 agent is enrolled with the selected agent policy.

Cancel Save and continue

Figure 7. Elastic agent policy

6. Click **Save and continue**.

View the ZIA Dashboards in Kibana

The following steps describe how to view ZIA dashboards in Kibana:

1. Log into Kibana.
2. From the **Analytics** tab, select **Dashboard**.
3. Search for Zscaler ZIA.

elastic Search Elastic

Dashboard

Dashboards Create dashboard

Search Zscaler ZIA Tags

Title	Description	Tags	Actions
<input type="checkbox"/> [Zscaler] [ZIA] Firewall Logs			
<input type="checkbox"/> [Zscaler] [ZIA] Web Logs			
<input type="checkbox"/> [Zscaler] [ZIA] Tunnel Logs			
<input type="checkbox"/> [Zscaler] [ZIA] DNS Logs			

Rows per page: 20 < 1 >

Figure 8. Elastic Dashboards dialog

4. Click the appropriate dashboard to start interacting with your Zscaler events in Elastic.

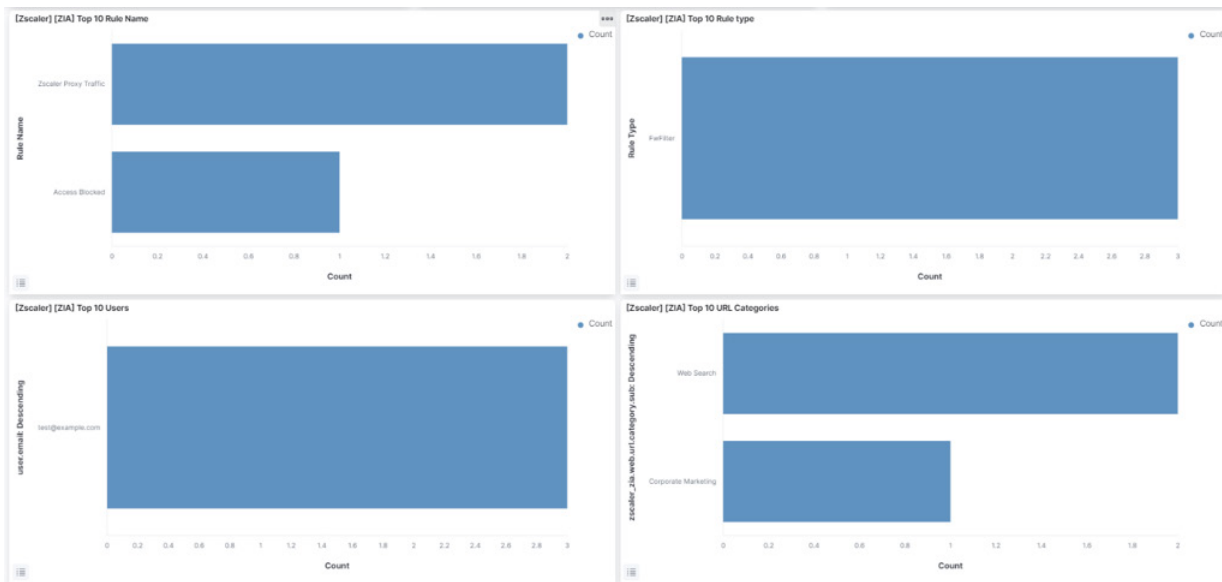


Figure 9. Elastic dashboards

5. From the **Management** drop-down menu, select **Fleet**.

The screenshot shows the Elastic Fleet management interface. The 'Data streams' tab is selected. A search bar contains 'Zscaler ZIA'. Below the search bar, a table lists the datasets:

Dataset	Type	Namespace	Integration	Last activity	Size	Actions
zscaler_zia.firewall	logs	default	zscaler_zia	Feb 14, 2022 @ 12:22:47	226B	...
zscaler_zia.alerts	logs	default	zscaler_zia	Feb 14, 2022 @ 12:21:49	22.9KB	...
zscaler_zia.dns	logs	default	zscaler_zia	Feb 14, 2022 @ 12:21:27	33.6KB	...
zscaler_zia.tunnel	logs	default	zscaler_zia	Feb 14, 2022 @ 12:20:07	11.8KB	...
zscaler_zia.web	logs	default	zscaler_zia	Feb 14, 2022 @ 11:08:04	54.2KB	...

At the bottom, it indicates 'Rows per page: 20' and a pagination control showing page 1.

Figure 10. Elastic dashboard details example

Using Elastic with ZPA

This section describes the Elastic setup required to receive logs from ZPA. The data is mapped to Elastic Common Schema (ECS) fields where applicable, and the remaining fields are written under `zscaler_zpa.<data-stream-name>.*`.

Setup Steps

1. Enable the integration with the TCP input.
2. Configure the Zscaler LSS Log Receiver to send logs to the Elastic agent that is running this integration. See [Configuring a Log Receiver](#) (government agencies, see [Configuring a Log Receiver](#)). Use the IP address/hostname of the Elastic agent as the **Log Receiver Domain** or **IP Address**, and use the listening port of the Elastic agent as the **TCP Port** on the **Add Log Receiver** configuration screen (see [ZPA Log Formats](#)).
3. Use supplied formats for the logs.
4. Enable the ZPA integration in Kibana.

ZPA Log Receiver Setup

For detailed information on setting up the ZPA log receiver, see [About the Log Streaming Service](#) and [Configuring a Log Receiver](#) (government agencies, see [About the Log Streaming Service](#) and [Configuring a Log Receiver](#)) sections in the Zscaler Help Portal.

- **Name & Description:** <customer-specified>
- **Domain or IP:** Use the IP address/hostname of the Elastic Agent
- **TCP port:** Use the listening port of the Elastic Agent

The log message is expected to be in JSON and in the specified formats.

ZPA Log Formats

The following are the log formats created that you can copy and paste into the **Log Stream Content** section of the **Add Log Receiver** dialog (depending on the type of feed created).



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

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

User Activity Log Format

User Activity Log Format, Default Port: 9018

```
{
  "LogTimestamp": %j{LogTimestamp:time},
  "Customer": %j{Customer},
  "SessionID": %j{SessionID},
  "ConnectionID": %j{ConnectionID},
  "InternalReason": %j{InternalReason},
  "ConnectionStatus": %j{ConnectionStatus},
  "IPProtocol": %d{IPProtocol},
  "DoubleEncryption": %d{DoubleEncryption},
  "Username": %j{Username},
  "ServicePort": %d{ServicePort},
  "ClientPublicIP": %j{ClientPublicIP},
  "ClientPrivateIP": %j{ClientPrivateIP},
  "ClientLatitude": %f{ClientLatitude},
  "ClientLongitude": %f{ClientLongitude},
  "ClientCountryCode": %j{ClientCountryCode},
  "ClientZEN": %j{ClientZEN},
  "Policy": %j{Policy},
  "Connector": %j{Connector},
  "ConnectorZEN": %j{ConnectorZEN},
  "ConnectorIP": %j{ConnectorIP},
  "ConnectorPort": %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{TimestampConnectionEnd:iso8601},
  "TimestampCATx": %j{TimestampCATx:iso8601},
  "TimestampCARx": %j{TimestampCARx:iso8601},
  "TimestampAppLearnStart": %j{TimestampAppLearnStart:iso8601},
  "TimestampZENFirstRxClient": %j{TimestampZENFirstRxClient:iso8601},
  "TimestampZENFirstTxClient": %j{TimestampZENFirstTxClient:iso8601},
  "TimestampZENLastRxClient": %j{TimestampZENLastRxClient:iso8601},
  "TimestampZENLastTxClient": %j{TimestampZENLastTxClient:iso8601},
  "TimestampConnectorZENSetupComplete": %j{TimestampConnectorZENSetupComplete:iso8601},
  "TimestampZENFirstRxConnector": %j{TimestampZENFirstRxConnector:iso8601},
  "TimestampZENFirstTxConnector": %j{TimestampZENFirstTxConnector:iso8601},
  "TimestampZENLastRxConnector": %j{TimestampZENLastRxConnector:iso8601},
  "TimestampZENLastTxConnector": %j{TimestampZENLastTxConnector:iso8601},
  "ZENTotalBytesRxClient": %d{ZENTotalBytesRxClient},
  "ZENBytesRxClient": %d{ZENBytesRxClient},
  "ZENTotalBytesTxClient": %d{ZENTotalBytesTxClient},
  "ZENBytesTxClient": %d{ZENBytesTxClient},
  "ZENTotalBytesRxConnector": %d{ZENTotalBytesRxConnector},
  "ZENBytesRxConnector": %d{ZENBytesRxConnector},
  "ZENTotalBytesTxConnector": %d{ZENTotalBytesTxConnector},
  "ZENBytesTxConnector": %d{ZENBytesTxConnector},
  "Idp": %j{Idp},
  "ClientToClient": %j{c2c},
  "ConnectorZENSetupTime": %d{ConnectorZENSetupTime},
  "ConnectionSetupTime": %d{ConnectionSetupTime}
}
```

User Status Log Format

User Status Log Format, Default Port: 9019

```
{
  "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{TimestampAuthenticatio
  n:iso8601}, "TimestampUnAuthentication": %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}], "SAMLAttributes": %j{SAMLAttributes}, "PosturesHit": [%j(,){PosturesHit}], "PosturesMiss": [%j(,){PosturesMiss}], "ZENLatitude":
  %f{ZENLatitude}, "ZENLongitude": %f{ZENLongitude}, "ZENCountryCode": %j{ZENCountryCode}, "FQDNRegistered": %j{fqdn_registered}, "FQDNRegisteredError":
  %j{fqdn_register_error}}\n
```

App Connector Status Log Format

App Connector Status Log Format, Default Port: 9015

```
{
  "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}, "TimestampAuthentication": %j{TimestampAuthenticatio
  n:iso8601}, "TimestampUnAuthentication": %j{TimestampUnAuthentication:iso8601}, "CPUUtilization": %d{CPUUtilization}, "MemUtilization": %d{MemUtilization}, "ServiceC
  ount": %d{ServiceCount}, "InterfaceDefRoute": %j{InterfaceDefRoute}, "DefRouteGW": %j{DefRouteGW}, "PrimaryDNSResolver": %j{PrimaryDNSResolver}, "HostUpTime": %j{HostUpTime}, "C
  onnectorUpTime": %j{ConnectorUpTime}, "NumOfInterfaces": %d{NumOfInterfaces}, "BytesRxInterface": %d{BytesRxInterface}, "PacketsRxInterface": %d{PacketsRxInterface}, "ErrorsRxI
  nterface": %d{ErrorsRxInterface}, "DiscardsRxInterface": %d{DiscardsRxInterface}, "BytesTxInterface": %d{BytesTxInterface}, "PacketsTxInterface": %d{PacketsTxInterface}, "Error
  sTxInterface": %d{ErrorsTxInterface}, "DiscardsTxInterface": %d{DiscardsTxInterface}, "TotalBytesRx": %d{TotalBytesRx}, "TotalBytesTx": %d{TotalBytesTx}}\n
```

Audit Log Format

Audit Log Format, Default Port: 9016

```
{
  "ModifiedTime": %j{modifiedTime:iso8601}, "CreationTime": %j{creationTime:iso8601}, "Modifie
  dBy": %d{modifiedBy}, "RequestID": %j{requestId}, "SessionID": %j{sessionId}, "AuditOldValue":
  %j{auditOldValue}, "AuditNewValue": %j{auditNewValue}, "AuditOperationType": %j{auditOper
  ationType}, "ObjectType": %j{objectType}, "ObjectName": %j{objectName}, "ObjectID": %d{objec
  tId}, "CustomerID": %d{customerId}, "User": %j{modifiedByUser}, "ClientAuditUpdate": %d{isCli
  entAudit}}\n
```

Browser Access Log Format

Browser Access Log Format, Default Port: 9017

```
{ "LogTimestamp":%j{LogTimestamp:time}, "ConnectionID":%j{ConnectionID}, "Exporter":%j{Ex
porter}, "TimestampRequestReceiveStart":%j{TimestampRequestReceiveStart:iso8601}, "Times
tampRequestReceiveHeaderFinish":%j{TimestampRequestReceiveHeaderFinish:iso8601}, "Times
tampRequestReceiveFinish":%j{TimestampRequestReceiveFinish:iso8601}, "TimestampRequestT
ransmitStart":%j{TimestampRequestTransmitStart:iso8601}, "TimestampRequestTransmitFinis
h":%j{TimestampRequestTransmitFinish:iso8601}, "TimestampResponseReceiveStart":%j{Times
tampResponseReceiveStart:iso8601}, "TimestampResponseReceiveFinish":%j{TimestampRespons
eReceiveFinish:iso8601}, "TimestampResponseTransmitStart":%j{TimestampResponseTransmitS
tart:iso8601}, "TimestampResponseTransmitFinish":%j{TimestampResponseTransmitFinish:iso
8601}, "TotalTimeRequestReceive":%d{TotalTimeRequestReceive}, "TotalTimeRequestTransmit"
:%d{TotalTimeRequestTransmit}, "TotalTimeResponseReceive":%d{TotalTimeResponseReceive},
"TotalTimeResponseTransmit":%d{TotalTimeResponseTransmit}, "TotalTimeConnectionSetup":%
d{TotalTimeConnectionSetup}, "TotalTimeServerResponse":%d{TotalTimeServerResponse}, "Met
hod":%j{Method}, "Protocol":%j{Protocol}, "Host":%j{Host}, "URL":%j{URL}, "UserAgent":%j{U
serAgent}, "XFF":%j{XFF}, "NameID":%j{NameID}, "StatusCode":%d{StatusCode}, "RequestSize":
%d{RequestSize}, "ResponseSize":%d{ResponseSize}, "ApplicationPort":%d{ApplicationPort},
"ClientPublicIp":%j{ClientPublicIp}, "ClientPublicPort":%d{ClientPublicPort}, "ClientPri
vateIp":%j{ClientPrivateIp}, "Customer":%j{Customer}, "ConnectionStatus":%j{ConnectionSt
atus}, "ConnectionReason":%j{ConnectionReason}, "Origin":%j{Origin}, "CorsToken":%j{CorsT
oken}}\n
```

Enabling ZPA Integration in Kibana

1. Log into Kibana.
2. From the **Management** drop-down menu, select **Integrations**.

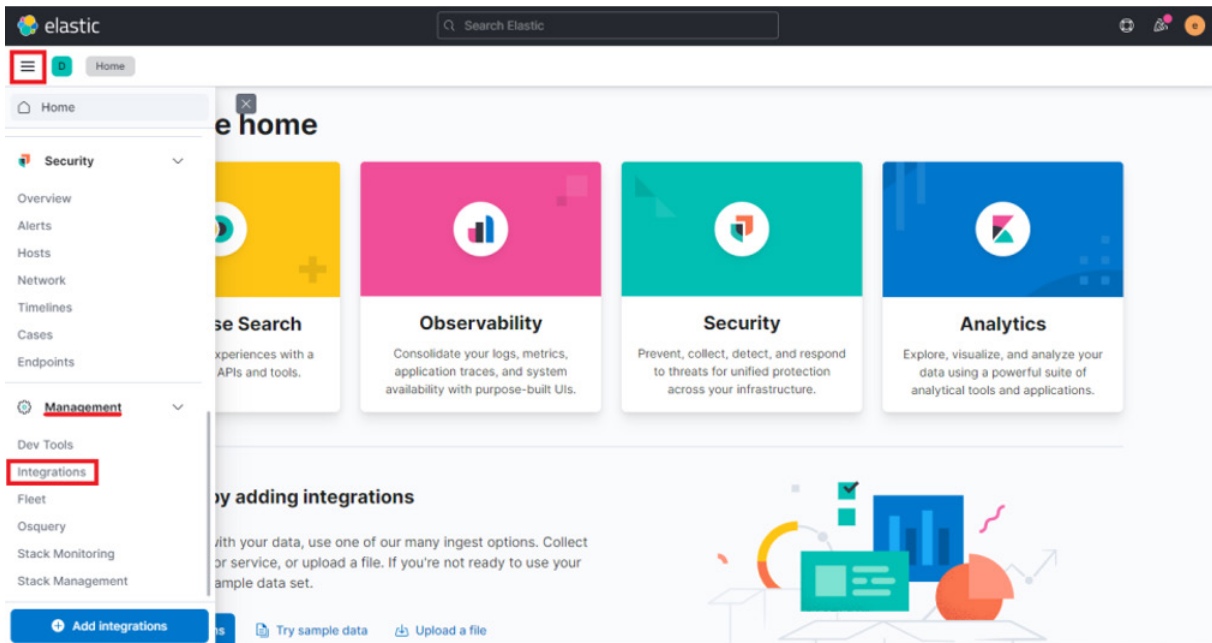


Figure 11. Elastic Integrations

3. Search for Zscaler ZPA, then select the **Zscaler Private Access** tile.

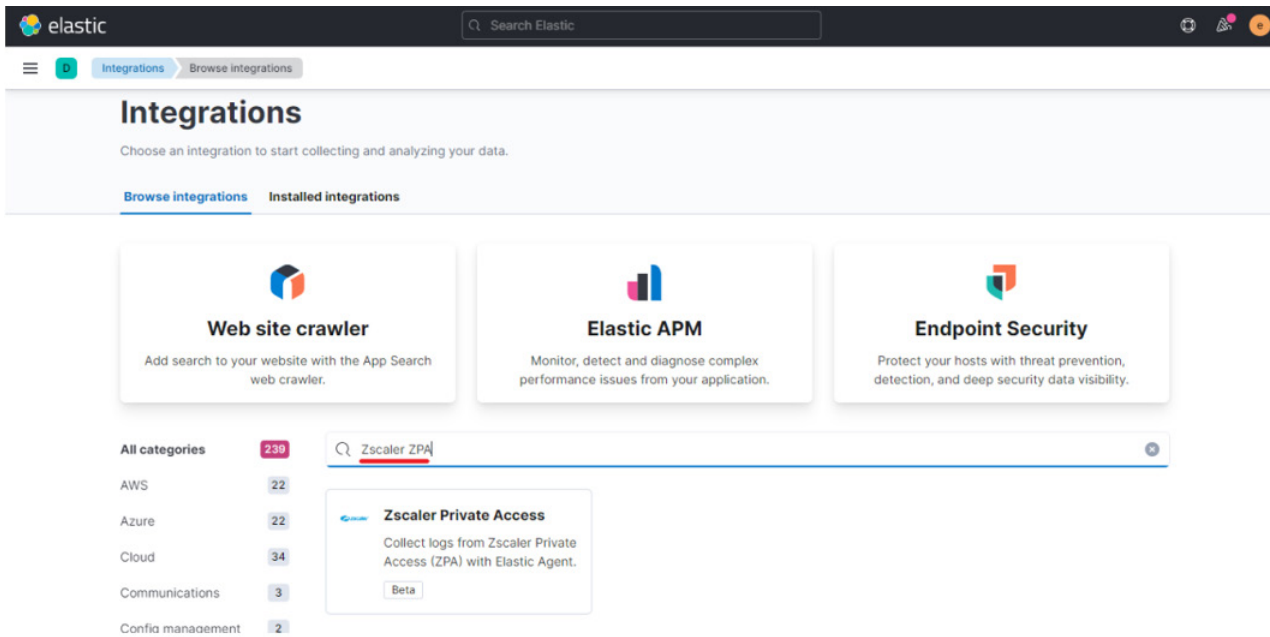


Figure 12. ZPA integrations

4. Enable the appropriate logs (e.g., App Connector Status, Audit, Browser Access, etc.).

elastic Search Elastic

Integrations Zscaler Private Access Add integration Send Feedback Fleet settings

☒ Collect Zscaler Private Access logs via TCP input

Settings
The following settings are applicable to all inputs below.

Listen Address
localhost
The bind address to listen for TCP connections. Set to 0.0.0.0 to bind to all available interfaces.
[Advanced options](#)

☒ Zscaler Private Access App Connector Status Logs
Collect Zscaler Private Access App Connector Status Logs using tcp input

Listen Port
9015
The TCP port number to listen on.

Preserve original event
☒
Preserves a raw copy of the original event, added to the field event.original
[Advanced options](#)

☒ Zscaler Private Access Audit Logs

Listen Port
9018

Cancel Save and continue

Figure 13. ZPA Log selection

5. Apply the integration to an **Agent policy** and ensure the agent you used when adding the feed in the ZPA Admin Portal is assigned to that policy.

elastic Search Elastic

Integrations Zscaler Private Access Add integration Send Feedback Fleet settings

Activity Logs
Collect Zscaler Private Access User Activity Logs using tcp input

Listen Port
9018
The TCP port number to listen on.

Preserve original event
☒
Preserves a raw copy of the original event, added to the field event.original
[Advanced options](#)

☒ Zscaler Private Access User Status Logs
Collect Zscaler Private Access User Status Logs using tcp input

Listen Port
9019
The TCP port number to listen on.

Preserve original event
☒
Preserves a raw copy of the original event, added to the field event.original
[Advanced options](#)

2 Apply to agent policy

Agent policy
Agent policies are used to manage a group of integrations across a set of agents

Agent policy
Default policy
1 agent is enrolled with the selected agent policy.
[Create agent policy](#)

Cancel Save and continue

Figure 14. Assign agent policy to feed

6. Click **Save and continue**.

Viewing ZPA Dashboards in Kibana

1. Log into Kibana.
2. From the **Analytics** tab, select **Dashboard**.
3. Search for `zscaler zpa`.

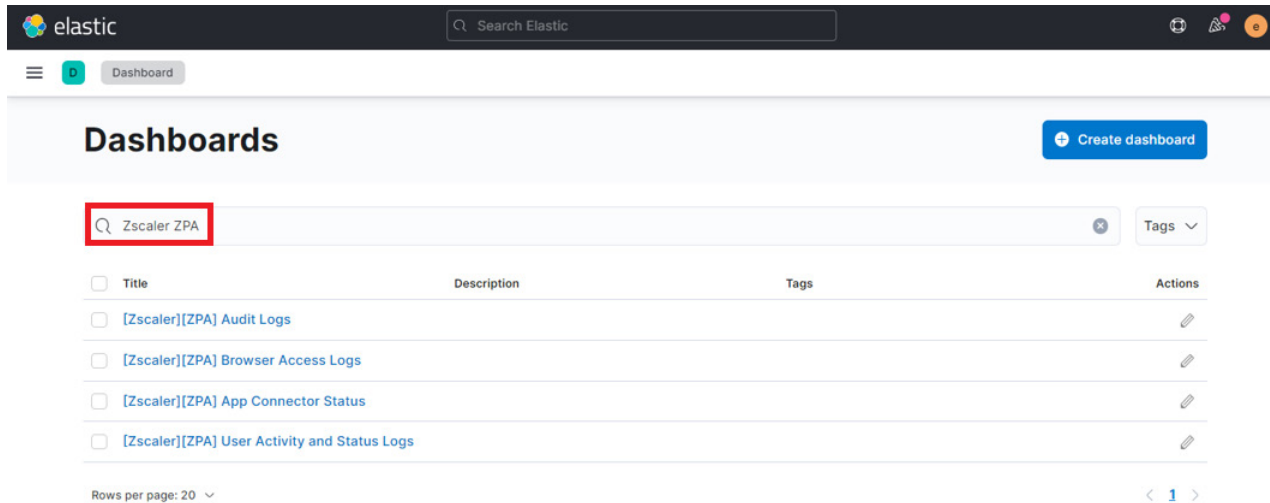


Figure 15. Elastic dashboards

4. Click the appropriate dashboard to start interacting with your Zscaler events in Elastic.

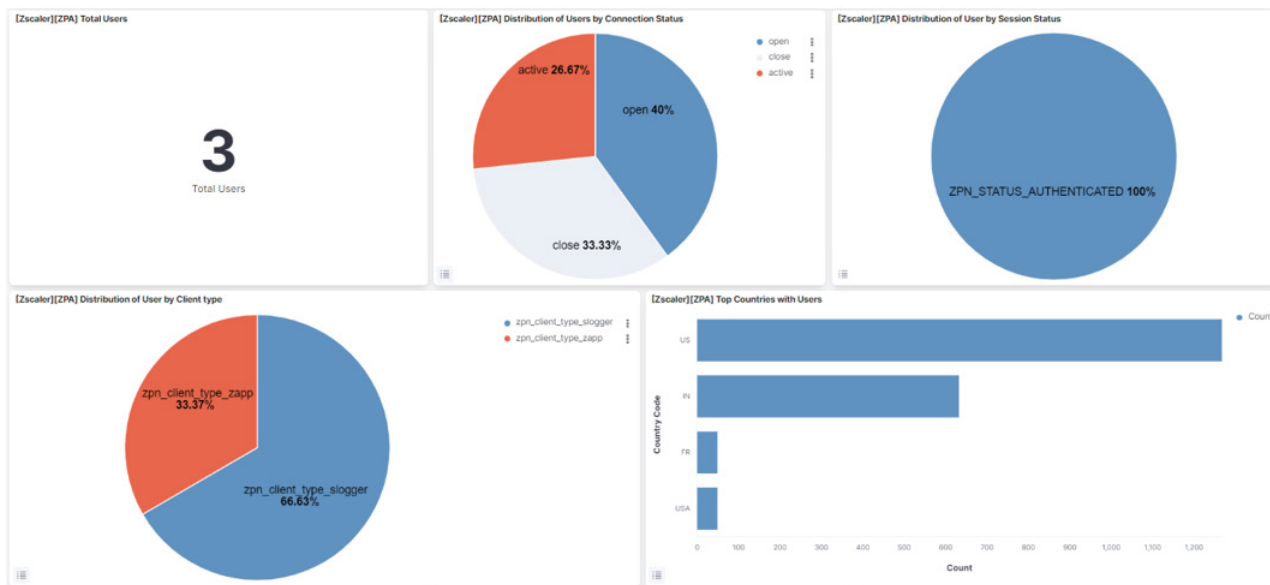
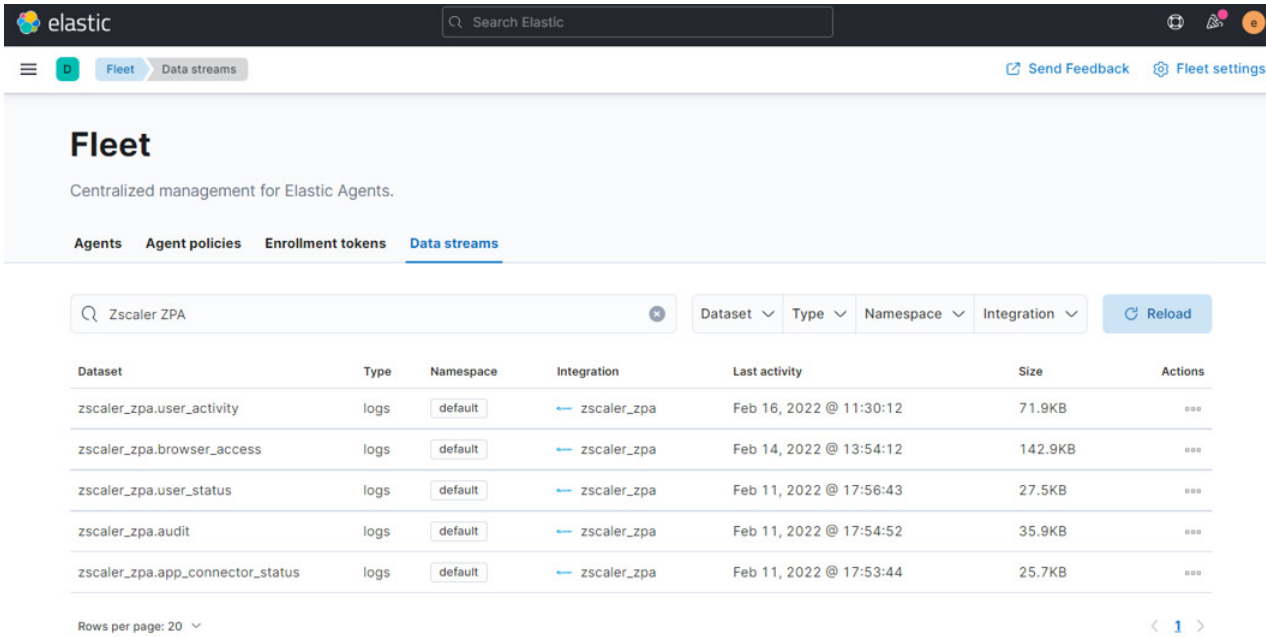


Figure 16. Elastic dashboard details

Zscaler ZPA Datastreams

From the **Management** drop-down menu, select **Fleet**.



The screenshot shows the Elastic Fleet interface. At the top, there's a search bar with "Zscaler ZPA" entered. Below the search bar, there's a table with columns: Dataset, Type, Namespace, Integration, Last activity, Size, and Actions. The table lists five data streams for Zscaler ZPA, all of type "logs" and namespace "default". The integration for all is "zscaler_zpa". The last activity dates range from Feb 11, 2022 to Feb 16, 2022. The sizes range from 25.7KB to 142.9KB. At the bottom, there's a pagination control showing "Rows per page: 20" and a page number "1".

Dataset	Type	Namespace	Integration	Last activity	Size	Actions
zscaler_zpa.user_activity	logs	default	zscaler_zpa	Feb 16, 2022 @ 11:30:12	71.9KB	...
zscaler_zpa.browser_access	logs	default	zscaler_zpa	Feb 14, 2022 @ 13:54:12	142.9KB	...
zscaler_zpa.user_status	logs	default	zscaler_zpa	Feb 11, 2022 @ 17:56:43	27.5KB	...
zscaler_zpa.audit	logs	default	zscaler_zpa	Feb 11, 2022 @ 17:54:52	35.9KB	...
zscaler_zpa.app_connector_status	logs	default	zscaler_zpa	Feb 11, 2022 @ 17:53:44	25.7KB	...

Rows per page: 20

< 1 >

Figure 17. Elastic Fleet window

For additional information on field format, refer to the [Elastic docs](#).

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**.

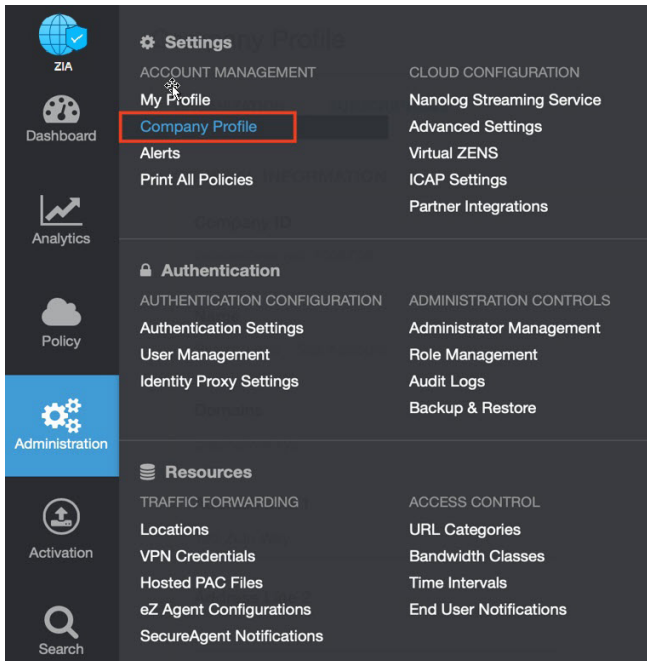


Figure 18. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

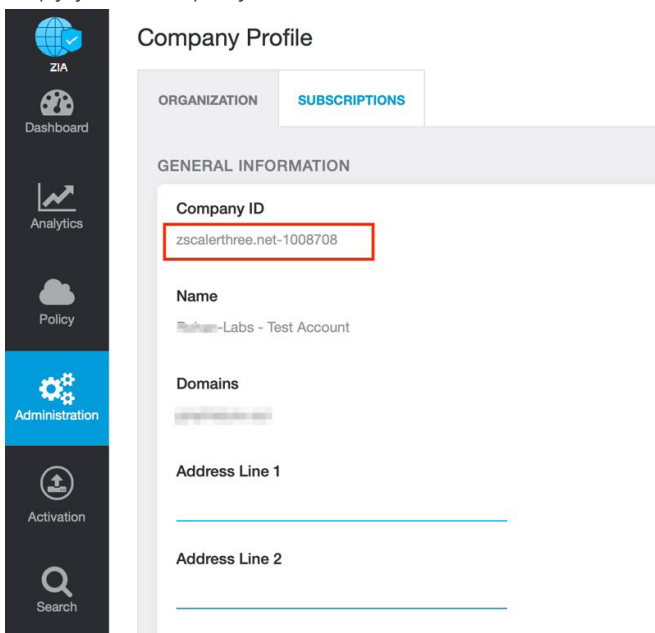


Figure 19. Company ID

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

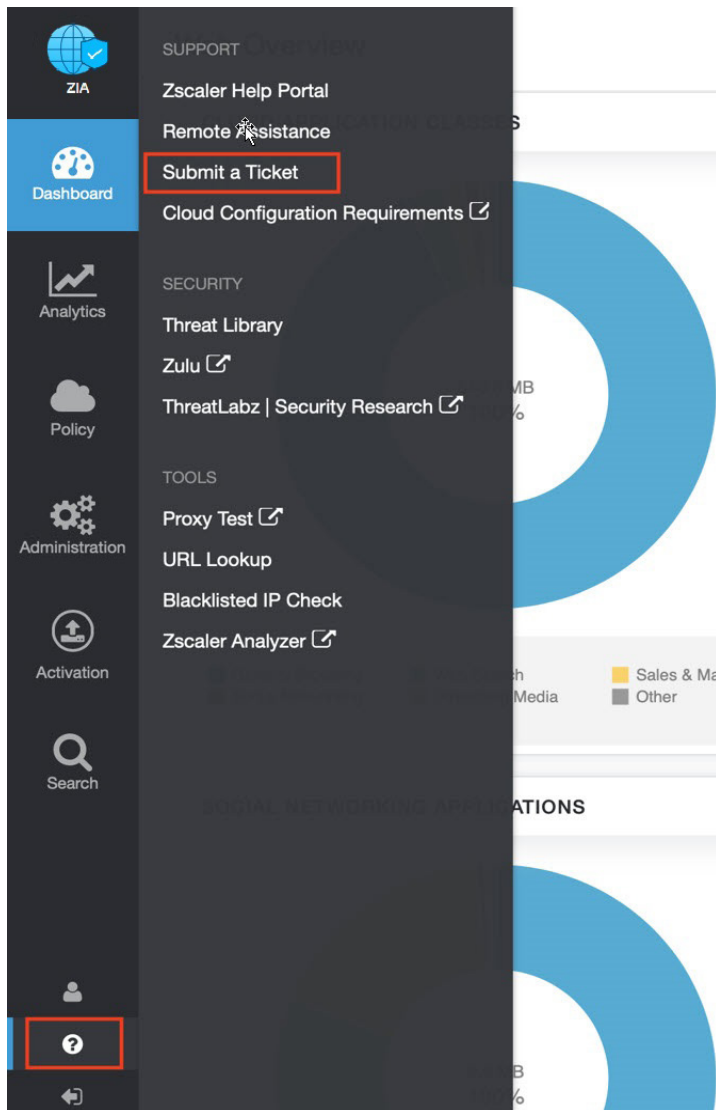


Figure 20. Submit a ticket