



ZSCALER AND NILE DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	6
Zscaler Overview	6
Nile Overview	6
Audience	6
Software Versions	6
Request for Comments	6
Zscaler and Nile Introduction	7
ZIA Overview	7
Nile Copilot Overview	8
Nile Resources	8
ZIA Configuration and Integration with Nile	9
Prerequisites	9
Configuration	10
ZIA Configuration Prerequisites	10
Partner Integration Key Configuration	10
SD-WAN Partner API Role Configuration	11
SD-WAN Partner API Client Configuration	13
Activate Pending Changes	15
Configure Local Firewall	15
SSE Instance Configuration in Nile Copilot	16
Configure Trust Engine Rule to Exercise SSE integration	18
Appendix A: Verifying ZIA Configuration	21

Appendix B: Checking Tunnel Status in ZIA Admin	22
Tunnel Data Visualization	22
Tunnel Logging	23
Appendix C: Checking the Audit Log for API Troubleshooting	24
Appendix D: Nile Integration Notes	25
Appendix E: Requesting Zscaler Support	26

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
SA	Security Association
SaaS	Software as a Service
SASE	Secure Access Service Edge
SSE	Security Service Edge
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

© 2024 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

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](#).

Nile Overview

Nile is disrupting the enterprise network market by building natively secure connectivity that modernizes IT operations with a new AI networking architecture, delivering enterprise networks entirely as a service. For the first time in the industry, the Nile Access Service integrates Zero Trust security and offers performance guarantees for connectivity, coverage, and availability. With Nile, IT organizations close the gap between their digital aspirations and legacy realities with superior connectivity that reduces the burden on critical IT resources. To learn more, refer to [Nile's website](#).

Audience

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

- [Zscaler Resources](#)
- [Nile Resources](#)
- [Appendix E: 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 Nile Introduction

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



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

ZIA Overview

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

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

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Nile Copilot Overview

Nile Copilot application suite is purpose-built for IT admins to enable the orchestration of the Nile Service Block and gain crucial visibility and control. With Copilot, you gain:

- Radically simplified provisioning
- Embedded Zero Trust security policies
- Full stack control and visibility

Nile Resources

The following table contains links to Nile support resources.

Name	Definition
Nile Help	Online help for Nile products.
Nile Support	Online tech support for Nile products.

ZIA Configuration and Integration with Nile

This document provides necessary information regarding the configuration and integration of ZIA service endpoint with Nile for forwarding and managing device traffic through SASE policies. This document's target audience are customers who are planning to integrate ZIA instances with Nile Copilot.

SSE is used for ZIA throughout the documentation unless the configuration is ZIA-specific. In cases where configuration is limited to ZIA, ZIA is used.

Prerequisites

Make sure the following prerequisites are met:

- Install a ZIA account.
- Enable Nile Trust Engine feature.
- Upgrade the Nile Elements with software that supports SSE integration and IPSec tunneling.

Configuration

This section covers three areas:

- Configuring an SSE instance in Nile Copilot.
 - Adding ZIA configuration needed to enable SSE integration in Nile Copilot.
 - Configuring Nile Copilot to communicate with SSE endpoint.
- Configuring a Trust Engine rule to forward traffic to the SSE endpoint.
- Checking expected auto-generated configuration on the SSE endpoint.

ZIA Configuration Prerequisites

There are three ZIA-specific configurations that a user must do to start ZIA integration with Nile Copilot.

- [Partner Integration Key Configuration](#)
- [SD-WAN Partner API Role Configuration](#)
- [Configure Local Firewall](#)

Partner Integration Key Configuration

This key is used to configure and maintain IPsec tunnel configuration. Users can follow these steps to configure a Partner Integration Key for Nile.

This must be done only once, and you can skip this step if a Partner Integration Key is already configured for Nile Integration.

1. Log in to your ZIA Admin Portal.
2. Go to **Administration > Settings > Partner Integrations**.

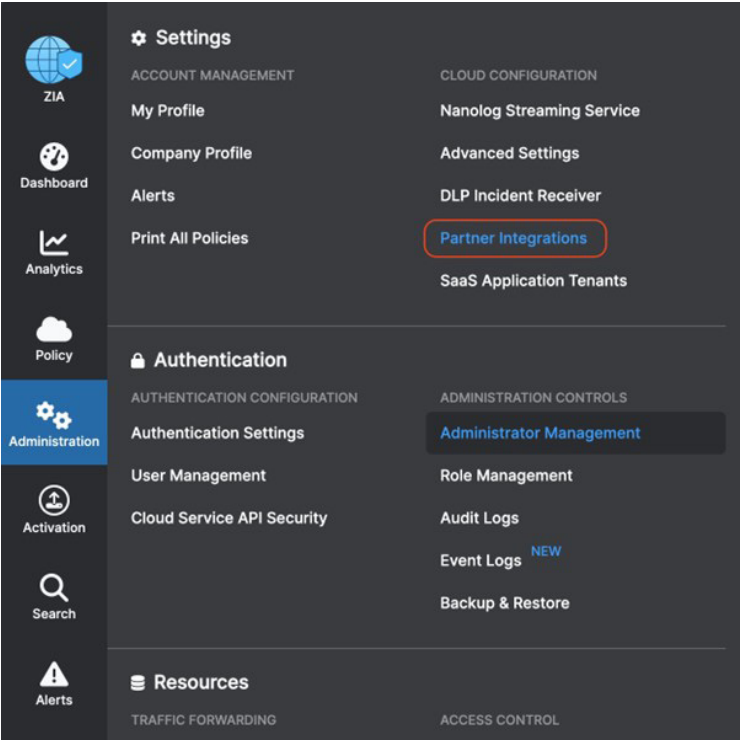


Figure 1. Partner Integrations

- On the **Partner Integrations** page, select the **SD-WAN** tab, then click **Add Partner Key**.

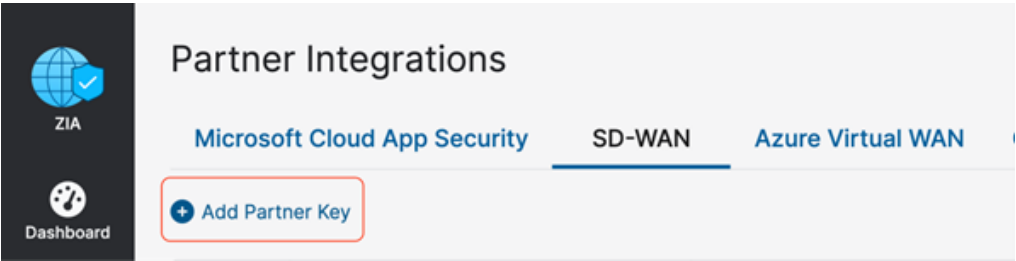


Figure 2. Add Partner Key

- In the window that displays, search for Nile and generate the key. Users can see the Partner Key listed in the **SD-WAN** table. This **Key** is used to configure an SSE Instance in Nile Copilot.

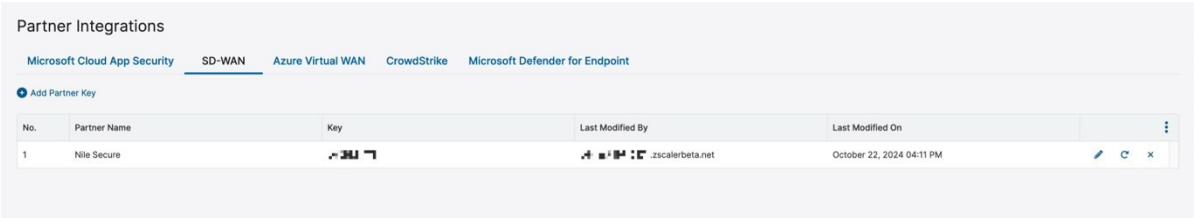


Figure 3. Partner SD-WAN Integrations

SD-WAN Partner API Role Configuration

If not created already, you must create a partner API role and assign it to the SD-WAN Partner API Client that is used to authenticate against the Zscaler ZIA Provisioning API.

- Go to **Administration > Authentication > Role Management**.

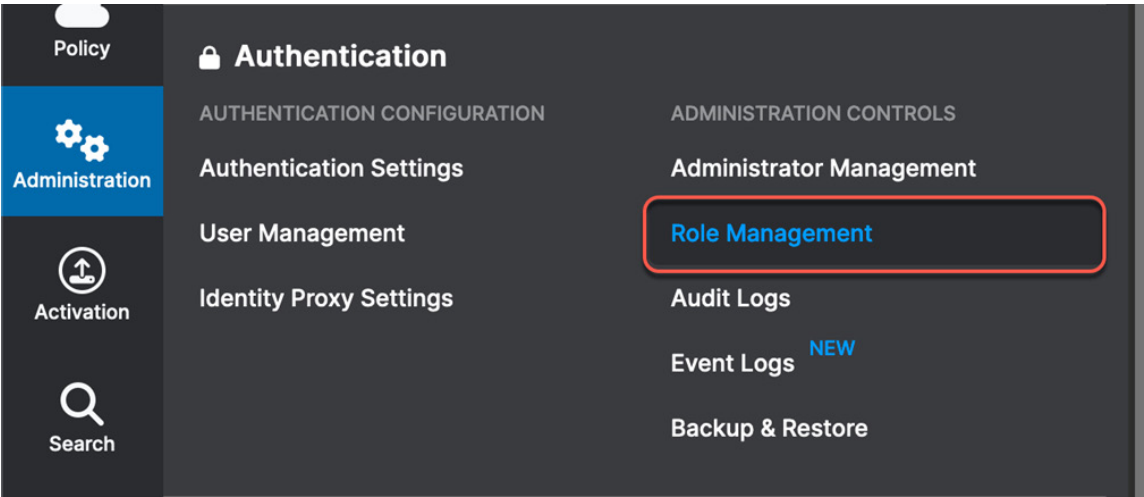


Figure 4. Adding a partner administrator role

- Click **Add Partner SD-WAN Partner API Role**. You use the partner API role to define and grant permission and access to an SD-WAN partner.

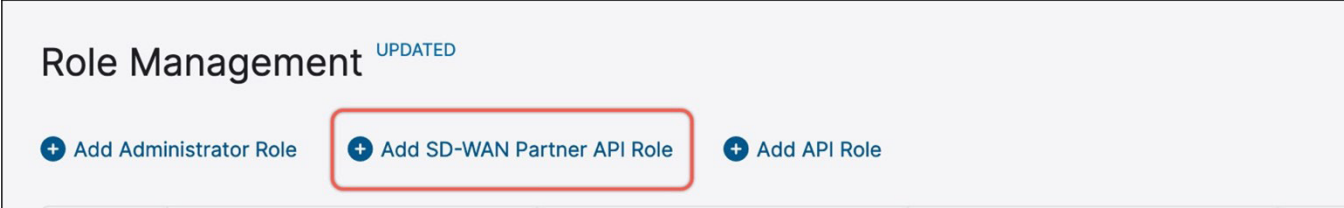


Figure 5. Add the partner administrator role

- Name the partner administrator role.
- Change **Access Control** to **Full**. This allows partner admins to view and edit VPN credentials and locations managed by Aruba Orchestrator via the ZIA Provisioning API. This control is necessary for the Aruba Orchestrator to create new VPN credentials and locations for branch locations.

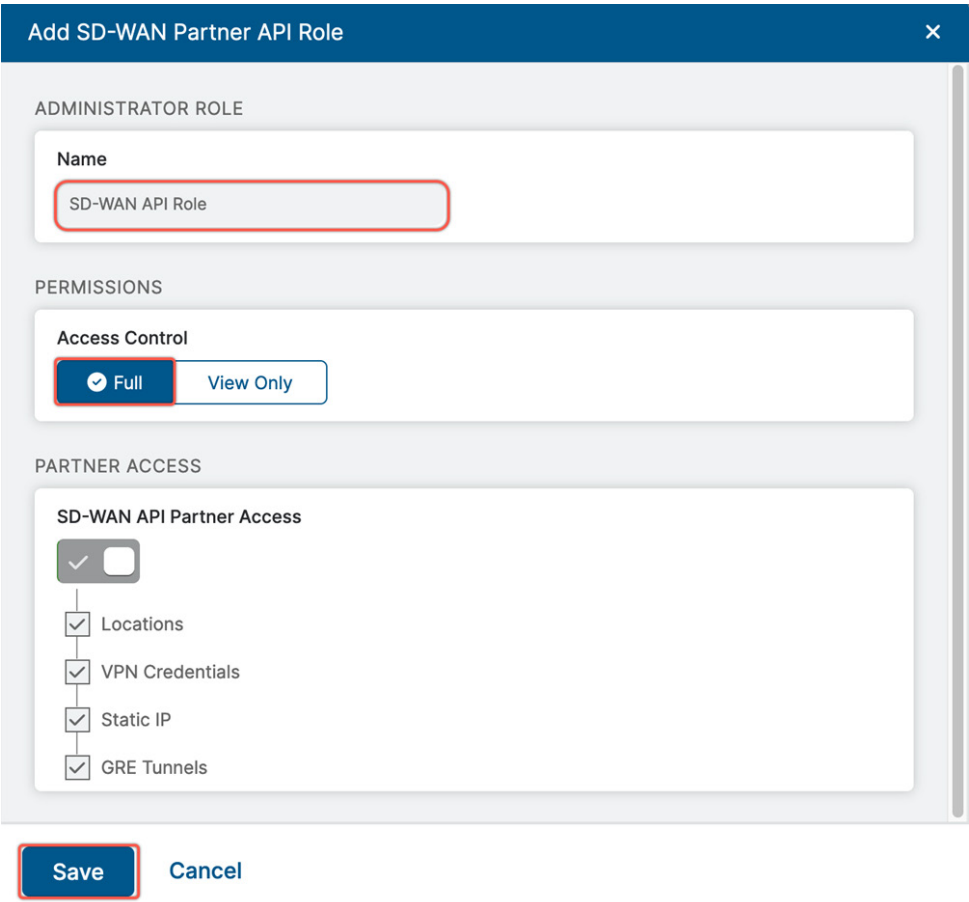


Figure 6. Creating a partner administrator role

- Click **Save**. You are returned to the previous dialog.

SD-WAN Partner API Client Configuration

Zscaler recommends this process to set up secure credentials with limited scope to access the Partner Key.

Do not use Admin Credentials for integration of SSE or a ZIA instance.

This must be done only once, and you can skip this step if Partner Credentials are already set up.

Partner API Client credentials are created using the following steps.

1. Log in to your ZIA Admin Portal.
2. Go to **Administration > Authentication > Administrator Management**.

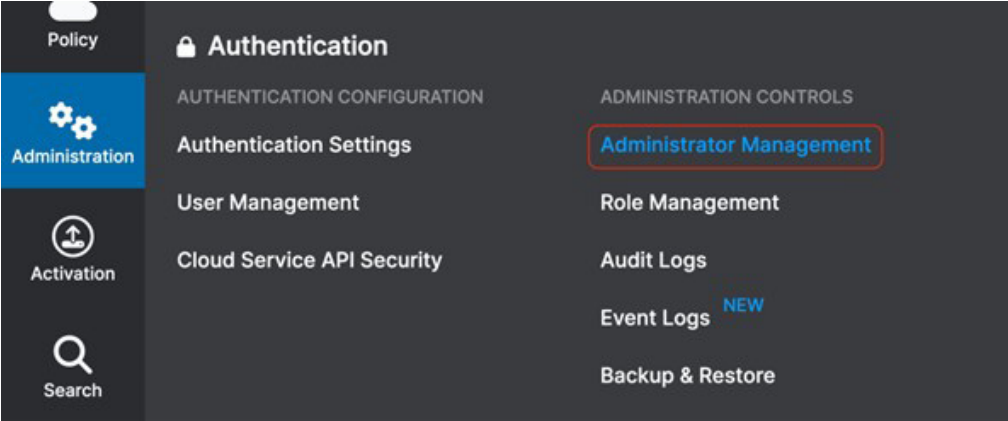


Figure 7. Administrator Management

3. On the **Administrator Management** page, click **Add SD-WAN Partner API Client**.

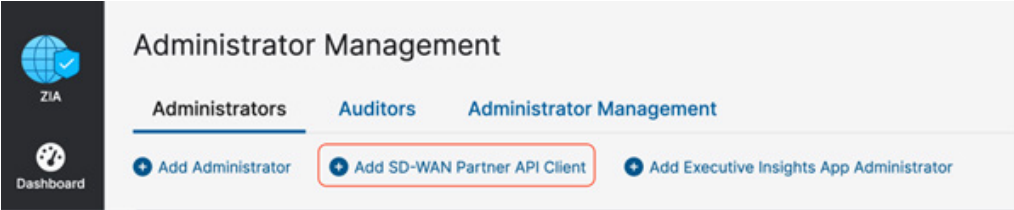


Figure 8. Add SD-WAN Partner API Client

4. In the Add SD-WAN Partner API Client window, provide required details and save the credentials. These credentials are needed to configure an SSE Instance in Nile Copilot.

Add SD-WAN Partner API Client

ADMINISTRATOR

Login ID

SamplePartner

@

Select your domain

▼

Email

samplepartner@your.domain

Name

Sample Partner

Partner Role

NONE

Select Required Role if needed ▼

Status

Enabled

▼

Comments

SET PASSWORD

Password

.....

Confirm Password

.....

Save

Cancel

Figure 9. Configure SD-WAN Partner API Client

5. Review the Partner API Client configured in the table.

Save the Email and Password settings for the Nile Admin Portal during [SSE Instance Configuration in Nile Copilot](#).

©2024 Zscaler, Inc. All rights reserved. 14

Activate Pending Changes

Go to **Activation** and activate the pending configurations.

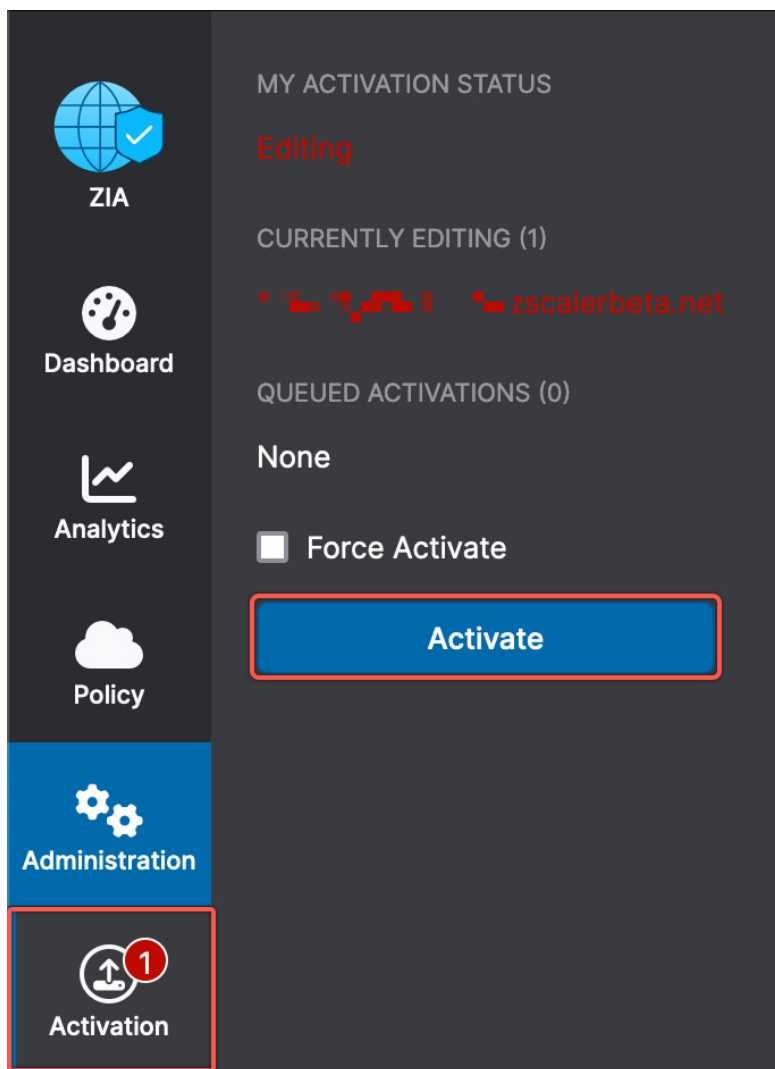


Figure 10. Activate pending changes

Configure Local Firewall

Make sure to unblock UDP port 500 and 4500 on the local firewall towards the internet. This ensures that the IPSec tunnels using NAT traversal mode are not blocked.

SSE Instance Configuration in Nile Copilot

This section covers the SSE Instance configuration in Nile Copilot. Use following steps to create the SSE integration instance.

1. Log in to the Nile Copilot.
2. Go to **Settings > Global Settings > Integrations**.
3. Click **Setup integration with third party solutions**.

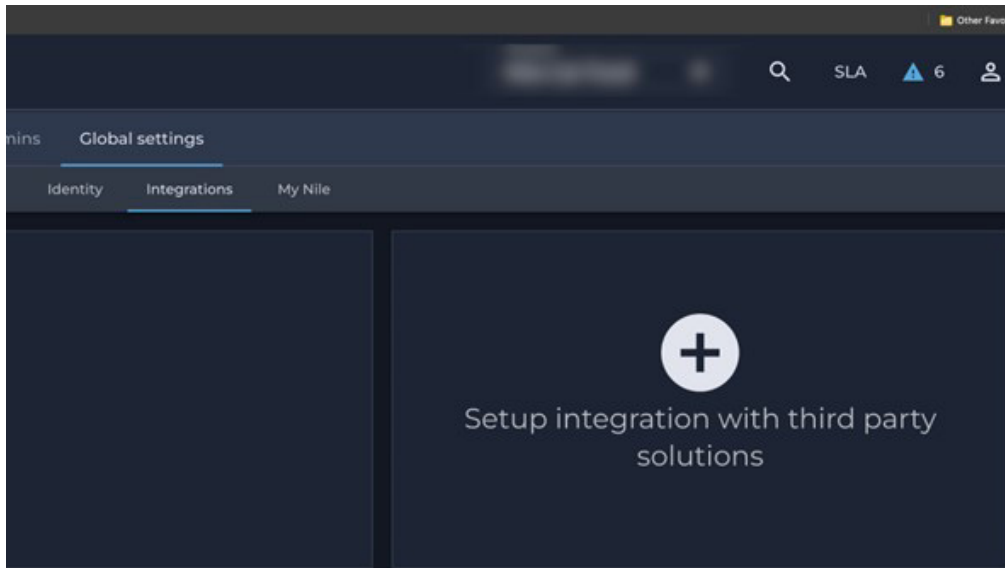


Figure 11. Setup integration with third party solutions

4. For the integration options, choose **SASE**.

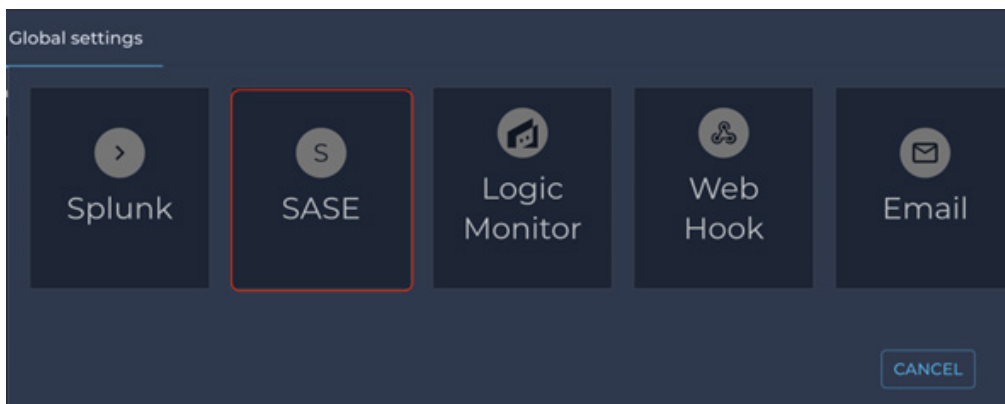
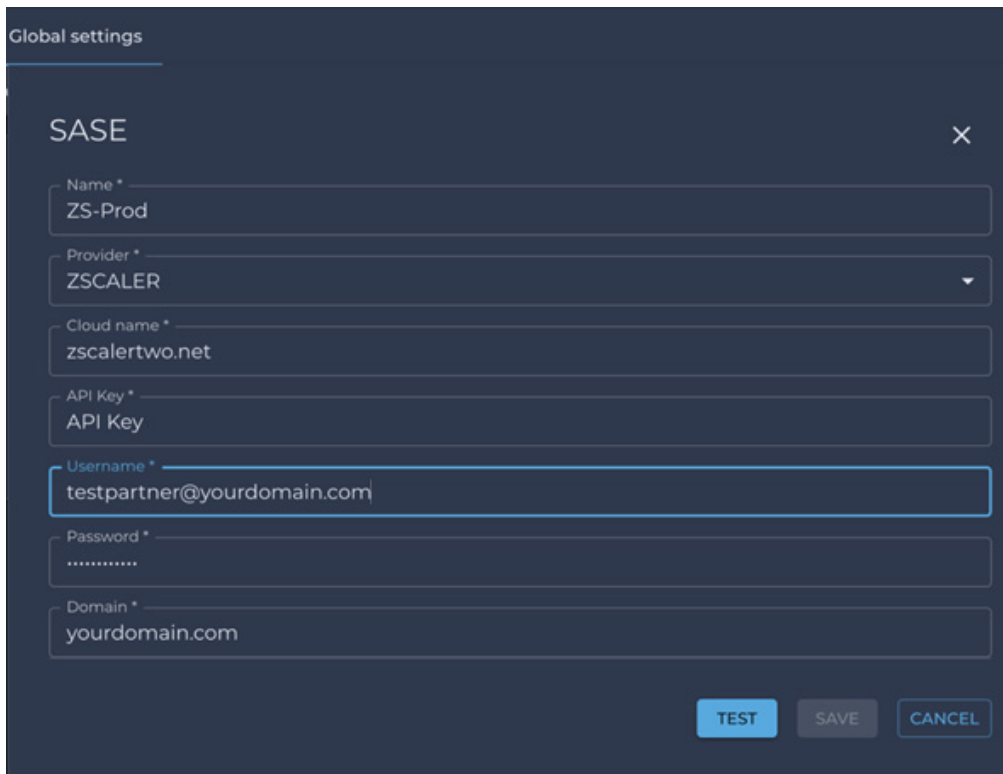


Figure 12. Integrations options

5. On the configuration dialog, fill in the required details.
 - a. Enter a **Name** for the instance.
 - b. For ZIA, select **ZSCALER** as the **Provider**.
 - c. Enter the ZIA cloud name domain for **Cloud name**. To learn more, see [What is My Cloud Name for ZIA](#) (government agencies, see [What is My Cloud Name for ZIA](#)).
 - d. Enter the **API key**.
 - e. Enter the **Username** and **Password** credentials.
 - f. Enter a **Domain**.
6. Click **TEST**.



The screenshot shows a 'Global settings' dialog box titled 'SASE'. It contains several input fields: 'Name' with the value 'ZS-Prod', 'Provider' with a dropdown menu showing 'ZSCALER', 'Cloud name' with the value 'zscalertwo.net', 'API Key' with the value 'API Key', 'Username' with the value 'testpartner@yourdomain.com', 'Password' with masked characters '*****', and 'Domain' with the value 'yourdomain.com'. At the bottom right, there are three buttons: 'TEST' (highlighted in blue), 'SAVE', and 'CANCEL'.

Figure 13. Global settings

7. When the configuration test is successful, save the configuration. The configuration is displayed in the Nile Copilot integrations list.
8. When complete, the SSE integration is available for use in internet-bound traffic management.

Configure Trust Engine Rule to Exercise SSE integration

This section covers creating rules for forward internet-based traffic to SSE integration configured in Nile Copilot.

1. Log in to the Nile Copilot.
2. Go to **Settings > Global Settings > Access Engine**.
3. If you are a first-time user, you can see two default rules in the rule table.
 - a. **Default Internal Rule:** This rule is applicable for all traffic with source and destination inside the Nile-managed network at a given site.
 - b. **Default External Rule:** This rule is applicable to all traffic going outside the Nile-managed network at a given site.

You cannot delete either of these rules, though you can choose to change the action of the default based on the available choices.

4. Add an **External Rule** to manage internet-bound traffic through SSE integration.
5. Click **Create Rule** and then choose **Create External Rule**.

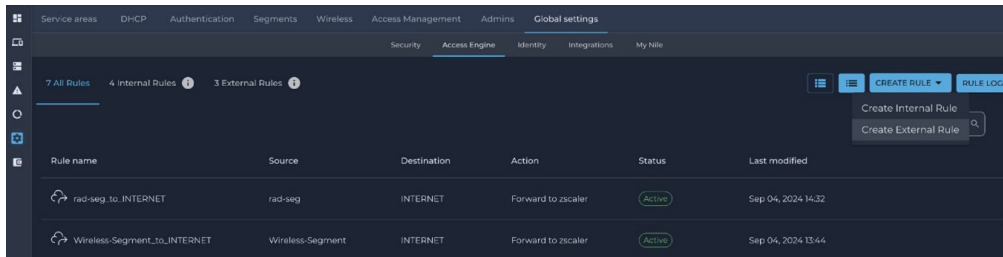


Figure 14. Create Rule

6. On the rule creation workflow page, select a segment, and then click **Next**.

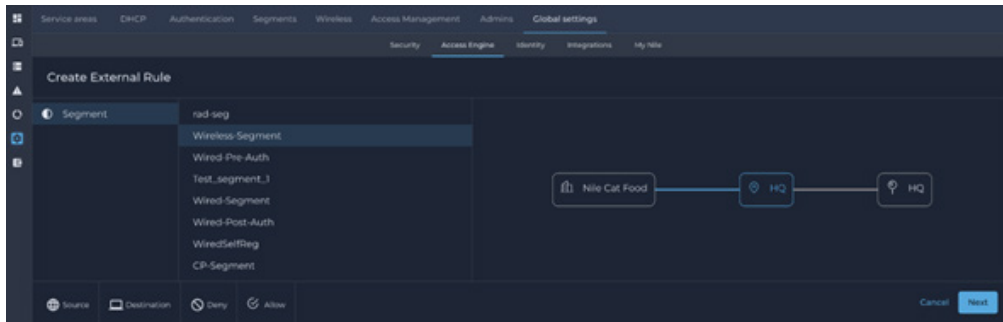


Figure 15. Create External Rule

7. Select **All Internet Bound Traffic**, then click **Next**.

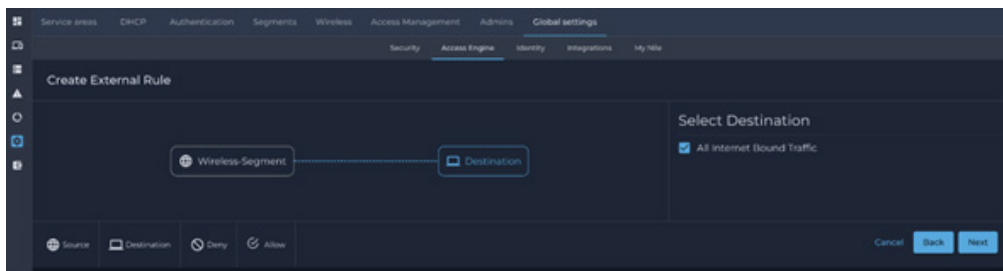


Figure 16. All Internet Bound Traffic

8. On the next window:
 - a. Select the **Zscaler** radio button representing the ZIA instance.
 - b. Enter the rule **Name** and **Description**.
 - c. Set the **Rule** state to **Active**.
 - d. (Optional) Choose the traffic to be forwarded to the local firewall if IPSec tunnels are impacted due to connectivity issues or other reasons.
 - e. Click **Save**. This creates the rule and lists it in the rule table. It can take up to two minutes for the rule to take effect.

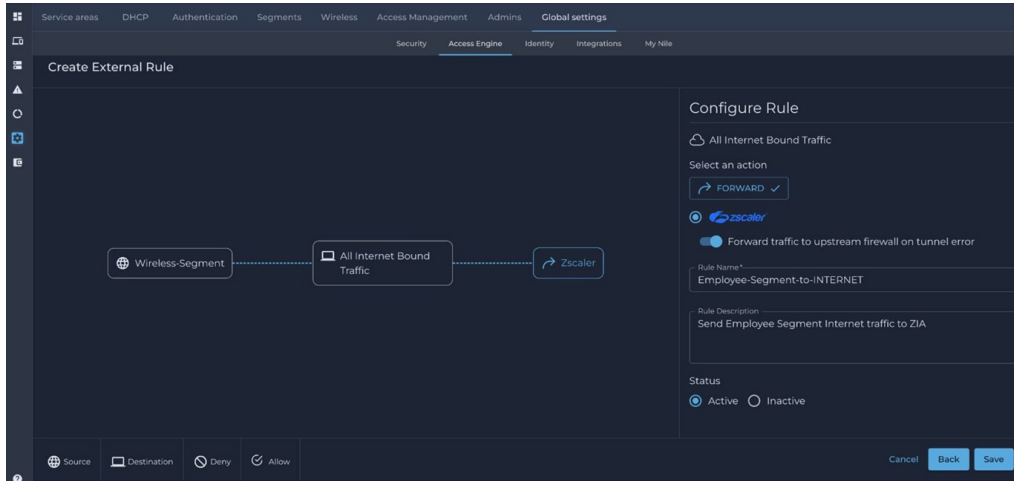


Figure 17. Configure Rule

You must add rules for each segment for which you want the traffic to be managed by the SSE instance.

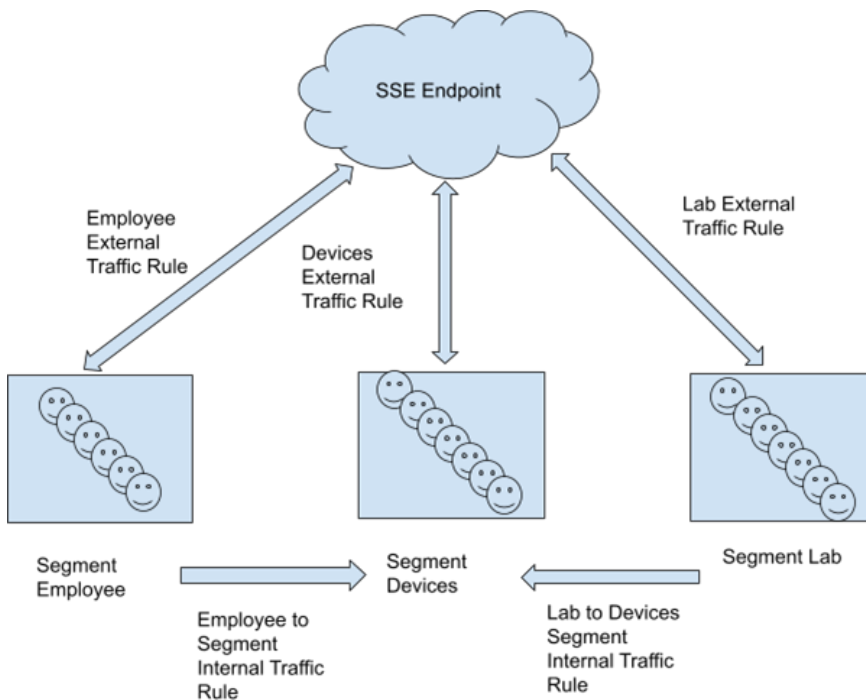


Figure 18. SSE endpoint architecture

Check Required Auto-Generated Configuration on ZIA

This section covers the configuration that is automatically generated on the ZIA side based on the integration with Nile Copilot. There is a specific schema that is followed when generating these configurations. IPSec tunnels are set up with the ZIA endpoint using Locations and Sublocations.

Locations in ZIA are configured for each site where internet traffic is managed using at least one segment forwarding internet traffic to ZIA. The naming schema is:

<Site Name in Nile Copilot>-<random number>

You can view locations in ZIA by going to **Administration > Resources > Location Management**.

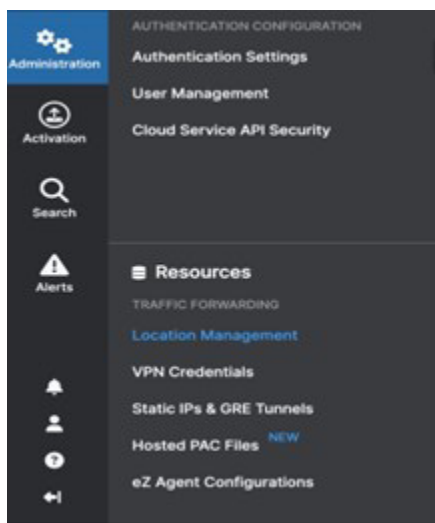


Figure 19. Location Management

Sublocations in ZIA are configured corresponding to each segment for which internet traffic is managed by ZIA at a given Location. The naming schema is:

<Segment Name in NileCopilot>-<random number>

To view sublocations:

1. Click **Location Management**. The **Location Management** table shows an entry populated for a location.
2. Click the number representing sublocation count against the location. This shows sublocation details and corresponding network subnet details as well.

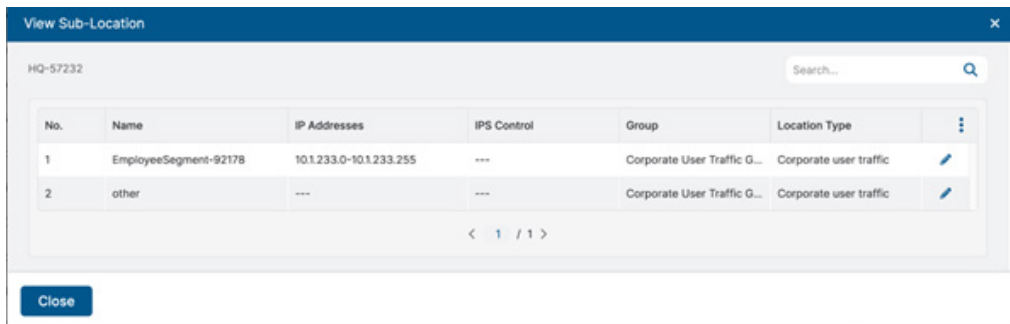


Figure 20. View Sublocations

Nile Copilot integration generates these configurations automatically. Do not manually change these configurations using the ZIA Admin Portal as the changes would not be persistent and can affect the network traffic in unexpected ways.

Appendix A: Verifying ZIA Configuration

Use the URL <https://ip.zscaler.com> to validate if you are transiting ZIA. The following figures show examples of what the page output should display if you are or are not transiting ZIA.



The IP information presented in both figures should not match and instead should be your client IP address when attempting this page view.



Connection Quality Zscaler Analyzer Cloud Health Security Research

The request received from you did not have an XFF header, so you are quite likely not going through the Zscaler proxy service.

Your request is arriving at this server from the IP address 209.37.255.2

Your Gateway IP Address is most likely 209.37.255.2

Figure 21. Non-working example

If you are transiting ZIA, you should see the following:

You are accessing this host via a Zscaler proxy hosted at Los Angeles in the zscalertwo.net cloud.

Your request is arriving at this server from the IP address 104.129.198.69

The Zscaler proxy virtual IP is 104.129.198.34.

The Zscaler hostname for this proxy appears to be zs2-qla1a1.

Figure 22. Working example

Appendix B: Checking Tunnel Status in ZIA Admin

If you want to check the status of tunnels to ZIA from your sites, ZIA provides the ability to see the traffic volume sent or received from your SD-WAN appliances and logging to see the current state of the tunnels via logging.

Go to **Analytics > Insights** and then click **Tunnel Insights**.

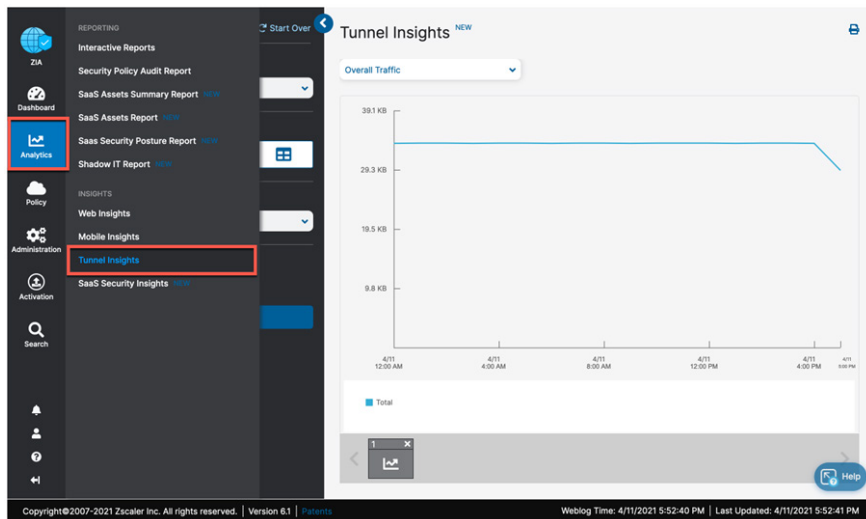


Figure 23. Tunnel Insights

Tunnel Data Visualization

In the Insights screen you can visualize and filter data in various ways. Configure the **Timeframe**, **Chart type**, and **Metrics** you want to view.

Additionally, you can filter the type of data shown in the chart, by clicking the filter carrot to expose a drop-down menu.

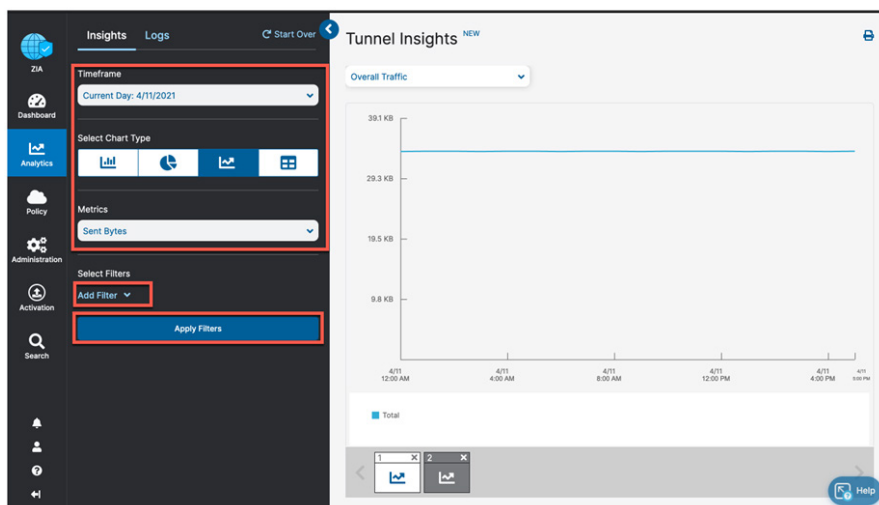


Figure 24. ZIA Tunnel Insight Charts

To learn more, see [ZIA Tunnel Insights](#) (government agencies, see [ZIA Tunnel Insights](#)).

Tunnel Logging

To assist in troubleshooting, you can also view the state of all tunnels for your tenant from the ZIA Admin Portal. Click **Logs**.

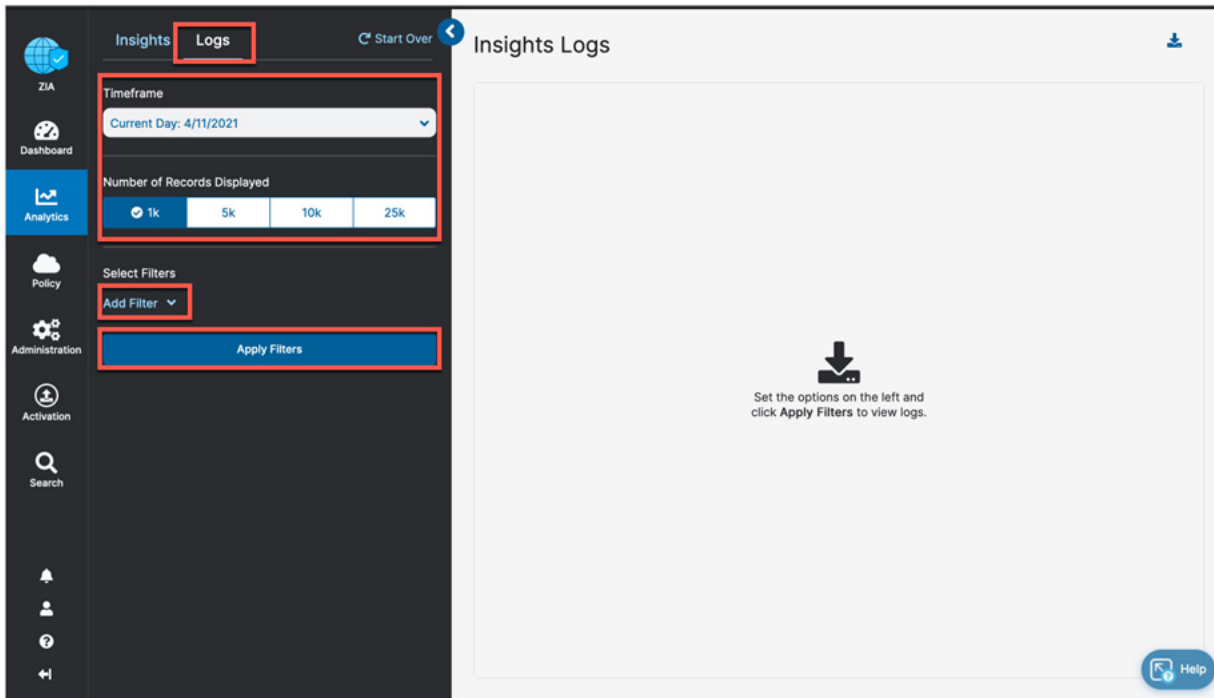


Figure 25. Viewing ZIA tunnel logs

From this window, you can filter and change the time frame for the tunnels and sites you want to investigate. To learn more, see [ZIA Tunnel Insights Logs](#) (government agencies, see [ZIA Tunnel Insights Logs](#)).

Appendix C: Checking the Audit Log for API Troubleshooting

ZIA provides the ability to view what changes are made to the tenant environment using the Audit Logging feature. You can also use ZIA view API calls into the platform.

Go to **Administration > Authentication > Audit Logs**.

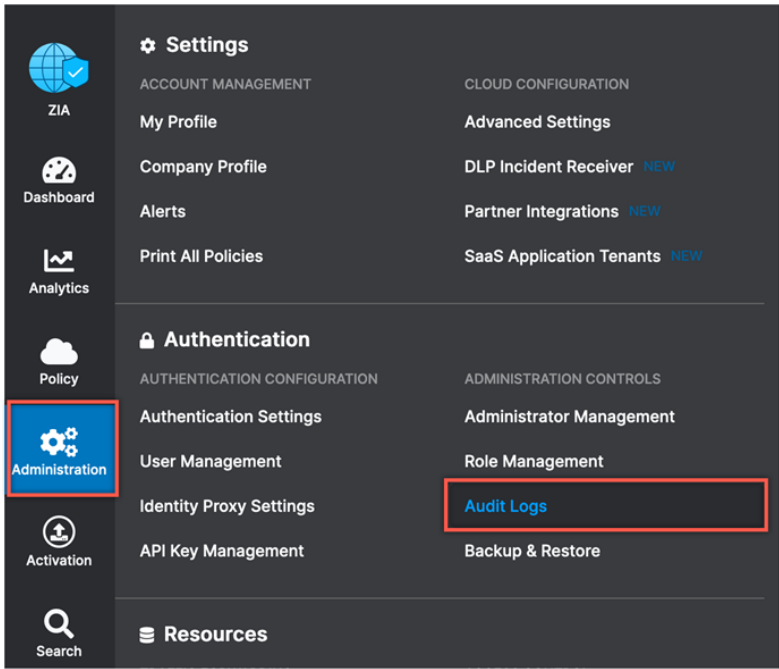


Figure 26. Navigate to ZIA Audit Logs

In the Audit Logs window, filter out all changes to only view the API calls by selecting **API** under the interface drop-down menu. A list of all the API interactions is displayed, and the **Result** column shows whether the call was successful or failed.

Audit Logs										
TIME RANGE		ACTION	CATEGORY	SUB-CATEGORY	INTERFACE	RESULT				
Current Day: 2/3/2022		All	All	All	API	All				
No.	Timestamp	Action	Category	Sub-Category	Resource	Admin ID	Client IP	Interface	Result	
1	February 03, 2022 - 06:43 PM	Delete	Traffic Forwarding Re...	Location	Guest	[REDACTED]	34.237.30.26	API	✓	⌵
2	February 03, 2022 - 06:43 PM	Update	Traffic Forwarding Re...	Location	SanJose2/INET1/3.NE_2	[REDACTED]	34.237.30.26	API	✓	⌵
3	February 03, 2022 - 06:43 PM	Delete	Traffic Forwarding Re...	Location	---	[REDACTED]	34.237.30.26	API	✓	⌵
4	February 03, 2022 - 06:42 PM	Activate	Activation	Activation	---	[REDACTED]	34.237.30.26	API	✓	⌵
5	February 03, 2022 - 06:41 PM	Create	Traffic Forwarding Re...	Location	Guest	[REDACTED]	34.237.30.26	API	✓	⌵
6	February 03, 2022 - 06:41 PM	Create	Traffic Forwarding Re...	Location	Guest	[REDACTED]	34.237.30.26	API	✓	⌵
7	February 03, 2022 - 06:41 PM	Delete	Traffic Forwarding Re...	Location	Guest	[REDACTED]	34.237.30.26	API	✓	⌵
8	February 03, 2022 - 06:41 PM	Delete	Traffic Forwarding Re...	Location	Guest	[REDACTED]	34.237.30.26	API	✓	⌵
9	February 03, 2022 - 06:41 PM	Update	Traffic Forwarding Re...	Location	SanJose1/INET2/2.NE_7	[REDACTED]	34.237.30.26	API	✓	⌵
10	February 03, 2022 - 06:41 PM	Update	Traffic Forwarding Re...	Location	SanJose2/INET2/3.NE_7	[REDACTED]	34.237.30.26	API	✓	⌵
11	February 03, 2022 - 06:41 PM	Create	Traffic Forwarding Re...	Location	Guest	[REDACTED]	34.237.30.26	API	✓	⌵
12	February 03, 2022 - 06:41 PM	Create	Traffic Forwarding Re...	Location	Guest	[REDACTED]	34.237.30.26	API	✓	⌵

Figure 27. ZIA Audit logs

Clicking the icon on the right of the Result column shows the API data that was created or updated from the call.

Appendix D: Nile Integration Notes

The following are details on Nile's automated integration work.

- Zscaler VPN credentials, locations, and sublocations are auto provisioned.
- Location
 - A location is created for every site per Nile Block. Location is created only when there is at least one segment at the site with a policy rule configured with action set to *forward to Zscaler*.
 - Nile does not configure gateway options for location nor change any gateway options updated by the customer. The customer is expected to configure them after the location is created.
- Sublocation
 - A sublocation is created for every segment with a policy rule with action set to *forward to Zscaler*.
 - A sublocation has all the subnets configured in the segment for the corresponding site.
 - Nile does not configure gateway options and the customer is expected to configure them as needed.
- VPN credentials
 - Four VPN credentials are configured for every site, with two as primary and the other two as secondary.
- Data path considerations
 - 2 Fan-out tunnels (a bundle) are kept UP against a Public Service Edge IP (primary). Traffic is ECMP load balanced over the bundle of SAs.
 - 2 IKE SAs with distinct local-ids are used to form the bundle of tunnels. IKE config for Secondary is kept cold-standby and SAs are initiated as needed, during a failover.
 - After a failover has happened to the secondary Public Service Edge IP, automatic fail-back when the primary Public Service Edge IP returns is not supported. You can trigger fail-back out-of-band via REST interfaces, if needed from the observability stack.
 - Dead Peer Detection (DPD) probe by Vector Packet Processing (VPP) stack is 3 X 30 seconds: 90+ seconds to declare a tunnel down against a primary.
 - After a tunnel is declared down, Nile re-inits IKE SA at 1 minute boundary (x 3 times) against the same primary Public Service Edge IP to be certain it's not an intermittent network connection issue that caused the tunnel to go down.

If SAs against primary Public Service Edge IP is still down, Nile initiates a fail-over to the secondary Public Service Edge IP and the tunnels return immediately within less than a second.

Appendix E: Requesting Zscaler Support

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

To contact Zscaler Support:

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

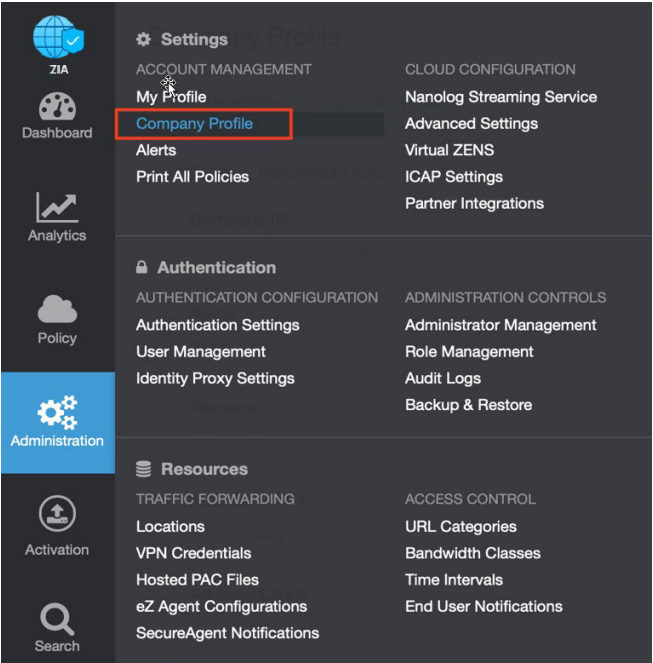


Figure 28. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

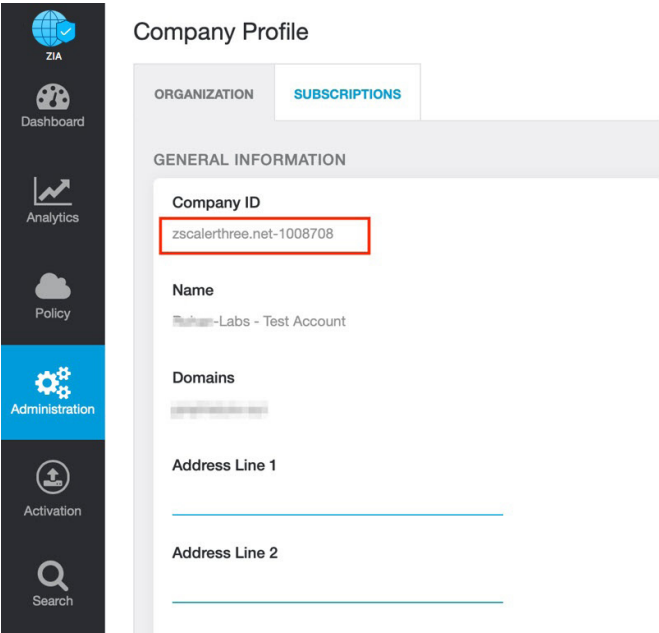


Figure 29. Company ID

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

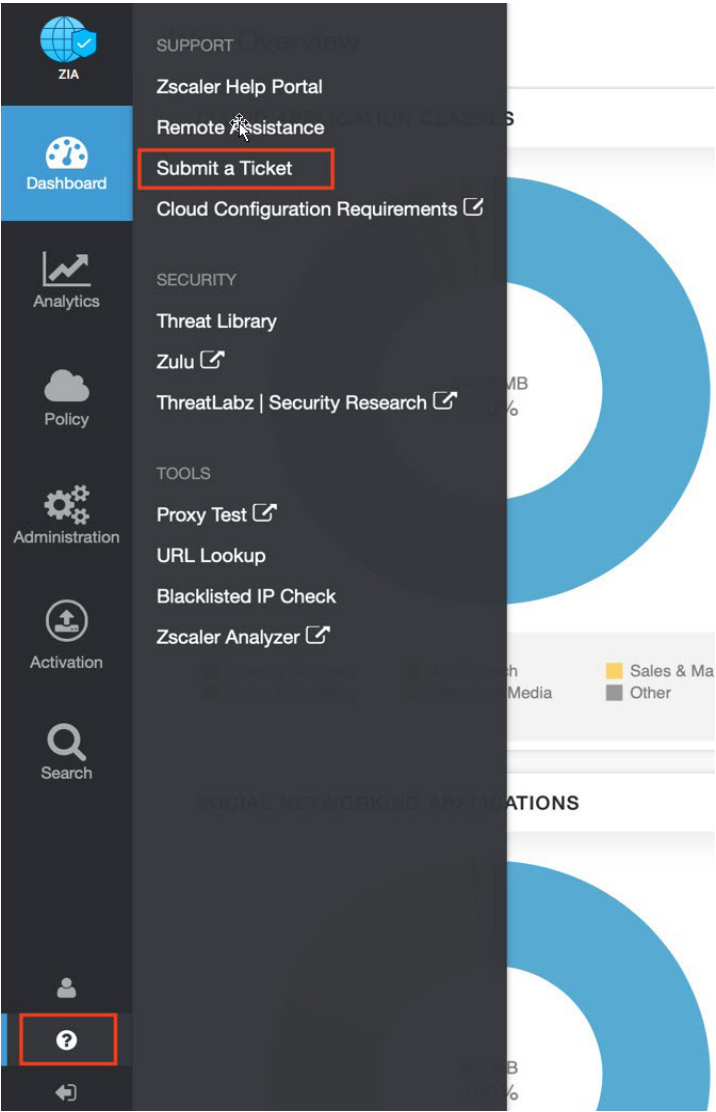


Figure 30. Submit a ticket