ZSCALER AND VERSA DEPLOYMENT GUIDE

NOVEMBER 2025, VERSION 2.0

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)
CPE	Common Platform Enumeration
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
VR	Virtual Router
VRF	Virtual Routing and Forwarding (Versa)
XFF	X-Forwarded-For (RFC7239)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website.

Versa Overview

Versa is unique among SASE vendors, providing an end-to-end solution that both simplifies and secures the modern network. Versa SASE, based on VOS, delivers a broad set of capabilities via the cloud and on-premises for building agile and secure enterprise networks, as well as highly efficient managed service offerings.

To learn more, refer to www.versa-networks.com.

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
- Versa 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 Versa Introduction

Overviews of the Zscaler and Versa 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.

Versa Secure SD-WAN Overview

Versa Secure SD-WAN is a comprehensive networking solution that provides end-to-end visibility, control, and security for your enterprise's digital transformation. It integrates software-defined networking and advanced security services into a single, unified platform.

It empowers businesses to scale their networks seamlessly, manage complexity, and optimize performance while ensuring robust security. Whether it's connecting remote branches, enhancing user experience, or securing sensitive data, Versa Secure SD-WAN offers a flexible and agile approach to network management and security.

Versa Resources

The following table contains links to Versa support resources.

Name	Definition
Versa Secure SD-WAN	Versa Secure SD-WAN is a cloud-delivered platform that unifies networking and security to provide reliable, secure, and simplified connectivity across branches, data centers, and multi-cloud environments.
Versa Support	Versa provides global 24x7 Standard Support as well as Premier Support services.
Versa Secure SD-WAN Documentation	Documentation on Versa SD-WAN's platform.

Overview

This document details configuring automated IPSec tunnel provisioning from the Versa Director to ZIA. Versa Operating System (VOS) devices integrate with Zscaler using a site-to-site IPSec VPN tunnel from the CPE to a Zscaler Public Service Edge. Versa Director provides workflow-based automation to configure IPSec tunnels from Versa SD-WAN CPEs to ZIA using the Zscaler API. You use template-based workflows to create the following tunnels and location:

- Two or more tunnels to primary and secondary Zscaler servers from each CPE for data forwarding.
- Location for each CPE.

Versa Director supports IPSec tunneling between the CPE to Zscaler servers. For multiple LAN VRs configured on the CPE, you can choose one or more VRs from which traffic is forwarded to Zscaler servers. For each internet link, a primary tunnel is created to the primary Public Service Edge server and a backup tunnel is created to the secondary Public Service Edge server.

Secure SD-WAN Topology

Versa Networks VOS interoperability with Zscaler uses a site-to-site IPSec VPN tunnel that allows VOS branch devices to direct traffic to a Zscaler local service node. Versa Secure SD-WAN devices forward internet- bound traffic to Zscaler's cloud security platform to ensure that all web traffic is secured.

The Zscaler peer type supports WAN and LAN networks as originating endpoints of the tunnel. For Zscaler peer type, you must provision primary and secondary tunnels from each CPE to the primary and secondary Public Service Edge servers for redundancy. For the virtual routing instance, you select a VPN profile to associate with the tunnel and with the LAN Virtual Routing and Forwarding (VRF) organization.

The following diagram illustrates the integration topology between Versa Active/Active SD-WAN devices and Zscaler primary and secondary servers.

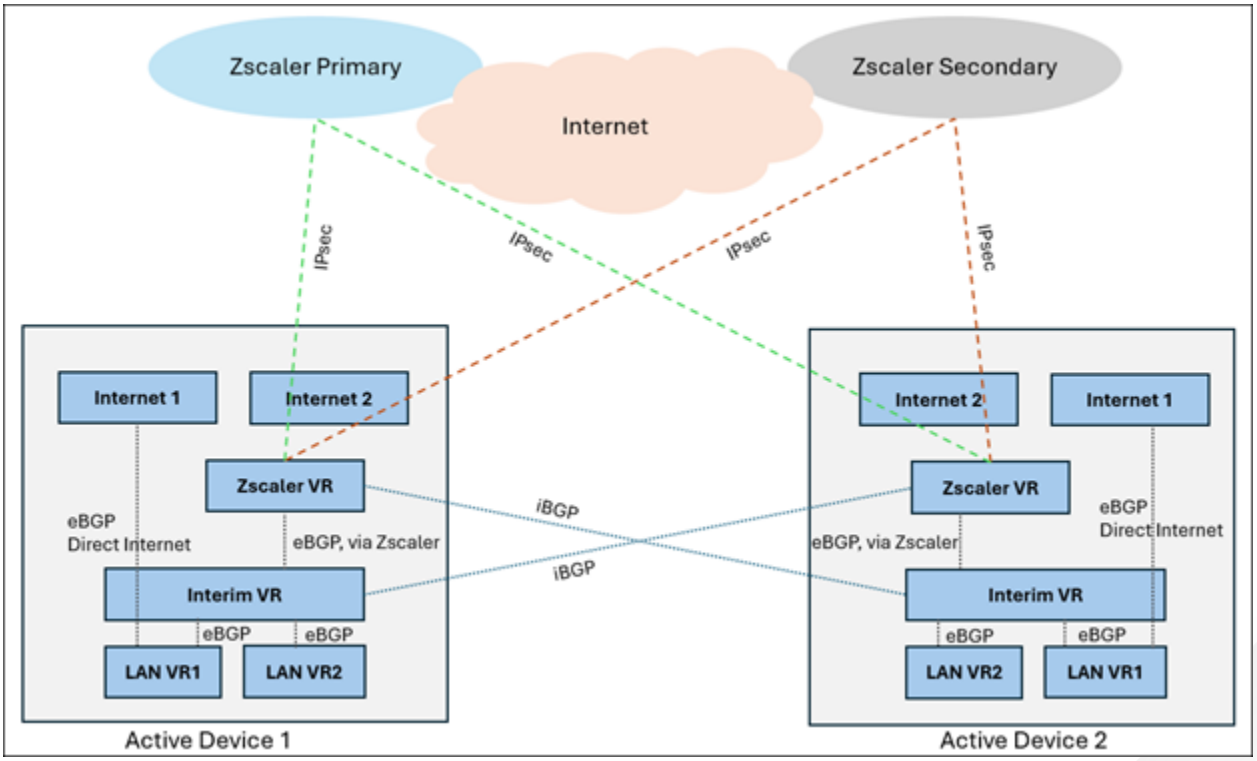

Figure 1. Zscaler and Versa architecture

The LAN VR1 and LAN VR2 are VRF instances and the Interim VR is used as a transit VRF which aggregates traffic from the LAN VRFs before forwarding it to Zscaler. Traffic originating from LAN VRFs is routed to the Interim VR and from the Interim VR, routing policies forward the traffic to the Zscaler VR. The Zscaler VR then sends the traffic through the established IPSec tunnels to either the Zscaler Primary or Zscaler Secondary server.

The Zscaler VRs have another cross-connect interface which are mapped to the Active-Active tunnels. The Active/Active setup ensures that if one device fails, the other device can forward traffic without any connectivity issues. To route the traffic to Zscaler Border Gateway Protocol (BGP) protocol is used internally on VOS. Zscaler only supports static next-hop routing from CPE devices.

Configuring ZIA

In this section, first configure the Zscaler side before configuring Versa SD-WAN.

Logging In to ZIA

Log in to Zscaler using your administrator account. If you are unable to log in using your administrator account, contact Zscaler Support.

Figure 2. Log in to Zscaler

Configure ZIA for API Access

Enable ZIA for API access by creating an SD-WAN partner key. The partner key is an API key that is used as one form of authentication. The second form of authentication is the admin partner username and password (covered later in this deployment guide). You can only use this admin credential for API calls.

Go to **Administration** > **Cloud Configuration** > **Partner Integrations**.

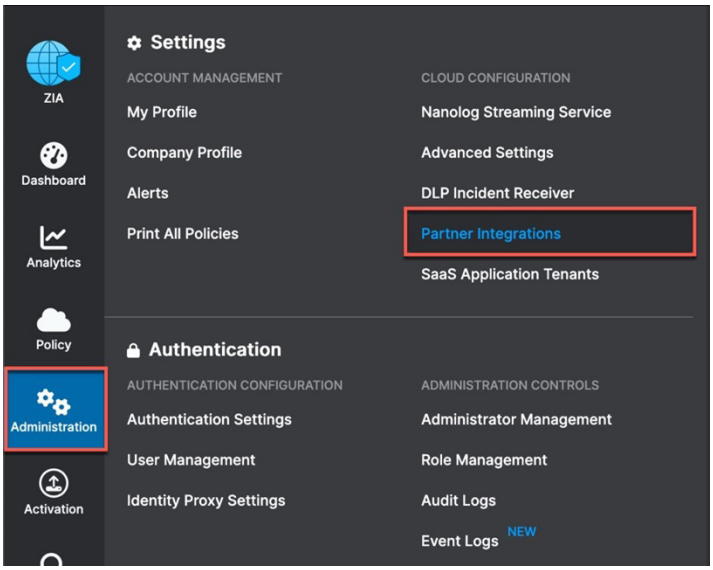

Figure 3. Configuring ZIA for API access

Adding SD-WAN Partner Key

In the ZIA Admin Portal:

1. Go to **Partner Integrations** > **SD-WAN** > **Add Partner Key**. The **Add Partner Key** dialog appears.

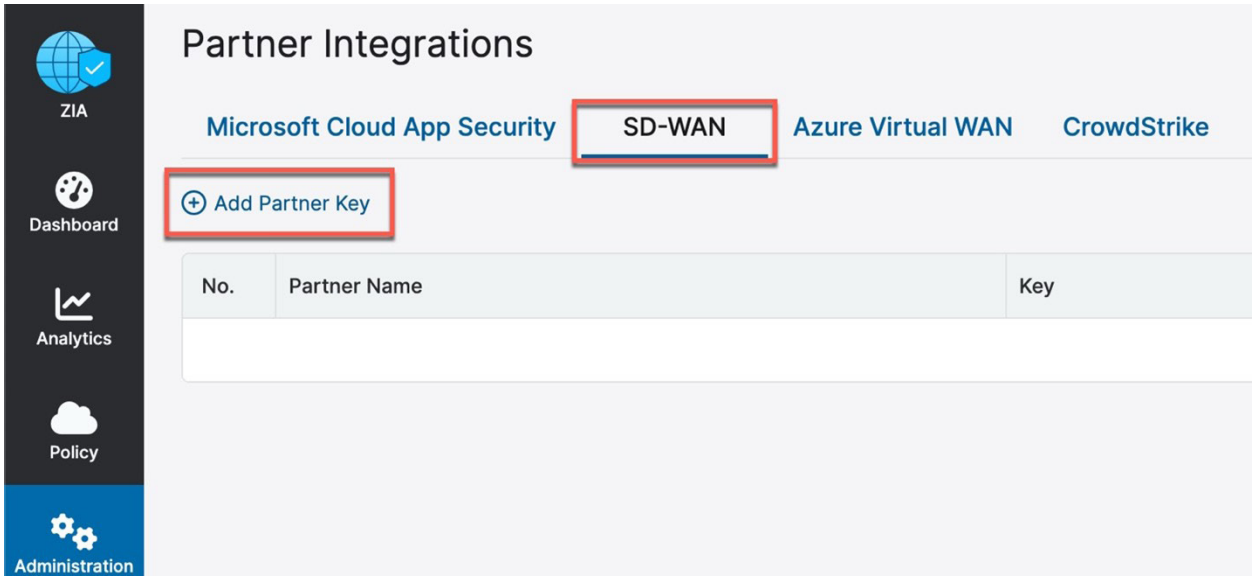

Figure 4. Add partner key

2. Enter or select from the drop-down menu the SD-WAN vendor for which you want to create a partner key.
3. After typing or selecting **Versa SD-WAN**, click **Generate**. You are returned to the prior page.

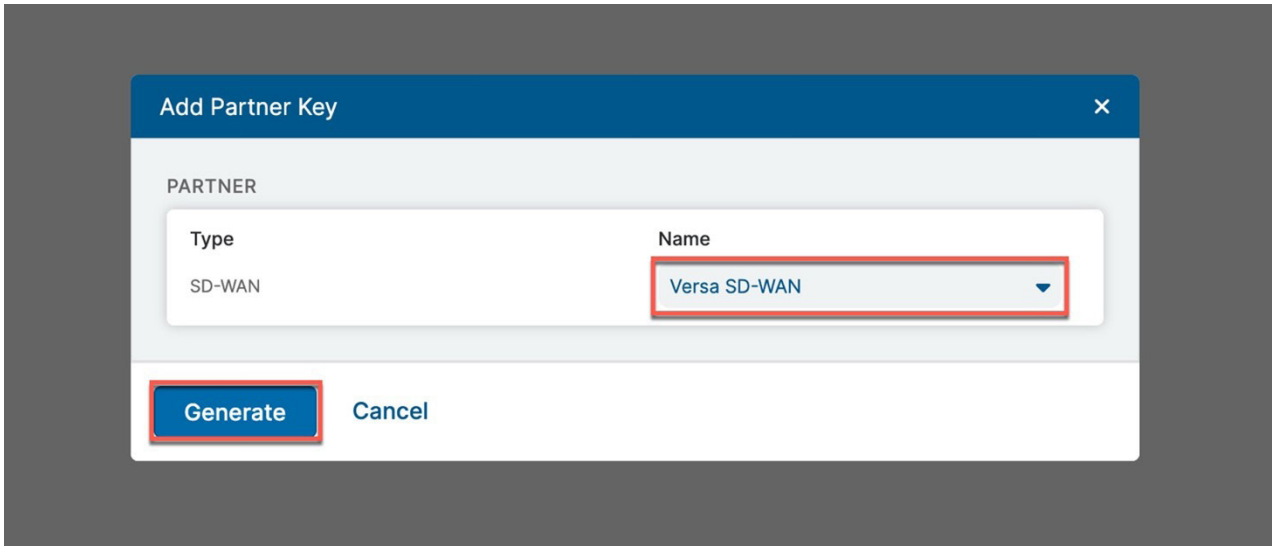

Figure 5. Add SD-WAN partner key

Verify SD-WAN Partner Key

After you return to the page, you see the partner key you created for Versa SD-WAN.

The key is not obfuscated as in the figure. The password is hidden for the purpose of this document.

You also see a red circle, with a number, above the Activation icon in the left-hand navigation. The configuration change that activates the partner key is pending. You must activate this change before the partner key is usable.

The key value is required for the procedure described in New Cloud Security Provider for Automated Deployment. Make sure to note the key value to enter it in the Versa Director later.

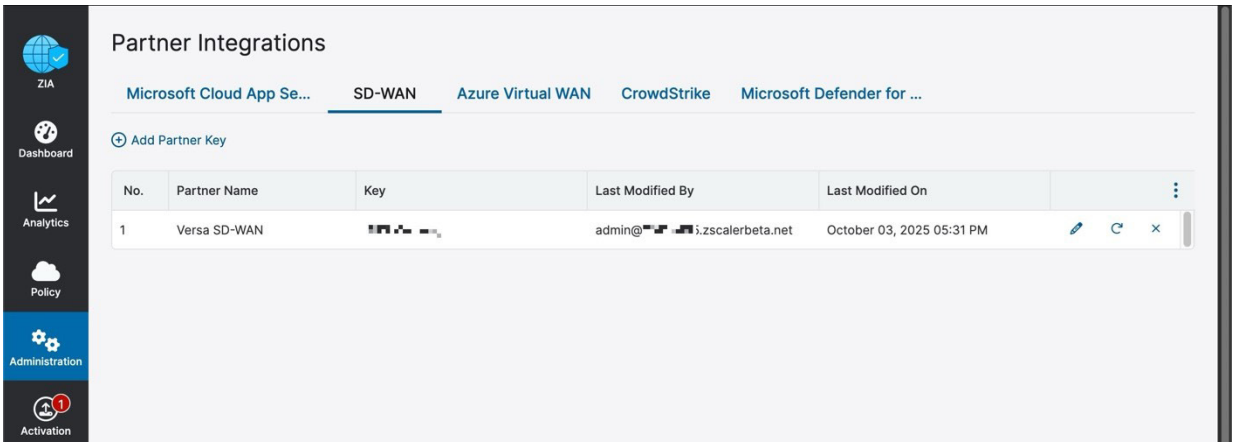

Figure 6. Verify SD-WAN partner key

Adding an SD-WAN Partner API Role

Next, you must create an SD-WAN Partner API Role. This administrator is authenticated against the Zscaler ZIA provisioning API.

In the ZIA Admin Portal:

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

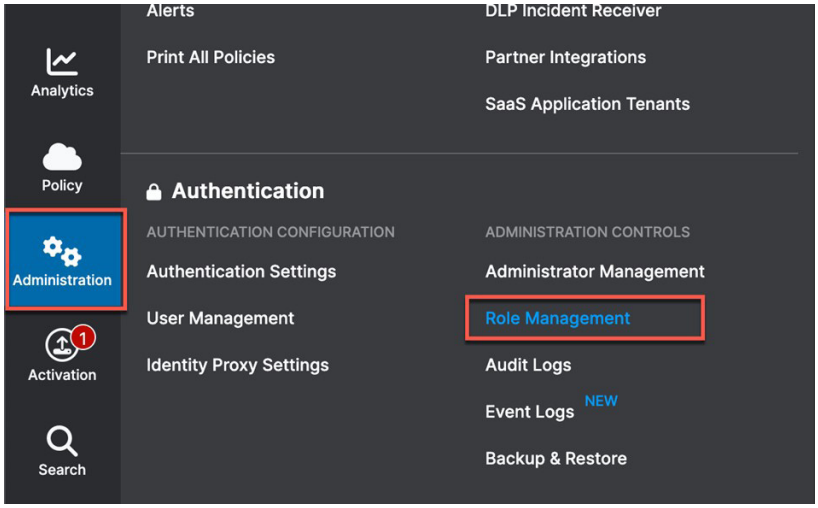

Figure 7. Adding SD-WAN Partner API Role

2. Click the **Add SD-WAN Partner API Role** option to display the **Add SD-WAN Partner API Role** dialog.

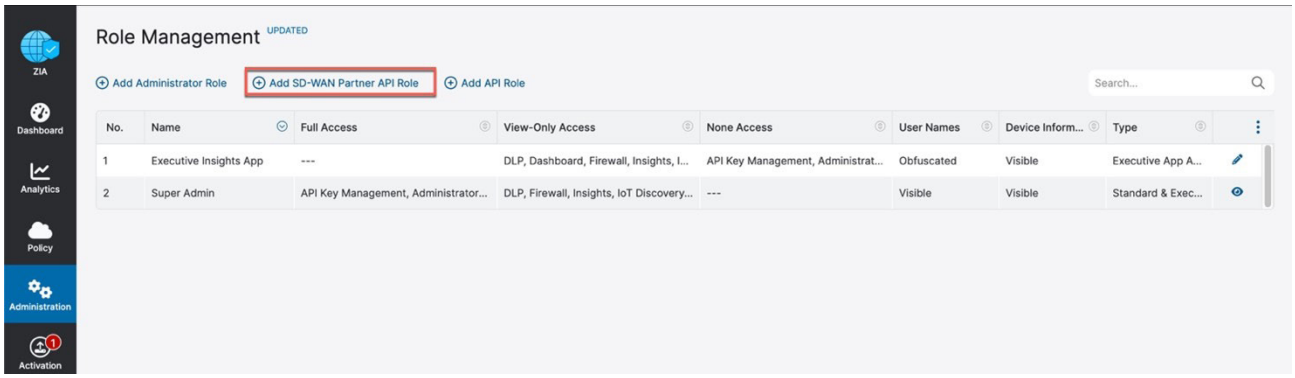

Figure 8. Add SD-WAN Partner API Role

An SD-WAN Partner API Role lets you define the permission and access granted to third-party partners (such as an SD-WAN partner).

3. After you name the SD-WAN Partner API Role, change the **Access Control** to **Full**. The **Full** toggle allows partner admins to view and edit VPN credentials and locations that Versa Director is managing via the ZIA provisioning API. This is necessary for the Versa Director to be able to create new VPN credentials and locations for branch locations.
4. Click **Save**. You are returned to the prior page.

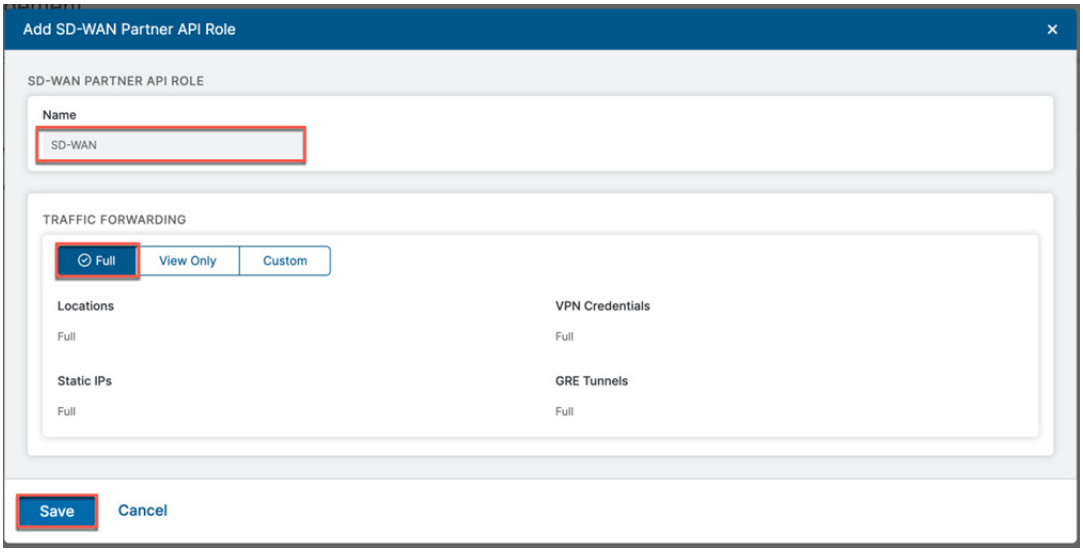

Figure 9. Creating SD-WAN Partner API Role

Administrator Management

The final step is creating an SD-WAN Partner API Client. In the ZIA Admin Portal:

1. Go to **Administration** > **Administration Controls** > **Administrator Management**.

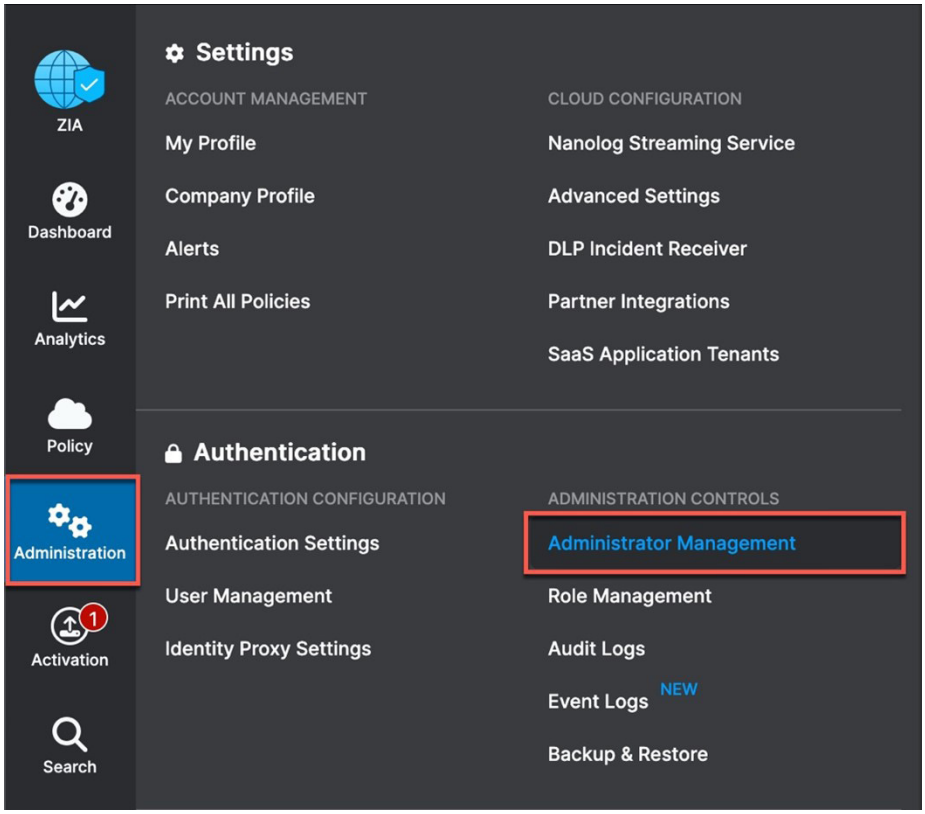

Figure 10. Administrator management

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

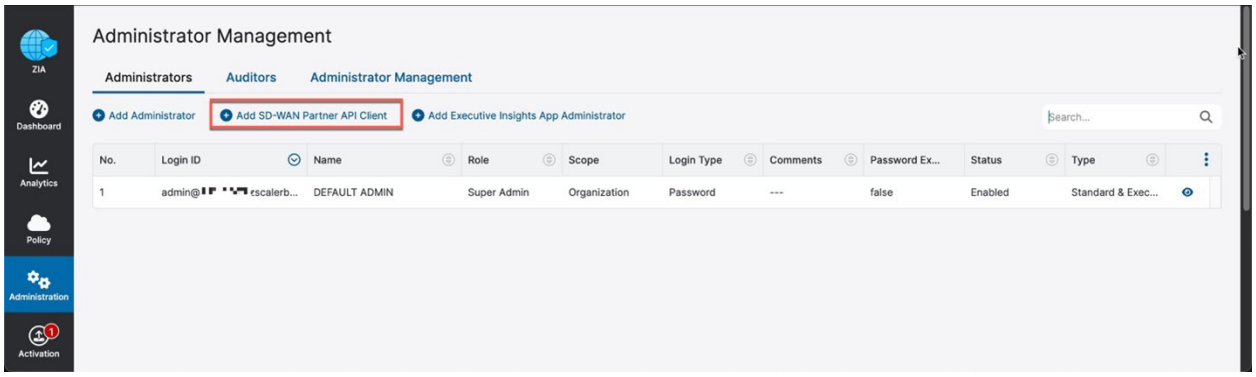

Figure 11. Admin SD-WAN Partner API Client

Save and copy the Login ID and Password so you can enter them in Versa Director.

3. Enter the information in the **Add SD-WAN Partner API Client** window and click **Save**.

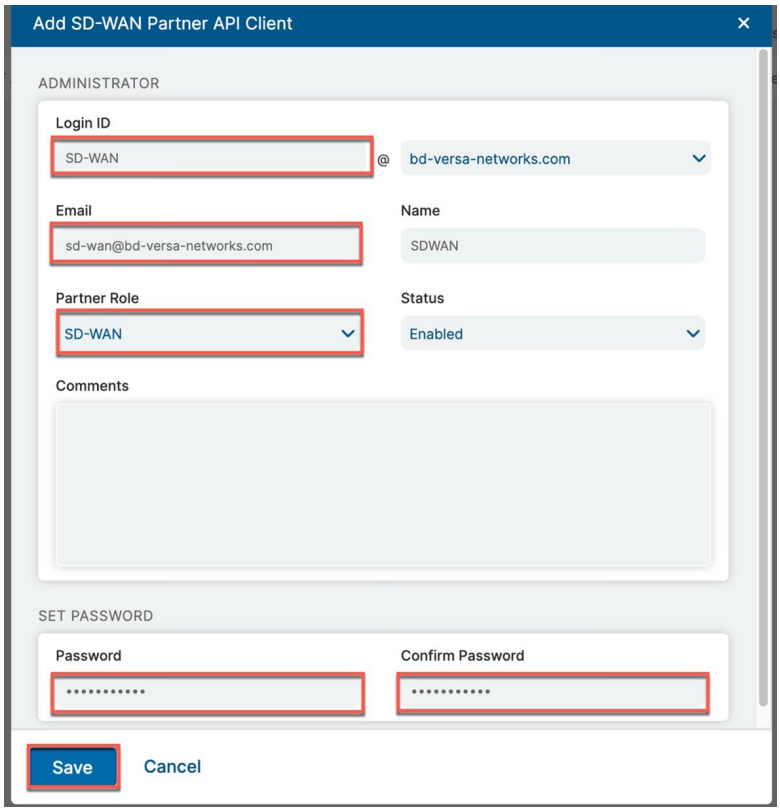

Figure 12. Creating SD-WAN Partner API Client

4. Activate the changes by going to **Activation** and clicking **Activate**.

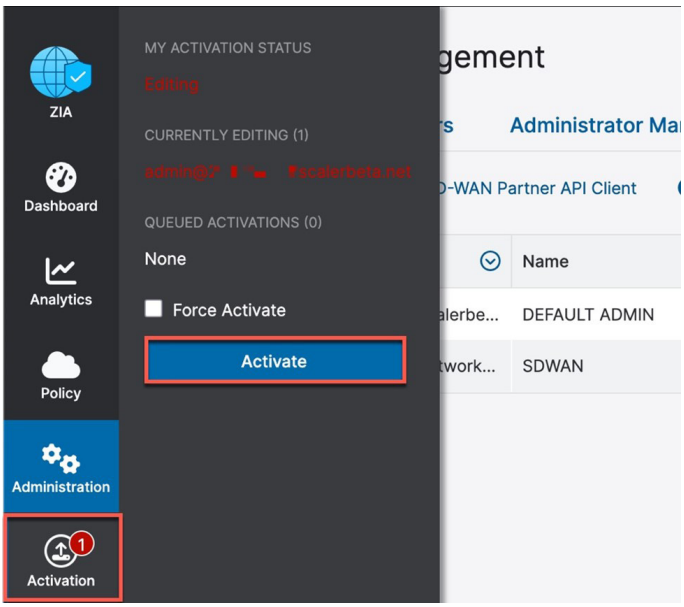

Figure 13. Activate pending changes

Verify Activation

After activating pending changes, you are returned to the prior page, and **Activation Completed** appears at the top of the window.

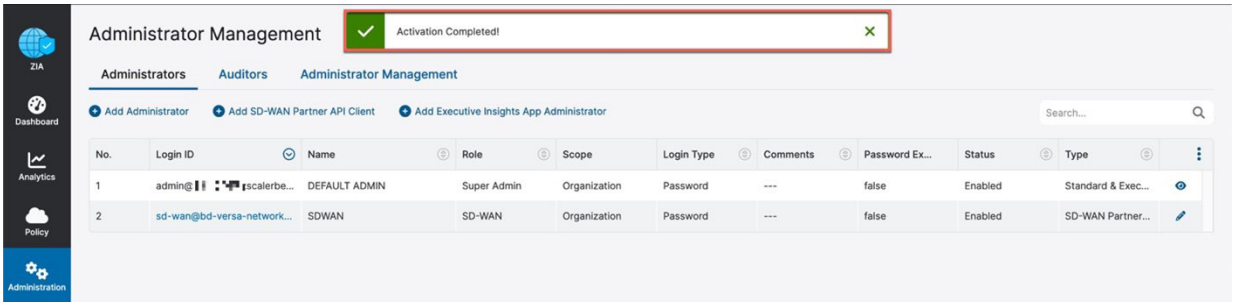

Figure 14. Verify activation

Configuring Versa Director

The following sections describe configuring Versa Director.

Create a CMS Cloud Connector in Versa Director

To establish a connection between a VOS device and Zscaler, and manage that connection through Versa Director, you must first configure a cloud management system (CMS) connector on Versa Director.

You can create only one CMS connector per tenant for Zscaler integration.

When you create the CMS cloud connector on Versa Director, you need the following information:

- Zscaler username and password that you configured in Administrator Management
- Cloud name and API key that you gathered in Adding SD-WAN Partner Key.

To create a CMS cloud connector in Versa Director:

1. Log in to Versa Director.
2. In **Director** view, select the **Administration** tab in the top menu bar.
3. Select **Connectors** > **CMS** in the left menu bar. The **CMS connectors** table is displayed.
4. Click the **Add** icon.

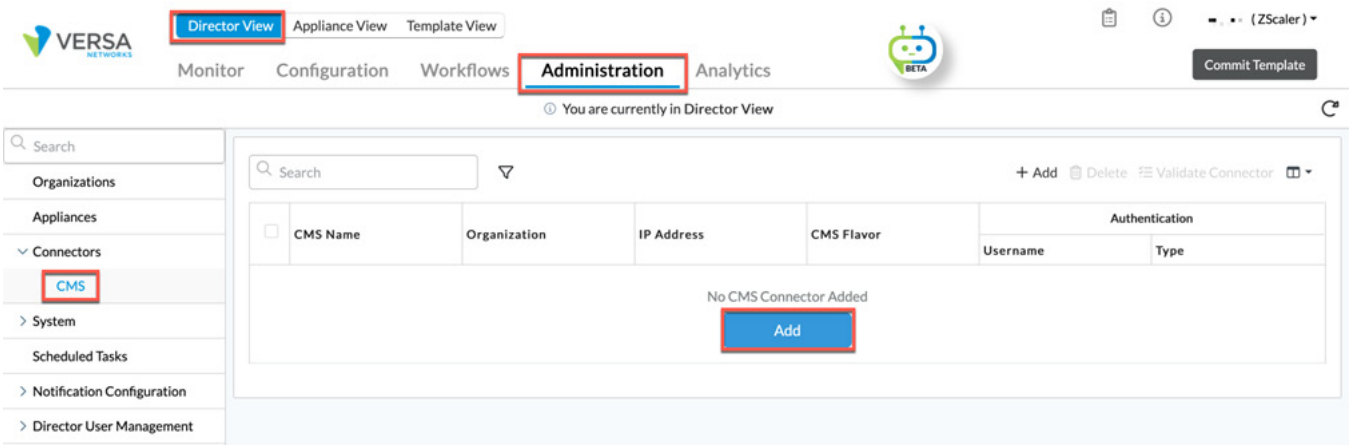

Figure 15. Configure CMS Connector

5. In the **Add CMS Connector** window, enter information for the following fields.
   a. **CMS Name**: (Required) Enter the name of the CMS connector. The name is a text string.
   b. **Organization**: (Required) Select an organization for the CMS connector.
   c. **CMS Flavor**: Select **Zscaler** for the type of cloud device.
   d. **Zscaler Username**: (Required) Enter the username of the Zscaler administrator account.
   e. **Zscaler Cloud Name**: (Required) Enter the Zscaler cloud name (i.e., `zscalerbeta`).
   f. **Zscaler API Key**: (Required) Enter the integration API key to access the Zscaler API.
   g. **Zscaler Password**: (Required) Enter the password of the Zscaler administrator account.

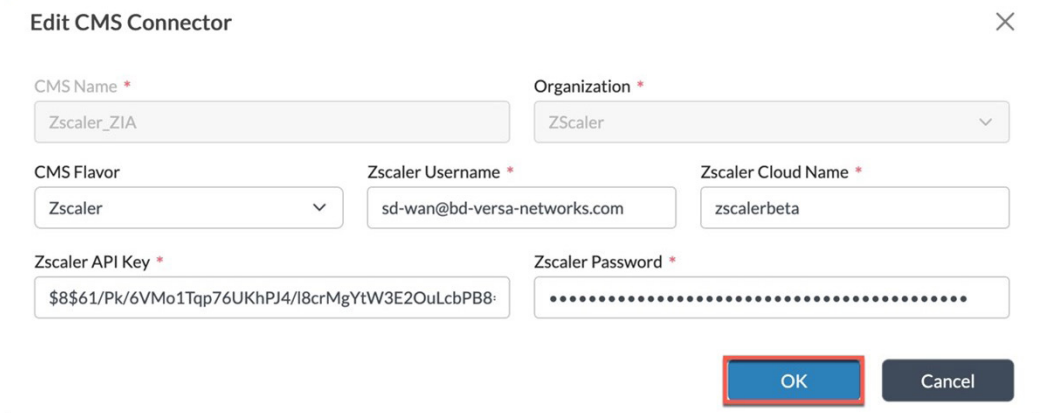

Figure 16. Populate ZIA API fields

Validate the CMS configuration

Next, ensure the entered data is correct and the Versa Director can connect to the ZIA API service.

Select the checkbox next to the previously created connector and then click the **Validate Connector** selection on the top right of the window:

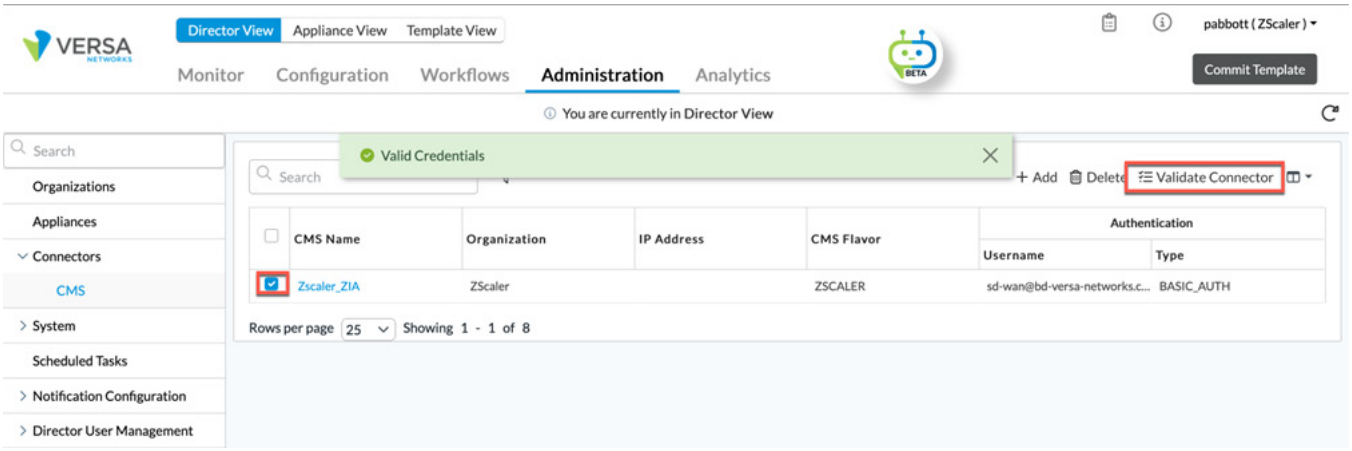

Figure 17. CMS Validation

A green popup indicates a successful API connection to the ZIA platform.

Configure a Site-to-Site Tunnel in a Workflow Template for Zscaler

To configure a site-to-site tunnel:

1. In **Director** view, select the **Workflows** tab in the top menu bar.
2. Select **Template** > **Templates** in the horizontal menu bar.
3. Select an SD-WAN post-staging template in the main pane. To create a new workflow template, see the [Versa documentation].

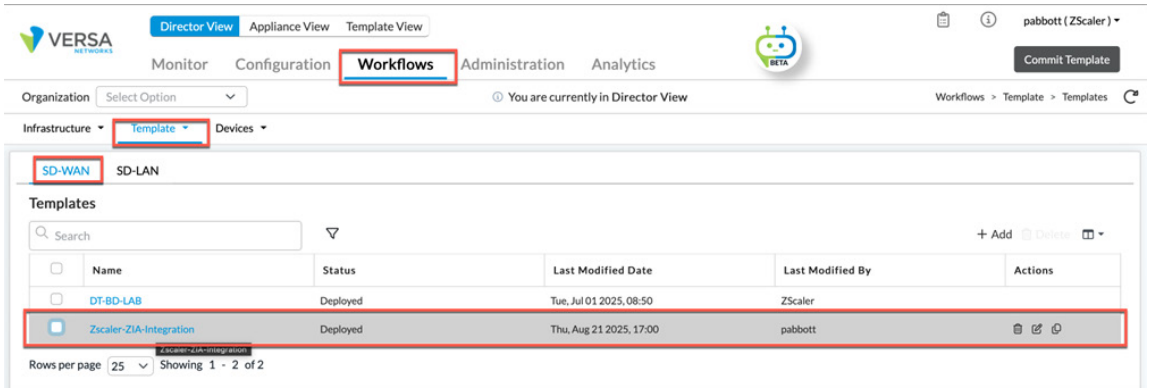

Figure 18. Configuring the SD-WAN Workflow Template

4. Click **Tunnels**. In the **Partner Site-to-Site Tunnels** section, click the **+ Add** icon.

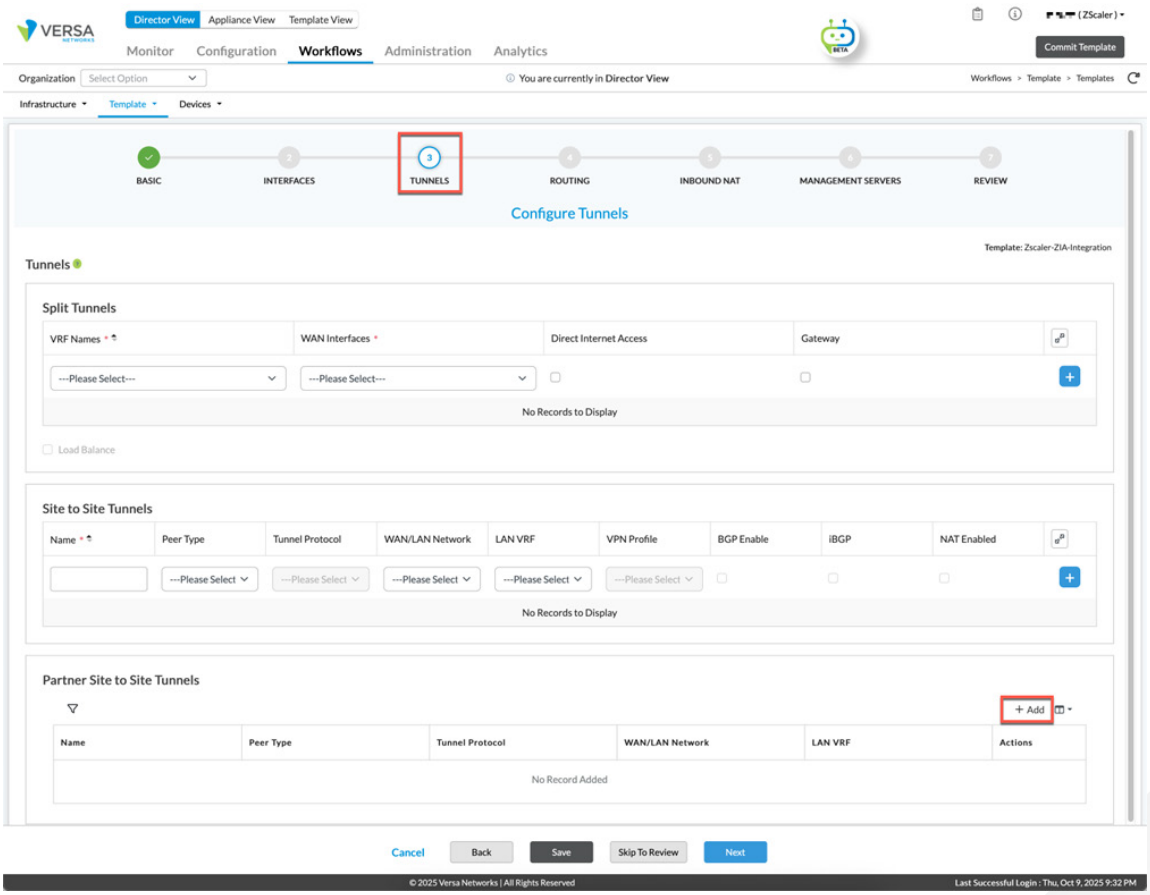

Figure 19. Site-to-Site Tunnels

5. In the **Partner Site-to-Site Tunnels** popup window, enter information for the following fields:
   a. **Name**: (Required) Enter a name for the site-to-site tunnel.
   b. **Peer Type**: Select the Zscaler peer type.
   c. **Tunnel Protocol**: Select the IPSec tunnel protocol to use to reach the peer.
   d. **WAN Network**: Select one or more WAN networks to use. This network is the originating endpoint of the tunnel. The highest priority is 1.
   e. **Organization**: Select the organization for which the site-to-site tunnel is created.
   f. **LAN VRF**: Select one or more virtual routing instances to use to reach the LAN.

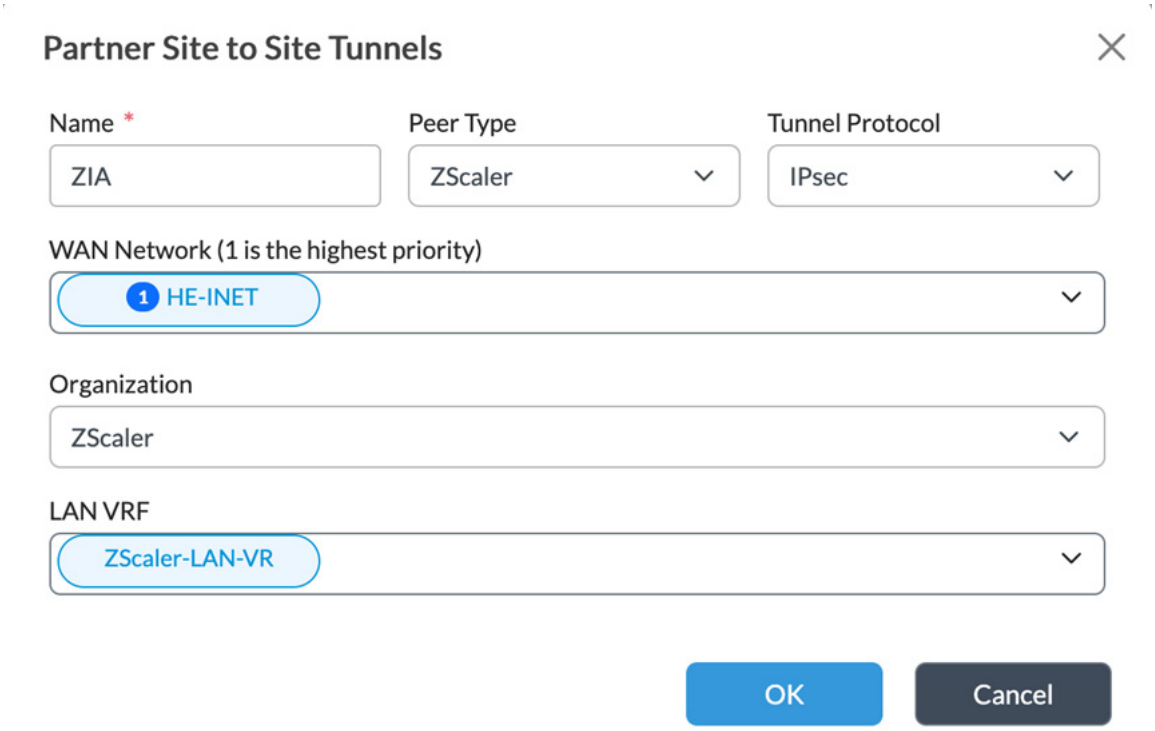

Figure 20. Configuring the tunnels to ZIA

6. Click **OK**, and then click **Save**.
7. If modifying an existing device:
   a. Click **Review**, and then click **Re-Deploy**.
   b. Commit the template.

Configure a Site-to-Site Tunnel in a Device Workflow for Zscaler

Apply the Workflow to a Device. To configure a Versa Director–Zscaler IPSec site-to-site tunnel for a device:

1. In **Director** view, select the **Workflows** tab in the top menu bar.
2. Select **Devices** > **Devices** in the left menu bar.
3. Select a device in the main pane.

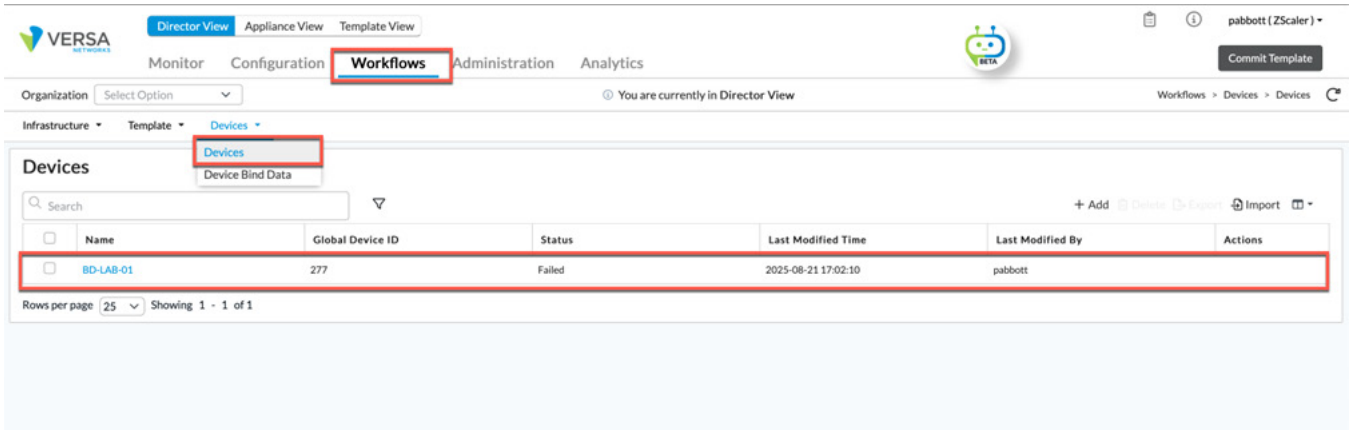

Figure 21. Configuring the Device Template

4. Click **Tunnel Information**. Select a tunnel name, and then click the **Add** icon. The tunnel displays in the Zscaler tunnels list. Note that you cannot configure a public IP address for tunnels created using an IPSec tunnel protocol. To create a new device workflow, see the Versa documentation.

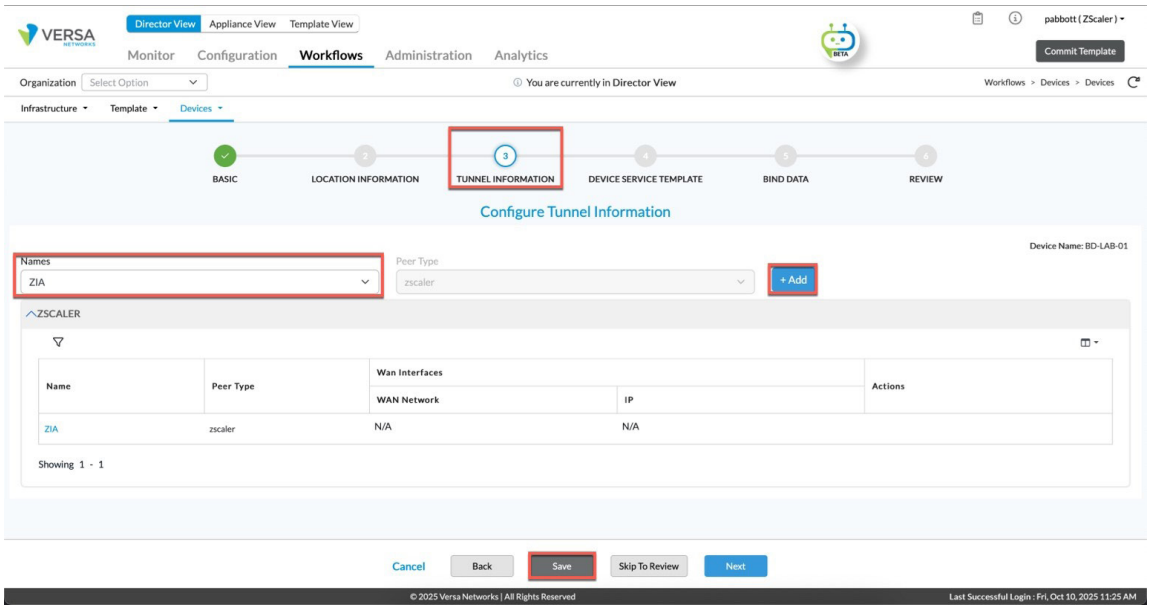

Figure 22. Assigning the ZIA Tunnel configuration to the device

5. Click **Save**.
6. If modifying an existing device:
   a. Click **Review**, and then click **Deploy**.
   b. Commit the Template.

Verify IPSec Tunnel Services

To verify IPSec tunnel services for a site-to-site tunnel:

1. In **Director** view:
   a. Select the **Monitor** tab in the top menu bar.
   b. Select **Devices** in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to **Appliance View**.

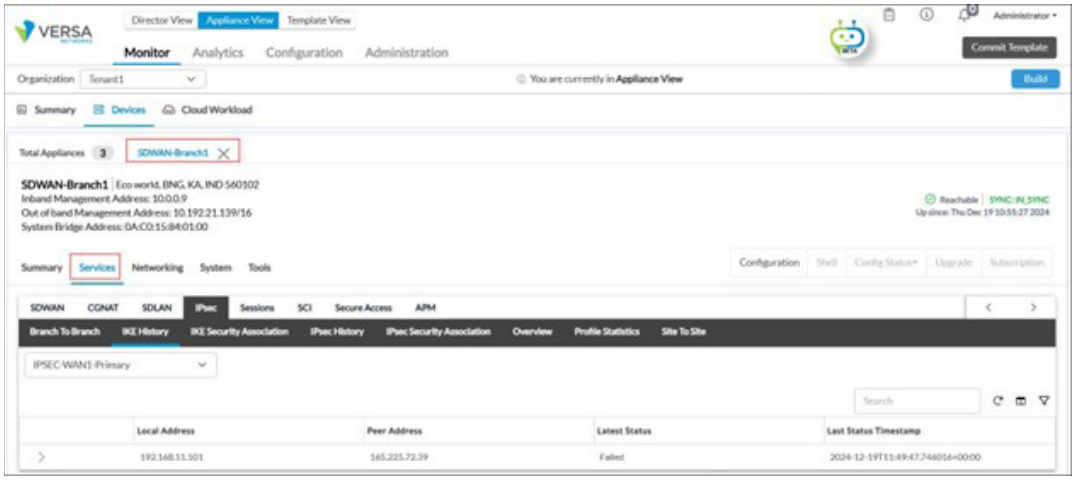

Figure 23. Monitoring IPSec

2. Select **Services** > **IPSec** in the horizontal device menu bar.
3. On the **IPSec** tab, select **IKE History**, and then select an IPSec tunnel. Click an entity to view the IKE history.

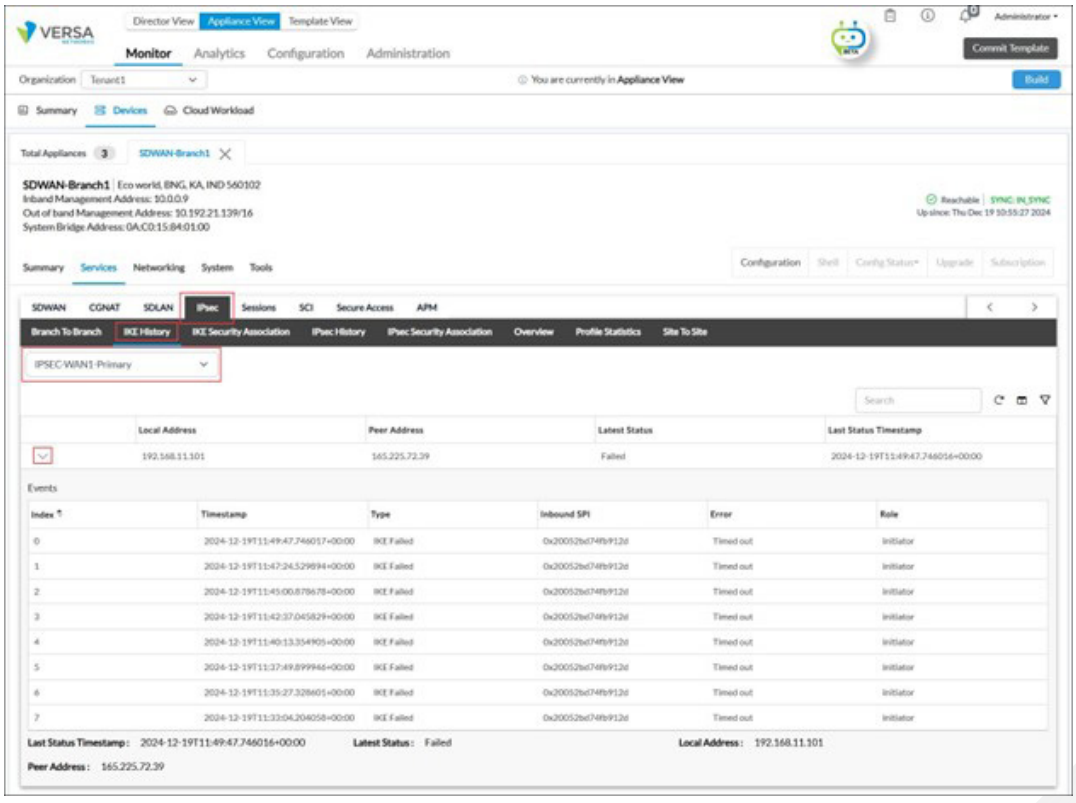

Figure 24. Selecting the ZIA tunnel

4. Select IKE Security Association, and then select an IPSec tunnel. Click an entity to view the IKE security details.

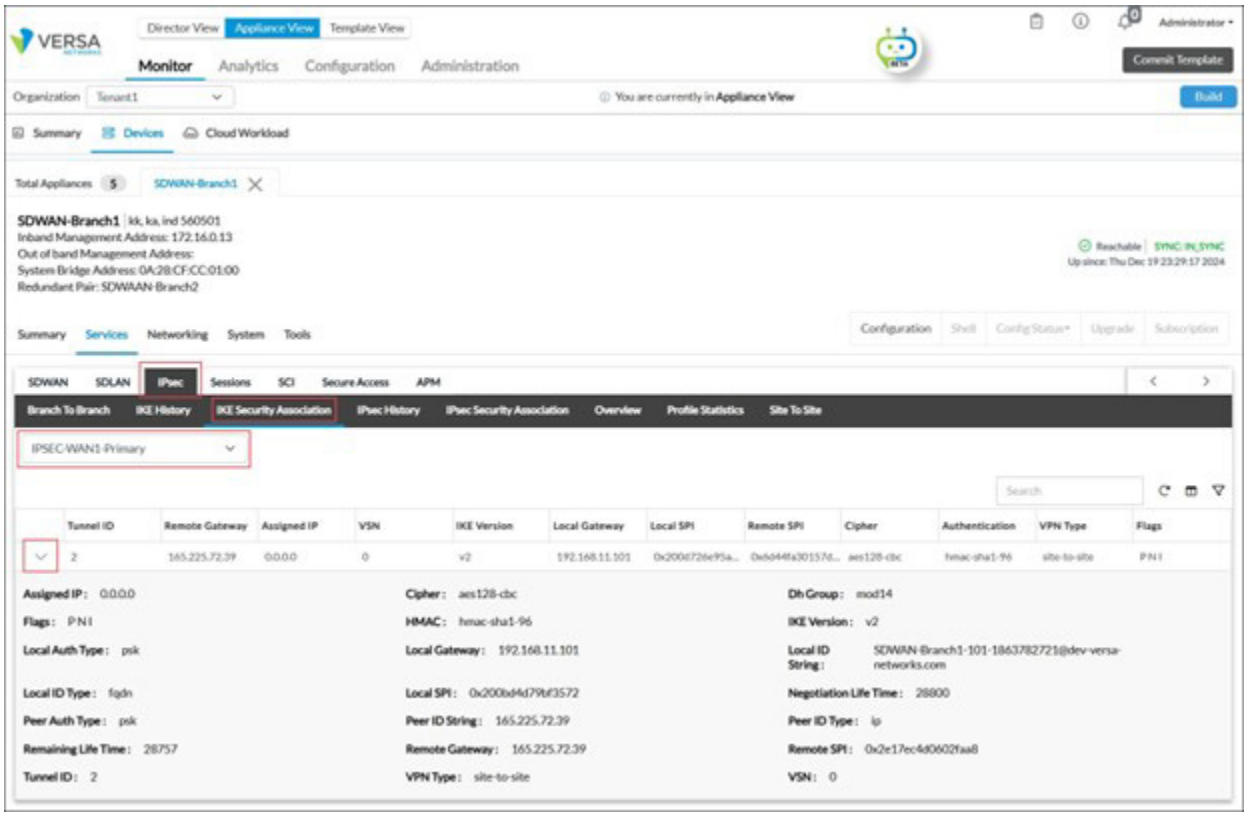

Figure 25. Viewing the ZIA tunnel state

Verify IPSec Tunnel Information from Zscaler

To verify IPSec tunnel information from Zscaler:

1. Log in to the ZIA Admin Portal.
2. Click **Analytics** > **Tunnel Insights**.

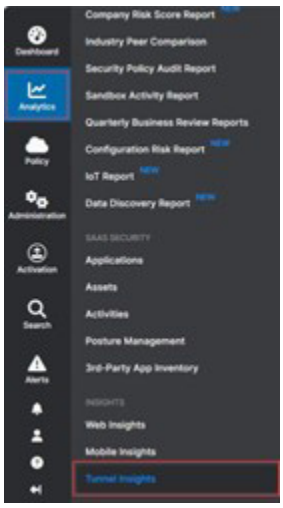

Figure 26. Navigate to Tunnel Insights

3. Select the **Insights** tab. To view the tunnel information, define the tunnel data type and filters and then click **Apply Filters**. You can select different data types to view from the drop-down menu above the chart.

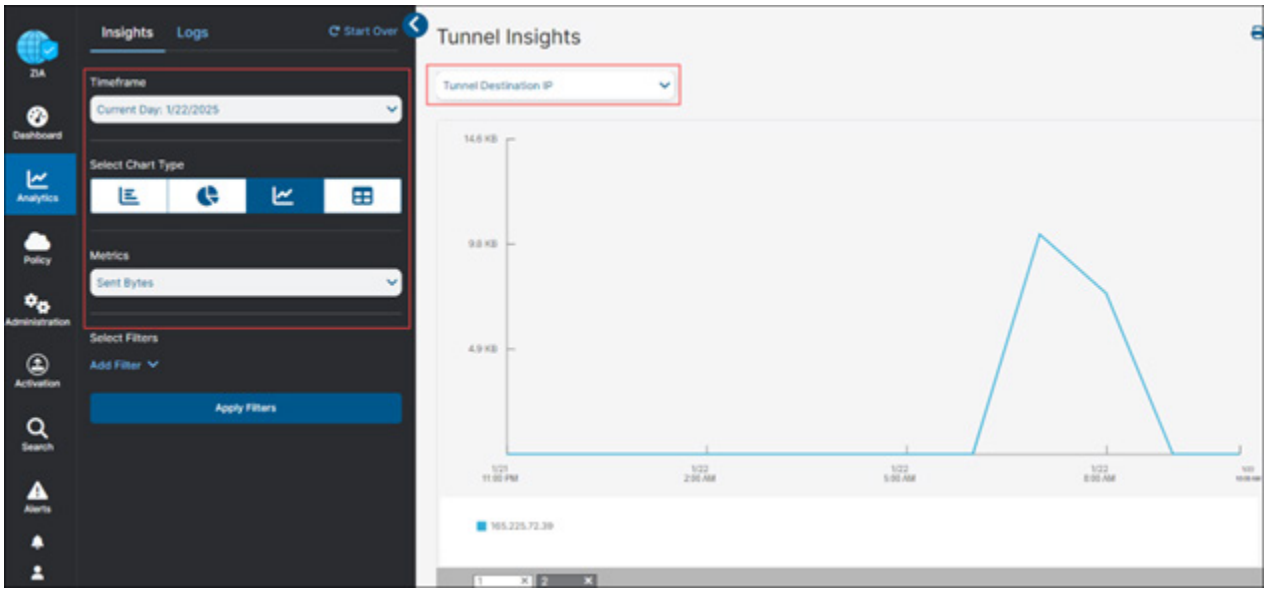

Figure 27. Viewing Tunnel Traffic Volume

4. Select the **Logs** tab. To view the tunnel logs, define the filters and then click **Apply Filters**.

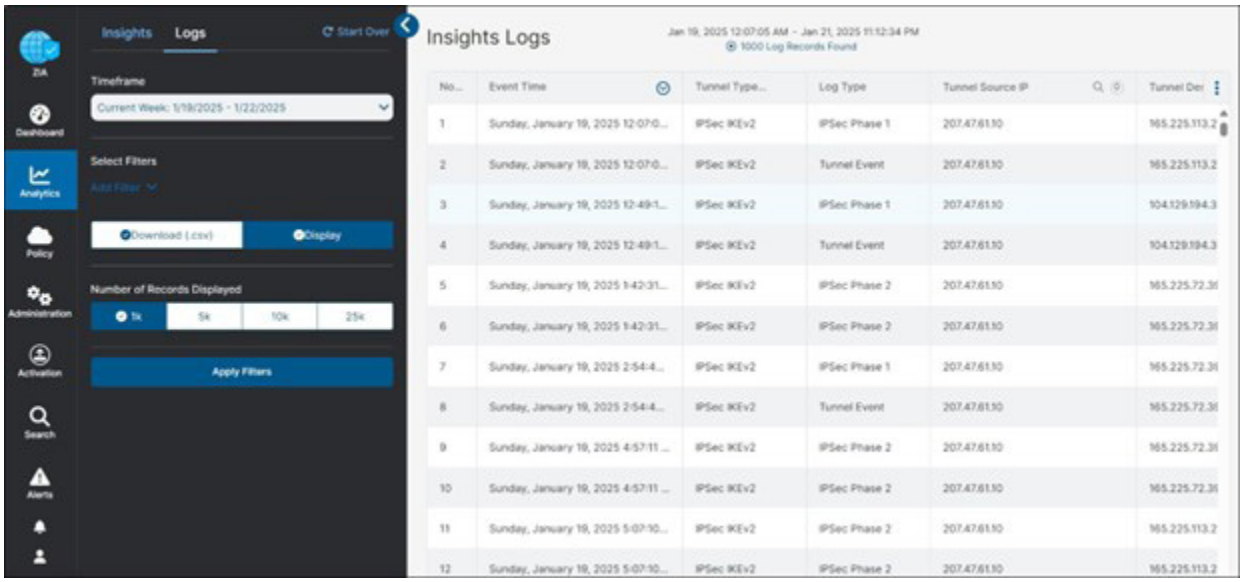

Figure 28. Viewing Tunnel Logs

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support:

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

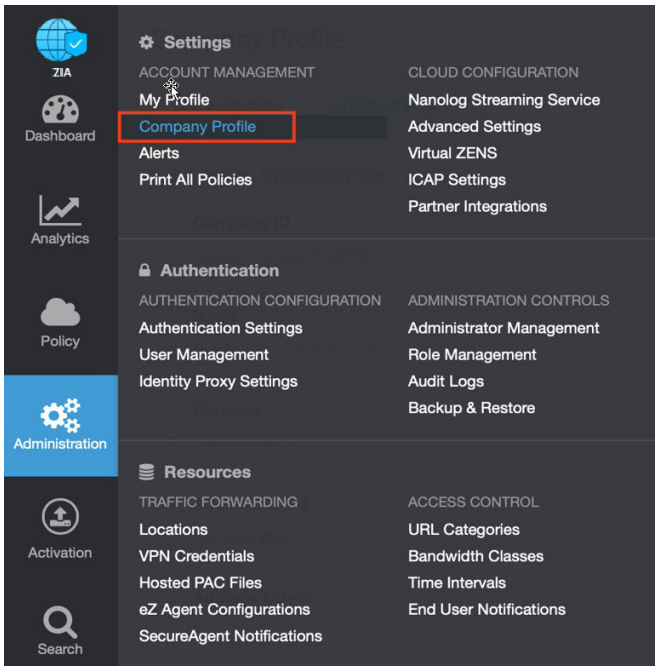

Figure 29. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

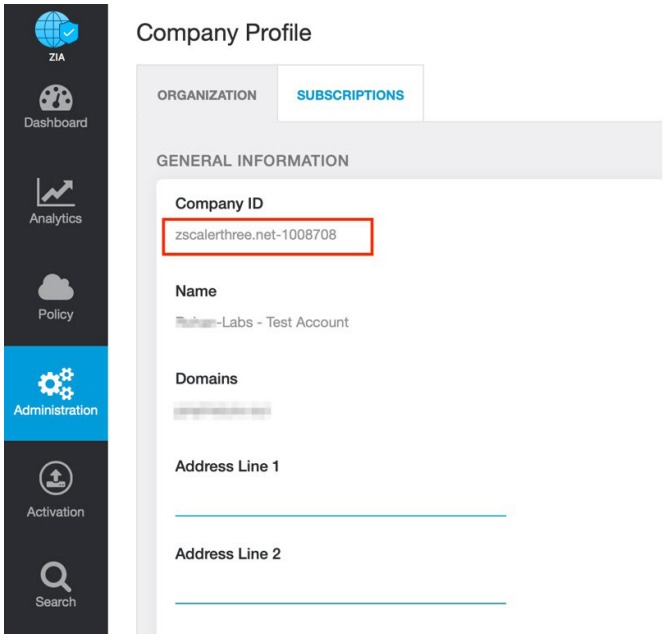

Figure 30. Company ID

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

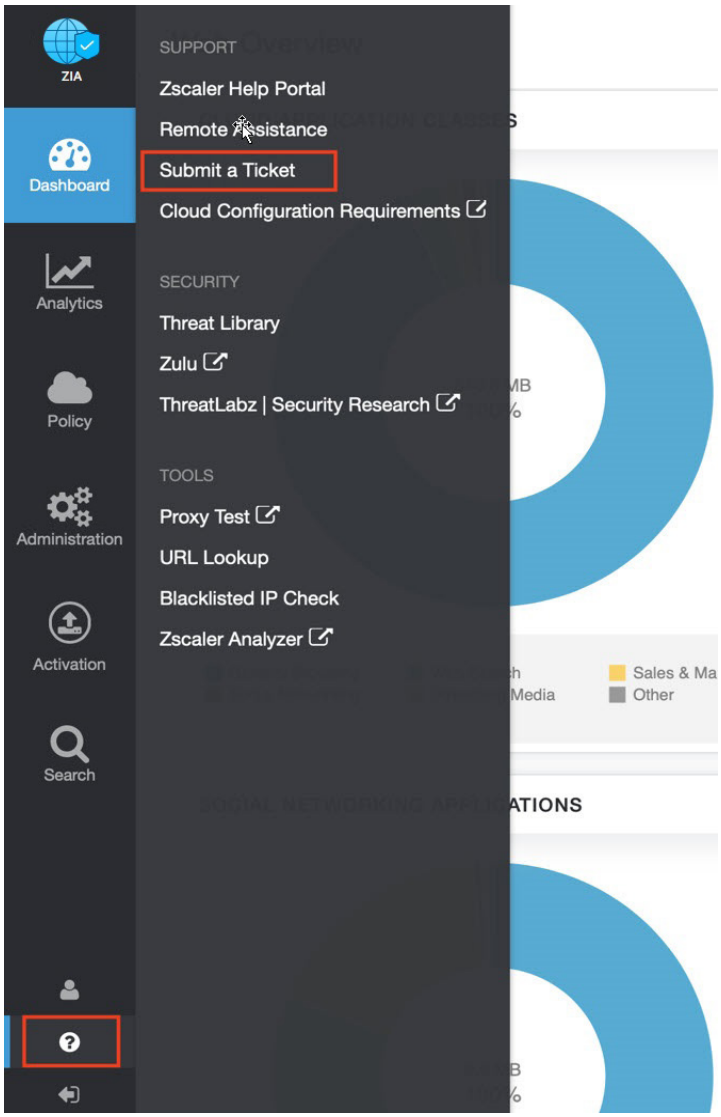

Figure 31. Submit a ticket

