zscaler™ | aruba a Hewlett Packard Enterprise company | silver peak®

ZSCALER AND ARUBA EDGECONNECT (SILVER PEAK) DEPLOYMENT GUIDE

FEBRUARY 2023, VERSION 5.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following terms and acronyms are used in this document. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
OAM	Operation, Administration, and Management
PFS	Perfect Forward Secrecy
SD-WAN	Software Defined Wide Area Network
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security (RFC5246)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

This document provides information on how to configure Zscaler and Aruba EdgeConnect (formerly Silver Peak) for deployment.

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. Flagship offerings Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) 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 the Zscaler website.

Aruba Overview

With more than 2,000 production deployments, customers have identified four unique areas of business value that showcase why they've chosen the Aruba EdgeConnect unified SD-WAN platform. The platform enables customers to build a unified WAN edge that is business-driven, delivers the highest quality of experience, and continuously adapts to changing business needs and network conditions. It is designed to enable enterprises to fully realize the transformational promise of the cloud. To learn more, refer to the Aruba SD-WAN product page.

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
- Aruba Resources
- Appendix E: Requesting Zscaler Support

Software Versions

This document was written using:

- Zscaler Internet Access v6.1
- Aruba Orchestrator v9.1.4.40142
- Aruba EdgeConnect Enterprise ECOS v9.1.1.3_91743

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 AWS Introduction

The following sections detail the Zscaler and partner products and services described in this guide.

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 it as a secure internet onramp—all you do is 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.

Aruba EdgeConnect Overview

The Aruba EdgeConnect SD-WAN edge platform enables enterprises to dramatically reduce the cost and complexity of building a WAN by leveraging broadband to connect users to applications. By empowering customers to use broadband connections to augment or replace their current MPLS networks, Aruba improves customer responsiveness, increases application performance, and significantly reduces capital and operational expenses by up to 90 percent.

Aruba Resources

The following table contains links to Aruba support resources.

Name	Definition
EdgeConnect and Zscaler Integration Guide - IPSec (for manual configurations)	Aruba EdgeConnect and Zscaler configuration manual (from Aruba).
Silver Peak Technical Demo: Integrating Zscaler into the Unity EdgeConnect™ SD-WAN Fabric	5-minute technical demonstration video that shows how Zscaler can be deployed to all locations with a single mouse click.
Zscaler and Silver Peak Solution Brief	Solution brief that shows how Silver Peak with Zscaler automate security policy enforcement for any user, application, or device across any location.
Silver Peak SD-WAN Deployment Guide	Aruba SD-WAN deployment guide (from Aruba).

Prerequisites

This guide provides GUI examples for configuring ZIA and Aruba Orchestrator. All examples in this guide presumes that the reader has a basic comprehension of IP networking. All examples in this guide explain how to provision new services with Zscaler and with Aruba SD-WAN. The prerequisites to use this guide are:

ZIA

- A working instance of ZIA (any cloud)
- Administrator login credentials

Silver Peak Orchestrator

- A working instance of Aruba Orchestrator, with administrator login credentials.
- One or more Aruba EdgeConnect appliances online and working

Configuring ZIA

This section demonstrates how to configure Zscaler before configuring Silver Peak.

Logging into ZIA

Log into Zscaler using your administrator account.

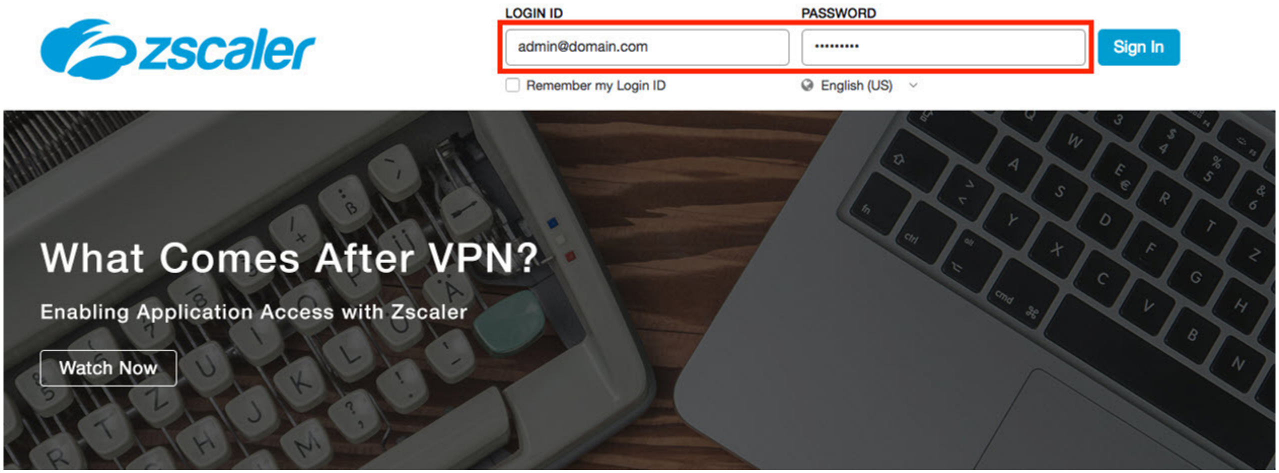


Figure 1. *Log into Zscaler*

If you are unable to log in using your administrator account, contact support (government agencies, see contact support).

Configure ZIA for API Access

The first step to enable ZIA for API access is creating an SD-WAN partner key. A partner key is an API key used as one form of authentication. A second form of authentication is the admin partner username and password, explained later in this Deployment Guide. You can use only this admin credential set for API calls—the admin credential doesn't work with the ZIA Admin Portal.

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

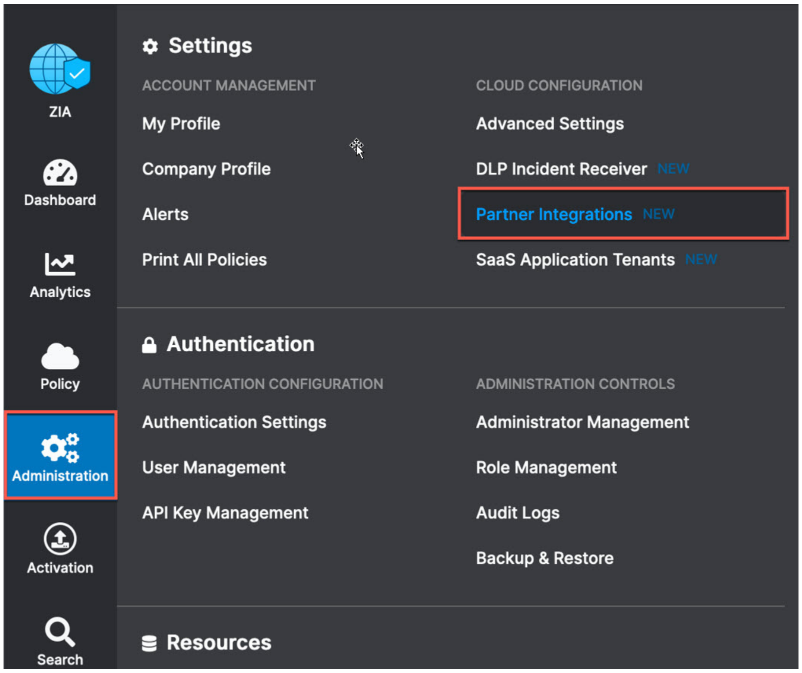
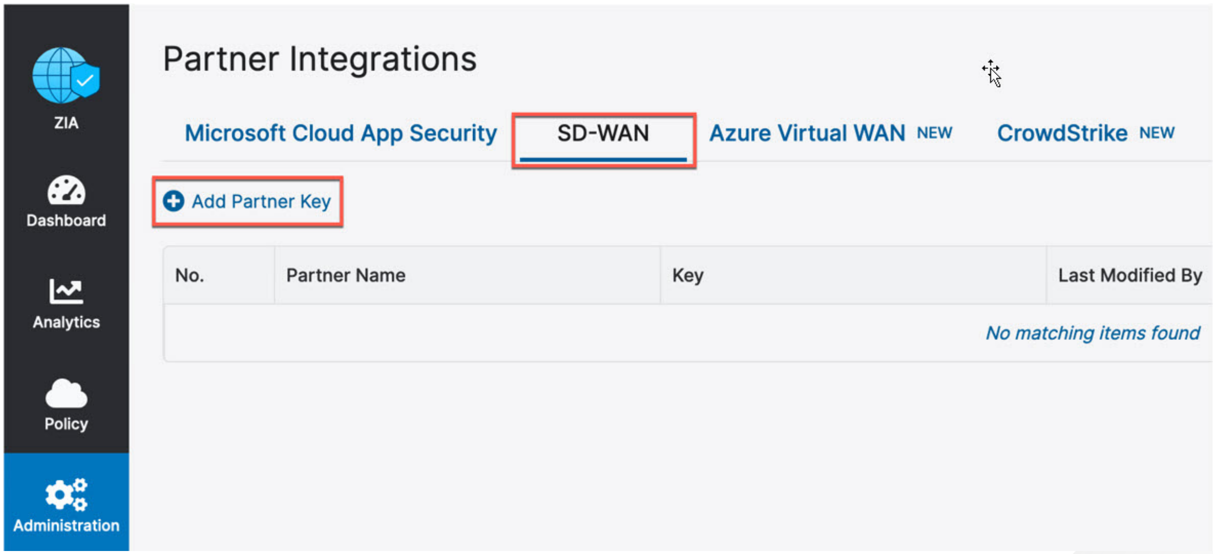


Figure 2. *Configuring ZIA for API access*

Adding SD-WAN Partner Key

In the **Partner Integration** section of the ZIA Admin Portal:

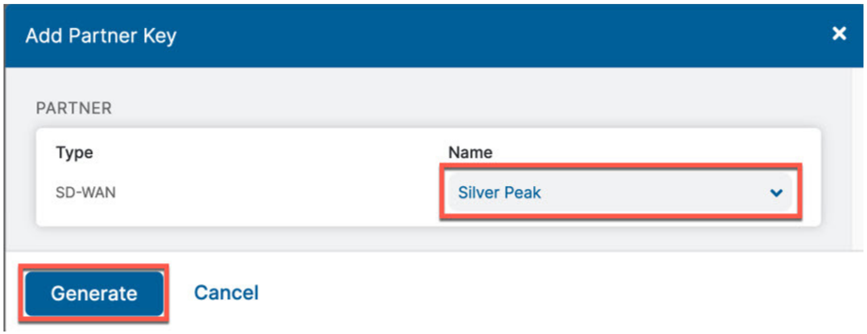
1. Select **SD-WAN** > **Add Partner Key**.



No.	Partner Name	Key	Last Modified By
			No matching items found

Figure 3. *Add a partner key*

2. The **Add Partner Key** dialog appears. On the right side of the window, type in or select the SD-WAN vendor from the drop-down menu.
3. Click **Generate**. You are returned to the prior screen.



PARTNER

Type: SD-WAN

Name: Silver Peak

Figure 4. *Add an SD-WAN partner key*

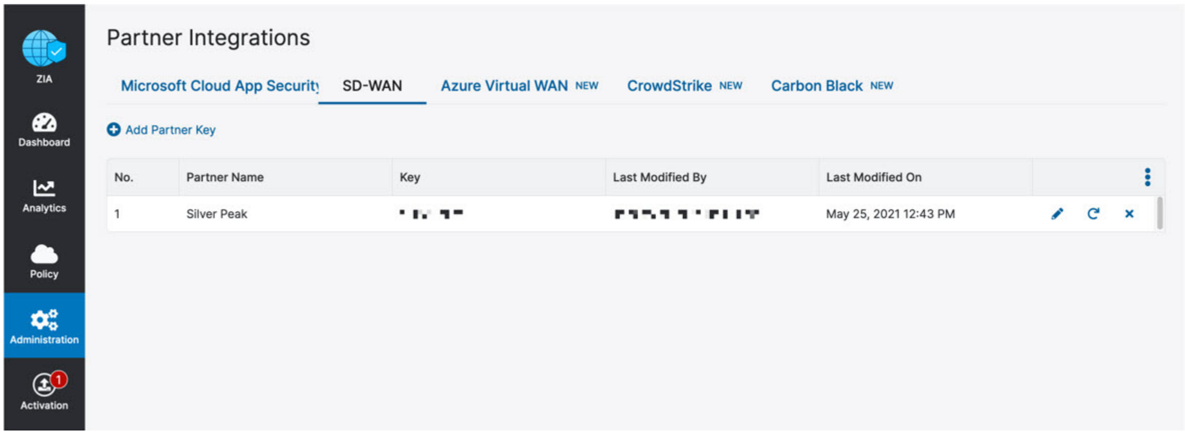
Verify SD-WAN Partner Key

The partner key for Silver Peak that you just created, appears on the screen.

(Password examples are blurred in this document.)

A red circle with a number above the **Activation** icon is shown. Although you created a partner key, the configuration change is pending. You must activate the change so that the configuration becomes active.

> The key value is required in Configuring ZIA API Credentials and Zscaler Cloud. Make sure to copy the key value for use in the Aruba Orchestrator.



No.	Partner Name	Key	Last Modified By	Last Modified On	
1	Silver Peak	[redacted]	[redacted]	May 25, 2021 12:43 PM	

Figure 5. *Verify the SD-WAN partner key*

> At this point, you can activate the change, but we recommend that you batch changes. This deployment guide tells you when to activate pending changes in batch.

Adding a Partner Administrator Role

You need to create a Partner Admin role and assign the role to the Administrator user that is used to authenticate against the Zscaler ZIA Provisioning API.

Navigate to **Administration** > **Authentication** > **Role Management**.

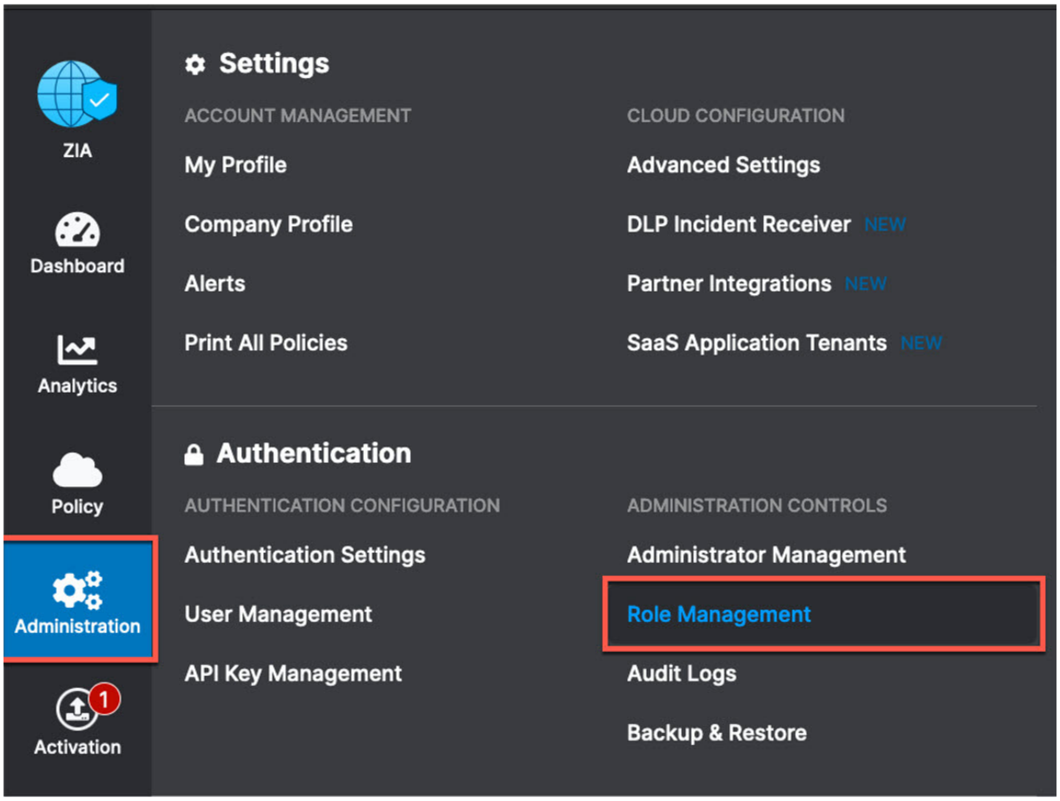
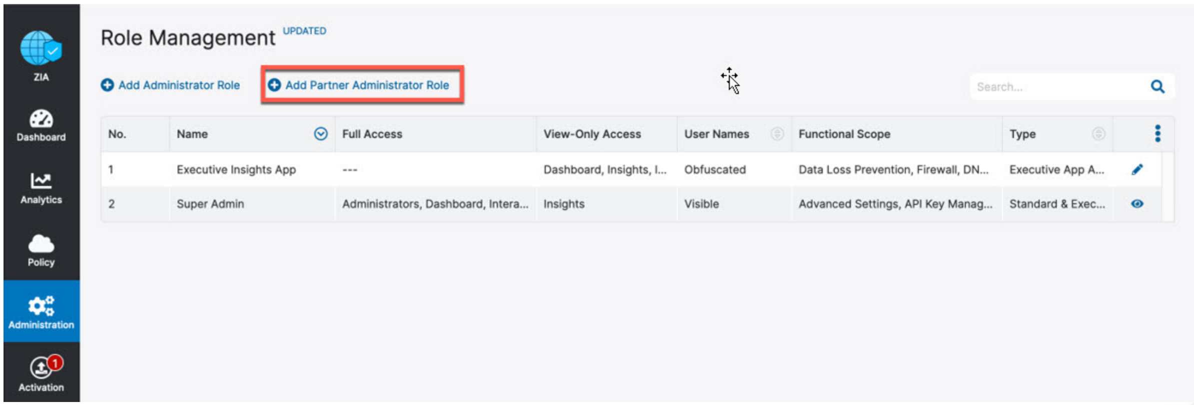


Figure 6. *Role Management controls*

Creating Partner Administrator Role

Complete the following steps:

1. Click the **Add Partner Administrator Role**.



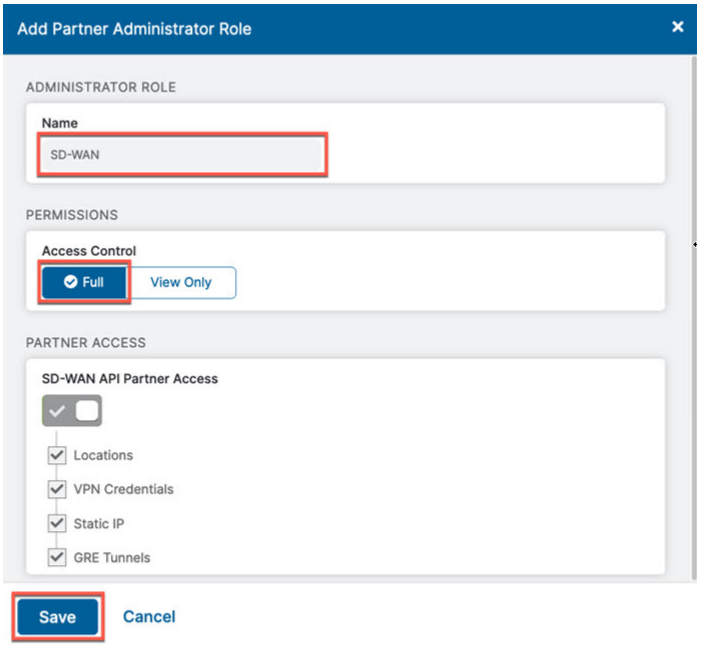
No.	Name	Full Access	View-Only Access	User Names	Functional Scope	Type
1	Executive Insights App	---	Dashboard, Insights, I...	Obfuscated	Data Loss Prevention, Firewall, DN...	Executive App A...
2	Super Admin	Administrators, Dashboard, Intera...	Insights	Visible	Advanced Settings, API Key Manag...	Standard & Exec...

Figure 7. *Add the partner administrator role*

You use the Partner Administrator role to define and grant permission and access to a third-party partner (such as a SD-WAN partner).

2. Name the partner administrator role.

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



Add Partner Administrator Role

ADMINISTRATOR ROLE

Name: SD-WAN

PERMISSIONS

Access Control: [✓ Full] View Only

PARTNER ACCESS

SD-WAN API Partner Access: ✓

☑ Locations

☑ VPN Credentials

☑ Static IP

☑ GRE Tunnels

Save Cancel

Figure 8. *Creating a partner administrator role*

4. Click **Save**. You are returned to the prior screen.

Administrator Management

The last step is creating a Partner Administrator. To create a Partner Administrator, navigate to **Administration** > **Administration Controls** > **Administrator Management**.

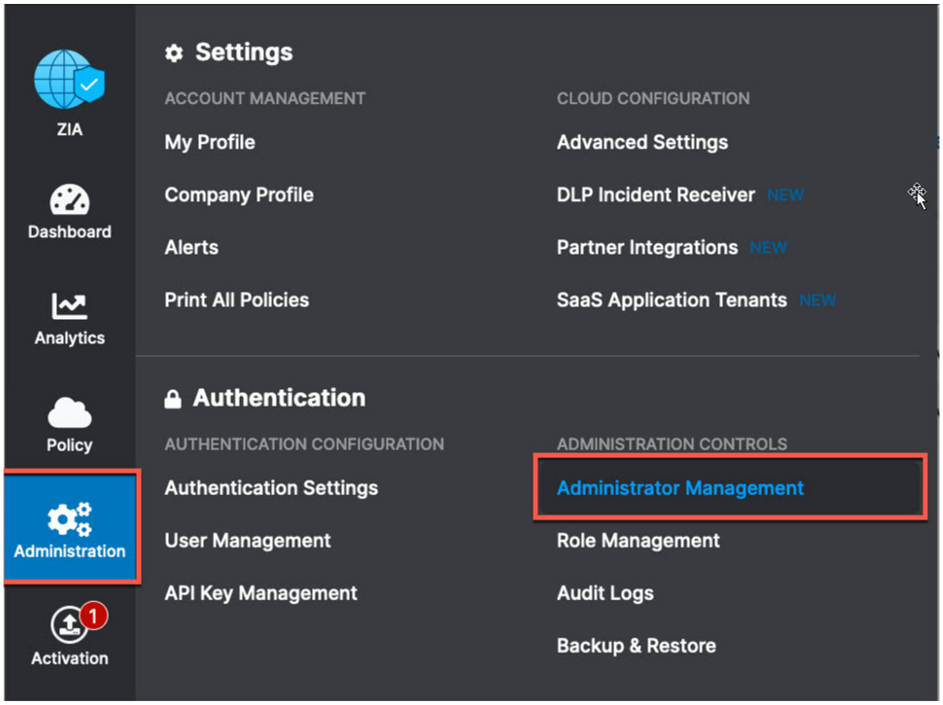
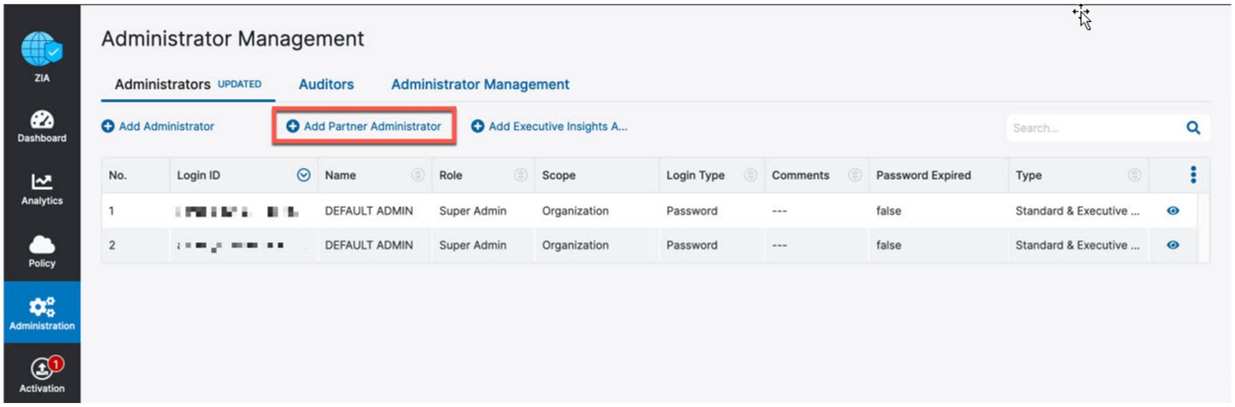


Figure 9. *Administrator Management*

Add Partner Administrator

On the **Administrator Management** page, click **Add Partner Administrator**. This opens the **Add Partner Administrator** page.

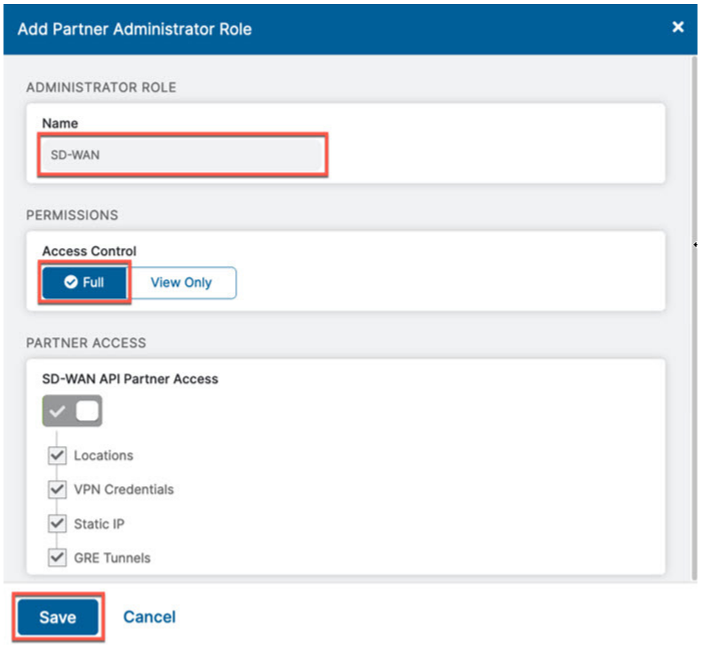


No.	Login ID	Name	Role	Scope	Login Type	Comments	Password Expired	Type
1	[redacted]	DEFAULT ADMIN	Super Admin	Organization	Password	---	false	Standard & Executive ...
2	[redacted]	DEFAULT ADMIN	Super Admin	Organization	Password	---	false	Standard & Executive ...

Figure 10. *Add Partner Administrator*

Creating Partner Administrator

1. In the **Add Partner Administrator** input box, fill in:
   - A **Login ID**
   - An **Email**
   - A **Partner Role**
2. Set the **Status** to **Enabled**.
3. Click **Save**.



Name: SD-WAN

Access Control: ● Full ○ View Only

SD-WAN API Partner Access: ✓

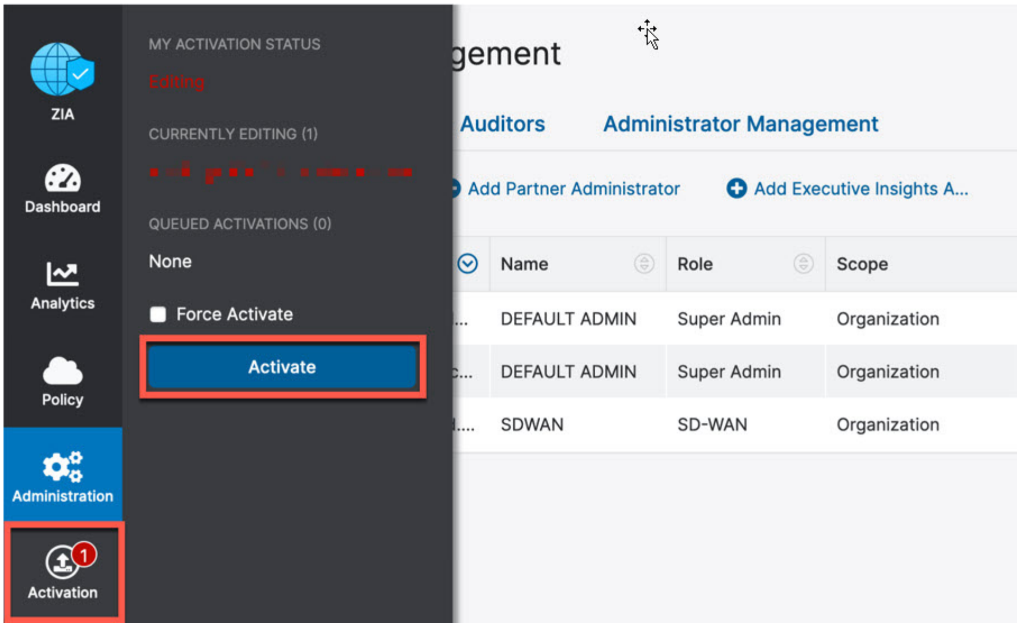
☑ Locations
☑ VPN Credentials
☑ Static IP
☑ GRE Tunnels

Figure 11. *Creating a partner administrator*

Save the Email and Password settings for Aruba Orchestrator to use for Configuring ZIA API Credentials and Zscaler Cloud.

Activate Pending Changes

Finally, navigate to **Activation** and activate the pending configurations.



MY ACTIVATION STATUS

Editing

CURRENTLY EDITING (1)

[redacted]

QUEUED ACTIVATIONS (0)

None

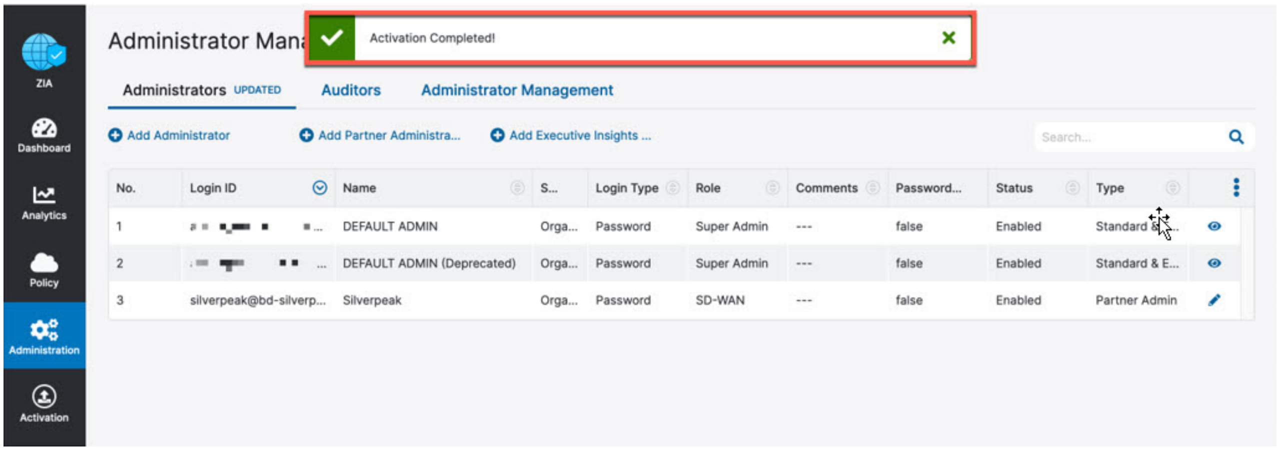
□ Force Activate

	Name	Role	Scope
...	DEFAULT ADMIN	Super Admin	Organization
c...	DEFAULT ADMIN	Super Admin	Organization
l....	SDWAN	SD-WAN	Organization

Figure 12. *Activate pending changes*

Verify Activation

After activating pending changes, verify that **Activation Complete** appears in the top of the window.



Activation Completed!

No.	Login ID	Name	S...	Login Type	Role	Comments	Password...	Status	Type
1	[redacted]	DEFAULT ADMIN	Orga...	Password	Super Admin	---	false	Enabled	Standard &...
2	[redacted]	DEFAULT ADMIN (Deprecated)	Orga...	Password	Super Admin	---	false	Enabled	Standard & E...
3	silverpeak@bd-silverp...	Silverpeak	Orga...	Password	SD-WAN	---	false	Enabled	Partner Admin

Figure 13. *Verify activation*

Configuring Automated IPSec Tunnels

In this section, you configure Aruba Orchestrator to provision ZIA. You use the settings that you saved in the prior section to complete this configuration.

Before starting, take note of the Aruba Orchestrator dashboard. This is what a live dashboard looks like. The screen capture shows only two devices, and therefore less activity is reported. To see more of the Aruba Orchestrator Dashboard, contact HPE and Aruba and request a full demo.

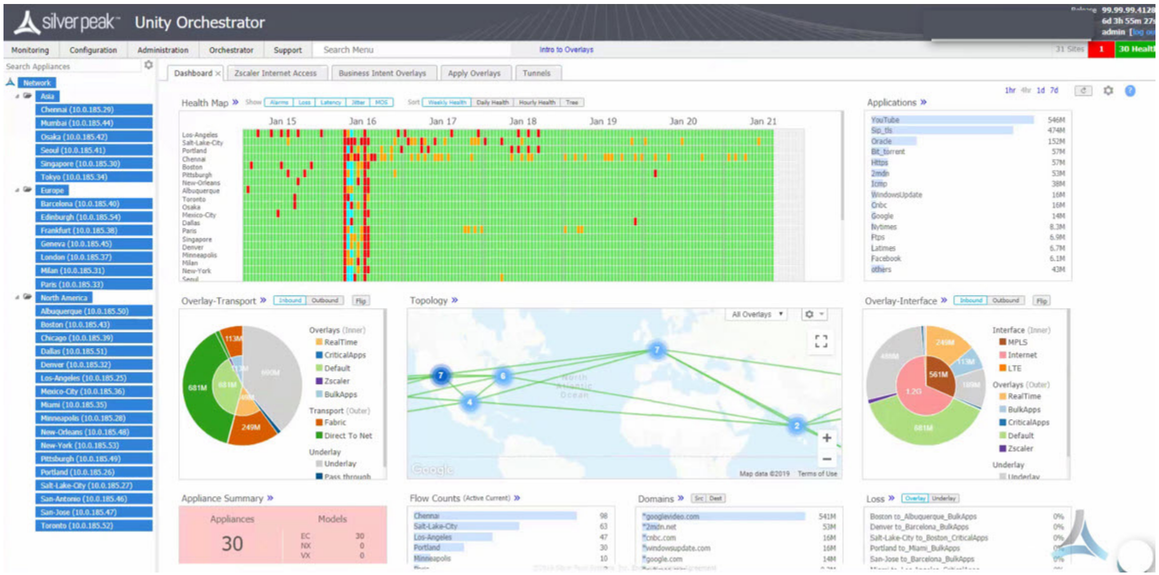


Figure 14. *Example of an Aruba Orchestrator dashboard*

Log into Aruba Orchestrator

1. Open a web browser and enter the URL to your Aruba Orchestrator instance. When the page loads, you see the Aruba login screen.
2. Enter your Aruba Orchestrator username and password. If you are unable to log in, email support@silver-peak.com.

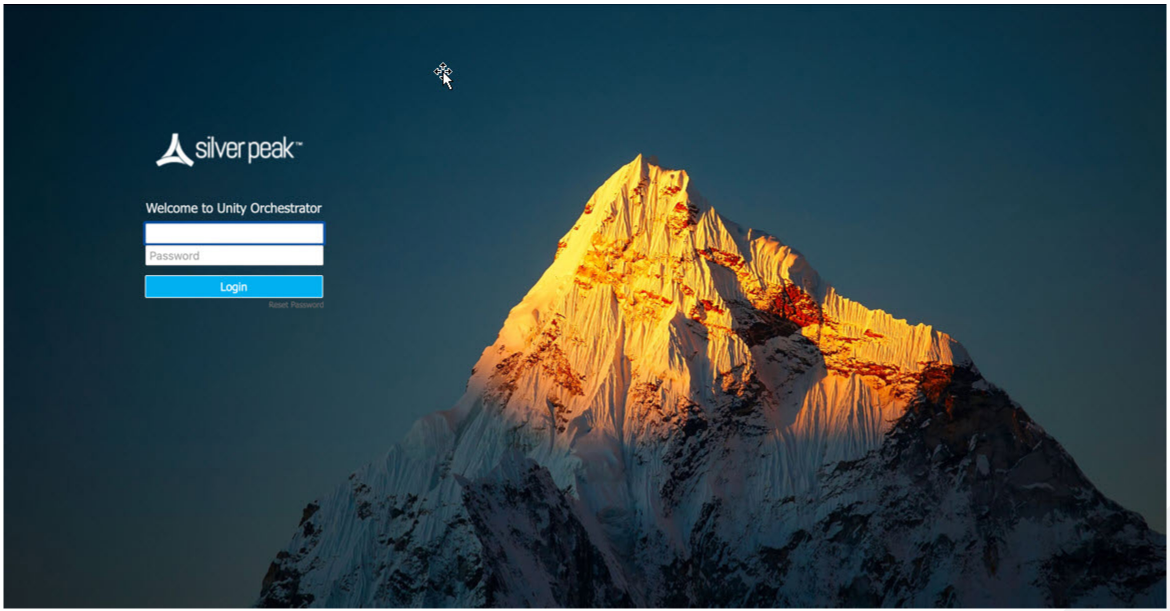


Figure 15. *Aruba Orchestrator login page*

Configure Cloud Services

First, configure the ZIA subscription by navigating to **Configuration** > **Cloud Services** > **Zscaler Internet Access**.

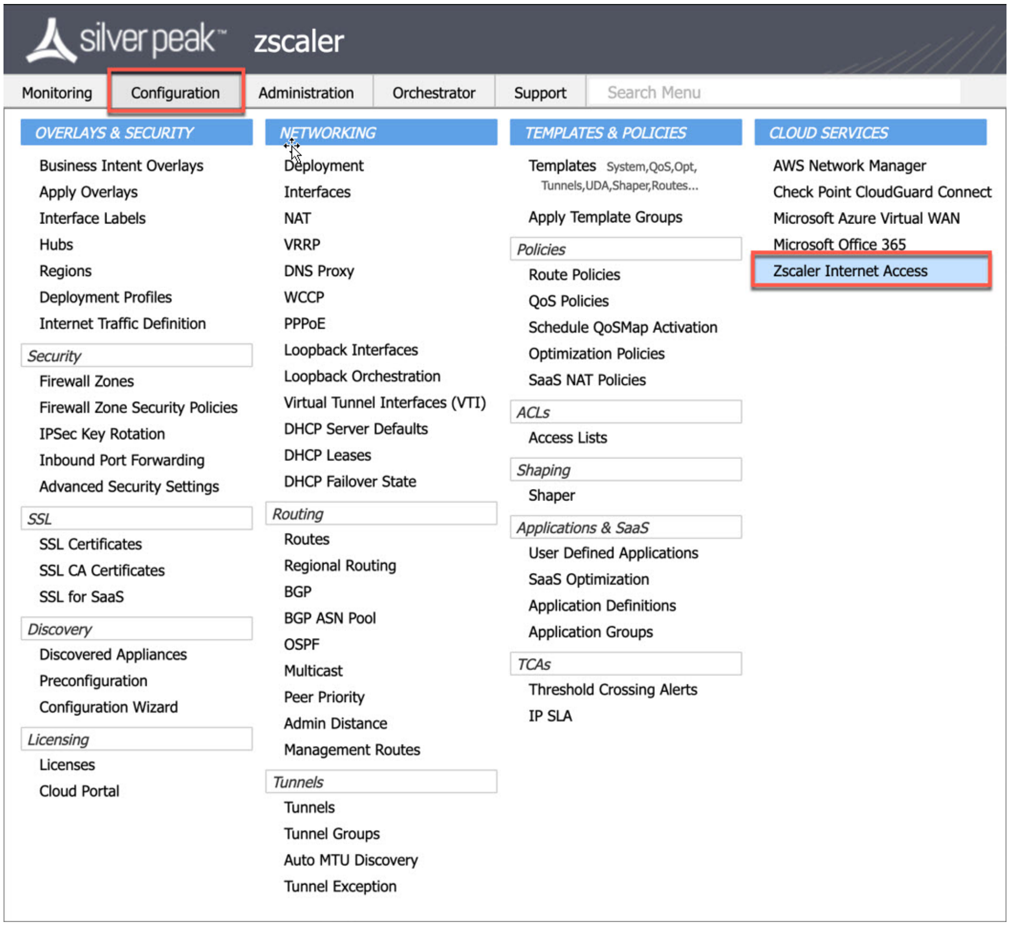


Figure 16. *Configuring cloud services*

Validate that the Desired Interface Labels are Selected

1. Ensure that you have the proper interface labels chosen to source tunnels from. In the **Zscaler Internet Access** tab, click **Interface Labels**.

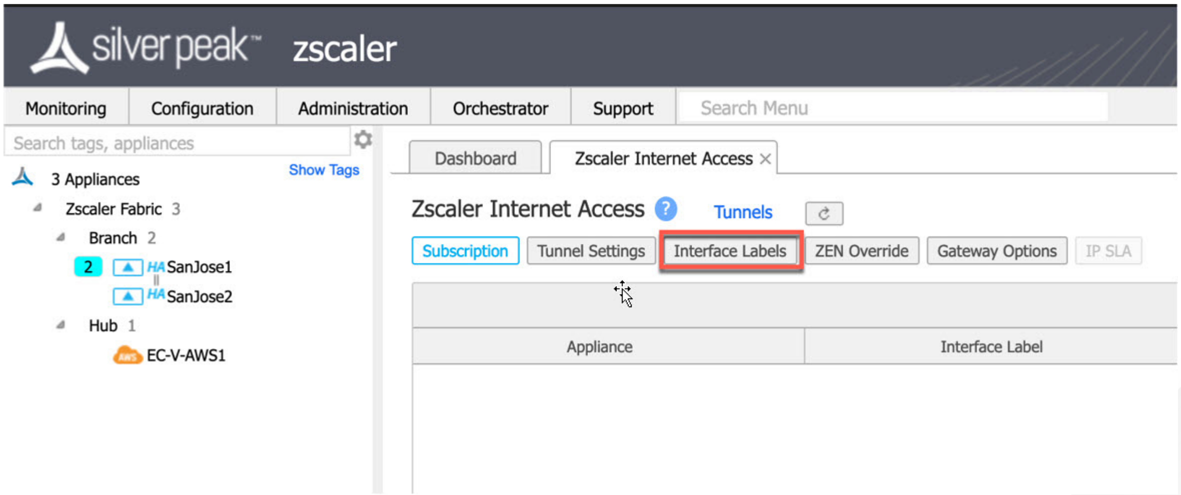
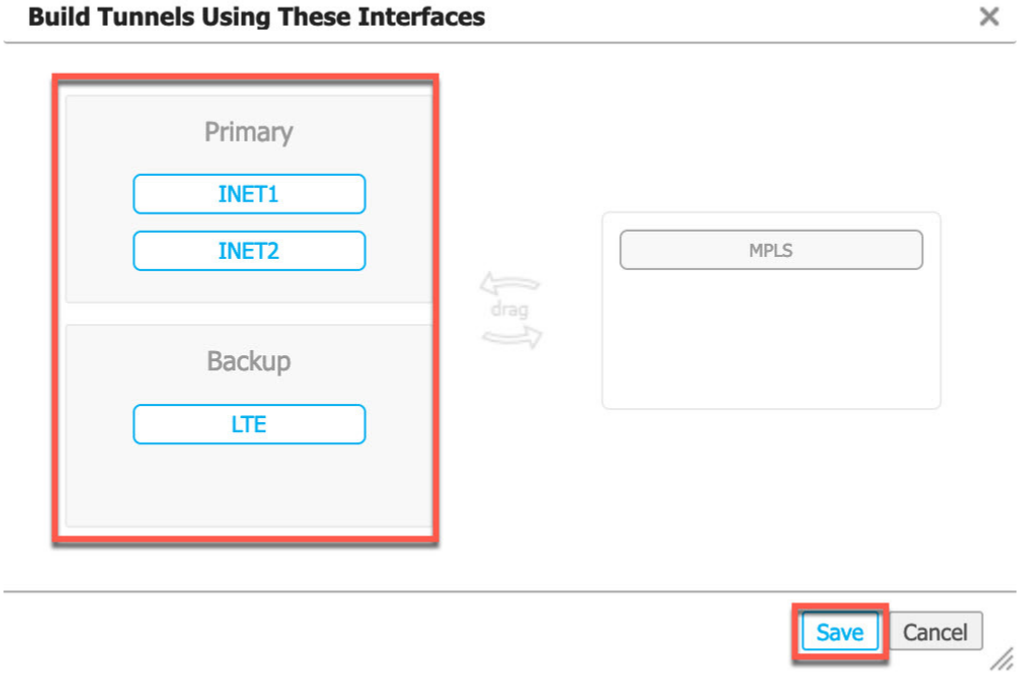


Figure 17. *Interface Labels*

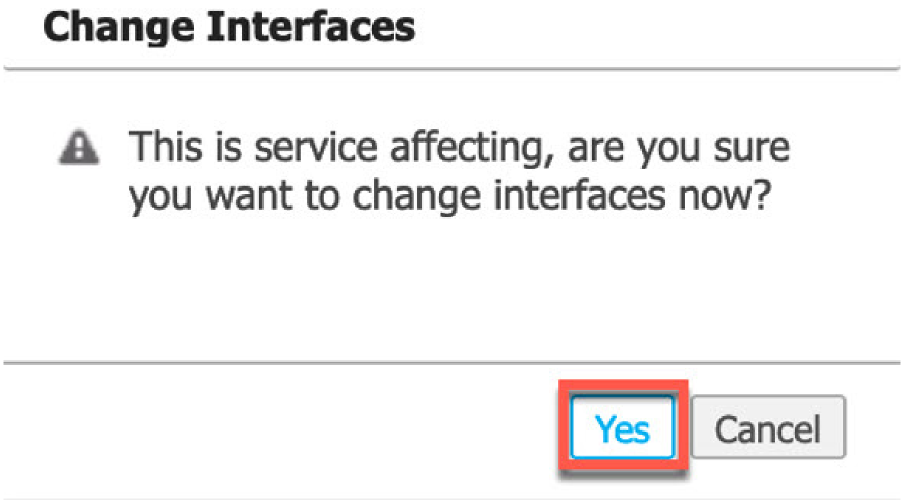
2. Validate that the correct Interface Labels are assigned as Primary and Backup sources for tunnel establishment to the ZIA endpoints.
3. Click **Save**.



Build Tunnels Using These Interfaces

Figure 18. *Choose interfaces for tunnel creation*

4. Drag the interface labels from the right to the left if required. Tunnels built to the ZIA Public Service Edges use these interfaces.
5. Click **Yes** to apply your changes.



Change Interfaces

This is service affecting, are you sure you want to change interfaces now?

Figure 19. *Apply the tunnel setting to interfaces*

Configure Tunnel Settings

EdgeConnect Enterprise can automatically provision both IPSec and GRE tunnels using the API automation Integrations. The steps are:

- Choosing the Interface Labels that are used to establish ZIA tunnels.
- Decide which type of tunnel is used for each label, GRE or IPSec.
- Configure the optimal settings for IPSec.

To configure tunnel settings:

1. In the **Zscaler Internet Access** tab, click **Tunnel Settings**. The **Tunnel Setting** window appears.

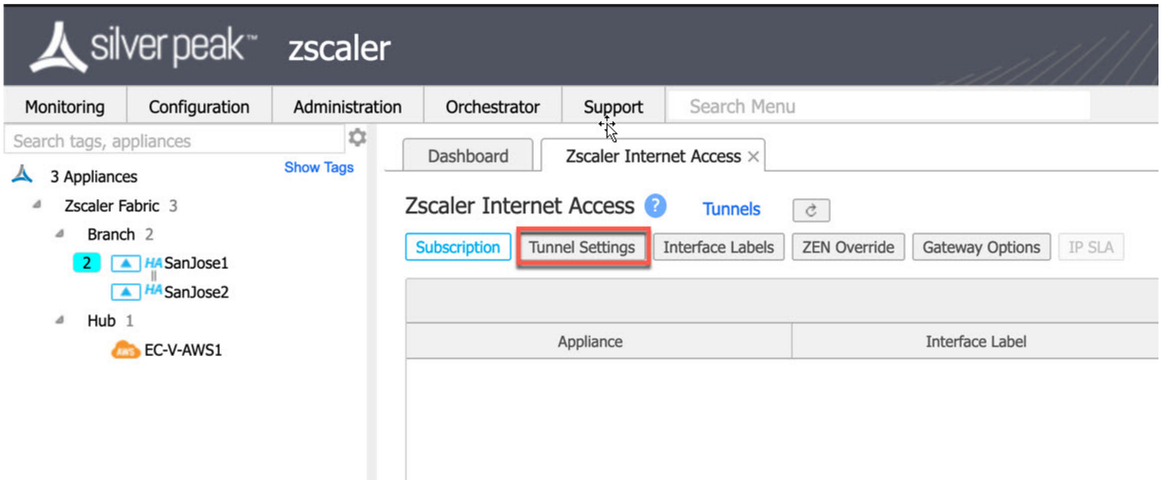
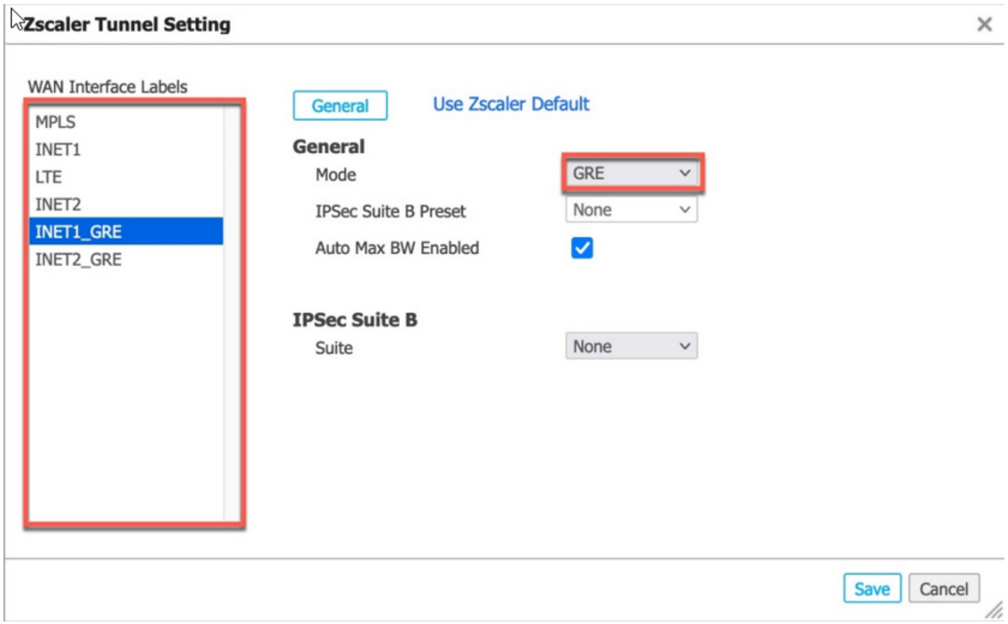


Figure 20. *Open the Tunnel Settings window*

2. Choose which **WAN Interface Label** to use for establishing tunnels to ZIA.
3. Select the **Tunnel Mode**.



Mode: GRE

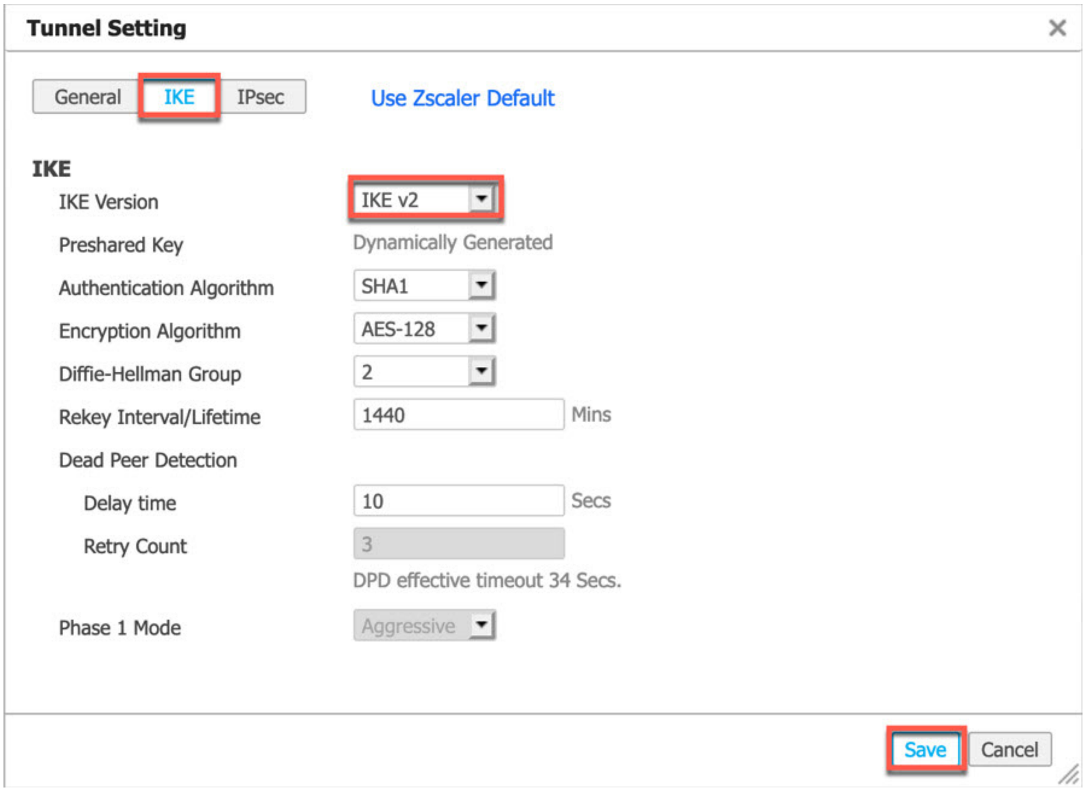
IPSec Suite B Preset: None

Auto Max BW Enabled: ☑

Suite: None

Figure 21. *Select Interface Label and choose Tunnel Mode*

4. For IPSec, click on the **IKE** tab and change the **IKE Version** to **IKE v2**.
5. Click **Save**.



Tunnel Setting

General | IKE | IPsec   Use Zscaler Default

IKE

IKE Version: IKE v2

Preshared Key: Dynamically Generated

Authentication Algorithm: SHA1

Encryption Algorithm: AES-128

Diffie-Hellman Group: 2

Rekey Interval/Lifetime: 1440 Mins

Dead Peer Detection

Delay time: 10 Secs

Retry Count: 3

DPD effective timeout 34 Secs.

Phase 1 Mode: Aggressive

Figure 22. *Configure IKE v2 for IPSec tunnels*

For GRE there are no settings changes necessary.

Configuring a ZIA Subscription

Select the **Subscription** tab.

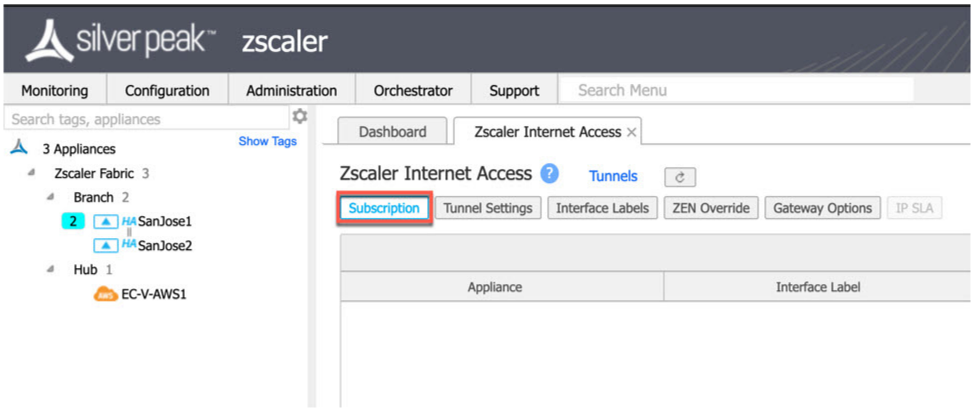


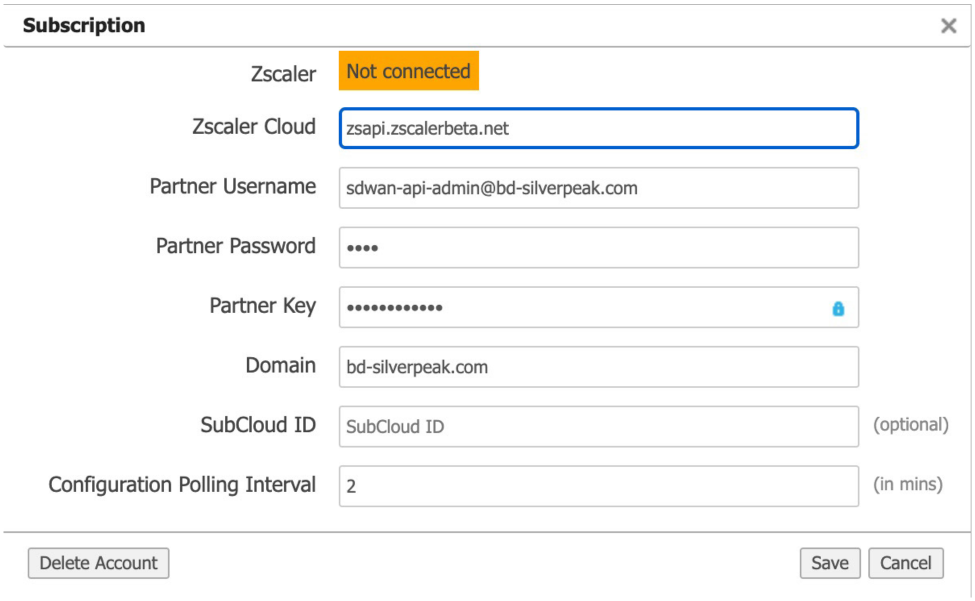
Figure 23. *Configuring a ZIA subscription*

Configuring ZIA API Credentials and Zscaler Cloud

Configure the ZIA cloud and your ZIA API credentials. For large production deployments, keep the **Configuration Polling Interval** setting at the default of 10 minutes. This increases the responsiveness of the API when you make frequent changes to the Zscaler cloud configuration.

If the customer uses a subcloud for DC selection, enter it into the **SubCloud ID** field.

When configuring the Zscaler Cloud field, ensure the cloud is prepended with zapi. Example: zsapi.zscalerbeta.net.



Subscription

Zscaler	Not connected	
Zscaler Cloud	zsapi.zscalerbeta.net	
Partner Username	sdwan-api-admin@bd-silverpeak.com	
Partner Password	••••	
Partner Key	••••••••••••	
Domain	bd-silverpeak.com	
SubCloud ID	SubCloud ID	(optional)
Configuration Polling Interval	2	(in mins)

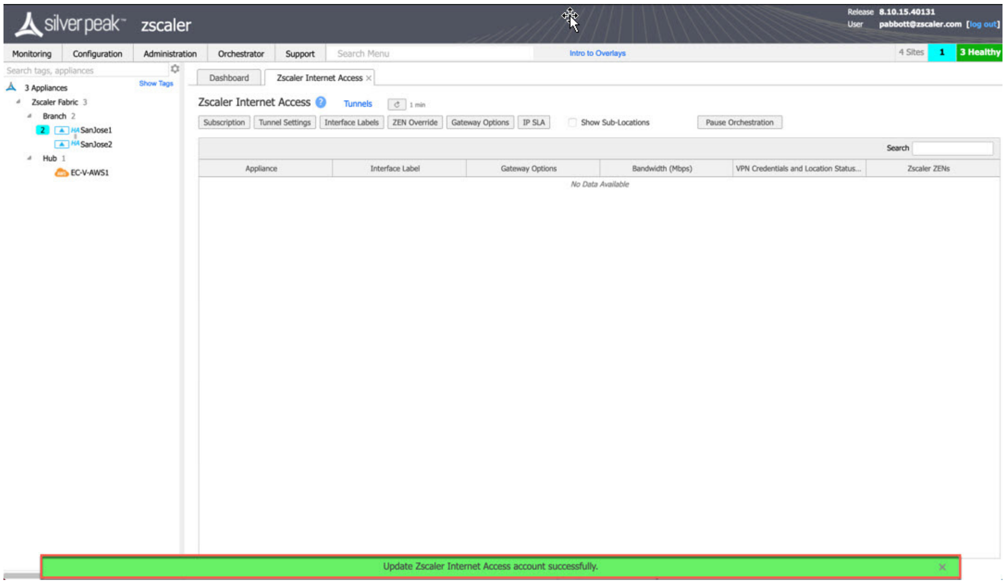
Figure 24. *Configuring API credentials*

Click **Save** to refresh the screen.

For demonstration and POC purposes, reduce the Polling Interval to a shorter timeframe (such as two minutes).

Verify ZIA Account Update

After you save your ZIA settings, the **Update Zscaler Internet Access account successfully** message appears at the bottom of the screen in a green box.



Zscaler Internet Access

Appliance	Interface Label	Gateway Options	Bandwidth (Mbps)	VPN Credentials and Location Status...	Zscaler ZENs

No Data Available

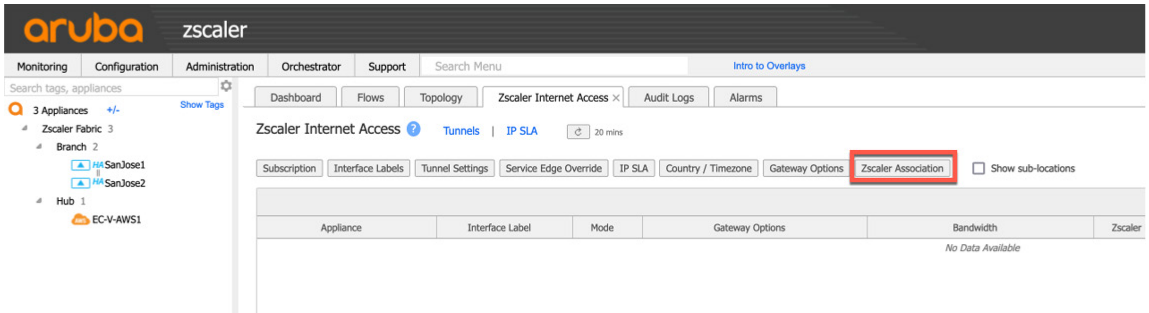
Update Zscaler Internet Access account successfully.

Figure 25. *Verifying a ZIA account update*

Associate Sites with ZIA for Automation

For recent releases of Aruba EdgeConnect for Enterprise, complete an additional step that allows for fine-grained control of which appliances to apply ZIA automation.

1. Click **Zscaler Association** button to bring up the selection window.



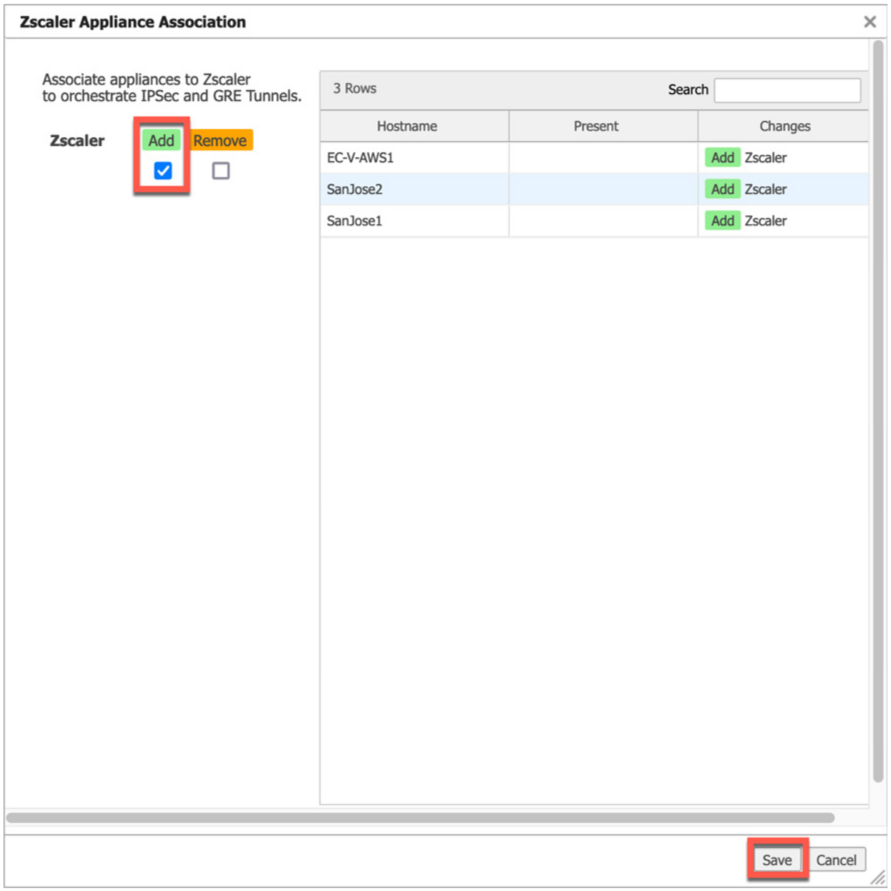
Zscaler Internet Access

Appliance	Interface Label	Mode	Gateway Options	Bandwidth	Zscaler

No Data Available

Figure 26. *How to access Zscaler Association of Appliances*

2. Select **Add** under Zscaler.
3. Click **Save**.


Zscaler Appliance Association

Associate appliances to Zscaler to orchestrate IPSec and GRE Tunnels.

Zscaler: Add ☑ Remove □

3 Rows

Hostname	Present	Changes
EC-V-AWS1		Add Zscaler
SanJose2		Add Zscaler
SanJose1		Add Zscaler

Figure 27. *Associating EdgeConnect Appliances to ZIA Automation*

Configuring Business Intent Overlays

Configure the Business Intent Overlays. Navigate to **Configuration** > **Overlays** > **Business Intent Overlays**.

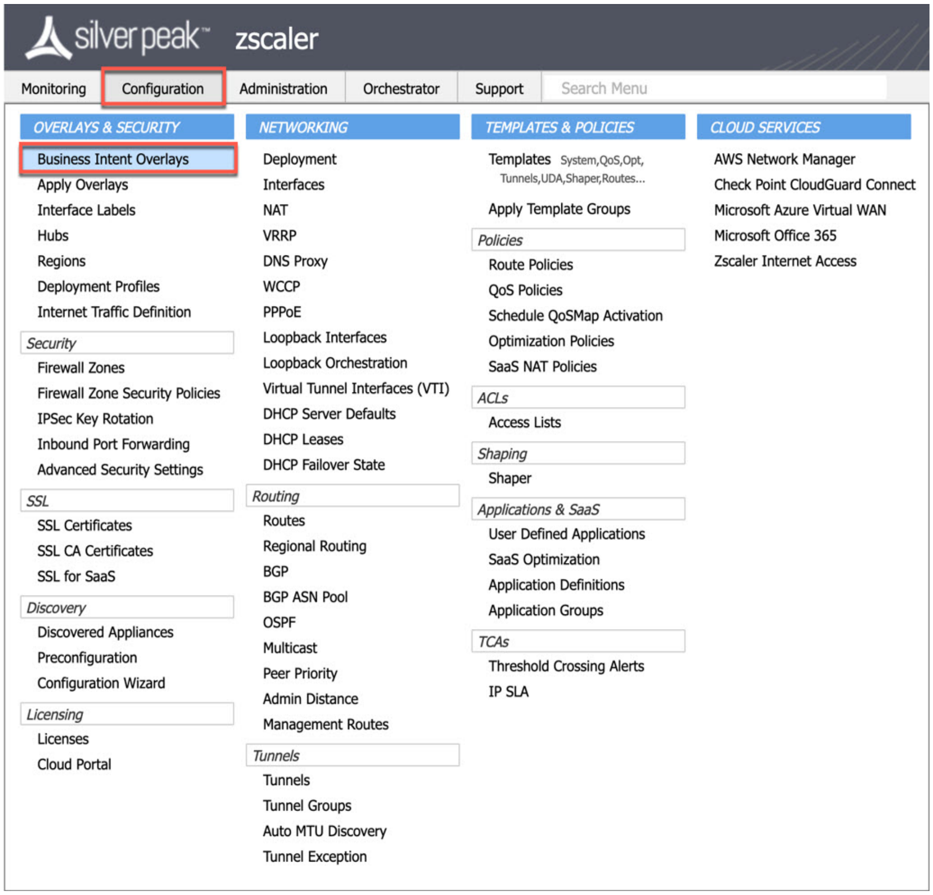
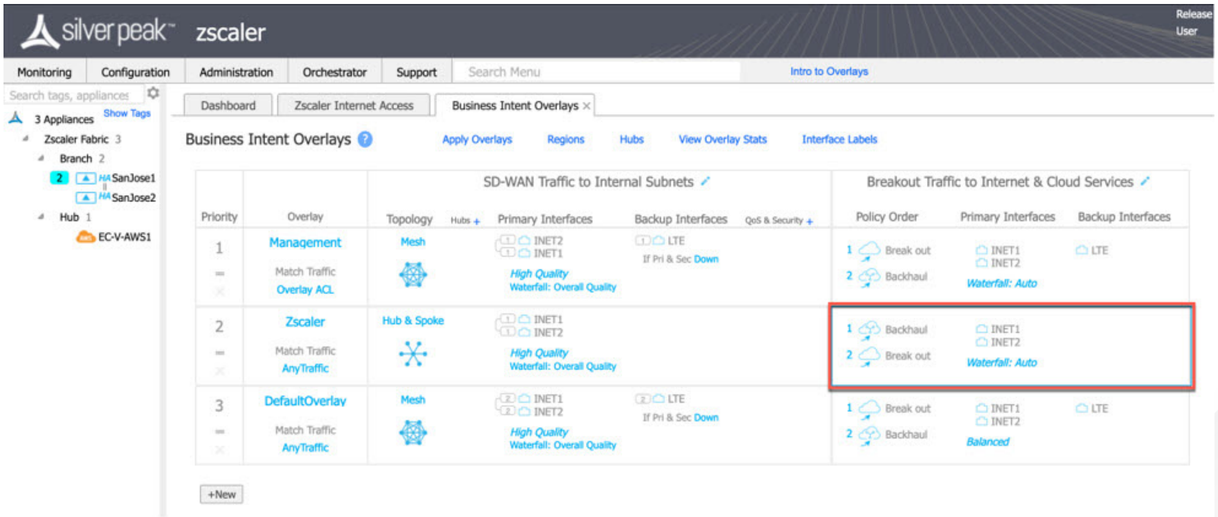


Figure 28. *Configuring business intent overlays*

Enabling Zscaler for Breakout Traffic

Look for the **Breakout Traffic to Internet & Cloud Services** section. Choose the overlay to configure use of ZIA. Then click anywhere within the red box to see more configuration options.

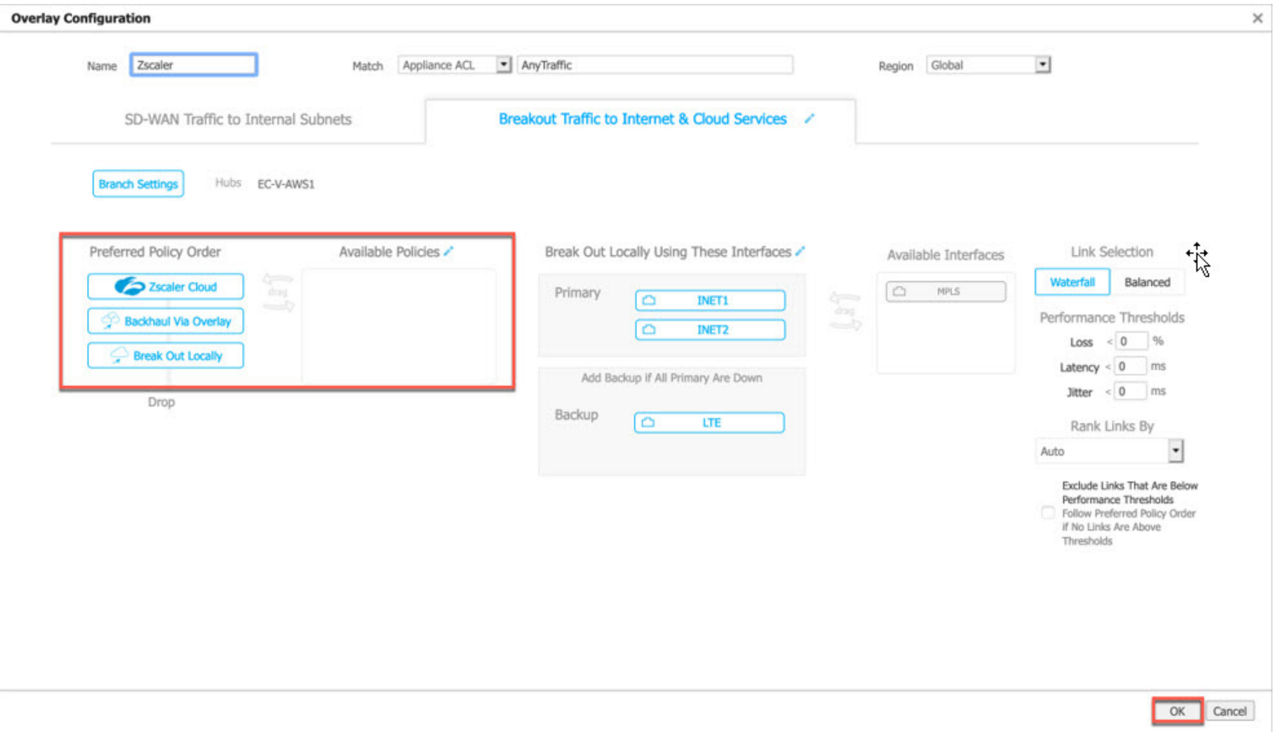


		SD-WAN Traffic to Internal Subnets					Breakout Traffic to Internet & Cloud Services		
Priority	Overlay	Topology	Hubs +	Primary Interfaces	Backup Interfaces	QoS & Security +	Policy Order	Primary Interfaces	Backup Interfaces
1	Management Match Traffic Overlay ACL	Mesh		INET2 INET1 High Quality Waterfall: Overall Quality	LTE If Pri & Sec Down		1 Break out 2 Backhaul	INET1 INET2 Waterfall: Auto	LTE
2	Zscaler Match Traffic AnyTraffic	Hub & Spoke		INET1 INET2 High Quality Waterfall: Overall Quality			1 Backhaul 2 Break out	INET1 INET2 Waterfall: Auto	
3	DefaultOverlay Match Traffic AnyTraffic	Mesh		INET1 INET2 High Quality Waterfall: Overall Quality	LTE If Pri & Sec Down		1 Break out 2 Backhaul	INET1 INET2 Balanced	LTE

Figure 29. *Enabling Zscaler for breakout traffic*

Configuring Preferred Policy Order

The goal of this step is to configure the **Preferred Policy Order** with **Zscaler Cloud** at the top of the list. The **Zscaler Cloud** button might be under **Available Policies**. If so, drag the button over to the left column. Then click **OK**.



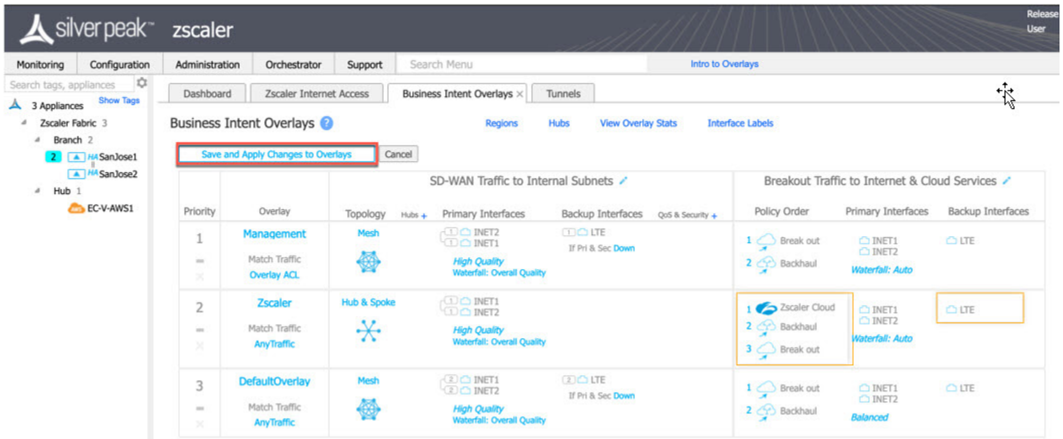
Overlay Configuration

Name: Zscaler   Match: Appliance ACL   AnyTraffic   Region: Global

Figure 30. *Configuring preferred policy order*

Apply Overlay Changes

Changes are reflected in **Business Intent Overlays** and are highlighted by yellow boxes. Click **Save** and **Apply Overlay Changes to Overlays**.

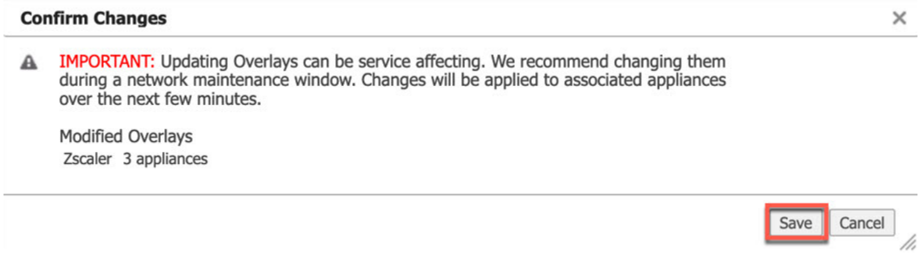


Business Intent Overlays

		SD-WAN Traffic to Internal Subnets			Breakout Traffic to Internet & Cloud Services		
Priority	Overlay	Topology	Primary Interfaces	Backup Interfaces	Policy Order	Primary Interfaces	Backup Interfaces
1	Management Match Traffic Overlay ACL	Mesh	INET2 INET1 High Quality Waterfall: Overall Quality	LTE If Pri & Sec Down	1 Break out 2 Backhaul	INET1 INET2 Waterfall: Auto	LTE
2	Zscaler Match Traffic AnyTraffic	Hub & Spoke	INET1 INET2 High Quality Waterfall: Overall Quality		1 Zscaler Cloud 2 Backhaul 3 Break out	INET1 INET2 Waterfall: Auto	LTE
3	DefaultOverlay Match Traffic AnyTraffic	Mesh	INET1 INET2 High Quality Waterfall: Overall Quality	LTE If Pri & Sec Down	1 Break out 2 Backhaul	INET1 INET2 Balanced	LTE

Figure 31. *Save and apply changes*

A confirmation dialog window displays to verify your changes. Click **Save**.



Confirm Changes

IMPORTANT: Updating Overlays can be service affecting. We recommend changing them during a network maintenance window. Changes will be applied to associated appliances over the next few minutes.

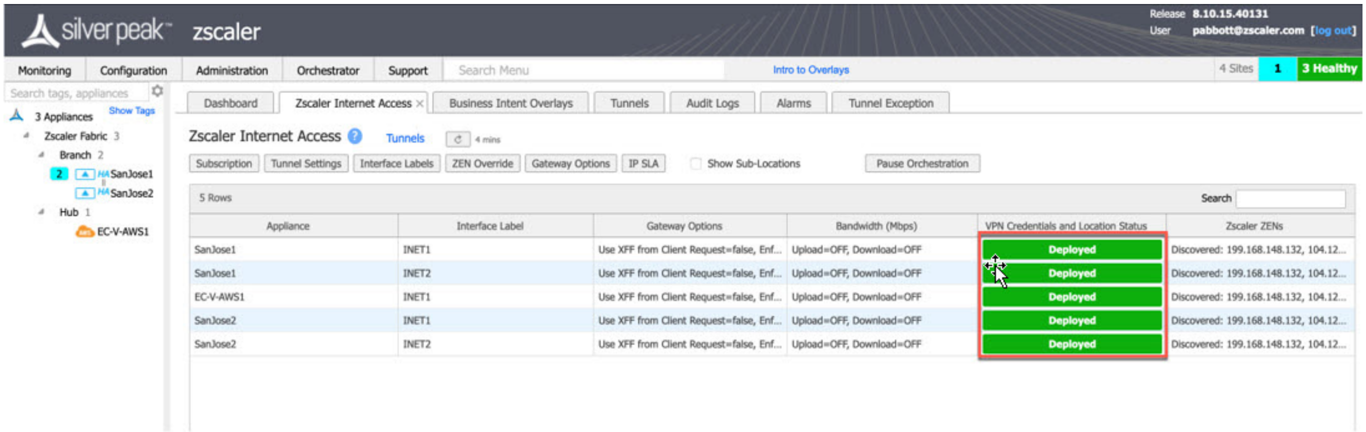
Modified Overlays
Zscaler 3 appliances

Figure 32. *Confirm changes*

Verifying Automated Tunnel Establishment

It can take 30-60 seconds before your initial tunnels are deployed. Navigate back to **Configuration** > **Cloud Services** > **Zscaler Internet Access**. You can see the provisioned **Appliances** and **Interface Labels**.

After establishing the IPSec tunnels, the Deployed tunnels appear highlighted in green.



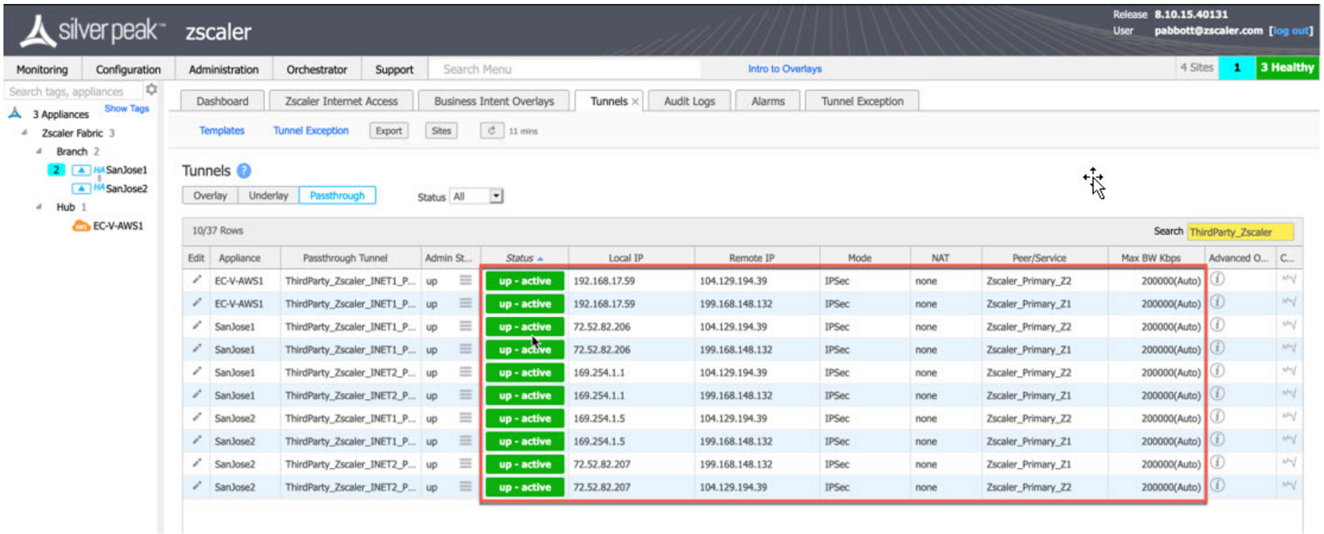
Appliance	Interface Label	Gateway Options	Bandwidth (Mbps)	VPN Credentials and Location Status	Zscaler ZENs
SanJose1	INET1	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
SanJose1	INET2	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
EC-V-AWS1	INET1	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
SanJose2	INET1	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
SanJose2	INET2	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...

Figure 33. *Verify automated tunnel establishment*

View Automated Tunnel Details

If you select **Tunnels** in the **Zscaler Internet Access** tab, you are brought to the **Tunnels** tab and can see more details for each configured tunnel (e.g., local IP, remote IP, tunnel mode, etc.).

Click the **Tunnels** selection in the **Zscaler Internet Access** tab to activate a filter in the search field that highlights only Zscaler tunnels.



Edit	Appliance	Passthrough Tunnel	Admin St...	Status	Local IP	Remote IP	Mode	NAT	Peer/Service	Max BW Kbps	Advanced O...	C...
✎	EC-V-AWS1	ThirdParty_Zscaler_INET1_P...	up	up - active	192.168.17.59	104.129.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	ⓘ	
✎	EC-V-AWS1	ThirdParty_Zscaler_INET1_P...	up	up - active	192.168.17.59	199.168.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	ⓘ	
✎	SanJose1	ThirdParty_Zscaler_INET1_P...	up	up - active	72.52.82.206	104.129.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	ⓘ	
✎	SanJose1	ThirdParty_Zscaler_INET1_P...	up	up - active	72.52.82.206	199.168.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	ⓘ	
✎	SanJose1	ThirdParty_Zscaler_INET2_P...	up	up - active	169.254.1.1	104.129.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	ⓘ	
✎	SanJose1	ThirdParty_Zscaler_INET2_P...	up	up - active	169.254.1.1	199.168.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	ⓘ	
✎	SanJose2	ThirdParty_Zscaler_INET1_P...	up	up - active	169.254.1.5	104.129.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	ⓘ	
✎	SanJose2	ThirdParty_Zscaler_INET1_P...	up	up - active	169.254.1.5	199.168.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	ⓘ	
✎	SanJose2	ThirdParty_Zscaler_INET2_P...	up	up - active	72.52.82.207	199.168.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	ⓘ	
✎	SanJose2	ThirdParty_Zscaler_INET2_P...	up	up - active	72.52.82.207	104.129.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	ⓘ	

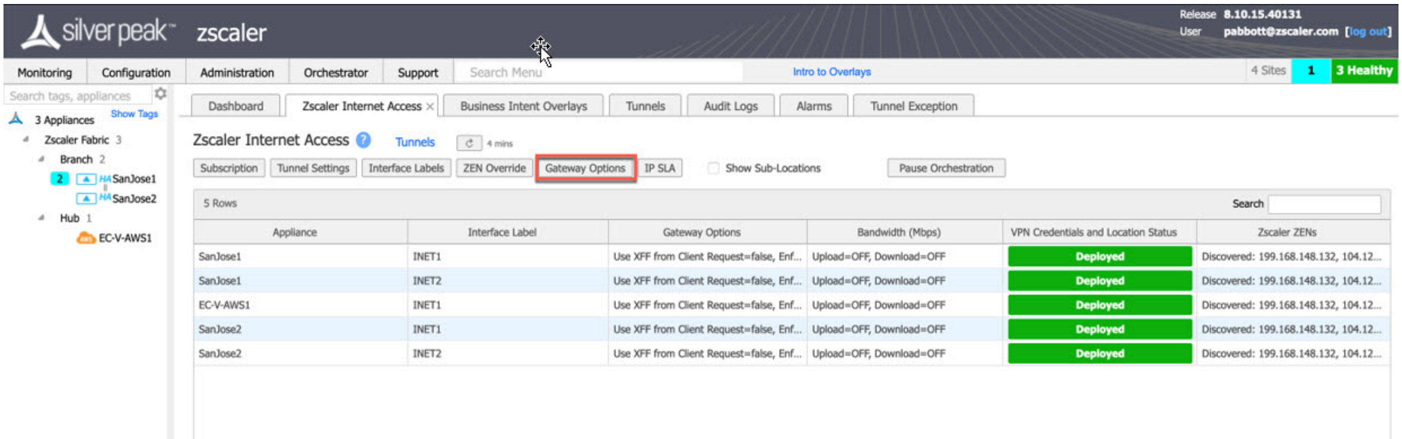
Figure 34. *View automated tunnel details*

Configuring Sub-Locations and Gateway Options

If you are new to Zscaler sub-locations, see ZIA About Sublocations (government agencies, see ZIA About Sublocations).

Configure Sub-location

Navigate back to the **Configuration** > **Cloud Services** > **Zscaler Internet Access** tab and click **Gateway Options** to configure a sub-location.

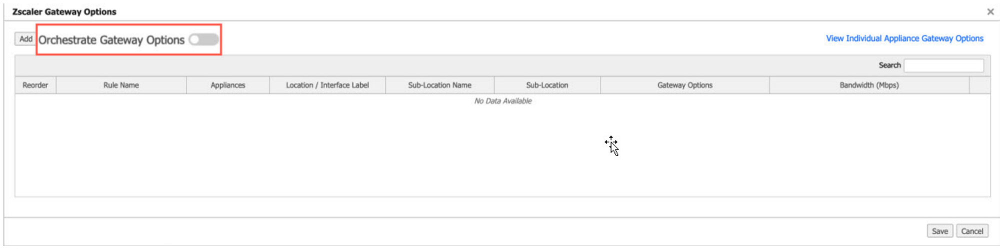


Appliance	Interface Label	Gateway Options	Bandwidth (Mbps)	VPN Credentials and Location Status	Zscaler ZENs
SanJose1	INET1	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
SanJose1	INET2	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
EC-V-AWS1	INET1	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
SanJose2	INET1	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...
SanJose2	INET2	Use XFF from Client Request=false, Enf...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12...

Figure 35. *Configure sub-location*

Enable Gateway Option Orchestration

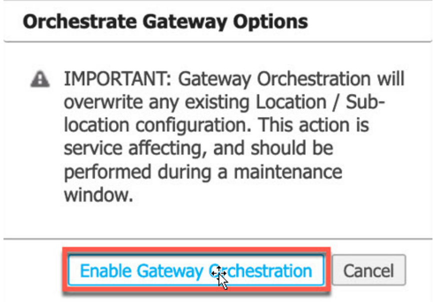
1. If this is your first time selecting **Gateway Options**, you must click the slider next to Orchestrate **Gateway Options**:


Zscaler Gateway Options
×
Add
Orchestrate Gateway Options
View Individual Appliance Gateway Options
Search
Save
Cancel

Reorder	Rule Name	Appliances	Location / Interface Label	Sub-Location Name	Sub-Location	Gateway Options	Bandwidth (Mbps)
				No Data Available			

Figure 36. *Enable gateway options*

2. A pop-up window appears. Click **Enable Gateway Orchestration** to continue.



Orchestrate Gateway Options

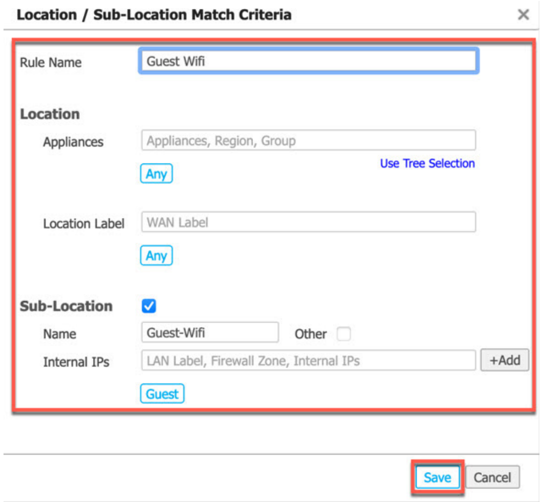
IMPORTANT: Gateway Orchestration will overwrite any existing Location / Sub-location configuration. This action is service affecting, and should be performed during a maintenance window.

Figure 37. *Enable gateway option orchestration*

Add Sub-Location

Click **Add**. The **Location / Sub-location Match Criteria** window appears. You need to configure:

1. The **Rule Name**, which is used only by Aruba Orchestrator. This is not the name of the sub-location that appears in ZIA
2. Select the EdgeConnect **Appliances** and **Location Label** that match this sub-location. Most deployments use "Any" for both appliances and location labels.
3. Configure the sub-location **Name** (e.g., Guest Wi-Fi) and the subnets that this gateway matches. The sub-location name is the name used in ZIA. In most cases, the sub-Location name is the same as the rule name that you set for Aruba Orchestrator. The **Subnets** field match an EdgeConnect interface label as configured in the **Deployment** screen of an EdgeConnect appliance.
4. Click **Save**.



Location / Sub-Location Match Criteria

Rule Name: Guest Wifi

Location

Appliances: Appliances, Region, Group — Any — Use Tree Selection

Location Label: WAN Label — Any

Sub-Location ☑

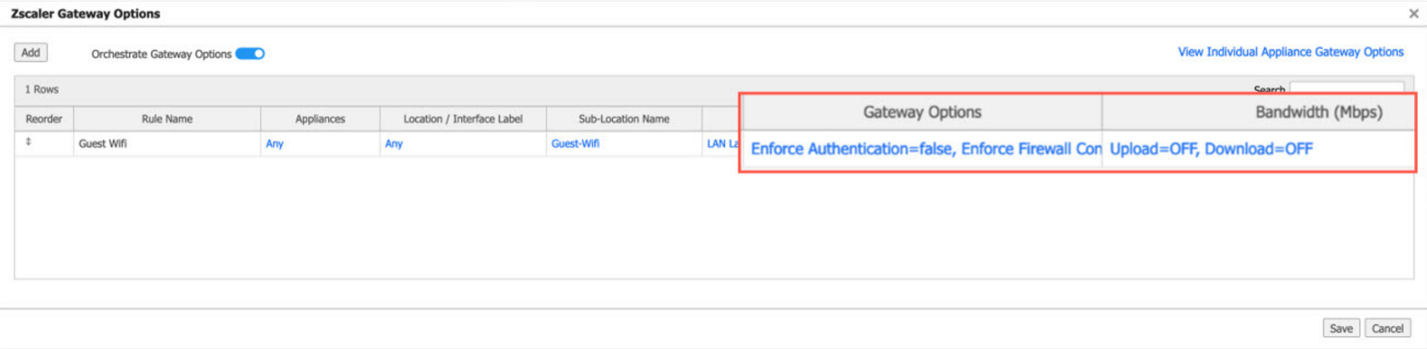
Name: Guest-Wifi — Other □

Internal IPs: LAN Label, Firewall Zone, Internal IPs — +Add — Guest

Figure 38. *Add sub-location*

Configure Gateway Options

After the screen refreshes, the sub-location that you configured appear. To configure gateway options for this sub-location, click **Gateway Options and Bandwidth**.



Zscaler Gateway Options

Orchestrate Gateway Options (on)

1 Rows

Reorder	Rule Name	Appliances	Location / Interface Label	Sub-Location Name		Gateway Options	Bandwidth (Mbps)
↕	Guest Wifi	Any	Any	Guest-Wifi	LAN La	Enforce Authentication=false, Enforce Firewall Con	Upload=OFF, Download=OFF

Figure 39. *Configure gateway options*

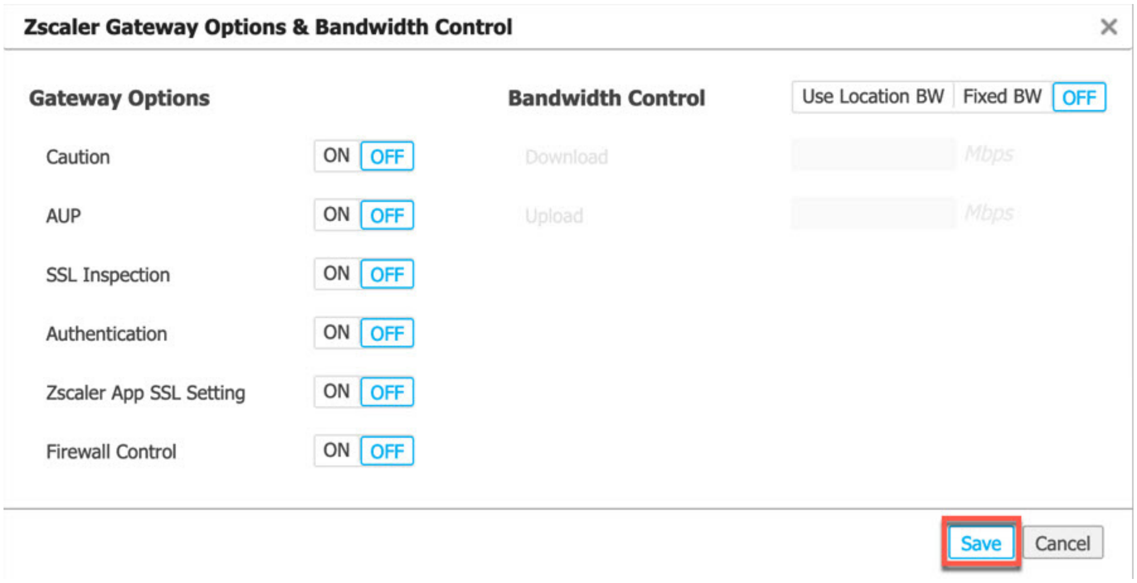
The **Zscaler Gateway Options** window appears.

Set Gateway Options

The **Gateway Options & Bandwidth Control** window allows you to enable or disable the sub-location gateway options.

Don't configure gateway options of features for which you do not have a ZIA subscription.

After selecting the gateway options, click **Save** and then click **Save** again in the main **Zscaler Gateway Options** window.



Zscaler Gateway Options & Bandwidth Control

Gateway Options

Caution: ON OFF

AUP: ON OFF

SSL Inspection: ON OFF

Authentication: ON OFF

Zscaler App SSL Setting: ON OFF

Firewall Control: ON OFF

Bandwidth Control: Use Location BW | Fixed BW | OFF

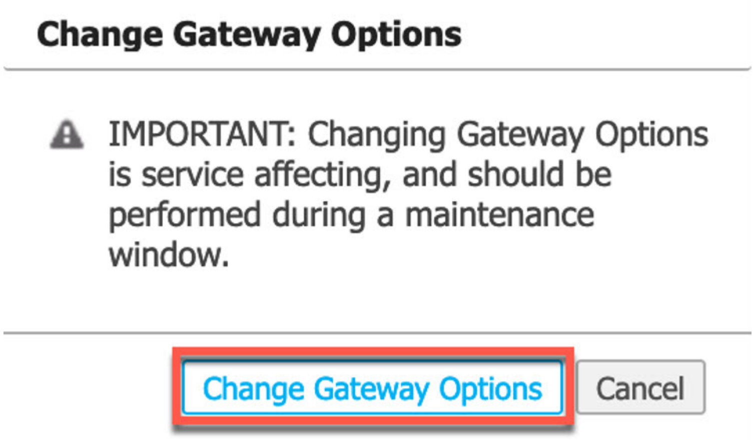
Download: Mbps

Upload: Mbps

Figure 40. *Set gateway options*

Change Gateway Options Confirmation

You see a confirmation window for the changed gateway options. Select **Change Gateway Options** to confirm your changes.



Change Gateway Options

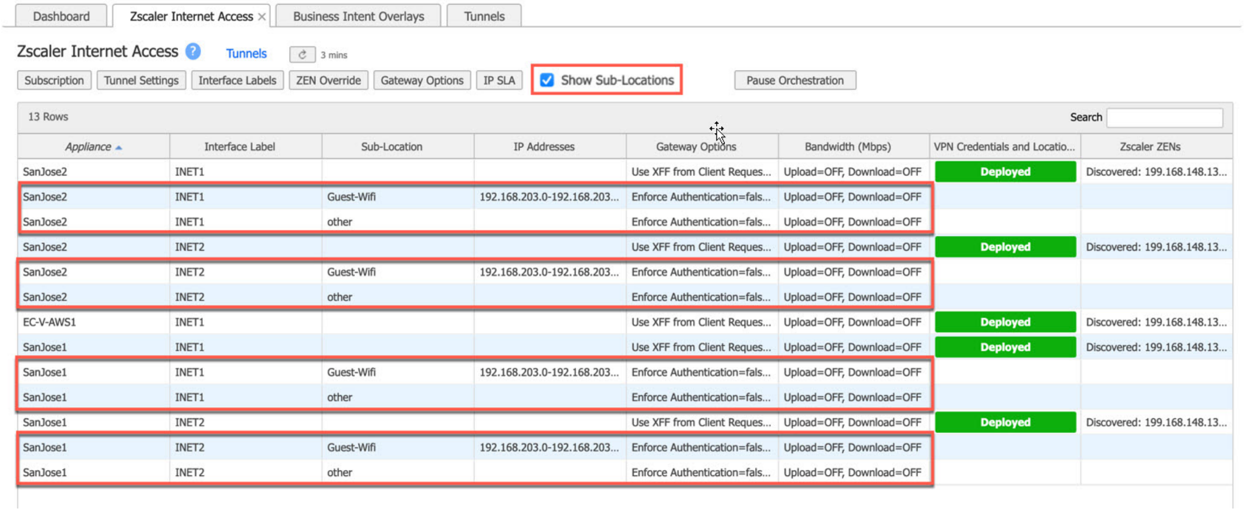
IMPORTANT: Changing Gateway Options is service affecting, and should be performed during a maintenance window.

Figure 41. *Change gateway options confirmation*

Verify Gateway Options

After applying the gateway options changes, select the **Show Sub-Locations** box.

After provisioning automation, the sub-locations and configure gateway options are applied to each tunnel.



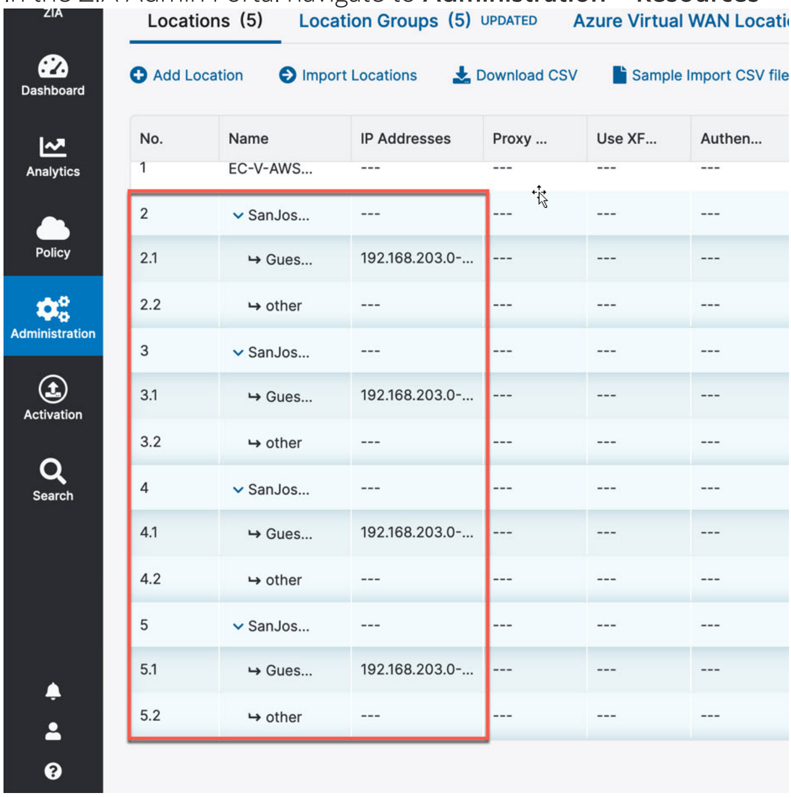
Appliance	Interface Label	Sub-Location	IP Addresses	Gateway Options	Bandwidth (Mbps)	VPN Credentials and Locatio...	Zscaler ZENs
SanJose2	INET1			Use XFF from Client Reques...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13...
SanJose2	INET1	Guest-Wifi	192.168.203.0-192.168.203...	Enforce Authentication=fals...	Upload=OFF, Download=OFF		
SanJose2	INET1	other		Enforce Authentication=fals...	Upload=OFF, Download=OFF		
SanJose2	INET2			Use XFF from Client Reques...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13...
SanJose2	INET2	Guest-Wifi	192.168.203.0-192.168.203...	Enforce Authentication=fals...	Upload=OFF, Download=OFF		
SanJose2	INET2	other		Enforce Authentication=fals...	Upload=OFF, Download=OFF		
EC-V-AWS1	INET1			Use XFF from Client Reques...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13...
SanJose1	INET1			Use XFF from Client Reques...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13...
SanJose1	INET1	Guest-Wifi	192.168.203.0-192.168.203...	Enforce Authentication=fals...	Upload=OFF, Download=OFF		
SanJose1	INET1	other		Enforce Authentication=fals...	Upload=OFF, Download=OFF		
SanJose1	INET2			Use XFF from Client Reques...	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13...
SanJose1	INET2	Guest-Wifi	192.168.203.0-192.168.203...	Enforce Authentication=fals...	Upload=OFF, Download=OFF		
SanJose1	INET2	other		Enforce Authentication=fals...	Upload=OFF, Download=OFF		

Figure 42. *Verify gateway options*

Verify Sub-Locations in ZIA

If you switch back to the ZIA Admin Portal, you can see the sub-locations configured by Aruba Orchestrator. If you select any of these sub-locations, you can view the gateway options configured by Aruba Orchestrator.

In the ZIA Admin Portal navigate to **Administration** > **Resources** > **Location Management**.



No.	Name	IP Addresses	Proxy ...	Use XF...	Authen...
1	EC-V-AWS...	---	---	---	---
2	SanJos...	---	---	---	---
2.1	↳ Gues...	192.168.203.0-...	---	---	---
2.2	↳ other	---	---	---	---
3	SanJos...	---	---	---	---
3.1	↳ Gues...	192.168.203.0-...	---	---	---
3.2	↳ other	---	---	---	---
4	SanJos...	---	---	---	---
4.1	↳ Gues...	192.168.203.0-...	---	---	---
4.2	↳ other	---	---	---	---
5	SanJos...	---	---	---	---
5.1	↳ Gues...	192.168.203.0-...	---	---	---
5.2	↳ other	---	---	---	---

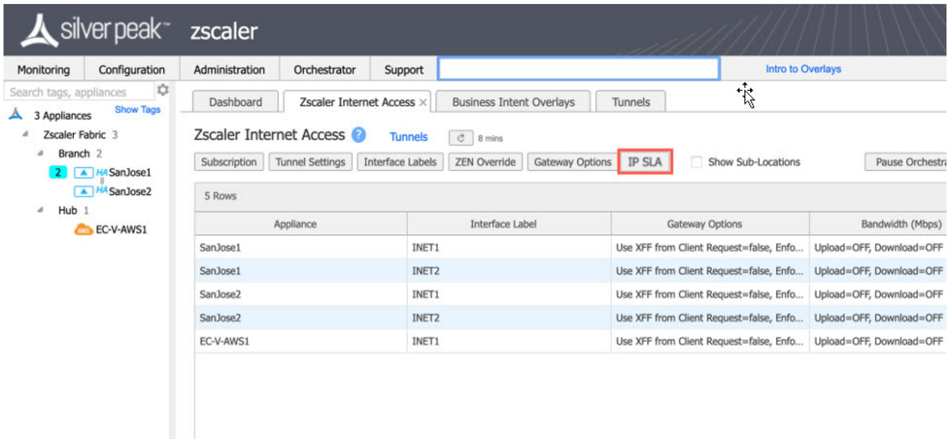
Figure 43. *Verify sub-locations in ZIA*

Configuring Layer-7 Health Checks for Automated Tunnels

This section configures Layer-7 health checks for automated tunnels.

Configuring Zscaler IP SLA

Access the IP SLA configuration in the **Zscaler Internet Access** tab. Click **IP SLA**.



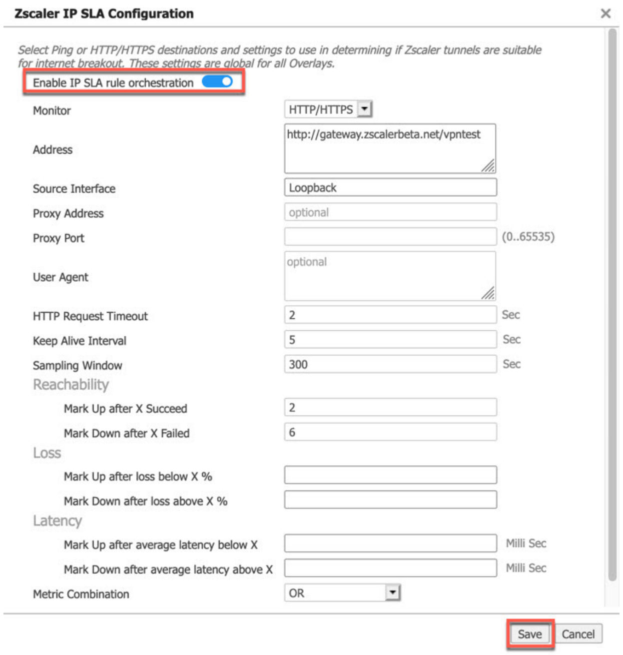
Appliance	Interface Label	Gateway Options	Bandwidth (Mbps)
SanJose1	INET1	Use XFF from Client Request=false, Enfo...	Upload=OFF, Download=OFF
SanJose1	INET2	Use XFF from Client Request=false, Enfo...	Upload=OFF, Download=OFF
SanJose2	INET1	Use XFF from Client Request=false, Enfo...	Upload=OFF, Download=OFF
SanJose2	INET2	Use XFF from Client Request=false, Enfo...	Upload=OFF, Download=OFF
EC-V-AWS1	INET1	Use XFF from Client Request=false, Enfo...	Upload=OFF, Download=OFF

Figure 44. *Configure IP SLA*

The **IP SLA Configuration** window appears.

Enable the IP SLA Probes for the Zscaler Tunnels

The **IP SLA Configuration** window appears. Click the toggle switch to enable service health checks through the Zscaler tunnels. The default values are already aligned to Zscaler recommendations, so click **Save**.



Zscaler IP SLA Configuration

Select Ping or HTTP/HTTPS destinations and settings to use in determining if Zscaler tunnels are suitable for internet breakout. These settings are global for all Overlays.

Enable IP SLA rule orchestration ●

Monitor	HTTP/HTTPS	
Address	http://gateway.zscalerbeta.net/vpntest	
Source Interface	Loopback	
Proxy Address	optional	
Proxy Port		(0..65535)
User Agent	optional	
HTTP Request Timeout	2	Sec
Keep Alive Interval	5	Sec
Sampling Window	300	Sec
Reachability		
Mark Up after X Succeed	2	
Mark Down after X Failed	6	
Loss		
Mark Up after loss below X %		
Mark Down after loss above X %		
Latency		
Mark Up after average latency below X		Milli Sec
Mark Down after average latency above X		Milli Sec
Metric Combination	OR	

Figure 45. *Edit the IP SLA rule*

The **Request Timeout** and **Keep Alive Interval** are recommendations. You might need to tune these values depending on your deployment.

Verify Zscaler IP SLA Rules

When configuring tunnels manually, you must also manually configure the IP SLA rules to validate the tunnel health.

Navigate to the IP SLA tab

1. Select the **IP SLA** option from the **Configuration Menu**.
2. Navigate to **Configuration** > **Templates and Policies** > **TCA** > **IP SLA**.

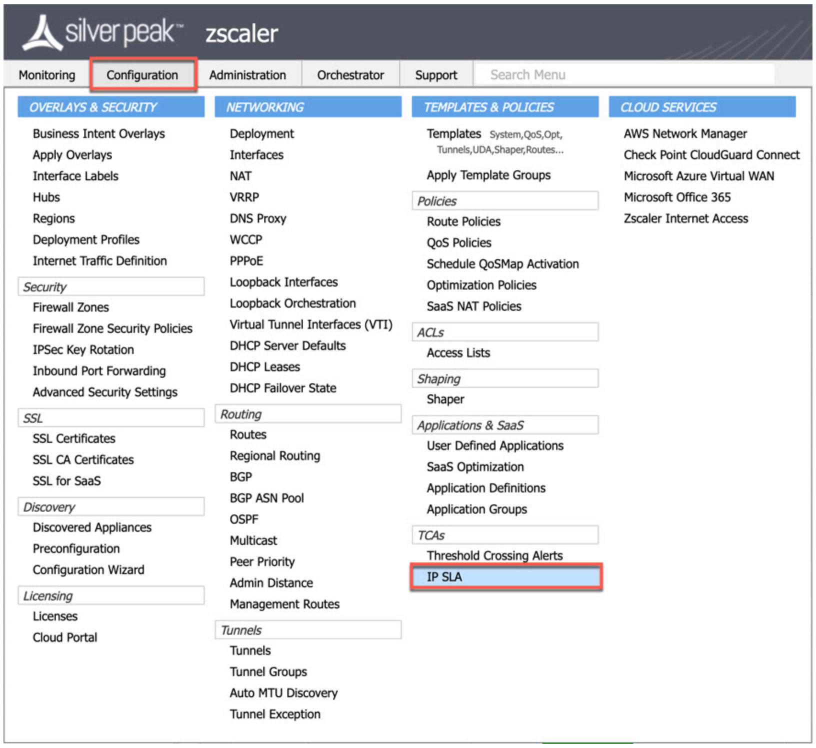
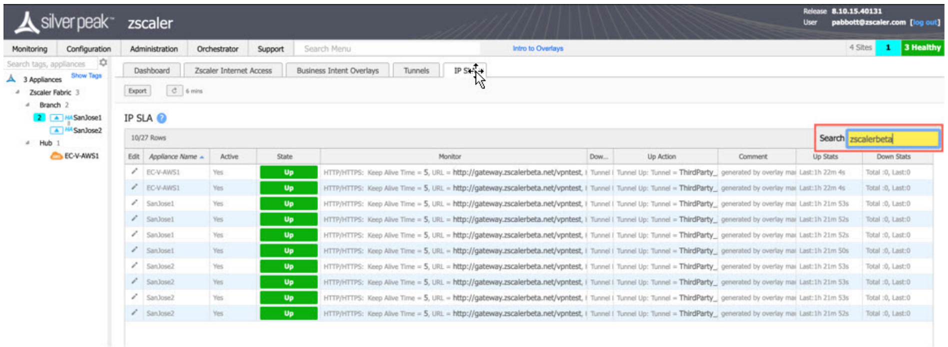


Figure 46. *Navigate to IP SLA settings*

Validate the Health Checks in the IP SLA Tab

You can filter and view the Zscaler IP SLA probes. Enter the ZIA cloud to which your tenant belongs.



10/27 Rows

Search zscalerbeta

Edit	Appliance Name	Active	State	Monitor	Dow...	Up Action	Comment	Up Stats	Down Stats
	EC-V-AWS1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 22m 4s	Total :0, Last:0
	EC-V-AWS1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 22m 4s	Total :0, Last:0
	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 53s	Total :0, Last:0
	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 52s	Total :0, Last:0
	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 52s	Total :0, Last:0
	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 50s	Total :0, Last:0
	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 53s	Total :0, Last:0
	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 53s	Total :0, Last:0
	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 53s	Total :0, Last:0
	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gateway.zscalerbeta.net/vpntest, I	Tunnel I	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mai	Last:1h 21m 52s	Total :0, Last:0

Figure 47. *Verify the IP SLA rule*

This filter shows only the health checks for Zscaler ZIA cloud.

Appendix A: Manual Tunnel Configuration

This appendix provides the steps for configuring ZIA tunnels manually. Both GRE and IPSec tunnels are covered.

Configuring Static IPs and GRE Tunnels

The ZIA Admin Portal now supports provisioning Static IPs for GRE tunnels. Support tickets are no longer required to setup GRE tunnels.

Navigate to **Administration** > **Resources** > **Static IPs & GRE Tunnels**.

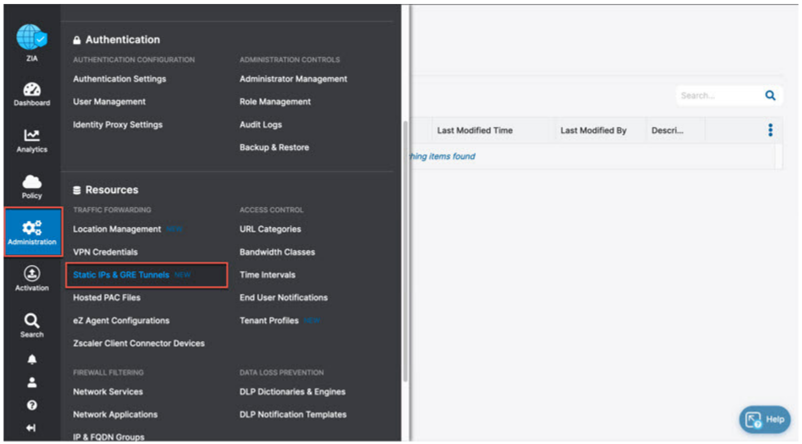
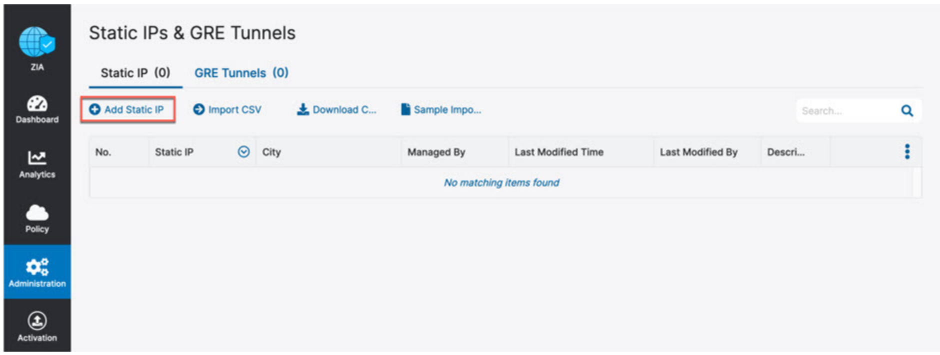


Figure 48. *Navigate to the static IPs and GRE tunnel configuration screen*

Add a Static IP Configuration

Click the **Add Static IP** selection from the page.



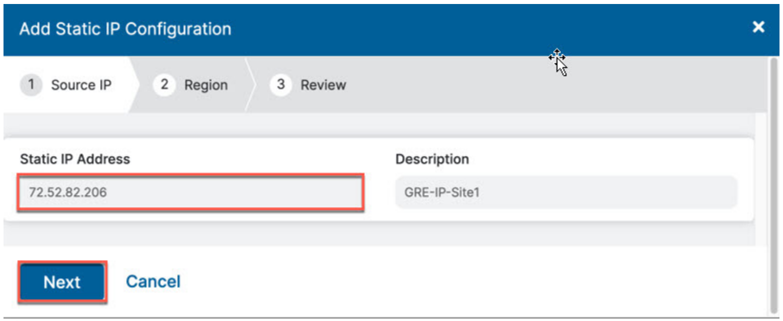
No.	Static IP	City	Managed By	Last Modified Time	Last Modified By	Descri...
No matching items found						

Figure 49. *Adding a static IP*

Enter the Static IP

In the **Add Static IP Configuration** window, complete the following steps:

1. Enter the public **Static IP Address** that initiates the tunnel connection.
2. Add a **Description**, if desired.



Static IP Address: 72.52.82.206

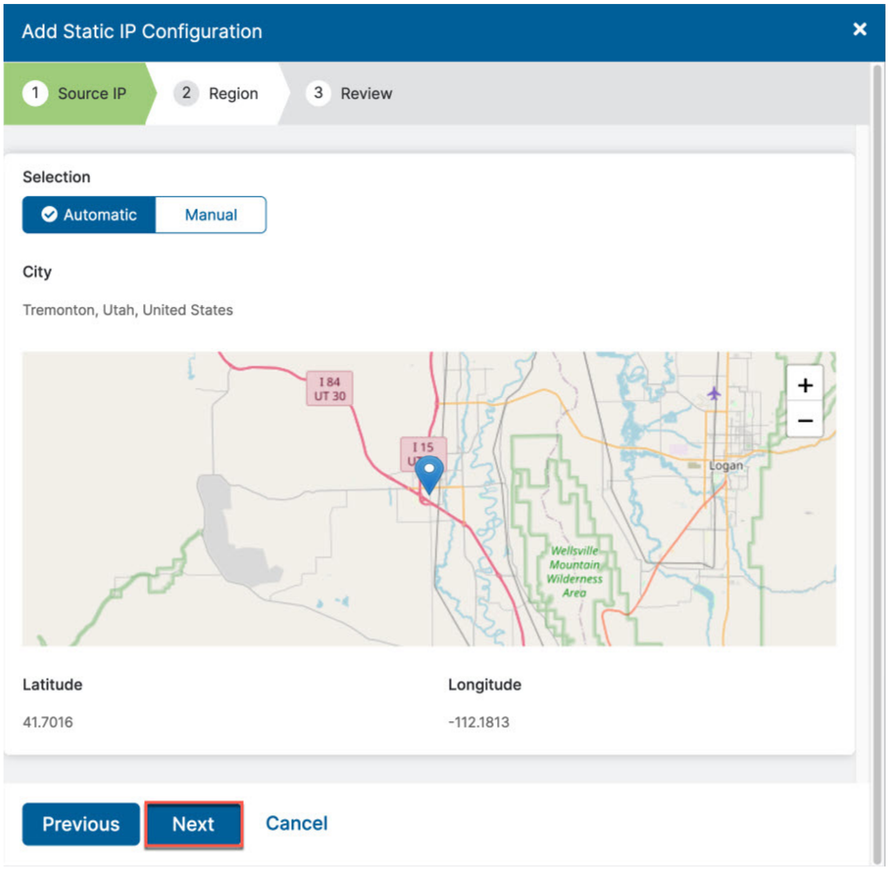
Description: GRE-IP-Site1

Figure 50. *Entering the static IP*

3. Click **Next** to continue.

Verify Geospatial Data

1. Verify that the geospatial location lookup is correct for the IP address entered. If not select **Manual** and enter the correct location data.
2. Click **Next**.



Selection: Automatic

City

Tremonton, Utah, United States

Latitude: 41.7016

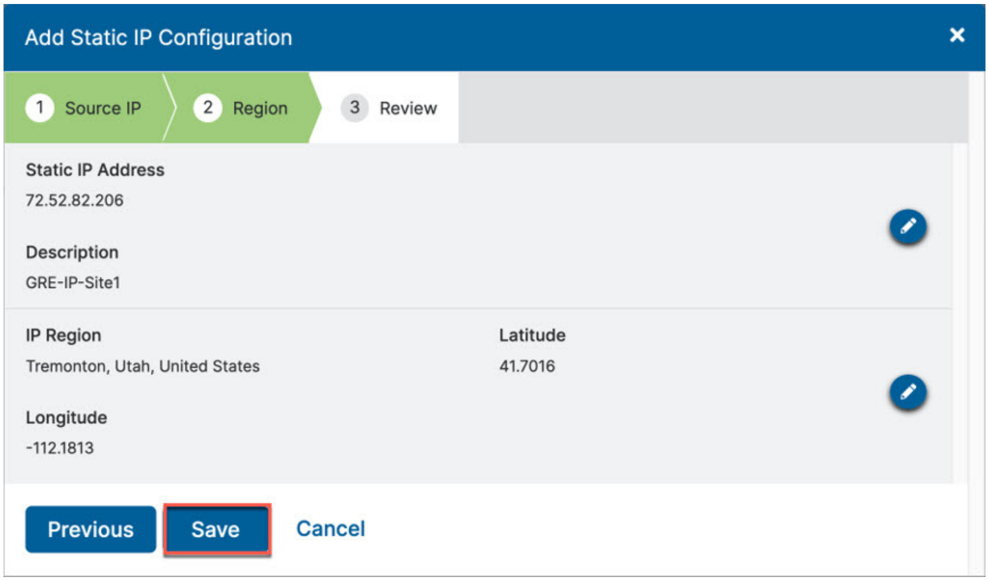
Longitude: -112.1813

Figure 51. *Verifying geospatial information*

The geospatial location information is used by the ZIA Central Authority to choose the best data centers for tunnel termination.

Review Information and Save

Review the information entered for the static IP and click **Save**.



Static IP Address
72.52.82.206

Description
GRE-IP-Site1

IP Region
Tremonton, Utah, United States

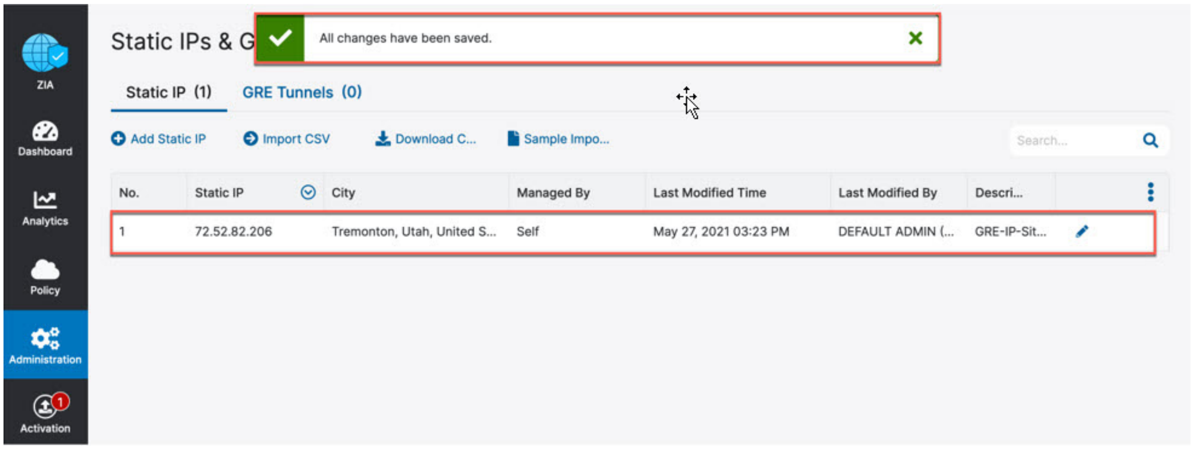
Latitude
41.7016

Longitude
-112.1813

Figure 52. *Review and save the static IP*

Validate that the Static IP Configuration is Saved

After you complete the Static IP provisioning and save the information, you see the message "All changes have been saved." The static IP is added to the list.



All changes have been saved.

No.	Static IP	City	Managed By	Last Modified Time	Last Modified By	Descri...
1	72.52.82.206	Tremonton, Utah, United S...	Self	May 27, 2021 03:23 PM	DEFAULT ADMIN (...	GRE-IP-Sit...

Figure 53. *Validate that the static IP was saved*

Next, complete the steps in Add a GRE Tunnel Configuration to assign the IP to a GRE tunnel.

Add a GRE Tunnel Configuration

Use the static IP that you created in section Add a Static IP Configuration to configure the GRE tunnel information.

Click the **GRE Tunnels tab** and then click **Add GRE Tunnel**:

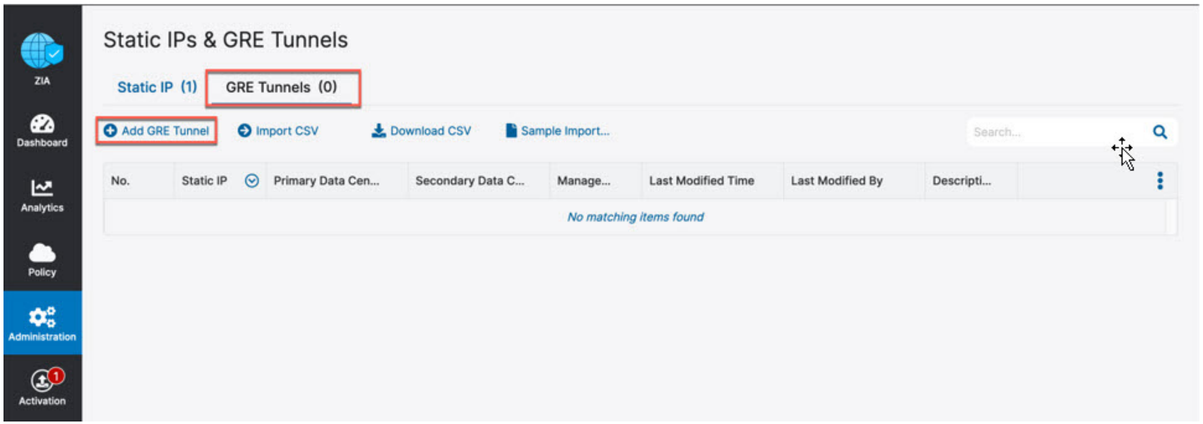
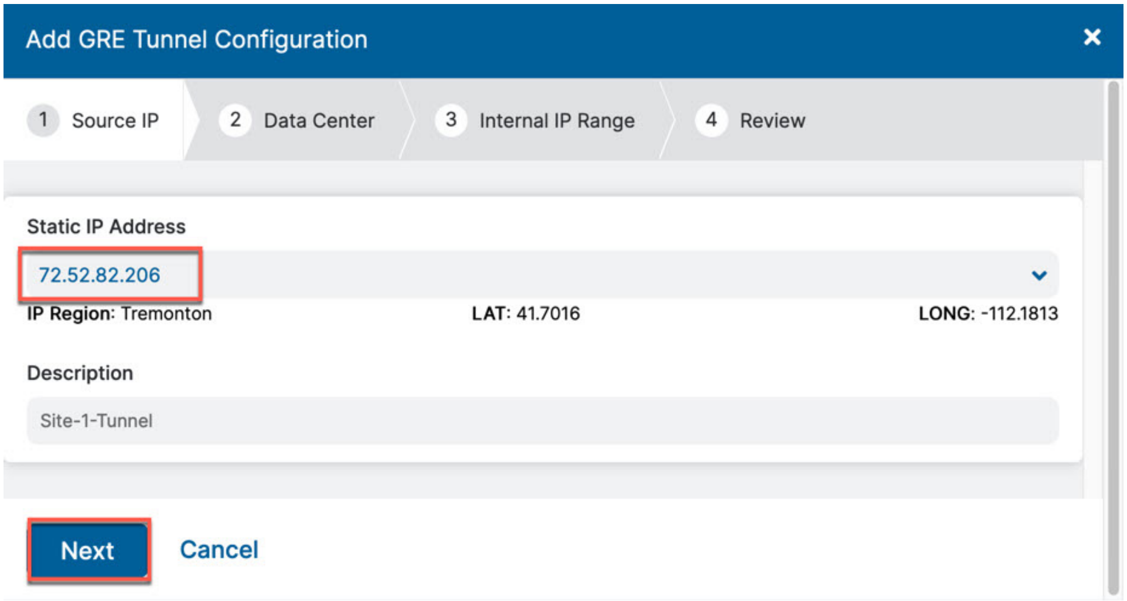


Figure 54. *Navigate to the GRE tunnel configuration screen*

Assign the Source IP to the Tunnel

1. In the **Add GRE Tunnel Configuration** window, choose the static IP address that is the GRE tunnel source.
2. Enter a **Description**, if desired.
3. Click **Next**.



Static IP Address: 72.52.82.206

IP Region: Tremonton LAT: 41.7016 LONG: -112.1813

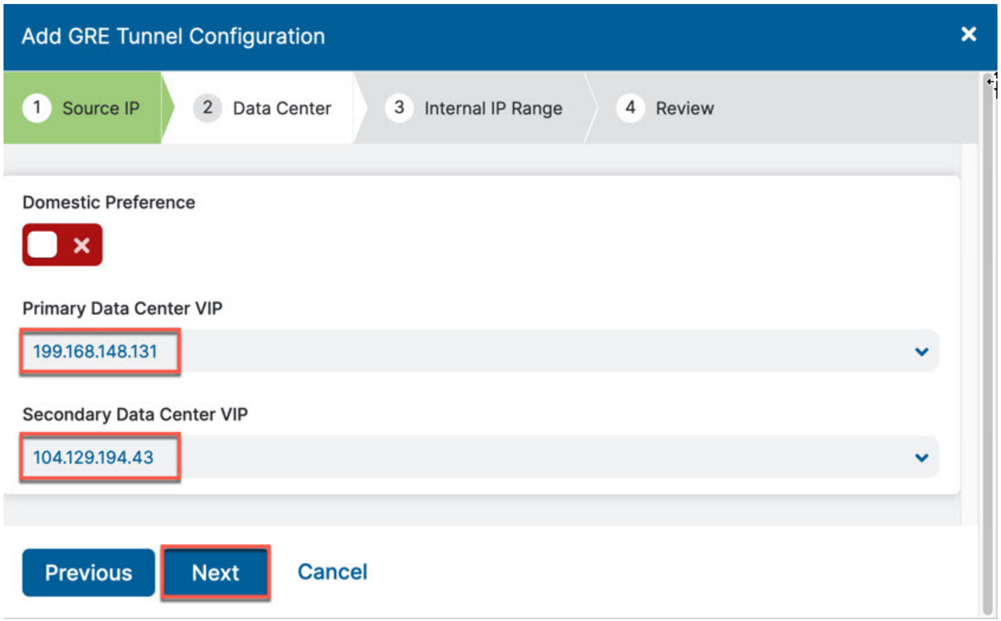
Description: Site-1-Tunnel

Figure 55. *Choose the GRE tunnel source IP*

Choose Data Centers for Tunnel Termination

With the geospatial information that was added from the static IP, the closest **Primary Data Center VIP** and **Secondary Data Center VIP** are chosen.

If you want to change these to different VIPs or DCs, select from the drop-down menu. Then click **Next**.



Add GRE Tunnel Configuration

Domestic Preference: ☒

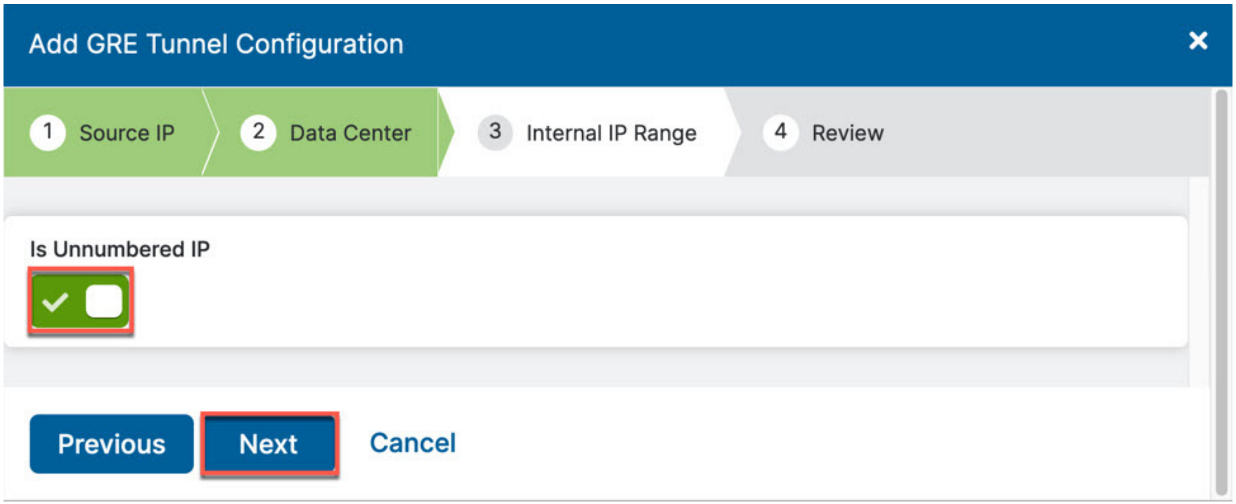
Primary Data Center VIP: 199.168.148.131

Secondary Data Center VIP: 104.129.194.43

Figure 56. *Choose the data centers for tunnel termination*

Select GRE Tunnel Internal IP Subnet

Aruba SD-WAN does not require IPs on their tunnel interfaces, so here simply enable **Is Unnumbered IP**. Click **Next** to review and save.



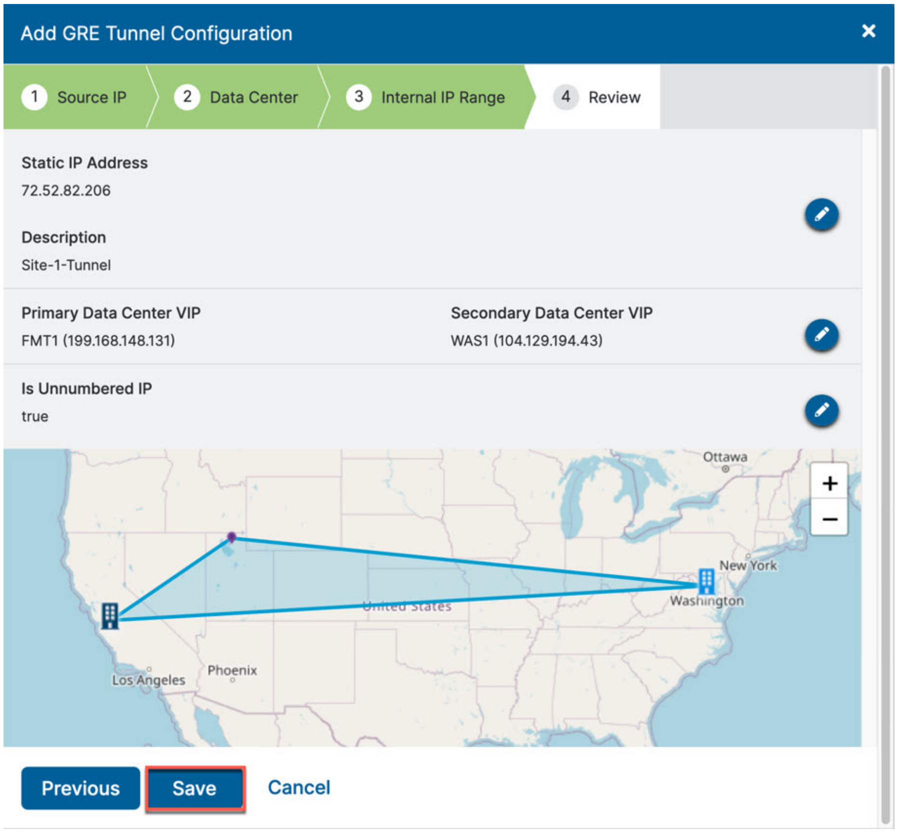
Add GRE Tunnel Configuration

Is Unnumbered IP: ✓

Figure 57. *Select the internal GRE IP range*

Save Tunnel Configuration

Review the configuration and click **Save**.



Add GRE Tunnel Configuration

1 Source IP | 2 Data Center | 3 Internal IP Range | 4 Review

Static IP Address
72.52.82.206

Description
Site-1-Tunnel

Primary Data Center VIP
FMT1 (199.168.148.131)

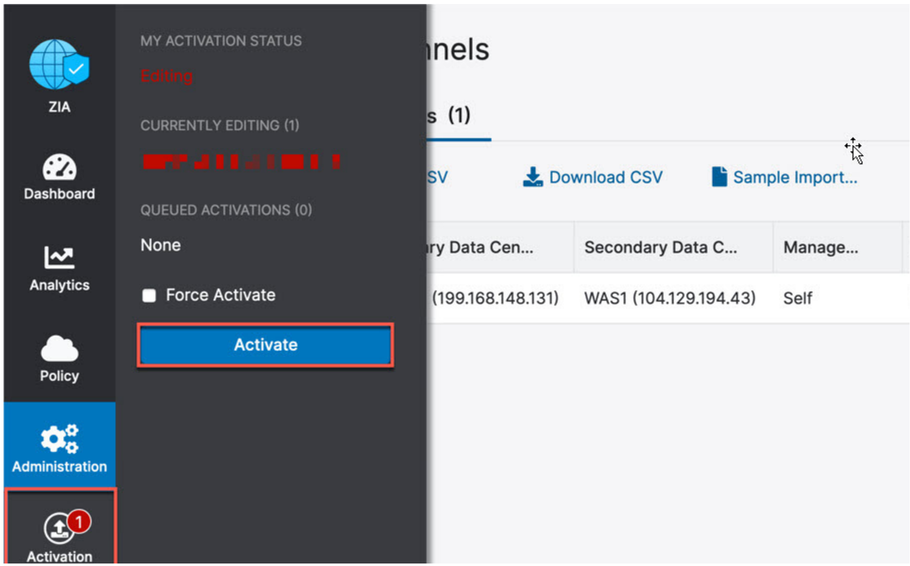
Secondary Data Center VIP
WAS1 (104.129.194.43)

Is Unnumbered IP
true

Figure 58. *Review and save the tunnel setup*

Activate and Verify All Configuration Changes

Finally, activate the saved configuration changes. Navigate to **Activation** and click **Activate** to activate the pending configurations.



MY ACTIVATION STATUS
Editing

CURRENTLY EDITING (1)
[redacted]

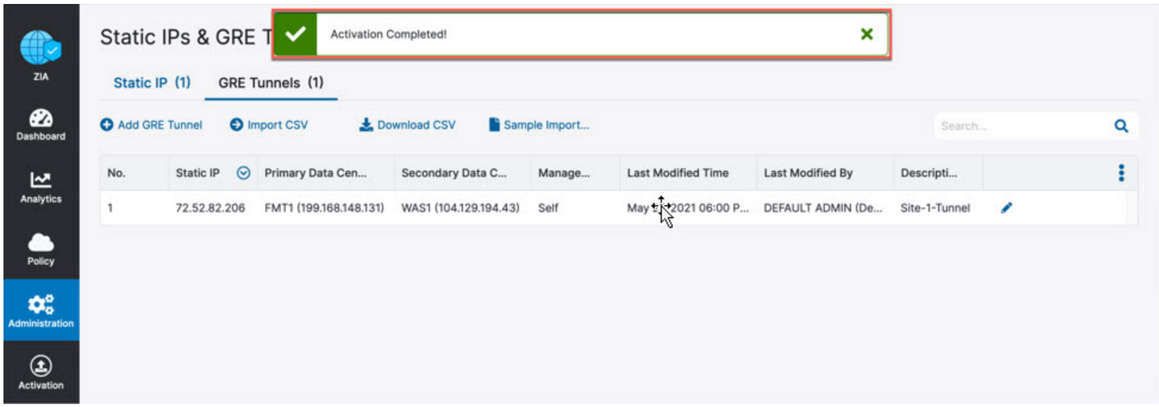
QUEUED ACTIVATIONS (0)
None

□ Force Activate

...ry Data Cen...	Secondary Data C...	Manage...
(199.168.148.131)	WAS1 (104.129.194.43)	Self

Figure 59. *Activate the GRE tunnel configuration*

The message **Activation Completed!** appears to indicate that your changes are live.



Activation Completed!

No.	Static IP	Primary Data Cen...	Secondary Data C...	Manage...	Last Modified Time	Last Modified By	Descripti...
1	72.52.82.206	FMT1 (199.168.148.131)	WAS1 (104.129.194.43)	Self	May [illegible] 2021 06:00 P...	DEFAULT ADMIN (De...	Site-1-Tunnel

Figure 60. *Verify that the GRE tunnel configuration was activated*

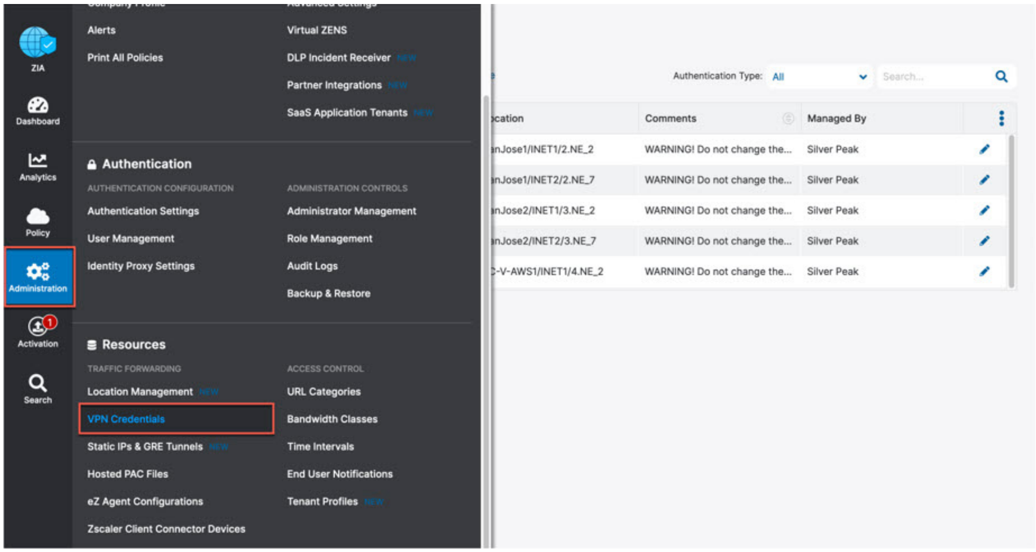
Adding VPN Credentials for Manual IPSec Tunnels

This section demonstrates how to add VPN credentials for manual IPSec tunnels.

Navigate to VPN Credentials

The first step in configuring an IPSec tunnel is to create a VPN credential in ZIA. The **VPN Credential** section creates a FQDN and Pre-Shared Key (PSK) for our IPSec session.

Navigate to **Administration** > **Resources** > **VPN Credentials**.

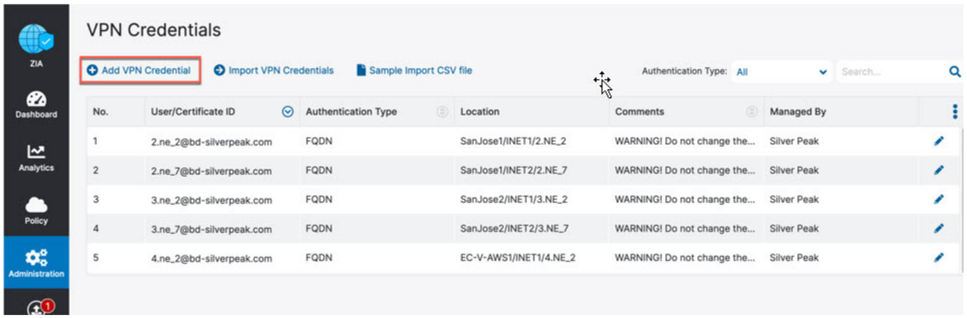


›cation	Comments	Managed By
›nJose1/INET1/2.NE_2	WARNING! Do not change the...	Silver Peak
›nJose1/INET2/2.NE_7	WARNING! Do not change the...	Silver Peak
›nJose2/INET1/3.NE_2	WARNING! Do not change the...	Silver Peak
›nJose2/INET2/3.NE_7	WARNING! Do not change the...	Silver Peak
C-V-AWS1/INET1/4.NE_2	WARNING! Do not change the...	Silver Peak

Figure 61. *Navigate to VPN credentials*

Add a VPN Credential

If you see **No Matching Items Found**, your ZIA instance does not have any VPN credentials configured. To add a VPN credential, click **Add VPN Credential** in the red box in the upper left.



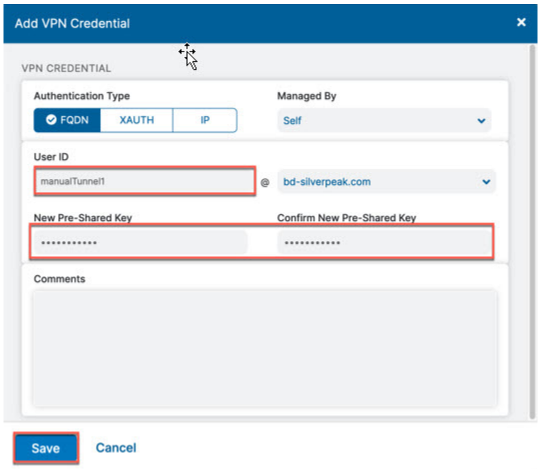
No.	User/Certificate ID	Authentication Type	Location	Comments	Managed By
1	2.ne_2@bd-silverpeak.com	FQDN	SanJose1/INET1/2.NE_2	WARNING! Do not change the...	Silver Peak
2	2.ne_7@bd-silverpeak.com	FQDN	SanJose1/INET2/2.NE_7	WARNING! Do not change the...	Silver Peak
3	3.ne_2@bd-silverpeak.com	FQDN	SanJose2/INET1/3.NE_2	WARNING! Do not change the...	Silver Peak
4	3.ne_7@bd-silverpeak.com	FQDN	SanJose2/INET2/3.NE_7	WARNING! Do not change the...	Silver Peak
5	4.ne_2@bd-silverpeak.com	FQDN	EC-V-AWS1/INET1/4.NE_2	WARNING! Do not change the...	Silver Peak

Figure 62. *Adding a VPN credential*

Enter VPN Credential Data

In the **Add VPN Credential** window, configure the **FQDN** and **Pre-Shared Key (PSK) for IKE**. You need to configure only the username portion of the FQDN, because the domain name is automatically added to the right of the name.

After configuring both the FQDN and PSK, click **Save** to continue.



Add VPN Credential

VPN CREDENTIAL

Authentication Type: FQDN

Managed By: Self

User ID: manualTunnel1 @ bd-silverpeak.com

New Pre-Shared Key: •••••••••••

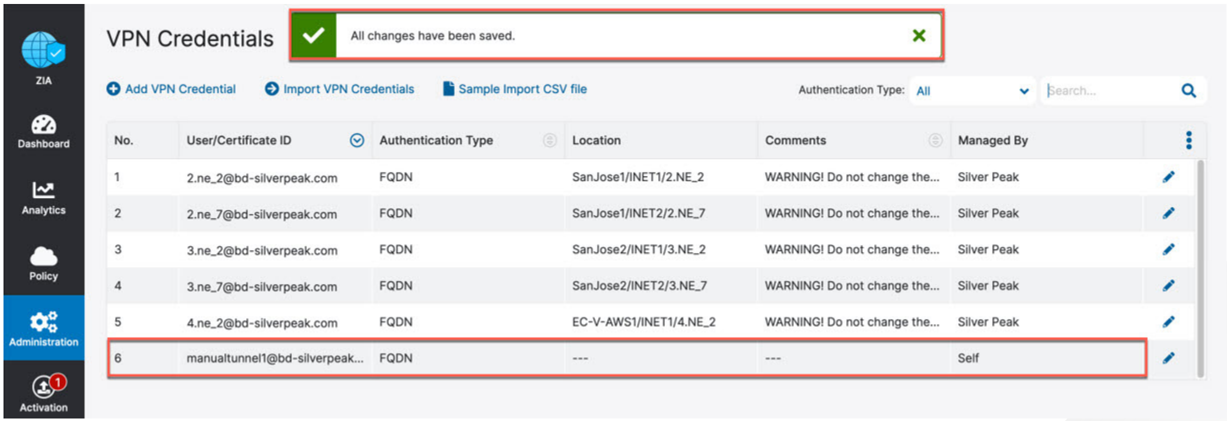
Confirm New Pre-Shared Key: •••••••••••

Comments

Figure 63. *Enter VPN credential data*

Verify VPN Credential

After you save the VPN credential, you see the message, **All changes have been saved**, in the top center of your screen. The VPN credential is shown underneath.



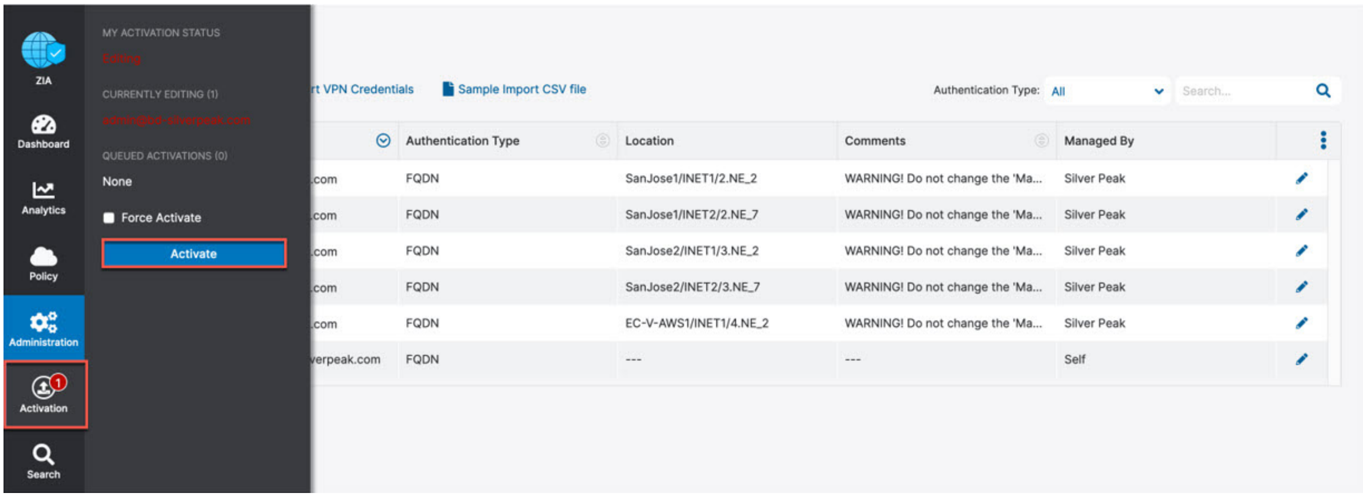
All changes have been saved.

No.	User/Certificate ID	Authentication Type	Location	Comments	Managed By
1	2.ne_2@bd-silverpeak.com	FQDN	SanJose1/INET1/2.NE_2	WARNING! Do not change the...	Silver Peak
2	2.ne_7@bd-silverpeak.com	FQDN	SanJose1/INET2/2.NE_7	WARNING! Do not change the...	Silver Peak
3	3.ne_2@bd-silverpeak.com	FQDN	SanJose2/INET1/3.NE_2	WARNING! Do not change the...	Silver Peak
4	3.ne_7@bd-silverpeak.com	FQDN	SanJose2/INET2/3.NE_7	WARNING! Do not change the...	Silver Peak
5	4.ne_2@bd-silverpeak.com	FQDN	EC-V-AWS1/INET1/4.NE_2	WARNING! Do not change the...	Silver Peak
6	manualtunnel1@bd-silverpeak...	FQDN	---	---	Self

Figure 64. *Verify location information and save*

Activate Pending Changes

Now save the changes. Navigate to **Activation** and click **Activate** to activate the pending configurations.



MY ACTIVATION STATUS

Editing

CURRENTLY EDITING (1)

admin@bd-silverpeak.com

QUEUED ACTIVATIONS (0)

None

□ Force Activate

Activate

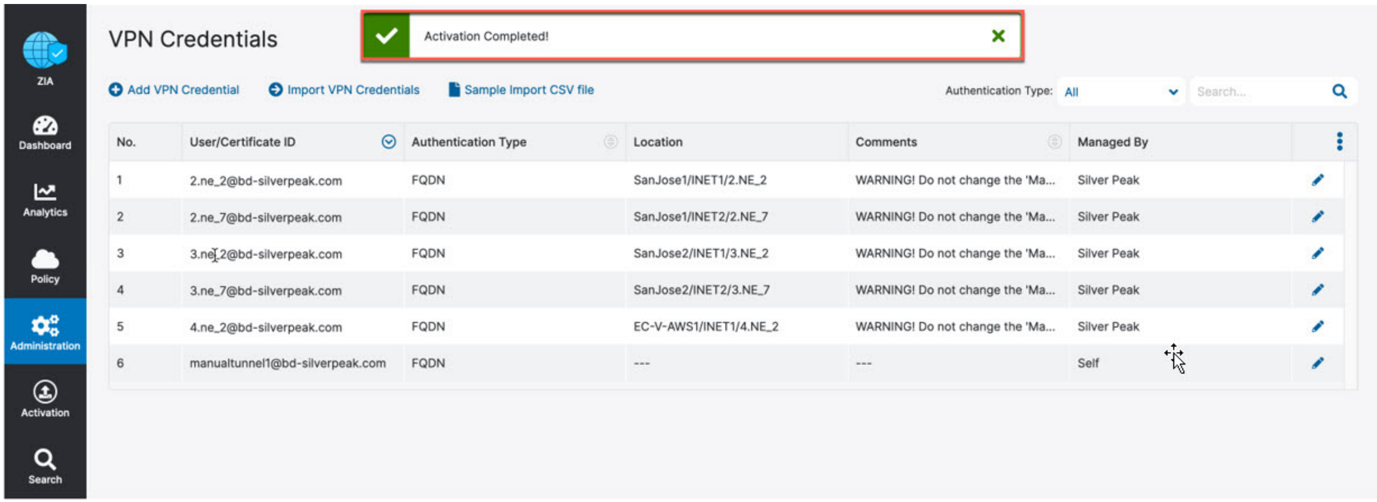
	Authentication Type	Location	Comments	Managed By
.com	FQDN	SanJose1/INET1/2.NE_2	WARNING! Do not change the 'Ma...	Silver Peak
.com	FQDN	SanJose1/INET2/2.NE_7	WARNING! Do not change the 'Ma...	Silver Peak
.com	FQDN	SanJose2/INET1/3.NE_2	WARNING! Do not change the 'Ma...	Silver Peak
.com	FQDN	SanJose2/INET2/3.NE_7	WARNING! Do not change the 'Ma...	Silver Peak
.com	FQDN	EC-V-AWS1/INET1/4.NE_2	WARNING! Do not change the 'Ma...	Silver Peak
erpeak.com	FQDN	---	---	Self

Figure 65. *Activate pending changes*

Verify the Activation

After you activate the pending changes, return to the prior page.

You see the message **Activation Completed** at the top of the window.



VPN Credentials

Activation Completed!

No.	User/Certificate ID	Authentication Type	Location	Comments	Managed By
1	2.ne_2@bd-silverpeak.com	FQDN	SanJose1/INET1/2.NE_2	WARNING! Do not change the 'Ma...	Silver Peak
2	2.ne_7@bd-silverpeak.com	FQDN	SanJose1/INET2/2.NE_7	WARNING! Do not change the 'Ma...	Silver Peak
3	3.ne_2@bd-silverpeak.com	FQDN	SanJose2/INET1/3.NE_2	WARNING! Do not change the 'Ma...	Silver Peak
4	3.ne_7@bd-silverpeak.com	FQDN	SanJose2/INET2/3.NE_7	WARNING! Do not change the 'Ma...	Silver Peak
5	4.ne_2@bd-silverpeak.com	FQDN	EC-V-AWS1/INET1/4.NE_2	WARNING! Do not change the 'Ma...	Silver Peak
6	manualtunnel1@bd-silverpeak.com	FQDN	---	---	Self

Figure 66. *Verify the activation*

Configuring a Location for Manual Tunnels

You must specify a location for the tunnel to access ZIA, if one is not present. If you aren't sure if you have a site configured, the following steps verify that a location is present.

Navigate to **Administration** > **Resources** > **Location Management**.

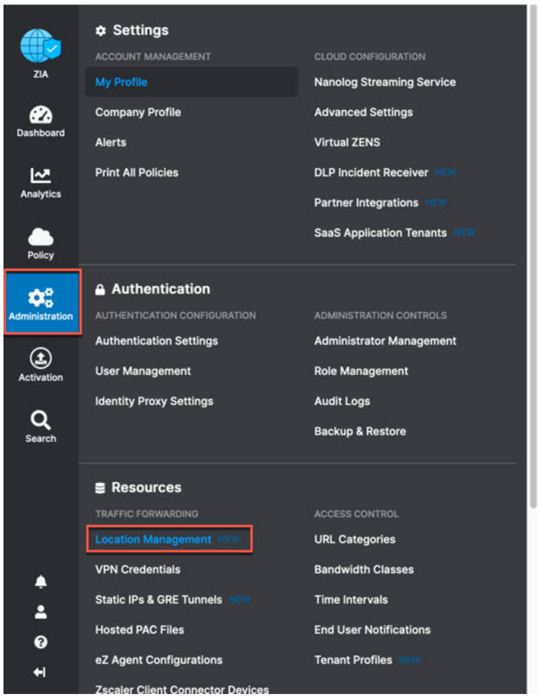
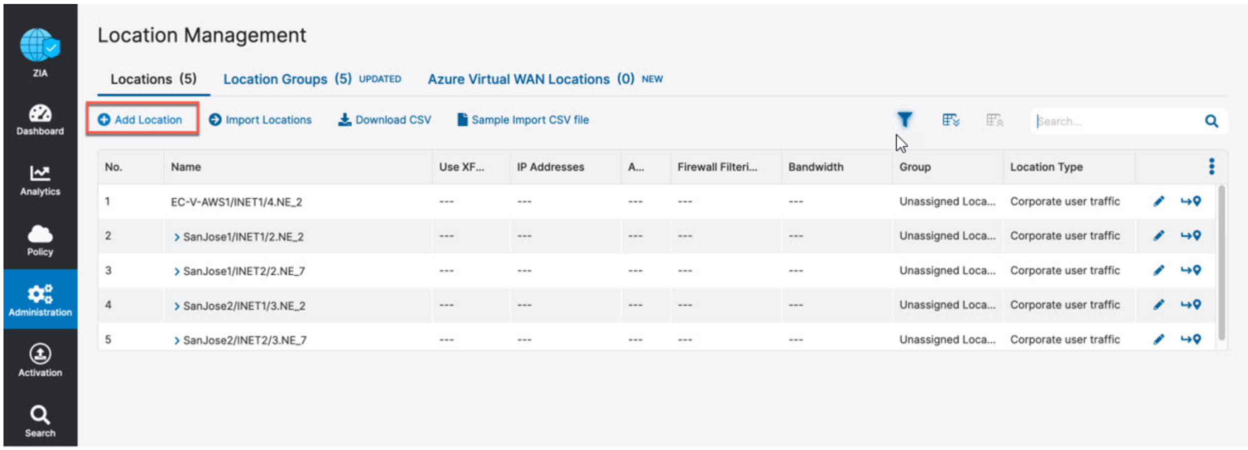


Figure 67. *Navigate to locations*

Add a Location

If you see the message **No Matching Items Found** then your ZIA instance does not have any locations configured.

To add a location, click **Add Location**. To edit any existing locations, click the **Edit** icon to the far right of the listed location.



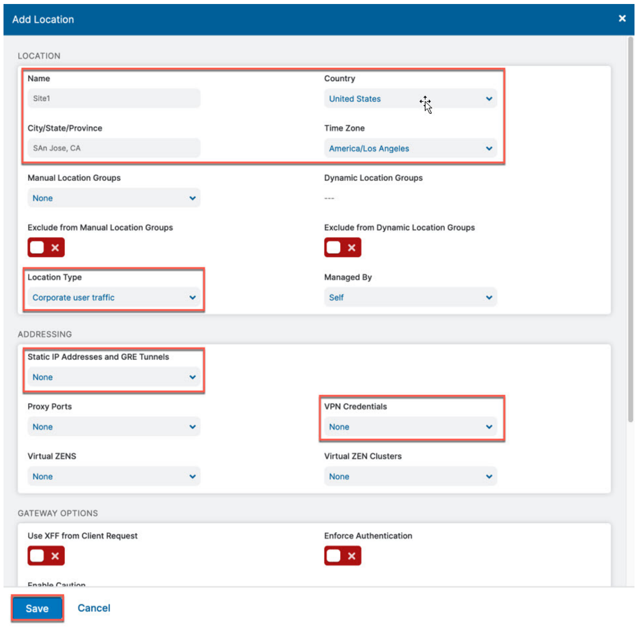
No.	Name	Use XF...	IP Addresses	A...	Firewall Filteri...	Bandwidth	Group	Location Type
1	EC-V-AWS1/INET1/4.NE_2	---	---	---	---	---	Unassigned Loca...	Corporate user traffic
2	> SanJose1/INET1/2.NE_2	---	---	---	---	---	Unassigned Loca...	Corporate user traffic
3	> SanJose1/INET2/2.NE_7	---	---	---	---	---	Unassigned Loca...	Corporate user traffic
4	> SanJose2/INET1/3.NE_2	---	---	---	---	---	Unassigned Loca...	Corporate user traffic
5	> SanJose2/INET2/3.NE_7	---	---	---	---	---	Unassigned Loca...	Corporate user traffic

Figure 68. *Add a location*

Enter the Location Data

Complete the fields.

1. The name of the location is used as a policy object within ZIA.
2. In the **Managed By** field, you can leave “Self”, which is used for administration through the web interface.
3. You need to choose a **Location Type** for the location as well.
4. Choose the appropriate **Location Group**, typically it is Corporate user traffic. For more information, see the online help section: [About Location Groups](#).


Add Location

LOCATION

Name: Site1
Country: United States
City/State/Province: SAn Jose, CA
Time Zone: America/Los Angeles
Manual Location Groups: None
Dynamic Location Groups: ---
Exclude from Manual Location Groups: ✕
Exclude from Dynamic Location Groups: ✕
Location Type: Corporate user traffic
Managed By: Self

ADDRESSING

Static IP Addresses and GRE Tunnels: None
Proxy Ports: None
VPN Credentials: None
Virtual ZENS: None
Virtual ZEN Clusters: None

GATEWAY OPTIONS

Use XFF from Client Request: ✕
Enforce Authentication: ✕
Enable Caution

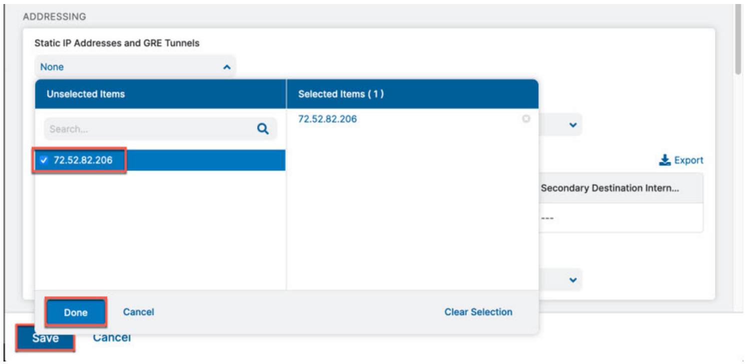
Figure 69. *Enter the location data*

You must enter either **Static IP Address(es)** or **VPN Credentials** to ensure the traffic incoming from the tunnels is mapped to the proper tenant policy. Add either the static IP address for GRE tunnels or VPN credentials if you use a manually created IPSec tunnel based on your needs as shown in the next two steps.

Add Static IP and GRE Tunnel to Location

The **Static IP Addresses and GRE Tunnels** dialog window shows the static IP you configured in section [Add a Static IP Configuration](#) and linked to a GRE tunnel in section [Add a GRE Tunnel Configuration](#).

1. Select the static IP and click **Done**. The static IP and traffic arriving on the GRE tunnel assigned are linked to this location.
2. When finished, click **Save** to continue.


ADDRESSING

Static IP Addresses and GRE Tunnels: None

Unselected Items: ☑ 72.52.82.206
Selected Items (1): 72.52.82.206

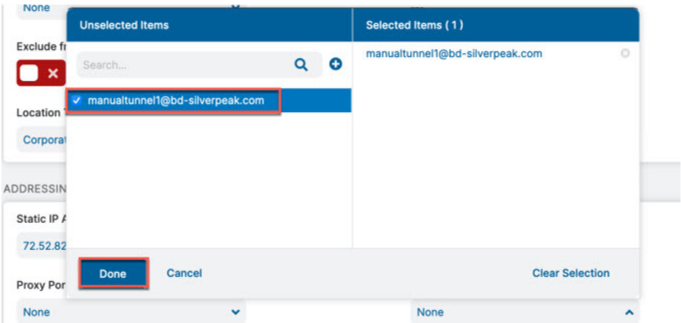
Secondary Destination Intern...: ---

Figure 70. *Select the static IP linked to the location*

Adding a VPN Credential to a Location

In the VPN credential dialog window, you can see the VPN credential you configured in the section Adding VPN Credentials for Manual IPSec Tunnels.

1. Select the VPN credential and click **Done**.
2. After you save the location, the location is coupled with the VPN credential.
3. When you have competed the fields, click **Save** to continue



Unselected Items

Search...

☑ manualtunnel1@bd-silverpeak.com

Selected Items (1)

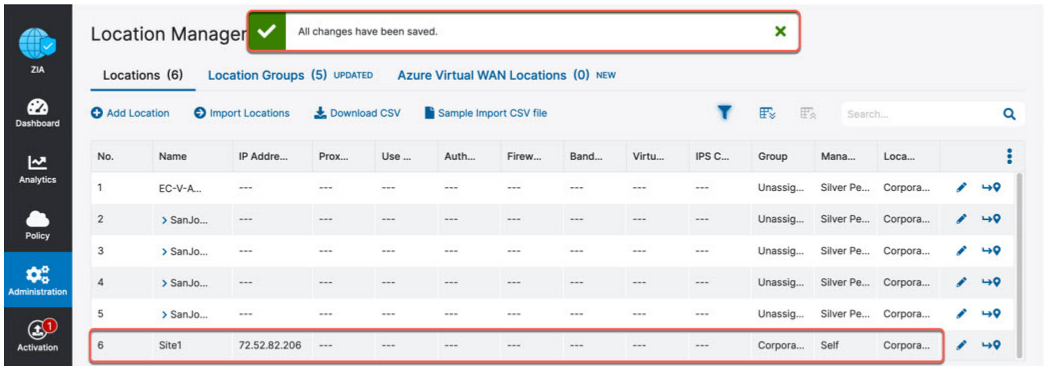
manualtunnel1@bd-silverpeak.com

Done | Cancel | Clear Selection

Figure 71. *Add VPN credential to location and save*

Confirm Changes Have Been Saved

The Location Manager shows the message **All changes have been saved** displayed in the top center of the screen after saving the location. The location is shown underneath.



Location Manager

All changes have been saved.

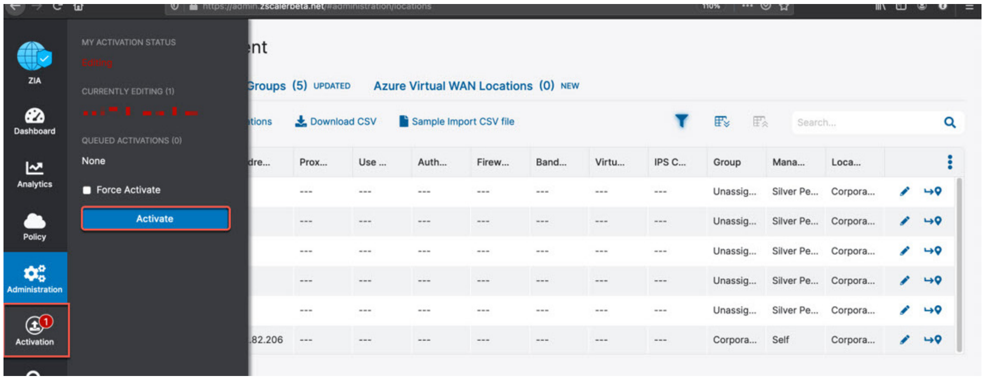
Locations (6) | Location Groups (5) UPDATED | Azure Virtual WAN Locations (0) NEW

No.	Name	IP Addre...	Prox...	Use ...	Auth...	Firew...	Band...	Virtu...	IPS C...	Group	Mana...	Loca...
1	EC-V-A...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
2	> SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
3	> SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
4	> SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
5	> SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
6	Site1	72.52.82.206	---	---	---	---	---	---	---	Corpora...	Self	Corpora...

Figure 72. *Confirm the changes have been saved*

Activate Pending Changes

Whenever you make a change in ZIA, you see a number over the **Activation** icon on the left-hand side menu.



MY ACTIVATION STATUS

Editing

CURRENTLY EDITING (1)

[redacted]

QUEUED ACTIVATIONS (0)

None

□ Force Activate

Activate

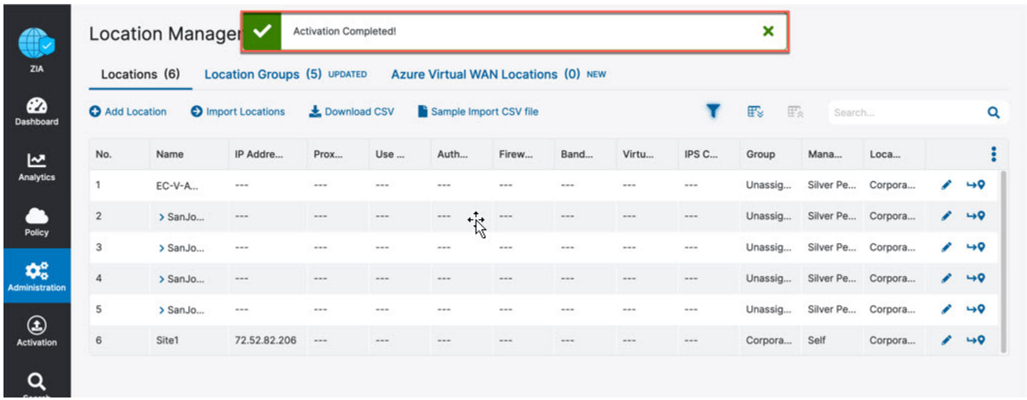
dre...	Prox...	Use ...	Auth...	Firew...	Band...	Virtu...	IPS C...	Group	Mana...	Loca...
	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
.82.206	---	---	---	---	---	---	---	Corpora...	Self	Corpora...

Figure 73. *Activate changes*

The number indicates you have changes pending in queue for activation. When you are ready to activate all changes in queue, click **Activate**.

Activation Confirmation

After you activate all pending changes, you see the message, **Activation Completed!**. At this point, all queued changes have been pushed into production. The changes take effect within seconds.



Location Manager

Activation Completed!

Locations (6) · Location Groups (5) UPDATED · Azure Virtual WAN Locations (0) NEW

No.	Name	IP Addre...	Prox...	Use ...	Auth...	Firew...	Band...	Virtu...	IPS C...	Group	Mana...	Loca...
1	EC-V-A...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
2	› SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
3	› SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
4	› SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
5	› SanJo...	---	---	---	---	---	---	---	---	Unassig...	Silver Pe...	Corpora...
6	Site1	72.52.82.206	---	---	---	---	---	---	---	Corpora...	Self	Corpora...

Figure 74. *Activation confirmation*

Now that you have defined a public IP associated to the location, you can start configuring the Aruba SD-WAN side

Manually Configure Tunnels on Aruba Orchestrator

Refer to Aruba Overview for links to the Aruba SD-WAN documentation. Refer to the documentation to manually configure IPSec and GRE tunnels in Aruba Orchestrator.

Appendix B: Configuring Layer-7 Health Checks for Manually Created Tunnels

This appendix describes configuring Layer-7 health checks for manually created tunnels.

Configuring Aruba SD-WAN IP SLA

Navigate to **Configuration** > **Templates & Policies** > **TCA** > **IP SLA**.

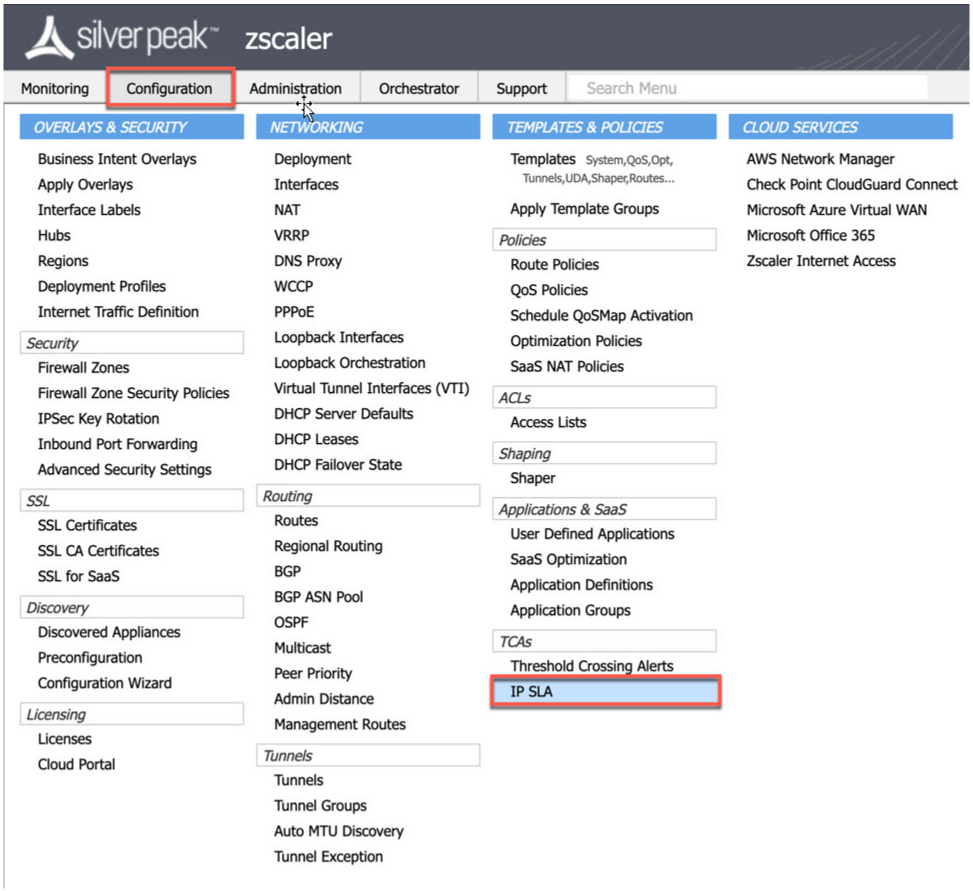
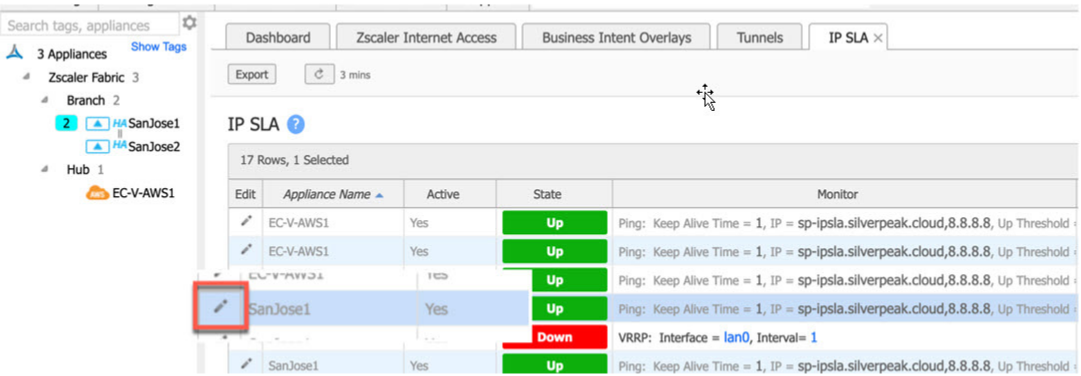


Figure 75. *Configure IP SLA*

Edit EdgeConnect IPSLA Rules

Click the **Edit** icon on the **IP SLA** tab for the appliance on which you want to configure the health check.



IP SLA

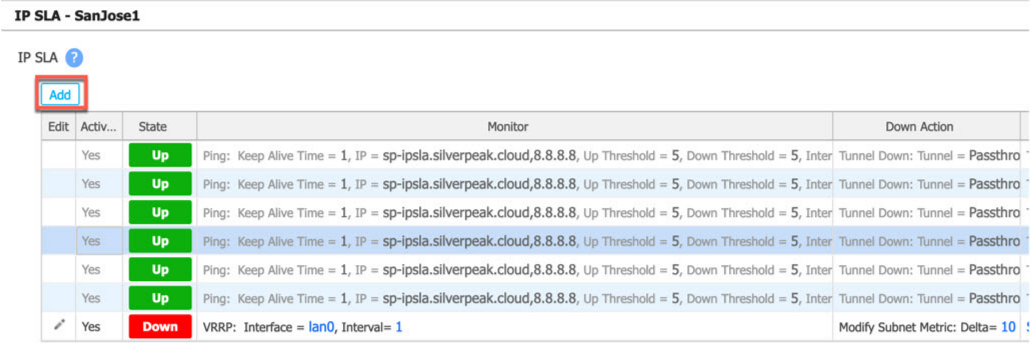
17 Rows, 1 Selected

Edit	Appliance Name	Active	State	Monitor
✎	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
✎	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
			Down	VRRP: Interface = lan0, Interval= 1
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold

Figure 76. *Edit the IP SLA rule*

Add Rule and Target

Click **Add** to create a new HTTP and HTTPS rule.



Edit	Activ...	State	Monitor	Down Action
	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
✎	Yes	Down	VRRP: Interface = lan0, Interval= 1	Modify Subnet Metric: Delta= 10

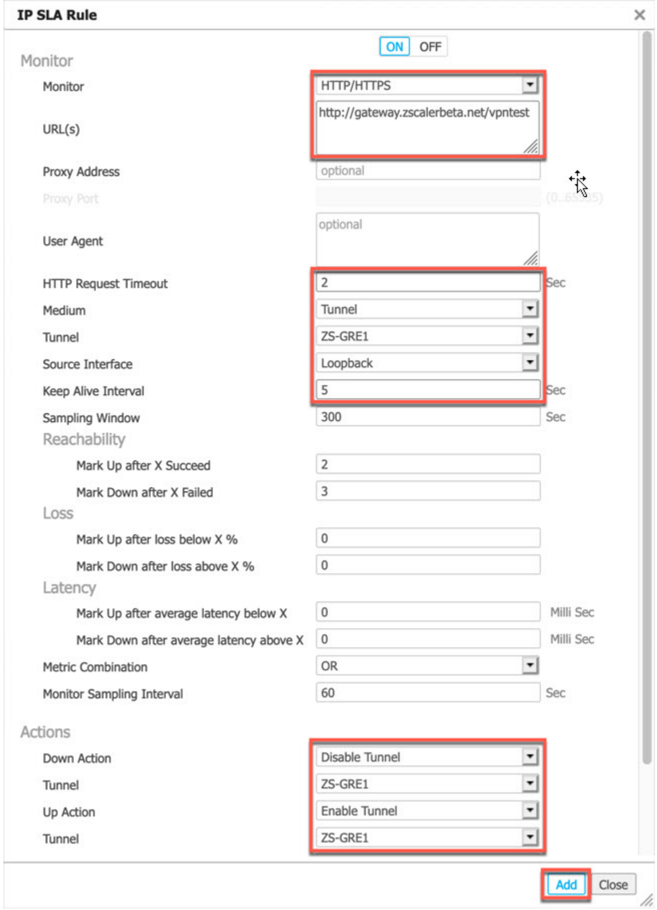
Figure 77. *Add rule and target*

Configure IP SLA Rule

Configure the IP SLA rule as follows:

Setting	Value
URL(s)	http://gateway.<cloud>.net/vpntest, replace <cloud> with your ZIA tenant cloud. Refer to the Monitoring GRE Tunnels (government agencies, see Monitoring GRE Tunnels) section for details.
HTTP Request Timeout	2 seconds
Medium	Tunnel
Tunnel	Choose the GRE tunnel that you want to monitor
Source Interface	Choose the **Loopback** interface
Keep Alive Interval	5 seconds
Down Action	Disable Tunnel
Tunnel	Tunnel from the **Medium** field
Up Action	Enable Tunnel
Tunnel	Tunnel from the **Medium** field
Down Action	Disable Tunnel

Request Timeout and **Keep Alive Interval** are recommendations. Tuning these values might be required, depending on your deployment.



IP SLA Rule

ON OFF

Monitor

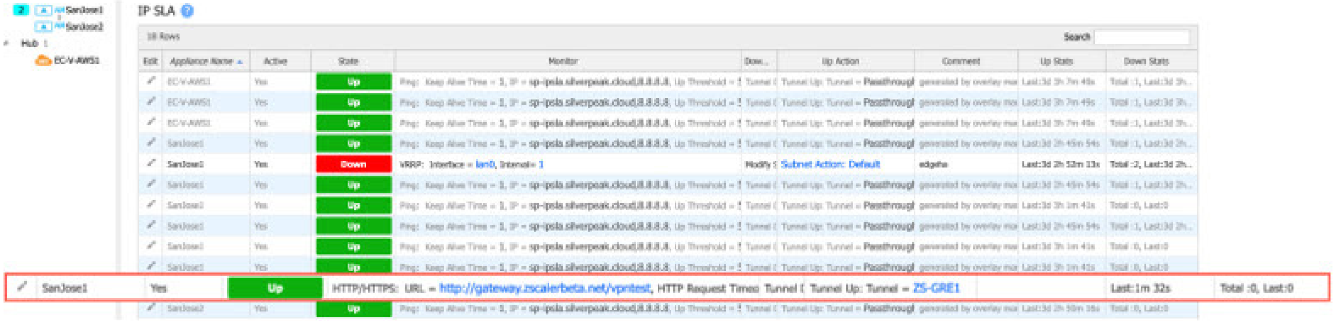
Monitor	HTTP/HTTPS	
URL(s)	http://gateway.zscalerbeta.net/vpntest	
Proxy Address	optional	
Proxy Port		(0..65535)
User Agent	optional	
HTTP Request Timeout	2	Sec
Medium	Tunnel	
Tunnel	ZS-GRE1	
Source Interface	Loopback	
Keep Alive Interval	5	Sec
Sampling Window	300	Sec
Reachability		
Mark Up after X Succeed	2	
Mark Down after X Failed	3	
Loss		
Mark Up after loss below X %	0	
Mark Down after loss above X %	0	
Latency		
Mark Up after average latency below X	0	Milli Sec
Mark Down after average latency above X	0	Milli Sec
Metric Combination	OR	
Monitor Sampling Interval	60	Sec

Actions

Down Action	Disable Tunnel
Tunnel	ZS-GRE1
Up Action	Enable Tunnel
Tunnel	ZS-GRE1

Figure 78. *Configure IP SLA rule*

Verify IP SLA Rule



Edit	Appliance Name	Active	State	Monitor	Dow...	Up Action	Comment	Up Stats	Down Stats
✎	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 3h 7m 48s	Total :1, Last:3d 3h...
✎	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 3h 7m 49s	Total :1, Last:3d 3h...
✎	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 3h 7m 48s	Total :1, Last:3d 3h...
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 2h 45m 54s	Total :1, Last:3d 2h...
✎	SanJose1	Yes	Down	VRRP: Interface = lan0, Interval= 1	Modify !	Subnet Action: Default	edgeha	Last:3d 2h 52m 13s	Total :2, Last:3d 2h...
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 2h 45m 54s	Total :1, Last:3d 2h...
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 3h 1m 41s	Total :0, Last:0
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 2h 45m 54s	Total :1, Last:3d 2h...
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 3h 1m 41s	Total :0, Last:0
✎	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 3h 1m 41s	Total :0, Last:0
✎	SanJose1	Yes	Up	HTTP/HTTPS: URL = http://gateway.zscalerbeta.net/vpntest, HTTP Request Timeo	Tunnel (	Tunnel Up: Tunnel = ZS-GRE1		Last:1m 32s	Total :0, Last:0
✎	SanJose2	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = !	Tunnel (	Tunnel Up: Tunnel = Passthrougl	generated by overlay mai	Last:3d 2h 50m 16s	Total :0, Last:0

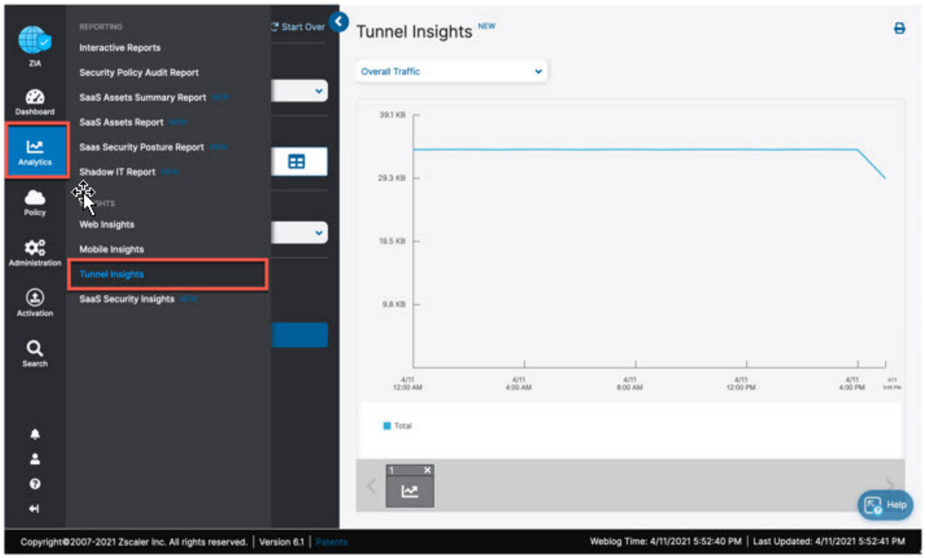
Figure 79. *Verify the IP SLA Rule*

You can also search a specific tenant cloud to see only Zscaler health checks.

Appendix C: Checking Tunnel Status in ZIA Admin Portal

You can check the status of tunnels to ZIA from your sites. , ZIA shows the traffic volume sent and received from your SD-WAN appliances, and also provides logs that show the current state of the tunnels.

Navigate to **Analytics** > **Insights** > **Tunnel Insights**.



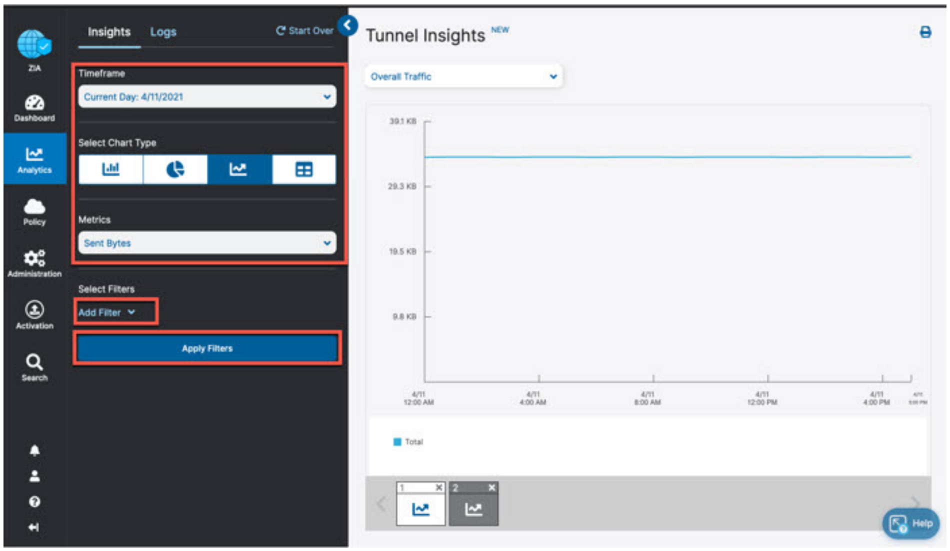
Copyright©2007-2021 Zscaler Inc. All rights reserved. | Version 6.1 | Patents

Weblog Time: 4/11/2021 5:52:40 PM | Last Updated: 4/11/2021 5:52:41 PM

Figure 80. *Navigate to tunnel insights*

Tunnel Data Visualization

Use **Insights** to visualize and filter data in various ways. You can configure time frames, chart type, and metrics that you want to view. Additionally, you can filter the type of data shown in the chart by using **Select Filters**.



Timeframe: Current Day: 4/11/2021

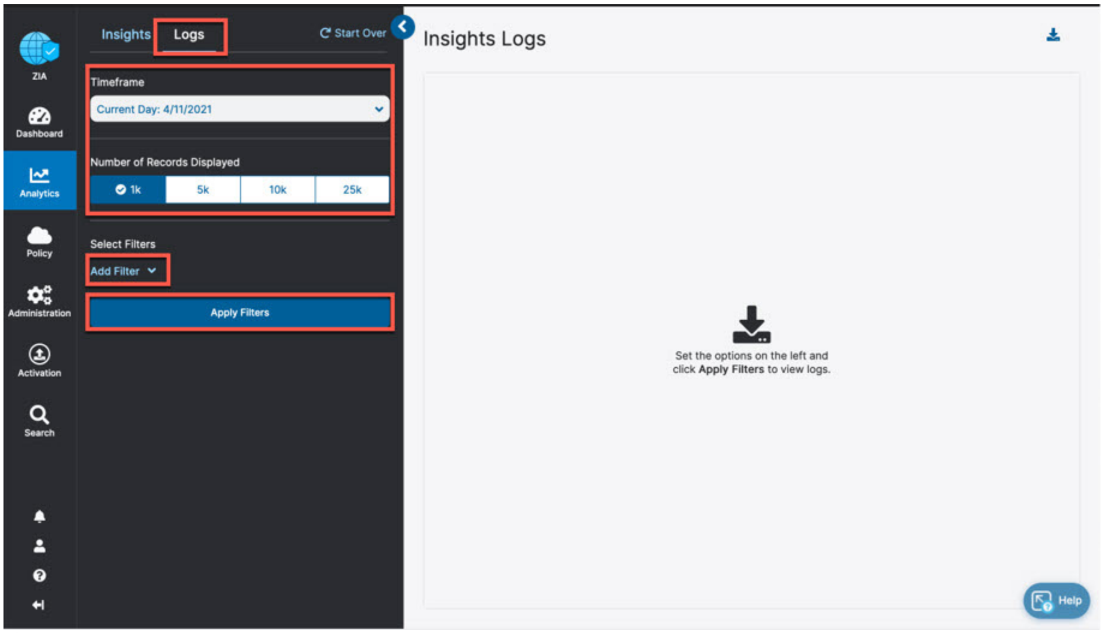
Metrics: Sent Bytes

Figure 81. *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 view the state of all tunnels for your tenant from the ZIA Admin Portal. Click **Logs**.



Insights Logs

Timeframe: Current Day: 4/11/2021

Number of Records Displayed: 1k (selected), 5k, 10k, 25k

Select Filters

Set the options on the left and click **Apply Filters** to view logs.

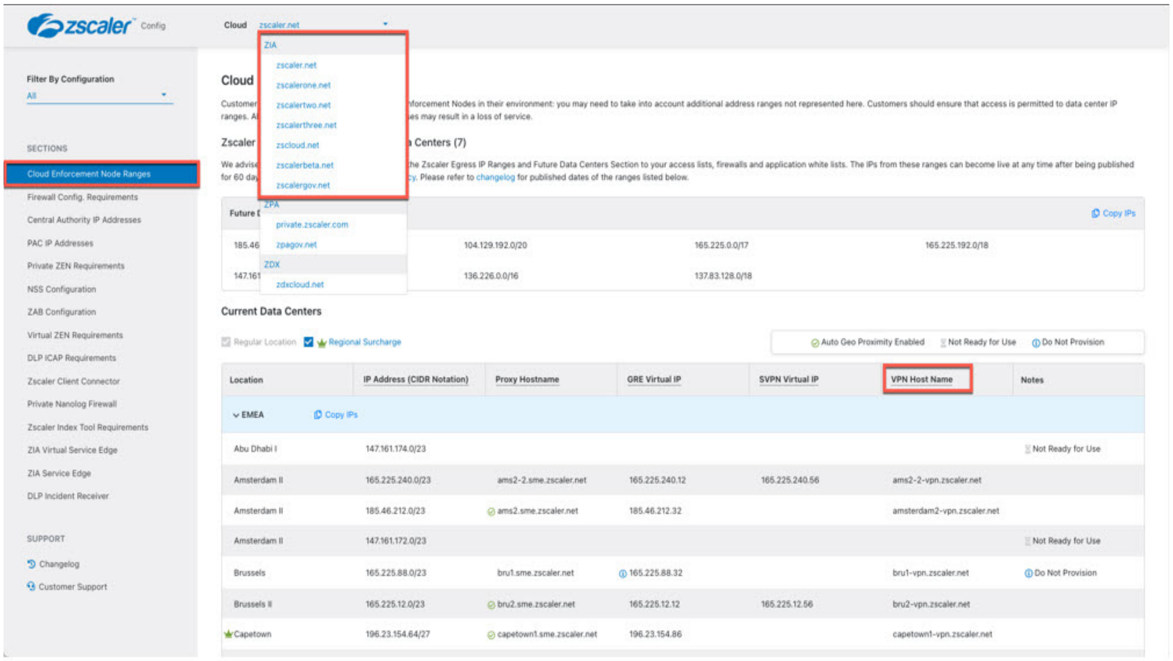
Figure 82. *Viewing ZIA tunnel logs*

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

Appendix D: Deriving the Zscaler IPSec VPN VIP

You can find Zscaler public IP endpoints on the Cloud Enforcement Node Ranges page (government agencies, see Cloud Enforcement Node Ranges). Use DNS hostnames as the destination for tunnels and proxies into the ZIA service. If the service or device that is the source of the traffic doesn't support DNS names (e.g., AWS customer gateways) you must derive the IP address from the DNS hostname of the endpoint.

1. When you go to the Cloud Enforcement Node Ranges page (government agencies, see Cloud Enforcement Node Ranges) to access all Zscaler public IP endpoints, make sure that you select the correct Zscaler cloud for your tenant.
2. Ensure that **Cloud Enforcement Node Ranges** is selected from the navigation frame
3. Choose the closest data center locations **VPN Host Name** to your AWS region



Cloud

Customer nforcement Nodes in their environment: you may need to take into account additional address ranges not represented here. Customers should ensure that access is permitted to data center IP ranges. A es may result in a loss of service.

Zscaler a Centers (7)

We advise he Zscaler Egress IP Ranges and Future Data Centers Section to your access lists, firewalls and application white lists. The IPs from these ranges can become live at any time after being published for 60 day y. Please refer to changelog for published dates of the ranges listed below.

Future [			
185.46	104.129.192.0/20	165.225.0.0/17	165.225.192.0/18
147.161	136.226.0.0/16	137.83.128.0/18	

Current Data Centers

Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	SVPN Virtual IP	VPN Host Name	Notes
EMEA						
Abu Dhabi I	147.161.174.0/23					Not Ready for Use
Amsterdam II	165.225.240.0/23	ams2-2.sme.zscaler.net	165.225.240.12	165.225.240.56	ams2-2-vpn.zscaler.net	
Amsterdam II	185.46.212.0/23	ams2.sme.zscaler.net	185.46.212.32		amsterdam2-vpn.zscaler.net	
Amsterdam II	147.161.172.0/23					Not Ready for Use
Brussels	165.225.88.0/23	bru1.sme.zscaler.net	165.225.88.32		bru1-vpn.zscaler.net	Do Not Provision
Brussels II	165.225.12.0/23	bru2.sme.zscaler.net	165.225.12.12	165.225.12.56	bru2-vpn.zscaler.net	
Capetown	196.23.154.64/27	capetown1.sme.zscaler.net	196.23.154.86		capetown1-vpn.zscaler.net	

Figure 83. *Zscaler public IP reference*

Use either **nslookup** or **dig** to get the IP address from the DNS hostname. For example:

```
dig ams2-2-vpn.zscaler.net


; <<>> DiG 9.10.6 <<>> ams2-2-vpn.zscaler.net

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38701

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 512
```

```
;; QUESTION SECTION:
;ams2-2-vpn.zscaler.net.          IN    A

;; ANSWER SECTION:
ams2-2-vpn.zscaler.net.     1800  IN    A     165.225.240.18

;; Query time: 50 msec
;; SERVER: 192.168.83.35#53(192.168.83.35)
;; WHEN: Thu Mar 25 22:32:28 PDT 2021
;; MSG SIZE  rcvd: 67
```

Appendix E: Requesting Zscaler Support

You might need to contact Zscaler Support to provision certain services. Zscaler support is also available to help troubleshoot configuration and service issues. Zscaler support is available 24/7/365.

To contact Zscaler Support:

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

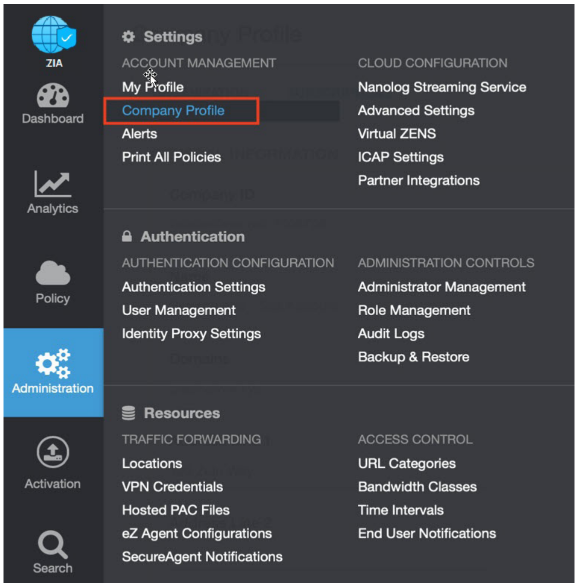
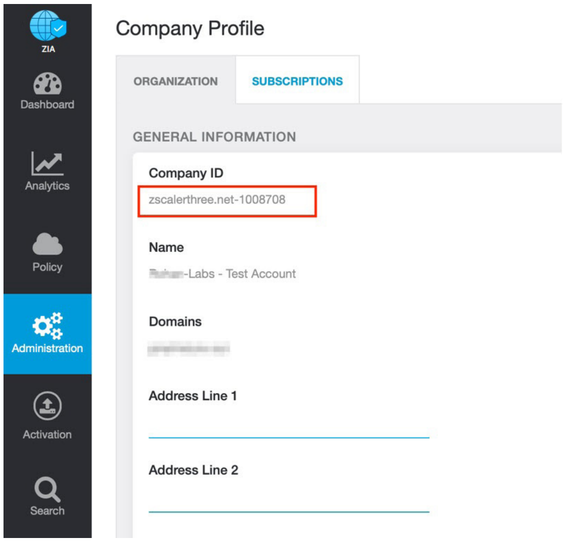


Figure 84. *Collecting details to open support case with Zscaler TAC*

2. Your company ID can be found under **Company ID**. Copy the ID for use in subsequent screens.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 85. *Save your company ID information*

3. Go to **?** > **Support** > **Submit a Ticket**.

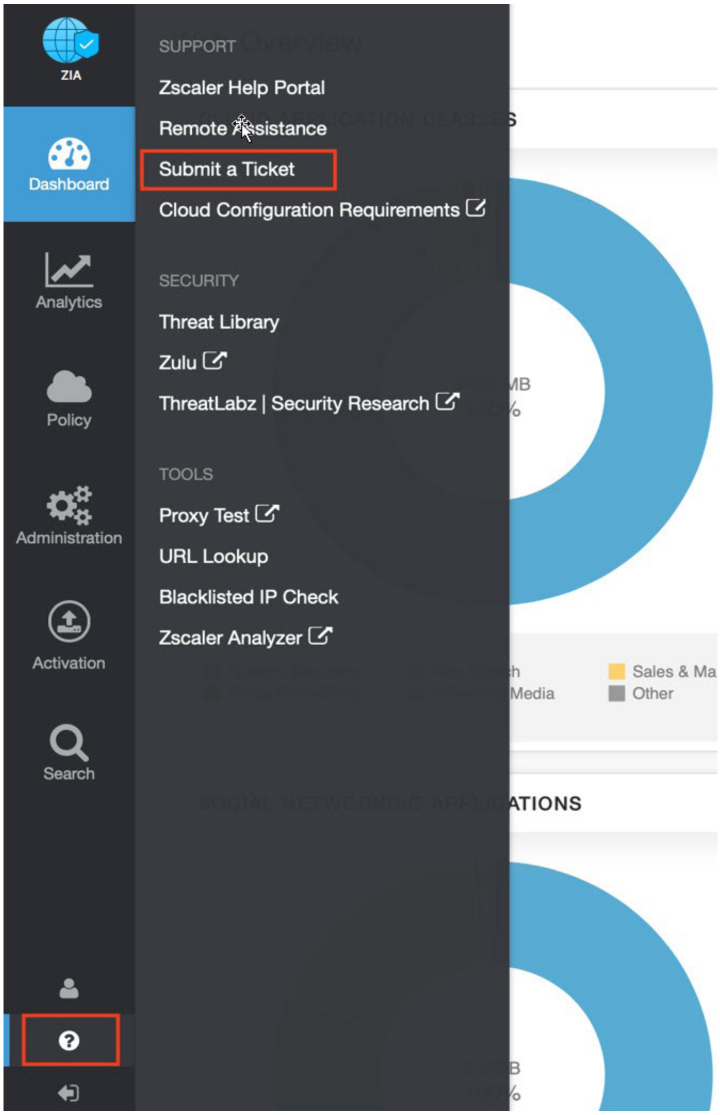
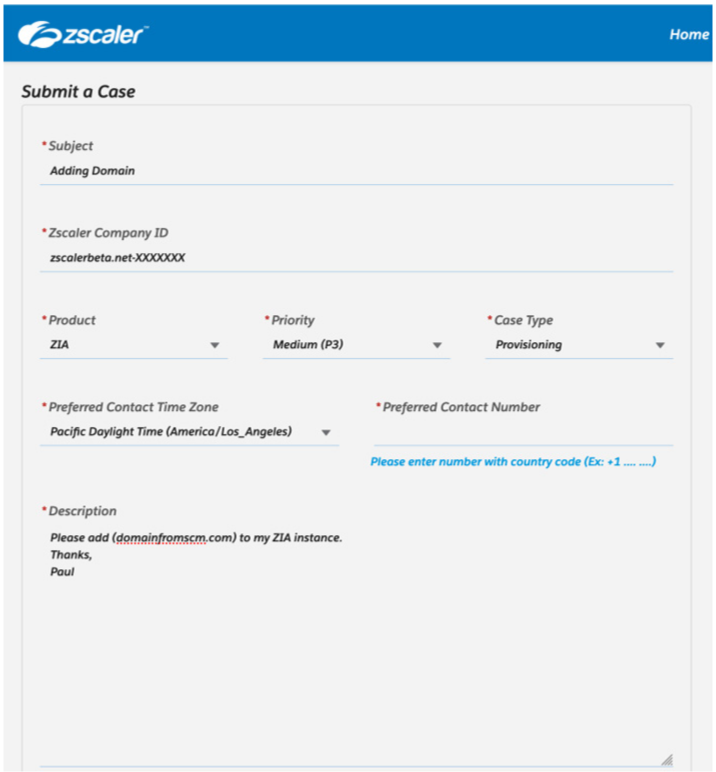


Figure 86. *Submit a ticket*

Adding Domain (Example)

Each support ticket asks targeted questions based on the Case Type. In the following example, the support ticket is a request to add an additional domain to a ZIA instance.



Submit a Case

*Subject
Adding Domain

*Zscaler Company ID
zscalerbeta.net-XXXXXXX

*Product
ZIA

*Priority
Medium (P3)

*Case Type
Provisioning

*Preferred Contact Time Zone
Pacific Daylight Time (America/Los_Angeles)

*Preferred Contact Number

Please enter number with country code (Ex: +1 ....)

*Description
Please add (domainfromscm.com) to my ZIA instance.
Thanks,
Paul

Figure 87. *Adding a domain*