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 6

About This Document 7

- Zscaler Overview 7
- Aruba Overview 7
- Audience 7
- Software Versions 7
- Request for Comments 7
- Zscaler Resources 8
- Aruba EdgeConnect Overview 9
- Aruba Resources 9
- Prerequisites 9
  - ZIA 9
  - Silver Peak Orchestrator 9

Configuring ZIA 10

- Logging into ZIA 10
- Configure ZIA for API Access 11
- Adding SD-WAN Partner Key 11
- Verify SD-WAN Partner Key 12
- Adding a Partner Administrator Role 13
  - Creating Partner Administrator Role 13
- Administrator Management 14
  - Add Partner Administrator 15
  - Creating Partner Administrator 15
  - Activate Pending Changes 16
  - Verify Activation 16

©2024 Zscaler, Inc. All rights reserved.

Configuring Automated IPSec Tunnels 17

Log into Aruba Orchestrator 17

Configure Cloud Services 18

Validate that the Desired Interface Labels are Selected 18

Configure Tunnel Settings 20

Configuring a ZIA Subscription 21

Configuring ZIA API Credentials and Zscaler Cloud 21

Verify ZIA Account Update 23

Associate Sites with ZIA for Automation 23

Configuring Business Intent Overlays 25

Enabling Zscaler for Breakout Traffic 25

Configuring Preferred Policy Order 26

Apply Overlay Changes 26

Verifying Automated Tunnel Establishment 27

View Automated Tunnel Details 28

Configuring Sub-Locations and Gateway Options 29

Configure Sub-location 29

Enable Gateway Option Orchestration 29

Add Sub-Location 30

Configure Gateway Options 30

Set Gateway Options 31

Change Gateway Options Confirmation 31

Verify Gateway Options 32

Verify Sub-Locations in ZIA 32

©2024 Zscaler, Inc. All rights reserved.

Configuring Layer-7 Health Checks for Automated Tunnels 33
Configuring Zscaler IP SLA 33
Enable the IP SLA Probes for the Zscaler Tunnels 33
Verify Zscaler IP SLA Rules 34
Navigate to the IP SLA tab 34
Validate the Health Checks in the IP SLA Tab 34
Appendix A: Manual Tunnel Configuration 35
Configuring Static IPs and GRE Tunnels 35
Add a Static IP Configuration 35
Add a GRE Tunnel Configuration 38
Activate and Verify All Configuration Changes 40
Adding VPN Credentials for Manual IPSec Tunnels 41
Navigate to VPN Credentials 41
Add a VPN Credential 42
Enter VPN Credential Data 42
Verify VPN Credential 42
Activate Pending Changes 43
Verify the Activation 43
Configuring a Location for Manual Tunnels 44
Add a Location 44
Enter the Location Data 45
Confirm Changes Have Been Saved 46
Activate Pending Changes 46
Activation Confirmation 47
Manually Configure Tunnels on Aruba Orchestrator 47

©2024 Zscaler, Inc. All rights reserved.

Appendix B: Configuring Layer-7 Health Checks for Manually Created Tunnels 48

Configuring Aruba SD-WAN IP SLA 48

Edit EdgeConnect IPSLA Rules 49

Add Rule and Target 49

Configure IP SLA Rule 50

Verify IP SLA Rule 51

Appendix C: Checking Tunnel Status in ZIA Admin Portal 52

Tunnel Data Visualization 52

Tunnel Logging 53

Appendix D: Deriving the Zscaler IPSec VPN VIP 54

Appendix E: Requesting Zscaler Support 56

Adding Domain (Example) 58

©2024 Zscaler, Inc. All rights reserved.

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)

©2024 Zscaler, Inc. All rights reserved.

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 or follow Zscaler on Twitter @zscaler.

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. Go to the Aruba SD-WAN product page for more information on Aruba SD-WAN.

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.

©2024 Zscaler, Inc. All rights reserved.

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, please contact your Zscaler Account Representative.

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 Browser 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.

©2024 Zscaler, Inc. All rights reserved.

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

©2024 Zscaler, Inc. All rights reserved.

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).

©2024 Zscaler, Inc. All rights reserved.

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**.

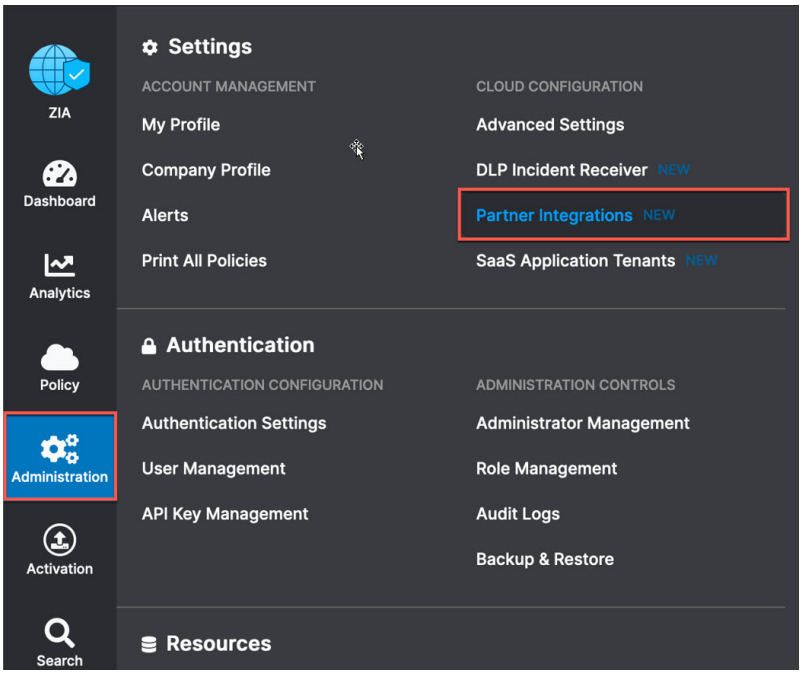

Figure 2. *Configuring ZIA for API access*

Adding SD-WAN Partner Key

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

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

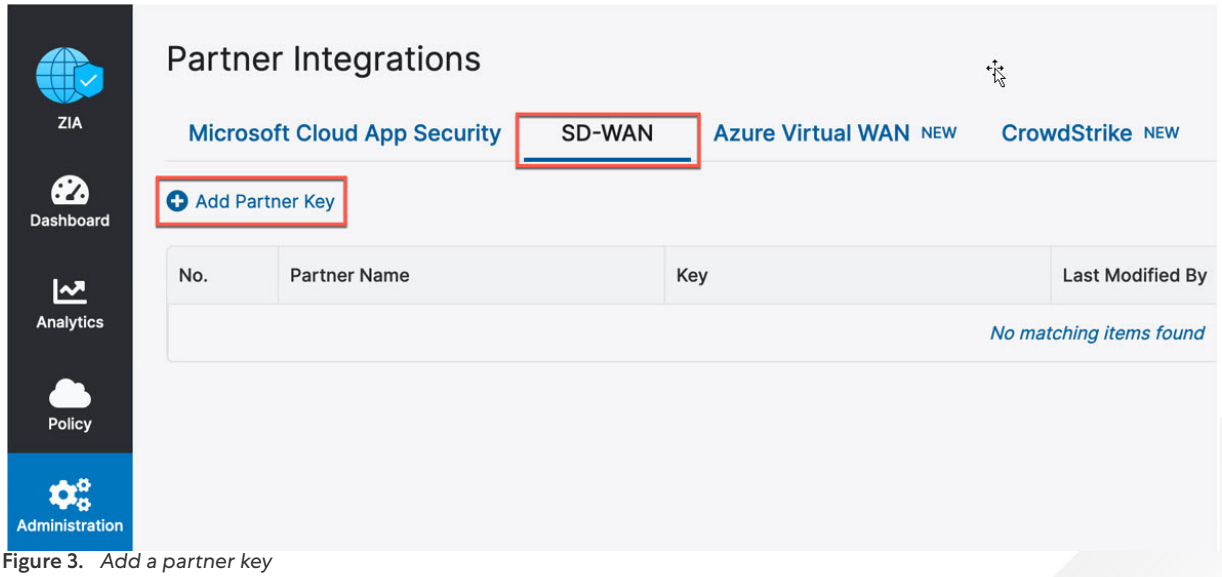

Figure 3. *Add a partner key*

©2024 Zscaler, Inc. All rights reserved.

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.

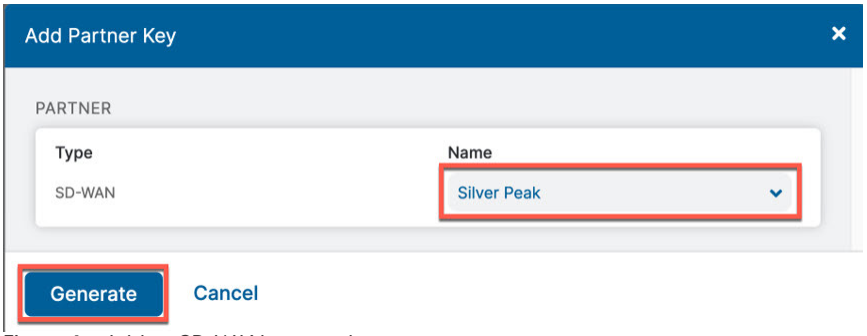

Figure 4. *Add an SD-WAN partner key*

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.

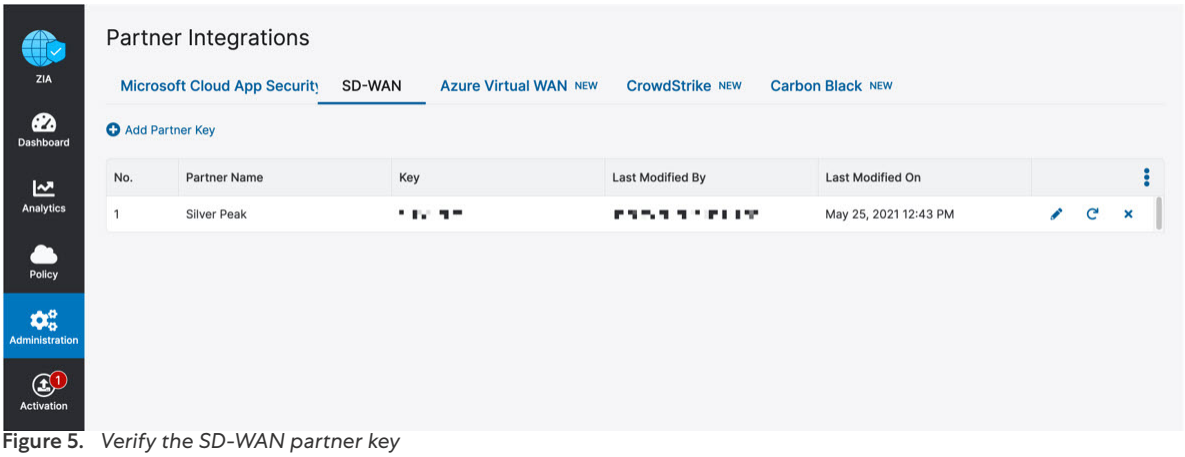

Figure 5. *Verify the SD-WAN partner key*

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.

©2024 Zscaler, Inc. All rights reserved.

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**.

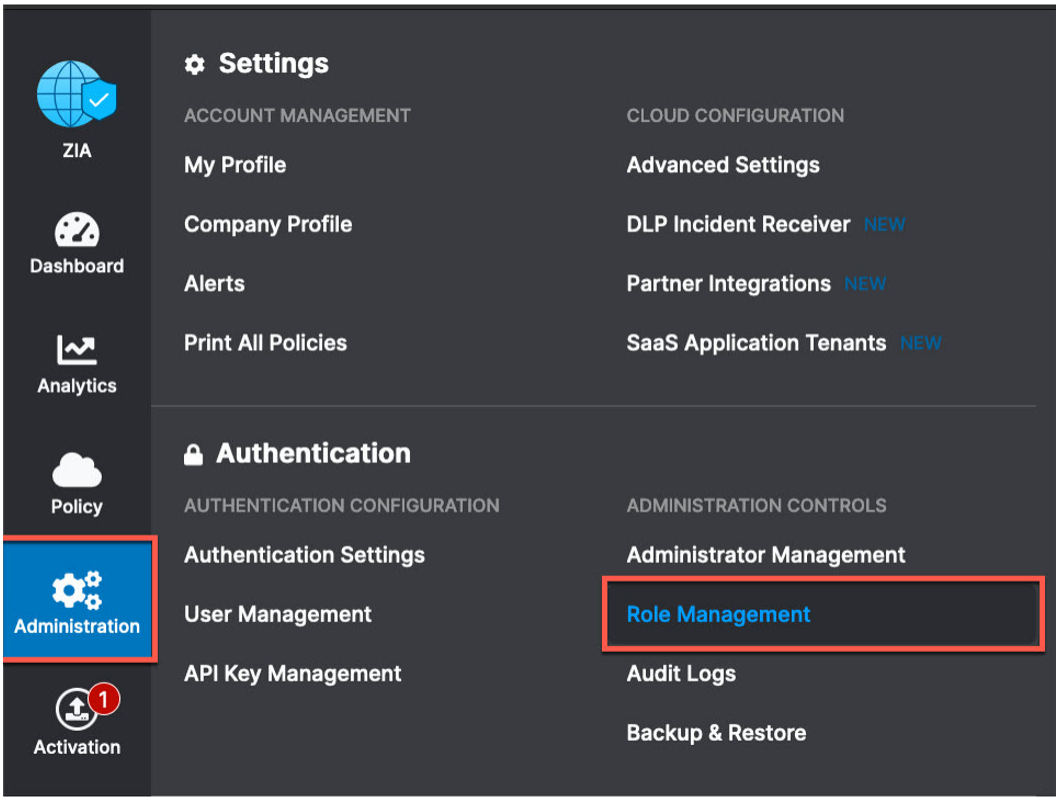

Figure 6. *Role Management controls*

Creating Partner Administrator Role

Complete the following steps:

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

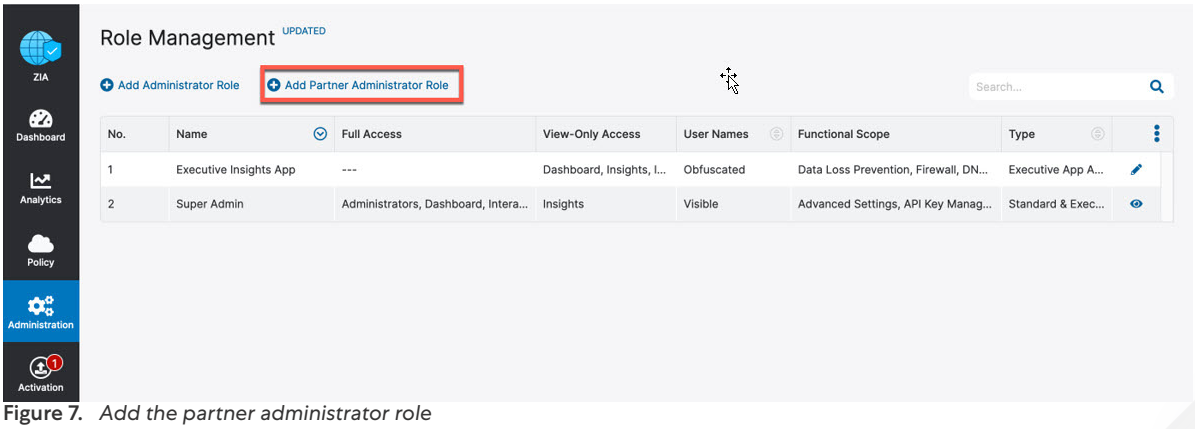

Figure 7. *Add the partner administrator role*

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.

©2024 Zscaler, Inc. All rights reserved.

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

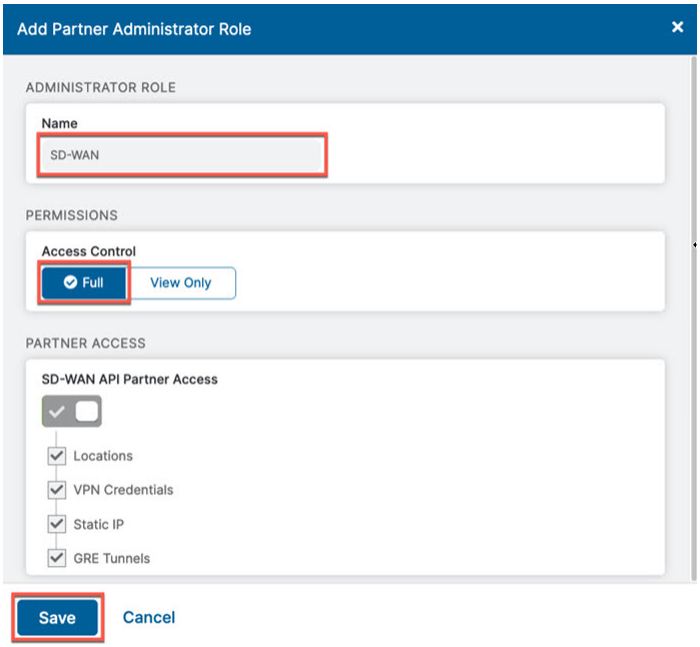

Figure 8. *Creating a partner administrator role*

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**.

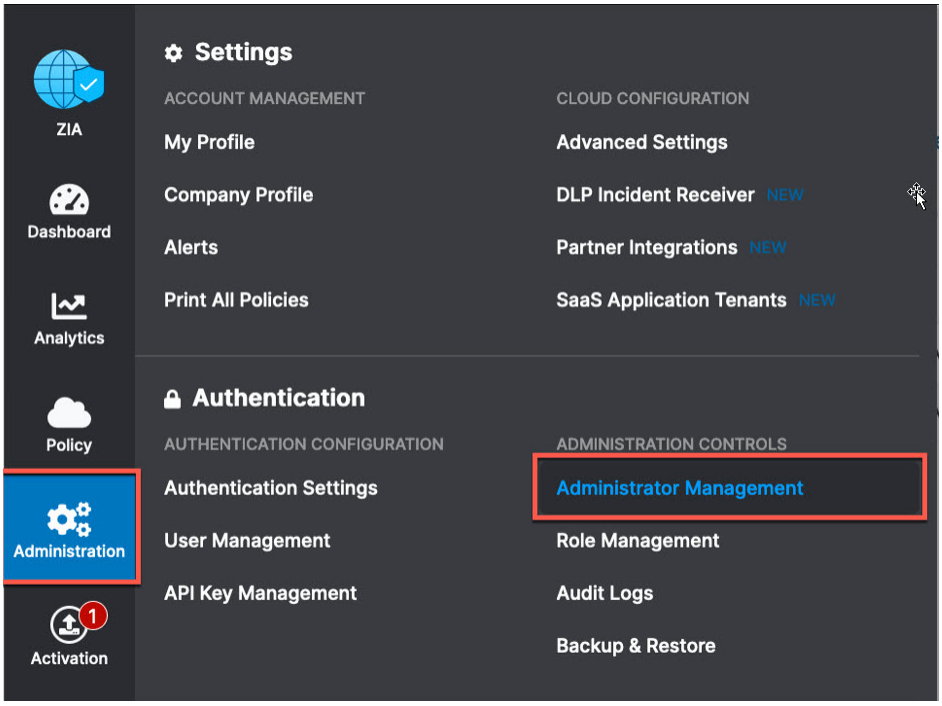

Figure 9. *Administrator Management*

©2024 Zscaler, Inc. All rights reserved.

Add Partner Administrator

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

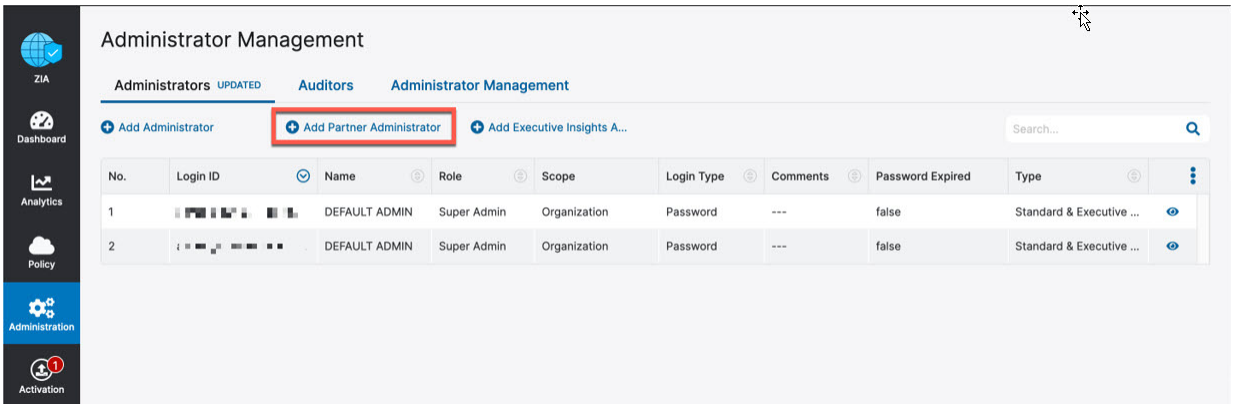

Figure 10. *Add Partner Administrator*

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**.

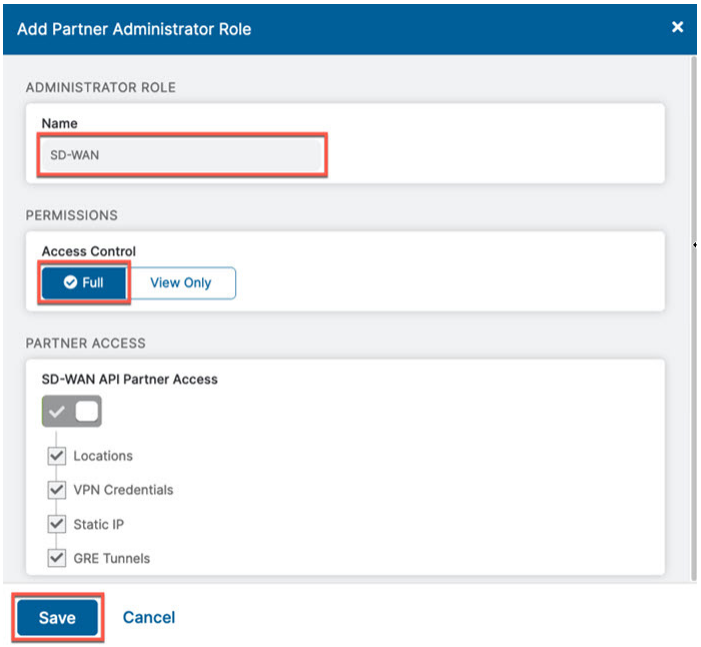

Figure 11. *Creating a partner administrator*

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

©2024 Zscaler, Inc. All rights reserved.

Activate Pending Changes

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

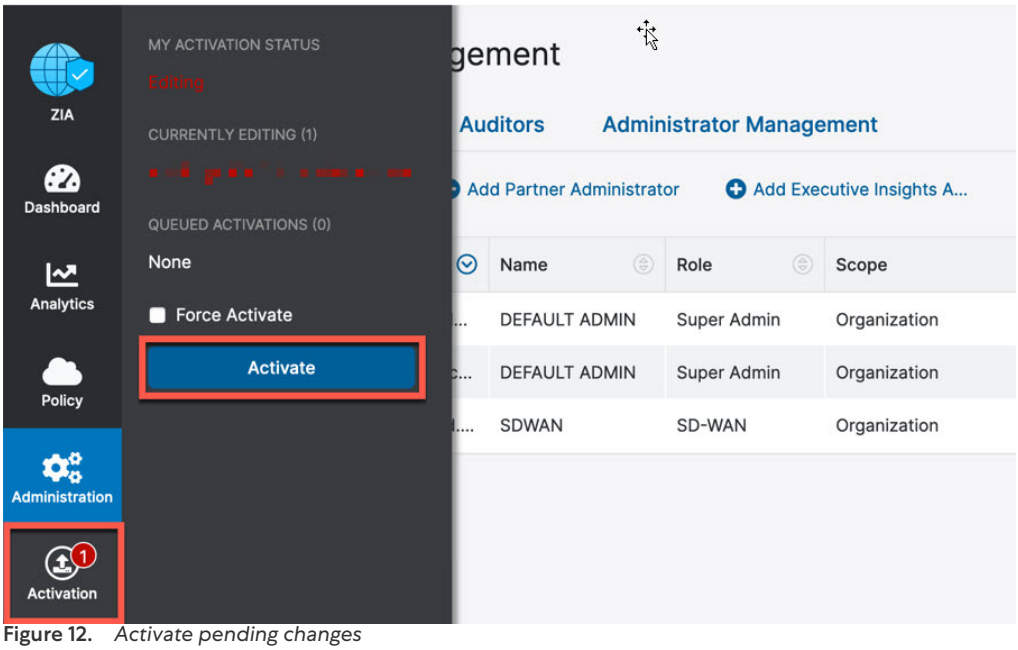

Figure 12. *Activate pending changes*

Verify Activation

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

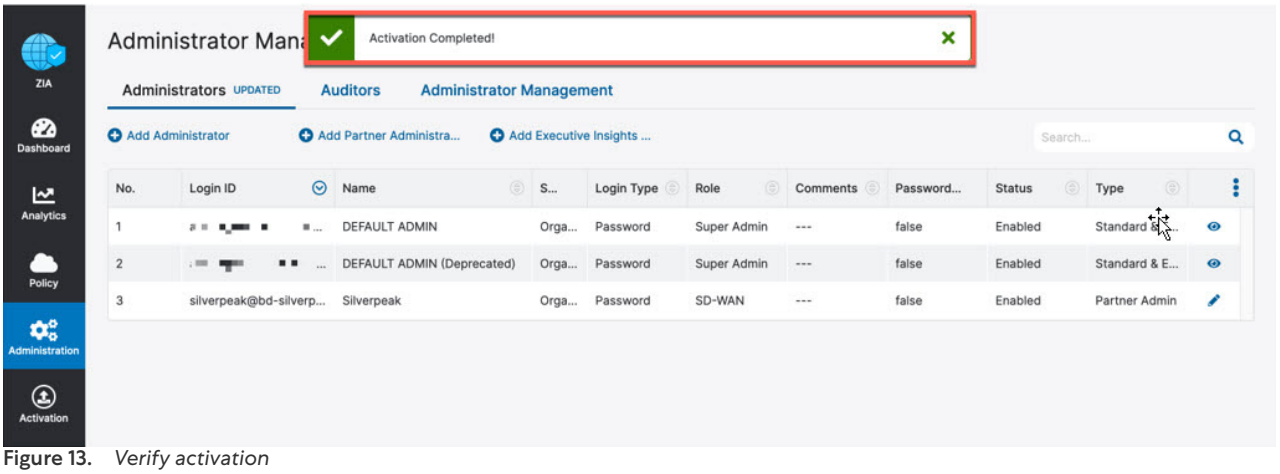

Figure 13. *Verify activation*

©2024 Zscaler, Inc. All rights reserved.

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.

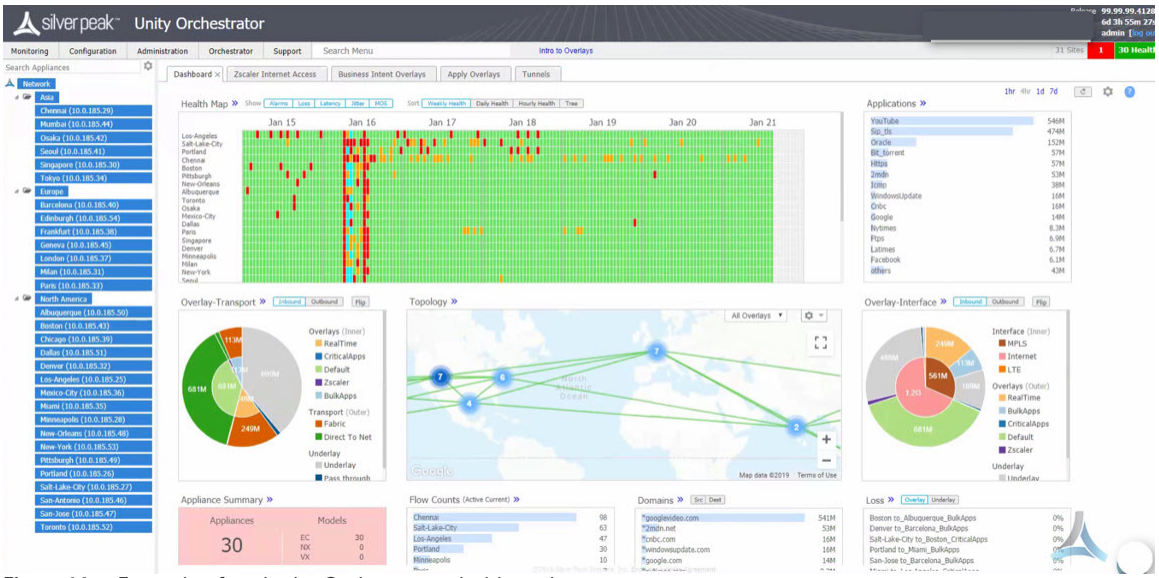

Figure 14. *Example of an Aruba Orchestrator dashboard*

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.

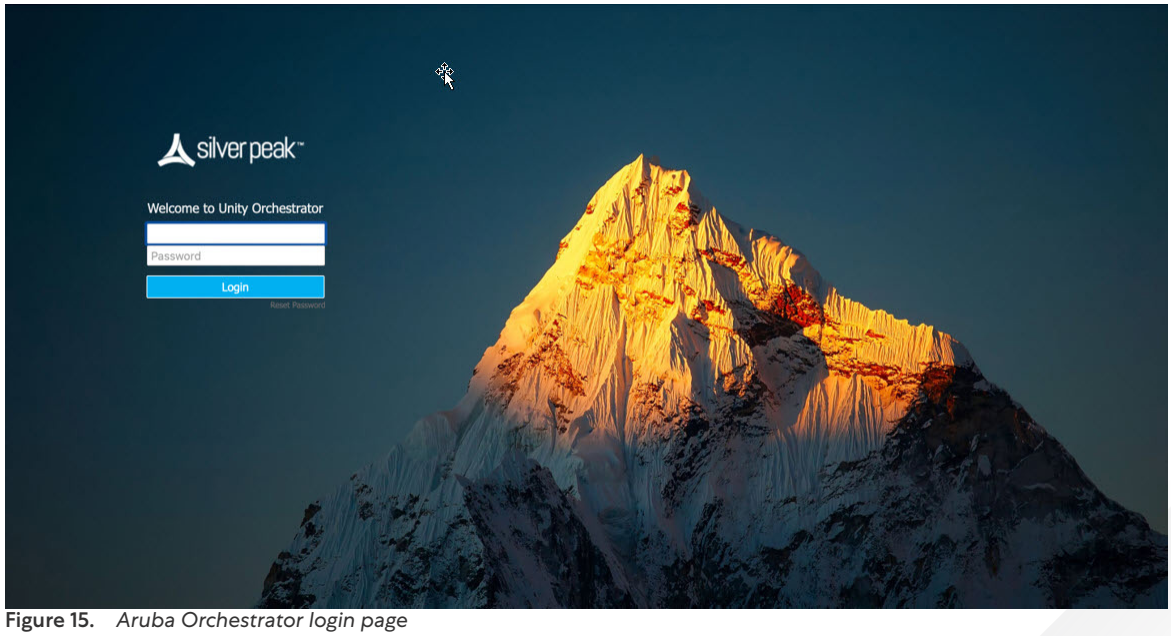

Figure 15. *Aruba Orchestrator login page*

©2024 Zscaler, Inc. All rights reserved.

Configure Cloud Services

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

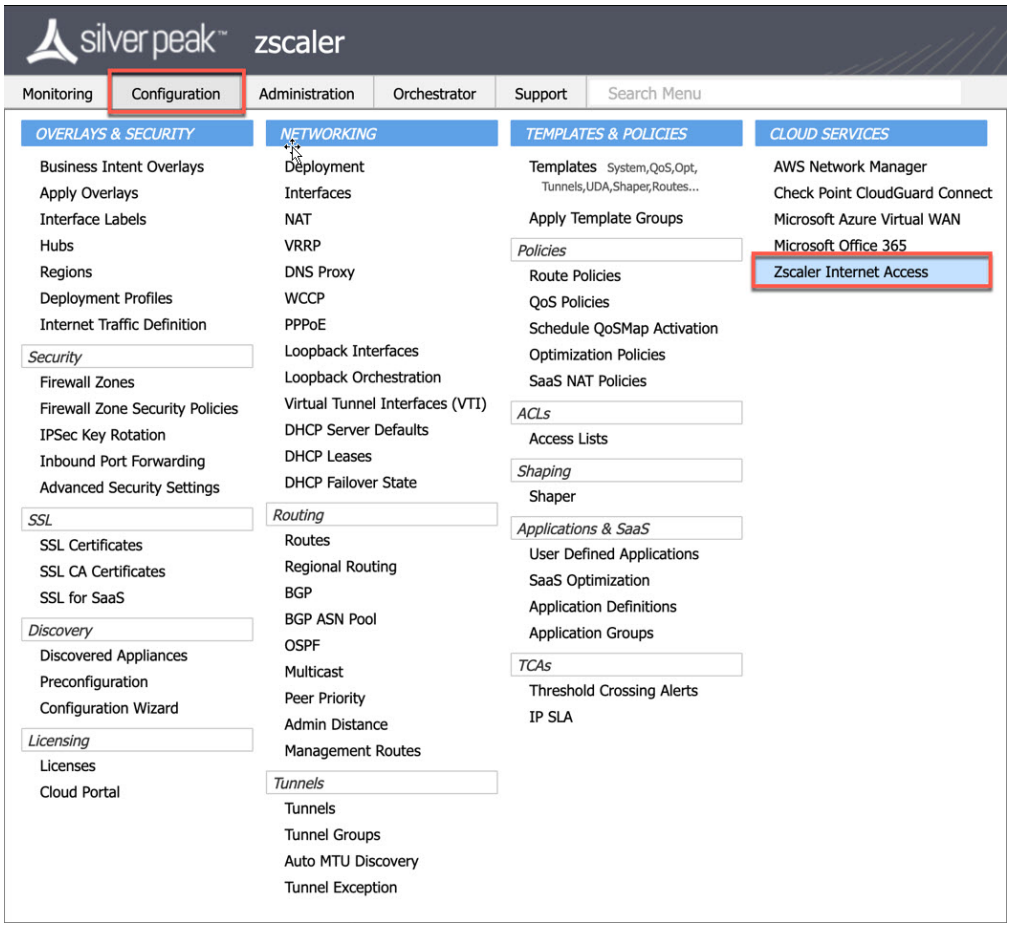

Figure 16. *Configuring cloud services*

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**.

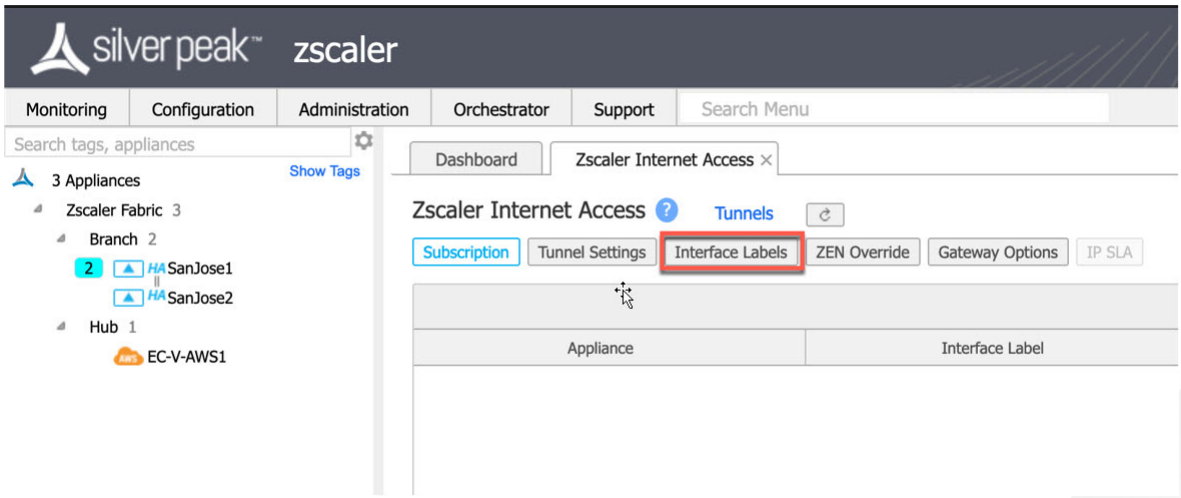

Figure 17. *Interface Labels*

©2024 Zscaler, Inc. All rights reserved.

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

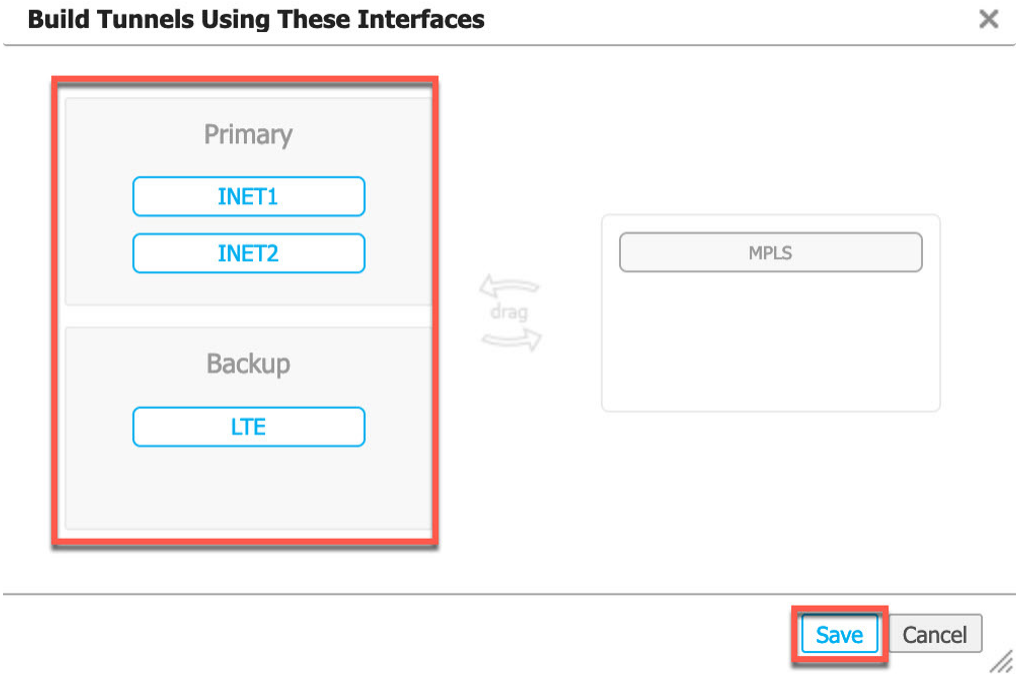

Figure 18. *Choose interfaces for tunnel creation*

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.

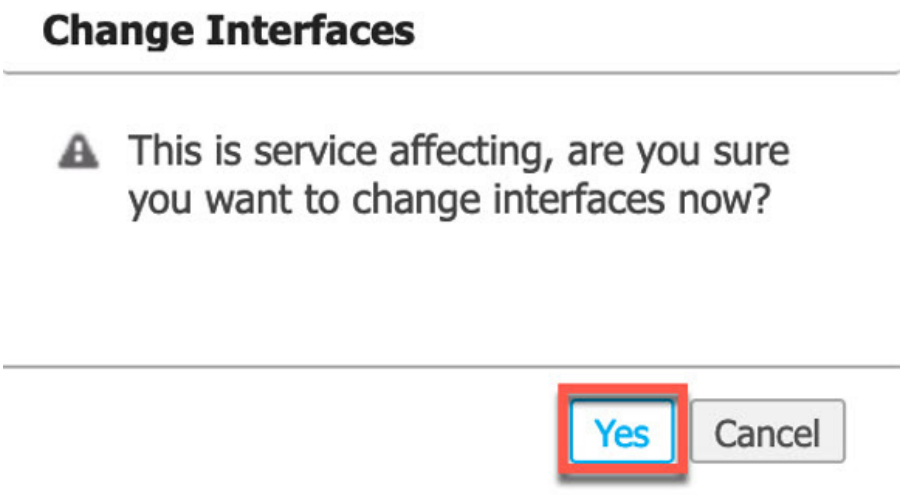

Figure 19. *Apply the tunnel setting to interfaces*

©2024 Zscaler, Inc. All rights reserved.

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.

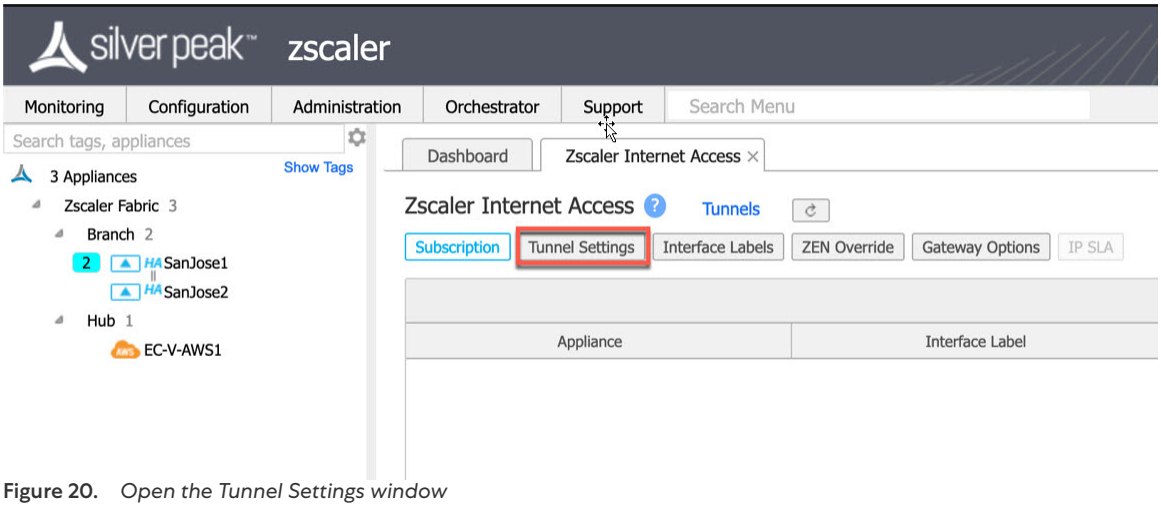

Figure 20. *Open the Tunnel Settings window*

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

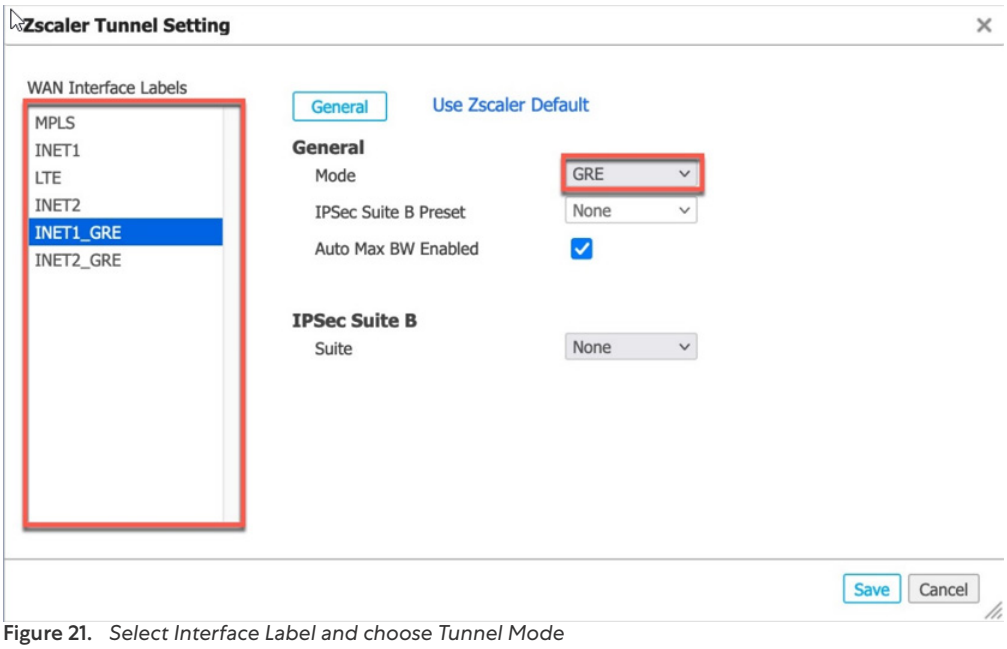

Figure 21. *Select Interface Label and choose Tunnel Mode*

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

©2024 Zscaler, Inc. All rights reserved.

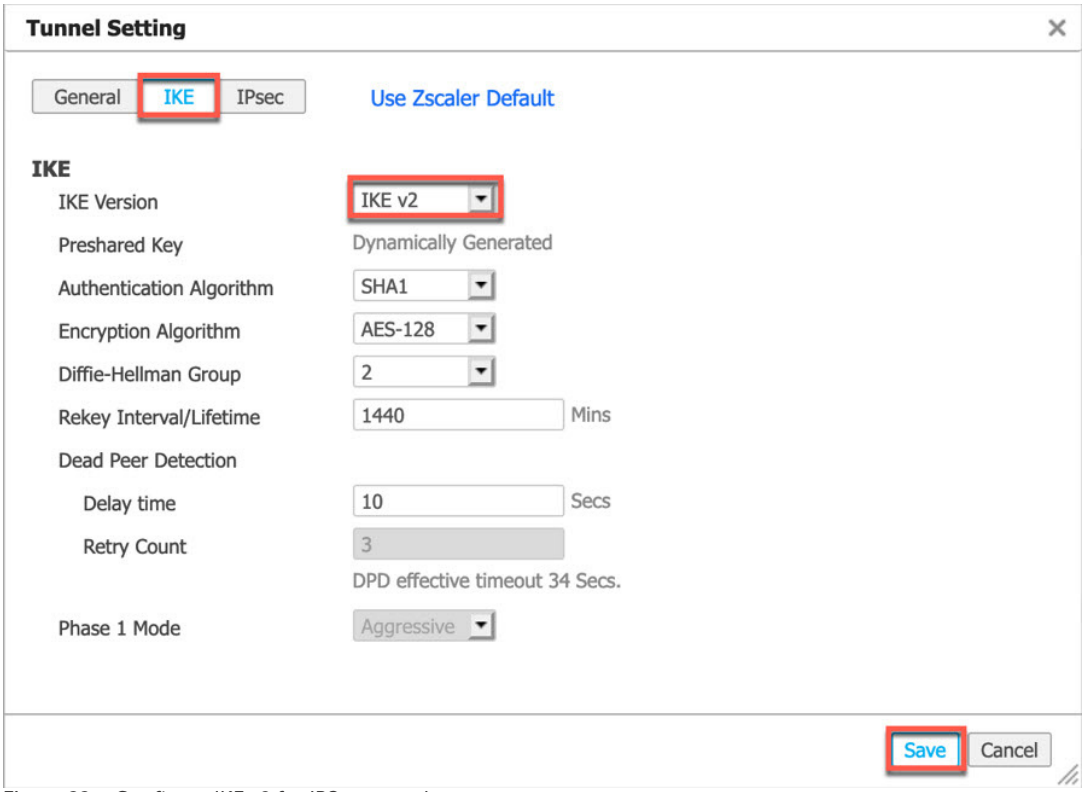

Figure 22. *Configure IKE v2 for IPSec tunnels*

For GRE there are no settings changes necessary.

Configuring a ZIA Subscription

Select the **Subscription** tab.

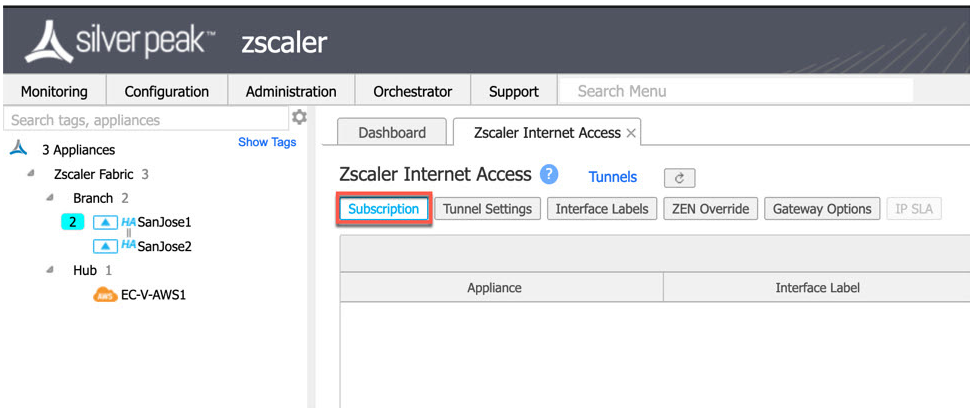

Figure 23. *Configuring a ZIA subscription*

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.

©2024 Zscaler, Inc. All rights reserved.

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.

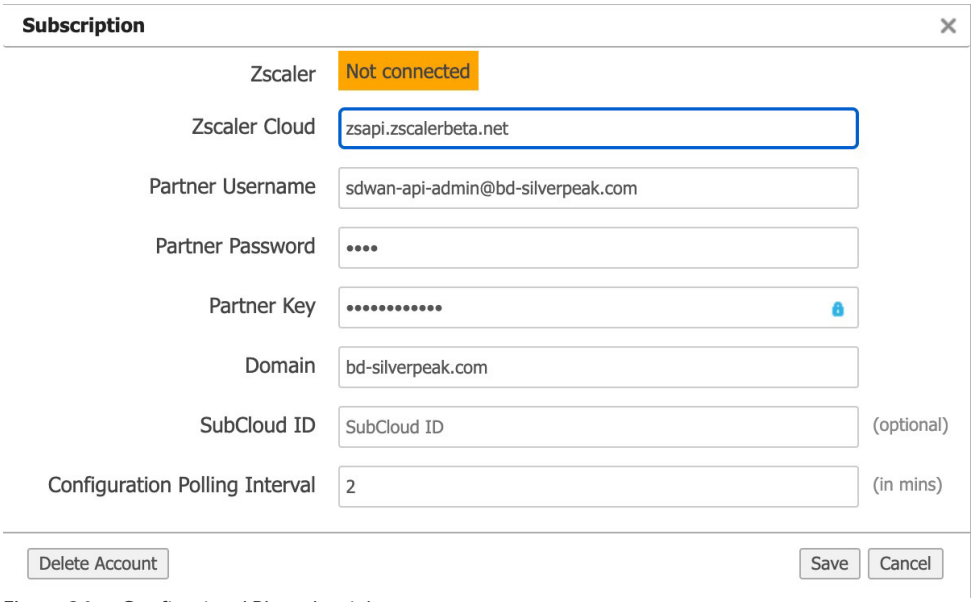

Figure 24. *Configuring API credentials*

Click **Save** to refresh the screen.

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

©2024 Zscaler, Inc. All rights reserved.

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.

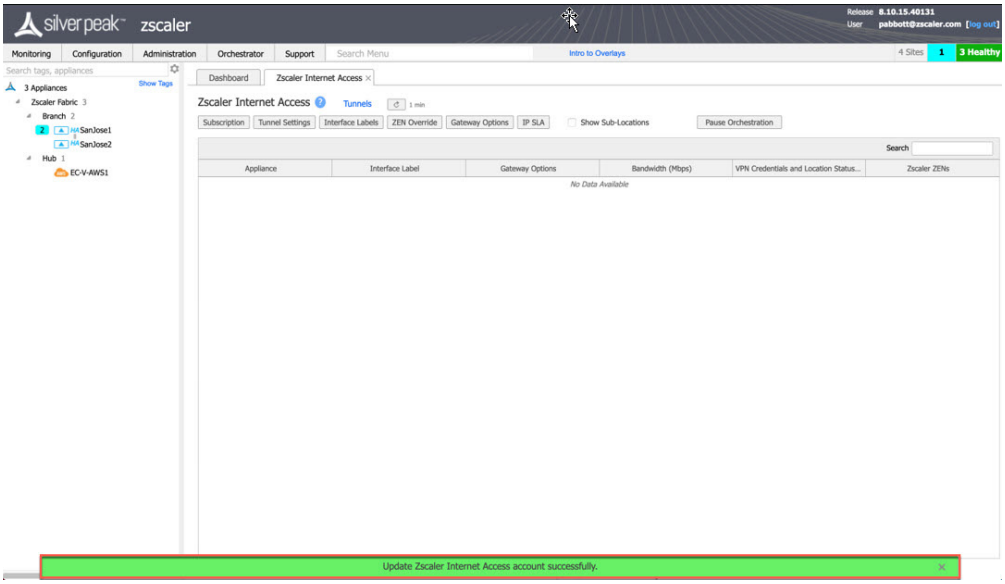

Figure 25. *Verifying a ZIA account update*

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.

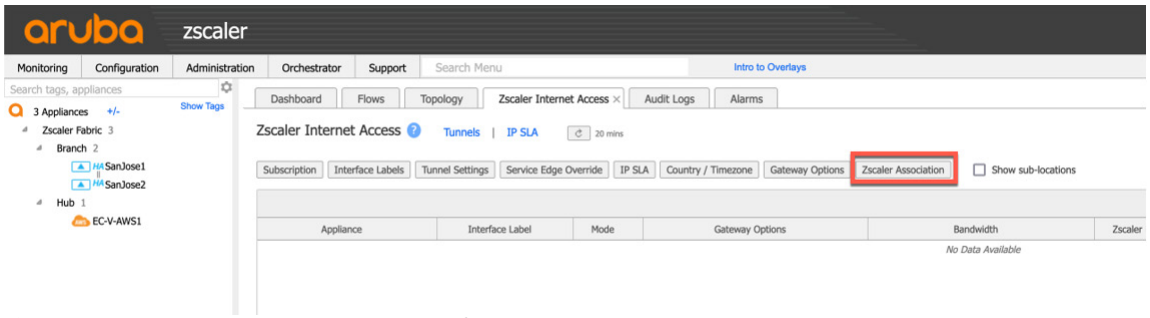

Figure 26. *How to access Zscaler Association of Appliances*

©2024 Zscaler, Inc. All rights reserved.

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

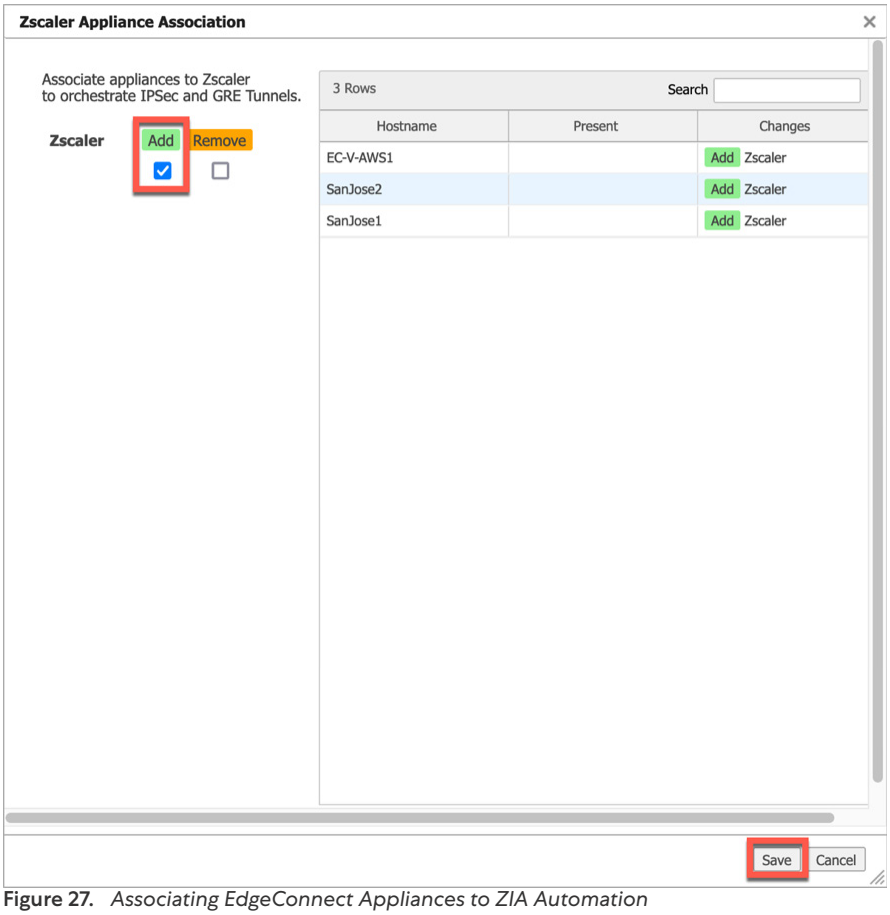

Figure 27. *Associating EdgeConnect Appliances to ZIA Automation*

©2024 Zscaler, Inc. All rights reserved.

Configuring Business Intent Overlays

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

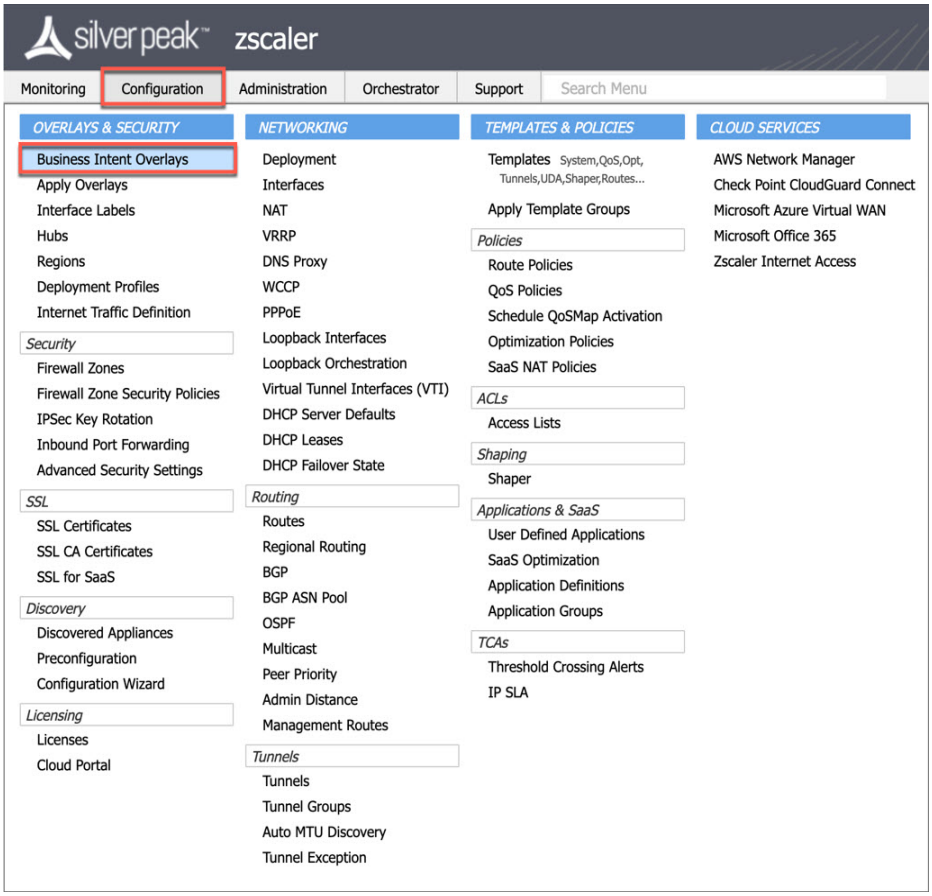

Figure 28. *Configuring business intent overlays*

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.

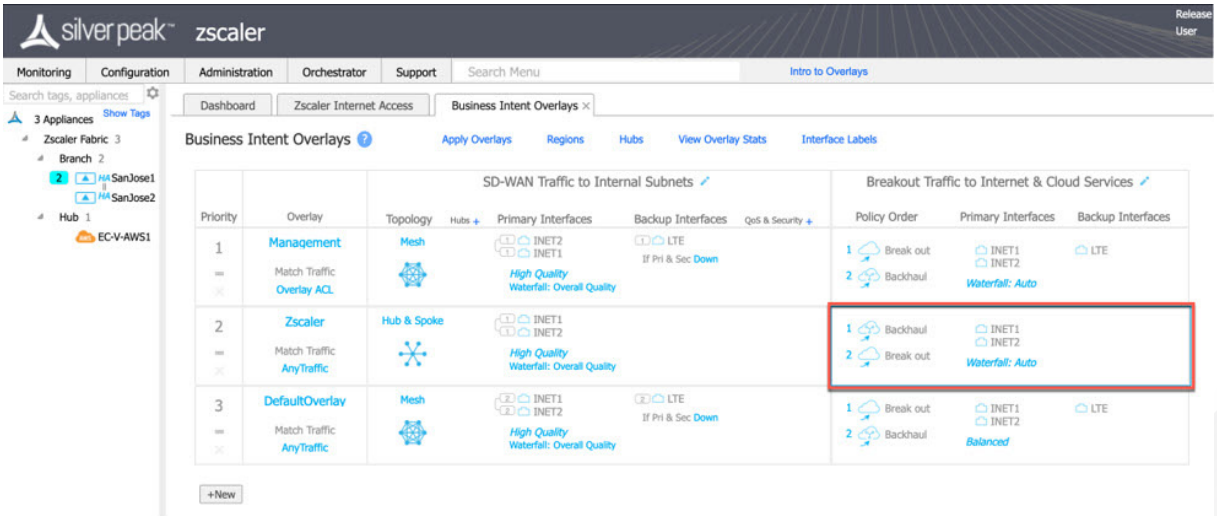

Figure 29. *Enabling Zscaler for breakout traffic*

©2024 Zscaler, Inc. All rights reserved.

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**.

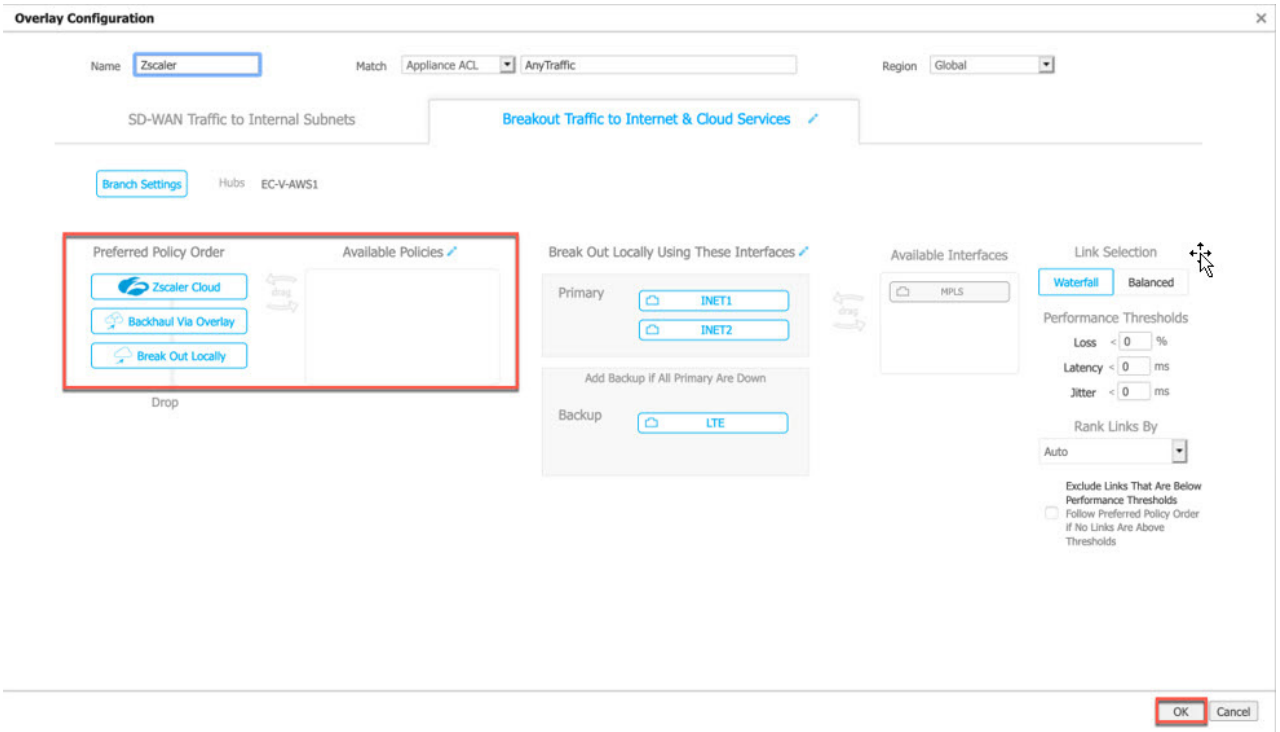

Figure 30. *Configuring preferred policy order*

Apply Overlay Changes

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

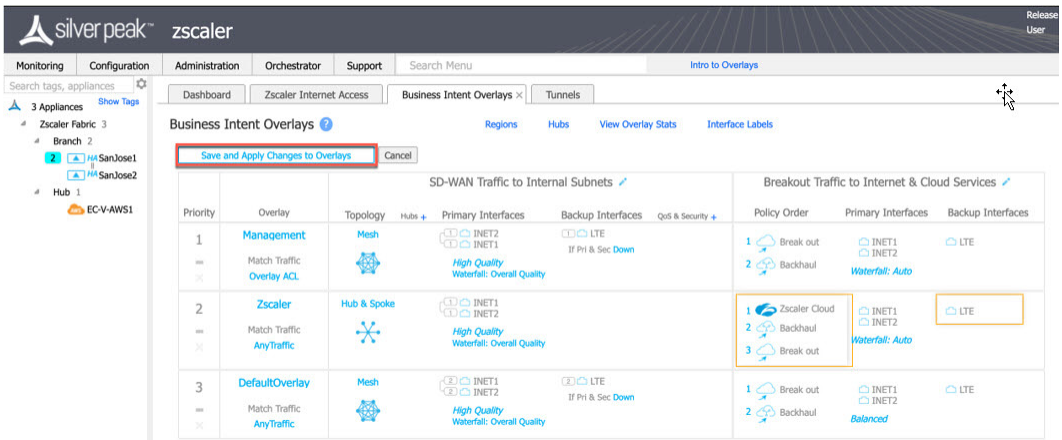

Figure 31. *Save and apply changes*

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

©2024 Zscaler, Inc. All rights reserved.

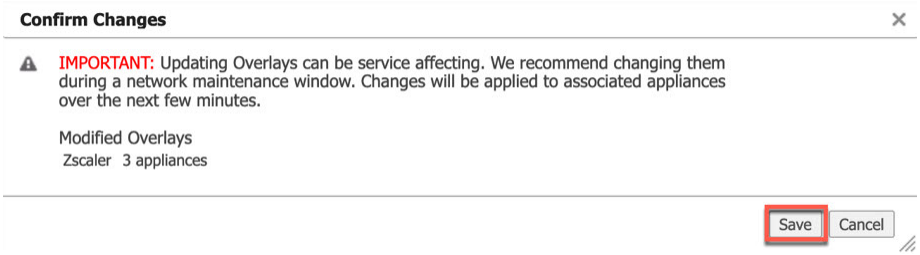

Figure 32. *Confirm changes*

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.

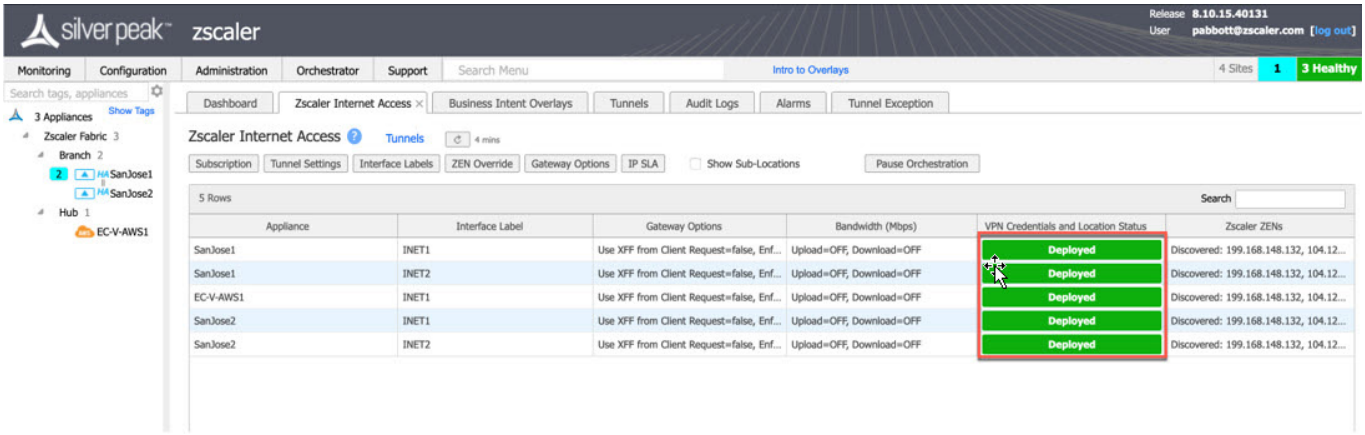

Figure 33. *Verify automated tunnel establishment*

©2024 Zscaler, Inc. All rights reserved.

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.

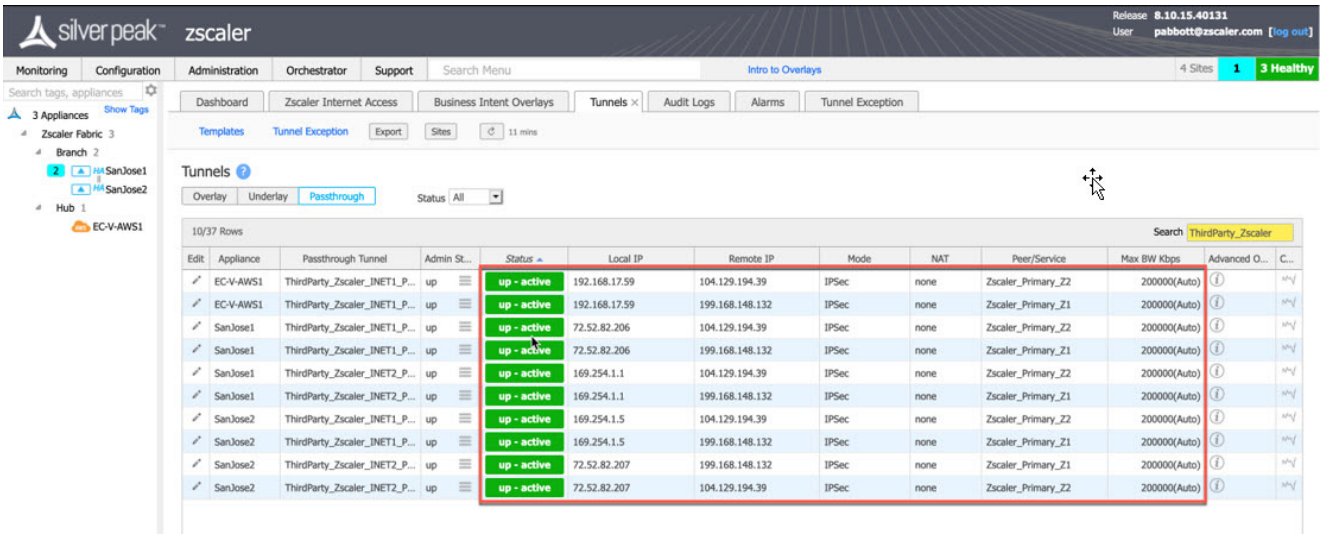

Figure 34. *View automated tunnel details*

©2024 Zscaler, Inc. All rights reserved.

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.

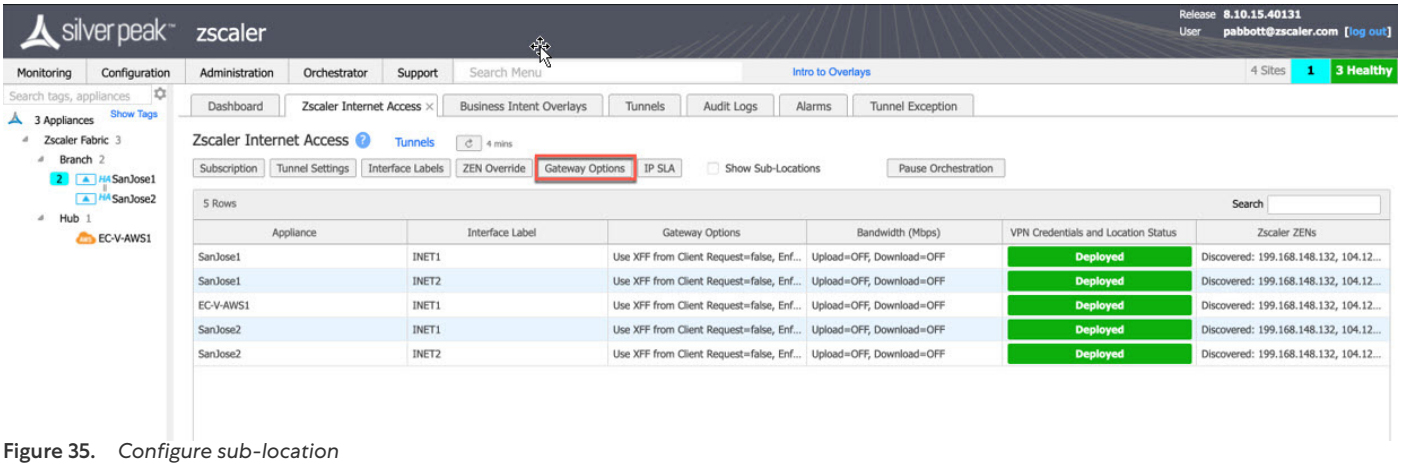

Figure 35. *Configure sub-location*

Enable Gateway Option Orchestration

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

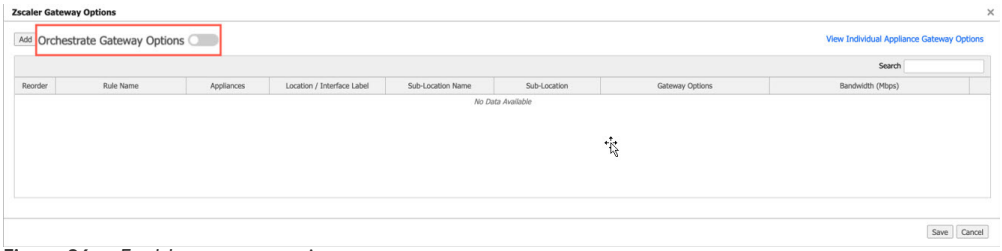

Figure 36. *Enable gateway options*

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

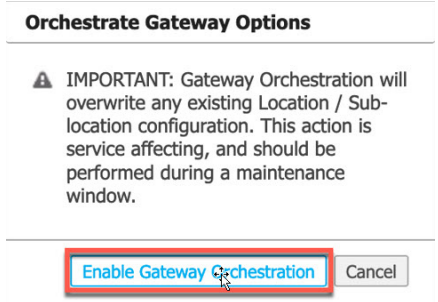

Figure 37. *Enable gateway option orchestration*

©2024 Zscaler, Inc. All rights reserved.

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**.

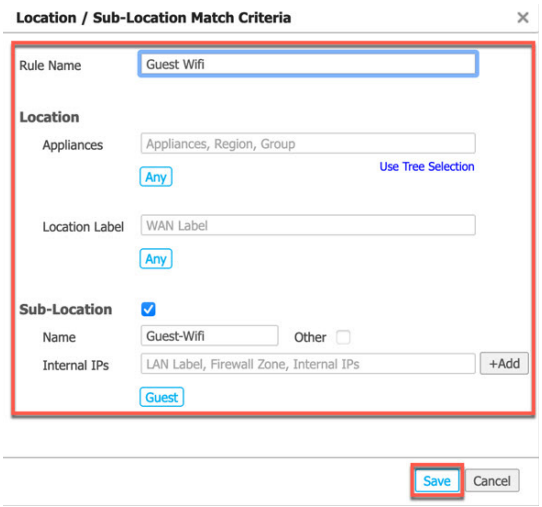

Figure 38. *Add sub-location*

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**.

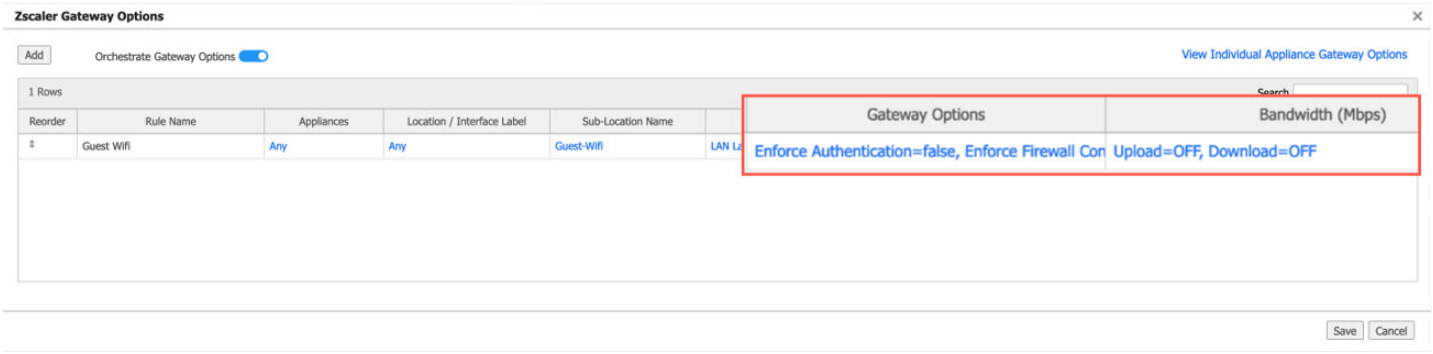

Figure 39. *Configure gateway options*

The **Zscaler Gateway Options** window appears.

©2024 Zscaler, Inc. All rights reserved.

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.

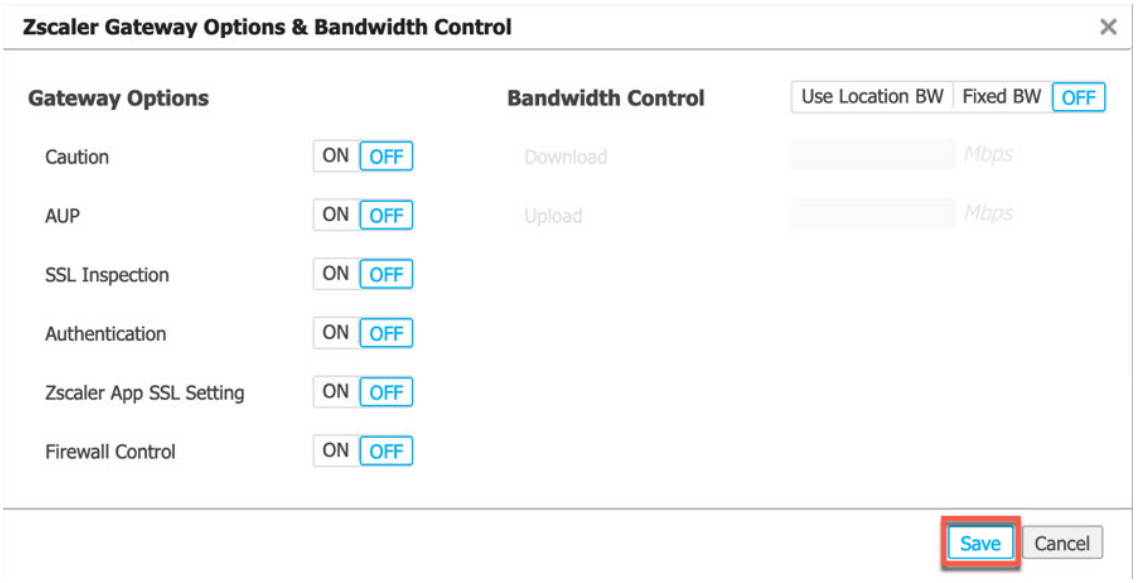

Figure 40. *Set gateway options*

Change Gateway Options Confirmation

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

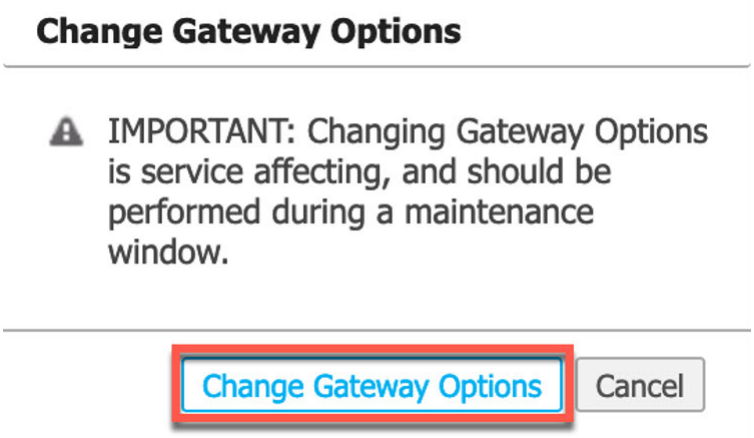

Figure 41. *Change gateway options confirmation*

©2024 Zscaler, Inc. All rights reserved.

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.

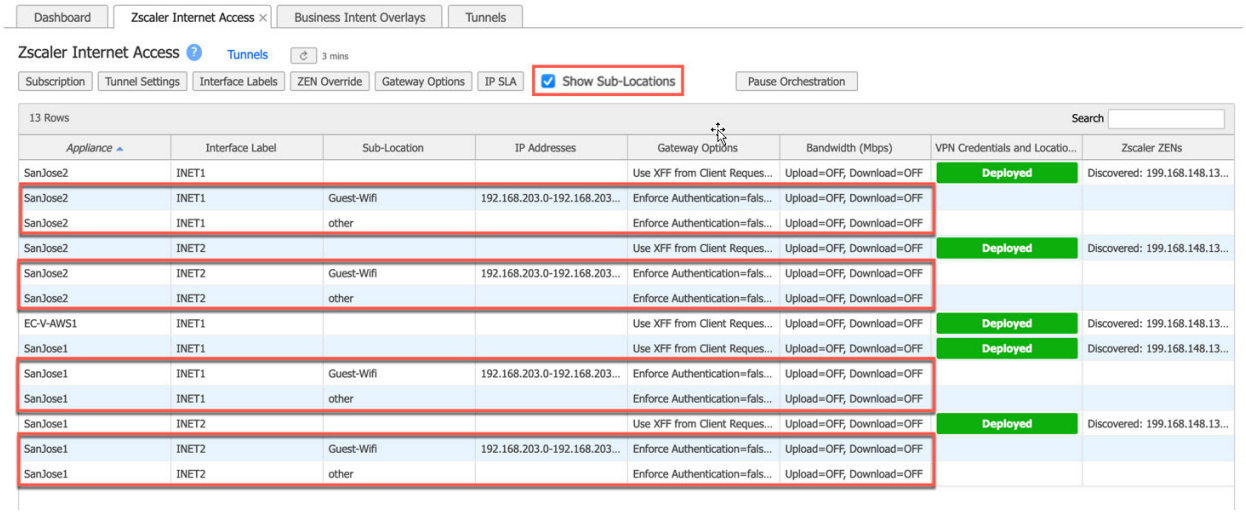

Figure 42. *Verify gateway options*

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**.

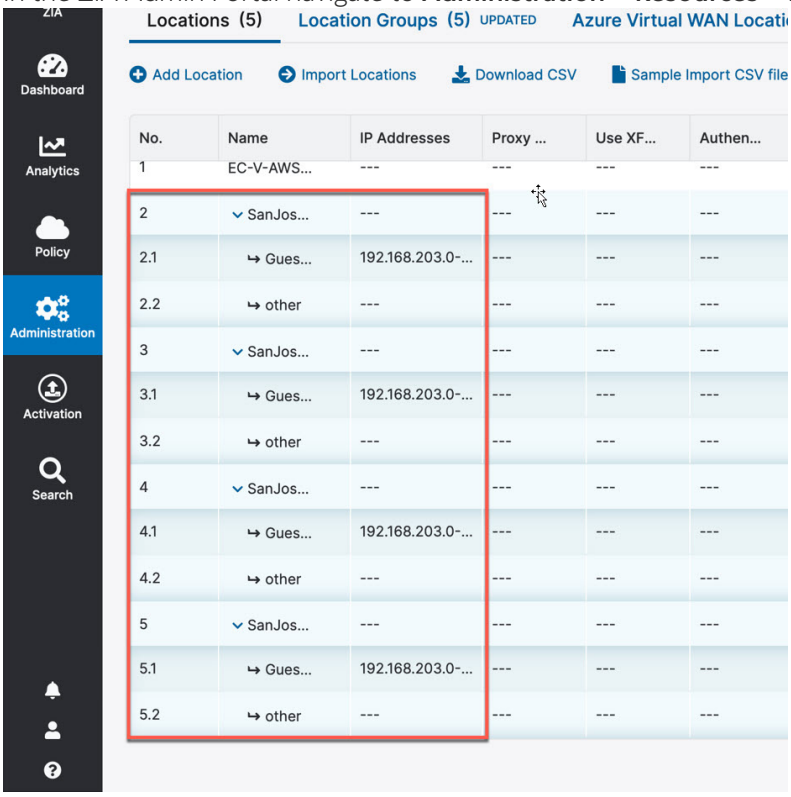

Figure 43. *Verify sub-locations in ZIA*

©2024 Zscaler, Inc. All rights reserved.

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**.

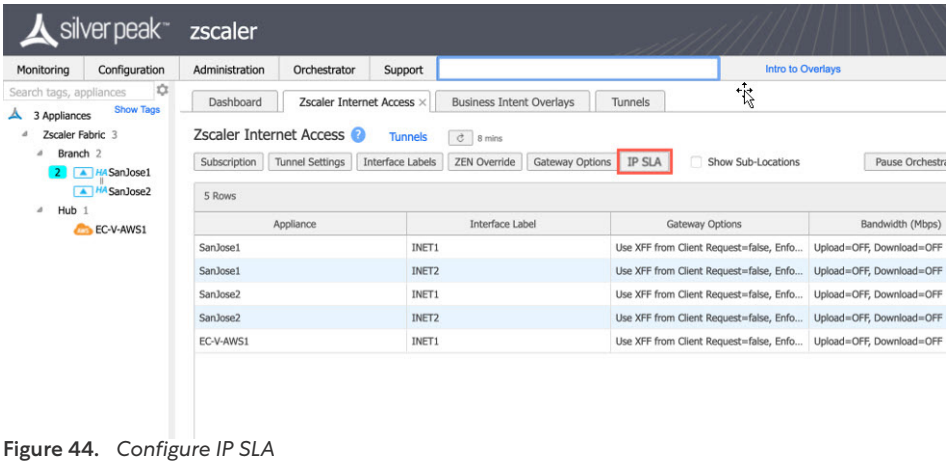

Figure 44. *Configure IP SLA*

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**.

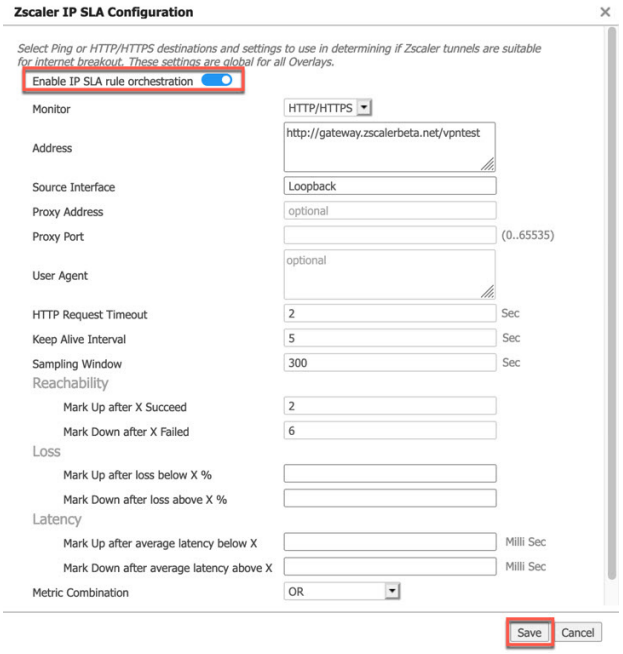

Figure 45. *Edit the IP SLA rule*

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

©2024 Zscaler, Inc. All rights reserved.

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**.

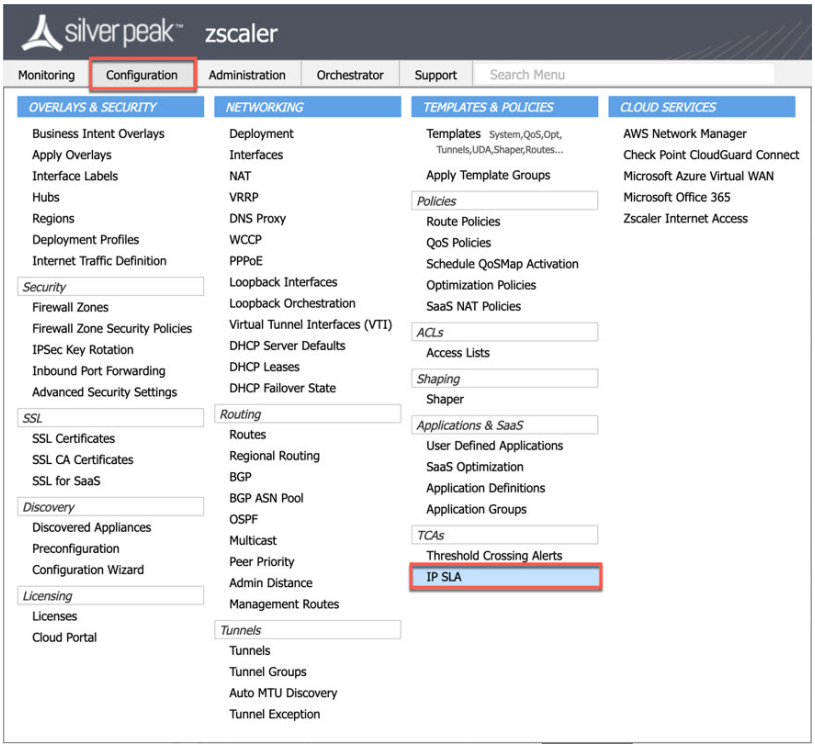

Figure 46. *Navigate to IP SLA settings*

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.

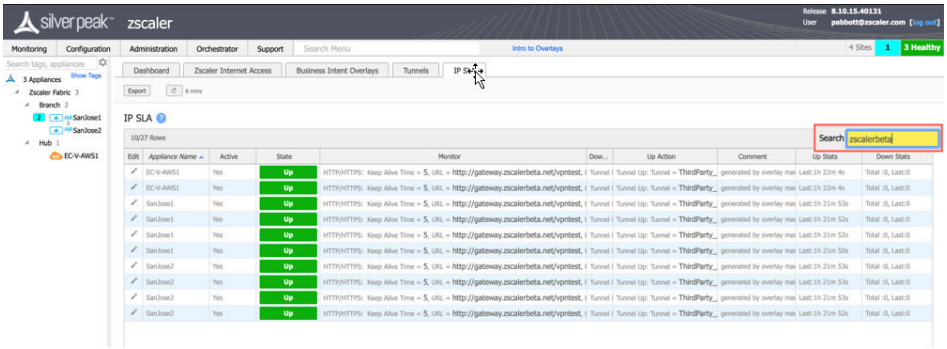

Figure 47. *Verify the IP SLA rule*

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

©2024 Zscaler, Inc. All rights reserved.

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**.

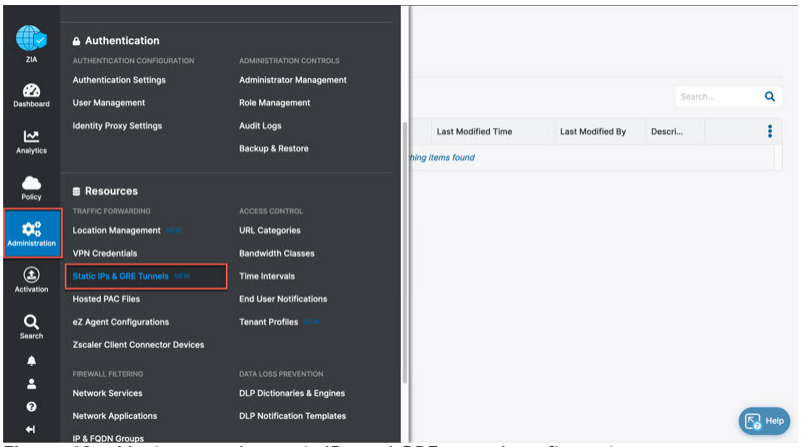

Figure 48. *Navigate to the static IPs and GRE tunnel configuration screen*

Add a Static IP Configuration

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

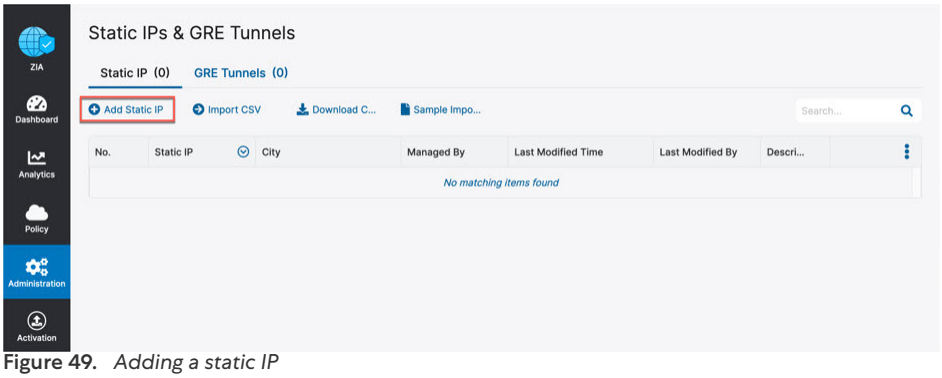

Figure 49. *Adding a static IP*

©2024 Zscaler, Inc. All rights reserved.

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.

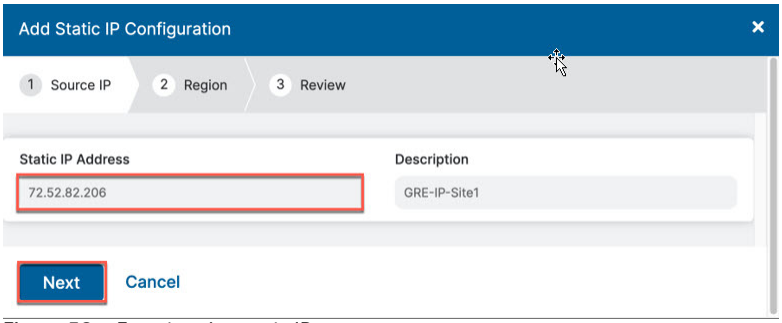

Figure 50. *Entering the static IP*

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**.

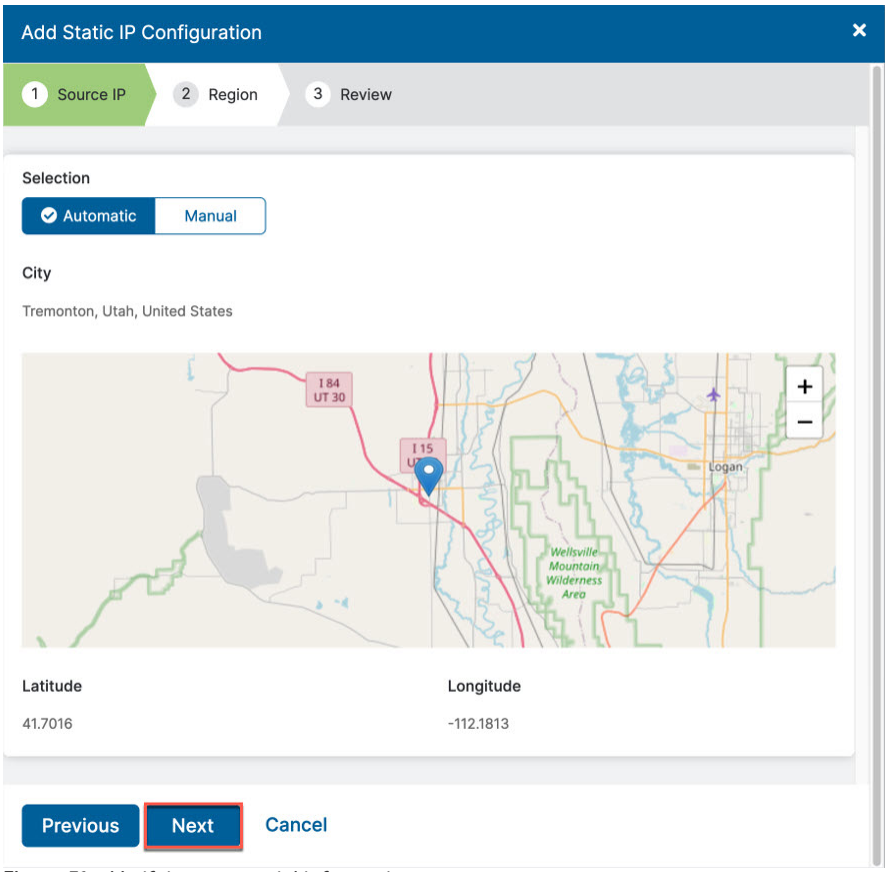

Figure 51. *Verifying geospatial information*

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

©2024 Zscaler, Inc. All rights reserved.

Review Information and Save

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

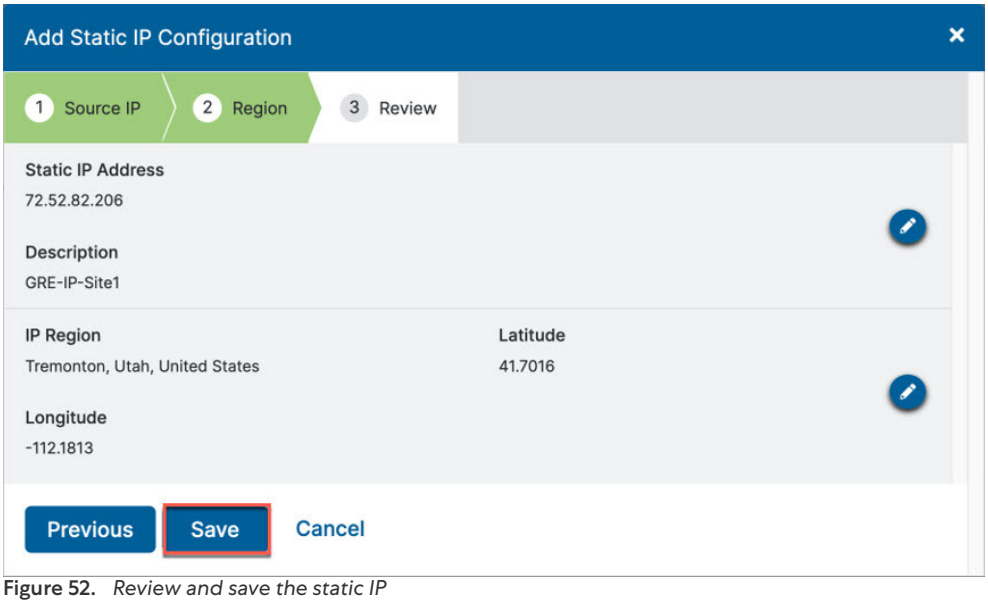

Figure 52. *Review and save the static IP*

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.

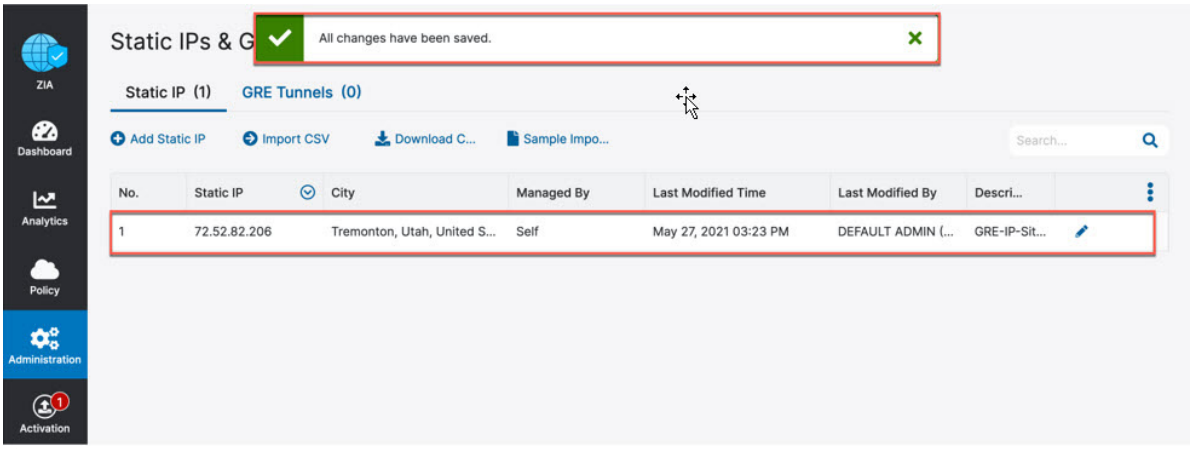

Figure 53. *Validate that the static IP was saved*

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

©2024 Zscaler, Inc. All rights reserved.

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**:

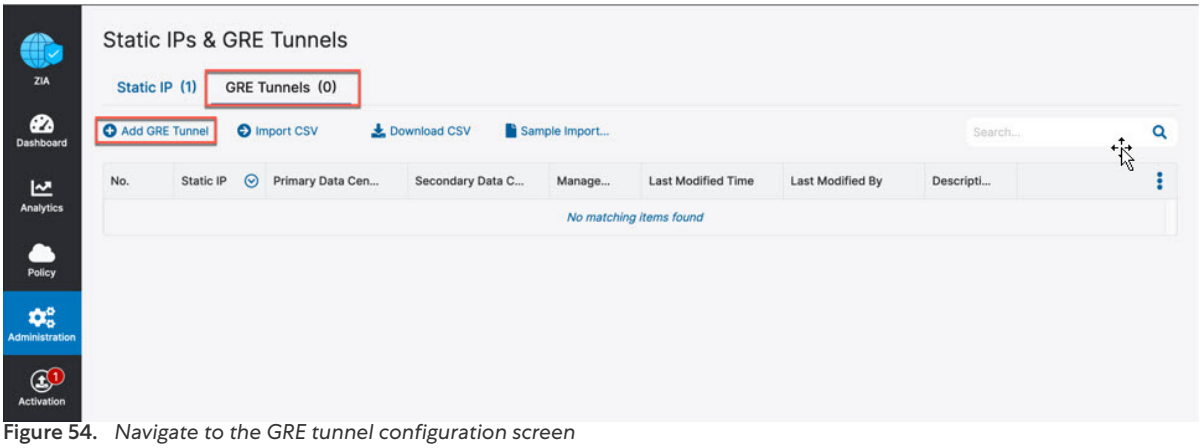

Figure 54. *Navigate to the GRE tunnel configuration screen*

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**.

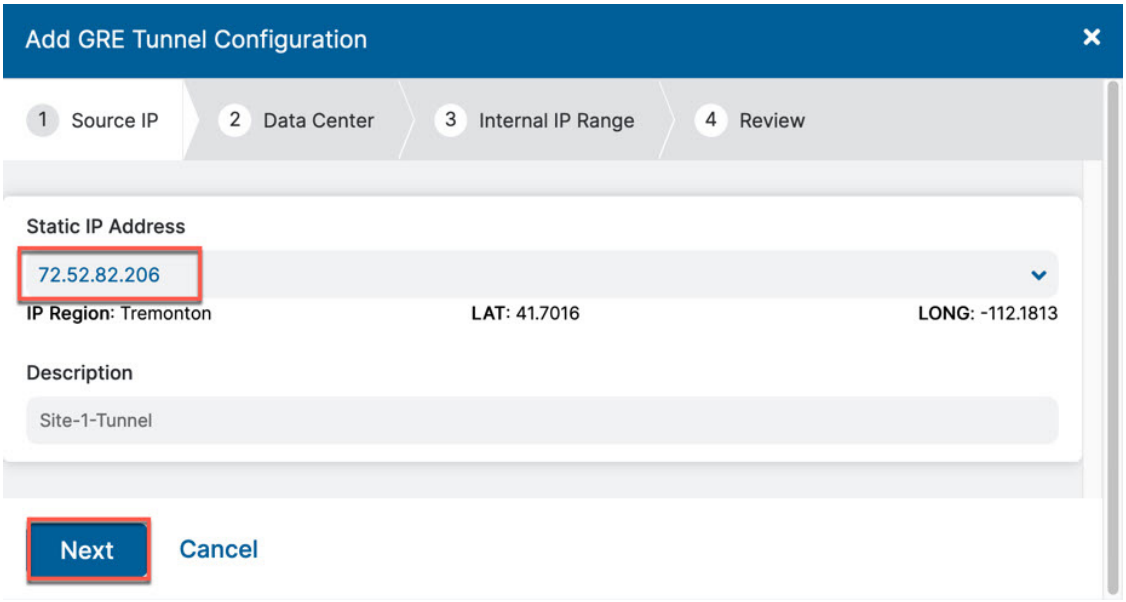

Figure 55. *Choose the GRE tunnel source IP*

©2024 Zscaler, Inc. All rights reserved.

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**.

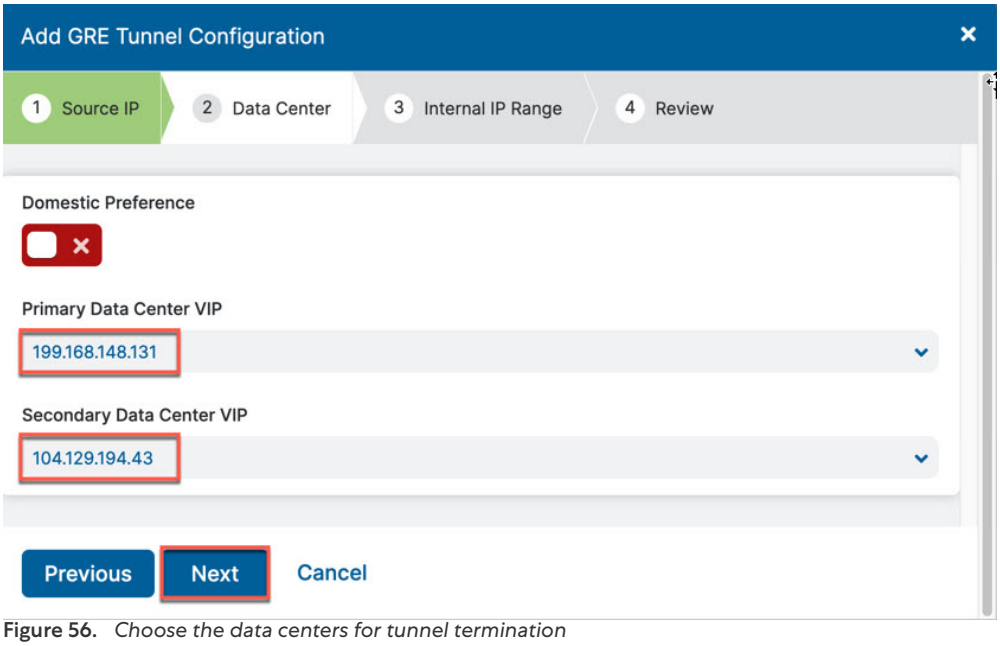

Figure 56. *Choose the data centers for tunnel termination*

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.

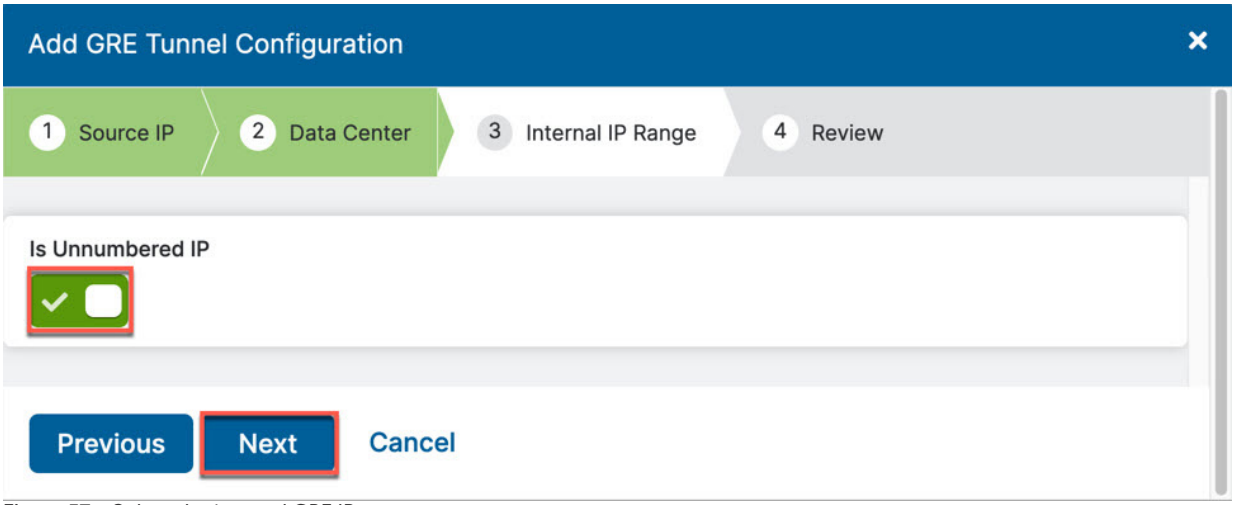

Figure 57. *Select the internal GRE IP range*

©2024 Zscaler, Inc. All rights reserved.

Save Tunnel Configuration

Review the configuration and click **Save**.

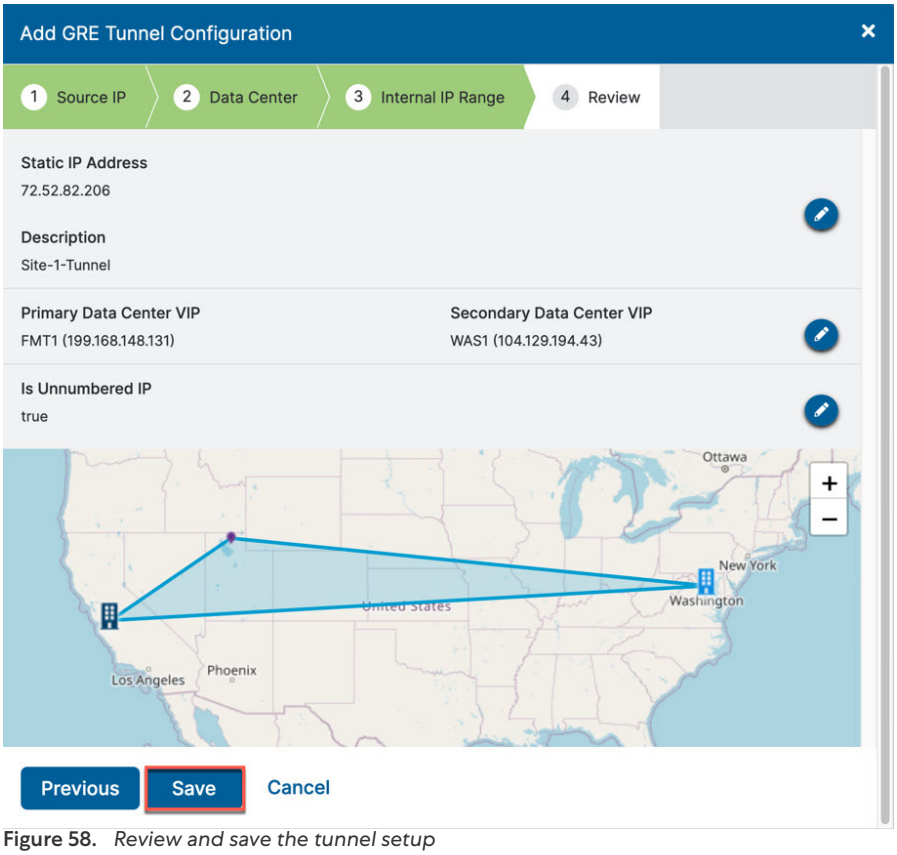

Figure 58. *Review and save the tunnel setup*

Activate and Verify All Configuration Changes

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

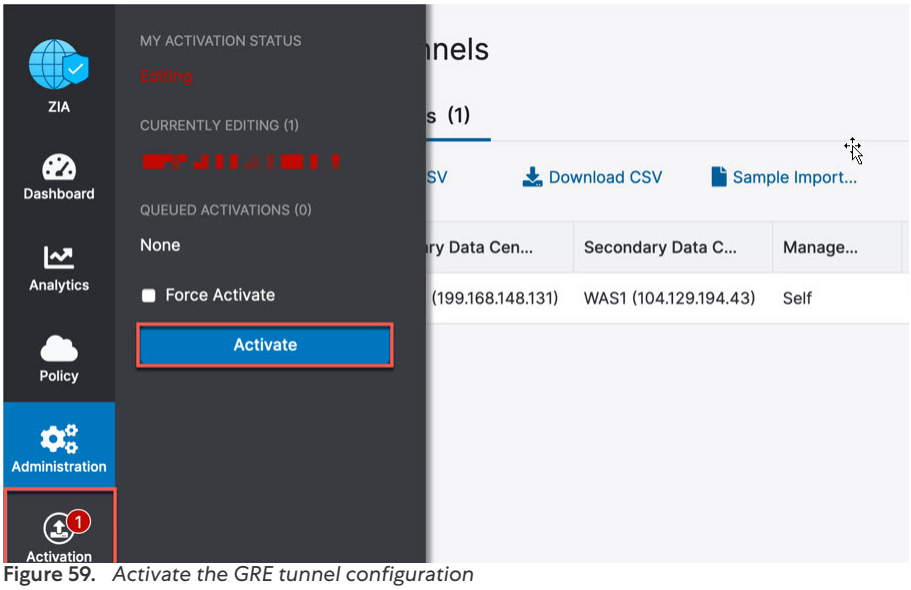

Figure 59. *Activate the GRE tunnel configuration*

©2024 Zscaler, Inc. All rights reserved.

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

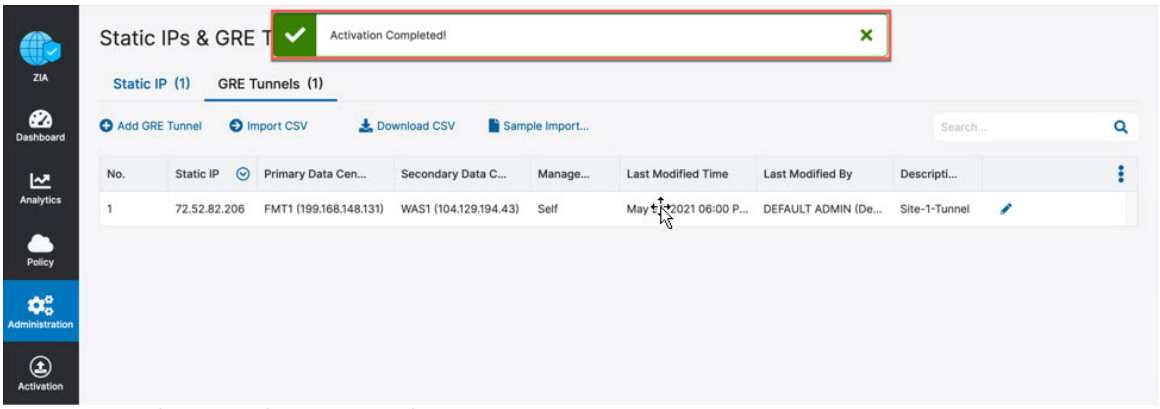

Figure 60. *Verify that the GRE tunnel configuration was activated*

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**.

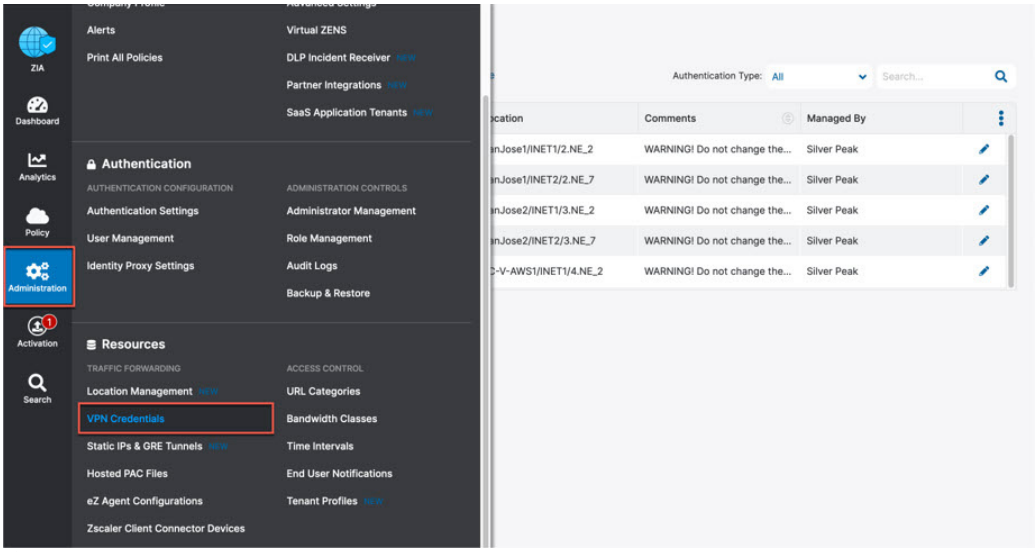

Figure 61. *Navigate to VPN credentials*

©2024 Zscaler, Inc. All rights reserved.

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.

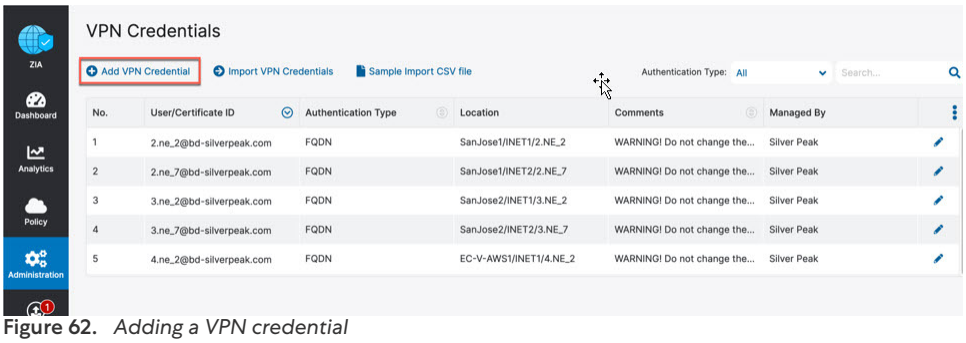

Figure 62. *Adding a VPN credential*

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.

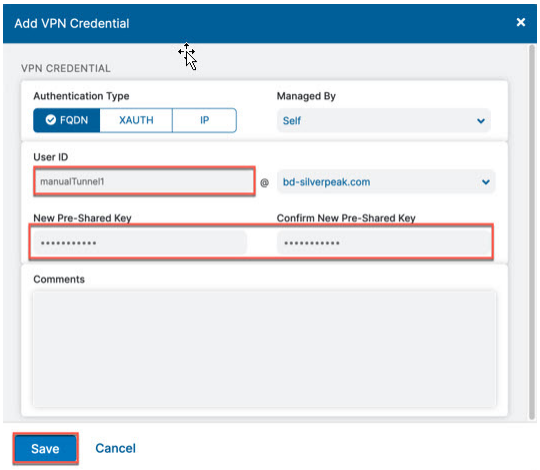

Figure 63. *Enter VPN credential data*

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.

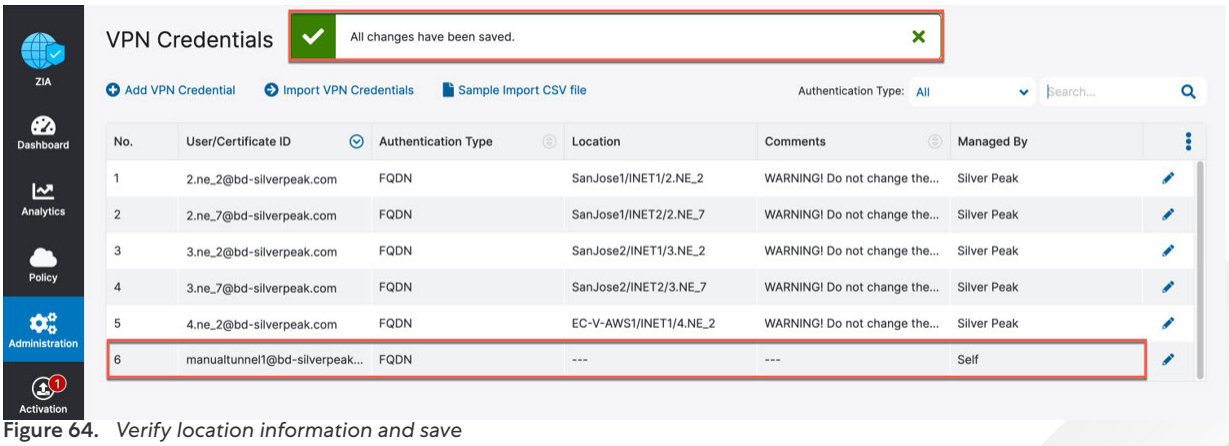

Figure 64. *Verify location information and save*

©2024 Zscaler, Inc. All rights reserved.

Activate Pending Changes

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

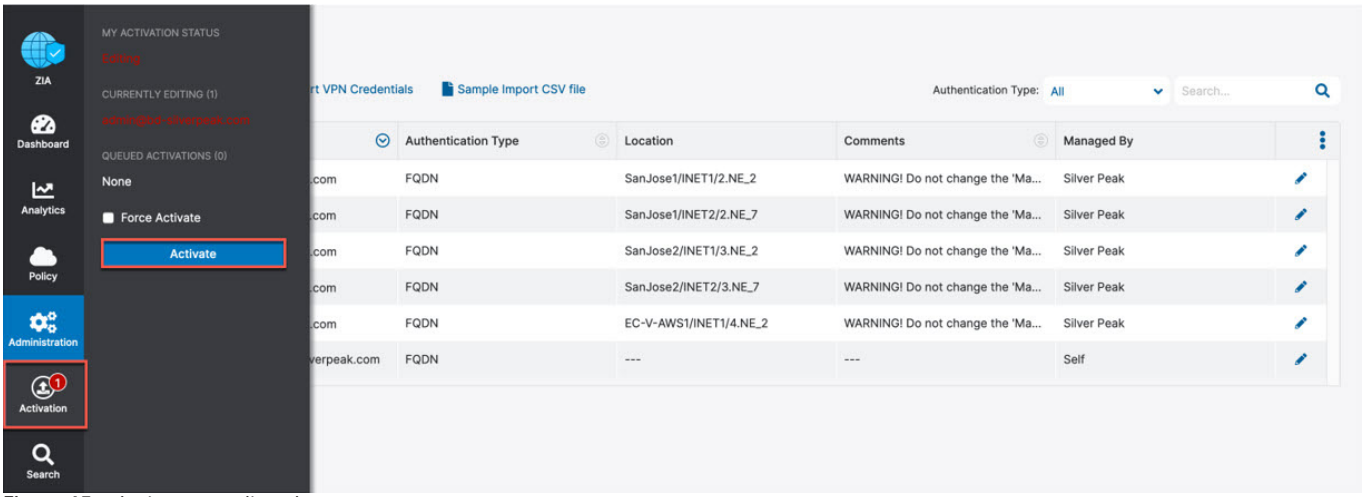

Figure 65. *Activate pending changes*

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.

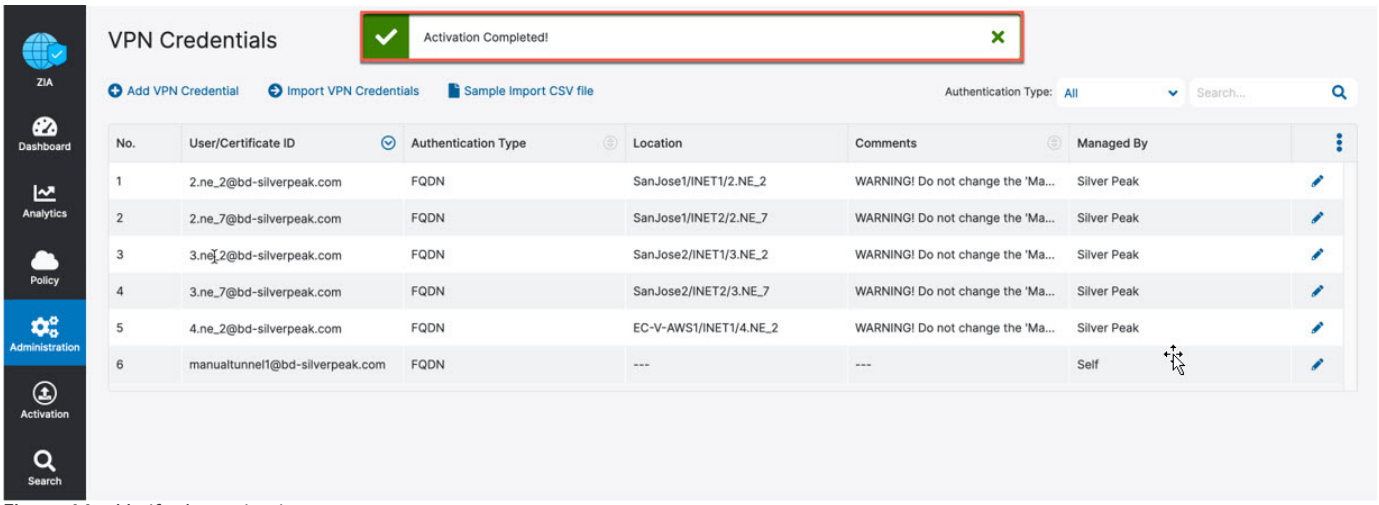

Figure 66. *Verify the activation*

©2024 Zscaler, Inc. All rights reserved.

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**.

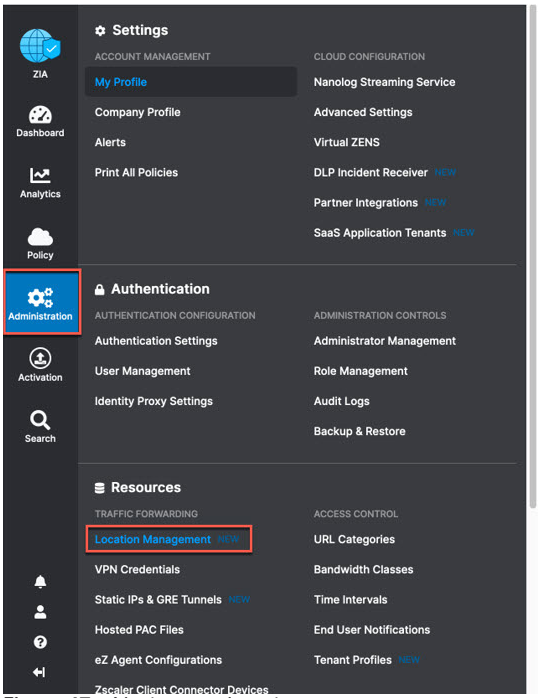

Figure 67. *Navigate to locations*

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.

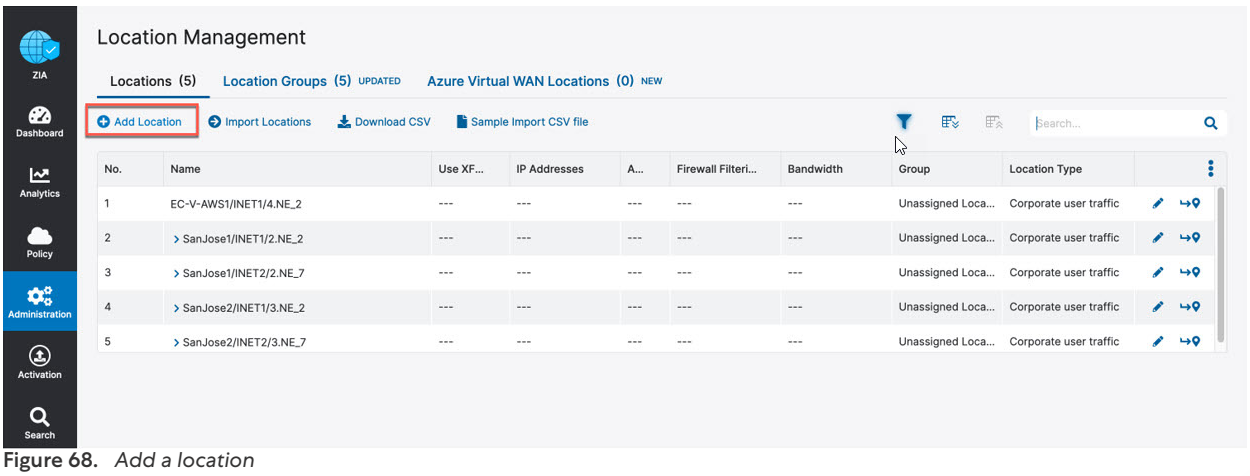

Figure 68. *Add a location*

©2024 Zscaler, Inc. All rights reserved.

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](#).

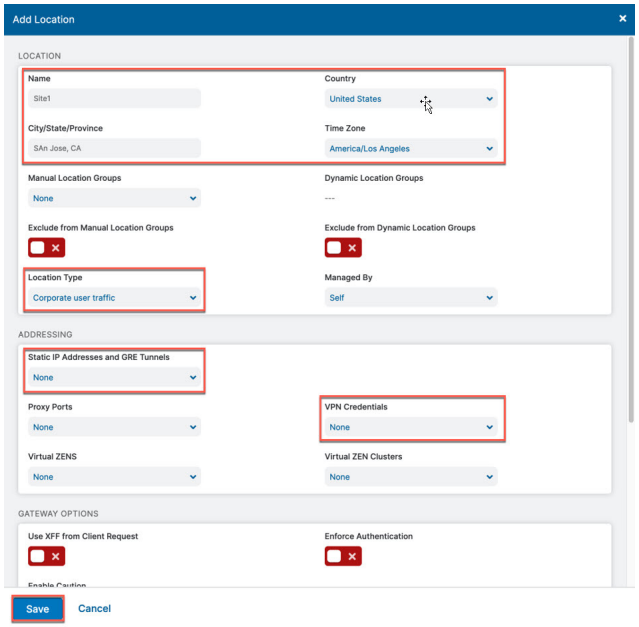

Figure 69. *Enter the location data*

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.

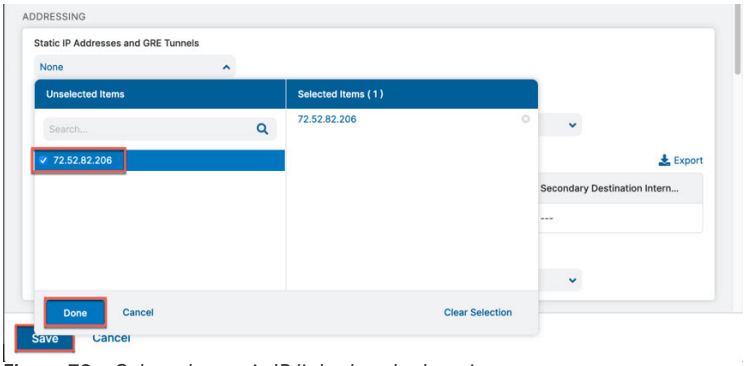

Figure 70. *Select the static IP linked to the location*

©2024 Zscaler, Inc. All rights reserved.

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

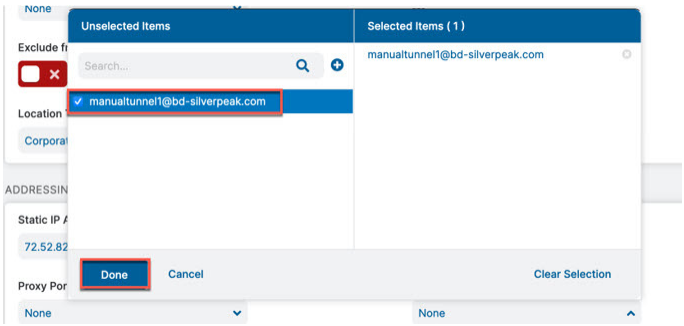

Figure 71. *Add VPN credential to location and save*

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.

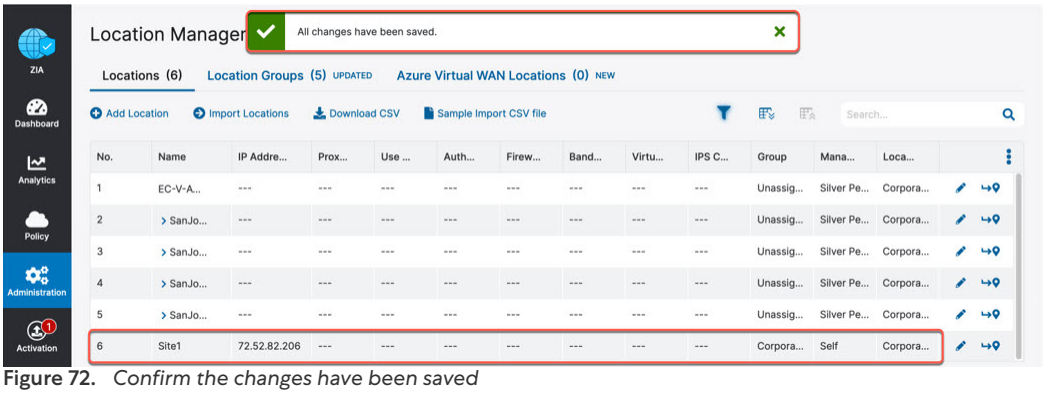

Figure 72. *Confirm the changes have been saved*

Activate Pending Changes

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

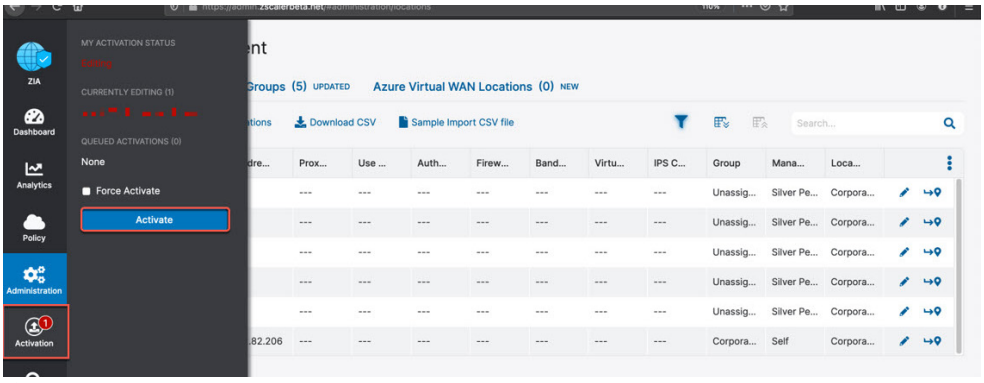

Figure 73. *Activate changes*

©2024 Zscaler, Inc. All rights reserved.

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.

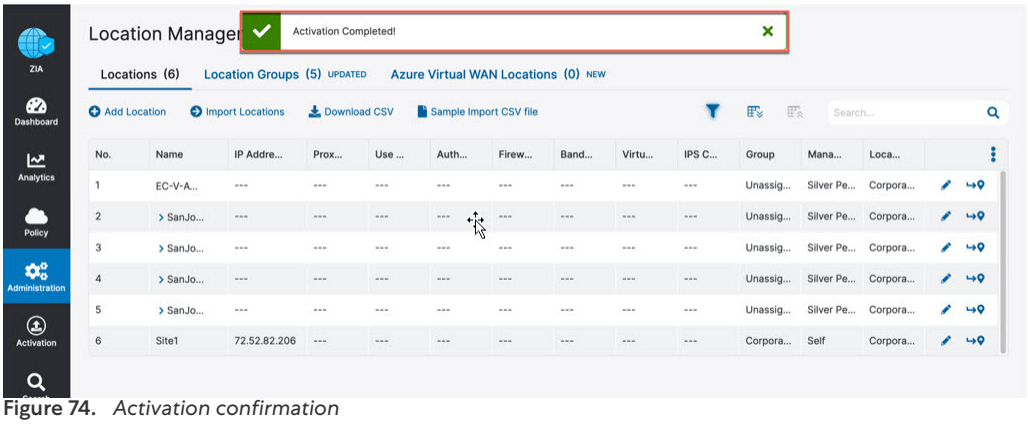

Figure 74. *Activation confirmation*

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.

©2024 Zscaler, Inc. All rights reserved.

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**.

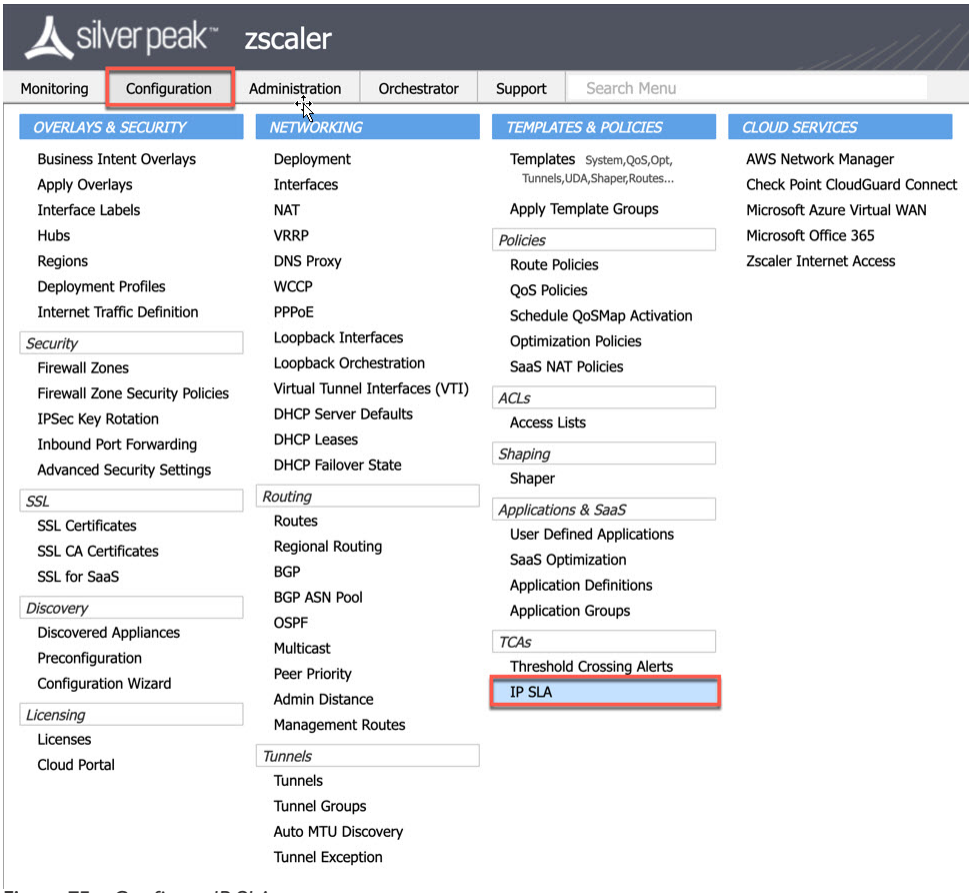

Figure 75. *Configure IP SLA*

©2024 Zscaler, Inc. All rights reserved.

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.

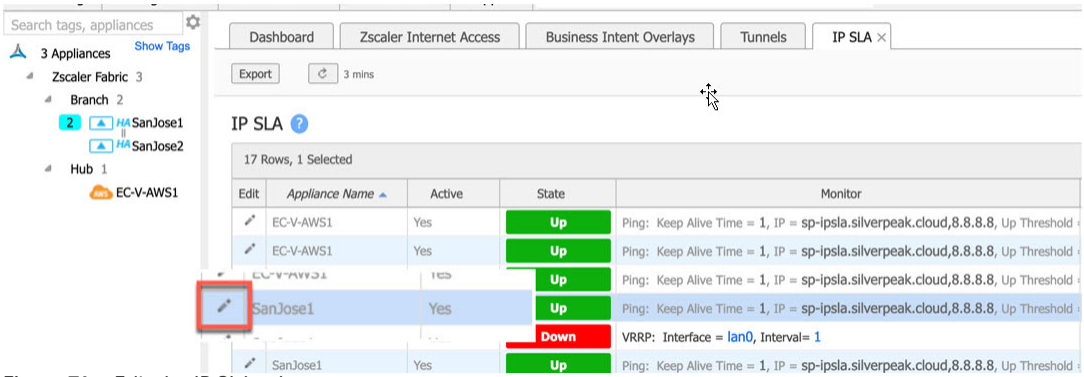

Figure 76. *Edit the IP SLA rule*

Add Rule and Target

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

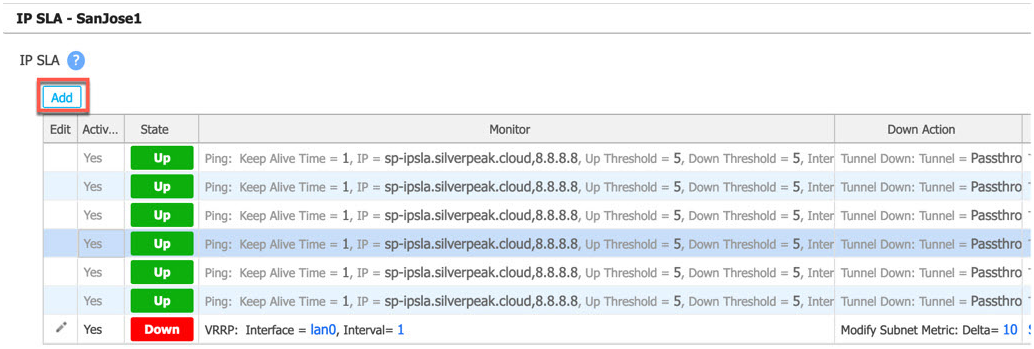

Figure 77. *Add rule and target*

©2024 Zscaler, Inc. All rights reserved.

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.

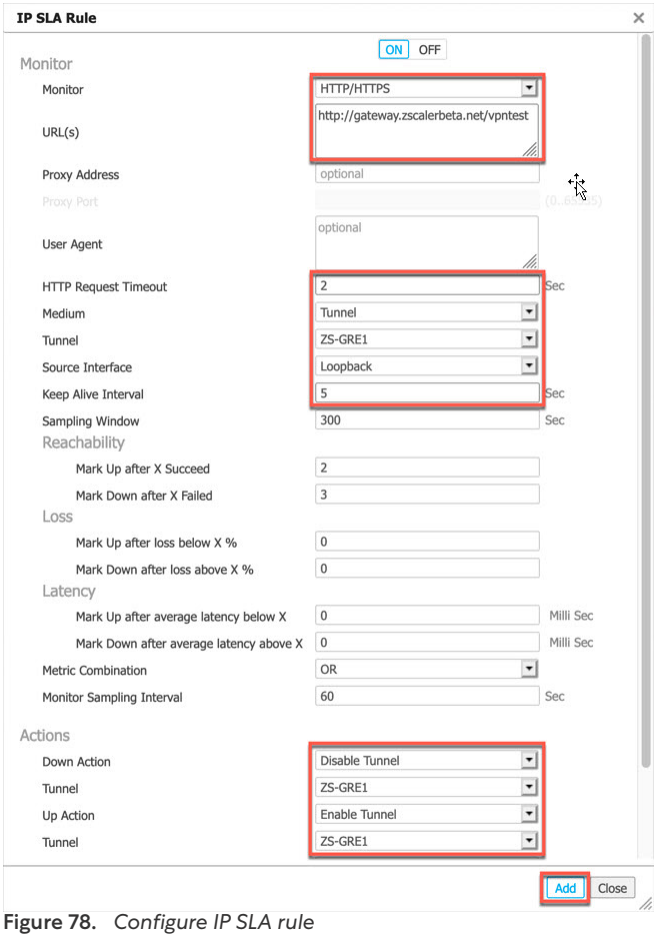

Figure 78. *Configure IP SLA rule*

©2024 Zscaler, Inc. All rights reserved.

Verify IP SLA Rule

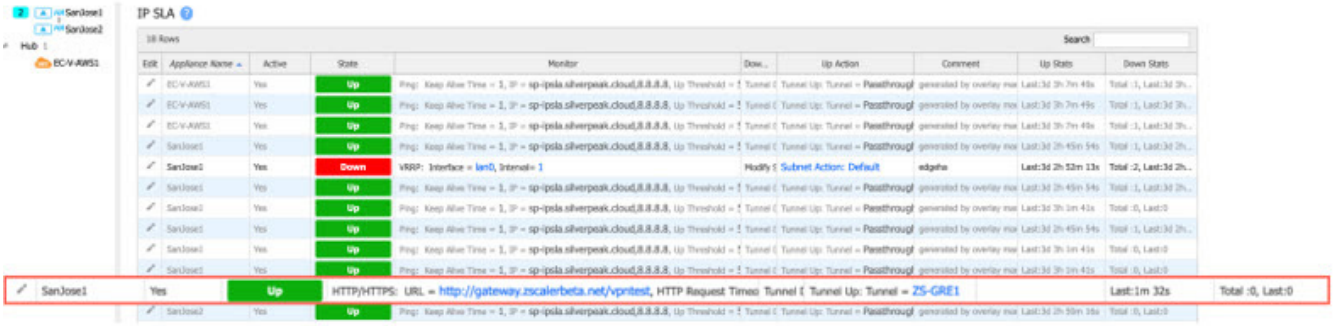

Figure 79. *Verify the IP SLA Rule*

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

©2024 Zscaler, Inc. All rights reserved.

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**.

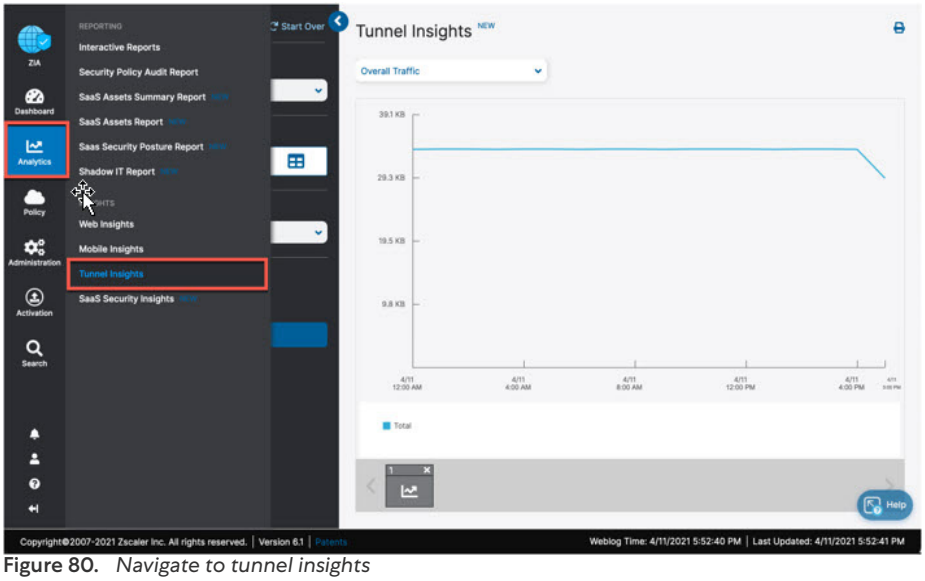

Figure 80. *Navigate to tunnel insights*

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**.

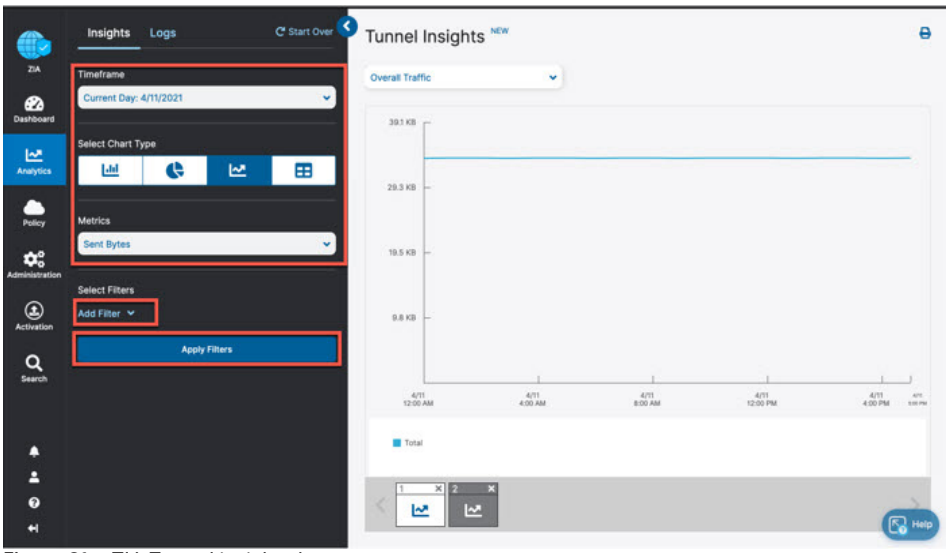

Figure 81. *ZIA Tunnel insight charts*

To learn more, see ZIA tunnel insights (government agencies, see ZIA tunnel insights).

©2024 Zscaler, Inc. All rights reserved.

Tunnel Logging

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

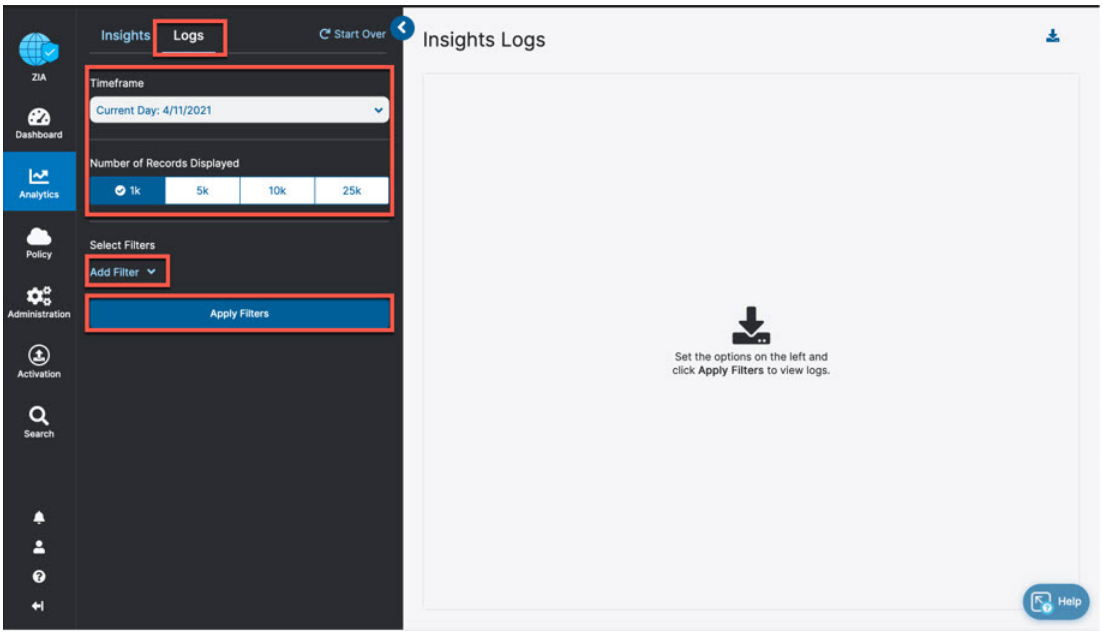

Figure 82. *Viewing ZIA tunnel logs*

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).

©2024 Zscaler, Inc. All rights reserved.

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

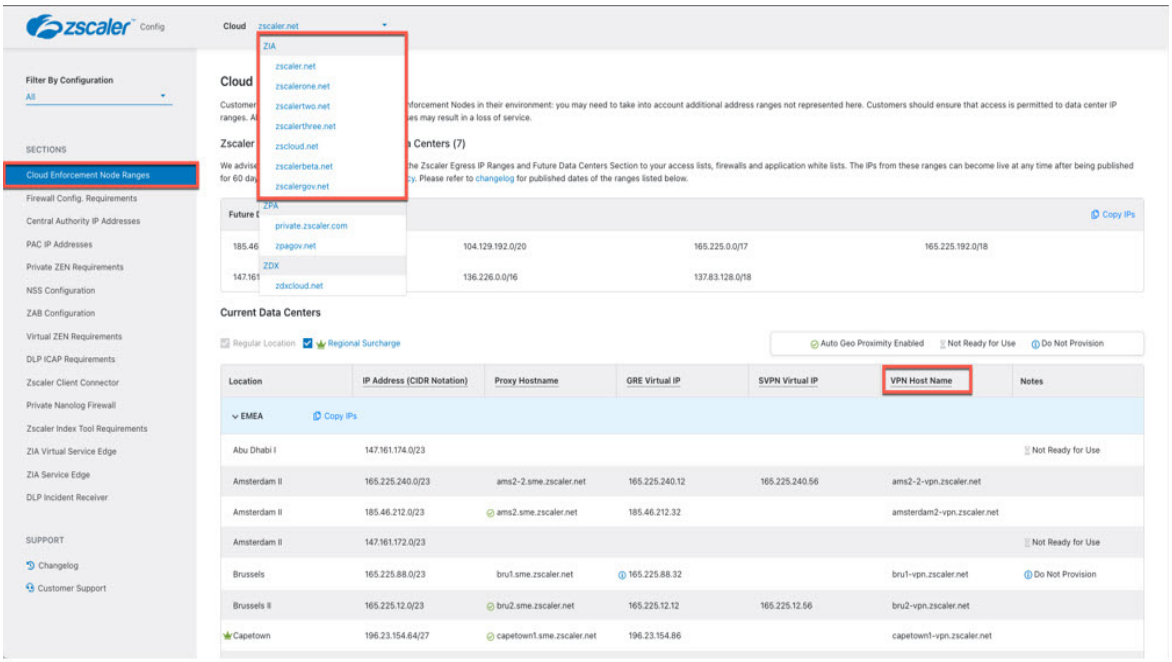

Figure 83. *Zscaler public IP reference*

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
```

©2024 Zscaler, Inc. All rights reserved.

```
;; 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
```

©2024 Zscaler, Inc. All rights reserved.

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**.

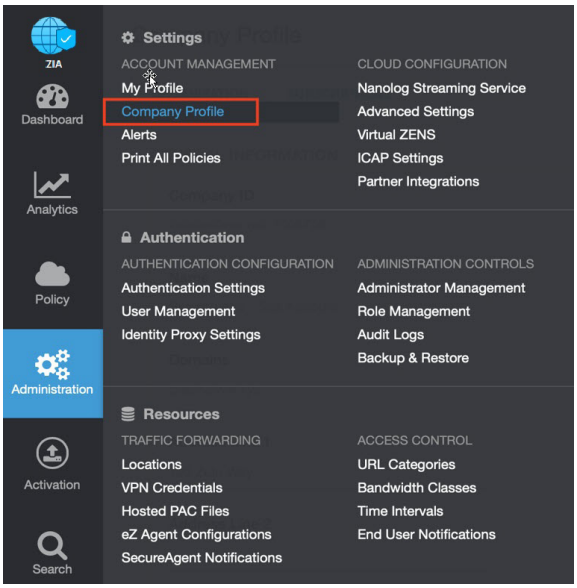

Figure 84. *Collecting details to open support case with Zscaler TAC*

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

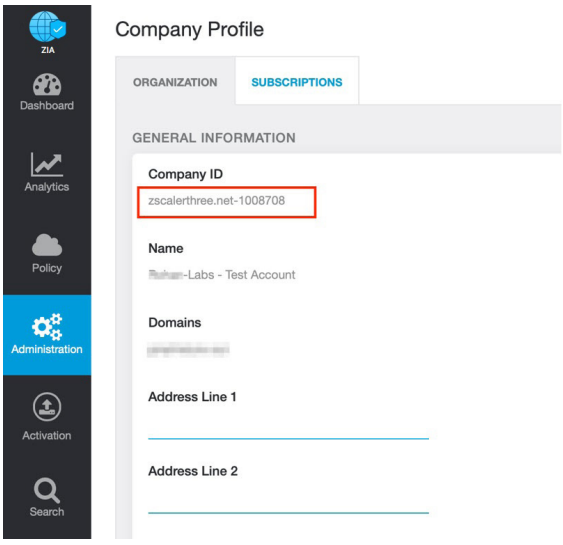

Figure 85. *Save your company ID information*

©2024 Zscaler, Inc. All rights reserved.

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

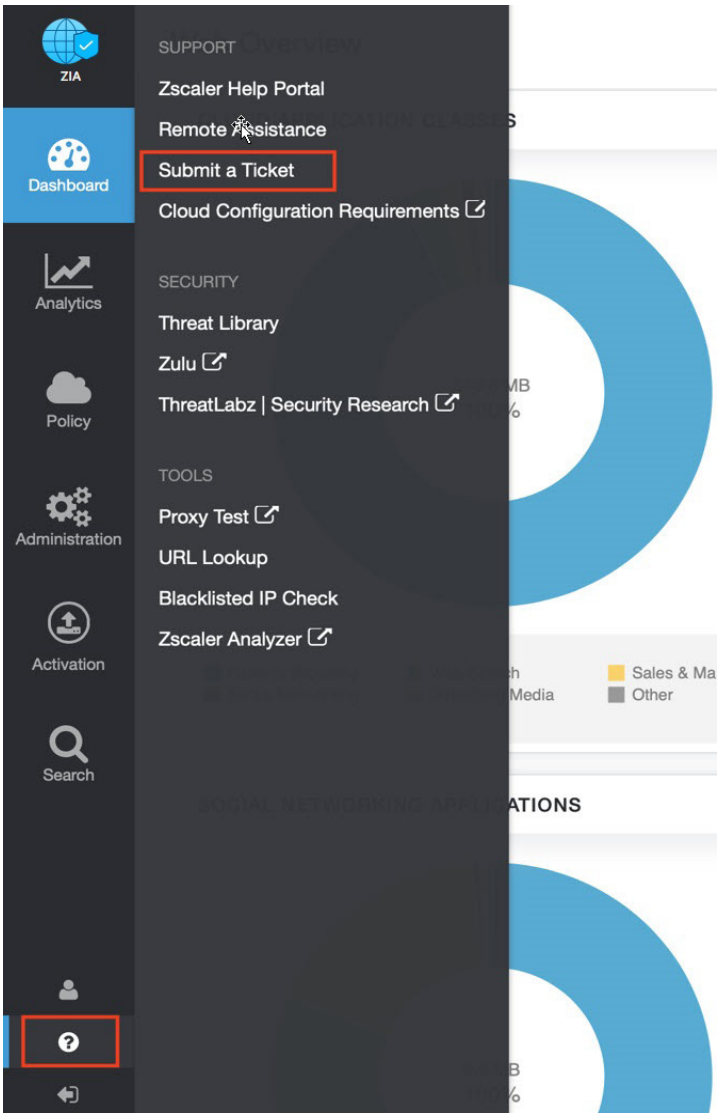

Figure 86. *Submit a ticket*

©2024 Zscaler, Inc. All rights reserved.

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.

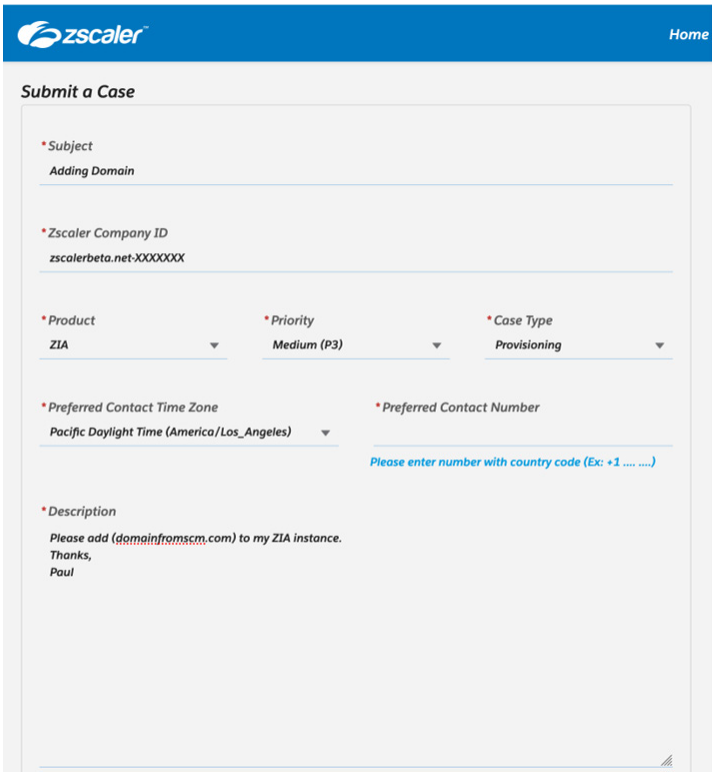

Figure 87. *Adding a domain*

©2024 Zscaler, Inc. All rights reserved.