

ZSCALER AND VMWARE DEPLOYMENT GUIDE

Contents

Terms and Acronyms	6
About This Document	7
Zscaler Overview	7
VMware Overview	7
Audience	7
Prerequisites	7
Software Versions	7
Request for Comments	7
Zscaler and VMware Introduction	8
ZIA Overview	8
ZPA Overview	8
Zscaler Resources	9
VMware SD-WAN	10
VMware Resources	10
Configuring Zscaler Internet Access (ZIA)	11
Logging into ZIA	11
Configure ZIA for API Access	12
Adding SD-WAN Partner Key	13
Verify SD-WAN Partner Key	14
Adding a Partner Administrator Role	15
Creating Partner Administrator Role	15
Administrator Management	16
Add Partner Administrator	17

Creating Partner Administrator	17
Active Pending Changes	18
Verify Activation	18
Configuring VMware SD-WAN	19
Configuring Automated IPSec and GRE Tunnels from the VCE	19
New Cloud Security Provider for Automated Deployment	19
Profile for Cloud Security Service	23
Monitor Provisioning Status	24
Network Services: Cloud Security Service Overview	24
Edge Override of Automated IPSec Tunnel Settings	25
Verify Tunnels are Up (Active)	25
Configuring Manual Tunnels from the VCE	26
New Cloud Security Provider for Manual Tunnels	26
Profile for Cloud Security Service	28
Edge Device Configuration for Manual Tunnels	29
Verify GRE Tunnel Configuration	31
Check and Verify Tunnel and CSS Provisioning Status	32
Configuring IPSec Tunnel from the VCG	33
New Non-SD-WAN Destination	33
Advanced Settings for Non SD-WAN Site	35
Enable Cloud VPN for a Profile	36
Check and Verify Tunnel and VCG Tunnel Provisioning Status	36
Configuring Gateway Options and Sub-Locations	37
Configuring Gateway Options for Edges	37
Configuring Sub-Locations	38
Verify Gateway Options and Sub-Locations in ZIA	39
Configuring Business Policy for ZIA	39
Configure Rule for VCE	40
Configure Rule for VCG	40

Appendix A: ZIA—Configuring Static IPs and GRE Tunnels	41
Add a Static IP Configuration	41
Enter the Static IP	42
Verify Geospatial data	42
Review Information and Save	43
Validate Static IP Configuration is Saved	43
Add a GRE Tunnel Configuration	44
Assign the Source IP to the Tunnel	44
Choose Data Centers for Tunnel Termination	45
Select GRE Tunnel Internal IP Subnet	46
Save Tunnel Configuration	47
Activate All Configuration Changes	48
Appendix B: Adding VPN Credentials for Manual Tunnel Creation	49
Go to VPN Credentials	49
Add a VPN Credential	49
Enter VPN Credential Data	50
Verify VPN Credential	50
Activate Pending Changes	51
Verify Activation	51
Appendix C: ZIA—Configuring a Location for Manual Tunnels	52
Add a Location	52
Enter Location Data	53
Add Static IP Location	54
Adding a VPN Credential to a Location	54

Confirm Changes Have Been Saved	55
Activate Pending Changes	55
Activation Confirmation	56
Appendix D: Verifying ZIA Configuration	57
Request Verification Page	57
Appendix E: Checking Tunnel Status in ZIA Admin	58
Tunnel Data Visualization	58
Tunnel Logging	59
Appendix F: Using the Audit Log for API Troubleshooting	60
Appendix G: Deriving the Zscaler IPSec VPN VIP	62
Appendix H: Requesting Zscaler Support	64

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSS	Comma-Separated Values
Cloud Security Service (VMware)	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
CSV	Comma-Separated Values
DC	Data Center
DMPO	Dynamic Multipath Optimization
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SSL	Secure Socket Layer (RFC6101)
VCE	VMware SD-WAN Edge
VCG	VMware SD-WAN Gateway
VCO	VMware SD-WAN Orchestrator
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access

About This Document

Zscaler Overview

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

VMware Overview

VMware (Nasdaq: [VMW](#)) software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. To learn more, refer to [VMware's website](#).

Audience

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

- [Zscaler Resources](#)
- [VMware Resources](#)
- [Appendix H: Requesting Zscaler Support](#)

Prerequisites

Zscaler Internet Access (ZIA)

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

VMware SD-WAN Orchestrator

- Enterprise account access to VMware SD-WAN Orchestrator
- Administrator login credentials
- One or more VMware SD-WAN Edge appliances with "Online" status in VMware SD-WAN Orchestrator

Software Versions

This document was written using ZIA v6.2 and VMware SD-WAN Orchestrator 5.0.

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 VMware Introduction

This guide provides GUI examples for configuring Zscaler Internet Access and VMware SD-WAN Orchestrator. All examples in this guide presume the reader has a basic comprehension of IP Networking. All examples in this guide explain how to provision new service with Zscaler and with VMware SD-WAN.



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

ZIA Overview

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

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

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

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

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a zero trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
ZIA Test Page	Provides information on your Zscaler cloud.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler IP Page	Add Zscaler Egress IP Ranges to your access lists, firewalls, and application allow lists.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
ZIA Test Page	Provides information on your Zscaler cloud.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler IP Page	Add Zscaler Egress IP Ranges to your access lists, firewalls, and application allow lists.
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.

VMware SD-WAN

SD-WAN is revolutionizing the traditional wide area networking landscape: complex, hardware-intensive, and hub-and-spoke networks are transformed into cloud-friendly, cost-effective, and agile architectures.

- VMware SD-WAN Orchestrators (VCOs) take care of simplified UI-based configurations, and function as the management plane of the solutions. The VCOs can be hosted on different premises supporting different consumption models from fully managed to on-premises.
- VMware SD-WAN Gateways (VCGs) are the control plane of the solution, helping to steer traffic between edges and towards the most optimal location for the cloud onramp.
- VMware SD-WAN Edges (VCEs) take care of the data plane connectivity between users and where data is located (public cloud, data center, SaaS applications). Edges leverage the SD-WAN overlay to achieve connectivity to one another, making the SD-WAN data plane agnostic to the underlying transport technology.

VMware Resources

The following table contains links to VMware support resources.

Name	Definition
VMware SD-WAN	Secure access service edge (SASE) platform that converges cloud networking and cloud security service.
VMware SD-WAN Support	Provides world-class technical assistance and personalized guidance to VMware SD-WAN customers 24/7/365.
VMware SD-WAN Knowledgebase	VMware knowledge base articles.

Configuring Zscaler Internet Access (ZIA)

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

Logging into ZIA

Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, [contact Zscaler Support](#). (government agencies, [contact Zscaler Support](#)).

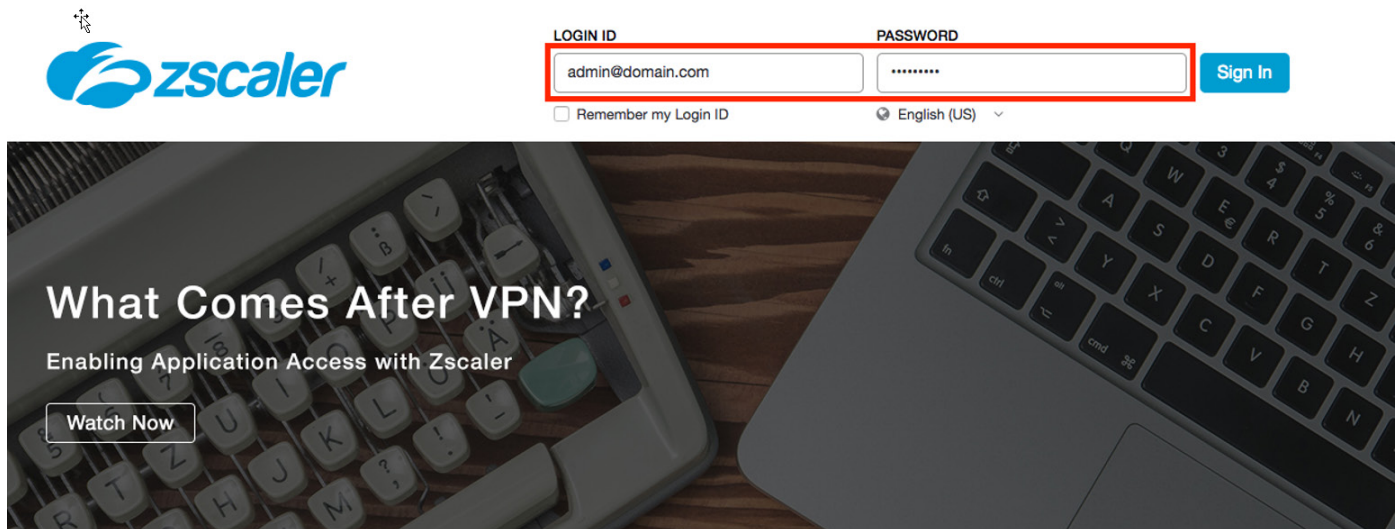


Figure 1. Log in to Zscaler

Configure ZIA for API Access

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

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

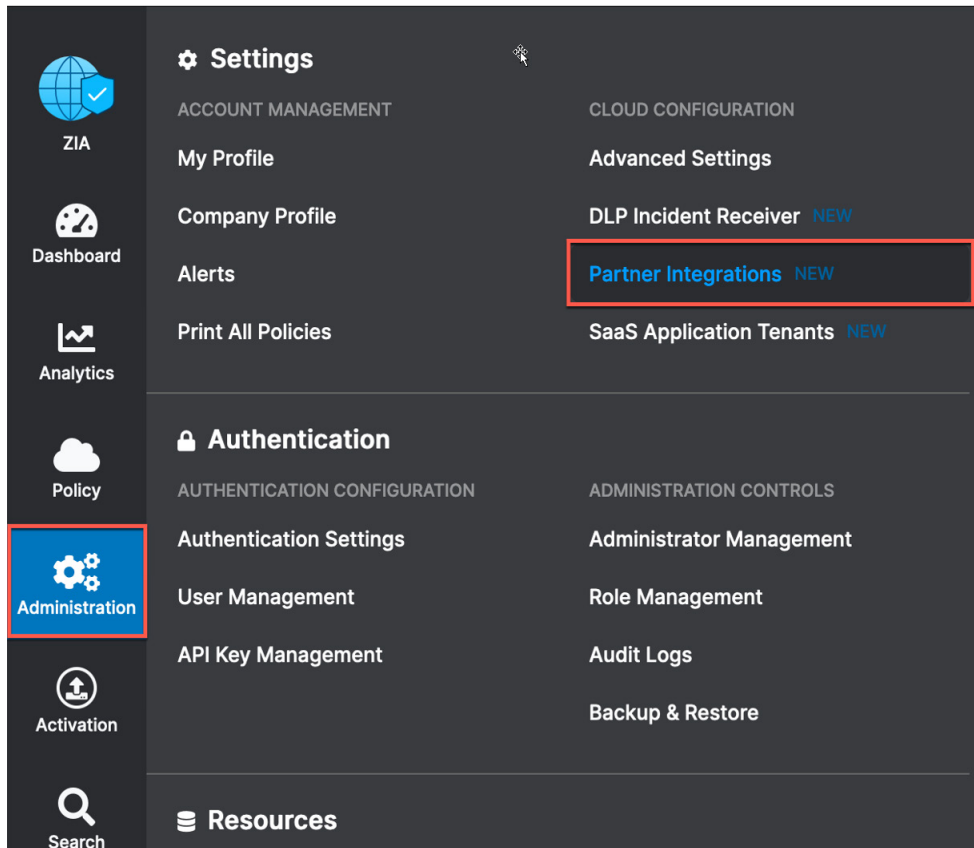


Figure 2. Configuring ZIA for API access

Adding SD-WAN Partner Key

In the **Partner Integrations** section of the ZIA Admin Portal, go to **SD-WAN > Add Partner Key**.

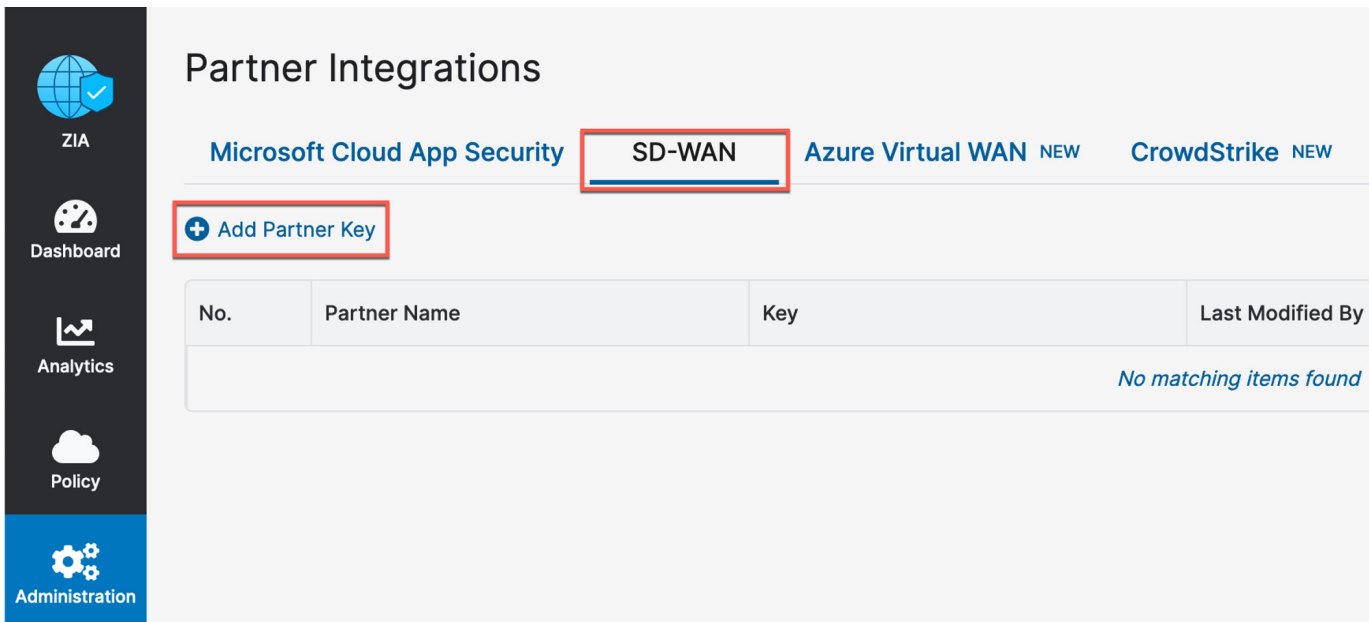


Figure 3. Add partner key

The **Add Partner Key** dialog appears. Type or select from the drop-down menu the SD-WAN vendor for which you want to create a partner key. After typing or selecting **VMware VeloCloud**, click **Generate**. You are returned to the prior page.

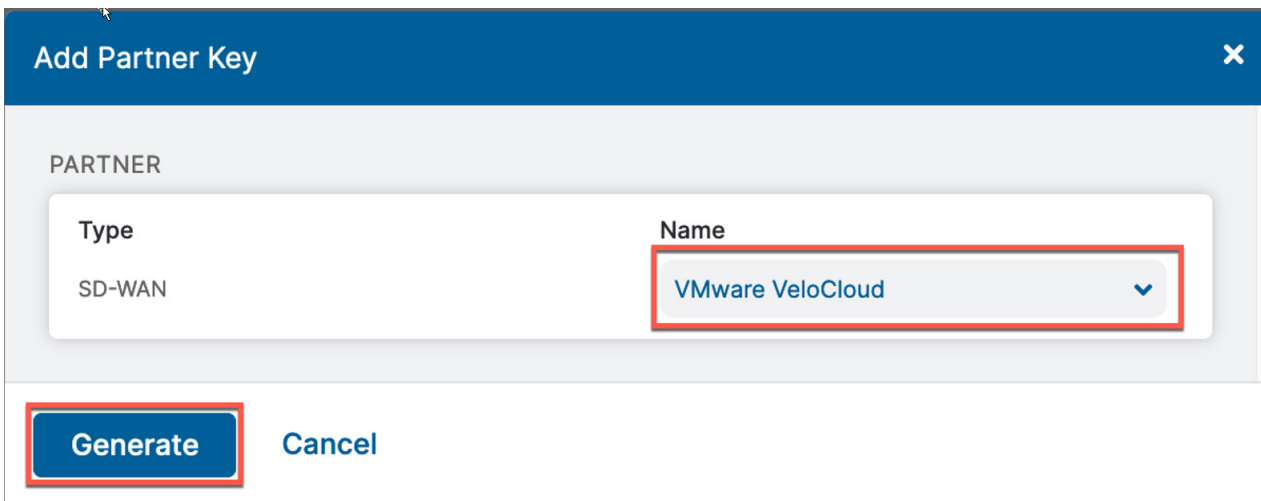


Figure 4. Add SD-WAN partner key

Verify SD-WAN Partner Key

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



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

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



The key value is required for the procedure described in [New Cloud Security Provider for Automated Deployment](#). Make sure to note the key value to enter it in the VCO later.

The screenshot shows the 'Partner Integrations' page in the Zscaler interface. The left-hand navigation menu includes ZIA, Dashboard, Analytics, Policy, Administration, and Activation (with a red circle and number 1). The main content area has tabs for 'Microsoft Cloud App Securit', 'SD-WAN' (selected), 'Azure Virtual WAN NEW', 'CrowdStrike NEW', and 'Carbon Black NEW'. Below the tabs is a '+ Add Partner Key' button. A table lists the partner keys:

No.	Partner Name	Key	Last Modified By	Last Modified On	
1	VMware VeloCloud	[REDACTED]	[REDACTED]	April 02, 2021 12:44 PM	[Edit] [Copy] [Delete]

Figure 5. Verify SD-WAN partner key

Adding a Partner Administrator Role

Next, you must create a Partner Administrator Role. This administrator is authenticated against the Zscaler ZIA provisioning API.

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

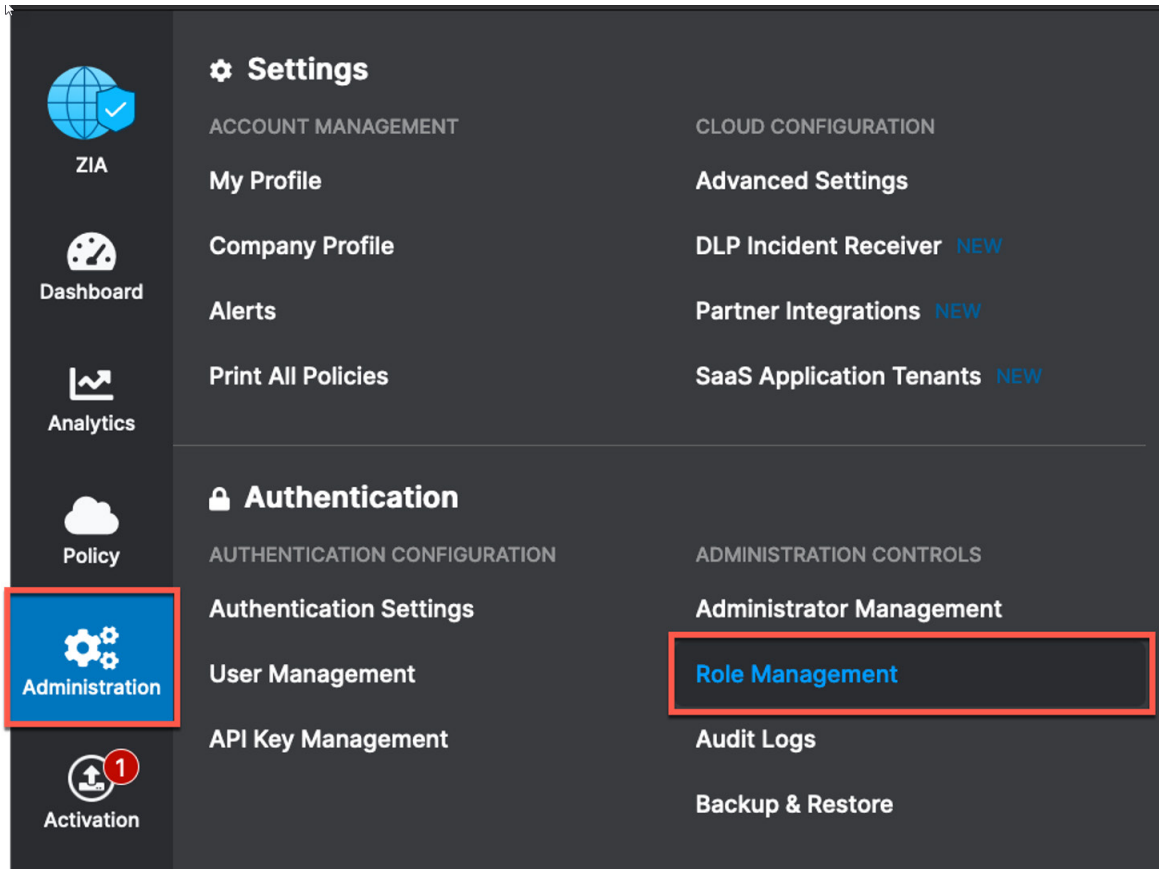


Figure 6. Adding Partner Administrator role

Creating Partner Administrator Role

Clicking the **Add Partner Administrator Role** option displays the **Add Partner Administrator Role** dialog.

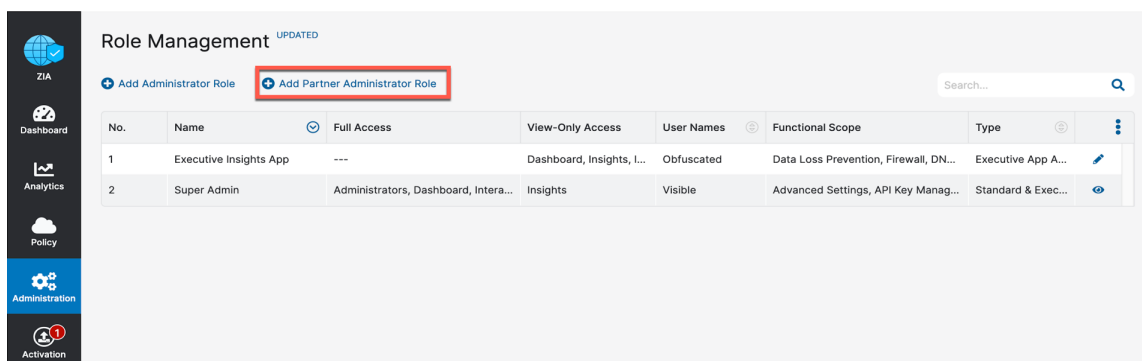


Figure 7. Add partner administrator role

A Partner Administrator Role lets you define the permission and access granted to third-party partners (such as a SD-WAN partner). After you name the Partner Administrator Role, change the **Access Control** to **Full**. The **Full** toggle allows partner admins to view and edit VPN credentials and locations that VCO is managing via the ZIA provisioning API. This is necessary for the VCO to be able to create new VPN credentials and locations for branch locations.

After you have completed these steps, click **Save**. You are returned to the prior page.

Figure 8. Creating partner administrator role

Administrator Management

The last step is creating a Partner Administrator. Go to **Administration > Administration Controls > Administrator Management**.

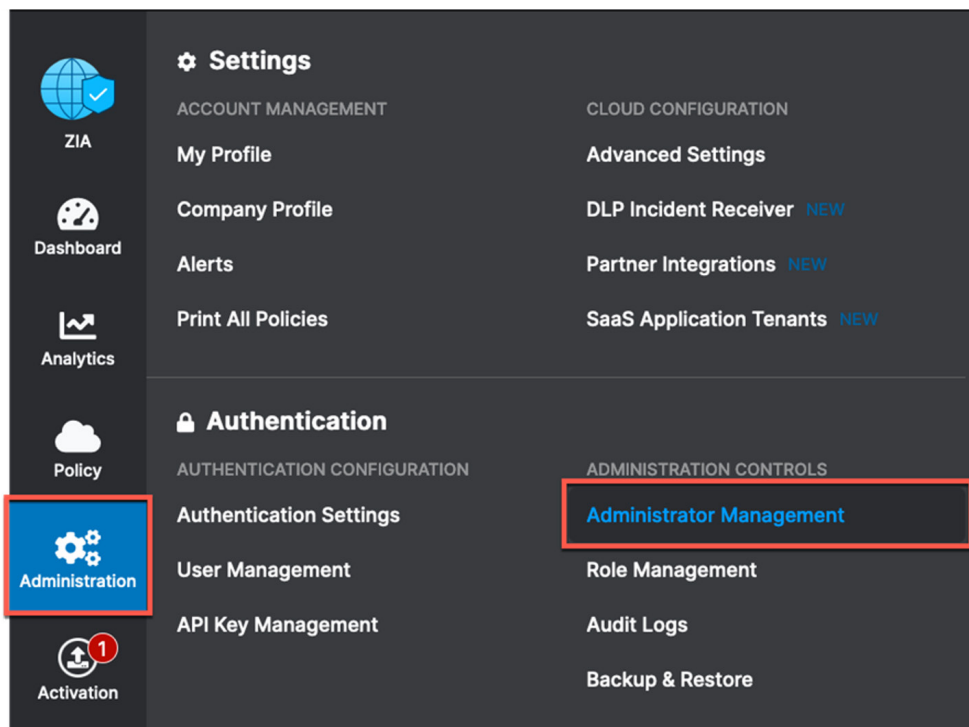


Figure 9. Administrator management

Add Partner Administrator

On the **Administrator Management** page, select **Add Partner Administrator**.

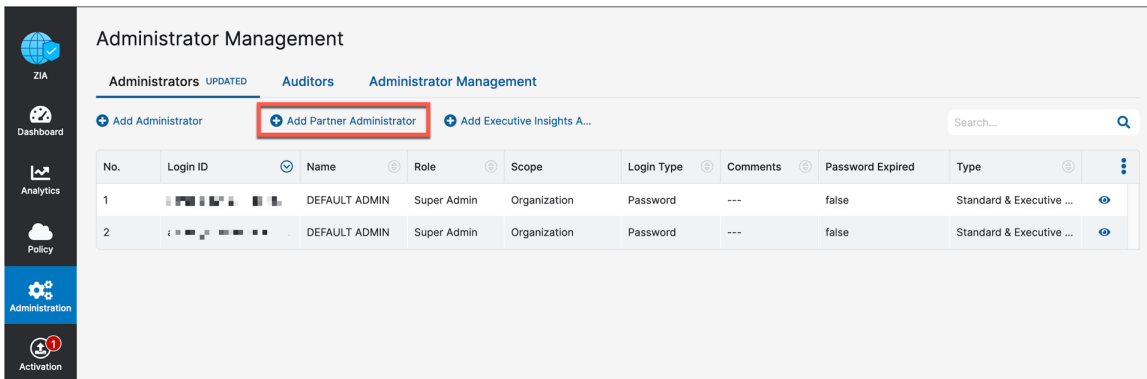


Figure 10. Admin partner administrator

Creating Partner Administrator

Fill in the fields in the **Add Partner Administrator** dialog, and click **Save**.

The screenshot shows the 'Add Partner Administrator' dialog box. It has a title bar with a close button. The form is divided into two main sections: 'ADMINISTRATOR' and 'SET PASSWORD'. In the 'ADMINISTRATOR' section, the 'Login ID' field is highlighted with a red box and contains 'sd-wan' followed by a dropdown menu showing '@ bd-velocloud.com'. Below it, the 'Email' field contains 'sd-wan@bd-velocloud.com' and the 'Name' field contains 'SDWAN'. The 'Partner Role' dropdown is set to 'SD-WAN'. The 'Comments' field is empty. In the 'SET PASSWORD' section, the 'Password' and 'Confirm Password' fields are highlighted with red boxes and contain masked characters. At the bottom, there are 'Save' and 'Cancel' buttons, with 'Save' highlighted by a red box.

Figure 11. Creating partner administrator



Save and copy the **Login ID** and **Password** so you can enter them in the VCO.

Active Pending Changes

Finally, the last step in the ZIA Admin Portal is activating the changes. Go to **Activation** and click **Activate**.

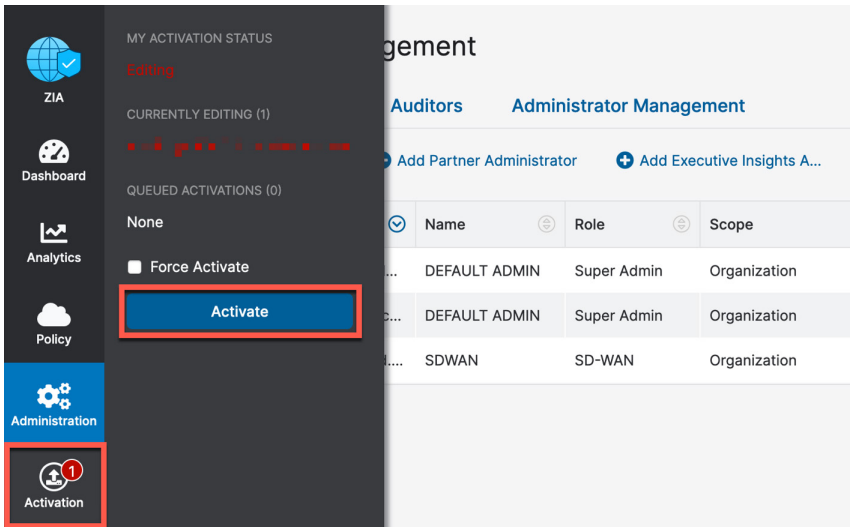


Figure 12. Activate pending changes

Verify Activation

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

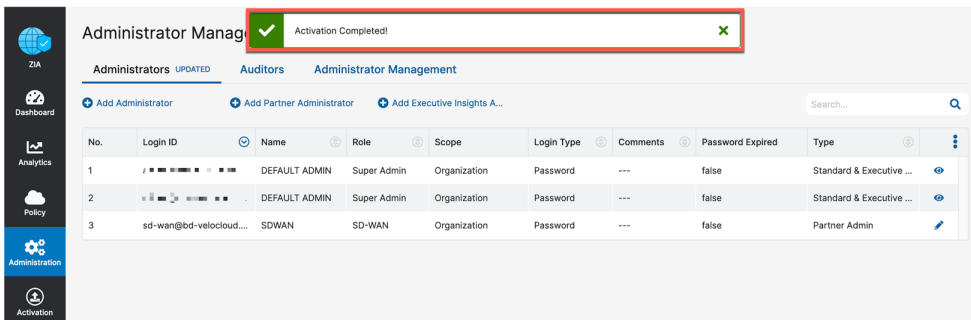


Figure 13. Verify activation

Configuring VMware SD-WAN

The following steps are based on procedures documented on the VMware website. This section covers three deployment models:

1. [Configuring Automated IPSec and GRE Tunnels from the VCE](#)
2. [Configuring Manual Tunnels from the VCE](#)
3. [Configuring IPSec Tunnel from the VCG](#)

The configuration is up-to-date as of VMware SD-WAN Release 4.5.0.

Configuring Automated IPSec and GRE Tunnels from the VCE

First, create a CloudSecurity Service Site entry for Zscaler.

Go to **Configure > Network Services > Cloud Security Service > New**.

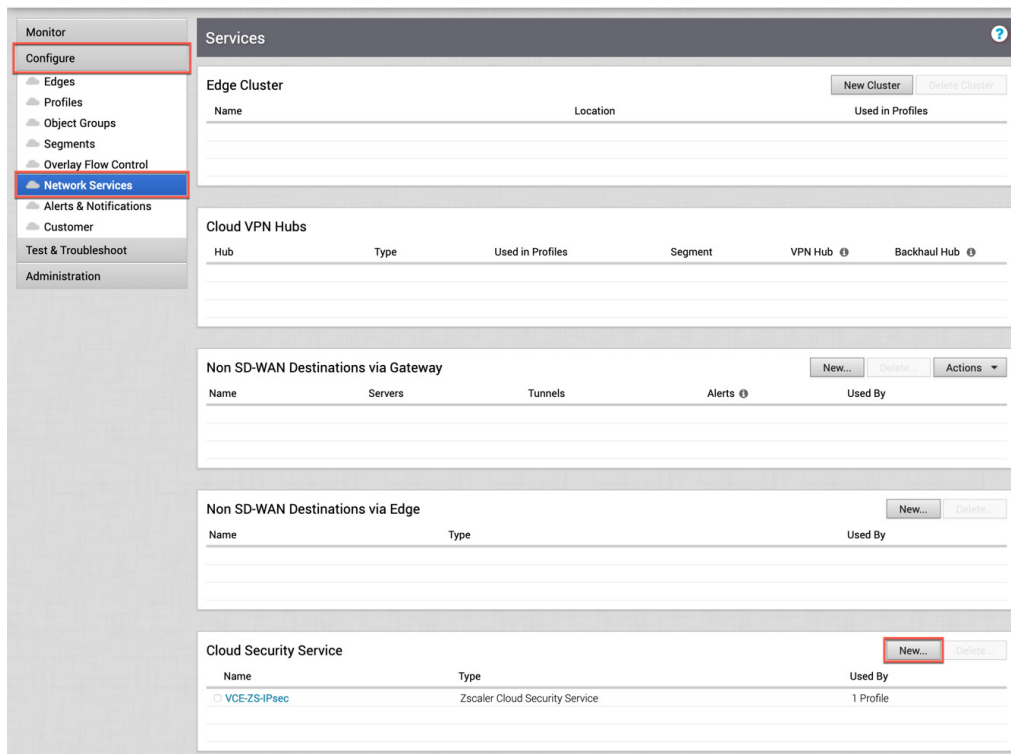


Figure 14. Configuring new cloud security service in the VMware UI

New Cloud Security Provider for Automated Deployment

After selecting **New**, a pop-up appears.

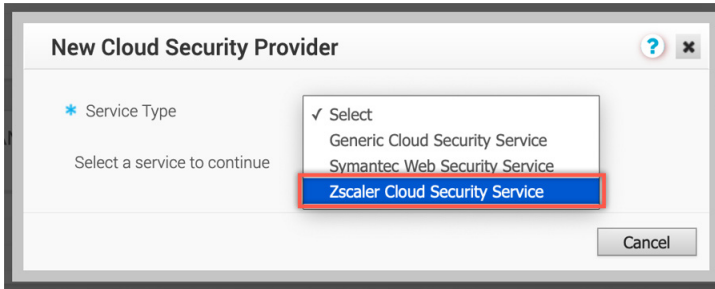


Figure 15. Choose security provider

Select **Zscaler Cloud Security Service** and fill out the required fields in the modal window.

There is very little difference between configuring a CSS for automated IPSec or for GRE tunnel provisioning. Everything with the service is the same except for changing the tunneling protocol.

Configure the following for the security provider:

1. **Automated Cloud Service:** Enable.
 - This engages the API automated provisioning.
 - Unchecked or Disabled is used for manual tunnel configuration, this is covered in the [Configuring Manual Tunnels from the VCE](#) section.
2. Set the **Tunneling Protocol** for traffic transport.
3. The **Domestic Preference** checkbox appears only when for GRE is selected as the tunneling protocol. Check this box if you require all ZIA traffic kept within the country boundaries.
4. **Zscaler Cloud:** Click the button next to Zscaler Cloud and choose the cloud for which the ZIA tenant is provisioned.
5. **Partner Admin Username:** Type the Partner Admin Login ID you provisioned in the ZIA Admin Portal from [Creating Partner Administrator](#).
6. **Partner Admin Password:** Type the partner admin password you provisioned.
7. **Partner Key:** Type the partner key you provisioned from [Verify SD-WAN Partner Key](#).
8. **Domain:** Type the domain name your ZIA instance is provisioned with (typically your company domain). Find the domain name by going to the **Administration > Company Profile** section in the ZIA Admin Portal. It is shown next to the domains list.
9. **Sub Cloud** is an optional parameter that ZIA customers use to have a custom pool of Data Centers for Geo-Location purposes. An example use case is for customers who have the Regional Surcharge DC Entitlement.
10. Click the **L7 Health Check** box to enable ZIA service liveliness testing.
 - Enabling this provides an SLA for the ZIA service. VMware's 5.0 release of the SD-WAN platform allows you to configure the L7 probes.
 - The values can be modified to suit the unique conditions for the configured CSS profile
 - Zscaler recommends the probe interval is not less than 3 seconds.
 - Zscaler recommends the probe retries are not less than 3.

11. The **Zscaler Login URL** field is an optional field. It provides a button to launch the ZIA Admin Portal from within the VMware SD-WAN Orchestrator.

- This field provides ease of connecting into the ZIA Admin Portal.
- If you are using an SSO or IdP provider for both ZIA and the VCO, you can use the providers ZIA application link to enable SSO login into the ZIA Admin Portal.

New Cloud Security Provider

Service Name: VCE-to-ZS-GRE
Service Type: Zscaler Cloud Security Service

1) Automate Cloud Service Deployment: ☒
 2) Tunneling Protocol: ☐ IPsec ☒ GRE
 3) Domestic Preference: ☐
 4) Zscaler Cloud: zscalerbeta.net
 5) Partner Admin Username: sd-wan@bd-velocloud.com
 6) Partner Admin Password: [masked]
 7) Partner Key: [masked]
 8) Domain: bd-velocloud.com
 Validate Credentials

10) L7 Health Check: ☒
 HTTP Probe Interval: 5 sec
 Number of Retries: 3
 RTT Threshold: 3000 msec

11) Zscaler Login URL: https://admin.zscalerbeta.net
 Login to Zscaler

Add Cancel
 Credentials have not been validated

Figure 16. GRE new cloud service provider

New Cloud Security Provider

Service Name: VCE-to-ZS-IPsec
Service Type: Zscaler Cloud Security Service

1) Automate Cloud Service Deployment: ☒
 3) Tunneling Protocol: ☒ IPsec ☐ GRE
 4) Zscaler Cloud: zscalerbeta.net
 5) Partner Admin Username: sd-wan@bd-velocloud.com
 6) Partner Admin Password: [masked]
 7) Partner Key: [masked]
 8) Domain: bd-velocloud.com
 9) Sub Cloud: [empty]
 Validate Credentials

10) L7 Health Check: ☒
 HTTP Probe Interval: 5 sec
 Number of Retries: 3
 RTT Threshold: 3000 msec

11) Zscaler Login URL: https://admin.zscalerbeta.net
 Login to Zscaler

Add Cancel
 Credentials have not been validated

Figure 17. IPsec new cloud security provider

12. After you have completed the fields, click **Validate Credentials**. When the API credentials are confirmed, click **Add**.

The screenshot shows the 'New Cloud Security Provider' dialog box. The 'Service Name' is 'VCE-to-ZS-GRE' and the 'Service Type' is 'Zscaler Cloud Security Service'. Under 'Automate Cloud Service', 'Deployment' is checked, 'Domestic Preference' is unchecked, and 'Tunneling Protocol' is set to 'GRE'. The 'Zscaler Cloud' dropdown is 'zscalerbeta.net'. The 'Partner Admin Username' is 'sd-wan@bd-velocloud.com', 'Partner Admin Password' and 'Partner Key' are masked with dots, and the 'Domain' is 'bd-velocloud.com'. A 'Validate Credentials' button is visible. Below this, 'L7 Health Check' is checked. The 'Zscaler Login URL' is 'admin.zscalerbeta.net' with a 'Login to Zscaler' button. At the bottom, the 'Add' button is highlighted with a red rectangle, and the 'Cancel' button is next to it.

Figure 18. Save cloud service provider configuration

13. Click **Add** to save the network service. If you have any errors in the data input, a red warning icon appears next to **Validate Credentials**, and **Add** remains dimmed and unclickable. Verify and correct any incorrect information.

The screenshot shows the 'New Cloud Security Provider' dialog box in an error state. The configuration fields are the same as in Figure 18. However, the 'Validate Credentials' button now has a red warning icon next to it. The 'Add' button at the bottom is dimmed and unclickable, while the 'Cancel' button remains active. An information icon (i) is visible to the left of the 'Add' button.

Figure 19. Check for cloud security provider errors

Profile for Cloud Security Service

In this section, go to **Configure > Profiles**. After you select the profile you want to use, select the **Device** tab. You need to configure:

1. **Cloud VPN**: Toggle the switch to the **On** position.
2. **Cloud Security Service**: Set it to **On**.
3. **Cloud Security Service**: Select the cloud security service you configured in the prior section.
4. **Tunneling Protocol**: This was set when configuring the CSS.

IPSec

1. **Hash**: Select **SHA1** or **SHA256**.
2. **Encryption**: Select **None**, **AES-128**, or **AES-256** per your requirements.
3. **Key Exchange Protocol**: **IKEv2** – Do not change this value unless specifically required.

GRE

There is nothing additional to configure when using automated GRE tunnel provisioning.

After you have completed these fields, select **Save Changes** in the upper right of your page. This causes the VCO to make outbound API calls to Zscaler and automatically configure all the edges using the profile.

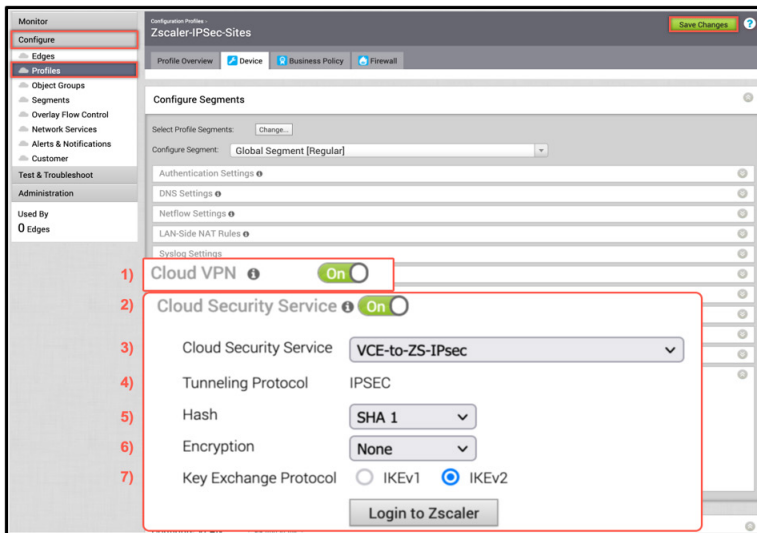


Figure 20. IPSec profile for cloud security service



Figure 21. GRE profile for cloud security service

Monitor Provisioning Status

Go to **Monitor > Events** and you see the events showing the VCO configuring the automatic IPSec tunnels for each edge.

Time	Event	Segment	Edge	User	Seve
Sat Oct 23, 13:21:09	CSS tunnels are up		VC-Edge-GRE		Alert
Sat Oct 23, 13:21:06	Edge Non SD-WAN Destination tunnel up	Global Segment	VC-Edge-GRE	073a2ef3-0dac-4...	Info
Sat Oct 23, 13:20:59	Configuration applied		VC-Edge-GRE		Info
Sat Oct 23, 13:20:49	Zscaler Location object created		VC-Edge-GRE		Info
Sat Oct 23, 13:20:49	Network Service created				Info
Sat Oct 23, 13:20:43	Call made to external API	Global Segment	VC-Edge-GRE		Info
Sat Oct 23, 13:20:37	Cloud Security Service site creation enqueued	Global Segment	VC-Edge-GRE	073a2ef3-0dac-4...	Info
Sat Oct 23, 13:20:29	Configuration applied		VC-Edge-GRE		Info
Sat Oct 23, 13:20:29	Configuration applied		VC-Edge-GRE		Info
Sat Oct 23, 13:20:13	Cloud Security enabled	Global Segment		pabbott@zscaler...	Info
Sat Oct 23, 13:20:13	Profile updated			pabbott@zscaler...	Info
Sat Oct 23, 13:14:10	Configuration applied		VC-Edge-IPsec		Info

Figure 22. API automation events

You see events in the log for all edges that are assigned to the updated profile.

Network Services: Cloud Security Service Overview

In addition to monitoring the event log for the status of the CSS provisioning, you can also go to the **Monitor > Network Services** view to see the status:

Name	Public IP	Status	Tunnel Status	Service Status	State Changed Time	Events	DeploymentStatus
1 VCE-to-ZS-GRE	199.168.148.131 104.129.194.45	●	↔ 1 ↔ 1	↔ 2	Sat Oct 23, 13:39:39 a minute ...	View	View
2 VCE-to-ZS-IPsec	199.168.148.132 104.129.194.39	●	↔ 1 ↔ 1	↔ 2	Sat Oct 23, 13:39:32 a minute ...	View	View

Figure 23. Network services CSS status

Edge Override of Automated IPSec Tunnel Settings

After a few minutes, the IPSec tunnels from the edges using the configured profile automatically establish IPSec tunnels from its public WAN interfaces as seen in the Events screen. For any parameter changes needed at specific sites:

1. Go to **Configure > Edges** and select the VCE you want to configure.
2. Select the **Device** tab.
3. In the **Cloud Security Service** section, select the **Enable Edge Override** option to change the IPSec parameter. You see the VPN credentials learned from the API automation entered in the **Credentials** field.
4. Configure individual sites with unique settings, as needed.
5. Modify the settings for an edge (highlighted in red).

If you configured a ZIA login URL in the CSS settings, Login to Zscaler is available as well..



Figure 24. Automated IPSec tunnel from VCE

The automated IPSec tunnel configuration is complete, and you can configure business policies to forward user traffic to Zscaler.

Verify Tunnels are Up (Active)

To verify the state of the automated tunnels (IPSec or GRE), go to **Monitor > Edges**. You might have to wait 30 seconds to see the primary tunnel establish. The standby tunnel remains gray until it becomes active, which only occurs if the primary tunnel fails.

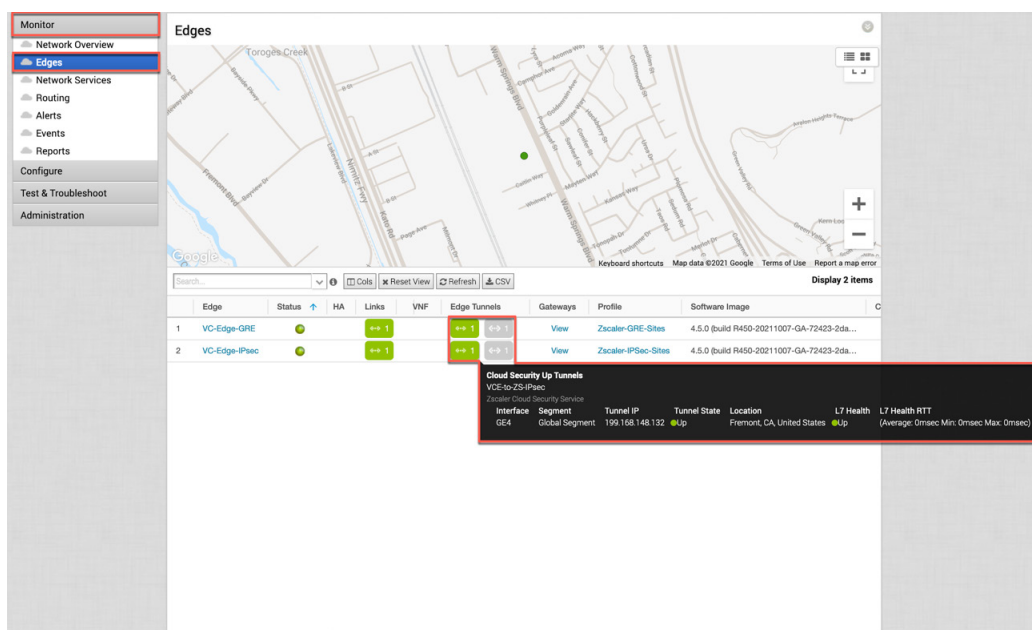


Figure 25. Monitor edge tunnels

Configuring Manual Tunnels from the VCE

Zscaler recommends performing the steps required in ZIA Admin Portal before performing the configuration in the VCO, otherwise the provisioning fails:

- Depending on whether this is a GRE or IPSec tunnel, locate the primary and secondary ZIA VPN endpoints from config.zscaler.com (government agencies, use config.zscaler.us).
 - For GRE:
 - Locate the primary and secondary ZIA GRE virtual IP endpoints from config.zscaler.com (government agencies, use config.zscaler.us).
 - Add the static IPs for the GRE tunnel source. Refer to [Appendix A: ZIA—Configuring Static IPs and GRE Tunnels](#).
 - For IPSec:
 - Locate the primary and secondary ZIA VPN hostname from config.zscaler.com (government agencies, use config.zscaler.us).
 - Create the IPSec VPN Credentials. Refer to [Appendix B: Adding VPN Credentials for Manual Tunnel Creation](#).
- Create a location and assign the GRE tunnel or IPSec VPN credentials to that location so that traffic gets the proper policy. Refer to [Appendix C: ZIA—Configuring a Location for Manual Tunnels](#).

New Cloud Security Provider for Manual Tunnels

First, you must create a cloud security service entry for Zscaler. Go to **Configure > Network Services > Cloud Security Service > New**.

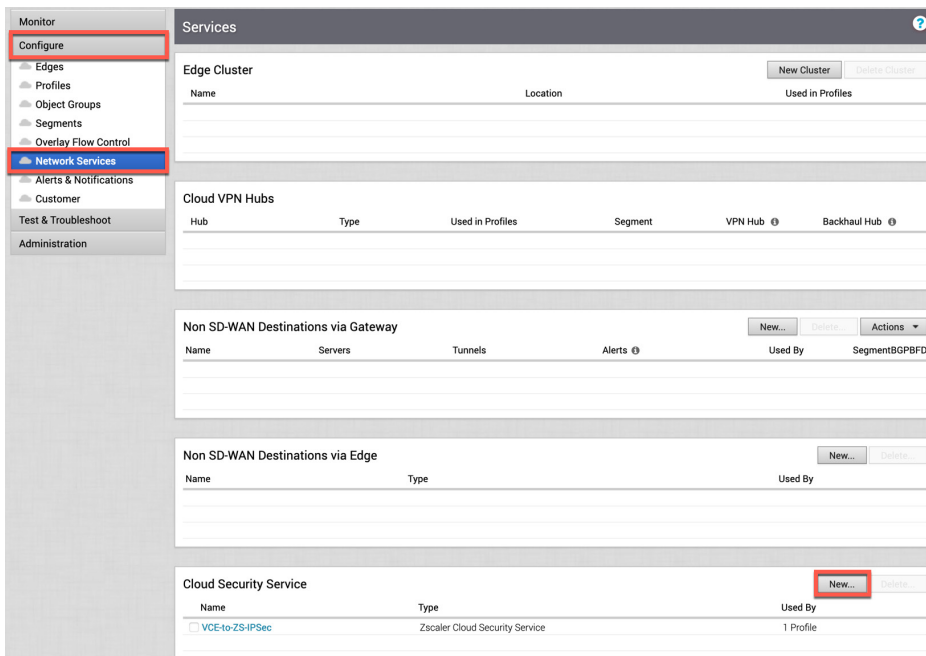


Figure 26. Configuring new cloud security service for GRE tunnels

Selecting **New** opens one of two dialogs (depending on whether you are configuring an IPSec or GRE tunnel). You need to configure:

1. **Service Name** and **Service Type**: Set the name of the service and choose **Zscaler Cloud Security Service** from the drop-down menu.

2. **Primary and Secondary Servers:** Input the IPsec VPN VIP or GRE VIP that you chose in the initial step at the beginning of this section from config.zscaler.com (government agencies, use config.zscaler.us). Use the IP page for the Zscaler cloud that you are provisioned in (e.g., Zscalerthree).
3. **Zscaler Cloud:** Select the cloud into which your tenant is provisioned. This is used for sending the L7 health check enabled in the next item.
4. **L7 Health Check:** Select this checkbox to ensure that service liveliness is enabled. VMware's 5.0 release of the SD-WAN platform lets you configure L7 probes.
 - You can modify the values to match unique conditions for the configured CSS profile:
 - Zscaler recommends the probe interval is not less than 3 seconds.
 - Zscaler recommends the probe retries are not less than 3.
5. **Zscaler Login URL:** (Optional) Enter the URL, which then provides a button to launch the ZIA Admin Portal from within the VMware SD-WAN Orchestrator.
 - The purpose of this field is to provide ease of connecting into the ZIA Admin Portal.
 - If you are using an SSO or IdP provider for both ZIA and the VCO, you can use the provider's ZIA application link to enable SSO login into the ZIA Admin Portal.

After you have completed filling in these fields, select **Add** to continue.

The screenshot shows the 'New Cloud Security Provider' dialog box with the following configuration:

- Service Name:** Manual-IPsec
- Service Type:** Zscaler Cloud Security Service
- Automate Cloud Service Deployment:** ☐
- Primary Server:** sunnyvale1-vpn.zscalerbeta.net
- Secondary Server:** was1-vpn.zscalerbeta.net
- Zscaler Cloud:** zscalerbeta.net
- L7 Health Check:** ☒
- Zscaler Login URL:** https://admin.zscalerbeta.net

At the bottom, there is a green 'Add' button and a grey 'Cancel' button.

Figure 27. IPsec new cloud security provider for manual tunnels

The screenshot shows the 'New Cloud Security Provider' dialog box with the following configuration:

- Service Name:** Manual-GRE
- Service Type:** Zscaler Cloud Security Service
- Automate Cloud Service Deployment:** ☐
- Primary Server:** 199.168.148.131
- Secondary Server:** 104.129.194.38
- Zscaler Cloud:** zscalerbeta.net
- L7 Health Check:** ☒
- Zscaler Login URL:** https://admin.zscalerbeta.net

At the bottom, there is a green 'Add' button and a grey 'Cancel' button.

Figure 28. GRE new cloud security provider for manual tunnels

Profile for Cloud Security Service

In this section, go to **Configure > Profiles**. After you select the profile you want to use, select **Device** tab. In the **Cloud Security Service** section, configure (depending on whether you are creating IPsec or GRE tunnels):

1. **Cloud VPN**: Set to **On**.
2. **Cloud Security Service**: Toggle it **On**.
3. **Cloud Security Service**: Select the cloud security service you configured in the prior section.
4. **Tunneling Protocol**: Set this to the primary and secondary server values that you set earlier for Tunnel Type. If this is set incorrectly, the tunnels won't establish.

IPSec

5. **Hash**: Select **SHA1** or **SHA256**.
6. **Encryption**: Select **None**, **AES-128**, or **AES-256** per your requirements.
7. **Key Exchange Protocol**: **IKEv2** – Do not change this value unless specifically required.

GRE

There is nothing additional to configure when using manual GRE tunnel provisioning. After you have completed these fields, select **Save Changes** in the upper right of your page.

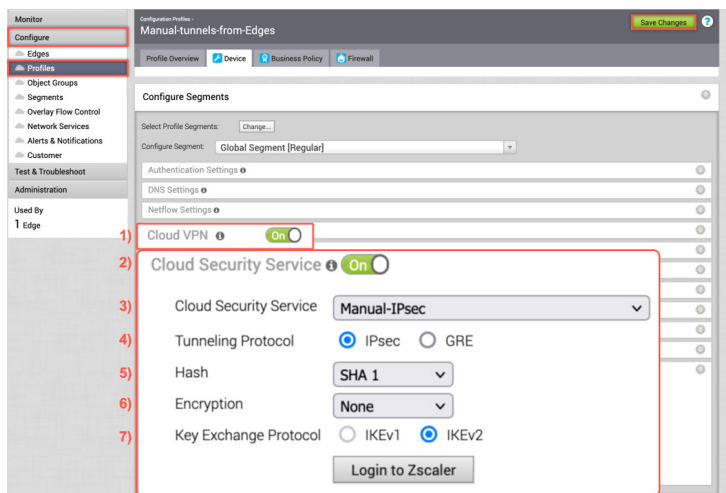


Figure 29. IPSec profile for cloud security service

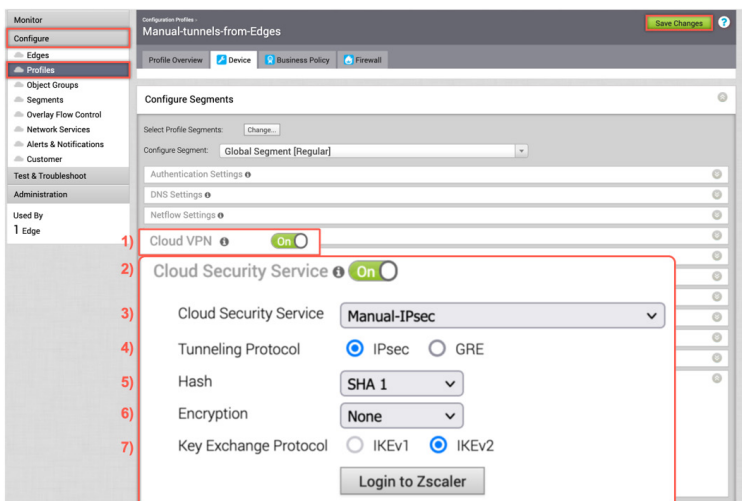


Figure 30. GRE profile for cloud security service

Edge Device Configuration for Manual Tunnels

Next, you need to go to **Configure > Edges** and select the VCE on which you want to manually configure the tunnels. Next, select the **Device** tab and then scroll down to the **Cloud Security Service** section to configure settings (depending on whether you are configuring IPsec or GRE tunnels):

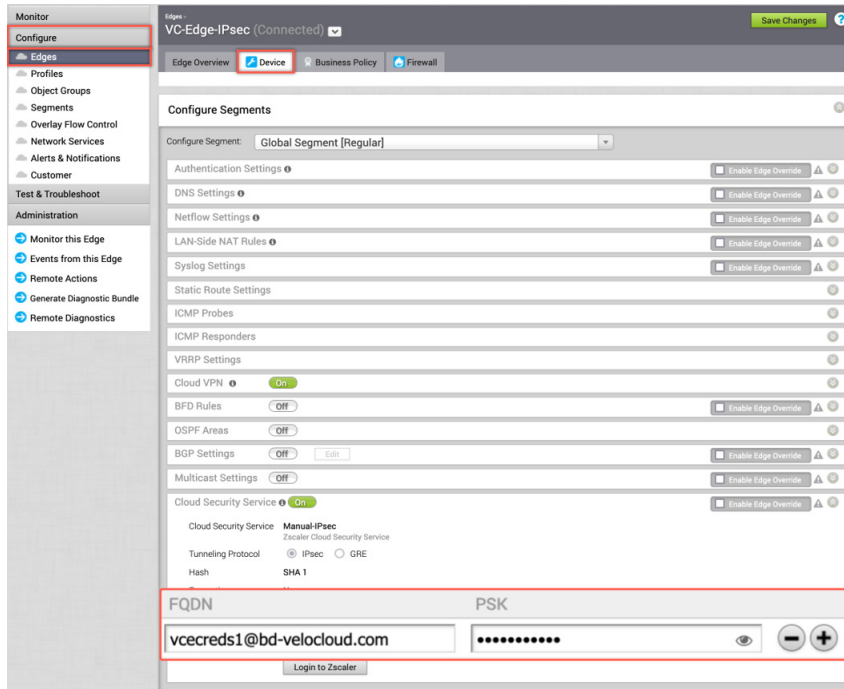


Figure 31. IPsec manual tunnels for edge (VCE)

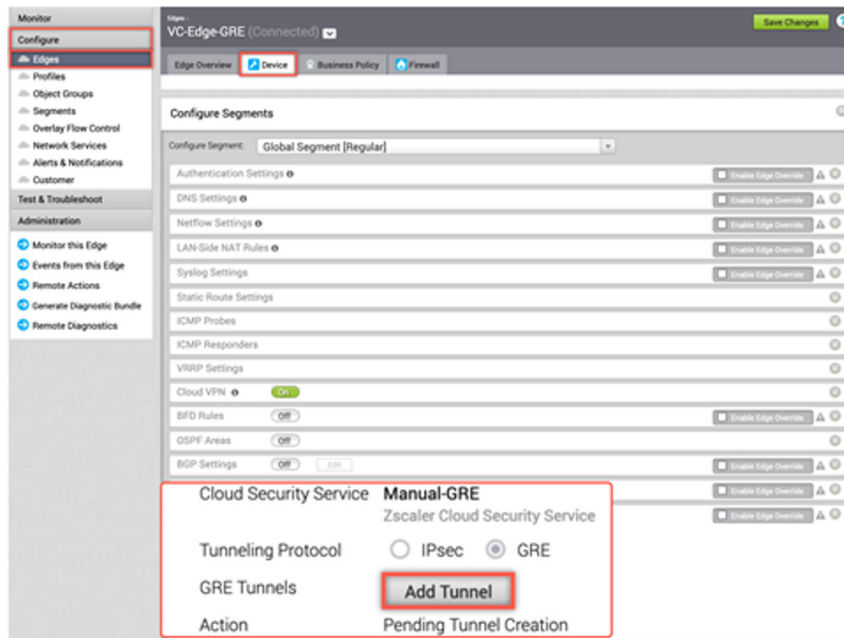


Figure 32. GRE manual tunnels for edge (VCE)

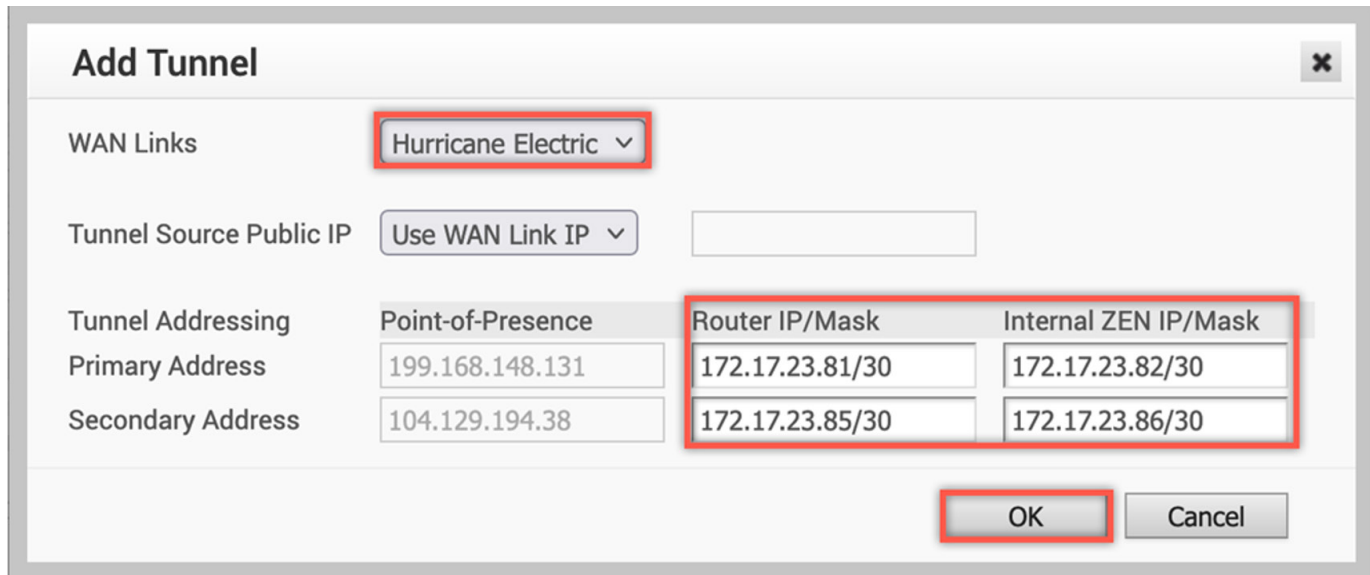
The **Cloud Security Service** section settings are inherited from the previous profile configuration step.

IPSec

1. Fill in the VPN credentials and PSK created in the steps at the beginning of this section.
2. Click **Save Changes** on top right of your page. Go to [Verify GRE Tunnel Configuration](#) to verify tunnel status.

GRE

Click **Add Tunnel** next to the **GRE Tunnels**. Enter the tunnel IP information in the dialog that is displayed.



The 'Add Tunnel' dialog box contains the following fields and values:

- WAN Links:** Hurricane Electric (selected)
- Tunnel Source Public IP:** Use WAN Link IP (selected)
- Tunnel Addressing:**
 - Point-of-Presence:**
 - Primary Address: 199.168.148.131
 - Secondary Address: 104.129.194.38
 - Router IP/Mask:** 172.17.23.81/30 (Primary), 172.17.23.85/30 (Secondary)
 - Internal ZEN IP/Mask:** 172.17.23.82/30 (Primary), 172.17.23.86/30 (Secondary)
- Buttons:** OK, Cancel

Figure 33. Input GRE tunnel details

Configure:

1. **WAN Link:** Select the WAN interface the GRE tunnel should source from (in this example, our lab WAN link is called "Hurricane Electric" in the preceding steps).
2. **Tunnel Addressing:** The **Router IP/Mask** and **Internal ZEN IP/Mask** is pulled from the steps at the beginning of this section. To learn more, see [Appendix A: ZIA—Configuring Static IPs and GRE Tunnels](#). Note the **Internal GRE IP** range is provided as a /29, where you must split the range with two sets of /30, as illustrated earlier.
3. Click **OK** to save and return to the device configuration page.

Verify GRE Tunnel Configuration

In the **Cloud Security Service** section, you see the WAN interface name (e.g., Hurricane Electric, which is the name of the WAN interface for the lab with which this guide was authored).

Click **Save Changes** after confirming your WAN interface name is correct.

The screenshot displays the Zscaler VMware UI configuration page for a Cloud Security Service. The left sidebar shows navigation options like Monitor, Configure, Edges, Profiles, Object Groups, Segments, Overlay Flow Control, Network Services, Alerts & Notifications, Customer, Test & Troubleshoot, and Administration. The main content area is titled 'VC-Edge-GRE (Connected)' and includes a 'Save Changes' button. Below this, there's a 'Configure Segments' section with a dropdown for 'Global Segment [Regular]'. A list of settings follows, each with an 'Enable Edge Override' checkbox: Authentication Settings, DNS Settings, Netflow Settings, LAN-Side NAT Rules, Syslog Settings, Static Route Settings, ICMP Probes, ICMP Responders, VRRP Settings, and Cloud VPN (which is 'On').

The 'Cloud Security Service' section is expanded, showing 'Manual-GRE' configuration. It includes a 'Tunneling Protocol' section with radio buttons for IPsec and GRE (selected). Below this is a 'GRE Tunnels' section with an 'Add Tunnel' button. The 'Details' section contains a table with 'WAN Links'. The table has two columns: 'Action' and 'WAN Links'. The 'Action' column contains 'Edit | Delete' (highlighted in a red box) and the 'WAN Links' column contains 'Hurricane Electric'. At the bottom of the 'Details' section is a 'Login to Zscaler' button.

Figure 34. Verify GRE tunnel configuration in the VMware UI

Check and Verify Tunnel and CSS Provisioning Status

To verify the state of the edge tunnels, go to **Monitor > Edges**. You might have to wait 30 seconds to see the primary tunnel (IPSec or GRE) establish. The standby tunnel remains gray until it becomes active, which only occurs if the primary tunnel fails.

Edge	Status	HA	Links	VM Status	VNF	Edge Tunnels	Gateways	Profile
1 VC-Edge-GRE	Up		1					Zscaler-GRE-Sites
2 VC-Edge-IPsec	Up		1			1		Zscaler-API-Sites

Figure 35. Monitor edge tunnels

You can also view the state of the CSS by navigating to **Monitor > Network Services** to view the current state of the services, CSS-related events, and the deployment status of the tunnels.

Name	Public IP	Status	Tunnel Status	Service Status	State Changed Time	Events	DeploymentStatus
1 VCE-to-ZS-GRE	199.168.148.131 104.129.194.45	Up	1	2	Sat Oct 23, 13:39:39 a minute ...	View	View
2 VCE-to-ZS-IPsec	199.168.148.132 104.129.194.39	Up	1	2	Sat Oct 23, 13:39:32 a minute ...	View	View

Figure 36. Network services CSS status

Configuring IPSec Tunnel from the VCG

Zscaler recommends that you perform the steps required to configure ZIA defined in [Configuring Zscaler Internet Access \(ZIA\)](#) before performing the VCO configuration:

- Locate the primary and secondary ZIA DC VPN endpoints from [config.zscaler.com](#) (government agencies, use [config.zscaler.us](#)) deriving the IP address from the DNS hostname. If you are not familiar with how to get the IP from a DNS name, refer to section [Appendix G: Deriving the Zscaler IPSec VPN VIP](#).
- Create the FQDN and PSK for the IPSec tunnels. Refer to section [Appendix B: Adding VPN Credentials for Manual Tunnel Creation](#).
- Create a location and assign the VPN credentials to that location so the traffic receives the proper policy. Refer to section [Appendix C: ZIA—Configuring a Location for Manual Tunnels](#).

New Non-SD-WAN Destination

First, create a non-SD-WAN destination entry for Zscaler. Go to **Configure > Network Services > Non-SD-WAN Destinations via Gateway > New**.

The screenshot shows the Zscaler VMware UI configuration page. The left sidebar has a 'Configure' tab selected, and 'Network Services' is highlighted. The main content area shows several sections: 'Edge Cluster', 'Cloud VPN Hubs', 'Non SD-WAN Destinations via Gateway', 'Non SD-WAN Destinations via Edge', and 'Cloud Security Service'. The 'Non SD-WAN Destinations via Gateway' section is expanded, and the 'New...' button is highlighted with a red box.

Non SD-WAN Destinations via Gateway						
Name	Servers	Tunnels	Alerts ⓘ	Used By	Segment	BGPBFD

Non SD-WAN Destinations via Edge		
Name	Type	Used By

Cloud Security Service		
Name	Type	Used By
<input type="checkbox"/> VCE-to-ZS-IPsec	Zscaler Cloud Security Service	0
<input type="checkbox"/> VCE-to-ZS-GRE	Zscaler Cloud Security Service	1 Profile
<input type="checkbox"/> Manual-IPsec	Zscaler Cloud Security Service	0
<input type="checkbox"/> Manual-GRE	Zscaler Cloud Security Service	1 Profile

Figure 37. Create new non-SD-WAN destination via gateway in the VMware UI

Selecting **New** opens a pop-up dialog, as shown in the following example.

Configure:

1. **Type:** Select **Zscaler**.
2. **Primary** and **Secondary VPN Gateway:** Obtain the IPsec VIP IP from the Zscaler IP pages (see [Appendix G: Deriving the Zscaler IPsec VPN VIP](#)). You should use the IP pages for the Zscaler cloud you are provisioned in (e.g., ZS3).
3. After you have completed filling in these fields, click **Next** to continue.

New Non SD-WAN Destination via Gateway...

* Name: VCG-to-ZS-IPsec

* Type: Zscaler

VPN Gateways

* Primary VPN Gateway: 199.168.148.132

Secondary VPN Gateway: 104.129.194.39

Next

Figure 38. Create new non-SD-WAN destination via gateway

Advanced Settings for Non SD-WAN Site

Select **Advanced** at the lower-left bottom. The window expands with additional configuration options.

Configure:

1. Select **Enable Tunnels** to ensure the configured tunnels appear when assigned to a profile.
2. **Local Auth Id**: User **FQDN**. Paste in your ZIA VPN Credential FQDN.
3. Click **Advanced** to reveal the PSK fields.
 - **Primary and Secondary VPN Gateway – PSK**: Paste in your ZIA VPN Credential PSK into all four PSK fields. The same FQDN is used for all tunnels.
4. Select **L7 Health Check** to enable ZIA service liveliness testing.
 - The 5.0 release of VMware's SD-WAN platform lets you configure L7 probes.
 - Zscaler recommends setting the probe interval to not less than 3 seconds.
 - Zscaler recommends setting probe retries to not less than 3.
5. Choose the Zscaler cloud that the tenant was provisioned into so that the proper L7 destination is checked.
There are multiple ways to configure VCG tunnels. This example shows a tunnel configuration with **Redundant Velocloud Cloud VPN** selected. See the [VMware SD-WAN documentation](#) for details and other options.
6. After you have completed these fields, select **Save Changes** in the lower right.

VCG-to-ZS-IPsec

Name: VCG-to-ZS-IPsec
 Type: Zscaler
 Enable Tunnel(s): ☒
 Tunnel mode: Active/Hot-Standby

Location: San Francisco, CA 94102, US
 Lat,Lng: 37.779701,-122.415901
[Update Location...](#)

Primary VPN Gateway
 Public IP: 199.168.148.132
 Tunnel Settings:
 PSK:
 Redundant Tunnel PSK:

Secondary VPN Gateway [Remove](#)
 Public IP: 104.129.194.39
 Tunnel Settings:
 PSK:
 Redundant Tunnel PSK:

Local Auth Id: User FQDN
 Zscaler Login URL: https://admin.zscalerbx
[Login to Zscaler](#)

L7 Health Check: ☒
 Zscaler Cloud: zscalerbeta.net
 HTTP Probe Interval: 5 sec
 Number of Retries: 3
 RTT Threshold: 3000 msec

Redundant VeloCloud Cloud VPN: ☒

[Advanced](#) [View IKE/IPSec Template](#) [Save Changes](#) [Close](#)

Figure 39. Advanced settings for non-SD-WAN destination via gateway

Enable Cloud VPN for a Profile

Next, go to **Configure** > **Profiles** and select the profile you want to enable.

1. Select **Device**.
2. Configure:
 - a. Toggle on **Cloud VPN**: Select it **On**.
 - b. Select **Enable**, then choose **Non-SD-WAN Site** from the drop-down menu.
3. Lastly, click **Save Changes** at the top right of the window to apply the profile changes.

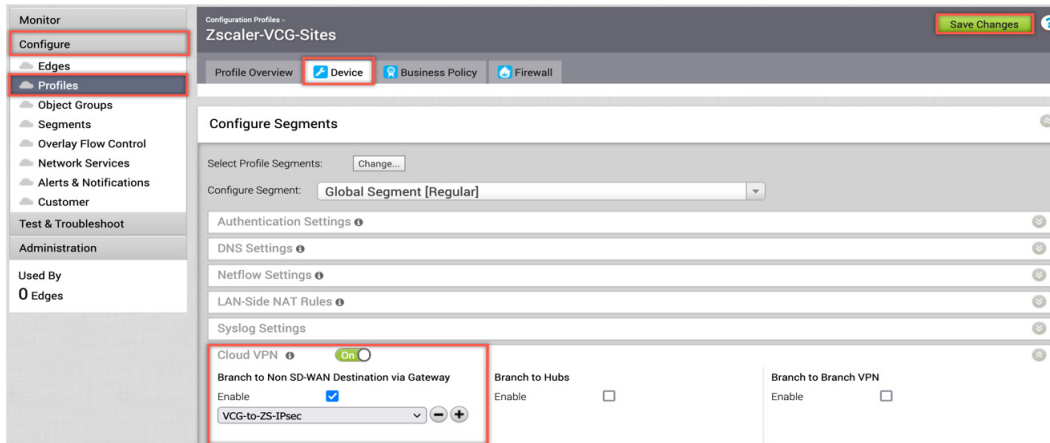


Figure 40. Enabling Zscaler connectivity from VCG on VMware SD-WAN VCO

Check and Verify Tunnel and VCG Tunnel Provisioning Status

You can view the state of the VCG tunnels by navigating to **Monitor** > **Network Services**. The window shows the current state of the services, CSS-related events, and the deployment status of the tunnels:

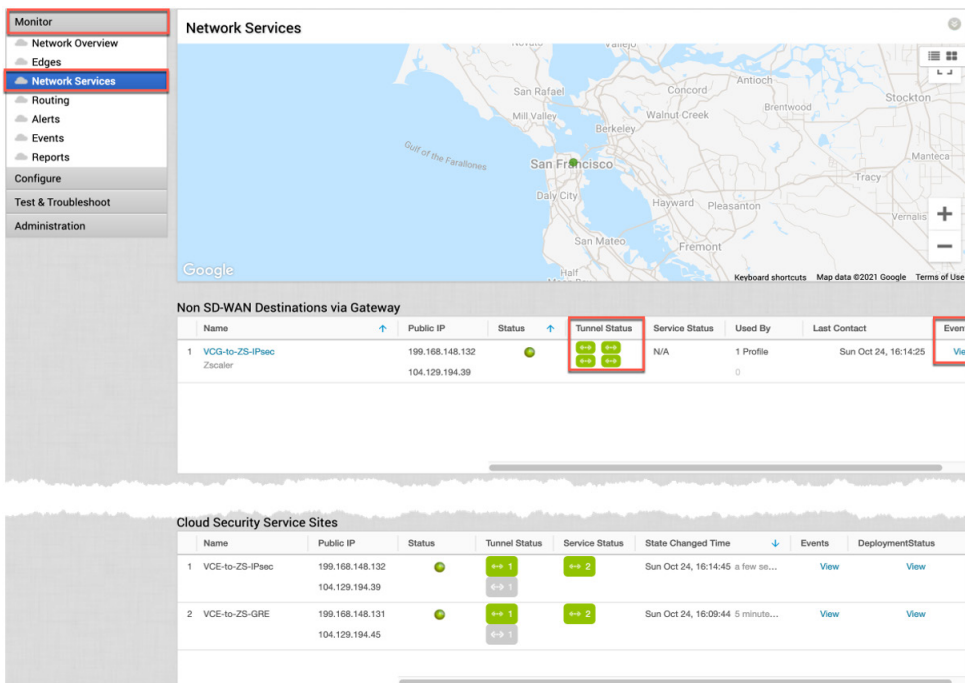


Figure 41. Network services non-SD-WAN destination via gateway status

Configuring Gateway Options and Sub-Locations

When using the API automation to configure ZIA, configure the gateway options and sub-locations on the SD-WAN platform as the information source for anything provisioned with the API.

Gateway options allow for granular control of traffic treatment as it travels into the ZIA platform. Sub-locations are child locations that are created to enforce unique treatment using gateway options for specific subnets as an exception to the main or parent location traffic.

To learn more, see [Configuring Locations](#) and [About Sub-Locations](#) (government agencies, see [Configuring Locations](#) and [About Sub-Locations](#)).

Configuring Gateway Options for Edges

As stated, it's better to configure gateway options and sub-locations from the VCO when using automated tunnels.

1. Go to **Configure > Edges > Device**, then scroll down to the Zscaler section of the page and expand the options by clicking the arrow button.

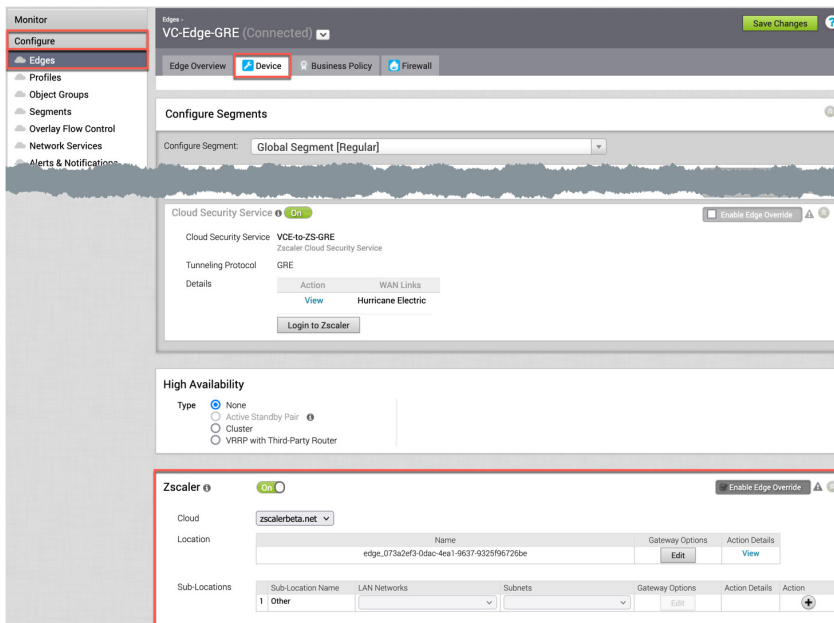


Figure 42. Go to gateway options and sub-locations

You see the parent location and its name. This is the name that displays in the **ZIA Admin Locations** page.

2. Click **Edit** to open a window showing the gateway options.

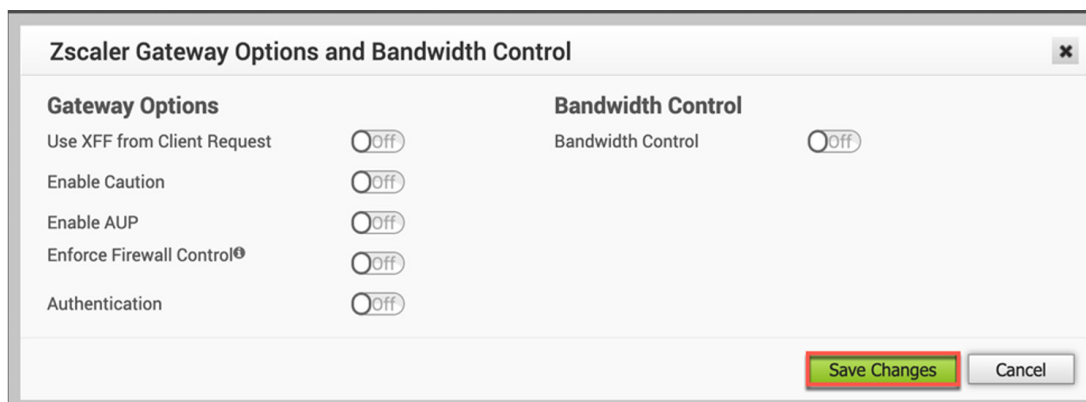
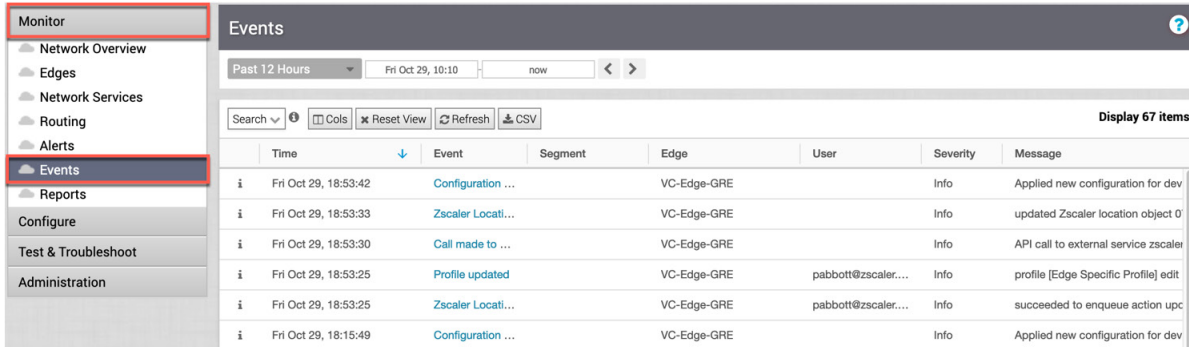


Figure 43. Set location gateway options

3. Be sure to consult the Zscaler Help Portal as some gateway options have prerequisites to function properly. By default, all options are disabled.
4. After you have enabled your desired options, click **Save** to have the VCO provision them in the ZIA platform. This might take a few minutes to appear in the ZIA platform.
5. Check the **Events** page under the **VCO Monitoring** section to observe the automation:



The screenshot shows the Zscaler interface with the 'Monitor' tab selected. The 'Events' section is active, displaying a table of events. The table has columns for Time, Event, Segment, Edge, User, Severity, and Message. The events listed are related to configuration updates and location management.

Time	Event	Segment	Edge	User	Severity	Message
Fri Oct 29, 18:53:42	Configuration ...		VC-Edge-GRE		Info	Applied new configuration for dev
Fri Oct 29, 18:53:33	Zscaler Locati...		VC-Edge-GRE		Info	updated Zscaler location object 0
Fri Oct 29, 18:53:30	Call made to ...		VC-Edge-GRE		Info	API call to external service zscaler
Fri Oct 29, 18:53:25	Profile updated		VC-Edge-GRE	pabbott@zscaler...	Info	profile [Edge Specific Profile] edit
Fri Oct 29, 18:53:25	Zscaler Locati...		VC-Edge-GRE	pabbott@zscaler...	Info	succeeded to enqueue action upc
Fri Oct 29, 18:15:49	Configuration ...		VC-Edge-GRE		Info	Applied new configuration for dev

Figure 44. Verify VCO automation

You can also check the Audit Log to see the API calls made to the ZIA platform as shown in [Appendix F: Using the Audit Log for API Troubleshooting](#).

Configuring Sub-Locations

You configure sub-locations and their individual gateway options by repeating step 1 of [Configuring Gateway Options for Edges](#).



The screenshot shows the Zscaler configuration window. The 'Zscaler' status is 'On'. The 'Cloud' is set to 'zscalerbeta.net'. The 'Location' is 'edge_073a2ef3-0dac-4ea1-9637-9325f96726be'. The 'Sub-Locations' table shows two sub-locations: 'Other' and 'guestwifi'. The 'guestwifi' sub-location has a LAN Network of 'GE1' and a Subnet of '192.168.99.0/24'.

Sub-Location Name	LAN Networks	Subnets	Gateway Options	Action Details	Action
1 Other			Edit	View	+
2 guestwifi	GE1	192.168.99.0/24	Edit	View	+ -

Figure 45. Go to gateway options and sub-locations

Under **Sub-Locations**, “guestwifi” was added to this edge. When creating a sub-location, you must assign at least one interface or VLAN to the sub-location due to ZIA mapping sub-locations to IP prefixes in the platform.

After assigning the interfaces to the sub-location you can then edit the gateway options for it as necessary. The gateway options window for sub-locations looks very similar to the one shown in Figure 43. The only difference is the Use XFF from Client Request which is only configurable at the main or parent location.

Lastly, click **Save** at the top right of the device configuration window. Then the VCO executes the automated provisioning to ZIA. You can confirm success by performing step 5 in [Configuring Gateway Options for Edges](#).

Verify Gateway Options and Sub-Locations in ZIA

To confirm that all the changes were applied to the locations in the ZIA Admin Portal, go to **Location Management** and click the **Edit** icon to view the details in the **Location** pop-up dialog. The gateway options set are visible in a column on the page.

The parent location has the **Authentication** option enabled.

No.	Name	IP Addresses	D...	Use XFF from Client Requ...	Authentication	Firewall Filtering	Bandwidth	Group	Location Type
1	> Site2	---	---	---	Enabled	---	---	Corporate User Traffic ...	Corporate user traffic
2	edge_073a2ef3-0dac-4ea1-9637...	72.52.82.204	---	---	Enabled	---	---	Unassigned Locations	Corporate user traffic
2.1	guestwifi	192.168.99.0-192.168.99.255	---	---	---	Enabled	---	Unassigned Locations	Corporate user traffic
2.2	other	---	---	---	---	---	---	Corporate User Traffic ...	Corporate user traffic

Figure 46. Viewing the automated gateway options and sub-locations in ZIA

To view newly created or updated sub-locations, click the arrow icon to the left of the parent location to reveal the sub-location rows. You can also check the Audit Log to see the API calls made to the ZIA platform as shown in [Appendix F: Using the Audit Log for API Troubleshooting](#).

Configuring Business Policy for ZIA

Create a business policy to send all internet-destined traffic to Zscaler after you have verified that the tunnels are up and healthy.

1. Go to **Configure > Profiles** and select your profile.
2. Next, select **Business Policy**, and then select **New Rule**.

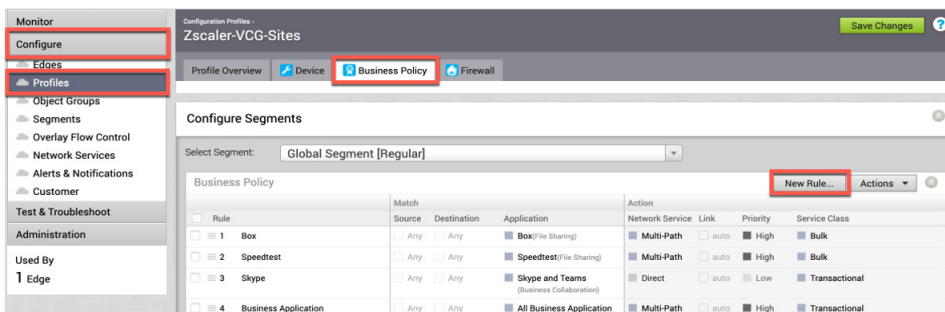


Figure 47. Configuring business policy for ZIA

Configure Rule for VCE

A pop-up dialog displays. Configure the VCE options as shown.

The 'Configure Rule' dialog is shown with the following settings:

- Rule Name:** Internet to Zscaler
- Match:**
 - Source:** Any
 - Destination:** Internet
 - Address Group:** Select
 - Port Group:** Select
 - Application:** Any
- Action:**
 - Priority:** Normal
 - Rate Limit:** Disabled
 - Network Service:** Internet Backhaul
 - Backhaul Hubs
 - Non SD-WAN Destination via Gateway
 - Non SD-WAN Destination via Edge / Cloud Security Service
 - VCE-to-Zscaler-GRI
 - Link Steering:** Auto
 - Inner Packet DSCP Tag: Leave as is
 - Outer Packet DSCP Tag: 0 - CS0/DF
 - NAT:** Disabled
 - Service Class:** Transactional

The OK button is highlighted with a red box.

Figure 48. Configure rule for edges using direct tunnel from VCE

Configure Rule for VCG

Configure the VCE options as shown in the **Configure Rule** dialog.

The 'Configure Rule' dialog is shown with the following settings:

- Rule Name:** Internet to Zscaler
- Match:**
 - Source:** Any
 - Destination:** Internet
 - Address Group:** Select
 - Port Group:** Select
 - Application:** Any
- Action:**
 - Priority:** Normal
 - Rate Limit:** Disabled
 - Network Service:** Internet Backhaul
 - Backhaul Hubs
 - Non SD-WAN Destination via Gateway
 - VCG-to-Zscaler-IPS
 - Link Steering:** Auto
 - Inner Packet DSCP Tag: Leave as is
 - Outer Packet DSCP Tag: 0 - CS0/DF
 - NAT:** Disabled
 - Service Class:** Transactional

The OK button is highlighted with a red box.

Figure 49. Configure rule for edges using tunnels from VCG

Appendix A: ZIA—Configuring Static IPs and GRE Tunnels

The ZIA Admin Portal supports provisioning static IPs for GRE tunnels.

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

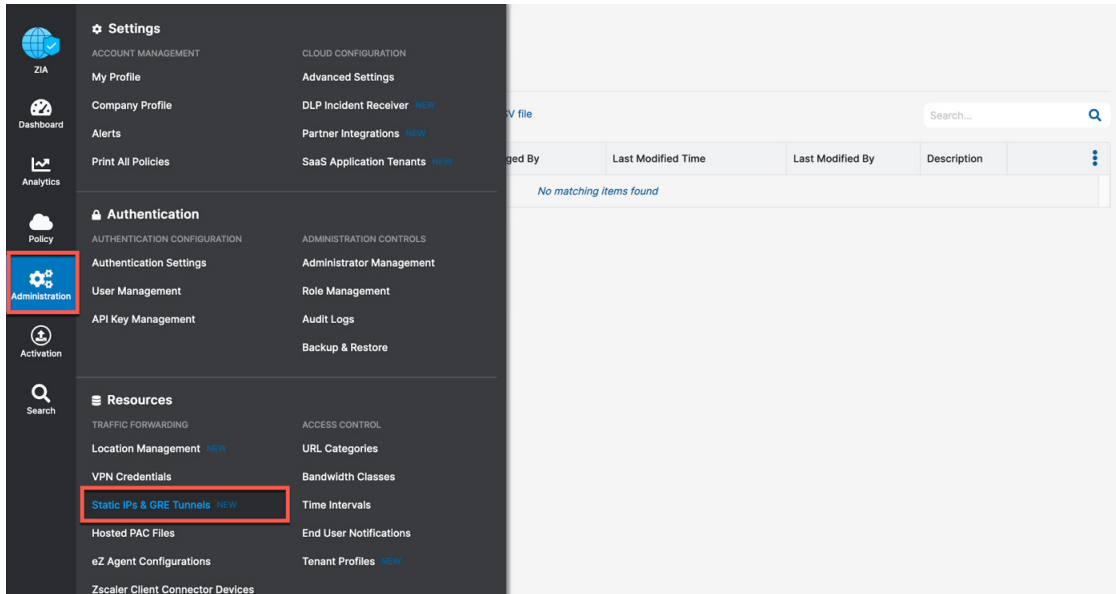


Figure 50. Go to Static IPs & GRE Tunnel configuration in the ZIA Admin Portal

Add a Static IP Configuration

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

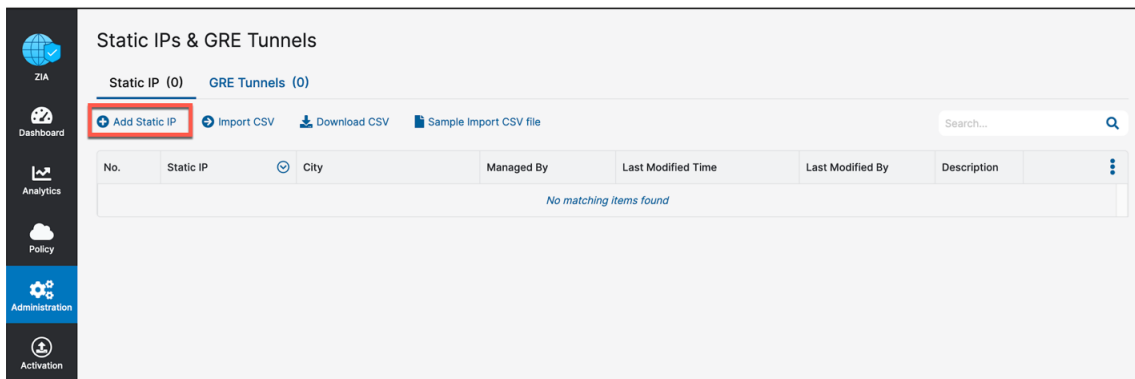
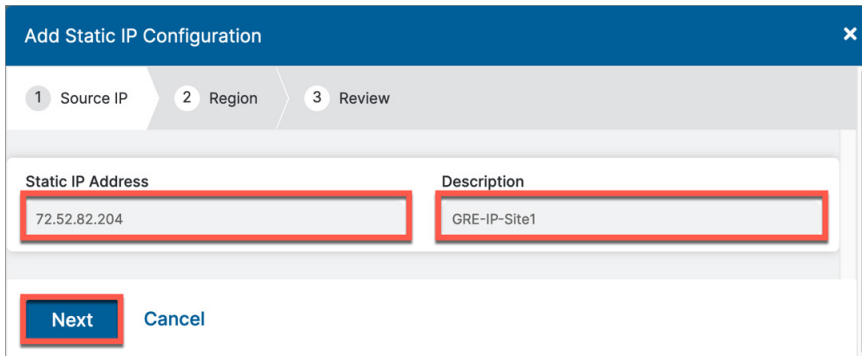


Figure 51. Adding a static IP

Enter the Static IP

In the **Add Static IP Configuration** wizard:

1. Enter the public **Static IP Address** that initiates the tunnel connection.
2. Add a **Description** if desired.
3. Click **Next** to continue.

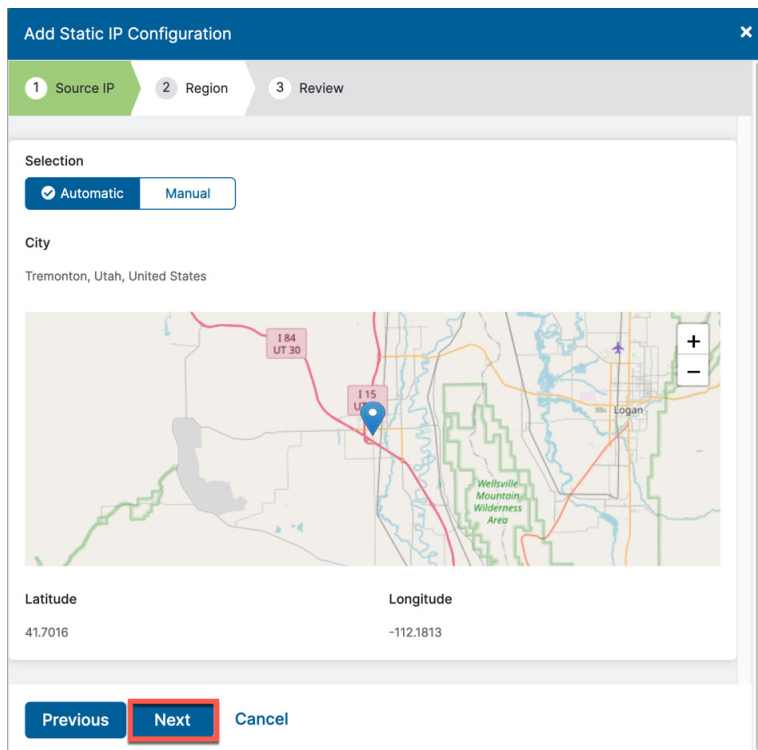


The screenshot shows the 'Add Static IP Configuration' wizard with three steps: 1. Source IP, 2. Region, and 3. Review. The 'Static IP Address' field contains '72.52.82.204' and the 'Description' field contains 'GRE-IP-Site1'. The 'Next' button is highlighted with a red box.

Figure 52. Entering the static IP

Verify Geospatial data

Next, verify that the Geospatial location lookup is correct for the IP address entered. If not, click **Manual** and enter the correct location. Then click **Next**.



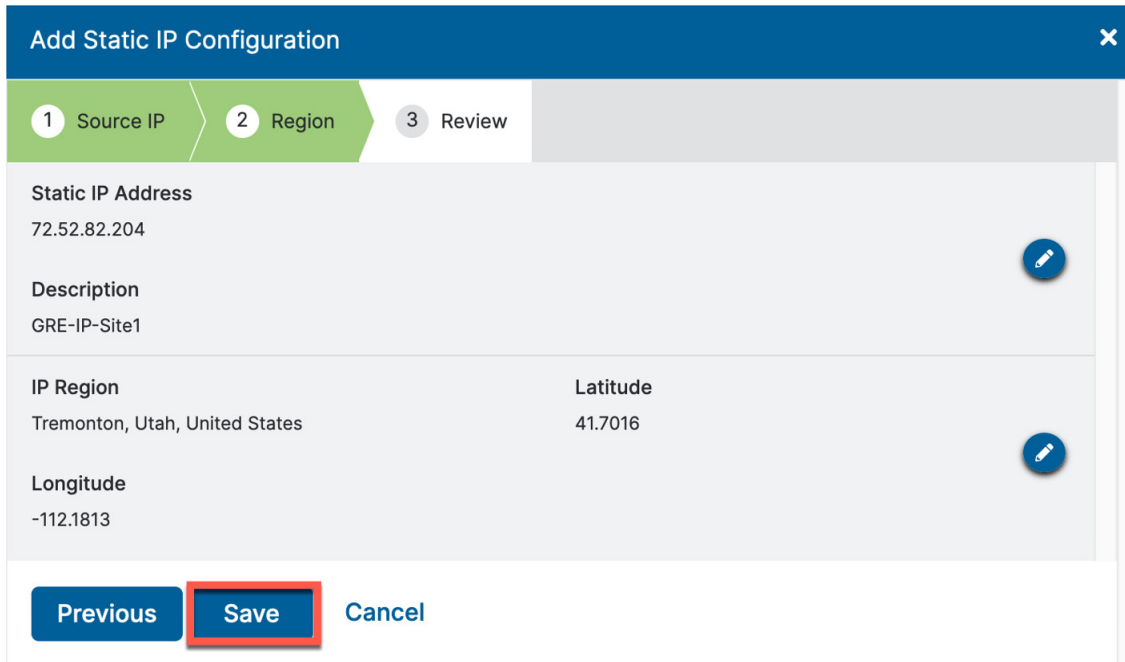
The screenshot shows the 'Add Static IP Configuration' wizard with three steps: 1. Source IP, 2. Region, and 3. Review. The 'Selection' section has 'Automatic' selected. The 'City' section shows 'Tremonton, Utah, United States'. A map shows the location of Tremonton, Utah, with a blue pin. The 'Latitude' is 41.7016 and the 'Longitude' is -112.1813. The 'Next' button is highlighted with a red box.

Figure 53. Verifying geospatial information

This information is used by the 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**.



Add Static IP Configuration [X]

1 Source IP > 2 Region > 3 Review

Static IP Address
72.52.82.204

Description
GRE-IP-Site1

IP Region
Tremonton, Utah, United States

Latitude
41.7016

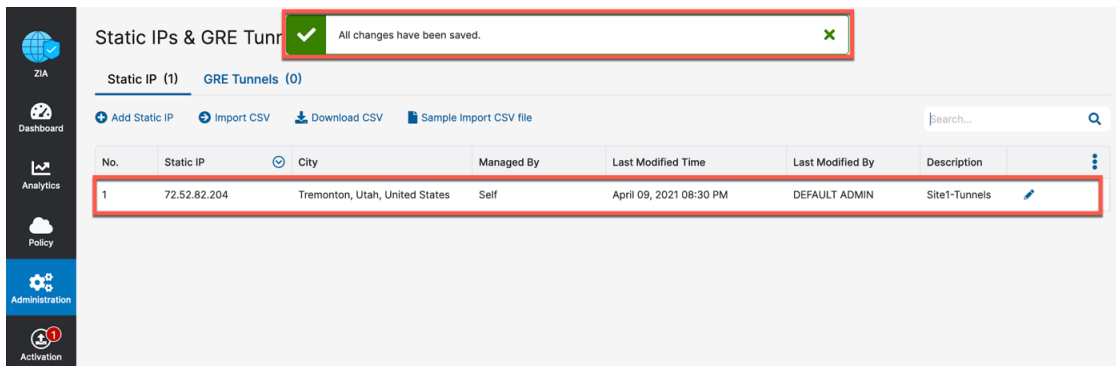
Longitude
-112.1813

Previous **Save** **Cancel**

Figure 54. Review and save the static IP

Validate Static IP Configuration is Saved

After completing the static IP provisioning wizard and saving, you see a message appear “All changes have been saved.” The Static IP is added to the list.



Static IPs & GRE Tunnels [X] All changes have been saved.

Static IP (1) GRE Tunnels (0)

+ Add Static IP + Import CSV Download CSV Sample Import CSV file Search...

No.	Static IP	City	Managed By	Last Modified Time	Last Modified By	Description
1	72.52.82.204	Tremonton, Utah, United States	Self	April 09, 2021 08:30 PM	DEFAULT ADMIN	Site1-Tunnels

Figure 55. Validate the static IP was saved

Add a GRE Tunnel Configuration

Using the static IP that was added from Add a Static IP Configuration, configure the GRE tunnel information. To start, click **GRE Tunnels** and then **Add GRE Tunnel**.

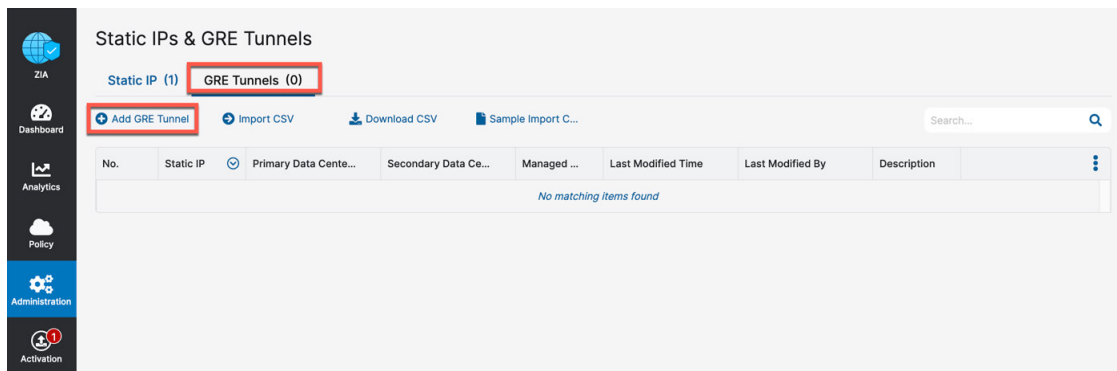


Figure 56. Go to the GRE tunnel configuration wizard

Assign the Source IP to the Tunnel

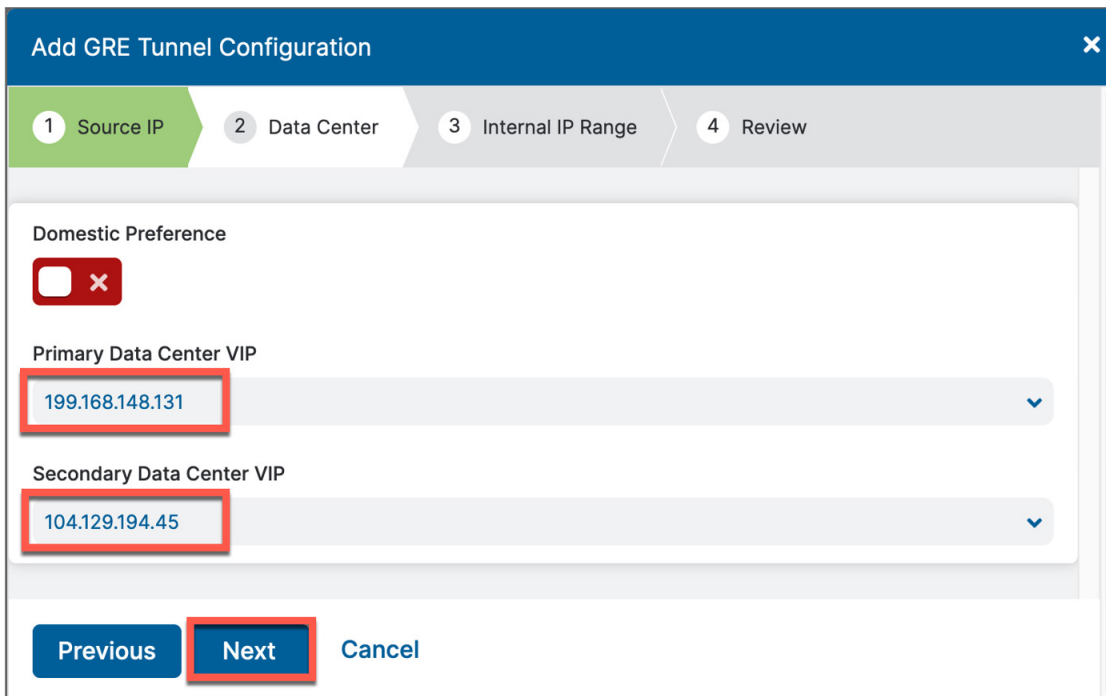
In the **Add GRE Tunnel Configuration** wizard, choose the static IP address that is the source of GRE tunnel and enter a **Description** if desired:

Figure 57. Choose the GRE tunnel source IP

Click **Next**.

Choose Data Centers for Tunnel Termination

Assuming the geospatial information from **Adding the Static IP** was correct, the **Primary Data Center VIP** and **Secondary Data Center VIP** are set automatically. If you want to change these to different VIPs or DCs, choose them from the drop-down menu.



Add GRE Tunnel Configuration [X]

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

Domestic Preference

☐ X

Primary Data Center VIP

199.168.148.131

Secondary Data Center VIP

104.129.194.45

Previous Next Cancel

Figure 58. Choose the data centers for tunnel termination

Click **Next**.

Select GRE Tunnel Internal IP Subnet

Choose an IP subnet (i.e., /29) as the source and destination for the GRE tunnel. This is a locally specific range and can be a subnet that is already in use.

Add GRE Tunnel Configuration [X]

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

Is Unnumbered IP

☒ [X]

Select Internal GRE IP Range

Search...

☒ 172.17.16.112 - 172.17.16.119

☐ 172.17.19.88 - 172.17.19.95

☐ 172.17.19.96 - 172.17.19.103

☐ 172.17.19.104 - 172.17.19.111

☐ 172.17.19.112 - 172.17.19.119

☐ 172.17.19.120 - 172.17.19.127

☐ 172.17.19.128 - 172.17.19.135

☐ 172.17.19.136 - 172.17.19.143

☐ 172.17.19.144 - 172.17.19.151

☐ 172.17.19.152 - 172.17.19.159

Internal GRE IP Range

172.17.16.112 - 172.17.16.119

Previous **Next** Cancel

Figure 59. Select the internal GRE IP range

Click **Next** to review and save.

Save Tunnel Configuration

Review the configuration and click **Save**.

Edit GRE Tunnel Configuration

1 Source IP

2 Data Center

3 Internal IP Range

4 Review

Static IP Address

72.52.82.204

Description

Site1-Tunnels

Primary Data Center VIP

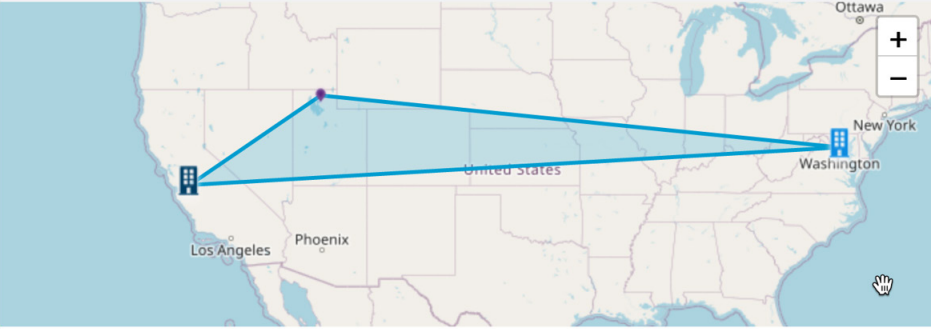
FMT1 (199.168.148.131)

Secondary Data Center VIP

WAS1 (104.129.194.45)

Internal GRE IP Range

172.17.19.112 - 172.17.19.119



Previous

Save

Cancel

Figure 60. Review and save the tunnel setup

Activate All Configuration Changes

Finally, activate the saved configuration changes. Go to **Activation** and click **Activate**.

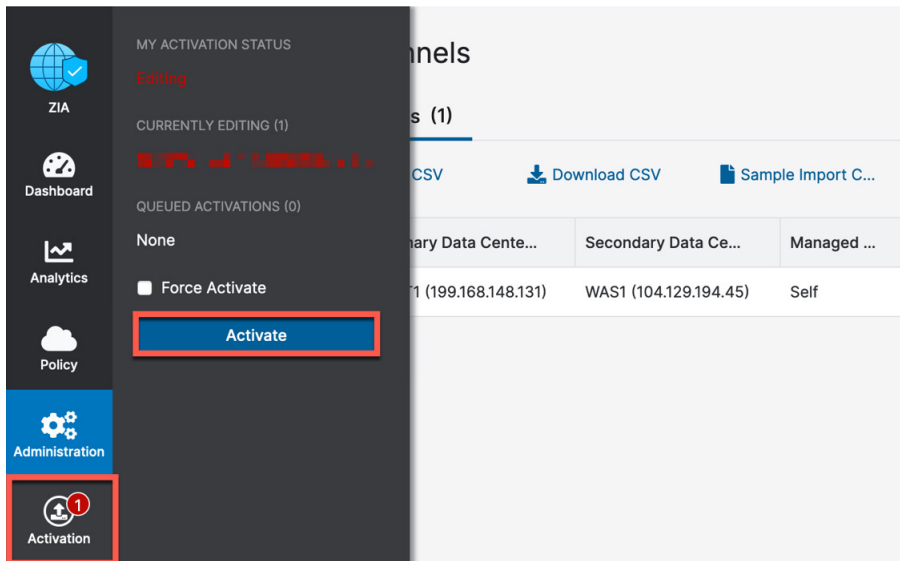


Figure 61. Activate the GRE tunnel configuration

The **Activation Completed!** pop-up indicates your changes are live.

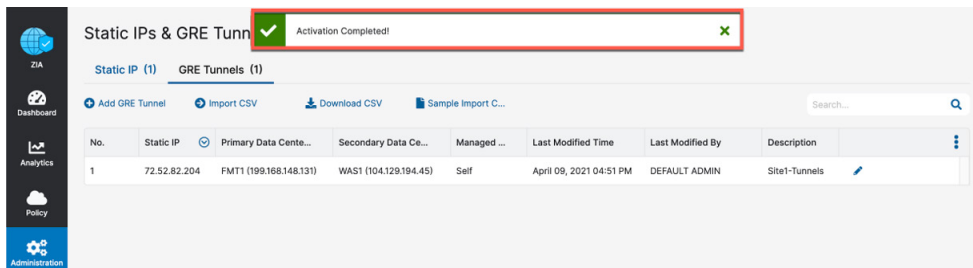


Figure 62. Verify the GRE tunnel configuration was activated

Appendix B: Adding VPN Credentials for Manual Tunnel Creation

The first step in configuring an IPSec tunnel is to create a VPN credential in ZIA.

Go to VPN Credentials

In the **VPN Credential** section, create a FQDN and pre-shared key (PSK) for your IPSec session.

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

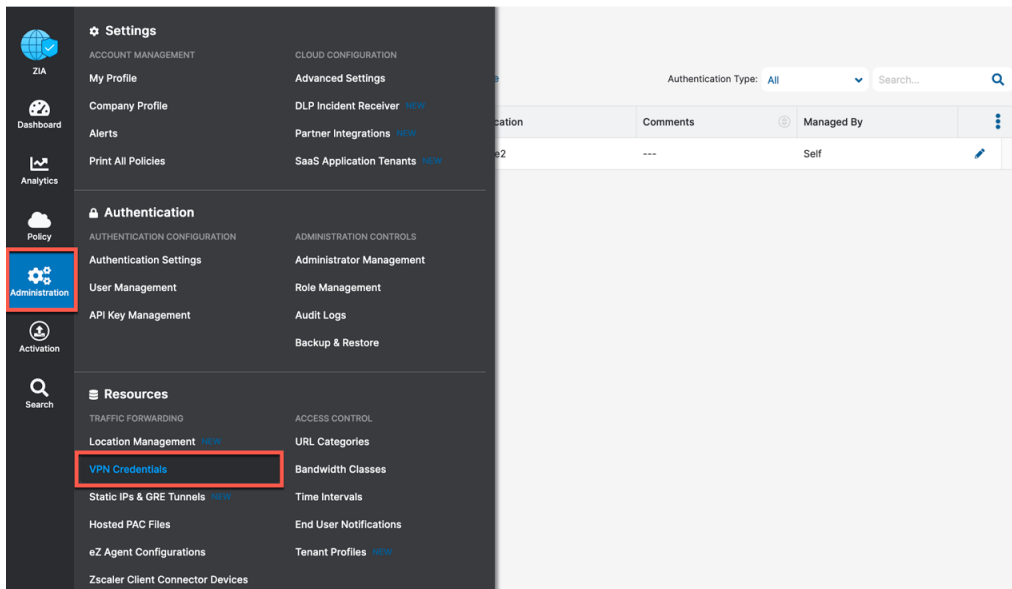


Figure 63. Go to VPN credentials

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**.

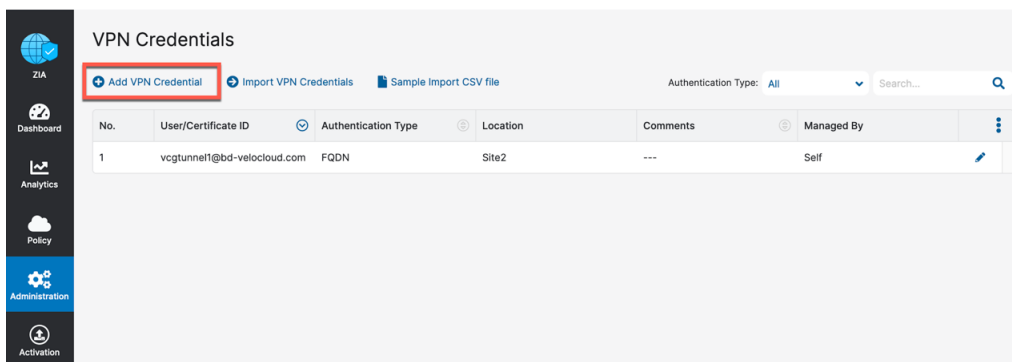


Figure 64. Adding a VPN credential

Enter VPN Credential Data

Configure the FQDN and PSK for IKE. For the FQDN, you only need to configure the username portion of the FQDN, as the domain name is automatically added to the right. After both the FQDN and PSK are configured, click **Save** to continue.

Add VPN Credential

VPN CREDENTIAL

Authentication Type: **FQDN** | XAUTH | IP

Managed By: Self

User ID: vcgtunnel2 @ bd-velocloud.com

New Pre-Shared Key: *****

Confirm New Pre-Shared Key: *****

Comments: Region2

Save Cancel

Figure 65. Enter VPN credential data

Verify VPN Credential

After saving the VPN credential, you see **All changes have been saved** in the top center of your page. You also see the VPN credential you created.

VPN Credentials ✓ All changes have been saved.

[Add VPN Credential](#)
[Import VPN Credentials](#)
[Sample Import CSV file](#)

Authentication Type: All Search...

No.	User/Certificate ID	Authentication Type	Location	Comments	Managed By
1	vcgtunnel1@bd-velocloud.com	FQDN	Site2	---	Self
2	vcgtunnel2@bd-velocloud.com	FQDN	---	Region2	Self

Figure 66. Verify location information and save

Activate Pending Changes

Save the changes. Go to **Activation** and click **Activate**.

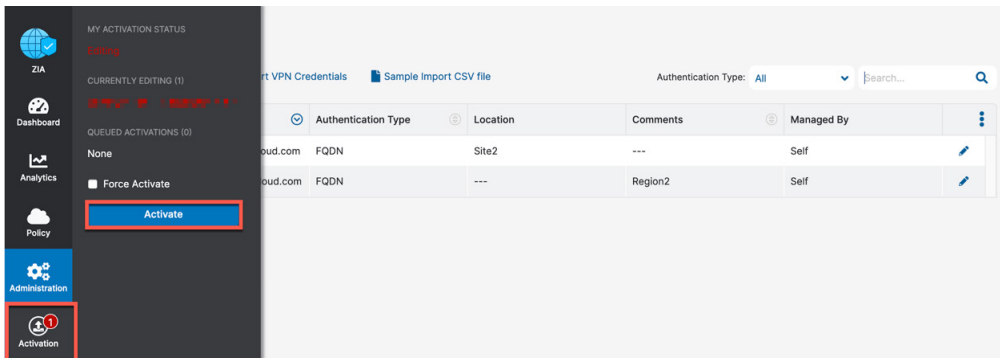


Figure 67. Activate pending changes

Verify Activation

After activating pending changes, you are returned to the previous page. **Activation Completed!** appears in the top of the window.

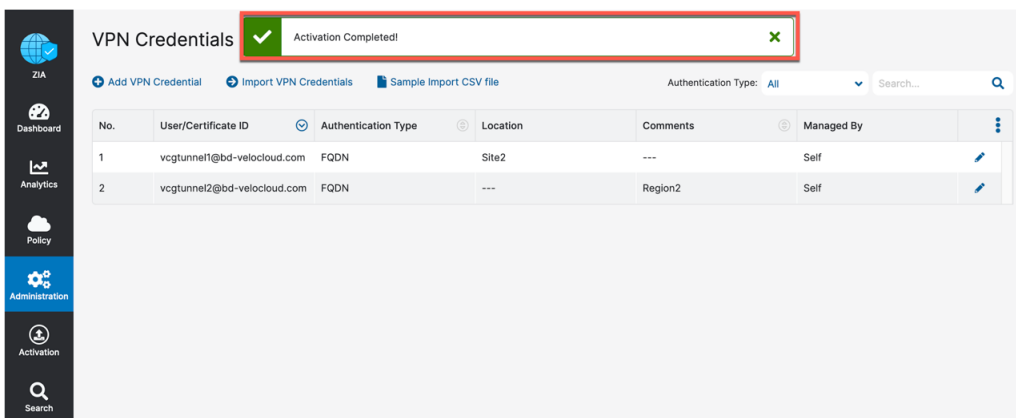


Figure 68. Verify activation

Appendix C: ZIA—Configuring a Location for Manual Tunnels

Add a location if one is not present for the tunnel to access ZIA. If you are uncertain if you already have a site configured, the following steps verify if a location is present.

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

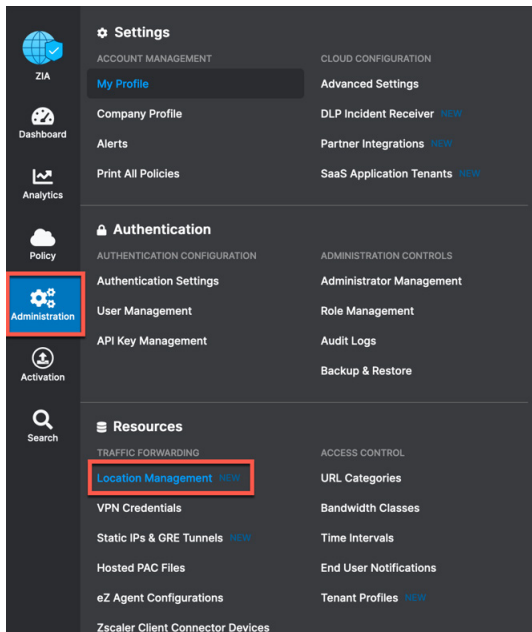


Figure 69. Go to locations

Add a Location

If you see **No Matching Items Found** in the **Location Management** wizard, your ZIA instance does not have any locations configured. To add a location, click **Add Location**. You can also edit any existing locations by clicking the **Edit** icon to the far right of the listed location.

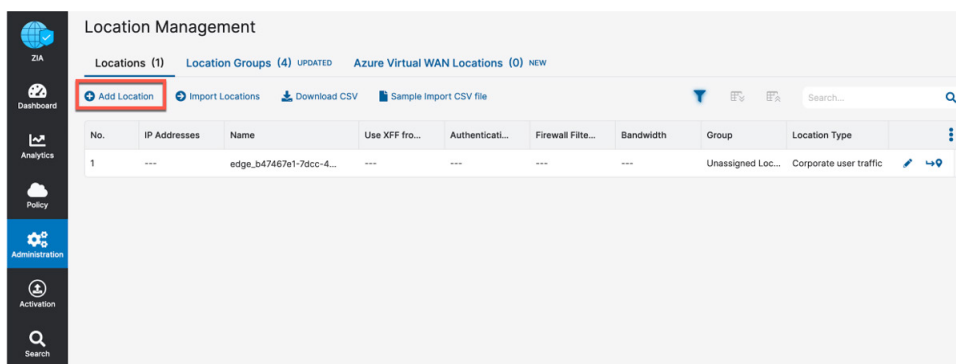


Figure 70. Add a location

Enter Location Data

Fill in the fields highlighted in the **Add Location** dialog.

1. The name of the location is used as a policy object within ZIA.
2. Leave the **Managed By** field as **Self** (because it is used for administration through the web interface).
3. Choose a **Location Type** from the drop-down menu (typically it is Corporate user traffic).
4. Choose the appropriate **Manual Location Groups**.

Figure 71. Enter location data

To learn more, see [About Location Groups](#) (government agencies, see [About Location Groups](#))

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 for a manually-created IPSec tunnel as shown in the next two steps.

Add Static IP Location

You see the static IP you configured in [Add a Static IP Configuration](#) and linked to a GRE tunnel in [Add a GRE Tunnel Configuration](#). Choose the static IP and click **Done**. This then links the static IP and traffic arriving on the GRE tunnel assigned to it to this location.

No.	Tunnel Sour...	Primary Des...	Secondary ...	Primary Destination Internal R...	Secondary Destination Intern...
1	72.52.82.204	199.168.148.131	104.129.194.45	172.17.19.112 - 172.17.19.115	172.17.19.116 - 172.17.19.119

Figure 72. Select the static IP that is linked to the location

When finished, click **Save** to continue.

Adding a VPN Credential to a Location

You see the VPN credential you configured in the [Appendix B: Adding VPN Credentials for Manual Tunnel Creation](#). Select the VPN credential and click **Done**. After you save the location, this couples the VPN credential to this location. When you have completed the fields, select **Save** to continue.

GATEWAY OPTIONS

Use XFF from Client Request ☒ X

Enforce Authentication ☒ X

Figure 73. Add VPN credential to location and save

Confirm Changes Have Been Saved

After saving the location you see **All changes have been saved** in the top center of your page. You also see the location you created.

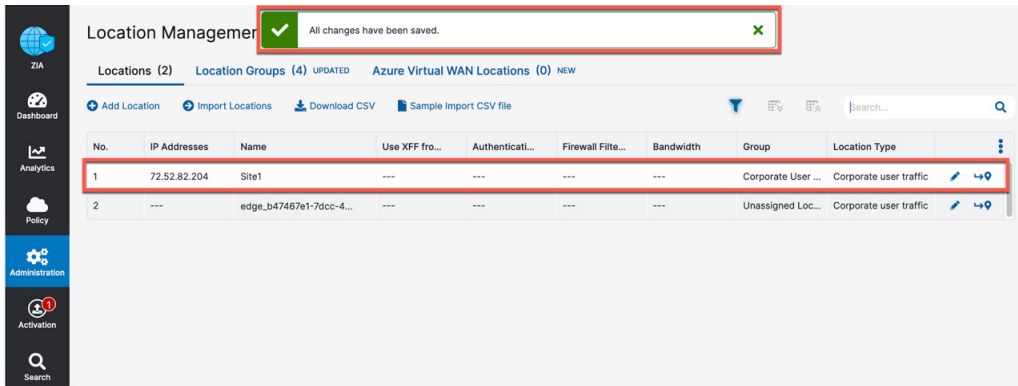


Figure 74. Confirm changes have been saved

Activate Pending Changes

Any time you make a change in ZIA, a number appears over the Activation icon on the left-side navigation.

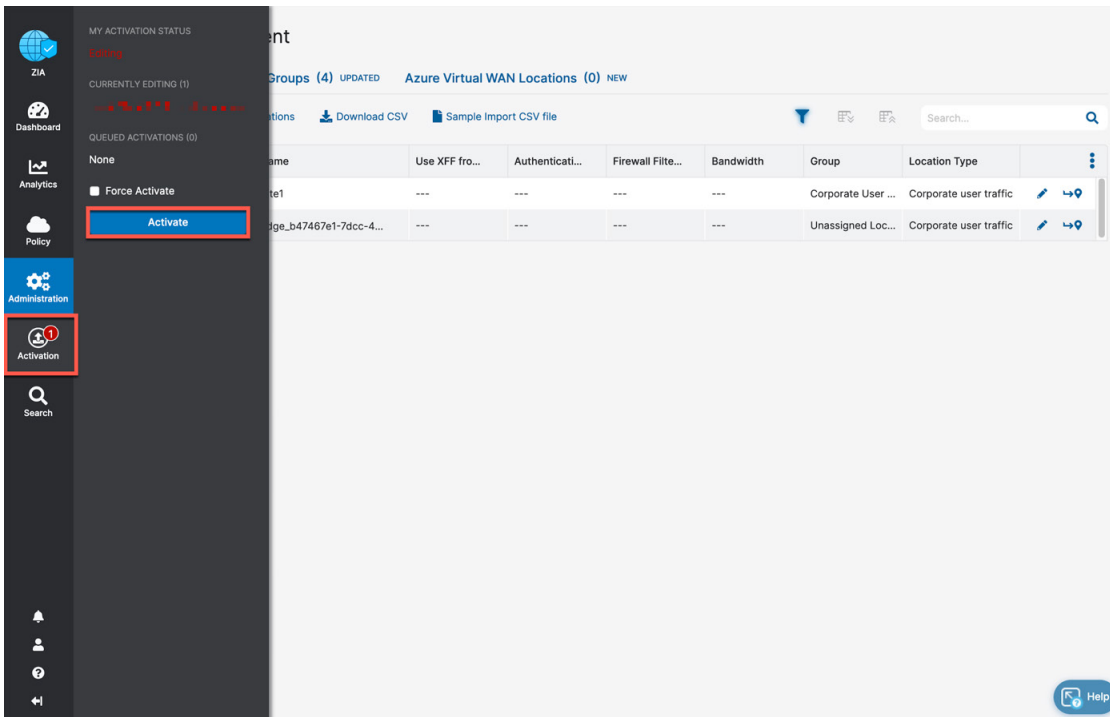


Figure 75. Activate changes

This lets you know that you have changes pending in queue for activation. When you are ready to activate all changes in queue, click **Activate**.

Activation Confirmation

After activating all pending changes, you see **Activation Completed**. At this point, all queued changes have been pushed into production. These changes take effect within seconds.

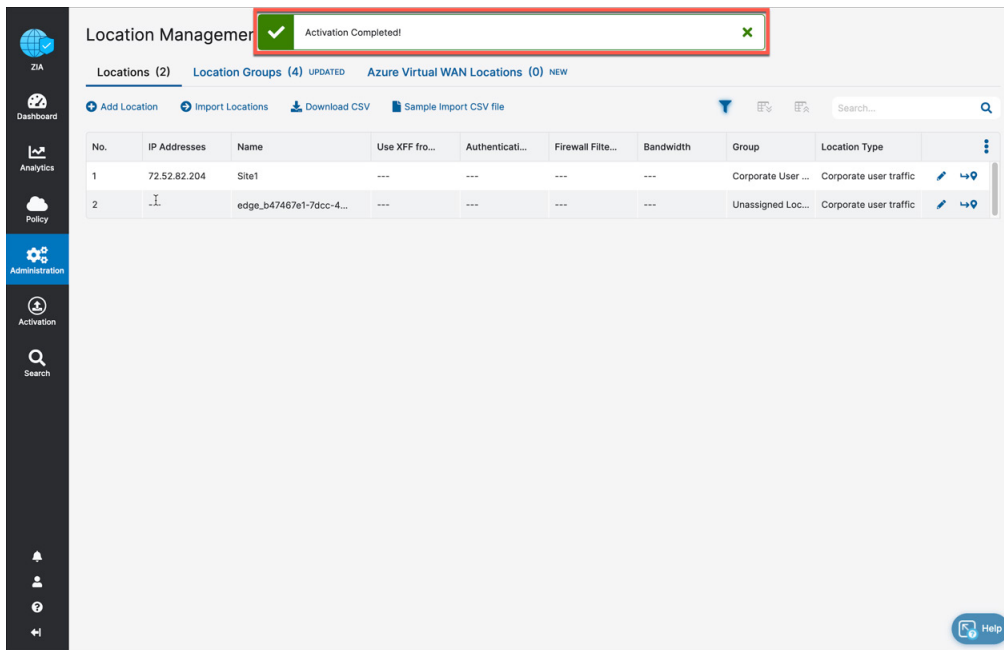


Figure 76. Activation confirmation

Now that you have a location, with a public IP associated with the location, you are ready to start configuring the VMware SD-WAN side.

Appendix D: Verifying ZIA Configuration

Request Verification Page

The URL <https://ip.zscaler.com> can validate if you are transiting ZIA. This section shows examples of what the page output displays if you are or are not transiting ZIA.



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



Connection Quality Zscaler Analyzer Cloud Health Security Research

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

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

Your Gateway IP Address is most likely 209.37.255.2

Figure 77. Non-working example

If you are transiting ZIA, you should see the following dialog.

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

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

The Zscaler proxy virtual IP is 104.129.198.34.

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

Figure 78. Working example

Appendix E: Checking Tunnel Status in ZIA Admin

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

Go to **Analytics > Insights > Tunnel Insights**.

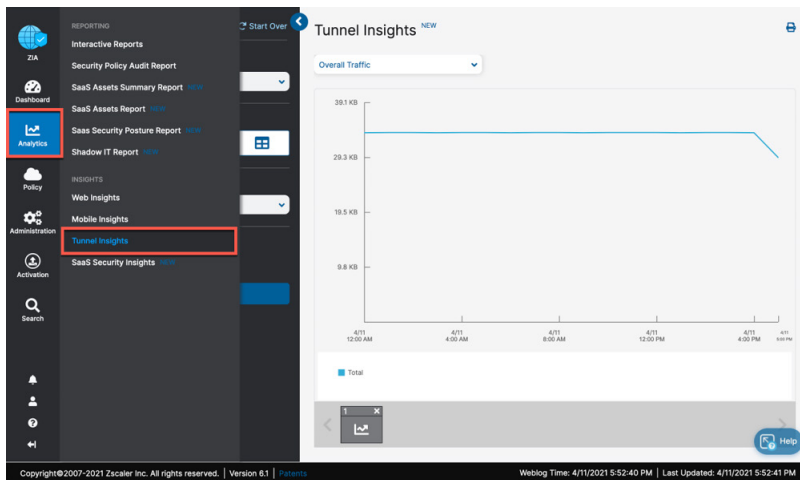


Figure 79. Go to tunnel insights

Tunnel Data Visualization

The **Tunnel Insights** page lets you visualize and filter data in various ways. Configure the **Timeframe**, **Chart type**, and **Metrics** you want to view.

Additionally, you can filter the type of data shown in the chart by clicking the **Filter** caret to expose a drop-down menu to select from.

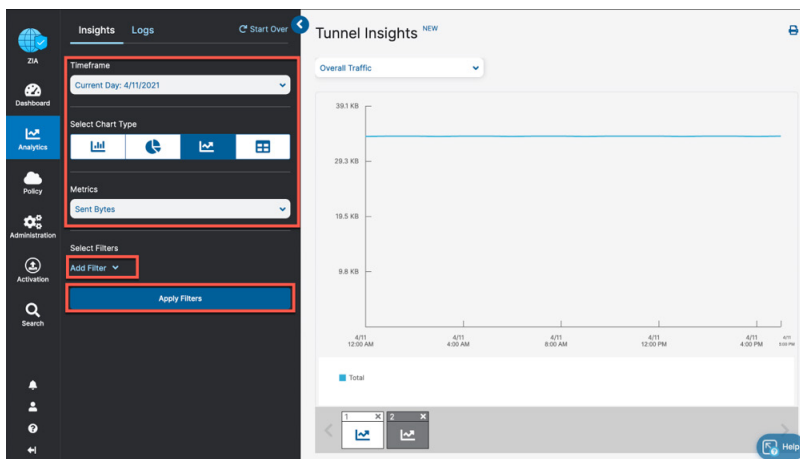


Figure 80. ZIA tunnel insight charts

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

Tunnel Logging

You can also view the state of all tunnels for your tenant from the ZIA Admin Portal to assist in troubleshooting. Click **Logs**:

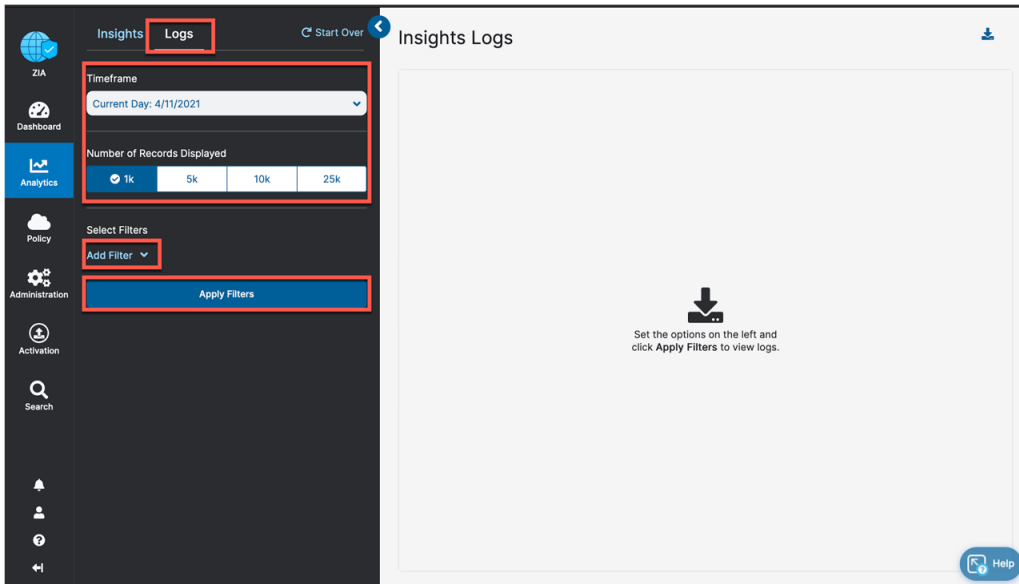


Figure 81. Viewing ZIA tunnel logs

From this page you can filter and change the timeframe for the tunnels and sites you would like to investigate. To learn more, see [ZIA Tunnel Insights Logs: Columns](#) (government agencies, see [ZIA Tunnel Insights Logs: Columns](#)).

Appendix F: Using the Audit Log for API Troubleshooting

ZIA lets you view the changes made to the tenant environment using the **Audit Logging** feature. You can also use the Audit Logging feature to view API calls into the platform.

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

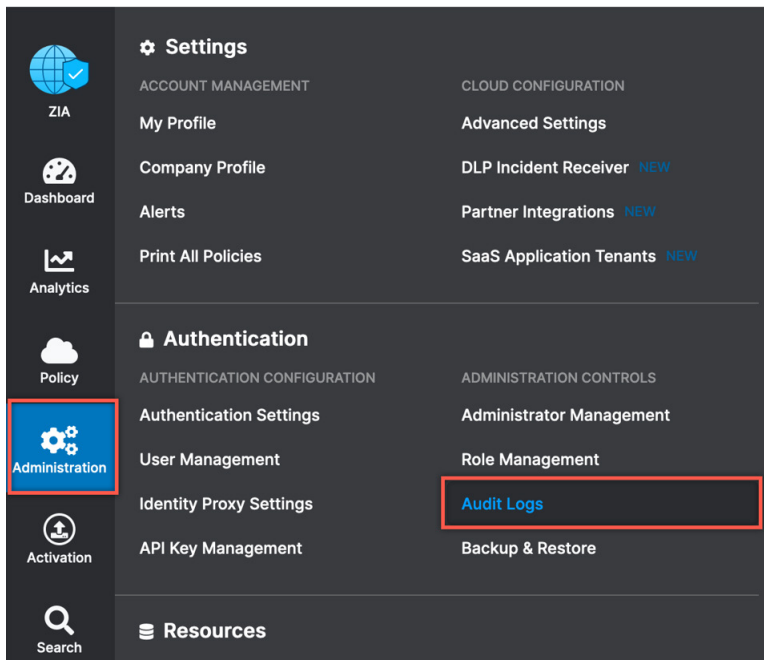


Figure 82. Go to ZIA audit logs

In the **Audit Logs** window, you can filter out all changes and view only the API calls by selecting **API** under the **Interface** drop-down menu.

 A screenshot of the ZIA Audit Logs window. The 'Interface' filter is set to 'API'. The table displays 12 audit log entries. The 'Result' column shows green checkmarks for successful calls and red X marks for failed calls. A red box highlights the 'Result' column.

No.	Timestamp	Action	Category	Sub-Category	Resource	Admin ID	Client IP	Interface	Result
1	October 24, 2021 - 11:36 PM	Sign Out	Login	Login	---	...	54.157.32.184	API	✓
2	October 24, 2021 - 11:36 PM	Create	Traffic Forwarding Re...	Location	edge_b47467e1-7d0c-4c3f-8641-9...	...	54.157.32.184	API	✓
3	October 24, 2021 - 11:36 PM	Create	Traffic Forwarding Re...	VPN Credentials	S866.L3FOA.E211.Va902@bd-veloc...	...	54.157.32.184	API	✓
4	October 24, 2021 - 11:36 PM	Sign In	Login	Login	---	...	54.157.32.184	API	✓
5	October 24, 2021 - 04:43 PM	Sign Out	Login	Login	---	...	54.157.32.184	API	✓
6	October 24, 2021 - 04:43 PM	Delete	Traffic Forwarding Re...	VPN Credentials	s866.L3FOA.E211.Va902@bd-veloc...	...	54.157.32.184	API	✓
7	October 24, 2021 - 04:43 PM	Delete	Traffic Forwarding Re...	Location	edge_b47467e1-7d0c-4c3f-8641-9...	...	54.157.32.184	API	✓
8	October 24, 2021 - 04:43 PM	Sign In	Login	Login	---	...	54.157.32.184	API	✓
9	October 24, 2021 - 04:14 PM	Sign Out	Login	Login	---	...	54.157.32.184	API	✓
10	October 24, 2021 - 04:14 PM	Create	Traffic Forwarding Re...	Location	edge_b47467e1-7d0c-4c3f-8641-9...	...	54.157.32.184	API	✓
11	October 24, 2021 - 04:14 PM	Create	Traffic Forwarding Re...	VPN Credentials	S866.L3FOA.E211.Va902@bd-veloc...	...	54.157.32.184	API	✓
12	October 24, 2021 - 04:14 PM	Sign In	Login	Login	---	...	54.157.32.184	API	✓

Figure 83. ZIA audit logs

This shows a list of all the API interactions, and the **Result** column shows whether the call was successful or not.

When you click the icons on the right of the **Result** column, they show the API data that was created or updated from the call:

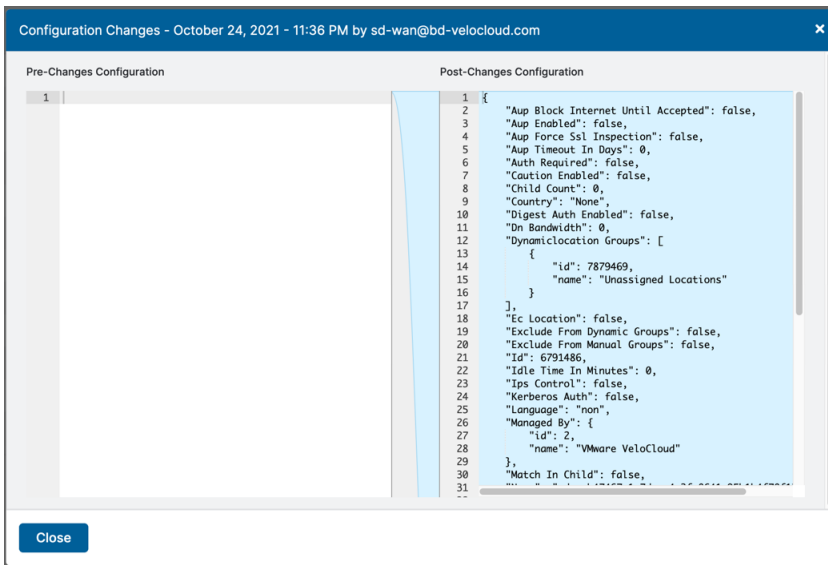


Figure 84. Examining audit log configuration change

Appendix G: Deriving the Zscaler IPsec VPN VIP

All Zscaler public IP endpoints are found at config.zscaler.com (government agencies, see config.zscaler.us). 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 (as is the case for AWS Customer Gateways), derive the IP address from the DNS hostname of the endpoint.

When you go to config.zscaler.com (government agencies, use config.zscaler.us), make sure you select the correct Zscaler cloud into which your tenant is provisioned, ensure that **Cloud Enforcement Node Ranges** is selected from the left-side navigation and then choose the closest **DC locations VPN Host Name** to your AWS region.

The screenshot shows the Zscaler Config console. On the left, the 'Cloud Enforcement Node Ranges' section is selected. The main area displays a table of 'Current Data Centers'. The 'VPN Host Name' column is highlighted in red. The table lists various data centers with their IP addresses, proxy hostnames, GRE Virtual IPs, and VPN Virtual IPs.

Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	SVN Virtual IP	VPN Host Name	Notes
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 85. Zscaler public IP reference

Then use either the `nslookup` or `dig` commands 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 H: Requesting Zscaler Support

You might need Zscaler Support for provisioning certain services, or 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**.

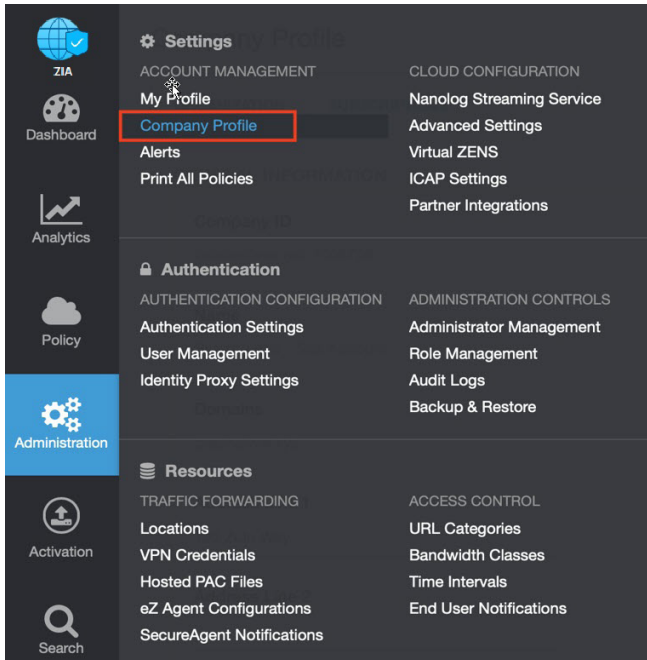


Figure 86. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

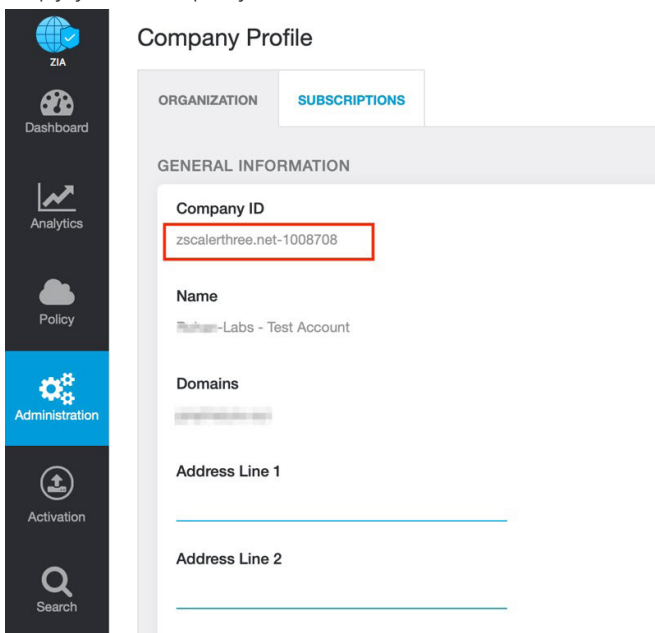


Figure 87. Company ID

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

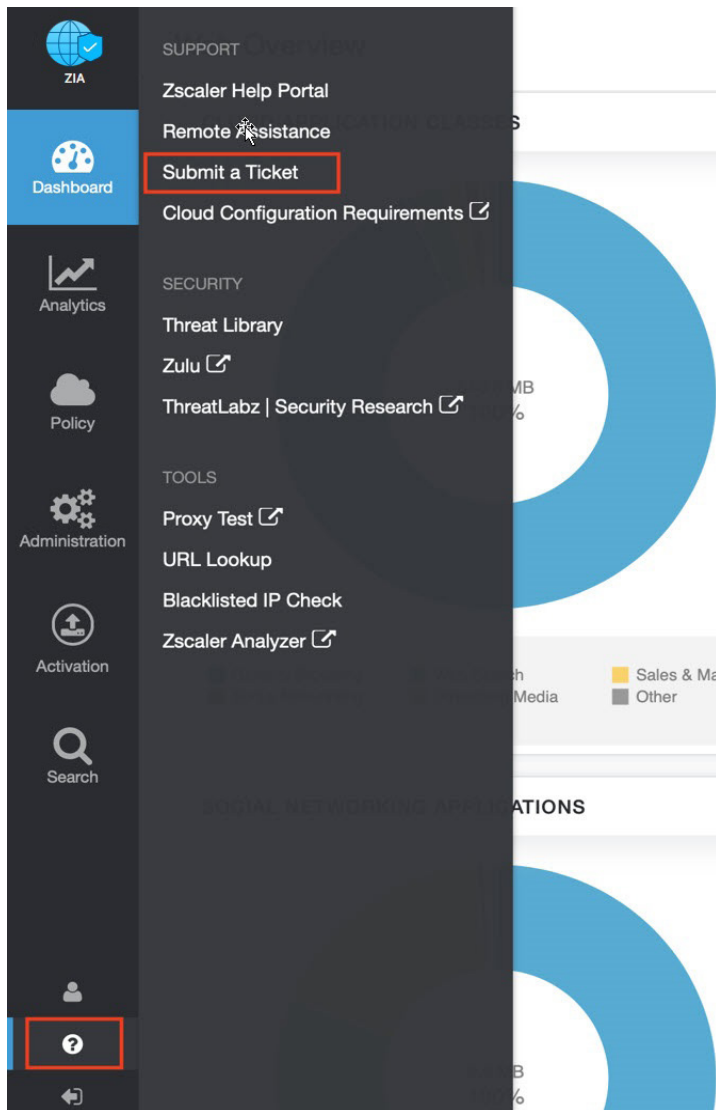


Figure 88. Submit a Ticket