





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

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

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

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

Terms and Acronyms

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

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

About This Document

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

Zscaler Overview

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

Aruba Overview

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

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 <u>partner-doc-support@</u> zscaler.com to offer feedback or corrections for this guide.
- For Zscaler employees: Contact <u>z-bd-sa@zscaler.com</u> to reach the team that validated and authored the integrations in this document.

Zscaler and AWS Introduction

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

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

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet onramp all you do is make Zscaler your next hop to the internet via one of the following methods:

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

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

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

Zscaler Resources

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

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

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

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

Aruba EdgeConnect Overview

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

Aruba Resources

The following table contains links to Aruba support resources.

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

Prerequisites

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

ZIA

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

Silver Peak Orchestrator

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

Configuring ZIA

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

Logging into ZIA

Log into Zscaler using your administrator account.



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

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**.

	Partne	er Integrations			***	
ZIA	Microso	oft Cloud App Security	SD-WAN	Azure Virtual WAN	NEW Crow	dStrike NEW
Dashboard	Add Part	tner Key		_		
~	No.	Partner Name		Кеу		Last Modified By
Analytics					No mate	ching items found
Policy						
Administration	d a partner key	v				

- 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.

Add Partner Key		×
PARTNER		
Туре	Name	
SD-WAN	Silver Peak	*
	Constitution	
Generate Cancel		

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 <u>Configuring ZIA API Credentials and Zscaler Cloud</u>. Make sure to copy the key value for use in the Aruba Orchestrator.

	Partn	er Integrations							
ZIA	Micro	soft Cloud App Security	SD-WAN	Azure Virtual WAN	EW CrowdStrike NEW Car	bon Black NEW			
Cashboard	🔂 Add Pa	artner Key							
<u>~</u>	No.	Partner Name		Кеу	Last Modified By	Last Modified On			÷
Analytics	1	Silver Peak		an an	000000000000000	May 25, 2021 12:43 PM	1	C	×
Policy									
Administration									
Activation									

Figure 5. Verify the SD-WAN partner key



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.

ZIA	Settings Account management My Profile	CLOUD CONFIGURATION Advanced Settings
Dashboard	Company Profile Alerts	DLP Incident Receiver NEW Partner Integrations NEW
Analytics	Print All Policies	SaaS Application Tenants NEW
Policy	Authentication Authentication	ADMINISTRATION CONTROLS
Administration	Authentication Settings User Management	Administrator Management Role Management
Activation	API Key Management	Audit Logs Backup & Restore

Figure 6. Role Management controls

Creating Partner Administrator Role

Complete the following steps:

1. Click the Add Partner Administrator Role.

	Role M	lanagement UPDATE	D					
ZIA	🕒 Add Adr	ninistrator Role • Add Pa	artner Administrator Role		+	Se	arch	۹
Dashboard	No.	Name	Full Access	View-Only Access	User Names 🛞	Functional Scope	Туре	:
I~*	1	Executive Insights App		Dashboard, Insights, I	Obfuscated	Data Loss Prevention, Firewall, DN	Executive App A	1
Analytics	2	Super Admin	Administrators, Dashboard, Intera	Insights	Visible	Advanced Settings, API Key Manag	Standard & Exec	0
Policy								
Administration								
Activation								

Figure 7. Add the partner administrator role

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

2. Name the partner administrator role.

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

Add Partner Administrator Role X
ADMINISTRATOR ROLE
Name SD-WAN
PERMISSIONS
Access Control View Only
PARTNER ACCESS
SD-WAN API Partner Access
VPN Credentials
Save Cancel

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

Administrator Management

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



Figure 9. Administrator Management

Add Partner Administrator

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

	Admi	nistrator Man	age	ment						+ 7 2	
ZIA	Admir	nistrators UPDATED	Au	ditors Admin	istrator Manage	ement					
Dashboard	🔂 Add A	dministrator	O Ac	d Partner Administrat	or 🕒 Add Exec	cutive Insights A				Search	۹
~	No.	Login ID	\odot	Name 💿	Role	Scope	Login Type 🛞	Comments 🛞	Password Expired	Туре	:
Analytics	1	100000000000000000000000000000000000000	191	DEFAULT ADMIN	Super Admin	Organization	Password	1011	false	Standard & Executive	0
Policy	2	· · · · ·	•	DEFAULT ADMIN	Super Admin	Organization	Password		false	Standard & Executive	0
Administration											
Activation											

Figure 10. Add Partner Administrator

Creating Partner Administrator

- 1. In the Add Partner Administrator input box, fill in:
 - $\cdot \land \mathsf{Login} \mathsf{ID}$
 - · An Email
 - $\cdot \, A \text{ Partner Role}$
- 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 <u>Configuring ZIA API Credentials and</u> <u>Zscaler Cloud</u>.

Activate Pending Changes

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

	MY ACTIVATION STATUS	ge	ment		
ZIA	CURRENTLY EDITING (1)	Au	ditors Admin	istrator Manage	ement
e 2		Ac	ld Partner Administrat	or 🔂 Add Exe	cutive Insights A
Dashboard	QUEUED ACTIVATIONS (0)				
	None	⊘	Name	Role	Scope
Analytics	Force Activate		DEFAULT ADMIN	Super Admin	Organization
Daliau	Activate	o	DEFAULT ADMIN	Super Admin	Organization
Policy		ł	SDWAN	SD-WAN	Organization
Administration	ativato ponding chongos				

Verify Activation

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

Aum		Administrator N	anager	nenc							
Add A	dministrator 🔂 Ad	d Partner Administra 😯 Add	I Executiv	e Insights				Se	arch		C
No.	Login ID 📀	Name	S	Login Type 💿	Role	Comments 🛞	Password	Status		Туре	
1		DEFAULT ADMIN	Orga	Password	Super Admin		false	Enabled		Standard &	0
2		DEFAULT ADMIN (Deprecated)	Orga	Password	Super Admin		false	Enabled		Standard & E	0
3	silverpeak@bd-silverp	Silverpeak	Orga	Password	SD-WAN		false	Enabled		Partner Admin	1

Configuring Automated IPSec Tunnels

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

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



Figure 14. Example of an Aruba Orchestrator dashboard

Log into Aruba Orchestrator

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



Figure 15. Aruba Orchestrator login page

Configure Cloud Services

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

太 silverpeak™	zscaler			
Monitoring Configuration	Administration Orchestrator	Support Search Menu		
OVERLAYS & SECURITY	NETWORKING	TEMPLATES & POLICIES	CLOUD SERVICES	
Business Intent Overlays Apply Overlays Interface Labels Hubs Regions Deployment Profiles Internet Traffic Definition <i>Security</i> Firewall Zones Firewall Zones Security Policies IPSec Key Rotation Inbound Port Forwarding	Deployment Interfaces NAT VRRP DNS Proxy WCCP PPPOE Loopback Interfaces Loopback Orchestration Virtual Tunnel Interfaces (VTI) DHCP Server Defaults DHCP Leases DHCP Eailwor State	Templates System, QoS, Opt, Tunnels, UDA, Shaper, Routes Apply Template Groups Policies Route Policies QoS Policies Schedule QoSMap Activation Optimization Policies SaaS NAT Policies ACLs Access Lists Shaping	AWS Network Manager Check Point CloudGuard Connec Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access	
SSL	Routing	Shaper		
SSL Certificates SSL CA Certificates SSL for SaaS	Routes Regional Routing BGP BGP ASN Pool	Applications & SaaS User Defined Applications SaaS Optimization Application Definitions		
Discovery Discovered Appliances Preconfiguration Configuration Wizard	OSPF Multicast Peer Priority	Application Groups TCAs Threshold Crossing Alerts IP SLA		
Licensing Licenses Cloud Portal	Management Routes Tunnels Tunnels			
	Auto MTU Discovery Tunnel Exception			

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**.

Monitoring Configuration	on Administration	Orchestrator	Support	Search Men	u		
earch tags, appliances	Show Tags	Dashboard	scaler Interne	t Access \times			
 Zscaler Fabric 3 		Zscaler Internet A	Access 🕐	Tunnels	Ċ		
 Branch 2 HA SanJose1 		Subscription	Settings	terface Labels	ZEN Override	Gateway Options	IP SLA
Hub 1			***				
ab EC-V-AWS1		App	pliance			Interface Label	

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

Build Tunnels Using These Interfaces	×

INET1 INET2		MPLS
Backup	drag	
LTE		

Figure 18. Choose interfaces for tunnel creation

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

Change Interfaces

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



Figure 19. Apply the tunnel setting to interfaces

Configure Tunnel Settings

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

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

To configure tunnel settings:

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

人silv	∕erpeak [™]	zscaler						
Monitoring Search tags, ap 3 Appliances Zscaler Fa Branch	Configuration pliances s bbric 3 o 2	Administration	Orchestrator Dashboard Scaler Internet	Support Zscaler Inter	Search Menu net Access × Tunnels	N Override	Gateway Ontions	TP SLA
2 🔺 Hub 1	HA SanJose1 HA SanJose2	_		Appliance			Interface Label	

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.

Scaler Tunnel Setting			:
WAN Interface Labels MPLS INET1 LTE INET2 INET1 GRE	General Use Zscale General Mode IPSec Suite B Preset	r Default GRE V None V	
INET2_GRE	Auto Max BW Enabled		
	Suite	None ~	
			Save
ure 21. Select Interfac	ce Label and choose Tunnel N	1ode	

0

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

unnel Setting		
General IKE IPsec	Use Zscaler Default	
KE		
IKE Version	IKE v2	
Preshared Key	Dynamically Generated	
Authentication Algorithm	SHA1 🔽	
Encryption Algorithm	AES-128	
Diffie-Hellman Group	2	
Rekey Interval/Lifetime	1440	Mins
Dead Peer Detection		
Delay time	10	Secs
Retry Count	3	1
	DPD effective timeout 3	34 Secs.
Phase 1 Mode	Aggressive 🔳	
		Save Cance

For GRE there are no settings changes necessary.

Configuring a ZIA Subscription

Select the **Subscription** tab.

لا sit	verpeak™	zscaler						
Monitoring	Configuration	Administration	Orchestrator	Support	Search Men	u		
Search tags, a	opliances	Show Tags	Dashboard	Zscaler Inte	rnet Access ×			
 Zscaler F 	abric 3	Z	scaler Intern	et Access 🤇	Tunnels	C		
Brance	h 2 HA SanJose1 HA SanJose2		Subscription	nnel Settings	Interface Labels	ZEN Override	Gateway Options	IP SLA
4 Hub	1 DEC-V-AWS1			Appliance			Interface Label	



Configuring ZIA API Credentials and Zscaler Cloud

Configure the ZIA cloud and your ZIA API credentials. For large production deployments, keep the **Configuration Polling Interval** setting at the default of 10 minutes. This increases the responsiveness of the API when you make frequent changes to the Zscaler cloud configuration. If the customer uses a subcloud for DC selection, enter it into the **SubCloud ID** field.

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

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

Figure 24. Configuring API credentials

Click **Save** to refresh the screen.

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

Verify ZIA Account Update

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

Monitoring Configuration	Administratio	n Orchestrator Support	Search Menu	Intro to	Overlays		4 Sites 1 3 Health
earch tags, appliances	\$	Daskhard Zeeles Inte					
3 Appliances	Show Tags	Dashboard Zscaler Inte	met Access ×				
Zscaler Fabric 3 Branch 2		Zscaler Internet Access	Tunnels C 1 min				
2 A HA SanJose1		Subscription Tunnel Settings	Interface Labels ZEN Override Ga	teway Options IP SLA Sho	w Sub-Locations Pa	use Orchestration	
MA SanJose2							Search
EC-V-AWS1		Appliance	Interface Label	Gateway Options	Bandwidth (Mbps)	VPN Credentials and Location Status	Zscaler ZENs
				No Dat	a Available		
			Update Ziscaler Int	emet Access account successfully	6		×

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.

aru	ba	zscaler										
Monitoring	Configuration	Administration	Orchestrator	Support	Search Menu	1		intro t	o Overlays			
Search tags, ag 3 Appliance Zscaler F Brance C C C Hub	as +/- abric 3 th 2 th SanJose1 th SanJose2	Show Tags	Dashboard Zscaler Interne Subscription Inte	Flows the Access of Access	Topology Tunnels Tunnel Settings	IP SLA C Service Edge Over	ccess × /	Audit Logs Alarms	Gateway Options	Zscaler Association	Show sub-locations	
ć	EC-V-AWS1		Appliar	nce	Interfac	ce Label	Mode	Gateway O	ptions	Bi	andwidth Data Available	Zscaler

Figure 26. How to access Zscaler Association of Appliances

2. Select **Add** under Zscaler.

3. Click Save.

caler Applia	nce Association			
Accociato an	pliances to Zscalar			
to orchestra	Add Remove	3 Rows	Sear	ch
Zecalor	pliances to Zscaler e IPSec and GRE Tunnels.	Hostname	Present	Changes
LSCalei		EC-V-AWS1		Add Zscaler
		SanJose2		Add Zscaler
		SanJose1		Add Zscaler
				Save Ca

Figure 27. Associating EdgeConnect Appliances to ZIA Automation

Configuring Business Intent Overlays

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

太 silver peak™	zscaler				
Monitoring Configuration	Administration Orchestrator	Support Search Menu			
OVERLAYS & SECURITY	NETWORKING	TEMPLATES & POLICIES	CLOUD SERVICES		
Business Intent Overlays Apply Overlays Interface Labels	Deployment Interfaces NAT	Templates System, QoS,Opt, Tunnels, UDA, Shaper, Routes Apply Template Groups	AWS Network Manager Check Point CloudGuard Connect Microsoft Azure Virtual WAN Microsoft Office 265		
Regions Deployment Profiles Internet Traffic Definition	DNS Proxy WCCP PPPoE	Policies Route Policies QoS Policies Schedule OoSMap Activation	Microsoft Office 365 Zscaler Internet Access		
Security Firewall Zones Firewall Zone Security Policies	Loopback Interfaces Loopback Orchestration Virtual Tunnel Interfaces (VTI)	Optimization Policies SaaS NAT Policies			
IPSec Key Rotation	DHCP Server Defaults	ACLs Access Lists			
Inbound Port Forwarding Advanced Security Settings	DHCP Failover State	Shaping Shaper			
SSL	Routing	Applications & SaaS			
SSL Certificates SSL CA Certificates SSL for SaaS	Routes Regional Routing BGP	User Defined Applications SaaS Optimization Application Definitions			
Discovery	BGP ASN POOL	Application Groups			
Discovered Appliances Preconfiguration Configuration Wizard	Multicast Peer Priority Admin Distance	TCAs Threshold Crossing Alerts IP SLA			
Licensing	Management Routes				
Licenses Cloud Portal	Tunnels				
	Tunnels Tunnel Groups Auto MTU Discovery Tunnel Exception				

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.

lonitoring	Configuration	Administra	tion Orchestrator	Support	Search Menu	Intro to	Overlays							
rch tags, ap	show Tags	Dashboard	Zscaler Intern	et Access	Business Intent Overlays \times									
Zscaler Fi	ibric 3	Business I	ntent Overlays 🤅		Apply Overlays Regions	cply Overlays Regions Hubs View Overlay Stats Interface Labels								
2	HA SanJose1	Delogity	Quadau		SD-WAN Traffic to Inte	rnal Subnets 🧭	Breakout Traf	fic to Internet & Clo	ud Services 🖌					
e Hub	EC-V-AWS1	1 =	Management Match Traffic Overlay ACL	Topology Mesh	Hubs + Primary Interfaces	Backup Interfaces Qos & Security +	Break out Backhaul	INET1 INET2 Waterfall: Auto	LTE					
		2	Zscaler Match Traffic AnyTraffic	Hub & Spok	e INET1 INET2 High Quality Waterfall: Overall Quality		1 💮 Backhaul 2 💭 Break out	INET1 INET2 Waterfall: Auto						
		3	DefaultOverlay Match Traffic	Mesh	INET1 INET2 High Quality Waterfall: Overall Quality	E Pri & Sec Down	1 a Break out 2 a Backhaul	INET1	C LTE					

+New

Figure 29. Enabling Zscaler for breakout traffic

Configuring Preferred Policy Order

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

Configuration			
Name Zscaler Match Appliance ACL SD-WAN Traffic to Internal Subnets B	AnyTraffic reakout Traffic to Internet & Cloud Services	Region Global •]
Branch Settings Hubs EC-V-AWS1 Preferred Policy Order Available Policies * Scaler Cloud Image: Cloud Backhaul Via Overlay Image: Cloud Break Out Locally Image: Cloud Drop Drop	Break Out Locally Using These Interfaces Primary INET INET Add Backup If All Primary Are Down Backup Inter	Available Interfaces	Link Selection Waterfall Balanced Verformance Thresholds Loss < 0 % Latency < 0 ms Jitter < 0 ms Rank Links By uto • Exclude Links That Are Below
			Performance Thresholds Poliow Preferred Policy Order If No Linis Are Above Thresholds

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**.

k silver	peak™	zscale	r						F
Monitoring Co	nfiguration	Administrat	ion Orchestrator	Support	Search Menu	Intro to	Overlays		
arch tags, applian	Ces D	Dashboar	d Zscaler Intern	et Access	Business Intent Overlays ×	Tunnels			+**
3 Appliances Zscaler Fabric Branch 2	3 San Jose I	Business :	Intent Overlays	erlays Ca	Regions H	Hubs View Overlay Stats Inte	erface Labels		-1
A Hub 1	SanJose2				SD-WAN Traffic to Inter	rnal Subnets 🥓	Breakout Traff	ic to Internet & Clo	ud Services 🥓
EC-	V-AWS1	Priority	Overlay	Topology	Hubs + Primary Interfaces	Backup Interfaces Qos & Security +	Policy Order	Primary Interfaces	Backup Interfaces
		1	Management Match Traffic Overlay ACL	Mesh	High Quality Waterfall: Overall Quality	If Pri & Sec Down	1 A Break out 2 A Backhaul	INET1 INET2 Waterfall: Auto	
		2 	Zscaler Match Traffic AnyTraffic	Hub & Spoke	High Quality		1 Scaler Cloud 2 Backhaul 3 Break out	INET1 INET2 Waterfall: Auto	🗅 LTE
		3 = ×	DefaultOverlay Match Traffic AnyTraffic	Mesh	INET1 INET2 High Quality Waterfall: Overall Quality	(2) 🖒 LTE If Pri & Sec Down	1 Break out 2 Backhaul	INET1	C LTE

Figure 31. Save and apply changes

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

Col	nfirm Changes	
A	IMPORTANT: Updating Overlays can be service affecting. We recommend changing them during a network maintenance window. Changes will be applied to associated appliances over the next few minutes.	
	Modified Overlays	
	Zscaler 3 appliances	

Figure 32. Confirm changes

Verifying Automated Tunnel Establishment

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

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

人silv	verpeak≃	zscaler	RU	Release 8.10.15.40131 User pabbott@zscaler.com [log											
Monitoring	Configuration	Administration	Orchestrator	Support	Search Menu		Intro 1	to Overlays				4 Sites	1 3 Healthy		
Search tags, ap	Show Tags	Dashboard	Zscaler Interne	et Access ×	Business Intent Overlays	Tunnels Audit Logs	Alan	ms T	funnel Exception						
 A Appliance Zscaler R 	abric 3	Zscaler Interr	net Access 📀	Tunnels	C 4 mins										
Brand	h 2	Subscription	funnel Settings	terface Labels	ZEN Override Gateway Op	tions IP SLA Show	ub-Locations	5	Pause Orchestration						
	HA SanJose1	5 Rows													
- Hub	EC-V-AWS1	Ap	ppliance		Interface Label	Gateway Options		Ban	dwidth (Mbps)	VPN Cre	dentials and Location Status	Zscaler ZE	Ns		
		SanJose1		INET1		Use XFF from Client Request=f	lse, Enf U	pload=OFF,	Download=OFF		Deployed	Discovered: 199.168.1	48.132, 104.12		
		SanJose1		INET2		Use XFF from Client Request=f	lse, Enf U	pload=OFF,	Download=OFF	1	Deployed	Discovered: 199.168.1	48.132, 104.12		
		EC-V-AWS1		INET1		Use XFF from Client Request=f	lse, Enf U	pload=OFF,	Download=OFF		Deployed	Discovered: 199.168.1	48.132, 104.12		
		SanJose2		INET1		Use XFF from Client Request=f	lse, Enf U	pload=OFF,	Download=OFF		Deployed	Discovered: 199.168.1	48.132, 104.12		
		SanJose2		INET2		Use XFF from Client Request=f	lse, Enf U	pload=OFF,	Download=OFF		Deployed	Discovered: 199.168.1	48.132, 104.12		

Figure 33. Verify automated tunnel establishment

View Automated Tunnel Details

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

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

人silv	ver peak-	zs	caler												Release 8.10.15.4 User pabbott@	0131 zscaler.com	n [log out]			
Monitoring	Configuration	Adm	inistration	Orchestrator	Support	S	earch	Menu			Intro to Ov	orlays			4 Sib	es 1	3 Health			
Search tags, ap	Show Tags	Da	shboard	Zscaler Internet	Access	Bus	iness	Intent Overlays	Tunnels ×	Audit Logs	Alarms	Tunnel Exception	1							
 Zscaler Fa 	abric 3	Te	mplates	Tunnel Exception	Export	Sites	1	C 11 mins												
Branch 2 Branch 2		Tunnels Overlay Pessthrough Status All														+tz				
0	EC-V-AWS1	10/3	7 Rows												Search ThirdParty_Zscaler					
	Edit	Appliance	Passthrough 1	Tunnel	Admin	St	Status 🔺	Local IP		Remote IP	Mode	NAT	Peer/Service	Max BW Kbps	Advanced O.	C				
		1	EC-V-AWS1	ThirdParty_Zscale	r_INET1_P	up	=	up - active	192.168.17.59	104.12	9.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	<u>(i)</u>	new			
		1	EC-V-AWS1	ThirdParty_Zscale	r_INET1_P	up	=	up - active	192.168.17.59	199.16	8.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	1	New			
		1	SanJose1	ThirdParty_Zscale	r_INET1_P	up	=	up - active	72.52.82.206	104.12	9.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	1	when			
		1	SanJose1	ThirdParty_Zscale	r_INET1_P	up	=	up - active	72.52.82.206	199.16	8.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	(i)	ww			
		1	SanJose1	ThirdParty_Zscale	r_INET2_P	up	=	up - active	169.254.1.1	104.12	9.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	1	NM			
		1	SanJose1	ThirdParty_Zscale	r_INET2_P	up	=	up - active	169.254.1.1	199.16	8.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	1	and			
		1	SanJose2	ThirdParty_Zscale	r_INET1_P	up	=	up - active	169.254.1.5	104.12	9.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)	1	way			
		1	SanJose2	ThirdParty_Zscale	r_INET1_P	up	=	up - active	169.254.1.5	199.16	8.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	1	ney			
		1	SanJose2	ThirdParty_Zscale	r_INET2_P	up	=	up - active	72.52.82.207	199.16	8.148.132	IPSec	none	Zscaler_Primary_Z1	200000(Auto)	1	Nº4/			
		1	SanJose2	ThirdParty_Zscale	r_INET2_P	up	=	up - active	72.52.82.207	104.12	9.194.39	IPSec	none	Zscaler_Primary_Z2	200000(Auto)		my			

Figure 34. View automated tunnel details

Configuring Sub-Locations and Gateway Options

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

Configure Sub-location

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

人silv	∕erpeak~	zscaler			÷				R	elease 8.10.15.40131 ser pabbott@zscaler.com [log out]		
Monitoring	Configuration	Administration	Orchestrator	Support	Search Menu		Intro to Overlays			4 Sites 1 3 Healthy		
Search tags, appliances		Dashboard	Zscaler Interne	t Access ×	Business Intent Overlays	Tunnels Audit Logs	Alarms T	unnel Exception				
Zscaler Fabric 3 Branch 2 Z A HASanJose1	Subscription	unnel Settings Ini	Tunnels terface Labels	C 4 mins ZEN Override Gateway Op	ptions IP SLA Show Sub-Loc	cations	Pause Orchestration					
4 Hub 1	MASanJose2	5 Rows								Search		
- 100 5	EC-V-AWS1	Ap	pliance		Interface Label	Gateway Options	Ban	dwidth (Mbps)	VPN Credentials and Location Status	Zscaler ZENs		
		SanJose1		INET1		Use XFF from Client Request=false, En	f Upload=OFF, I	Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12		
		SanJose1		INET2		Use XFF from Client Request=false, Enf	f Upload=OFF, I	Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12		
		EC-V-AWS1		INET1		Use XFF from Client Request=false, En	f Upload=OFF, I	Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12		
		SanJose2		INET1		Use XFF from Client Request=false, En	f Upload=OFF, I	Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12		
		SanJose2		INET2		Use XFF from Client Request=false, En	f Upload=OFF, I	Download=OFF	Deployed	Discovered: 199.168.148.132, 104.12		

Figure 35. Configure sub-location

Enable Gateway Option Orchestration

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

Zscaler Ga	teway Options							×
Add Orc	hestrate Gateway Option	s 🗩					View Individual Appliance Gatewo	vy Options
							Search	
Reorder	Rule Name	Appliances	Location / Interface Label	Sub-Location Name	Sub-Location	Gateway Options	Bandwidth (Mbps)	
				No Data	a Available			
						+**		
						14		
							Save	Cancel

Figure 36. Enable gateway options

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



Figure 37. Enable gateway option orchestration

Add Sub-Location

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

- 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.
- 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.

Rule Name	Guest Wifi	
Location		
Appliances	Appliances, Region, Group	
	Usi	e Tree Selection
Location Label	WAN Label	
	Any	
Sub-Location		
Name	Guest-Wifi Other	
Internal IPs	LAN Label, Firewall Zone, Internal IPs	+Ad
	Guest	
		Save Cancel

Configure Gateway Options

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

Zscaler Ga	ateway Options							×
Add	Orchestrate Gateway Option	is 💶)					View Individual Appliance Gateway Option	s
1 Rows							Search	7.1
Reorder	Rule Name	Appliances	Location / Interface Label	Sub-Location Name	1	Gateway Options	Bandwidth (Mbps)	
\$	Guest Wifi	Апу	Any	Guest-Wifi	LAN La	Enforce Authentication=false, Enforce Firewall Cor	Upload=OFF, Download=OFF	
							Save Cance	el



The Zscaler Gateway Options window appears.

Set Gateway Options

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

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

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

Zscaler Gateway Option	Zscaler Gateway Options & Bandwidth Control X							
Gateway Options		Bandwidth Control	Use Location BW	Fixed BW OFF				
Caution	ON OFF							
AUP	ON OFF							
SSL Inspection	ON OFF							
Authentication	ON OFF							
Zscaler App SSL Setting	ON OFF							
Firewall Control	ON OFF							
				Save				

Figure 40. Set gateway options

Change Gateway Options Confirmation

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

Change Gateway Options

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



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.

Dashboard Zscaler	Internet Access × Busin	ness Intent Overlays	unnels				
Zscaler Internet Acces	SS ? Tunnels 👌	3 mins					
Subscription Tunnel Settin	gs Interface Labels ZEN	Override Gateway Options	IP SLA Show Sub-	ocations Pause	Orchestration		
13 Rows						Si	earch
Appliance 🔺	Interface Label	Sub-Location	IP Addresses	Gateway Options	Bandwidth (Mbps)	VPN Credentials and Locatio	Zscaler ZENs
SanJose2	INET1			Use XFF from Client Reques	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13
SanJose2	INET1	Guest-Wifi	192.168.203.0-192.168.203	Enforce Authentication=fals	Upload=OFF, Download=OFF		
SanJose2	INET1	other		Enforce Authentication=fals	Upload=OFF, Download=OFF		
SanJose2	INET2			Use XFF from Client Reques	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13
SanJose2	INET2	Guest-Wifi	192.168.203.0-192.168.203	Enforce Authentication=fals	Upload=OFF, Download=OFF		
SanJose2	INET2	other		Enforce Authentication=fals	Upload=OFF, Download=OFF		
EC-V-AWS1	INET1			Use XFF from Client Reques	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13
SanJose1	INET1			Use XFF from Client Reques	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13
SanJose1	INET1	Guest-Wifi	192.168.203.0-192.168.203	Enforce Authentication=fals	Upload=OFF, Download=OFF		
SanJose1	INET1	other		Enforce Authentication=fals	Upload=OFF, Download=OFF		
SanJose1	INET2			Use XFF from Client Reques	Upload=OFF, Download=OFF	Deployed	Discovered: 199.168.148.13
SanJose1	INET2	Guest-Wifi	192.168.203.0-192.168.203	Enforce Authentication=fals	Upload=OFF, Download=OFF		
SanJose1	INET2	other		Enforce Authentication=fals	Upload=OFF, Download=OFF		

Figure 42. Verify gateway options

Verify Sub-Locations in ZIA

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

U Add L			Jownload CS		e import (
No.	Name	IP Addresses	Proxy	Use XF	Authe
1	EC-V-AWS				
2	✓ SanJos		13		· · · · · · ·
2.1	⇔ Gues	192.168.203.0			
2.2	↔ other				
3	✓ SanJos				
3.1	↔ Gues	192.168.203.0			
3.2	↦ other				
4	✓ SanJos				
4.1	⇔ Gues	192.168.203.0			
4.2	↦ other				
5	✓ SanJos				
5.1	⇔ Gues	192.168.203.0			
5.2	↦ other				

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

Figure 43. Verify sub-locations in ZIA

Configuring Layer-7 Health Checks for Automated Tunnels

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

Configuring Zscaler IP SLA

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

太 silver peak~	zscaler			
Monitoring Configuration	Administration Orchestrator	Support	Intro to C	Overlays
Search tags, appliances	Dashboard Zscaler Internet A	Access × Business Intent Overlays	Tunnels	
 J Appliances Zscaler Fabric 3 Branch 2 Branch 2 HA SanJose1 HA SanJose2 	Zscaler Internet Access ? Subscription Tunnel Settings Inter 5 Rows	Tunnels C 8 mins face Labels ZEN Override Gateway Op	tions IP SLA Show Sub-Locations	Pause Orchestra
Hub 1	Appliance	Interface Label	Gateway Options	Bandwidth (Mbps)
	SanJose1	INET1	Use XFF from Client Request=false, Enfo	Upload=OFF, Download=OFF
	SanJose1	INET2	Use XFF from Client Request=false, Enfo	Upload=OFF, Download=OFF
	SanJose2	INET1	Use XFF from Client Request=false, Enfo	Upload=OFF, Download=OFF
	SanJose2	INET2	Use XFF from Client Request=false, Enfo	Upload=OFF, Download=OFF
	EC-V-AWS1	INET1	Use XFF from Client Request=false, Enfo	Upload=OFF, Download=OFF

Figure 44. Configure IP SLA

The IP SLA Configuration window appears.

Enable the IP SLA Probes for the Zscaler Tunnels

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

Enable IP SLA rule orchestration	ii Overidys.	
Monitor	HTTP/HTTPS	
	http://gateway.zscalerbeta.net/vontest	1
Address		
Source Interface	Loopback]
Proxy Address	optional	
Proxy Port		(065535)
User Agent	optional	
HTTP Request Timeout	2	Sec
Keep Alive Interval	5	Sec
Sampling Window	300	Sec
Reachability		
Mark Up after X Succeed	2	
Mark Down after X Failed	6	
Loss		_
Mark Up after loss below X %]
Mark Down after loss above X %]
Latency		
Mark Up after average latency below X		Milli Sec
Mark Down after average latency above X		Milli Sec
Metric Combination	OR -	



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

Verify Zscaler IP SLA Rules

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

Navigate to the IP SLA tab

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

太 silver peak™	zscaler				
Monitoring Configuration	Administration Orchestrator	Support Search Menu			
OVERLAYS & SECURITY	NETWORKING	TEMPLATES & POLICIES	CLOUD SERVICES		
Business Intent Overlays Apply Overlays Interface Labels	Deployment Interfaces NAT	Templates System, QoS, Opt, Tunnels, UDA, Shaper, Routes Apply Template Groups	AWS Network Manager Check Point CloudGuard Connect Microsoft Azure Virtual WAN		
Hubs	VRRP	Policies	Microsoft Office 365		
Regions Deployment Profiles Internet Traffic Definition	DNS Proxy WCCP PPPoE	Route Policies QoS Policies Schedule QoSMap Activation	Zscaler Internet Access		
Security Firewall Zones	Loopback Orchestration	SaaS NAT Policies			
Firewall Zone Security Policie	s Virtual Tunnel Interfaces (VTI)	ACLs			
IPSec Key Rotation	DHCP Server Defaults	Access Lists			
Inbound Port Forwarding	DHCP Leases	Shaping			
Advanced Security Settings		Shaper			
SSL	Routing	Applications & SaaS			
SSL Certificates SSL CA Certificates SSL for SaaS	Regional Routing BGP	User Defined Applications SaaS Optimization Application Definitions			
Discovery	BGP ASN POOL	Application Groups			
Discovered Appliances	Multicast	TCAs			
Preconfiguration	Peer Priority	Threshold Crossing Alerts			
Configuration wizard	Admin Distance	IP SLA			
Licensing	Management Routes				
Licenses Claud Partal	Tunnels				
Cloud Portal	Tunnels				
	Tunnel Groups				
	Auto MTU Discovery				
	Tunnel Exception				

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.

ل sil	/erpeak~	zs	caler				<i>911</i> 111111			Release 8.10.1 User pabbo	5.40131 tt@zscaler.com [log ot		
Monitoring	Configuration	Adn	ninistration O	rchestrator	Support	Search Menu	Intro to Overlays			4	Sites 1 3 Healt		
earch tags, ap	pliances O	Da	shboard Zs	caler Interne	Access Bu	usiness Intent Overlays Tunnels IP Serve							
3 Appliances Zscaler Flabric 3 Branch 2 To the second s	Биро	Toport C town											
	h 2 MasanJose1	IP S	la 😧										
	SanJose2	10/2	27 Rows							Search 2	scalerbeta		
0	EC-V-AWS1	Edit	Appliance Name	Active	State	Monitor	Dow	Up Action	Comment	Up Stats	Down Stats		
		1	EC-V-AWS1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, i Tunnel	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mail	Last:1h 22m 4s	Total :0, Last:0		
		1	EC-V-AWS1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, I Tunnel	Tunnel Up: Tunnel = ThirdParty_	generated by overlay man	Last:1h 22m 4s	Total :0, Last:0		
		1	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, i Tunnel	Tunnel Up: Tunnel = ThirdParty_	generated by overlay man	Last:1h 21m 53s	Total :0, Last:0		
		1	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, I Tunnel	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mail	Last:1h 21m 52s	Total :0, Last:0		
		1	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, i Tunnel	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mail	Last:1h 21m 52s	Total :0, Last:0		
		1	SanJose1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, i Tunnel	I Tunnel Up: Tunnel - ThirdParty_	generated by overlay mail	Last:1h 21m 50s	Total :0, Last:0		
		1	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, i Tunnel	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mail	Last:1h 21m 53s	Total :0, Last:0		
		1	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, i Tunnel	Tunnel Up: Tunnel = ThirdParty_	generated by overlay mail	Last:1h 21m 53s	Total :0, Last:0		
		1	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, i Tunnel	Tunnel Up: Tunnel - ThirdParty_	generated by overlay mail	Last:1h 21m 53s	Total :0, Last:0		
		1	SanJose2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = http://gatewa	y.zscalerbeta.net/vpntest, I Tunnel	I Tunnel Up: Tunnel = ThirdParty_	generated by overlay mail	Last:1h 21m 52s	Total :0, Last:0		

Figure 47. Verify the IP SLA rule

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

Appendix A: Manual Tunnel Configuration

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

Configuring Static IPs and GRE Tunnels

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

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



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

Add a Static IP Configuration

Click the Add Static IP selection from the page.



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.

Add Static IP Configuration		<u>م</u>	×
1 Source IP 2 Region	3 Review	. <u>17</u>	
Static IP Address		Description	
72.52.82.206		GRE-IP-Site1	
Next Cancel			
Figure 50. Entering the st	atic 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.

Review Information and Save

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

Add Static IP Configuration	×
1 Source IP 2 Region 3 Review	
Static IP Address 72.52.82.206 Description GRE-IP-Site1	٥
IP Region L Tremonton, Utah, United States 4 Longitude -112.1813	atitude 11.7016
Previous Save Cancel	

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.

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**:

ZIA	Static IP Static IP (Ps & GRE	Tunnels Tunnels (0)]							
Dashboard	Add GRE Tu	unnel 🕤 li	mport CSV	🛓 Do	ownload CSV 🛛 🖺 Sa	mple Import			Search	+‡+	۹
₩.	No.	Static IP 📀	Primary Data 0	en	Secondary Data C	Manage	Last Modified Time	Last Modified By	Descripti	14	÷
Analytics						No matchi	ng items found				
Policy											
Administration											
Activation											

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.

		×
1 Source IP 2 Data Center 3	Internal IP Range 4 Review	
Statio ID Address		
72.52.82.206		~
P Region: Tremonton	LAT: 41.7016	LONG: -112.1813
Description		
Site-1-Tunnel		

Figure 55. Choose the GRE tunnel source IP

Choose Data Centers for Tunnel Termination

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

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

Add GRE Tunnel Configuration	×
1 Source IP 2 Data Center 3 Internal IP Range 4 Review	+
Domestic Preference	
Primary Data Center VIP 199.168.148.131	
Secondary Data Center VIP 104.129.194.43	
Previous Next Cancel	

Figure 56. Choose the data centers for tunnel termination

Select GRE Tunnel Internal IP Subnet

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

Add GRE Tunnel Configuration						
1 Source IP 2 Data Center 3 Internal IP Range 4 Review						
Is Unnumbered IP						
Previous Next Cancel						



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

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

O Add G	RE Tunnel	Import C	sv 🛓 D	lownload CSV 🛛 📔 San	nple Import			Search		2
No.	Static IP	OPrima	ry Data Cen	Secondary Data C	Manage	Last Modified Time	Last Modified By	Descripti		
1	72.52.82.20	6 FMT1	(199.168.148.131)	WAS1 (104.129.194.43)	Self	May 22021 06:00 P	DEFAULT ADMIN (De	Site-1-Tunnel	1	

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.

ZIA Dashbaard	Alerts Print All Policies	Virtual ZENS DLP Incident Receiver 144W Partner Integrations 144W SaaS Application Tenants 145W	cation	Authentication Type: All	V Managed By	Search	Q :
Analytics Policy	Authentication AUTHENTICATION CONSIDURATION Authentication Settings User Management identity Proxy Settings	ADMINISTRATION CONTROLS Administrator Management Role Management Audit Logs Backup & Restore	n.Jose1/INET1/2.NE_2 n.Jose1/INET2/2.NE_7 n.Jose2/INET/3.NE_2 n.Jose2/INET2/3.NE_7 2-V-AWS1/INET1/4.NE_2	WARNINGI Do not change the WARNINGI Do not change the WARNINGI Do not change the WARNINGI Do not change the	Silver Peak Silver Peak Silver Peak Silver Peak Silver Peak		
Activation Q Search	E Resources TRAFFIC FORWARDNO Location Management 1879 VPN Credentials Static IPs & ORE Tunnels 1879 Hosted PAC Files eZ Agent Configurations Zscaler Client Connector Devices	ACCESS CONTROL URL Categories Bandwidth Classes Time Intervals End User Notifications Tenant Profiles (IEX)					

Figure 61. Navigate to VPN credentials

Add a VPN Credential

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

Add V	PN Credential S Import VPN C	Credentials 🛛 🖺 Sample Im	port CS	/ file	Authentication Type: AI	*	Search
No.	User/Certificate ID	Authentication Type		Location	Comments	Managed By	:
1	2.ne_2@bd-silverpeak.com	FQDN		SanJose1/INET1/2.NE_2	WARNING! Do not change the	Silver Peak	1
2	2.ne_7@bd-silverpeak.com	FQDN		SanJose1/INET2/2.NE_7	WARNING! Do not change the	Silver Peak	1
3	3.ne_2@bd-silverpeak.com	FQDN		SanJose2/INET1/3.NE_2	WARNING! Do not change the	Silver Peak	1
4	3.ne_7@bd-silverpeak.com	FQDN		SanJose2/INET2/3.NE_7	WARNING! Do not change the	Silver Peak	1
5	4.ne_2@bd-silverpeak.com	FQDN		EC-V-AWS1/INET1/4.NE_2	WARNING! Do not change the	Silver Peak	1

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.

Authentication Type	Managed By Self	~
User ID		
manualTunnel1	@ bd-silverpeak.com	*
New Pre-Shared Key	Confirm New Pre-Shared Ke	ay.
		9
Comments		

Figure 63. Enter VPN credential data

Verify VPN Credential

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

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

Figure 64. Verify location information and save

Activate Pending Changes

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

ZIA		rt VPN Credent	ials 🛛 📑 Sample Import CSV file		Authentication Type:	All 🗸 Search	٩
Dashboard	admin@bd-sliverpeak.com	⊘	Authentication Type	Location	Comments	Managed By	
~	None	.com	FQDN	SanJose1/INET1/2.NE_2	WARNING! Do not change the 'Ma	Silver Peak	1
Analytics	Force Activate	.com	FQDN	SanJose1/INET2/2.NE_7	WARNING! Do not change the 'Ma	Silver Peak	1
	Activate	.com	FQDN	SanJose2/INET1/3.NE_2	WARNING! Do not change the 'Ma	Silver Peak	1
Policy		.com	FQDN	SanJose2/INET2/3.NE_7	WARNING! Do not change the 'Ma	Silver Peak	1
•		.com	FQDN	EC-V-AWS1/INET1/4.NE_2	WARNING! Do not change the 'Ma	Silver Peak	1
Administration		verpeak.com	FQDN			Self	1
Activation							
Q Search							

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.

Add V	PN Credential 🛛 🕤 Import VPN Creden	tials Sample Import CSV file		Authentication Type:	All 🗸 Search	
No.	User/Certificate ID	Authentication Type	Location	Comments	Managed By	
1	2.ne_2@bd-silverpeak.com	FQDN	SanJose1/INET1/2.NE_2	WARNING! Do not change the 'Ma	Silver Peak	
2	2.ne_7@bd-silverpeak.com	FQDN	SanJose1/INET2/2.NE_7	WARNING! Do not change the 'Ma	Silver Peak	
3	3.nef_2@bd-silverpeak.com	FQDN	SanJose2/INET1/3.NE_2	WARNING! Do not change the 'Ma	Silver Peak	
4	3.ne_7@bd-silverpeak.com	FQDN	SanJose2/INET2/3.NE_7	WARNING! Do not change the 'Ma	Silver Peak	
5	4.ne_2@bd-silverpeak.com	FQDN	EC-V-AWS1/INET1/4.NE_2	WARNING! Do not change the 'Ma	Silver Peak	
6	manualtunnel1@bd-silverpeak.com	FQDN			Self	

Figure 66. Verify the activation

Q

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.

O Add I	Location 📀 Import Locations 🛃 Download	I CSV 📑 Samp	le Import CSV file				T 🗗 🕅	search		
							6			
No.	Name	Use XF	IP Addresses	A	Firewall Filteri	Bandwidth	Group	Location Type		
1	EC-V-AWS1/INET1/4.NE_2						Unassigned Loca	Corporate user traffic		→(
2	> SanJose1/INET1/2.NE_2						Unassigned Loca	Corporate user traffic	1	ь (
3	> SanJose1/INET2/2.NE_7						Unassigned Loca	Corporate user traffic		4
4	> SanJose2/INET1/3.NE_2						Unassigned Loca	Corporate user traffic	1	4
5	> SanJose2/INET2/3.NE_7						Unassigned Loca	Corporate user traffic		4

Figure 68. Add a location

Enter the Location Data

Complete the fields.

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

		Country	
Site1		United States	
ity/State/Province		Time Zone	
SAn Jose, CA		America/Los Angeles 🗸	
anual Location Groups		Dynamic Location Groups	
None	*		
clude from Manual Location Grou	ips	Exclude from Dynamic Location Groups	
ocation Type		Managed By	
Corporate user traffic	~	Self 🗸	
RESSING			
RESSING tatic IP Addresses and GRE Tunne None oxy Ports	is V	VPN Credentials	
RESSING atic IP Addresses and GRE Tunne None oxy Ports None	ls ~	VPN Credentials Nons v	
RESSING Latic IP Addresses and GRE Tunne Vone None rtual ZENS	is V	VPN Credentials None	
RESSING attle IP Addresses and GRE Tunne kone voy Ports kone trual ZENS kone	is ~	VPN Credentials None v Virtual ZEN Clusters None v	
RESSING able IP Addresses and GRE Tunne kone trust ZENS kone EWAY OPTIONS	is •	VPN Credentials None v Virtual ZEN Clusters None v	
RESSING table IP Addresses and GRE Tunne kone oropy Ports None EWAY OPTIONS se XEF from Client Request	is •	VPN Credentials None Virtual ZEN Clusters None V	

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 <u>Add a Static IP</u> <u>Configuration</u> and linked to a GRE tunnel in section <u>Add a GRE Tunnel Configuration</u>.

- 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.

None	^		
Unselected Items		Selected Items (1)	
Search	۹	72.52.82.206	•
✓ 72.52.82.206			🛓 Expor
			Secondary Destination Intern
			~

Figure 70. Select the static IP linked to the location

Adding a VPN Credential to a Location

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

- 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

None	Unselected Items			Selected Items (1)	
Exclude fr	Search	٩	0	manualtunnel1@bd-silverpeak.com	0
Location	manualtunnel1@bd-silverpeak.com				
ADDRESSIN					
Static IP # 72.52.82	_				
Proxy Por	Done			Clear Selection	
None	~			None	~

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.

Loca	tion Manag	ger 🗸 🗚	l changes h	ave been save	ed.					×				
Locat	cation O Im	port Locations	(5) UPDAT	ED Azur	e Virtual W	AN Locatio	ns (0) NEW			F. F	Searc			
No.	Name	IP Addre	Prox	Use	Auth	Firew	Band	Virtu	IPS C	Group	Mana	Loca		
1	EC-V-A									Unassig	Silver Pe	Corpora	1	₩
2	> SanJo									Unassig	Silver Pe	Corpora	1	₩
3	> SanJo									Unassig	Silver Pe	Corpora	1	÷۹
4	> SanJo									Unassig	Silver Pe	Corpora	1	₩٩
5	> SanJo	1111					1111			Unassig	Silver Pe	Corpora		₩٩
6	Site1	72.52.82.206								Corpora	Self	Corpora	1	₩

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.

		ent												
ZIA		Groups	(5) UPDATE	D Azur	e Virtual W	AN Location	ns (O) NEW							
Dashboard		itions	🛓 Downlo	ad CSV	Sample Imp	oort CSV file			•	E T	Searc	h		۹
₩.	None	dre	Prox	Use	Auth	Firew	Band	Virtu	IPS C	Group	Mana	Loca		:
Analytics	Force Activate									Unassig	Silver Pe	Corpora	1	₩ 0
Policy	Activate									Unassig	Silver Pe	Corpora	1	₩Q
										Unassig	Silver Pe	Corpora	1	÷₽
Administration										Unassig	Silver Pe	Corpora	1	÷۹
<u></u>										Unassig	Silver Pe	Corpora	1	₩Ŷ
Activation		.82.206								Corpora	Self	Corpora	1	÷۹

Figure 73. Activate changes

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

Activation Confirmation

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

Locat	ions (6) Lo	cation Groups	(5) UPDATI	ED Azur	e Virtual WA	N Locatio	ns (0) NEW	6						
🖸 Add L	ocation 🕘 Im	port Locations	🛓 Downlo	oad CSV	Sample Imp	ort CSV file			Ŧ	er: e	Searc	h		
No.	Name	IP Addre	Prox	Use	Auth	Firew	Band	Virtu	IPS C	Group	Mana	Loca		
1	EC-V-A									Unassig	Silver Pe	Corpora	1	
2	> SanJo				+					Unassig	Silver Pe	Corpora	1	
3	> SanJo				''					Unassig	Silver Pe	Corpora	1	
4	> SanJo									Unassig	Silver Pe	Corpora	1	
5	> SanJo									Unassig	Silver Pe	Corpora	1	
6	Site1	72.52.82.206								Corpora	Self	Corpora	1	

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

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

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

Configuring Aruba SD-WAN IP SLA

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

لا sil	verpeak™	zscaler				
Monitoring	Configuration	Administration	Orchestrator	Support	Search Menu	
OVERLAYS	& SECURITY	NETWORKING	5	TEMPLAT	ES & POLICIES	CLOUD SERVICES
Business I Apply Over Interface I Hubs Regions Deploymer Internet Tr	ntent Overlays rlays .abels nt Profiles raffic Definition	Deployment Interfaces NAT VRRP DNS Proxy WCCP PPPoE		Template Tunnels, Apply Te <i>Policies</i> Route Po QoS Poli Schedule	2S System,QoS,Opt, UDA,Shaper,Routes mplate Groups Ilicies cies 2 QoSMap Activation	AWS Network Manager Check Point CloudGuard Connect Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access
Security Firewall Zc Firewall Zc IPSec Key Inbound P	ones one Security Policies Rotation ort Forwarding	Loopback Inte Loopback Orce Virtual Tunne DHCP Server DHCP Leases	erfaces chestration I Interfaces (VTI) Defaults	Optimiza SaaS NA ACLs Access L Shaping	tion Policies T Policies ists	
Advanced	Security Settings	DHCP Failove	r State	Shaper		
SSL Certifi SSL CA Ce SSL for Sa	cates rtificates aS	Routes Regional Rou BGP BGP ASN Poo	ting	Application User Det SaaS Op Applicati	ns & SaaS ined Applications timization on Definitions	
Discovery Discovered Preconfigu Configurat	d Appliances iration ion Wizard	OSPF Multicast Peer Priority	~	Applicati TCAs Thresho IP SLA	on Groups d Crossing Alerts	
Licensing Licenses	-1	Management	Routes			
Cloud Port	a	Tunnels Tunnel Group Auto MTU Dis Tunnel Excep	is scovery tion			

Figure 75. Configure IP SLA

Edit EdgeConnect IPSLA Rules

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

Search tags, appliances	Da	shboard Zscale	Internet Access	Business	Intent Overlays Tunnels IP SLA ×
 Zscaler Fabric 3 Branch 2 	Expo	rt C 3 mins			
 HA SanJose1 HA SanJose2 Hub 1 	17 F	LA 🕜 Rows, 1 Selected			
C-V-AWS1	Edit	Appliance Name 🔺	Active	State	Monitor
	1	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
	1	EC-V-AWS1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
	· DA	-A-WAADT	165	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
	/ Sa	anJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold
-	1	-**		Down	VRRP: Interface = lan0, Interval= 1
	1	SanJose1	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold

Figure 76. Edit the IP SLA rule

Add Rule and Target

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

IP	SLA -	SanJos	e 1		
IP	SLA 🌔	2			
	Add				
	Edit	Activ	State	Monitor	Down Action
		Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter-	Tunnel Down: Tunnel = Passthro
		Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
		Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
		Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
		Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
		Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold = 5, Down Threshold = 5, Inter	Tunnel Down: Tunnel = Passthro
	1	Yes	Down	VRRP: Interface = Ian0, Interval= 1	Modify Subnet Metric: Delta= 10

Figure 77. Add rule and target

Configure IP SLA Rule

lΞ

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 <u>Monitoring GRE Tunnels</u> (government agencies, see <u>Monitoring GRE Tunnels</u>) section for details.</cloud></cloud>
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.

lonitor	ON OFF	
Monitor	HTTP/HTTPS	Γ
URL(s)	http://gateway.zscalerbeta.net/vpntest	
Proxy Address	optional	-tə
		(06535)
User Agent	optional	
HTTP Request Timeout	2	Sec
Medium	Tunnel	1
Tunnel	ZS-GRE1	1
Source Interface	Loopback	1
Keep Alive Interval	5	Sec
Sampling Window Reachability	300	Sec
Mark Up after X Succeed	2	
Mark Down after X Failed	3	
Loss		
Mark Up after loss below X %	0	
Mark Down after loss above X %	0	
Latency	0	MIII Con
Mark Up after average latency below X	0	Milli Sec
Matria Combineties	OP -	I Pilli Sec
Meniter Compliant Interval	CR	Sec
Monitor sampling Interval	00	380
ctions		-
Down Action	Disable Tunnel	1
Tunnel	ZS-GRE1	1
Up Action	Enable Tunnel	
Tunnel	ZS-GRE1	

Verify IP SLA Rule

2 A ret Sankosel	IP SLA 🔞										
Sandose2	18 Ross Search										
CO BC/V AWS1	Edit Applance Name	Active	State	Honitor	DOM.,	Up Action	Comment	Up Stats	Down Stats		
	✓ 80.9.30801	Ves	Up	Fing: Kosy Alos Time = 1, 29 = sp-ipsia.shterpeak.cloud,8.8.8.8, 10 Treated =	Tunnal I	Tunnel Lip: Tunnel - Passthrough	generaled by overlay a	nar Lastrik Sh Zey 40a	Total 13, Last23d Sh-		
	✓ EC-V-AWS1	Yes .	Up	Ping: Keep Alve Time = 1, IP = sp-ipsia.silverpeak.cloud,8.8.8.8, Up Threshold =	Tured I	Tunnel Up: Tunnel - Passthroug	generalied by overlay a	nex Last:3d 3h 7m 49s	Total : 1, Last:3d 3%.		
	# BOW-AWSI	Yest	Up	Ping: Keep Also Time = 1, $P = sp-ipsia.shverpeak.cloud,8.8.8.8, Up Threshold =$	Tynnell	Tunnei Up: Tunnel - Pesetbrough	generated by overlay a	nar Last:34 35 7m 40s	Total : 3, Last:3d Str.		
	✓ Sanlosei	Yes .	Ψp	Ping: Keep Alve Time = 1, IP = sp-ipsia silverpeak.cloud,8.8.8.8, Up Threshold =	Tannel I	Tunnel Up: Tunnel - Passtbrough	generaled by overlay a	ner Lasträd 2h-45in 54s	Totof 11, Last 34 2h		
	/ Seriousi	Yes	Down	VBRP: Interface = kanD, Internal= 1	Hodity :	Subnet Action: Default	edgeha	Last:3d 2h 52m 13s	Total :2, Last:3d 2h		
	✓ SavJosei	Yes .	Up	Prog. Keep New Time = 1, IP = sp-ipsla.sheepeak.cloud,8.8.8.8, Up Threshold =	Turnet	Turnel Up: Turnel - Pasthrough	generated by overlay a	nox Lasti3d 2h-45in 54s	Yold 11, Last 34 25		
	/ Satisal	Yes	Up	Ping: Keep Alive Time = 1, IP = sp-ipsia.shverpeak.cloud,8.8.8.8, Up Threshold =	Tunnel (Tunnel Up: Tunnel = Paesthrough	generated by overlay a	ner Last:3d 3h lim 41s	Total :0, Last:0		
	✓ SarJoset	Yes	Up	Prog: Keep Alve Time = 1, IP = sp-ipsla.silverpeak.cloud,8.8.8.8, Up Threshold =	Taneal I	Tunnel Up: Tunnel - Passtbroug	generated by overlay r	nai Lasti 34 2h 45in 54s	Total 1, Last M 2h.		
	/ Sational	Ven.	Up	Prog: Keep Nive Time = 1, IP = sp-ipsia.silverpeak.cloud,8.8.8.8, Up Threshold =	Tunnel	Tunnel Up: Tunnel - Pasethrough	generated by overlay a	nee Last:3d 3h im 4is	Total :0, Last:0		
	✓ Sauloset	Yes	Up	Ping: Keep Alve Time = 1, IP - sp-ipsla.silverpeak.cloud,8.8.8.8, Up Time/rold =	Tintel	Tunnel Up: Tunnel - Passthrough	generated by overlay r	na Last 34 3h tin 41s	Total 10, Laston		
SanJose1	Yes	Up	HTTP/HTTP	5: URL = http://gateway.zscalerbeta.net/vpntest, HTTP Request Ti	meo Tu	nnel I, Tunnel Up: Tunnel -	ZS-GRE1		Last:1m 32s	Total :0, Las	
	✓ SatUre2	Yes	Up	Ping: Keep Also Time = 1, IP = sp-ipsia silverpaak.cloud,8.8.8.8, Up Threshold =	Turnel I	Turnel Up: Tunnel - Passthrough	generated by overlay a	NOT LANE 34 27- 50 yr 164	Total 10, Laston		

Figure 79. Verify the IP SLA Rule

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

Appendix C: Checking Tunnel Status in ZIA Admin Portal

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

	REPORTING	Cf Start Over 🤇	Tunnel Insight	IS NEW			0
ZIA	Security Policy Audit Report		Overall Traffic	•			
2	SaaS Assets Summary Report	×					
Dashboard	SaaS Assets Report 1000	· · · · · · · · · · ·	39.1 KB				
Analytics	Saas Security Posture Report 1999	•	29.3 KB -				
Policy	Web Insidhts						
•:	Mobile Insights	× .	19.5 KB -				
Administration	Tunnel Insights						
Activation	SaaS Security Insights		9.8 KB -				
Q Search						1	
			4/11 12:00 AM	4/11 4:00 AM	4/11 8:00 AM	4/11 12:00 PM	4/11 411 4:00 PM 510 PM
٠			Total				
-			1 ×				
0			< M				
+			10000				Help
Copyright	2007-2021 Zscaler Inc. All rights reserved.	Version 6.1 Patent			Weblog Time: 4/11/202	21 5:52:40 PM Last Upda	ted: 4/11/2021 5:52:41 PM

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**.

۲	Insights Logs C ^e Start Over	Tunnel Insight	S ^{NEW}				0
ZIA	Timeframe	Overall Traffic					
Cashboard	Current Day: 4/11/2021.	^{391 КВ} Г					
Analytics	Select Chart Type						-
Policy	Metrics	29.3 KB					
¢° Administration	Sent Bytes 🗸	19.5 KB —					
(1) Activation	Select Fiters Add Fiter	9.8 KB —					
Q Search	Apply Filters						
		4/11 12:00 AM	4/11 4:00 AM	4/11 8:00 AM	4/11 12:00 PM	4/11 4:00 PM	475. 1.00 PM
•		Total					
• •			2			G	Help



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

Tunnel Logging

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



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 <u>ZIA Tunnel Insights Logs: Columns</u> (government agencies, see <u>ZIA Tunnel Insights Logs: Columns</u>).

Appendix D: Deriving the Zscaler IPSec VPN VIP

You can find Zscaler public IP endpoints on the <u>Cloud Enforcement Node Ranges</u> page (government agencies, see <u>Cloud</u> <u>Enforcement Node Ranges</u>). 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.

- When you go to the <u>Cloud Enforcement Node Ranges</u> page (government agencies, see <u>Cloud Enforcement Node</u> <u>Ranges</u>) 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

	ZIA						
ilter By Configuration	Cloud zscalerone.net Customer ranges. A zscalertwo.net	vforcement Nodes es may result in a	in their environment: you may need loss of service.	I to take into account additional address	a ranges not represented he	re. Customers should ensure that acces	s is permitted to data center IP
ECTIONS	Zscaler zscloud.net	a Centers (7)					
Cloud Enforcement Node Ranges	We advise zscalerbeta.net for 60 day zscalergov.net	the Zscaler Egress cy. Please refer to	IP Ranges and Future Data Centers changelog for published dates of th	s Section to your access lists, firewalls a ne ranges listed below.	nd application white lists. T	The IPs from these ranges can become li	e at any time after being publish
Firewall Config. Requirements	ZPA Enture f						O Correl
entral Authority IP Addresses	private.zscaler.com						Br copy .
AC IP Addresses	185.46 zpagov.net	104	4.129.192.0/20	165.225.0.0/17		165.225.192.0/18	
rivate ZEN Requirements	ZDX 147.161	136	5.226.0.0/16	137.83.128.0/18			
ISS Configuration	zdxcloud.net						
AB Configuration	Current Data Centers						
rirtual ZEN Requirements	🖾 Regular Location 😾 🛶 Regio	nal Surcharge			Auto Geo	Proximity Enabled S Not Ready for	Jse O Do Not Provision
ULP ICAP Requirements							
scaler Client Connector	Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	SVPN Virtual IP	VPN Host Name	Notes
rivate Nanolog Firewall scaler Index Tool Requirements	v EMEA 🚺 Copy I	Ps					
IA Virtual Service Edge	Abu Dhabi I	147.161.174.0/23					S Not Ready for Use
IA Service Edge	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	
JLP Incident Receiver	Amsterdam II	185.46.212.0/23	@ams2.sme.zscaler.net	185.46.212.32		amsterdam2-vpn.zscaler.net	
SUPPORT	Amsterdam II	147.161.172.0/23					Not Ready for Use
Changelog	Brussels	165.225.88.0/23	bru1.sme.zscaler.net	() 165.225.88.32		bru1-vpn.zscaler.net	Do Not Provision
			1997	107 007 10 10		The American Street	
Customer Support	Brussels II	165.225.12.0/23	Ø bruZ.sme.zscaler.net	100.220.12.12	100.220.12.00	bruz-vpn.zscaler.net	

Figure 83. Zscaler public IP reference

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

dig ams2-2-vpn.zscaler.net

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

- ;; global options: +cmd
- ;; Got answer:
- ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38701
- ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

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

;; QUESTION SECTION:

;ams2-2-vpn.zscaler.net. IN A

;; ANSWER SECTION:

ams2-2-vpn.zscaler.net. 1800 IN A 165.225.240.18

;; Query time: 50 msec

;; SERVER: 192.168.83.35#53(192.168.83.35)

;; WHEN: Thu Mar 25 22:32:28 PDT 2021

;; MSG SIZE rcvd: 67

Appendix E: Requesting Zscaler Support

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

To contact Zscaler Support:

1. Go to Administration > Settings > Company profile.



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

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



Figure 85. Save your company ID information

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



Figure 86. Submit a ticket

Adding Domain (Example)

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

omit a case					
Subject Adding Domain					
Zscaler Company 1 zscalerbeta.net-XXX	D KXXX				
Product		* Priority		* Case Type	
ZIA		Medium (P3)		Provisionina	*
,			Please enter numb	per with country code (Ex:	+1)
Description					
Description	f <u>romscm</u> .com) t	o my ZIA instance.			
Please add (<u>domain</u> Thanks, Paul					
Please add (<u>domain</u> Thanks, Paul					
Please add (<u>domain</u> Thanks, Paul					

Figure 87. Adding a domain