<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terms and Acronyms</td>
</tr>
<tr>
<td>About This Document</td>
</tr>
<tr>
<td>Zscaler Overview</td>
</tr>
<tr>
<td>Zscaler Resources</td>
</tr>
<tr>
<td>Aruba Overview</td>
</tr>
<tr>
<td>Aruba Resources</td>
</tr>
<tr>
<td>Audience</td>
</tr>
<tr>
<td>Software Versions</td>
</tr>
<tr>
<td>Request for Comments</td>
</tr>
<tr>
<td>Prerequisites</td>
</tr>
<tr>
<td>ZIA</td>
</tr>
<tr>
<td>Silver Peak Orchestrator</td>
</tr>
<tr>
<td>Configuring ZIA</td>
</tr>
<tr>
<td>Logging into ZIA</td>
</tr>
<tr>
<td>Configure ZIA for API Access</td>
</tr>
<tr>
<td>Adding SD-WAN Partner Key</td>
</tr>
<tr>
<td>Verify SD-WAN Partner Key</td>
</tr>
<tr>
<td>Adding a Partner Administrator Role</td>
</tr>
<tr>
<td>Creating Partner Administrator Role</td>
</tr>
<tr>
<td>Administrator Management</td>
</tr>
<tr>
<td>Add Partner Administrator</td>
</tr>
<tr>
<td>Creating Partner Administrator</td>
</tr>
<tr>
<td>Activate Pending Changes</td>
</tr>
<tr>
<td>Verify Activation</td>
</tr>
</tbody>
</table>
Configuring Automated IPSec Tunnels

Log into Aruba Orchestrator
Configure Cloud Services
Validate that the Desired Interface Labels are Selected
Configure IPSec for IKEv2
Configuring a ZIA Subscription
Configuring ZIA API Credentials and Zscaler Cloud
Verify ZIA Account Update
Configuring Business Intent Overlays
Enabling Zscaler for Breakout Traffic
Configuring Preferred Policy Order
Apply Overlay Changes
Verifying Automated Tunnel Establishment
View Automated Tunnel Details

Configuring Sub-Locations and Gateway Options

Configure Sub-location
Enable Gateway Option Orchestration
Add Sub-Location
Configure Gateway Options
Set Gateway Options
Change Gateway Options Confirmation
Verify Gateway Options
Verify Sub-Locations in ZIA

Configuring Layer-7 Health Checks for Automated Tunnels

Configuring Zscaler IP SLA
Enable the IP SLA Probes for the Zscaler Tunnels
Verify Zscaler IP SLA Rules 30
   Navigate to the IP SLA tab 30
   Validate the Health Checks in the IP SLA Tab 30

Appendix A: Manual Tunnel Configuration 31
   Configuring Static IPs and GRE Tunnels 31
      Add a Static IP Configuration 31
      Add a GRE Tunnel Configuration 34
      Activate and Verify all Configuration Changes 36
   Adding VPN Credentials for Manual IPSec Tunnels 37
      Navigate to VPN Credentials 37
      Add a VPN Credential 38
      Enter VPN Credential Data 38
      Verify VPN Credential 38
      Activate Pending Changes 39
      Verify the Activation 39
   Configuring a Location for Manual Tunnels 40
      Add a Location 40
      Enter the Location Data 41
      Confirm Changes Have Been Saved 42
      Activate Pending Changes 42
      Activation Confirmation 43
   Manually Configure Tunnels on Aruba Orchestrator 43

Appendix B: Configuring Layer-7 Health Checks for Manually Created Tunnels 44
   Configuring Aruba SD-WAN IP SLA 44
   Edit EdgeConnect IPSLA Rules 44
   Add Rule and Target 45
   Configure IP SLA Rule 45
   Verify IP SLA Rule 46
Appendix C: Checking Tunnel Status in ZIA Admin Portal 47

Tunnel Data Visualization 47
Tunnel Logging 48

Appendix D: Deriving the Zcaler IPSec VPN VIP 49

Appendix E: Requesting Zcaler Support 51

Gather Support Information 51
  Obtain Company ID 51
  Save Company ID 51
  Enter Support Section 52
Adding Domain (Example) 53
## Terms and Acronyms

The following terms and acronyms are used in this document.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC 2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC 2409)</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security (RFC 2411)</td>
</tr>
<tr>
<td>OAM</td>
<td>Operation, Administration, and Management</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>Software Defined Wide Area Network</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (RFC 6101)</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security (RFC 5246)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC 7239)</td>
</tr>
<tr>
<td>ZAPP</td>
<td>Zscaler End-point Client Application</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
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. For more information on Zscaler, Go to the Zscaler website or follow Zscaler on Twitter @zscaler.

Zscaler Resources

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
<tr>
<td>ZIA Overview</td>
<td>Overview of ZIA and ZIA resources.</td>
</tr>
<tr>
<td>ZIA Test Page</td>
<td>Verifies whether your internet access is secured by Zscaler services, and which Zscaler data center used by the customer.</td>
</tr>
<tr>
<td>Zscaler IP Page</td>
<td>Displays configuration parameters for Zscaler ZIA and ZPA.</td>
</tr>
</tbody>
</table>

Aruba Overview

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

Aruba Resources

The following table contains links to Aruba support resources.

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

### 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:

- Appendix E: Requesting Zscaler Support
- Zscaler Resources
- Aruba Resources

### Software Versions

This document was written using:

- Zscaler Internet Access v6.1
- Aruba Orchestrator v8.10.15.40131
- Aruba EdgeConnect v8.3.3.1_85995

### Request for Comments

- **For Prospects and Customers:** We value reader opinions and experiences. Please contact us at 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.

### 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, as shown in Figure 1.

If you are unable to log in using your administrator account, contact support.
Configure ZIA for API Access

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

Navigate to Administration > Cloud Configuration > Partner Integrations.

Adding SD-WAN Partner Key

In the Partner Integration section of the ZIA Admin Portal:

1. Select SD-WAN > Add Partner Key.
2. The **Add Partner Key** dialog appears. On the right side of the window, type in or select the SD-WAN vendor from the drop-down menu.

3. Click **Generate**. You are returned to the prior screen.

![Add Partner Key](image)

**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.)

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

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

![Partner Integrations](image)

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

---

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

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

Navigate to Administration > Authentication > Role Management.

Creating Partner Administrator Role

Complete the following steps:

1. Click the Add Partner Administrator Role.

   ![Add Partner Administrator Role](image)

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

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**.
Add Partner Administrator

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

**Figure 10. Add Partner Administrator**

Creating Partner Administrator

1. In the Add Partner Administrator input box, fill in:
   - A Login ID
   - An Email
   - A Partner Role

2. Set the Status to Enabled.

3. Click Save.

**Figure 11. Creating a partner administrator**

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

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

![Activate pending changes](image1)

Verify Activation

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

![Verify activation](image2)
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.

![Image](example-of-an-aruba-orchestrator-dashboard.png)

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.

![Image](aruba-orchestrator-login-page.png)

Figure 15. Aruba Orchestrator login page
Configure Cloud Services

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

Validate that the Desired Interface Labels are Selected

1. Ensure that you have the proper interface labels chosen to source tunnels from. In the Zcaler Internet Access tab, click Interface Labels.
2. Validate that the correct Interface Labels are assigned as Primary and Backup sources for tunnel establishment to the ZIA endpoints.

3. Click **Save**.

**Build Tunnels Using These Interfaces**

4. Drag the interface labels from the right to the left if required. Tunnels built to the ZIA Public Service Edges use these interfaces.

5. Click **Yes** to apply your changes.

**Change Interfaces**

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

**Figure 18. Choose interfaces for tunnel creation**

**Figure 19. Apply the tunnel setting to interfaces**
Configure IPSec for IKEv2

IKEv2 is the recommended Phase-1 negotiation protocol for Zscaler.

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

![Tunnel Setting window](image)

Figure 20. Open the Tunnel Settings window

2. In the Tunnel Setting window, click the IKE tab and change the IKE Version to IKE v2.
3. Click Save.

![Configure IKE v2 for IPSec tunnels](image)

Figure 21. Configure IKE v2 for IPSec tunnels
Configuring a ZIA Subscription

Select the Subscription tab.

Figure 22. Configuring a ZIA subscription

Configuring ZIA API Credentials and Zscaler Cloud

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

Figure 23. Configuring API credentials

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

Click Save to refresh the screen.
Verify ZIA Account Update

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

![Figure 24. Verifying a ZIA account update](image)

Configuring Business Intent Overlays

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

![Figure 25. Configuring business intent overlays](image)
Enabling Zscaler for Breakout Traffic

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

![Figure 26. Enabling Zscaler for breakout traffic](image)

Configuring Preferred Policy Order

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

![Figure 27. Configuring preferred policy order](image)
Apply Overlay Changes

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

![Figure 28. Save and apply changes](image)

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

![Figure 29. Confirm changes](image)

Verifying Automated Tunnel Establishment

After selecting Save in the preceding step, 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, you should see the Deployed tunnels in highlighted in green.

![Figure 30. Verify automated tunnel establishment](image)
View Automated Tunnel Details

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

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

Figure 31. View automated tunnel details
Configuring Sub-Locations and Gateway Options

If you are new to Zscaler sub-locations, review the ZIA About Sublocations help.

Configure Sub-location

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

![Configure sub-location](image)

Enable Gateway Option Orchestration

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

![Enable gateway options](image)

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

![Enable gateway option orchestration](image)
Add Sub-Location

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

1. The Rule Name, which is used only by Aruba Orchestrator. This is not the name of the sub-location that appears in ZIA.
2. Select the EdgeConnect Appliances and Location Label that should be matched for this sub-location. Most deployments use “Any” for both appliances and location labels.
3. Configure the sub-location Name (e.g., Guest Wi-Fi) and the subnets that this gateway should match. 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 should match an EdgeConnect interface label as configured in the Deployment screen of an EdgeConnect appliance.
4. Click Save.

Configure Gateway Options

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

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.

Figure 37. Set gateway options

Change Gateway Options Confirmation

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

Figure 38. Change gateway options confirmation
Verify Gateway Options

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

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

---

Verify Sub-Locations in ZIA

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

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

---

**Figure 39. Verify gateway options**

**Figure 40. 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.

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.
**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**.

![Navigate to IP SLA settings](image)

**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.

![Verify the IP SLA rule](image)

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.

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.

![Figure 47. Entering the static IP](image)

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 48. Verifying geospatial information](image)

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](image)

Figure 49. 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.

![Static IPs & GRE Tunnels](image)

Figure 50. Validate that the static IP was saved

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

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

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

Figure 51. Navigate to the GRE tunnel configuration screen

Assign the Source IP to the Tunnel

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

Figure 52. 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.

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.
Save Tunnel Configuration

Review the configuration and click **Save**.

![Add GRE Tunnel Configuration](image)

**Figure 55. Review and save the tunnel setup**

Activate and Verify all Configuration Changes

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

![Activate GRE Tunnel Configuration](image)

**Figure 56. Activate the GRE tunnel configuration**
The message **Activation Completed!** appears to indicate that your changes are live.

![Activation Completed](image1.png)

Figure 57. 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**.

![VPN Credentials](image2.png)

Figure 58. 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.

![Figure 59. Adding a VPN credential](image)

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

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

![Figure 60. Enter VPN credential data](image)

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. Below the message, you see the VPN credential that you created.

![Figure 61. Verify location information and save](image)
Activate Pending Changes

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

Verify the Activation

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

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

Figure 62. Activate pending changes

Figure 63. Verify the activation
Configuring a Location for Manual Tunnels

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

Navigate to Administration > Resources > Location Management.

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.
**Enter the Location Data**

Complete the fields.

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

![Figure 66. Enter the location data](image)

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

**Add Static IP and GRE Tunnel to Location**

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

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

![Figure 67. Select the static IP linked to the location](image)
Adding a VPN Credential to a Location

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

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

![Figure 68. Add VPN credential to location and save](image)

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. Below this, you should see the location you created.

![Figure 69. Confirm the changes have been saved](image)

Activate Pending Changes

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

![Figure 70. Activate changes](image)

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 should take effect within seconds.

Figure 71. Activation confirmation

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

Manually Configure Tunnels on Aruba Orchestrator

Refer to [Aruba Resources](#) 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.

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.
Add Rule and Target

Click Add to create a new HTTP and HTTPS rule.

Configure IP SLA Rule

Configure the IP SLA rule as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL(s)</td>
<td><a href="http://gateway">http://gateway</a>.&lt;cloud&gt;.net/vpntest</td>
</tr>
<tr>
<td></td>
<td>replace &lt;cloud&gt; with your ZIA tenant cloud. Refer to the Monitoring GRE Tunnels section for details.</td>
</tr>
<tr>
<td>HTTP Request Timeout</td>
<td>2 seconds</td>
</tr>
<tr>
<td></td>
<td>Tunnel</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Choose the GRE tunnel that you want to monitor</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Choose the Loopback interface</td>
</tr>
<tr>
<td>Keep Alive Interval</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Down Action</td>
<td>Disable Tunnel</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Tunnel from the Medium field</td>
</tr>
<tr>
<td>Up Action</td>
<td>Enable Tunnel</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Tunnel from the Medium field</td>
</tr>
<tr>
<td>Down Action</td>
<td>Disable Tunnel</td>
</tr>
</tbody>
</table>

Request Timeout and Keep Alive Interval are recommendations. Tuning these values might be required, depending on your deployment.
You can also search a specific tenant cloud to see only Zscaler health checks.
Appendix C: Checking Tunnel Status in ZIA Admin Portal

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

Navigate to Analytics > Insights > Tunnel Insights.

![Tunnel Insights](image)

Figure 77. 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.

![Insights](image)

Figure 78. ZIA Tunnel insight charts

For further information, refer to the ZIA tunnel insights help.
Tunnel Logging

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

From the Logs window, you can filter and change the time frame for the tunnels and sites that you want to investigate. See the *ZIA Tunnel Insights Logs: Columns* help for details on the options.
Appendix D: Deriving the Zscaler IPSec VPN VIP

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

1. When you go to the Cloud Enforcement Node Ranges page 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.

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

This appendix describes how to contact your Zscaler support team.

Gather Support Information

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, year-round.

Obtain Company ID

Zscaler Support needs you to provide your Company ID. The company ID is how Zscaler uniquely identifies each customer. Navigate to Administration > Settings > Company profile.

Save Company ID

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

Figure 81. Collecting details to open support case with Zscaler TAC

Figure 82. Save your company ID information
Enter Support Section

Navigate to ? > Support > Submit a Ticket. Alternatively, you can go directly to the Submit Ticket page.

Figure 83. 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.

![Image](image_url)

Figure 84. Adding a domain