## Table of Contents

1  **Zscaler and Aruba SD-WAN** .......................................................... 11  
   1.1  **Prerequisites** ........................................................................... 11

2  **Configuring Zscaler Internet Access (ZIA)** ................................. 12  
   2.1  **Configuring Zscaler Internet Access** ....................................... 12  
      2.1.1  Logging into ZIA ................................................................. 12
   2.2  **Configure ZIA for API Access** .................................................. 13  
      2.2.1  Adding SD-WAN Partner Key ........................................... 14  
      2.2.2  Verify SD-WAN Partner Key ............................................ 16
      2.2.3  Creating Partner Administrator Role ................................. 18
      2.2.4  Administrator Management ............................................. 20
      2.2.5  Add Partner Administrator ............................................... 21
      2.2.6  Creating Partner Administrator ........................................ 22
      2.2.7  Active Pending Changes .................................................. 23
      2.2.8  Verify Activation .............................................................. 24

3  **Configuring Automated IPsec Tunnels** ....................................... 25  
   3.1  Log into Aruba Orchestrator ..................................................... 26
   3.2  **Configure Cloud Services** ...................................................... 27
   3.3  **Validate the desired Interface Labels are Selected** ................. 28
   3.4  **Configure IPsec for IKE v2** .................................................. 31
   3.5  **Configuring ZIA Subscription** .............................................. 33
   3.6  **Configuring ZIA API Credentials and Zscaler Cloud** ............ 34
   3.7  **Verify ZIA Account Update** ................................................ 35
   3.8  **Configuring Business Intent Overlays** .................................. 36
   3.9  **Enabling Zscaler for Breakout Traffic** ................................ 37
   3.10  **Configuring Preferred Policy Order** .................................... 38
   3.11  **Apply Overlay Changes** ..................................................... 39
   3.12  **Verifying Automated Tunnel Establishment** ......................... 40
   3.13  **View Automated Tunnel Details** ......................................... 41

4  **Configuring Sub-locations and Gateway Options** ....................... 42  
   4.1  **Configure Sub-location** ....................................................... 42
   4.2  **Enable Gateway Option Orchestration** .................................. 43
   4.3  **Add Sub-location** ............................................................. 44
   4.4  **Configure Gateway Options** ................................................ 45
   4.5  **Set Gateway Options** ......................................................... 46
   4.6  **Change Gateway Options Confirmation** ............................... 47
   4.7  **Verify Gateway Options** .................................................... 48
   4.8  **Verify Sub-locations in ZIA** ................................................ 49

5  **Configuring Layer-7 Health Checks for Automated Tunnels** .......... 51  
   5.1  **Configuring Zscaler IP SLA** ............................................... 51
   5.2  **Enable the IP SLA probes for the Zscaler Tunnels** ................. 52
   5.3  **Verify Zscaler IP SLA rules** ............................................... 53
      5.3.1  Navigate to the IP SLA tab ............................................... 53
      5.3.2  Validate the Health Checks in the IP SLA Tab .................... 54
6  Appendix A: Manual Tunnel Configuration .................................................................55
6.1  Configuring Static IP’s and GRE Tunnels .............................................................55
6.1.1  Add a Static IP Configuration .........................................................................56
6.1.1.1  Enter the Static IP ..................................................................................56
6.1.1.2  Verify Geospatial data ...........................................................................57
6.1.1.3  Review Information and Save ...................................................................58
6.1.1.4  Validate Static IP Configuration is Saved ...............................................59
6.1.2  Add a GRE Tunnel Configuration ....................................................................60
6.1.2.1  Assign the Source IP to the Tunnel .........................................................61
6.1.2.2  Choose Data Centers for Tunnel Termination .......................................62
6.1.2.3  Select GRE Tunnel Internal IP Subnet .....................................................63
6.1.2.4  Save Tunnel Configuration ......................................................................64
6.1.3  Activate and Verify all Configuration Changes ..............................................65
6.2  Adding VPN Credentials for manual IPsec tunnels ............................................67
6.2.1  Navigate to VPN Credentials .........................................................................67
6.2.2  Add a VPN Credential ...............................................................................68
6.2.3  Enter VPN Credential Data ..........................................................................69
6.2.4  Verify VPN Credential................................................................................70
6.2.5  Activate Pending Changes ...........................................................................71
6.2.6  Verify Activation ..........................................................................................72
6.3  Configuring a Location for Manual Tunnels .........................................................73
6.3.1  Add a Location.............................................................................................74
6.3.2  Enter Location Data .....................................................................................75
6.3.2.1  Add Static IP / GRE Tunnel to Location ...............................................76
6.3.2.2  Adding a VPN Credential to a Location ...............................................77
6.3.3  Confirm Changes Have Been Saved .............................................................78
6.3.4  Activate Pending Changes ..........................................................................79
6.3.5  Activation Confirmation ..............................................................................80
6.4  Manually Configure Tunnels on Aruba Orchestrator ...........................................80
7  Appendix B: Configuring Layer-7 Health Checks for manually created tunnels ....81
7.1  Configuring Aruba SD-WAN IP SLA .................................................................81
7.2  Edit Edge Connect IPSLA rules ......................................................................82
7.3  Add Rule and Target .......................................................................................82
7.4  Configure IP SLA Rule ....................................................................................83
7.5  Verify IP SLA Rule ..........................................................................................85
8  Appendix C: Checking tunnel status in ZIA Admin .................................................86
8.1  Tunnel Data Visualization ...............................................................................87
8.2  Tunnel Logging ...............................................................................................88
9  Appendix D: Deriving the Zscaler IPSEC VPN VIP ...............................................89
10 Appendix E: Requesting Zscaler Support ...............................................................91
10.1  Gather Support Information ..........................................................................91
10.1.1  Obtain Company ID ..................................................................................91
10.1.2  Save Company ID .....................................................................................92
10.1.3  Open Support Ticket ..................................................................................93
10.2  Adding Domain (Example) ............................................................................94
# Table of Figures

Figure 2.1.1-A: Log into Zscaler ................................................................. 12  
Figure 2.2-A: Configuring ZIA for API Access ........................................... 13  
Figure 2.2.1-A: Add Partner Key .............................................................. 14  
Figure 2.2.1-B: Add SD-WAN Partner Key ................................................. 15  
Figure 2.2.2-A: Verify SD-WAN Partner Key ............................................. 16  
Figure 2.2.2-B: Adding Partner Administrator Role .................................... 17  
Figure 2.2.3-A: Add Partner Administrator Role ....................................... 18  
Figure 2.2.3-B: Creating Partner Administrator Role ................................... 19  
Figure 2.2.4-A: Administrator Management ............................................. 20  
Figure 2.2.5-A: Admin Partner Administrator .......................................... 21  
Figure 2.2.6-A: Creating Partner Administrator ....................................... 22  
Figure 2.2.7-A: Activate Pending Changes .............................................. 23  
Figure 2.2.8-A: Verify Activation ............................................................ 24  
Figure 3-A: Example Dashboard of Aruba Orchestrator .............................. 25  
Figure 3.1-A: Aruba Orchestrator Login Page ......................................... 26  
Figure 3.2-A: Configuring Cloud Services ................................................ 27  
Figure 3.3-A: Interface Labels .................................................................. 28  
Figure 3.3.1-A: Choose interfaces for tunnel creation ............................. 29  
Figure 3.3.2-A: Apply tunnel setting to interfaces .................................... 30  
Figure 3.4-A: Open Tunnel Settings dialog ............................................. 31  
Figure 3.4-B: Configure IKE v2 for IPsec tunnels .................................... 32  
Figure 3.5-A: Configuring ZIA Subscription ............................................. 33  
Figure 3.6-A: Configuring API Credentials ............................................. 34  
Figure 3.7-A: Verifying ZIA Account Update .......................................... 35  
Figure 3.8-A: Configuring Business Intent Overlays ............................... 36  
Figure 3.9-A: Enabling Zscaler for Breakout Traffic ............................... 37  
Figure 3.10-A: Configuring Preferred Policy Order ................................. 38  
Figure 3.11-A: Save and Apply Changes .................................................. 39  
Figure 3.11-B: Confirm Changes ............................................................. 39  
Figure 3.12-A: Verify Automated Tunnel Establishment ........................... 40  
Figure 3.13-A: View Automated Tunnel Details ...................................... 41  
Figure 4.1-A: Configure Sub-location ...................................................... 42  
Figure 4.2-A: Enable Gateway Options ................................................... 43  
Figure 4.2-B: Enable Gateway Option Orchestration ................................ 43  
Figure 4.3-A: Add Sub-location ............................................................... 44  
Figure 4.4-A: Configure Gateway Options ............................................ 45  
Figure 4.5-A: Set Gateway Options .......................................................... 46  
Figure 4.6-A: Change Gateway Options Confirmation ............................ 47
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7-A</td>
<td>A: Verify Gateway Options ........................................ 48</td>
</tr>
<tr>
<td>4.8-A</td>
<td>A: Verify Sub-locations in ZIA .................................... 50</td>
</tr>
<tr>
<td>5.1-A</td>
<td>A: Configure IP SLA ............................................... 51</td>
</tr>
<tr>
<td>5.2-A</td>
<td>A: Edit IP SLA rule .................................................. 52</td>
</tr>
<tr>
<td>5.3.1-A</td>
<td>A: Navigate to IP SLA settings .................................... 53</td>
</tr>
<tr>
<td>5.3.2-A</td>
<td>A: Verify IP SLA Rule ............................................... 54</td>
</tr>
<tr>
<td>6.1-A</td>
<td>A: Navigate to Static IPs &amp; GRE Tunnel configuration screen .. 55</td>
</tr>
<tr>
<td>6.1.1-A</td>
<td>A: Adding a Static IP ............................................... 56</td>
</tr>
<tr>
<td>6.1.1.1-A</td>
<td>A: Entering the Static IP .......................................... 56</td>
</tr>
<tr>
<td>6.1.1.2-A</td>
<td>A: Verifying Geospatial information ............................. 57</td>
</tr>
<tr>
<td>6.1.1.3-A</td>
<td>A: Review and save the Static IP ................................ 58</td>
</tr>
<tr>
<td>6.1.1.4-A</td>
<td>A: Validate the Static IP was saved ............................. 59</td>
</tr>
<tr>
<td>6.1.2-A</td>
<td>A: Navigate to the GRE Tunnel Configuration screen ........... 60</td>
</tr>
<tr>
<td>6.1.2.1-A</td>
<td>A: Choose the GRE tunnel source IP .............................. 61</td>
</tr>
<tr>
<td>6.1.2.2-A</td>
<td>A: Choose the Data Centers for tunnel termination ............ 62</td>
</tr>
<tr>
<td>6.1.2.3-A</td>
<td>A: Select the Internal GRE IP Range ............................ 63</td>
</tr>
<tr>
<td>6.1.2.4-A</td>
<td>A: Review and save the tunnel setup ............................ 64</td>
</tr>
<tr>
<td>6.1.3-A</td>
<td>A: Activate the GRE Tunnel configuration ........................ 65</td>
</tr>
<tr>
<td>6.1.3-B-A: A: Verify the GRE Tunnel configuration was Activated 66</td>
<td></td>
</tr>
<tr>
<td>6.2.1-A</td>
<td>A: Navigate to VPN Credentials .................................... 67</td>
</tr>
<tr>
<td>6.2.2-A</td>
<td>A: Adding a VPN Credential ........................................ 68</td>
</tr>
<tr>
<td>6.2.3-A</td>
<td>A: Enter VPN Credential Data ...................................... 69</td>
</tr>
<tr>
<td>6.2.4-A</td>
<td>A: Verify Location Information and Save ........................ 70</td>
</tr>
<tr>
<td>6.2.5-A</td>
<td>A: Activate Pending Changes ....................................... 71</td>
</tr>
<tr>
<td>6.2.6-A</td>
<td>A: Verify Activation .................................................. 72</td>
</tr>
<tr>
<td>6.3-A</td>
<td>A: Navigate to Locations ............................................ 73</td>
</tr>
<tr>
<td>6.3.1-A</td>
<td>A: Add a Location .................................................... 74</td>
</tr>
<tr>
<td>6.3.2-A</td>
<td>A: Enter Location Data ............................................... 75</td>
</tr>
<tr>
<td>6.3.2.1-A: A: Select the Static IP that will be linked to the Location 76</td>
<td></td>
</tr>
<tr>
<td>6.3.2.2-A</td>
<td>A: Add VPN Credential to Location and Save ................... 77</td>
</tr>
<tr>
<td>6.3.3-A</td>
<td>A: Confirm Changes Have Been Saved ............................. 78</td>
</tr>
<tr>
<td>6.3.4-A</td>
<td>A: Activate Changes .................................................. 79</td>
</tr>
<tr>
<td>6.3.5-A</td>
<td>A: Activation Confirmation .......................................... 80</td>
</tr>
<tr>
<td>7.1-A</td>
<td>A: Configure IP SLA ............................................... 81</td>
</tr>
<tr>
<td>7.2-A</td>
<td>A: Edit IP SLA rule ................................................... 82</td>
</tr>
<tr>
<td>7.3-A</td>
<td>A: Add Rule and Target .............................................. 82</td>
</tr>
<tr>
<td>7.4-A</td>
<td>A: Configure IP SLA Rule ............................................ 84</td>
</tr>
<tr>
<td>7.5-A</td>
<td>A: Verify IP SLA Rule ................................................ 85</td>
</tr>
<tr>
<td>8-A</td>
<td>A: Navigate to Tunnel Insights ..................................... 86</td>
</tr>
<tr>
<td>8.1-A</td>
<td>A: ZIA Tunnel Insight Charts ..................................... 87</td>
</tr>
<tr>
<td>8.2-A</td>
<td>A: Viewing ZIA tunnel logs ........................................ 88</td>
</tr>
</tbody>
</table>
Figure 9-A: Zscaler Public IP reference ................................................................. 89
Figure 9-B: IP address lookup ................................................................................ 90
Figure 10.1.1-A: Obtaining Company ID ................................................................. 91
Figure 10.1.2-A: Save Company ID ......................................................................... 92
Figure 10.1.3-A: Enter Support Section ................................................................. 93
Figure 10.2-A: Adding Domain Example ................................................................. 94
# Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD</td>
<td>Dead Peer Detection <em>(RFC 3706)</em></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation <em>(RFC2890)</em></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange <em>(RFC2409)</em></td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security <em>(RFC2411)</em></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 <em>(RFC6101)</em></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security <em>(RFC5246)</em></td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For <em>(RFC7239)</em></td>
</tr>
<tr>
<td>ZAPP</td>
<td>Zscaler End-point Client Application</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access <em>(Zscaler)</em></td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access <em>(Zscaler)</em></td>
</tr>
</tbody>
</table>
About This Document

Zscaler Overview

Zscaler (Nasdaq: ZS), Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to 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, please visit www.zscaler.com or follow them on Twitter @zscaler.

Aruba SD-WAN Overview

With more than 2,000 production deployments, customers have identified four unique areas of business value as the reasons 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, continuously adapts to changing business needs and network conditions. It is designed to enable enterprises to fully realize the transformational promise of the cloud. For more information on Aruba SD-WAN please visit https://www.arubanetworks.com/products/sd-wan/.
Audience

This guide is written for Zscaler Administrators, IT Administrators, and IT Analysts responsible for deploying, monitoring and managing SaaS services in an Enterprise environment. For additional product and company resources, please refer to the Appendix section.

Document Authors

This document was authored by Solution Architects in the Zscaler Business Development / Technical Alliances team (aka “BD SA”). All solutions validated within this guide have been jointly reviewed by both vendors.

Software Revisions

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 / Customers:** We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at:
  - partner-doc-support@zscaler.com

- **For Zscaler Employees:** If you are trying to reach the team that validated and authored the integrations contained within this document, please contact us at:
  - z-bd-sa@zscaler.com
1 Zscaler and Aruba SD-WAN

1.1 Prerequisites

This guide will provide GUI examples for configuring Zscaler Internet Access (ZIA) and Aruba Orchestrator. All examples in this guide presume the reader has a basic comprehension of IP Networking. All examples in this guide will explain how to provision new service with Zscaler and with Aruba SD-WAN. The prerequisites to use this guide are:

Zscaler Internet Access (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
2 Configuring Zscaler Internet Access (ZIA)

2.1 Configuring Zscaler Internet Access

In this section, we will configure the Zscaler side first before configuring Silver Peak.

2.1.1 Logging into ZIA

Log into Zscaler using your administrator account, as shown in Figure 2.1.1-A. If you are unable to log in using your administrator account, please contact support:


![Figure 2.1.1-A: Log into Zscaler](image)
2.2 Configure ZIA for API Access

The first step we need to do to enable ZIA for API access is to create a SD-WAN “Partner Key”. The Partner Key is simply an API key, which will be used as one form of authentication. The second form of authentication will be admin partner username and password, which will be explained further in this Deployment Guide. This admin credential set can only be used for API calls and will not work with the ZIA admin UI. Please follow the navigation below, which is also depicted in Figure 2.2-A.

Navigation: Administration → Cloud Configuration → Partner Integrations
2.2.1 Adding SD-WAN Partner Key

At the “Partner Integration” section of the ZIA Admin UI, please select “SD-WAN” and then “Add Partner Key”, as shown in Figure 2.2.1-A.
A window will appear, as shown in Figure 2.2.1-B. One the right side of the window, you can type in or select from the drop-down arrow on the right, which SD-WAN vendor you wish to create a Partner Key for. After typing or selection “Silver Peak”, click on “Generate”. After, you will return to the prior screen.

Figure 2.2.1-B: Add SD-WAN Partner Key
2.2.2 Verify SD-WAN Partner Key

Once you return to the screen shown in Figure 2.2.2-A, you should see the Partner Key you created for Silver Peak. *Note: The Key will not be obfuscated as is in the figure.* The password has been hidden for the purpose of this document. You should also see a red circle, with a number, above the “Activation” icon. Although we have created a Partner Key, the configuration change is pending. Only after activation the change will this configuration become active.

**Note:** The “Key” value will be required in Step 3.6. Make sure to copy it down as you will need to enter them in the Aruba Orchestrator.

---

**Figure 2.2.2-A: Verify SD-WAN Partner Key**

Key obfuscated for security

At this point, you could active the change, but we suggest you batch changes. With this said, this Deployment Guide will tell you when you should activate pending changes.
Adding a Partner Administrator Role

A Partner Admin role will need to be created so it can be assigned to the Administrator user that will be used to authenticate against the Zscaler ZIA Provisioning API.

Navigation: Administration → Authentication → Role Management

![Figure 2.2.2-B: Adding Partner Administrator Role](image-url)
2.2.3 Creating Partner Administrator Role

Clicking on the “Add Partner Administrator Role” option will bring up a window.

![Figure 2.2.3-A: Add Partner Administrator Role](image)
By creating a *Partner Administrator Role*, we can define the permission and access we wish to grant to a third-party partner, such as an SD-WAN partner. Once you name the *Partner Administrator Role*, change the Access Control to “Full”, as shown in Figure 2.1.1-A. The toggle “Full” allows partner admins to view and edit VPN credentials and Locations that Aruba Orchestrator is managing via ZIA Provisioning API. This is necessary for the Aruba Orchestrator to be able to create new VPN Credentials and Locations for branch locations. Once you have completed these steps, click “Save”. After you will be returned to the prior screen.

![Figure 2.2.3-B: Creating Partner Administrator Role](image-url)
2.2.4 Administrator Management

The last step required is creating a *Partner Administrator*. Please follow the navigation below, which is also depicted in Figure 2.2.4-A.

**Navigation:** Administration → Administration Controls → and then click Administrator Management

*Figure 2.2.4-A: Administrator Management*
2.2.5 Add Partner Administrator

Once you arrive to the “Administrator Management” page, please select “Add Partner Administrator”, as shown in Figure 2.2.5-A. A user input screen will appear, which is shown in the next section.

![Figure 2.2.5-A: Admin Partner Administrator](image)

Login ID’s obfuscated for security
2.2.6 Creating Partner Administrator

Once the “Add Partner Administrator” input box appears, fill in the fields with red boxes around them, as shown in Figure 2.2.6-A. Once this is completed, click “Save”.

**Note:** Save Email and Password settings as you will need to enter them in Aruba Orchestrator during step 3.6.

![Figure 2.2.6-A: Creating Partner Administrator](image-url)
2.2.7 Active Pending Changes

Finally, we have reached our last step in the Zscaler ZIA Admin UI. You can now navigate to “Activation” and activate the pending configurations, as shown in Figure 2.2.7-A.

![Figure 2.2.7-A: Activate Pending Changes](image-url)

Login ID obfuscated for security
2.2.8 Verify Activation

After activating pending changes, you should be returned to the prior page, and “Activation Complete” should appear in the top of the window, as shown in Figure 2.2.8-A.

![Figure 2.2.8-A: Verify Activation](image)

Login ID’s Obfuscated for security
3 Configuring Automated IPsec Tunnels

In this section, we will configure Aruba Orchestrator to provision Zscaler Internet Access. We will need the settings you were asked to save in the prior section to complete this configuration. Before we start, please take note of the Aruba Orchestrator dashboard shown in Figure 3-A. This is what a live dashboard looks like. We point this out because the screen captures taken in our lab have only two devices, and therefore less activity to report. If you would like to see more of the Aruba Orchestrator Dashboard, please contact HPE / Aruba and request a full demo.

![Figure 3-A: Example Dashboard of Aruba Orchestrator](image-url)
3.1 Log into Aruba Orchestrator

Open a web browser and enter the URL to your Aruba Orchestrator instance. When the page loads, you should see the screen in Figure 3.1-A. Please enter your Aruba Orchestrator username and password. If you are unable to log in, please email support@silver-peak.com.

Figure 3.1-A: Aruba Orchestrator Login Page
3.2 Configure Cloud Services

First we need to configure the ZIA subscription by navigating to Configuration → Cloud Services → Zscaler Internet Access.

![Figure 3.2-A: Configuring Cloud Services](image-url)
3.3 Validate the desired Interface Labels are Selected

You need to ensure that you have the proper interface labels chosen to source tunnels from. In the Zscaler Internet Access tab, click on "Interface Labels".

![Figure 3.3-A: Interface Labels]
Then validate that the correct Interface Labels are assigned as Primary and Backup source(s) for tunnel establishment to the ZIA endpoints and click “Save”.

Drag the interface labels from the right to the left if required.

These are the interfaces which tunnels will be built to the ZIA Public Service Edges.
And click “Yes” to apply your changes.

Figure 2.2.8-C: Apply tunnel setting to interfaces
3.4 Configure IPsec for IKE v2
IKEv2 is the recommended Phase-1 negotiation protocol for Zscaler currently. In the Zscaler Internet Access tab, click the “Tunnels” button. This will open a pop-up “Tunnel Setting” window.

![Open Tunnel Settings dialog](image)

*Figure 3.4-A: Open Tunnel Settings dialog*
In the pop-up window, click on the “IKE” selection and change the “IKE Version” to “IKE v2” as shown in Figure 3.4-B: Configure IKE v2 for IPsec tunnels.

Then click the “Save” button.
3.5 Configuring ZIA Subscription

Next select “Subscription” as shown in Figure 3.5-A.

![Figure 3.5-A: Configuring ZIA Subscription](image-url)
3.6 Configuring ZIA API Credentials and Zscaler Cloud

Next configure the ZIA cloud you are provisioned in and your ZIA API credentials. For large production deployments the Configuration Polling Interval setting should be left at the default of 10 minutes. This will increase the responsiveness of the API when making frequent changes to the Zscaler Cloud configuration.

![Subscription](image)

**Figure 3.6-A: Configuring API Credentials**

Note: For demonstration / POC purposes the Polling Interval can be reduced to a shorter timeframe such as 2 minutes.
3.7 Verify ZIA Account Update

After saving your ZIA settings, the screen will refresh as shown below. At the bottom of the screen, you should see a green callout that says "Update Zscaler Internet Access account successfully".

![Figure 3.7-A: Verifying ZIA Account Update](image-url)
3.8 Configuring Business Intent Overlays

Next we need to configure Business Intent Overlays. You need to navigate to: Configuration → Overlays → Business Intent Overlays.

Figure 3.8-A: Configuring Business Intent Overlays
3.9  Enabling Zscaler for Breakout Traffic

Once the screen refreshes, look for the “Breakout Traffic to Internet & Cloud Services” section. Choose the overlay that you would like to configure to use ZIA as shown in Figure 3.9-A. Then click anywhere within the red box shown below. This will then open a pop-up window with more configuration options.

![Figure 3.9-A: Enabling Zscaler for Breakout Traffic](image-url)
3.10 Configuring Preferred Policy Order

Your screen may look slightly different. The goal of this step is to configure the “Preferred Policy Order” with “Zscaler Cloud” on top. The “Zscaler Cloud” tab might be under “Available Policies”. If so, you simply need to drag this over. One you have completed this step, click “Ok”.

![Figure 3.10-A: Configuring Preferred Policy Order](image-url)
3.11 Apply Overlay Changes

You will then see the changes reflected in the Business Intent Overlays highlighted by yellow boxes, click the “Save and Apply Overlay Changes to Overlays” button.

Figure 3.11-A: Save and Apply Changes

Next you should be present a confirmation to confirm you changes. You should select “Save”.

Figure 3.11-B: Confirm Changes
3.12 Verifying Automated Tunnel Establishment

After selected “Save” in the last step, it may take 30-60 seconds until your initial tunnels are deployed. You need to navigate back to: Configuration → Cloud Services → Zscaler Internet Access, there you will see the different EdgeConnects and Interfaces provisioned.

Once IPsec tunnels start to establish, you should see “Deployed” in green, as shown below.

![Figure 3.12-A: Verify Automated Tunnel Establishment](image-url)
3.13 View Automated Tunnel Details

If you select “Tunnels” in the Zscaler Internet Access tab, you will then be brought to the Tunnels tab and see more details to each configured tunnel, such as the local IP, remote IP, tunnel mode, …etc.

Clicking the “Tunnels” selection within the Zscaler Internet Access tab will automatically put a filter in the search field to only highlight Zscaler Tunnels.

![Figure 3.13-A: View Automated Tunnel Details](image)

Login ID’s Obfuscated for security
4 Configuring Sub-Locations and Gateway Options

If you are new to Zscaler Sub-locations, we suggest you review:

https://help.zscaler.com/zia/about-sub-locations

4.1 Configure Sub-location

You need to navigate back to: Configuration → Cloud Services → Zscaler Internet Access tab, there you will see the “Gateway Options” button.

To configure a Sub-location, select “Gateway Options”.

Figure 4.1-A: Configure Sub-location
4.2 Enable Gateway Option Orchestration

If this is your first time selecting “Gateway Options”, you will need to toggle the “Orchestrate Gateway Options” slider:

![Image of Zscaler Gateway Options interface with Orchestrate Gateway Options slider highlighted.]

*Figure 4.2-A: Enable Gateway Options*

Then the following pop-up should appear. Select “Enable Gateway Orchestration” to continue.

![Image of Orchestrate Gateway Options pop-up with warning message and Enable Gateway Orchestration button highlighted.]

*Figure 4.2-B: Enable Gateway Option Orchestration*
4.3 Add Sub-location

Next select “Add”, which will open a pop-up titled “Location / Sub-location Match Criteria”. You will need to configure:

1) The “Rule Name” is only used within Aruba Orchestrator. This is not the name of the Sub-location that will appear in ZIA.

2) Select which EdgeConnect Appliances and Location Labels should be matched for this Sub-location. Most deployment will use “Any” for both Appliances and Location Label.

3) Configure the Sub-location “Name” (e.g. Guest Wifi) and the subnets to match for. The Sub-location Name will be the name used in ZIA. In most cases the Sub-Location “Name” will be the same as the “Rule Name”. The Subnets field should be configured to match a EdgeConnect interface label as configured in the Deployment screen for an EdgeConnect appliance. Figure 4.3-A shows that the “Guest” lan-side label has been selected.

4) Select “Save”.

![Figure 4.3-A: Add Sub-location](image-url)
4.4 Configure Gateway Options

Once the screen is refreshed, you should see the Sub-location you configured. To configure Gateway Options for this sub-location, click the “Gateway Options / Bandwidth” cell and a pop-up window will open.

![Gateway Options configuration](image-url)

*Figure 4.4-A: Configure Gateway Options*
4.5 Set Gateway Options

Here is where you will toggle on/off the Gateway Options to be used by this Sub-location. Note: you should not configure Gateway Options to features you do not have a ZIA subscription for. Once you have completed selecting Gateway Options, select “Save” and then click “Save” again in the main Zscaler Gateway Options window.

*Figure 4.5-A: Set Gateway Options*
4.6 Change Gateway Options Confirmation

You will be presented a confirmation window to configure the changing of Gateway Options. You need to confirm this by selecting “Change Gateway Options”.

![Change Gateway Options Confirmation](image)

*Figure 4.6-A: Change Gateway Options Confirmation*
4.7 Verify Gateway Options

After Applying the Gateway Options changes, you will then need to tick the “Show Sub-Locations” box as shown in the below figure.

We will now see the Sub-locations applies to each tunnel once the provisioning automation completes, with the selected Gateway Options configured.

![Figure 4.7-A: Verify Gateway Options](image-url)
4.8 Verify Sub-locations in ZIA

If you switch back to ZIA, you should now see the Sub-locations configured by Aruba Orchestrator. If you select on any of these Sub-locations, you will be able to view the Gateway Options configured by Aruba Orchestrator as well.

In the ZIA Admin Console navigate to: Administration → Resources → Location Management

![Locations Table]

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>IP Addresses</th>
<th>Proxy...</th>
<th>Use XF...</th>
<th>Authen...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EC-V-AWS...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>v SanJos...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.1</td>
<td>Gues...</td>
<td>192.168.203.0-...</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.2</td>
<td>other</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>v SanJos...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3.1</td>
<td>Gues...</td>
<td>192.168.203.0-...</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3.2</td>
<td>other</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>v SanJos...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4.1</td>
<td>Gues...</td>
<td>192.168.203.0-...</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4.2</td>
<td>other</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td>v SanJos...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>5.1</td>
<td>Gues...</td>
<td>192.168.203.0-...</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>5.2</td>
<td>other</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
Figure 4.8-A: Verify Sub-locations in ZIA
5 Configuring Layer-7 Health Checks for Automated Tunnels

5.1 Configuring Zscaler IP SLA

Access the IP SLA configuration in the Zscaler Internet Access Tab.

Figure 5.1-A: Configure IP SLA
5.2 Enable the IP SLA probes for the Zscaler Tunnels

In the IP SLA configuration window that appears, click the toggle to enable service health checks through the Zscaler tunnels. The default values are already aligned to Zscaler recommendations, so just click “Save”.

![Zscaler IP SLA Configuration](image)

*Figure 5.2-A: Edit IP SLA rule*

The above **Request Timeout** and **Keep Alive Interval** are recommendations. Tuning of these values may be required depending on your deployment.
5.3 Verify Zscaler IP SLA rules
When configuring tunnels manually you must also manually configure the IP SLA rules to validate the tunnel health.

5.3.1 Navigate to the IP SLA tab

Select the IP SLA option from the Configuration Menu:

Configuration → Templates and Policies → TCA → IP SLA:

![Figure 5.3.1-A: Navigate to IP SLA settings](image-url)
5.3.2 Validate the Health Checks in the IP SLA Tab

You can filter to only view the Zscaler IP SLA Probes by entering the ZIA cloud that your tenant is a member of as seen in the below figure.

![Figure 5.3.2-A: Verify IP SLA Rule](image)

You can search for your ZIA cloud to only see the Health Checks for Zscaler.
6 Appendix A: Manual Tunnel Configuration

This appendix provides the steps for configuring ZIA tunnels manually, both GRE and IPsec are covered here if your requirement are not covered by the IPSec automation.

6.1 Configuring Static IP’s and GRE Tunnels

The ZIA Admin UI now supports provisioning Static IPs for GRE Tunnels, no longer are support tickets required to setup GRE tunnels.

Navigation: Administration → Resources → Static IPs & GRE Tunnels:

![Figure 6.1-A: Navigate to Static IPs & GRE Tunnel configuration screen](image-url)
6.1.1 Add a Static IP Configuration

Click on the “Add Static IP” selection from the page:

![Static IPs & GRE Tunnels](image)

**Figure 6.1.1-A: Adding a Static IP**

6.1.1.1 Enter the Static IP

In the window the appears:
- Enter the public static IP that will initiate the tunnel connection
- Add a Description if desired

![Add Static IP Configuration](image)

**Figure 6.1.1.1-A: Entering the Static IP**

Click “Next” to continue.
6.1.1.2 Verify Geospatial data

Next, verify the Geospatial location lookup is correct for the IP address entered. If not click the “Manual” button and enter the correct location data. Then click “Next”:

![Figure 6.1.1.2-A: Verifying Geospatial information](image)

This information will be used by the ZIA Central Authority to choose the best Data Centers for tunnel termination.
6.1.1.3 Review Information and Save

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

Figure 6.1.1.3-A: Review and save the Static IP
6.1.1.4 Validate Static IP Configuration is Saved

After completing the Static IP provisioning wizard and clicking save, you should see a message appear "All changes have been saved." And the Static IP added to the list.

![Image of Static IPs configuration]

*Figure 6.1.1.4-A: Validate the Static IP was saved*

Next go onto step 6.1.2 to assign the IP to a GRE tunnel.
6.1.2 Add a GRE Tunnel Configuration

With the Static IP that has been added from section 6.1.1 we need to configure the GRE Tunnel information, click on “GRE Tunnels” and then on “Add GRE Tunnel” from the screen:

![Figure 6.1.2-A: Navigate to the GRE Tunnel Configuration screen](image)
6.1.2.1 Assign the Source IP to the Tunnel

In the window that appears, choose the static IP address that will be the source of GRE tunnel and enter a Description if desired:

![Add GRE Tunnel Configuration](image)

*Figure 6.1.2.1-A: Choose the GRE tunnel source IP*

Then click “Next”.
6.1.2.2 Choose Data Centers for Tunnel Termination

Now, with the Geospatial information from adding the Static IP the closest Data Center VIP and Next Closet Data Center VIP will be chosen. If you want to change these to different VIP’s or DC’s, choose them from the Dropdown.

![Figure 6.1.2.2-A: Choose the Data Centers for tunnel termination](image)

Then click “Next”.
6.1.2.3 Select GRE Tunnel Internal IP Subnet

Aruba SD-WAN does not require IP’s on their tunnel interfaces, so here simply toggle the “Is Unnumbered IP” slider.

Click “Next” to review and save.

![Add GRE Tunnel Configuration](image)
6.1.2.4 Save Tunnel Configuration

Review the configuration and click “Save”

Figure 6.1.2.4-A: Review and save the tunnel setup
6.1.3 Activate and Verify all Configuration Changes

Finally, we need to activate the saved configuration changes:

![Activation screenshot](image)

*Figure 6.1.3-A: Activate the GRE Tunnel configuration*

You can now navigate to “Activation” and activate the pending configurations, as shown above.
The “Activation Completed!” pop-up will appear to indicate your changes are now live.

**Figure 6.1.3-B: Verify the GRE Tunnel configuration was Activated**
6.2  Adding VPN Credentials for manual IPsec tunnels

6.2.1  Navigate to VPN Credentials

The first step in configuring an IPsec tunnel is to create a VPN Credential in ZIA. In the VPN Credential section, we will create a FQDN and Pre-Shared Key (PSK) for our IPsec session.

Navigation: Administration → Resources → and then click VPN Credentials.

![Figure 6.2.1-A: Navigate to VPN Credentials](image)
6.2.2 Add a VPN Credential

In Figure 6.2.2-A, 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” that is identified in the red box in the upper left.

![Figure 6.2.2-A: Adding a VPN Credential](image-url)
6.2.3 Enter VPN Credential Data

In Figure 58, configure the FQDN and Pre-Shared Key (PSK) for IKE. For the FQDN, you only need to configure the username portion of the FQDN as the domain name is automatically added to the right. Once both the FQDN and PSK are configured, click “Save” to continue.

![Figure 6.2.3-A: Enter VPN Credential Data](image-url)
6.2.4 Verify VPN Credential

In Figure 6.2.4-A, after saving the VPN Credential, you see “All changes have been saved” in the top center of your screen. If you look below this, you should see the VPN Credential you created.

![Figure 6.2.4-A: Verify Location Information and Save]
6.2.5  Activate Pending Changes

Now we need to save the changes. You can now navigate to “Activation” and activate the pending configurations, as shown in Figure 6.2.5-A.
6.2.6 Verify Activation

After activating pending changes, you should be returned to the prior page, and “Activation Completed!” should appear in the top of the window, as shown in Figure 6.2.6-A.

![Figure 6.2.6-A: Verify Activation](image)
6.3 Configuring a Location for Manual Tunnels

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

**Navigation:** Administration → Resources → and then click Location Management.

*Figure 6.3-A: Navigate to Locations*
6.3.1 Add a Location

In Figure 6.3.1-A, if you see “No Matching Items Found”, your ZIA instance does not have any locations configured. To add a location, click Add Location that is identified in the red box in the upper left. You can also edit any existing locations by clicking the Edit symbol to the far right of the listed location.

![Figure 6.3.1-A: Add a Location](image)
6.3.2 Enter Location Data

In Figure 6.3.2-A, fill in the fields within the red boxes. The name of the location is used as a policy object within ZIA. The “Managed By” field you can leave alone as “Self” is used for administration through the web interface. You need to choose a “Location Type” for the location as well. Choose the appropriate Location Group, typically it is “Corporate user traffic”. See here for more information: https://help.zscaler.com/zia/about-location-groups
You must enter either **Static IP Address(es)** or **VPN Credentials** to ensure the traffic incoming from the tunnels is mapped to the proper tenant policy. Add either the Static IP address for GRE tunnels or VPN Credentials if a manually created IPsec tunnel based on your needs as shown in the next two steps.

### 6.3.2.1 Add Static IP / GRE Tunnel to Location

In *Figure 6.3.2.1-A*, you will see the Static IP you configured in section 6.1.1 and linked to a GRE tunnel in section 6.1.2. Choose it and click “Done”. This will then link the Static IP and Traffic arriving on the GRE tunnel assigned to it to this Location. When finished click the “Save” button to continue.

*Figure 6.3.2.1-A: Select the Static IP that will be linked to the Location*
6.3.2.2 Adding a VPN Credential to a Location

In Figure 6.3.2.2-A, you should see the VPN Credential you configured in the section 6.2. Select it and click “Done”. From there, once you save the Location itself, this will couple the VPN Credential to this Location. When you have competed the fields, select “Save” to continue.

![Figure 6.3.2.2-A: Add VPN Credential to Location and Save](image-url)
6.3.3 Confirm Changes Have Been Saved

In *Figure 6.3.3-A*, after saving the Location, you see “*All changes have been saved.*” in the top center of your screen. If you look below this, you should see the Location you created.

*Figure 6.3.3-A: Confirm Changes Have Been Saved*
6.3.4 Activate Pending Changes

Anytime you make a change in ZIA, you will see a number over the Activation image on the left-hand side menu.

![Figure 6.3.4-A: Activate Changes](image)

Login ID obfuscated for security

This lets you know that you have changes pending in queue for activation. When you are ready to activate all changes in queue, click the blue “Activate” button.
6.3.5 Activation Confirmation

After activating all pending changes, you should see “Activation Completed!” in the red box. At this point, all queued changes have been pushed into production. These changes should take effect within seconds.

![Location Manager](image)

**Figure 6.3.5-A: Activation Confirmation**

This this point, you have a location, with a public IP associated to the location, and are ready to start configuring the Aruba SD-WAN side.

6.4 Manually Configure Tunnels on Aruba Orchestrator

Refer to *Appendix G: Aruba SD-WAN Resources* for links to the Aruba SD-WAN documentation to manually configure IPsec and GRE tunnels in the Aruba Orchestrator.
7 Appendix B: Configuring Layer-7 Health Checks for manually created tunnels

7.1 Configuring Aruba SD-WAN IP SLA

Navigate to and click on the "IP SLA" option under the Configuration → Templates → TCA’s sub-heading.

![Figure 7.1-A: Configure IP SLA](image-url)
7.2 Edit Edge Connect IPSLA rules
Click the Pencil / Edit Icon in the IP SLA tab for the appliance you want to configure the Health Check on.

![Figure 7.2-A: Edit IP SLA rule](image)

7.3 Add Rule and Target
Click “Add” to create new HTTP/HTTPS rule.

![Figure 7.3-A: Add Rule and Target](image)
### 7.4 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>Monitor</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>URL(s)</td>
<td>Error! Hyperlink reference not valid.</td>
</tr>
<tr>
<td></td>
<td>&lt;cloud&gt; should be your ZIA tenant cloud</td>
</tr>
<tr>
<td></td>
<td>Refer to this <a href="#">LINK</a> and the section titled Monitoring GRE Tunnels for details.</td>
</tr>
<tr>
<td>HTTP Request Timeout</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Medium</td>
<td>Tunnel</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Choose the GRE tunnel you wish to monitor</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Choose the <em>Loopback</em> 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 <em>Medium</em> field</td>
</tr>
<tr>
<td>Up Action</td>
<td>Enable Tunnel</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Tunnel from the <em>Medium</em> field</td>
</tr>
</tbody>
</table>

The above Request Timeout and Keep Alive Interval are recommendations. Tuning of these values may be required depending on your deployment.
Figure 7.4-A: Configure IP SLA Rule
7.5 Verify IP SLA Rule

![IP SLA Rule](image)

You may also search for the cloud that your tenant is located to only see Zscaler Health checks.
8 Appendix C: Checking tunnel status in ZIA Admin

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

Navigation: Analytics → Insights → and then click Tunnel Insights.

![Figure 8-A: Navigate to Tunnel Insights](image-url)
8.1 Tunnel Data Visualization

In the Insights screen you have the ability to visualize and filter data in various ways. Configure the Timeframe, Chart type, and Metrics you wish to view. Additionally, you can filter the type of data shown in the chart, by clicking the “filter” carrot to expose a dropdown menu to select from.

8.2 Tunnel Logging

To assist in troubleshooting you can also view the state of all tunnels for your tenant from the ZIA Admin UI. Click on the “Logs” button:

![Figure 8.2-A: Viewing ZIA tunnel logs](image)

From this screen you can then filter and change the timeframe for the tunnels and sites you would like to investigate. Please see the ZIA Tunnel Insights Logs: Columns help for details on the options: [https://help.zscaler.com/zia/tunnel-insights-logs-columns](https://help.zscaler.com/zia/tunnel-insights-logs-columns)
9 Appendix D: Deriving the Zscaler IPSEC VPN VIP

All Zscaler public IP endpoints can be found at https://config.zscaler.com/. It is preferred to use DNS hostnames as the destination for Tunnels and Proxies into the ZIA service. If the service or device that is the source of the traffic doesn’t support DNS names, as is the case for AWS Customer Gateways you will need to derive the IP address from the DNS hostname of the endpoint.

When you go to the above URL, make sure you select the correct Zscaler Cloud that your tenant is provisioned into, ensure that Cloud Enforcement Node Ranges is selected from the navigation frame and then choose the closest DC locations VPN Host Name to your AWS region.

![Figure 9-A: Zscaler Public IP reference](image-url)
Then use either `nslookup` or `dig` to get the IP address from the DNS hostname, example:

```
➜  ~ dig 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
```

*Figure 9-B: IP address lookup*
10 Appendix E: Requesting Zscaler Support

10.1 Gather Support Information

Zscaler support is sometimes required for the provisioning of certain services. Zscaler support is also available to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

10.1.1 Obtain Company ID

First, let’s grab our Company ID, which is how Zscaler uniquely identifies a given customer. The navigation is: Administration → Settings → and then click Company profile.

![Figure 10.1.1-A: Obtaining Company ID]

Figure 10.1.1-A: Obtaining Company ID
10.1.2 Save Company ID

Your company ID can be found in the red box below. Please copy this ID somewhere convenient as we will need it in subsequent screens.

![Company Profile](image)

*Figure 10.1.2-A: Save Company ID*
10.1.3 Open Support Ticket

Now that we have our company ID, we are ready to open a support ticket. The navigation is: “?” → Support → and then click “Submit a Ticket”. You can also go directly to the Submit Ticket page by visiting https://help.zscaler.com/submit-ticket.

Figure 10.1.3-A: Enter Support Section
10.2 Adding Domain (Example)

*Figure 10.2-A shows an example of how a support ticket is generally made. Each support ticket will ask targeted questions as a Ticket Type is defined. In this example below, we are requesting a domain be added to our ZIA instance.*

*Figure 10.2-A: Adding Domain Example*
11 Appendix F: Zscaler Resources

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/

11.1 Zscaler IP Page
https://config.zscaler.com/
12 Appendix G: Aruba SD-WAN Resources

EdgeConnect and Zscaler Integration Guide - IPSEC (for manual configurations)

EdgeConnect and Zscaler Integration Guide - GRE (for manual configurations)

Silver Peak Technical Demo: Integrating Zscaler into the Unity EdgeConnect SD-WAN fabric.

Zscaler and Silver Peak Solution Brief

Silver Peak SD-WAN Deployment Guide