# Table of Contents

1 Zscaler and VeloCloud ................................................................. 7  
   1.1 Prerequisites ........................................................................... 7

2 Configuring Zscaler Internet Access (ZIA) ................................. 8  
   2.1 Configuring Zscaler Internet Access ........................................ 8  
      2.1.1 Logging into ZIA ............................................................... 8
   2.2 Configure ZIA for API Access .................................................. 9  
      2.2.1 Adding SD-WAN Partner Key .......................................... 10
      2.2.2 Add SD-WAN Partner Key ............................................... 11
      2.2.3 Verify SD-WAN Partner Key ............................................ 12
      2.2.4 Adding a Partner Administrator Role ............................... 13
      2.2.5 Add Partner Administrator Role ..................................... 14
      2.2.6 Creating Partner Administrator Role ................................. 15
      2.2.7 Administrator Management ........................................... 16
      2.2.8 Add Partner Administrator .............................................. 17
      2.2.9 Creating Partner Administrator ...................................... 18
      2.2.10 Active Pending Changes .............................................. 19
      2.2.11 Verify Activation ............................................................ 20

3 Configuring VMware SD-WAN ....................................................... 21  
   3.1 Configuring Automated IPsec Tunnel from VCE ....................... 22  
      3.1.1 New Cloud Security Provider for Automated Deployment .......... 23
      3.1.2 Profile for Cloud Security Service .................................... 24
      3.1.3 Automated IPsec Tunnel for Edge .................................... 26
      3.1.4 Verify Tunnels are Up (Active) ........................................ 27
   3.2 Configure GRE Tunnel to ZIA from VCE ................................. 28  
      3.2.1 New Cloud Security Provider for GRE .............................. 29
      3.2.2 Profile for Cloud Security Service .................................... 30
      3.2.3 GRE Tunnel for Edge ..................................................... 31
      3.2.4 GRE Tunnel Details From Zscaler .................................... 32
      3.2.5 Verify GRE Tunnel Configuration ................................... 33
      3.2.6 Verify Tunnels are Up (Active) ........................................ 34
   3.3 Configuring IPsec Tunnel from VCG ....................................... 35  
      3.3.1 New Non-VeloCloud Site ............................................... 35
      3.3.2 Create Non-VeloCloud Site ............................................ 36
      3.3.3 Advanced Settings for Non-VeloCloud Site ....................... 37
      3.3.4 Enable Cloud VPN ....................................................... 38
      3.3.5 Verify Tunnels are Up (Active) ........................................ 39
   3.4 Configuring Business Policy for ZIA ...................................... 40  
      3.4.1 Configure Rule for VCE ................................................... 41
      3.4.2 Configure Rule for VCG ................................................... 42

# Prerequisites
- Configure Rule for VCG
- Verify Tunnels are Up (Active)
- Enable Cloud VPN
- Advanced Settings for Non-VeloCloud Site
- Create Non-VeloCloud Site
- New Non-VeloCloud Site
- New Cloud Security Provider for Automated Deployment
- Profile for Cloud Security Service
- Automated IPsec Tunnel for Edge
- Verify Tunnels are Up (Active)
- New Cloud Security Provider for GRE
- Profile for Cloud Security Service
- GRE Tunnel for Edge
- GRE Tunnel Details From Zscaler
- Verify GRE Tunnel Configuration
- Verify Tunnels are Up (Active)
- Configure Rule for VCE
- Configure Rule for VCG
4 Appendix A: Configuring ZIA for GRE Tunnel ........................................... 43
  4.1 Provision GRE Tunnel ............................................................................. 43
  4.2 Navigate to Locations ........................................................................... 43
  4.3 Add a Location ....................................................................................... 44
  4.4 Enter Location Data ............................................................................... 45
  4.5 Verify Location Information and Save ................................................... 46
  4.6 Confirm Changes Have Been Submitted ................................................. 47
  4.7 Activate Changes ................................................................................... 48

5 Appendix B: Configuring ZIA for IPsec Tunnel .......................................... 49
  5.1 Navigate to VPN Credentials ................................................................. 49
  5.2 Add a VPN Credential ........................................................................... 50
  5.3 Enter VPN Credential Data ..................................................................... 51
  5.4 Verify VPN Credential .......................................................................... 52
  5.5 Navigate to Locations ............................................................................ 53
  5.6 Add a Location ....................................................................................... 54
  5.7 Enter Location Data ............................................................................... 55
  5.8 Add VPN Credential to Location and Save ............................................ 56
  5.9 Confirm Changes Have Been Saved ....................................................... 57
  5.10 Activate Pending Changes ................................................................... 58
  5.11 Activation Confirmation ...................................................................... 59

6 Appendix C: Requesting Zscaler Support .................................................... 60
  6.1 Gather Support Information .................................................................... 60
    6.1.1 Obtain Company ID ........................................................................ 60
    6.1.2 Save Company ID ........................................................................... 61
    6.1.3 Open Support Ticket ....................................................................... 62
  6.2 GRE Provisioning Request (Example) ....................................................... 63
  6.3 Adding Domain (Example) ..................................................................... 64

7 Appendix D: Verifying ZIA Configuration .................................................... 65
  7.1 Request Verification Page ....................................................................... 65

8 Appendix E: Zscaler Resources .................................................................. 66
  8.1 Zscaler IP Pages .................................................................................... 66

9 Appendix F: VeloCloud Resources ............................................................... 67
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Central Authority (Zscaler)</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DMPO</td>
<td>Dynamic Multipath Optimization</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection <em>(RFC 3706)</em></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation <em>(RFC 2890)</em></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange <em>(RFC 2409)</em></td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security <em>(RFC 2411)</em></td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Share Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer <em>(RFC 6101)</em></td>
</tr>
<tr>
<td>VCE</td>
<td>VeloCloud Edge</td>
</tr>
<tr>
<td>VCG</td>
<td>VeloCloud Gateway</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For <em>(RFC 7239)</em></td>
</tr>
<tr>
<td>ZCC</td>
<td>Zscaler Client Connector</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
About This Document

Zscaler Overview

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.

VMware SD-WAN Overview

VMware software powers the world’s complex digital infrastructure. The company’s cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit https://www.vmware.com/company.html.
Audience

This guide is written for network administrators, network analysts, and IT administrators responsible for deploying, monitoring and managing Enterprise branch network. For additional product and company resources, please refer to the Appendix section.

Software Revisions

This document was written using Zscaler Internet Access v6.0 and VeloCloud Orchestrator 3.4 (Pre-GA).

Request for Comments

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.
1 Zscaler and VeloCloud

1.1 Prerequisites

This guide will provide GUI examples for configuring Zscaler Internet Access and VeloCloud 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 VeloCloud. The prerequisites to use this guide are:

**Zscaler Internet Access (ZIA)**

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

**VMware SD-WAN Orchestrator**

- Enterprise account access to VMware SD-WAN Orchestrator
- Administrator login credentials
- One or more VeloCloud Edge appliances with “Online” status in VMware SD-WAN Orchestrator
2 Configuring Zscaler Internet Access (ZIA)

2.1 Configuring Zscaler Internet Access

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

2.1.1 Logging into ZIA

Log into Zscaler using your administrator account, as show in Figure 1. If you are unable to log in using your administrator account, please contact support:


Figure 1: Log Into Zscaler
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.

Navigation: Administration -> Cloud Configuration -> Partner Integrations

![Configuring ZIA for API Access](image)

Figure 2: Configuring ZIA for API Access
2.2.1 Adding SD-WAN Partner Key

Once you arrive to the “Partner Integration” section of the ZIA Admin UI, please select “SD-WAN” and then “Add Partner Key”, as shown in Figure 3.

Figure 3: Add Partner Key
2.2.2 Add SD-WAN Partner Key

A window will appear, as shown in Figure 4. 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 “VMware VeloCloud”, click on “Generate”. After, you will return to the prior screen.

Figure 4: Add SD-WAN Partner Key
2.2.3 Verify SD-WAN Partner Key

Once you return to the screen shown in Figure 5, you should see the Partner Key you created for VMware VeloCloud. Note: You will not see “REMOVED” in red letters. 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: Save the “Key” value as you will need to enter them in VeloCloud.

![Figure 5: Verify SD-WAN Partner Key](image)

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

Figure 6: Adding Partner Administrator Role
2.2.5 Add Partner Administrator Role

Figure 7: Add Partner Administrator Role
2.2.6 Creating Partner Administrator Role

By creating a Partner Administrator Role, we can define the permission and access we wish to grant to a third party partner, such as a SD-WAN partner. Once you name the Administrator Role, change the Access Control to “Full”, as shown in Figure 13. The toggle “Full” allows partner admins to view and edit VPN credentials and Locations that VeloCloud Orchestrator is managing via ZIA Provisioning API. This is necessary for Unity Orchestrator to be able to create new VPN Credentials and Locations for branch locations. Once you have completed these steps, then click “Save”. After you will be returned to the prior screen.
2.2.7 Administrator Management

The last step required is creating a Partner Administrator. Please follow the navigation below, which is also depicted in Figure 9.

Navigation: Administration -> Administration Controls -> and then click Administrator Management

Figure 9: Administrator Management
2.2.8 Add Partner Administrator

Once you arrive to the “Administrator Management” page, please select “Add Partner Administrator”, as show in Figure 10. A user input screen will appear, which is shown in the next section.

![Figure 10 Admin Partner Administrator](image-url)
2.2.9 Creating Partner Administrator

Once the “Add Partner Administrator” input box appears, fill in the fields with red boxes around them, as shown in Figure 11. Once this is completed, click “Save”.

Note: Save these settings as you will need to enter them in Unity Orchestrator.

Figure 11: Creating Partner Administrator
2.2.10 **Active Pending Changes**

Finally we have reached our last step in the Zscaler Admin UI. You can now navigate to “Activation” and activate the pending configurations, as shown in Figure 12.

![Figure 12: Active Pending Changes](image-url)
2.2.11 Verify Activation

After activating pending changes, you should return to the prior page, and “Activation Complete” should appear in the top of the window, as shown in Figure 13.

![Figure 13: Verify Activation](image-url)
3 Configuring VMware SD-WAN

This section will cover 3 deployment models:

1) Configuring Automated IPsec Tunnels from VeloCloud Edge (VCE)
2) Configuring GRE Tunnel to ZIA from VeloCloud Edge (VCE)
3) Configuring IPsec Tunnel from VeloCloud Gateway (VCG)

The configuration are up to date as of VMware SD-WAN Release 4.0.0.
3.1 Configuring Automated IPsec Tunnel from VCE

First we need to create a Non-VeloCloud Site entry for Zscaler. Navigate to Configure -> Network Services -> Cloud Security Service -> New.

![Figure 14: Configuring new Cloud Security Service](image)
After selecting “New”, a pop-up should appear, as shown below. You need to configure:

1) **Service Type**: Zscaler Cloud Security Service
2) **Automated Cloud Service**: Enable
3) **Zscaler Cloud**: Type in the name of the Zscaler cloud you are provisioned in.
4) **Partner Admin Username**: Type in the *Partner Admin Username* you provisioned.
5) **Partner Admin Password**: Type in the *Partner Admin Password* you provisioned.
6) **Partner Key**: Type in the *Partner Key* you provisioned.
7) **Domain**: Type in the domain name your ZIA instance is provisioned with (typically your company domain).

Once you have completed filling in these fields, select “Add” to continue.
3.1.2 Profile for Cloud Security Service

In this section, navigate to Configure -> Profiles. Once you select the profile you wish to use, select “Device”. You need to configure:

1) Cloud Security Service: Select it “On”
2) Cloud Security Service: Select the Cloud Security Service you configured in the prior section
3) Tunneling Protocol: IPsec
4) Hash: Select SHA1 or SHA256
5) Encryption: Select None, AES-128 or AES-256 per your requirements
6) Key Exchange Protocol: IKEv2

Once you have completed these fields, select “Save Changes” in the upper right of your screen. This will cause the VMware orchestrator to make outbound API calls to Zscaler and automatically configure all the Edge sites using the Profile.
Navigate to Monitor > Events and you should see the events showing the orchestrator configuring the automatic IPsec Tunnels for each Edge site.

Figure 17: API Automation Events
3.1.3 Automated IPsec Tunnel for Edge

After a few minutes, the IPsec Tunnels from the Edges using the configured Profile should automatically establish IPsec Tunnels from its public WAN interfaces. For any parameter changes needed at specific sites, you may navigate to Configure -> Edges -> and select the VCE you want to configure and check the Enable Edge Override option to change the IPsec parameter.

If there are no changes from the Profile and the API call succeeded for the Edge, you should see the Credentials automatically populated. The automated IPsec tunnel configuration is complete, and you may configure Business Policies to forward user traffic to Zscaler.

![Automated IPsec Tunnel from VCE](image)

Figure 18: Automated IPsec Tunnel from VCE
3.1.4 Verify Tunnels are Up (Active)

To verify the state of the Automated IPsec tunnel, navigate to Monitor -> Edges. You may have to wait 30 seconds, but you should see the primary IPsec tunnel establish. The standby tunnel will remain grey until it becomes active, which should only occur if the primary IPsec tunnel fails.

![Monitor Edge Tunnels](image)

Figure 19: Monitor Edge Tunnels
3.2 Configure GRE Tunnel to ZIA from VCE

First we need to create a Cloud Security Service entry for Zscaler. Navigate to Configure -> Network Services -> Cloud Security Service -> New.

Figure 20: Configuring new Cloud Security Service for GRE tunnels
### 3.2.1 New Cloud Security Provider for GRE

After selecting “New”, a pop-up should appear, as shown below. You need to configure:

![New Cloud Security Provider](image)

**Figure 21: New Cloud Security Provider for GRE**

1) **Service Type:** Zscaler Cloud Security Service

2) **Primary and Secondary Server:** Obtain the GRE VIP IP from the Zscaler IP Pages (look at Appendix). You should use the IP Pages for the Zscaler cloud you are provisioned in (e.g. ZS3).

Once you have completed filling in these fields, select “Add” to continue.
3.2.2 Profile for Cloud Security Service

In this section, navigate to Configure -> Profiles. Once you select the profile you wish to use, select “Device”. You need to configure:

1) **Cloud Security Service**: Select it “On”

2) **Cloud Security Service**: Select the Cloud Security Service you configured in the prior section

3) **Tunneling Protocol**: Select GRE

Once you have completed these fields, select “Save Changes” in the upper right of your screen.
3.2.3 GRE Tunnel for Edge

Next you need to navigate to Configure -> Edges -> and select the VCE you want to configure the GRE tunnel on. Next select “Device” and then scroll down to configure:

1) **Cloud Security Service**: Select it “On”.

2) **GRE Tunnel**: Select “Add Tunnel”.

Figure 23: GRE Tunnel for Edge (VCE)
3.2.4 GRE Tunnel Details From Zscaler

After selecting “Add Tunnel”, a pop-up should appear, as shown below. You want to configure:

![Add Tunnel Pop-Up]

Figure 24: Input GRE Tunnel Details

1) **WAN Link**: Select the WAN interface the GRE tunnel should source from (in our example, our lab WAN link is called “Hurricane Electric”).

2) **Tunnel Addressing**: The Router IP/Mask and Internal ZEN IP/Mask is provided by Zscaler. If you have not already opened a support ticket with Zscaler to have a GRE Tunnel provisioned, please Section 6, Appendix C: Requesting Zscaler Support.

Once you have completed these fields, select “Ok to continue.”
3.2.5 Verify GRE Tunnel Configuration

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

![Cloud Security Service](image)

*Figure 25: Verify GRE Tunnel Configuration*
3.2.6 Verify Tunnels are Up (Active)

To verify the state of the GRE tunnel, navigate to Monitor -> Edges. You may have to wait 30 seconds, but you should see the primary GRE tunnel establish. The standby tunnel will remain grey until it becomes active, which should only occur if the primary GRE tunnel fails.

Figure 26: Monitor Edge GRE Tunnel State
3.3 Configuring IPsec Tunnel from VCG

3.3.1 New Non-VeloCloud Site

First we need to create a Non-SD-WAN Destination entry for Zscaler. Navigate to Configure -> Network Services -> Non-SD-WAN Destinations via Gateway -> New.

![Create New Non-SD-WAN Destination via Gateway](image)

Figure 27: Create New Non-SD-WAN Destination via Gateway
3.3.2 Create Non-VeloCloud Site

After selecting “New”, a pop-up should appear, as shown below. You need to configure:

![Create New Non-SD-WAN Destination via Gateway](image)

**Figure 28: Create New Non-SD-WAN Destination via Gateway**

1) **Type**: Select “Zscaler”  
2) **Primary and Secondary VPN Gateway**: Obtain the IPSec VIP IP from the Zscaler IP Pages (look at Appendix). You should use the IP Pages for the Zscaler cloud you are provisioned in (e.g. ZS3).

Once you have completed filling in these fields, select “Next” to continue.
3.3.3 Advanced Settings for Non-VeloCloud Site

Next select “Advanced” at the lower-left bottom. The window should expand with additional configuration options, as show below in Figure 28. You need to configure:

1) **Local Auth Id**: User FQDN. Below, paste in your ZIA VPN Credential FQDN.

2) **Primary and Secondary VPN Gateway – PSK**: Paste in your ZIA VPN Credential PSK.

Once you have completed these fields, select “Save Changes” in the lower right.
3.3.4 Enable Cloud VPN

Next you need to navigate to **Configure -> Profiles -> and select the Profile** you want to enable. Next select “Device” and then scroll down to configure:

![Configuration Profile](image)

**Figure 30: Enabling Zscaler Connectivity from VCG on VMware Orchestrator**

1) **Cloud VPN**: Select it “On”.

2) **Enable**: Select the Non-VeloCloud Site in the drop down.
3.3.5 Verify Tunnels are Up (Active)

To verify the state of the IPsec tunnel from VCG, navigate to Monitor -> Network Services. You may have to wait 30 seconds, but you should see the primary and secondary IPsec tunnels establish. The redundant tunnels, if configured will remain grey until they becomes active, which should only occur if the primary and secondary IPsec tunnels fail.

![Monitor Network Services Tunnel State from VCG](image)

Figure 31: Monitor Network Services Tunnel State from VCG
3.4 Configuring Business Policy for ZIA

In this section we will create a Business Policy to send all Internet destined traffic to Zscaler. Navigate to Configure -> Profiles -> and select your Profile. Next, select “Business Policy”, and then select “New Rule”.

Figure 32: Configuring Business Policy for ZIA
3.4.1 Configure Rule for VCE

After selecting “New”, a pop-up should appear, as shown below. You need to configure:

![Configure Rule](image)

Figure 33: Configure Rule for Edges Using Direct Tunnel from VCE
3.4.2 Configure Rule for VCG

Figure 34: Configure Rule for Edges Using Tunnels from VCG
4 Appendix A: Configuring ZIA for GRE Tunnel

4.1 Provision GRE Tunnel

GRE tunnels need to be provisioned manually. If you do not yet have your GRE Tunnel details, please open a support ticket. You will need to provide a publicly-routable source IP address. You are provided with a provisioned primary and secondary GRE tunnel. The instructions to open a Zscaler support ticket for GRE provisioning is in section 5, “Appendix C: Requesting Zscaler Support”

4.2 Navigate to Locations

After logging in, add a location if one is not present for GRE access to 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 Locations.

Figure 50: Navigate to Locations
4.3 Add a Location

In Figure 51, 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 any location that is listed.

Figure 51: Add a Location
4.4 Enter Location Data

The data in the red box in Figure 52 must be entered. Fill in Name, State/Province, Country, Time Zone, and under Addressing, under Static IP Addresses, pick the source IP address of your GRE tunnel.

![Figure 52: Enter Location Data](image)

**Note:** If the Static IP Addresses drop-down box does not show the IP address to your new location, please refer to section “Appendix C: Requesting Zscaler Support”. A support ticket will need to be created to have the public IP address of your location present to associate to your new location. The next section will provide examples with a Public IP address defined prior.
4.5 **Verify Location Information and Save**

Now that you have entered your location information, you are ready to save your new location. Please click **Save** to continue.

![Image of the Add Location screen](image.png)

**Figure 53: Verify Location Information and Save**
4.6 **Confirm Changes Have Been Submitted**

Once you click **Save**, the screen will refresh and you should see **All Changes have been saved** on the top of the page. Below that, you should see the new location.

![Figure 54: Confirm Changes Have Been Submitted](image)

At this point, although we have saved our new location, it has only submitted the change for pending activation. If you wanted to make other changes throughout ZIA, you could. None of these changes would get applied until they are activated, which allows you to batch groups of changes as you require. Only upon activation do the changes get pushed to ZEN nodes.
4.7 Activate Changes

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

![Activation Image]

Figure 55: Activate Changes

This lets you know that you have changes pending in queue for activation. When you are ready to activate all changes in queue, click the blue Activate button.
5 Appendix B: Configuring ZIA for IPsec Tunnel

5.1 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 56: Navigate to VPN Credentials](image-url)
5.2 Add a VPN Credential

In Figure 57, 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 57: Adding a VPN Credential
5.3 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 58: Enter VPN Credential Data](image-url)
5.4 Verify VPN Credential

In Figure 59, 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 59: Verify Location Information and Save
5.5 Navigate to Locations

After the VPN credential has been added, it needs to be linked to a location. Add a location if one is not present for IPSec access to 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 Locations.
5.6 Add a Location

In Figure 61, 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 61: Add a Location
5.7 **Enter Location Data**

In Figure 62, 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. Lastly, under **VPN Credentials**, select the VPN credential you configured in the prior steps. Once you select the drop down, the screen in the next section will appear.

![Add Location Screen](image_url)

*Figure 63: Enter Location Data*
5.8 **Add VPN Credential to Location and Save**

In Figure 64, you should see the VPN Credential you configured in the prior section. Select it and click **Save**. From there, once you save the Location itself, this will couple the VPN Credential to this Location. When you have completed the fields, select **Save to continue.**
5.9  Confirm Changes Have Been Saved

In Figure 65, 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 65: Confirm Changes Have Been Saved](image-url)
5.10 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 66: Activate Changes](image)

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.
5.11 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.

This this point, you have a location, with a public IP associated to the location, and are ready to start configuring the VMware SD-WAN side.
6 Appendix C: Requesting Zscaler Support

6.1 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.

6.1.1 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 70: Obtaining Company ID](image-url)
6.1.2 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.

![Figure 71: Save Company ID](image-url)
6.1.3 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 72: Enter Support Section
6.2 **GRE Provisioning Request (Example)**

Figure 80 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 GRE service be provisioned with our public IP information.

![GRE Provisioning Example](image)

Figure 80: GRE Provisioning Example
6.3 Adding Domain (Example)

Figure 81 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 81: Adding Domain Example
7 Appendix D: Verifying ZIA Configuration

7.1 Request Verification Page

The URL https://ip.zscaler.com can be used to validate if you are transiting ZIA. In Figure 90 and 91 below, you will see examples of what the page output should display if you are or are not transiting ZIA.

Note: the IP information presented in both figures should not match and instead should be your client IP address when attempting this page view.

![Figure 90: Non-working Example](image)

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

Your request is arriving at this server from the IP address 209.37.255.2
Your Gateway IP Address is most likely 209.37.255.2

![Figure 91: Working Example](image)

If you are transiting ZIA, you should see the following:
8 Appendix E: 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/

8.1 Zscaler IP Pages

https://ips.zscaler.net/cenr/
https://ips.zscalerbeta.net/cenr/
https://ips.zscalerone.net/cenr/
https://ips.zcalerntwo.net/cenr/
https://ips.zscalerthree.net/cenr/
Appendix F: VeloCloud Resources

VeloCloud
http://www.velocloud.com/

VeloCloud Support
http://www.velocloud.com/customers/support