# Table of Contents

1 Zscaler and Silver Peak ........................................................................................................... 6
   1.1 Prerequisites ................................................................................................................ 6

2 Configuring Zscaler Internet Access (ZIA) ......................................................................... 7
   2.1 Configuring Zscaler Internet Access .......................................................................... 7
      2.1.1 Logging into ZIA .................................................................................................... 7
   2.2 Configure ZIA for API Access ................................................................................. 8
      2.2.1 Adding SD-WAN Partner Key ............................................................................. 9
      2.2.2 Add SD-WAN Partner Key ................................................................................ 10
      2.2.3 Verify SD-WAN Partner Key ............................................................................. 11
      2.2.4 Adding a Partner Administrator Role ............................................................... 12
      2.2.5 Add Partner Administrator Role ...................................................................... 13
      2.2.6 Creating Partner Administrator Role ............................................................... 14
      2.2.7 Administrator Management ............................................................................. 15
      2.2.8 Add Partner Administrator .............................................................................. 16
      2.2.9 Creating Partner Administrator ...................................................................... 17
      2.2.10 Active Pending Changes ................................................................................. 18
      2.2.11 Verify Activation .............................................................................................. 19

3 Configuring Automated IPsec Tunnels ............................................................................. 20
   3.1 Log into Unity Orchestrator ..................................................................................... 21
   3.2 Configure Cloud Services ...................................................................................... 22
   3.3 Configuring ZIA Subscription .................................................................................. 23
   3.4 Configuring ZIA API Credentials and Zscaler Cloud .............................................. 24
   3.5 Verifying ZIA API Credentials and Zscaler Cloud .................................................. 25
   3.6 Verify ZIA Account Update .................................................................................... 26
   3.7 Configuring Business Intent Overlays .................................................................... 27
   3.8 Enabling Zscaler for Breakout Traffic .................................................................... 28
   3.9 Configuring Preferred Policy Order ....................................................................... 29
   3.10 Confirm Changes ................................................................................................... 30
   3.11 Verifying Automated Tunnel Establishment .......................................................... 31
   3.12 View Automated Tunnel Details .......................................................................... 32

4 Configuring Sub-Locations and Gateway Options ......................................................... 33
   4.1 Configure Sub-location ........................................................................................... 33
   4.2 Enable Gateway Option Orchestration .................................................................. 34
   4.3 Add Sub-location .................................................................................................... 35
   4.4 Configure Gateway Options .................................................................................. 36
   4.5 Set Gateway Options ............................................................................................. 37
   4.6 Change Gateway Options Confirmation ............................................................... 38
4.7 Verify Gateway Options.................................................................................................... 39
4.8 Verify Sub-locations in ZIA .......................................................................................... 40

5 Appendix A: Configuring ZIA for GRE Tunnel............................................................... 41
5.1 Provision GRE Tunnel ................................................................................................ 41
5.2 Navigate to Locations ................................................................................................. 41
5.3 Add a Location ............................................................................................................ 42
5.4 Enter Location Data .................................................................................................... 43
5.5 Verify Location Information and Save ...................................................................... 44
5.6 Confirm Changes Have Been Submitted .................................................................. 45
5.7 Activate Changes ....................................................................................................... 46

6 Appendix B: Configuring ZIA for IPsec Tunnel .............................................................. 47
6.1 Navigate to VPN Credentials .................................................................................... 47
6.2 Add a VPN Credential .............................................................................................. 48
6.3 Enter VPN Credential Data ....................................................................................... 49
6.4 Verify VPN Credential ............................................................................................. 50
6.5 Navigate to Locations ............................................................................................... 51
6.6 Add a Location ......................................................................................................... 52
6.7 Enter Location Data .................................................................................................. 53
6.8 Add VPN Credential to Location and Save ............................................................. 54
6.9 Confirm Changes Have Been Saved ...................................................................... 55
6.10 Activate Pending Changes .................................................................................... 56
6.11 Activation Confirmation ........................................................................................ 57

7 Appendix C: Requesting Zscaler Support ..................................................................... 58
7.1 Gather Support Information ...................................................................................... 58
7.1.1 Save Company ID .................................................................................................. 59
7.1.2 Enter Support Section .......................................................................................... 60
7.2 GRE Provisioning Request (Example) ..................................................................... 61
7.3 Adding Domain (Example) ...................................................................................... 62

8 Appendix D: Verifying ZIA Configuration ..................................................................... 63
8.1 Request Verification Page .......................................................................................... 63

9 Appendix E: Zscaler Resources .................................................................................... 64
9.1 Zscaler IP Pages ....................................................................................................... 64

10 Appendix F: Silver Peak Resources ............................................................................ 65
# 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>(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>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>(RFC 6101)</em></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security <em>(RFC 5246)</em></td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For <em>(RFC 7239)</em></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

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.

Silver Peak Overview

Silver Peak, the global SD-WAN leader, offers networking software that enables enterprises to build a modern WAN that drives maximum value from existing and ongoing cloud and digital transformation investments by delivering a self-driving wide area network that continuously learns and adapts to the needs of the business. Thousands of globally distributed enterprises have deployed the Unity EdgeConnect™ SD-WAN edge platform across 100 countries.
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 Silver Peak Orchestrator v 8.10.10.40179.

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 Silver Peak

1.1 Prerequisites

This guide will provide GUI examples for configuring Zscaler Internet Access (ZIA) and Silver Peak Unity 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 Silver Peak. 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 Silver Peak Unity Orchestrator 8.10.10.40179, or greater, with administrator login credentials.
- One or more Unity 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 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

![Figure 2: Configuring ZIA for API Access](image)
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](image-url)
2.2.2 Add SD-WAN Partner Key

A window will appear, as shown in Figure 4. On 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 selecting “Silver Peak”, 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 Silver Peak. 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 Silver Peak.

---

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

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

Next we need to create a Partner Admin Role. The Partner Admin Role is used to define the partner access to the SD-WAN resource.

Navigation: Administration -> Administrator Controls -> Role Management.

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

Once you arrive to the “Role Management” section of the ZIA Admin UI, select “Add Partner Administrator Role”, as shown in Figure 7.

![Figure 7: Add Partner Administrator Role](image)
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 8. The toggle “Full” allows partner admins to view and edit VPN credentials and Locations that Unity 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.

Figure 8: Creating Partner Administrator Role
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

![Administrator Management](image)

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.

![Image of Add Partner Administrator](image-url)

Figure 10 Admin Partner Administrator
2.2.9 Creating Partner Administrator

Once the “Add Partner Administrator” input box appears, fill in the fields with red boxes around then, 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](image-url)
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 be returned 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 Automated IPsec Tunnels

In this section, we will configure Unity 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 Unity Orchestrator dashboard shown in Figure 20. 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 Unity Orchestrator Dashboard, please contact Silver Peak and request a full demo.

![Figure 20: Example Dashboard of Unity Orchestrator](image)

Figure 20: Example Dashboard of Unity Orchestrator
3.1 Log into Unity Orchestrator

Open a web browser and enter the URL to your Unity Orchestrator instance. When the page loads, you should see the screen in Figure 21. Please enter your Unity Orchestrator username and password. If you are unable to log in, please email support@silver-peak.com.

Figure 21: Unity 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 21: Configuring Cloud Services](image)

Figure 21: Configuring Cloud Services
3.3 Configuring ZIA Subscription

Next select “Subscription” as shown in Figure 22.

Figure 22: Configuring ZIA Subscription
3.4 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. For demonstration purposes the Polling Interval can be reduced to a shorter timeframe such as 2 minutes. This will increase the responsiveness of the API when making frequent changes to the Zscaler Cloud configuration.

![Figure 23: Configuring API Credentials](image)

Figure 23: Configuring API Credentials
3.5 Verifying ZIA API Credentials and Zscaler Cloud

Once you have configured your settings, Unity will attempt to verify the settings. If the settings are valid, you will see “Connected” instead of “Not Connected”. Once connected, select “Save” to continue.

Figure 24: Verifying ZIA API Credentials
3.6 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 25: Verifying ZIA Account Update
3.7 Configuring Business Intent Overlays

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

Figure 26: Configuring Business Intent Overlays
3.8 Enabling Zscaler for Breakout Traffic

Once the screen refreshes, look for the “Breakout Traffic to Internet & Cloud Services” section. Then click anywhere within the red box shown below. This will then open a pop-up with more configuration options.

![Figure 27: Enabling Zscaler for Breakout Traffic](image)
3.9 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 28: Configuring Preferred Policy Order
3.10 Confirm Changes

Next you should be presented with a confirmation to confirm your changes. You should select “Save”.

![Figure 29: Confirm Changes](image-url)
3.11 Verifying Automated Tunnel Establishment

After selected “Save” in the last step, it may take 30-60 seconds until your initial tunnels are deployed. Once IPsec tunnels start to establish, you should see “Deployed” in green, as shown below.

![Figure 30: Verify Automated Tunnel Establishment](image-url)
### 3.12 View Automated Tunnel Details

If you select “Tunnels”, you will then see more details to each configured tunnel, such as the local IP, remote IP, tunnel mode, …etc.

![View Automated Tunnel Details](image)

**Figure 31: View Automated Tunnel Details**
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

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

![Figure 32: Configure Sub-location]
4.2 Enable Gateway Option Orchestration

If this is your first time selecting “Gateway Options”, the following pop-up should appear. Select “Enable Gateway Orchestration” to continue.

![Enable Gateway Orchestration pop-up](image)

Figure 33: 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 Unity. This is not the name of the Sub-location that will appear in ZIA.

2) Select which Silver Peak 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. Guess 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 SilverPeak interface label as configured in the Deployment screen for an EdgeConnect appliance. Figure 34 shows that the “Guest” lan-side label has been selected.

4) Select “Save”.

![Image of Sub-location configuration](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” cell and a pop-up window will open.

![Gateway Options Configuration](image)

Figure 35: 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”.

![Set Gateway Options](image)

Figure 36: 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”.

Figure 37: Change Gateway Options Confirmation
4.7 Verify Gateway Options

We should now see the Sub-locations applies to each tunnel, with the selected Gateway Options configured.

Figure 38: Verify Gateway Options
4.8 Verify Sub-locations in ZIA

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

![Figure 39: Verify Sub-locations in ZIA](image-url)
5 Appendix A: Configuring ZIA for GRE Tunnel

5.1 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 6, Appendix C: Requesting Zscaler Support.

5.2 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 60: Navigate to Locations
5.3 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 any location that is listed.

![Add Location](image)

Figure 61: Add a Location
5.4 Enter Location Data

The data in the red box in Figure 62 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 62: 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.
5.5 *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.

![Figure 63: Verify Location Information and Save](image-url)
5.6 **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 64: 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.
5.7 Activate Changes

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

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.

Figure 65: Activate Changes
6 Appendix B: Configuring ZIA for IPsec Tunnel

6.1 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 66: Navigate to VPN Credentials](image)
6.2 Add a VPN Credential

In Figure 67, 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 67: Adding a VPN Credential
6.3 Enter VPN Credential Data

In Figure 68, 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 68: Enter VPN Credential Data](image)
6.4 Verify VPN Credential

In Figure 69, 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 69: Verify Location Information and Save](image-url)
6.5 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.

Figure 70: Navigate to Locations
6.6 **Add a Location**

In *Figure 71*, 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.

![Add Location](image)

*Figure 71: Add a Location*
6.7 **Enter Location Data**

In Figure 72, 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.

![Figure 72: Enter Location Data](image-url)
6.8 Add VPN Credential to Location and Save

In Figure 73, 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 competed the fields, select “**Save** to continue.

![Figure 73: Add VPN Credential to Location and Save](image-url)
6.9 **Confirm Changes Have Been Saved**

In Figure 74, 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.
6.10 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 75: 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.
6.11 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.

Figure 76: Activation Confirmation

This point, you have a location, with a public IP associated to the location, and are ready to start configuring the Silver Peak side.
Appendix C: Requesting Zscaler Support

7.1 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.

The navigation is: Administration -> Settings -> and then click Company profile

Figure 80: Collecting details to open support case with Zscaler TAC
7.1.1 Save Company ID

Copy the Company ID, as shown below.

![Company Profile](image)

Figure 81: Company ID
7.1.2 Enter Support Section

Now that we have our company ID, we are ready to open a support ticket. The navigation is: Dashboard -> Support -> Submit a Ticket.

Figure 82: Submit ticket
7.2 GRE Provisioning Request (Example)

Figure 90 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.

Figure 90: GRE Provisioning Example
7.3 Adding Domain (Example)

*Figure 91* 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.

![Submit Ticket](image)

*Figure 91: Adding Domain Example*
8 Appendix D: Verifying ZIA Configuration

8.1 Request Verification Page

The URL https://ip.zscaler.com can be used to validate if you are transiting ZIA. In Figure 100 and 101 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 100: 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 101: Working Example](image)

If you are transiting ZIA, you should see the following:

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

Your request is arriving at this server from the IP address 104.129.198.69
The Zscaler proxy virtual IP is 104.129.198.34.
The Zscaler hostname for this proxy appears to be za2-qla1a1.
9 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/

9.1 Zscaler IP Pages

https://ips.zscaler.net/cenr/
https://ips.zscalerbeta.net/cenr/
https://ips.zscalerone.net/cenr/
https://ips.zscalertwo.net/cenr/
https://ips.zscalerthree.net/cenr/
10 Appendix F: Silver Peak Resources

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