Zscaler Internet Access (ZIA) and Silver Peak SDWAN Deployment Guide

March 2019

Version 1.0
# Table of Contents

1 Document Overview ........................................................................................................ 5  
   1.1 Document Audience .................................................................................................. 5  
   1.2 Software Revisions ................................................................................................. 5  
   1.3 Request for Comments ............................................................................................ 5  
   1.4 Document Prerequisites ......................................................................................... 6  
   1.5 Document Revision Control ................................................................................... 7  
   1.6 Lab Topology and Configuration Overview .......................................................... 8  

2 Configuring ZIA for API Tunnel Provisioning .............................................................. 9  
   2.1 Logging into ZIA ...................................................................................................... 9  
   2.2 Verify Zscaler Internet Access (ZIA) State ............................................................ 10  
      2.2.1 Check for existing Locations ............................................................................ 10  
      2.2.2 Verify Locations .............................................................................................. 11  
      2.2.3 Check for existing VPN Credentials ............................................................... 12  
      2.2.4 Verify VPN Credential ..................................................................................... 13  
   2.3 Configure ZIA for API Access ............................................................................... 14  
      2.3.1 Adding SD-WAN Partner Key ......................................................................... 15  
      2.3.2 Add SD-WAN Partner Key .............................................................................. 16  
      2.3.3 Verify SD-WAN Partner Key .......................................................................... 17  
      2.3.4 Adding a Partner Administrator Role .............................................................. 18  
      2.3.5 Add Partner Administrator Role ...................................................................... 19  
      2.3.6 Creating Partner Administrator Role ............................................................... 20  
      2.3.7 Administrator Management ............................................................................ 21  
      2.3.8 Add Partner Administrator ............................................................................. 22  
      2.3.9 Creating Partner Administrator ...................................................................... 23  
      2.3.10 Active Pending Changes .............................................................................. 24  
      2.3.11 Verify Activation ............................................................................................ 25  

3 Configuring Silver Peak Unity Orchestrator ............................................................... 26  
   3.1 Verify Access to Unity Orchestrator ...................................................................... 27  
      3.1.1 Log into Unity Orchestrator ............................................................................ 27  
      3.1.2 Unity Orchestrator Dashboard ....................................................................... 28  
      3.1.3 Configure Zscaler Internet Access Settings in Orchestrator ......................... 29  
      3.1.4 Configuring ZIA Subscription in Orchestrator ................................................. 30  
      3.1.5 Verify ZIA Subscription Settings ..................................................................... 31  
      3.1.6 Alternative Way To Verify ZIA Subscription Settings ................................... 32  
      3.1.7 ZIA Tunnel Settings ......................................................................................... 33  
      3.1.8 Zscaler Tunnel Setting Defaults .................................................................... 34  
      3.1.9 Verify Tunnel Setting .................................................................................... 35  
      3.1.10 Verify Interface labels from the deployment .................................................. 36  
      3.1.11 Verify WAN interface label names ................................................................. 37  
      3.1.12 Select Interface Order .................................................................................... 38  
      3.1.13 Configure Business Intent Overlay .............................................................. 39
3.1.14 Set the Preferred Policy Order for Internet Traffic ................................................. 40
3.1.15 Preferred Policy Order with Zscaler Cloud as the primary .................................. 41
3.1.16 Save Business Intent Overlay ................................................................................. 42
3.1.17 Verify Zscaler Status in Orchestrator ..................................................................... 43
3.1.18 Verify Locations and VPN Credentials in ZIA Admin UI ...................................... 44

4 Verify Configuration with Zscaler Test Page ................................................................. 45
  4.1 Request Verification Page ......................................................................................... 45

5 Requesting Zscaler Support ......................................................................................... 46
  5.1 Gather Support Information .................................................................................... 46
    5.1.1 Obtain Company ID ......................................................................................... 46
    5.1.2 Save Company ID ............................................................................................ 47
    5.1.3 Enter Support Section .................................................................................... 48

6 Appendix A: Zscaler Resources .................................................................................... 49

7 Appendix B: Silver Peak Resources .............................................................................. 50
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC2409)</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security (RFC2411)</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 (RFC6101)</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security (RFC5246)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC7239)</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>
1 Document Overview

This Deployment Guide document will provide GUI and CLI examples for configuring Zscaler Internet Access (ZIA) and Silver Peak SD-WAN. The guide is intended for standing up proof-on-concept topologies and demos, for evaluating interoperability, and joint integration. This guide should not be used to configure either vendor platform for production use. For production deployments, please contact Zscaler or Silver Peak for post-sale deployment assistance.

**Note:** This document explains how to configure ZIA and Silver Peak Unity Orchestrator for automating the provisioning of IPsec using the ZIA API. At this time, only IPsec is supported using the ZIA API. If you want to enable GRE, this can be manually configured in Silver Peak Unity Orchestrator. For more details, please view this document:


1.1 Document Audience

This document was designed for Network Engineers and Network Architects. All examples in this guide presume the reader has a basic comprehension of IP Networking. For additional product and company resources, please refer to the Appendix section.

1.2 Software Revisions

This document was written using Zscaler Internet Access v5.7 and Silver Peak Unity Orchestrator 8.6.0.40399.

1.3 Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact partner-doc-support@zscaler.com.
1.4 Document Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 5.6 (or newer)
- Administrator login credentials to ZIA

Silver Peak

- A working instance of Silver Peak Unity Orchestrator 8.6, or greater, with administrator login credentials.
- One or more Unity EdgeConnect appliances online and working
## 1.5 Document Revision Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Change Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>March 2019</td>
<td>Initial document created by Zscaler and Silver Peak</td>
</tr>
</tbody>
</table>
1.6 Lab Topology and Configuration Overview

This document is based on the following lab topology with two branch offices. One location is “SilverPeak-Site-A” and the other location is “Silverpeak-Site-B”. Both Unity EdgeConnect appliances at these branches will tunnel to Zscaler using IPsec. These IPsec tunnels will be configured by Unity Orchestrator making API calls to ZIA. Each of the EdgeConnect appliances will have three WAN interfaces configured. Two of the three WAN interfaces are used to build the tunnels with Silver Peak Unity Orchestrator for automating the provisioning of IPsec using the ZIA API.

Figure 1: Lab Topology Diagram

Note: This topology and proposed configuration is for demonstration purposes and is not necessarily what should be deployed by customers.
2 Configuring ZIA for API Tunnel Provisioning

2.1 Logging into ZIA

First, we will setup the Zscaler side of this service. The required steps for this section are:

- Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, please contact support: https://help.zscaler.com/submit-ticket.
2.2 Verify Zscaler Internet Access (ZIA) State

2.2.1 Check for existing Locations

If your ZIA instance is new, there should not be any “Locations” present. To verify if Locations have been configured, please use the navigation below, also shown in Figure 3 below.

Navigation: Administration -> Resources -> and then click Locations.

Figure 3: Navigate to Locations
2.2.2 Verify Locations

In Figure 4, if you see “No Matching Items Found”, your ZIA instance does not have any locations configured. Remember how to navigate to this section in the ZIA admin UI. This section of the ZIA admin UI console will show locations configured by Silver Peak Unity, later in this deployment guide.

![Figure 4: Verify Location](image)

**Note:** It is common for ZIA deployments to have 1 location per physical location. The amount of locations can scale to the largest of Enterprise networks.
2.2.3 Check for existing VPN Credentials

If your ZIA instance is new, there should not be any “VPN Credentials” present. To verify if VPN Credentials have been configured, please use the navigation below, also shown in Figure 5 below.

**Navigation**: Administration -> Resources -> and then click VPN Credentials.

![Figure 5: Navigate to VPN Credentials](image)
2.2.4 Verify VPN Credential

In Figure 6, if you see “No Matching Items Found”, your ZIA instance does not have any VPN Credentials configured. Remember how to navigate to this section in the ZIA admin UI. This section of the ZIA admin UI console will show locations configured by Silver Peak Unity, later in this deployment guide.

Figure 6: Verify VPN Credentials
2.3 **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 7.

**Navigation:** Administration -> Cloud Configuration -> and then click **Partner Integrations**

![Figure 7: Configuring ZIA for API Access](image-url)
2.3.1 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 8.

Figure 8: Add Partner Key
2.3.2 Add SD-WAN Partner Key

A window will appear, as shown in Figure 9. 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 9: Add SD-WAN Partner Key
2.3.3 Verify SD-WAN Partner Key

Once you return to the screen shown in Figure 10, 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 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 Unity Orchestrator.

![Partner Integrations](image)

**Figure 10: Verify SD-WAN Partner Key**

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

Figure 11: Adding Partner Administrator Role
2.3.5 Add Partner Administrator Role

Figure 12: Add Partner Administrator Role
2.3.6 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 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 13: Creating Partner Administrator Role](image-url)
2.3.7 Administrator Management

The last step required is creating a Partner Administrator. Please follow the navigation below, which is also depicted in Figure 14.

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

Figure 14: Administrator Management
2.3.8 Add Partner Administrator

Once you arrive to the “Administrator Management” page, please select “Add Partner Administrator”, as show in Figure 15. A user input screen will appear, which is shown in the next section.

![Figure 15: Admin Partner Administrator](image-url)
2.3.9 Creating Partner Administrator

Once the “Add Partner Administrator” input box appears, fill in the fields with red boxes around then, as shown in Figure 16. Once this is completed, click “Save”.

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

![Add Partner Administrator](image)

**Figure 16: Creating Partner Administrator**
2.3.10 **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 17*.

![Figure 17: Active Pending Changes](image-url)
2.3.11 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 18.

**Figure 18: Verify Activation**
3 Configuring Silver Peak Unity Orchestrator

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-url)

Page 26 of 50
3.1 Verify Access to Unity Orchestrator

3.1.1 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](image)
3.1.2 Unity Orchestrator Dashboard

After logging into Orchestrator successfully, you will arrive at the dashboard. As mentioned at the beginning of this section, our lab has two devices with minimal traffic, so status screens graphs, and gauges will not be rich in data. From here we are ready to start configuring Unity Orchestrator to initiate API calls to ZIA.

![Orchestrator Dashboard view](image-url)

Figure 22: Orchestrator Dashboard view
3.1.3 Configure Zscaler Internet Access Settings in Orchestrator

First, let’s configure the global ZIA settings. This consists of the data you were asked to save (e.g. Partner Key, …etc). Go to “Configuration menu” then Networking navigate to “Zscaler Internet Access” and select it, as shown in Figure 23.

![Figure 23: Navigating to Configure ZIA API Settings in Orchestrator](image-url)
3.1.4 Configuring ZIA Subscription in Orchestrator

Select the “Subscription” tab to enter our ZIA API Partner credentials. Fill in the required information. See the highlighted red box shown in Figure 24, enter in the ZIA API settings you were asked to save. When finished, click “Save” and return to the prior screen to verify the connection to the Zscaler cloud portal.

Figure 24: Configuring ZIA Subscription
3.1.5 Verify ZIA Subscription Settings

After entering and saving your ZIA Subscription settings, verify the green box at the bottom of the screen shows a successful Zscaler account update, as shown in Figure 25. If you receive an error, please return to the prior step and reenter the data or contact ZScaler support.

Figure 25: Verify ZIA Subscription Settings
3.1.6 Alternative Way To Verify ZIA Subscription Settings

Return to the Zscaler Subscription tab once more and will see a green or orange indication in the Zscaler API credentials are correct. An example is shown in Figure 26, below.

![Subscription Settings](image)

Figure 26: Verify ZIA Subscription Settings show a connection to Zscaler
3.1.7 ZIA Tunnel Settings

Next configure the tunnel settings, as shown in Figure 27.

Figure 27: ZIA Tunnel Settings
3.1.8 Zscaler Tunnel Setting Defaults

This step may be redundant, but just in case, please click “Use Zscaler Default” to ensure the proper settings are applied.

Figure 28: Zscaler Tunnel Setting Defaults
3.1.9 Verify Tunnel Setting

After saving the tunnel settings a green banner will appear stating “Update Zscaler tunnel setting successfully”. The next step is to configure the interfaces that will be used to build the tunnels.

![Figure 29: Verify Tunnel Settings](image-url)
3.1.10 Verify Interface labels from the deployment

Before selecting the interface labels in the Zscaler Internet Access settings, we need to verify the deployment configuration for the EdgeConnect appliance. The deployment will show the interface label name used for the WAN transports. Select the EdgeConnect appliance then select Appliance menu followed by Deployment as shown in Figure 30.

Figure 30: Selecting Deployment from the Appliance Menu
3.1.11 Verify WAN interface label names

The label names are highlighted in a red rounded rectangle. The two label names are INET1 for WAN1 and LTE for WAN2. In this example the EdgeConnect appliance has three WAN transports configured WAN0, WAN1 and WAN2. The label name INET1 and LTE will be used for selecting the preferred interface order in ZIA which is the next step in the process.

![Figure 31: Verifying the label name for WAN1](image-url)
3.1.12 Select Interface Order

Next return to the Zscaler Internet Access setting. Drag and drop the INET1 to the Preferred Interface Label Order. INET1 should be on top of the list. If there are more than two interfaces make sure the primary interface is at the top. In Figure 32, we show two interfaces, INET1 as primary and LTE as the backup. Zscaler Internet Access will build the tunnels using the interfaces in the Preferred Interface Label order.

![Figure 32: Drag and Drop Preferred Interface Label Order](image-url)
3.1.13 Configure Business Intent Overlay

After completing the preferred interface label order for Zscaler Internet Access. Go to Configuration Menu and under OVERLAYS select Business Intent Overlays.

![Business Intent Overlays menu](image)

Figure 33: Selecting the Business Intent Overlays menu
3.1.14 Set the Preferred Policy Order for Internet Traffic

In the Business Intent Overlay screen, select the Overlay name you like to configure to use Zscaler cloud. Keep in mind as you make edits to the overlay it will be a global change and it will affect all appliances that have the overlay applied. Last, scroll down to the Internet Traffic and click on the policy Zscaler Cloud and hold then drag it over to the top of Break out locally.

Figure 34: Configure Preferred Policy Order in Internet Traffic
3.1.15  **Preferred Policy Order with Zscaler Cloud as the primary**

The policy order as shown in *Figure 35* will send internet bound traffic first to the Zscaler Cloud. If the Zscaler cloud service is unavailable, then it will drop to the next policy. If we are unable to break out locally or backhaul the traffic via the Overlay then all traffic will be dropped per the preferred policy order.

*Figure 35: Example of Policy Order*
3.1.16  **Save Business Intent Overlay**

As we save Overlays, the overlay manager will start the automation process in creating the tunnels to nearest ZEN cloud portal.

![Figure 36: Pending Status](image)

**Figure 36: Pending Status**
3.1.17 Verify Zscaler Status in Orchestrator

That was the last step. We should now start to see the “VPN Credential and Location” status change as tunnels are established. At first, the tunnels should say “Pending”, as shown in Figure 36. Once the tunnels are established to ZIA, the tunnels should say “Deployed”, as shown in Figure 38.

Figure 37: Pending Status

Figure 38: Deployed Status
3.1.18 Verify Locations and VPN Credentials in ZIA Admin UI

At this point in the Deployment Guide, we want to switch back to the ZIA Admin UI. We want to verify that ZIA was configured. We should see VPN Credentials and Locations that correspond to the branch locations in Unity Orchestrator. For our lab, we should see VPN Credentials, as shown in Figure 39.

![Figure 39: Verify VPN Credentials in ZIA Admin UI](image)

We should also see Locations, as shown in Figure 40.

![Figure 40: Verify Locations in ZIA Admin UI](image)
4 Verify Configuration with ZScaler Test Page

4.1 Request Verification Page

The URL https://ip.zscaler.com can be used to validate if you are transiting ZIA. This is what you will see if you are not transiting ZIA.

![Figure 50: Non-working Example](image)

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

![Figure 51: Working Example](image)
5  Requesting Zscaler Support

5.1  Gather Support Information

Zscaler support is required to provision new locations for GRE or IPsec service. Zscaler support is also available to help troubleshoot configuration and service issues, and is available 24/7 hours a day, all year.

5.1.1  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.

![Image of Zscaler interface showing Company Profile]

Figure 52: Obtaining Company ID
5.1.2 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 53: Save Company ID
5.1.3 Enter Support Section

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.

Figure 54: Enter Support Section
6 Appendix A: Zscaler Resources

Zscaler: Getting Started
https://help.zscaler.com/zia/getting-started

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/
7 Appendix B: 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