



Zscaler and Riverbed Deployment Guide

January 2018

Version 1.3

Table of Contents

1	About This Document	3
2	Zscaler and Riverbed	5
2.1	Prerequisites	5
3	Configuring IPsec from Riverbed to ZIA	6
3.1	Configuring Riverbed Steel Connect Manager (SCM)	7
3.1.1	Log into SteelConnect Manager (SCM)	7
3.1.2	SteelConnect Manager Dashboard	8
3.1.3	SteelConnect Manager Network Design	9
3.1.4	Configuring Zscaler in Network Design	10
3.1.5	Downloading VPN Config	11
3.1.6	Logging into ZIA	12
3.1.7	ZIA Dashboard	13
3.1.8	Import VPN Credentials	14
3.1.9	VPN Credential Import Status	15
3.1.10	Activate VPN Credential Changes	16
3.1.11	Locations	17
3.1.12	Adding Location	18
3.1.13	Activate Location Changes	19
3.1.14	Verifying Tunnel Activation in SCM	20
3.1.15	Quick Recap	21
3.1.16	Enable Break-out Routing Towards Zscaler	22
4	Requesting Zscaler Support	23
4.1	Gather Support Information	23
4.1.1	Obtain Company ID	23
4.1.2	Save Company ID	24
4.1.3	Open Support Ticket	25
4.2	GRE Provisioning Request (Example)	26
4.3	Adding Domain (Example)	27
5	Verifying ZIA Configuration	28
5.1	Request Verification Page	28
6	Appendix A: Zscaler Resources	29
7	Appendix B: Riverbed Resources	30

Terms and Acronyms

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DPD	Dead Peer Detection (<i>RFC 3706</i>)
GRE	Generic Routing Encapsulation (<i>RFC2890</i>)
IKE	Internet Key Exchange (<i>RFC2409</i>)
IPSec	Internet Protocol Security (<i>RFC2411</i>)
PFS	Perfect Forward Secrecy
SCM	SteelConnect Manager (Riverbed)
SSL	Secure Socket Layer (<i>RFC6101</i>)
XFF	X-Forwarded-For (<i>RFC7239</i>)
ZIA	Zscaler Internet Access (Zscaler)
ZEN	Zscaler Enforcement Node (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

1 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.

Riverbed Overview

Riverbed as a company has a long legacy of market leadership. Riverbed pioneered WAN optimization, and since then, has expanded their solutions for the software-defined era. Riverbed's SD-WAN (software-defined WAN) solution provides a powerful yet simple solution for designing, deploying and managing distributed networks for today's cloud-connected enterprises. Riverbed is at the center of hybrid networking, the cloud, SD-WAN, SaaS, mobile, big data, and infrastructure visibility. In short, Riverbed is building a software-defined architecture for digital business. For more information on Riverbed, please visit www.riverbed.com.

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 v5.5 and Riverbed SteelConnect v2.9.1.50.

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.

2 Zscaler and Riverbed

2.1 Prerequisites

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

Zscaler Internet Access (ZIA)

- A working instance of ZIA
- Administrator login credentials

SteelConnect Manager (SCM)

- A working instance of SteelConnect
- Administrator login credentials
- One or more SD-WAN capable appliances with “Online” status in SCM

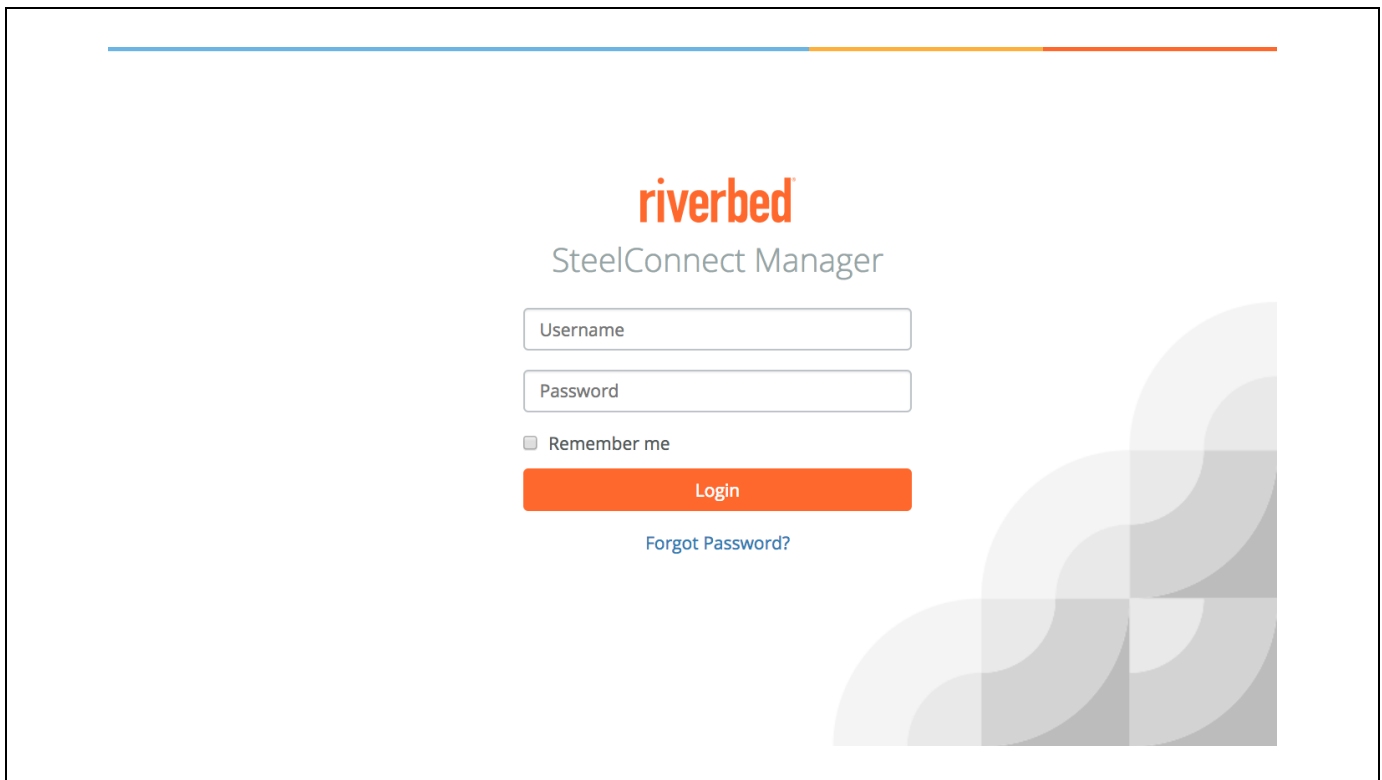
3 Configuring IPsec from Riverbed to ZIA

This section will require access to two separate management portals. Riverbed SteelConnect Gateway devices are configured using SteelConnect Manager. Zscaler Internet Access service is configured through the Zscaler admin. Both admin consoles are web-based portals.

3.1 Configuring Riverbed Steel Connect Manager (SCM)

3.1.1 Log into SteelConnect Manager (SCM)

Open a web browser and enter the URL to your SteelConnect Manager instance. When the page loads, you should see the screen in *Figure 1: SteelConnect Manager Portal Login*.



The image shows the login page for the SteelConnect Manager portal. At the top, there is a horizontal bar with a blue-to-orange gradient. Below this, the "riverbed" logo is displayed in orange, followed by the text "SteelConnect Manager" in a smaller, grey font. The login form consists of two input fields: "Username" and "Password". Below these fields is a checkbox labeled "Remember me". A prominent orange "Login" button is positioned below the checkbox. Underneath the button is a blue link that says "Forgot Password?". The right side of the page features a decorative graphic of overlapping grey circles.

Figure 1: SteelConnect Manager Portal Login

If you are unable to log into SteelConnect Manager, you can contact Riverbed support: https://support.riverbed.com/content/support/contact_support.html.

3.1.2 SteelConnect Manager Dashboard

After logging into SteelConnect Manager, you will arrive at the SteelConnect Manager “Dashboard”, shown in *Figure 2: SteelConnect Manager Dashboard*. The SteelConnect dashboard will display a geographic map of your sites. On the left side of the screen, you will see drop-down menus to navigate through SteelConnect Manager.

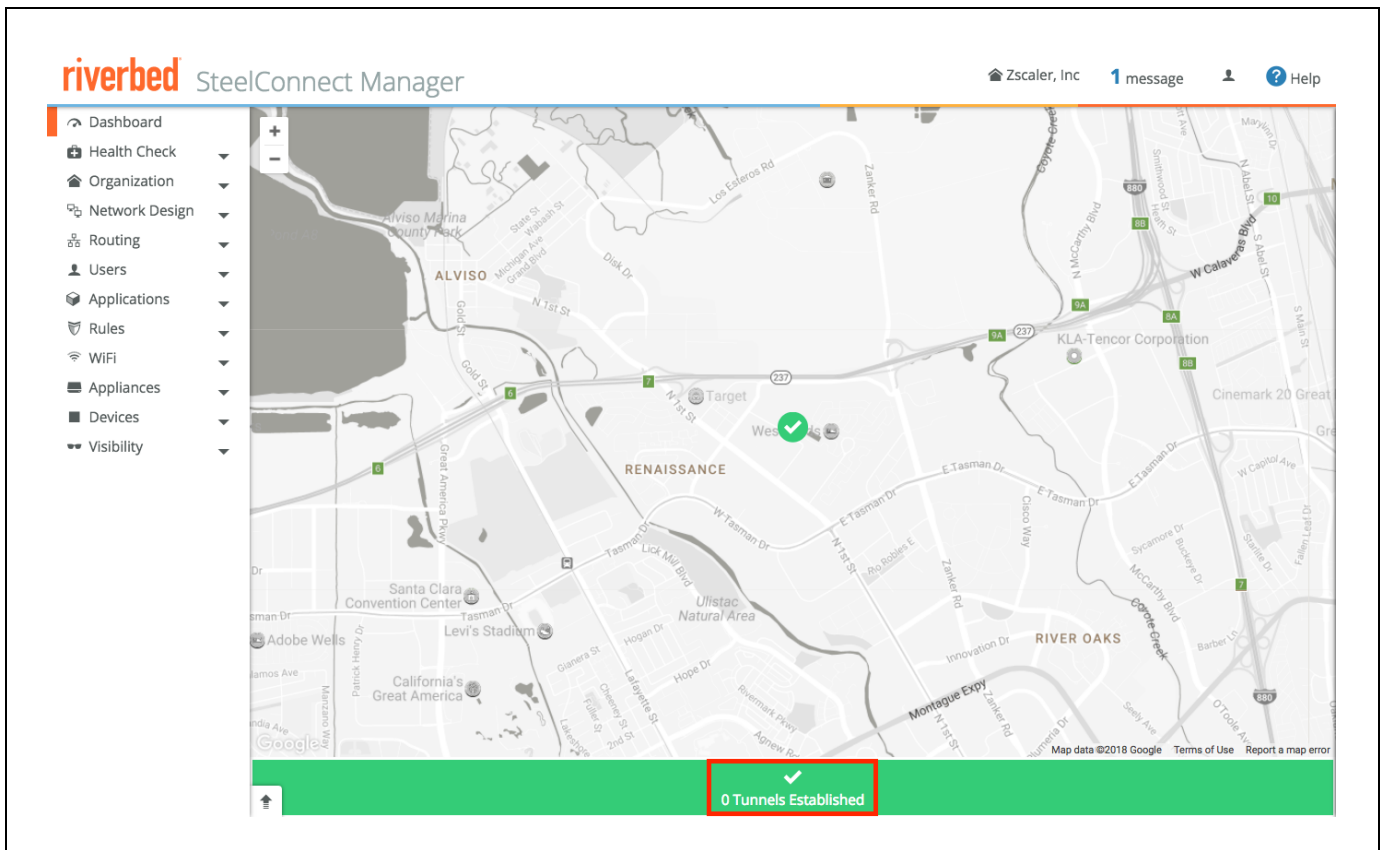
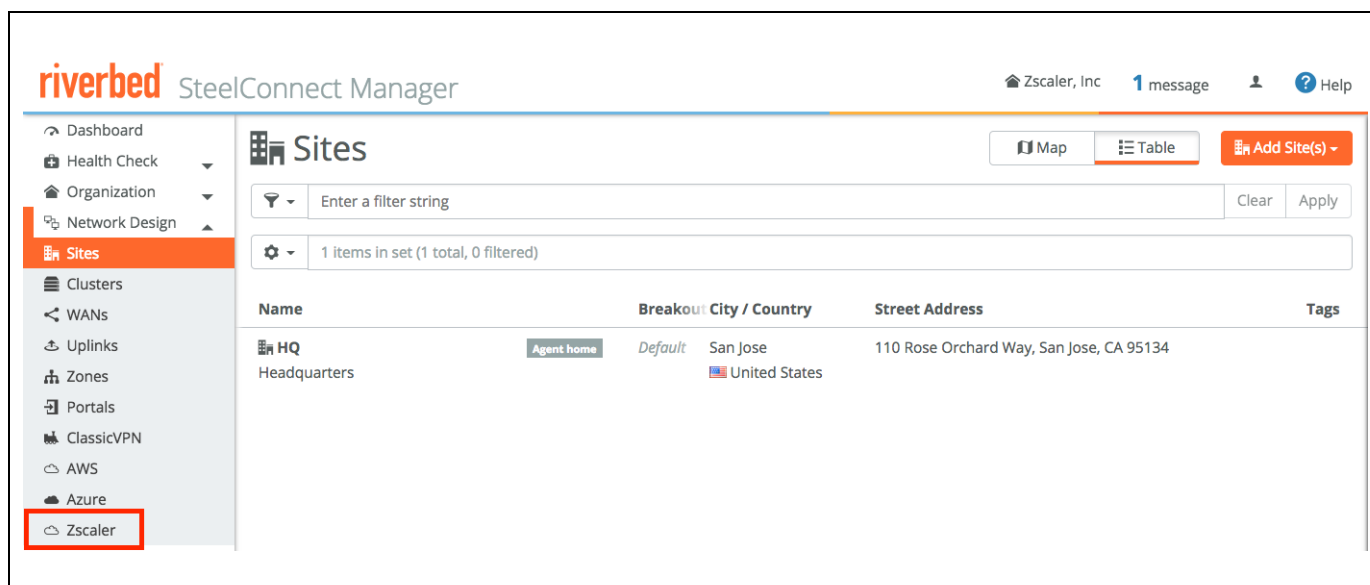


Figure 2: SteelConnect Manager Dashboard

In the upper right, you may have messages to read. On the bottom of the page, you will see a summary of the quantity of tunnels that are established. Although the device we are using for this guide is online, no tunnels are provisioned at this time, and therefore zero tunnels are established.

3.1.3 SteelConnect Manager Network Design

To start configuring SteelConnect Manager for ZIA, we first need to navigate to **Network Design** -> **Zscaler**. After clicking on Network Design, the screen should update and look similar to *Figure 3: Network Design*.



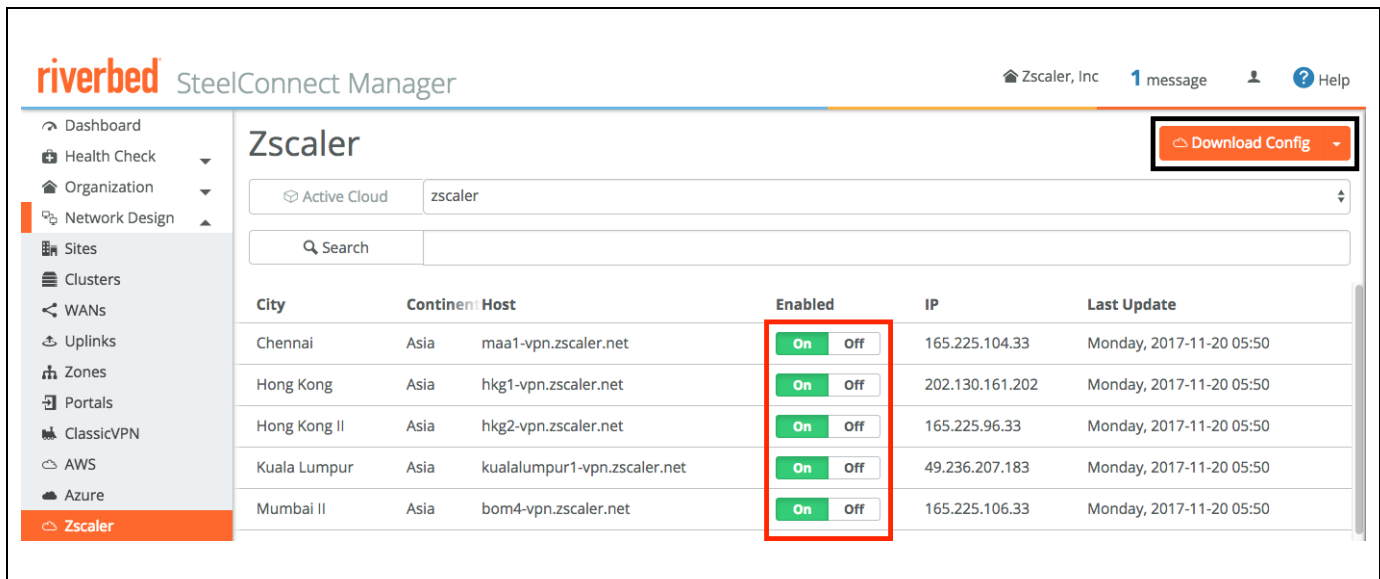
The screenshot shows the Riverbed SteelConnect Manager interface. The left sidebar contains a navigation menu with the following items: Dashboard, Health Check, Organization, Network Design, Sites (highlighted), Clusters, WANs, Uplinks, Zones, Portals, ClassicVPN, AWS, Azure, and Zscaler (highlighted with a red box). The main content area is titled 'Sites' and includes a search bar, a filter button, and a table of sites. The table has the following columns: Name, Breakout City / Country, Street Address, and Tags. The table contains one row for the 'HQ' site, which is the 'Headquarters' located in 'San Jose, United States' at '110 Rose Orchard Way, San Jose, CA 95134'. The 'Tags' column for this site includes 'Agent home' and 'Default'.

Name	Breakout City / Country	Street Address	Tags
HQ Headquarters	San Jose United States	110 Rose Orchard Way, San Jose, CA 95134	Agent home Default

Figure 3: Network Design

3.1.4 Configuring Zscaler in Network Design

After selecting **Zscaler** in **Network Design**, the screen should look similar to *Figure 4: Configuring Zscaler in Network Design*.



City	Continent	Host	Enabled	IP	Last Update
Chennai	Asia	maa1-vpn.zscaler.net	On	165.225.104.33	Monday, 2017-11-20 05:50
Hong Kong	Asia	hkg1-vpn.zscaler.net	On	202.130.161.202	Monday, 2017-11-20 05:50
Hong Kong II	Asia	hkg2-vpn.zscaler.net	On	165.225.96.33	Monday, 2017-11-20 05:50
Kuala Lumpur	Asia	kualalumpur1-vpn.zscaler.net	On	49.236.207.183	Monday, 2017-11-20 05:50
Mumbai II	Asia	bom4-vpn.zscaler.net	On	165.225.106.33	Monday, 2017-11-20 05:50

Figure 4: Configuring Zscaler in Network Design

There are two areas on this screen we want to focus on. First, the red box around the **Enabled** click boxes. This is where you can toggle which ZIA ZENs are eligible for use. By default, all ZIA ZENs are toggled to “On” (enabled). The second area we want to focus on is the black box around the **Download Config** button. This button will generate a csv file of VPN configuration parameters, which we will import into Zscaler. This will reduce the amount of manual data entry required once we configure the Zscaler side for IPsec.

Note: *Figure 4* states that the *Active Cloud* is “Zscaler”. This document was written using the “zscalerbeta” cloud. The *Active Cloud* setting must align to your Zscaler account.

3.1.5 Downloading VPN Config

After selecting **Download Config**, the screen should present a pop-up. The pop-up will provide you a domain name that must be added to your ZIA account. This domain will be used for FQDN-base IPsec authentication.

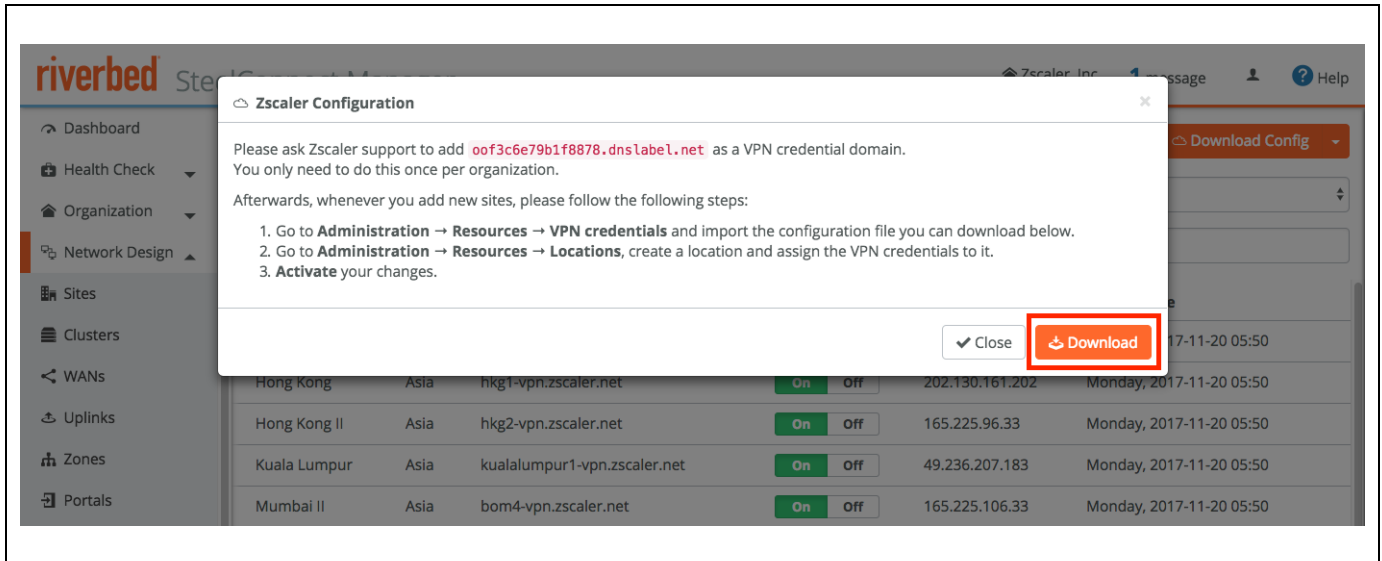


Figure 5: Downloading VPN Config

After you save the domain name, select **Download**, which in *Figure 4* has a red box around the button. Your browser will then start downloading the csv file. Make sure you remember where this file is saved to later import in ZIA.

3.1.6 Logging into ZIA

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>.



The screenshot shows the Zscaler login interface. At the top left is the Zscaler logo. To its right are two input fields: 'LOGIN ID' containing 'admin@domain.com' and 'PASSWORD' containing '*****'. A red rectangle highlights these two fields. To the right of the password field is a blue 'Sign In' button. Below the login fields are two options: a checkbox for 'Remember my Login ID' and a language selector set to 'English (US)'. Below the login form is a large banner image showing a keyboard and a laptop. The banner text reads 'What Comes After VPN?' followed by 'Enabling Application Access with Zscaler' and a 'Watch Now' button.

Figure 6: Log Into Zscaler

3.1.7 ZIA Dashboard

After logging into Zscaler, you will arrive at the Zscaler Dashboard, as shown in *Figure 7*. From here we want to navigate to **Administration** -> **Resources** -> **VPN Credentials**.

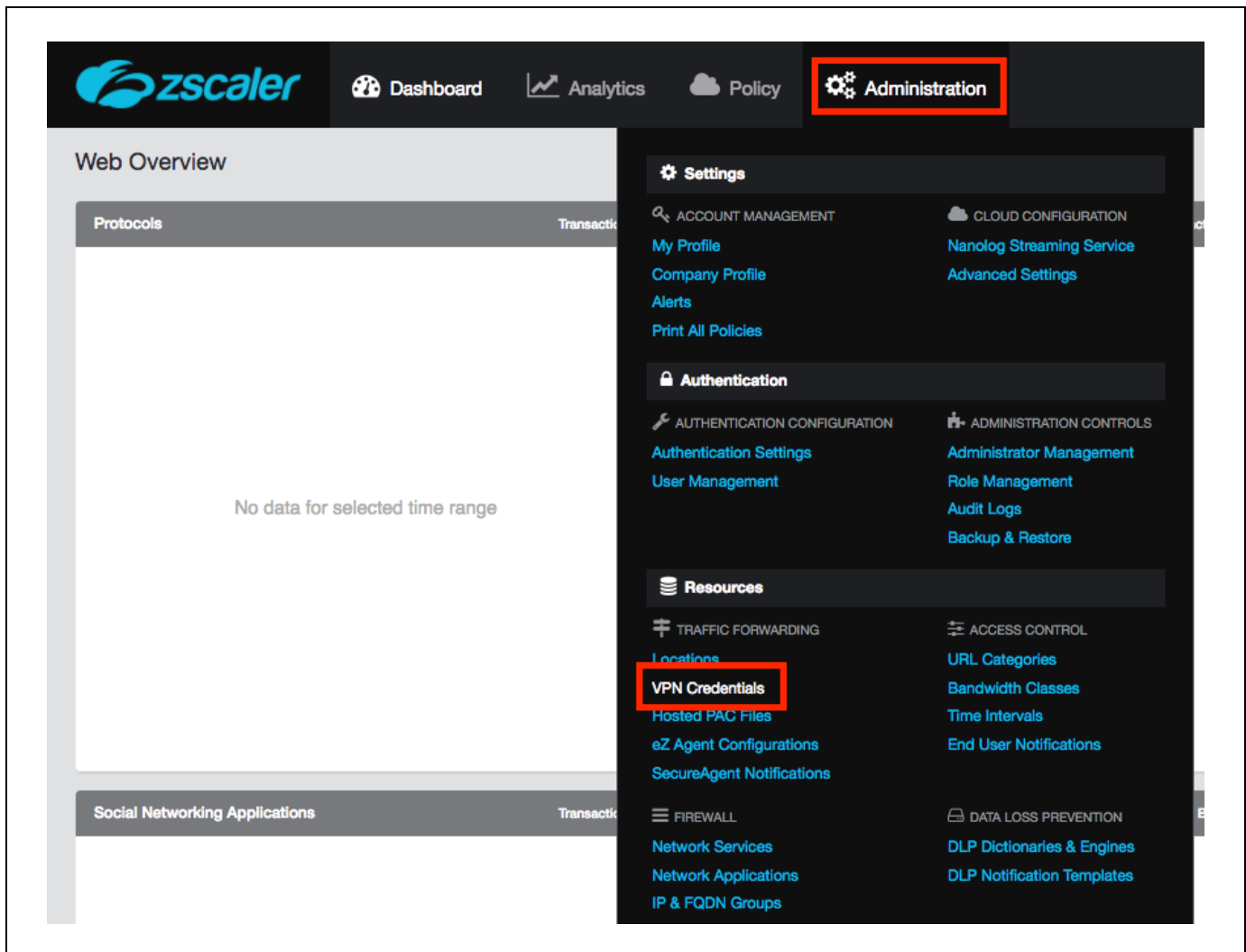


Figure 7: Navigate to Resources -> VPN Credentials

3.1.8 Import VPN Credentials

After navigating to the VPN Credentials section of Zscaler, look for the Import button, as shown in *Figure 8*. After selecting this option, you will be prompted to select a file to upload. The file you need to provide is the .csv file that was generate by SteelConnect Manager, which contained the VPN settings.

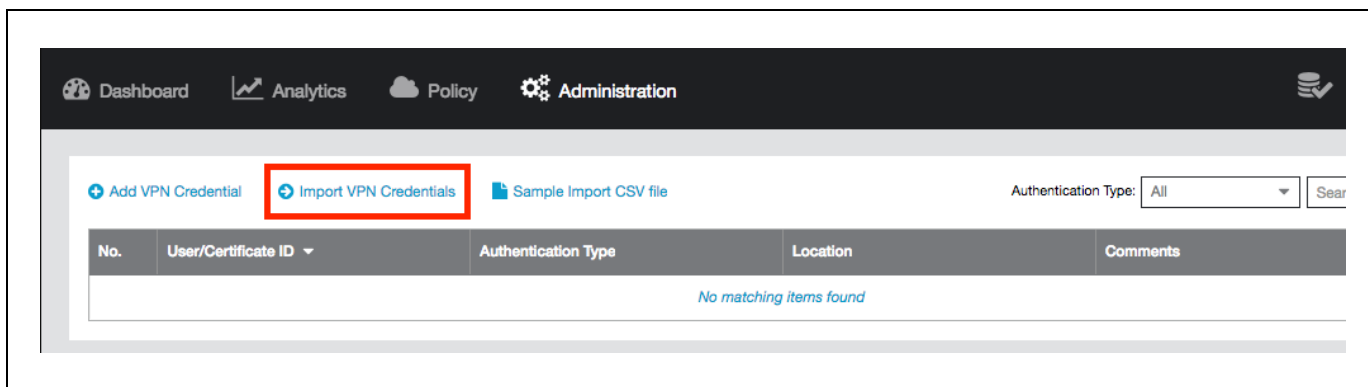


Figure 8: Import VPN Credentials

3.1.9 VPN Credential Import Status

After you upload the .csv file to Zscaler, you should see at the top of the screen “CSV File Import Complete”, as shown in *Figure 9*. A pop-up window should also be present, which will provide more details to the actual import process.

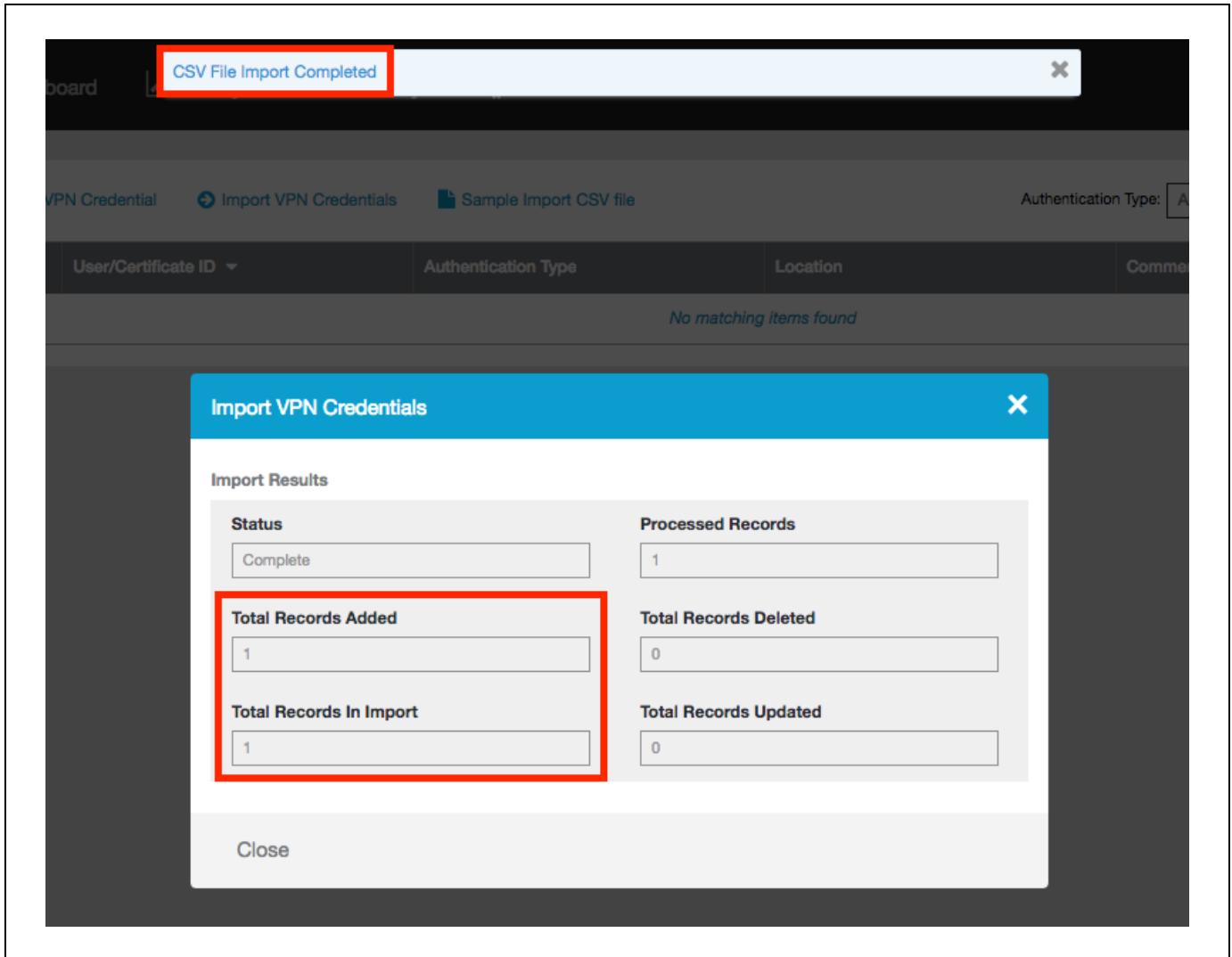


Figure 9: VPN Credential Import Status

In the example shown in Figure 9, we successfully added 1 record, which also was the only record we imported. These import results will vary depending on the quantity of devices you are importing and based on how many records may be present from prior imports.

3.1.10 Activate VPN Credential Changes

After closing **Import Results** pop-up, you should see “All Changes have been saved” at the top of your screen, as shown in Figure 10. You should also see in the upper-right that a pending change needs to be activated. Until this change is activated, this change will not go live in Zscaler.

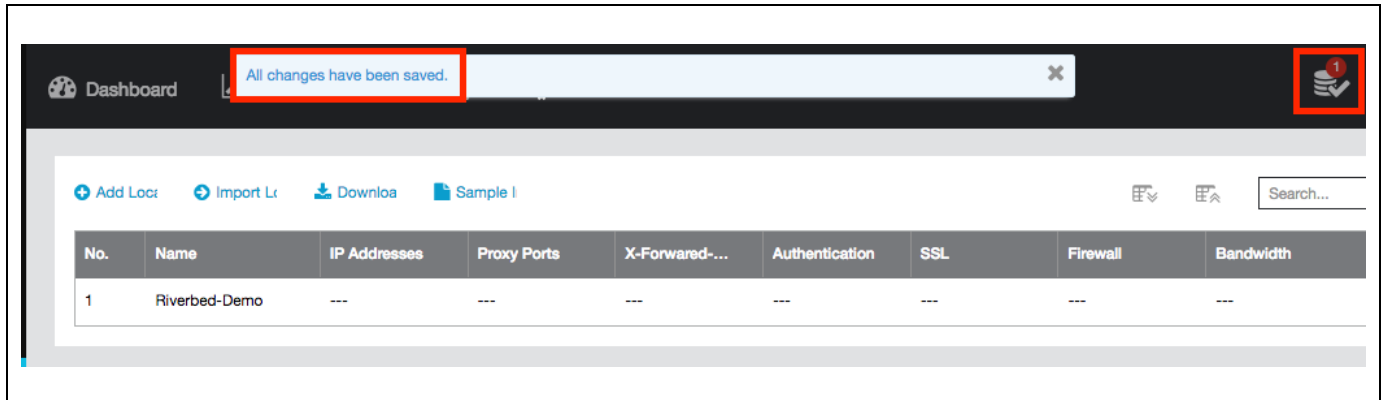


Figure 10: Active VPN Credential Changes

3.1.11 Locations

Next we need to create a location for the VPN Credentials we uploaded. This tab can be found above where we selected VPN Credentials, **Administration** -> **Resources** -> **Locations**.

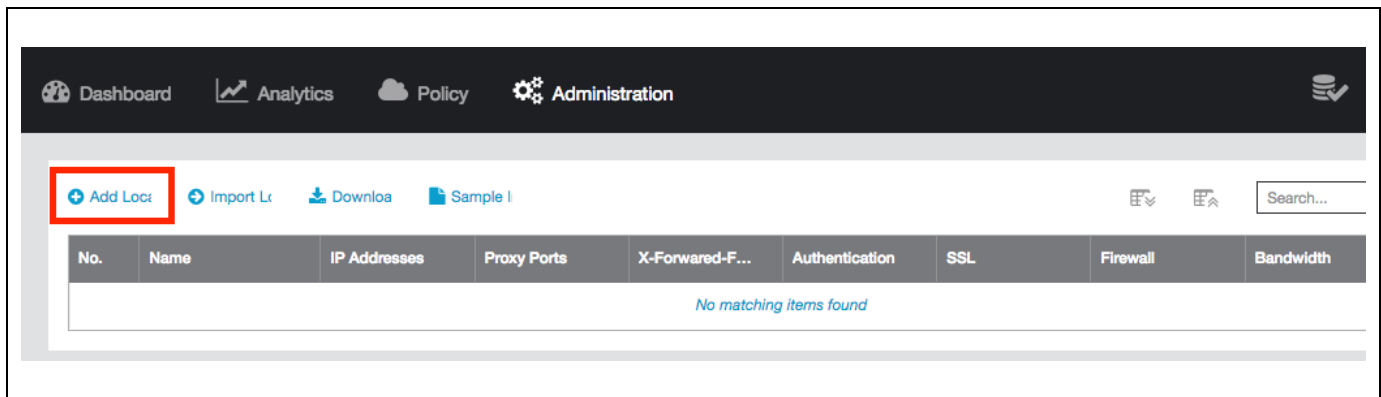


Figure 11: Locations

After navigating to Locations, as shown in *Figure 11*, look for Add Locations. This has a red square around it in *Figure 11*, and select it.

3.1.12 Adding Location

Once selecting **Add Location**, the screen should look similar to Figure 12. You will need to populate the Name, Country, State/Province, Time Zone, and VPN Credentials fields.

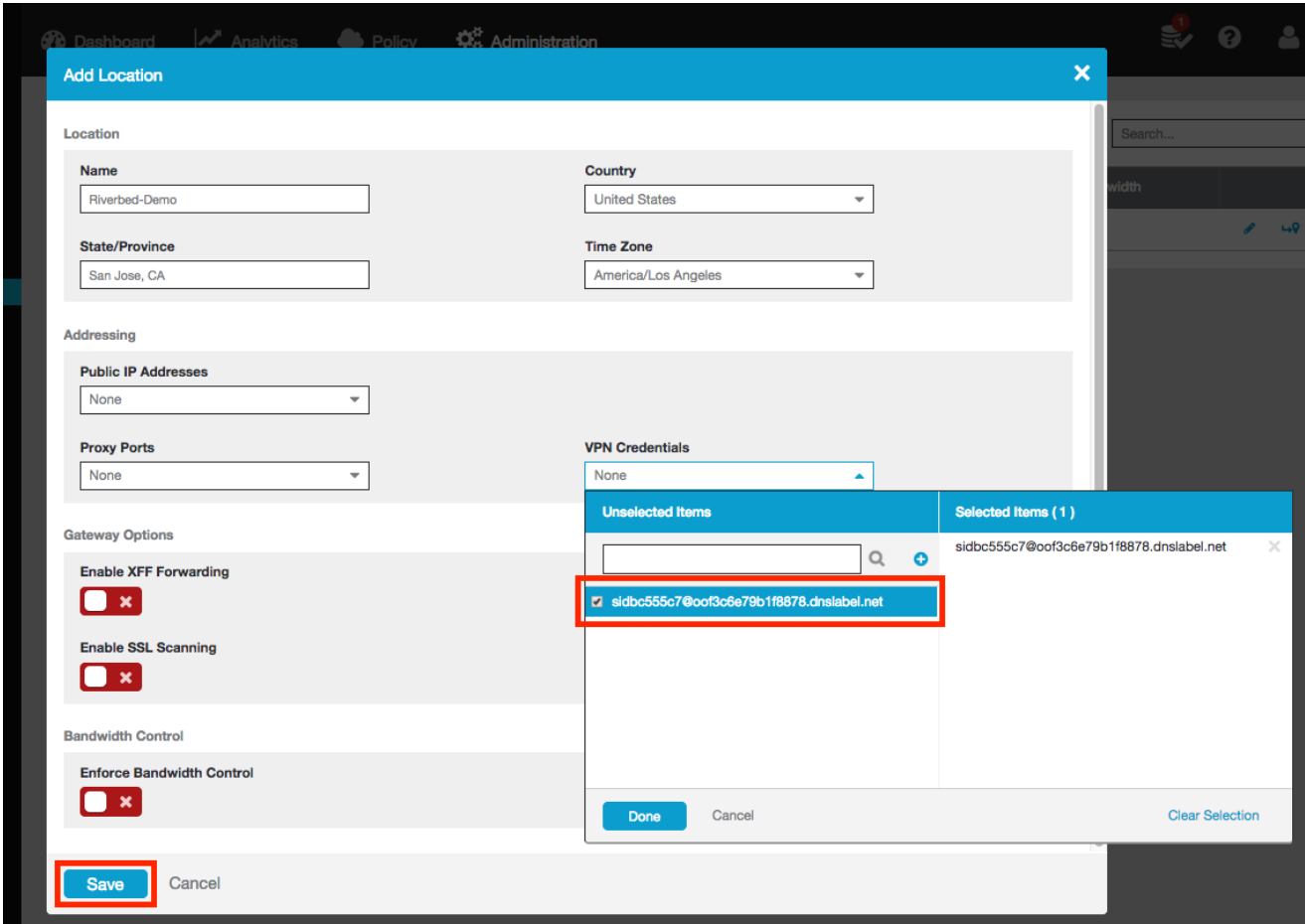


Figure 12: Adding a Location

In the VPN Credentials section, you should see one or more FQDNs. In our lab example, we only have one FQDN to select, which was provided in the .csv file we imported from Riverbed. After completing all fields, select **Save** to continue.

3.1.13 Activate Location Changes

After saving the new location, you should see the screen refresh. Look at the top of your screen and you should see “All changes have been saved”, as shown in *Figure 13*. You should also see in the upper right corner that we again have pending changes that require activation. Activate these changes. Next we will transition back to the SteelConnect Manager.

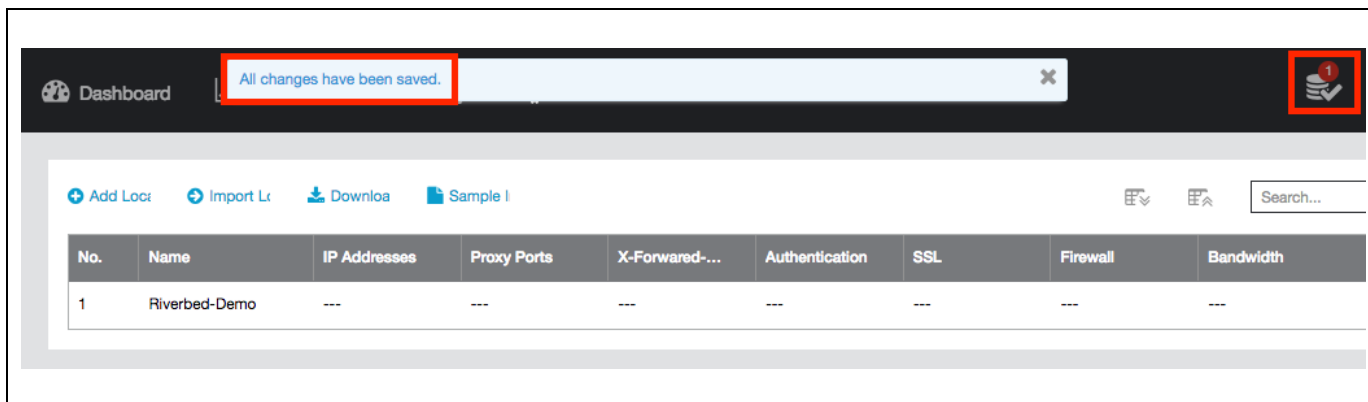


Figure 13: Activating Location Changes

3.1.14 Verifying Tunnel Activation in SCM

If you are not back in SteelConnect Manager, please open it. If everything has been configured correctly to this point, you should see at the bottom of your screen the IPsec tunnels coming “online”, as shown in *Figure 14*.

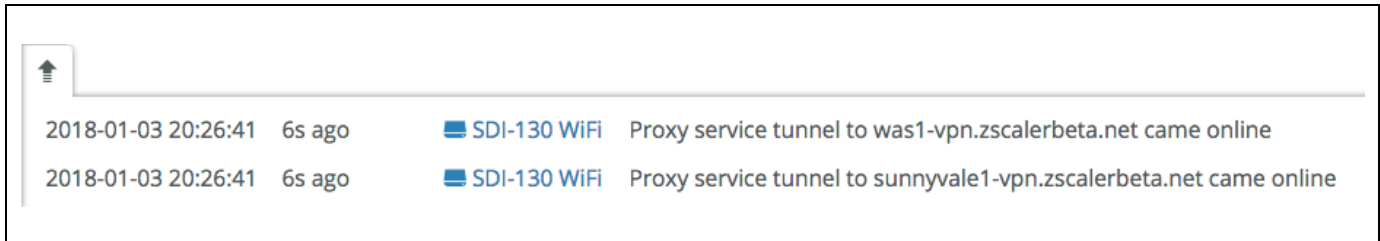


Figure 14: Verifying Tunnel Activation

If you return to the SteelConnect Manager Dashboard, you should now see the Tunnels Established quantity increase by 2, as shown in *Figure 15*:

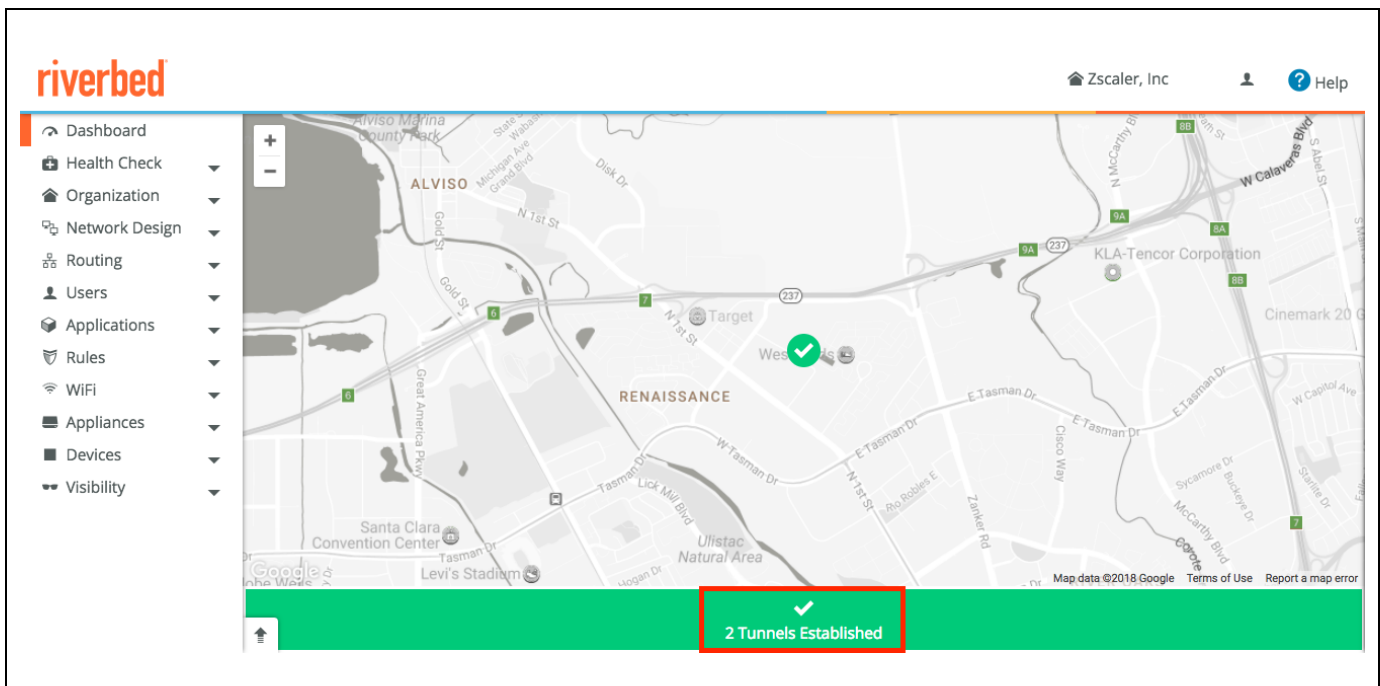


Figure 15: Tunnels Established on SCM Dashboard

3.1.15 Quick Recap

At this point, let's highlight a few points that may not be obvious:

1) Although Zscaler has over 100 datacenters around the world, we never had to specify which branch location points to which Zscaler datacenter. This is because SteelConnect Manager is able to determine the closest Zscaler datacenters by latency testing, and then establish tunnels to the best performing locations.

2) We have IPsec tunnels up, yet we have never seen any IPsec configuration parameters. This is because Riverbed knows Zscaler preferred settings and has set them for you.

3.1.16 Enable Break-out Routing Towards Zscaler

If our tunnels are online at this point, we have one last major step. Although the tunnels are established, SteelConnect Manager needs to be configured to change how it handles break-out routing. At present, all Internet based traffic will egress through the Internet connection. We need to configure SteelConnect Manager to instead send all Internet based traffic through the tunnels to Zscaler.

In SteelConnect Manager, we need to navigate to **Organization -> Networking Defaults**.

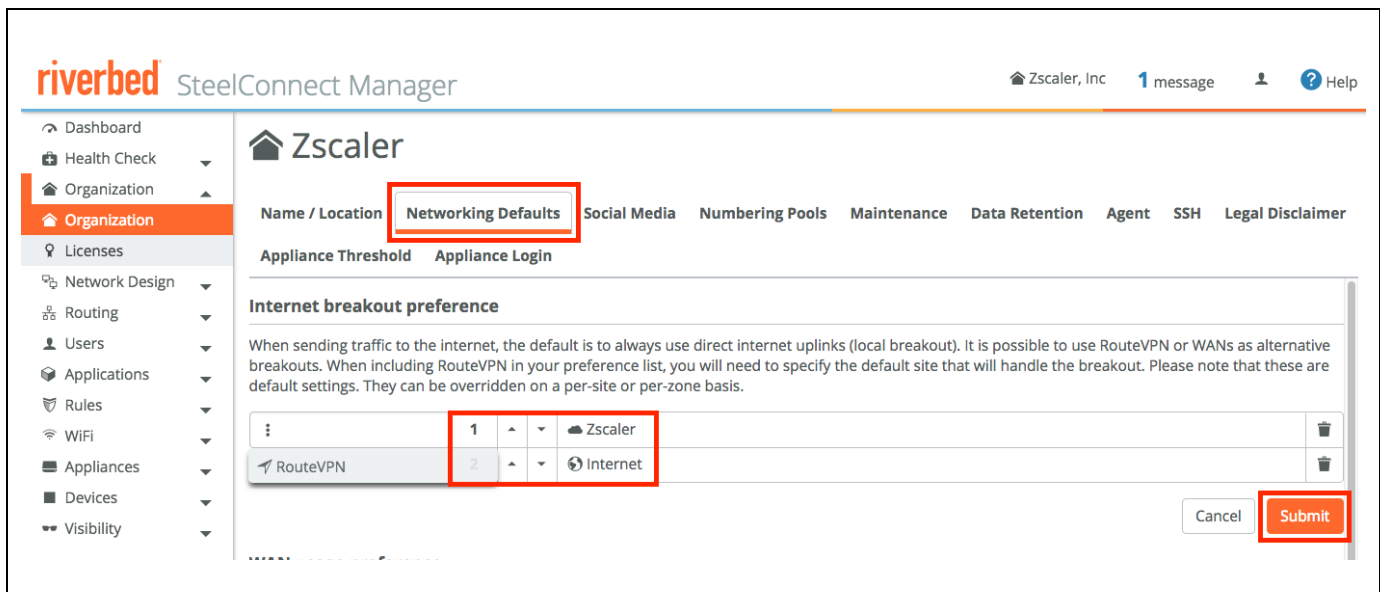


Figure 16: Activating Location Changes

Once to navigate to **Network Defaults**, you need to add **Zscaler** and move it to the #1 position, above **Internet**. This will ensure **Internet traffic** is sent to Zscaler first. Note, **Internet Traffic** is everything except the networks managed and known by SteelConnect Manager. In the unlikely event that Zscaler is not available, traffic will be sent out to the Internet. Note: Each SteelConnect Gateway will have two IPsec tunnels: one to a primary and backup Zscaler datacenter, hence why the unavailability of Zscaler is unlikely.

Note: This global decision can be overridden for exceptions on a *Site*, *Zone*, and specific *Rule* basis.

After selecting **Submit**, we are ready to test if we are transiting Zscaler. Please skip to *Section 5* and follow the step there.

4 Requesting Zscaler Support

4.1 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.

4.1.1 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**.

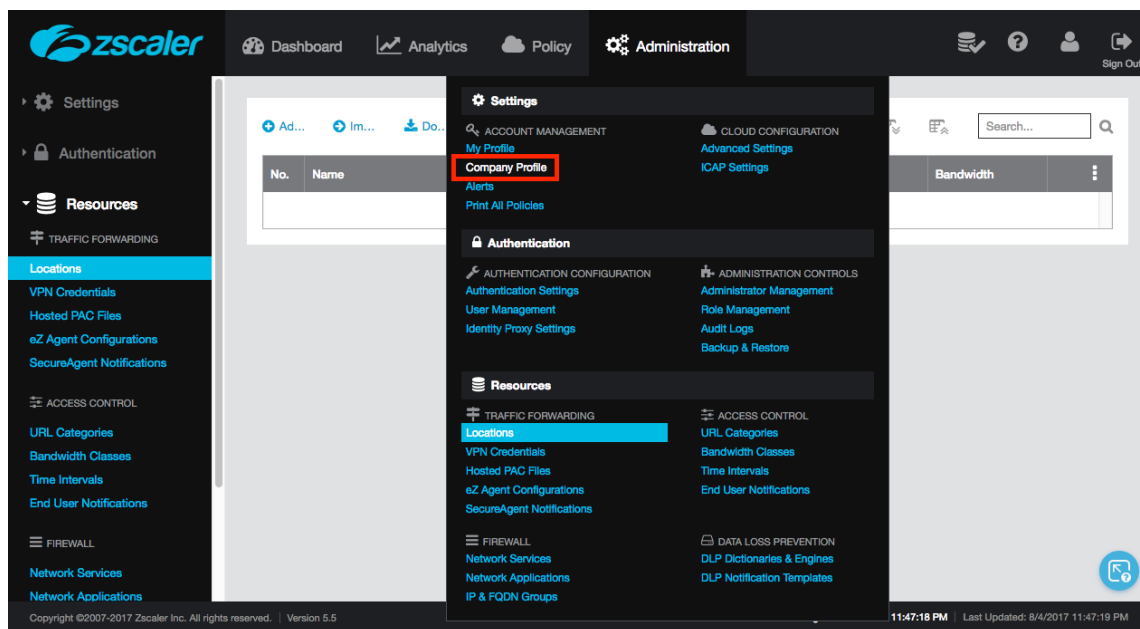
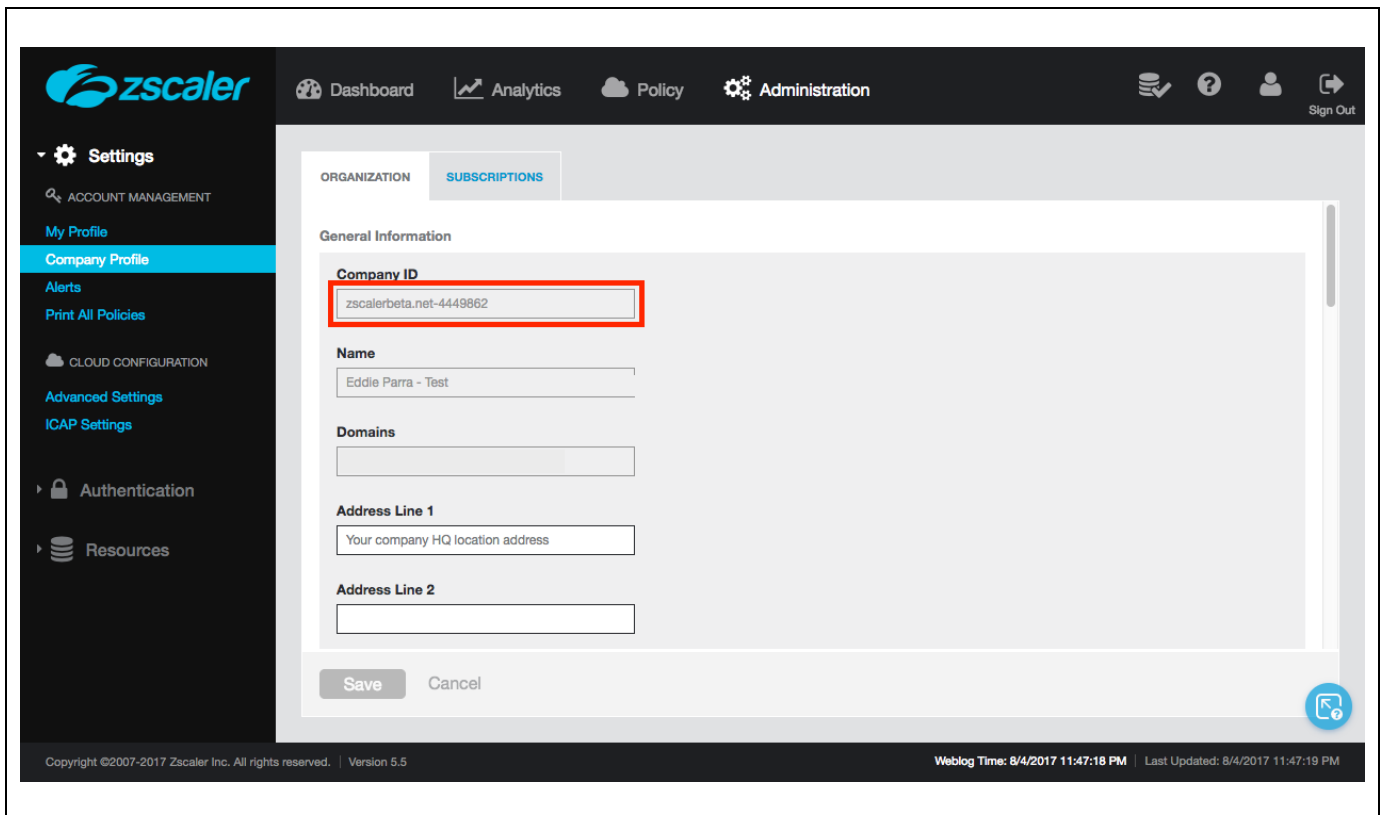


Figure 20: Obtaining Company ID

4.1.2 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.



The screenshot displays the Zscaler Administration console interface. On the left is a dark sidebar with navigation options: Settings (expanded), ACCOUNT MANAGEMENT, My Profile, Company Profile (highlighted), Alerts, Print All Policies, CLOUD CONFIGURATION, Advanced Settings, ICAP Settings, Authentication, and Resources. The main content area has a top navigation bar with Dashboard, Analytics, Policy, and Administration. Below this, there are tabs for ORGANIZATION and SUBSCRIPTIONS. The 'General Information' section contains several form fields: 'Company ID' (highlighted with a red box and containing 'zscalerbeta.net-4449862'), 'Name' (containing 'Eddie Parra - Test'), 'Domains' (empty), 'Address Line 1' (containing 'Your company HQ location address'), and 'Address Line 2' (empty). At the bottom of the form are 'Save' and 'Cancel' buttons. The footer shows copyright information, version 5.5, and a timestamp: 'Weblog Time: 8/4/2017 11:47:18 PM | Last Updated: 8/4/2017 11:47:19 PM'.

Figure 21: Save Company ID

4.1.3 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>.

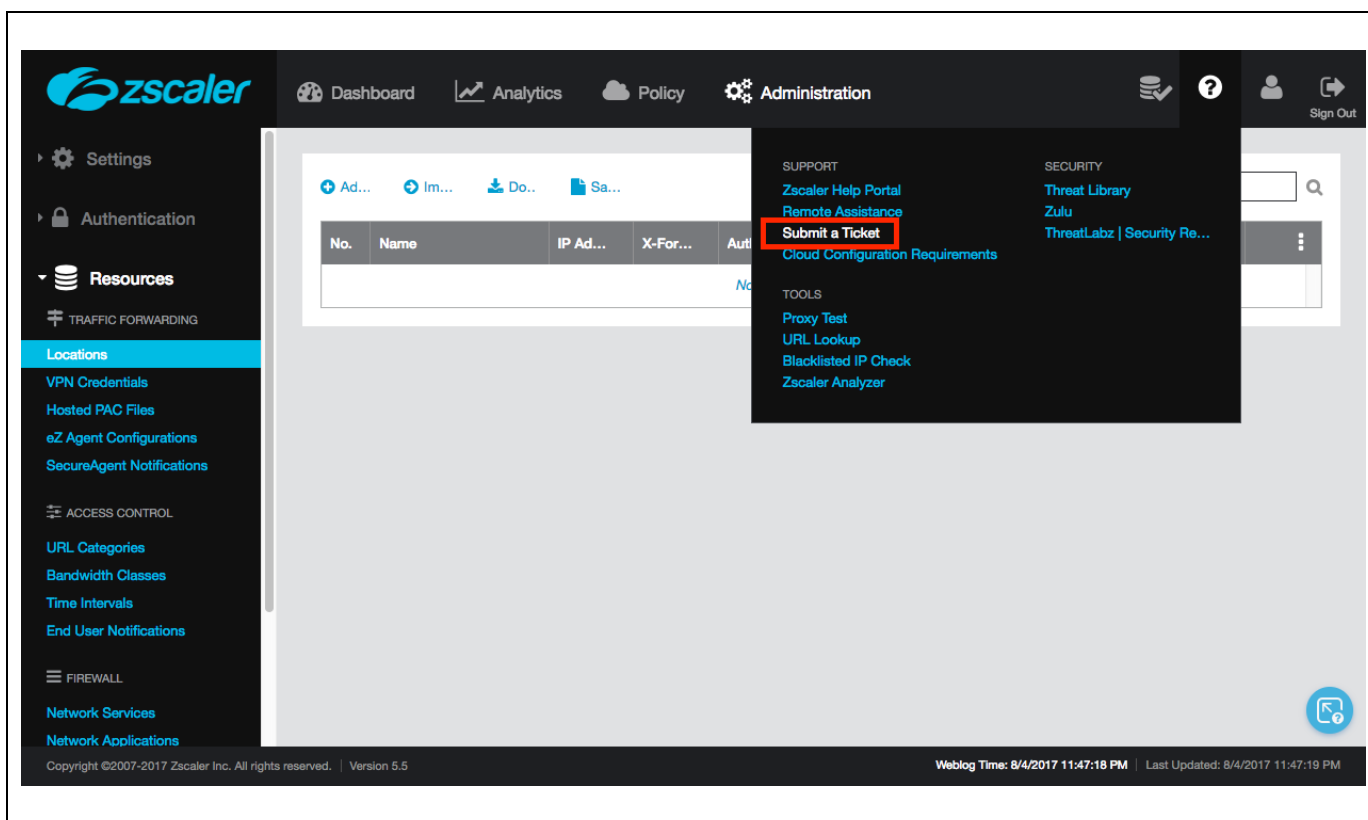


Figure 22: Enter Support Section

4.2 GRE Provisioning Request (Example)

Figure 23 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.

Submit Ticket

We have a dedicated ticket submission page for partners, so if you are a partner, go here instead:
<https://help.zscaler.com/mssp-submit-ticket>

Contact Email *

youremail@yourdomain.com

Issue Subject *

Provision GRE

CC List (separate multiple email addresses with a comma)

Description *

My company ID is: zscalerbeta.net-#####.
Please provision a GRE tunnel for location 207.46.23.22. This location is in CA, San Jose.
Thanks,

Customer Type *

Current Customer

Ticket Type *

Task

Priority *

Normal

Area *

Provisioning

Provisioning *

GRE Tunnel

Contact Name *

Organization *

Contact Phone

Requester Time Zone *

-- Select --

Upload a file (often helps troubleshoot issues)

Choose File

No file chosen

Search our knowledge base

Escalate Support Ticket

[Zscaler Analyzer tool >](#)
[Support Best Practice Guide >](#)

Submit

Figure 23: GRE Provisioning Example

4.3 Adding Domain (Example)

Figure 24 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

We have a dedicated ticket submission page for partners, so if you are a partner, go here instead:
<https://help.zscaler.com/mssp-submit-ticket>

Contact Email *

Issue Subject *

CC List (separate multiple email addresses with a comma)

Description *

Customer Type *

Ticket Type *

Priority *

Area *

Provisioning *

Contact Name *

Organization *

Contact Phone

Requester Time Zone *

Upload a file (often helps troubleshoot issues)

youremail@yourdomain.com

Adding Domain

My company ID is: zscalerbeta.net-#####.
Please add (domainfromscm.com) to my ZIA instance.
Thanks,
Eddie

Current Customer

Task

Normal

Provisioning

Add/Remove Domain

-- Select --

Choose File No file chosen

Search our knowledge base

Escalate Support Ticket

[Zscaler Analyzer tool >](#)
[Support Best Practice Guide >](#)

Submit

Figure 24: GRE Provisioning Example

5 Verifying ZIA Configuration

5.1 Request Verification Page

The URL <https://ip.zscaler.com> can be used to validate if you are transiting ZIA. In *Figure 25* and *Y* 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 25: Non-working Example

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



Figure 26: Working Example

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: Riverbed Resources

Riverbed

<https://www.riverbed.com/>

SteelConnect Gateway Devices

<https://www.riverbed.com/products/steelconnect.html>

Riverbed Support

https://support.riverbed.com/content/support/contact_support.html