ZSCALER AND CLOUDGENIX DEPLOYMENT GUIDE

MAY 2024, VERSION 2.1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't 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. To learn more, see Zscaler's website or follow Zscaler on Twitter @zscaler.

Palo Alto Networks Overview

Palo Alto Networks (NASDAQ: PANW), parent company of CloudGenix, innovates to outpace cyberthreats so organizations can confidently embrace technology. They provide next-gen cybersecurity to thousands of customers globally across all sectors. Their cybersecurity platforms and services are backed by threat intelligence and strengthened by automation. Whether deploying products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, Palo Alto Networks is committed to helping ensure each day is safer than the one before. To learn more, refer to Palo Alto Networks' website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- Zscaler Resources
- CloudGenix Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler software.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and CloudGenix Introduction

Overviews of the Zscaler and CloudGenix applications are described in this section.

⚠ If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

CloudBlade Overview

The Palo Alto Networks CloudBlade platform integrates branch services into the SASE fabric without needing to update your branch appliances or controllers, thus eliminating service disruptions and complexity. This cloud-based API architecture automates deployments of third-party services, enabling organizations to simplify network operations and multicloud connectivity and expedite deployments. The CloudGenix SD-WAN CloudBlade platform allows customers to deliver branch services at speed and scale. The core of CloudBlade is the Layer 3 to Layer 7 application-aware CloudGenix SD-WAN Instant-On Network (ION) appliance that powers the application flow system for policy enforcement in the branch from the cloud. The platform provides secure access to the ION appliances that enable API programming to automate UI workflows with customized templates to significantly reduce the operational complexity.

CloudGenix Resources

The following table contains links to CloudGenix support resources.

Name	Definition
CloudGenix Access CloudBlade Integration Guide	CloudBlade online documentation.
Palo Alto LIVEcommunity	Online community forum.
Palo Alto Networks Customer Support	Online Support portal.

CloudGenix SD-WAN ZIA Integration Requirements

As enterprises rely on SaaS or Cloud-based delivery models for business-critical applications, there's a compelling need for per-application policy enforcement without increasing remote office infrastructure. Traditional hardware-router based approaches are limited by heavy-handed "all or nothing" policies for direct-to-internet versus policy enforcement per-application. Additionally, because router-based approaches are packet-based versus application-session based, they fail to meet application session-symmetry requirements, causing network and security outages.

- Integrate with ZIA
- Prerequisites
- Plan the Deployment
- Acquire the Zscaler Information

Integrate with ZIA

The integration of CloudGenix SD-WAN SD-WAN and ZIA, allows customers to have a lightweight remote office hardware footprint, while still being able to provide a full suite of application-specific security policies.

To facilitate this integration, CloudGenix SD-WAN Release 5.1.1 and later provide CloudBlades to automatically integrate the CloudGenix SD-WAN Controller, Remote CloudGenix SD-WAN ION devices, and ZIA Public Service Edges, formerly Zscaler Enforcement Nodes (ZENs).

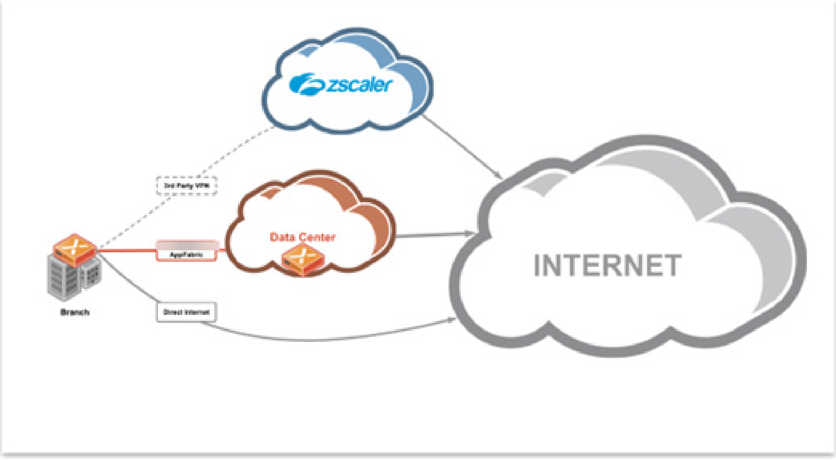


Figure 1. ZIA and CloudGenix SD-WAN integration

Prerequisites

The following items are required for configuring CloudGenix SD-WAN and ZIA integration:

CloudGenix SD-WAN

- An active CloudGenix SD-WAN subscription.
- CloudGenix SD-WAN AppFabric deployed at one or more locations.
- Physical and/or virtual ION devices running Release 5.1.9 or later.

Zscaler

- An active ZIA instance (in any cloud).
- Administrator login credentials for this instance.
- A partner administrator account and partner key.

Plan the Deployment

The primary way to architecturally accomplish the CloudGenix SD-WAN and ZIA integration is through IPSec Standard VPNs and GRE tunnels from remote ION device endpoints to Zscaler. The Zscaler Integration CloudBlade automatically creates, manages, and maintains the IPSec and GRE Standard VPN tunnels by entering tags on the appropriate CloudGenix SD-WAN objects.

Starting with release version 2.0.0, the Zscaler CloudBlade supports both IPSec and GRE tunnels. ZIA has launched APIs that you can use to build GRE tunnels to Zscaler nodes from branches that require high throughput. Each GRE tunnel can have up to 1 Gbps bandwidth.

The AUTO-zscaler-GRE tag is added to a site tag and a circuit tag to create the GRE tunnels. The site tag is extended for sublocation, custom endpoint, and other options, while the circuit tag is a static tag. A single interface on the device supports both the IPSec tunnels (AUTO-zscaler tag) and GRE tunnels (AUTO-zscaler-GRE tag). If a circuit is tagged with both AUTO-zscaler and AUTO-zscaler-GRE tags on an interface, then both IPSec and GRE tunnels are established to the specific Public Service Edges.

You must configure and link the CloudGenix SD-WAN interface to Zscaler through a partner administrator account, and an SD-WAN partner key to facilitate this tag-based configuration.

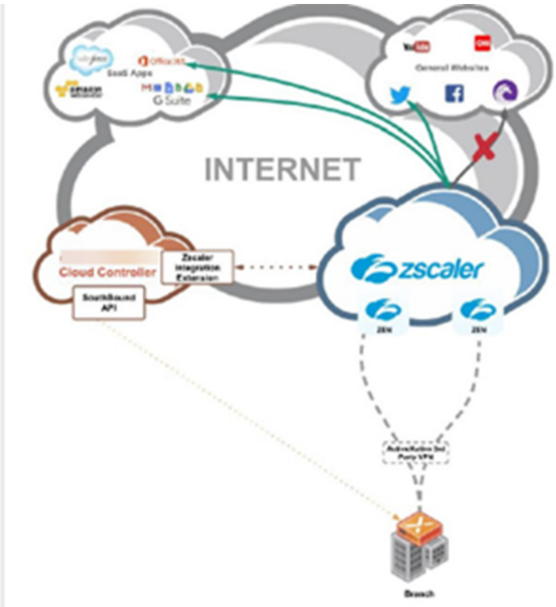


Figure 2. ZIA and CloudBlade deployment

Use the following steps to complete the integration:

1. Create a partner administrator role, create a partner administrator account and assign the role, and generate an SD-WAN partner key from the ZIA Admin Portal.
2. Configure and install the Zscaler CloudBlade in the CloudGenix SD-WAN Portal.
3. Assign tags to objects in the CloudGenix SD-WAN Portal to automatically integrate those objects to Zscaler.
4. Edit application network policy rules to send traffic to the Zscaler.

Prior to configuring the Zscaler CloudBlade in the CloudGenix SD-WAN Portal, make sure that the user account you are logged in with has an IP session lock disabled.

Acquire the Zscaler Information

Before configuring CloudGenix SD-WAN to integrate with Zscaler, perform the following steps:

1. Create a partner administrator role with full access controls for Locations and VPN Credentials. From version 2.0.0 or later, you can also include access controls for options Static IP and GRE Tunnels.

   a. From **Administration**, click **Role Management**.

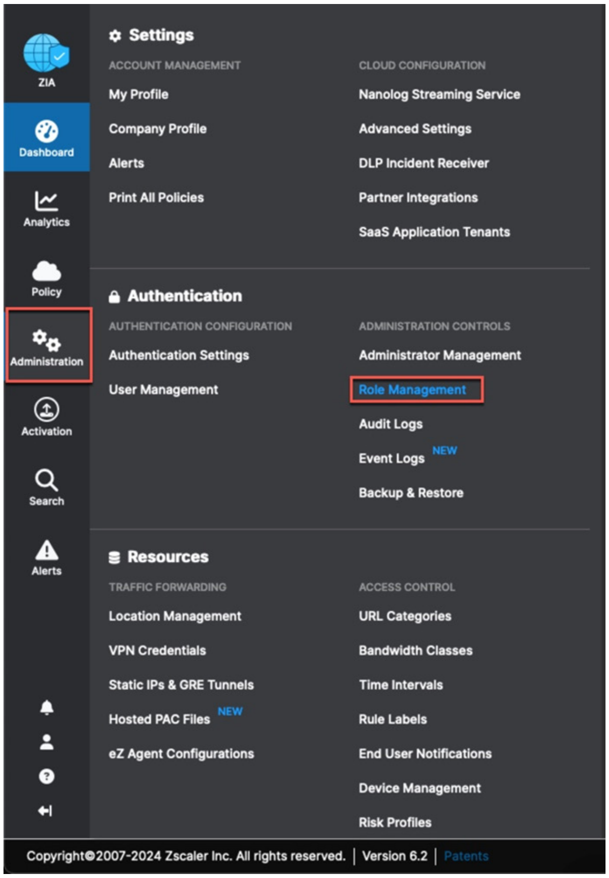
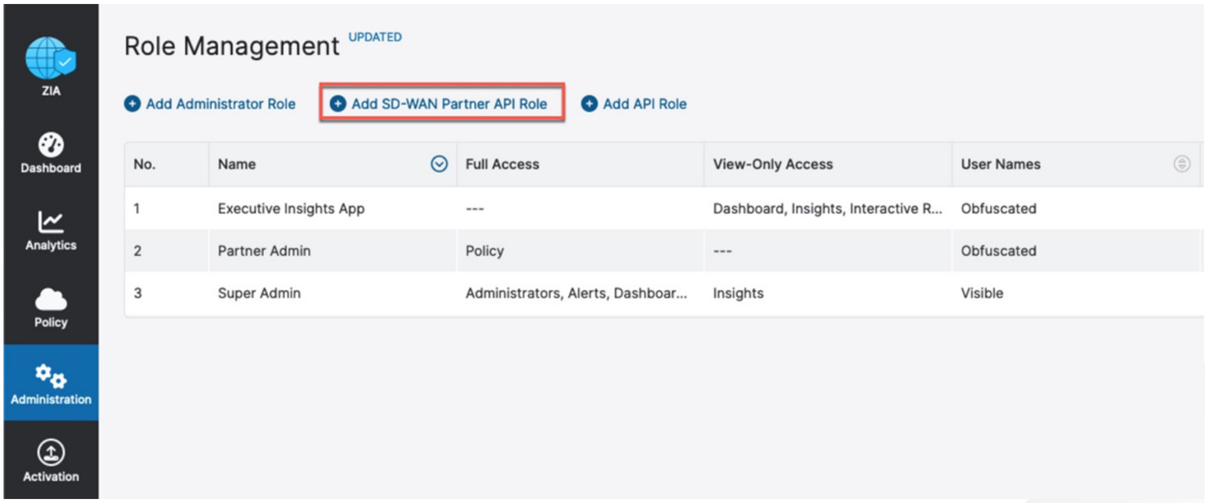


Figure 3. Role Management

   b. Click **Add SD-WAN Partner API Role**.

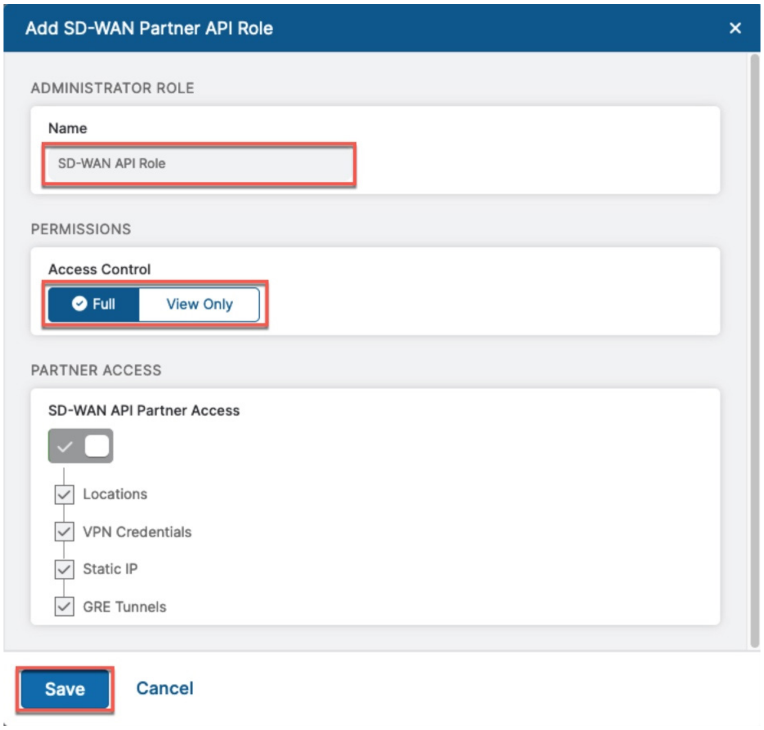


No.	Name	Full Access	View-Only Access	User Names
1	Executive Insights App	---	Dashboard, Insights, Interactive R...	Obfuscated
2	Partner Admin	Policy	---	Obfuscated
3	Super Admin	Administrators, Alerts, Dashboar...	Insights	Visible

Figure 4. Add SD-WAN Partner API Role

c. In the **Add SD-WAN Partner API Role** window, select **Full** for **Access Control**.

d. In the **Partner Access** section, select the **Locations** and **VPN Credentials** checkboxes.



Add SD-WAN Partner API Role ×

ADMINISTRATOR ROLE

Name: SD-WAN API Role

PERMISSIONS

Access Control: [✓ Full] View Only

PARTNER ACCESS

SD-WAN API Partner Access

☑ Locations

☑ VPN Credentials

☑ Static IP

☑ GRE Tunnels

Save Cancel

Figure 5. Add SD-WAN Partner API Role

e. Click **Save**.

From version 2.0.0, in the **Partner Access** section, you can also select the options **Static IP** and **GRE Tunnels**.

2. Create a partner administrator account and assign the Partner Admin role created in Step 1.

a. From **Administration**, select **Administrator Management**.

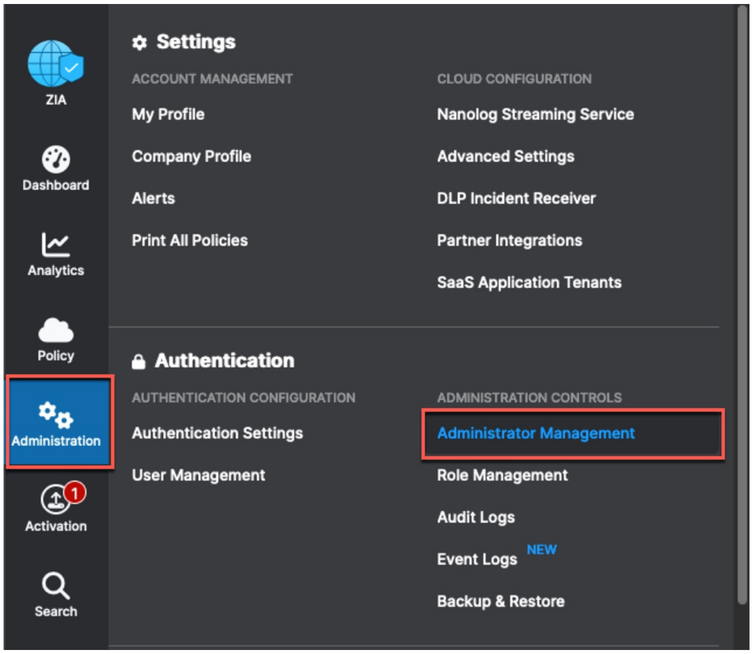
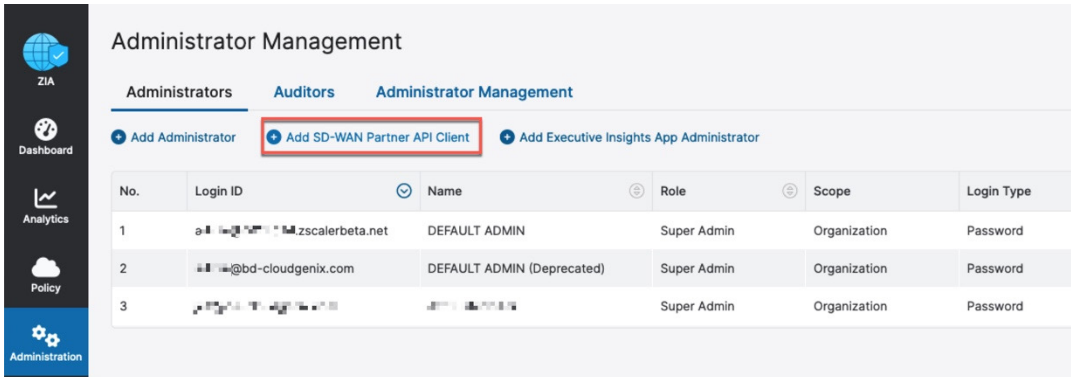


Figure 6. Administrator Management

b. In the **Administrator Management** window, click **Add SD-WAN Partner API Client**.

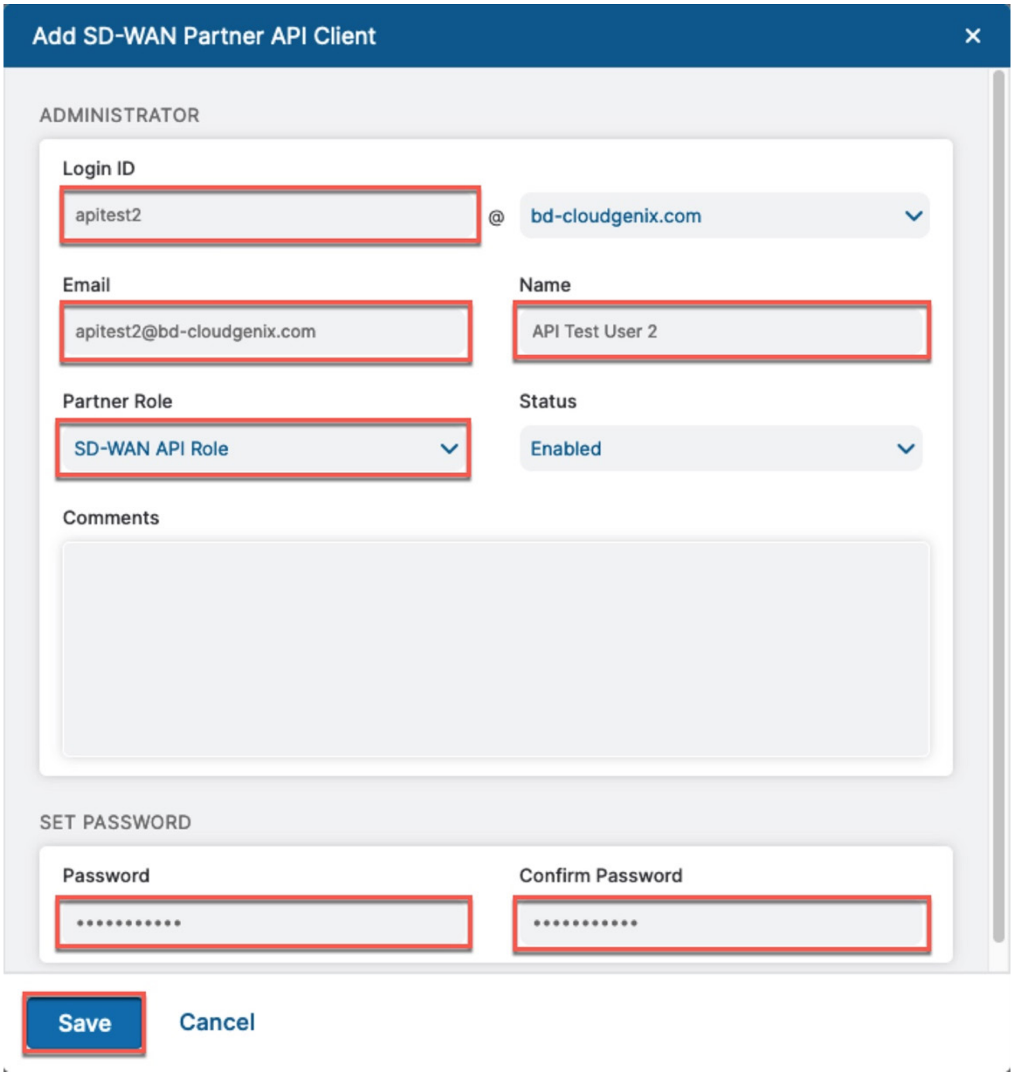


No.	Login ID	Name	Role	Scope	Login Type
1	[redacted].zscalerbeta.net	DEFAULT ADMIN	Super Admin	Organization	Password
2	[redacted]@bd-cloudgenix.com	DEFAULT ADMIN (Deprecated)	Super Admin	Organization	Password
3	[redacted]	[redacted]	Super Admin	Organization	Password

Figure 7. Add SD-WAN Partner API Client

c. Select **SD-WAN API Role** as the **Partner Role**.

d. Click **Save**.



ADMINISTRATOR

Login ID: apitest2 @ bd-cloudgenix.com

Email: apitest2@bd-cloudgenix.com

Name: API Test User 2

Partner Role: SD-WAN API Role

Status: Enabled

Comments:

SET PASSWORD

Password: •••••••••••

Confirm Password: •••••••••••

Figure 8. SD-WAN API Role

3. Generate an SD-WAN partner Key.
   a. From **Administration**, select **Partner Integrations**.

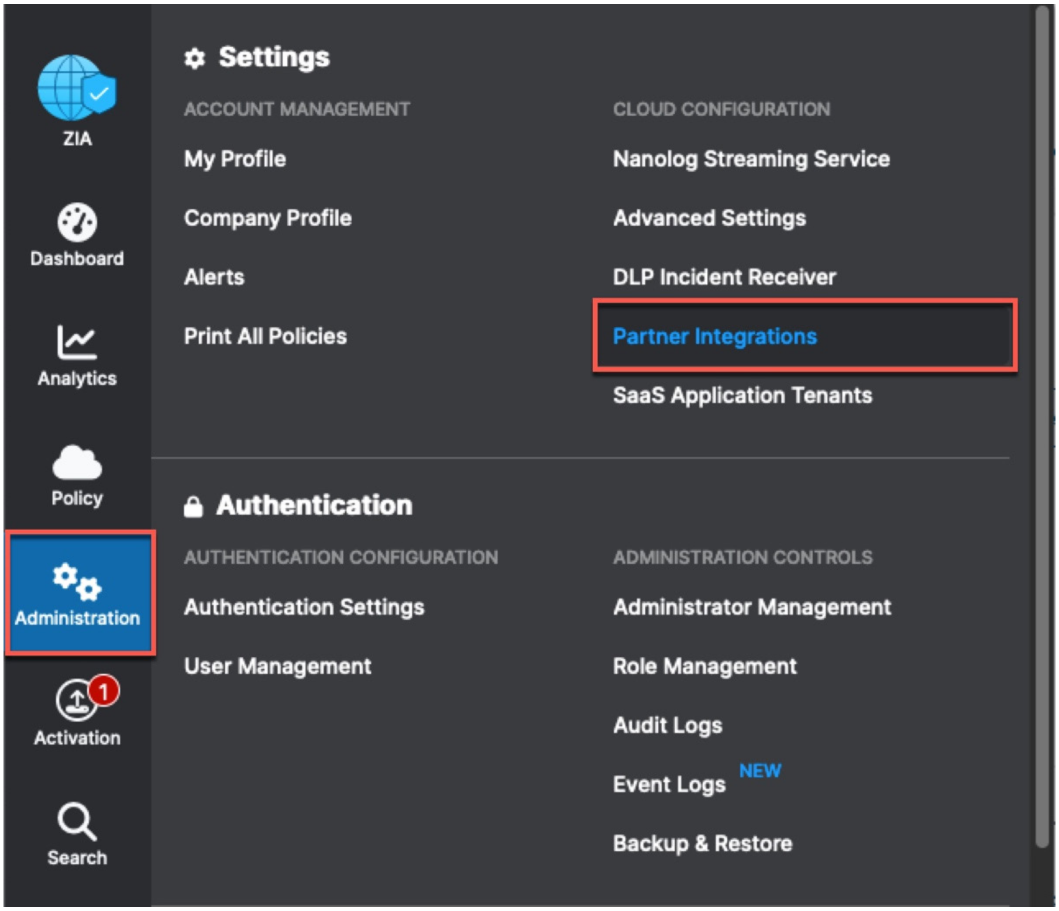
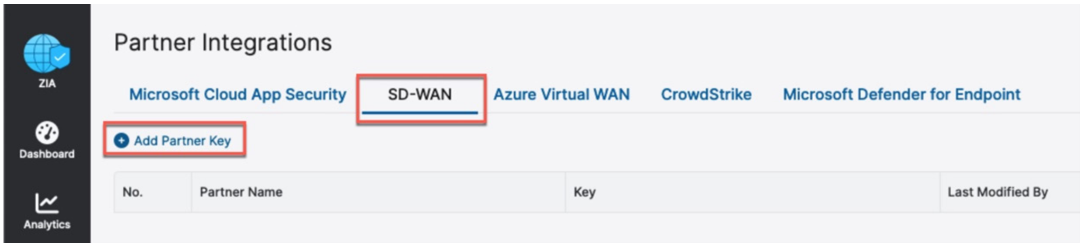


Figure 9. Partner Integrations

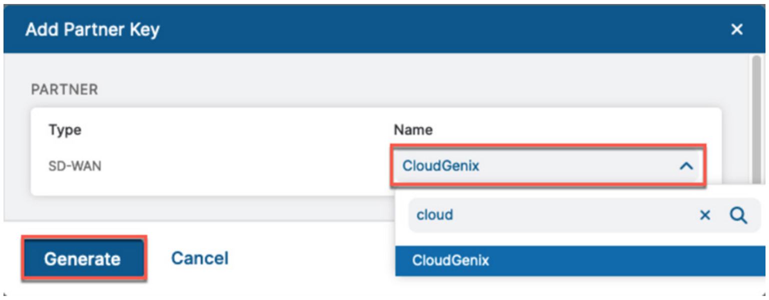
   b. On the **SD-WAN** tab, click **Add Partner Key**.



No.	Partner Name	Key	Last Modified By

Figure 10. Add Partner Key

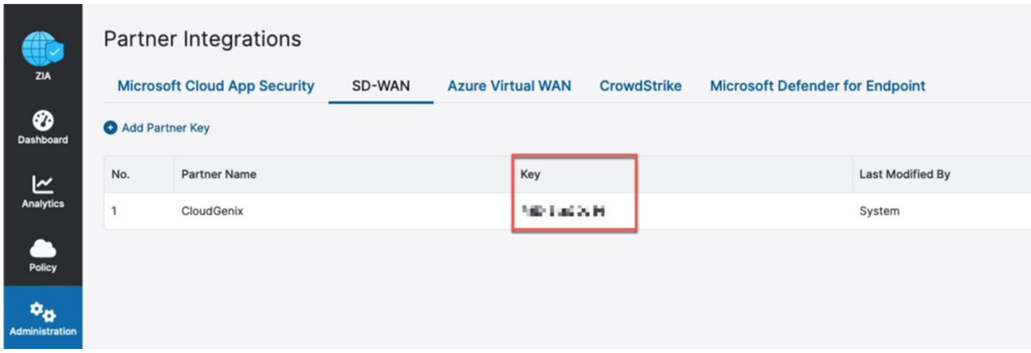
   c. In the **Add Partner Key** window, choose **CloudGenix** from the available selections.



Type	Name
SD-WAN	CloudGenix

Figure 11. Add Partner Key

d. The value of the key is displayed in the **Key** field. Copy this key, as it is needed during the configuration process.

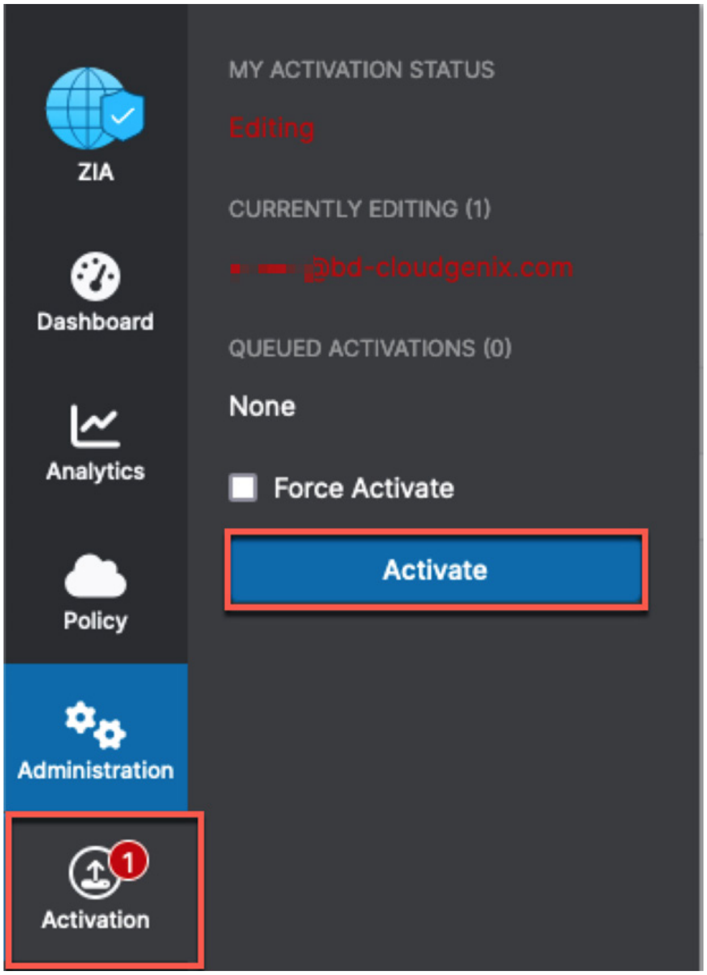


Partner Integrations

No.	Partner Name	Key	Last Modified By
1	CloudGenix	[redacted]	System

Figure 12. Partner Key

4. Activate pending changes on Zscaler by going to the **Activation** window and clicking **Activate**.



MY ACTIVATION STATUS

Editing

CURRENTLY EDITING (1)

[redacted]@bd-cloudgenix.com

QUEUED ACTIVATIONS (0)

None

□ Force Activate

Figure 13. Activate changes

If you want to increase the Static IP and GRE tunnel limit to a desired number from the default value of 100, contact Zscaler Support.

Configure and Install the Zscaler Integration CloudBlade

The following sections describe how to configure and install the Zscaler with CloudBlade.

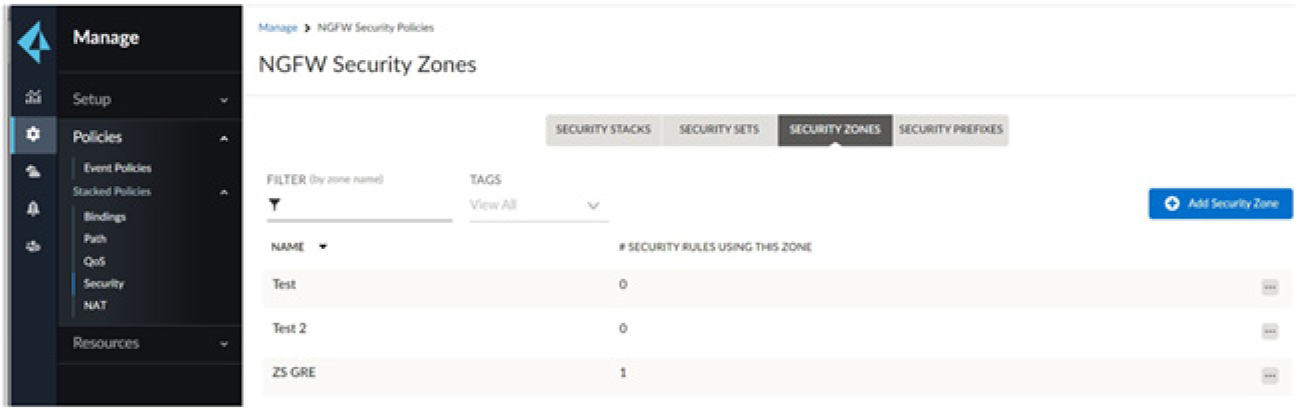
- Create Security Zone and Security Policy for GRE Tunnels Creation
- Configure and Install the Zscaler Integration
- Assign Tags to Objects in CloudGenix SD-WAN
- Validate the Zscaler Configuration
- Edit Application Network Policy Rules
- Understand Service and Data Center Groups
- Verify Standard VPN Endpoints
- Assign Domains to Sites
- Use Groups in Network Policy Rules
- Use a Group in Stacked Policies

Create Security Zone and Security Policy for GRE Tunnels Creation

GRE tunnels created by the Zscaler CloudBlade require a security policy (v1) or security policy set (v2) to be applied to the site for tunnel creation. You must create the security policy and zone, and map them to the site. The CloudBlade automatically places the servicelink GRE tunnel into the security zone. CloudBlade typically creates two GRE tunnels, a Primary tunnel to Data Center One and a Secondary GRE tunnel to Data Center Two.

If a policy or zone is removed later, CloudBlade ignores all GRE operations performed on that site. This includes creating, updating or re-querying.

1. Add a security zone.
   a. Select **Manage** > **Policies** > **Stacked Policies** > **Security**.
   b. Go to **Security Zones** and add a **Security Zone**.



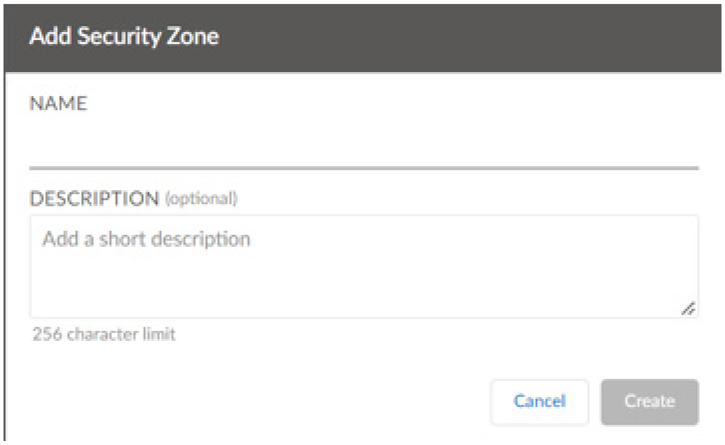
NGFW Security Zones

NAME	# SECURITY RULES USING THIS ZONE
Test	0
Test 2	0
ZS GRE	1

Figure 14. Security zones

c. Enter a **Name** for the security zone and an optional description.

d. Click **Create**.



Add Security Zone

NAME

DESCRIPTION (optional)

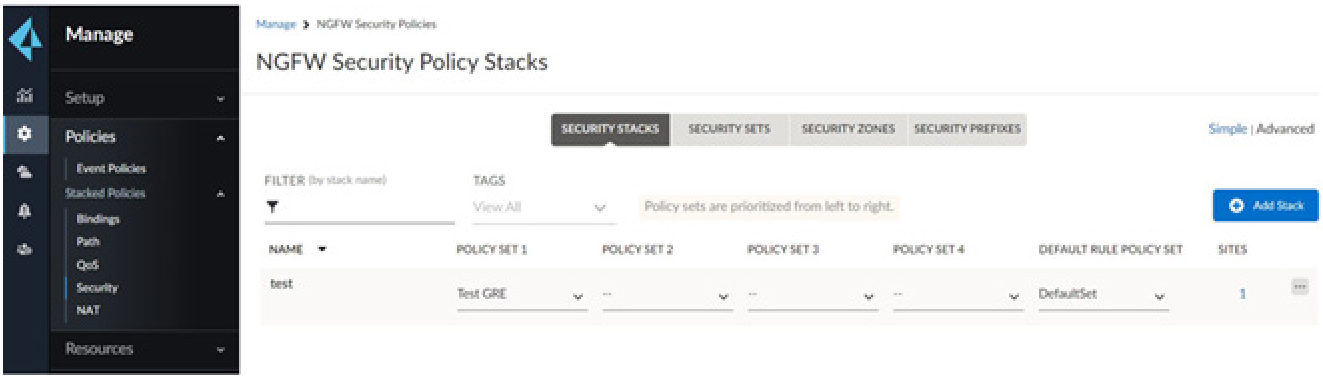
Add a short description

256 character limit

Figure 15. Create a Security Zone

2. Add a security policy stack.

a. Select **Manage** > **Policies** > **Stacked Policies** > **Security** and add a **Stack**.



NGFW Security Policy Stacks

FILTER (by stack name)

TAGS: View All

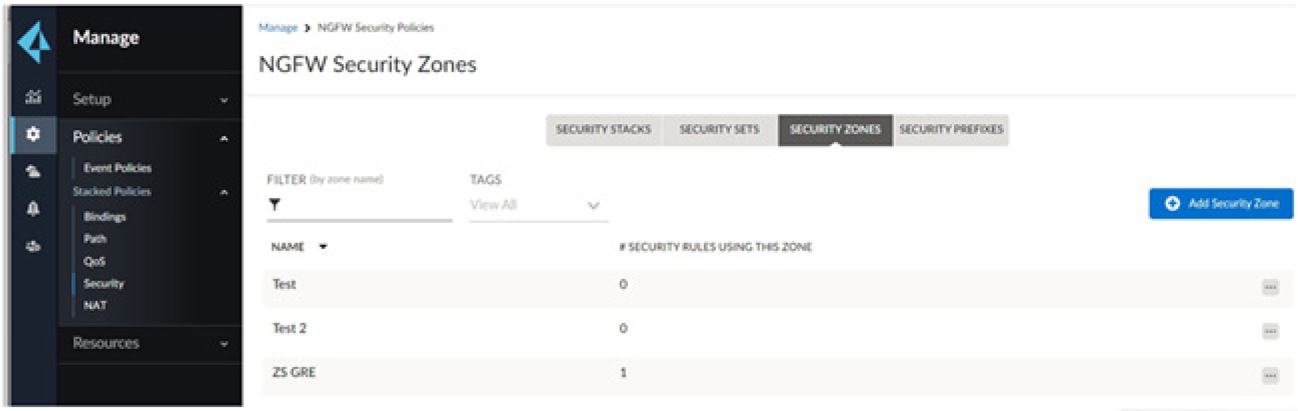
Policy sets are prioritized from left to right.

NAME	POLICY SET 1	POLICY SET 2	POLICY SET 3	POLICY SET 4	DEFAULT RULE POLICY SET	SITES
test	Test GRE	--	--	--	DefaultSet	1

Figure 16. Policy Stacks

b. Enter a name for the Security stack, select the security policy zone created previously.

c. Click **Save**.



NGFW Security Zones

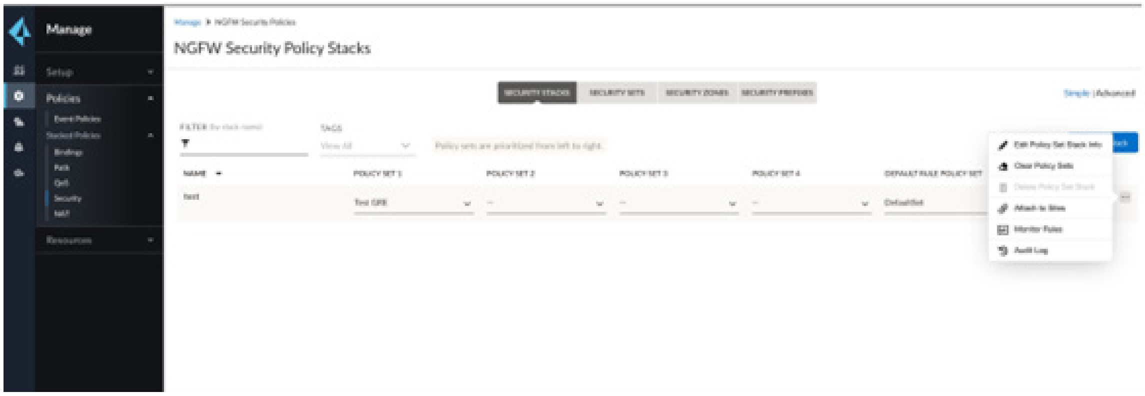
FILTER (by zone name)

TAGS: View All

NAME	# SECURITY RULES USING THIS ZONE
Test	0
Test 2	0
ZS GRE	1

Figure 17. Security zones

3. Bind the security policy to the site.
    a. Select **Manage** > **Policies** > **Stacked Policies** > **Security Stacks**.
    b. From the ellipsis menu for a security policy, select **Attach to Sites**.

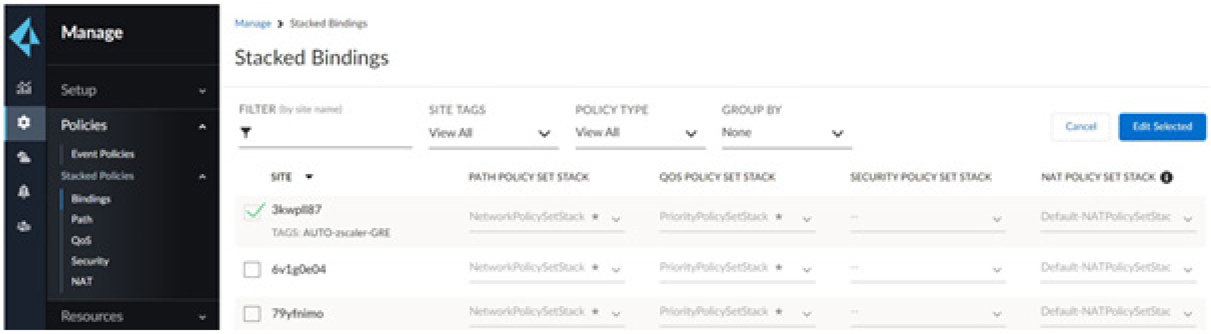


NGFW Security Policy Stacks

NAME	POLICY SET 1	POLICY SET 2	POLICY SET 3	POLICY SET 4	DEFAULT RULE POLICY SET
test	Test GRE	--	--	--	DefaultSet

Figure 18. Attach to sites

    c. Select the site and click **Edit Selected**.

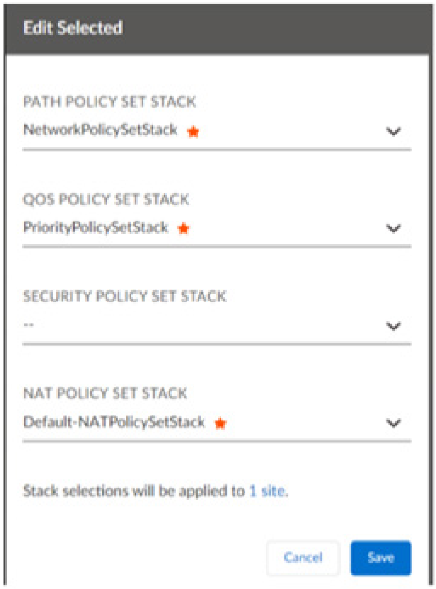


Stacked Bindings

	SITE	PATH POLICY SET STACK	QOS POLICY SET STACK	SECURITY POLICY SET STACK	NAT POLICY SET STACK
✓	3kwpll87 TAGS: AUTO-zscaler-GRE	NetworkPolicySetStack ★	PriorityPolicySetStack ★	--	Default-NATPolicySetStac
□	6v1g0e04	NetworkPolicySetStack ★	PriorityPolicySetStack ★	--	Default-NATPolicySetStac
□	79yfnimo	NetworkPolicySetStack ★	PriorityPolicySetStack ★	--	Default-NATPolicySetStac

Figure 19. Edit Selected

    d. Review or edit your security policies.
    e. Click **Save**.


Edit Selected

PATH POLICY SET STACK
NetworkPolicySetStack ★

QOS POLICY SET STACK
PriorityPolicySetStack ★

SECURITY POLICY SET STACK
--

NAT POLICY SET STACK
Default-NATPolicySetStack ★

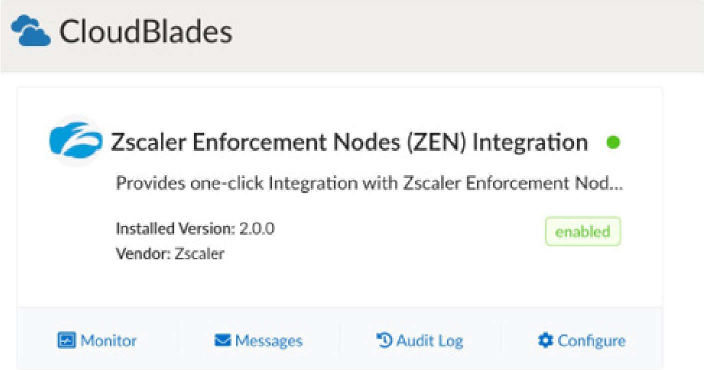
Stack selections will be applied to 1 site.

Figure 20. Save security policies

Configure and Install the Zscaler Integration

Configure the CloudGenix SD-WAN CloudBlade to prepare the CloudGenix SD-WAN Controller for integration.

1. From the CloudGenix SD-WAN Portal, click the **CloudBlades** tab.
2. In **CloudBlades**, locate the **Zscaler Enforcement Nodes (ZEN) Integration CloudBlade**. If CloudBlade does not appear, contact CloudGenix SD-WAN support team.



CloudBlades

Zscaler Enforcement Nodes (ZEN) Integration

Provides one-click Integration with Zscaler Enforcement Nod...

Installed Version: 2.0.0

Vendor: Zscaler

enabled

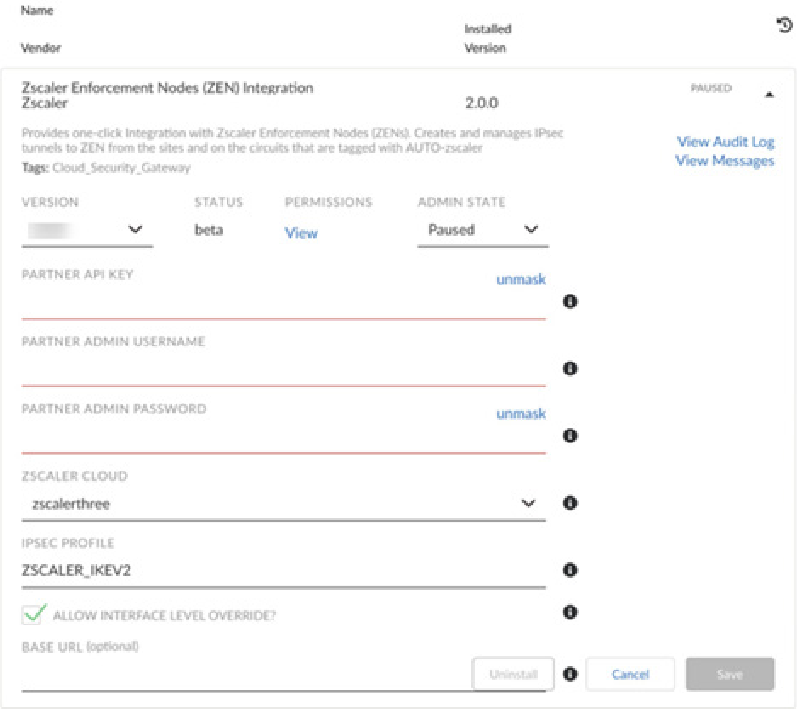
Figure 21. CloudBlade integration

3. Click **Configure** on the CloudBlade card to display the installation page. Enter the following information:
   a. From the **Version list**, select the required version.
   b. For **Admin State**, retain **Enabled**, which is the default value.
   c. For **API Key**, provide the SD-WAN key generated in the previous section.
   d. For **Partner Admin Username** and **Partner Admin Password**, provide the partner administrator account details created in the previous section.
   e. For Zscaler cloud, select the Zscaler cloud to which your subscription is attached (zscalerthree in the following example).

> From version 2.1.0 and later, the CloudBlade supports govcloud (which supports only IPSec tunnels).

   f. Specify the **IPSec Profile name** (case sensitive). The default is ZSCALER_IKEV2, which should be preprovisioned along with the CloudBlade allocation. The created tunnels are identified based on the tags created (AUTO-zscaler for IPSec and AUTO-zscaler-GRE for GRE; version 2.0.0 and later).
   g. If you select **Allow Interface Level Override** for the IPSec profile, it allows administrators to change the IPSec profile referenced at the Standard VPN tunnel level without the CloudBlade overriding this change. This is typically useful in the case of troubleshooting scenarios.
   h. (Optional) Provide the base URL. If left blank, the base URL is derived from the admin username domain.

4. After you configure the settings, click **Install** (or **Save**, if CloudBlade was previously installed).



Name
Vendor

Installed Version

Zscaler Enforcement Nodes (ZEN) Integration
Zscaler

2.0.0

PAUSED

Provides one-click Integration with Zscaler Enforcement Nodes (ZENs). Creates and manages IPsec tunnels to ZEN from the sites and on the circuits that are tagged with AUTO-zscaler

Tags: Cloud_Security_Gateway

View Audit Log
View Messages

VERSION	STATUS	PERMISSIONS	ADMIN STATE
	beta	View	Paused

PARTNER API KEY: unmask

PARTNER ADMIN USERNAME

PARTNER ADMIN PASSWORD: unmask

ZSCALER CLOUD: zscalerthree

IPSEC PROFILE: ZSCALER_IKEV2

☑ ALLOW INTERFACE LEVEL OVERRIDE?

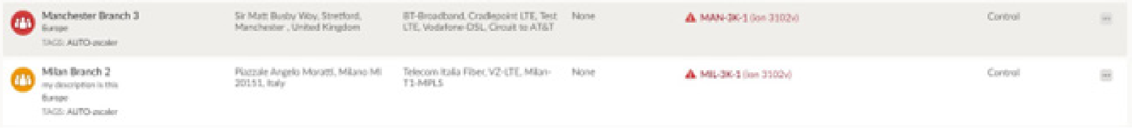
BASE URL (optional)

Figure 22. Install CloudBlade

Assign Tags to Objects in CloudGenix SD-WAN

After CloudBlade is configured, the next task is to tag CloudGenix SD-WAN sites and circuit categories to denote which sites and circuit types are candidates for auto Standard VPN tunnel and GRE tunnel creation to Zscaler.

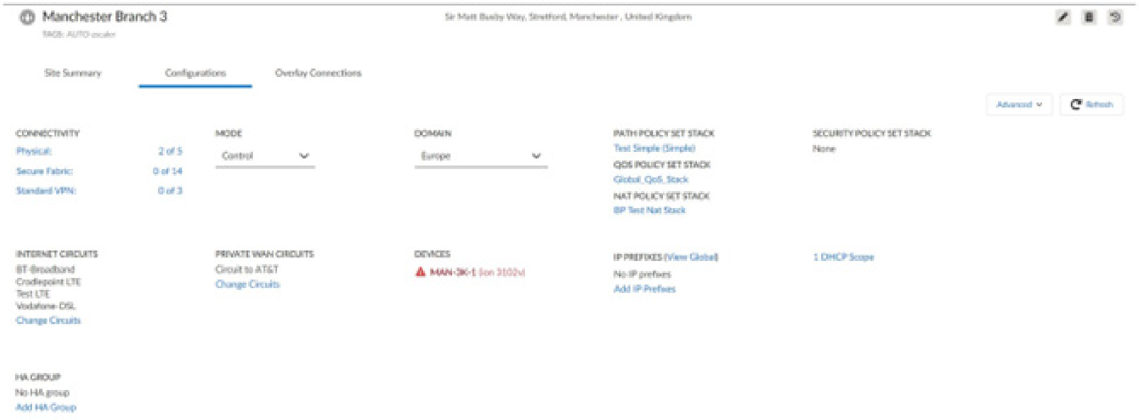
1. From the CloudGenix SD-WAN web interface, click **Manage** > **Setup** > **Sites**.
2. Click the site to bring up the site details (search for a site to connect to Zscaler).



Manchester Branch 3 Europe TAGS: AUTO-zscaler	Sir Matt Busby Way, Stretford, Manchester , United Kingdom	BT-Broadband, Cradlepoint LTE, Test LTE, Vodafone-DSL, Circuit to AT&T	None	MAN-3K-1 (ion 3102v)	Control
Milan Branch 2 my description is this Europe TAGS: AUTO-zscaler	Piazzale Angelo Moratti, Milano MI 20151, Italy	Telecom Italia Fiber, VZ-LTE, Milan-T1-MPLS	None	MIL-3K-1 (ion 3102v)	Control

Figure 23. Sites

3. Click **Edit** (on the top right of the site details screen).



Manchester Branch 3
TAGS: AUTO-zscaler

Sir Matt Busby Way, Stretford, Manchester , United Kingdom

CONNECTIVITY
Physical: 2 of 5
Secure Fabric: 0 of 14
Standard VPN: 0 of 3

MODE: Control

DOMAIN: Europe

PATH POLICY SET STACK: Test Simple (Simple)
QOS POLICY SET STACK: Global_QoS_Stack
NAT POLICY SET STACK: BP Test Nat Stack

SECURITY POLICY SET STACK: None

INTERNET CIRCUITS
BT-Broadband
Cradlepoint LTE
Test LTE
Vodafone-DSL
Change Circuits

PRIVATE WAN CIRCUITS
Circuit to AT&T
Change Circuits

DEVICES
MAN-3K-1 (ion 3102v)

IP PREFIXES (View Global)
No IP prefixes
Add IP Prefixes

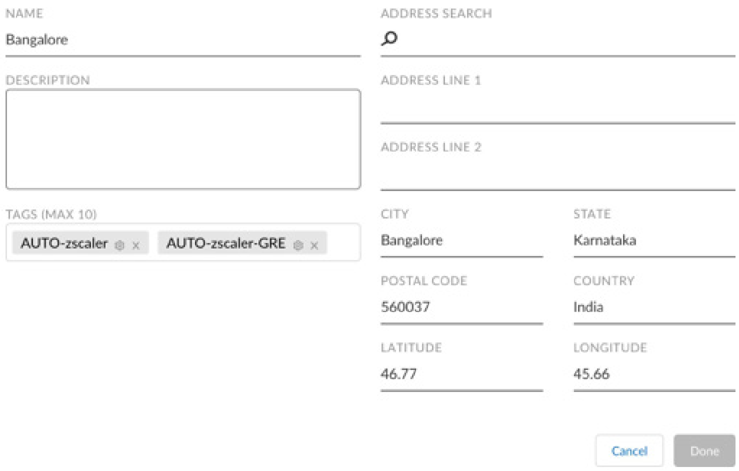
1 DHCP Scope

HA GROUP
No HA group
Add HA Group

Figure 24. Edit site

4. On the **Edit Site** dialog, in the **Tags** field, type `AUTO-zscaler (IPSec)` and `AUTO-zscaler-GRE (GRE)` for tunnel creation (case sensitive).

   If you remove any one of the tags, this deletes the respective tunnel (all configurations are deleted) while the other tunnel continues to operate.



NAME: Bangalore

ADDRESS SEARCH

DESCRIPTION

ADDRESS LINE 1

ADDRESS LINE 2

TAGS (MAX 10): AUTO-zscaler, AUTO-zscaler-GRE

CITY: Bangalore

STATE: Karnataka

POSTAL CODE: 560037

COUNTRY: India

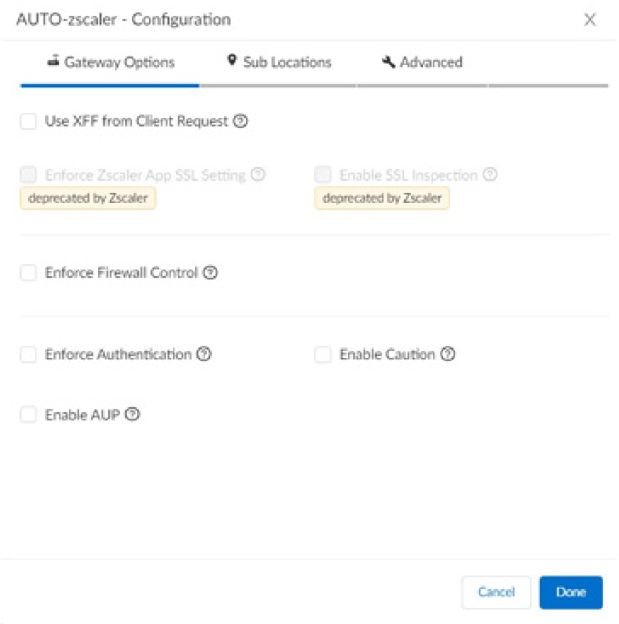
LATITUDE: 46.77

LONGITUDE: 45.66

Figure 25. Edit Site tags

5. Select the **Configure** icon to configure the gateway options as required by your security team.

   a. If configuring gateway options only at the parent location level, specify the options as needed. This implies that all traffic from this location is subject to the options configured here.



AUTO-zscaler - Configuration

□ Use XFF from Client Request

□ Enforce Zscaler App SSL Setting — deprecated by Zscaler

□ Enable SSL Inspection — deprecated by Zscaler

□ Enforce Firewall Control

□ Enforce Authentication

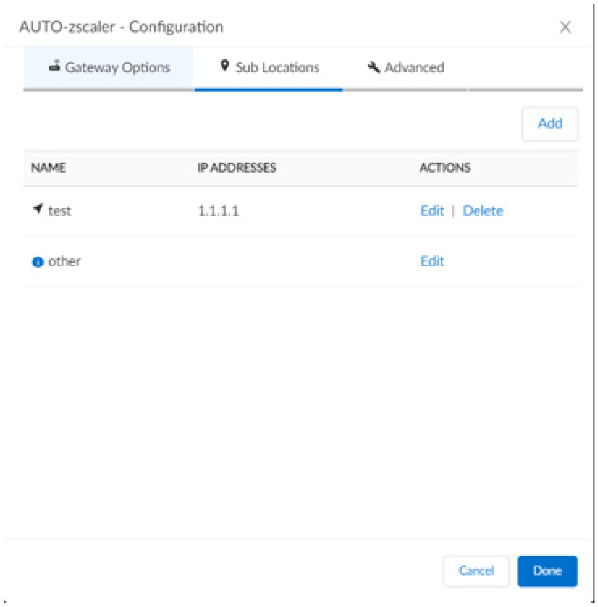
□ Enable Caution

□ Enable AUP

Figure 26. Gateway options

The gateway options, **Enforce Zscaler App SSL Setting** and **Enable SSL Inspection**, shown in the following image, are deprecated by Zscaler.

b. If you must configure different gateway option settings for different sources of traffic from this site, then specify the appropriate sublocation definition and settings from the **Sub Locations** tab.



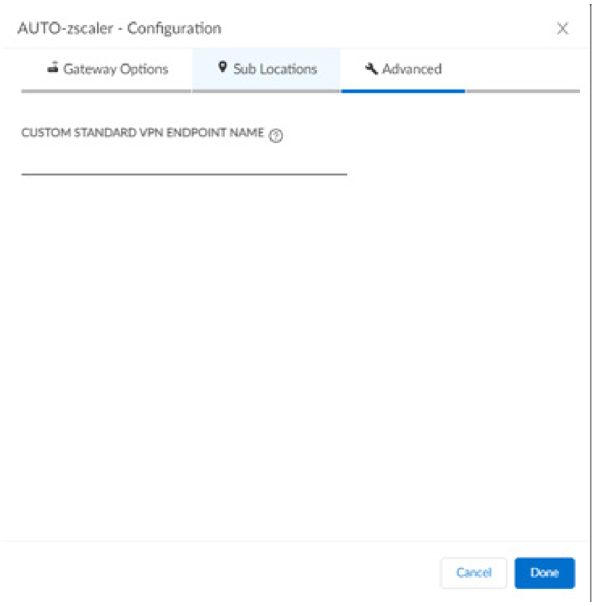
NAME	IP ADDRESSES	ACTIONS
test	1.1.1.1	Edit | Delete
other		Edit

Figure 27. Sub Locations tab

In the **Sub Locations** tab, options **Enforce Zscaler App SSL Setting** and **Enable SSL Inspection** are deprecated, and the option **Use XFF from Client Request** is disabled.

c. If you create a sublocation, make sure to specify the gateway options for the other location.

d. Specify the endpoint under the **Advanced** tab if there's a requirement to use a custom Standard VPN endpoint instead of the one that CloudBlade manages and maintains.



CUSTOM STANDARD VPN ENDPOINT NAME

Figure 28. Advanced tab

The Standard VPN endpoint name is case sensitive and must be previously configured under **Stacked Policies** > **Service & DC Groups** > **Endpoints** > **Standard VPN**.

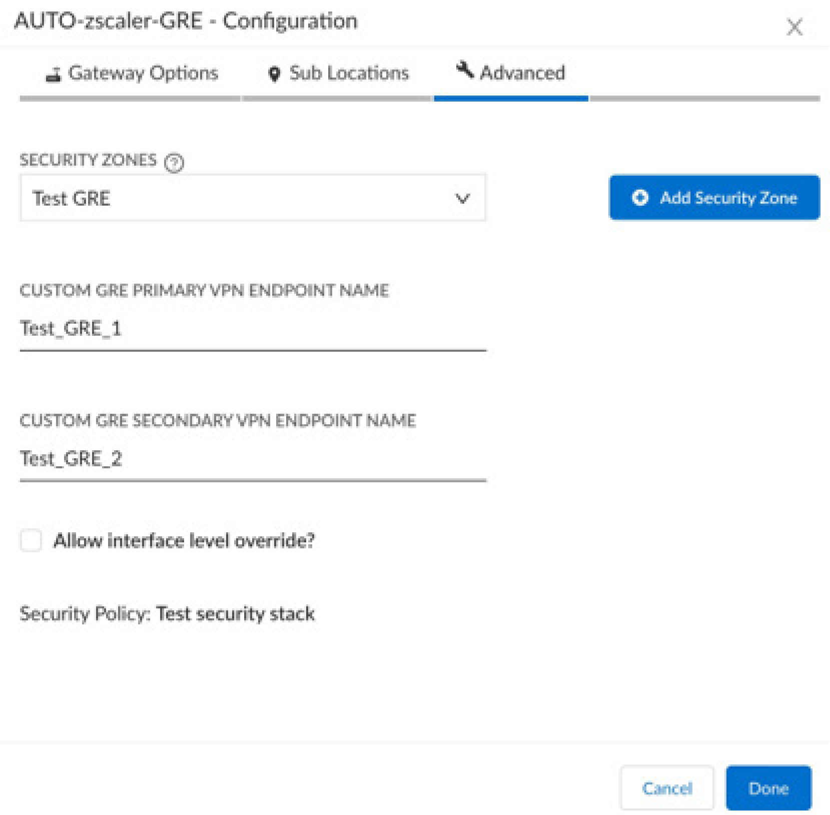
e. To configure the GRE tunnel options under the **Advanced** tab, select the preconfigured Security Zone from the drop-down menu and select the **Custom Endpoint** for both primary and secondary tunnels (version 2.0.0 or later).

The GRE endpoint for both primary and secondary tunnels is case sensitive and must be configured under **Resources** > **Service & DC Groups** > **Endpoints** > **Standard VPN**.

While using the custom endpoints for GRE tunnels, ensure that the IP addresses are available in the list of the closest data centers, and the IP addresses belong to data centers of different locations.

AUTO-zscaler and AUTO-zscaler-GRE tag values must be the same for both Gateway Options and Sub Locations.

6. Click **Done**.


AUTO-zscaler-GRE - Configuration

SECURITY ZONES: Test GRE

CUSTOM GRE PRIMARY VPN ENDPOINT NAME: Test_GRE_1

CUSTOM GRE SECONDARY VPN ENDPOINT NAME: Test_GRE_2

□ Allow interface level override?

Security Policy: Test security stack

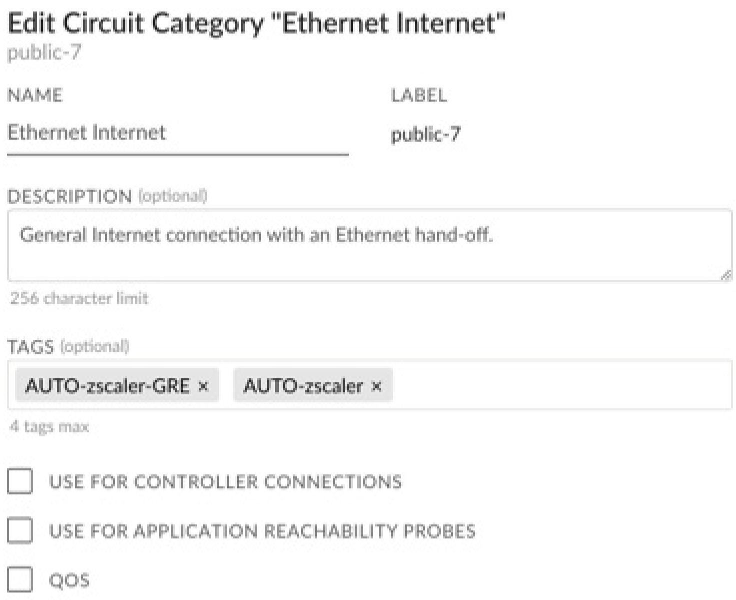
Figure 29. Save the configuration

Tag the Circuit Categories

Now that the site has been tagged as enabled for Zscaler, tag the circuit categories to use to establish a Standard VPN or GRE tunnel to Zscaler.

This capability is useful if you want only specific types of circuits to be used for Zscaler integration or explicitly exclude certain circuit types. For example, a customer might not want to use their metered LTE circuit for Standard VPN establishment.

1. From the CloudGenix SD-WAN web interface, click **Policies** > **Stacked Policies**.
2. Click **Circuit Categories**.
3. Find the circuit categories that are associated with your sites from which you want the system to automatically build the tunnels. Edit the circuit category and enter `AUTO-zscaler` and `AUTO-zscaler-GRE` (case sensitive) in the **Tags** field.



Edit Circuit Category "Ethernet Internet"

public-7

NAME: Ethernet Internet

LABEL: public-7

DESCRIPTION (optional): General Internet connection with an Ethernet hand-off.

256 character limit

TAGS (optional): AUTO-zscaler-GRE × AUTO-zscaler ×

4 tags max

□ USE FOR CONTROLLER CONNECTIONS

□ USE FOR APPLICATION REACHABILITY PROBES

□ QOS

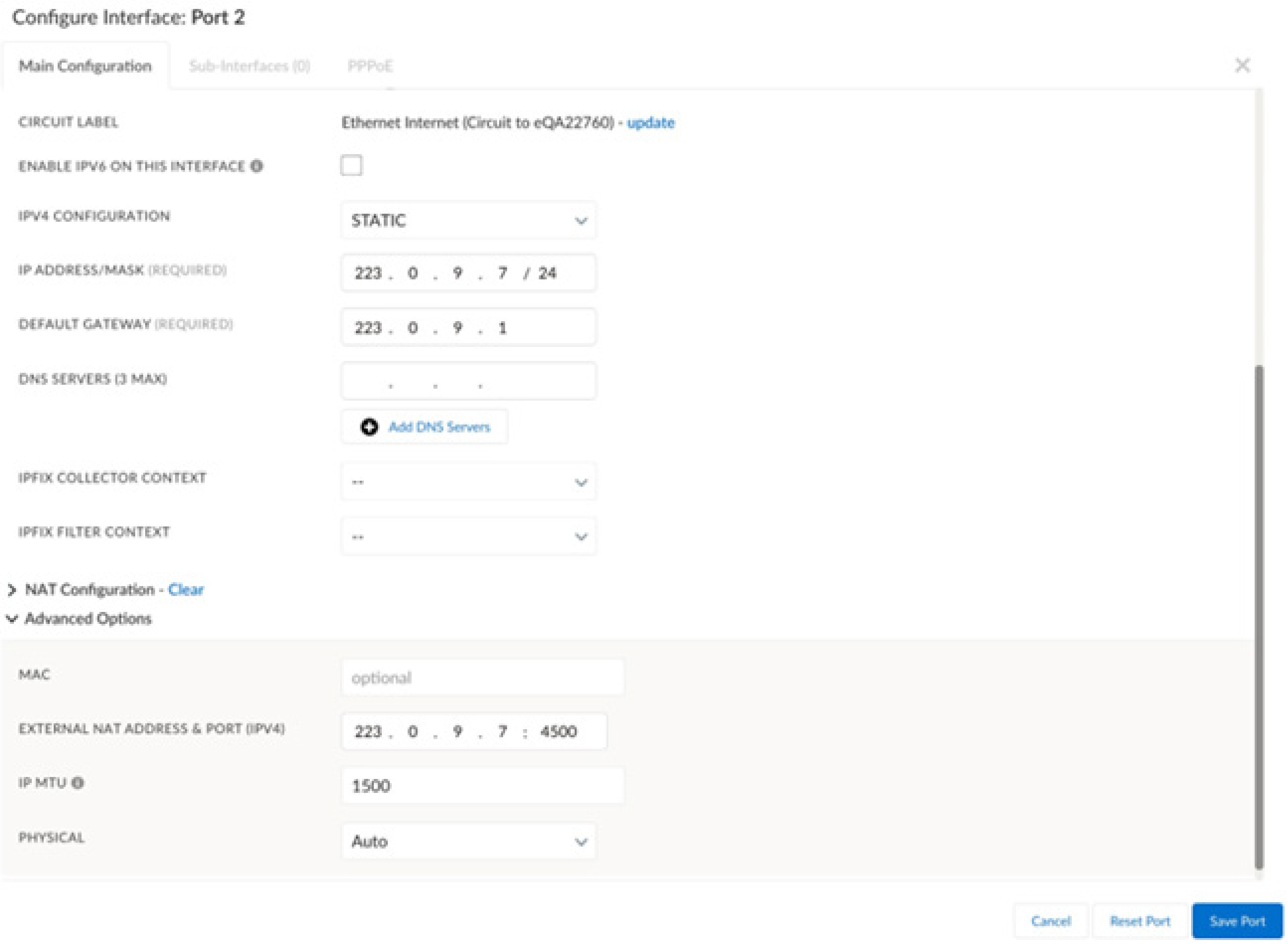
Figure 30. Edit Circuit Category

4. Click **Update**.

After this configuration is completed, Standard VPN IPSec/GRE tunnels connecting the CloudGenix SD-WAN ION device and Zscaler begins the creation or onboarding process in the next integration cycle. It can take several integration cycles for the tunnels to appear and be active on the CloudGenix SD-WAN portal.

Configure Parent Interface for Tunnels

1. After the circuit is tagged, add the circuit as part of the circuit label on the parent interface (Port 2 in this case).



Configure Interface: Port 2

CIRCUIT LABEL: Ethernet Internet (Circuit to eQA22760) - update

ENABLE IPV6 ON THIS INTERFACE: □

IPV4 CONFIGURATION: STATIC

IP ADDRESS/MASK (REQUIRED): 223 . 0 . 9 . 7 / 24

DEFAULT GATEWAY (REQUIRED): 223 . 0 . 9 . 1

DNS SERVERS (3 MAX): . . .

IPFIX COLLECTOR CONTEXT: --

IPFIX FILTER CONTEXT: --

MAC: optional

EXTERNAL NAT ADDRESS & PORT (IPV4): 223 . 0 . 9 . 7 : 4500

IP MTU: 1500

PHYSICAL: Auto

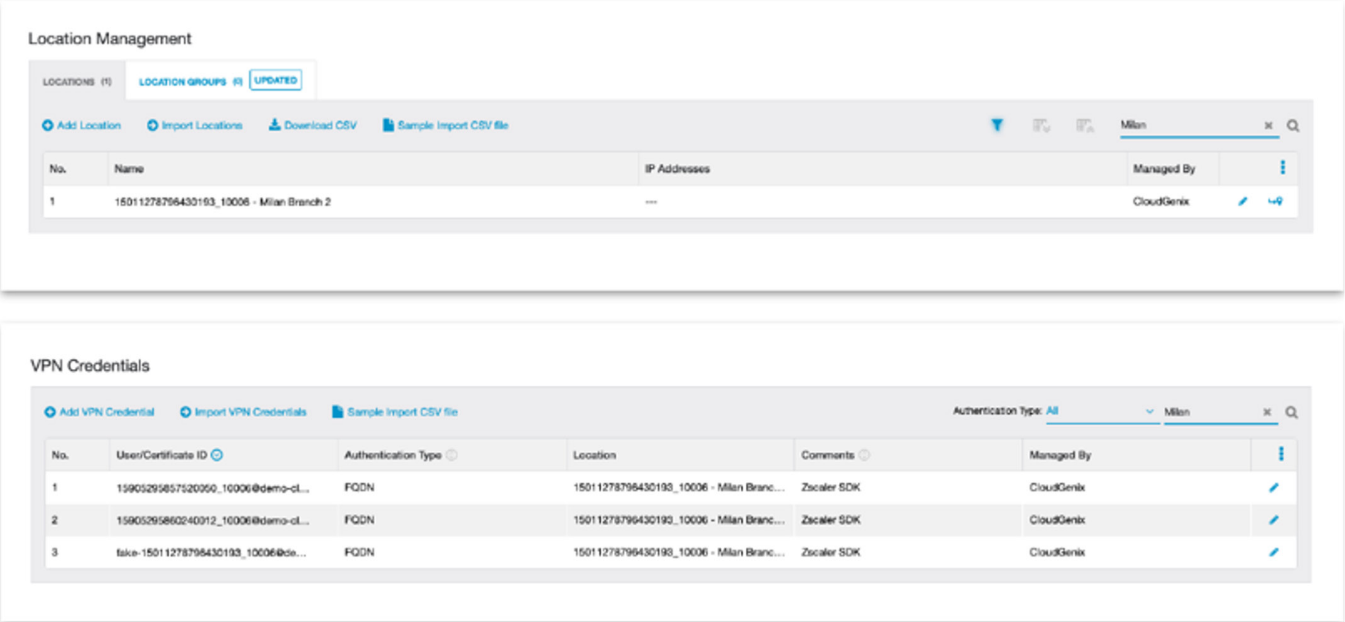
Figure 31. Circuit label

2. Additionally, from version 2.1.0, establishing GRE tunnels requires a usable public IP.
   a. If the interface is connected directly to the internet and a public IP is available, provide the public IP as part of the DHCP or Static IP address. Do not block the Public IP by any firewall.
   b. If the interface is behind a NAT, provide the public IP address in the External NAT Address section.

If you change an IP as part of the static public address or NAT address, the existing tunnels are deleted, and new tunnels established. The polling to identify these changes happens in 10-minute intervals.

Validate the Zscaler Configuration

The Zscaler CloudBlade provisions locations and unique VPN credentials per tunnel within Zscaler. The following is a sample output of the deployment for the Milan Branch 2 site from the ZIA Admin Portal. This site has two circuits. Note that there is a third "fake" VPN credential that is never used but is part of the initial location creation and onboarding process.



Location Management

No.	Name	IP Addresses	Managed By
1	15011278796430193_10006 - Milan Branch 2	---	CloudGenix

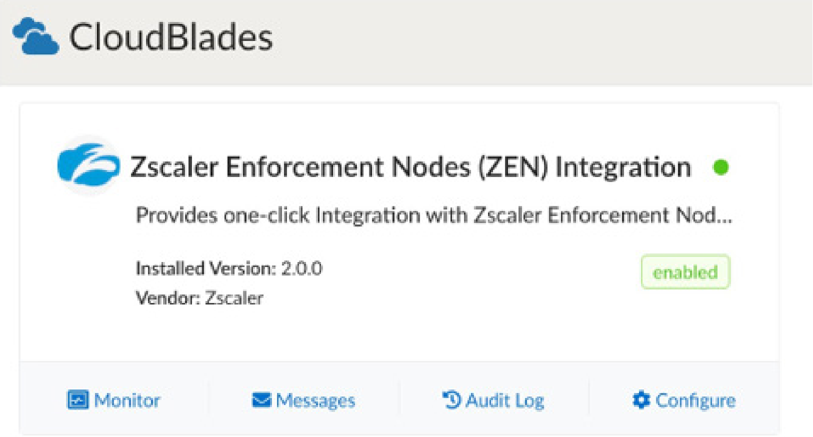
VPN Credentials

No.	User/Certificate ID	Authentication Type	Location	Comments	Managed By
1	15905295857520050_10006@demo-cl...	FQDN	15011278796430193_10006 - Milan Branc...	Zscaler SDK	CloudGenix
2	15905295860240012_10006@demo-cl...	FQDN	15011278796430193_10006 - Milan Branc...	Zscaler SDK	CloudGenix
3	fake-15011278796430193_10006@de...	FQDN	15011278796430193_10006 - Milan Branc...	Zscaler SDK	CloudGenix

Figure 32. CloudBlade deployment

Validate the status of the deployment and tunnels on the CloudBlades page as follows:

1. On the **CloudBlades** window, click **Monitor**.



CloudBlades

Zscaler Enforcement Nodes (ZEN) Integration

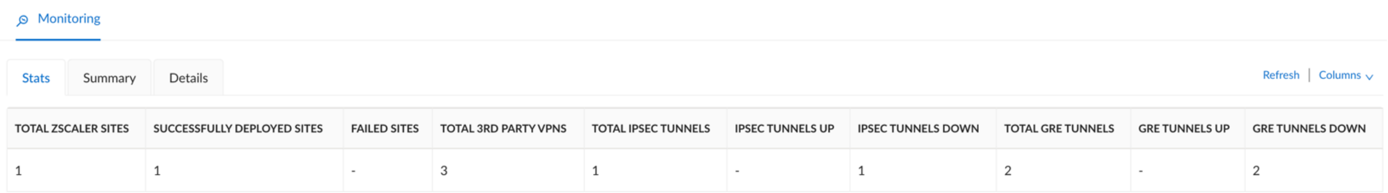
Provides one-click Integration with Zscaler Enforcement Nod...

Installed Version: 2.0.0

Vendor: Zscaler

Figure 33. Monitor

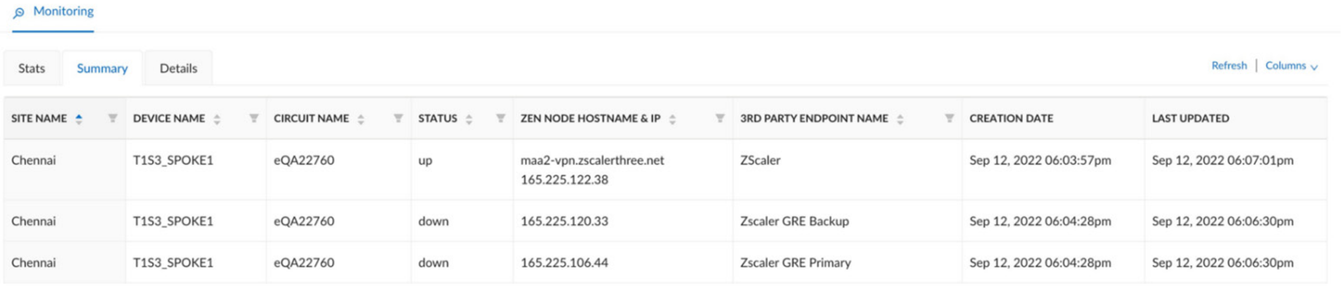
2. Select the **Stats** tab to see information on the Zscaler sites and status of the IPSec and GRE tunnels.



TOTAL ZSCALER SITES	SUCCESSFULLY DEPLOYED SITES	FAILED SITES	TOTAL 3RD PARTY VPNS	TOTAL IPSEC TUNNELS	IPSEC TUNNELS UP	IPSEC TUNNELS DOWN	TOTAL GRE TUNNELS	GRE TUNNELS UP	GRE TUNNELS DOWN
1	1	-	3	1	-	1	2	-	2

Figure 34. Stats

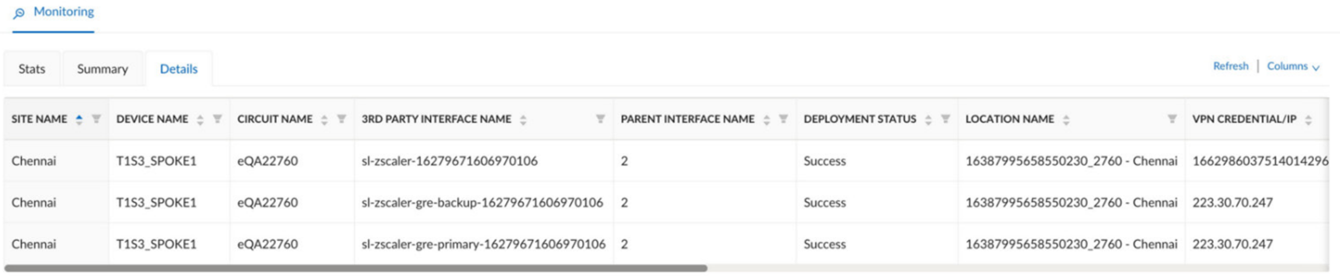
3. Select the **Summary** tab to see an overview of all the connected sites, each **ZEN Node** endpoint (Public Service Node), and name of the third-party endpoints.



SITE NAME	DEVICE NAME	CIRCUIT NAME	STATUS	ZEN NODE HOSTNAME & IP	3RD PARTY ENDPOINT NAME	CREATION DATE	LAST UPDATED
Chennai	T1S3_SPOKE1	eQA22760	up	maa2-vpn.zscalerthree.net 165.225.122.38	ZScaler	Sep 12, 2022 06:03:57pm	Sep 12, 2022 06:07:01pm
Chennai	T1S3_SPOKE1	eQA22760	down	165.225.120.33	Zscaler GRE Backup	Sep 12, 2022 06:04:28pm	Sep 12, 2022 06:06:30pm
Chennai	T1S3_SPOKE1	eQA22760	down	165.225.106.44	Zscaler GRE Primary	Sep 12, 2022 06:04:28pm	Sep 12, 2022 06:06:30pm

Figure 35. Summary

4. Select the **Details** tab to view the **Deployment Status** and the configuration details. These details are helpful for troubleshooting.



SITE NAME	DEVICE NAME	CIRCUIT NAME	3RD PARTY INTERFACE NAME	PARENT INTERFACE NAME	DEPLOYMENT STATUS	LOCATION NAME	VPN CREDENTIAL/IP
Chennai	T1S3_SPOKE1	eQA22760	sl-zscaler-16279671606970106	2	Success	16387995658550230_2760 - Chennai	1662986037514014296
Chennai	T1S3_SPOKE1	eQA22760	sl-zscaler-gre-backup-16279671606970106	2	Success	16387995658550230_2760 - Chennai	223.30.70.247
Chennai	T1S3_SPOKE1	eQA22760	sl-zscaler-gre-primary-16279671606970106	2	Success	16387995658550230_2760 - Chennai	223.30.70.247

Figure 36. Details

Edit Application Network Policy Rules

After CloudBlade configures the appropriate Standard VPN objects within CloudGenix SD-WAN and Zscaler, the administrator can reference the path (Standard VPN) and service group (Zscaler) within application network policies. The ION devices make intelligent per-app path selections using the network policies to chain multiple path options together in Active-Active and Active-Backup modes.

Example:

- Application A: Take Standard VPN direct to Zscaler.
- Application B: Take Standard VPN direct to Zscaler; Backup to Direct Internet.
- Application C: Go to Internet via CloudGenix SD-WAN Data Center; Backup to Standard VPN direct to Zscaler.
- Application D: Use only Direct Internet.

The CloudGenix SD-WAN Secure Application Fabric (AppFabric) enables granular controls for virtually unlimited number of policy permutations down to the subapplication level. Here are some of the most common examples of how traffic policy can be configured per application:

- Send all internet-bound traffic from a set of branches to a Zscaler data center (Blanket Greylist).
- Send all internet-bound traffic from a set of branches to a Zscaler data center, with the exception of specific known applications (Greylist-Whitelist).
- Send all internet traffic direct to the internet except for certain applications needing additional inspection or security (Whitelist-Greylist).

Understand Service and Data Center Groups

CloudGenix SD-WAN uses mapping of Standard VPN services and CloudGenix SD-WAN data centers to allow flexibility when creating network policy rules, while accounting for uniqueness across sites. For example, an administrator could create a single network policy that directs all HTTP and SSL internet-bound traffic through the closest Public Service Edge in the region if it is available and meets the application SLA if the administrator leverages a CloudGenix SD-WAN Data Center site as a transit point.

This is where the concept of endpoints, groups, and domains come into play. To leverage the underlying resources available to an administrator, it is important to understand how an endpoint, group, and domain work in the CloudGenix SD-WAN system.

- Endpoint. A service endpoint is a label representing a specific location or network service. It can be of type CloudGenix SD-WAN, specifically CloudGenix SD-WAN Data Centers for Data Center transit services, or of type Standard VPN. In this release, the only Standard VPN service that can be configured VPNs to cloud security services. However, in a subsequent release, there could be other network services that would use this same construct.
- Group. A service group is a label representing a set of common service endpoint types. This service group label is used in network policy rules to express intent to allow or force traffic to the defined service endpoints. It can be of type CloudGenix SD-WAN or Standard VPN and might contain zero or more service endpoints.
- Domain. A domain is a collection of groups which can be assigned to a set of sites. There can be multiple domains defined, but a site can only be assigned to one domain at a time.

A site uses only the endpoints configured in a group within a domain that is assigned to the site. The same group, however, can be in multiple domains with different service endpoints, allowing you to use the same policy across different sites utilizing different endpoints.

Use the following figure to further explore the concept of endpoints, groups, and domains.

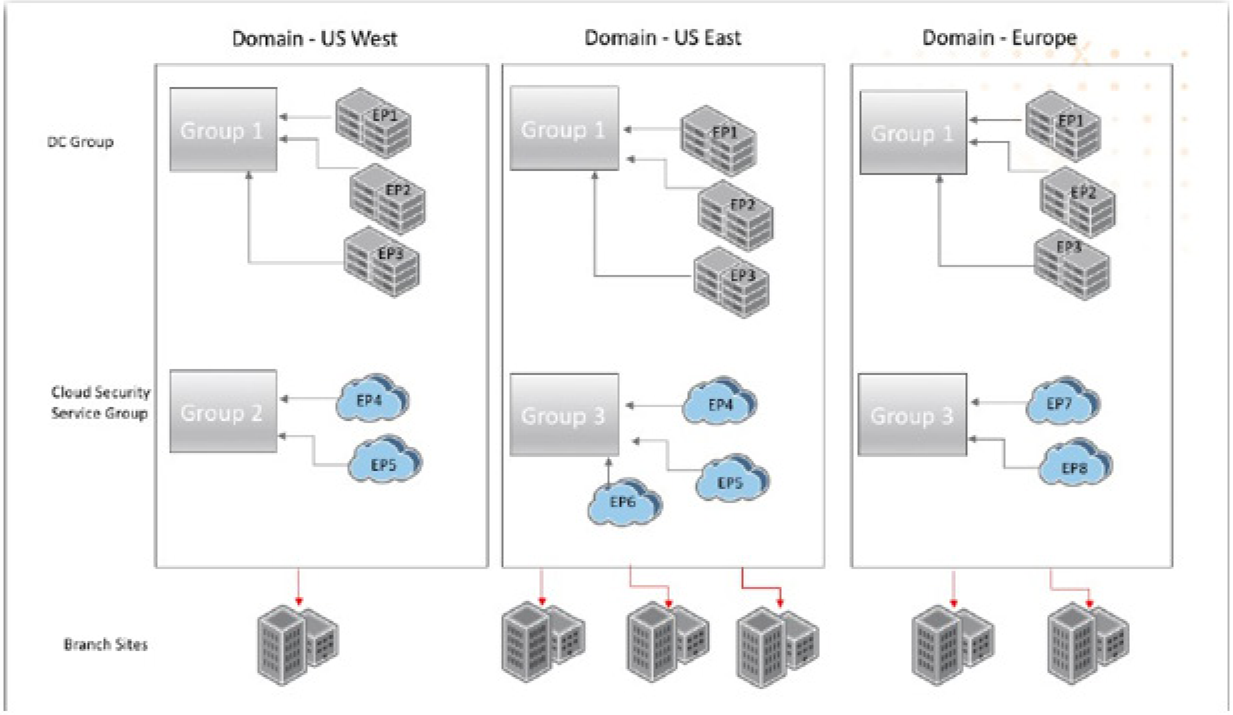
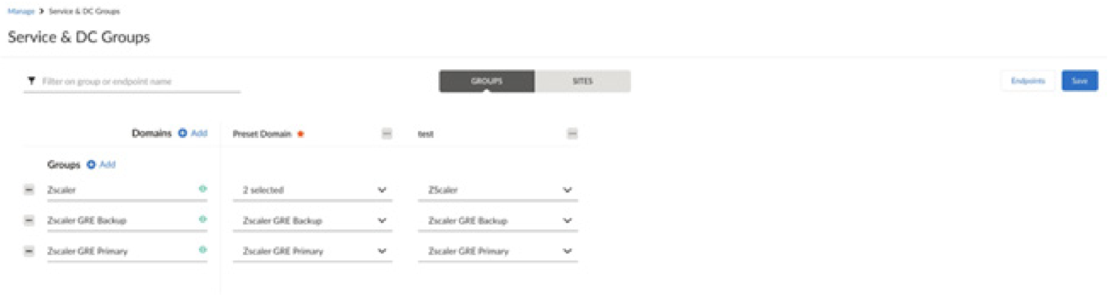


Figure 37. Endpoints, Groups, and Domains

The illustration displays how endpoints added to a group are associated with a domain. The domains are then bound to a site, thus mapping Standard VPN services or CloudGenix SD-WAN data centers uniquely for each site. Note that a group, with different endpoints, can be mapped to one or more domains and a domain can be mapped to one or more sites.

Another example to illustrate the concept is shown next as a screenshot. For a customer with sites in North America and Europe that has one CloudGenix SD-WAN-enabled data center in each region and has adopted Zscaler within each region, the domain mapping is accomplished as follows:


Manage > Service & DC Groups
Service & DC Groups
Filter on group or endpoint name
GROUPS
SITES
Endpoints
Save

Domains Add	Preset Domain *	test
Groups Add		
Zscaler	2 selected	ZScaler
Zscaler GRE Backup	Zscaler GRE Backup	Zscaler GRE Backup
Zscaler GRE Primary	Zscaler GRE Primary	Zscaler GRE Primary

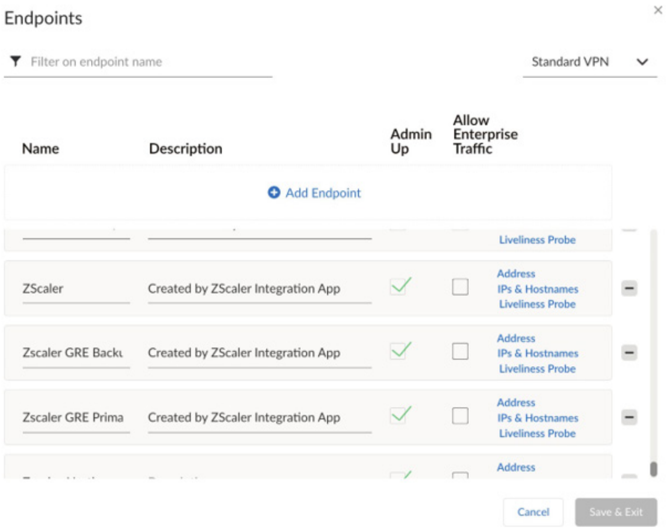
Figure 38. Example deployment

- The Zscaler CloudBlade creates a single group Zscaler with a single Standard VPN endpoint.
- The Standard VPN endpoint has all possible Zscaler hostnames, and based on a latency check, the ION builds a VPN tunnel to the closest Public Service Edge.
- From version 2.0.0, the Zscaler CloudBlade creates two groups: Zscaler GRE Primary and Zscaler GRE Backup.
- You can add the same endpoint to more than one group.
- Only one active group and one backup group can be used in a network policy rule.

Verify Standard VPN Endpoints

With the Zscaler CloudBlade installed, Standard VPN endpoint with hostnames for IPSec and IPs for GRE are created automatically. There is no action required, the following steps are provided only for reference.

1. From the CloudGenix SD-WAN web interface, go to **Manage** > **Resources** > **Service & DC Groups**.
2. Select **Endpoints** and filter by Standard VPN.



Name	Description	Admin Up	Allow Enterprise Traffic	
ZScaler	Created by ZScaler Integration App	✓	□	Address IPs & Hostnames Liveliness Probe
Zscaler GRE Backu	Created by ZScaler Integration App	✓	□	Address IPs & Hostnames Liveliness Probe
Zscaler GRE Prima	Created by ZScaler Integration App	✓	□	Address IPs & Hostnames Liveliness Probe

Figure 39. Standard VPN

The hostnames programmed for this endpoint are displayed under the **Hostnames** tab.

The ION device assigned to sites and circuit types with the AUTO-zscaler tag performs a latency check for each hostname listed under the Standard VPN endpoint. The list is sorted based on the fastest to the slowest response. The first reachable hostname is used to build the Standard VPN.

If the Public Service Edge hostname selected becomes unavailable after the IPSec tunnel is established, either by IPSec DPD or via the Layer 7 health probe specified on the Standard VPN endpoint (see the following figure), the ION device attempts to establish a new IPSec VPN to the next hostname in the ordered list.

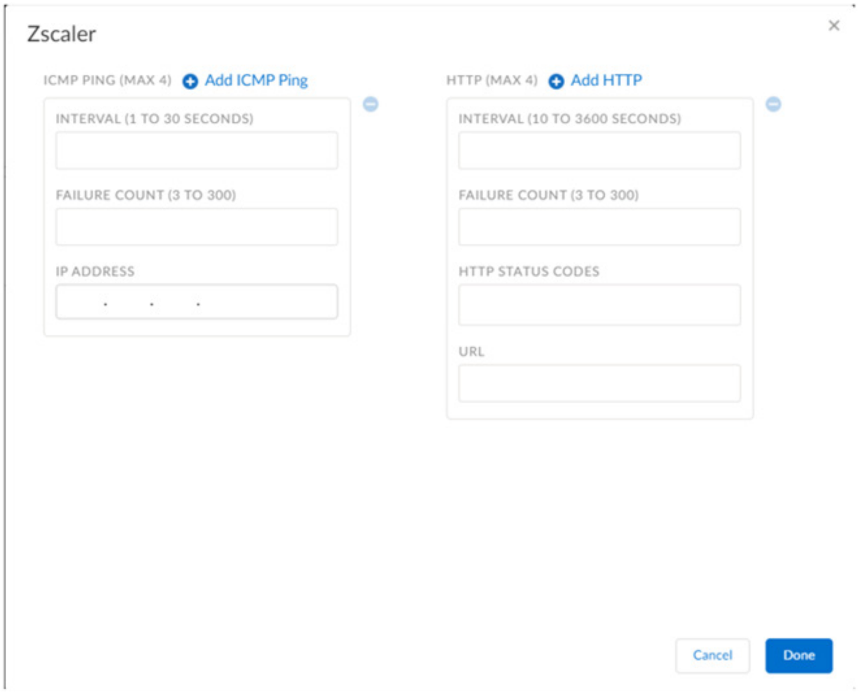


Figure 40. New IPSec VPN

In CloudBlade version 2.0.0, GRE does not establish a new VPN if the current IP is not reachable. You can update the GRE tunnels to the new data center IPs by using the Zscaler-requery-GRE-IPs tag on the site.

Since no action is required here, proceed to verifying Groups and Domains.

Verify Standard VPN Group

With the Zscaler CloudBlade installed, a Standard VPN group is automatically created as Zscaler, Zscaler GRE Primary, and Zscaler GRE Backup.

There is no action required, as the domains associated with a site that has been tagged with AUTO-zscaler or AUTO-zscaler-GRE automatically has the group and endpoint configured.

If more than one endpoint is a part of a group, all the endpoints are considered equal in network policy path selection.

Finally, proceed to binding domains to sites.

Assign Domains to Sites

Binding a domain is essentially mapping a site to a domain, enabling access to all the endpoints within groups/domain. You can map different domains to different sites, but you can map only one domain per site. The following workflow is only for reference, since there are no configuration changes required for the Zscaler CloudBlade.

To bind a domain to a site:

1. Click **Resources** > **Service & DC Groups** > **Sites**.
2. From the **Domain list** next to each site, select the appropriate domain. To edit information for all sites at a time, click **Edit All**.
3. Click **Save**.

Use Groups in Network Policy Rules

Before you can use a Standard VPN in a policy rule, you must define service endpoint groups. Each group can have one or more CloudGenix SD-WAN data centers or Standard VPN service endpoints. A group is used in policy rules. The domain defining the mappings for endpoints to groups must be assigned to a site for the policy rules using the group to be effective.

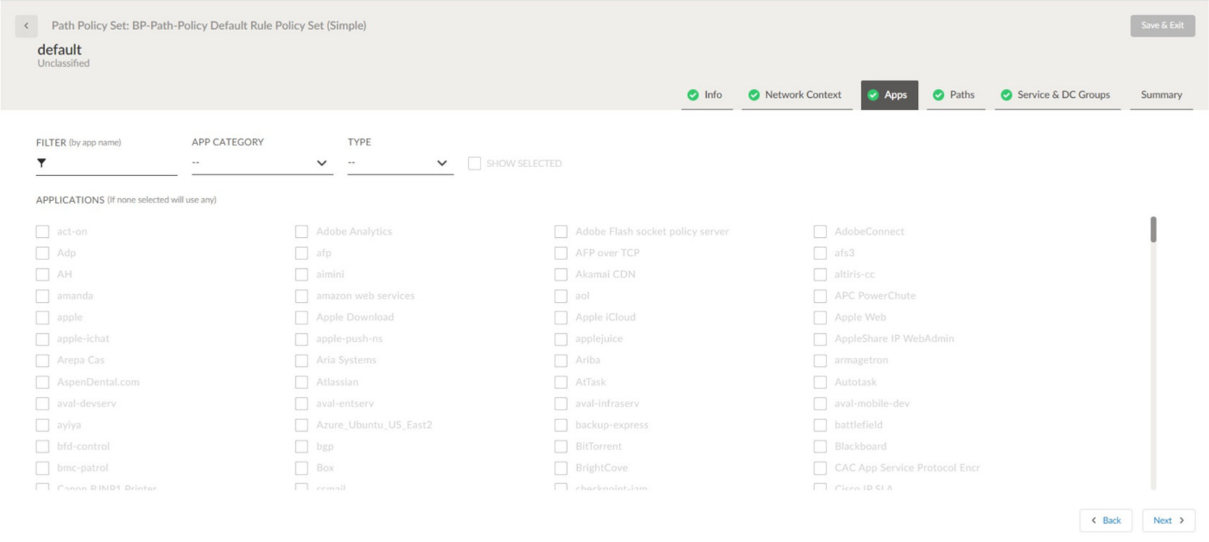
There are four combinations of Active/Backup groups that you can use in Policies. You can select just one CloudGenix SD-WAN group or one non-CloudGenix SD-WAN group as an active or backup path in policies. For example:

Active Group	Backup Group	Example
Standard VPN	CloudGenix SD-WAN	Internet-bound SSL traffic from a branch site transits through the Cloud Security Service. In the event all Standard VPN paths to any of the endpoints in the Primary Cloud Security Service group are not available, internet-bound SSL traffic transits through one of the CloudGenix SD-WAN data center endpoints assigned to that via the CloudGenix SD-WAN VPN.
CloudGenix SD-WAN	Standard VPN	Internet-bound SSL traffic from a branch site transits through one of the CloudGenix SD-WAN data center endpoints assigned to that group via the CloudGenix SD-WANs. In the event all CloudGenix SD-WAN VPNs to all of the Data Center endpoints in the group are unavailable, internet-bound SSL traffic transits through the Cloud Security Service via one of the Standard VPN paths to any of the endpoints in the Standard VPN group.
Standard VPN	Standard VPN	Internet-bound SSL traffic from a branch site transits through the primary cloud security service via one of the Standard VPN paths to any of the endpoints in the primary cloud security service group. In the event all Standard VPNs are down to all endpoints in the primary group, the internet-bound SSL traffic transits through the backup cloud security service via one of the Standard VPN paths to the endpoints that are part of the backup group.
CloudGenix SD-WAN	CloudGenix SD-WAN	Internet-bound SSL traffic from a branch site transits through one of the CloudGenix SD-WAN data center endpoints assigned to the active group via the VPNs. In the event all CloudGenix SD-WAN VPNs to all of those endpoints are down, internet-bound SSL traffic transits through one of the CloudGenix SD-WAN data center endpoints assigned to the backup group via the CloudGenix SD-WAN VPNs.

Use a Group in Stacked Policies

To use a group in Stacked Policies:

1. Go to **Policies** > **Stacked Policies** > **Path** > **Path Sets**, and then select a path policy set.
2. Within the policy set, select a rule to edit or add a new rule.
3. Go to **Apps** and select the required applications or confirm that the required applications are selected.



Path Policy Set: BP-Path-Policy Default Rule Policy Set (Simple)

default
Unclassified

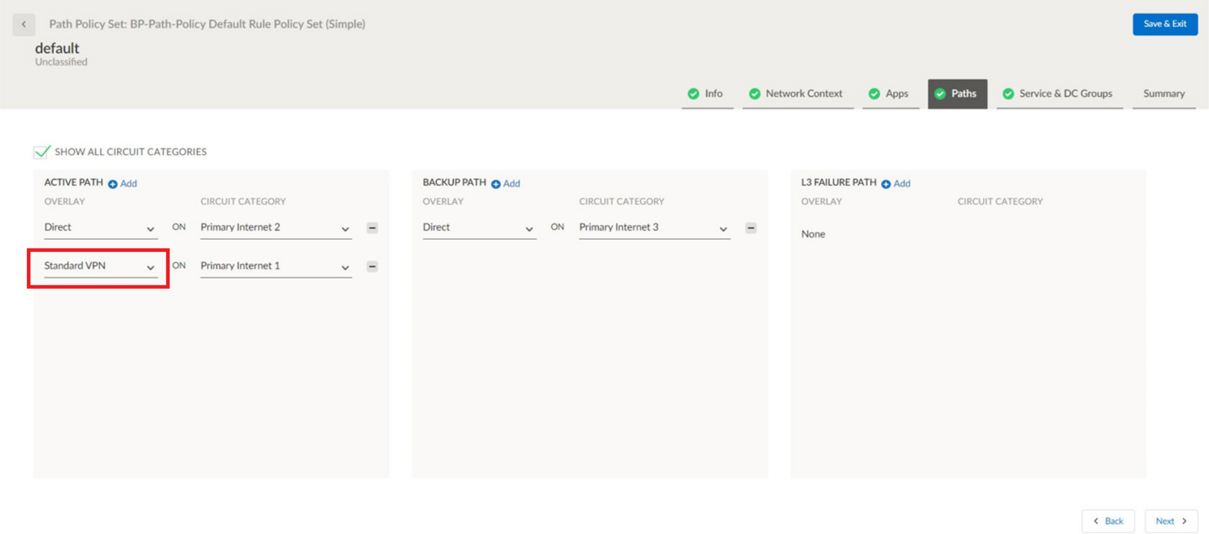
FILTER (by app name):
APP CATEGORY: --
TYPE: --
□ SHOW SELECTED

APPLICATIONS (If none selected will use any)

□ act-on
□ Adp
□ AH
□ amanda
□ apple
□ apple-ichat
□ Arepa Cas
□ AspenDental.com
□ aval-devserv
□ ayiya
□ bfd-control
□ bmc-patrol
□ Canon BJNP1 Printer
□ Adobe Analytics
□ afp
□ aimini
□ amazon web services
□ Apple Download
□ apple-push-ns
□ Aria Systems
□ Atlassian
□ aval-entserv
□ Azure_Ubuntu_US_East2
□ bgp
□ Box
□ ccmail
□ Adobe Flash socket policy server
□ AFP over TCP
□ Akamai CDN
□ aol
□ Apple iCloud
□ applejuice
□ Ariba
□ AtTask
□ aval-infraserv
□ backup-express
□ BitTorrent
□ BrightCove
□ checkpoint-iam
□ AdobeConnect
□ afs3
□ altiris-cc
□ APC PowerChute
□ Apple Web
□ AppleShare IP WebAdmin
□ armagetron
□ Autotask
□ aval-mobile-dev
□ battlefield
□ Blackboard
□ CAC App Service Protocol Encr
□ Cisco IP SLA

Figure 41. Apps

4. On the **Paths** tab, select the **Active** and/or **Backup** path as Standard VPN on <circuit category> or Any Public/Private to allow the system to use any/all paths of that type.



Path Policy Set: BP-Path-Policy Default Rule Policy Set (Simple)

default
Unclassified

☑ SHOW ALL CIRCUIT CATEGORIES

ACTIVE PATH
OVERLAY: Direct ON CIRCUIT CATEGORY: Primary Internet 2
OVERLAY: Standard VPN ON CIRCUIT CATEGORY: Primary Internet 1

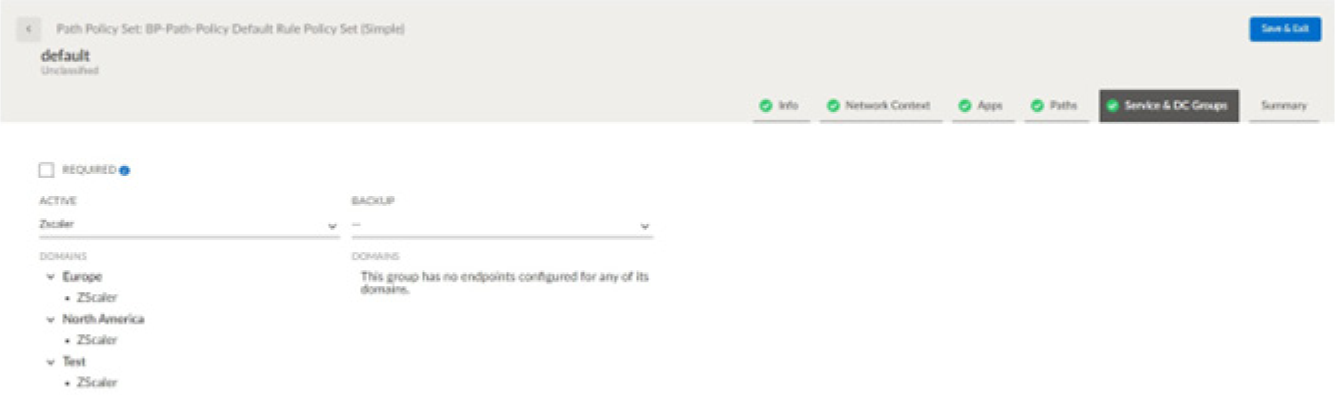
BACKUP PATH
OVERLAY: Direct ON CIRCUIT CATEGORY: Primary Internet 3

L3 FAILURE PATH
OVERLAY: None

Figure 42. Paths

You can mix Standard VPNs with other available paths—private, public, direct or VPNs.

5. On the **Service & DC Group** tab, select **Zscaler** as the Standard VPN group.
6. Click **Save & Exit**.



default
Unclassified

☐ REQUIRED

ACTIVE: Zscaler

BACKUP: --

DOMAINS
- Europe
  - ZScaler
- North America
  - ZScaler
- Test
  - ZScaler

DOMAINS
This group has no endpoints configured for any of its domains.

Figure 43. Service & DC Group

If Standard VPN path is used in a network policy, then you must have a Standard VPN Service & DC Group defined in the policy for the traffic to transit through that group. If not, traffic is blackholed.

If Required is selected, traffic always transits through the Service & DC Group. If not selected, traffic might transit through the Service & DC Group per policy.

Manage and Troubleshoot the Zscaler CloudBlade

The following sections detail various operations and troubleshooting scenarios related to the integration process.

- Enable, Pause, Disable, and Uninstall the CloudBlade
- Installation Troubleshooting
- Troubleshoot Standard VPNs
- Zscaler Location Gateway Options

Enable, Pause, Disable, and Uninstall the CloudBlade

After CloudBlade is set up, operations can be done using the CloudBlade panel. These operations have various effects on the tunnels and configurations in CloudGenix SD-WAN and Zscaler.

- Set the CloudBlade to Enabled. Enabled is the standard expected mode of operation for CloudBlade. CloudBlade runs every 60 seconds, find any new Sites or Circuits with the appropriate tags, and configure the integration on Zscaler and CloudGenix SD-WAN. In addition, during this integration run, if any settings were previously modified manually on either CloudGenix SD-WAN or Zscaler (for example VPN credentials changed, or Location deleted in Zscaler), these are reverted to the known good state automatically.
- Set the CloudBlade to Paused. Pausing CloudBlade stops all future integration runs but leaves any created objects intact. This stops any future objects from getting created but does not prevent removal of any unconfigured/ untagged objects on either CloudGenix SD-WAN or Zscaler.
- Set the CloudBlade to Disabled. Disabling the CloudBlade tells the system to remove and delete all configurations created by the CloudBlade. This can cause communication interruptions if the policy isn't set to use other paths. The IPSec policies, IKE policies, and CloudGenix SD-WAN endpoints and Service & DC groups aren't automatically deleted and must be removed manually.
- Uninstalling CloudBlade. Uninstalling CloudBlade removes the configuration for CloudBlade, and immediately stops any changes by CloudBlade. Uninstalling CloudBlade doesn't automatically remove configuration from all sites and objects. You can uninstall and reinstall CloudBlade to facilitate upgrades or downgrades to different versions without traffic interruption. To completely remove all items, set the CloudBlade to Disabled for 2–3 integration run periods (180 seconds) before uninstalling the CloudBlade.

Installation Troubleshooting

A few common scenarios administrators should be aware of when attempting to do the initial installation of the Zscaler CloudBlade.

- Wrong API Key or Partner Admin Credentials
- CloudGenix SD-WAN Standard VPNs Not Created

Wrong API Key or Partner Admin Credentials

If an administrator incorrectly enters the API key or Partner Admin credentials, the system alerts the administrator by reporting the status in the CloudBlades window.

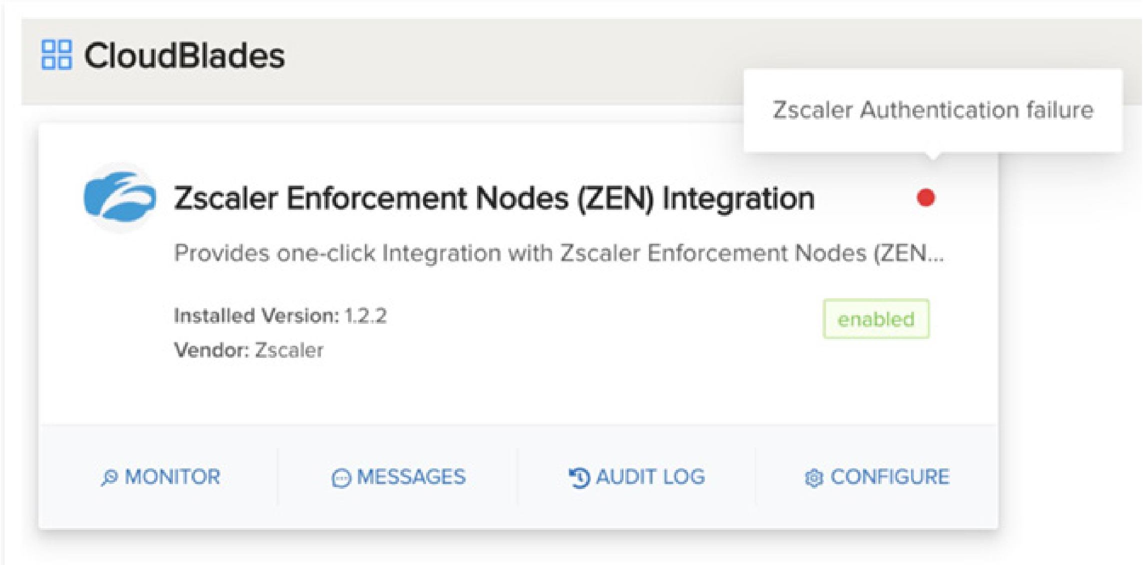
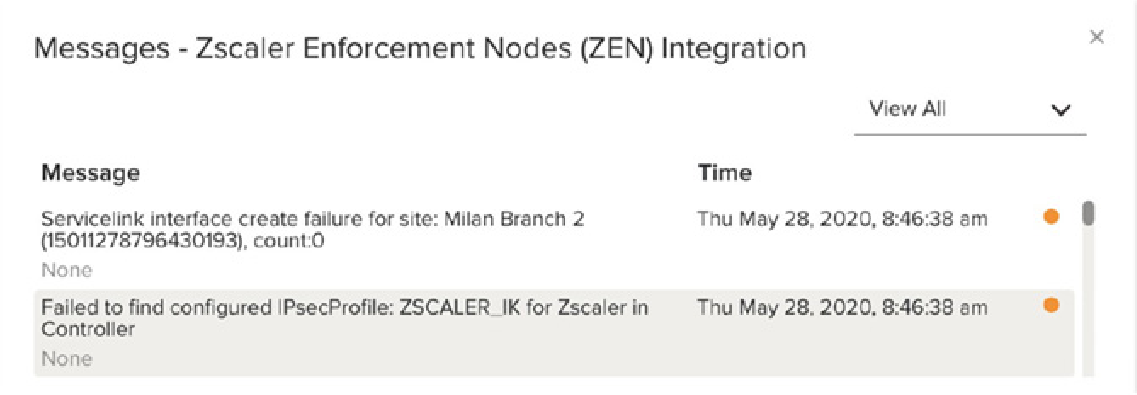

CloudBlades
Zscaler Authentication failure
Zscaler Enforcement Nodes (ZEN) Integration
Provides one-click Integration with Zscaler Enforcement Nodes (ZEN...
Installed Version: 1.2.2
Vendor: Zscaler
enabled
MONITOR
MESSAGES
AUDIT LOG
CONFIGURE

Figure 44. CloudBlade alert

CloudGenix SD-WAN Standard VPNs Not Created

There could be a scenario in which all user credentials, keys, and tokens are correct, and the Zscaler Location and VPN credential objects are also created. However, the CloudGenix SD-WAN VPNs are not created. This can be due to the pre-built IPSec profiles based on Zscaler's recommended best practices, which have not been allocated to your CloudGenix SD-WAN tenant. Another reason could be that the custom IPSec profile name specified in your CloudBlade configuration does not exist (or has a typo in it).

Validate this condition by selecting the Messages link on the CloudBlade card and looking for an error message similar to the following.



Message	Time
Servicelink interface create failure for site: Milan Branch 2 (15011278796430193), count:0 None	Thu May 28, 2020, 8:46:38 am
Failed to find configured IPsecProfile: ZSCALER_IK for Zscaler in Controller None	Thu May 28, 2020, 8:46:38 am

Figure 45. CloudBlade message

To verify that these IPSec profiles exist, go to Stacked Policies > IPSec Profiles, and check if the profiles shown in the example below are displayed. If these two profiles are not present, contact CloudGenix SD-WAN support. Or create your own IPSec profile and that name in your CloudBlade configuration.

The next section covers troubleshooting issues after CloudBlade is installed.

Troubleshoot Standard VPNs

Start with the Zscaler Test Page to verify and troubleshoot client traffic to and through ZIA Public Service Edges. All application and path metrics are collected and reported, and all application monitoring alarms and alerts are generated for Standard VPNs. To troubleshoot Standard VPNs, view Alerts and Alarms, Connectivity of Standard VPNs at the site level, and Activity charts to view possible issues with the VPN. In addition, device toolkit commands can be used to view Standard VPN stats, status, and summary.

Use the Zscaler Test Page

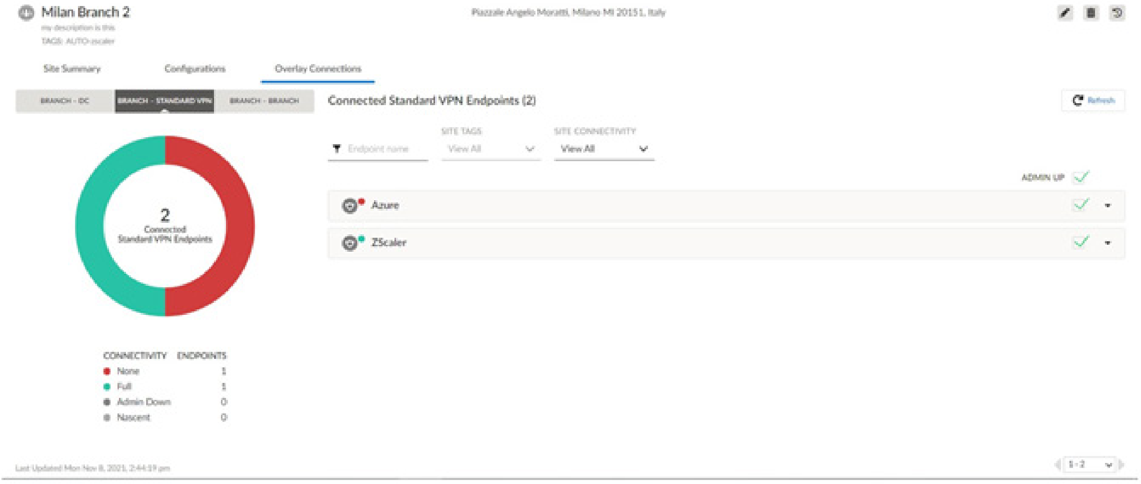
Zscaler provides a diagnostic page that allows for verification and troubleshooting of client traffic to and through Public Service Edges. To access the page from any client, open the link http://ip.zscaler.com.

For more details on this tool, see [Verifying a User's Traffic is Being Forwarded to the Zscaler Service]().

View Standard VPN at Site Level

The Map provides a quick view of interface status at the site level.

Select **Map**, select a site, and under **Connectivity**, click **Standard VPN** to view the status of the Standard VPN.



Milan Branch 2

my description is this

TAGS: AUTO-zscaler

Piazzale Angelo Moratti, Milano MI 20151, Italy

Connected Standard VPN Endpoints (2)

- Azure ✓
- ZScaler ✓

CONNECTIVITY	ENDPOINTS
None	1
Full	1
Admin Down	0
Nascent	0

Last Updated Mon Nov 8, 2021, 2:44:19 pm

Figure 46. Standard VPN status

View Alerts and Alarms

If a Standard VPN tunnel interface is down, an alarm is raised, just like it would for any other interface within the system.

View Activity Charts

Activity Charts can be filtered based on paths, including Standard VPNs. Traffic analytics can be viewed through Network Analytics, Media Analytics, and Flow Browser Charts for Standard VPNs.

From Quick Filters, under WANs, make sure to select **Standard VPN**. Or, from **Paths**, select a specific Standard VPN to display analytics for that path.

Zscaler Location Gateway Options

CloudBlade version 1.2.2 supports the following gateway options:

Options	Corresponding CloudGenix Access for Networks Tag
Use XFF from Client Request	Gateway Options: <True | False>Sub Locations: Disabled
Enforce Zscaler App SSL Setting	Deprecated
Enable SSL Inspection	Deprecated
Enforce Firewall Control	<True | False>
Enforce Authentication	<True | False>
Enable IP Surrogate	<True | False>Idle time: <val>Idle time metric: <minutes | hours | days>
Enable Surrogate IP for Known Browsers	<True | False>Refresh time: <val>Refresh time metric: <minutes | hours | days>
Enable Caution	<True | False>

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

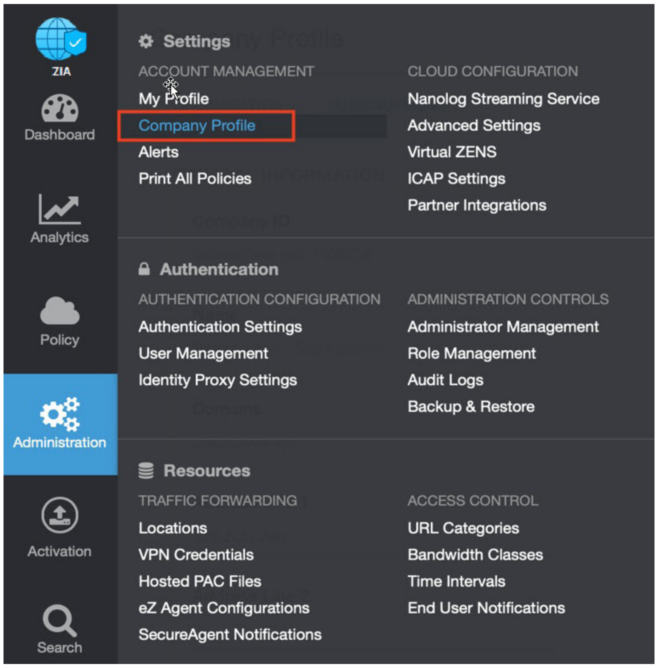
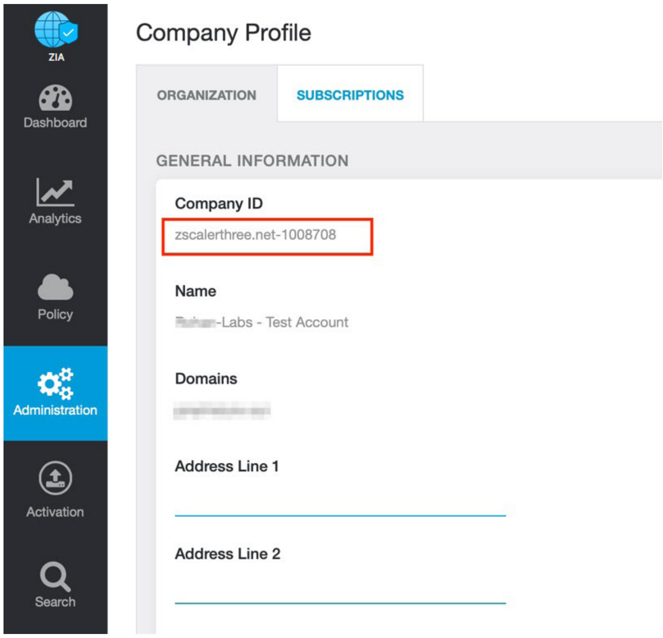


Figure 47. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 48. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

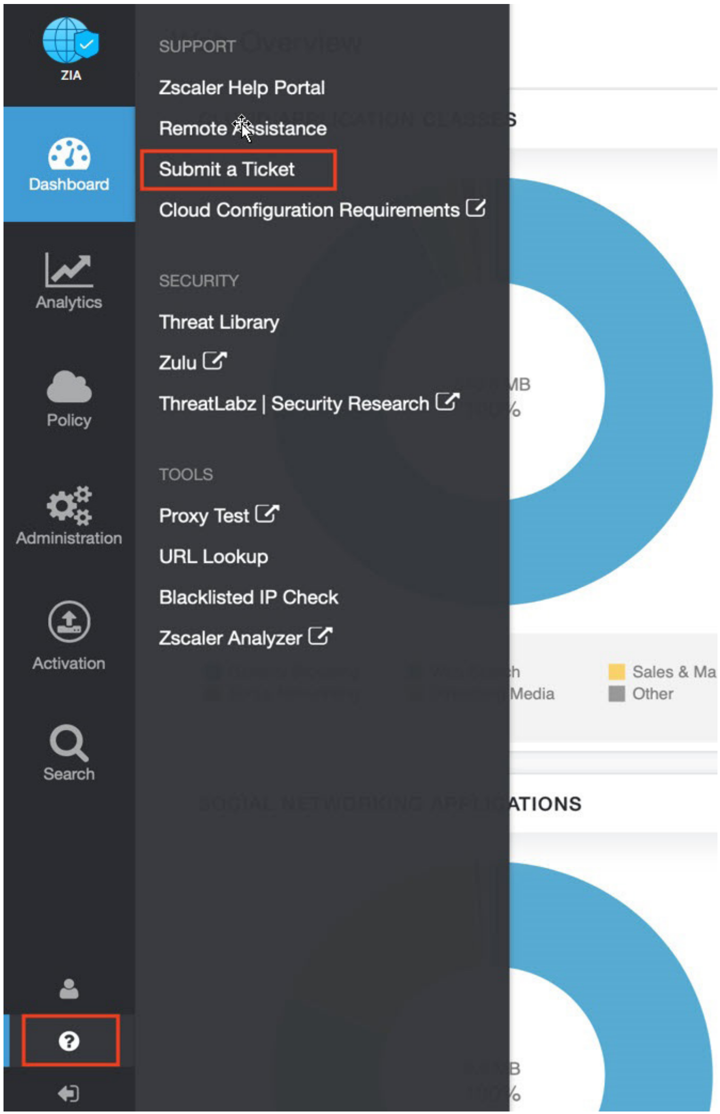


Figure 49. Submit a ticket