CloudGenix Customer Support

For technical issues, contact CloudGenix Customer Support.

PHONE: 1-844-800-2469, Ext. 2
EMAIL: support@cloudgenix.com
INTEGRATING WITH ZSCALER INTERNET ACCESS........................................................................4
PREREQUISITES..................................................................................................................5
PLANNING THE DEPLOYMENT...............................................................................................6
ACQUIRE THE ZSCALER INFORMATION...............................................................................8
CONFIGURE AND INSTALL THE ZSCALER INTEGRATION CLOUDBLADE ......................12
ASSIGN TAGS TO OBJECTS IN THE CLOUDGENIX PORTAL.............................................14
VALIDATING ZSCALER CONFIGURATION............................................................................18
EDIT APPLICATION NETWORK POLICY RULES.................................................................18
UNDERSTANDING SERVICE AND DATA CENTER GROUPS.............................................19
VERIFY THIRD PARTY VPN ENDPOINTS ..........................................................................21
VERIFY THIRD PARTY GROUP .........................................................................................23
ASSIGNING DOMAINS TO SITES.......................................................................................24
USE GROUPS IN NETWORK POLICY RULES ....................................................................25
MANAGING AND TROUBLESHOOTING THE ZSCALER INTEGRATION CLOUDBLADE ......30
ENABLING, PAUSING, DISABLING AND UNINSTALLING THE INTEGRATION.................30
INSTALLATION TROUBLESHOOTING...............................................................................31
Wrong API Key or Partner Admin credentials ..................................................................31
Improper Settings for CloudGenix User Doing Initial Installation ..................................32
CloudGenix 3rd Party VPNs Not Created .........................................................................34
TROUBLESHOOTING THIRD PARTY VPNS......................................................................35
USE THE ZSCALER TEST PAGE ......................................................................................35
VIEW THIRD PARTY VPN ON THE DASHBOARD ............................................................36
VIEW THIRD PARTY VPN AT SITE LEVEL ........................................................................37
VIEW ALERTS AND ALARMS .........................................................................................38
VIEW ACTIVITY CHARTS ..................................................................................................39
USE THE DEVICE TOOLKIT ............................................................................................40
Integrating with Zscaler Internet Access

As enterprises rely on SaaS or Cloud-based delivery models for business-critical applications, there is 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.

The integration of CloudGenix SD-WAN and Zscaler Internet Access (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 Release 5.1.1 and later provides a CloudBlade to automatically integrate the CloudGenix Controller, Remote CloudGenix IONs and ZIA Public Service Edge. ZIA Public Service Edge is the new name for what was previously known as “Zscaler Enforcement Node” or ZEN.
Prerequisites

The following items are required for configuring CloudGenix and Zscaler Internet Access integration:

CloudGenix

- An active CloudGenix subscription.
- CloudGenix AppFabric deployed at one or more locations.
- Physical and/or virtual ION devices running Release 5.1.1 or later.

Zscaler

- An active Zscaler Internet Access Instance (in any cloud)
- Administrator login credentials for this instance.
- A partner administrator account and partner key
Planning the Deployment

The primary way to architecturally accomplish the CloudGenix and Zscaler Internet Access integration is via Third Party IPSEC VPNs from remote ION endpoints to Zscaler. The Zscaler Integration CloudBlade provides the automatic creation, management, and maintenance of the 3rd party IPSEC VPN tunnels by simply entering ‘tags’ on the appropriate CloudGenix objects.

To facilitate this tag-based configuration, the CloudGenix Portal must be configured and linked to Zscaler via a partner administrator account and an SD-WAN partner key.
The following are the steps to complete the integration:

<table>
<thead>
<tr>
<th>Steps</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a partner administrator role, create a partner administrator account and assign the role, and generate an SD-WAN partner key from the Zscaler portal</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure and install the Zscaler Integration CloudBlade in the CloudGenix Portal</td>
</tr>
<tr>
<td>Step 3</td>
<td>Assign tags to objects in the CloudGenix Portal to automatically integrate those objects to Zscaler</td>
</tr>
<tr>
<td>Step 4</td>
<td>Edit application network policy rules to send traffic to the Zscaler</td>
</tr>
</tbody>
</table>

**Note:** Prior to configuring the Zscaler Integration CloudBlade in the CloudGenix portal, make sure that the user account you are logged in with has **IP session lock disabled**. For more information, refer to *Improper Settings for CloudGenix User Doing Initial Installation*. 
Acquire the Zscaler Information

Before configuring CloudGenix to integrate with Zscaler, perform the following:

1. Create a partner administrator role with full access controls to Locations and VPN Credentials.
2. Create a partner administrator account and assign the partner role from step 1.
3. Generate a SD-WAN partner Key
4. Activate Pending Changes on Zscaler.
Configure and Install the Zscaler Integration CloudBlade

Next, configure the CloudGenix CloudBlade to prepare the CloudGenix Controller for integration.

1. From the CloudGenix Portal, click on the logged-in user Email Address to bring up the System Menu, then choose CloudBlades.

2. In CloudBlades, locate the Zscaler Enforcement Nodes (ZEN) Integration CloudBlade. If this CloudBlade does not appear, please contact CloudGenix Support.

*ZEN Public Service Edge is the new name for what was previously known as “Zscaler Enforcement Node” or ZEN. This document still has references to the old name of ZEN.*
3. Clicking on the **Zscaler Enforcement Nodes (ZEN) Integration CloudBlade** will bring up the installation page. Please fill out the following information:
   a. For **Version**, please select the version to use, or leave for the default.
   b. For **Admin State**, leave **Enabled**.
   c. For **API Key** provide the SD-WAN key generated in the previous section.
   d. For **Admin username** and **password** provide the partner administrator account created in the previous section.
   e. For **Zscaler cloud**, provide which Zscaler cloud your subscription is attached to (zscaletherthree in the below example).
   f. Optionally, provide the **base URL** otherwise this will be derived from the admin username domain.

4. Once the settings have been set, press the **Install** button (Or, **Save** if the CloudBlade was previously installed.)

<table>
<thead>
<tr>
<th>Zscaler Integrator</th>
<th>CloudGenix</th>
<th>Zscaler</th>
<th>Not installed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VERSION</strong></td>
<td>1.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NAME</strong></td>
<td>rainier_release</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATUS</strong></td>
<td>gay</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PERMISSIONS</strong></td>
<td>View</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ADMIN STATE</strong></td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>API KEY</strong></td>
<td>jhi3aq9v1</td>
<td>mock</td>
<td></td>
</tr>
<tr>
<td><strong>ADMIN USERNAME</strong></td>
<td><a href="mailto:apitext2@demo-cloudgenix.com">apitext2@demo-cloudgenix.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ADMIN PASSWORD</strong></td>
<td>************</td>
<td>unfitapk</td>
<td></td>
</tr>
<tr>
<td><strong>ZSCALER CLOUD</strong></td>
<td>zscaletherthree</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BASE URL (OPTIONAL)</strong></td>
<td>demo-cloudgenix.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ZIA Public Service Edge is the new name for what was previously known as “Zscaler Enforcement Node” or ZEN.**
Assign Tags to Objects in the CloudGenix Portal

Once the CloudBlade is configured, the next task is to tag CloudGenix sites and circuit categories to denote which sites and circuit types are candidates for auto 3rd party tunnel creation to Zscaler.

1. From the CloudGenix Portal, click Map.

2. Search for a site you wish to connection to Zscaler. Click on the site to bring up the site summary screen.
3. On the side of the site summary panel, click the Edit (✓) icon. The site panel now transforms to the Edit Site Info dialog.

4. Look for the field **TAGS**. In this field, add **AUTO-zscaler** (case sensitive).
5. Click **Save**.

Now that the site has been tagged enabled for Zscaler, we need to tag the circuit categories that can be used to establish a 3\textsuperscript{rd} party tunnel to Zscaler.

**Note:** 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 may not want to use their metered LTE circuit for 3\textsuperscript{rd} party VPN establishment.

1. From the CloudGenix Portal, click **Stacked Policies**

2. Select **Circuit Categories**

3. Find the circuit categories that are associated to your site(s) that you want the system to automatically build 3\textsuperscript{rd} party VPN tunnels from, and tag with **AUTO-zscaler** (case sensitive).
4. Click **Save**.

Once this configuration has been completed, on the next integration cycle (60 seconds), 3rd party IPSEC tunnels to connect the CloudGenix ION and Zscaler will begin the creation/onboarding process. It may take several integration cycles for the tunnels to appear and be active on the CloudGenix portal.
Validating Zscaler Configuration

The Zscaler Integration CloudBlade will provision Locations and unique VPN Credentials per tunnel within Zscaler. Below is a sample output from the Zscaler portal of what was deployed for the Manchester Branch 3 site in the previous section which has 2 circuits.

Edit Application Network Policy Rules

Once the CloudBlade configures the appropriate 3rd party objects within CloudGenix and Zscaler, the administrator can reference the path (3rd party VPN) and service group (Zscaler) within application network policies. The ION devices will 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 3rd Party VPN direct to Zscaler.
- **Application B**: Take 3rd Party VPN direct to Zscaler; Backup to Direct Internet.
- **Application C**: Go to Internet via **CloudGenix Data Center**; Backup to 3rd Party VPN direct to Zscaler.
- **Application D**: Use only Direct Internet.

The CloudGenix secure Application Fabric (AppFabric) enables granular controls for virtually unlimited number of policy permutations down to the sub-application 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 datacenter. (**Blanket Greylist**)
- Send all internet-bound traffic from a set of branches to a Zscaler datacenter 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)

In order modify application policy, the following steps should be performed. They will be detailed in the following sections:

1. Understanding Service and Data Center Groups
2. Verify Third Party VPN Endpoints
3. Configure Third Party Groups
4. Assign Domains to Sites
5. Use Groups in Network Policy Rules

Understanding Service and Data Center Groups

CloudGenix uses mapping of Third Party services and CloudGenix data centers to allow flexibility when creating network policy rules, while accounting for uniqueness across sites. For example, an administrator may want to create a single network policy that directs all HTTP and SSL Internet bound traffic through the closest Zscaler Enforcement Node (ZEN) in the region if it’s available and meets application SLA, but if not, may leverage a CloudGenix 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 system.

**Endpoint** - A service **endpoint** is a label representing a specific location or network service. It can be of type CloudGenix, specifically CloudGenix Data Centers for Data Center transit services, or of type 3rd party. In this release, the only 3rd party service that can be configured are 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 label representing a set of common service **endpoint** types. This service group label will be used in network policy rules to express intent to allow or force traffic to the defined service endpoint(s). It can be of type CloudGenix or 3rd party and may 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 may only be assigned to **one** domain at a time.

Note that a site will be able to use **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.
Let us further explore the concept of endpoints, groups, and domains using the following illustration and screenshot.

The illustration displays how endpoints added to a group are associated with a domain. The domains are then bound to a site, thus mapping 3rd party services or CloudGenix 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 below as a screenshot. For a customer with sites in North America and Europe that has one CloudGenix-enabled data center in each region and has adopted Zscaler within each region the domain mapping is accomplished as follows:

Note:
- The Zscaler CloudBlade creates a single group Zscaler with a single 3rd party Endpoint.
- The 3rd party endpoint has all possible Zscaler hostnames, and based on a latency check the ION will build a VPN tunnel to the closest ZIA Public Service Edge.
- The same endpoint can be added to more than one group.
- Only one active group and one backup group may be used in a network policy rule.
Verify Third Party VPN Endpoints

With the Zscaler Integration installed, a single 3rd party Endpoint with all ZIA Public Service Edge hostnames will automatically be created. There is no action required, but the below is provided as a reference.

1. From the CloudGenix portal click **Stacked Policies** and select **Service & DC Groups**

   ![CloudGenix Portal Stadium Policies](image)

2. Select **Endpoints** and filter by **3rd Party**

   ![CloudGenix Portal Endpoints](image)

3. Below is the list of hostnames programmed for this endpoint.

   ![CloudGenix Endpoint List](image)
The ION assigned to sites and circuit types with the **AUTO-zscaler** tag will perform a latency check to each hostname listed in the 3rd party endpoint. The list will be sorted by fastest to slowest response, and the first reachable hostname will be used to build the 3rd party VPN.

4. If the ZIA Public Service Edge hostname selected becomes unavailable after IPSEC establishment, either by IPSEC DPD OR via the Layer 7 health probe specified on the 3rd party endpoint (see figure below), the ION will attempt to establish a new IPSEC VPN to the next hostname in the ordered list.

Since no action is required here, proceed to verifying **Groups** and **Domains**.
Verify Third Party Group

With the Zscaler Integration installed, one 3rd party group will automatically be created:

- Zscaler

There is no action required as the domains associated to a site which has been tagged with AUTO-zscaler will automatically have the group and endpoint configured.

In the below example sites that are bound to the Preset Domain, Europe, and North America domains all must have 1 or more sites that were tagged with AUTO-zscaler.

Note: If more than one endpoint is part of a group, they will be considered as equal in network policy path selection.

Finally, proceed to binding domains to sites.
Assigning Domains to Sites

Binding a domain is essentially mapping a site to a domain, enabling access to all the endpoints within groups/domain. Different domains can be mapped to different sites, but only one domain may be mapped per site. The below is a reference work flow as there is no configuration changes required for the Zscaler integration.

To bind a Domain to Sites:

1. From Policies, select Service & DC Groups.
2. Select Sites.
3. From the drop-down next to each site, select the appropriate domain. Or, to bulk edit all sites, select the Edit All button.
4. Finally, click Save.
Use Groups in Network Policy Rules

Before you can use a 3rd party VPN in a policy rule, you need to have defined service endpoint groups. Each group can have one or more CloudGenix data centers or 3rd party service endpoints. A group will be 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. For more information, refer to managing services and data center groups.

There can be four combinations of Active/Backup groups that can be used in Policies. You may select just one CloudGenix group or one non-CloudGenix group as an active or backup path in policies. For example:

<table>
<thead>
<tr>
<th>Active Group</th>
<th>Backup Group</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party</td>
<td>CloudGenix</td>
<td>Internet-bound SSL traffic from a branch site will transit through the Cloud Security Service. In the event all 3rd party VPN paths to any of the endpoints in the Primary Cloud Security Service group are not available, internet-bound SSL traffic will transit through one of the CloudGenix data center endpoints assigned to that group via the CloudGenix VPN.</td>
</tr>
<tr>
<td>CloudGenix</td>
<td>Third-Party</td>
<td>Internet-bound SSL traffic from a branch site will transit through one of the CloudGenix data center endpoints assigned to that group via the CloudGenix VPNs. In the event all CloudGenix VPNs to all of the Data Center endpoints in that group are unavailable, internet-bound SSL traffic will transit through the Cloud Security Service via one of the 3rd party VPN paths to any of the endpoints in the Third-party group.</td>
</tr>
<tr>
<td>Third-Party</td>
<td>Third-Party</td>
<td>Internet-bound SSL traffic from a branch site will transit through the primary cloud security service via one of the 3rd party VPN paths to any of the endpoints in the primary cloud security service group. In the event all 3rd party VPNs are down to all endpoints in the primary group, the Internet bound SSL traffic will transit through the backup cloud security service via one of the 3rd party VPN paths to the endpoints that are part of the backup group.</td>
</tr>
<tr>
<td>CloudGenix</td>
<td>CloudGenix</td>
<td>Internet-bound SSL traffic from a branch site will transit through one of the CloudGenix data center endpoints assigned to the active group via the CloudGenix VPNs. In the event all CloudGenix VPNs to all of those endpoints are down, internet-bound SSL traffic will transit through one of the CloudGenix data center endpoints assigned to the backup group via the CloudGenix VPNs.</td>
</tr>
</tbody>
</table>
To use a group in a policy – **Stacked Policies:**

1. **From Stacked Policies**, select a path policy set.

2. **Within the policy set select a rule to edit or add a new rule.**

3. **Select the apps of interest or confirm the apps of interest are selected.**
4. On the Paths tab select the Active and/or Backup path as 3rd party VPN on <circuit category> or Any Public / Private to allow the system to use any/all paths of that type.

![Path Policy Set: CloudGenix East Coast Policy Set](image)

**Note:** You can mix 3rd party VPNs with other available paths – private, public, direct or VPNs.

5. On the Service & DC Group tab select the 3rd party group Zscaler and click Save.

![Path Policy Set: CloudGenix East Coast Policy Set](image)

**Note:**
- If 3rd party VPN is used in a network policy, then you must have a 3rd party Services and DC Group defined in the policy for the traffic to transit through that group. If not, traffic will be black-holed.
- If Required is selected, traffic will always transit through the Services and DC Group. If not selected, traffic may or may not transit through the Services and DC Group per policy.
To use a group in policy – Policies(Original):

1. From Policies(Original), select an application and click the 🆕 icon next to it. Alternatively, you may select Edit Group to edit priority and path for all applications within that group.

![Policy Configuration](image)

2. On the Paths tab, select 3rd Party VPN as either Active or Backup path.

   **Note:** You can mix 3rd party VPNs with other available paths – private, public, direct or VPNs.

![Policy Path Configuration](image)

3. Click Next to navigate to the Services and DC Group tab. Choose a group from either the Active or Backup drop-down lists.
Note:

- If 3rd party VPN is used in a network policy, then you must have a 3rd party Services and DC Group defined in the policy for the traffic to transit through that group. If not, traffic will be black-holed.
- If Required is selected, traffic will always transit through the Services and DC Group. If not selected, traffic may or may not transit through the Services and DC Group per policy.

4. Click Save to save the policy rule.
Managing and Troubleshooting the Zscaler Integration CloudBlade

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

Enabling, Pausing, Disabling and Uninstalling the Integration.

After the Integration has been set up, operations can be done in the CloudBlade panel. These operations have various effects on the Tunnels and configurations in CloudGenix and Zscaler.

- **Set the CloudBlade to Enabled**
  This is the standard, expected mode of operation for the CloudBlade. The CloudBlade will run every 60 seconds find any new Sites/Circuits with the appropriate tags, and configure the integration on Zscaler and CloudGenix. In addition, during this integration run if any settings were previously modified manually on either CloudGenix or Zscaler (e.g. VPN credentials changed, or Location deleted in Zscaler) these will be reverted to the known good state automatically.

- **Set the CloudBlade to Paused**
  Pausing the 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 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 policy is not set to use other paths. Note that IPSEC policies, IKE policies, and CloudGenix Endpoints and Service and DC groups are not automatically deleted and must be removed manually.

- **Uninstalling the CloudBlade**
  Uninstalling the CloudBlade removes the configuration for the CloudBlade, and immediately stops any changes by the CloudBlade. Uninstalling the CloudBlade does not automatically remove configuration from all sites and objects. The CloudBlade may be Uninstalled and Reinstalled to facilitate upgrades or downgrades to different versions without traffic interruption. To completely remove all items, please 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

If an administrator incorrectly enters the API key or partner Admin credentials the system may end up in a state where the CloudGenix objects are created, but the Zscaler location and VPN keys are not. The end result is there will be alarms that the VPNs are down on the sites for which they were configured. If this occurs check the **Messages** output for Configuration Failures under the CloudBlade.
Improper Settings for CloudGenix User Doing Initial Installation

When the CloudBlade configuration is submitted, a custom role is created within CloudGenix and an API AUTH token is generated and assigned to this custom role. The Zscaler Integration CloudBlade uses this AUTH token when making API calls to CloudGenix. Since this AUTH token is generated by the user account that is doing the configuration, it will inherit the IP session lock property of that user. If the user default and tenant level configuration is enabled (which is the default) or if the tenant level configuration is disabled but the user account is set to enabled, both scenarios will result in the below error when trying to do the initial installation of the CloudBlade.

To resolve this **set IP session lock to disabled** on the user account being used to perform the installation. This can be done under **User Administration > Edit User > IP Session Lock = disabled**.
CloudGenix 3rd Party VPNs Not Created

There could be a scenario in which all user credentials, keys, and tokens are correct, also the Zscaler Location and VPN credential objects are created. However, the CloudGenix VPNs are not created. The likely cause of this failure are the pre-built IPSEC profiles based off of Zscaler’s recommended best practices have not been allocated to your CloudGenix tenant.

To verify these IPSEC profiles exist go to Stacked Policies -> IPSEC Profiles and look for the below. If these 2 profiles are not present please contact CloudGenix support.

The next section will go over troubleshooting once the integration has been installed.
Troubleshooting Third Party VPNs

Start with the Zscaler Test Page to verify and troubleshoot client traffic to and through ZIA Public Service Edge. All application and path metrics will also be collected and reported, and all application monitoring alarms and alerts will be generated for Third Party VPNs. To troubleshoot Third Party VPNs, view Alerts and Alarms, Connectivity of Third Party 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 Third Party 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 ZIA Public Service Edge. To access the page from any client, open the link http://ip.zscaler.com.

For more details on this tool, refer to the Zscaler Knowledgebase article, “How can I check if a user’s traffic is going to Zscaler?”
View Third Party VPN on the Dashboard

In addition to direct and VPN internet and private WAN paths, the CloudGenix Dashboard will now display traffic on the 3rd Party VPN link.
View Third Party VPN at Site Level

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

Select MAP, select a site, and under Connectivity, click 3rd Party to view the status of the 3rd Party VPN.
View Alerts and Alarms

If a Third Party tunnel interface is down, an alarm will be raised, just like it would for any other interface within the system.
View Activity Charts

Activity Charts can be filtered based on paths, including Third Party VPNs. Traffic analytics can be viewed through Network Analytics, Media Analytics, and Flow Browser Charts for 3rd Party VPNs.

From **Quick Filters**, under **WANs**, make sure to select **3rd Party VPN**. Or, from **Paths**, select a specific 3rd party VPN to display analytics for that path.
Use the Device Toolkit

The following device toolkit commands will provide Third Party VPN status and statistics.

**dump servicelink summary**

```
Branch ION 3000# dump servicelink summary
------------------- SERVICE LINKS -------------------
Total      : 1
TotalUP    : 1
TotalDown  : 0
-------------------
SlDev       SlName                          Status ParentDev LocalIP               Peer                 IpsecProfile
-------------
sl8         sl-z scaler-15132962570970071   up     eth2   70.35.55.124         104.129.202.10 ZSCALER_IKEV1
```

**dump servicelink stats**

```
Branch ION 3000# dump servicelink stats slname=sl-z scaler-15132962570970071

No of times IkeRekeyed : 0
No of times ChildRekeyed: 1
No of times HoldDown   : 0
No of times TunnelUp   : 2
No of times TunnelDown : 1
No of Incoming Bytes   : 784132205
No of Outgoing Bytes   : 64453909
No of Incoming Packets : 879522
No of Outgoing Packets : 865410
```

**dump servicelink status**

```
Branch ION 3000# dump servicelink status slname=sl-z scaler-15132962570970071

Servicelink : sl8
IkeSa:
  Version : 1
  State    : Up
  Local IP : 70.35.55.124
  Local ID : 15451095560390112@demo.cloudgenix.com
  Remote IP : 104.129.202.10
  Remote ID : 104.129.202.10
  Encryption Algo : AES_CBC_128
  Integrity Algo  : HMAC_SHA1_96
  Rekey Time     : 2018-12-19 11:35:32.572152899 +0000 UTC (52971s)
  Dhgroup       : MODP_1024

ChildSa:
  SPI In       : 977a8bf8
  SPI Out      : 06d97102
  Encryption Algo : NULL
  Integrity Algo  : HMAC_MD5_96
  Dhgroup       :
  Rekey Time     : 2018-12-19 03:30:22.572259909 +0000 UTC (23861s)
  Life Time      : 2018-12-19 03:54:50.572263595 +0000 UTC (25329s)
  Install Time   : 2018-12-18 19:54:50.572261339 +0000 UTC (3471s)

Peer configured on service endpoint
  Service endpoint name: ZScaler
  Order of connection Try:
    Ipv4Addr: 104.129.202.10 HostName: sjc4-vpn.zscalerthree.net
    Ipv4Addr: 165.225.50.22 HostName: seal-vpn.zscalerthree.net
    Ipv4Addr: 165.225.34.44 HostName: dfw1-vpn.zscalerthree.net
    Ipv4Addr: 165.225.0.165 HostName: ch1-vpn.zscalerthree.net
    Ipv4Addr: 104.129.206.161 HostName: atl2-vpn.zscalerthree.net
    Ipv4Addr: 165.225.36.30 HostName: yto2-vpn.zscalerthree.net
    Ipv4Addr: 165.225.48.10 HostName: was1-vpn.zscalerthree.net
```
dump servicelink endpoints

Branch ION 3000# dump serviceendpoints all

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>AdminUp</th>
<th>AllowEnterpriseTraffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC us-east-1</td>
<td>cg-transit</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>ZScaler</td>
<td>non-cg-transit</td>
<td>true</td>
<td>false</td>
</tr>
</tbody>
</table>

Branch ION 3000# dump serviceendpoints endpoint=ZScaler

Name           : ZScaler
Type           : non-cg-transit
AdminUp        : true
AllowEnterpriseTraffic : false

LivelinessProbe:
HTTP LivelinessProbe

URL            : http://gateway.zscalerthree.net/vpntest
Interval       : 10
FailureCount   : 3
HttpStatusCodes: 200

ServiceLinkPeer:
Hostnames:
  ams2-vpn.zscalerthree.net
  bru1-vpn.zscalerthree.net
  fra4-vpn.zscalerthree.net
  lon3-vpn.zscalerthree.net
  mil2-vpn.zscalerthree.net
  osl2-vpn.zscalerthree.net
  par2-vpn.zscalerthree.net
  tlv1-vpn.zscalerthree.net
  waw1-vpn.zscalerthree.net
  at12-vpn.zscalerthree.net
  ch11-vpn.zscalerthree.net
  dfw1-vpn.zscalerthree.net
  sjc4-vpn.zscalerthree.net
  sea1-vpn.zscalerthree.net
  yto2-vpn.zscalerthree.net
  was1-vpn.zscalerthree.net
  akl1-vpn.zscalerthree.net
  hkg3-vpn.zscalerthree.net
  bom4-vpn.zscalerthree.net
  sel3-vpn.zscalerthree.net
  shal-vpn.zscalerthree.net
  sin4-vpn.zscalerthree.net
  syd3-vpn.zscalerthree.net
  yto4-vpn.zscalerthree.net
  jnb2-vpn.zscalerthree.net

For more information on device toolkit commands, refer to the CloudGenix Device Toolkit Reference Guide.