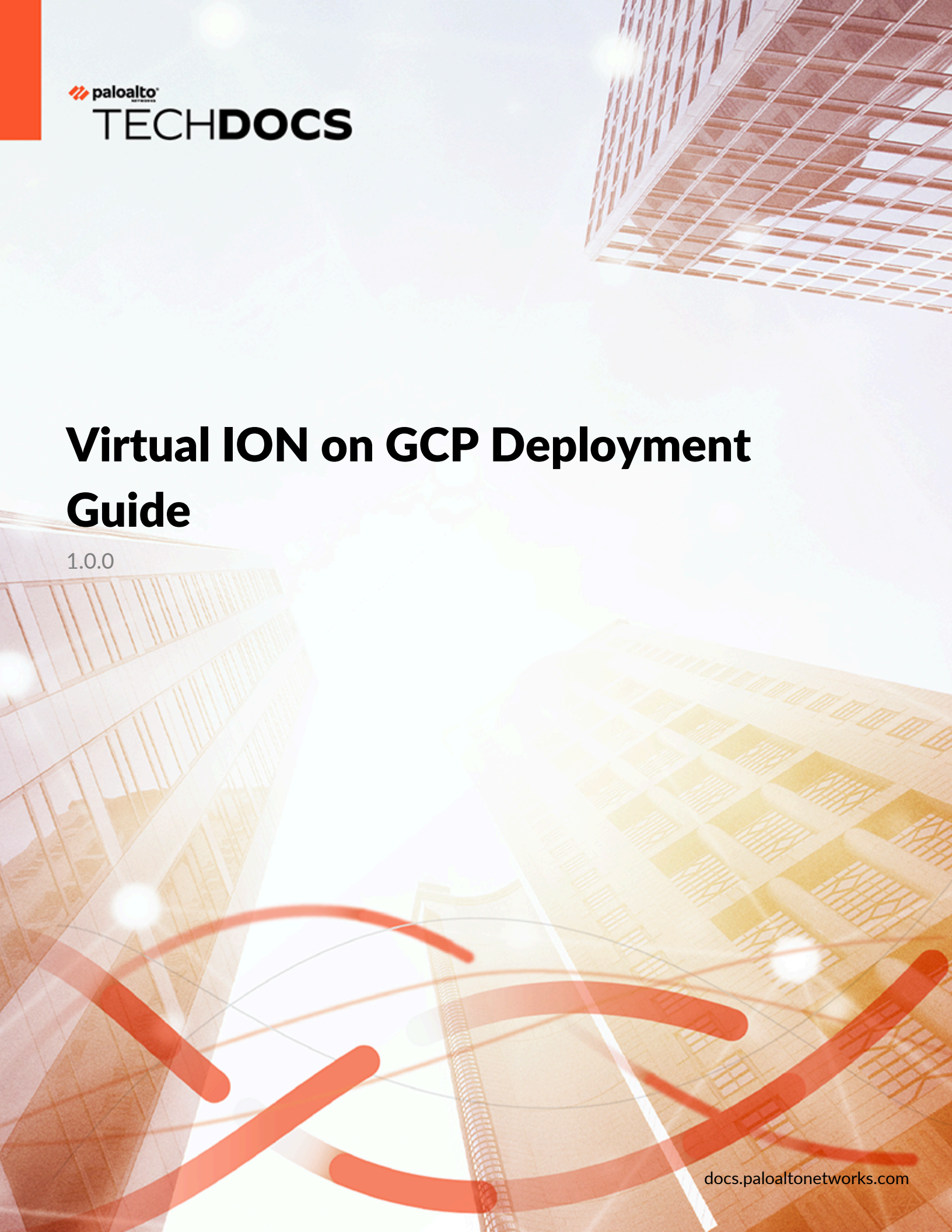
paloalto TECHDOCS

Virtual ION on GCP Deployment Guide

1.0.0



docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 20, 2022

Table of Contents

Plan a Prisma SD-WAN GCP Virtual Deployment

The Prisma SD-WAN virtual ION devices can be deployed to Google GCP. It is intended for network administrators who plan to extend the Prisma SD-WAN fabric between existing OR to be deployed data centers in GCP VPCs, thereby allowing administrators to align their WAN policies with business intent for performance, security, and compliance.

Prerequisites

Prisma SD-WAN

An active Prisma SD-WAN subscription with sufficient licenses to install at least 1 x v7108 ION.

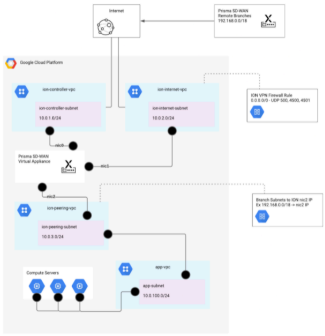
Google GCP

A GCP account with access to the following APIs:

- Compute Engine API
- Cloud Deployment Manager V2 API
- Cloud Runtime Configuration API

Prisma SD-WAN GCP Reference Architecture

The Prisma SD-WAN GCP reference architecture shows an example of branch deployments connecting to applications hosted in different GCP VPCs with the Prisma SD-WAN ION in GCP, acting in a data center deployment model.



With cloud services such as GCP, there may be a single VPC with workloads behind it as previously shown. However, there may be instances where there are multiple workloads and associated VPCs. In order to accomplish this, Google implements VPC Peering.

For more complex deployments where HA (High Availability) Virtual Appliances are needed and/or multi-region support with deployment automation, see the ***GCP-NCC CloudBlade Integration Guide*** *on the* Prisma SD-WAN Documentation.

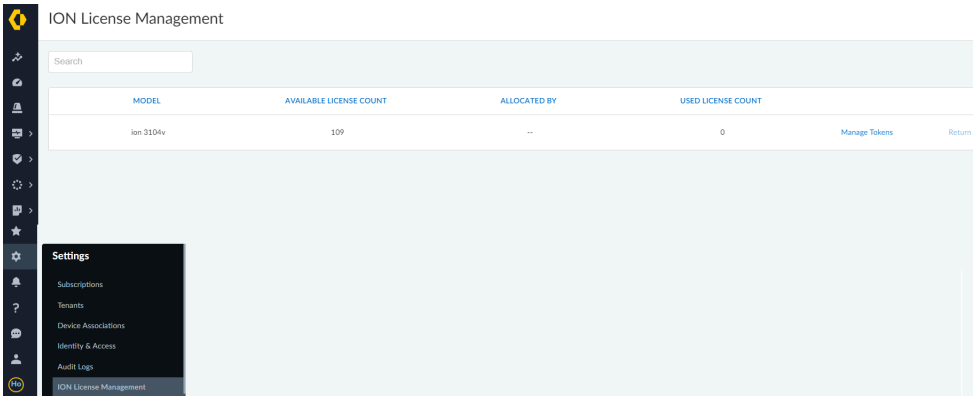
Virtual ION Licensing and Token Management

For virtual form factors in Prisma SD-WAN, the instance(s) are bound to an authorization token. This provides a set of controls to prevent unauthorized virtual devices to be added to an environment.

In order to deploy a Virtual ION using the Prisma SD-WAN deployment template in GCP, you must first log in to the Prisma SD-WAN portal and generate a token for the appropriate model.

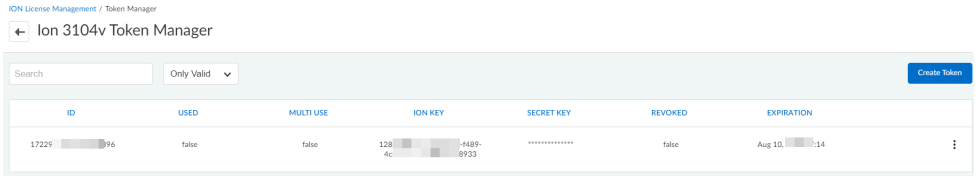
*Only a **Super User** role can generate the authorization tokens.*

STEP 1 | Log in to the Prisma SD-WAN portal and select **Settings** > **ION License Management** > **Manage Tokens**.

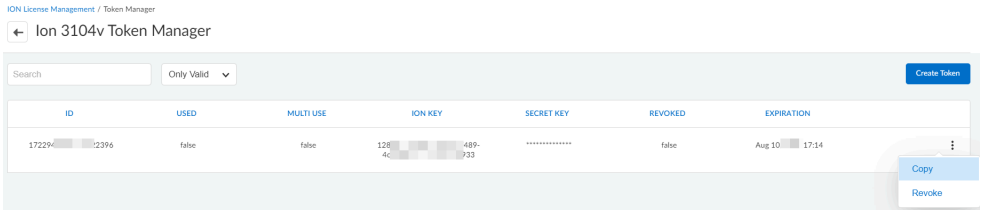


STEP 2 | Create **Create Token**.

Single-use or Multi-use tokens can be generated through the Prisma SD-WAN portal. If deploying more than one ION device of the same model type within a 48-hour period, select **Multi Use** token, otherwise select **Single Use** token.



STEP 3 | Copy the **ION Key** and **Secret Key** that will be used during the AWS deployment. These are mapped to the values of ion_key and secret_key in the AWS environment.



Prisma SD-WAN to GCP Deployment

Prisma SD-WAN Virtual ION Deployment on GCP Prerequisites

Before deploying the Virtual IONs you will need to create 3 VPCs and associated subnets in the region you intend to deploy the ION. For example,

Controller VPC

- Controller Subnet: 10.0.1.0/24

Internet VPC

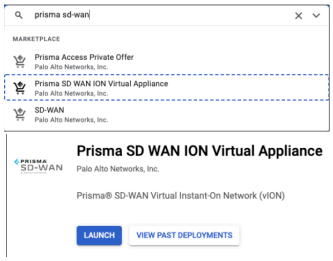
- Internet Subnet: 10.0.2.0/24

Peering VPC

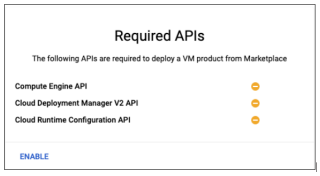
- Peering Subnet: 10.0.3.0/24

Use the Prisma SD-WAN GCP Deployment Template

STEP 1 | Login to the GCP web interface, search and select **Prisma SD WAN ION Virtual Appliance** to launch.

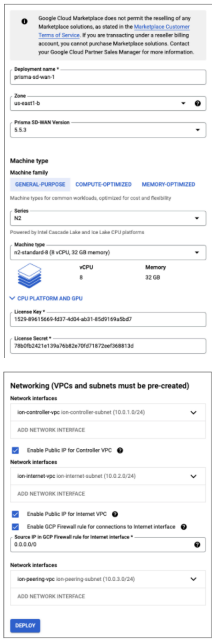


If you do not have the required APIs enabled you can do so here:



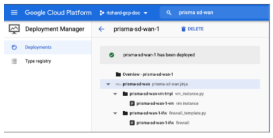
STEP 2 | On the deployment screen, complete the following sections:

1. **Deployment Name** (can use default).
2. Availability **Zone** to deploy ION, should match the region for the subnets you created previously.
3. Current **version** is 5.5.3, ION can be upgraded to latest version once deployed from the Prisma SD-WAN web interface.
4. Use the **License Key** that was generated from the Prisma SD-WAN web interface.
5. Use the **License Secret** that was generated from the Prisma SD-WAN web interface.
6. On the **Controller Interface**, select the **Controller VPC/Subnet** you created previously and ensure **Enable Public IP** is selected.
7. On **Internet Interface**, select the **Internet VPC/Subnet** you created previously and ensure **Enable Public IP** is selected. Add 0.0.0.0/0 to the Source IP GCP Firewall to permit VPN traffic from the Prisma SD-WAN Branches
8. On **Peering Interface**, select the **Peering VPC/Subnet** you created previously.



9. Click **Deploy** to start the deployment of the virtual appliance.

   Once deployment is complete you will see the following screen.



STEP 3 | Finally, reserve the external IP address assigned to your internet port (nic1).

This IP address is used to terminate the SD-WAN VPNs and must be static. Navigate to VPC networks -> External IP addresses, you should see the output below.

STEP 4 | Select the external IP address associated with nic1 and reserve it.

Claim the Prisma SD-WAN ION and Assign to a Site

The ION will show up as **Unclaimed:Online** under the **Map > Unclaimed Devices** section of the Prisma SD-WAN web interface when connected to the Prisma SD-WAN controller.

It can take up to 10 minutes for the ION to show up in the Controller.

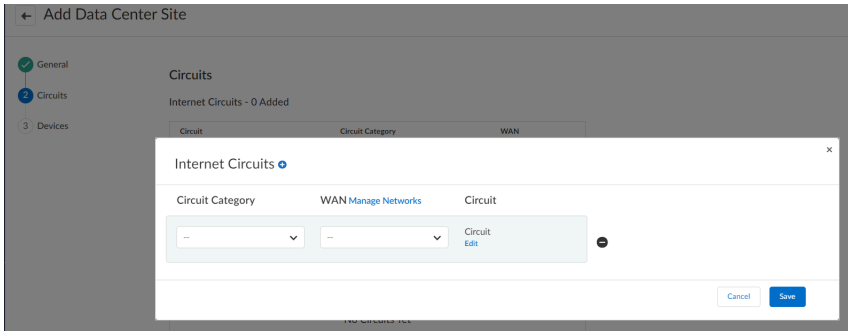
STEP 1 | Claim the device by selecting **Workflows** > **Prisma SD-WAN Setup** > **Devices** > **Unclaimed Devices** > **Claim the device**.

It will transition to an offline state while going through the claiming process.

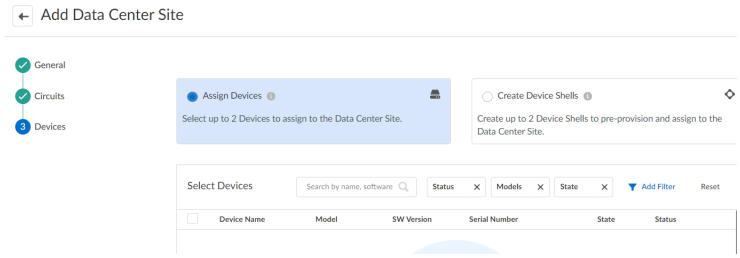
STEP 2 | Create a Data Center Site while the device is being claimed.

Although this workflow depicts how to assign the vION to a data center site, you can also assign the vION to a branch site or a branch gateway site. However, Prisma SD-WAN does not support high availability for vIONs deployed at a branch site or a branch gateway site.

1. Select **Workflows** > **Prisma SD-WAN Setup** > **Data Centers** > **Add Site**.
2. Enter a name for the site and other site details and click **Next**.
3. Add an Internet Circuit in the **Circuits** section and click **Next**.

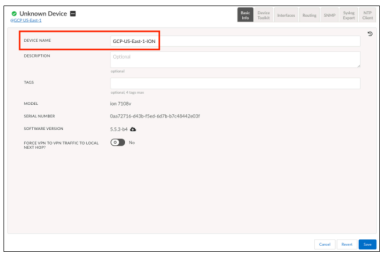


4. Assign the device to the data center by selecting **Assign Devices** and selecting the ION device from the list of **Select Devices** and **Save**.



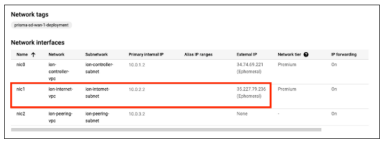
STEP 3 | Once the device is successfully assigned, click on the device name (ion 7108v) to enter the device configuration screen.

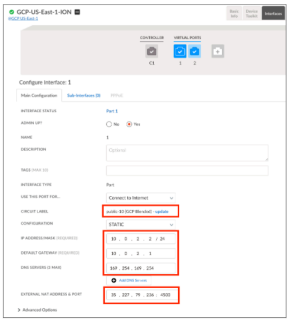
Provide a **Device Name**.



STEP 4 | Configure **Port 1**.

Assign the Internet WAN **Circuit Label** you created in step 2, the IP address assigned to the interface (nic1) in the Internet VPC and providing the external NAT address and port. To determine the interface and external (ephemeral) IP addresses navigate to the GCP portal and find the Public IP address provisioned for the internet interface **Compute > VM > Select VM**.

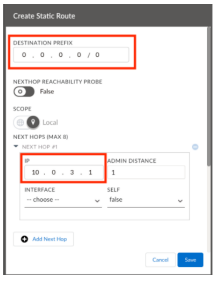




STEP 5 | Configure **port 2**.

Select **Admin Up** as **Yes**, **Use this port** to **Peer with a Network**, and set for **DHCP**.

STEP 6 | Configure a static default route pointing to the gateway of port 2 (the 1st IP address of the private subnet specified in the peering subnet).



STEP 7 | Switch the site to **Control** mode and verify the VPNs are up and active.

Proceed to the next section to finalize the GCP deployment steps.

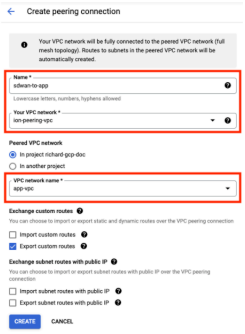
Configure GCP

STEP 1 | Login to the GCP portal and navigate to **VPC Network**. First, peer the Prisma SD-WAN peering VPC to an App VPC.

STEP 2 | Enter the **VPC Network Peerings** configuration section to set up VPC peering between the Prisma SD-WAN VPC and each of your application VPCs.

STEP 3 | Create a VPC Connection from the Prisma SD-WAN VPC to the Application VPC.

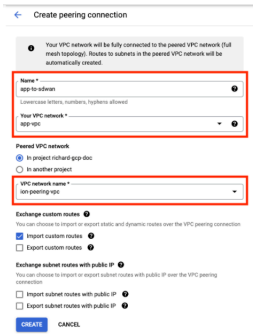
Specify the SD-WAN peering VPC and the remote VPC you wish to peer with from the provided list. Ensure that **Export Custom Routes** is selected on this peering.



STEP 4 | A second peering must be done in the opposite direction for the two VPCs to be fully peered.

Ensure that **Import Custom Routes** is selected on this peering.

When both the peerings are complete, the status will show as **Active**.



STEP 5 | In order for return traffic from the application back to the on-premise networks to be sent through the Prisma SD-WAN virtual appliance we need to add a static route in the peering

VPC subnet route table pointing back to the ION device as the next-hop for corporate subnets.

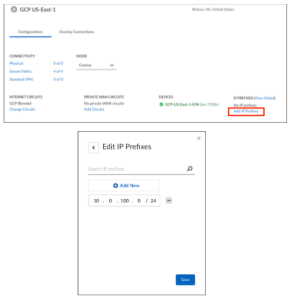
In the example shown, 10.0.3.2 is the IP address of the peering port of the Virtual ION device and 192.168.0.0/18 is the summary prefix of all remote sites that have Prisma SD-WAN ION devices deployed.

The route is imported in your App VPC.

By default VPCs have GCP Firewall enabled and incoming traffic from outside your network is blocked. You must enable inbound firewall rules in SD-WAN and App VPC to permit Branch to Application Traffic.

STEP 6 | From the Prisma SD-WAN web interface, go to **Map** > **GCP Site** to bring up the menu and **Add IP Prefixes**.

Advertise the GCP application VPC prefixes into the Prisma SD-WAN fabric by defining them on the GCP data center site.



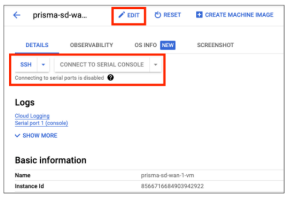
Traffic destined to the prefix (10.0.1000.0/24) is sent directly to GCP over one or more Prisma SD-WAN Internet VPN paths. This assumes that the traffic destined to these applications and prefixes match a path policy rule that allows VPN over a public path.

Use GCP Serial Console to Access Virtual ION Device

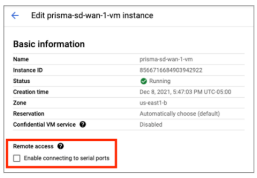
You must connect the console of the Virtual ION device for troubleshooting.

STEP 1 | Navigate to **VM Instances** and select the Virtual ION device.

The serial port is disabled by default.



1. **Edit** the Virtual Machine and select **Enable connecting to serial ports**.



2. Click **Save**.

STEP 2 | Select **Connect to Serial Console**.

For an unclaimed device the default credentials are:

- *Login: elem-admin*
- *Password: hackle628)bags*

For a claimed device use the device toolkit usernames and passwords.

