Prisma SD-WAN Virtual ION on Azure Deployment Guide

Prerequisites

Prisma SD-WAN

- An active Prisma SD-WAN subscription with sufficient licenses to install at least 1 x vION (in this document we use a vION 7108).

Microsoft Azure

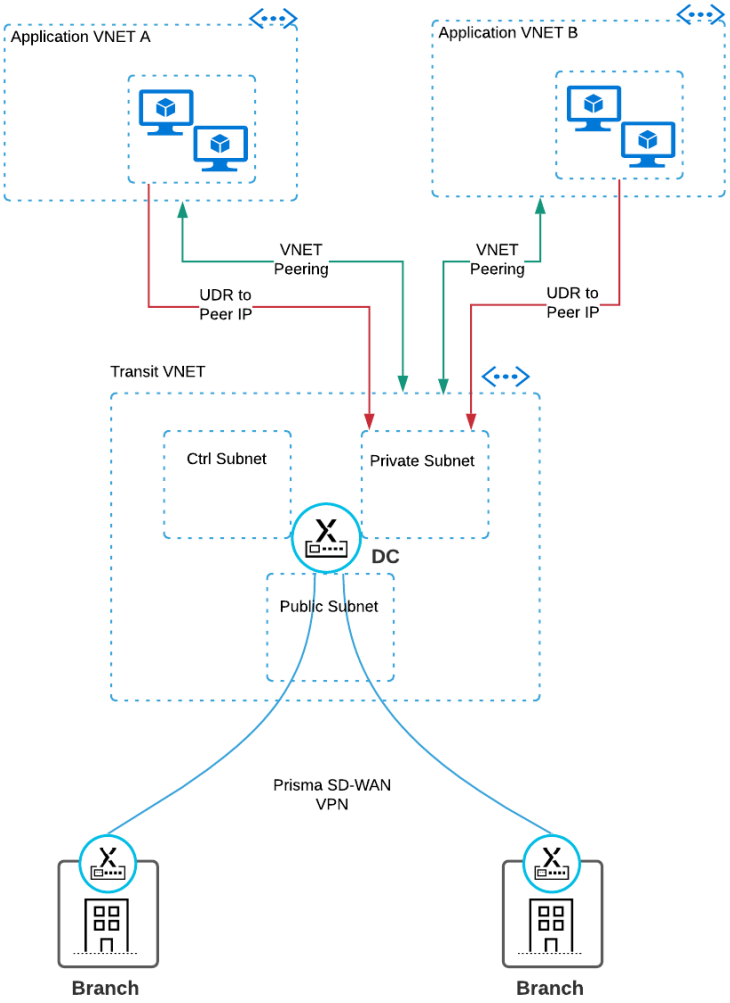
- An Azure account with permissions to create and update Azure Resource Groups, VNET (Virtual Network) and Virtual Machines. This can be accomplished with a custom role with just the required permissions, or using a Contributor role.
- An active Azure marketplace subscription to the Prisma SD-WAN ION Virtual Appliance.
- Create a new Azure Resource Group for this deployment. The deployment template does not support existing resource groups.

Plan a Prisma SD-WAN Azure Virtual Deployment

This guide provides instructions for deploying Prisma SD-WAN ION devices to Microsoft Azure. It is intended for network administrators who plan to extend the Prisma SD-WAN fabric between existing or, to be deployed Datacenters in Azure VNETs hosting applications and the rest of the corporate locations. Thereby allowing administrators to align their WAN policies with business intent for performance, security, and compliance.

Figure 1 shows an example of branch deployments connecting to applications hosted in different Azure VNETs, with a Prisma SD-WAN ION in Azure acting in a Datacenter deployment model.

Figure 1: Prisma SD-WAN Azure Reference Architecture



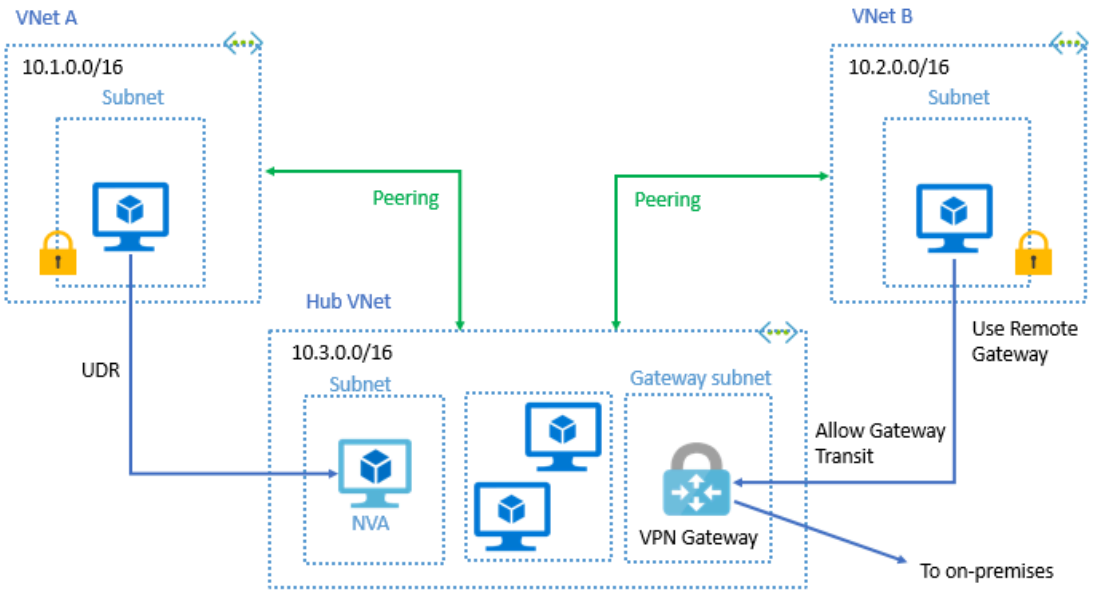
With cloud services such as Azure, there may be a single Resource Group with workloads behind it as previously shown. However, there may be instances where there are multiple workloads and associated resource groups.

In order to accomplish this, Microsoft implements Virtual network peering. With this type of deployment, a Prisma SD-WAN ION may be placed in the logical location where the Azure VPN Gateway is shown in Figure 2, depending on the design of the organization.

Further information on VPN Gateway Peering can be found here:

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

Figure 2: Microsoft Transit Virtual Network Peering



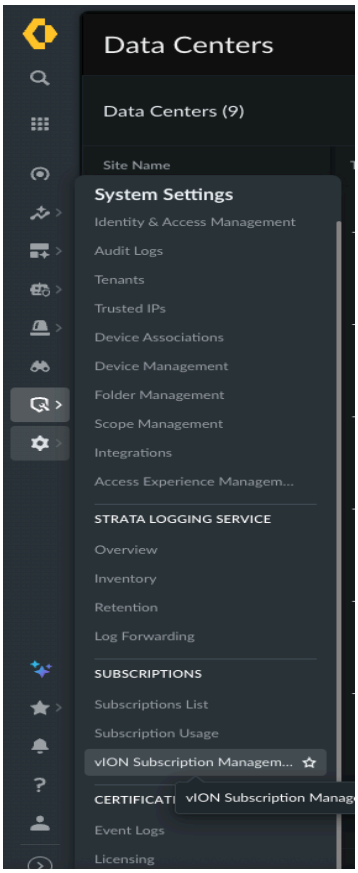
Virtual ION Licensing and Token Management

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

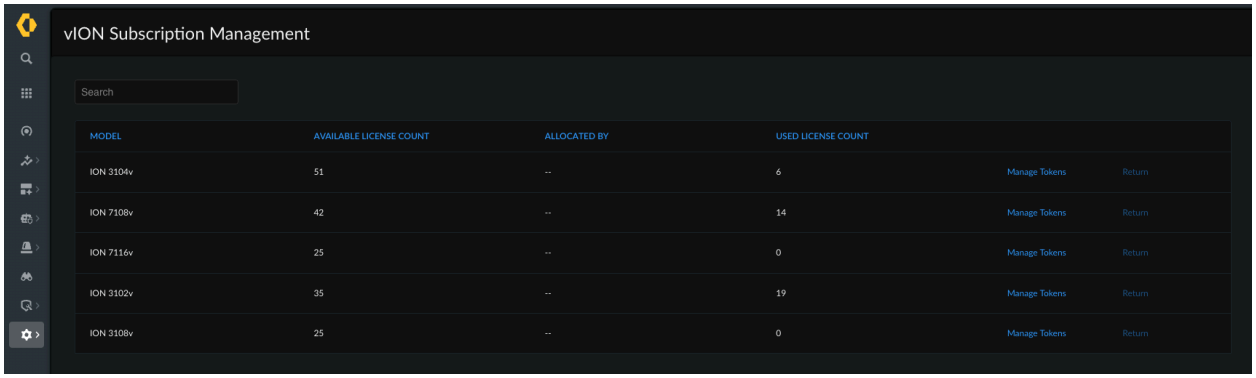
Generate Tokens

In order to deploy a Virtual ION using the Prisma SD-WAN Deployment Template in Azure you must first login to the Strata Cloud Manager (Strata Cloud Manager) for your Prisma SD-WAN implementation and generate a token for the appropriate model.

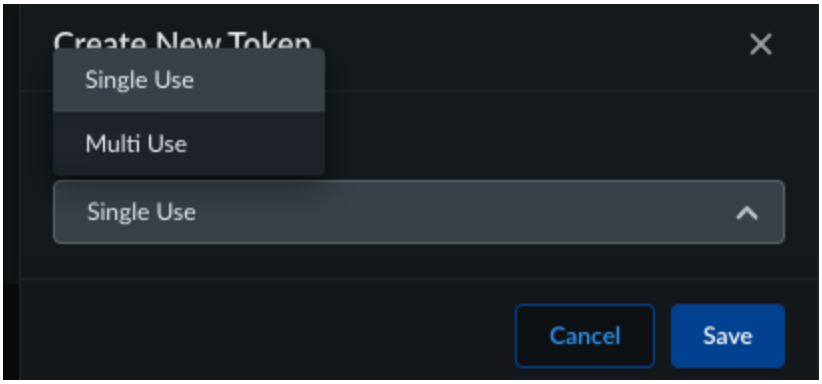
1. Login to the Strata Cloud Manager Portal and navigate to **System Settings -> vION Subscription Management**.



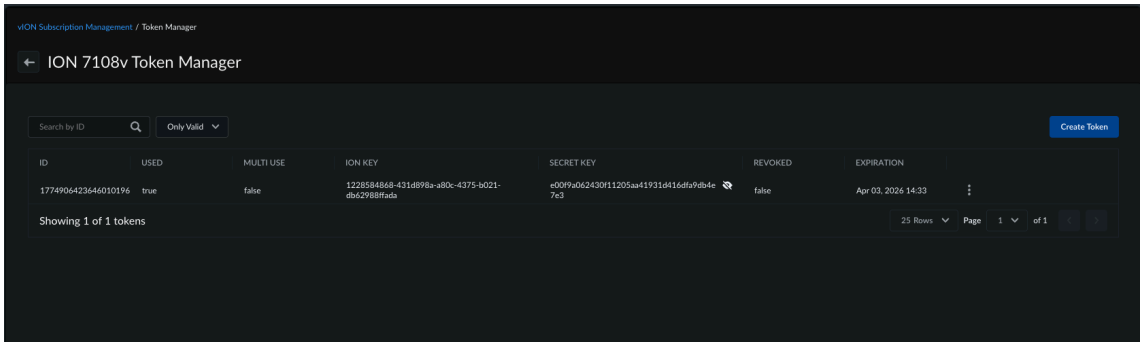
2. To generate a token select **Manage Tokens** next to the ION model that will be deployed.



3. Select **Create Token** to generate a new token. Single-use or Multi-use tokens can be generated through the Strata Cloud Manager Portal. If deploying more than one ION of the same model type within a 48-hour period, select **Multi Use** token, otherwise select **Single Use** token. A single-use token can only activate one device. Using it a second time will result in a token rejection error. If you need to deploy multiple devices of the same model within 48 hours, use a multi-use token.



4. Copy the ION Key and Secret Key. You will enter these values in the Azure deployment template in the next section.



Example from the copy operation (you only copy the values of **ION Key** and **Secret Key** to paste into the deployment template properties):

- **Example Key**: 1092-1cdfe421-466c-41dd-8c47-08a573348cf6
- **Example Secret**: 34ddd1744e2c5cc4d5114089e8d43a6035d7297b

  Note: These are example values only. Do not use these values in your deployment. Replace them with the tokens you generated above.

Deploy Prisma SD-WAN to Azure

Using the Prisma SD-WAN Azure Deployment Template

1. Login to the Azure Portal and navigate to the Marketplace. Search for **Prisma SD-WAN vION Solution Template** and select **Create.**

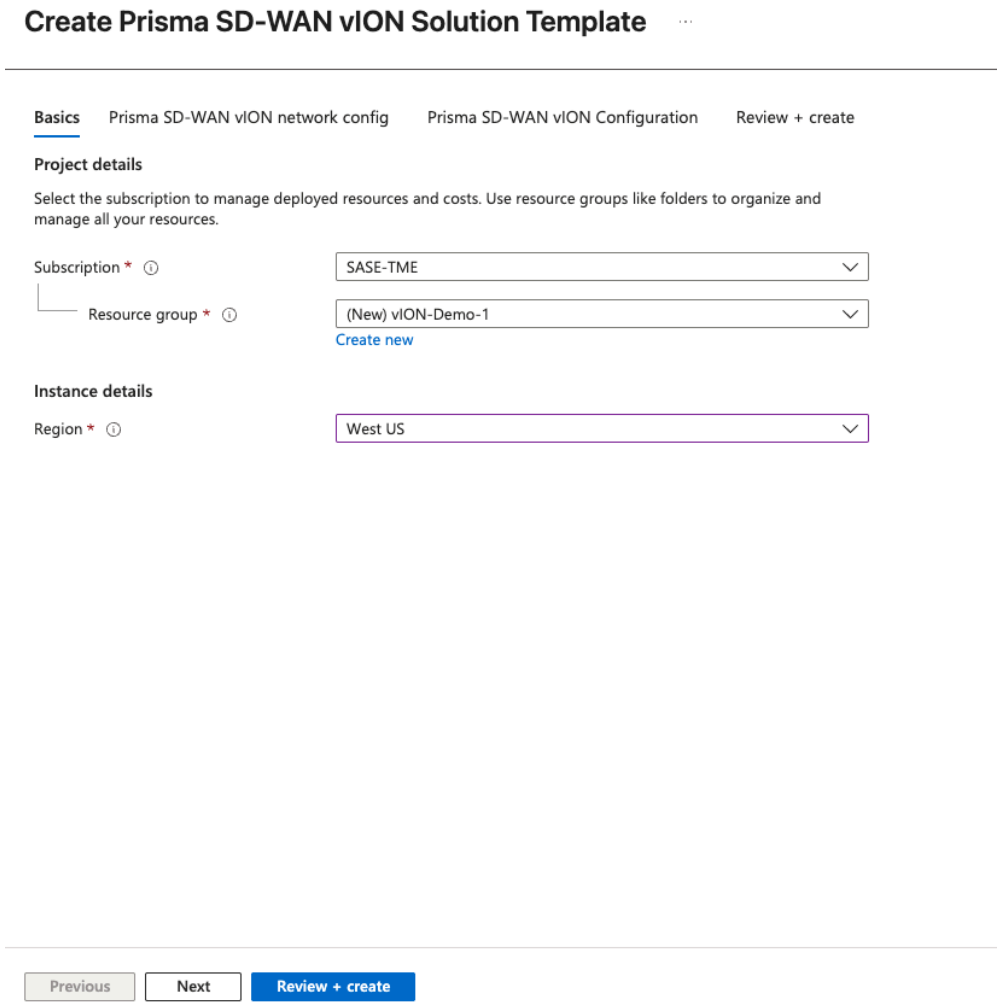
2. On the next screen click **Create.**

3. In the Basic tab you will have the following options:

- Subscription
  - Select the appropriate Azure subscription you wish to use to deploy the Virtual Appliance.
- Resource Group
  - Create a new resource group to deploy the Virtual ION and associated resources.

    Note: In this release you can only deploy a new resource group, you cannot use an existing resource group

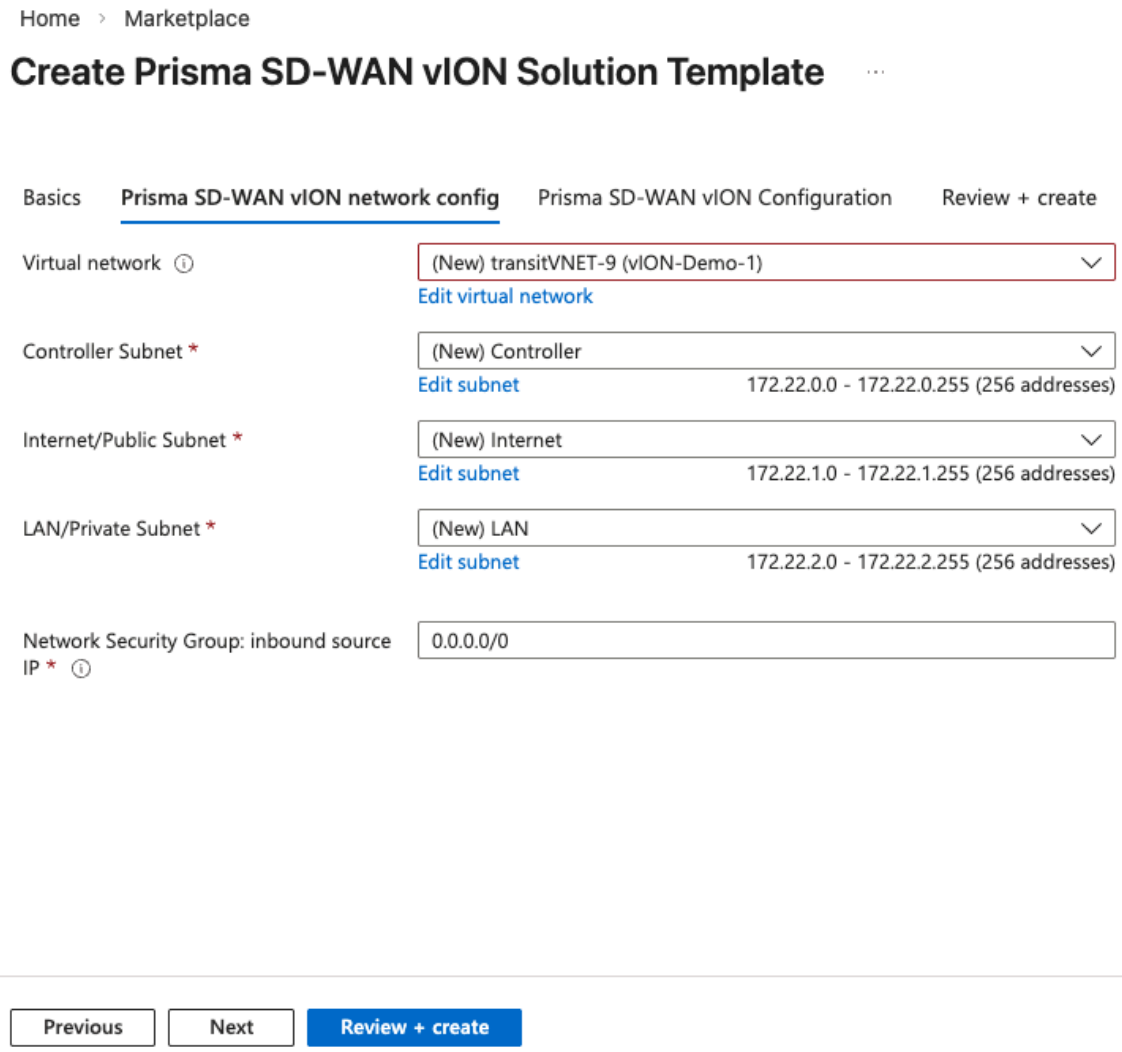
- Region
  - Select the Azure Compute Region where you want to deploy the Virtual Appliance.



4. Select **Next:**

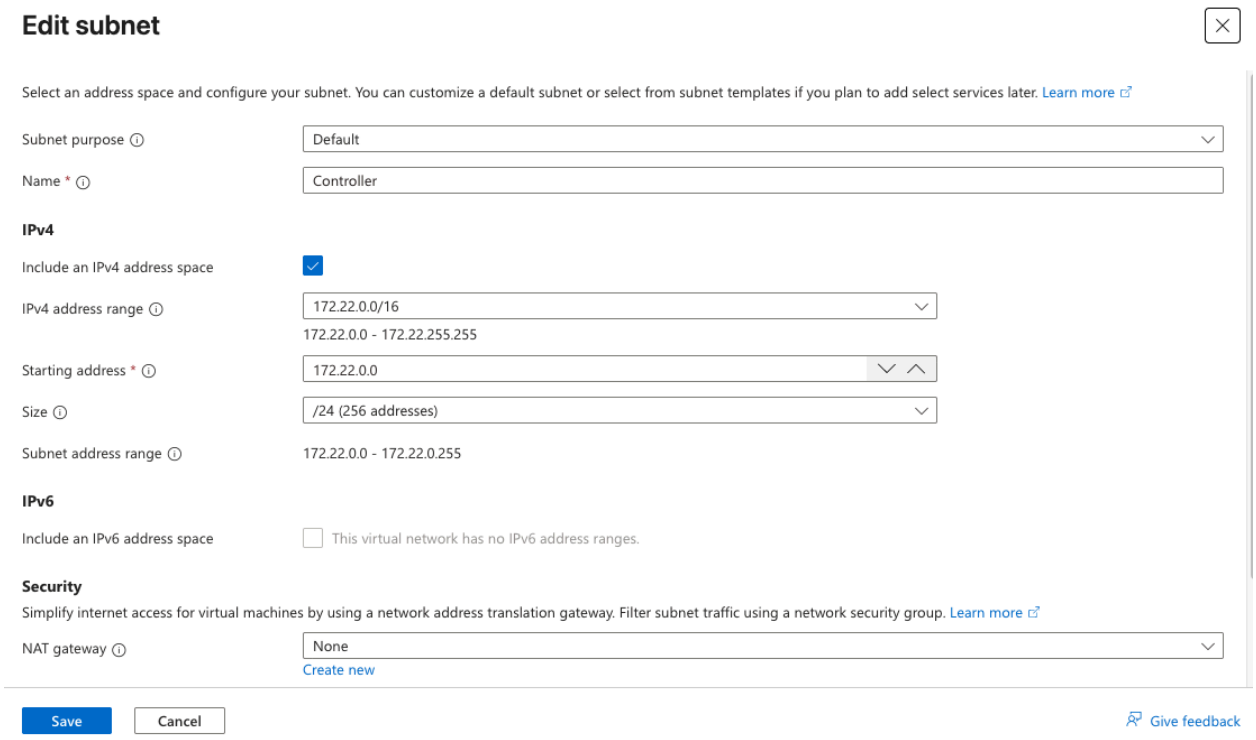
On the Prisma SD-WAN vION network config tab you will have the following options:

- Virtual Network
  - Virtual Network: transitVNET
  - Controller Subnet: 10.x.0.0/24
  - Internet/Public Subnet: 10.x.1.0/24
  - LAN/Private Subnet: 10.x.2.0/24
- Network Security Group: Inbound source IP
  - The NSG by default will allow only UDP 500/4500 inbound. If you wish to modify the sources you can specify here. It's recommended to leave this as the default 0.0.0.0/0 setting.



Note: These are the default values, if you want to customize these settings select **Edit subnet** and complete.

If using a custom VNET ensure that each of the subnets is at least a /29 and falls within the range of the VNET address range you select.

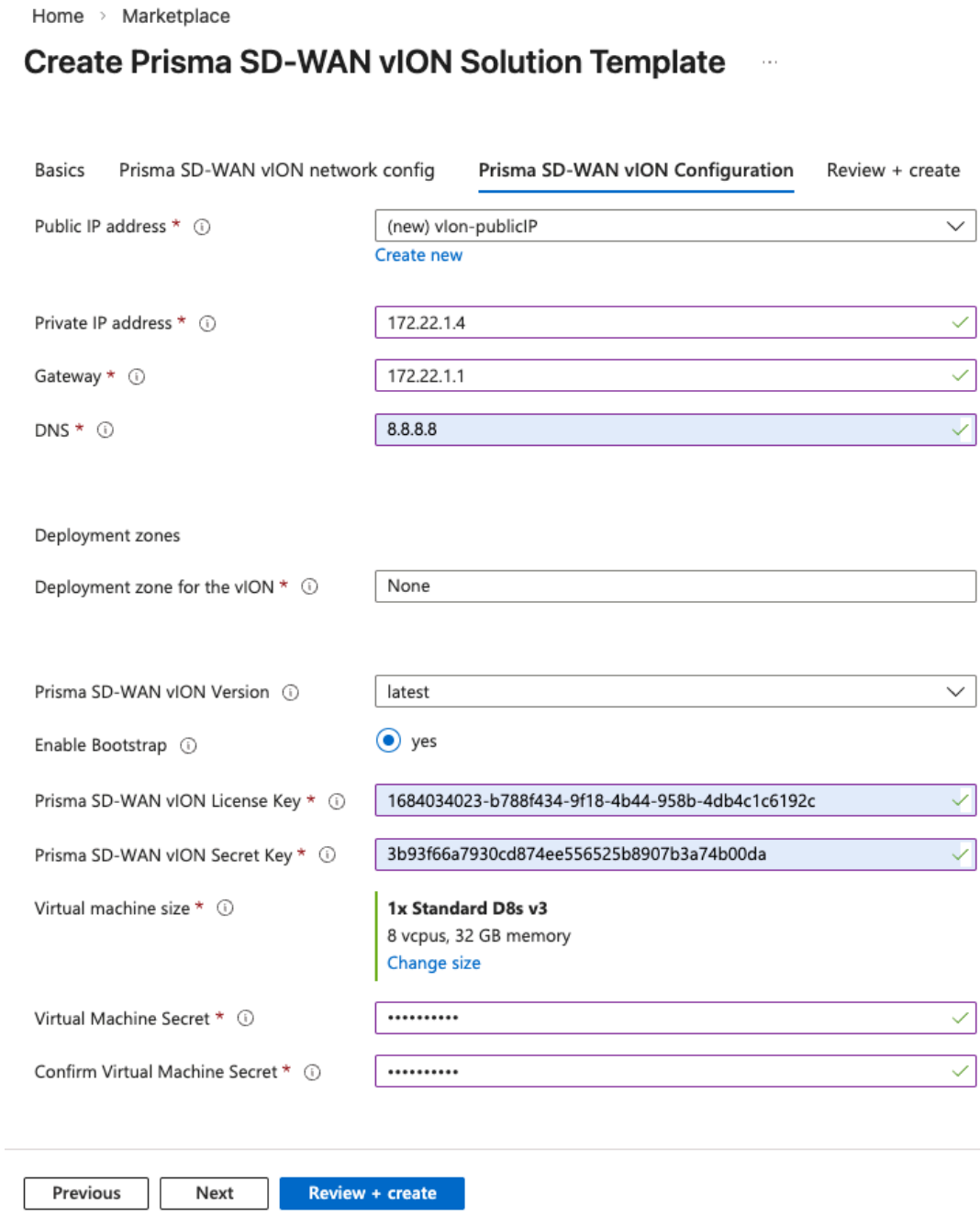


5. Once complete,click on **Next:**

On the Prisma SD-WAN vION Configuration tab complete the following:

- Public IP address
  - Name of the Public IP Address for Port 1 that will be created. You can choose the default or click on **Create new**
- Private IP Address
  - IP address in the **Internet Subnet** that will be assigned to the Virtual IONs Port 1 interface.
  - **Note**: Azure reserves the first 3 IPs in any subnet, choose at least the 4th available IP addresses in the **Internet Subnet** (from the screen before this one).
- Gateway
  - By default Azure assigns the first IP address of a subnet as the default gateway. Use the **Internet Subnet's** first IP address (from the example above 10.x.1.1).
- DNS
  - DNS IP address for Port 1, you can use Azure's own DNS "168.63.129.16" or any public DNS eg 8.8.8.8 or 1.1.1.1.
- Prisma SD-WAN vION Version
  - Software version of the Virtual Appliance to deploy, recommended to use the latest version.
- Prisma SD-WAN vION License Key

    - Use the License Key that was generated from the Strata Cloud Manager Portal.
- Prisma SD-WAN vION Secret Key
    - Use the Secret Key that was generated from the Strata Cloud Manager Portal.
- Virtual Machine Size
    - Leave at the default selection. If the default VM size is unavailable in your region, contact Palo Alto Networks Support for a list of supported alternative VM sizes
- Virtual machine secret. Use vIONVM@12345 or similar of length ≥ 12 characters including at least one Capital letter, number and special character



6. Click on **Review + create** now Azure will validate the configuration against the deployment template.

Home › Marketplace

Create Prisma SD-WAN vION Solution Template ...

Basics

Subscription	SASE-TME
Resource group	vION-Demo-1
Region	West US

Prisma SD-WAN vION network config

Virtual network	transitVNET-9
Controller Subnet	Controller
Address prefix (Controller Subnet)	172.22.0.0/24
Internet/Public Subnet	Internet
Address prefix (Internet/Public Subnet)	172.22.1.0/24
LAN/Private Subnet	LAN
Address prefix (LAN/Private Subnet)	172.22.2.0/24
Network Security Group: inbound sourc...	0.0.0.0/0

Prisma SD-WAN vION Configuration

Public IP address	vIon-publicIP
Domain name label	-
Private IP address	172.22.1.4
Gateway	172.22.1.1
DNS	8.8.8.8
Deployment zone for the vION	None
Prisma SD-WAN vION Version	latest
Enable Bootstrap	yes
Prisma SD-WAN vION License Key	1684034023-b788f434-9f18-4b44-958b-4db4c1c6192c
Prisma SD-WAN vION Secret Key	3b93f66a7930cd874ee556525b8907b3a74b00da
Virtual machine size	Standard_D8s_v3
Virtual Machine Secret	**********

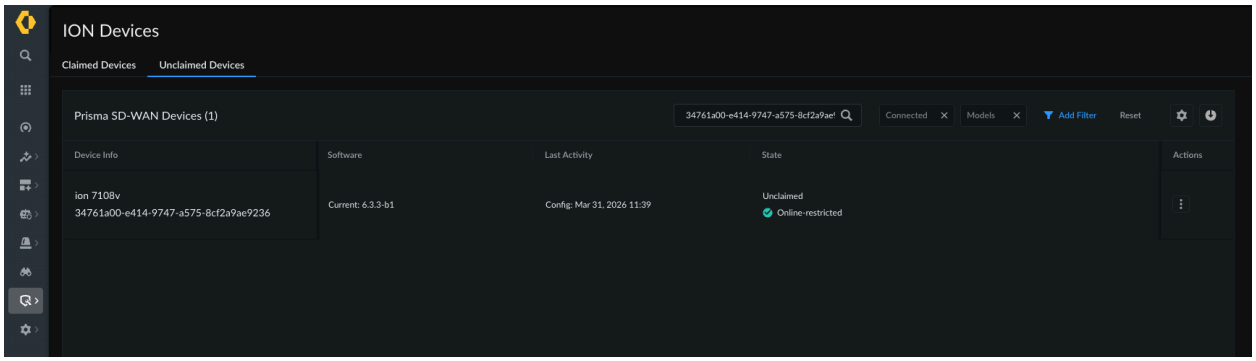
Previous | Next | Create

7. . Once validated, click on **Create** to deploy the virtual appliance.

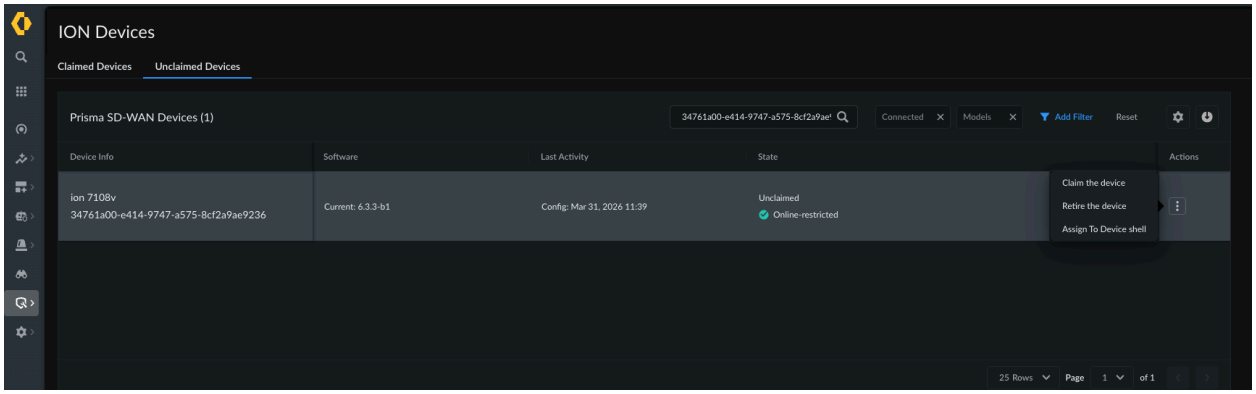
Claim the Prisma SD-WAN ION and Assign to a Datacenter

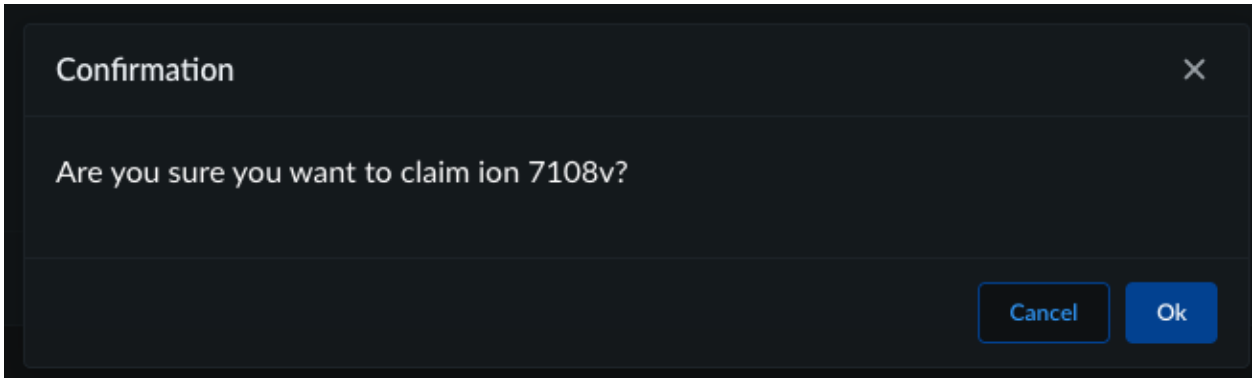
1. After the ION successfully boots (this will take a few minutes), as long as it can connect to the Prisma SD-WAN controller it will show up in Strata Cloud Manager as Unclaimed: Online-restricted under the **Configuration -> Prisma SD-WAN -> ION Devices -> Unclaimed Devices (tab)** section of the portal.

Note: It can take up to 10 minutes for the ION to show up in the Controller If the device does not appear after 10 minutes: (1) verify the vION VM is running in the Azure portal, (2) confirm outbound UDP 500/4500 and TCP 443 are not blocked, (3) use the Azure Serial Console (see Troubleshooting) to check the device status. Contact Palo Alto Networks Support if the device remains offline..

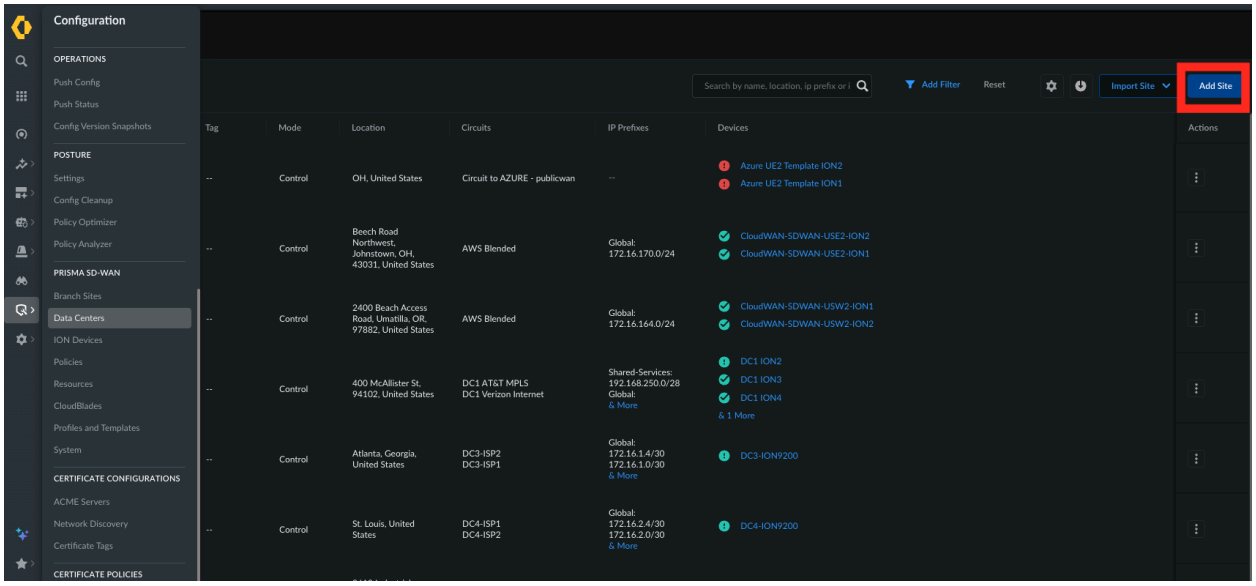


2. Claim the device. It will transition to an offline state while going through the claiming process.

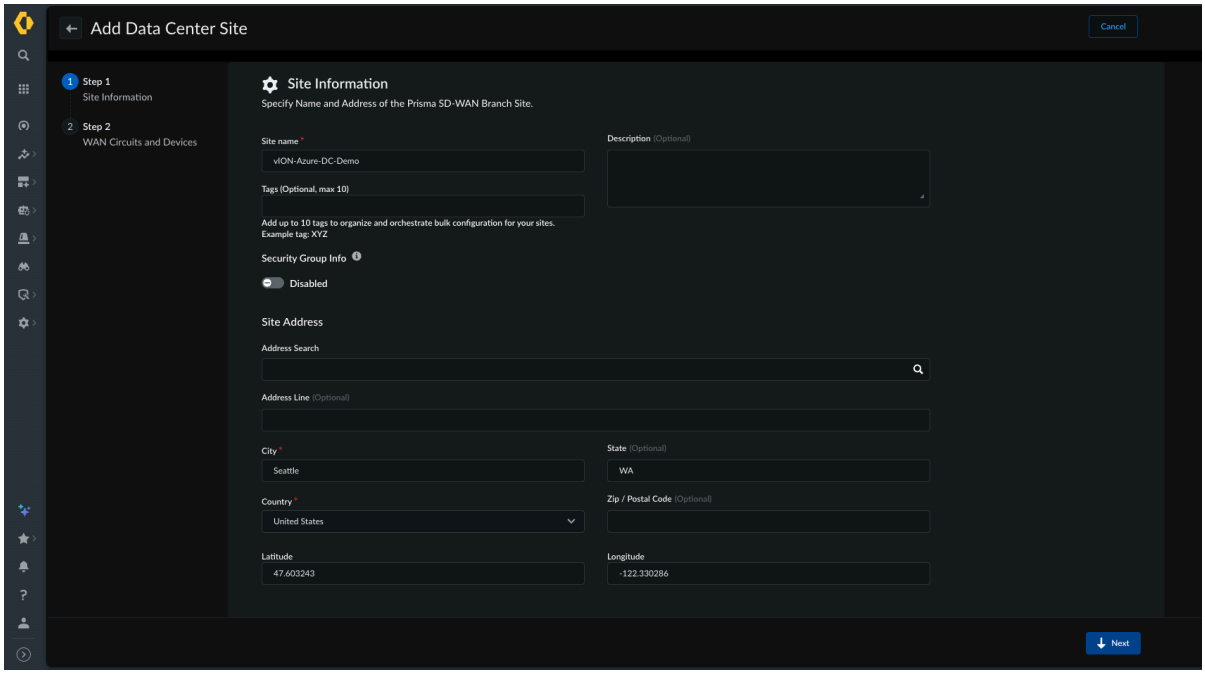




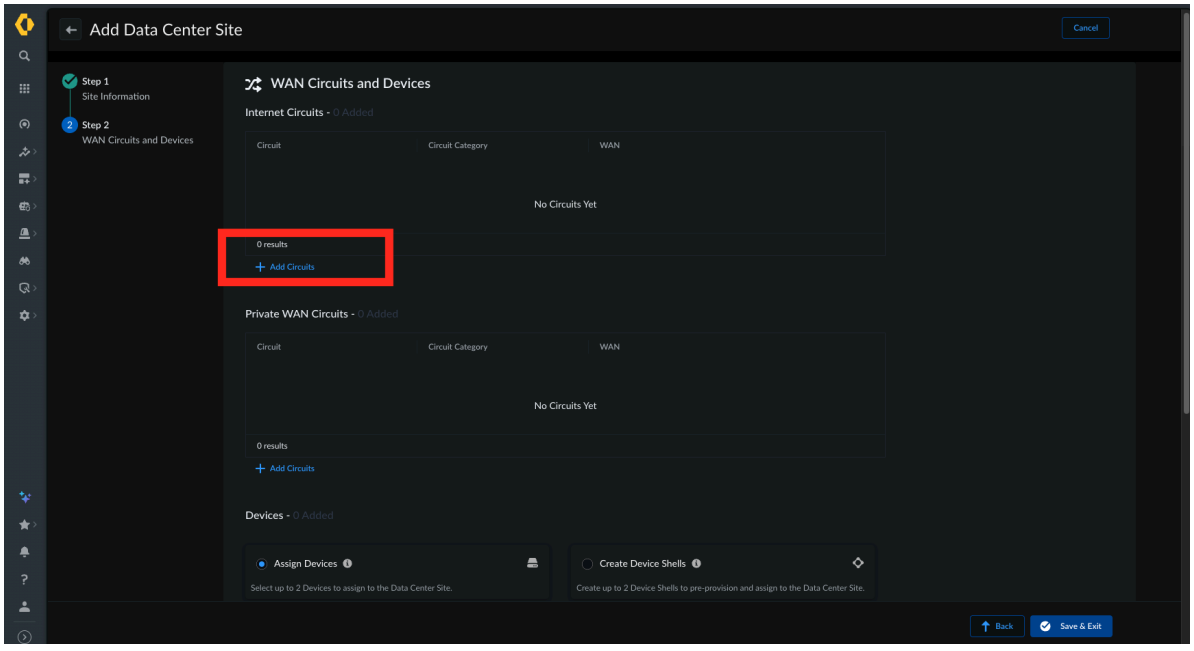
3. While the device is being claimed, create a Data Center Site. On the Strata Cloud Manager go to **Configuration -> Prisma SD-WAN -> Data Centers** and click on **Add Site**.



4. In the Add Data Center Site dialog fill in a **Site Name, Address, City, State, Country**

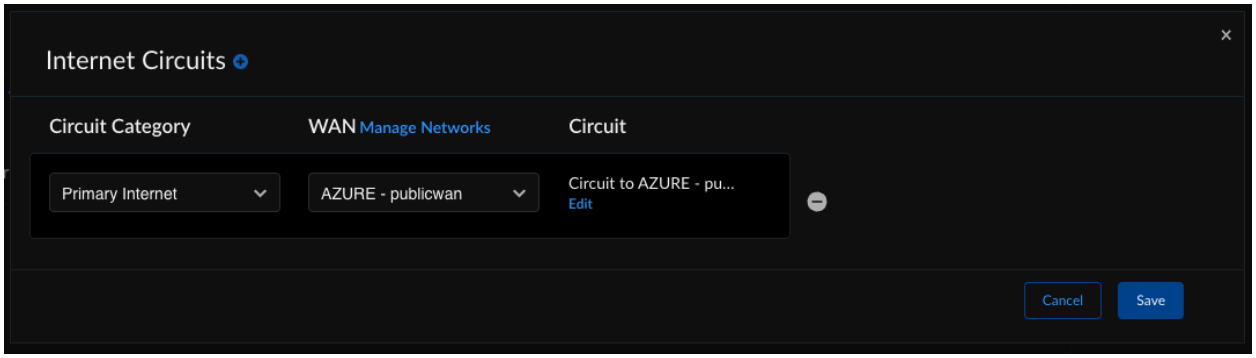


5. Click on **Next**: to get to the WAN Circuits and Devices Dialog. Under Internet Circuits, click on **+ Add Circuits**

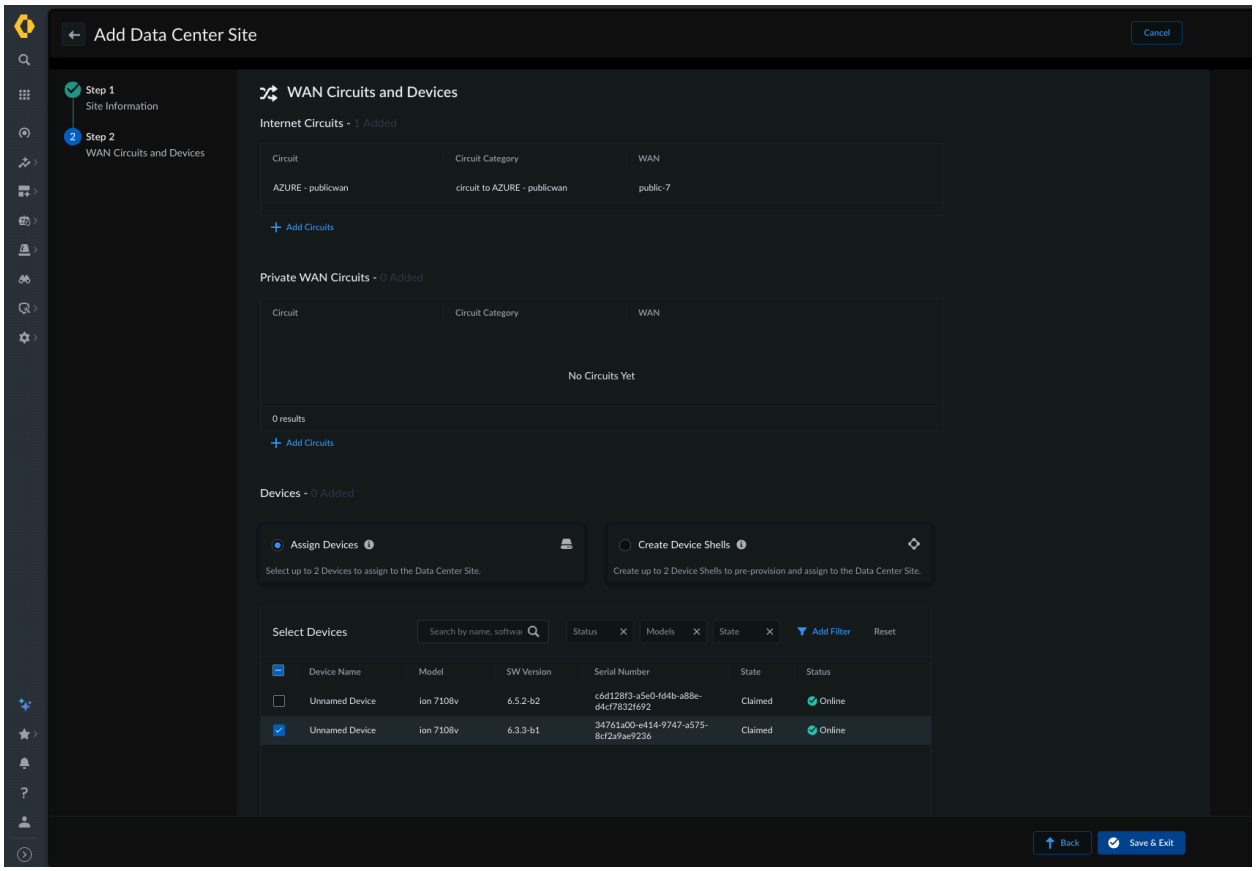


Select Internet as the circuit category. For the provider, choose Azure WAN if it exists in your configuration, or create a new provider label. For guidance on circuit labels, see

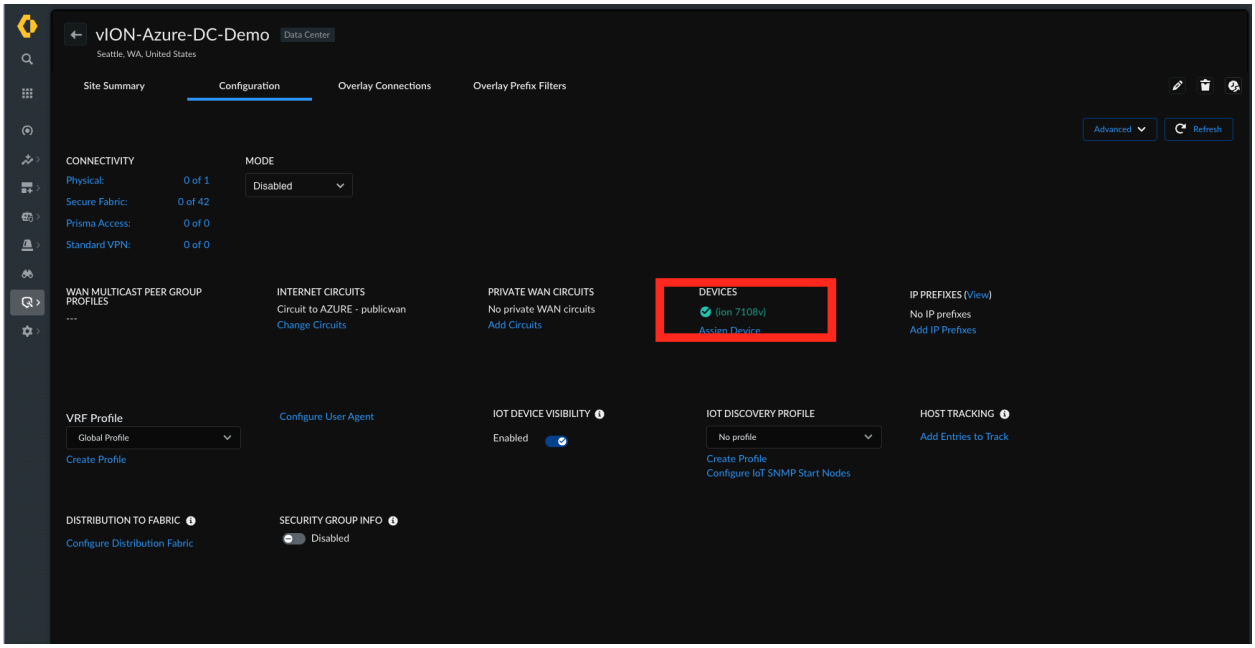
https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-sites/configure-circuit-categories. Click on **Save**.



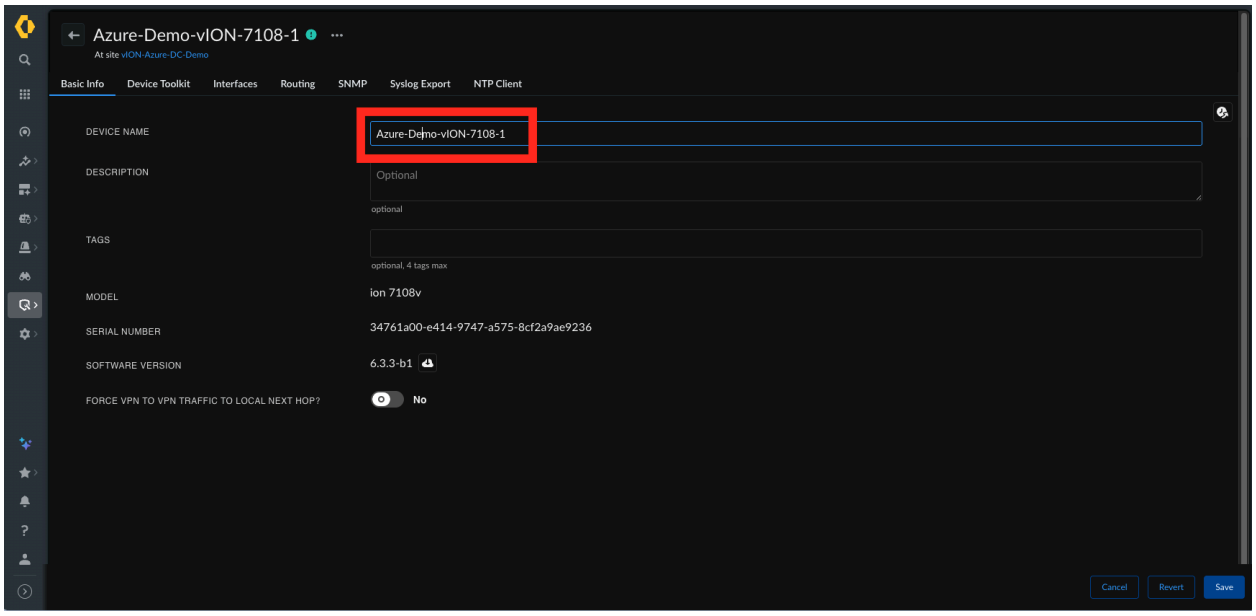
6. Under **Assign Devices** select the ION device you claimed earlier and click **Save & Exit**.



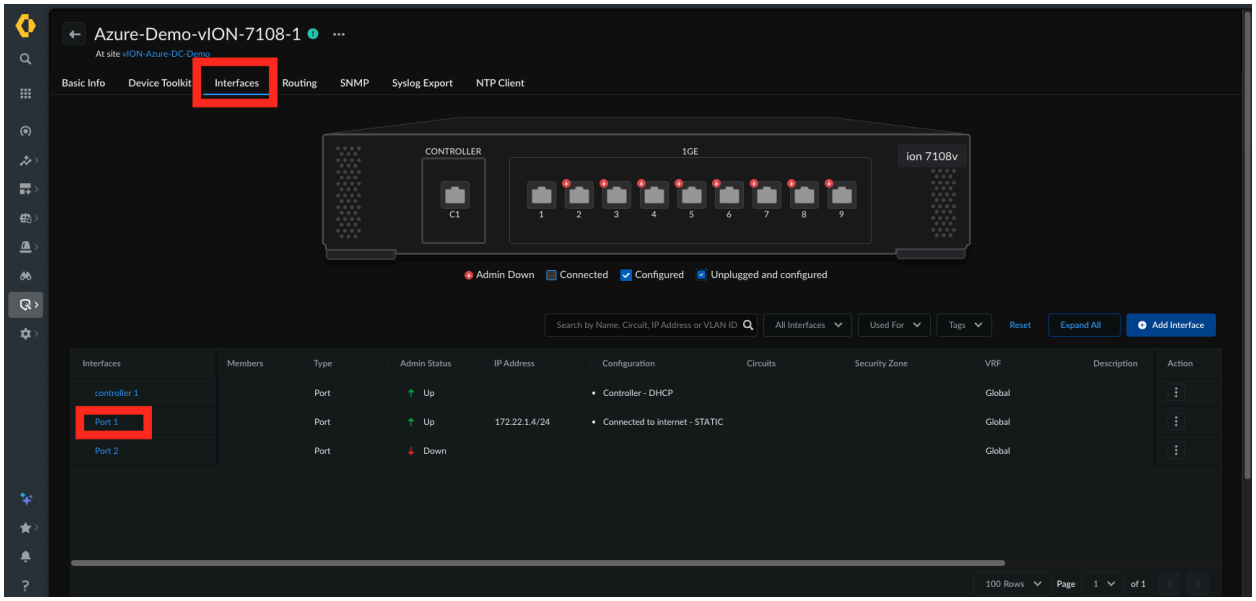
7. Once the device is successfully assigned you will be taken to the Configuration tab for the DC. Click on the assigned device under **Devices**



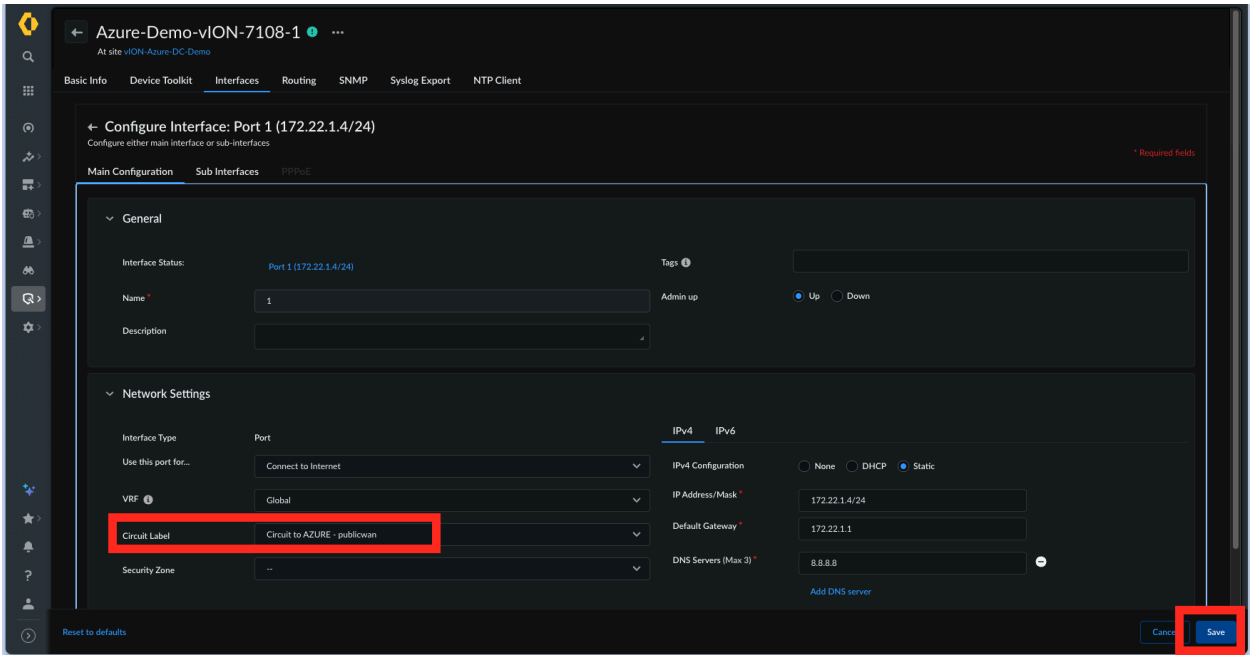
Provide a **Device Name** and click **Save**.



8. Configure Port 1 of the vION by assigning the Internet WAN circuit label you created in Step 5. To do this click on the **Interfaces** tab, and then on **Port 1**:

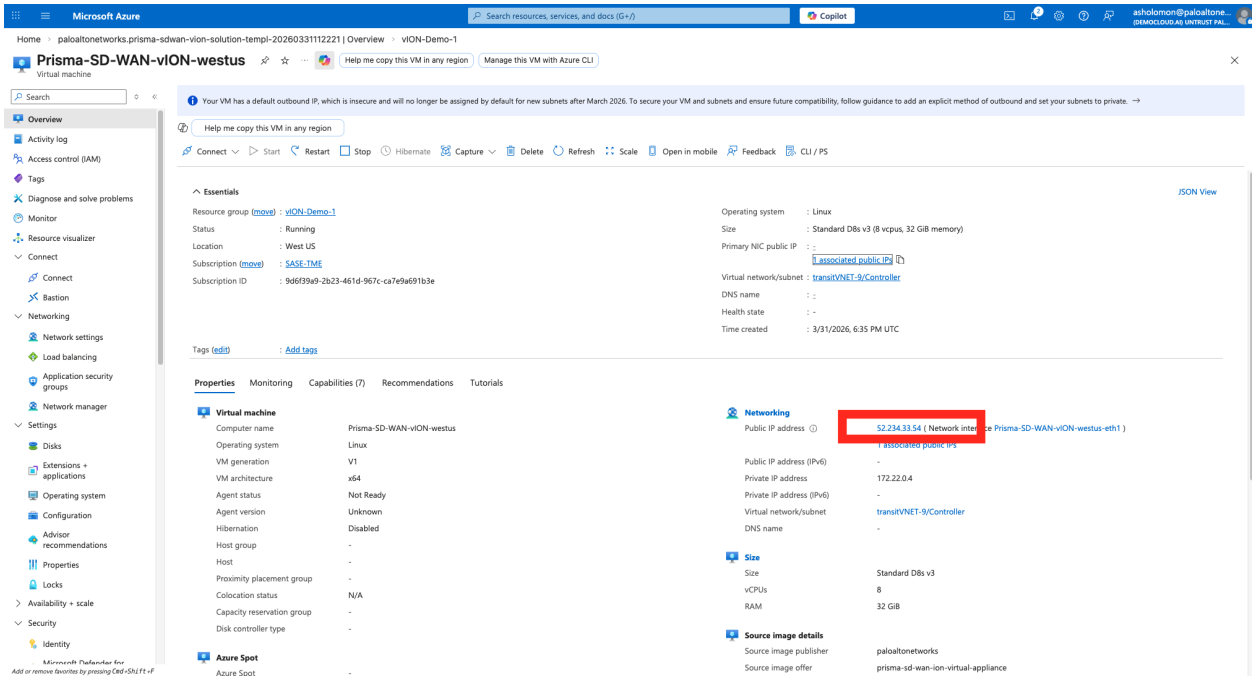


Then under the **Circuit Label** dropdown choose the label created in the earlier step and then click **Save**:

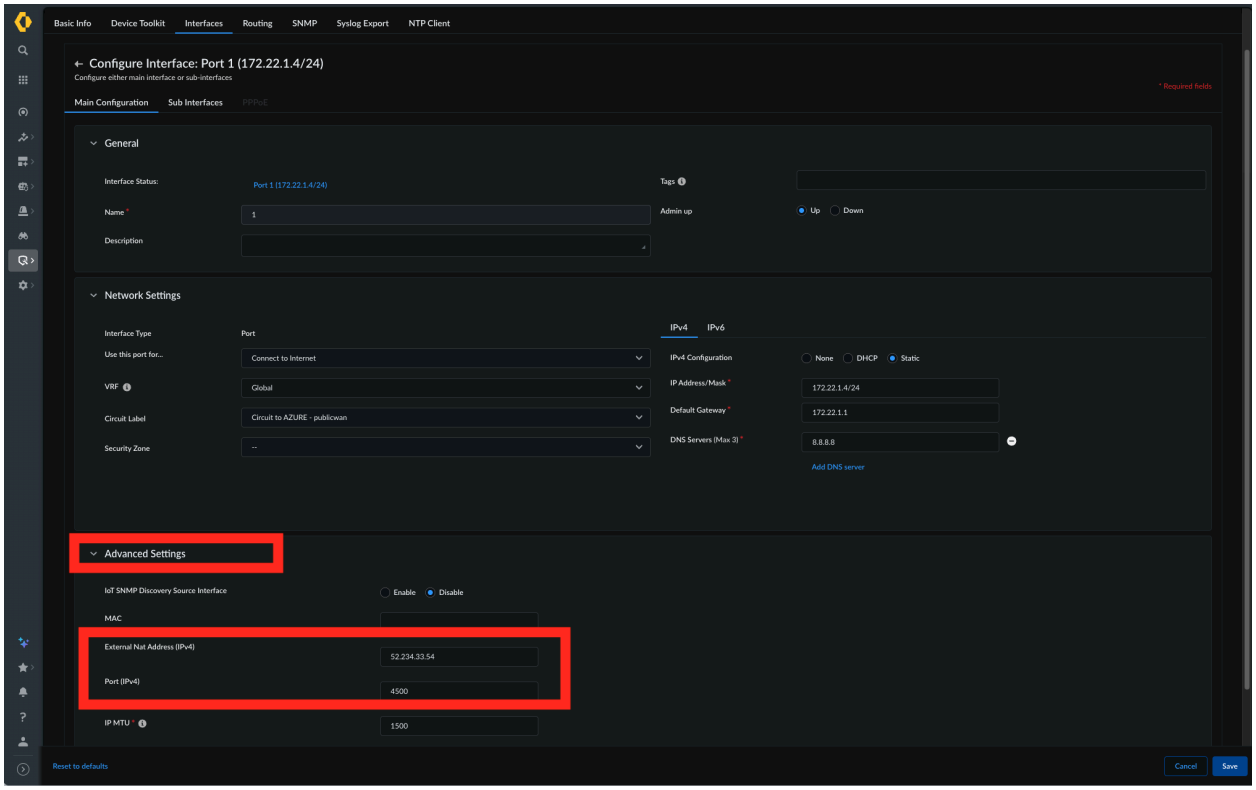


We now can configure the external NAT address and port.

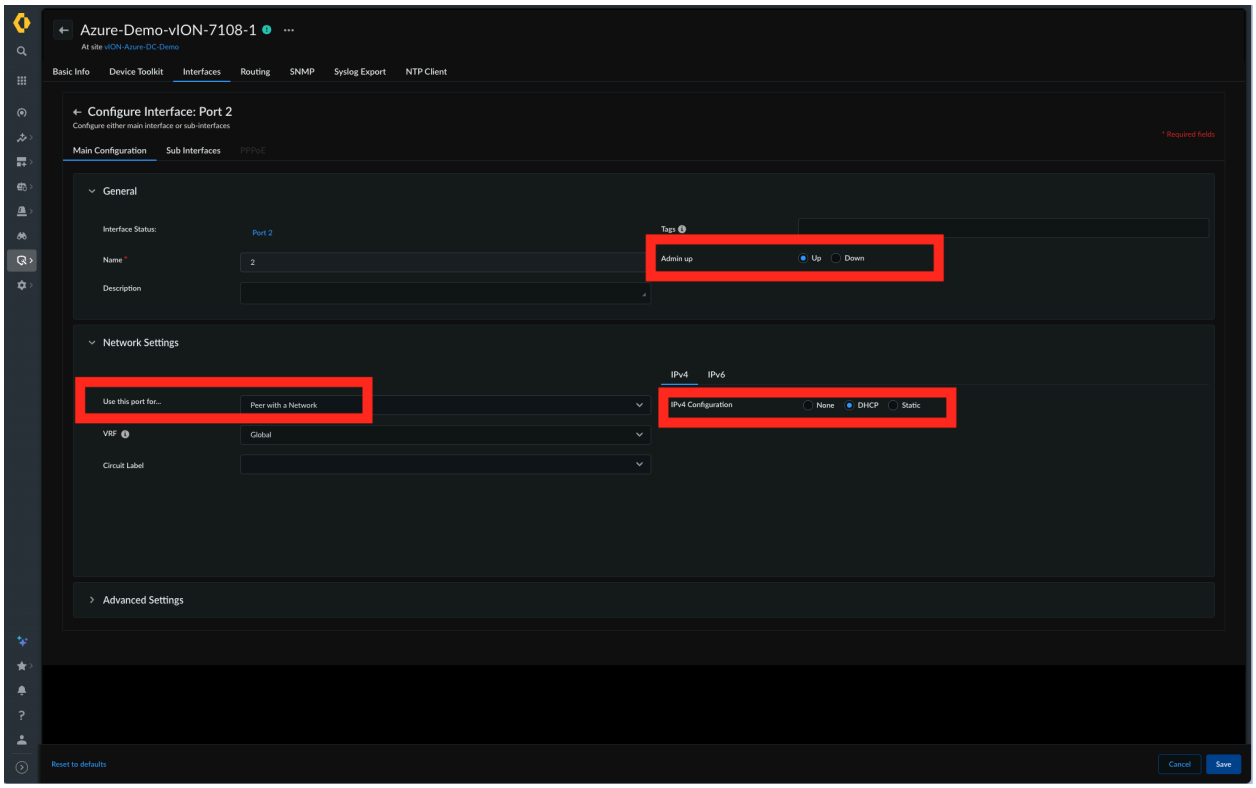
9. To find the external IP address go to the Azure portal and find the Public IP address provisioned in the resource group.



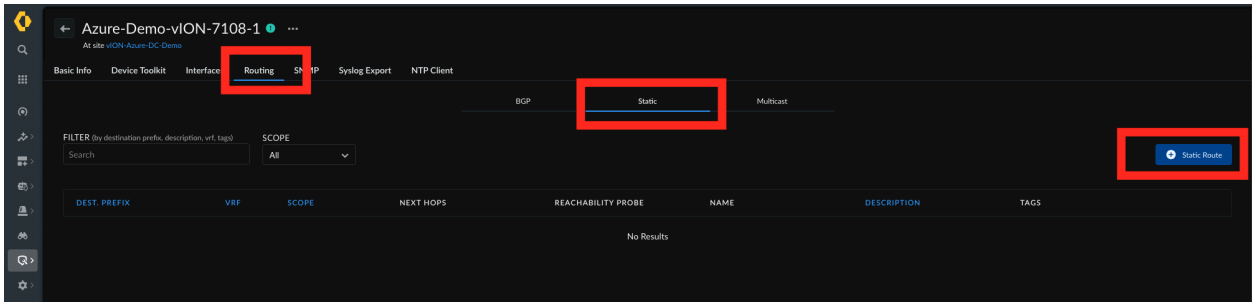
Take that IP address and go to the interface configuration for Port 1 of the vION, and under **Advanced Settings** enter the IP address in **External NAT Address (IPv4)** field and enter port 4500 under the **Port (IPv4)** field. Click on **Save**:



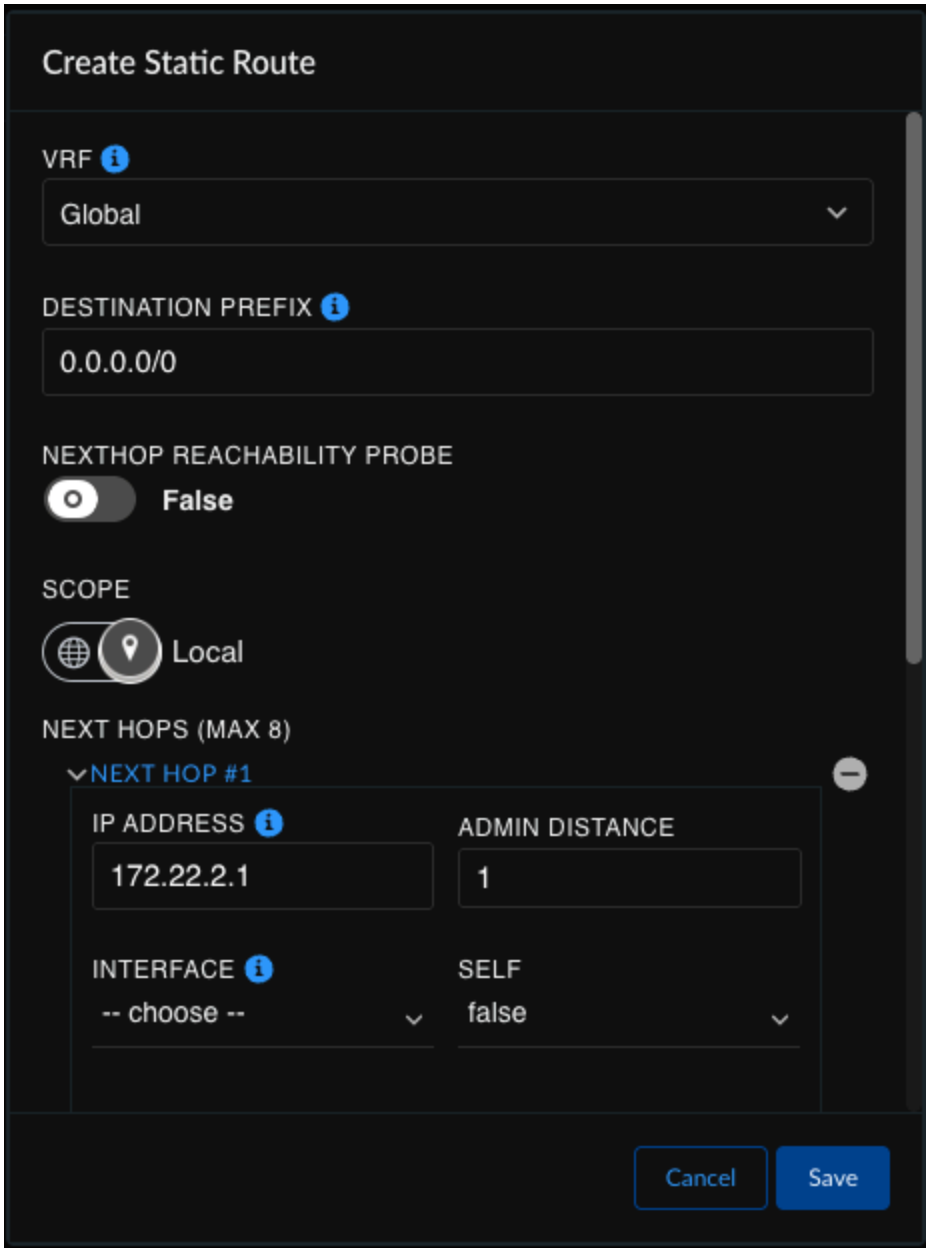
10. Configure port 2 to be **Admin Up** and Use this port to: **Peer with a Network**, and set for **DHCP**.



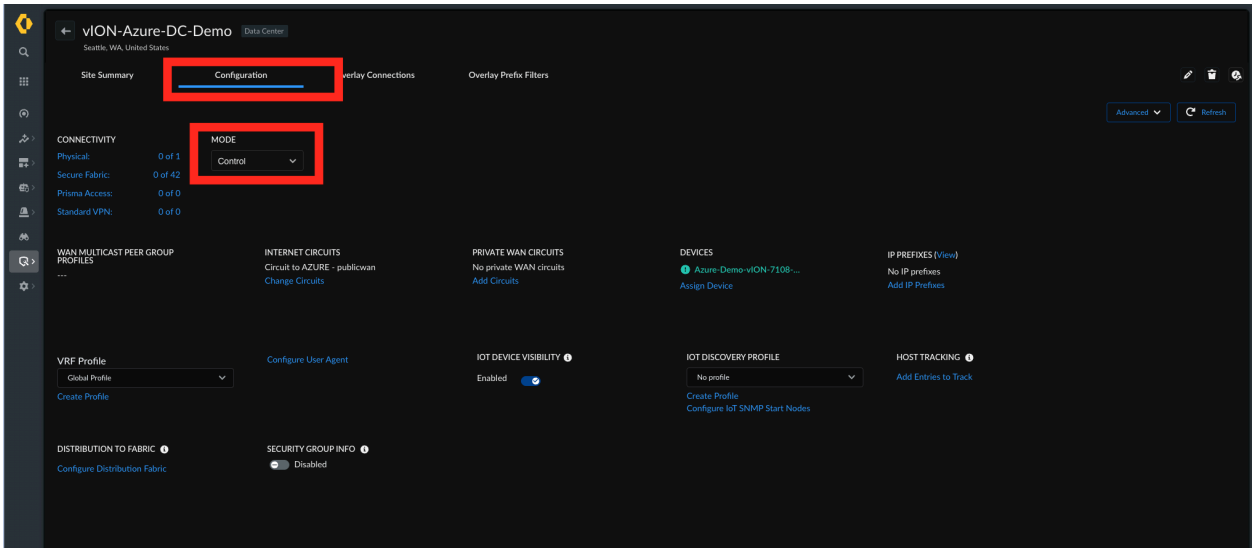
11. Under the vION's configuration go to the **Routing** tab, click on the **Static** tab, and then on the **+ Static Route** button.

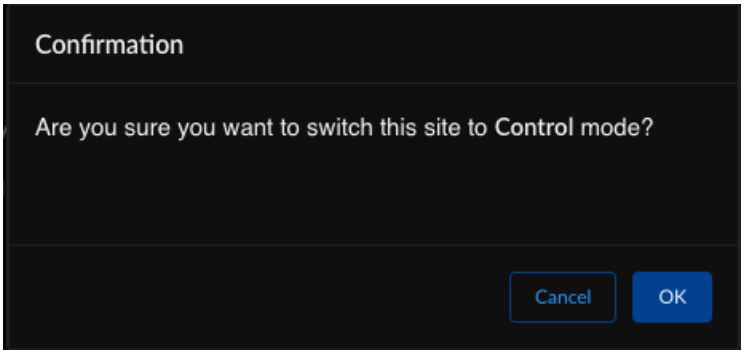


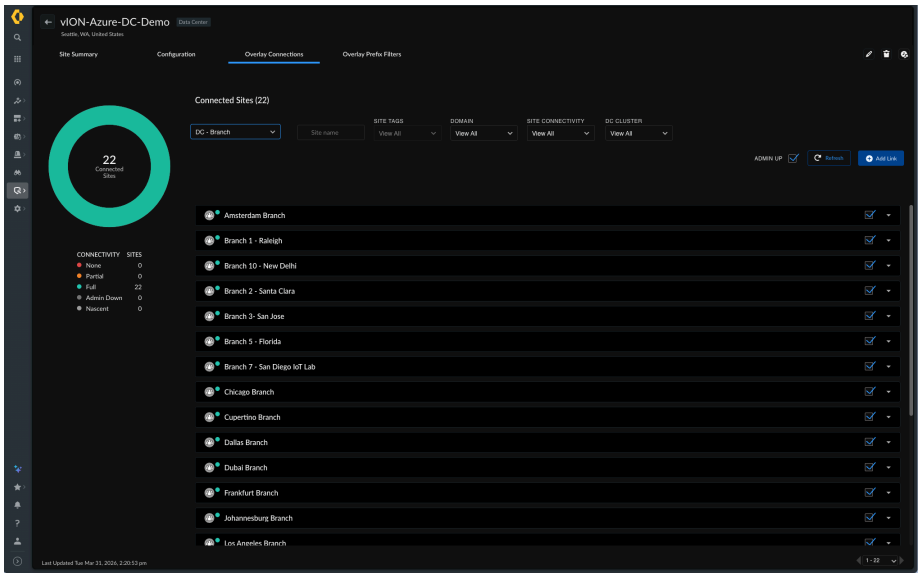
Configure a static default route pointing to the gateway of port 2 (the 1st IP address of the private subnet specified in the deployment template).



12. Go to the DC site configured earlier, under the **Configuration** tab under **Mode** switch the site to **Control** mode and verify the VPNs are up and active (this may take a few minutes). If VPNs do not come up within 5 minutes: verify Port 1 External NAT Address and Port settings are correct, confirm the NSG allows inbound UDP 500/4500, and check the Azure Serial Console for error messages.



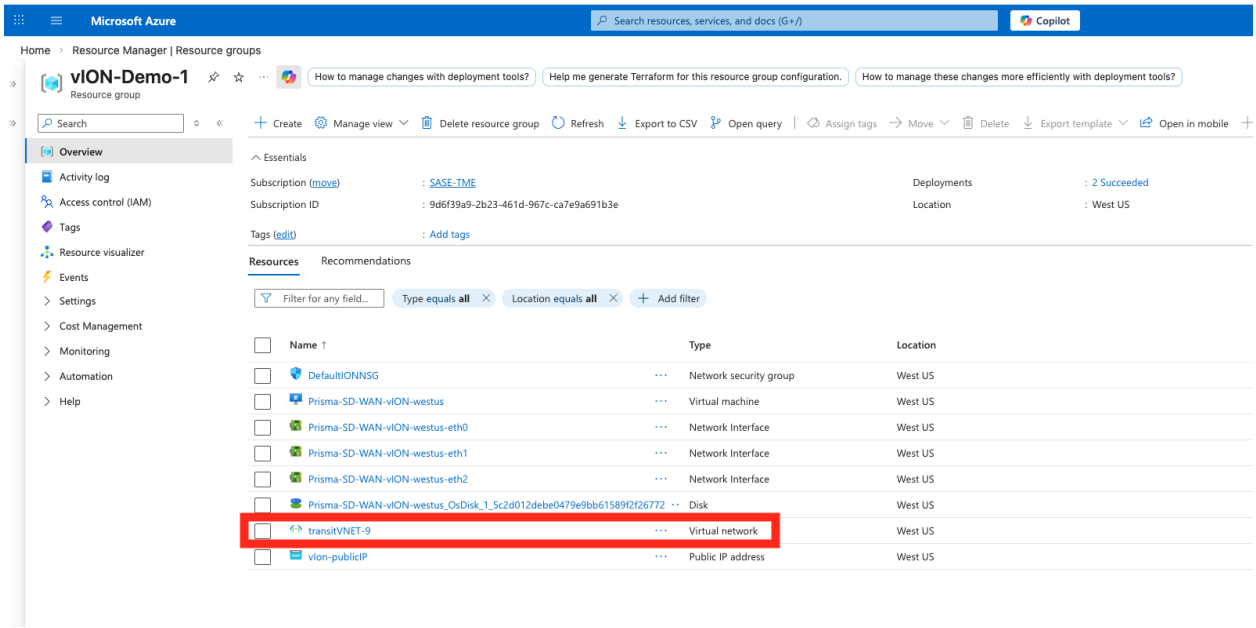




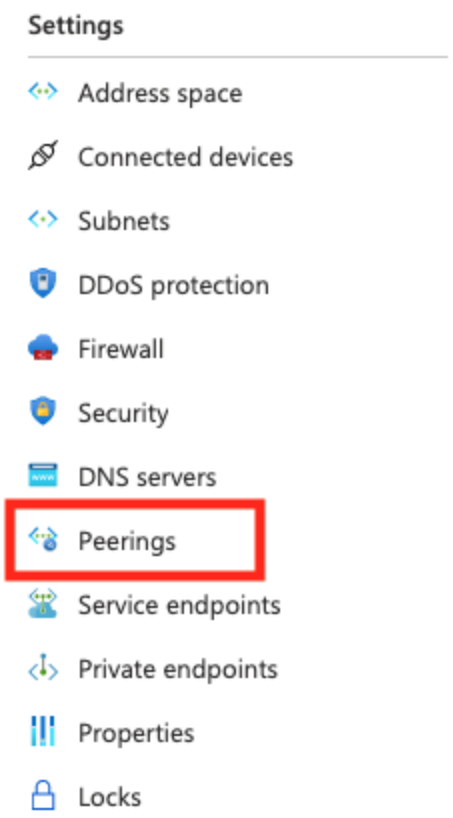
Proceed to the next section to finalize the Azure deployment steps.

Finalize Azure Configuration

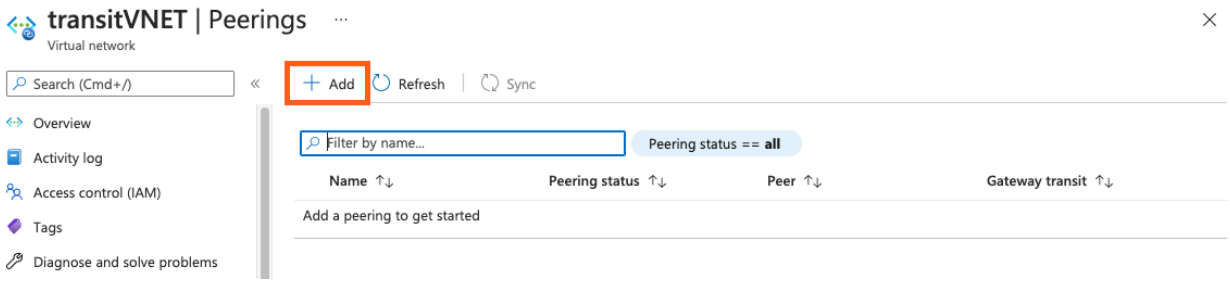
1. Login to the Azure Portal and go into the **Resource group** that was created via the deployment template select the VNET object.

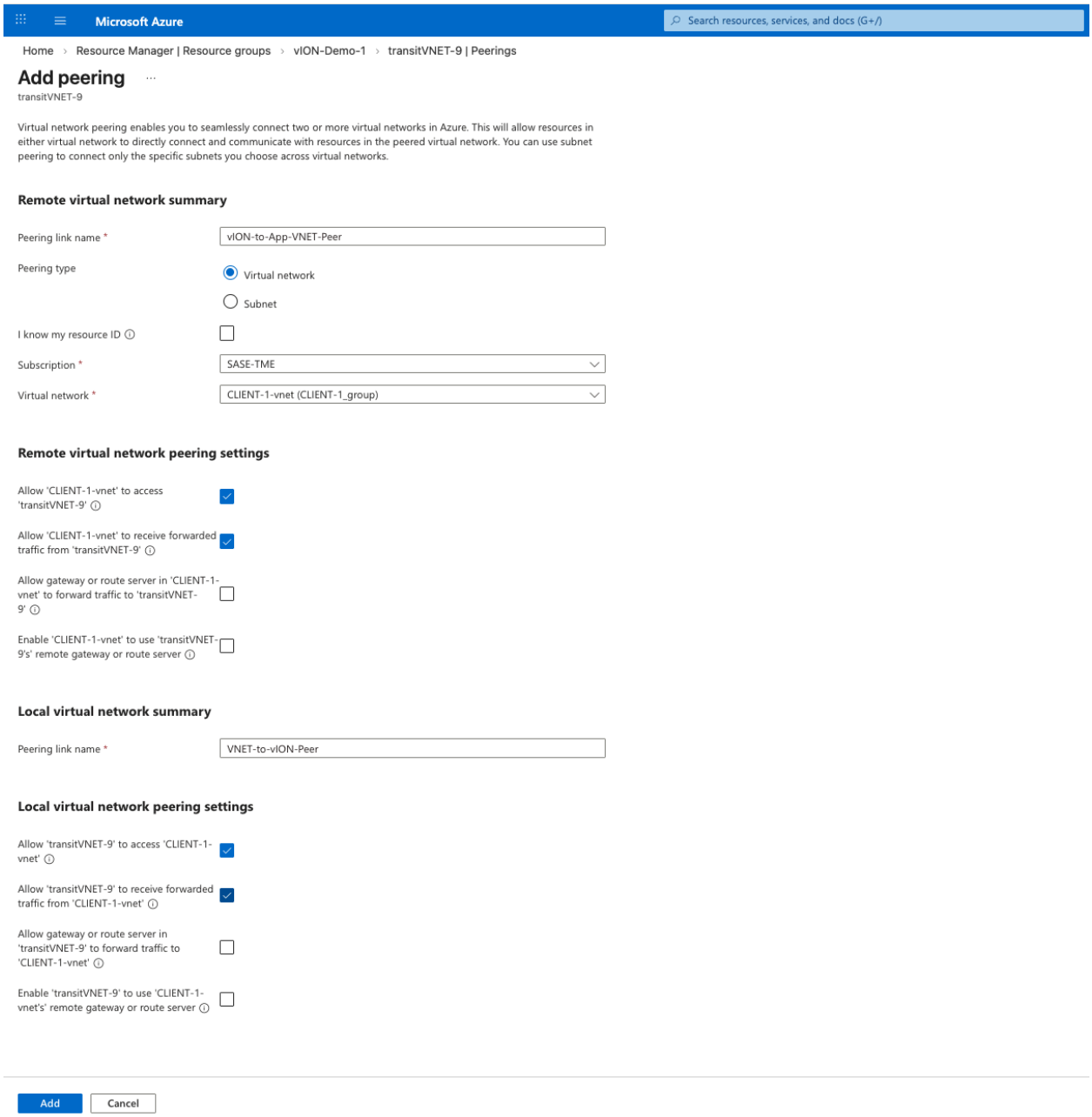


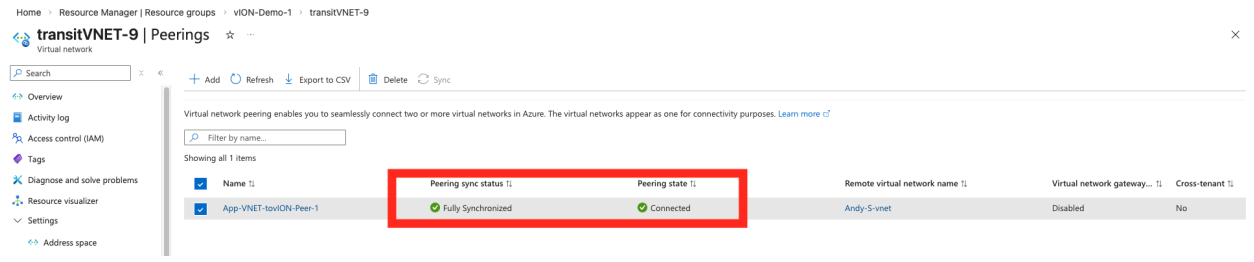
2. Enter the **Peerings** configuration section to set up VNET peering between the Prisma SD-WAN VNET and each of your application VNETs.



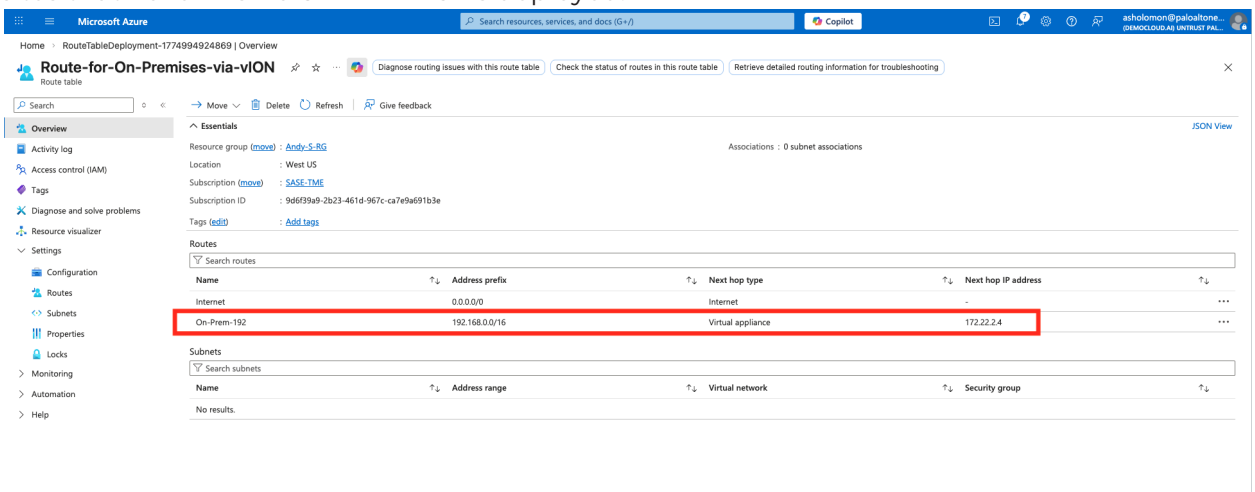
3. Add a VNET peering relationship from the Prisma SD-WAN VNET to the application VNETs. Specify the VNET you wish to peer with from the drop-down, select the checkbox to allow traffic to and from the remote VNET. Once completed, verify the peering status is connected.





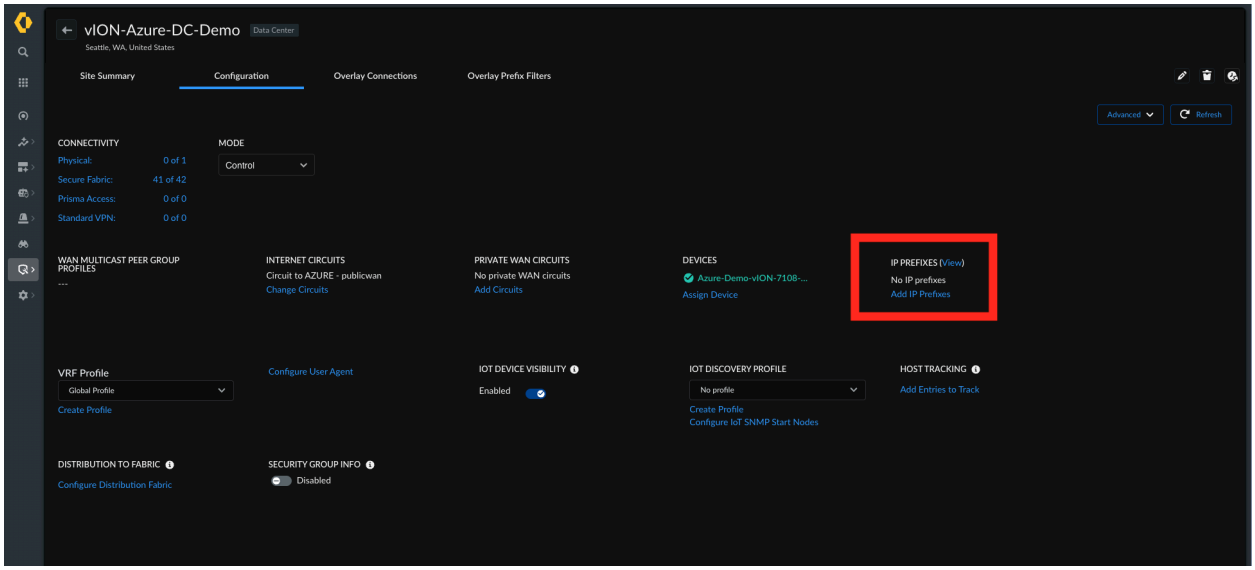


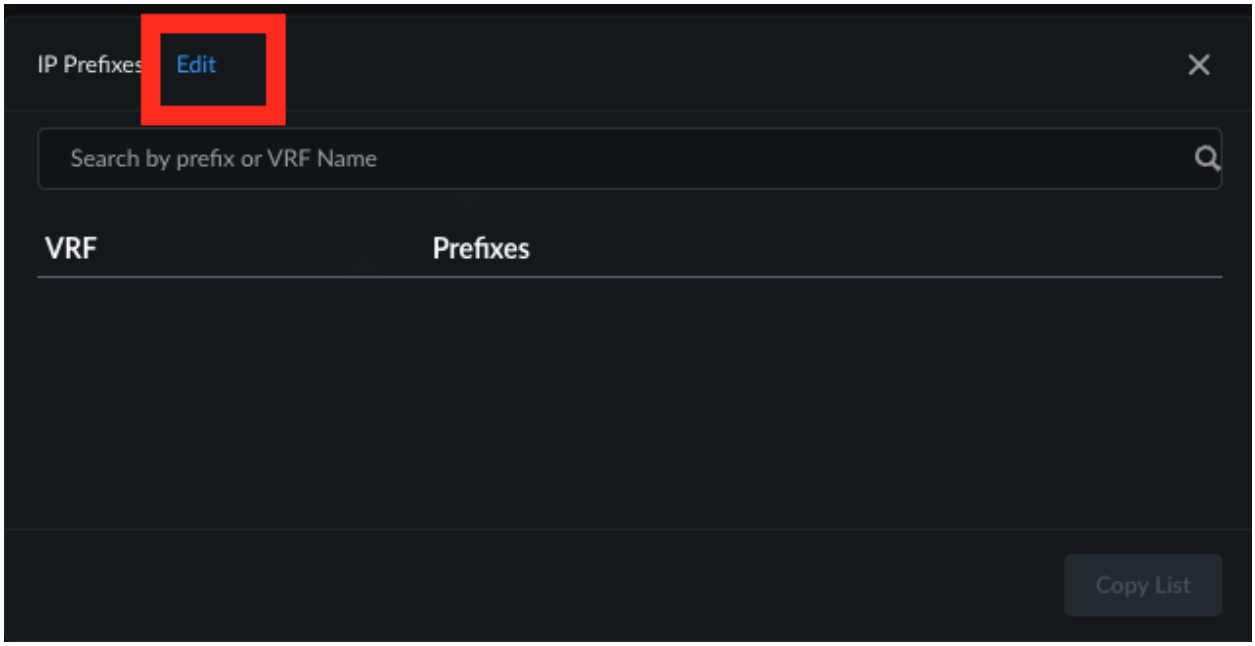
4. In order for return traffic from the application back to the on-premises networks to be sent via the Prisma SD-WAN VPN, add a static virtual appliance route in the application VNET subnet route table pointing back to the ION as the next hop for corporate subnets. In the below screenshot example 172.22.2.4 is the IP address of the Peering port of the ION 7K and 192.168.0.0/16 is the summary prefix of all remote sites that have Prisma SD-WAN IONs deployed.

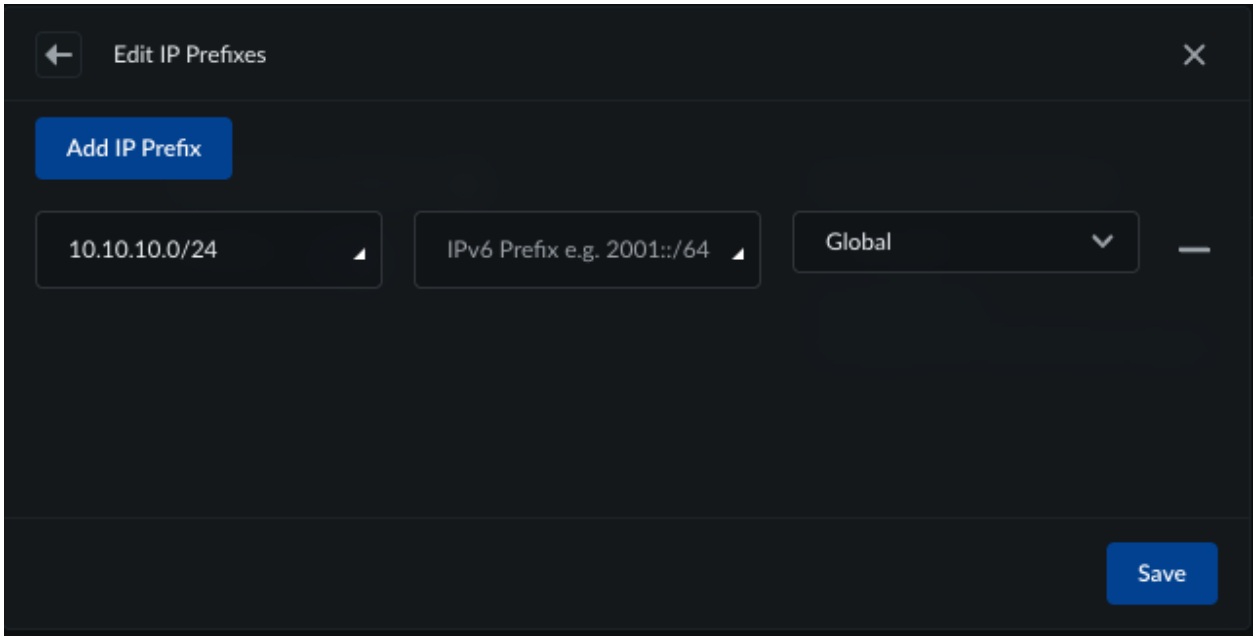


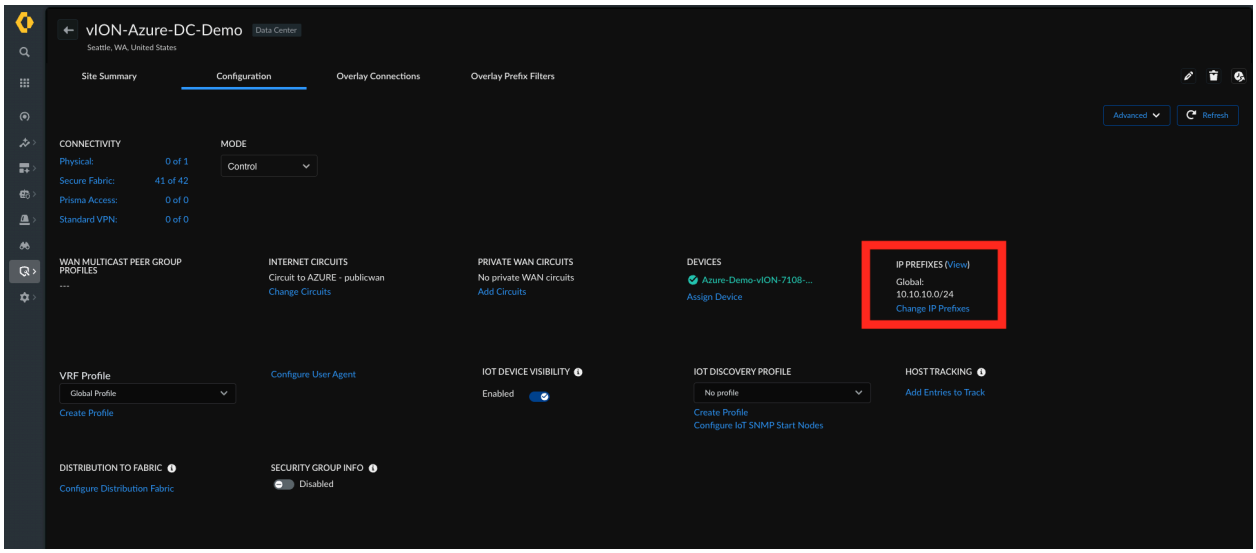
Note: It is assumed a route table is already deployed within the application VNET for which the application VMs are associated, including the relevant subnet associations. For more information on using route tables within Azure see here.

5. Advertise the Azure application VNET prefixes into the Prisma SD-WAN fabric by defining them on the Azure DC Site. From the **Configuration -> Prisma SD-WAN** -> **Data Centers**, click on the DC you created to bring up the menu, click on the **Configuration** tab to **Add IP Prefixes.** Enter each prefix in CIDR notation (e.g., 10.10.10.0/24). Add one prefix per entry.









Once completed traffic destined to the prefix (10.10.10.0/24) will be able to be sent directly to Azure over one or more Prisma SD-WAN Internet VPN paths.

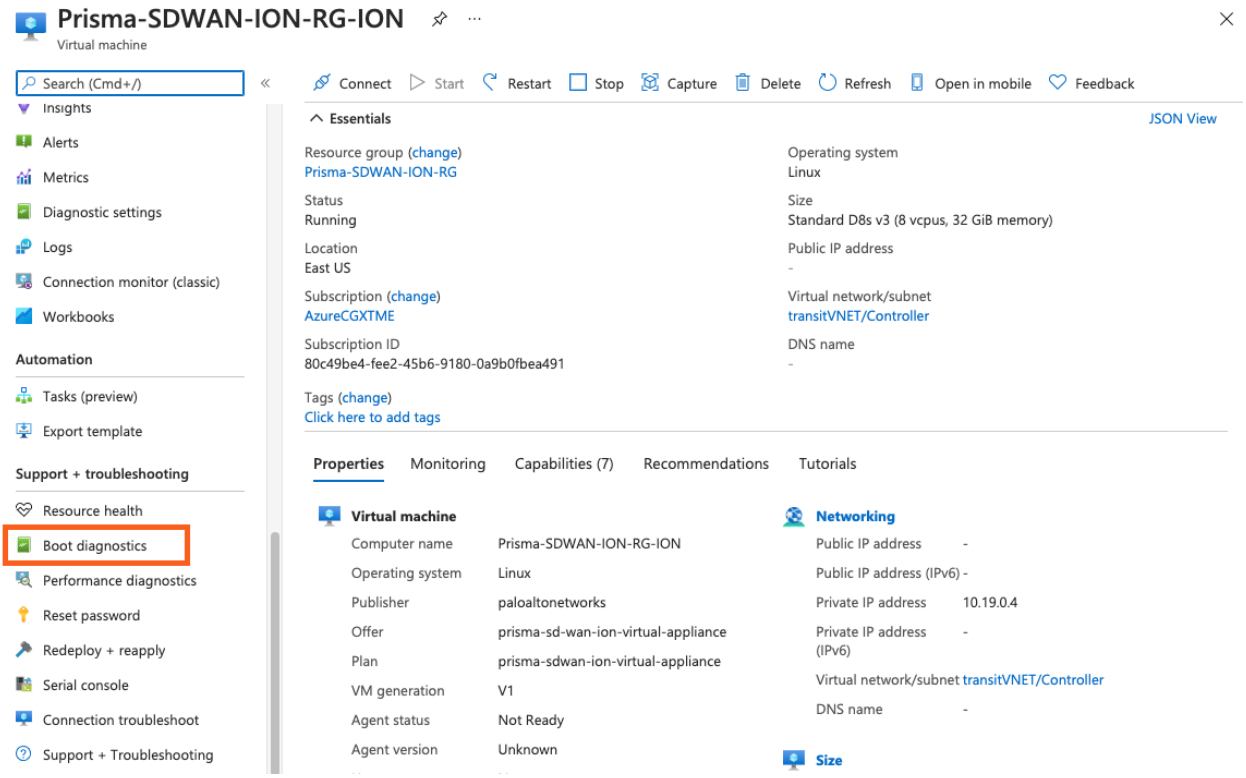
This assumes that the traffic destined to these applications and prefixes match a path policy rule that allows VPN over a public path. For more information review the **Prisma SD-WAN Stacked Policies**.

Troubleshooting

Using Azure Serial Console to access Virtual ION

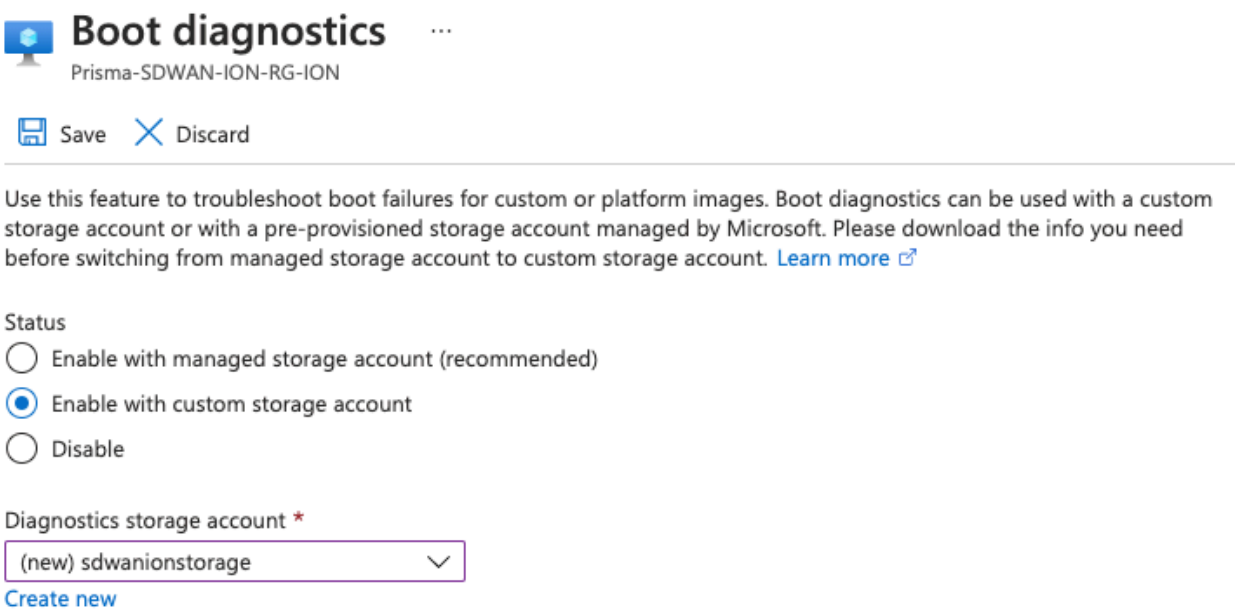
You may need to connect the console of the vION for troubleshooting, to connect follow these steps.

Step 1. Navigate to the Virtual Machine in the **Resource group** where the vION was deployed and select **Boot Diagnostics.**

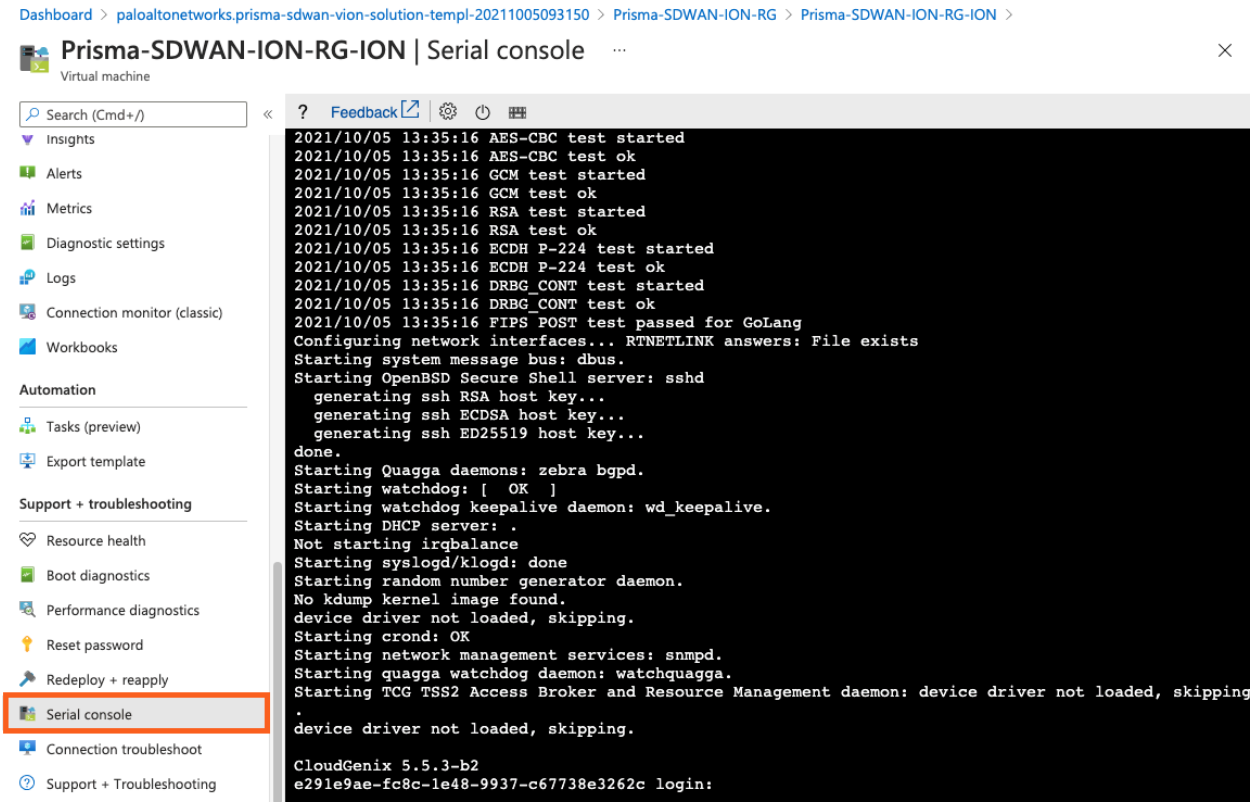


Step 2: Enable boot diagnostics by selecting **Enable with custom storage account** and choose an existing or create a new storage account.

Note: Enabling boot diagnostics with a storage account incurs Azure storage costs. Disable boot diagnostics after resolving the issue to avoid ongoing charges.



Step 3. From the **Support + Troubleshooting** in the left hand navigation bar of the virtual machine select **Serial Console.**



Note: 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.

Important: Change any default credentials immediately after initial setup.

