



TECHDOCS

Virtual ION on Azure Deployment Guide

1.0.0

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2021-2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

March 22, 2022

Table of Contents

Plan a Prisma SD-WAN Azure Virtual Deployment.....	5
Prerequisites to Prisma SD-WAN Azure Deployment.....	6
Prisma SD-WAN Azure Virtual Deployment.....	7
Manage Virtual ION Licenses and Tokens.....	9
Deploy Prisma SD-WAN to Azure.....	11
Deploy Using the Prisma SD-WAN Azure Deployment Template.....	12
Deploy vIONs with (High Availability) HA in Azure.....	16
Claim the Prisma SD-WAN ION and Assign to a Datacenter.....	19
Finalize Azure Configuration.....	22
Use Azure Serial Console to access Virtual ION.....	25

Plan a Prisma SD-WAN Azure Virtual Deployment

Prisma SD-WAN Azure Virtual Deployment guide provides instructions for deploying Prisma SD-WAN ION devices to Microsoft Azure. This guide is intended for network administrators.

- [Prerequisites to Prisma SD-WAN Azure Deployment](#)
- [Prisma SD-WAN Azure Virtual Deployment](#)
- [Manage Virtual ION Licenses and Tokens](#)

Prerequisites to Prisma SD-WAN Azure Deployment

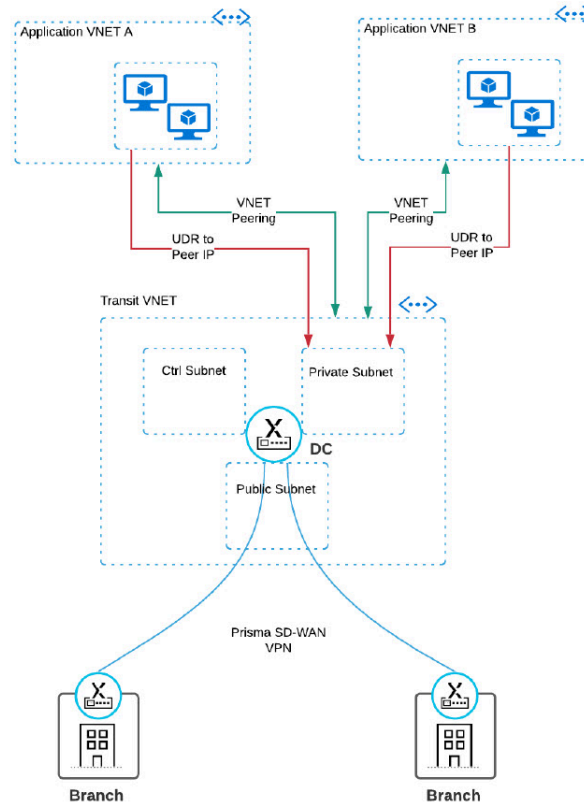
The following considerations are required to be met for the Prisma SD-WAN Azure deployment:

- Prisma SD-WAN
 - An active Prisma SD-WAN subscription with sufficient licenses to install at least 1 x v7108 ION.
- Microsoft Azure
 - An Azure account with permissions to create and update Azure Resource Groups, VNET (Virtual Network) and Virtual Machines.
 - An active Azure marketplace subscription to the Prisma SD-WAN ION Virtual Appliance.

Prisma SD-WAN Azure Virtual Deployment

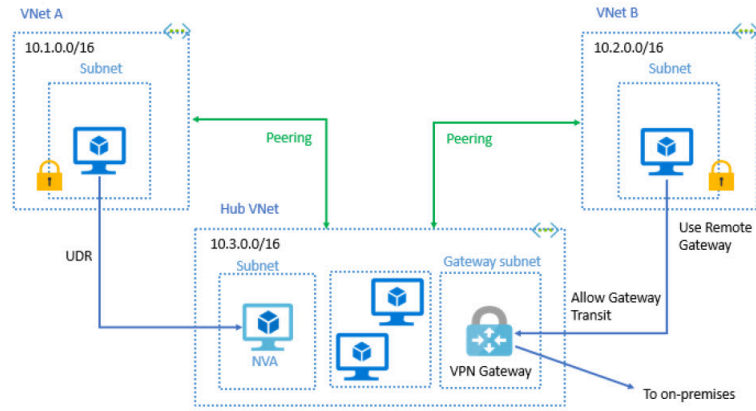
The Prisma SD-WAN Azure Virtual Deployment guide provides instructions for deploying Prisma SD-WAN ION devices to Microsoft Azure. It is intended for network administrators who plan to extend the Prisma SD-WAN fabric between existing or, to be deployed data centers in Azure VNETs hosting applications 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 data center deployment model.



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.

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 is shown depending on the design of the organization. Refer [here](#) for more information on VPN Gateway Peering.



Manage Virtual ION Licenses and Tokens

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

To deploy a Virtual ION using the Prisma SD-WAN Deployment Template in Azure you must first login to the Prisma SD-WAN portal and generate a token for the appropriate model.

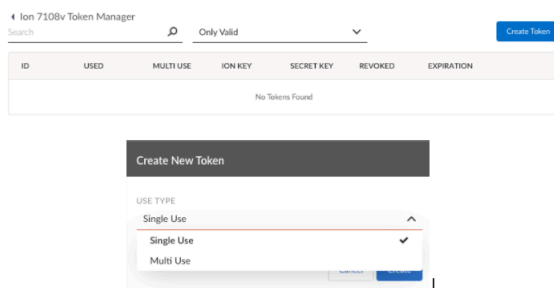


*Only a **Super User** role can generate the authorization tokens.*

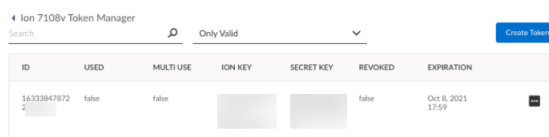
STEP 1 | Log in to the Prisma SD-WAN portal and select **Settings > ION License Management > Manage Tokens**.

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 Azure deployment. These are mapped to the values of `ion_key` and `secret_key` in the Azure environment.



Deploy Prisma SD-WAN to Azure

- [Deploy Using the Prisma SD-WAN Azure Deployment Template](#)
- [Deploy vIONs with \(High Availability\) HA in Azure](#)
- [Claim the Prisma SD-WAN ION and Assign to a Datacenter](#)
- [Finalize Azure Configuration](#)
- [Use Azure Serial Console to access Virtual ION](#)

Deploy Using the Prisma SD-WAN Azure Deployment Template

STEP 1 | Log in to the Azure Portal and navigate to the Marketplace. Search for **Prisma SD-WAN vION Solution Template for Azure Cloud** and select **Create**.



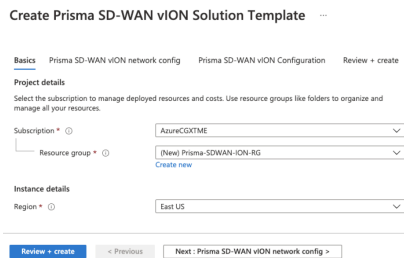
STEP 2 | In the **Basic** tab you will have the following options:

- **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.



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.



STEP 3 | Select Next: Prisma SD-WAN vION network config.

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 is recommended to leave this as the default 0.0.0.0/0 setting.

The screenshot shows the 'Prisma SD-WAN vION network config' page. It includes the following configuration options:

- Virtual network: (new) transitVNET
- Controller Subnet: (new) Controller (10.19.0.0/24)
- Internet/Public Subnet: (new) Internet (10.19.1.0/24)
- LAN/Private Subnet: (new) LAN (10.19.2.0/24)
- Network Security Group: inbound source IP: 0.0.0.0/0

Navigation buttons at the bottom include 'Review + create', '< Previous', and 'Next: Prisma SD-WAN vION Configuration >'.



*These are the default values, if you want to customize these settings select **Create new** 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.

The 'Create virtual network' dialog shows the following configuration:

- Name: CustomVNET
- Address space: 10.100.0.0/16 (10.100.0.0 - 10.100.255.255 (65536 addresses))

Subnet name	Address range	Address
Controller	10.100.0.0/24	10.100.0.0 - 10.100.0.255 (256 addresses)
Internet	10.100.1.0/24	10.100.1.0 - 10.100.1.255 (256 addresses)
LAN	10.100.2.0/24	10.100.2.0 - 10.100.2.255 (256 addresses)

STEP 4 | Once complete, click **Next: Prisma SD-WAN vION Configuration**.

STEP 5 | 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.
- Domain name label: Must be unique
- Private IP Address: IP address in the Internet Subnet that will be assigned to the Virtual IONs Port 1 interface.



Azure reserves the first 3 IP addresses in any subnet, chose from the 4th available IP address in the Internet Subnet.

- Gateway: First IP address from the Internet Subnet
- DNS: DNS IP address for Port 1, you can use Azure’s own DNS 168.63.129.16# or any public DNS for example 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 Licence Key: Use the License Key that was generated from the Prisma SD-WAN portal.
- Prisma SD-WAN vION Secret Key: Use the License Key that was generated from the Prisma SD-WAN portal.
- Virtual Machine Size: Leave at the default selection.

The screenshot shows the 'Prisma SD-WAN vION Configuration' tab in the Azure portal. The form contains the following fields and values:

- Public IP address: (new) Internet-Interface-PublicIP
- Domain name label: tmeion1
- Private IP address: 10.19.1.4/24
- Gateway: 10.19.1.1
- DNS: 8.8.8.8
- Prisma SD-WAN vION Version: latest
- Enable Bootstrap: yes
- Prisma SD-WAN vION License Key: 1092-72eb-5c2d-fa12-4d01-b21a-bd49b-4db1ac8
- Prisma SD-WAN vION Secret Key: 346d91744e2c5cc6d5114089e043a6035d7297b
- Virtual machine size: 1x Standard D8s v3 (8 vcpus, 32 GB memory)

STEP 6 | Click **Next: Review + Create now**, Azure will validate the configuration against the deployment template.

Create Prisma SD-WAN vION Solution Template ...

Validation Passed

Basics

Subscription	AzureCGXTME
Resource group	Prisma-SDWAN-ION-RG
Region	East US

Prisma SD-WAN vION network config

Virtual network	transitVNET
Controller Subnet	Controller
Address prefix (Controller Subnet)	10.19.0.0/24
Internet/Public Subnet	Internet
Address prefix (Internet/Public Subnet)	10.19.1.0/24
LAN/Private Subnet	LAN
Address prefix (LAN/Private Subnet)	10.19.2.0/24
Network Security Group: inbound sourc...	0.0.0.0/0

Prisma SD-WAN vION Configuration

Public IP address	Internet-Interface-PublicIP
Domain name label	tmeion1
Private IP address	10.19.1.4/24
Gateway	10.19.1.1
DNS	8.8.8.8
Prisma SD-WAN vION Version	latest
Enable Bootstrag	yes
Prisma SD-WAN vION License Key	1092-████████████████████b4db1ac8
Prisma SD-WAN vION Secret Key	34d-████████████████████7297b
Virtual machine size	Standard_D8s_v3

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

Deploy vIONs with (High Availability) HA in Azure

Use the Azure high availability (HA) templates to deploy the vIONs in Prisma SD-WAN using the marketplace solution.

STEP 1 | Create a **Resource Group** in the desired region in Azure.

Find the Marketplace listing of Prisma SD-WAN vION solution template and select **Prisma SD-WAN vION HA Solution Template**.



STEP 2 | Deploy the pair of vIONs by following the steps in the solution template.

1. Select the correct **Subscription, Resource Group, and Region.**



2. Configure the virtual networks required for the HA vIONs.
The template creates a new **Virtual network** with six subnets:

- ION 1 Controller
- ION 1 Internet/Public
- ION 1 LAN/Private
- ION 2 Controller
- ION 2 Internet/Public
- ION 2 LAN/Private

If you choose to use an existing virtual network, ensure that the selected **Virtual network** consists of six subnets.



3. Configure the Private IP addresses for the internet or Public of each vION required for the vIONs to reach the controller over the WAN interface.

- Configure the IP address for the Internet/Public subnet and the Gateway.
- Take note of the Internet/Public subnet for each ION.
- For the IP address, assign any address in the subnet other than the first four prefixes in the subnet (Azure uses these and are reserved).
- For the Gateway address, use the first available IP address in the subnet.
- For the DNS address, use a well-known public DNS service (For example, 8.8.8.8 or 1.1.1.1).

4. Configure the [Availability Zones](#) or **Sets**.



- When deploying in an **Availability Zone**, ensure that the Azure region you are deploying supports zones. If the region does not, you can use an **Availability Set**.
- Enter a numerical value for the Zone parameter for each ION. This is typically a numeric value and is a number in the range of 1-3. When you use the same zone number for both

vIONs, the vIONs are deployed in the same zone, and there will be no use of an Availability Set.

- Specify **None** as the zone value, if there is no Zone support in the region you're deploying or you wish to use an availability set. The vIONs thereby will be deployed in an Availability Set (across different fault or update domains) within the same region.

5. Configure the vION **License and Secret Keys** obtained from Prisma SD-WAN Controller.



6. Configure the vION version. It's recommended to use the default configuration.

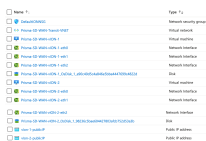


STEP 3 | Confirm if all resources are fully deployed and appear in the resource group created.

If the zones configured are correct and are supported in Azure, the vIONs will be deployed according to the specified availability zones. You can view and access the vIONs in the Prisma SD-WAN portal.



It can take a while for the resources to be fully deployed and the vIONs to connect to the controller.



Mark the availability zone as **None**, to create the following resource within the resource group.




STEP 4 | If Availability zones are not configured, verify the vIONs deployed across different fault domains by accessing the vION instance overview page in the Azure portal.



*You must deploy both vIONs in the same resource group along with one virtual network containing six subnets; three each for each vION's controller, internet, and LAN interfaces. You can now **claim** and **configure** the IONs in the Prisma SASE portal.*

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


After the ION successfully boots, as long as it can connect to the Prisma SD-WAN controller it will show up as Unclaimed: Online under the Map -> Unclaimed Devices section of the portal.

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

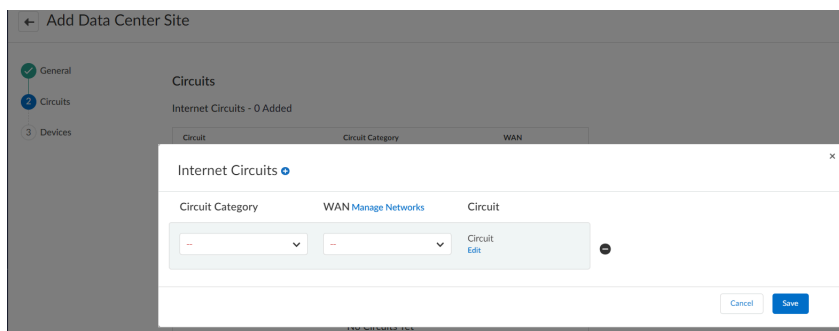
STEP 1 | Claim the device by selecting **Workflows > Prisma SD-WAN Setup > Devices > Unclaimed Devices > Claim the device**.

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

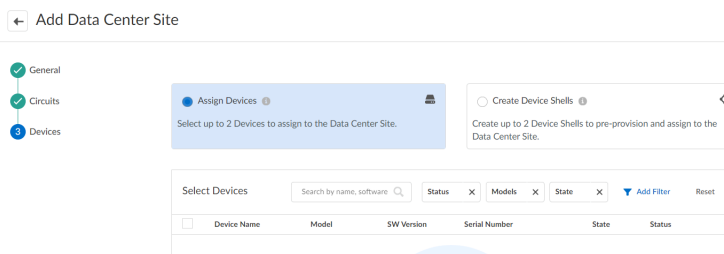
STEP 2 | Create a Data Center Site while the device is being claimed.

 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**.

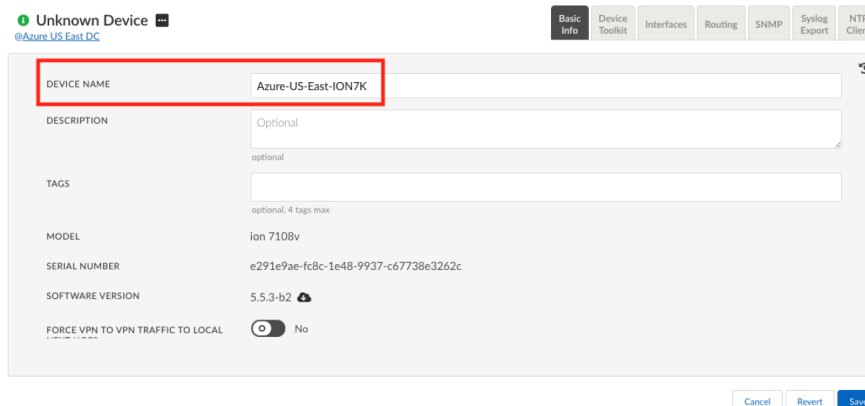


4. Assign the device to the data center by selecting **Assign Devices** and selecting the ION device from the list of **Select Devices** and **Save**.

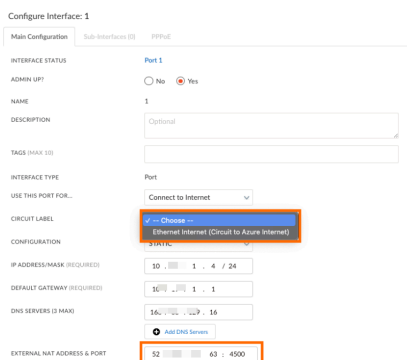
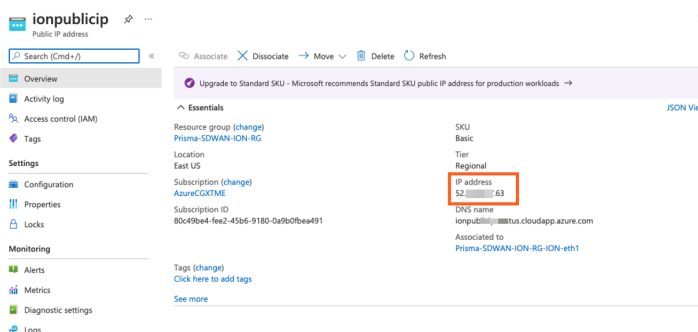


STEP 3 | Once the device is successfully assigned, click the device name to enter the device configuration screen.

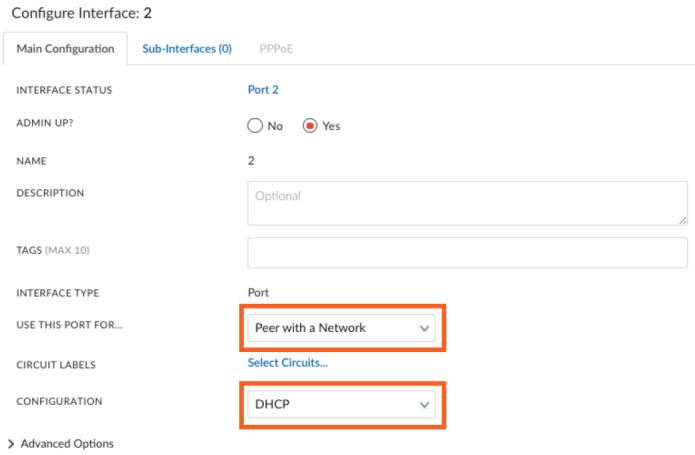
1. Enter a Device Name.



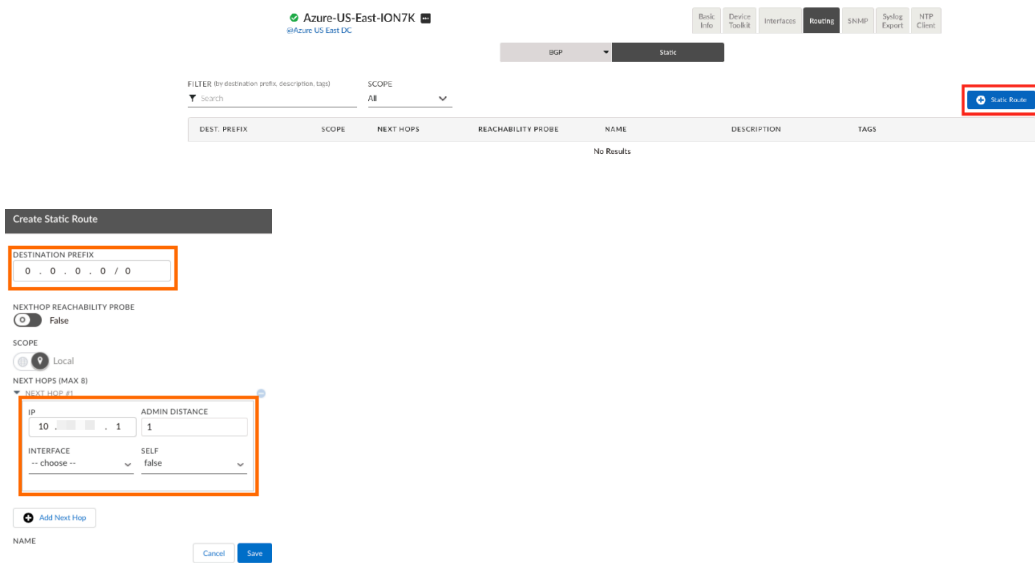
2. Configure Port 1, by assigning the Internet WAN circuit label you created in step 2 and providing the external NAT address and port. To figure out the external IP address go to the Azure portal and find the Public IP address provisioned in the resource group.



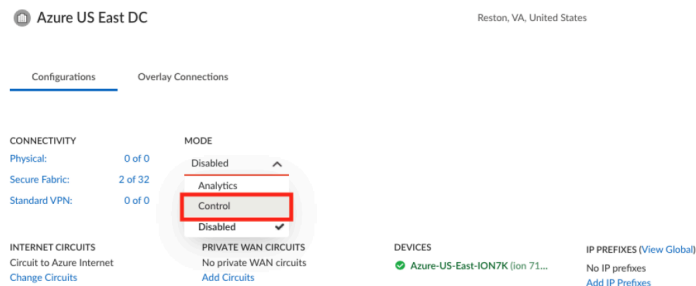
3. Configure port 2 to be Admin Up and Use this port to: Peer with a Network, and set for DHCP.



STEP 4 | 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).



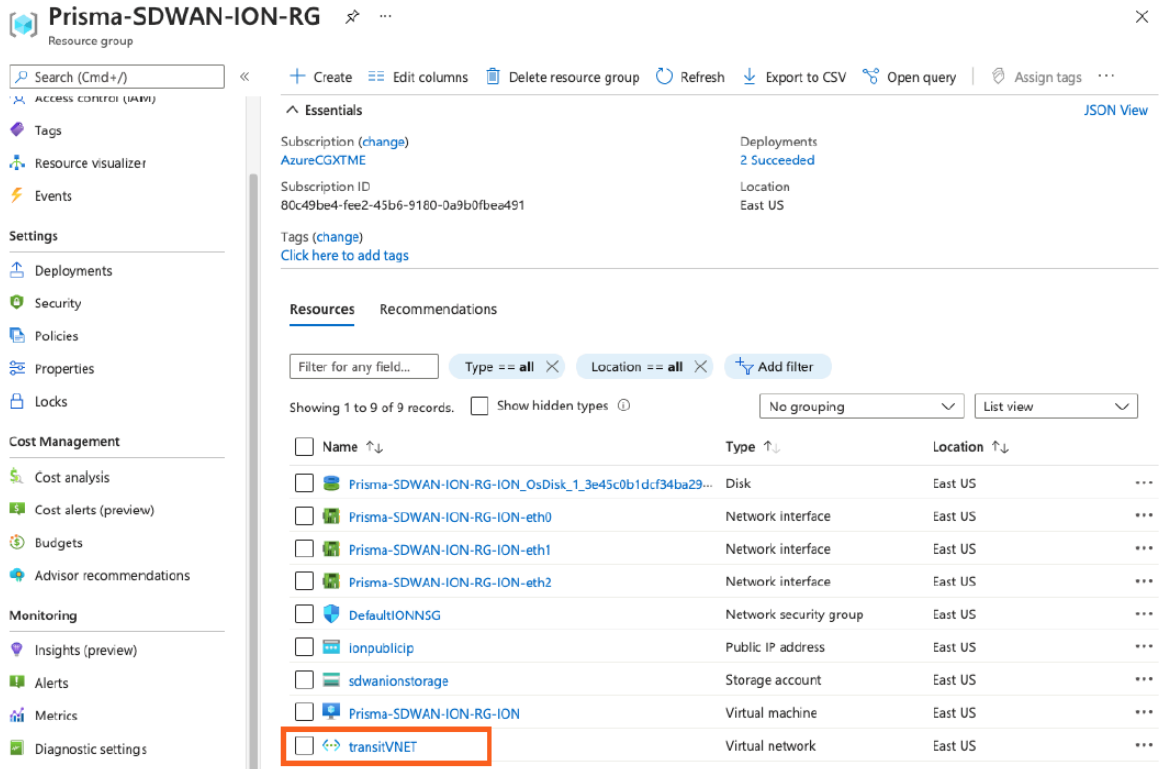
STEP 5 | Switch the site to **Control** mode and verify the VPNs are up and active.



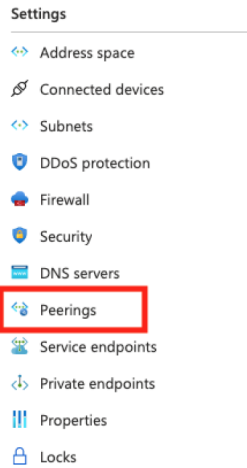
Proceed to the next section to finalize the Azure deployment steps.

Finalize Azure Configuration

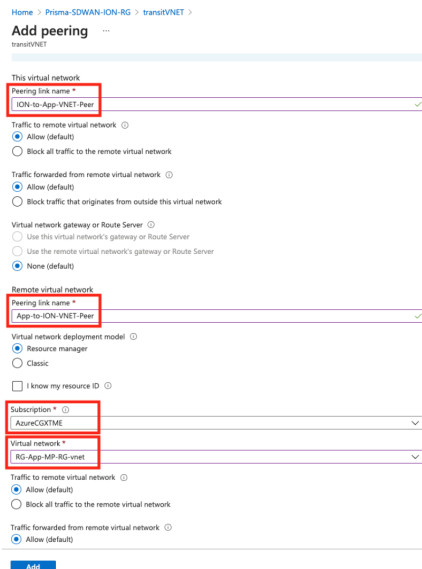
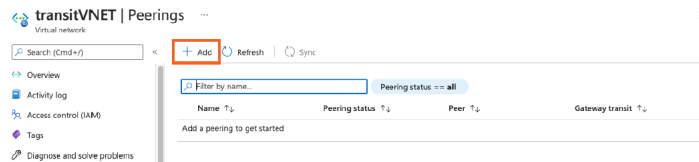
STEP 1 | Login to the Azure Portal and go into the Resource group that was created via the deployment template select the VNET object.



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

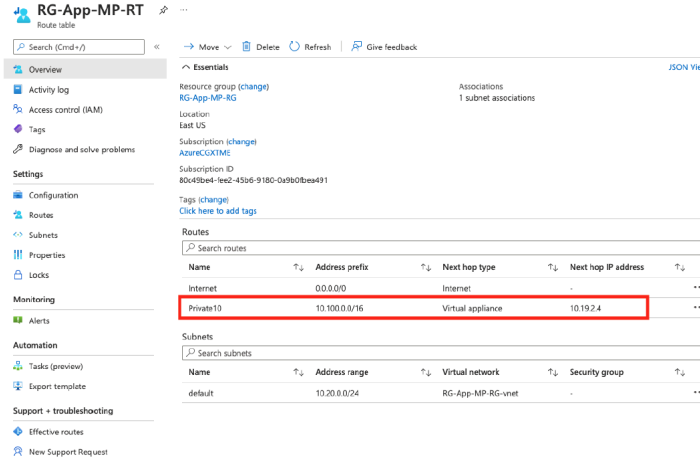


STEP 3 | Add a VNET peering relationship from the Prisma SD-WAN VNET to the application VNETs. Specify the VNET you wish to peer with from the drop-down, select the check box to allow traffic to and from the remote VNET. Once complete, verify the peering status is connected.



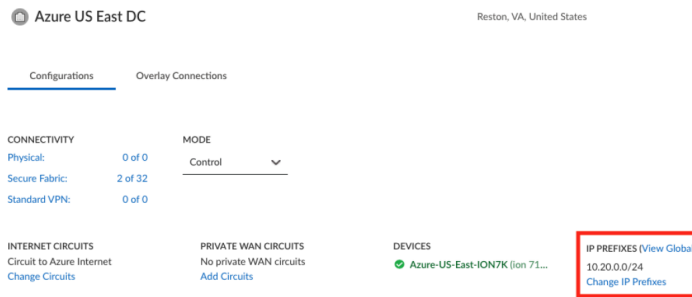
STEP 4 | In order for return traffic from the application back to the on-premise networks to be sent through the Prisma SD-WAN VPN, add a static virtual appliance route in the application VNET subnet route table pointing back to the ION as the next hop for corporate subnets.

In the below example, 10.19.2.4 is the IP address of the Peering port of the ION 7K and 10.100.0.0/16 is the summary prefix of all remote sites that have Prisma SD-WAN IONs deployed.



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.

STEP 5 | Advertise the Azure application VNET prefixes into the Prisma SD-WAN fabric by defining them on the Azure data center site. From the Prisma SD-WAN portal, go to **Map > Azure Site > Site** to bring up the menu to **Add IP Prefixes**.



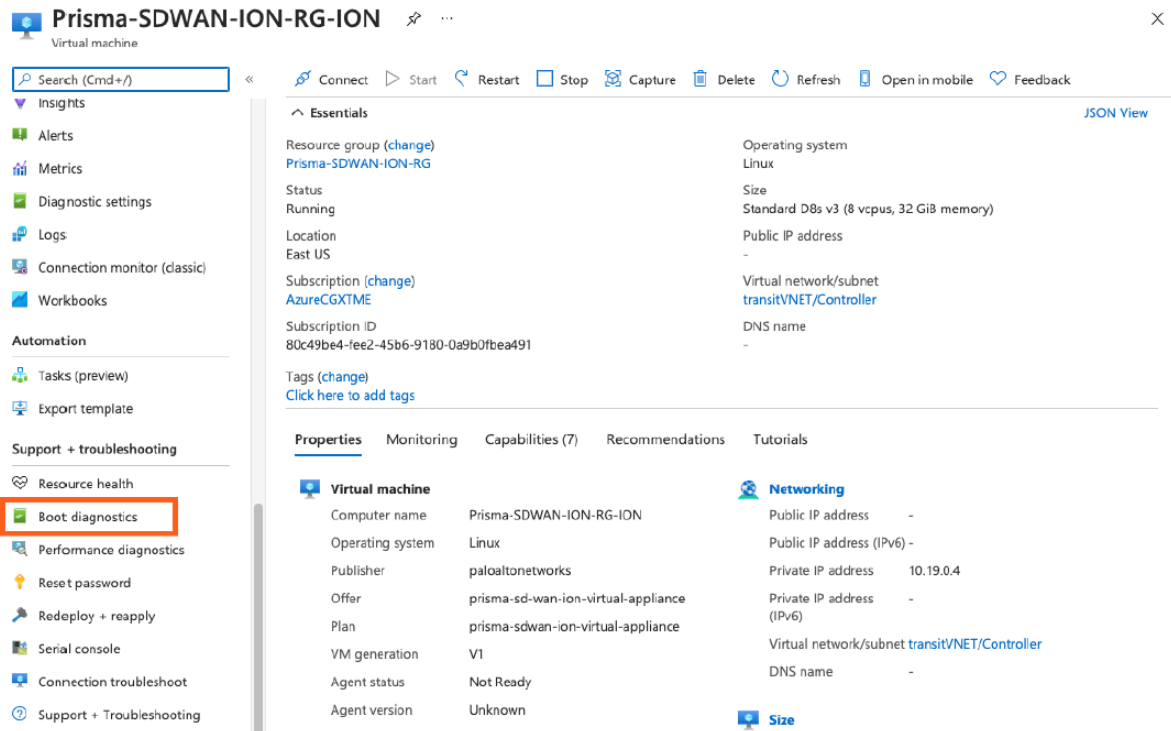
Once complete, traffic destined to the prefix (10.20.0.0/24) will be sent directly to Azure over one or more Prisma SD-WAN Internet VPN paths.

This assumes that the traffic destined to these applications and prefixes match a path policy rule that allows VPN over a public path.

Use Azure Serial Console to access Virtual ION

To connect to the console of the vION using the Azure serial console:

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.

Boot diagnostics ...

Prisma-SDWAN-ION-RG-ION


 Save  Discard

Use this feature to troubleshoot boot failures for custom or platform images. Boot diagnostics can be used with a custom storage account or with a pre-provisioned storage account managed by Microsoft. Please download the info you need before switching from managed storage account to custom storage account. [Learn more](#) 

Status

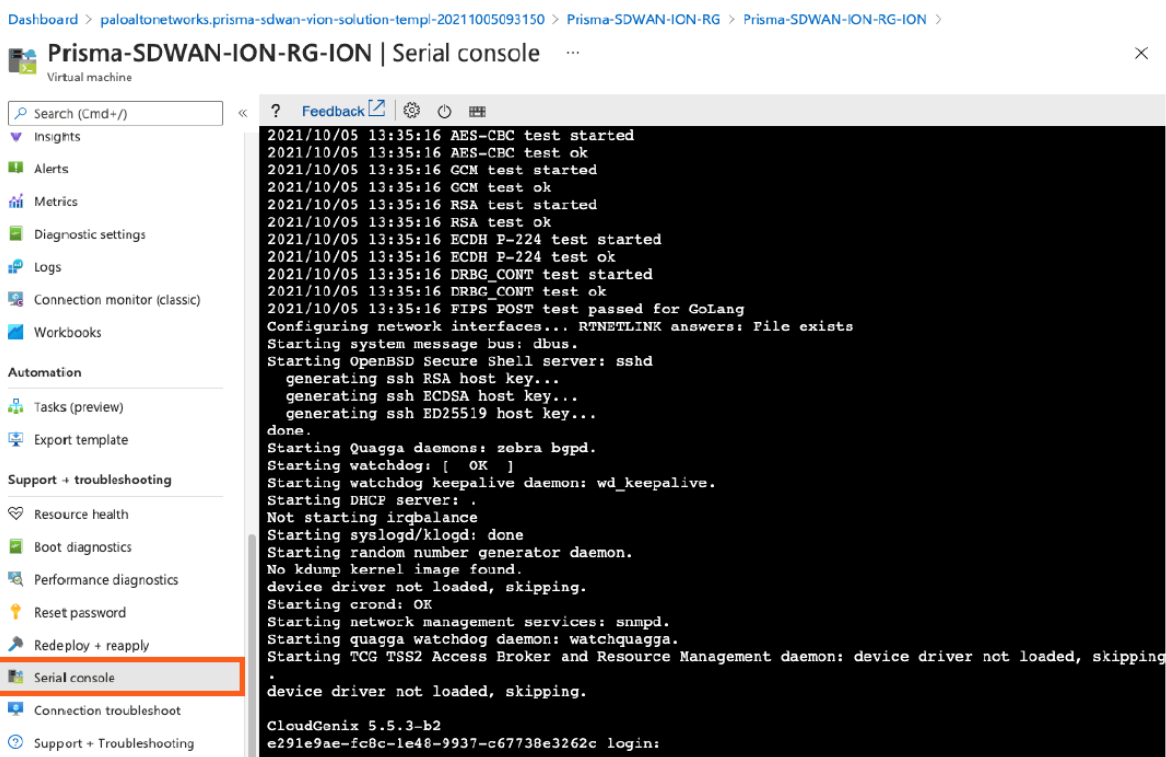
- Enable with managed storage account (recommended)
- Enable with custom storage account
- Disable

Diagnostics storage account *

(new) sdwanionstorage 

[Create new](#)

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



For an unclaimed device the default credentials are:

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

For a claimed device use the device toolkit user names and passwords.

