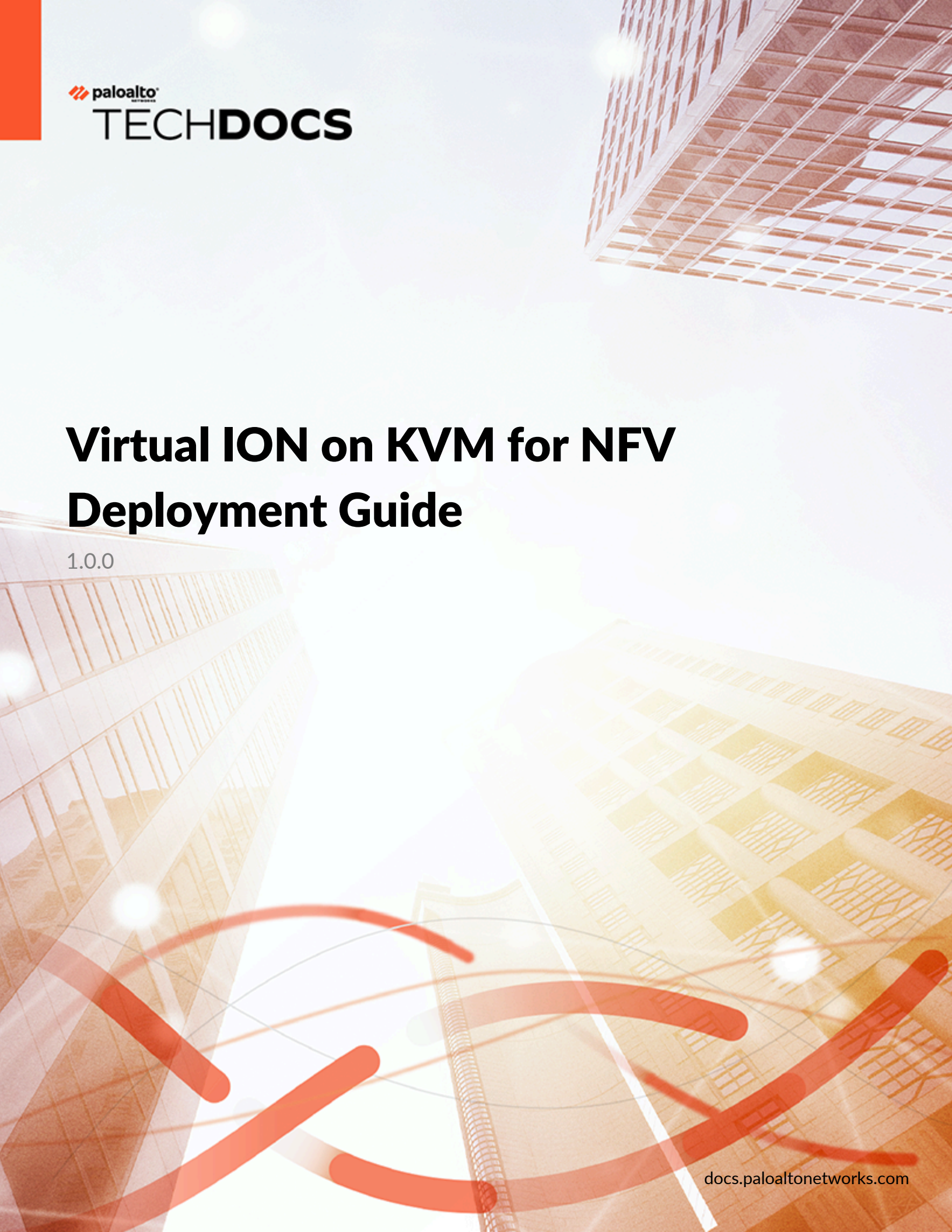
paloalto TECHDOCS

Virtual ION on KVM for NFV 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

March 22, 2022

Table of Contents

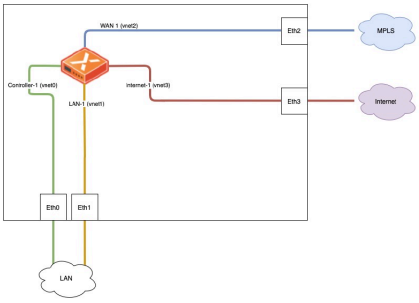
Prisma SD-WAN NFV Virtual Deployment

The Prisma SD-WAN Virtual ION on Kernel-based Virtual Machine (KVM) for Network Functions Virtualization (NFV) Deployment Guide introduces the essential concepts and components for licensing, and installation/deployment of a Prisma SD-WAN Virtual Form Factor device within an orchestration environment supporting KVM.

Prisma SD-WAN NFV Virtual Deployment Prerequisites

The Prisma SD-WAN Virtual ION on KVM for Network Functions Virtualization (NFV) Deployment Guide focuses specifically on deployment on standard NFV deployments. NFV can be instantiated and in many different forms and Prisma SD-WAN deployed on top of the NFV environment.

A virtual ION device can be deployed to an NFV host and assigned to either a branch or data center type of site. The design and deployment considerations are different between a branch and data center site. The VM deployment options such as the number of interfaces needed for the VM, how the virtual network interfaces are bound to physical NICs, etc. will vary based on these requirements. The following figure shows an example of a branch deployment where the virtual ION device is the WAN router terminating the MPLS and internet circuits.



To successfully deploy and configure Prisma SD-WAN in an NFV environment the vION model type and role should be determined prior to implementation. Download the latest release image from Palo Alto Networks and for sizing and resources requirements, refer to the SD-WAN datasheet and the Prisma SD-WAN documentation.

In summary, the supported NFV environment must meet the following requirements.

Deploy in standard NFV deployments, some examples are as follows:

- Linux-generic KVM on actively supported distribution releases (Ubuntu, CentOS/RHEL, and so on.)
- Advance NFV
- Oracle Cloud
- Sienna NFV

The Server or the generic uCPE hardware must meet the following requirements:

- x86 CPU host processor with 64-bit processing
- Hardware virtualization support

In order to facilitate the deployment of Prisma SD-WAN ION devices to an NFV host, Prisma SD-WAN provides the virtual image in a **qcow** format per model type.

Model Name	vCPU	Memory (GB)	Disk (GB)	Throughput (Mbps)
ION 3102v	2	8	40	100

Model Name	vCPU	Memory (GB)	Disk (GB)	Throughput (Mbps)
ION 3104v	4	8	40	200
ION 3108v	8	8	40	350
ION 7108v	8	32	100	500

Manage Virtual Form Factor (VFF) Licensing

Follow these steps for Virtual Form Factor (VFF) licensing.

STEP 1 | Order a specific set of virtual ION device model(s).

STEP 2 | Create licenses.

Prisma SD-WAN creates tenant specific license keys per model equal to the order count.

STEP 3 | Generate tokens.

- Tokens are generated via the portal by a customer administrator.
- Single use or multi use tokens, that are valid for 96 hours, are assigned during VM deployment.

STEP 4 | Deploy the ION VFF.

1. Deploy the ION VM to the NFV host.
2. Assign the ION device key and secret key through the NFV console wizard.

STEP 5 | Add to inventory.

- On boot up, the virtual ION device will connect to the controller and show up in inventory as **Online-Restricted**.
- Used license count for the appropriate model will increment.

STEP 6 | Claim and assign the ION device.

The customer administrator can now claim the device and assign it to a site.

Generate Tokens

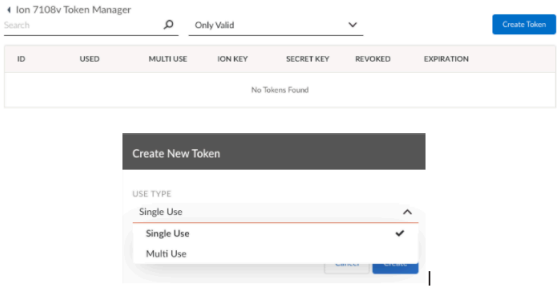
For virtual form factors in Prisma SD-WAN, the instance(s) are bound to an authorization token. This provides for a set of controls to prevent unauthorized virtual devices to be added to an environment. Once the Prisma SD-WAN account team or support team has confirmed that the licenses have been allocated to the customer tenant, the customer administrator must login to the Prisma SD-WAN portal and generate a token for the appropriate model.

STEP 1 | Log in to the Strata Cloud Manager, select **Settings** > **ION License Management** > **Manage Tokens**.

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

STEP 2 | Select **Create Token** to generate a new token.

Single-use or Multi-use tokens can be generated through the Prisma SD-WAN 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.



STEP 3 | Copy the **ION Key** and **Secret Key** that will be used during the KVM deployment.

The ION Key and Secret Key are mapped to the values of **ion_key** and **secret_key** in the NFV environment.

For example, {**token_id**: 14915310801150069, **ion_key**: 59e66a2f-74f9-4313-a544-724ac6b2136e, **secret_key**: 89dbf1472385ca326395771e16b17a3a64e6958c}

Prisma SD-WAN to an NFV Environment Orchestration Deployment

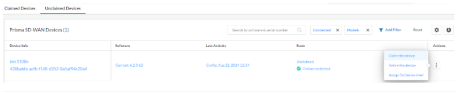
Prisma SD-WAN supports the deployment of virtual IONs to NFV environments using orchestration/automation. There are a multitude of Orchestration platforms in use by customers, with differing capabilities and integrations. The key requirements for an orchestration platform when implementing Prisma SD-WAN inside the NFV environment consist of the ability to pass metadata to the virtual ION device such as the ION Key and the Secret Key.

Ensure to have provisions for NFV/ION console access in event of provisioning / deployment issues.

Claim the ION Device and Assign to a Site

After the ION device successfully boots up, as long as it can connect to the Prisma SD-WAN controller, it will show up as **Unclaimed: Online** under **Workflows** > **Prisma SD-WAN Setup** > **Devices** > **Unclaimed Devices**. The ION device can take up to 10 minutes to show up in the Controller.

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



Select **Workflows** > **Prisma SD-WAN Setup** > **Data Centers** > **Add Site**.

1. On the General tab, enter basic information for the **Site NameCity** and **Country** for the site and click **Next** to proceed to configure circuits for the site.

   Complete Site Name and Address (Using address search is recommended).
2. On the Circuits tab, click **Add Circuits** to add Internet Circuits and Private WAN Circuits.

   By default, there are a few pre-defined configure circuits in the system that you may use when you configure the site. You can edit these labels or rename any of the remaining categories through Circuit Categories under Stacked Policies.
3. On the Devices tab, select **Assign Devices** and select from the available devices to assign or **Create Device Shells** to create up to 2 Device Shells to pre-provision and assign to the Data Center Site depending on your requirement. Click **Save & Exit**.

   You can view the summary of the newly added data center.

   The ION device and the site are now ready to be configured just like any other physical ION device.

Deploy Prisma SD-WAN Manually to an NFV or KVM Host

The steps below go through the deployment of the above example topology using **virt-install** and **virsh utilities**, but your KVM management tool of choice could be used to deploy the virtual machine as well.

STEP 1 | Upload the provided **qcow** image to the KVM host.

STEP 2 | Prepare the host by creating the appropriate interfaces to bind the ION virtual machine interfaces to the physical interfaces of the host.

1. The following example command sequence binds bridge br0 to the eth0 physical interface of the host.
   1. ip link add name br0 type bridge
   2. ip link set br0 up
   3. ip link set eth0 up
   4. ip link set eth0 master br0
2. Repeat the steps for each interface and Layer 3/bridge (br1, br2,b3, eth1, eth2, and eth3).

STEP 3 | Execute the **virt-install** command with the following options set:

1. **-name**=the name of the virtual machine.
2. **-vcpu**=the vCPU requirement for the model as listed in the vCPU table.
3. **-memory**=the memory requirement for the model as listed in the vCPU tabletable.
4. **-disk**=the location of the **qcow** image on the KVM host.
5. **-network**=reference the virtual interfaces to attach to this VM. Specify at a minimum 3 for data center deployments and 4 for branch deployments.

```
virt-install --name 3102v-kvm-1 --vcpus 2 --memory 8192 --
disk /var/lib/libvirt/images/3102v-kvm.qcow2 --import --
network bridge=br0,model=e1000 --network bridge=br1,
model=e1000 --network bridge=br2,model=e1000 -- network
 bridge=br3,model=e1000
```

6. **-host-device**=reference the SR-IOV interfaces to attach to this VM.

```
virt-install --name 3102v-kvm-1 --vcpus 2 --memory
 8192 --disk /var/lib/libvirt/images/3102v-kvm.qcow2
 --import --network bridge=br0,model=e1000 --network
 bridge=br1,model=e1000 --network bridge=br2,
model=e1000 --import --host-device 45:0a.0
```


STEP 4 | Connect to the virtual console of the running VNF with **virsh console <vm name>** and run the Virtual Form Factor setup wizard.

Example output:

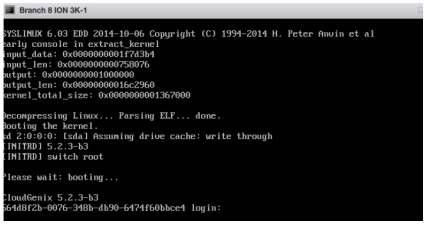
```
Current Hardware: CPU count: 2(None) Memory count: 8G Disk
 capacity: Unknown Network devices: 4
Select an ION model: 1)ion 3102v2)ion 3104v3)ion 3108v4)ion
 7108vChoose a Number or (Q)uit: 2 CPU: Passed (needed 2)
 Memory: Passed (needed 8.0G) Disk: Could not verify (needs
 40.0G) Network: Passed (needed 4) Select an item to modify,
 or submit config: 1)Model : ion 3102v 2)ION Key : 3)Secret
 Key :4)Controller 1 : Controller - DHCP 5)Port 1 : Disabled/
Unused 6)Port 2 : Disabled/Unused 7)Port 3 : Disabled/Unused
 8)Port 4 : Disabled/Unused 9)Port 5 : Disabled/Unused 10)Port
 6 : Disabled/Unused 11)Port 7 : Disabled/Unused 12)Port 8 :
 Disabled/Unused 13)Port 9 : Disabled/Unused 14)Submit and
 restartChoose a Number or (Q)uit: 2 Enter ION Key[None]: 2e4606d5-
da92-4376-98c3-cbc08fcee8a5 Select an item to modify, or submit
 config: 1)Model : ion 3102v 2)ION Key : 2e4606d5-da92-4376-98c3-
cbc08fcee8a5 3)Secret Key :4)Controller 1 : Controller - DHCP
 5)Port 1 : Disabled/Unused 6)Port 2 : Disabled/Unused 7)Port
 3 : Disabled/Unused 8)Port 4 : Disabled/Unused 9)Port 5 :
 Disabled/Unused 10)Port 6 : Disabled/Unused 11)Port 7 : Disabled/
Unused 12)Port 8 : Disabled/Unused 13)Port 9 : Disabled/Unused
 14)Submit and restartChoose a Number or (Q)uit: 3 Enter ION
 secret[None]: 3aca3f3cbae4792d7ca30c4841f71bf8e246e65c Select
 an item to modify, or submit config: 1)Model : ion 3102v
 2)ION Key : 2e4606d5-da92-4376-98c3-cbc08fcee8a5 3)Secret
 Key : 3aca3f3cbae4792d7ca30c4841f71bf8e246e65c4)Controller 1 :
 Controller - DHCP 5)Port 1 : Disabled/Unused 6)Port 2 : Disabled/
Unused 7)Port 3 : Disabled/Unused 8)Port 4 : Disabled/Unused
 9)Port 5 : Disabled/Unused 10)Port 6 : Disabled/Unused 11)Port 7 :
 Disabled/Unused 12)Port 8 : Disabled/Unused 13)Port 9 : Disabled/
Unused 14)Submit and restartChoose a Number or (Q)uit: 7 Port 1:
 1)Role : Disable2)Cancel Port changes3)Apply and returnChoose
 a Number or (Q)uit: 1 Select Port Role: 1)Internet facing port
 (PublicWAN)2)Bypass Port Pair 1 (WAN Port)3)Bypass Port Pair 1
 (LAN Port)4)Bypass Port Pair 2 (WAN Port)5)Bypass Port Pair 2
 (LAN Port)6)Bypass Port Pair 3 (WAN Port)7)Bypass Port Pair 3
 (LAN Port)8)Bypass Port Pair 4 (WAN Port)9)Bypass Port Pair 4
 (LAN Port)10)Disabled/UnusedChoose a Number or (Q)uit: 1 Port 1:
 1)Role : PublicWAN 2)Config via : DHCP3)Cancel Port changes4)Apply
 and returnChoose a Number or (Q)uit: 2 Select Port Configuration:
 1)DHCP2)Static ConfigurationChoose a Number or (Q)uit: 2
 Port 1: 1)Role : PublicWAN 2)Config via : STATIC3)Address :
 0.0.0.0/0 4)Gateway : 0.0.0.0 5)DNS 1 : 0.0.0.0 6)DNS 2 :
 0.0.0.0 7)Cancel Port changes8)Apply and returnChoose a Number
 or (Q)uit: 3 Enter Interface IP/mask[0.0.0.0/0]: 172.22.2.223/23
 Port 1: 1)Role : PublicWAN 2)Config via : STATIC3)Address :
 172.22.2.223/23 4)Gateway : 0.0.0.0 5)DNS 1 : 0.0.0.0 6)DNS 2 :
 0.0.0.0 7)Cancel Port changes8)Apply and returnChoose a Number
 or (Q)uit: 4 Enter gateway[0.0.0.0]: 172.22.2.1 Port 1: 1)Role :
 PublicWAN 2)Config via : STATIC3)Address : 172.22.2.223/23
 4)Gateway : 172.22.2.1 5)DNS 1 : 0.0.0.0 6)DNS 2 : 0.0.0.0
 7)Cancel Port changes8)Apply and returnChoose a Number or
```



```
 (Q)uit: 5Enter DNS address[0.0.0.0]: 8.8.8.8 Port 1: 1)Role :
 PublicWAN 2)Config via : STATIC3)Address : 172.22.2.223/23
 4)Gateway : 172.22.2.1 5)DNS 1 : 8.8.8.8 6)DNS 2 : 0.0.0.0
 7)Cancel Port changes8)Apply and returnChoose a Number or (Q)uit:
 8 Select an item to modify, or submit config: 1)Model : ion
 3102v 2)ION Key : 2e4606d5-da92-4376-98c3-cbc08fcee8a5 3)Secret
 Key : 3aca3f3cbae4792d7ca30c4841f71bf8e246e65c4)Controller 1 :
 Controller - DHCP 5)Port 1 : Disabled/Unused 6)Port 2 : Disabled/
Unused 7)Port 3 : PublicWAN — STATIC 8)Port 4 : Disabled/Unused
 9)Port 5 : Disabled/Unused 10)Port 6 : Disabled/Unused 11)Port
 7 : Disabled/Unused 12)Port 8 : Disabled/Unused 13)Port 9 :
 Disabled/Unused 14)Submit and restartChoose a Number or (Q)uit:
 14 WARNING! After this configuration is submitted, all hardware
 will be signed, logged, and permanently tied to the ION Key/Secret
 Key in the Prisma SD-WAN Cloud Controller. WHAT THIS MEANS is that
 hardware cannot be added/removed (disks, network cards) after this
 'SUBMIT' function. If any hardware changes are required beyond
 this 'SUBMIT', the ION will need to be re-deployed with a new ION
 Key and Secret Key. If there is a need to add or remove hardware,
 please answer 'N' below and shut down the ION and make the changes
 now. Submit these changes now?[N]: Y
```

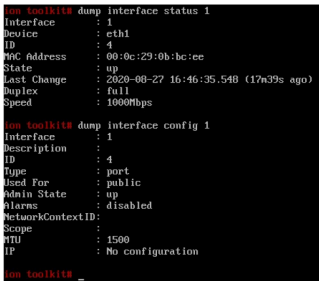

Configure Static IP Addressing for ION devices in Virtual Environments

With virtualized workload environments, Prisma SD-WAN expects IP addressing via DHCP for all interface types (Controller, Public, and Private LAN interfaces). If the Prisma SD-WAN ION device requires a static IP address assignment, you can configure the ION device once it boots up into the virtualization environment. In the subsequent examples, we will configure the ION device's Port 1 for internet connectivity which will then allow connection to the controller.



You will need to log in to the ION device with the unclaimed device credentials. These will be provided by your Prisma SD-WAN team.

STEP 1 | Log in to the ION device and verify that the interface did not receive an IP address.

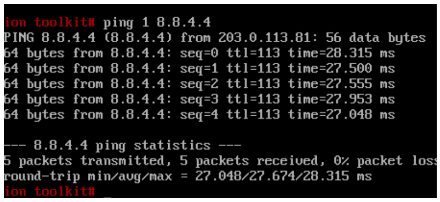


STEP 2 | To configure the Port 1 on the ION device, you can configure the port based on the appropriate IP addressing for your environment.

```
ion toolkit# config interface 1 ip static address=203.0.113.81/30
 gw=203.0.113.82 dns=8.8.4.4
```

Once configured, verify that the appropriate port is now configured correctly.

STEP 3 | Test the interface for internet connectivity, which will then allow the ION device to contact the controller and show up as an unclaimed device.



Metadata Missing or Incorrect Information

Metadata Missing

In some situations, metadata that needs to be passed to the ION device during its instantiation in a virtualization may not be present when the device boots. Also, in the instance of a manual installation (i.e. KVM), the metadata needs to be entered manually.The primary metadata that gets passed to the ION device during its instantiation process is:

- ION Type
- ion_key
- secret_key

If an orchestration platform instantiated the ION device, and the instantiation did not request/accept the basic setup parameters listed above, then rebuild the ION device.

Metadata Incorrect

After instantiating an ION either through automation/orchestration or manually as in the case of KVM, there may be an instance where the metadata was entered incorrectly. In either scenario, if metadata is entered, and the ION device is booted and is at the login prompt (as seen from the console), the virtual ION device must be destroyed and recreated.When the **ion_key** and **secret_key** are combined with the creation of the virtual ION device, they are used to digitally sign the ION device. Due to this incorrect signing which cannot be changed, the ION device will be unusable and will need to be recreated.

