paloalto TECHDOCS

Virtual ION on VMware 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

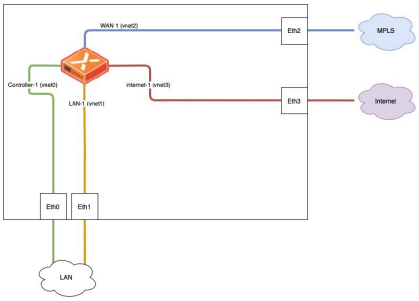
Prisma SD-WAN Virtual ION VMware Deployment

The Prisma SD-WAN Virtual ION on VMware Deployment Guide introduces the essential concepts and components for licensing, and installation/deployment of a Prisma SD-WAN Virtual Form Factor device within a VMware environment.

Prisma SD-WAN Virtual ION Deployment on VMware Prerequisites

The Prisma SD-WAN Virtual ION on VMware Deployment Guide focuses specifically on VMware's vCenter and ESXi with their associated configuration and deployment details. This guide provides instructions for deploying Prisma SD-WAN ION devices to a host server running VMware's ESXi. It is intended for network administrators who plan to extend the Prisma SD-WAN SD-WAN fabric to sites that leverage ESXi as the virtualization platform of choice for their VNFs, thereby allowing administrators to align their WAN policies with business intent for performance, security, and compliance.

A virtual ION device can be deployed to a VMware host and assigned to either a branch or data center type of site. The design and deployment considerations are different between a branch site and a data center site. The VM deployment options such as the number of interfaces needed for the VM, the way in which the virtual network interfaces are bound to the physical NICs, etc. will vary based on these requirements. For legacy deployments using Layer 2 bypass or for H/A deployments with virtual inline pairs, special attention needs to be given to allow MAC Spoofing, Forged Transmits, and Promiscuous Mode on a vSwitch/Port Group within VMware. 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 following requirements must be met:

- The Virtual ION device must be deployed on a system with AES-NI capable CPU.
- The Virtual ION is deployed in the VMware Host
- The vMotion is not supported for the virtual ION deployment
- ESXi 6.0 and later are supported.
- vCenter 6.0 and later are supported.
- Ensure to configure correct time-settings on the VM server that hosts the Virtual ION.
- OVA Deployment supported via:
  - vCenter 6.0 and higher (vCenter web client)
  - oESXi 6.5 and higher (ESXi web client)

For more information, refer to the Virtual Form Factor Data Sheet. Determine the Model type *and sizing / role to prior to implementation.*

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

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 to a VM during OVA deployment.

STEP 4 | Assign tokens.

The ION device key and secret key are used when the OVA is deployed.

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

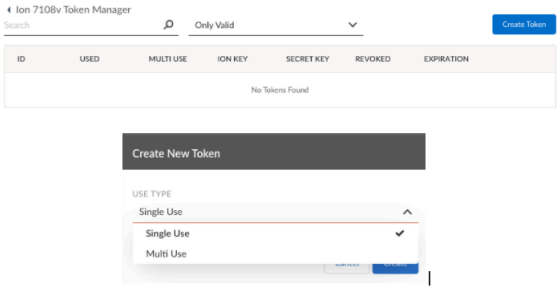
For virtual form factors in Prisma SD-WAN, the instance(s) are bound to an authorization token. This provides a set of controls to prevent unauthorized virtual devices to be added to an environment. Once the Prisma SD-WAN account team or support team has confirmed that the licenses have been allocated 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**.

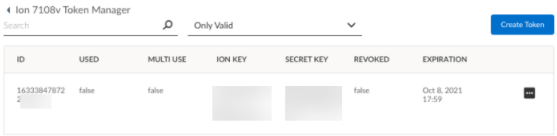
*Only a **Super User** role can generate the authorization tokens.*

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 you use during the virtual appliance deployment.



Copy the values of **ION Key** and **Secret Key** to paste into the deployment template properties.

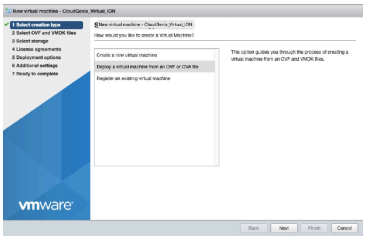
Prisma SD-WAN to a VMware Host Deployment

Prisma SD-WAN will provide the OVA images for the platforms that were purchased. VFF can be deployed using the OVA images and token keys generated from the portal. VFF is deployed using vCenter Web Client or the ESXi Web Client (ESXi 6.5 and higher).

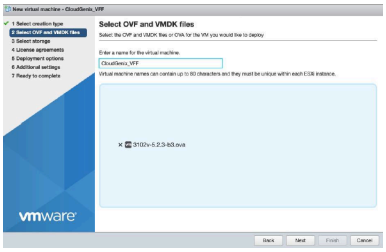
Deploy Prisma SD-WAN to a VMware Host

Prisma SD-WAN will provide the OVA images for the platforms that were purchased. VFF can be deployed using the OVA images and token keys generated from the portal. VFF is deployed using vCenter Web Client or the ESXi Web Client (ESXi 6.5 and higher). The following workflow(s) are shown using the ESXi Web Client.

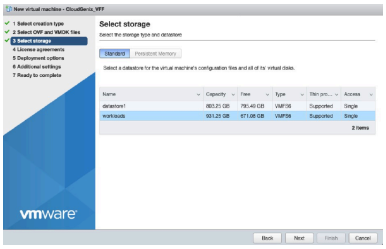
STEP 1 | From the web client, choose **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



STEP 2 | Select the OVA file and provide a name for the virtual machine.

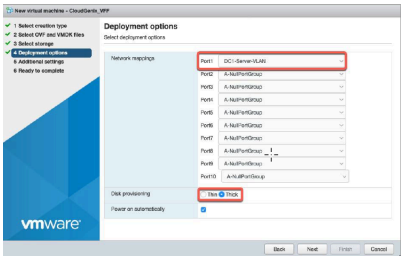


STEP 3 | Name the VM and place the VM in a desired storage location.



STEP 4 | Select a deployment option.

The best practice is to thick provision the disks, although thin provision could also be used.

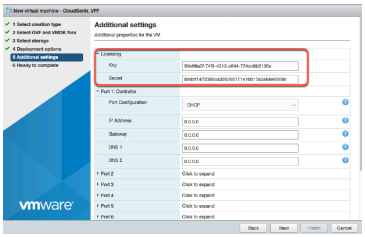


STEP 5 | Configure additional settings.

1. Add tokens (**ion_key** and **secret_key**) copied from the **License Management** screen on the controller.
2. At a minimum, assign port 1 (Controller port) to a vSwitch port profile that will be able to communicate with the controller.

   The port profile should allow for the VFF to request and obtain a DHCP address. Optionally, you can also assign the other ports to an appropriate vSwitch port profile.
3. Leave the controller port setting at the default value to obtain an IP address via DHCP.

   Port configuration can be set to Static IP, but the VM will need to be accessed and controller port configured via the Device Toolkit to bring up communications to the Prisma SD-WAN controller.
4. (Optional) Configure the other ports as per their specific roles.



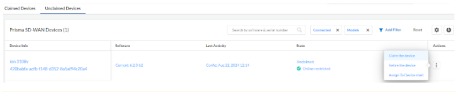
STEP 6 | Click **Finish** to complete the deployment and power on the VFF.

Once imported and started, the device should now show up in the controller as **unclaimed**. Claim the device and assign to a site to configure.

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.

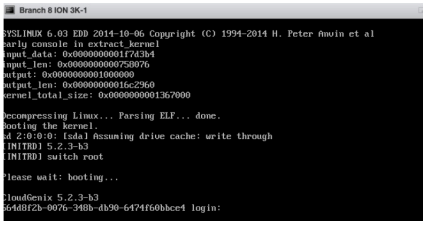
   By default, there are a few pre-defined configure circuits in the system that you may use when you configure the site. You can edit these labels or rename any of the remaining categories through Circuit Categories under Stacked Policies.
3. On the Devices tab, select **Assign Devices** and select from 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.

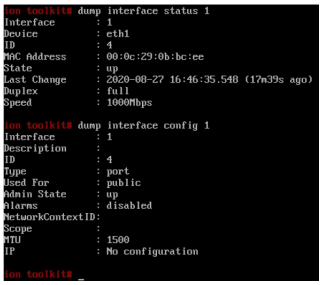
Configure Static IP Addressing for ION devices in Virtual Environments

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.

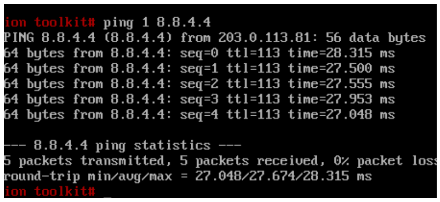


STEP 2 | To configure the Port 1 on the ION device, you can configure the port based on the appropriate IP addressing for your environment.

```
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.

