**OmniVista 2500 NMS
Version 4.7R1**

**Remote Access Point and
VPN VA Installation Guide**

Alcatel·Lucent
Enterprise

October 2022

Revision A

Part Number 060831-10

Table of Contents

Remote Access Points and VPN Tunnel Components

A Remote Access Point (RAP) is an AP with a management tunnel and a data tunnel to a remote OmniVista Enterprise (OVE) Server. An OmniVista Cirrus (OVC) Managed AP is technically not considered a RAP since there are no Management VPN Server details to be configured. An OVC managed AP already uses an OpenVPN connection for Management communications with a VPN Server in the OVC Cloud infrastructure. However, it is possible that an OVC Managed AP might need a Data VPN Tunnel to a VPN Server in the Enterprise.

Components of the solution include:

- Stellar APs
- OVE/OVC
- RAP VPN Server for Data VPN and/or Management VPN
- Gateways and routers at customer network.

VPN for Management and Data (OVE Managed APs)

Typically, a local AP in the Enterprise learns its OV IP address via DHCP option 138. A local AP in the Enterprise is managed by OV in the Enterprise directly. An AP at a remote site cannot be managed by OV in the enterprise as it will not be reachable directly. The connection and communication need to happen via a VPN tunnel. An out-of-the-box AP that is not supplied with DHCP option 138 will first register with the OVC Activation Server allowing it to be configured as a RAP.

If the RAP is OVE managed:

1. The first connection, out-of-the-box, is to the OVC Device Registration Server. It retrieves the setup parameters for RAP including the OVE IP to which it will connect.

2. The keys and parameters are exported to the RAP VPN Server at corporate HQ.

3. The RAP then establishes a Wireguard VPN tunnel over which it connects to be managed by OVE.

4. A Data VPN tunnel must be setup in OVE between the RAP and the VPN server. The tunnel keys and parameters can be exported to the VPN server at corporate HQ.

5. Once the Data VPN tunnel is established it can be used to tunnel the required end user services to corporate HQ.

Key points when RAP is managed by OVE:

- The OVC Device Catalog provides options to register the AP as a RAP. This is required to setup the Management VPN to the RAP Virtual Appliance (VA) appliance located in corporate HQ. The administrator should register the AP as a RAP, which allows for pre-provisioning the RAP VPN VA public IP/OVE on-premise IP/Security Keys etc.
- Data VPN configuration is done from OVE on the managed AP. This is required to setup the Data VPN tunnel to the RAP VA appliance located in corporate HQ.
- WLAN Service configuration is done from OVE that is managing the RAP.

VPN for Data Only (OVC Managed APs)

An OVC managed AP can be configured for an encrypted Data VPN Tunnel to a remote VPN Server. The AP needs to be setup with the Wireguard VPN Server endpoint details allowing the AP to tunnel data traffic to the VPN server at corporate HQ.

If RAP is to be managed by OVC.

1. The first connection out-of-the-box for the AP is to the OVC Device Registration Server to confirm it is an OVC registered AP.

2. The AP establishes and OpenVPN connection to be managed by OVC.

3. A Data VPN tunnel from the RAP is setup on the OVC, and the tunnel keys and parameters can be exported to the VPN server at corporate HQ.

4. Once the Data VPN tunnel is established, it can be used to tunnel the required end user services to corporate HQ.

Key points when a RAP is managed by OVC:

- The administrator registers the AP in the OVC Device Catalog as a standard OVC managed AP. No Management VPN is required as the AP is managed by OVC.
- Data VPN configuration is done from OVC on the managed AP. This is required to setup the Data VPN tunnel to the RAP VA appliance located in corporate HQ.
- WLAN Service configuration is done from OVC that is managing the AP.

Prerequisites

- ESXi versions 6.5, 6.7, and 7.0.2 are supported (ESXi 5.5 is **not** supported).
- Hyper-V 2016, 2019, and 2022
- Supported Stellar RAP version is AWOS 4.0.1.44 and higher.
- OmniVista 2500 version 4.6R2 to 4.7R1 is supported.

Network Topology

Within this document we will use the following network topology:

Part No. 060831-10, Rev. A
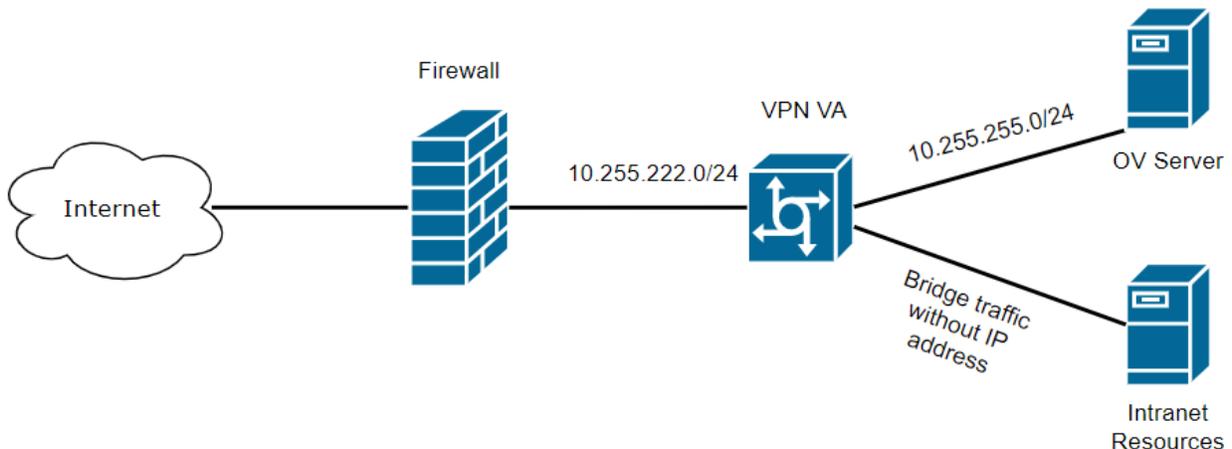
Remote Access Points and VPN Tunnel Configuration

You can configure an offsite, RAP that can be managed by your local OVE installation through a VPN Tunnel. Remote APs are added to the Device Catalog using a "Freemium version of OmniVista Cirrus, the cloud-based version of OmniVista. You then must deploy a VPN Tunnel Server Virtual Appliance (VPN VA).

When the AP(s) is connected to the network, it automatically contacts the OmniVista Cirrus Activation Server, which downloads the necessary IP and VPN configurations and the AP is added to the List of Managed Devices and manageable by your local OVE installation. The following sections detail the steps required to deploy RAPs:

1. Creating an OmniVista Cirrus Freemium Account

2. Adding Remote APs to the Device Catalog

3. Deploying/Configuring the VPN Tunnel Server

Note that when you add Remote APs to the Device Catalog (Step 2) you will need to enter information about the VPN Server, which is configured in Step 3. Determine your VPN Server configuration **before** starting.

> **Note:** The Remote AP feature is supported on Stellar APs running AWOS 4.0.0.40 and higher. For the latest features, AWOS 4.0.1.44 and higher is required.

> **Note**: Tagged and untagged traffic can be tunneled through VPN tunnels.

Creating an OmniVista Cirrus Freemium Account

OmniVista Cirrus offers a "Freemium" account which is used to add Remote APs. Follow the steps below to create an OmniVista Cirrus "Freemium" Account.

1. Go to the OV Registration Portal.
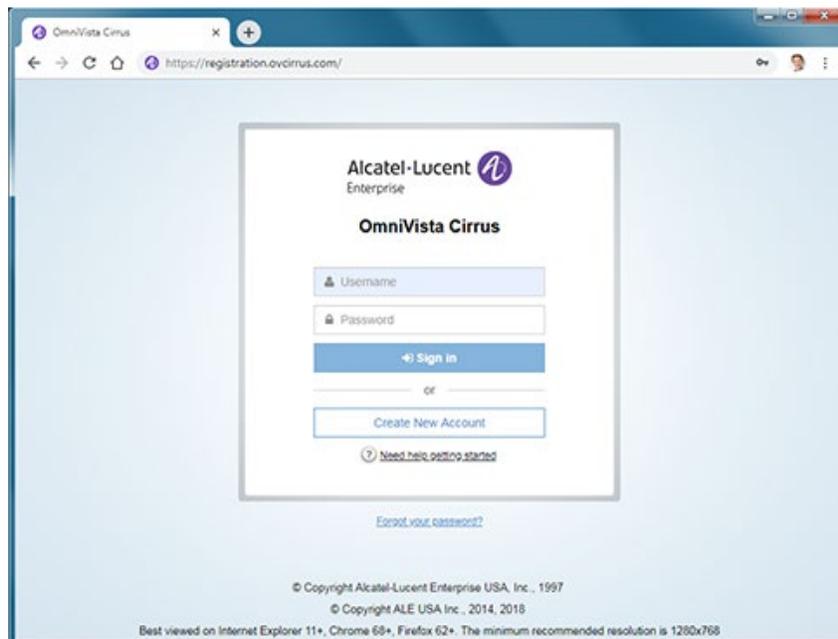
2. Click on the **Create a New Account** button. The Create New Account Screen will appear.

3. Complete the fields. Fields marked with an asterisk (*) are required. At the bottom of each screen, click **Continue** to move to the next screen. Note that the username you enter will be used to log into OmniVista Cirrus once your account is created. Also note that the e-mail address you enter will be used to verify your account and complete the process. When you have completed and reviewed all of the fields, accept the terms and conditions and click on the **Create Account** button. A Confirmation Screen will appear.
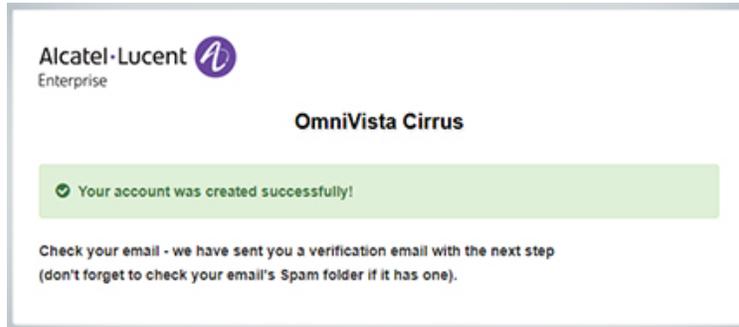
4. Go to the e-mail account you entered in Step 3 above. You will receive an e-mail from ALE USA Inc (noreply@ovcirrus.com) containing instructions and a verification link. Click on the **Go to Verify Account** link. The Set Password Screen will appear.

> **Important Note:** There is a link in the body of the email to download the required device OS software for OmniVista Cirrus. APs must be running a minimum software version of AWOS 4.0.0.44. Click on the link to download the software. If necessary, you can use this software to upgrade your devices.

5. Create and confirm your password, then click on the **Save** button. The Confirmation Screen below will appear.
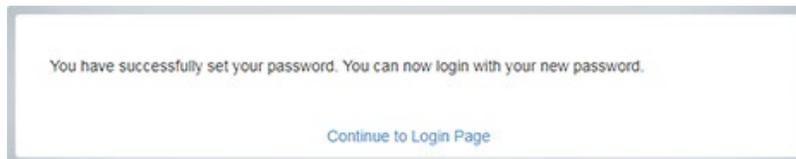
6. Click on the **Continue to Login Page** link and log into OmniVista Cirrus using the username and password you created. After successful login, the OmniVista Cirrus Freemium Dashboard will appear.
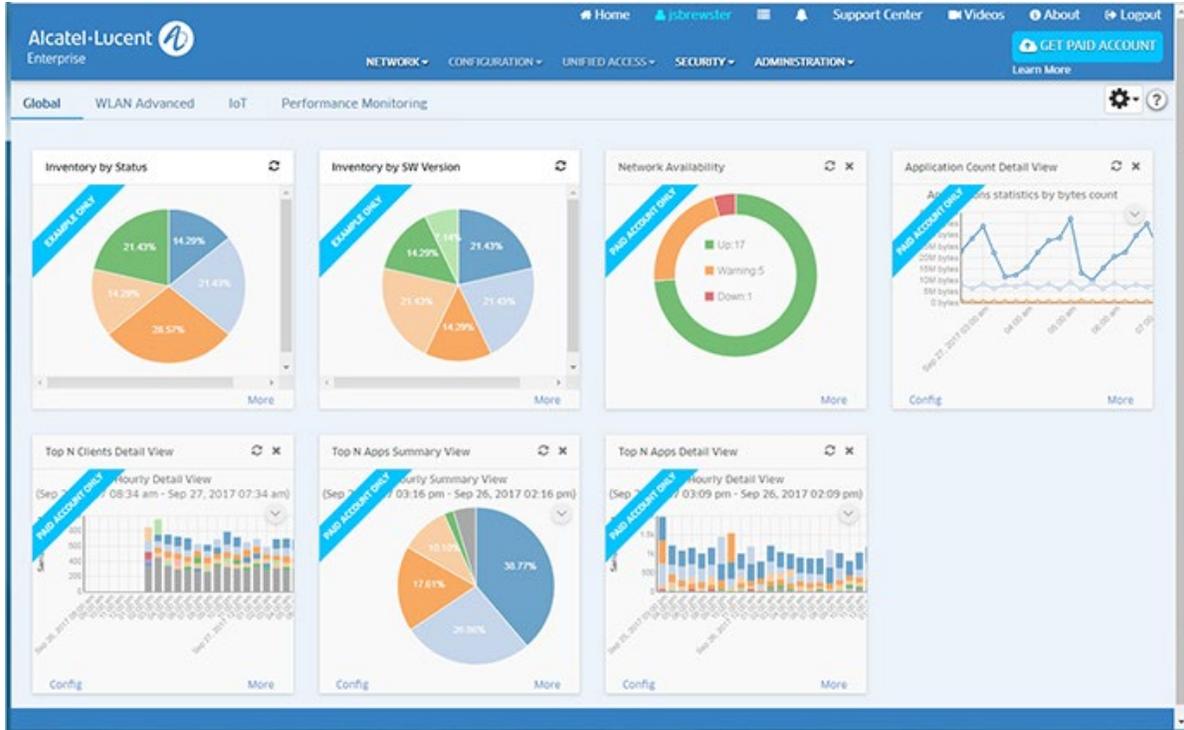
> **Note:** You will continue to log into https://registration.ovcirrus.com using the username and password you created to access your OmniVista Cirrus Freemium Account.

Adding Remote APs to the Device Catalog

Remote APs are added using the Device Catalog application. You can add APs one-at-a-time or import multiple APs at once using a .csv file.

Adding Remote APs Manually

1. Select **Network - Inventory - Device Catalog** to bring up the Device Catalog application.
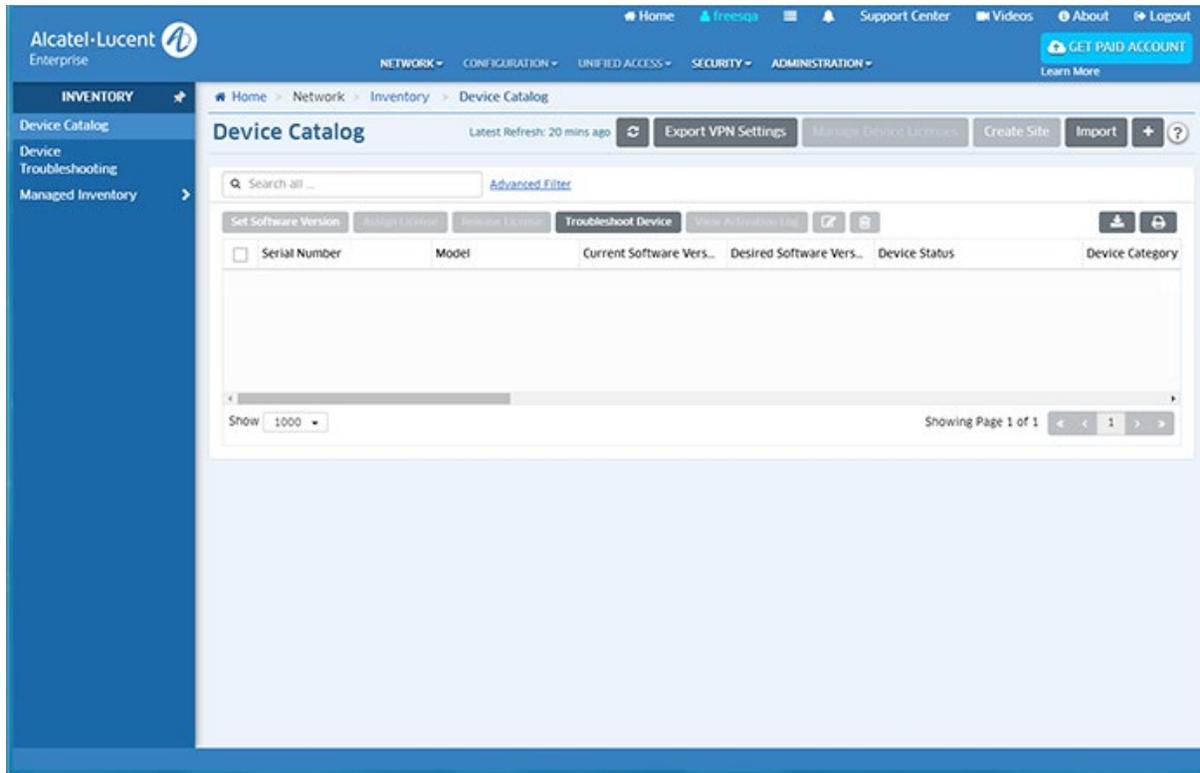
2. Click on the Add icon (**+**) in the upper-right corner of the screen to bring up the Add a Device Screen.

3. Enter the AP **Serial Number**, in the **Device Type** drop-down select **Stellar AP**, then enable the **Is this a Remote AP Field** to open the Remote AP configuration fields (shown below).

4. Complete the fields as described below, then click on the **Save VPN Settings and Create Device** button to add the AP to the Device Catalog.

- **MAC Address -** The MAC address of the AP.

- **Is This a Remote AP -** Click the slider to "Yes".

- **VPN Settings -** The VPN Tunnel configuration between the VPN Server and the OmniVista Enterprise Server. Select the **Create New VPN Settings** radio button to initially configure a Tunnel. Once you configure and save Tunnel Settings, they are saved under the VPN Settings Name and you can simply select **Choose Existing VPN Settings** to select an existing VPN configuration when adding Remote APs.

    - **VPN Settings Name -** Enter a name for the VPN configuration.

    - **Server's Public IP -** The VPN Server's Public IP address (configured on one of the interfaces when you installed the VPN VA). This is the IP address used by Remote APs to connect to the VPN Server. And this is the interface through which traffic originating from inside the Enterprise Network flows to the Remote site.

    - **Port -** The VPN Public IP Server Port.

    - **Server's VPN IP -** The VPN Server's Private IP address within the virtual network (must be in the same network as the client pool). This is the tunnel interface through which traffic originating from the Remote AP flows to reach a destination inside the Enterprise Network.

- **OmniVista Enterprise Server IP -** The IP address of the OmniVista Enterprise Server that will manage the devices.
  - **Client VPN IP Address Pool -** The range of addresses available to assign to Remote APs.
    - **IP Range -** Enter a starting and ending IP address range.
    - **Shorthand Mask -** Enter a shorthand mask for the IP Range
    - **Subnet Mask -** Enter the subnet mask for the Client VPN IP Address Pool.

Importing Multiple Remote APs

You can add multiple Remote APs at once by importing a .csv file containing the APs and any relevant information.

1. Select **Network - Inventory - Device Catalog** to bring up the Device Catalog application.
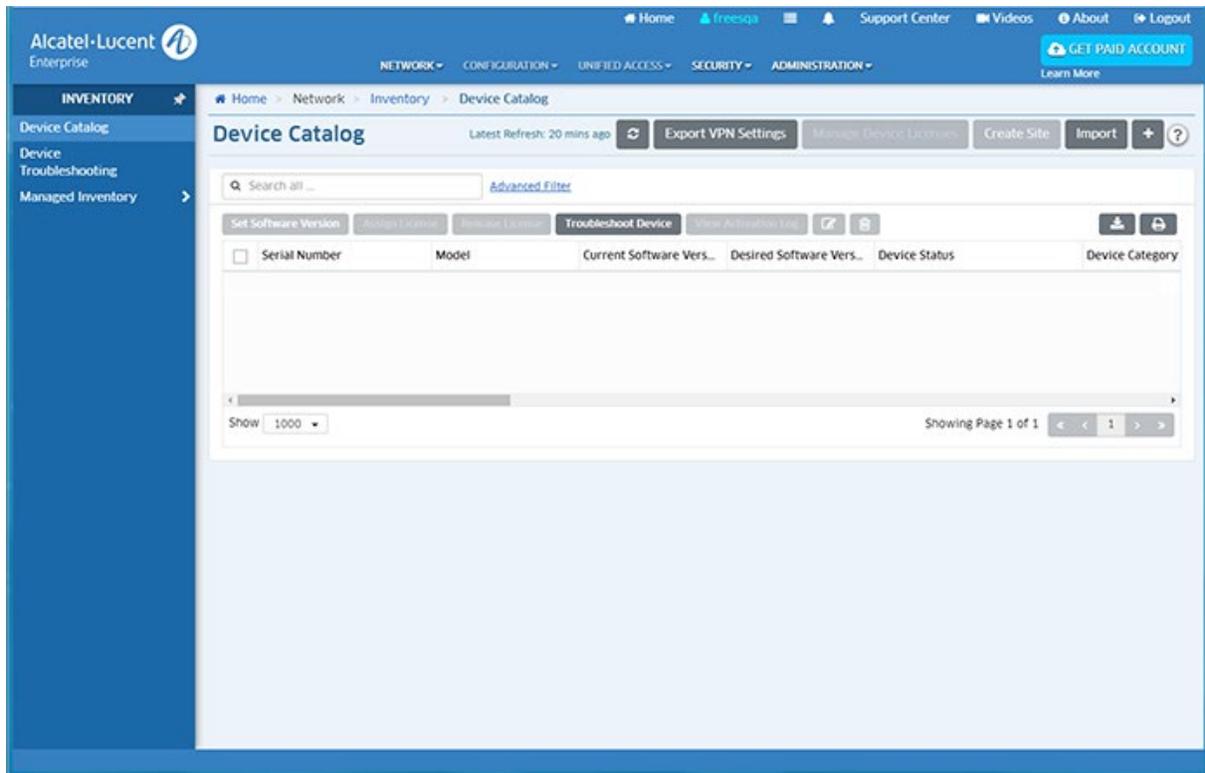
2. Click on the **Import** button in the upper-right corner of the screen to bring up the Import Devices Screen.

3. Click on the **Browse** button to locate the .csv file containing the APs, then click on the **Import** button at the bottom of the screen. The APs in the file will be imported into the Device Catalog.

If necessary, click on the **Template** button to open or download an import template file (shown below).

Modify the Template with AP Serial Numbers and any additional information you want to add. If you want to add VPN Setting information (VpnSettingName), the RAP field **must** be "TRUE". Save the file, and then go to Step 3 to import the file and add the APs to the Device Catalog.

An example of an import file for Remote APs is shown below.

Deploying/Configuring the VPN Tunnel Server

A Virtual Private Network (VPN) Virtual Appliance (VA) is required for managing Remote Access APs and securely tunneling data from devices at remote locations. The following sections details the steps for deploying and configuring a VPN VA.

Recommended VPN VA Configurations

The VPN VA and NIC configurations are based on the number of Remote APs being managed.

- **VPN VA Configuration** (Based on the number of Remote APs)
  - 1 - 100 APs - 4 vCPUs, 2GB RAM
  - 100 - 250 APs - 6 vCPUs, 4GB RAM
  - 250 - 500 APs - 8 vCPUs, 8GB RAM
  - 500 - 1,000 APs - 12 vCPUs, 16GB RAM.

    Note: Higher scale is based on CPU/Memory calculated per RAP. For deployments with more than 250 RAPs, it is recommended that you deploy a second VPN VA Server.

- **NICs - 1G vs.10G** (Based on expected throughput)

  - 10 - 20Mbps expected VPN throughput per RAP, if local breakout is serving all internet needs.

  - 20 - 100Mpbs expected VPN throughput per RAP, if all traffic is tunneled through VPN.

  - 10G NIC is standard for more than 500 APs. For increased throughput use 2 x 10G NIC (NIC Teaming).

- **NIC Teaming**

  - NIC Teaming is supported when deploying the VPN Virtual Appliance. Click here for details.

Known Limitations

- RAP VPN VA does not support redundancy.

Deploying the VPN Virtual Appliance

Deploy the VPN VA on your Hypervisor. The VA can be deployed on VMware or Hyper-V. After deploying the VA, configure the VA and complete the installation.

Deploying the Virtual Appliance on VMware

1. Download and unzip the OVF package. You will be using the OVF File and both VMDK Files (disk 1 and disk 2) for the installation. **The Zip file also contains an *.mf File. Delete the *.mf File from the folder <u>before</u> importing the files in Step 5**.

2. Log into VMware ESXi.
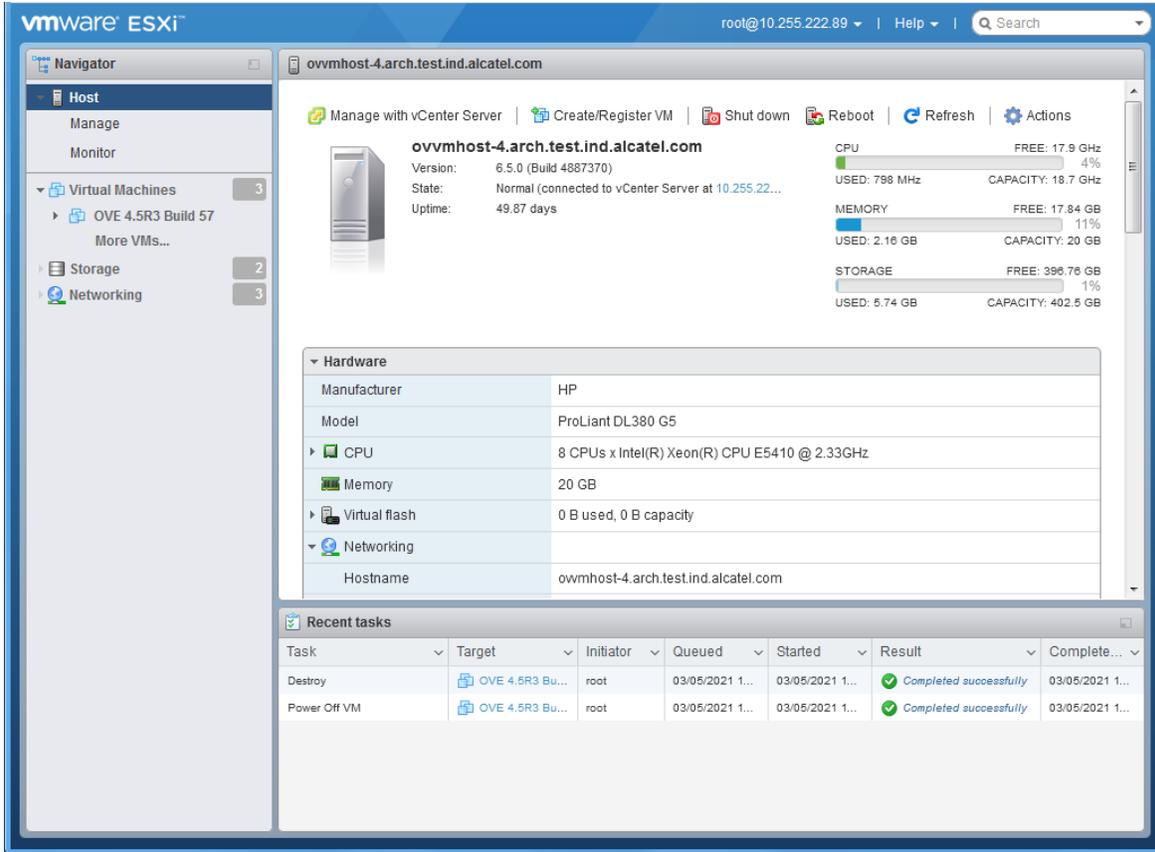
3. Select the Host on which you want to install the VPN VA and **click on Create/Register VM**. The first screen of the New Virtual Machine Wizard appears.
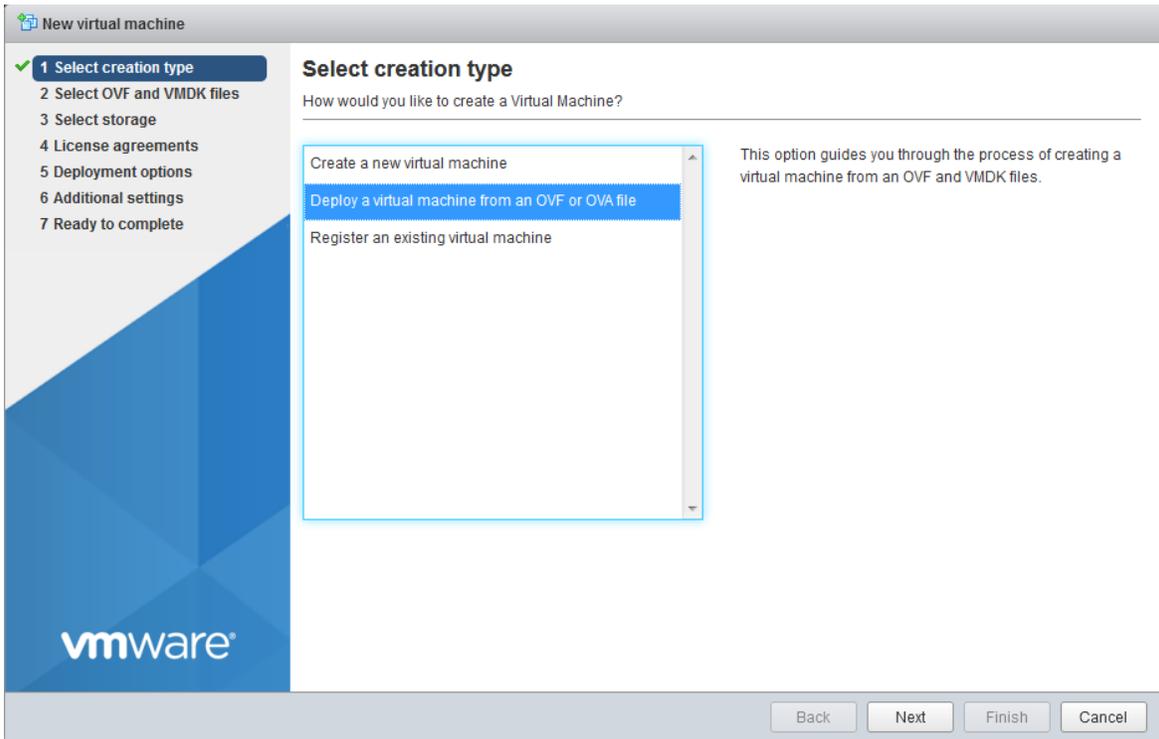
4. Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
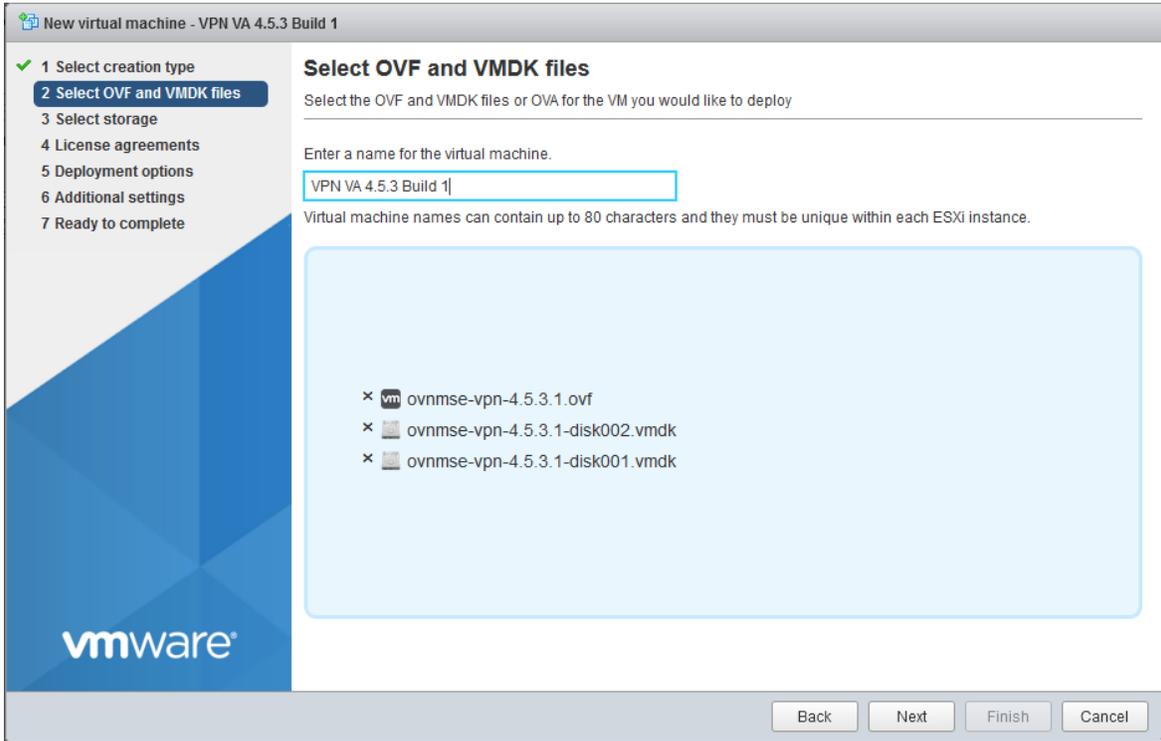
5. Enter a name for the VM (e.g., VPN VA 4.5.3 Build 1), click to locate and select the downloaded installation files (or drag the files into the window), then click **Next**. Remember, do **not** include the *.mf File; only the *ovf file and the two *vmkd Files.
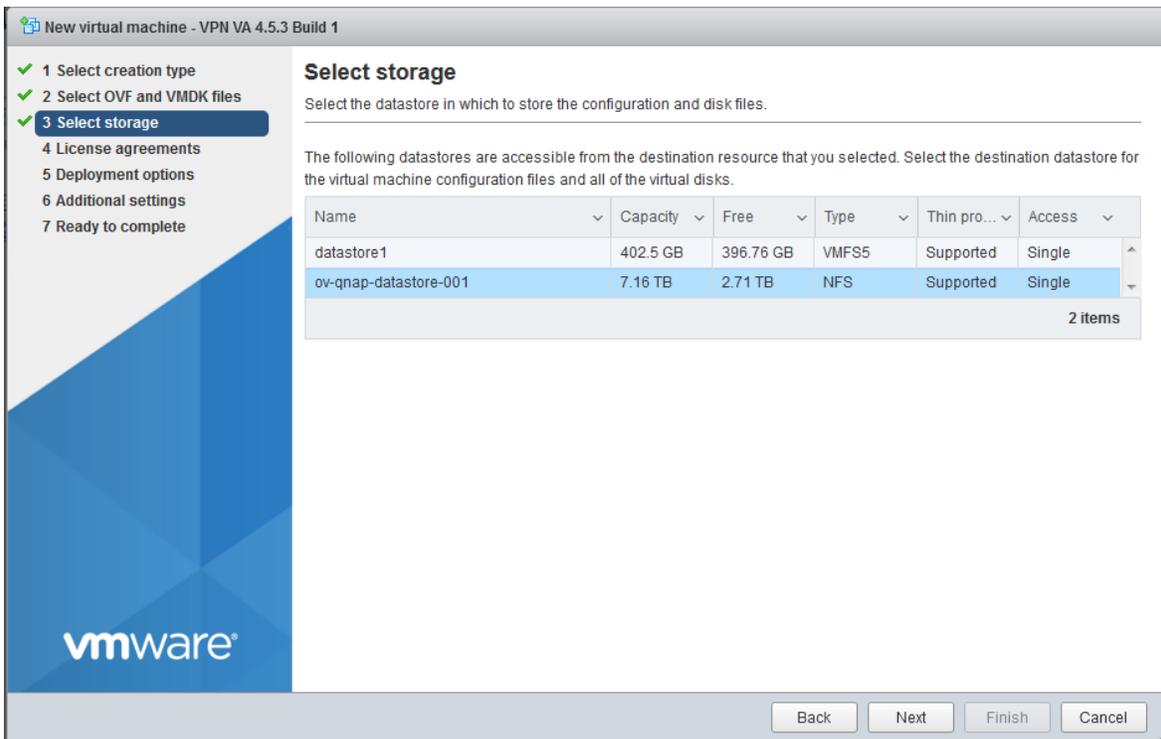
6. Select the destination storage where the template is to be deployed, then click **Next**.
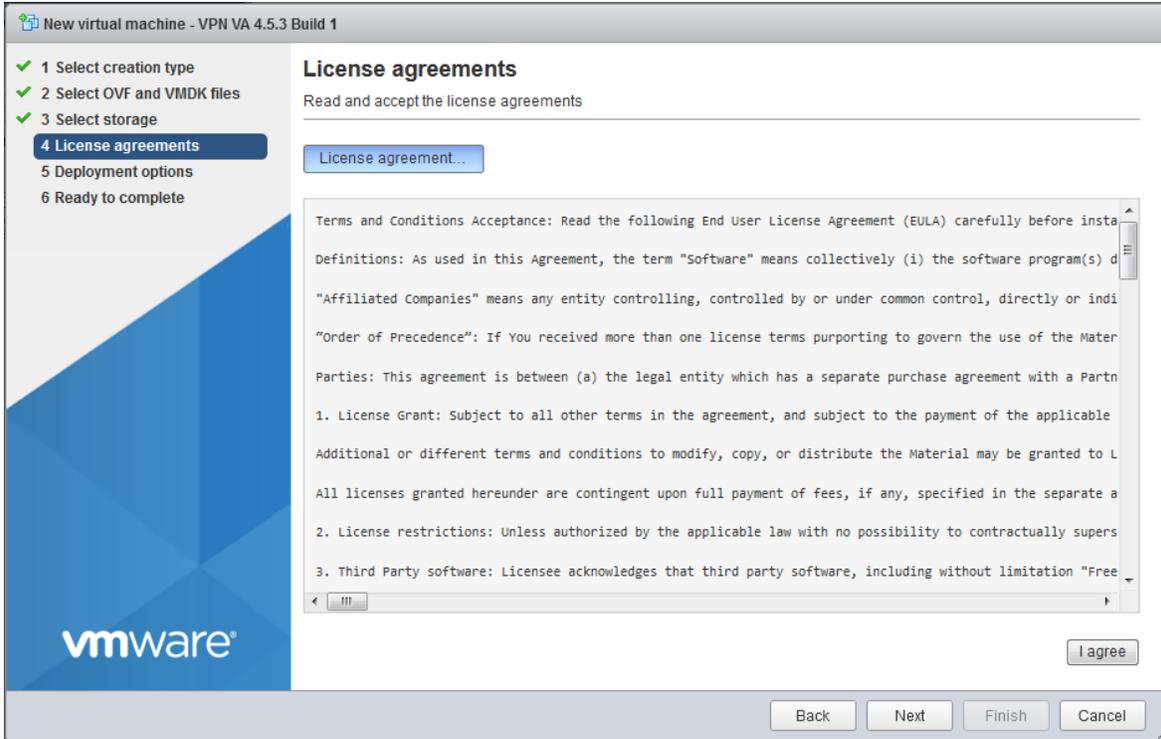
7. Review the License Agreement, click **I agree**, then click **Next**.
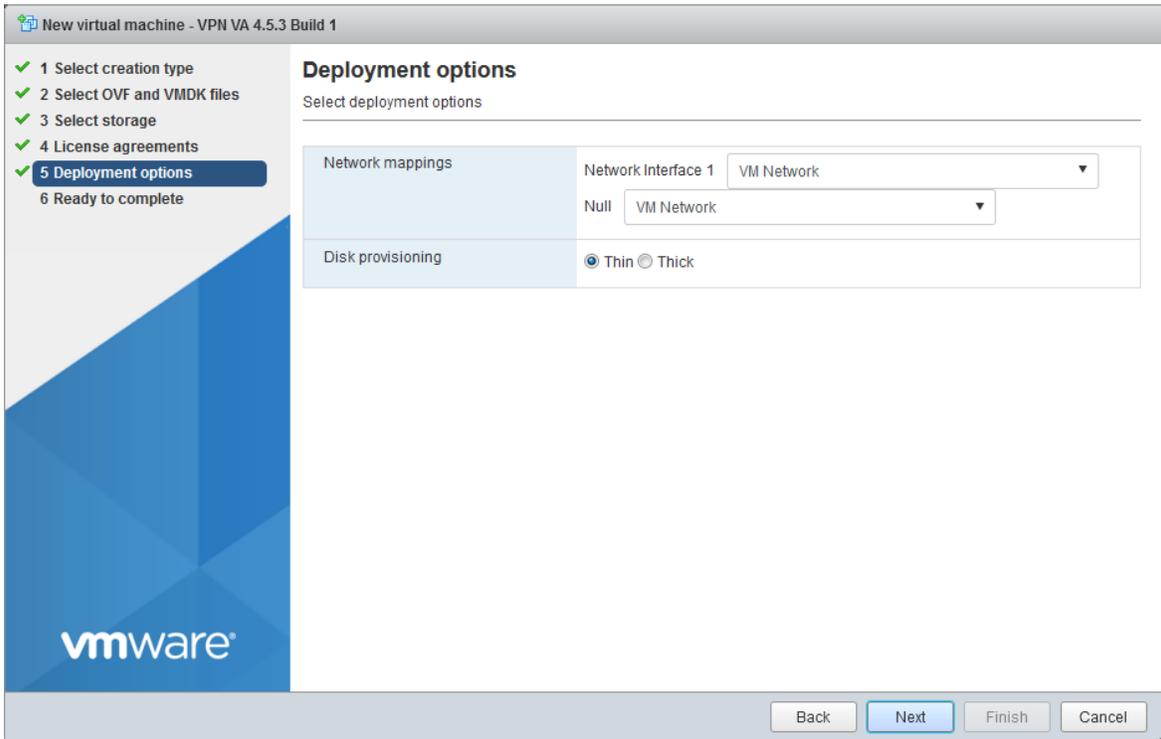
8. In the **Network mapping** field, select the Destination network that the deployed VM will use. In the **Disk provisioning** field, select **Thin**. Click **Next**.
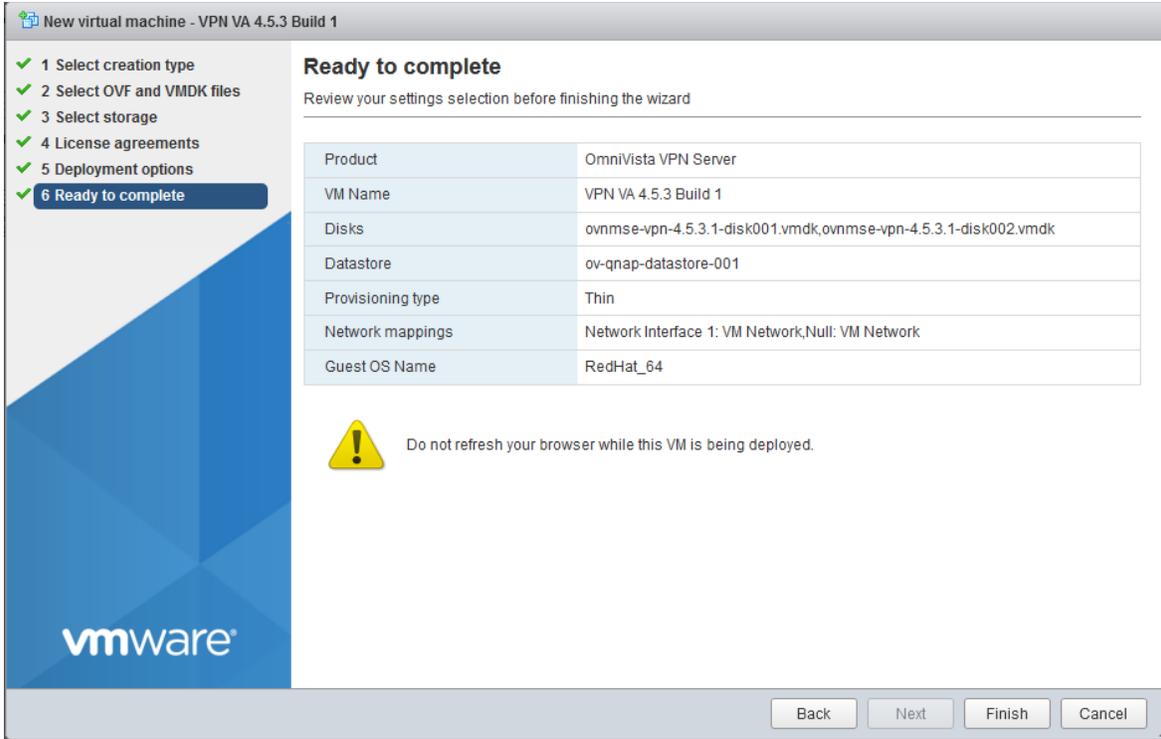
9. Review the configuration and click **Finish**. You will be returned to the main screen with the deployment progress displayed in the **Recent tasks** table.
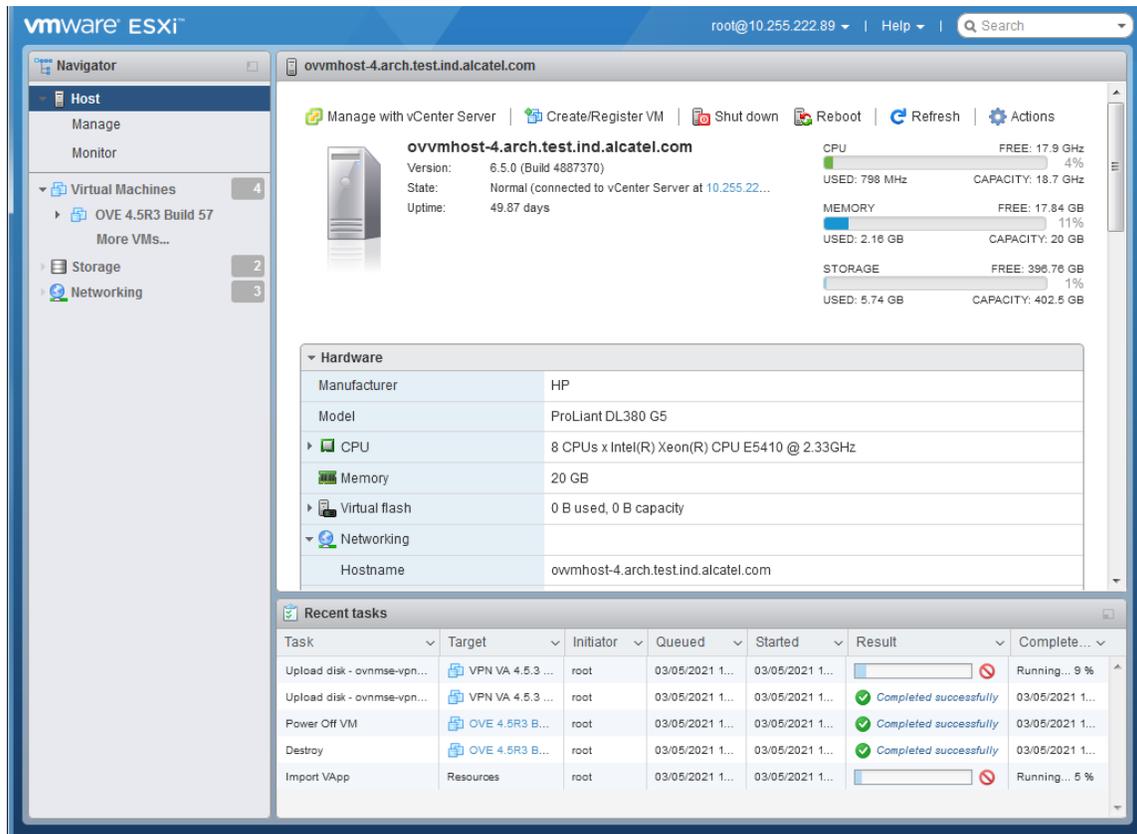
10. When the installation is complete (indicated by all three files showing "Completed Successfully" in the Result column of the Recent tasks table), click on **Virtual Machines** in the Navigator Tree on the left side of the screen to display a list of VMs. Select the VM you just deployed. Basic details for the VM are displayed, as shown below.
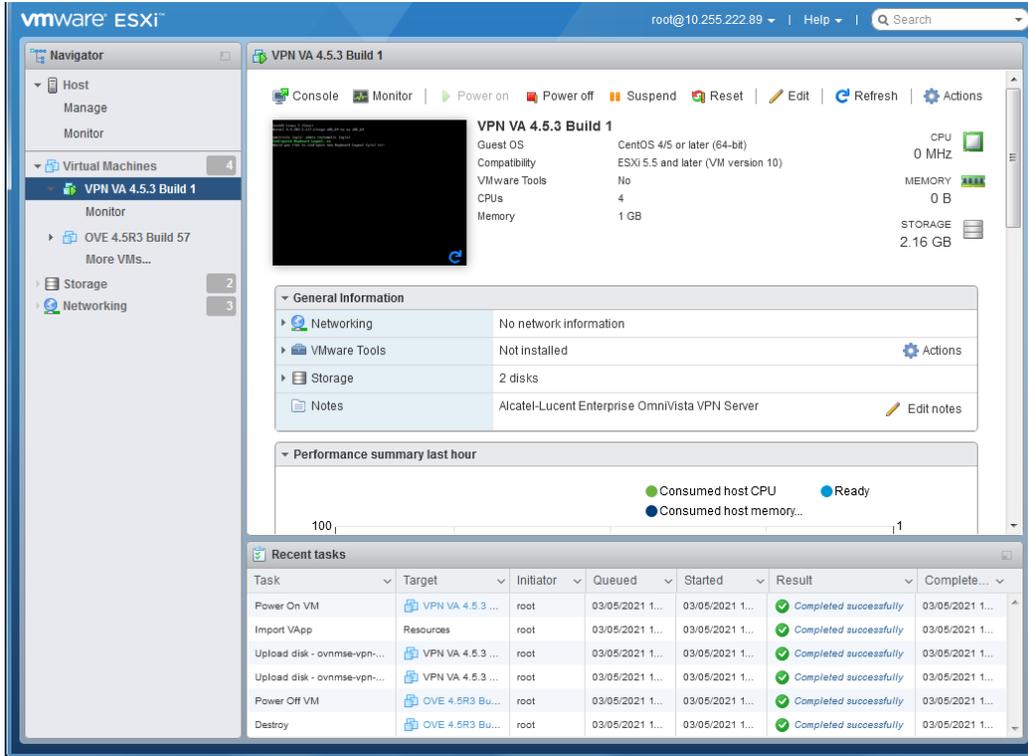
Important Notes:

- On the ESXi VM, configure the VLAN the NIC dedicated to bridged traffic (the interface without the managed IP Address), as follows:

  - Configure VLAN 0 if you want Untagged VLAN traffic to be tunneled through VPN tunnels.

  - Configure VLAN 4095 if you want Tagged VLAN traffic to be tunneled through VPN tunnels.
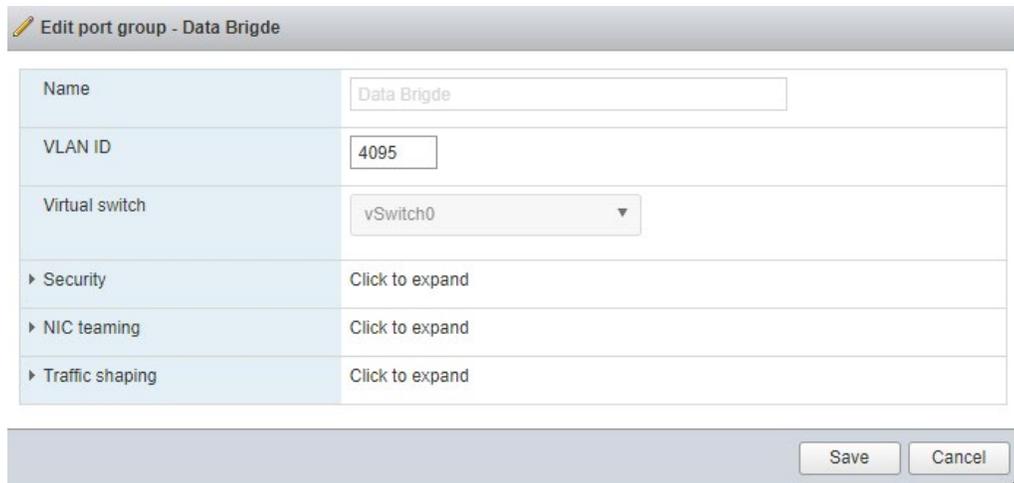
- On the ESXi VM, enable Promiscuous Mode for the above NIC. If the "Override" checkbox is enabled, make sure Promiscuous Mode, MAC address changes, and Forged transmits are set to "Accept".

- Inherit from vSwitch means this port group uses the same setting as vSwitch0; so, make sure vSwtich0 is set to "Accept" for Promiscuous Mode, MAC address changes, and Forged transmits. Or you can set Accept directly in the port group setting.

11. Click on the small Console Screen or click on Console at the top of the screen and select **Open Browser Console** to open a Console and go to Configuring the VPN Virtual Appliance to complete the installation.

Deploying the VPN VA with NIC Teaming

1. From ESXi Web GUI, go to **Networking** and select the **Virtual switches** tab. Choose the virtual switch and click on **Add Uplink**.
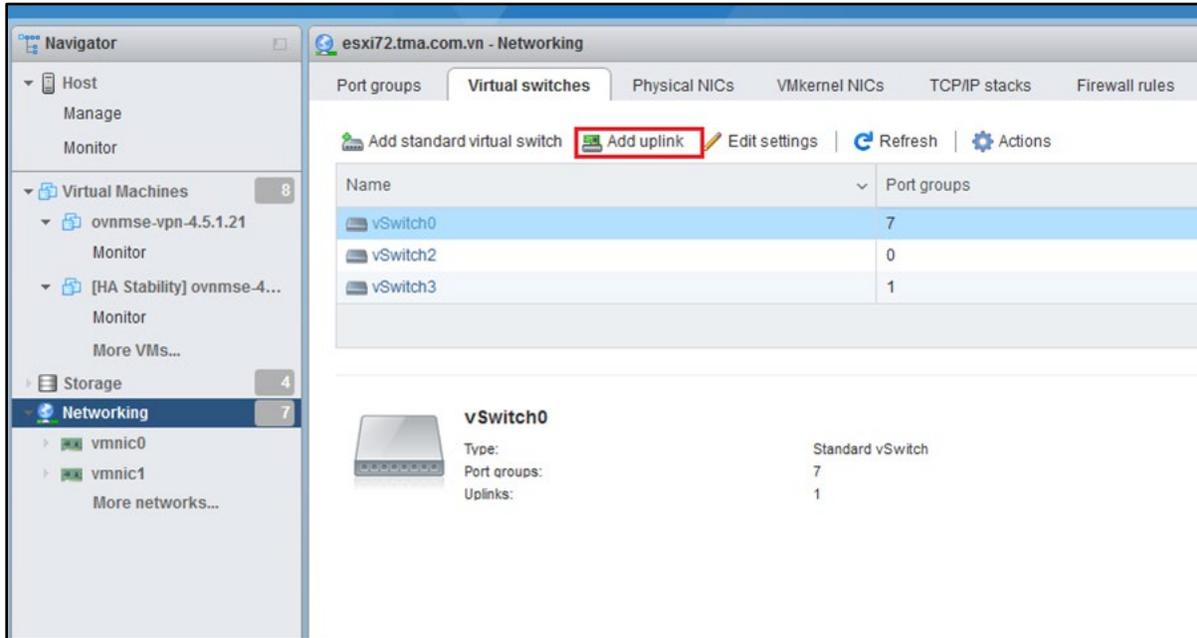
2. Select the uplink.
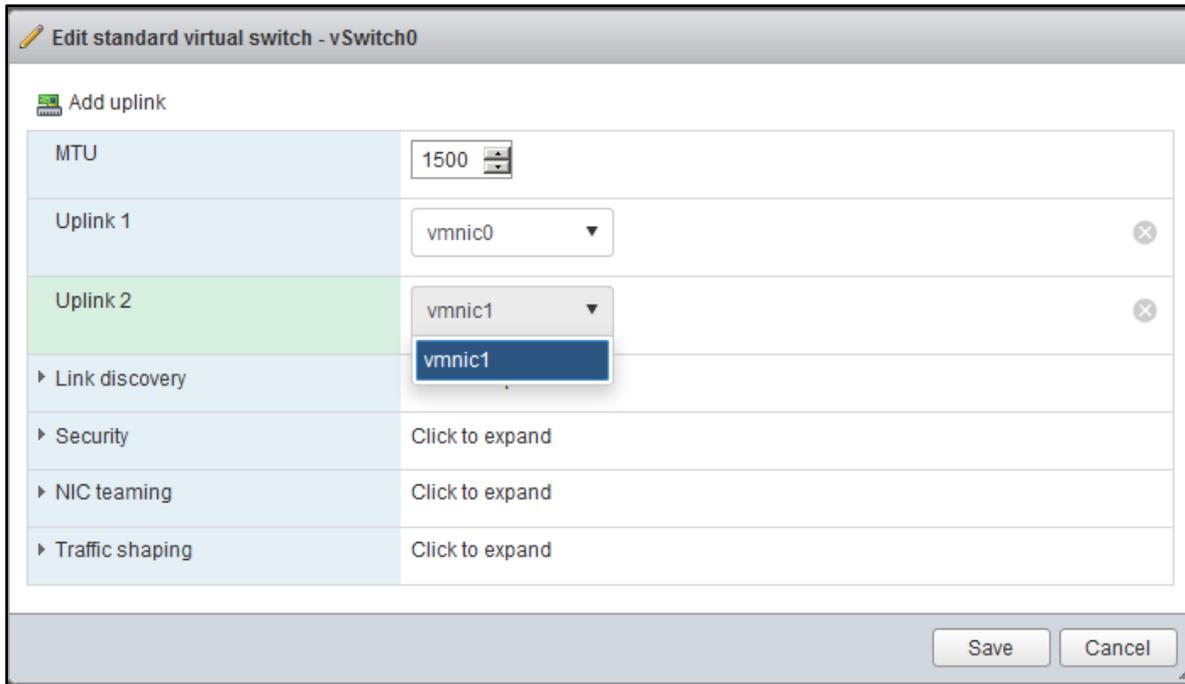
3. Edit the virtual switch and configure the load balancing rule.
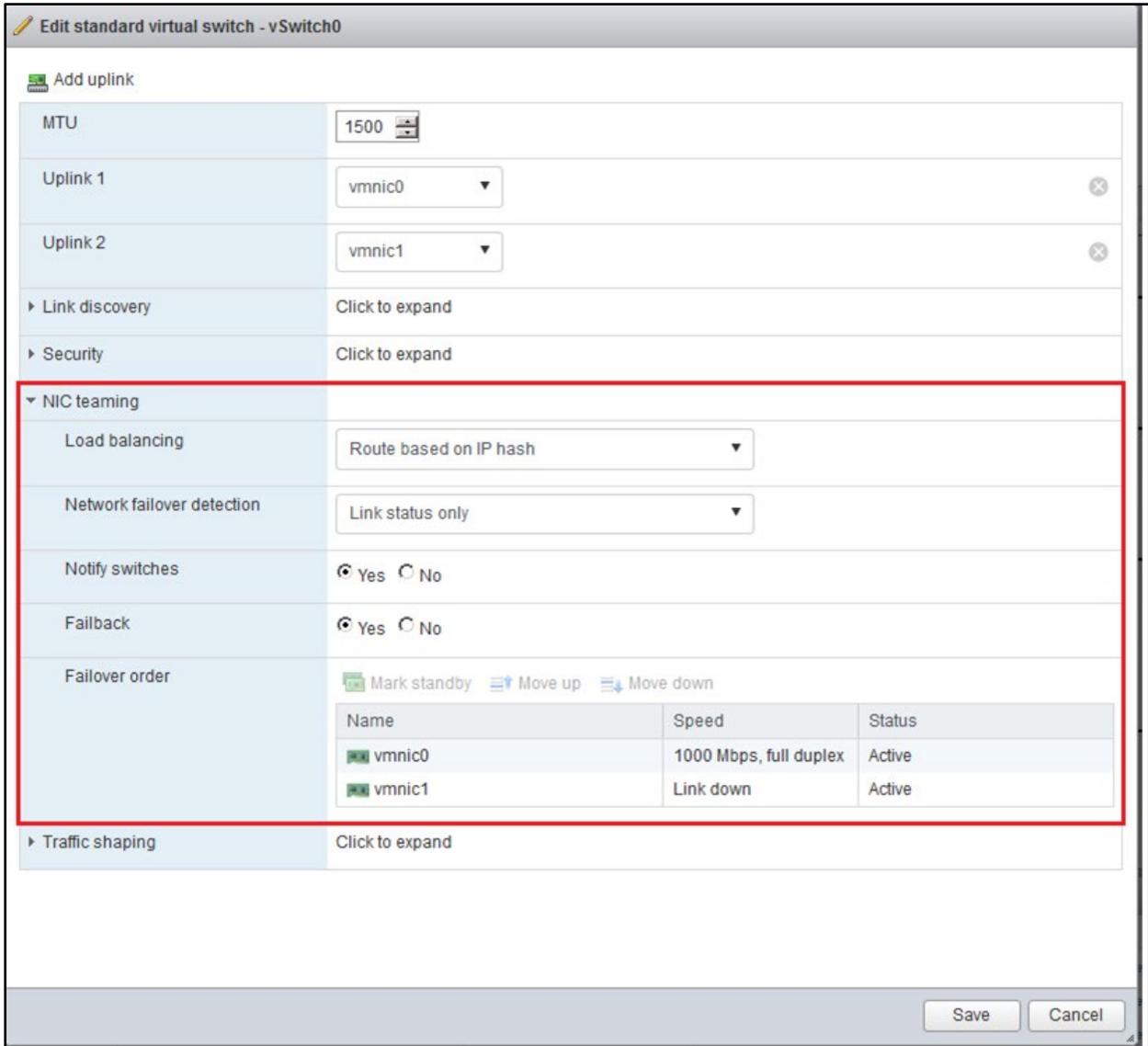
Deploying the Virtual Appliance on Hyper-V

1. Download and unzip the OVF package. You will be using the OVF File and both VMDK Files (disk 1 and disk 2) for the installation (ovnmse-vpn-4.5.3.1.ovf, ovnmse-vpn-4.5.3.1-disk001.vmdk and ovnmse-vpn-4.5.3.1-disk002.vmdk). **The Zip file also contains an *.mf File. Delete the *.mf File from the folder <u>before</u> importing the files in Step 2**. Note that the screenshots below depict 4.5.2 files. The steps are the same for 4.5.3.

Name ▲	Date modified	Type	Size	
📁 hyperv	9/9/2020 2:35 PM	File folder		
📄 ovnmse-vpn-4.5.2.5.mf	9/9/2020 2:35 PM	MF File	1 KB	
🔷 ovnmse-vpn-4.5.2.5.ovf	9/9/2020 2:35 PM	OVF File	29 KB	
💾 ovnmse-vpn-4.5.2.5-disk001.vmdk	9/9/2020 2:35 PM	VMware virtual disk ...	783,200 KB	
💾 ovnmse-vpn-4.5.2.5-disk002.vmdk	9/9/2020 2:35 PM	VMware virtual disk ...	101 KB	

2. Import the VM into Hyper-V.
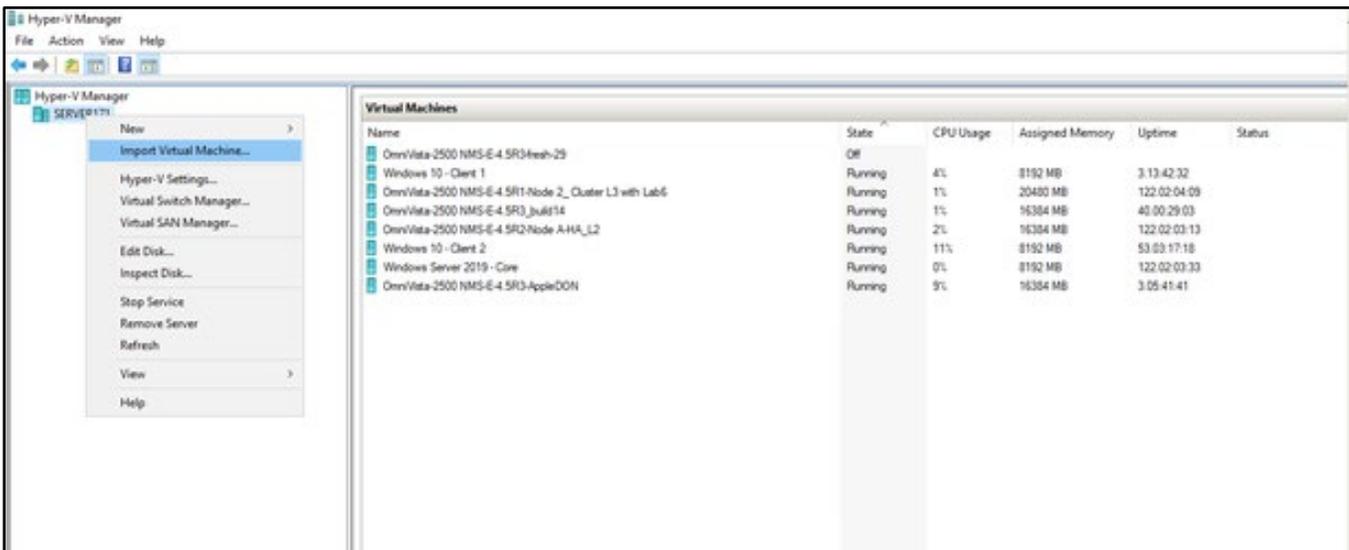
3. Select the location folder to Hyper-V source of VPN VA.

Part No. 060831-10, Rev. A
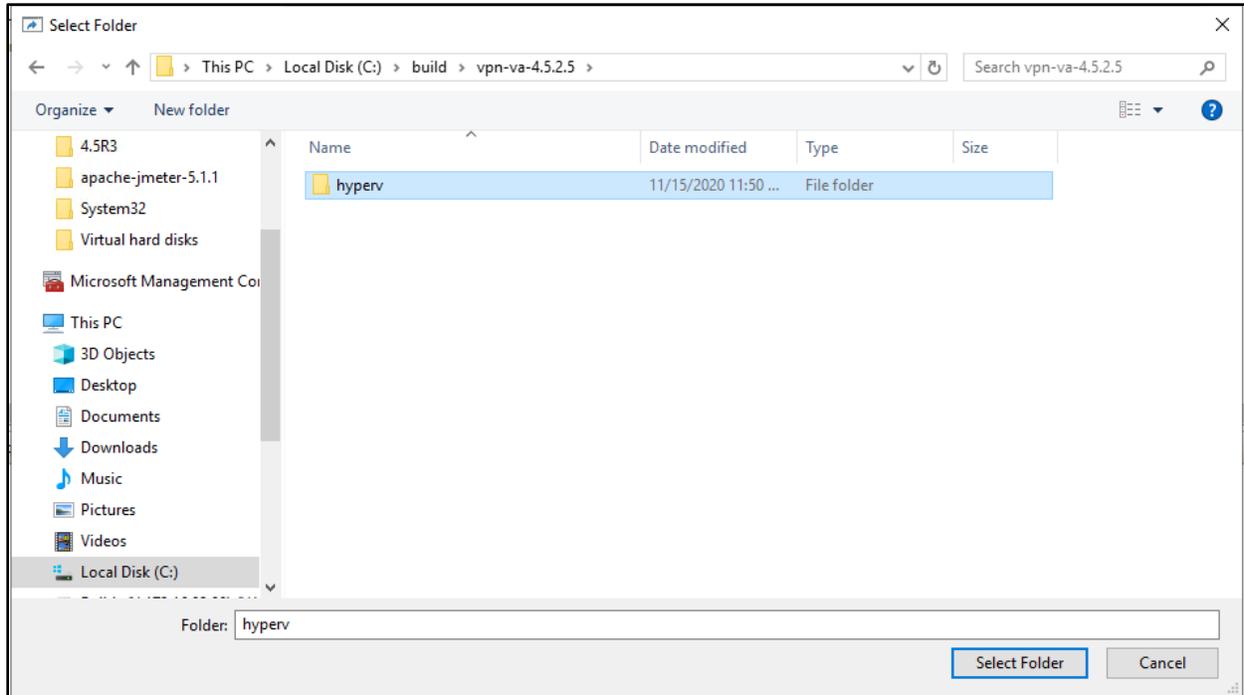
4. Select the Import Type: **Copy the Virtual Machine**.
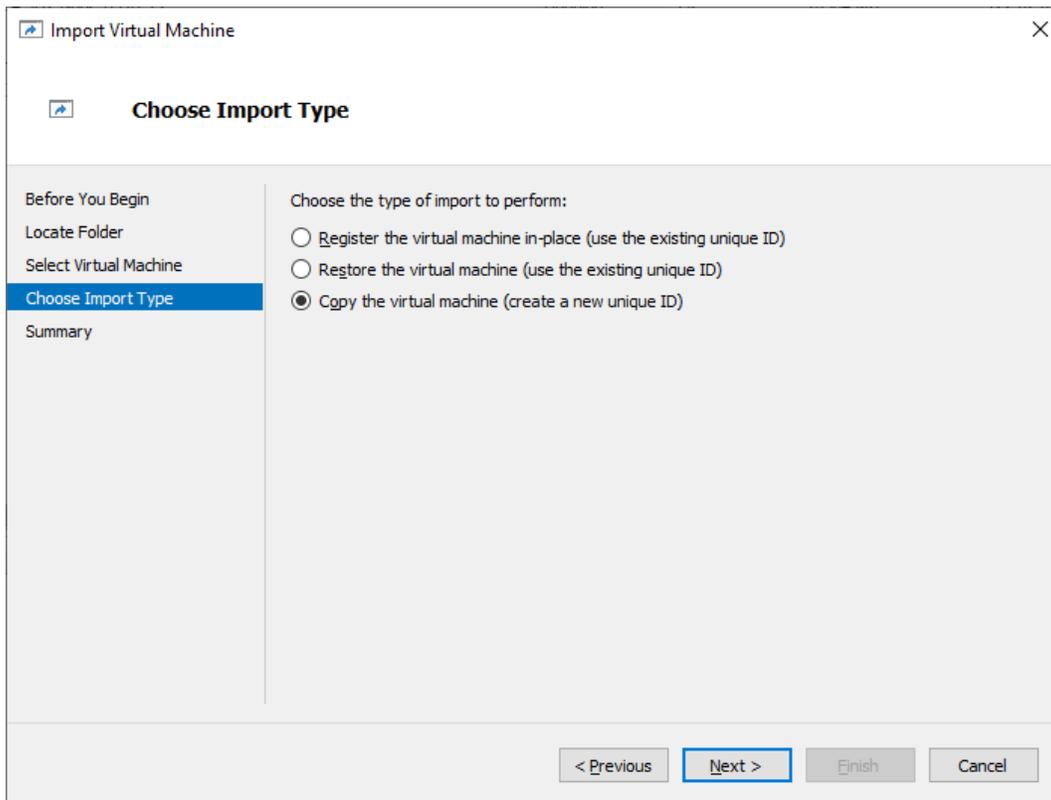
5. Choose Destination and Storage Folder. You can use the default or customize the location.

6. Click **Finish** to complete the VA import.
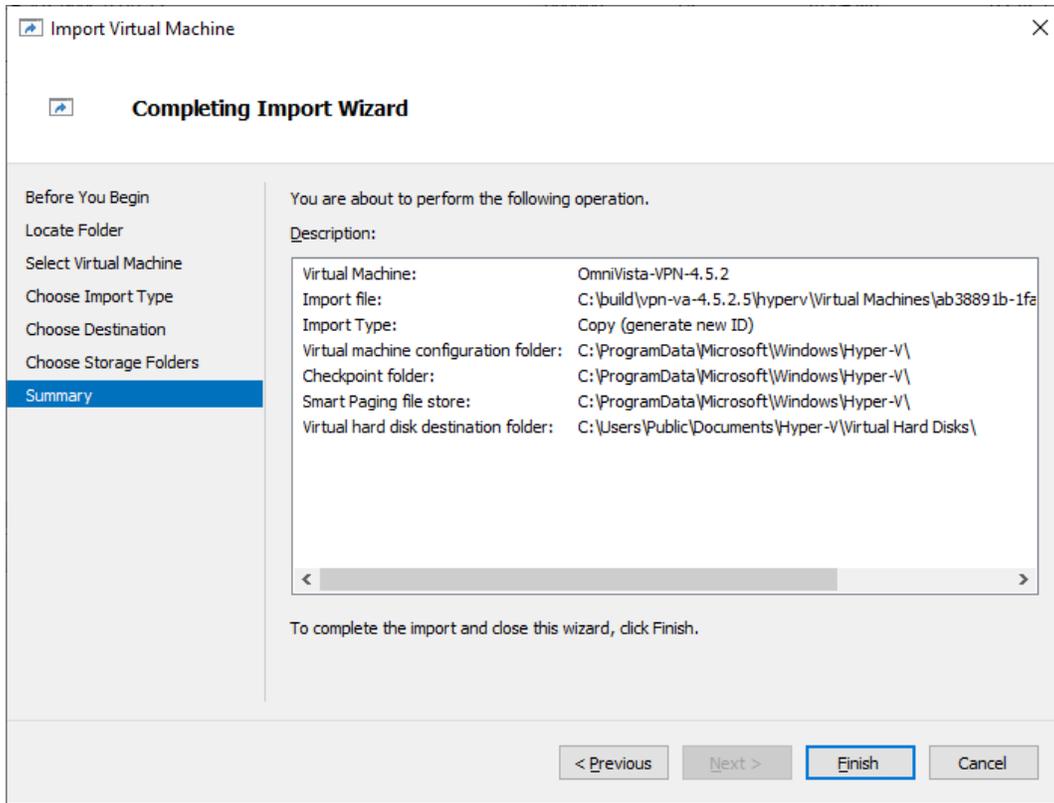
7. Edit the Virtual machine and remove the Network interface.
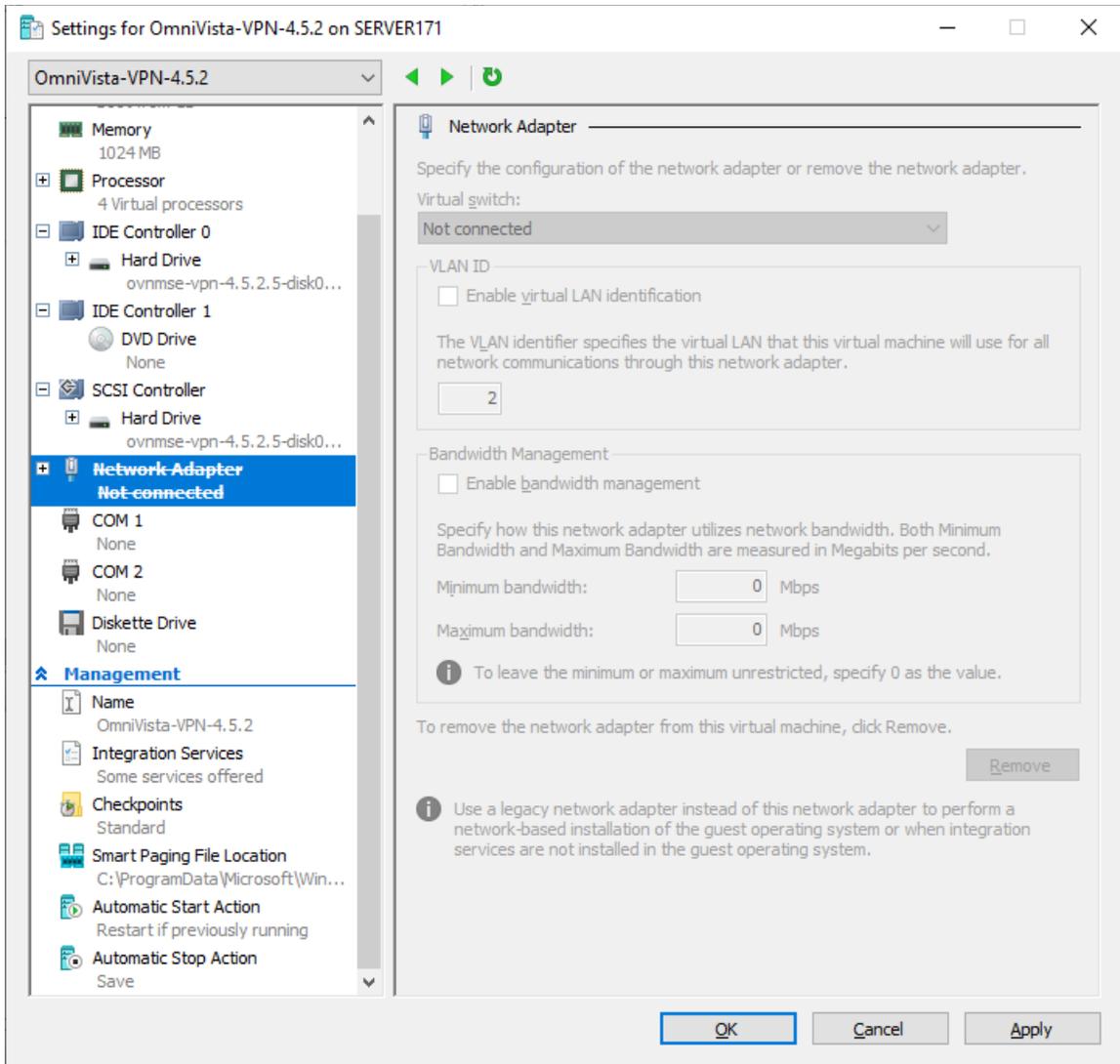
8. Run the commands below on Power shell to creating 3 Network Adapters.

```
1. For ($Count=0; $Count -le 2; $Count ++)
2. {
3. Add-VMNetworkadapter -VMName OmniVista-VPN-4.5.2 -Name "Eth$Count"
   }
```

9. Create an "External" Hyper-V virtual switch.
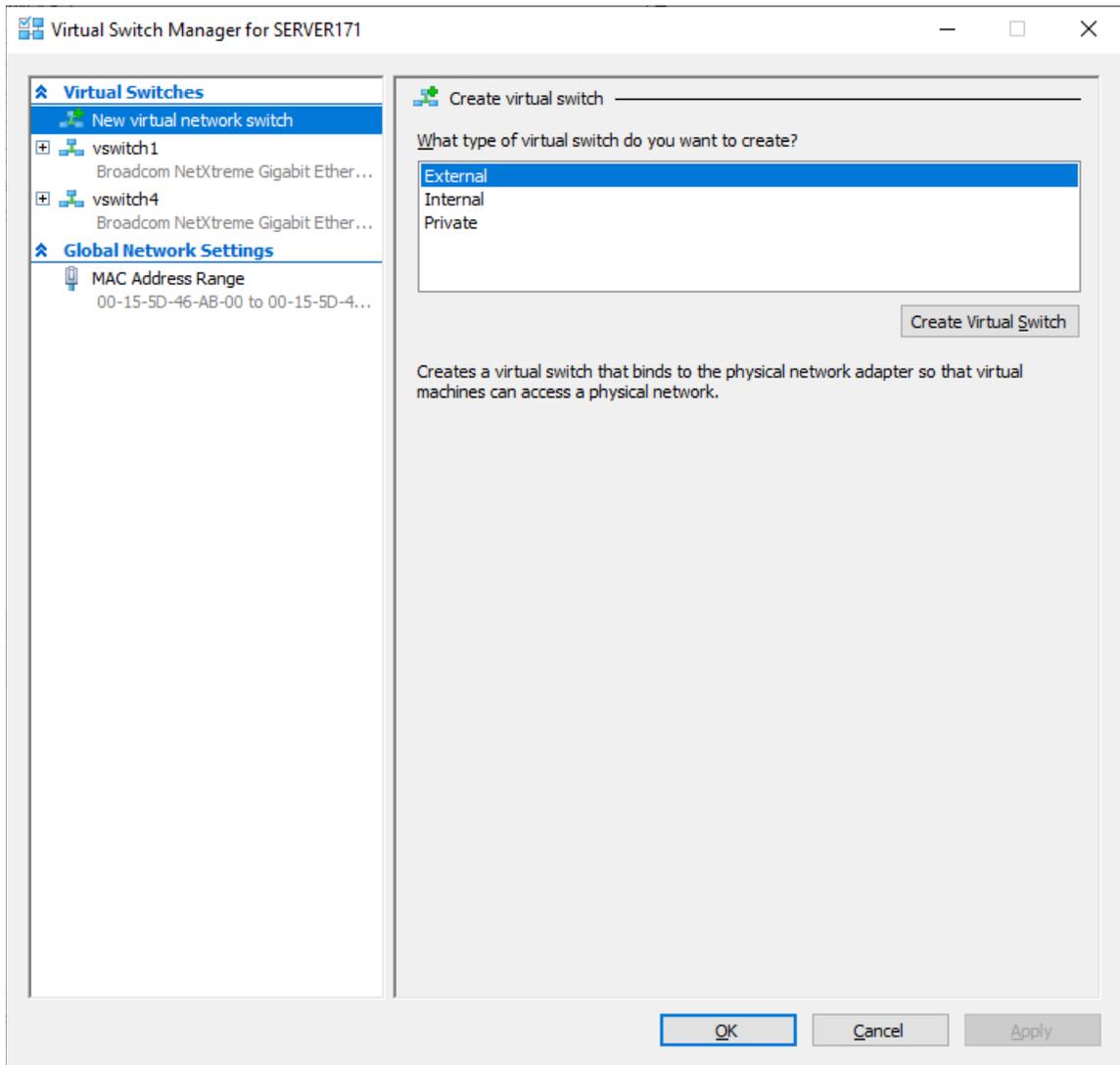
10. Attach to the Physical network interface.
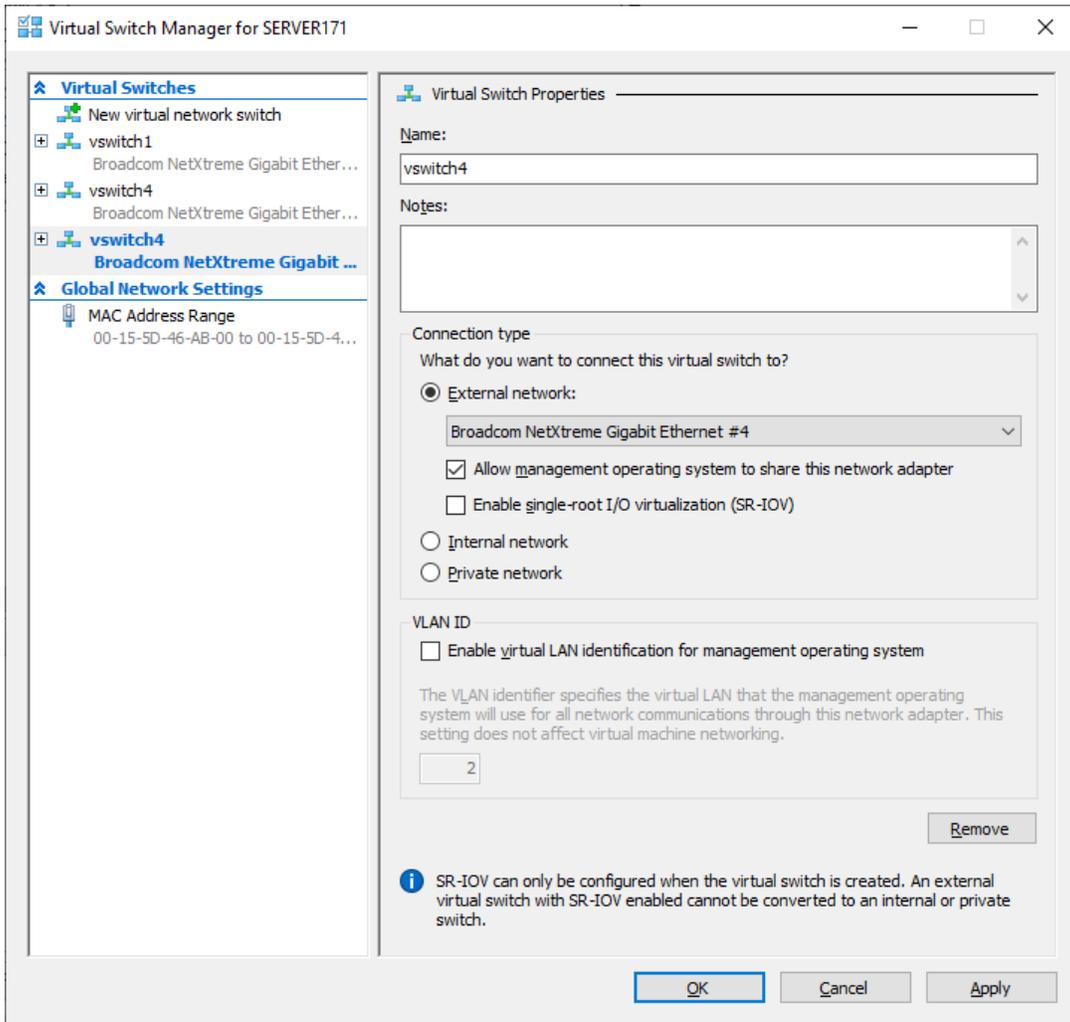
11. Use Eth0 for the public interface, Eth1 for the private interface, and Eth2 for the bridge interface.
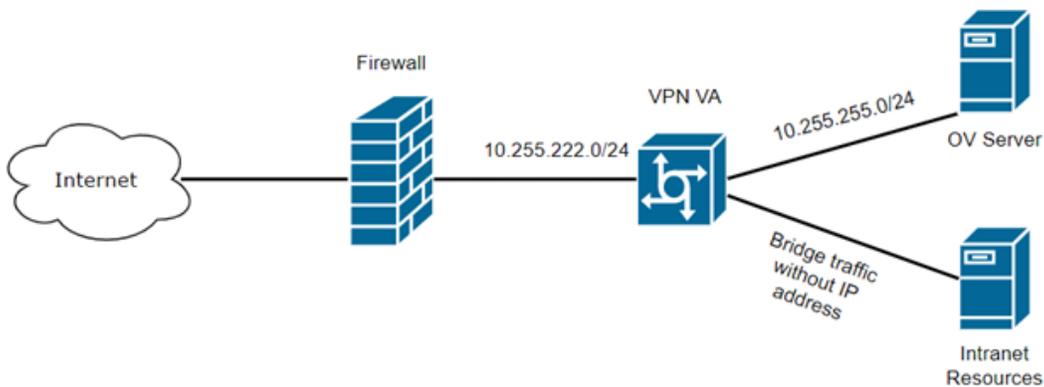
12. Edit the VPN virtual machine. Select **Enable virtual LAN identification** on **Eth0** and map to public VLAN (e.g., VLAN 70)
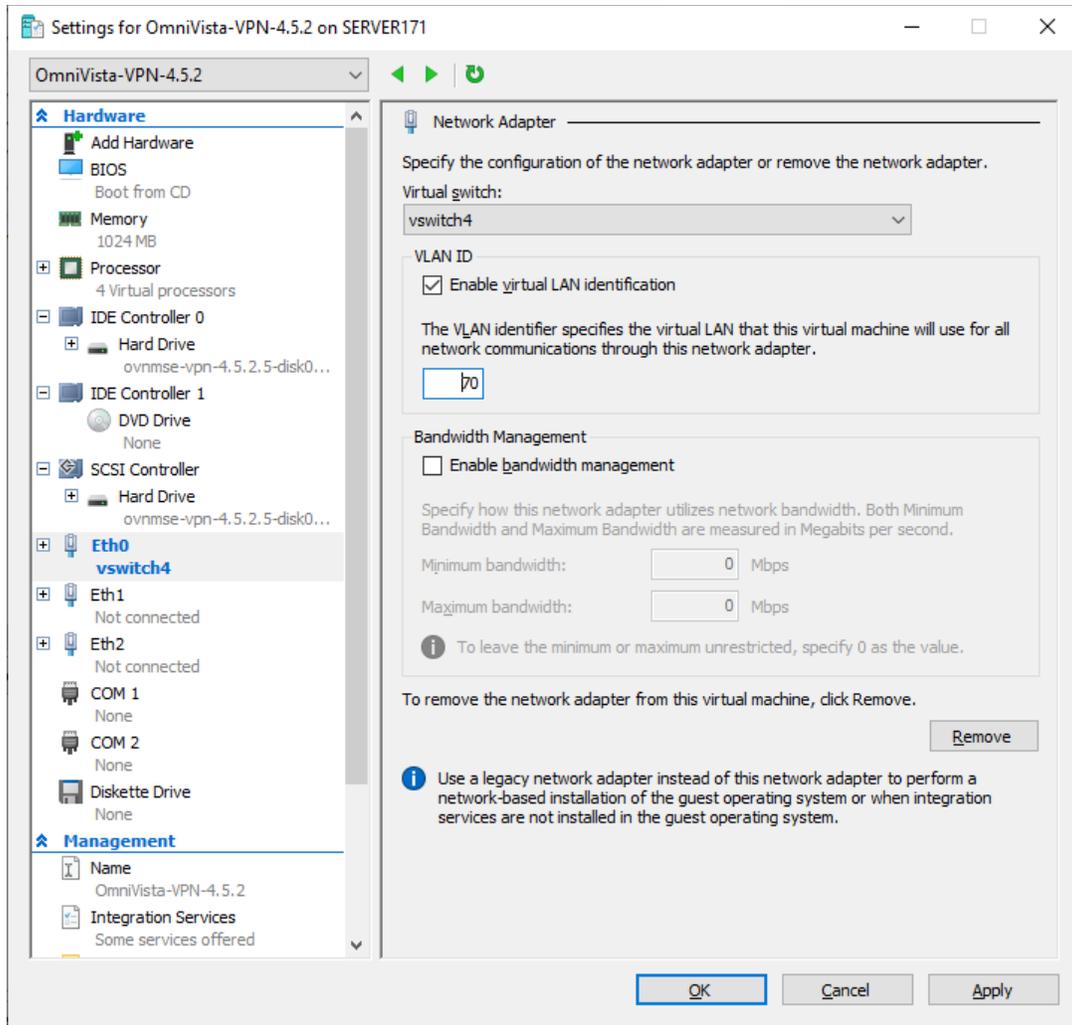
13. Select **Enable virtual LAN identification** on Eth1 and map to private VLAN (e.g., VLAN 1000).
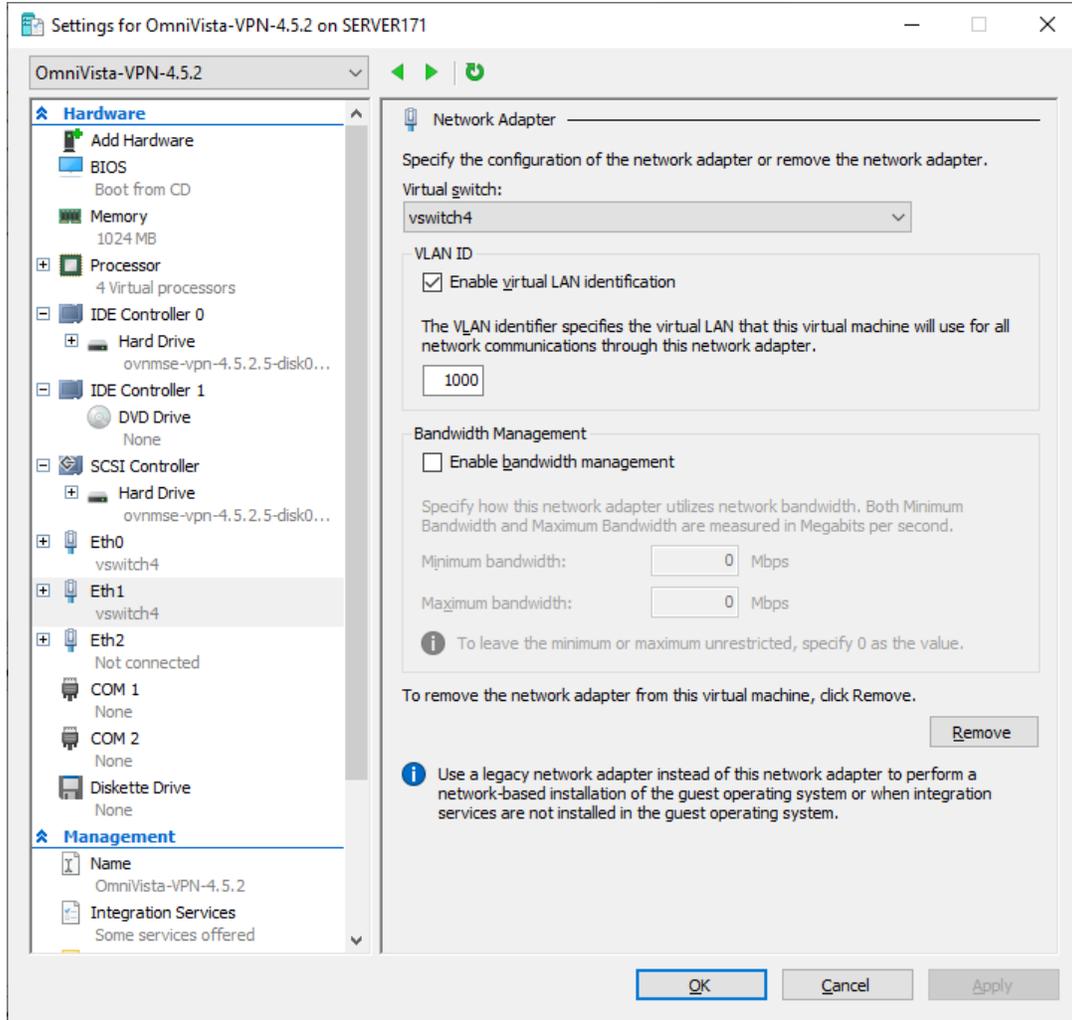
14. Expand **Eth2**, under **Advanced Features** select the option **Enable MAC address spoofing**.
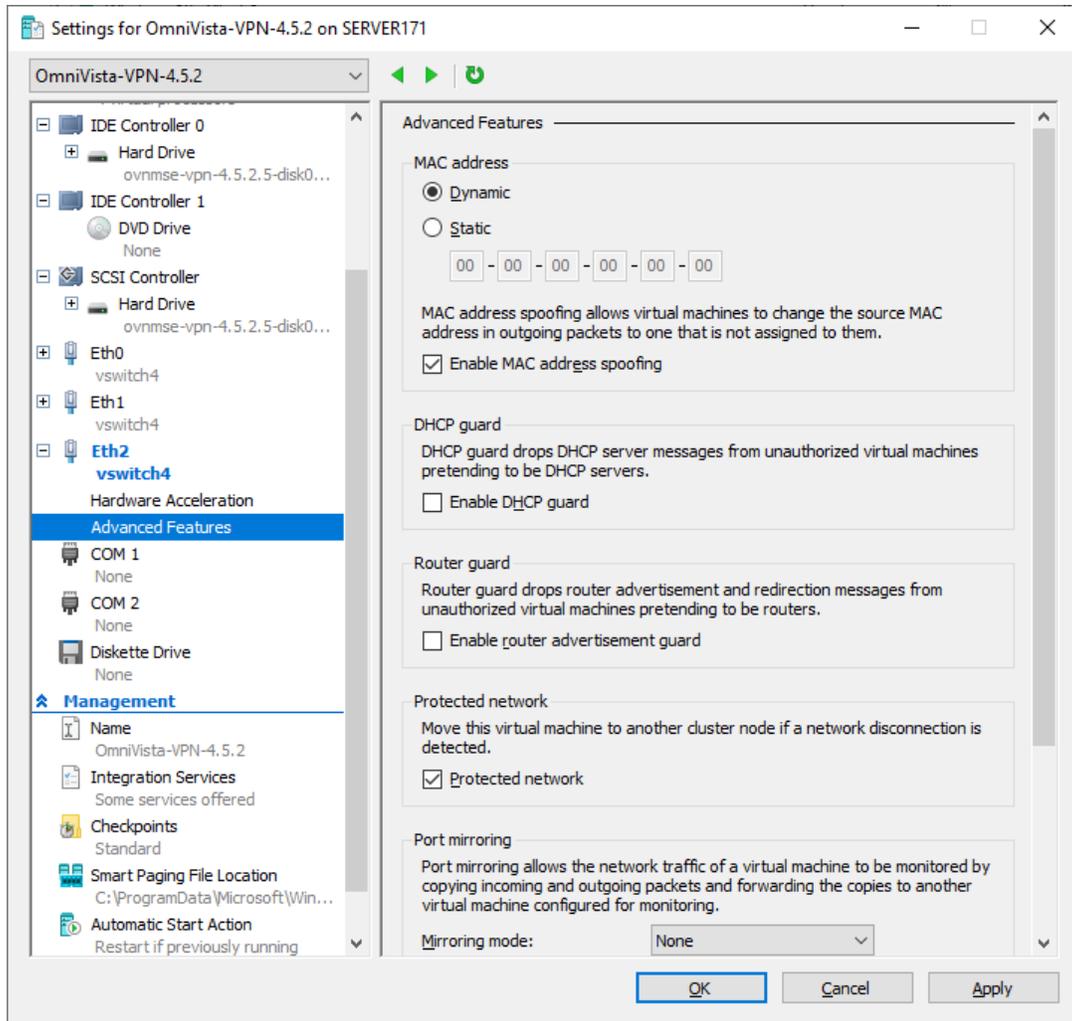
15. Configure the Trunk Mode for Eth2 using the command below command in the power shell.

```
Set-VMNetworkAdaptervlan -VMName OmniVista-VPN-4.5.2 -
VMNetworkAdapterName "Eth2"-Trunk -AllowedVlanIdList "201, 202" -
NativeVlanId 0
```

16. Verify that Trunk Mode is successfully enabled using the commands below.

```
Get-VMNetworkAdapterVlan -VMName OmniVista-VPN-4.5.2
```

17. Start the VPN virtual machine and perform the setup.

Deploying the VPN VA with NIC Teaming

1. Open Server Manager - Local Server.
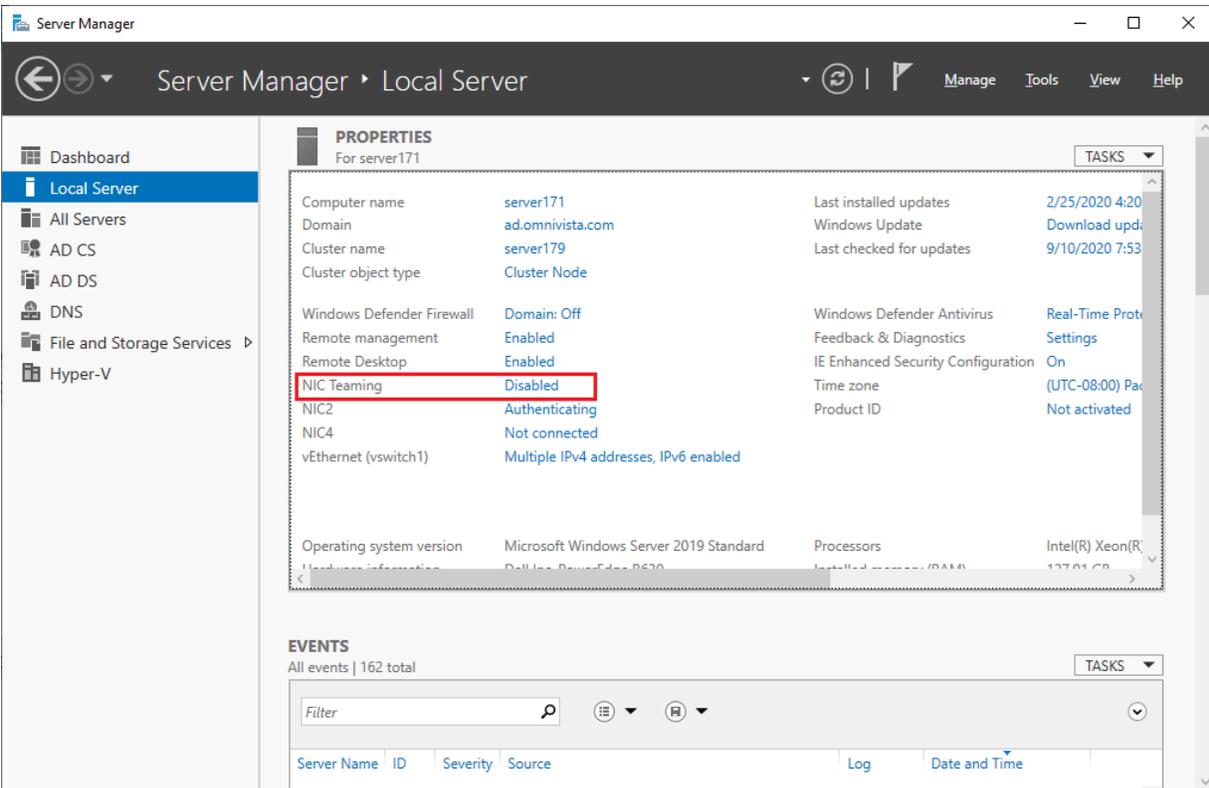
2. Edit NIC Teaming - **New Team**.
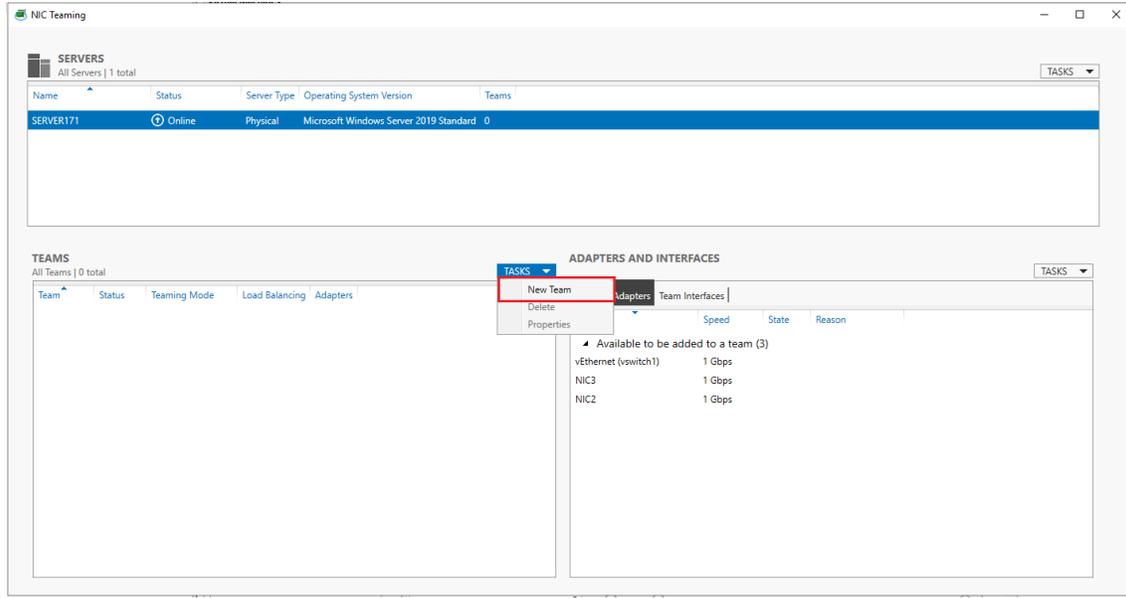
3. Choose NIC members, Teaming mode, and Load balancing mode, then click **OK**.
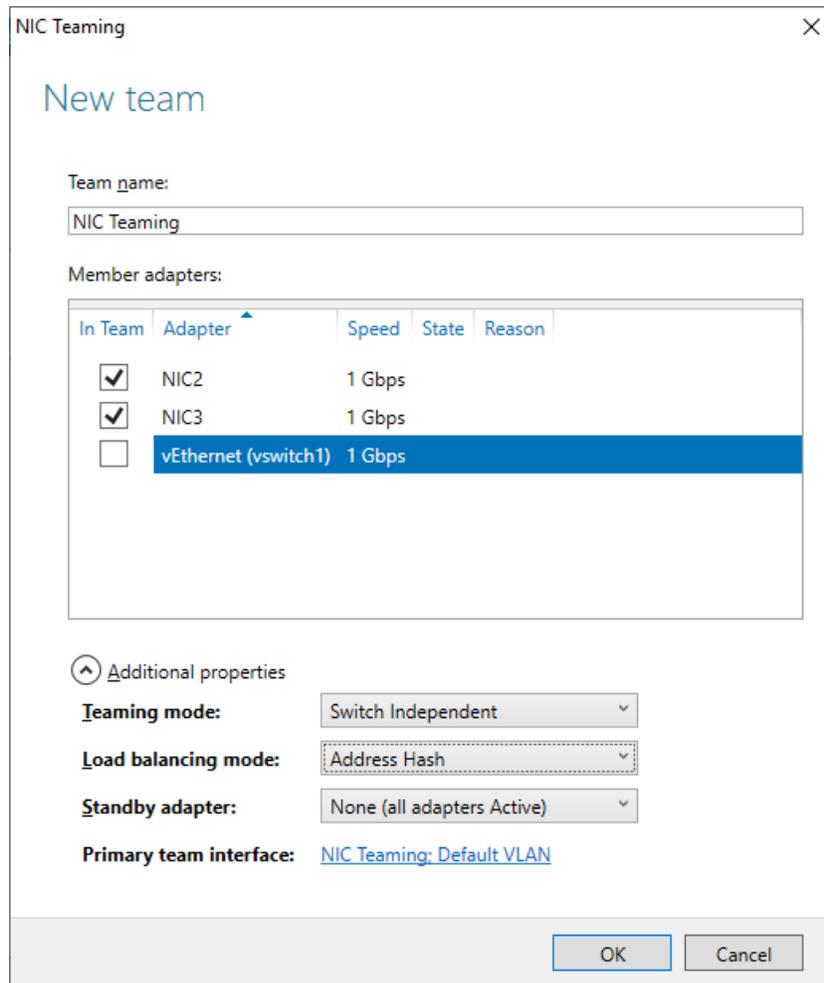
4. Create a Hyper-V virtual switch and attach to the NIC Teaming interface, then click **OK**.
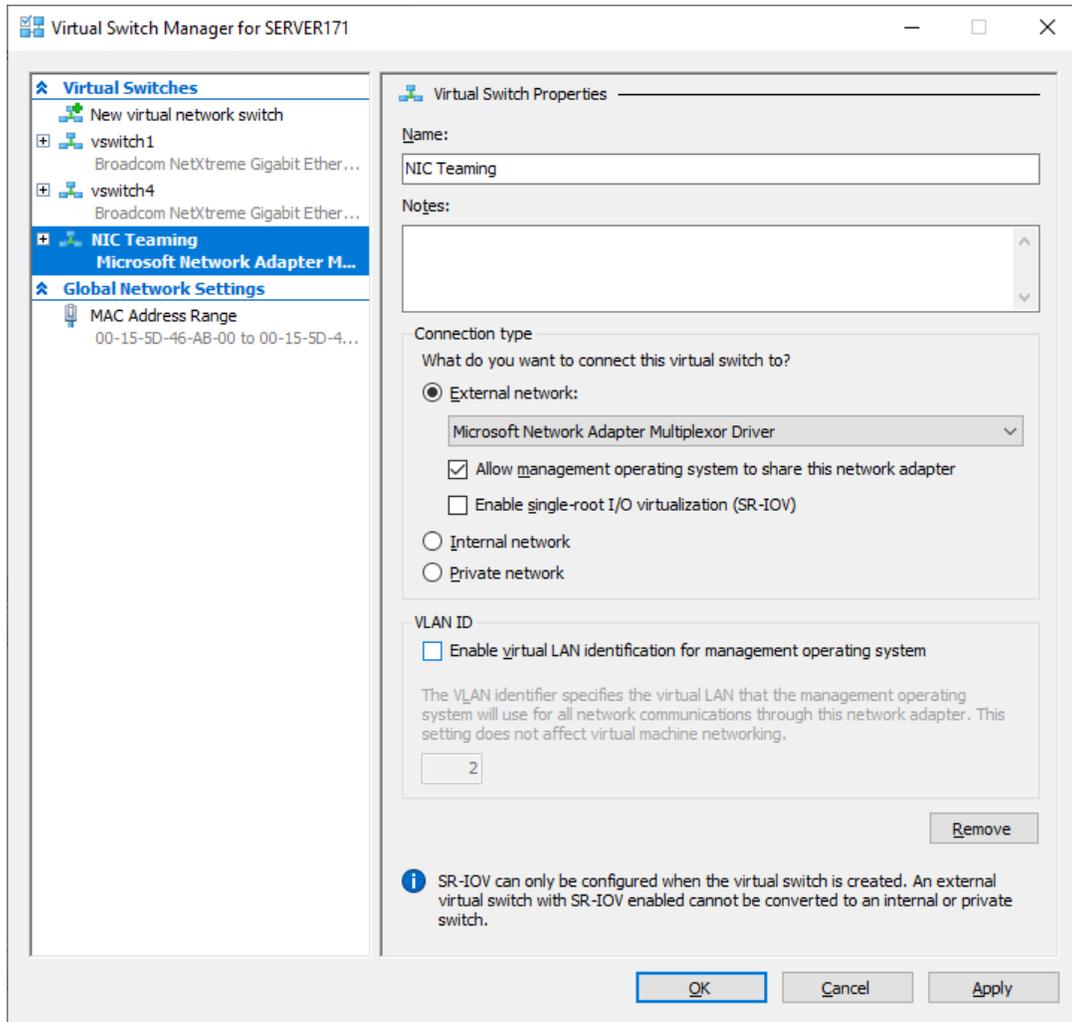
5. Edit the VM network interface. Change the Virtual Switch to **NIC Teaming**.
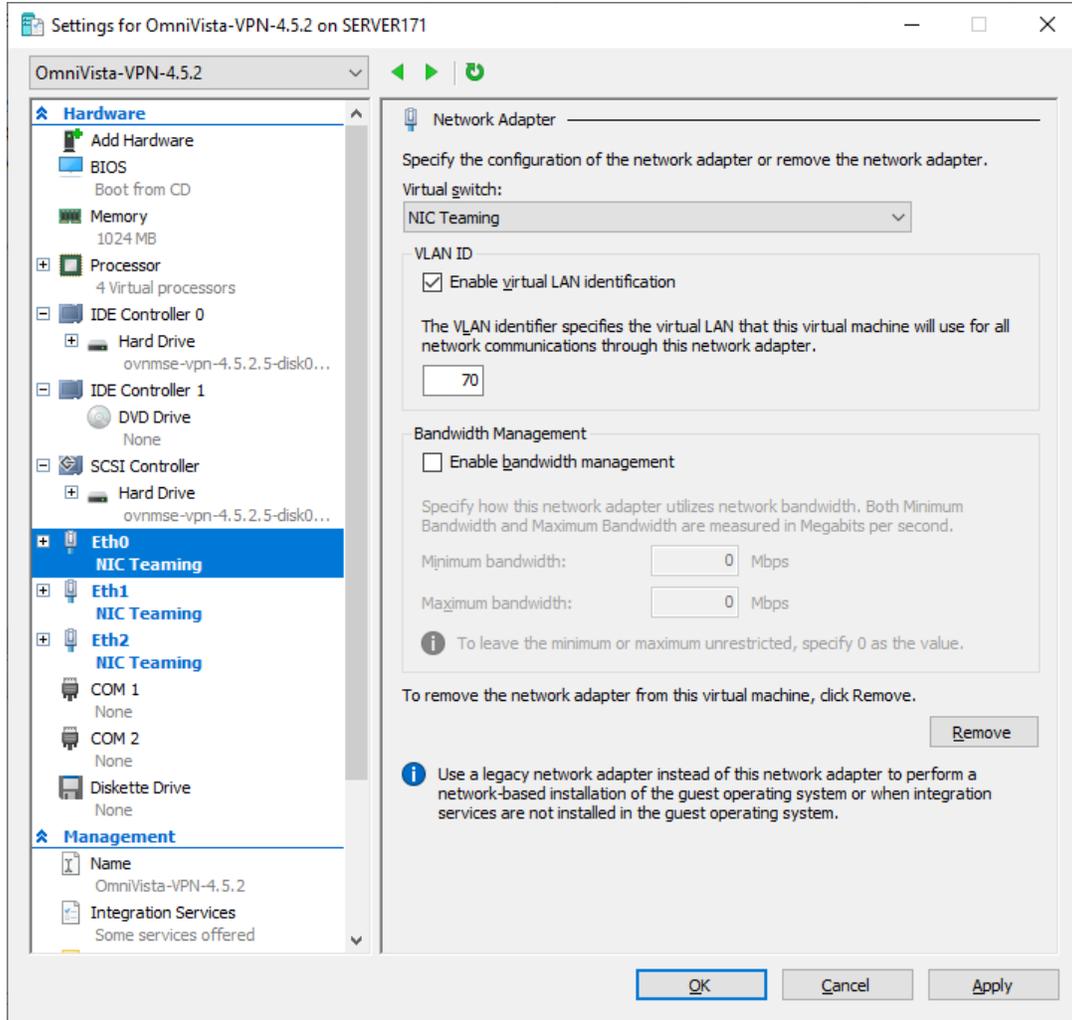
NIC Teaming Compatible Modes				
Layer 2 Switch Mode	**NIC Teaming Mode**	**Load Balancing Mode**	**Stand-By Adapter**	**Worked?**
Switch Independent	Switch Independent	Address Hash	None	Yes
Switch Independent	Switch Independent	Address Hash	NIC1/NIC2	Yes
Switch Independent	Switch Independent	Hyper-V Port	None	No
Switch Independent	Switch Independent	Hyper-V Port	NIC1/NIC2	No
Switch Independent	Switch Independent	Dynamic	None	No
Switch Independent	Switch Independent	Dynamic	NIC1/NIC2	No
Linkagg static	Linkagg static	Address Hash	None	Yes
Linkagg static	Linkagg static	Hyper-V Port	None	Yes
Linkagg static	Linkagg static	Dynamic	None	Yes

NIC Teaming Compatible Modes				
Layer 2 Switch Mode	**NIC Teaming Mode**	**Load Balancing Mode**	**Stand-By Adapter**	**Worked?**
LACP	LACP	Address Hash	None	Yes
LACP	LACP	Hyper-V Port	None	Yes
LACP	LACP	Dynamic	None	Yes

Configuring the VPN Virtual Appliance

Once the VPN is deployed, perform the following steps to complete the installation:

1. Complete the Installation
2. Configure NICs
3. Configure Routes
4. Configure Network Settings (DNS, Gateway)
5. Configure an SSH Service
6. Upload VPN Settings to the VPN Server
7. Configure the VPN Service
8. Configure VPN Endpoints

Complete the Installation

1. Launch the Hypervisor Console for the VPN VA. You will be automatically logged in and the Keyboard Layout Prompt will appear. Press **Enter** if you do not want to change the default keyboard layout (US), or enter **y** then press **Enter** to change the default keyboard layout

```
CentOS Linux 7 (Core)
Kernel 4.4.203-1.el7.elrepo.x86_64 on an x86_64

omnivista login: admin (automatic login)
Configured Keyboard Layout: us
Would you like to configure new Keyboard Layout [y¦n] (n):
```

2. The End User Agreement will appear. Press the spacebar to scroll through the agreement. When you reach the end of the agreement, enter **y** and Press **Enter** to accept the agreement.

```
Proactive Lifestyle Management Product Exhibit

This Product Exhibit defines the special terms and conditions applicable to the ProActive Lifestyle
Management product.  This Exhibit is a complement to the End User License Agreement (the "EULA") and
 incorporates by reference the terms and conditions of the Agreement to the extent relevant to the R
AP Software. In case of conflict of terms between this Product Exhibit and the EULA, this Addendum s
hall prevail as far as the RAP Software is concerned.  All of the defined terms and conditions set f
orth in the EULA have the same meaning in this Product Addendum.

ProActive Lifecycle Management

The ProActive Lifecycle Management (PALM) feature may be chosen during installation, it collects and
 stores information such as; the make, model and serial number of Licensee's devices, the device sof
tware version numbers and system uptime information and such other information that would, in Licens
ors sole discretion, be utilized to improve the customer experience. The information helps us to dia
gnose potential problems, if any, in the software. We may or may not use the diagnostic information,
 in our sole discretion, to provide support solutions, including updates, upgrades or services packs
, if any are made generally available. We will not use the ProActive Lifecycle Management feature to
 track, collect or upload any data that personally identifies You (such as your name, address, email
 address) except Customer information provided to us by You. Licensee may opt-out of providing this
data during installation of the Software by, as the case may be, checking or un-checking the box adj
acent to the ProActive Lifecycle Management feature option. If the box next to the ProActive Lifecyc
le Management feature option is not checked the option will not be activated. If You decide to activ
ate the ProActive Lifecycle Management feature after full installation, You may do so by following t
he instructions on the Preference page for ProActive Lifecycle Management in You OmniVista 2500 clie
nt. Your use of the software constitutes your acknowledgment and agreement to the terms of use. © Co
pyright Alcatel-Lucent Enterprise USA, Inc., 1997 © Copyright ALE USA Inc., 2014, 2020

Accept End-User License Agreement (y/n): _
```

3. The Admin Password Prompt will appear. Enter and confirm the Admin Password for the VM and press **Enter**.

```
*******************************************************************************************
* Configure "admin" password                                                             *
*******************************************************************************************
You must remember the new passwords in order to manage the Virtual Appliance and OmniVista.
Length of new password must be >= 8 and <= 30 characters
Enter new password: _
```

4. The VM will reboot. When the reboot is complete, the OmniVista Login Prompt will appear. Enter the OmniVista Login (admin) and press **Enter**; then enter the Admin Password you configured in Step 3 and press **Enter**.

```
CentOS Linux 7 (Core)
Kernel 4.4.203-1.el7.elrepo.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 VPN VA
Release Version: 4.5.3
Build Number: 1
Build Date: 2020-11-23
omnivista login: admin
Password:
```

5. The Main Menu will appear with the **Network Interfaces** option highlighted.

Configure NICs

```
Main Menu

< Network Interfaces                                                          >
< Network Routes                                                             >
< Network Services...                                                        >
< Network Settings...                                                        >
< VPN Endpoints...                                                           >
< VA Settings...                                                             >
< Maintenance...                                                             >
< Apply Configuration Changes                                               >
< Logout                                                                     >
```

1. With the **Network Interfaces** option highlighted, press **Enter** to bring up the **Menu for Network Interfaces** Screen.

```
Menu for Network Interfaces

1. NIC1:
      Name: eth0
      IP:
      Prefix length: 0
      MAC: 00:50:56:af:cb:cd
2. NIC2:
      Name: eth1
      IP:
      Prefix length: 0
      MAC: 00:50:56:af:82:28
3. NIC3:
      Name: eth2
      IP:
      Prefix length:
      MAC: 00:50:56:af:a8:7f


Please select NIC to modify:

< OK                                                                         >
< Exit                                                                       >
```

2. At the **Please select NIC to modify** prompt at the bottom of the screen, enter the number of the NIC you want to configure (e.g., 1), use the Down Arrow to highlight **OK** and press **Enter**.

```
Menu for Configure a network interface

      Name: eth0
      IP: 10.255.222.97
      Prefix length: 24
      MAC: 00:50:56:af:cb:cd

Please input IPv4:
Please input prefix length:

< Save                                                                       >
< Exit                                                                       >
```

3. Enter the VPN Public **IPv4 address** (e.g.,10.255.222.97) use the Down Arrow to move to the **Prefix Length** field and enter the prefix length (e.g., 24) for the IP address. Move the Down Arrow to highlight **Save** and press **Enter**, then press **Enter** at the **OK** Confirmation Prompt. The following prompt will appear.

```
The configuration has been saved successfully!
< OK                                                            >
```

4. Repeat the process in Step 3 above to configure the OVE Server IP address. This is the interface that will be used to connect to the OVE Server.

```
Menu for Configure a network interface

     Name: eth1
     IP: 10.255.255.98
     Prefix length: 24
     MAC: 00:50:56:af:82:28

Please input IPv4: _
Please input prefix length:

< Save                                                          >
< Exit                                                          >
```

> **Note:** To set up a Data Tunnel, you use the third NIC on the VA. You must not configure an IP address for this NIC because it will be a Layer 2 Tunnel. **You also need to enable "Promiscuous Mode" for this NIC in your Hypervisor**.

5. Press **Enter** to return to the Main Menu.

```
Main Menu

< Network Interfaces                                            >
< Network Routes                                                >
< Network Services...                                           >
< Network Settings...                                           >
< VPN Endpoints...                                              >
< VA Settings...                                                >
< Maintenance...                                                >
< Apply Configuration Changes                                   >
< Logout                                                        >
```

6. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

```
Main Menu

< Network Interfaces                                            >
< Network Routes                                                >
< Network Services...                                           >
< Network Settings...                                           >
< VPN Endpoints...                                              >
< VA Settings...                                                >
< Maintenance...                                                >
< Apply Configuration Changes                                   >
< Logout                                                        >
```

7. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

```
Would you like to apply all configuration ?

Note: VA will restart some services


< OK                                                                    >
< Exit                                                                   >
```

Configure Routes

If necessary, configure a Network Route.

```
Main Menu

< Network Interfaces                                                     >
< Network Routes                                                         >
< Network Services...                                                    >
< Network Settings...                                                    >
< VPN Endpoints...                                                       >
< VA Settings...                                                         >
< Maintenance...                                                         >
< Apply Configuration Changes                                           >
< Logout                                                                 >
```

1. On the Main Menu Screen, highlight **Network Routes** and press **Enter**.

```
Menu for Network Routes

     The system does not contain any routes

< Add a network route                                                   >
< Exit                                                                   >
```

2. With **Add a Network Route** highlighted, press **Enter**.

```
Menu for Add a network route

Please input subnet: 198.206.186.0
Please input prefix length: 24
Please input gateway: 10.255.255.98

< Save                                                                   >
< Exit                                                                   >
```

3. Enter the **Network Route Subnet**, use the Down Arrow the enter the **Prefix Length**, and the **Gateway**. Use the Down Arrow to move to **Save**, then press **Enter**.

```
Would you like to apply ? Add a network route

     Subnet: 198.206.186.0
     Prefix length: 24
     Default gateway: 10.255.255.98



< Save                                                                   >
< Exit                                                                   >
```
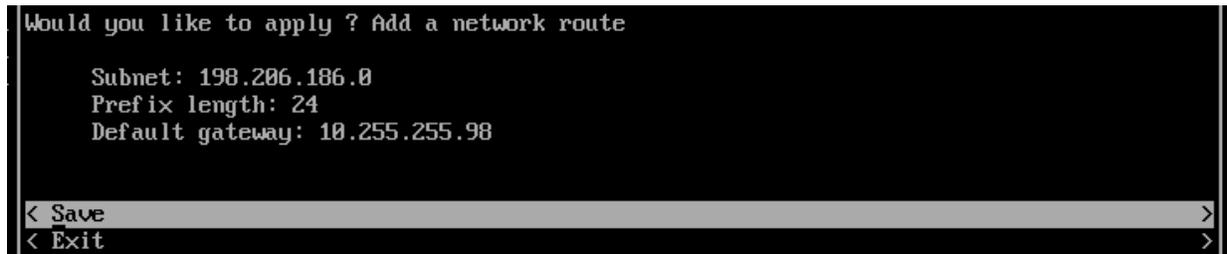
4. At the Confirmation Prompt, with **Save** highlighted, press **Enter**, then press **OK** at the next Confirmation Prompt. The Network Route will be added and Main Menu will appear.

```
Main Menu

< Network Interfaces                                                      >
< Network Routes                                                          >
< Network Services...                                                     >
< Network Settings...                                                     >
< VPN Endpoints...                                                        >
< VA Settings...                                                          >
< Maintenance...                                                          >
< Apply Configuration Changes                                            >
< Logout                                                                  >
```

5. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

```
Main Menu

< Network Interfaces                                                      >
< Network Routes                                                          >
< Network Services...                                                     >
< Network Settings...                                                     >
< VPN Endpoints...                                                        >
< VA Settings...                                                          >
< Maintenance...                                                          >
< Apply Configuration Changes                                            >
< Logout                                                                  >
```

6. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

```
Would you like to apply all configuration ?

Note: VA will restart some services

< OK                                                                      >
< Exit                                                                    >
```
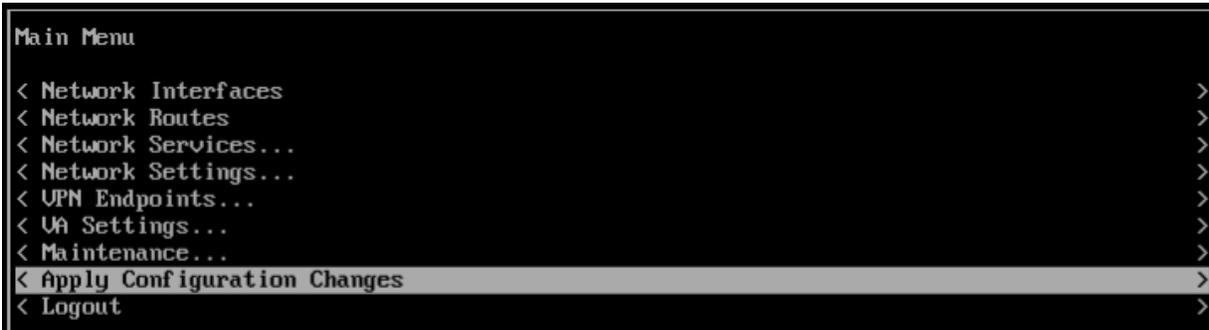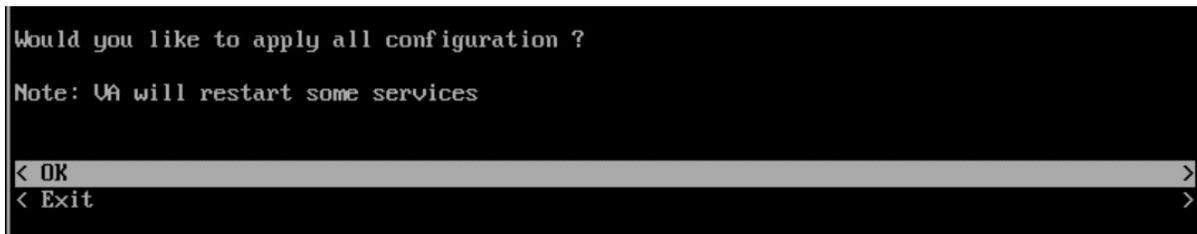
Configure Network Settings (DNS, Gateway)

If necessary, configure a DNS; and configure a Default Gateway for public network access.

```
Main Menu

< Network Interfaces                                                      >
< Network Routes                                                          >
< Network Services...                                                     >
< Network Settings...                                                     >
< VPN Endpoints...                                                        >
< VA Settings...                                                          >
< Maintenance...                                                          >
< Apply Configuration Changes                                            >
< Logout                                                                  >
```

1. On the Main Menu Screen, highlight **Network Settings** and press **Enter**.

```
Network Settings

< Show current configuration                                                    >
< Configure a network setting...                                               >
< Exit                                                                         >
```

2. Highlight **Configure a Network Setting** and press **Enter**.

```
Configure a network setting

< Configure DNS                                                                >
< Configure NTP                                                                >
< Configure Default Gateway                                                    >
< Exit                                                                         >
```

3. With **Configure DNS** highlighted, press **Enter**.

```
Menu for Configure DNS

Enter DNS server list
by separating with commas IP addresses: 198.206.1.3

< Save                                                                         >
< Exit                                                                         >
```

4. Enter a **DNS Server IP address(es)**, use the Down Arrow to highlight **Save**, and press **Enter**.

```
Would you like to save ? Configure DNS

The IP(s): 198.206.1.3

< Yes                                                                          >
< No                                                                           >
```

5. Press **Enter**, then press **Enter** at the next Confirmation Prompt.

```
Configure a network setting

< Configure DNS                                                                >
< Configure NTP                                                                >
< Configure Default Gateway                                                    >
< Exit                                                                         >
```

6. Highlight **Configure Default Gateway** and press **Enter**.

```
Menu for Configure Default Gateway

Enter the IP: 10.255.222.1

< Save                                                                         >
< Exit                                                                         >
```

7. Enter the **Gateway IP address**, use the Down Arrow to highlight **Save** and press **Enter**.

```
Would you like to save the configuration default gateway ?

     IP:  10.255.222.1

< Yes                                                                    >
< Exit                                                                   >
```

8. Press **Enter**, then press **Enter** at the next Confirmation Prompt.

```
Configure a network setting

< Configure DNS                                                          >
< Configure NTP                                                          >
< Configure Default Gateway                                              >
< Exit                                                                   >
```

9. Highlight **Exit** and press **Enter** until you return to the Main Menu.

```
Main Menu

< Network Interfaces                                                     >
< Network Routes                                                         >
< Network Services...                                                    >
< Network Settings...                                                    >
< VPN Endpoints...                                                       >
< VA Settings...                                                         >
< Maintenance...                                                         >
< Apply Configuration Changes                                           >
< Logout                                                                 >
```

10. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

```
Main Menu

< Network Interfaces                                                     >
< Network Routes                                                         >
< Network Services...                                                    >
< Network Settings...                                                    >
< VPN Endpoints...                                                       >
< VA Settings...                                                         >
< Maintenance...                                                         >
< Apply Configuration Changes                                           >
< Logout                                                                 >
```

11. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

```
Would you like to apply all configuration ?

Note: VA will restart some services



< OK                                                                     >
< Exit                                                                   >
```

Configure an SSH Service

Configure an SSH Service on the VA to enable an SSH connection to upload the VPN Settings File.

```
Main Menu

< Network Interfaces                                                      >
< Network Routes                                                         >
< Network Services...                                                    >
< Network Settings...                                                    >
< VPN Endpoints...                                                       >
< VA Settings...                                                         >
< Maintenance...                                                         >
< Apply Configuration Changes                                           >
< Logout                                                                 >
```

1. On the Main Menu Screen, highlight **Network Services** and press **Enter**.

```
Network Services

< Show current configuration                                             >
< Configure a network service                                            >
< Delete network services                                                >
< Exit                                                                    >
```

2. Highlight **Configure a Network Service** and press **Enter**.

```
Menu for Configure a network service

Please choose the service

< ssh                                                                     >
< vpn_                                                                    >
< Exit                                                                    >
```

3. With **SSH highlighted,** press **Enter**.

```
Menu for ssh

Please select the IP

    [1] 10.255.222.97
    [2] 10.255.255.98

Please input your option: 1

Enter the port: 2222

< Save                                                                    >
< Exit                                                                    >
```

4. Enter the number corresponding to the address (e.g., 1), and use the Down Arrow to enter the SSH Port Number. Use the Down Arrow to highlight **Save** and press **Enter**.

```
Would you like to save the configuration ?

     IP: 10.255.222.97
     Port: 2222

< Yes                                                                    >
< No                                                                     >
```

5. With **Yes** highlighted, press **Enter** at the Confirmation Prompt.

```
The configuration has been saved successfully!

< OK                                                                     >
```

6. Press **Enter** at the final Confirmation prompt and press **Enter** until you return to the Main Menu.

7. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

```
Main Menu

< Network Interfaces                                                     >
< Network Routes                                                         >
< Network Services...                                                    >
< Network Settings...                                                    >
< VPN Endpoints...                                                       >
< VA Settings...                                                         >
< Maintenance...                                                         >
< Apply Configuration Changes                                           >
< Logout                                                                 >
```

8. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

```
Would you like to apply all configuration ?

Note: VA will restart some services

< OK                                                                     >
< Exit                                                                   >
```

Upload the VPN Settings to the VPN Server

If you have not already done so, you must export the VPN Settings file from your OmniVista Freemium account to your computer. You will then FTP this file to the VPN VA to configure the VPN Service. If you have already exported the VPN Settings to your computer, go to Step 4.

1. Go to the Device Catalog Screen (Network – Device Catalog) of your OmniVista Freemium account.
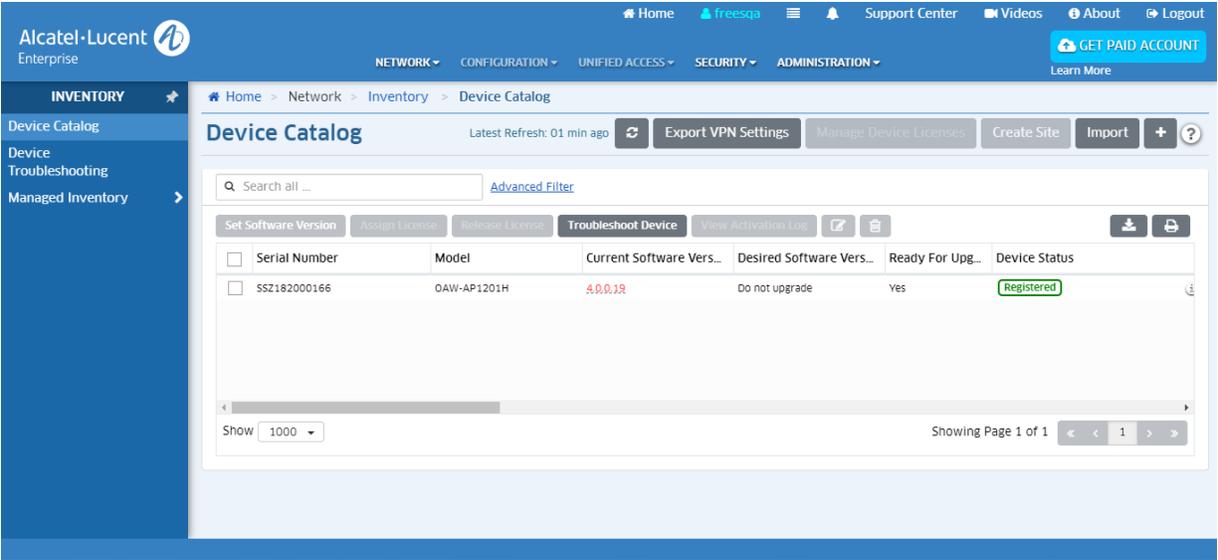
2. Click on the **Export VPN Settings** button at the top of the screen. Note that you do not have to wait until APs reach "Registered" status. Once APs are added to the Device Catalog you can export the VPN settings for the APs.

The file must contain the list of all RAPs (peers) with their IP Addresses and Public Keys as shown below:

```
[Peer]
PublicKey = w7dRCdRmrC7axxxxxx967Yw3iann3sgT+nbX1T3hlA=
AllowedIPs = 10.180.2.7/32
```

3. Select the VPN Settings that you want to use (e.g., LAB4) and click **Export**. The file will be downloaded to your computer (e.g., LAB4.conf).

4. SFTP the VPN Settings File (e.g., LAB4.conf) to the **vpn_profile** Directory (/opt/OmniVista_ 2500_NMS/data/vpn_conf/vpn_profile) on the VPN VA.

>   **Important Note**: Do not change the name of the VPN Settings file.
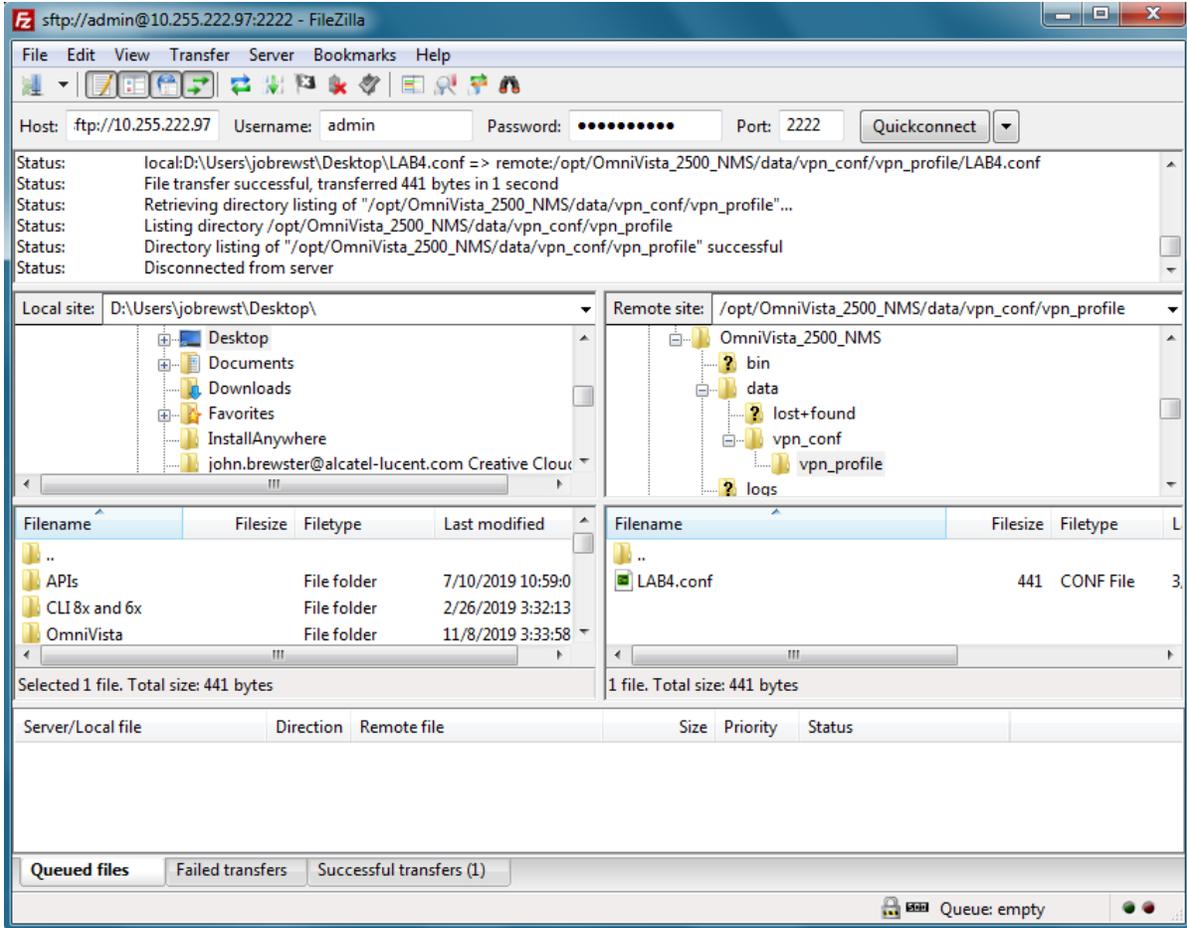
> **Important Note:** Any time you modify VPN settings you must generate a New VPN Settings File and FTP the file to the VPN Server.

Configure the VPN Service

Configure a VPN Management Service on the VA.

1. From the Main Menu, highlight **Network Services** and press **Enter**.

```
Network Services

< Show current configuration                                              >
< Configure a network service                                            >
< Delete network services                                                >
< Exit                                                                    >
```

2. Highlight **Configure a Network Service** and press **Enter**.

```
Menu for Configure a network service

Please choose the service

< ssh                                                                     >
< vpn_                                                                    >
< Exit                                                                    >
```

3. Highlight **VPN** and press **Enter**.

```
Menu for VPN

Please input appended name: vpn_management

Please select the IP

     [1] 10.255.222.97
     [2] 10.255.255.98

Please input your option: 1

Enter the port: 9001

< Save                                                                    >
< Exit                                                                    >
```

4. Enter a name for the service after the underscore (e.g., vpn_management), then use the Down Arrow to select the number of the NIC on which you want to create the service (e.g., 1). This is the NIC of the VPN VA Public IP address. Then use the Down Arrow again to enter the Port Number. This is the port number of the VPN VA Public IP address. Use the Down Arrow to highlight **Save** and press **Enter**.

```
Would you like to save the configuration ?

     Name: vpn_management
     IP: 10.255.222.97
     Port: 9001

< Yes                                                                     >
< No                                                                      >
```

5. Press **Enter**, then press **Enter** at the next Confirmation Prompt. Select **Exit** until you return to the Main Menu.

6. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

```
Main Menu

< Network Interfaces                                                          >
< Network Routes                                                             >
< Network Services...                                                        >
< Network Settings...                                                        >
< VPN Endpoints...                                                           >
< VA Settings...                                                             >
< Maintenance...                                                             >
< Apply Configuration Changes                                               >
< Logout                                                                     >
```

7. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

```
Would you like to apply all configuration ?

Note: VA will restart some services



< OK                                                                         >
< Exit                                                                       >
```

Configure VPN Endpoints

Attach the VPN Settings File to the VPN Service.

```
Main Menu

< Network Interfaces                                                          >
< Network Routes                                                             >
< Network Services...                                                        >
< Network Settings...                                                        >
< VPN Endpoints...                                                           >
< VA Settings...                                                             >
< Maintenance...                                                             >
< Apply Configuration Changes                                               >
< Logout                                                                     >
```

1. From the Main Menu, highlight **VPN Endpoints** and press **Enter**.

```
VPN Endpoints

< Show current configuration                                                >
< Configure a VPN endpoint                                                  >
< Exit                                                                       >
```
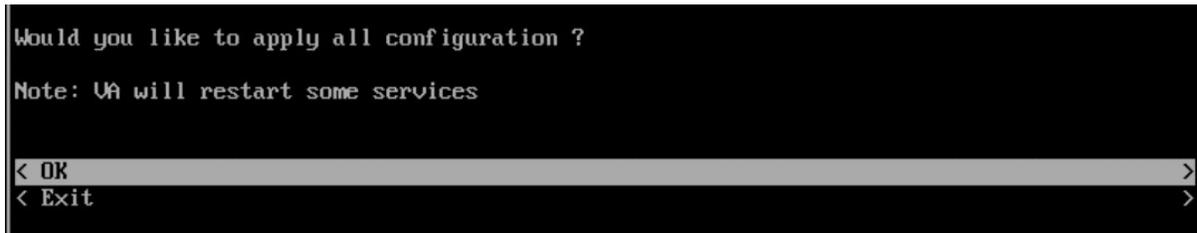
2. Highlight **Configure a VPN Endpoint** and press **Enter**.

```
VPN Endpoints
  <
  <
  < Menu for Configure a VPN endpoint

      Please choose the VPN server configuration
            [1] vpn_management

      Type your option:1

      Please select the configuration file

            [1] LAB4.conf

      Type your option: 1

      Please select interface to enable Layer 2 Data VPN, or None for regular VPN
            [1] eth2
            [2] None (Layer 3 VPN)

      Type your option: 2


      < Save                                                                    >
      < Exit                                                                    >
```

3. Select the number for the **VPN Server Configuration** (e.g., 1 - vpn_management). This is the VPN Service you created in the previous section. Use the Down Arrow to select the **VPN Settings Configuration File** (e.g., 1 - LAB4.conf); then use the Down Arrow to select the interface for Regular VPN (e.g., 2 – None); use the Down Arrow to select **Save**, and press **Enter**.

```
Would you like to save the configuration ?:

      VPN Service name: vpn_LAB4.conf
      Configuration file: LAB4.conf
      Bridge Interfaces: None (Layer 3 VPN)


< Save                                                                          >
< Exit                                                                          >
```

4. Press **Enter** at the next Confirmation Prompt. Select **Exit** until you return to the Main Menu.

5. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

```
Main Menu

< Network Interfaces                                                            >
< Network Routes                                                               >
< Network Services...                                                          >
< Network Settings...                                                          >
< VPN Endpoints...                                                             >
< VA Settings...                                                               >
< Maintenance...                                                               >
< Apply Configuration Changes                                                  >
< Logout                                                                       >
```

6. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

```
Would you like to apply all configuration ?

Note: VA will restart some services


< OK                                                                    >
< Exit                                                                   >
```

Configuring the VPN Data Tunnel

Once the Management VPN tunnel is configured, follow the steps below to configure a VPN Data tunnel. An L2GRE tunnel will be created between the Remote AP and the VPN Server and it will be used to tunnel the remote employee's data traffic.

**1.** Go to **Network –> AP Registration -> Data VPN Server** to add a Data VPN Server.

```
Data VPN Servers

  Edit VPN Server
                                                                              (*) indicates

              Name      VPN_Server_Conf

       Description


  Server's Public IP     195.128.146.179/24          Server's      6550        ∨  ∧
                                                       Port

   Server's VPN IP       192.168.0.1

  Client VPN IP Address Pool
```
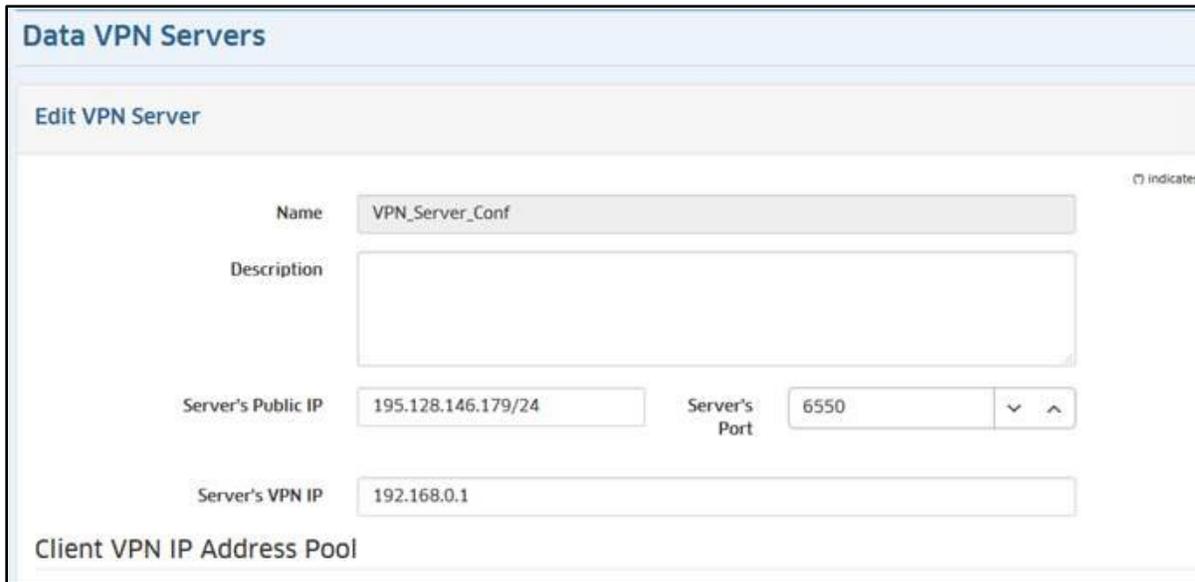
Name	User-configured name for the VPN configuration.
Server's Public IP	The VPN Server's Public IP address (configured when you installed the VPN VA). This is the IP address used by Remote APs to connect to the VPN Server. And this is the interface through which traffic originating from inside the Enterprise Network flows to the Remote site.
Port	The VPN Server Port.
Server's VPN IP	The VPN Server's Private IP address within the virtual network (must be in the same network as the client pool). This is the interface through which traffic originating from the Remote AP flows to reach a destination inside the Enterprise Network.
Client VPN IP Address Pool	The range of addresses available to assign to Remote APs. You can select IP range and insert a range of IP addresses, or a shorthand mask.

2. Go to the AP Group Screen (Network - AP Registration - AP Group) and edit the AP Group used to manage Remote APs.
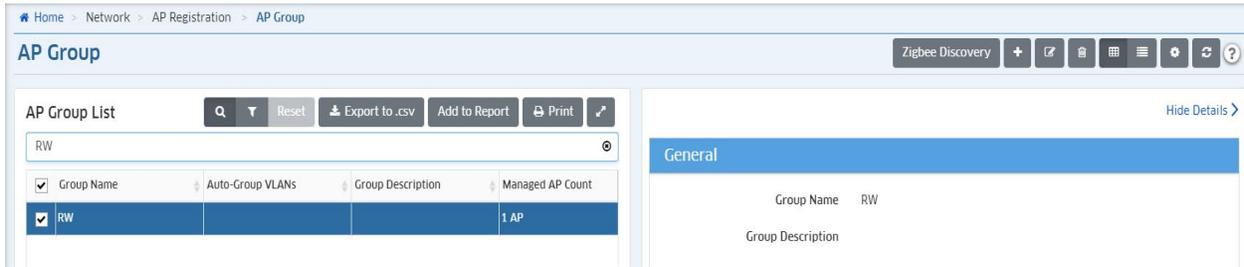
3. Assign the Data VPN Server to the AP Group (mandatory to set up the Data VPN Tunnel).
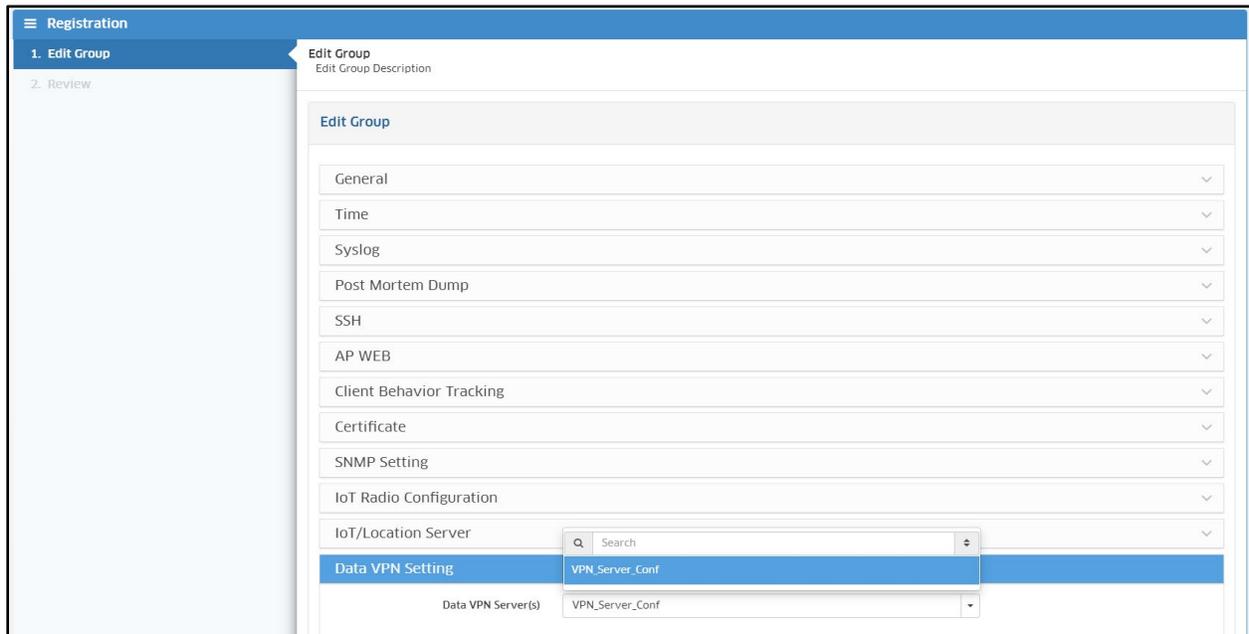
4. Go to the Data VPN Servers Screen and click on the **Export VPN Settings** button.

5. Select the VPN Settings that you want to use and click **Export VPN Settings**. The file will be downloaded to your computer. The file must list all RAPs with their IP Addresses and Public Keys as shown below:

```
[Peer]
PublicKey = opNxg1UpN2Pv/9S2HaxxxxxyfJYAIbOHSRDo78r+To=
AllowedIPs = 192.168.1.2/32
```

6. SFTP the VPN Settings File to the **vpn_profile** Directory (/opt/OmniVista 2500_NMS/data/vpn_conf/vpn_profile) on the VPN VA. See Upload the VPN Settings to the VPN Server.

> **Note**: Do not change the name of the VPN Settings file.

7. Configure the VPN service for Data Tunnel.

```
Menu for UPN

Please input appended name: vpn_data

Please select the IP

    [1] 10.255.222.97
    [2] 10.255.255.98

Please input your option: 1

Enter the port: 9002

< Save                                                              >
< Exit                                                              >
```

8. Configure VPN Endpoints. Be sure to select the right ethernet interface for bridging traffic (e.g., eth2 without IP Address).

Configure VPN Endpoints

Attach the VPN Settings File to the VPN Service.

```
Main Menu

< Network Interfaces                                                >
< Network Routes                                                    >
< Network Services...                                               >
< Network Settings...                                              >
< UPN Endpoints...                                                 >
< UA Settings...                                                   >
< Maintenance...                                                   >
< Apply Configuration Changes                                      >
< Logout                                                           >
```

1. From the Main Menu, highlight **VPN Endpoints** and press **Enter**.

```
UPN Endpoints

< Show current configuration                                       >
< Configure a UPN endpoint                                         >
< Exit                                                             >
```

2. Highlight **Configure a VPN Endpoint** and press **Enter**.

```
Menu for Configure a VPN endpoint

Please choose the VPN server configuration
     [1] vpn_data
     [2] vpn_management

Type your option:1

Please select the configuration file

     [1] LAB4.conf
     [2] VPN_Server_Conf.conf

Type your option: 2

Please select interface to enable Layer 2 Data VPN, or None for regular VPN
     [1] eth2
     [2] None (Layer 3 VPN)

Type your option: 1



< Save                                                                        >
< Exit                                                                        >
```

3. Select the number for the **VPN Server Configuration** (e.g., 1 - vpn_data). This is the VPN Service you created in the previous section. Use the Down Arrow to select the **VPN Settings Configuration File** (e.g., 2 – VPN_Server_Conf.conf); then use the Down Arrow to select the interface for bridged traffic (e.g., 1 – eth2); use the Down Arrow to select **Save**, and press **Enter**.

```
Would you like to save the configuration ?:

     VPN Service name: vpn_data
     Configuration file: VPN_Server_Conf.conf
     Bridge Interfaces: eth2


< Save                                                                        >
< Exit                                                                        >
```

4. Press **Enter** at the next Confirmation Prompt. Select **Exit** until you return to the Main Menu.

5. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

```
Main Menu

< Network Interfaces                                                          >
< Network Routes                                                             >
< Network Services...                                                        >
< Network Settings...                                                        >
< VPN Endpoints...                                                           >
< VA Settings...                                                             >
< Maintenance...                                                             >
< Apply Configuration Changes                                               >
< Logout                                                                     >
```

6. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

```
Would you like to apply all configuration ?

Note: VA will restart some services


< OK                                                                    >
< Exit                                                                  >
```
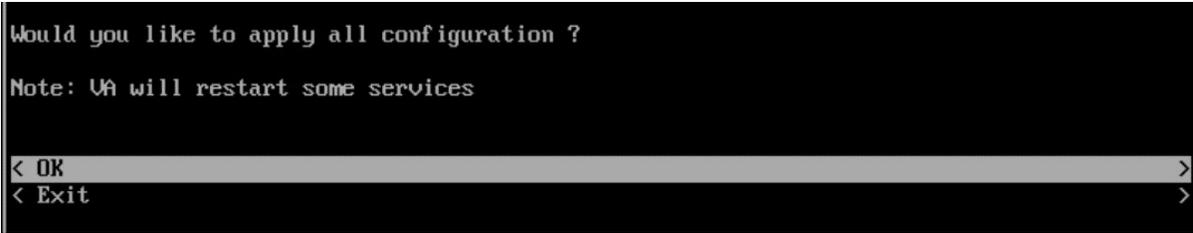
Create an SSID for the VPN Data Tunnel

Once the VPN Data tunnel is configured an SSID and Access Role Profile must be created to tunnel the user traffic. For example:

1. Create an SSID.

```
> Select WLAN > SSIDs > SSIDs
  > Click on the + button
    > SSID Service Name: EmployeesX (X = R-Lab number)
    > SSID: <filled automatically>
    > Usage: Enterprise Network for Employees (802.1X)
    > Click on Create & Customize

    > Allowed Band: All
    > Encryption Type: WPA3_AES

Default VLAN/Network:
VLAN(s): untagged
Use Tunnel: checked
Tunnel ID:0
GRE Tunnel Server IP Address/data VPN Server: select profile created at previous section
Support of Entropy: Disabled
Allow Local Breakout: Disabled (will be supported with AWOS 4.0.1)

Authentication Strategy
> RADIUS Server: UPAMRadiusServer
> Click on Manage Employee Accounts

// Employee account creation //
> Click on the + button
  > Username: Employee
  > Password: password
  > Click on Create
> Click on Close
```

2. Select the SSID and AP Group, save and apply.

SSID Service Name	Employees0 ▼
SSID	Employees0
AP Group(s)	1 selected AP Group(s) [Change Selection]
	☑ Set same schedule for all selected AP Groups | Edit Schedule ⧉ ⓘ
	🔍 Search all ...
	default group ⓘ
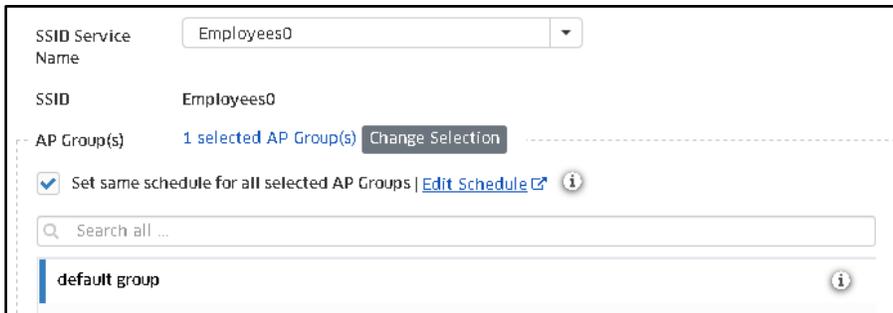
3. OmniVista 2500 will push the configuration to the Remote Access Point allowing users to connect to the SSID just configured.
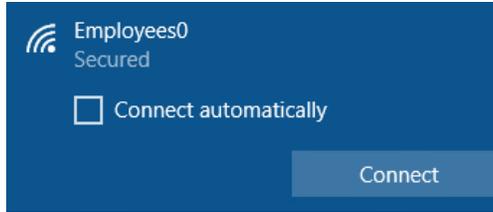
SSID with Tagged VLAN

To configure an SSID with a tagged VLAN, configure the VLAN fields in the SSIDs application as shown in the example below.
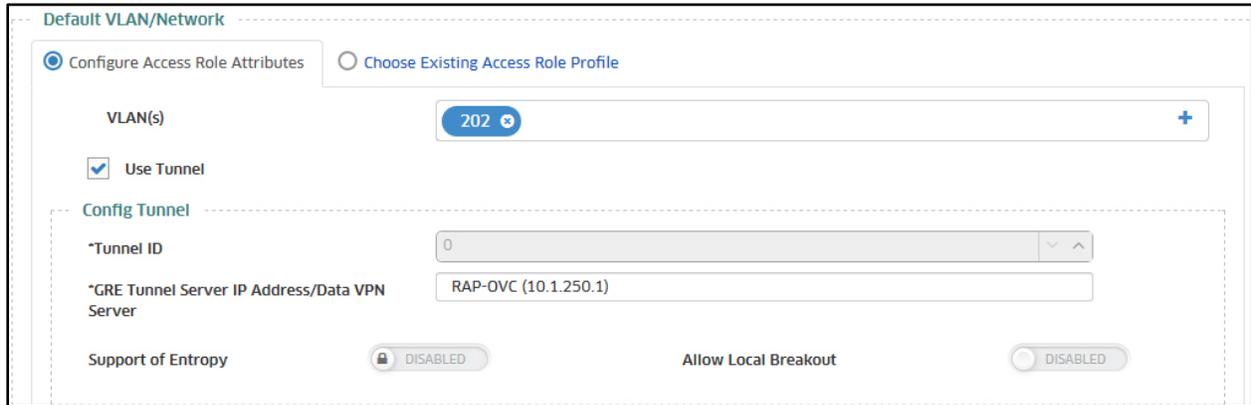
SSID with Untagged VLAN

To configure an SSID with an untagged VLAN, configure the VLAN fields in the SSIDs application as shown in the example below.
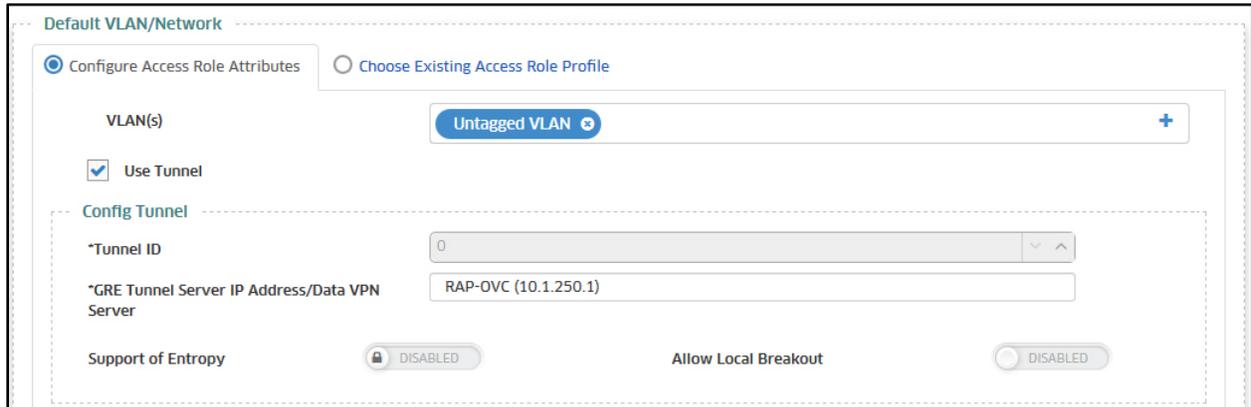
Configuring Switches for Tagged/Untagged Traffic

The CLI Commands below are used to configure AOS 8.x and AOS 6.x Switches for tagged and untagged traffic.

- **AOS 8.x**

  - For Tagged VLAN: `vlan [vlan_num] member port/linkagg [port_num/agg_num] tagged`

  - For Untagged VLAN: `vlan [vlan_num] member port/linkagg [port_num/agg_num] untagged`

- **AOS 6.x**

  - For Tagged VLAN: `vlan [vlan_num] 802.1q [port_num/ agg_num]`

  - For Untagged VLAN: `vlan [vlan_num] port default [port_num/agg_num]`

SSID with Local Breakout

To configure an SSID with an Local Breakout, configure the VLAN fields in the SSIDs application as shown in the example below.
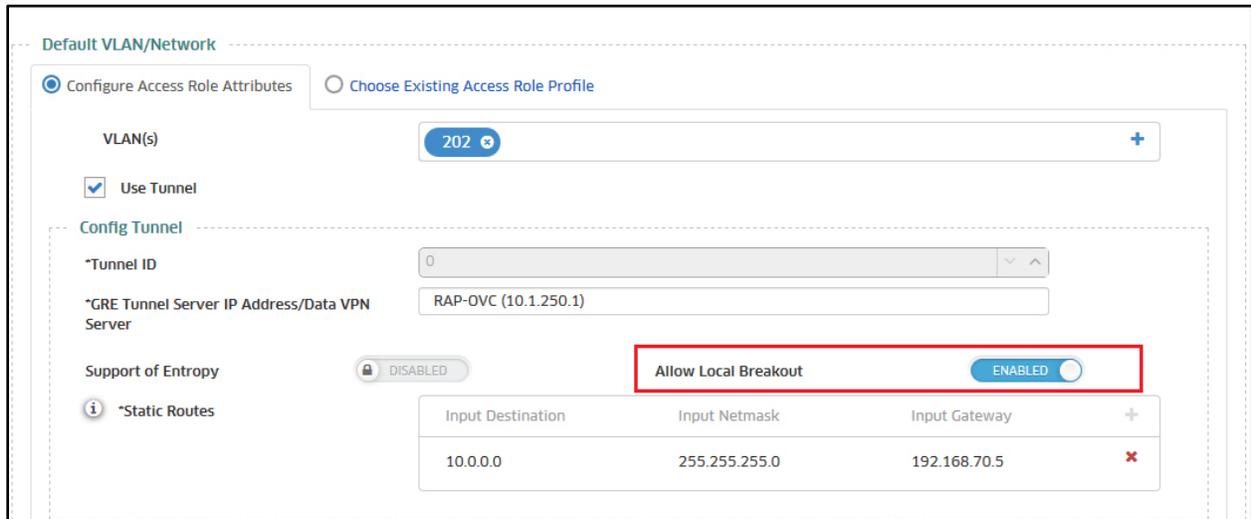
- **Allow Local Breakout -** Enables/Disables Local Breakout on the tunnel. If enabled, enter the Static Route(s) to be used for entering the Tunnel. All other traffic will go out through the local network. Make sure you have applied the relevant Data VPN Server to AP Groups in the SSID before choosing Data VPN Server as the Tunnel endpoint. To apply a Data VPN Server to an AP Group, go to the AP Groups page (Network - AP Registration - AP Group) and edit the Data VPN Setting for the group. Note that only one VLAN inside the tunnel (tunnel ID must be set to 0) can be enabled with Local Breakout.

- **Static Routes -** Specify the static routes to be used for entering the tunnel. All other traffic will go out through the local network.

  - Avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the Tunnel. For example, if VLAN ID = 41 is specified to be carried within the Tunnel and if the network subnet that corresponds to VLAN 41 is 192.168.41.0, the AP will automatically set up this route and make sure traffic destined for 192.168.41.0 will enter the Tunnel. The AP will automatically set up this route and make sure traffic with VLAN ID = 41 will enter the Tunnel. Do not specify an explicit Route with Destination = 192.168.41.0, as that will confuse the AP and lead to poor performance.

- The static routes specified will be accumulated on an AP across all SSIDs assigned to the AP. For example, if you have two SSIDs configured on the same AP and configure SSID1 to use Tunnel Profile T1 with Static Routes A and B, and configure SSID2 to use Tunnel Profile T2 with Static Routes C and D, all of the routes (A, B, C, and D) will be applicable for SSID 1 and SSID 2.

- Across all of the routes applied on an AP from the different SSIDs, make sure any destination IP subnet is specified only once. Each route applied on an AP should be for a different IP subnet, even across the SSIDs. Also, avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the tunnel. The AP will automatically set up such routes. If a route to IP subnet X already exists in an SSID and that SSID is applied to an AP, another route to the same IP subnet X must not be specified in the same or a different SSID that is applied to the same AP.

    Note: Local Breakout troubleshooting tips can be found in the Basic Troubleshooting Checklist.

Creating a Tunnel Profile for 1201H Downlink Ports

1. Create a Tunnel Profile in Unified Access in OmniVista (Unified Access – Template - Tunnel Profile).

2. Go to the Access Role Profile Screen (Unified Access – Template – Access Role), select the Tunnel Profile you created in Step 1, and apply the profile to the AP Group with Mapping method: "Map to VLAN and Tunnel".
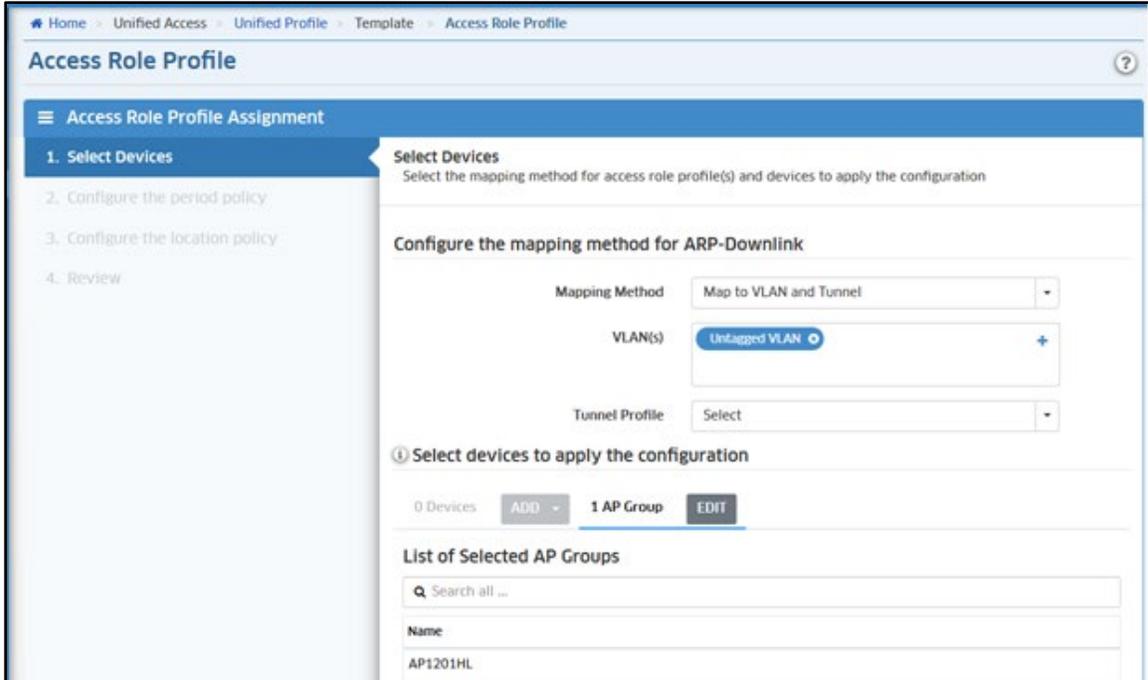
3. Create an Access Authentication Profile (Unified Access – Template – Access Auth Profile) and apply it to the AP (AP Group).

Configuring an Access Auth Profile for an AP Downlink Port

If you have a Premium or Business Account, you can assign an Access Auth Profile to a Downlink Port on Stellar AP1201H, AP1201HL, and AP1311 Devices. Profiles are displayed/configured on the OmniVista Access Auth Profile Screen (Unified Access – Unified Profile – Template – Access Auth Profile).

1. Create a profile in the Access Auth Profile Table and click on the **Apply to Devices** button.

2. On the Access Auth Profile Assignments Window (see below) click on the **ADD/EDIT** button next to **AP Group** and select an AP Group(s).

3 When assigning the profile to an AP Group, you can select an Ethernet port(s) (up to 3 ports, depending on the AP model – Eth1, Eth2, Eth3). OmniVista will apply the profile to the selected ports on supported APs/ports in the AP Group, and ignore unsupported APs/ports in the Group.
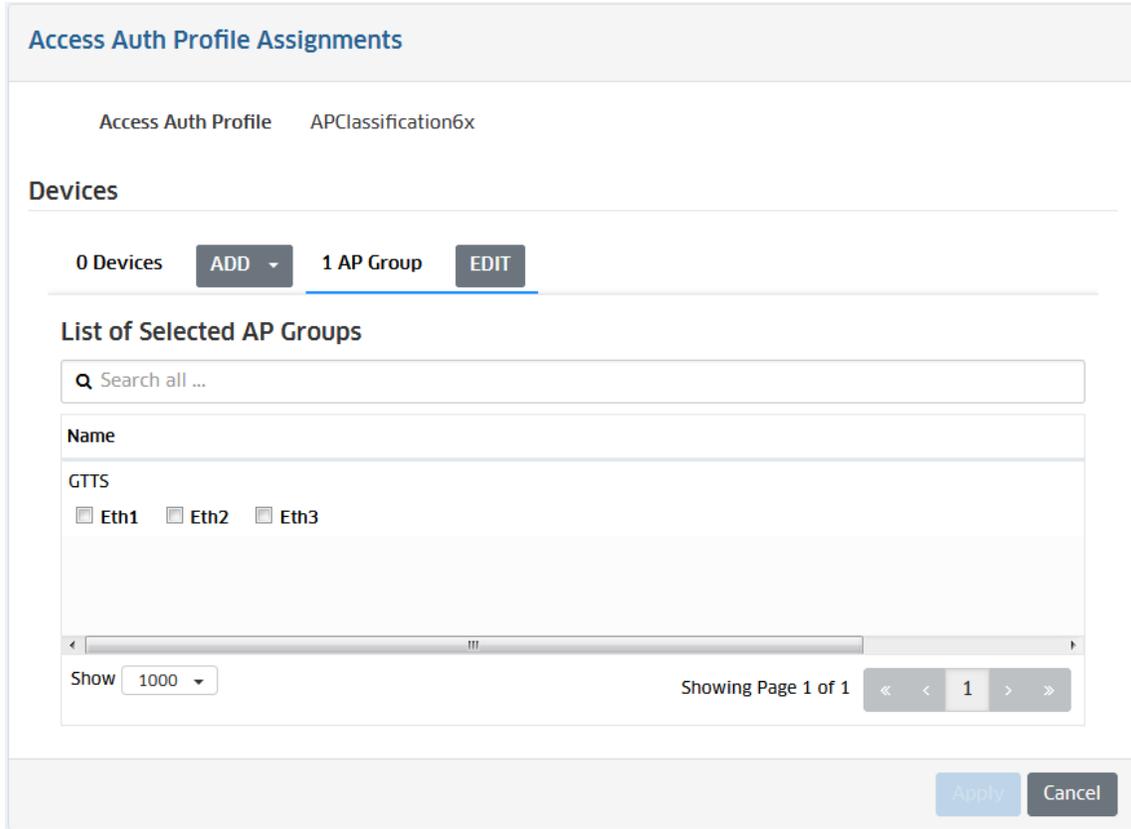
Add a Route to Reach the VPN VA from OmniVista

1. On The Virtual Appliance Menu, select **2 – Configure the Virtual Appliance** to bring up the Configure The Virtual Appliance Menu.

```
*******************************************************************************
* Configure The Virtual Appliance                                            *
*******************************************************************************
* [1] Help                                                                   *
* [2] Display Current Configuration                                          *
* [3] Configure IPs and Ports                                                *
* [4] Configure Default Gateway                                              *
* [5] Configure Hostname                                                     *
* [6] Configure DNS Server                                                   *
* [7] Configure Timezone                                                     *
* [8] Configure Route                                                        *
* [9] Configure Network Size                                                 *
* [10] Configure Keyboard Layout                                             *
* [11] Update OmniVista Web Server SSL certificate                           *
* [12] Enable/Disable AP SSL Authentication                                  *
* [13] Enable/Disable Admin SSH                                              *
* [14] Configure NTP Client                                                  *
* [15] Configure Proxy                                                       *
* [16] Change screen resolution                                             *
* [17] Configure the other Network Cards                                     *
* [0] Exit                                                                   *
*******************************************************************************
(*) Type your option: _
```

2. Select **8 – Configure Route**.

```
*******************************************************************************
* Configure Route                                                            *
*******************************************************************************
* [1] Help                                                                   *
* [2] Show Current Routes                                                    *
* [3] Add Route v4                                                           *
* [4] Del Route v4                                                           *
* [0] Exit                                                                   *
*******************************************************************************
(*) Type your option: _
```

3. Select **3 – Add Route v4** to add the route. OmniVista should reach the NIC that the VPN VA used to connect to the corporate network (e.g., 10.255.255.0/24).

```
*******************************************************************************
* Configure Route                                                            *
*******************************************************************************
* [1] Help                                                                   *
* [2] Show Current Routes                                                    *
* [3] Add Route v4                                                           *
* [4] Del Route v4                                                           *
* [0] Exit                                                                   *
*******************************************************************************
(*) Type your option: 3
(*) Please input subnet: 10.255.255.0
(*) Please input netmask: 255.255.255.0
(*) Please input gateway: 192.168.71.1
Would you like to add a route:
        subnet: 10.255.255.0
        netmask: 255.255.255.0
        gateway: 192.168.71.1
[y|n] (y):
The configuration has been set
Press [Enter] to continue
```

4. Select **2 - Show Current Routes** to review the configuration.

```
****************************************************************************
* Configure Route                                                         *
****************************************************************************
* [1] Help                                                                *
* [2] Show Current Routes                                                 *
* [3] Add Route v4                                                        *
* [4] Del Route v4                                                        *
* [0] Exit                                                                *
****************************************************************************
(*) Type your option: 2
Current routes:
Route Route 1: 10.255.255.0/255.255.255.0 via 192.168.71.1
```

Using Dual Stack Lite ISP Connections with Stellar RAPs

In the following network topology, the ISP router is using Dual Stack Lite (DS-Lite) technology:
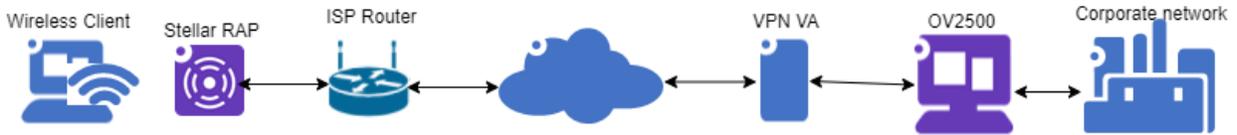
When configuring a RAP network that interacts with a DS-Lite router, the following general configuration guidelines are recommended:

	TCPMSS		
	GRE	**WG**	**WG + DS-Lite**
Management VPN Profile	N/A	1380	1352
Data VPN Profile	N/A	1380	1300
	MTU		
	GRE	**WG**	**WG + DS-Lite**
Data VPN/GRE Tunneling	1500	1546	1376

The above values can be modified as follows:

- **Management VPN Profile TCPMSS** – edit on the OV Cirrus Freemium VPN Servers screen.
- **Data VPN Profile TCPMSS** – edit on the OV 2500/OV Cirrus Data VPN Servers screen (Network – AP Registration – Data VPN Server).
- **Data VPN/GRE Tunneling MTU** – edit on the OV 2500/OV Cirrus SSIDs screen (WLAN – SSIDs).

Upgrading the VPN VA

The sections below detail upgrading the VPN on [VMware](#) and [Hyper-V](#). If you have configured a VPN for Remote Access APs, backup VPN Settings Files at the following directory: */opt/OmniVista_2500_NMS/data/vpn_conf/vpn_profile* **before** upgrading.

Upgrading on VMware

This section documents an example of upgrading on VMware from version 4.6R2 to 4.7R1. The steps are the same for later upgrades.

1. Take a snapshot of the current VA.
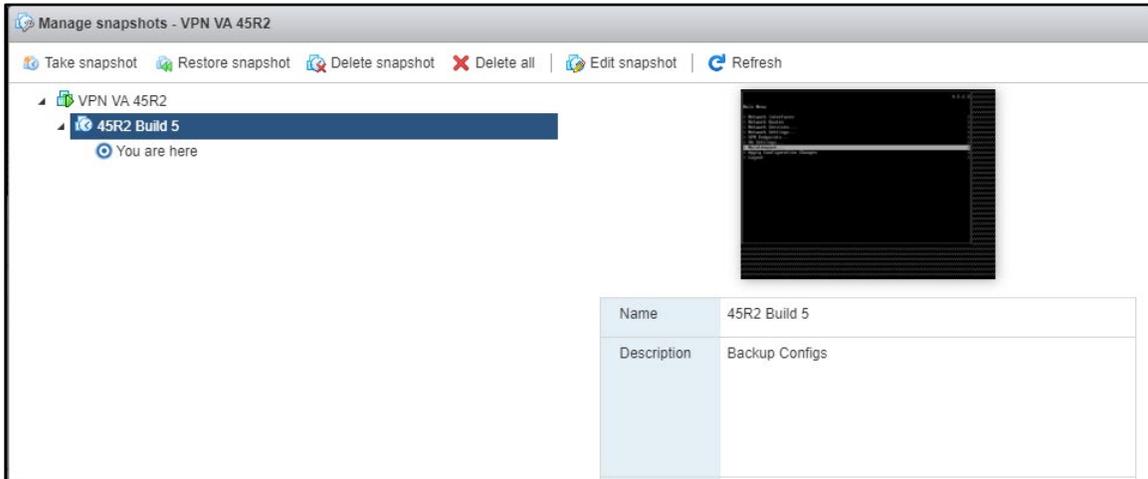
2. Power off the existing VA (e.g., VPN VA 46R1).
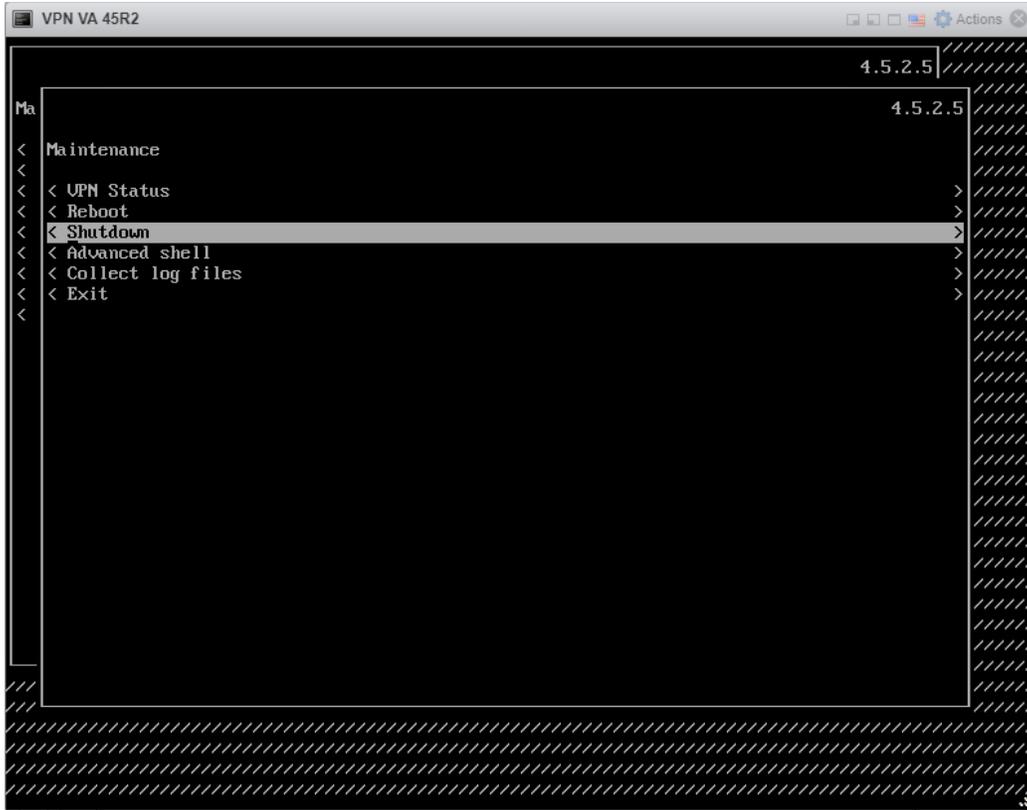
3. Deploy a new OVF template using the new version files (e.g., 45R3 Build 1).
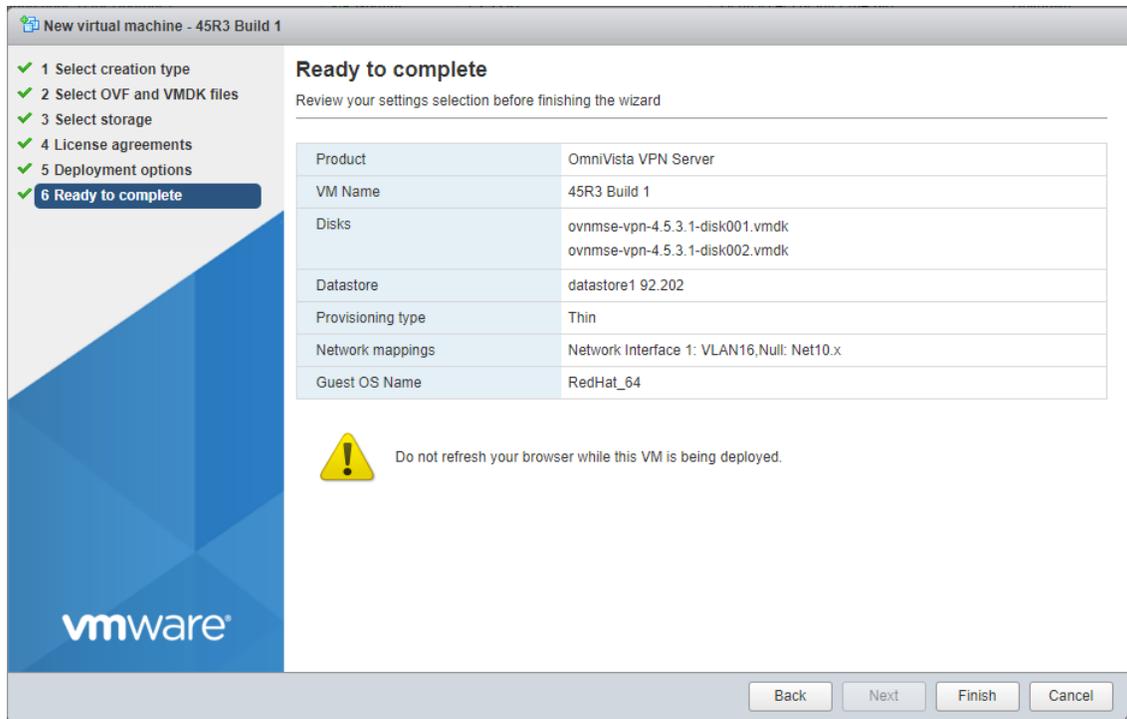
4. Copy the OS virtual disk file to the location of current VA (VPN VA 45R2). On the VMWare ESXi web client, click "Datastore browser".
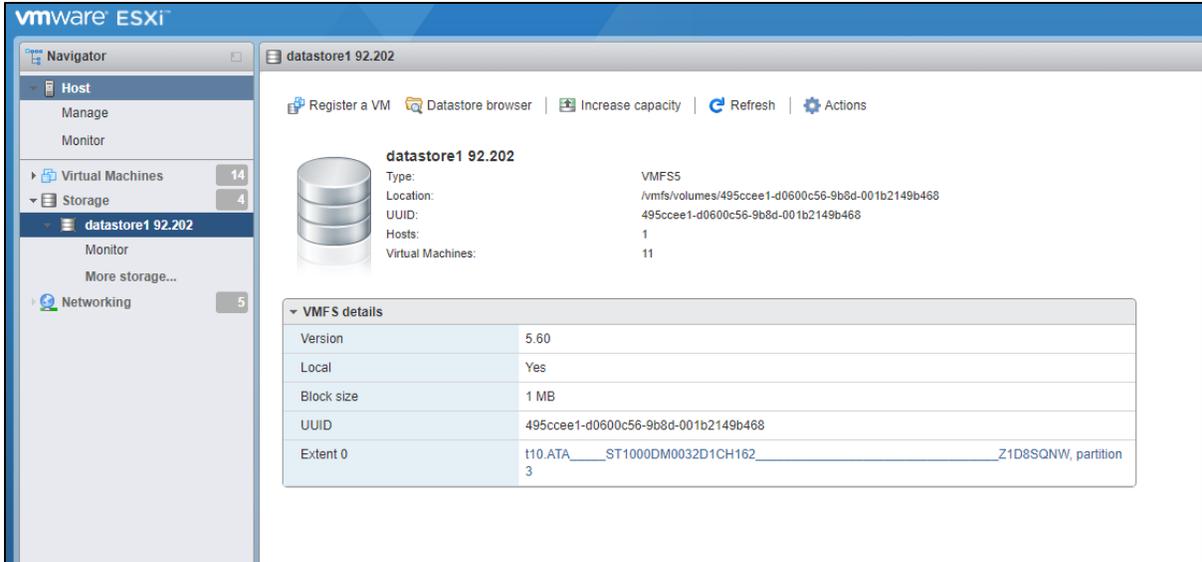
a. In the Datastore browser, highlight the upgrade file (e.g., 45R3 Build 1.vmdk)
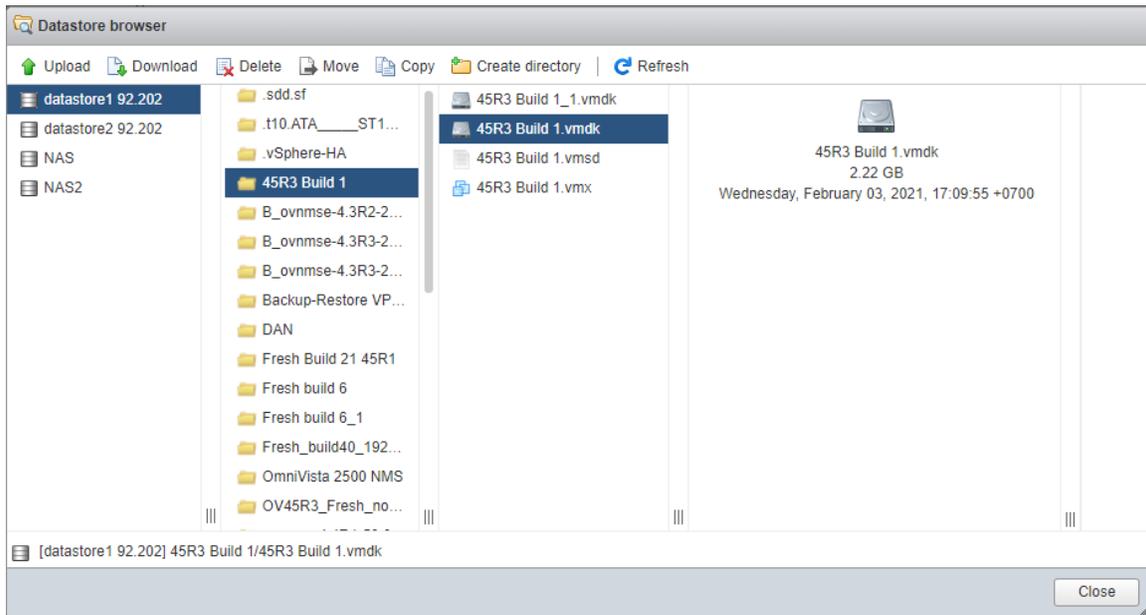
b. Click "Copy" and select the destination folder (e.g., VPN VA 45R2).
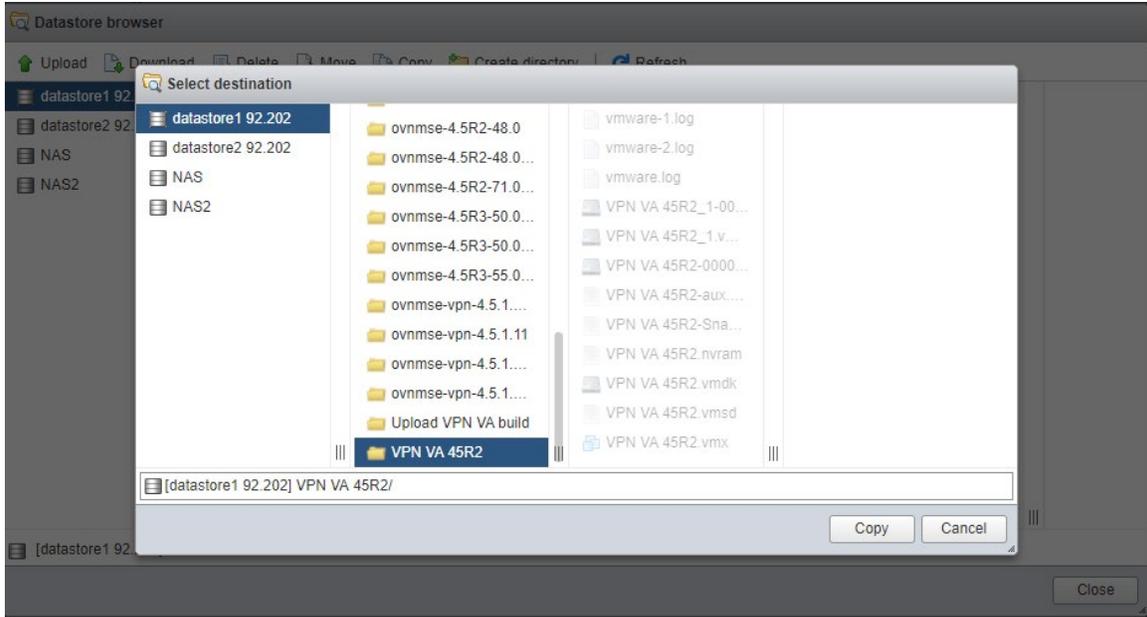
c. Verify the copy.
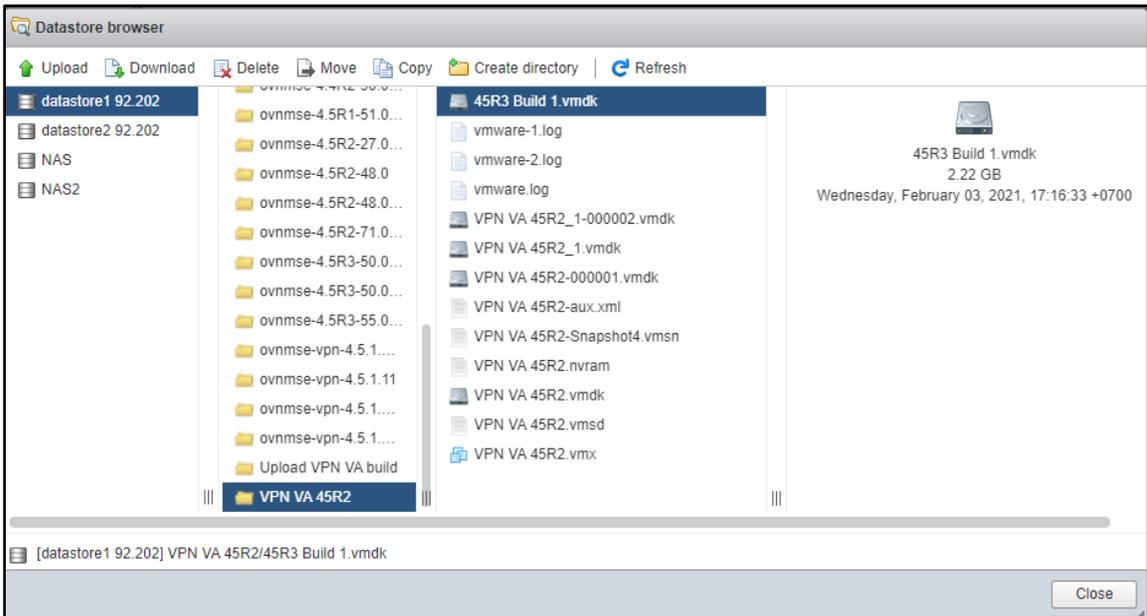
5. Remove Hard Disk 1, IDE controller 0 disk from the current VA. In the VMWare ESXi Web Client, edit the existing VA, remove HD1 and check "Delete files from database" then click **Save**.
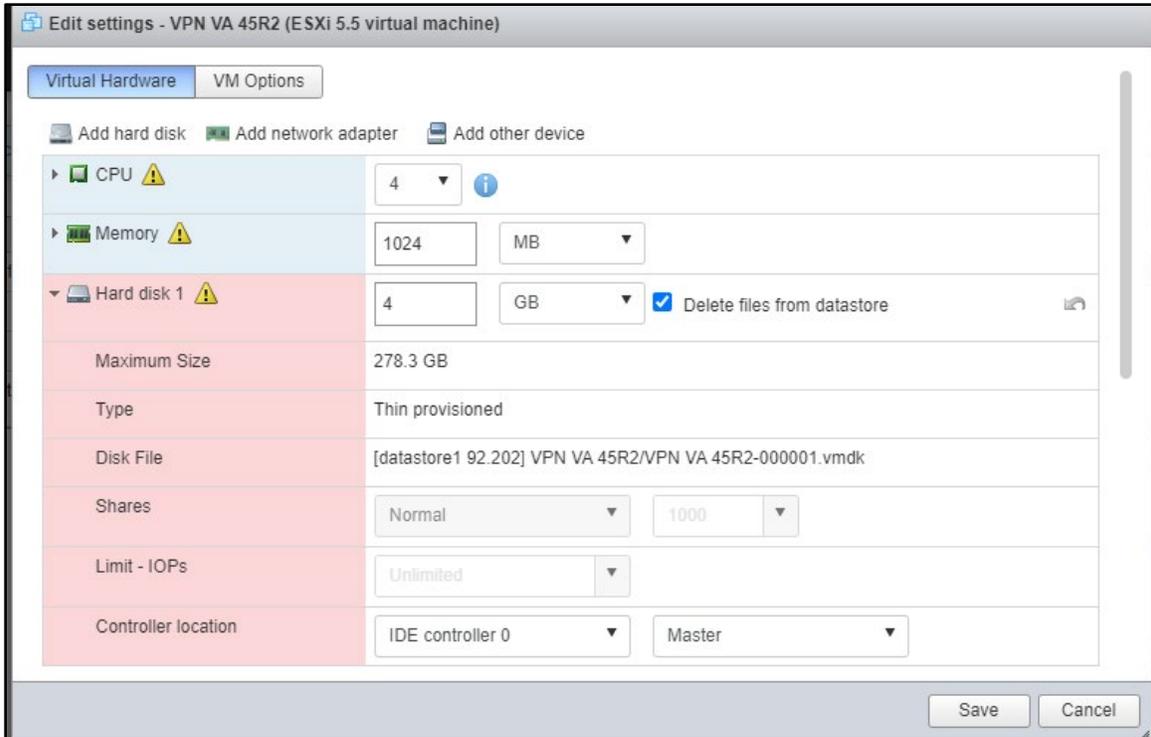
Note: Make sure you only remove hard disk 1 (this is the. vmdk snapshot file that we created in Step 1). Do not delete the original hard disk on the location of the current VA in the datastore browser. If you delete the original hard disk in the first deployment, you may get an error when you revert snapshot files.

6. Recreate the disk with new copied virtual disk file.

> **a.** Edit the existing VA. Got to **Virtual Hardware** - **Add hard disk** - **Existing hard disk**.
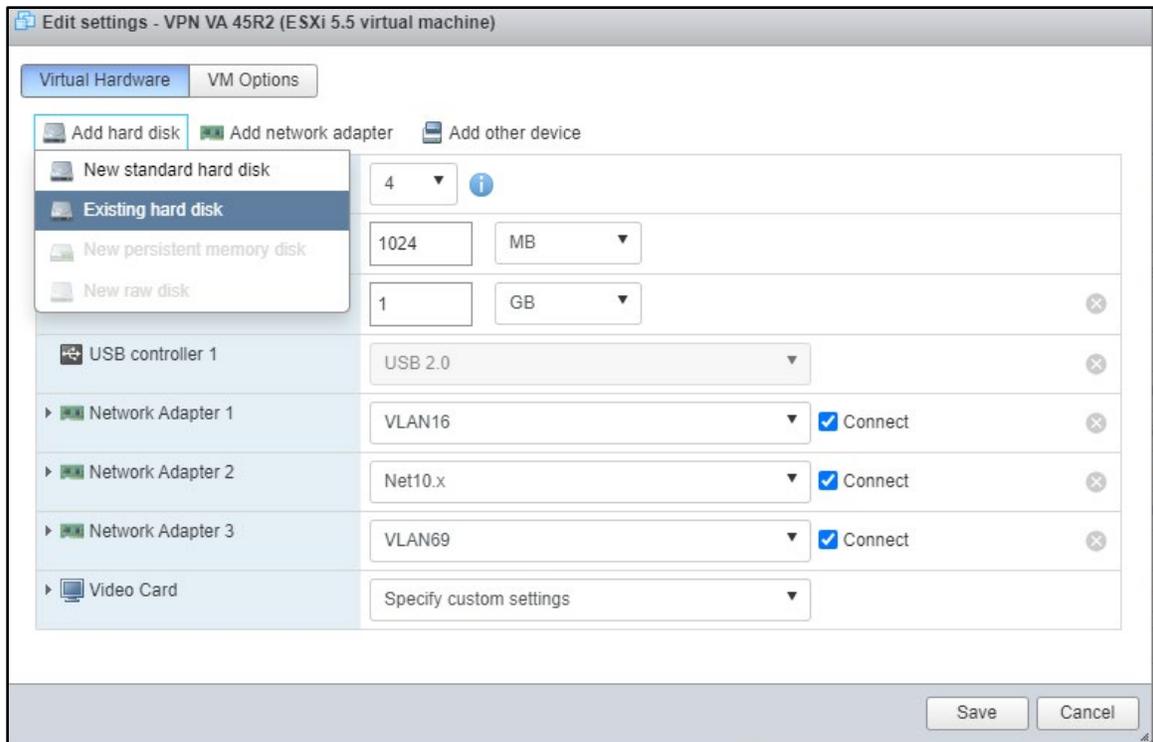
b. Select the virtual hard disk file (e.g., 45R3 Build 1.vmdk).
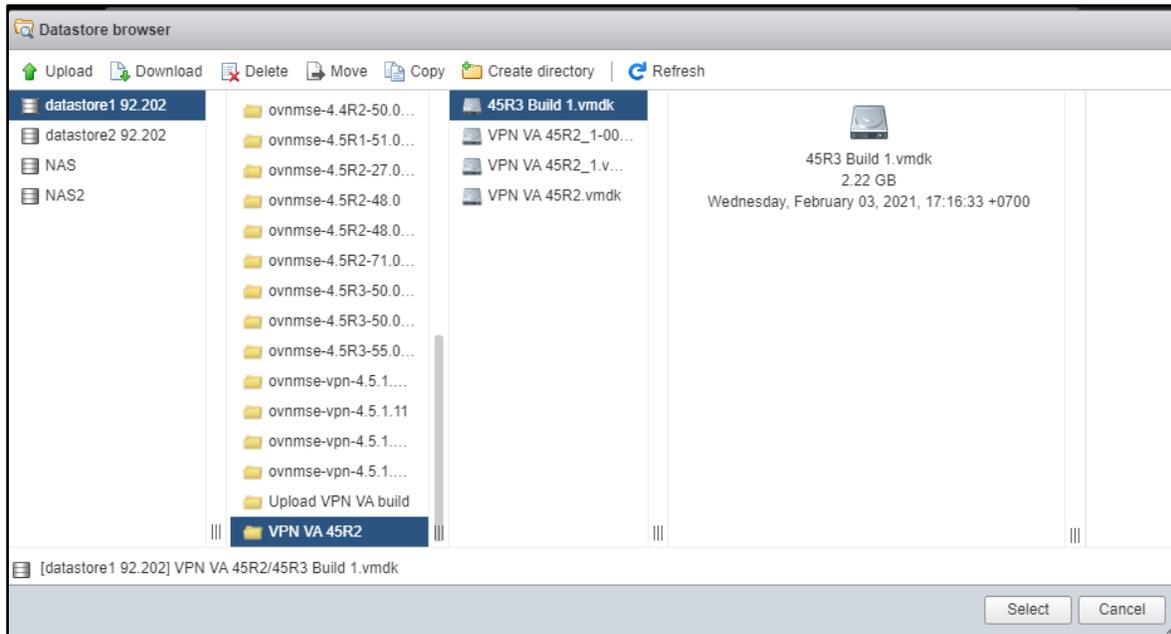
c. Make sure the New Hard disk is set as "IDE controller 0" – "Master". then click **Save**.

7. Power on the VA (e.g., VPN VA 45R2).

Upgrading on Hyper-V

1. Shutdown the VPN server from the VPN VA menu.

2. Extract the new VPN VA files.

**3.** Copy the OS virtual disk file from folder new VPN_VA\hyperv\Virtual Hard Disks to the location of the current VA (OmniVista-VPN-4.5.1).

To the location of the current VA.

4. Edit the existing VA. Select the **Virtual hard disk** radio button. Click on the **Browse** button to browse hard disk 1 to locate the new OS hard disk image, then click on the **Apply** button.
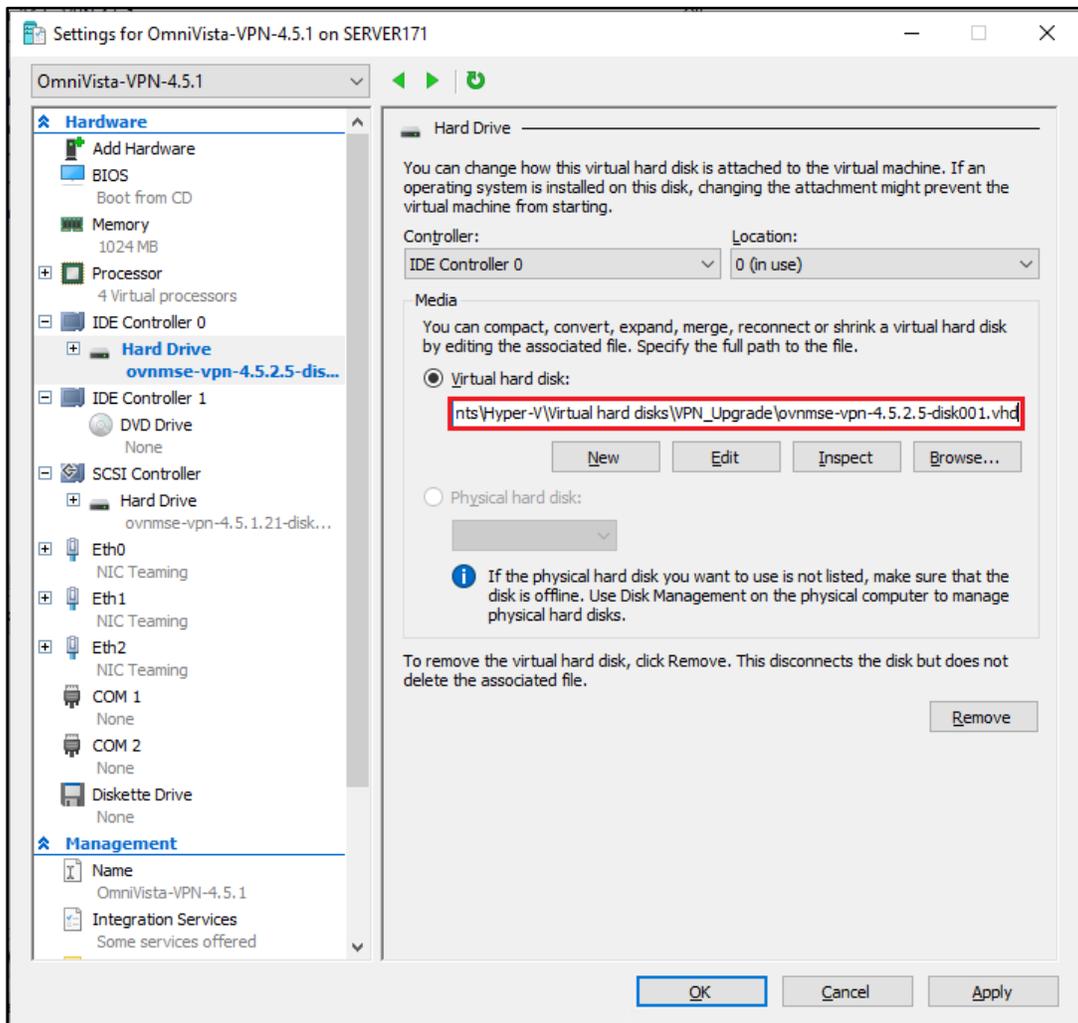
5. Restart the VA.
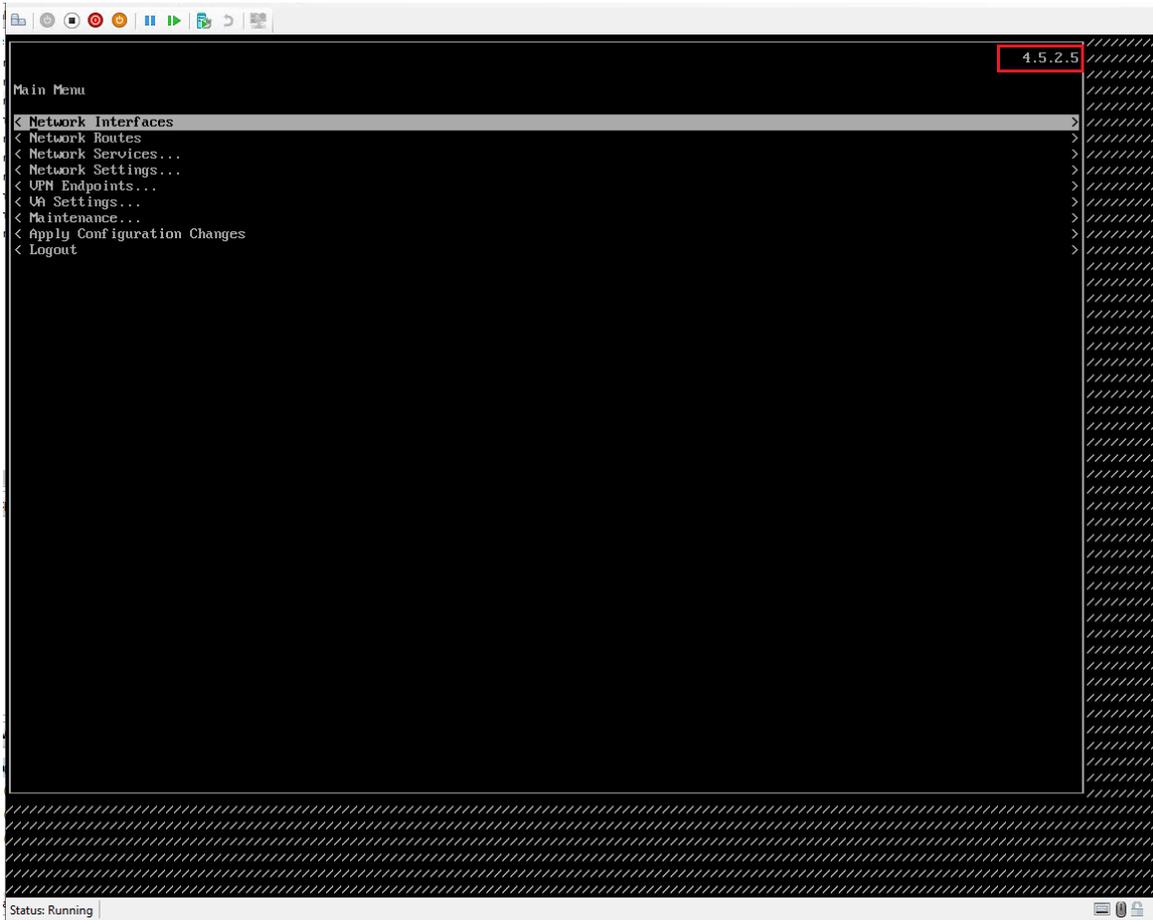
Basic Troubleshooting Checklist

- If the AP Management VPN Tunnel is down:
  - Check if tunnel interface was created using command "wg" on VPN VA (we assume we cannot action this command on RAP because it is not reachable).
  - Verify that the AP's IP Address is present in the VPN.conf file imported to VPN-VA.
  - Verify that the firewall is not blocking traffic in both ways (from outside company, from VPN-VA).
- If the AP Management VPN Tunnel is UP but AP is not registered in OV:
  - Check if you can ping the AP's IP Address from OV.
  - Check if you have configured the static route on OV for AP wg0 IP subnets.
- If AP Data VPN Tunnel is down:
  - Check if the tunnel interface was created by using command "wg" on VPN VA and on RAP. At this stage, the VPN config must be pushed to AP in /tmp/config/datavpn.conf.
  - Check the Data VPN Server is mapped to respective AP Group.
  - check if the AP has received IP on wg1 interface with command "ifconfig wg1".

- Check that the IP Address is present in the Data-VPN.conf file imported to VPN-VA.

- Verify that the firewall is not blocking traffic in both ways (from outside company, from VPN-VA).

- If both tunnels are UP but client does not get DHCP lease:

  - Check if the client is present in the AP association list with command "ssudo sta_list" and he mapped to the tunnel ID of the Data VPN Server, command "brctl show" could be action to have additional information (ath0x interface must be associated to br-g1 interface).

  - Check if the Client's MAC Address is learnt on the corporate access switch where we bridge the traffic.

  - Check the switch config for DHCP replay (ip helper, dhcp-snooping).

- If client is not able to access LAN network:

  - Client is not able to ping any device or gateway within same subnet. Make sure that Promiscuous Mode is enabled and set to "Accept" on the vswitch (by default this is set to reject).

  - Promiscuous Mode is enabled but it is not working. Check if the Override checkbox is disabled. If enabled ensure the setting is set to "Accept".

Useful Logs and Commands

- Collect VPN VA logs from VA menu.
- Collect RAP logs from OmniVista (OVE or OVC) –> Administration –> Audit –> Collect Support Info.
- Check if RAP received DATA Management config files from OV Cirrus.
  - cat /etc/config/rap.conf
- Check if RAP received DATA VPN config files from OVE or OVC.
  - cat /var/config/datavpn.conf
- Check the **sta_list**, **wg show** and **ip -d link** command outputs.

  For **sta_list** output, check the TUNNELID and FARENDIP of the VPN VA Server.

STA_MAC	IPv4	IPv6	OnlineTime
b0:72:bf:d0:63:de	172.28.1.51	fe80::8389:64ed:fbd4:e730	8

RX	TX	FREQ	AUTH	Final_role	VLANID	TUNNELID	FARENDIP
4237	5860	5GHz	PSK	__RAP3	0	0	DVPN-132

For **wg show** check the public key, listening port, peer endpoint, allowed ips, the time since handshake and that transfer and received are incrementing.

root@AP-D2:00_RAP2:~# wg show

interface: wg0

  public key: BOpBbWqvxFKEZ8gAVJACaVY4Lp5d6cKSK5y1+QH05i4=

  private key: (hidden)

  listening port: 58161

peer: hfbchhiCJHOZz5UMh1BVbvDfWqRICpgwm7I1o6Jh1QI=

  endpoint: 198.206.185.132:9093

  allowed ips: 172.16.198.254/32, 172.20.0.155/32

  latest handshake: 3 seconds ago

  transfer: 267.09 KiB received, 625.22 KiB sent

  persistent keepalive: every 5 seconds

For **ip -d** link check that the interfaces gre0, gretap0, wg0 are present with an MTU lower than 1500.

root@AP-D2:00_RAP2:~# ip -d link

…

gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN mode DEFAULT group default

  link/gre 0.0.0.0 brd 0.0.0.0 promiscuity 0

  gre remote any local any ttl inherit nopmtudisc

gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN mode DEFAULT group default qlen 1000

  link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff promiscuity 0

  gretap remote any local any ttl inherit nopmtudisc

wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN mode DEFAULT group default

  link/none promiscuity 0

  wireguard

Local Breakout Troubleshooting

The following scenarios may be encountered when enabling the Local Breakout function if certain configurations are incorrect.

AP May Get Improper DNS Server IP Address

Problem Description: After enabling Local Breakout, an AP will get an IP address from Corporate HQ, which also contains the DNS server IP. This DNS server IP will cause problems with the AP.

Example:

An AP powers up, gets its IP address and DNS Server IP address "A" from its local network, and registers with OVC. The AP gets the Data VPN configuration with Local Breakout enabled from OVC, and the AP gets its IP address and DNS Server IP address "B" from the Corporate HQ via data tunnel.

At this moment, the AP has two DNS Server IP addresses - A and B. When the AP tries to access OVC'FQDN, it will randomly use DNS Server A or B. If DNS Server B cannot resolve OVC'FQDN, the AP will be down in OVC.

Solution:

Configure the correct Corporate HQ DNS Server.

Client May Get Improper DNS Server IP Address

Problem Description: After enabling Local breakout, a client will get its IP address from Corporate HQ which also contains a DNS Server IP address. The DNS Server IP may affect the client Internet access speed.

Example 1:

A client gets its IP address (e.g.,192.168.41.10/24) and DNS Server IP address (e.g., 192.168.10.177/24 from Corporate HQ. The Local Breakout configuration contains route 192.168.10.0/24. When a client attempts to access youtube.com, it first must send a DNS request, then then DNS request could be forwarded to Corporate HQ via tunnel.

Example 2:

A client gets its IP address (e.g., 192.168.41.10/24, and DNS Server IP address (e.g., 192.168.10.177/24 from Corporate HQ. The Local Breakout configuration does not contain route 192.168.10.0/24. When the client attempts to access youtube.com, it must first send a DNS request to the AP's local network. If there is a DNS Server with IP 192.168.10.177 and it cannot be found, the client will fail to access the website.

Example 3:

A client gets its IP address (e.g., 92.168.41.10/24) and DNS Server IP address (e.g., 219.141.136.10) from Corporate HQ.

The DNS IP address is from a network operator in China. There are three network operators; and if your local network is from network operator A, the client can send a DNS request to the DNS Server belonging to network operator B, but it would be slow.

If the client's local network is from network operator A, but it gets the DNS Server IP address belonging network operator B (assume that 219.141.136.10 belongs to network operator B), when the client attempts to access youtube.com or any other URL, it will be slow.

Solution:

Configure the correct DNS Server from Corporate HQ; the client needs to configure its DNS Server.

AP May Disconnect with its Local Network

Problem Description: After enabling Local breakout, the AP controls client traffic based on a static route configured with Local Breakout, but the AP traffic packet is also controlled by a static route.

Example:

The Local Breakout configuration contains route 192.168.10.0/24, but there is also subnet - 192.168.10.0/24 within AP's local network. If the AP attempts to access to 192.168.10.100, which is contained in AP's local network, it will fail because the packet will be forward to the tunnel and sent to Corporate HQ.

Solution:

Caution must be taken when configuring the Local Breakout to avoid overlap with the AP's local network.