Remote Access Point and VPN VA Installation Guide

August 2020

Revision B

Part Number 060688-10

ALE USA Inc.
26801 West Agoura Road
Calabasas, CA 91301
+1 (818) 880-3500

Table of Contents

Remote Access Points and VPN Tunnel Components

A Remote Access Point (RAP) is an AP with a management tunnel to a remote OVE, regardless of whether a Data VPN is enabled or not. An 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 a 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:

- 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 needs 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 connect to.

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. Optionally, a Data VPN tunnel can 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:

- OVC device catalog provides options to register the AP as RAP. This is required to setup the Management VPN to the RAP VA appliance located in corporate HQ. The administrator should register the AP as 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 RAP is managed by OVC:

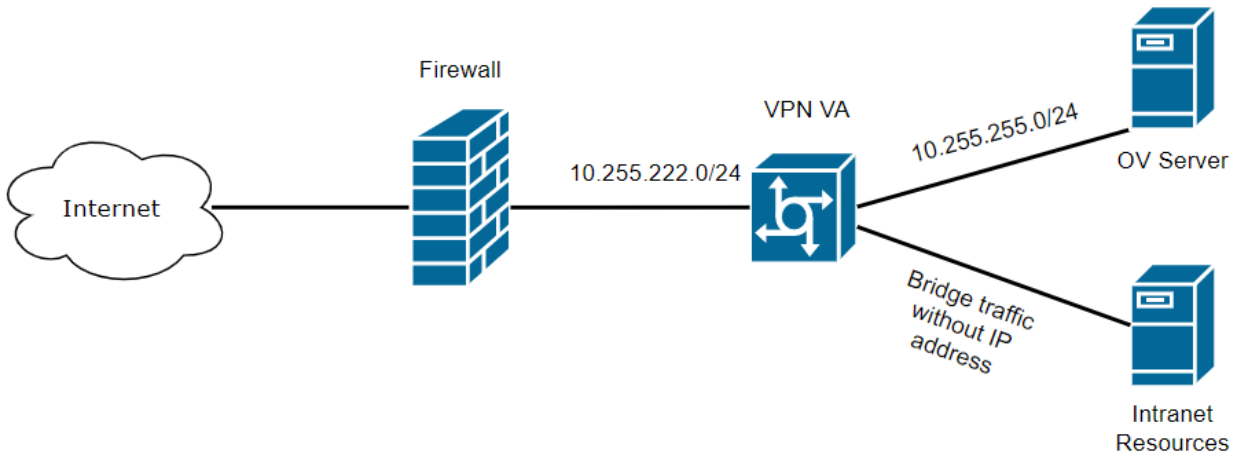
- The administrator registers the AP in the OVC device catalog as a standard OVC managed AP. No Management VPN is required as the AP is managed by OVC.
- Data VPN configuration is done from OVC on the managed AP. This is required to setup the Data VPN tunnel to the RAP VA appliance located in corporate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

Prerequisites

- ESXi versions 6.0, 6.5, and 7.0 are supported (ESXi 5.5 is not supported).
- Stellar RAP version is AWOS 4.0.0 is supported. AWOS 4.0.0.1064 (Maintenance Release) is recommended.
- OmniVista 2500 version 4.5R1 is supported.

Network Topology

Within this document we will use the following network topology:



Remote Access Points and VPN Tunnel Configuration

You can configure an offsite, remote AP as a Remote Access Point (RAP) that can be managed by your local OmniVista Enterprise 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 install a VPN Tunnel Server Virtual Appliance (VPN VA) (see the *OmniVista Enterprise 4.5R1 Installation and Upgrade Guide* for installation instructions).

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 will be added to the List of Managed Devices and manageable by your local OmniVista Enterprise installation. The following sections detail the steps required to deploy Remote Access Points:

1. Creating an OmniVista Cirrus Freemium Account

2. Adding APs to the Device Catalog

3. Deploying/Configuring the VPN Tunnel Server

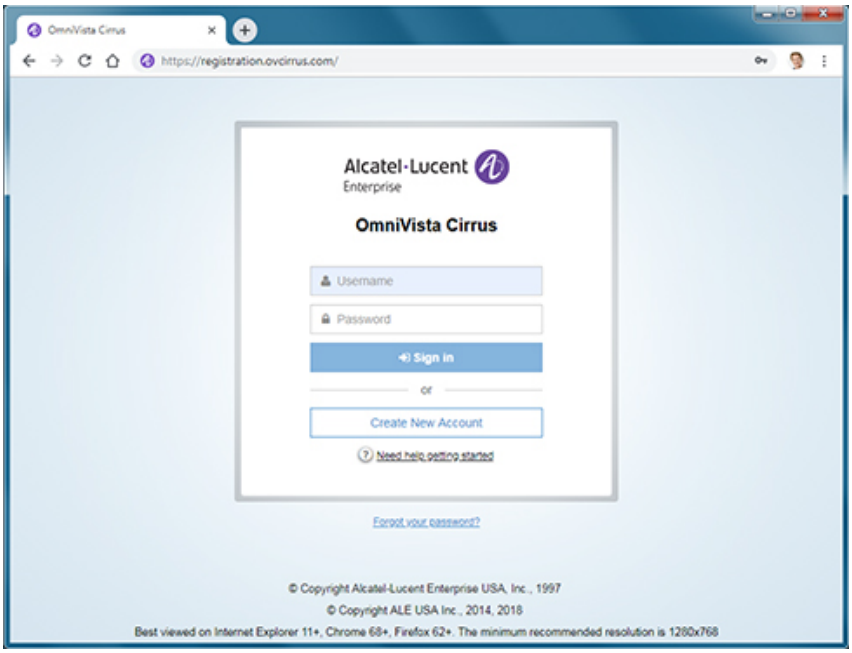
Note: The Remote AP feature is only supported on Stellar APs running AWOS 4.0.0.40 and higher.

Note: Only untagged traffic can currently 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.

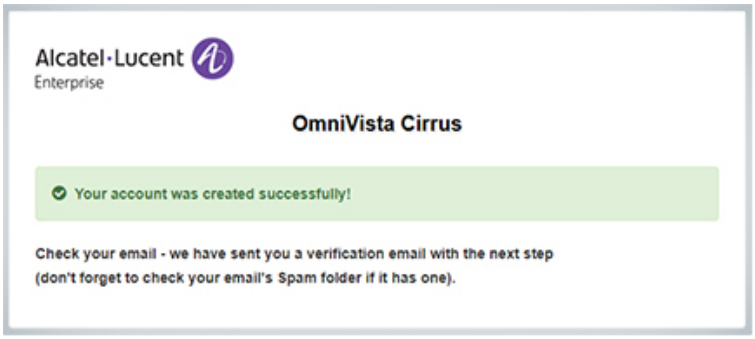
1. Go to the OV Registration Portal.



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

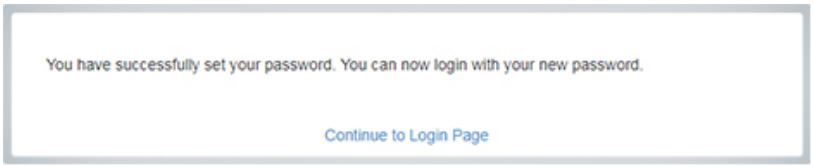
completed and reviewed all of the fields, accept the terms and conditions and click on the **Create Account** button. A Confirmation Screen will appear.



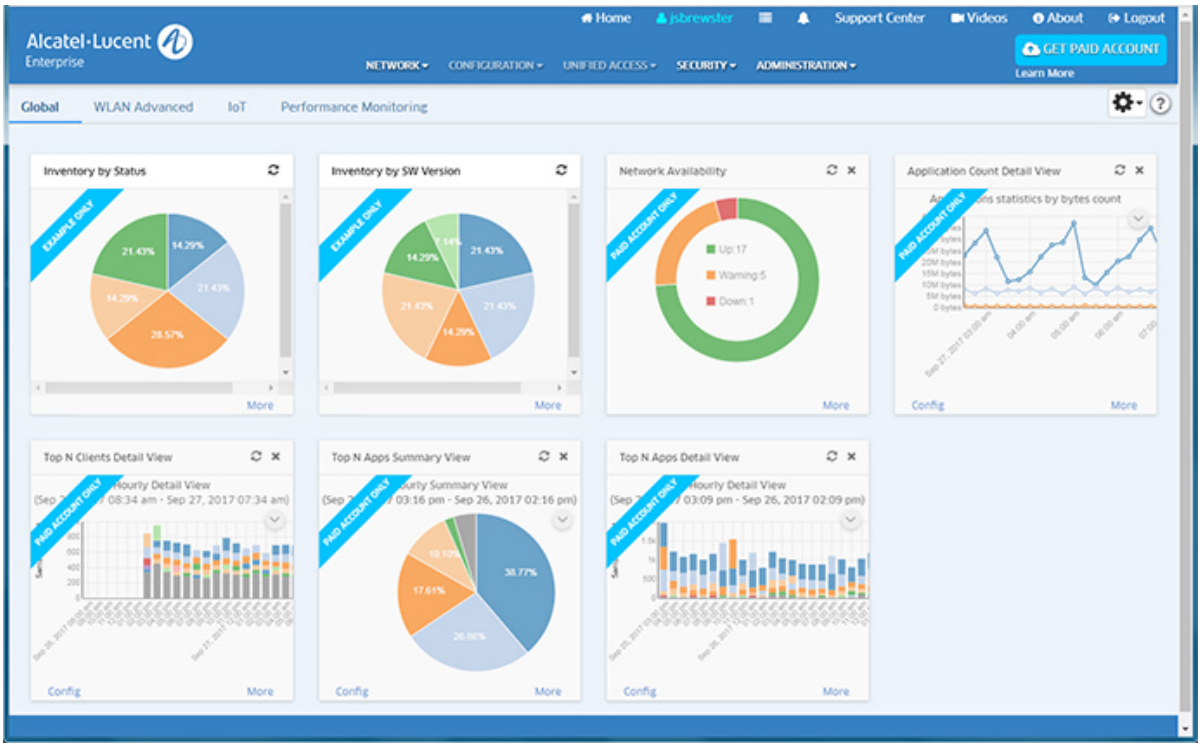
4. Go to the e-mail account you entered in Step 3 above. You will receive an e-mail from ALE USA Inc (noreply@ovcirrus.com) containing instructions and a verification link. Click on the **Go to Verify Account** link. The Set Password Screen will appear.

> **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 4.0.0.40. 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.

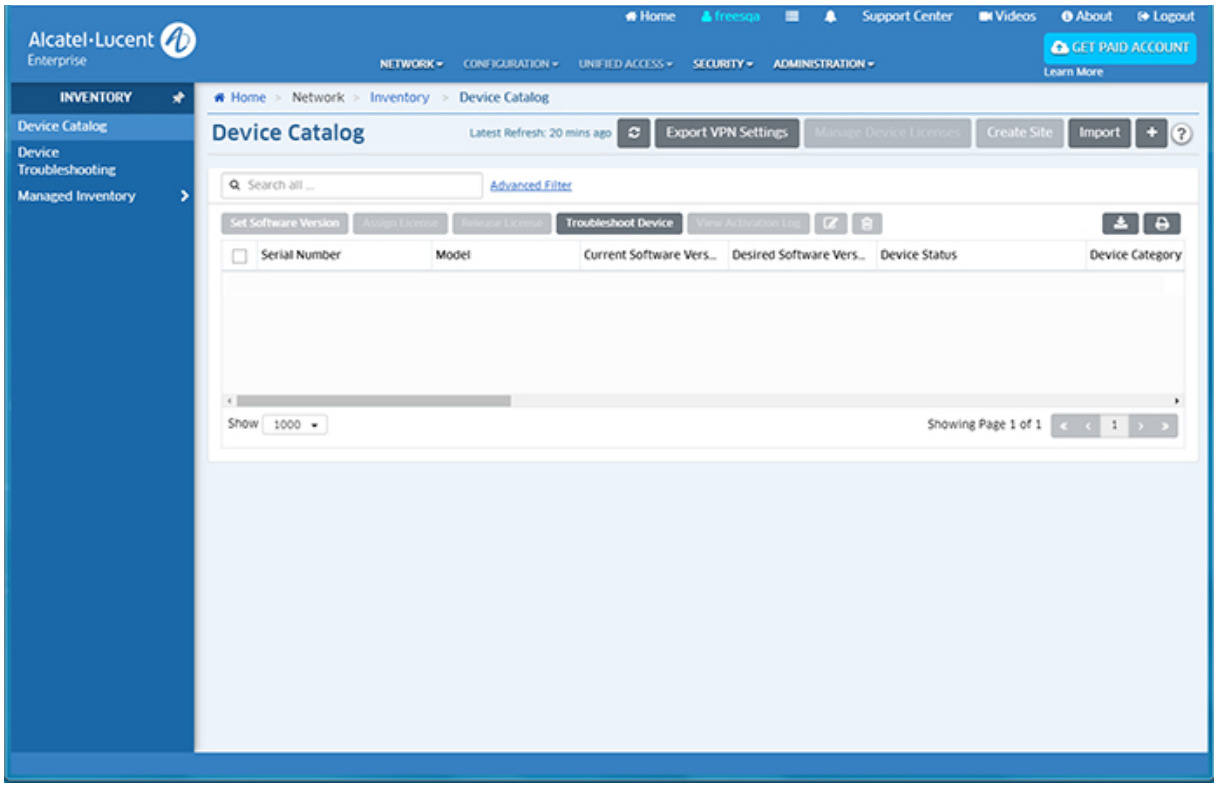


Note: You will continue to log into https://registration.ovcirrus.com using the username and password you created to access your OmniVista Cirrus Freemium Account.

Add Remote APs

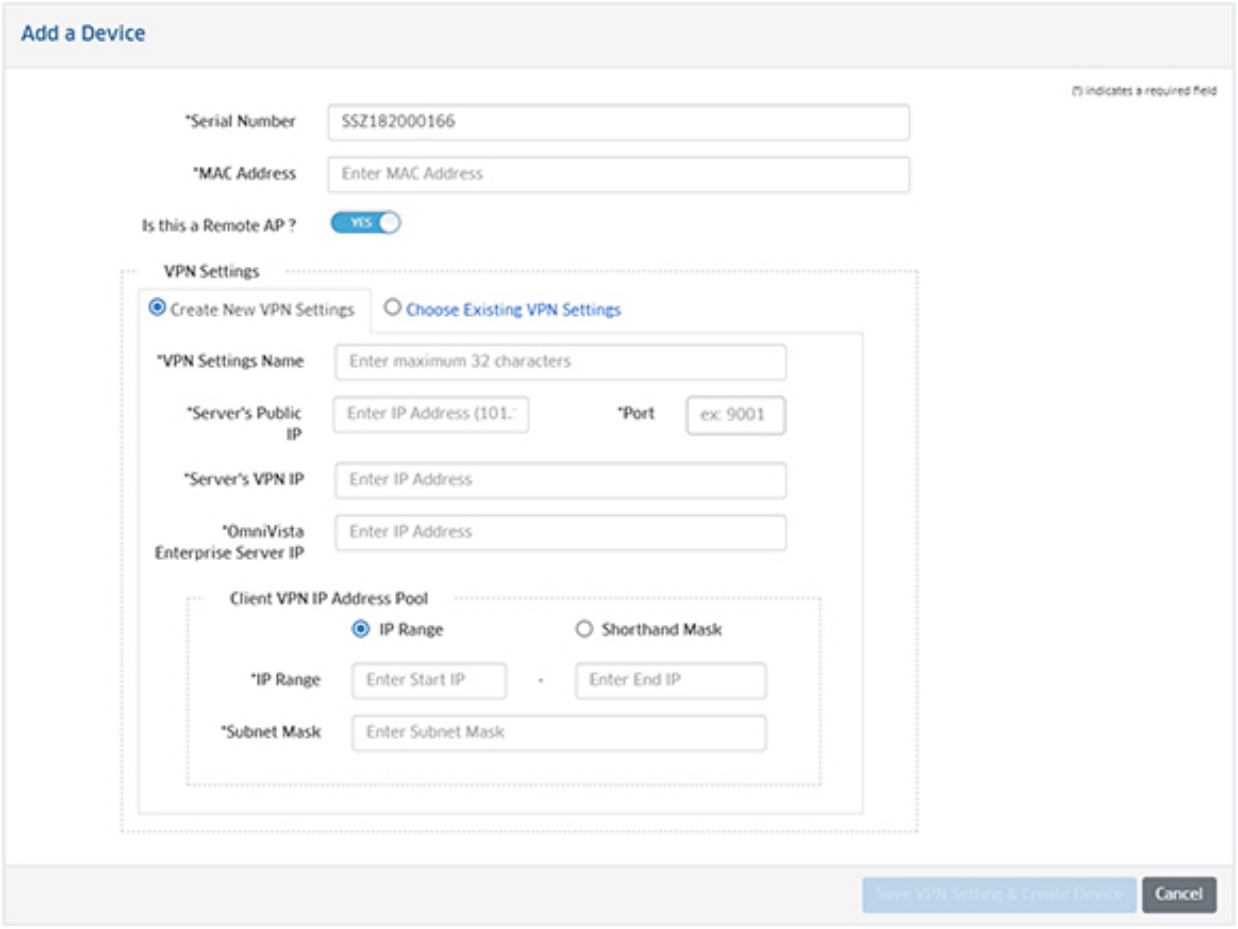
Remote APs are added using the Device Catalog application.

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**, then enable the **Is this a Remote AP Field** to open the Remote AP configuration fields.



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 -** User-configured 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.

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

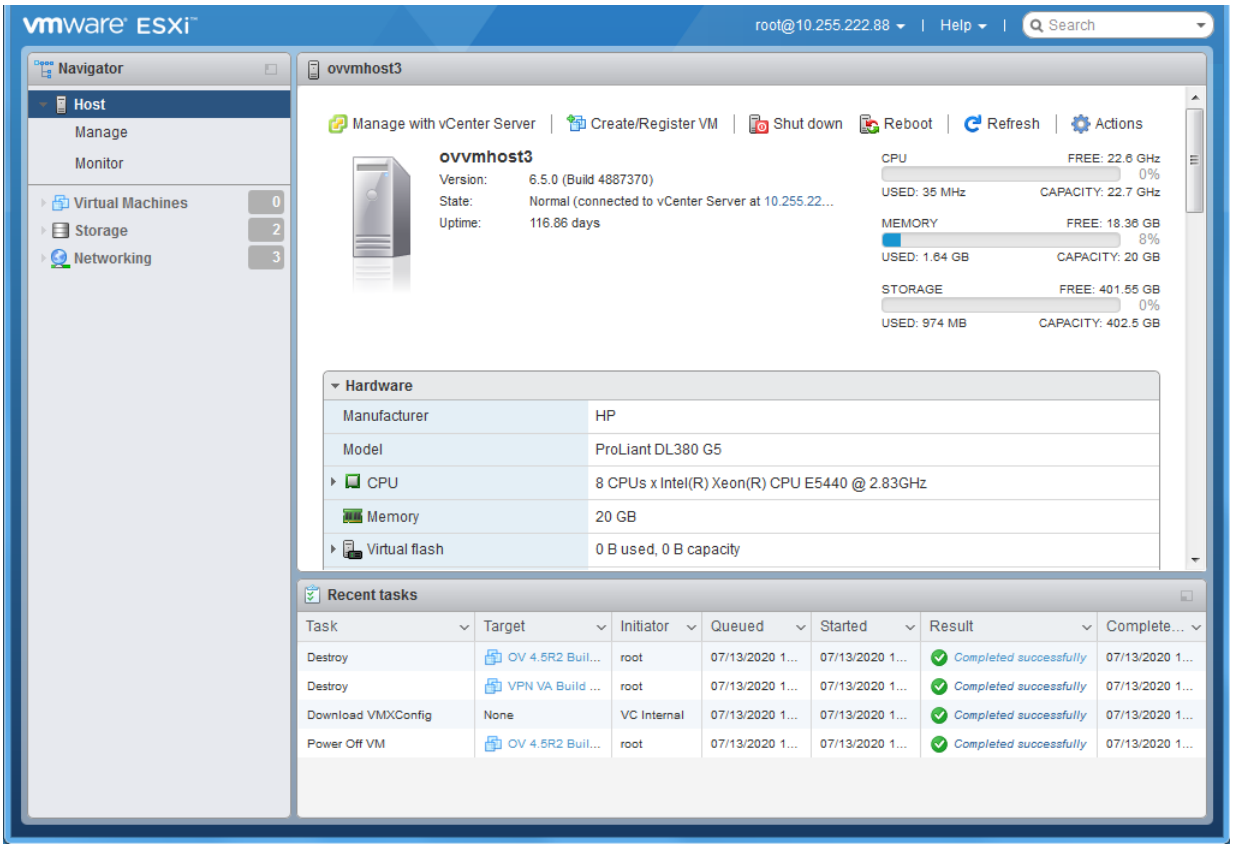
    Note: Higher scale is based on CPU/Memory calculated per RAP unit. For deployments greater than 64 RAPs it's suggested to contact ALE TSS/Support for recommendations on planning and rollout.
- **NICs - 1G vs.10G** (Based on expected throughput)
  - 10 - 20Mbps expected VPN throughput per RAP, if local breakout is serving all internet needs.
  - 20 - 100Mpbs expected VPN throughput per RAP, if all traffic is tunneled through VPN.

Deploying the VPN Virtual Appliance

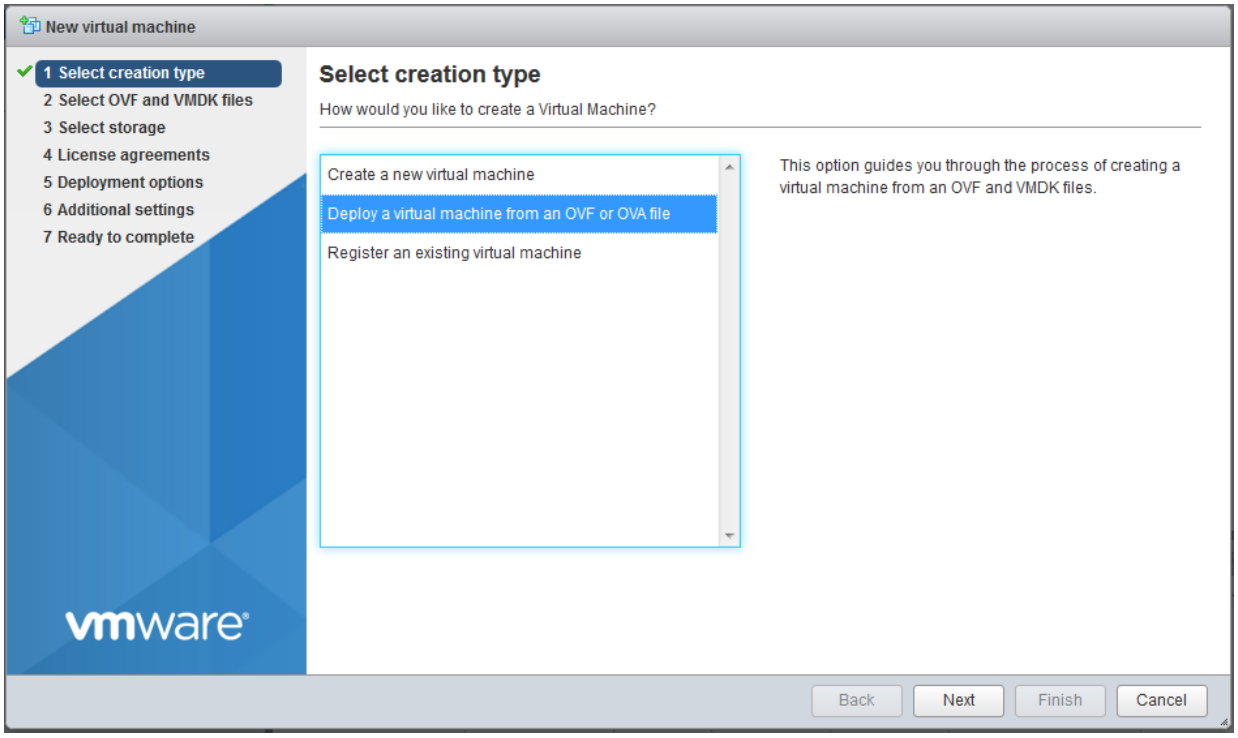
Deploy the VPN VA on your Hypervisor. The steps below show the steps to deploy the VA on VMware. After deploying the VA, configure the VA and complete the installation.

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 before importing the files in Step 5**.

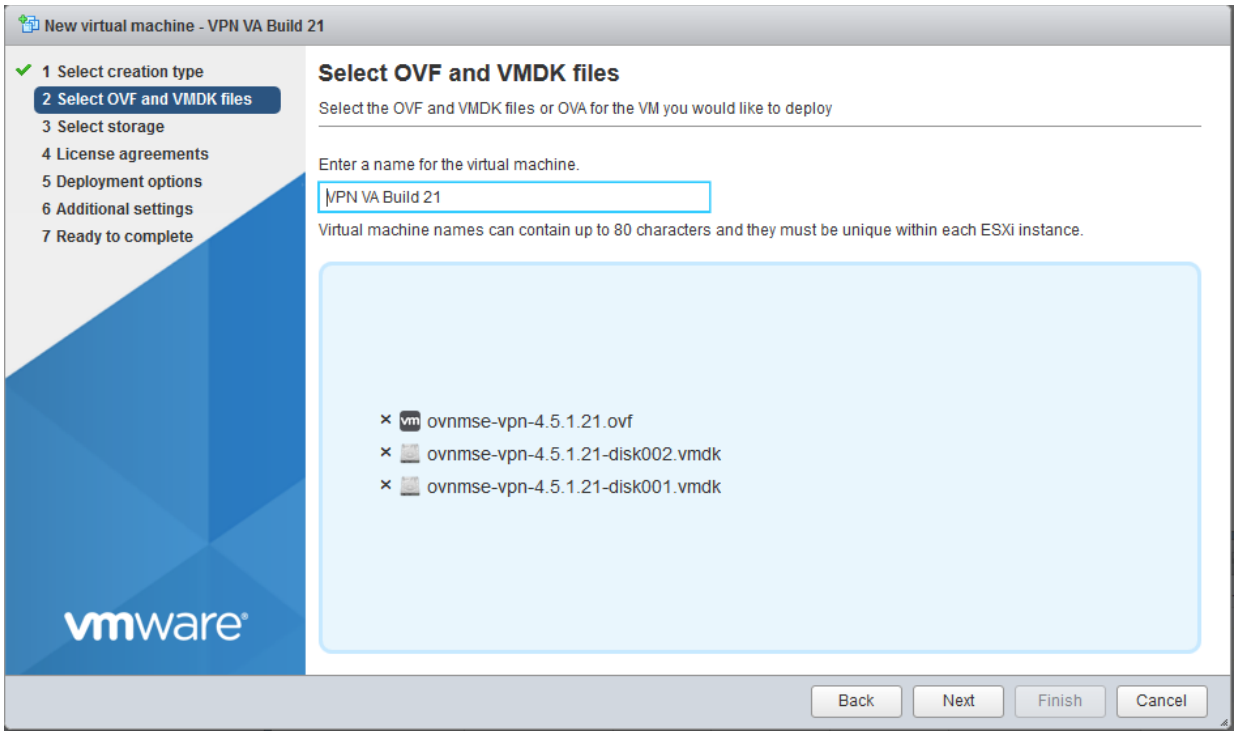
2. Log into VMware ESXi.



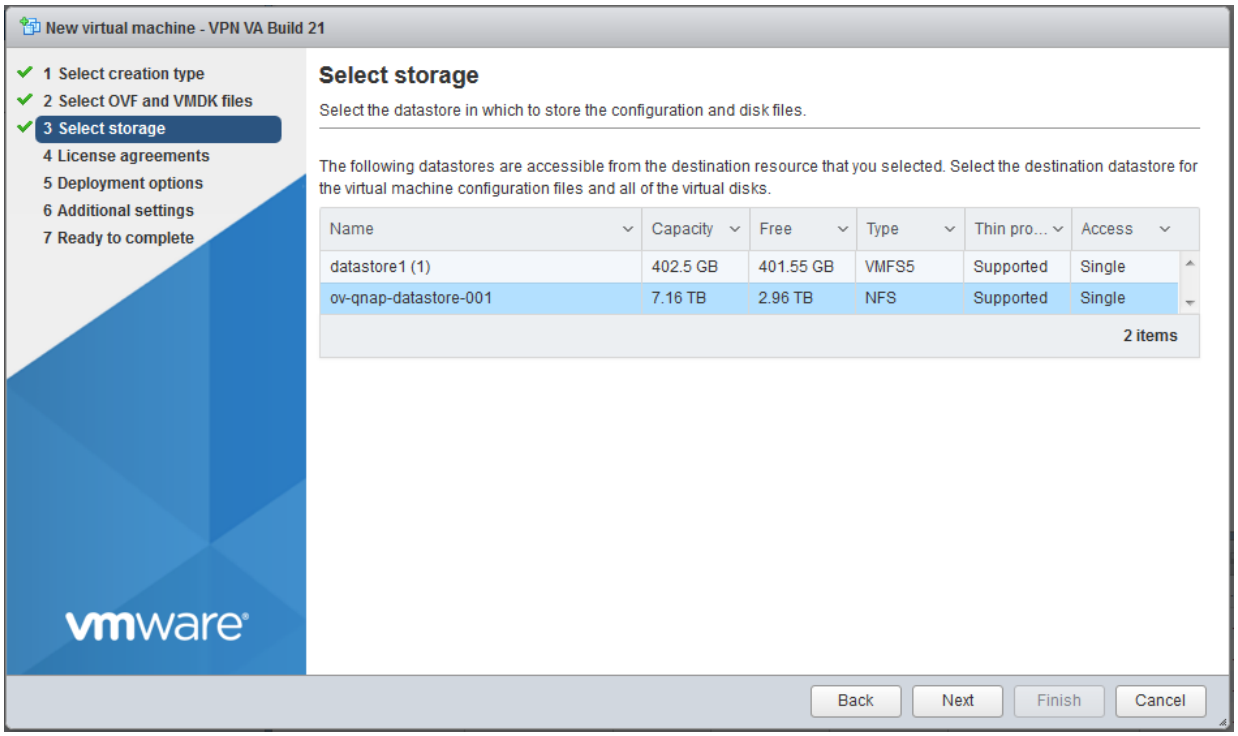
3. Select the Host on which you want to install the VPN VA and **click on Create/Register VM**. The first screen of the New Virtual Machine Wizard appears.



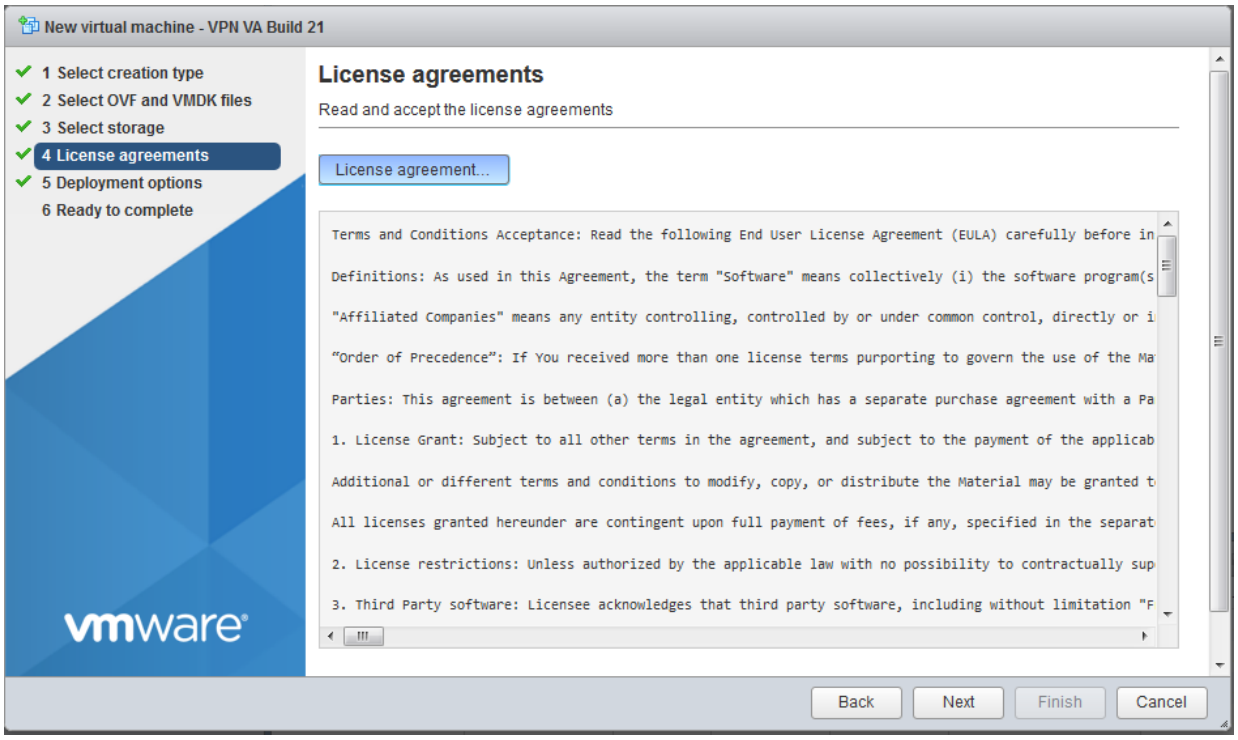
4. Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



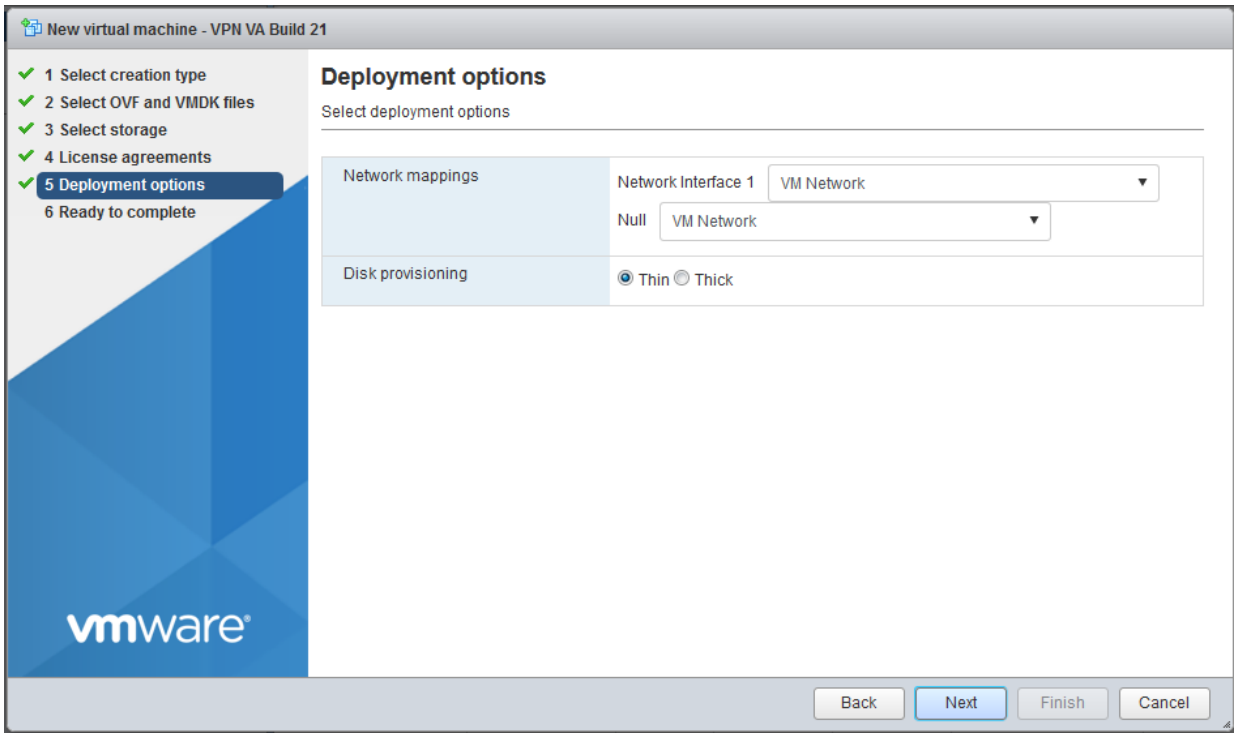
5. Enter a name for the VM (e.g., VPN VA Build 21), click to locate and select the downloaded installation files (or drag the files into the window), then click **Next**. Remember, do **not** include the *.mf File; only the *ovf file and the two *vmkd Files.



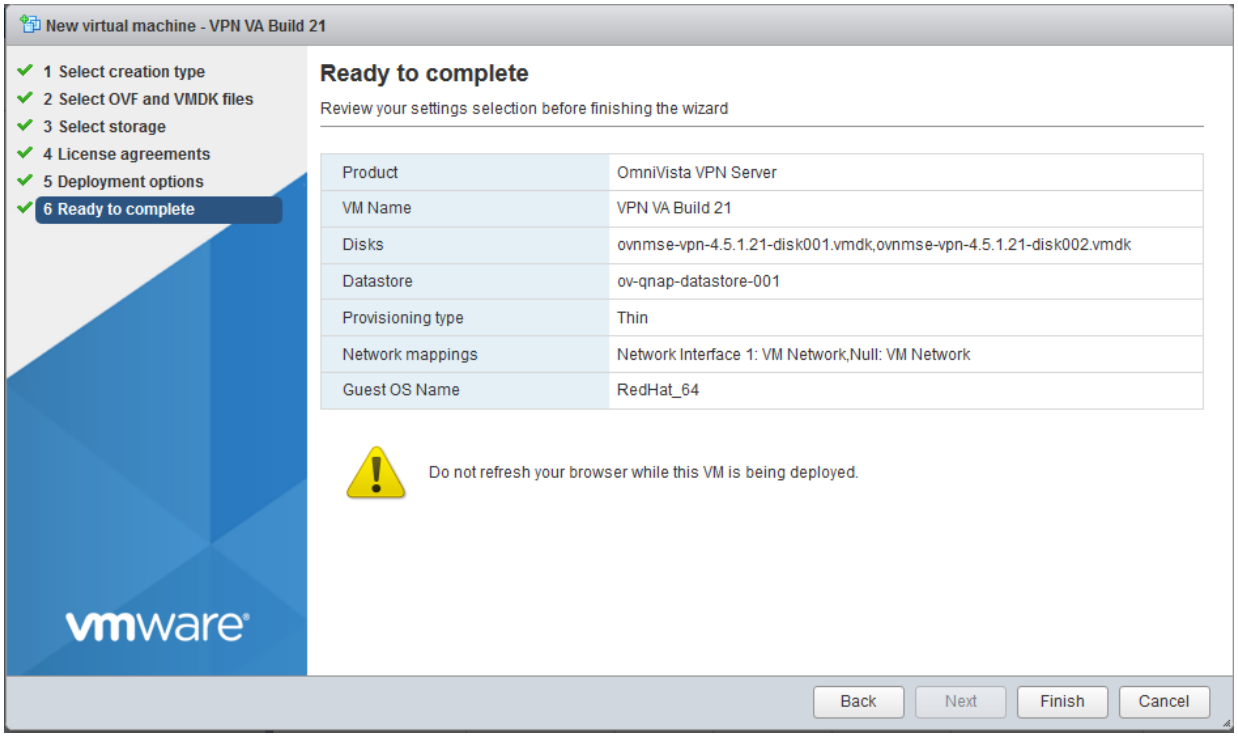
6. Select the destination storage where the template is to be deployed, then click **Next**.



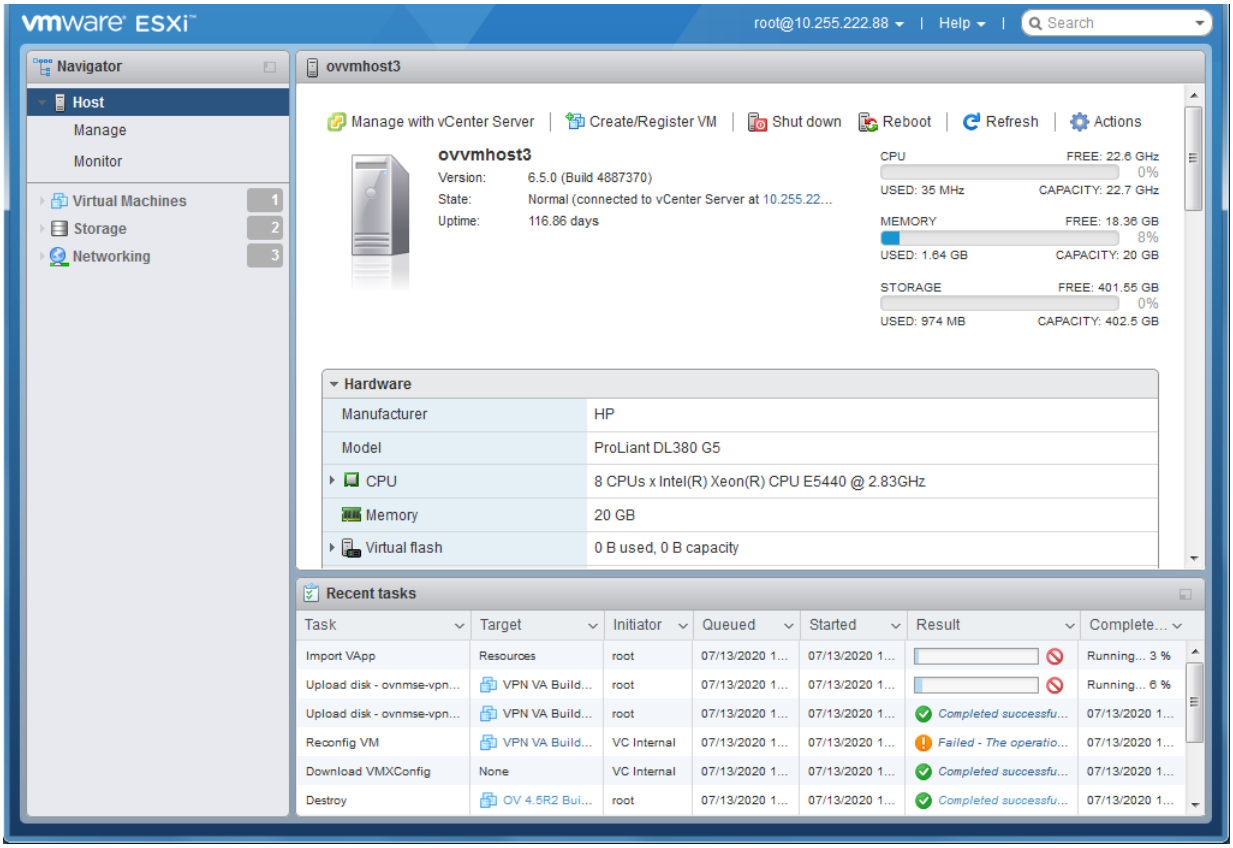
7. Review the License Agreement, click **I agree**, then click **Next**.



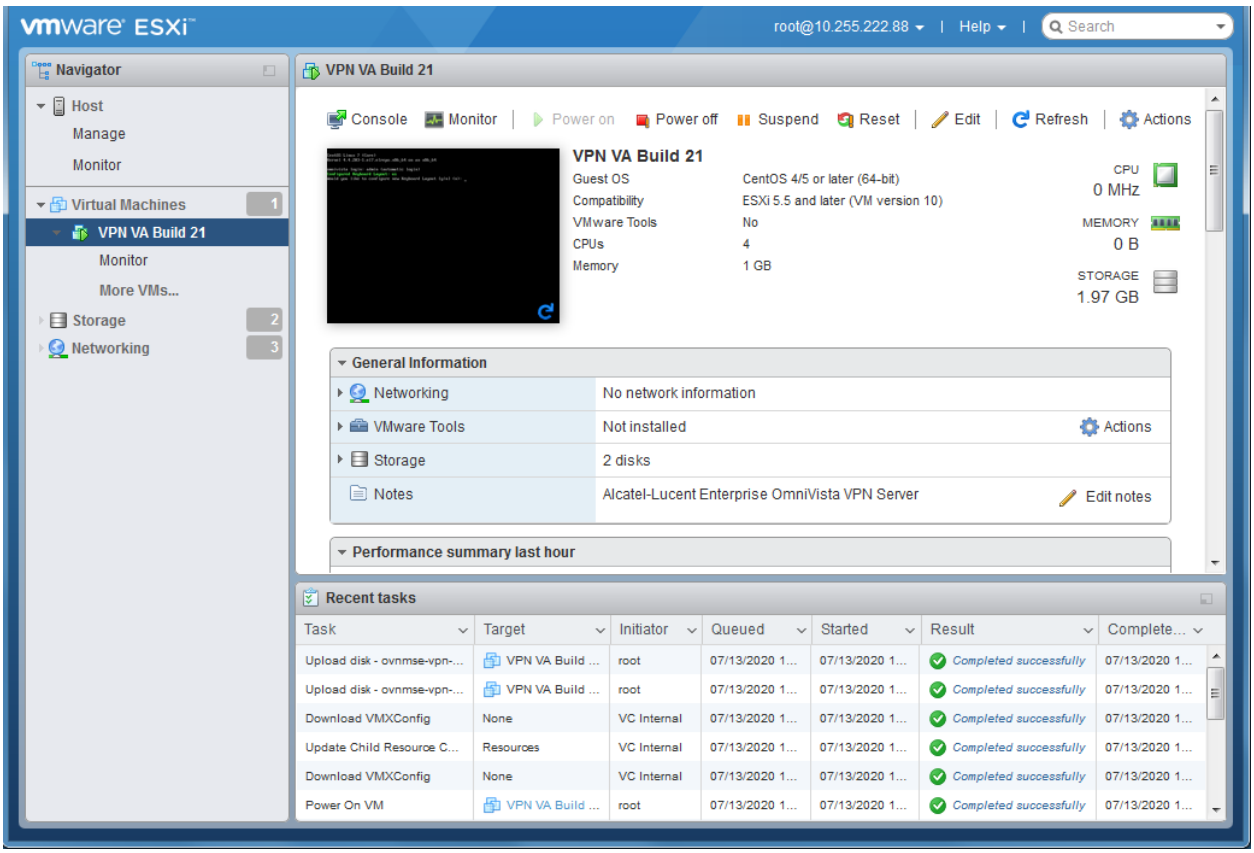
8. In the **Network mapping** field, select the Destination network that the deployed VM will use. In the **Disk provisioning** field, select **Thin**. Click **Next**.



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.

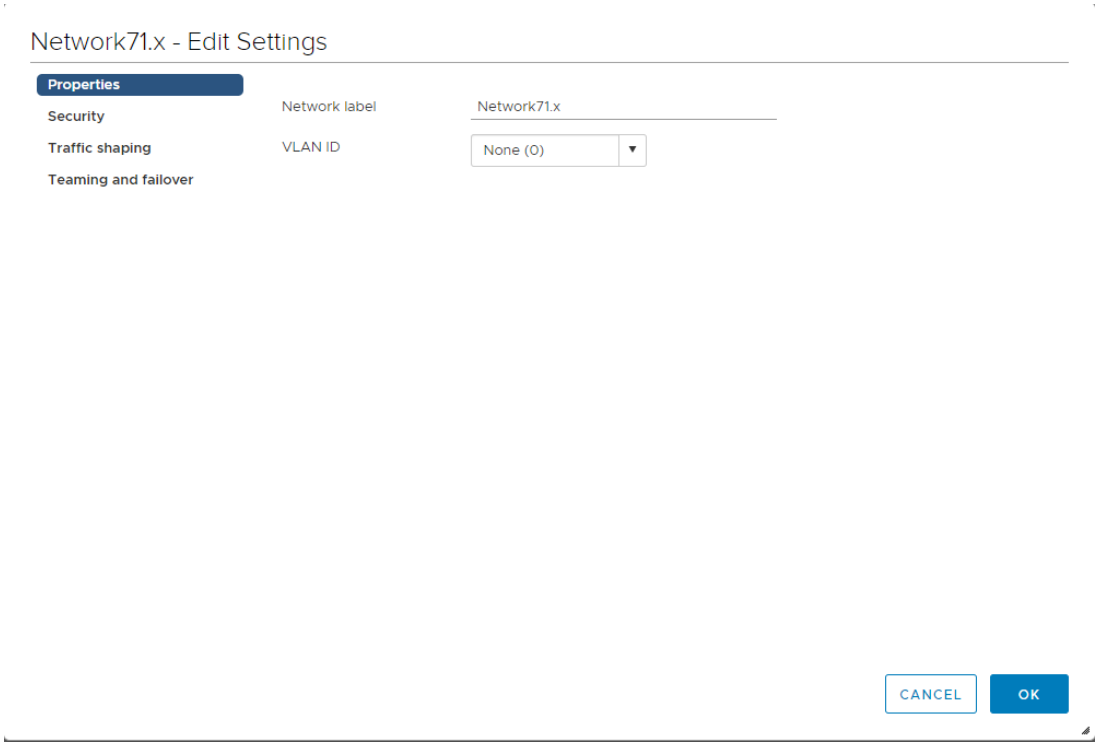


10. When the installation is complete (indicated by all three files showing “Completed Successfully” in the Result column of the Recent tasks table), click on **Virtual Machines** in the Navigator Tree on the left side of the screen to display a list of VMs. **Select the VM you just deployed. Basic details for the VM are displayed, as shown below.**

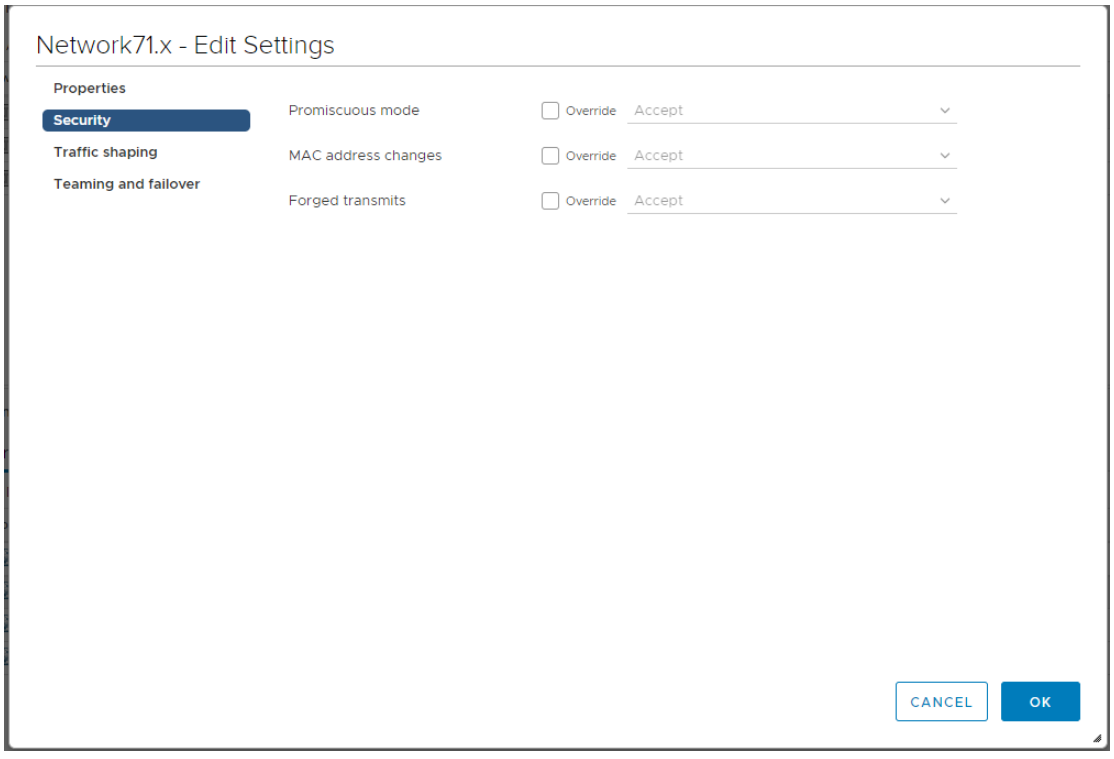


Important Notes:

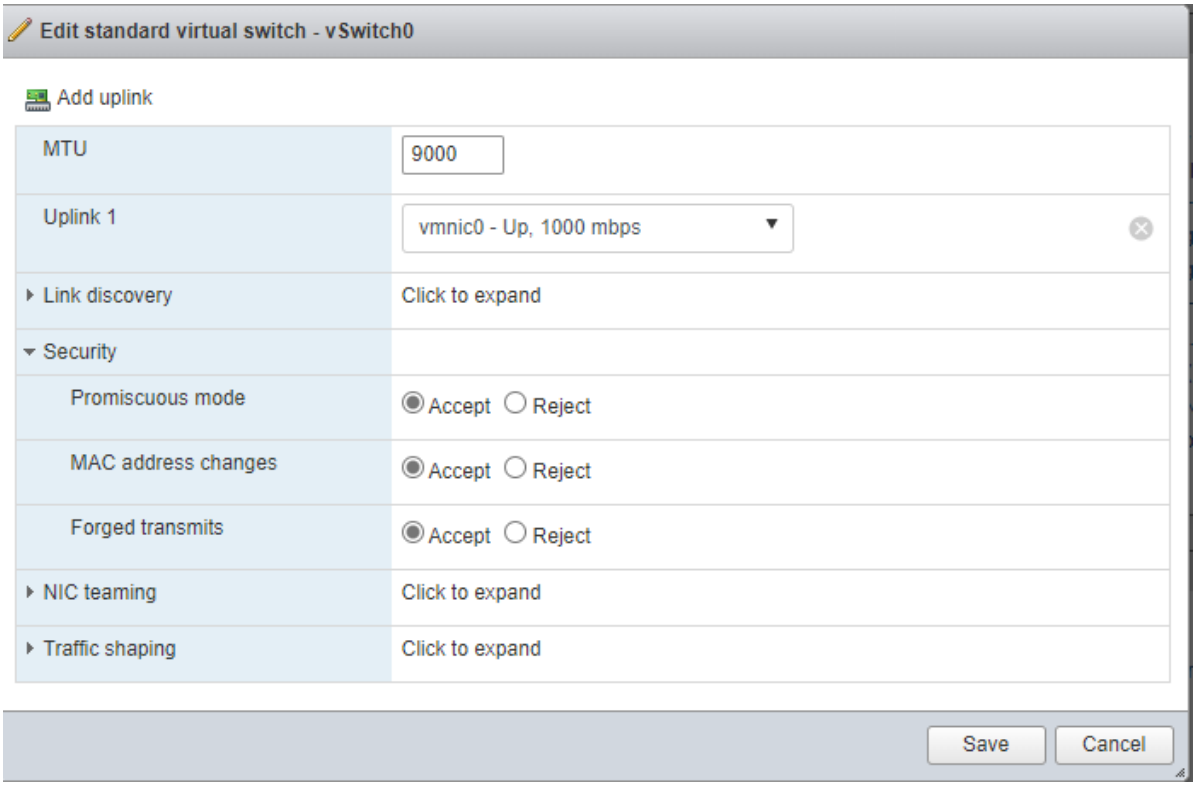
- On the ESXi VM, do not manage the VLAN on the NIC dedicated to bridged traffic - the interface without IP Address managed.



- On the ESXi VM, enable Promiscuous Mode for the above NIC. If the “Override” checkbox is enabled, make sure Promiscuous Mode is 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. 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.

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 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:
```

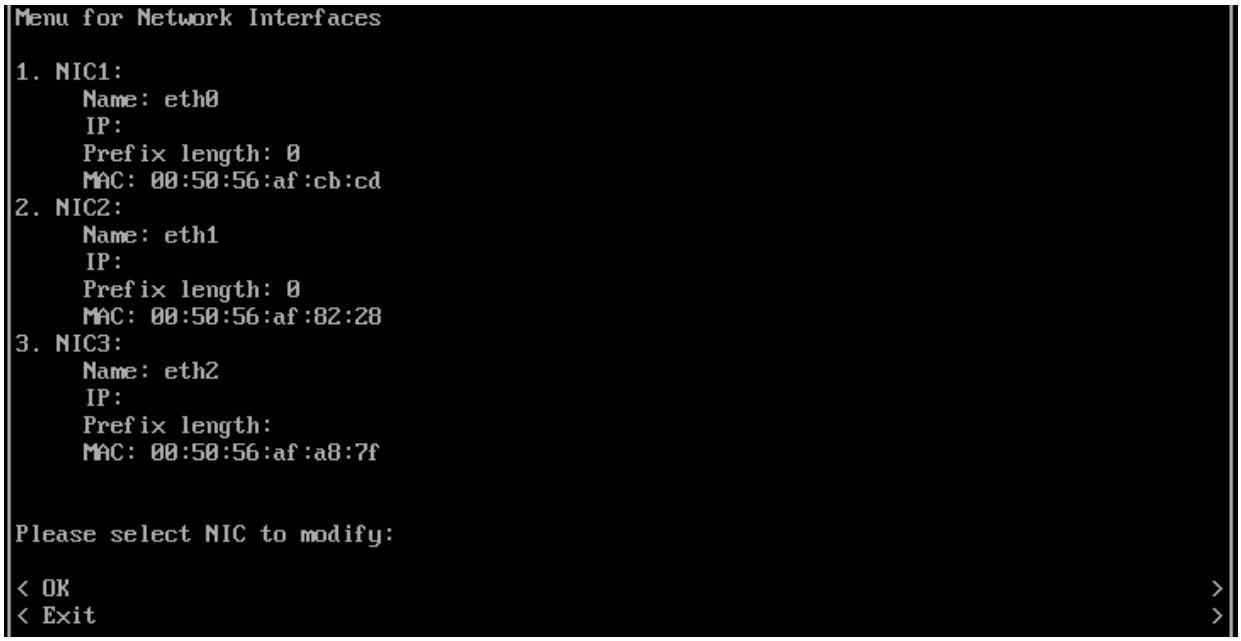
4. The VM will reboot. When the reboot is complete, the OmniVista Login Prompt will appear. Enter the OmniVista Login (admin) and press **Enter**; then enter the Admin Password you configured in Step 3 and press **Enter**.

```
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: 4.5.1
Build Number: 21
Build Date: 2020-04-17
omnivista login: admin
Password: _
```

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

Configure NICs

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



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**.

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.

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.

> **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.

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

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

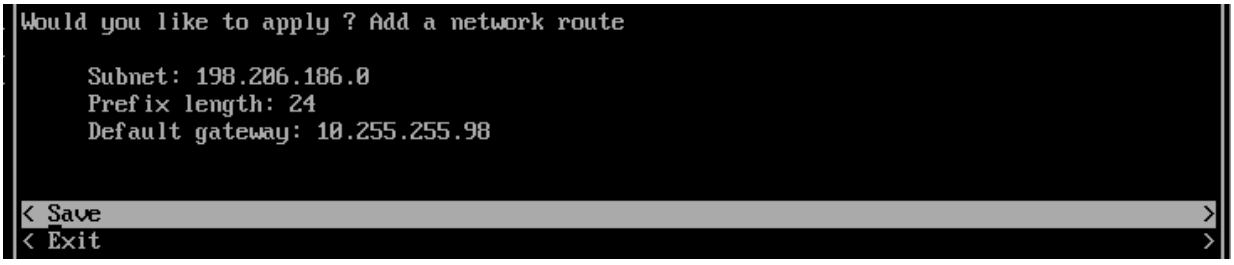
Configure Routes

If necessary, configure a Network Route.

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

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

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**.



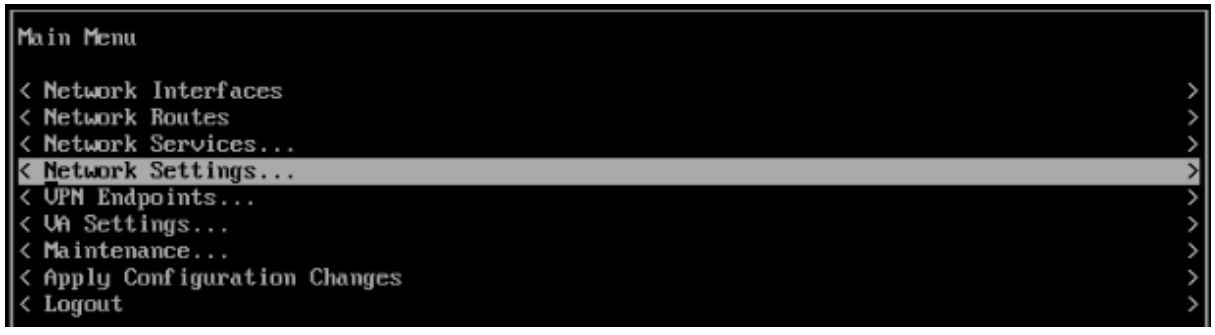
4. At the Confirmation Prompt, with **Save** highlighted, press **Enter**, then press **OK** at the next Confirmation Prompt. The Network Route will be added and Main Menu will appear.

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

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

Configure Network Settings (DNS, Gateway)

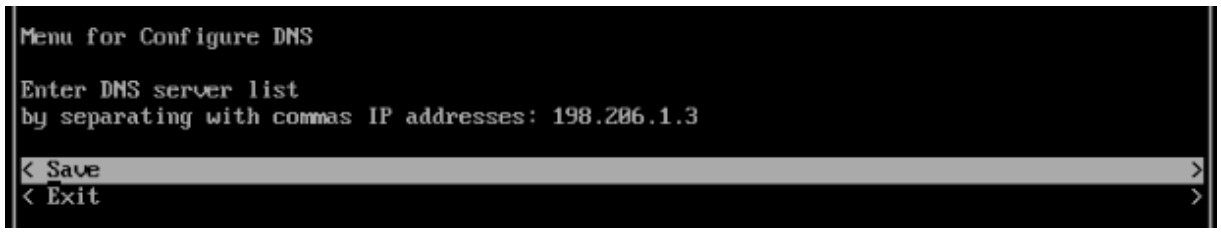
If necessary, configure a DNS; and configure a Default Gateway for public network access.



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

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

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



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

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

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

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

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

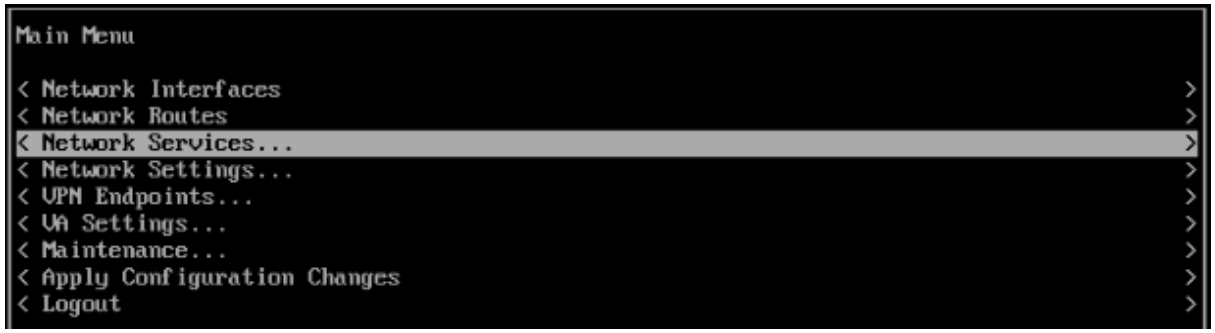
9. Highlight **Exit** and press **Enter** until you return to the Main Menu.

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

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

Configure an SSH Service

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



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

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

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

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**.

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

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

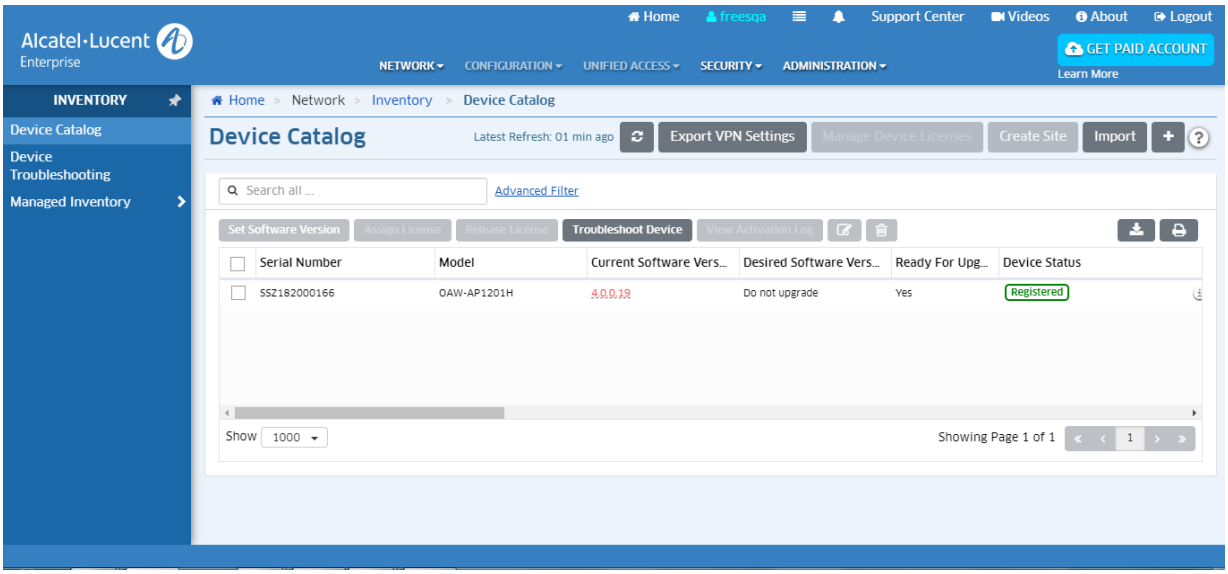
7. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

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

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. Wait for the AP to reach “Registered” Status, then **c**lick on the **Export VPN Settings** button at the top of the screen.

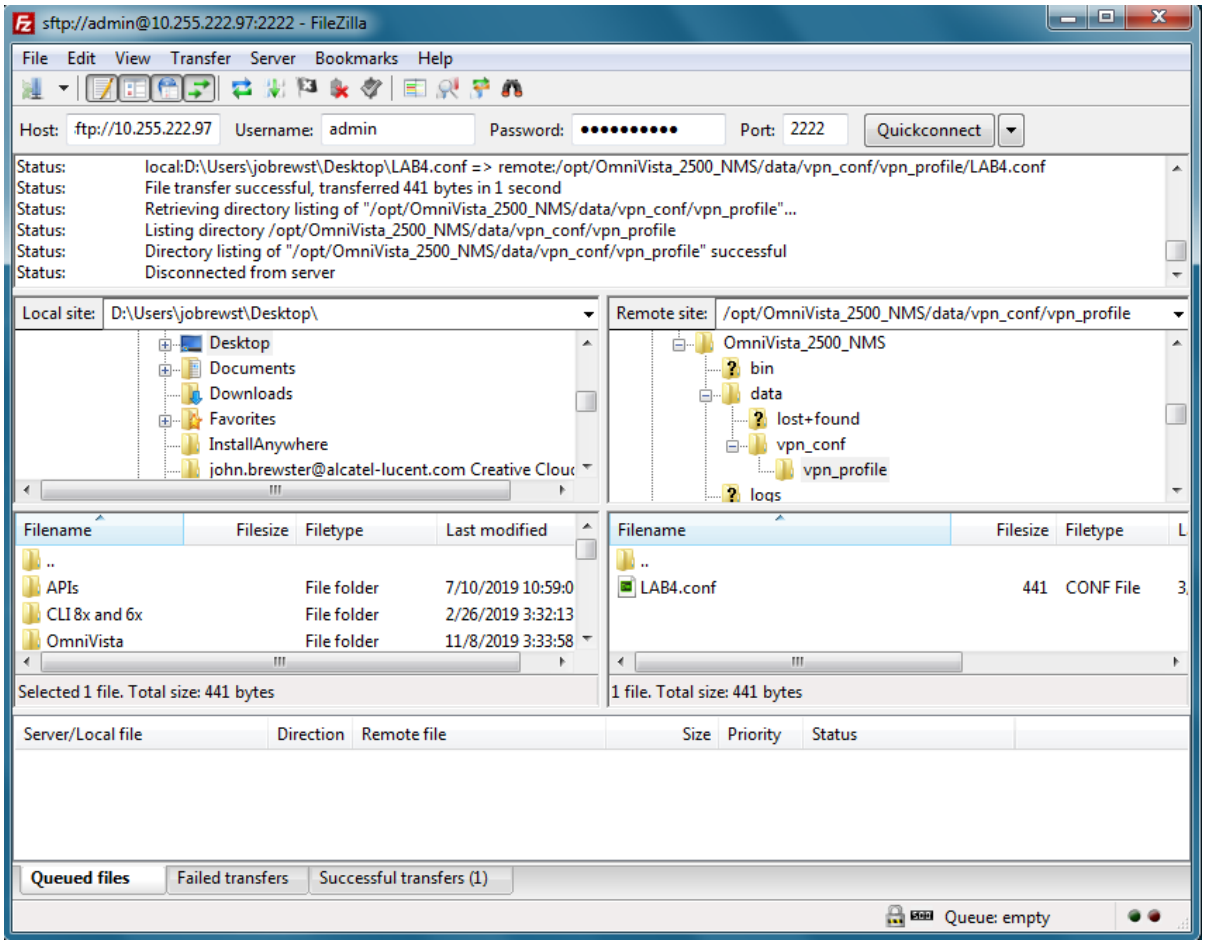
The file must contain the list of all RAPs (peers) with their IP Addresses and Public Keys as shown below:

```
[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.

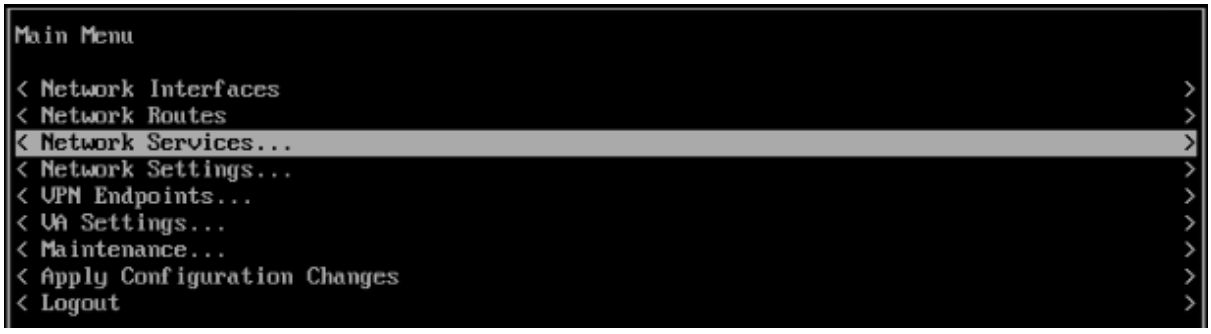
Important Note: Do not change the name of the VPN Settings file.



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**.

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

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

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**.

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**.

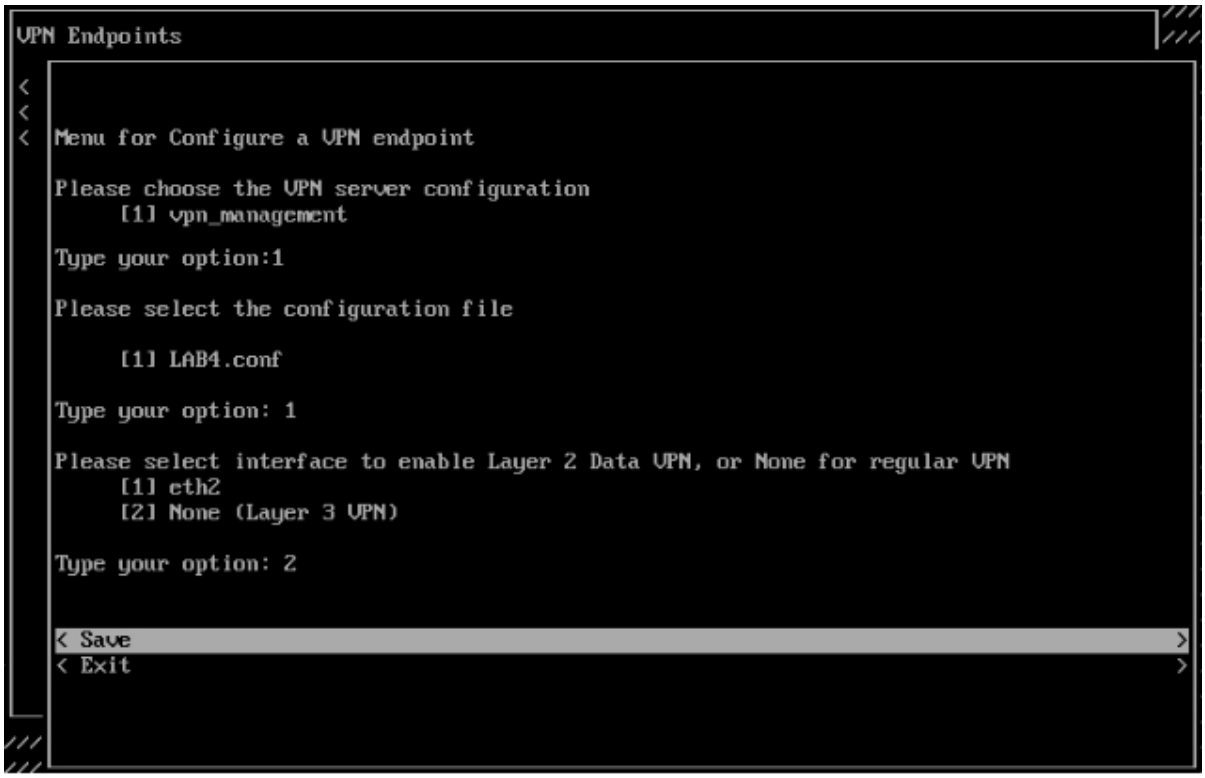
7. The following Confirmation Prompt will appear. Press **Enter** to apply the configuration. When the process is complete, the Main Menu will appear.

Configure VPN Endpoints

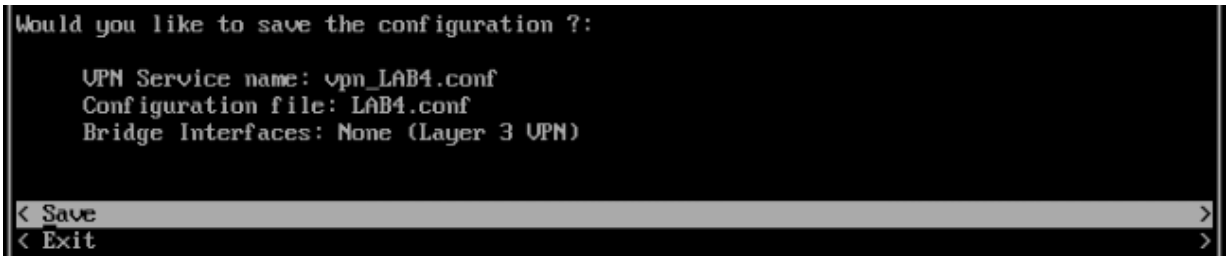
Attach the VPN Settings File to the VPN Service.

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

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



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**.



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

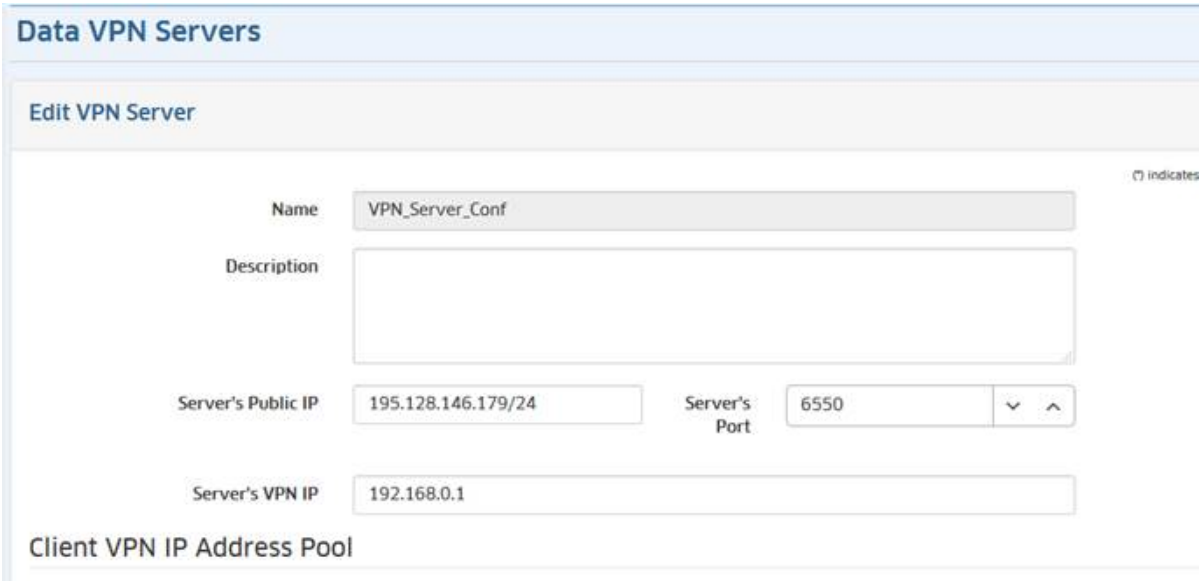
5. Use the Down Arrow to highlight **Apply Configuration Changes** and press **Enter**.

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

Configuring the VPN Data Tunnel

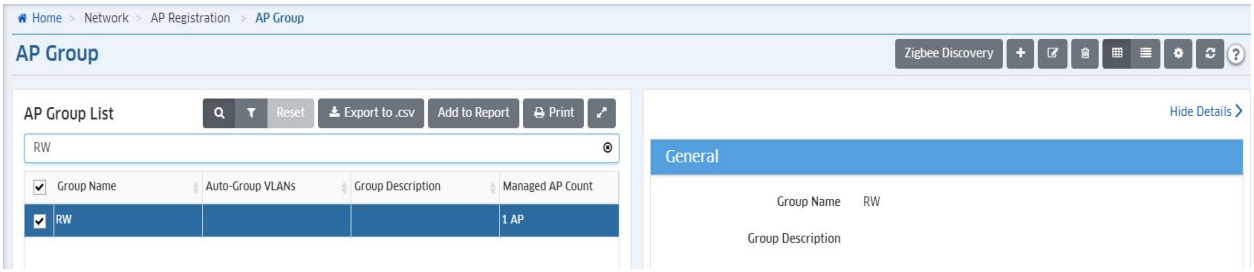
Once the Management VPN tunnel is configured, follow the steps below to configure a VPN Data tunnel. An L2GRE tunnel will be created between the Remote AP and the VPN Server and it will be used to tunnel the remote employee's data traffic.

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

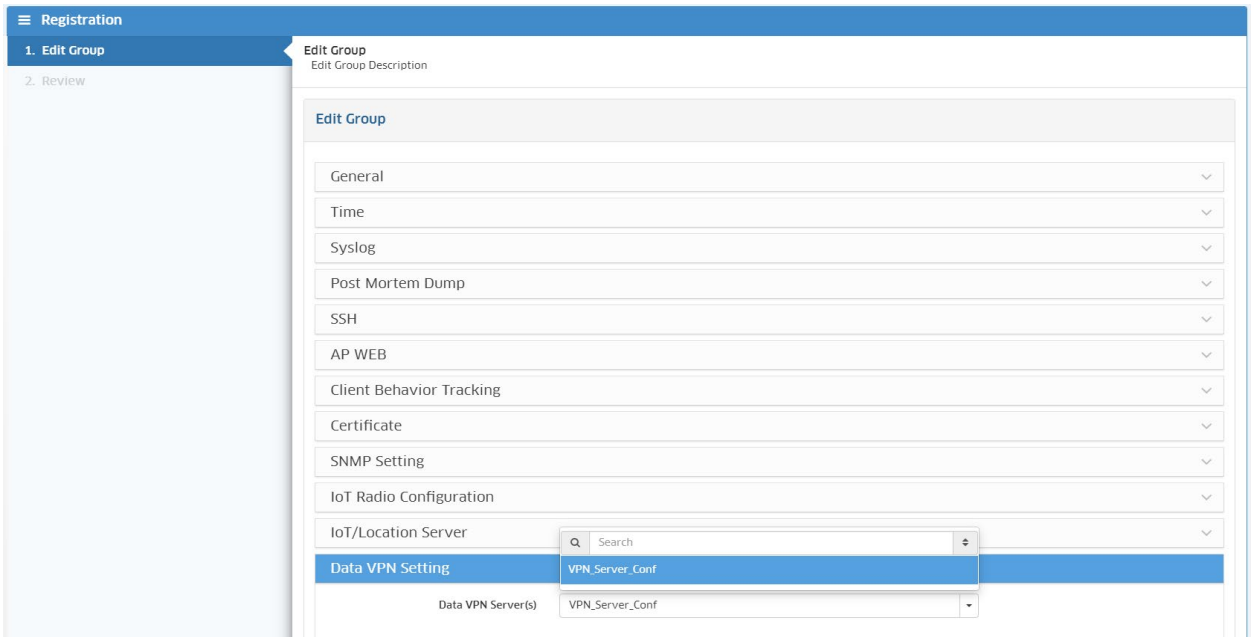


Name	User-configured name for the VPN configuration.
Server's Public IP	The VPN Server's Public IP address (configured when you installed the VPN VA). This is the IP address used by Remote APs to connect to the VPN Server. And this is the interface through which traffic originating from inside the Enterprise 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.

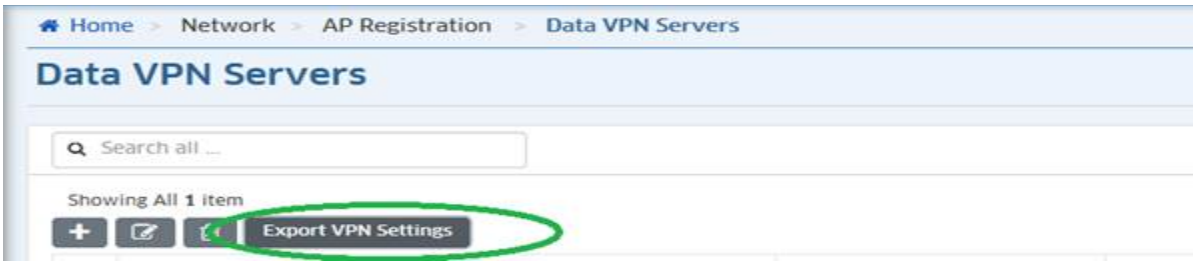
2. Go to the AP Group Screen (Network - AP Registration - AP Group) and edit the AP Group used to manage Remote APs.



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.

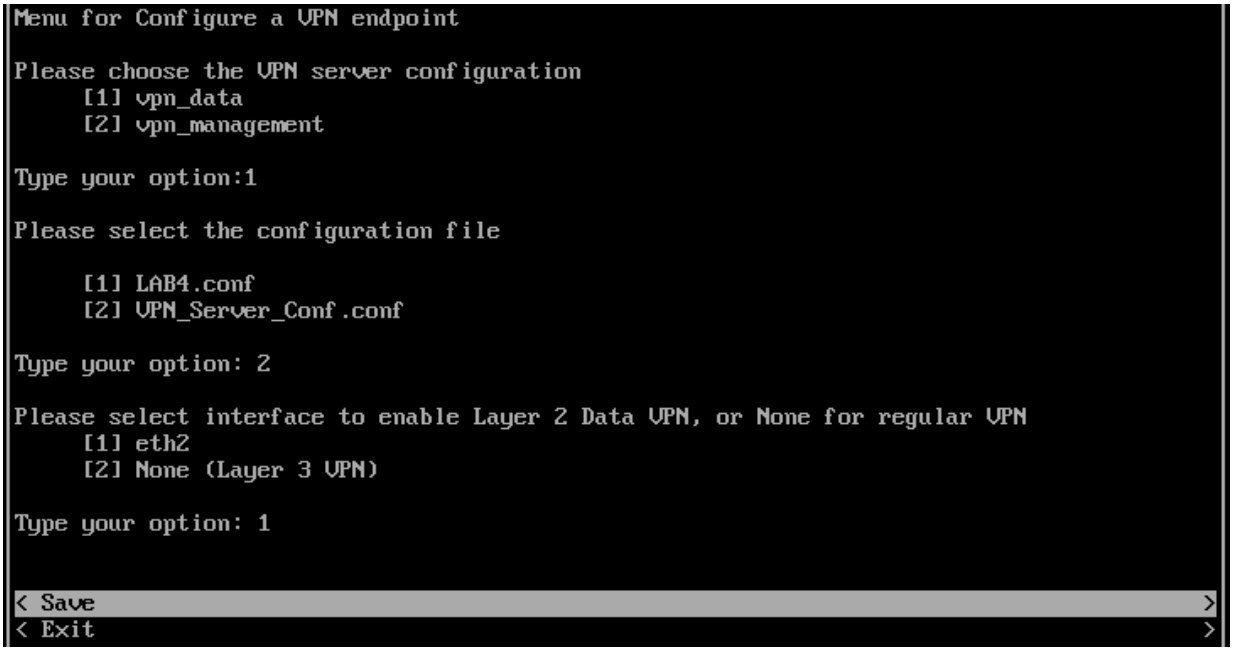
8. Configure VPN Endpoints. Be sure to select the right ethernet interface for bridging traffic (e.g., eth2 without IP Address).

Configure VPN Endpoints

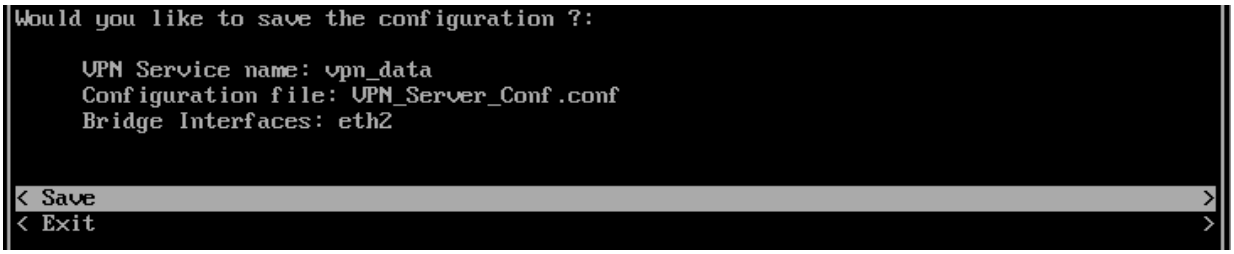
Attach the VPN Settings File to the VPN Service.

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

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



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**.



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**.

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                                                                        >
```

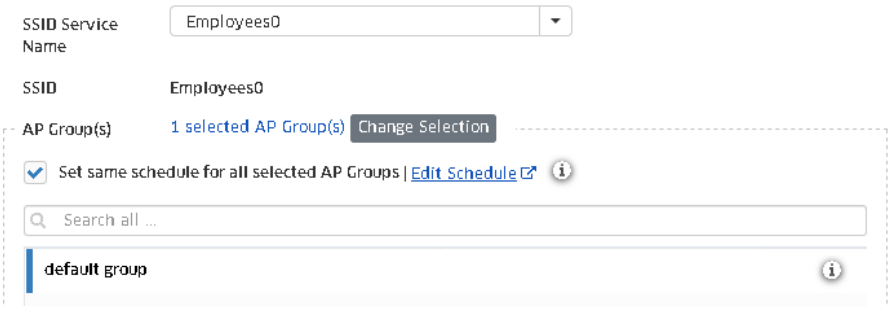
Create an SSID for the VPN Data Tunnel

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

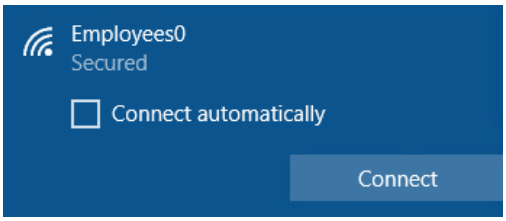
1. Create an SSID.

```
> 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.



3. OmniVista 2500 will push the configuration to the Remote Access Point allowing users to connect to the SSID just configured.



Add a Route to Reach the VPN VA from OmniVista

```
**********************************************************************************************************
* The Virtual Appliance Menu                                                                             *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Configure The Virtual Appliance                                                                    *
* [3] Run Watchdog Command                                                                               *
* [4] Upgrade/Backup/Restore VA                                                                          *
* [5] Change Password                                                                                    *
* [6] Logging                                                                                            *
* [7] Login Authentication Server                                                                        *
* [8] Power Off                                                                                          *
* [9] Reboot                                                                                             *
* [10] Advanced Mode                                                                                     *
* [11] Set Up Optional Tools                                                                             *
* [12] Convert to Cluster                                                                                *
* [13] Join Cluster                                                                                      *
* [0] Log Out                                                                                            *
**********************************************************************************************************
(*) Type your option:
```

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.

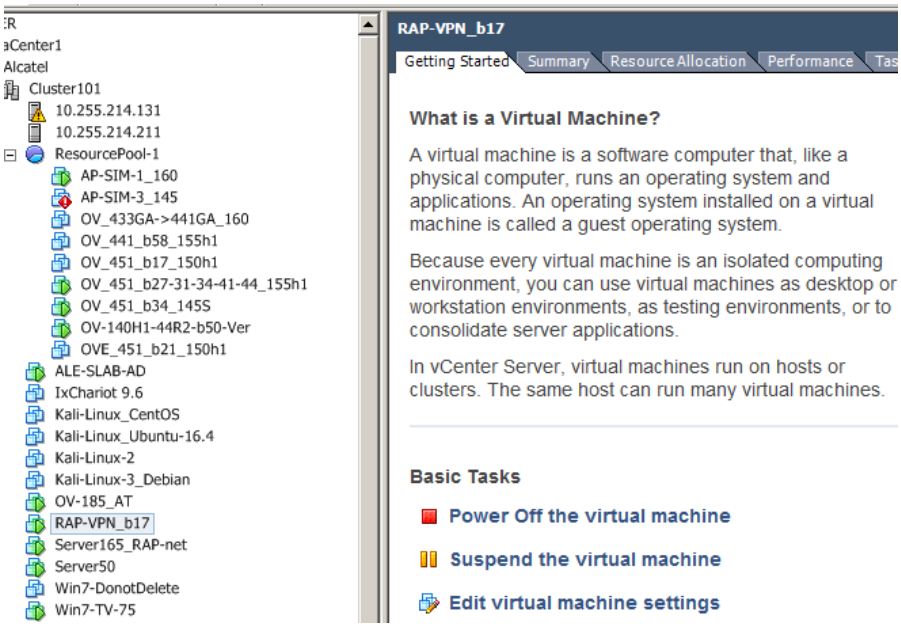
```
**********************************************************************************************************
* Configure Route                                                                                        *
**********************************************************************************************************
* [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
```

Upgrading the VPN VA

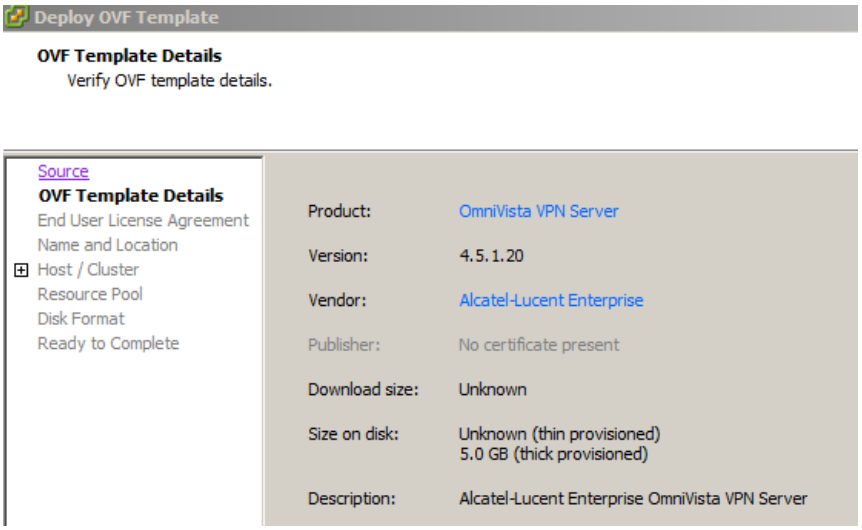
This section documents an example upgrade from version 4.5.1.17 to 4.5.1.20. Details shown on VMWare. The following summarizes the process of upgrading a VPN VA.

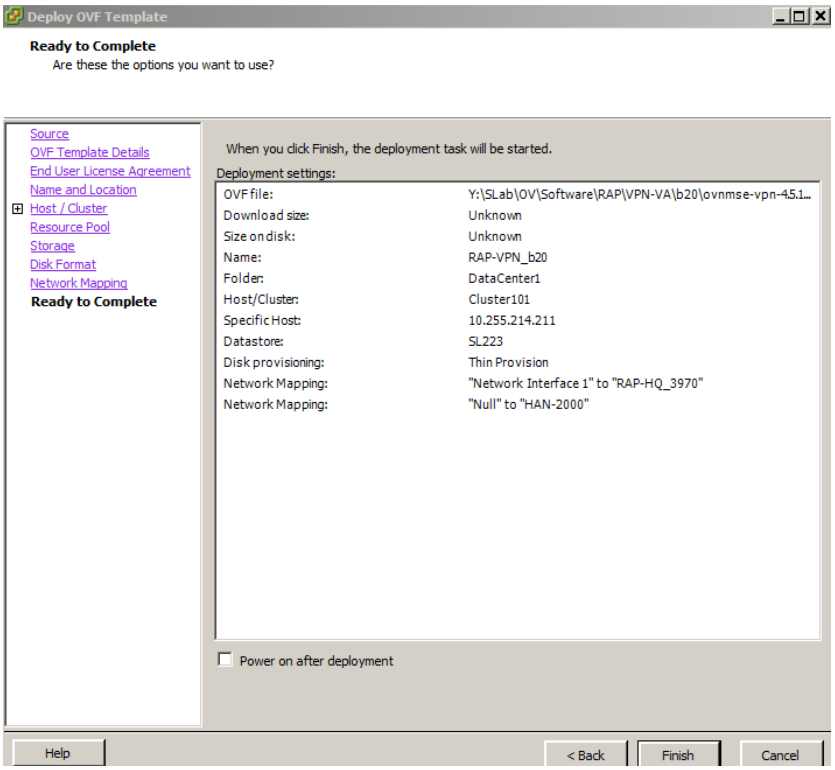
- Power off the VA.
- Deploy new OVF template.
- Copy the OS virtual disk file to the location of current VA.
- Remove (0,0) IDE disk from the VA.
- Recreate the disk with new copied virtual disk file.
- Power on the VA.

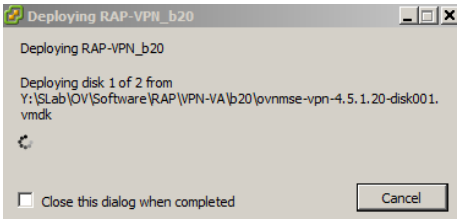
1. Power off the existing VA (RAP-VPN_b17).

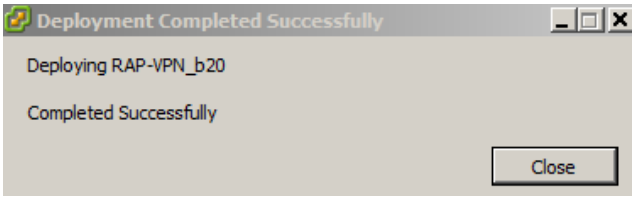


Deploy a new OVF template using the 4.5.1.20 version files.

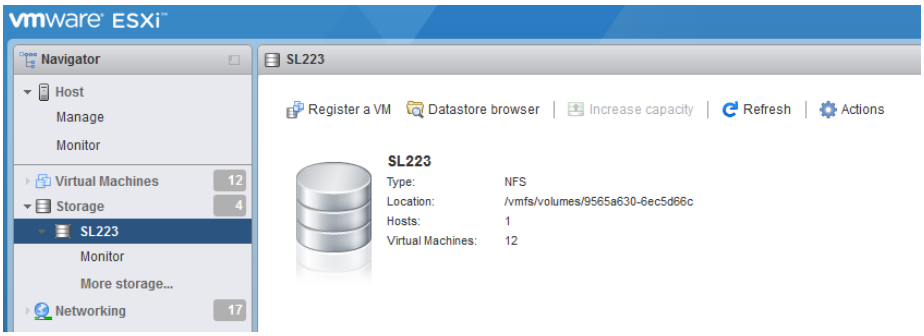




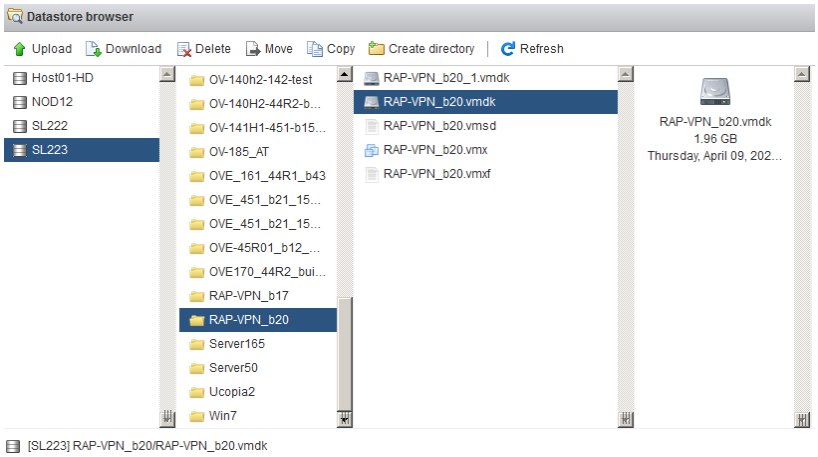




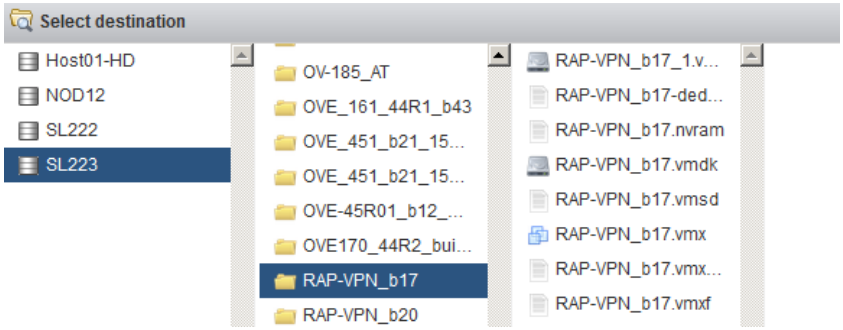
2. Copy the OS virtual disk file (RAP-VPN_b20.vmdk) to the location of current VA (RAP-VPN_b17). On VMWare web client, click "Datastore browser".



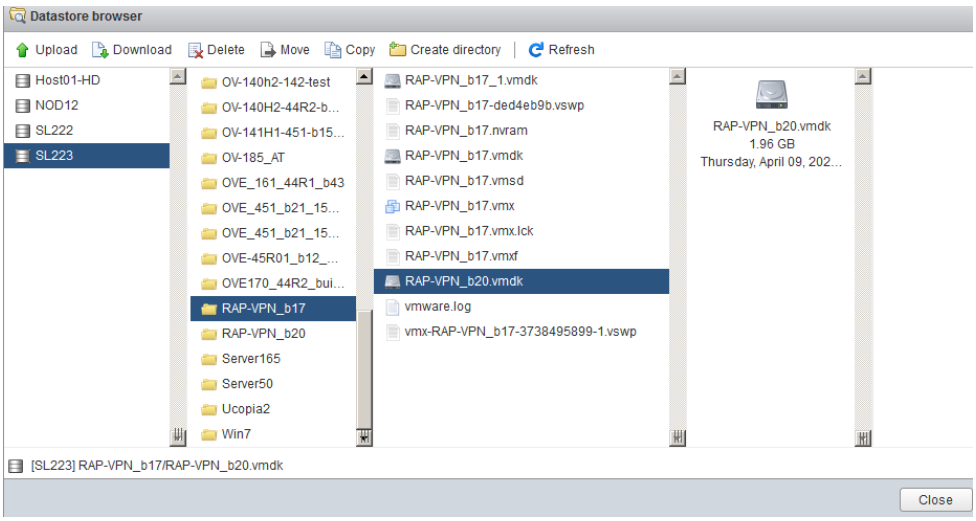
a. In the Datastore browser, highlight the file (RAP-VPN_b20.VMDK).



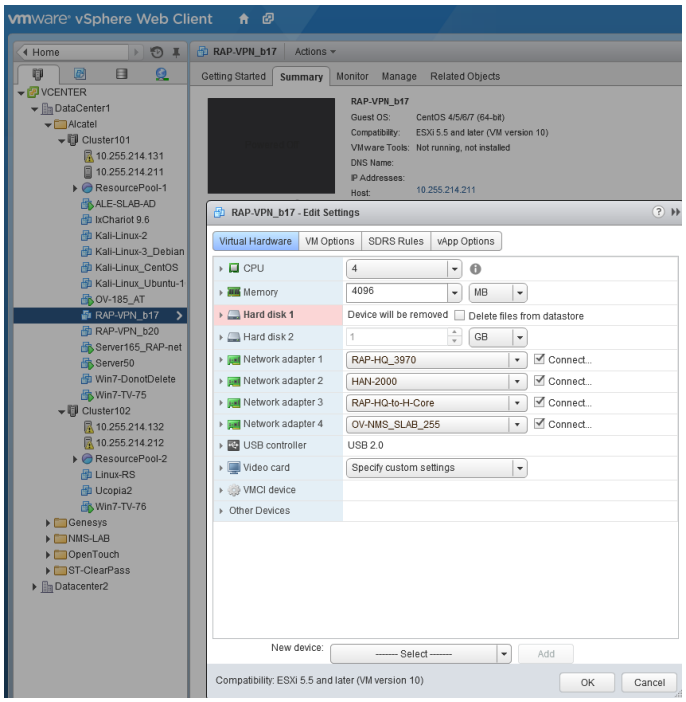
b. Click “Move” and select the destination folder (RAP-VPN_b17).



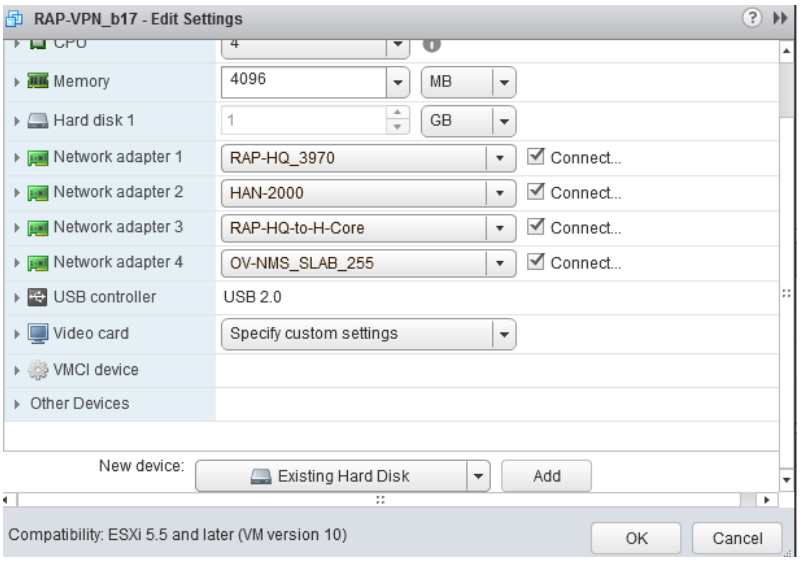
c. Verify the move.



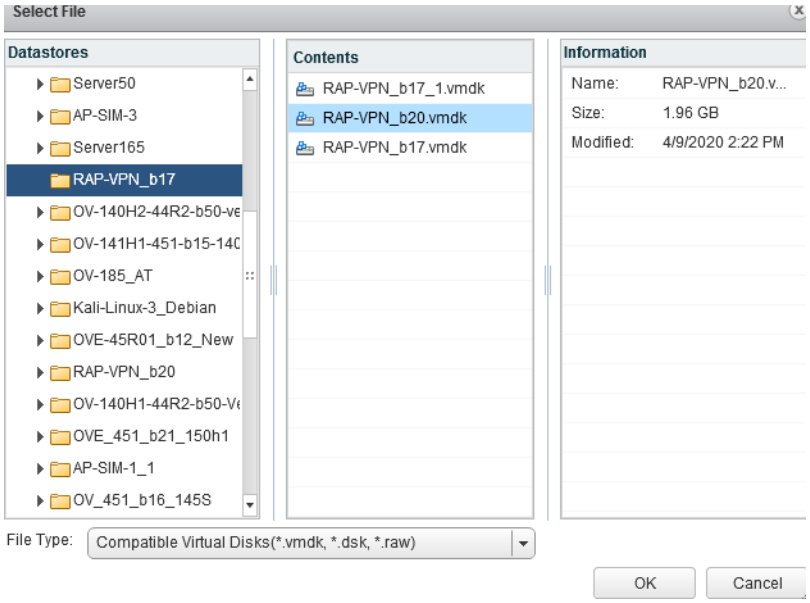
3. Remove Hard Disk 1, (0,0) IDE disk from the current VA. In vSphere Web Client, edit the existing VA, remove HD1 and click OK.



4. Recreate the disk with new copied virtual disk file, "RAP-VPN_b20.vmdk". New device >> Existing Hard Disk>> Add.



a. Select the virtual hard disk file (RAP-VPN_b20.vmdk):



5. Power on the VA (RAP-VPN_b17).

Be patient, it will take some time for all of the services to come up.

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