

# **Table of Contents**

Remote Access Points and VPN Tunnel Components	1
VPN for Management and Data (OVE Managed APs)	1
VPN for Data Only (OVC Managed APs)	2
Prerequisites	2
Network Topology	2
Remote Access Points and VPN Tunnel Configuration	3
Creating an OmniVista Cirrus Freemium Account	3
Adding Remote APs to the Device Catalog	5
Adding Remote APs Manually	5
Importing Multiple Remote APs	8
Deploying/Configuring the VPN Tunnel Server	10
Recommended VPN VA Configurations	10
Known Limitations	11
Deploying the VPN Virtual Appliance	11
Deploying the Virtual Appliance on VMware	11
Deploying the Virtual Appliance on Hyper-V	21
Configuring the VPN Virtual Appliance	33
Complete the Installation	34
Configure NICs	36
Configure Routes	38
Configure Network Settings (DNS, Gateway)	39
Configure an SSH Service	42
Upload the VPN Settings to the VPN Server	43
Configure the VPN Service	45
Configure VPN Endpoints	47
Configuring the VPN Data Tunnel	49
Configure VPN Endpoints	51
Create an SSID for the VPN Data Tunnel	53
SSID with Tagged VLAN	54
SSID with Untagged VLAN	54
SSID with Local Breakout	55
Creating a Tunnel Profile for 1201H Downlink Ports	56
Configuring an Access Auth Profile for an AP Downlink Port	57
Add a Route to Reach the VPN VA from OmniVista	58

Using Dual Stack Lite ISP Connections with Stellar RAPs			
Upgrading the VPN VA	61		
Basic Troubleshooting Checklist	63		
Useful Logs and Commands	63		
Local Breakout Troubleshooting	65		
-			

# **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 preprovisioning 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, 7.0.2, 8.0 are supported (ESXi 5.5 is not supported).
- Hyper-V 2016, 2019, and 2022
- Supported Stellar RAP version is AWOS 4.0.4.6007 and higher.
- The virtual appliance version 4.8.1.2 is certified for use with OmniVista 2500 4.8R1 and OmniVista Cirrus version 4.8.1.
- RAP VPN VA version 4.8.1.2.

## **Network Topology**

Within this document we will use the following network topology:



# **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 4.0.4.6007 and higher. For the latest features, AWOS 4.0.4.6007 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 <u>OV Registration Portal</u>.

Alcatel·Lucent Enterprise OmniVista Cirrus	
▲ Usemame	
A Password	
+) Sign in	
or	
Create New Account	
Need help setting started	
Ecrect.vour.commercit2	

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 <u>add APs one-at-a-time</u> or <u>import multiple APs</u> at once using a .csv file.

### Adding Remote APs Manually

1. Select Network - Inventory - Device Catalog to bring up the Device Catalog application.

Alcatel+Lucent	Ø	NETWI	DRK+ CONFIGURATION	Home 🔺	reesqa 🔳 🌲	Support Center 🖬 🕅	Videos   About   Copput  Copput Co
INVENTORY	*	# Home > Network > Invento	ry > Device Catalog				
Device Catalog		Device Catalog	Latest Refresh: 2	0 mins ago 🗢 Export V	PN Settings Manag	e Bévrog Licenses 🚺 Gr	reate Site Import + ?
Device Troubleshooting							
Managed Inventory	>	Q search all _	Advanced Fi	iter			
		Set Software Version	mie Jehase Lorme	Troubleshoot Device	e Auftreaktion Log.  🗭	8	<b>± </b>
		Serial Number	Model	Current Software Vers	Desired Software Ver	s Device Status	Device Category
		Show 1000 •				Showing Pag	, ke 1 of 1

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

Add a Device		
		(") indicates a required field
*Serial Number	ex: SSZ17000000	
Device Type	LAN Device	
Desired Software Version	Do Not Upgrade	
		Create

**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).

*Serial Number	SSZ182000166		
	C-11-1107 1-11-1-1		
MAC ADDRESS	Enter MAX, Address		
Is this a Remote AP ?	( HS )		
VPN Settings			
Create New VPN Setti	ngs O Choose Existing	VPN Settings	
"VPN Settings Name	Enter maximum 32 char	acters	
"Server's Public IP	Enter IP Address (101.	*Port ex 9001	
"Server's VPN IP	Enter IP Address		
*OmniVista Enterprise Server IP	Enter IP Address		
Client VPN IP	Address Pool		
	IP Range	O Shorthand Mask	
"IP Range	Enter Start IP	Enter End IP	
*Subnet Mask	Enter Subnet Mask		

**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.

Alcatel·Lucent 🕖	III Home 🔺 freesqs 📰 🌲 Support Center III Videos 🔮 About 🔅 Logout NETWORK - CONFIGURATION - UNIFIED ACCESS - SECURITY - ADMINISTRATION - LINE More Logout Logout
INVENTORY 📌	W Home > Network > Inventory > Device Catalog
Device Catalog	Device Catalog Latest Refresh: 20 mins ago C Export VPN Settings Minuse Device Lucroses Greate Site Import + ?
Device Troubleshooting	
Managed Inventory >	Q. Search all Advanced Filter
	Set Software Version 🛛 Asign Company Transfer Lorman Transferboot Device 🛛 View Antimative Leg. 📝 😫 📥 🖨
	Serial Number Model Current Software Vers., Desired Software Vers., Device Status Device Category
	Show 1000 •         Showing Page 1 of 1 • • • 1 > >

**2.** Click on the **Import** button in the upper-right corner of the screen to bring up the Import Devices Screen.

Import devices					
	*File	Choose File	Browse	🛓 Template	(°) indicates a required field
					Import Cancel

**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).

I	ਜ਼ <del>5</del> • ∂ - ਜ	;	device	s_sample_template-1.csv [	Read-Only] - Excel	Brewster	John 🗹 —	οx
F	ïle Home	Insert Page Layo	ut Formulas	Data Review View	Acrobat	? Tell me what you	want to do	Aµ Share
Get (	Get       Properties       All +       Edit Links       Sort       Filter       Filter       Total							~
H2	23 🔻 :	$\times \checkmark f_x$						~
	А	В	С	D	E	F	G	H
1	SerialNumber	MacAddress	SiteId	GeoLocation	RAP	VpnSettingName	2	
2	R328102P		BANGALORE_Site	gps[13.057152::77.5950	46]			
3	T49Q0728	34:e7:0b:00:0e:80		26801 Agoura Rd:: Ago	ura Hills:: CA 9130	1:: USA (NOTE - u	se :: as delim inste	ad of comma)
4	ABC123456789		CALABASAS_Site					
5	DEF123456780	34:e7:0b:00:0e:81		gps[34.170864::-118.60	5576]			
6	RAP123456789				TRUE	vpn-server1		
7	SSZ123456780							
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22		 						
	de	vices_sample_templa	ate-1 (+)		: [4]			
Rea	ady 🔠 🗉 – 🕂 100%							

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.

I	<b>ਜ਼ •</b> - ੇ	÷ ∓		devi	ces_sample	_template_1.	csv [Read-O	nly] - Excel	[	Brewster J	ohn 🖻	-		×
F	ile Home	e Insert Page Lay	out	Formulas	Data	Review	View A	crobat	♀ Tell me w	hat you w	ant to do		R₁ si	hare
Pa Clip	ste 💉 B	libri • 11 • I <u>U</u> •   ⊞ •   <u>⊅</u> Font	A A • <u>A</u> •		∎ ॐ • ≣ •≣ •≣	Ge \$ € ↓ ↓ ↓ ↓	neral ▼ ▼ % ۶ .00 umber 5	₽ Conditi ₽ Format Cell Sty	ional Formatt as Table * les * Styles	ing - a	Delete  Format Cells	$\sum_{x} \cdot \sum_{z}^{A} \cdot x \cdot x$ $\bigcup_{x} \cdot \sum_{z}^{A} \cdot x$ Editing		^
P3	8 *	: × ✓ f <sub>x</sub>												٧
	А	В	С	D	E	F	G	н	I	J	К	L	м	
1	SerialNumbe	er MacAddress	SiteId	GeoLocati	RAP	VpnSetti	ngName							
2	SSZ18200125	8 34:E7:0B:03:C7:70			TRUE	LAB6								
3	SSZ18200125	9 12:34:56:78:30:09			TRUE	LAB6								
4	SSZ18200126	0 12:34:56:78:30:01			TRUE	LAB6								
5	SSZ18200126	1 DC:08:56:2D:4E:F0			TRUE	LAB6								
6	SSZ18200126	2 DC:08:56:2D:62:10			TRUE	LAB6								
7	SSZ18200126	3 DC:08:56:2D:57:60			TRUE	LAB6								
8	SSZ18200126	4 DC:08:56:0D:C4:90			TRUE	LAB6								
9	SSZ18200126	5 DC:08:56:0D:30:E0			TRUE	LAB6								
10	SSZ18200126	6 DC:08:56:0D:30:E1			TRUE	LAB6								
11	SSZ18200126	7 DC:08:56:0D:30:E2			TRUE	LAB6								
12	SSZ18200126	8 DC:08:56:0D:30:E3			TRUE	LAB6								
13	SSZ18200126	9 DC:08:56:0D:30:E4			TRUE	LAB6								
14	SSZ18200127	0 DC:08:56:0D:30:E5			TRUE	LAB6								
15	SSZ18200127	1 DC:08:56:0D:30:E6			TRUE	LAB6								
16	SSZ18200127	2 DC:08:56:0D:30:E7			TRUE	LAB6								
17	SSZ18200127	3 DC:08:56:0D:30:E8			TRUE	LAB6								
18	SSZ18200127	4 DC:08:56:0D:30:E9			TRUE	LAB6								
19	SSZ18200127	5 DC:08:56:2D:50:00			TRUE	LAB6								
20	SSZ18200127	6 DC:08:56:2D:50:01			TRUE	LAB6								
21	SSZ18200127	7			TRUE	LAB6								
22	SSZ18200127	8			TRUE	LAB6								-
	<	devices_sample_temp	late_1	+				: •						Þ
Rea	dy										<b>_</b>	-	+ 100	%

## 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 <u>deploying</u> and <u>configuring</u> a VPN VA.

## **Recommended VPN VA Configurations**

The VPN VA and NIC configurations are based on the number of Remote APs being managed. The number of Virtual NICs supported by RAP VPN VA are limited only by the hypervisor. RAP VPN VA does not impose any limits on this.

- 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 <u>here</u> 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 <u>VMware</u> or <u>Hyper-V</u>. After deploying the VA, <u>configure the VA and complete the installation</u>.

### 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.

vmware <sup>,</sup> Esxi <sup></sup>		root@10.25	55.222.89 -   Help -   Q Search	•			
📲 Navigator	ovvmhost-4.arch.test.ind.alcatel.com						
Host         Manage         Monitor         ▼ ♥ Virtual Machines         3         ▶ ♥ OVE 4.5R3 Build 57         More VMs         ▶ ■ Storage       2         ▶ ● Networking       3	Manage with vCenter Server     Yovmhost-4.arch Version: 6.5.0 (Bu State: Normal ( Uptime: 49.87 da	Create/Register VM   Bo Shut down .test.ind.alcatel.com ild 4887370) connected to vCenter Server at 10.255.22 ys	CPU       FREE: 17.9 GHz         USED: 798 MHz       CAPACITY: 18.7 GHz         MEMORY       FREE: 17.84 GB         USED: 2.16 GB       CAPACITY: 20 GB         STORAGE       FREE: 396.76 GB         USED: 5.74 GB       CAPACITY: 40.7 GB	* III			
	▼ Hardware	_					
	Manufacturer	HP					
	Model	ProLiant DL380 G5					
	F 🔲 CPU	8 CPUs x Intel(R) Xeon(R) CPU E5410 @ 2.33GHz					
	🛲 Memory	20 GB					
	🕨 🔚 Virtual flash	0 B used, 0 B capacity					
	👻 😡 Networking						
	Hostname	owmhost-4.arch.test.ind.alcatel.com		-			
	🕄 Recent tasks						
	Task v Target	✓ Initiator ✓ Queued ✓ State	arted v Result v Complete.	×			
	Destroy 🔂 OVE 4.5R3	Bu root 03/05/2021 1 03	/05/2021 1 🔮 Completed successfully 03/05/2021	1			
	Power Off VM 🚯 OVE 4.5R3	Bu root 03/05/2021 1 03	V05/2021 1 Completed successfully 03/05/2021	1			

**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.

🔁 New virtual machine			
<ul> <li>Select creation type</li> <li>Select OVF and VMDK files</li> <li>Select storage</li> <li>License agreements</li> </ul>	Select creation type How would you like to create a Virtual Machine?		This option quides you through the process of creating a
5 Deployment options 6 Additional settings 7 Ready to complete	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine		virtual machine from an OVF and VMDK files.
		Ţ	
<b>vm</b> ware <sup>®</sup>			Back Next Finish Cancel

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

🔁 New virtual machine - RAP VA 4.8.1	Build 2
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Ready to complete</li> </ul>	Select OVF and VMDK files         Select the OVF and VMDK files or OVA for the VM you would like to deploy         Enter a name for the virtual machine.         RAP VA 4.8.1 Build 2         Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
	<ul> <li>vm ovnmse-vpn-4.8.1.2.ovf</li> <li>ovnmse-vpn-4.8.1.2-disk001.vmdk</li> <li>ovnmse-vpn-4.8.1.2-disk002.vmdk</li> </ul>
vmware	
	Back Next Finish Cancel

**5.** Enter a name for the VM (e.g., VPN VA 4.8.1 Build 2), 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.

🖆 New virtual machine - RAP VA 4.8.1	Build 2						
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Ready to complete</li> </ul>	Select storage Select the storage type and datastore Standard Persistent Memory Select a datastore for the virtual machine's c	configuration file:	s and all of its' v	virtual disks.			
	Name ~	Capacity 🗸	Free ~	Туре	Thin pro ~	Access	~
	datastore 71.207	924 GB	21.2 GB	VMFS5	Supported	Single	
	NAS	10.74 TB	1.23 TB	NFS	Supported	Single	
						2 it	ems
vmware							
3			Ba	ack N	ext Finis	h C	ancel

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

🔁 New virtual machine - RAP VA 4.8.1	Build 2
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 License agreements</li> <li>5 Deployment options</li> </ul>	License agreements Read and accept the license agreements License agreement
6 Ready to complete	Terms and Conditions Acceptance: Read the following End User License Agreement (EULA) carefully before insti Definitions: As used in this Agreement, the term "Software" means collectively (i) the software program(s) ( "Affiliated Companies" means any entity controlling, controlled by or under common control, directly or ind: "Order of Precedence": If You received more than one license terms purporting to govern the use of the Mater Parties: This agreement is between (a) the legal entity which has a separate purchase agreement with a Part 1. License Grant: Subject to all other terms in the agreement, and subject to the payment of the applicable Additional or different terms and conditions to modify, copy, or distribute the Material may be granted to I
<b>vm</b> ware*	All licenses granted hereunder are contingent upon full payment of fees, if any, specified in the separate ; 2. License restrictions: Unless authorized by the applicable law with no possibility to contractually super: 3. Third Party software: Licensee acknowledges that third party software, including without limitation "Free lagree
	Back Next Finish Cancel

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

🔁 New virtual machine - RAP VA 4.8.1 I	Build 2	
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> </ul>	Deployment options Select deployment options	
<ul> <li>✓ 4 License agreements</li> <li>✓ 5 Deployment options</li> <li>✓ 6 Ready to complete</li> </ul>	Network mappings	Network Interface 1     Network71.x     ~       Null     Network71.x     ~
	Disk provisioning	Thin      Thick
	Power on automatically	
<b>vm</b> ware*		
		Back Next Finish Cancel

**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**.

P New virtual machine - RAP VA 4.8.1	Build 2	
<ul> <li>✓ 1 Select creation type</li> <li>✓ 2 Select OVF and VMDK files</li> <li>✓ 3 Select storage</li> </ul>	Ready to complete Review your settings selection before finit	shing the wizard
<ul> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Ready to complete</li> </ul>	Product VM Name Files	OmniVista VPN Server RAP VA 4.8.1 Build 2 Ruppeo van 4.8.1 2 disk001 vmdk
	Datastore	ovnmse-vpn-4.8.1.2-disk002.vmdk NAS
	Provisioning type Network mappings	Thin Network Interface 1: Network71.x,Null: Network71.x
	Guest OS Name Do not refresh your brows	RedHat_64
<b>vm</b> ware		Back Next Finish Cancel

**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.

a RAP VA 4.8.1 Build 2										
Console Monitor	Power on Power	er off 🔢 Suspend 🔄 Restart 丨 ,	🖌 Edit   🧲 Refresh   🥸	Actions						
		RAP VA 4.8.1 Build 2 Guest OS Compability VMware Tools CPUs Memory	CentOS 4/5 or later (64-bit) ESXI 5 5 virtual machine No 4 2 GB							O MHZ 0 MHZ 0 B storage 0 B
▼ General Information					11	▼ Hardware Co	Infiguration			
Metworking	No network i	information				P CPU		4 vCPUs		
+ 📾 VMware Tools	Unknown					Memory		2 GB		
► I Storage	2 disks					• 🛄 Hard disk	1	8 GB		
Notes	Alcatel-Luce	nt Enterprise OmniVista VPN Server		🥖 Edit notes	1	+ 🛄 Hard disk	2	1 GB		
					1	🖶 USB contr	oller	USB 2.0		
						• MI Network a	dapter 1	Network71.	x (Connected)	
						• MIN Network a	dapter 2	Network71.	x (Connected)	
						• MI Network a	dapter 3	Network71.	x (Connected)	
						Video card	1	4 MB		
						Others		Additional H	lardware	
						<ul> <li>Resource Co</li> </ul>	nsumption	0.000		
						Consumed	I host CPU	0 MHz		
						Consumed	host memory	0 MB		
						Active gue	st memory	0 MB		
Recent tasks										
ask	~	Target	✓ Initiator	~ Queued		~	Started	~	Result 🔺 🗸 🗸 🗸	completed 🕶 🗸 🗸
pload disk - ovnmse-vpn-4.8.1.2-disk001.v	mdk (1 of 2)	PAP VA 4.8.1 Build 2	admin	08/16/2023 09:	52:58		08/16/2023 09:52:58		R	unning 9 %
pload disk - ovnmse-vpn-4.8.1.2-disk002.v	mdk (2 of 2)	B RAP VA 4.8.1 Build 2	admin	08/16/2023 09:	:52:58		08/16/2023 09:52:58		Completed successfully 08	B/16/2023 09:53:06
nport VApp		Resources	admin	08/16/2023 08:	:57:55		08/16/2023 08:57:55		<b>R</b>	unning 51 %
nport VApp		Resources	admin	08/16/2023 08:	:49:31		08/16/2023 08:49:31		<b>N</b> R	unning 79 %
ower On VM		B (Dev) Capex 71.141 48R1_B40_ANHVO	admin	08/16/2023 09:	:07:41		08/16/2023 09:07:41		Completed successfully 09	8/16/2023 09:07:54
ower Off VM		[Dev] Capex 71.141 48R1_B40_ANHVO	admin	08/16/2023 09:	:07:23		08/16/2023 09:07:23		Completed successfully 01	8/16/2023 09:07:34

**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.

Console Monitor	Power on OP ower of I Supp VPN VA 4.8.1 Build 2 Guest OS Compatibility VMware Tools CPUS Memory	end Y Reset   / Edit CentOS 4/5/6/7 (64-bit) ESXI 5.5 virtual machine No 4 2.6B	C Refresh	Actions		O MHZ O MHZ O B STORAGE 5.3 GB
VMware Tools is not installed in     Actions  General Information     Networking	this virtual machine. VMware Tools allows de	tailed guest information to be displa	ayed as well as allowing	you to perform operations on the	he guest OS, e.g. graceful shutdown, reboot, etc. You should install VMwar 4 vCPUs	re Tools.
2				M (2012)		
VMware Tools	VMware Tools is not installed.	ð	Actions	E Memory	2 GB	
VMware Tools     Storage	VMware Tools is not installed. 2 disks	0	Actions	E Memory ⊐) Hard disk 1	2 GB 8 GB	
VMware Tools Storage Notes	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN	l Server	Actions	E Memory Hard disk 1	2 GB 8 GB 1 GB	
A VMware Tools Storage Ø Notes	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN	l Server 🖋 E	Actions and a construction of the construction	Memory Hard disk 1 Hard disk 2 USB controller	2 GB 8 GB 1 GB USB 2 0	
VMware Tools  Storage  Notes Performance summary last hour	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN	i Server 💉 E	Actions	Hard disk 1 Hard disk 2 USB controller Network adapter 1	2 GB 8 GB 1 GB USB 2 0 Internal (Connected)	
VMware Tools  Storage  Notes Performance summary last hour	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN	Server PE	Actions	5 Memory Hard disk 1 Hard disk 2 USB controller 3 Network adapter 1	2 GB 8 GB 1 GB USB 2 0 internal (Connected) internal (Connected)	
VMware Tools  Storage  Storage  Notes  Performance summary last hour	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN Consu	I Server F E med host CPU Ready 2 med host memory	Actions	Memory Hard disk 1 Hard disk 2 USB controller  Network adapter 1 U 0.19 %	2 GB 8 GB 1 GB USB 2 0 internal (Connected) internal (Connected) internal (Connected)	
VWware Tools  Storage  Storage  Performance summary last hour	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN © Consul © Consul	I Server  I Server  Ready  Ready Ready  Ready Ready  Ready Ready  Ready Ready  Ready Re	Actions 2 ( dit notes 2 ( 023/08/16 14:56:30 Consumed host CP Ready	5 Memory ∃ Hard disk 1 ⇒ Hard disk 2 & USB controller a, Network adapter 1 U 0.19 % 0.06 %	2 GB 8 GB 1 GB USS 2.0 internal (Connected) internal (Connected) internal (Connected) 4 MB	
VMware Tools  Storage  Storage  Notes  Performance summary last hour  Cooperations  Door Door Door Door Door Door Door Doo	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN Consul	I Server E E med host CPU Ready 2 med host memory	Actions	B         Memory           Hard disk 1           Hard disk 2           & USB controller           a, Network adapter 1           U         0.19 %           0.06 %           mory (right axis)         0.78 GB	2 GB 8 GB 1 GB USB 2 0 internal (Connected) internal (Connected) 4 MB Additional Hardware	
V Wware Tools  Storage  Storage  V Ware  Performance summary last hour  V  V  V  V  V  V  V  V  V  V  V  V  V	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN Consul Consul	I Server E med host CPU Ready a med host memory	Actions	B         Memory           Arad disk 1           Hard disk 2           & USB controller           a, Network adapter 1           U         0.19 %           0.06 %           mory (right axis)         0.78 GB           Resource Consumption	2 GB 8 GB 1 GB USS 2 0 internal (Connected) internal (Connected) internal (Connected) 4 MB Additional Hardware	
VWware Tools  Strage  Strage  Voice  Performance summary last hour  Voice  Voice  0  Voice  0  0  0  0  0  0  0  0  0  0  0  0  0	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN Consul	UServer E med host CPU Ready Z med host mmory	Actions	B         Memory           Arad disk 1	2 GB 8 GB 1 GB USB 2 O internal (Connected) internal (Connected) internal (Connected) 4 MB A dditional Hardware	
VMware Tools     Storage     Vmare Tools     Storage     Vmare Tools     Notes  Performance summary last hour      Votes      Vmare tools     Vmare tools	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN Consur Consur Consur	Server E med host CPU Pready 2 med host memory	Actions a factor of the second	B Memory	2 GB 8 GB 1 GB 1 GB 1 GB 1 GB 1 GB 2 O 1 Gomected) 1 Internal (Connected) 1 Internal (Connected) 1 Internal (Connected) 4 MB A dottional Hardware 0 MHz 0 MHz 0 MB	
VMware Tools     Storage     Storage     Notes  Performance summary last hour      00 Gene     100     00	VMware Tools is not installed. 2 disks Alcatel-Lucent Enterprise OmniVista VPN Consur Consur Consur	I Server E E	Actions 2 4 dit notes 2 4 dit notes 2 4 dit notes 2 4 2 5 2 6 3 1 3 1 3 2 4 2 6 3 1 3 1 3 1 3 2 4 4 5 6 4 5 6 5 7 6 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	B         Memory           B         Hard disk 1           B         Hard disk 2           W USB controller         0.19 %           0. Network adapter 1         0.19 %           0.06 %         0.06 %           mory (right axis)         0.78 GB           V         0.19 %           0.06 %         0.06 %           Consumed host CPU         0.06 %           Gonsumed host CPU         5           Setting used thermory         5	2 GB 8 GB 1 GB 1 GB 1 GB 1 GB 1 GB 1 GB 2 O 1 Internal (Connected) 1 Internal (Connected) 1 Internal (Connected) 4 MB Additional Hardware 0 MHz 0 MHz 0 MB	

#### **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.

Name		
VLAN ID	4095	
Virtual switch	vSwitch0	
Security	Click to expand	
NIC teaming	Click to expand	
Traffic shaping	Click to expand	

 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".

🥒 Edit port group - Data Brigde	
Name	
VLAN ID	4095 🜩
Virtual switch	vSwitch0
▼ Security	
Promiscuous mode	○ Accept ○ Reject ● Inherit from vSwitch
MAC address changes	○ Accept ○ Reject ● Inherit from vSwitch
Forged transmits	○ Accept ○ Reject ● Inherit from vSwitch
► NIC teaming	Click to expand
▶ Traffic shaping	Click to expand
	Save Cancel

• 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.

Add uplink		
MTU	1500	
Uplink 1	vmnic0 - Up, 1000 mbps 🔻	0
Link discovery	Click to expand	
- Security		
Promiscuous mode	● Accept ○ Reject	
MAC address changes	Accept      Reject	
Forged transmits	Accept      Reject	
NIC teaming	Click to expand	
Traffic shaping	Click to expand	

**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 <u>Configuring the VPN Virtual Appliance</u> 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**.

		<u> </u>
Navigator	Q esxi72.tma.com.vn - Networking	
✓ ☐ Host Manage Monitor	Port groups Virtual switches Ph	ysical NICs VMkernel NICs TCP/IP stacks Firewall rules
Virtual Machines     Virtual Machines     ovnmse-vpn-4.5.1.21     Monitor     Gi [HA Stability] ovnmse-4     Monitor	Name VSwitch0 VSwitch2 VSwitch3	<ul> <li>Port groups</li> <li>7</li> <li>0</li> <li>1</li> </ul>
More VMs  Storage  Networking  Networking  Networking  More networks	vSwitch0 Type: Port groups: Uplinks:	Standard vSwitch 7 1

2. Select the uplink.

🥒 Edit standard virtual switch -	vSwitch0	
🔜 Add uplink		
MTU	1500	
Uplink 1	vmnic0 V	8
Uplink 2	vmnic1 Vmnic1	$\otimes$
► Link discovery	vmnic1	
▶ Security	Click to expand	
► NIC teaming	Click to expand	
▶ Traffic shaping	Click to expand	
		Save Cancel

**3.** Edit the virtual switch and configure the load balancing rule.

Uplink 1	vmnic0 🔻		¢		
Uplink 2	vmnic1 •		6		
Link discovery	Click to expand				
Security	Click to expand				
NIC teaming					
Load balancing	Route based on IP hash				
Network failover detection	Link status only				
Notify switches	€ Yes C No				
Failback	© Yes C No				
Failover order	Mark standby 📑 Move up	≣₄ Move down			
	Name	Speed	Status		
	Max vmnic0	1000 Mbps, full duplex	Active		
	M vmnic1	Link down	Active		

## 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-4.8.1.2.ovf, ovnmse-vpn-4.8.1.2-disk001.vmdk and ovnmse-vpn-4.8.1.2-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**.

Name	Date modified	Туре	Size
] hyperv	8/15/2023 12:46 PM	File folder	
ovnmse-vpn-4.8.1.2.mf	8/15/2023 12:47 PM	MF File	1 KB
ovnmse-vpn-4.8.1.2.ovf	8/15/2023 12:47 PM	OVF File	29 KB
ovnmse-vpn-4.8.1.2-disk001.vmdk	8/15/2023 12:47 PM	VMDK File	1,644,331 KB
ovnmse-vpn-4.8.1.2-disk002.vmdk	8/15/2023 12:47 PM	VMDK File	101 KB

#### **2.** Import the VM into Hyper-V.

					Нуре	r-V Manager		
File Action Vie	ew Help							
🗢 🄿 🔁 📰	?							
Hyper-V Mana	ger	Virtual Machir	ies					
	Import Virtual Machine	Name	<b>^</b>	State	CPU Usage	Assigned Memory	Uptime	Status
		OmniVista-VPN-4	.8.1	Off				
	Hyper-V Settings							
	Virtual Switch Manager							
	Virtual SAN Manager	-						
	Edit Disk							
	Inspect Disk							
	Stop Service							
	Remove Server							
	Refresh							
	View 🕨							
	Help							

3. Select the location folder to Hyper-V source of VPN VA.

2		Select Fold	ler			x
. € 💿 🕶 🕇 🎩	< Local Disk (C:)	► OV Builds ► vpn-va-4.8.1.2 ►	<u>ب</u> ج	Search vpn-va-4.8.1.	2	,o
Organize 👻 New fo	lder				-	0
E Desktop	^ Name	*	Date modified	Туре	Size	
🚺 Downloads 🖳 Recent places	🍌 hype	rv	8/15/2023 12:46 PM	File folder		
<ul> <li>This PC</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> </ul>	Ξ					
🙀 Network	~ <		Ш			>
F	older: vpn-va-4	.8.1.2				
				Select Folder	Cancel	

4. Select the Import Type: Copy the Virtual Machine.

	Import Virtual Machine
Choose Imp	ort Type
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Summary	Choose the type of import to perform: <ul> <li>Register the virtual machine in-place (use the existing unique ID)</li> <li>Restore the virtual machine (use the existing unique ID)</li> <li>Copy the virtual machine (create a new unique ID)</li> </ul>
	< Previous Next > Finish Cancel

- 5. Choose Destination and Storage Folder. You can use the default or customize the location.
- 6. Click Finish to complete the VA import.

	Import Virtual I	Machine		x
Completing I	mport Wizard			
Before You Begin Locate Folder Select Virtual Machine	You are about to perform the following Description:	Operation.		1
Choose Import Type Choose Destination Choose Storage Folders Summary	Virtual Hacline. Import file: Import Type: Virtual machine configuration folder: Checkpoint folder: Smart Paging file store: Virtual hard disk destination folder:	C: \OV Builds\vpr-va-4.8.1.2\hyp Copy (generate new ID) C:\ProgramData\Wicrosoft\Windo C:\ProgramData\Wicrosoft\Windo C:\ProgramData\Wicrosoft\Windo C:\Users\Public\Documents\Hype	erv\Virtual Machines\ab38891Ł wws\Hyper-V\ wws\Hyper-V\ ws\Hyper-V\ r-V\Virtual Hard Disks\	t
	< IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	II vizard, dick Finish.	<b>&gt;</b>	
	[	< Previous Next >	Finish Cancel	]

7. Edit the Virtual machine and remove the Network interface.

Settings for OmniVista-VPN-4.8.1 on HYPERV87					
OmniVista-VPN-4.8.1	] ∢ ▶   Q				
★ Hardware       ▲         ▲       ▲         ▲       ■         ■       ■	Image: Specify the configuration of the network adapter or remove the network adapter.         Virtual switch:         Not connected         VLAN ID         Enable virtual LAN identification         The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.         2				
DVD Drive None     SCSI Controller     General Drive ovrmse-vpn-4.8.1.2-disk0      Ovrmse-vpn-4.8.1.2-disk0      Com 1     None     Com 2     Mone	Bandwidth Management         Enable bandwidth management         Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.         Minimum bandwidth:       0         Mbps         Maximum bandwidth:       0         Mbps         More than the minimum of maximum unrestricted, specify 0 as the value.				
None Diskette Drive None None None None None None None Non	To remove the network adapter from this virtual machine, dick Remove.           Remove           Image: statistic state of the state of				
C:\ProgramData\Microsoft\Win	OK Cancel Apply				

- 8. Run the commands below on Power shell to create 3 Network Adapters.
  - 1. For (\$Count=0; \$Count -le 2; \$Count ++)
    2. {
    3. Add-VMNetworkadapter -VMName OmniVista-VPN-4.5.2 -Name "Eth\$Count"
    }

    Administrator: Windows PowerShell

    Yindows PowerShell

    Yindows PowerShell

    S C:\Users\Administrator>
    PS C:\User

9. Create an "External" Hyper-V virtual switch.



10. Attach to the Physical network interface.

12 Vi	rtual Switch Manager for HYPERV87
★ Virtual Switches         Image: Second State         Image: Second Sta	Virtual Switch Properties
Global Network Settings     MAC Address Range     00-15-5D-DD-57-00 to 00-15-5D-D	Connection type What do you want to connect this virtual switch to? External network: Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client) #44   Allow management operating system to share this network adapter Allow management operating system to share this network adapter Cable single-root I/O virtualization (SR-IOV) Internal network Private network VLAN ID Enable virtual LAN identification for management operating system The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
	Remove     SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.     OK Cancel Apply

**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)

	=	
A Hardware	<u>^</u>	📱 Network Adapter
M Add Hardware		Specify the configuration of the network adapter or remove the network adapter.
Boot from CD		Virtual quitteb
Memory		vewitch4
1024 MB		
🗄 🛄 Processor		VLAN ID
4 Virtual processors		Enable virtual LAN identification
IDE Controller 0		The VLAN identifier specifies the virtual LAN that this virtual machine will use for all
Hard Drive		network communications through this network adapter.
IDE Controller 1		70
DVD Drive		
None	≡	Bandwidth Management
🖃 🐼 SCSI Controller		Enable bandwidth management
🗄 🧰 Hard Drive		Specify how this patwork adapter utilizes patwork handwidth. Both Minimum
ovnmse-vpn-4.8.1.2-disk0		Bandwidth and Maximum Bandwidth are measured in Megabits per second.
Wetwork Adapter		Minimum bandwidth: 0 Mbos
vswitch+ ■ 0 Etb0		
vswitch4		Maximum bandwidth: 0 Mbps
🗄 📮 Eth1		To leave the minimum or maximum unrestricted, specify 0 as the value.
vswitch4		
Eth2		To remove the network adapter from this virtual machine, click Remove.
		Remove
{\\.\pipe\		
1 COM 2		Use a legacy network adapter instead of this network adapter to perform a network-based installation of the quest operating system or when integration
None		services are not installed in the guest operating system.
Diskette Drive		
None		
× management	- 1	
OmniVista-VPN-4.8.1		

**13.** Select **Enable virtual LAN identification** on Eth1 and map to private VLAN (e.g., VLAN 1000).

A U		
Add Hardware	<u> </u>	₩ Network Adapter
		Specify the configuration of the network adapter or remove the network adapter.
Boot from CD		Virtual switch:
Memory		vswitch4
1024 MB		VI AN TO
🗄 🔲 Processor		VLAN LD
4 Virtual processors		
IDE Controller 0		The VLAN identifier specifies the virtual LAN that this virtual machine will use for all
ovnmse-vpn-4.8, 1, 2-disk0		network communications through this network adapter.
IDE Controller 1		1000
DVD Drive		
None	≡	Bandwidth Management
🖃 🐼 SCSI Controller		Enable bandwidth management
🗄 🧰 Hard Drive		Specify how this network adapter utilizes network bandwidth. Both Minimum
ovnmse-vpn-4.8.1.2-disk0		Bandwidth and Maximum Bandwidth are measured in Megabits per second.
INETWORK Adapter vswitch4		Minimum bandwidth: 0 Mbps
Eth0		
vswitch4		Maximum bandwidth: 0 Mbps
• 🖞 Eth1		To leave the minimum or maximum unrestricted, specify 0 as the value.
vswitch4		
		To remove the network adapter from this virtual machine, click Remove.
		Remove
" (), \pipe \	E	
T COM 2		Use a legacy network adapter instead of this network adapter to perform a network-based installation of the quest operating system or when integration
None		services are not installed in the guest operating system.
📕 Diskette Drive		
None		
x management	$+ \parallel$	
OmniVista-VPN-4.8.1		

**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-4.8.1 -
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-4.8.1

Z	Administrato	or: Windo	ws PowerShell	_ □	x
PS C:\Users\Adminis	trator> Get-VMNetwork/	AdapterVla	an -VMName OmniVista-	-VPN-4.8.1	<u>^</u>
VMName	VMNetworkAdapterName	Mode	VlanList		
OmniVista-VPN-4.8.1 OmniVista-VPN-4.8.1 OmniVista-VPN-4.8.1 OmniVista-VPN-4.8.1 PS C:\Users\Adminis	Network Adapter Eth0 Eth1 Eth2 trator> _	Untagged Access Access Trunk	70 1000 0,201-202		

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

## Deploying the VPN VA with NIC Teaming

**1.** Open Server Manager - Local Server.

Server Manager	ppager 🖡 Local Ser	a vor	🕶 🙃   🚩 Manane Tr	- D
Server wa		Vei		<u></u>
🔛 Dashboard	For server171			TASKS 🔻
Local Server All Servers AD CS	Computer name Domain Cluster name	server171 ad.omnivista.com server179	Last installed updates Windows Update Last checked for updates	2/25/2020 4:20 Download upda 9/10/2020 7:53
AD DS	Cluster object type	Cluster Node		
<ul> <li>B DNS</li> <li>■ File and Storage Services </li> <li>■ Hyper-V</li> </ul>	Windows Defender Firewall Remote management Remote Desktop	Domain: Off Enabled Enabled	Windows Defender Antivirus Feedback & Diagnostics IE Enhanced Security Configuration	Real-Time Prote Settings On
	NIC2 NIC2 NIC4 vEthernet (vswitch1)	Disabled Authenticating Not connected Multiple IPv4 addresses, IPv6 enabled	Time zone Product ID	(UTC-08:00) Pac Not activated
	Operating system version	Microsoft Windows Server 2019 Standard	Processors	Intel(R) Xeon(R)
	EVENTS All events   162 total			TASKS 💌
	Filter Server Name ID Severit	y Source	Log Date and Time	•

### 2. Edit NIC Teaming - New Team.

IC Teaming									-	
SERVERS All Servers   1 1	otal								TAS	KS T
ame	Status	Server Type	Operating System Version	Teams						
RVER171	Online	Physical	Microsoft Windows Server 2019 Standard	0						
EAMS   Teams   0 total				TASKS 🔻	ADAPTERS AND INTER	(FACES			TASKS	•
Team Statu	s Teaming Mode	Load Balancin	ig Adapters	New Tea	m Adapters Team	Interfaces				
				Propertie	•5	Speed	State Reason			
					<ul> <li>Available to be ad</li> </ul>	ded to a team (3	)			
					vEthernet (vswitch1)	1 Gbps				
					NIC3	1 Gbps				
					AUG2	1.01				
					NIC2	1 Gbps				
					NIC2	1 Gbps				
					NIC2	1 Gbps				
					NIC2	1 Gbps				
					NIC2	1 Gbps				
					NIC2	1 Gbps				
					NIC2	1 Gbps				

3. Choose NIC members, Teaming mode, and Load balancing mode, then click OK.

NIC Teaming			×
New team			
Team <u>n</u> ame:			
NIC Teaming			
Member adapters:			
In Team Adapter	Speed State Reason		
✓ NIC2	1 Gbps		
✓ NIC3	1 Gbps		
vEthernet (vswitch	1) 1 Gbps		
▲ Additional properties			
Teaming mode:	Switch Independent	~	
Load balancing mode:	Address Hash	~	
Standby adapter:	None (all adapters Active)	~	
Primary team interface:	NIC Teaming; Default VLAN		
	Г	01	<b>C</b>
		UK	Cancel

4. Create a Hyper-V virtual switch and attach to the NIC Teaming interface, then click **OK**.

X       Virtual Switches         X       New virtual network switch         Broadcom NetXtreme Gigabit Ether       Name:         Name:       NIC Teaming         Microsoft Network Adapter M       Notes:         On-15-5D-46-AB-00 to 00-15-5D-4       Onenction type         What do you want to connect this virtual switch to?       External network:         Microsoft Network Adapter Multiplexor Driver       Virtual Allow management operating system to share this network adapter         Connection type       Internal network:         Microsoft Network Adapter Multiplexor Driver       Virtual Xalow management operating system to share this network adapter         Internal network       Private network         VID       Internal network         VEN ID       Enable girgle-root I/O virtualization (SR-IOV)         Internal network       Private network         VEN ID       Enable girdle of all network communications through this network adapter. This setting does not affect virtual machine networking.         Z       Remove	Virtual Switch Manager for SERVER171	
SR-IOV can only be configured when the virtual switch is created. An external	<ul> <li>Virtual Switches</li> <li>New virtual network switch</li> <li>Second NetXtreme Gigabit Ether</li> <li>Second NetXtreme Gigabit Ether</li> <li>NUC Tearning Microsoft Network Adapter M</li> <li>Global Network Settings</li> <li>MAC Address Range 00-15-5D-46-AB-00 to 00-15-5D-4</li> </ul>	Virtual Switch Properties   Name:   NIC Teaming   Notes:   Connection type   What do you want to connect this virtual switch to?    External network: Microsoft Network Adapter Multiplexor Driver Allow management operating system to share this network adapter Enable gingle-root I/O virtualization (SR-IOV) Internal network Private network VLAN ID Enable yirtual LAN identification for management operating system The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking. 2 SR-IOV can only be configured when the virtual switch is created. An external

5. Edit the VM network interface. Change the Virtual Switch to NIC Teaming.

OmniVista-VPN-4.8.1	▼
<ul> <li>★ Hardware</li> <li>M Add Hardware</li> <li>BIOS Boot from CD</li> <li>■ Memory 1024 MB</li> <li>■ Processor 4 Virtual processors</li> <li>■ IDE Controller 0</li> <li>■ Hard Drive ovnmse-vpn-4.8.1.2-disk0</li> <li>■ IDE Controller 1</li> <li>DVD Drive None</li> <li>SCSI Controller 1</li> <li>DVD Drive None</li> <li>SCSI Controller 1</li> <li>Network Adapter vswitch4</li> <li>■ U Eth0 NIC Teaming</li> </ul>	Network Adapter Specify the configuration of the network adapter or remove the network adapter. Virtual switch: NIC Teaming VLAN ID VLAN ID Enable virtual LAN identification The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter. 70 Bandwidth Management Enable bandwidth management Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second. Minimum bandwidth: Maximum bandwidth: 0 Mbps
<ul> <li>Eth1 vswitch4</li> <li>Eth2 vswitch4</li> <li>COM 1 \\.\pipe\</li> <li>COM 2 None</li> <li>Diskette Drive None</li> <li>Management</li> <li>Name OmriVista-VPN-4.8.1</li> </ul>	<ul> <li>To leave the minimum or maximum unrestricted, specify 0 as the value.</li> <li>To remove the network adapter from this virtual machine, click Remove.</li> <li>Remove</li> <li>Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.</li> </ul>

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	
LACP	LACP	Address Hash	None	Yes	

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

## **Configuring the VPN Virtual Appliance**

**Note:** Keep the default settings in the OVF for Guest OS, VM Compatibility and NIC type (E1000), as shown below:

		2 6 6 6	
Linx Dever 0.7 5:05.0-2003.1.etheck.a00.j04 on an a00.j04 Exact Alexandriatest Distription Daniblists 2000 UPB UB Unstant 2. Maderi 2. Dite: INCO-00-11 to the unb conside with: masteril cambleau cachyd	Guest OS	CentOS 4/5/6/7 (64-bit)	
nta legin: almin (antematic legin) agin: Hel Pay In H7-46:54 on tigi UNIQUE constraint failed: ve.setting.mme	VMware Tools	No	
ists arol Reghoord Lagont: us yaw like to configure waw Reghourd Lagont (gin) GD: _	CPUs	4	
	Memory	2 GB	
dit settings - VPN VA 4.1 9 USB controller 1	C 8.1 Build 2 (ESXi 5.5 virtual machine) USB 2.0		
			×
ä, Network Adapter 1	internal	·	×
Status	Connect at power on		
Adapter Type	E1000	~	
MAC Address	Automatic		
ä, Network Adapter 2	internal	~	×
Status	Connect at power on		
Adapter Type	E1000	~	
MAC Address	Automatic ~ 00:0c:29:e3:92:b2		
ä, Network Adapter 3	internal	~	×
Status	Connect at power on		
	E1000	~	
Adapter Type			
Adapter Type MAC Address	Automatic Y 00:0c:29:e3:92:bc		

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

- 1. <u>Complete the Installation</u>
- 2. Configure NICs
- 3. Configure Routes
- 4. <u>Configure Network Settings</u> (DNS, Gateway)
- 5. <u>Configure an SSH Service</u>
- 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

Oracle Linux Server 8.7 Kernel 5.15.0-3.60.5.1.el8uek.x86\_64 on an x86\_64 Product Name: Alcatel-Lucent Enterprise OmmiVista 2500 UPN VA Release Version: 4.8.1 Build Number: 1 Build Date: 2023-08-02 Activate the web console with: systemctl enable --now cockpit.socket ommivista login: admin (automatic login) Last login: Wed Aug 9 13:52:51 on tty1 Configured Keyboard Layout: us Would you like to configure new Keyboard Layout [y1n] (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.

#### ProActi∨e 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 th 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**.



**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**.



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

## **Configure NICs**

Main Menu	
< Network Interfaces	>
< Network Routes	>
< Network Services	>
< Network Settings	>
< UPN Endpoints	>
< UA 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: ethZ
Ir: Profix longth:
Please select NIC to modifu:
< OK >
< Exit >
< EXIL >

**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.

Main Menu	
< Network Interfaces	>
< Network Routes	>
< Network Services	>
< Network Settings	>
< VPN Endpoints	>
< VA Settings	>
< Maintenance	>
< Apply Configuration Changes	>
< Logout	$\rightarrow$

**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.

Main Menu	
< Network Interfaces	>
< Network Routes	>
< Network Services	$\rightarrow$
< Network Settings	>
< VPN Endpoints	>
< VA Settings	>
< Maintenance	>
< Apply Configuration Changes	>
< Logout	>

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.

Main Menu	
< Network Interfaces	$\rightarrow$
< Network Routes	<
< Network Services	>
< Network Settings	>
< VPN Endpoints	>
< VA Settings	>
< Maintenance	>
< Apply Configuration Changes	>
< Logout	>
	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.



### 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.

Main Menu	
< Network Interfaces	>
< Network Routes	>
< Network Services	$\rightarrow$
< Network Settings	>
< VPN Endpoints	$\rightarrow$
< VA Settings	>
< Maintenance	>
< Apply Configuration Changes	>
< Logout	>

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.

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	>
< Opn_	>
< 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	
K 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**.



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

The	conf iguration	has	been	saved	successfully!
< 01	K				>

**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 SFTP 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.

**Note:** If you add an AP to the Device Catalog in your OmniVista Freemium account after exporting the VPN Settings file, you will have to redo the export, SFTP, and reconfigure the VPN VA.

**1.** Go to the Device Catalog Screen (Network – Device Catalog) of your OmniVista Freemium account.

Alcatel·Lucent				🖶 Home 🔒 fre	esqa 🔳 🌲 Su	ipport Center 🛛 🗖 Vi	deos 🚯 About 🕞 Logout
Enterprise			NETWORK - CONFIGURATION -	UNIFIED ACCESS - SECUR	ITY - ADMINISTRATION -		Learn More
INVENTORY	*	Home > Network >	Inventory > Device Catalog				
Device Catalog		Device Catalog	Latest Refresh: 0	1 min ago 😂 🛛 Export VPI	N Settings Manage D	evice Licenses Crea	ate Site Import 🕂 ?
Device Troubleshooting							
Managed Inventory	<b></b>	Q Search all	Advanced Fil	ter			
, in the second s		Set Software Version	Assign License Release License	Troubleshoot Device View	Activation Log 🛛 🕜 🗍 💼		<b>4</b> B
		Serial Number	Model	Current Software Vers	Desired Software Vers	Ready For Upg Dev	vice Status
		SSZ182000166	OAW-AP1201H	4.0.0.19	Do not upgrade	Yes	gistered)
						_	
		4	_				•
		Show 1000 -				Showing Page	1 of 1 《 < 1 > »

**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.

Select A VPN Setting To Export	
LAB4 Server's Public IP: 172.16.92.199; Port: 9001; Server's VPN IP: 12.12.12.1; OmniVista Enterprise Server IP: 12	92.168.70.143; Client VPN IP Address Pool: IP Range
Total: 1 page	« < <b>1</b> > »
	Export Cancel

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

```
[Peer]
PublicKey = w7dRCdRmrC7axxxxx967Yw3iann3sgT+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.

5ftp://admin@10.2	255.222.97:2222 -	FileZilla									x
File Edit View T	ransfer Server	Bookmar	ks Help								
1 - 7:00	🖵 🛱 🕷 I	з 💺 🛷	🗈 🕺 🌮 🛝								
Host: ftp://10.255.2	22.97 Usernam	admin	Password	•	•••••	Port:	2222	Quickcon	nnect 🔻		
Status: loca	l:D:\Users\jobrew	st\Desktop	\LAB4.conf => remote;	/opt/0	OmniVista_2500_I	NMS/da	ita/vpn_c	onf/vpn_prof	ile/LAB4.con	F	•
Status: File	transfer successfu	l, transferr	ed 441 bytes in 1 second	  C/_l_+							
Status: Listi	na directory /opt	OmniVista	2500 NMS/data/vpn c	onf/v	pn profile	_prome					
Status: Dire	ctory listing of "/o	pt/OmniV	ista_2500_NMS/data/vp	n_cor	f/vpn_profile" su	iccessfu	il				
Status: Disc	onnected from se	rver									-
Local site: D:\Users\	jobrewst\Deskto	>\		•	Remote site:	/opt/Or	nniVista_	2500_NMS/da	ata/vpn_conf/	/vpn_profile	•
· · · · · · · · · · · · · · · · · · ·	E Desktop				i i i i i i i i i i i i i i i i i i i	OmniVi	sta_2500_	NMS			
	Documents					? bin					
	🐌 Downloads				<b></b>	📗 data	1				
	🛯 🙀 Favorites					👔 I	ost+foun	d			
	🕛 InstallAnywh	ere				ė 🌗 🖞	/pn_conf				
	john.brewste	r@alcatel-l	lucent.com Creative Clo	uc 🕋			📙 vpn_p	rofile			
				•		? logs					*
Filename	Filesize	Filetype	Last modified	^	Filename				Filesiz	e Filetype	L
\mu					J 🛺						
📔 APIs		File folder	7/10/2019 10:59	):0	LAB4.conf				44:	L CONF File	3,
📔 CLI 8x and 6x		File folder	2/26/2019 3:32:	13							
🔒 OmniVista		File folder	11/8/2019 3:33:	58 🔻							
•	111			Þ.	•		III				
Selected 1 file. Total s	ize: 441 bytes				1 file. Total size	: 441 by	tes				
Server/Local file	Dire	ction Rer	mote file		Size	Priority	Statu	s			
Queued files	Failed transfers	Successf	ul transfers (1)								
								800	Queue: empt	y 🏼 🖷	•

**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.

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**.



**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	>
< UPN Endpoints	>
< VA Settings	>
< Maintenance	>
K 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.



## **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 Re	gistration ->	Data \	/PN Serv	<b>ver</b> to a	add a	Data	VPN S	Server.
------	-----------------	---------	---------------	--------	----------	-----------------	-------	------	-------	---------

dit VPN Server				
Name	VPN_Server_Conf			
Description				
Server's Public IP	195.128.146.179/24	Server's	6550	× ^
Server's Public IP	195.128.146.179/24	Server's Port	6550	× ^

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.

W Home > Network > AP Registration > AP Group								
AP Group							Zigbee Discovery 🕇 🕼 🕅 🖩 🗐 🗘 🤅	
AP Group List	Q T Reset 🛓	Export to .csv Add to R	teport 🕒 Print 🖍				Hide Details >	
RW			۲		General			
Group Name	Auto-Group VLANs	Group Description	Managed AP Count			Crown Name	DW	
RW			1 AP			Group Description	NT	

3. Assign the Data VPN Server to the AP Group (mandatory to set up the Data VPN Tunnel).

■ Registration					
1. Edit Group	Edit Group				
2. Review					
	Edit Group				
	General		~		
	Time		~		
	Syslog		~		
	Post Mortem Dump				
	SSH				
	AP WEB				
	Client Behavior Tracking		~		
	Certificate		~		
	SNMP Setting		~		
	IoT Radio Configuration		~		
	IoT/Location Server	Q Search +	~		
	Data VPN Setting	VPN_Server_Conf			
	Data VPN Server(s)	VPN_Server_Conf			

4. Go to the Data VPN Servers Screen and click on the Export VPN Settings button.

ion 🔹 Data VPN Servers	
	ion > Data VPN Servers

**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/9S2HaxxxxyfJYAIbOHSRDo78r+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 <u>Upload the VPN Settings to the VPN Server</u>.

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

7. Configure the VPN service for Data Tunnel.

Menu for VPN	
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	
< <u>Save</u> < 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	1
< Network Interfaces	5
< Network Routes	>
< Network Services	>
< Network Settings	>
< UPN Endpoints	>
< VA Settings	>
< Maintenance	2
< Apply Configuration Changes	2
< Logout	

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.

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.



### 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.

<pre>&gt; Select WLAN &gt; SSIDs &gt; SSIDs &gt; Click on the + button &gt; SSID Service Name: EmployeesX (X = R-Lab number) &gt; SSID: <filled automatically=""> &gt; Usage: Enterprise Network for Employees (802.1X) &gt; Click on Create &amp; Customize</filled></pre>
<pre>&gt; Allowed Band: All &gt; Encryption Type: WPA3_AES</pre>
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
<pre>// Employee account creation // &gt; Click on the + button &gt; Username: Employee &gt; Password: password &gt; Click on Create &gt; Click on Close</pre>

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

SSID Service Name	Employees0 T	
SSID	Employees0	
p- AP Group(s)	1 selected AP Group(s) Change Selection	1
✓ Set same sche	dule for all selected AP Groups   Edit Schedule 🗗 🛈	
Q Search all		
default group	(	i)

**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.

Default VLAN/Network				
Oconfigure Access Role Attributes	O Choose E	xisting Access Role Profile		
VLAN(s)		202 🛛		+
✓ Use Tunnel				
Config Tunnel				
*Tunnel ID		0		
*GRE Tunnel Server IP Address/D Server	ata VPN	RAP-OVC (10.1.250.1)		
Support of Entropy	DISA	ABLED	Allow Local Breakout	DISABLED

## 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.

Default VLAN/Network						
Configure Access Role Attributes	O Choose E	xisting Access Role I	Profile			
VLAN(s)		Untagged VLAN	N 8		+	•
✓ Use Tunnel						
Config Tunnel						
*Tunnel ID		0			~ ~	
*GRE Tunnel Server IP Address/ Server	Data VPN	RAP-OVC (10.1.2)	50.1)			
Support of Entropy	DIS/	ABLED	Allow Local	Breakout	DISABLED	

## 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.

onfigure Access Role Attributes O Choose	e Existing Access Role Profile			
VLAN(s)	202 😂			+
✓ Use Tunnel				
Config Tunnel				
*Tunnel ID	0		~ ^	
*GRE Tunnel Server IP Address/Data VPN Server	RAP-OVC (10.1.250.1)			
Support of Entropy	DISABLED	Allow Local Breakout	ENABLED	)
i *Static Routes	Input Destination	Input Netmask	Input Gateway	+
	10.0.0	255 255 255 0	192 168 70 5	×

- 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 <u>Basic Troubleshooting</u> <u>Checklist</u>.

## Creating a Tunnel Profile for 1201H Downlink Ports

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

	LAN+WLAN	menu 🖌 🧹 🏕 Home 🔒	admin 🔳 🦺	? Help 📑 Videos	🚯 About 🕞 Logout
Enterprise	NETWORK - CONFIG	SURATION - UNIFIED ACCESS -	SECURITY - ADMINIST	TRATION - UPAM -	WLAN -
< TEMPLATE 🖈	Home > Unified Access > Unified	Profile > Template > Tur	nnel Profile		
Access Auth Profile	Tunnel Profile				?
WLAN Service (Expert)	Create Tunnel Profile				
Access Role Profile					(") indicates a required field
AAA Server Profile	*Name	Downlink Port			
Access Policies	(i) *Tunnel ID	)		~ ^	
Access Classification	*GRE Tunnel Server IP Address/Data VPN Server	RAP OVC (10.1.250.1)			
Customer Domain	Support of Entropy	DISABLED	Allow Local Breakout	DISABLED	
SPB Profile					
Far End IP					Create Cancel
Static Service					
VXLAN Profile					
Tunnel Profile					
Legacy Wireless > Profiles					
Global Configuration >					
			Unackr	nowledged Alarms: 999	9 <b>*</b> 0 <b>0</b> 999+

**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".

# Home > Unified Access > Unified Profile > T	emplate > Access Role Profile		
Access Role Profile			3
■ Access Role Profile Assignment			
1. Select Devices	Select Devices Select the mapping method for access role	profile(s) and devices to apply the configura	ation
2. Configure the period policy			
3. Configure the location policy	Configure the mapping method for	ARP-Downlink	
4. Review	Mapping Method	Map to VLAN and Tunnel	•
	VLAN(5)	Untagged VLAN O	+
	Tunnel Profile	Select	•
	() Select devices to apply the confi	guration	
	0 Devices ADD - 1 AP Group	EDIT	
	List of Selected AP Groups		
	Q Search all		
	Name		
	AP1201HL		

**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.

Access Auth Profile A	PClassification6x			
vices				
0 Devices ADD -	1 AP Group EDIT			
List of Selected AP Gro	ups	_		
<b>Q</b> Search all				
Name				
GTTS				
Eth1 Eth2 Eth3				
•	III			4
Show 1000 -		Showin	g Page 1 of 1	$\langle 1 \rangle \gg$

### 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.

***************************************	<del>i n n</del>
* Configure The Virtual Appliance	×
***************************************	HHH
* L1] Help	÷H
* [2] Display Current Configuration	H
* [3] Configure IPs and Ports	H
* [4] Configure Default Gateway	H
× [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	×
***************************************	<del>i x x</del>
(*) Type your option: _	

#### 2. Select 8 – Configure Route.



**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).



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



# 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.

1. Deploy a new VPN VA 4.8.1.2

**2.** Select the port group for 3 Network Adapters same as the old VPN VA but all the statuses are disconnected.

Add hard disk Add network adapter Add other device     CPU 4     2 GB     2 GB     Amemory 2     2 GB     Amemory 2     Amemory 2     2 GB     Amemory 2     Amemory 3     Amemory 2     Amemory 3        Amemory 3          <	Virtual Hardware VM Options					
> CPU 4   2 GB   > Memory 2   > Hard disk 1 8   6B Note that Hard Disk 1 Default = 8GB   > Hard disk 2 1   • USB controller 1 USB 2.0   USB 2.0 ·   > 'a, Network Adapter 1 Net71x   Net71x ·   Connect   > 'a, Network Adapter 2 VMM Network for VMM Application   > 'a, Network Adapter 3 Net10x	🖨 Add hard disk 🛛 🚊 Add networ	k adapter	📰 Add	other de	evice	
Memory 2 GB     Hard disk 1     Hard disk 2     I     GB     Hard disk 2     USB controller 1   USB 2.0      Sig, Network Adapter 1     Net71x     NetWork Adapter 2        VMM Network for VMM Application     Specify custom settings	CPU	4 ~ (	0			
> Hard disk 1 8   > Hard disk 2 1   • USB controller 1 USB 2.0   USB 2.0 ·   > 'a, Network Adapter 1 Net71x   > Net71x ·   Connect   > 'a, Network Adapter 2   VMM Network for VMM Application   > 'a, Network Adapter 3   Net10x   Specify custom settings	>  Memory	2	GB	~		
> Hard disk 2 1   • USB controller 1 USB 2.0   > 'ā, Network Adapter 1 Net71x   > 'ā, Network Adapter 2 VMM Network for VMM Application   > 'ā, Network Adapter 3 Net10x	> 📇 Hard disk 1	8	GB	~	Note that Hard Disk 1 Default = 8GB	×
<ul> <li>USB controller 1</li> <li>USB 2.0</li> <li>So, Network Adapter 1</li> <li>Net71x</li> <li>Connect</li> <li>Network Adapter 2</li> <li>VMM Network for VMM Application</li> <li>Connect</li> <li>Net10x</li> <li>Connect</li> </ul>	> 🕞 Hard disk 2	1	GB	~		×
> 'ā, Network Adapter 1     Net71x          Connect         Connect        > 'ā, Network Adapter 2     VMM Network for VMM Application         Connect         Connect         Specify custom settings	⊷ USB controller 1	USB 2.0			~	
> 'b, Network Adapter 1     Net71x     ~ □ Connect       > 'b, Network Adapter 2     VMM Network for VMM Application     ~ □ Connect       > 'b, Network Adapter 3     Net10x     ~ □ Connect						×
> Tig, Network Adapter 2     VMM Network for VMM Application <ul> <li>Connect</li> <li>Net10x</li> <li>Connect</li> </ul> Specify custom settings <ul> <li>Image: Specify custom settings</li> <li>Image: Specify custom settings</li></ul>	😋 Network Adapter 1	Net71x			∽ □ Connect	×
Specify custom settings	> 🔄 Network Adapter 2	VMM Netwo	ork for VMM	Applica	tion ~ Connect	×
Specify custom settings	> 🛱 Network Adapter 3	Net10x			✓ □ Connect	×
Video Card	> 🖵 Video Card	Specify cust	tom settings		~	

- 3. Configure all options on VPN VA, except the option VPN Endpoints
  - a. Configure NICs
  - b. Configure Routes
  - c. Configure Network Settings (DNS, Gateway)
  - d. Configure an SSH Service
  - e. Configure the VPN Service
- 4. Shutdown the old VPN VA 4.5.3 Build 1.
- 5. Change the status of 3 Network Adapters to connected.

Virtual Hardware VM Options						
🖨 Add hard disk 🛛 🚊 Add netw	ork adapter	📰 Add d	other device			
CPU	4 ~	0				
E Memory	2	GB	~			
Hard disk 1	8	GB	~			×
Hard disk 2	1	GB	~			×
⊷ USB controller 1	USB 2.0			~		
						×
🛱 Network Adapter 1	Net71x			~	Connect	×
🔄 Network Adapter 2	VMM Netwo	ork for VMM	Application	~	Connect	×
🖻 Network Adapter 3	Net10x			~	Connect	×
🖵 Video Card	Specify cust	om settings		~		

**6.** Import Backup VPN profile to the new VPN VA 4.8.1 Build 2 in the directory /opt/OmniVista\_2500\_NMS/data/vpn\_conf/vpn\_profile.

7. Configure option VPN endpoints the same as the configuration of the old VPN VA.

Notes:

- The VPN VA upgrade process applies to VMware and Hyper-V.
- The old VPN VA 4.5.3 Build 1 continues to run until step 4.
- The RAP will be disconnected with the VPN VA from Step 4 to Step 7. The AP downtime happens in a short time (~5 minutes).
- The default Hard Disk size is 8GB for RAP VPN VA 4.8.1.

# **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 8 fe80::8389:64ed:fbd4:e730 RX ТΧ FREQ AUTH Final\_role VLANID TUNNELID FARENDIP 4237 PSK 0 0 5860 5GHz RAP3 **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 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.