

# **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
Add Remote APs	5
Deploying/Configuring the VPN Tunnel Server	8
Recommended VPN VA Configurations	8
Deploying the VPN Virtual Appliance	8
Configuring the VPN Virtual Appliance1	5
Configuring the VPN Data Tunnel	30
Create an SSID for the VPN Data Tunnel	34
Add a Route to Reach the VPN VA from OmniVista	5
Upgrading the VPN VA	6
Basic Troubleshooting Checklist	1
Useful Logs and Commands4	-2

# **Remote Access Points and VPN Tunnel Components**

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

Components of the solution:

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

# VPN for Management and Data (OVE Managed APs)

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

If the RAP is OVE managed:

**1.** The first connection, out-of-the-box, is to the OVC device registration server. It retrieves the setup parameters for RAP including the OVE IP to connect to.

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

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

**4.** Optionally, a Data VPN tunnel can be setup in OVE between the RAP and the VPN server. The tunnel keys and parameters can be exported to the VPN server at corporate HQ.

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

Key points when RAP is managed by OVE:

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

# VPN for Data Only (OVC Managed APs)

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

If RAP is to be managed by OVC.

**1.** The first connection out-of-the-box for the AP is to the OVC device registration server to confirm it is an OVC registered AP.

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

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

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

Key points when RAP is managed by OVC:

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

## **Prerequisites**

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

## **Network Topology**

Within this document we will use the following network topology:



# **Remote Access Points and VPN Tunnel Configuration**

You can configure an offsite, remote AP as a Remote Access Point (RAP) that can be managed by your local OmniVista Enterprise installation through a VPN Tunnel. Remote APs are added to the Device Catalog using a "Freemium version of OmniVista Cirrus, the cloud-based version of OmniVista. You then must install a VPN Tunnel Server Virtual Appliance (VPN VA) (see the *OmniVista Enterprise 4.5R1 Installation and Upgrade Guide* for installation instructions).

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

- 1. Creating an OmniVista Cirrus Freemium Account
- 2. Adding APs to the Device Catalog
- 3. Deploying/Configuring the VPN Tunnel Server

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

Note: Only untagged traffic can currently be tunneled through VPN tunnels.

## **Creating an OmniVista Cirrus Freemium Account**

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

1. Go to the OV Registration Portal.

🥝 OmniVista Cinus 🛛 🗙 🛨		-	•	×
← → C ① @ https://registration.o	vcirrus.com/	04	9	÷
	Alcatel-Lucent 🕖			
	Enterprise			
	OmniVista Cirrus			
	& Username			
	A Password			
	+8) Sign in			
	or			
	Create New Account			
	Need help setting started			
	Eerool.voor.eassacord?			
	© Copyright Alcatel-Lucent Enterprise USA, Inc., 1997			
Best viewed on Internet Fire	© Copyright ALE USA Inc., 2014, 2018 Invert 11a Chrome 68a Eirefry 62a. The minimum recommended resolution	in 1280v768		

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.

Alcatel-Luc Enterprise	ent 🕖
	OmniVista Cirrus
O Your accou	int was created successfully!
Check your ema	I - we have sent you a verification email with the next step

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

**Important Note:** There is a link in the body of the email to download the required device OS software for OmniVista Cirrus. APs must be running a minimum software version of AWOS 4.0.0.40. Click on the link to download the software. If necessary, you can use this software to upgrade your devices.

**5.** Create and confirm your password, then click on the **Save** button. The Confirmation Screen below will appear.



**6.** Click on the **Continue to Login Page** link and log into OmniVista Cirrus using the username and password you created. After successful login, the OmniVista Cirrus Freemium Dashboard will appear.



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

## Add Remote APs

Remote APs are added using the Device Catalog application.

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

🖷 Home 🔺 freesqa 📰 🌲 Support Center 📾 Videos 💽 About 🔅 Lopout
NETWORK - CONSIGURATION - UNLITED ACCESS - SECURITY - ADMINISTRATION -
Home > Network > Inventory > Device Catalog
Device Catalog Latest Refresh: 20 mins ago 😂 Export VPN Settings Municipe Device Licenses Create Site Import + 🤉
Q. Search all Advanced filter
Set Software Version 🛛 Assign License 🗍 Troubleshoot Device 🛛 Year Activation Log 🖉 😫 📥 🖨
Serial Number Model Current Software Vers. Desired Software Vers. Device Status Device Category
Show 1000 • Showing Page 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			
"Serial Number	ex: \$\$217000000		(7) indicates a required field
Desired Software Version	Do not Upgrade	•	
			Create Cancel

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

Remote Access Point and VPN VA Installation GL	uide
--	------

*Serial Number	SSZ182000166	
'MAC Address	Enter MAC Address	
Is this a Remote AP ?	YES	
VPN Settings		
Create New VPN Setti	O Choose Existing VPN Settings	
"VPN Settings Name	Enter maximum 32 characters	
*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	
*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 User-configured name for the VPN configuration.
  - Server's Public IP The VPN Server's Public IP address (configured on one of the interfaces when you installed the VPN VA). This is the IP address used by Remote APs to connect to the VPN Server. And this is the interface through which traffic originating from inside the Enterprise Network flows to the Remote site.
  - **Port** The VPN Public IP Server Port.
  - Server's VPN IP The VPN Server's Private IP address within the virtual network (must be in the same network as the client pool). This is the tunnel interface through which traffic originating from the Remote AP flows to reach a destination inside the Enterprise Network.

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

# Deploying/Configuring the VPN Tunnel Server

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

- VPN VA Configuration (Based on the number of Remote APs)
  - 1 100 APs 4 vCPUs, 2GB RAM
  - 100 250 APs 6 vCPUs, 4GB RAM

**Note**: Higher scale is based on CPU/Memory calculated per RAP unit. For deployments greater than 64 RAPs it's suggested to contact ALE TSS/Support for recommendations on planning and rollout.

- NICs 1G vs.10G (Based on expected throughput)
  - 10 20Mbps expected VPN throughput per RAP, if local breakout is serving all internet needs.
  - 20 100Mpbs expected VPN throughput per RAP, if all traffic is tunneled through VPN.

## **Deploying the VPN Virtual Appliance**

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

**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" ESXi"		root@10.255	5.222.88 -   Help -   🝳 Search	•
Navigator	ovvmhost3			
<ul> <li>Host</li> <li>Manage</li> <li>Monitor</li> <li>Virtual Machines</li> <li>Storage</li> <li>Storage</li> <li>Networking</li> <li>Storage</li> </ul>	Manage with vCenter Server  Vorsion: 6.5.0 (B State: Normal Uptime: 116.86	Create/Register VM   Bo Shut down uild 4887370) (connected to vCenter Server at 10.255.22 days	n Reboot CPU FREE: 22.6 GHz CPU FREE: 22.6 GHz USED: 35 MHz CAPACITY: 22.7 GHz MEMORY FREE: 18.36 GB USED: 1.64 GB CAPACITY: 20 GB STORAGE FREE: 401.55 GB USED: 974 MB CAPACITY: 402.6 GB	E
	▼ Hardware			
	Manufacturer	HP		
	Model	ProLiant DL380 G5		
	CPU	8 CPUs x Intel(R) Xeon(R) CPU E544	40 @ 2.83GHz	
	Memory	20 GB		
	🕨 🏣 Virtual flash	0 B used, 0 B capacity		-
	Recent tasks			
	Task ~ Target	✓ Initiator ✓ Queued ✓ Sta	arted V Result V Complet	e ~
	Destroy 🔂 OV 4.5R2 B	Buil root 07/13/2020 1 07/1	13/2020 1 Or/13/202	0 1
	Destroy 👘 VPN VA Bui	ild root 07/13/2020 1 07/	13/2020 1 Ompleted successfully 07/13/202	0 1
	Download VMXConfig None	VC Internal 07/13/2020 1 07/1	13/2020 1 Or Completed successfully 07/13/202	0 1
	Power Off VM	uil root 07/13/2020 1 07/1	13/2020 1 Completed successfully 07/13/202	0 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?	
5 Deployment options 6 Additional settings 7 Decidu to complete	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file	virtual machine from an OVF and VMDK files.
r reay to complete	Register an existing virtual machine	
<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 - VPN VA Build	21
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> </ul>	Select OVF and VMDK files
3 Select storage 4 License agreements 5 Deployment options	Enter a name for the virtual machine.
6 Additional settings 7 Ready to complete	MPN VA Build 21 Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
<b>vm</b> ware <sup>*</sup>	<ul> <li> <ul> <li>                 ovnmse-vpn-4.5.1.21.ovf                 </li> <li>                 ovnmse-vpn-4.5.1.21-disk002.vmdk</li></ul></li></ul>
	Back Next Finish Cancel

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

	Select storage						
2 Select OVF and VMDK files	Select the datastore in which to store the cor	nfiguration and d	lisk files.				
3 Select storage     4 License agreements     5 Deployment options     6 Additional settings	The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.						
6 Additional settings 7 Ready to complete	Name ~	Capacity ~	Free ~	Type ~	Thin pro ~	Access >	/
	datastore1 (1)	402.5 GB	401.55 GB	VMFS5	Supported	Single	-
	ov-qnap-datastore-001	7.16 TB	2.96 TB	NFS	Supported	Single	
<b>vm</b> ware <sup>*</sup>							

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

🔁 New virtual machine - VPN VA Build	21	
<ul> <li>✓ 1 Select creation type</li> <li>✓ 2 Select OVF and VMDK files</li> <li>✓ 3 Select storage</li> </ul>	License agreements Read and accept the license agreements	ì
<ul> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Ready to complete</li> </ul>	License agreement	
	Terms and Conditions Acceptance: Read the following End User License Agreement (EULA) carefully before in 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 i "Order of Precedence": If You received more than one license terms purporting to govern the use of the Ma	
	Parties: This agreement is between (a) the legal entity which has a separate purchase agreement with a Pa 1. License Grant: Subject to all other terms in the agreement, and subject to the payment of the applicab	
	Additional or different terms and conditions to modify, copy, or distribute the Material may be granted t All licenses granted hereunder are contingent upon full payment of fees, if any, specified in the separat	
	<ol> <li>License restrictions: Unless authorized by the applicable law with no possibility to contractually sup</li> <li>Third Party software: Licensee acknowledges that third party software, including without limitation "F -</li> </ol>	
VIIIWare	Back Next Finish Cancel	Ŧ

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

🔁 New virtual machine - VPN VA Build 21					
<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     VM Network       Null     VM Network			
	Disk provisioning	● Thin <sup>®</sup> Thick			
<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**.

🔁 New virtual machine - VPN VA Build	21			
<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 finishing the wizard			
<ul> <li>4 License agreements</li> <li>5 Deployment options</li> </ul>	Product	OmniVista VPN Server		
✓ 6 Ready to complete	VM Name	VPN VA Build 21		
	Disks	ovnmse-vpn-4.5.1.21-disk001.vmdk,ovnmse-vpn-4.5.1.21-disk002.vmdk		
	Datastore	ov-qnap-datastore-001		
	Provisioning type	Thin		
	Network mappings	Network Interface 1: VM Network, Null: VM Network		
	Guest OS Name	RedHat_64		
	Do not refresh your brow	ser while this VM is being deployed.		
<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.

<b>vm</b> ware <sup>®</sup> ESXi <sup>®</sup>		root@10.255.	222.88 🗸   Help 🗸   🝳 Search 🚽
Navigator	ovvmhost3		
E Host     Manage     Monitor      Grivirual Machines     1      Government     Storage     Qovernment     Storage     3	Manage with vCenter Server  vovmhost3 Version: 6.5.0 (E State: Normal Uptime: 116.86	Create/Register VM   Do Shut down huld 4887370) (connected to vCenter Server at 10.255.22 days	Reboot       CRefresh       Actions         CPU       FREE: 22.8 GHz       0%         USED: 35 MHz       CAPACITY: 22.7 GHz         MEMORY       FREE: 18.96 GB         USED: 1.64 GB       CAPACITY: 20 GB         STORAGE       FREE: 401.55 GB         USED: 974 MB       CAPACITY: 402.5 GB
	- Hardware		
	Manufacturer	HP	
	Model	ProLiant DL380 G5	
	F 🖬 CPU	8 CPUs x Intel(R) Xeon(R) CPU E5440	) @ 2.83GHz
	Memory	20 GB	
	🕨 🔚 Virtual flash	0 B used, 0 B capacity	-
	Recent tasks		
	Task v Target	✓ Initiator ✓ Queued ✓ Starte	ed 🗸 Result 🗸 Complete 🗸
	Import VApp Resources	root 07/13/2020 1 07/13/	(2020 1 🛛 🚫 Running 3 %
	Upload disk - ovnmse-vpn 👔 VPN VA Bui	Id root 07/13/2020 1 07/13/2	/2020 1 Nunning 6 %
	Upload disk - ovnmse-vpn 🚰 VPN VA Bui	Id root 07/13/2020 1 07/13/	(2020 1 📀 Completed successfu 07/13/2020 1
	Reconfig VM 👘 VPN VA Bui	Id VC Internal 07/13/2020 1 07/13/	2020 1 ] Failed - The operatio 07/13/2020 1
	Download VMXConfig None	VC Internal 07/13/2020 1 07/13/	2020 1 Completed successfu 07/13/2020 1
	Destroy OV 4.5R2 B	ui   root   07/13/2020 1   07/13/	2020 1 Completed successfu 07/13/2020 1

**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.** 

<b>vm</b> ware" Esxi"			root@10.255.222.88 👻	Help 🗸   🝳 Search 🔷
Pee Navigator	🗗 VPN VA Build 21			
▼ 📱 Host Manage	Console 🛃 Monitor	Power on Power of VPN VA Build 21	off 🔢 Suspend 🧐 Reset   🥒 B	Edit   C Refresh   🏟 Actions
Monitor	have ( $1.420\pm0.10$ have adds, but not only of the set	Guest OS Compatibility	CentOS 4/5 or later (64-bit) ESXi 5.5 and later (VM version 10)	O MHZ
🝷 🗗 VPN VA Build 21		VM ware Tools	No	MEMORY
Monitor More VMs		Memory	* 1 GB	STORAGE 1.97 GB
E Storage		G		
> 🧕 Networking 🛛 🔹 3	▼ General Information			
	Metworking	No network info	rmation	
	▶ 🕋 VMware Tools	Not installed		🔅 Actions
	▶ 🗐 Storage	2 disks		
	Division Notes	Alcatel-Lucent E	Enterprise OmniVista VPN Server	🥒 Edit notes
	✓ Performance summary la	ast hour		
	😨 Recent tasks 🔹			
	Task v Target	t 🗸 Initiator 🗸	Queued ~ Started ~ Res	ult v Complete v
	Upload disk - ovnmse-vpn 🖆 VP	N VA Build root	07/13/2020 1 07/13/2020 1 🔮 0	Completed successfully 07/13/2020 1 🔺
	Upload disk - ovnmse-vpn 👘 VP	N VA Build root	07/13/2020 1 07/13/2020 1 🔮 0	Completed successfully 07/13/2020 1
	Download VMXConfig None	VC Internal	07/13/2020 1 07/13/2020 1 🔮 0	Completed successfully 07/13/2020 1
	Update Child Resource C Resource	ces VC Internal	07/13/2020 1 07/13/2020 1 🔮 0	Completed successfully 07/13/2020 1
	Download VMXConfig None	VC Internal	07/13/2020 1 07/13/2020 1 🔮 0	Completed successfully 07/13/2020 1
	Power On VM		0//13/2020 1 0//13/2020 1 💟 0	compreted successfully 07/13/2020 1

#### **Important Notes:**

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

Security	Network label	Network71.x		
Traffic shaping	VLAN ID	None (0)	•	
Teaming and failover				

- CANCEL OK
- On the ESXi VM, enable Promiscuous Mode for the above NIC. If the "Override" checkbox is enabled, make sure Promiscuous Mode is set to "Accept".

Properties				
Security	Promiscuous mode	Override	Accept	~
Traffic shaping	MAC address changes	Override	Accept	~
Teaming and failover	Forged transmits	Override	Accept	~

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

Zedit standard virtual switch - vSwitch0				
🔜 Add uplink				
MTU	9000			
Uplink 1	vmnic0 - Up, 1000 mbps 🔻 📀			
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			
	Save Cancel			

**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.

## **Configuring the VPN Virtual Appliance**

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

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

## Complete the Installation

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

CentOS Linux 7 (Core) Kernel 4.4.203-1.el7.elrepo.x86\_64 on an x86\_64 omnivista login: admin (automatic login) Configured Keyboard Layout: us Would you like to configure new Keyboard Layout [yɨn] (n):

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

#### Proactive Lifestyle Management Product Exhibit

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

ProActive Lifecycle Management

The ProActive Lifecycle Management (PALM) feature may be chosen during installation, it collects and stores information such as; the make, model and serial number of Licensee's devices, the device sof tware version numbers and system uptime information and such other information that would, in Licens ors sole discretion, be utilized to improve the customer experience. The information helps us to dia gnose potential problems, if any, in the software. We may or may not use the diagnostic information, in our sole discretion, to provide support solutions, including updates, upgrades or services packs, if any are made generally available. We will not use the ProActive Lifecycle Management feature to track, collect or upload any data that personally identifies You (such as your name, address, email address) except Customer information provided to us by You. Licensee may opt-out of providing this data during installation of the Software by, as the case may be, checking or un-checking the box adj acent to the ProActive Lifecycle Management feature option. If the box next to the ProActive Lifecycle Management feature after full installation, You may do so by following t he instructions on the Preference page for ProActive Lifecycle Management in You OmmiVista 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**

۲	lain Menu	
<	(Network Interfaces	>
R	(Network Routes	>
k	(Network Services	>
k	(Network Settings	>
k	( VPN Endpoints	>
k	(VA Settings	>
k	(Maintenance	>
k	( Apply Configuration Changes	>
k	Logout	>

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

Menu for Network Interfaces
1. NIC1:
Name: eth0
IP:
Prefix length: 0
MAC: 00:50:56:af:cb:cd
2. NIC2:
Name: eth1
IP:
Prefix length: 0
MAC: 00:50:56:af:82:28
3. NIC3:
Name: eth2
IF: Due Circ Lewreth
rreitx length:
Please select NIC to modify:
< OK >
< Exit >

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



**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.

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

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

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

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



## **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.

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

**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	>
<pre>&lt; Network Routes </pre>	~
< Network Settings	>
< VPN Endpoints	>
< VA Settings	>
< Maintenance	>
< 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	
< 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 FTP this file to the VPN VA to configure the VPN Service. If you have already exported the VPN Settings to your computer, go to Step 4.

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

Alcatel·Lucent				🖶 Home 🔺 fr	eesqa 🔳 🌲 Su	upport Center	■ Videos	ogout UNT
encerprise			NETWORK CONFIGURATION	UNIFIED ACCESS      SECUR	ADMINISTRATION		Learn More	
INVENTORY	*	Home > Network >	Inventory > Device Catalog					
Device Catalog		Device Catalog	Latest Refresh:	01 min ago 😂 🛛 Export VP	N Settings Manage D	evice Licenses	Create Site Import +	2
Device								
Troubleshooting		Q Search all	Advanced F	ilter				
Managed Inventory	<b>&gt;</b>							_
		Set Software Version	Assign License Release License	Troubleshoot Device View	Activation Log 📝 👔	Ì	📥 🛛 🖨	
		Serial Number	Model	Current Software Vers	Desired Software Vers	Ready For Upg	Device Status	
		SSZ182000166	OAW-AP1201H	4.0.0.19	Do not upgrade	Yes	Registered	(i
		•						+
		Show 1000 -				Showing F	Page 1 of 1 < < 1 > >	
								_

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

Select A VPN Setting To Export	
LAB4 Server's Public IP: 172.16.92.199; Port: 9001; Server's VPN	N IP: 12.12.12.1; OmniVista Enterprise Server IP: 192.168.70.143; Client VPN IP Address Pool: IP Range
Total: 1 page	« < 1 > »
	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.

🔁 sftp://admin@10.255.222.97:2222 - FileZilla										
File Edit View Transfer Server Bookmarks Help										
Host: ftp://10.255.22	2.97 Username:	admin	Password:	•••••	Port:	2222	Quickcon	nnect 🔻		
itatus: local:D:\Users\jobrewst\Desktop\LAB4.conf => remote:/opt/OmniVista_2500_NMS/data/vpn_conf/vpn_profile/LAB4.conf										
Status: File transfer successful, transferred 441 bytes in 1 second Status: Patiening directory listing of "(ant/Omp)/ista 2500 NMS/data/upp, conf/upp, profile"										
Status: Listin	g directory /opt/0	OmniVista_2500_NMS/	data/vpn_conf/	vpn_profile	prome					
Status: Direc	tory listing of "/or	pt/OmniVista_2500_NN	/IS/data/vpn_co	nf/vpn_profile" s	uccessfu	d in the second s				
Status: Disco	onnected from ser	ver								Ψ.
Local site: D:\Users\	obrewst\Desktop	λ	•	Remote site:	/opt/Or	nniVista_	2500_NMS/da	ata/vpn_conf/v	pn_profile	•
±	📰 Desktop				OmniVi	sta_2500_	NMS			
<b>.</b>	Documents				👔 bin					
	🗼 Downloads			] –	📗 data					
	Favorites				<mark>?</mark>	ost+four	d			
	InstallAnywhe iobp browstor	re Øslestel lucent com (	restive Claure T			/pn_conf	rofilo			
•	john.brewsten	waicater-lucent.com c	reative clout		2 logs	p vpn_p	rome			-
Filename	Filesize F	iletype Last	modified ^	Filename	. 1045			Filesize	Filetype	L
	F	ile folder 7/10	/2019 10:59:0	I AB4.conf				441	CONF File	3
CLI 8x and 6x	F	ile folder 2/26	/2019 3:32:13							
🚺 OmniVista	F	ile folder 11/8	/2019 3:33:58 🔻							
•	m		•	•		111				۱.
Selected 1 file. Total si	ze: 441 bytes			1 file. Total size	e: 441 by	tes				
Server/Local file	Direc	tion Remote file		Size	Priority	Statu	IS			
Queued files	ailed transfers	Successful transfers (1	.)							
							🔒 500 (	Queue: empty	۲	•

**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.

_		
M	ain Menu	
<	Network Interfaces	>
<	Network Routes	>
<	Network Services	>
<	Network Settings	>
<	VPN Endpoints	>
<	VA Settings	>
<	Maintenance	>
<	Apply Configuration Changes	>
<	Logout	>

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



## **Configure VPN Endpoints**

Attach the VPN Settings File to the VPN Service.



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



2. Highlight Configure a VPN Endpoint and press Enter.



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



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

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



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



## **Configuring the VPN Data Tunnel**

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

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

dit VDN Server					
uit veivei					
					n
Name	VPN_Server_Conf				
Description					
Description Server's Public IP	195.128.146.179/24	Server's	6550	~ ^	
Description 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.

# Home > Network > A	P Registration > AP Group						
AP Group							Zigbee Discovery 🕇 🕼 🕼 🖩 🖉 🗘 🤅
AP Group List	Q T Reset 🛓	Export to .csv Add to	o Report 🛛 🖨 Print 🛛 🖍				Hide Details >
RW			۲	ļ	General		
Group Name	Auto-Group VLANs	Group Description	Managed AP Count			Group Name	PW
RW			1 AP			Group Description	

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

1. Edit Group	Edit Group Edit Group Description		
2. ICIUI	Edit Group		
	General		~
	Time		ж <sup>а</sup>
	Syslog		~
	Post Mortem Dump		~
	SSH		v
	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.

Home > Network > AP Registrat	on > Data VPN Servers
Data VPN Servers	
Q Search all	
Showing All 1 item	
+ 🕜 👔 Export VPN Settings	

**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>S</u> ave < Exit	$\rightarrow$

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

## **Configure VPN Endpoints**

Attach the VPN Settings File to the VPN Service.

Main Menu	
< Network Interfaces	>
< Network Routes	>
< Network Services	_>
< Network Settings	>
< UPN Endpoints	>
< VA Settings	>
< Maintenance	->
< Apply Configuration Changes	>
< 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.



**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: <b>UPAMRadiusServer</b> > Click on <b>Manage Employee Accounts</b>
<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	•
SSID	Employees0	
AP Group(s)	1 selected AP Group(s) Change Selection	
✓ Set same sched	dule for all selected AP Groups   <u>Edit Sched</u>	<u>dule</u> 🗗 🛈
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.



## Add a Route to Reach the VPN VA from OmniVista

жнэ	нн	***************************************	H-H
ю 1	he	Virtual Appliance Menu	Эн
нн-	ннэ	***************************************	H-H
₩ [	11	Help	э
₩ [	21	Configure The Virtual Appliance	э
<b>₩</b> [	31	Run Watchdog Command	э
<b>₩</b> [	41	Upgrade/Backup/Restore VA	э
<b>₩</b> [	51	Change Password	ж
<b>₩</b> [	61	Logging	э
<b>₩</b> [	71	Login Authentication Server	э
<b>₩</b> [	81	Power Off	э
<b>₩</b> [	91	Reboot	э
<b>₩</b> [	10]	Advanced Mode	э
¥ [	11]	Set Up Optional Tools	э
¥ [	12]	Convert to Cluster	×
* [	13]	Join Cluster	э
×	01	Log Out	ж
жжэ		***************************************	÷
(*)	Tu	pe your option:	

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

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

2. Select 8 – Configure Route.

×	<del>ся к я я</del>	*****	******	***************************************
×	Conf	igure	Route	
÷	<del>(жжжж</del>	*****	******	***************************************
×	[1]	Help		
×	[2]	Show C	urrent	Routes
×	[3]	Add Ro	ute v4	
×	[4]	Del Ro	ute v4	
×	[0]	Exit		
÷	****	*****	******	***************************************
()	e) Ty	pe you	r optio	on: _

**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)

***************************************	XX
* Configure Route	×
***************************************	××
* [1] Help	×
* [2] Show Current Routes	×
* [3] Add Route 🕫	×
* [4] Del Route v4	×
* [0] Exit	×
***************************************	××
(*) Type your option: 3	
(*) Please input subnet: 10.255.255.0	
(*) Please input netmask: 255.255.26	
(*) Please input gateway: 192.168.71.1	
Would you like to add a route:	
subnet: 10.255.255.0	
netmask: 255.255.255.0	
gateway: 192.168.71.1	
[yin] (y):	
The configuration has been set	
Press [Enter] to continue	

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



# Upgrading the VPN VA

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

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

1. Power off the existing VA (RAP-VPN\_b17).

R	RAP-VPN_b17
aCenter1 Alcatel 월 Cluster101	Getting Started Summary Resource Allocation Performance Tas
10.255.214.131     10.255.214.211     10.255.214.211     ResourcePool-1     AP-SIM-3_145     OV_433GA->441GA_160     OV_441_b58_155h1     OV_451_b17_150h1	<ul><li>What is a Virtual Machine?</li><li>A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.</li><li>Because every virtual machine is an isolated computing</li></ul>
<ul> <li>OV_451_b27-31-34-41-44_155h1</li> <li>OV_451_b34_1455</li> <li>OV-140H1-44R2-b50-Ver</li> <li>OVE_451_b21_150h1</li> <li>ALE-SLAB-AD</li> <li>IxChariot 9.6</li> <li>Kali-Linux_CentOS</li> <li>Kali-Linux_Ubuntu-16.4</li> <li>Kali-Linux_Ubuntu-16.4</li> </ul>	environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications. In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.
Kali-Linux-2     Kali-Linux-2     Sebian     Koli-Linux-3_Debian     Ov-185_AT     RAP-VPN_b17     Server165_RAP-net     Concentral	Basic Tasks  Power Off the virtual machine  Suspend the virtual machine
Win7-DonotDelete	Edit virtual machine settings

Deploy a new OVF template using the 4.5.1.20 version files.



😰 Deploy OVF Template						
Ready to Complete						
Are these the options you	want to use?					
Source OVF Template Details End User License Agreement Name and Location Host / Cluster Resource Pool Storage Disk Format Network Mapping Ready to Complete	When you dick Finis Deployment settings OVF file: Download size: Size on disk: Name: Folde: Host/Cluster: Specific Host: Datastore: Disk provisioning: Network Mapping:	sh, the deployment task will be st Y:\SLabi Unknow Waknow RAP-VPP DataCer Cluster1 10.255.2 SL223 Thin Pro "Networ "Null" to	ent task will be started. Y:\SLab\OV\Software\RAP\VPN-VA\b20\ovnmse-vpn-4.5.1 Unknown Unknown RAP-VPN_b20 DataCenter1 Cluster101 10.255.214.211 SL223 Thin Provision "Network Interface 1" to "RAP-HQ_3970" "Null" to "HAN-2000"			
	Power on after d	leployment				
J						
Help			< Back	Finish	Cancel	
Deploying RAP-VPN_b20 Deploying RAP-VPN_b20 Deploying disk 1 of 2 from Y:\SLab\OV\Software\RAP\VPN-VA\b20\ovnmse-vpn-4.5 vmdk	_ 🗆 🗙	Deployment Co Deploying RAP-VPN Completed Success	mpleted Succe I_b20 :fully	essfully		×
Close this dialog when completed	Cancel					Close

2. Copy the OS virtual disk file (RAP-VPN\_b20.vmdk) to the location of current VA (RAP-VPN\_b17). On VMWare web client, click "Datastore browser".

vmware <sup>®</sup> ESXi <sup>®</sup>			
Carl Navigator		■ SL223	
✓ ☐ Host Manage Monitor		💕 Register a VM 🛛 Datastore browser   🗷 Increase capacity   🦿 Refresh   🏠 Actions	
<ul> <li>→ D Virtual Machines</li> <li>→ Storage</li> <li>→ St223</li> <li>Monitor</li> <li>More storage</li> <li>→ A tworking</li> </ul>	12 4	SL223 Type: NFS Location: /vmfs/volumes/9565a630-6ec5d66c Hosts: 1 Virtual Machines: 12	

a. In the Datastore browser, highlight the file (RAP-VPN\_b20.VMDK).



b. Click "Move" and select the destination folder (RAP-VPN\_b17).

🗟 Select destination				
Host01-HD	 OV-185 AT		RAP-VPN_b17_1.v	<b>A</b>
NOD12	 OVE_161_44R1_b43		RAP-VPN_b17-ded	
SL222	OVE_451_b21_15		RAP-VPN_b17.nvram	
🧮 SL223	i OVE_451_b21_15		RAP-VPN_b17.vmdk	
	📁 OVE-45R01_b12		RAP-VPN_b17.vmsd	
	📁 OVE170_44R2_bui		RAP-VPN_b17.vmx	
	ar RAP-VPN_b17		RAP-VPN_b17.vmx	
	a RAP-VPN_b20		RAP-VPN_b17.vmxf	

#### c. Verify the move.



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

vmware <sup>,</sup> vSphere Web Clie	ent 🔒 🖉		
( Home ) 🕲 I	RAP-VPN_b17 Actions -		
	Getting Started Summary	Monitor Manage Related Objects	
	Province of	RAP-VPN_bt7           Guest OS:         CentOS 4/5/6/7 (64-bit)           Compatibility:         ESXI5 5 and later (VM ver VM ware Tools):           VM ware Tools:         Not running, not installed DNS Name:           IP Addresses:         Host:           10:255:214.211         10:255:214.211	rsion 10)
ALE-SLAB-AD	🔁 RAP-VPN_b17 - Edit Set	tings	(?)
Hali-Linux-2	Virtual Hardware VM Opt	ions SDRS Rules vApp Options	
All-Linux_CentOS	> 🖬 CPU	4 🔹 🖲	
Kali-Linux_Ubuntu-1	Memory	4096 v MB	•
RAP-VPN_b17	+ 🛄 Hard disk 1	Device will be removed 📃 Delete file	s from datastore
RAP-VPN_b20     Repart 65 RAP-pet	+ 🛄 Hard disk 2	1 GB	•
Server50	Metwork adapter 1	RAP-HQ_3970	<ul> <li>Connect</li> </ul>
B Win7-DonotDelete	Network adapter 2	HAN-2000	<ul> <li>Connect</li> </ul>
Win/-IV-75	Metwork adapter 3	RAP-HQ-to-H-Core	✓ Connect
10.255.214.132	Network adapter 4	OV-NMS_SLAB_255	<ul> <li>Connect</li> </ul>
10.255.214.212	▶ 🔂 USB controller	USB 2.0	
Linux-RS	Video card	Specify custom settings	•
🔀 Ucopia2	► WCI device		
Win7-TV-76	<ul> <li>Other Devices</li> </ul>		
► The second seco			
	New device:	Select 💌	Add
	Compatibility: ESXi 5.5 and I	ater (VM version 10)	OK Cancel

**4.** Recreate the disk with new copied virtual disk file, "RAP-VPN\_b20.vmdk". New device >> Existing Hard Disk>> Add.

🔁 RAP-VPN_b17 - Edit Set	tings	(?) ▶
	4 🗸 🗸	
Memory	4096 v MB v	
▶ 🛄 Hard disk 1	1 GB 💌	
Metwork adapter 1	RAP-HQ_3970 🔹 🗹 Connect	
Metwork adapter 2	HAN-2000 🔹 Connect	
Metwork adapter 3	RAP-HQ-to-H-Core	
Metwork adapter 4	OV-NMS_SLAB_255   Connect	
🕨 🖶 USB controller	USB 2.0	::
▶ 🛄 Video card	Specify custom settings	
VMCI device		
<ul> <li>Other Devices</li> </ul>		
New device:	🚍 Existing Hard Disk 🔹 Add	•
•		•
Compatibility: ESXi 5.5 and I	ater (VM version 10) OK	Cancel

a. Select the virtual hard disk file (RAP-VPN\_b20.vmdk):

#### Select File Datastores Information Contents RAP-VPN b20.v. Name: Server50 AP-VPN\_b17\_1.vmdk ▶ C AP-SIM-3 BAP-VPN\_b20.vmdk Size: 1.96 GB Modified: 4/9/2020 2:22 PM 📥 RAP-VPN\_b17.vmdk Server165 TRAP-VPN\_b17 ▶ OV-140H2-44R2-b50-ve OV-141H1-451-b15-140 OV-185\_AT Kali-Linux-3 Debian OVE-45R01\_b12\_New ▶ TRAP-VPN b20 OV-140H1-44R2-b50-Ve OVE\_451\_b21\_150h1 AP-SIM-1\_1 OV\_451\_b16\_145S File Type: Compatible Virtual Disks(\*.vmdk, \*.dsk, \*.raw) Ŧ OK Cancel

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

**5.** Power on the VA (RAP-VPN\_b17).

OV-185_AT	
RAP-VPN_b17	Hard disk 1
AP-VPN_b20	Actions - RAP-VPN_b17
Server165_RA	🛒 Open Console
Server50	Power On
A Win7-DonotDe	Shut Down Guest OS

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

# **Basic Troubleshooting Checklist**

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

- Check that the IP Address is present in the Data-VPN.conf file imported to VPN-VA.
- Verify that the firewall is not blocking traffic in both ways (from outside company, from VPN-VA).
- If both tunnels are UP but client does not get DHCP lease:
  - Check if the client is present in the AP association list with command "ssudo sta\_list" and he mapped to the tunnel ID of the Data VPN Server, command "brctl show" could be action to have additional information (ath0x interface must be associated to br-g1 interface).
  - Check if the Client's MAC Address is learnt on the corporate access switch where we bridge the traffic.
  - Check the switch config for DHCP replay (ip helper, dhcp-snooping).
- If client is not able to access LAN network:
  - Client is not able to ping any device or gateway within same subnet. Make sure that Promiscuous Mode is enabled and set to "Accept" on the vswitch (by default this is set to reject).
  - Promiscuous Mode is enabled but it is not working. Check if the Override checkbox is disabled. If enabled ensure the setting is set to "Accept".

# **Useful Logs and Commands**

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

For **sta\_list** output, check the TUNNELID and FARENDIP of the VPN VA Server.

STA_MAC	IPv4	IPv6	OnlineTime	
b0:72:bf:d0:63:de	172.28.1.51	fe80::8389:64ed:fbd4:e	730	8

RX	ТΧ	FREQ	AUTH	Final_role	VLANID	TUNNELID	FARENDIP
4237	5860	5GHz	PSI	KRA	P3 0	0	DVPN-132

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

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

interface: wg0

public key: BOpBbWqvxFKEZ8gAVJACaVY4Lp5d6cKSK5y1+QH05i4=

private key: (hidden)

listening port: 58161

peer: hfbchhiCJHOZz5UMh1BVbvDfWqRICpgwm7I1o6Jh1QI=

endpoint: 198.206.185.132:9093

allowed ips: 172.16.198.254/32, 172.20.0.155/32

latest handshake: 3 seconds ago

transfer: 267.09 KiB received, 625.22 KiB sent

persistent keepalive: every 5 seconds

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

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

•••

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

link/gre 0.0.0.0 brd 0.0.0.0 promiscuity 0

gre remote any local any ttl inherit nopmtudisc

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

link/ether 00:00:00:00:00 brd 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