

Wave OpenVPN Server Guide for Wave 4.5 © 2014 by Vertical Communications, Inc. All rights reserved.

Vertical Communications and the Vertical Communications logo and combinations thereof and Vertical ViewPoint and Wave Contact Center are trademarks of Vertical Communications, Inc. All other brand and product names are used for identification only and are the property of their respective holders.

#### LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY

Vertical Communications, Inc. makes no representation or warranties with respect to the accuracy or completeness of the content of this publication and specifically disclaims any implied warranty of merchantability or fitness for any particular purpose, and shall not be liable for any loss of profit or any other commercial damage, including but not limited to, special, incidental, or consequential.

#### COPYRIGHT STATEMENT

This publication contains proprietary and confidential information of Vertical Communications, Inc. The contents of this document may not be disclosed, copied or translated by third parties, in any form, or by any means known, or not now known or conceived, without prior explicit written permission from Vertical Communications, Inc.

Vertical Communications, Inc. reserves the right to revise this publication and to make changes in content without notice.



# What's new in this version

#### **REVISED FOR THIS VERSION**

The following sections have been deleted from Chapter 2:

- Added section "OpenVPN Server configuration options" on page 1-2.
- Chapter 2 has been extensively rewritten to reflect the off-Wave configuration option introduced in Wave 4.5.

Text in blue indicates an addition or change in this version.

For details on everything that's new in Wave 4.5, see the Wave 4.5 Release Notes.



# Contents

## What's new in this version

## Contents

# Chapter 1 Introducing Wave OpenVPN Server

Overview	1-1
OpenVPN Server vs NAT traversal	1-2
OpenVPN Server configuration options	1-2
If you are already using OpenVPN Server in Wave 4.0	1-2
Requirements	1-3
Application server requirements	1-3
Network requirements	1-3
VPN configuration settings	1-3

# Chapter 2 Installing and Configuring Wave OpenVPN Server

About VMware vSphere Hypervisor <sup>™</sup>	2-1
Creating the OpenVPN virtual machine	2-2
Logging in to the virtual machine 2	2-20
Changing network settings for your environment 2	2-23
Configuring network routing 2	2-25
Configuring the Wave Server 2	2-26

## Chapter 3 Setting Up Users and Phones

About VPN phone users	3-1
Security concerns when configuring a user's VPN credentials 3-2	
Configuring VPN for a user	3-2
Specifying a user's VPN credentials	3-2

#### Contents

Enabling VPN on a user's IP phone	3-4
Configuring VPN on a user's IP phone	3-5
Troubleshooting problems	3-9

# Index



# Introducing Wave OpenVPN Server

#### CHAPTER CONTENTS

Overview	1-1
OpenVPN Server configuration options.	1-2
Requirements	1-3

#### Overview

OpenVPN Server allows phones outside of your network to behave the same as local phones. With OpenVPN Server, when a remote user goes off-hook, the user's phone automatically connects to your network. The OpenVPN Server extends your private network and its resources to support remote users with all the functionality and security available to local users.

OpenVPN Server is supported on the following Vertical IP Edge 5000i Gigabit phones, which include a built-in virtual private network client. This client uses the OpenVPN protocol to support a secure connection to the Wave Server.

- Vertical IP Edge 5000i-LLCDG Large LCD screen phone
- Vertical IP Edge 5000i-24G 24-button phone

**Important:** There are many third-party devices that also support the OpenVPN protocol. The Wave Gigabit-E SIP phones can be used with those devices, but Vertical cannot support them all. The Wave OpenVPN Server is a supported implementation of this protocol from Vertical.

For more information:

- For installation and configuration instructions, see Chapter 2.
- For steps to configure users in Wave and set up phones, see Chapter 3.



#### **OpenVPN Server vs NAT traversal**

OpenVPN Server is the preferred method to enhance remote phone integration. Another method is NAT traversal, which is less secure than OpenVPN Server but is supported on all Vertical Edge SIP phones. For more about NAT traversal, see Chapter 6 in the *Wave Global Administrator Guide*.

**Warning:** Using OpenVPN Server and NAT on the **same** Wave Server is not supported—this is a security threat and results may be unpredictable.

#### **OpenVPN Server configuration options**

There are two ways to configure OpenVPN Server:

• **Off-Wave configuration**. Choose this mode to use Wave's own VPN Server. The Off-Wave configuration process is simpler than with custom deployment (described below). Although you still need to install the OpenVPN virtual machine using VMware vSphere Hypervisor<sup>TM</sup>, most of the Windows and Wave configuration tasks are handled for you automatically.

The Wave 4.5 version of this guide focuses exclusively on off-Wave configuration.

• **Custom Deployment**. Choose this mode if your system configuration already includes a a VPN Server as well as a hardware router that supports VPN, and you want to use them with Wave.

Custom Deployment mode is the equivalent of the OpenVPN Server configuration method introduced in Wave 4.0.

If you choose this mode, you are responsible for all configuration tasks. You may find the Wave 4.0 version of the *Wave OpenVPN Server Guide* to be a helpful starting point.

#### If you are already using OpenVPN Server in Wave 4.0

If you are already using OpenVPN Server in Wave 4.0, do not make any changes to your current configuration before upgrading to Wave 4.5. The upgrade process automatically changes your configuration type to Custom Deployment, the equivalent of the OpenVPN Server configuration method introduced in Wave 4.0. All of your current settings will be retained, no additional steps are required, and you do not need to make any other changes after upgrading.



## Requirements

#### **Application server requirements**

The virtual machine where OpenVPN Server runs requires the following resources on your applications server:

- Minimum 1 processor core
- 2 GB RAM
- 20 GB hard drive space
- VMware vSphere Hypervisor, a free platform for running a virtual machine on an applications server. For download instructions, see Chapter 2.

#### **Network requirements**

- Public IP Address port-forwarded to OpenVPN Server, using Port 1194 UDP.
- Routing in the network default gateway to the VPN phone subnet.
- The Wave Server and the OpenVPN server should be on same subnet.
- Create an RSA certificate for securing VPN connections.

#### **VPN** configuration settings

The following VPN configuration settings need to be configured for each network:

- Static IP / Netmask for the openvpn virtual machine.
- DHCP subnet for VPN clients.
- A username and password for each VPN user.



# Installing and Configuring Wave OpenVPN Server

#### CHAPTER CONTENTS

About VMware vSphere Hypervisor™	2-1
Creating the OpenVPN virtual machine	2-2
Logging in to the virtual machine	. 2-20
Changing network settings for your environment	. 2-23
Configuring network routing	. 2-25
Configuring the Wave Server	. 2-26

**Important:** The information in this chapter assumes that you have a basic familiarity with virtual machines.

## About VMware vSphere Hypervisor™

VMware vSphere Hypervisor is a free platform for running a virtual machine on an applications server. For more about Hypervisor, see:

http://www.vmware.com/products/vsphere-hypervisor/overview. html

This guide does not cover the installation of the VMWare platform. Refer to the VMware documentation for details on setting up vSphere Hypervisor.



## **Creating the OpenVPN virtual machine**

- 1. Download the OpenVPN.zip file from V-Connect, and extract file to a location on your applications server that has 20 GB of free space. There will be two VMDK files:
  - OpenVPN\_deploy
  - OpenVPN\_deploy-flat
- 2. Launch the vSphere Client (included with Hypervisor) and log in using the credentials for your Hypervisor.





🚱 10.0.1.62 - vSphere Clier	nt						_ 8 ×
File Edit View Inventory	Administration Plug-ins Help						
🖸 🖸 🛕 Home	▶ 👸 Inventory 🕨 👘 Inventory						
1. Ct							
10.0.1.62	localhost.BUTLER VMware ESXI, 5.1.0, 7	799733   Evaluation (60 d	days remaining)				_
	Getting Started Summary Virtual Mac	nines Resource Allocation	Performance Config	uration Local Users	& Groups Ev	ents Permission	15
	Hardware	View: Datastores D	evices				
	Health Status	Datastores		Refresh De	lete Add Stor	rage Rescan	Al
	Processors	Identification	A Device	Drive Type	Capacity	Free Type	
	Storage	(g catastoret	Browse Datastore		1.01 10	1.01 ID VMP;	20
	Networking		Rename				
	Storage Adapters		Unmount				
	Advanced Settings		Delete				
	Power Management		Refresh				
	Software	•	Properties				
	Licensed Features	Datastore Detail	Copy to Clipboard Ctr	1+C		Proper	ties
	Time Configuration	datastore1 Location: /vmfs/vc	Jumes/5138a765-0b823	14a-c2d3-001cc09f79	49	1 TB Capacity	-
	DNS and Routing	Hardware Acceleration	n: Unknown		980.00	MB Used	
	Authenbcabon Services Virtual Machine Startuo/Shutdown				1.0		
	Virtual Machine Swapfile Location						
	Security Profile	Path Selection					
	Host Cache Configuration System Resource Allocation	<	Dronartiae	Evt.	ante		<u> </u>
	Agent VM Settings						-
Recent Tasks			Name,	Target or Status cont	ains: •		Clear )
Name	Target Status Details	Initiated by Requ	uested Start Ti 🔽 Sta	rt Time	Completed Tir	me	

3. On the Configuration tab, right-click on the datastore and choose **Browse Datastore**.



- 🔗 10.0.1.62 vSphere ( \_ 8 × File Edit View Inventory Administration Plug-ins Help 🔥 Home 🕨 👸 Inventory 🕨 🛅 Inventory 5 0 10.0.1.62 localhost.BUTLER VMware ESXi, 5.1.0, 799733 | Evaluation (60 days remaining) rce Allocation Performance Configuration Local Users & Group a Started Sum - 0 × 🚱 Datastore Brow wser - [datastore1] n All. 8 8 B X 🕗 8 B D Upload files to this datastore store1] / Folders Search 1FS5 Modif 10 Size Type Path Name F ٠ • Resource Al Agent VM Settings **Recent Tasks** Name, Target or Status contains: -Initiated by Requested Start Ti... V Start Time Name Target Status Details Completed Time
- 4. In the Datastore Browser, click the **Upload files to this datastore** button on the toolbar.



5. Click Upload File.



6. Select both files and then click **Open**.

🔗 Datastore Browser - [datas	store1]				-	
🚱 Upload Items					×	
G 🗢 🗼 • Computer •	Butler-Data (F:) + OpenVPN		👻 🌇 Search	OpenVPN	2	
Organize 👻 New folder				iii • E	1 🕡	Modif
<u>م</u>	Name *	Date modified	Туре	Size	1	
Cibraries	OpenVPN deploy	2/21/2013 8:41 PM	VMDK File	1 KB		
Documents     Music	OpenVPN deploy-flat	2/21/2013 8:41 PM	VMDK File	20,971,520		
Pictures						
Videos						
Computer						
Local Disk (C:)						
Butler-Data (F:)						
Data (Z:)						
						F
🙀 Network 📃						
. 🎘 10.0.1.2						-
ALEXA-LAPTOP						
File on						
riie na	me. [OpenvPi4_depioy				-	
			0	pen Canc	el	
					11.	



10.0.1.62 - vSphere Clie	nt												_ 8 >
File Edit View Inventory	Administrat	ion Plug-ins H	Help										
New	•	Virtual Ma	chine Ctrl+N										
Deploy OVF Template		Resource	Pool Ctrl+O										
Export		Add Permi	ssion Ctrl+P										
Report	•	localhost.BU1	LER VMware E	5Xi, 5.1.0, 7	99733	Evaluation	1 (60 day	s remaining)					
Browse VA Marketplace		Getting Starte	dSummary	Virtual Mach	ines Re	source Allo	cation	erformance C	onfiguration	Local User	s & Groups	Events Pern	nissions
Print Maps	+	Hardware			View:	Datasto	res Devi	tes					î
Exit		Health St	atus		Datas	stores			R	efresh De	elete Add S	torage I	Rescan All
		Processor	s		Iden	tification	~	Device	Drive 1	Гуре	Capacity	Free	Туре
		Memory				datastorel		Local ATA Dis	(t Non-S	Œ	1.81 TB	1.81 TB	VMFS5
		<ul> <li>Storage</li> </ul>											
		Networkir	lg										
		Storage A	Idapters										
		Network /	Adapters										
		Advanced	Settings										
		Power Ma	nagement		41								F
		Software											
		Licensed	Features		Datas	store Deta	ils						Properties
		Time Con	fouration		data	store1					1	.81 TB Capi	acity 📥
		DNS and	Routing		Loca	ation: /v dware Accel	mts/volun	1es/5138a765-0	b82314a-c2d3	3-001cc09f79	949 980.	00 MB 🔲 U	lsed
		Authentic	ation Services				crooth.	onknorm			1	.81TB 🔲 F	ree
		Virtual Ma	chine Startup/Shu	tdown									
		Virtual Ma	chine Swapfile Lo	cation									
		Security P	rofile										
		Host Cad	ne Configuration		Path	Selection		Pronartiae		Evi	tonte		
		System R	esource Allocation		•								
		Agent VM	Settings										
Recent Tasks								N	ame, Target o	r Status con	tains: •		Clear
Name	Target		Status	Details	Initi	ated by	Request	ed Start Ti 🔽	Start Time		Completed	Time	
Manipulate file paths			Completed		root		3/7/2013	1:57:23 PM	3/7/2013 1:	57:23 PM	3/7/2013 1:	57:23 PM	
Manipulate file paths			Completed		root		3/7/2013	1:57:18 PM	3/7/2013 1:	57:18 PM	3/7/2013 1:	57:18 PM	

7. Click File > New > Virtual Machine.

The Create New Virtual Machine wizard starts.



8. In the Configuration screen, choose **Custom**. This allows you to specify the drive to be used. Click **Next** to continue.





9. In the Name and Location screen, enter a **Name** for the new virtual machine, and then click **Next**.





10. In the Storage screen, select the datastore where you copied the VM disk image. Note that you do not specify the VM disk itself on this screen, just the datastore. Click **Next** to continue.

ame and Location torage rtual Machine Version uest Operating System PUs emory etwork	Name	Drive Type Non-SSD	Capacity Provisioned 1.81 TB 980.00 MB	Free Type 1.81 TB VMFS5	Thin P
tual Machine Version uest Operating System PUS emory etwork	datastore1	Non-SSD	1.81 TB 980.00 MB	1.81 TB VMF55	Suppo
Controller t a Disk ly to Complete	▼ Disable Storage	DR5 for this virtual n	nachine		
	Select a datastore:				
	Name	Drive Type	Capacity   Provisioned	Free Type	Thin Pro



11. In the Virtual Machine Version screen, choose VMWare 8 and then click Next.





12. In the Guest Operating System screen, choose Linux as the Guest Operating System and then select CentOS 4/5/6 (32-bit) from the Version drop-down list.

🚱 Create New Virtual Machine		
Guest Operating System	southers to use with this with a suching	Virtual Machine Version: 8
speary the guest operating	system to use with this virtual machine	
Conflouration Name and Location Storage Wrbad Machine Version Guest Operating System CPUs Memory Network SCSI Controller Scelect a Disk Ready to Complete	Guest Operating System:	ppropriate defaults for
Help	Deban GNU/LINUX 5 (54-bit) Deban GNU/LINUX 5 (32-bit) Deban GNU/LINUX 6 (54-bit) Deban GNU/LINUX 4 (52-bit) Asianux 4 (54-bit) Asianux 3 (54-bit) Asianux 3 (54-bit) Orade Linux 4/5/6 (54-bit) Orade Linux 4/5/6 (54-bit) Ubuntu Linux (54-bit) Ubuntu Linux (54-bit) Other 2.6.x Linux (54-bit)	Vext > Cancel



13. In the CPUs screen, specify the number of processors needed, and then click **Next**. The default values are typically adequate.

Create New Virtual Machin	1e			_ 🗆 ×
CPUs	al cours for the side of an alter		Virtual	Machine Version: 8
Select the number of virtu	Jai CPUs for the virtual machine.			
	_			
Configuration	Number of virtual eacheter			
Storage	Number of Virtual sockets.			
Virtual Machine Version	Number of cores per virtual socket:	1 💌		
CPUs	Total number of cores:	1		
Memory	The number of virtual CPI is that you	I can add to a VM		
Network SCSI Controller	depends on the number of CPUs on	the host and the		
Select a Disk	number of CPOS supported by the g	uest 03.		
Ready to Complete				
	The virtual CPU configuration specif might violate the license of the gues	ied on this page at OS.		
	Click Help for information on the nur	nher of		
	processors supported for various gu	lest operating		
	systems.			
	J			
Help			< Back Next >	Cancel



14. In the Memory screen, specify the amount of RAM needed, and then click **Next**. The default value of MB is typically adequate.





15. In the Network screen, specify the number of network adaptors needed., and then click **Next**. The default values are typically adequate.

Create New Virtual Machin	ie	
Network Which network connection	ns will be used by the virtual machine?	Virtual Machine Version:
Configuration Name and Location Storage Virtual Machine Version Gelds Guest Operating System CPUs Memory Network SCSI Controller Scient a Disk Ready to Complete	Create Network Connections How many NICs do you want to connect?          I       I         Network         NIC 1:       VM Network         If supported by this virtual machine version, more than 4 virtual machine is created, via its Edit Settings dialog.         Adapter choice can affect both networking performance and the VMware KnowledgeBase for more information on choose supported for various guest operating systems and hosts.	Connect at Power On Flexible T T NICs can be added after the migration compatibility. Consult ing among the network adapters
Help	< Bi	ack Next > Cancel



16. In the SCSI Controller screen, keep the default value, and then click Next.

🚱 Create New Virtual Machine		_O×
SCSI Controller Which SCSI controller type	would you like to use?	Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Advanced Options Ready to Complete	SCSI controller  C Bust.ogic Parallel (not recommended for this guest OS)  C LSI Logic Parallel  C LSI Logic SAS  C VMware Paravirtual	
Help	< Back	Next > Cancel









18. In the Select Existing Disk screen, browse to the location of the files that you uploaded to the datastore previously, and then click **Next**.

🔗 Create New Virtual Mach	ine			_ 0 ×
Select Existing Disk Which existing disk do y	ou want to use as this virtu	al disk?		Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System	Disk File Path		Brow	ise
CPUs Memory	Browse Datastores	;		-IIX
Network SCSI Controller	Look in: Datastores	s	- E	
Select a Disk	Name	Capacity	Free space	
Advanced Options	datastore1	1.81 TB	1.81 TB	
ready to complete				
	File type:	Compatible Virtual Dis	iks (*.vmdk, *.dsk, *. 💌	Open Cancel
Help			< Back	Next > Cancel

Double-click on the datastore, and then select the OpenVPN file and click OK.

**Note:** If you don't see the OpenVPN file, make sure that you uploaded both VMDK files (OpenVPN\_deploy and OpenVPN\_deploy-flat) as described earlier. You won't see the OpenVPN file in the datastore unless you downloaded both files.



19. In the Advanced Options screen, leave all settings unchanged. These are expert settings that should not be changed unless you are experienced VMware user and you are addressing a specific issue. Click **Next** to continue.

Create New Virtual Machine Advanced Options These advanced options do	e not usually need to be changed.	ual Machine Version: 8
Confouration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network Solid Controller Select Existing Disk Advanced Options Ready to Complete	Specify the advanced options for this virtual disk. These options do not normally need be changed. Virtual Device Node SCSI (0:0) Mode Independent Independent disks are not affected by snapshots. C Persstent Changes are immediately and permanently written to the disk. C Norpersistent Changes to this disk are discarded when you power off or revert to the snapshot.	3
Help	< Back Next >	Cancel



20. In the Ready to Complete screen, review your selections and then click Finish.

🚱 Create New Virtual Machine		<u>_</u> _×
Ready to Complete Click Finish to start a task th	at will create the new virtual machine	Virtual Machine Version: 8
Ready to Complete Click Finish to start a task th Name and location Storage Wrtual Machine Version Guest Operating System CPUS Memory Network SCSI Controller Select 2005 Select Stating Disk Advanced Options Ready to Complete	at will create the new virtual machine Settings for the new virtual machine: Name: Host/Cluster: Datastore: Guest OS: CPUs: Memory: NICs: NICs: NICs: NIC1 Network: NIC1 Network: NIC1 Network: NIC1 Type: SCSI Controller: Create disk: Virtual Device Node: Disk file path: Disk mode:	OpenVFN localhost.BUTLER datastore1 CentOS 4/5/6 (32-bit) 1 2048 MB 1 VM Network Flexible LSILogicParallel Use existing disk SCSI (0:0) [datastore1]OpenVPN_deploy.vmdk Persistent
Help	Edit the virtual machine settings bef     Creation of the virtual machine (VM     system. Install a guest OS on the V	ore completion ) does not include automatic installation of the guest operating M after creating the VM. <a href="https://www.cancel.org"><a href="https://www.cancel.org">Sancel</a></a>



## Logging in to the virtual machine

The following steps describe how to log into the OpenVPN Server virtual machine.

1. In the vSphere Client, right-click the OpenVPN Server virtual machine, and then choose **Open Console**.





2.



3. Right-click on the Virtual Machine and choose **Start**. Then choose **Connect** from the same right-click menu.



4. Double-click on the **openVPN** user.



5. Enter the Vertical default password, Vertical4VoIP!. and then click Log In.





#### Changing network settings for your environment

The following steps describe how to give your VPN server network access to support connecting to VPN phones.

1. From the desktop, click **System > Preferences > Network Connections**.



2. On the Wired tab, click **Add**. If a network connection is already displayed, click **Edit** instead.

	Net	work Connectio	ns			
Wired	Wireless	Mobile Broadb	and	3	VPN	DS
Name		Las	st Use	d	1	Add
Auto eth1		no	w		E	dit
					De	lete
						<u>C</u> lose



3. In the Editing dialog, click the IPv4 Settings tab and make the following changes:

<b>1</b>	ininazia.		Editing Au	to et	h0		×
Connection	n <u>n</u> ame: :t <u>a</u> utom	Au	ito eth0 ally				
Wired 80	02.1x Se	curit	y IPv4 Sett	tings	IPv6 Setti	ngs	_
Method:	Manu	al				0	
Addres	ses						
Addre	ess	Net	mask	Gat	eway	Add	
10.10	.10.10	255	.255.255.0	10.1	10.10.1	Delete	
DNS se	ervers:		10.10.10.2,	10.10	0.10.3		
Search	Search domains:		domain.com				
DHCP	client ID	:					
⊠ Rec	quire IPv	4 ad	dressing for	this (	connection	to complete <u>R</u> outes	
🗹 Availab	ole to all	usei	rs		<u>C</u> ancel	Apply	

• Select Manual from the Method drop-down list.

**Important:** Do not leave the default **Automatic (DHCP)** as with this setting, a network address reassignment would cause all VPN phones to stop working.

- In the Addresses section, you provide information for the OpenVPN server to operate on the same subnet as the Wave Server. Click Add to add a static address:
  - Enter the static **IP Address** that will be used for the VPN server on your network. Make a note of this IP address so that you can enter it according to the steps in "Configuring the Wave Server" on page 2-26.
  - Enter the Netmask for the network the VPN server will reside on.
  - Enter the default **Gateway** for this network.
- Enter your own **DNS servers** for this network, separated by commas.
- Click **Routes** to enter static routes only if necessary.
- Click **Apply** to save your changes.

## **Configuring network routing**

Work with your network administrator to complete this step. Detailed instructions to accomplish the following tasks cannot be provided here as they depend on the network firewall or router used in your network.

- Set up forwarding for port 1194 to the same port on the OpenVPN server.
- Verify that you can make a connection to the OpenVPN server from outside the network.

A simple way to do this is to download an OpenVPN client for your laptop, for example:

https://openvpn.net/index.php?option=com\_content&id=357

Then, point the client at the public IP address of the network firewall, and login to OpenVPN.

• Your network must be configured to make the OpenVPN server the destination gateway for all traffic directed to the VPN phones from the rest of the network. A route statement entered on the network gateway is the simplest way to accomplish this.

For example, in a network where the default gateway is 10.1.1.1, the Wave Server is 10.1.1.8, and the VPN server has been assigned a local IP address of 10.1.1.15, you would add a route statement similar to the following to the 10.1.1.1 gateway:

IP Route 10.10.2.0 255.255.255.0 10.1.1.15

**Note:** The command to enter the route statement depends on the specific hardware of the default gateway.



## **Configuring the Wave Server**

#### To configure OpenVPN Server on the Wave Server

- 1. In the Global Administrator Management Console, click **IP Telephony**, located in the PBX Administration section.
- 2. Select **System Parameters > VPN Settings** in the left pane.

IP Telephony	
Signaling Protocols SIP System Parameters Advanced Codec Settings DTMF Transport Settings Quality of Service (QOS) TMV Settings Coll Routing Default Inbound Routing Signaling Control Points Bandwidth Management Zones	VPN Settings
	Restore Apply Done Help

- 3. Select the Enable VPN Support checkbox.
- 4. Enter the following information:
  - **Public IP Address**. Enter the Public IP address of the router or firewall that you port-forwarded to according to the steps in "Changing network settings for your environment" on page 2-23.
  - **Port**. Enter 1194.
  - Maintenance IP Address. Enter the IP address of the OpenVPN server. This IP address must be reachable by the Wave Server.



Note the following:

- The **Settings** buttons accesses advanced settings that should only be modified if you are directed to do so by Vertical Technical Support. These settings are described in detail in the WaveHelp topic for this tab. To view this topic:
  - Launch WaveHelp.
  - Expand the Contents pane.
  - Choose IP Telephony Configuration > Configuring Wave OpenVPN Server.
  - Scroll down to "Off Wave OpenVPN Server advanced settings".
- Upload VPN Certificate is only used if you are configuring OpenVPN Server using the Custom Deployment option, not covered in this guide.
- 5. Click **Done** to save your changes.



# **Setting Up Users and Phones**

#### CHAPTER CONTENTS

About VPN phone users	. 3-1
Security concerns when configuring a user's VPN credentials	. 3-2
Configuring VPN for a user	. 3-2
Configuring VPN on a user's IP phone	. 3-5
Troubleshooting problems	. 3-9

#### About VPN phone users

With OpenVPN Server, when a remote user goes off-hook, the phone automatically connects to the Wave network. Then, a VPN phone user's experience is exactly the same as that of a local user in the office—all phone features and commands work the same. For example:

- To call another Wave user, just go off-hook and dial the user's extension.
- To call an external number, enter the access code (typically "7" or "9") and then dial the 7- or 10-digit number.

VPN phone users need to be aware of the following:

- When using ViewPoint Desktop with a VPN phone, a user needs to verify the station number of the VPN phone if it's not his or her primary phone. For example, an employee who has a phone at home as well as in his office needs to change ViewPoint from the default station to the station number of the VPN phone when working from home.
- ViewPoint Desktop still requires that the remote user's computer itself be connected to the Wave Server via VPN—having a VPN phone does not provide that capability.
- A VPN phone may go into a bad state if the user's network connection is disrupted. This is rare, but it can prevent incoming calls or result in no audio. The simple fix is to reboot the VPN phone.



## Security concerns when configuring a user's VPN credentials

There are two ways to configure the user's VPN credentials on the phone:

- Via User/Group Management. This method is easier for the Wave administrator. However, this method is less secure because the credentials will be sent to the phone through the TFTP server which is inherently not secure. If there are any security concerns, configure the user's VPN credentials using the phone.
- Via the phone itself. This requires some extra effort on the part of the end user, but is more secure. See "Configuring VPN on a user's IP phone" on page 3-5.

## Configuring VPN for a user

You enable VPN on a per-user basis. Configuring VPN for a user consists of two steps:

- **Specifying the user's VPN credentials**. The same VPN username and password are used whether the user uses the ViewPoint Mobile Softphone or a supported VPN phone, or both.
- **Enabling VPN on the user's supported phone**. This task only applies if the user is configured with one of the supported phone models listed on page 1-1.

## Specifying a user's VPN credentials

Perform the following steps to specify a user's VPN credentials. How you do so depends on where the user's phone is located:

- **In network:** The user's phone is located inside the same LAN as the Wave Server, behind the firewall. For easiest configuration, phones should be inside the LAN for initial deployment.
- Not in network: The user's phone is located outside of the LAN.



#### To specify a user's VPN credentials

- 1. In the Global Administrator Management Console, click User/Group Management, located in the PBX Administration section.
- 2. Edit the user, and select **User > VPN** in the left pane.

👮 IP Server - User	×
Category	User \ VPN
	User name:
Pre <u>v</u> ious Ne <u>x</u> t	OK Cancel Help

- 3. Do one of the following:
  - **In network:** Click **Regenerate Credentials** to generate the user's VPN credentials, which will be automatically downloaded to the user's ViewPoint Mobile Softphone and/or supported IP phone.
  - Not in network: Enter a Username and Password manually, then make a note of the password so that the user can enter it on the phone itself. Alternatively, the user can configure his or her phone according to the steps in "Configuring VPN on a user's IP phone" on page 3-5, and tell you the password that was entered so that you can update the field here.
- 4. Click **OK** to save your changes.



#### Enabling VPN on a user's IP phone

Perform these steps only if the user is configured to use one of the supported IP phones listed on page 1-1.

#### To enable VPN on a user's IP phone

- 1. In the Global Administrator Management Console, click User/Group Management, located in the PBX Administration section.
- 2. Edit the user, and select **Phone > Networking** in the left pane.

🤶 Untitled - User	×
Category	Phone \ Networking
User     Voice Mail     Orice Mail     Orice Mail     Orice Mail     Orice Adding     Orice Station Features     Original Station Features     Original Station     Original Station	<ul> <li>Phone is located outside Wave's LAN</li> <li>Phone uses NAT</li> <li>Configure phone to use the default Wave STUN servers</li> <li>Configure phone to discover its global address using STUN</li> <li>STUN gerver:</li></ul>
	OK Cancel Help

- 3. Select the Phone is located outside Wave's LAN checkbox.
- 4. Click Phone uses VPN.
- 5. Click **OK** to save your changes.



## Configuring VPN on a user's IP phone

The information in this section applies to the supported phone models listed on page 1-1.

**Note:** If you already entered the user's VPN credentials via User/Group Management as described in "Configuring VPN for a user" on page 3-2, you do not need to re-enter them according to the following steps.

**Important**: Phones to be used with Wave OpenVPN Server must first be staged locally on a Wave Server running Wave 4.0. This will allow the 4.0 firmware that supports the latest VPN features to be downloaded to the phones, so that future firmware upgrades will be able to be downloaded via VPN itself.

1. On the phone, press the MENU key.





- \*\*
   NON FEB 25 11:538

   Configuration Menu

   1.Network Configuration

   2.SIP Configuration

   3.Phone Settings

   4.Call Preferences

   5.Directory

   6.Set to Default

   7.Lock/Unlock Config

   + Drovinus
- 2. Scroll through the Configuration Menu and select Lock/Unlock Config.

3. Enter the Configuration Menu password using the phone's keypad. This password protects some configuration options when changing them from the phone's keypad. The default password is 22222.



4. Press **OK** to return to the Configuration Menu.



5. Select Network Configuration.



6. Select VPN.





7. Select Password.



8. Enter the user's VPN password using the phone's keypad. (This is the user password that you created as described "Configuring VPN for a user" on page 3-2.) Alternatively, tenter a password here and then enter it on the User \ VPN tab in User/Group Management.



Press **Mode** to change the input mode between Upper Case, Lower Case, Numeric, and Symbols.

9. Press **OK** to save your changes.



## **Troubleshooting problems**

Here are some quick tips when troubleshooting problems with VPN phone operation:

- If the phone is stuck at "VPN trying", check to see if the phone is getting local IP. To do so, cancel from "VPN trying" and then navigate the phone menu to verify local IP). If the phone is not getting local IP, troubleshoot the network or specify a static local IP.
- If the phone is stuck at "VPN trying", verify that the phone has received the correct time from a public time server—SIP phones receive this from Wave's time server. To do so, cancel "VPN trying" and check the time displayed on phone. If the phone shows a 00:xx time (where xx could be any number) and you aren't doing this troubleshooting at midnight, then it is likely you don't have a correct time server.

#### Do the following:

1. Log on to the phone's web page (browse to the phone's local IP address with port 8000, for example:

http://192.168.2.1:8000

The default login credentials are:

- User name = private
- Password = lip.
- 2. From the menu, choose Network Time Configuration.
- 3. Verify that the time server specified in **SNTP Server Address** is a public time server accessible by the VPN phone. For a list of public time servers, see:

http://tf.nist.gov/tf-cgi/servers.cgi

- 4. Reboot the phone.
- Reboot phone at least twice. (Occasionally more than one reboot may fix the problem.)
- Check the router and verify that SIP ALG is disabled.



If the VPN phone connects but does not register with the Wave Server, you likely have a routing problem.

Verify you can ping the phone's VPN address from the Wave Server. To determine the phone's VPN address:

- 1. Press the Gear icon on the phone.
- 2. Select **#1 Network Configuration**.
- 3. Select **#11 VPN**.
- 4. Select **#6 Status**.
- 5. Select **#2 VPN Server IP**.

Log on to the remote desktop of the Wave Server and ping that IP address. To do so:

- 1. Click on the Start button and then choose **Run**.
- 2. Type **CMD**.
- 3. Type ping <IP Address> where <IP Address> is the VPN IP address.

If the ping times out, then check the route statement you entered on the local network gateway.

- Some routers are now blocking inbound connections even when initiated by internal devices on your network. If this is the case on your network, then VPN may never connect. To address this problem, on your router port-forward port 1194 to the phone's IP address.
- Verify with the Wave administrator that the phone is configured with the correct VPN user name and password.

**Note:** This is *not* the Wave user name and password—this is a *separate* set of credentials for VPN access, created on the OpenVPN server.



# Index

## Α

about OpenVPN Server, 1-1 security concerns, 3-2 VMware vSphere Hypervisor, 2-1

## С

configuring network routing, 2-25 user phone, 3-5 VPN for user, 3-2 Wave Server, 2-26

#### Ν

network routing configuring, 2-25 network settings changing for your environment, 2-23

## 0

OpenVPN Server about, 1-1 requirements, 1-3 supported phones, 1-1 OpenVPN virtual machine changing passwords, 2-20 creating, 2-2 logging in, 2-20

### R

requirements, 1-3

## S

security concerns, 3-2 supported phones, 1-1

## U

user configuring, 3-2 phone, 3-5

## V

VMware vSphere Hypervisor about, 2-1

## W

Wave Server configurig, 2-26

Vertical Wave OpenVPN Server Guide