Wave OpenVPN Server Guide for Wave 4.5

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

Index

Introducing Wave OpenVPN Server

CHAPTER CONTENTS

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™, 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

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

About VMware vSphere Hypervisor™

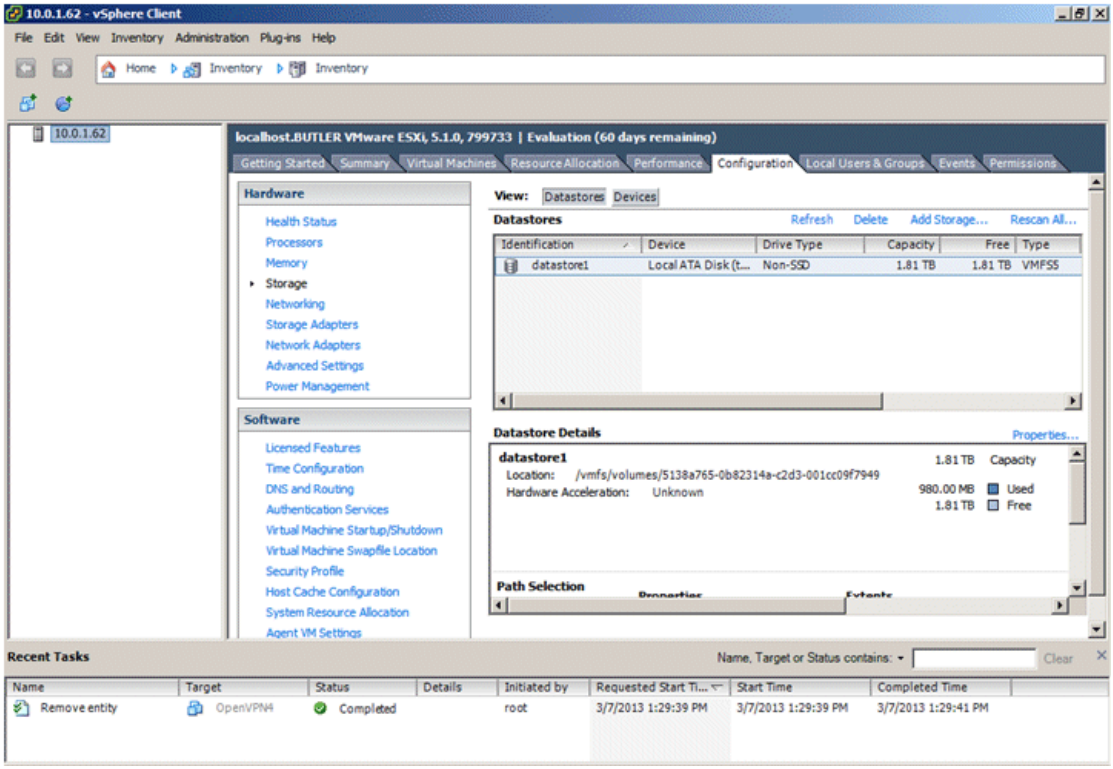
VMware vSphere Hypervisor is a free platform for running a virtual machine on an applications server. For more about Hypervisor, see:

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

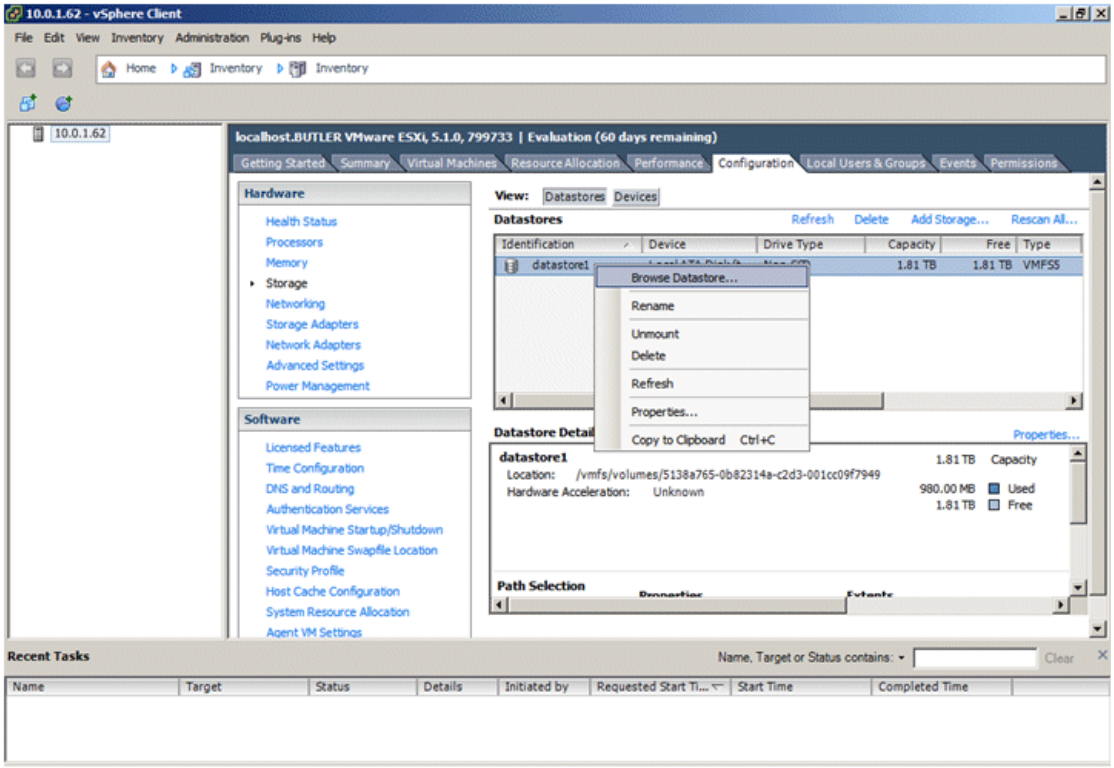
This guide does not cover the installation of the VMWare platform. Refer to the VMware documentation for details on setting up vSphere Hypervisor.

Creating the OpenVPN virtual machine

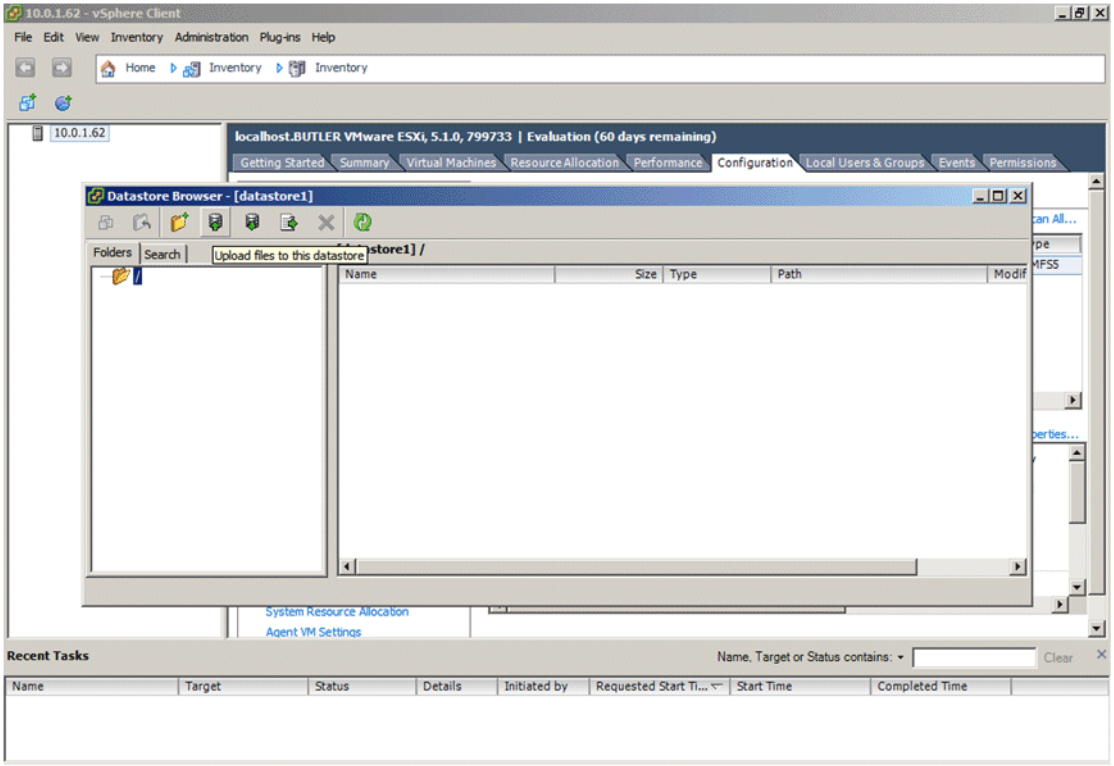
1. Download the OpenVPN.zip file from V-Connect, and extract file to a location on your applications server that has 20 GB of free space. There will be two VMDK files:
   - OpenVPN_deploy
   - OpenVPN_deploy-flat
2. Launch the vSphere Client (included with Hypervisor) and log in using the credentials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



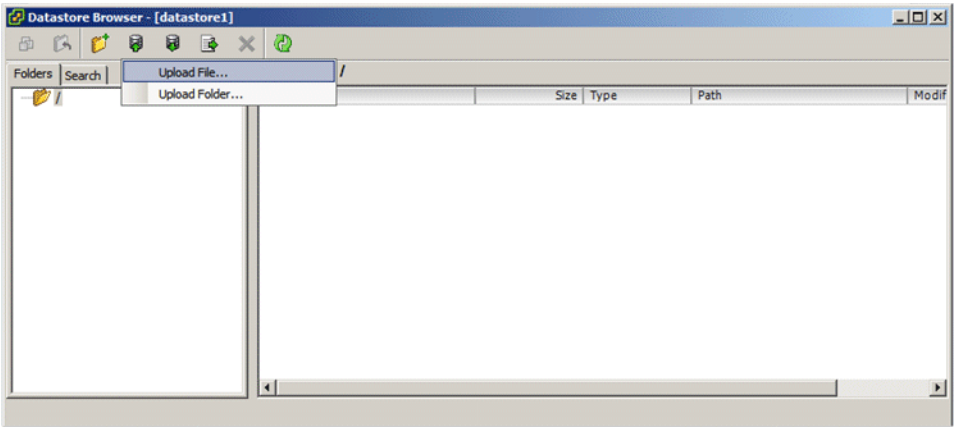
3. On the Configuration tab, right-click on the datastore and choose **Browse Datastore**.



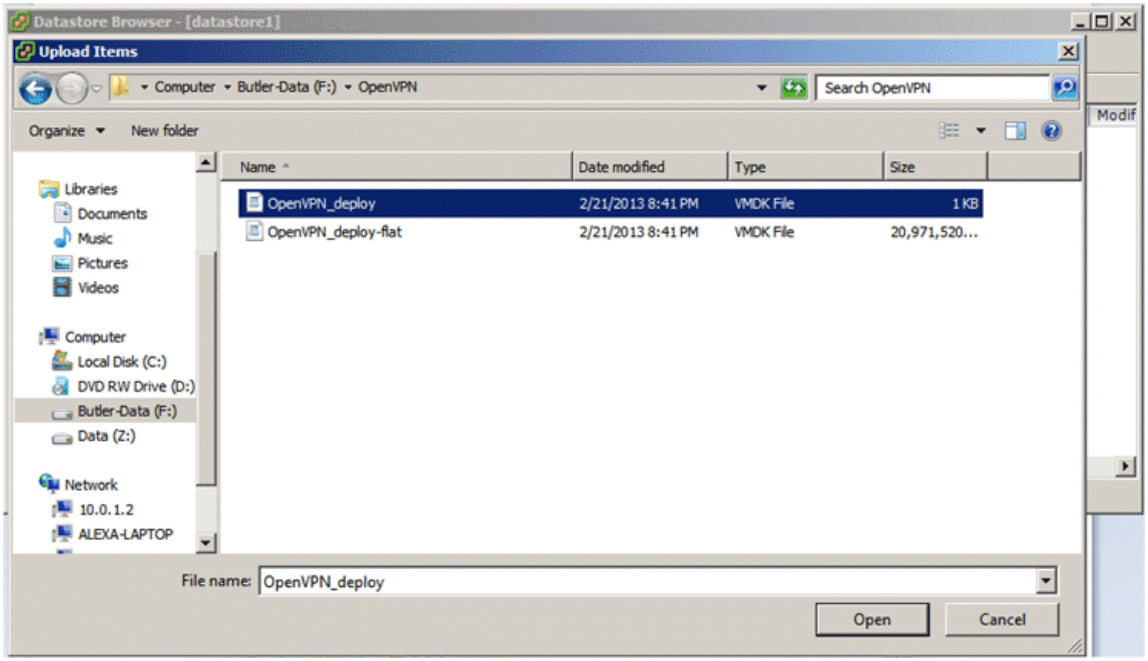
4. In the Datastore Browser, click the **Upload files to this datastore** button on the toolbar.



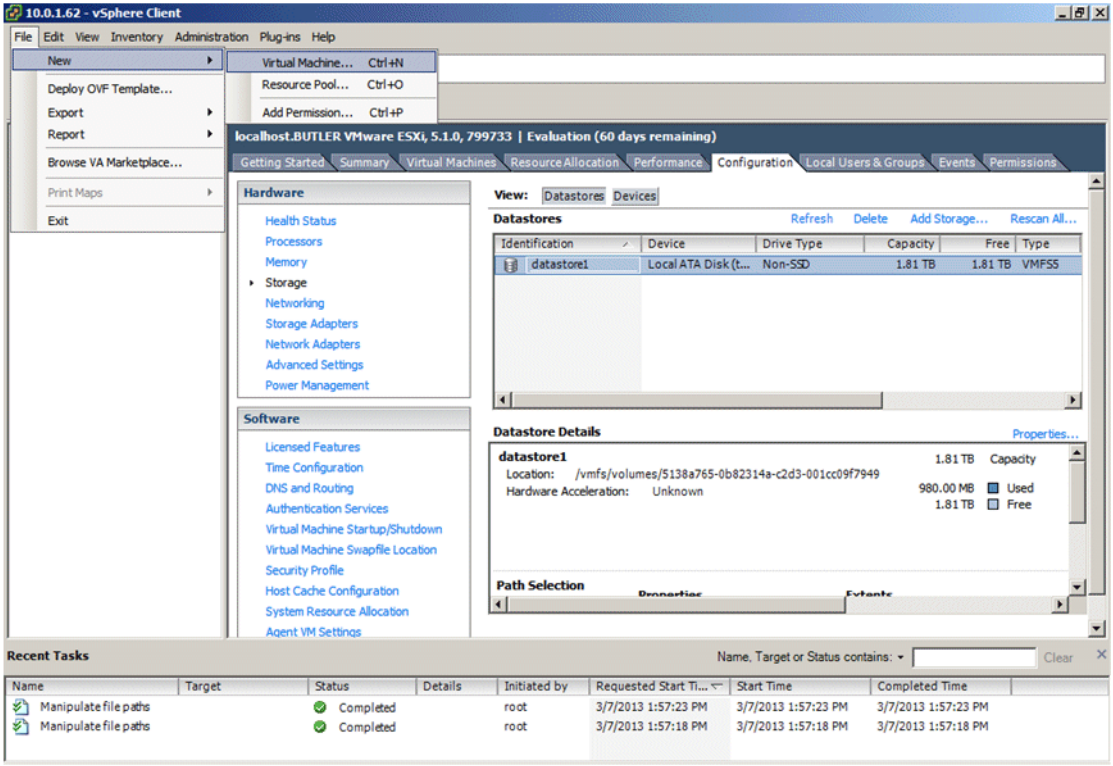
5. Click **Upload File**.



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

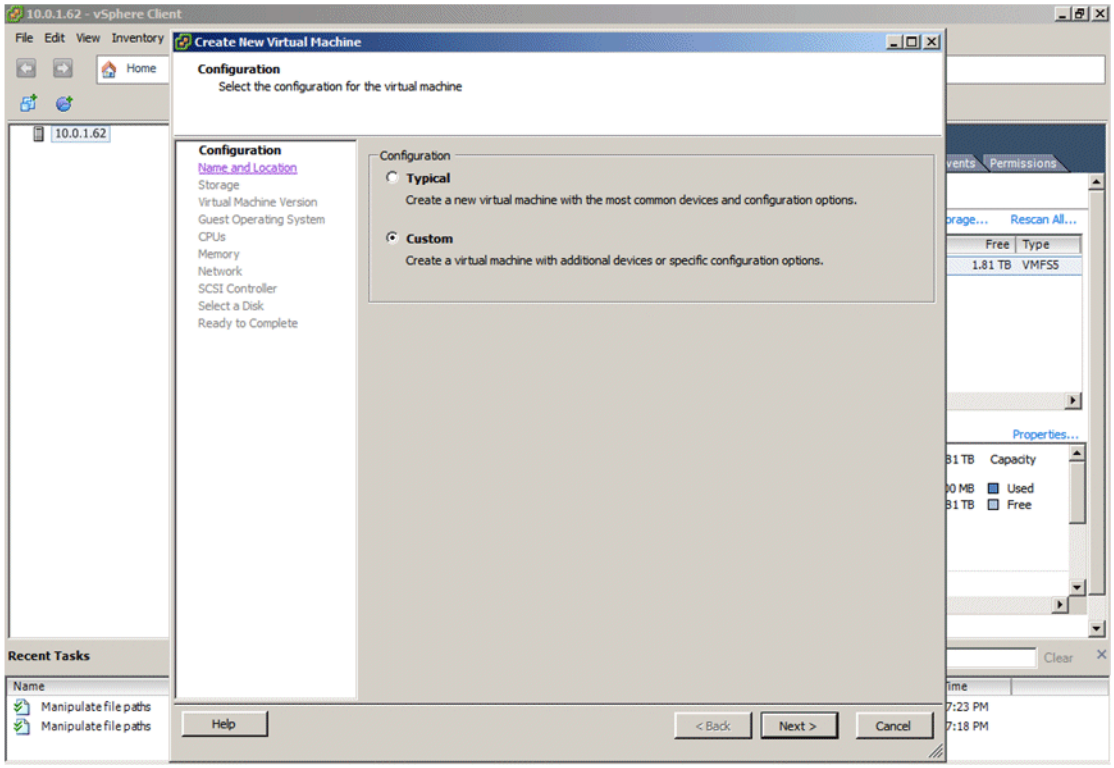


7. Click **File > New > Virtual Machine**.

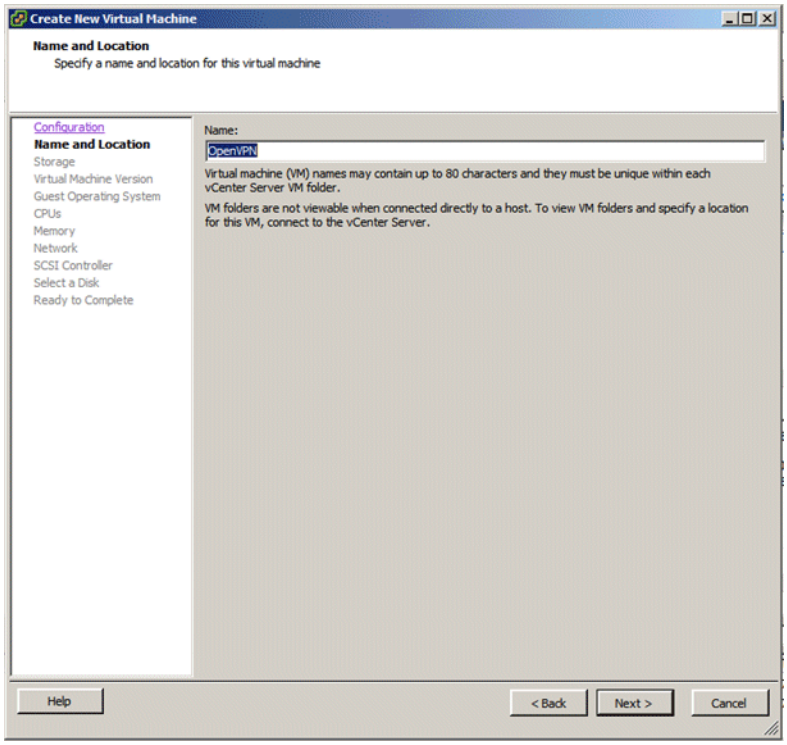


The Create New Virtual Machine wizard starts.

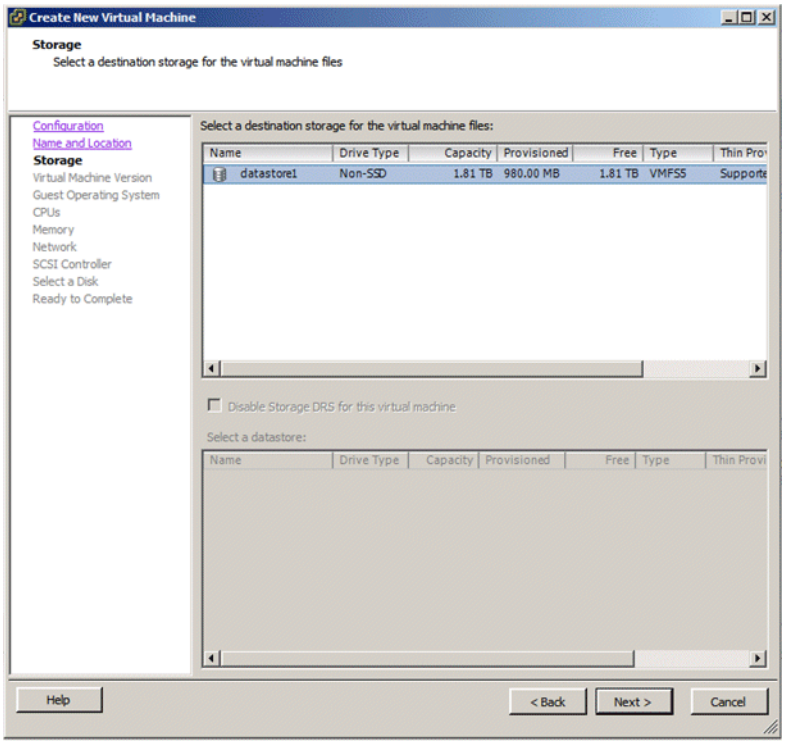
8. In the Configuration screen, choose **Custom**. This allows you to specify the drive to be used. Click **Next** to continue.



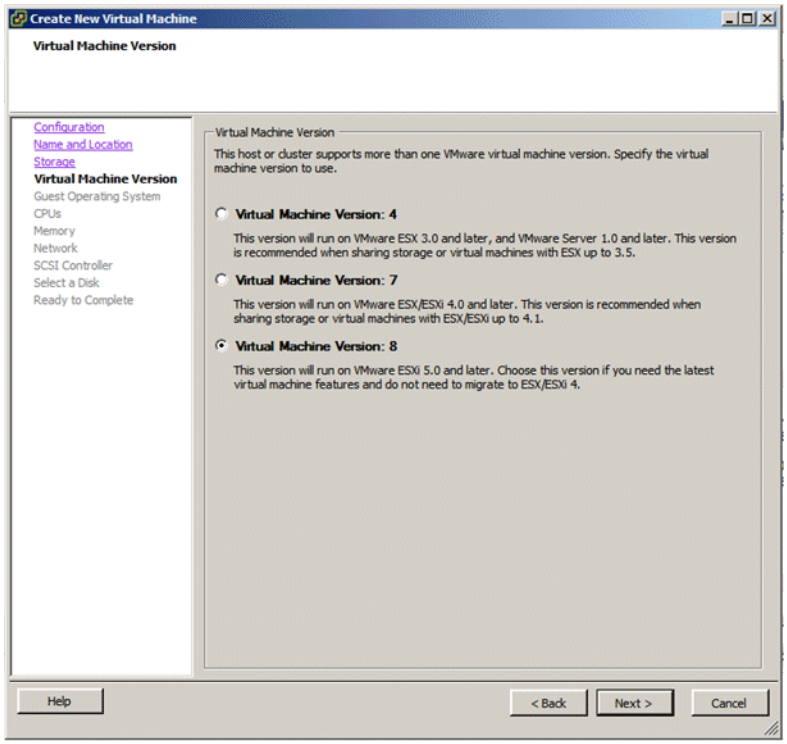
9. In the Name and Location screen, enter a **Name** for the new virtual machine, and then click **Next**.



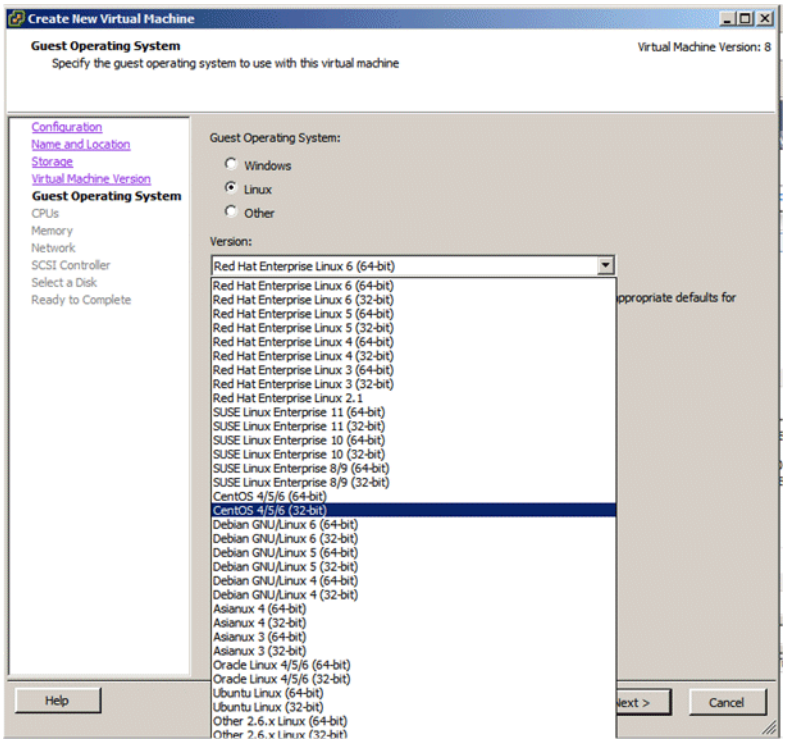
10. In the Storage screen, select the datastore where you copied the VM disk image. Note that you do not specify the VM disk itself on this screen, just the datastore. Click **Next** to continue.



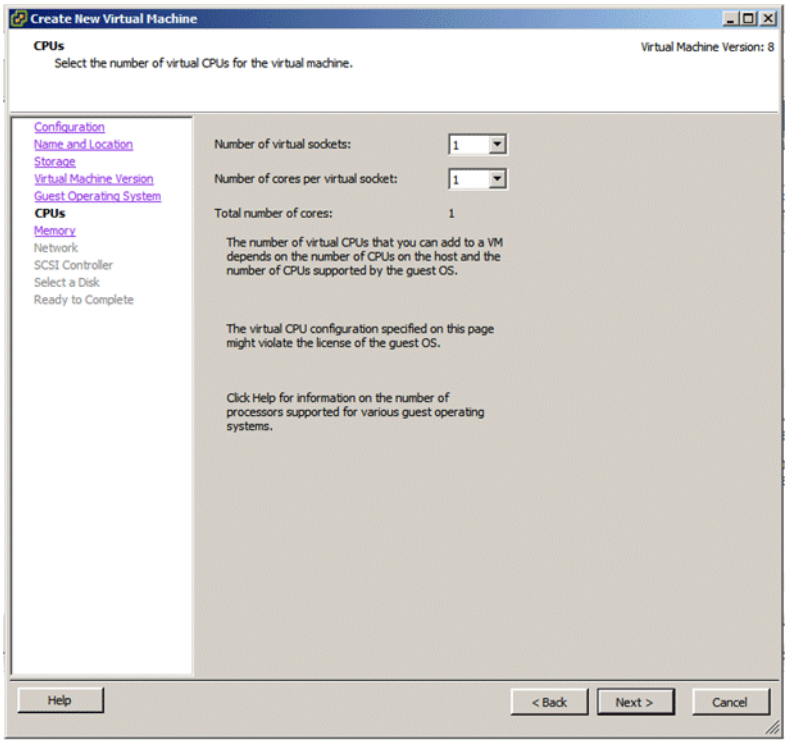
11. In the Virtual Machine Version screen, choose **VMWare 8** and then click **Next**.



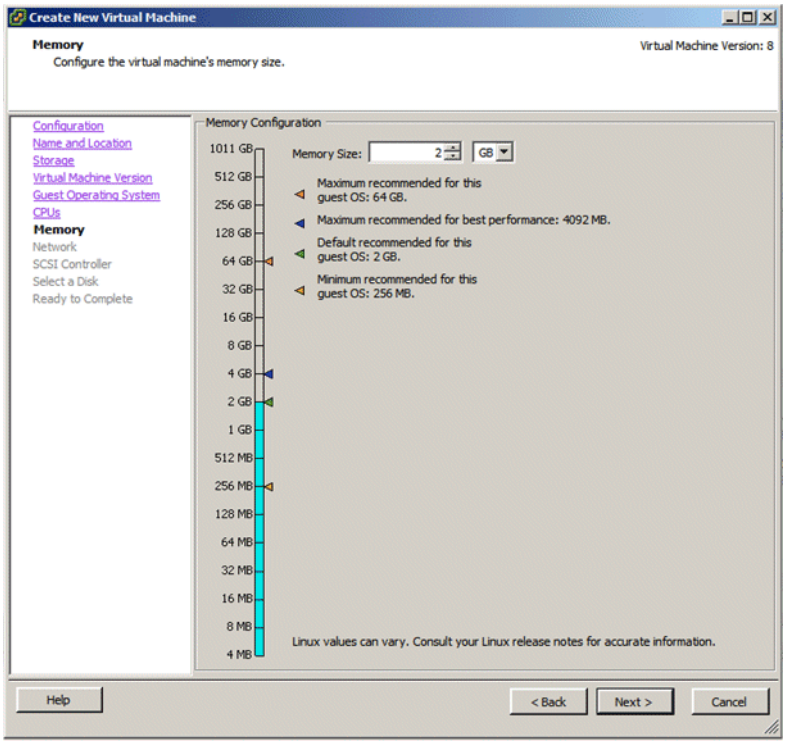
12. In the Guest Operating System screen, choose **Linux** as the **Guest Operating System** and then select **CentOS 4/5/6 (32-bit)** from the **Version** drop-down list.



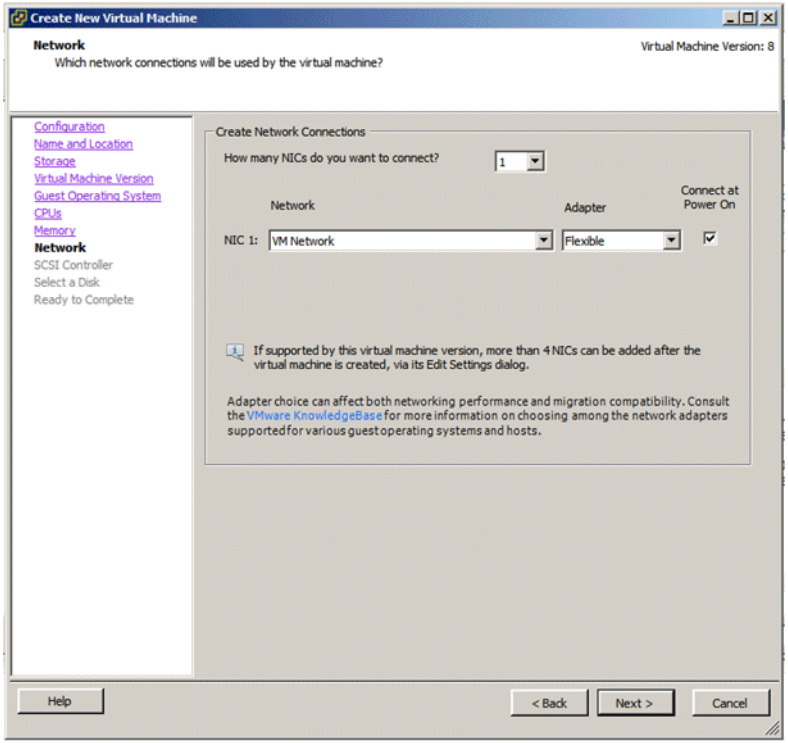
13. In the CPUs screen, specify the number of processors needed, and then click **Next**. The default values are typically adequate.



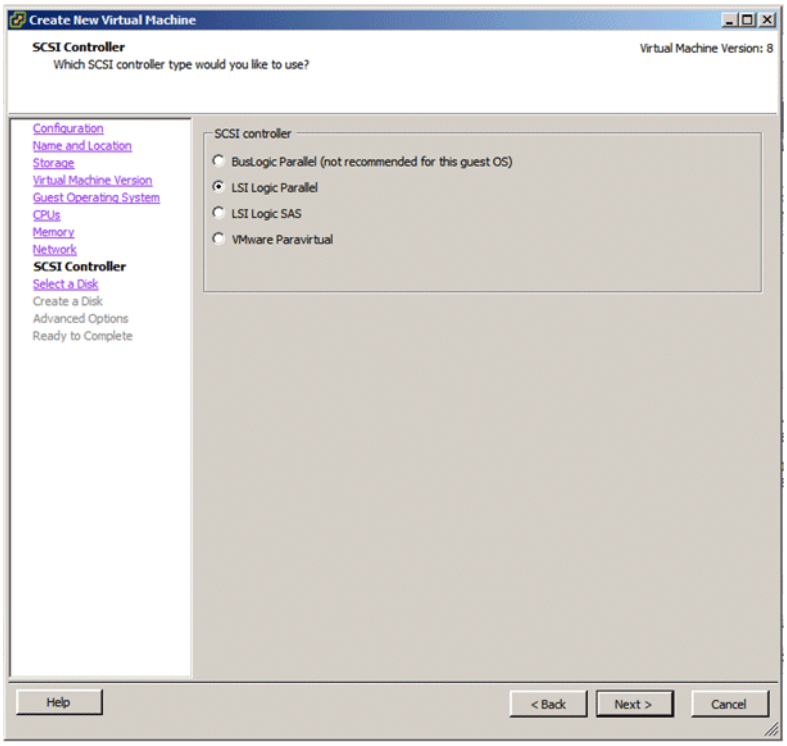
14. In the Memory screen, specify the amount of RAM needed, and then click **Next**. The default value of MB is typically adequate.



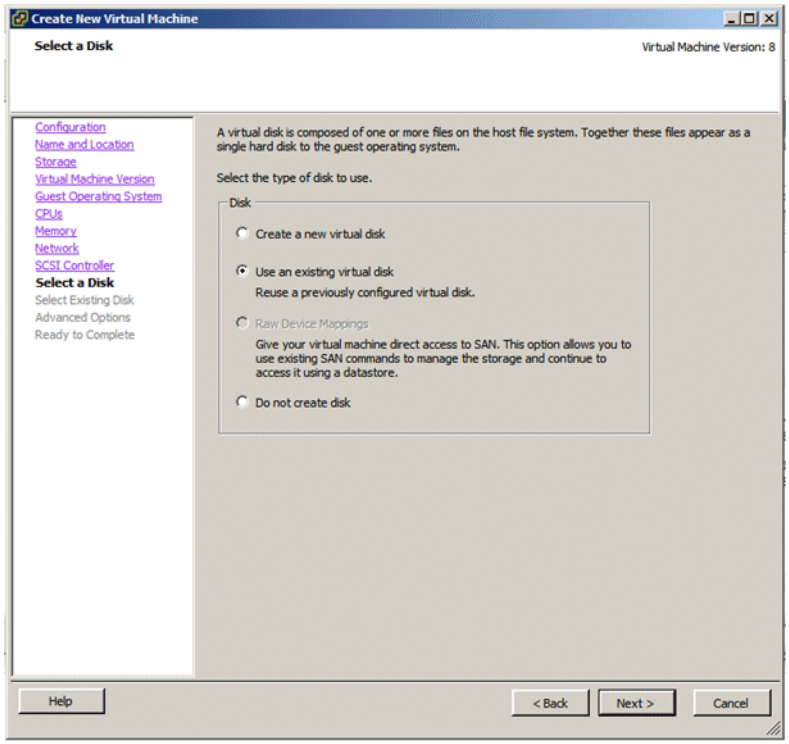
15. In the Network screen, specify the number of network adaptors needed., and then click **Next**. The default values are typically adequate.



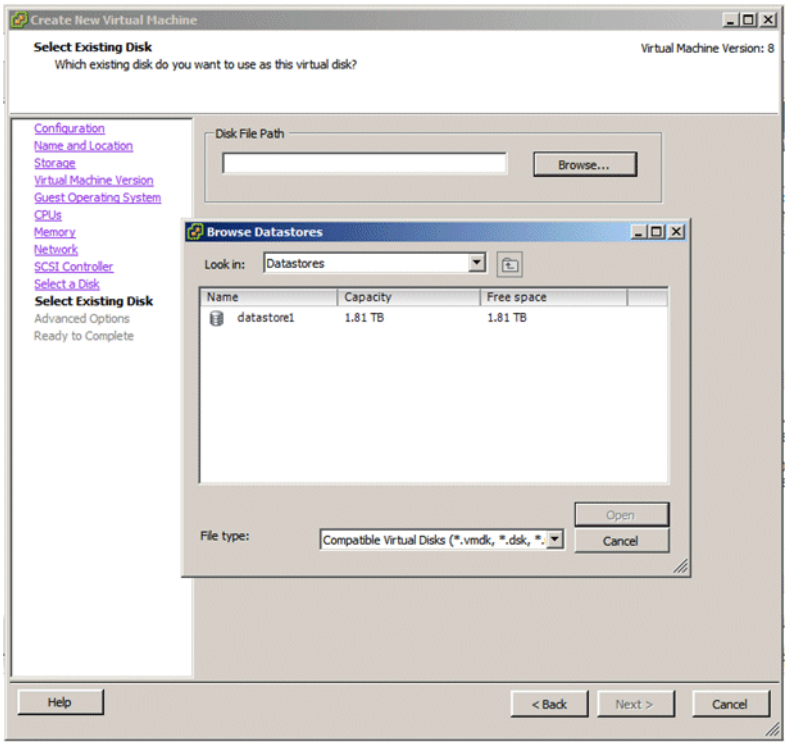
16. In the SCSI Controller screen, keep the default value, and then click **Next**.



17. In the Select a Disk screen, click **Use an existing virtual disk**, and then click **Next**.



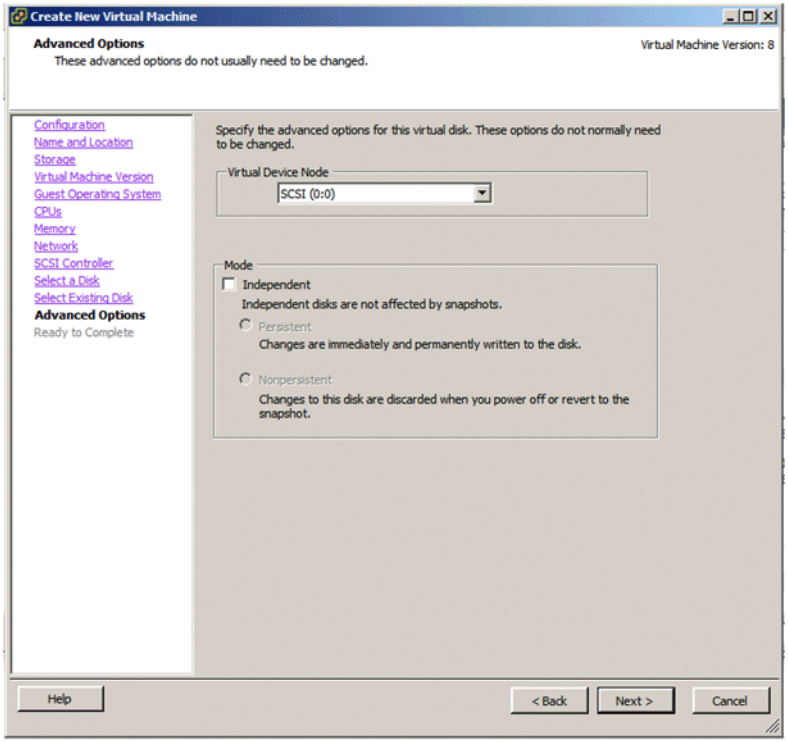
18. In the Select Existing Disk screen, browse to the location of the files that you uploaded to the datastore previously, and then click **Next**.



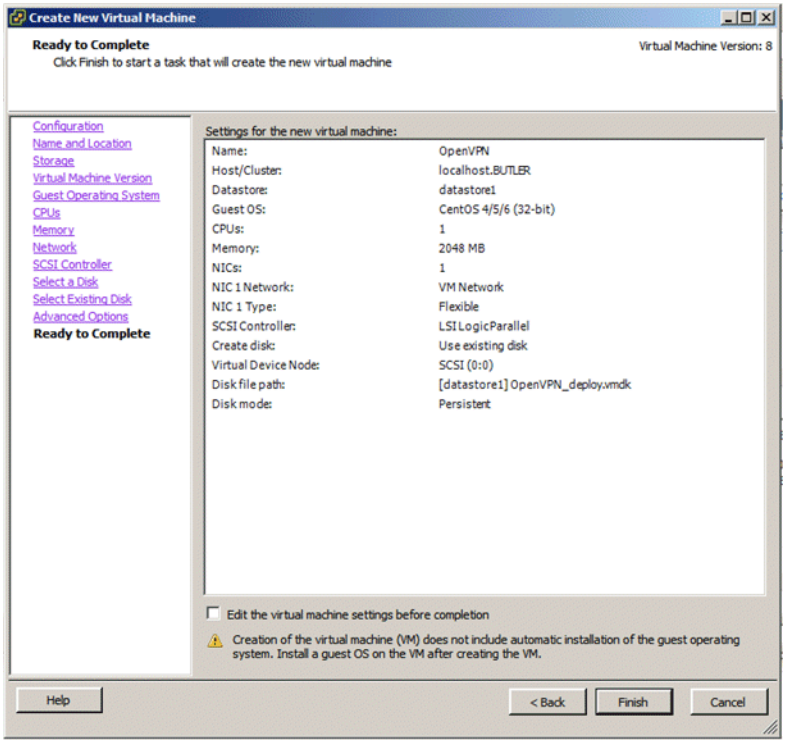
Double-click on the datastore, and then select the OpenVPN file and click **OK**.

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.



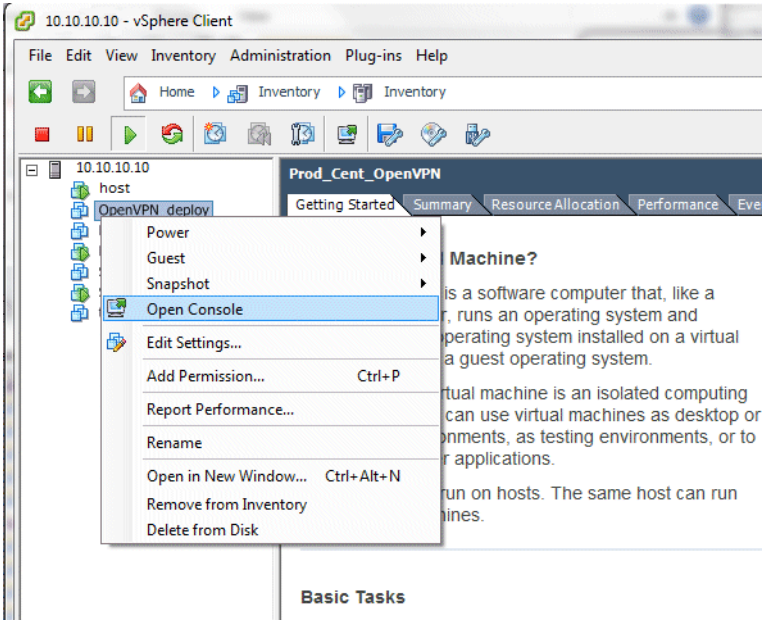
20. In the Ready to Complete screen, review your selections and then click **Finish**.



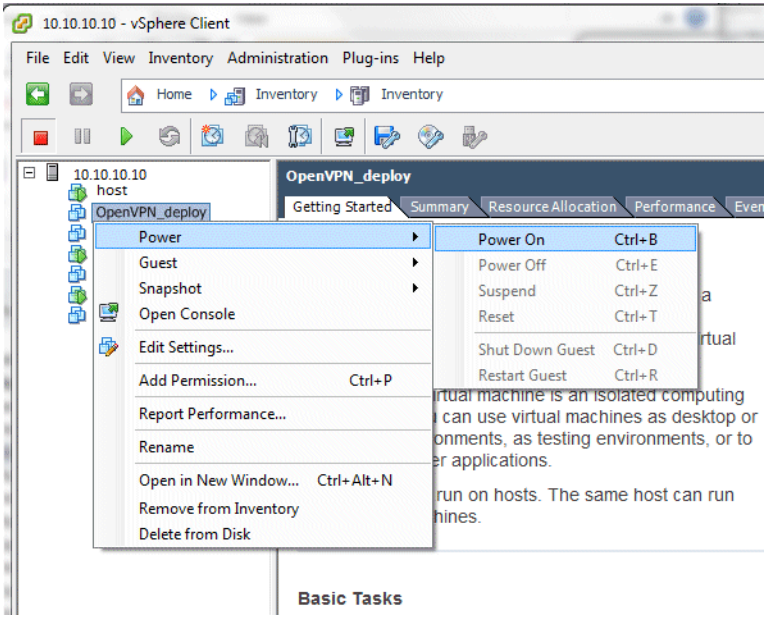
Logging in to the virtual machine

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**.

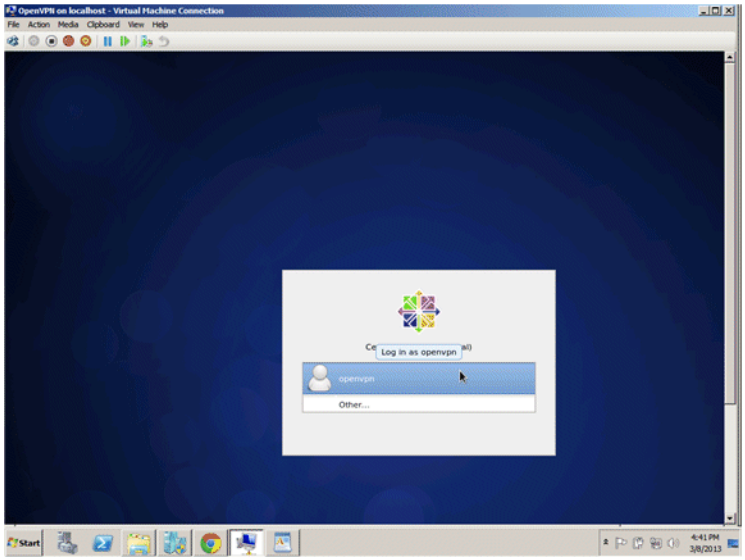


2. Right-click the OpenVPN Server virtual machine, and then choose **Power > Power On**.

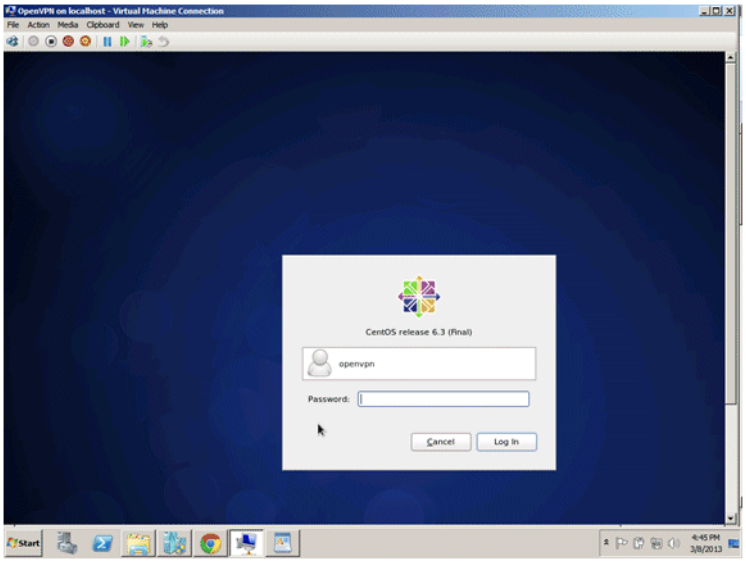


3. Right-click on the Virtual Machine and choose **Start**. Then choose **Connect** from the same right-click menu.

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



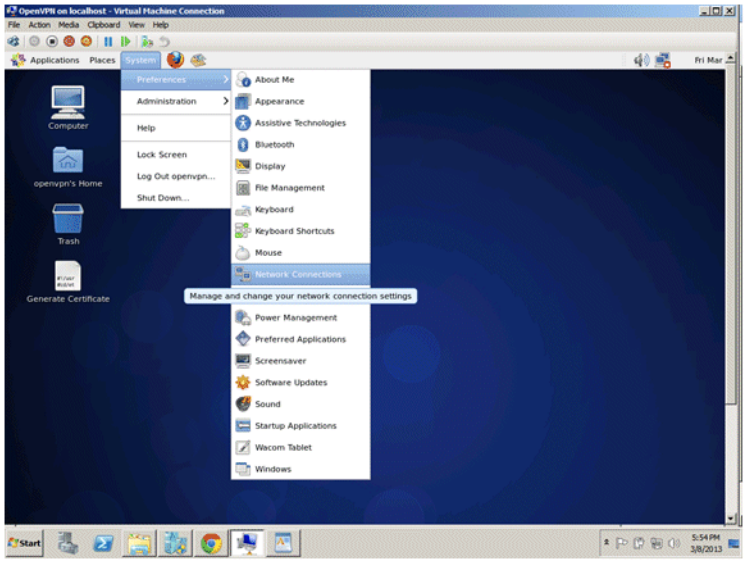
5. Enter the Vertical default password, **Vertical4VoIP!**. and then click **Log In**.



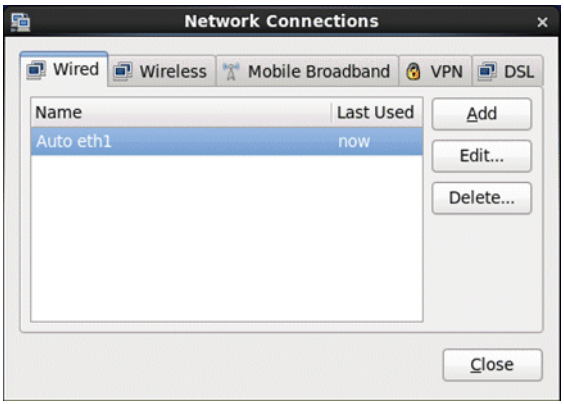
Changing network settings for your environment

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

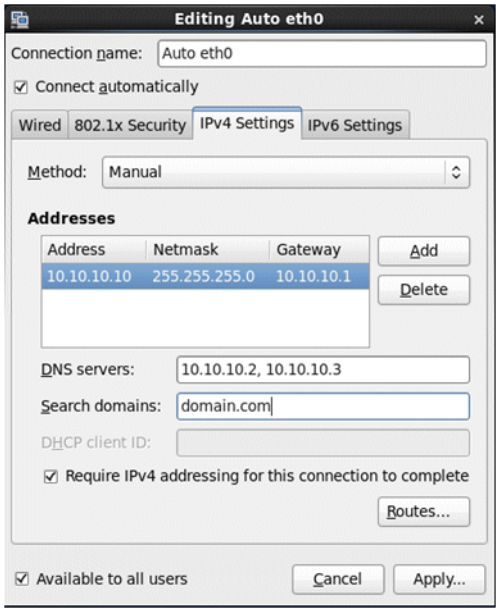
1. From the desktop, click **System > Preferences > Network Connections**.



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



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



- 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:

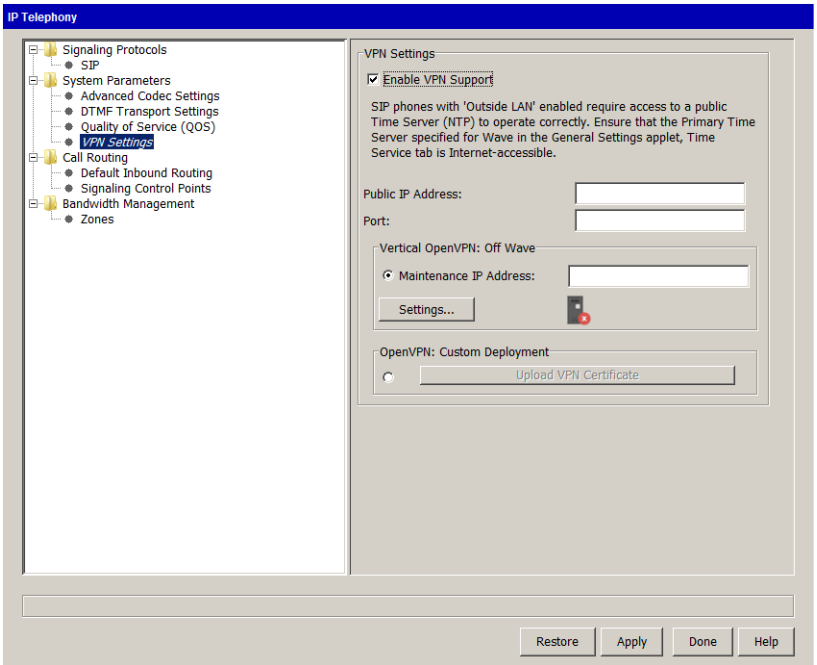
  IP Route 10.10.2.0 255.255.255.0 10.1.1.15

  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.



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

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.

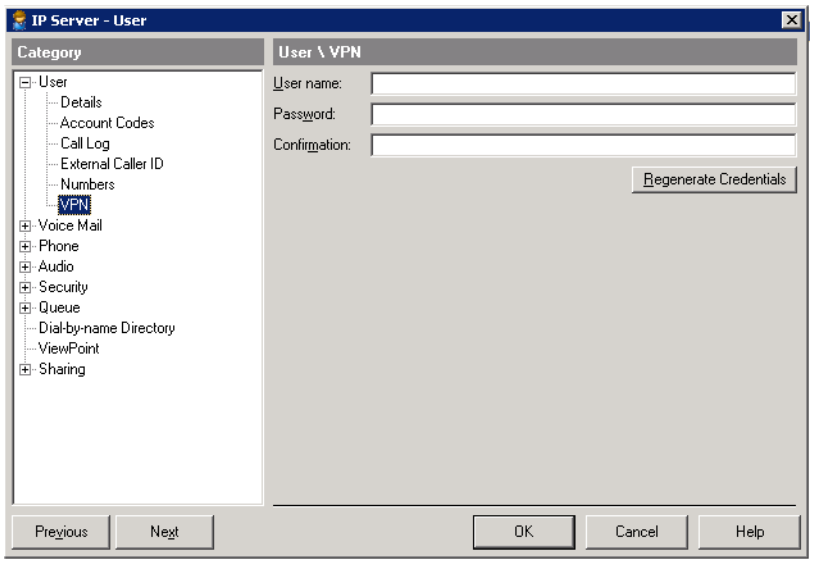
Specifying a user's VPN credentials

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.



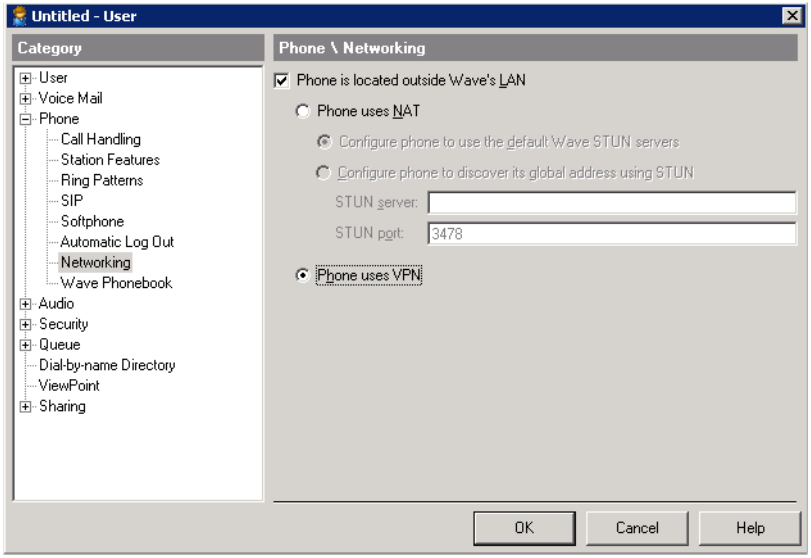
3. Do one of the following:
   - **In network:** Click **Regenerate Credentials** to generate the user's VPN credentials, which will be automatically downloaded to the user's ViewPoint Mobile Softphone and/or supported IP phone.
   - **Not in network:** Enter a **Username** and **Password** manually, 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.



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

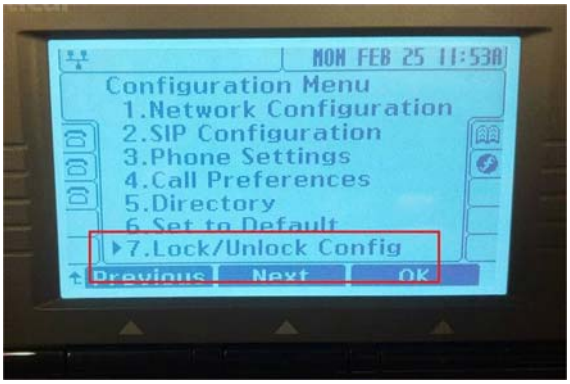
The information in this section applies to the supported phone models listed on page 1-1.

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.

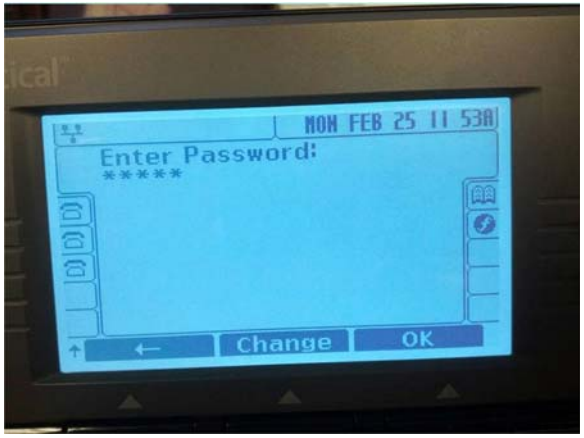
Important: Phones to be used with Wave OpenVPN Server must first be staged locally on a Wave Server running Wave 4.0. This will allow the 4.0 firmware that supports the latest VPN features to be downloaded to the phones, so that future firmware upgrades will be able to be downloaded via VPN itself.

1. On the phone, press the MENU key.

2. Scroll through the Configuration Menu and select **Lock/Unlock Config**.

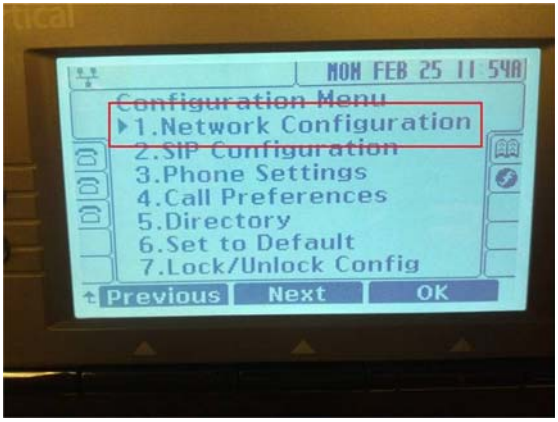


3. Enter the Configuration Menu password using the phone's keypad. This password protects some configuration options when changing them from the phone's keypad. The default password is 22222.

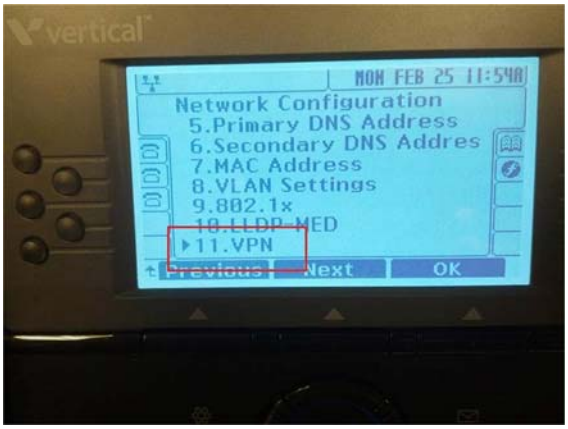


4. Press **OK** to return to the Configuration Menu.

5. Select **Network Configuration**.

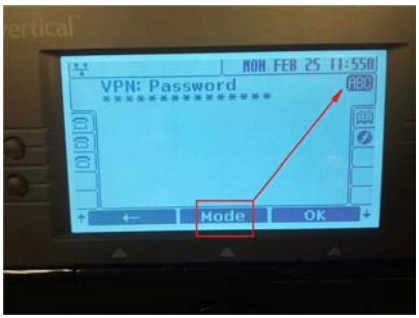


6. Select **VPN**.



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