Wave
OpenVPN Server
Guide

Release 4.0

March 2014

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

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

- **Updated step 6 in section “Editing your OpenVPN Network settings”** on page 2-32:

  6. To change the DNS server, find the following two lines:

  ```
  push “dhcp-option DNS 10.10.1.2”
  push “dhcp-option DNS 8.8.4.4”
  ```

  - Change “10.10.1.2” to the primary DNS server used by your local network.
  - Change “8.8.4.4” to the secondary DNS server on your local network.

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

For details on everything that’s new in Wave 4.0, see the *Wave 4.0 Release Notes*.

Contents

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 Wave Gigabit-E SIP 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.*

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.

Chapter 2

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™

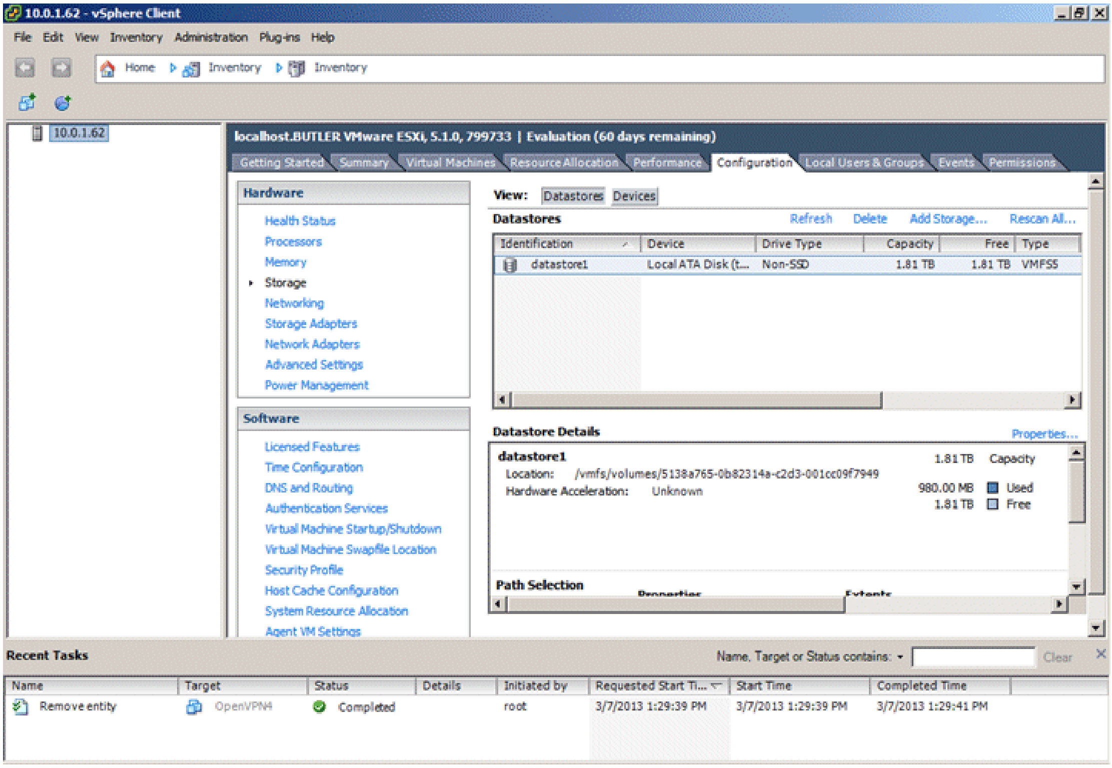
VMware vSphere Hypervisor is a free platform for running a virtual machine on an applications server. For more about Hypervisor, see:

```
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.


10.0.1.62 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.0.1.62
localhost.BUTLER VMware ESXi, 5.1.0, 799733 | Evaluation (60 days remaining)
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions
Hardware
Health Status
Processors
Memory
Storage
Networking
Storage Adapters
Network Adapters
Advanced Settings
Power Management
Software
Licensed Features
Time Configuration
DNS and Routing
Authentication Services
Virtual Machine Startup/Shutdown
Virtual Machine Swapfile Location
Security Profile
Host Cache Configuration
System Resource Allocation
Agent VM Settings
View: Datastores Devices
Datastores
Refresh Delete Add Storage... Rescan All...
Datastore Details
Properties...
Path Selection
Properties
Extents
Recent Tasks
Name, Target or Status contains:
Clear

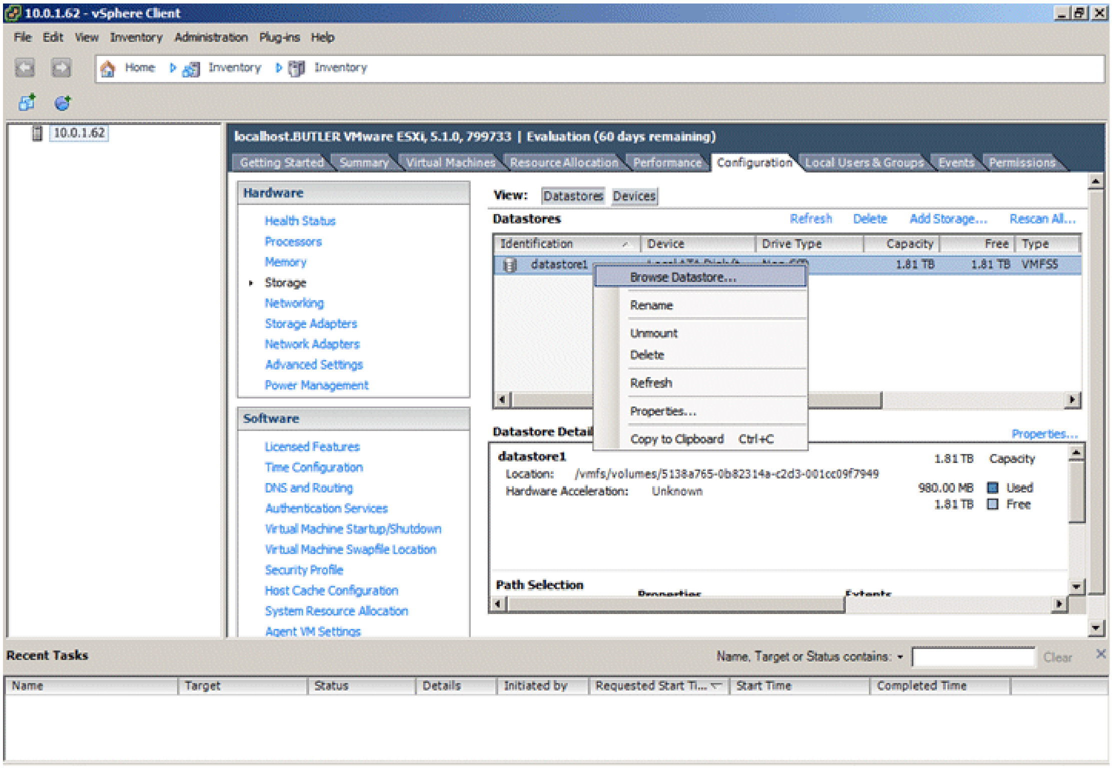
Identification	Device	Drive Type	Capacity	Free	Type
datastore1	Local ATA Disk (t...	Non-SSD	1.81 TB	1.81 TB	VMFS5

datastore1
Location: /vmfs/volumes/5138a765-0b82314a-c2d3-001cc09f7949
Hardware Acceleration: Unknown

1.81 TB Capacity
980.00 MB ■ Used
1.81 TB □ Free

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Remove entity	OpenVPN4	Completed		root	3/7/2013 1:29:39 PM	3/7/2013 1:29:39 PM	3/7/2013 1:29:41 PM

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



Identification	Device	Drive Type	Capacity	Free	Type
datastore1	Local ATA Disk (t...	Non-SSD	1.81 TB	1.81 TB	VMFS5

datastore1

Location: /vmfs/volumes/5138a765-0b82314a-c2d3-001cc09f7949

Hardware Acceleration: Unknown

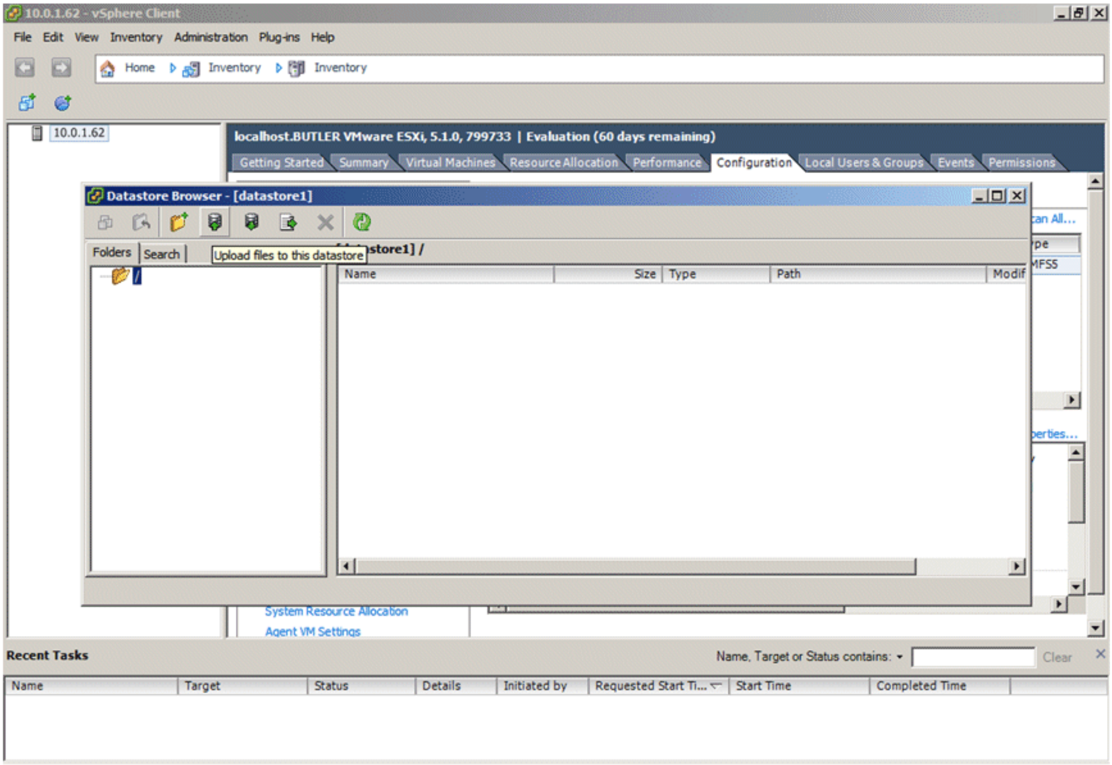
1.81 TB Capacity

980.00 MB ■ Used

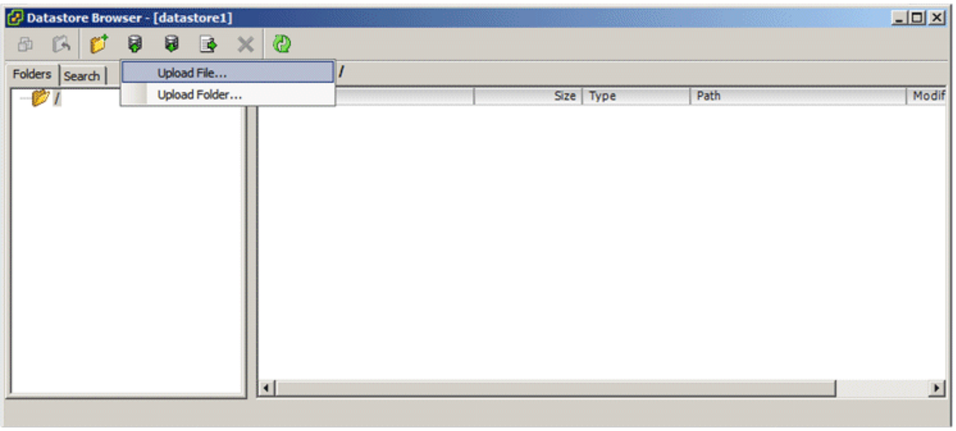
1.81 TB □ Free

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time

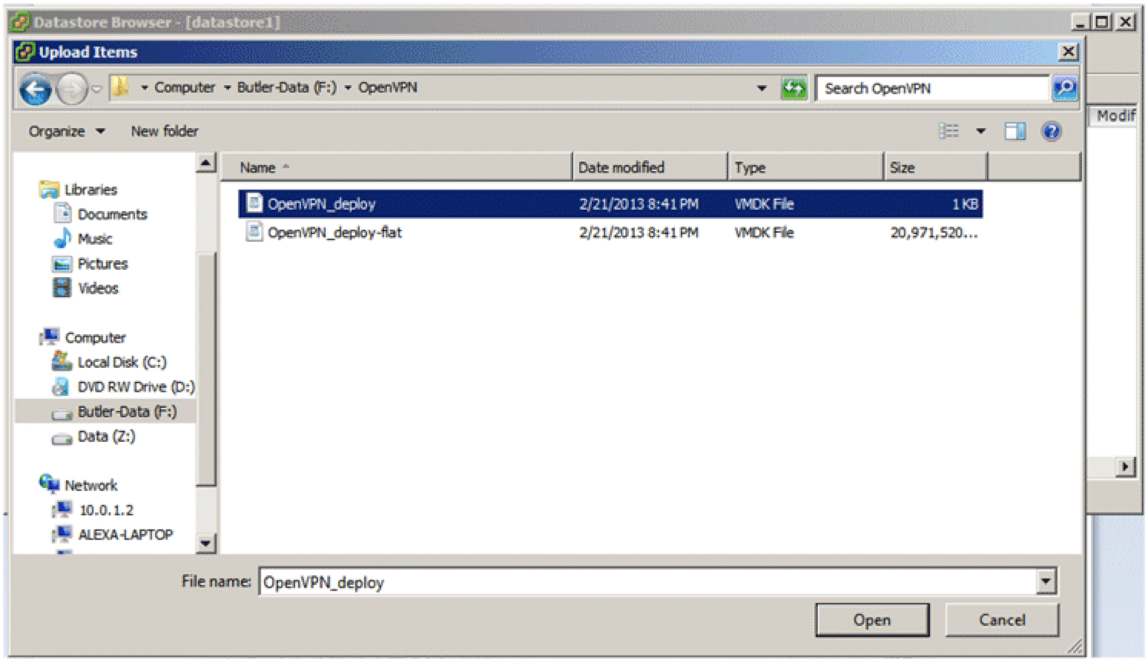
4. In the Datastore Browser, click the **Upload files to this datastore** button on the toolbar.


10.0.1.62 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.0.1.62
localhost.BUTLER VMware ESXi, 5.1.0, 799733 | Evaluation (60 days remaining)
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions
Datastore Browser - [datastore1]
Folders Search
Upload files to this datastore
store1] /
Name Size Type Path Modif
System Resource Allocation
Agent VM Settings
Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by Requested Start Ti... Start Time Completed Time

5. Click **Upload File**.



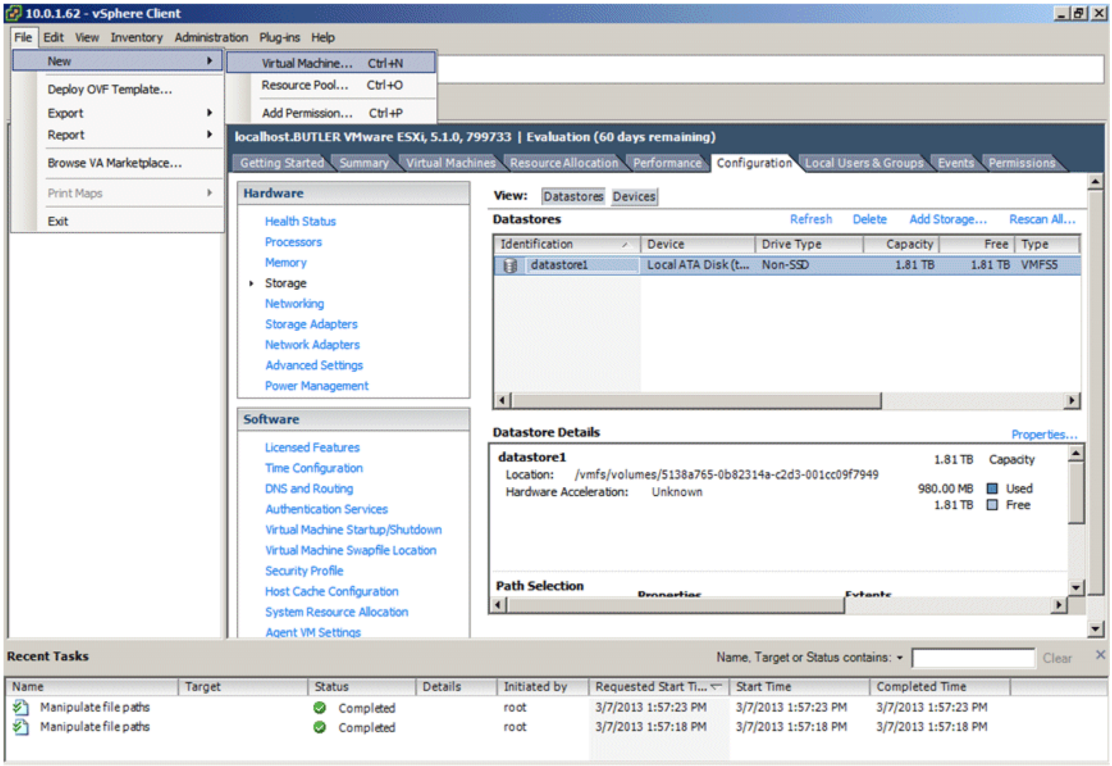
6. Select both files and then click **Open**.



Name	Date modified	Type	Size
OpenVPN_deploy	2/21/2013 8:41 PM	VMDK File	1 KB
OpenVPN_deploy-flat	2/21/2013 8:41 PM	VMDK File	20,971,520...

File name: OpenVPN_deploy

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



Identification	Device	Drive Type	Capacity	Free	Type
datastore1	Local ATA Disk (t...	Non-SSD	1.81 TB	1.81 TB	VMFS5

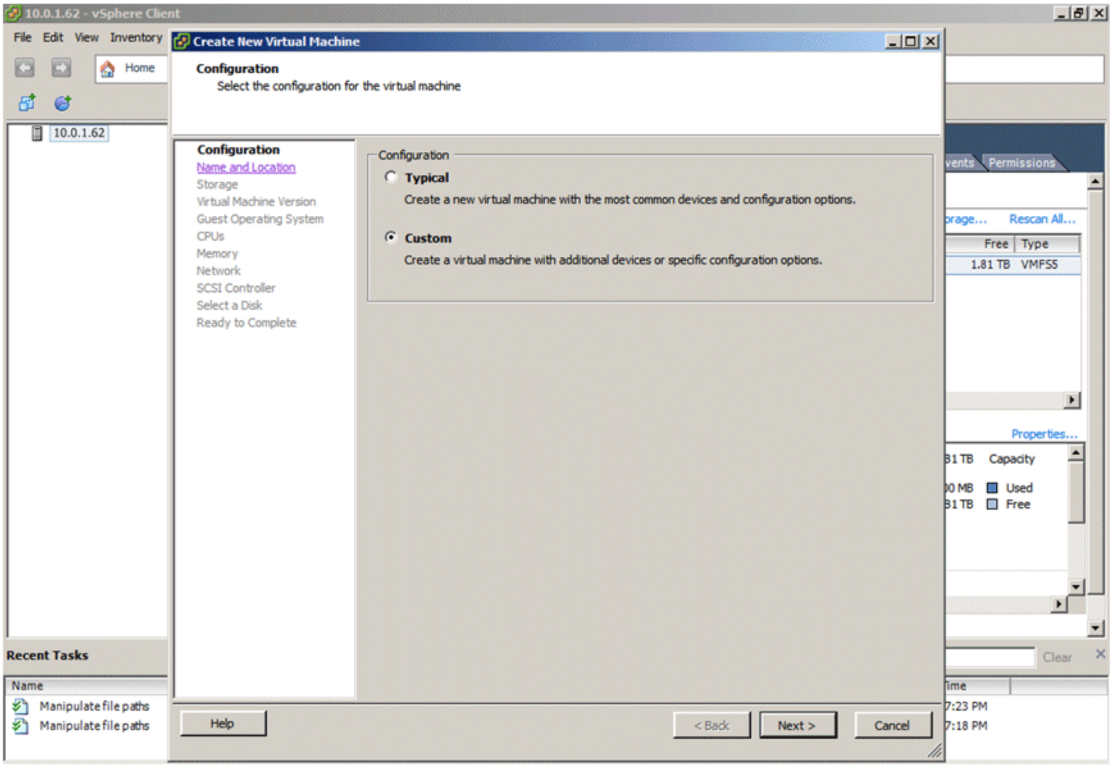
datastore1
Location: /vmfs/volumes/5138a765-0b82314a-c2d3-001cc09f7949
Hardware Acceleration: Unknown

1.81 TB	Capacity
980.00 MB	■ Used
1.81 TB	□ Free

Name	Target	Status	Details	Initiated by	Requested 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

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.



Configuration

Select the configuration for the virtual machine

Configuration

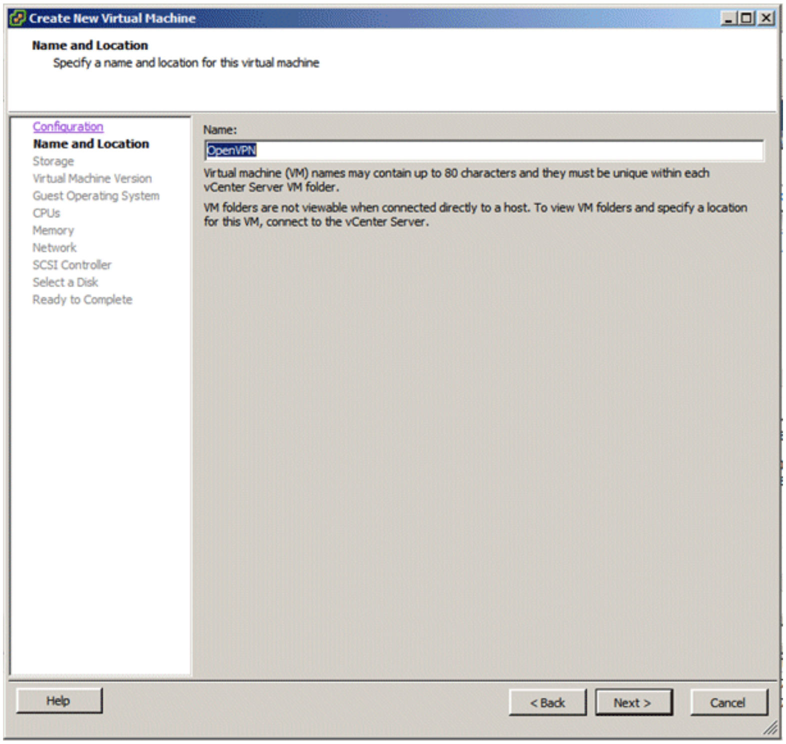
○ **Typical**

Create a new virtual machine with the most common devices and configuration options.

● **Custom**

Create a virtual machine with additional devices or specific configuration options.

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

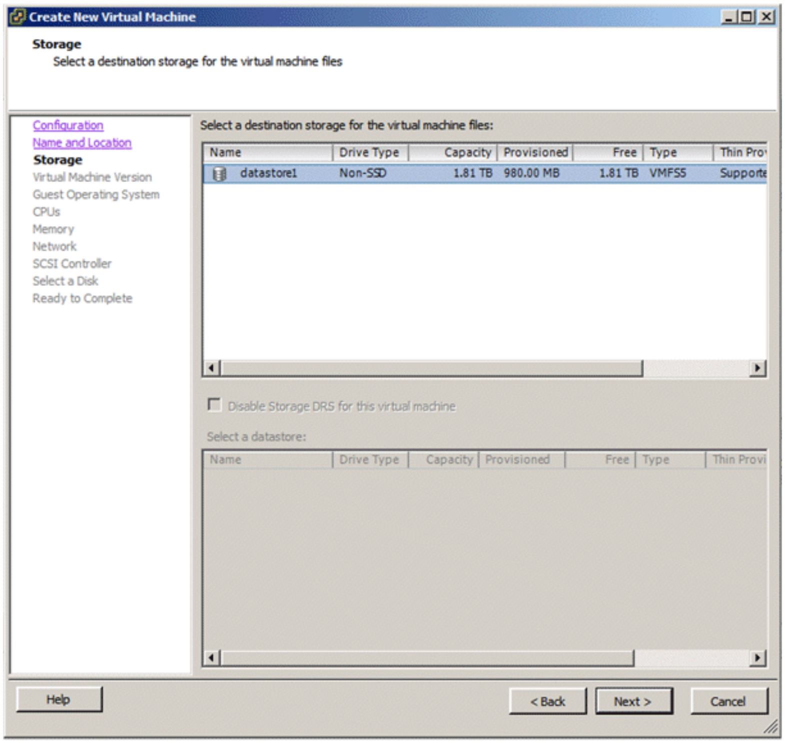


Name: OpenVPN

Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.

VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.

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.



Create New Virtual Machine

Storage

Select a destination storage for the virtual machine files

Select a destination storage for the virtual machine files:

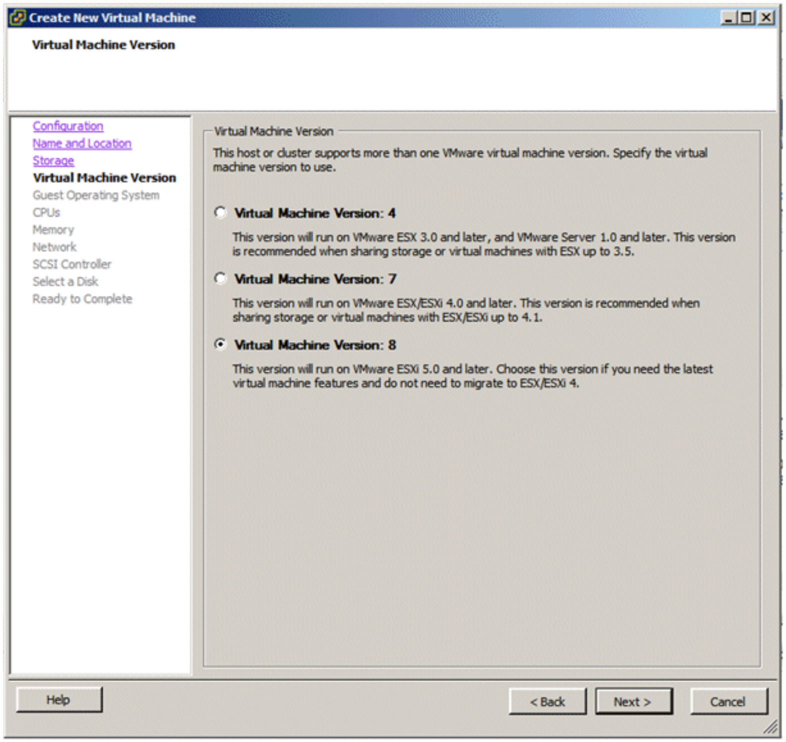
Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1	Non-SSD	1.81 TB	980.00 MB	1.81 TB	VMFS5	Supporte

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi

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



Virtual Machine Version

Virtual Machine Version

This host or cluster supports more than one VMware virtual machine version. Specify the virtual machine version to use.

○ **Virtual Machine Version: 4**

This version will run on VMware ESX 3.0 and later, and VMware Server 1.0 and later. This version is recommended when sharing storage or virtual machines with ESX up to 3.5.

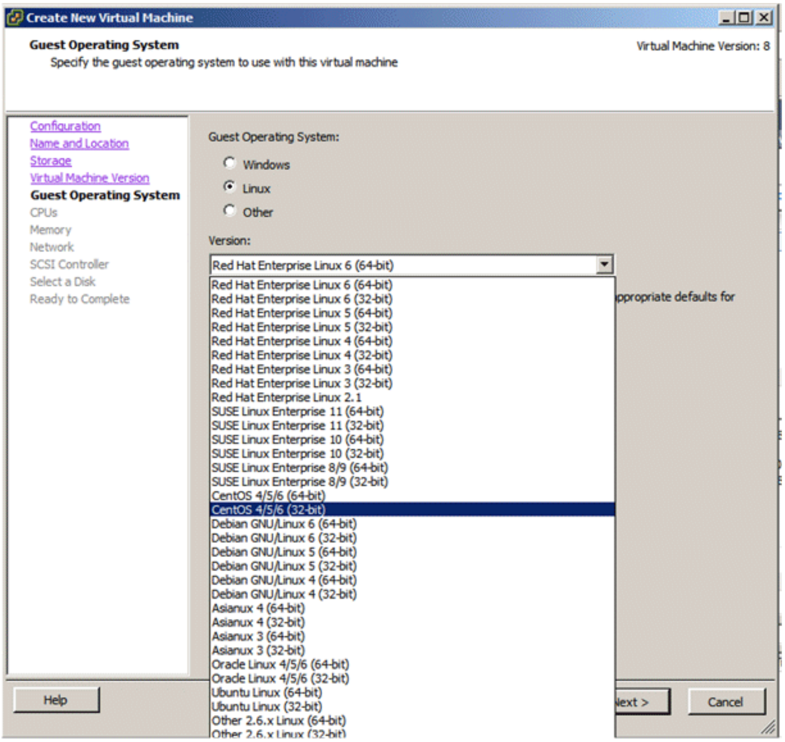
○ **Virtual Machine Version: 7**

This version will run on VMware ESX/ESXi 4.0 and later. This version is recommended when sharing storage or virtual machines with ESX/ESXi up to 4.1.

● **Virtual Machine Version: 8**

This version will run on VMware ESXi 5.0 and later. Choose this version if you need the latest virtual machine features and do not need to migrate to ESX/ESXi 4.

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
Specify the guest operating system to use with this virtual machine

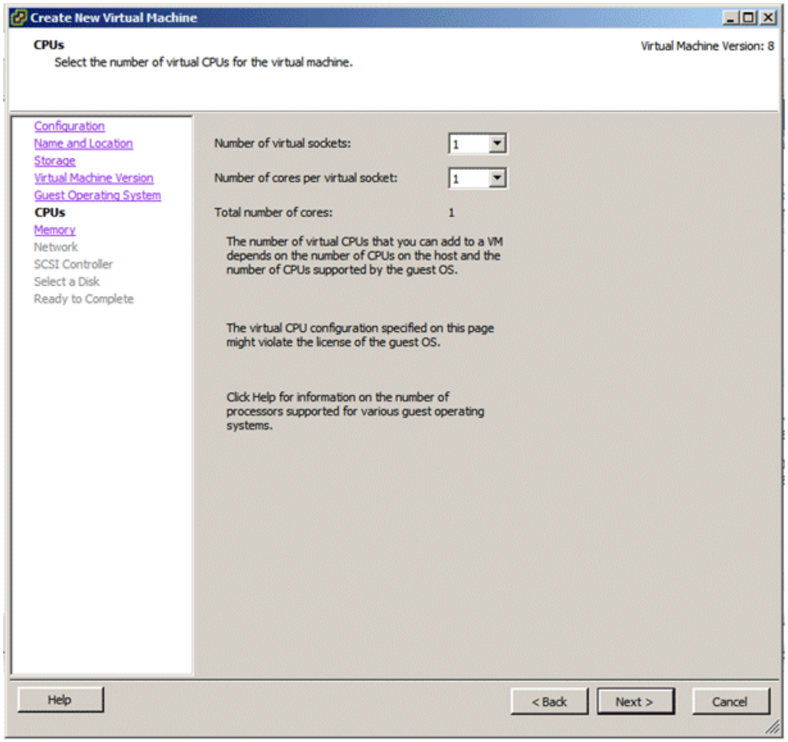
Virtual Machine Version: 8

Guest Operating System:
○ Windows
● Linux
○ Other

Version:
Red Hat Enterprise Linux 6 (64-bit)

Configuration
Name and Location
Storage
Virtual Machine Version
Guest Operating System
CPUs
Memory
Network
SCSI Controller
Select a Disk
Ready to Complete
Red Hat Enterprise Linux 6 (64-bit)
Red Hat Enterprise Linux 6 (32-bit)
Red Hat Enterprise Linux 5 (64-bit)
Red Hat Enterprise Linux 5 (32-bit)
Red Hat Enterprise Linux 4 (64-bit)
Red Hat Enterprise Linux 4 (32-bit)
Red Hat Enterprise Linux 3 (64-bit)
Red Hat Enterprise Linux 3 (32-bit)
Red Hat Enterprise Linux 2.1
SUSE Linux Enterprise 11 (64-bit)
SUSE Linux Enterprise 11 (32-bit)
SUSE Linux Enterprise 10 (64-bit)
SUSE Linux Enterprise 10 (32-bit)
SUSE Linux Enterprise 8/9 (64-bit)
SUSE Linux Enterprise 8/9 (32-bit)
CentOS 4/5/6 (64-bit)
CentOS 4/5/6 (32-bit)
Debian GNU/Linux 6 (64-bit)
Debian GNU/Linux 6 (32-bit)
Debian GNU/Linux 5 (64-bit)
Debian GNU/Linux 5 (32-bit)
Debian GNU/Linux 4 (64-bit)
Debian GNU/Linux 4 (32-bit)
Asianux 4 (64-bit)
Asianux 4 (32-bit)
Asianux 3 (64-bit)
Asianux 3 (32-bit)
Oracle Linux 4/5/6 (64-bit)
Oracle Linux 4/5/6 (32-bit)
Ubuntu Linux (64-bit)
Ubuntu Linux (32-bit)
Other 2.6.x Linux (64-bit)
Other 2.6.x Linux (32-bit)
ppropriate defaults for
Help
lext >
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 Machine

CPUs
Select the number of virtual CPUs for the virtual machine.

Virtual Machine Version: 8

Number of virtual sockets: 1

Number of cores per virtual socket: 1

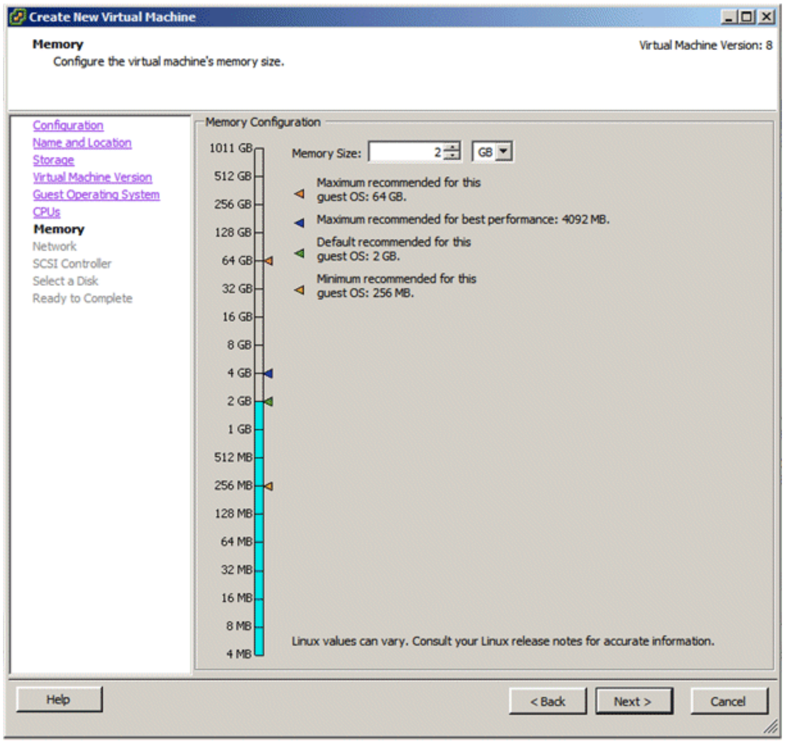
Total number of cores: 1

The number of virtual CPUs that you can add to a VM depends on the number of CPUs on the host and the number of CPUs supported by the guest OS.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

Click Help for information on the number of processors supported for various guest operating systems.

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



Memory
Configure the virtual machine's memory size.

Virtual Machine Version: 8

Memory Configuration

Memory Size: 2 GB

Maximum recommended for this guest OS: 64 GB.

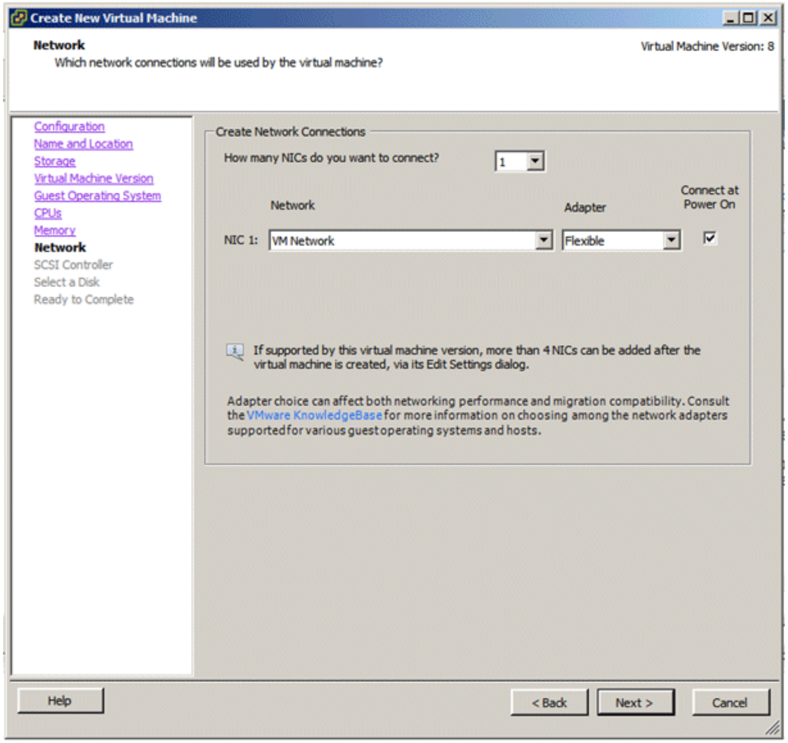
Maximum recommended for best performance: 4092 MB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 256 MB.

Linux values can vary. Consult your Linux release notes for accurate information.

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



Network
Which network connections will be used by the virtual machine?

Virtual Machine Version: 8

Create Network Connections

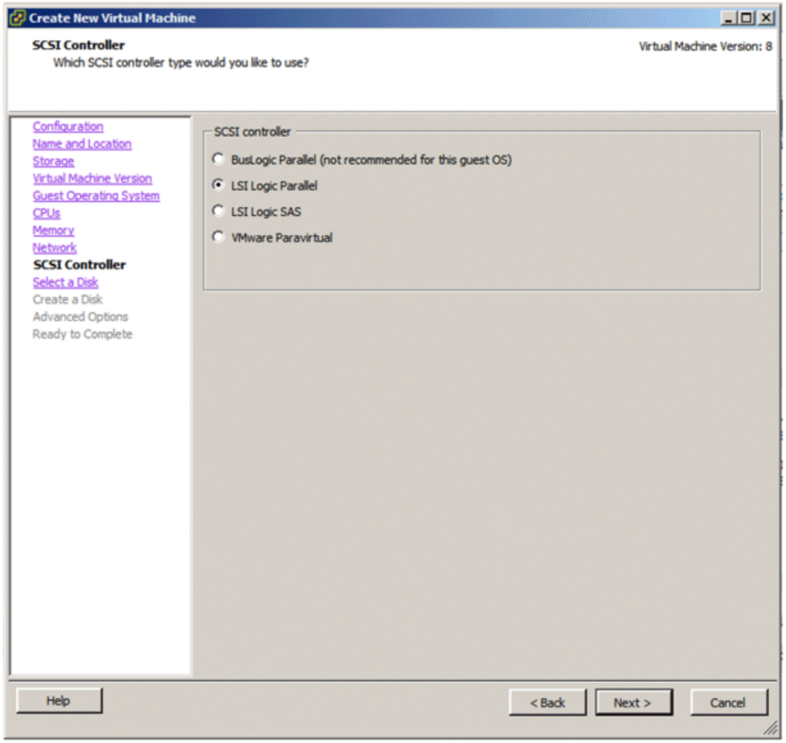
How many NICs do you want to connect? 1

	Network	Adapter	Connect at Power On
NIC 1:	VM Network	Flexible	☑

If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supportedfor various guestoperating systems and hosts.

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



SCSI Controller

Which SCSI controller type would you like to use?

Virtual Machine Version: 8

SCSI controller

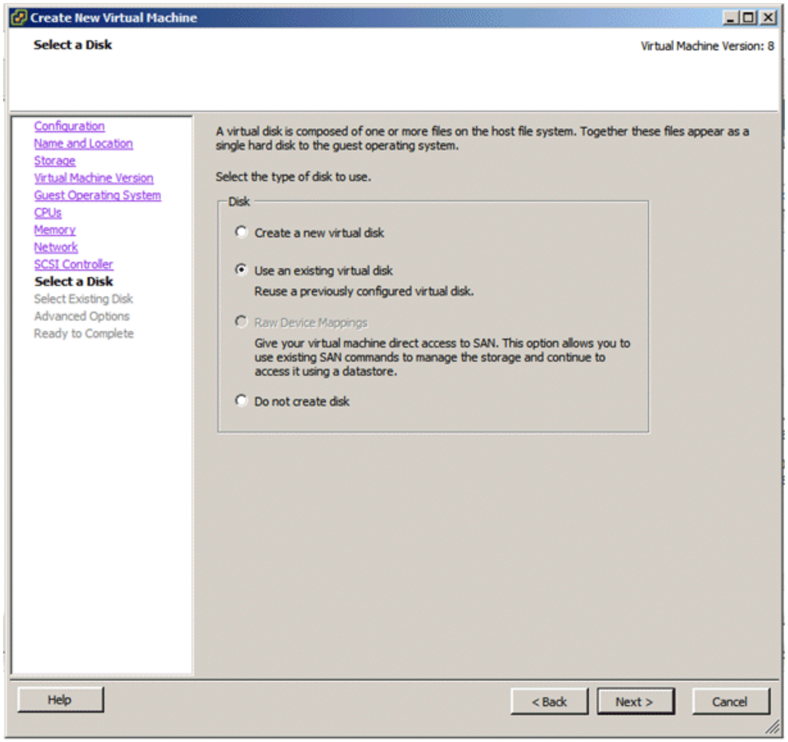
○ BusLogic Parallel (not recommended for this guest OS)

● LSI Logic Parallel

○ LSI Logic SAS

○ VMware Paravirtual

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



Create New Virtual Machine

Select a Disk

Virtual Machine Version: 8

A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

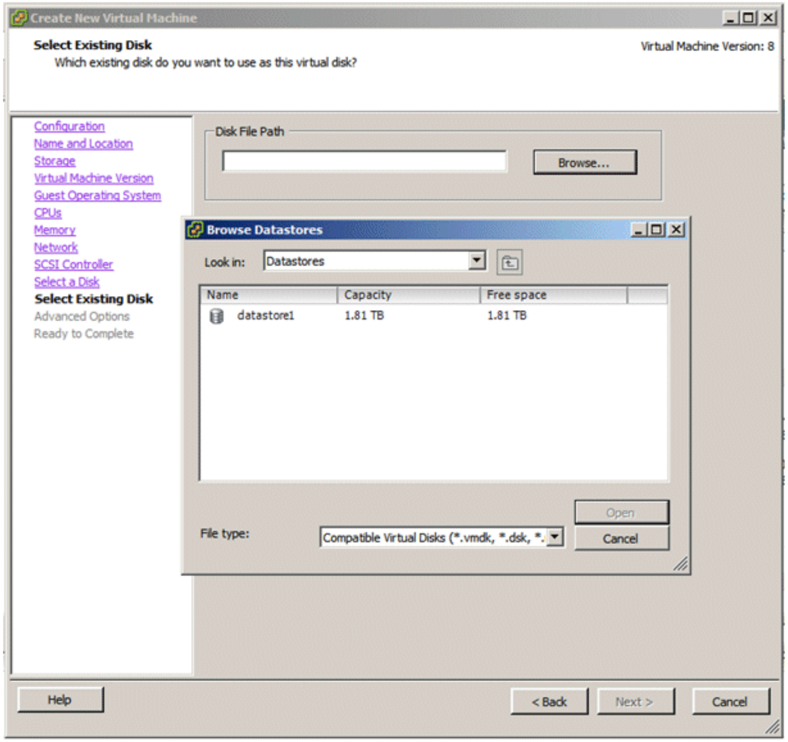
○ Create a new virtual disk

● Use an existing virtual disk
Reuse a previously configured virtual disk.

○ Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

○ Do not create disk

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**.



Select Existing Disk
Which existing disk do you want to use as this virtual disk?

Virtual Machine Version: 8

Disk File Path

Look in: Datastores

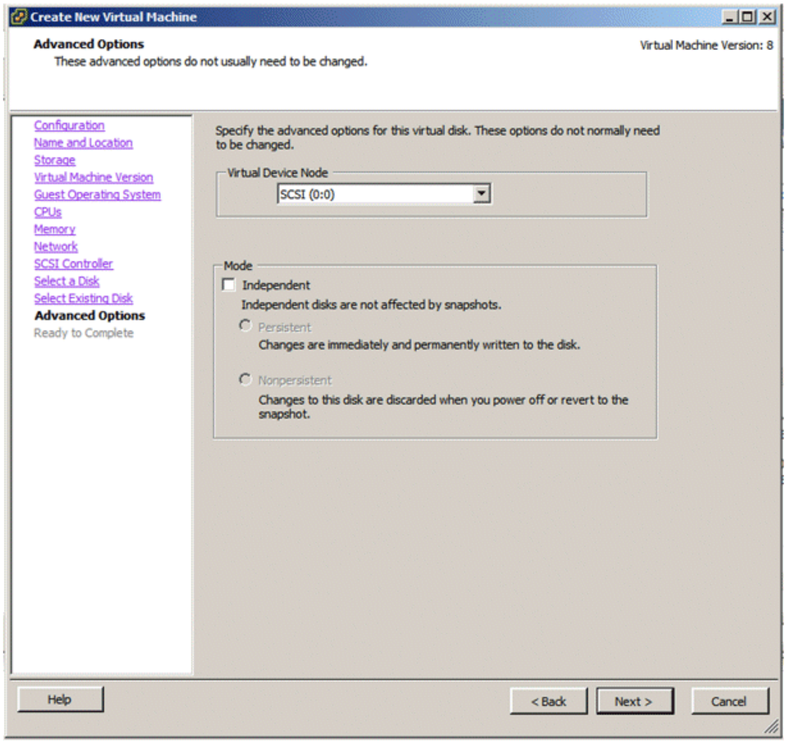
Name	Capacity	Free space
datastore1	1.81 TB	1.81 TB

File type: Compatible Virtual Disks (*.vmdk, *.dsk, *.

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.



Advanced Options

These advanced options do not usually need to be changed.

Virtual Machine Version: 8

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node: SCSI (0:0)

Mode

□ Independent

Independent disks are not affected by snapshots.

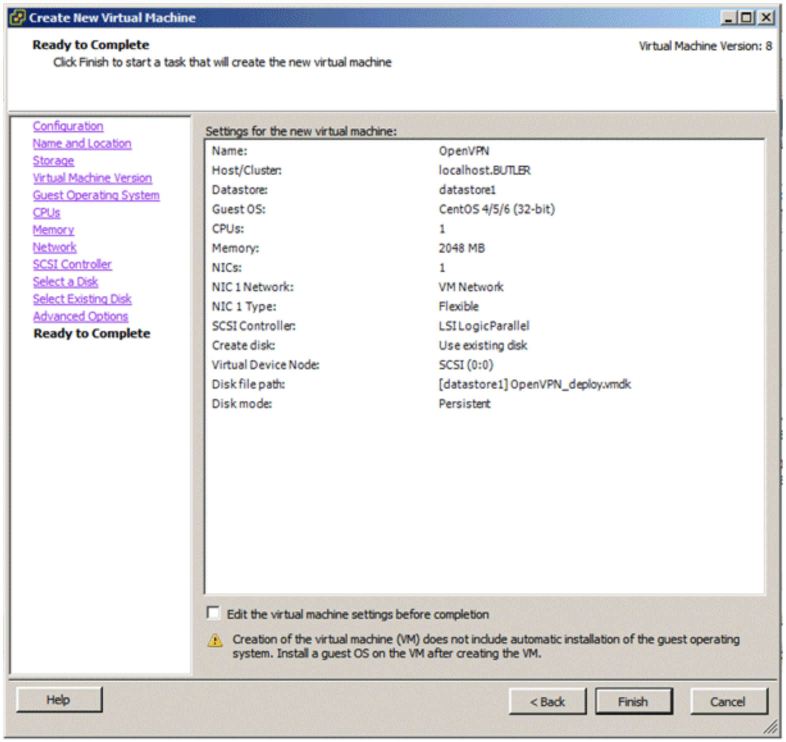
○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

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



Ready to Complete
Click Finish to start a task that will create the new virtual machine

Virtual Machine Version: 8

Settings for the new virtual machine:

Name:	OpenVPN
Host/Cluster:	localhost.BUTLER
Datastore:	datastore1
Guest OS:	CentOS 4/5/6 (32-bit)
CPUs:	1
Memory:	2048 MB
NICs:	1
NIC 1 Network:	VM Network
NIC 1 Type:	Flexible
SCSI Controller:	LSI LogicParallel
Create disk:	Use existing disk
Virtual Device Node:	SCSI (0:0)
Disk file path:	[datastore1] OpenVPN_deploy.vmdk
Disk mode:	Persistent

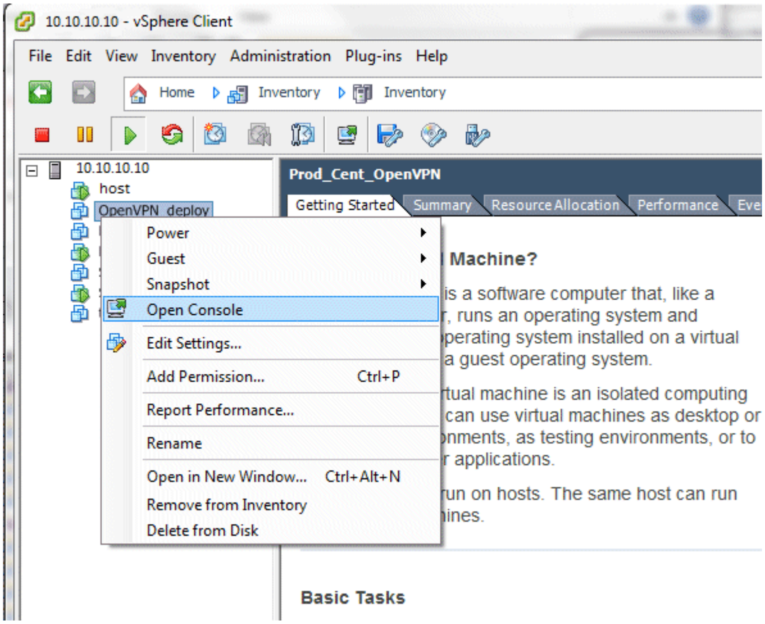
☐ Edit the virtual machine settings before completion

⚠ Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.

Logging in to the virtual machine and changing passwords

The following steps describe how to log into the OpenVPN Server virtual machine and change the root and OpenVPN passwords.

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

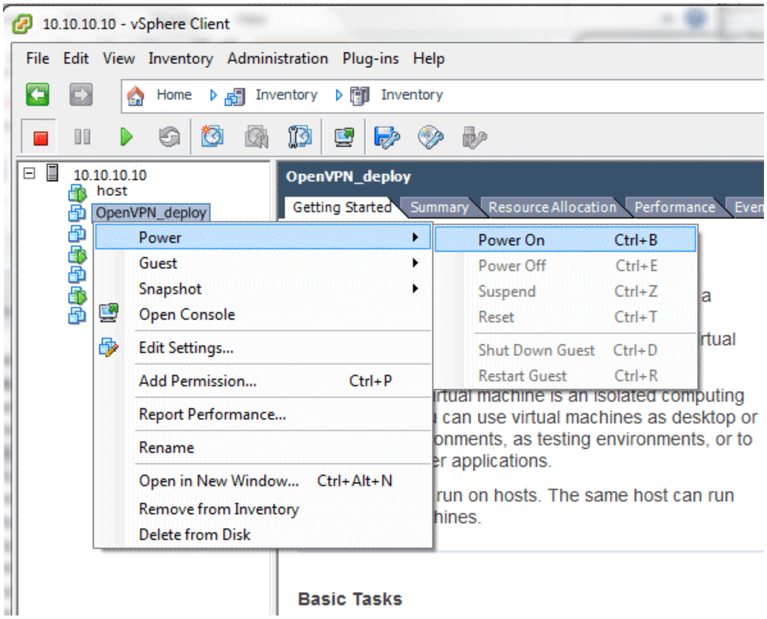


is a software computer that, like a
r, runs an operating system and
perating system installed on a virtual
a guest operating system.

tual machine is an isolated computing
can use virtual machines as desktop or
nments, as testing environments, or to
r applications.

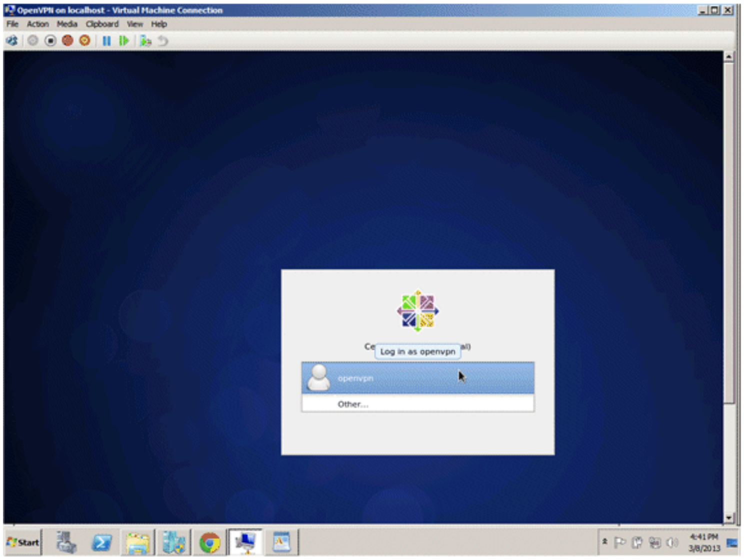
un on hosts. The same host can run
ines.

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

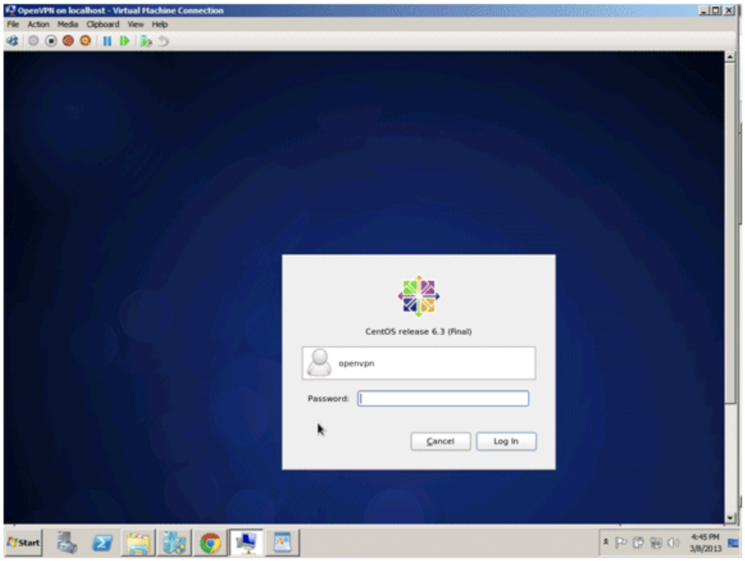


3. Right-click on the Virtual Machine and choose **Start**. Then choose **Connect** from the same right-click menu.

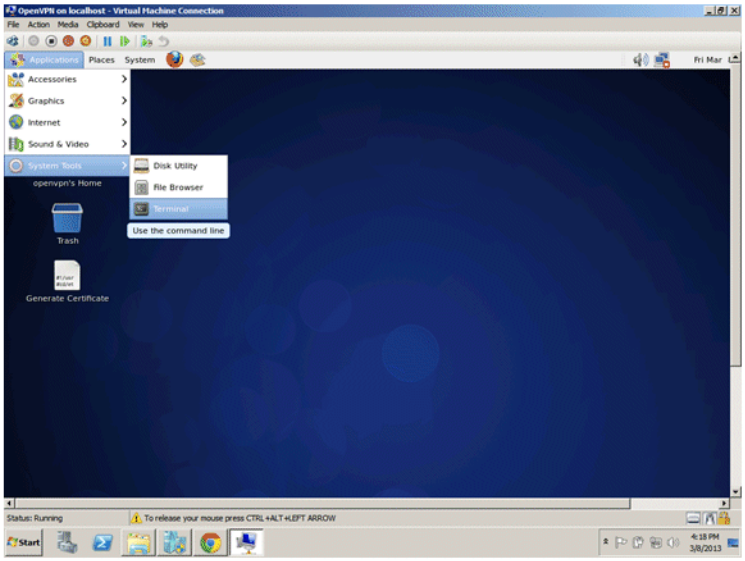
4. Double-click on the **openVPN** user.


OpenVPN on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Log in as openvpn
openvpn
Other...
Start
4:41 PM
3/8/2013

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


OpenVPN on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
CentOS release 6.3 (Final)
openvpn
Password:
Cancel
Log In
Start
4:45 PM
3/8/2013

6. To open a terminal, click **Applications > System Tools > Terminal**.



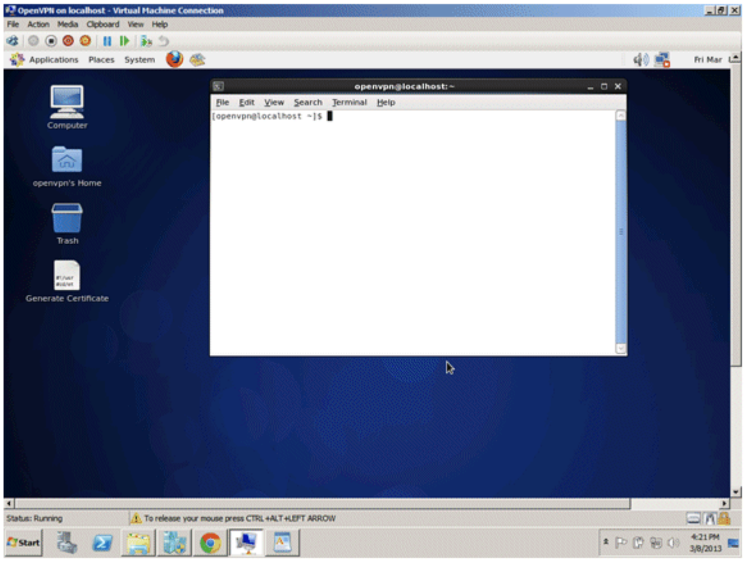
7. To change the OpenVPN password:

   a. Type `passwd` and press **Enter**.

   b. Enter the new password

   c. Enter the new password again to confirm it.

8. To elevate your privileges to a super user, type `SU` and press **Enter**.


OpenVPN on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places System
Fri Mar
Computer
openvpn's Home
Trash
Generate Certificate
openvpn@localhost:~
File Edit View Search Terminal Help
Status: Running
To release your mouse press CTRL+ALT+LEFT ARROW
Start
4:21 PM
3/8/2013

```
[openvpn@localhost ~]$
```

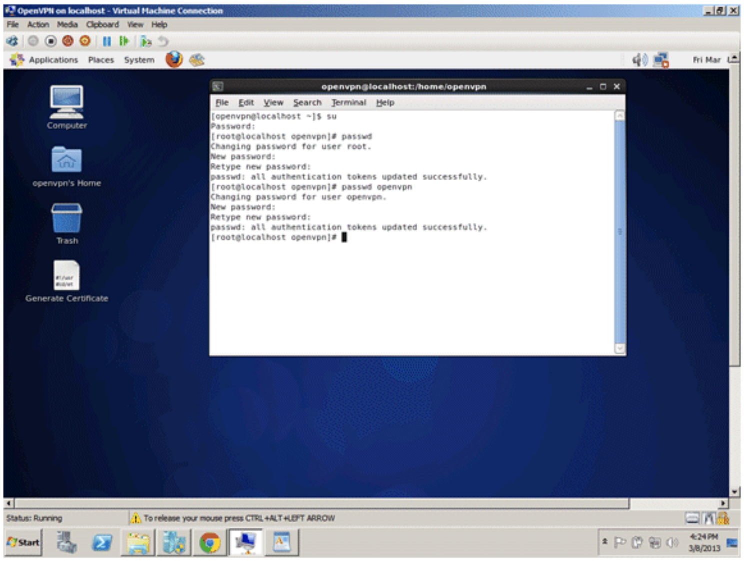
When you are prompted, enter the password **Vertical4VoIP!**.

9. To change the root password:

   a. Type `passwd` and press **Enter**.

   b. Enter the new password.

   c. Enter the new password again to confirm it.

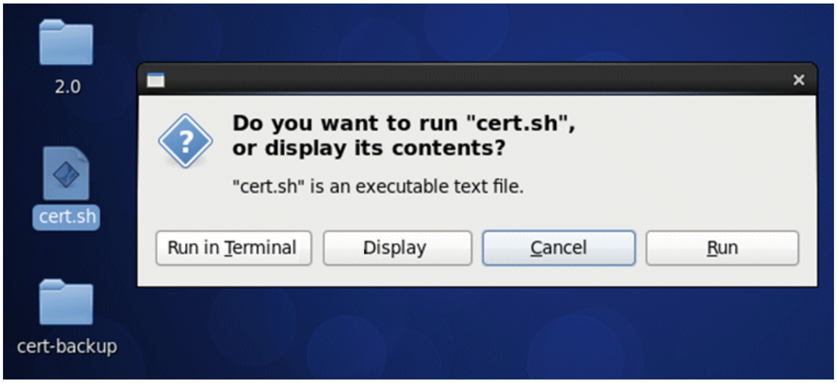

OpenVPN on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places System
Fri Mar
Computer
openvpn's Home
Trash
Generate Certificate
openvpn@localhost:/home/openvpn
File Edit View Search Terminal Help
Status: Running
To release your mouse press CTRL+ALT+LEFT ARROW
Start
4:24 PM
3/8/2013

```
[openvpn@localhost ~]$ su
Password:
[root@localhost openvpn]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost openvpn]# passwd openvpn
Changing password for user openvpn.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost openvpn]# █
```

Generating the certificate

When you generate the OpenVPN server according to following steps, you create a certificate good for 10 years. After 10 years, the certificates will expire, and you will need to renew the certification manually.

1. On the desktop, double click **cert.sh**.
2. When prompted, click **Run in Terminal**.



Do you want to run "cert.sh", or display its contents?

"cert.sh" is an executable text file.

3. The process will pause so that you can enter information to be incorporated into the certificate request. Each of the following fields appears—you can enter your company data in any field, press **Enter** to use the default value displayed in brackets, or type a period (.) and press **Enter** to leave the field blank.

Note: These fields are informational and do not impact operation of the system.

Country Name: Enter a value or accept the default.

State or Province Name: Enter a value or accept the default

Locality Name: Enter a value or accept the default.

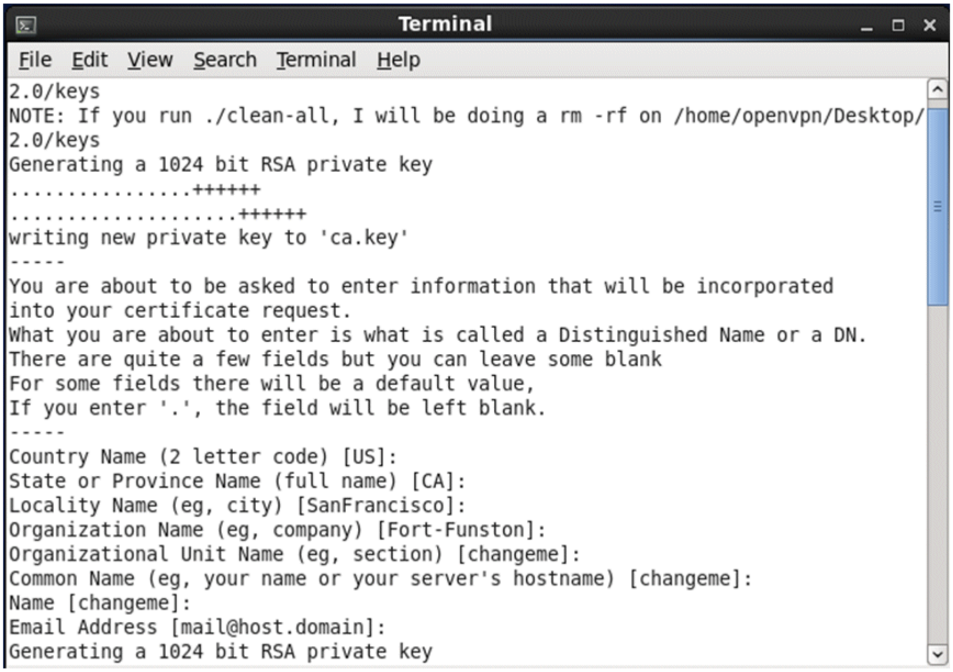
Organization Name: Enter a value or accept the default.

Organization Unit Name: Enter a value or accept the default.

Common Name: Enter your server hostname.

Name: Enter a value or accept the default.

Email Address: Enter a value or accept the default.



```
2.0/keys
NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/openvpn/Desktop/
2.0/keys
Generating a 1024 bit RSA private key
................++++++
....................++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:
Name [changeme]:
Email Address [mail@host.domain]:
Generating a 1024 bit RSA private key
```

4. Respond to the final prompts:

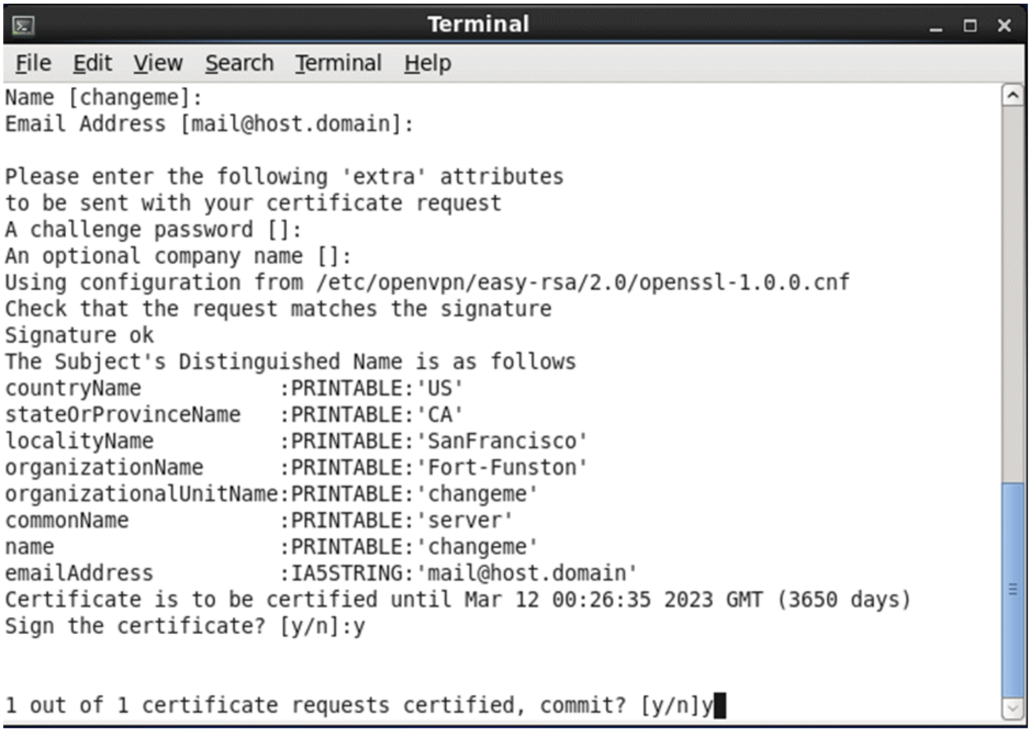
   Common Name: Enter `server`.

   A challenge password: Accept the default.

   An optional company name: Enter a value or accept the default.

   Sign the certificate: Enter `y`.

   1 out of 1 certificate requests certified, commit?: Enter `y`.



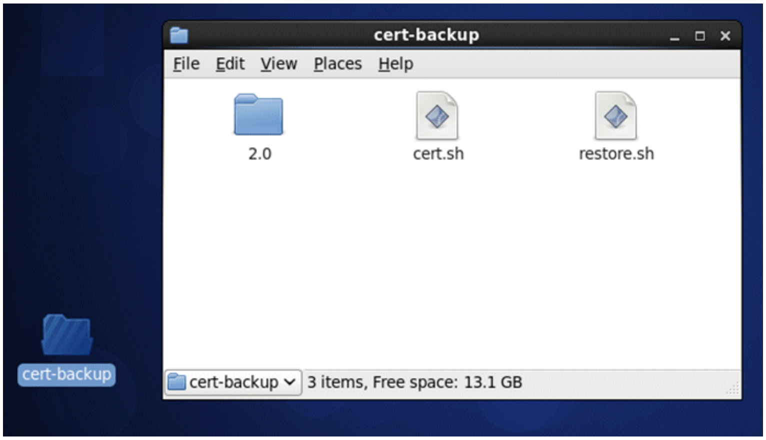
```
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'mail@host.domain'
Certificate is to be certified until Mar 12 00:26:35 2023 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
```

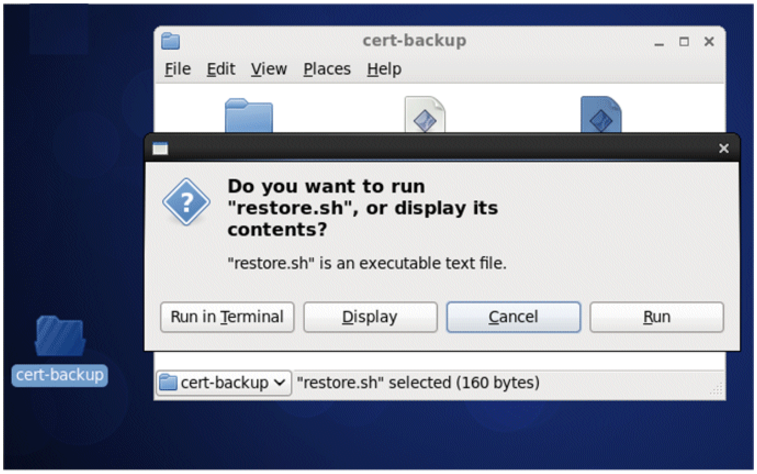
5. When the process completes, cert.sh and the 2.0 folder will be moved from the desktop to the cert-backup folder to prevent accidently re-running the script.

If the certificates ever need to be re-built for any reason, open the cert-backup folder and double-click restore.sh.



3 items, Free space: 13.1 GB

When prompted, click **Run in Terminal**.



Do you want to run "restore.sh", or display its contents?

"restore.sh" is an executable text file.

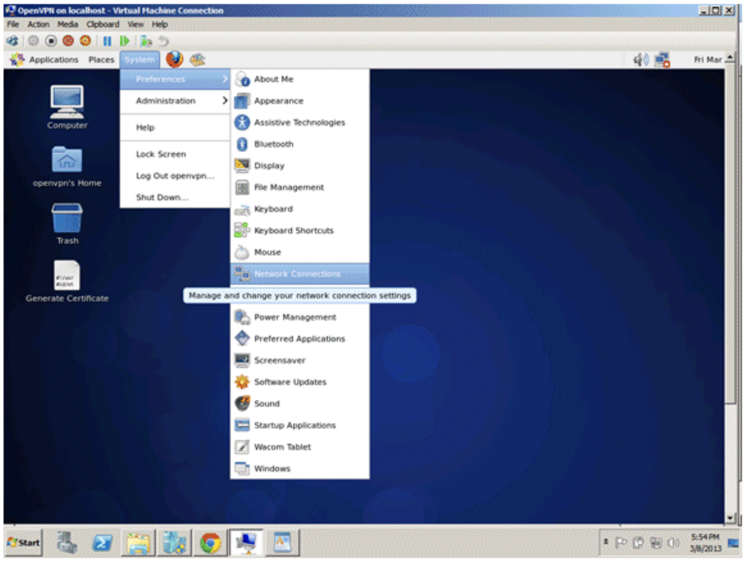
"restore.sh" selected (160 bytes)

The previously-created certificates will be deleted, and cert.sh and the 2.0 folder are moved back to the desktop so you can re-rerun the certificate process.

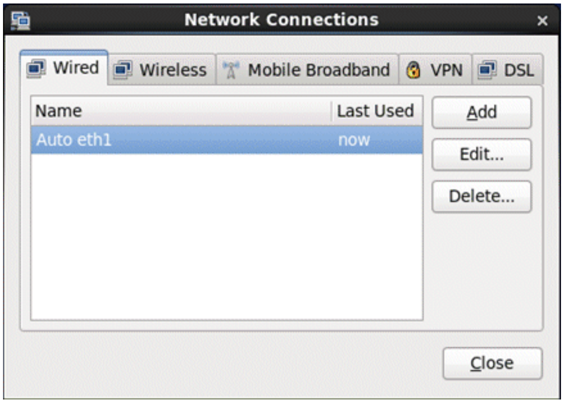
Changing network settings for your environment

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**.

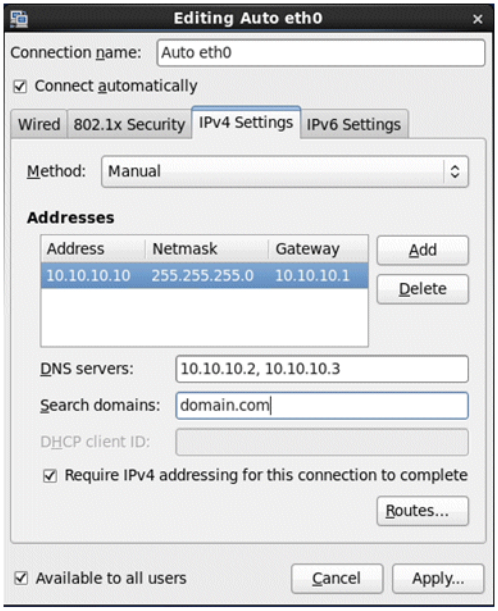


2. On the Wired tab, click **Add**. If a network connection is already displayed, click **Edit** instead.



Name	Last Used
Auto eth1	now

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



Editing Auto eth0

Connection name: Auto eth0

☑ Connect automatically

Method: Manual

Addresses

Address	Netmask	Gateway
10.10.10.10	255.255.255.0	10.10.10.1

DNS servers: 10.10.10.2, 10.10.10.3

Search domains: domain.com

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

☑ Available to all users

- 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 in Wave later.
  - 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.

Editing your OpenVPN Network settings

OpenVPN runs a DHCP server to assign IP addresses to VPN phones. You need to choose an IP address range that works within your network's larger address schema. Consult with your network administrator before setting these options. Do not change any other settings not specifically described in the following steps.

1. To open a terminal, click **Applications > System Tools > Terminal**.
2. To elevate your privileges to a super user, type `SU` and press **Enter**.

   When you are prompted, enter the password **Vertical4VoIP!**.
3. Using the VI Editor, type the following command and click **Enter**:

   ```
   vi /etc/openvpn/openvpn.conf
   ```

   The text of the openvpn.conf file will appear. You will need to edit a few values.
4. Type `i` to enter input mode. Use the arrow keys to navigate through the file.
5. Find this line:

   ```
   #change ip address to vpn client dhcp network address
   ```

   Below it there is a line that says:

   ```
   “server 10.10.2.0 255.255.255.0”
   ```

   This setting specifies the IP range assigned to the VPN phones. Do not change these settings unless your network already includes the 10.10.2.0 subnet. In that case, choose a different subnet from the subnet the Wave Server is on.

   Important: Do NOT try to set this setting for the same subnet as the Wave Server.

   - `“10.10.2.0”` is the default network address range for the VPN phones.
   - `“255.255.255.0”` is the subnet mask for the VPN phones.
6. To change the DNS server, find the following two lines:

   ```
   push “dhcp-option DNS 10.10.1.2”
   ```

   ```
   push “dhcp-option DNS 8.8.4.4”
   ```

   - Change `“10.10.1.2”` to the primary DNS server used by your local network.
   - Change `“8.8.4.4”` to the secondary DNS server on your local network.

7. Optionally, to change the Domain, find this line:

   ```
   "dhcp-option DOMAIN yourdomain.com"
   ```

   - Change `"yourdomain.com"` to your network domain name. Note that this option is not currently used for any feature.

8. Press **Esc** to exit insert mode and return to command mode.

9. To save the file and exit, type the following command and press **Enter**—you must use lower case when typing this command.

   ```
   :wq!
   ```

Adding users

A user account is needed for each phone that will be set up to use VPN. Create an account for each user as described below, and record the data for later entry into User/Group Management in the Wave Global Administrator Console, as described on "Configuring VPN for a user" on page 3-2.

You can add users from the terminal or desktop.

To add users from the terminal

1. To open a terminal, click **Applications > System Tools > Terminal**.

2. To elevate your privileges to a super user, type `SU` and press **Enter**.

   When you are prompted, enter the password **Vertical4VoIP!**.

3. To add a user, type the following command and press **Enter**:

   ```
   useradd <username>
   ```

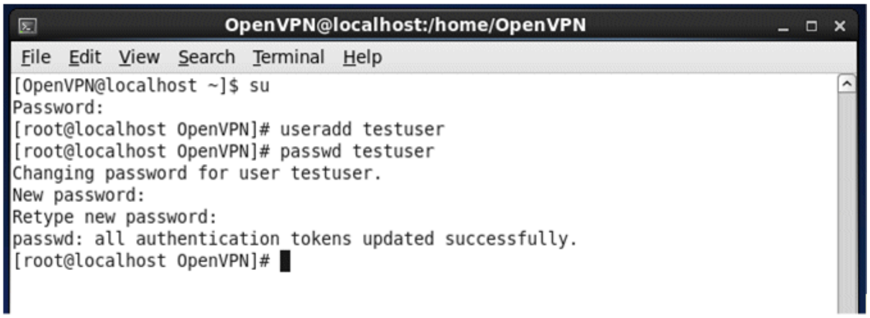
   where `<username>` is replaced by the username the phone will log in with.

4. To add a password for the new user, type the following command and press **Enter**:

   ```
   passwd <username>
   ```

   where `<username>` is replaced by the username you just created.

When you are prompted to add and verify a password, do so.



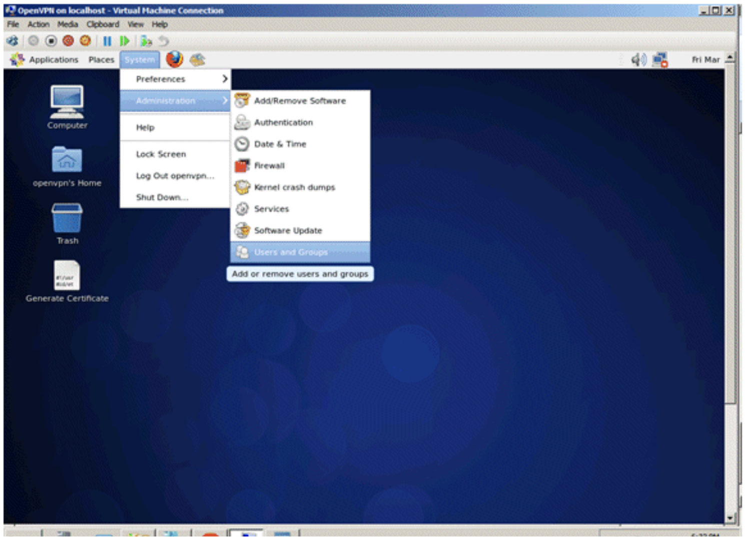
OpenVPN@localhost:/home/OpenVPN
File Edit View Search Terminal Help

```
[OpenVPN@localhost ~]$ su
Password:
[root@localhost OpenVPN]# useradd testuser
[root@localhost OpenVPN]# passwd testuser
Changing password for user testuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost OpenVPN]# 
```

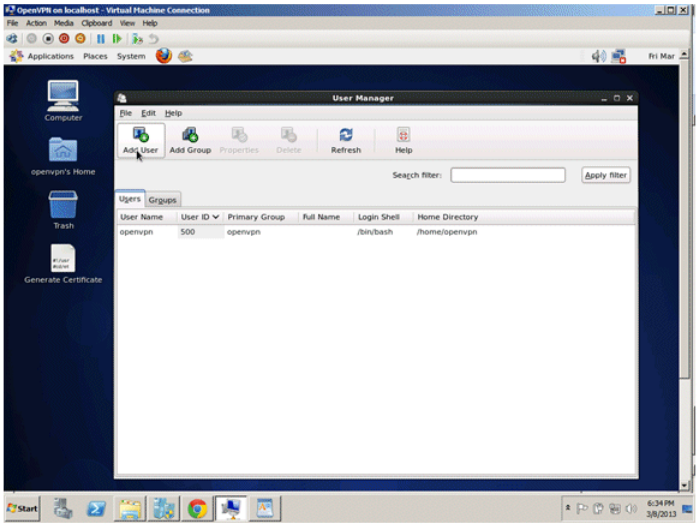
Repeat for next user by typing `useradd <username>`.

To add users from the desktop

1. Click **System > Administration > Add Users and Groups**.

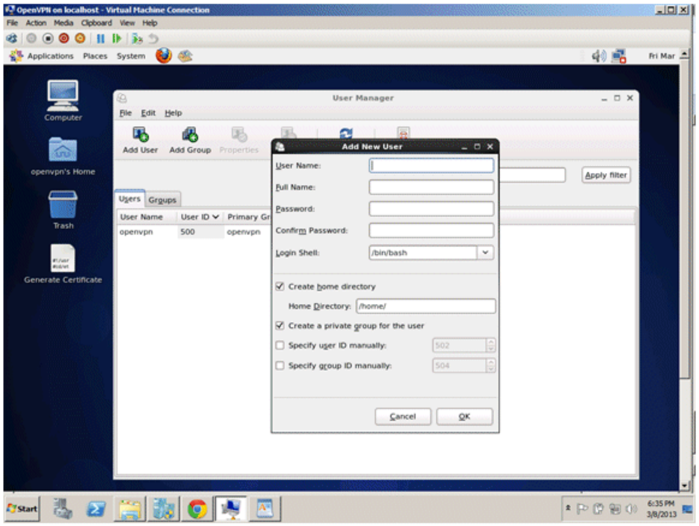


2. Click **Add User**.



User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
openvpn	500	openvpn		/bin/bash	/home/openvpn

3. In the Add New User dialog, enter the **User Name**, and then enter and confirm the user’s **Password**.



User Name:
Full Name:
Password:
Confirm Password:
Login Shell: /bin/bash
☑ Create home directory
Home Directory: /home/
☑ Create a private group for the user
☐ Specify user ID manually: 502
☐ Specify group ID manually: 504

4. Click **OK**, and then repeat to add the next user.

Downloading the certificate from OpenVPN Server

The certificate file needs to be loaded on the Wave Server.

To get access to the certificate

1. To open a terminal, click **Applications > System Tools > Terminal**.
2. To elevate your privileges to a super user, type `SU` and press **Enter**. Super user privileges are required because the file is in the keys folder which is restricted access.

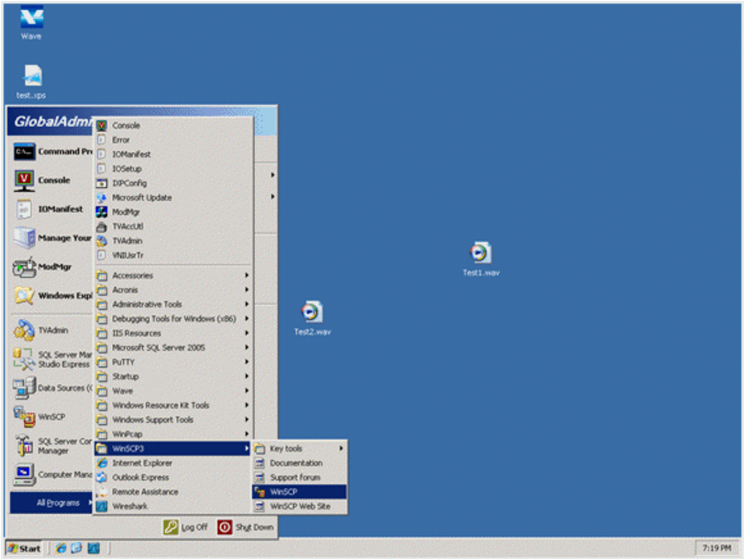
   When you are prompted, enter the password **Vertical4VoIP!**.
3. To copy the certificate from the keys folder to a folder you can get to, type the following command.

   ```
   cp /etc/openvpn/easy-rsa/2.0/keys/ca.crt /etc/openvpn
   ```

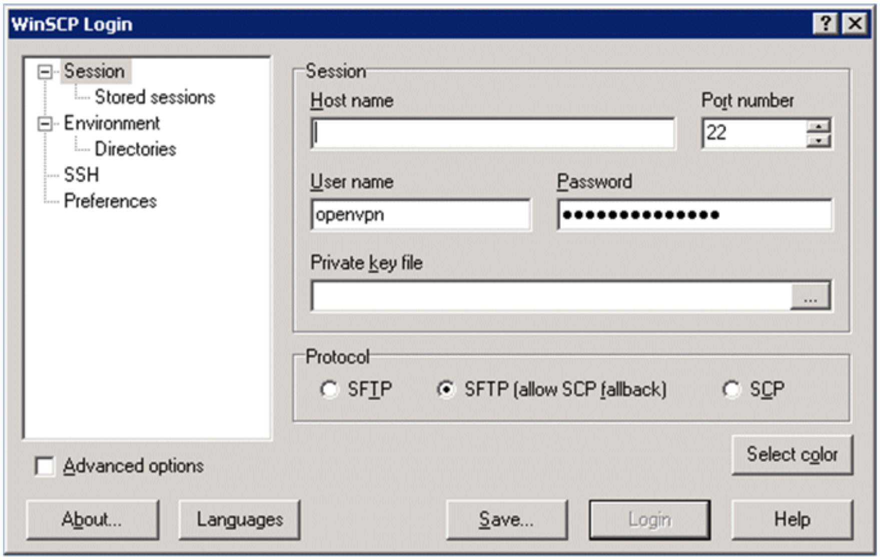
   The certificate is now located in the /etc/openvpn folder.

To copy the key to the Wave Server

4. Login to the Wave Server desktop.
5. Choose **Start > All Programs > WinSCP3**, and then and click on **WinSCP**.



6. In the WinSCP Login dialog, make the following changes.



Port number: 22

User name: openvpn

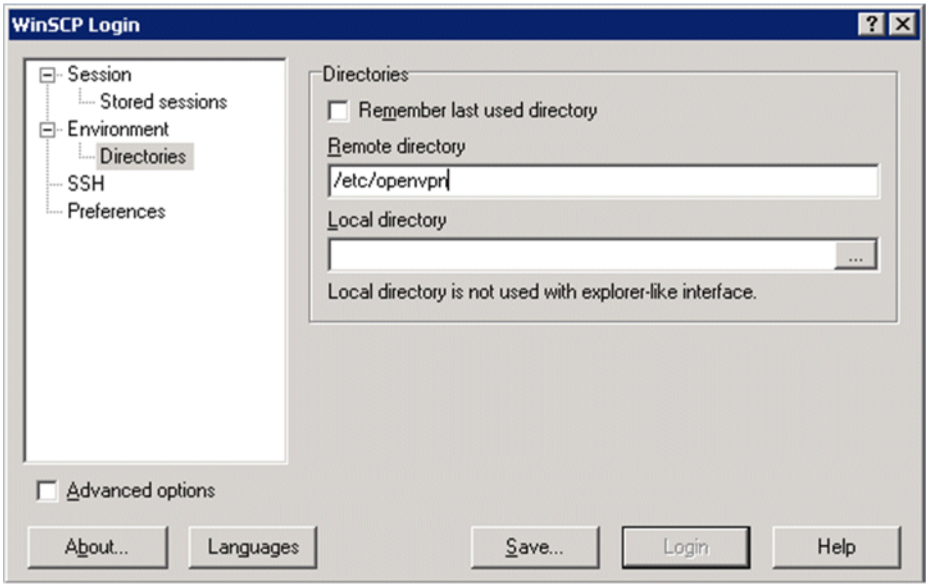
Password: ●●●●●●●●●●●●●●●

Protocol: ○ SFTP ● SFTP (allow SCP fallback) ○ SCP

- **Host name**. Enter the IP address of the OpenVPN server.
- **Port number**. Do not change this value.
- **User name**. Enter **openvpn**.
- **Password**. Enter the new OpenVPN password that you changed earlier.

7. Click on **Directories** in the left pane.

8. For **Remote directory**, enter `/etc/openvpn`.



WinSCP Login

Directories

☐ Remember last used directory

Remote directory: /etc/openvpn

Local directory:

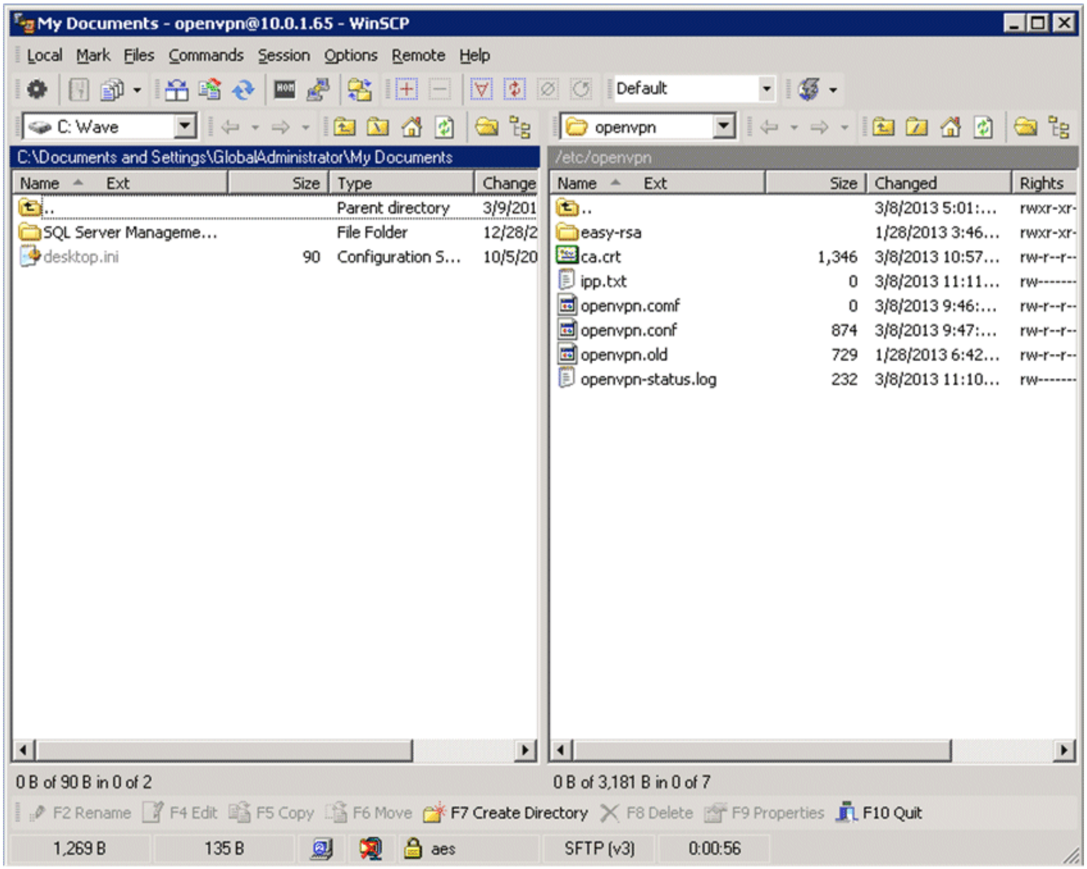
Local directory is not used with explorer-like interface.

☐ Advanced options

9. Click **Save** and then click **Login**.

10. If a dialog opens indicating that the Private key for this server is not recognized, click **Yes** to save the key.

11. You will now see the openvpn server directory in the right pane, and the Wave My Documents folder in the left pane.



My Documents - openvpn@10.0.1.65 - WinSCP

C:\Documents and Settings\GlobalAdministrator\My Documents

Name	Ext	Size	Type	Change
..			Parent directory	3/9/201
SQL Server Manageme...			File Folder	12/28/2
desktop.ini		90	Configuration S...	10/5/20

/etc/openvpn

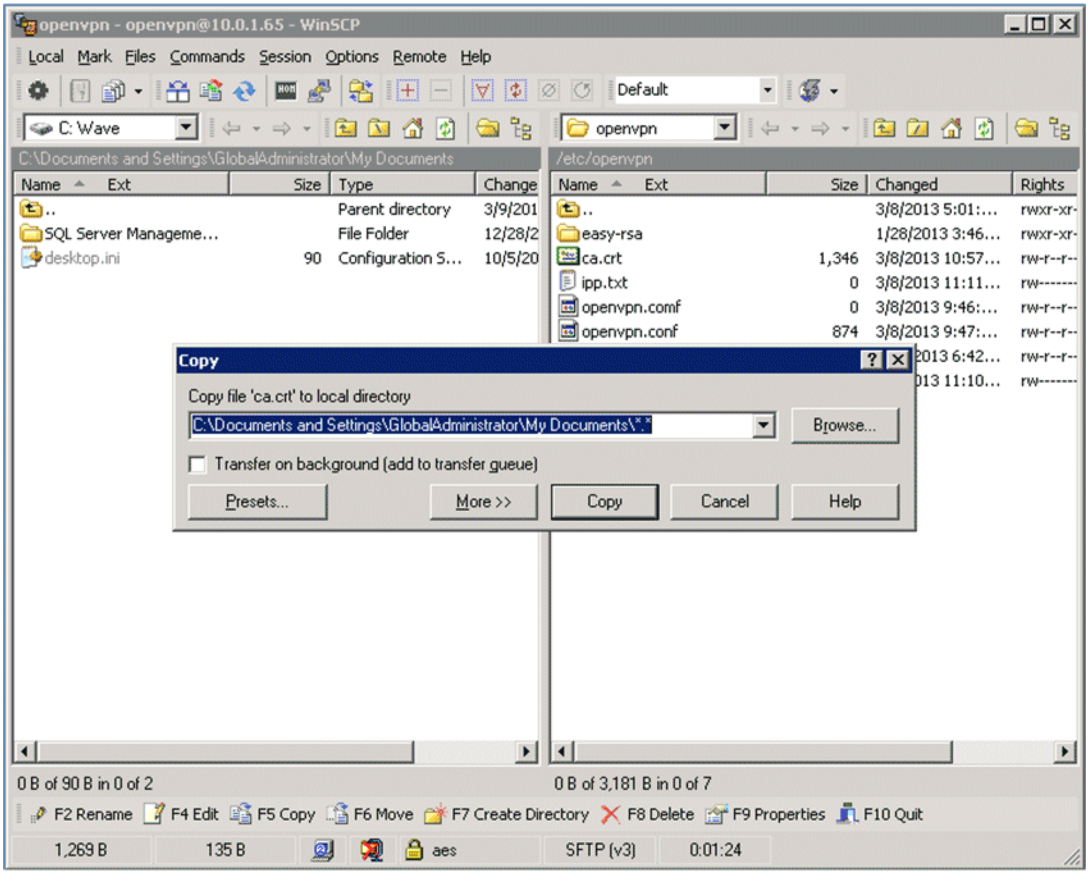
Name	Ext	Size	Changed	Rights
..			3/8/2013 5:01:...	rwxr-xr-
easy-rsa			1/28/2013 3:46...	rwxr-xr-
ca.crt		1,346	3/8/2013 10:57...	rw-r--r--
ipp.txt		0	3/8/2013 11:11...	rw-------
openvpn.comf		0	3/8/2013 9:46:...	rw-r--r--
openvpn.conf		874	3/8/2013 9:47:...	rw-r--r--
openvpn.old		729	1/28/2013 6:42...	rw-r--r--
openvpn-status.log		232	3/8/2013 11:10...	rw-------

0 B of 90 B in 0 of 2

0 B of 3,181 B in 0 of 7

1,269 B 135 B aes SFTP (v3) 0:00:56

12. Click and drag the CA.Crt file from the right pane to the left. Click **Copy** when you see this dialog:



C:\Documents and Settings\GlobalAdministrator\My Documents

Name	Ext	Size	Type	Change
..			Parent directory	3/9/201
SQL Server Manageme...			File Folder	12/28/2
desktop.ini		90	Configuration S...	10/5/20

/etc/openvpn

Name	Ext	Size	Changed	Rights
..			3/8/2013 5:01:...	rwxr-xr-
easy-rsa			1/28/2013 3:46...	rwxr-xr-
ca.crt		1,346	3/8/2013 10:57...	rw-r--r--
ipp.txt		0	3/8/2013 11:11...	rw-------
openvpn.comf		0	3/8/2013 9:46:...	rw-r--r--
openvpn.conf		874	3/8/2013 9:47:...	rw-r--r--
			2013 6:42...	rw-r--r--
			013 11:10...	rw-------

Copy

Copy file 'ca.crt' to local directory

C:\Documents and Settings\GlobalAdministrator\My Documents*.*

□ Transfer on background (add to transfer queue)

0 B of 90 B in 0 of 2

0 B of 3,181 B in 0 of 7

1,269 B 135 B aes SFTP (v3) 0:01:24

13. Exit WinSCP.

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 Open VPN 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 use one of the user accounts you created earlier to 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
  ```

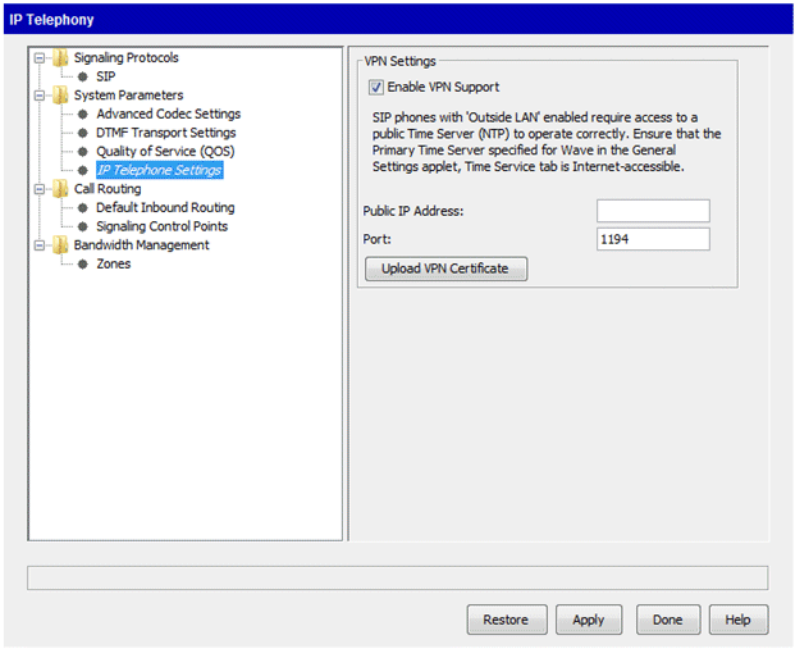
  Note: The command to enter the route statement depends on the specific hardware of the default gateway.

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 > IP Telephone Settings** in the left pane.



IP Telephony

- Signaling Protocols
  - SIP
- System Parameters
  - Advanced Codec Settings
  - DTMF Transport Settings
  - Quality of Service (QOS)
  - *IP Telephone Settings*
- Call Routing
  - Default Inbound Routing
  - Signaling Control Points
- Bandwidth Management
  - Zones

VPN Settings

☑ Enable VPN Support

SIP phones with 'Outside LAN' enabled require access to a public Time Server (NTP) to operate correctly. Ensure that the Primary Time Server specified for Wave in the General Settings applet, Time Service tab is Internet-accessible.

Public IP Address:

Port: 1194

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 previously.

   - **Port**. Enter 1194.

5. Click **Upload VPN Certificate**. Browse to the location where you saved the CA.crt file when you copied it from OpenVPN Server. Select the CA.crt file, and then click **Upload Certificate File**.

6. 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:

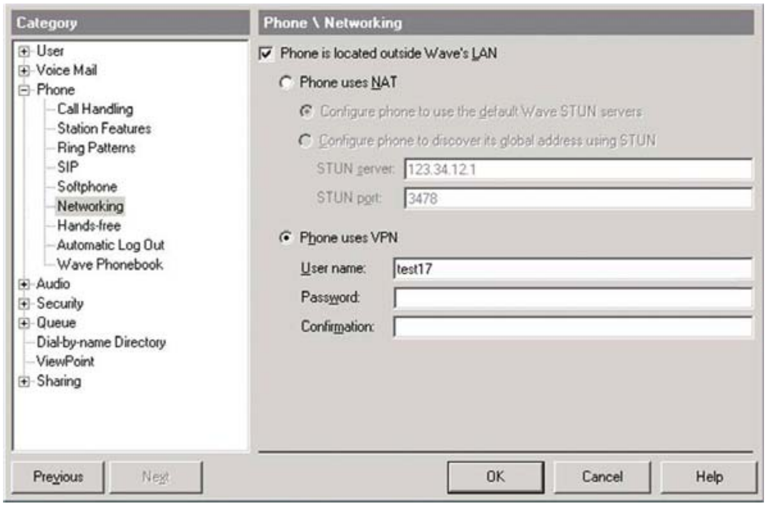
- **Via User/Group Management**. This method is easier for the Wave administrator, because the user name and password can be supplied at the same time that VPN is enabled for the user, as described in "Configuring VPN for a user" on page 3-2. However, this method is less secure because the credentials 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 SIP phone" on page 3-3.

Configuring VPN for a user

You enable VPN on a user-by-user basis. Each user must be defined with one of the supported phone models listed on page 1-1.

To enable VPN for a user

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.



☑ Phone is located outside Wave's LAN

○ Phone uses NAT

● Configure phone to use the default Wave STUN servers

○ Configure phone to discover its global address using STUN

STUN server: 123.34.12.1

STUN port: 3478

● Phone uses VPN

User name: test17

Password:

Confirmation:

3. Select the **Phone is located outside Wave's LAN** checkbox.
4. Click **Phone uses VPN**.
5. Enter a **User name** and **Password** combination that you created as described in "Adding users" on page 2-33.

   Important: If you have any security concerns, enter these credentials directly on the phone itself, as described in "Configuring VPN on a user's SIP phone" on page 3-3.
6. Click **OK** to save your changes for this user.

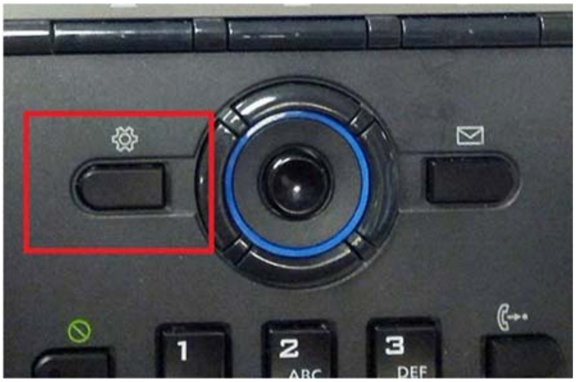
Configuring VPN on a user's SIP phone

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

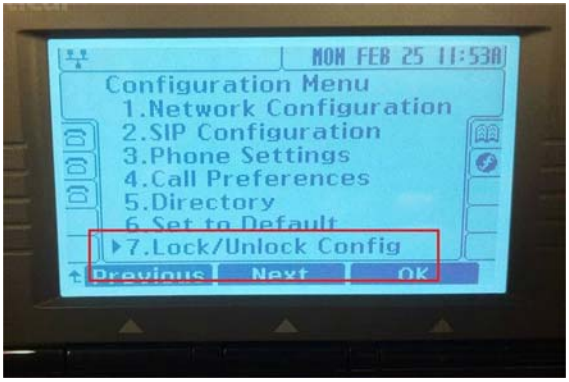
Note: If you already entered the user's VPN credentials via User/Group Management as described in "Configuring VPN for a user" on page 3-2, you do not need to re-enter them according to the following steps.

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.

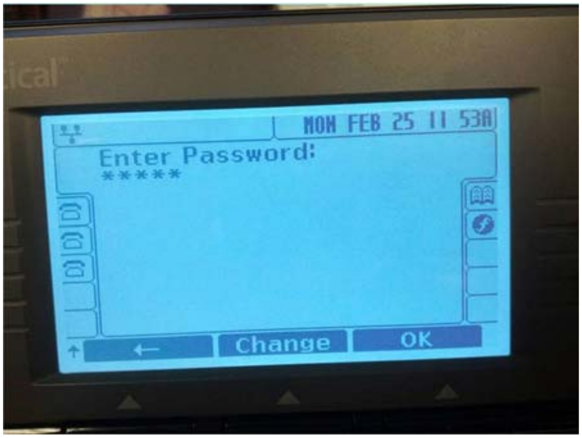
1. On the phone, press the MENU key.



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

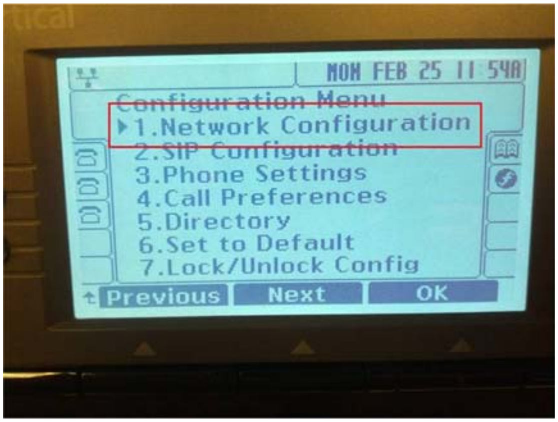


3. Enter the Configuration Menu password using the phone’s keypad. This password protects some configuration options when changing them from the phone’s keypad. The default password is 22222.

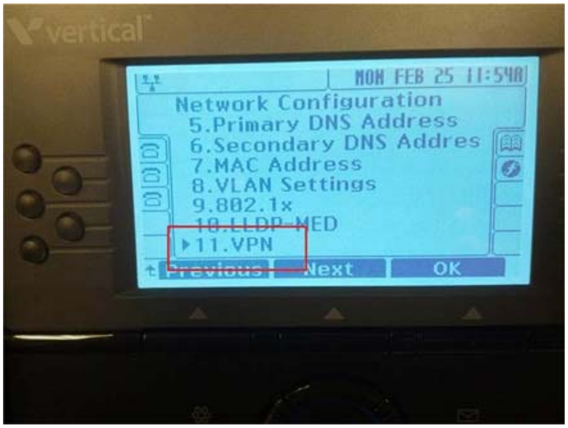

Enter Password:
*****

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

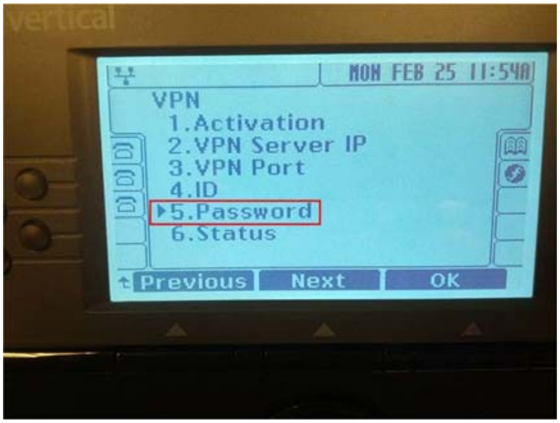
5. Select **Network Configuration**.



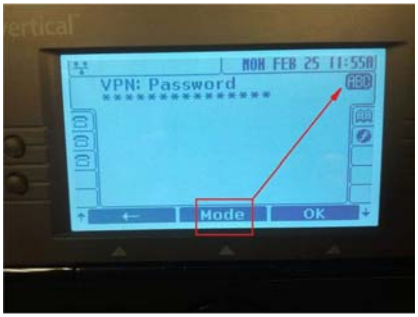
6. Select **VPN**.



7. Select **Password**.



8. Enter the user's VPN password using the phone's keypad. (This is the user password that you supplied as described "Configuring VPN for a user" on page 3-2.)



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