

# **VPN Client Software Reference Guide**

Compatible Systems Corporation  
4730 Walnut Street  
Suite 102  
Boulder, Colorado 80301

303-444-9532  
800-356-0283  
<http://www.compatible.com>

VPN Client Software Reference Guide  
Version 3.8  
Copyright © 1999, Compatible Systems Corporation

All rights reserved. IntraPort, RISC Router, MicroRouter and CompatiView are trademarks of Compatible Systems Corporation. Other trademarks are the property of their respective holders.

Part number: A00-1857

FCC Notice: This product has been certified to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC Rules. It is designed to provide reasonable protection against radio or television communication interference in a commercial environment. Operation of this equipment in a residential area could cause interference with radio or television communication.

**About This Manual 3**

---

**Chapter 1 - Introduction to the VPN Client Software 4**

---

OBTAINING THE VPN CLIENT SOFTWARE	4
GETTING HELP WITH THE VPN CLIENT SOFTWARE	5
Sources for End Users	5
Sources for System Administrators	5

**Chapter 2 - Installing and Running the Windows and Mac OS Clients 6**

---

WINDOWS AND MAC OS VPN CLIENT SOFTWARE INSTALLATION	6
Installing the Windows 95/98 VPN Client Software	6
Installing the Windows NT VPN Client Software	6
Installing the Mac OS VPN Client Software	7
CUSTOMIZING THE LOGO	8
Creating an Icon on the General Tab	9
Creating a Customized Desktop Icon	9
CREATING A CUSTOMIZED HELP FILE	10
About the Mac OS VPN Client Help Tab	10
Adding a Help Tab to the Windows VPN Client	10
Creating a Customized Config File	11
RUNNING THE VPN CLIENT SOFTWARE	12
Setting Up a Login	12
ESTABLISHING TUNNEL SESSIONS	13
VPN Client Window	13
VPN Client Connect Window	13
VPN CLIENT SOFTWARE REFERENCE	15
VPN Client Properties Window	15
General Tab	15
Configuration Tab	16
Login Properties Window (Windows and Mac OS)	17
VPN Encryption Password Window	19
Prompt for Secret Window	19
RADIUS Login Window	19
Logging Tab	20
VPN Client Icon and the Windows Task Bar	21

VPN Client Mac OS Pull-down Menu	21
USING SECURID WITH THE VPN CLIENT	22
<b>Chapter 3 - Installing and Running the Linux and Solaris Clients</b>	<b>25</b>
<hr/>	
INSTALLING THE LINUX VPN CLIENT SOFTWARE	25
Linux VPN Client Overview	25
System Requirements	25
Unpacking the Linux Client Files	26
Installing the VPN Client Files	26
About the Linux Client Install Script	26
INSTALLING THE SOLARIS CLIENT SOFTWARE	27
Unpacking the Solaris Client Files	27
Installing the Solaris Client Files	27
About the Solaris Client Install Script	28
ESTABLISHING TUNNEL SESSIONS	28
LINUX AND SOLARIS OPERATIONAL COMMANDS	29
open_tunnel Command	29
<b>Chapter 4 - Creating a VPN Client Config File</b>	<b>31</b>
<hr/>	
Exiting the VPN Client	31
Section Names	32
SAMPLE VPN CLIENT CONFIG FILE	35
<b>Appendix A - Uninstalling the Windows NT Client</b>	<b>36</b>
<hr/>	
<b>Appendix B - Manually Installing the Windows NT VPN Network Driver</b>	<b>37</b>
<hr/>	

---

## About This Manual

This manual documents Compatible System's VPN Client software, v3.8x for Windows, v3.8x for Mac OS, v3.8x for Linux and v. 3.8x for Solaris. It is divided into three main sections: the installation and configuration of the GUI clients (Windows and Mac OS); the installation and configuration of the command line clients (Linux and Solaris); and the creation of a VPN Client config file. Setting up a config file is optional for the Windows and Mac clients, but is required for the Linux and Solaris clients.

❖ **Note:** *To assist remote users with the installation and setup of the VPN Client, this information is also available in the Technical Support section of the Compatible Systems Web site at: <http://www.compatible.com/>*

# Chapter 1 - Introduction to the VPN Client Software

Remote users may run client software either from a machine connected to the Internet via a dial-up PPP connection or from a machine connected via an Ethernet LAN to the Internet (including connections through most cable modems and xDSL devices).

## Obtaining the VPN Client Software

You may obtain the VPN Client software in any of the ways noted below, depending on the preference/policy of your organization.

- From a diskette provided by your network administrator
- Downloaded from your organization's internal Web site
- Downloaded over the Internet from the Compatible Systems Web site as follows:
  1. Use your browser to access <http://www.compatible.com/>, and find the link on our home page to "Software Downloads"
  2. Select the product and software version you want. Due to government restrictions on the export of encryption technology you will be asked to fill out a software request form. If the request is received from a computer outside the U.S. or Canada, we will help you to determine whether export is permitted under the licenses and/or license exceptions granted to us by the U.S. Department of Commerce, Bureau of Export Administration. Otherwise, the location of the software will be sent to you via e-mail once the request has been processed.

Check with your network administrator if you have questions about obtaining client software.

---

## Getting Help with the VPN Client Software

### Sources for End Users

If you have a question about the VPN Client Software and can't find the answer in one of the manuals included with the product, please contact your system administrator or internal help desk.

### Sources for System Administrators

If you have a question about the VPN Client Software and can't find the answer in one of the manuals included with the product, there are several ways to get technical support.

1. Visit the technical support section of our Web site (<http://www.compatible.com>).

This site includes extensive technical resources which may answer many of your questions. You can also request technical support by filling out a brief form. **Technical support requests received via the Web form will receive expedited treatment.**

2. Send support questions via e-mail to [support@compatible.com](mailto:support@compatible.com).
3. Call Compatible Systems Corporation at 1-800-356-0283.

# Chapter 2 - Installing and Running the Windows and Mac OS Clients

## Windows and Mac OS VPN Client Software Installation

### Installing the Windows 95/98 VPN Client Software

The Windows 95/98 VPN Client software will run on any machine with a Pentium™ 90 or faster processor.

To install the Windows 95/98 Client:

- Run the WinVPNClientx.xx program (where x.xx is the version number) by double-clicking on it. The setup program will transfer all necessary files to the destination volume of your choice.

### Installing the Windows NT VPN Client Software

The Windows NT Client software requires Windows NT 4.0 with Service Pack 3, 4, 5, or 6 and Remote Access Service installed. If a previous version of the Windows NT Client was installed, it must be uninstalled before a new client can be successfully installed and used. See Appendix A for details on uninstalling older versions of the client.

❖ **Note:** *If Remote Access Service is not installed, you must install it before the client will work. We also strongly recommend that you install Windows NT 4.0 Service Pack 4 or later, even if it is already on the system. Other network-related installations may have overwritten older versions of files contained in the Service Pack.*

To install the Windows NT Client:

1. First you must copy the Windows NT VPN Client file (and the associated release notes) to a temporary folder on your hard drive (i.e. C:\temp).
2. Run the NTPVPNClientx.xx program (where x.xx is the version number) by double-clicking on it. The setup program will transfer all necessary files to the destination volume of your choice and will

launch a macro which automatically installs an IntraPort VPN Access Server network driver.

3. While the macro is running (it begins by opening an MS DOS window) **DO NOT** touch keys on the keyboard or the mouse. There will be several pauses while the macro opens different screens and types information in for you. Be patient and wait until you are prompted to restart your computer. Click on the appropriate button to complete the installation.

❖ **Note:** *If the macro is unsuccessful, you may manually install the IntraPort VPN Access Server network driver by following the instructions in Appendix B.*

## Installing the Mac OS VPN Client Software

The Mac OS VPN Client software will run on any Macintosh or compatible machine with a PowerPC CPU, Mac OS 7.6 or later and Open Transport 1.1.1 or later.

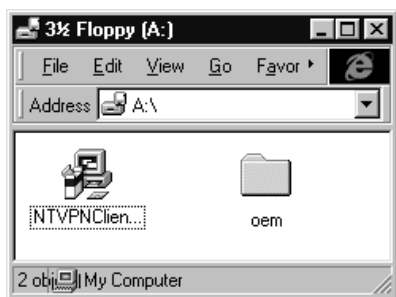
To install the Mac OS Client:

1. Run the MacVPNClientx.xx.sea.hqx program (where x.xx is the version number) by double-clicking on it (you will need a program such as StuffIt or BinHex to expand it).
2. Select a destination for the self extracting archive, then click "Save."
3. Go to the selected destination and double-click on the self extracting archive. The installation program will allow you to drag the VPN Client software to the computer system's hard disk.
4. After the installation is complete, a dialog box will open which allows you to restart your computer. Click "Restart."

## Customizing the Logo

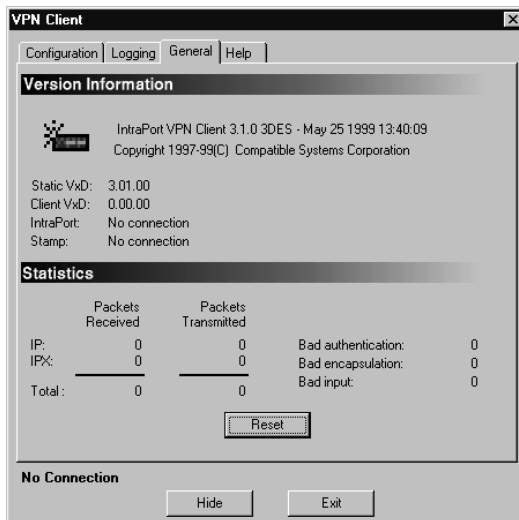
This section describes how to place a company logo (or any customized logo) in the VPN Client program that is sent to remote users. This customized logo can be placed as an icon on the start menu, as a shortcut on the desktop, and on the VPN Client dialog box that is used for establishing a connection. Choose either one or both of these options.

First you must create a new folder (a subdirectory) in the VPN Client directory called “oem.” This folder should reside in the same directory as the install file.



OEM Folder

## Creating an Icon on the General Tab



General Tab with Customized Logo

1. Create a file of the logo (recommended size 64 x 64 pixels) and name it **logo.bmp**.
2. Save it in the oem folder.

This will be the logo that gets placed on the General tab.

## Creating a Customized Desktop Icon

1. Create a file of the icon and name it **oem.ico**.
2. Save it in the oem folder.

This icon will be placed on the start menu beside VPN Client, and as a shortcut on the desktop.

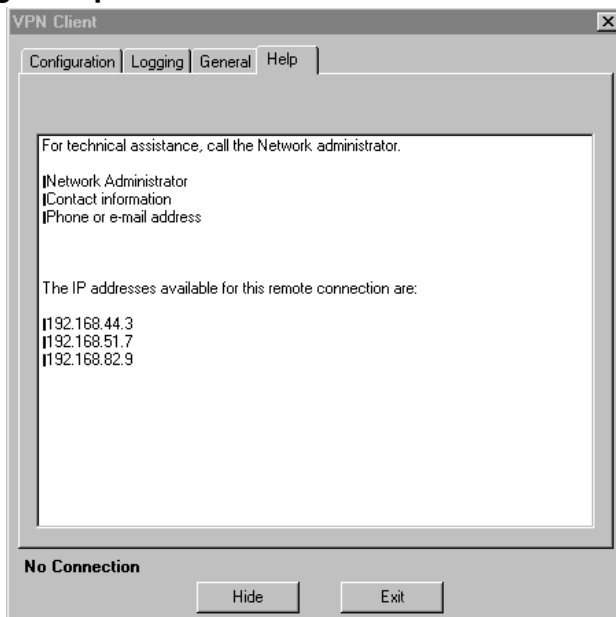
## Creating a Customized Help File

This section describes how to access or create customized help files. A customized help file can contain information specifically designed for remote users. For example, the help file could have contact information for technical support questions, a listing of the available IP addresses and their locations, or special instructions for the remote user.

### About the Mac OS VPN Client Help Tab

A help file is automatically installed when the VPN Client is installed on the Macintosh. It is a text file located in the System Folder:Extensions folder on the System Disk of the Macintosh. The file is named “CSC VPN Help.” This file can be opened and edited using any word processing application and must be saved as a simple text (.txt) file. If this file is removed, then the Help tab will not appear in the VPN Client.

### Adding a Help Tab to the Windows VPN Client



Customized Help Tab

A help file is not part of the Windows VPN Client. The help file can be created using the following instructions.

1. Create a text file and name it **help.txt**.
2. Save it in the oem folder (for information on creating the oem folder, see Customizing the Logo).

When the VPN Client is installed, a help tab will be included in the VPN Client dialog box. This help file will contain the information in the text file that was created.

## Creating a Customized Config File

Administrators (Windows only) may distribute a customized configuration file for each user. This 'pre-configured' vpn\_config file must be saved in the OEM directory that was created for that user.

The file must be named "vpn\_config" and can be created with any text editing program, but it must be saved as a plain text file, without any file extension.

(For more information on the vpn\_config file, see Creating a VPN Client Config File.)

## Running the VPN Client Software

This section of the manual contains a list of the essential steps and basic information needed to begin using the VPN Client software. All of the features of the VPN Client software, including screen shots, are documented in detail in the next section, VPN Client Software Reference.

### Setting Up a Login

The administrator may set up a “pre-configured” login configuration for each user, or the user may be instructed to set up their own configuration.

If the administrator has already set up a login configuration for a particular user, this file will exist in the OEM folder, which resides in the same directory as the install file (for information on creating the oem folder, see Customizing the Logo).

Contact the administrator to determine your login configuration needs.

To set up your own login:

1. Double click on the VPN Client icon. The VPN Client window will open.
2. Click on the Configuration tab.
3. Click on the Add button. The Login Properties window will open.
4. Enter appropriate login parameters. This information should be provided by the network administrator. At a minimum, you need:

- Login Name

❖ **Note:** *If you intend to use the auto-login feature, it is recommended that you do not use any spaces in your login name (Windows only).*

- IP Address or domain name of the IntraPort VPN Access Server you will be logging into
5. Click OK.

You may repeat this process to add multiple logins.

## Establishing Tunnel Sessions

Tunnel sessions may be established manually with the VPN Client window, or automatically with the VPN Client Connect window (Windows clients only).

### VPN Client Window

To establish a tunnel session through the VPN Client Properties window:

1. Double click on the VPN Client icon. The VPN Client Properties window will open.
2. Click on the Configuration tab.
3. Select a login by clicking on it.
4. Click on the Connect button. If this is the first time you are logging on, or if the VPN Group configuration in the IntraPort VPN Access Server requires it, the Prompt for Secret window will open.
5. Enter your Shared Secret. You may also be prompted for a RADIUS password and Authentication secret. Enter any other required passwords.
6. Click OK.

If the connection is successful, a black dot will appear next to the login name and a connection message will appear at the bottom of the window.

❖ **Note:** *When the VPN Client is connected, only traffic destined for the remote networks which were made accessible in the IntraPort VPN Access Server's configuration by your network administrator will be tunneled. All other Internet traffic will be sent as usual.*

### VPN Client Connect Window

If the **Auto Connect before Logon** box on the Configuration tab is checked, the VPN Client connect screen will appear in the upper left hand corner of your screen each time you start up your computer (Windows clients only).

❖ **Note:** *Do not hit Ctrl-Alt-Del to log on to your computer until the VPN Client Connect Window appears. The VPN Client is the last service on the NT boot-up, please be patient.*

You may also open the VPN Client Connect window by double-clicking

## 14 Chapter 2 - Installing and Running the Windows and Mac OS Clients

---

on the **VPNAutoStart** file, located in the folder where the install program resides.



VPN Client Connect

To establish a tunnel session through the VPN Client Connect screen, click on the button that represents the preferred method of connection. Contact the administrator to determine the method of connection for each user.

### Connect to VPN Server via:

**Phonebook** - This button brings up the system phone book, which contains dial-up options for the user.

❖ **Note:** *If the phonebook button is grayed out, it means that you do not have RAS installed. Check with the system administrator if you wish to have this option available.*

**LAN** - This will connect the user through the local LAN.

Once a VPN Client connection has been established, the user can log on to the network as usual.

## VPN Client Software Reference

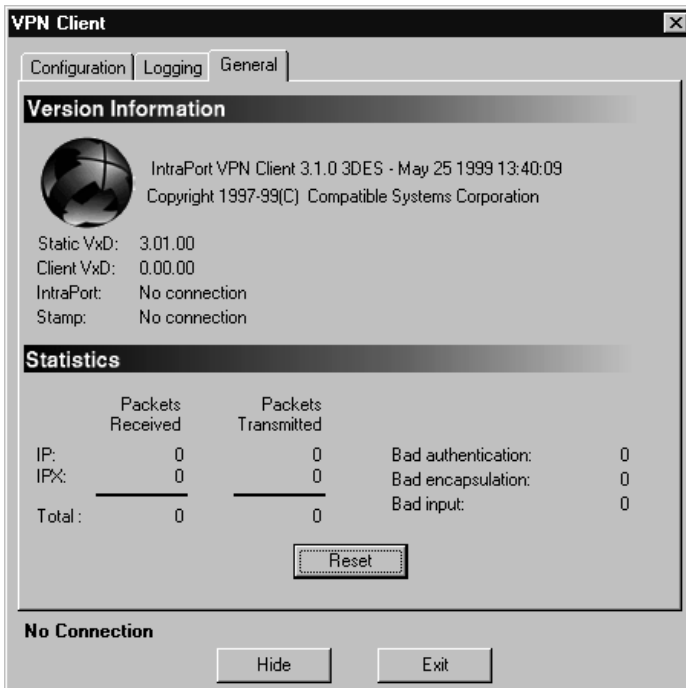
This section of the manual documents all of the windows and features of the VPN Client software.

❖ **Note:** *The Mac OS and Windows VPN Clients are virtually identical in content. Screen shots on the following pages are applicable to both environments.*

### VPN Client Properties Window

This window's tabbed sections allow you to set up logins, view statistics and set other client parameters.

#### General Tab



This tab displays VPN Client information and packet statistics for sessions.

**Reset.** This button clears out the displayed statistics.

**Hide.** This button hides the VPN Client screen.

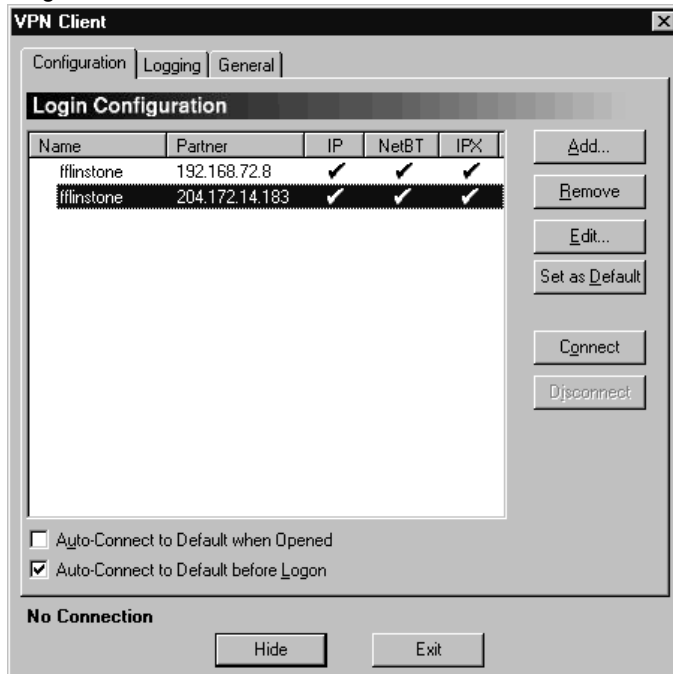
**Exit.** This button closes the VPN Client software.

## 16 Chapter 2 - Installing and Running the Windows and Mac OS Clients

### Statistics

If the **TallyBytes** keyword has been set, the number of bytes tunneled by the connected user is recorded and displayed in this section of the general tab. These values are only valid when a user is connected. For more information on the TallyBytes keyword, see Creating a VPN Client Config File.

### Configuration Tab



The Configuration tab contains a list of login configurations.

**Add.** This button allows you to create a new login.

**Remove.** This button allows you to delete a login.

**Edit.** This button allows you to make changes to the selected login.

**Set as Default.** If the **Auto-Connect to Default when Opened** box is checked, then this button sets a selected login to be run when the VPN Client is loaded. That login will also be the one selected when the screen is opened.

**Connect.** This button attempts to establish a secure tunnel to an Intraport VPN Access Server using the selected login.

You may be prompted for a Shared Secret if this is the first time you have connected, or if the VPN Group Configuration in the IntraPort VPN Access Server requires it. See the Prompt for Secret Window section later in this guide.

If the connection is successful, a black dot will appear next to the user's name and a connection message will appear at the bottom of the window.

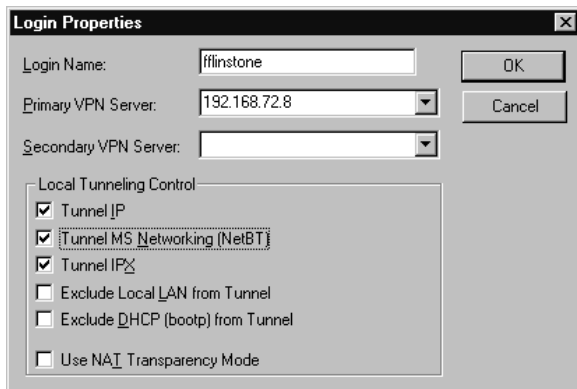
**Disconnect.** This button disconnects an active tunnel session.

**Auto-Connect to Default when Opened.** This box sets whether the default login will automatically connect to the IntraPort VPN Access Server when the VPN Client software is opened.

**Auto-Connect to Default before Logon.** This box sets whether the default login will automatically connect to the IntraPort VPN Access Server before logging into the VPN Client. This will enable users log into the VPN Client before they are connected to the network.

When this box is checked, the VPN Client Connect window will appear in the top left corner of the screen upon start-up. For more information on the VPN Client Connect window, see [Establishing Tunnel Sessions](#).

### Login Properties Window (Windows and Mac OS)



This window is accessed by selecting either the **Add** or **Edit** buttons in the Connections tab.

**Login Name.** This is the name of the tunnel user. This name must also be configured in the IntraPort VPN Access Server and/or an authentication service it is using (e.g., RADIUS, SecurID, etc.). See the Reference Guide for your IntraPort VPN Access Server for more information on how to set up an authentication service to work with your device.

## 18 Chapter 2 - Installing and Running the Windows and Mac OS Clients

---

**Primary VPN Server.** This is the IP address or fully qualified domain name of the IntraPort VPN Access Server that the client software will connect to.

**Secondary VPN Server.** This is the IP address or domain name of an alternate IntraPort VPN Access Server that the client software will connect to if the primary IntraPort is unreachable.

### **Local Tunneling Control**

**Tunnel IP** (default = checked). This box enables IP-in-IP tunneling to the **IPNet** configured in the IntraPort VPN Access Server. This will only work if the VPN Group configuration in the IntraPort VPN Access Server also has an **IPNet** configured

**Tunnel AppleTalk.** This box is currently disabled (Macintosh OS only).

**Tunnel MS Networking (NetBT)** (default = checked). This box enables Microsoft networking functionality over IP transport (Windows only). This will only work if the VPN Group configuration in the IntraPort VPN Access Server also has the **TunnelNetBT** keyword enabled.

**Tunnel IPX** (default = checked). This box enables connections to IPX servers during client sessions (Windows only). This will only work if the VPN Group configuration in the IntraPort VPN Access Server also has a **LocalIPXNet** configured.

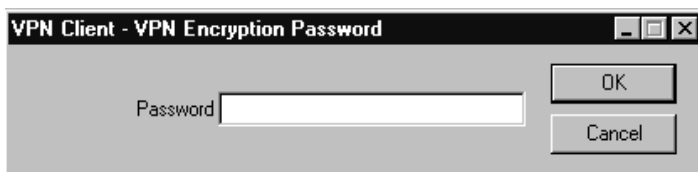
**Exclude Local LAN from Tunnel** (default = unchecked). If this box is checked, then local LAN traffic will not be tunneled. This will only work if the VPN Group configuration in the IntraPort VPN Access Server also has the **ExcludeLocalLAN** keyword enabled.

**Exclude DHCP (bootp) from Tunnel** (default = unchecked). If this box is checked, DHCP traffic will not be tunneled.

**Use NAT Transparency Mode** (default = unchecked). This box enables NAT (Network Address Translation) for client sessions. If there are problems connecting through a NAT device or through an ISP, checking this box may help by using the HTTP protocol for the session.

❖ **Note:** *If the Use NAT Transparency Mode box is checked, then the VPN Group configuration for this user must have an ESP transform set and it must be listed before any AH transforms in the configuration. The transforms (i.e., IKE protection pieces) are set in the IntraPort Server's IKE Configuration tab in the VPN Group Configuration dialog box (using CompatiView) or in the [VPN Group<Name>] section of the configuration (using the command line).*

### VPN Encryption Password Window



This window will appear only if the **EncryptPasswords** keyword has been set in the [VPN Users] section. The VPN Encryption Password should be an alphanumeric string no more than 60 characters in length.

This keyword should be used in conjunction with the **SaveSecrets** keyword in the [VPN Group<Name>] section. For more information on the **EncryptPasswords** keyword, see *Creating a VPN Client Config File*.

❖ **Note:** *Do not lose this password. This password is not saved on the system. If it is forgotten, the user will have to delete the Shared Key in the [VPN User] section, and start over.*

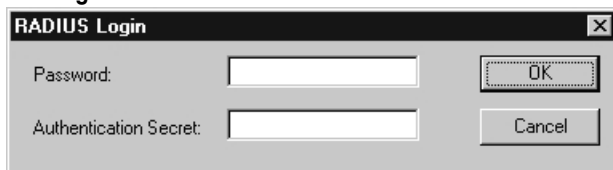
### Prompt for Secret Window



This window is accessed by clicking on the **Connect** button in the Connections tab. This window will only appear if this is the first time the user has connected to the IntraPort VPN Access Server or if the VPN Group configuration in the Server requires it.

**Shared Secret.** This is the user's shared secret. This must match the user's **Shared Secret** configured in the IntraPort VPN Access Server.

### RADIUS Login Window



This window will appear after the Prompt for Secret window, if this is the first time you have connected to the IntraPort VPN Access Server or

## 20 Chapter 2 - Installing and Running the Windows and Mac OS Clients

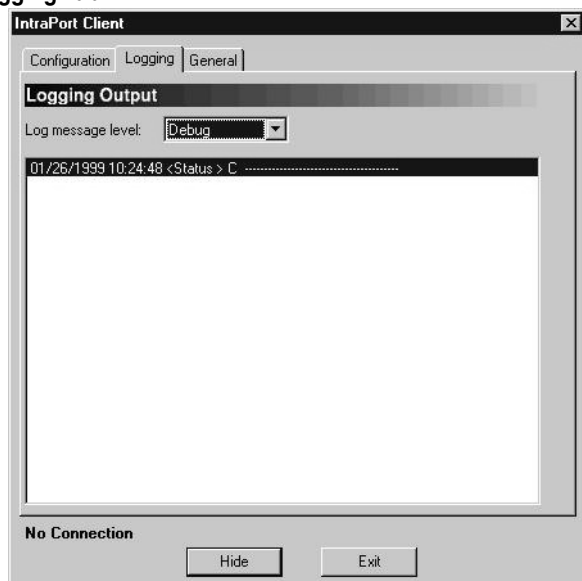
---

if the VPN Group configuration in the Server requires it.

**Password.** This is the RADIUS secret for this login. This must match the secret configured in the RADIUS server.

**Authentication Secret.** This box will only appear if the RADIUS server uses PAP for authentication instead of CHAP. This must match the **PAP Auth Secret** configured in the IntraPort VPN Access Server's RADIUS section.

### Logging Tab



The Logging tab displays statistics and tunnel connection logs for troubleshooting purposes.

**Log message level.** This pull down menu determines the detail of messages logged. The log information is displayed in the window below. The **Debug** level reports every action of the device and should not be used on a day-to-day basis since it generates a large number of log messages. However, it can provide detailed information about the connection conversation between the VPN Client and the IntraPort VPN Access Server.

### VPN Client Icon and the Windows Task Bar



VPN Client Icon



VPN Client Icon in the Windows Tool Tray

If you are using a Windows machine, the VPN Client Icon will appear in the Windows tool tray. Once a tunnel connection has been established, the Client Icon will turn into a globe and begin spinning. Right clicking on the VPN Client icon in the Windows task bar activates the following pull-down menu.



Windows Task Bar Pull-Down Menu

**Open** brings up the VPN Client window.

**Exit VPN Client** exits the Windows VPN Client and can only be selected if the VPN Client window is closed.

### VPN Client Mac OS Pull-down Menu



Mac OS Pull-Down Menu

If you are using a Macintosh, a File menu will appear at the top of the screen.

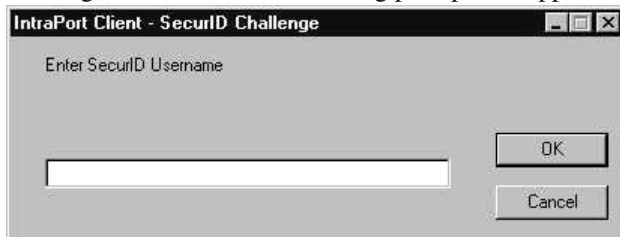
**Close** closes the VPN Client window.

**Quit** exits the Mac OS VPN Client.

## Using SecurID with the VPN Client

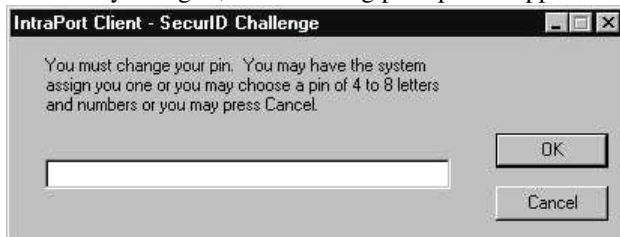
Client configurations which have been set up to use SecurID will have several special user prompts.

If the VPN Client Configuration in the IntraPort VPN Access Server has been set up so that the SecurID user name is different from the IntraPort login name, then the following prompt will appear:



SecurID UserName Entry Dialog Box

The first time you log in, the following prompt will appear:



SecurID New PIN Entry Dialog Box

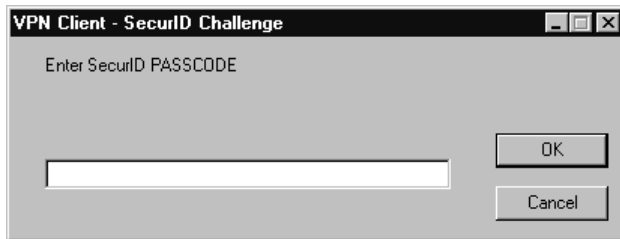
You may either enter a PIN and click OK or leave the edit box blank and click Cancel in order to have the system generate a PIN. If the system generates the PIN, the following prompt will appear:



System-Generated SecurID PIN Dialog Box

You must memorize or otherwise note the PIN before clicking OK.

If this is not the first time you have logged in, the following prompt will appear:

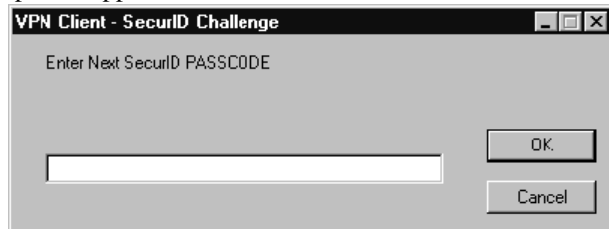


Enter PASSCODE Dialog Box.

The PASSCODE consists of your PIN plus the current code from the user's SecurID token.

If the PASSCODE is accepted, a client tunnel is created and the globe starts spinning. On a Macintosh, the globe is in the upper right-hand corner of the VPN Client window. On a Windows machine, the globe is in the Windows task bar.

If the PASSCODE is unacceptable for some reason, the following prompt will appear:



Next PASSCODE Dialog Box

You must wait until the token code changes from the one just entered and then try again. If the PASSCODE is still unacceptable, the following prompt will appear:

SecurID access denied.

You may try again or you may need to contact the system administrator for assistance.

## 24 Chapter 2 - Installing and Running the Windows and Mac OS Clients

---

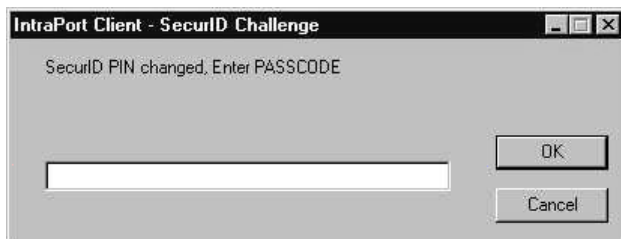
The administrator may set the SecurID server to require users to change their PINs. If that is the case, then the following prompt will appear:



SecurID Change PIN Dialog Box

You may either enter a PIN and click OK or leave the edit box blank and click Cancel in order to have the system generate a PIN. If the system generates the PIN, you must memorize or otherwise note the PIN before clicking OK.

You will then be prompted for the new PASSCODE by the following prompt:



SecurID PASSCODE Entry Dialog Box

If the PASSCODE is accepted, a client tunnel is created and the globe starts spinning.

# Chapter 3 - Installing and Running the Linux and Solaris Clients

Both the Linux and Solaris VPN Clients require the use of a client config file, which was documented earlier in *Creating a Client Config File*. The installation procedures are similar for both, although there are subtle differences between the two clients so they have been documented separately. Establishing tunnel sessions and other application commands are nearly identical so they have been documented together for both clients.

## Installing the Linux VPN Client Software

This set of instructions will help guide you through the installation of the Linux VPN Client. It assumes you are familiar with Linux and have installed other software applications.

### Linux VPN Client Overview

The Linux VPN Client consists of two discrete parts.

- The driver, which is a loadable module
- A command line interface

The command line interface and some parts of the driver are distributed in binary form only. The command line interface, as a regular user mode program, has little dependence on particular distributions of Linux.

#### System Requirements

The Linux Client requires the following.

- Linux kernel 2.0.36 or 2.2.5-15 (Intel)

The Linux kernel must support loadable modules. The Compatible Systems Linux Client has only been tested with Red Hat 5.2 and 6.0 Linux using kernel versions 2.0.36 and 2.2.5-15, respectively.

## Unpacking the Linux Client Files

The Linux VPN Client is provided as a compressed tar file. To unpack the files after downloading them into a temp folder, copy the Linux VPN Client file to a directory. Unpack the files using the `zcat` and `tar` commands.

Example:

```
zcat COMPvpn-Linux-2.2.5-15-i686-991013-v3.30.tar.z | tar
xvf -
```

This will create a directory called `COMPvpn` in the chosen directory.

## Installing the VPN Client Files

You will need to login as root or SuperUser to run the install script.

If a machine has had the Linux VPN Client previously installed, it is recommended that you remove the old client before installing the new one.

To install the files needed for the Compatible Systems VPN Client type the following commands, in the order given:

1. Type the following commands, in the order given:

```
cd COMPvpn
./vpn_install
```

2. At the prompt for what directory to install the VPN Client applications, you can either use the default directory (`usr/local/bin`), choose a directory in your user's path or make sure the directory is in your user's path.

After installation, you should either reboot or issue the `/etc/rc.d/init.d/vpn start` command to enable the VPN service. To disable it, issue the `/etc/rc.d/init.d/vpn stop` command.

### About the Linux Client Install Script

During the installation process, the module is compiled and linked and then copied to either the directory `/lib/modules/preferred/COMPvpn`, if it exists, or to `/lib/modules/"system"/COMPvpn`. The application binaries are copied to the specified destination directory.

The startup file `/etc/rc.d/init.d/vpn` is created to enable and disable the VPN service. The links `/etc/rc3.d/S85vpn` and `/etc/rc5.d/S85vpn` are added to run level 3 and run level 5. This allows the tunnel server to start up at boot in run levels 3 and 5.

## Installing the Solaris Client Software

This set of instructions will help guide you through the installation of the Solaris VPN Client. It assumes you are familiar with Solaris and software applications.

The Solaris VPN Client software will run on any Sparc™ machine running a 32 bit Solaris OS 2.5.1 or later.

Some Solaris machines run a 64 bit kernel by default. In order to use the Solaris VPN Client, you must run the 32 bit version of the kernel. One way to do this is to specify `kernel/unix` as the boot file as in the following example:

```
ok boot kernel/unix
```

You can then install the client using the instructions which follow.

To run the client, you will have to repeat this step each time you reboot, or else you can change the setting permanently in the EEPROM. (See your Solaris documentation for information on the EEPROM.)

## Unpacking the Solaris Client Files

The Solaris VPN Client is provided as a compressed tar file. To unpack the files after downloading them into a temp folder, copy the Solaris VPN Client file to a directory. Unpack the files using the `zcat` command.

Example:

```
zcat COMPvpn-SunOS-5.7-sun4u-991013-v3.30.tar.z | tar xvf -
```

This will create a directory called `COMPvpn` in the chosen directory.

## Installing the Solaris Client Files

You must be logged on as root in order to install or remove the Solaris files. To install the files needed for the Compatible Systems VPN Client:

1. Type the following command:  

```
pkgadd -d . COMPvpn
```
2. At the prompt for what directory to install the VPN Client applications, you can either use the default directory (by hitting Enter), choose a directory in your user's path or make sure the directory is in your user's path.
3. You will also be prompted for what Ethernet adapter to use. The default of `hme` is appropriate for 100 Mbps Ethernet devices. It

should be changed to 1e for 10 Mbps Ethernet devices.

4. Answer Yes to any other prompts to complete the installation.
5. Reboot the machine.

#### About the Solaris Client Install Script

During the installation, the line

```
hme -1 0 vpnmod
```

is added to the `/etc/iu.ap` file in order to enable the autopush facility at startup. The module is copied to the `/kernel/strmod` directory which is in the system's module search path.

A vpn service startup script, `/etc/rc3.d/S85vpn`, is added to run level 3. This allows the tunnel server to start up at boot in run levels 3.

To uninstall a package, the `pkgrm` command is used:

```
pkgrm COMpvpn
```

The `pkginfo` command gives information about installed packages.

For more information on other useful package-related commands, type:

```
man pkgadd.
```

## Establishing Tunnel Sessions

The Linux and Solaris VPN Clients are launched from a shell. To create a VPN tunnel, the **open\_tunnel** application must be started with a valid client config file in the directory `/etc/vpn_config`. (Information on the required content of the client config file is given in *Creating a Client Config File*).

Type a command with the following format for the `open_tunnel` application:

```
open_tunnel <IntraPort IP address> <user name>
```

## Linux and Solaris Operational Commands

This section of the manual documents all of the commands of the Linux and Solaris VPN Client software.

### open\_tunnel Command

Usage: **open\_tunnel** [-e] [-n] [-r] [-d hme | le | eth0] [-h] <IntraPort IP address> <user name>

- e** Exclude Local LAN.
- n** Enable NAT transparency mode.
- r** Use RADIUS.
- d hme | le | eth0** Specifies the Ethernet type (hme or le for Solaris, eth0 for Linux).
- x** Increase debug level.
- h** Shows this help message.

This command establishes an active tunnel to the specified IntraPort VPN Access Server IP address for the specified user.

The -e option (Exclude Local LAN) indicates that local LAN traffic will not be tunneled. Because this is a less secure option, this will only work if the VPN Group configuration in the IntraPort VPN Access Server also has the **ExcludeLocalLAN** keyword enabled. This feature can also be set using the [VPN Users] section of the configuration file.

The -n option enables NAT (Network Address Translation) for client sessions. If there are problems connecting through a NAT device or through an ISP, checking this box may help by using the HTTP protocol for the session. This feature can also be set using the [VPN Users] section of the configuration file.

❖ **Note:** *If the -n option is enabled, then the VPN Group configuration for this user must have an ESP transform set and it must be listed before any AH transforms in the configuration. The transforms (i.e., IKE protection pieces) are set in the IntraPort Server's IKE Configuration tab in the VPN Group Configuration dialog box (using CompatiView) or in the [VPN Group<Name>] section of the configuration (using the command line).*

The default device type is hme.

Example: `open_tunnel 198.162.16.155 hopper`

Terminating the `open_tunnel` command with Ctrl-C will close the tunnel.

`close_tunnel` Command

## 30 Chapter 3 - Installing and Running the Linux and Solaris Clients

---

Usage: **close\_tunnel** [-d hme | le | eth0] [-h]

**-d hme | le | eth0** Specifies the Ethernet type (hme or le for Solaris, eth0 for Linux).

**-h** Shows this help message.

This command closes the active tunnel.

---

## Chapter 4 - Creating a VPN Client Config File

This section of the manual describes how to set up a configuration file that resides on the host directory and can be used as a template for remote users.

A config file is required for the Linux and Solaris clients and is automatically created as part of the client installation process.

For the Windows and Mac clients, setting up a config file is optional. A config file allows the administrator to manage the IP addresses, password, and secrets that are disclosed to remote users.

The file can be created with any text editing program, but it must be saved as a plain text file, without any file extension.

For Windows, the file must be named “vpn\_config” and reside in the directory the client application was installed in (usually C:\Program Files\IntraPort Client).

Administrators (Windows only) may also distribute a customized configuration file for each user. This ‘pre-configured’ vpn\_config file must be saved in the OEM directory that was created for that user. For more information on the OEM directory, see Customizing the Logo.

For Mac OS, the file must be named “VPN Client Preferences” and reside in the preferences directory.

For Linux and Solaris, the created file is named “/etc/vpn\_config”. This file must be edited and customized for the local environment.

Examples:

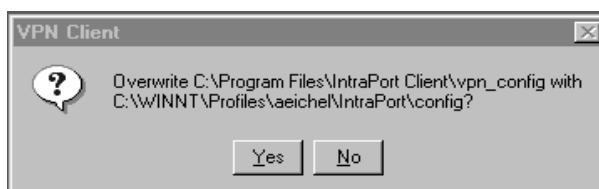
```
NT      C:\WINNT\Program files\IntraPort Client\vpn_config
Win 95/98  C:\WINDOWS\Program files\IntraPort Client\vpn_config
Macintosh  System Disk:System Folder:Preferences:IntraPort Client Preferences
Linux and Solaris:/etc/vpn_config
```

### Exiting the VPN Client

A vpn\_config file is created each time the user exits the VPN Client program. This file is created and saved in the same directory the client application was installed in (usually C:\Program Files\IntraPort Client),

even if it has been moved to another directory.

The `vpn_config` is overwritten each time the client is used, unless otherwise specified. Each time the user exits the VPN Client, a prompt will appear:



Under normal circumstances, the user should answer *No* to this prompt. This is crucial if there is more than one user utilizing the same `vpn_config` file. There is only one `vpn_config` file per machine, but there can be multiple users.

## Section Names

The `vpn_config` file has three valid section names, **[VPN User]**, **[VPN Partner Alias]**, and **[VPN General]**. The section names are not case sensitive.

### [VPN Partner Alias]

This section is used for aliasing IntraPort IP addresses to a text string that has some meaning to the user. This section has no keywords. *Alias Name* is case sensitive.

*<Alias Name> = IP Address*

*Alias Name* is any text string less than 80 characters. The *IP Address* is a valid IP address of an IntraPort VPN Access Server to which the client may connect. Domain names are not allowed.

### [VPN Users]

This section of the configuration defines the IntraPort VPN Access Server users' login information. If there is a parsing error in the configuration text file, then the user will not appear in the Client GUI.

Keywords recognized in this section are described below.

**UserName** = *string*

The **UserName** keyword identifies a unique user. This name must also be configured in the IntraPort VPN Access Server and/or an authentication service it is using (e.g., RADIUS, SecurID, etc.). See

the Reference Guide for your IntraPort VPN Access Server for more information on how to set up an authentication service to work with your device.

The string may be between one and 60 alphanumeric characters. If the string contains spaces or other special characters, it must be enclosed in quotes. This entry must always be the first on the line.

**IPPrimary** = *<Alias Name> | <IP address> | <domain name>*

The **IPPrimary** keyword sets the alias name, IP address or fully qualified domain name of the IntraPort VPN Access Server that the client software will connect to.

**IPSecondary** = *<Alias Name> | <IP address> | <domain name>*

The **IPSecondary** keyword sets the alias name, IP address or fully qualified domain name of the IntraPort VPN Access Server that the client software will connect to if the primary IntraPort is unreachable.

**SharedKey** = *<pass phrase>*

The **SharedKey** keyword sets the shared secret for this user. The pass phrase is used to generate session keys which are then used to authenticate and/or encrypt each packet received from or sent to the Client. This must match the **Shared Key** configured for this user in the IntraPort VPN Access Server.

**RADIUSPassword** = *string*

The **RADIUSPassword** keyword should be set to match the user's secret or password configured in the RADIUS server.

**PAPAuthSecret** = *<pass phrase>*

The **PAPAuthSecret** keyword sets a secret to be used by the IntraPort VPN Access Server and Client to authenticate and encrypt packets exchanged between them before they are passed on to the RADIUS server. This is only used if the RADIUS server uses PAP for authentication instead of CHAP. This must match the **PAP Auth Secret** configured in the IntraPort VPN Access Server's RADIUS section.

**IPEnabled** = [ TRUE | FALSE | 1 | 0 ]

When the **IPEnabled** keyword is TRUE, or 1, then IP-in-IP tunneling to the **IPNet** configured in the IntraPort VPN Access Server.

**IPXEnabled** = [ TRUE | FALSE | 1 | 0 ]

When the **IPXEnabled** keyword is TRUE, or 1, then IPX connections to IPX servers will be enabled during Client sessions.

**NetBTEnabled** = [ TRUE | FALSE | 1 | 0 ]

When the **NetBTEnabled** keyword is TRUE, or 1, then Microsoft

networking functionality over IP transport will be enabled during Client sessions.

**ExcludeLocalLAN** = [ TRUE | FALSE | 1 | 0 ]

When the **ExcludeLocalLAN** keyword is TRUE, or 1, then local LAN traffic will not be tunneled. Because this is a less secure option, this will only work if the VPN Group configuration in the IntraPort VPN Access Server also has the **ExcludeLocalLAN** keyword enabled.

For the Linux and Solaris clients, this feature can also be set using the `-e` parameter with the `open_tunnel` command.

**UsefTCP** = [ TRUE | FALSE | 1 | 0 ]

When the **UsefTCP** keyword is TRUE, or 1, then NAT (Network Address Translation) will be enabled for client sessions. If there are problems connecting through a NAT device or through an ISP, enabling this feature may help by using the HTTP protocol for the session.

For the Linux and Solaris clients, this feature can also be set using the `-n` parameter with the `open_tunnel` command.

❖ **Note:** *If UsefTCP is enabled, then the VPN Group configuration for this user must have an ESP transform set and it must be listed before any AH transforms in the configuration. The transforms (i.e., IKE protection pieces) are set in the IntraPort Server's IKE Configuration tab in the VPN Group Configuration dialog box (using CompatiView) or in the [VPN Group<Name>] section of the configuration (using the command line).*

### [VPN General]

This section is used for setting the general operations of the VPN client. These settings will affect every user in the `vpn_config` file. Currently, the password encryption operation is on a 'per VPN User' basis.

Keywords recognized in this section are described below.

**EncryptPasswords** = [ TRUE | FALSE | 1 | 0 ]

When **EncryptPasswords** keyword is TRUE or 1, the Shared Key, RADIUSPassword, and PAPAuthSecret pass phrases will be encrypted for every user in the `vpn_config` file. This will cause the user to be prompted for an encryption password when trying to connect.

**TallyBytes** = [ TRUE | FALSE | 1 | 0 ]

When **TallyBytes** keyword is TRUE or 1, the number of bytes

tunneled by each user is recorded and displayed. The byte count is recorded in the `vpn_config` file for each user with the keywords `RXBytes` and `TXBytes` in the `[VPN User]` section.

The byte counts for the connected user are displayed on the General tab. The displayed values are for the current session and only valid when a user is connected.

❖ **Note:** *The byte count is accumulated 'per-session' in the `vpn_config` file. Clicking the reset button on the General tab will set the byte counts back to zero.*

## Sample VPN Client Config File

The following example shows what the text config file would look like for IntraPort VPN Access Server user FFlintstone, who needs to be able to dial in to both a central office and a warehouse.

```
[VPN Partner Alias]
L.A. Office = 192.168.72.8
Central Warehouse = 204.172.14.183

[VPN Users]
UserName = FFlintstone
IPPrimary = L.A. Office
SharedKey = Wilma
RADIUSPassword = Pebbles
IPEnabled = True
NetBTEnabled = True

[VPN Users]
UserName = FFlintstone
IPPrimary = Central Warehouse
SharedKey = Dino
RADIUSPassword = GreatGazoo
IPEnabled = True
NetBTEnabled = True

[VPN General]
EncryptPasswords = True
TallyBytes = True
```

## Appendix A - Uninstalling the Windows NT VPN Client

Before installing a new version of the Windows NT VPN Client, any older versions of the Client must be uninstalled. The Unwise program which is included with the VPN Client software (located in the IntraPort Client folder) should be used to uninstall the Client. If for some reason there is no Unwise program, then the Windows uninstaller (under Control Panel>Add/Remove Programs) can be used.

Neither the Unwise program for Windows NT Client version 2.x nor the Windows uninstaller program will automatically uninstall the Compatible driver, so you must remove it yourself. To remove the driver:

1. Go to Control Panel>Network and click on the Protocols tab.
2. Select the Compatible Systems VPN Transport driver.
3. Click on the Remove button.
3. Reboot the computer.

Now you may install the client (see Installing the Windows NT VPN Client Software).

❖ **Note:** *The Unwise program included with the Windows NT Client versions 3.x and greater will automatically remove the driver, so these additional steps are not necessary.*

## Appendix B - Manually Installing the Windows NT VPN Network Driver

The Windows NT Client setup program automatically launches a macro which should install the IntraPort VPN Access Server network driver (see Installing the Windows NT VPN Client Software for more information on the setup program and macro.) The Windows NT system requires that an IntraPort network driver be installed before the VPN Client will work. If the macro fails for any reason, you may use the following instructions to manually install the driver.

1. Install Windows NT VPN Client software (see Installing the Windows NT VPN Client Software for more information).
2. Log on to the NT system as Administrator.
3. Open “My Computer,” then “Control Panel.” Double-click on “Network.”
4. Click on the “Protocols” tab and then click on “Add.”
5. When the “Select Network Protocol” dialog box comes up, click on “Have Disk.”
6. Fill in the path to the Windows NT folder you copied or downloaded the files to earlier (i.e., C:\temp). Then click “OK.”
7. When the “Select OEM Option” dialog box comes up, “Compatible Systems VPN Intermediate Driver” should be highlighted. Click “OK” to begin installing the driver.
8. After the driver is installed, click “Close” in “Network.”
9. NT will display a message letting you know that your machine needs to be restarted. Click “Now.”

**38 Appendix B - Manually Installing the Windows NT VPN Network Driver**

---