

IntraPort 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>

IntraPort Client Software Reference Guide
Version 1
Copyright © 1999, Compatible Systems Corporation

All rights reserved. IntraPort Enterprise, 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.

IntraPort Client Software Installation and Configuration Instructions **1**

ABOUT THIS MANUAL	1
INTRODUCTION TO THE INTRAPORT CLIENT SOFTWARE	1
INTRAPORT CLIENT SOFTWARE INSTALLATION	2
Installing the Windows 95/98 IntraPort Client Software	2
Installing the Windows NT IntraPort Client Software	2
Installing the Windows NT IntraPort Network Driver	2
Installing the Mac OS IntraPort Client Software	3
RUNNING THE INTRAPORT CLIENT SOFTWARE	4
INTRAPORT CLIENT SOFTWARE REFERENCE	5
IntraPort Client Properties Window	5
General Tab Settings	5
Configuration Tab Options	6
User Properties Window	7
Diagnostics Window Settings	9
IntraPort Client Icon and the Windows Task Bar	10
IntraPort Client Mac OS Pull-down Menu	10
USING SECURID WITH THE INTRAPORT CLIENT	11

IntraPort Client Software Installation and Configuration Instructions

About This Manual

This manual documents Compatible System's IntraPort Client software, v2.5 for Windows and v2.2 for Mac OS. It is divided into two main sections: installation instructions and configuration of user accounts.

Introduction to the IntraPort Client Software

The IntraPort Client software is the same for all Compatible Systems IntraPort VPN Access Servers. While the configuration screens are nearly identical for all supported client platforms, the installation instructions vary depending on client platform and operating system.

❖ **Note:** *To assist remote users with the installation and setup of the IntraPort Client, this information is also available in the technical support section of the Compatible Systems website at:*
<http://www.compatible.com/>

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).

You may obtain the IntraPort Client software in any of the ways noted below, depending on the preference/policy of your organization. Check with your network administrator if you have questions about obtaining client software.

- On the CD-ROM which was shipped with your Compatible Systems networking device.
- 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, and click on the appropriate file to download it.

❖ **Note:** *These files are also accessible directly via Anonymous FTP at <ftp.compatible.com/files/>.*

IntraPort Client Software Installation

Installing the Windows 95/98 IntraPort Client Software

The Windows 95/98 IntraPort Client software will run on any machine with a 486 or faster processor.

To install the Windows 95/98 Client from the CD-ROM:

1. Insert the CD-ROM and open the Windows 95 folder in the IntraPort Access Servers/IntraPort Clients directory.
2. Run the Setup program by double-clicking on it. The setup program will transfer all necessary files to the destination volume of your choice.

To install the Windows 95/98 Client after downloading to a local disk or your hard drive, simply run the Setup program by double-clicking on it. The setup program will transfer all necessary files to the destination volume of your choice.

Installing the Windows NT IntraPort Client Software

The Windows NT Client software requires Windows NT 4.0 with Service Pack 3 or later and Remote Access Service installed. If Remote Access Service is not installed, you must install it before the client will work.

To install the Windows NT Client from the CD-ROM:

1. Insert the CD-ROM and open the Windows NT folder in the IntraPort Access Servers/IntraPort Clients directory.
2. Copy the files in the folder to a temporary folder on your hard drive (i.e. C:\temp).
3. Run the IPClientNT program by double-clicking on it. The setup program will transfer all necessary files to the destination volume of your choice.

To install the Windows NT Client after downloading it into a temp folder, simply run the IPClientNT program by double-clicking on it. The setup program will transfer all necessary files to the destination volume of your choice.

Installing the Windows NT IntraPort Network Driver

In addition to the Client software, the Windows NT system also requires that an IntraPort network driver be installed before the IntraPort Client will work.

1. Install Windows NT 4.0 Service Pack 3 or later. **Even if Service Pack 3 or a later Service Pack is on the system you should reinstall it.** Other network-related installations may have overwritten older versions of files contained in the Service Pack.

❖ **Note:** *The NT driver attempts to ensure that Service Pack 3 or later has been installed on the system in order to avoid system instability. Running the NT driver with earlier files (that may have been recopied by other installations) can result in system problems.*

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 STEP 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."

Installing the Mac OS IntraPort Client Software

The Mac OS IntraPort 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 from the CD-ROM:

1. Locate the CD-ROM which was included with the IntraPort VPN Access Server. Insert the disk and open the Macintosh folder in the IntraPort Access Servers/IntraPort Clients directory.
2. Run the MacClient.sea.hqx program by double-clicking on it (you will need a program such as StuffIt or BinHex to expand it).
3. Select a destination for the self extracting archive, then click "Save."
4. Go to the selected destination and double-click on the self extracting archive. The installation program will allow you to drag the IntraPort Client software to the computer system's hard disk.
5. After the installation is complete, a dialog box will open which allows you to restart your computer. Click "Restart."

To install the Mac OS Client after downloading to a diskette or your hard drive:

1. Run the MacClient.sea.hqx program 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 IntraPort 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."

Running the IntraPort Client Software

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

First, you will need to set up a user configuration.

1. Double click on the IntraPort Client icon. The IntraPort Client Properties window will open.
2. Click on the Configuration tab.
3. Click on the Add button. The User Properties window will open.
4. Enter appropriate user login parameters. Much of the information required should be provided by your network administrator. At a minimum, you need:
 - User Name
 - Primary IP Address (of the IntraPort VPN Access Server you will be logging into.)
 - Tunnel Management information, which will vary depending on the management Method chosen (by selecting either Manual or RADIUS from the pull-down menu).
 - A. If the Method is Manual, you will need to enter the following:
 - Authentication Secret
 - Encryption Method
 - Encryption Secret (required if PLE, DES or 3DES was selected as the Encryption Method)
 - B. If the Method is RADIUS, you will need to enter the following:
 - Login Password
 - Encryption Method
 - Tunnel Secret
5. Click OK.

You may repeat this process to add multiple user configurations. To establish a tunnel session:

1. Double click on the IntraPort Client icon. The IntraPort Client Properties window will open.
2. Click on the Configuration tab.
3. Select a user configuration by clicking on it.
4. Click on the Connect button. On Windows machines, the IntraPort Client icon in the Windows task bar becomes a globe and starts spinning when connected. On Mac OS machines, the globe icon in the upper right corner of the IntraPort Client Properties window spins when connected.

❖ **Note:** *When the IntraPort 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 routed as normal.*

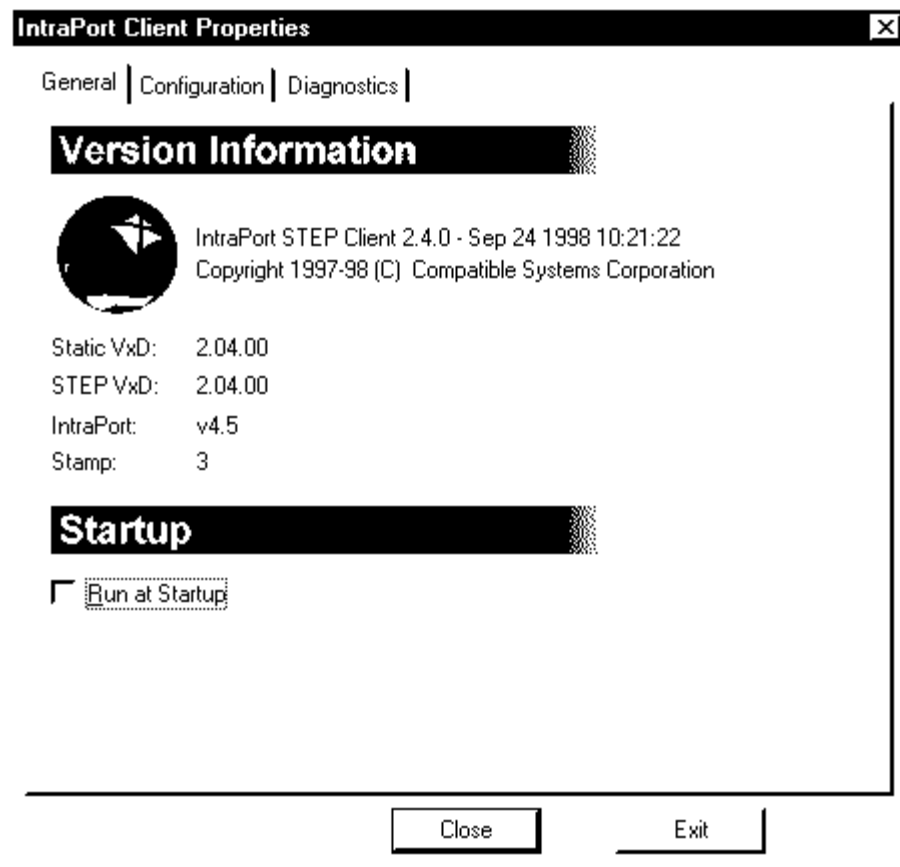
IntraPort Client Software Reference

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

IntraPort Client Properties Window

This window's three tabbed sections allow you to set up user configurations and set other client parameters.

General Tab Settings

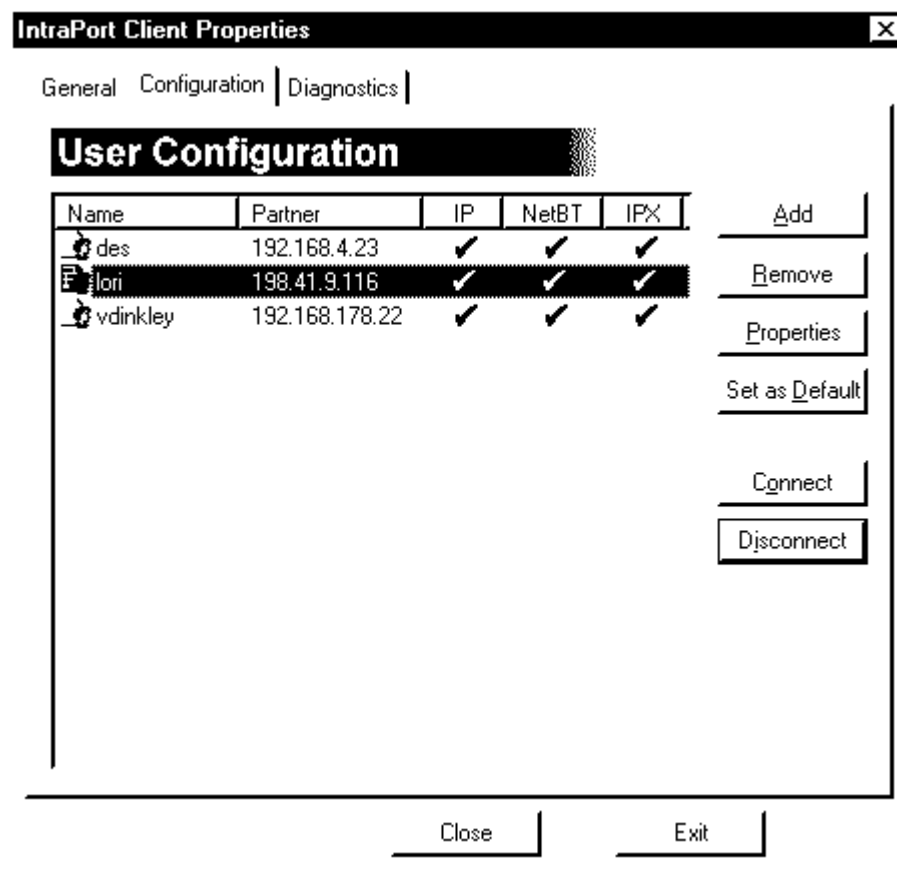


This tab displays IntraPort Client information and determines whether a connection will be attempted upon startup of the host computer.

Run at Startup (default = unchecked). When this box is checked, the IntraPort Client software will attempt to establish a tunnel for the default configuration automatically each time its host computer is started.

The IntraPort Client software or a shortcut to it must also be placed in the Startup Items folder in the System Folder (for Mac OS) or the StartUp folder under Windows/Start Menu/Programs (for Windows). This option is typically left unchecked so that client tunnels will only be established when needed.

Configuration Tab Options



The Configuration tab contains a list of user configurations.

Add. This button allows you to add a set of user login parameters.

Remove. This button allows you to remove a set of user login parameters.

Properties. This button allows you to edit the selected set of user login parameters.

Set as Default. If the **Run at Startup** box is checked, then this button marks the selected login to be run when the IntraPort client is loaded. That set of login parameters will also be selected when the screen is opened.

Connect. This button attempts to establish a secure tunnel to an Intraport server using the selected set of login parameters. On Windows machines, the IntraPort Client icon in the Windows task bar becomes a globe and starts spinning when connected. On Mac OS machines, the globe icon in the upper right corner of the IntraPort Client Properties window spins when connected.

Disconnect. This button disconnects an active tunnel session. When disconnected, the globe icon stops spinning.

User Properties Window

This window is accessed by selecting either the **Add** or **Properties** buttons in the Configuration tab.

Manual Login

User Name. Enter the name of the tunnel user. This name must also be configured in the IntraPort VPN Access Server.

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

Secondary IP Address. 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.

Method. Select a login method to be used. If the **Manual** method is used, the IntraPort VPN Access Server performs user authentication. The **RADIUS** method allows a RADIUS server to be used

User Properties

User Name:

Primary IP Address:

Secondary IP Address:

Tunnel Management

Method:

Prompt for Secrets

Login Password:

Encryption Method:

Tunnel Secret:

Tunneling

Enable IP

Enable NetBT

Enable IPX

RADIUS Login

Prompt for Secrets. (default = unchecked). When this box is checked, the user will have to enter his or her passwords and/or secrets prior to establishment of a tunnel.

If the client is unable to connect to the IntraPort because of authentication problems, it will prompt the user to enter a new password or secret. This prevents a tunnel being established by an unauthorized user.

If the box is not checked, the passwords and secrets entered below are saved on the user's hard disk. In this case, the user doesn't have to enter the secret each time before a connection is established.

Authentication Secret. This field appears only when Manual has been selected. Enter the desired authentication secret here. This must match the **Authentication Secret** field configured in the IntraPort VPN Access Server using CompatiView (or the value configured for the **Auth** keyword in the [**STEP Users**] section using text-based configuration).

Login Password. This field appears only when RADIUS has been selected. Enter the login server password here. This must match the password configured in the RADIUS server's user database.

Encryption Method (default = fixed). This pull-down menu selects whether an encryption algorithm is used.

If **None** is selected, then the tunnel session will be sent in the clear in both directions.

If **Fixed** is selected, then Personal Level Encryption will be used to scramble the data in both directions using a fixed key.

If **PLE** is selected, then Personal Level Encryption will be used to scramble the data in both directions using a key generated from the encryption secret (see below).

If **DES** is selected, then the DES algorithm will be used. DES provides better security than PLE, but also requires more time to operate. If **3DES** is selected, then triple DES encryption will be used.

Encryption Secret. This field appears only when **Manual** has been selected. Enter the desired encryption secret here. This must match the **Encryption Secret** field configured in the IntraPort using CompatiView (or the value configured for the **Encrypt** keyword in the [**STEP Users**] section using text-based configuration).

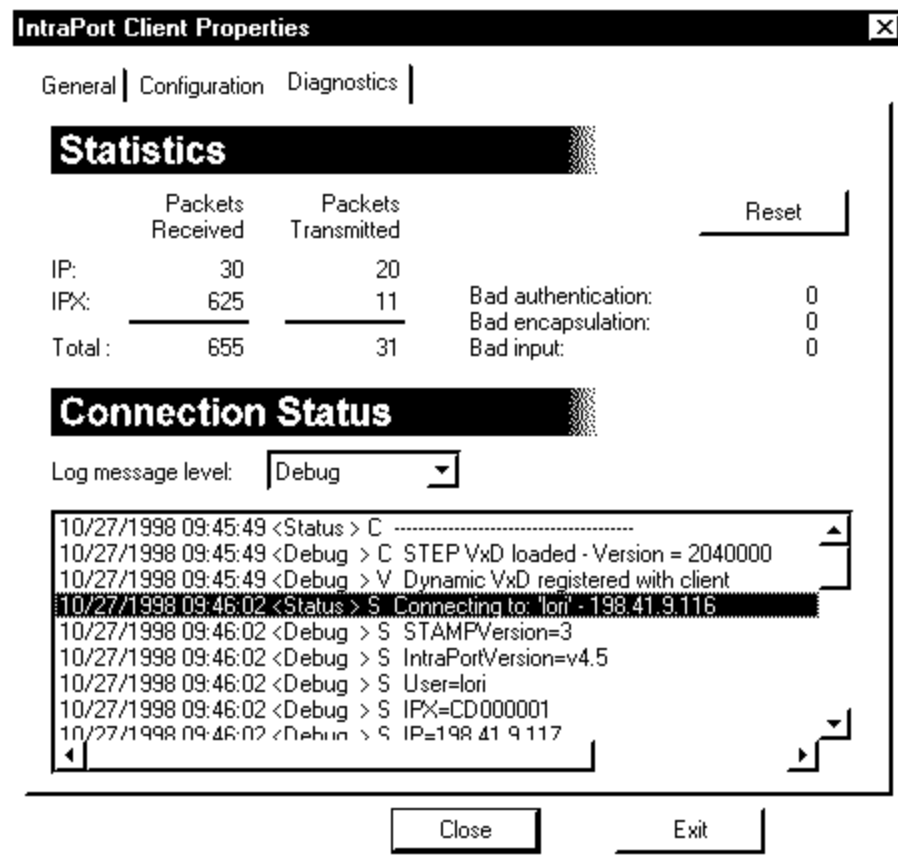
Tunnel Secret. This field appears only when **RADIUS** has been selected. Enter the tunnel secret here. This must match the **Tunnel Secret** field which was entered in the RADIUS server's user database.

Enable IP (default = checked). IP must be enabled for the client to tunnel IP-in-IP to the **IPNet** configured in the IntraPort VPN Access Server.

Enable NetBT (default = checked). This box enables Microsoft networking functionality over IP transport (Windows only).

Enable IPX (default = checked). IPX must be enabled in order to connect to IPX servers at the central site (Windows only).

Diagnostics Window Settings



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

Reset. This button clears out the displayed statistics.

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 client and the IntraPort VPN Access Server.

IntraPort Client Icon and the Windows Task Bar



IntraPort Client Icon



IntraPort Client Icon in the Windows Tool Tray

If you are using a Windows machine, the IntraPort 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 IntraPort Client icon in the Windows task bar activates the following pull-down menu.

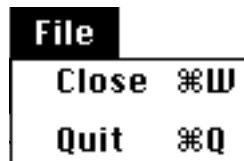


Windows Task Bar Pull-Down Menu

Open brings up the IntraPort Client Properties window.

Exit STEP Client exits the Windows IntraPort Client and can only be selected if the IntraPort Client Properties window is closed.

IntraPort 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 IntraPort Client Properties window.

Quit exits the Mac OS IntraPort Client.

Using SecurID with the IntraPort Client

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

If the Client configuration has been set up so that the SecurID user name is different from the IntraPort user name (using the **STEP Client Name** section), then the following prompt will appear:

Enter SecurID User Name.

The first time a user logs in, the following prompt will appear:

Enter your new SecurID PIN, containing 4 to 8 characters, or select OK to have the system generate a new PIN.

If the system generates the PIN, the user must memorize or otherwise note the PIN before clicking OK.

If this is not the first time a user has logged in, the following prompt will appear:

Enter SecurID PASSCODE.

The PASSCODE consists of the user's 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 IntraPort 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:

Enter Next SecurID PASSCODE.

The user 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.

The user may try again or may need to contact the system administrator for assistance.