Stac

USER'S GUIDE

REACHOUT®

for
Microsoft® Windows NT®

Your serial number is on the back of your ReachOut CD-ROM case.
Write this number on your Product Registration card before you mail it.

Limitation of Liability

The information contained herein is subject to change without notice. Stac, Inc. reserves the right to make changes to any product herein to improve its functioning or design. Although the information in this document has been carefully reviewed and is believed to be reliable, Stac, Inc. does not assume any liability arising out of the application or use of any product described herein. Stac, Inc. does not authorize the use of the product as a critical component in a life support system where a malfunction or failure of the product may reasonably be expected to result in significant injury or threaten life. The inclusion of Stac, Inc. products in life support systems applications implies that the user assumes all risk of such use and in so doing indemnifies Stac, Inc. against all damages.

Acknowledgements

01908 (12/96)

ReachOut

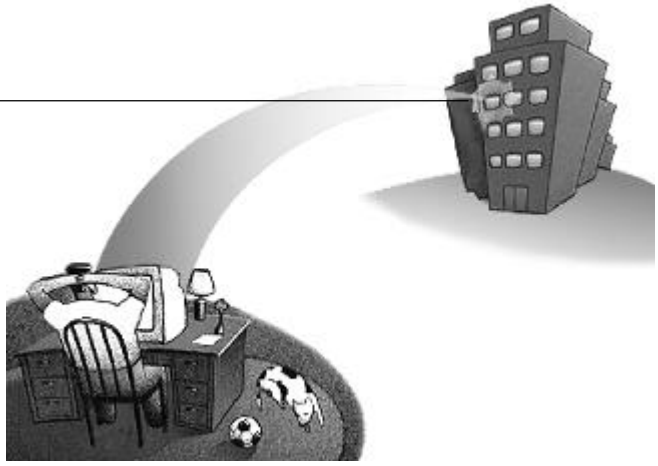
TABLE OF CONTENTS

1 ReachOut INTRODUCTION

Welcome to ReachOut!

Can't make it to the office today? No problem. Get your work done wherever you are. With ReachOut®, you don't have to be at the office to be productive. Connect to your office computer from anywhere and work as if you were actually there.

The computer you want to connect to is ready and waiting for your call—wherever you are.



ReachOut must be running on the computer you want to connect to *(the computer waiting for calls)* and the one you're using to make the connection *(the computer making the call)*. Chapter 3, *Getting Connected*, explains how to connect using a modem, a local network or the Internet, a Dial-Up Networking connection, or FTP. Chapter 4, *Remote Access*, explains how to use ReachOut for remote control and ReachOut Explorer.

ReachOut at Home or the Office

Use your modem (regular or ISDN) and telephone line, your local network (NetWare, NetBIOS, or TCP/IP), the Internet, or a Dial-Up Networking connection to connect to any computer running ReachOut. If the computer is logged onto the network, use network resources as usual. If the computer is not logged onto the network, you can log it onto the network while connected.

You can connect to another Windows® 95 or Windows NT® computer directly using the Windows direct cable connection. You'll need a *null modem serial cable*. Chapter 3, *Getting Connected*, has more details.

ReachOut Away from Home or the Office

Put ReachOut on your laptop computer if you're going to be away from home or the office. Use your modem (regular or ISDN) to connect to a ReachOut computer that is waiting for your call. Or use the SuperFTP™ Client to exchange files with any FTP server.

ReachOut is also useful for providing technical support over modems and networks.

ReachOut Over the Internet

You can use ReachOut for remote control and file transfer when both computers are connected to the Internet.

If you are at a computer that can connect to the Internet but doesn't have ReachOut installed, ReachOut Passport™ makes it easy to download the components that let you access and control your computer at the office. Of course, your office webmaster must set this up in advance.

Note: Chapter 8, ReachOut Passport, *covers the use of ReachOut Passport. You can install Passport through SETUP if you like.*

What's Great? What's New?

ReachOut for Windows NT extends the features of ReachOut for Windows 95 to the newest platform. Here are some key features that make it easy for you to be even more productive:

- ✓ **Integrated with Windows NT User Manager.** ReachOut uses the established Windows NT user groups and user profiles to manage remote access and security.
- ✓ **Connect to a remote computer quickly and easily.** Create *connection icons* that include all the information you need to connect to another computer. To connect, just double-click an icon. Create as many connection icons as you want.
- ✓ **A single ReachOut window for worldwide communications.** One ReachOut window lets you connect to other ReachOut computers or allow connections to your computer.
- ✓ **Connect to multiple computers at once.** ReachOut lets you control or exchange files with several ReachOut computers at the same time.
- ✓ **Get up and running quickly.** Because your modems and networks are already set up, you don't have to waste time configuring them when you install ReachOut. Let Windows NT figure out how you can communicate, and you're ready to go.
- ✓ **Install and use ReachOut in minutes.** The Setup wizard helps install ReachOut. Once installed, the New Connection wizard is available to help you define your first connection.
- ✓ **Take advantage of all Windows functions.** Right-click a ReachOut connection icon to bring up context menus and have immediate access to frequently used commands.
- ✓ **Transfer files via FTP (File Transfer Protocol).** ReachOut provides an "Explorer-like" window to help you transfer data over the Internet. Use SuperFTP™ Client to connect to any FTP server on the Internet and transfer files with drag and drop.

- ✓ **Transfer files faster**. ReachOut uses improved modem protocol management (SmartStream) to reduce the amount of time it takes to transfer data over a modem. On average, you can transfer data 10 to 15 percent faster than with previous versions of ReachOut.
- ✓ **Connect to a DOS, Windows 3.1, Windows for Workgroups, or Windows 95 ReachOut computer as before.** Even if the remote computer has not been upgraded to the latest version of Windows, you can still connect and work as before with any computer running ReachOut 5.0 or later. (Computers running ReachOut under DOS cannot connect to ReachOut for Windows NT. See Chapter 3 for more information about getting connected.)
- ✓ **Transfer files using "drag and drop."** Move or copy files between two ReachOut computers using ReachOut Explorer.
- ✓ **Synchronize files with a simple point and click.** ReachOut features SmartSend™ and RapidSync™ to help you update your files and folders quickly and easily. Update all files or just the ones that changed with one click.

Using ReachOut

ReachOut is easy to use. Here's what you do:

Run ReachOut on the computer you are using and the one you want to connect to. The computer you want to connect to must be ready and waiting for your call.

Create connection icons on the computer you'll use to make calls so you can connect quickly to a remote computer. The connection wizard guides you.

Connect to a ReachOut computer, and work as if you were sitting in front of it.

Once you've connected to a ReachOut computer, work the way you normally do. If the computer is logged onto the network, you can transfer files, read your e-mail, get on the Internet, chat with co-workers, or print documents.

In addition, use ReachOut Explorer and SuperFTP Client to transfer files between the computer you're using and the one you're connected to. See Chapter 4, *Remote Access*, for more information.

About This Guide

This User's Guide helps you get ReachOut up and running on your computer so you can start working immediately.

Chapter 2, *Installation*, helps you set up ReachOut on your computer. The Setup wizard guides you through the process.

Chapter 3, *Getting Connected*, helps you prepare your computer to make and receive calls. It covers creating connection icons for fast connections to another ReachOut computer via modem (regular or ISDN), network, FTP, Dial-Up Networking, or direct cable.

Chapter 4, *Remote Access*, explains what you can do once you're connected to a ReachOut computer. You'll learn how to use the computer via remote control, transfer files and folders with ReachOut Explorer, synchronize files and folders with SmartSend and RapidSync, and chat with co-workers.

Chapter 5, *Security*, covers protecting your computer from intruders.

Chapter 6, *Configuration*, explains how to tell ReachOut about changes to your modem or network configuration.

Chapter 7, *For Supervisors*, is for the ReachOut supervisor. It explains how to place ReachOut on the network for public installation, and how to implement security at the supervisor level.

Chapter 8, *Passport*, shows how to install and use ReachOut Passport. It also includes information webmasters will need to incorporate Passport in their web sites.

Getting Help

The extensive ReachOut Help is available online when you need it. Get detailed information about ReachOut, as well as helpful procedures, with a simple point and click.

To...	Do this...
Get information about the window or dialog box on your screen.	Click the *Help* button.
Search for specific topics.	Choose *Help Topics* from the Help menu to view a list of available topics.
Find out how to perform a specific task.	Choose *How To* from the *Help* menu.
Get information on Stac services and support.	Choose *Product Support* from the *Help* menu.

Where To Get More Information

If you have Internet access, check Stac's home page on the World Wide Web (http://www.stac.com) for the latest information about ReachOut. Choose *Stac Home Page* from the *Help* menu to get details on what's available and connect directly.

If you don't have Internet access but have a modem, check Stac's Download Service (619/794-3711) for the latest ReachOut news.

2 ReachOut INSTALLATION

It takes only a few minutes to install ReachOut. This chapter explains how to install ReachOut on a Windows NT 4.0 computer.

Note: You must have Windows NT Administrator rights to install ReachOut on your system.

If you're the ReachOut Supervisor, you can place ReachOut on a network drive from which your users can install. This allows you to tailor the installation and control security at the ReachOut Supervisor level. For details, see Chapter 7, *For Supervisors*.

In this chapter...

Getting Ready to Install

Before installing ReachOut, make sure your computer can handle it. You must have:

- Windows NT 4.0 or later, either workstation or server, running on the computer.
- At least 8 MB of available disk space
- The ReachOut for Windows NT software (CD-ROM, floppy disks, or Setup files distributed to you or located on your company's network)

Note: To install ReachOut under DOS or any other Windows version, follow the instructions in the appropriate User's Guide.

For Connections to ReachOut Computers

You can connect to a ReachOut computer via modem or network. If the computers are cabled together under Windows, you can use any supported and available network to connect. ReachOut supports the following:

Modem: Hayes AT compatible 14,400 bps or higher, or ISDN modem (internal or external) recommended. If Windows supports your modem, so does ReachOut.

Network: Novell NetWare IPX/SPX, any compatible NetBIOS, and Internet (TCP/IP).

Dial-Up Networking: You can use any Windows NT Dial-Up Networking connections through ReachOut.

Direct cable: You can use Windows direct cable connection between serial ports on Windows NT and Windows 95 computers. Chapter 3, *Getting Connected*, and Windows Help include information about setting up and using Windows Direct Cable Connection. Once the computers are connected under Windows using a specially chosen modem definition, you can use NetBIOS, NetWare IPX/SPX, or TCP/IP, if the protocol is on both computers. All Windows NT and Windows 95 systems support NetBIOS.

For FTP Connections

You can use the SuperFTP Client to connect to any FTP server over the Internet and exchange files. SuperFTP Client includes many advanced features, such as multiple connections. Check the online Help within the FTP window once ReachOut has made the first connection.

Installing ReachOut

You must have Windows NT Administrator rights to install ReachOut.

Your standard copy of ReachOut comes with a license for you to use it. You can install it on two computers, then connect to one from the other. If you access a computer from several locations, you can install ReachOut on all the calling systems.

Chapter 7, *For Supervisors*, explains why you might need to install ReachOut from a network and shows how to do it. Each user who installs ReachOut from the network must have a valid ReachOut license. If you are installing ReachOut from a network drive, ask your ReachOut supervisor where to find the setup files on the network.

You can install ReachOut directly from the CD-ROM. If one of your computers doesn't have a CD-ROM drive, you may have access to a computer that does. Just load the CD-ROM and examine its folder structure. You can either copy the entire hierarchy to a network drive or create a set of floppy disks for use in installing ReachOut. The CD-ROM case includes instructions for ordering a set of floppy disks.

To install from CD-ROM or floppy disks

1. Insert the CD-ROM or Disk 1 into the drive.
2. Click the Windows Start button, then choose Settings.
3. Choose Control Panel from the submenu.
4. Double-click Add/Remove Programs.
5. On the Install/Uninstall tab, click Install.
6. Click Next.
7. Follow the instructions on your screen to run SETUP.EXE.

Your ReachOut serial number is located on the back of the CD-ROM case.

8. Repeat these instructions to install ReachOut on your other computer.

To install ReachOut from the network

1. Ask your ReachOut supervisor where to find the ReachOut files.
2. Click the Windows Start button, then choose Settings. Choose Control Panel from the submenu.
3. Double-click Add/Remove Programs.
4. On the Install/Uninstall tab, click Install.
5. Click Next.
6. Type the full path to the Setup file on the network or click Browse to search for it.
7. Follow the instructions on your screen.

Note: See Chapter 7, For Supervisors, *for information about setting up ReachOut on the network for user installation. This allows you to control ReachOut security at a global level.*

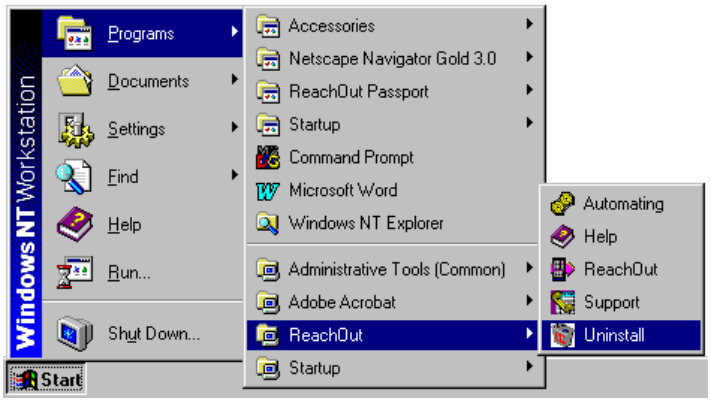
Upgrading ReachOut

Earlier versions of ReachOut do not work on a Windows NT computer. If you had an earlier version installed when you upgraded to Windows NT, you'll want to remove it before installing the new version. You can just delete the ReachOut folder, however, you'll have to create the connection icons again for the new ReachOut version.

Note: You can still connect to computers running ReachOut versions 5.0 and later under DOS, Windows 3.1, Windows for Workgroups, or Windows 95. For more details about backward compatibility, see Connecting to a Different Version of ReachOut *in Chapter 3.*

Starting ReachOut

Setup adds ReachOut to your Program Files folder or the folder you specified during ReachOut installation. It also adds a shortcut to your desktop.



To...	Use this command...
Write scripts for use in automating ReachOut (most useful for automating file transfers).	Automating
Get ReachOut Help.	Help
Start ReachOut.	ReachOut
Implement global security for all users who installed ReachOut with SETUP PUBLIC.	Supervisor Security (available only if you installed ReachOut with SETUP SHARED)
Get information for contacting Stac.	Support
Remove ReachOut from your computer.	Uninstall

To start ReachOut

1. Double-click the ReachOut icon on the desktop.

   The first time you start ReachOut, the Create New Connection wizard opens to help you create a connection icon so you can connect to another computer.

2. See Chapter 3, *Getting Connected*, for information on creating connection icons and using ReachOut.

Registering ReachOut

To take advantage of ReachOut support services, you must register ReachOut. Register by phone or complete and mail the registration card in your ReachOut package.

In addition, when you register we'll add you to our mailing list so you receive information about new products, product upgrades, and more.

3 ReachOut GETTING CONNECTED

Now that you've installed ReachOut, you can begin using it immediately to connect to other computers. ReachOut lets you connect with multiple computers at the same time.

You'll create and use connection icons to make all your ReachOut connections. A wizard helps you create them and a right-click makes it easy to edit the properties. Once you connect to a computer, you can remotely control it or exchange files through ReachOut Explorer. You can also use Dial-Up Networking and FTP through ReachOut.

In this chapter...

Using ReachOut

After installing ReachOut, you are ready to make connections. Use the following guidelines, then see the rest of this chapter for details on creating connection icons and making ReachOut connections.

To let a ReachOut computer connect to you

1. Double-click the ReachOut icon on the desktop.
2. By default, ReachOut waits for all connections while it is running.

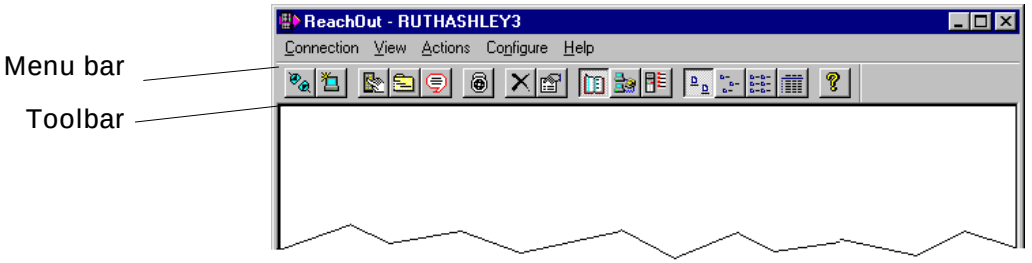
   To limit or prevent connections, use *Options* on the *Configure* menu. (See *Waiting for Calls* on page 16.)

To connect using ReachOut

1. Start ReachOut.
2. If necessary, create a connection icon. (See *Connection Icons* on page 17.)
3. To connect, do one of the following:
   - Select the connection icon and click  on the toolbar, or press ENTER, or choose *Connect* from the *Connection* menu.
   - Double-click the connection icon.
   - Right-click the connection icon and choose *Connect*.
4. If appropriate, click  for remote control or  for ReachOut Explorer in the toolbar. (See Chapter 4, *Remote Access*, for details.)

To disconnect ReachOut

- Make sure the connection icon is selected, then click  in the toolbar or choose *Disconnect* from the *Connection* menu.



To...	Use...
Create a new connection icon.	
Connect to a ReachOut computer, or terminate a connection.	
Control a ReachOut computer.	
Transfer files between ReachOut computers using ReachOut Explorer.	
Start ReachOut Chat and exchange messages with other users.	
Implement security measures.	
Remove a connection icon.	
View connection icon properties.	
View your address book connection icons.	
View connection icons for all defined Dial-Up Networking servers.	
View connection icons for all ReachOut computers waiting on the network.	
Change how your connection icons appear.	
Start Reach Out Help.	

Waiting for Calls

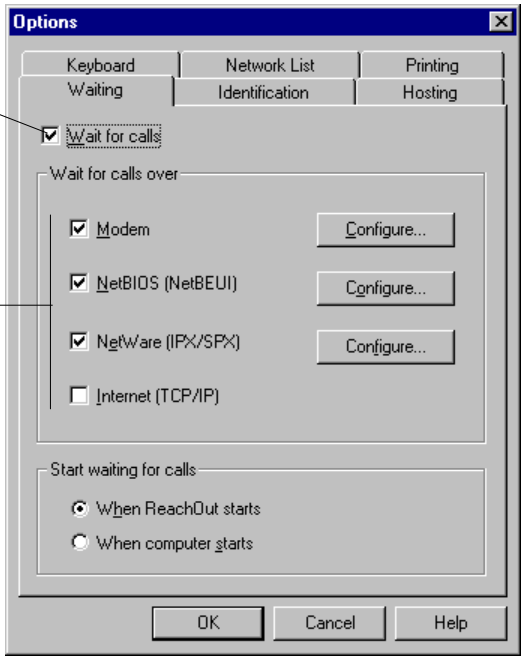
By default, your Windows NT computer is ready to receive calls over a modem or local network whenever ReachOut is running. You can choose to block all calls or some types of calls. See Chapter 6, *Configuration*, for more details.

To verify or change the current waiting status

1. Choose *Options* from the *Configure* menu.

The ✓ indicates that ReachOut is ready to receive calls from other ReachOut computers.

You can choose the type of calls you want to receive.



2. To prevent calls, uncheck any of the four connection types or uncheck *Wait for calls* to disallow all calls.
3. If you prefer to have ReachOut start waiting for calls as soon as you start your computer, select *When computer starts*. This takes effect when you restart the computer.

Note: If you installed ReachOut from the network, your ReachOut supervisor may have limited your ability to change waiting options.

Connection Icons

A connection icon lets you connect to another ReachOut computer, a Dial-Up Network, or an FTP site. All types of connection icons can appear in a ReachOut window. These are the most common ones:

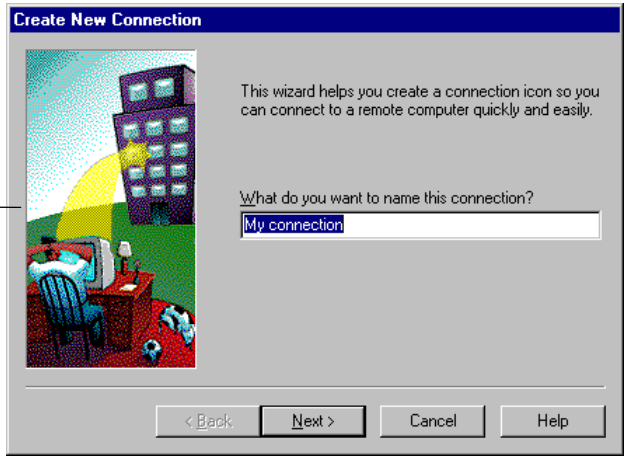
- Modem connections are used for standard and ISDN modems, as well as to start Dial-Up Networking and direct cable connections from within ReachOut.
- Network connections let you connect across a NetWare, NetBIOS, or TCP/IP network(such as the Internet).
- Dial-Up Networking connections let you use remote node, with or without remote access.
- FTP connections are used to connect directly to an FTP site for file transfer.

Creating Connection Icons

Creating connection icons is a snap with the New Connection wizard. Or, if you have a NetWare or NetBIOS network (see page 20), you can ask ReachOut to list the waiting ReachOut computers so you can select one.

To create a connection icon

1. If necessary, click  on the toolbar to start the New Connection wizard.



Create as many connection icons as you like using the New Connection wizard.

2. Type a name that helps you identify the computer you will connect to (such as *My office computer*, *My Home*, or *Office FTP Site*), then click Next.
3. On the next screen, choose how you will connect (Modem, Network, Dial-Up Networking, or Internet FTP) and click Next.
4. On the next screen, enter the appropriate values (you'll find more details in the rest of this chapter).
   - For Modem or Dial-Up Networking, enter the phone number.
   - For Network, choose the network type (NetWare, NetBIOS, or TCP/IP) and provide the name or number of the computer.
   - For Internet FTP, enter the IP address or domain name.
5. On the next screen, click *Finish*.

   The connection icon appears in the ReachOut window.

Changing Connection Icon Properties

ReachOut can use most connection icons as soon as they are created. It prompts for any needed User ID and password information. You can supply individual information for each connection icon by right-clicking and choosing *Properties*.

To add connection information

1. Right-click the connection icon and choose *Properties*.
2. Choose the *Options* tab and click the *Specify Remote Computer Password* button.
3. Type the *User name* and *Password* as needed.

Note: Chapter 6, Configuration, includes more details on configuring the different connection types.

Using Connection Icons

ReachOut stores each connection icon you create in a file named *iconname*.RCO and adds each connection icon to your address book.

The network view lets you copy the icon for any ReachOut computer on the network to your address book. The first time you connect to a Dial-Up Networking server, its icon appears in your address book as well. View the connection icons by large or small icons, detail, or list view. Right-click any connection icon to modify it or view its properties.

To see ...	Click ...
Icons in your address book	
All Dial-Up Networking icons	
Connection icons for all ReachOut computers waiting on NetWare or NetBIOS	

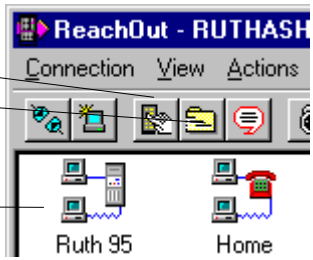
Note: Click all three buttons to view all connections at once. You can right-click icons that aren't already in your address book and choose Add to Address Book *if you like.*

You can drag any connection icon to your desktop for quick access. Double-clicking this icon will start ReachOut if necessary and make the connection immediately.

Making Connections

When you're ready to connect to another ReachOut computer, and that computer is ready to receive your call, make the connection. Here's what you do:

1. Select the action you want (either remote control or ReachOut Explorer)
2. Double-click the connection icon.



You can connect to as many remote computers as you want, and use remote control, ReachOut Explorer, and Chat with any or all of them at the same time. More than one computer can connect to you, as well;

however, only one caller can use remote control at a time. Other connected callers are limited to ReachOut Explorer and Chat.

Connecting over a Network or Modem

When you connect to another ReachOut computer using a network or modem, you can control the connected computer remotely or use ReachOut Explorer to exchange files. Both computers must have ReachOut running; one computer must be waiting. You can connect to any computer running ReachOut 5.0 or later and those computers can connect to you.

Note: The only exception is that a computer running ReachOut under DOS cannot connect to a Windows NT computer. See Connecting to a Different Version of ReachOut *on page 26 for more information about connecting to previous versions of ReachOut.*

NetWare or NetBIOS Networks

When you create connection icons, you can ask ReachOut to list the waiting computers on a local network and choose one or just type the computer's network name.

When using a local network, click  to display connection icons for all ReachOut computers waiting on that network. These icons include green dots indicating that they are waiting and ready to go. You can double-click to start the connection or right-click and copy the icon to your address book.

Note: When you create a network connection icon, ReachOut displays a screen from which you can select a ReachOut computer on the network. If the computer you want is not in the list, it may be because it is not logged onto the network; you can type the computer's name in the field. If you don't know the computer's name, ask the owner. If you are creating a network connection icon for use in direct cable connection, use the other computer's ReachOut name.

Internet (TCP/IP)

A connection icon for connecting to a waiting computer over the Internet must include the computer's IP address or full domain name. You can insert it when you create the connection icon. If the IP address is dynamic, you can modify the properties just before making the connection. Connect both computers to the Internet in the usual way. Then use ReachOut to connect the two over the TCP/IP network.

ReachOut can't create a network list for computers waiting over the Internet.

Modems

In most cases, you'll configure your modem under Windows so that its features apply to any use. When you create connection icons, you enter the telephone number, with area code if needed.

Note: Before connecting to a waiting computer via modem, make sure your Windows modem dialing properties are set to access an outside line, if necessary. Use the Start *menu and choose* Control Panel *from the* Settings *menu, then change* Dialing Properties *for Modem.*

Connecting via Dial-Up Networking

The Dial-Up Networking client is installed automatically with Windows NT. It allows a computer to connect to a Dial-Up Networking (or RAS) server and become a *remote node* on the network. Once a computer becomes a remote node, its user has access to network services that would be available if the user were physically on the network. ReachOut uses Windows Dial-Up Networking connections over a modem. Make sure you can connect to a Dial-Up Networking server using Windows before you try it with ReachOut, since ReachOut uses the same properties. Once you are connected to the server, ReachOut uses network connections.

ReachOut extends Dial-Up Networking by giving you the ability to *remotely control* a Dial-Up Networking server or any computer on that network, as long as it is running ReachOut. Windows NT allows direct cable connections as a type of Dial-Up Networking, and ReachOut supports these as well.

Dial-Up Networking Connection Icons

The Dial-Up Networking connection list you see in ReachOut automatically contains any Dial-Up connections you have defined under Windows. You can use them to connect to a Dial-Up Networking server from within ReachOut even if that server does not have ReachOut installed.

If you want to use ReachOut once connected to the Dial-Up Networking server, you can create a ReachOut connection icon to make the connection and take you directly to a computer waiting for ReachOut calls.

To create a Dial-Up Networking (DUN) connection icon

1. Click New Connection on the toolbar.
2. Type a name for your connection icon and choose OK.
3. Choose *Dial-Up Networking*, then OK.
4. In the resulting window, choose *New* or a predefined Microsoft Dial-Up Networking connection.

   If you choose *New*, a wizard lets you define a new Windows Dial-Up Networking connection.
5. Type the ReachOut name of the computer.

   The ReachOut computer can be the server or another ReachOut computer on that network. This icon will connect you directly to the computer you name.
6. Click *Finish*.

When you connect to a Dial-Up Networking server with a ReachOut icon, you have several options:

- Use ReachOut to control the computer named in the connection icon. This can be the server itself or a different computer on that network.
- Once connected to the server, use a ReachOut network connection icon to connect to another ReachOut computer on that network, using the server as a *gateway*.
- Act as a remote node on the network.

Once ReachOut is connected to a remote access server, you'll see the RAS monitor open on the taskbar.

To connect to a Dial-Up Networking server

1. Click a Dial-Up Networking icon in your address book.
2. If necessary, click  to see the DUN connections already defined under Windows NT.

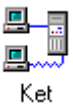
   You will connect to the computer named in the icon's *Calling Options* properties if that computer is waiting for network calls.
3. If necessary, choose  for ReachOut Explorer or  for remote control from the toolbar.

Note: In order to connect to Novell's Dial-Up Networking (Remote Node Server) through ReachOut, you must first connect to the server under Windows using a Microsoft DUN connection for the NetWare Connect object. When you configure the object under Windows, enter the password and check "Save Password," then make the connection. NetWare does not prompt you for a missing password as other servers do. After the first time, you can connect from ReachOut.

Even if the server is not a ReachOut computer, you can use ReachOut to connect to and control another computer on that network. If you connect with Microsoft's standard connection icon or if you used the server computer name in the ReachOut connection icon, you can still control another ReachOut computer.

To control a different computer on the network

1. While you are a remote node on the Dial-Up Network, open ReachOut on your local computer, if it is closed.



2. Double-click a network connection icon in your personal address book or network list.

   You can create a connection icon after being connected to the network if you like. Just open ReachOut and work as usual.

Note: When a Dial-Up Networking (or RAS) server is waiting for DUN calls, it will not receive ReachOut modem calls. If the server has ReachOut installed, make sure it is not "Waiting for calls" over a modem. In addition, make sure the computer from which you are making the connection is not "Waiting for calls" over a modem. Any ReachOut connection you make after establishing the Dial-Up Networking connection are network connections.

To connect to a DUN server with ReachOut installed via standard ReachOut modem connection, make sure "No caller access" is checked in the Dial-Up Networking server properties.

Connecting via Direct Cable

You can also use ReachOut between two Windows NT or Windows 95 computers (or one of each) that have a physical direct cable connection between serial ports. In Windows NT, you set up direct connections as part of Dial-Up Networking, which requires a special modem definition. Once you complete the Windows connection (through Windows or ReachOut), you make a ReachOut Network connection using a network protocol running on both computers.

To create the Dial-Up Networking icon for Windows NT

1. In the Control Panel, choose Modems.
2. Click *Add*.
3. Check *Don't detect the modem* so you can select it from a list.
4. Select the top modem: *Dial-Up Networking Serial Cable between 2 PCs*.
5. Choose the port you will use.

Note: See the ReachOut for Windows 95 User's Guide for details about setting up a direct cable connection using Windows 95.

To physically connect the computers

- Use a null modem serial cable between two serial ports.

To use ReachOut over a direct cable connection

1. Connect the two computers with a serial null-modem cable.
2. Establish the DUN connection from either Windows NT or ReachOut.

   In ReachOut, click  to show the defined DUN connections. Right-click the icon you want and choose *Copy to Address Book* to make it permanent.
3. Define a network connection icon specifying the selected network protocol and naming the other computer.

   It might help to include “Direct 1” in the DUN connection icon name and “Direct 2” in the ReachOut connection icon name.

4. Double-click the network connection icon you created using the selected network protocol for the direct cable connection.
5. If necessary, click the Remote Control or ReachOut Explorer button on the toolbar. You can use any ReachOut tools once you are connected.

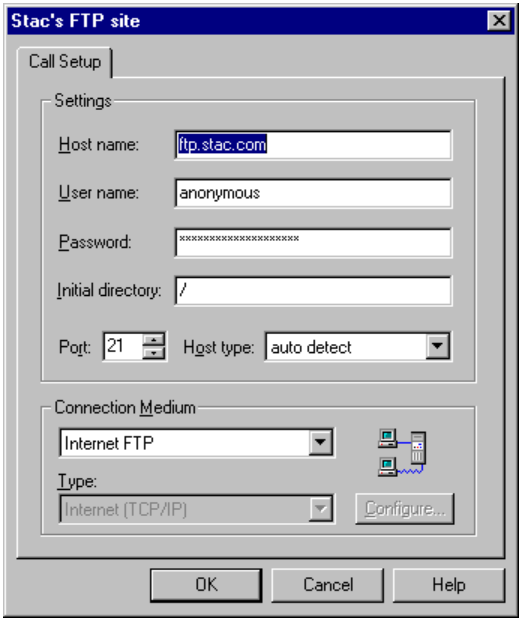
Connecting via FTP

You can also use ReachOut to connect to an FTP site on the Internet.

To create the connection icon:

1. Start the connection wizard and type a name for the connection icon.
2. Choose Internet FTP as the connection type.
3. Enter the host name of the FTP server, along with the User name and Password if you like.

You can right-click the icon and change its properties at any time.



Once ReachOut makes the FTP connection, you can transfer files as needed.

Connecting to a Different Version of ReachOut

ReachOut 7.0 communicates with ReachOut 5.0 or later running on Windows NT, Windows 95, or Windows 3.1*x*. You can to connect to a waiting ReachOut computer or have one connect to you.

There are only a few limitations when you try to connect a computer running ReachOut for Windows NT with a computer running ReachOut for Windows 95 or ReachOut for Windows & DOS:

- A computer running ReachOut under DOS cannot call a Windows NT computer. (You can connect the other way, however.)

- You also need to use uppercase passwords in any Windows NT user accounts that other versions of ReachOut use to connect—unless you specifically upgrade the Windows 95 and Windows 3.1 versions of ReachOut to ones that let you make calls using mixed-case passwords. To learn how to do this, see the Read Me file in the ReachOut folder.

What You See When You Connect

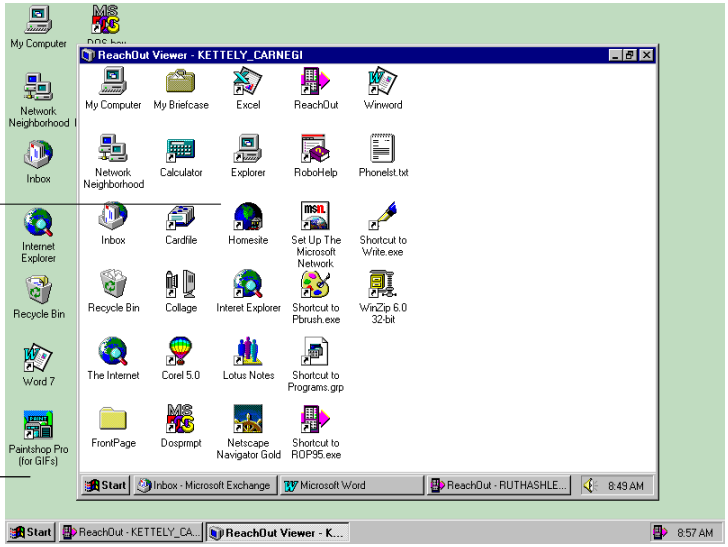
When you connect to a computer, what you see depends on the action you want to perform. The appearance of your screen when you use remote control depends on the relative resolutions of the monitors involved. Chapter 4, *Remote Access*, includes information on using remote control while you are connected. ReachOut Explorer and FTP use special windows.

Remote Control

Under remote control, the desktop of the computer being controlled appears in a *viewing window* on your desktop.

The viewing window shows the computer you connected to. The computer's ReachOut name appears on the viewing window's title bar.

Your desktop



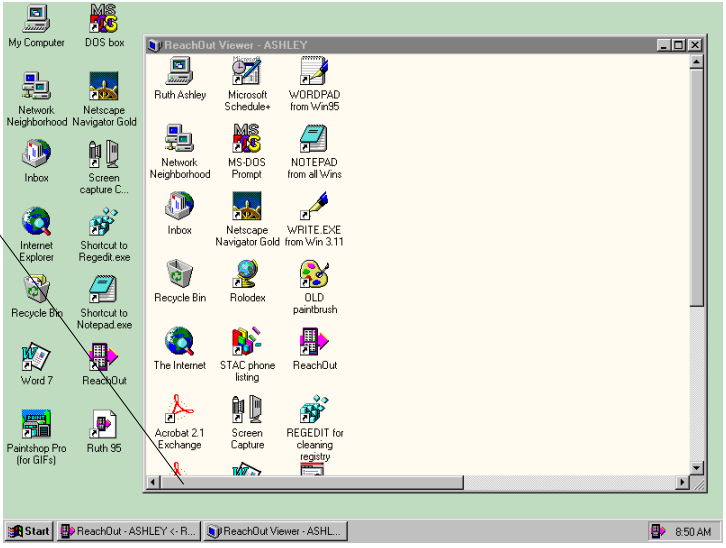
Controlled monitor has lower resolution

If the other computer's monitor is a lower screen resolution than your monitor (for instance, it is 640x480 and your monitor is 800x600), the computer's desktop appears within a full viewing window as shown in the previous figure. There are no scroll bars. Size and move the window on your desktop as you would any window. To switch back to your desktop, move the cursor outside the viewing window and click.

Controlled monitor has higher resolution

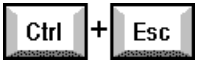
If the other computer's monitor is a higher screen resolution than your monitor (for instance it is 800x600 and your monitor is 640x480), the computer's desktop appears within a scrollable viewing window on your desktop.

Use scroll bars to bring into view parts of the remote desktop you



To move different parts of the window into view, use scroll bars. You can also use *scaling* or *panning* to adjust the display. See Chapter 4 for details.

Both monitors have the same resolution

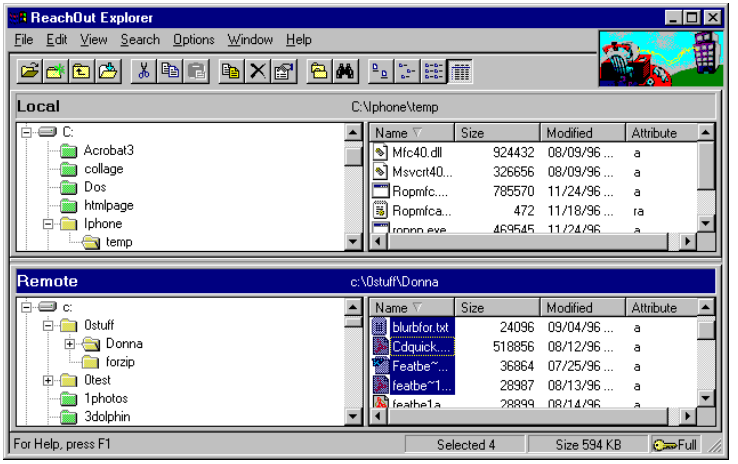


If both monitors are the same screen resolution, the viewing window may cover your entire desktop. To bring up your local computer's task bar, press CTRL+ESC. To size the viewing window, click once on your

local taskbar's Start menu to clear it, then right-click the viewing icon. From the Control menu, choose *Restore*.

ReachOut Explorer

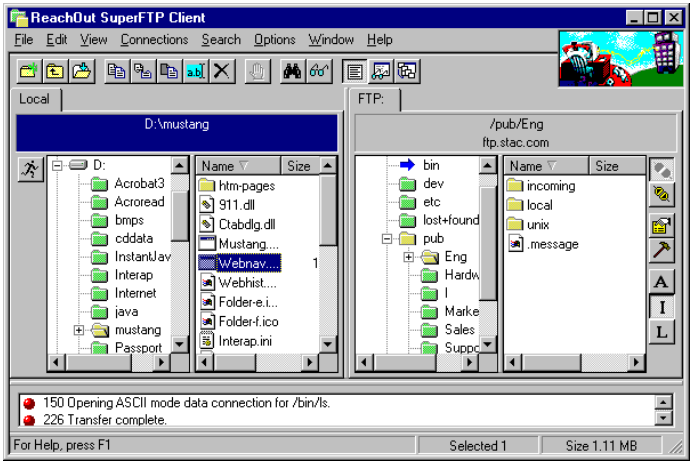
In ReachOut Explorer, ReachOut shows folders from both connected computers. Just drag and drop to copy files between computers.



Chapter 4, *Remote Access*, explains how to use ReachOut Explorer.

FTP

An FTP connection results in an FTP window. You can drag and drop as with any FTP client.



4 ReachOut REMOTE ACCESS

ReachOut lets you connect to as many remote computers as you want; you can even connect to them all at the same time. Here's what you can do when you connect to another ReachOut computer:

Control it remotely 

Transfer files 

Exchange messages 

You can also connect to any number of Internet FTP hosts using ReachOut **SuperFTP Client**. The FTP hosts you connect to do not have to have be ReachOut computers.

In this chapter...

Using Remote Control

When you connect to a computer for remote control, use the computer the way you would if you were in front of it.

To use remote control

1. Use ReachOut to connect to the computer.
2. Click  to start remote control.

- **Work with documents and run applications as usual**. Open, read, change, save, and print documents at the remote site.
- **Access and use network resources**. If the computer you connected to is logged onto the network, access drives and network folders as usual: read your e-mail, print to network printers, transfer files. See *Transferring Files* on page 40 for details on how to transfer files between ReachOut computers.
- **Get on the Internet**. If you don't have Internet access on the computer you are using, you can connect to a ReachOut computer that has Internet access and start that computer's Web browser, such as Netscape. Once you're on the Internet, work as usual.

- **Change system settings**. If you have the right access to the computer you're connected to, you can change some of its ReachOut settings. See Chapter 5, *Security*, for details.
- **Control multiple computers**. You can connect to more than one computer at a time and remotely control any number of them. Each computer appears in a separate viewing window, and you'll see the name of that computer in the viewing window's title bar.

Adjusting the Viewing Window

While remotely controlling a computer, you may need to adjust the way the computer appears within your viewing window. You can resize the window or turn it into a full screen view so that you no longer see your local desktop in the background. Use *scaling* and *panning* from your computer to adjust the other computer's desktop.

Sizing the Viewing Window

The viewing window works just like any other window on your desktop. You can move or resize the window to position it conveniently, or minimize the window to an icon on the taskbar.

If you maximize the viewing window, one of the following will happen:

If your resolution is...	A maximized viewing window appears...
Higher than the remote computer's resolution	Smaller than your desktop
The same as the remote computer's resolution	**Full screen**: The same size as your desktop, without a title bar or scroll bars
Lower than the remote computer's resolution	**Full screen**: Larger than your desktop (with scroll bars)

If you are viewing a remote computer in full screen mode and need to get back to the local desktop, you can use the "toggle screen key" to restore the viewing window back to its previous size. The default toggle

screen key is CTRL+SHIFT+T. Choose *Options* from the *Configure* menu and change to a different toggle key on the *Keyboard* tab if necessary.

Panning in the Viewing Window

Panning allows you to define unique *pan keys* (mouse, or mouse and keyboard combinations) that you use to view parts of the other computer's desktop you can't see. You can also use scroll bars in the viewing window to move parts into view.

To choose a pan key

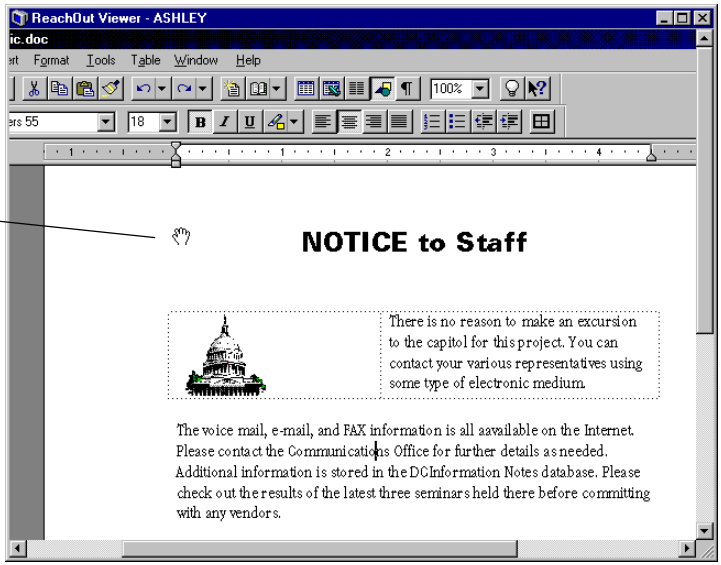
1. Choose *Options* from your ReachOut *Configure* menu.
2. On the *Keyboard* tab, choose a pan key from the *Pan key* field and click *OK.*

To use panning

1. Point to any location in the viewing window.
2. Use your defined pan key to move the computer's desktop within your viewing window.

   For instance, if the SHIFT plus right-mouse button was the pan key, you'd press the SHIFT key while pressing and dragging the right-mouse button to move the computer's desktop within your viewing window. The next figure shows the pan cursor that appears during panning.

While the pan key is active, the cursor changes to a *pan cursor*.

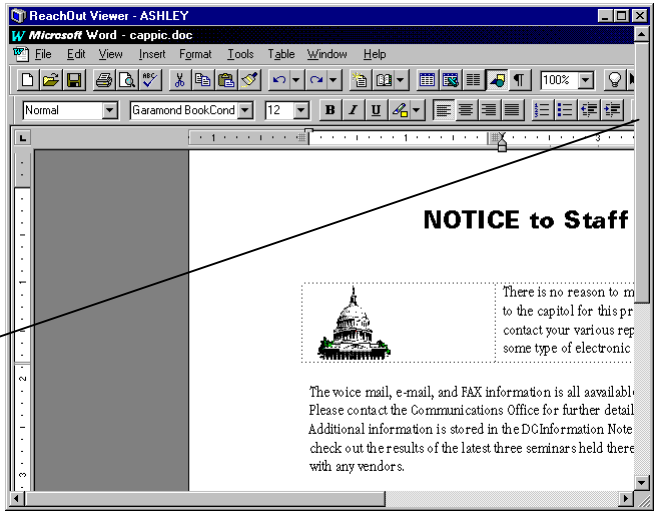


3. Release the pan key once the desktop is where you want.

Scaling the Remote Desktop

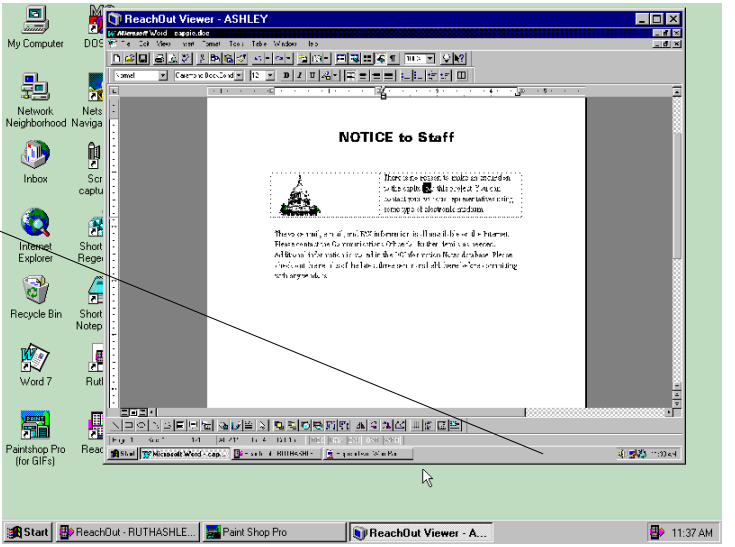
Scaling shrinks the computer's desktop to fit within your viewing window. The next two figures show a connection to a remote computer. The first figure shows the computer's desktop when it is not scaled in the viewing window.

Scroll bars let you see the entire desktop when it is not scaled.



Scaling is connection specific. You apply scaling to a computer you are connected to, or as a connection icon property.

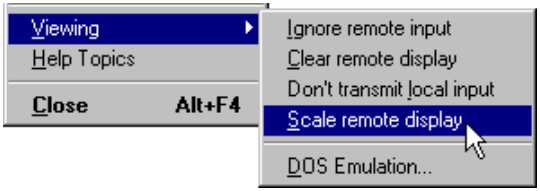
The viewing window has no scroll bars when scaled. Drag its corners to size it.



Note: When you scale a computer for viewing, it may be difficult to view the computer's desktop clearly within your viewing window because of the size of your screen.

To scale the other computer's display

1. Click the icon at the top left corner of the viewing window to open the Control menu.
2. Choose *Viewing.*



3. Choose *Scale remote display.*

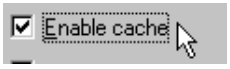
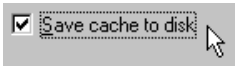
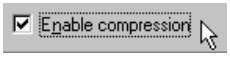
This setting is not saved between sessions. If you want to have the remote display always scaled to fit in the viewing window, set this option in the properties of the connection icon.

Optimizing Viewing

Each time you connect to a computer, ReachOut paints the computer's desktop on your screen. This can cause noticeable slowing on local networks. By default, ReachOut caches graphics to memory or disk and compresses all data used in refreshing the screen to speed up viewing. When ReachOut uses a disk cache, it saves data between connections, speeding up the process next time you connect.

To optimize viewing

1. Right-click the computer's connection icon and choose *Properties* from the context menu.
2. On the *Options* tab, make these entries:

To...	Check this...
Have ReachOut store graphics for reuse	
Save stored graphics for use between sessions	
Compress graphics during remote control	

Remote Control Security

As a caller, you have some control over what a user at the remote computer can do while you are viewing it. You can enable or disable some security features before you make the connection, or while you are actually controlling the computer. However, your ability to prevent users from accessing the computer might be limited by the security settings that are already in effect for that computer.

Disabling Keyboard and Mouse Input

During remote control, you can disable the remote computer's keyboard and mouse—users at the other computer won't be able to use the keyboard or mouse while you are connected.

To disable the remote computer's keyboard and mouse during remote control

1. Click the icon at the top left corner of the viewing window to open the Control menu.
2. Choose *Viewing.*
3. Choose *Ignore remote input.*

This setting is not saved between sessions. If you always want the remote keyboard and mouse disabled, you can set this option in the properties of the connection icon.

Controlling Viewing of a Computer

You can clear the remote computer's display during remote control so no one can see what you are doing. When a computer's display is cleared, it appears as if it is turned off. You might use this feature if you are accessing sensitive documents on the other computer.

To clear the remote computer's display

1. Click the icon at the top left corner of the viewing window to open the Control menu.
2. Choose *Viewing.*
3. Choose *Clear remote display.*

This setting is not saved between sessions. If you always want the remote display disabled, you can set this option in the properties of the connection icon.

Transferring Data via the Clipboard

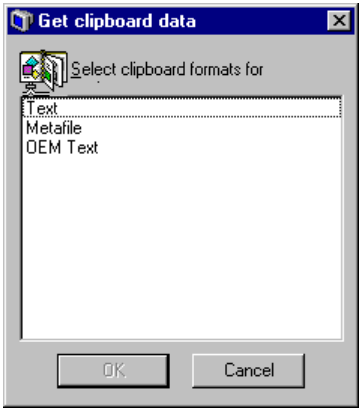
Use the ReachOut *Remote Clipboard* to transfer data between two ReachOut computers during remote control. Use the Remote Clipboard to transfer a small amount of data (for instance, if you want to copy a paragraph from a document). For large (or graphic-intensive) files, use ReachOut Explorer or FTP to transfer the data.

Note: If a user at the remote computer has disabled the Remote Clipboard feature, you won't be able to copy and paste this way.

To copy and paste between computers

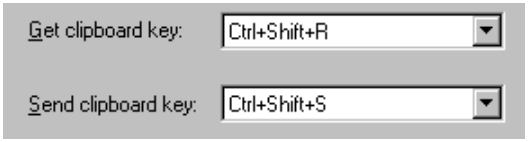
1. Connect to the other computer and start remote control.
2. Open any document on the local or the remote computer and copy the data you want.

3. Click the icon at the top left corner of the viewing window to open the Control menu.
4. Choose one of the following:
   - *Get Clipboard*, if you are copying from the remote computer to the local computer.
   - *Send Clipboard*, if you are copying from the local computer to the remote computer.
5. If the information you're transferring can be sent in more than one format, you'll see a dialog box asking you to choose which one you want.



   Select the appropriate type or types and press ENTER. You must select at least one type or nothing will be transferred.
6. Switch to the document where you want to paste and choose the application's paste command (usually on the *Edit* menu).

ReachOut provides hot keys you can use to get and send clipboard contents quickly and easily.



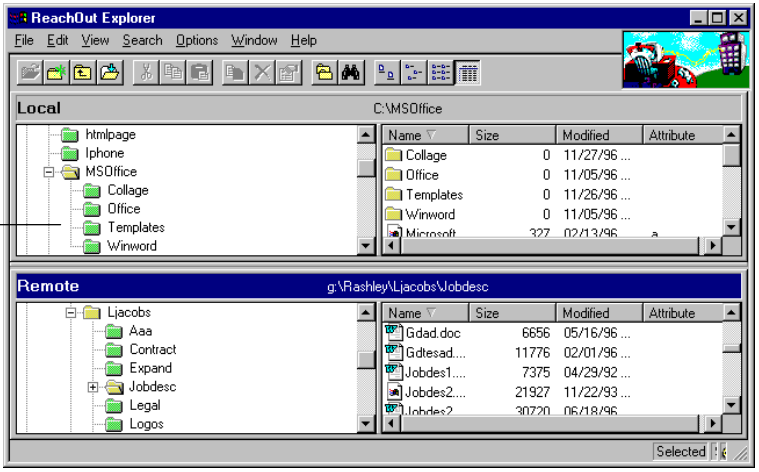
To change the clipboard hot keys

1. Choose *Options* from the *Configure* menu.
2. Choose the *Keyboard* tab.
3. Select one of the options: None, or the key with CTRL, CTRL+SHIFT, or ALT.

Transferring Files

Use *ReachOut Explorer* to transfer files and folders between two ReachOut computers. Use ReachOut Explorer much as you would use Windows Explorer.

Drag and drop files and folders between your computer (local) and the one you're connected to (remote).



If the computer you connected to allows you full transfer access, you can also create folders, copy, move, rename, and delete files and folders.

Note: You can implement security measures to prevent unwanted transfers of files to and from your computer. For more information see Chapter 5, Security.

To copy files between ReachOut computers

1. Click *ReachOut Explorer* on the toolbar.
2. Double-click the computer's connection icon.
3. Choose existing files or folders from the *local* or *remote window*, then drag them where you want them copied and release.

Note: Data transfer speed depends on the connecting device you're using: modem, network, ISDN line, or direct cable. The faster the transmission device, of course, the faster the transfer.

Transferring Files with Long Names

If you transfer files with long file names to a Windows 3.1, Windows for Workgroups (WFW), or DOS computer, ReachOut converts the names to DOS naming conventions (an eight-letter name with a three-character file extension). Spaces in the file name become underscore (_) characters. For instance, "My status report.doc" becomes MY_STATU.DOC. Unlike the standard Windows method of renaming files, ReachOut uses a full eight characters of the name instead of adding a tilde (~) character and a number to indicate missing letters. This means that you must be careful when copying several files with similar long file names to a previous version of Windows, because they might overwrite one another.

Using ReachOut Explorer Tools

The buttons in the toolbar make it easy to accomplish most tasks:

To...	Use this tool...
Open the selected file in the active window.	
Create a new folder in the active window.	

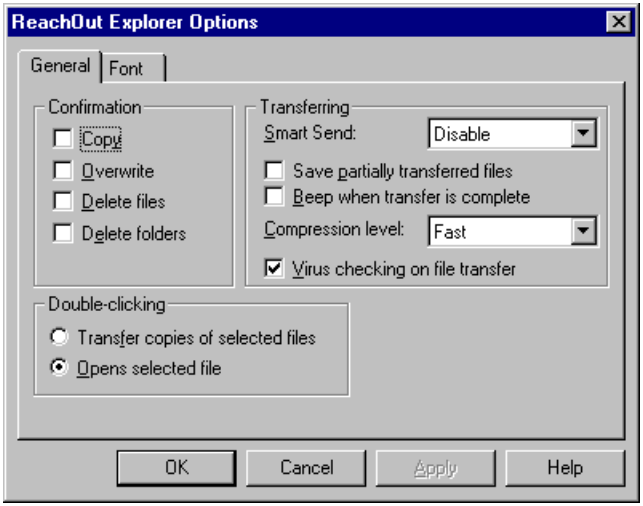
To...	Use this tool...
Go up one folder from where you are in the active window.	
Open the Go To Folder dialog box so you can switch to a different folder on the active window.	
Cut a file or folder from the active window.	
Make a copy of a selected file or folder in the active window.	
Paste a file in the active window.	
Automatically transfer the selected file or folder in the active window to the other computer.	
Delete a file or folder in the active window.	
View Properties for the selected file or folder on the active window.	
Synchronize files or folders on the connected computers. Older files are replaced with newer versions.	
Search for a specific file or folder on your computer or the one you're connected to.	
Change how files and folders appear in the active window.	

Optimizing File Transfers

If files to be transferred are large or contain graphics, you can compress them during modem transfer to save time and money. Use ReachOut Explorer options to specify how files are transferred between the two connected computers.

To optimize file transfers

1. Choose *General* from the *Options* menu



2. In the *Confirmation* section, specify when you want ReachOut Explorer to ask you to confirm operations; these are the same options Windows gives you.
3. In the *Transferring* section, specify a SmartSend level and compression level, as well as how to handle partial or completed file transfers. (See the next section for details on SmartSend and compression.)
4. In the *Double-clicking* section, specify the effect of double-clicking selected files; you can have ReachOut copy files immediately to the current folder of the connected computer or open the selected file.

Optimizing Transfers with SmartSend™

Normally, ReachOut transfers complete files when you copy them. You can optimize data transfers with SmartSend when you transfer files that already exist on the other computer with matching names and paths. SmartSend transfers only the differences between the matching files.

When you use Standard SmartSend, ReachOut identifies matching files, then compares their dates, times, and sizes. If these values match, ReachOut doesn't transfer the file at all. If any of the values are

different, ReachOut identifies the differences and updates the files on the target computer. When you use Vigorous SmartSend, ReachOut checks for differences in all matching files and transfers them.

Files and folders you transfer between two computers must exist in the same folder structure on both computers. Use ReachOut Explorer Options (*General* tab) to enable SmartSend and set the level.

To...	Choose...
Identify and transfer differences in files with matching names and paths that have different sizes, dates, or times.	Standard
Identify and transfer differences in all files with matching names and paths.	Vigorous
Transfer full files regardless of differences.	Disable

Compressing for Faster Transfers

ReachOut gives you three compression options for maximizing your data transfers: Fast, Standard, and Maximum. You decide how long ReachOut should take to compress the files. Here are some suggested settings for optimizing file transfer speeds.

If you are transferring...	Choose...
Very small files, or files over a fast connection (such as a local network)	Fast
Very large files (>10 MB), or files over a slow connection (such as a modem)	Standard
Very large files (>10 MB) over a slow connection (such as a modem)	Maximum
Files that are already compressed	Disable

Synchronizing with RapidSync™

An alternative to dragging and dropping files and folders from one computer to the other is to use RapidSync to synchronize the two computers quickly. Files and folders with matching names are made to match the latest one. Files and folders that exist on one computer are duplicated on the other computer. After choosing the two folders, you can ask ReachOut to include subfolders, synchronize only files that already exist, or transfer in one direction only.

Note: Your SmartSend options apply when ReachOut transfers files during synchronizing folders, as well as during regular file transfers.

To synchronize files and folders

1. Connect to the computer, and click ReachOut Explorer on the toolbar.
2. In the *Local* and *Remote* windows, make the folders in which you want to synchronize files active.

3. Click *Synchronize folders* on the ReachOut Explorer toolbar.
4. Choose any options and click *OK*.

   ReachOut synchronizes the two based on your options.

Scheduling File Transfers

If you need to transfer files between ReachOut computers at a specific time and you can't be there to do it personally, use the Automating tool to write a ReachOut script for a scheduled file transfer.

For details on writing and using scripts, see ReachOut Help.

Chatting Online

ReachOut *Chat* is an effective way to communicate with a user at another ReachOut computer. You type a message and the user you want to chat with can respond with a message. You, or the other user, can start Chat.

Use Chat to talk to the person at the remote

To chat

1. Connect to the other computer; make sure the connection icon of the computer you want to chant with is selected.

2. Click *Chat* on the ReachOut toolbar.

   ReachOut opens Chat on both computers.

Read received messages in the upper part of the window

Type messages in the lower part of the window

3. Type your message or see the instructions for copy and paste.

If the other computer doesn't respond, you can page it. The user hears a sound similar to a telephone ring.

To page a user

- Click *Page* on the Chat menu bar.

Copying and Pasting in Chat

With Chat, you can copy text to your Local Chat window from another source. For instance, you can copy text from WordPad or your e-mail, and paste it into your Local Chat window. The connected user will see the text you pasted.

You can also copy messages from the connected computer. If you don't select text to copy, Chat copies the entire contents of the message window. If you select text to copy, only the selected text will be copied.

To copy text from the chat window

1. Select the text you want to copy. (To copy all text, click once to deselect all the text).
2. Choose *Copy from Host* (or *Copy from Viewer*) on the *Edit* menu.
3. Open the destination document where you want to place the text, and paste as usual.

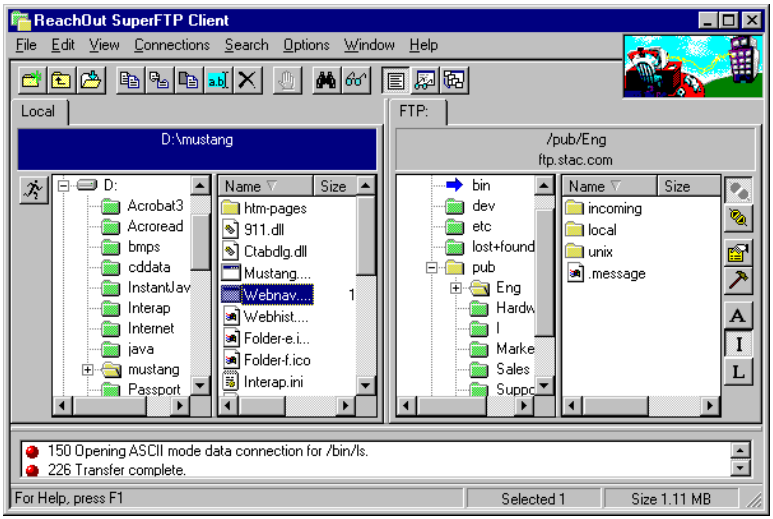
To paste text from a document into the Chat window

1. Copy the text from the source document.
2. Choose *Paste from Host* (or *Paste from Viewer*) on your *Edit* menu.

Internet File Transfers With FTP

Create an Internet FTP connection icon to connect to any FTP host and transfer files. The FTP host does not have to have ReachOut.

When you make the connection, you see a window that looks much like ReachOut Explorer. This is ReachOut SuperFTP Client.



To copy files between computers

1. Select the files to be copied.
2. Drag them to the appropriate folder.
3. Drop them.

To disconnect from the FTP host

- Close the SuperFTP Client window.

5 ReachOut SECURITY

When you give remote users full access to your computer, they can:

- Use all your applications.
- Change, copy, save, move, and delete your files and folders.
- Transfer files and folders to and from your computer.
- Change your ReachOut settings.

You may not want just anyone to have that much control over your computer. Using *ReachOut Security*, protect your computer by determining the level of access other users have.

If you're the ReachOut supervisor, you can implement security globally by installing ReachOut on the network and having users install ReachOut from the network. See *Setting Global ReachOut Security* in Chapter 7.

Note: *If you installed ReachOut from a shared copy on the network, you may not be able to override supervisor-level security settings.See Chapter 7,* for Supervisors, *for details.*

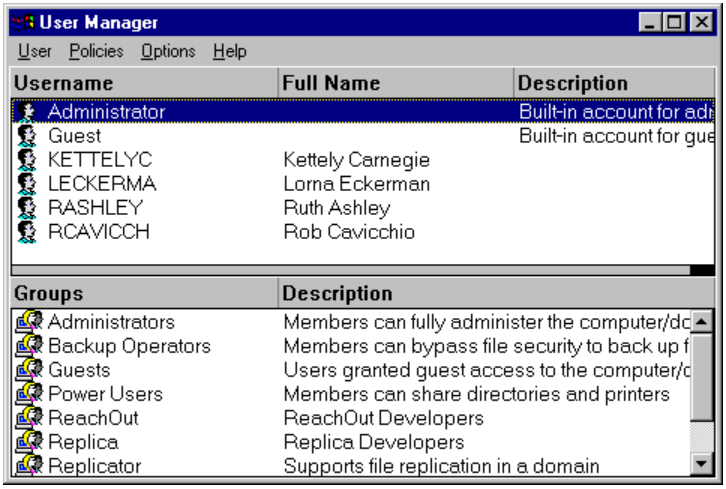
In this chapter...

User Accounts and Passwords

Use *passwords* to prevent unauthorized access to your computer. When a person tries to connect to your computer, ReachOut asks for a password. If the person provides the correct password, ReachOut allows the connection. You can determine the number of times a person can enter the password incorrectly before ReachOut terminates the connection attempt.

Issuing Passwords

In Windows NT, you issue passwords by giving each Windows user an *account* on the computer. The details of this account determine what the user can do when logged on to the computer. It doesn't matter how the user logs on—by physically starting up the computer, or by connecting from a remote system. Either way, the same user account determines the person's rights on that computer.



ReachOut for Windows NT fully obeys Windows NT user accounts. If you already have accounts set up for the users that you expect to connect to this computer with ReachOut, then your ReachOut password security is already in place. Just open ReachOut, and anyone with a valid user account can connect.

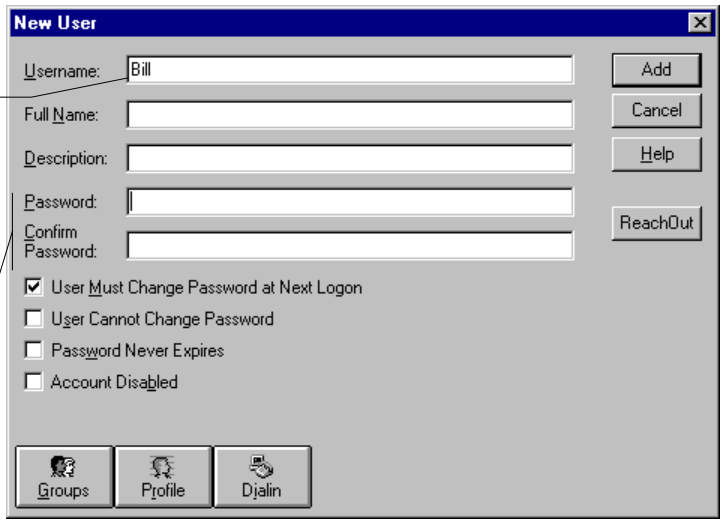
If you want to add user accounts to this computer or to change a user's password, you can do so directly through ReachOut.

Note: Not all users are allowed to add or change user accounts and passwords. If you are not a member of the "Administrators" user group on the Windows NT computer, you might not be able to do this.

To create or change a user account

1. From ReachOut's *Configure* menu, choose *Users* to open the Windows NT User Manager.
2. To create a new account, choose *New User* from User Manager's *User* menu.

   To change an account, double-click the user name.



If this is a new user, type a user name here.

Enter and confirm the passsword. It is case-sensitive, and it can be up to 14 characters long.

3. Enter the user's name and password, or change other settings as needed.

   IMPORTANT! The password is case-sensitive, so "PASSWORD" is not the same as "password". By default, ReachOut for Windows 95 and ReachOut for Windows & DOS always store passwords in uppercase letters, so if you want users to be able to connect with other versions of ReachOut, you must either give them passwords that are entirely uppercase, or upgrade the other version of ReachOut so that it can send mixed-case passwords. To learn how to do this, see the Read Me file in the ReachOut folder.

4. Choose *OK*.

Disabling Passwords

You can disable or delete a user account through User Manager.

IMPORTANT! Deleting a user account is an irreversible action. Even if you later add a user account with the same name, you cannot automatically regain that user's privileges. It is generally a better idea to disable the account rather than delete it.

To Disable a User Account

1. From ReachOut's *Configure* menu, choose *Users.*
2. Double-click the user name for the account you want to disable.
3. Check the *Account Disabled* box.

4. Choose *OK.*

Allowing Connections Without Passwords

For tight security, you should assign a password to each user account. However, there may be circumstances under which passwords are not necessary.

Suppose you want to allow guest access on a user account with limited rights. To make connecting easy for guest users, you do not want to require a password on this account. In this case, you can define a user account that does not require a password.

To create a user account with no password

1. From ReachOut's *Configure* menu, choose *Users*.
2. From User Manager's *User* menu, choose *New User*.

   If you want to remove the password from an existing account (such as the default "Guest" account), double-click the user name for that account instead.

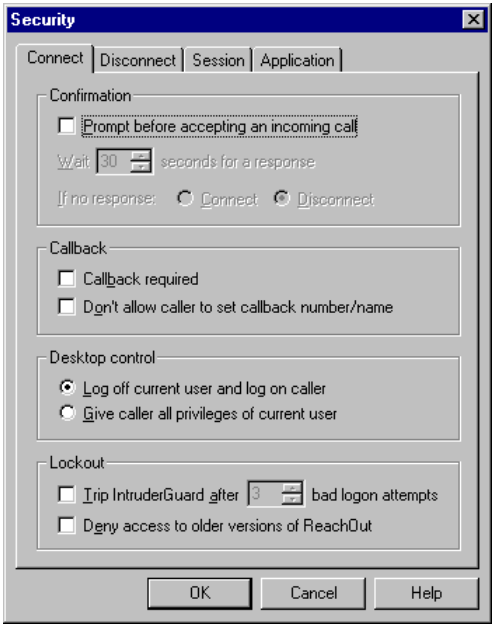
Note: If you are editing an existing user account, the account must first be set up to permit a blank password. To set this option, highlight the user and choose Account *from the* Policies *menu.*

3. For a new account, type a user name in the first field.
4. Leave the *Password* and *Confirm Password* fields blank. If you've already entered a password, simply delete it.
5. Choose *OK*.

A ReachOut user who connects using this account will still have to enter the user name ("Guest"). The user will be prompted for a password, but can simply choose *OK* without entering a password.

Additional Logon Security

In addition to passwords and standard Windows NT security, you can enable many ReachOut-specific security settings to help protect your computer. You can find many of these security settings by choosing *Security* from the *Options* menu. The *Connect* page lets you control access with logon privileges, callback, and connection confirmation, while the *Disconnect* page lets you decide what happens to your computer when someone disconnects from it.



To implement the security measures that are most appropriate for your environment, you will probably want to use a combination of Windows security and ReachOut security. This section covers some of the highlights of both. For complete details on security features, see ReachOut Help and Windows Help.

Note: If you have a shared installation of ReachOut, the ReachOut supervisor can turn on security features and prevent you from changing them. If this is the case, some of these options might be disabled in your copy of ReachOut.

The following pages explain how to protect you computer using these techniques:

- **Protect against intruders.** Decide how many times a person can enter an invalid password while trying to connect to your computer. A person who can't enter the correct password within the specified number of tries is locked out of the computer. You can set lockout security on an individual user level with Windows NT User Manager, or on a global level with ReachOut IntruderGuard.
- **Use callbacks**. If you don't want to take the chance of someone guessing your password and successfully connecting to your computer, use *callback* to verify calls before allowing a connection. Once a person calls your computer, ReachOut automatically terminates the connection and then calls the computer back at an expected number (for a modem connection) or by a specific ReachOut computer name or Internet address (for a network connection). You can also use callbacks to reverse telephone charges.
- **Confirm connections while you use your computer.** If you are using your computer while it is set to wait for calls, decide whether or not to allow connections to your computer.
- **Restart your computer on disconnect**. When a connection to your computer is terminated, restart the computer and ReachOut, which automatically logs off any users. You can set ReachOut up to automatically wait for calls when the computer restarts.

Protecting Against Intruders

In many cases, passwords alone do not provide enough security. You want to be sure that people cannot simply guess a password needed to connect to your computer. Intelligent intruders could write programs that quickly attempt millions of potential passwords—with a very real possibility of breaking your computer's password security.

To prevent this from happening, you can use *lockouts* to keep users from connecting again once they've tried and failed to connect. Lockouts can be implemented on an individual user level through User Manager, or on a global level through ReachOut security options.

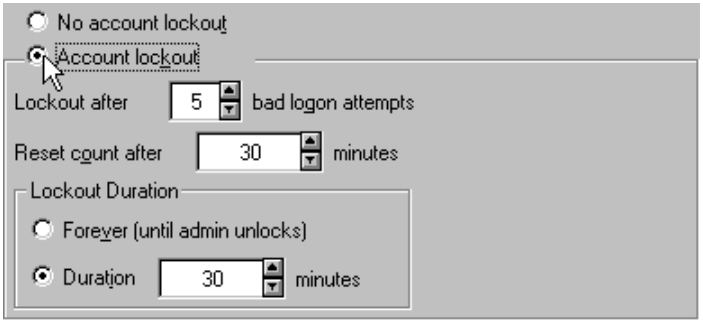
- For **individual account lockouts**, invalid passwords entered by any one user effectively freeze that user's account, preventing that user—and only that user—from connecting.
- For the **ReachOut IntruderGuard**, invalid passwords entered by *any* users effectively disable ReachOut, preventing *any* user from connecting.

Individual Account Lockouts

An individual account lockout prevents a user from connecting after that user has entered an incorrect password several times. When an individual user is locked out, other users can still connect. If you want to lock out all users when an individual password is incorrectly entered a certain number of times, you need to use the ReachOut IntruderGuard.

To add lockout security to a user account

1. From ReachOut's *Configure* menu, choose *Users*.
2. Select the account for which you want to add lockout security.
3. From the User Manager *Policies* menu, choose *Account*.
4. In the lower half of the Account Policy dialog box, choose the *Account lockout* option.



5. Change any other lockout options you want to set.

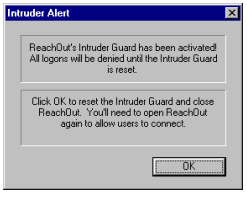
   By default, Windows sets the number of bad logon attempts allowed to 5. For tighter security, you can lower this number so that fewer logon attempts are allowed.

   Help

   For details on the other lockout options, choose *Help*.

6. Choose *OK*.

ReachOut IntruderGuard Security



The ReachOut IntruderGuard triggers an error on your computer if too many unsuccessful connection attempts are made in a row. Instead of locking out only one user, the IntruderGuard, once activated, prevents ReachOut from accepting calls entirely—effectively locking out all users. The only way to reset the IntruderGuard and allow connections again is to physically go to the ReachOut computer and close the Intruder Alert dialog box.

The IntruderGuard counts invalid logon attempts from all users—so even if each user enters only one incorrect password, the IntruderGuard will be activated once the total number of consecutive incorrect passwords entered by all users reaches the value you set in the ReachOut Security dialog box.

To enable the IntruderGuard

1. Choose *Security* from the *Configure* menu.
2. Under *IntruderGuard*, check *Lock out all callers*.

   The IntruderGuard is set to enable automatically after 3 retries. You can type or select a different number.

3. Choose *OK.*

Note: Unlike individual account lockouts, IntruderGuard security works for ReachOut connections only. Users can still log onto the computer through another method, such as Windows networking or file sharing.

Protecting Your Computer With Callback

In addition to protecting your computer with passwords, you can use *callback* to protect your computer even more by verifying calls to your computer before allowing a connection. When a person tries to connect, ReachOut will call the computer back at an expected number or by a specific Internet address or ReachOut computer name before allowing the connection.

You can also use callback to reverse telephone charges. For instance, if you are calling your computer at work from home and you don't want to pay for the call, you can set up your computer at work to call you back when you try to connect. When you call the computer, it will call you back at an expected number or by a specific name. Once satisfied, it will allow the connection.

Note: Callbacks work only on local Windows user accounts. If the waiting computer is on a Windows NT domain, you cannot set a ReachOut callback for a user account that is defined on the domain.

To set a callback

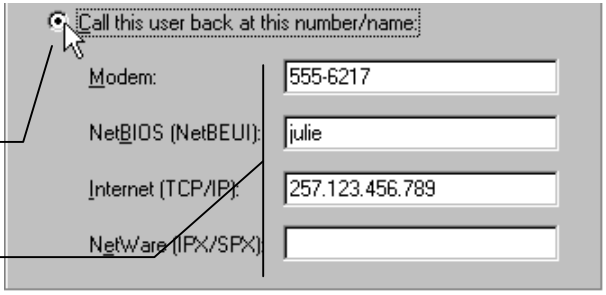
1. From ReachOut's *Configure* menu, choose *Users*.

   Note: To set a ReachOut callback, you must open User Manager through ReachOut. This option is not available if you run User Manager from the Windows Start *menu.*

2. Double-click the user account for which you want to set a callback.
3. Choose *ReachOut*.
4. Under *Call back*, choose *Call this user back at this number/name*.

Choose this option to have ReachOut automatically call back the connecting user.

Type the callback information in these fields.



5. Type the phone number or network name that you want ReachOut to use to call the user back.

   Be sure to enter the information next to the appropriate connection type. If you want the user to be able to connect with more than one connection type, you can enter callback information for each connection type. ReachOut will detect how the call came in and select the appropriate information to use when calling back.

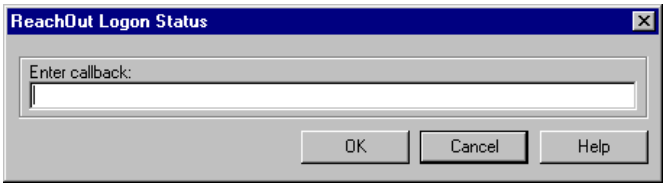
6. Choose *OK*.

If you are using callback with callers who use varied phone numbers, you can let ReachOut ask for the number to call back. This is useful if a user routinely connects from different locations and you want to reverse telephone charges—for example, if an employee is on a business trip. However, this use of callback is *not* a security measure.

To have ReachOut prompt for a callback

1. From ReachOut's *Configure* menu, choose *Users.*
2. Double-click the user account for which you want to set the callback.
3. Choose *ReachOut.*
4. Under *Call back*, choose *Set by caller.*
5. Choose *OK*.

The connecting user will see the following message prompting for the callback name or number. In most cases, this is a phone number where the user is waiting.



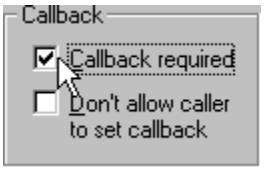
ReachOut will disconnect, then call back at the number or name the caller supplies. The computer that originated the call still acts as the calling computer and can use remote control or ReachOut Explorer.

Callback Security Options

At times, you might want to force all user accounts to use callbacks when connecting to your computer. Instead of changing the properties of each user account, you can simply have ReachOut deny access to the accounts that do not have callbacks set up.

To enforce callbacks

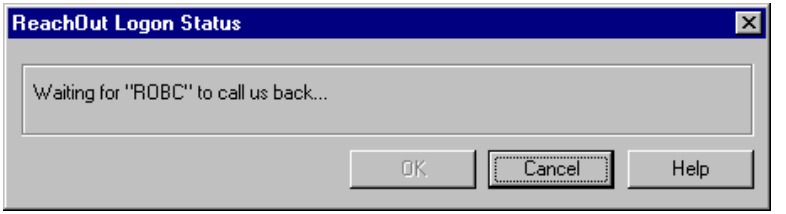
1. Choose *Security* from the *Configure* menu.
2. On the *Connect* tab, check *Callback required*.



3. To make ReachOut also deny access to accounts that let the caller enter the callback number, check the box labeled *Don't allow caller to set callback number/name*.
4. Choose *OK*.

Connecting to a Callback Computer

When you connect to a computer that is set up for callbacks, you see a message similar to this before you are allowed to connect.



While you're viewing this message, the other computer is verifying your connection and calling you back. Once the connection is made again, you can perform whatever actions you want (such as remote control or file transfer)—as long as you have access rights for those actions.

Determining Who's Logged On

If you're using your computer when another user attempts to remotely control it, one of two things must happen:

- You stay logged on, and the caller temporarily gains the rights you have to your computer.
- The caller is logged on (and you are logged off), giving you the rights the caller has to the computer.

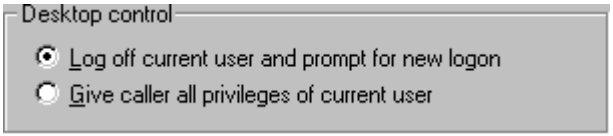
You can choose how you want ReachOut to handle this situation.

Note: You can also have ReachOut prompt you whenever a user tries to connect, and decide at that time whether or not to let the user in. For information about this feature, see Confirming Connections, *on page 62.*

IMPORTANT! If you have ReachOut log the caller on, Windows NT must close all open programs and display the logon prompt when a caller tries to use remote control. To have this happen without breaking the ReachOut connection, you need to set ReachOut to wait for calls as soon as the computer starts. Set this option by choosing Options *from ReachOut's* Configure *menu.*

To choose which user is logged on

1. From ReachOut's *Configure* menu, choose *Security*.
2. Under *Desktop control*, choose what you want ReachOut to do when a remote user tries to control your computer.



3. Choose *OK*.

Note: This setting applies only to remote control users; it does not affect callers who only use ReachOut Explorer. For file transfers, each connected user has the rights assigned by that person's user account.

Logging Off Disconnected Users

When the caller disconnects, you have the choice of leaving that caller logged onto the computer, or having ReachOut automatically log the caller off. If you decide to log the caller off, you might also want to have the computer restart just to clear the system and make sure there aren't any problems preventing users from reconnecting.

To choose what happens upon disconnection

1. From ReachOut's *Configure* menu, choose *Security*.
2. Choose the *Disconnect* tab.
3. Under *When a call is disconnected*, choose what you want ReachOut to do.

Note: If you have your computer restart and you want users to be able to connect again, you'll need to tell ReachOut to start waiting for calls when the computer starts. Set this option by choosing Options *from the* Configure *menu.*

4. Choose *OK*.

Confirming Connections

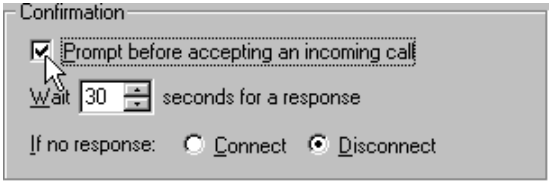
Even if a person has a valid password, you can set up your computer to notify you when that person tries to connect. This allows you to verify the password before allowing the connection.

You might choose to confirm connection attempts for either of the following reasons:

- As an added security measure, so that a user at the waiting computer must personally confirm each caller before allowing that caller access to the computer.
- As a convenience, if someone might be already using the computer when a caller tries to connect. Turning on confirmation notifies the current user of the connection attempt and gives that user a chance to save any work, or to prevent remote control until the computer is no longer in use.

To let you confirm all connections

1. Choose *Security* from the *Configure* menu.
2. Check the box labeled *Prompt before accepting an incoming call*.



3. Type or select the number of seconds you want to give the current user to respond to the prompt.

4. Next to *If no response*, choose what you want to happen if no one responds to the confirmation prompt. For tight security, choose *Disconnect* so that no unconfirmed callers get through.
5. Choose *OK*.

Remote Control Security

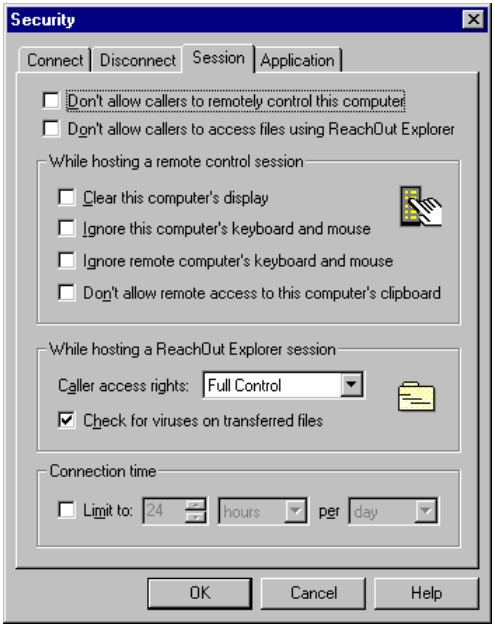
You can use ReachOut's security features to limit what a user can do with your computer during a remote control session.

On a global level, you can determine whether a person can copy data from your Clipboard using ReachOut's Remote Clipboard. You can also set up your computer to automatically end a connection if the other computer hasn't used your computer after a specific amount of time.

You can also prevent the caller's keyboard and mouse actions from being transmitted to your computer, or disable remote control entirely.

To set remote control security

1. Choose *Security* from the *Configure* menu.
2. Make changes on the *Session* tab, and choose *OK*.



Protecting Your Files

The most important thing on your computer is its files. By default, everyone who connects to your computer has *Full* file access rights.They can copy, delete, create, and rename your files and folders. You can change file access rights on a global level, or on a file-by-file basis.

Windows NT and ReachOut give you many ways to control rights to files. You can use any or all of the following methods to specify what rights users have to access specific files on your computer:

- You can prevent remote control of your computer.
- You can limit or prevent the use of ReachOut Explorer to create, change, rename, delete, or copy your files.
- If a file is on a disk or a disk partition that uses the NT file system (NTFS), you can set the properties of a file or a folder to specify which users have access to that file or folder.

ReachOut Explorer Security

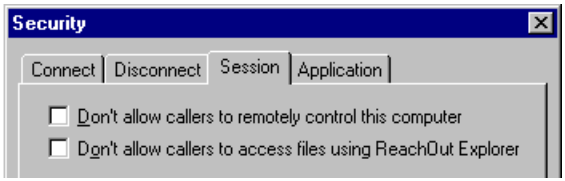
You can set a default level of access to your files:

- **Full Control**, which lets users create, change, move, delete, rename, and copy files and folders, as well as take ownership and decide who has access to files.
- **Change**, which lets users create, change, delete, rename, and copy files and folders.
- **Read/Write**, which lets users copy files and folders to and from your computer—but not move, rename, or delete your files and folders.
- **Read**, which lets users copy your files and folders to their computers, but not create, change, or delete files and folders on your computer.

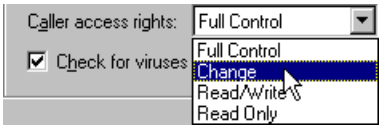
A connected ReachOut Explorer user never has more access than the level you choose under ReachOut security—regardless of the user's individual rights to files on the computer.

To set file access for ReachOut Explorer

1. From the ReachOut *Configure* menu, choose *Security*.
2. Choose the *Session* tab.
3. To prevent access completely, check *Don't allow callers to access files using ReachOut Explorer*.



4. Under *Caller access rights*, choose the maximum level of file access you want all connecting users to have. Choose *Full Control*, *Change*, *Read/Write*, or *Read Only*.



Note: If you installed ReachOut from the network, you can't override ReachOut supervisor security.

5. Choose *OK*.

IMPORTANT! ReachOut Explorer security does not apply to remote control users who access your computer's files through your Windows desktop. To limit file access for remote control users, you must edit the file properties of the appropriate files and folders. The next section explains how to do this.

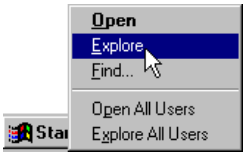
Windows NT File and Folder Security

Windows NT lets you set permissions on files and folders that are stored on a disk or a disk partition that is formatted to use the NT file system (NTFS). You can decide who has access to any given file or folder, as well as what level of access each user has.

Note: This level of security is not available on drives that use the standard DOS (FAT) file system.

Normally, you assign access to files and folders by *groups* of users, not by individual users (although you can do either). Therefore, you need to be sure that your user groups are named in a convenient way and that all users belong to the correct groups. Once you've done this, you can easily assign file rights to particular groups.

To set access rights to a file or a folder



1. Open Windows Explorer.

   You can do this by right-clicking the Windows *Start* menu and choosing *Explore*.

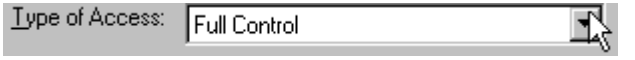
2. Browse to the file or folder for which you want to set permissions.
3. Right-click the file or folder and choose *Properties*.
4. Choose the *Security* tab.

   If you don't see a *Security* tab, the file or folder is not stored in an NT file system. You cannot set individual access rights for this file or folder.

5. Choose the *Permissions* button.
6. Use the *Add* and *Remove* buttons to place groups of users in the list.

   Tip! *If you choose* Add *and then choose the* Show Users *button, you can add individual users as well as groups to the permission list.*

7. To determine the level of file access each group has, select the group and choose the access level you want from the *Type of Access* list.



8. Choose *OK*, and close the Properties dialog box.

Note: Whether you can change the permissions on a file or a folder depends on who owns the file. To learn more about ownership, choose the Ownership *button on the* Security *page, then choose* Help.

Virus Checking

Anyone you give "Full Control" or "Change" access may copy data to and from your computer. You might consider enabling ReachOut virus checking on your computer if you want to ensure that files transferred to your computer are virus free.

Note: ReachOut can't virus check compressed (such as ZIP) files.

To have ReachOut check files for viruses

1. From ReachOut's *Configure* menu, choose *Security*.
2. Choose the *Session* tab.
3. Check the option *Check for viruses on transferred files*.
4. Choose *OK*.

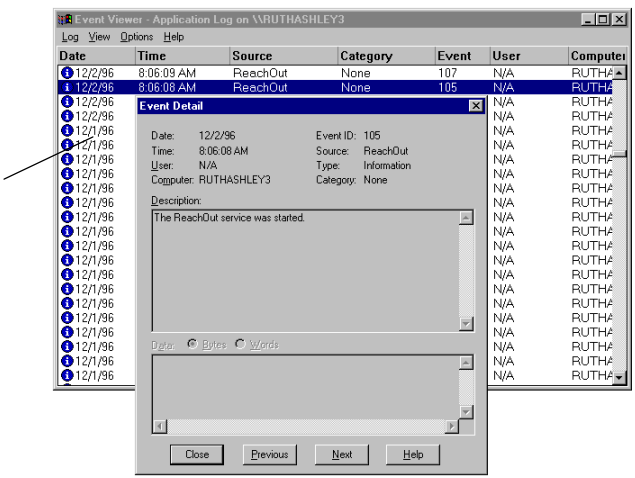
Auditing ReachOut Events

ReachOut records important information about the ReachOut program and connections to your computer in the Windows Event Log. The Event Log shows who connected to your computer, how long the connection lasted, and any unsuccessful connection attempts.

To view the Windows Event Log

1. Choose *Event Log* from the ReachOut *View* menu.

The Event Log shows successful and unsuccessful connections to and from your computer.



2. Double-click an event to see the details.

Giving Access to ReachOut

All of the security measures you implement do little good if anyone can change them. Before you finally let ReachOut users connect to your computer, you should check ReachOut's *application security* settings to make sure you have given rights to change ReachOut settings to the correct users.

For example, you probably don't want most callers to be able to change ReachOut's security settings. If they could, then they could simply connect and turn off the security features that you implement. To prevent this, you can tell ReachOut exactly which users are to be given access to the security settings, so ReachOut knows not to let others in.

To administer ReachOut application rights to a user, that user must be part of one or more user groups defined on your computer. Windows comes with six built-in user groups, including the "Administrators" group. *Members of the "Administrators" group can always change any ReachOut settings*, regardless of which groups you select in the application security settings. If you want to have full control over all ReachOut settings, make sure you are an Administrator on your own computer.

By default, ReachOut application security contains the following settings:

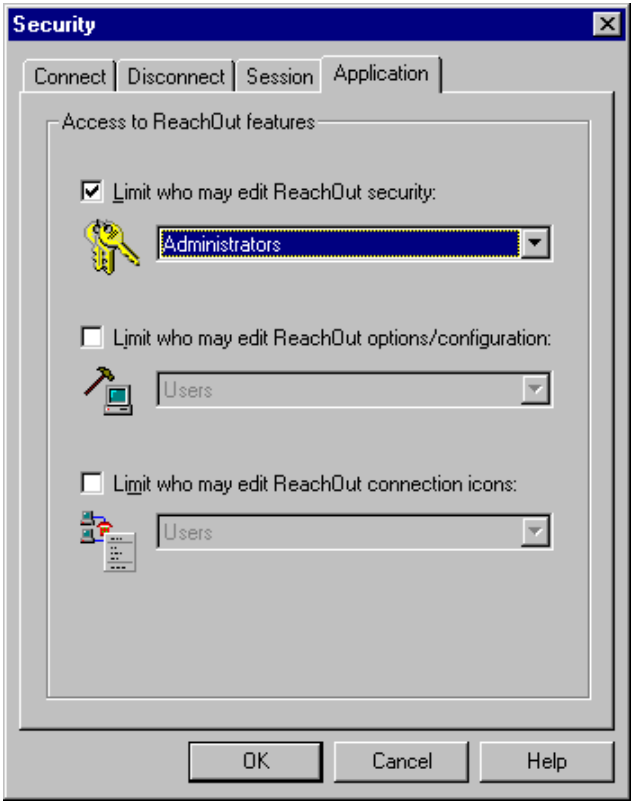
These settings...	May be changed by...
Security	Administrators
Options and configuration	Everyone
Connection Icons (creating, editing, or deleting)	Everyone

To limit who may access ReachOut

1. From ReachOut's *Configure* menu, choose *Security.*
2. Choose the *Application* tab.

3. For any or all of the three areas (security, options, and connection icons), check the *Limit who may edit* box.
4. For each group of settings you limit access to, choose which group of users you want to grant the access to.

   Keep in mind that members of the "Administrators" group can change any settings. If you want to limit access to a group of settings so that *only* members of the "Administrators" group can change them, simply choose *Administrators* in the list.
5. Choose *OK.*



6 ReachOut CONFIGURATION

Windows configures your modem or network, so you normally don't have to configure them to use ReachOut. You'll find detailed help on configuration and troubleshooting in Windows Help.

This chapter includes configuration information you might need to modify modem or network configurations and make ReachOut connections. Once you can connect, you'll only have to worry about configuration if you have multiple modems, if your computer is on more than one type of network, or you change the hardware or the software that controls your communications.

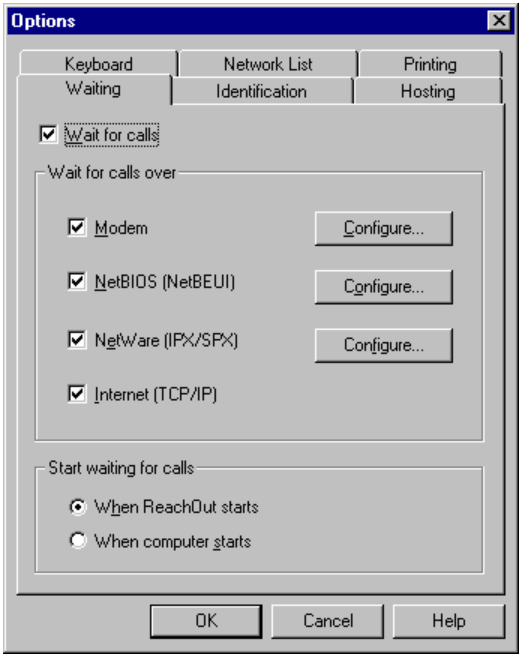
In this chapter...

ReachOut Configure Menu

The *Configure* menu lets you set ReachOut Security, access the Windows NT User Manager, and set options that affect how you use ReachOut.

The *Security* and *Users* commands are covered in Chapter 5, *ReachOut Security*.

When you choose *Options* from the *Configure* menu, ReachOut presents a multiple-tabbed dialog box. This chapter covers the Waiting, Identification, and Network List options.



Settings on the Hosting, Keyboard, and Printing tabs deal specifically with remote control. See Chapter 4, *Remote Access*, for more details.

Configuring Waiting Options

You can tell ReachOut to start waiting for calls when your computer starts or when you start ReachOut. For better control over when calls can be accepted, choose *When ReachOut starts*. To allow callers to

connect any time the computer is running, choose *When computer starts*.

You can use additional measures to control which calls are received. See *Confirming Connections* in Chapter 5 for details on how to determine whether incoming calls get through.

Your computer can wait for calls over a modem or on any of three network protocols: NetWare, NetBIOS, or TCP/IP (Internet protocol). The configuration details are different for each. Modem configuration is handled through standard Windows NT dialog boxes.

Note: If you installed ReachOut from a network, the supervisor may have limited the ways you can wait for a call. See your network administrator if you can't access the type you need.

Configuring Your Modem

You may need to change the way your modem is set up to communicate with another computer's modem (for instance, the other computer's modem can only receive data at 9600 bps, and your modem is set up to always connect at 28,800). At times, the communication line can interfer with your connection and you will want to select a lower speed that works.

If a connection icon uses the modem in a unique way, you will want to configure it individually. You can configure the modem properties for each connection icon and tailor the configuration for each.

If you switched modems or if you moved your modem to a different communication (COM) port, you can configure it within Windows or within ReachOut. To make the changes affect all uses of the modem under Windows NT, modify your configuration under Windows NT directly, using Control Panel.

IMPORTANT! Changes you make to the modem configuration under ReachOut apply only to ReachOut. If you make any modem configuration changes under ReachOut, later changes to the Windows NT modem configuration won't affect ReachOut because the information is stored separately.

Configuration a Modem for Waiting

You can configure a modem globally to apply to all incoming ReachOut calls. If you use your modem with other applications as well, you'll probably want to do any global configuration under Windows NT.

To configure a modem for incoming calls

1. Choose *Options* from the *Configure* menu.
2. Choose the *Waiting* tab and check *Modem*.
3. Click the *Configure* button next to *Modem*.
4. If you have more than one modem, choose the one you want to configure from the list. Be sure the *Wait on this modem* box is checked, then choose *Configure*.
5. Modify the modem's property sheet as needed.

Note: If you change any of your modem settings through ReachOut, the settings apply only when you use ReachOut. Changes you make to that modem later under Windows NT have no effect under ReachOut.

Waiting Over Multiple Modems

ReachOut can wait for calls on any or all of your modems. Just make sure the *Wait on this modem* box is checked when each modem is selected in the Waiting Modem dialog box. (Refer to the previous set of instructions on configuring a modem.) Of course, only one caller can use any given modem line at one time.

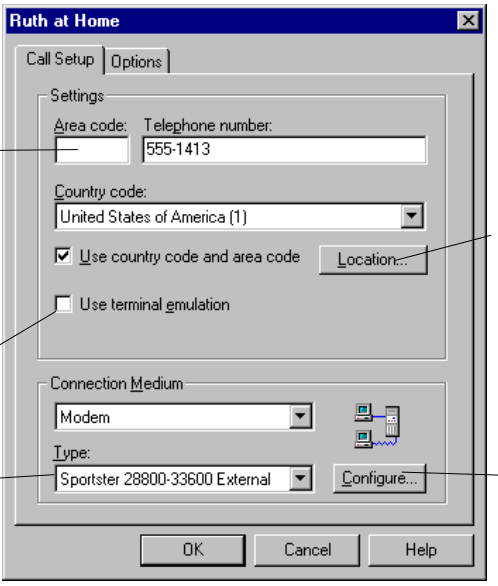
Configuring a Modem for Connection Icons

You can change the modem properties for any connection icon individually. These apply to outgoing ReachOut calls only.

To modify properties for a connection icon

1. Right click the connection icon and choose *Properties*.

   ReachOut displays a dialog box like this one. The information you see was supplied when you created the connection icon. You can make changes as indicated on the next page.



Change the phone number

If the connection needs terminal emulation, check it here. ReachOut will ask if necessary.

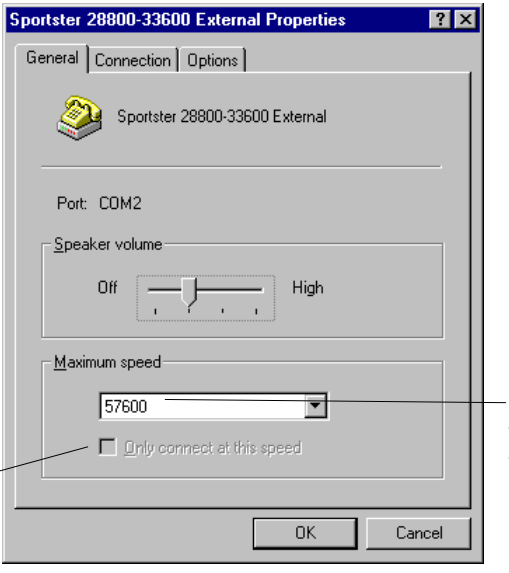
Choose a different modem

Change the location you are calling from

Configure the current modem

2. Change the *Connection Medium* to *Modem* if necessary. To make specific modem changes, click the modem's *Configure* button. ReachOut opens the property sheet. In most cases, you should make these changes under Windows NT so they apply to all applications.

3. Modify the Windows modem property sheet as needed.

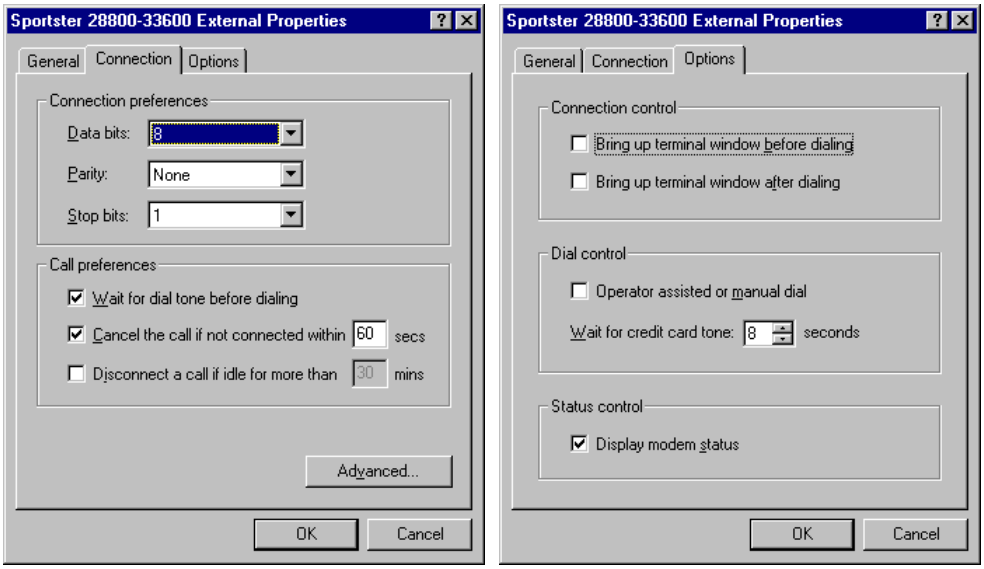


Check *Only connect at this speed* if line noise interferes or if you suspect hardware problems.

Maximum speed fields help you test your modem.

The *Connection* tab lets you provide additional information about how to connect. This is where you set the parameters for the connection. You can also change the timeout defaults that apply when ReachOut is establishing a modem connection.

The modem properties *Options* tab lets you to specify options such as operator-assisted dialing or credit card calls. You can also have Windows open a terminal window so you can type specific modem commands.



Problems Connecting Via Modem?

If you're having problems connecting to a computer over a modem, check the number you are trying to reach, the modem itself, and the cable.

- Make sure the number is correct and that you used the right area code. If you need a special dialing prefix (such as 9), make sure Windows knows it. Open Modems in the Windows Control Panel and click the *Dialing Properties* button. (If you didn't check *Use country code and area code*, ReachOut doesn't recognize the 9 you put in Dialing Properties.)

- Make sure your modem has power and is connected to a phone line. This is a bit different for internal and external, standard and ISDN modems, but check the documentation for your modem if you aren't sure it is connected right.
- Make sure the modem cable **is not** a null modem cable; you need those only for direct cable connections. You might want to try a different cable to see if the problem goes away.
- Try connecting to a different computer. This will help you identify whether the problem is with your modem or with where you are trying to connect.
- Have someone else try to connect to your computer. This will let you know if you have problems with incoming calls as well.

If you have the correct number and cable and you're still having problems, try isolating the problem by connecting to Stac's Download Services via Windows HyperTerminal (see the *Accessories* menu) rather than with ReachOut. If you connected without problems, then make sure you're connecting to the remote computer using a valid number and password.

Changing Your Network Settings

When you connect two ReachOut computers via a company's local area network or via the Internet, the communication process requires the communication protocols on the computers to be set up correctly. When you install ReachOut on the computers, it detects and selects the correct communication protocol automatically.

For example, on a Novell NetWare network, the communication protocol is usually IPX/SPX. On the Internet, the communication protocol is TCP/IP. The NetBEUI communication protocol, which is compatible with NetBIOS, is usually used for a network based on Windows 95, Windows for Workgroups, Windows NT, or LAN Manager, with computers directly connected.

Many networks support several protocols. For example, your company may use NetWare IPX/SPX for the primary LAN. But users will use TCP/IP when they connect to the Internet and NetBEUI (a form of NetBIOS) when they use direct cable connections.

ReachOut makes it easy for you to provide any additional information you want for each communication protocol. Choose *Options* from the *Configure* menu to change the settings. For specific information, you may have to check with your network administrator.

To change your network settings

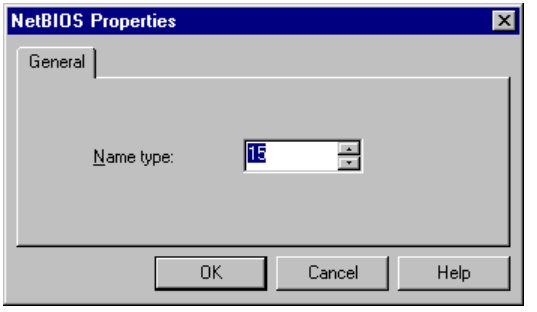
1. Choose *Options* from the *Configure* menu.
2. On the *Waiting* tab, choose the network type you want to change.
3. On the resulting window, make the appropriate changes.

   A typical window for each network is shown in the next section.

To remotely change the communication protocols for the computer you're connected to, you'll need to have the proper access to that computer.

NetBIOS

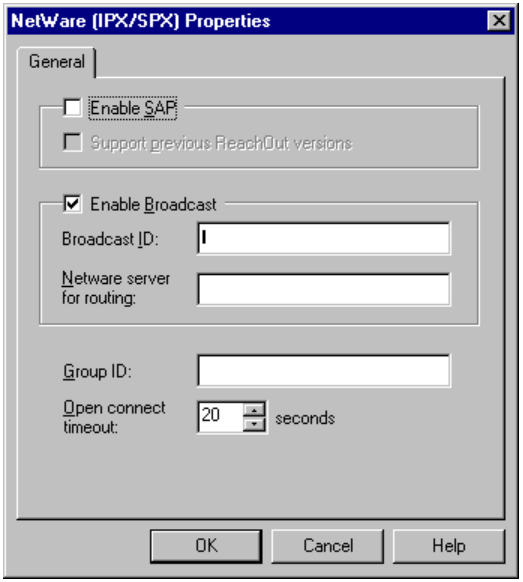
Choosing to configure a NetBIOS network results in this window:



If you have trouble connecting over a NetBIOS compatible network, including NetBEUI, make sure the protocol is installed and works for your other communications. If so, you might want to change the *Name type* to 32.

NetWare IPX/SPX

Choosing to configure a NetWare IPX/SPX network results in this window:



For NetWare, you can enable SAP or Broadcast as the connection method. If you *Enable SAP,* you can choose to support previous ReachOut versions if needed.

If you choose to *Enable Broadcast*, you can supply a *Broadcast ID*, which means you'll only be able to communicate with other ReachOut computers that have the same Broadcast ID. Other ReachOut computers won't even appear in your network list. You probably won't need a *NetWare server for routing* unless you have a complex network with many segments, but it's a good idea to specify your login server anyway. If your network list doesn't seem to include all the waiting ReachOut computers, specifying your login server might solve the problem.

If you specify a *Group ID*, you will only be able to connect with other computers that have the same Group ID specified. By default, all ReachOut computers have the same Group ID.

To change how long ReachOut waits for a computer to respond when it tries to make a connection over the NetWare network, change the *Open connect timeout*.

Internet

You don't need any special configuration to use ReachOut across the Internet. Both computer must be on the Internet (using a windows based TCP/IP protocol), and one computer must be waiting over the Internet. The calling computer must use the Internet hostname or the specific IP address of the waiting computer.

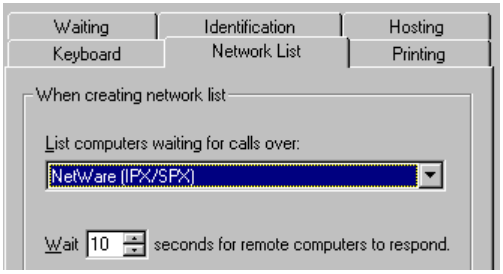
Problems Connecting Via Network?

If you can't connect from a connection icon you created, the computer may not be ready and waiting. Check the Network List view in ReachOut and make sure it is available.

Check your network configuration on both your computer and the one you are trying to connect to. Make sure you have specified the correct communications protocol for your network. Make sure the computers do not have different Broadcast or Group IDs. If networks on both computers are configured correctly, the systems should connect. If not, check with your network administrator.

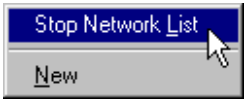
Configuring Network List Options

You can control how ReachOut prepares the network list of ReachOut computers waiting on a NetWare or NetBIOS network that you can display in the ReachOut window. ReachOut does not generate a network list of computers waiting on the Internet.



Choose the network type (NetWare or NetBIOS). Then specify how long to wait for computers to respond. A very large or complex network may take more time to identify all the computers.

The network list is updated continually while it is displayed. When waiting computers respond, ReachOut displays their icons immediately. At regular time intervals, ReachOut resends the network list request to see if any new computers are waiting for calls. By default, ReachOut waits ten seconds for computers to respond before resending the network list request. You can decrease this number to get updates more often, or you can increase the number to give waiting computers more time to respond to each request.



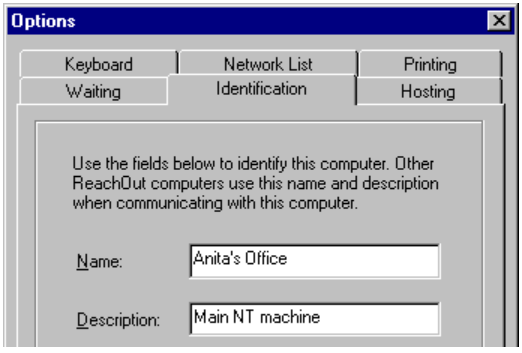
Tip! *If a continually updated network list is getting in your way, you can stop the list at any time by right-clicking in the ReachOut window and choosing* Stop Network List. *To continue updating the list at a later time, right-click again and choose* Start Network List.

Identifying Your Computer

When you installed ReachOut, your Windows NT computer name automatically became your ReachOut computer name. This name appears in network lists and is used by others to connect to your computer over a network.

To change your computer's ReachOut name

1. Choose *Options* from the *Configure* menu.
2. On the *Identification* tab, enter a new name.
   You can use up to 15 characters.



3. In the *Description* field, add a short description.
   The description appears in network lists.

Troubleshooting Connections

If you've set up your modem or network and you can't make a ReachOut connection, you might want to check the Troubleshooting section of ReachOut Help. It contains a number of useful suggestions that might help you solve connection problems.

7 ReachOut FOR SUPERVISORS

Your users will be accessing their computers from home, on the road, and other locations. As the ReachOut supervisor, you can protect your company's data by implementing security globally. You have several options:

- **Install ReachOut on the network**. Require that users install ReachOut from your network to pick up your security settings. You can also customize ReachOut so that your users install only certain components.
- **Use ReachOut Supervisor Security to set global ReachOut security**. You can set minimum security and require callbacks to ensure that only authorized users are accessing the computers. Your settings prevent users from making less secure settings on their copy of ReachOut.
- **Require that users dial in to a gateway system.** This allows you to verify computers dialing in before they connect to company computers.
- **Allow Internet access only to those who need it.** Make sure your company's firewall (network security system) allows access only to those people who need to have the ability to access your computers via the Internet. Make sure your users understand that they should not give their computer's IP address to just anyone.

In this chapter...

Installing ReachOut on the Network

As the ReachOut supervisor, putting ReachOut in a network directory from which your users can install ReachOut allows you to centralize and control ReachOut. With a network installation, you can:

- **Customize ReachOut so that your users install only the components you want them to install or only the ones they need.** For example, you can customize ReachOut so that once it is installed on a user's computer, the user can only use the computer to make calls and not be allowed to wait for calls.
- **Implement global security measures that affect all your ReachOut users.** For example, you can force callbacks, refuse all connection attempts after three incorrect password entries, force a a minimum level of security for file transfers with ReachOut Explorer, and so on.

IMPORTANT! To install ReachOut on the network, you'll need a multi-user ReachOut license.

Network Installation Options

You have three options for making ReachOut available to your users from a network drive. The next section includes details for all three options.

1. Copy the contents of the ReachOut Setup disks onto a network drive. With this type of installation, you can't enforce global security. Users will need to implement their own ReachOut security measures.
2. Install ReachOut on a network drive using SETUP SHARED and have your users run SETUP from this directory to install only essential ReachOut system files on their computers and use the remaining files directly from the network directory. This

installation option allows you to define a *minimum level of security* for all ReachOut users who installed ReachOut from the SHARED network installation.

3. Install ReachOut on a network drive using SETUP SHARED, and write an installation script to customize ReachOut for your users. This allows you to customize ReachOut and implement global security.

Copying ReachOut CD-ROM to the Network

For convenience, you may want users to install individual copies of ReachOut on their workstations from a network location.

To copy ReachOut to the network

1. Insert the CD-ROM into a CD-ROM drive.
2. Locate a network folder with at least 15 MB space.
3. Create a folder to hold the data; name it something like *ROshare*.
4. Within Windows NT, drag the entire set of files and folders to the network folder.

Users can now run SETUP.EXE from the DISK1 folder much the same way they would if they were installing ReachOut directly from CD-ROM or floppy disks.

Note: ReachOut security will not be implemented globally. Users will have to implement their own security measures.

Installing ReachOut Shared

Run SETUP SHARED to install a multi-user ReachOut license on a network drive for public installation. During this type of installation, ReachOut does the following:

- Copies ReachOut public installation files to the specified network folder. To install ReachOut at their workstations, your users just run SETUP from that directory.
- Installs crucial system files in a folder on your local computer.
- Installs SECURITY.EXE on the computer you choose, which allows you to specify global security settings.

When your users run SETUP, ReachOut copies only the necessary ReachOut files to their computers. When you and your users run ReachOut, most of the files are accessed directly from the ReachOut network directory.

To install ReachOut for public use

1. Choose *Run* from the *Start* menu.
2. In the Run box, type the path to Disk 1 and enter SETUP SHARED instead of SETUP.
3. Click *OK*.

   The Setup wizard steps you through the process. It will ask you to select a network drive to install ReachOut, a local folder for installing ReachOut, and a computer on which to install Supervisor Security.

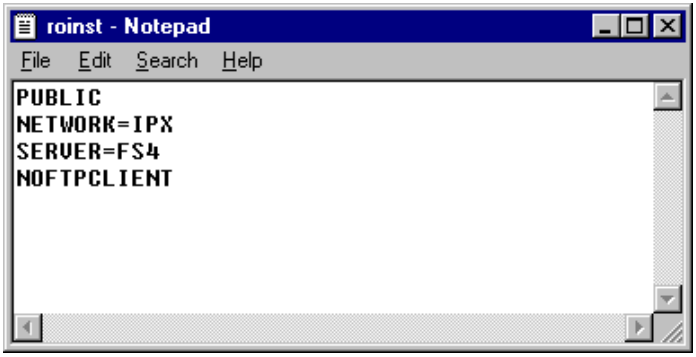
After installing ReachOut with SETUP SHARED, you will probably want to set global security before users install ReachOut. See *Setting Global ReachOut Security* on page 89 for details.

Scripts for Custom Network Installation

Create the script using any text editor such as Windows Notepad or WordPad. If the same script applies to all users, you can modify an existing file named ROINST. If you have different scripts for different users, tell each user to run SETUP *scriptname* on the network drive (*scriptname* is the name of the script file).

When you have installed ReachOut with SETUP SHARED, you can write an installation script that customizes ReachOut for your users; use any text editor. The default script (named **ROINST**) includes PUBLIC as the only command. To enforce shared security settings, you must include PUBLIC as the first line of any script. This tells SETUP that it is doing a public installation when users run SETUP.

In the script, you can add keywords to customize ReachOut. Save the file with the same name if you want it to apply to all your users. If different users need different setup scripts, you can create several files and save them with different names. The figure shows an example script that forces a user to connect to another ReachOut computer via NetWare, and prevents the use of SuperFTP Client to connect to Internet FTP hosts.



For complete details on the entries you can make in the script, search for “scripting” in Help. The following table lists some of the more commonly used keywords for installation scripts. The online help includes complete information.

Note: There is a limit to the length of each line in the script. ReachOut ignores anything after the first 200 characters on a line.

To do this...	Type this line...
Install only ReachOut data files and configuration files.	PUBLIC
Install ReachOut to a specific folder.	TARGET=path_name
Specify a directory under which a user can install to any subfolder.	TARGET=path_name\%1
Configure to make calls only.	TYPE=Viewer
Don't allow use of the FTP client.	NOFTPCLIENT
Set the network type for making or receiving calls.	NETWORK=network_protocol [Types: NetBIOS, IPX (*for NetWare*), and Winsock (*for Internet*)]
Set the computer's name.	NAME=computer_name
Allow users to type the computer name with the install command (for instance: SETUP MYCOMPUTER).	NAME=%1
Set a NetWare server for routing.	SERVER=server_name

To create a new installation script

1. Use any text editor and create a new file.
2. Type the installation commands and settings you want. Include PUBLIC as the first line in the script file.
3. Save the file as Read-Only.
4. Have users install with SETUP *scriptname* so ReachOut will copy the necessary files to the user's computer.

Note: If you modify the file ROINST instead of creating a new one, all your users need to do to install ReachOut is to run SETUP.

Setting Global ReachOut Security

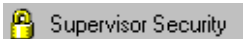
The first step in implementing global ReachOut security is to install ReachOut on the network running SETUP SHARED, and have your users do a public installation from the network. The previous section in this chapter explains how to do this.

The second step is to run ReachOut Supervisor Security and implement the security features you want to apply to all users who install ReachOut from the network.

Note: ReachOut Supervisor Security has no effect on ReachOut's FTP connections. However, you can prevent users from making FTP connections by adding NOFTPCLIENT to an installation script.

When users do a public installation of ReachOut, they will not be able to override your security settings. If, for example, you force callbacks, your users cannot bypass callbacks. If you change the settings later, the new settings apply to all public installations of ReachOut.

To run ReachOut supervisor security



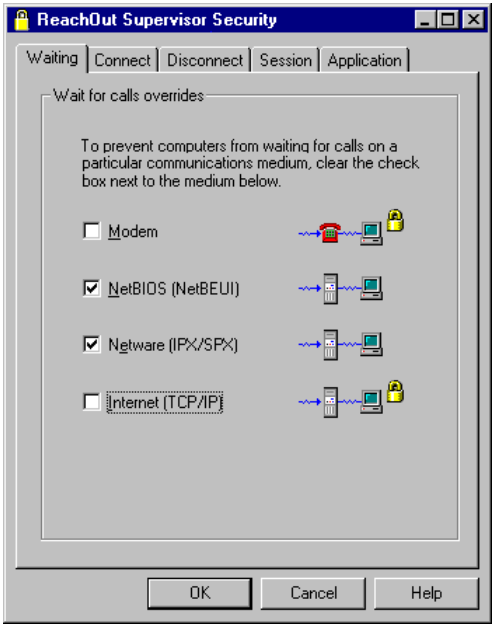
1. From the Windows *Start* menu, choose *Programs*.
2. Choose *ReachOut*.
3. Choose *Supervisor Security*.
4. In the ReachOut Supervisor Security window, make the desired global security settings.

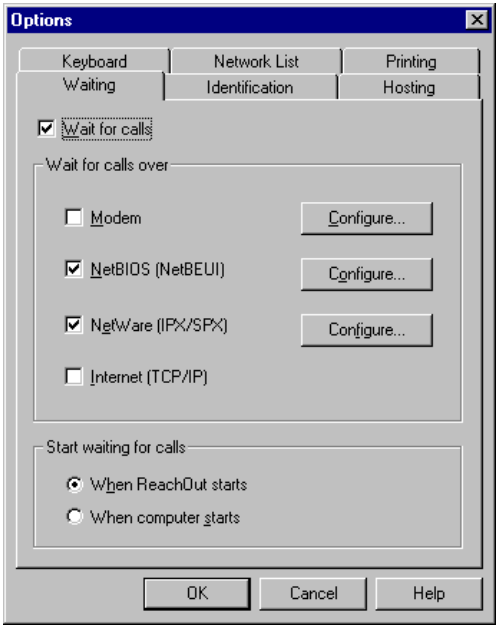
The Supervisor Security settings are summarized on the following pages. In most cases they work exactly as described for individual users in Chapter 5. Any settings you turn on here, however, are disabled for individual users, so they can't shut them off.

Waiting Security

You can prevent users from receiving calls on any or all of the connection types. By default, ReachOut accepts calls over any modem or network that is present on the user's computer. If you want to prevent calls from connecting over the Internet, uncheck *Internet*. To prevent receiving of direct modem calls, uncheck *Modem*. You'll see locks appear next to the connection types that you have made unavailable to users.

Note: These settings prevent incoming calls only. Users can still make outgoing connections over any connection types their computers are set up for.

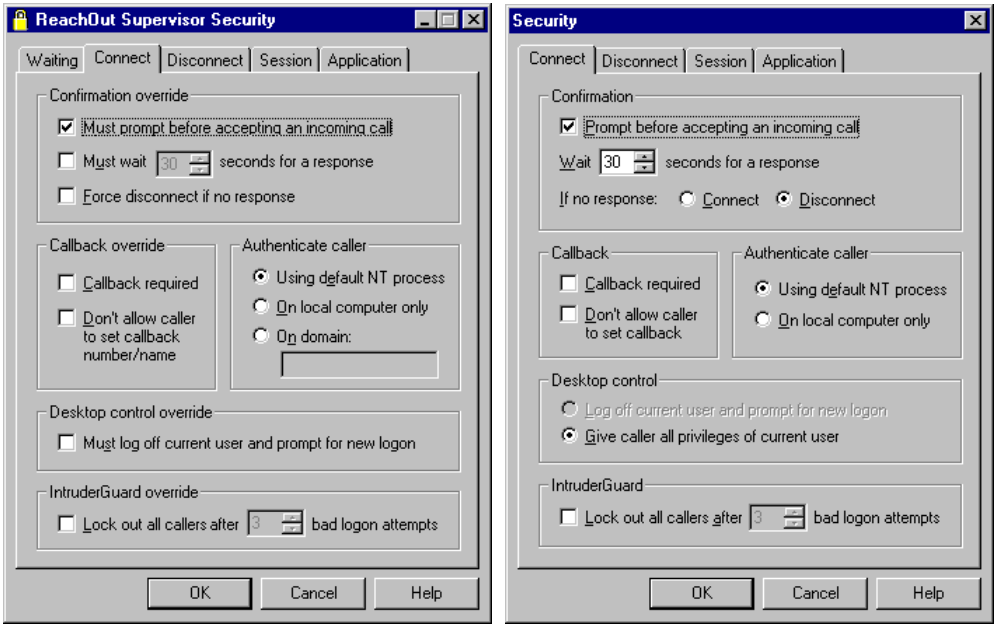




Connection Security

You can force users to use prompts, callbacks, logons, and lockout at the level you require to ensure that incoming connections are secure. The fields on the Supervisor Security *Connect* tab parallel those on the ReachOut Security *Connect* tab reached through the *Configure* menu. You can specify overrides that enforce the security or usage limits you need.

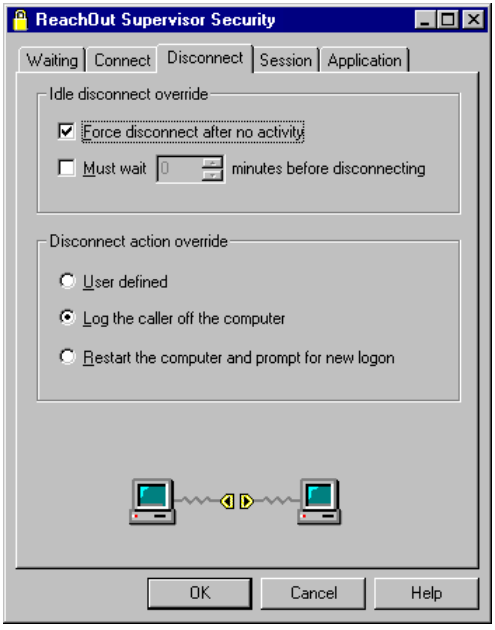
The *Confirmation override* group of fields lets you set confirmation limits; this is unchecked by default. If you require callbacks or deny caller-specified callbacks as a supervisor, users are limited to your requirements.

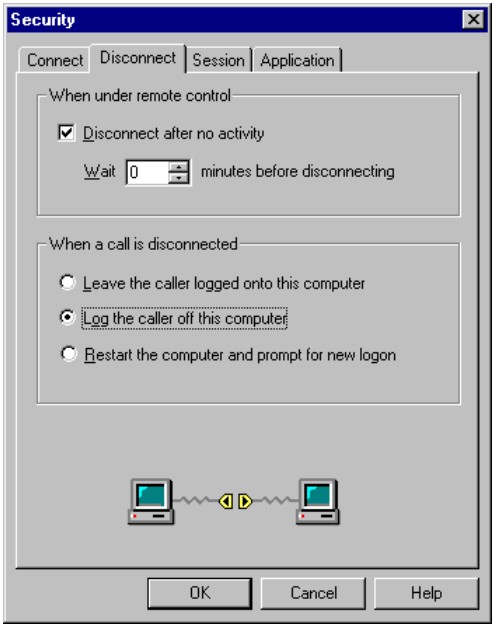


You can also constrain desktop control and IntruderGuard (lockout) conditions.

Disconnection Security

You can force a connected computer to disconnect after a time of no activity. By default, *Force disconnect after no activity* is off.

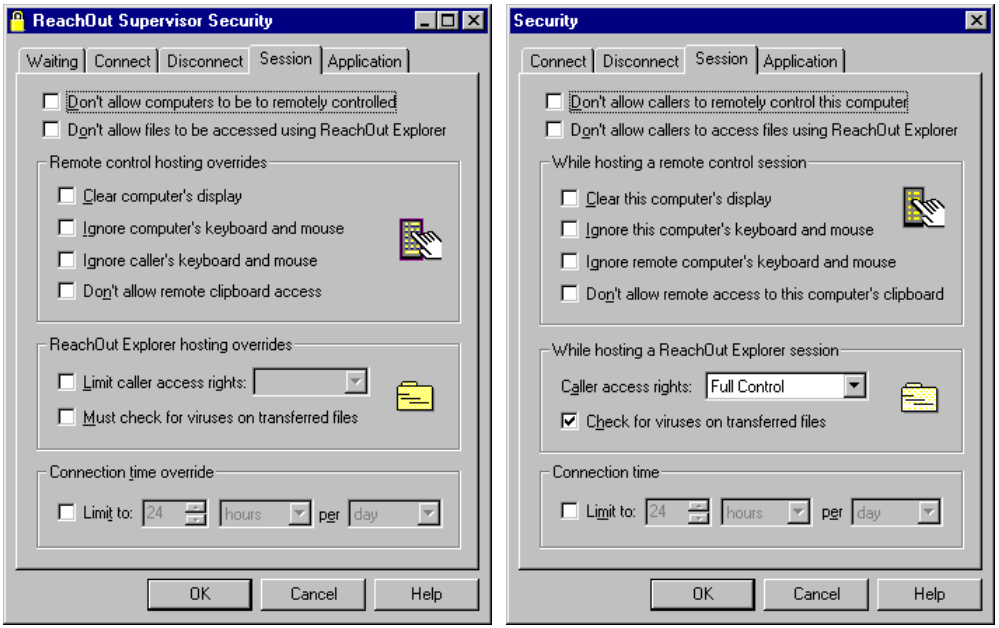




You can also specify the effect when two connected computers are disconnected. Users are constrained to the same effect.

Session Security

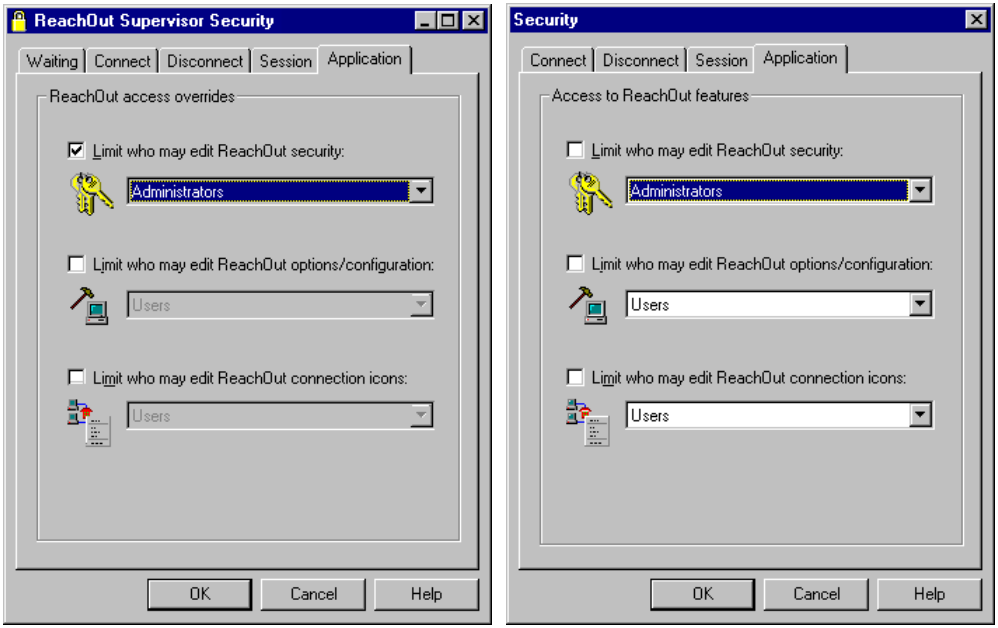
For the hosting computer, you can deny remote control and/or ReachOut Explorer access. You can also specify global file access rights, as well as limit the connection time. For remote control, you can force the computer's screen to clear, ignore input devices from either connected computer, or disable remote access to the Clipboard.



For ReachOut Explorer, you can set a global access limit.

Application Security

Members of the Windows NT “Administrators” group on any computer always have full access to ReachOut and its settings. Using application security, you can specify one additonal NT user group that may edit ReachOut security, edit ReachOut configuration, or edit ReachOut connection icons.



Chapter 5, *ReachOut Security*, has more information about creating user accounts and assigning users to Windows NT user groups.

Setting Global Internet Security

It's up to you to allow or deny access to your company's data via the Internet. If your company does not have a firewall (network security system), users can connect without your knowledge. If a computer is set up for anonymous logins, anyone can connect and have access to your company's important data.

Make sure you've taken all the necessary precautions to protect against unauthorized users as described in Chapter 5, *Security*.

8 ReachOut PASSPORT

ReachOut Passport™ lets you remotely control other computers from within your web browser. With Passport, you can connect to any computer around the world that's on the Internet and running ReachOut.

While you're browsing the Internet, click a remote control link in a web page and your browser starts ReachOut Passport to make the connection. Locally, you can also create Passport connection icons to connect to waiting ReachOut computers over the Internet or over another Windows-based TCP/IP network.

This chapter shows you how to use ReachOut Passport as well as how to set it up in your own web site to give users access to ReachOut computers.

In this chapter ...

Introduction

ReachOut Passport lets users control waiting ReachOut computers over the Internet or any other Windows-based TCP/IP network. It is easy to install and use, both for people who just click a local connection icon or a hyperlink from a web page and for webmasters who make ReachOut Passport links available to users.

ReachOut Passport always runs within a web browser. When you install or download Passport, you get the components needed to run with the type of browser that Passport finds in your system:

- A Plug-in for browsers like Netscape Navigator™ 2.0 or higher.
- An ActiveX Control for browsers like Microsoft Internet Explorer™ 3.0 or higher.

Passport reaches its greatest potential when embedded in a web page, because users are freed from their local computers. They can download Passport for the current browser from any computer on the Internet when they need to make a connection.

You can also use Passport locally, without clicking on hyperlinks. Here are some ways you might want to use Passport locally:

- To create connection files to control your own connections.
- To make connections using connection icons on your local computer.

Note: Passport supports remote control of a computer waiting on the Internet. It does not support ReachOut Explorer and it does not receive calls.

ReachOut Passport from a Web Site

Most Passport users depend on links built into a web site to provide connections to waiting ReachOut computers. Passport users can control the computer remotely as soon as the connection is made. The first time they use Passport, they can download the plug-in or let Passport handle downloading the ActiveX Control.

The company webmaster builds the hypertext pages that provide links to waiting ReachOut computers. The last part of this chapter (starting on page 109) shows webmasters how set up pages so users can connect to waiting ReachOut computers.

IMPORTANT LICENSING INFORMATION!
Each ReachOut computer to which you provide access through Passport acts as a Host computer and requires a separate licensed copy of ReachOut. Each Host computer's primary user is legally entitled to download as many copies of Passport as needed to control that computer and other ReachOut computers from anywhere in the world. Users who do not have a licensed copy of ReachOut are not entitled to download ReachOut Passport. You can contact Stac for information about a Multiple-License Agreement or Site License.

Reachout Passport Locally

Users can use ReachOut Passport in a browser locally to connect to waiting ReachOut computers, after creating Passport connection icons. These icons work much like standard ReachOut connection icons. While Passport connection icons may look like ReachOut's connection icons, they are not interchangeable.

ReachOut Passport Requirements

To install and use ReachOut Passport, you must have:

- Windows 95 or Windows NT 3.51 or later on your computer

- Access to the Internet or another Windows-based TCP/IP network
- A web browser
  - ➢ Plug-in compatible, such as Netscape Navigator 2.0 running on Windows 95 or Windows NT 3.51 or 4.0
  - ➢ ActiveX Control compatible, such as Microsoft Internet Explorer 3.0 running on Windows 95 or Windows NT 4.0

The computer you want to connect to must be:

- Running Microsoft Windows NT, Windows 95, or Windows 3.1 or higher
- On the same TCP/IP network as your computer
- Running ReachOut 5.0 or higher
- Waiting for calls

Installing ReachOut Passport

You can install ReachOut Passport in three basic ways; this section explains all three:

- Download the components you need from a web page when you need them
- Install for local use from ReachOut Setup
- Install for webmaster use from ReachOut Setup

Download from a Web Site

If your company has included Passport links on web pages, you don't have to install Passport at all. When you encounter a Passport link in a web page, just follow any instructions there. (If you already have installed or downloaded Passport, just click the link and control.) The web page should include complete instructions on what to do, as summarized below.

Passport ActiveX Control

If your browser supports ActiveX Controls, as Internet Explorer 3.0 and later browsers do, coding on the page locates the control, downloads it, installs it, and connects to the computer you chose. Depending on your browser's security settings, you may see the VeriSign certificate attesting to the safety of the downloaded files.

If Passport is not able to download the ActiveX Control and connect to the requested computer, you may have your browser security level set to reject all downloads.

To allow downloads

1. Start Internet Explorer.
2. Choose View from the Options menu.
3. On the Security tab, click the Safety Level button.
4. Click the Medium level, then choose OK.

Passport will notify you before downloading files.

Passport Plug-In

If you browser supports Netscape-compatible plug-ins, the web page probably includes instructions for downloading a compressed file (NPROP.EXE), running it to extract files, and copying the files to the appropriate folders. After you restart the browser, Passport is installed and you can click the hyperlink to connect to the waiting computer.

Note: Once you've downloaded the Passport plug-in files to your computer, you won't have to do it again.

The Passport plug-in requires that three Microsoft files (MFC40.DLL, MSVCRT.DLL, and WININET.DLL) be present in the WINDOWS/SYSTEM, WINNT/SYSTEM32, or WINNT35/SYSTEM32 folder. Microsoft supplies them with much of its software (including Internet Explorer 3.0).

If not, your web site should allow you to download the files. The file ROPMFC.EXE contains MFC40.DLL and MSVCRT.DLL; download the file, run to extract the files, and copy them to the folder. The file WINTDIST.EXE or WINT351.EXE contains WININET.DLL; running it extracts the files and places them in the appropriate directory.

Basic Passport Install

If you choose *ReachOut Passport* when setting up ReachOut, Setup installs Passport components for the browsers it detects. If you have both Netscape Navigator and Internet Explorer, for example, Setup installs components for using Passport on both browsers and stores them where the browsers can locate them.

If you didn't choose *ReachOut Passport* when you ran ReachOut Setup, you can run it again and just check *ReachOut Passport*.

Webmaster Setup Install

Webmasters need a different set of files than do Passport users. They need copies of crucial files for putting on the web site for users to download. And they need a set of sample HTML pages that demonstrate the code that makes Passport work.

Note: The webmaster version of Setup copies files but does not place them in other locations. For convenience, you may want to run Setup a second time to install Passport for local use.

To install ReachOut Passport for webmasters

1. On the *Start* menu, choose *Run*.
2. Insert the CD-ROM or disk #1 into the appropriate drive and type *d:*SETUP –W
3. Follow the instructions on the screen.

- Check only *ReachOut Passport*.
- On the Choose Setup Type screen, choose *Typical*.

Note: If you are upgrading ReachOut Passport, restart Windows before running Passport.

Using ReachOut Passport

ReachOut Passport is included with ReachOut 7.0 and runs on any Windows 95 or Windows NT 3.51 or later system. You can use it to connect to any computer running ReachOut under Windows.

Starting Passport from a Web Page

Clicking a link for a Passport connection automatically starts Passport if the appropriate control files are available. When you click the hyperlink, you'll see the Passport window in your browser as Passport establishes the connection. When you supply the access information, you'll be connected, ready to control the computer.

When you disconnect from the ReachOut computer, you'll see the Passport window again in your browser.

Starting Passport from Your Desktop

Since Passport always runs within a browser, you can't start it directly. However, Setup puts ReachOut Passport in the Start menu Programs list with entries for two Passport startup files: *Plug-In Browser* and *ActiveX Control Browser*. Choose one of these, and your default browser starts automatically.

Note: When you click one of these, Passport opens an HTM file using your default browser. Be sure to choose the appropriate startup file for your default browser.

If default browser is ...	Choose ...	To use ...
Netscape Navigator or a plug-in compatible browser	Plug-in Browser	rop_np.htm
Microsoft Internet Explorer or an ActiveX compatible browser	ActiveX Control Browser	rop_ocx.htm

Note: Instead of opening a startup file, you can open a connection file if you have any. Connection files are named with ROP extensions; each corresponds to a connection icon. They are stored in the ReachOut Passport folder. You can make a shortcut to the connection icon on your desktop for quick access.

To start Passport from a running browser

- Type any Passport startup file's full name, including path, in the browser's input field, just as you would a URL, *or*
- Drag the file into the browser's window.

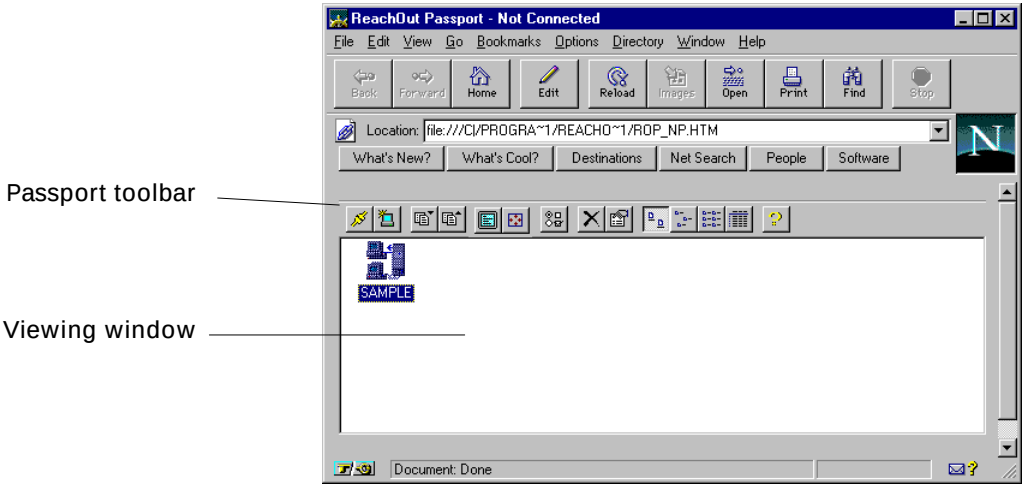
The Passport Viewer

Whenever the Passport window appears in your browser, you can use it to connect to waiting ReachOut computers. The default connection icon (SAMPLE) is not set up to connect to anything. You can create connection icons, much as you do in ReachOut. You won't get all the features of ReachOut, but you'll be able to remotely control a waiting ReachOut computer over the Internet.

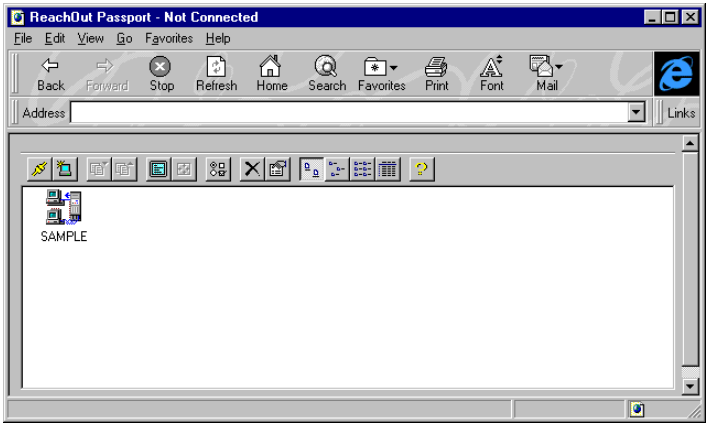
The Passport toolbar and the viewing window make up the Passport area in the browser. If you are connected to a ReachOut computer, you'll see that desktop in the viewing window. Just click the icon on the far left of the toolbar to disconnect.

When ReachOut Passport is not connected to another computer, the viewing window contains any connection icons you have created; the SAMPLE icon does not connect to anything. After you create connection icons, you can use Passport to connect to ReachOut computers that are waiting on the Internet or other TCP/IP network.

Here's how Passport looks in Netscape Navigator.



The toolbar and viewing window look the same under Internet Explorer.



Passport Toolbar

Once Passport is connected to a ReachOut computer, whether through a connection icon or through a web link, you can remotely control a computer just as you would with a computer using standard ReachOut.

Since Passport doesn't have menus, you'll use the toolbar for most actions.

To do this ...	Click ...
Connect using selected icon	
Disconnect from the connected computer	
Create a new connection icon	
Send the local clipboard to the remote one	
Get the remote clipboard into the local one	
Enlarge Passport to fill the entire screen	
Scale the remote desktop to fit in Passport	
Choose settings for ReachOut Passport printing, file storage, and DOS emulation	
Delete the selected icon	
Change or read properties of selected icon	
Display connection icons in this style	
Get help using ReachOut Passport	

Passport Connection Icons

Passport connection icons let you connect directly to a ReachOut computer waiting on the Internet. To make a connection, Passport requires three pieces of information:

- The computer's name or IP address
- A user name ReachOut expects on that computer
- A password correponding to that user name

The connection icon requires only the first; you may include user ID and password if you like.

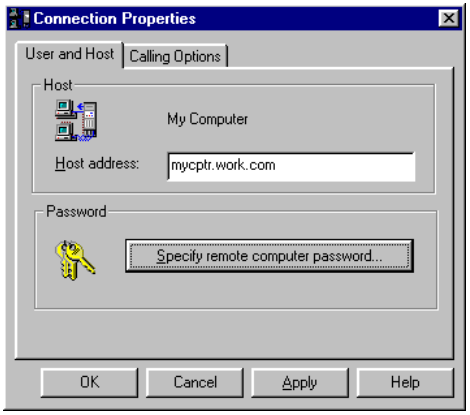
To create a connection icon

1. Click  on the Passport toolbar.

   The connection icon appears in the Passport viewing window with a default name.

2. Change the name of that icon to something meaningful, such as *My Office*.

3. Click  on the toolbar or right-click the icon and choose *Properties*.



4. In the *Host address* field, type the computer's IP address or full domain name.

   Note: Passport locates computers more quickly by IP address.

5. If you wish, click *Specify remote computer password* and type the information.

   For security reasons, you may want to leave it unspecified so that Passport will prompt users for the information.

6. If necessary, choose the *Options* tab. These are the same properties as in standard ReachOut.

When a connection icon appears in ReachOut Passport, you can use it to connect to the specified computer if ReachOut is waiting for calls.

To connect to a waiting computer

1. Select a connection icon.
2. Click  on the Passport toolbar.

Or connect in one step by double-clicking the connection icon.

For detailed information about how ReachOut Passport works, see its online Help.

How ReachOut and Passport Differ

In a few cases, you use ReachOut Passport differently from standard ReachOut. In ReachOut Passport:

- Only remote control connections to computers waiting over the Internet or another Windows-based TCP/IP network are valid.
- No ReachOut files are needed. Passport stores its connection files in its own installation folder.

- Any local connection icons are available when Passport is open but you aren't connected.
- Connection files use extension ROP, not RCO. They are specific to Passport. ReachOut and Passport do not share connection files.
- You use the toolbar icons rather than commands to:

  - Scale remote display to fit entirely within the Passport window (Scale Display button)
  - Set printer options (Options button)
  - Transfer data between the computers (Get/Send Clipboard buttons)
- Panning is not available.
- There is no hot key to cycle the remote computer's running applications.
- Passport can't receive calls, use ReachOut Explorer, or Chat.
- Passport can't force a connected computer to restart on disconnect.

Putting Passport on the Web

Note: The remainder of this chapter contains information for webmasters to use when putting ReachOut Passport on their web sites.

ReachOut Passport lets users control a waiting ReachOut computer over the Internet. Passport contains two products in one: an ActiveX Control and a browser plug-in. The ActiveX Control works automatically to get any needed files and connect to a computer. The plug-in requires that the needed files be available on the user's computer in order to make the connection. As webmaster, it is up to you to put the files in appropriate locations and include HTML code that references them.

IMPORTANT! Before putting Passport in a web site, install it using SETUP –W to make sure you have the files you need.

Required Files

Setup puts Passport files in the folder you specify, and also creates a subfolder named Sample Website. It contains sample HTML pages that you can use as a guide in putting ReachOut Passport on your own site.

Note: Change to the Sample Website folder and double-click START.HTM to look at the sample pages locally. The links and download paths are incomplete, but you'll be able to see how the pages fit together and how they are coded.

Passport also requires that users have several Microsoft files in WINDOWS\SYSTEM, WINNT\SYSTEM32, or WINNT35\SYSTEM32; they are installed with Internet Explorer and many other Microsoft products. You can also download them from *http://www.stac.com/rop*.

- To get MFC40.DLL and MSVCRT40.DLL, users can download ROPMFC.EXE, run ROPMFC.EXE to extract the files, then copy both to the appropriate SYSTEM folder.
- To get WININET.DLL, users run WINTDIST.EXE or WINT351.EXE to extract the files and puts them in the appropriate location.

You can have users download the files from your web site or directly from Stac's web site.

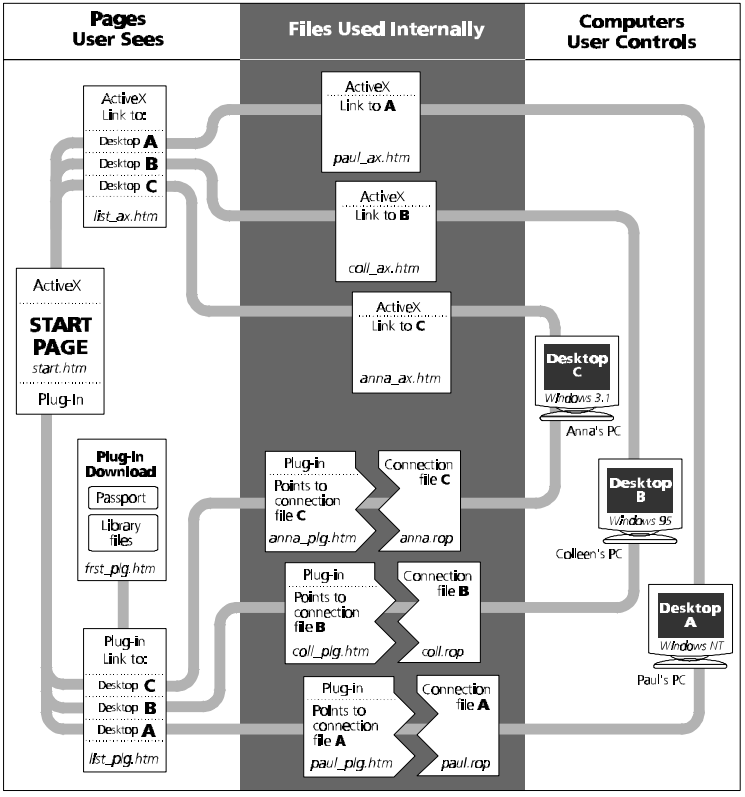
Sample Website Structure

The diagram on the next page shows the structure of the sample web site. It includes the names of HTM files from the sample, and shows the types of files you have to create to let Passport connect to three computers. You can easily modify this plan to fit your needs.

The left side shows the pages the user may see when browsing the site. Clicking on a link in LIST_AX.HTM or LIST_PLG.HTM connects the user to one of the computers shown on the right side of the page. The files in the middle of the diagram are required to make Passport work.

- The starting page (START.HTM) offers a choice between an ActiveX control and plug-in compatible browser. You might want to use HTTPS or another secure method to prevent unauthorized users from going beyond this page.

  The user must know what kind of browser will be used. Once that choice is made, the user sees a list of remote computers.



- A similar list appears for each type of browser (LIST_AX.HTM or LIST_PLG.HTM). The user makes a choice, responds to login prompts, and is connected to the ReachOut computer shown in the right column. If your site has just one or two computers to control, you might want to combine the starting page and the lists.

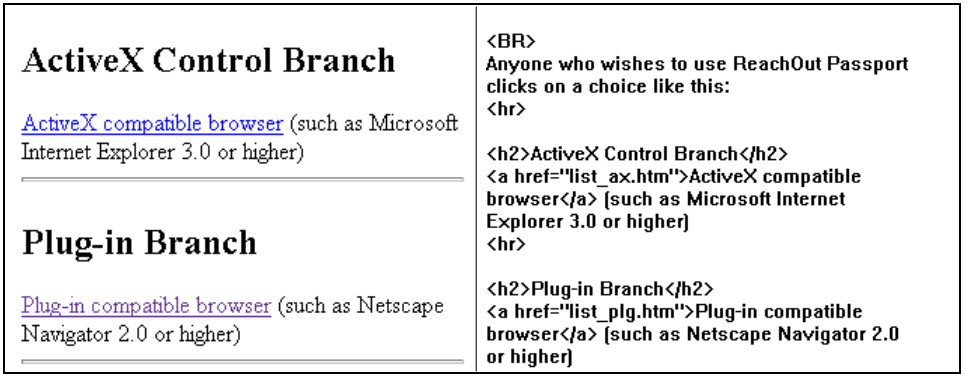
The middle section of the diagram shows pages and files that the user never sees. Passport uses these behind the scenes to establish the connection to the computers shown on the right of the diagram.

- The user never sees the pages with the coding that sets up the links. For ActiveX controls, the page contains an OBJECT tag with PARAM attributes that identify the control and establish the connection. For plug-in links, the page contains an EMBED tag naming a connection file that establishes the parameters for the connection.

Sample ReachOut Passport Pages

This section demonstrates the essential coding in the sample web site pages included with Passport. Your Sample Website subfolder contains files that you can modify or use as a guide in putting Passport on your company's web site. The connection information and download targets in the pages are incomplete. You will have to customize this information.

The first Passport page asks the user what type of links are desired. The Plug-in method works with both Netscape and Internet Explorer. Notice that each choice links to a standard HTML page.



ActiveX Control Coding

The following illustrates the page that appears if the user chooses the ActiveX branch. You can see how it looks on screen and how it is coded with simple HTML tags. Notice that we used a table to allow for evenly aligned graphics. You can use any type of list if you prefer.

When the user clicks a link, such as **Colleen McDonald**, the next page (COLL_AX.HTM) downloads the ActiveX control if necessary, gets any Microsoft files if necessary, runs the ActiveX control, and presents the desktop for remote control. The user will have to enter a password.

Choose a remote computer.

Colleen McDonald

Paul Jefferson

Anna Lenore Smith

```
<TABLE BORDER=0>
<TR>
<TD ALIGN=CENTER> <img border=0
hspace=10 src="face23.gif">
<TD ALIGN=LEFT> <A HREF="coll_ax.htm">
<B>Colleen McDonald</B></A>
<TR>
<TD ALIGN=CENTER> <img border=0
hspace=10 src="exec13.gif">
<TD ALIGN=LEFT> <A
HREF="paul_ax.htm"><B> Paul
Jefferson</B></A>
<TR>
```

The ActiveX control coding is similar for all three computer connections. The only required difference is the *HostAddress* value.

```
<BODY>
<object
        classid="clsid:a1d23d83-b31c-11cf-9246-0000e202bb2b"
        type="application/x-oleobject"
        codebase="http:ropx.cab#Version=7,0,0,0"
        id=ropctl
        align=center
        width = 100%
        height = 90%
>
<param name="HostAddress" value="nnn.nnn.nnn.nn">
<param name="UserName" value="">
<param name="Password" value="">
<param name="EnableCache" value=0>
<param name="SaveCache" value=0>
<param name="EnableCompression" value=0>
<param name="DisableInput" value=0>
<param name="DontTransmitInput" value=0>
<param name="ScaleDisplay" value=0>
<param name="ClearDisplay" value=0>
</object>
```

Use a separate HTML file for each connection in your list, with different connection information in the parameters. You'll want to copy the tag from one of the supplied files to make sure it is entered correctly. Use the version information supplied.

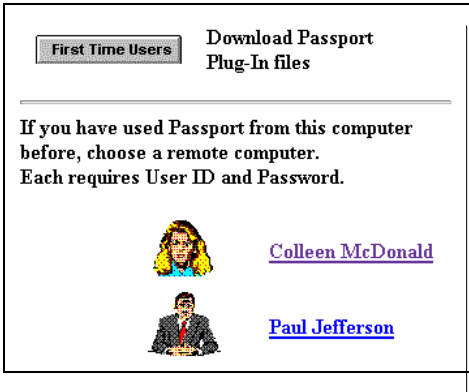
Within the OBJECT tag itself, you'll have to supply the CODEBASE path and version number information. The original version number for the ActiveX Control is 7,0,0,0. You'll have to modify the value if you upgrade to a later version. The OBJECT tag with its attributes is identical for all your connection pages. For each connection, you'll have different information for the first PARAM tag. You must supply the full domain name or IP address of the desired connection; you may supply the UserName and Password, but most people prefer to omit the access information for added security. The last seven parameters can each have a value of 1 (ON) or 0 (OFF). The example shows them in ReachOut's default state.

The OBJECT tag syntax for using Passport is shown in the *Reference Section* at the end of this chapter.

IMPORTANT! The required Microsoft Foundation Class libraries and WININET.DLL are installed in WINDOWS\SYSTEM or WINNT\SYSTEM32 with Microsoft Internet Explorer. If a user is missing WININET.DLL, MFC40.DLL or MSVCRT40.DLL, the control accesses the files automatically from the Stac web site.

Plug-in Use Coding

If the user chooses the plug-in branch, the next page offers a choice using the Passport plug-in. You can see how it looks on screen and how it is coded. Notice that we used a table to allow for evenly aligned graphics. You can use any type of list if you prefer. Except for the names of the linked files, the lists are identical for ActiveX control and plug-in browsers. (The *First Time Users* button is explained on page 116.)




```
<TD><A HREF="first_plg.htm"><img border=0
src="1time.gif"></a></td>
<TD><b>Download Passport Plug-In files</b></td>
</TABLE>
<hr>
<b>If you have used Passport from this computer before, choose a
remote computer.<br>Each requires User ID and Password.</b>
<blockquote><blockquote>
<TABLE BORDER=0>
<TR>
<TD ALIGN=CENTER> <img border=0 hspace=10 src="face23.gif">
<TD ALIGN=LEFT> <A HREF="coll_plg.htm"> <B>Colleen
McDonald</B></A>
<TR>
<TD ALIGN=CENTER> <img border=0 hspace=10
src="exec13.gif">
<TD ALIGN=LEFT> <A HREF="paul_plg.htm"><B> Paul
```

When all the files are in place, clicking a hyperlink causes Passport to connect to the specified ReachOut computer. The linked page uses the plug-in to get the connection file (ROP) that accesses the waiting ReachOut computer. The user will probably have to enter a password. Below is the code for the linked page and the connection file.

Plug-In Connection HTML Page	ROP Connection File
<BODY> <EMBED SRC="colleen.rop" TYPE=application/x-rop WIDTH=800 HEIGHT=600> </BODY>	[Connection] HostAddress=nnn.nnn.nnn.nn UserName= Password= EnableCache=1 SaveCache=1 EnableCompression=1 DisableInput=0 DontTransmitInput=0 ScaleDisplay=0 ClearDisplay=0

The plug-in connection page can rely on the EMBED tag, as shown in the example, or it can reference the connection file directly in the HREF attribute of the A tag. The EMBED tag tells the browser where to find the connection file and what plug-in to use in processing it. You'll have to insert the appropriate connection file name for each connection.

You can create connection files using any text editor. Passport creates them automatically when you create connection icons using your local copy of Passport.

- When you create a connection icon in Passport, the name you assign to the icon becomes the filename, with the extension ROP.
- If you create the file by hand, be sure to use all ten fields. To let Passport prompt for the user ID and password, leave the *UserName=* and *Password=* fields blank.

Put the ROP file in the folder that contains your HTM files. Syntax for the EMBED tag and connection file are included in the *Reference Section* at the end of the chapter.

First time Passport Plug-In Users

To use Passport with a browser that doesn't support ActiveX Controls, your users will have to download the files they need and move them to the appropriate folders. The sample web site uses a First Time Users button to link to a page (FRST_PLG.HTM) that tells users what to do and makes the process easy for them.

Here are some things to keep in mind:

- Tell users how to decide what they need, and provide text or a button to click for downloading.

- ROPNP.EXE contains the plug-in and help files. Setup installed it in your Passport folder. You should put it on your own web site. After downloading and extracting, users must copy ROPNP.DLL to the plugins folder and the HLP and CNT files to WINDOWS\HELP or WINNT\HELP.

- ROPMFC.EXE contains Microsoft Foundation Class libraries Passport depends on. Microsoft installs them with Internet Explorer and other products, so they are not included in ROPNP.EXE. Your users need these if WINDOWS\SYSTEM or WINNT\SYSTEM32 does not contain MFC40.DLL and MSVCRT40.DLL. You can point directly to *http://ftp.stac.com/rop/ropmfc.exe*, or you can manually download the file from the ReachOut Passport Web page and put a copy on your web site.

- WINTDIST.EXE (for Windows 95 and Windows NT 4.0) and WINT351.EXE both contain the Microsoft file WININET.DLL, which the plug-in depends on. Microsoft installs it automatically with Internet Explorer and many other products, so it is not included in the ROPNP.EXE download. Your users will need it if WINDOWS\SYSTEM, WINNT35\SYSTEM32, or WINNT\SYSTEM32 does not contain WININET.DLL. Installing Passport puts these files in the ReachOut Passport Webmaster folder. You can manually download the files from the ReachOut Passport Web page, or point directly to them at *http://ftp.stac.com/rop*.

Your web page will have to

- Make sure any files users may have to download are available.
- Tell users how to run the downloaded files and where to move the resulting files.

Reference Section

This section summarizes the components you need in placing ReachOut Passport on a web site.

Stac maintains a web page where you can download the latest version of crucial ReachOut Passport files. Connect to *www.stac.com/rop* at any time and download the files you need or reference them directly from your web pages.

Feature	ActiveX	Plug-in
Coding tag	<OBJECT>	<EMBED>
Connection info	<PARAM> tags	ROP connection file
Download files	Automatic, if needed	User clicks button
Storage of files	Automatic	User moves files

ActiveX Controls

The OBJECT tag specifies the information needed to locate the ActiveX control (ROP.OCX), determine if a new one is needed, download ROPX.CAB if needed, get any Microsoft files needed, and run the control.

The items in ***bold italics*** indicate what you have to customize.

See ANNA_AX.HTM

```
<OBJECT
 CLASSID="clsid:a1d23d83-b31c-11cf-9246-
0000e202bb2b"
 TYPE="application/x-oleobject"
 CODEBASE="http:[path]ropx.cab#Version=7,0,0,0"
 ID=ropctl
 ALIGN=CENTER
 WIDTH=100%
 HEIGHT=90%
>
<PARAM NAME="HostAddress" VALUE="name or IP">
<PARAM NAME="UserName" VALUE="userID">
<PARAM NAME="Password" VALUE="password">
<PARAM NAME="EnableCache" VALUE=1>
<PARAM NAME="SaveCache" VALUE=1>
<PARAM NAME="EnableCompression" VALUE=1>
<PARAM NAME="DisableInput VALUE=0>
<PARAM NAME="DontTransmitInput" VALUE=0>
<PARAM NAME="ScaleDisplay" VALUE=0>
<PARAM NAME="ClearDisplay" VALUE=0>
</OBJECT>
```

If you have an updated ROPX.CAB, change the CODEBASE attribute to specify an updated version number. The registry entry for ROP.OCX includes version information and a later one signals the system to download and use the new ActiveX Control.

You can change any of the PARAM values.

- The *HostAddress* must be the full domain name or permanent IP address of the ReachOut computer.
- The *UserName* and *Password* provide access information. Leaving their *VALUE*s blank forces the user to enter access information.
- The last seven values can be 0 (OFF) or 1 (ON).

Security

ROPX.CAB is certified by VeriSign, Inc., for your protection and that of your users. If a new version of Passport's ActiveX Control (ROPX.CAB) is downloaded, a certificate may appear, depending on the user's security settings.

You may want to add additional security to your web site to protect the connections you have established from wandering eyes. You can use HTTPS or some other system that requires password access to pages that contain Passport links.

Plug-in Requirements

The EMBED tag names the plug-in and indicates where the connection file is. The items in ***bold italics*** are the ones you have to customize.

See ANNA_PLG.HTM

```
<EMBED
  SRC="[path/]filename.ROP"
  TYPE=application/x-rop
  WIDTH=800
  HEIGHT=600>
```

Note: The WIDTH and HEIGHT attributes are required. This example shows typical values.

The connection file is ASCII text. Creating a Passport connection icon creates a connection file for you, or you can create these files manually. To force users to enter access information, leave the *UserName* and *Password* field values blank. The last seven fields can be 0 (OFF) or 1 (ON). The example shows ReachOut's default settings.

See ANNA.ROP

```
[connection]
HostAddress=full domain name or IP address
UserName=UserID
Password=password
EnableCache=1
SaveCache=1
EnableCompression=1
DisableInput=0
DontTransmitInput=0
ScaleDisplay=0
ClearDisplay=0
```

If you prefer, you can use a tag like <A HREF="passport/anna.rop"> instead of EMBED to reference the connection file directly

Microsoft Files

MFC40.DLL, MSVCRT.DLL, and WININET.DLL must be present in WINDOWS\SYSTEM, WINNT\SYSTEM32, or WINNT35\SYSTEM32 on the local computer.

If necessary, you and/or the user can download ROPMFC.EXE from *http://www.stac.com/rop*. Run ROPMFC to extract MFC40.DLL and MSVCRT.DLL, then copy them to the appropriate SYSTEM folder.

Obtain WININET.DLL by extracting either WINTDIST.EXE or WINT351.EXE. These files can be downloaded from Stac's web site or you can get them from the ReachOut Passport Webmaster folder. Run the appropriate file to install WININET.DLL and store it correctly.

Tips to Make Passport Work Well on Your Site

- Allow for both ActiveX and plug-in compatible browsers.
- For both ActiveX and plug-in compatible branches, use a separate HTML page for each computer connection link. The user doesn't see these pages, but the system needs them.
- Tell users what to do or what happens the first time a computer uses Passport, and make sure all needed files are available.
- Make sure the linked-to computers really have ReachOut running and are waiting on the Internet; Passport can't connect if they aren't.

In Summary

Feel free to use our sample pages and graphics as you wish in preparing your web site to use Passport.

E

F

G

H

S

T