



# **IP Office 4.2**

## **IP Office Remote Access**

#### Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

#### Documentation Disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

#### Link Disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

#### License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s): Designated System(s) License (DS).

End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

#### Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

#### Third-Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at: <http://support.avaya.com/ThirdPartyLicense/>

#### Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com). For additional support telephone numbers, see the Avaya Support web site (<http://www.avaya.com/support>).

#### Trademarks

Avaya and the Avaya logo are registered trademarks of Avaya Inc. in the United States of America and other jurisdictions. Unless otherwise provided in this document, marks identified by "®," "TM" and "SM" are registered marks, trademarks and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

#### Documentation information

For the most current versions of documentation, go to the Avaya Support web site (<http://www.avaya.com/support>) or the IP Office Knowledge Base (<http://marketingtools.avaya.com/knowledgebase/>).

#### Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1 800 628 2888 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>.

# Contents

## 1. Introduction

1.1 Purpose .....	7
1.2 Scope .....	8
1.3 Preferred Solution.....	9

## 2. Making A Remote Connection

2.1 IP Office Remote Access Server (RAS).....	12
2.1.1 IP Office ISDN Remote Access Example .....	13
2.1.2 IP Office Analog Remote Access Example.....	14
2.1.3 Static NAT Options in IP Office Firewalls (IP Office 4.2+).....	15
2.1.4 Dial Up Modem Connectivity.....	16
2.1.5 Internet Connectivity .....	17
2.1.6 Virtual Private Network (VPN) Connectivity.....	18

## 3. IP Office Remote Manager

3.1 Setting Up the Dial Up Connection.....	22
3.2 Connection Settings.....	26
3.3 Additional Configuration.....	28

## 4. Preparing For Installation

4.1 Symantec pcAnywhere System Requirements.....	30
4.2 User Rights Requirements.....	30
4.3 Installation Options .....	31
4.4 The Difference Between A Host And A Remote.....	31

## 5. Symantec pcAnywhere Installation

5.1 Installing The Full Product Version.....	34
5.2 Installing A Custom Version.....	37

## 6. Symantec pcAnywhere Configuration

6.1 Starting Symantec pcAnywhere.....	40
6.2 Setting Up The Host.....	40
6.3 Configuring Advanced Host Properties.....	45
6.3.1 Connection Info.....	45
6.3.2 Callers.....	46
6.3.3 Security Options.....	48
6.3.4 Encryption.....	49
6.3.5 Conference.....	50
6.3.6 Comments.....	51
6.3.7 Settings.....	51
6.3.8 Protect Item.....	52
6.4 Changing The Default Port Numbers On The Host.....	53
6.5 Configuring Advanced Remote Properties .....	58
6.5.1 Connection Info.....	60
6.5.2 Settings.....	61
6.5.3 Remote Control.....	61
6.5.4 Encryption.....	63
6.5.5 Comments.....	63
6.5.6 Protect Item.....	64
6.6 Changing The Default Port Numbers On The Remote .....	64

## 7. Remote Capabilities

## 8. Alternative Remote Access Solutions

8.1 BeAnywhere.....	72
---------------------	----

8.2 eBLVD .....	72
8.3 GoToMyPc Corporate .....	73
8.4 Laplink Everywhere.....	73
8.5 LogMeIn Pro.....	74
8.6 Microsoft Remote Desktop Connection.....	74
8.7 PROXY/Enterprise.....	75
8.8 Radmin .....	76
8.9 Remote Desktop Control.....	76
8.10 RemotePC.....	77
8.11 VNC Personal Edition .....	77
8.12 WebEx PCNow .....	78

## 9. Summary

Index .....	0
-------------	---



# **Chapter 1.**

# **Introduction**



# 1. Introduction

Avaya's customers and Business Partners are requesting remote access standards for controlling and managing IP Office. Currently there are several methods being employed by business partners and field technicians at the time of installs to increase ease of ongoing maintenance and troubleshooting, should the need arise.

The purpose of this document is to look at a remote access solution for IP Office that will allow management of both the IP Office system and any application servers that reside on the customers' network. Having a consistent proven remote access solution will allow Avaya to be able to setup, document and test the solution and certify its operation release over release.

Avaya has chosen pcAnywhere from Symantec as the preferred solution for remote access and remote control for IP Office. This document will explore the installation and configuration of pcAnywhere to work with IP Office and will also look at some alternative remote access solutions that are available.

For the purposes of this document IP Office release 4.2 and Symantec pcAnywhere 12.1 have been used, although most of the fundamentals apply to all versions.

## 1.1 Purpose

The problem that faces IP Office support and provisioning teams today is that not all IP Office solutions include dedicated line/modem access into the customer control unit, and even if it is provided rarer still is direct access available to the often included application server that hosts the many IP Office applications (such as Voicemail Pro, Compact Contact Center, Conferencing Center, ContactStore, etc.) The fact remains that modem based connectivity has limiting factors in that it does not usually completely or adequately cover the entire deployed IP Office solution when IP Office applications are involved.

From a support perspective having a defined and tested remote access solution is highly desirable. This enables Avaya to create a configuration that can be tested over and over with each new release of IP Office software to fully prove that known functionality has not been compromised. It is also beneficial to customers of Avaya, be it end users, field technicians, support engineers, Business Partners or Distributors, to have a standard setup that is fully tested and documented.

The purpose for the Remote Access Solutions Best Practices Guide is to ensure that field technicians, support engineers and Business Partners have reliable access to IP Office systems. Reliable access is critical for support personnel when gathering data during troubleshooting reported issues. Once best practices have been published Avaya can ensure the highest level of technical support and turnaround time to resolve field issues reported by our customers. This document aims to standardize the implementation and maintenance methods that are currently being used with success by Business Partners and remote field technicians.

---

## 1.2 Scope

This Best Practices Guide provides detailed instructions on how to implement and utilize Symantec pcAnywhere and also offers an overview of the following remote access methods:

- [BeAnywhere](#) <sup>[72]</sup>
- [eBLVD](#) <sup>[72]</sup>
- [GoToMyPc](#) <sup>[73]</sup>
- [Laplink Everywhere](#) <sup>[73]</sup>
- [LogMeIn](#) <sup>[74]</sup>
- [Microsoft Remote Desktop](#) <sup>[74]</sup>
- [Proxy Networks](#) <sup>[75]</sup>
- [Radmin](#) <sup>[76]</sup>
- [Remote Desktop Control](#) <sup>[76]</sup>
- [Remote PC](#) <sup>[77]</sup>
- [VNC](#) <sup>[77]</sup>
- [Webex PCNow](#) <sup>[78]</sup>

The methods of remote access covered in this Best Practices Guide were chosen because they meet the following list of criteria that are necessary to for reliable troubleshooting or controlling of an IP Office System remotely.

- Secure access
- Allows access through corporate firewalls (proxies through corporate websites)
- Allows access to alarming notification (and the ability to accumulate historical alarm data)
- Reliable and efficient (keeps a secure connection and is capable of file transfer)
- Allows traceability
- Allows callout capability
- Is backward compatible



## 1.3 Preferred Solution

In order to have a defined and tested solution for remote access and remote control of the IP Office system and associated server applications Avaya has chosen to adopt pcAnywhere from Symantec.

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information.

As an industry leader in providing platform-agnostic software solutions, Symantec is critically dependent on highly functional, open, and interoperable industry standards. Symantec has founded and now leads many industry standards efforts, and most Symantec products are based on standards.

Symantec pcAnywhere software has continued to build on its reputation by offering best in class features and strong security while maintaining ease of use. The customer will easily recognize the software brand and since pcAnywhere has been one of the leading remote access solutions most support groups and customers alike will be familiar with it, minimizing the learning curve needed to operate the software.

Symantec pcAnywhere version 12.1 provides a feature-rich, secure, and reliable remote control solution to accelerate resolution of helpdesk calls. You can use your desktop computer, laptop, or mobile device to work across multiple platforms. Easy-to-use and streamlined connectivity with greater platform support allows comprehensive control of IP Office and the associated applications:

- Offers heterogeneous host and remote platform support across Windows (including Vista), Linux, and Mac OS X; all hosts can also be accessed from Microsoft Pocket PC devices or Web browsers.
- Powerful capabilities allow users to upload and download files across different platforms while in session.
- Shared session shadowing capabilities allowing local and remote teams to see the same session and collaborate.
- Gateway option enables real-time discovery of and connection to multiple devices behind firewalls and NAT devices, that mitigates private and dynamic IP challenges, and minimizes port opening and forwarding.
- Host invitation feature simplifies the process of hosts establishing a reverse connection from behind firewalls and NAT devices.
- User interface provides simple, graphical, task-based options.
- The Symantec pcAnywhere Access Server option facilitates the discovery of and connection to multiple pcAnywhere hosts from anywhere, regardless of location or network configuration. (Sold separately; works in conjunction with pcAnywhere 12.x.)
- AES encryption algorithm gives users a choice of all available cipher strengths (128-bit, 192-bit, and 256-bit) in addition to the currently offered RC4 symmetric algorithm and other options (pcAnywhere encoding, public key, or none). pcAnywhere encryption is FIPS 140-2 validated.
- Supports multiple authentication methods, enabling customers to use existing network authentication user names and passwords with pcAnywhere.
- Symantec pcAnywhere Mobile™ permits a connection to and remote control of a standard pcAnywhere host from a current market-standard Microsoft Pocket PC device over any TCP/IP connection, including wireless (cellular, Bluetooth, and WiFi).
- Bandwidth auto-detect allows users to optionally detect the actual connection speed (bandwidth) of each connection, and adjust settings that affect performance during lower-bandwidth connections.
- Deploy a limited-functionality, single-use host to computers that do not have a host running.



# **Chapter 2.**

## **Making A Remote Connection**

---

## 2. Making A Remote Connection

Before any remote access software can be used to take control of a remote PC you need to make a data connection to the customer site, this could be a dial up RAS, VPN or Internet connection.

A connection needs to be established between the PC running the remote software (this is the PC that is used to take control) to the PC acting as a host (this is the PC that will be controlled). Once a connection is established then the remote access software can be used to take control.

### 2.1 IP Office Remote Access Server (RAS)

IP Office provides built in RAS functionality allowing external users to dial in to the local area network from modems, terminal adapters and routers. Dial in users can be authenticated by using CHAP (encrypted passwords) or PAP (which does not support encryption). To further enhance security a specified location can be set which restricts remote access from only that location or a designated callback number can be used, thereby minimizing the threat of unauthorized remote access. IP Office's integral firewall, service quotas and time profiles can all be applied to remote access calls.

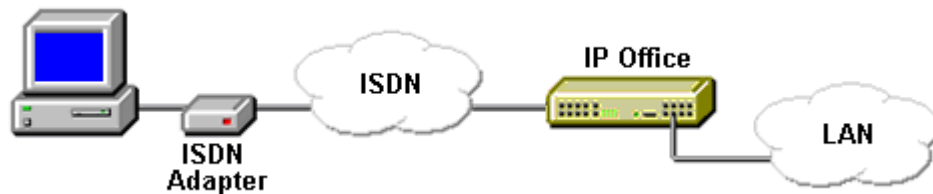
Dependant on the type of trunk connection on the IP Office system either an ISDN adapter (modem) or an analog modem can be used to make the connection. The first analog trunk port on Small Office Edition control units, IP400 ATM4 trunk cards and IP500 analog trunk cards can be set to modem operation (V.32 with V.42 error correction). This allows the trunk to answer incoming modem calls and be used for system maintenance.

When modem operation is enabled the trunk can only be used for analog modem calls. The default system short code \*9000\* can be used to toggle this setting. For the Small Office Edition control unit, when on, the control unit status LED flashes alternate red/green. When the remote access session is finished the \*9000\* short code must be dialed again to set the port back to normal operation.

The analog modem is sufficient if you are only running a remote IP Office Manager session across the connection however the bandwidth is not sufficient for a pcAnywhere session to be used. The V.32 modem supports a data connection speed of 9600 bits per second, the minimum recommended data rate for pcAnywhere is 19,200.

A plug in modem daughter card with 12 V.90 modems can be installed in the IP406v2 and IP412 but is not supported in the IP500. An alternative solution for analog access would be to install a modem onto the PC which has the pcAnywhere software installed, this would also need to have a suitable analog line for operation.

## 2.1.1 IP Office ISDN Remote Access Example



### 1. Create a User

A user called RemoteManager is available by default in the IP Office configuration. This default user can be used for remote access or another user created if necessary. If using this default user it is advisable to change the default password that is set.

For a new user the required details are:

- In the User tab - Enter a Name and Password. IP Office is case sensitive. Remember to take care with passwords as this is a remote access link into your network.
- In the Dial In tab - Ensure that Dial In On is ticked. The Firewall Profile and Time Profile are optional.

### 2. Create a RAS Entry

- A RAS entry called DialIn is available by default in the IP Office configuration.
- For a new RAS entry the required details are:
  - In the RAS tab - Enter the same name as the user that you created earlier. Again, remember this is case sensitive.

### 3. Create an Incoming Call Route

- An incoming call route for dial-in access (labeled DialIn) is available by default in the IP Office configuration. Additional configuration (Bearer Capability setting) is available if necessary.
- For a new Incoming Call Route entry the required details are:
  - Set the Bearer Capability to Any Data.
  - In the Destination drop-down list, select the RAS entry created above.
  - The values that you enter for any of the other fields will depend on whether the remote user will be calling in on a particular line, number or from a set ICLID.

### 4. Is a Return IP Route Needed?

- Go to Step 5.

### 5. Create an IP Route (Optional)

- If the remote user has an IP address that is not in the same domain as the IP Office, then an IP Route is needed for return data. This is not necessary if the remote user's dial-up connection method is set to 'Obtain an IP Address Automatically' and the IP Office's DHCP mode is set to Server or Dial In. If using the default RemoteManager user an IP route already exists in the IP Office configuration.
- Enter the IP Address and IP Mask of the remote system.
- In the Destination drop-down list select the RAS entry created above.
- Note: *Symantec pcAnywhere ISDN connectivity is only supported in North America and Europe.*

---

## 2.1.2 IP Office Analog Remote Access Example



Configuration for a connection from an analog modem is very similar to the ISDN example. However the IP Office must be able to answer modem calls. This can be done in the following ways;

### Modem Cards

For the IP406v2 and IP412 a modem card can be installed. This card allows the IP Office system to answer V.90 analog modem calls. The Internal Modem Card allows the IP Office system to support 12 simultaneous modem calls.

### Analog Trunk Modem

On systems with an ATM4 trunk card and on the Small Office edition, the first analog trunk can be set to answer V.32 modem calls. This is done by checking the Modem Enabled option on the analog line settings or using the default short code \*9000\* to toggle this service on or off

When using an analog modem, the Bearer Capability of the incoming call route used should be Any Voice. If using Any Voice ensure that you don't have another 'Blank' incoming entry with a different destination in the Incoming Call Routes.

It is recommended to use a specific DDI/DID number with the bearer set to Any. This is so all types of remote access can be used. This requires a spare DDI/DID number.

### 2.1.3 Static NAT Options in IP Office Firewalls (IP Office 4.2+)

The Static NAT table allows the firewall to perform address translation between selected internal and external IP addresses. Up to 64 internal and external IP address pairs can be added to the Static NAT section of a Firewall Profile. When static NAT entries are added to a Firewall Profile, only traffic that matches one of the static NAT entries (plus all the other firewall settings) is allowed.

This feature is intended for incoming remote access using applications such as pcAnywhere, IP Office Manager and the Voicemail Pro Client. The address translation is used for destinations such as an IP Office Voicemail Pro server or the IP Office's own LAN1 address.

If there are any entries in the Static NAT settings of a Firewall Profile, each packet attempting to pass through the firewall must match one of the static NAT pairs or else the packet will be dropped.

In this example Firewall profile two static NAT pairs have been setup. The internal IP address 192.168.42.11 is the IP Office LAN1 address and 192.168.42.123 is the Voicemail Pro server.

The screenshot shows the 'Firewall Profile' configuration window with the 'Dial\_Up' profile selected. The 'Static NAT' tab is active, displaying a table with two entries:

	Internal IP Address	External IP Address
▶	192 . 168 . 42 . 11	10 . 0 . 0 . 11
	192 . 168 . 42 . 123	10 . 0 . 0 . 123
*		

The destination address of incoming packets is checked for a matching External IP Address. If a match is found, the target destination address is changed to the corresponding Internal IP Address. The source address of outgoing packets is checked for a matching Internal IP Address. If a match is found, the source address is changed to the corresponding External IP Address. Using this example above the IP Office would appear to have the IP address 10.0.0.11 and not its actual IP address of 192.168.42.11.

The screenshot shows the 'Select IP Office' window. The 'Release 4.2' section is expanded, showing a list of IP Office instances:

Name	IP Addr...	Type	Version
<b>Release 4.2</b>			
<input type="checkbox"/> 406v2	10.0.0.11	IP 406 DS	4.2 (5)

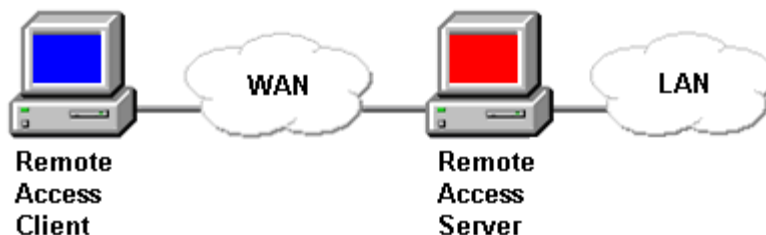
Below the list, there is a 'TCP Discovery Progress' bar and a 'Unit/Broadcast Address' dropdown menu set to '255.255.255.255'. There are 'Refresh', 'OK', and 'Cancel' buttons at the bottom.

Note: Even when a static NAT address match occurs, the other settings on the Firewall Profile Standard and Custom tabs are still applied and may block the packet.

## 2.1.4 Dial Up Modem Connectivity

If it is not possible to take advantage of the built in RAS features of the IP Office then an analog or ISDN modem (terminal adapter) can be connected to the PC that you want to access and manage remotely. The modem could be connected to a port on the IP Office system or it could be connected to its own dedicated line.

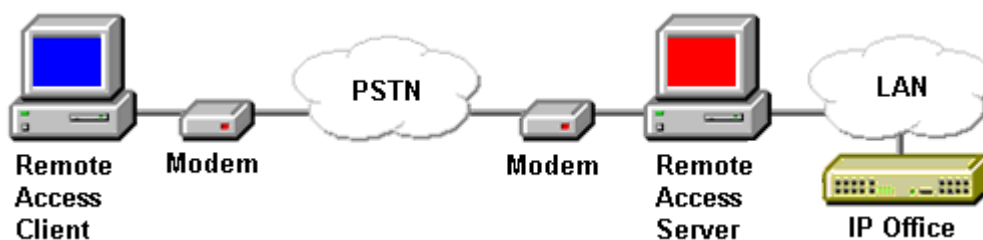
A dial-up remote access connection consists of a remote access client, a remote access server and a wide area network (WAN) infrastructure as shown below.



### PSTN Connection

The PSTN is the most common network used for dial-up remote access. The equipment needed consists of an analog modem at the remote access client and an analog modem at the remote access server.

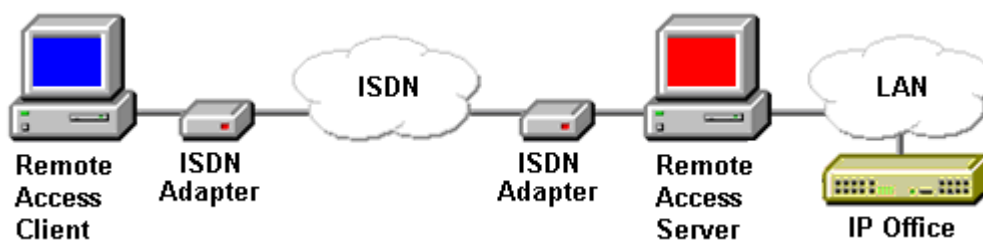
Because PSTN was not designed for data transmission, there are limits to the maximum bit rate of a PSTN connection. The maximum theoretical bit rate supported by PSTN connections is 33,600 bits per second or 33.6 Kbps. The V.90 standard is very often referred to as offering 56 Kbps, in fact the standard supports a speed of 33.6 Kbps for upload and 56 Kbps for download. This download speed is only achieved where part of the infrastructure in the connection is digital. For a typical analog RAS dial up connection this speed is unlikely to be reached as the signal is converted from analog-digital and then digital-analog again.



### ISDN Connection

ISDN is a digital replacement of PSTN. ISDN provides a single digital network to handle voice, data, fax, and other services over existing local loop wiring. ISDN behaves like an analog phone line except that it is a digital technology with higher data rates and a much lower connection time. ISDN offers multiple channels, with each channel operating at 64 Kbps. Because the network is digital from end to end, there are no analog-to-digital conversions.

The equipment needed consists of an ISDN adapter for the remote access client and the remote access server. Remote access clients typically use Basic Rate ISDN (BRI) with two 64-Kbps channels; large organizations typically use Primary Rate ISDN (PRI) with 23 64-Kbps channels.



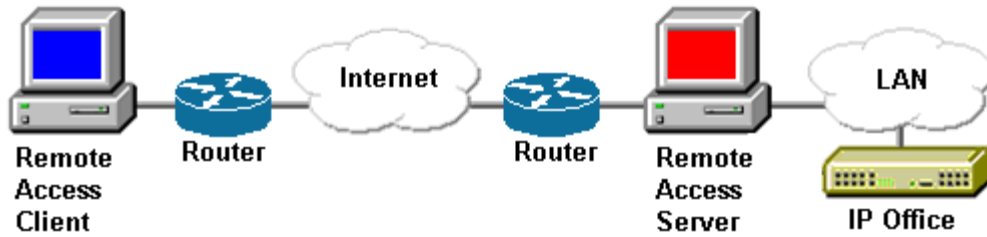
Note: Symantec pcAnywhere ISDN connectivity is only supported in North America and Europe.



### 2.1.5 Internet Connectivity

If a modem and trunk line are not available for accessing the customer site then it may be possible to connect to the site using the internet. Symantec pcAnywhere lets you connect to a host computer over the Internet, provided that both the host and the remote computers have Internet access.

To support inbound connections from a pcAnywhere remote, you must configure the router at the customer site to direct incoming data from the pcAnywhere ports to the internal IP address of the host computer.

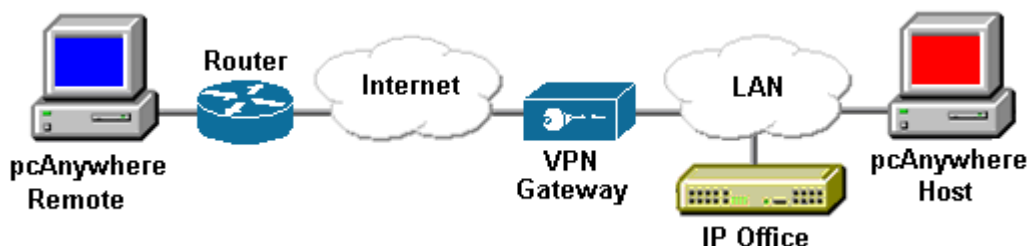


For pcAnywhere to function correctly, the local IP address of the pcAnywhere host computer must use a static IP address so that the IP address does not change.

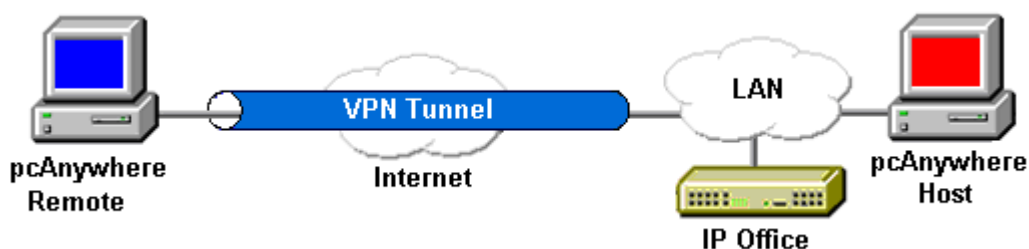
Symantec pcAnywhere uses port 5631 as the TCP (Data) and port 5632 as the UDP (Status) ports. Opening these ports allows the pcAnywhere information to pass through the router to the host, located behind the router. The router must be configured to send this information to the particular pcAnywhere host computer. This is called "port forwarding. If the router includes a firewall, ensure that both pcAnywhere ports are open.

## 2.1.6 Virtual Private Network (VPN) Connectivity

Virtual private networks (VPN) are point-to-point connections across a private or public network such as the Internet. In a typical VPN deployment, a client initiates a virtual point-to-point connection to a remote access server over the Internet. Taking advantage of the internet provides the functionality and security of private WAN connections at a lower cost than dial-up or leased line connections.



The VPN connectivity option requires the customer to provide an IPSec VPN compatible gateway/router for establishing the IPSec VPN connection. Information on how to connect to the VPN device must be provided by an Administrator at the customer site.



Once the remote user connects to the corporate network using the VPN the remote computer becomes a node on the network and can then use pcAnywhere to connect to the target computer using TCP/IP.

# **Chapter 3.**

## **IP Office Remote Manager**

---

### 3. IP Office Remote Manager

The IP Office system is easily managed through the IP Office Manager application. IP Office Manager is a Windows PC software application that connects to the IP Office system using TCP/IP. It can be on the same LAN as the IP Office, remote on the WAN, or connected via the Remote Access Server with a Router or modem.

The following Remote Manager example uses an ISDN dial up connection and the default IP Office RAS configuration that is setup out of the box for remote management and takes you through the steps required to create a dial up connection. Once the dial up connection is established it will be possible to use the IP Office Manager application installed on a local PC to manage the remote IP Office system.

This example assumes that your local PC and the remote IP Office system are on different subnets and the following settings have been left as default in the IP Office configuration:

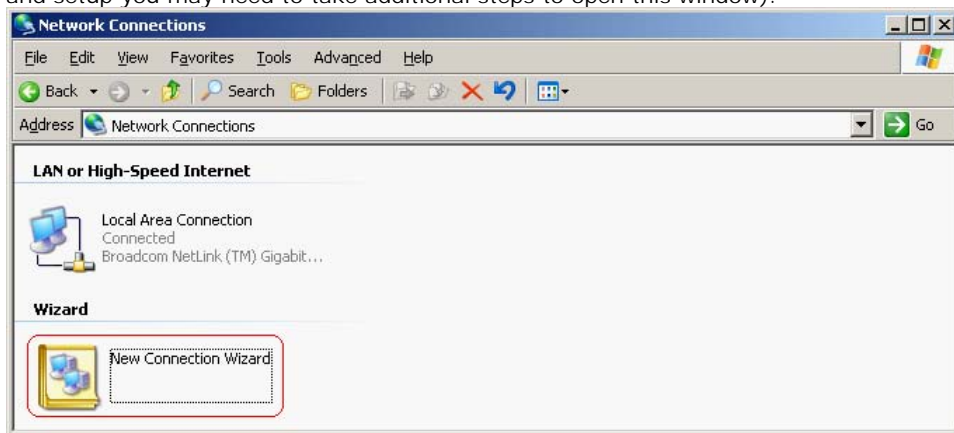
- The IP Office is acting as DHCP server (if this is not the case make sure that the DHCP mode is set to DialIn).
- The RAS entry called DialIn exists.
- The user called RemoteManager exists and the option called Dial In On found on the Dial In tab for this user is checked.
- There is a default incoming call route with a destination of DialIn and the bearer capability is set to Any Data.



## 3.1 Setting Up the Dial Up Connection

Before the dial up connection can be created you must ensure that your dial up device is installed and working, it is connected to a line and the Microsoft Windows service called Remote Access Connection Manager is running.

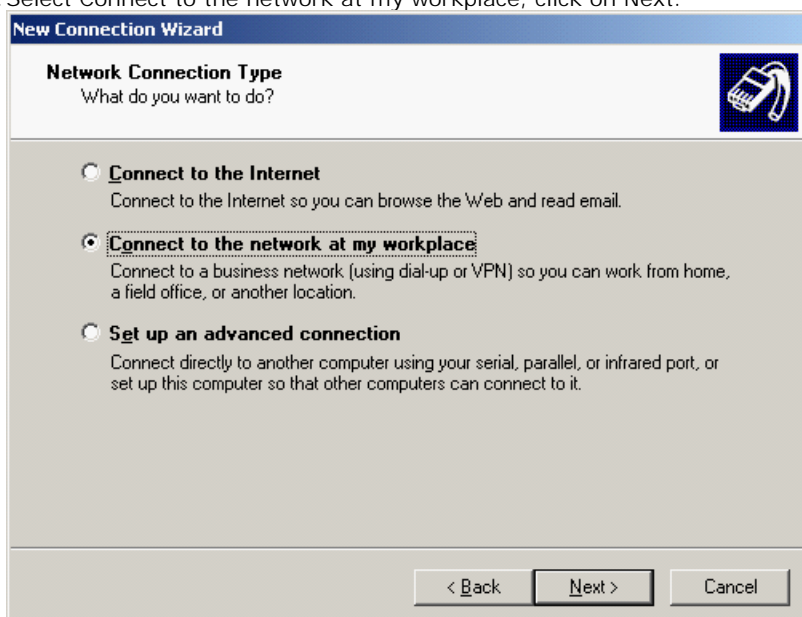
1. Click on the Start menu, choose Control Panel and then select Network Connections. (Depending on operating system and setup you may need to take additional steps to open this window).



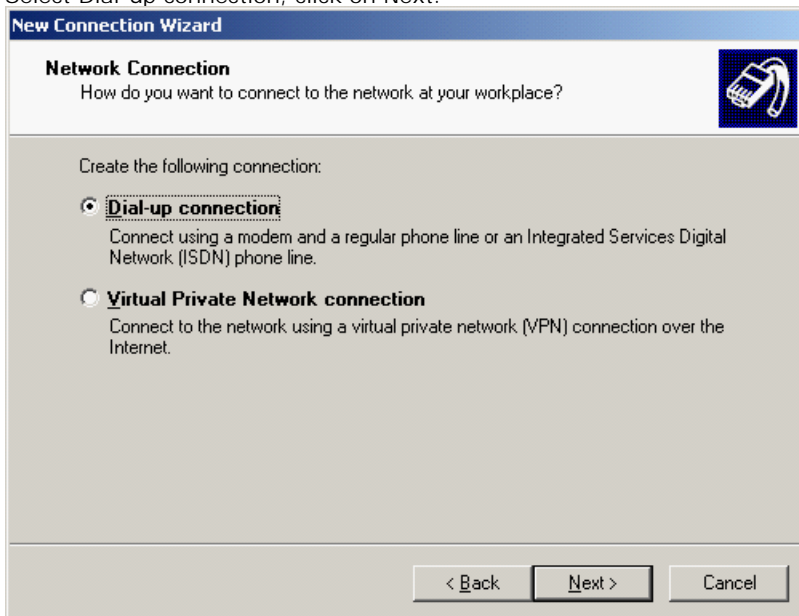
2. Double click the New Connection Wizard. The New Connection Wizard will start, click on Next.



3. Select Connect to the network at my workplace, click on Next.



4. Select Dial-up connection, click on Next.



**New Connection Wizard**

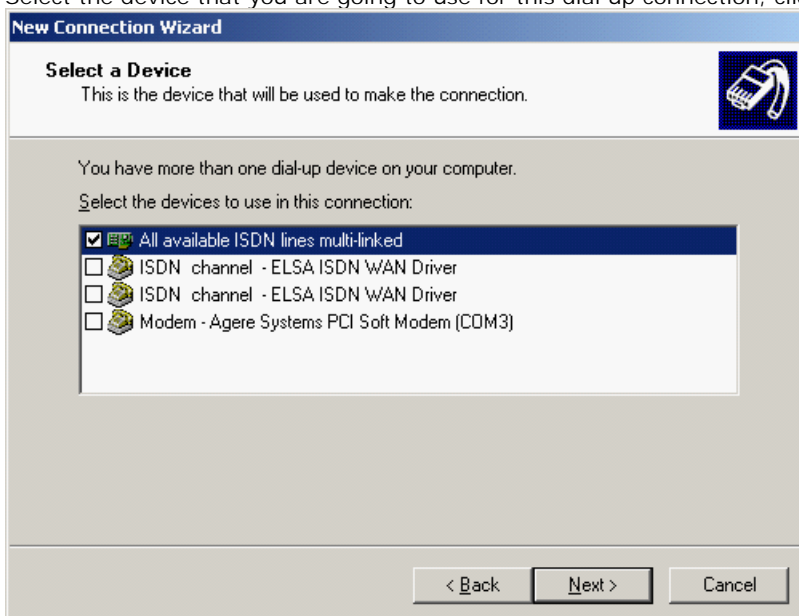
**Network Connection**  
How do you want to connect to the network at your workplace?

Create the following connection:

- ☒ **Dial-up connection**  
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
- ☐ **Virtual Private Network connection**  
Connect to the network using a virtual private network (VPN) connection over the Internet.

< Back   Next >   Cancel

5. Select the device that you are going to use for this dial up connection, click on Next.



**New Connection Wizard**

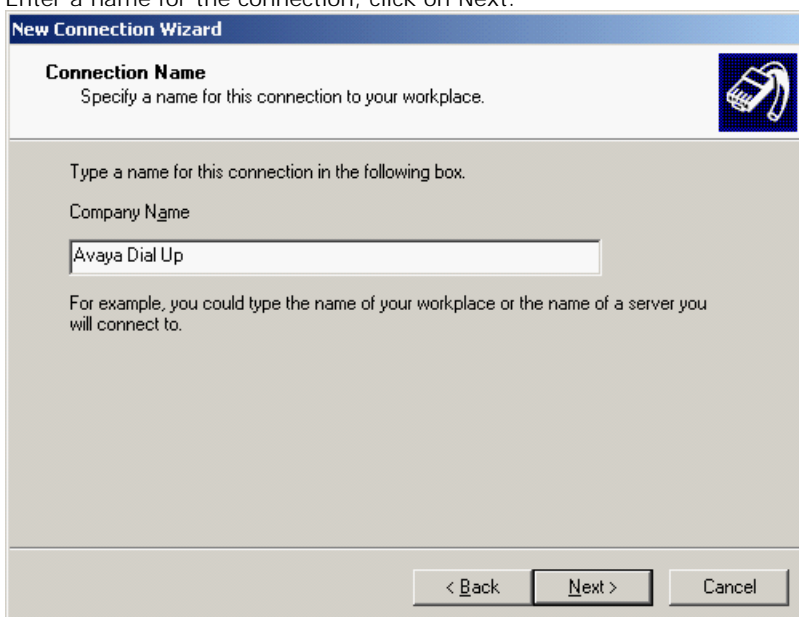
**Select a Device**  
This is the device that will be used to make the connection.

You have more than one dial-up device on your computer.  
Select the devices to use in this connection:

- ☒ All available ISDN lines multi-linked
- ☐ ISDN channel - ELSA ISDN WAN Driver
- ☐ ISDN channel - ELSA ISDN WAN Driver
- ☐ Modem - Agere Systems PCI Soft Modem (COM3)

< Back   Next >   Cancel

6. Enter a name for the connection, click on Next.



**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

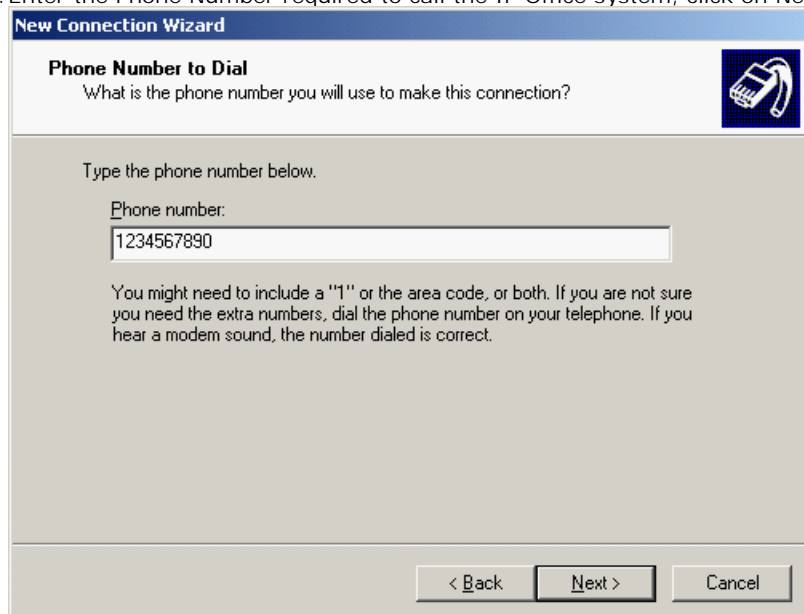
Company Name

Avaya Dial Up

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back   Next >   Cancel

7. Enter the Phone Number required to call the IP Office system, click on Next.



**New Connection Wizard**

**Phone Number to Dial**  
What is the phone number you will use to make this connection?

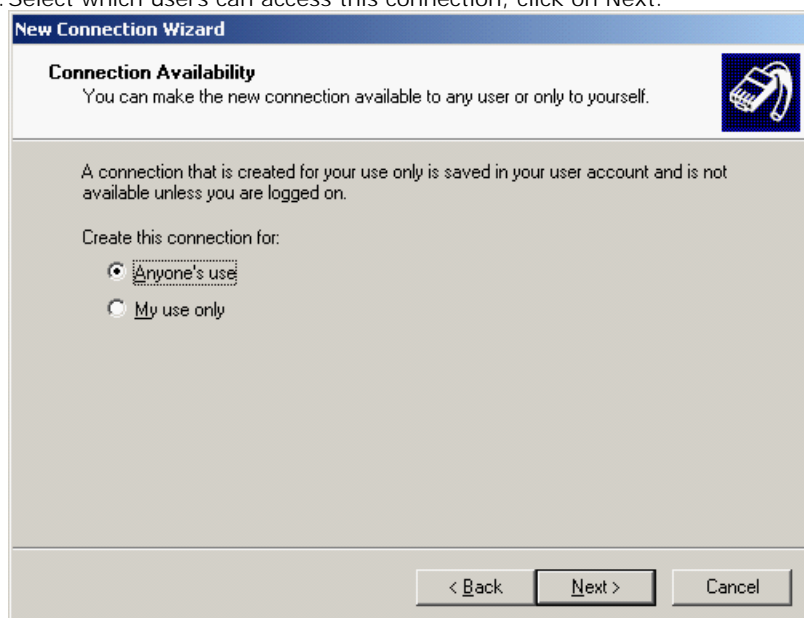
Type the phone number below.

Phone number:  
1234567890

You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.

< Back   Next >   Cancel

8. Select which users can access this connection, click on Next.



**New Connection Wizard**

**Connection Availability**  
You can make the new connection available to any user or only to yourself.

A connection that is created for your use only is saved in your user account and is not available unless you are logged on.

Create this connection for:

☒ Anyone's use  
☐ My use only

< Back   Next >   Cancel

9. To complete the setup click on Finish.



**New Connection Wizard**

**Completing the New Connection Wizard**

You have successfully completed the steps needed to create the following connection:

**Avaya Dial Up**

- Share with all users of this computer

The connection will be saved in the Network Connections folder.

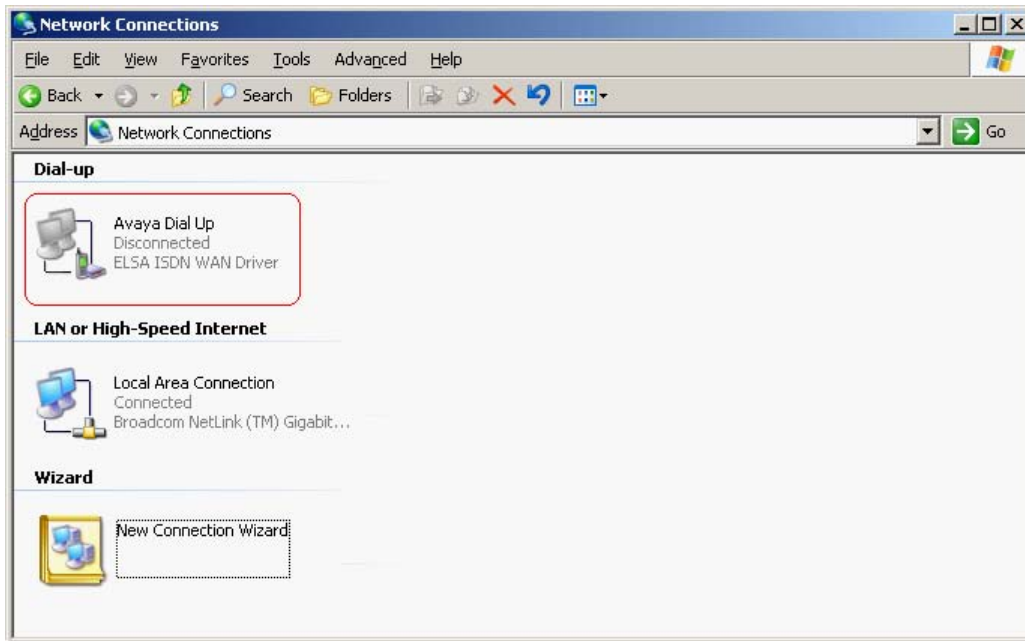
☐ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

< Back   Finish   Cancel



Once you click on Finish the connection screen should open automatically. If you chose not to place a shortcut for this connection onto the desktop then you can access the connection at a future time by opening the Network Connections window and double clicking on the connection item.



## 3.2 Connection Settings

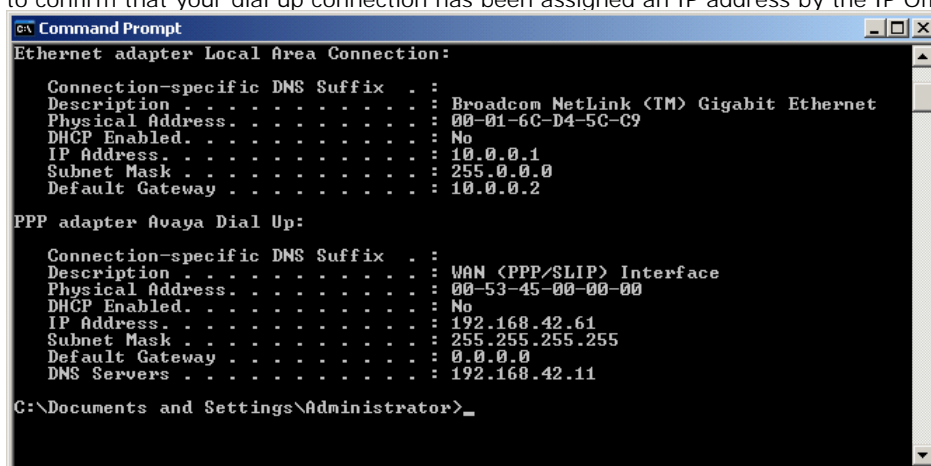
1. With the connection window open enter the user name and password required to connect to the IP Office system. The default user name is RemoteManager and the password is thepword. If you want to save these details then select the appropriate option.



2. Click on Dial to start the connection to the IP Office, you should see the current progress of the call, this will include dialing, verifying user name and password and registration of your computer on the network.

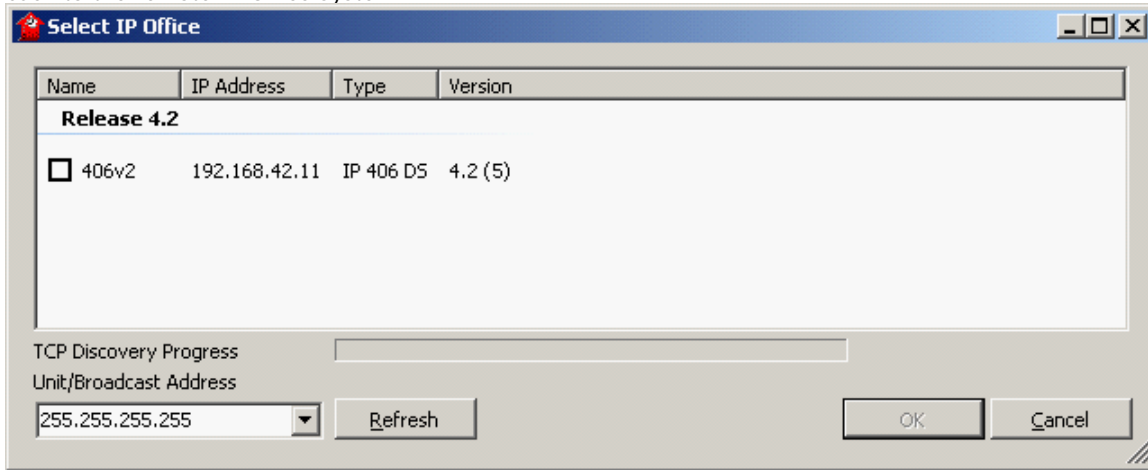


3. After the connection is made you can open a command prompt window on your local PC and use the ipconfig command to confirm that your dial up connection has been assigned an IP address by the IP Office system.



4. Once you have confirmed that you have successfully acquired an IP address you can then open the IP Office Manager application.

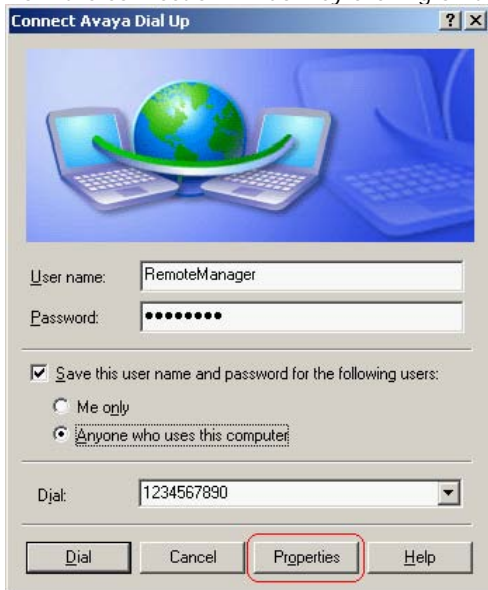
5. With the Manager application running click on File | Open Configuration or click on the Open Configuration icon on the toolbar, the Manager should find the remote IP Office system. You can then open, modify and save the configuration back to the remote IP Office system.



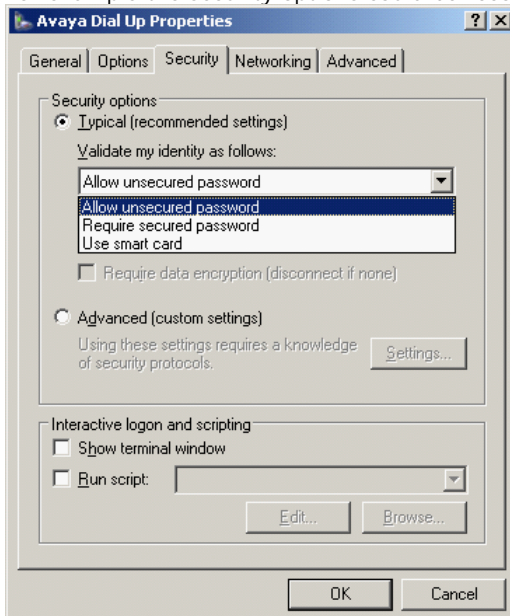
6. With the connection established you can also run the System Status Application, System Monitor and the Voicemail Pro Client. You could also open a pcAnywhere connection over this dial up connection and run the applications locally on the host PC.

### 3.3 Additional Configuration

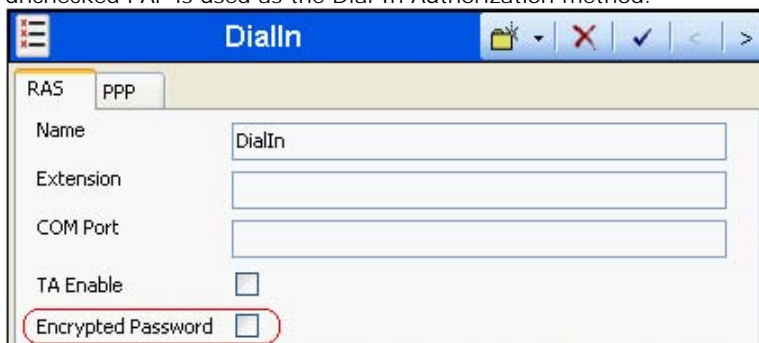
1. The details given above are enough to enable a basic dial up connection. Further configuration options are available from the connection window by clicking on the Properties button.



2. For example the security options could be reconfigured so that a secured password (CHAP) is required.



3. If a secured password is required then you also need to re-configure the DialIn RAS connection in the IP Office configuration. If the Encrypted Password box is checked then Dial In users are sent a CHAP challenge, if the box is unchecked PAP is used as the Dial In Authorization method.



# **Chapter 4.**

## **Preparing For Installation**

---

## 4. Preparing For Installation

Installation procedures might vary, depending on your work environment and which installation option you choose. You can choose a full product installation or a custom installation package that includes only the functionality that you need.

Before you install pcAnywhere, ensure that your computer meets the system requirements.

### 4.1 Symantec pcAnywhere System Requirements

The minimum resources that are required to install Symantec pcAnywhere Windows Host, Remote, Gateway and Web Remote are:

Operating Systems	Requirements
Windows 2000 Professional / Server / Advanced Server	Operating system requirements as defined by Microsoft
Windows XP Home/Professional (32-bit and 64-bit)	Internet Explorer 6.0 or later
Windows 2003 Server Standard/Enterprise (32-bit and 64-bit)	Java Runtime Environment 1.4.2 or later required for pcAnywhere Web Remote
Windows Vista Ultimate / Business / Enterprise / Home Premium / Home Basic (32-bit and 64-bit)	233MHz or faster processor 128MB of RAM 35MB of available hard disk space CD or DVD drive

The minimum resources that are required to install Symantec pcAnywhere Mobile are:

Operating Systems	Requirements
Windows Mobile 2003 SP1 for Pocket PC / Pocket PC Phone Edition or later	1MB of available RAM for installation

### 4.2 User Rights Requirements

Users must have administrator rights to install pcAnywhere. If you are logged on to a Vista computer as a non-administrator user, during the pcAnywhere installation, you will be prompted to enter administrator credentials. Windows XP restricts users who are assigned to the limited user or guest accounts from installing or uninstalling software, changing system-wide settings, or adding, editing, or deleting user accounts.

During the installation process, you might be required to restart the computer. If so, after the computer restarts, you must log on again using the same user credentials to ensure proper functionality.

## 4.3 Installation Options

The installation options that are available on the Symantec pcAnywhere installation CD are:

Installation Option	Description
Full version of Symantec pcAnywhere	Includes the host and remote components that you need for remote control, file transfer, and remote management tasks.  Runs on Windows operating systems only.
pcAnywhere components	Includes the components that you need to support pcAnywhere connections across multiple platforms, on mobile devices, and through Network Address Translation (NAT) devices.
Administrator tools	Includes tools to assist you in using and administering pcAnywhere.
Custom installations	Includes custom installation packages that contain only the functionality that you need.

## 4.4 The Difference Between A Host And A Remote

When two computers are connected using pcAnywhere they function in a client/server relationship. The host computer, as the server, waits for connections from a remote computer and provides the requested services.

When you configure a host computer, you control who can connect to the host computer and what level of access the remote user should have. For example, you can restrict a remote user from restarting the host computer. The remote computer, as the client, connects to the host computer and specifies the actions that should be carried out.





# **Chapter 5.**

# **Symantec pcAnywhere**

# **Installation**

## 5. Symantec pcAnywhere Installation

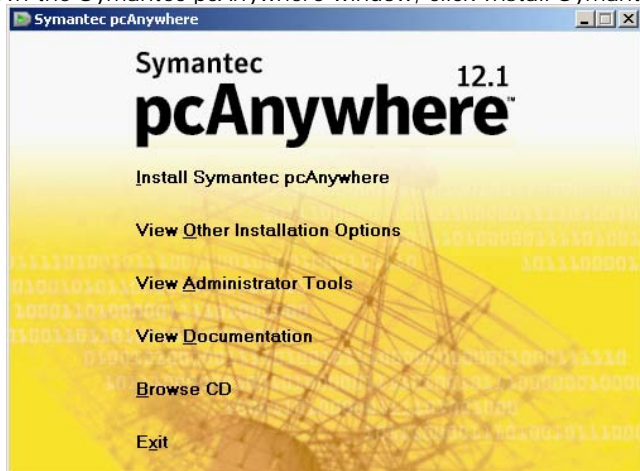
The full product version includes host, remote control, remote management, and file transfer features. In the Corporate and Retail versions, this includes the Host Administrator tool.

### 5.1 Installing The Full Product Version

1. Insert the Symantec pcAnywhere CD into the CD-ROM drive.

- If the installation window does not appear automatically after you insert the pcAnywhere installation CD, manually run the setup program, and then continue with the installation procedures.

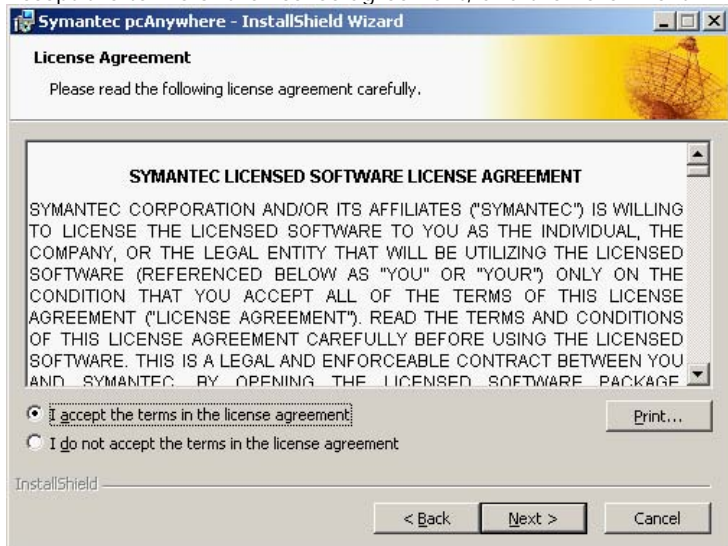
2. In the Symantec pcAnywhere window, click Install Symantec pcAnywhere.



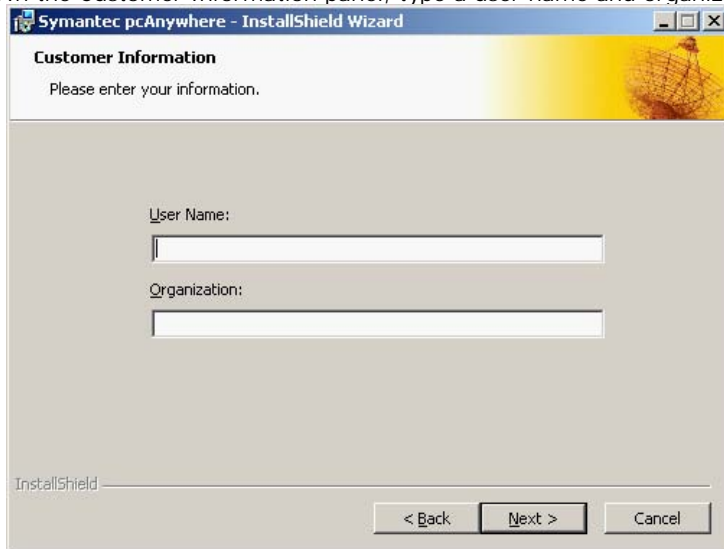
3. In the Welcome panel, click Next.



4. Accept the terms of the license agreement, and then click Next.



5. In the Customer Information panel, type a user name and organization.



**Symantec pcAnywhere - InstallShield Wizard**

**Customer Information**

Please enter your information.

User Name:

Organization:

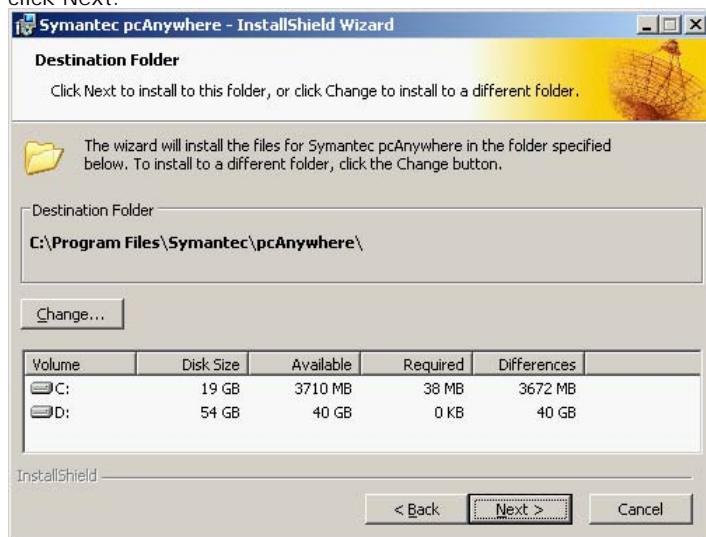
InstallShield

< Back   Next >   Cancel

6. Click Next.

7. In the Destination Folder panel, do one of the following:

- To install pcAnywhere in the default data directory, click Next.
- To change the installation directory, click Change. In the Change Current Destination Folder panel, browse to the folder location in which you want to install pcAnywhere, and then click OK. Then, in the Destination Folder panel, click Next.



**Symantec pcAnywhere - InstallShield Wizard**

**Destination Folder**

Click Next to install to this folder, or click Change to install to a different folder.

The wizard will install the files for Symantec pcAnywhere in the folder specified below. To install to a different folder, click the Change button.

Destination Folder  
**C:\Program Files\Symantec\pcAnywhere\**

Change...

Volume	Disk Size	Available	Required	Differences
C:	19 GB	3710 MB	38 MB	3672 MB
D:	54 GB	40 GB	0 KB	40 GB

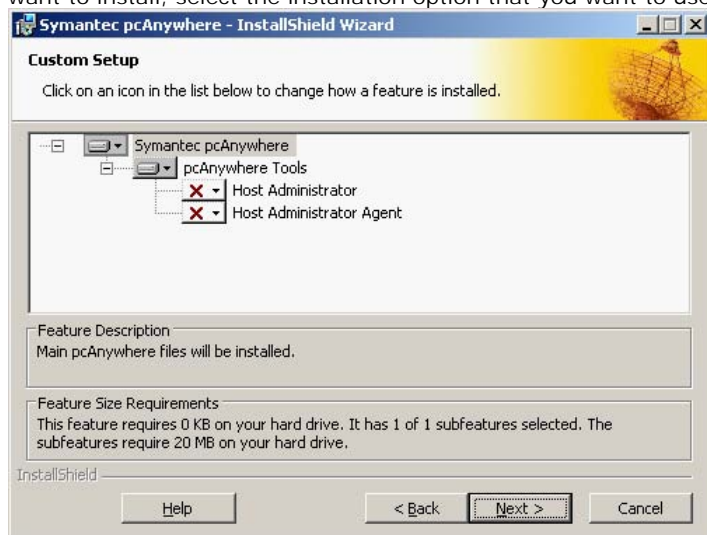
InstallShield

< Back   Next >   Cancel

8. In the Custom Setup panel, do one of the following:

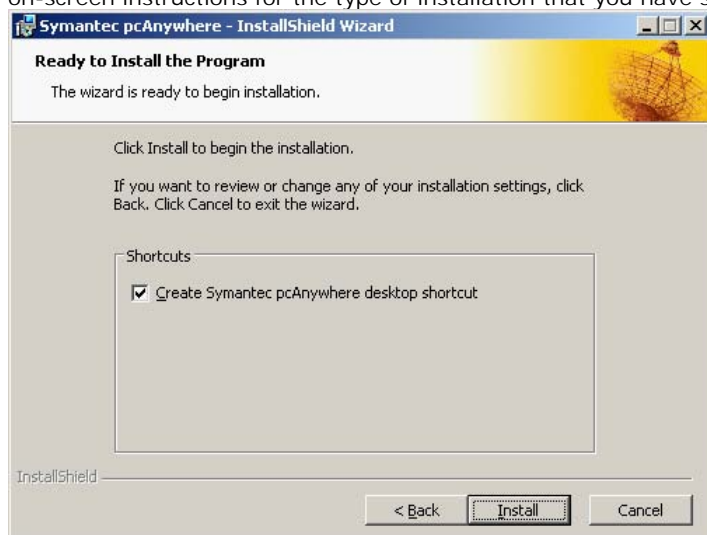
- To install pcAnywhere using the program default settings, click Next.

- To customize the installation or install administrator tools, click the down arrow next to the component that you want to install, select the installation option that you want to use, and then click Next.

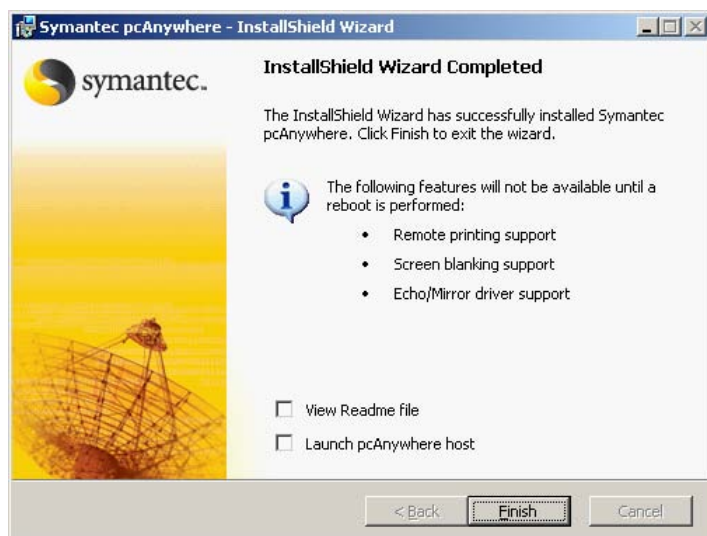


9. In the Ready to Install the Program panel, select the programs that you want to place on the desktop as shortcuts.

- The pcAnywhere program icon is placed on the desktop by default. If you do not want to create this shortcut on your desktop, uncheck the Create Symantec pcAnywhere desktop shortcut check box. Click Install and follow the on-screen instructions for the type of installation that you have selected.



10. Click Finish when the installation is complete.



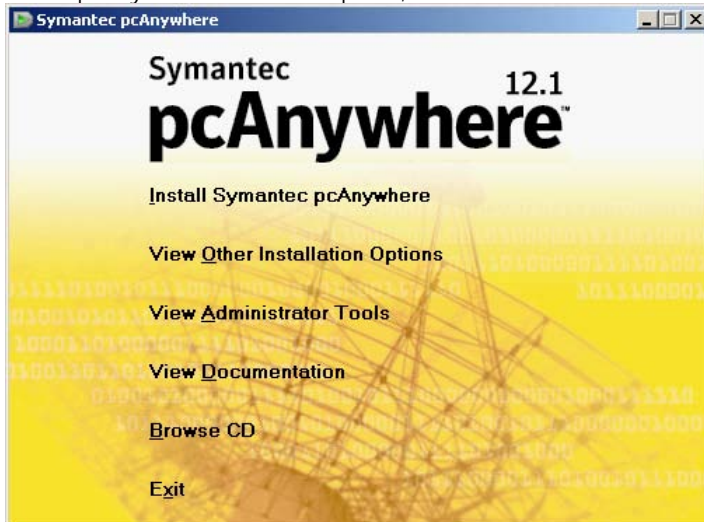
- If your computer requires updates to system files, you will be prompted to restart your computer. This step is necessary to ensure proper functionality.

## 5.2 Installing A Custom Version

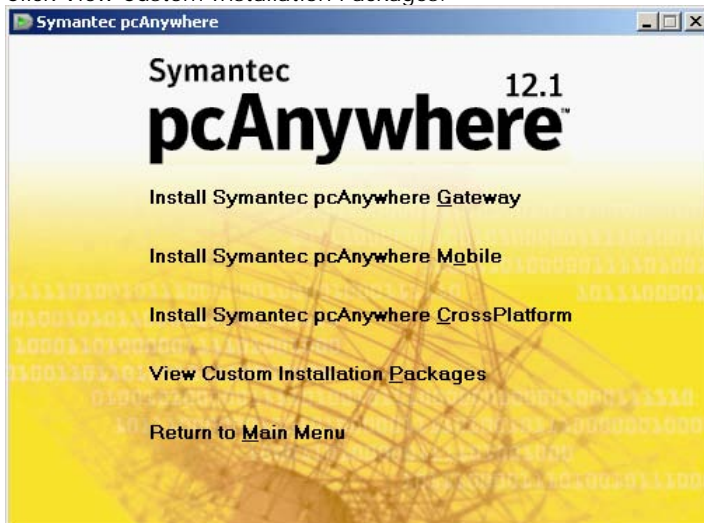
Symantec pcAnywhere lets you install a custom installation package that contains only the functionality that you need. Use these installation procedures as a guideline. Installation procedures might vary, depending on the type of installation.

To install a custom version

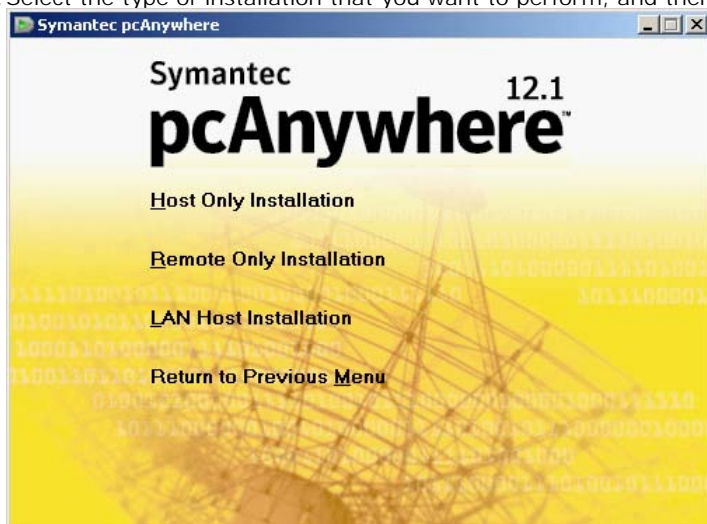
1. Insert the Symantec pcAnywhere CD into the CD-ROM drive.
  - If the installation window does not appear automatically after you insert the pcAnywhere installation CD, manually run the setup program, and then continue with the installation procedures.
2. In the pcAnywhere installation panel, click View Other Installation Options.



3. Click View Custom Installation Packages.



4. Select the type of installation that you want to perform, and then follow the on-screen instructions.



Package	Description
Host Only Installation	<p>Installs the host features that are needed to support network and modem connections. Excludes remote features.</p> <p>Select this option if you only want to receive connections or if you want to install pcAnywhere on two computers, where one computer is a host and the other is a remote.</p>
Remote Only Installation	<p>Installs the remote features that are needed to connect to a host computer for remote control, remote management, and file transfer. Excludes host features.</p> <p>Select this option if you only want to initiate connections or if you want to install pcAnywhere on two computers, where one computer is a host and the other is a remote.</p>
LAN Host Installation	<p>Installs the host features that are needed to support network connections only. Excludes remote features.</p> <p>Select this option if you only want to receive connections or if you want to install pcAnywhere on two computers, where one computer is a host and the other is a remote.</p>

# **Chapter 6.**

## **Symantec pcAnywhere Configuration**



---

## 6. Symantec pcAnywhere Configuration

The following section takes you through the basics of configuring the host and remote to allow communication to take place. Some of the more advanced features, such as encryption, are covered briefly. Symantec pcAnywhere is highly configurable and reference should be made to the user guide, the administration guide and the online help files for further guidance.

### 6.1 Starting Symantec pcAnywhere

Symantec pcAnywhere is installed in the Windows Program Files folder by default. During installation, pcAnywhere optionally lets you place a program icon on the

Windows desktop from which you can open the program. You can also open pcAnywhere from the Windows Start menu.

### 6.2 Setting Up The Host

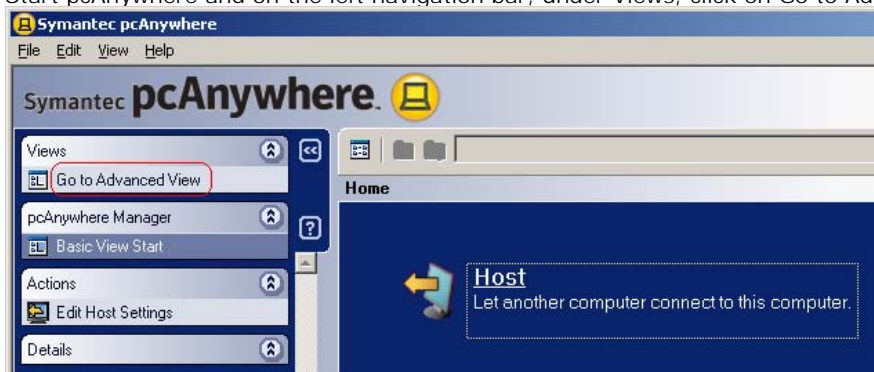
As a host, you let authorized remote users connect to your computer and take control of it. The remote user sees your computer screen and can open files or programs that you have given the user permission to access. Before remote users can connect to your computer, you must set up your computer to allow the connections. You must specify the connection type, what method to use to ensure that remote users have permission to access your computer, and other session options.

This information is stored in a host connection item file (.bhf), which appears as an icon in the Hosts window. The host connection item files are stored in the Symantec\pcAnywhere\Hosts (in Vista, C:\Program Data\Symantec\pcAnywhere\Hosts) folder in the Windows ALLUSERSPROFILE data directory.

The Connection Wizard guides you through the process of configuring your computer (the host computer) to allow another computer (the remote computer) to connect to it.

To use the Connection Wizard to configure a host connection:

1. Start pcAnywhere and on the left navigation bar, under Views, click on Go to Advanced View.

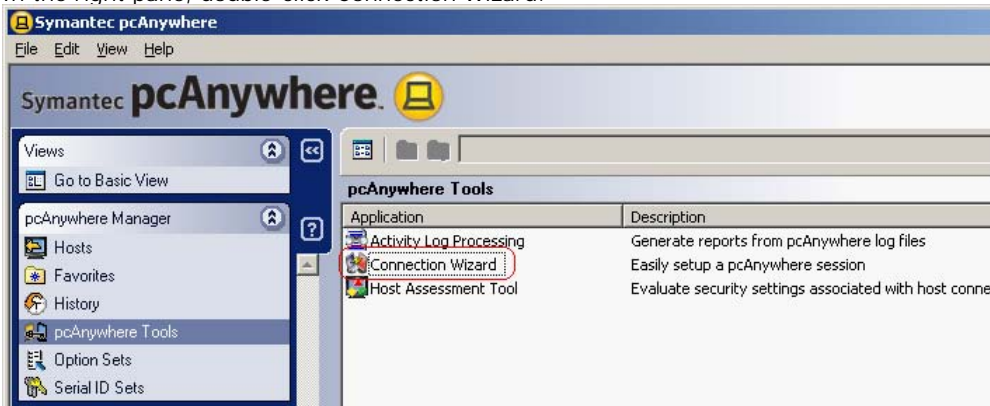


2. In Advanced View, on the left navigation bar, under pcAnywhere Manager, click pcAnywhere Tools.

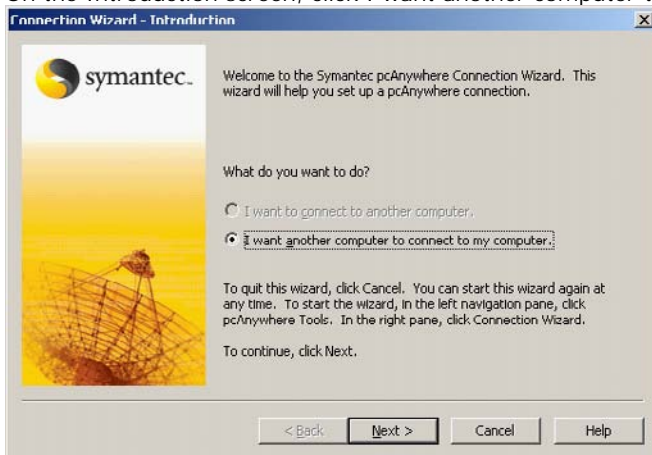




3. In the right pane, double-click Connection Wizard.



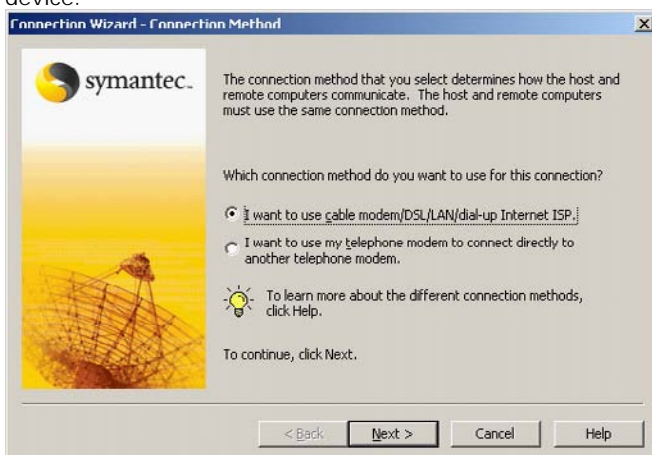
4. On the Introduction screen, click I want another computer to connect to my computer, and then click Next.



5. Select one of the following:

- I want to use cable modem/DSL/LAN/dial-up Internet ISP
- I want to use my telephone modem to connect directly to another telephone modem

6. The wizard automatically detects the connection devices that are available on your computer. If your computer has multiple connection devices, choose the device that you want to use for the connection that you are configuring. For example, if the remote computer uses a phone modem, you should select the phone modem as your connection device.

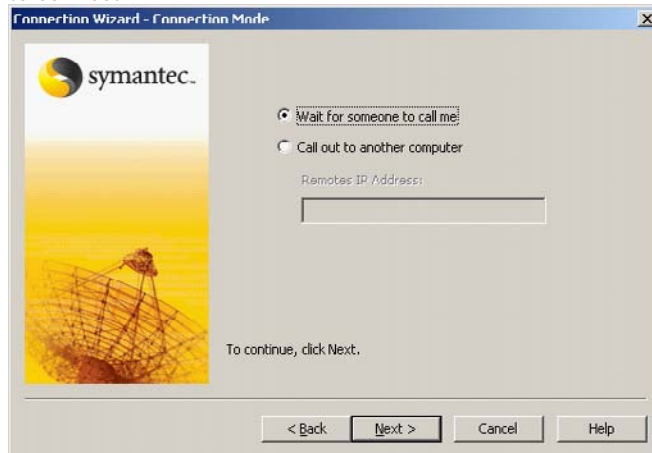


6. Click Next.

7. In the Connection Mode panel, select one of the following:

- Wait for someone to call me
- Call out to another computer

- In the Remotes IP Address box, type the IP address or modem phone number of the computer to which you want to connect.



8. Click Next.

9. In the Authentication Type panel, select one of the following:

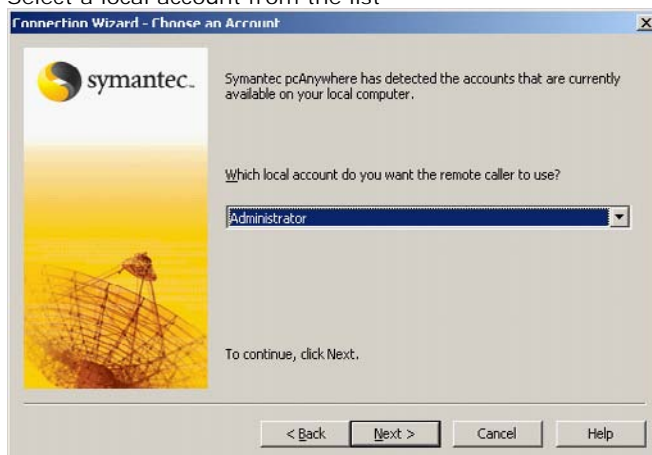
- I want to use an existing Windows account - Validates a user or group by checking a list that is maintained on a workstation or shared directory. The Connection Wizard detects the accounts that are available on your local computer.
- I want to set up a user name and password - Uses pcAnywhere Authentication to verify whether a remote user has permission to connect to the host by checking the list of users and passwords that are maintained on the host computer. This method of authentication is the least secure.



10. Click Next.

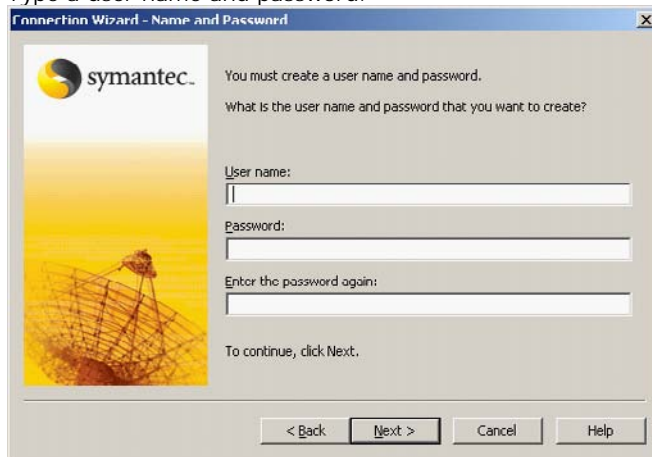
11. Do one of the following:

- If you have chosen to use an existing Windows account:
  - Select a local account from the list



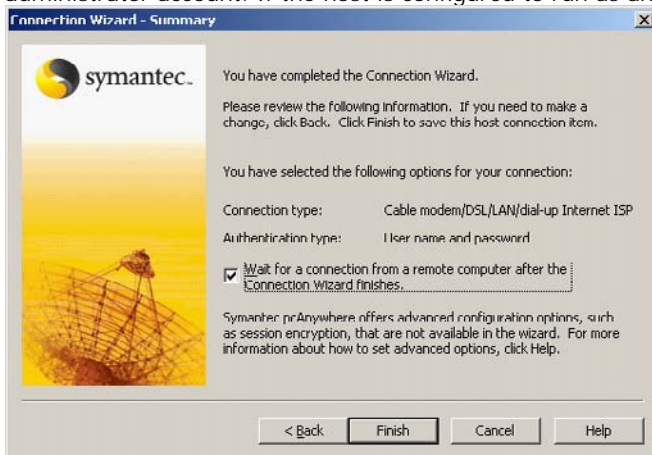
- Or if you have chosen to set up a user name and password:

- Type a user name and password.

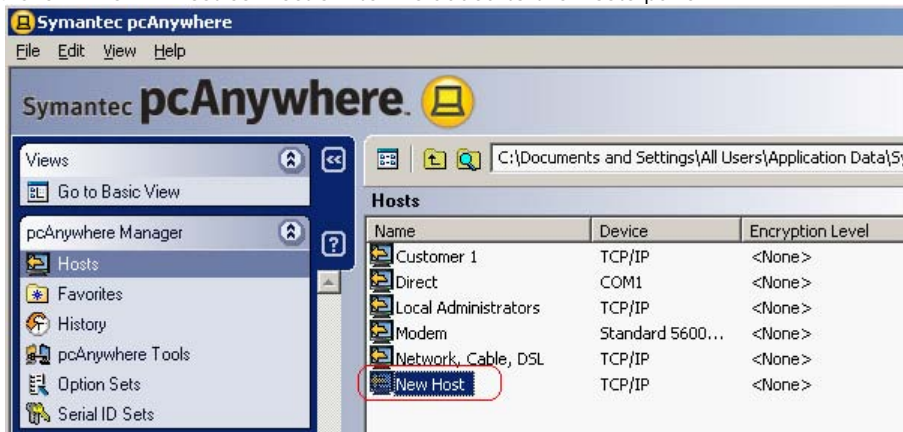


12. Click Next.

13. On the Summary screen, verify the settings. To start the host session upon closing the wizard, check Wait for a connection from a remote computer after the Connection Wizard finishes. In Windows Vista, the operating system might prompt you to approve this action. You do not receive this prompt if you are logged on to the built-in administrator account. If the host is configured to run as an application, the prompts are not given.



14. Click Finish. A host connection item is added to the Hosts pane.

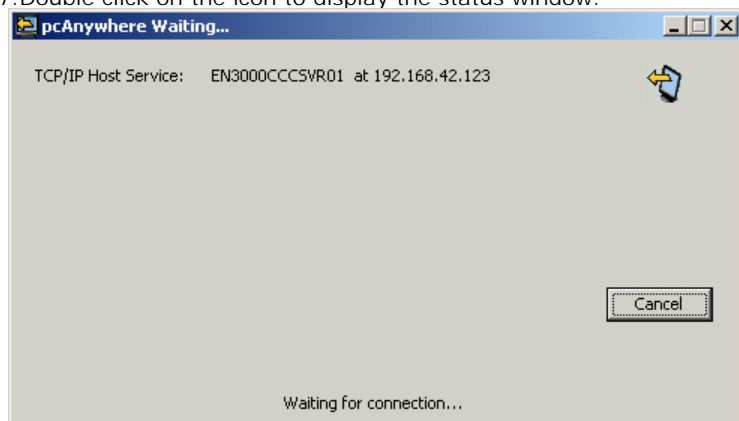


15. To name the connection item, in the Symantec pcAnywhere window, in the Hosts pane, type the name that you want to give the host connection item and then press Enter.

16. If you selected to start the host session, the Symantec pcAnywhere Waiting icon appears in the Windows system tray.



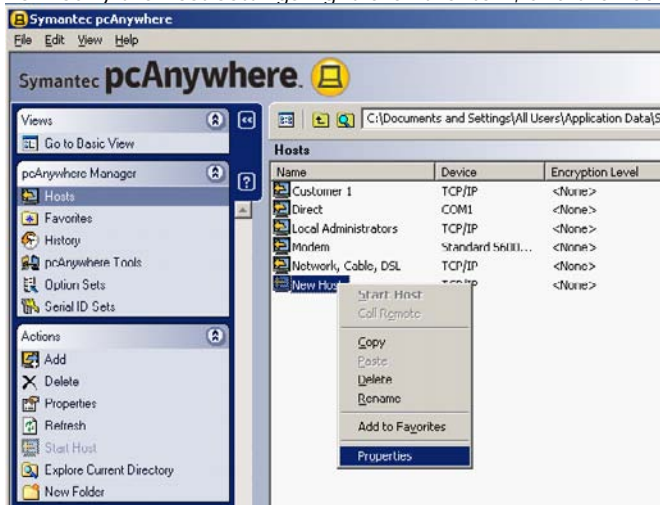
17. Double click on the icon to display the status window.



## 6.3 Configuring Advanced Host Properties

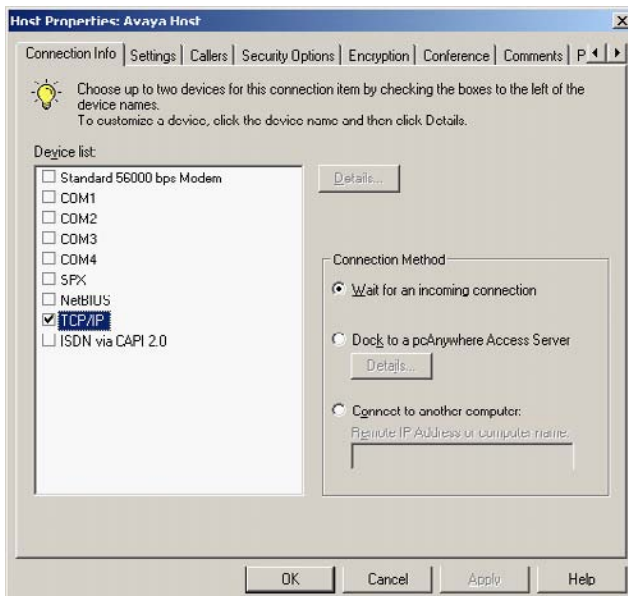
The Connection Wizard allows the setup of the minimum configuration that is required to configure the host. For more control over your connections you can use the Advanced option to create or modify host connection items. Advanced properties provide access to further options that are not available in the Connection Wizard, such as host startup options and public-key encryption.

1. To modify the host settings right-click the item, and then select Properties.



### 6.3.1 Connection Info

A connection device is the interface that handles communication between the host and remote computers. A host computer can wait for a connection from two devices. A host can accept only one connection at a time. When a remote establishes a connection on one device, the other device is not available until the session ends.

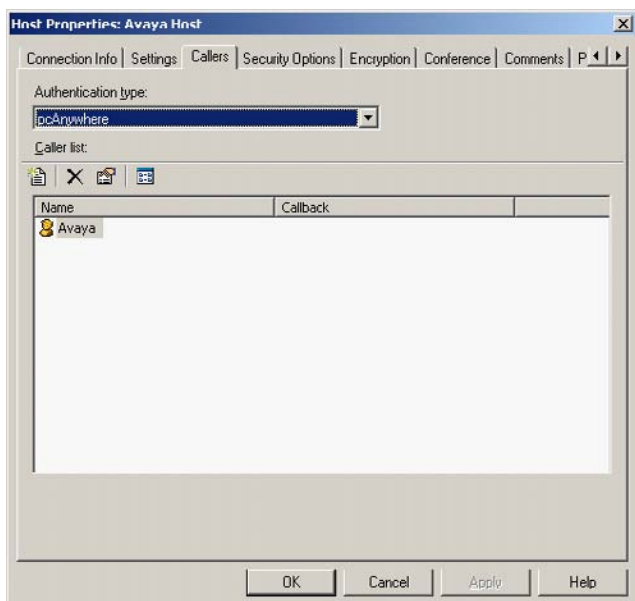


## 6.3.2 Callers

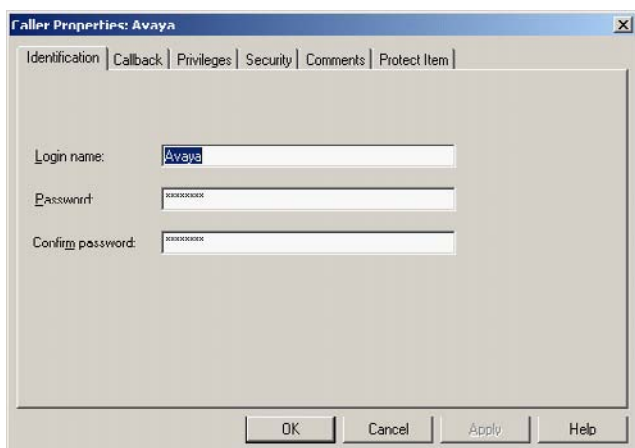
Caller rights let you limit the level of access that a remote user has to your computer. You can control whether a user can perform certain functions, such as restarting your computer or canceling your host session.

You can also prevent users from performing file transfer operations or stopping a process that is running. If you want to let a remote user synchronize or clone folders on your computer, you must enable upload and download privileges.

In the Callers tab right-click the caller item that you want to configure, and then click Properties.

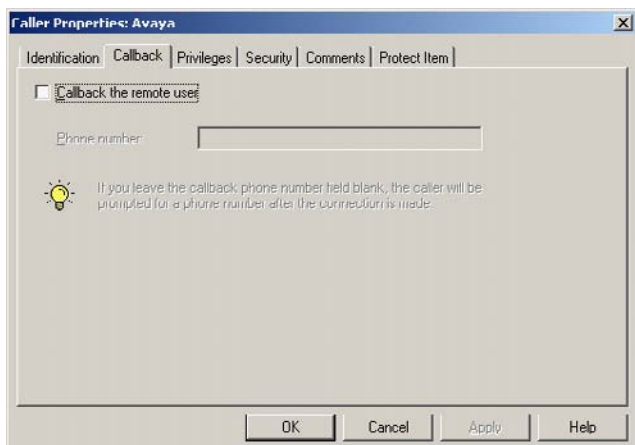


The Identification tab shows the details of the logon account for the Remote user that was setup during the host configuration. This screen will appear differently dependant on the Authentication type chosen.

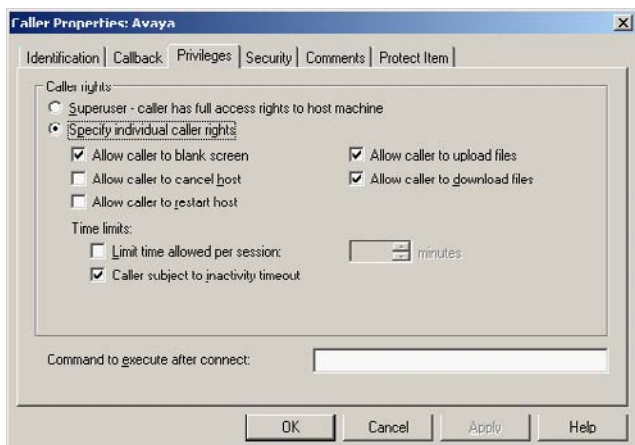


If a modem is being used for the remote connection then a Callback tab will be visible. The Callback feature lets you confirm the identity of a remote user who is connecting over a modem or ISDN.

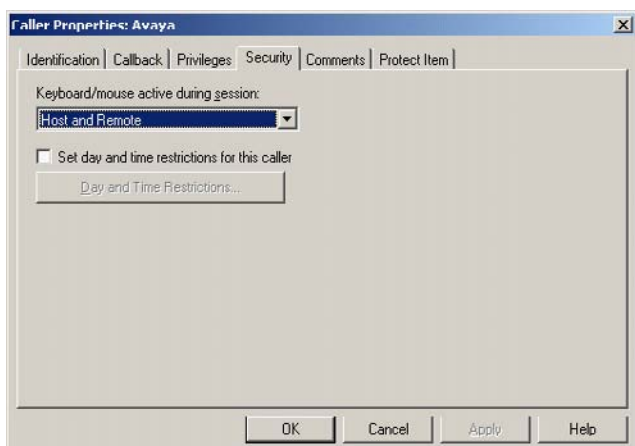
When a remote user attempts to connect to the host, the host computer terminates the connection, and then calls back the remote computer at a preconfigured number. If the remote computer is not waiting for a connection at that number, the host cancels the session.



The Privileges tab allows you to setup what this user can do when they are connected to the host PC. They can either be a Superuser, which gives the user full access rights, or you can select the options for which you want to allow or restrict access.

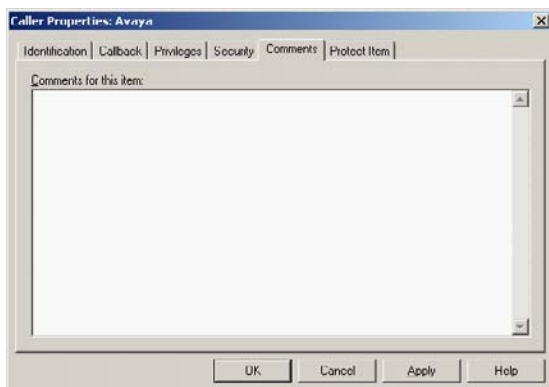


Symantec pcAnywhere lets both the host user and the remote user use the keyboard and mouse during a session. From the Security tab you can change this setting to restrict control for the keyboard and mouse for a specific user or group of users. You can also setup date and time restrictions.

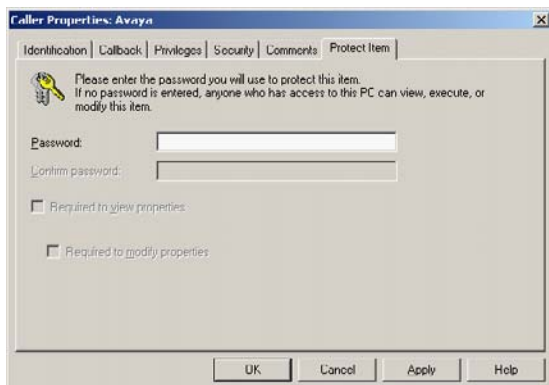




The Comments tab is used to record any information that is relevant to this connection.

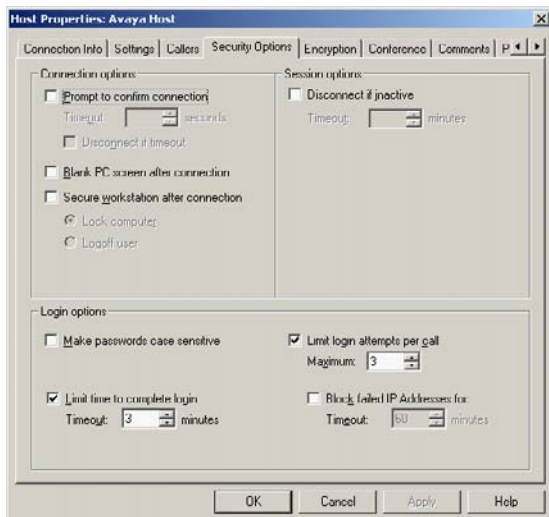


To protect the caller configuration settings you can set a password in the Protect Item tab. By setting a password you can stop users from viewing or modifying the caller settings unless they know the password.



### 6.3.3 Security Options

The Security Options tab is used to configure a number of security options that prevent the host computer from unauthorized access and protect the security of the session.





### 6.3.4 Encryption

Encryption is a method of encoding or scrambling data to prevent unauthorized users from reading or tampering with the data. Modern methods of computer cryptography use complex mathematical algorithms to encrypt and decrypt data. Symantec pcAnywhere uses a standard combination of public-key cryptography and symmetric encryption algorithms to ensure that the data you send cannot be read or altered by unauthorized users while in transit.

The Symantec Cryptographic Module that is included in Symantec pcAnywhere contains algorithms that provide AES encryption at varying key lengths. The Symantec Cryptographic Module has received Federal Information Processing Standards (FIPS) 140-2 certification. The FIPS 140-2 Security Requirements for Cryptographic Modules is a set of standards developed by the National Institute of Standards and Technology (NIST). The FIPS 140-2 standards apply to federal agencies that use cryptographic based security systems to protect sensitive but unclassified information in computer and telecommunication systems. This security technology is mandated for many government and financial institutions in the United States and Canada.

#### Symmetric Encryption

Symmetric encryption encrypts and decrypts data using a set of symmetric cryptographic keys that are randomly generated for each connection. These keys are negotiated and exchanged using standard protocols for anonymous key exchange. During a session, both the sender and the recipient share these keys.

The benefit of symmetric encryption is that it is easy to set up, however, it is not without risk. Because the keys are exchanged anonymously, it is possible for someone to intercept the data during the initial key exchange, manipulate the keys used for this exchange, and discover the symmetric key. This type of vulnerability is known as a Man in the Middle attack. The recipient has no way of verifying that the data actually came from the person who originally sent it.

You can select the symmetric encryption algorithm that best suits your security and performance needs. Each algorithm uses a string of bits known as a key to perform the calculations. You can strengthen the level of encryption by selecting a key length. The larger the key length, the greater the number of potential patterns that can be created. This makes it more difficult to break the encryption code. A larger key length creates stronger encryption, but it might also result in slower performance. The key lengths that are available depend on the type of algorithm that you select and your computer's operating system.

#### Public-key Encryption

Public-key encryption requires that both the sender and recipient have a digital certificate and an associated public/private key pair. The public key is distributed freely as part of the digital certificate; however, the private key is a closely guarded secret. The private key can decrypt what the public key encrypts.

Like symmetric encryption, public-key encryption encrypts and decrypts data by using the same set of symmetric cryptographic keys. The difference is in the key exchange protocol that is used. While symmetric encryption uses an anonymous protocol, public-key encryption uses a strongly authenticated protocol.

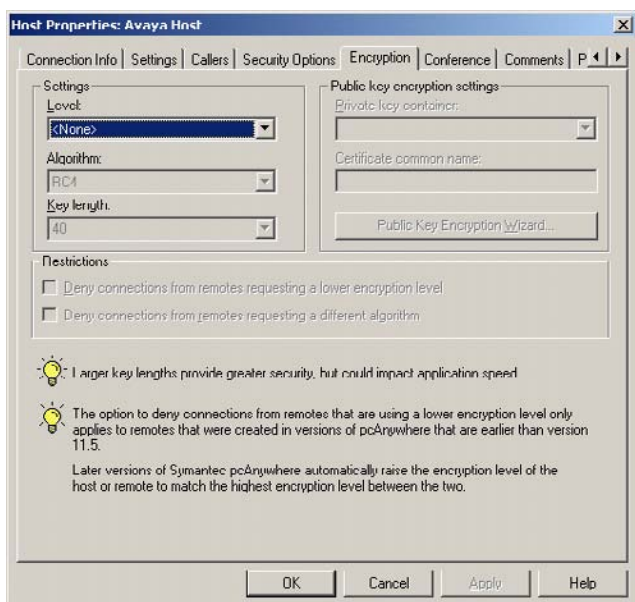
During the key exchange, the sender generates a symmetric key and encrypts it using the recipient's public key. Only the recipient can decrypt this data using a private key, which is never exchanged. For this reason, public-key encryption is invulnerable to a Man in the Middle attack.

When deciding whether to use encryption and which method to use, you must balance performance with the need for security. Using strong encryption can protect the privacy and integrity of your data. However, it might also slow performance because stronger encryption requires more resources to process and transfer the data.

In the Encryption tab you can select the level of encryption that the connection will use. This can be set to:

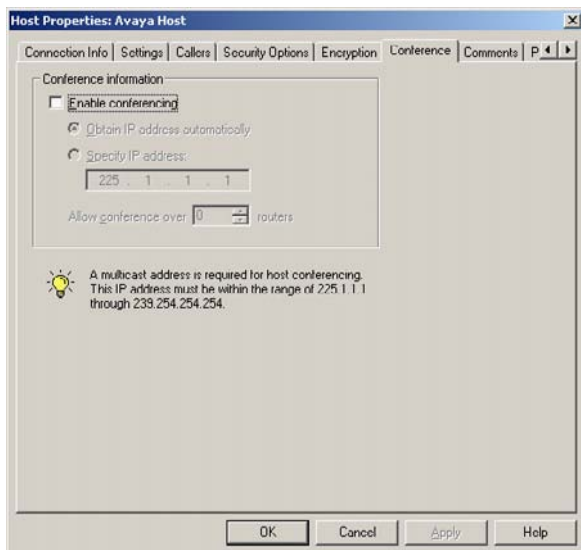
- None – Sends data without encrypting it.
- pcAnywhere encoding – Scrambles the data using a mathematical algorithm so that it cannot be easily interpreted by a third party.
- Symmetric – Encrypts and decrypts data using a cryptographic key.
- Public Key - Encrypts and decrypts data using a cryptographic key. Both the sender and recipient must have a digital certificate and an associated public/private key pair.

When using Symmetric or Public Key encryption you must also choose the Algorithm to use, RC4 or AES, and set the key length (40 or 128 for RC4, and 128, 192 or 256 for AES).



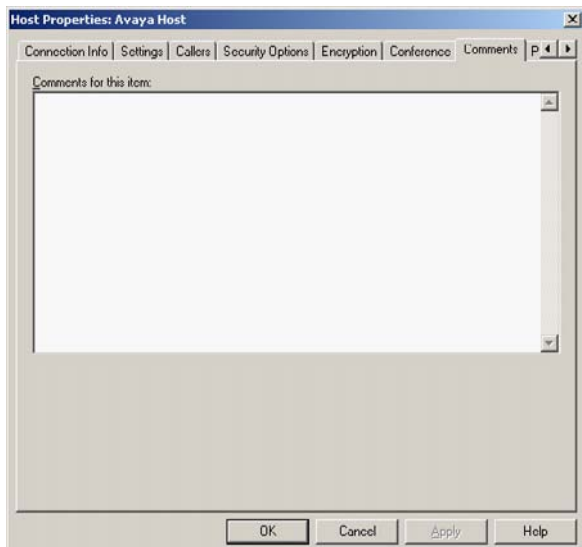
### 6.3.5 Conference

Conferencing lets multiple remote users connect to a single host and simultaneously view what is happening on the host screen. For example, you can host a conference to conduct a software training demonstration. A conference is basically a remote control session, except that multiple remote users connect to the host at the same time. The first caller can connect using any connection device. However, subsequent callers must use a TCP/IP network connection. The first remote user to establish a connection controls the host. Other users can view the activity on the host screen, but cannot take control of the host.



### 6.3.6 Comments

The Comments tab is used to record any information that is relevant to this connection.



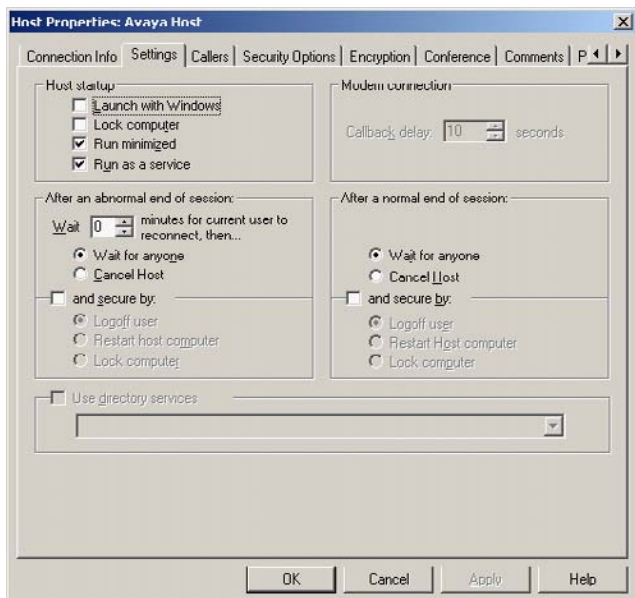
### 6.3.7 Settings

Symantec pcAnywhere lets you configure a host connection item to start automatically when you launch Windows. To protect against unauthorized access, if you configure a host to start automatically, you should also use the Windows lock computer feature.

The pcAnywhere host automatically runs as Windows service. This option lets you take advantage of the inherent security and performance features of the operating system. You must have administrator rights on the computer to run a service.

Additionally, Symantec pcAnywhere does not currently support setting a host to run as an application on Vista. After connecting to the host while running as an application on Windows Vista, if the remote user attempts a task that requires administrator privileges (for example, right-clicking My Computer > Manage), a request to enter administrator credentials appears on the host machine, but not on the remote machine, so the user cannot proceed.

The settings screen allows you to setup the host startup and end of session options. By default the host startup option "Launch with Windows" is not selected. This means that the Symantec pcAnywhere service will not run automatically when Windows starts. If you reboot the host PC and this option is not selected you will not be able to connect to the PC again until someone locally logs on to the PC and restarts the host service.



---

## 6.3.8 Protect Item

To protect the host configuration settings you can set a password in the Protect Item tab. By setting a password you can stop remote users from viewing or modifying the host settings unless they know the password.

The screenshot shows a Windows-style dialog box titled "Hst Properties: Avaya Hst". It has a tabbed interface with the following tabs: Settings, Callers, Security Options, Encryption, Conference, Comments, and Protect Item. The "Protect Item" tab is currently selected. Inside the dialog, there is a key icon and a message: "Please enter the password you will use to protect this item. If no password is entered, anyone who has access to this PC can view, execute, or modify this item." Below this message are two text input fields: "Password:" and "Confirm password:". Underneath these fields are three unchecked checkboxes: "Required to view properties", "Required to execute", and "Required to modify properties". At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

## 6.4 Changing The Default Port Numbers On The Host

Symantec pcAnywhere uses ports 5631 and 5632 for connections. These ports are registered, and in most cases, you do not need to change them. Symantec pcAnywhere uses the data port for data transmissions. It uses the status port to wait for connections and to exchange status information.

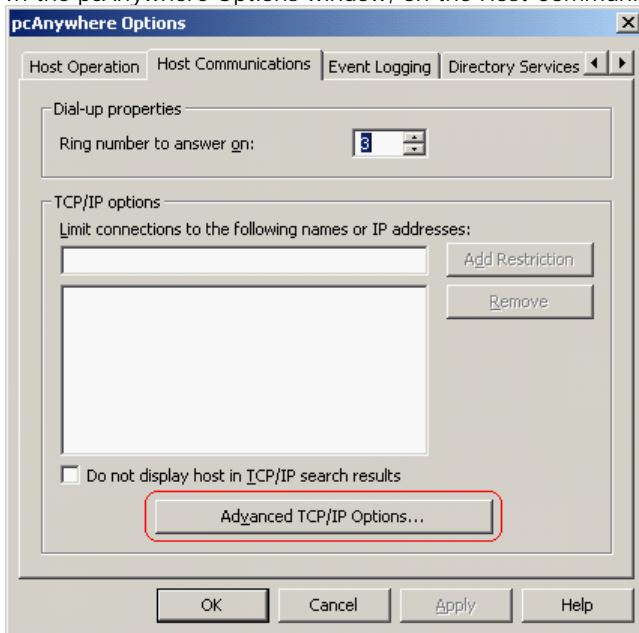
If you change the port numbers on the host computer, all remote users who want to connect to the host computer must also change their port settings to match.

To change the default port numbers on the host:

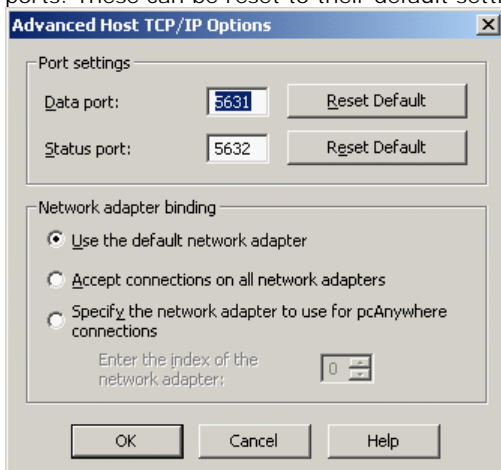
1. In the Symantec pcAnywhere window, on the Edit menu, click Preferences.



2. In the pcAnywhere Options window, on the Host Communications tab, click Advanced TCP/IP Options.



3. In the Advanced Host TCP/IP Options window enter the new port numbers that should be used for the data and status ports. These can be reset to their default settings by clicking on the Reset Default buttons.



## Setting Up The Remote

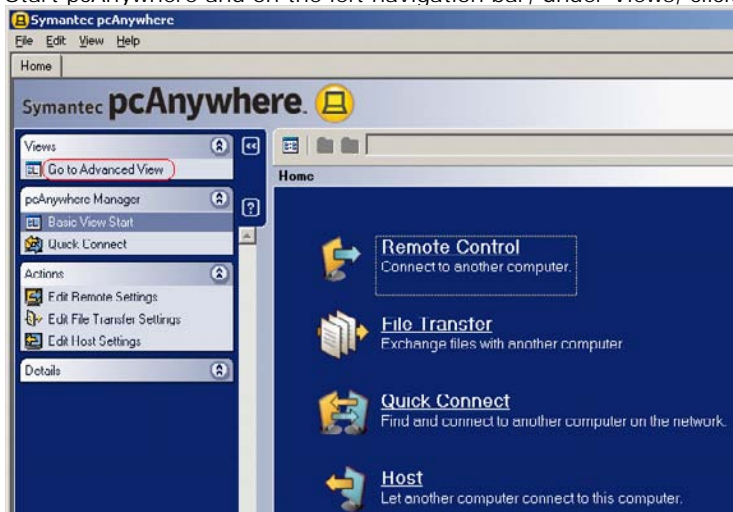
Before you can connect to a host computer, you must set up your computer with the connection and security settings required to make the connection. This information is stored in a remote connection item file (.chf), which appears as an icon in the Remotes window.

The remote connection item files are stored in the pcAnywhere program data directory (:\ProgramData\Symantec\pcAnywhere\Remotes).

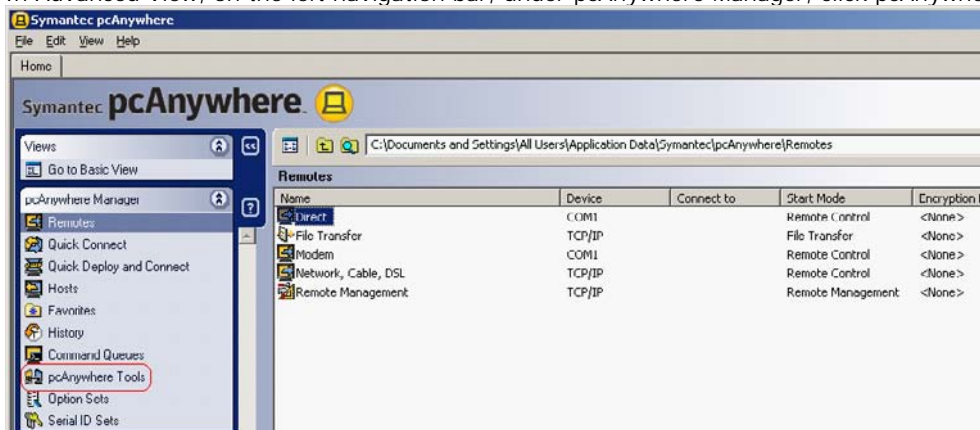
The Connection Wizard guides you through the process of configuring your computer (the remote computer) to connect to another computer (the host computer).

To use the Connection Wizard to configure a remote connection:

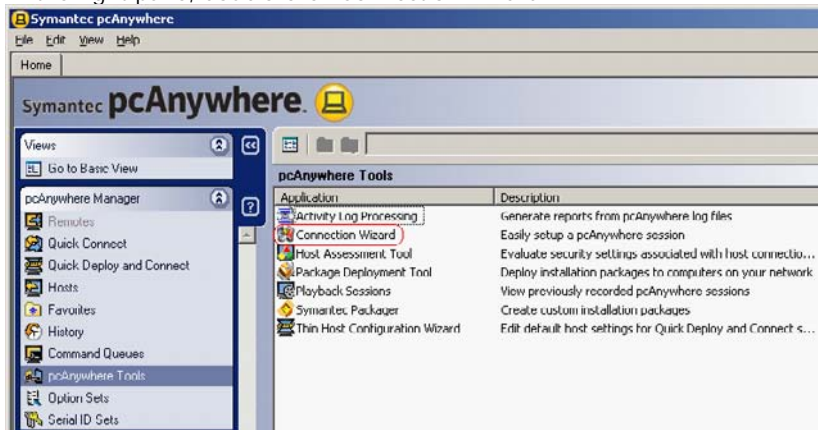
1. Start pcAnywhere and on the left navigation bar, under Views, click on Go to Advanced View.



2. In Advanced View, on the left navigation bar, under pcAnywhere Manager, click pcAnywhere Tools.



3. In the right pane, double-click Connection Wizard.

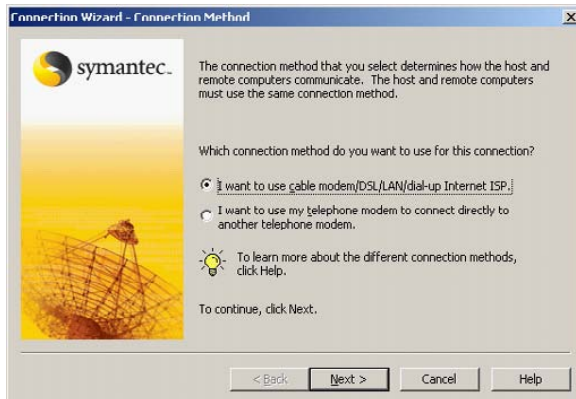


4. On the Introduction screen, click I want to connect another computer, and then click Next.



5. Select one of the following:

- I want to use cable modem/DSL/LAN/dial-up Internet ISP
- I want to use my telephone modem to connect directly to another telephone modem

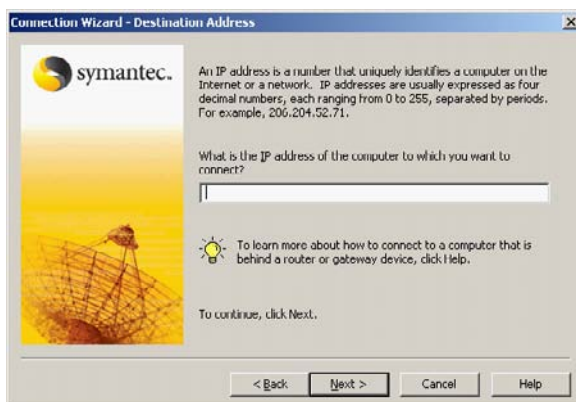


The wizard automatically detects the connection devices that are available on your computer. If your computer has multiple connection devices, choose the device that you want to use for the connection that you are configuring. For example, if the host computer uses a phone modem, you should select the phone modem as your connection device.

6. Click Next.

7. In the Destination Address panel, do one of the following:

- Type the IP address of the computer to which you want to connect.  
This option is available for cable modem/DSL/LAN/dial-up Internet ISP connections only. If the host computer is on a private network, use the IP address of the router. The host's administrator must configure the router to allow the connection.
- Type the phone number of the computer to which you want to connect.  
This option is available for phone modem connections only.



8. Click Next.

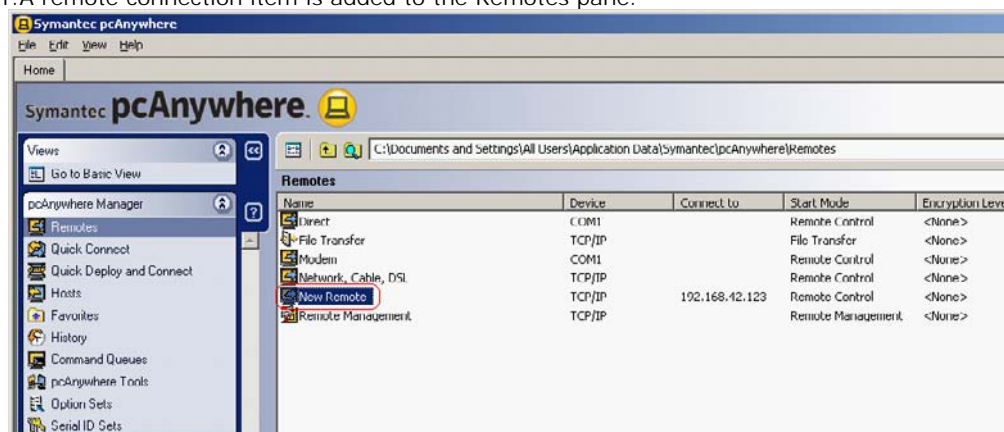


9. On the Summary screen, verify the settings. To start the remote session upon closing the wizard, check **Connect to a host computer after the Connection Wizard finishes.**



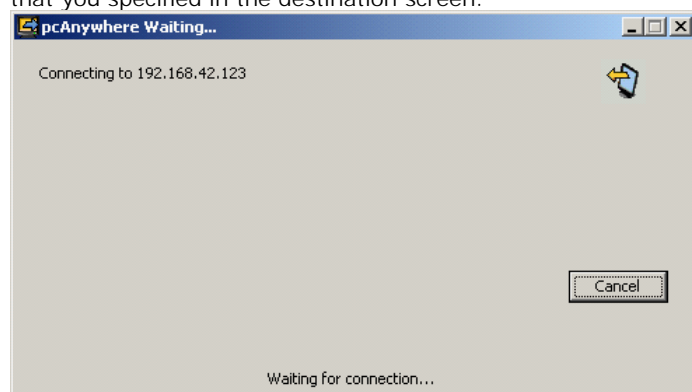
10. Click **Finish**.

11. A remote connection item is added to the Remotes pane.



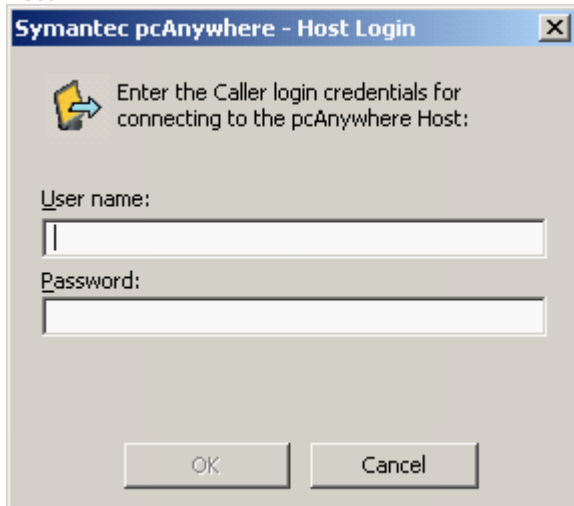
12. To name the connection item, in the Symantec pcAnywhere window, in the Remotes pane, type the name that you want to give the remote connection item and then press **Enter**.

If you selected to connect to the host computer pcAnywhere attempts to connect to the IP Address or telephone number that you specified in the destination screen.





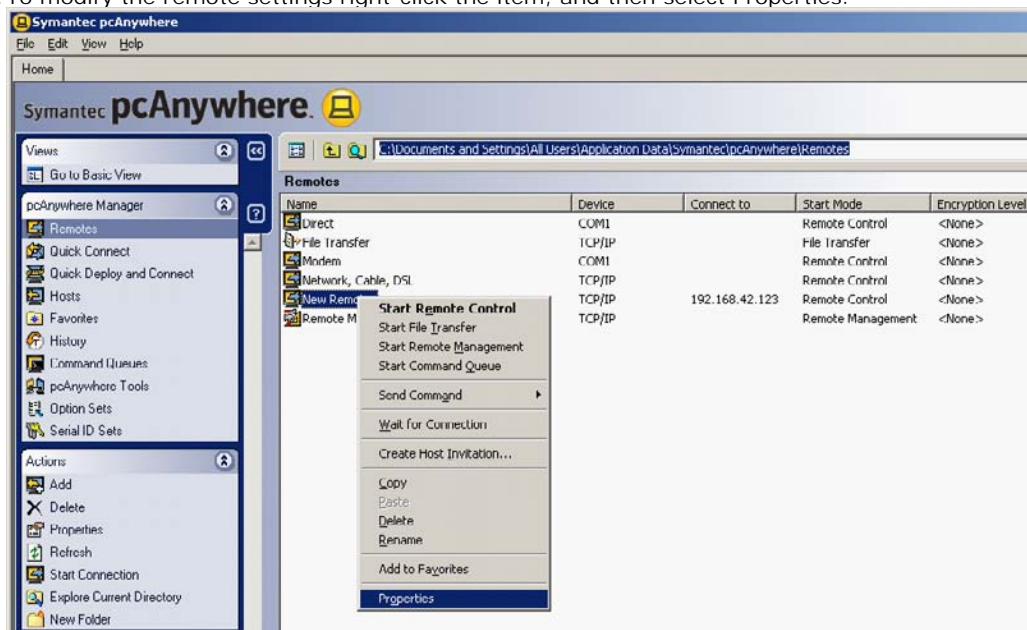
If your computer is on a network and you did not specify the host computer's IP address, pcAnywhere searches your subnet for available hosts. You can select a host computer from the list. If the host computer can be contacted successfully then the Host Login window should appear. After you have successfully logged on you can take control of the Host.



## 6.5 Configuring Advanced Remote Properties

If any of the advanced properties were setup on the host then these settings need to be configured before the remote PC can successfully connect to the host PC. Advanced properties provide access to all available remote configuration options. This includes options that are not available in the Connection Wizard, such as directory services and public-key encryption.

1. To modify the remote settings right-click the item, and then select Properties.





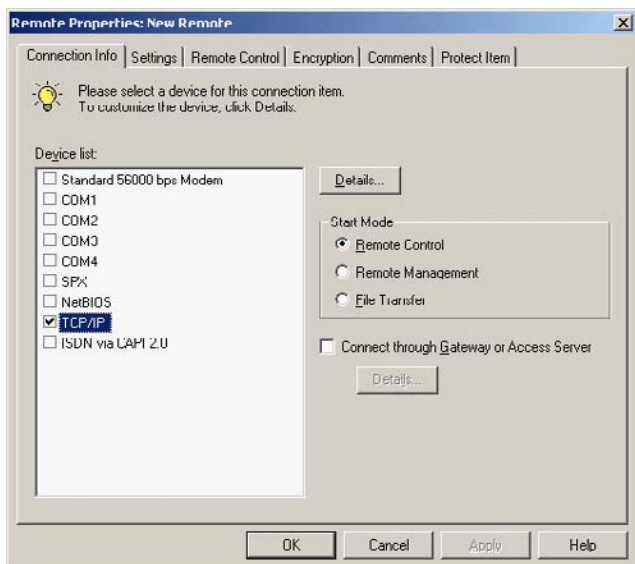
---

## 6.5.1 Connection Info

A connection device is the interface that handles the communication between the host and remote computers. A connection device might be a modem or ISDN, a network protocol, or a port. The connection device that you choose depends on the host and remote environments. Both computers must use the same type of connection device to connect.

When you are configuring a remote connection you can select the start mode that you want to use for the connection. The options available are:

- **Remote Control**  
Lets you control a host computer remotely and work as though you are sitting in front of it. During a remote control session, video and data are transferred between the host computer and the remote computer. The host computer handles all of the processing of the requests that are sent by the remote. Only the input and output information (for example, keyboard, mouse, and video information) are transferred between the computers. Because only minimal data needs to be transferred between each computer, remote control results in faster performance than other forms of remote networking and minimizes the risk of losing data.
- **Remote Management**  
Lets you remotely administer a host computer using common administrator tools (such as the Task Manager, Command Prompt, and Registry Editor). Remote management mode lets you quickly troubleshoot and resolve problems on a host computer without the overhead of a full remote control session. A remote management session uses less bandwidth than a full remote control session because only the data needs to be transferred between the host and remote computers.
- **File Transfer**  
Lets you transfer files between a host and remote computer using a two-pane window that functions like Windows Explorer. You can navigate to the files and folders that you need, transfer files and folders to and from another computer, and synchronize content. Files transfer in the background so that you can continue to work or queue other files. A file transfer session uses less bandwidth than a full remote control session because only the data needs to be transmitted between the host and remote computers.

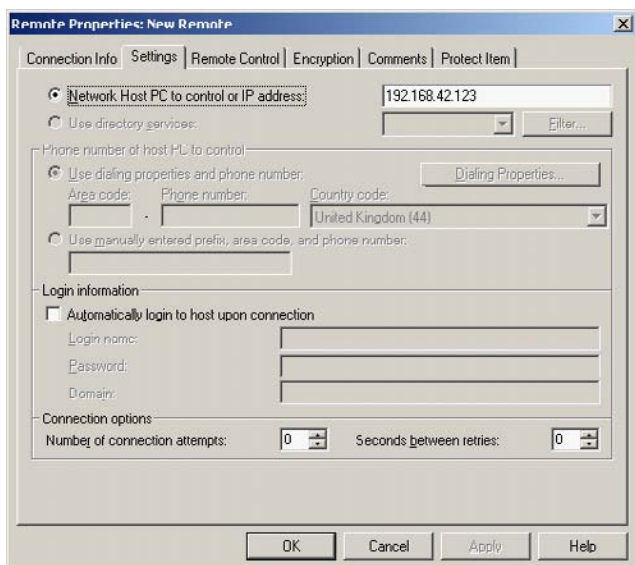


You can also configure a remote connection to automatically connect through a pcAnywhere Gateway or Access Server if your remote access environment includes these tools.

## 6.5.2 Settings

The options on the Settings tab let you configure the information that is needed to connect to the host computer. The options that are available depend on the connection device that you select.

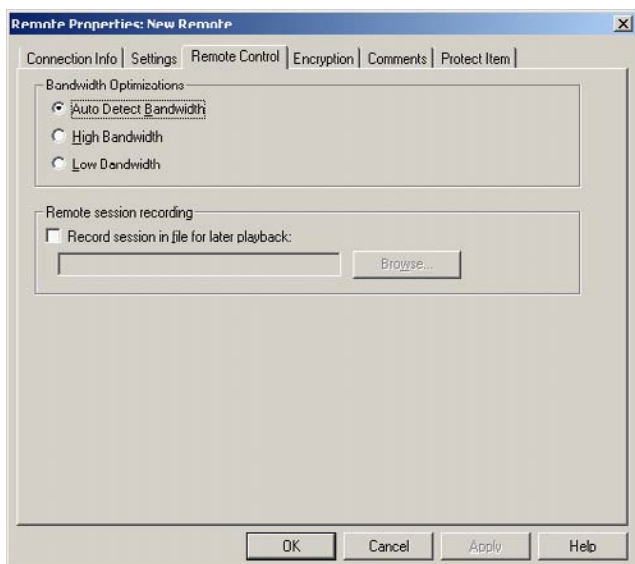
You can optionally configure the remote connection to automatically login to the host computer so that you are not prompted to enter the login name and password each time that you connect.



## 6.5.3 Remote Control

Symantec pcAnywhere automatically detects the connection speed when you make a connection, unless you change this setting, and automatically applies performance settings based on the connection type. High bandwidth is used for high-speed connections, such as LANs and cable modems. Symantec pcAnywhere optimizes video resolution and speed for high bandwidth connections. Low bandwidth is used for low-speed connections, such as analog modems. Symantec pcAnywhere uses a lower video resolution for low bandwidth connections to optimize speed.

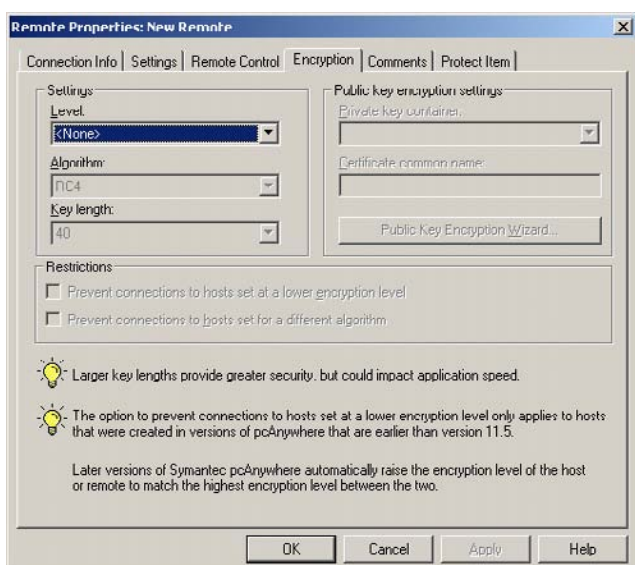
It is also possible to record a session, which can be played back at a later time. Recorded sessions are saved as .rcd files in the pcAnywhere data directory unless you specify another file location. Sessions are played back in a replay window, which shows the host screen and each action that you performed during the recording.



---

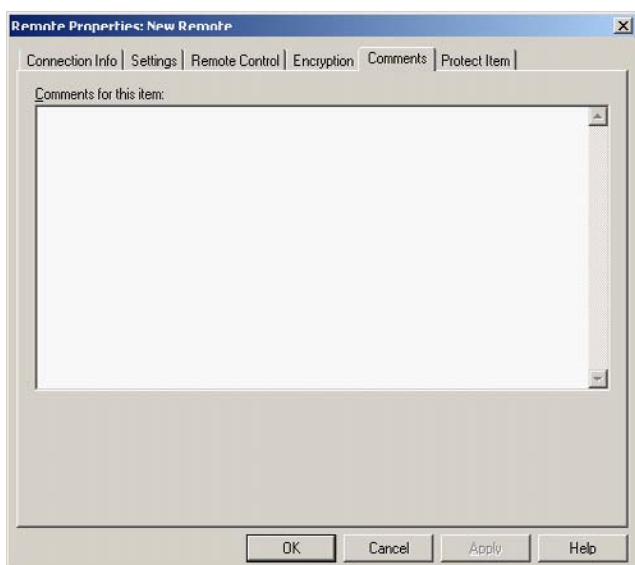
## 6.5.4 Encryption

Symantec pcAnywhere lets you protect the data stream between the host and remote computer by using encryption. If encryption has been setup on the host computer then the settings on the remote computer must be setup in the same way.



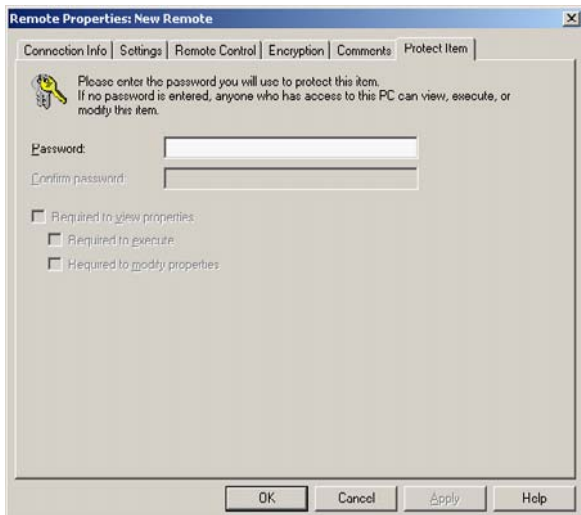
## 6.5.5 Comments

The Comments tab is used to record any details or information that is relevant to this connection.



## 6.5.6 Protect Item

To protect the remote configuration settings you can set a password in the Protect Item tab. By setting a password you can stop remote users from viewing or modifying the remote settings unless they know the password.



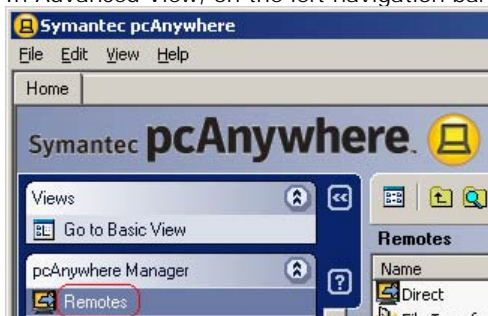
## 6.6 Changing The Default Port Numbers On The Remote

Symantec pcAnywhere uses ports 5631 and 5632 for connections. These ports are registered, and in most cases, you do not need to change them. Symantec pcAnywhere uses the data port for data transmissions. It uses the status port to wait for connections and to exchange status information.

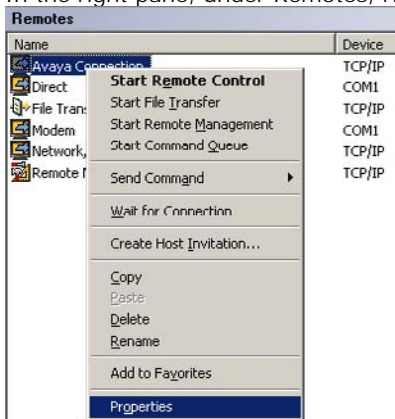
If you want to connect to a host computer that uses custom port numbers, you must change the port settings in your remote connection item to match.

To change the default port numbers on the remote:

1. In Advanced View, on the left navigation bar, under pcAnywhere Manager, click Remotes.

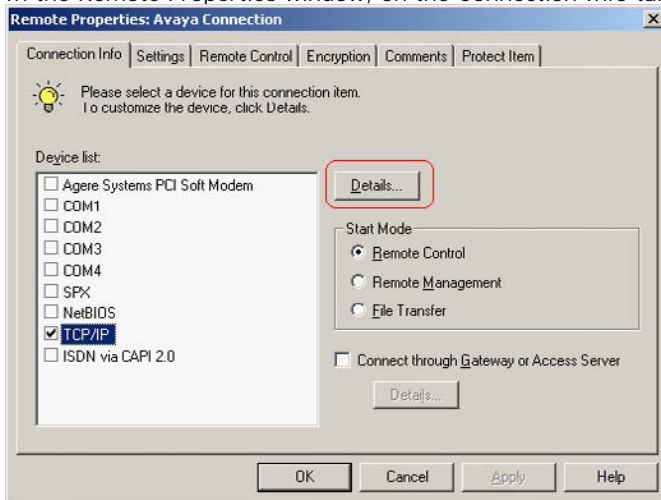


2. In the right pane, under Remotes, right-click the connection item that you want to configure, and then click Properties.





3. In the Remote Properties window, on the Connection Info tab, check TCP/IP and then click on Details.



4. In the TCP/IP window, under Specify ports to match host settings, change the ports numbers to the same number used by the host PC.



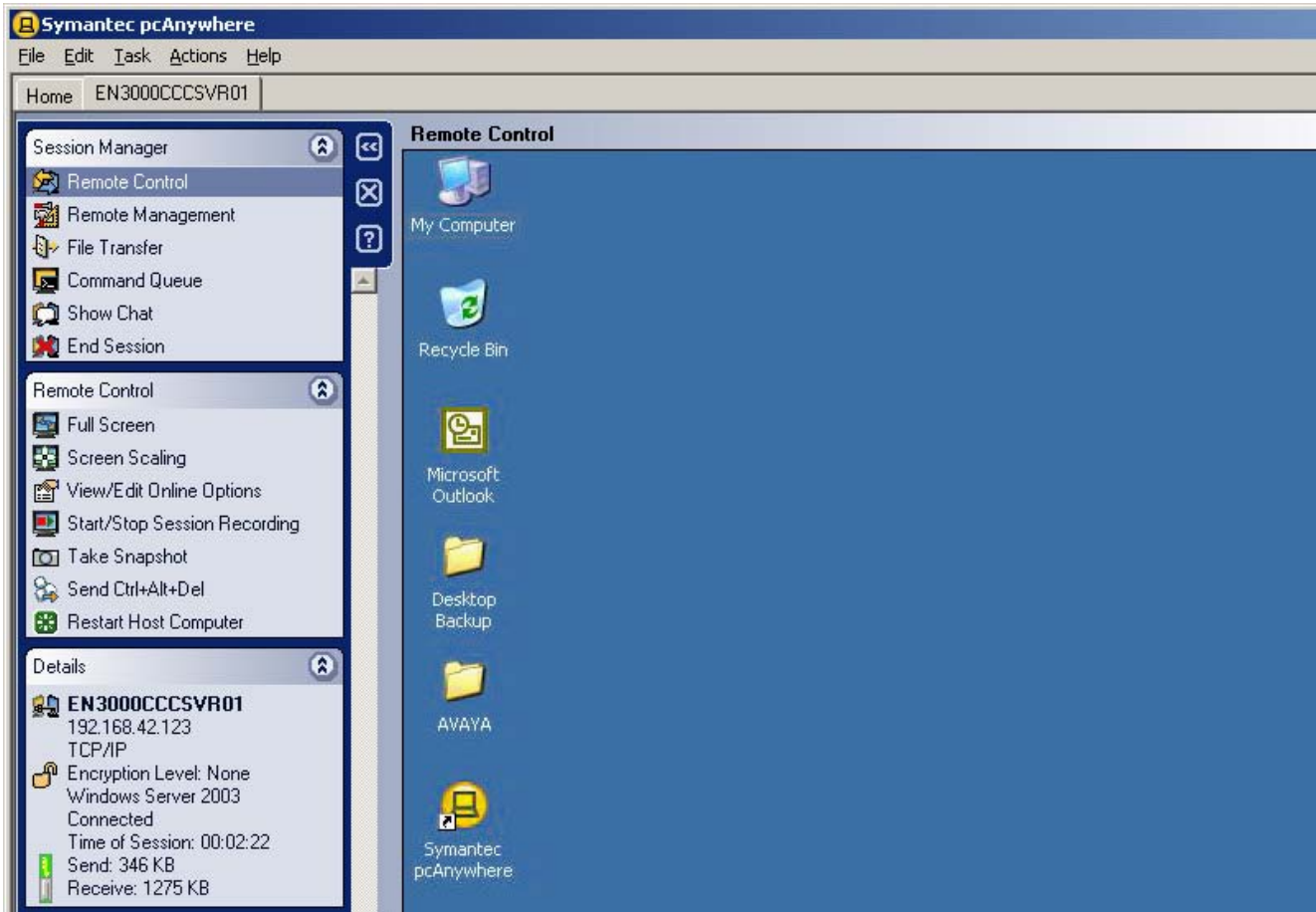


# **Chapter 7.**

## **Remote Capabilities**

## 7. Remote Capabilities

Once you establish a connection, the Session Manager window appears on your computer. The navigation bar on the left of the window lets you switch modes, perform tasks that are related to the mode that you have selected, and view details about the connection. The right pane displays the host computer screen. The arrow buttons let you expand and collapse the navigation bar.



---

Session Manager Options

- **Remote Control**  
Lets you control a host computer remotely and work as though you are sitting in front of it. During a remote control session, video and data are transferred between the host computer and the remote computer. The host computer handles all of the processing of the requests that are sent by the remote. Only the input and output information (for example, keyboard, mouse, and video information) are transferred between the computers. Because only minimal data needs to be transferred between each computer, remote control results in faster performance than other forms of remote networking and minimizes the risk of losing data.
- **Remote Management**  
Lets you remotely administer a host computer using common administrator tools (such as the Task Manager, Command Prompt, and Registry Editor). Remote management mode lets you quickly troubleshoot and resolve problems on a host computer without the overhead of a full remote control session. A remote management session uses less bandwidth than a full remote control session because only the data needs to be transferred between the host and remote computers.
- **File Transfer**  
Lets you transfer files between a host and remote computer using a two-pane window that functions like Windows Explorer. You can navigate to the files and folders that you need, transfer files and folders to and from another computer, and synchronize content. Files transfer in the background so that you can continue to work or queue other files. A file transfer session uses less bandwidth than a full remote control session because only the data needs to be transmitted between the host and remote computers.
- **Command Queue**  
The Command Queue lets you view file transfer operations that are in progress, modify pending operations, and set up command queue files to automate tasks. File transfer send, receive, and synchronize commands that are performed in the File Transfer window are automatically added to the Command Queue and run in the background. Symantec pcAnywhere lets you save these commands in a queue file (.cqf) to use later, or you can create your own command queue file. For example a command queue file could be used to distribute and install software updates on one or more computers.
- **Show Chat**  
During a remote control session, the host and remote users can have a typed conversation in a chat window. Either the host or remote user can initiate a chat session. This feature is helpful for sending brief messages or instructions.



# **Chapter 8.**

## **Alternative Remote Access Solutions**

---

## 8. Alternative Remote Access Solutions

Symantec pcAnywhere is just one of a number of remote access packages available today. The following section gives an overview of some alternative solutions that can also be used to remotely manage IP Office and its associated applications.

### 8.1 BeAnywhere

BeAnywhere is a software application that, when installed on the server (host PC), allows remote connectivity from a viewer (remote PC) with a web browser and an internet connection.

BeAnywhere delivers the following features:

- Remote Control - BeAnywhere allows you to access your remote computer just as if you were sitting directly in front of it. BeAnywhere gives you a fast, easy, secure and affordable solution to access your computer from anywhere in the world. Access your email, applications and files with only a computer and an internet connection.
- Transfer Files - Securely share files, send and receive complete files or folders and control the priority of the ongoing transfers. You can also restrict the access to a specific folder, upload only, download only, etc.
- File Share - BeAnywhere allows you to securely share files that are too large for email by sending a link to the file instead of having to attach the file to the email. File Share generates a secure link that the recipient uses to download a file directly from your computer. You can control how long the file will be available, to whom and how many times it can be downloaded.
- Sync Files - Synchronize and update files between host and remote computers.
- Always On - As long as your computer is turned on and connected to the internet, BeAnywhere will give you access from wherever you are in the world. BeAnywhere runs in NT service mode in the background.
- Security Architecture - All communications between the server (host PC) and viewer (viewer PC) use a digital signature and are encrypted with an RC4 compatible algorithm with a 2048 bit key to protect the privacy of all information exchanged between computers during a remote session.
- Authentication - Made through a user/password combination known only to the user and is never kept in a database on a central server.
- Universal Networking - BeAnywhere gives you Zero Configuration. This means that you don't need to worry about firewalls, routers, NAT traversal, port configurations, etc.

Further information about BeAnywhere can be found at the following location:

<https://secure.beanywhere.com/en/default.asp>.

### 8.2 eBLVD

eBLVD Remote Desktop is an Internet-based solution that allows access to a remote PC from any computer that has a web browser and public Internet access. eBLVD is not a free service but is easy to set up, easy to use and offers secure and reliable access. Users pay a flat monthly fee for real-time and secure firewall friendly access between computers.

eBLVD delivers the following features:

- Remote Access - Access your PC and all applications from any web browser in real time.
- File Transfer - Copy files back and forth between computers.
- Text Chat - Integrated text chat provides instant communication without the need for a telephone call.
- Session Recording - Save your remote session to a video file for later review.
- Remote Deployment - The corporate-level packages include user management and the ability to deploy the software to remote machines, with no restart required.
- Firewall Friendly - The remote desktop applet works with both hardware and software firewalls. No configuration is required.
- Low Bandwidth Requirement - Connect and work over any speed internet connection - even a modem.
- No Software to Maintain - Remote Desktop is a self-maintaining service, with no additional infrastructure or IT resources required. All software is deployed from within the web browser.
- Secure Access - All data is transferred using 128-bit Secure Sockets Layer (SSL) security. Dual-password protection provides additional security.
- Guest Access - Create an auxiliary account to temporarily allow others access to a PC.
- Free Updates - All software updates are always included free of charge.

Further information about eBLVD can be found at the following location: <http://www.eblvd.com/rdooverview.aspx>.



## 8.3 GoToMyPc Corporate

Citrix GoToMyPC Corporate comes with a variety of end-user and administrator features to make it easy and secure to fully access and control your PCs from anywhere. Citrix GoToMyPC Corporate provides powerful built-in security. Its robust and encompassing security model does not require end-user configuration. An SSL-encrypted Web site and 128-bit Advanced Encryption Standard (AES) encryption ensure the privacy of all remote connections.

Administrators have complete control over the use of GoToMyPC Corporate in their organizations and can tailor GoToMyPC Corporate to meet existing corporate security policies. The centralized Administration Center also supports real-time monitoring, password management, end-point management and two-factor authentication.

GoToMyPC Corporate delivers the following features:

- Automatic 2-Minute Setup - Automatically installs and configures itself. No restart required.
- Drag-and-Drop File Transfer - Transfer files and folders from one PC to another by simply dragging and dropping between viewer and host.
- File Sync - Easily synchronize files and folders between host PC and client computer.
- Remote Printing - Print documents from a host PC to local printer - no driver installation or setup needed.
- Guest Invite - Invite a guest to temporarily view a host PC for on-the-fly collaboration or sales demos- includes integrated chat and drawing tools.
- Fast Performance - Connect to a host PC in seconds and enjoy fast in-session performance.
- AES (Advanced Encryption Standard) - 128-bit keys automatically protect data stream; file transfers; and keyboard and mouse input.
- Authentication - Dual passwords and end-to-end user authentication.
- Log-In History - View all log-in attempts and spot any unauthorized activity.
- PocketView - Securely access a host PC from any Pocket PC, Windows® Mobile or Windows CE wireless device.

Further information about GoToMyPC Corporate can be found at the following location: <http://www.gotomypc.com/corp>

## 8.4 Laplink Everywhere

Laplink Everywhere is a software application that enables remote access and control of a remote PC from any web-enabled device with Internet access. All that is required to initiate a remote session is installing the Laplink Everywhere software application on the PC that will be accessed remotely (the host PC).

Laplink Everywhere delivers the following features:

- Firewall Connect Technology - Secure connection through corporate firewalls provides complete access to all files, applications, and resources on the remote PC during remote access session.
- Microsoft Remote Desktop Protocol – Native integration of Microsoft's Remote Desktop Protocol to extend Remote Desktop allows remote control over the Internet and through firewalls.
- Local Printing Control – Download remote documents to the local machine to print hard copies immediately.
- Remote Desktop Search – Search, manipulate or forward remote files, read email or surf Internet Favorites from any web-enabled device with an Internet connection.
- File Transfer – Send files of any size or type securely using Laplink's patented SpeedSynch technology.
- Handheld Compatibility – Remote access with user-friendly interface from any Pocket PC, Palm, Windows Mobile or Symbian-based device.
- No Plug-Ins Required – Remote PC access from a computer that doesn't allow remote control clients to be installed.
- Auto-Synch – Data downloaded while online can be modified offline and auto-synched during next online session.
- 128-bit SSL Encryption
- Zero-Footprint Technology – Erases all traces of remote access session once logged out.
- User Authentication – Prevents unauthorized users from accessing remote data.
- Customizable Guest Access – Allows limitation of remote drives or folders that guests can access on remote PC.

Further information about Laplink Everywhere can be found at the following location: <http://www.laplink.com/ile>.

---

## 8.5 LogMeIn Pro

LogMeIn Pro enables you to access PCs securely over the web from anywhere with an Internet connection - at home, on the road, at customer sites or on vacation. Work as though you were right in front of your computer.

The only computer that requires the LogMeIn application is the host computer that will be controlled (the PC at the customer site). The remote PC that will be used to access the customer site does not require LogMeIn to be installed.

Some configuration may be required to make LogMeIn Pro work with certain firewalls. Similarly, configuration of proxy settings may be required.

LogMeIn delivers the following features:

- Remote Control - Instant access to your remote PC from anywhere with an internet connection.
- Drag & Drop - Seamlessly drag and drop files and folders between connected PCs.
- File Transfer - Move files quickly between PCs.
- Remote Printing - Automatically print files from your remote PC to your local printer.
- Mini Meeting - Invite a colleague to your PC for an online meeting; view only or full control.
- Sharing - Share files with others, even those too large for email.
- File Sync - Synchronize files and folders on both PCs in seconds.
- Security - 256-bit SSL encryption anchors powerful security.
- P2P Performance - Directly communicate with remote computers via patent pending point-to-point connection for optimum speed and performance.

Further information about LogMeIn Pro can be found at the following location: <https://secure.logmein.com/products/pro>.

## 8.6 Microsoft Remote Desktop Connection

Microsoft Remote Desktop enables you to connect to a computer across the Internet from any computer, Pocket PC, or Smartphone with Internet access and a web browser. Once connected, Remote Desktop gives you mouse and keyboard control over your computer including access to files, applications, and e-mail.

The Remote Desktop Connection software communicates over a TCP/IP network connection using RDP 5.2. This protocol is based on the International Telecommunications Union's (ITU) T.120 protocol, an international, standard, multi-channel protocol used first in Microsoft NetMeeting® conferencing software. It is tuned for high and low bandwidth environments and also supports three levels of encryption.

Microsoft Remote Desktop delivers the following features:

- Remote control - Computer support staff can view and control a Terminal Services session. Sharing input and display graphics between two Terminal Services sessions gives a support person the ability to diagnose and resolve problems remotely.
- Encryption - RDP uses RSA Security's RC4 cipher, a stream cipher designed to efficiently encrypt small amounts of data. RC4 is designed for secure communications over networks. Beginning with Windows 2000, administrators can choose to encrypt data by using a 56- or 128-bit key.
- Bandwidth reduction features - RDP supports various mechanisms to reduce the amount of data transmitted over a network connection. Mechanisms include data compression, persistent caching of bitmaps, and caching of glyphs and fragments in RAM. The persistent bitmap cache can provide a substantial improvement in performance over low-bandwidth connections, especially when running applications that make extensive use of large bitmaps.
- Roaming disconnect - A user can manually disconnect from a Terminal Services session without logging off. The user is automatically reconnected to their disconnected session when he or she logs back onto the system, either from the same device or a different device. When a user's session is unexpectedly terminated by a network or client failure, the user is disconnected but not logged off.
- Clipboard mapping - Users can delete, copy, and paste text and graphics between applications running on the local computer and those running in a Terminal Services session, and between sessions.
- Print redirection - Applications running within a Terminal Services session can print to a printer attached to the client device.

Further information about Microsoft Remote Desktop Connection can be found at the following location: <http://www.microsoft.com>.

## 8.7 PROXY/Enterprise

PROXY/Enterprise from PROXY Networks, allows your helpdesk administrators to deliver remote support to customers. Combined with enterprise management and monitoring tools, PROXY/Enterprise gives you total control of remote management in your networks. PROXY/Enterprise ensures real-time access to remote machines by creating and maintaining a persistent network of secure remote control connections within your network. Any remote machine is available when you need it.

PROXY/Enterprise enables helpdesk personnel to reach remote machines anywhere, even if they are behind another firewall or even a NAT. You never have to worry about finding IP addresses or opening ports in firewalls. PROXY/Enterprise combines state-of-the-art encryption (256-bit AES) with FIPS-compliant SSL for the most secure remote control connections available today.

PROXY/Enterprise delivers the following features:

- Firewall friendliness - Access remote machines behind out-of-organization firewalls, eliminating potential challenges finding Hosts behind NAT devices
- Centralized administration - Access Hosts with one click, Simplify the discovery and connection to multiple Hosts from anywhere, regardless of location or network configuration. Maintain connection to multiple Hosts simultaneously
- Real-time dashboard - Obtain a quick view of all open access sessions in your environment at any time
- OpenSSL - Connect with confidence via SSL transport to ensure the highest standards of end-to-end communications security and integrity
- Strong encryption - AES 256-bit encryption ensures your remote control activity is secure and unauthorized leaking of data is minimized
- Many-to-one simultaneous connections - Support online collaboration and training, Use your Proxy remote control network for employee, partner or customer training.
- Remote administration - Connect to unattended machines, Remotely configure all settings, including access rights and security policies via the Gateway Administrator
- Reporting & logging - Investigate all remote control activity and access requests via Proxy logs for auditing, archiving and accountability.
- Screen recording & playback - Capture all activity on remote computer screen with High Fidelity screen recording. Record simultaneous remote control sessions with no impact on bandwidth consumption.

Further information about PROXY/Enterprise can be found at the following location:

<http://www.proxynetworks.com/products/enterprise/index.html>.

---

## 8.8 Radmin

Radmin (Remote Administrator) is a fast and secure remote control and remote access software that enables you to work on a remote computer as if you were sitting right in front of it and access it from multiple places.

Radmin delivers the following features:

- Radmin Server 3.2 supports Windows Vista/XP/2008/2003/2000 (32-bit) and Windows Vista/XP/2008/2003 (64-bit) operating systems. Radmin Viewer 3.2 supports Windows Vista/XP/2008/2003/2000/ME/98/95/NT4.0 (32-bit) and Windows Vista/XP/2008/2003 (64-bit) operating systems.
- File Transfer - You can securely drag and drop any files via Radmin's Explorer-like interface to or from a remote computer in encrypted mode. Radmin has a feature it uses when copying files that allows updating of only that part of a file which is different on both machines. This feature is called "Delta Copy" since only the difference between files ('delta') is copied. It lets you continue copying after a network fault from the place where the fault occurred rather than from the beginning. This feature is used automatically when any file is being copied to or from the remote machine.
- Multi-user text and voice chats - Text Chat, Voice Chat and Send Message modes, help communicate with a person who operates a remote computer that you are connecting to.
- Windows Security or Kerberos Authentication - Radmin can use either Windows security with Active Directory and Kerberos support or its own security with individual user permissions and secure login/password authentications. Radmin security uses Diffie-Hellman based key exchange with 2048-bit key size. Additional IP filters restrict access to specific hosts and networks.
- 256-bit AES Encryption (for all data streams) – All data, screen images, mouse movement, and keyboard signals are encrypted.
- Multiple Monitors Support - Radmin supports simultaneous multiple connections to the same remote screen. This means that you can invite multiple users to view a screen remotely or you can view or control several remote screens from your own computer's screen.
- Unique DirectScreenTransfer Technology – Radmin uses a video hook kernel mode driver to boost the capture rate to hundreds of screen updates per second, while using a special low-bandwidth optimization.

Further information about Radmin can be found at the following location: <http://www.radmin.com>.

## 8.9 Remote Desktop Control

Remote Desktop Control allows the user to remotely control any computer, running under the Microsoft Windows system in a TCP/IP local area network or the Internet. The user can see a remote desktop on his or her own screen and use the mouse and keyboard to control the connected computer remotely. Software needs to be installed on the host and remote computers.

Remote Desktop Control delivers the following features:

- Supports multiple connections at the same time.
- Different work modes: "view only" and "full control".
- Different display modes: "windowed", "full screen", and "scaled".
- File transfer between local and remote computers
- Remote power management (remote shutdown, reboot, logoff, etc.)
- Strong connection security. The software uses strong and industrially trusted program-defense algorithms, such as RSA320, GOST256, MD5, and others.
- Runs as a service on the NT systems.
- Works through the firewalls and supports DHCP.
- Online Gateway edition of Remote Desktop Control software lets you connect with a remote PC via the Internet when the remote computer has no external IP address.
- Low network load, due to optimized data compression algorithms.
- Supports high screen resolutions and color depths.
- Uses a log file to log the events and solve connection problems.
- User-friendly and intuitive graphic interface.

Further information about Remote Desktop Control can be found at the following location:  
<http://www.remote-desktop-control.com>.

## 8.10 RemotePC

RemotePC allows you to securely access your Internet enabled computer, from any location, within seconds. For this, the 'viewer' application must be installed on the local computer, while the remote computer should be enabled with the 'host' application. You can also connect to your remote computer using a web browser.

To ensure utmost security of data, communication between the remote host and the local viewer computer is encrypted using 128-bit RC4/SSL.

RemotePC delivers the following features:

- Fast Logins - Logins are quick, secure and rarely take more than 5 seconds. No lengthy applet downloads via browser each time you login.
- Remote Access through web browser - You can connect to your remote computer using a web browser. Log on to your RemotePC account from the RemotePC website. You will see a list of all the available hosts (remote computers) in your account. Select the host you wish to access and enter the Host Key to access it.
- Utmost data security as all communication between the computers of the technical support personnel and the customer is encrypted using 128-bit RC4/SSL.
- Invite a Guest - This feature lets you invite an associate to temporarily access your computer from a remote location.
- Firewalls and Proxy Servers - Works behind most firewalls and proxy servers.
- No IP Address - Host computer does not require a static IP address.
- Remote Printing - Ability to print directly from your remote host computer to a printer connected to your local viewer computer.
- Easy File Transfers - Easy transfer of data between host and viewer computers. Even allows for access and transfer of contents from a mapped network drive. Also supports a two-way clipboard that makes it easy to copy and paste information quickly.
- PC Maintenance - Reboot the customer's computer and automatically reconnect to continue with the support session.
- Reporting - Detailed reports/history of all your remote support sessions.
- Remote Printing - Print from customer's computer to a printer available at the support end (Available with Windows XP, 2000, Windows Server 2003).

Further information about RemotePC can be found at the following location: <http://www.remotepc.com>.

## 8.11 VNC Personal Edition

VNC stands for Virtual Network Computing. It is remote control software which allows you to view and fully interact with one computer desktop (the "VNC server") using a simple program (the "VNC viewer") on another computer desktop anywhere on the Internet.

VNC is in widespread active use by many millions throughout industry, academia and privately. There are several versions to choose from, including a free version and some substantially enhanced commercial versions.

VNC Personal Edition delivers the following features:

- Integrated Session Security - Integrated Session Security provides protection from connection snooping, man-in-the-middle attacks and packet-tampering attacks, to name but a few.
- One-Port HTTP & VNC - One-Port HTTP & VNC allows VNC Server to serve VNC Viewer for Java and VNC sessions through a single TCP port, simplifying NAT and firewall configuration.
- HTTP Proxy Support - HTTP Proxy Support allows you to configure VNC Viewer to connect through various web proxies and filters, making it as simple to use as a web browser.
- Desktop Scaling - Desktop Scaling to a particular size, by a particular ratio, or dynamically to whatever size you choose.
- Windows Firewall Integration - Windows Firewall Integration, making VNC Server more straightforward to deploy.
- File Transfer - File Transfer allows you to copy files between your server and viewer computers over the VNC connection—no need for additional configuration.
- Integrated Address Book - An Integrated Address Book makes it simple to store shortcuts to VNC Servers conveniently and securely.
- Chat - Chat allows text-based communication between server and viewer to simplify collaboration or remote support.

---

Further information about VNC Personal Edition can be found at the following location:  
<http://www.realvnc.com/products/personal/index.html>.

## 8.12 WebEx PCNow

WebEx PCNow is an Internet-based solution that allows access to a host PC from any remote computer or mobile phone with a web browser and public Internet access. The WebEx PCNow service requires a flat monthly and provides reliability access.

Webex PCNow delivers the following features:

- Unlimited remote desktop control – Access data, email, and files on the host PC anytime, from anywhere. There is no software to install on the remote PC or mobile phone.
- Fast and easy setup – Setup is automated and takes a few minutes. Any computer or mobile device that can browse the web can easily set up and use PCNow.
- Total security – Several levels of authentication can be set up when accessing the host PC, including phone authentication, 128 bit SSL encryption, firewall friendly through ports 80 and 443, inactivity timeouts that terminate sessions after specified period of time, and special application level access control allows access only to selected applications to prevent remote access to critical system applications.
- Guest screen sharing – Allows you to invite a second viewer to share your screen remotely and grant them access to control or view.
- Remote printing – Allows you to print any document from the remote computer to your local printer to obtain a hard copy immediately.
- File sync and transfer – Allows you to synchronize files and folders between PCs or simply transfer files from one computer to another.
- Remote sound – Allows you to hear system sounds (such as alerts) from the remote PC to be played on your local PC.
- Multi-monitor support – Allows you to view multiple monitors at the remote location.

Further information about Webex PCNow can be found at the following location: <http://pcnow.webex.com>.

# Chapter 9.

## Summary

---

## 9. Summary

Remote access gives you the ability to access a remote computer from a distant location. It provides much more than just a connection to a remote computer, it allows you to take control and administer the computer as if you were sitting in front of it.

For Business Partners and support organizations remote access allows trouble shooting, programming changes and upgrades to take place without ever needing to dispatch an engineer to the customer site unless absolutely necessary. Not only can this provide a quicker and more efficient service to the end user but it also makes your engineers more productive, reduces costs, and allows them to dedicate more of their time to looking after customers and less time on the road. In today's environmentally conscious world this is also a much greener solution.

There are many remote access software solutions available in the market today and a number of factors will influence your decision making when choosing which package is best for your organization.

Cost is just one of those factors that need to be taken into account. There are free applications, packages that have a one time charge for each deployed instance of the software, or those that have ongoing recurring costs. The free software applications do not offer the same level of functionality that a paid solution would but that doesn't necessarily make them less capable.

Security will be a major concern when looking at the best solution, there are a large number of companies who will not allow remote access due to security concerns. Surveys have shown that larger companies are more likely to allow remote access compared to smaller ones.

For these customers who have these concerns some of the web based solutions are a good option for them. These tend to make an outbound connection to a secure server which the support organization must connect to before a remote access session can be established. The customer can also limit when access is available by only running the service when needed. These solutions are also more firewall friendly, not normally requiring any reconfiguration of the customer firewall to allow their operation. Having a poorly configured firewall could leave the corporate LAN open to attack.

Another consideration as to what software and what method of connectivity is best will depend on who will require remote access and where are they based. If they are based in one or two locations then equipment and resources can be pooled at each location. However, if the support organization has a distributed or mobile work force it becomes prohibitive to provide the same equipment to everyone. An engineer may not always have access to a telephone line or a modem, but internet access is relatively easy to gain access to.

A final consideration should be given to how easy or how difficult a particular solution is to deploy and use. Some solutions need a knowledgeable person to install and configure them, some allow you to pre-build a package for ease of deployment while other solutions need little configuration or even configure themselves. With a large remote access deployment having to manage remote access software versions could also give cause for concern.

In summary there is not one solution that stands head and shoulders above another, there are a large number of solutions that will deliver the required functionality admirably. Whatever combination of cost, security, equipment requirements, ease of install and ease of use works for your organization is the best solution to use to support your customers.





Performance figures and data quoted in this document are typical, and must be specifically confirmed in writing by Avaya before they become applicable to any particular order or contract. The company reserves the right to make alterations or amendments to the detailed specifications at its discretion. The publication of information in this document does not imply freedom from patent or other protective rights of Avaya or others.

Intellectual property related to this product (including trademarks) and registered to Lucent Technologies have been transferred or licensed to Avaya.

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

This document contains proprietary information of Avaya and is not to be disclosed or used except in accordance with applicable agreements.

Any comments or suggestions regarding this document should be sent to "wgctechpubs@avaya.com".

© 2008 Avaya Inc. All rights reserved.

Avaya  
Unit 1, Sterling Court  
15 - 21 Mundells  
Welwyn Garden City  
Hertfordshire  
AL7 1LZ  
England.

Tel: +44 (0) 1707 392200  
Fax: +44 (0) 1707 376933

Web: <http://marketingtools.avaya.com/knowledgebase>