The Host PC

A pcAnywhere host PC can be accessed and remotely controlled by one or more remote users. After connecting to a host PC, the remote user can access files, folders, and applications as if they were physically working at the host PC. The host user can control access to the host PC by requiring either pcAnywhere or Windows caller authentication.

Many options that affect a remote control connection are set in a connection item at the host PC. These options allow you to:

- Determine who has control of keyboard and mouse activity during a remote control session (host, remote, or both host and remote user).
- Automatically run pcAnywhere whenever Windows starts.
- Restart the host PC after disconnecting a remote control session.
- Blank the host's screen during a session to protect activity on the host from unauthorized viewing.
- Prevent usage of the host PC during a session to prevent accidental canceling of the host.
- Restrict the number of login attempts to enhance security on the host PC.
- Use data encryption technology to enhance the security of transferred information.

Gateway Host Overview

The pcAnywhere gateway host allows network users to share a communications device, usually a modem, attached to any PC on the network. The gateway provides dial-in and dial-out services that allow network users to use the modem on the gateway PC to make connections. In addition, a gateway PC can allow a remote user to dial in to the gateway modem, then be connected to a pcAnywhere host on the network.

All gateway configuration information is included in the gateway connection item. Gateway options include:

- **Bi-directional** - allows other PCs on the network to both send and receive calls through the gateway.
- **Inactivity Timeout** - specifies the length of time the host allows for inactivity before automatically terminating the session with a remote PC.
- **Class** - places the gateway PC in a category of gateways sharing similar characteristics. For example, an administrator may create a class of gateways called "9600" for all gateway PCs using 9600 bps modems.

 Setting up a PC as a Gateway does not prevent you from using the gateway PC for other tasks.

Conference Host Overview

A conference host allows multiple users to simultaneously connect and view the host activities. For example, the host user can conduct a software training demonstration that can be viewed by any remote caller connected to the host PC.

A conference host is remotely controlled by the first remote caller to connect. All other callers can only view the activity taking place on the host PC and can use some utility functions such as saving screens and recording sessions.

The first remote caller can connect using any connection device. Other callers connecting to view the host session must make a TCP/IP network connection.

Data encryption

pcAnywhere can encrypt data using any of the following encryption methods:

Public-key: Provides the highest level of session security by using pre-defined keys distributed by a certificate authority. Public key encryption is slower than other encryption methods, but the private key (the key used to decrypt data) is not shared.

Symmetric: Uses similar session security options as public key, however, it does not use certificate authority issued certificates for authenticating callers. Symmetric encryption is fast but requires sharing the key if the encrypted data is given to others.

pcAnywhere: Provides minimum data security by using a simple transformation of data to prevent data interception by third parties. Modern encryption methods rely on a cryptographic key - typically a long string of alphanumeric characters - to determine how an encryption algorithm scrambles and unscrambles the data. A cryptographic system that uses key pairs, that is, a public key and a matching private key, is known as public key cryptography. A system that uses a single key to encrypt and decrypt data is known as symmetric cryptography.

pcAnywhere uses a combination of public key and symmetric encryption methods. By combining both techniques, pcAnywhere takes advantage of the strengths of each method:

pcAnywhere encryption

pcAnywhere data encryption applies a simple transformation to data so that the datastream cannot be easily interpreted by a third party. This is the only encryption level compatible with earlier versions of pcAnywhere.

Public-key encryption

Public-key encryption uses key pairs - a public key that encrypts data and a corresponding private key that decrypts data. A unique public key and private key are generated for each user. These key pairs, along with the user's name, is stored in a certificate issued by a certificate authority.

When one person needs to send encrypted data to another, the sender encrypts the data using the public key of the recipient. Since only the private key can decrypt data, the public key can be shared with anyone.

To decrypt the data, the recipient uses their own private key.

- Some pre-configuration is required to ensure that both the host and remote have access to the appropriate key pairs.
- When public-key encryption is selected, pcAnywhere uses public key encryption to authenticate the caller and establish a connection, then uses the faster symmetric encryption to secure the session.

 Public-key encryption requires CryptoAPI 2.0, available in Windows NT 4.0 Service Pack 3, or Microsoft Internet Explorer 4.0.

Public key components

The following components comprise the total public key encryption method:

Microsoft-compatible certificates: You may obtain personal certificates (or key pairs) from a commercial certificate authority or through an internal certificate server.

After the certificate has been installed, it appears in the private-key list box on the host and remote security options property page.

Certificate store: A certificate is a data document containing a person's name, public key, and the signature of the certificate authority that issued the certificate. A certificate store is a secure database containing one or more certificates. To locate the public key for a session, pcAnywhere searches a certificate store for the certificate belonging to the current caller.

pcAnywhere uses certificate stores in any of the following formats:

- A Microsoft-compatible certificate store.
- A standard PKCS#7 cryptographic message.
- A single encoded certificate.

The host needs access to a certificate store containing the remote's certificate, and the remote needs access to a certificate store containing the host's certificate. You must specify the filename of the certificate store in the Application Options>System Setup property page.

Certificate common name: Every host and remote caller should be configured with the common name from its own certificate. The name is provided on the Security Options property page of the host and remote connection item. When a connection is attempted, the common name for the host and the remote are verified for authenticity.

Symmetric encryption

When symmetric encryption is selected, pcAnywhere generates a unique public key and uses this key to encrypt and safely pass the symmetric key used to encrypt the session. Because the public key is not obtained from a certificate authority it does not provide the level of caller authentication that total public-key encryption does.


To enhance caller authentication when using symmetric encryption, use pcAnywhere's individual caller privileges option.

The symmetric encryption level is available on any operating system that suports the CryptoAPI, such as Windows NT 4.0. For the Windows 95 operating system, CryptoAPI 1.0 is available with OSR2 or with Microsoft Internet Explorer 3.0 and higher.

Encryption technical information

With CryptoAPI, cryptographic functions are actually performed by a Cryptographic Service Provided (CSP), or low-level cryptography driver, which functions as part of the operating system. Microsoft provides a basic CSP as part of Windows NT and Internet Explorer. This basic CSP can be replaced by third-party products.

pcAnywhere uses the default Prov_RSA_FULL CSP and the RC4 symmetric algorithm. Any CSP classed as PROV_RSA_FULL that provides RC4 can support pcAnywhere.

Many important parameters are determined by the CSP in use. For example, the basic Microsoft CSP uses 512-bit public keys and 40-bit session keys. Other CSPs use different key lengths.

Please visit the Microsoft website for more details on CryptoAPI and available CSPs.

Host Security Overview

The following list is a summary of the security features available in this version of pcAnywhere:

Options that protect host configurations

- **Protect Item**— password protects connection items to prevent unauthorized users from changing or using the connection item.
- **Lock NT Workstation**— locks a Windows NT workstation with a password to prevent unauthorized users from accessing the host PC.
- **Use Windows 95 Screen Saver**—locks a Windows 95 workstation by assigning a password to your Windows 95 screen saver to prevent unauthorized users from accessing the unattended host PC.
- **End of Session or Loss of Connection**—allows you to choose the mode to which the host PC returns after a session disconnects. You can also choose to log off the user on the host PC.
- **Blank the Host Screen**—blanks the host screen after a connection to prevent users at the host site from viewing the activities on the host PC.
- **Lock Host Keyboard/Mouse**—locks the host or remote PC's keyboard and mouse during a remote control session to prevent unauthorized users from using the PC during a session.

Options that control connections to the host PC

- **Use pcAnywhere Authentication with pcAnywhere privileges**—uses pcAnywhere caller authentication and caller privileges.
- **Use Windows authentication with pcAnywhere privileges**—uses Windows domain authentication with pcAnywhere's caller privileges.
- **Use Windows authentication and Windows privileges**—(available only in Windows NT), uses Windows Domain authentication to verify callers and Windows Security to assign caller privileges on the host PC.
- **Caller Password**—allows a host user to assign unique passwords to all callers connecting to the host PC. These passwords can be case-sensitive to enhance the security on the host.
- **Callback**—allows the host user to store a remote caller's phone number. When the caller connects and logs on to the host PC, the host disconnects the connection and calls back the remote caller at the using the phone number stored in the caller's item.
- **Prompt to Confirm Connection**—allows the host user to acknowledge the remote caller and permit connection to the host PC.
- **Limit Login Attempts**—restricts the number of times a remote caller can attempt to log in to the host PC.
- **Limit Time to Complete Login**—restricts the amount of time a remote caller has to correctly enter their login name and password.
- **Encryption**—allows the host user to choose one of three levels of data encryption to protect the integrity of data being transferred by the host PC.
- **Allow any Caller to Reconnect**—restricts a re-connection to the host PC to the caller that was signed on to the host at the time of the abnormal disconnect. This prevents unauthorized viewing of information that may have been left on the host screen during the previous session.

Security options that control remote caller privileges on the host PC

- **Individual Caller Rights**—allows the host user to specifically select the privileges a caller has on the host PC. These privileges include:
    - Blanking the host screen after connecting.

- Canceling the host, preventing other connections.
- Restarting the host PC after ending the session.
- Sending or receiving files on the host PC.
- Accessing drives on the host PC.

- **Limiting the Session**—allows a host user to control the amount of time a remote caller is connected to the host PC.
- **Subject Caller to Inactivity Timeout**—allows the host user to disconnect a user after a specified time of inactivity.

Options that monitor activities on the host PC

- **pcA Logging**—allows the host user to create a log file of session activities on the host PC. This log file can be stored locally, or can be stored to a central server.
- **SNMP**(Simple Network Management Protocol)—pcAnywhere supports this Windows component that allows a computer to be monitored remotely with third party management tools.
- **Windows NT Event Log**—captures and saves application events to a file that can be viewed and used for diagnostic and monitoring purposes.

To use callback

On the host PC:

1 Right-click the host PC connection item for the host that is going to call back a remote PC.

2 Choose Properties from the drop-down menu.

3 Click the Callers tab. You must select a caller authentication method to use callback.

4 Right-click the caller item for the remote PC you want to call back.

5 Choose Properties from the drop-down menu.

6 Click the Callback tab.

7 Check **Call back the remote user**.

8 Type the phone number of the remote PC.

{button ,PI(`',`About_Callback_')} About Callback

To wait for a call

On the host PC:

1 Click Be a Host PC on the pcAnywhere action bar.

2 Double-click the host connection item for the host you want to launch.

A host can wait for a call on more than one device. When the host answers a call on one device, the other device is not available until the first session ends.

To call a remote PC

On the host PC:

1 Click Be a Host PC on the pcAnywhere action bar.

2 Right-click the host connection item.

3 Choose Call Remote from the drop-down menu.

To cancel a waiting host

On the host PC:

- Right-click the pcAnywhere waiting icon  in the system tray and choose Cancel Host from the pcAnywhere menu.

The waiting host is canceled and the pcAnywhere main program displays.

To set host options

On the host PC:

1 Click Be A Host PC on the pcAnywhere action bar.

2 Right-click the host connection item and choose Properties from the drop-down menu.

3 Click the Settings tab.

4 Select the options this host connection item will use for remote control sessions.

To set host security options

On the host PC:

1 Click Be A Host PC on the pcAnywhere action bar.

2 Right-click the host connection item and choose Properties from the drop-down menu.

3 Click the Security Option tab.

4 Select options to protect the security of the PC when it is used as a pcAnywhere host.

{button ,JI(`',`Host_Security')} More about host security

To blank the host PC's screen for all sessions

On the host PC:

1 Right-click the host connection item and choose Properties from the drop-down menu.

2 Click the Security Options tab.

3 Check **Blank this PC Screen After Connection Made**.

To protect host drives on the host PC from access

On the host PC:

1 Right-click the host PC connection item and choose Properties from the drop-down menu.

2 Click Callers.

You must select a caller authentication method and create a caller list to use the drive protect feature of pcAnywhere.

3 Right-click the caller item for whom you want to set host drive access.

4 Choose Properties from the caller drop-down menu.

5 Click the Privileges tab.

6 Click Set Drive Access.

7 Select the drive access privileges you want this caller to have.

To create a caller item

On the host PC:

1 Click Be A Host PC on the pcAnywhere action bar.

2 Right-click the host connection item for the host to which the caller will connect.

3 Choose Properties from the drop-down menu.

4 Click the Callers tab.

5 Choose an authentication option.

6 Double-click the Add Caller icon to start the Add Caller wizard.

7 Follow the instructions on your screen and click Finish to complete the wizard.

 To change the default settings for the new caller, right-click the new caller item and choose Properties from the caller drop-down menu.

To set caller login name & password

On the host PC:

1 Click Be A Host PC on the pcAnywhere action bar.

2 Right-click the host connection item.

3 Choose Properties from the drop-down menu.

4 Click the Callers tab.

You must select a caller authentication method to use callers.

5 Right-click the caller item whose password you want to set and choose Properties from the drop-down menu.

6 Type a login name and password for this caller.

To set caller security privileges

On the host PC:

1 Click Be A Host PC on the pcAnywhere action bar.

2 Right-click the host connection item and choose Properties from the drop-down menu.

3 Click the Callers tab.

4 Right-click the caller item whose privileges you want to set.

You must select a caller authentication method to use callers.

5 Choose Properties from the caller drop-down menu.

6 Click the Privileges tab.

7 Do one:

- Check Superuser to grant this caller all rights and privileges appearing on the Advanced property page.
- Select individual rights and session privileges for this caller.

To create a Superuser

On the host PC:

1 Click Be A Host PC on the pcAnywhere action bar.

2 Right-click the host connection item and choose Properties from the drop-down menu.

3 Click the Callers tab.

4 Right-click the caller item whose privileges you want to set.

You must select a caller authentication method to use callers.

5 Choose Properties from the caller drop-down menu.

6 Click the Privileges tab and check the Superuser option.

To select a caller folder

On the host PC:

1 Click Be A Host PC on the pcAnywhere action bar.

2 Right-click the host connection item whose caller folder you want to select.

3 Choose Properties from the drop-down menu.

4 Click the Callers tab.

5 Select a caller authentication method to use.

6 Click the folder browse tool and select a folder to contain all caller items for this host.

 If the folder browse icon is not displayed in the Callers toolbar, customize pcAnywhere's toolbars to include the folder browse icon.

To select data encryption

Data encryption can be selected on both the host PC and the remote PC.

1 Right-click the host or remote connection item for which you want to select data encryption.

2 Choose Properties from the drop-down menu.

3 Click the Security Options tab.

4 Select the level of encryption to use during a session.

5 Check **Deny Lower Encryption Level** if you want to prevent connections with PCs that use a lower encryption level.

 Earlier versions of pcAnywhere support pcAnywhere encryption only. Checking the Deny Lower Encryption Level will prevent connections with PCs using pcAnywhere versions 2.0, 5.0, and 7.x.

To access the host online menu

The host online menu is only available during a connection with a remote PC.

- Right-click pcAnywhere in Session on the taskbar, and point to pcAnywhere.

  The host's online menu appears with the following options:

- **End Session** - disconnects the current session.
- **File Transfer** - starts a file transfer connection that can be controlled by either the host or remote user.
- **Chat** - brings up the Chat window on the host and remote PC, allowing the host and remote user to type a conversation. Use this option when there is only one phone line available.

To start file transfer from the host PC

During a remote control session:

1 Right-click the pcAnywhere icon  in the system tray.

2 Choose File Transfer from the host's online menu.

3 Choose one:

- **Controlled by Host** - opens the File Manager window on the host PC.
- **Controlled by Remote** - opens the File Manager window on the remote PC.

To open chat window on the host

During a remote control session:

- Right-click the pcAnywhere icon  in the system tray and choose Chat from the host's online menu.

To configure a conference host

On the host PC:

1 Click the host connection item you want to configure.

2 Do one of the following:

- Right-click the selected item and choose Properties from the drop-down menu.
- Choose Properties from the File menu.

3 Click the Conference tab.

4 Check **Enable Conferencing** to allow multiple callers to connect and view the activities on the host PC.

5 Do one of the following:

- Click Obtain IP Address Automatically to select an IP address from any valid Class D addresses.
- Click Specify IP Address to type an IP address within the range of 225.1.1.1 through 239.254.254.254.

To end a session from the host PC

1 Right-click the pcAnywhere icon  in the system tray.

2 Choose End Session from the host's online menu.

Schedule a host

You can schedule a pcAnywhere host to wait for a call at a particular time of day. The method used to schedule a host varies depending on the host PC's operating system.

- For the Windows 9x and Windows 2000 environment, use Norton Program Scheduler.
- For Windows 98 or Microsoft's IE 4.0 or higher, use Task Scheduler.
- For the Windows NT environment, use the Schedule Service (AT command) feature..

Setup a gateway

Any PC that can use two connection devices can be used as a gateway host.

To configure a gateway PC:

1 Click Be A Gateway on the pcAnywhere action bar.

2 Double-click Add Be A Gateway Item to create a gateway connection item.

To modify gateway settings:

1 Click Be A Gateway on the pcAnywhere action bar.

2 Right-click the gateway connection item and choose Properties from the drop-down menu.

3 Choose a connection device to use for incoming and outgoing calls.

4 Click the Settings tab.

5 Click Bidirectional to allow the gateway to be used for receiving and routing incoming calls as well as for dialing outgoing calls.

6 Click Inactivity timeout to set the number of minutes of inactivity allowed on the gateway host before automatically disconnecting the session.

7 Type a class name if this gateway is part of a group of gateways. For example, an administrator may create a class called "9600"' for all gateways using 9600 baud modems.

Create a bidirectional gateway

On the gateway PC:

1 Click Be A Gateway on the pcAnywhere action bar.

2 Right-click the gateway connection item and choose Properties from the drop-down menu.

3 Click the Settings tab.

4 Check Bidirectional.

5 Click the Connection Info tab.

6 Check a device in each column. (Remote PCs can "call in" to either device and reach a host PC through the other device.)

About Callback

The callback feature can be used to reverse phone charges or as an additional security measure on the host PC. After the remote caller has logged on to the host, the host disconnects the call and calls back the remote caller using the phone number listed in the caller's connection item.

Use callback only for connections made using modems as connection devices. Network or direct connections cannot use the callback feature.

If you do not type the remote PC's phone number at the host, the remote PC user is prompted to enter a phone number at the time of connection to the host PC.

 If you want to use callback when connecting to a gateway, the gateway must be configured as bi-directional.

Caller authentication

To secure the host PC from access by unauthorized callers, choose one of the three authentication methods available in pcAnywhere 9.0:

- **Use pcAnywhere Authentication with pcAnywhere privileges**—-uses pcAnywhere's caller information to verify callers and assign caller privileges.
- **Use Windows authentication with pcAnywhere privileges**—-uses Windows domain authentication to verify callers and uses pcAnywhere's caller information to assign caller privileges.
- **Use Windows authentication and Windows privileges**-(available only in Windows NT)— uses Windows Domain authentication to verify callers and Windows Security to assign caller privileges on the host PC.

 Click the Help button on the Callers property page for detailed information on authentication.

pcAnywhere caller authentication

- **Use pcAnywhere Authentication with pcAnywhere privileges**—-uses pcAnywhere's caller information to verify callers and assign caller privileges.
- **Use Windows authentication with pcAnywhere privileges**—-uses Windows domain authentication to verify callers and uses pcAnywhere's caller information to assign caller privileges.
- **Use Windows authentication and Windows privileges**-(available only in Windows NT)— uses Windows Domain authentication to verify callers and Windows Security to assign caller privileges on the host PC.