

# Installing a Secure pcAnywhere 10.5 Host on Windows

## Introduction

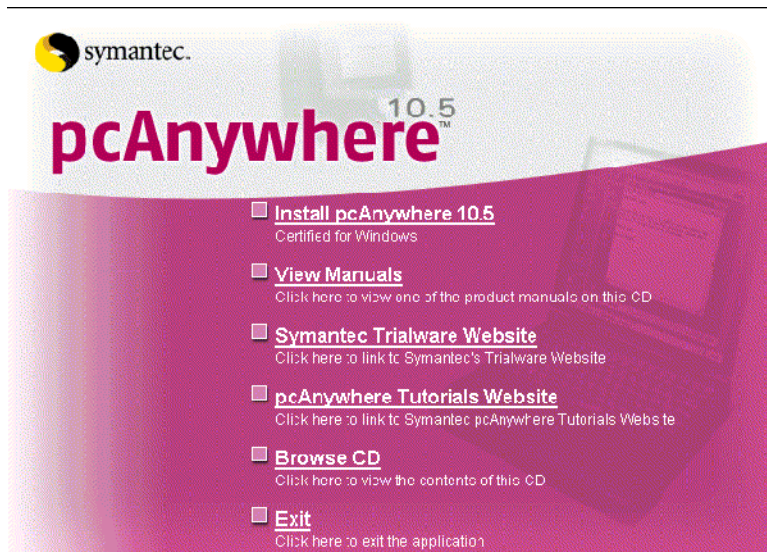
This is the procedure I used to set-up a secure pcAnywhere 10.5 host on Windows 2000 Professional. This procedure should work similarly for other versions of pcAnywhere and Windows.

The primary benefit of this procedure is that it uses **self-generated certificates** for the encryption. This means that you do not need to purchase the certificates from Verisign or another company.

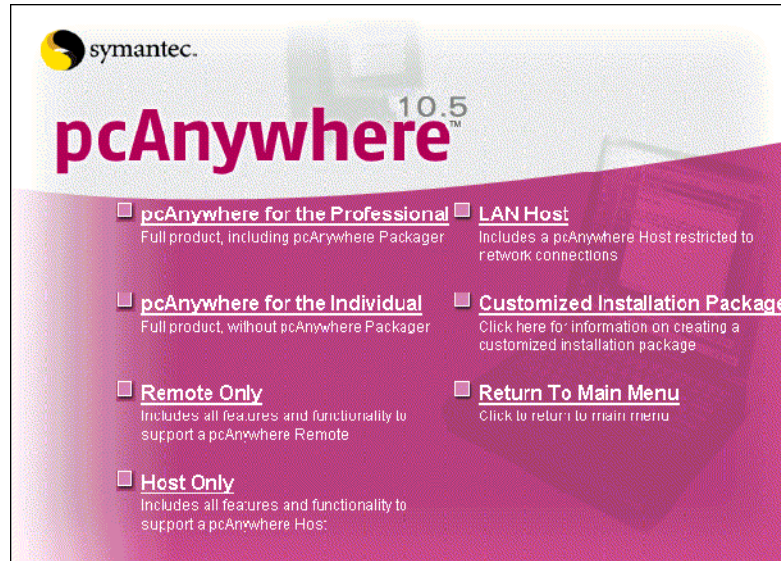
This information is provided as-is with NO WARRANTY expressed or implied. You agree to use it at your own risk. The author(s) cannot be held liable for the use or misuse of this information.

## Procedure

Insert the pcAnywhere CD into the drive. This should automatically bring up a menu that looks like this:



Select Install pcAnywhere 10.5. This will bring up a menu that looks like this:



Select LAN Host.

This will bring up a setup wizard.

Follow the instructions on the screens to install it.

Once finished, it will ask you to update the pcAnywhere software.

Allow it to run the update.

If it asks you to register the product, you can do so, or hit the Skip button.

Once the installation is finished, it will ask to restart the computer. Allow it to do so.

Once the machine reboots, you should see an icon on the desktop for Symantec pcAnywhere. It should look like this:



To use public-key encryption, we will need to generate a certificate for the host and each of the remote users.

To create the certificate for the host, login to a Linux machine that has OpenSSL installed and type these commands:

```
cd /usr/share/ssl/certs
```

```
make [TheNameOrIPofTheHost].pem For example, I used: 192_168_1_254.pem
```

Answer the following questions that will come up (I gave example answers here):

```
Country Name (2 letter code) [GB]:US
```

```
State or Province Name (full name) [Berkshire]:Texas
```

```
Locality Name (eg, city) [Newbury]:Plano
```

```
Organization Name (eg, company) [My Company Ltd]:JAMM Consulting Inc
```

```
Organizational Unit Name (eg, section) []:Web Services
```

```
Common Name (eg, your name or your server's hostname) []: [The IP address  
or name of the server, for example 192.168.1.254]
```

```
Email Address []:admin@JAMMConsulting.com
```

---

Export the public key in a pkcs#7 file (substitute the name of your certificate in both places I used it below):

```
openssl crl2pkcs7 -nocrl -certfile 192_168_1_254.pem -outform DER -out  
192_168_1_254.p7b
```

Create a pkcs#12 file to hold the private and public keys (substitute the name of your certificate in both places I used it below):

```
openssl pkcs12 -export -nodes -in 192_168_1_254.pem -out  
192_168_1_254.p12
```

This will ask you for an export password twice, hit enter without typing anything on both inputs.

For each of the remote users, generate a certificate for them:

```
make [UserName].pem (Example: NeilAggarwal.pem)
```

Answer the following questions that will come up (I gave example answers here):

```
Country Name (2 letter code) [GB]:US
```

```
State or Province Name (full name) [Berkshire]:Texas
```

```
Locality Name (eg, city) [Newbury]:Plano
```

```
Organization Name (eg, company) [My Company Ltd]:JAMM Consulting Inc
```

```
Organizational Unit Name (eg, section) []:Web Services
```

```
Common Name (eg, your name or your server's hostname) []: [The remote  
user's name, for example: Neil Aggarwal]
```

```
Email Address []:admin@JAMMConsulting.com
```

---

Export the public key in a pkcs#7 file (substitute your user's name in both places I used it below):

```
openssl crl2pkcs7 -nocrl -certfile NeilAggarwal.pem -outform DER -out  
NeilAggarwal.p7b
```

Create a pkcs#12 file for the public and private keys (substitute your user's name in both places I used it below):

```
openssl pkcs12 -export -nodes -in NeilAggarwal.pem -out  
NeilAggarwal.p12
```

This will ask you for an export password twice, hit enter without typing anything on both inputs.

On the host machine, create a folder `c:\Program Files\Symantec\pcAnywhere\Certs`

Copy the host's `.p12` file into the `Certs` directory.

Copy the `.p7b` files for each of the remote users into the `Certs` directory.

Using Windows Explorer, navigate to the `Certs` directory.

Double-click on the `.p12` file you generated for the host machine.

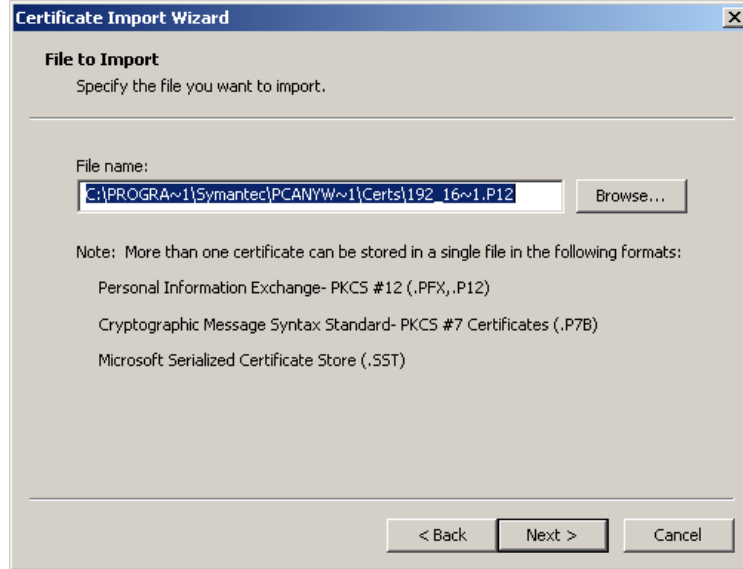
This will start the Certificate Import Wizard.

You should first encounter the Welcome panel for the wizard. It should look like this:



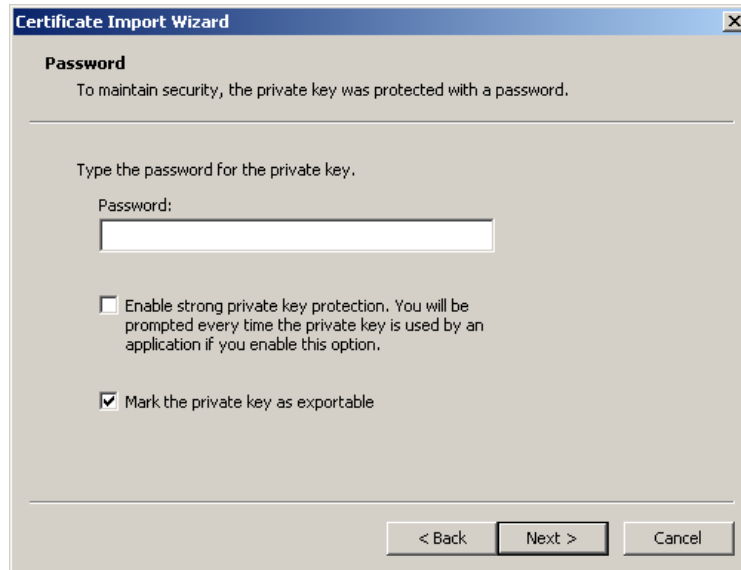
Hit the `Next` button.

This will bring you to a panel asking for the file you want to import. It should look like this:



Confirm that the file name input is pre-filled with the full path to the .p12 file for the host and hit the **Next** button.

This will bring you to a panel asking for the password to use for the private key. It should look like this:

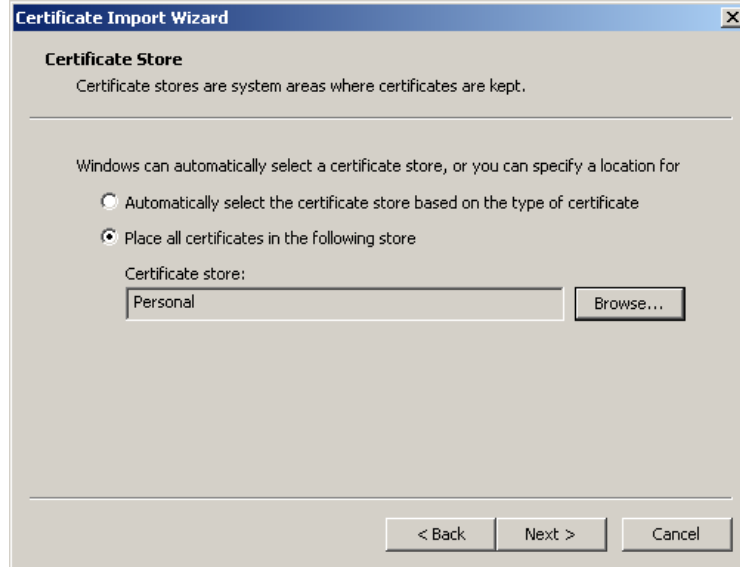


Do the following:

1. Leave the password input blank
2. Ensure the **Enable strong private key protection** box is not checked
3. Check the box for **Mark the private key as exportable**

The result should look like the panel pictured above. When finished, hit the **Next** button.

This will bring you to a panel asking for the certificate store to use. It should look like this:



Do the following:

1. Select the radio button for Place all certificates in the following store
2. Hit the Browse button
3. On the choose dialog that comes up, select the Personal store and hit the OK button to close the browse dialog

The result should look like the panel pictured above. When finished, hit the Next button.

This will bring you to the Completing the Certificate Import Wizard panel. It should look like this:



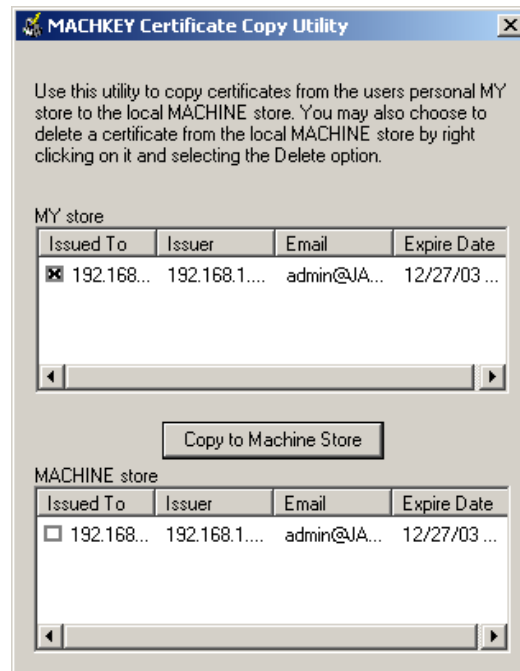
Hit the Finish button.

You should get a dialog stating that the import was successful. It should look like this:



Hit the OK button to close it.

Using Windows Explorer, navigate to `c:\Program Files\Symantec\pcAnywhere` and double-click on the `MachKey.exe` program. This will bring up a window that looks like this:



This shows you a listing of the certificates in your personal store and the machine's store. We need to copy the host certificate we just imported into the machine store. To do so, select the certificate with the host computer's name or IP address and hit the `Copy to Machine Store` button. This will add the certificate to the machine store as shown in the picture above. When finished, close the MachKey utility.

Copy the `certcons.exe` file from `c:\Program Files\Symantec\pcAnywhere` into the `Certs` directory you created earlier.

Go to a DOS prompt and do the following:

```
cd c:\Program Files\Symantec\pcAnywhere\Certs
```

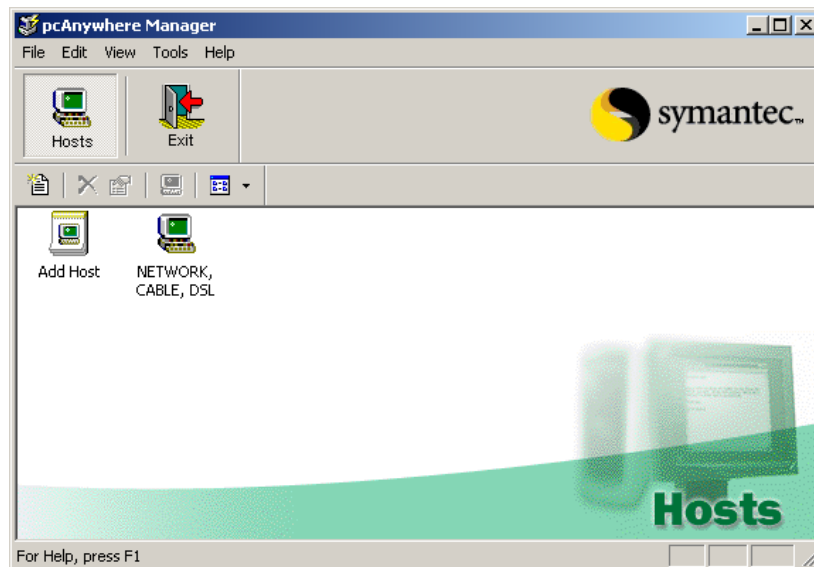
```
certcons pca.store [The names of each of the remote user's .p7b files, separated by spaces]
```

Exit the DOS prompt.

Double-click the pcAnywhere icon to run it.

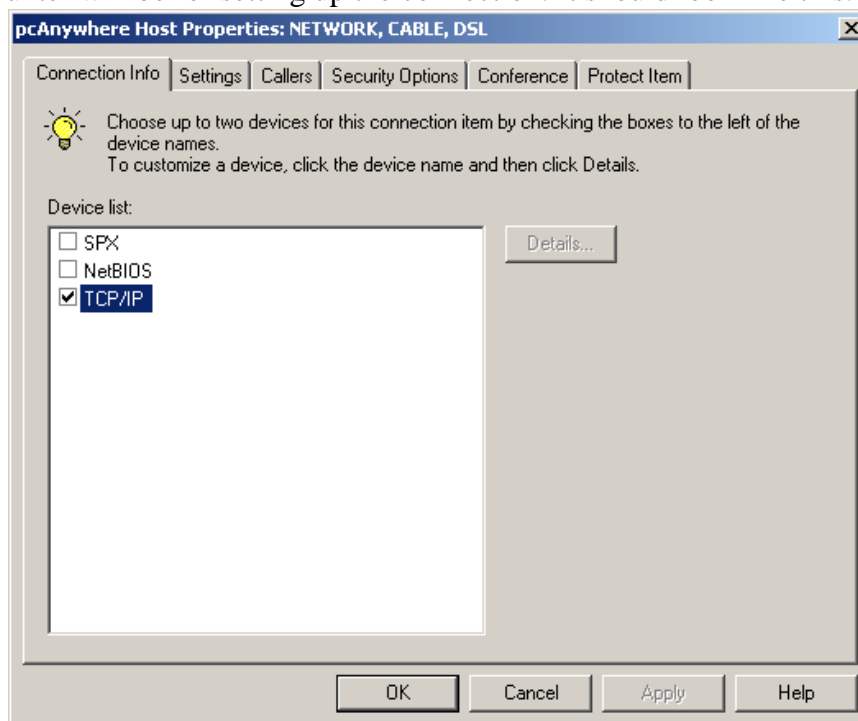
If it asks you to register the product, you can do so, or hit the `Skip` button.

Once pcAnywhere loads, you will get this screen:



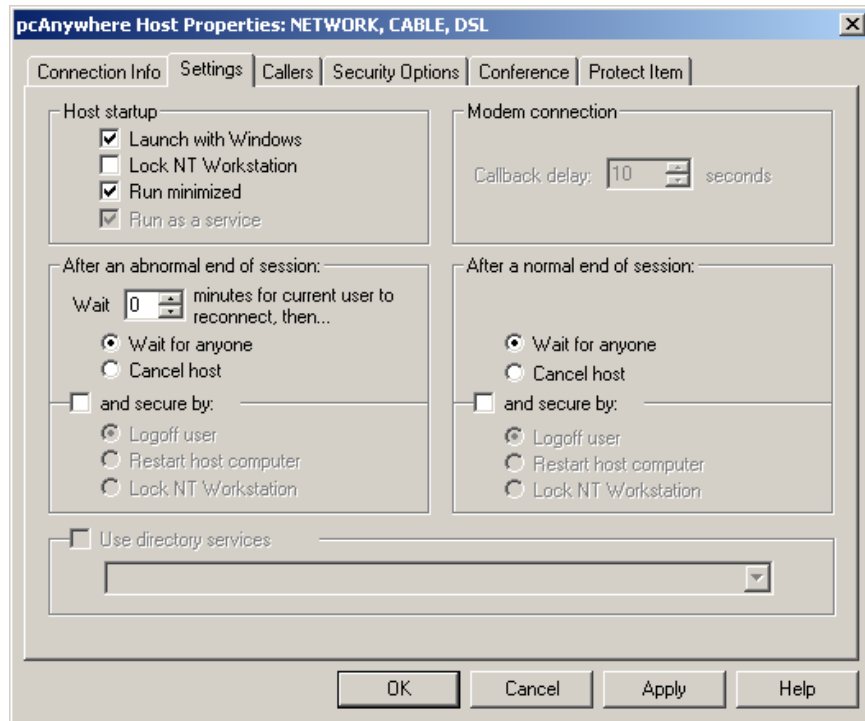
Right-click on the host icon for Network, Cable, DSL and select Properties

This will bring up a dialog to allow you to configure the host's properties. The first panel you encounter will be for setting up the connection. It should look like this:



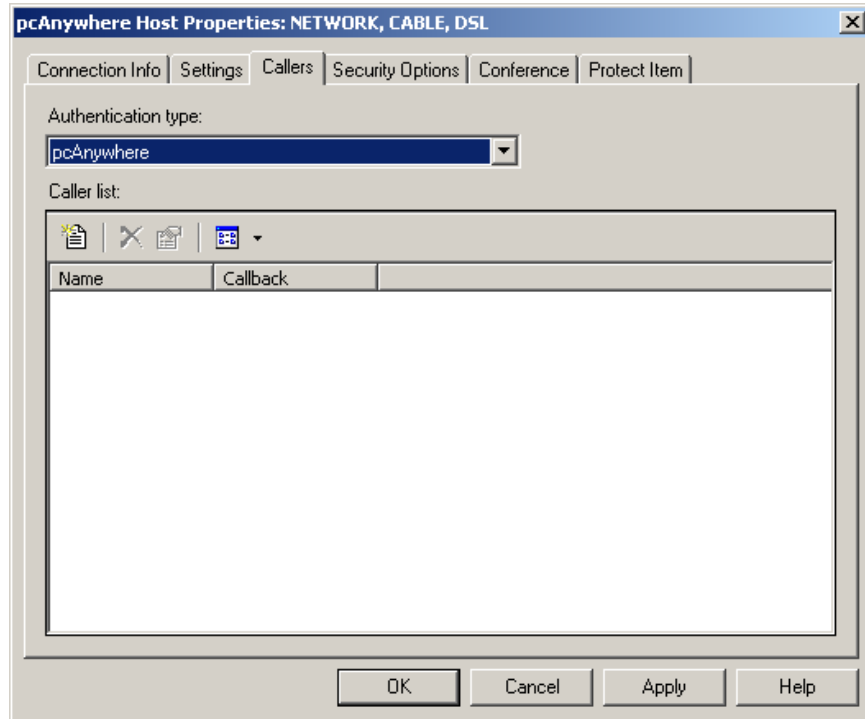
Confirm that TCP/IP is checked.

Click on the Settings tab. This should bring up this pane:




Check the box to Launch with Windows. It should look like the panel pictured above.

Click on the Callers tab. It should bring up a panel that looks like this:

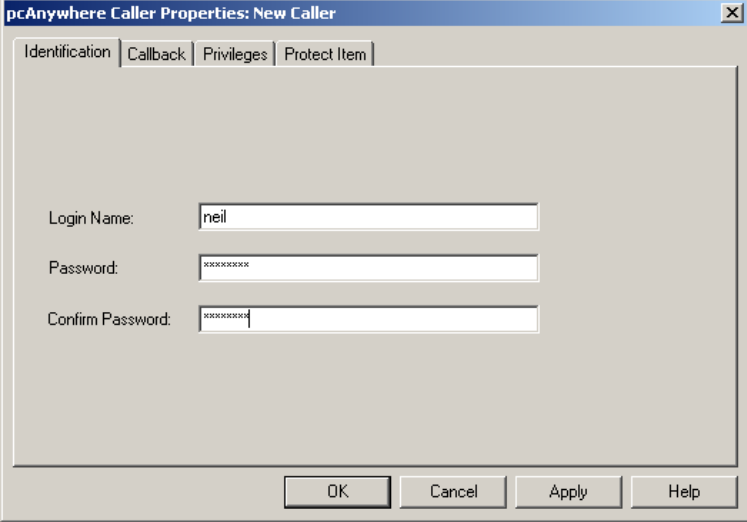


We need to create accounts for each of the remote users that will be logging into the host machine.

To create an account for a user, do the following:

Hit the `New Item` icon. It should look like this: 

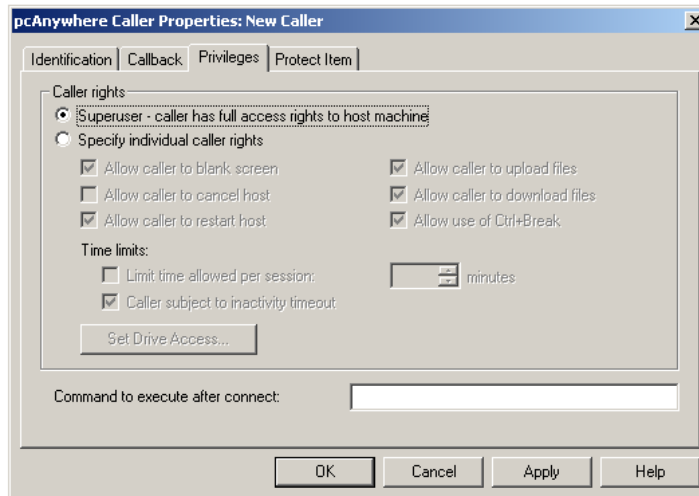
This will bring up a dialog to allow you to configure the user's account. The first panel you should see is the `Identification` panel. It should look like this:



The screenshot shows a dialog box titled "pcAnywhere Caller Properties: New Caller". It has four tabs: "Identification", "Callback", "Privileges", and "Protect Item". The "Identification" tab is active. It contains three text input fields: "Login Name" (containing "neil"), "Password" (containing "xxxxxxxx"), and "Confirm Password" (containing "xxxxxxxx"). At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

Fill in the user's login and password in the fields provided.

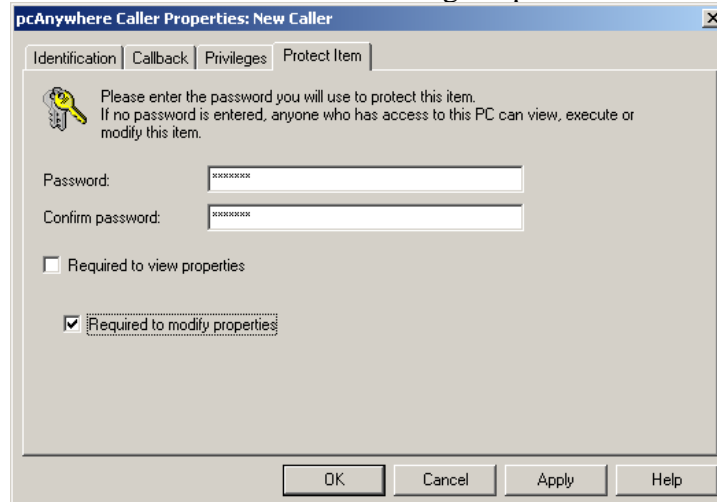
Click on the `Privileges` tab. This will bring up a dialog to allow you to set the privileges this use has. It should look like this:



If you want this user to have full access to the host machine, select the radio button for `Superuser`.

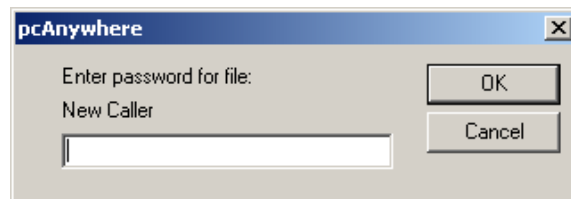
If you want to restrict what this user may do, select the radio button for `Specify individual caller rights` and select what rights you would like the caller to have.

Click on the `Protect Item` tab. You should get a panel that looks like this:



Because this is a server, we do not want any user to be able to modify the rights we are assigning to them or other users. Therefore, it is important to require a password before allowing anyone to modify the properties we just set-up. To do this, enter a password in the two password boxes (The second password box will become accessible when you enter a password in the first one) and check the box next to `Required to modify properties`.

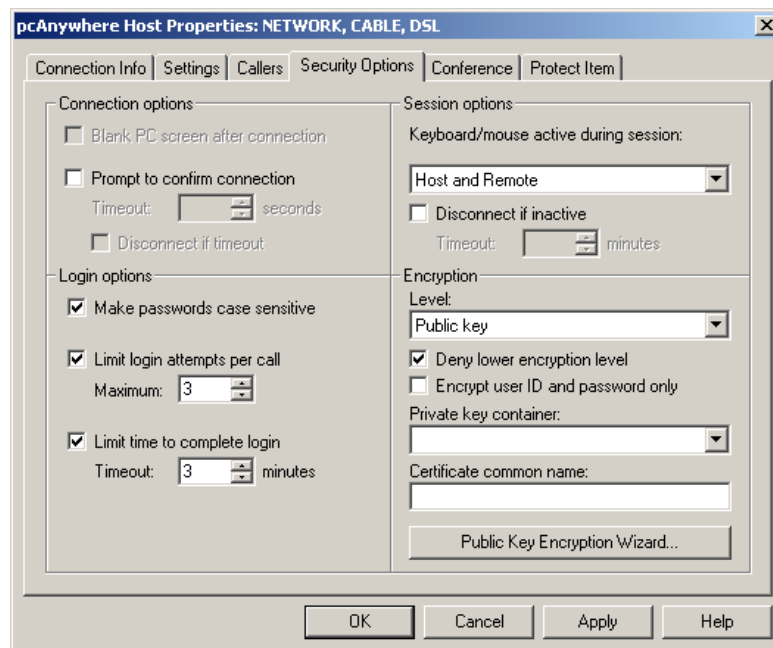
Hit the **OK** button on the caller properties dialog. This will bring up a dialog asking for the password to this caller's properties file so it may write to it. It should look like this:



Enter the password you just created in the **Protect Item** panel above and hit the **OK** button.

This will close the caller properties dialog and drop you back into the **Callers** tab of the host's properties. You should see the caller you just created in the listing of callers.

Click on the **Security Options** tab. You should get a panel that looks like this:



Do the following:

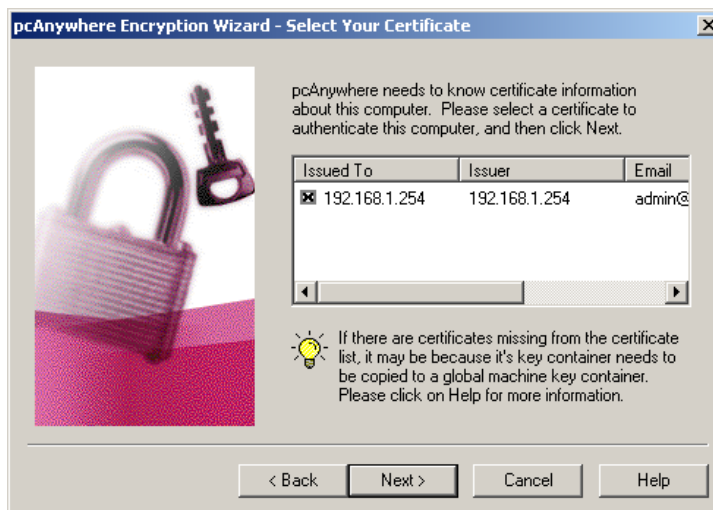
1. Check the box next to **Make passwords case sensitive**
2. In the encryption area, select **Public key** under the **Level** selection box
3. Check the box next to **Deny lower encryption level**
4. Make sure the box next to **Encrypt user ID and password only** is not checked
5. Hit the button for **Public key Encryption Wizard**

This will bring up the Public Key Encryption Wizard. You should get a screen that looks like this:



Hit the `Next` button.

This will bring you to a panel to select the host's certificate. It should look like this:



Check the box next to the certificate for the host machine and hit the `Next` button.

This will bring you to a panel to select your certificate store. It should look like this:



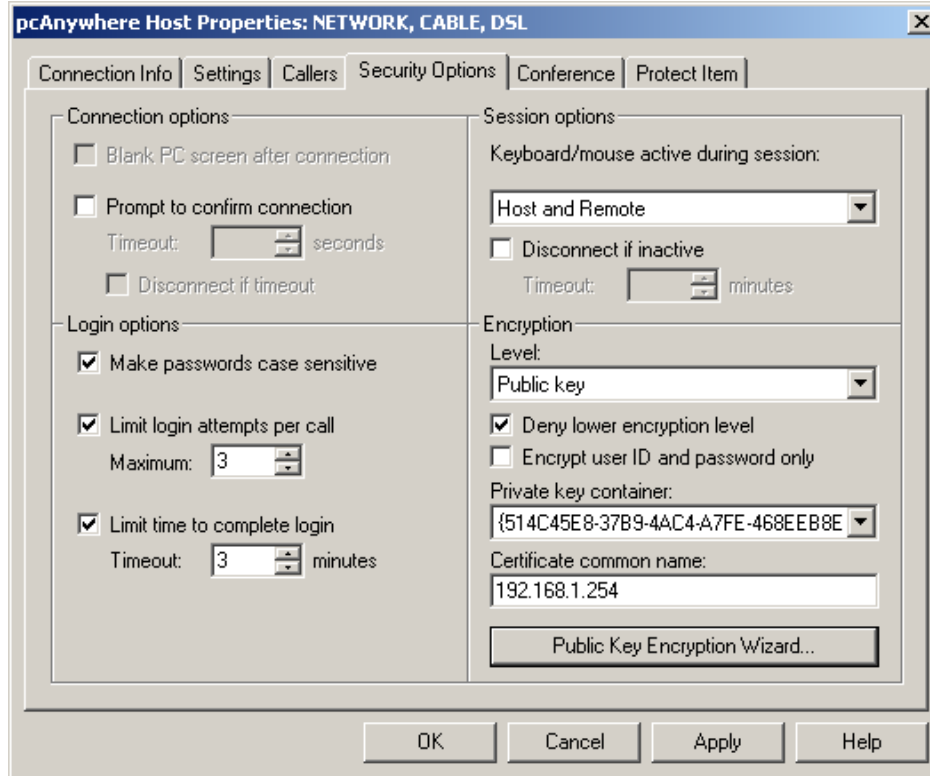
Hit the **Browse** button. In the chooser dialog that comes up, navigate to the `pca.store` file in the `Certs` directory and hit **OK** to close the chooser dialog. When finished, hit the **Next** button.

This will bring you to a confirmation pane that looks like this:



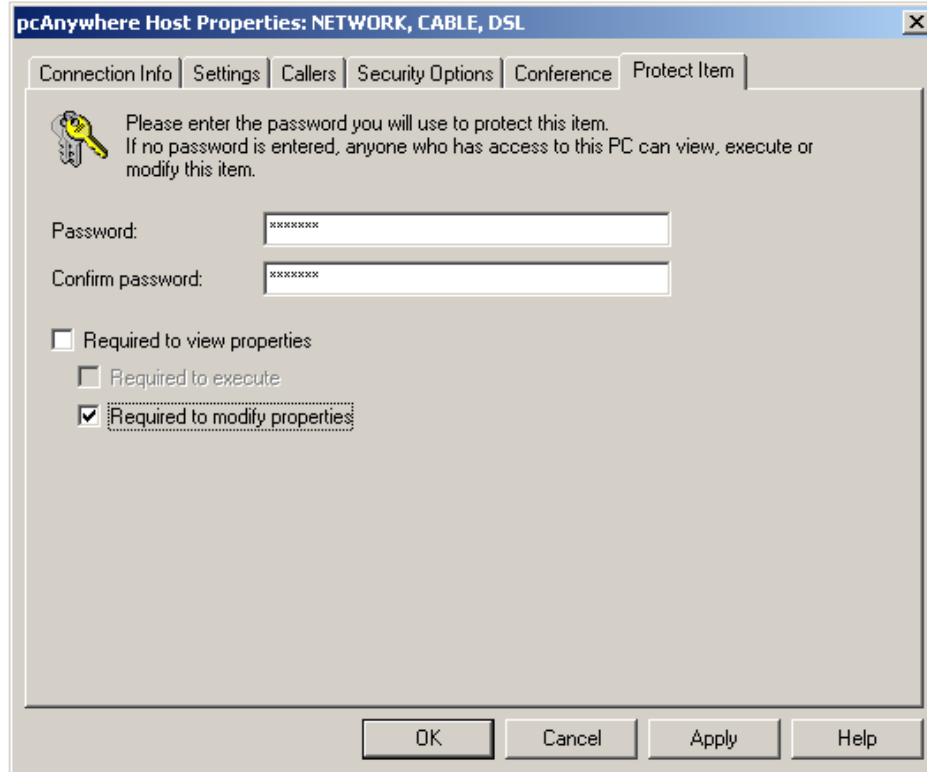
Hit the **Finish** button.

This will take you back to the Security Options tab in the properties for the host. It should look like this:



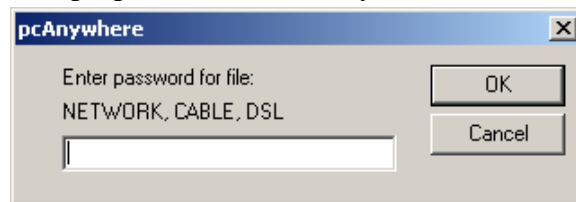
Note that the Private key container and Certificate common name inputs have been filled-in.

Click on the `Protect Item` tab. You should get a panel that looks like this:



Once again, because this is a server, we do not want any user to be able to modify the host's configuration. Therefore, it is important to require a password before allowing anyone to modify the properties we just set-up. To do this, enter a password in the two password boxes (The second password box will become accessible when you enter a password in the first one) and check the box next to `Required to modify properties`.

Hit the `OK` button on the host properties dialog. This will bring up a dialog asking for the password to this host's properties file so it may write to it. It should look like this:



Enter the password you just created in the `Protect Item` panel above and hit the `OK` button.

This will close the host's properties dialog and drop you back into the main screen for pcAnywhere.

Double-click on the `Network`, `Cable`, `DSL` host to initialize it and make sure everything works.

Exit `pcAnywhere` and reboot the computer.

When the computer comes up, there should be an icon in the system tray stating that `pcAnywhere` is waiting for a connection.

## Setting up Driver for Remote Printing

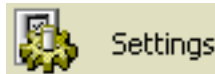
If you would like to print to a local printer while remotely logged into the server, `pcAnywhere` supports remote printing.

To set-up the driver on the server, do the following:

Click on the `Start` button on the bottom right corner of the screen. It should look like this:



In the menu that comes up, select `Settings`. It should look like this:



In the menu that comes up, select `Control Panel`. It should look like this:



This should bring up the control panel window.

Once in the control panel, double-click on the `Printers` icon. It should look like this:



Printers

This will bring up a window that shows you the current printers installed on the computer. Double click on the `Add Printer` icon. It should look like this:



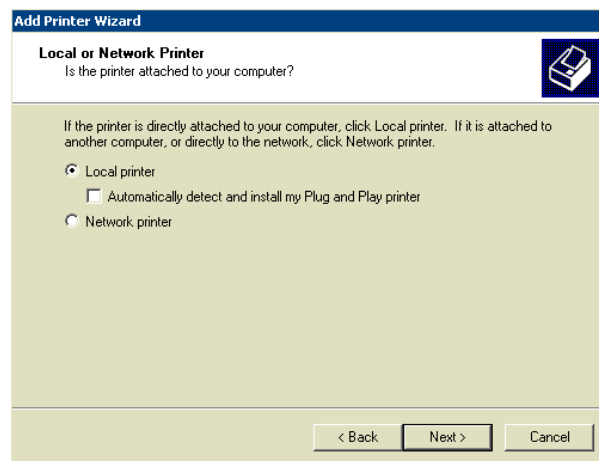
Add Printer

This will bring up the Add Printer wizard. It should look like this:



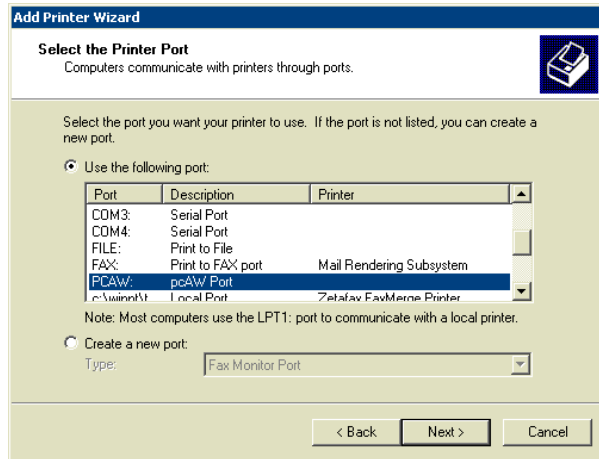
Hit the `Next` button on the introduction screen.

This will bring up a screen asking if the printer is a local or network printer. It should look like this:



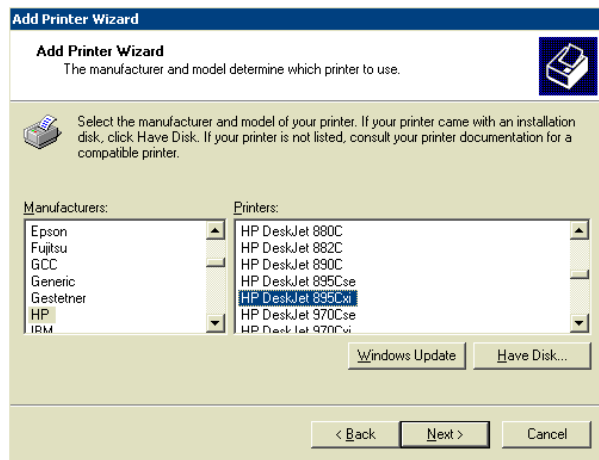
Select the radio button for `Local printer`, make sure the checkbox for `Automatically detect and install my Plug and Play printer` is **not** checked, and hit the `Next` button.

This will bring up a window to select the printer port. It will look like this:



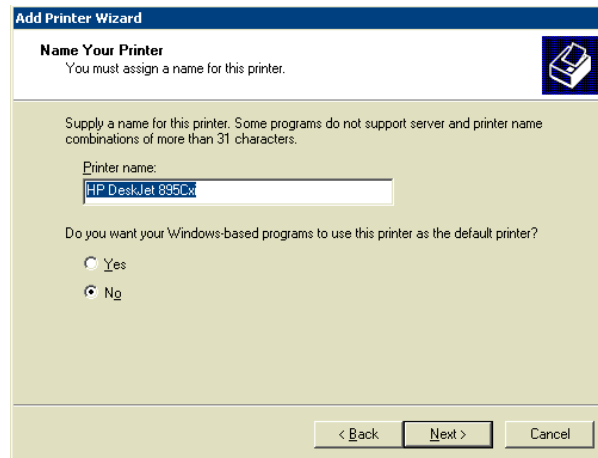
Select the PCAW: port and hit the Next button.

This will bring up a dialog to select the printer driver for the remote printer. It should look like this:



Select the manufacturer and printer model of the remote printer (I have illustrated this example with an HP DeskJet 895Cxi) and hit the Next button.

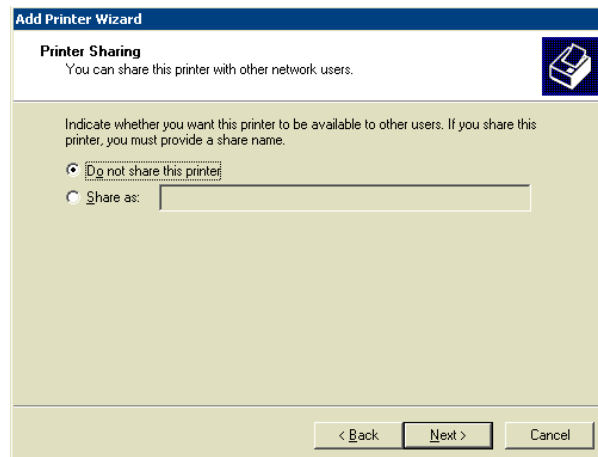
This will bring up a window asking you to name the printer. It should look like this:



The screenshot shows a window titled "Add Printer Wizard" with a sub-header "Name Your Printer". Below the sub-header, it says "You must assign a name for this printer." and includes a printer icon. The main text reads: "Supply a name for this printer. Some programs do not support server and printer name combinations of more than 31 characters." There is a text input field labeled "Printer name:" containing the text "HP DeskJet 895Cx". Below this, it asks "Do you want your Windows-based programs to use this printer as the default printer?" with two radio buttons: "Yes" (unselected) and "No" (selected). At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Give the printer a name, make sure you select the radio button for No under Do you want your Windows-based programs to use this printer as the default printer? and hit the Next button.

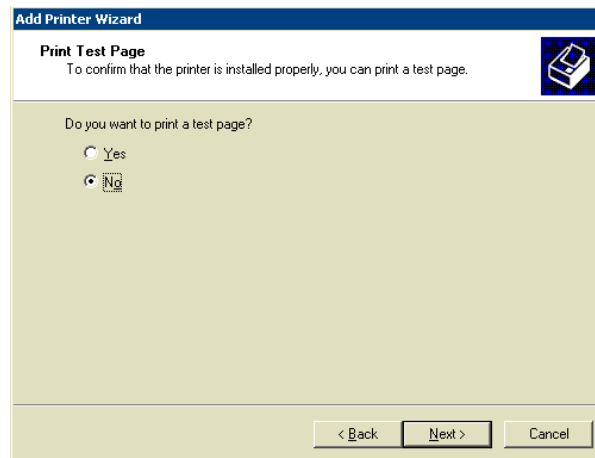
This will bring up a window asking if you would like to share the printer. It should look like this:



The screenshot shows a window titled "Add Printer Wizard" with a sub-header "Printer Sharing". Below the sub-header, it says "You can share this printer with other network users." and includes a printer icon. The main text reads: "Indicate whether you want this printer to be available to other users. If you share this printer, you must provide a share name." There are two radio buttons: "Do not share this printer" (selected) and "Share as:" (unselected). The "Share as:" option has an empty text input field next to it. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Select the radio button for Do not share this printer and hit the Next button.

This will bring up a window asking for you to print a test page. It should look like this:



Select the radio button for No and hit the Next button.

This will bring up a window to tell you that you have completed the Add Printer Wizard. It should look like this:



Hit the Finish button. This will install the driver and close the Add Printer Wizard.

Now, when you are connected to the host from a remote machine, you will be able to print to the default printer on the remote computer from windows programs running on the host by selecting the printer you just installed on the host machine.

## Setting up Remote Printing from DOS programs

To set-up remote printing from DOS programs to a remote printer driver you set-up using the procedure above, you will need to create a mapping from the `lpt1:` printer port to the remote printer driver.

Click on the `Start` button on the bottom right corner of the screen. It should look like this:



In the menu that comes up, select `Settings`. It should look like this:



In the menu that comes up, select `Control Panel`. It should look like this:



This should bring up the control panel window.

Once in the control panel, double-click on the `Printers` icon. It should look like this:



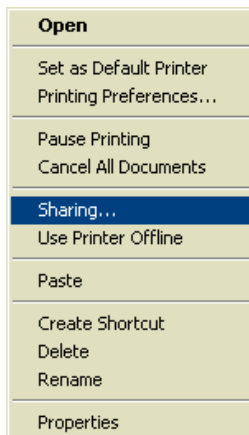
Printers

This will bring up a window that shows you the current printers installed on the computer. There should be an icon for the remote printer driver. It should look like similar to this:

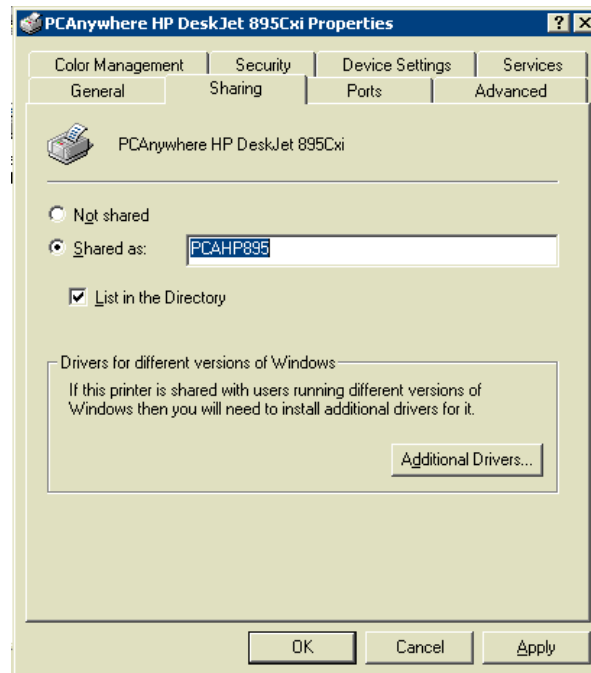


PCAnywhere  
HP DeskJet  
895Cxi

Right-click on the icon for your remote printer. This will bring up a menu. From that menu, Select `Sharing`.



This will bring up a window to allow you to share the printer. It should look like this:



Select the radio button next to `Shared as:`, give it a name, and hit the `OK` button. This will close the sharing properties window.

Now, find out the name of the host computer. To do so, double-click on the `System` icon in the Control Panel. It should look like this:



Click on the `Network Identification` tab in the System Properties window. The computer name will be next to a label `Full computer name:`. You will need to make a note of the full computer name. Once finished, close the Control Panel window.

Next, create a batch file to install the mapping of the `lpt1:` printer port to the remote printer driver. It should have this content:

```
net use lpt1: \\[Full Computer Name]\[Share name] /persistent:yes
```

For example, if you host computer's name is `myHost` and you gave the remote printer a share name of `pcPrinter`, the batch file should contain this content:

```
net use lpt1: \\myHost\pcPrinter /persistent:yes
```

Finally, create a batch file to remove the mapping of the lpt1: port. It should contain this content:

```
net use lpt1: /delete
```

Let JAMM Consulting secure your network  
and systems!

Visit us at <http://www.JAMMConsulting.com> for examples of our work  
and how we can grow your business.

