

## Cisco VPN Client Installation:

*This document only applies to users who can authenticate to Active Directory in the Department of Electrical and Computer Engineering.*

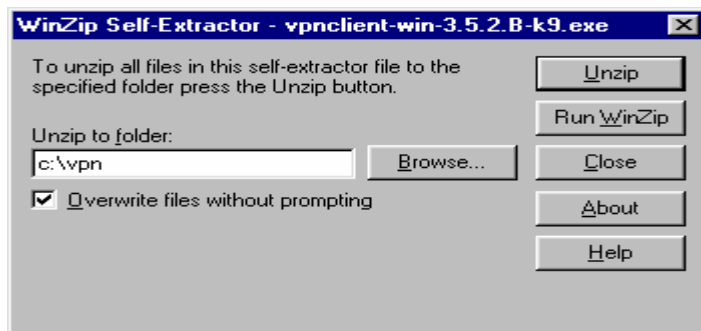
**Windows XP Users Take Note:** Before starting the VPN setup you need to set the following:

- Click on: **Start, Settings, Control Panel**
- Ensure you have the **Classic View** selected. (there is a selection on the left, if it says **Switch to Category View**, leave it, if it says **Switch to Classic View**, do it)
- Once in **Control Panel**, click on, **System**, Select the **Hardware** tab, and the **Driver Signing** button;
- Click the **Ignore** radio button under **What Action do you want Window to take?**

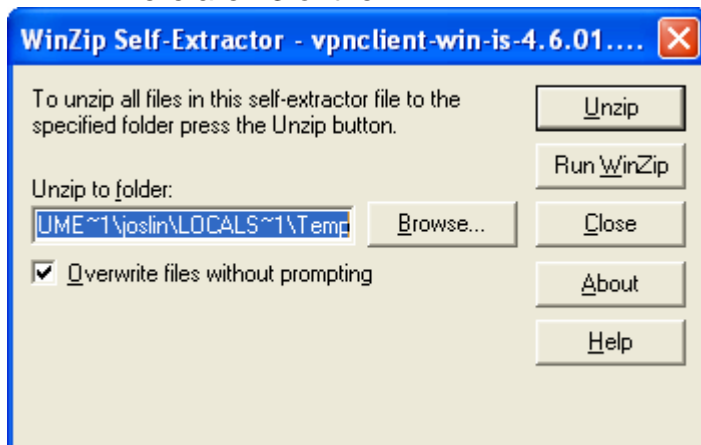
*The following assumes you have retrieved the VPN installation self-extracting file and stored it in **c:\vpn** folder.*

### Unzip the VPN installation self-extracting file

- Go to the **c:\vpn** folder and double click on the installation file
- You will get a screen like the following depending on the Unzip program you have.
- Change the **Unzip to folder:** path to your **c:\vpn** folder, just to keep all the files together.



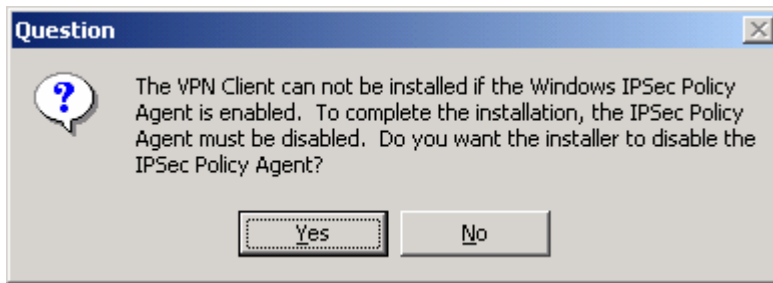
- There are 13 of them.



### Run Setup

- Go to the **c:\vpn** folder and double-click on the **Setup.exe** (the icon has little sails)

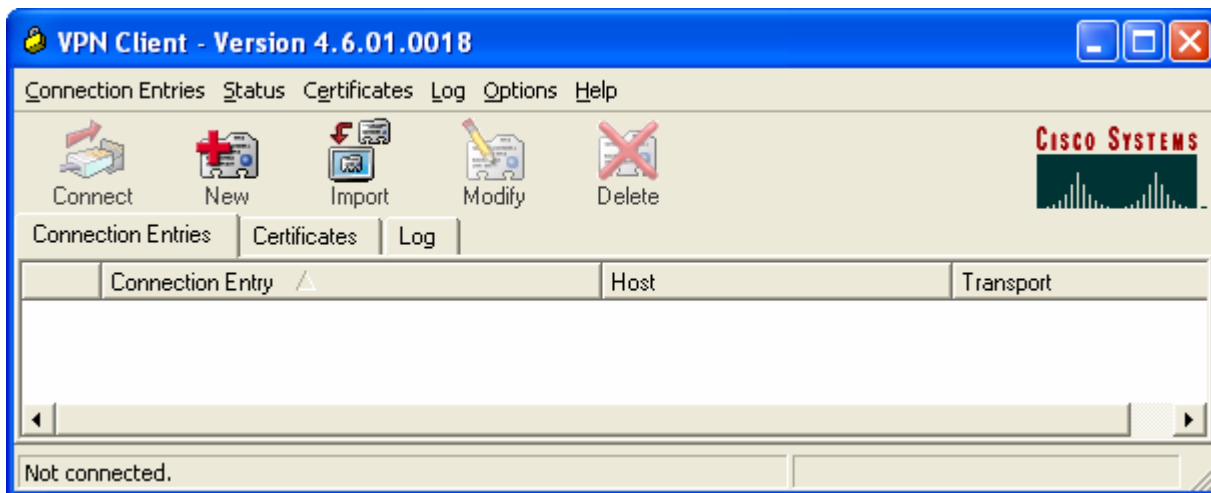
- The following screen appears if you are running Windows 2000. Just Click **Yes**



- At the welcome screen, click **Next**
- **Agree** with the License Agreement
- Accept the default install location
- The program installs and prompts you to re-start your computer, do that.

## Configure Cisco Systems VPN Client

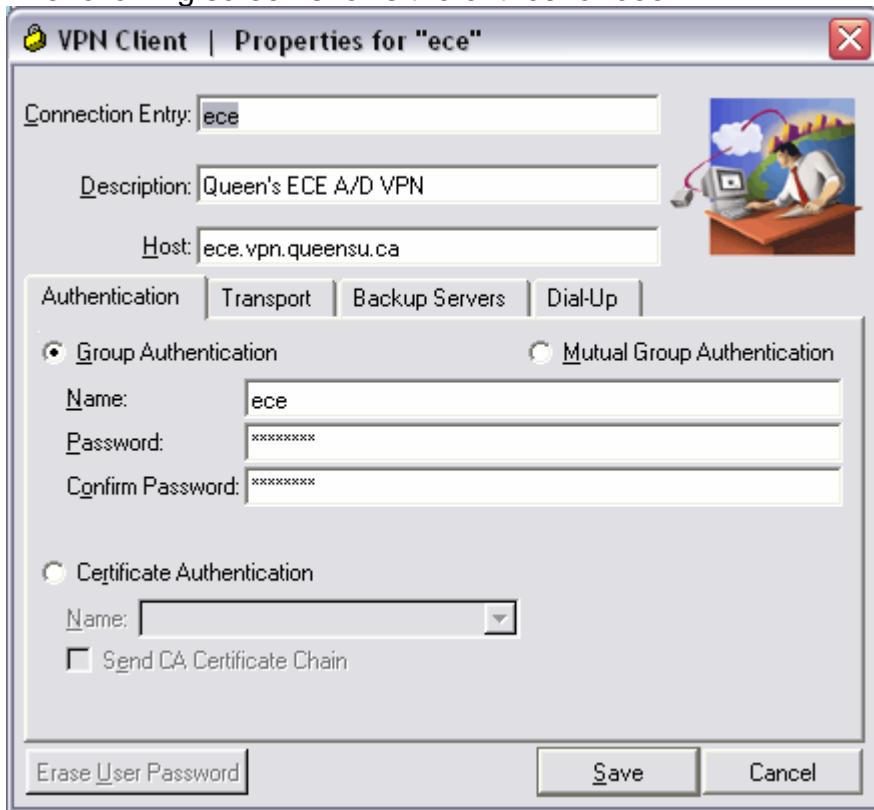
- With your pc rebooted click on:
  - **Start, All Programs, Cisco Systems VPN Client, VPN Client**
- You will have the following screen.
- Click On **New**



## Create New VPN Connection Entry - *Authentication Tab*

- In the **Connection Entry** box you will enter either **ece**.
- In **Description**: **Queen's ECE A/D VPN**
- In the Host box enter: **ece.vpn.queensu.ca**
- Make sure the **Group Authentication** radio button is selected.
- Enter your server name in the **Name** field: **ece**
- The **Passwords** field exactly as shown (including case): **nYWbAanIa**

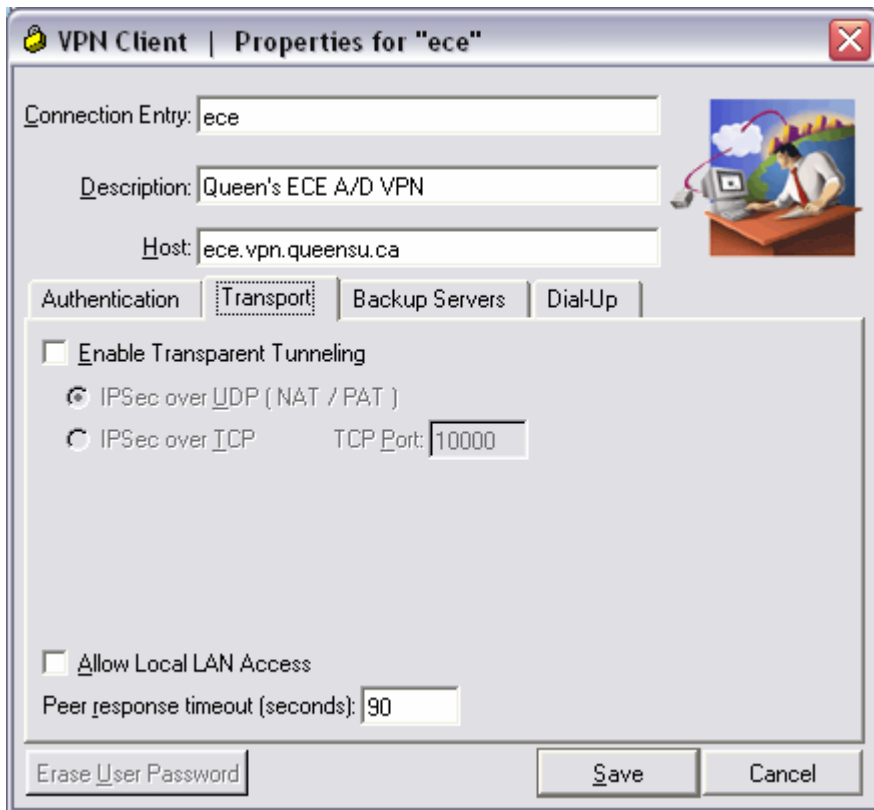
The following screen shows the entries for **ece**



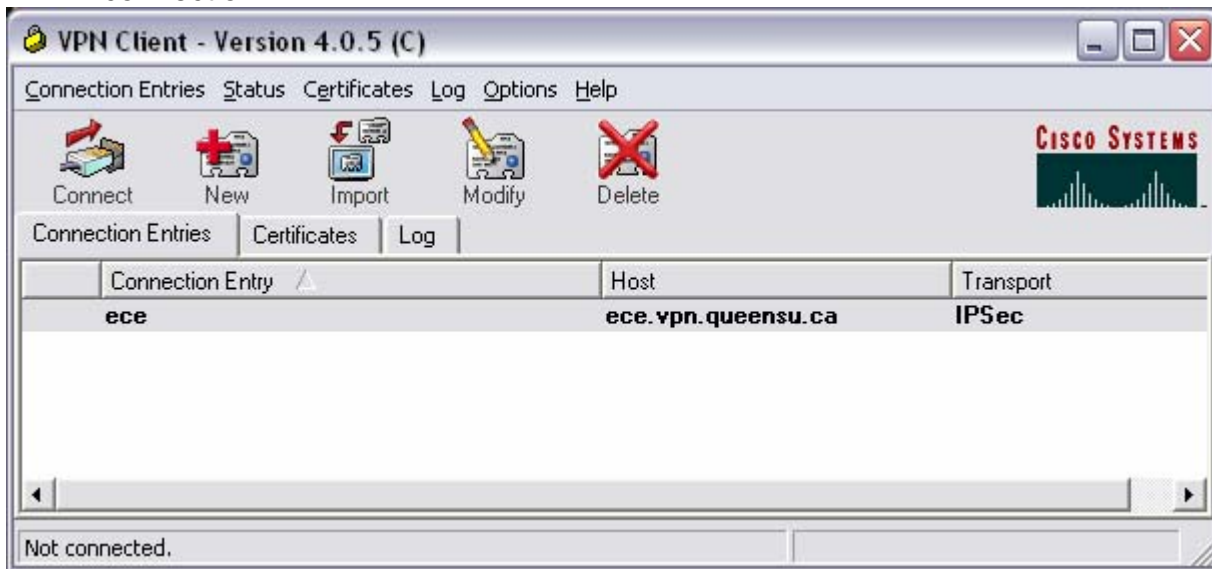
The screenshot shows a Windows-style dialog box titled "VPN Client | Properties for 'ece'". It contains several input fields and tabs. The "Connection Entry" field is set to "ece", the "Description" is "Queen's ECE A/D VPN", and the "Host" is "ece.vpn.queensu.ca". There are four tabs: "Authentication", "Transport", "Backup Servers", and "Dial-Up". The "Authentication" tab is active, showing two radio button options: "Group Authentication" (selected) and "Mutual Group Authentication". Under "Group Authentication", there are three text boxes: "Name" (set to "ece"), "Password" (masked with asterisks), and "Confirm Password" (masked with asterisks). Under "Mutual Group Authentication", there is a "Name" dropdown menu and a checkbox for "Send CA Certificate Chain" which is unchecked. At the bottom, there are three buttons: "Erase User Password", "Save", and "Cancel".

## Create New VPN Connection Entry - *Transport* Tab

- Click to the **Transport** tab
- Uncheck the **Enable Transport Tunneling** box, unless you are running a Proxy server; not likely.
- You can also uncheck: **Allow local LAN access**
- The screen will look as follows



- Click **Save** - you should be back to this screen, you will see an entry for your new VPN connection.



- You can always get to this screen by clicking on
  - Start, All Programs, Cisco Systems VPN Client, VPN Client

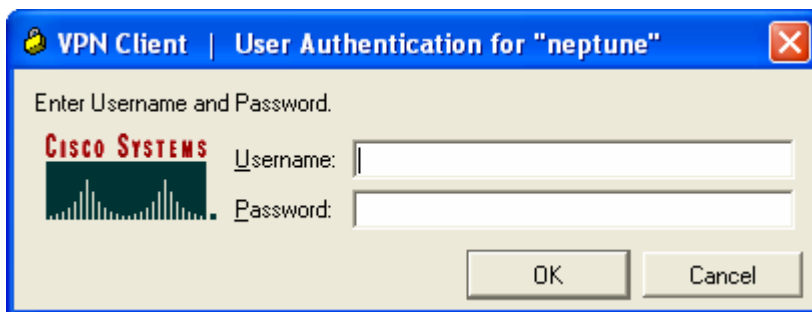
## You are then ready to actually run the VPN client,

The following are the sequence of events necessary to authenticate with the VPN server and therefore allow you access to your Active Directory file server or allow to run secure admin programs such as QWS3270 (access to PCICS, MVS) and GQL.

- Establish your network connection, either by dialing into the Queens V:90 toll line or using your internet connection provider at home or on the road.
- Click on: Start, **All Programs, Cisco Systems VPN Client, VPN Client**



- Highlight your connection and click the **Connect** button, you will see the following screen:
- At the following screen, enter your Net-ID username and password and click: **OK**
- This tells the VPN server that you are authorized to use this VPN connection.

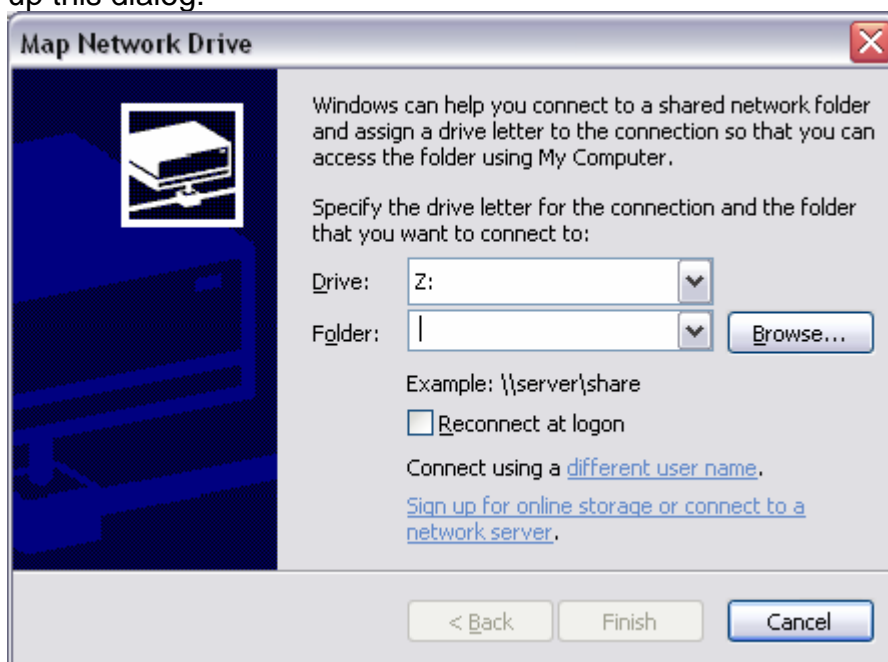


- If all goes well the screen will minimize and your connection will be completed. You can carry on connecting to the A/D fileserver, running QWS3270 (MVS, PCICS) or GQL.

## Accessing the A/D fileserver

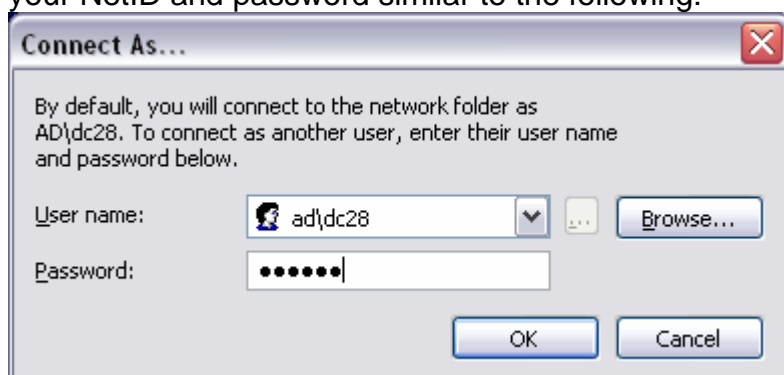
When connecting remotely using VPN, your A/D file shares won't automatically mount on your computer. You will have to add them manually. Do the following:

1. **Start > My Computer >** right-click and choose **Explore** from the context-sensitive menu
2. In the **My Computer** window, choose **Tools > Map Network Drive...** which brings up this dialog:



3. In **Drive**, choose "I" from the drop down. In **Folder**, type:  
\\clusfile4.ad.queensu.ca\acshare\$\ece\shared
4. Click **Finish**. The I drive should be added to the list of drives available.
5. Repeat step 2 and then choose "H" in **Drive** and in **Folder**, type:  
\\clusfile4.ad.queensu.ca\acshare\$\ece\users\[username]  
replacing [username] with your Net-ID username, for **grad students**, use:  
\\clusfile4.ad.queensu.ca\acshare\$\ece\grads\[username]

If the connections fail, you may not be logged on to your local computer using your Net-ID account. Try the above again, but click **Connect using a different user name** and enter your NetID and password similar to the following:



You will need to use your Net-ID user name preceded by **ad\** just like the example above. Then enter your Net-ID in the **Password** field.