

VPN Client Installation Instructions (Internal OME-RESA network)

May 29, 2008
updated October 1, 2008

merregae.wine@omeresanet

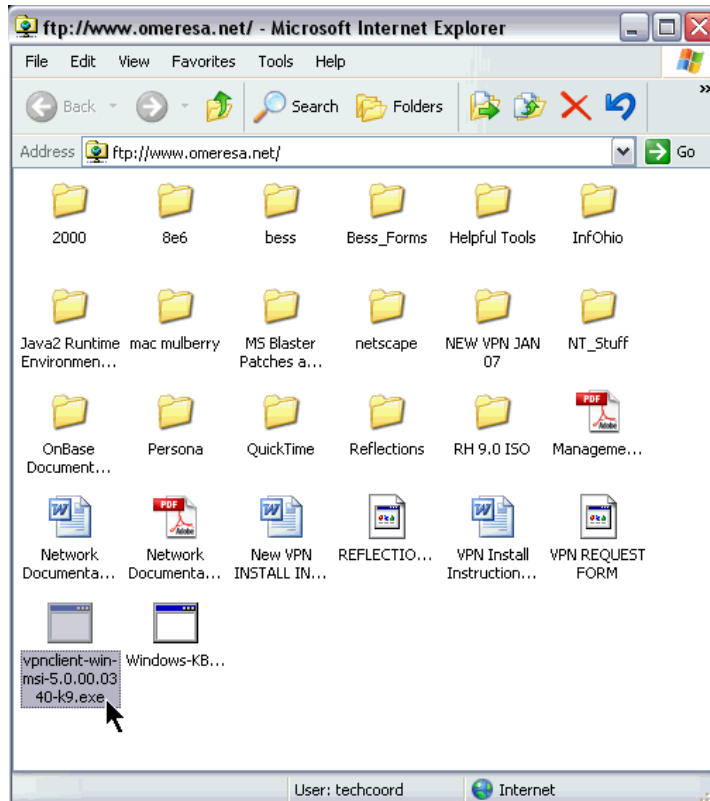
Download the correct VPN Client for your OS.

Open a browser and type in:

`ftp://techcoord@www.omeresanet`

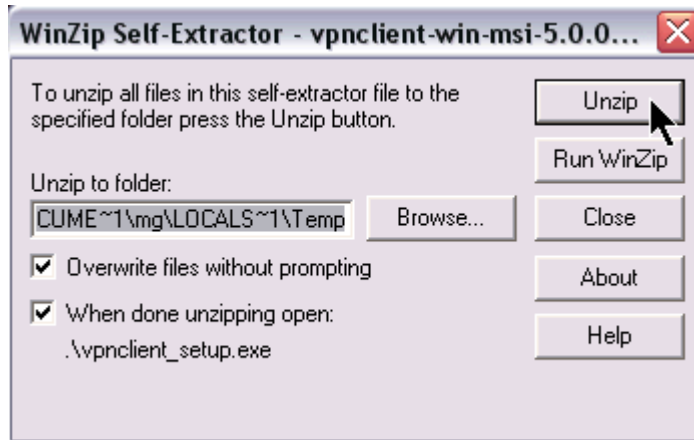
Username and password provided by OME-RESA staff

Drag the file `vpnclient-win.msi-5.0.00.0340-k9.exe` to your desktop.



Close the browser when download is complete.

Double-click the executable file (or unzip to a folder on your desktop)

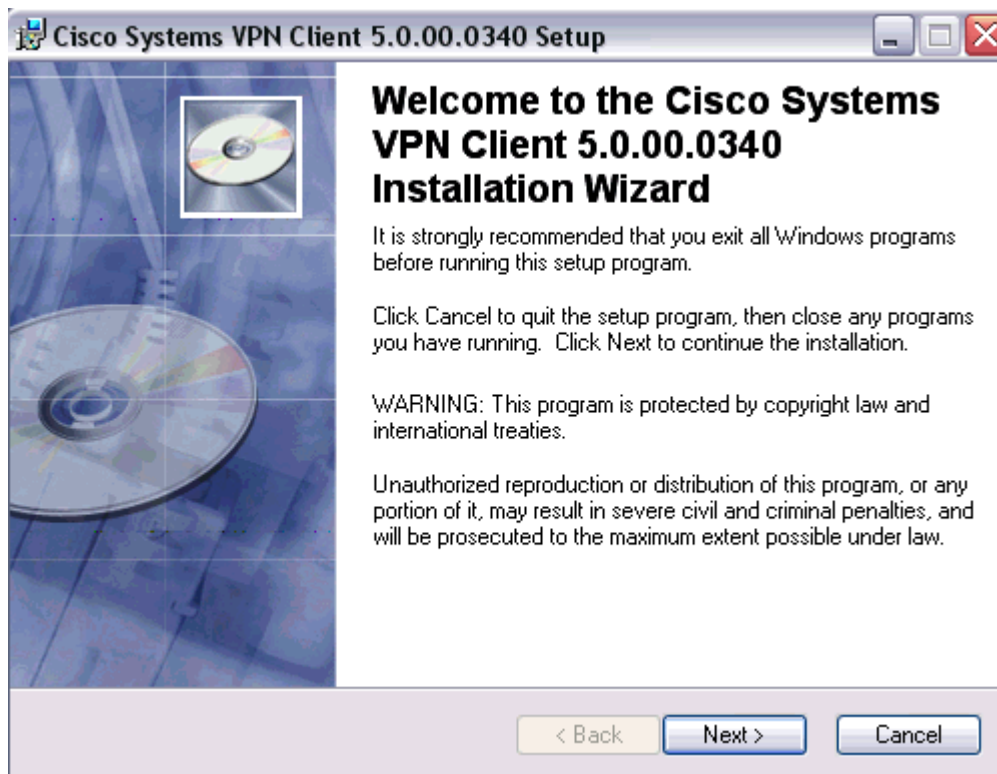


Open the extracted folder (if you create one) - some Operating systems will run the file automatically for you (depends on your OS).

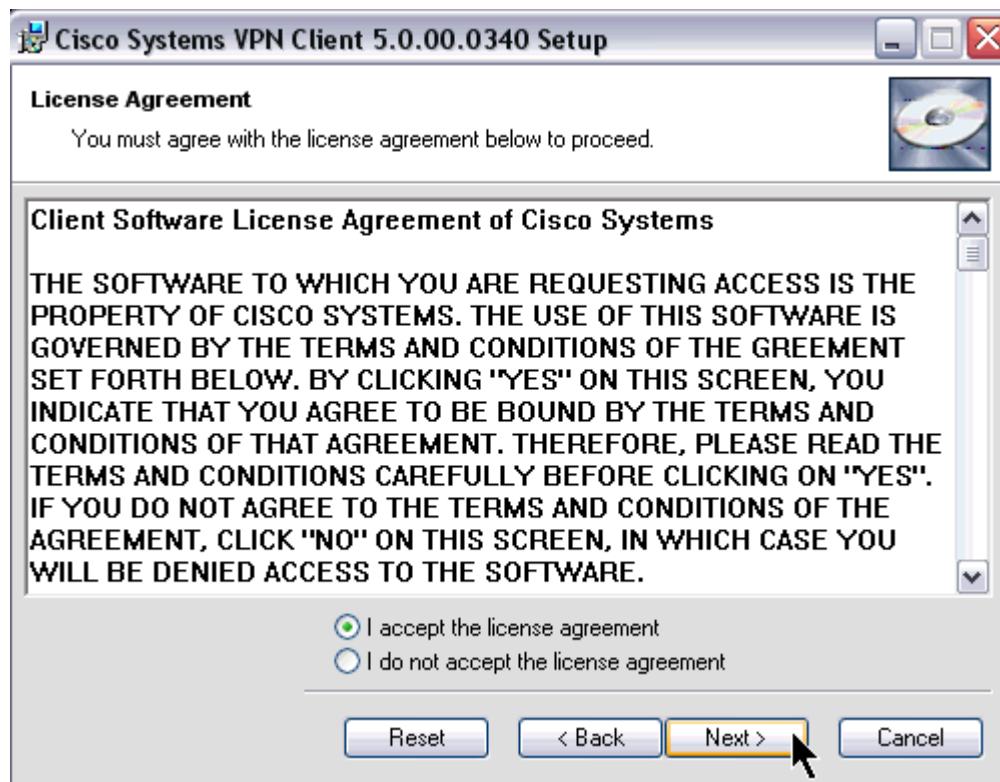
Double-click the vpnclient_setup.exe (if your OS doesn't open the setup for you automatically).

You should see a Welcome screen.

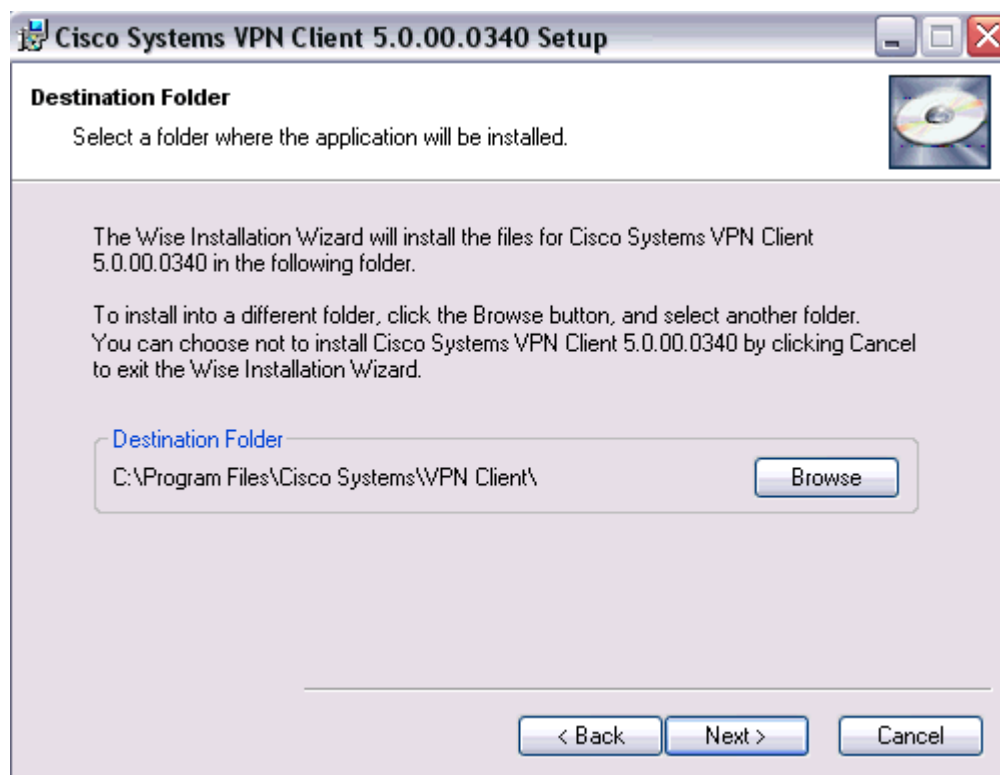
Click on Next.



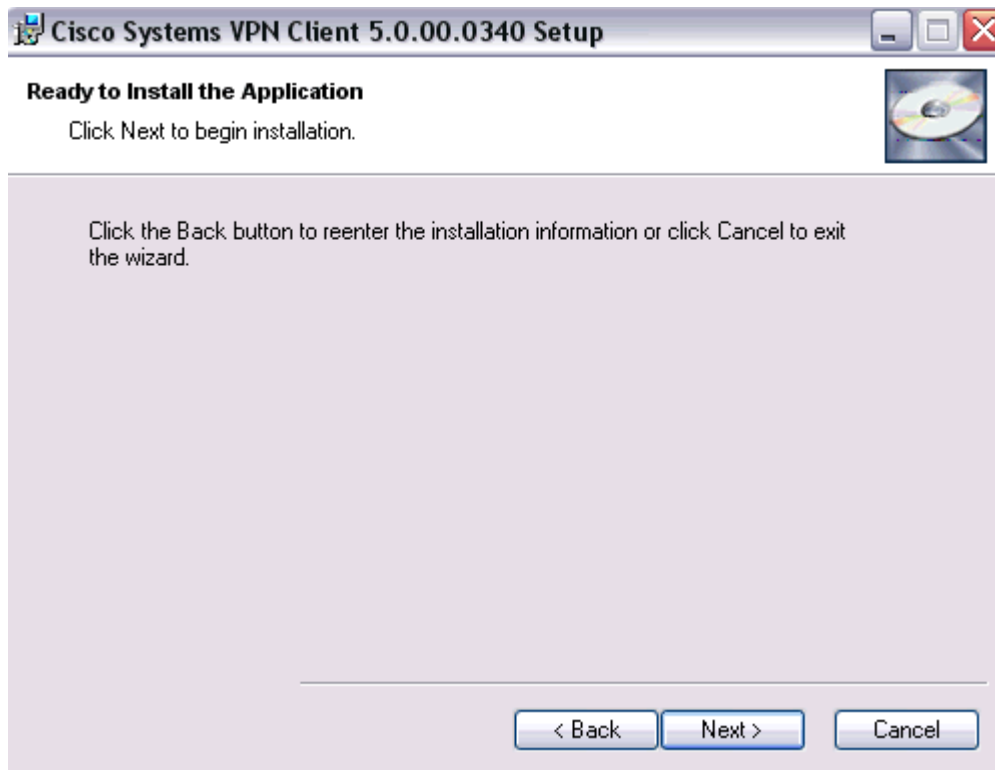
Accept the agreement and click Next.



Choose the default folder and click Next.

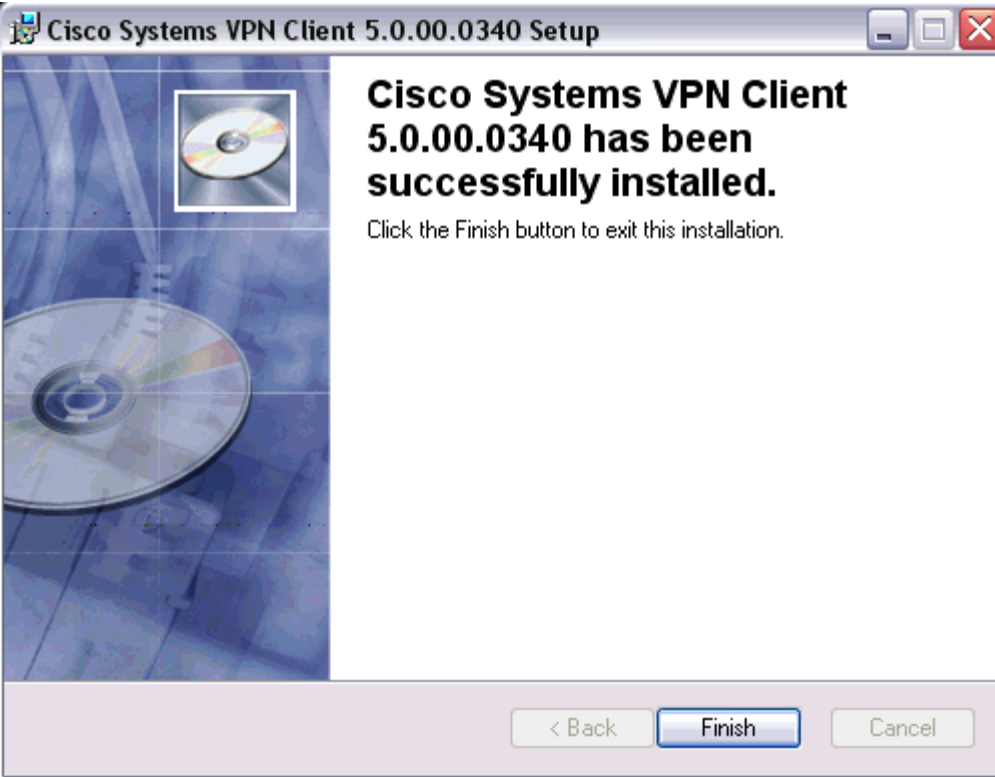


Ready to Install, click Next.

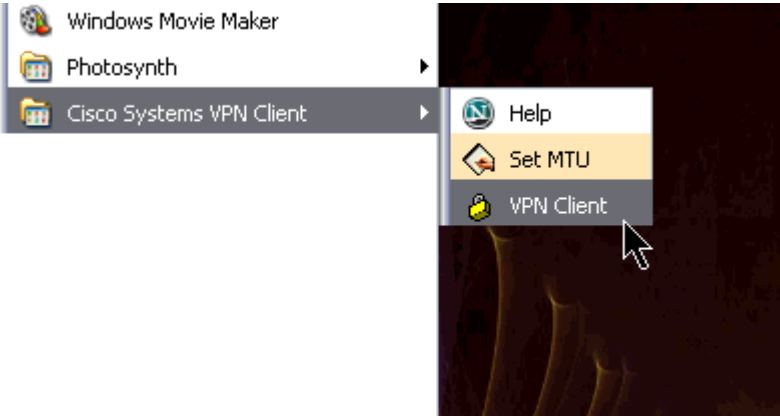


Let the application install, takes a little while during certain areas.

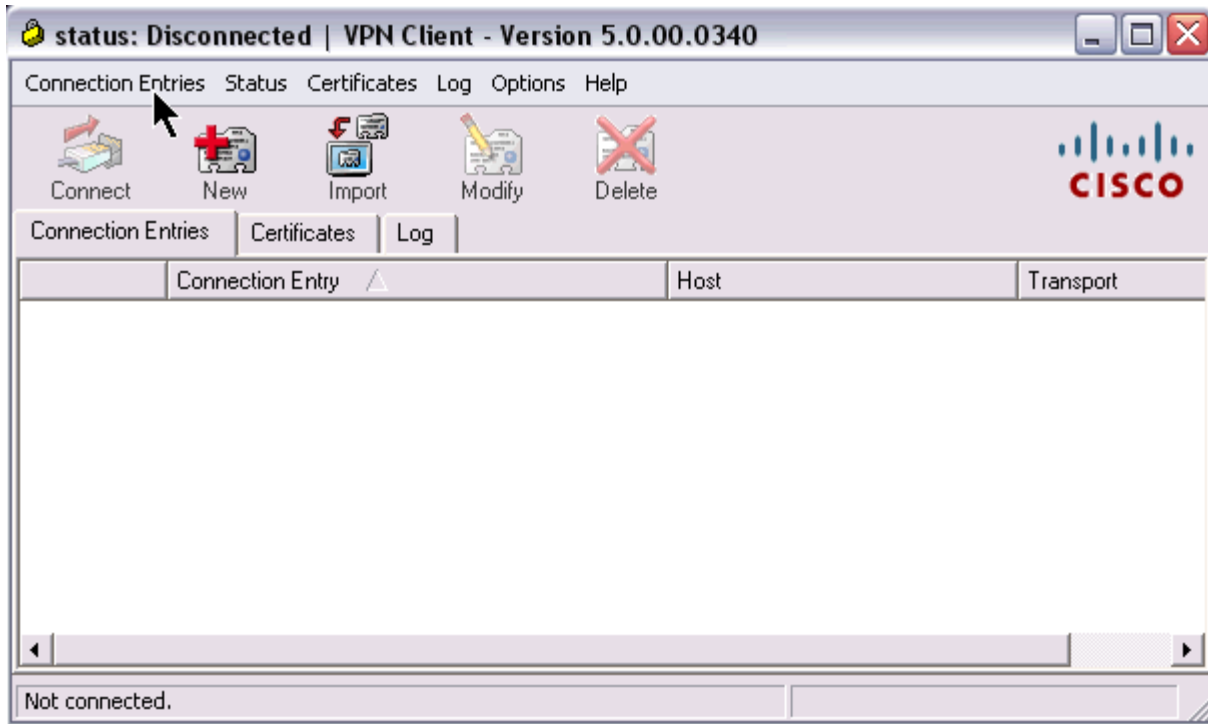
Click Finish and restart your system.



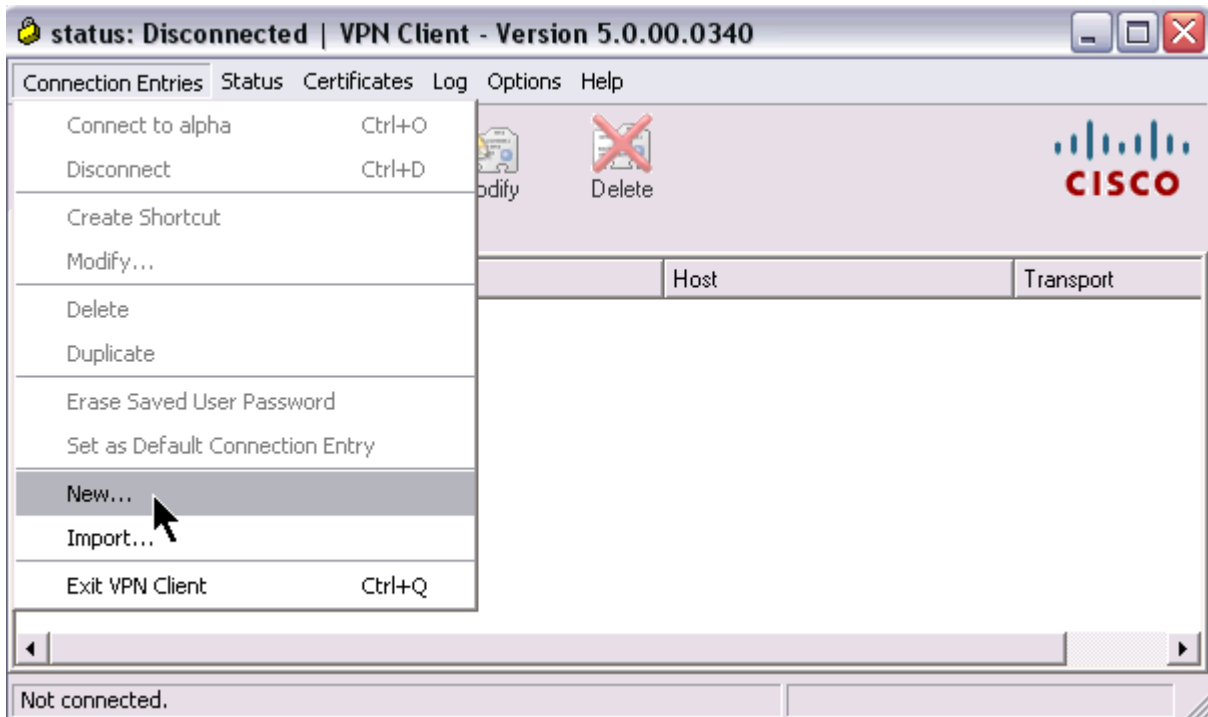
Go to Start, Programs, Cisco Systems VPN Client, and open the VPN Client (yellow padlock)



Choose Connection Entries



Choose New (or Modify if previously configured)



Connection Entry = (give your session a name, for example "alpha")

Host = 10.100.0.2

Group Authentication (Name and password provided by OME-RESA staff)

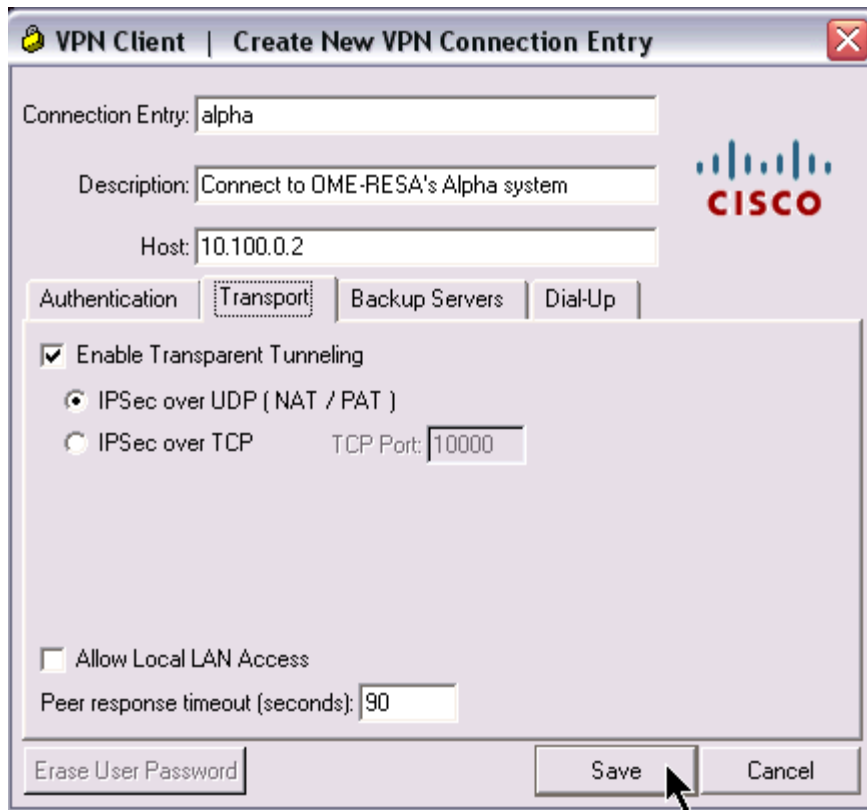
The screenshot shows a window titled "VPN Client | Create New VPN Connection Entry". It contains several input fields: "Connection Entry" with the value "alpha", "Description" with "Connect to OME-RESA's Alpha system", and "Host" with "10.100.0.2". There are four tabs: "Authentication", "Transport", "Backup Servers", and "Dial-Up". The "Authentication" tab is selected, and within it, the "Transport" sub-tab is active. Two radio buttons are present: "Group Authentication" (selected) and "Mutual Group Authentication". Below these are three password fields: "Name" (containing "GroupName"), "Password" (redacted with "*****"), and "Confirm Password" (redacted with "*****"). Under the "Certificate Authentication" section, there is a "Name" dropdown menu and a checkbox for "Send CA Certificate Chain". At the bottom, there are three buttons: "Erase User Password", "Save", and "Cancel". A Cisco logo is located on the right side of the dialog.

Click on the Transport tab.

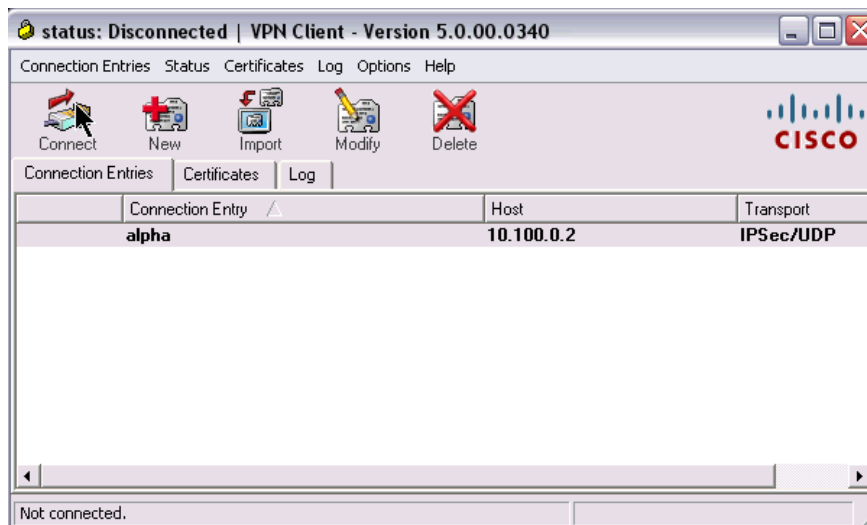
Check mark in Enable Transparent Tunneling

Choose IPsec over UDP

Save



Click the Connect icon



Enter the username and password assigned by OME-RESA staff.



You will see a message "Negotiating security clearance..."

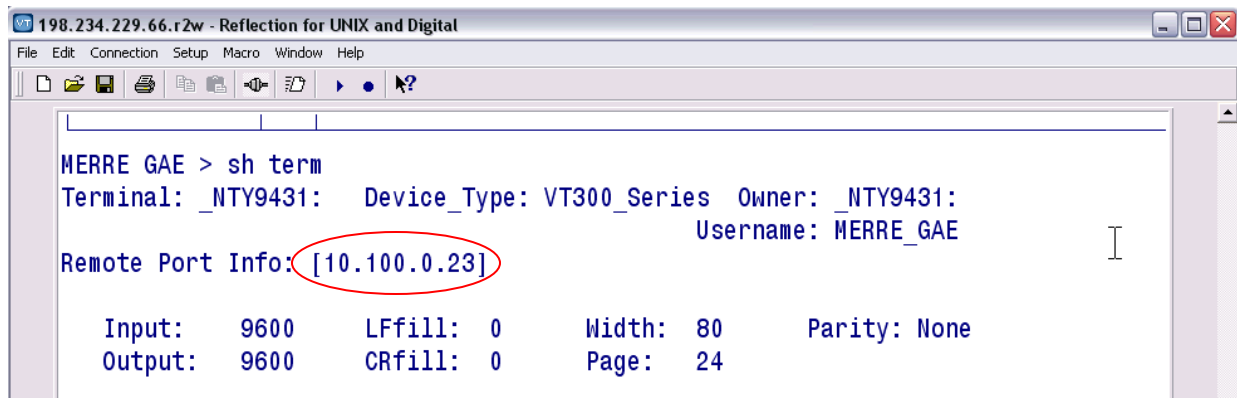
When the application connects, the little yellow padlock icon will minimize to the taskbar on the bottom right of your desktop and will be running in the background.



To check the connection, Open a Reflection session using your Alpha username and password.

At your name prompt, type in "show term"

If the Remote Port Info = 10.100.0.xx you are using the VPN client to connect.



If the Port Info shows the IP address of your local machine (such as 10.10.14.85) you are not connected via the VPN client.