

# Brazosport College VPN Connection Installation and Setup Instructions

**Draft 2**  
**March 24, 2005**

## Introduction

This is an initial draft of these instructions. These instructions have been tested by the IT department on multiple computers. However, VPN software is more complex to install, configure and use than other software you may have used. You should be prepared to spend several hours installing, configuring and testing this software before using it effectively.

The instructions in this document describe how to install and configure the Check Point Virtual Private Network (VPN) client for use in accessing network resources on the college network via an unsecured network. Examples of unsecured networks include home cable modem or DSL connections, wireless networks (whether on campus or off campus), hotel rooms with broadband or wireless network access, etc. Anyone who wants to access campus network resources like file servers via an unsecured network **MUST** use a VPN connection. Access to these resources is denied by the firewall unless you use a VPN connection.

All employees of the college are permitted to download and install the VPN software on their home or other non-college owned computers. The software is available at no cost to you. The college has purchased licenses for the VPN server that will allow you to access the college network.

**DO NOT install this software on your college-owned computer. Contact the IT department for assistance if you want to use this software on a college-owned computer including laptops.**

## What is a VPN?

VPN stands for Virtual Private Network. VPNs came into use a few years ago as a way to create a secure connection using an unsecured network. The typical use for VPN software is to create a secure “tunnel” across the public internet.

The VPN software encrypts, or scrambles the data going into the tunnel at the remote end, perhaps an employee's home, a hotel room, etc. At the other end of the connection, the VPN server (sometimes called a VPN concentrator) un-encrypts the data and transmits it to the destination. Data traveling in the other direction is encrypted by the VPN server, transmitted through the tunnel and un-encrypted by the VPN client software.

The internet is a very public network. There are many places where a malicious user could possibly "sniff" or intercept network traffic. For many activities, this isn't that much of a problem. It isn't a major problem if someone intercepts data transmitted when you access a news web site or software vendor's web site. However, most users do not want an unknown third party to intercept sensitive data like credit card numbers, student data, online purchase information, banking or other financial information. Many types of data carry significant legal penalties if an employee allows them to be exposed. Examples would include student data that is exposed or compromised by an employee of the college.

Many internet users have accessed secure web sites when ordering products via web pages or using services like online banking. These secure web sites provide an encrypted connection between the web browser and the remote web server. A VPN connection encrypts ALL traffic between the VPN client and the VPN server. This makes it possible to offer services remotely that would otherwise be too risky to use over the public internet. For example, the college does not allow users to access network file shares on the Windows BCNET domain from remote locations. This is because doing so is a tremendous security risk and would allow malicious users to access large amounts of sensitive data. The VPN software makes it possible to access this sensitive data securely even over very unsecure networks like the internet.

### What To Do Before Installing the VPN Software

First, in order to access the VPN server and establish a secure connection, you must have an account that has been enabled for VPN access. To have your account enabled, contact the IT department. Note that VPN access uses your e-mail username and password to establish the VPN connection, not your BCNET username and password. In some cases, you may use the same username and password for both systems.

Second, you should verify that your home or other computer's connection to the internet is capable of successfully accessing the college network via the VPN connection. Consult the system requirements in the next section. Modem connections ARE NOT suitable for use with the VPN software.

Third, you should be aware that installing the VPN software on your home or other non-college-owned computer may cause problems with that computer. The

VPN software installation process will make changes to the network settings on the computer. These changes should not cause problems but it is possible that installing the VPN software will cause other programs on your computer to stop working or to work incorrectly. The IT department will attempt to help you debug these problems, if they occur, but the IT department has limited ability to assist you with problems on non-college-owned computers. In any case, you as the user assume all responsibility for any damages caused to your home computer if you install the VPN software on it.

Fourth, you should determine whether or not you have a need for installing the VPN software. If you are only accessing college e-mail servers from home, you do not need the VPN software. If you are accessing sensitive or other private data or you want to access any file shares on campus (including your personal "P" drive or departmental file shares) you MUST use the VPN software. The firewall will not allow access to these resources unless you use the VPN software.

### System Requirements for Using VPN Software

- 1) Windows XP Home or Professional - The VPN software is supported on Windows XP Home or Professional only. Windows 98 users must upgrade to Windows XP in order to use the VPN client software.
- 2) Broadband connection – Modem connections are not suitable for using the VPN software. You must use a broadband connection at home like DSL or cable modem. Most wireless networks should be capable of supporting the VPN connection as long as there is sufficient bandwidth between the wireless network and the college's network.
- 3) Up to date antivirus and anti-spyware software – By using the VPN software to connect to the college network, your home computer becomes a de facto extension of the college network. This means that viruses, trojans, spyware and other malicious software on your home computer can now infect the college network. Therefore, it is VITAL that you have up to date antivirus software on your home computer. If not, PLEASE do not install the VPN software until you have remedied this situation.

### Instructions for Installing VPN Software

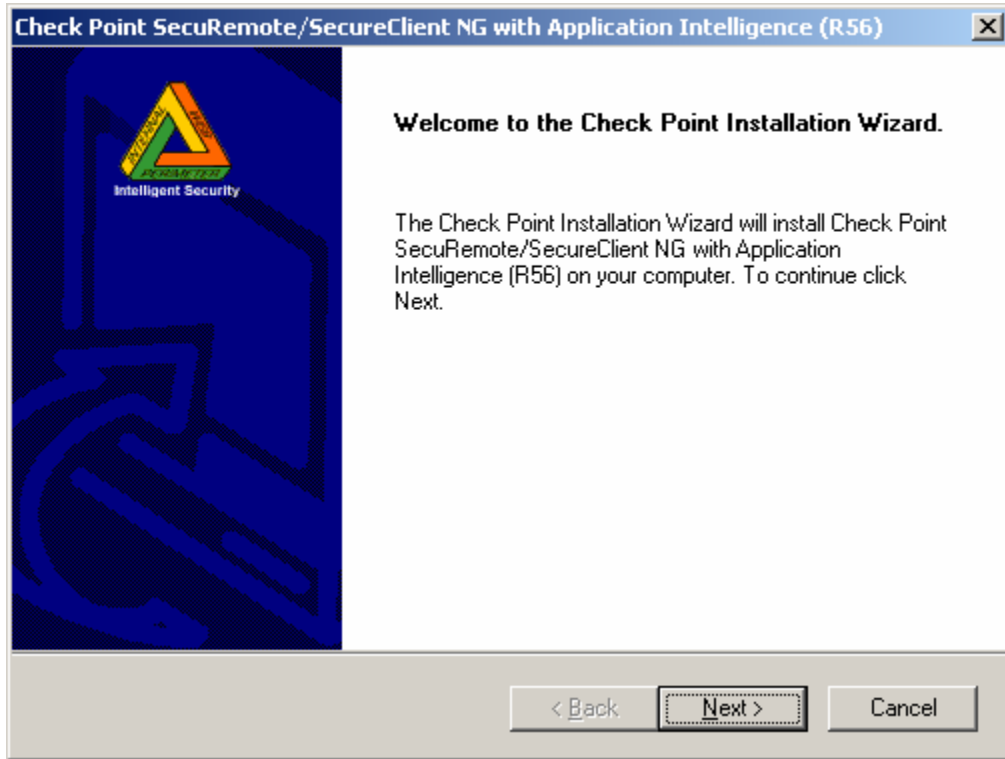
1) Download the VPN client software. The software and these instructions can be found on the Brazosport College IT support web site at:

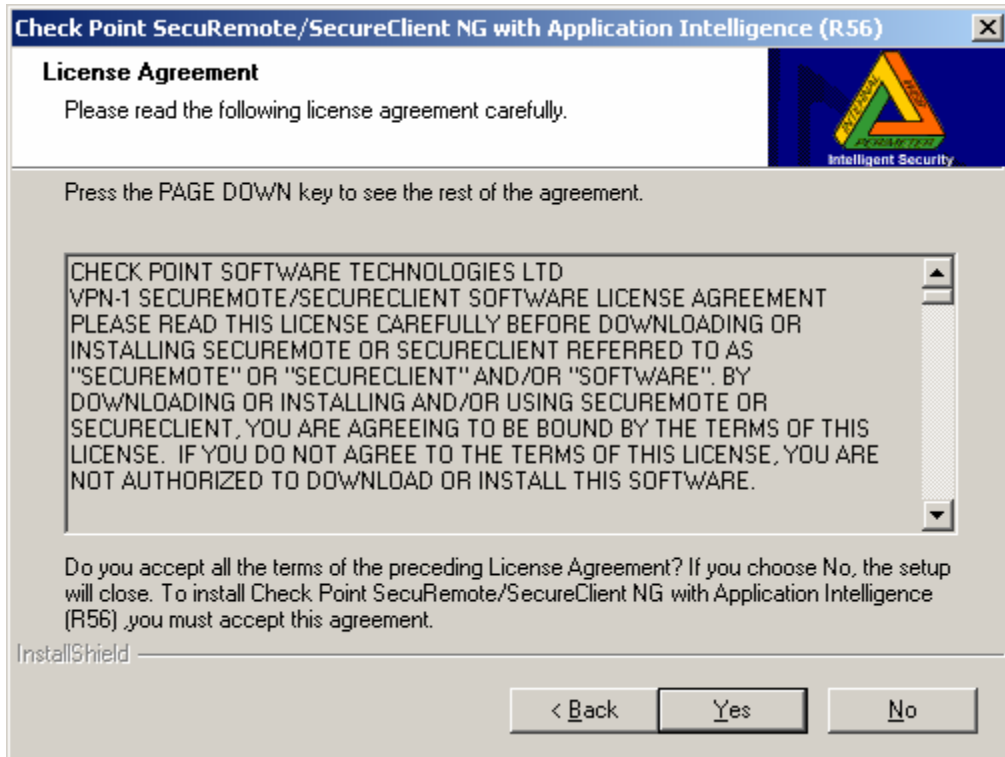
<http://www.brazosport.edu/it/vpn>

When you download the client software, be sure to save it to a local drive rather than a network drive. The VPN client installation process will terminate any open

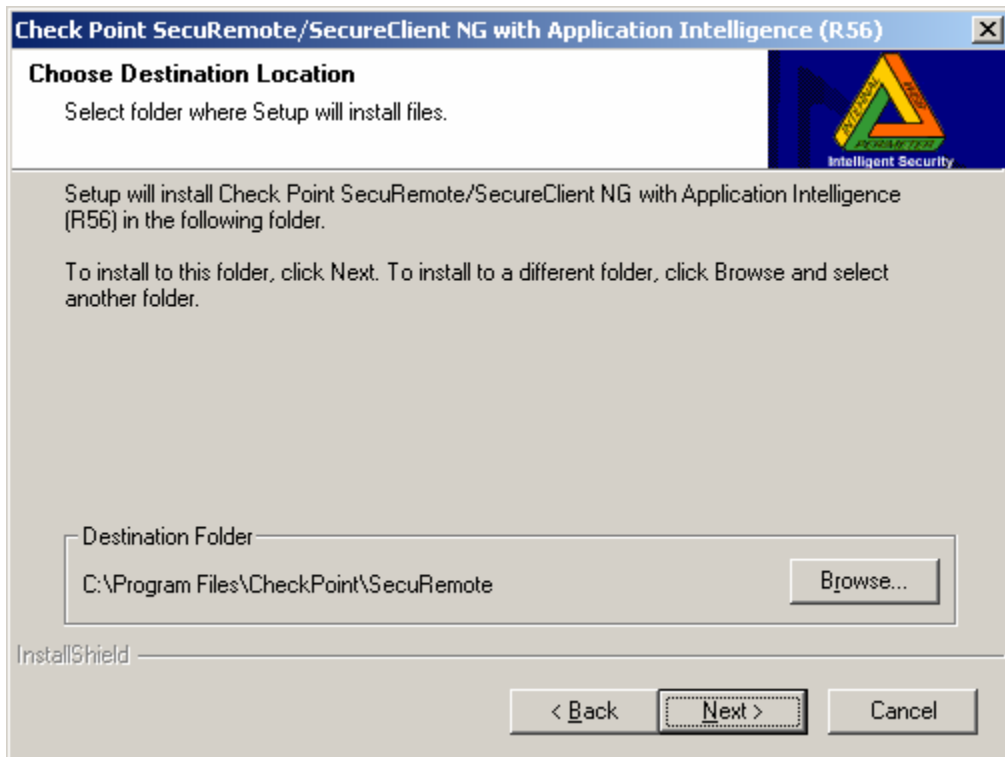
network connections that you have. This may result in problems with the installation if you are attempting to install from a file saved on a networked drive.

The installation process is a typical Windows software installation. Click Next to begin the installation. Then select Yes to accept the license agreement.

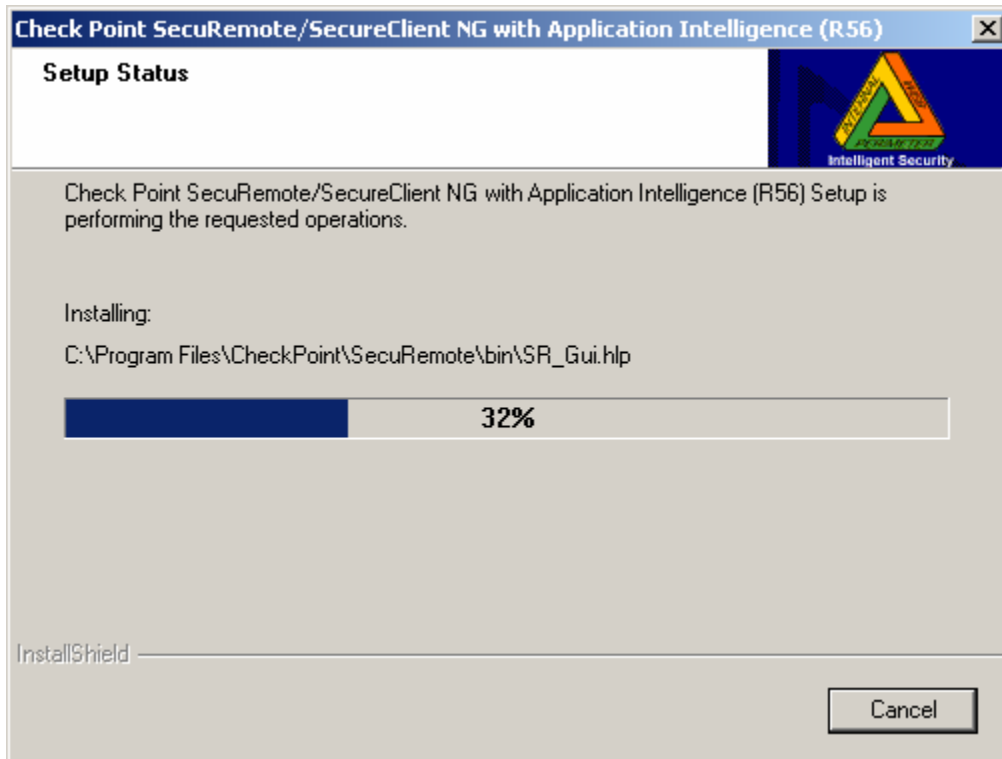




You can install the software in the default location or any other location you choose.

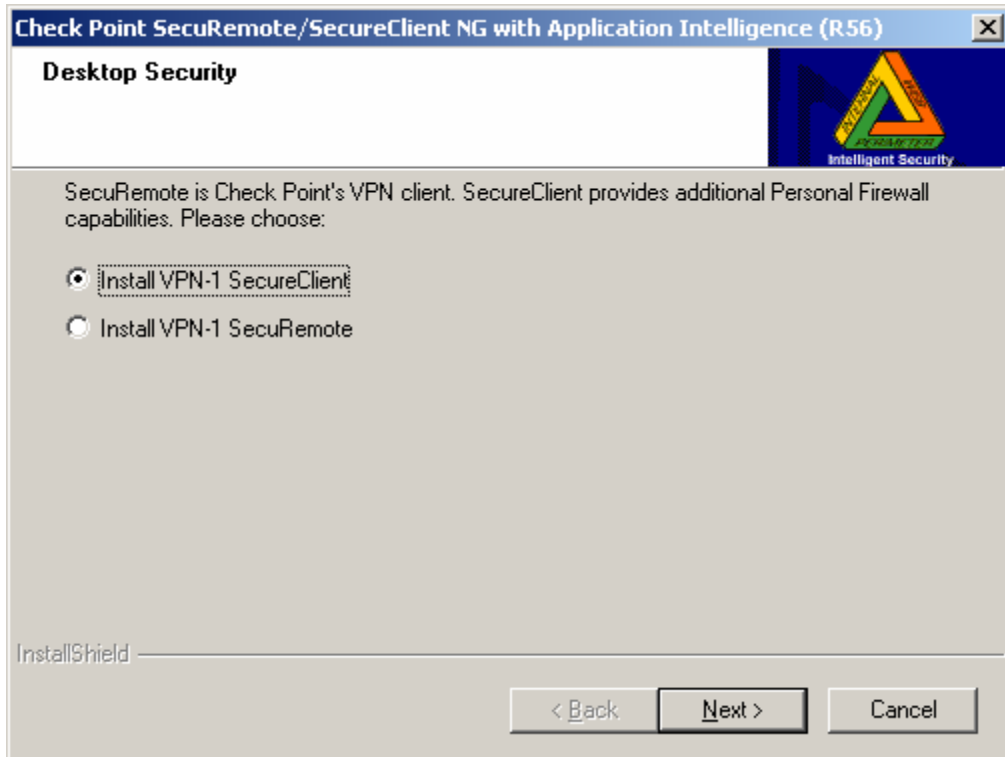


The installation process will then proceed to copy files.

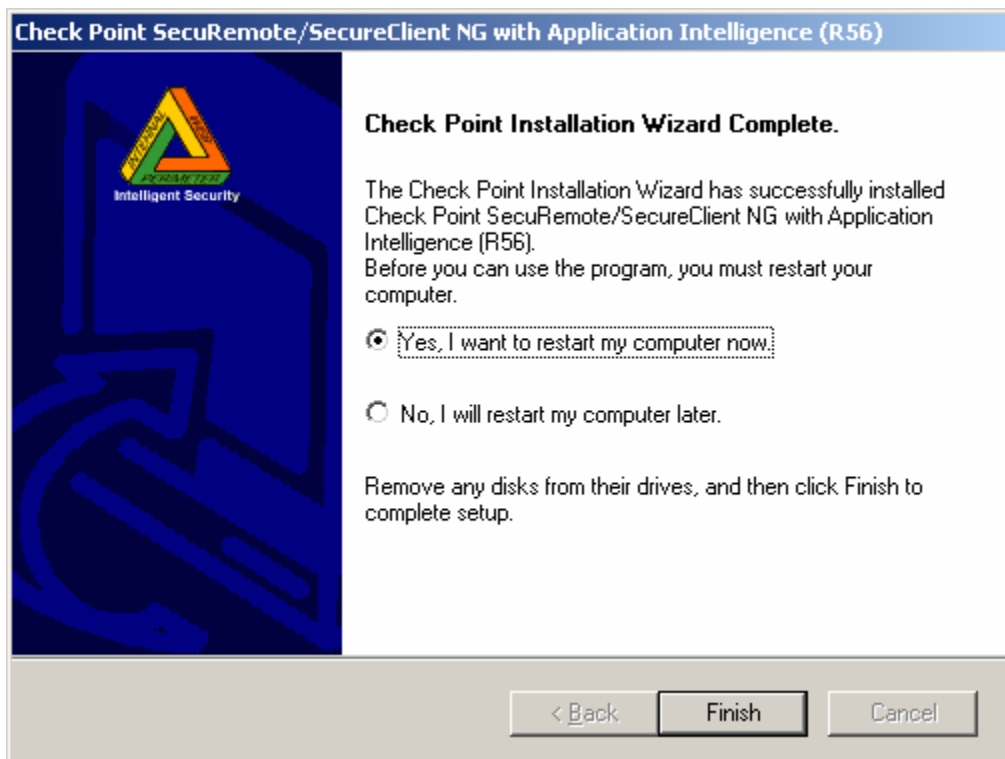


**This is a very important step.** You MUST choose the Install VPN-1 SecureClient option. The college firewall will not accept VPN connections using SecuRemote. When you make a connection to the college VPN server using SecureClient, it puts your computer into a special secure mode which prevents an attacker from attacking the college network via your network. For example, if you have a network at home, an attacker on that network could use your VPN connection to attack the college network. Your VPN connection bypasses the normal firewall rules so this could have severe consequences. SecureClient prevents this from happening.

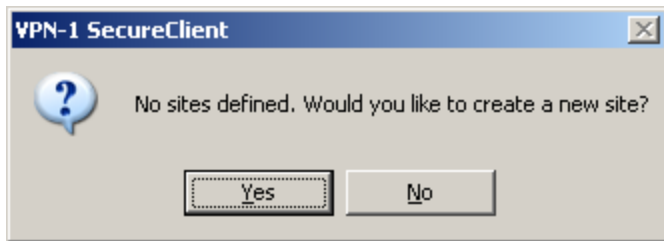
You should be aware that during a VPN connection with SecureClient other network services on the computer may not work due to this secure mode. These services will be restored when you discontinue your VPN connection to the college.



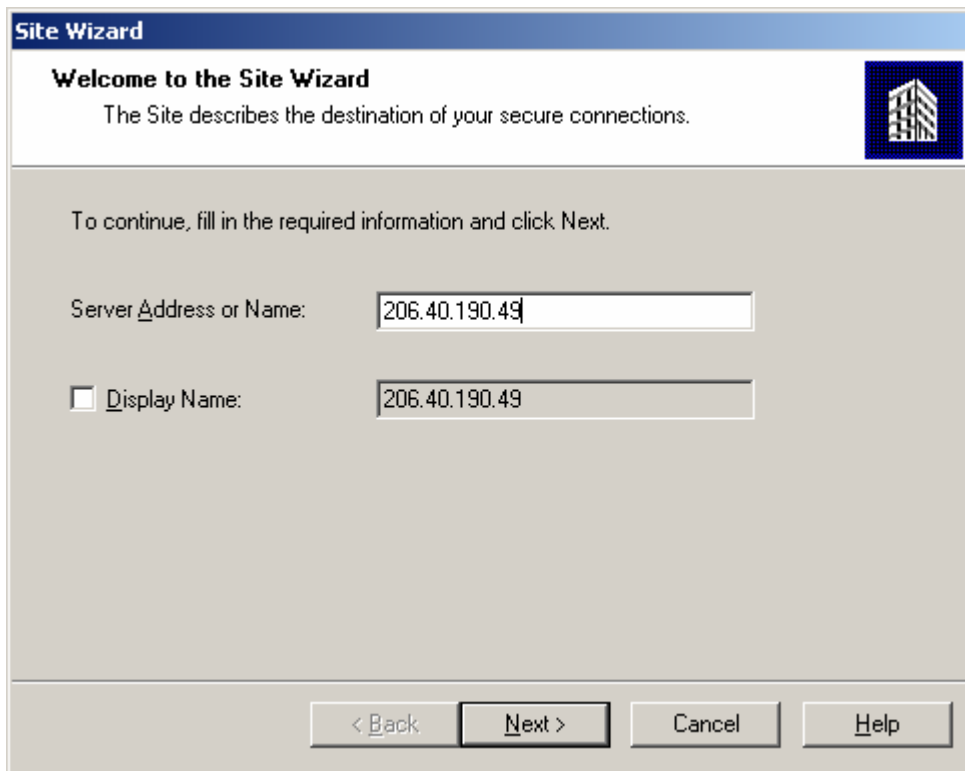
The installation process will complete. If you are ready to begin configuring the VPN software to make a connection, restart your computer.



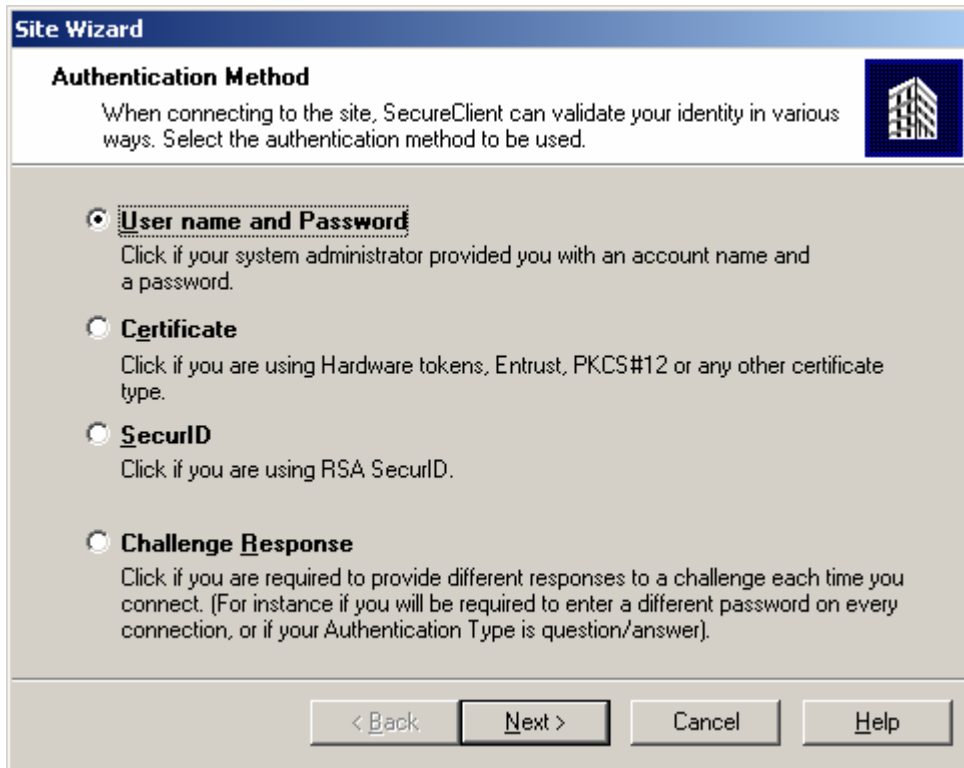
After you restart your computer, you are ready to begin configuring the VPN client software. In the system tray is a key icon, click it and you will be prompted to set up a new site since no sites should be defined. Select “Yes”.



In the Server Address or Name field, enter the IP address of our VPN server which is currently 206.40.190.49. You can optionally enter a display name by checking the Display Name box and entering text in the name field. A good display name might be Brazosport College VPN or something similar. This text will be displayed when you start the VPN client and want to make a connection.



We are using “User name and Password” authentication. By default, the correct button should be selected but you can change it if it is not the one selected.



The screenshot shows a dialog box titled "Site Wizard" with a blue header bar. Below the header, the title "Authentication Method" is displayed in bold. To the right of the title is a small icon of a building. Below the title, there is a paragraph of text: "When connecting to the site, SecureClient can validate your identity in various ways. Select the authentication method to be used." Below this text are four radio button options, each with a bold title and a descriptive paragraph:

- User name and Password**  
Click if your system administrator provided you with an account name and a password.
- Certificate**  
Click if you are using Hardware tokens, Entrust, PKCS#12 or any other certificate type.
- SecurID**  
Click if you are using RSA SecurID.
- Challenge Response**  
Click if you are required to provide different responses to a challenge each time you connect. (For instance if you will be required to enter a different password on every connection, or if your Authentication Type is question/answer).

At the bottom of the dialog box, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

In the User Details screen, enter your e-mail username and password. This may be different than your BCNET login used for campus network resources like logging onto your college computer.

**Site Wizard**

**User Details**  
Specify User name and password.

User name:

Password:

< Back   Next >   Cancel   Help

Accept the default of Standard connectivity on this screen.

**Site Wizard**

**Select Connectivity Settings**  
Select Standard or Advanced connectivity settings.

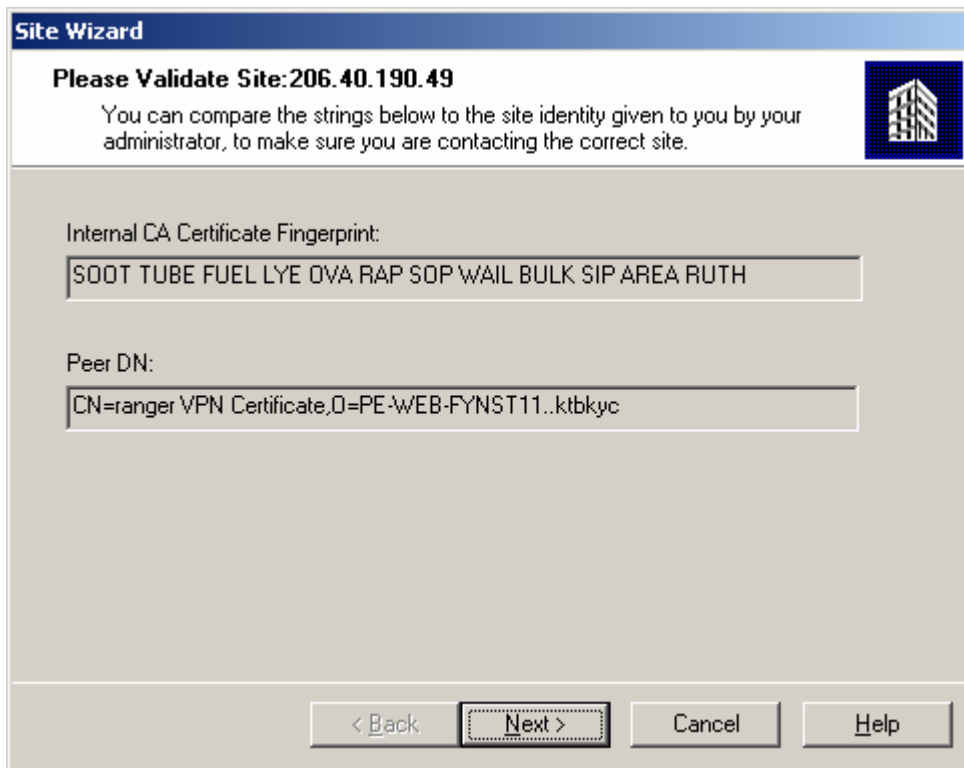
SecureClient will now obtain site information from your server.  
Click Advanced only if you experience networking difficulties using Standard settings.

**Standard**

**Advanced**

< Back   Next >   Cancel   Help

The VPN client software will now make an initial connection to the VPN server at the college in order to verify that you are attempting to connect to the right server. The CA Certificate validation screen asks you to verify that you are in fact connecting to the college's server rather than some other server. It is possible for someone to spoof the identity of a server so this step provides confirmation of the identity of the college's server. You should check to make sure that the information in both the Internal CA Certificate Fingerprint and Peer DN fields matches the information in the screen image below. If not, you should discontinue the configuration process and contact the college IT department for assistance.



The image shows a Windows-style dialog box titled "Site Wizard". The title bar is blue with the text "Site Wizard" in white. Below the title bar, there is a header section with a blue background containing the text "Please Validate Site: 206.40.190.49" and a small icon of a building. Below this, there is a paragraph of text: "You can compare the strings below to the site identity given to you by your administrator, to make sure you are contacting the correct site." The main area of the dialog box is light gray and contains two text input fields. The first field is labeled "Internal CA Certificate Fingerprint:" and contains the text "SOOT TUBE FUEL LYE OVA RAP SOP WAIL BULK SIP AREA RUTH". The second field is labeled "Peer DN:" and contains the text "CN=ranger VPN Certificate,O=PE-WEB-FYNST11..ktbkyc". At the bottom of the dialog box, there are four buttons: "< Back", "Next >", "Cancel", and "Help". The "Next >" button is highlighted with a dashed border.

**Site Wizard**

**Please Validate Site: 206.40.190.49**

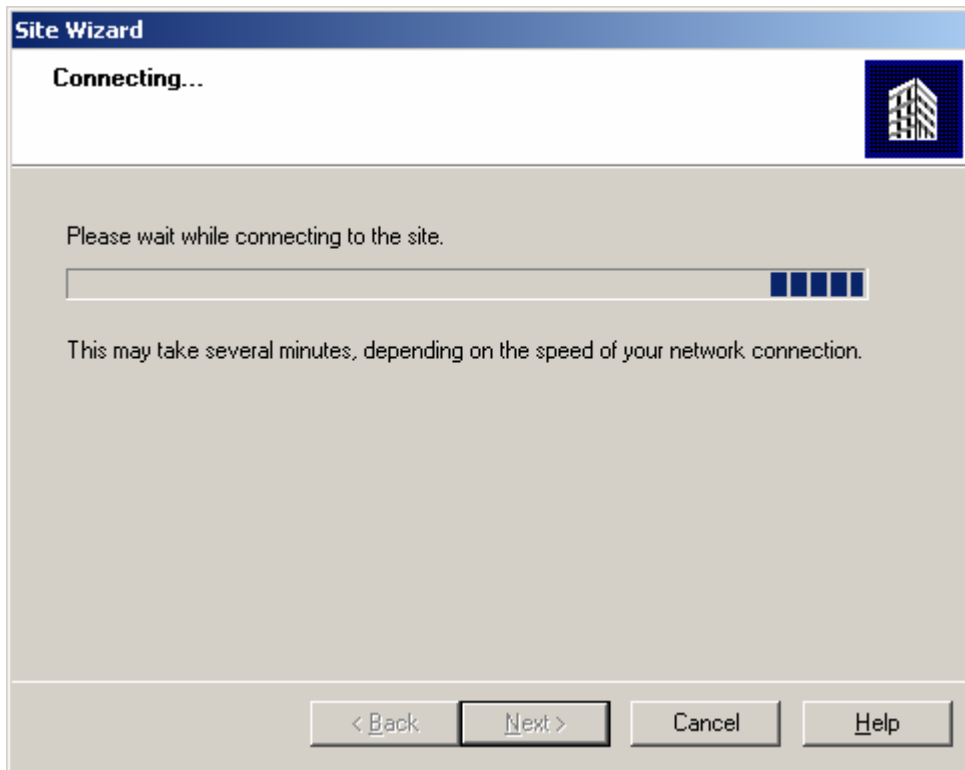
You can compare the strings below to the site identity given to you by your administrator, to make sure you are contacting the correct site.

Internal CA Certificate Fingerprint:  
SOOT TUBE FUEL LYE OVA RAP SOP WAIL BULK SIP AREA RUTH

Peer DN:  
CN=ranger VPN Certificate,O=PE-WEB-FYNST11..ktbkyc

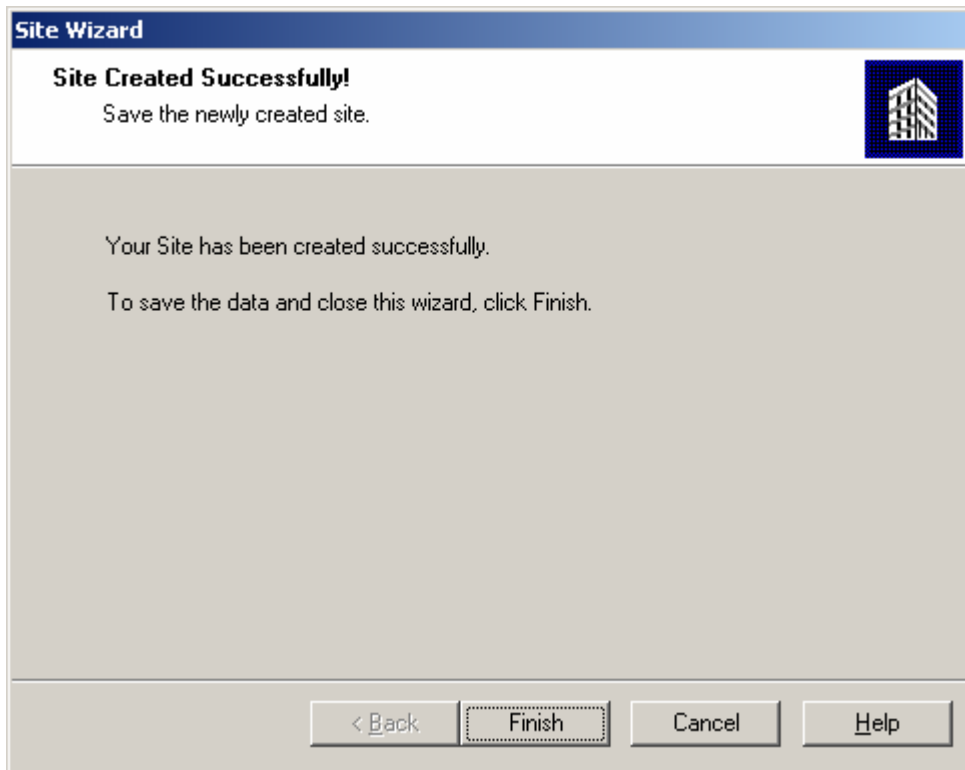
< Back   Next >   Cancel   Help

The VPN software will now make an initial attempt to contact the VPN server to actually establish a connection.

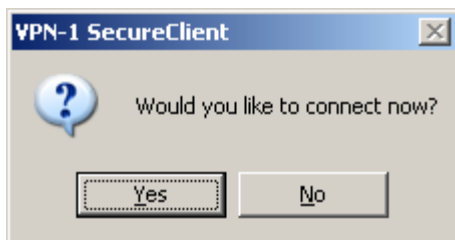


It really may take several minutes for this process to occur or to timeout. If, after waiting several minutes, you receive a message telling you it has failed, you should hit the Back button to retry it at least once. If it fails two or three times, you'll need to contact the IT department for assistance.

In most cases, you'll see the following screen indicating that you are ready to begin using the VPN software.

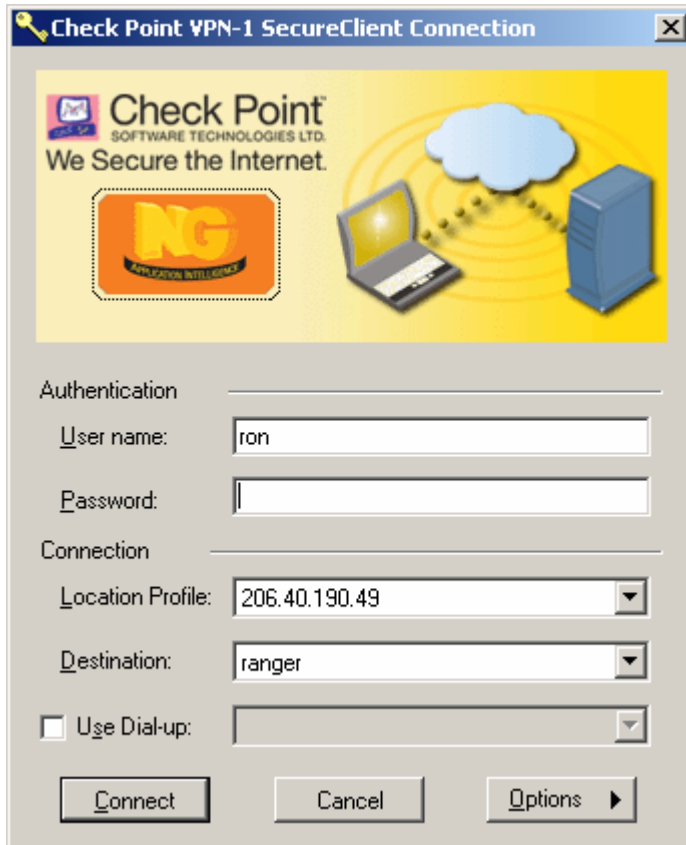


Click Finish to continue. Select Yes to make your first connection to the college VPN server.

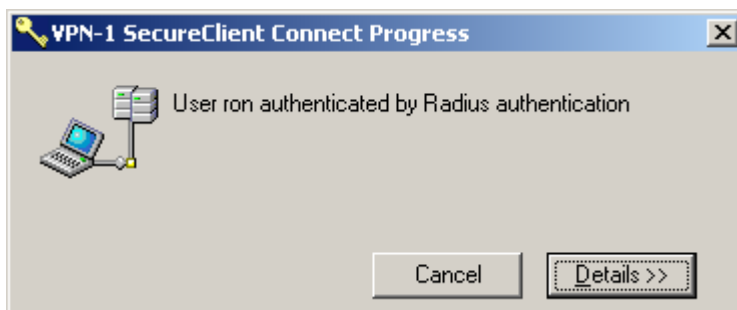


### Using the VPN Client Software

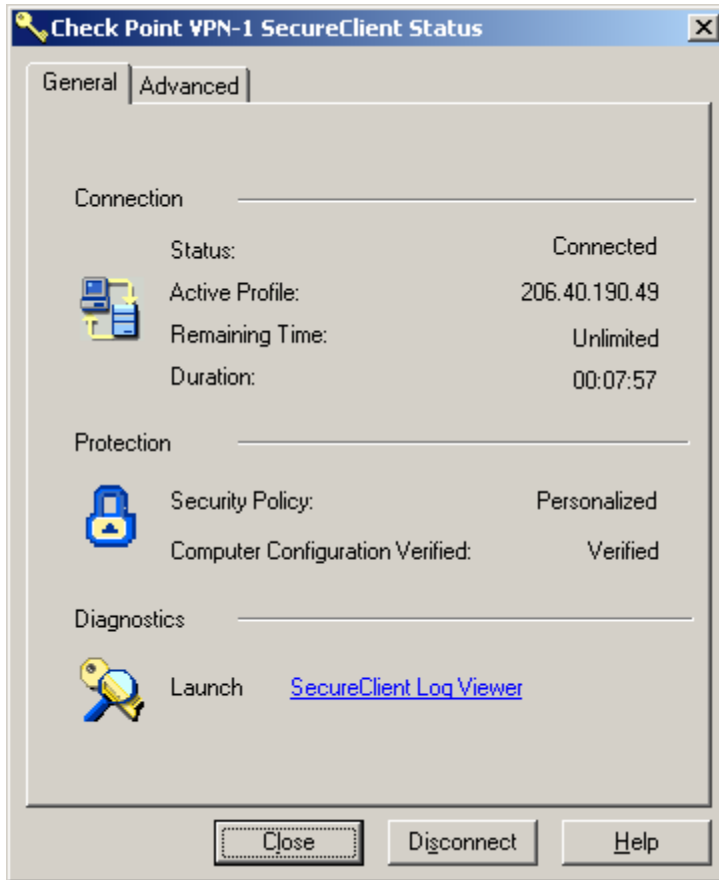
The screen below is how you will log onto the VPN server at the college when you want to access college network resources. You should enter your password in the field provided and select Connect.



If the connection is successful, you'll see a screen indicating that you've been authenticated. Note that it says you were authenticated by RADIUS authentication because the VPN server used a protocol called RADIUS to verify your username and password on the college's e-mail server cluster (gator7/gator8).

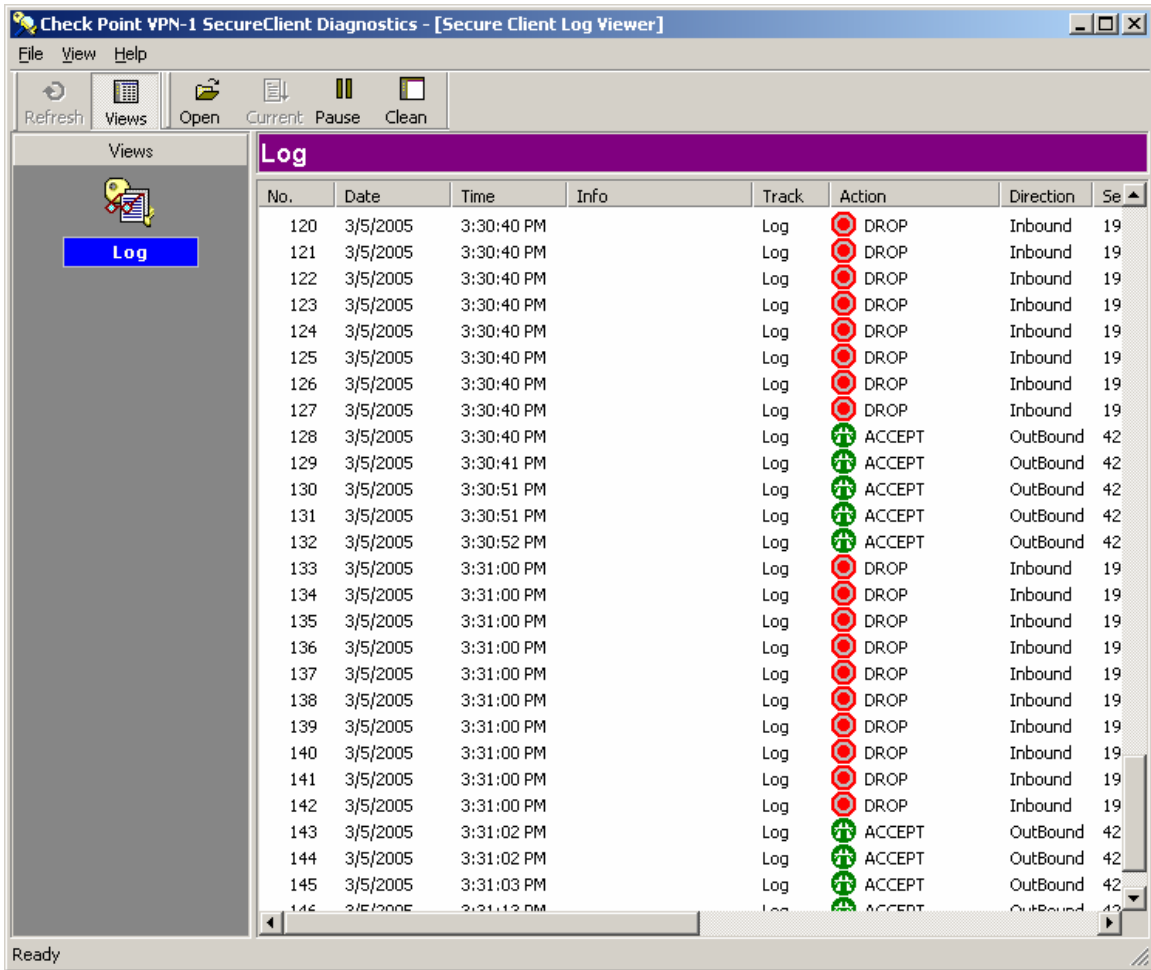


Place your cursor over the key icon in the system tray to see the status of your VPN connection. For more detailed status information, right click the key icon and select Status.

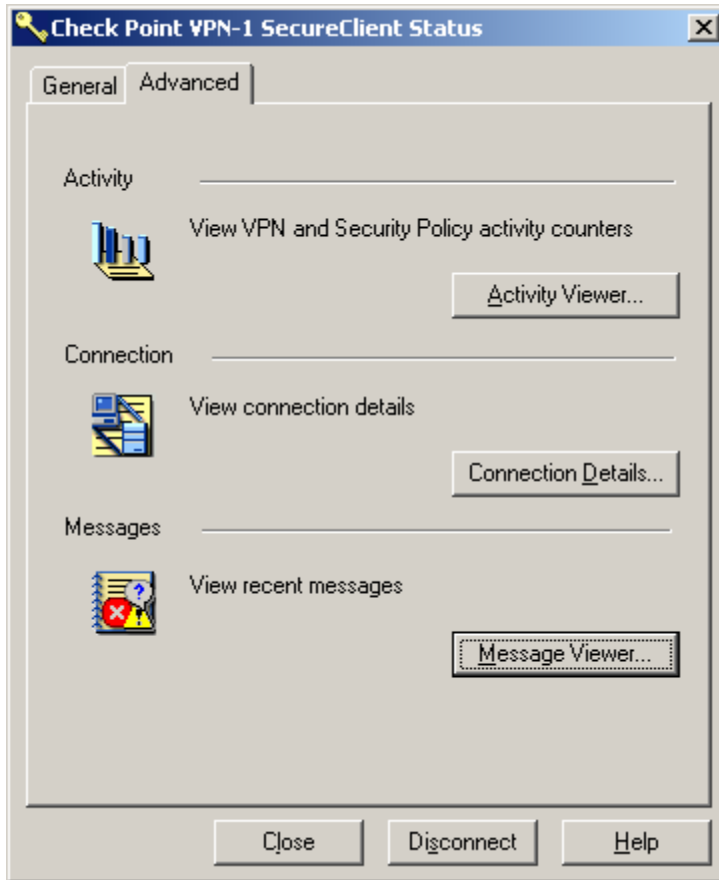


The status screen should show that your Status is Connected. If not, there is something wrong.

Note that you can access the Log Viewer from this screen or you can right click the key icon in the System Tray. Select Tools and then Launch SecureClient Log View.



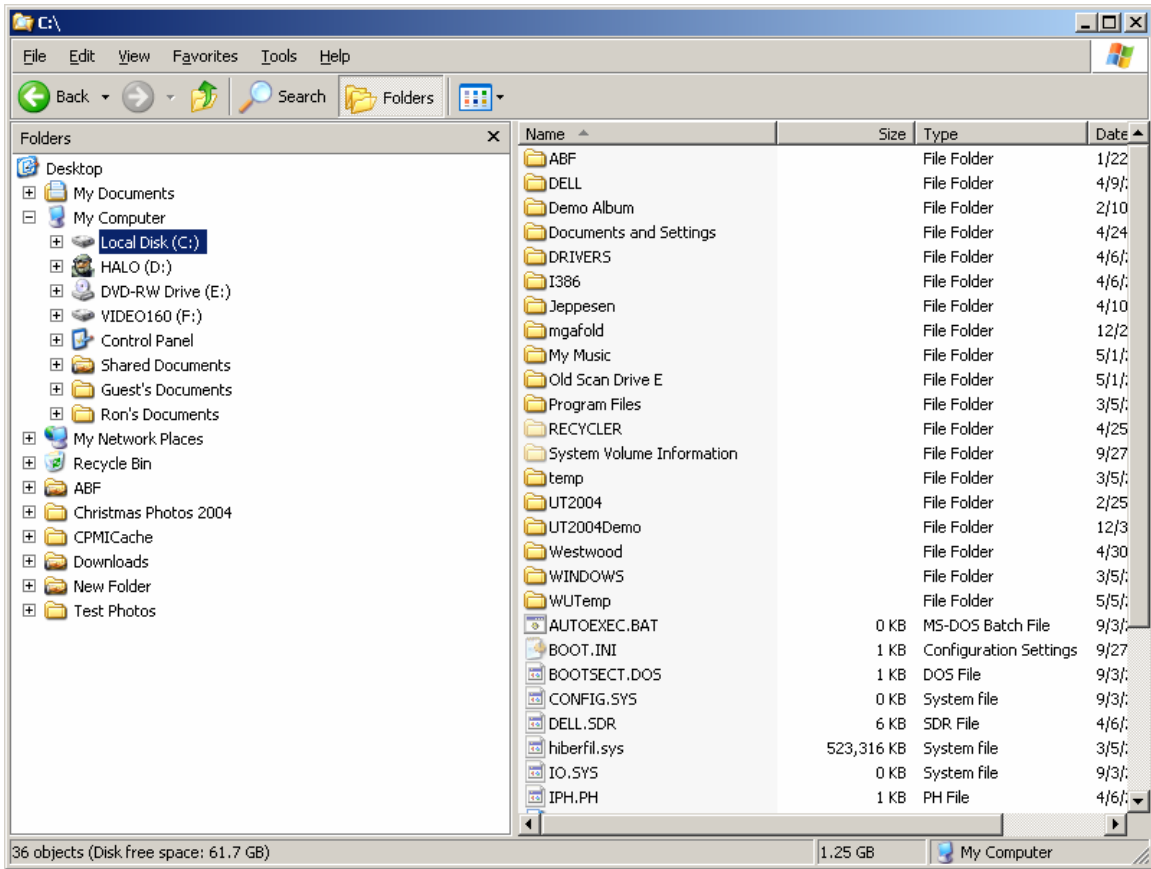
Selecting the Advanced tab in the Status window gives you additional details about your connection.



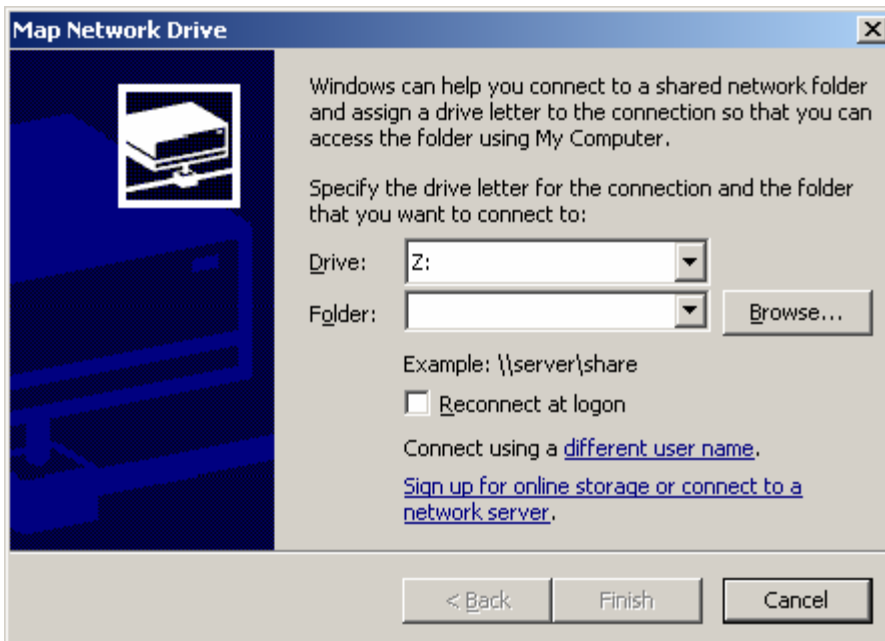
This information may be helpful in debugging problems if the connection does not work for some reason.

### Using College Network Resources Over Your VPN Connection

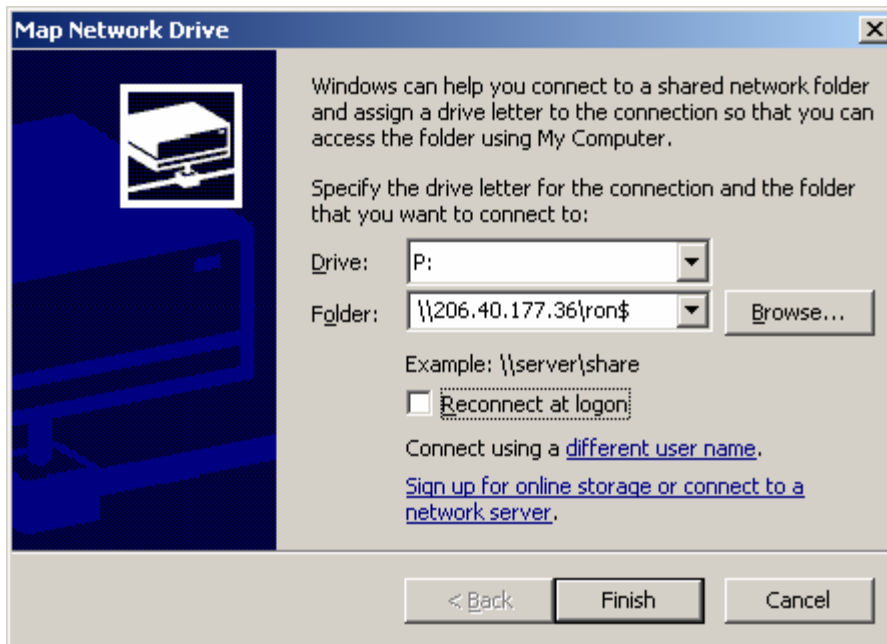
Assuming that the VPN connection is working, you should now be able to access campus file shares including your personal share or P drive. To map a drive, right click the Start button and select Explore.



On the Tools menu, select Map Network Drive.



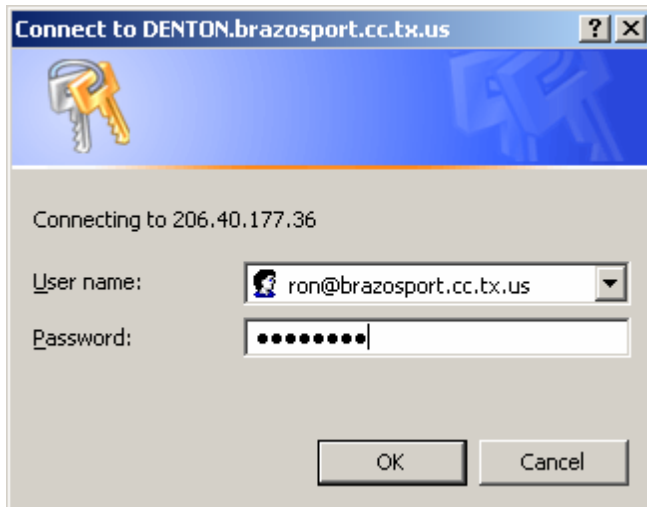
In the Drive dropdown box, select an unused drive letter like P:. In the Folder dropdown box, enter the IP address of the server you want to connect to as well as the share name. For most campus file shares, the server IP address is 206.40.177.36. The share name will be your BCNET account username unless you are trying to connect to your departmental file share. In the example below, the BCNET user Ron is mapping the P: drive to his personal share on the file server. You should change the username Ron to your own username.



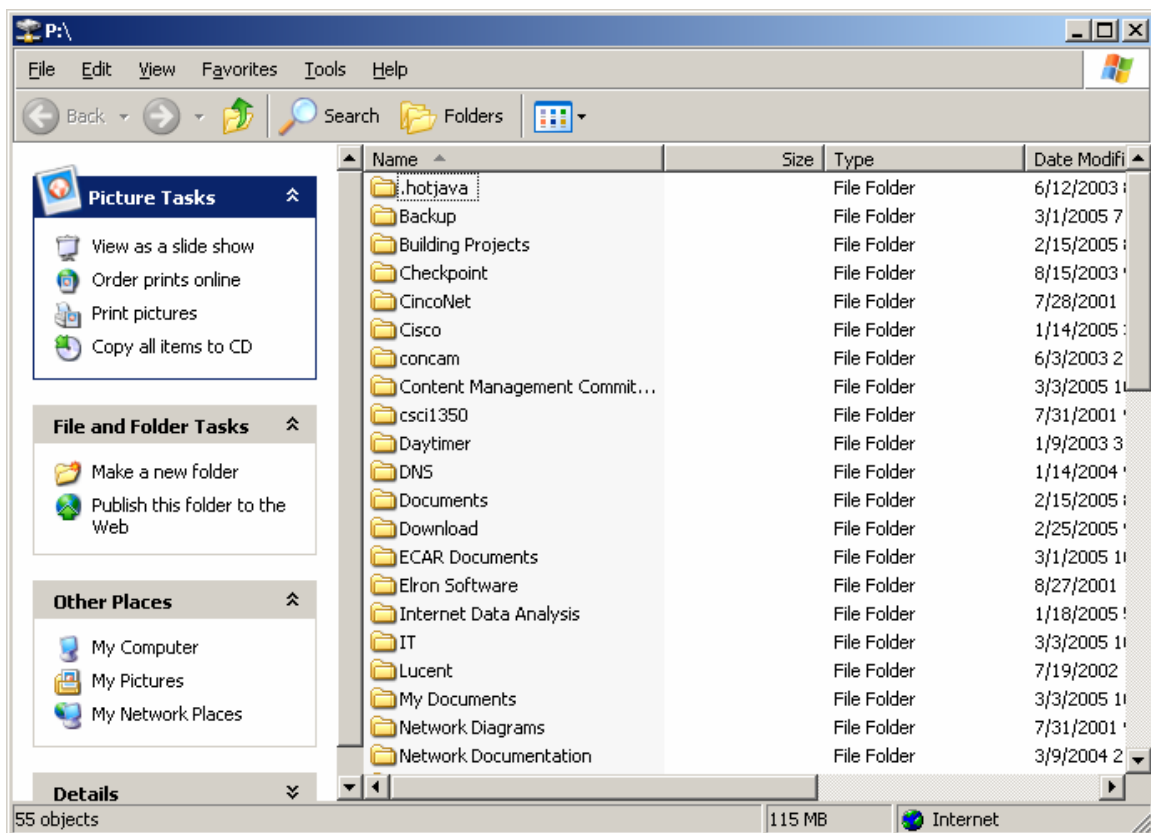
You probably should not check the “Reconnect at logon” check box. If you do, your computer will attempt to map this share every time you restart or logon. If your VPN connection is not active, the VPN client will prompt you to connect. Click Finish to map the drive.

You should now see a dialog box asking you to enter your username and password. Note that the example says denton.brazosport.cc.tx.us but you may see tyler.brazosport.cc.tx.us or other server names depending on which file share you are attempting to map your drive to.

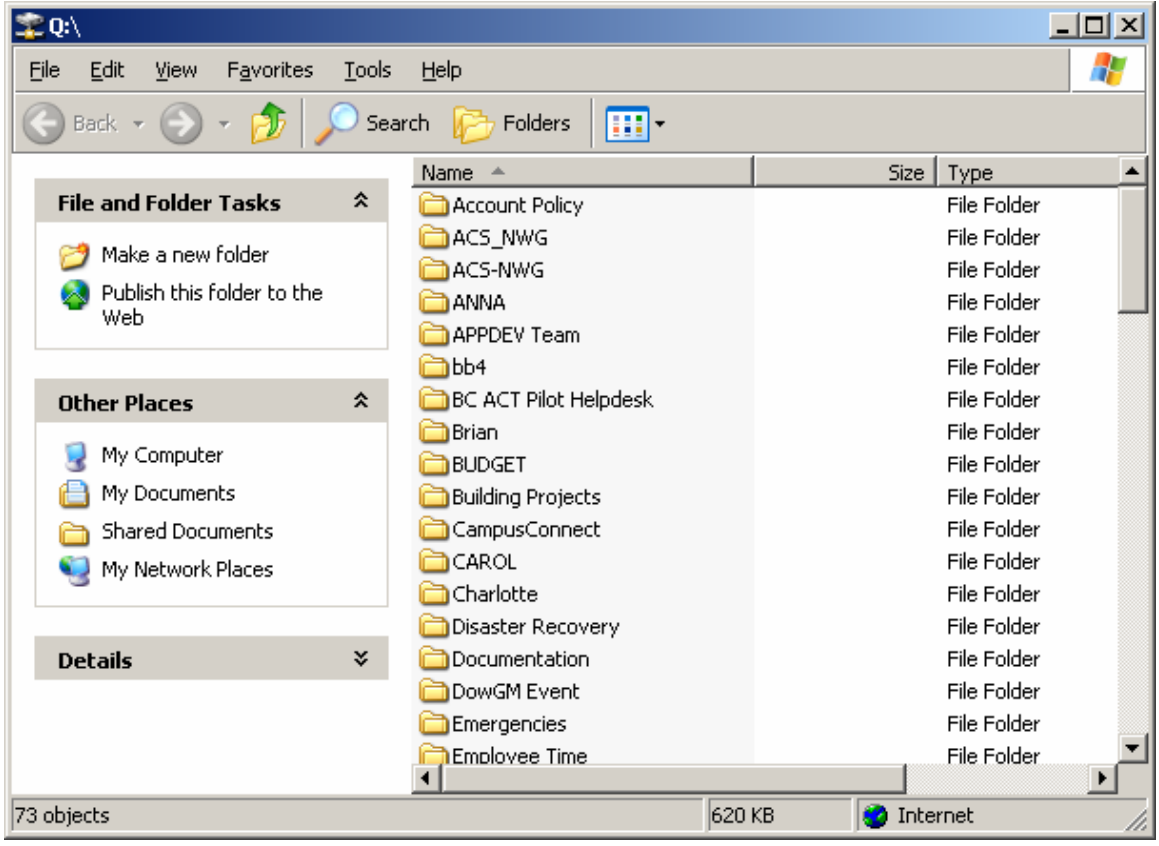
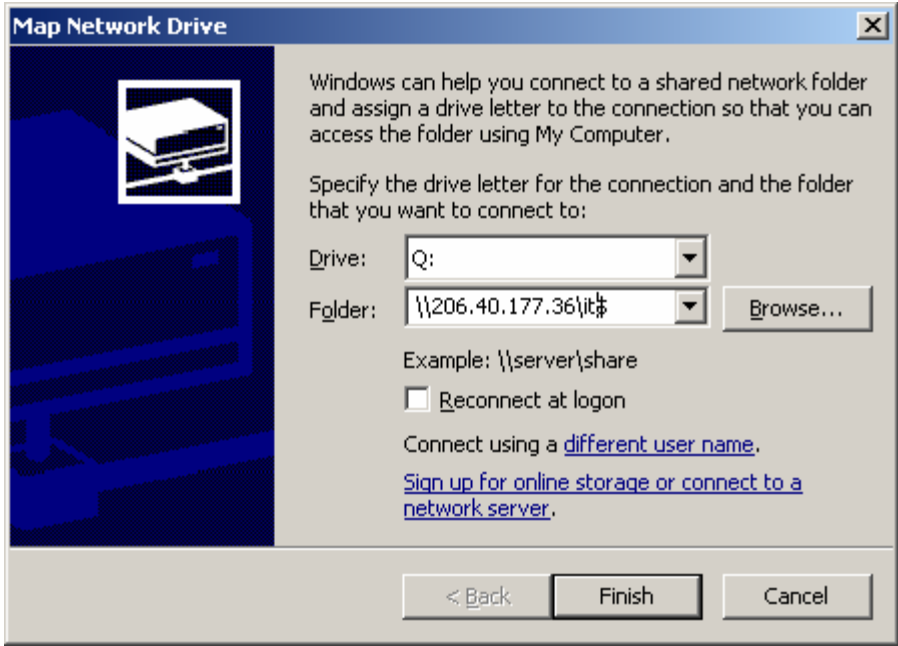
In the username field, enter your BCNET username followed by @brazosport.cc.tx.us. Enter your BCNET password in the password field and hit enter or click the OK button.



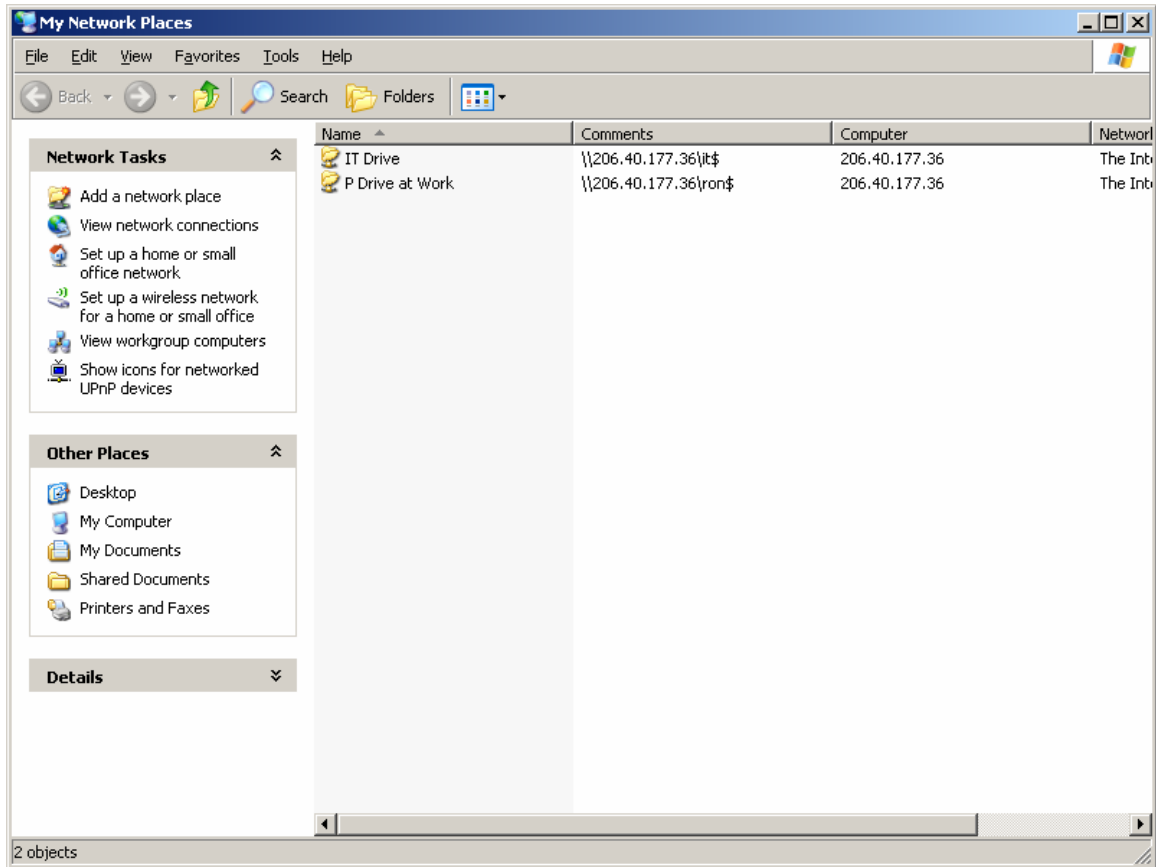
If everything worked, you should see a Windows Explorer window popup showing the drive letter you have mapped to as well as the folders in the share.



Once you've mapped a drive, you can map additional drive letters without having to enter your username and password again until you log off or reboot. In the example below, the user is mapping drive letter Q: to the IT department share on the same file server.



There is another way to access network resources in Windows XP by selecting My Network Places from the Start menu. Selecting “Add a network place” brings up the Add Network Place Wizard. Although it is possible to access your file shares using this wizard, the IT department has found that the performance is much slower than doing it by mapping the drive as described above. It may be so slow as to be unusable and may cause data loss. The IT department highly recommends that you do not use the wizard.



Now that you have mapped a drive, you should be able to use the files and folders on it just as if you were on campus using your college-owned computer. You can open files, copy files, edit files, etc. You can even access networked printers at the college and print your documents directly to them.