

# Using the TCNJ SSL VPN

## Introduction

The College has implemented Juniper Networks' SSL VPN solution, NetConnect, to provide an easy to use VPN for the College community. The SSL VPN can be used to securely access on-campus resources from anywhere on the Internet.

## Requirements

- TCNJ login and password (*e.g. your email login and password*)
- Windows XP/2000, MacOS X, or Linux (*while the SSL VPN works with Linux, the College is not providing support for Linux users at this time*)
- Java Virtual Machine 1.4.2 or higher
- A web browser (*the College has tested IE 6, Firefox 1.0+ and Safari*)

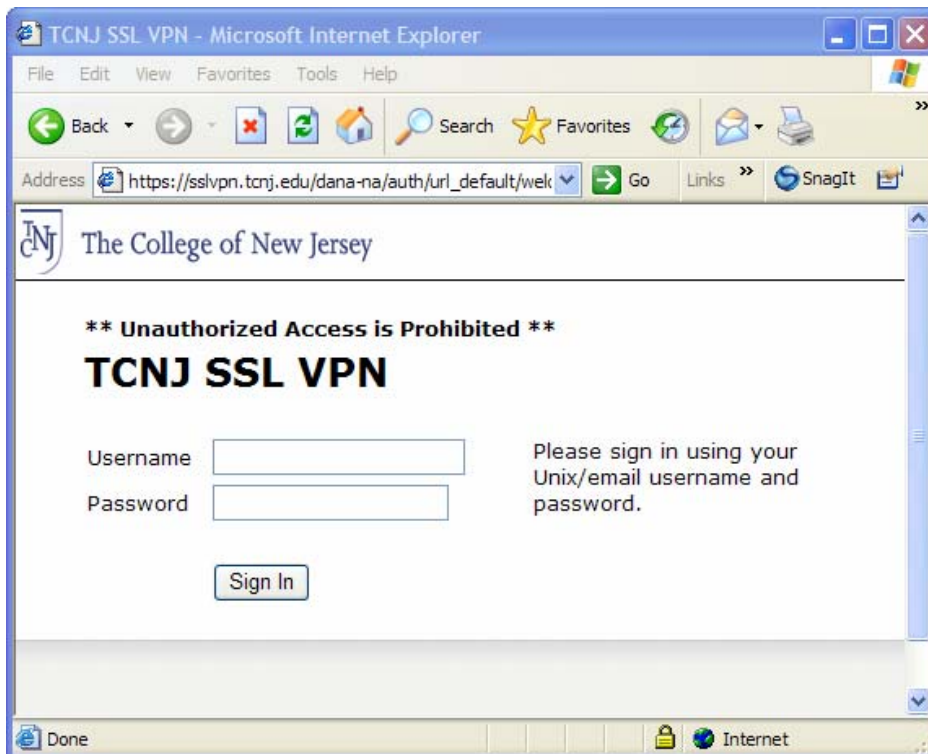
**Note that Windows 95/98/Me as well as Mac OS 9 are not supported.**

## Getting Started

Open your web browser and point it to the following URL

<http://tcnjvpn.tcnj.edu>

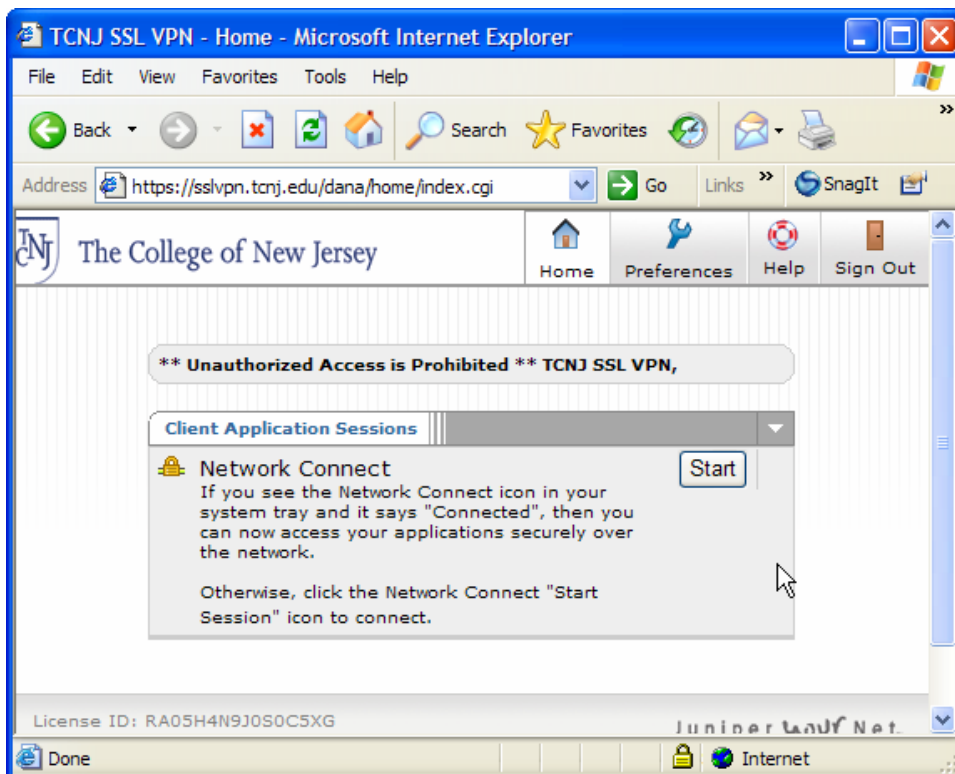
You should see the login page below.



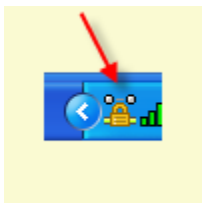
Enter your Unix/email login name and password in the respective boxes and click the “Sign In” button.

The first time you use the SSL VPN, it will download and install a small VPN client on your computer. You may need to click through some warning boxes that pop-up. It is safe to agree to continue. The next time you use the SSL VPN from the same computer, the process will go much quicker since you won’t have to install anything.

After the SSL VPN successfully starts up, you should see the following in the web browser.



You should also see the following icon on the system tray in the lower right hand side of your screen. We refer to this as the “little alien” icon, since it looks like a little alien even though it is supposed to be a lock icon over a network cable. The two dots above the lock will blink when there is network traffic going over the SSL VPN.

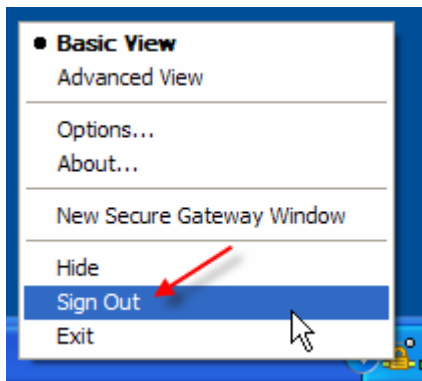


If you don’t see this icon, you should click the “Start” button on the Network Connect page that is currently displayed in your browser.

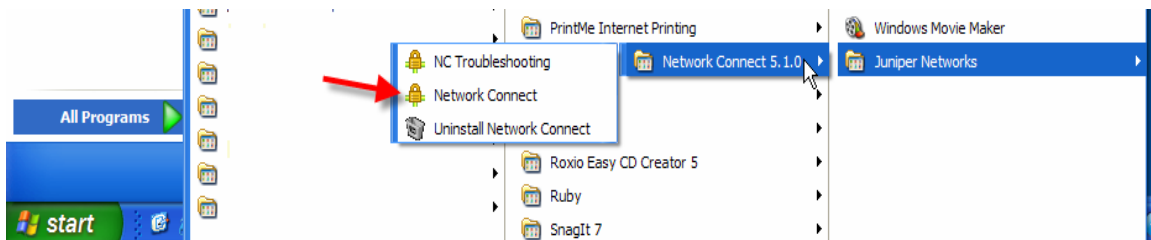
Once connected, you should be able to access most on-campus resources and any resource the traditional VPN was able to access. The SSL VPN uses “split tunneling” which means that when you access TCNJ systems, it will direct the traffic over the SSL VPN. If you are accessing a non-TCNJ system (e.g. [www.google.com](http://www.google.com)), your connection will not go over the SSL VPN but will instead go directly from your computer to the site you want to visit. With split tunneling, there is no bandwidth penalty for browsing non-TCNJ sites while being connect to the TCNJ SSL VPN. Once the SSL VPN is started, you do not need to keep the web browser open for the SSL VPN to continue to function.

It should be noted that there are timeout values set for the SSL VPN. If no traffic passes over the SSL VPN for 60 minutes or more, the SSL VPN will automatically end your session (idle timeout). In addition, the maximum amount of time you can be on the SSL VPN in any single session is 24 hours (max session length). So, if you tend to always be connected, you will need to re-login at least once each day.

When you are done using the SSL VPN, you should sign out. You can do this by right-clicking on the icon in the system tray and choosing “Sign Out” from the pop-up menu.



When you want to start another SSL VPN session, you can either point your browser back to <http://tenjvpn.tcnj.edu/> or launch it from your Start menu.



### **Getting Started on MacOS X and Linux**

While these instructions have focused on the Microsoft Windows platform, the basic concepts should work on MacOS X and Linux desktops. Both require a Java Runtime to be installed (minimum 1.4.2 but recommend 5.0/1.5.0). Safari on the Mac should work fine. TCNJ IT is currently unable to provide support for home Linux systems.

## **Troubleshooting**

While testing the SSL VPN, the testers ran into a few issues. If you run into problems getting the SSL VPN to work, one of these solutions may solve your problem.

**Problem #1:** Your browser hangs after logging in, but before or while the SSL VPN client is being installed.

**Solution #1:** Quit the browser and go into your Start > Control Panel > Add/Remove Programs section. Look for “Juniper Network Network Connect” and remove it if it exists. Also, remove any “Java 2 Runtime Environment” or “J2SE Runtime Environment” items. Now go to <http://www.java.com/> and click on the “Download Now” icon. After you install the latest Java Runtime, restart your browser and try the SSL VPN again.

**Problem #2:** I still can't seem to get the SSL VPN client to automatically download and install.

**Solution #2:** You can try manually downloading and installing the client. Go back to the SSL VPN web page and click on the “Manual SSL VPN Client Install” download link. Select the Network Connect client appropriate for your operating system.

**Problem #3:** You were able to login to the SSL VPN and the SSL VPN client seemed to install okay, but it just doesn't work.

**Solution #3:** Make sure the SSL VPN icon is in the system tray and is not greyed-out. If it isn't in the system tray, try clicking the “Start” button on the Network Connect web page. If that doesn't work, check to make sure you don't have any other VPN clients installed such as CheckPoint VPN client, Cisco VPN client or Netscreen VPN client. Other VPN clients may interfere with the SSL VPN client operations. Either disable them or use the Add/Remove Program option in the Control Panel to delete the other VPN clients.

**Problem #4:** I keep getting disconnected from the SSL VPN after leaving my machine for a while.

**Solution #4:** There are two timeout values for the SSL VPN. One is an “idle timeout” which is set for 60 minutes. If no traffic passes over the SSL VPN for 60 minutes, it will end your session. You should get a pop-up about 5 minutes prior to warn you. The other timeout value is a “max session length.” This is the maximum amount of time you can be signed onto the SSL VPN for a given session. This is set to 24 hours. After 24 hours, the SSL VPN will end your session, and you will need to login again. It should also warn you about 5 minutes prior.