

Accessing Network Resources Using *Network Connect Mode* on the Secure Remote Access Service

Overview

Computing Services and Systems Development has implemented a secure remote access solution to permit University students, faculty, and staff to access restricted University online resources. The Secure Remote Access Service allows members of the University community to remotely and securely access a wide range of network resources from Windows applications.

Before you connect to the service, your computer will be scanned by a **Health Check**. The Health Check will check your computer for the following items:

- Operating system is Windows XP with Service Pack 2 or Windows Vista. (Macintosh and Linux systems are not being checked at this time.)
- Microsoft Automatic Software Update turned on so you can receive the latest security patches.
- The latest version of Symantec Anti-Virus with LiveUpdate turned on so you can receive the latest virus definitions.
- A software firewall must be installed and enabled on your computer.

If your computer fails the Health Check for any reason, you will not be permitted to connect to the University's network resources until the failure is resolved.

The Secure Remote Access Service provides different modes of operation depending on user requirements. This document explains how to use the Network Connect Mode to access University resources. An example of such an application is the KeyAccess license compliance software used in the Faculty Computing Program. Network Connect Mode is for Windows, Macintosh, and Linux computers. To arrange to have Network Connect Mode configured for your computer, contact the Technology Help Desk at 412 624-HELP [4357]. Please see the "Additional Capabilities" section of this document for more information about the capabilities of the Secure Remote Access Service.

Connecting to the Secure Remote Access Service

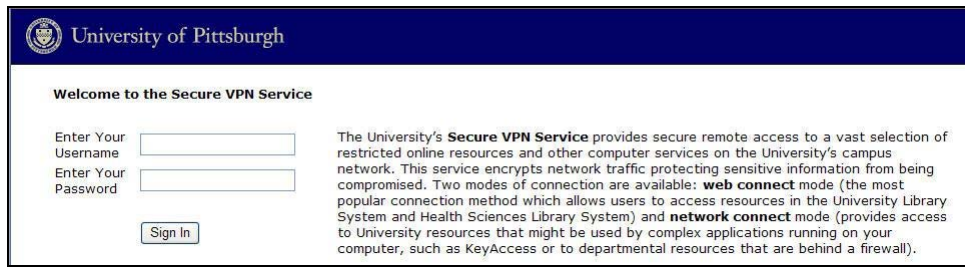
To connect to the Secure Remote Access Service, complete the following steps.

1. Open a Web browser such as Internet Explorer, Netscape or Firefox. In the address bar at the top of the screen, type <https://sremote.pitt.edu> and then press the **Enter** key.

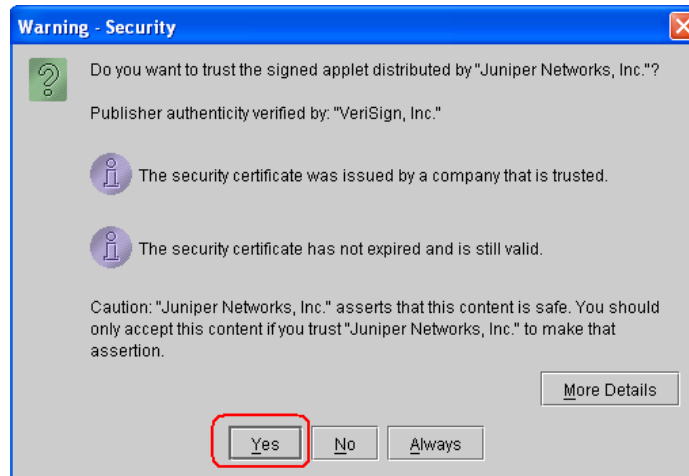
Note: The following operating system and web browser combinations have been confirmed as compatible with Secure VPN. If your operating system or web browser is NOT on the following list, but still works with Secure VPN, please be advised that it is not guaranteed to be compatible with future service upgrades.

Windows XP with SP2 or Windows Vista	Internet Explorer 6.0 or 7.0, Firefox 2.0 with Sun JRE 1.5
Mac OS X (10.4)	Safari 2.0 running Java 1.5

2. You will be prompted to sign in to the Secure Remote Access Service. Type your University Computer Account username and password into the appropriate boxes on the screen.
3. Click the **Sign In** button.

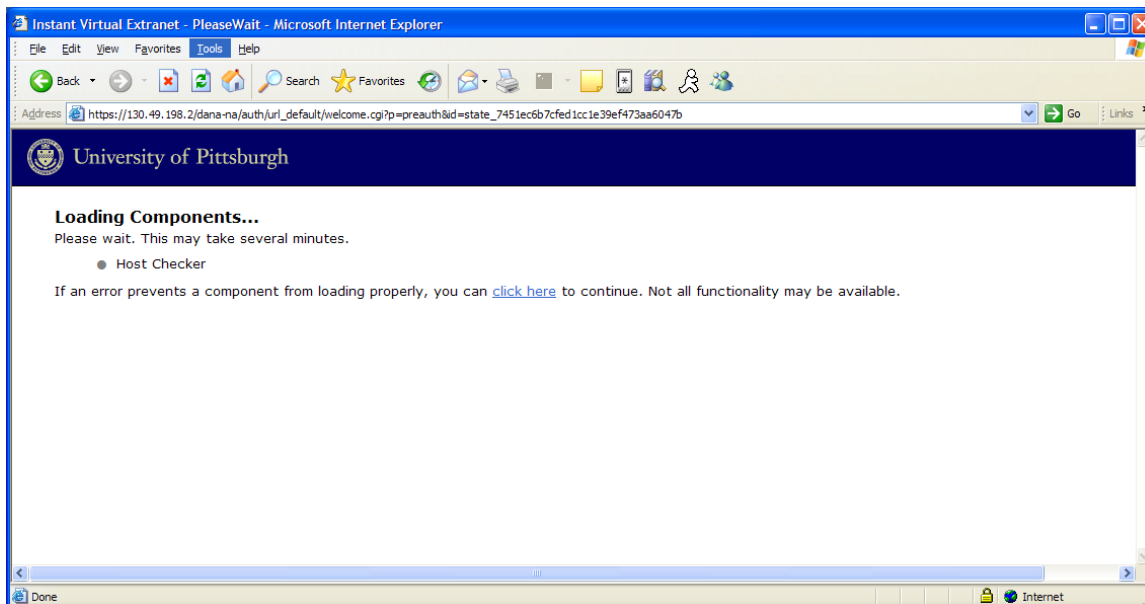


Note: After you click the **Sign In** button you may see a security warning window asking if you want to trust the applet distributed by Juniper Networks, Inc. If this window displays, click the **Yes** button to proceed.



Health Check Screen

After you click the **Sign In** button, you will see the Host Checker screen. This screen indicates that the Secure Remote Access Service is determining whether certain computer security features are active on your workstation. This process may take a few minutes to complete.

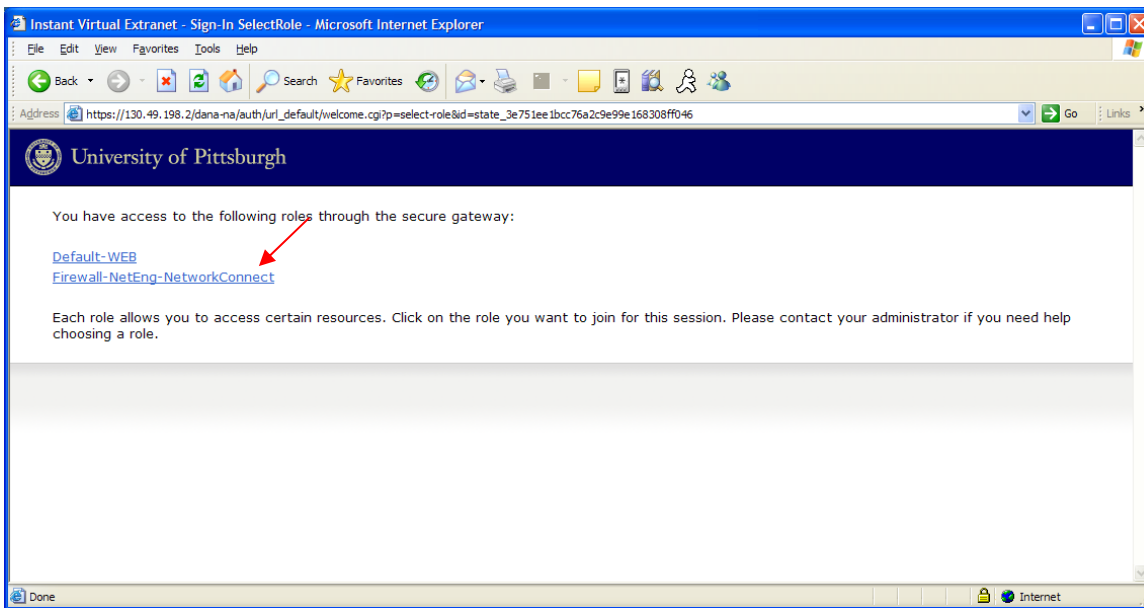


Role Selection Screen

After signing in, most Network Connect users will be presented with a menu screen listing “roles” that are available to them. The “Default-WEB” role is the basic Secure Remote Access Service mode available to all users. It provides Web-only access to licensed

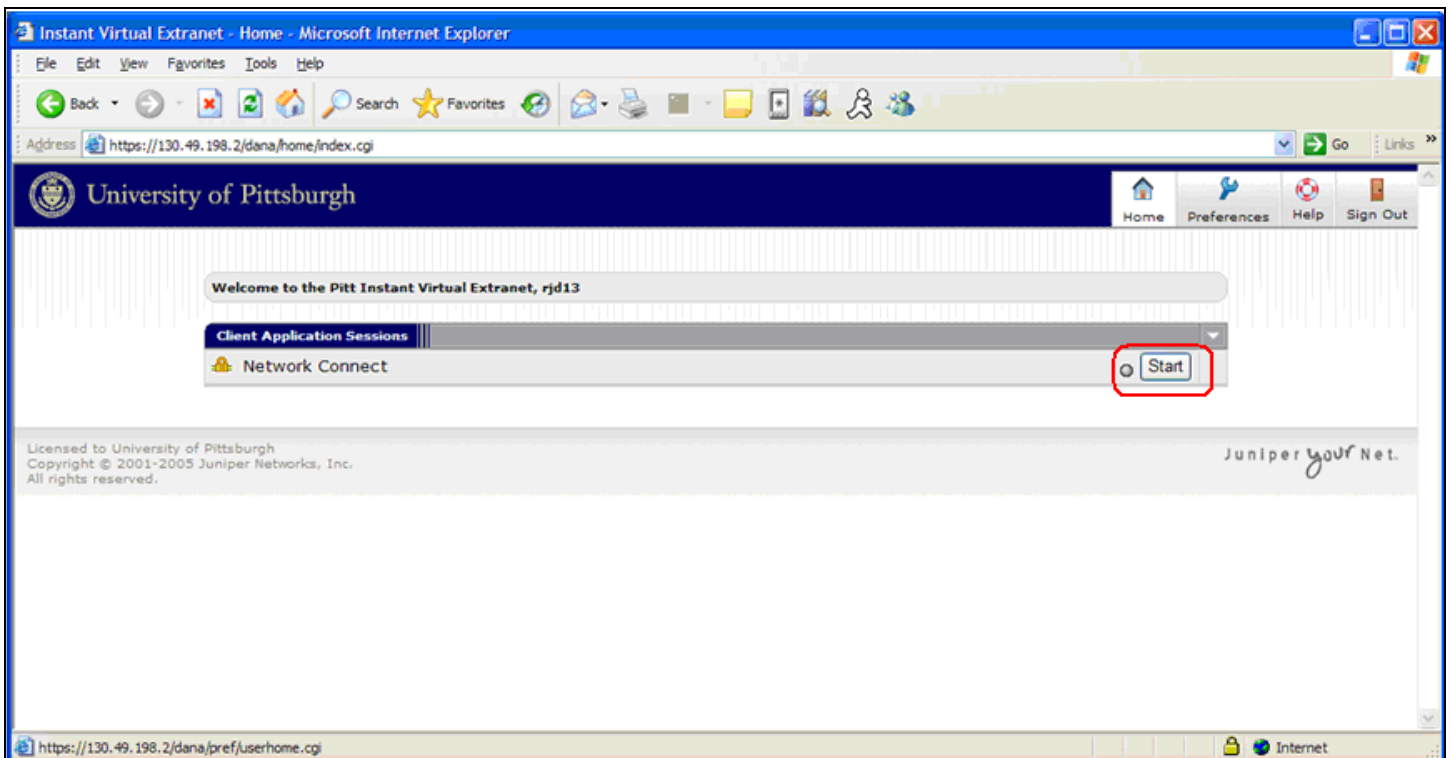
Library resources. The “Default-WEB” role is explained in a separate help sheet titled *Accessing Web and Web-Enabled Applications Using the Secure Remote Access Service*.

Roles for Network Connect access and support for complex workstation applications will usually appear below the “Default-WEB” role. Select the Network Connect role that you wish to use by clicking on the appropriate link.



Network Connect Launch

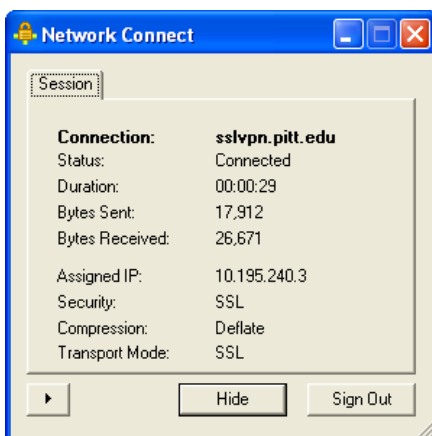
After selecting a Network Connect role, you will see an initial **Welcome** screen that indicates Network Connect Mode is available. To begin the connection process, click on the **Start** button.



Network Connect Activation

The Network Connect Mode of the Secure Remote Access Service provides the capability to communicate information between University network resources and the remote client workstation. Screens indicating that the Network Connect application is launching may appear temporarily. After the Network Connect VPN tunnel has been established, a new icon will be visible in the system tray area of Windows machines. Similar notification is provided to Macintosh users.

Note: Opening the SSL VPN system tray icon provides details about the connection that might be useful if you need to diagnose a suspected connectivity problem.

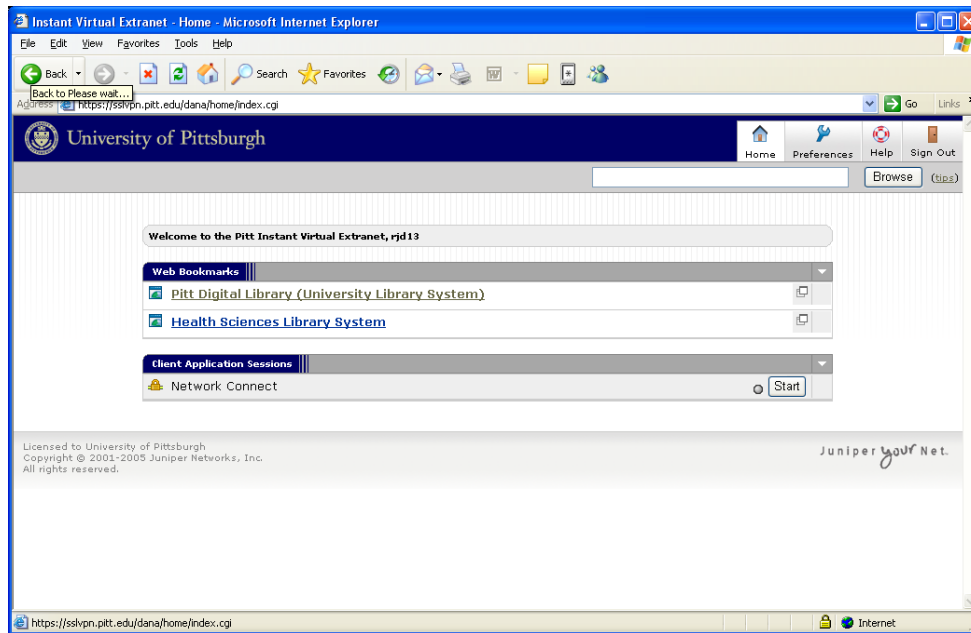


Once Network Connect Mode is activated, TCP (including NetBIOS over TCP/IP), UDP, and ICMP network traffic from applications running on the remote workstation and with a PittNet destination will be automatically sent across the secure connection that has been established.

Note: Additional enhanced capabilities are available for users with unusual network connectivity requirements. Please refer to the "Additional Capabilities" section of this document for details.

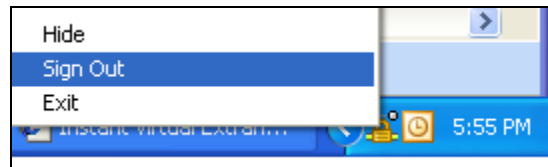
A department may direct users to the Secure VPN Network Connect mode for many reasons. The most common uses are connection to files and directories on a firewalled server or accessing an Exchange server from a full-featured e-mail client. Once the Network Connect Mode is established, users can navigate to mapped drives or launch Outlook just as they would at a computer on the University campus. Departments may also utilize Network Connect mode to run other applications or to provide access to restricted resources. To access files and directories, users will need to know the network path to the resources and should contact their departmental IT staff for directions and assistance. For further details and assistance, the Network Connect Mode user should contact the department's IT support staff.

The Initial Welcome Screen for some users will also provide the option for a concurrent connection to Web resources, such as links to content provided through the University Library System. By selecting the Library links, you can simultaneously run your complex network application while also using a Web browser to access restricted destinations through the University's network.



Disconnecting from the Secure Remote Access Service

To disconnect from the Secure Remote Access Service in Network Connect mode, right click on the **Network Connect** icon in the system tray of your workstation and select **Sign Out**.



Note: Prior to ending the connection, you should terminate any applications running on your computer that use the secure connection.

You may use the Secure Remote Access Service for a maximum of four hours at a time. After four hours you will be automatically disconnected from the service. You will also be automatically disconnected from the Secure Remote Access Service if your session is idle for thirty minutes.

Questions and Feedback

Please contact the Technology Help Desk at 412 624-**HELP** [4357] for additional information, assistance, or to provide feedback on this service. Please be sure to note when calling that you are using the Secure Remote Access Service. The Technology Help Desk is available 24 hours a day, seven days a week to answer all of your technology-related questions. Questions can also be submitted via the Web at technology.pitt.edu.