

## Accessing Restricted University Online Resources Using Network Connect on the Secure Remote Access Service

### Table of Contents

Overview.....	1
Connecting to the Secure Remote Access Service.....	2
Health Check Screen.....	3
Role Selection Screen .....	3
Network Connect Launch .....	3
Network Connect Activation .....	4
Disconnecting from the Secure Remote Access Service.....	4
Get Help.....	4

### Overview

The Secure Remote Access service is a secure remote access solution that allows University students, faculty, and staff to access restricted University online resources when off-campus or while using Wireless PittNet. This service can be accessed using a simple Web browser—no special software is required. University faculty and staff can connect to the Secure Remote Access service using one of two connection methods: Web Connect or Network Connect. Web Connect provides instant access to restricted University Web Resources such as online library journals. Network Connect provides access to network firewall-protected resources that a user has been approved to use. Please refer to the *Accessing Restricted University Online Resources Using Web Connect on the Secure Remote Access Service* document for more information on the Web Connect connection method.

These instructions explain how to use the Network Connect connection method to access restricted resources or applications that require a secure connection. An example of such an application is the KeyAccess license compliance software used in the Faculty Computing Program. Network Connect is for Windows, Macintosh, and Linux computers. You must be approved by your Responsibility Center Administrator to access Network Connect. To arrange to have the Network Connect role configured for your computer, contact the Technology Help Desk at 412 624-HELP [4357].

Specific security features must be active on your computer while using the Secure Remote Access service. Before connecting through the Network Connect connection method, 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 3, Windows Vista with Service Pack 1, or Windows 7.  
**Note:** Macintosh and Linux systems pass the health check.
- Microsoft Automatic Software Update turned on so you can receive the latest security patches.
- The latest version of Symantec Endpoint Protection with Live Update 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

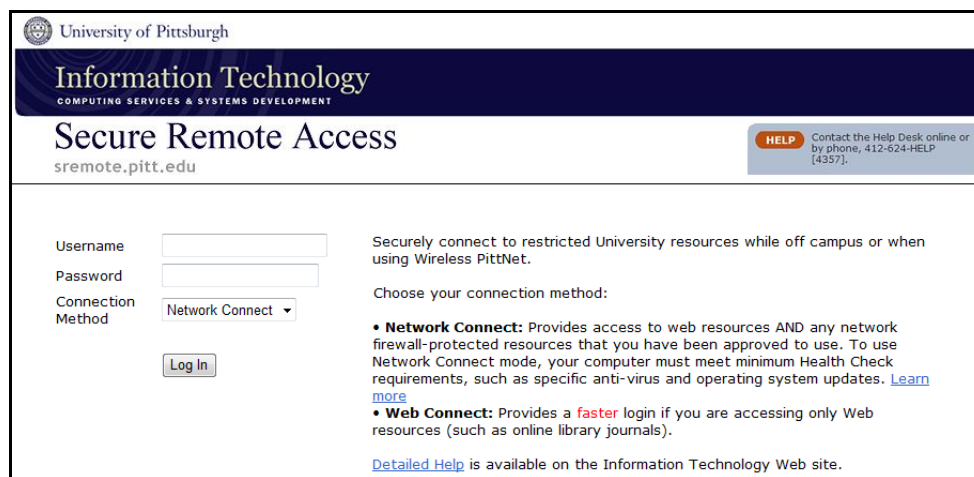
**Note:** The following operating system and web browser combinations have been confirmed as compatible with the Secure Remote Access service. If your operating system or web browser is NOT on the following list, but still works with the Secure Remote Access service, please be advised that it is not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

Operating Systems	Browsers
Windows XP with Service Pack 3	Internet Explorer 7.0 or 8.0, Firefox 3.5 with Sun JRE 6
Windows Vista with Service Pack 1	Internet Explorer 7.0 or 8.0, Firefox 3.5 with Sun JRE 6
Windows 7	Internet Explorer 8.0, Firefox 3.5 with Sun JRE 6
Mac OS X (10.5 or 10.6)	Safari 3.2 with Sun JRE 6

## Connecting to the Secure Remote Access Service

To connect to the Secure Remote Access Service using the Network Connect method, complete the following steps.

1. You must be approved by your Responsibility Center Administrator to access Network Connect.
2. Open a Web browser (such as Internet Explorer) to <https://sremote.pitt.edu/>.



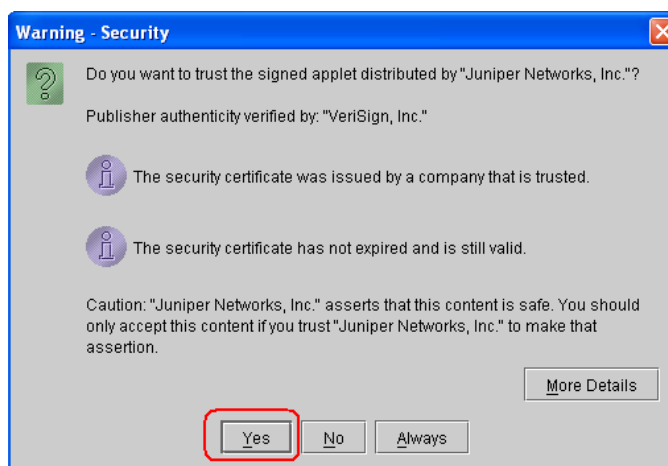
The screenshot shows the 'Secure Remote Access' login page for the University of Pittsburgh. The page header includes the University of Pittsburgh logo and the text 'Information Technology COMPUTING SERVICES & SYSTEMS DEVELOPMENT'. Below the header, the title 'Secure Remote Access' is displayed with the URL 'sremote.pitt.edu'. A 'HELP' button is located in the top right corner, with the text 'Contact the Help Desk online or by phone, 412-624-HELP (4337)'. The main content area contains a login form with fields for 'Username', 'Password', and 'Connection Method'. The 'Connection Method' dropdown menu is set to 'Network Connect'. A 'Log In' button is positioned below the form. To the right of the form, there is explanatory text: 'Securely connect to restricted University resources while off campus or when using Wireless PittNet. Choose your connection method:'. Two bullet points describe the connection methods: 'Network Connect' (provides access to web resources and firewall-protected resources) and 'Web Connect' (provides a faster login for web resources). A 'Detailed Help' link is provided at the bottom of the explanatory text.

3. Enter your University Computing Account username and password.
4. Select **Network Connect** from the **Connection Method** drop-down menu.

**Note:** For select users with a specific Network Connect role, and a Connection Method option does not appear, click on the **Sign In** button to proceed.

5. Click the **Log In** button.

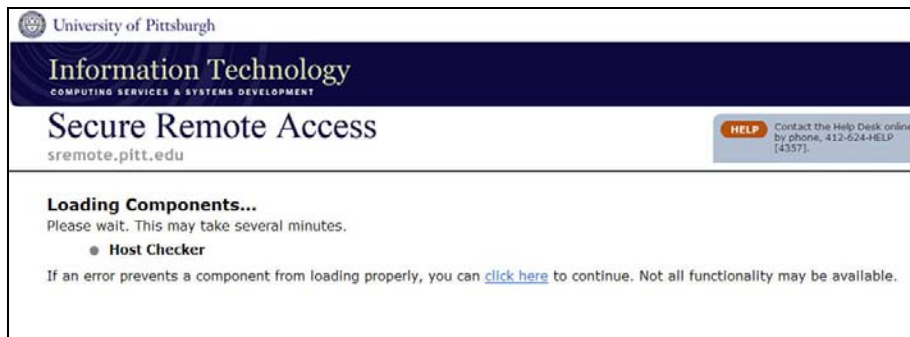
**Note:** After you click the **Log In** or **Sign In** button you may see a security warning window asking if you want to trust the applet distributed by Juniper Networks, Inc. If this window displays, click the **Yes** button to proceed.



6. Start the application that requires a secure connection, such as database client or KeyAccess.

## Health Check Screen

After you click the **Log 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. You should follow any additional steps to download, install and run the health checker. This process may take a few minutes to complete.



## Role Selection Screen

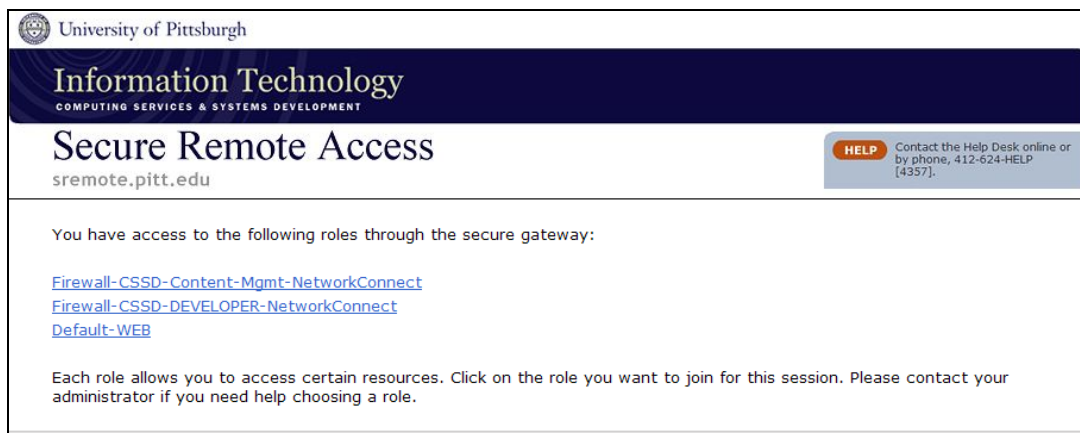
After signing in, most Network Connect users will be presented with a screen containing links to “roles” that are available to them. Having a secure remote access role lets you securely access a network-firewall protected resource.

The “Default-Web” link role allows you to securely access restricted web resources. Roles for Network Connect access appear above the “Default-WEB” role.

**Note:** If the “Default-WEB” role does not display, contact your responsibility center administrator to request it.

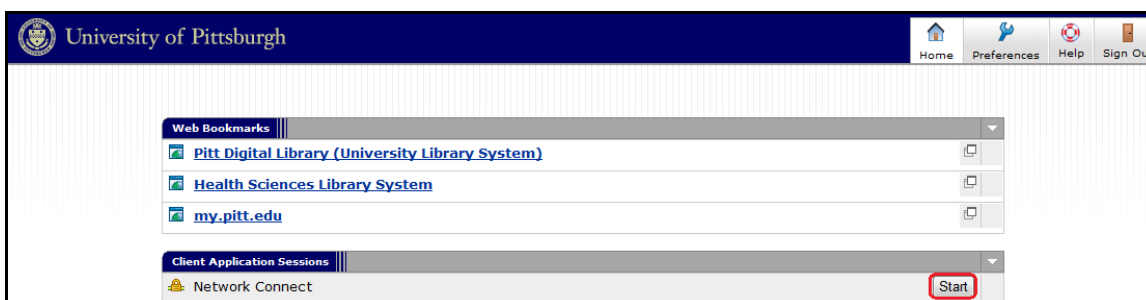
**Note:** If a Network Connect role has not been configured for you, you will see the standard Web Connect Welcome screen.

1. Select the Network Connect role that you wish to use by clicking on the appropriate link.



## Network Connect Launch

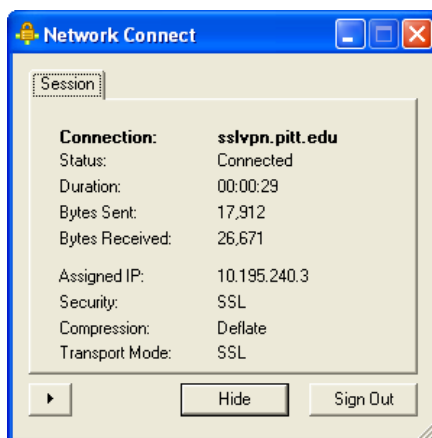
After selecting a Network Connect role, you will see an initial **Welcome** screen. To begin the connection process, locate **Network Connect** and click on the **Start** button.



## Network Connect Activation

The Network Connect connection method 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 Secure Remote Access system tray icon provides details about the connection that might be useful if you need to diagnose a suspected connectivity problem.

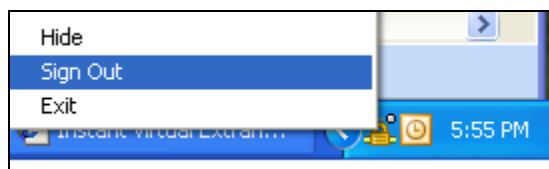


Once a Network Connect session is activated, TCP (including NetBIOS over TCP/IP), UDP, and ICMP network traffic from applications running on the remote workstation and with a PittNet destination will be automatically sent across the secure connection that has been established. To access restricted University online resources, you must use the links provided in the Secure Remote Access welcome screen.

A department may direct users to the Secure Remote Access Network Connect method for many reasons. The most common uses are connection to files and directories on a firewalled server. Once the Network Connect session 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 the Network Connect method 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 method user should contact the department's IT support staff.

## Disconnecting from the Secure Remote Access Service

To disconnect from the Secure Remote Access Service, 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.

## Get Help

The Technology Help Desk at 412 624-**HELP** [4357] is available 24 hours a day, seven days a week to answer your technology-related questions. Questions can also be submitted via the Web at [technology.pitt.edu](http://technology.pitt.edu).