University of Pittsburgh
Computing Services and Systems Development (CSSD)

Technology Help Desk
412-624-HELP [4357]
technology.pitt.edu

Connecting to the Secure Remote Access Service with the Cisco IPSec VPN Client (Windows)

Overview

The Secure Remote Access service (sremote.pitt.edu) can be used by University students, faculty, and staff to access restricted University online resources when off campus or while using Wireless PittNet. These resources include data on departmental servers or databases. The service also enables you to use the SSH or RDP protocols to access remote computers. The Secure Remote Access service can be used with a Web browser—no special software is required.

A separate, supplemental VPN service is also available to meet more specialized needs. It provides the same functionality as the Secure Remote Access service but requires installation of the Cisco IPSec VPN client.

The instructions in this document explain how to configure your Windows computer to use the Cisco IPSec VPN client.

Note: Using this service with Windows 8 requires updating a registry setting. Please contact the Technology Help Desk for assistance.

Connection Requirements

You must be approved by your Responsibility Center Account Administrator to access restricted network resources using Secure Remote Access with the Cisco IPSec VPN client. Contact the Technology Help Desk at 412-62**4-HELP** [4357] to request the service.

Prior to installing the Cisco IPSec VPN application, you must obtain the following:

- a network connect role (configured by the Technology Help Desk)
- a pre-shared text key (provided by your department's IT administrator or Responsibility Center administrator)
- group name information (provided by your department's IT administrator or Responsibility Center administrator)

You must also have administrative privileges to your computer, and it must meet the following requirements:

- Windows XP or higher (32-bit or 64-bit)
- Microsoft TCP/IP installed
- At least 50 MB of free hard disc space
- Minimum of 128 MB RAM

Note: Known issues occur with use of the following: a tethered Internet connection, Smart card authentication for ST Microelectronics models, McAfee versions prior to 4.6, or Tablet PC 2004/2005.

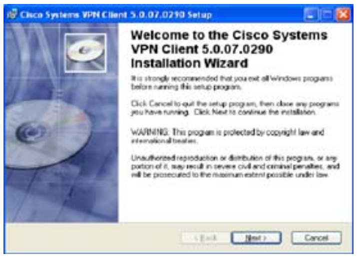
Install the IPSec Client

1. Log in to My Pitt, click the **Software Download Service** on the right-hand side of the screen, then click the **Software Download Service Login** link.

2. Select **Cisco** from the **Vendor** menu and click the **Remote Access 32-bit** link or the **Remote Access 64-bit** link.

3. Download the Cisco Systems VPN client for your Windows computer.

4. Extract the compressed files and double click the **Cisco for Windows 32-bit or 64-bit** file. A setup wizard will guide you through the installation.



Cisco Systems VPN Client 5.0.07.0290 Setup

Welcome to the Cisco Systems VPN Client 5.0.07.0290 Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

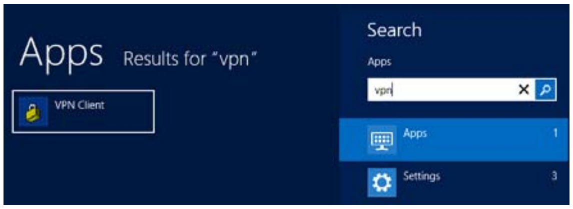
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Configure the IPSec Client

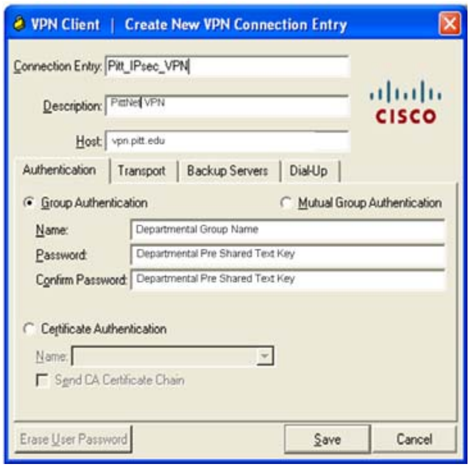
1. Click the **Start** menu, select the **Cisco Systems VPN Client** folder, then select **Start the VPN Client**.

   Note: If you are using Windows 8, you can type VPN from the tiled **Start** screen and then click the **VPN Client icon**.



2. Click the **New** connection type icon New .

3. Enter the following connection entry settings:
   a. **Connection Entry:** Choose a connection name, such as Pitt IPSec VPN
   b. **Description:** PittNet VPN
   c. **Host:** vpn.pitt.edu


VPN Client | Create New VPN Connection Entry

Connection Entry: Pitt_IPsec_VPN

Description: PittNet VPN

Host: vpn.pitt.edu

● Group Authentication ○ Mutual Group Authentication

Name: Departmental Group Name

Password: Departmental Pre Shared Text Key

Confirm Password: Departmental Pre Shared Text Key

○ Certificate Authentication

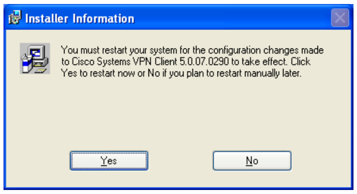
Name:

□ Send CA Certificate Chain

4. Click the **Authentication** tab, select the **Group Authentication** option, then enter the following settings:
   a. **Name:** Your department's group name
   b. **Password:** Your department's pre-shared text key or shared password
   c. **Confirm Password:** Your department's pre-shared text key or shared password

5. Click the **Save** button.

6. Click Yes to restart your machine and complete the installation.

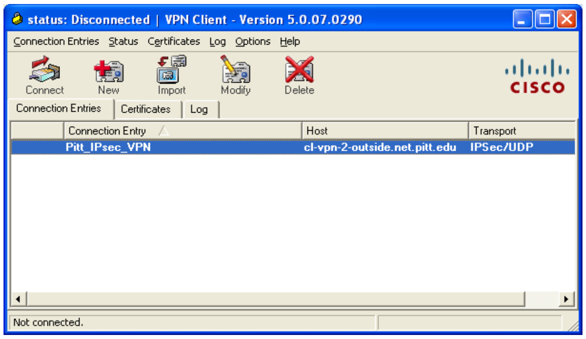

Installer Information

You must restart your system for the configuration changes made to Cisco Systems VPN Client 5.0.07.0290 to take effect. Click Yes to restart now or No if you plan to restart manually later.

Establish a Secure Connection

1. Double click the **Cisco IPSec Client** on your desktop, then select the **VPN configuration** from the **Connection Entry** list. The VPN connection entry list window will display.

2. Click the IPSec connection listed under the **Connection Entry** column.

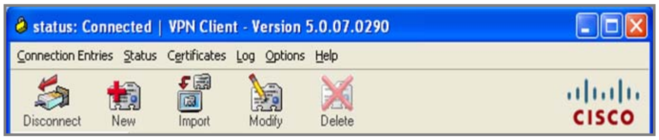


status: Disconnected | VPN Client - Version 5.0.07.0290

Connection Entry	Host	Transport
Pitt_IPsec_VPN	cl-vpn-2-outside.net.pitt.edu	IPSec/UDP

Not connected.

3. Click the **Connect** button .
4. Enter your University Computing Account username and password when prompted and click the **OK** button.



status: Connected | VPN Client - Version 5.0.07.0290

5. A VPN icon will display in your menu bar once the connection has been established.

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

Disconnect from the Service

1. Close any applications that are using the secure connection.

2. Click the **Disconnect** button .

   Note: You may use the Secure Remote Access Service for up to four hours at a time or may be idle up to 30 minutes before you will be automatically disconnected from the service.

Get Help

The Technology Help Desk at 412-62**4-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.**