



University Computing & Telecommunications Virtual Private Networking: How To/Self/Help Guide – Windows Vista Operating System

E-Mail: SupportCenter@uhcl.edu • Phone: 281-283-2828 • Fax: 281-283-2969 • Box: 230 • <http://www.uhcl.edu/UCT>

A VPN (Virtual Private Network) provides a secure, encrypted tunnel from your computer to UHCL's network when off campus. UHCL offers VPN software to allow authenticated, secure access to many UHCL resources from home. In order to utilize this service you must have:

1. A broadband connection.
2. Windows Vista (for these instructions; other operating systems have other instructions).

Support for VPN is limited. Read the entire document before proceeding and refer to the troubleshooting section before contacting the Support Center at 281-283-2828.

Minimum Requirements

We cannot guarantee functionality or provide support for systems that do not meet the following minimum requirements.

- Operating System: Windows Vista
- Pre-existing broadband Internet connection, such as DSL or Cable. Dial up access is *not* supported.
- Before setting up your VPN connection, make sure Windows Vista is up to date by running Windows Update

WARNING: These instructions are not intended for use on your office's desktop computer. Computers on the UHCL campus are already connected to the UHCL network and do not require VPN.



Configuring a VPN Connection on your home computer

1. Click on the Windows button in the lower left corner of your screen and choose “Control Panel” from the menu.
2. Click “Network and Internet.”
3. Click “Network and Sharing Center.”

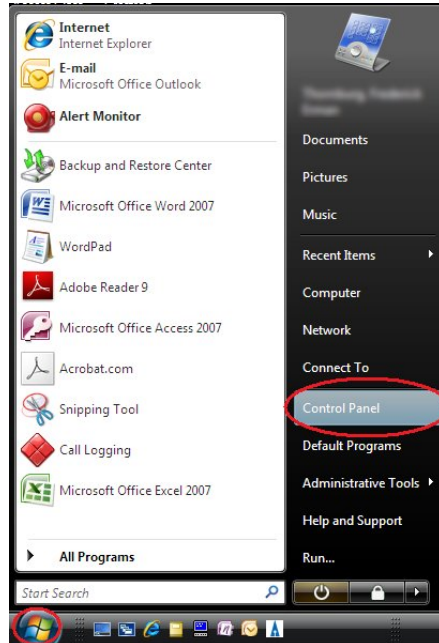


Figure 1

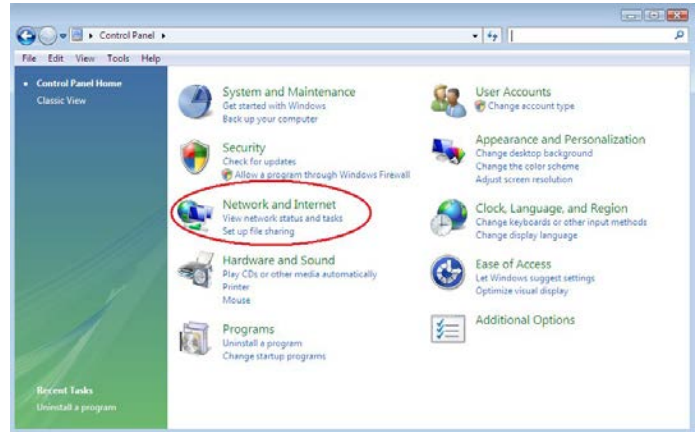


Figure 2

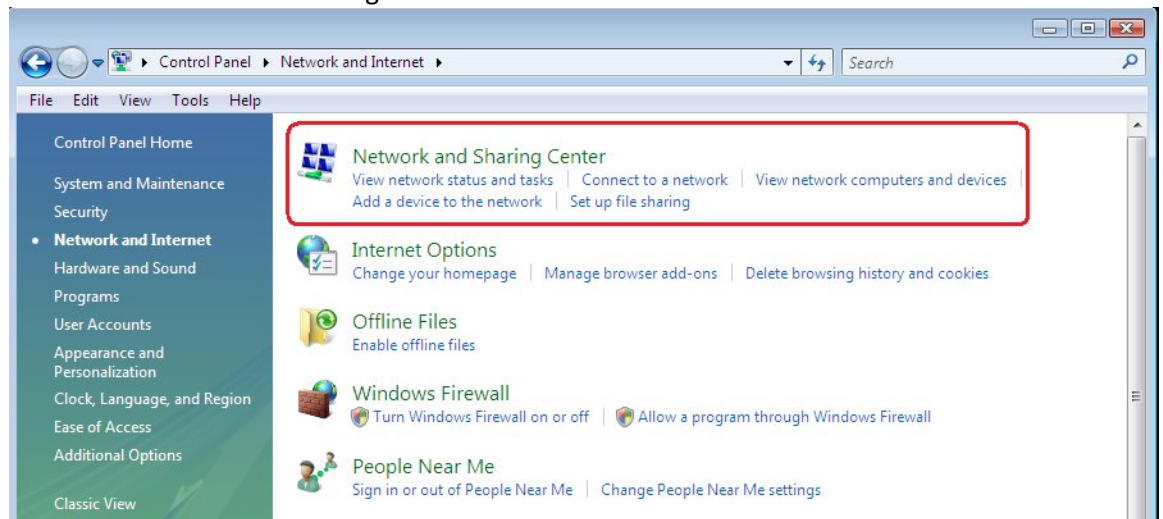


Figure 3



University Computing & Telecommunications Virtual Private Networking: How To/Self/Help Guide – Windows Vista Operating System

E-Mail: SupportCenter@uhcl.edu • Phone: 281-283-2828 • Fax: 281-283-2969 • Box: 230 • <http://www.uhcl.edu/UCT>

4. Under “Change your networking settings” click “Set up a new connection or network.”
5. Click “Connect to a workplace.”
6. Click “No, create a new connection.”
7. Choose “Use my Internet Connection (VPN).”



Figure 4

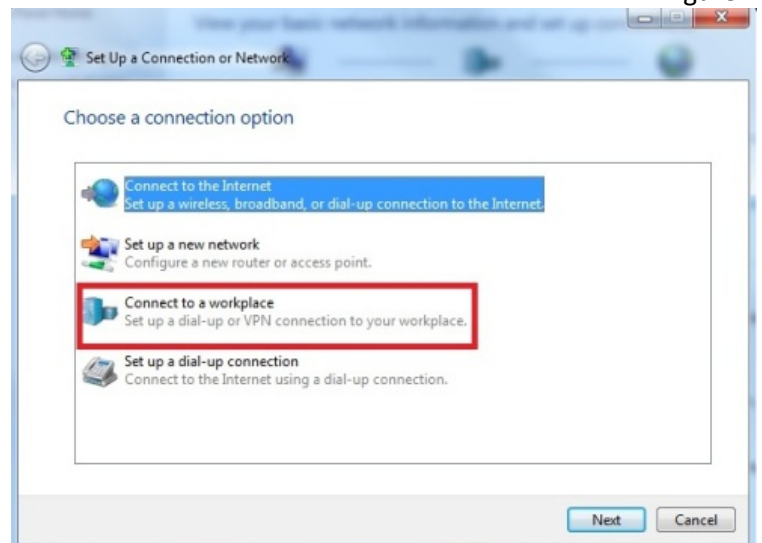


Figure 5

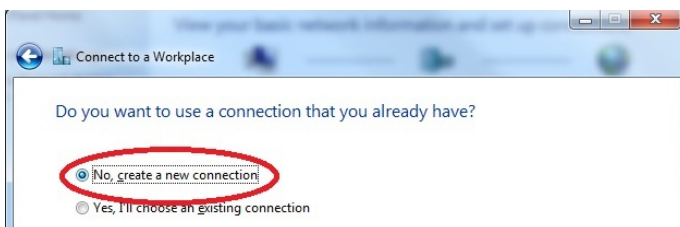


Figure 6



Figure 7



8. Use the following settings:

Internet address:

vpn.uhcl.edu

Destination name:

UHCL VPN Connection

- *Uncheck* “Use a smart card.”
- *Uncheck* “Allow other people to use this connection.”
- *Check* “Don’t connect now; just set it up so I can connect later.”

9. Click “Next.”

10. Type your UHCL User name – this is the same user name (or user id) that you would use to log on to your office computer on campus.

- *Uncheck* “Show characters.”
- *Uncheck* “Remember this password.”

UCT recommends that you do not ‘save’ this password. Your password is required to change every 120 days; storing it here will require you to edit your connection settings every time you change your password or risk having your account locked.

11. Click “Create.”

Your VPN connection is now ready to use!

12. Click “Connect now” – You will be prompted for your password.

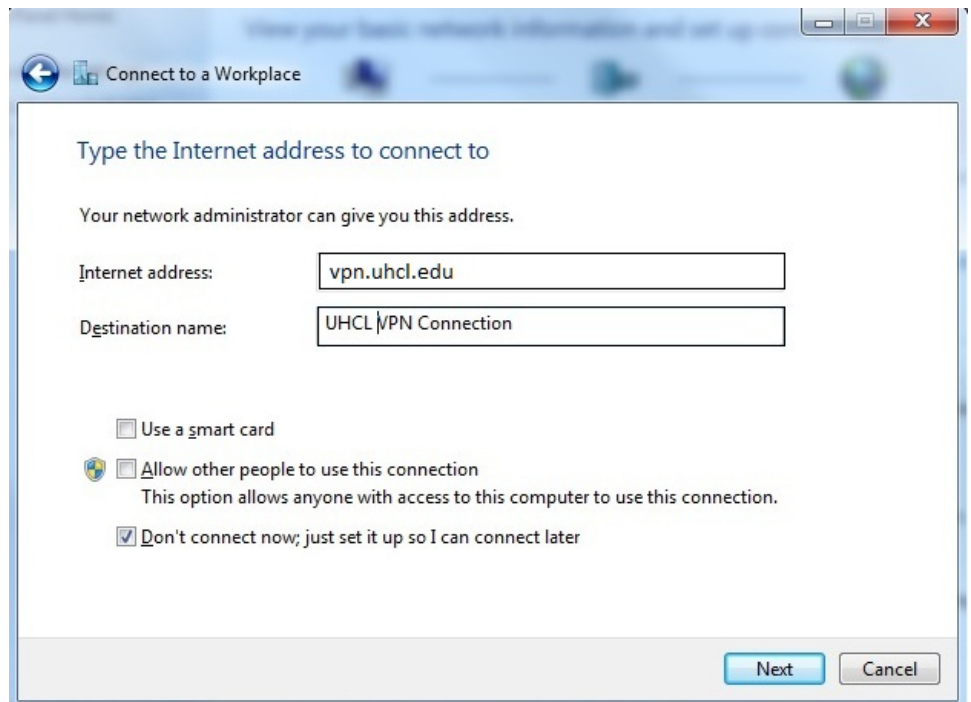


Figure 8



Figure 9



University Computing & Telecommunications Virtual Private Networking: How To/Self/Help Guide – Windows Vista Operating System

E-Mail: SupportCenter@uhcl.edu • Phone: 281-283-2828 • Fax: 281-283-2969 • Box: 230 • <http://www.uhcl.edu/UCT>

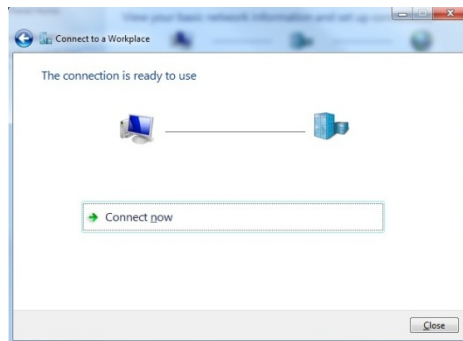


Figure 10



Figure 11



University Computing & Telecommunications Virtual Private Networking: How To/Self/Help Guide – Windows Vista Operating System

E-Mail: SupportCenter@uhcl.edu • Phone: 281-283-2828 • Fax: 281-283-2969 • Box: 230 • <http://www.uhcl.edu/UCT>

Connecting to VPN

1. Click on the Windows button in the lower left corner of your screen and choose “Control Panel” from the menu.
2. Click “Network and Internet.”
3. Click “Network and Sharing Center.”
4. Click “Connect to a network.”
5. Choose UHCL from the list under “Dial-up and VPN.”
6. Click “Connect”
7. You will be prompted to login.
8. To disconnect, click on the “Disconnect” link under your UHCL VPN connection in the “Network and Sharing Center.”



Figure 12

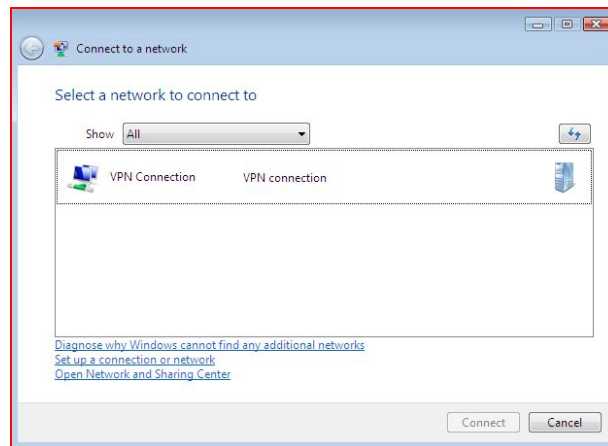


Figure 13



Figure 14

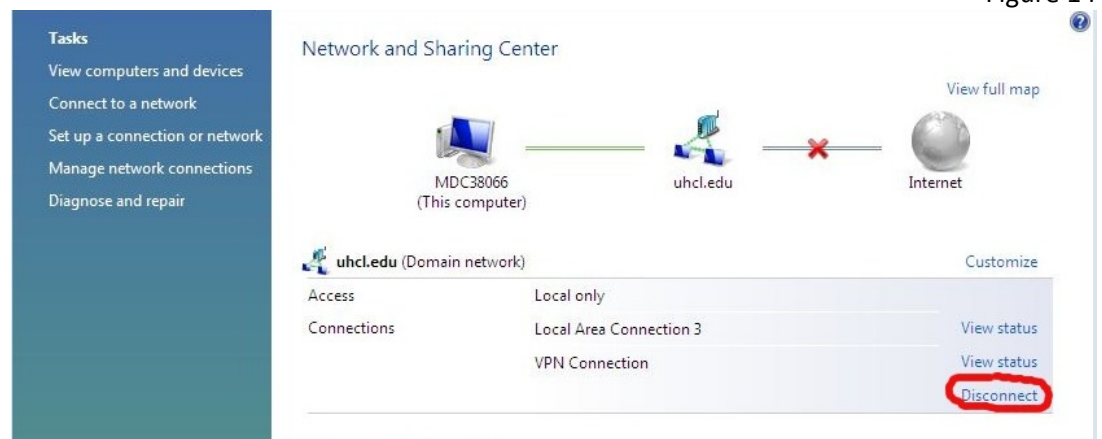


Figure 15



University Computing & Telecommunications Virtual Private Networking: How To/Self/Help Guide – Windows Vista Operating System

E-Mail: SupportCenter@uhcl.edu • Phone: 281-283-2828 • Fax: 281-283-2969 • Box: 230 • <http://www.uhcl.edu/UCT>

Troubleshooting

Support for VPN is limited; the only support offered is this documentation; telephone support is *not* offered for VPN.

- Disconnect from VPN and verify that normal Internet access is working. If normal Internet access is not working, you cannot connect to the UHCL network via VPN. UCT cannot troubleshoot or support your home's (or other location's) Internet connection. Please contact your service provider.
- If you have recently had to change your password on campus, but are using a saved password in your VPN settings your saved password might be incorrect. Remove your saved password from your VPN settings.

Connecting to your Office computer

Once you have VPN properly set up and connected, you will need to use Remote Desktop to connect to your files and applications on your office computer.

Using Remote Desktop

1. Click the Start button; choose All Programs, then Accessories, then select Remote Desktop Connection. If you have a shortcut on your desktop, double click on Remote Desktop Connection Icon. You can also type Remote Desktop Connection into the search field on the start menu.
2. Click the options icon in the lower left corner of the Remote Desktop Connection screen.
3. Input tag number for your office computer. Note that your computer's tag number should be preceded by a capitol letter 'P' (all desktop computers running Windows XP, Windows Vista or Windows 7 – some computers have a different designation, but they are not covered by this document.).

Example: P12345

4. Input your Username and password, just as if you were logging in on campus.

Example: UHCL\YourUserName

5. Click Connect.

You will be connected to your system in your office. This is the recommended means of remotely accessing your computer. Using this method ensures full access to all your files, applications, and ensures that any items you update or change will get properly backed up.