

About the Virtual Private Network (VPN)

1. [Introduction](#)
2. [Why use a VPN?](#)
3. [Advantages of a VPN](#)
4. [What's the difference between a VPN and "remote desktop"?](#)
5. [Who can use the VPN?](#)
6. [Using the VPN](#)
 - [Windows and Internet Explorer](#)
 - [Install the VPN client](#)
 - [Using the VPN client after installation](#)
 - [Windows and Firefox/Chrome/other browsers](#)
 - [Mac OS X](#)
 - [Running the Mac VPN client](#)
 - [Manual installation of the VPN client](#)
 - [Ubuntu](#)
 - [Connecting to the VPN from mobile devices](#)
10. [Accessing subscription-based resources through the VPN](#)
11. [Laptops already joined to the campus Active Directory Services \(ADS\)](#)
12. [FAQ](#)
13. [Technical details for support staff](#)

Introduction

Information Systems & Technology (IST) provides a Virtual Private Network (VPN) service to the campus community to facilitate telecommuting and other access to campus-based network resources. The VPN uses the public Internet to connect a remote computer, such as a home computer or a laptop, securely to the uWaterloo network. The underlying principle is to make the remote computer seem as if it were physically connected to the campus network. [Log on the campus VPN](#).

[Back to top](#)

Why use a VPN?

Off-campus computers are subject to various network restrictions:

- uWaterloo network border policies prevent certain high-risk network traffic, such as Windows file-sharing (getting at your "network drive") and Unix/Linux X-Windows protocols.
- Some website and other network resources are restricted to uWaterloo computers only.
- There are certain computer systems on campus that use "private addresses" that are restricted to use on campus.
- Consumer Internet Service Providers (ISPs) sometimes implement restrictions on the kind of traffic that can be transmitted, or impose limits (such as email message size).

A VPN connection bypasses these restrictions by making the client appear as if it were on campus. The VPN provides a private address on Waterloo's network in the subnet 172.16.36.0/22.

[Back to top](#)

Advantages of a VPN

Access to network resources

The most apparent advantage of the VPN is that it allows users off-campus to connect to network resources such as network drives.

Simple to use

Once the VPN connection is started, it works in the background to manage all traffic between the off-campus computer and the campus resources. There is no need to start special file-transfer programs or other software to get at campus resources. Only traffic destined for the University of Waterloo goes through the campus VPN "tunnel". Traffic from your computer to other Internet sites does not go through our VPN.

Connection security

VPN connections are encrypted end-to-end, using the same Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption that secure websites use. This means that e-mail, file-sharing, web-browsing, calendars - all of the data between the off-campus and on-campus computers is encrypted and secure.

Improved campus-wide strategy for IT security

With the campus VPN in place, it is now possible for IT managers on campus to be more pro-active in securing services. In particular, websites that provide sensitive services can be restricted to campus addresses only, and off-campus access can be provided through the authenticated VPN connection.

What's the difference between a VPN and "remote desktop"?

Many people already connect to campus network resources by using [Remote Desktop](#) (RDP) to connect to their campus workstation from off-campus.

- RDP works by transmitting the video (and sometimes sound) signals from the on-campus system to the off-campus system and then transmitting keyboard and mouse signals from off-campus to the on-campus system.
- RDP provides some security, but with a VPN, the entire traffic stream is encrypted to the same degree as a secure website ("https" or SSL/TLS encryption).
- RDP is a Windows-based product for connecting to Windows computers and terminal servers. There are clients for Mac or Linux users to connect to Windows computers as well.

RDP is now blocked at the campus boundary. When you need to use RDP, a VPN connection is simply established first, using the Cisco AnyConnect client (obtained from [campus VPN website](#)), then the RDP connection is established as before. Instructions for obtaining and installing the Cisco AnyConnect client are outlined below.

[Back to top](#)

Who can use the VPN?

As of November 2012, the VPN service is available to all University of Waterloo staff, faculty, graduate students and undergraduate students.

[Back to top](#)

Using the VPN

The web access and VPN device's network address is "<https://cn-vpn.uwaterloo.ca/+CSCOE+/logon.html>". In the AnyConnect client, the "Connect to" location is "cn-vpn.uwaterloo.ca".

If you only need to access on-campus web sites, using the VPN can be done without installing any software on your home computer. You can use the VPN website to access other websites. Most users, however, will need to install the VPN client software in order to get access to all campus network resources. In this case, you would run the Cisco AnyConnect client software, then do what you need to do to access the resource. For example, you would start the VPN client before running site-licensed software on your laptop that needs to connect to our license server, or before starting your Remote Desktop client.

Below are detailed instructions for connecting using various operating systems.

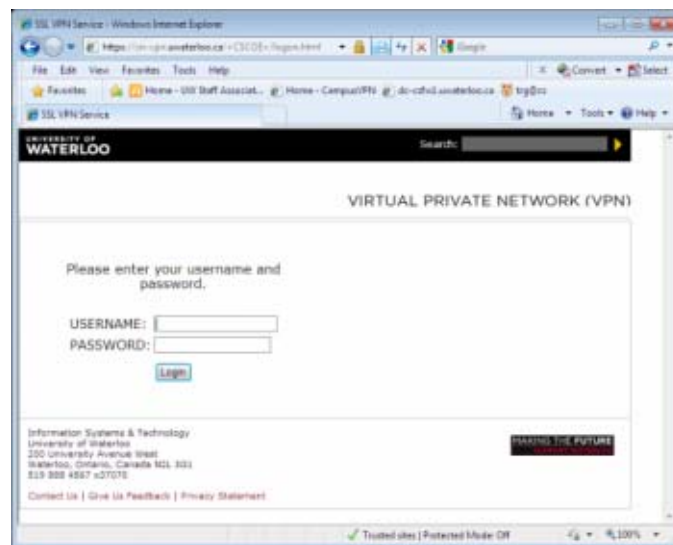
- [Windows and Internet Explorer](#)
- [Windows and Firefox/Chrome/other browsers](#)
- [Mac OS X](#)
- [Ubuntu](#)
- [Connecting to the VPN from mobile devices](#)

Windows and Internet Explorer

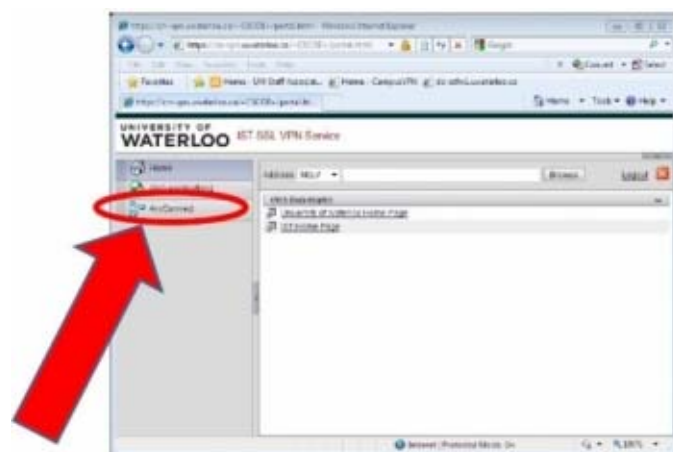
The following screen snapshots were taken from a Windows 7 Enterprise (64-bit edition) system. The snapshots you see may look different depending on the version you are using. Note that you will need administrator permissions on the system in order to do the following installation.

Install the VPN client

1. Log into the VPN service with your University of Waterloo Identity and Access Management (WatIAM) credentials.



2. Click "AnyConnect" to go to the installation web page.



3. Click "Start AnyConnect" to begin installation of the client. If the client is already installed, this button will simply start a connection.

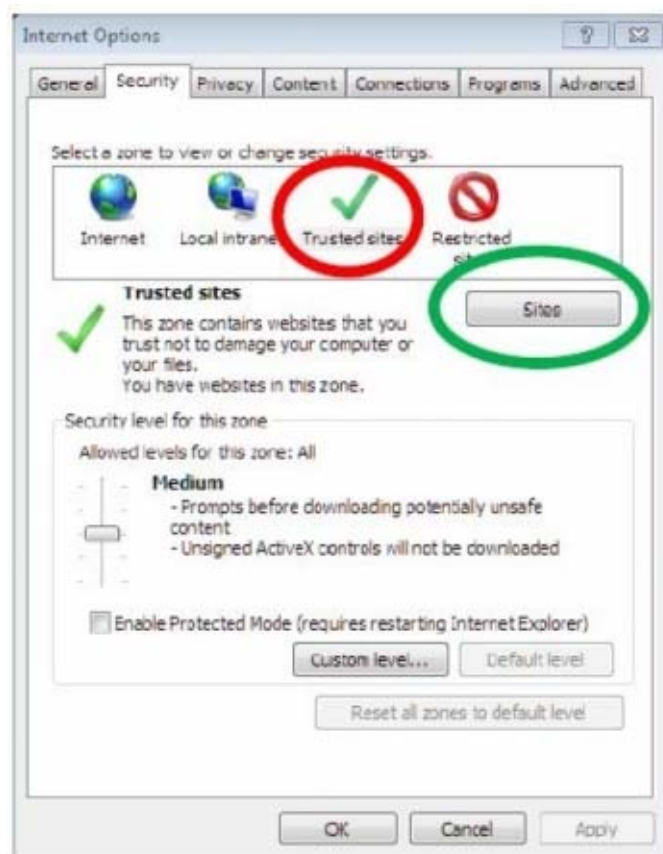


4. Windows 7 and Vista users, please take note of the notice shown below the button:

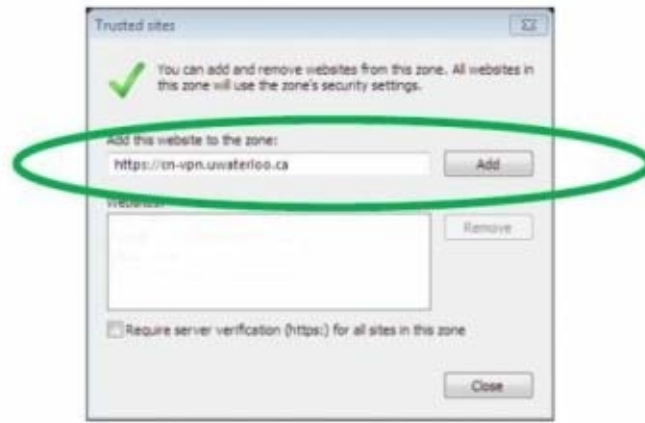
Attention Windows 7 and Vista Users

Adding a security appliance to the list of trusted sites is required for Internet Explorer 7.0 or later on Windows 7 and Vista.

5. Before proceeding, you must add the site "https://cn-vpn.uwaterloo.ca" to your Internet Explorer "Trusted Sites" list. In Internet Explorer, go to the "Tools" menu and select "Internet Options". Then, go to the "Security" tab, select "Trusted Sites" and click the "Sites" button:



6. The site address should be filled in automatically (if not, enter "https://cn-vpn.uwaterloo.ca"). Click "Add" to add the site.



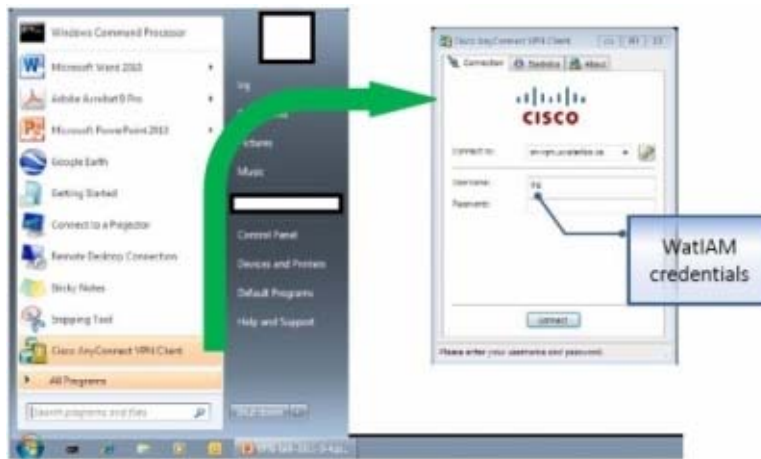
7. As the installation proceeds, you will see various VPN Client Downloader/Cisco AnyConnect VPN Client message windows appear. You may also receive a Windows "User Account Control" prompt to allow the installation to proceed, and you may see warnings about "Active X installation". These are normal and you can proceed.
8. When the installation is completed, you will see the client connection window appear:



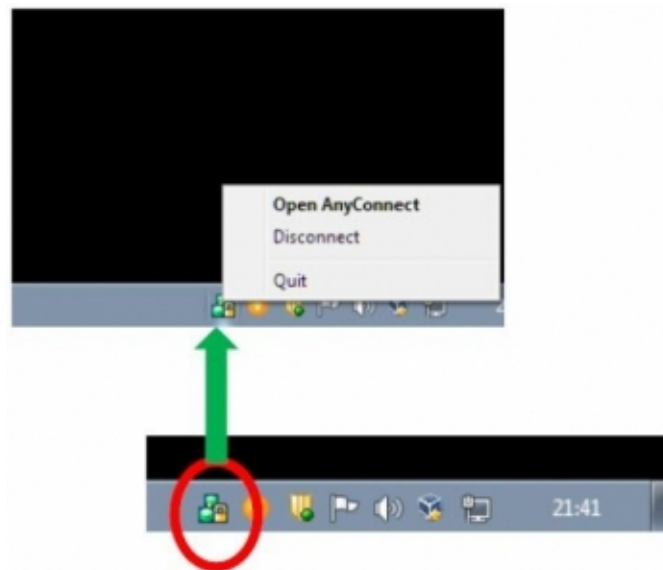
[Back to top](#)

Using the VPN client after installation

The installation process only needs to be done once. After the client is installed, you can use the "Start Menu" item to launch the client connection window.



When the VPN client is running, you will see an icon in the taskbar notification area (lower right corner). This can be used to control the VPN connection.

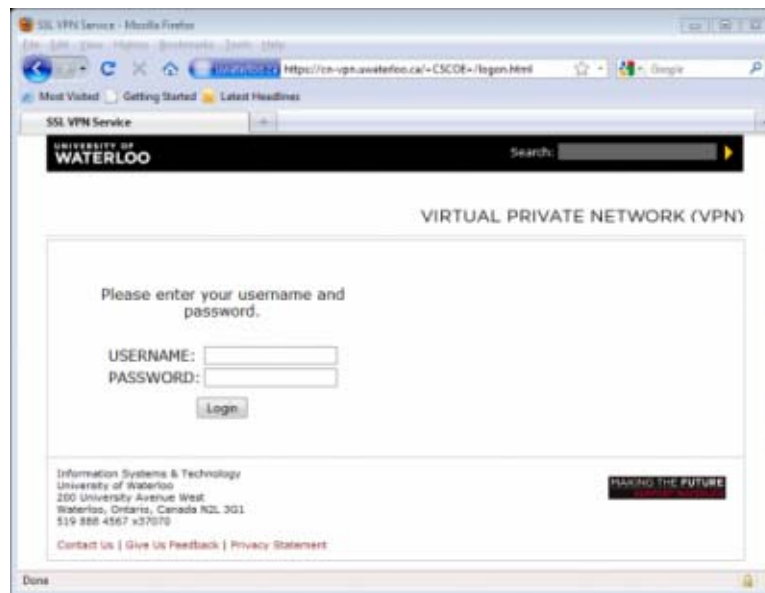


Windows and Firefox/Chrome/other browsers

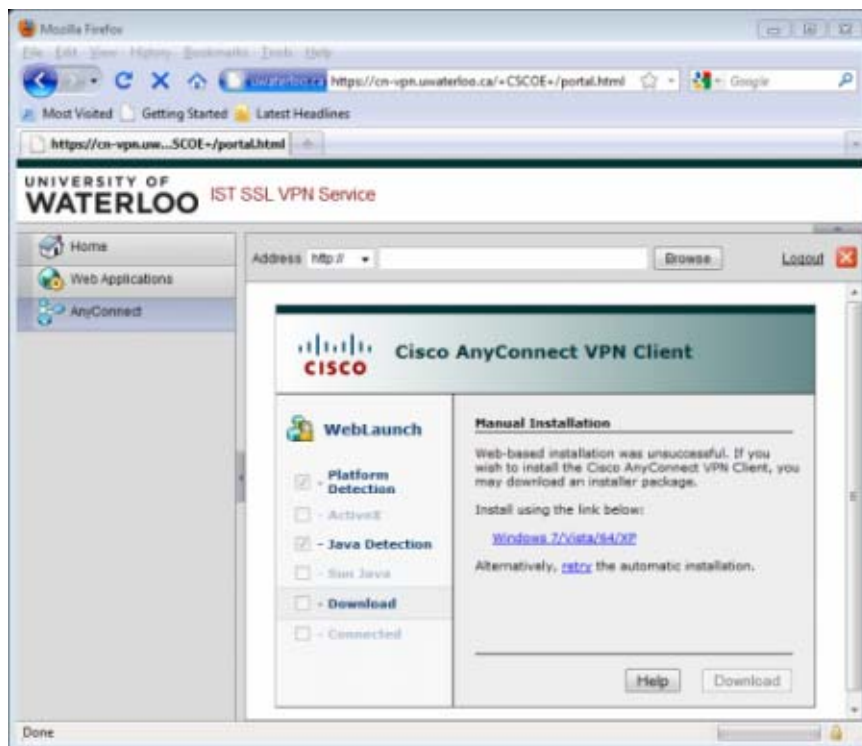
Under Windows with browsers other than Internet Explorer (IE), installation of the VPN client requires downloading and running an installer package. The end result is the same as the IE case, that is, a client application you start from the Windows program menu ("Start button").

The examples in this section were run on a Windows 7 Enterprise (64-bit) system using the Firefox web browser (version 3.16).

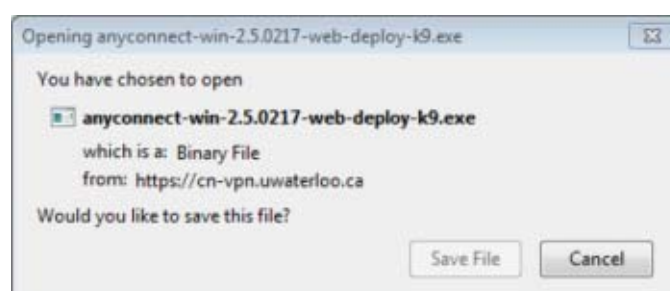
1. To begin, go the the [VPN website](#), and log in with your WatiAM credentials:



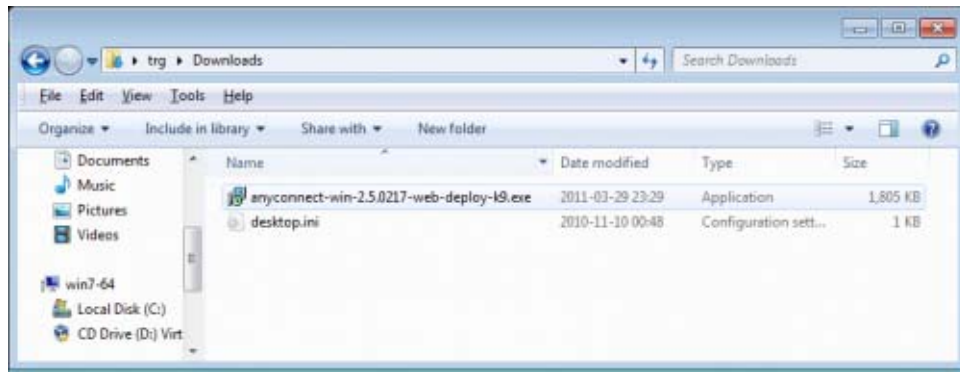
2. Go to the "AnyConnect" installation page (click "AnyConnect" at the left), and click "Start AnyConnect". The web-based installer will attempt to determine whether or not an automated install can be done. It will conclude that you need to download an installer package:



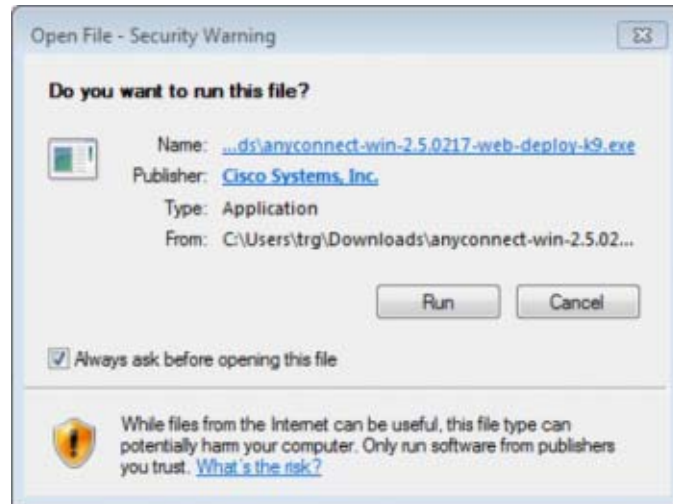
3. Click on the download link to begin downloading the installer. For Firefox, you will be prompted for a location into which to save the file (other browsers may have different default behaviours — these instructions will assume that you have downloaded the installer package):



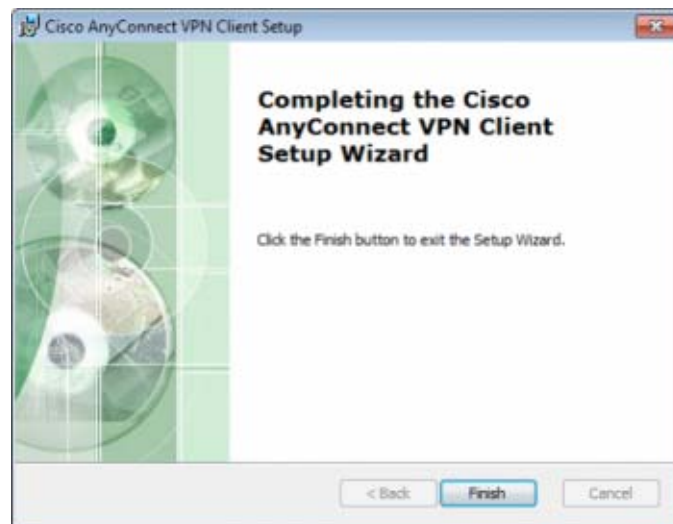
4. Download the installer package, and open a file browser to the location where the file was downloaded. In this example, it is the "Downloads" folder used by default by Firefox:



5. Double-click the filename to run the installer. For most system configurations you will likely receive a security warning—you can safely click "Run" to proceed:



6. A typical Windows installer wizard will then step through the installation (including a requirement for you to accept the Cisco software licence). Eventually, the installation wizard will complete: click "Finish".



Once the client is installed, you can run it via the Windows "Start Menu" button: the menu item is "Cisco AnyConnect VPN Client". For more details and screen snapshots, see the section "[Using the VPN client after installation](#)" above.

[Back to top](#)

Mac OS X

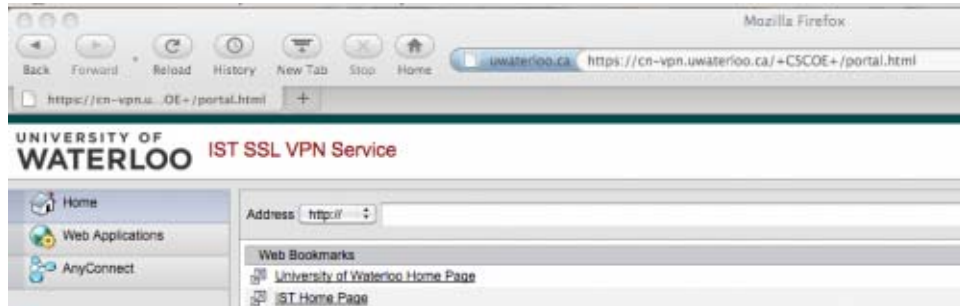
The following discussion is based on Mac OS X 10.9 (Mavericks). The snapshots you see may look different depending on the version you are using.

1. To begin, log into the [VPN website](#) with your WatIAM credentials.

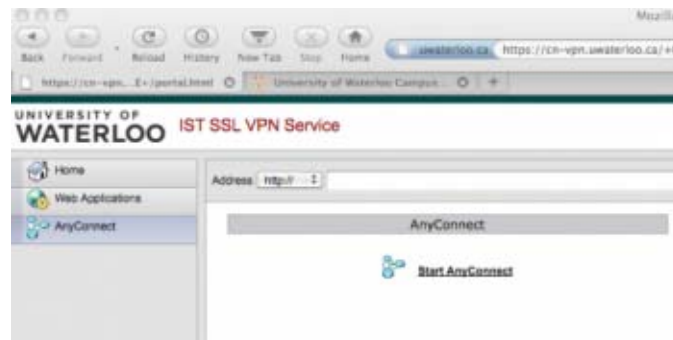


A screenshot of the VPN login page. It has a dark grey header with the word "Login" in white. Below the header, the text "Please enter your username and password." is centered. There are two input fields: "USERNAME:" and "PASSWORD:". Below these fields is a "Login" button.

2. From the VPN home page, click "AnyConnect" (in the left side-bar) to go to the client installation page:



3. Click "Start AnyConnect" and the installer will attempt to install the client software (*vpndownloader.app*).



4. It will first attempt to determine which version of Java you have installed (if any) and then run the appropriate Java applet. You may be asked to accept a security certificate:

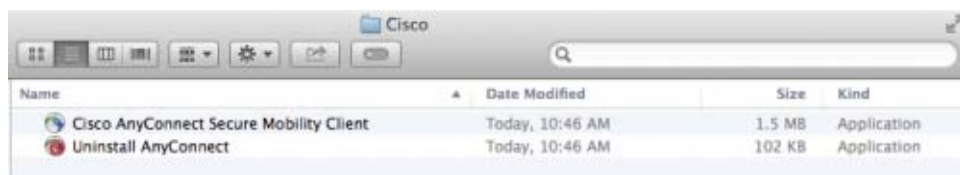


Click "Trust". You will also have to authenticate with your Mac administration credentials to install the software. If all goes well you should see:



Running the Mac VPN client

You do not need to repeat the installation process each time you want to use the VPN. The installation process installs the Cisco VPN client into the Applications folder. You can run it from there or add it to your Dock.



If you haven't connected before, you will need to specify the VPN server `cn-vpn.uwaterloo.ca` as shown below.



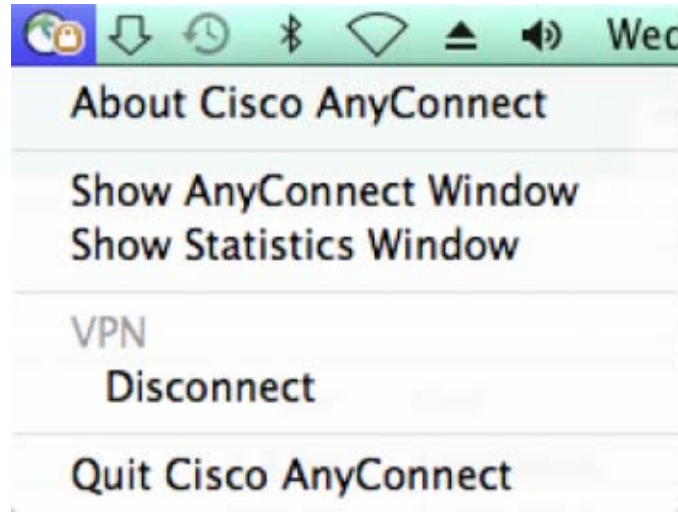
1. Select "cn-vpn.uwaterloo.ca". This brings you to a login window where you can authenticate with your WatIAM credentials.



2. Successful authentication with the VPN client will result in:



- When the client is active, the VPN connection can be controlled from the Menu Bar icon:



Manual installation of the VPN client

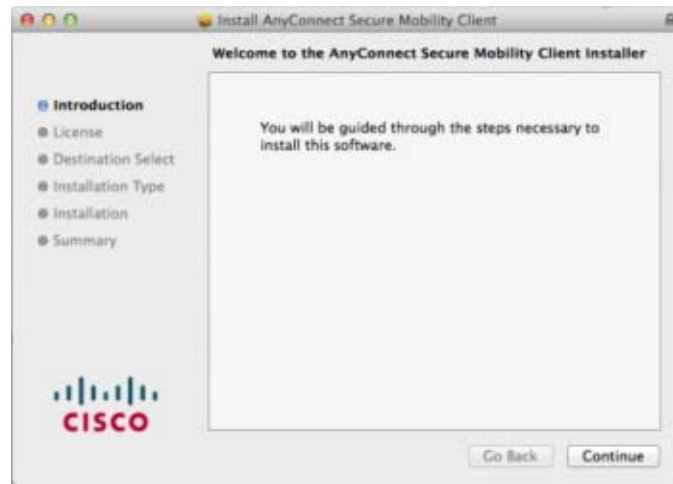
- In some circumstances (unique to specific system configurations), the automatic installation will fail and you will be prompted to download an installer package. The link will be tailored to your environment, e.g. "Mac OS X 10.8+ (intel)":



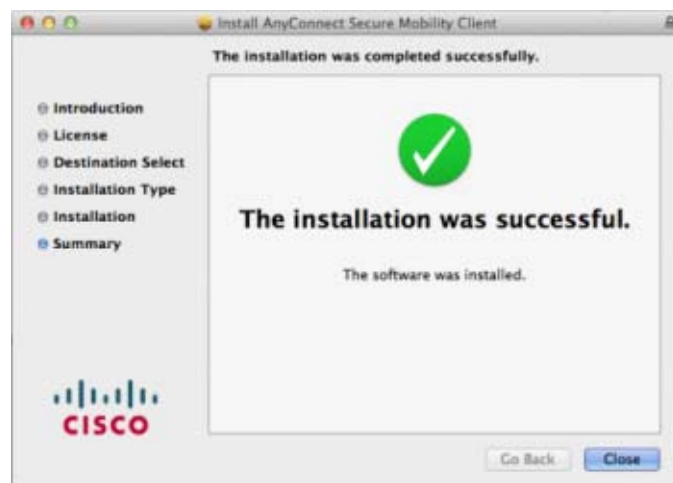
- Click the link. A vpnsetup.dmg package will be downloaded to your downloads folder. Open this disk image and double-click the "vpn.pkg" icon:



- A window appears saying, "This package will run a program to determine if the software can be installed." Choose "Continue". The Cisco AnyConnect VPN Client Installer window will appear. Choose "Continue", and follow the prompts. You will be required to enter your Mac's administrative credentials.



4. A successful installation will end with:



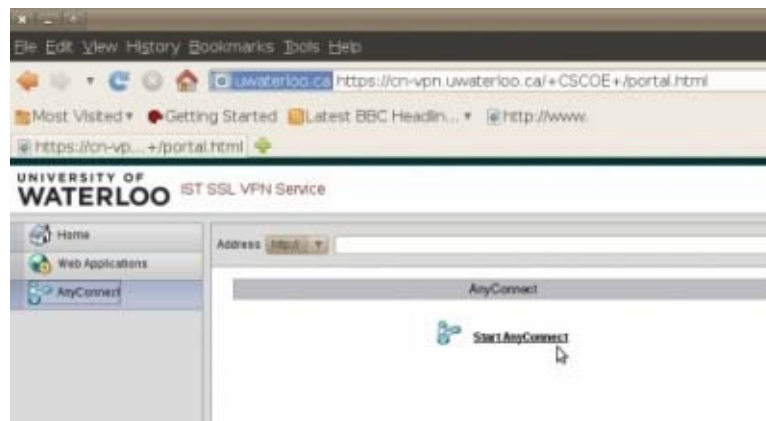
The client is installed into the Applications folder. You can run it from there, or add it to your Dock. See [running the Mac client](#) for details.

[Back to top](#)

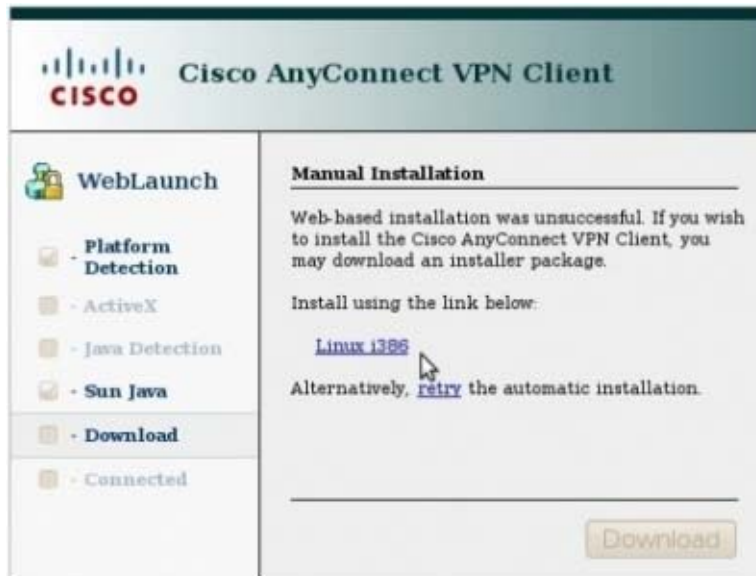
Ubuntu

The following discussion is based on an Ubuntu 10.04 distribution.

1. To begin, log into the [VPN website](#) with your WatIAM credentials. From the VPN home page, click "AnyConnect" (in the left side-bar) to go to the client installation page:



2. Click "Start AnyConnect" and the installer will attempt to install the client software. It will first attempt to determine which version of Java you have installed (if any) and then run the appropriate Java applet. In our experience, this step always fails, regardless of the version of Java installed. Instead, you will be prompted to download an installer package. The link will be tailored to your environment (one of "Linux i386", as shown in the example, or "Linux x86_64" for 64-bit platforms):



3. This link will download a file called *vpnsetup.sh* to the standard download location for your system (varies depending on which browser you use, and how you have the download options set).

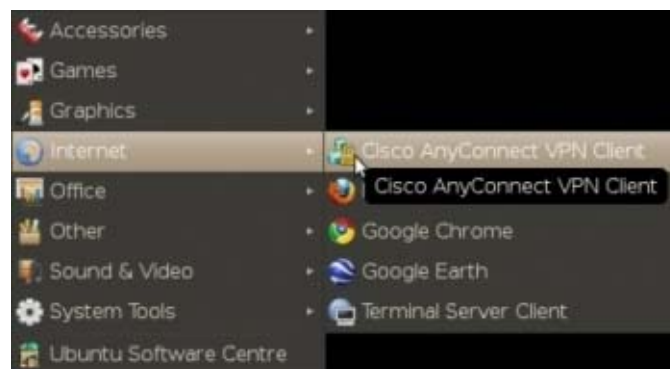


4. Wherever it lands, you must open a command window (terminal, xterm or similar) and chdir to the folder containing the downloaded file. You must then mark the file as executable, *chmod o+x vpnsetup.sh* and then, as administrator, run the setup script, *sudo ./vpnsetup.sh*

```
smcarr@smcarr-netbook:~$ cd Downloads/
smcarr@smcarr-netbook:~/Downloads$ ls -l
total 4540
-rw-r--r-- 1 smcarr smcarr 4647991 2011-03-18 14:58 vpnsetup.sh
smcarr@smcarr-netbook:~/Downloads$ chmod o+x vpnsetup.sh
smcarr@smcarr-netbook:~/Downloads$ sudo ./vpnsetup.sh
```

The setup places the client application at */opt/cisco/vpn/bin/vpnui*.

5. The installer should create an "Applications"—"Internet" menu icon called "Cisco AnyConnect VPN Client":



We have observed however that in some circumstances the menu item isn't created correctly. You can create your own via the "System"—"Preferences"—"Main Menu" tool. The VPN client executable is located at */opt/cisco/vpn/bin/vpnui* and a suitable icon is */opt/cisco/vpn/pixmaps/vpnui48.png*.

6. When you run the client (either via the command-line or from the desktop Graphical User Interface (GUI)), the client GUI window will appear. Click "Connect" and use your WatIAM credentials to start a connection.



7. When the VPN client is running, an icon will appear in the System Tray:



You can use this icon to control the client.

Connecting to the VPN from mobile devices

The campus VPN requires the use of the Cisco AnyConnect client software on your mobile device. **Your device's built-in VPN client cannot be configured to connect to our SSL VPN.**

Not all devices are supported. Please see [Cisco's FAQ](#) for the list of supported devices. Depending on the OS version, iPhones and Android devices are supported.

Please locate the Cisco AnyConnect client for your device through its official application repository. Only the PC clients are available for download from the campus VPN website.

Authentication to the VPN from your mobile device is via your WatIAM user ID and password.

[Back to top](#)

Accessing subscription-based resources through the VPN

The uWaterloo Library and some academic departments have subscriptions for electronic journals and other online resources. In most cases, access to these resources is restricted to on-campus Internet Protocol (IP)

addresses.

The VPN technology cannot circumvent this practice directly. When using the VPN from home or elsewhere, traffic to the electronic resource website (for example, a journal website) will not be sent through the VPN because the resource is not on campus. Instead, the VPN client sends requests in the "usual" way for the off-campus system. This will appear to be from an address that is not a uWaterloo IP address, and so access is typically not automatically granted as it would be for an on-campus computer.

Fortunately, the [uWaterloo Library has a portal web page](#) that VPN users can use to access most subscription and licenced/restricted-access resources. From there you can reach all of the subscription-based resources that are available to the library.

[Back to top](#)

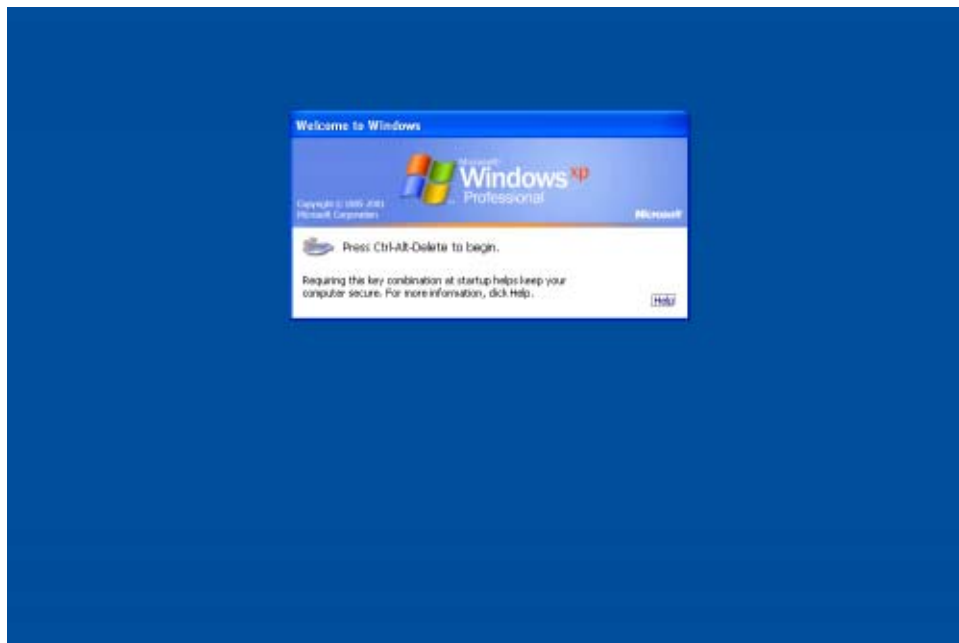
Laptops already joined to the campus Active Directory Services (ADS)

For laptops (or any remote uWaterloo workstations) that are joined to the campus ADS Windows Active Directory, you can log into the domain via the VPN. This will make your laptop behave exactly as if it were on campus. This feature will be particularly valuable for users who travel and are using their uWaterloo laptops in hotels, airports and at other public access points. The [connection security aspects](#) of the VPN are particularly important in such situations.

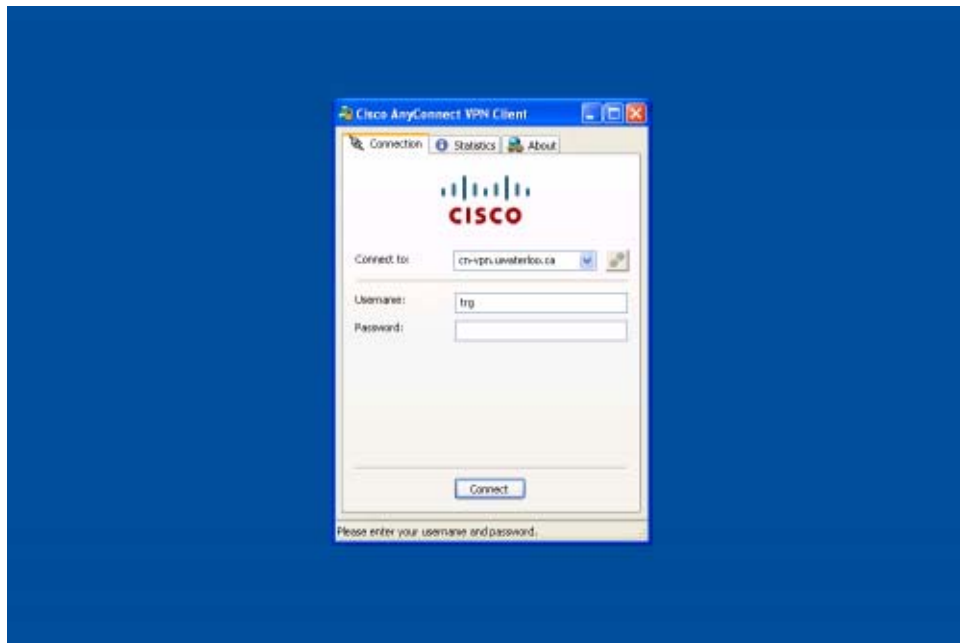
To use your ADS laptop via the VPN, you must first [install the VPN client](#). Subsequently, whenever you start up your laptop and "Ctrl+Alt+Delete" to get to the login prompt, you will first be presented with the VPN client login panel. If you wish to login to the VPN, do so, and you will then receive the standard login prompt for your domain account. If you don't want to log in via the VPN at that time, simply cancel the VPN prompt and log in as you would do normally.

Shown below are some screen snapshots of the ADS domain login process from a remote location. In this example the remote system is an XP system, but the same sequence applies to Windows 7.

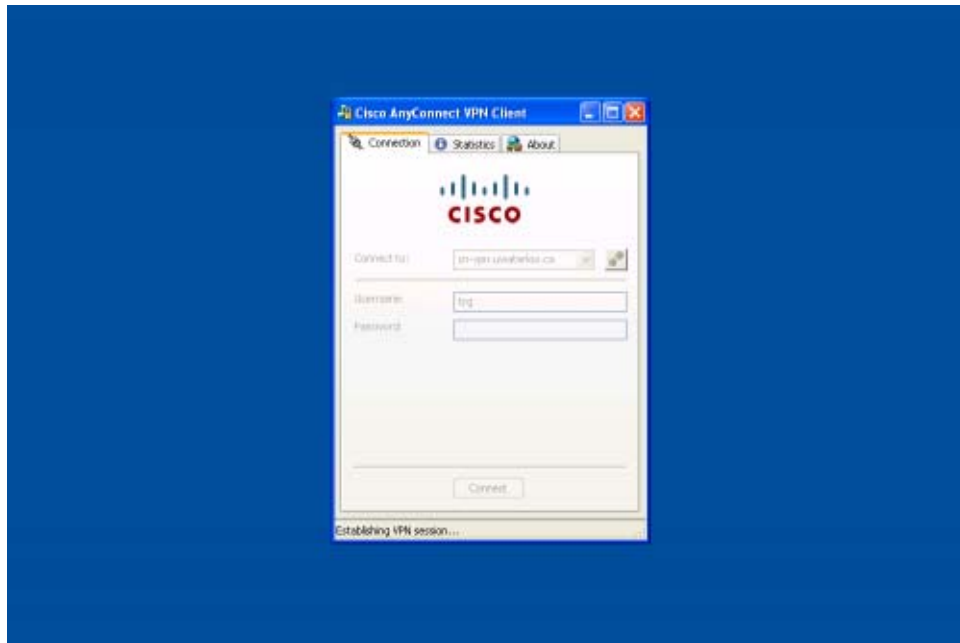
1. At system startup, you receive the "Press Ctrl-Alt-Delete" prompt as usual.



2. Instead of the receiving the Windows login prompt, you see the VPN login prompt. If you do not want to log into the VPN, simply close the window and the Windows login will appear.

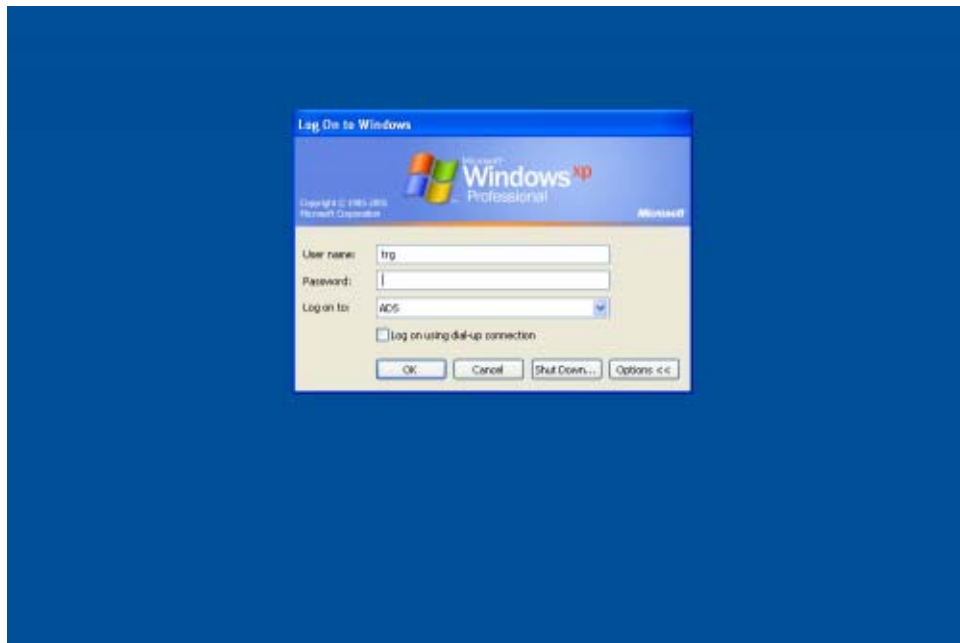


3. Enter your VPN credentials and press "Connect". As the VPN client starts up, you may see some messages appear at the bottom of the window (e.g. "Checking for profile updates", "Establishing VPN - Initializing connection..."). These messages are normal.



4. Eventually, the VPN client window will disappear and be replaced with the standard Windows login prompt. Login as usual to your ADS account.

[Back to top](#)



FAQ

Question 1: Under Windows 7 with Internet Explorer, I received the following error when I tried to install the client software:



What should I do?

Answer 1: This error indicates that you have not added the campus VPN server to your "Trusted Sites" list. See above for [detailed instructions](#).

Question 2: What's the address I need to map my campus network drive onto a remote computer?

Answer 2: The address of your network drive depends on whether you are a Nexus or ADS user, and which department/faculty/unit you are in. In general, it will be something of the form, \\server-name\userid.

Your local IST Client Services Representative or faculty service desk can assist you with determining the correct address.

[Back to top](#)

Technical details for support staff

Client-side modifications

- The AnyConnect client installs as a networking pseudo-device, e.g. "Cisco AnyConnect VPN Virtual Miniport Adapter for Windows x64" for 64-bit Windows 7.
- The client pseudo-device will be assigned an address in the 172.16.36.0/22 range.
- The DNS name associated with the dynamic IP address will be *IP-address.dynamic.uwaterloo.ca*, for example *172-16-36-55.dynamic.uwaterloo.ca*.
- A split-tunnel routing model is used. Traffic to 129.97/16 and 172.16/12 will be routed via the VPN connection, and all other traffic will use the client's normal default route. A explicit routing entry to the VPN server at 129.97.2.197 will likely appear in the client routing tables.

- The VPN server will not route any non-uWaterloo traffic (i.e. destination networks 129.97/16 or 172.16/12) to an off-campus address. A typical user scenario is that after starting the VPN, they can get to campus addresses, but not anywhere else. In this situation the failure is probably on the client-side with its routing setup.
- The number of routing hops to an on-campus address will likely be reduced, although the first hop may take more time.

Debugging commands

Windows

The *vpncli* command is installed into the program directory where the GUI client is installed.

```
ipconfig /all  
route print  
tracert  
vpncli
```

Mac OS X, Linux

The commandline interface command *vpn* is installed into the *bin* directory where the VPN client is installed.

```
ifconfig -a  
route  
ip route  
traceroute  
vpn
```

Also, the Cisco AnyConnect Client GUI has some information (the "Statistics" tab and the "Details" button) that might be useful for debugging problems.

[Back to top](#)