

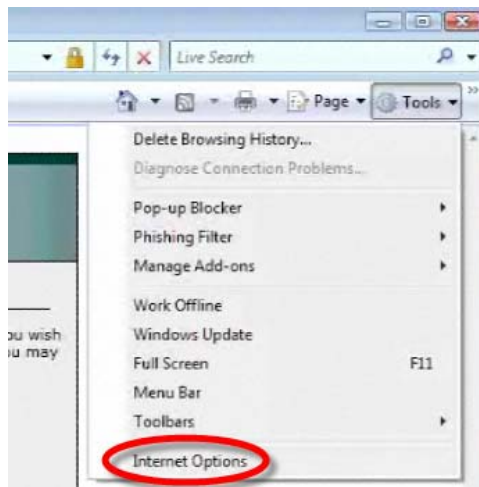
## MSCITS Central IT SSL VPN Service

December 16, 2009

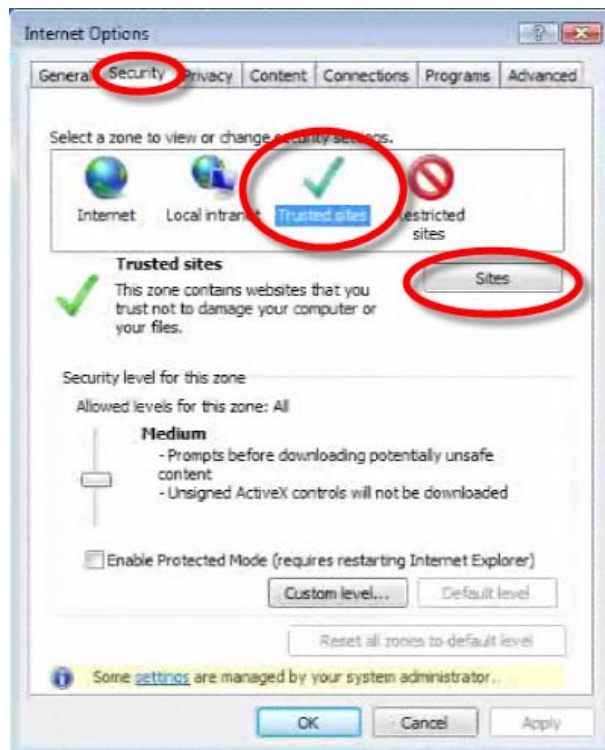
*This document is provided as a general guideline for establishing a VPN connection. Your results may be slightly different, and the screens may present slightly different information depending upon your browser and Operating System version.*

*Additionally, if your computer is running any security software that may prevent you from establishing a VPN connection, you may need it to be reconfigured or temporarily turned off while making the connection*

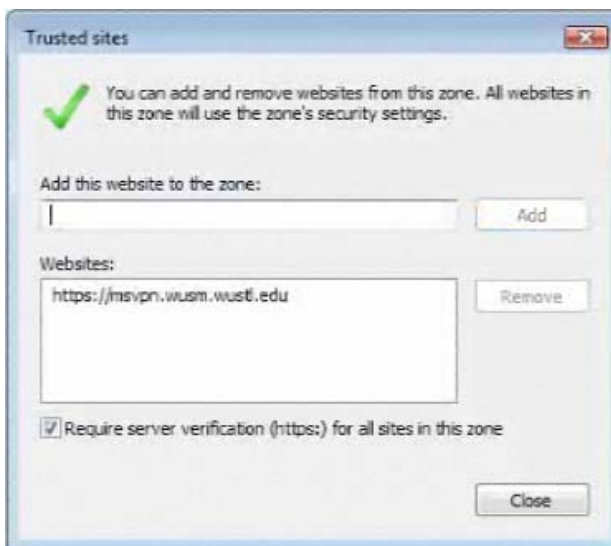
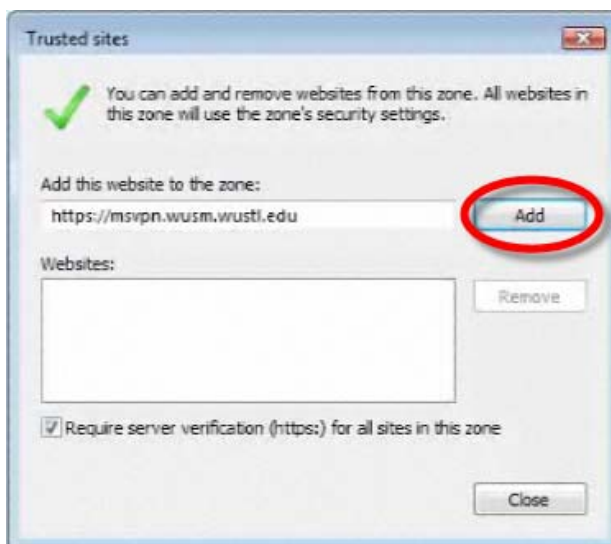
Click **Tools** and select **Internet Options**:



Click the Security tab, click on Trusted sites, check Enable Protected Mode and click the Sites button:



Add <https://msvpn.wusm.wustl.edu> and you should see this in the list of Websites:



Click Close and click OK.

To invoke the service for the very first time, browse to the URL

<https://msvpn.wusm.wustl.edu>

You will see the following page. Enter your domain and username with your domain password.

The screenshot shows the Washington University School of Medicine SSL VPN Gateway login page. The header includes the university logo and the text "SSL VPN Gateway". The main content area has a "Login" section on the left with a form for "Domain\Username:" and "Password:", and a "Login" button. To the right, a message states: "You have reached the Washington University School of Medicine SSL VPN Gateway. This is a restricted and monitored resource. To gain access, or if you are having trouble connecting, please contact your departments Help Desk." Below this message is a table of department contact information.

Department	Phone #
Central IT Service Desk(MSCITS)	362-7798
FPP-IS	935-0909
ITC Helpdesk (Surgery)	362-4540
Internal Medicine	362-2165
Neurology	747-1165
PAIS	747-5555
Pathology	362-9137
Radiology	362-8475
WUPCF	362-9500

The browser status bar at the bottom shows "Done" and "Trusted sites".

Once you are authenticated, you will be presented with the following page. Please select "Continue" to move on to the installation.

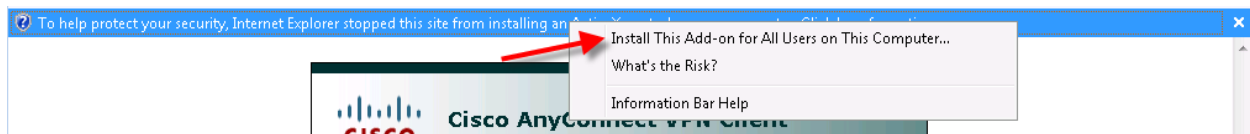
The screenshot shows the Cisco SSL VPN Service welcome dialog box. The header includes the Cisco logo and the text "SSL VPN Service". The main content area contains a welcome message: "Welcome to the Washington University Clinical Operations Network (WUCON). You are in a secured environment. You agree to protect the confidentiality of clinical systems and patient data contained within the private network by using the VPN client software only when required to access this data within WUCON. Be sure to observe WUCON security policies. Any noncompliance with these requirements will constitute a security violation and will be reported to the management of the WUCON user." Below the message are "Cancel" and "Continue" buttons.

The browser status bar at the bottom shows "Done" and "Trusted sites".

The installation will continue and it will move on to the next steps.

At any point during the installation, if you are prompted for permission to continue, then click “Continue” or “Allow” to continue with the installation.

Click on the information bar at the top of the website and click “Install This Add-on for All Users on This Computer”



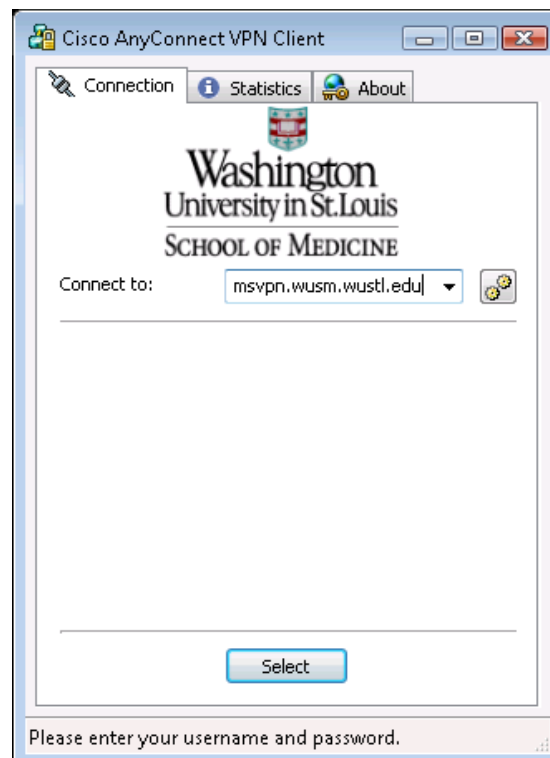
Click Install



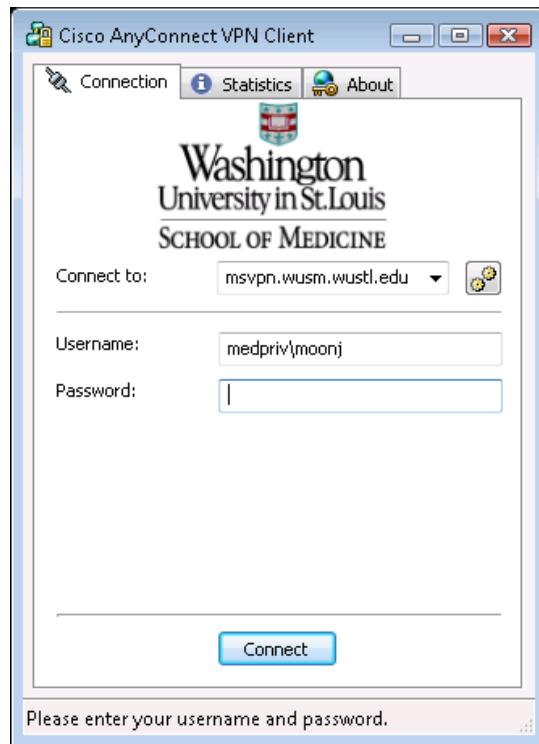
When you see this screen the installation has completed successfully and you can close the browser. You are connected to the MSCITS SSL VPN service.



Any time after this you do not need to use the browser to start up the SSL VPN service. You just need to invoke the program “Cisco AnyConnect VPN Client” from the Start menu -> All Programs. When you do, you will see either of the two following two panels. If you see this one, click on Select to move to the next.



Or, you might see the following one. If so, go ahead and enter your domain password and select “Connect”.



Following this panel, you will be presented with the following. Select Accept and you will be connected to the SSL VPN service.

