

MAC Web Based VPN Connectivity Details and Instructions

UMDNJ's Web-based VPN utilizes an SSL Based Cisco Application that provides VPN functionality without having to install a full client for end users running Microsoft Windows XP, Windows 2000, MAC OS X, or Linux.

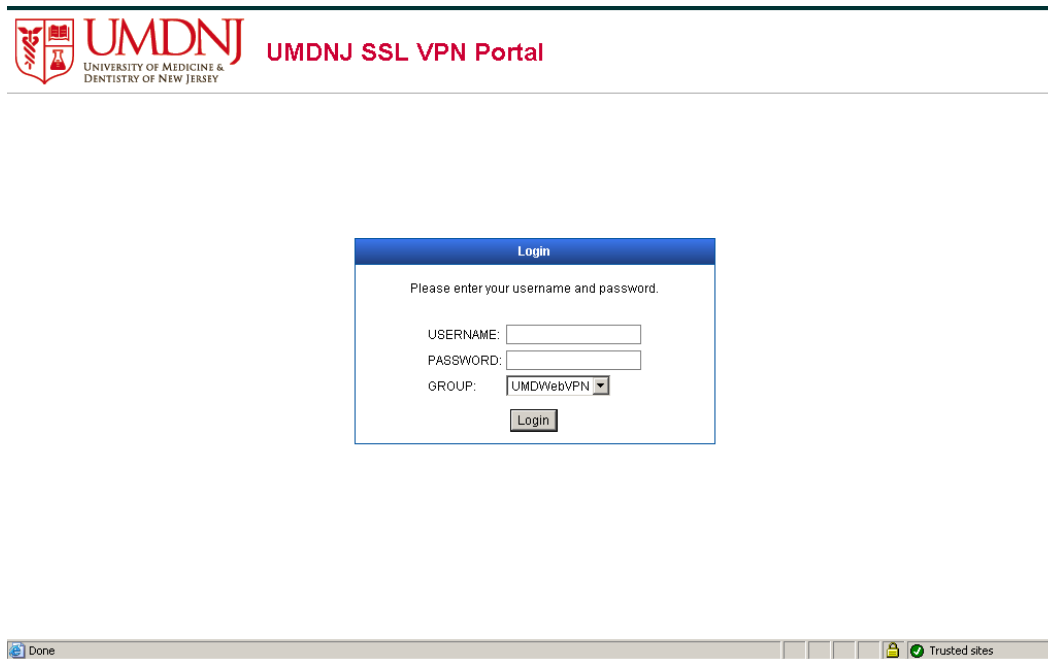
The VPN concentrator is available via the web and can be reached at the following address:

Newark VPN Concentrator -- <https://nwvpn.umdj.edu>*

(note: The URL listed above can only be accessed using https, http will not work as it's not secure connection. If http is used to access the URL, the user will receive a "page not found" error)

* This site is only accessible from outside the UMDNJ Network.

The screen shots that follow are what the user should see upon connecting to the web based VPN. Some images may be slightly different on each system.



UMDNJ
UNIVERSITY OF MEDICINE &
DENTISTRY OF NEW JERSEY

UMDNJ SSL VPN Portal

Login

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP:

Login

Done Trusted sites

Figure 1

After selecting Yes on the Security Alert, you will be prompted to provide login credentials for accessing the WebVPN Services (Figure 1). At this screen, enter your CORE Account credentials, and select Login.

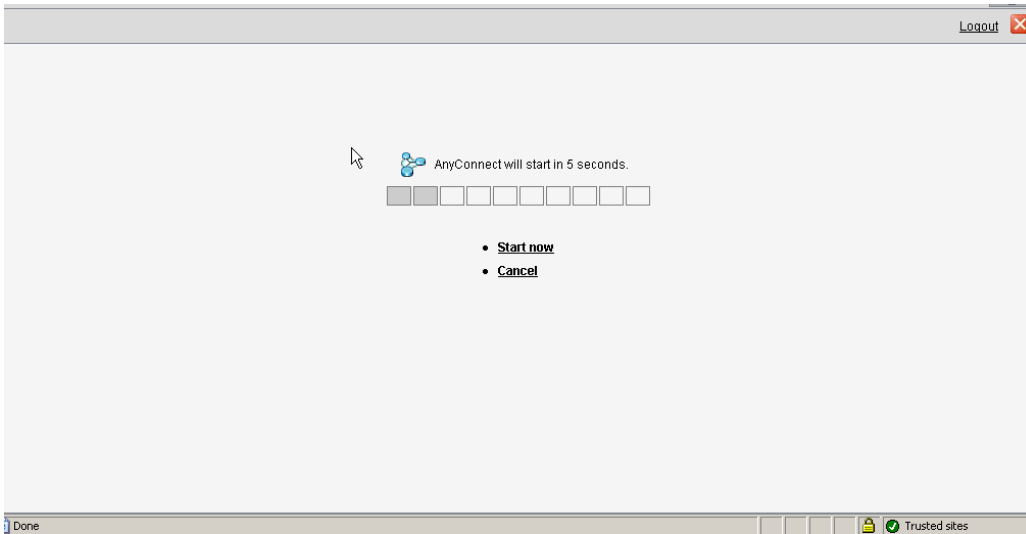


Figure 2

The SSL AnyConnect client will auto install after 5 seconds, as shown in Figure 2.



Figure 3

If you receive a warning similar to the above, select Yes to continue (Figure 3).



Figure 4

If prompted, enter your Mac login credentials and click OK (Figure 4).

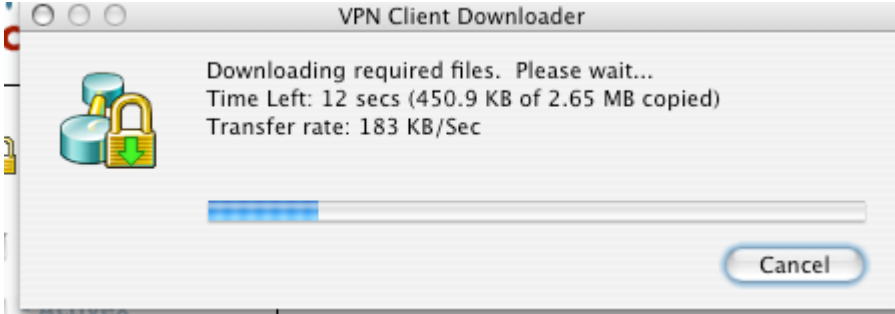


Figure 5
The SSL WebVPN client will begin downloading (Figure 5).



Figure 6

This screen informs the user that a Cisco SSL VPN Client is temporarily being installed on the end users system. The Cisco SSL VPN Client for WebVPN is a thin-client application. In most cases, the user initializing the connection should not need Administrator Level Rights on the local machine (Figure 6).



Figure 7
A window will open letting the user know that a secure connection has been established (Figure 7).

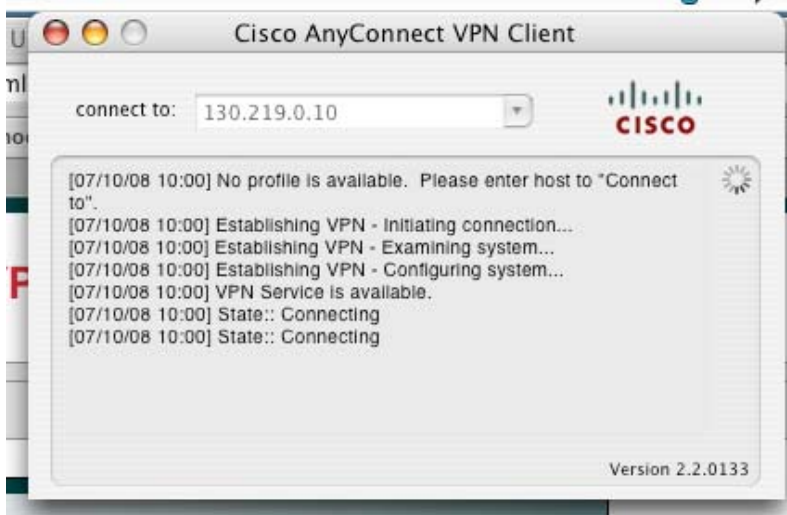


Figure 8

A status window will display negotiations (Figure 8).

At this point, you can minimize or close your browser window.

You are now connected to the University network. Any applications that require a secure connection can be used.

When you are finished with University business, always remember to end your VPN session. This is illustrated in the below screenshot.

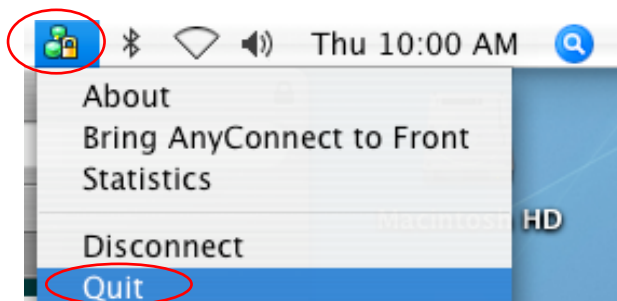


Figure 9

On the top right you will see the WebVPN icon showing the connection. If you click the icon, you will have the option of viewing the statistics of the connection, disconnecting, or quitting the application (Figure 9).

Choose “Quit”, when you are ready to terminate the connection.

Terminology

Thin-Client: A thin client is an application program that communicates with an application server and relies for most significant elements of its business logic on a separate piece of software, an application server, typically running on a host computer located nearby in a LAN or at a distance on a WAN or MAN.

A thin client does most of its processing on a central server/device with as little hardware and software as possible at the user's location, and as much as possible at some centralized managed site.

Certificate: (also known as a public key certificate) In cryptography, a public key certificate is a certificate which uses a digital signature to bind together a public key with an identity, information such as the name of a person or organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI), the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (self-signed certificate) or other users ("endorsements").

VPN: A virtual private network (VPN) is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a wider network. VPN message traffic can be carried over a public networking infrastructure (e.g. the Internet) on top of standard protocols, or over a private network with a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

VPN involves two parts: the protected or "inside" network, which provides physical and administrative security to protect the transmission; and a less trustworthy, "outside" network or segment (usually through the Internet). Generally, a firewall sits between a remote user's workstation or client and the host network or server. As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter. A known trusted person, sometimes only when using trusted devices, can be provided with appropriate security privileges to access resources not available to general users.

Concentrator: In telecommunication, the term concentrator has the following meanings:

In data transmission, a functional unit that permits a common path to handle more data sources than there are channels currently available within the path. A concentrator usually provides communication capability between many low-speed, usually asynchronous channels and one or more high-speed, usually synchronous channels. Usually different speeds, codes, and protocols can be accommodated on the low-speed side. The low-speed channels usually operate in contention and require buffering.

A device that connects a number of circuits, which are not all used at once, to a smaller group of circuits for economy.

ISP usually use concentrators to enable modem dialin, this kind of concentrator is sometimes called a modem concentrator or a remote access concentrator.

SSL: Secure Socket Layer is a cryptographic protocol which provides secure communications on the Internet for such things as e-mail, faxing, and other transfers.

SSL provides endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated, while the client remains unauthenticated; mutual authentication requires public key infrastructure (PKI) deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.