How do I Install and Use the Cisco VPN Any Connect Client for the Berkeley Campus?

"The Cisco virtual private network (VPN) client allows a computer to make secure network connections via specific equipment called VPN concentrators located on the campus network. Using the VPN, all network traffic between your computer and the VPN concentrator is encrypted. In addition, the VPN allows you to connect to other systems as if your computer were on campus, whether or not it actually is physically located on the Berkeley "campus network."

– From software.berkeley.edu

This document includes step by step instructions that will cover the following four areas

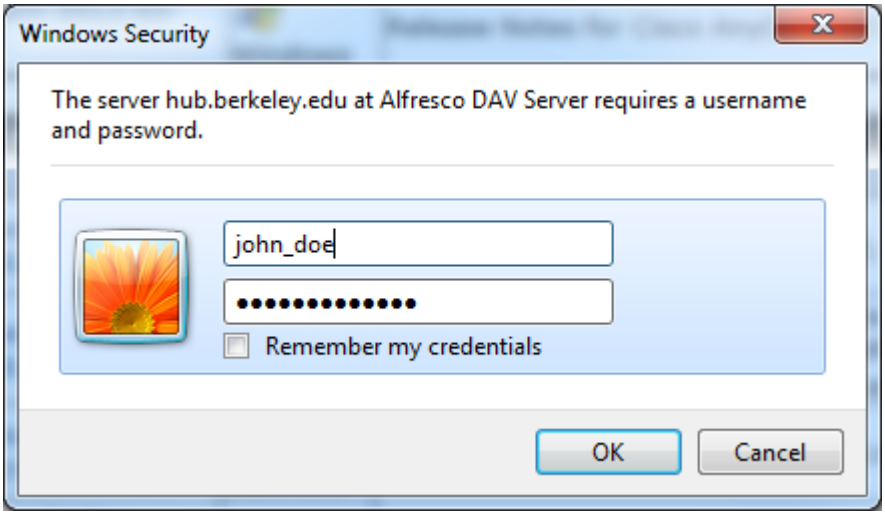
- Installing the Cisco Virtual Private Network (VPN)
- Connecting to the VPN
- Mapping a Haas Drive

Note: *Before you install the new version of the Cisco VPN make sure that any previous versions of the program are* ***uninstalled****. If you do uninstall a previous version,* ***make sure to reboot your computer afterwards to clear the registry****.*

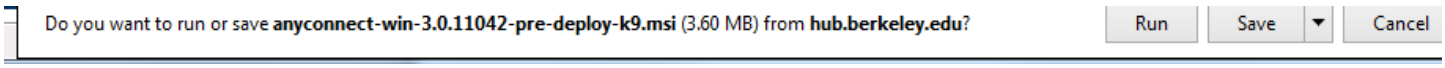
Step	Procedure
1	***Installing the Cisco VPN*** **a.** To install the Cisco VPN you will need to first download it from http://software.berkeley.edu **b.** Select the appropriate download link for your platform (i.e. Windows, Macintosh, Linux…) *Please note that if you are using Windows 8 you may need to install the Early Adopter Version*

Cisco VPN - Current Version 3.0.11042		
Name	**Platform**	**Description**
anyconnect-win-3.0.11042-pre-deploy-k9.msi	Windows	VPN Client Only for Windows XP SP3, Vista SP2, Win 7 SP1.
anyconnect-win-3.0.11042-pre-deploy-k9.zip	Windows	VPN Client for Windows XP SP3, Vista SP2, Win 7 SP1 .zip file. Full installation package on Windows platforms. This includes installation packages for DART, NAM, VPN, Telemetry, Hostscan, and WebSecurity components.
anyconnect-macosx-i386-3.0.11042-k9.dmg	Macintosh	VPN Client for Mac OS X versions 10.5 (32-bit only), 10.6, 10.7 and 10.8 (32 and 64 bit).
anyconnect-predeploy-linux-3.0.11046-k9.tar.gz	Linux	VPN Client for Linux 32-bit (RHEL5, RHEL6, Ubuntu 9.x, Ubuntu 10.x)
anyconnect-predeploy-linux-64-3.0.11046-k9.tar.gz	Linux	VPN Client for Linux 64-bit (RHEL5, RHEL6, Ubuntu 9.x, Ubuntu 10.x)
anyconnect-win-3.0.11042-pre-deploy-k9.iso	Windows	VPN Client for Windows XP SP3, Vista SP2, Win 7 SP1 .iso file. Full installation package on Windows platforms. This includes installation packages for DART, NAM, VPN, Telemetry, Hostscan, and WebSecurity components.
anyconnect30rn-2013-03-20.pdf	Windows	Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.0

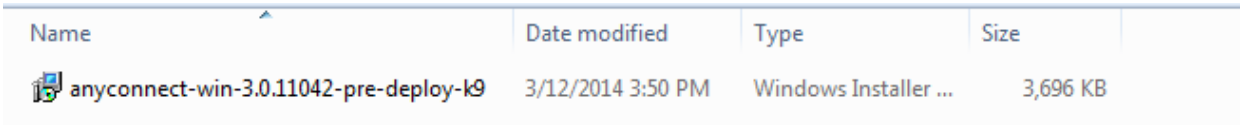
Step	Procedure
2	You'll be prompted for your **Calnet ID** and **passphrase**.



Step	Procedure
3	At the bottom of the page you will be asked if you'd like to **Save** or **Run** the program. Choose whatever option you wish.

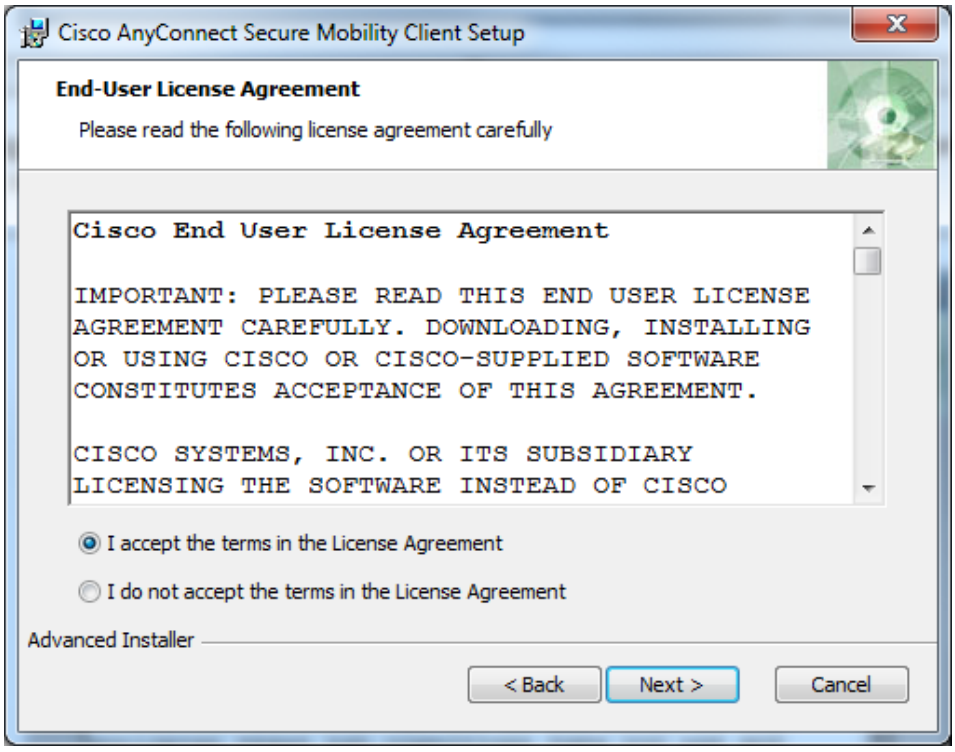


Step	Procedure
4	If you downloaded the installer, go to the place where you saved it and double click to open it.

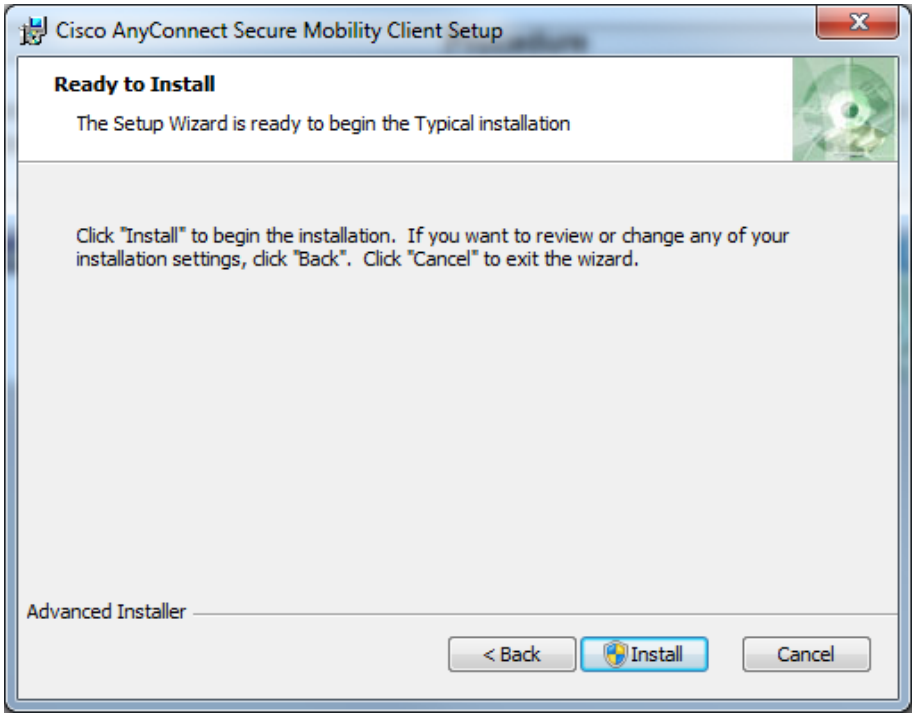


Step	Procedure
5	After you **double click** on the file you downloaded, choose **Run**. Then you will see a window like the one below. Click **Next**.

Step	Procedure
6	At the **License Agreement** window choose the radio button "**I accept the license agreement**", and then click **Next**. Click **Next** at the **Destination Folder** window.



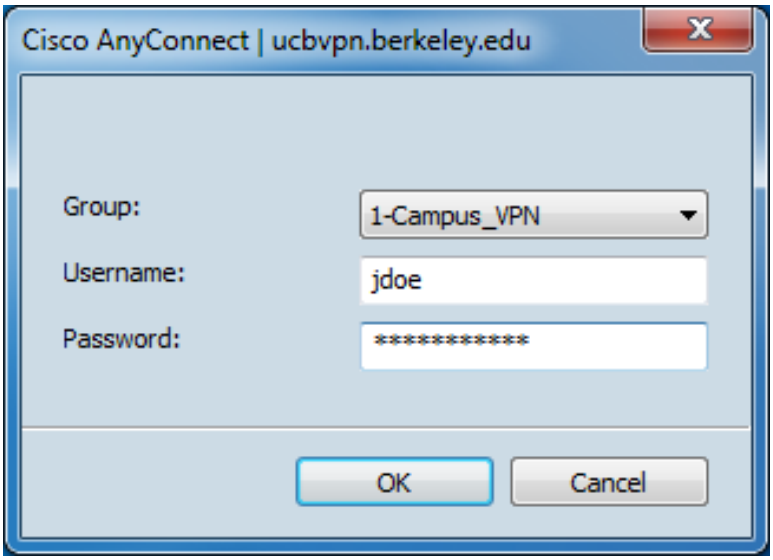
Step	Procedure
7	Click **Install** at the **Ready to Install the Application** window. The Cisco VPN will start to install. This will take around 1.5 minutes.



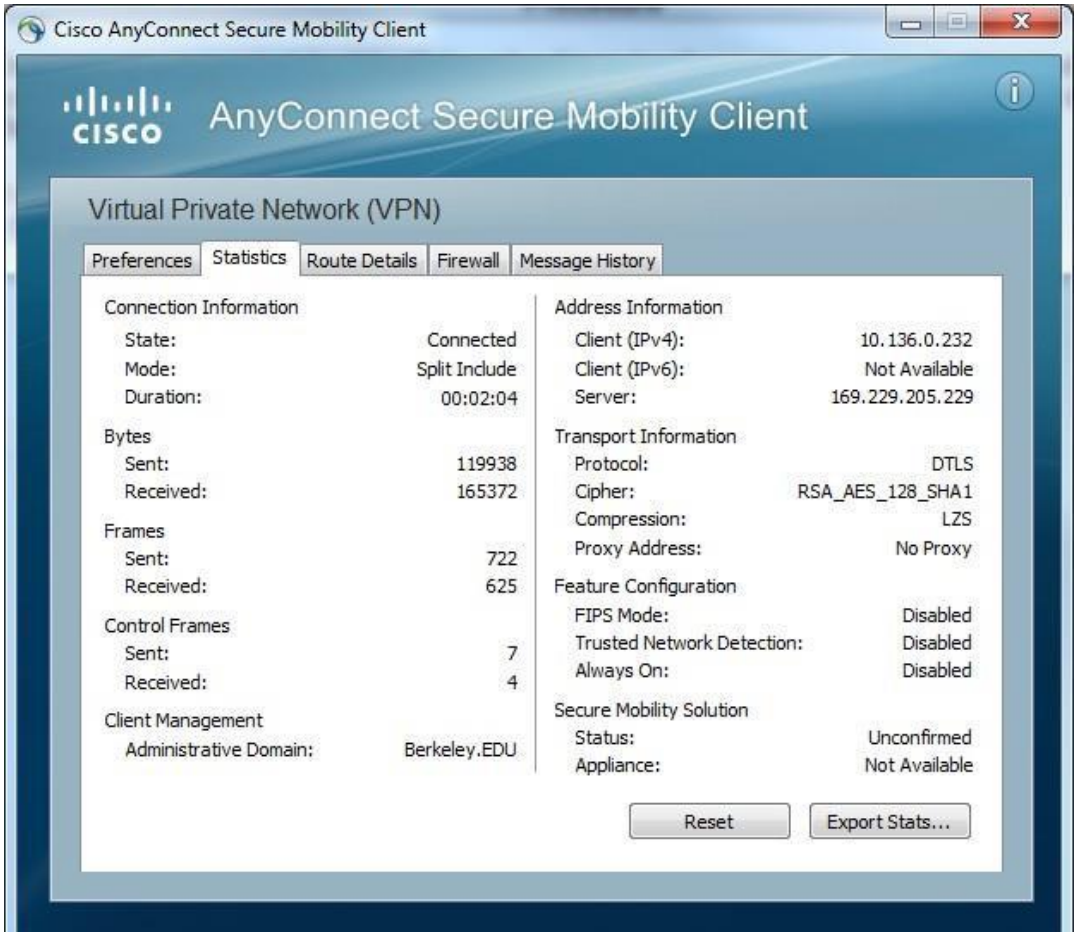
Step	Procedure
8	After the Cisco VPN finishes installing you will see the window below. Click **Finish**. If prompted, **reboot** your computer.

Step	Procedure
9	***Connecting to the VPN*** a. **Open** the **Cisco VPN Client**. b. Under VPN Ready to connect. Enter "**ucbvpn.berkeley.edu**" (without quotes). c. **Click** the **Connect** button.

Step	Procedur
10	a. After a few seconds you will be asked for your credentials b. Enter your CalNet ID and passphrase, then click the **OK** button to log into the VPN. c. You will then see the **VPN Client Banner** window on the lower right hand corner of the screen as the VPN tries to connect

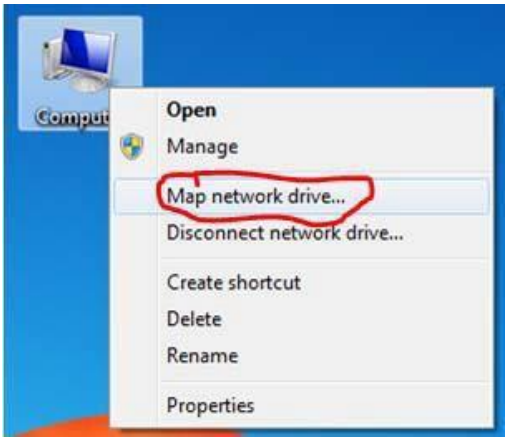


Step	Procedure
11	a. Once you are connected **double-click** on the Cisco AnyConnect icon with a lock that is in your taskbar (bottom right corner of the screen) to confirm your connection details—such as your **Connection State**, the **Server Address**, and the **Time Connected** (Duration). b. If you are having difficulty connecting to the VPN server, visit the following website: https://kb.berkeley.edu/jivekb/entry.jspa?external ID=2665

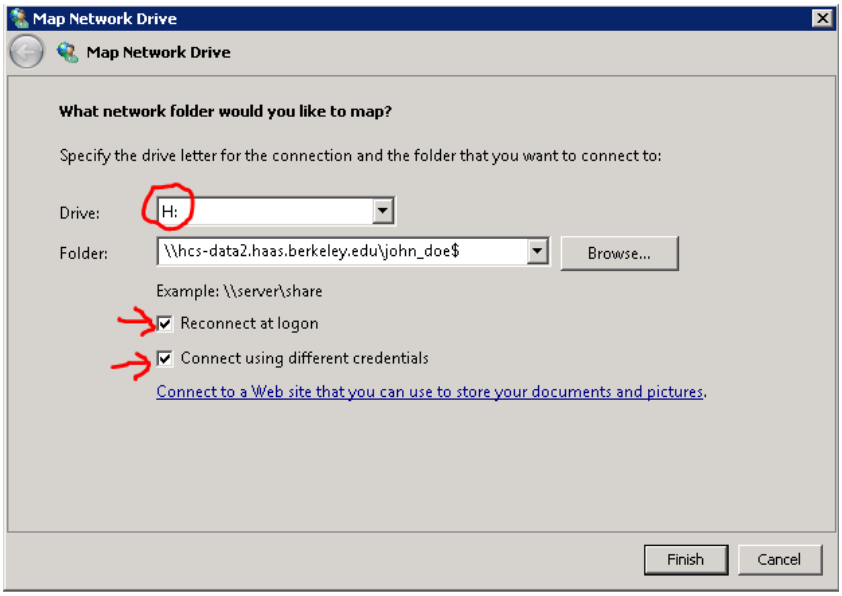


Step	Procedur
12	That is it. You have now installed and connected to the Cisco VPN. You can now access Haas resources such as the **Terminal Servers** or your Haas **H drive**. Below are the instructions for mapping a Haas drive.

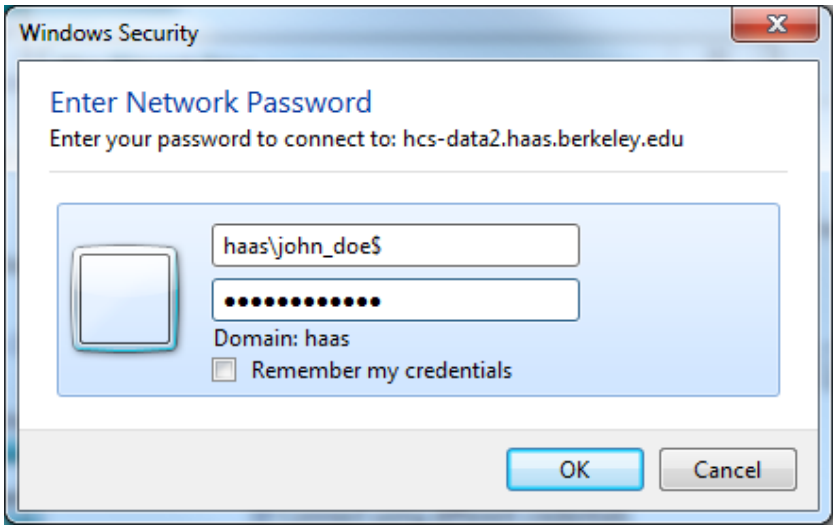
13	***Mapping a Haas Drive*** To map a drive, go to the **Start** menu > **Computer** > **Map Network Drive , or right click** on the **Computer** icon on your desktop and select **Map Netw ork Drive** In the example below we will map a student's **H drive**. This is the **Home drive** for any Haas user. **Note**: *Please see the end of this document for a list of all the Haas drives and the different paths students, faculty and staff should use to map their drives.*



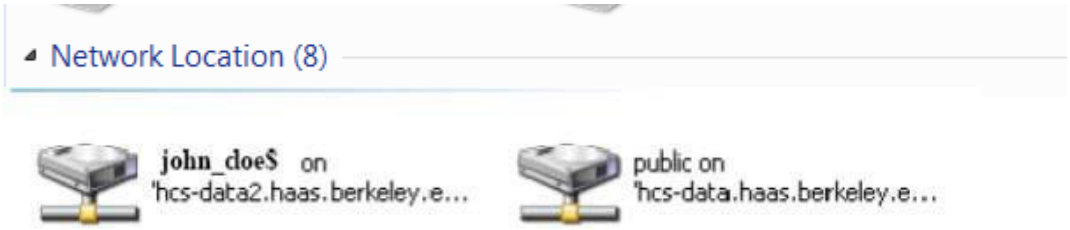
Step	Procedure
14	a. Choose an available drive letter, we suggest **H** for your **Home** drive. If you are a student type the following path for your H drive: **\\hcs-data2.haas.berkeley.edu*username$*** (i.e. if your username is *john_doe*, you would type:*\\hcs-data2\john_doe$)* **Note:** *Please see the list at the end of this document for all the drives Haas students, faculty, or staff can map through the Cisco VPN, and the paths each group should use.* b. You have the option of leaving the box "**Reconnect at logon**" checked, however, your computer will try to connect to the drive(s) you mapped **every time you log on**, and you will see the message "**Could not reconnect all netw ork drives**" in the system tray. On the other hand, if you leave this box checked you will not need to go through Steps 15a and b to connect to your drive(s) again. All you will need to do in the future is enter your Haas credentials —after you log in to the VPN of course. c. Next, **click** on the link "Connect using a **different user name**".



Step	Procedure
15	a. In the **Connect As ….** window, enter your **Haas username** in the following manner: User name: **haas*username*** Password: **Your Haas passw ord** b. Click **OK**, and then **Finish**.



Step	Procedure
16	The drive that you mapped should open after a few seconds. If not, open **double click on Computer**, and the drive should have appeared under **Network Drives**. You can open the drive from there and start using it as you normally would when you are at Haas. Please see the end of this document for a list of the different drives you can map.



Students

Drive Letter	Name	Path	Sample
H	Home Drive	**\\hcs-data2.haas.berkeley.edu\username$**	\\hcs-data2.haas.berkeley.edu\john_doe$
P	Public Drive	**\\hcs-data.haas.berkeley.edu\public**	\hcs-data.haas.berkeley.edu\public

Faculty and Staff

Drive Letter	Name	Path	Sample
H	Home Drive	**\\hcs-data.haas.berkeley.edu\username$**	\\hcs-data.haas.berkeley.edu\john_doe$
P	Public Drive	**\\hcs-data.haas.berkeley.edu\public**	\\hcs-data.haas.berkeley.edu\public