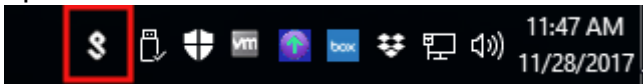


If connecting from outside the UCSF Network, including UCSF Guest wireless connections, you will need to use your Pulse Secure VPN Client Application to connect to the UCSF Network

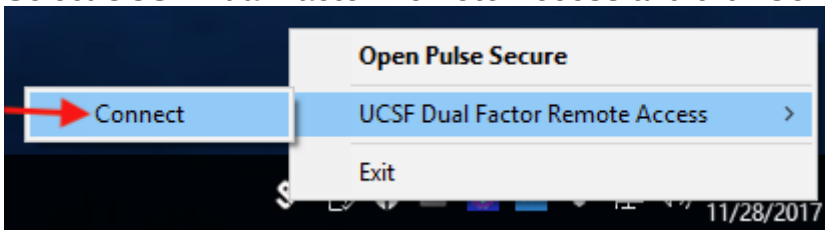
You will need to download the Network Connect application if you have not already done so. Please go to "<http://software.ucsf.edu/applications/vpn.html>" and download the "

Pulse Secure for Windows Instructions

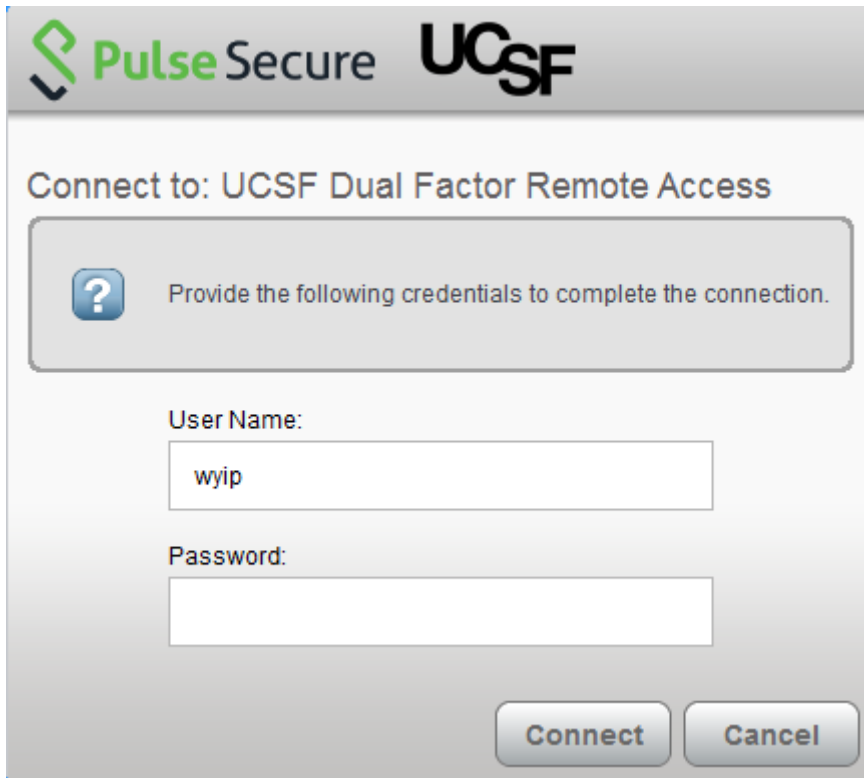
1. Download^[1] the Pulse Secure for Windows VPN client installer
2. Double click the downloaded installation package to install
3. Once the installation is complete, click on the **Pulse Secure** icon in the system tray to open the Pulse menu



4. Select **UCSF Dual Factor Remote Access** and click **Connect**

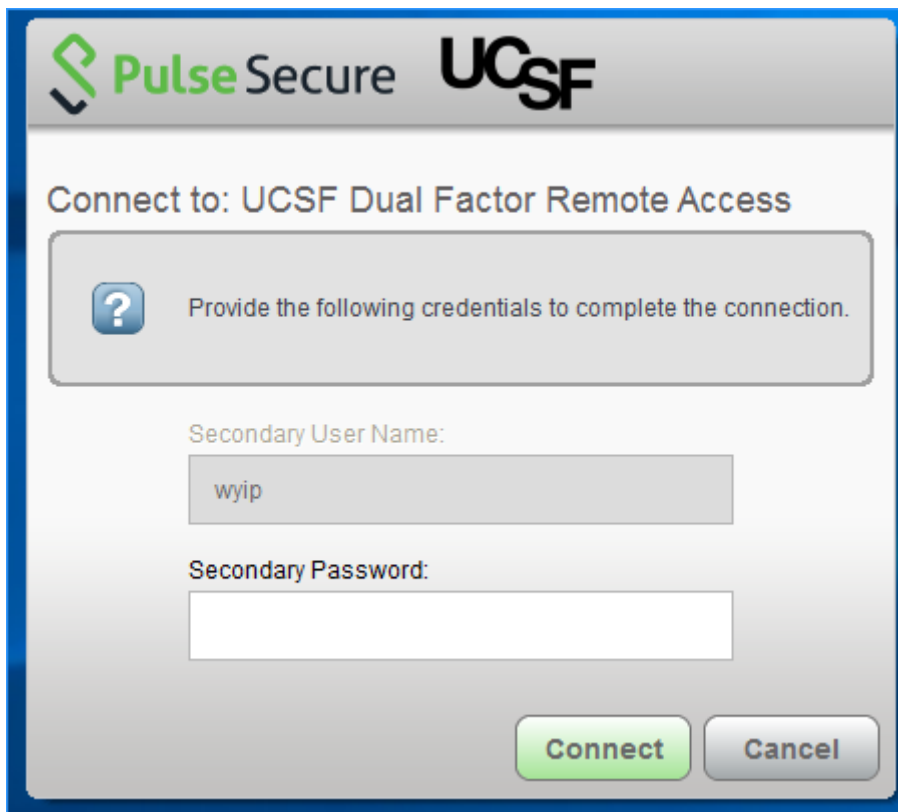


5. Enter UCSF username and password and click **Connect**



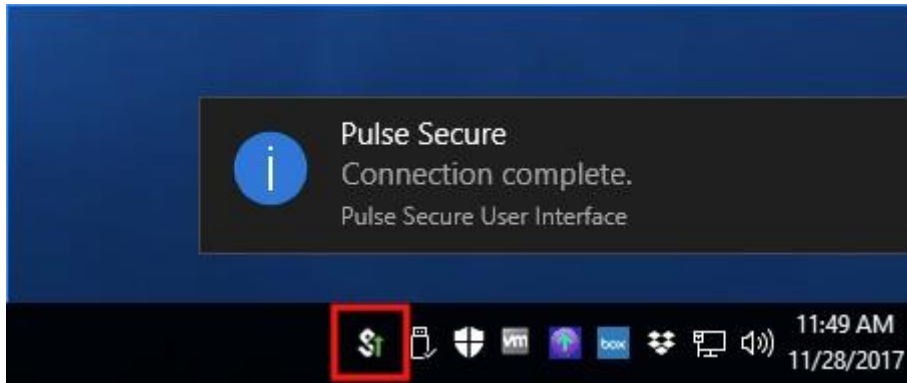
The image shows a Pulse Secure login window for UCSF. The title bar says "Pulse Secure UCSF". Below the title bar, it says "Connect to: UCSF Dual Factor Remote Access". There is a message box with a question mark icon that says "Provide the following credentials to complete the connection." Below this, there are two input fields: "User Name:" with the text "wyip" and "Password:" which is empty. At the bottom right, there are two buttons: "Connect" and "Cancel".

6. Use one of the [Duo authentication methods](#) [2] to provide a **Secondary Password** and click **Connect**

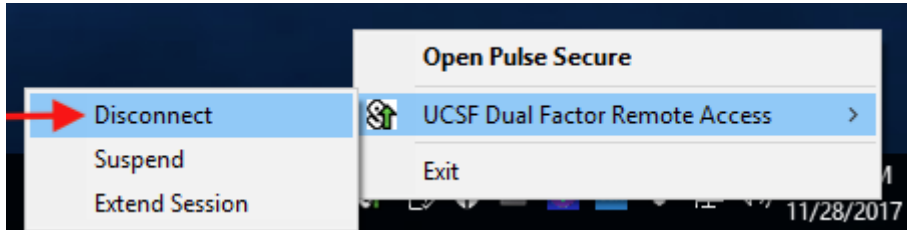


The image shows the same Pulse Secure login window for UCSF, but with a blue border. The title bar says "Pulse Secure UCSF". Below the title bar, it says "Connect to: UCSF Dual Factor Remote Access". There is a message box with a question mark icon that says "Provide the following credentials to complete the connection." Below this, there are two input fields: "Secondary User Name:" with the text "wyip" and "Secondary Password:" which is empty. At the bottom right, there are two buttons: "Connect" and "Cancel".

7. Pulse Secure will minimize to the taskbar, and the icon in the system tray will change indicating that it is connected to the UCSF network

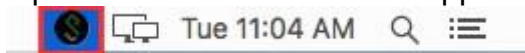


8. To disconnect Pulse Secure from the UCSF network, click on the **Pulse Secure** tray icon, select **UCSF Dual Factor Remote Access**, and click **Disconnect**

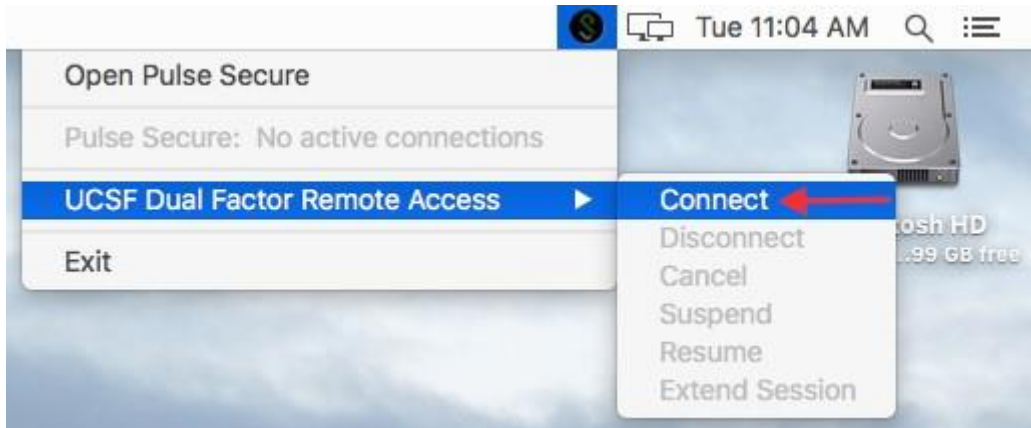


Pulse Secure for Mac Instructions

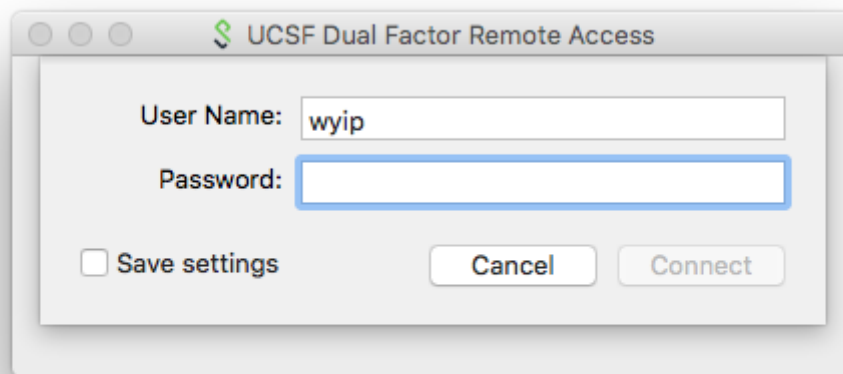
1. [Download](#) [1] the Pulse Secure for Mac VPN client installer
2. Double click the downloaded package and follow the prompts to install
3. Open Pulse Secure from the Applications folder, and click on the Pulse Secure icon



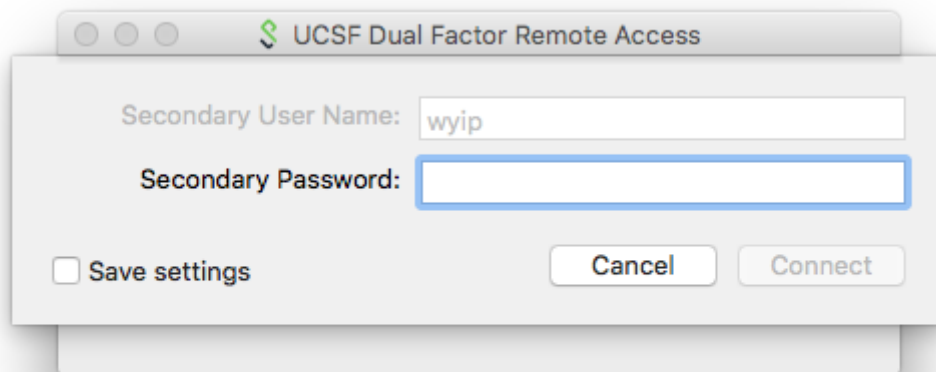
4. Select **UCSF Dual Factor Remote Access** and click **Connect**



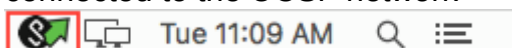
5. Enter UCSF username and password and click **Connect**



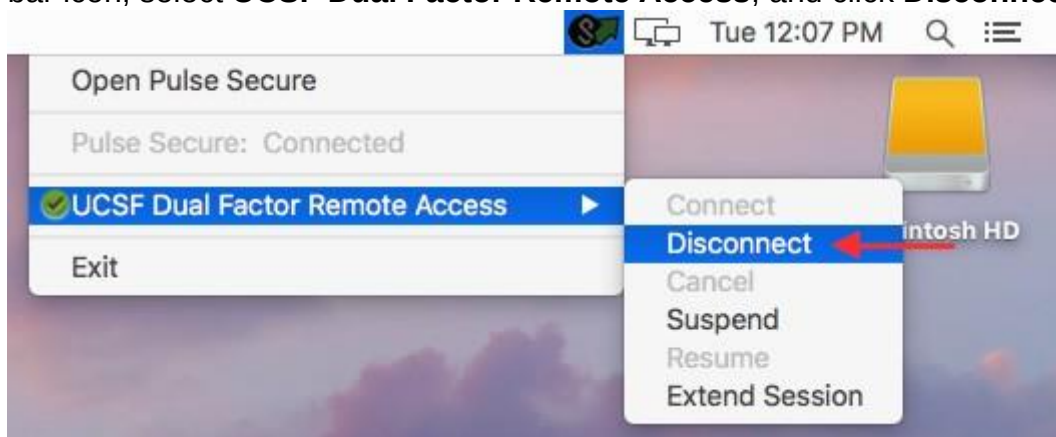
6. Use one of the [Duo authentication methods](#)^[2] to provide a Secondary Password and click **Connect**



7. Pulse Secure will minimize to the menu bar and the icon will change indicating that it is connected to the UCSF network



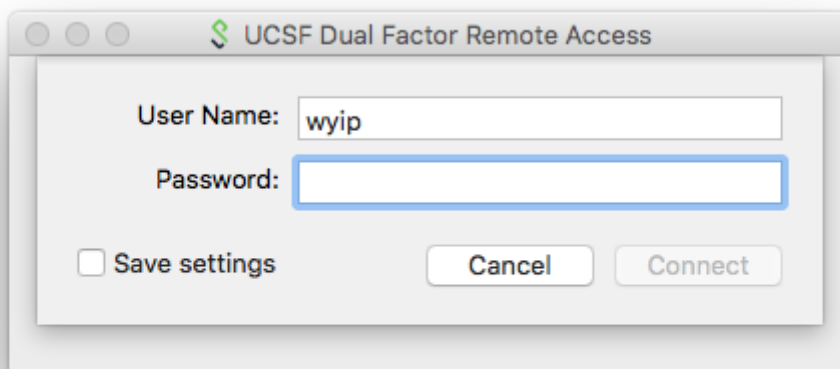
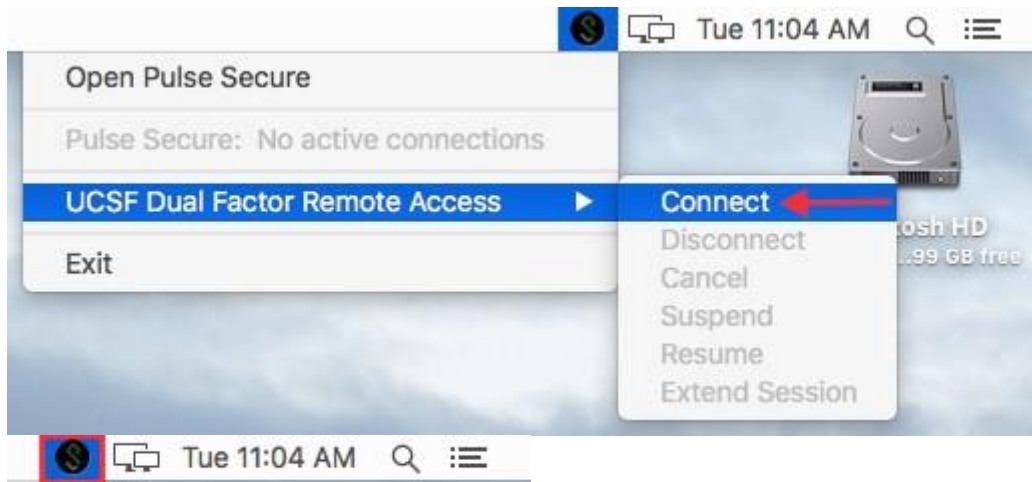
8. To disconnect Pulse Secure from the UCSF network, click on the Pulse Secure menu bar icon, select **UCSF Dual Factor Remote Access**, and click **Disconnect**



Required Service Information

VPN_[3]

Images

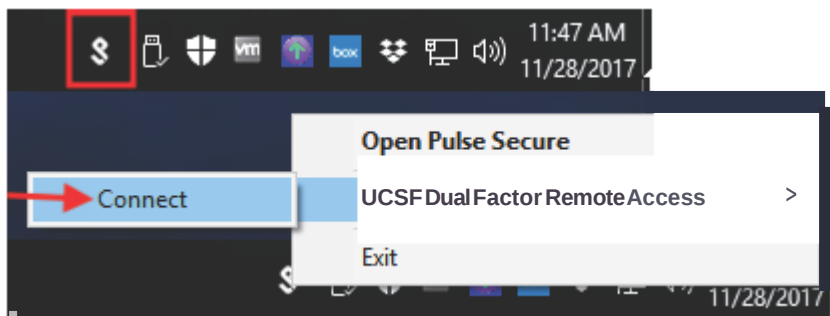


S UCSF Dual Factor Remote Access

--;cond:::a | lse1 ':\|"'IP' wyip

Secondary Password:

0 Save settings



ul Secure IJQ;f

Connect to: UCSF Dual Factor Remote Access

Provide the following credentials to complete the connection.

User Name:

| wyip

Password:



(Connect J (Cancel J

Connect to: UCSF Dual Factor Remote Access

li2J

Provide the following credentials to complete the connection.

Secondary UserName:

wyip

Secondary Password:

Connect

Cancel



Pulse Secure

Connection complete.

Pulse Secure User Interface



11:49 AM
11/28/2017

Open Pulse Secure



UCSF Dual Factor Remote Access

Exit

Disconnect

Suspend

Extend Session

Open Pulse Secure

ted

✓ UCSF Dual Factor Remote Access

Exit

Connect

Disconnect

Suspend

Extend Session



Intosh HD

C:\ Tue 11:09 AM Q.

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Site Login Site Index

Suggest an IT Improvement | © UC Regents

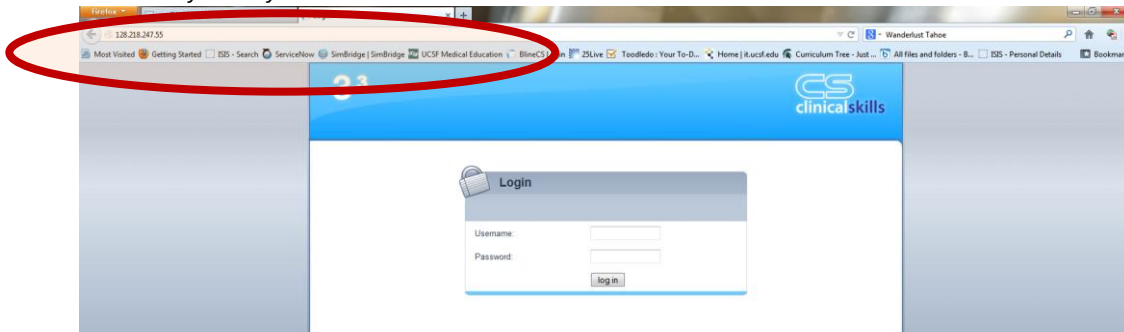
Source URL: <https://it.ucsf.edu/services/vpn/configure/how-log-vpn>

Links:

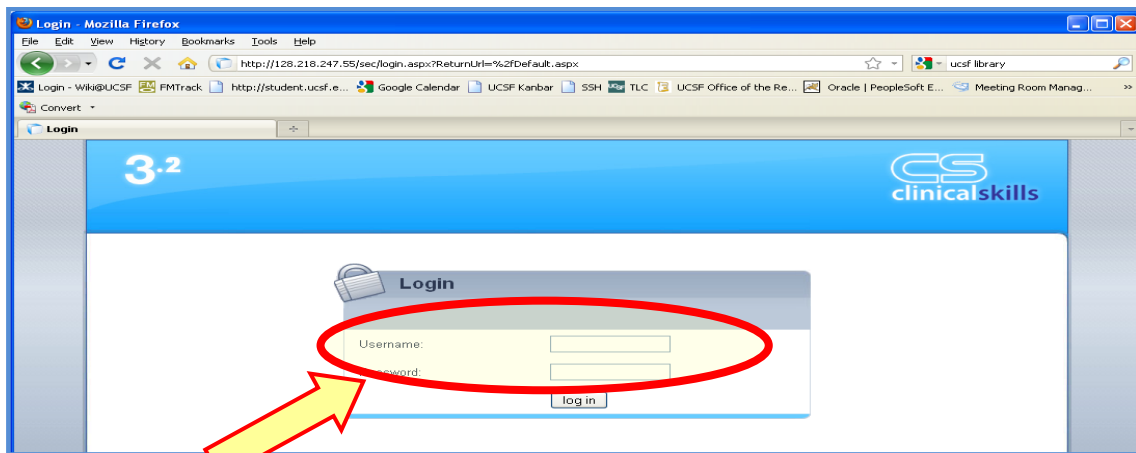
- [1] <https://software.ucsf.edu/content/vpn-virtual-private-network>
- [2] <https://it.ucsf.edu/services/duo-two-factor-authentication/additional/duo-authentication-methods>
- [3] <https://it.ucsf.edu/services/vpn>

Now you can open any browser such as Chrome and Firefox.

1. Within the browser open a new tab or window and type **128.218.247.55** in the browser address field and press the enter button on your keyboard



2. You should now see the following B-line Clinical Skills logon window



Username account information: The account name is the same account name you use to logon to UCSF Campus email. The account name is generally one of the three following options:

1. Last name and first initial (e.g. Michael Smith would be SmithM) and the password is the same password you use for your Campus email.
2. Student Campus ID number used for the UCSF MyAccess system (e.g. SF123456) and the password is the same password you use for your Campus email.
3. Issued user or group B-Line IDs and passwords on the day of the learning activity.

NOTE: UCSF Network connections, including UCSFWPA Wireless connections, can bypass the step of using the remote VPN@UCSF connection, and can connect directly to the B-line Clinical Skills interface.

Steps:

1. Open web browser (Firefox and/or Internet Explorer)

2. Type **128.218.247.55** in the Go To Address field and click the return key (enter button)

