Revised 02/05/2022

ACCESSING QUARTUS PRIME

This document contains information for accessing the software program needed in the ECE102 labs: **Quartus Prime**.

You will be using Quartus Prime for all the lab exercises in ECE102. It is the interfacing software for the Altera DE0-CV FPGA development board. The document includes information for both MAC OSX and Windows users. Keep in mind that this software package will be useful to you in future courses.

- ***IMPORTANT:*** Before proceeding with this tutorial, please create an Engineering account if you don't already have one. Creating an engineering account will provide you with login credentials that you will need in order to access the engineering resources/software available to you as an engineering student. *These credentials may be different from your CSU eID and password that you use for Canvas and RAMweb*. You can create an account by visiting the CSU ETS website by clicking on the link below:

  https://www.engr.colostate.edu/ets/tools/create-account/

- Select "Log-In with CSU Single Sign-On
- Enter your CSU eID and password (The same credentials for Canvas and RAMweb)
- Follow the instructions and enter the appropriate information.

NOTE: Your request for an engineering account may take 1-2 days to go through, so please be sure to submit this request ***at least 1 day before*** your first ECE102 lab session.

Option 1: On Campus

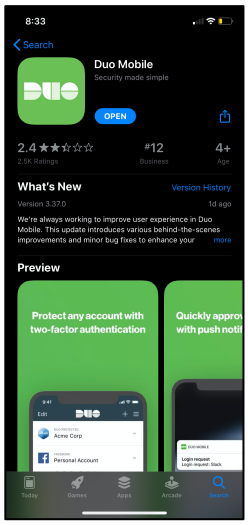
This is the most straightforward and easiest way to access the Quartus Prime software. You simply sign into any computer in the C207 lab with your *engineering account*.

- NOTE: It is best to save all your work on your *U-drive* (home folder) so that you can access that material whether you're on-campus or off-campus. This is especially important because you may not always be able to access the same computer and/or access the labs in general, so it is crucial that you can access your lab material wherever you are.

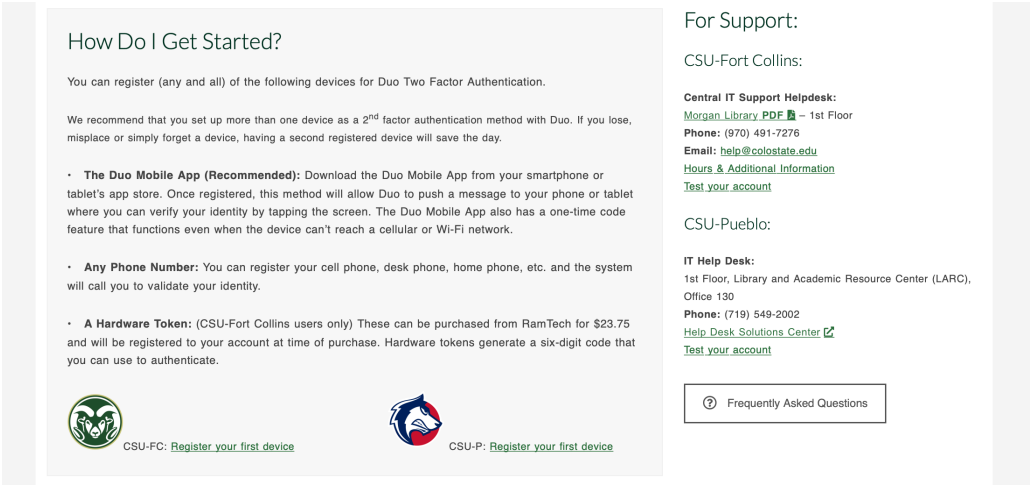
Option 2: Off-Campus (Virtual Classroom)

You can access the software while being off-campus through what is known as the "Virtual Classroom". The Engineering Virtual Classroom is a way for you to gain access to most of the Engineering software from a remote location. To access the Virtual Classroom, you will need to download and install three applications: *DUO Mobile App*, *Pulse Secure*, and *Microsoft Remote Desktop*. Follow the step-by-step instructions below to set up the Virtual Classroom on your computer:

- Using your smartphone, download the *DUO Mobile App* from your phone's store.



- Using your desktop/PC computer, go to https://www.acns.colostate.edu/duo/
- Scroll down and navigate to "How do I get Started?"
- Click on the "Register your first device" link



How Do I Get Started?

You can register (any and all) of the following devices for Duo Two Factor Authentication.

We recommend that you set up more than one device as a 2nd factor authentication method with Duo. If you lose, misplace or simply forget a device, having a second registered device will save the day.

- **The Duo Mobile App (Recommended):** Download the Duo Mobile App from your smartphone or tablet's app store. Once registered, this method will allow Duo to push a message to your phone or tablet where you can verify your identity by tapping the screen. The Duo Mobile App also has a one-time code feature that functions even when the device can't reach a cellular or Wi-Fi network.
- **Any Phone Number:** You can register your cell phone, desk phone, home phone, etc. and the system will call you to validate your identity.
- **A Hardware Token:** (CSU-Fort Collins users only) These can be purchased from RamTech for $23.75 and will be registered to your account at time of purchase. Hardware tokens generate a six-digit code that you can use to authenticate.

CSU-FC: Register your first device

CSU-P: Register your first device

For Support:

CSU-Fort Collins:

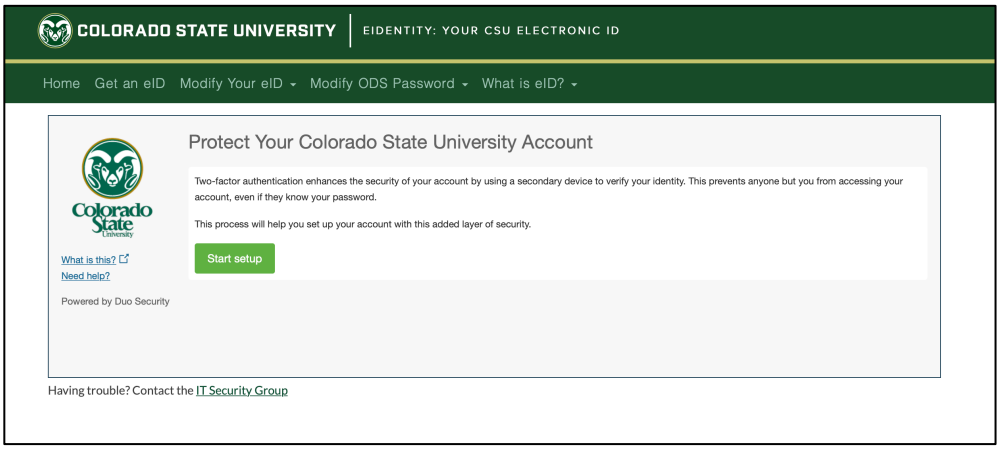
Central IT Support Helpdesk:
Morgan Library PDF – 1st Floor
Phone: (970) 491-7276
Email: help@colostate.edu
Hours & Additional Information
Test your account

CSU-Pueblo:

IT Help Desk:
1st Floor, Library and Academic Resource Center (LARC), Office 130
Phone: (719) 549-2002
Help Desk Solutions Center
Test your account

Frequently Asked Questions

- You will be redirected to a page that requires you to enter you CSU eID and password. Enter your credentials to continue with device registration.
- If the following page below doesn't pop up, then hover over "Modify your eID" and click on "DUO self-service"

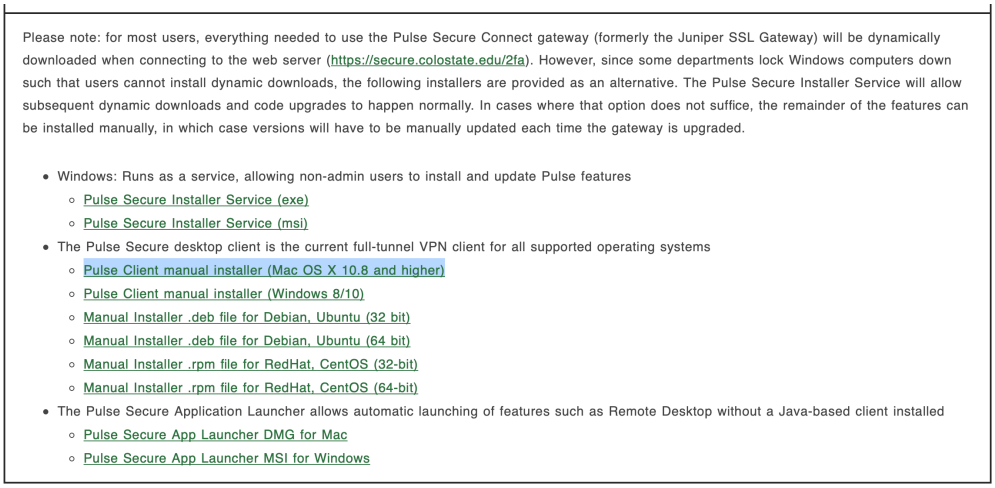


- Click "Start setup"
- Select the type of device you would like to use. We recommend choosing "mobile phone". Then click continue and enter your phone number.
- Click continue and select the type of phone you have.
- Select "I have DUO Mobile installed"
- A new screen will appear with a barcode.
- From your smartphone device, open the *Duo Mobile App*. Tap the "+" button. Scan the barcode shown on your desktop/PC computer.
- Once you have scanned the barcode, the webpage page will now display the barcode with a green check mark across it and your DUO Mobile app will now display "Colorado State University" with a 6-digit code below it. Click continue on the webpage.
- A new page will display showing "My Settings & Devices". Click "Continue to Login"
- Select the option of your choice. "Send a push" is the easiest and simplest way which we recommend using.
- Your smartphone will now push a notification. Simply click on the notification, and select "Approve"
- You have now verified your identity and have successfully set up your second factor authorization method.

Now, you will have to download and install the *Pulse Secure* app to establish a Virtual Private Network (VPN). This process is different for MAC OSX and WINDOWS users, so follow the instructions below based off which system you use. (Windows Users should jump ahead to page 8)

MAC OSX USERS:

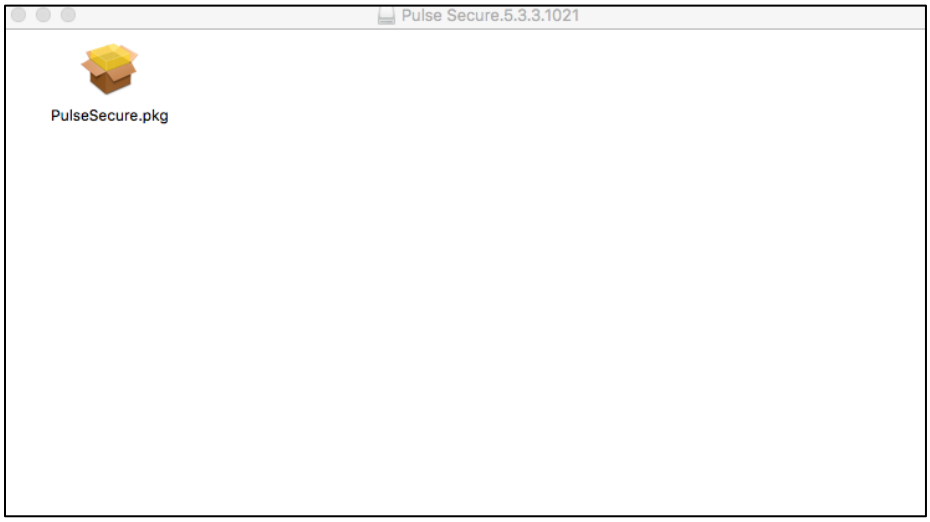
- Go to https://www.acns.colostate.edu/security/#1478123291089-f3918698-6eec
- Select "Pulse Client Manual Installer (MAC OSX 10.8 and Higher)"



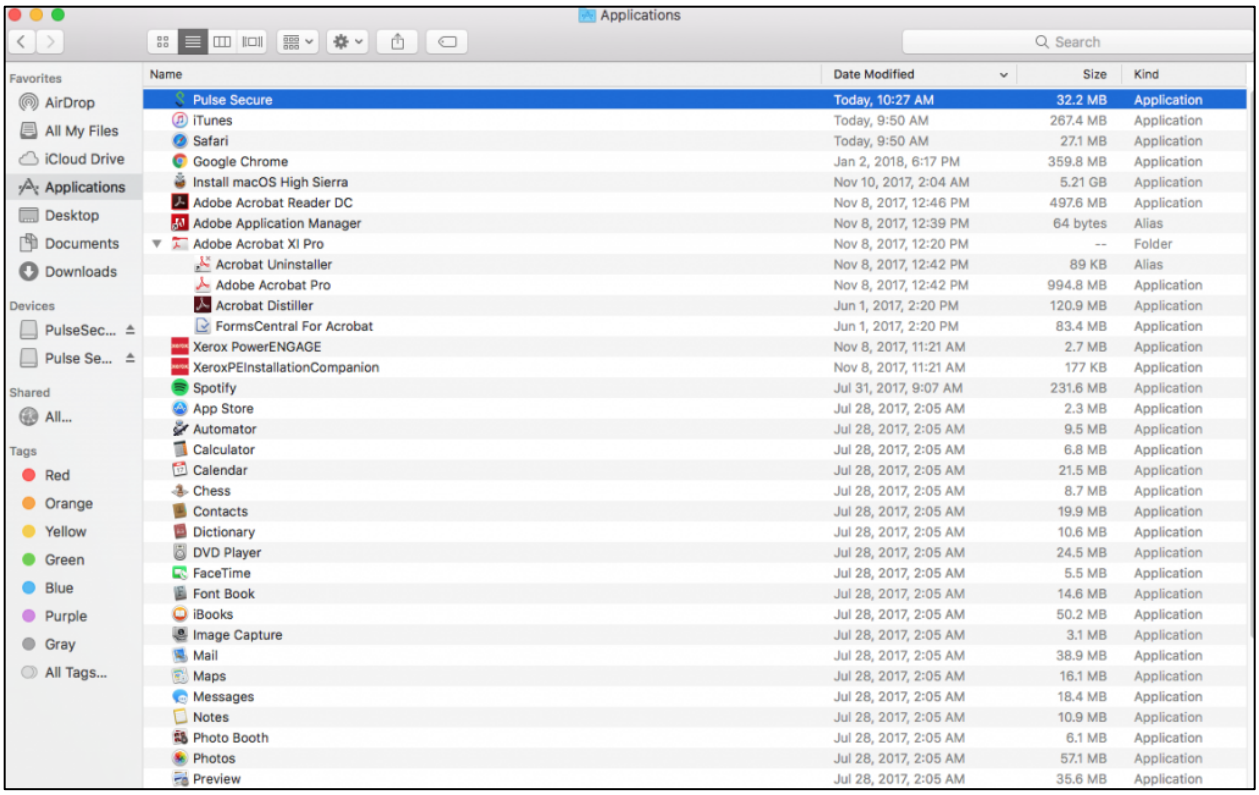
Please note: for most users, everything needed to use the Pulse Secure Connect gateway (formerly the Juniper SSL Gateway) will be dynamically downloaded when connecting to the web server (https://secure.colostate.edu/2fa). However, since some departments lock Windows computers down such that users cannot install dynamic downloads, the following installers are provided as an alternative. The Pulse Secure Installer Service will allow subsequent dynamic downloads and code upgrades to happen normally. In cases where that option does not suffice, the remainder of the features can be installed manually, in which case versions will have to be manually updated each time the gateway is upgraded.

- Windows: Runs as a service, allowing non-admin users to install and update Pulse features
  - Pulse Secure Installer Service (exe)
  - Pulse Secure Installer Service (msi)
- The Pulse Secure desktop client is the current full-tunnel VPN client for all supported operating systems
  - Pulse Client manual installer (Mac OS X 10.8 and higher)
  - Pulse Client manual installer (Windows 8/10)
  - Manual Installer .deb file for Debian, Ubuntu (32 bit)
  - Manual Installer .deb file for Debian, Ubuntu (64 bit)
  - Manual Installer .rpm file for RedHat, CentOS (32-bit)
  - Manual Installer .rpm file for RedHat, CentOS (64-bit)
- The Pulse Secure Application Launcher allows automatic launching of features such as Remote Desktop without a Java-based client installed
  - Pulse Secure App Launcher DMG for Mac
  - Pulse Secure App Launcher MSI for Windows

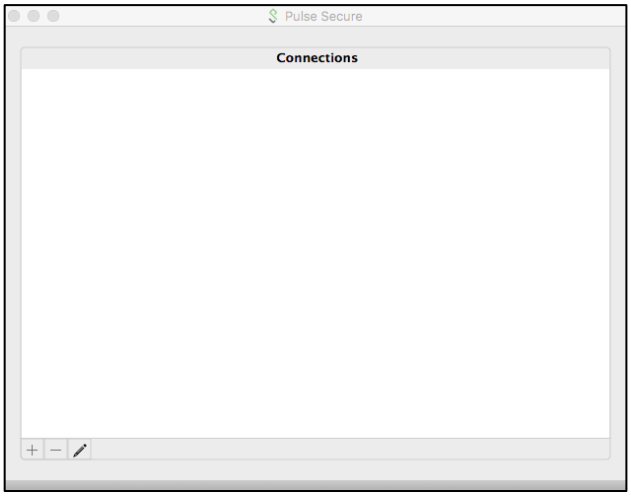
- To initiate the client install double-click on the downloaded Pulse Secure package file. Click Continue then Install. Keep the default settings during the rest of the installation.



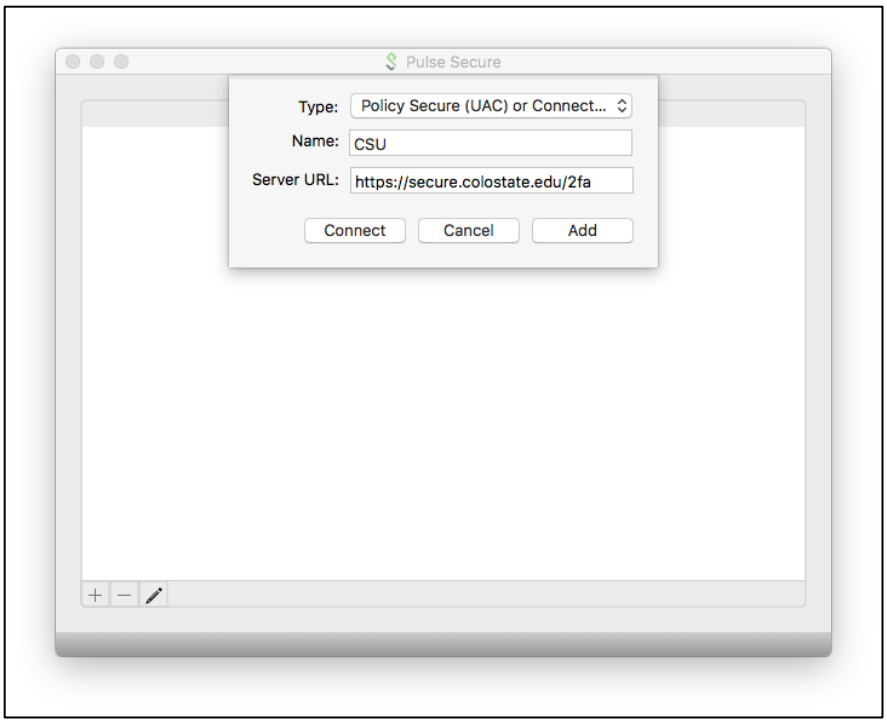
- When the installation is finished you should see a new icon in Applications named Pulse Secure.



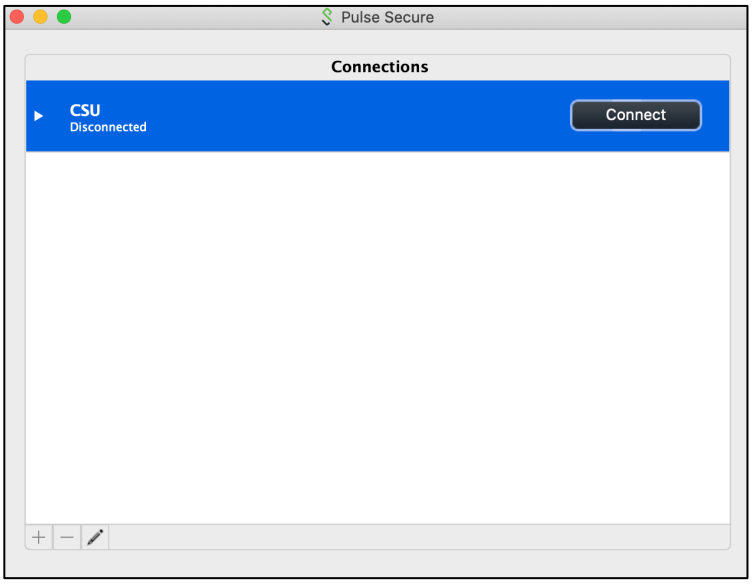
- In Applications, click on Pulse Secure. A Connections window should appear. Click on the "+" icon to open and add connection window.



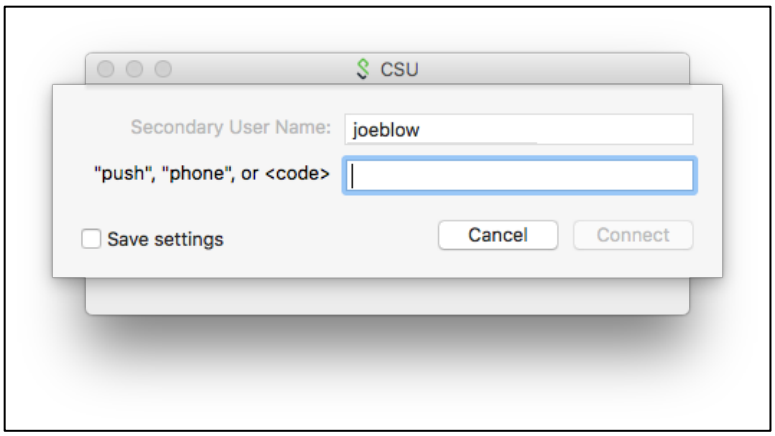
- In the add connection window keep UAC or SSL-VPN as the default type. You can name the connection whatever you want — for example, CSU. Enter the server URL for the secure gateway: https://secure.colostate.edu/



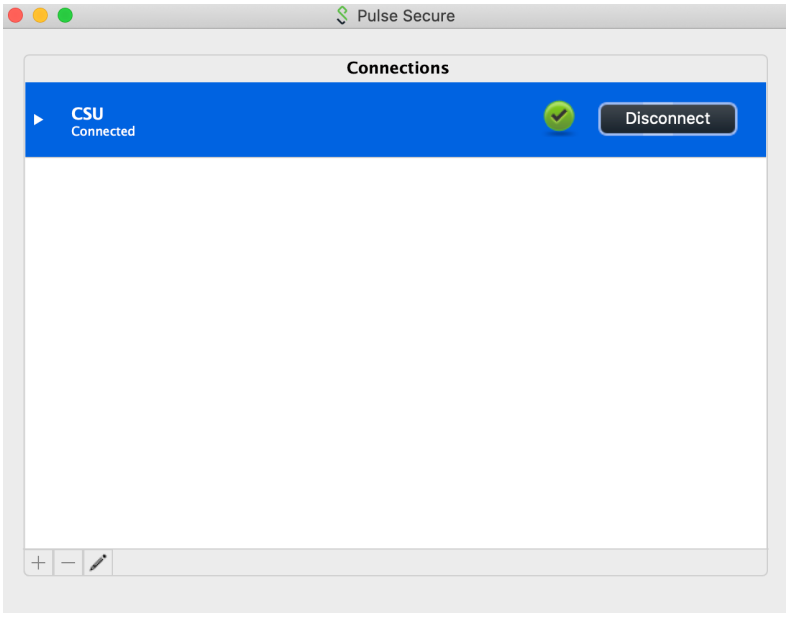
- When you have finished entering the connection information click “Add” to save the connection. The box will disappear and you will now see an option named “CSU”. On the right-hand side of that, click Connect.



- A small dialog box will pop up titled “Pre-Sign in Notification”. Click Proceed.
- A login box should appear. Enter your **CSU eID and password**, enable the Save settings box, then click Connect. Another box will pop up that looks like the one below:



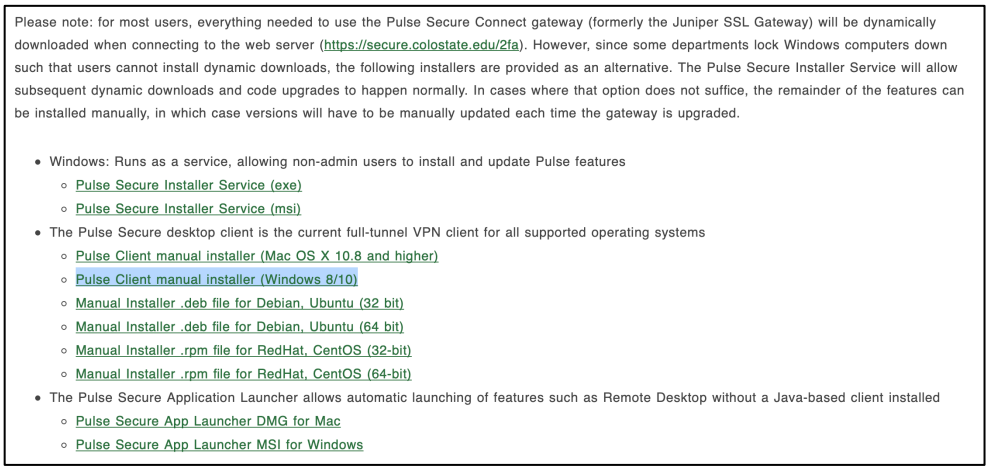
- IMPORTANT! Before Pulse Secure can connect, it will need you to supply your second authentication factor that you set up using the *DUO Mobile App*.
    - In the blank field, type “push” without the quotation marks. Once you have supplied this, the DUO Mobile App will push a notification on your mobile device. Simply open the notification on your device and click “Approve”. Pulse is now connected to the CSU network.



- From here you are now ready to start up Microsoft RDP client to connect to the Virtual Lab. Skip ahead to page 11.

WINDOWS USERS:

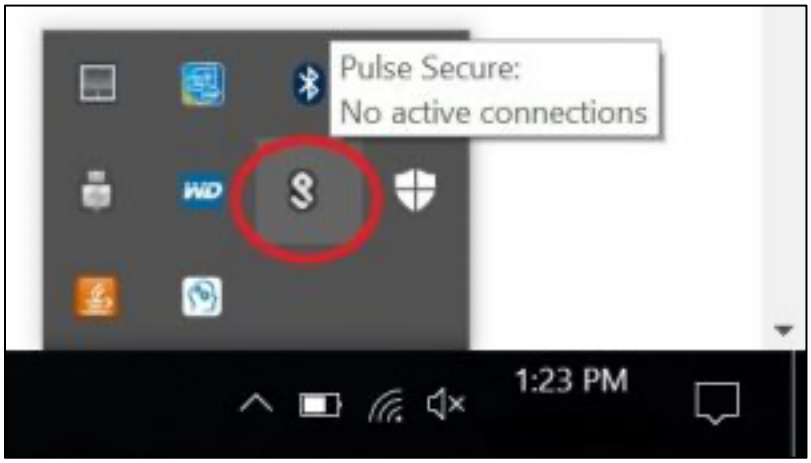
- Go to https://www.acns.colostate.edu/security/#1478123291089-f3918698-6eec
- Select “Pulse Client Manual Installer (Windows 8/10)”



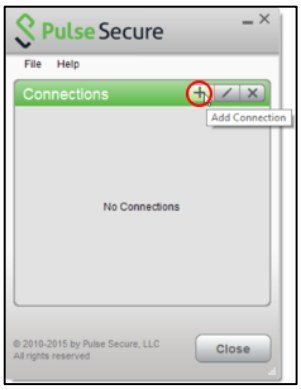
Please note: for most users, everything needed to use the Pulse Secure Connect gateway (formerly the Juniper SSL Gateway) will be dynamically downloaded when connecting to the web server (https://secure.colostate.edu/2fa). However, since some departments lock Windows computers down such that users cannot install dynamic downloads, the following installers are provided as an alternative. The Pulse Secure Installer Service will allow subsequent dynamic downloads and code upgrades to happen normally. In cases where that option does not suffice, the remainder of the features can be installed manually, in which case versions will have to be manually updated each time the gateway is upgraded.

- Windows: Runs as a service, allowing non-admin users to install and update Pulse features
  - Pulse Secure Installer Service (exe)
  - Pulse Secure Installer Service (msi)
- The Pulse Secure desktop client is the current full-tunnel VPN client for all supported operating systems
  - Pulse Client manual installer (Mac OS X 10.8 and higher)
  - Pulse Client manual installer (Windows 8/10)
  - Manual Installer .deb file for Debian, Ubuntu (32 bit)
  - Manual Installer .deb file for Debian, Ubuntu (64 bit)
  - Manual Installer .rpm file for RedHat, CentOS (32-bit)
  - Manual Installer .rpm file for RedHat, CentOS (64-bit)
- The Pulse Secure Application Launcher allows automatic launching of features such as Remote Desktop without a Java-based client installed
  - Pulse Secure App Launcher DMG for Mac
  - Pulse Secure App Launcher MSI for Windows

- Double click on the file and install Pulse Secure. Keep default settings during the installation.
- After the install finishes, you should see new icon in the lower right corner of your screen in the system.

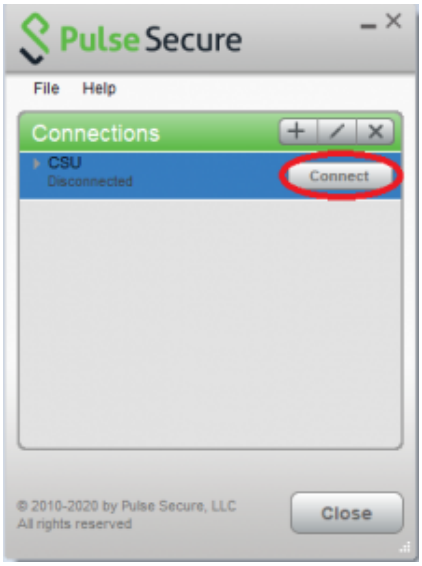


- Click on the Pulse icon and select “Open Pulse Secure”. Click on the “+” icon.



- In the next window, keep the default type as “UAC or SSL-VPN”.
    - For name, you can put in what you want. In the following example we use “CSU”. Finally, enter the server URL: https://secure.colostate.edu/

- Click to “Add” button. You should now see the following:



- At this point, click the "Connect" button and a new window will pop up prompting you to login with your **CSU eID and password.** Click the "Save settings" check box, then click the "Connect" button.

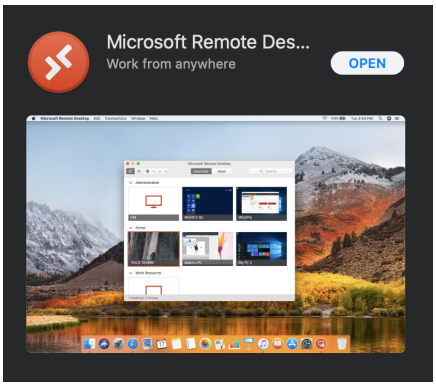
- At this point a request for a Secondary password will pop up. This is DUO Secondary Authentication. We recommend selecting "Send Me A Push". You will receive a notification on the mobile device you registered at the beginning of the tutorial. Open the notification, and select "Approve".
- You should get a green check on the Pulse Secure window next to "CSU" indicating you are connected. Keep in mind, every time you update your eID password, it will

not automatically update in Pulse. You will need to manually enter in and save the new entry.

- From here you are now ready to start up RDP client to connect to the Virtual Lab. Skip ahead to page 12.

MAC OSX USERS:

- Download and install "Microsoft Remote Desktop" from the App Store



- Download the connection file

- Double click the downloaded file, and ignore any certificate warnings.

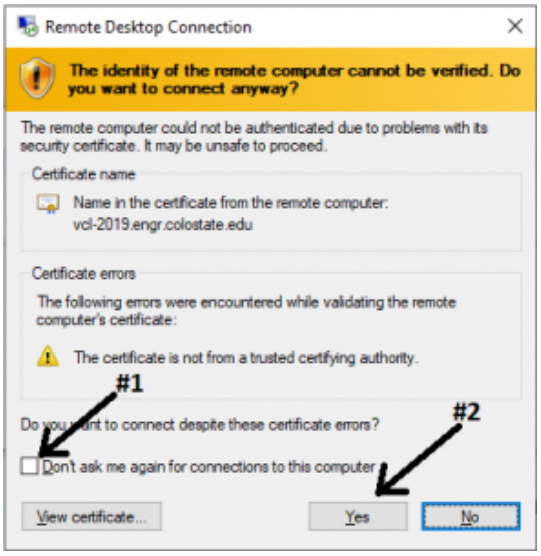
- Move the .rdp file to your desktop for future use (it's typically downloaded to your Downloads folder)

- Login using your Engineering username and password. For your username please format it as follows: "**engr.colostate.edu\username**"

- You have now established a remote connection to the Engineering Virtual Classroom and can access Quartus Prime.

WINDOWS USERS:

- Download the connection file
- Double click the downloaded file.
- When you get a warning similar to the image example below, check the “Don’t ask me again….” option



- Login using your Engineering username and password. For your username please format it as follows: “**engr.colostate.edu\username**“
- You have now established a remote connection to the Engineering Virtual Classroom and can access Quartus Prime.