Setting up CU Secure VPN service for Mac

1/29/2018
## Contents

Why we are doing this .................................................................................................................. 2  
Register for CU Secure.................................................................................................................. 2  
Installing the VPN desktop client ................................................................................................. 5  
  Apple computing device ........................................................................................................... 5  
  Updating your Duo profile using the self-service portal ................................................................. 16  
Troubleshooting tips....................................................................................................................... 21  
  VPN Access Portal .................................................................................................................. 21  
  GlobalProtect Desktop Client ................................................................................................... 21  
  Duo Registration and Mobile Client ............................................................................................ 22  
  General Connection Troubleshooting Tips .................................................................................. 23
Why we are doing this

The purpose of CU Secure is to provide an extra layer of security to your account when using VPN services to help prevent attackers from using your password information to access CU resources.

CU Secure uses something you know (your password), something you have (your computing device or phone), and somewhere you are (on or off campus), to validate that you are the approved person to access CU resources.

The following are the instructions for using CU Secure for VPN on a Windows PC and a Mac.

Register for CU Secure

1. Install Duo Mobile to your mobile device from the Apple App store, Google Play or the Microsoft Store.

   **Important!** There are multiple Duo apps. Please install the Duo Mobile app with the green logo, as shown.

2. Enroll for CU Secure by clicking on the access portal for your primary campus:

   **Important!** You cannot be connected to the CU Denver or CU Anschutz trusted networks to access to these portals or they will show an error.
   a. CU Denver: https://dc-vpn.ucdenver.edu
   b. Anschutz Medical Campus: https://amc-vpn.ucdenver.edu

3. Login with your CU network username and password.

   **Duo Authentication**

   Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

   This process will help you set up your account with this added layer of security.

   [Start setup button]

   [Logo: DUO]

   [Image: DUO Login]

   [Text: Protect Your CU Secure Account]

Office of Information Technology
UNIVERSITY OF COLORADO
DENVER | ANSCHUTZ MEDICAL CAMPUS
4. Select your preferred device type to receive the authentication request from the Duo application. We recommend using your mobile device, if possible.

**Duo Authentication**

5. If you've selected a mobile phone, input the phone number of the device and select the type of phone.
6. If you’ve chosen to authenticate using a mobile phone or tablet, install the app for your device from the iPhone App Store or Google Play for Android. Search for Duo Mobile.

7. After installing the smart phone app, scan the barcode to activate and link to your phone.
8. Choose your preferred authentication method and Save your preferences.

**Duo Authentication**

Installing the VPN desktop client

**Apple computing device**
Each campus has its own VPN access portal: [https://dc-vpn.ucdenver.edu](https://dc-vpn.ucdenver.edu) and [https://amc-vpn.ucdenver.edu](https://amc-vpn.ucdenver.edu). Using an Apple Mac computing device, login in to your campuses’ access portal as follows:

1. Copy and paste the access portal installation link for your campus into your preferred browser and enter your user name and password.
2. Select your preferred Duo authentication method.
   a. Duo Push:

   **Duo Authentication**

   ![Duo Authentication Interface]

   - **Duo Push RECOMMENDED**
   - **Send Me a Push**

   ![Click Approve to authenticate for VPN.]

   - **Approve**
   - **Deny**
b. Call Me:

Duo dials your registered phone.

Press any key on your phone to authenticate to VPN.
c. Passcode:

Click Enter a Passcode to authenticate via text.

7-digit code is texted to your phone.

You have 5 minutes to enter the passcode texted to your phone and click Log In.
3. Once authenticated, you will be directed to the Palo Alto website to download the GlobalProtect VPN client that is appropriate for your computer.

Select Download Mac32/64 bit GlobalProtect agent to install on a Mac.
4. By default, the installer is downloaded to your *Downloads* folder. Go to Finder and double-click `GlobalProtect.pkg`.

5. Select where you would like to install the software.
6. Check the box for GlobalProtect.

7. Click Install to begin the installation.
8. Enter your network credentials and click Install Software.

9. Close the installer.
**Note:** If you are running High Sierra, you may need to complete the following steps. If not, skip to step 14.

10. Open System Preferences.

![System Preferences](image)

11. Click on Security and Privacy.

12. High Sierra may generate a message informing that PaloAlto installed software and asking whether you would like to allow. Click the box to allow the software installation.
13. At the top of your Mac, you should see an icon that looks like a globe. Click on the globe.

14. Enter your campus VPN access portal address: dc-vpn.ucdenver.edu or amc-vpn.ucdenver.edu

15. Log in with your network username and password.
16. Select your preferred authentication method.

17. After completing your authentication method, you will see a Connecting screen.
18. You are now connected to your campus’s network through VPN.

![VPN connected](image)

**Updating your Duo profile using the self-service portal**

Duo provides a self-service registration portal that allows you to add and remove devices, as well as update your authentication preferences. Perform the following tasks to add a device or update your preferences.

1. Log into CU Secure by clicking on the access portal for your primary campus:
   a. CU Denver: [https://dc-vpn.ucdenver.edu](https://dc-vpn.ucdenver.edu)
   b. Anschutz Medical Campus: [https://amc-vpn.ucdenver.edu](https://amc-vpn.ucdenver.edu)
2. Login with your network username and password.

3. Click Add a new device or My Settings & Devices in the left-hand navigation.
4. Authenticate using your preferred method.

5. Select the type of device you are adding from the available options and click Continue. In this example, we are adding a work phone.
6. Enter the phone you would like to add and click Continue.

![Image of phone number entry interface]

**Note:** You can enter an international number by selecting a different country from the country drop-down.

7. Your new number is added.

**Duo Authentication**

![Image of Duo Authentication settings interface]

**Note:** You can set defaults for your preferences for your devices and login method.
a) Select your default device.

**Duo Authentication**

b) Select your default contact method.

**Duo Authentication**
Troubleshooting tips

VPN Access Portal

Q: Do I need to reinstall the VPN access portal client each time I connect to VPN?
No. With the exception of periodic software updates, you will not need to reinstall the client.

Q: Do we have a VPN access portal for each campus?
Yes, each campus has its own portal. These are dc-vpn.ucdenver.edu and amc-vpn.ucdenver.edu

Q: From where can I connect to VPN access portal?
You can connect from any remote location that is not on the campuses' trusted or wired networks. These include guest wireless, your home office, Starbucks, the mountains, the beach, etc.

Q: Can I connect to VPN from the campuses' wired networks?
No. You must be disconnected from the campuses' trusted networks.

Q: I can’t connect to https://dc-vpn.ucdenver.edu and https://amc-vpn.ucdenver.edu from the Guest wireless network.

a) If you are connecting on campus, ensure that you are fully disconnected from the trusted networks. Disconnect from your docking station to remove the wired connection, disconnect from CU Anschutz or CU Denver wireless, connect to CU Anschutz Guest or CU Denver Guest, and then try connecting to the appropriate client for your campus.

b) If you are connecting off-campus, try clearing your browser cache or go to a site you haven’t connected to before to ensure you are on the Guest wireless. You will see the Guest wireless “Accept” page prior to connection.

GlobalProtect Desktop Client

Q: My VPN client says GlobalProtect and is not CU branded. Is this malware?
No. GlobalProtect is the branding for our campuses’ new VPN client from software vendor PaloAlto. GlobalProtect is safe to use.

Q: Is there a GlobalProtect client for Linux users?
Yes. Download the Linux client from https://www1.ucdenver.edu/docs/default-source/offices-oit-documents/vpn-client-software/global-protect-4-1-7-0-7-signed.apk?sfvrsn=851496b8_2&download=true.

Important! The Linux process is different from Windows and Mac. Linux users must contact the OIT Service Desk for a passcode with which to connect. Linux documentation will be posted on OIT’s Service Impacting Projects tab for CU Secure at https://www1.ucdenver.edu/offices/office-of-information-technology/news/article/office-of-information-technology/cu-secure-our-campuses-multi-level-initiative-to-make-your-data-more-secure!
Q: Will the Cisco AnyConnect client go away or can I use this instead of GlobalProtect?
Yes. The Cisco AnyConnect client will be discontinued eight weeks after go-live on March 29. You must begin using the new process after March 29.

Q: Can I connect to amc-anywhere.ucdenver.edu or auraria-anywhere.ucdenver.edu with the GlobalProtect client?
No. Please use the new clients dc-vpn.ucdenver.edu and amc-vpn.ucdenver.edu.

Q: I can’t connect to VPN using my installed version of GlobalProtect.
Under Programs, right-click on Palo Alto Networks > GlobalProtect > Uninstall. Uninstall and reinstall the agent.

Duo Registration and Mobile Client

Q: Is there a mobile client for all devices?
Yes. Duo Mobile exists for Android, Apple and Windows devices.

Q: Do I have to use a mobile device to authenticate to Duo?
No. You may also register a landline phone, like your office or home phone, and Duo will call you on that device to authenticate.

Q: Can I register my work or home email to authenticate to Duo?
No. Duo requires a landline phone or mobile device (smart phone or tablet) to perform multifactor authentication.

Q: I am accessing from China and am unable to connect.
China has a regulatory restriction on VPN clients that are not approved by the Chinese government. Please check with your provider to determine if their firewall allows VPN.
General Connection Troubleshooting Tips

Q: I am connected to the guest wireless network, but can’t connect to https://dc-vpn.ucdenver.edu and https://amc-vpn.ucdenver.edu.

   a) Verify that your browser brought up the guest wireless acceptance page and that you have clicked Accept.
   b) Try clearing your browser cache to clear out past connections.

Q: I am accessing from off campus and am unable to connect to VPN.
   a) Check that you are connected to a wireless network or hotspot.
   b) Verify that the location from which you are connecting allows access to VPN clients.

Q: Does clicking on the “remember me for 12 hours” check box on the Duo window work?
   No. Clicking on “remember me for 12 hours” does not work due to limitations in system.

Q: Will the multifactor authentication I use to access my personal information via the CU Resources tab in UCD Access change to the new process?
   Not at this time. Please continue to authenticate within UCD Access using the current process. In the future, OIT will implement the current process on our portal access and at that time, the current process may change for accessing your personal information.