

# How to install and connect to Global VPN on a PC

(This is a 2 phase process)

## PHASE 1:

1. Depending your PC you can have a 32-bit or a 64-bit operating system. Most systems are 64-bit. Click the link below for the downloadable link then scroll down to select "Install VPN for Windows 64 bit"

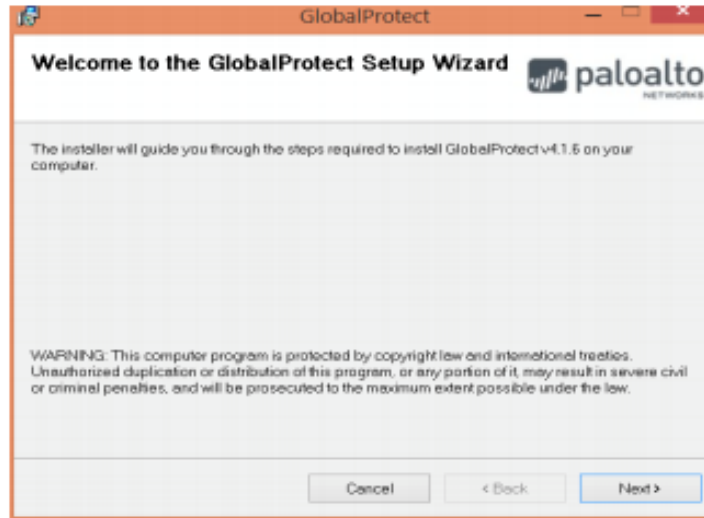
<https://www1.ucdenver.edu/offices/office-of-information-technology/software/how-do-i-use/vpn-and-remote-access>

Download and install the new VPN Palo Alto Global Protect based on the device that you want to use:

GlobalProtect VPN Download Options	GlobalProtect Installation Instructions
<a href="#">Install VPN for Windows 32 bit</a> Not sure which version to download after reviewing the How-to Guide? <a href="#">Contact the service desk.</a>	<a href="#">How-to for Windows</a>  <a href="#">View a short PC instructional video</a>
<a href="#">Install VPN for Windows 64 bit</a> Not sure which version to download after reviewing the How-to Guide? <a href="#">Contact the service desk.</a>	<a href="#">How-to for Windows</a>  <a href="#">View a short PC instructional video</a>
<a href="#">Install VPN for Mac OS X 10.11 or later</a>	<a href="#">How-to for Mac</a>  <a href="#">View a short Mac instructional video</a>
Download and install the VPN client for your mobile device by going to the Apple App Store or Google Play.	
<a href="#">Install VPN for Linux</a>	<a href="#">How-to for Linux</a>

---

2. Look for the agent download file in your browser's download window or your *Downloads* folder. Double-click the .MSI file to install.
3. Click Next in the GlobalProtect Setup Wizard screen.

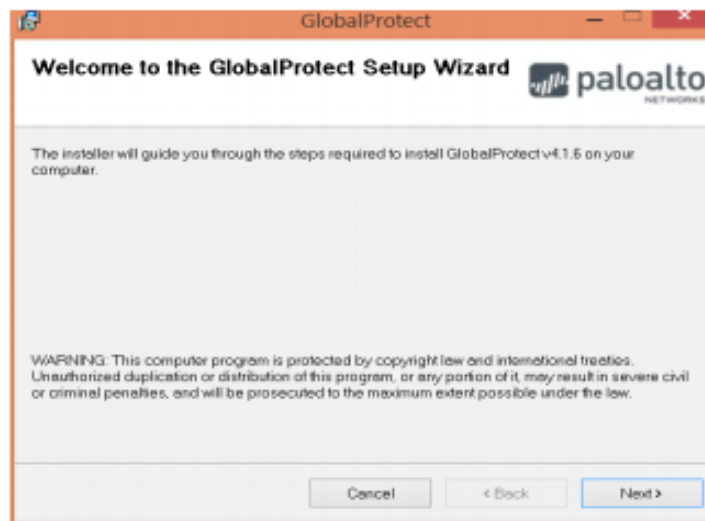


1. There are two steps for using the university's new VPN:
  - a. Register and install [Duo Security](#).
  - b. Download and install [GlobalProtect VPN](#).

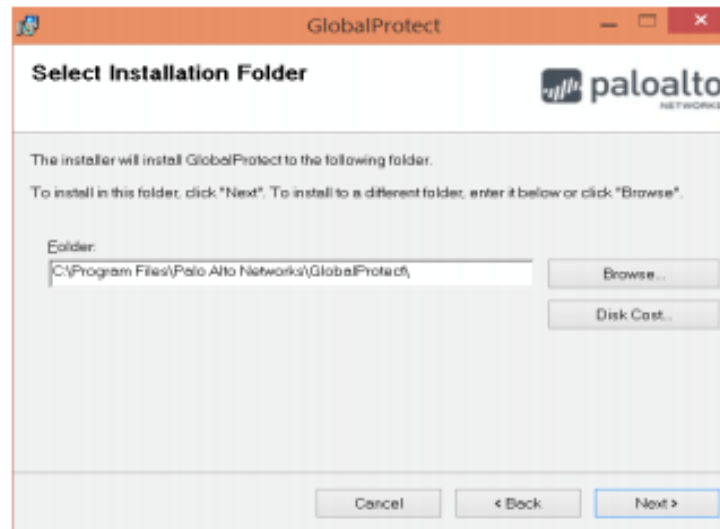


**Important!** Be sure to select the appropriate download for your device – either Windows 32 bit GlobalProtect agent or Windows 64 bit GlobalProtect agent. Check your Windows operating system to determine which version is downloaded. For Windows 7 go to: Start > right-click Computer > Properties > under System; for Windows 10: Start > type This PC > right-click This PC > Properties > under System. For additional assistance, refer to the [Microsoft Support Site](#) or contact the OIT Service Desk at [oit-servicedesk@ucdenver.edu](mailto:oit-servicedesk@ucdenver.edu).

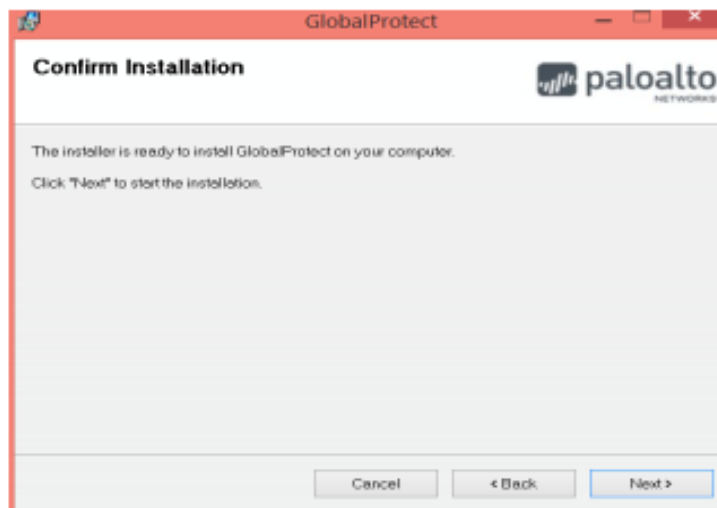
2. Look for the agent download file in your browser's download window or your *Downloads* folder. Double-click the .MSI file to install.
3. Click Next in the GlobalProtect Setup Wizard screen.



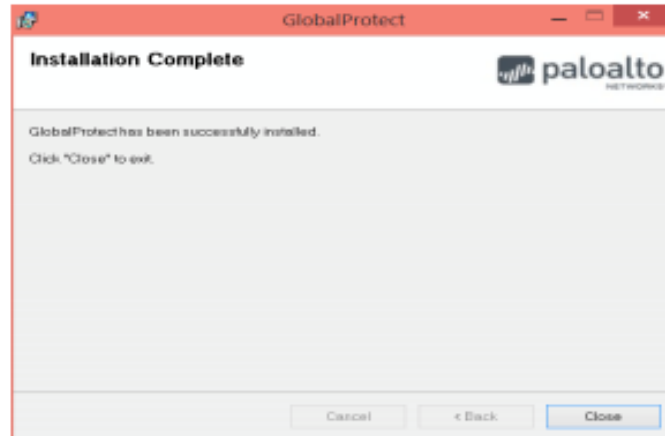
4. Select where you would like the application to be installed. We recommend keeping the default folder location. Click Yes when the pop-up window displays the message asking if you want to install the software.



5. Click Next to confirm the installation.



6. Close the installer following successful installation.



- You have now completed the installation process for the university's multi-factor VPN process.

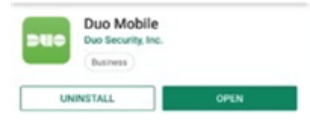
*Next you must install and register for the Duo app because Global VPN requires duo authentication to log in...*

## PHASE 2:

### How to install and register for Duo

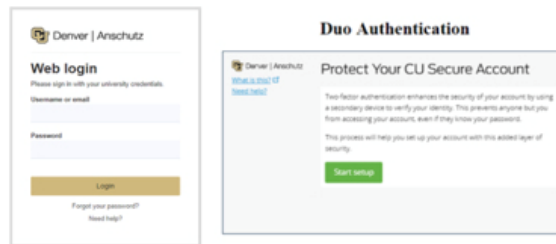
1. Before registering with Duo, we **highly recommend** installing the Duo Mobile app on your preferred mobile device, e.g., your smartphone. The app is available from the Apple App Store, Google Play or the Microsoft Store. **Important!** There are multiple Duo apps. Please install the Duo Mobile app with the green logo.

During app installation, click "Allow access to camera" so that you can scan the barcode that will be generated during Duo registration.



2. The next step is to register with Duo. From your laptop or desktop computer go to: <https://passport.ucdenver.edu/CUSecure.php>.

Login with your CU network Username (type in your "Username" not your email address) and Password. The Duo Authentication "Start setup" message will appear.



3. Select your preferred device type to receive the authentication request from the Duo application and click Continue.



4. If you've selected a mobile phone, input the phone number and select the type of phone.



5. A barcode should appear on your computer screen. Using the mobile app that you installed in Step 1, scan the barcode with your phone to activate the Duo authentication service. (If you're using a Landline for authentication, you will skip this step.)



6. On the next screen, next to "When I log in", make sure "Ask me to choose an authentication method" is selected in the dropdown box.



7. Next, select your preferred authentication method and save your preferences. You will have the option to choose: a.) **Duo Push**, b.) **Call Me**, or c.) **Passcode**.

**Instructions for your preferred authentication method are provided below:**

a. To choose **Duo Push** (recommended method):



b. To choose **Call Me**:

The first screenshot shows the 'Duo Authentication' screen with the 'Call Me' option selected and highlighted by a yellow box. An arrow points to a text box that says 'Duo dials the phone you registered in Step 5.' The second screenshot shows the same screen with a blue bar at the bottom that says 'Answer: Press any key on your phone to log in.' An arrow points to a text box that says 'Press any key on your phone to authenticate.'

c. To choose **Passcode**:

The first screenshot shows the 'Duo Authentication' screen with the 'Passcode' option selected and highlighted by a yellow box. An arrow points to a text box that says 'Click Enter a Passcode to authenticate. A code is texted to your phone. (Be sure you clicked "Allow notifications" during the installation process.)' The second screenshot shows the same screen with a text input field containing '118888' and a 'Log In' button highlighted by a yellow box. An arrow points to a text box that says 'You will have 5 minutes to enter the passcode texted to your phone and then click Log In.'

- You have now completed the registration process for setting up multi-factor authentication with Duo!
- Thank you for your support in maintaining the university's secure environment.