GlobalProtect VPN Installation and User Guide for Linux

1. There are two steps for using the university's new VPN:
   a. Register and install Duo Security. This step must be completed first!
   b. Download and install GlobalProtect VPN.

Important! The Palo Alto GlobalProtect app for Linux ***only*** supports the following: CentOS 7, Red Hat Enterprise Linux (RHEL) 7 and Ubuntu 14.04 and later releases.

2. Install the GlobalProtect client for Linux available on the CU Secure / Multi-factor authentication site VPN download table.

   - Additional download and installation reference material from Palo Alto is available here.

3. Once downloaded, unzip the package. The basic command information to use GlobalProtect VPN for Linux is:

   - `$ globalprotect connect --portal amc-vpn.ucdenver.edu`

     or

   - `$ globalprotect connect --portal dc-vpn.ucdenver.edu`

4. Enter the VPN portal **amc-vpn.ucdenver.edu**

5. Log in with your network Username (type in your **Username** – not your email address) and Password, this will use your default DUO authentication method such as DUO push.

6. Alternatively, you may also enter your password and the authentication method you want to use, separated with a comma. It will look something like this:

   password,*authentication_method*

In place of *authentication_method*:

Type...	To...
password,***passcode***	Log in using a passcode, either generated with Duo Mobile, sent via SMS, generated by your hardware token, or provided by an administrator. Examples: "mypass123,123456" or "mypass123,1456789"
password,**push**	Push a login request to your phone (if you have Duo Mobile installed and activated on your iOS, Android, or Windows Phone device). Just review the request and tap "Approve" to log in.
password,**phone**	Authenticate via phone callback.
password,**sms**	Get a new batch of SMS passcodes. Your login attempt will fail — log in again with one of your new passcodes.

You can also add a number to the end of these factor names if you have more than one device registered. For example, **push2** will send a login request to your second phone, **phone3** will call your third phone, etc.

7. You will see the following messages displayed:
    a. Retrieving configuration...
    b. Discovering network...

8. After completing this process, you will see a message from GlobalProtect that you are securely connected.

Please note: If the Global Protect application displays a certificate error, you must acknowledge before you authenticate. When you next connect, you will not be prompted with the certificate error message.