Published on *University of Colorado* (https://www.cu.edu)

Get into the habit of always connecting to CU’s VPN [1]

May 19, 2025 by ES and UIS Communications [2]

Accessing the internet on an unsecured Wi-Fi network means your private information and device data could be publicly exposed. That’s why a virtual private network (VPN) is essential for maintaining online security and privacy.

When working from home, you can securely connect your device to CU’s network via the VPN. It will encrypt your internet traffic and mask your device’s personal details, including location.

In addition, the VPN is required for accessing internal resources and CU applications, like shared drives and CU-Data.

It is **highly recommended** for all CU System administration staff to connect to the VPN at the beginning of every workday. This protects CU’s information, documents and data from hacks, data leaks, tracking and unauthorized usage.

Configuring your VPN settings

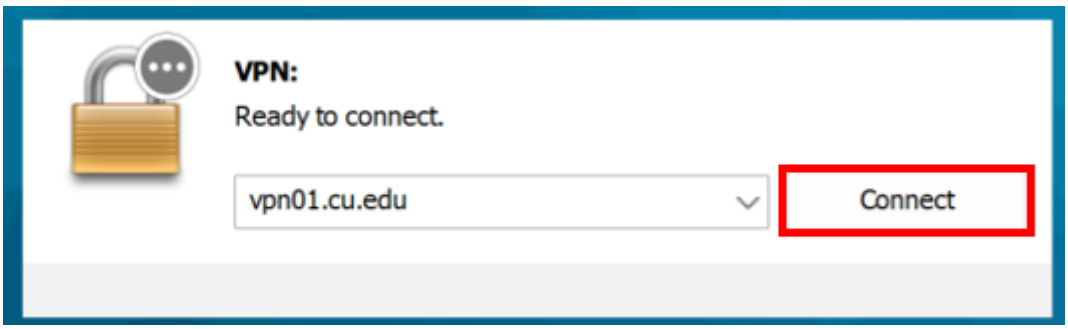
CU’s VPN, Cisco AnyConnect, has three options for connection: **1-System-SplitTunnel-Idp**, **2-System-FullTunnel-Idp** and **3-System-Idp**. Choose the VPN group that best fits what you are accessing.

- **1-System-SplitTunnel-Idp (recommended):** Recommended for most staff. Splits your traffic through the VPN and the open network, depending on the application you are using and its security requirements. Web browsers and device peripherals (e.g. wireless printers) work best on the split tunnel.
- **2-System-FullTunnel-Idp:** For staff using applications or accessing data that requires maximum security, such as student and financial information.
- **3-System-Idp:** For non-employees who need to use the VPN.

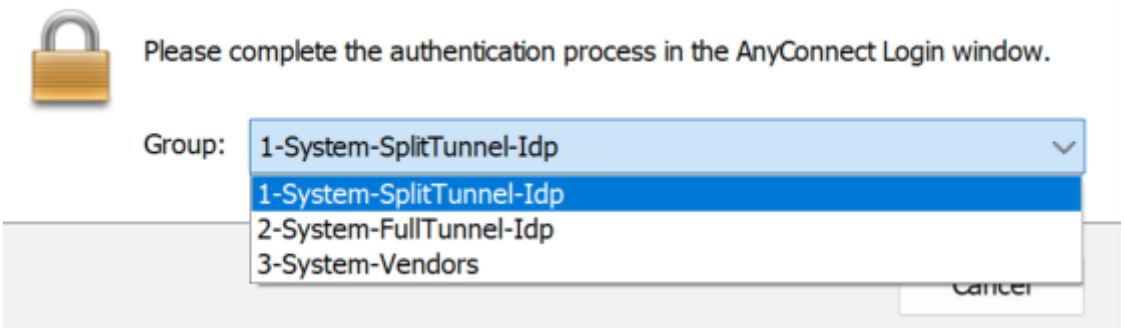
Connecting to the VPN

1. Open **Cisco AnyConnect**.

2. Click **Connect**.

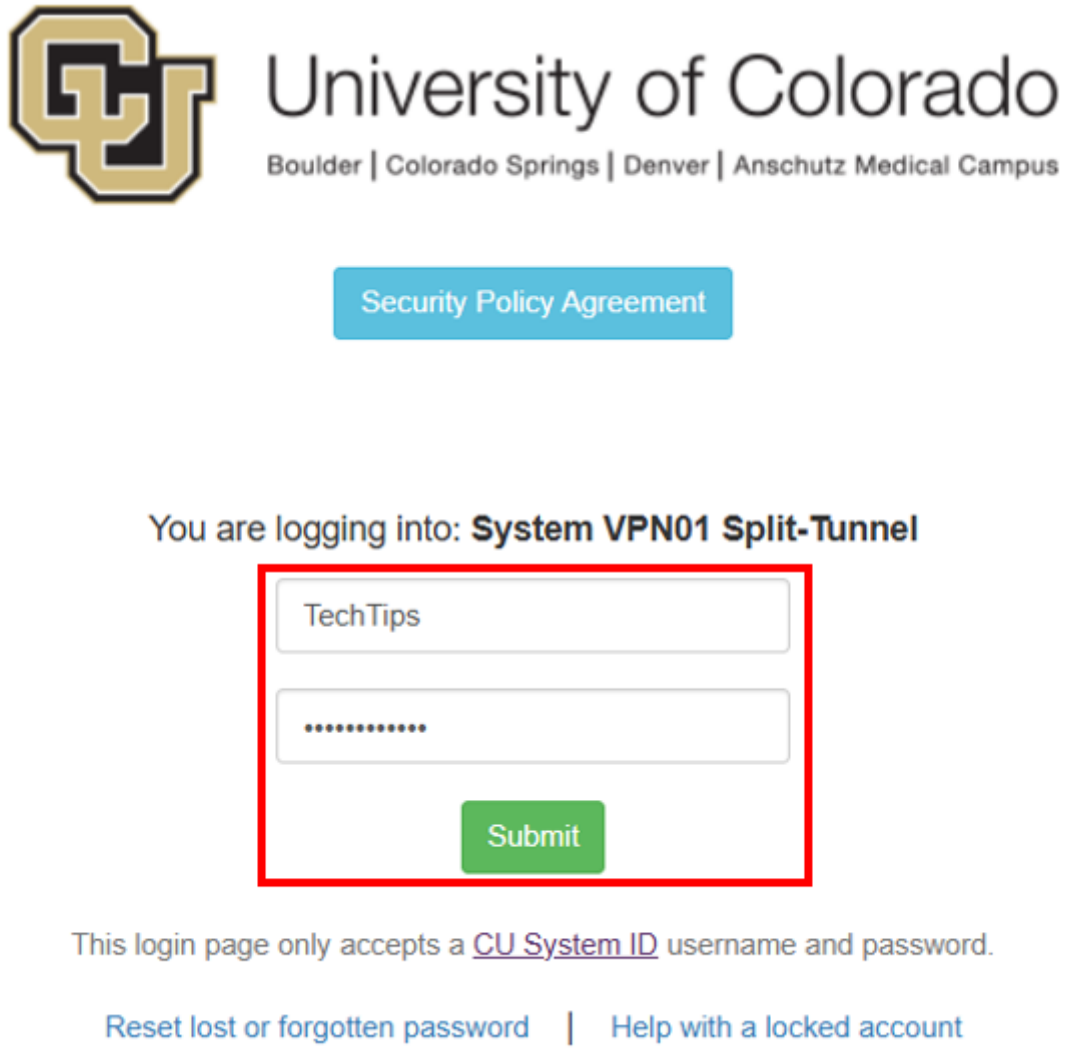


3. The VPN login and group selection windows will open. Select the appropriate group from the group selection window.

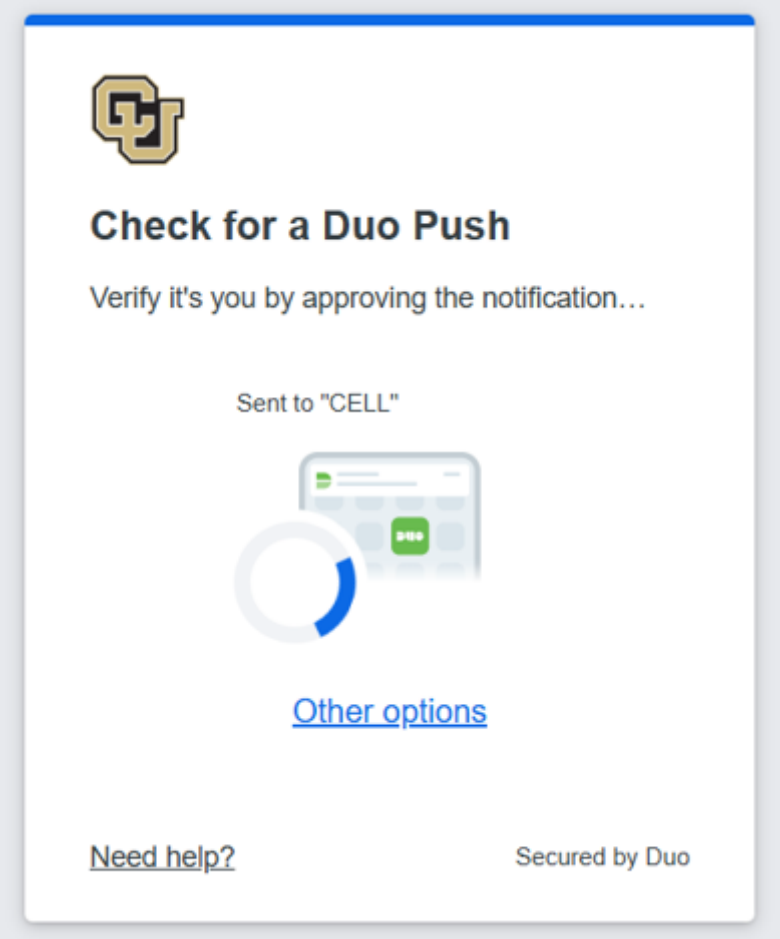


TIP: The group selection window is often hidden behind the login window. Minimize the login window to access group selection.

4. Sign in your CU employee login.



5. Complete the DUO MFA security challenge.



6. You are now connected to CU's VPN.

Curious about how Duo multifactor authentication (MFA) keeps you and CU safe? See our It takes two: Using multifactor authentication to stay safe online [3]tip for more information

vpn [4]

Display Title:
Get into the habit of always connecting to CU’s VPN
Send email when Published:
No

Source URL:https://www.cu.edu/blog/tech-tips/get-habit-always-connecting-cu%E2%80%99s-vpn

Links
[1] https://www.cu.edu/blog/tech-tips/get-habit-always-connecting-cu%E2%80%99s-vpn
[2] https://www.cu.edu/blog/tech-tips/author/166688 [3] https://www.cu.edu/blog/tech-tips/it-takes-two-using-multifactor-authentication-stay-safe-online [4] https://www.cu.edu/blog/tech-tips/tag/vpn