

The Ursinus VPN (Virtual Private Network)

What is “VPN”?

To use and access certain software or resources on the Ursinus College network from off campus, you will need to connect to the Ursinus VPN. Connecting through the VPN provides a connection that mirrors the connection you would have as if you were on campus.

Examples of Ursinus resources requiring connection to the VPN from off campus:

- The Ursinus shared drive – the “S” drive.
- Colleague Production UI

Example of Ursinus resources that DO NOT require connecting to the Ursinus VPN from off campus:


- Ursinus email – Microsoft Outlook
- Canvas
- Microsoft Office 365
- Colleague Self-Service

The VPN can only be used on Windows and Macintosh computers. The VPN cannot be used on mobile devices such as phones, iPads and Android tablets.



Connecting to the Ursinus VPN

Initial login and installation

1. Go to <https://vpn.ursinus.edu>. You will see the following webpage login and then multi-factor authentication (MFA) prompt. Enter your Ursinus username and password and approve your MFA.

Connecting to  paloalto

Sign-in with your Ursinus College account to access Palo Alto Networks - GlobalProtect

**Ursinus College**

Sign In

 Remember me
Sign In
[Need help signing in?](#)

2. If you have not set up your multi-factor authentication, you will need to follow the steps as listed in the Multi-Factor Authentication instructions which assists in setting up a second method of credential authentication using one of the choices listed here:

Choose one of the options that include:

- a. **Okta Verify**, which you can use by installing the Okta Verify app on your mobile device. With Okta Verify, you have the option to have an authorization ‘pushed’ to your device or you can choose to enter or scan a code within the app. Follow the instructions to choose your mobile device type (e.g. Apple, Android), open the Okta Verify app on your mobile device and walk through the choices and setup steps. If you choose push verification, you will receive a notification on your device that you will need to approve. If you choose to receive a code, open the Okta Verify app on your mobile device, and enter the code you received or scan the barcode provided on your computer.
- b. **SMS Authentication or Text Message Code**. Follow the instructions by providing your cell phone number and clicking Send Code. You will receive a text message. Enter that code when prompted and select Verify.
- c. **Yubikey** (For special cases only. Send request to Tech Support).

3. After successfully logging in, you can proceed to Downloading and installing the VPN software. Click on one of the links provided to download the VPN software needed for your system – Windows 32 bit, Windows 64 bit (most windows systems), or Mac. After downloading, start the installer and follow prompts to click ‘next’ and finish the install.



GlobalProtect Portal

[Download Windows 32 bit GlobalProtect agent](#)

[Download Windows 64 bit GlobalProtect agent](#)

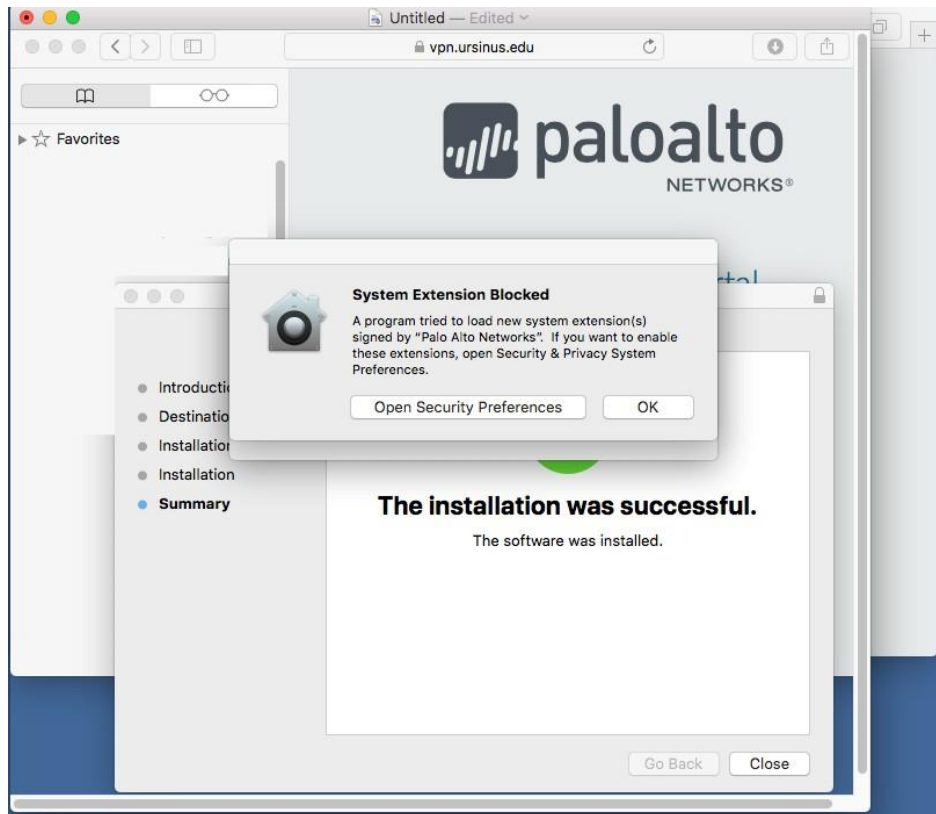
[Download Mac 32/64 bit GlobalProtect agent](#)

Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.

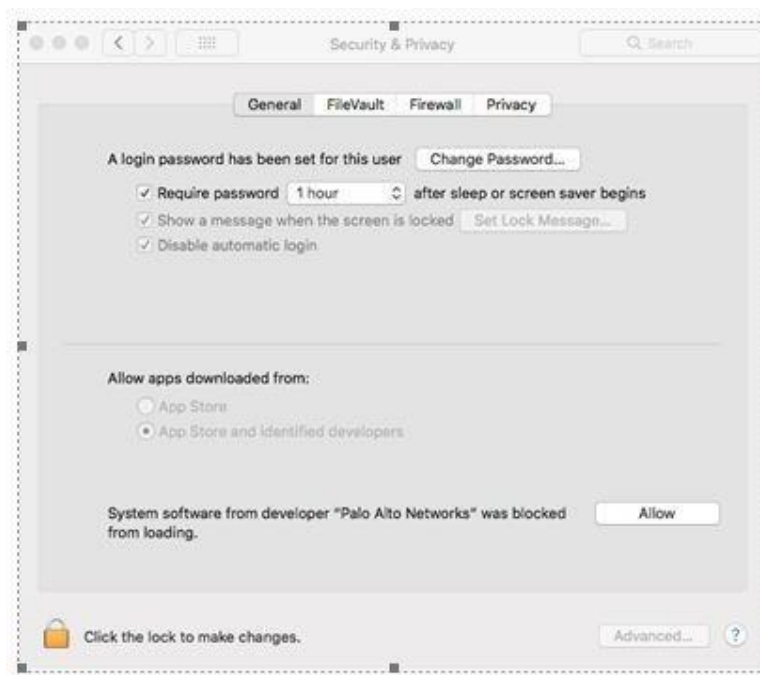
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.

Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

For Macintosh, when installing the GlobalProtect software, you may receive a pop-up window titled “System Extension Blocked”. Within this box, click “Open Security Preferences”:

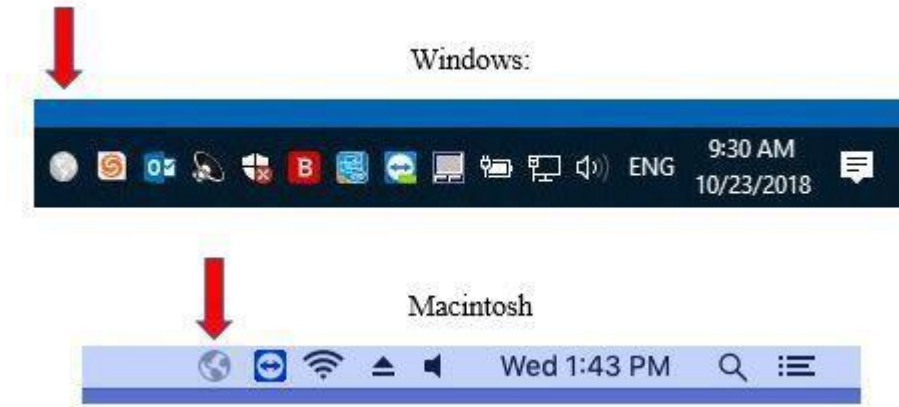


After clicking “Open Security Preferences”, another window will pop-up. Click the “Allow” button and follow through to install.

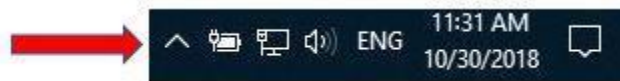


After install, the GlobalProtect VPN software icon will be located in the lower right-hand side of the Windows taskbar, and the upper right-hand side of the Mac menu bar.

The icon is a round globe (grayed out when not connected):



To save space on the Windows task bar, some task bars are reduced, but can be expanded by clicking the 'up triangle' as shown here:



After clicking the arrow, the hidden icons will appear. This may be where the VPN/GlobalProtect icon may be located – click the Globe and continue with directions below to finish initial setup or for connecting in the future:




Connecting to the VPN after it is installed


1. Clicking the 'globe' icon opens the following box. Enter **vpn.ursinus.edu** in the box and click connect. The 'vpn.ursinus.edu' should be saved for future use when connecting to the vpn.



2. After entering the portal address in directions above and clicking 'Connect', the connection is started.

After connection, enter your Ursinus username and password and click 'sign in'.

Connecting to 

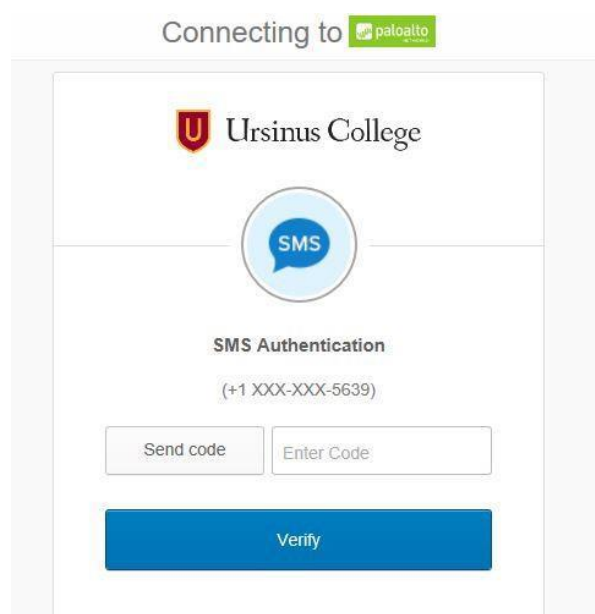
 Ursinus College

Sign In

Remember me

[Need help signing in?](#)

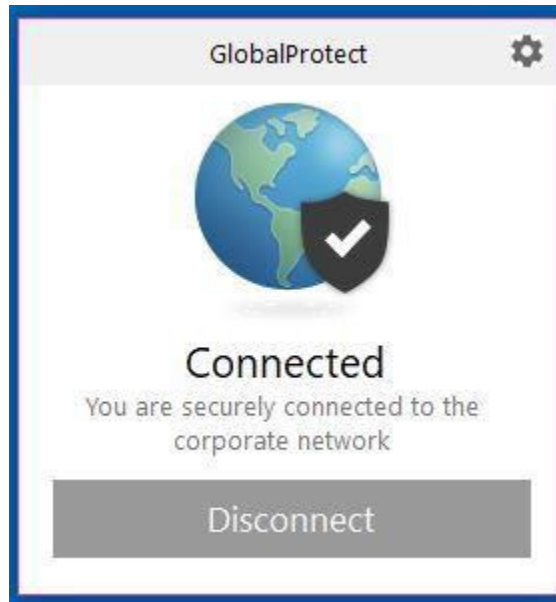
3. You will then be prompted for your multi-factor authentication. Depending on the method of MFA you chose, you will need to enter a code or approve the connection in the Okta Verify app. The SMS/Text method of using MFA is shown below. If using the Okta verify app, you will need to go to the app on your device and accept the prompt. If you are using the SMS/Text method, you will see the below pic. You must click the 'Send code' button and a code will be sent to your phone in a text message. You must then enter that code in the 'Enter code' box, then click 'Verify'. If entered correctly you should be fully connected to the VPN:



4. After connecting, you will see the globe icon change to a blue color with a check mark on the icon.



5. Clicking the icon will display the following. Once connected you will have the same access as if you were on-campus.



6. To Disconnect, click the globe icon and click the Disconnect button in the GlobalProtect window.

If you have any questions or issues, please email techsupport@ursinus.edu or call us at 610-409-3789.