



Registering 2-Factor Authentication (first time login off campus)

2-Factor Authentication is required for off campus access to the OneLogin Application Portal, which includes Google Workspace, Canvas, Zoom and many other campus applications.

1. Visit login.muhlenberg.edu
2. Login with your Muhlenberg network credentials
3. The following Authentication Factors are available for 2-factor authentication to secure your account. Note: **OneLogin Mobile App (OneLogin Protect)** is the recommended method.
 - a. OneLogin Mobile App (search for OneLogin Protect in your app store) is the recommended method for 2-factor authentication at home and abroad. Once registered THAT instance of the app must remain on your device. Do not delete it.
 - b. OneLogin Mobile SMS - If you have a mobile device that does not support a one time password app, SMS text messaging can be used as a backup authentication method. If you do not have a phone number preset in your OneLogin profile, you will need to add one. If the number in your profile needs to be updated, you must contact the OIT Help Desk at 484-664-3566.
 - c. Google Authenticator
One Time Password (OTP) app for 2-factor authentication. Once registered THAT instance of the app must remain on your device. Do not delete it.
 - d. Yubikeys (hardware token) - a physical device that will generate the second factor. A Yubikey is a device that you have to plug into your computer. Yubikeys are available online for purchase - <https://www.yubico.com/products/yubikey-hardware/>.
4. Follow the OneLogin prompts to complete the process.

You may be prompted to change your password when logging in if the existing password has expired. We recommend changing your original password as soon as possible.

Need help registering your 2-factor authentication? Contact the OIT Help Desk at [helpdesk@muhlenberg.edu/484-664-3566](mailto:helpdesk@muhlenberg.edu) or check out online documentation and video tutorials - <https://www.muhlenberg.edu/offices/oit/2factor.html>.