

## Multi-Factor Authentication

**What is multi-factor authentication?** Multi-Factor Authentication (MFA) is a login or credential verification practice that adds an extra layer of protection on top of your user name and password. With MFA, when you sign in, you will be prompted for your user name and password, the first factor, and then another prompt for authentication communicated through your MFA device, the second factor. The MFA device most often is a personal cell phone or email.

**When will I be prompted to use it?** When you sign in to VPN from off-campus, when you connect to 365 from certain off-campus locations, and periodically when you sign in to Colleague.

### How do I set up multi-factor authentication?

- Go to [connect.ursinus.edu](https://connect.ursinus.edu) and sign in using your Ursinus username and password.
- Select your name in the top navigation menu and choose Settings.
- Under Extra Verification, choose the verification you wish to set up and click Setup. Options include:
  - a. Okta Verify, which you can use by installing the Okta Verify app on your mobile device. You will have the option to have an authorization 'pushed' to your device or you can choose to receive a code. 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.
  - b. Security Key or Biometric Authenticator. (For special cases only. Send request to Tech Support).
  - c. SMS Authentication - 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.

✓ Extra Verification	
Extra verification increases your account security when signing in to Okta and other applications you use	
Okta Verify	Set up
Security Key or Biometric Authenticator	Set up
SMS Authentication	Set up

- If desired, you can set up additional verification methods (e.g. you want the option of using Okta Verify or receiving a text message).

**What do I need to do when multi-factor authentication is triggered?**

- If you are using Okta Verify, a push notification will be sent to the mobile app that you will need to verify.
- If you are using Text Message Code, you will receive a text message on your mobile device and will need to enter that code when prompted.

**How do I test or verify my settings?**

- After completing MFA setup, logout of Okta
- Log back into Okta ([connect.ursinus.edu](https://connect.ursinus.edu)) using your Ursinus username and password.
- Select your name in the top navigation menu, choose Settings and click the Edit Profile button.
- You will have to verify your password then be prompted for MFA verification
- Successful MFA verification will show your Okta profile

If you have any questions or issues, please email [techsupport@ursinus.edu](mailto:techsupport@ursinus.edu) or call us at 610-409-3789.