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 and periodically when you sign in to Colleague.

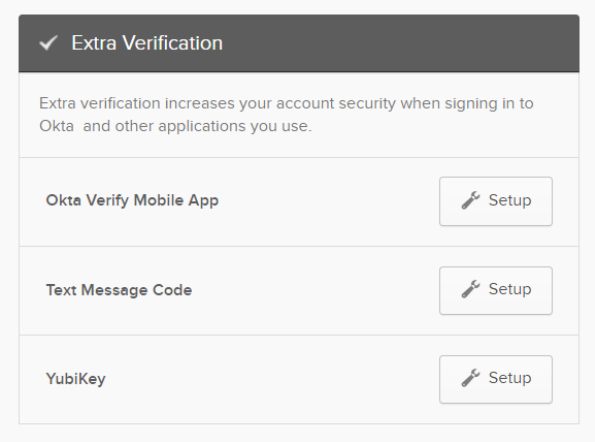
How do I set up multi-factor authentication? You should be prompted to set it up the first time you sign in to VPN or Colleague. Otherwise, follow the instructions below:

- Go to https://ursinus.okta.com 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 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. **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).



- Repeat these steps if you want to set up a second verification process (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 and you will need to enter the code showing in the app when prompted or authorize the prompt.
- 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.

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