How to log into O365, after MFA Factors have been set up

Note: these instructions are for users who have already added MFA to Office 365 and completed their first-time MFA factor setup.

Step 1 – When you log into Office 365 (includes Email, OneDrive, and SharePoint) – using https://portal.office.com/ for example – you may be prompted to “Pick an account” or enter your University email address to sign in. Click Next.

Step 2 – You will be prompted to enter your UVID and password (first authentication factor).
Step 3 – If you are not connected to the University network, an “Approve sign in request” screen may appear (second authentication factor).

Note: The example below shows the prompt for a user who has selected the mobile push notification delivery method. This prompt will vary depending on the delivery method you have configured (e.g. push notification from app, code from app, code from text message, phone call).

![Approve sign in request](image)

Note the following when logging into Office 365:

- During authentication, please be sure to complete the entire process in a timely manner (i.e. within 15 minutes).
- Whether you need to complete both verification steps every time you log in depends on your location, your settings, and a variety of other factors.
  - If your device is connected to the University network, you will not be prompted for MFA.
  - If your device is not connected to the University network, you may be prompted for MFA.
    - On the “Approve sign in request” screen, there is a box you can check so that MFA only prompts you for the second factor or verification every 60 days.
      - This check box needs to be selected for each different browser and computer/device you log in with if you want to use the 60-day grace period.
      - The 60-day check box should only be selected if you are the sole user of the current device.