

Multi-Factor Authentication - Steps for Using MFA

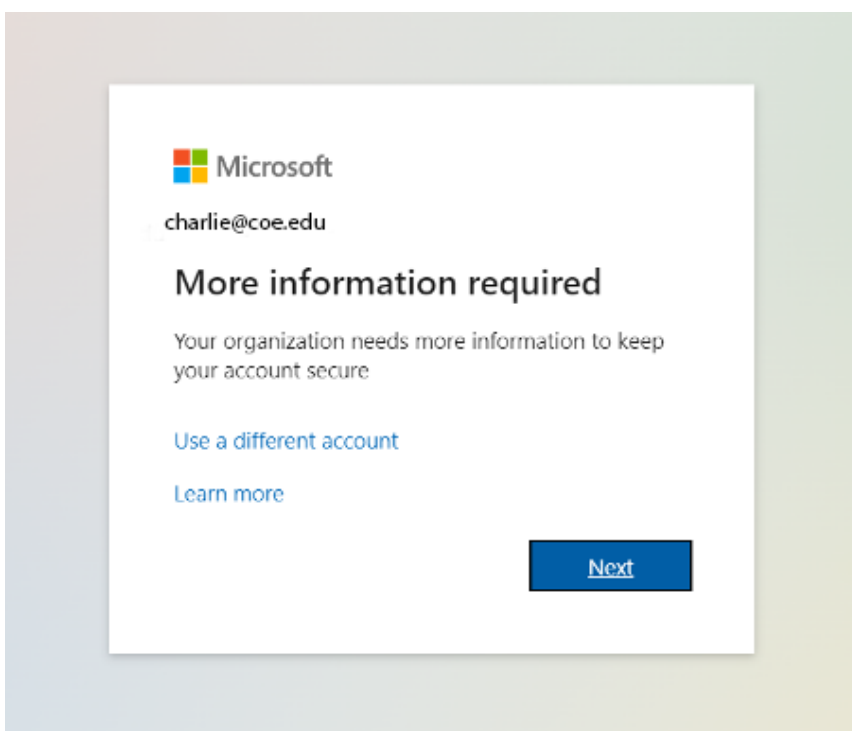
Last Reviewed July 2025

Please follow the below steps for setting up MFA and utilizing the Azure platform.

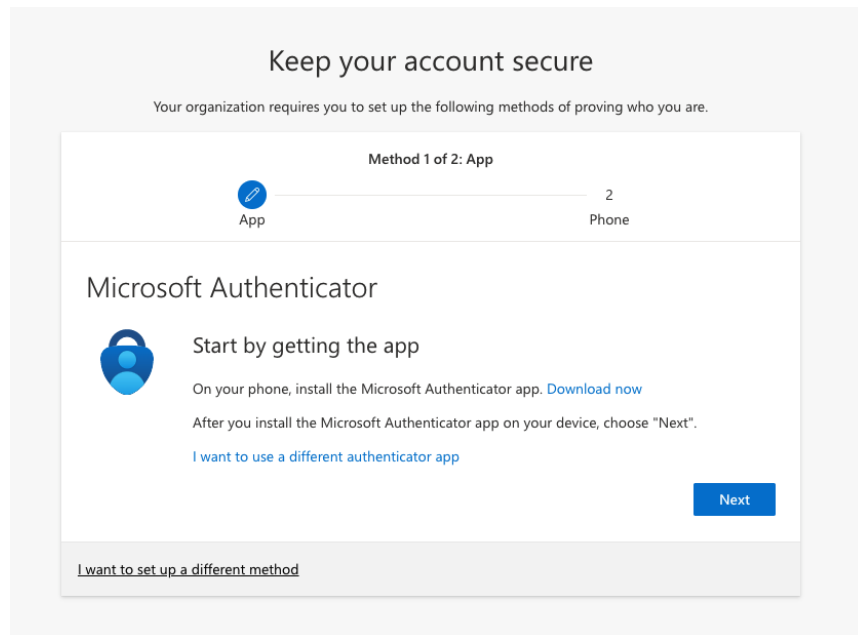
For the best results, please follow this process on a computer. If possible, we encourage you to print these directions and follow along or view the directions next to your web browser on your computer. Please follow the steps in this document closely for the most seamless experience and the best results.

You will need a secondary device (such as a mobile phone) to complete the process and need to be connected to the internet or a data plan. If you do not have a secondary device to use for authentication, please contact the IT Office for assistance.

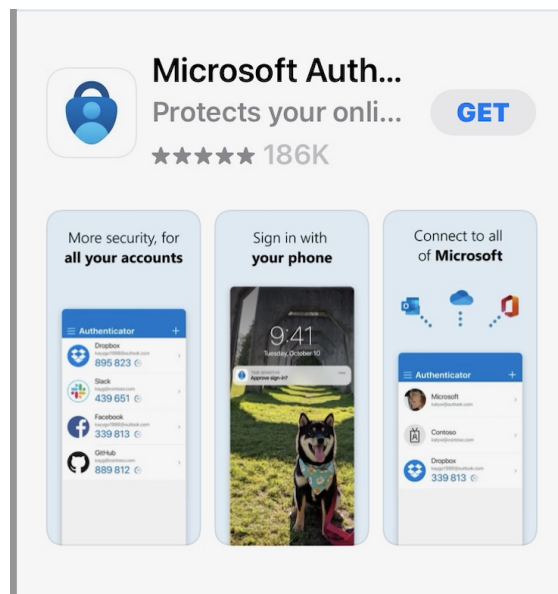
1. To begin, open a web browser and visit apps.coe.edu on your computer.
2. Log in with your username (Coe email) and network password. (If your Coe email address is already on the login screen [when you click the portal link](#) (see below), simply click "Next").



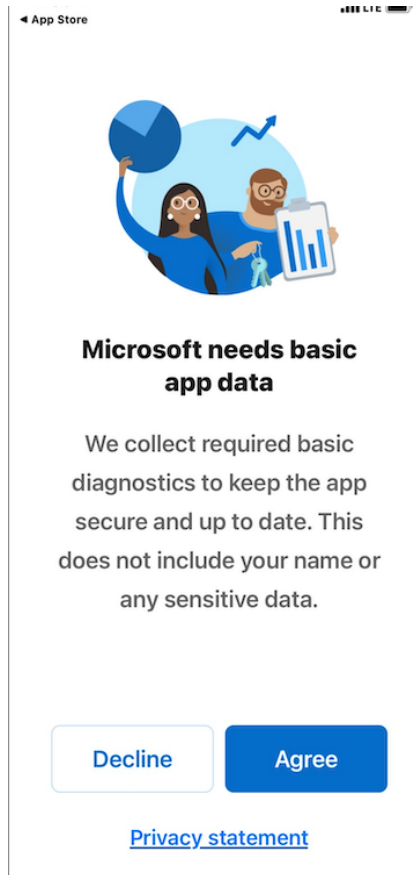
3. You will see the below screen and be prompted to download the [Microsoft Authenticator app](#) on a secondary device (typically a mobile device such as a phone or tablet).



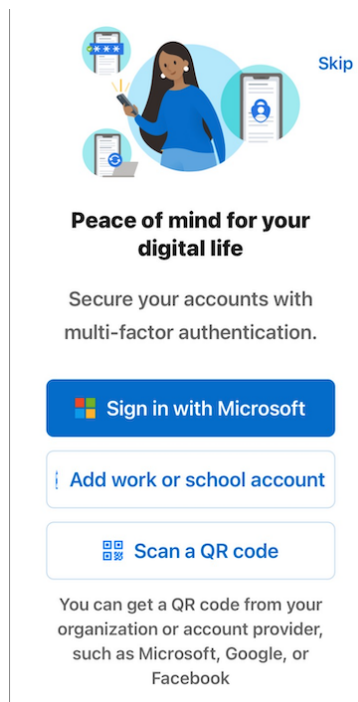
- To install the app on your phone or tablet, go to the App Store (Apple Devices) or Google Play (Android Devices) and search “Microsoft Authenticator”. You will see the below app. **There is no fee to download this app and it should look just like the icon below. (It may not be the first app to show up in your app store).**



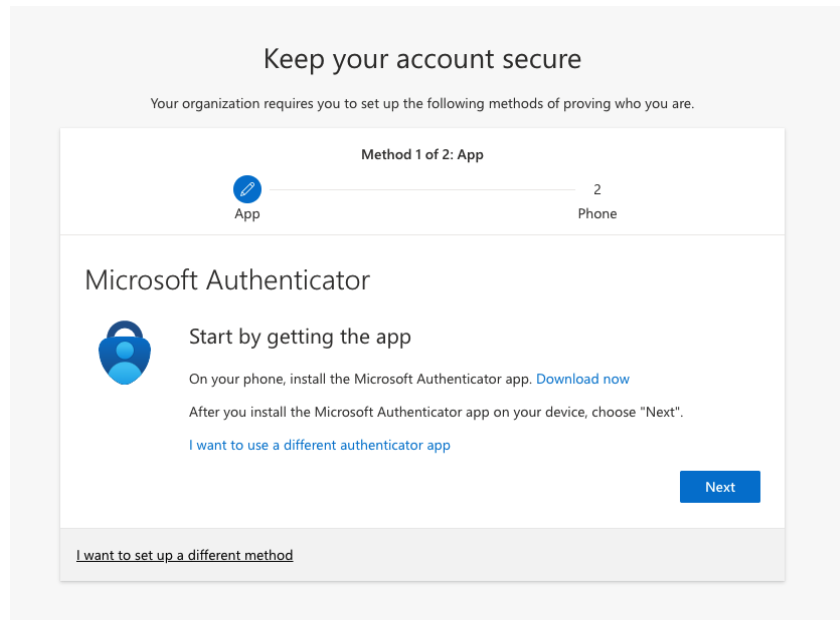
- This app will be used for authentication on your secondary device (typically a mobile device such as a phone). You will have the option to use a different authentication app but use of the Microsoft Authenticator app is recommended.
- Once you’ve downloaded the app, you will see the following screen on your secondary device. Select “Agree” (on your secondary device):



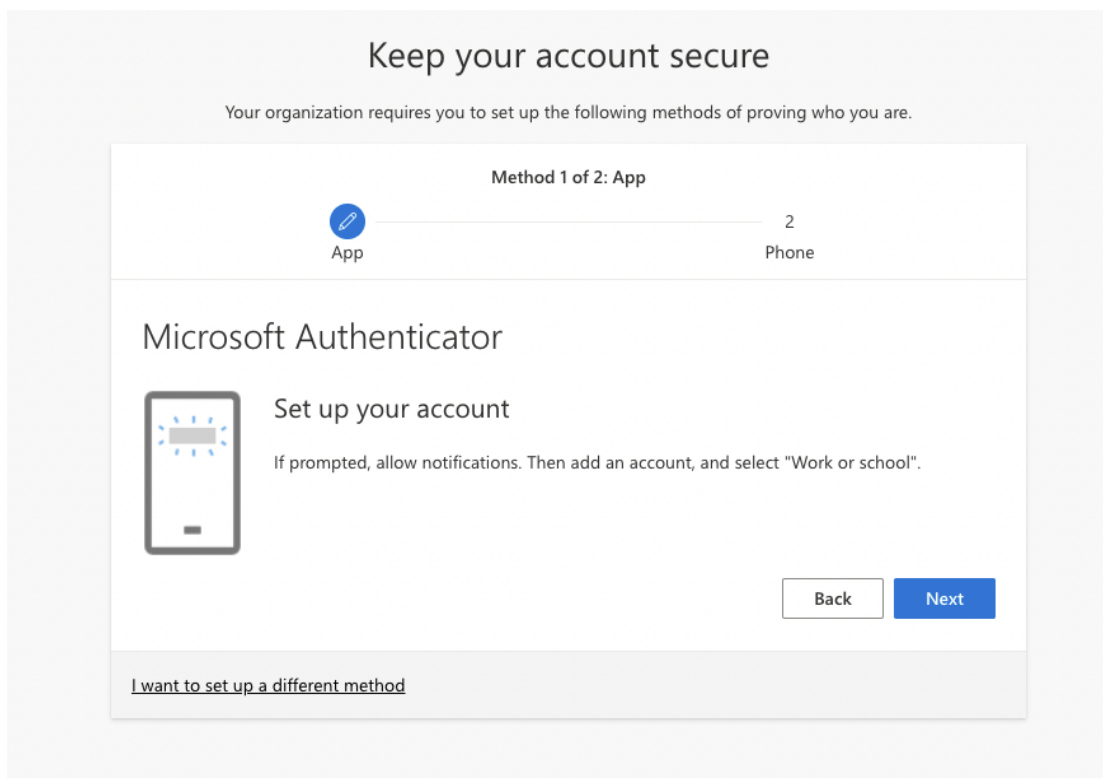
7. Once you select "Agree" on your secondary device, the following screen will appear on your secondary device. (Do not click "Skip").



8. When you see the above screen on your mobile device, go back to your computer screen and choose "Next". (See below for reference.)



9. After you select “Next” on the computer screen, you’ll see the below screen on your computer. (Do not select “Work or school” on your computer screen or on your phone). Once you see this screen, go back to your secondary/mobile device.



10. On your secondary/mobile device click “Scan QR code” (on the screen from step 7).
- Note: If your mobile device does not have the ability to Scan the QR code, click “Add work or school account” on your phone and mobile device and follow the on screen instructions. Using the QR code option will be the most seamless option.*
11. After you select “Scan QR code” on your secondary/mobile device, click “Next” on your computer screen (see screenshot in step 9). Then a QR code will appear on your computer screen:

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 1 of 2: App

App 2 Phone

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".



Can't scan image?

Back Next

[I want to set up a different method](#)

12. Scan the QR code on your computer screen, using your secondary/mobile device. (Be sure to scan the QR code through the Microsoft Authenticator mobile app, not through your phone's camera app). A notification will pop up on your secondary device asking if you would like to allow push notifications from the Microsoft Authenticator app. Select "Approve".
13. After you scan the QR code, click "Next" on your computer to move to the next screen.
14. After you scan the QR code, a pop up notification will appear on your secondary/mobile device asking if you approve of the sign-in using your Coe email address. Hit approve:

☰ Credentials



Accept a verifiable credential for more control of your identity

Some websites and organizations now offer verifiable credentials. They make account setup simpler and safer, while giving you more visibility

Approve sign-in?

coe.edu
charlie@coe.edu

Deny Approve

☰ ☒ Scan a QR code

[Learn about Verifiable Credentials](#)

15. Once you approve the pop up notification on your secondary/mobile device, this screen will appear on your computer. Select “Next” on your computer screen.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 1 of 2: App

App Phone

Microsoft Authenticator

Notification approved

Back Next

[I want to set up a different method](#)

16. On your computer screen you will be prompted to enter your cell phone number (see below). Enter your cell number to receive a text message code and hit “Next”. (Note: If you do not have a cell phone number, you can enter a land line or office number and utilize the “Call me” option. If you choose this option, follow the on-phone prompts to complete setup.)

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

App Phone

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United States (+1) Enter phone number

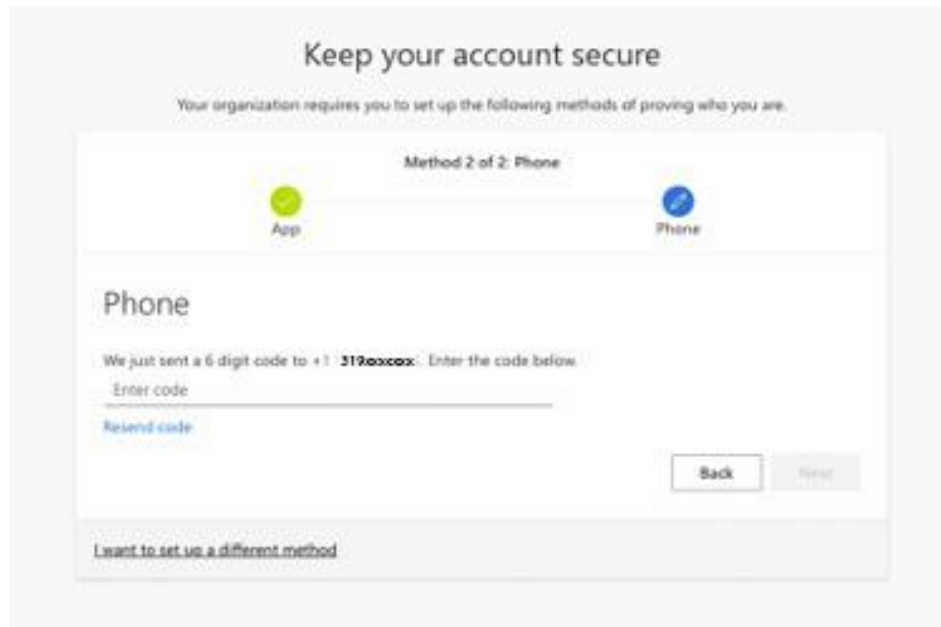
☒ Text me a code
☐ Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next

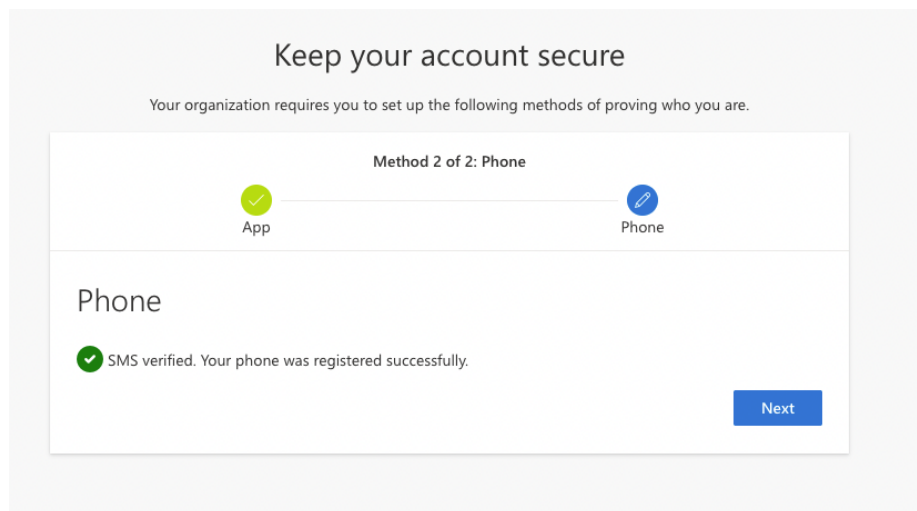
[I want to set up a different method](#)

17. The below screen will then appear on your computer. At the same time you will receive a text message on your phone containing a 6 digit code. Enter the 6 digit code into the space provided on your computer screen (see below):

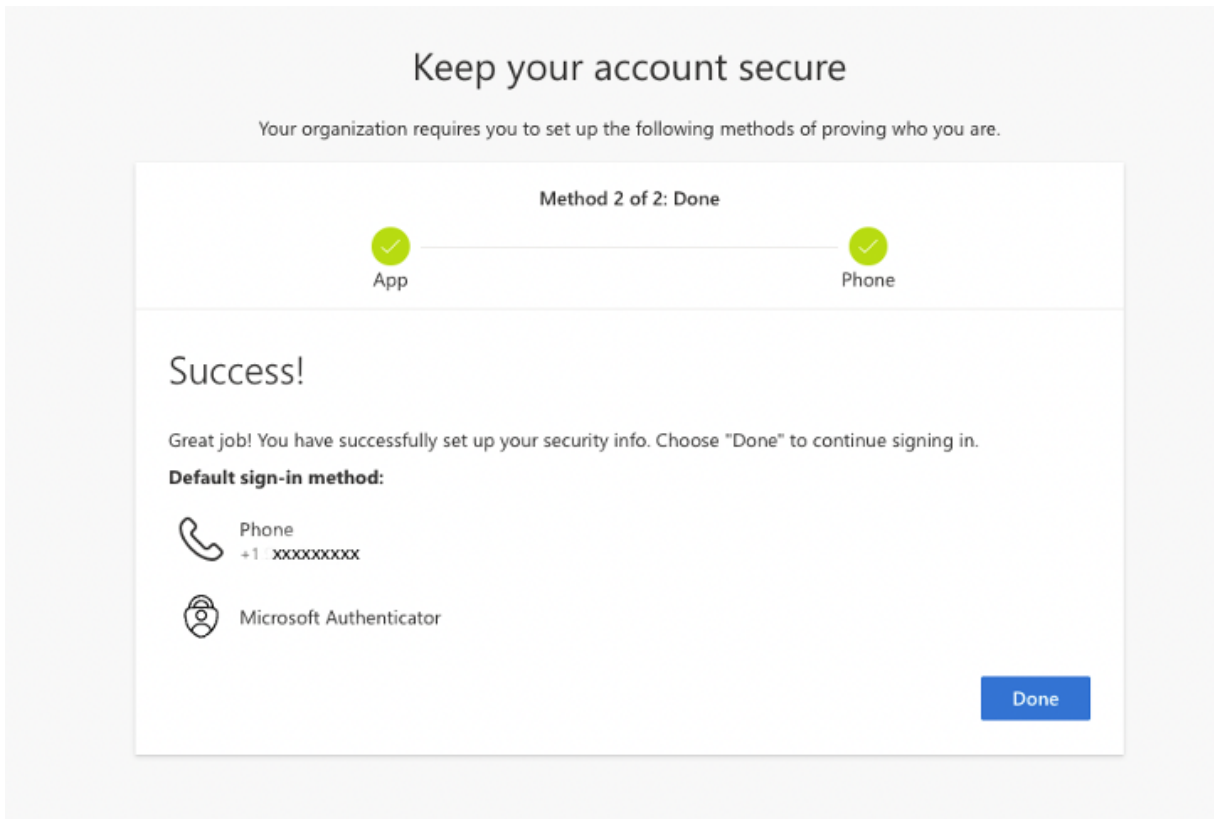


18. Once you've entered the code in the "Enter code" box, hit "Next".

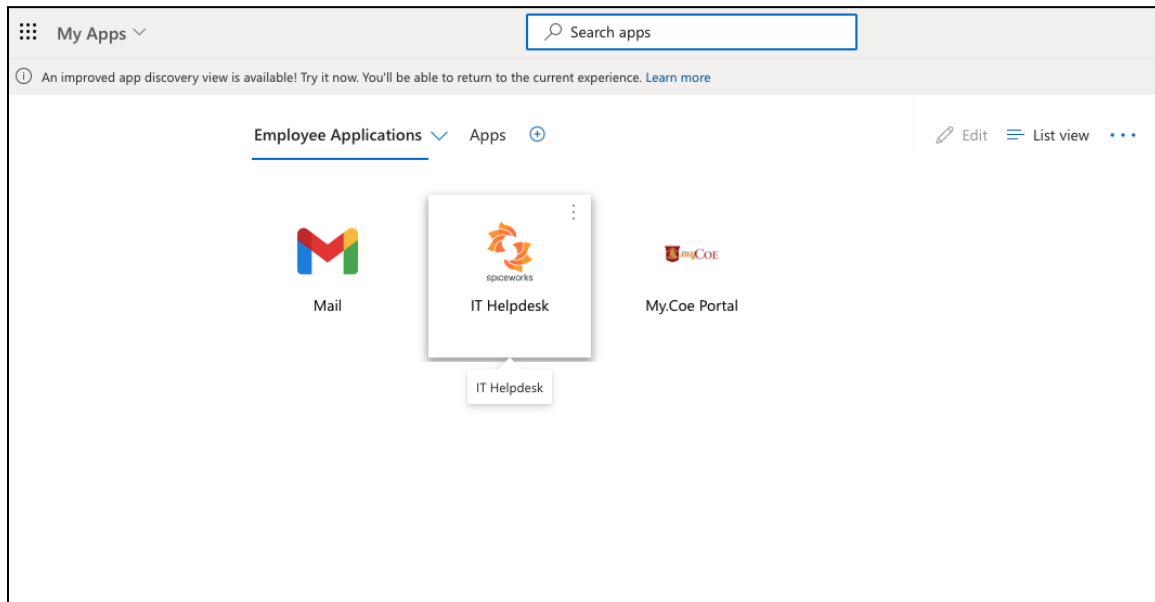
19. This screen will appear. Hit "Next".



20. The below screen will appear on your computer screen. Click "Done". You may be prompted to "approve the new sign in request" on your phone/secondary device. Approve the request and your account setup process has been completed!



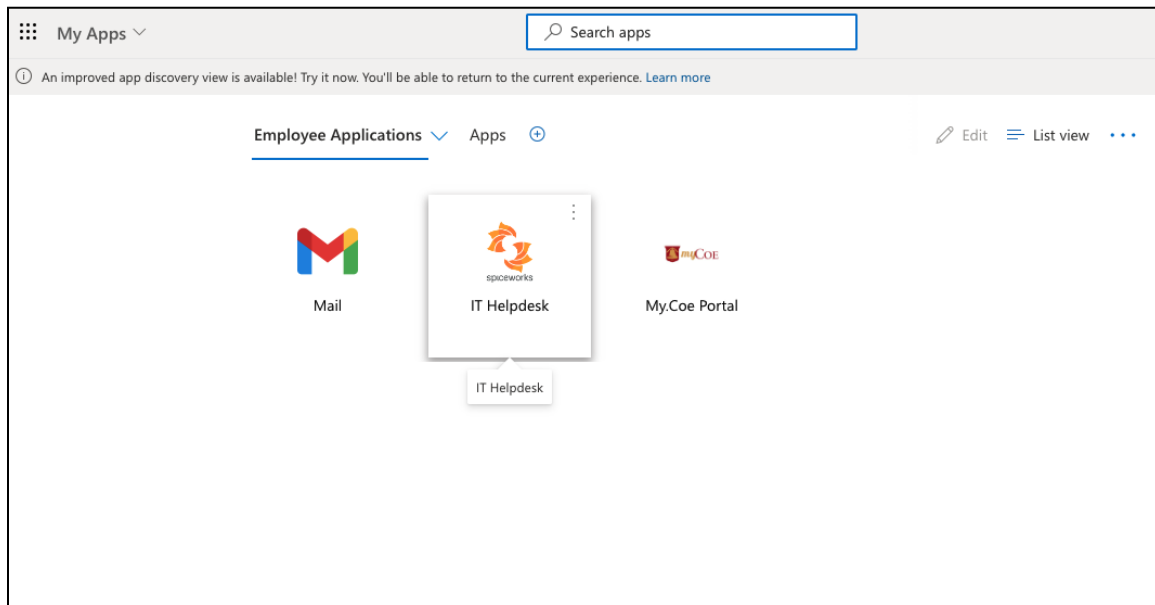
21. Once you've completed the account setup process, you will be directed to your Azure portal. See example below:



22. Click the links/icons in your portal, for easy access to these Coe systems.

What is the Azure portal for?

The Azure platform/portal manages the MFA process and contains links (the icons) to campus systems, allowing for access to other campus systems with as few clicks as possible. Here is an example screenshot. All systems that are integrated into the Azure platform can be accessed from your portal simply by clicking on the appropriate icon. (Note: Some systems utilizing MFA may not be accessible through this platform immediately. But the IT team is working to integrate as many systems as possible into the platform for ease of use.):



What will the Azure login process look like after the first time?

1. Visit apps.coe.edu.
2. Log in with your username (Coe email) and network password.
3. You will be prompted on a secondary device to accept a push notification from Microsoft Authenticator.
4. Once the push notification is accepted, you will have access to the Azure portal and other campus systems.