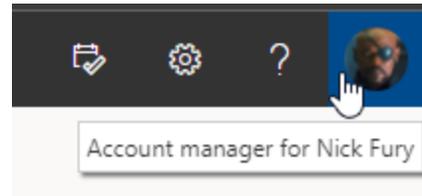
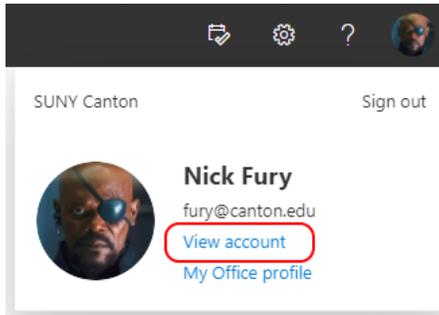


Setup for Multifactor Authentication (MFA) and Self-Service Password Reset (SSPR)

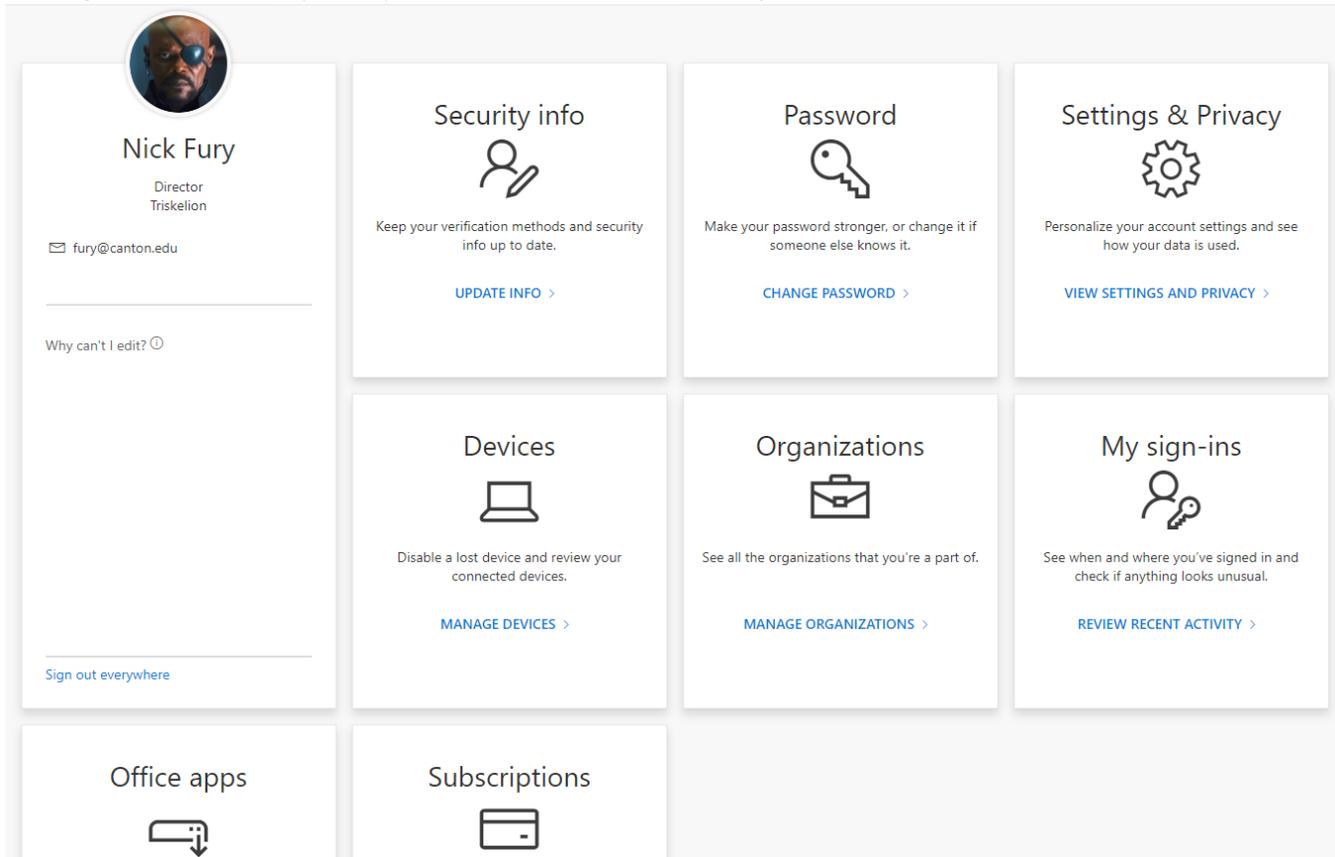
Login to the Microsoft 365 portal (<https://portal.office.com>) with your Canton [NetID](#).

Once logged in, click on your account profile in the upper right of the portal page.

In the dropdown that opens, click on **View account**.



The **My Account** site (<https://myaccount.microsoft.com/>) will open in a new browser tab.



Click on **UPDATE INFO** on the **Security info** tile.

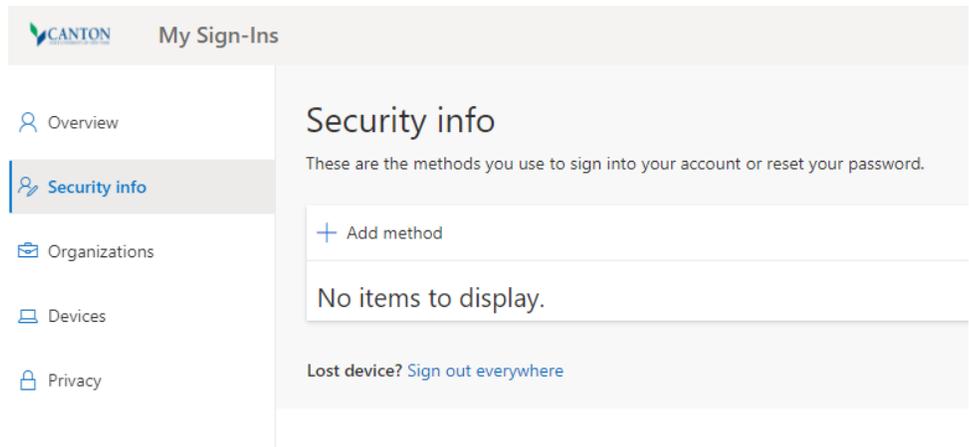
Security info



Keep your verification methods and security info up to date.

[UPDATE INFO >](#)

The My Sign-Ins page will open to the Security info section, where you are able to add methods for your second factor.



My Sign-Ins

Security info

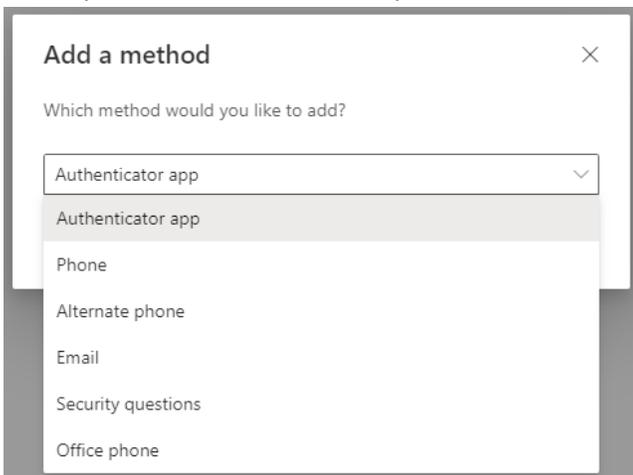
These are the methods you use to sign into your account or reset your password.

+ Add method

No items to display.

Lost device? [Sign out everywhere](#)

When you click on **Add method**, you will see the methods available for setup:



Add a method

Which method would you like to add?

Authenticator app

Authenticator app

Phone

Alternate phone

Email

Security questions

Office phone

Authenticator App

- Authenticator apps, which are typically installed on your cell phone, provide a second factor either through a push notification or a generated code. The preferred app is the [Microsoft Authenticator](#), which is available for IOS and Android mobile devices and is the only authenticator app that provides push notifications. Authenticator apps can be used for both MFA and SSPR.

Phone

- You can use your cell phone as your second factor by having a code sent to your phone by SMS, or by receiving a voice call from Microsoft and acknowledging it with a key press. You can add additional phone numbers for voice call acknowledgement only. The phone method can be used for both MFA and SSPR.

Email

- You can use an alternate email address as a second factor for SSPR only. An alternate email cannot be used for MFA.

Security questions

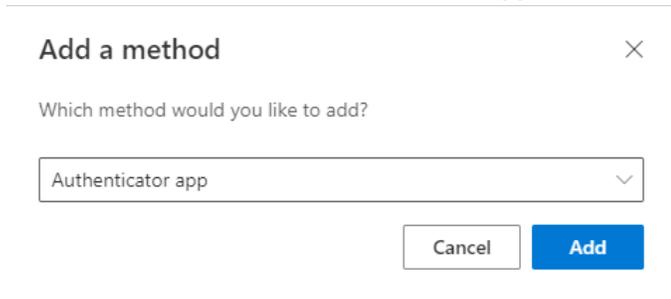
- Security questions can be setup as a second factor for SSPR only. Security questions cannot be used for MFA.

For whichever method you select, step through the setup directions. You should setup more than one method for MFA so you can have a backup option in case your default method is not available.

The most common issue we have seen is where someone has an authenticator app as their only MFA method and they get a new phone. Their authenticator app is linked to their old phone, and they don't have a backup method enabled, such as a voice call or text message. In this instance, the Help Desk has to be notified so that the individual's MFA settings can be cleared and new methods setup.

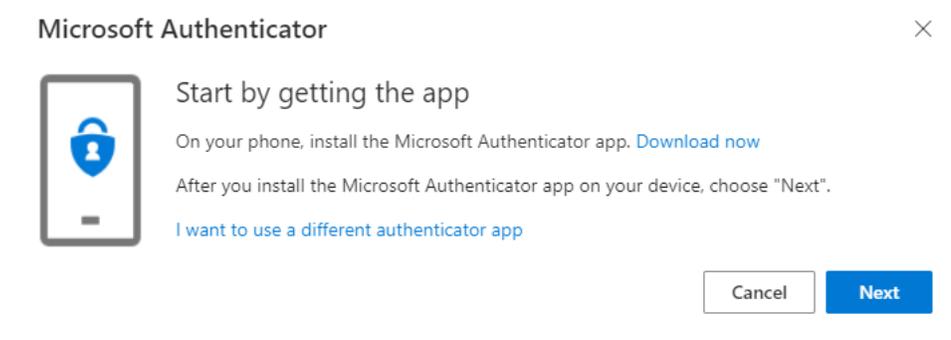
In the following example, we will step through the setup of the Microsoft Authenticator

For Add a method, select **Authenticator app...**

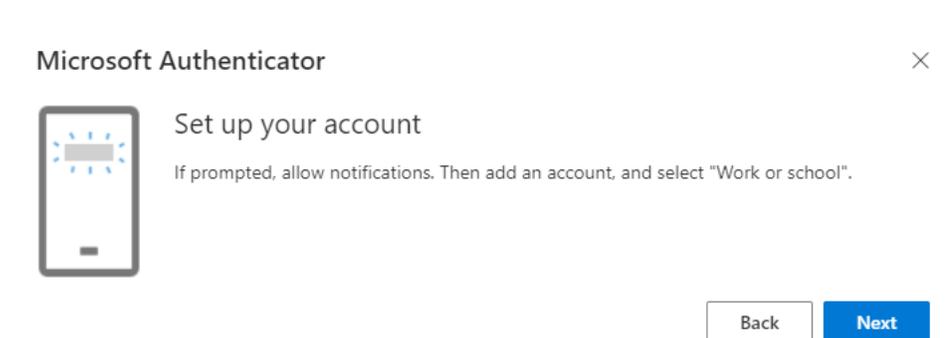


Click **Add**.

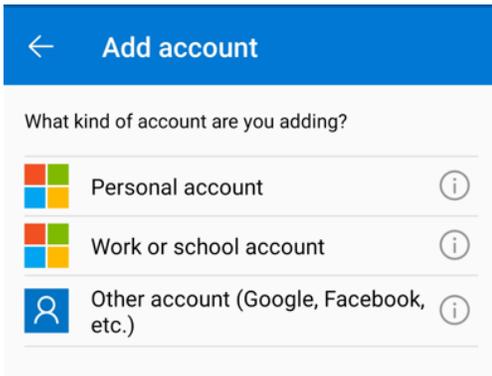
If you haven't already, download and install the Microsoft Authenticator on your phone.



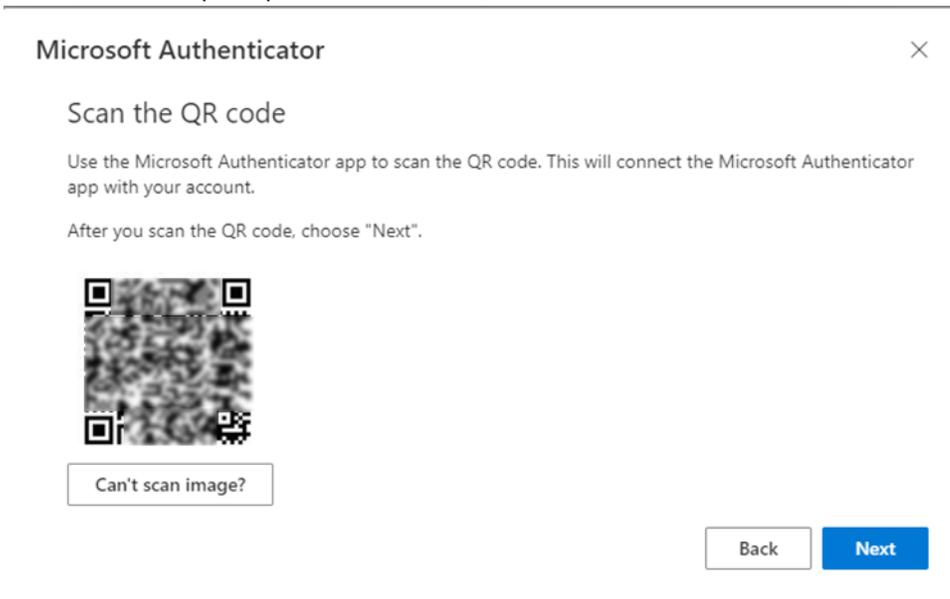
Once you have the Microsoft Authenticator installed, click **Next**.



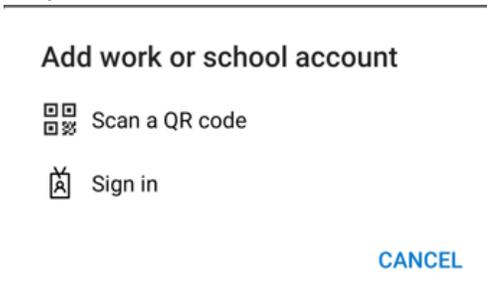
On your phone, open the Microsoft Authenticator and click Add account. Select Work or school account



When you are at the prompt to scan a QR code in your Microsoft Authenticator, click **Next** on your MFA setup. You will then be prompted to scan the QR code.

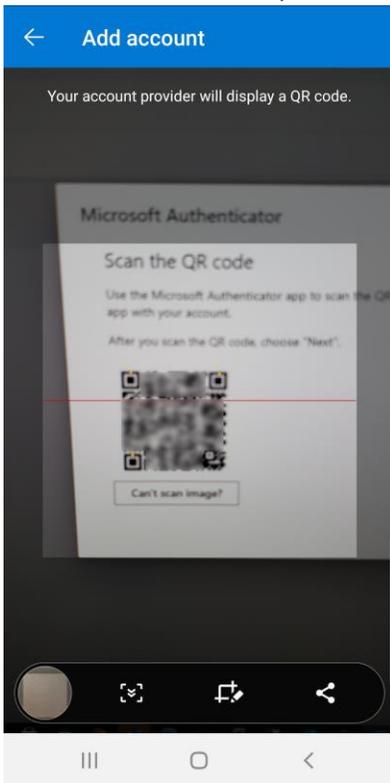


On your Microsoft Authenticator, click **Scan a QR code**.



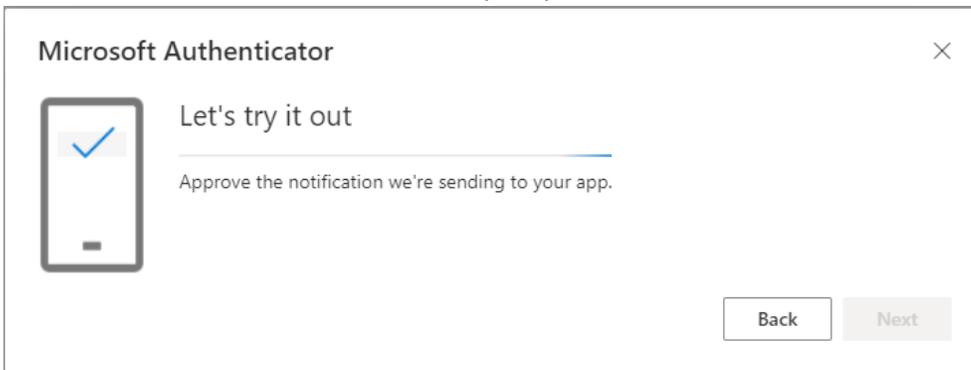
You may need to allow the Authenticator app to access the camera.

Scan the QR code with your Authenticator app.

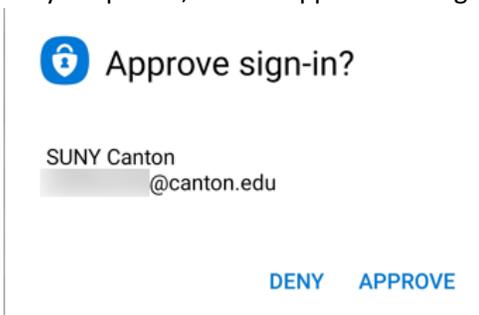


Once the QR code has been successfully scanned, click **Next** on your MFA setup.

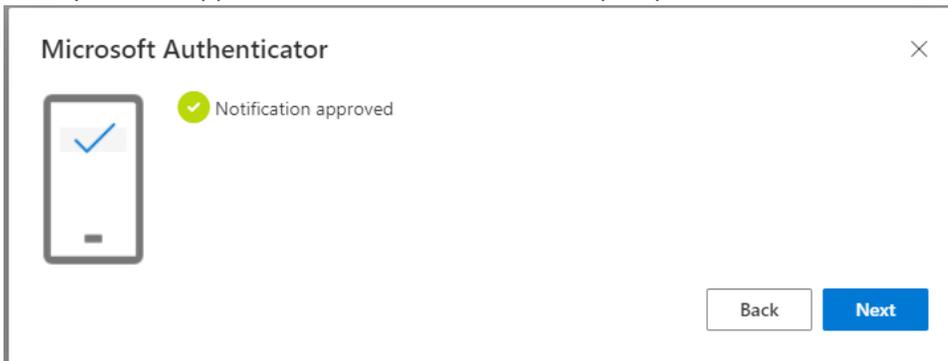
An MFA notification will then be sent to your phone..



On your phone, click to approve the sign-in notification.

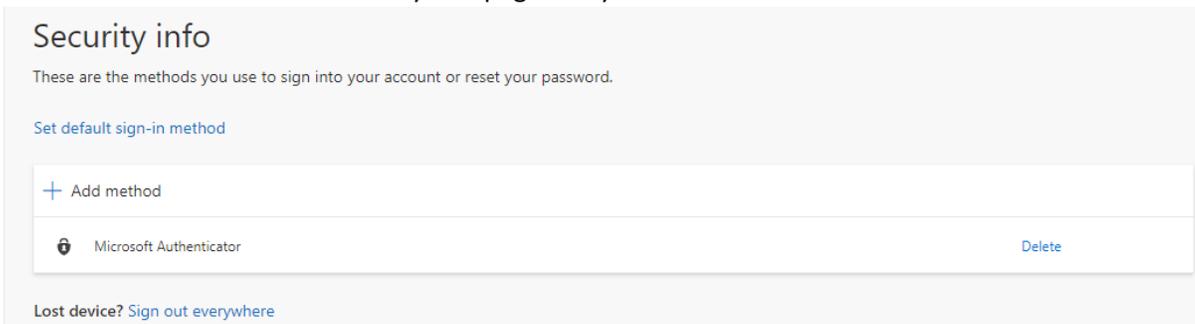


Once you have approved the notification, the setup of your Microsoft Authenticator is complete.

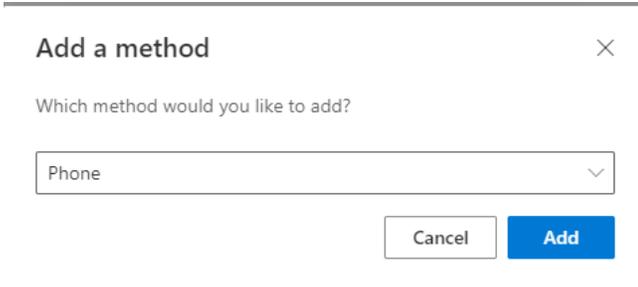


Click **Next**

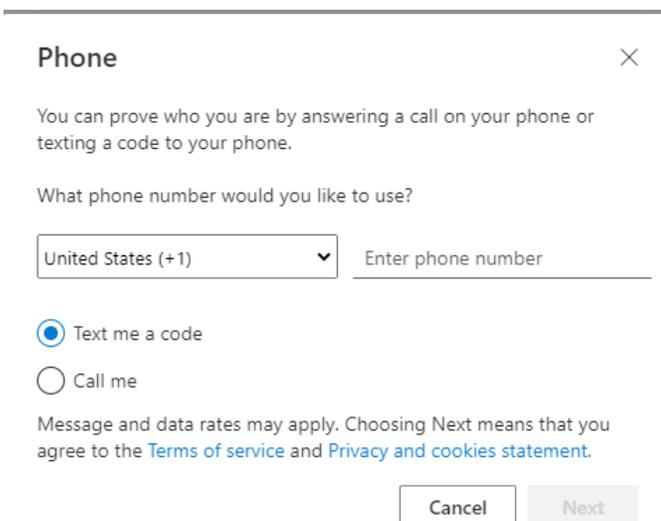
You will be returned to the Security info page and you should see the Microsoft Authenticator listed.



As mentioned, you should add another method as an alternate MFA method so you have a backup option. The other supported method for MFA is using a phone for text or voice calls. Click Add method and select Phone.



Click **Add**



Enter in your phone number, including area code. Select whether you want to receive a text with a code, or a voice call. Click **Next** and you will then need to approve the option you selected.

If it was **Text me a code**, you will receive a code and will need to enter it on the following screen...

Phone ✕

We just sent a 6 digit code to +1 315 ██████ Enter the code below.

Enter code

[Resend code](#)

Once you enter the code and click **Next**, you should receive confirmation that your phone has been registered.

Phone ✕

 SMS verified. Your phone was registered successfully.

If it was **Call me**, you will receive a voice call from Microsoft with instructions to follow to approve the option.

Phone ✕

We're calling +1 315 ██████ now.

Once approved, you should receive confirmation that your phone has been registered.

Phone ✕

 Call answered. Your phone was registered successfully.

You should now see your phone listed as another method that can be used for MFA and SSPR.

Security info

These are the methods you use to sign into your account or reset your password.

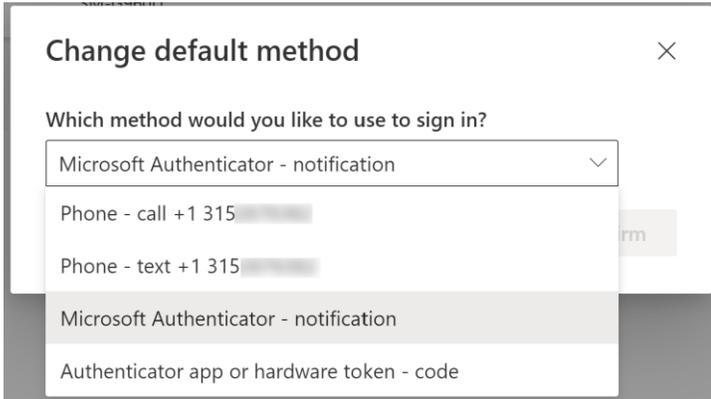
Default sign-in method: Microsoft Authenticator - notification [Change](#)

+ Add method			
	Phone	+1 315 ██████	Change Delete
	Microsoft Authenticator	SM-G960U	Delete

Your default sign-in method will be listed.

Default sign-in method: Microsoft Authenticator - notification [Change](#)

You can change your default method by clicking Change and selecting a different method from the dropdown.

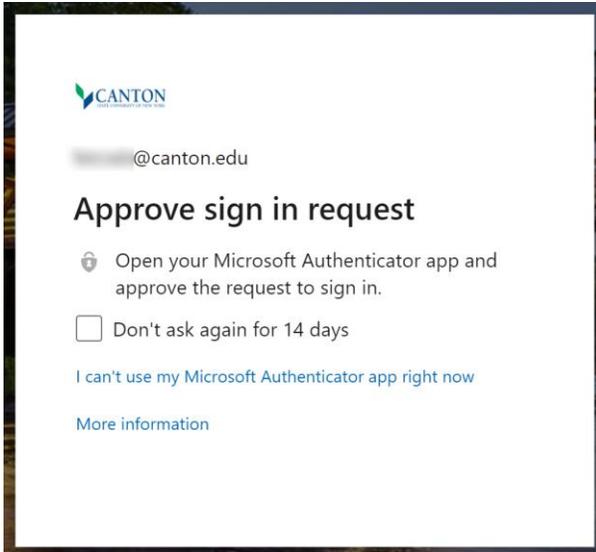


The screenshot shows a dialog box titled "Change default method" with a close button (X) in the top right corner. Below the title, it asks "Which method would you like to use to sign in?". A dropdown menu is open, showing the current selection "Microsoft Authenticator - notification" and a list of other options: "Phone - call +1 315 [redacted]", "Phone - text +1 315 [redacted]", "Microsoft Authenticator - notification" (highlighted), and "Authenticator app or hardware token - code".

What does the MFA prompt look like?

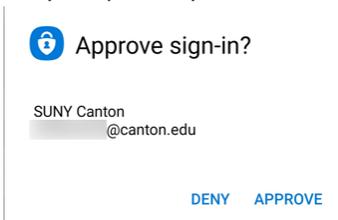
For a resource that requires you to MFA, you will login as you normally would with your Canton NetID. However, after you enter in your password, you will be prompted to complete your second factor.

With the Microsoft Authenticator as the default sign-in method



The screenshot shows a mobile-style prompt with the SUNY CANTON logo at the top. Below the logo is the email address "[redacted]@canton.edu". The main heading is "Approve sign in request". There are two instructions: "Open your Microsoft Authenticator app and approve the request to sign in." and "Don't ask again for 14 days" with an unchecked checkbox. At the bottom, there are two links: "I can't use my Microsoft Authenticator app right now" and "More information".

On your phone you will receive a prompt to approve your sign-in.



The screenshot shows a mobile notification-style prompt. It starts with a blue shield icon and the text "Approve sign-in?". Below that, it says "SUNY Canton" and "[redacted]@canton.edu". At the bottom, there are two buttons: "DENY" and "APPROVE".

Once approved, you will be signed into the resource.