

Set up Entra multi-factor authentication (MFA)

Audience: Faculty, staff, students

Introduction

The university recommends using the Microsoft Authenticator app to authenticate. This option is the most secure and works over Wi-Fi and mobile networks. If you don't want to use the Microsoft Authenticator app, you can set your authentication method to a phone call or passcode via text message (SMS). Follow the [Add a backup authentication method](#) instructions to add a phone number as your authentication method.

Entra MFA authentication methods:

- Authenticator app/mobile app (notification/code) - **RECOMMENDED**
- Phone (text/call)
- Alternate phone (call)
- Office phone (call)

You must be enrolled in at least one of the above methods. However, we highly recommend that you enrol in multiple methods to have backup/alternative options if needed. For example, even if your mobile device is enrolled, you can enrol a phone to use as a second factor. This will help you sign in if the Authenticator app is unavailable.

 You will need a computer and a mobile (or alternate) device to set up Entra MFA.

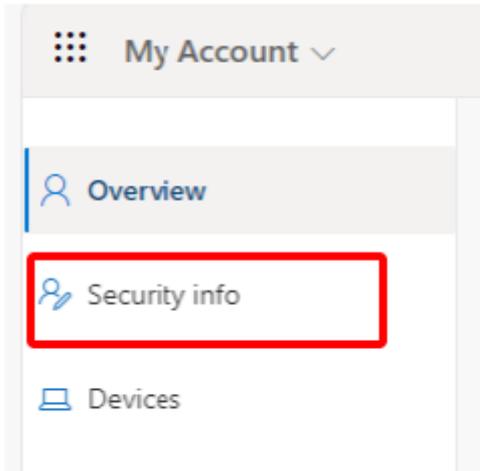
1. (On your phone) Download and install Authenticator

On your mobile device, download and install the latest version of the Microsoft Authenticator app based on your operating system.

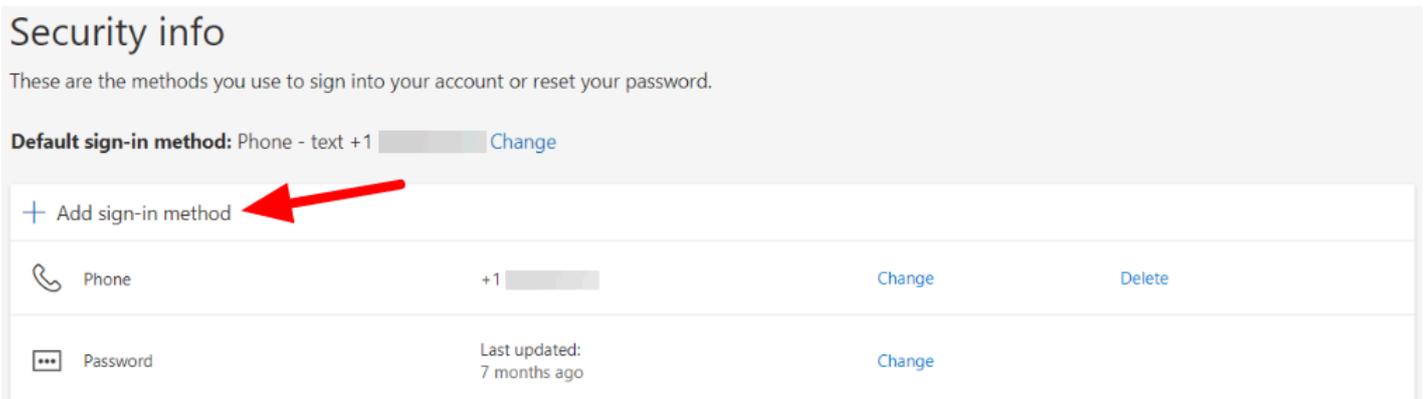
- [Apple iOS](#)
- [Google Android](#)

2. (On your computer) Add Microsoft Authenticator as a sign-in method

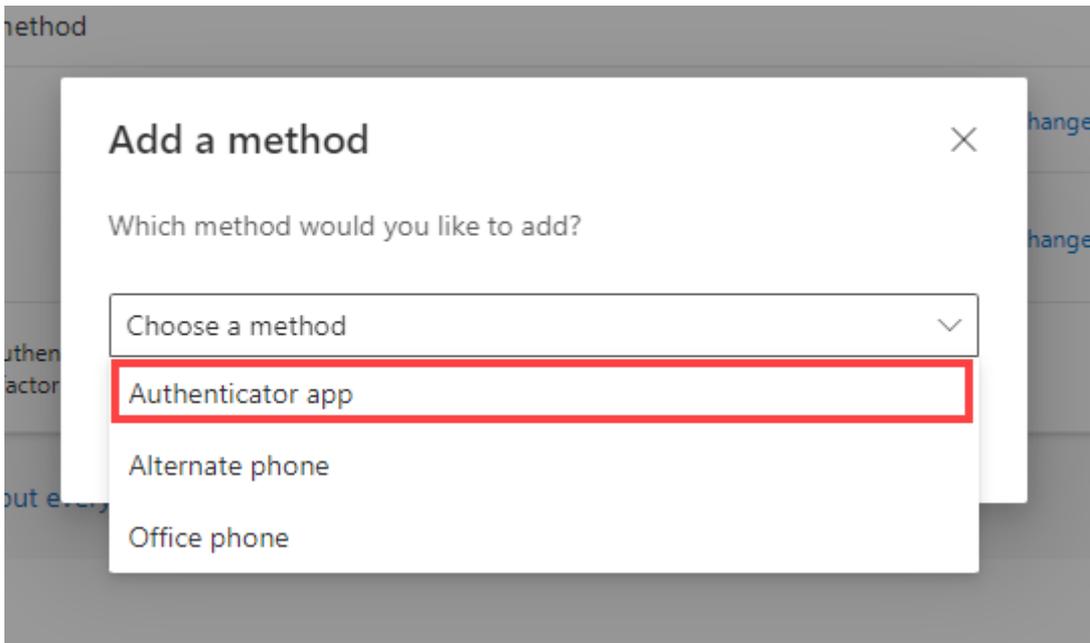
- a. Go to <https://mysignins.microsoft.com> and select **Security info**.



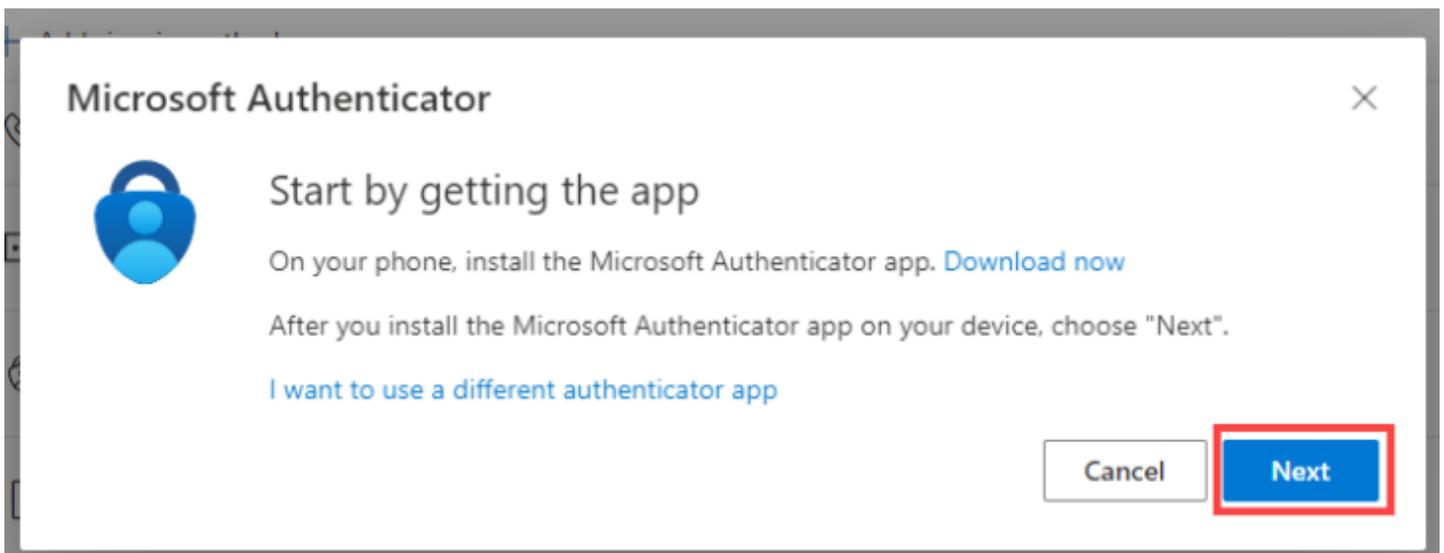
- b. On your **Security info** page, select **Add sign-in method**.



- c. Choose **Authenticator app** from the drop-down menu and select **Add**. The **Start by getting the app** screen opens.



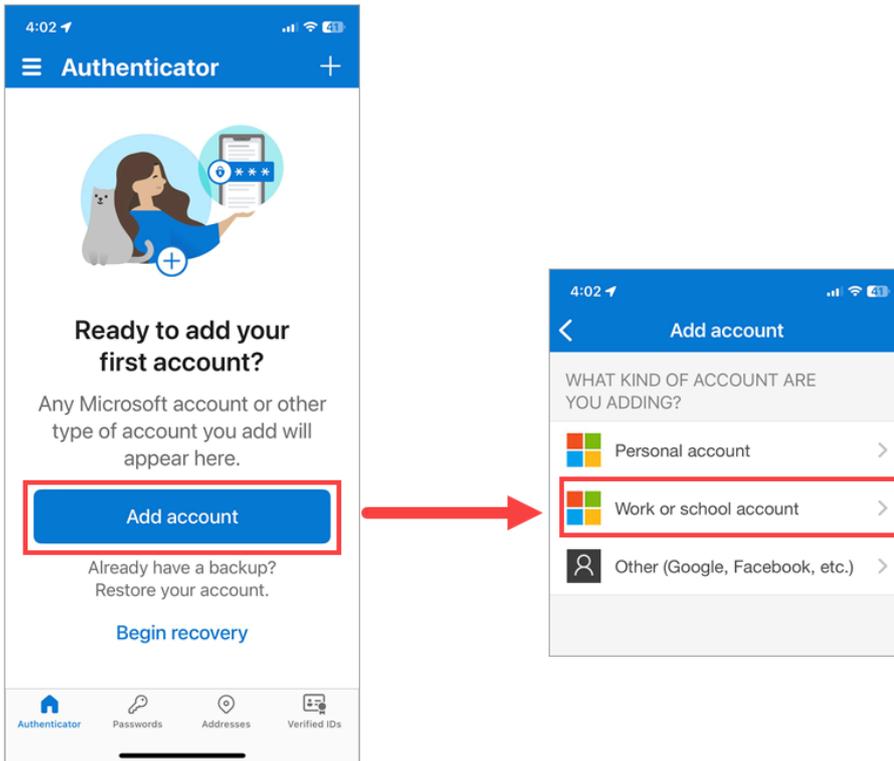
- d. On the **Start by getting the app** screen on your computer, select **Next**. The **Set up your account** screen opens.



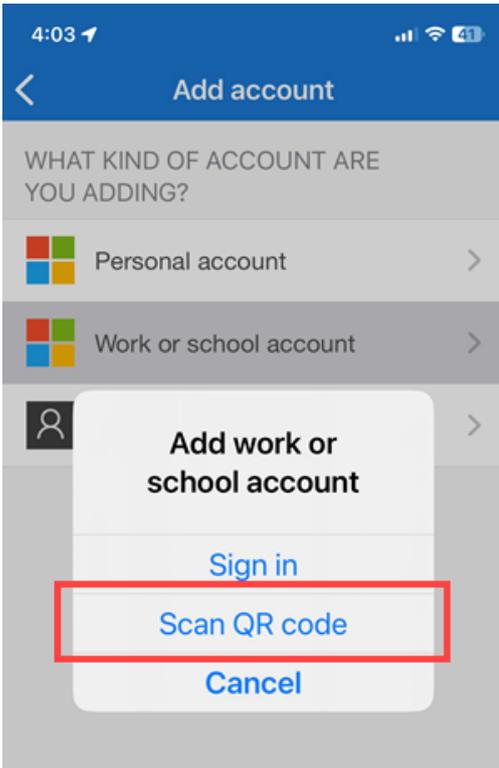
❗ If the setup window times out, sign in again and repeat steps b and c to restart the process.

3. (On your phone) Add your UM account to the Authenticator app

- a. Open the Authenticator app on your mobile device and accept the privacy policy. Allow notifications if prompted.
- b. Select **Add account**, then choose **Work or school account**.

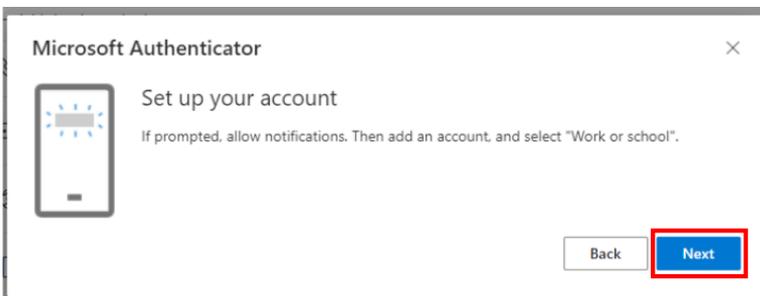


- c. In the **Add work or school account** dialogue box, select **Scan QR code**.



4. (On your computer) Go to the "Scan the QR code" screen

On the **Set up your account** screen, select **Next**. A QR (Quick Response) code is displayed.



5. (On your phone) Scan the QR code

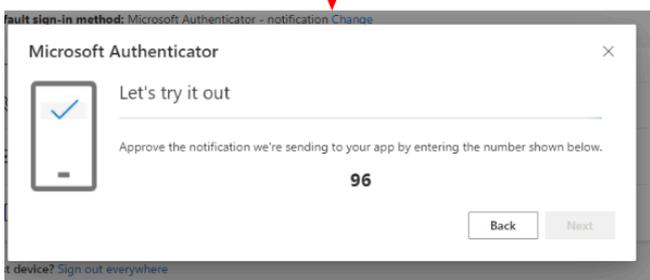
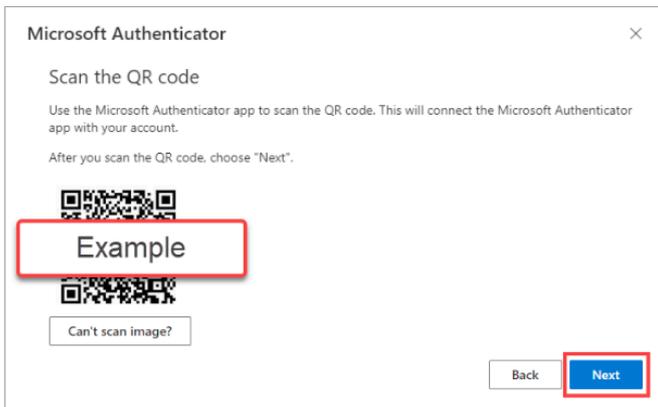
Use your mobile device to scan the QR code. Your University of Manitoba account will be added to the app.

 The option to scan the QR code is located in the **Verified IDs** section of the app.

 If you cannot scan the QR code, choose "**Can't scan image?**" under the QR code on your computer and follow the instructions.

6. (On your computer) Go to the "Let's try it out" screen

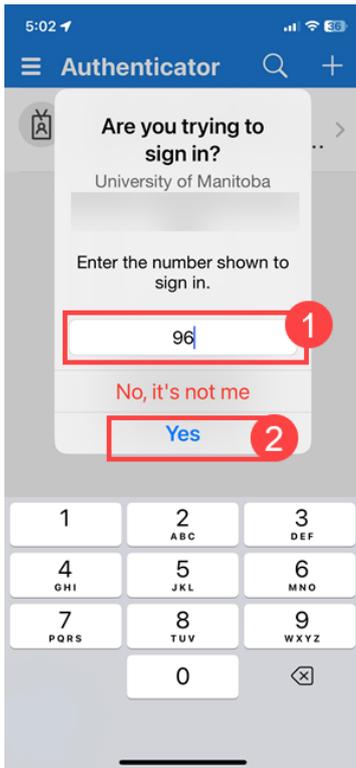
On the Scan the QR code screen, select **Next**. The **Let's try it out** screen will give you a two-digit number to enter in your Authenticator app and a notification will be sent to your phone.



7. (On your phone) Test your second-factor verification

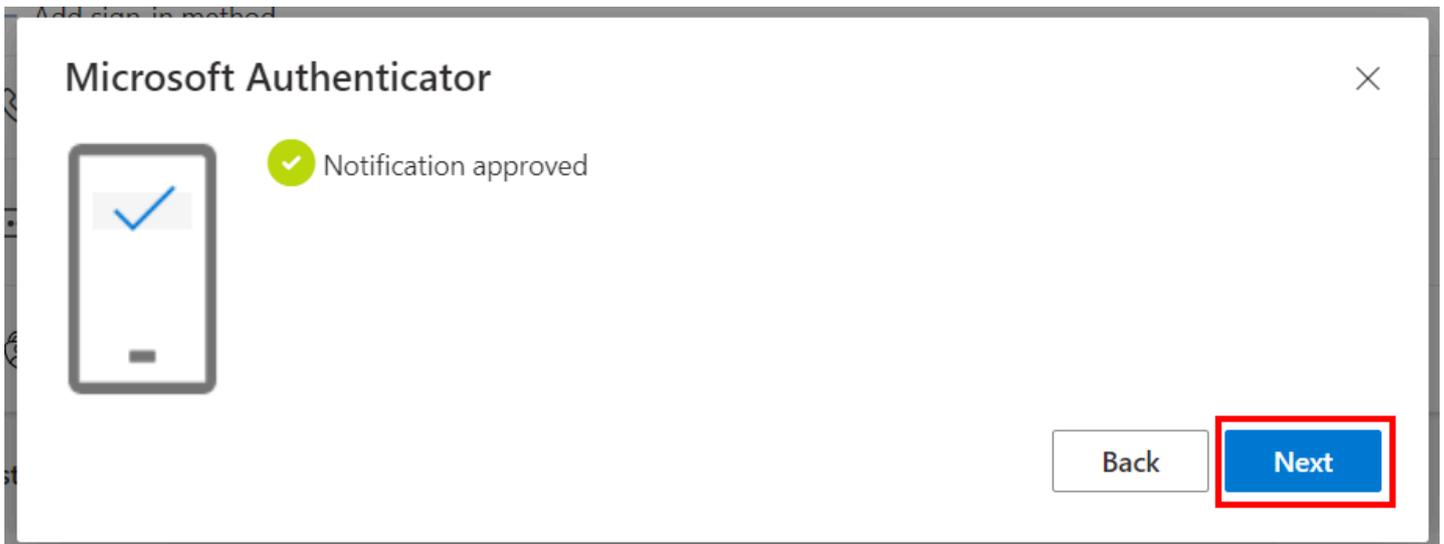
a. Select the notification to open the Authenticator app.

- b. In the Authenticator app, enter the two-digit number shown on your computer screen and select **Yes** to approve the notification.



8. (On your computer) Notification approved

- a. If successful, a **Notification approved** message appears on your computer. Select **Next**.



- b. Microsoft Authenticator is now added as a sign-in method on your **Security Info** page. Your **Default sign-in method** should be "Microsoft Authenticator - notification."
 - If Authenticator is not listed as your default sign-in method, proceed to step [9. Set Microsoft Authenticator as your default sign-in method.](#)

- If Authenticator is listed as your default sign-in method, skip to step [10. Add a backup authentication method](#).

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 sign-in method

	Phone	+1 <input type="text"/>	Change	Delete
	Password	Last updated: 7 months ago	Change	
	Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone X		Delete

9. Set Microsoft Authenticator as your default sign-in method

Follow the instructions below only if **Microsoft Authenticator - notification** is not listed as the "Default sign-in method" on your Security Info page.

1. On your Security info page, next to **Default sign-in method:** select **Change**.
2. Choose **App based authentication – notification** from the drop-down menu and select **Confirm**. Your default method is updated, and **Microsoft Authenticator – notification** is set as the default sign-in method.

10. Add a backup authentication method

Set a backup authentication method if you forget or lose your mobile device.

1. Navigate to <https://mysignins.microsoft.com> and select **Security info**.
2. Select **Add a method**.
3. From the drop-down menu, select **Phone** (or Alternate phone or Office phone).
4. Enter a phone number.
5. Choose **Text a code** or **Call me** and select **Next**. Microsoft will send a verification code to the phone number you added.
6. Enter the verification code on your screen and select **Next**.
7. Select **Done**.

 For the Alternate phone and Office phone methods, the only option is **Call me**.

Additional resources

Related pages

- [Set up MFA](#) (IST website)
- [Set up the Microsoft Authenticator app as your verification method - Microsoft Support](#)
- [Common problems with two-step verification for a work or school account](#)
- [Change your two-step verification method and settings](#)