**Education Quality and
Accountability Office**

EQAO

# Multi-Factor Authentication (MFA) User Guide

Set Up Your Account for Multi-factor
Authentication to Access the
EQAO Data Reporting Tool

## Introduction

EQAO and its technology partners have implemented an enhanced cyber-protection measure called multi-factor authentication (MFA) for users who are accessing the EQAO data reporting tool. MFA protects you by requesting additional verification of your identity when you attempt to access the EQAO data reporting tool.

## What You Need Before You Log In

To set up MFA, you must use a mobile-enabled device (i.e., smartphone). There are two methods supported for the initial setup:

1) Microsoft Authenticator App
2) Phone

**Note**: The Microsoft Authenticator App can only be downloaded on a mobile device, not your personal computer.
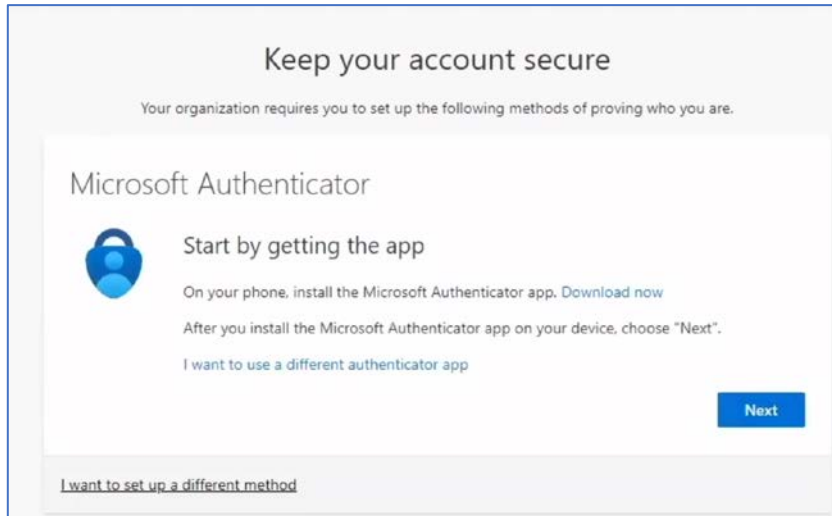
## Setup Using Microsoft Authenticator App

You will need to download and install the application on your smartphone prior to setting up your MFA account.

Each time you log into the EQAO data reporting tool, a notification will be sent to your smartphone. You will then need to open the Microsoft Authenticator app.

Microsoft Authenticator (iPhone)

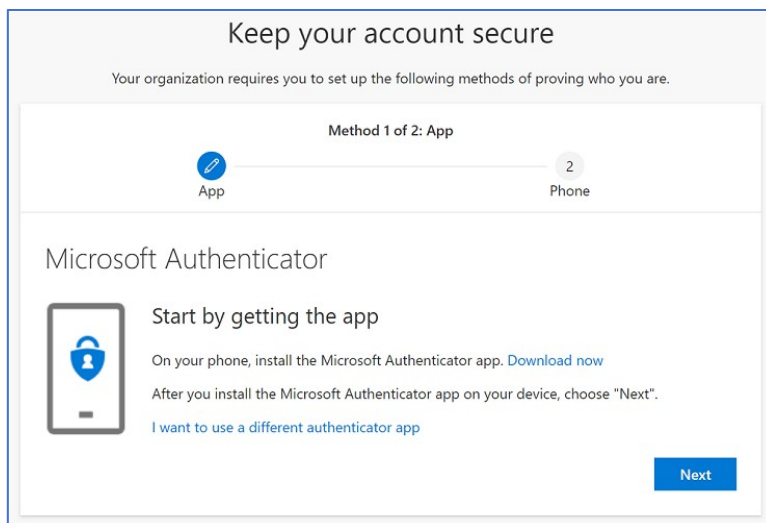Microsoft Authenticator (Android)

1. When you log into the EQAO data reporting tool for the first time, you will be prompted with:



2. After you select **Next** from the prompt, a **Keep your account secure**

   **wizard** will appear.

   Note: If you want to use an authenticator app other than the Microsoft Authenticator app, select the **I want to use a different authenticator app** link.

   If you want to set up using a phone call or text message, you can select the **I want to set up a different method** link. Click here for instructions on this method.



3. If you have not yet downloaded the app, you can Select **Download now** to download and install the Microsoft Authenticator app on your mobile device, and then select **Next**. For more information about how to download and install the app, see Download and install the Microsoft Authenticator app.

4. Remain on the **Set up your account** page while you set up the
   Microsoft Authenticator app on your mobile device.

5. On your mobile device, open the Microsoft Authenticator app, select to allow notifications (if prompted), and select **Add account** from the **Customize and control** icon on the upper-right (**+**) icon.
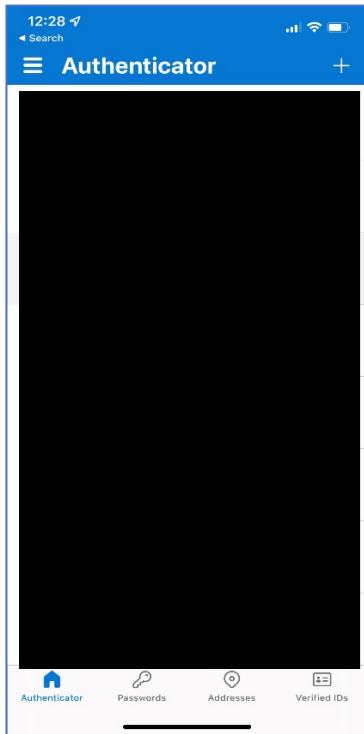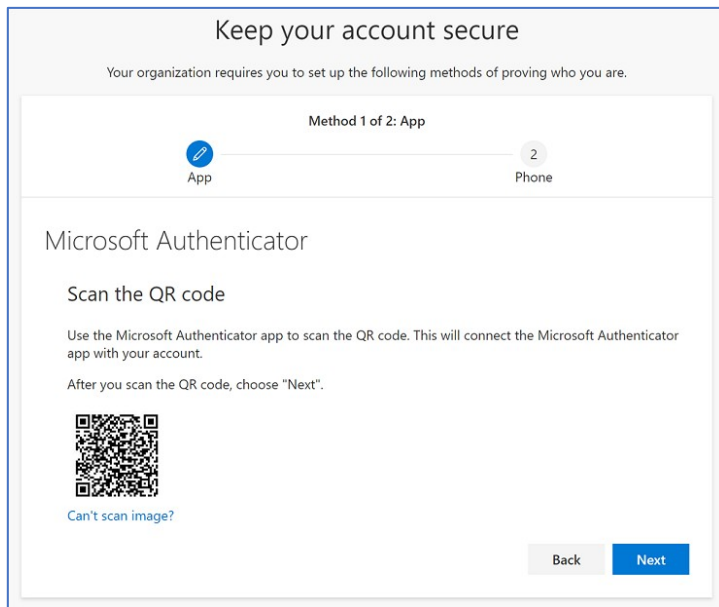


6. Select **Work or school account**.

   **Note**: If this is the first time you are setting up the Microsoft Authenticator app, you may receive a prompt asking whether you wish to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You must select **Allow** so the authenticator app can access your camera to take a picture of the QR code in the next step.



---
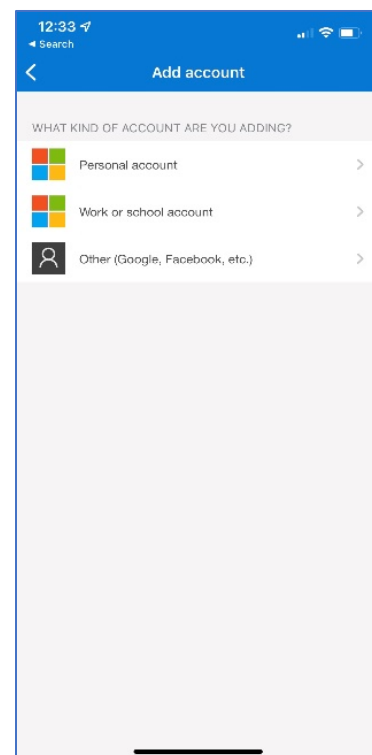
7. Return to the **Set up your account** page on your computer, and then select **Next**. The **Scan the QR code** page will appear.
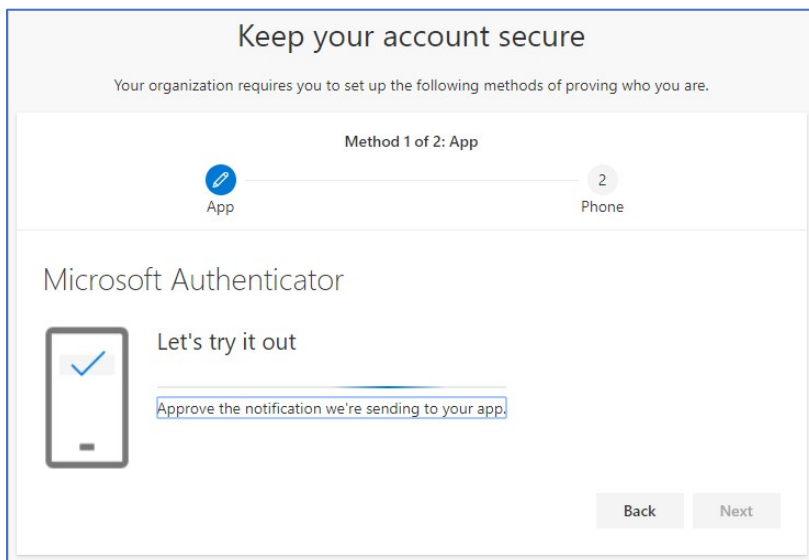


The Microsoft Authenticator app should successfully add your work or school account without requiring any additional information from you.

8. Scan the provided QR code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your work or school account in **Step 6**.

If the QR code reader can't read the code, you can select **Can't scan image?** and manually enter the code and URL into the authenticator app. For more information about manually adding a code, see Manually add an account to the app.

A notification will be sent to the Microsoft Authenticator app on your mobile device, to test your account.

9.  Approve the notification in the Microsoft Authenticator app, then select **Next**.
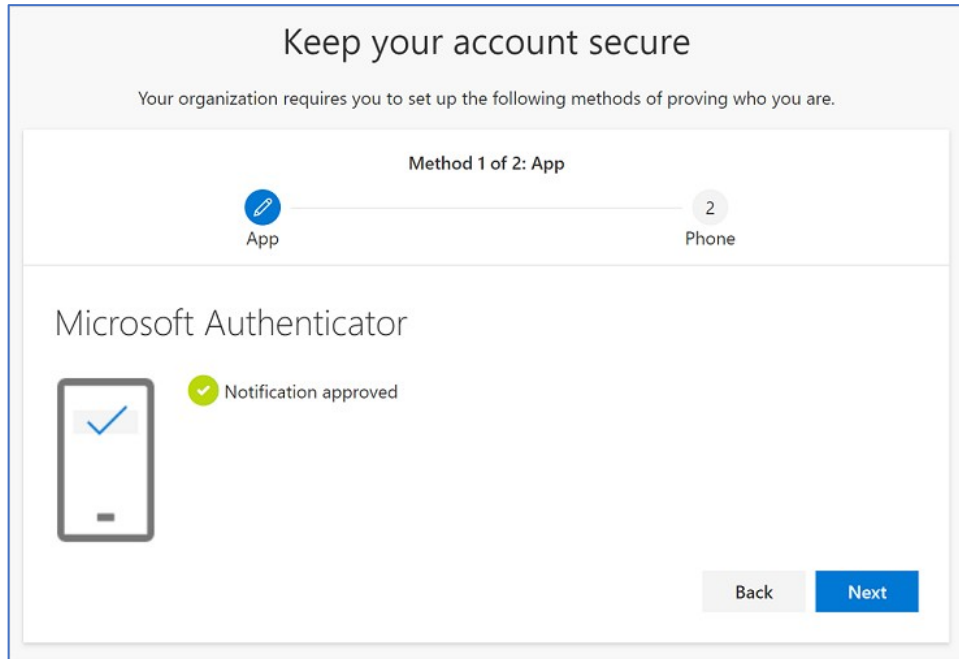


Your security information is updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.

# Setup Using Phone

1. On the **Phone** setup page, choose whether you want to receive a text message or a phone call, and then select **Next**. If you choose to receive a text message, you must use the phone number of a device that can accept text messages. (For the purposes of this example, we are using text messages.)



A text message will be sent to your phone number. If you prefer to get a phone call, the process is the same; however, you will receive a phone call with instructions instead of a text message.

2. Enter the code provided by the text message sent to your phone, and then select **Next**. If you have a problem entering the code, select **Resend code**. If you prefer to change the authentication method, select **I want to set up a different method**.

3. Review the success notification, and then select **Next**.
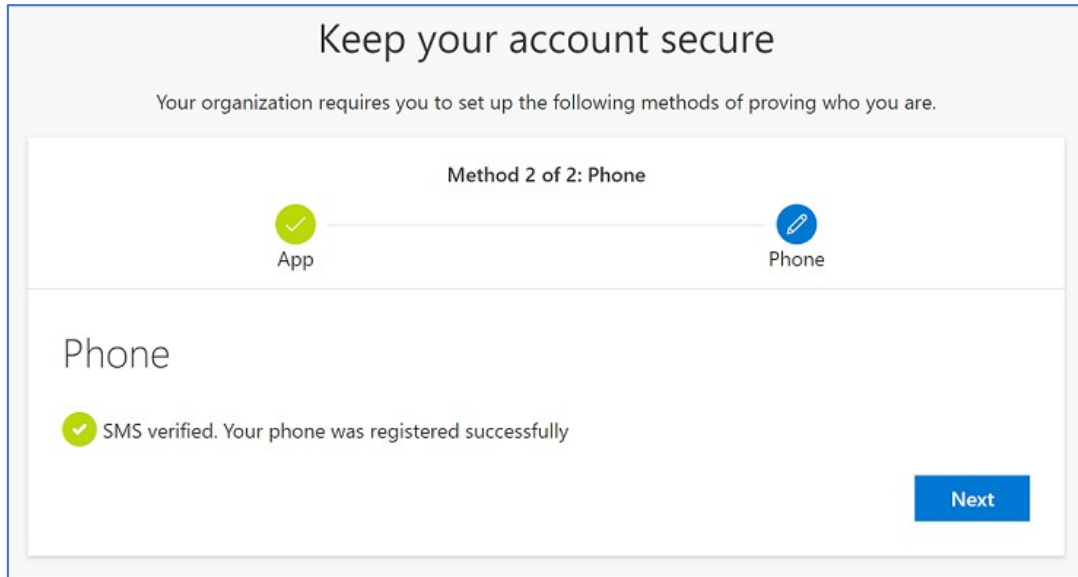


Your security information is updated to use text messaging or phone call to verify your identity when using two-step verification.

4. Review the **Success** page to verify that you have successfully set up Microsoft Authenticator via the phone method and then select **Done**.