Microsoft MFA Registration – Microsoft Office & Remote Access

If you wish to access any Microsoft Office application from your mobile device, or on any computer outside of Kettering Health Network, you must register for Microsoft Multi-Factor Authentication (MFA).

If you wish to access Microsoft Outlook (KHN email) on your mobile device, Microsoft MFA is now required. Instructions for configuring the Outlook mobile app can be found for iPhone here, and for Android here.

In addition, any Kettering employee, with a **Kettering 5- or 6-digit ID number or DR number,** who accesses the KHN Secure Access Portal from a remote location, **MUST BE** a registered user of Microsoft MFA using one of the approved Microsoft MFA authentication methods described below:

- Push notifications via the Microsoft Authenticator Mobile App (preferred method and most secure)
- A direct phone call to your authentication phone

How to Register for Microsoft MFA

1. Download & install the Microsoft Authenticator app for your mobile device in the iPhone (App Store) or Android (Google Play Store).
2. Visit https://aka.ms/mfasetup to begin set up for Microsoft MFA. **Please note you are encouraged to perform this part of the registration process from a desktop or laptop computer**.
3. Sign in with your KHN email address and click Next

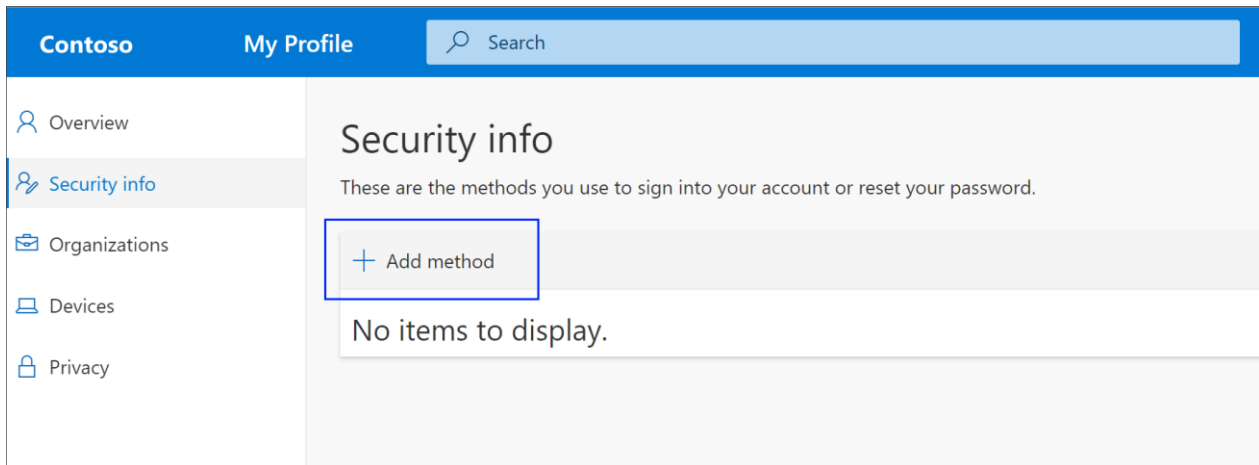# Microsoft MFA Registration – Microsoft Office & Remote Access
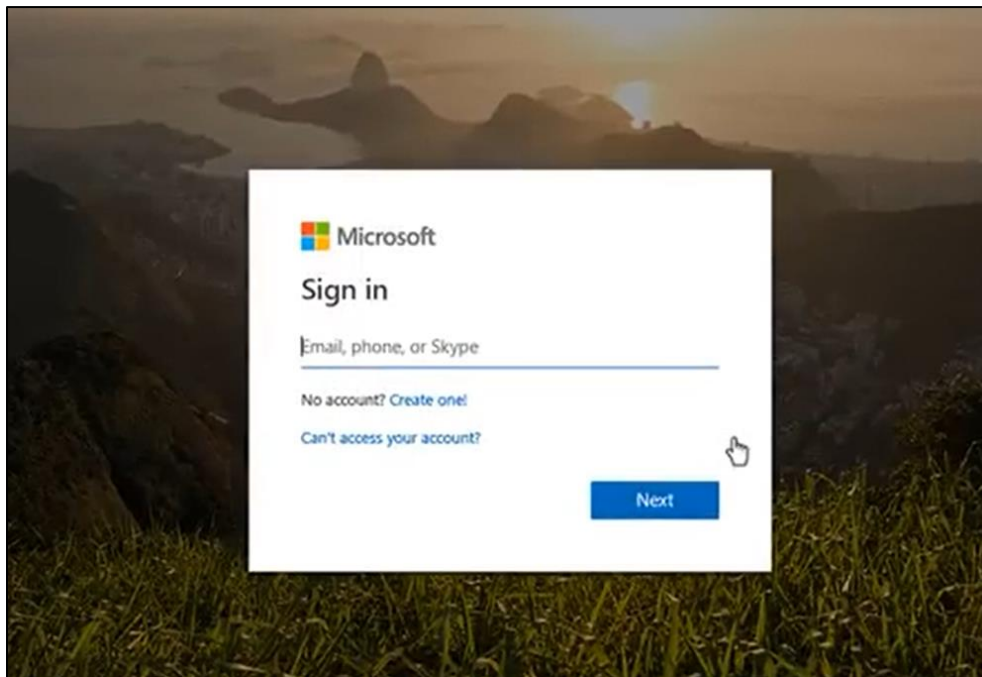
4. Sign in with your network password and click Next
5. To continue set up, click Next
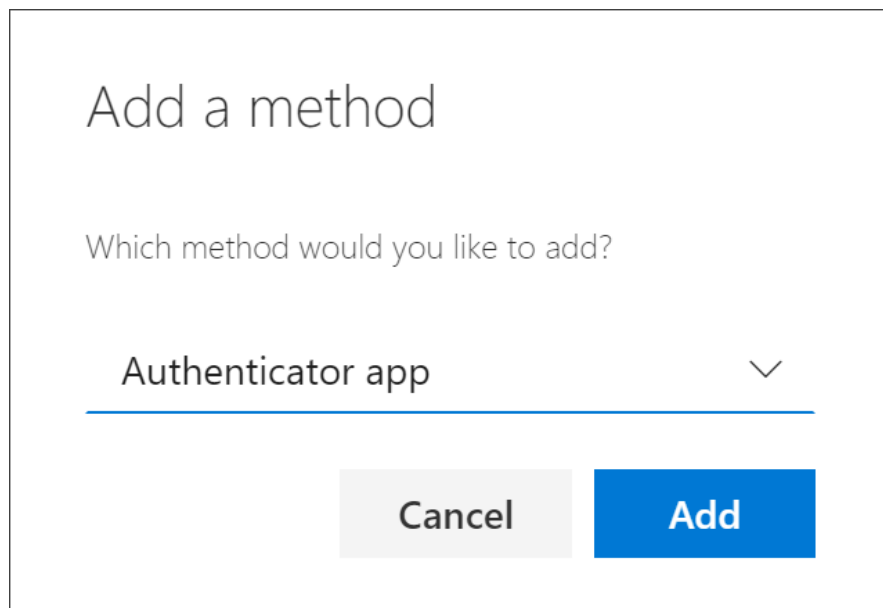6. Select Security Info from the left navigation pane or from the link in the Security Info block
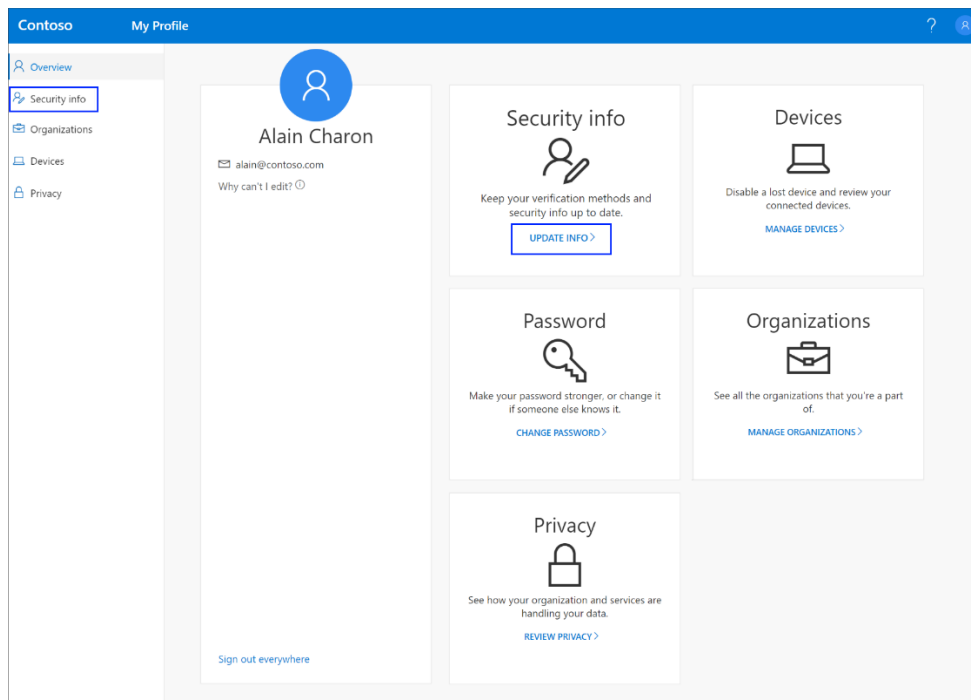
7. Select Add Method from the Security info page

# Microsoft MFA Registration – Microsoft Office & Remote Access

8. On the **Add a method** page, select **Authenticator app** from the drop-down list, and then select **Add**.


9. On the **Start by getting the app** page, 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.

Microsoft MFA Registration – Microsoft Office & Remote Access
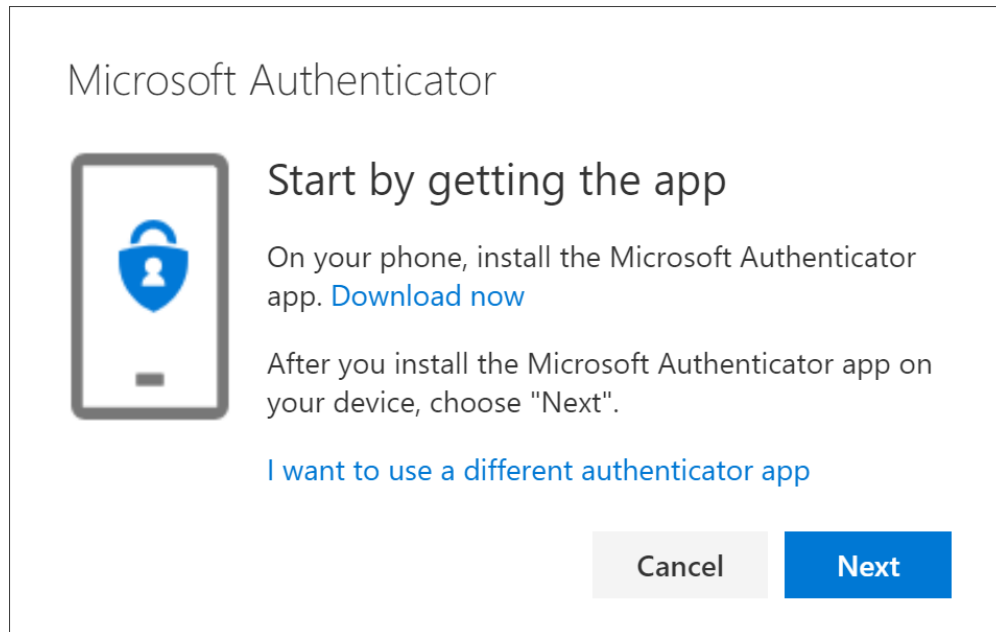
10. Remain on the **Set up your account** page while you set-up the Microsoft Authenticator app on your mobile device.
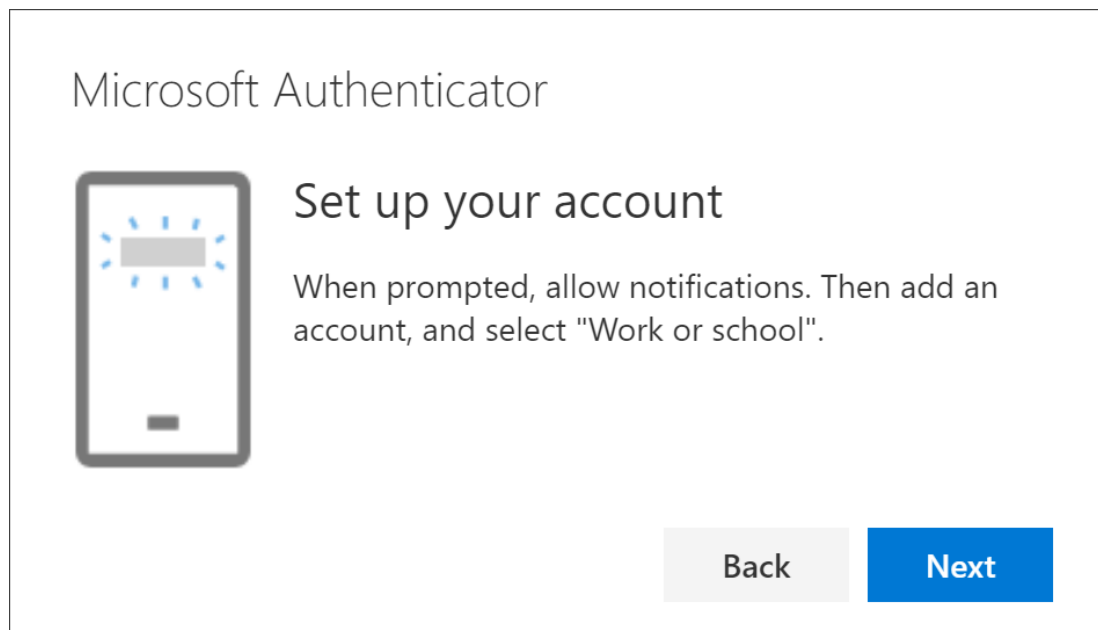
11. Open the Microsoft Authenticator app, select to allow notifications (if prompted), select **Add account** from the **Customize and control** icon on the upper-right, and then select **Work or school account**.

Note:
If this is the first time you're setting up the Microsoft Authenticator app, you might receive a prompt asking whether 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.

12. Return to the **Set up your account** page on your computer, and then select **Next**.

   The **Scan the QR code** page appears.
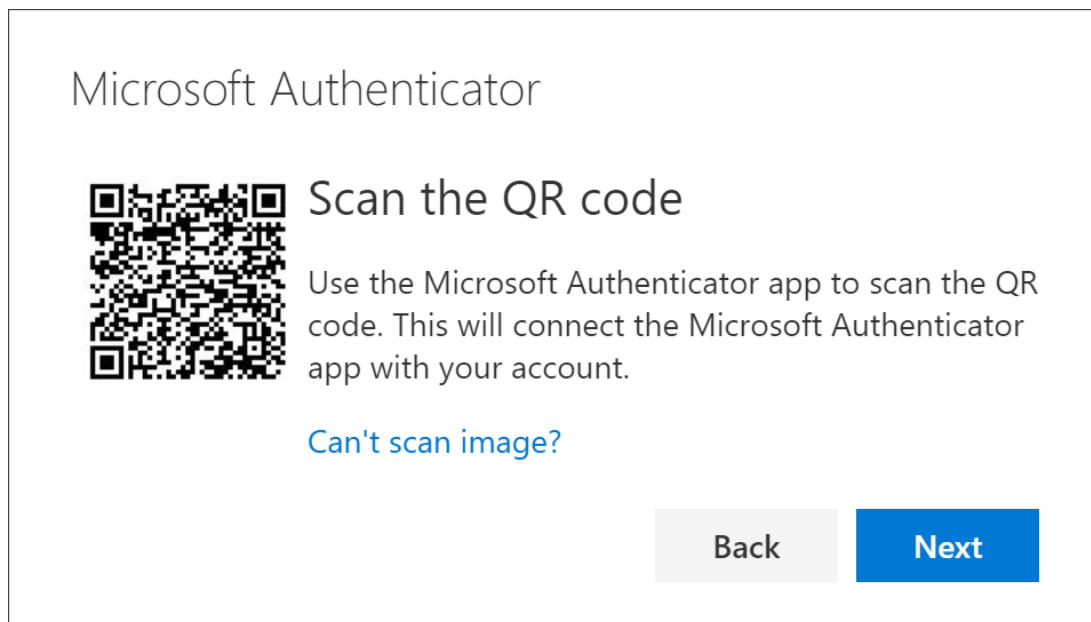
13. Scan the provided code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your work or school account in Step 11.

    The Authenticator app should successfully add your work or school account without requiring any additional information from you. However, if the QR code reader can't read the code, you can select the **Can't scan the QR code link** and manually enter the code and URL into the Microsoft Authenticator app. For more information about manually adding a code, see [Manually add an account to the app](#).
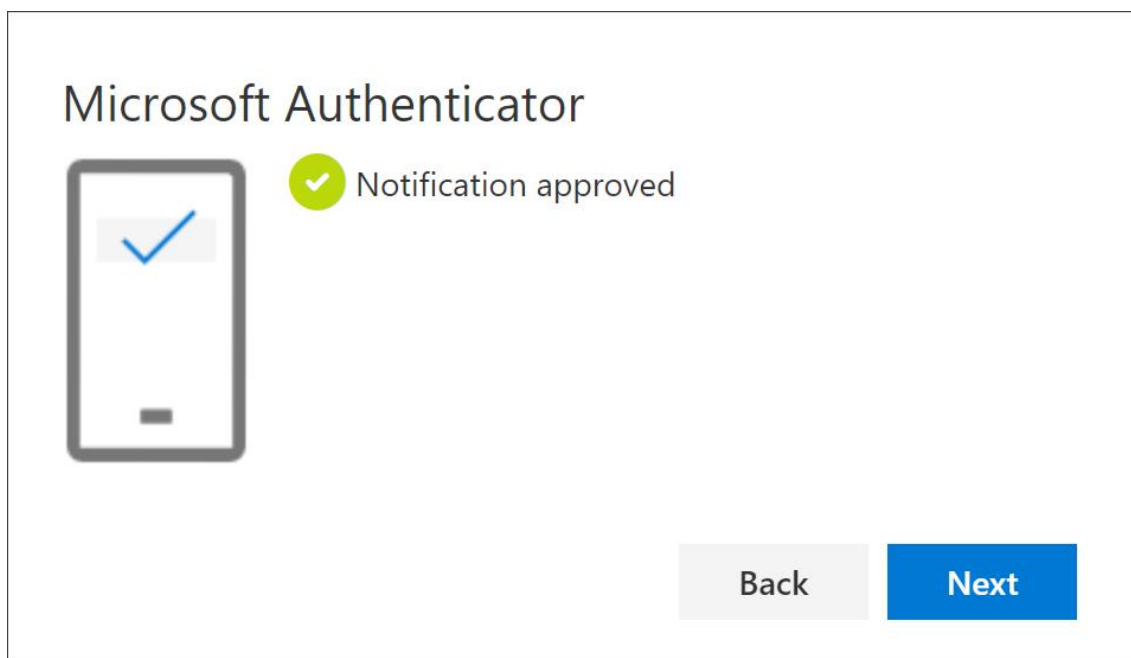
14. Select **Next** on the **Scan the QR code** page on your computer.

    A notification is sent to the Microsoft Authenticator app on your mobile device, to test your account.
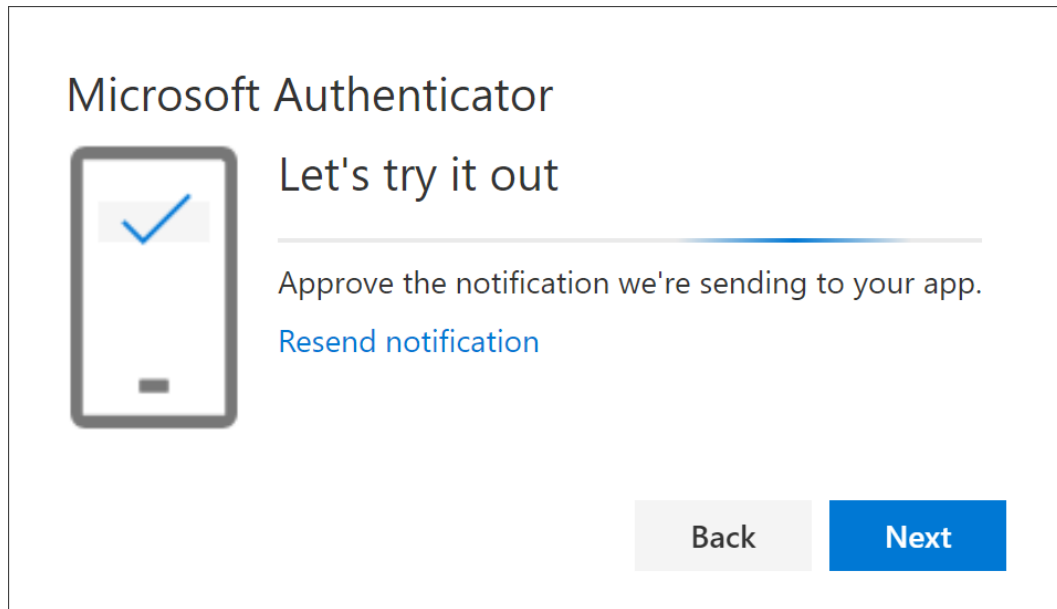
15. Approve the notification in the Microsoft Authenticator app, and then select **Next**.

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

Change your default security info method

Microsoft MFA Registration – Microsoft Office & Remote Access

If you want the Authenticator app to be the default method used when you sign-in to your work or school account using two-factor verification or for password reset requests, you can set it from the Security **info** page.
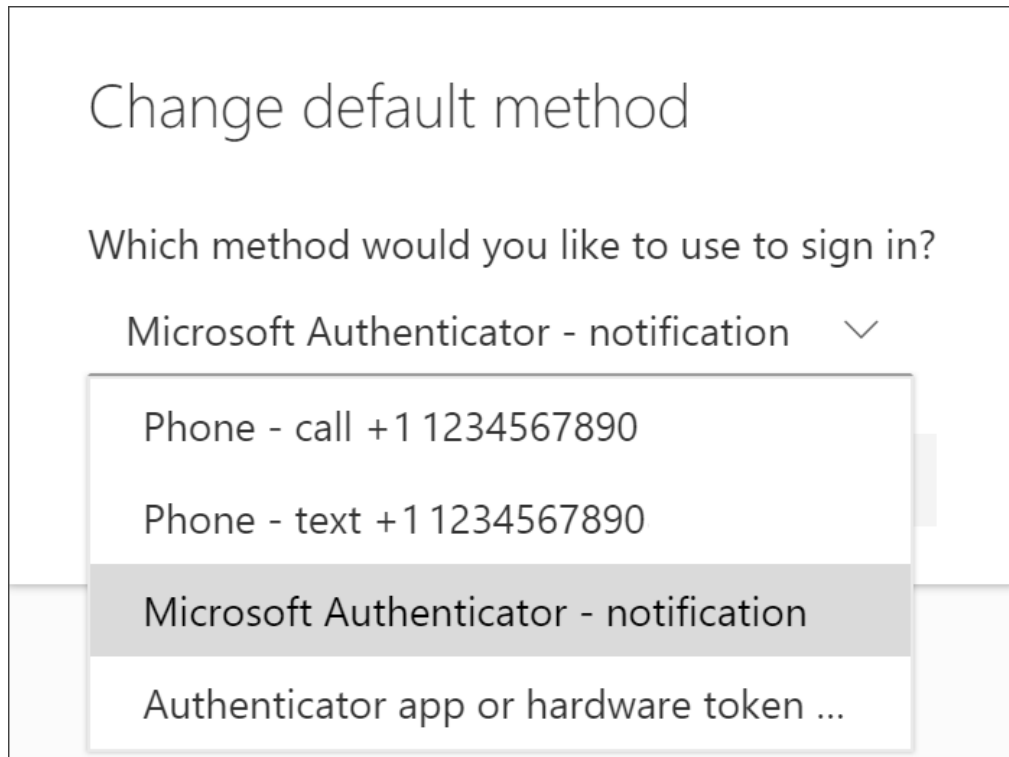
To change your default security info method

1. On the **Security info** page, select the **Change** link next to the **Default sign-in method** information.
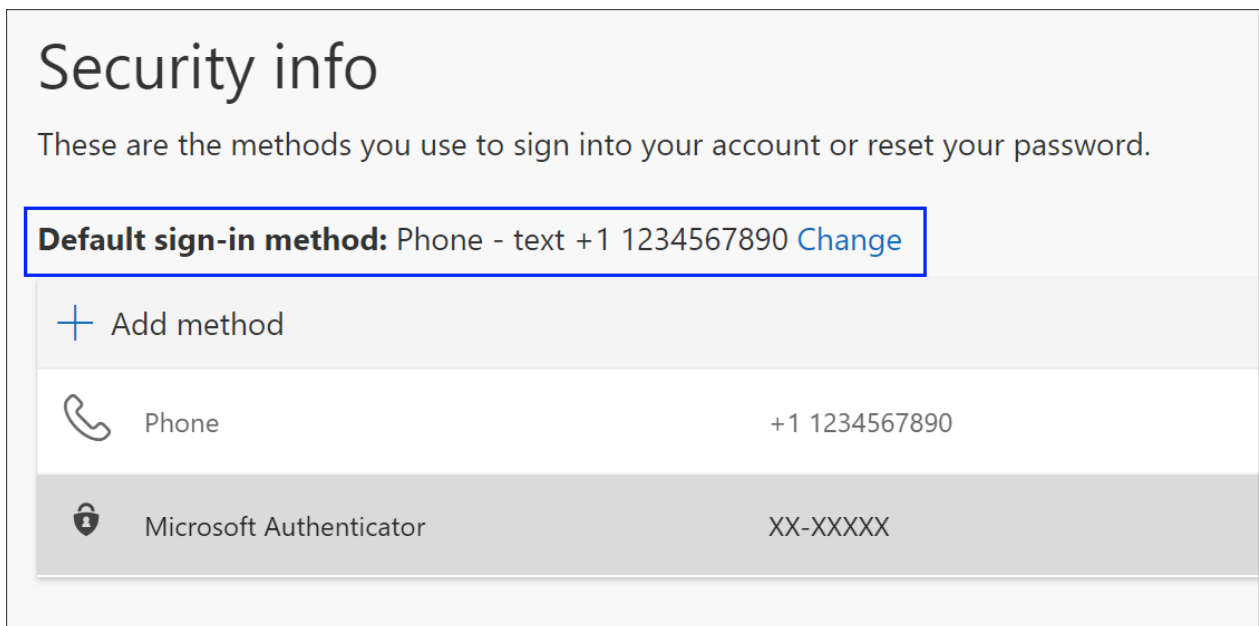
2. Choose **Microsoft Authenticator - notification** from the drop-down list of available methods. If you're not using the Microsoft Authenticator app, select the **Authenticator app or hardware token** option.

Microsoft MFA Registration – Microsoft Office & Remote Access

3. Select **Confirm**.

    The default method used for sign-in changes to the Microsoft Authenticator app.

For more information, click here to watch a short instructional video created by Microsoft for How to Register for Multi Factor Authentication.

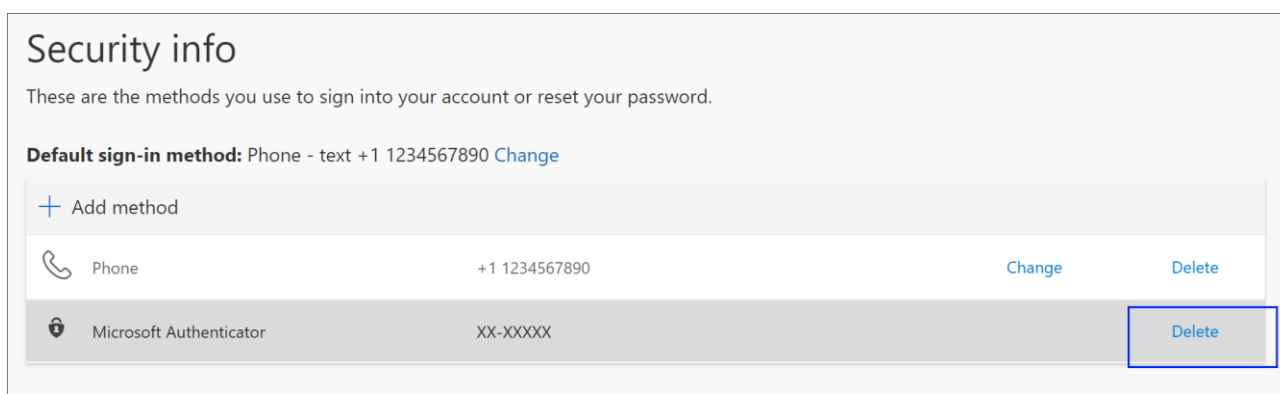# Delete your Authenticator app from your Security info methods

If you no longer want to use your Authenticator app as a security info method, you can remove it from the **Security info** page. This works for all authenticator apps, not just the Microsoft Authenticator app. After you delete the app, you'll have to go into the authenticator app on your mobile device and delete the account.

 Important

If you delete the authenticator app by mistake, there's no way to undo it. You'll have to add the authenticator app again, following the steps in the **Set up the Authenticator app** section of this article.

To delete the Authenticator app

1. On the **Security info** page, select the **Delete** link next to the Authenticator app.

2. Select **Yes** from the confirmation box to delete the Authenticator app. After the Authenticator app is deleted, it's removed from your Security info and it disappears from the **Security info** page. If the Authenticator app is your default method, the default will change to another available method.
3. Open the Authenticator app on your mobile device, select **Edit accounts**, and then delete your work or school account from the Authenticator app.

   Your account is completely removed from the Authenticator app for two-factor verification and password reset requests.