



Microsoft
Authenticator

Set up the Microsoft Authenticator app

The Microsoft Authenticator app helps you sign in to your accounts if you use two-factor verification. You can use the Microsoft Authenticator app in multiple ways, including: Two-factor verification, Phone sign-in, and Code generation.



UNIVERSITY SYSTEM
of MARYLAND

What is the Microsoft Authenticator app?

The Microsoft Authenticator app helps you sign-in to your accounts if you use two-factor verification (2FV).

You can use the Microsoft Authenticator app in multiple ways, including:

- **Notification.** Respond to a prompt for authentication after you sign in with your username and password.
- **Passwordless sign-in.** Sign-in without entering a password, using your username, the authenticator app, and your mobile device with your fingerprint, face, or PIN.
- **Verification code.** As a code generator for any other accounts that support authenticator apps.

The Microsoft Authenticator app installation is required before beginning the mobile device Multi-Factor Authentication (MFA) client setup. The Microsoft Authenticator App is available for mobile devices on these operating systems: Android, iOS, and Windows.

For more information about how to download and install the app, see [Download and install the Microsoft Authenticator app](#) article of this document.

Security vs password reset verification

Security info methods are used for both two-factor security verification and for password reset. However, not all methods can be used for both.

SECURITY VS PASSWORD RESET VERIFICATION	
Method	Used for
Authenticator app	Two-factor verification (2FV) and password reset authentication.
Text messages	Two-factor verification (2FV) and password reset authentication.
Phone calls	Two-factor verification (2FV) and password reset authentication.
Security key	Two-factor verification (2FV) and password reset authentication.
Email account	Password reset authentication only. You'll need to choose another method for two-factor verification (2FV).
Security questions	Password reset authentication only. You'll need to choose another method for two-factor verification (2FV).

Tools and Terms

Microsoft Authenticator App:

Helps you sign-in to your accounts if you use two-factor verification (2FV).

Two-Factor Verification (2FV):

Two-factor verification (2FV) helps you to access your accounts more securely, especially while viewing sensitive information. Because passwords can be forgotten, stolen, or compromised, two-factor verification (2FV) is an additional security step that helps protect your account by making it harder for other people to break in. This extra layer of security for your Office 365 account is designed to ensure that you're the only person who can access your account, even if someone knows your password.

Articles in this document

[What is the Microsoft Authenticator App?](#)

[Download and install the Microsoft Authenticator App](#)

[Set up the Microsoft Authenticator app from the Security info page](#)

[Set up Authenticator App from your phone](#)

[Change your default security info method](#)

[Delete the authenticator app](#)

Download and install the app

Install the latest version of the Microsoft Authenticator app, based on your operating system:

Google Android. On your Android device, go to Google Play to [download and install the Microsoft Authenticator app](#).

Apple iOS. On your Apple iOS device, go to the App Store to [download and install the Microsoft Authenticator app](#).

Important! *If you're not currently on your mobile device, you can still get the Microsoft Authenticator app by sending yourself a download link from the [Microsoft Authenticator page](#).*

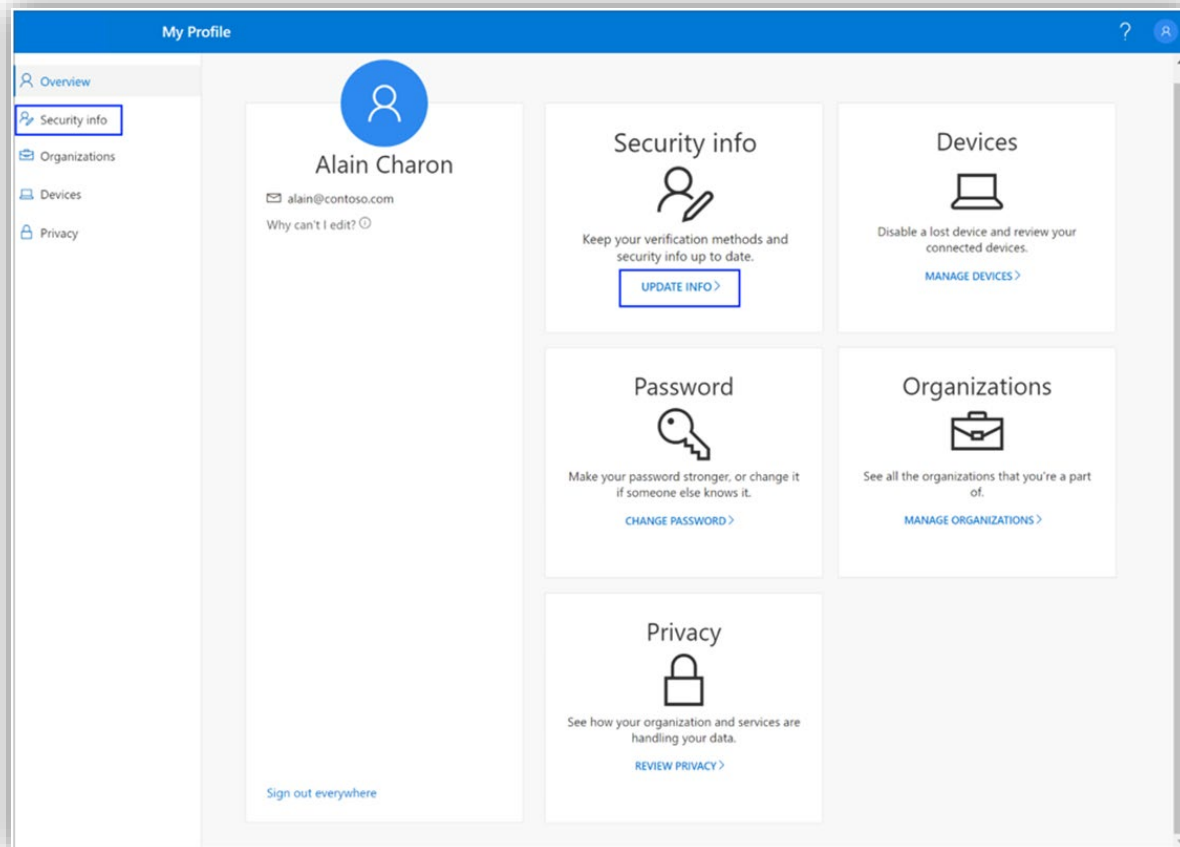
Setting up the Microsoft Authenticator app

You can follow these steps to add your two-factor verification (2FV) and password reset methods. After you've set this up the first time, you can return to the **Security info** page to add, update, or delete your security information. If you're prompted to set this up immediately after you sign in to your work or school account, see the detailed steps in the [Set up your security info from the sign-in page prompt](#) article.

Set up the Microsoft Authenticator app from the Security info page

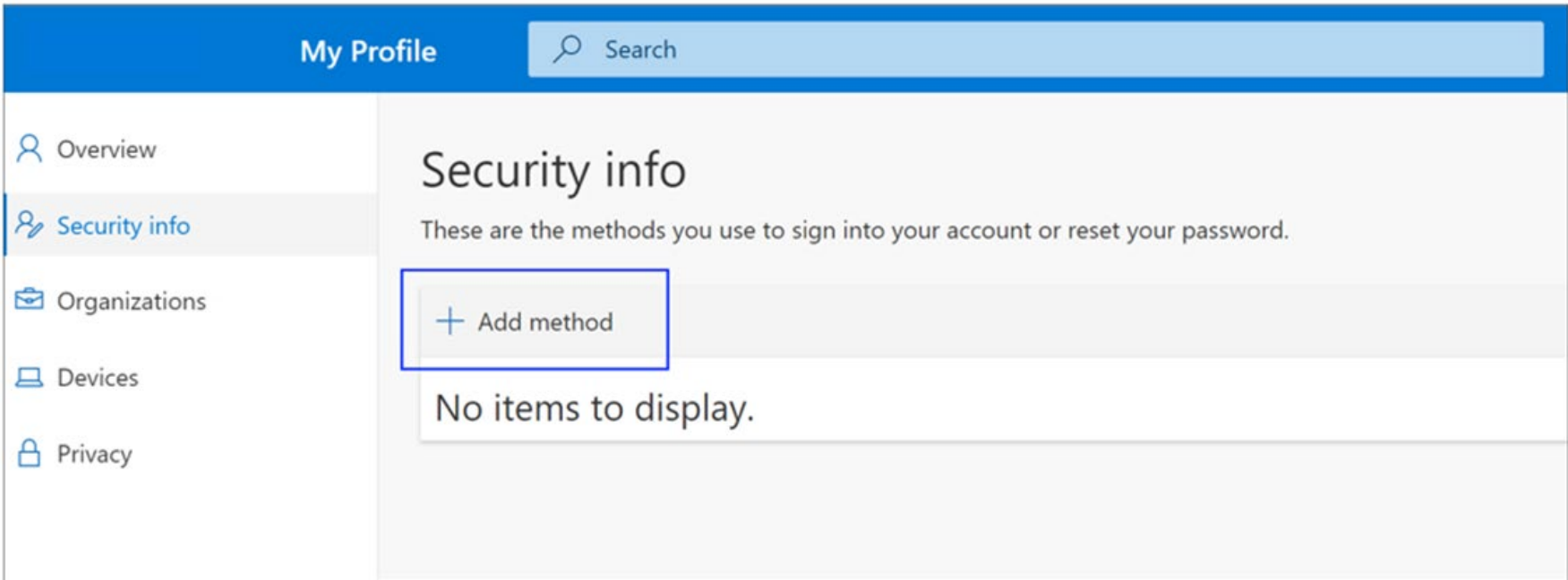
You can use an authentication app as one of your security info methods. To set up the Microsoft Authenticator app

1. Sign in to your work or school account and then go to your <https://myaccount.microsoft.com/> page.



Security Info Page

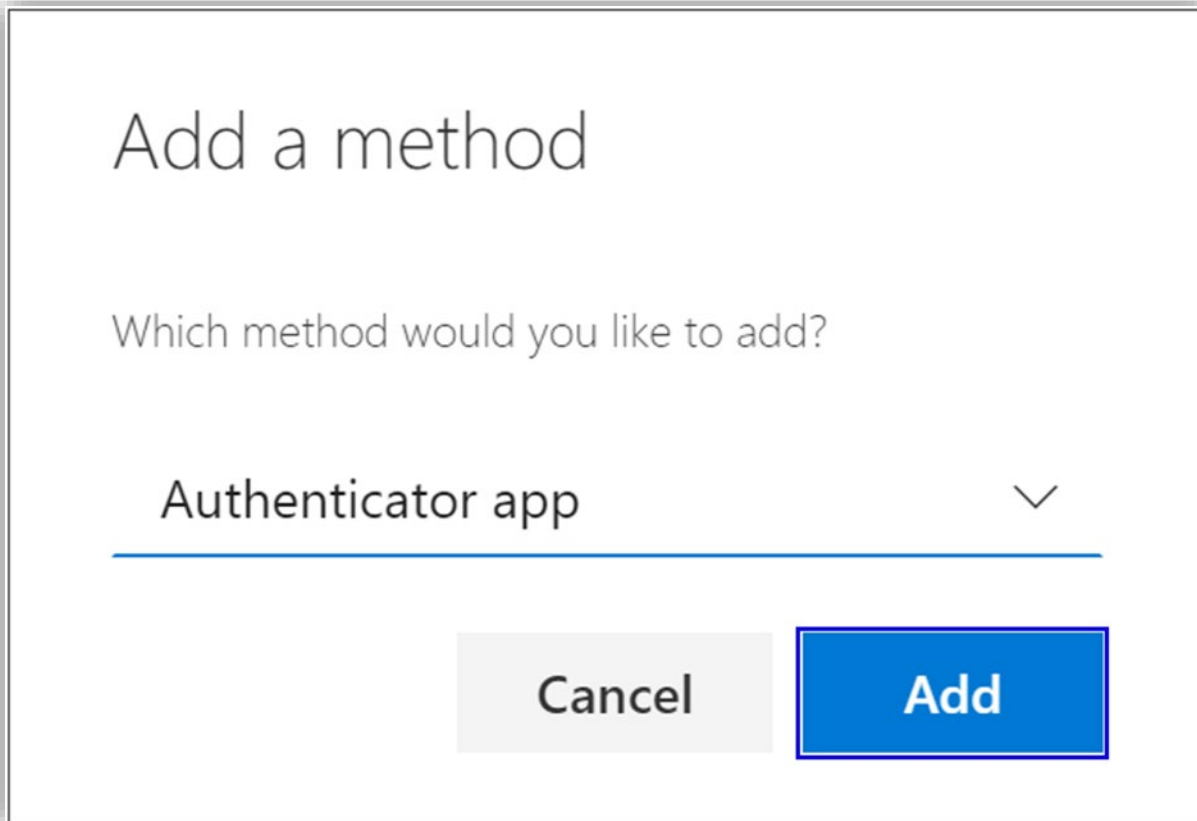
2. Select **Security info** from the left navigation pane or from the link in the **Security info** block, and then select **Add method** from the **Security info** page.



The screenshot shows the 'My Profile' page in a Microsoft account interface. The left navigation pane includes 'Overview', 'Security info', 'Organizations', 'Devices', and 'Privacy'. The 'Security info' section is active, displaying the title 'Security info' and the subtitle 'These are the methods you use to sign into your account or reset your password.' A blue box highlights the '+ Add method' button. Below this, a message states 'No items to display.'


Add A Method

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



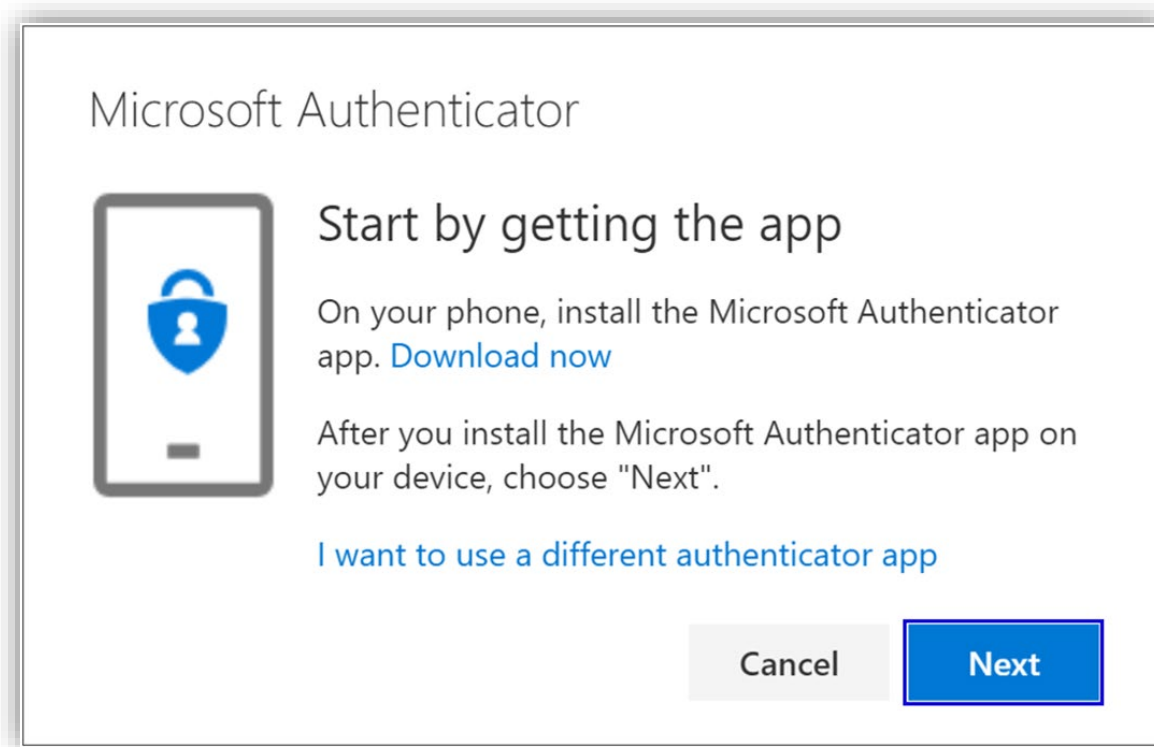
Add a method

Which method would you like to add?

Authenticator app 

Get The App

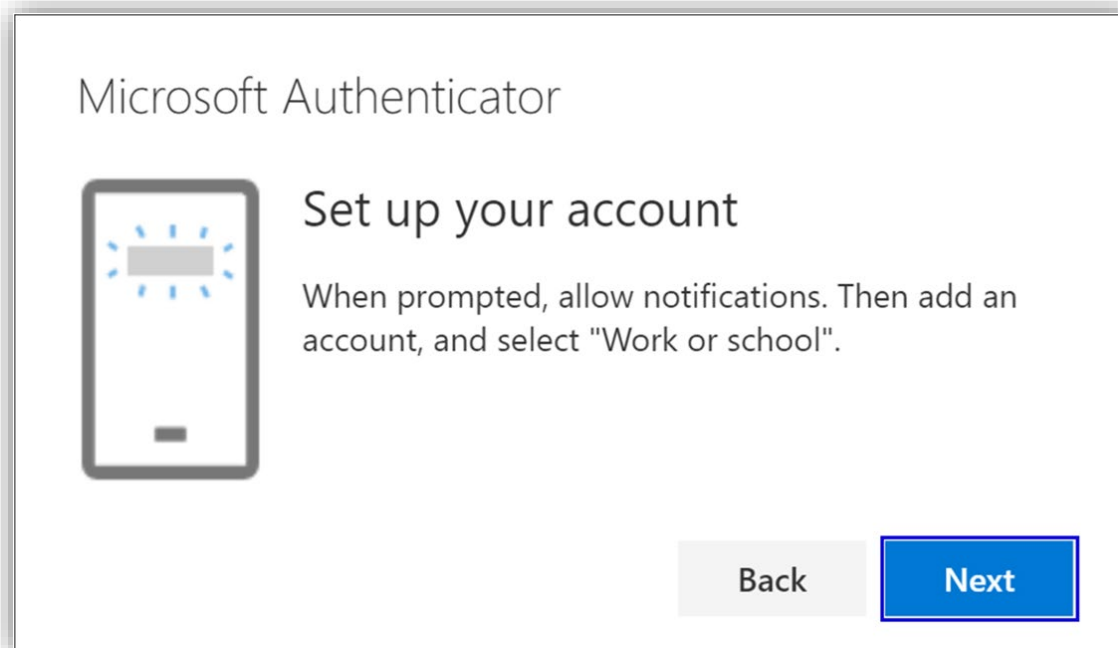
4. On the **Start by getting the app** page, select **Download now** to download and install the Microsoft Authenticator app on your mobile device, and then select **Next**.



For more information about how to download and install the app, see [Download and install the Microsoft Authenticator app](#) article of this document.

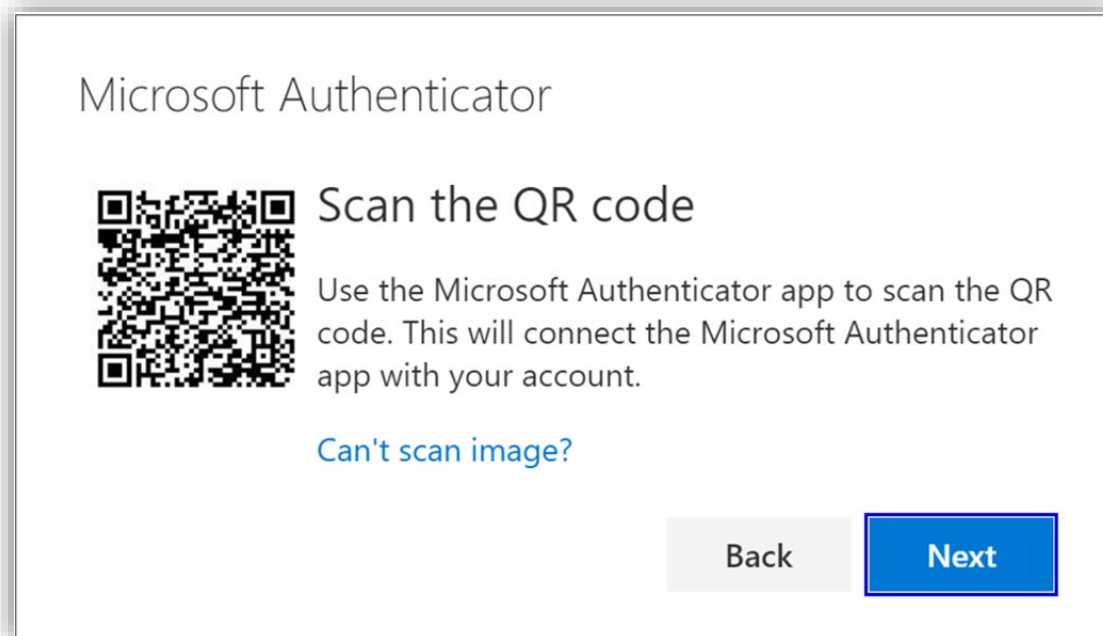
Set Up Your Account

5. Remain on the **Set up your account** page while you set up the Microsoft Authenticator app on your mobile device.
6. 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**.



Scan QR Code

7. Return to the **Set up your account** page on your computer, and then select **Next**. The **Scan the QR code** page appears.
8. 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 6.

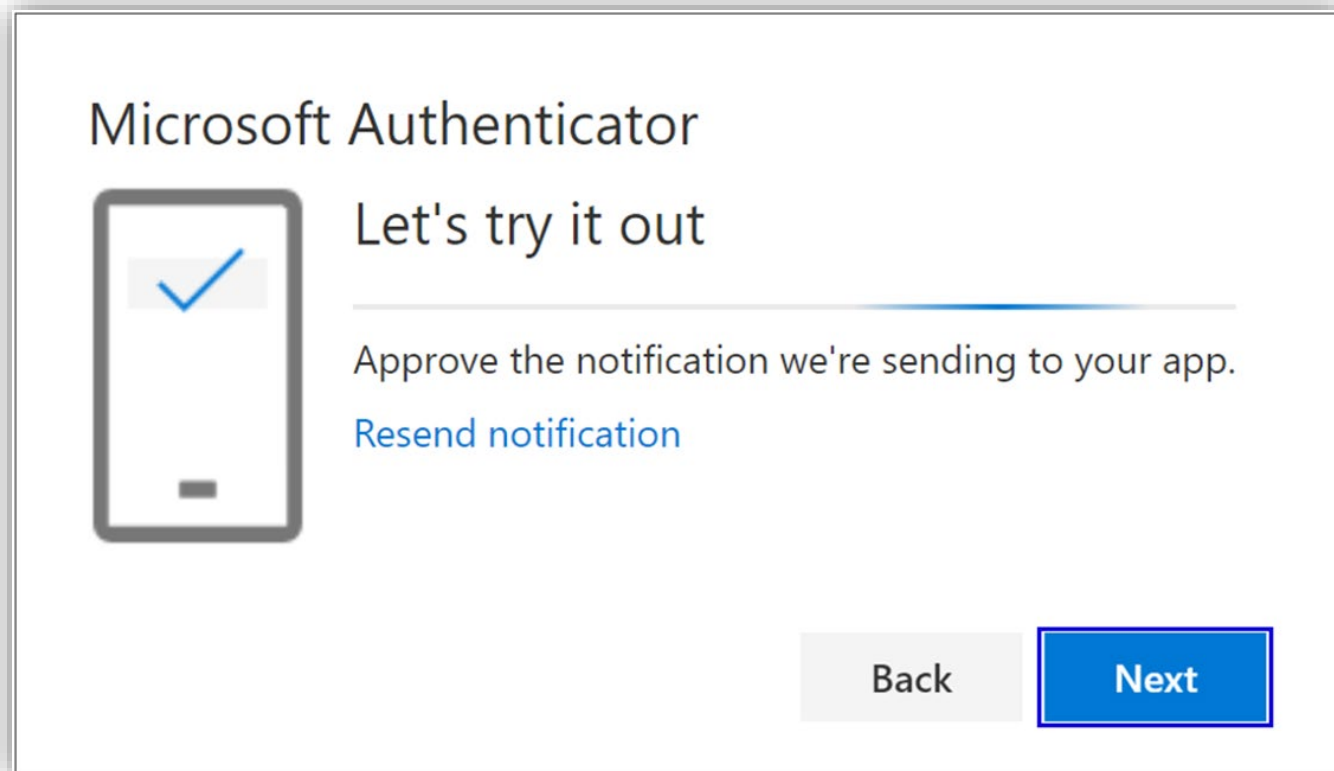


Notes:

- *iPhone users may have to enable the camera in Settings in order to scan.*
- *If you can't use your phone camera, you'll have to manually enter the 9-digit code and the URL. For more information about manually adding a code, see [Manually add an account to the app](#).*

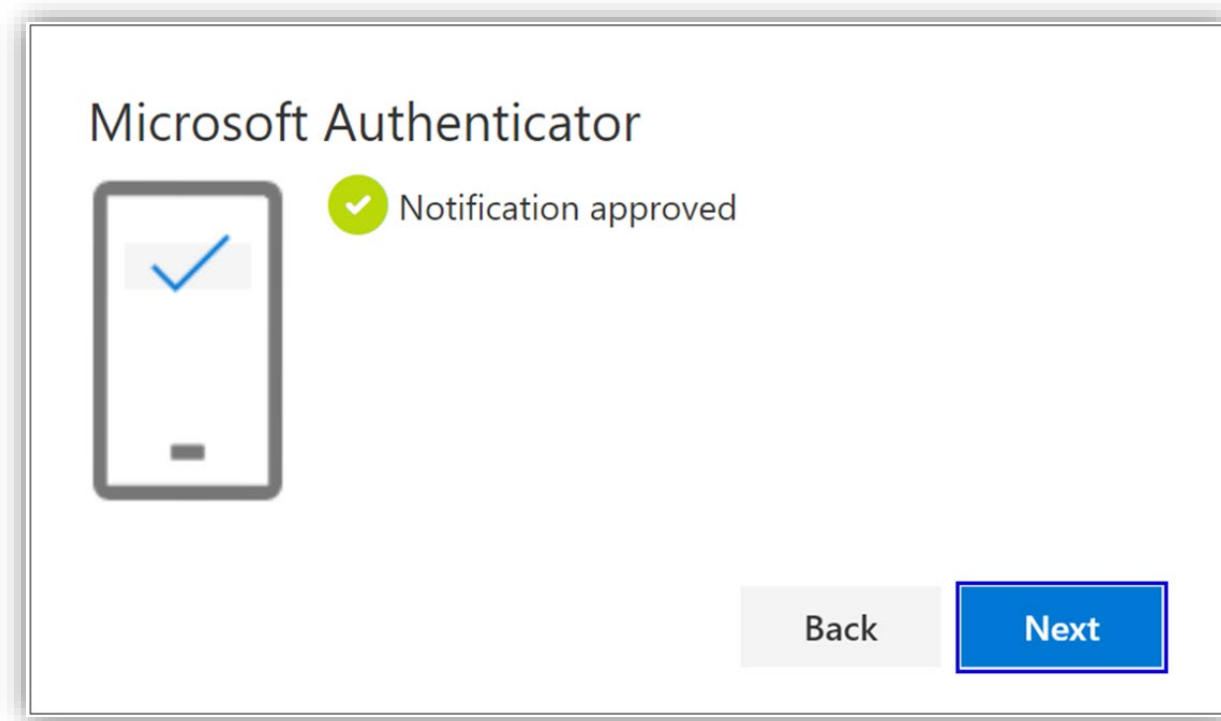
Try It Out

9. 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.



Notification Approved

10. 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 (2FV) or password reset.

Set up Authenticator App from your phone

Install the latest version of the Microsoft Authenticator app, based on your operating system:

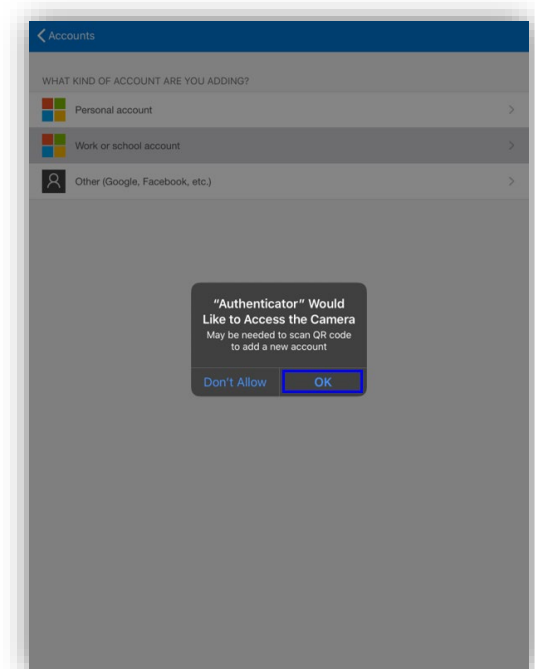
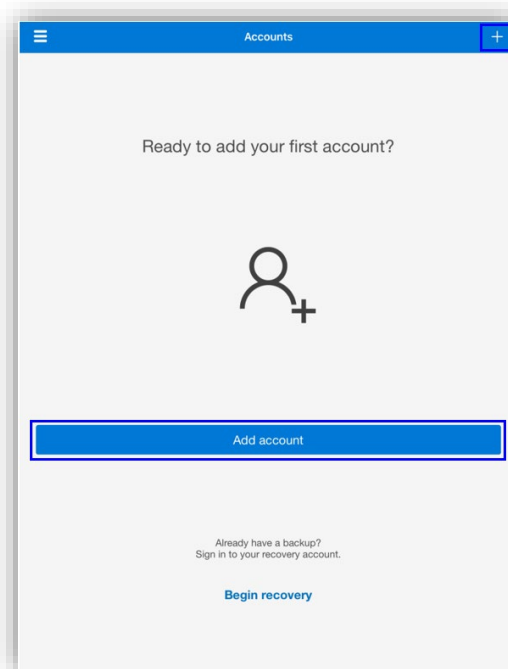
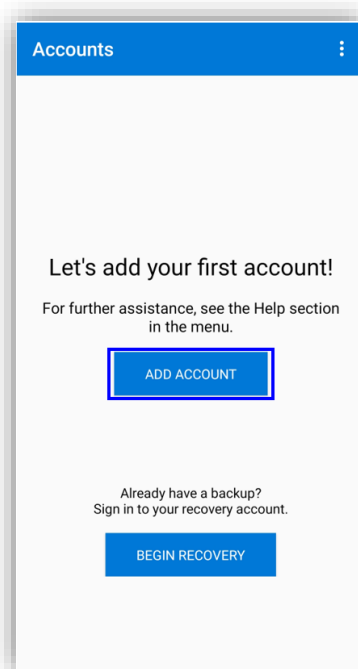
Google Android. On your Android device, go to Google Play to [download and install the Microsoft Authenticator app](#).

Apple iOS. On your Apple iOS device, go to the App Store to [download and install the Microsoft Authenticator app](#).

Important! *If you're not currently on your mobile device, you can still get the Microsoft Authenticator app by sending yourself a download link from the [Microsoft Authenticator page](#).*

Add account to Microsoft Authenticator

6. Open the Microsoft Authenticator app on your phone.
7. Tap the **+** > **Work or school account**.

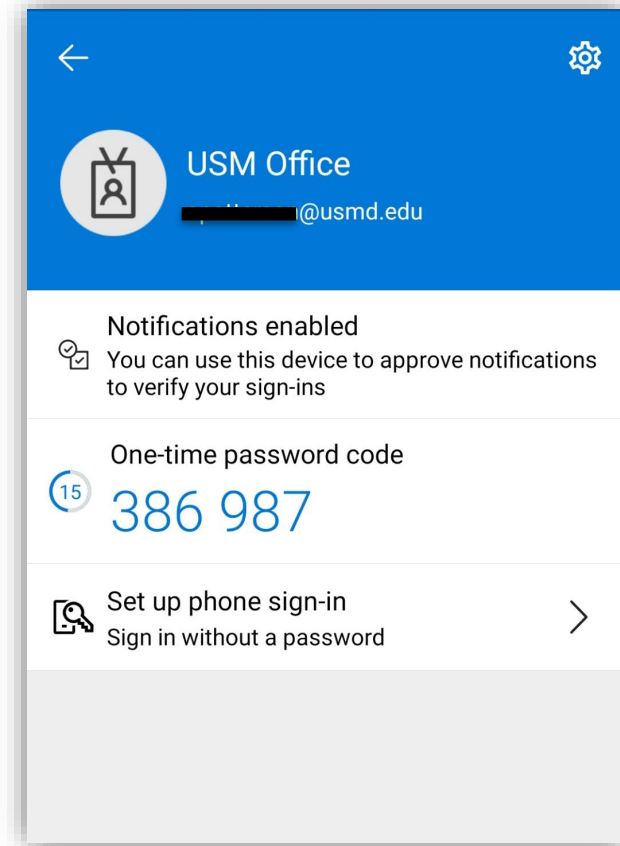
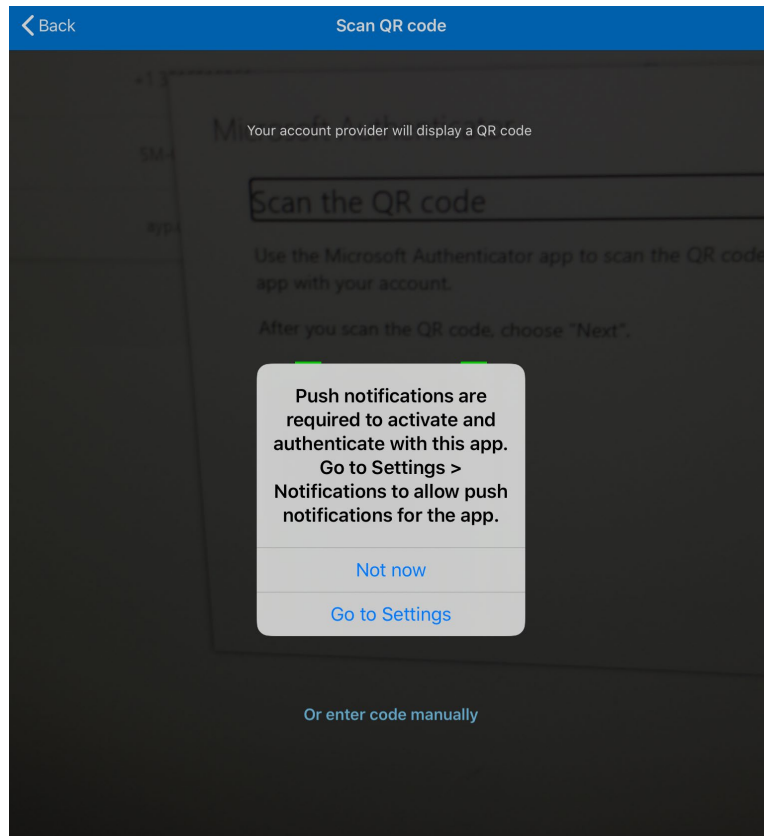


Notes:

- *iPhone users may have to enable the camera in Settings in order to scan.*
- *If you can't use your phone camera, you'll have to manually enter the 9-digit code and the URL.*

Add account to Microsoft Authenticator

- Your account will be added automatically to the app and will display a six-digit code.



Note: Push notifications are required to activate and authenticate with this app.

Confirm activation status on your computer

10. Switch back to your computer and click **Done**.
11. Now wait for the **Checking activation status** text to finish configuring your phone.
12. When it's complete, you'll be able to click the **Contact me** button on the right.

Additional security verification

Secure your account by adding phone verification to your password. [View video](#)

Step 1: How should we contact you?

Mobile app ▼

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

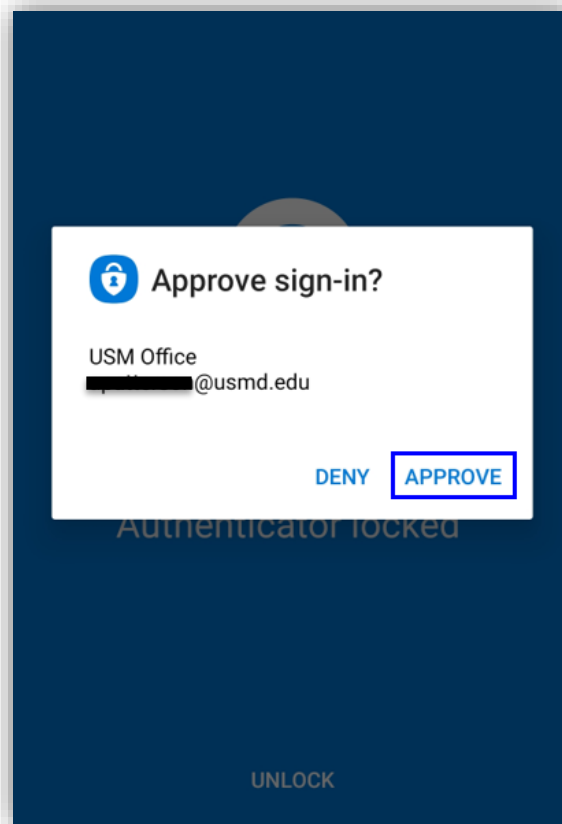
To use these verification methods, you must set up the Azure Authentication app.

Mobile app has been configured for notifications and verification codes.

Note: *If configuration fails, just delete retry the previous steps again.*

Approve sign in on your phone

13. Switch back to your phone and you'll see a notification for a new sign in.
14. Go to the Microsoft Authenticator app.
15. Tap **Approve** to allow it.



Finish set up

16. Back on the computer, follow any prompts that you might see such as adding a mobile number.
17. You're good to go!



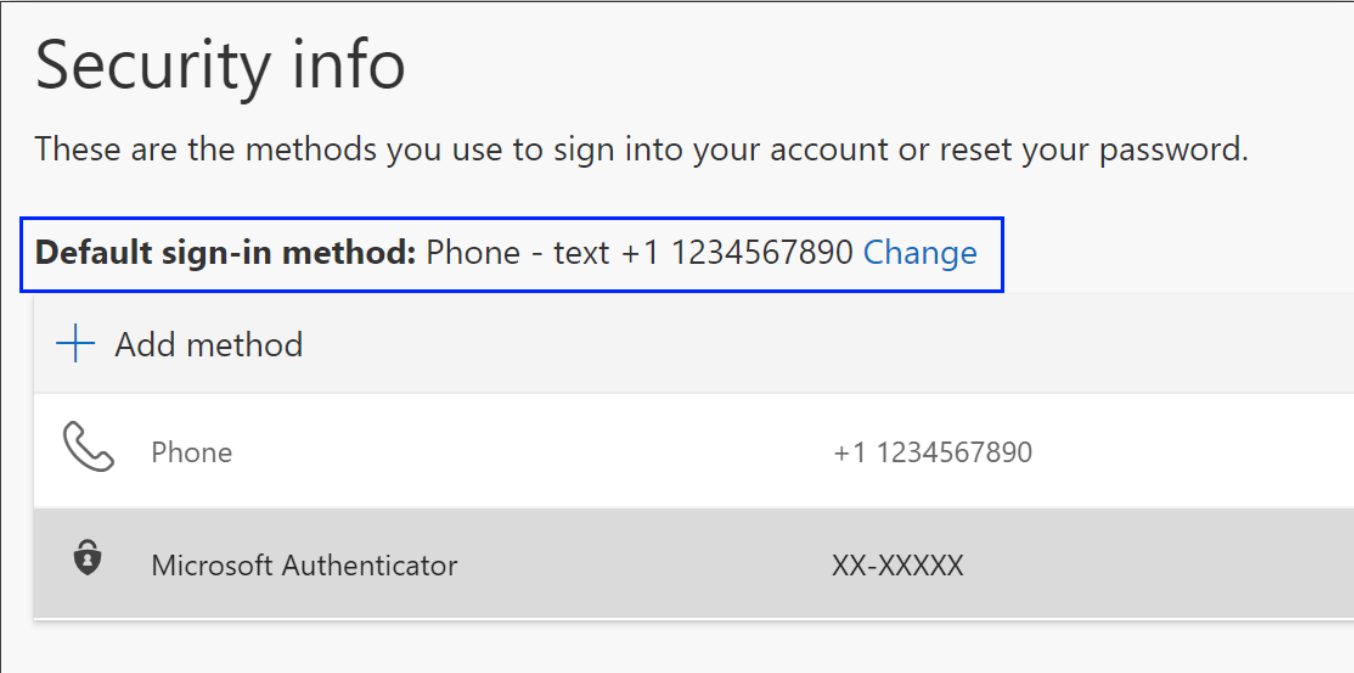
From now on, whenever you have a new sign in or add your Microsoft 365 work or school account to an app, you'll open the Authenticator app on your phone and tap **Approve**.

Change your default security info method



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 (2FV) 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.

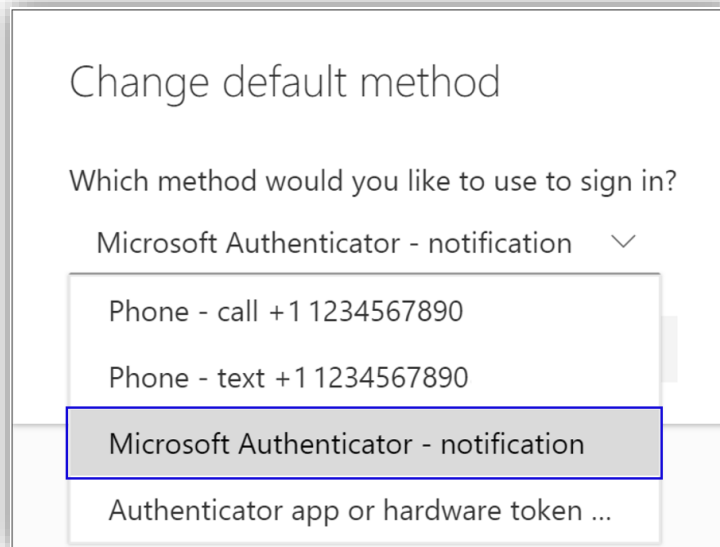


The screenshot shows the 'Security info' page. At the top, it says 'Security info' and 'These are the methods you use to sign into your account or reset your password.' Below this, there is a blue-bordered box containing the text 'Default sign-in method: Phone - text +1 1234567890 Change'. Underneath, there is a '+ Add method' button. Below that, there are two rows of security methods. The first row is 'Phone' with a phone icon and the number '+1 1234567890'. The second row is 'Microsoft Authenticator' with a shield icon and the text 'XX-XXXXX'.

Security info		
These are the methods you use to sign into your account or reset your password.		
Default sign-in method: Phone - text +1 1234567890 Change		
+ Add method		
	Phone	+1 1234567890
	Microsoft Authenticator	XX-XXXXX

Set up the Microsoft Authenticator app from the Security info page

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.
3. Select **Confirm**.



Change default method

Which method would you like to use to sign in?

Microsoft Authenticator - notification ▾

- Phone - call +1 1234567890
- Phone - text +1 1234567890
- Microsoft Authenticator - notification**
- Authenticator app or hardware token ...

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

Additional security info methods

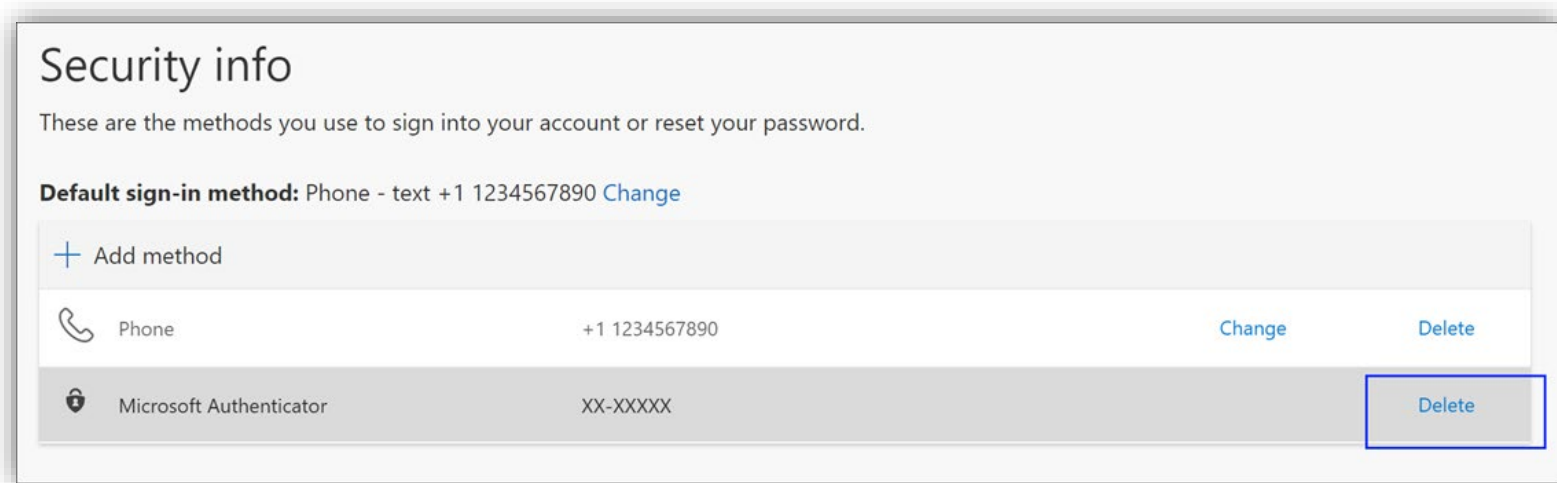
You have additional options for how your USM Office 365 account contacts you to verify your identity, based on what's you're trying to do. The options include:

- **Mobile device text.** Enter your mobile device number and get a text a code you'll use for two-step verification (2FV) or password reset. For step-by-step instructions about how to verify your identity with a text message (SMS), see [Set up security info to use text messaging \(SMS\)](#).
- **Mobile device or work phone call.** Enter your mobile device number and get a phone call for two-step verification (2FV) or password reset. For step-by-step instructions about how to verify your identity with a phone number, see [Set up security info to use phone calls](#).
- **Security key.** Register your Microsoft-compatible security key and use it along with a PIN for two-step verification (2FV) or password reset. For step-by-step instructions about how to verify your identity with a security key, see [Set up security info to use a security key](#).
- **Email address.** Enter your work or school email address to get an email for password reset. This option isn't available for two-step verification (2FV). For step-by-step instructions about how to set up your email, see [Set up security info to use email](#).
- **Security questions.** Answer some security questions created by your administrator for your organization. This option is only available for password reset and not for two-step verification (2FV). For step-by-step instructions about how to set up your security questions, see the [Set up security info to use security questions](#) article

Delete the authenticator app

If you haven't setup MFA, you can do the following to register for both:

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 (2FV) and password reset requests.

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.

If you have any further questions, concerns or need assistance with the Microsoft Authenticator App, please contact the USM-IT Dept. at geeks@usmd.edu



UNIVERSITY SYSTEM
of MARYLAND