Set up the Microsoft Authenticator app as your verification method

You can follow these steps to add your two-factor verification 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.

If what you're seeing on your screen doesn't match what's being covered in this article, it means that your administrator hasn't turned on this experience yet. Until this experience is turned on, you must follow the instructions and information in the **Set up my account for the two-step verification** section.

Note: If you don't see the authenticator app option, it's possible that your organization doesn't allow you to use this option for verification. In this case, you'll need to choose another method or contact your organization's help desk for more assistance.

Security versus password reset verification

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

Method	**Used for**
Authenticator app	Two-factor verification and password reset authentication.
Text messages	Two-factor verification and password reset authentication.
Phone calls	Two-factor verification and password reset authentication.
Security key	Two-factor verification and password reset authentication.
Email account	Password reset authentication only. You'll need to choose a different method for two-factor verification.

Security questions	Password reset authentication only. You'll need to choose a different method for two-factor verification.

Set up the Microsoft Authenticator app from the Security info page

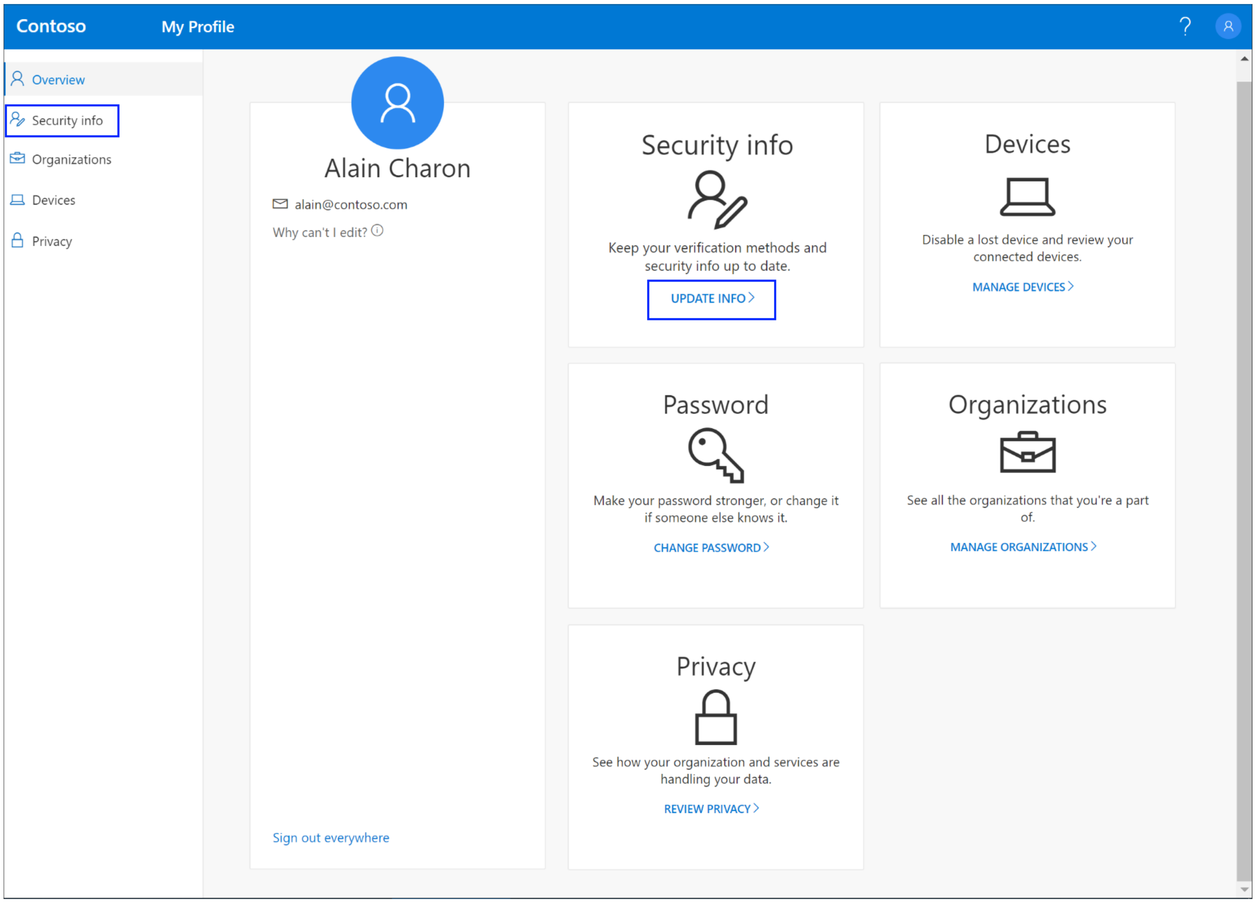
Depending on your organization’s settings, you might be able to use an authentication app as one of your security info methods. You aren't required to use the Microsoft Authenticator app, and you can choose a different app during the setup process. However, this article uses the Microsoft Authenticator app.

Important:

- If you have set up the Microsoft Authenticator app on five different devices or if you've used five hardware tokens, you won't be able to set up a sixth one, and you might see the following error message:
- `You can't set up Microsoft Authenticator because you already have five authenticator apps or hardware tokens. Please contact your administrator to delete one of your authenticator apps or hardware tokens.`

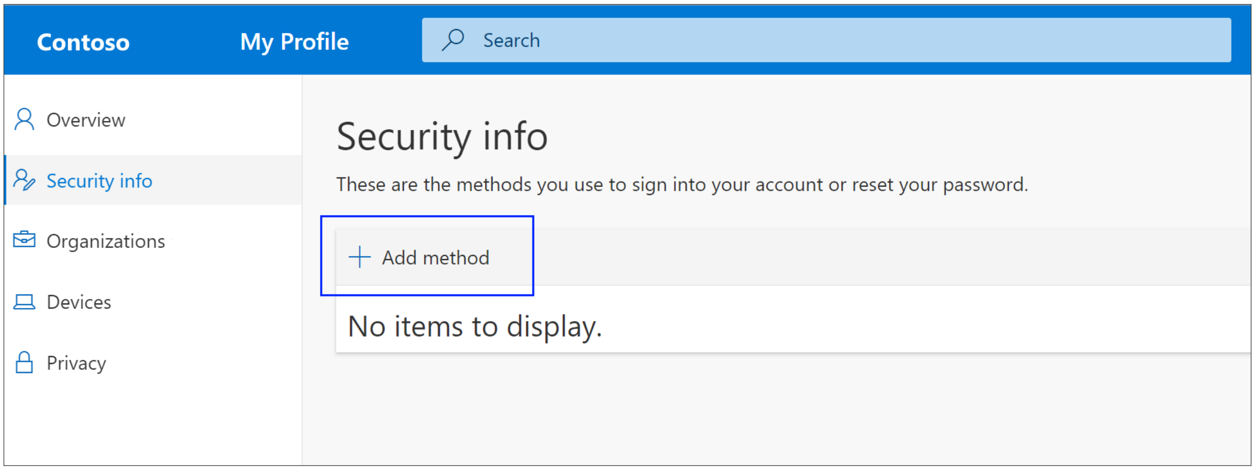
To set up the Microsoft Authenticator app

1. Sign in to your work or school account and then go to your My Account portal.

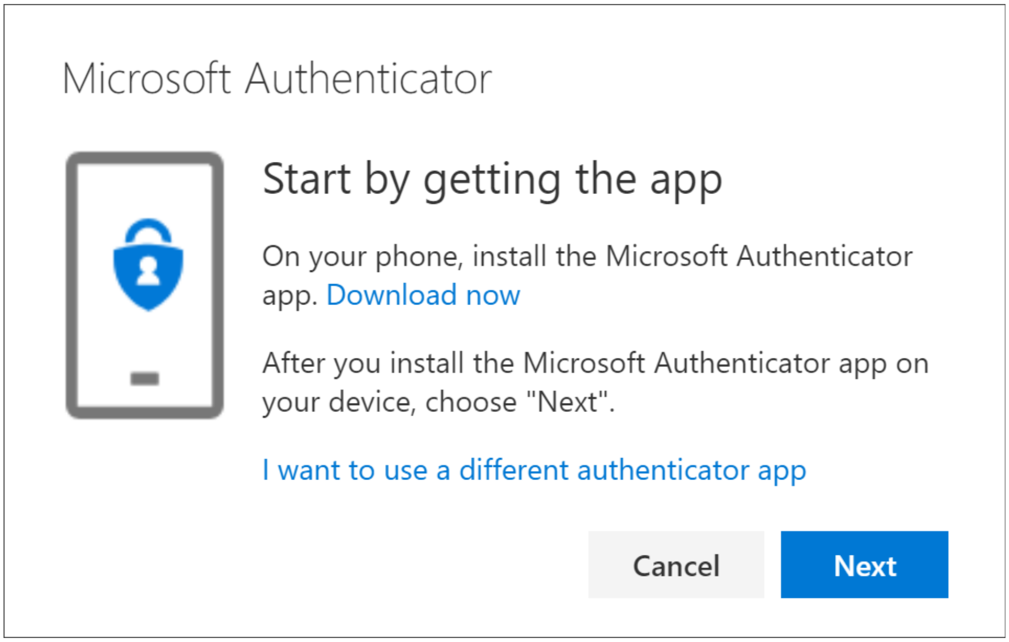


Contoso
My Profile
?
Overview
Security info
Organizations
Devices
Privacy
Alain Charon
alain@contoso.com
Why can't I edit?
Sign out everywhere
Security info
Keep your verification methods and security info up to date.
UPDATE INFO >
Devices
Disable a lost device and review your connected devices.
MANAGE DEVICES >
Password
Make your password stronger, or change it if someone else knows it.
CHANGE PASSWORD >
Organizations
See all the organizations that you're a part of.
MANAGE ORGANIZATIONS >
Privacy
See how your organization and services are handling your data.
REVIEW PRIVACY >

2. Select **Security info** in the left menu or by using the link in the **Security info** pane. If you have already registered, you'll be prompted for two-factor verification. Then, select **Add method** in the **Security info** pane.



3. On the **Add a method** page, select **Authenticator app** from the list, and then select **Add**.
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.
    - If you want to use an authenticator app other than the Microsoft Authenticator app, select **I want to use a different authenticator app**.
    - If your organization lets you choose a different method besides the authenticator app, you can select **I want to set up a different method**.



Microsoft Authenticator

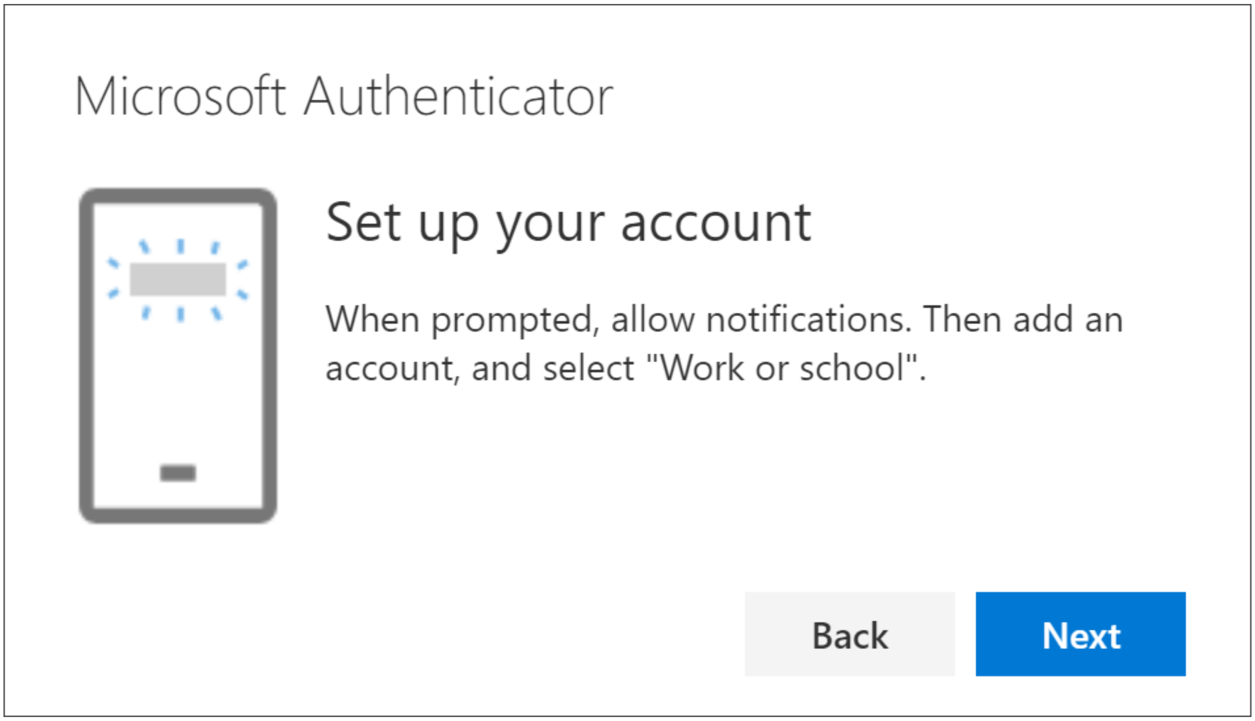
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

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



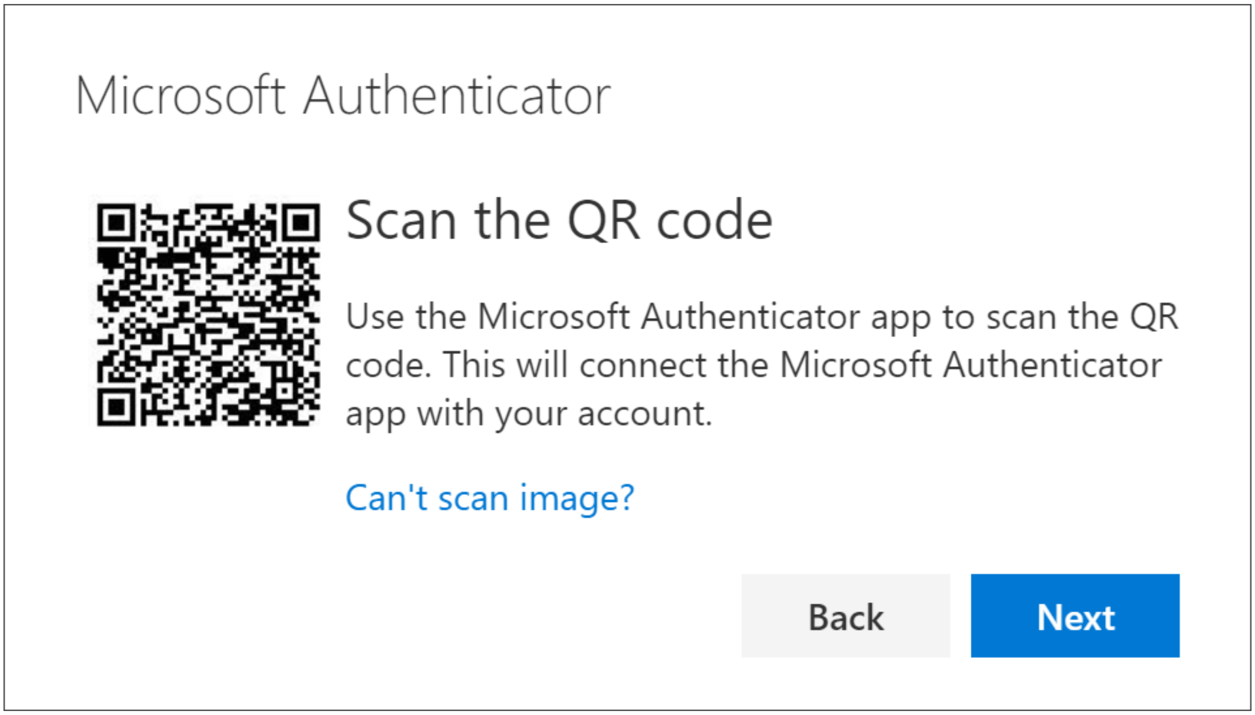
Microsoft Authenticator

Set up your account

When prompted, allow notifications. Then add an account, and select "Work or school".

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.

   Note: The first time you set 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. If you don't allow the camera, you can still set up the authenticator app, but you'll need to add the code information manually. For information about how to add the code manually, see see Manually add an account to the app.
7. Return to the **Set up your account** page on your computer, and then select **Next**. The Scan the QR code page appears.



Microsoft Authenticator

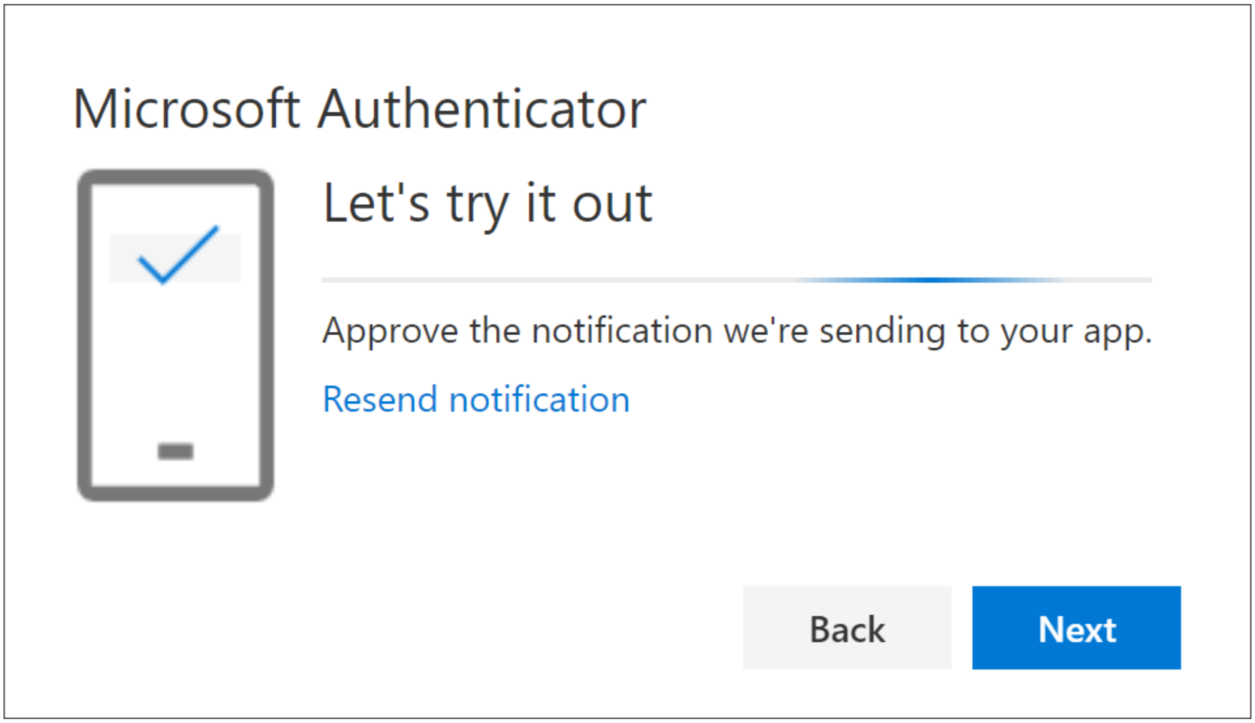
Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

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.
9. 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 **Can't scan the QR code** 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.

10. 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.



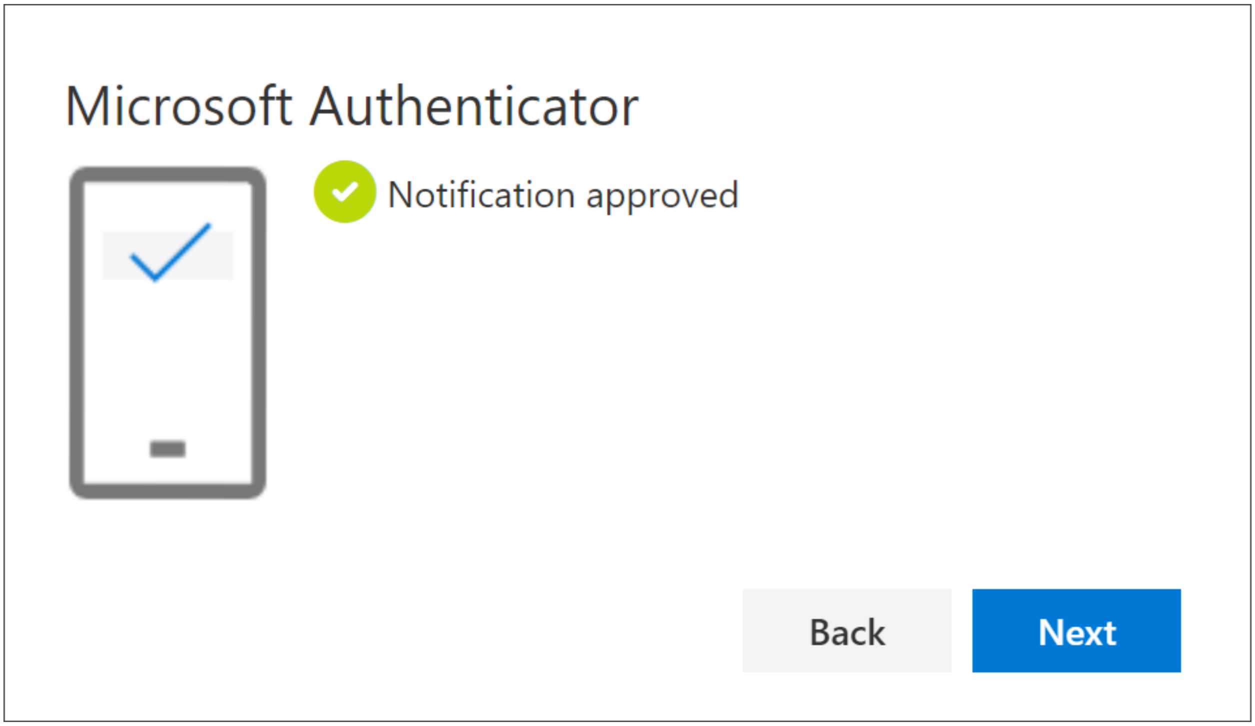
Microsoft Authenticator

Let's try it out

Approve the notification we're sending to your app.

Resend notification

11. 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.



Microsoft Authenticator

Notification approved

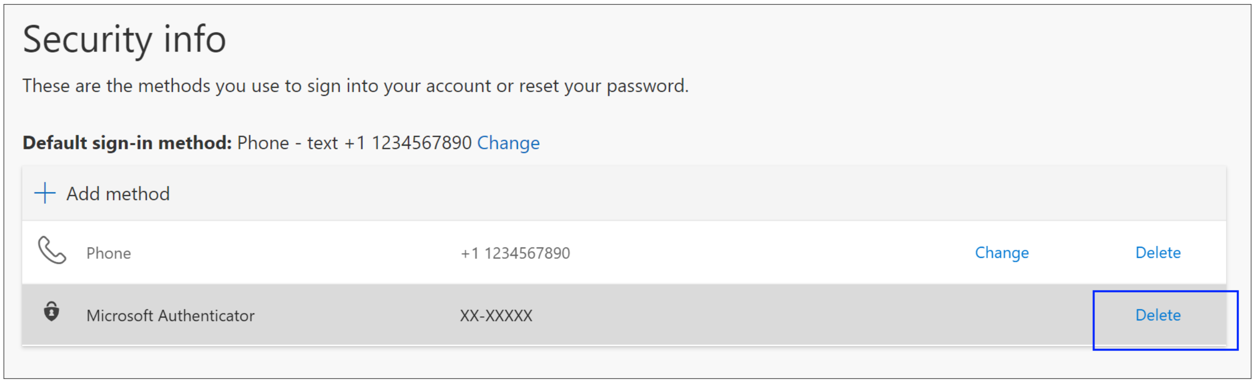
Delete your authenticator app from your security info methods

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 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.



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

Phone	+1 1234567890	Change	Delete
Microsoft Authenticator	XX-XXXXX		Delete

2. Select **Yes** when asked to confirm 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 changes 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.
4. Your account is completely removed from the authenticator app for two-factor verification and password reset requests.

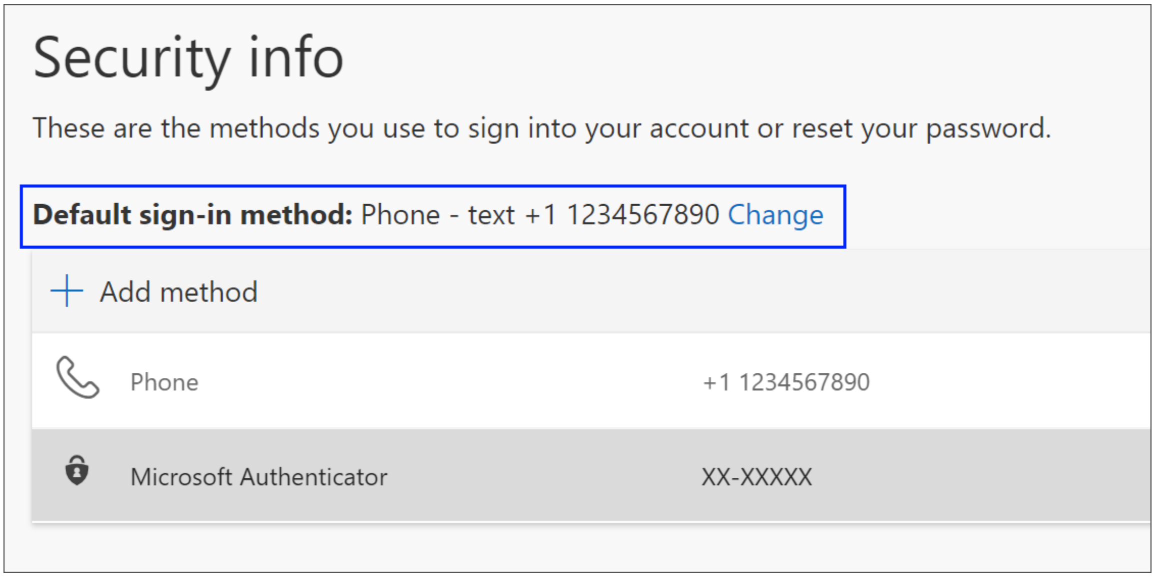
Change your default security info method

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 or for password reset requests, you can set it from the Security info page.

Note: If your default sign-in method is a text or call to your phone number, then the SMS code or voice call is sent automatically during multifactor authentication. As of June 2021, some apps will ask users to choose **Text** or **Call** first. This option prevents sending too many security codes for different apps. If your default sign-in method is the Microsoft Authenticator app (which Microsoft recommends), then the app notification is sent automatically.

To change your default security info method

1. On the **Security info** page, select **Change** next to the **Default sign-in method** information.



Security info

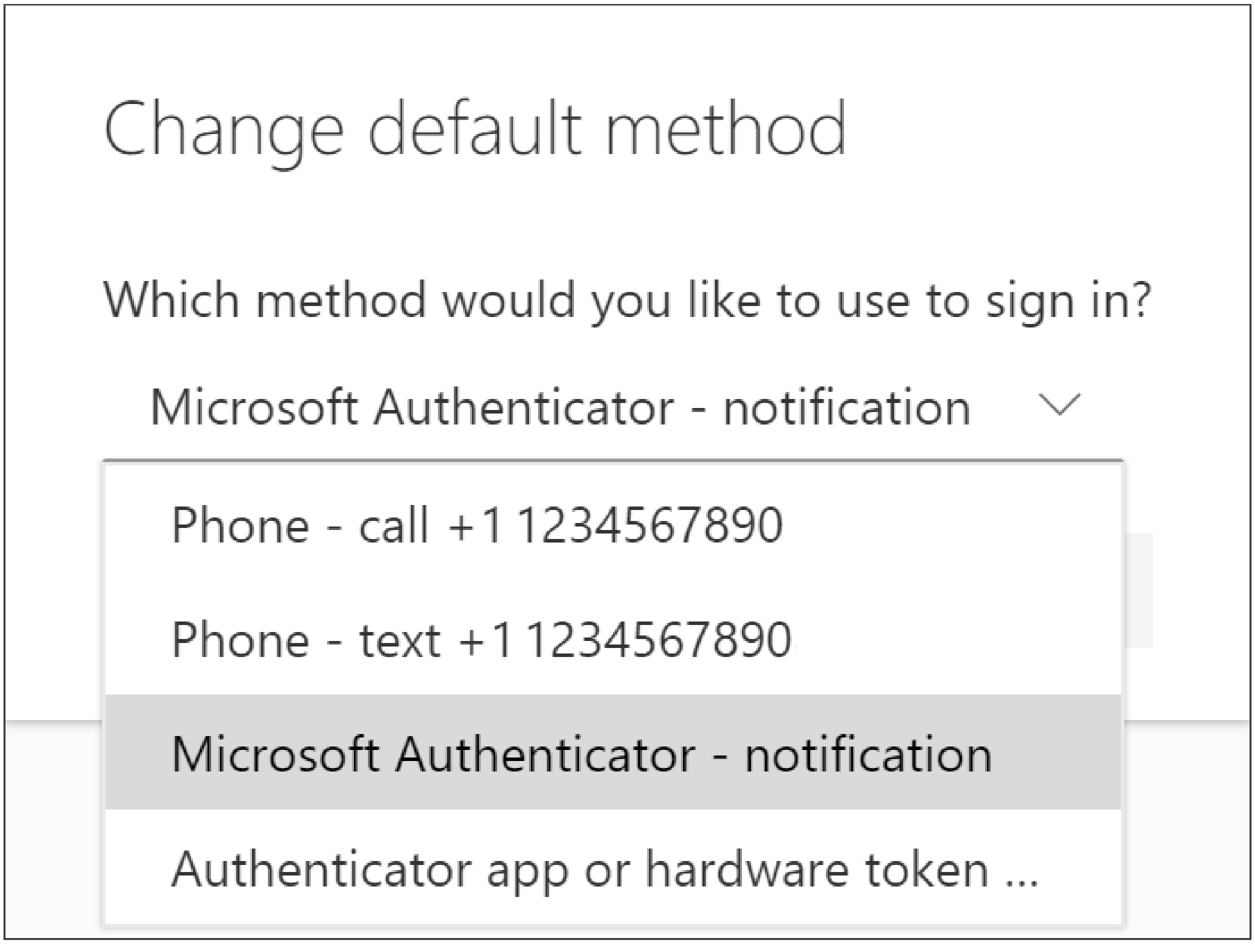
These are the methods you use to sign into your account or reset your password.

Default sign-in method: Phone - text +1 1234567890 Change

+ Add method

☎ Phone	+1 1234567890
Microsoft Authenticator	XX-XXXXX

2. Choose **Microsoft Authenticator - notification** from the list of available methods. If you're not using the Microsoft Authenticator app, select the **Authenticator app or hardware token** option.



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 ...

3. Select **Confirm**. The default method used for sign-in changes to the Microsoft Authenticator app.

Additional security info methods

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

- Mobile device text: Enter your mobile device number and get a text code you'll use for two-step verification 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 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 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. 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. For step-by-step instructions about how to set up your security questions, see the Set up security info to use security questions article.

Note: If some of these options are missing, it's most likely because your organization doesn't allow those methods. If this is the case, you'll need to choose an available method or contact your administrator for more help.

How to use the Microsoft Authenticator app

Microsoft account dashboard

With this free app, you can sign in to your personal or work/school Microsoft account without using a password. You'll use a fingerprint, face recognition, or a PIN for security.

Why use the Microsoft Authenticator app?

1. The authenticator app is a secure and convenient way to prove who you are.
2. You can use the Authenticator app as a way to sign in if you forget your password.
3. You can use the app to back up and restore all your other account credentials.
4. You can also use the Microsoft Authenticator to sign in to your non-Microsoft accounts.

How to set up the Microsoft Authenticator app

1. Download & install the Microsoft Authenticator app to your mobile device.
2. Sign in to your account security dashboard.
3. Select **Add a new way to sign in or verify** and choose **Use an app**.
4. If you've already installed the app, select **Next** to display a QR code appears on the screen.
5. In the authenticator app, select [three dots] then **+ Add account**.
6. Choose the account type and select Scan a QR code.
7. Scan the code shown on the screen in step 4.
8. Select **Finish** on the PC to complete the setup.

Using Authenticator account backup and restore

The Microsoft Authenticator app backs up your account credentials and related app settings, such as the order of your accounts, to the cloud.

Important:

- You need a personal Microsoft account to act as your recovery account.
- iOS users must also have an iCloud account.

Turn on cloud backup:

1. Select **Settings** > **Backup** and then turn on **Cloud** or **iCloud backup**.

To recover your information:

1. Open the Microsoft Authenticator app on your mobile device and select **Begin recovery**.
2. Sign in to your recovery account using the personal Microsoft account you used during the backup process. Your account credentials are recovered to the new device.