

## Download and install the Microsoft Authenticator app

### Download and install the app

1. Install the latest version of the Authenticator app, based on your operating system:
2. Google Android. On your Android device, go to Google Play to [download and install the Authenticator app](#).
3. Apple iOS. On your Apple iOS device, go to the App Store to [download and install the Authenticator app](#).

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

Set up two step verification on Authenticator.

To secure your account, the Authenticator app can provide you with a code you provide additional verification to sign in. No need to wait for texts or calls. The following instructions ensure only you can access your information.

Install the Authenticator app

To install the Authenticator app on an Android device, scan the QR code below or [open the download page from your mobile device](#).



2. To install the Authenticator app on For iOS, scan the QR code below or [open the download page from your mobile device](#).



## Set up the Authenticator app

After you install the Authenticator app, follow the steps below to add your account:

1. Open the Authenticator app.
2. Select (+) in the upper right corner.
3. Point your camera at the QR code or follow the instructions provided in your account settings.

After your account appears in your Authenticator app, you can use the one-time codes to sign in. For more information and support on the Authenticator App, open the [Download Microsoft Authenticator](#) page.

### Next steps

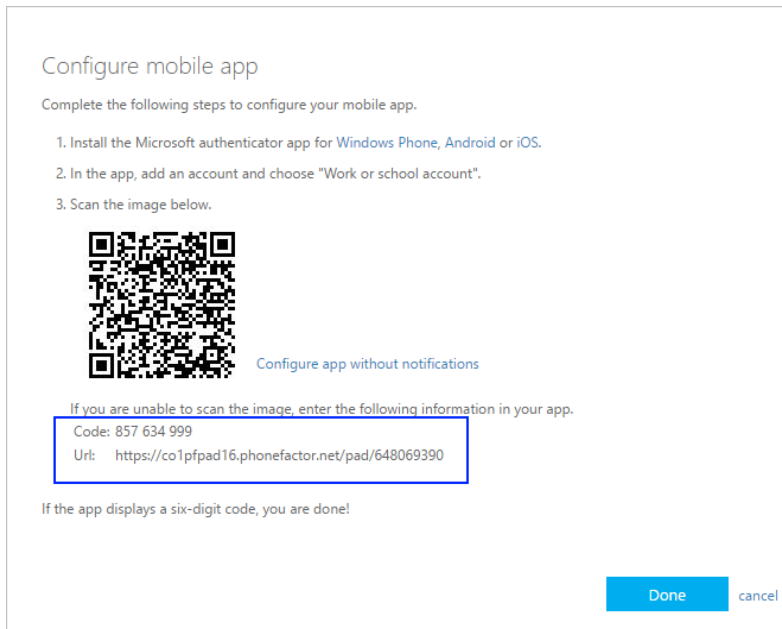
[Set up security info to use text messaging \(SMS\)](#). Enter your mobile device number and get a text a code you'll use for two-step verification or password reset.

[Set up security info to use phone calls](#). Enter your mobile device number and get a phone call for two-step verification or password reset.

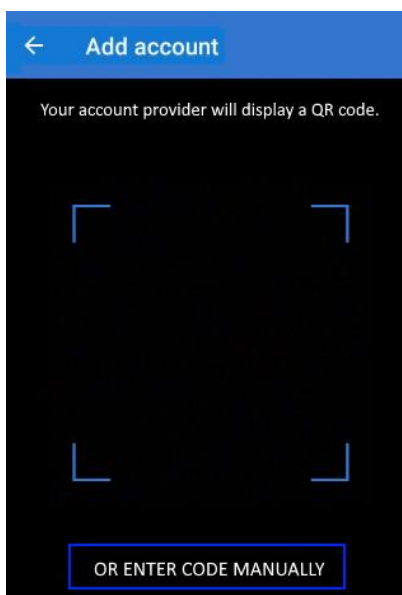


## Add your work account.

1. On your computer, note the **Code and Url** information on the **Configure mobile app** page. Keep this page open so you can see the code and URL.



2. Open the Authenticator app, select **Add account** from the **Customize and control** icon in the upper-right, and then select **Work or school account**.
3. Select **OR ENTER CODE MANUALLY**.



4. Enter the Code and URL from Step 1, and then select **Finish**.



- The **Accounts** screen of the app shows you your account name and a verification code. For additional security, the verification code changes every 30 seconds preventing someone from using a code multiple times.

## Set up the Microsoft Authenticator app from the Security info page.

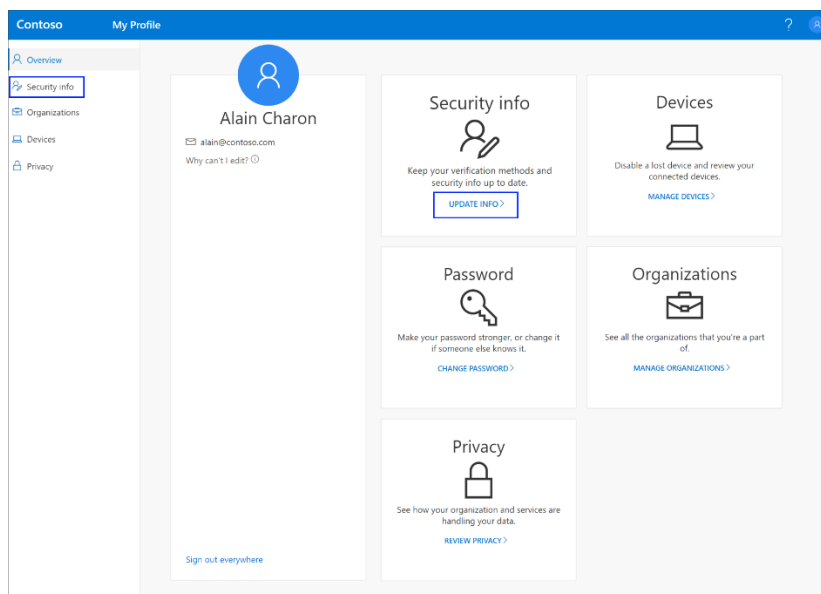
Depending on your organization's settings, you might be able to use an authentication app as one of your security info methods. You aren't required to use the Microsoft Authenticator app, and you can choose a different app during the set-up process. However, this article uses the Microsoft Authenticator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

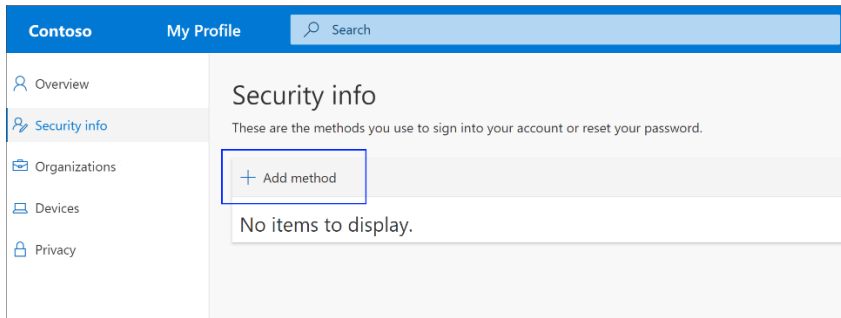
To set up the Microsoft Authenticator app

- Sign in to your work or school account and then go to your [My Account portal](#).

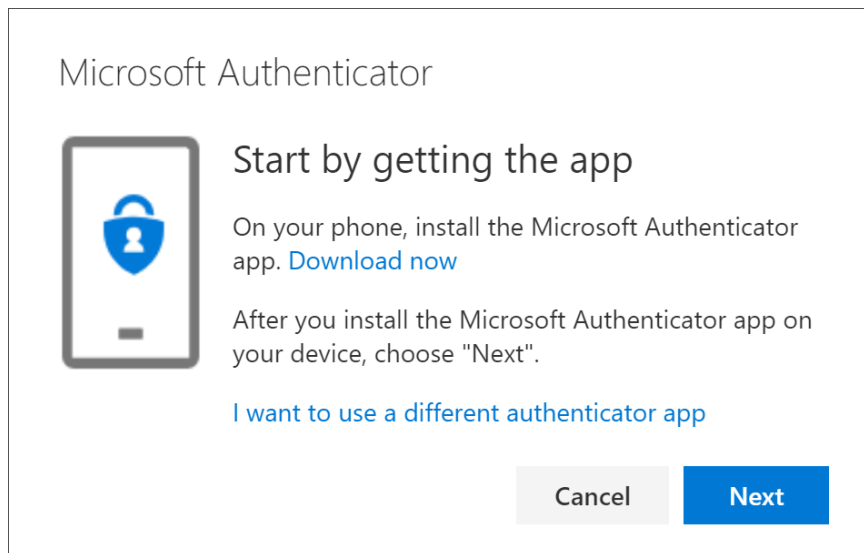


- Select **Security info** in the left menu or by using the link in the **Security info** pane. If you have already registered, you'll be prompted for two-factor verification. Then, select **Add method** in the **Security info** pane.



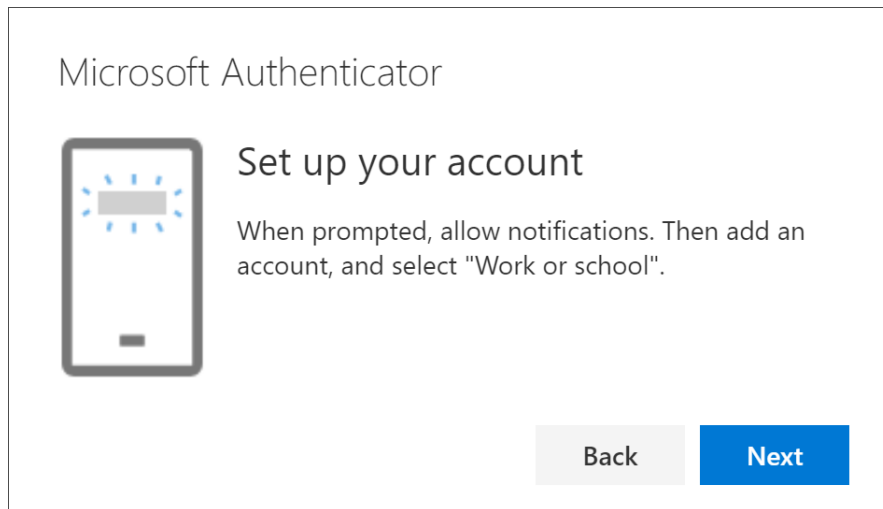


3. On the **Add a method** page, select **Authenticator app** from the list, and then select **Add**.
4. On the **Start by getting the app** page, select **Download now** to download and install the Microsoft Authenticator app on your mobile device, and then select **Next**. For more information about 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**.



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

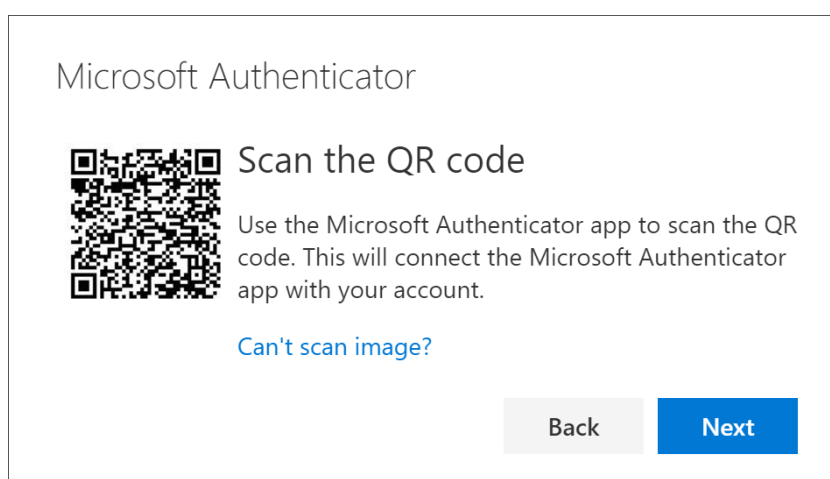




6. Open the Microsoft Authenticator app, select to allow notifications (if prompted), select **Add account** from the **Customize and control** icon on the upper-right, and then select Work or school account.

**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 [Manually add an account to the app](#).

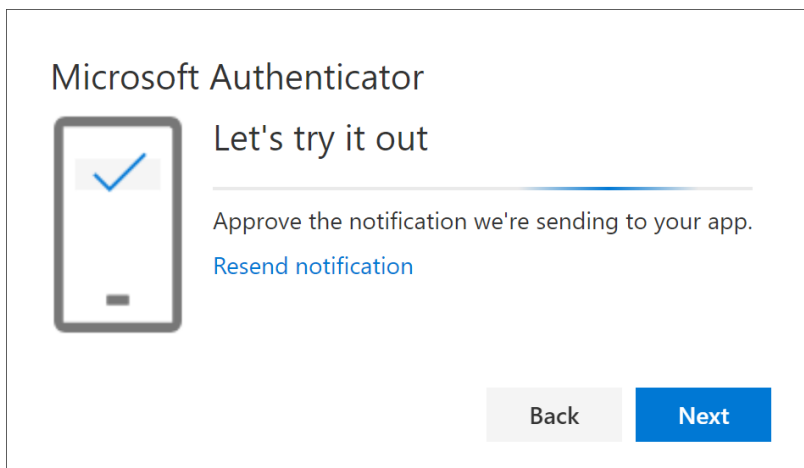
7. Return to the **Set up your account** page on your computer, and then select **Next**. The Scan the QR code page appears.



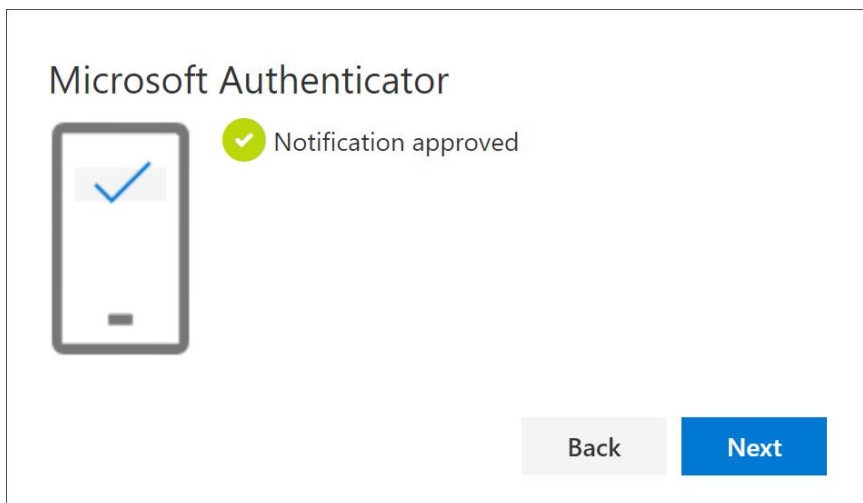
8. Scan the provided code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your work or school account in Step 6.



- 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](#).
- 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.



- 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.



Delete your authenticator app from your security info methods.

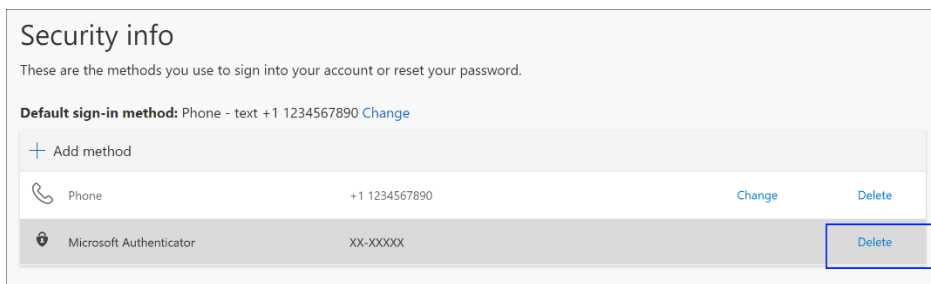
If you no longer want to use your authenticator app as a security info method, you can remove it from the **Security info** page. This works for all authenticator apps, not just the Microsoft

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.



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.

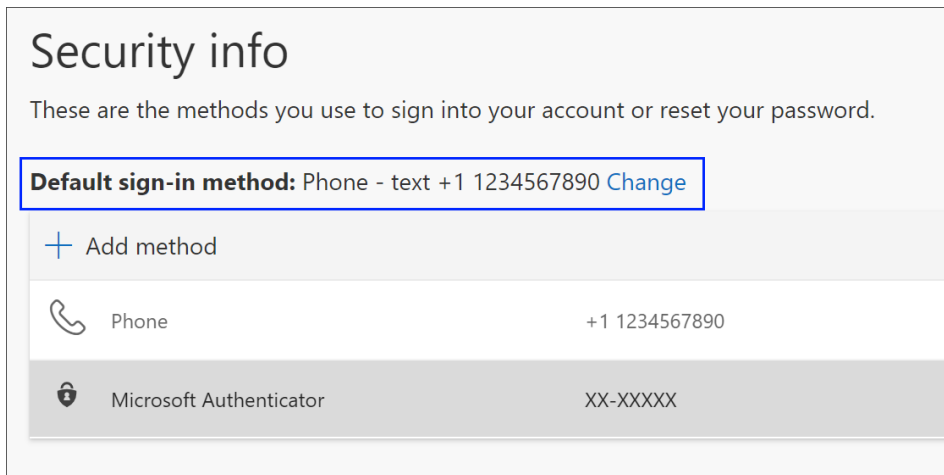
**Note:** If your default sign-in method is a text or call to your phone number, then the SMS code or voice call is sent automatically during multifactor authentication. As of June 2021, some apps will ask users to choose **Text** or **Call** first. This option prevents sending too many security codes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

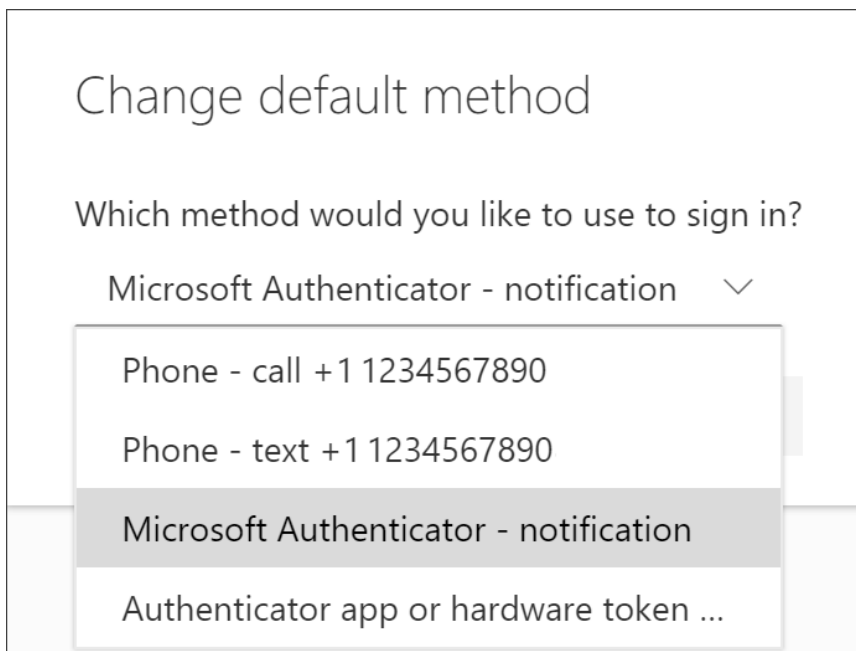
These are the methods you use to sign into your account or reset your password.

**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.



**For Assistance:**

1. Support email :

[Sc-it@sedcocal.com](mailto:Sc-it@sedcocal.com)

2. Important Contact Details:

Name	Landline	Mobile
Mohamed ElHakim	690 6511	050 107 7794
Lujain Qassim	690 6874	054 851 8898

