

Follow these steps if you are prompted to set up your security info immediately after you sign-in to your Alliant account.

You will only see this prompt if you have not set up the security info required by Alliant. If you've previously set up your security info, but you want to make changes, you can follow the steps in the various method-based how-to articles. For more information, see [Add or update your security info overview](#).

Sign into your Alliant account

After you sign into your Alliant account, you will see a prompt that asks you to provide more information before it lets you access your account.



mfatest@alliant.edu

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)

Set up your security info using the wizard

Follow these steps to set up your security info for your Alliant account from the prompt.

This is only an example of the process. The type and number of methods available or required for two-factor verification can vary if you are a student or an employee. You will be required to setup at least one of the verification methods that supports that functionality (Authenticator App, text messages and phone calls). If your role does not require two-factor verification, you may also have access to setup the methods (email and security questions) which can only be used for self-service password reset.

In this example, we're showing the steps required to configure the Microsoft Authenticator app and a mobile phone number for text messages.

1. After you select **Next** from the prompt, a “**Keep your account secure**” wizard appears, showing the first method available for you to set up. For this example, it's the Microsoft Authenticator app.

*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 use a different method besides the authenticator app, you can select the “**I want to set up a different method**” link.*

Keep your account secure

Your organization requires you to set up some methods of proving who you are.

1 App 2 Phone

Microsoft Authenticator



Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

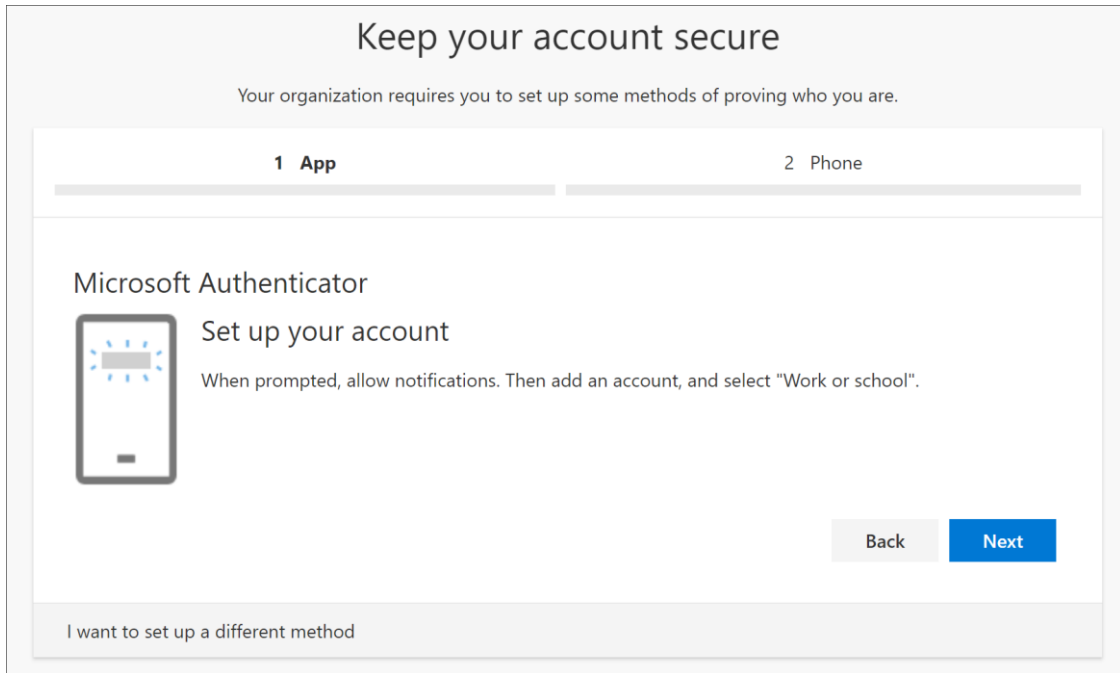
After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

Next

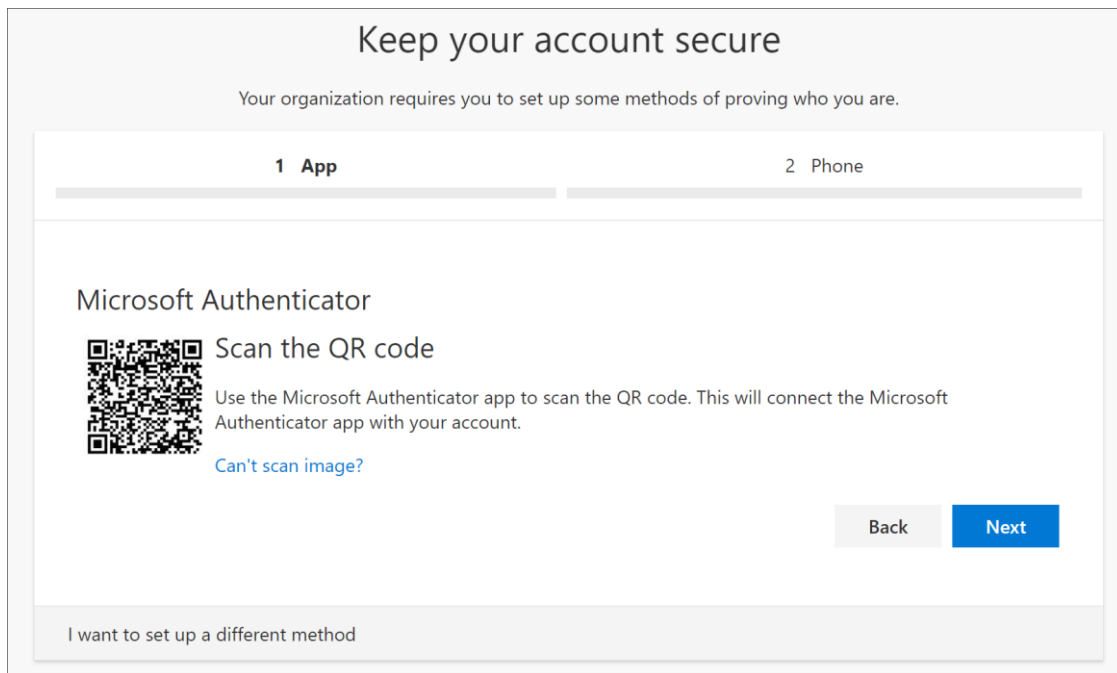
[I want to set up a different method](#)

2. 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, follow this link: [Download and install the Microsoft Authenticator app](#).



3. Remain on the “**Set up your account**” page on your computer while you set up the Microsoft Authenticator app on your mobile device.
4. 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**.
5. Return to the **Set up your account** page on your computer, and then select **Next**.

The **Scan the QR code** page appears.

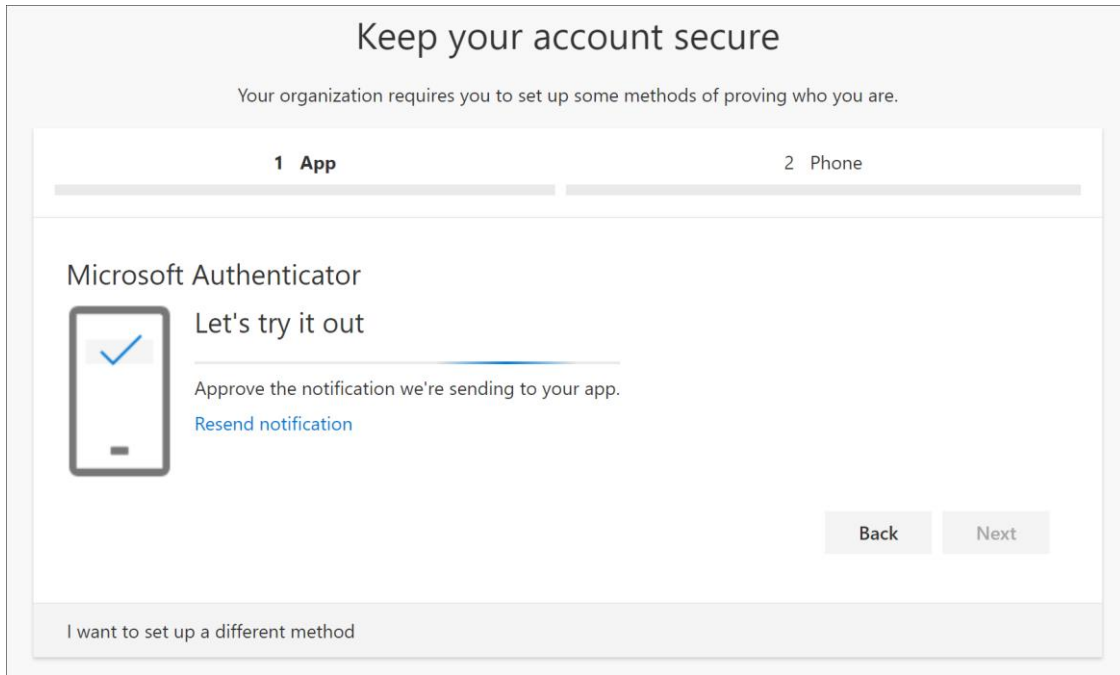


6. Scan the provided code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your work or school account in Step 5.

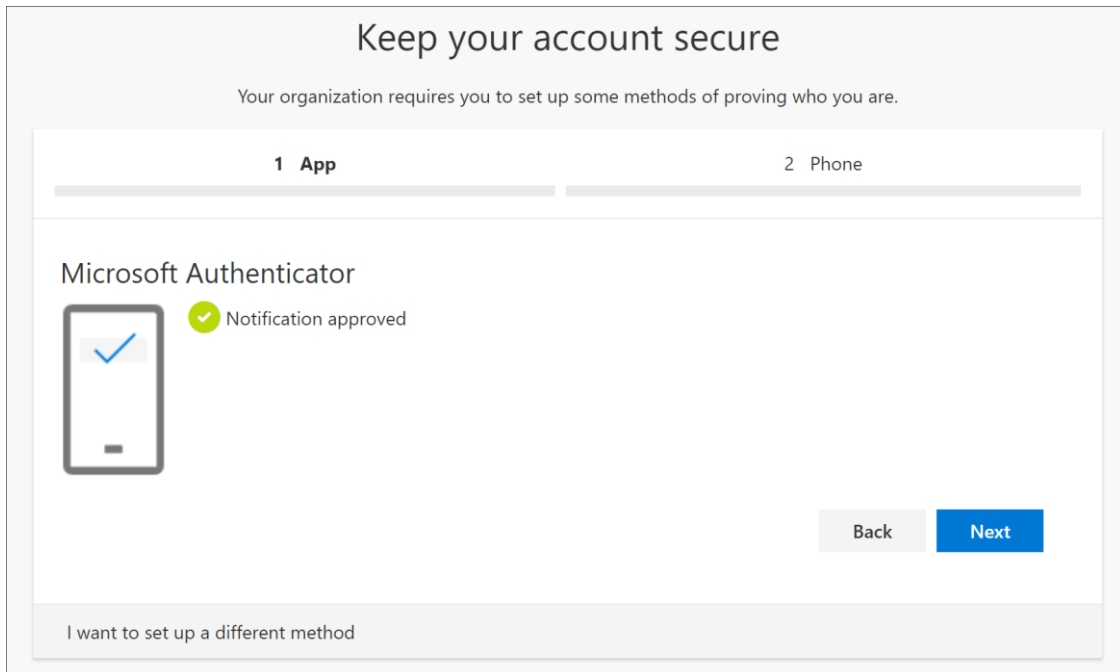
The authenticator app should successfully add your work or school account without requiring any additional information from you. However, if the QR code reader can't read the code, you can select the **Can't scan the QR code link** and manually enter the code and URL into the Microsoft Authenticator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

7. 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.



8. 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.

9. On the **Phone** set up page, choose whether you want to receive a text message or a phone call, and then select **Next**. For the purposes of this example, we're using text messages, so you must use a phone number for a device that can accept text messages.

Keep your account secure

Your organization requires you to set up some methods of proving who you are.

1 App 2 Phone

Phone

Which phone number would you like to use?

+1 1234567890

Call me

Text me a code

Next

I want to set up a different method

A text message is sent to your phone number. If you prefer to get a phone call, the process is the same. However, you'll receive a phone call of a text message.

10. Enter the code provided by the text message sent to your mobile device, and then select **Next**.

Keep your account secure

Your organization requires you to set up some methods of proving who you are.

1 App 2 Phone

Phone

We just sent a code to +1 1234567890

Enter code

Resend code

Back Next

I want to set up a different method

11. Review the success notification, and then select **Done**.

Keep your account secure

Your organization requires you to set up some methods of proving who you are.

1 App

2 Phone

Phone

Call answered

[Done](#)

[I want to set up a different method](#)

Your security info is updated to use text messaging as a backup method to verify your identity when using two-step verification or password reset.

12. Review the **Success** page to verify that you've successfully set up both the Microsoft Authenticator app and a phone (either text message or phone call) method for your security info, and then select **Done**.

Keep your account secure

Your organization requires you to set up some methods of proving who you are.


1 App


2 Phone

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method: Microsoft Authenticator - notification

 Phone
+1 1234567890

 Microsoft Authenticator

[Done](#)

[I want to set up a different method](#)

Next steps

- To change, delete, or update default security info methods, see:
 - [Set up security info for an authenticator app.](#)
 - [Set up security info for text messaging.](#)
 - [Set up security info to use phone calls.](#)
 - [Set up security info to use email.](#)
 - [Set up security info to use pre-defined security questions.](#)
- For information about how to sign in using your specified method, see [How to sign in.](#)
- Reset your password if you've lost or forgotten it, from the [Password reset portal](#) or follow the steps in the [Reset your work or school password](#) article.