Multi Factor Authentication (MFA)

Multi Factor Authentication is a security feature of your Trinity account, that requires you to login with your username and password as you have previously, but also requires an additional means of authentication, such as a text message, phone call, or push notification to verify the sign in. This prevents a malicious user from being able to compromise your account after they have compromised your username and password, as they would not have the phone required to verify the sign in.

Once you have set up MFA, if you receive a prompt to approve your sign-in while you are not actively logging into a Trinity resource, DO NOT APPROVE IT, and immediately contact the IT Helpdesk via phone.

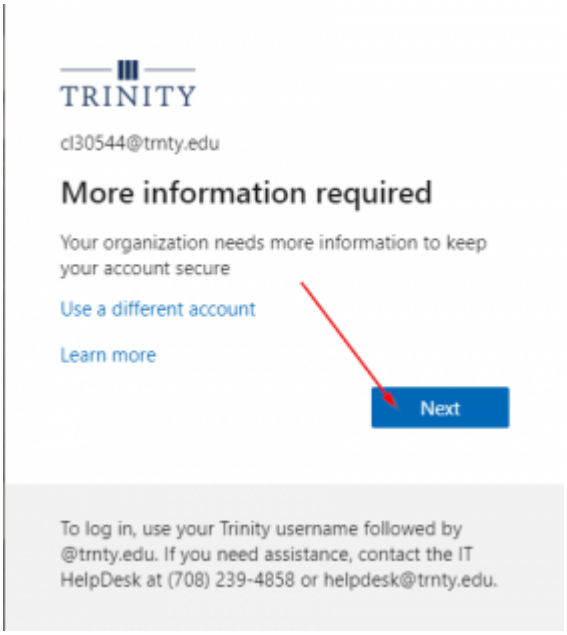
To configure MFA, please follow the steps below:

NOTE: You will need to begin this process on a computer, not your phone.

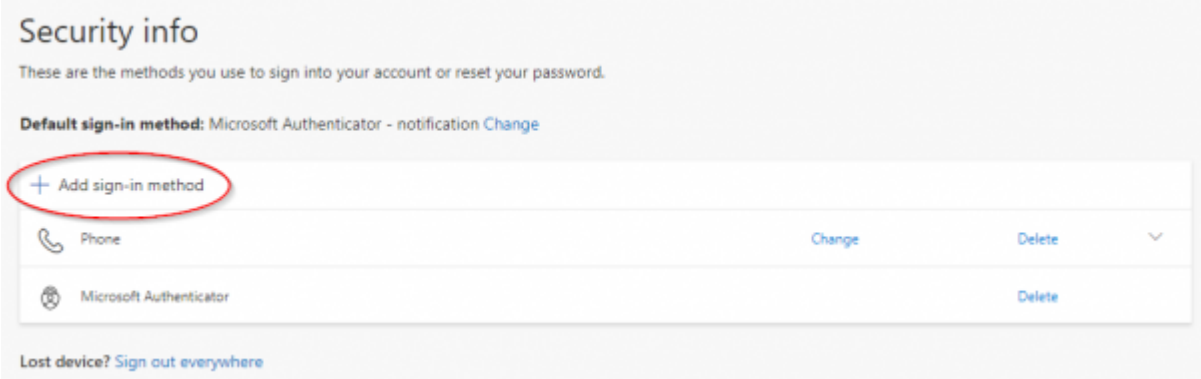
1. On a *computer*, navigate to https://aka.ms/mfasetup.

2. If you are not already signed in, enter your Trinity credentials.

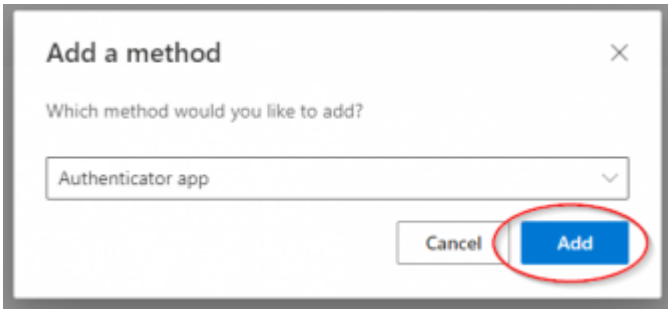
3. For faculty/staff, you will be prompted to enter additional information to secure your account. Simply click **Next**.



For students, or if you have already set up MFA and are setting up another method, you will see the page below, with or without MFA methods already listed. Click **Add sign-in method**.

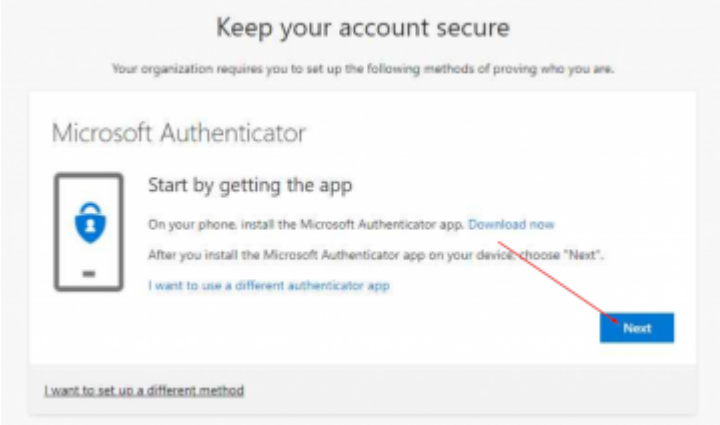


You will be prompted to choose the method you would like to add - we recommend the **Authenticator app** option. Click **Add**.



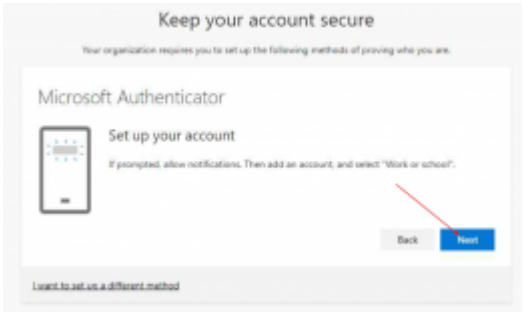
4. To complete the MFA setup, you will need to configure two methods of authentication. The default option is the **Authenticator app** - we highly recommend this as it is quick and simplest to use in daily life. To set it up, click **Next**.

Alternatively, if you wish to use a different method, you may select “I want to set up a different method” instead.

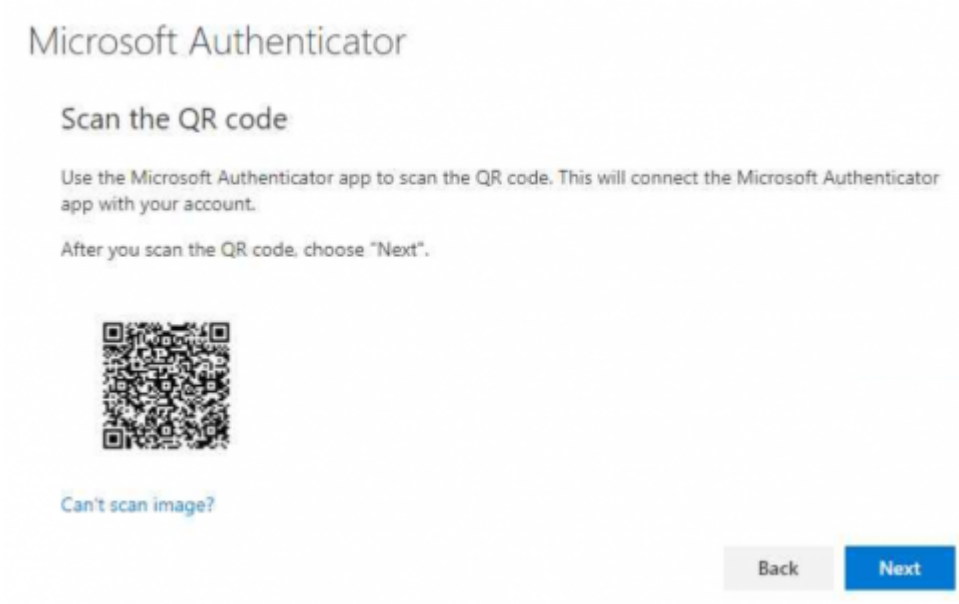


5. You will need to download the Authenticator app on your phone if you have not already done so. This can be done by navigating to: https://aka.ms/getMicrosoftAuthenticator on your *phone*, or searching for “Microsoft Authenticator” in the App Store or Play Store.

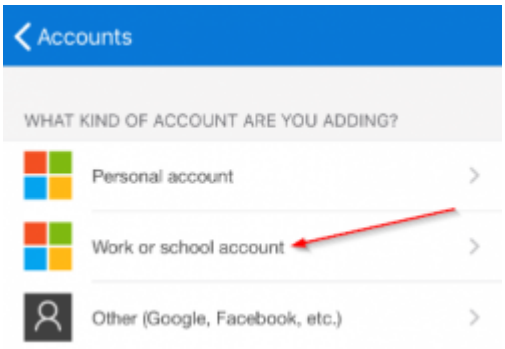
6. Once installed on your phone, launch the app, and if prompted, **allow notifications** from the app. This will allow for easy authentications later. Then click **Next** on your *computer*.



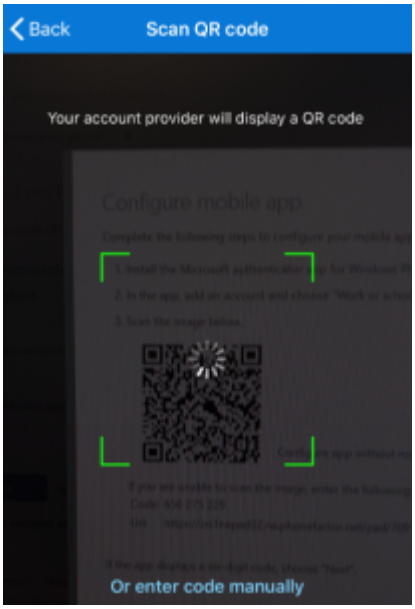
7. You will then be presented with a QR code on your *computer*. You will need to scan this code from the Microsoft Authenticator app on your phone. Leave the QR code on your screen, and proceed with the next few steps.



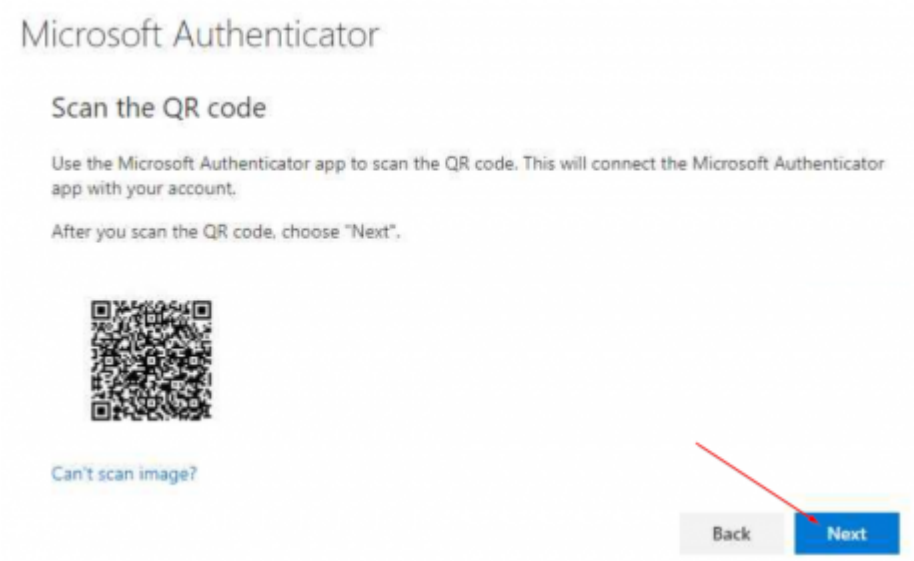
8. In the Microsoft Authenticator app on your *phone*, tap **Add an account**, and select **Work or school account**. Select **Scan a QR code**. You will likely need to allow permissions to your camera at this point - make sure to accept or allow these permissions.



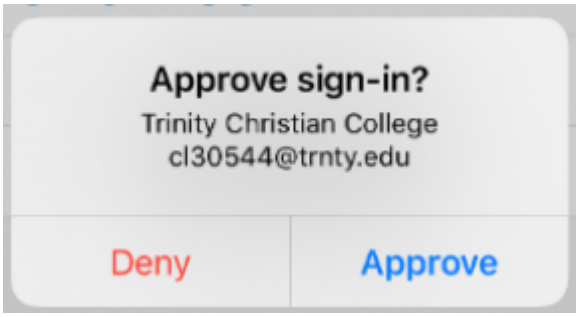
9. The Microsoft Authenticator app will prompt you to scan the QR Code that is currently displayed on your computer (**allow permissions to your camera first**, if prompted).
NOTE: If your phone is older or camera permissions were not allowed, the app may prompt you for a **Code** and **URL** instead of allowing you to scan the QR code. If that is the case, click **Can't scan image?** on your *computer.* It will then show a code and URL that you will need to type into the app exactly as shown.



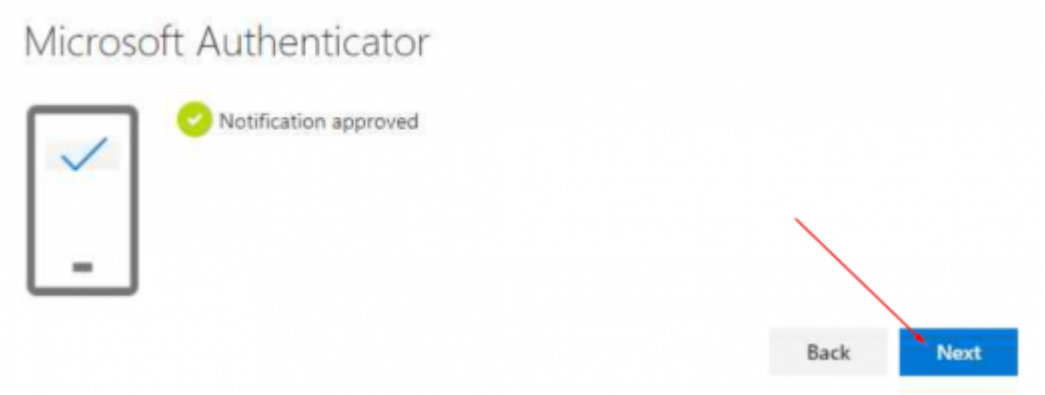
10. Once your account appears in the list in the Microsoft Authenticator app, click the **Next** button on the popup on your *computer*.

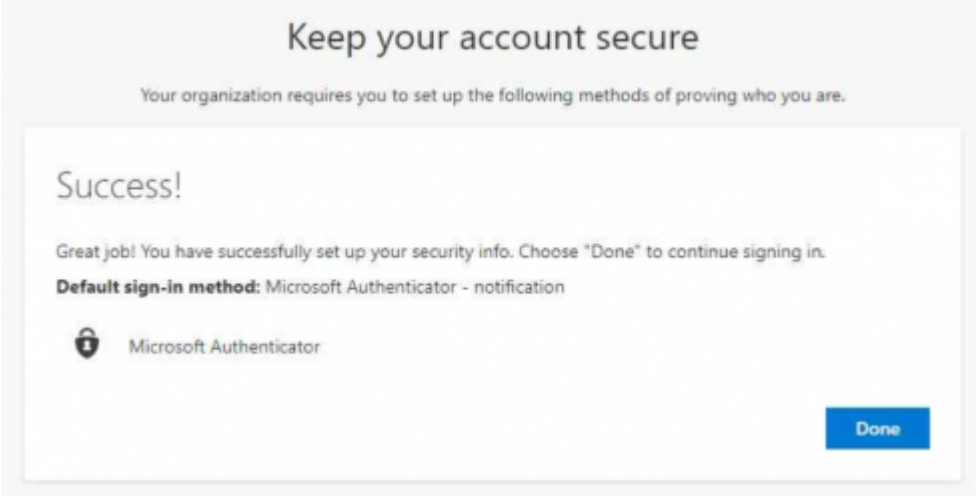


11. Shortly after clicking next, you will receive a test pop-up on your *phone* to either approve or deny the sign in request. Tap **Approve**.



12. The app setup process is now complete! Click **Next** on your *computer* to continue.



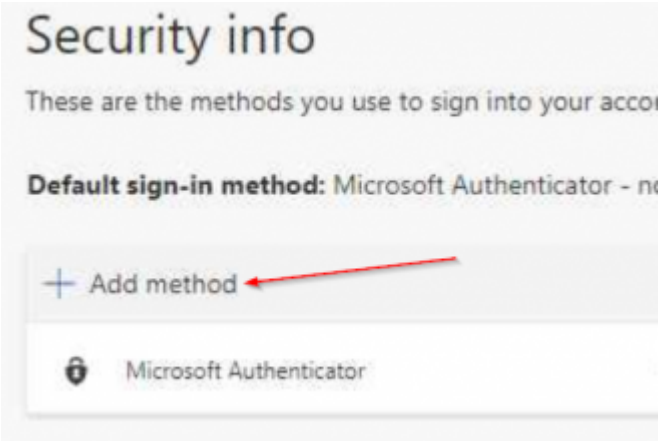


13. After completing the App setup process, **we strongly recommend adding a secondary authentication method** in case you misplace or replace your phone.

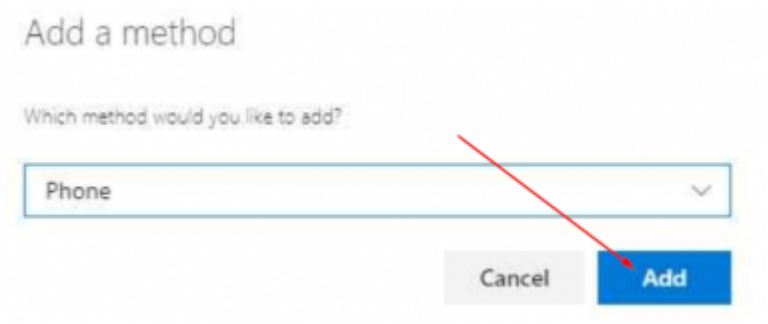
If you were directed elsewhere, navigate to https://aka.ms/mfasetup again (Security Info is the page you want to be on - if you're already there, continue).

You may be prompted to authenticate again, and potentially use your newly configured authenticator app.

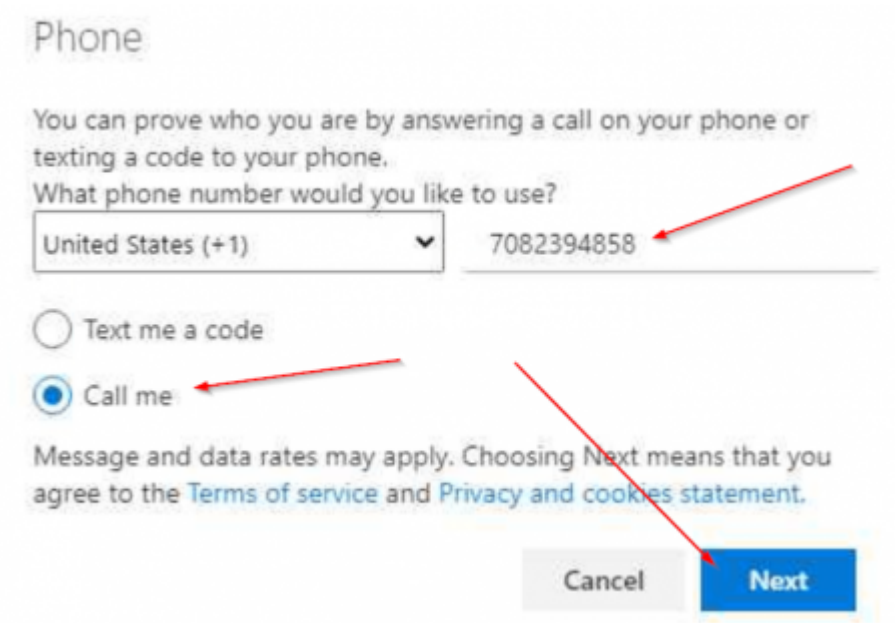
Once signed in, you should be at the Security Info page. Click the **Add method** button.



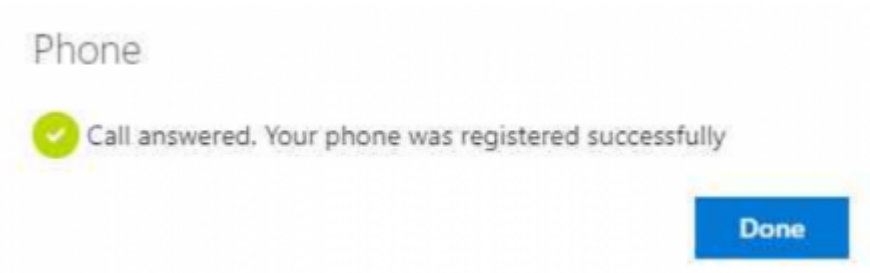
Select one of the options from the dropdown - we recommend using **Phone** as your secondary authentication method. Select an option and click **Add**.



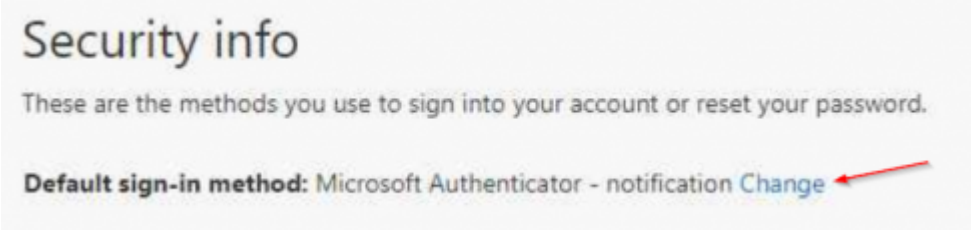
On the next page, enter your phone number (or other form of verification, if selected), select if you would like a phone call or a text message, then click **Next**. Note: You may use your office phone, but keep in mind you can only access that phone from on campus, and it cannot receive text messages.



If you chose the call option, your phone will be called, simply **answer the phone and press the pound (#) key.** If you chose the text message option, you will receive a text message with a one time code in it. **Enter it when prompted on the site and click Next.** - One this is complete, you have successfully configured your phone as a secondary authentication method. Click **Done**.



Once you have followed these steps, MFA has been configured. When attempting to access sensitive applications, or accessing Trinity data from off-campus, you may be prompted to authorize your sign-in via one of your configured MFA methods. When prompted for MFA, it will attempt to use whichever method you selected as default. If for some reason you cannot use that method, simply select **Sign in another way**, and choose one of your other MFA methods. If you would like to change your default authentication method, navigate back to https://aka.ms/mfasetup, authenticate if needed, then select **Change** next to Default sign-in method.



From this popup, you are able to select a new authentication method, then confirm the change.