

Setup Azure MFA: Mobile App Method

Cloud Version
Identity & Access Management



Overview

What is MFA?

Multi-factor authentication (MFA) is a technology Trinity Health uses to verify your identity when accessing certain applications from outside of a Trinity Health facility or on a personal device. The MFA service that Trinity Health uses is called Azure MFA.

Requirements

You need two separate devices.

- Computer (personal or work)
- Smartphone

Setup Azure MFA: Mobile App Method

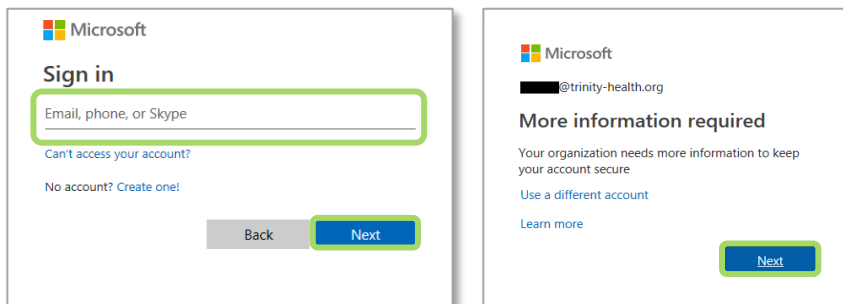
Please follow the instructions below carefully before reaching out to the **Service Desk**.

Make sure your smartphone can access the internet.

If you have a Trinity Health email address, your Azure login ID (also known as a **UPN**) will be the same as your Trinity Health email address. You can look up your UPN using the following link if you are on the Trinity Health network or VPN: <https://findmyupn.trinity-health.org/>

[Computer]

1. On the computer (laptop/desktop), go to: <https://aka.ms/mfasetup>
2. On the **Sign in** screen, enter your Trinity Health email/UPN, and click **Next**.
3. On the **Enter password** screen, enter your network password, and click **Next**.
4. On the **More information required** screens, click **Next**.



[Smartphone]

5. On your smartphone, complete one of the following options:
 - **Option 1:** Scan the following QR code that matches your smartphone type



Apple App Store



Google Play Store

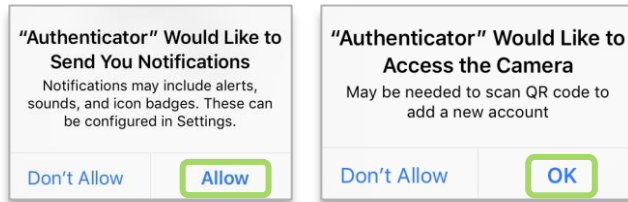
- **Option 2:** Search for the **Microsoft Authenticator** app in the **Apple App Store** or **Google Play Store**

Setup Azure MFA: Mobile App Method (continued)

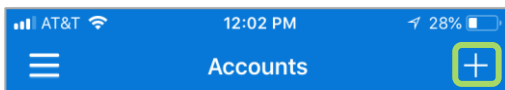
- Install the free **Microsoft Authenticator** app.

The Microsoft Authenticator app is free, and it does not have any in-app purchases.

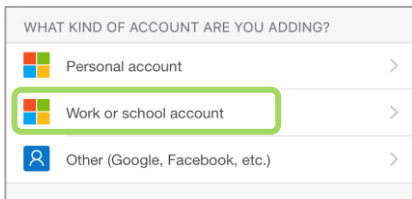
- Open the **Microsoft Authenticator** app.
- If prompted to allow the Microsoft Authenticator app to send notifications and access the camera, choose **Allow** or **OK** on each screen.



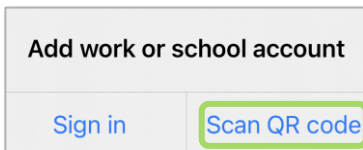
- In the **Microsoft Authenticator** app, choose the **+** in the upper right corner to add a new Account.



- On the **What kind of account are you adding** screen, choose **Work or school account**.



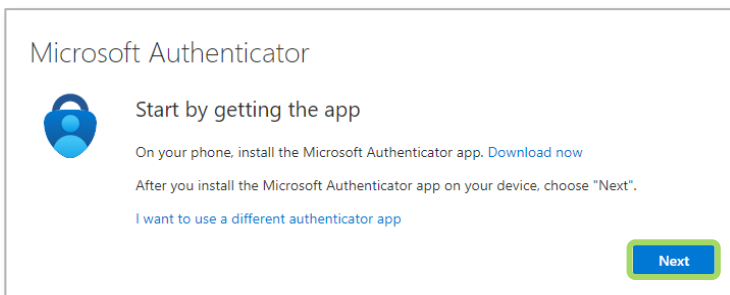
- On the **Add work or school account** screen, choose **Scan QR code**.



- The app on your smartphone or tablet will be using its camera to find/scan QR codes, and soon the web page will display a QR code to scan.

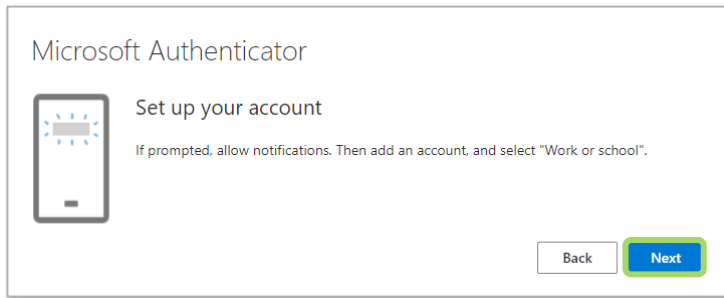
[Computer]

- On the **Start by getting the app** screen on the computer, click **Next**.



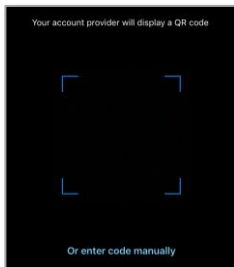
Setup Azure MFA: Mobile App Method (continued)

14. On the **Set up your account** screen, click [Next](#).



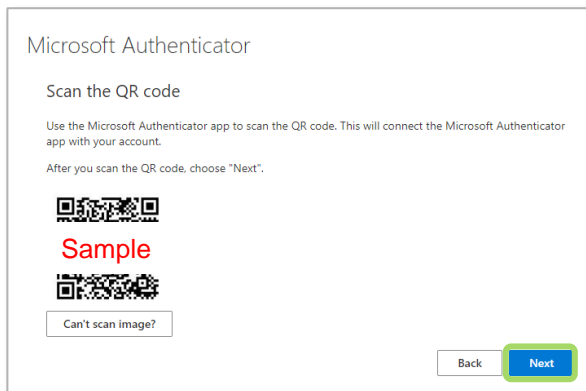
[Smartphone]

15. Hold your smartphone up to the computer screen so that it can scan the **QR code**.

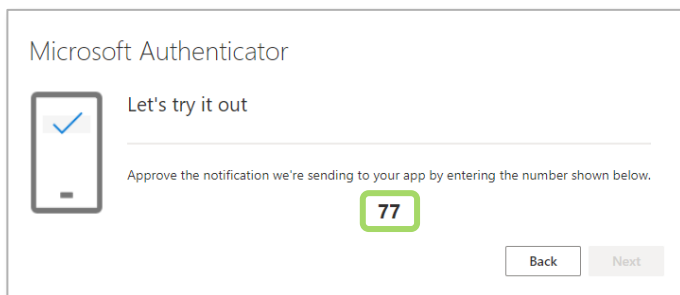


[Computer]

16. On the **Scan the QR code** screen on the computer, click [Next](#).



17. Read the number on the **Let's try it out** screen.



Setup Azure MFA: Mobile App Method (continued)

[Smartphone]

18. Enter the number from the **Let's try it out** screen on the computer into the **Are you trying to sign in?** notification on the smartphone, and then choose **Yes** on the notification.

[Computer]

19. On the **Notification approved** screen on the computer, click **Next**.

20. On the **Success** screen, click **Done**.



You're done! Going forward, you will be prompted to use MFA every time you access certain Trinity Health applications from outside of a Trinity Health facility or on a personal device.

Account Management

You can return to <https://aka.ms/mfasetup> at any time to manage your Azure MFA account.

More Information

MFA, sometimes called “2-factor authentication,” helps protect against unauthorized access to your accounts and the personal and Trinity Health data they contain. Once MFA is set up, each time you log into an application that requires MFA from outside the Trinity Health network, you will be required to respond to an MFA challenge to confirm your identity.