Overview

Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution for users who are logging in to Office 365 applications (for example, Outlook O365) when not on the Trinity Health network. MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication, offering users a choice of two verification methods: a phone call prompt or mobile app pop-up notice prompt (recommended).

This job aid provides instructions for enrolling in MFA so that when you log into an O365 app, your identity is verified using the mobile app, which sends you a pop-up notification, and then you respond as prompted. This is the preferred method, and it provides the greatest security. If you prefer to get a phone call for verification, see the job aid titled: Enrolling in MFA to Access O365 with a Phone Call Prompt.

When do I need to enroll in MFA?

- **Important:** Enroll in MFA as soon as possible. Due to security constraints, the window of opportunity for enrolling will close 31 days from the first day you are able to enroll. After that, you will be required to complete a system Access Request form for permission to enroll.
- When on an untrusted network (for example, your home network) you will not be able to access any O365 resources (such as Outlook O365) until you enroll in MFA.

What do I need to enroll in MFA?

- You need two separate devices. This enrollment process cannot be completed from a single device.
- You must have an Internet connected device with a web browser to access the MFA enrollment web site.
- You will need a separate Internet connected iOS or Android smart phone or tablet on which to receive an authentication prompt as a second factor of authentication. This will be the device that you will use going forward for all logins that require MFA.

**Note:** These instructions are for first time enrollment in Azure MFA and will not need to be repeated for each O365 login. Once MFA enrollment is completed, you will be able to use it anytime MFA is required to access O365.

Install and Setup Microsoft Authenticator on Your Smart Phone

First, you will download and install Microsoft Authenticator on the smart phone or tablet you have chosen to use as your second factor of authentication. In the next section, on your Trinity Health laptop or computer, you will sign in, enroll on the Azure MFA website, and setup your security authentication method.

1. Go to your smart phone or tablet's app store (Apple App Store or Google Play Store). Search for, download, and install the Microsoft Authenticator app on your mobile device.
2. Once installed, tap Open.
3. Once you open the App, you will see these prompts at various times. When prompted to allow the app to send you notifications or use your camera, tap **Allow** or **OK** on each screen. This is important because you will need to scan a QR code later.

**Note:** If you previously denied the app this type of access, you will need to enable it to use MFA now.

4. On the Microsoft Authenticator app, tap the + in the upper right corner to add a new Account.

5. When the screen opens that asks, "What kind of account are you adding?" tap **Work or school account**.

---

**Trinity Health Device: Setup Security Authentication Method on MFA Web Site**

**Note:** The next group of steps must be performed on a different Internet connected device with a web browser. You must not use the device with the Microsoft Authenticator app.

1. In the other device’s web browser, go to: [https://aka.ms/mfasetup](https://aka.ms/mfasetup)
2. On the **Sign in** screen, enter your Trinity Health email address. Click **Next**.
3. On the next screen, enter your network password. Click **Next**.
4. You will then be prompted for more information. Click **Next** on each of these screens.
5. On the **Start by getting the app** screen, click **Next**.

6. On the **Set up your account** screen, click **Next**.

7. The **Scan the QR code** screen will display a **QR code**.
8. Since you have given permission to the app to use your smart phone or tablet’s camera, the app on your smart phone or tablet should now be using its camera to find/scan QR codes. Use the camera to scan the **QR code**.
9. After scanning the **QR Code**, click **Next** on the **Scan the QR code** screen.

**Note:** If you are not able to scan the QR code, you may Click **Can’t scan image?** to get a code that you can enter manually.
10. The system will send an authorization request to your mobile device to test the setup.
11. Tap Approve on the notification on your mobile device to continue.

![Image of Microsoft Authenticator app](image)

12. On the Let's try it out screen, click Next.

![Image of Microsoft Authenticator app](image)

13. On the Success! screen, click Done.

![Image of Microsoft Authenticator app](image)

Your MFA account is configured, and you will now be able to approve MFA authentication requests on your mobile device when logging into O365 apps on your Trinity Health device.

You will not need to complete enrollment steps again, but you can return to [https://aka.ms/mfasetup](https://aka.ms/mfasetup) at any time to manage your account or change your authentication method.

You will now be able to log into O365 apps (for example, Outlook O365) when not on the Trinity Health network.