Cleveland Clinic

Microsoft Authenticator Application Set-up and Enrollment

If you have ever needed access (or think you may need access in the future for some reason) to single sign on (SSO) applications such as Outlook, Kronos or Workday to check your email, timecard or pay slip when you're not connected to Cleveland Clinic's network, you need to follow the instructions below to enroll in the Microsoft Authenticator app to keep your access.

The Symantec VIP app has been our second layer of security to authenticate your identity when working offline. It generates a one-time security code that you are required to enter—after you enter your network password—to gain access to these SSO applications. You need to know that Symantec VIP is being replaced by the Microsoft Authenticator app. Our goal is for all caregivers to be enrolled in Microsoft Authenticator by the end of the first quarter.

Note: Do not delete the Symantec VIP app yet. Some single sign-on applications may still require you to use it until we remove it.

I Need to Make an Exemption Request

If you require an exemption request from the Microsoft Authenticator enrollment process, you need to follow the three steps listed.

To access the exemption website, you must be logged on to Cleveland Clinic's network or contact the ITD Service Desk at 216.444.4357 for help.

1. Logon to the Exemption request website.
2. Select the link **Add myself to Azure MFA exception list**.
3. Choose a reason from the available options and select **Save**.

Self-Service Steps to Set-up the Microsoft Authenticator App

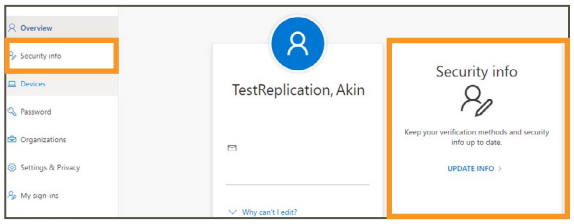
Follow the steps below to add the Microsoft Authenticator app to your account.

To start the enrollment process, you will need either a Cleveland Clinic-issued or personal mobile device and a computer that's connected to Cleveland Clinic's network to establish and verify your connection authentication.

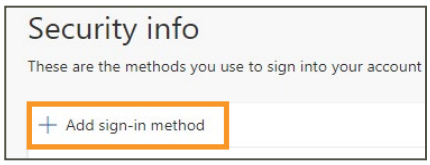
Using your computer

1. Visit the **My Account portal** (https://myaccount.microsoft.com). Open a new browser window and **sign in** to your work account.
2. Select **Security Info** in the left menu option or use the link in the Security info pane.

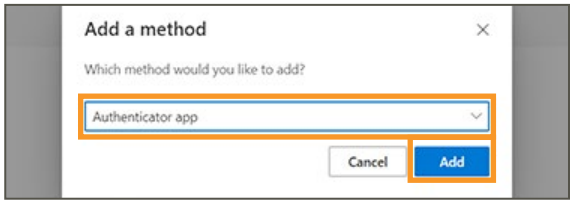
   Note: If you have already registered a sign-in method, you'll be prompted for two-factor verification. Then, select **Add method** in the Security info pane.



3. Select + **Add sign-in method**.



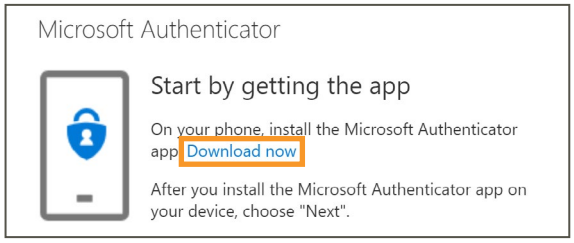
4. Choose **Authenticator app** from the list and then select **Add**.



Microsoft Authenticator Application Set-up and Enrollment

Using your computer and mobile device

5. You'll get this reminder about the Microsoft Authenticator app.



   If you use a Cleveland Clinic-issued or personal mobile device and the app is already downloaded, you can bypass steps 5 and 6. Continue with the enrollment process and select Next.

   Otherwise, you can either select the **Download now** link on your computer screen to scan a QR code with your mobile device, or select a link below to visit the appropriate store associated with your device type.

   Apple App Store (iOS)
   https://apps.apple.com/us/app/microsoft-authenticator/id983156458

   Google Play store (Android)
   https://play.google.com/store/apps/details?id=com.azure.authenticator

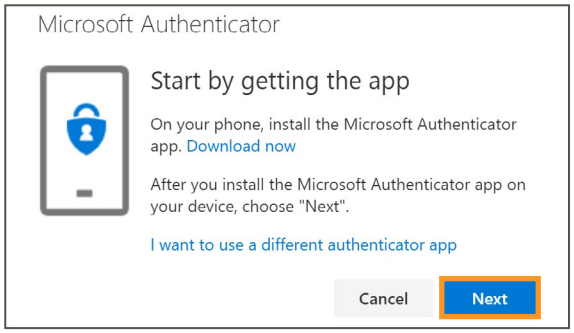
   Note: Be sure to use the free Microsoft Authenticator app when downloading it from the Apple App Store or Google Play store. **See app image below**.

   - Follow the app download prompts. The Microsoft Authenticator app should now appear on your mobile device so you are now ready to continue enrollment.

     Note: Caregivers with iPhone devices will need to know their Apple ID in order to download.

6. **Don't select Next on the screen until you have confirmed the Microsoft Authenticator app is downloaded on your mobile device.**

   - Once the app has been downloaded, select **Next** on your computer screen.



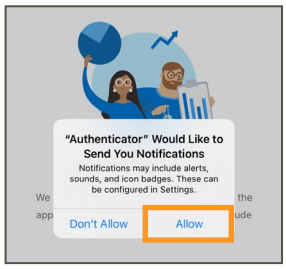
Microsoft Authenticator Application Set-up and Enrollment

Using your computer and mobile device

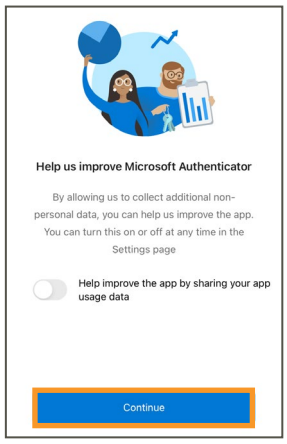
7. Open the **Microsoft Authenticator app** on your mobile device. If prompted, select **Allow** to enable notifications.

   Note: Best practice is to **allow** push notifications.

   - Select **Accept** to acknowledge Microsoft privacy statement.

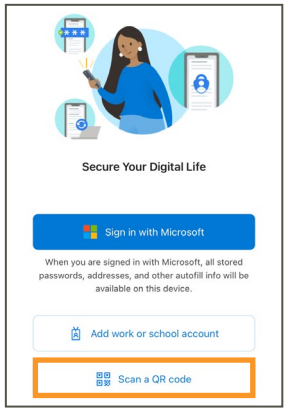


8. Verify that **"Help improve the app by sharing your app usage data"** is unselected (gray) and select **Continue**.

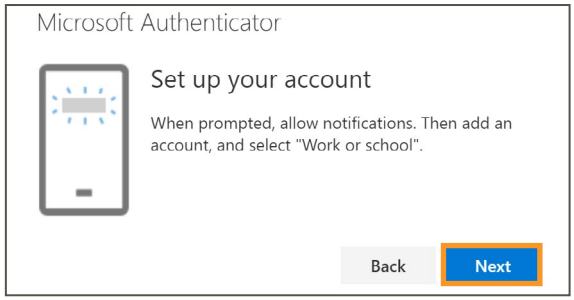


9. Select **Scan a QR code**.

   Note: If prompted to allow Authenticator to access the camera, select **OK**.



10. Return to your computer. Select **Next** in the **"Microsoft Authenticator - Setup your account"** window.



Microsoft Authenticator Application Set-up and Enrollment

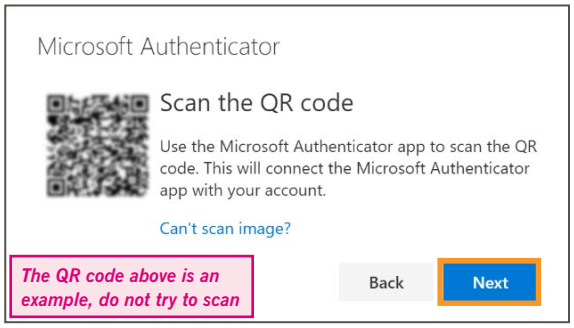
Using your computer and mobile device

11. Using the Microsoft Authenticator app on your mobile device:

- **Scan the QR code that appears on your computer**. Hold your phone camera at your computer screen and point at the QR code to scan it.

- Select **Next** on your computer.

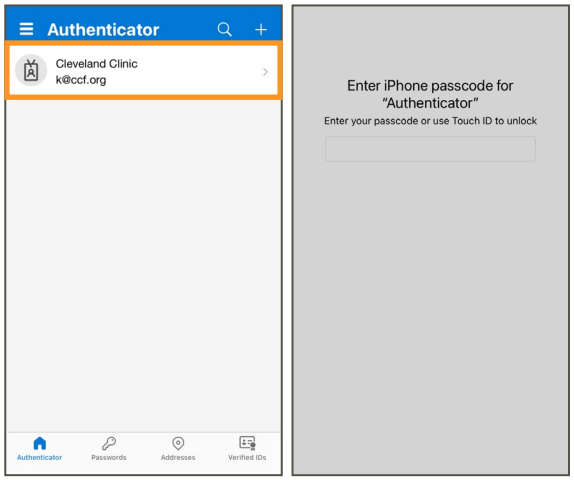
Note: If you select the **"Can't scan image?"** link, you will receive a code and a URL to manually enter and validate.



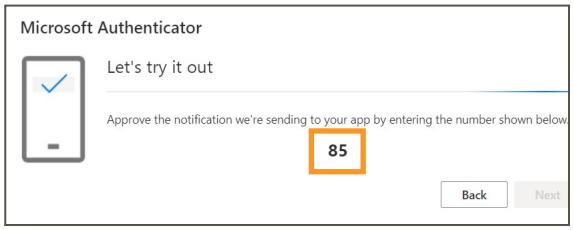
12. The Microsoft Authenticator app should successfully add your work account without requiring any additional information from you.

Your account will appear as authenticated with the Microsoft Authenticator app, and your email address will appear.

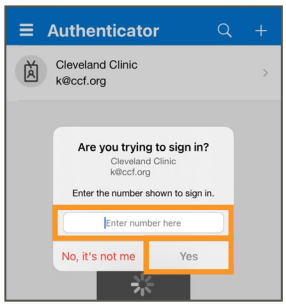
Note: Any time you step away from the Microsoft Authenticator app while it's still opened on your device, you will be required to unlock your mobile device to return to the app.



13. The **"Microsoft Authenticator - Let's try it out"** window on your computer indicates a notification is being sent to your Microsoft Authenticator app, and contains a security code number that you need to type into the Authenticator app to validate your account.

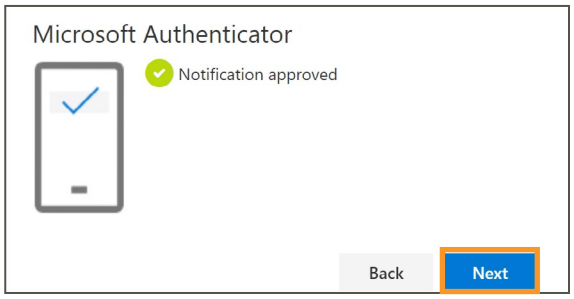


- Enter the provided security code into the Microsoft Authenticator app on the phone and then select **Yes**.



Microsoft Authenticator Application Set-up and Enrollment

14. This confirms that the notification has been approved on your Microsoft Autheticator app. Select **Next** on your computer.

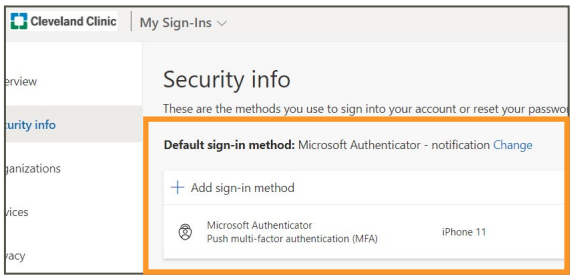


All Set - You Are Now Enrolled

Now that your two-step verification security information is updated and set as your default in the app, your identity is ready to be verified each time you want to access Cleveland Clinic apps when you're not logged into our network.

- The **My Account portal** (https://myaccount.microsoft.com). will now display your secure device on the **Security info** page, and at any time you can return to add or delete trusted devices.

  If you get a new mobile device, you will be required to download the Microsoft Authenticator app again and re-register.

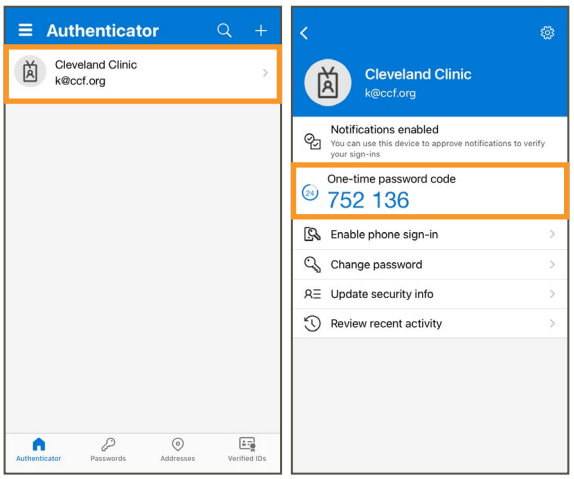


One-Time Security Passcode

Whenever you need a one-time security passcode for MFA (multi-factor authentication), return to your **Microsoft Authenticator app**.

- Access the one-time security passcode by selecting on your **Cleveland Clinic account** to reveal it, as shown in the image.

This can be used when you're not connected to Cleveland Clinic's network or for an MFA prompt.



Support

If you have questions or need assistance, contact the IT Service Desk at 216.444.4357.

Note: If you delete the Microsoft Authenticator app off your device or get a new mobile device, download the app again and contact the IT Service Desk to re-register the device.

Microsoft Authenticator Application Set-up and Enrollment

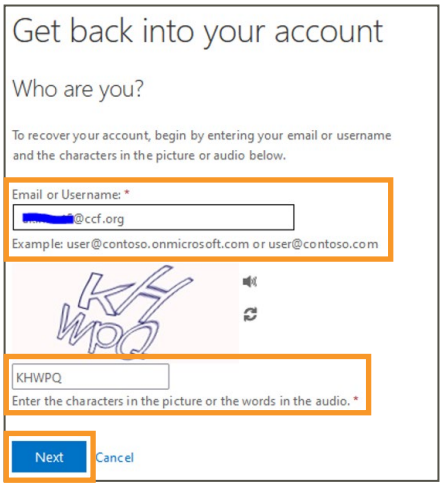
Appendix

Confirm Enrollment

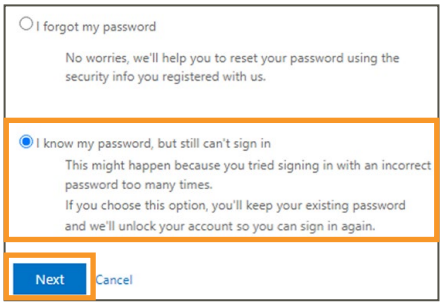
If you'd like to take additional steps to confirm your Microsoft Authenticator enrollment, below are some steps you can follow.

1. Browse to https://changepassword.ccf.org, then scroll down to the bottom of the page and select **Get Started**.

2. You will see a screen that says "Get back into your account." Enter your **User ID**, which is your Cleveland Clinic email address (e.g. doakesj@ccf.org).
   - Enter the characters shown in the picture on the screen to verify you're not a robot and then select **Next**.



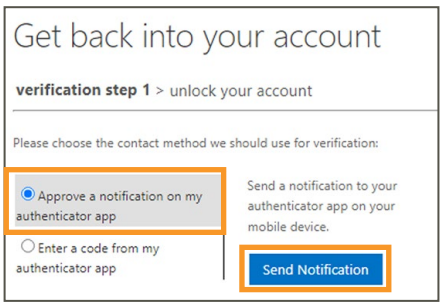
3. On the following screen, select **I know my password, but I still can't sign in** and then select **Next**.



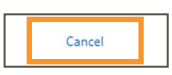
4. On the next page, select **Approve a notification on my authenticator app** and select **Send Notification**.

   If you successfully registered, you will receive a Microsoft Authenticator notification to your phone.

   If you did not successfully register, nothing will happen and you will need to redo the Microsoft Authenticator registration.



5. Select **Cancel** on the screen or just shut the browser page to stop the process.

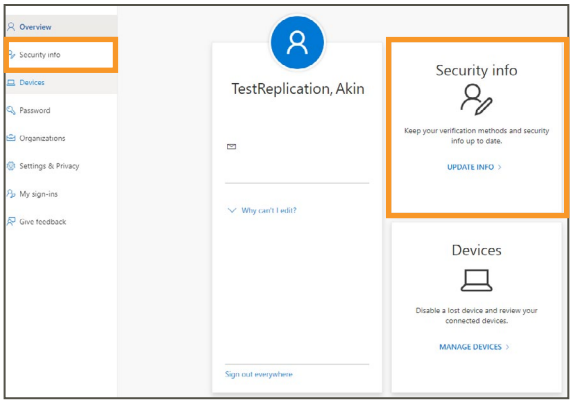


Microsoft Authenticator Application Set-up and Enrollment

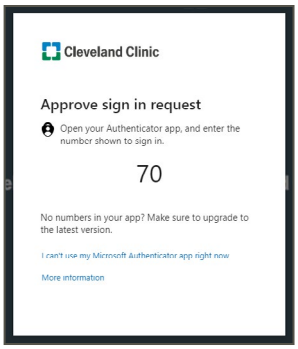
Appendix

Update Your Microsoft Authentication App or Add an Additional Device

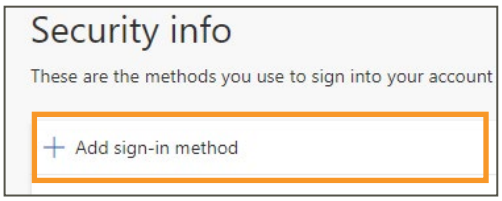
1. Visit the **My Account portal** (https://myaccount.microsoft.com) and **sign in** to your work account.
2. On the landing page under **Security Info**, select **Update info**.



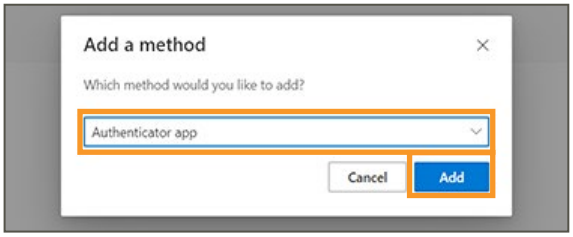
3. To validate your current authentication method, open your **Microsoft Authenticator app** and **enter the number** provided to sign in to your account.



4. You can add more devices by selecting **Add sign-in method**.



5. Choose **Authenticator app** from the list and then select **Add**.



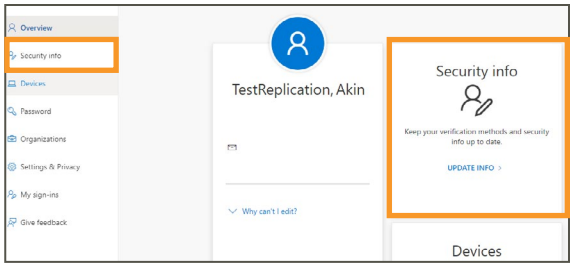
Microsoft Authenticator Application Set-up and Enrollment

Appendix

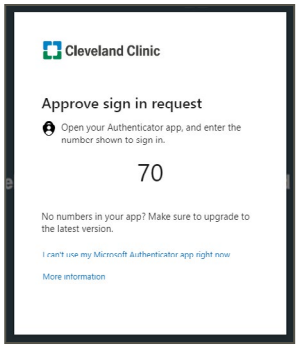
Misplaced or Stolen Device

If a secondary authenticator method exists, you can manage the update yourself.

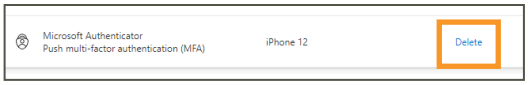
1. Visit the **My Account portal** (https://myaccount.microsoft.com) and **sign in** to your work account.
2. On the landing page under **Security Info**, select **Update info**.



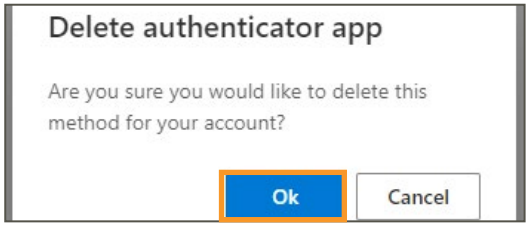
3. To validate your current authentication method, open your **Microsoft Authenticator app** and **enter the number** shown to sign in.



4. Select **Delete** on the device you would like to remove.



   - Select **Ok**.



If a secondary authenticator does not exist.

1. On the landing page under **Security Info,** select **Sign out everywhere**.
2. Contact the IT Service Desk at 216.444.4357 to request a reset for Authenticator's sign in method.