This Guide is to enable employees to use web-based email while not at work.

You may do this at home.

1. **All employees must install Microsoft Authenticator to use Basic Services:**
   
   1.1 [Setup Microsoft Authenticator - Registration Instructions](#)

2. **Once you are working from home, complete this step for Basic Services:**

   2.1 [Accessing Office 365 Applications Including Outlook](#)

**Appendix** - [Microsoft Authenticator FAQ](#)

For additional Basic Services details see the expanded

[Guide for working at home - COVID-19 Employee Basic Services](#)

[How-to-Videos for Basic Service features (Accessible from Home)](#)
Pre-Requisites:

- Be on a computer with an Internet connection
- Have your Android / Apple iOS smartphone or tablet device
- Set your device to be on your mobile carrier’s network, not Wi-Fi
  ➢ On your device, temporarily disable Wi-Fi during this registration process. Some issues have been traced back to using Wi-Fi.

Begin Registration

From your Android or Apple iOS device

1. On your Android or Apple iOS device, navigate to Google Play or the App Store, search for “Microsoft Authenticator” and click “Install” or “GET” to install Microsoft Authenticator on your device.

   ![Microsoft Authenticator](image)

   Once installed, the app icon will look like this:

   ![Authenticator Icon](image)

2. On your device, disable WiFi.
From a computer with an Internet connection

1. On a computer with an Internet connection, register for Microsoft Authenticator by going to this website: https://aka.ms/MFASetup

2. For your account, use your “[lastname.firstname]@mayo.edu” email address and then click “Next”.

3. You will get the prompt “More information required”, click “Next”.
4. You will then be presented with the “Additional Security Verification” prompt:

![Additional security verification]

**Step 1:**

a. How should we contact you: **Select “Mobile app” (only option)**

b. How do you want to use the mobile app?: Select “Receive Notifications for Verification” (recommended)

c. Click “Set up”

d. After clicking Set up, you should receive the "Configure Mobile App" prompt on your computer

e. Pause - **Do NOT** click "Next" - Proceed to Step 2

![Configure mobile app]

3/23/2020 9:52 AM
Step 2:

a. Go to your Android or Apple iOS device and **open the Microsoft Authenticator app**

b. Add a new account:
   - On Android, Click the Menu button (three vertical dots in the upper right) and then “Add account”.
   - On iOS, click on the “Plus” symbol in the upper right.

Choose “Work or school account”.

c. Position your Android or Apple iOS device to Scan the Quick Response Code (Scan QR Code) on your computer screen. Reference the image in Step 1e above. Should capture the whole image inside the blue corners in your camera view on your device.
d. Once accepted, check your computer for activation status:

![Image of mobile app setup](image)

e. Once scanning is complete, click the “Next” button:

![Image of mobile app setup](image)

f. On your computer, you will see the “Additional Security Verification” prompt:

![Additional security verification](image)
g. Now look on your **Android or Apple iOS device** for the authentication response and select “Approve”.

*This option is a push to the user and all that is required is user approval - "Deny" or "Approve".*

![Authentication response on Android or Apple iOS device](image)

h. Configuration is now complete. Click “Done”.

*After successful registration, you may now re-enable your Wi-Fi.*

![Additional security verification](image)

i. You may also see this as the final screen shot. You may now close the setup window.
Accessing Office 365 Applications (Including Outlook)

1. On your computer, launch your preferred browser (See here for list of recommendations from Microsoft) and go to https://office.com.

2. Your first time to this page, it will appear like this, please click on “Sign in”. If it does not, or it signs you into a non-Mayo Clinic account, please log out in the upper right, and at the first page, please choose “Switch to a different account”
3. Fill in your Mayo Clinic email address on the first part of the Sign in screen and click on “Next”

4. On the next screen, verify your email address is correct, and enter in your password (same password you use to login to your device on campus). You may also check “Keep me signed in” if you wish, and then click “Sign in”

5. You will be prompted for MFA “Approve sign in request”

6. Now look to your device you set up Microsoft Authenticator on, you should have a notification to “Approve” or “Deny”
- Or Navigate to the Microsoft Authenticator app on your device and Click “Approve”

7. Use the appropriate icon to launch the Office365 application you wish to use -- Outlook, Word, Excel, etc.

8. Outlook can be accessed directly by going to https://outlook.office.com

Outlook on the Web E-mail allows for attachments to be downloaded to OneDrive. If employees need to edit attachments, it is recommended to save the file to a folder in OneDrive.

If you need further information, please visit https://support.office.com/.
Q. Why is the Registration Configuration not reaching my mobile device?
A. Verify that your device is connected to your mobile carrier's network, not Wi-Fi.
   - On your device, temporarily "Turn-Off" Wi-Fi during this registration process. Some issues have been traced back to using Wi-Fi. After successful registration, you may re-enable your Wi-Fi.

Q. How is Microsoft Authenticator (Azure MFA) different from the RSA SecurID? How does it differ from DUO? Why are multiple MFA tools being rolled-out?
A. Mayo Clinic's upcoming upgrade to a new, cloud-based version of Microsoft Office products called Office 365, a new user authentication tool will be used as well, Microsoft Authenticator (Azure MFA). This solution will be used to provide an added level of security when you are outside the Mayo Clinic network and connecting to Microsoft Office 365 Cloud applications. Multi-Factor Authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the users identify: what the user knows (password) and what the user has (security token). Mayo Clinic currently uses multiple MFA solutions to provide enhanced security due to various security and licensure requirements. Additional efforts will be ongoing to streamline these MFA tools while still meeting all the business and security needs of the organization.

Q. Why do we need to use Multi-Factor Authentication when connecting to my Mayo Clinic Email externally?
A. Using Multi-Factor Authentication is an important first step to protecting Mayo Clinic confidential, proprietary, employee, and patient information. It ensures the right people have the right access to the right systems.

Q. What type of token/authentication will I use with Microsoft Authenticator?
A. Microsoft Authenticator (Azure MFA) uses “push” authentication. You will receive a confirmation on your device from the Microsoft Authenticator App asking you to “Approve” or “Deny”.

Q. What types of mobile devices are supported?
A. You will need an Android or Apple iOS smartphone or tablet device.

Q. Can Mac computers be used?
A. Yes.

Q. What versions are required?
A.
   - Microsoft Authenticator – current version is 6.4.8 or later
   - iPhone / iPad / iPod – iOS 8.0 or later
   - Android – requires 4.4 or newer
Q. What do I need to do if my mobile device is lost, stolen, damaged, or restored?
A. Contact the Mayo Clinic Help Desk and they will assist with doing a "Microsoft Authenticator Account Reset" so that you can "Re-Register" for Azure MFA. After Reset, refer to "Microsoft Authenticator – Registration instructions" for instructions on Re-Registering.

Q. I recently got a new phone and now I’m not able to access my Mayo Clinic Email externally?
A. Contact the Mayo Clinic Help Desk and they will assist with doing a "Microsoft Authenticator Account Reset" so that you can "Re-Register" for Azure MFA. After Reset, refer to "Microsoft Authenticator – Registration instructions" for instructions on Re-Registering.

Q. Can I get an "Emergency Access Code"?
A. No. Unlike RSA SecurID, Microsoft Authenticator does not provide a 'temporary emergency access code'. Contact the Mayo Clinic Help Desk and they will assist with doing a "Microsoft Authenticator Account Reset" so that you can "Re-Register" for Azure MFA. After Reset, refer to "Microsoft Authenticator – Registration instructions" for instructions on Re-Registering.

Q. I’ve deleted the Microsoft Authenticator app from my smartphone and now I can’t access my Mayo Clinic Email externally?
A. Contact the Mayo Clinic Help Desk and they will assist with doing a "Microsoft Authenticator Account Reset" so that you can "Re-Register" for Azure MFA. After Reset, refer to "Microsoft Authenticator – Registration instructions" for instructions on Re-Registering.

Q. Can I have the Microsoft Authenticator app on more than one device?
A. You can install Microsoft Authenticator App on more than one device. Ongoing it will prompt both devices with the needed authentication code and the user can select from whichever device they are currently using.

Q. What if I already have a Microsoft Authenticator Account for personal use, can it be used for Mayo Clinic too?
A. Yes, it can be used for both personal and work use. The user would need to enter their Mayo Clinic email versus their home email on the logon screen.

Q. Will the new Office365 Webmail require Microsoft Authenticator, if it’s accessed on campus?
A. No. It will only require MFA when external to the Mayo Clinic network.

Q. Will I need Mobile Device management (MDM) for this to work?
A. No. Microsoft Authenticator (Azure MFA) will be needed when users are outside the Mayo Clinic network and connecting to Office 365 to access their Mayo Clinic email and calendar while external to Mayo Clinic. Essentially, this will be the new version for Web Browser access to your Mayo Clinic Email (replacing mcmail.mayo.edu and imail.mayo.edu). This is independent from Mobile Device Management.

Q. Can I use the Microsoft Authenticator internationally?
A. Yes, Microsoft Authenticator can be used internationally. The app will work on their mobile device without having a Wi-Fi connection by using the following steps:
1. Click on “Sign in another way”

   ![Microsoft sign-in page](image1)

   Lastname.Firstname@mayo.edu

   Approve sign in request

   We've sent a notification to your mobile device.
   Please respond to continue.

   Having trouble? [Sign in another way]

   More information

2. Click on “Use verification code from my mobile app”

   ![Microsoft verification code page](image2)

   Lastname.Firstname@mayo.edu

   Verify your identity

   Approve a request on my Microsoft Authenticator app

   Use a verification code from my mobile app

   More information

   Cancel

3. Open "Microsoft Authenticator" app on your device

4. Enter the six-digit code from the app and click “Verify”

   ![Microsoft enter code page](image3)

   Lastname.Firstname@mayo.edu

   Enter code

   Please type in the code displayed on your authenticator app from your device

   Code

   More information

   Verify

**Q. During registration, what happens if the QR Code is not scanning?**
A. The scanning of the QR Code will be required to complete the registration of Microsoft Authentication. Most commonly issues related to scanning the QR Code involve:
- The phone moving too much during scanning
- The cursor being over the QR code
- Be patient, scanning could take up to 30 seconds
- Keep your device active so it's ready
If these tips don't help you to scan the QR code, it is recommended you start the registration process over.

Q. Is there a way for the Help Desk to use the verification code if the user is unable to scan the code?
A. The user will need to be logged in to the website "MFA Setup" (see Registration instructions), which would make it not possible for support staff to assist the user with this piece of the process.

Q. Would the Help Desk/Support Staff be able to go into an Admin portal that has a code and provide that to a user?
A. Unlike RSA SecurID, this option is not available. Our instance of Azure MFA is completely in the Cloud versus having on-prem servers (which would allow this option.)

Q. I am registering for Microsoft Authenticator using a non-Mayo Clinic device (aka Personal computer) and the process is not working according to the Registration instructions. What am I doing wrong?
A. Registration of Microsoft Authenticator (Azure MFA) instructs users to register while they are using a Mayo Clinic workstation; however, it is possible to use a personal computer as long as it is connected to the Internet.

Q. I am not at work. Is there a way I can register without being at a Mayo Clinic workstation?
A. It is possible to use a personal computer provided it is connected to the Internet.

Q. My registration steps didn’t work; it’s stuck on Step 2. It says: “We did not receive a response. Please try again.”
A. This may have occurred because the “Next” button was clicked instead of the “Set up” button on the previous screen prompt. Refer to Microsoft Authenticator (Azure MFA) Registration instructions.

Additional security verification

Step 2: Let’s make sure that we can reach you on your Mobile App device
We did not receive a response. Please try again.
Correlation ID: b38ec1bc-6754-4be9-b213-7b7444ad9bce
Session ID: 3107356-6828-48dd-b942-828ef05a026e
Timestamp: