
Employee Packet Basic Service

Basic Information Technology Services
Table of Contents

This Guide is for employees able to work by accessing web-based email, calendar, and web-based Microsoft OneDrive or SharePoint to perform remote work. Web-based Microsoft Office applications will look slightly different but maintains much of the same functionality as on-site access. Information regarding Telecommunications setup or changes as well as how to remotely join a Skype meeting from your online Office 365 calendar are included as well.

1. All employees must install Microsoft Authenticator to use Basic Services:
   1.1 Setup Microsoft Authenticator - Registration Instructions
   1.2 Microsoft Authenticator FAQ

2. If you are still on campus, please complete these steps for Basic Services:
   2.1 OneDrive Quick User Guide - Install
   2.2 For any Telecommunication related teleworking questions or requests please complete and submit the following form: Change Existing Phone or Line Features

3. Once you are working from home, complete these steps for Basic Services:
   3.1 Accessing Office 365 Applications Including Outlook
   3.2 Joining Skype Meeting via the Web
   3.3 Ready Access Audio-Only Telecom Information QRG
Setup Microsoft Authenticator – Registration Instructions

**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](image1)

   Once installed, the app icon will look like this:

   ![Authenticator Icon](image2)

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](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”.

---

**[Image of Microsoft Authenticator sign-in screen]**
4. You will then be presented with the “Additional Security Verification” prompt:

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
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 showing the mobile app setup process](image)

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

![Image showing the mobile app setup process](image)

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

![Image showing the 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”.

![Screen shot of approval prompt](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.
Microsoft Authenticator FAQ

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”

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

3. Open “Microsoft Authenticator” app on your device
4. Enter the six-digit code from the app and click “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.
Q. On Registration Step 1a, I get the following error:

Sorry, something went wrong...

Ensure that cookies are enabled then click sign out and try again.

A. This may be a cookie issue. Check these settings on IE:

Microsoft Internet Explorer 8.0 - 11.0
Select the 'Tools->Internet Options' menu item, and then open the 'Privacy' tab - you can then adjust the slider to block or allow various categories of cookie. Alternatively by clicking 'Advanced...' you can exercise finer control over the browser's behavior, choosing whether to accept, block, or prompt for cookies originating either on the website you are visiting (first party cookies) or originating from websites other than the one you are visiting (third party cookies, typically used by banner advertisements hosted on an advertiser's website).
Q. My phone is not getting the Azure push during registration and therefore it's failing.
A. This could be caused from an issue with the Wi-Fi that's being used; may be security in the Wi-Fi that's blocking. If possible, the user should switch their mobile device to use the mobile signal instead of the Wi-Fi signal and see if that resolves the issue.

Q. I have Registered successfully for Microsoft Authenticator (Azure MFA). I'm now trying to access O365 by going to https://office.com (workstation). The link isn't working for me - I'm getting this error?

 adapté

Something went wrong

We couldn’t find a mailbox for this recipient. Either they don’t have a mailbox or don’t have a license assigned.

More details...

Refresh the page

A. This error message is the result of your Mayo Clinic email account failing to migrate.
OneDrive Quick User Guide

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

2. Your first time to this page, it will appear like the picture below, please click on “Sign in”. If it does not, or it signs you into a non-Mayo account, please log out in the upper right, and at the first page, please choose “Switch to a different account”. If it brings up a screen with “Pick an account”, and your Mayo Clinic email address is available, please select it to continue.

3. Click on the OneDrive app to open it.
4. You will want to save any files, that you wish to have access to while off-site, to your OneDrive. This is your network (Cloud) storage, that you can access from anywhere you have an Internet connection.

5. To upload your files, click on Upload > Files in the OneDrive toolbar to browse for your files.

6. If the files are located on your personal drive (H:/U:), you will want to select that location from the left-hand side of the window and then select the file(s) you wish to add. If they are located on the desktop or another folder, you will need to select that location from the left-hand side as well. Note: You may select/deselect multiple files in the location by holding the ctrl key on your keyboard and then clicking on the files. Click “Open”.

Repeat this step for all files you wish to upload or will need access to while off-site.

For more information on how to utilize OneDrive, please see the Microsoft user guide:

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”

![Microsoft Sign in](image1)

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”

![Microsoft Enter password](image2)

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”

![Microsoft Authenticator](image3)
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/.
Joining Skype Meeting via the Web

You can join Skype for Business meetings via the web using Microsoft’s Skype meeting web app.

First you must configure your audio devices to work with Windows. See your computer manufacturer or documentation for assistance.

It is recommended to have both speaker/headphone and a microphone for full audio participation. However you can join and just type in the meeting chat if you are unable to speak.

Skype for Business meetings will have an invite that looks like this:

Join Skype Meeting
Trouble Joining? Try Skype Web App

Join by phone

+1 (507) 293-0000,123456# (Minnesota)   English (United States)

Find a local number

Conference ID: 123456

Forgot your dial-in PIN? Help

If you only need audio, and the Skype meeting has the “join by phone” section, call 1-(507)293-0000 from any phone and use the conference ID listed followed by the # sign to join the meeting by phone with audio only.

If your meeting does not have the phone section, or you need to view video or shared material, perform the following steps.

1. Click on the “Try Skype Web App” link.
2. This should launch your default browser. Click on “Install and join with Skype Meetings App (web)”
   - Note: If you have already installed this plugin, you can click the word “here” where it says “Already installed? Click here to join with Skype Meeting App (web)”.

3. This will bring up the save/run dialog for your browser. You must run and install this plugin to connect to the meeting.

4. Once installed, your browser will show you the “All Set!” page, please click “join the meeting” where it says “Try to join the meeting again”.

3/15/2020 4:19 PM
5. If Skype presents a pop-up that asks if you want to join the meeting, please select “Yes”. You may also want to check the box for “Always join meetings from this address”.

6. Next is the Welcome screen. You can click below the field on the line that says “Sign in if you are from the organizer’s company”, or you can fill out your name and click “Join”. It’s advised you use your first name and last name for identification purposes.
7. If you chose “Sign in if you are from the organizer’s company”, enter in your LANID and password used to log in to your computer on campus. You will need to include “mfad\" before your LAN ID.

8. You will then either be placed into a Virtual Lobby to wait for someone else in the meeting to accept you in (just entered your name), or will be placed automatically into the meeting (entered your LAN ID and password).

9. Enjoy your meeting!

10. Once the meeting is complete, just close the window, and the “Join Meeting” browser window. You will want to open a new window for your next Skype meeting.
Scheduling a Ready Access audio-only teleconference

1. Get the Chairperson information:
   Example: 866-365-4406 7-digit access code 1234567
2. Create an “Invitation Template”
   Example:
   Please join John Doe to Discuss Collaboration Tools Teleconference: December 24, 2012, at 4-5 pm CST.
   Ready Access #: 866-365-4406
   7 Digit Access Code #: 1234567
   Include any other agenda items or details
   For assistance during the meeting, dial "00" or call 1-888-447-1119
3. Schedule meeting in OUTLOOK and include the "Invitation Template"

Starting a Ready Access audio-only teleconference

When it is time for the conference call, the Chairperson:
1. Dials the Ready Access Phone Number, 866-365-4406.
2. Enters the 7-digit access code.
3. When prompted, identifies oneself as the Chairperson, and follows the recorded prompts.
4. Enters the chair pass code for security.

When it is time for the conference call, the Participants:
1. Dials the Ready Access Phone Number, 866-365-4406.
2. Enters the Seven Digit Access Number.
3. Waits (will be placed on hold) until the chairperson arrives to start the conference.

For assistance during the meeting, dial "00" or call 1-800-473-0602

Changing your Ready Access Passcode

1. Dial the conference number, 866-365-4406.
2. Enter your 7-digit access code followed by #
3. Press *
4. Enter current Chairperson Passcode followed by #
5. Press 2 for "Account Options"
6. Press 1 to “Change Chairperson Passcode”
7. Enter new passcode (four to nine digits in length), followed by #
   NOTE: Avoid repeating digits, and the same number as your extension number
8. Listen for confirmation, then hang up or press the * key to start your conference
   The system will then verify your new passcode and return you to "Account Options".

Call Charges
The cost to utilize the Ready Access Teleconference service is $.0125 per minute per “connection” within the United States.
Example - Five separate callers plus the Chairperson equals six connections. If they have a 60 minute teleconference, the charges would be:
Six (connections) X Sixty (minutes) X $.0125 per minute = $4.50.
Charges begin when the chairperson starts the call and end when the chairperson disconnects the call.