



The first-time users remotely login to a UMHW view session, they'll be required to register Multi-Factor Authentication.

Step 1:

From your mobile device

Obtain the Microsoft Authenticator App from the App Store or Google/Android Play Store. If you already have the Microsoft Authenticator App, move to step 2.

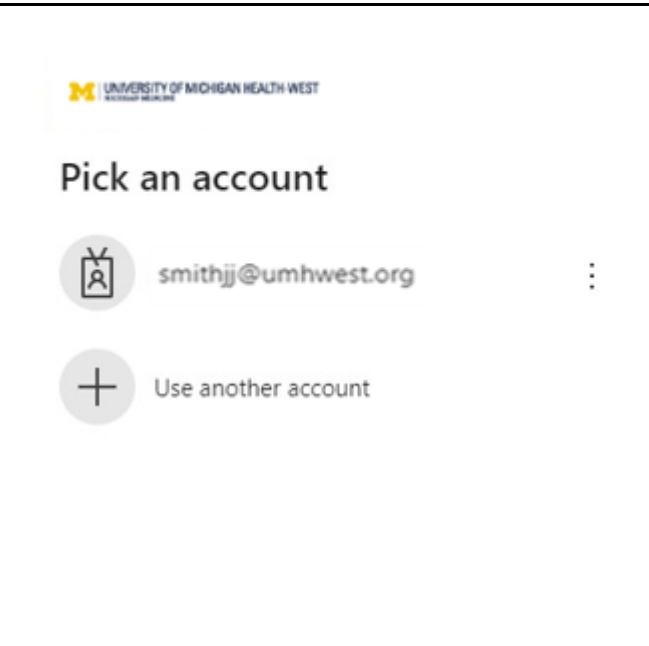


Step 2:

On Your Computer:

You may be prompted to pick an account. Pick your UMHW account or select "Use another account" if you don't see your UMHW account isn't listed.

If you get an error stating we're having trouble signing you in see common errors section page 7





Step 3:

Follow the Microsoft Sign In process.

You must sign in using your username@umhwest.org

Example –

SmithJJ@umhwest.org



Sign in

username@umhwest.org

[Can't access your account?](#)

Back

Next

Step 4:

Enter your UMHW network password and choose “Sign In”.



← smithjj@umhwest.org

Enter password

Password

[Forgot my password](#)

Sign in

Step 5:

Choose “Next” at the screen stating more information is required.



smithjj@umhwest.org

More information required


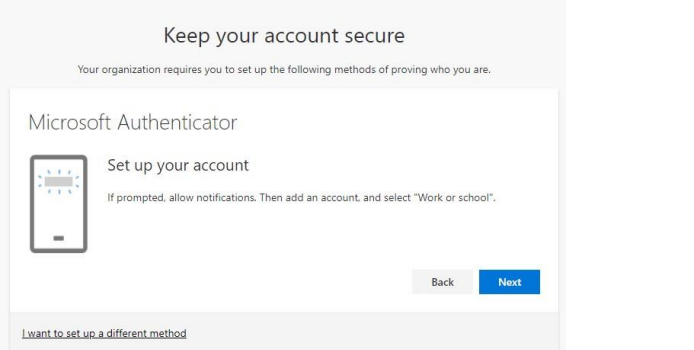
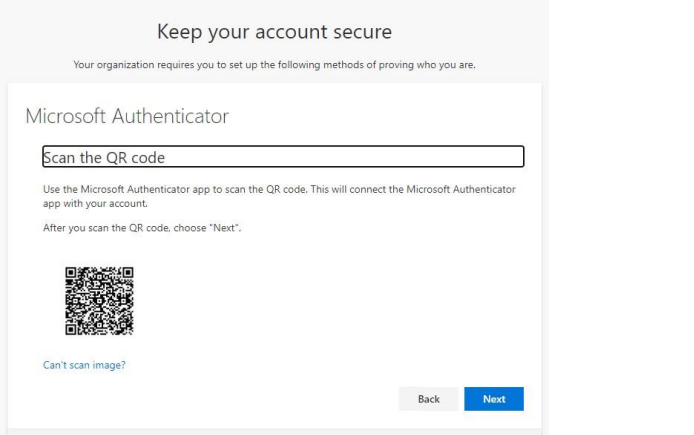
Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next



<p>Step 6:</p> <p>You will be presented with the following screen. Please leave the default settings selected for the Microsoft Authenticator App.</p> <p>Select Next.</p>	 <p>The screenshot shows the Microsoft Authenticator app installation screen. It has the title 'Microsoft Authenticator' and the heading 'Start by getting the app'. Below this, there is a small icon of a smartphone with a blue shield. The text reads: 'On your phone, install the Microsoft Authenticator app. Download now'. Below that, it says 'After you install the Microsoft Authenticator app on your device, choose "Next".' and 'I want to use a different authenticator app'. At the bottom right, there is a blue 'Next' button. At the bottom left, there is a link: 'I want to set up a different method'.</p>
<p>Step 7:</p> <p>You will be presented with the following screen. Please leave the default settings selected for the Microsoft Authenticator App.</p> <p>Select Next.</p>	 <p>The screenshot shows a 'Keep your account secure' screen. It has the heading 'Keep your account secure' and a sub-heading 'Your organization requires you to set up the following methods of proving who you are.' Below this, there is a box titled 'Microsoft Authenticator' with the heading 'Set up your account'. It says 'If prompted, allow notifications. Then add an account, and select "Work or school".' At the bottom right, there are 'Back' and 'Next' buttons. At the bottom left, there is a link: 'I want to set up a different method'.</p>
<p>Step 8:</p> <p>You will be presented with the similar screen. Please leave the default settings selected for the Microsoft Authenticator App.</p> <p>Proceed to step 9</p> <p>**DO NOT HIT NEXT UNTIL YOU HAVE SUCCESSFULLY SCANNED YOUR PERSONAL QR CODE – THIS WILL BE DETAILED IN STEP 13**</p>	 <p>The screenshot shows a 'Keep your account secure' screen. It has the heading 'Keep your account secure' and a sub-heading 'Your organization requires you to set up the following methods of proving who you are.' Below this, there is a box titled 'Microsoft Authenticator' with the heading 'Scan the QR code'. It says 'Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.' and 'After you scan the QR code, choose "Next".' Below the text is a QR code. At the bottom left, there is a link: 'Can't scan image?'. At the bottom right, there are 'Back' and 'Next' buttons.</p>



Step 9:

On your mobile device:

Open the Authenticator app on your mobile device.

** At any point the authenticator may ask for permissions to send notifications, please select allow. This allows the authenticator to send push notifications for access approval.

At any point the authenticator may ask for permissions to access the camera, please select allow. This allows the authenticator to use your camera to scan QR codes **



Microsoft Authenticator - Ap...

Step 10:

Choose +

If you are already using the Microsoft Authenticator App for any other accounts, also select the "+" symbol.



Ready to add your first account?

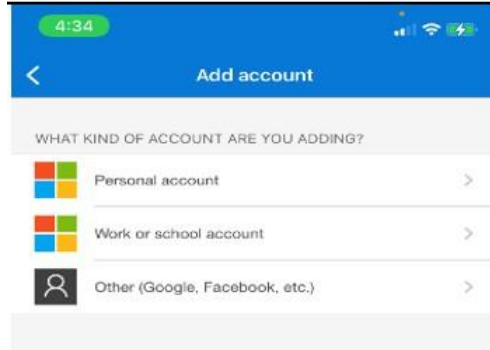


Add account



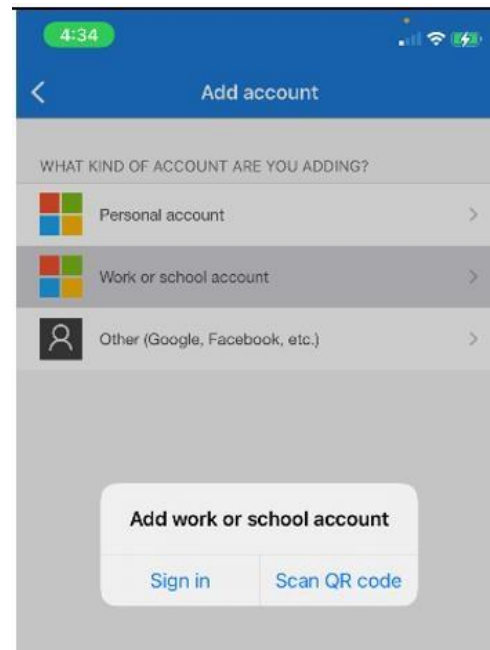
Step 11:

Choose "Work or school account".



Step 12:

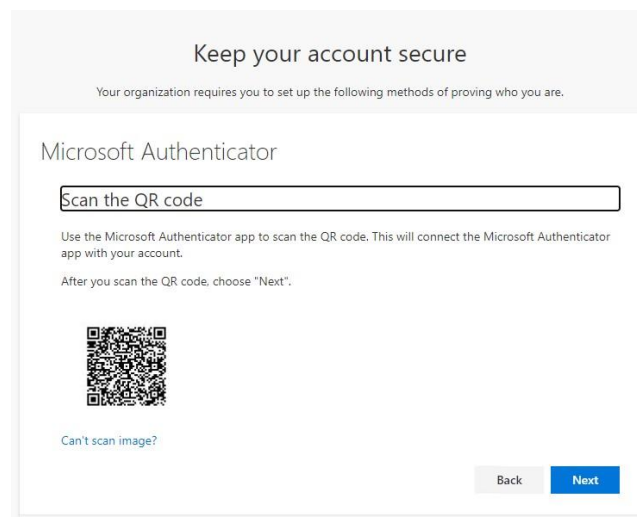
The notification to scan the QR code will appear. Select "Scan QR Code".



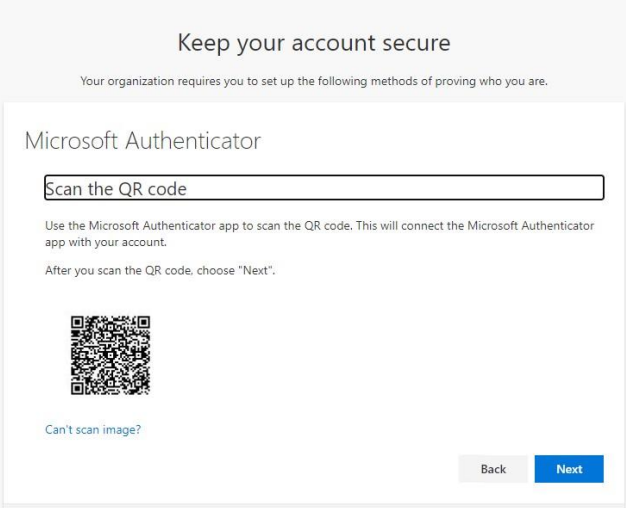
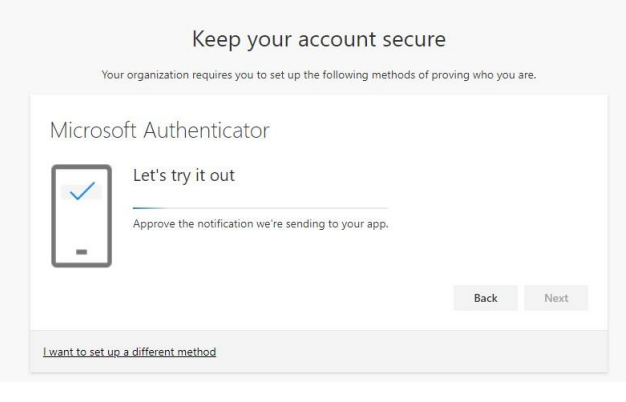
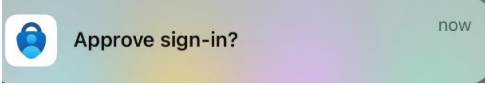
Step 13:

Using your mobile device scan the QR code displayed on your computer browser using the authenticator application.

After scanning you should now see your account populate on the authenticator application.





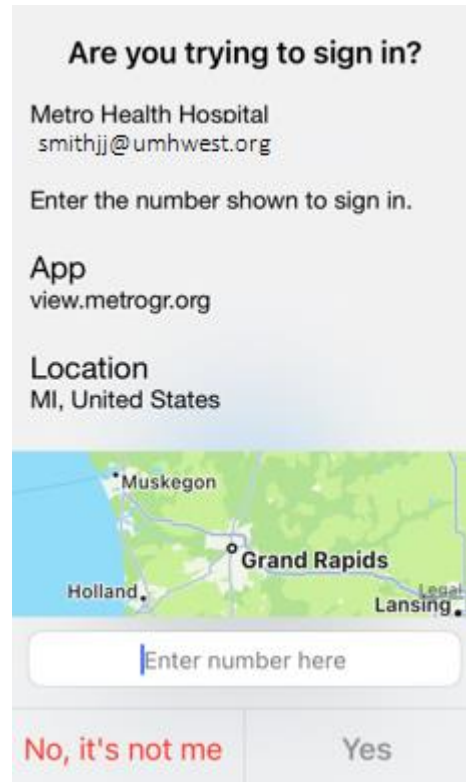
<p>Step 14:</p> <p>From your view session or onsite computer</p> <p>Select "Next" from the browser window.</p>	 <p>The screenshot shows a web page titled "Keep your account secure" with the subtext "Your organization requires you to set up the following methods of proving who you are." Below this is a "Microsoft Authenticator" section with a text input field labeled "Scan the QR code". Below the field is a QR code and the text "Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account. After you scan the QR code, choose 'Next'." At the bottom right are "Back" and "Next" buttons.</p>
<p>Step 15:</p> <p>Microsoft will send an approval request to your mobile device to verify the two-factor authentication functionality is working as expected.</p>	 <p>The screenshot shows a web page titled "Keep your account secure" with the subtext "Your organization requires you to set up the following methods of proving who you are." Below this is a "Microsoft Authenticator" section with a checkmark icon and the text "Let's try it out" and "Approve the notification we're sending to your app." At the bottom right are "Back" and "Next" buttons. At the bottom left is a link "I want to set up a different method".</p>
<p>Step 16:</p> <p>From your mobile device</p> <p>Open the push notification received.</p>	 <p>The screenshot shows a mobile push notification with a blue checkmark icon and the text "Approve sign-in?" and "now".</p>



Step 17:

From your mobile device

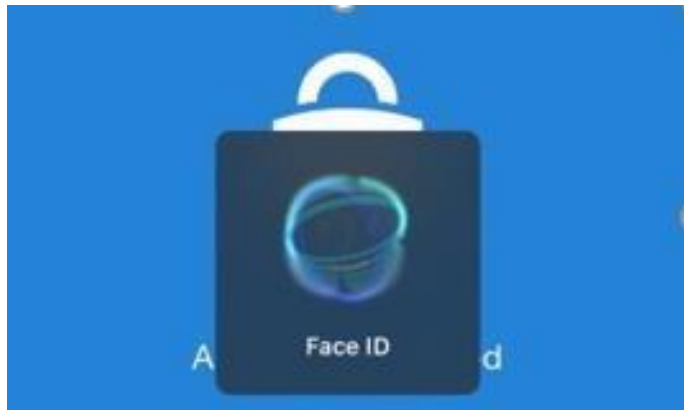
Enter the number displayed on the computer screen and select **Yes**.



You may be prompted to scan Biometrics or enter a Device Pin depending on the configuration within the Microsoft Authenticator App – App Lock settings.

App Lock also helps ensure that you're the only one who can approve notifications by prompting for your PIN or biometric any time you approve a sign-in notification. You can turn App Lock on or off on the Authenticator Settings page.

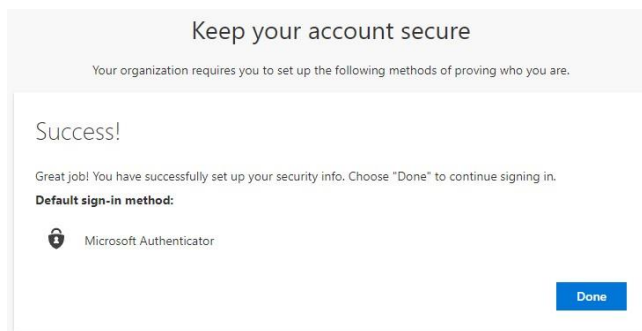
By default, App Lock is turned on when you set up a PIN or biometric on your device.



Step 18:

From your view session or onsite computer

Once you've approved the notification, select "Next".





Step 18:

You will be presented with the following screen.

Great job! You have successfully set up your security info.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

 Microsoft Authenticator

Done



Common Errors & Trouble Shooting

1. Sorry, but we're having trouble signing you in. – Does not exist in tenant.

Sign in

Sorry, but we're having trouble signing you in.

AADSTS90072: User account 'yr11@ s.edu' from identity provider 'https://sts.windows.net/64b0362e-85c0-4e95-a4ce-5651d96cb739/' does not exist in tenant 'Metro Health Hospital' and cannot access the application 'https://view.metrogr.org/portal'(view.metrogr.org) in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account

Troubleshooting details

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Request Id: 28edc87d-8f45-4aa3-9b13-ca8b0df2ce00

Correlation Id: 1344dc88-1eb5-4529-9ceb-aa46b6eee02c

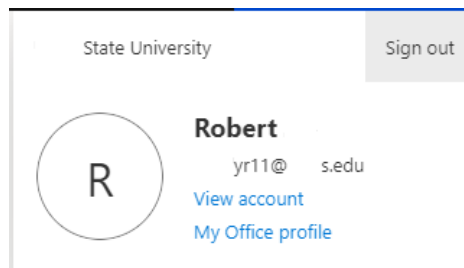
Timestamp: 2021-08-01T18:33:25Z

Message: AADSTS90072: User account 'yr11@ s.edu' from identity provider 'https://sts.windows.net/64b0362e-85c0-4e95-a4ce-5651d96cb739/' does not exist in tenant 'Metro Health Hospital' and cannot access the application 'https://view.metrogr.org/portal'(view.metrogr.org) in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account

Flag sign-in errors for review: [Enable flagging](#)

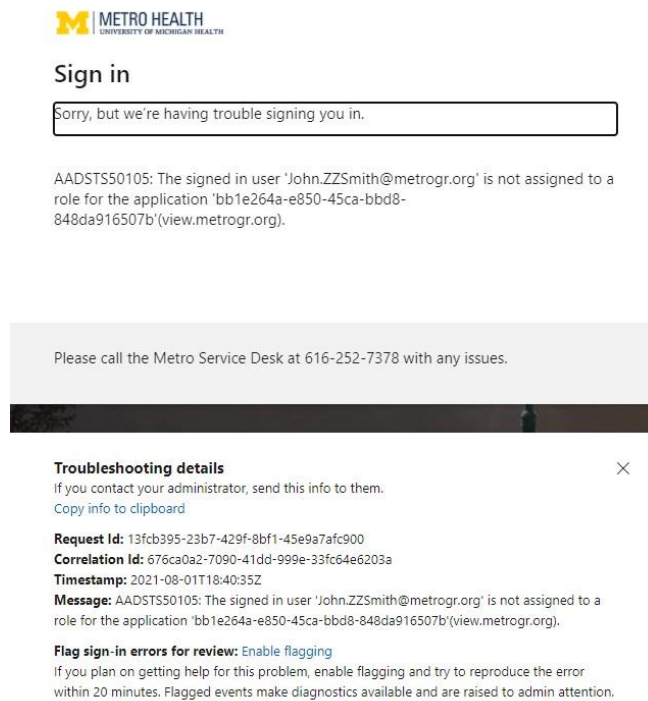
If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

The user trying is trying to authenticate to the Metro View Application while being signed into another account – for example a school, work, or personal Office 365 account. To fix this visit <https://portal.office.com> select your account in the top right of your browser and sign out.



Once your successfully logged out, please try again.

2. Sorry, but we're having trouble signing you in. – is not assigned to a role.

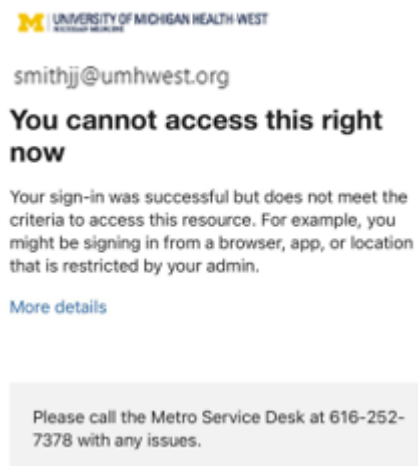


The screenshot shows a Metro Health login page with the following content:

- M METRO HEALTH** UNIVERSITY OF MICHIGAN HEALTH
- Sign in**
- A text box containing the message: "Sorry, but we're having trouble signing you in."
- A message: "AADSTS50105: The signed in user 'John.ZZSmith@metrogr.org' is not assigned to a role for the application 'bb1e264a-e850-45ca-bbd8-848da916507b'(view.metrogr.org)."
- A grey box with the text: "Please call the Metro Service Desk at 616-252-7378 with any issues."
- Troubleshooting details** (with a close button 'X')
 - If you contact your administrator, send this info to them.
 - Copy info to clipboard
 - Request Id:** 13fcb395-23b7-429f-8bf1-45e9a7afc900
 - Correlation Id:** 676ca0a2-7090-41dd-999e-33fc64e6203a
 - Timestamp:** 2021-08-01T18:40:35Z
 - Message:** AADSTS50105: The signed in user 'John.ZZSmith@metrogr.org' is not assigned to a role for the application 'bb1e264a-e850-45ca-bbd8-848da916507b'(view.metrogr.org).
 - Flag sign-in errors for review:** [Enable flagging](#)
 - If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

The user is not allowed to login remotely. Please contact your manager/Director for assistance.

3. You cannot access this right now.



The screenshot shows a Metro Health login page with the following content:

- M UNIVERSITY OF MICHIGAN HEALTH WEST** MICHIGAN MEDICINE
- smithjj@umhwest.org
- You cannot access this right now**
- Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.
- [More details](#)
- A grey box with the text: "Please call the Metro Service Desk at 616-252-7378 with any issues."

User sign in was successful – but from an un-allowed device. The only way to register 2FA is through mobile application QR code scanning.

4. I'm trying to login directly from the mobile application.



Users are not allowed to login directly to the phone application. The only way to register 2FA through the mobile application is QR code scanning.

5. My App isn't working, and phone continually spins.

- Close your browser or view client.
- Begin registration process again, but at step 6 select-I want to setup a different method.
- Follow prompts to set up phone>SMS texting

Microsoft Authenticator



Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

Next

[I want to set up a different method](#)

