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

<table>
<thead>
<tr>
<th>Step 1:</th>
</tr>
</thead>
<tbody>
<tr>
<td>From your mobile device</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Your Computer:</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

*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

Step 4:
Enter your UMHW network password and choose “Sign In”.

Step 5:
Choose “Next” at the screen stating more information is required.
Step 6:
You will be presented with the following screen. **Please leave the default settings selected for the Microsoft Authenticator App.**
Select Next.

Step 7:
You will be presented with the following screen. Please leave the default settings selected for the Microsoft Authenticator App.
Select Next.

Step 8:
You will be presented with the similar screen. Please leave the default settings selected for the Microsoft Authenticator App.

Proceed to step 9

**DO NOT HIT NEXT UNTIL YOU HAVE SUCCESSFULLY SCANNED YOUR PERSONAL QR CODE – THIS WILL BE DETAILED IN STEP 13**
**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.

**Step 10:**

Choose +

If you are already using the Microsoft Authenticator App for any other accounts, also select the “+” symbol.
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.
Step 14:
From your view session or onsite computer
Select “Next” from the browser window.

Step 15:
Microsoft will send an approval request to your mobile device to verify the two-factor authentication functionality is working as expected.

Step 16:
From your mobile device
Open the push notification received.
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”.

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:

Expressed by: Microsoft Authenticator
Step 18:
You will be presented with the following screen.

Great job! You have successfully set up your security info.
Common Errors & Trouble Shooting

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

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

3. You cannot access this right now.

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