

FMOLHS Azure Multi-Factor Authentication Instructions

AZURE MULTI-FACTOR AUTHENTICATION (MFA)

On **Tuesday, May 30, 2023**, FMOLHS will change multi-Factor authentication from Imprivata MFA to Microsoft Azure MFA. Between **November 1, 2022 – May 30, 2023**, Team Members will have an opportunity to enroll in Azure Multi-Factor Authentication by using the below instructions.

By enrolling in Azure MFA, you will be able to utilize Self Service Password Reset (SSPR). This tool will allow you to reset your password without having to call the IS Support Center/Help Desk.

SAFEGUARDING OUR MINISTRY

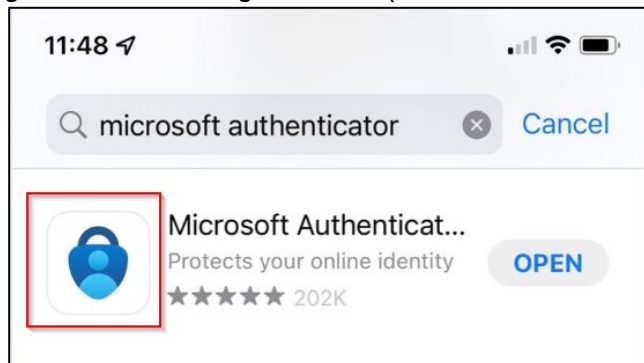
- Never share your password, with anyone!
- Never approve an MFA prompt if you didn't initiate it (An attacker could be trying to use your login).
- Never post sensitive information on social media. This includes pictures where screens are visible in the background.

Keep all assets safe by:

- Never leaving devices unattended such as laptops, in a car unattended.
- Being sure that information accessed at home is not viewed by family or friends.
- Use the *Report Phishing* button to report an email you think is suspicious – Never click links in emails where you aren't familiar with the sender.

STEP 1 - PHONE

Download and install the Microsoft Authenticator App on your phone. You may already have the application installed if you are using it for another organization (i.e. school or bank).

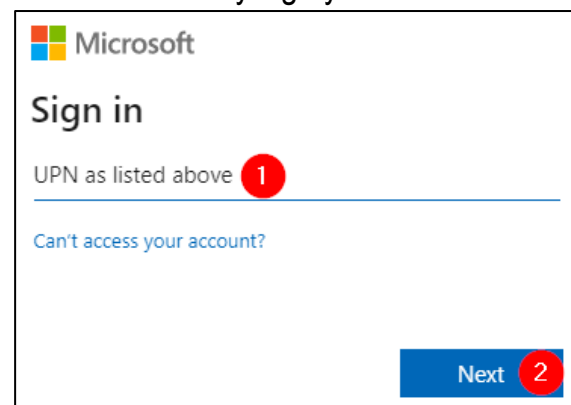


Do not download the authenticator App. It will ask you for to pay for a subscription. This is not the right application.



STEP 2 - COMPUTER

On your computer, go to <https://mysignins.microsoft.com/security-info> and Login with your username/password. If you are already on the FMOLHS network, it will automatically sign you in.



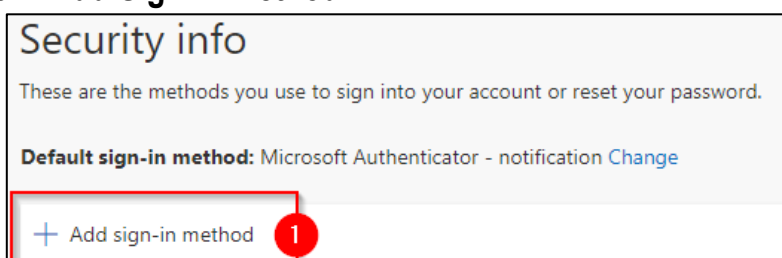
ENROLL 2 METHODS

You will need to **Register 2 methods** for MFA. You'll need to register the Microsoft Authenticator Application on your phone and choose one from the choices provided.

After selecting your first method, you will have to click "+ Add sign-in method" again to add the second method. - We require two methods, but you can add more if needed.

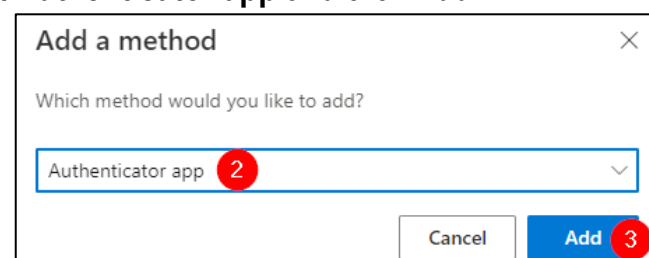
STEP 3 - COMPUTER

Click **+Add Sign-in method**



STEP 4 - COMPUTER

Select **Authenticator app** and click **Add**.

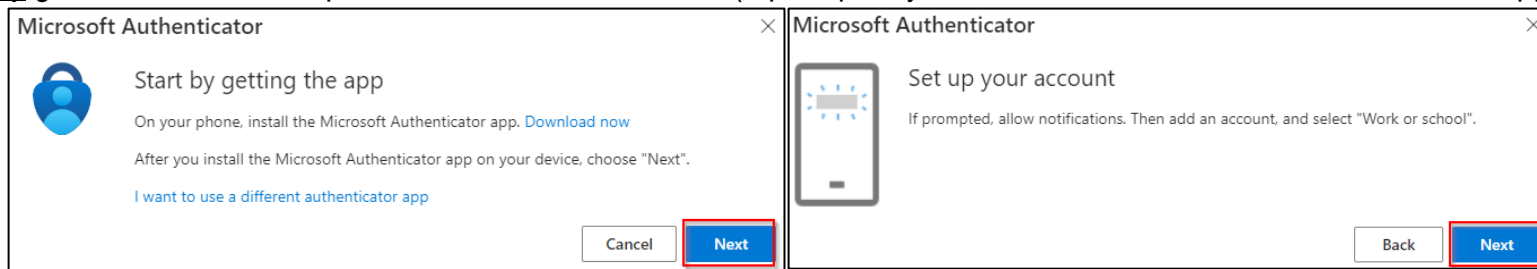


The IS Support Center can be reached 24 hours a day, 7 days a week, by phone at (866) 532-4772 or online at <http://issc>.

AZURE MFA INSTRUCTIONS

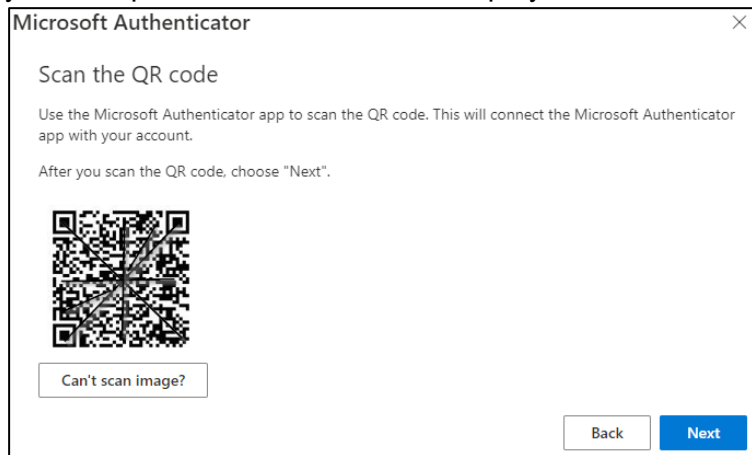
STEP 5 - COMPUTER

You may get asked these two questions. Click **Next** on both. (If prompted you will need to allow notifications from this app.)



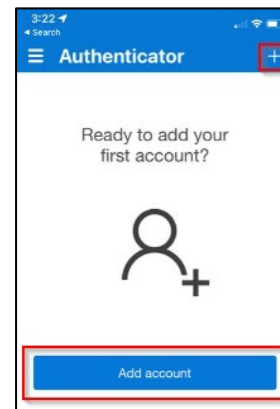
STEP 6 - COMPUTER

On your computer, the QR code will display.



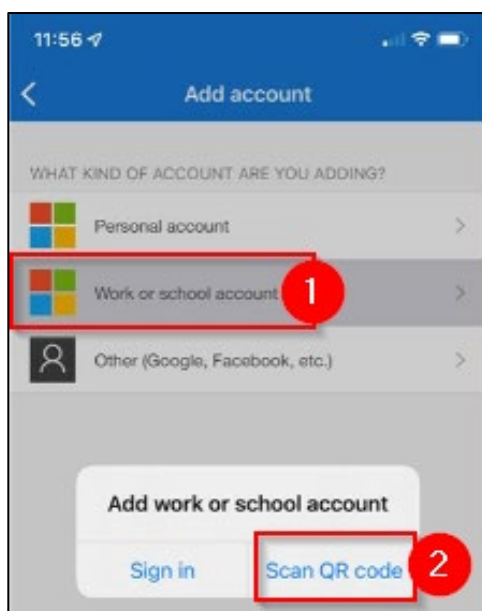
STEP 7 - PHONE

Open the app on your phone and click **Add Account** or the + in the upper right-hand corner.



STEP 8 - PHONE

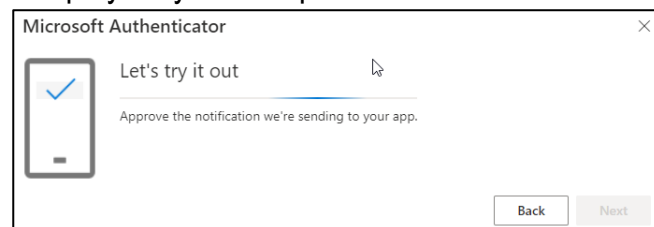
1. Click **Work or school Account**
2. Click **Scan QR code**.
3. Scan the QR code displayed on your computer using your camera on your phone and click **Next** on your screen.



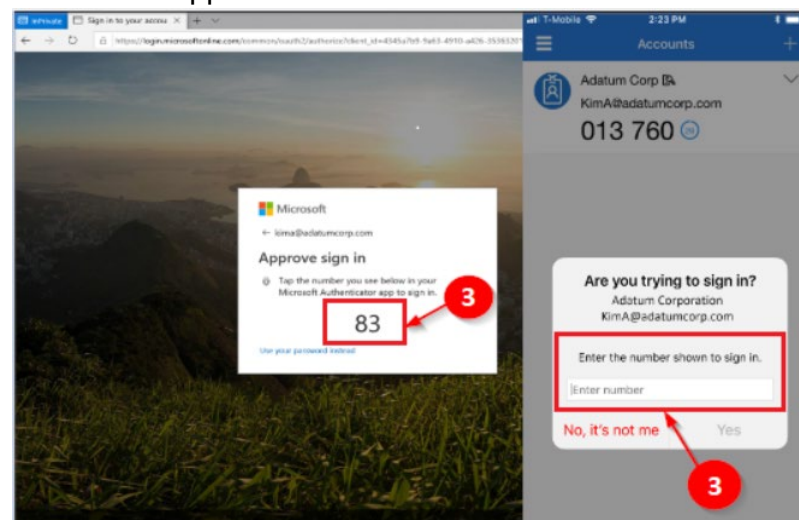
STEP 9 - PHONE & COMPUTER

Click **Approve** to accept the approval notification.

This will display on your computer:



A unique number will display on your computer. Type the unique number displayed on your computer into Microsoft Authenticator app.



STEP 10 - COMPUTER

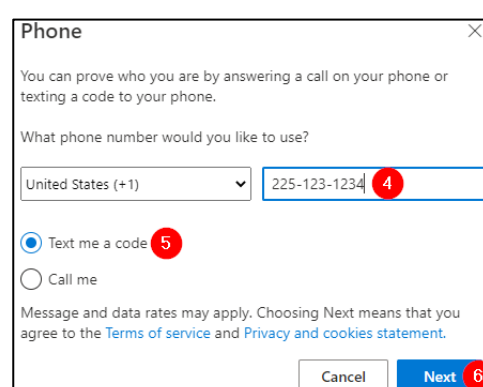
On your computer, Enroll **2nd Sign-in Method**:
On Main screen, click **+Add sign-in method**.

In this example, we are choosing **Phone**. You can choose any **second authentication method**.

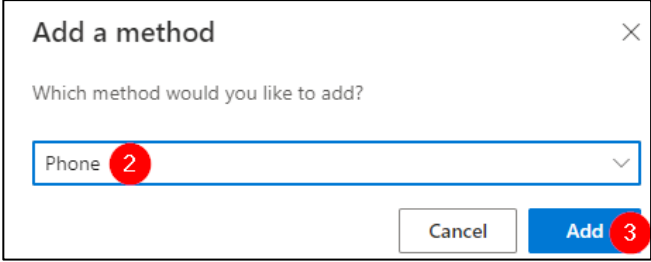
Use the drop-down menu and choose **Phone**.

STEP 11 - COMPUTER

Enter your phone number with area code and Click **Text me a code**.

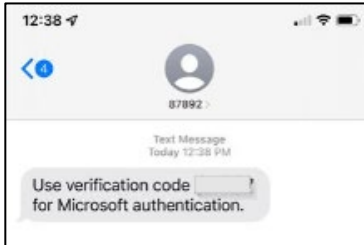


AZURE MFA INSTRUCTIONS

 <p>Add a method</p> <p>Which method would you like to add?</p> <p>Phone 2</p> <p>Cancel Add 3</p>	
---	--

STEP 12 - PHONE

On your phone, a code was texted to you. Use the code that is texted to you and put it in the box on your computer.



STEP 13 - COMPUTER

On your computer, Click **Done**. You can register more methods if you choose. Only two authentication methods are required.

