

Azure Multi-Factor Authentication Registration

(formally Microsoft Sign-in Verification tool)

In our continuing efforts to enhance the security of critical data, Main Line Health is improving safeguards to access data and applications. Azure MFA provides additional security by requiring a second form of authentication for external access to MLH provided applications (i.e., Self Service, VPN, access.mlhs.org, Office 365) when accessed from outside the MLH network.

Please Note: A mobile phone or pager will be required

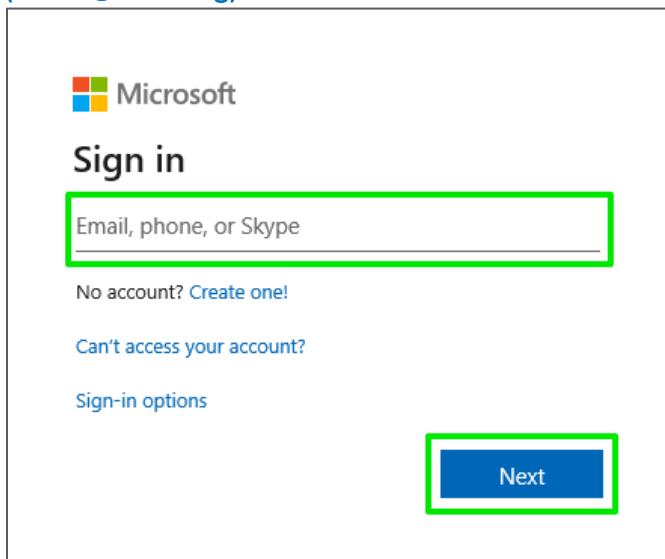
All external access to MLH provided applications (e.g., Employee Self Service, Office 365) requires the use of a two-factor authentication tool: now Azure cloud MFA. At the time when you access Employee Self Service remotely, Azure MFA will automatically contact you via a text message to your smartphone or pager. Once that step is completed, you will have access to logon to Employee Self Service or other MLH-provided apps. **Please refer to the instruction below for setting up your Azure Multi-Factor Authentication Registration.**

******These instructions are specific to MFA Registration ONLY******

No other login methods have been modified (i.e., Citrix logins, AnyConnect) and will remain as they were prior to this MFA remote access upgrade.

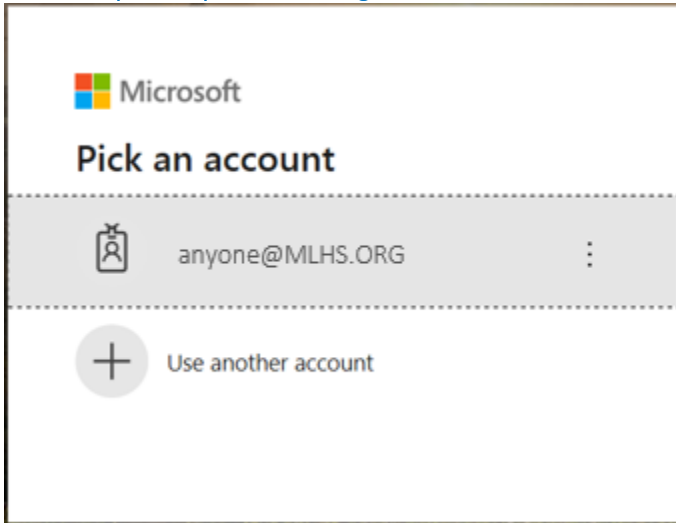
Initial registration process instructions

1. Connect to <https://aka.ms/mfasetup>
2. Enter your **MLH email address** (yourname@mlhs.org) and click **Next**
Please note: If you do not have an MLH email address, enter your windows logon + @mlhs.org (zabcd@mlhs.org)



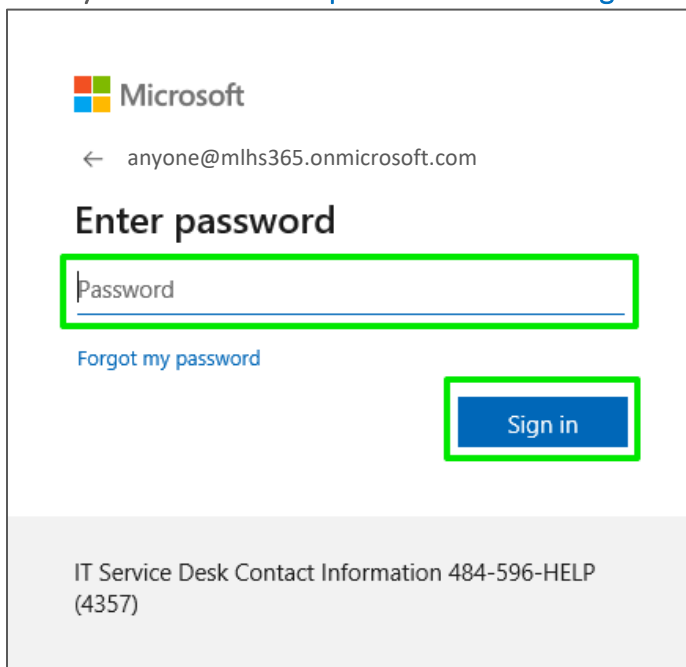
The screenshot shows the Microsoft sign-in interface. At the top left is the Microsoft logo. Below it is the heading 'Sign in'. There is a text input field with the placeholder text 'Email, phone, or Skype'. Below the input field are three links: 'No account? Create one!', 'Can't access your account?', and 'Sign-in options'. At the bottom right is a blue button labeled 'Next'. The input field and the 'Next' button are highlighted with green rectangular boxes.

Or if you previously logged in to Office 365, Online Outlook, SharePoint, but had not yet registered for MFA, you may see the image below:

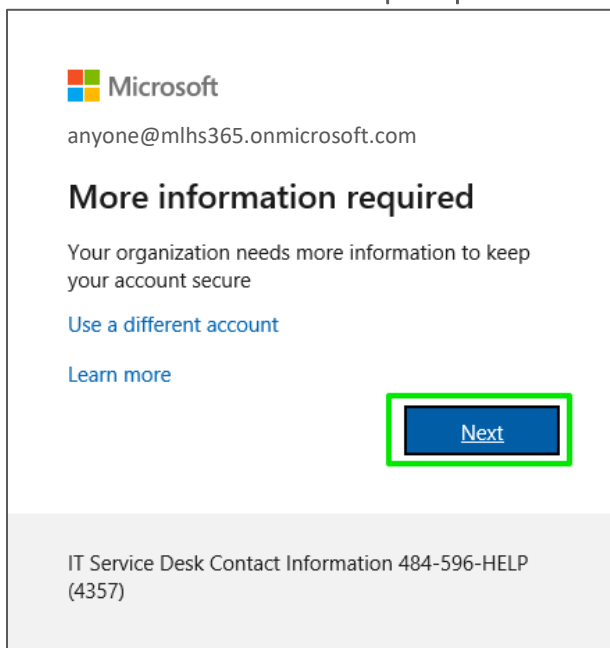


(If your account is not listed, Select Use another account, and follow the on-screen prompts)

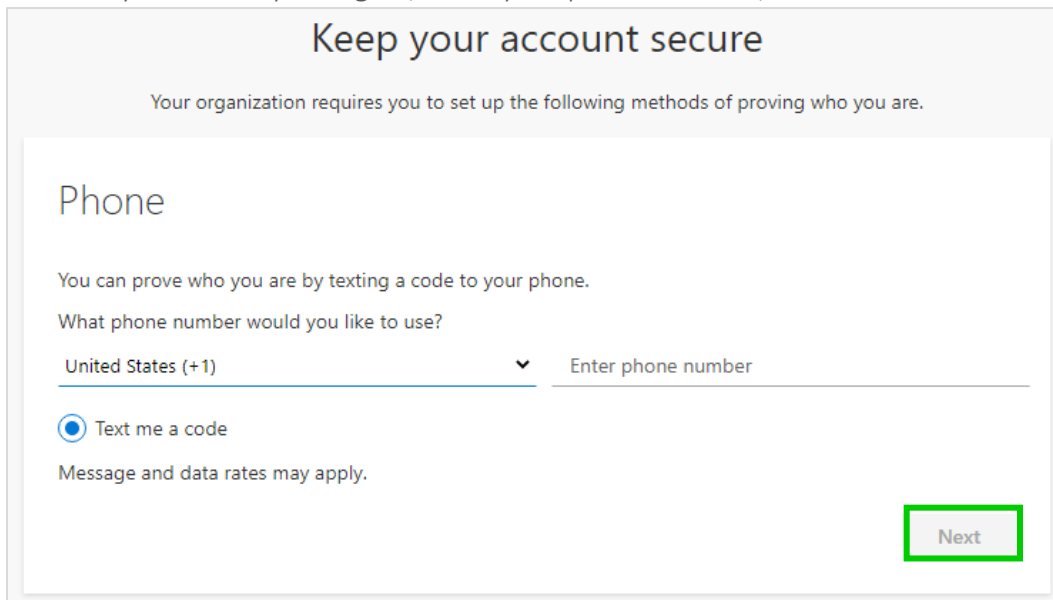
3. Enter your [MLH network password](#) and click [Sign in](#)



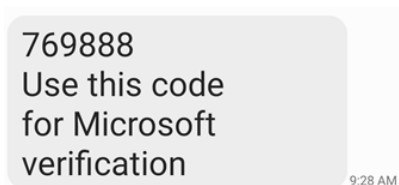
4. Click **Next** at this information prompt



5. You will be prompted to add a phone number to secure your account
- a. Insert the mobile phone number or device contact number you wish to use for account security.
 - b. Select your country or region, enter your phone number, and click **Next**.



6. On the mobile phone or pager you will receive a security verification text message – this could be from random numbers (example: 97671, 69829 etc.)



7. Enter the security code that appears on your screen – and select [Next](#).

Keep your account secure

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

Phone

We just sent a 6 digit code to +1 1234567890. Enter the code below.

Enter code

[Resend code](#)

Back Next

8. You should receive 'SMS Verified!' message below Click [Next](#).

Keep your account secure

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

Phone

✓ SMS verified. Your phone was registered successfully

Next

9. Once you have received the 'Success!' message below, you will have successfully completed your Azure MFA registration. Click [Done](#).

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: Phone - text 1234567890

Phone
+1 1234567890

Done

Still need Help or have additional questions?

Please contact the IT Service Desk at 484.596.4357 with any questions or forward an email to helpdesk@mlhs.org.