

Overview:

Multi-Factor Authentication (MFA) is an additional method of confirming who you are when you log on to Southlake computer systems (including email) from a remote location. The primary factor for authentication that you normally use is your username and password. This factor is “something you know.” The second factor is “something you have”. In our case, we are enabling the use of mobile phones as that second factor for the convenience of authorized individuals. When you use both of these methods together, it provides MFA. This is not required when you access systems onsite.

At Southlake, MFA may be required when accessing a computer system that contains sensitive information like Personal Health Information (PHI) from outside our protected internal network (such as your home, or off-site office). MFA helps protect our sensitive information by providing additional assurance of your identity. This has become a standard security measure across organizations.

Enrollment Process:

For the next steps, **you will need your smart phone and a computer.**

1. First, download the Microsoft Authenticator App on your smart phone. You can find the app in the Apple App Store for iPhone, or Google Play Store for Android. It may look slightly different, depending on your device.

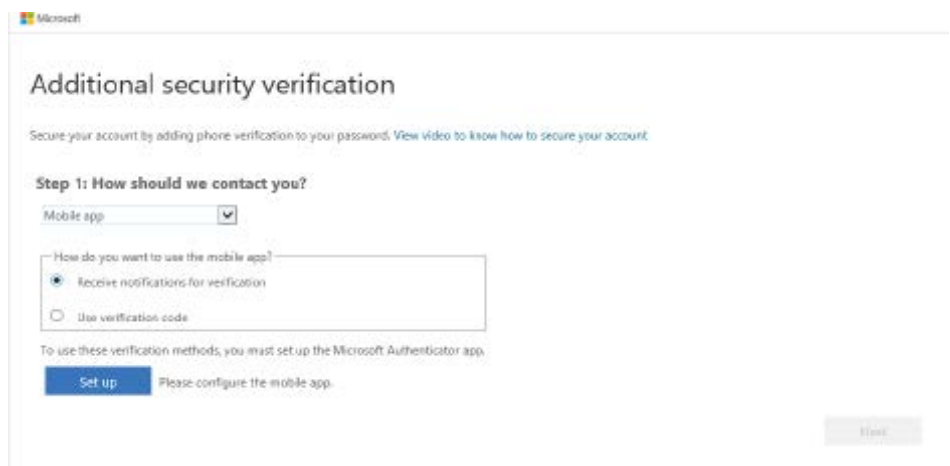


Microsoft Authenticator 
Microsoft Corporation
#33 in Productivity
★★★★★ 4.7, 315 Ratings
Free



2. On your computer, browse to the Multi-Factor Authentication User Portal: <https://aka.ms/mfasetup>
 - ▶ Logon with your Southlake network/email User ID and Password.

3. You will see this screen (left). Select the first option “Receive notifications for verification” and click on “Set up”:

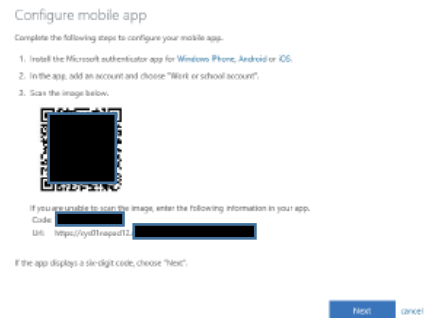


The screenshot shows the Microsoft Authenticator setup page. The title is "Additional security verification". Below the title, it says "Secure your account by adding phone verification to your password. View video to know how to secure your account." The main heading is "Step 1: How should we contact you?". There is a dropdown menu for "Mobile app" with a downward arrow. Below that, there is a section "How do you want to use the mobile app?" with two radio button options: "Receive notifications for verification" (which is selected) and "Use verification code". At the bottom, there is a blue "Set up" button and a note: "To use these verification methods, you must set up the Microsoft Authenticator app." There is also a "Next" button in the bottom right corner.

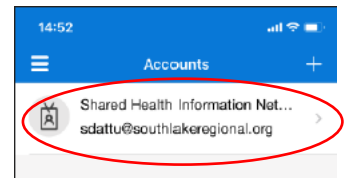
4. Launch the Microsoft Authenticator App on your smart phone.
5. Select “Add Account”, then select “Work or School Account”.

- The Microsoft Authenticator App will prompt you to scan the QR code. Please point your smart phone camera to the QR code on your monitor screen.

PLEASE SCAN THE QR CODE FROM YOUR COMPUTER SCREEN AND NOT QR CODE ON THESE INSTRUCTIONS.

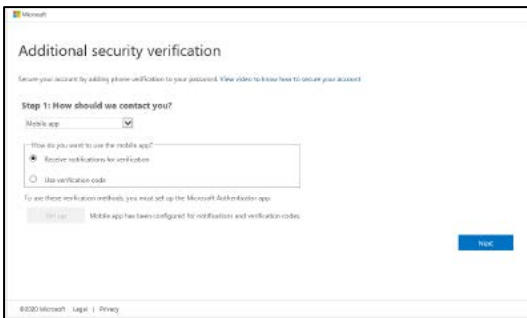


- Once scanned, the Microsoft Authenticator App will automatically show your work account under Accounts.



- On your screen:

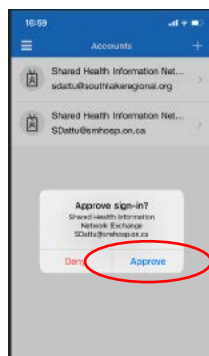
Click on "Next":



You will see this:



- Check your smart phone; you will receive a notification on your Microsoft Authenticator App to approve. Click "Approve".



- Click on "Done".
- You are now registered and setup for MFA.