

Multi-Factor Authentication (MFA) with the Microsoft Authenticator App

August 2023

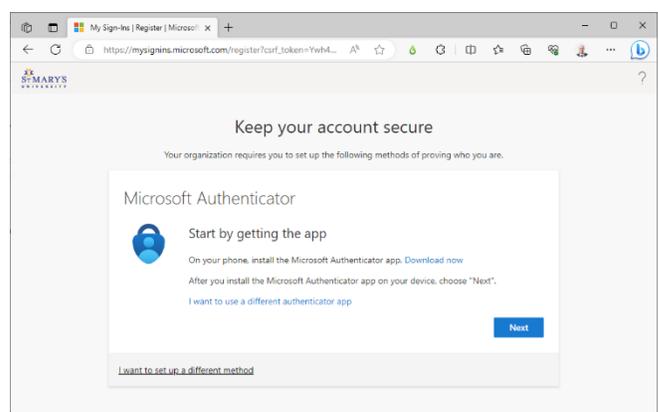
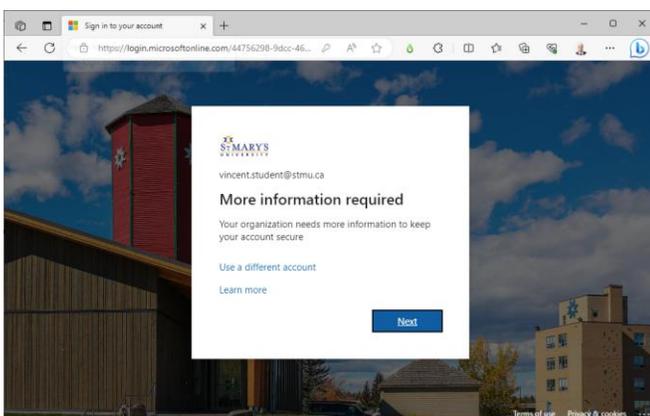
Signing into your account with your username and password, which is proving your identity to the system, this process is known as authentication. Using just your username and password for authentication is a single factor of authentication. Unfortunately, this is no longer secure enough. Usernames like the ones we use at StMU are easy to figure out, and since passwords can be hard to remember, many choose to reuse passwords on many different sites, or choose passwords that are simple or easy to guess.

We now join many online services, such as shopping sites, banks, social media, and Microsoft as well, to require Multi-Factor Authentication or MFA. You may also see some sites refer to this as Two-Step Verification, but the premise is the same. When you sign into your @stmu.ca account for the first time on a new device or app (like a web browser) you shall be prompted for an additional verification beyond your username and password. You'll require a second factor to prove your identity to the system.

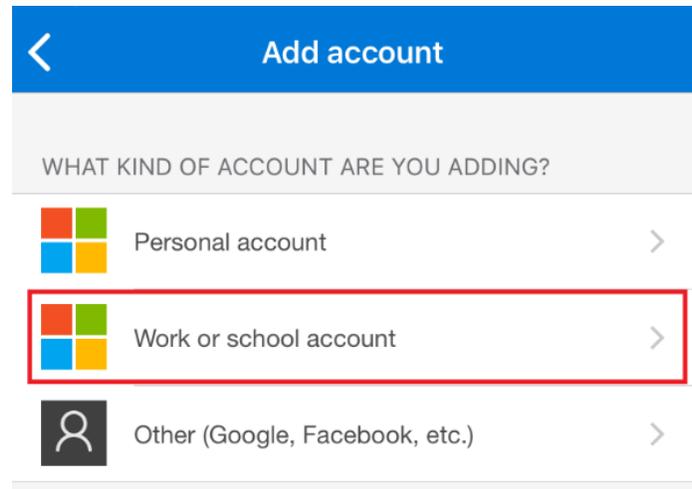
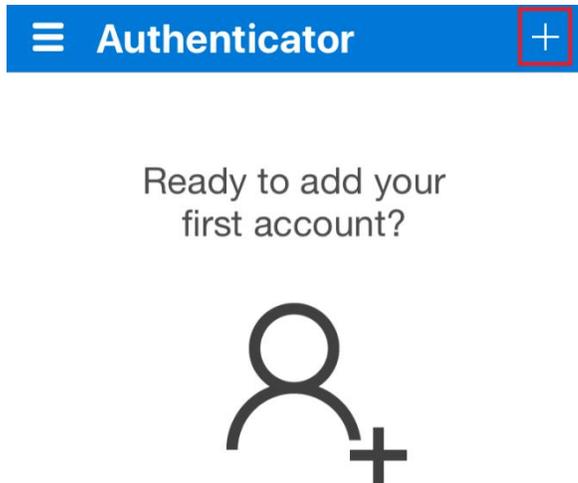
In the case of our MFA implementation at StMU, we are requiring users to install the Microsoft Authenticator app on a mobile device to use as a second factor of authentication. This is a free app download for users of Apple or Android mobile devices. The app is available in the App Store (for Apple devices, such as an iPhone or iPad) or Google Play Store (for devices running Android, such as a Samsung Galaxy phone or tablet or Google Pixel phone). For more information on the Microsoft Authenticator app, including links to download the app on your device, please visit <https://www.microsoft.com/en-ca/security/mobile-authenticator-app> in your web browser. You'll want to have the Microsoft Authenticator app installed to prepare for the next steps.

Please note that if you do not currently have the Microsoft Authenticator app installed on your device, you may need to update the version of iOS (Apple) or Android (Samsung, Google, etc.) on your device in order to successfully install the Microsoft Authenticator app. Additionally, the time on your device must be correct for your local time for the Microsoft Authenticator to work.

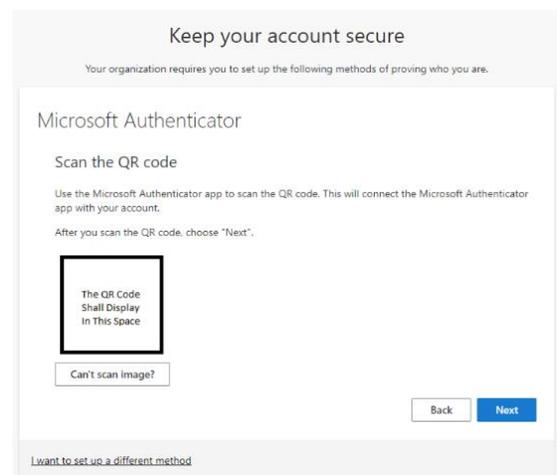
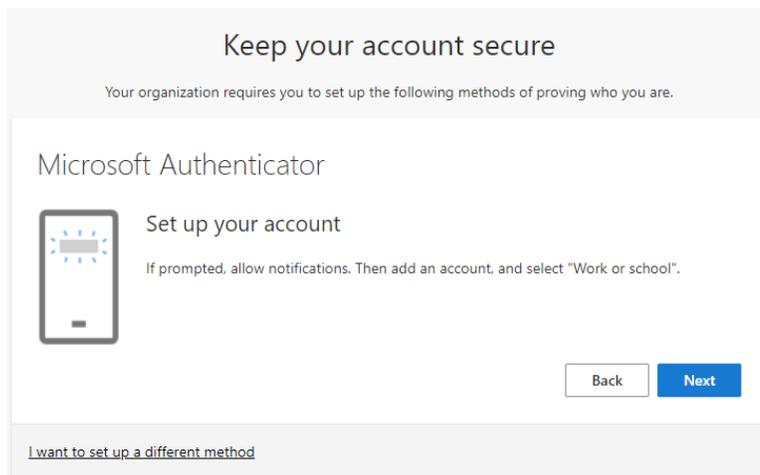
When MFA is enabled on your account, the system shall prompt for additional security information the next time you sign in to your @stmu.ca account to access online services on your computer, such as Microsoft 365 for your Exchange Online Email, or online services that use the Single Sign-On (SSO) for Microsoft 365, such as D2L Brightspace. A sample of the computer screens follows:



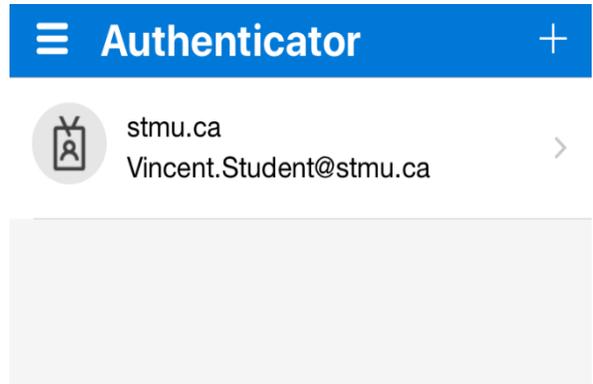
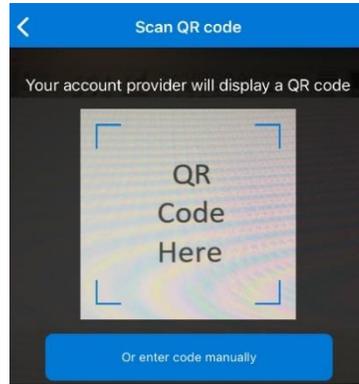
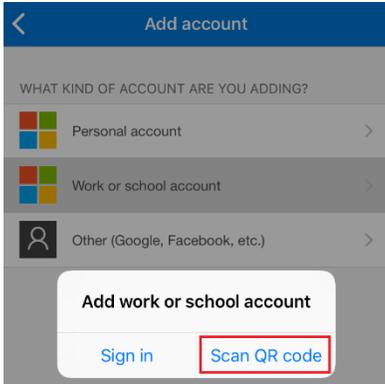
To complete the process to configure your Microsoft Authenticator app, please click on the next button on both of the above screens on your computer. On your mobile device please open the Microsoft Authenticator app and click on the '+' sign in the upper right corner and choose the Work or school account option. You may receive a prompt asking to allow notifications for the Microsoft Authenticator app, as well as for permission to access your camera to take a picture of the QR Code in the next step. Please allow both of these changes for the Microsoft Authenticator app to work correctly. A sample of the mobile device screens follows:



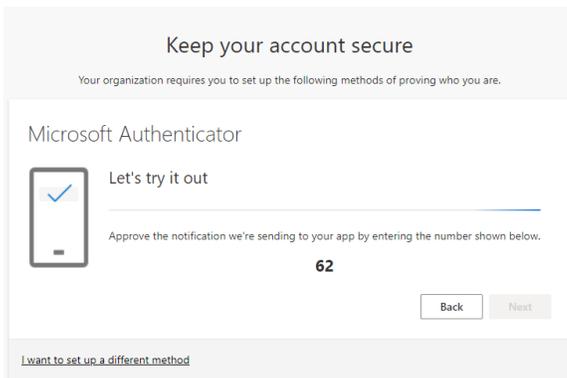
On the computer, please continue the process of configuring the Microsoft Authenticator app by clicking the next button on the first screen, to generate the QR Code to be displayed on the second screen. Please note that we have put in a placeholder graphic for the QR Code. A sample of the computer screens follows:



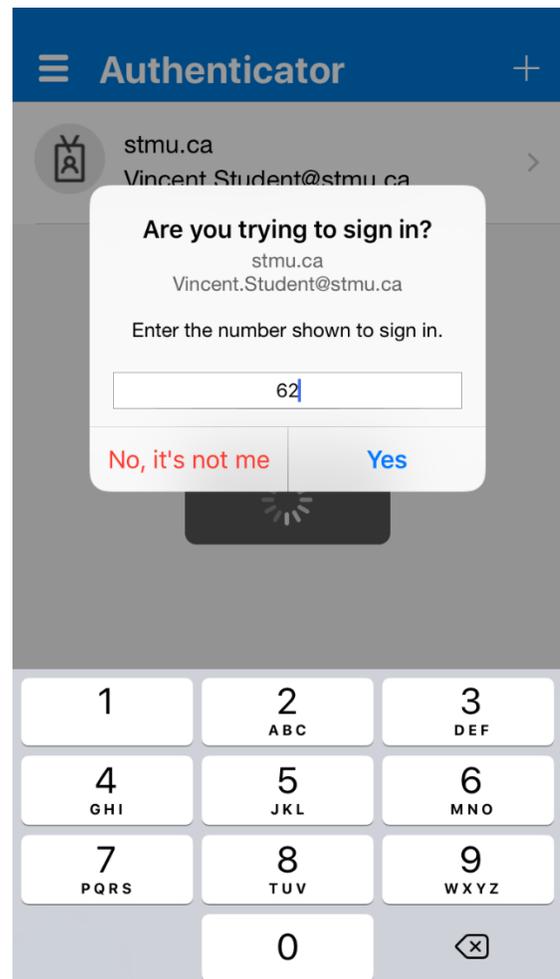
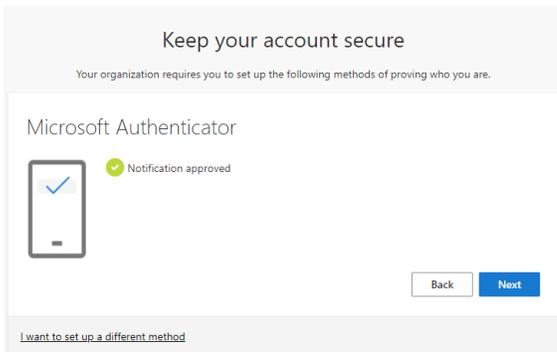
You'll want to use the camera on your mobile device to scan the QR code from your computer by pointing it at your computer display. This process may take some time to complete. Once the process is complete, you'll see an entry in your Microsoft Authenticator app for your @stmu.ca account. If this process did not complete successfully, please try again, and if you are still having issues, please reach out to helpdesk@stmu.ca for assistance. A sample of the phone screens follows on the next page:



Once the Authenticator App shows the @stmu.ca account, please click on the next button on your computer, a new screen appears requesting to try out the new Microsoft Authenticator app for your account. Please note the number on the screen, you will need to enter this on the phone to confirm that this is working. A sample of the computer screen is below on the right:

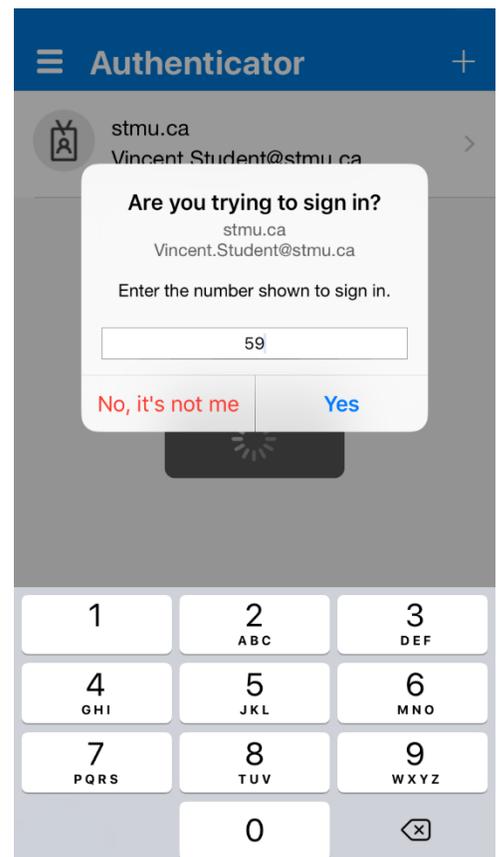
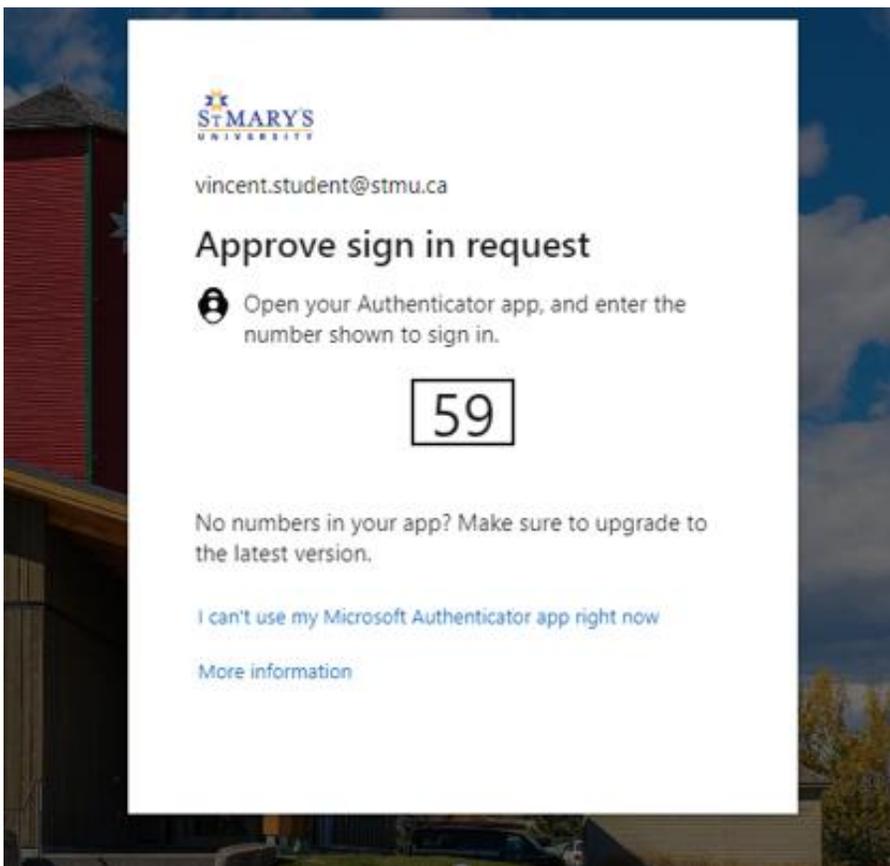


On your phone, you should be prompted asking 'Are you are trying to sign in?' and asking for the number shown above. Please enter the number and tap on the Yes button. A sample of the phone screen is on the left and a sample of the confirmation screen on the computer is below:



Please note that the process to configure the Microsoft Authenticator app has only to be completed once on your mobile device; however, if you change devices, you'll need to configure the Microsoft Authenticator app again.

Once MFA has been enabled on your account, and has been configured as per the instructions above, you'll receive prompts to approve your sign in request when you sign in on a new device or web browser, or the first time you sign in after changing your password. This generally doesn't happen very often, and after that you'll be using your username and password as you normally do. A sample of the screen on the computer is below on the left, and a sample of screen on the phone is on the right:



One of the major benefits of enabling MFA is that we are also able to Self-Service Password Reset (SSPR). Once the Microsoft Authenticator has been configured on your account, and MFA has been enabled, we also enable SSPR on your account.

Users with SSPR enabled on their account are now able to click on the Forgot my password link on the Microsoft 365 login page, or visit <https://aka.ms/sspr> on the web, and follow the instructions, instead of contacting the IT Help Desk to reset your password (if you have forgotten your password) or unlock your account (if you have tried the incorrect password too many times).

If you have any questions or concerns regarding the MFA and the Microsoft Authenticator app, or any other IT issues, please contact the IT Help Desk at helpdesk@stmu.ca via email. Thank you for your patience and understanding in this matter.