City University of Seattle

Multifactor Authentication FAQ

Frequently Asked/Answered Questions

What is Multifactor Authentication?

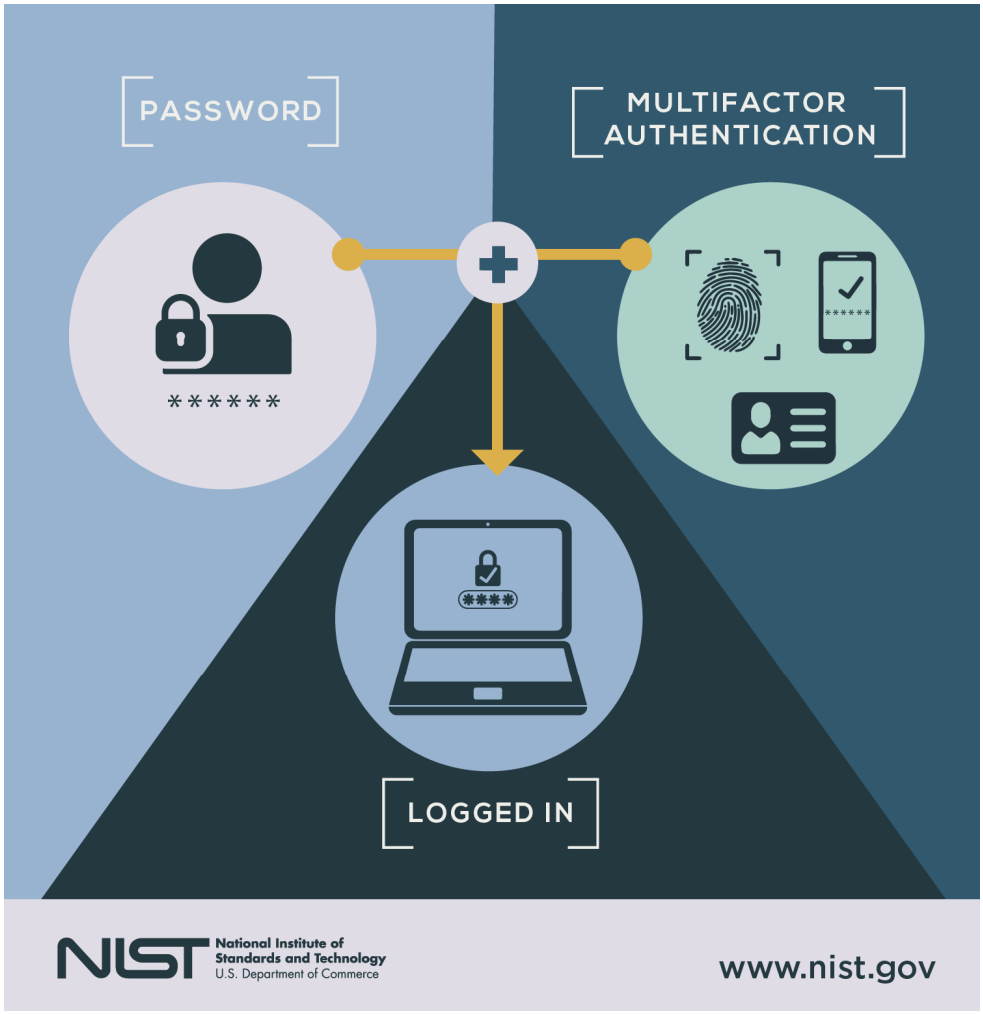
MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account.

Your credentials can fall into any of these three categories:

- something you know (like a password or PIN),
- something you have (like a smart card or phone),
- or something you are (like your fingerprint).

Your credentials must come from two different categories to enhance security – so entering two different passwords would not be considered multi-factor.

CityU students will be able to log-in to various student accounts with their credentials to access their email, Blackboard, and other pertinent information using MFA. The University MFA setup will use a combination of password and authentication app that can be downloaded to a mobile device.



What is Single Sign-On?

Single sign-on (SSO) is a centralized user authentication service in which one set of login credentials can be used to access multiple applications. User experience benefits by enabling users to access all of their applications from one location, with a single set of credentials. CityU's Single Sign-On experience is managed through Microsoft.

What Student Systems will MFA affect?

The systems listed will need students to authenticate when logging in for the first time or directly include:

- University Email/Outlook
- Library Databases
- Personal Course Reading List (Leganto)
- BlackBoard
- Additional Microsoft Services (i.g. One Drive)
- My.CityU.Edu Dashboard
- My.CityU.Edu Student Center Links

What is the most recommended authentication method?

The most recommended authentication method is the Microsoft Authenticator App. The preferred method for most users is "*Receive Notification*" which requires just a single click to authenticate within the app. The alternative verification method requires manually typing a code displayed when you open the Microsoft Authenticator app or receive a verification phone call.

Do I need to Authenticate every time I log into a system?

Yes, students accessing their Office 365 email will need to authenticate each time. For logins to Office 365 via the web, you will have the option to have your browser "remember" you and will see this option when you log in.

What if I change my number?

If you change your number, students can use the self-service portal at https://myworkaccount.microsoft.com to reset their authentication method.

Students may also contact CityU's 24/7 tech support at https://techsupport.cityu.edu

If you are keeping the same mobile device and just changing the number, the Microsoft Authenticator app will still work. If you are getting a new number and a new mobile device, the app will need to be installed again.

What if I am outside of the US/Canada?

If you do not have mobile service while out of the country, you will need to install the Microsoft Authenticator app, which will work with Wi-Fi service.

What are my Authentication Options?

You will be able to choose a primary authentication method when you register, which you can change or update at any time. Current options are outlined below:

Verification Method	Description
Mobile Notification *(Microsoft Authenticator Required)*	A push notification is sent to the authenticator app on your smartphone asking you to Authenticate your log in.
Verification Code *(Microsoft Authenticator Required)*	The Mobile Microsoft Authenticator app will generate a verification code that updates every 30 seconds. You will be asked to enter the most current verification code in the sign-in screen.
Text Messages	A text message with a 6-digit code is sent to your mobile device that you will input to complete the authentication process
Phone Calls	A call is placed to your mobile phone asking you to verify you are signing in. Press the # key to complete the authentication process.

I forgot my password?

If you're a student or staff member and need to get back into your account, go to https://aka.ms/**sspr**.

Self-Service Password Reset (**SSPR**) is an Azure Active Directory (AD) feature that enables users to reset their passwords without contacting IT staff for help.

Students may also contact CityU's 24/7 tech support at https://techsupport.cityu.edu for password reset assistance.