Accessible Multi-Factor Authentication (MFA) Options at CUNY

This document identifies which Multi-Factor Authentication (MFA) features work best for individuals with different types of disabilities. Using the Microsoft Authenticator and related authentication methods such as TOTP, FIDO2, and Yubico OTP, it evaluates common accessibility barriers and highlights the most inclusive options for each user group. The goal is to help CUNY ensure that all students, faculty, and staff can securely access their accounts using authentication methods that best fit their individual accessibility needs.

CUNY IT Help: CUNY Login MFA Instruction Documents

Setting Up and Using Your iPhone as a CUNY Login MFA FIDO2 Factor

Setting Up and Using Your Android Phone as a CUNY Login MFA FIDO2 Factor

Acronym Guide

- TOTP (Time-Based One Time Password): the set of 6-digit numbers displayed and refreshed every 30 seconds on an authenticator app such as Microsoft Authenticator, Google Authenticator, or Oracle Authenticator. Requires the download of an authenticator application ("app") on your phone. Lasts for 30 seconds before expiring.
- FIDO2 (Fast Identity Online 2): FIDO2 (Fast Identity Online 2): creates a passkey that can be used across FIDO2-compliant devices, such as certain Windows and Mac computers, iOS and Android phones, and USB security keys. These devices support multiple authentication methods (e.g., Face ID, fingerprint, PIN, or QR code).
- Yubico OTP (One-Time Password): another option for a physical security key that plugs into the computer's USB drive. The presence of the key in the USB authenticates the request.

1. Visual Impairments (Blindness, Low Vision)

Potential Barriers	Accessible Alternative Features
• Reading time-limited numeric codes in the app without good screen reader support.	• **FIDO2 Biometrics** (Face ID, fingerprint) bypasses code entry.
• Matching numbers for push approval if layout is not screen-reader friendly.	• **Yubico OTP** physical security key is an accessible alternative as it does not require any visual interaction.

In summary - for Blind and Low Vision users, it is most ideal to likely for someone with low vision to either use a security key (using FIDO2 or Yubico), plugged in to ensure uninterrupted authentication, or to establish a biometric – touch or eye gaze – through their personal devices (using FIDO2).

2. Hearing Impairments (Deaf, Hard of Hearing)

Potential Barriers	Accessible Features
• No major barriers, as Microsoft Authenticator or Oracle Authenticator does not rely on voice or phone call-based verification.	• **FIDO2 Biometrics**: Does not rely on user's hearing for authentication.
	• **TOTP passcodes**: Presented in an accessible, visual format.

In summary – for Hearing Impairment, this comes down to personal preference, as there are no audio cues with MFA. TOTP or FIDO2 (QR code, password, or biometrics such as touch/eye gaze) are both recommended and can be used at the user's preference.

3. Mobility/Physical Disabilities (Limited Hand Use, Motor Impairments)

Potential Barriers	Accessible Features
• Users may not be able to use fingerprints as an authentication method	• **FIDO2 Biometrics:** Hands-free options such as Windows Hello or Face ID are effective alternatives.
• Repeated manual entry of codes may be difficult.	• **Yubico OTP:** NFC-enabled versions allow tap-to-authenticate with mobile devices which reduce need for inserting USB keys.
• Smaller user interface elements could cause trouble with precise tapping.	

In summary – for Mobility/Physical Disabilities, a security key from FIDO2/YUBICO or FIDO2 for biometrics such as eye gaze/touch on personal computer are recommended. TOTP is not recommended for the student with motor/physical disabilities.

4. Cognitive Disabilities (Memory, Processing, Attention Challenges)

Potential Barriers	Accessible Features
• Remembering and entering 6-digit rotating codes in time.	• **FIDO2 Biometrics:** Bypasses code memorization and provides for quick authentication while allowing for a low cognitive load.
• Confusing navigation if multiple accounts are set up.	• **Yubico OTP:** Uses a single physical gesture, such as a tap or inserting the key and does not involve codes or typing.

In summary – for Cognitive Disabilities, a security key from FIDO2/YUBICO or FIDO2 for biometrics such as eye gaze/touch on personal computer is recommended. TOTP is not recommended for the student with cognitive disabilities.

5. Speech Disabilities

Potential Barriers	Accessible Features
• Not applicable — Microsoft Authenticator does not use voice biometrics.	• All methods (biometrics, codes, passwordless options) remain fully accessible.

In summary – for Speech Disabilities, this comes down to personal preference, as there are no speech cues with MFA. TOTP or FIDO2 (QR code, password, or biometrics such as touch/eye gaze) are both recommended and can be used at the user's preference.

6. Neurological Conditions (Epilepsy, Migraines)

Potential Barriers	Accessible Features
• Rapid flashing animations in system user interface (not in Authenticator itself, but in OS-level	• **FIDO2 Biometrics** (Face ID, fingerprint) bypasses any flashing

Potential Barriers	Accessible Features
notifications) could trigger symptoms.	animation and allows for quick authentication.
• The expiration time for the passcode entry is short and can cause a potential cognitive load.	• **TOTP passcodes** in plain text, although the timer can potentially be a deterrent for some users .

In summary – for Neurological Disabilities, this comes down to personal preference as to which is preferred to avoiding flashing mechanisms. TOTP or FIDO2 (QR code, password, or biometrics such as touch/eye gaze) are both recommended and can be used at the user's preference.

Further Recommendations

- **Set Up Multiple Methods:** Configure more than one MFA option (e.g., FIDO2 on multiple devices) to ensure continued access if one method fails.
- **Complete Setup in One Session:** Finish setup and verification in the same session to prevent incomplete activation.
- **Phone-Free Alternative:** Windows PC users can download Oracle Authenticator from the Microsoft Store to generate one-time passwords (OTPs) directly on their computer, without a phone.
- **Hardware Key Support:** Yubico keys support multiple protocols (OTP, FIDO2) and are available in USB-A, USB-C, Lightning, and NFC formats.