CUNY Multi-Factor Authentication (MFA) on New Device

Note: Important Before You Begin

You must have access to your **current device** that is already set up with **CUNY Login Multi-Factor Authentication (MFA)** in order to complete the self-service setup on your new device.

If you **no longer have access to your old device**, you will need to contact the **Hunter College Help Desk** to request an MFA reset before proceeding.

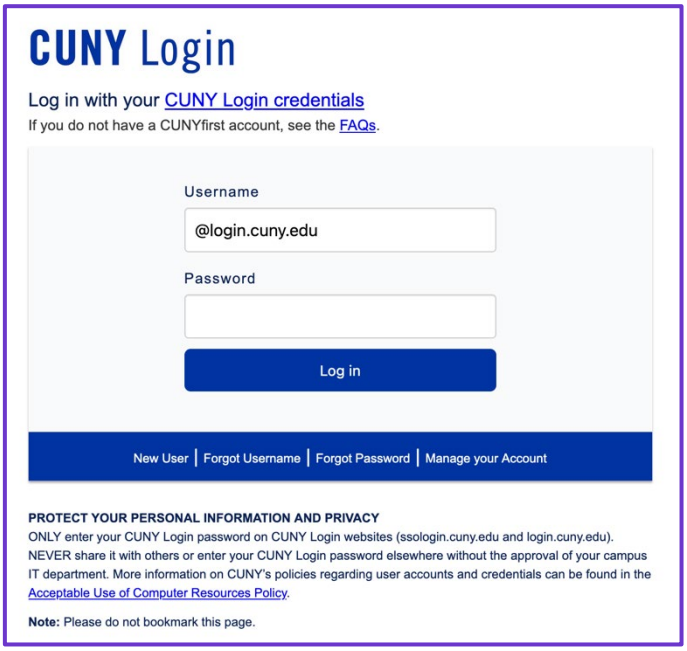
Email: helpdesk@hunter.cuny.edu
Located: Hunter North Room 303

Accessing CUNY MFA Self-Service

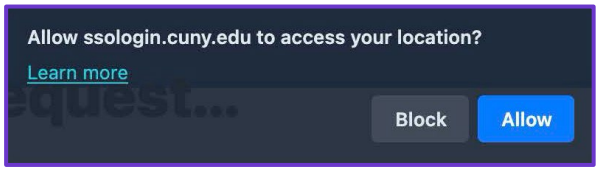
1. In a new web browser window, open the CUNY MFA Self-Service: (https://sso login.cuny.edu/oaa/rui)

The CUNY Login page displays

2. Enter your CUNY Login username and password, then click **Log in**:

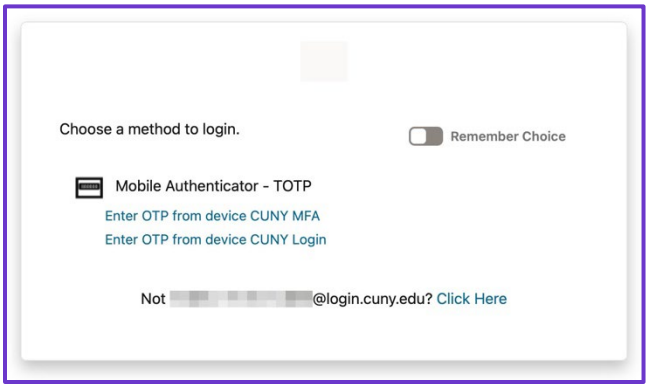


- If you are also prompted to share your location with ssologin.cuny.edu, click **Allow**.



3. If you previously did not toggle, **Remember Choice** a window will appear prompting you to **choose your MFA login method** from a list of your previously established CUNY MFA authentication factors.

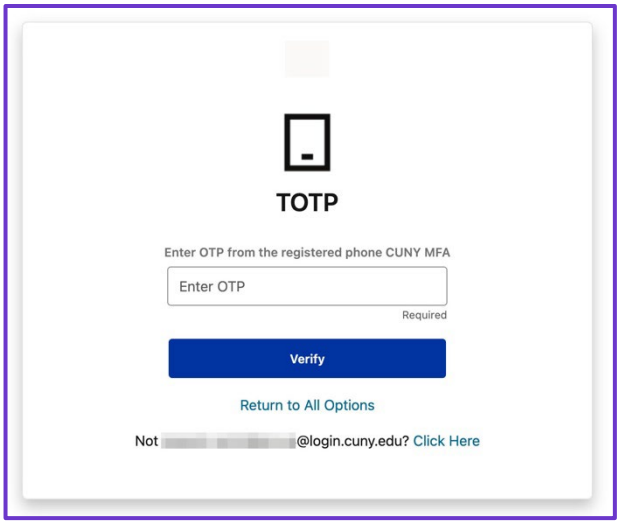
- Select **Enter OTP from device** along with the friendly name you assigned when setting up your MFA on your old device

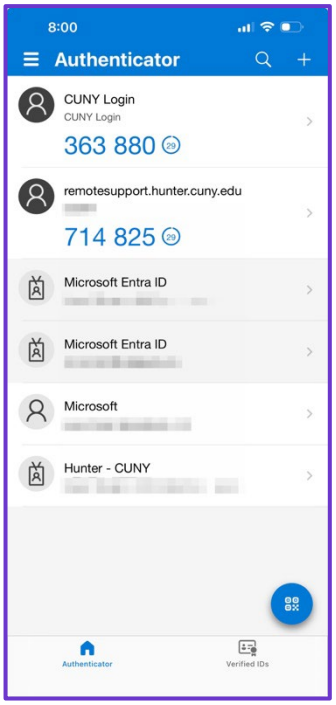


4. Next you will see the **TOTP screen**, prompting you to **enter the OTP** from your **old or previously set-up device**.

- Use your old device to retrieve the one-time passcode (OTP) from the Microsoft Authenticator.
  - Open the **Microsoft Authenticator** App

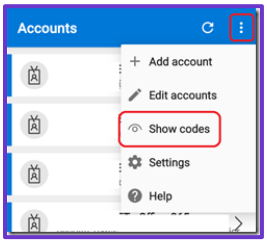
  - In the **Enter OTP from the registered phone field**, enter the one-time passcode from Microsoft Authenticator
  - Click **Verify**



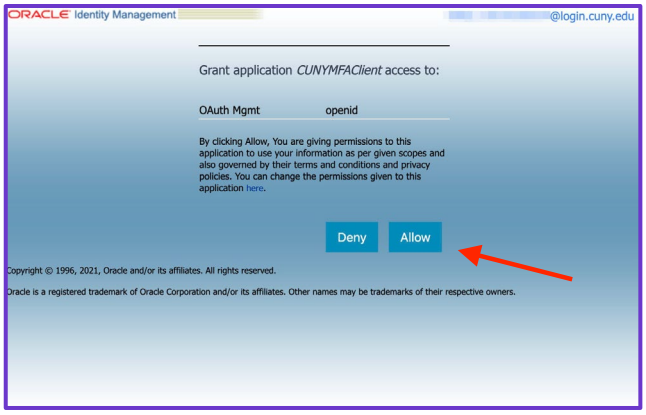


Note for Android Users:
By default, Microsoft Authenticator hides the 6-digit codes.
Tap the **three-dot menu (⋮)** in the top right and select "**Show codes**" to make the OTP visible.

You can also tap an individual account row to reveal its code temporarily.

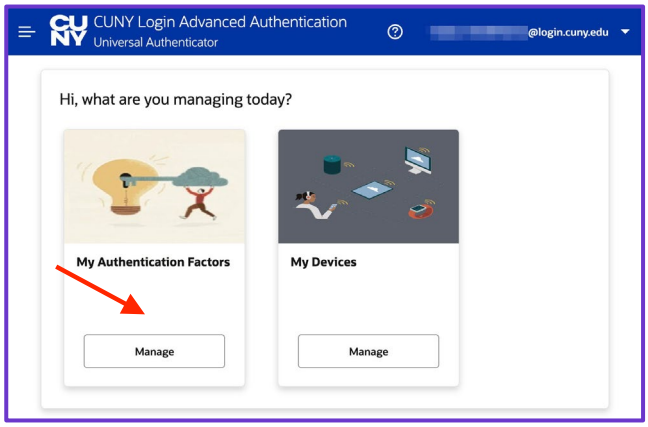


5. An **Oracle Access Manager** confirmation page appears requesting permission for the *CUNYMFAClient* application to secure your account.



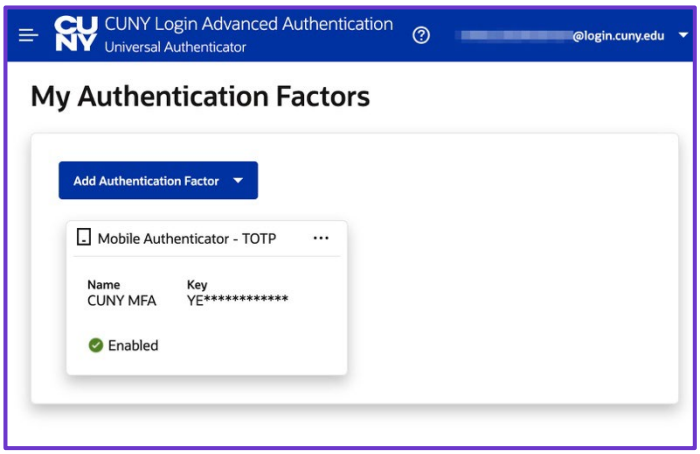
➢ Click **Allow** to continue

6. The **CUNY Login Advanced Authentication** page appears with two management options.



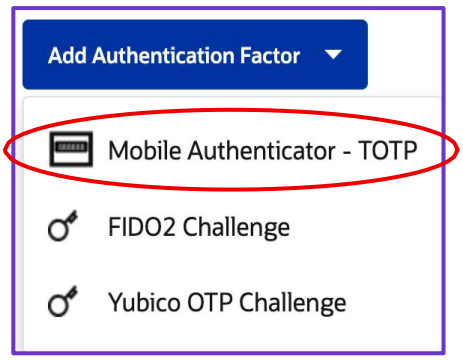
➢ Under **My Authentication Factors** click **Manage**

7. The **My Authentication Factors** page is displayed, listing your previously registered CUNY MFA - Mobile Authenticator TOTP.

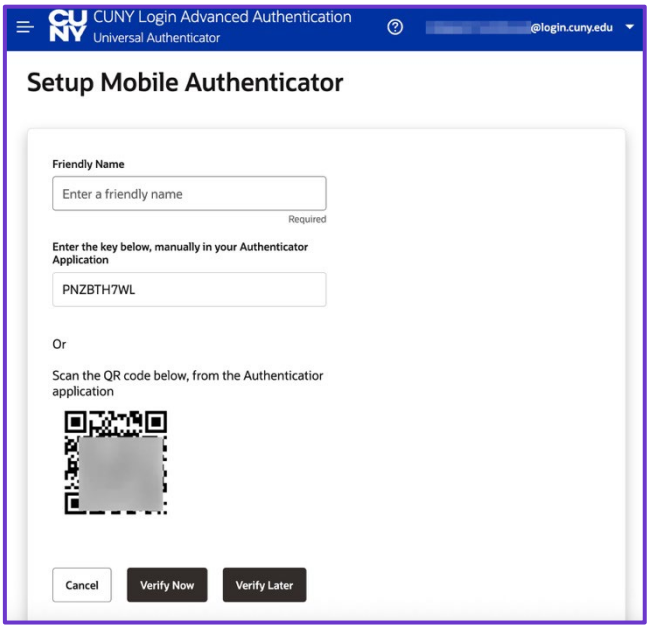


➢ Select the drop-down menu **Add Authentication Factor**

➢ Choose **Mobile Authenticator - TOTP**

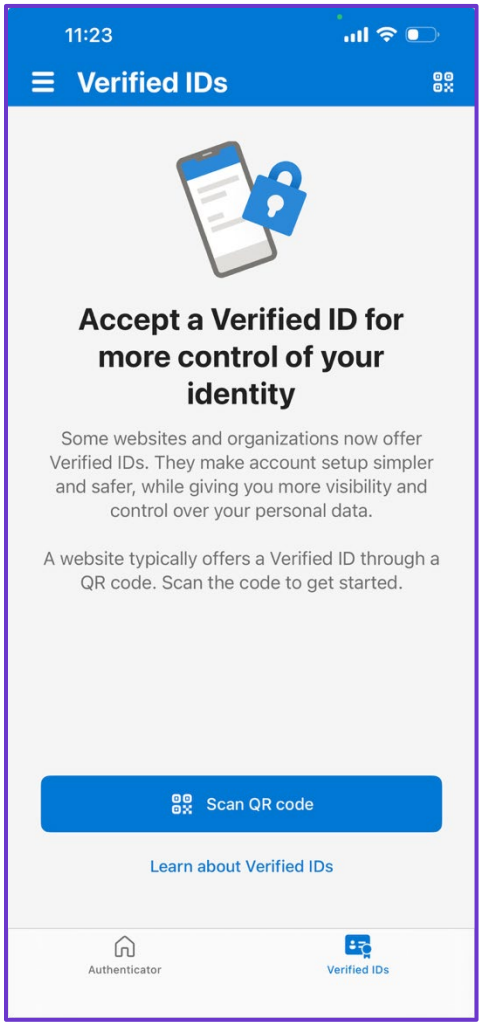


8. The **Setup Mobile Authenticator** page is displayed.

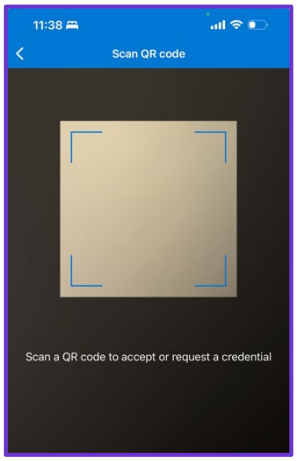


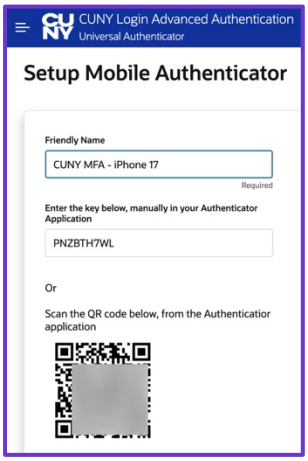
- Enter a **Friendly Name** - Type a short, descriptive name that helps you distinguish this **CUNY MFA** setup and identify the **device** being used.
  (for example: *CUNY MFA - iPhone 17)*

9. Open the **Microsoft Authenticator app** on your **new device**.

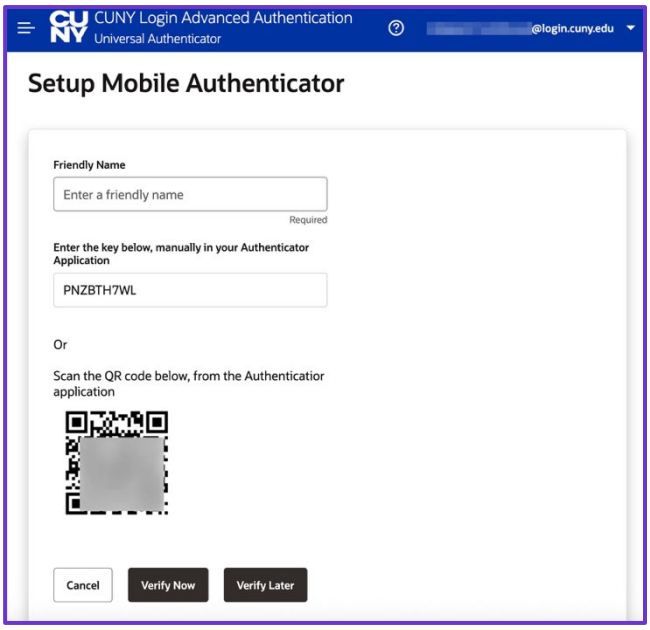


- Tap **Verified IDs** at the bottom right of the screen
- Tap **Scan QR Code**
- Use your device's **camera window** on the **Scan QR Code** page to scan the QR code displayed on the **Setup Mobile Authenticator** page on your computer
  - If prompted, allow the Microsoft Authenticator app to access your camera to scan the QR Code.





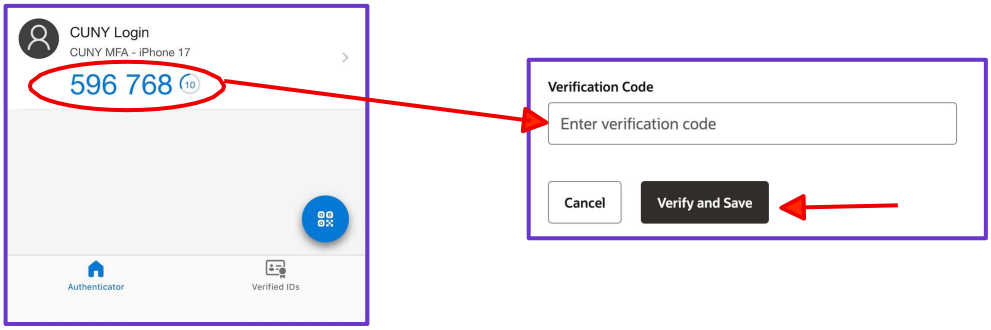
10. Complete the verification process.



- Once the QR code has been successfully scanned, your **Microsoft Authenticator** app will generate a **6-digit verification code** for your new CUNY MFA setup.

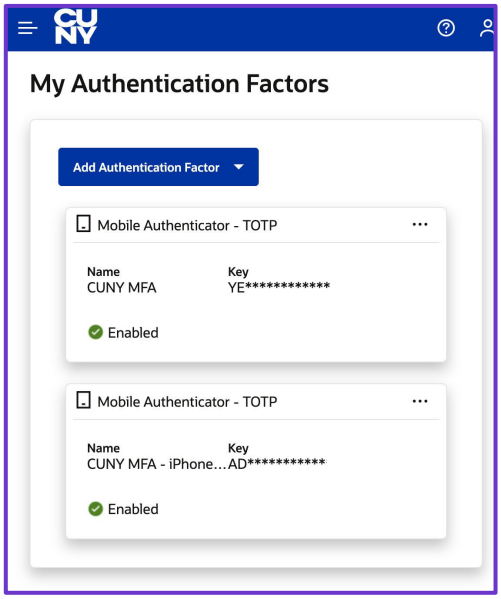
  ➢ Click **Verify Now** to confirm and activate the new authentication factor.
  (*Allow a few seconds for the Verification Code text box to appear below*)

  ➢ Enter the 6-digit verification code (OTP) from your newly configured CUNY MFA in the **Microsoft Authenticator** app.



  ➢ Click **Verify and Save** to complete the setup.

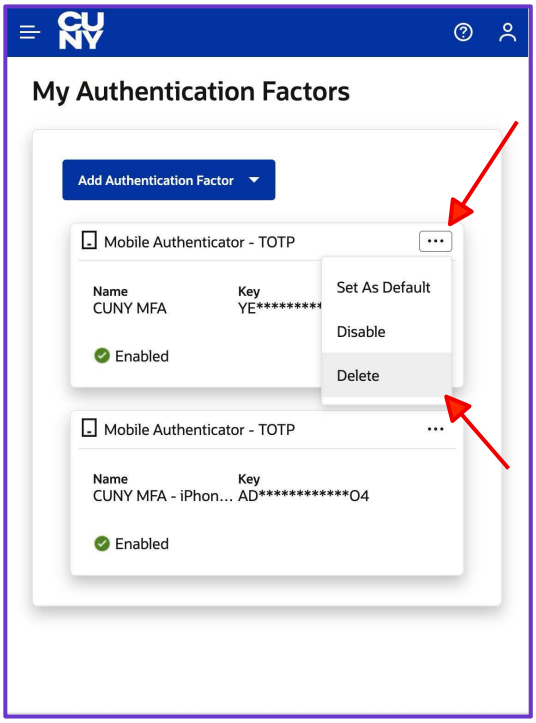
11. At this point, both authentication factors are displayed.



- **My Authentication Factors** page now shows your **newly added CUNY MFA** alongside your **previous MFA.**
- The green checkmark **Enabled** confirms that your new device has been successfully registered and is ready for use.

***You can now proceed to **remove** your **old MFA factor** in the next step.

12. Cleaning Up your MFA factors



Now that your new **CUNY MFA** is successfully set up and enabled, you can remove your **old** authentication setup.

To remove the old authentication factor from CUNY Login:

- Locate your **old MFA entry** on **My Authentication Factors** page
- Click the **three dots (…)** in the upper-right corner of the old factor's box
- Select **Delete**

13. Testing your newly configured CUNY MFA

You have successfully set up **CUNY MFA** on your new device.

To verify your setup:

- Log out and sign back into a CUNY Login-protected service (for example, **CUNYfirst**, **Brightspace**, or **CUNY Zoom**).
- When prompted for MFA, use your new device's **Microsoft Authenticator** app to enter the verification code.

If the verification is successful, your new MFA setup is complete, and you can now use this device for all future CUNY MFA **TOTP** (Time-Based One-Time Password) prompts.

If you encounter any issues signing in or receiving codes,
*please contact the **Hunter College Help Desk** at* helpdesk@hunter.cuny.edu

Thank you for helping keep our CUNY systems and personal information secure by setting up CUNY Multi-Factor Authentication (MFA).

Your participation plays an important role in protecting the University community from unauthorized access and maintaining the safety of our digital environment.