

Setting Up and Using CUNY Login MFA

CUNY is adding multi-factor authentication (MFA) to CUNY Login. CUNY Login MFA will provide more secure access to CUNY applications and services and better protect your and CUNY's data from cyberattacks.

CUNY Login MFA is separate from the [Microsoft MFA implementation](#) required when using Microsoft 365 applications and services.

This document provides the following:

- Instructions on how to install the Microsoft Authenticator app on your mobile phone
- A short video tutorial on setting up and using CUNY Login MFA
- Brief instructions on setting up CUNY Login MFA
- Brief instructions on responding to CUNY Login MFA prompts
- Brief instructions on how to set up CUNY Login MFA **without a smartphone**

How to install Microsoft Authenticator on your mobile phone

Please download and install it from either the [Apple App Store](#) or [Google Play](#) or by scanning the QR codes below. Once downloaded, follow the prompts.



Google Play



App Store

Video Tutorial

We recommend watching the following Streams video for a quick overview on setting up and using **CUNY Login MFA**: [Setting Up CUNY Login MFA](#)

Setting Up CUNY Login MFA for the First Time

To set up CUNY MFA factors, you will need a mobile device (preferably a smartphone) and a computer (laptop or desktop)

The following one-time procedure provides instructions on setting up CUNY Login MFA TOTP (Time-based One-Time Password) for use with the Microsoft Authenticator mobile app when you have access to a computer as well as your phone.

1. In a new web browser window, open [CUNY MFA Self-Service](https://ssologin.cuny.edu/oa/rui) (<https://ssologin.cuny.edu/oa/rui>)
2. The CUNY Login page displays.

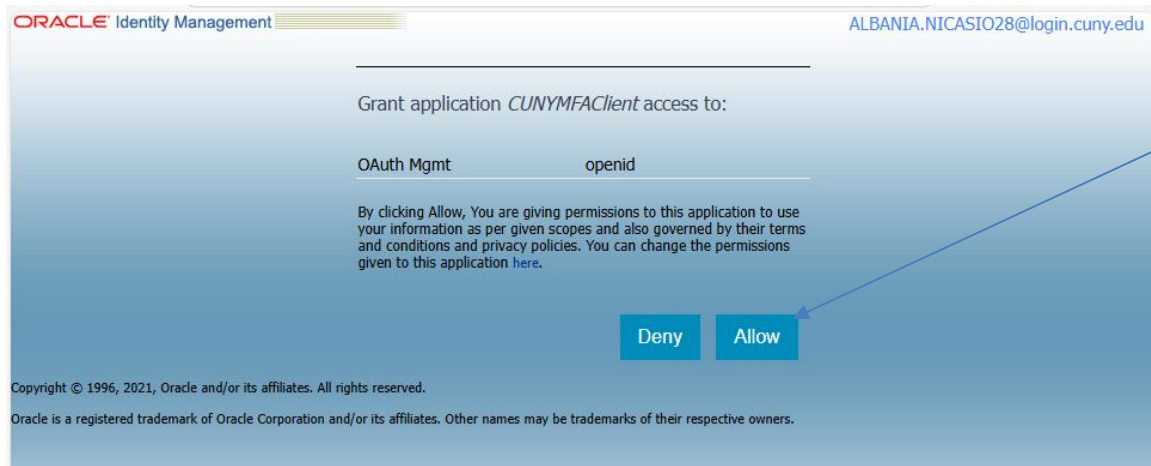
3. Enter your CUNY Login username and password, then click **Log in**.

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

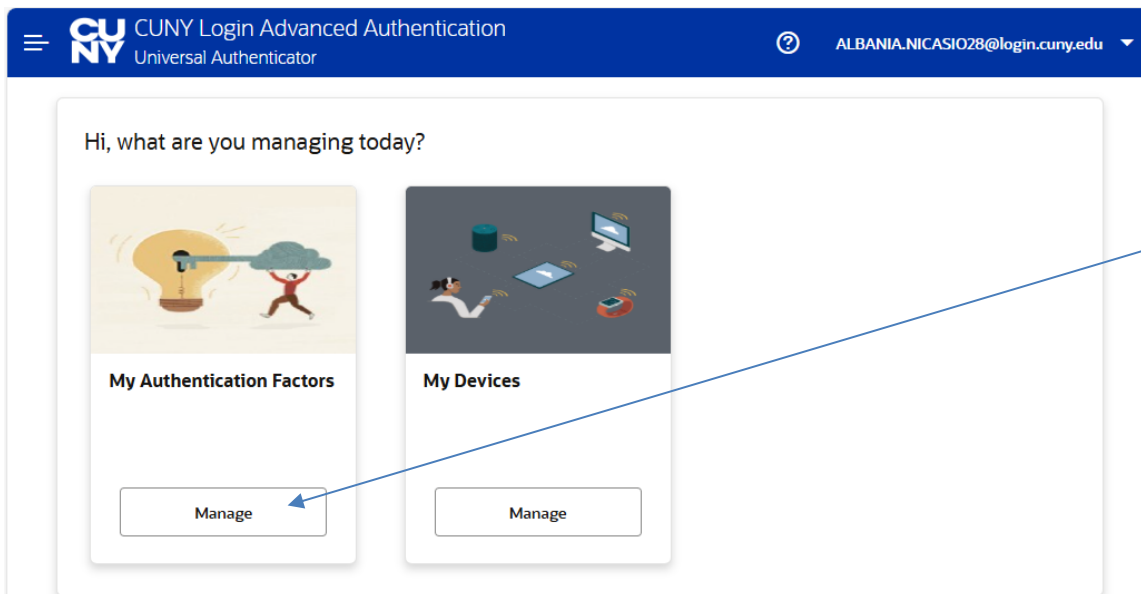
An Oracle Access Manager page is displayed with a confirmation message, with the instruction to click OK to continue.

4. Click **OK** to acknowledge the message.

An Oracle Identity Management page is displayed asking you to grant access to continue.



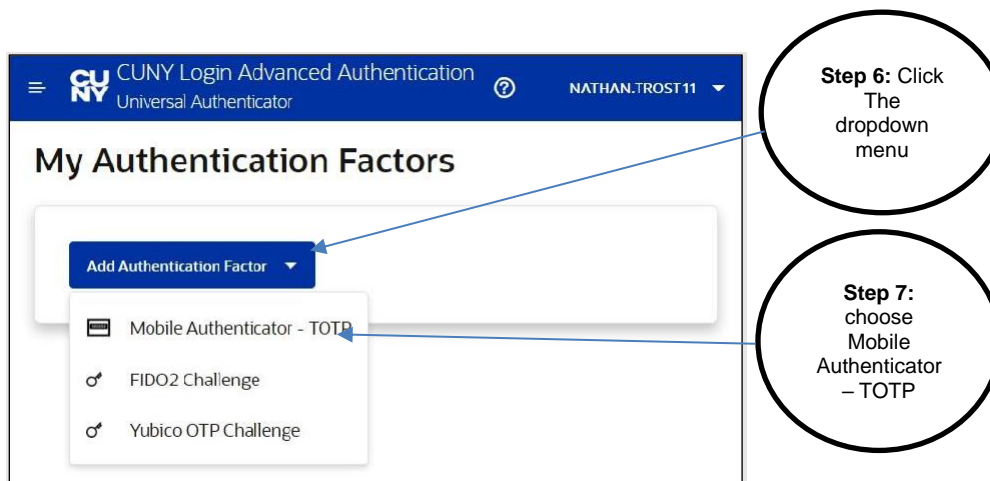
The following page is displayed.



5. Click **Manage** in the **My Authentication Factors** tile.

The CUNY Login Advanced Authentication – My Authentication Factors page is displayed.

6. Click on **Add Authentication Factor** to display the list of authentication factor methods.



7. Click on the drop-down menu, choose **Mobile Authenticator – TOTP** (Time-based One-Time Password).
8. The CUNY Login Advanced Authentication - Setup Mobile Authenticator page is displayed.
9. A new window will appear. Please see the picture below.

Step 10: Enter a friendly name (CUNY Login MFA)

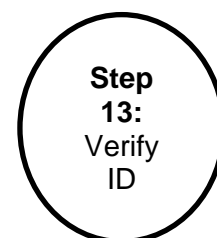
Step 11: Click on verify Now

Step 10: In the **Friendly Name** field, type a name (such as “**CUNY Login MFA**”) to easily distinguish CUNY Login MFA from any other accounts in Microsoft Authenticator.

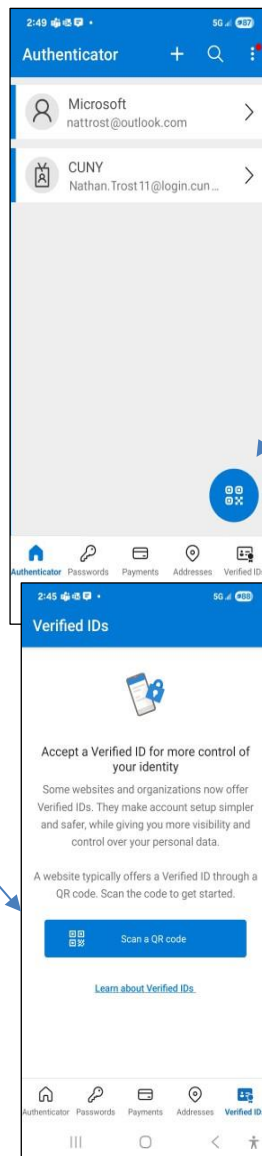
Step 11: Once you enter the “friendly name” click on Verify now.

Please Note: If you are using Microsoft Authenticator on an iPhone, consider using hyphens or underscores instead of spaces in the Friendly Name field. Some older iPhones may replace the spaces in the friendly name with %20 when the Friendly Name is added to the Microsoft Authenticator mobile app.

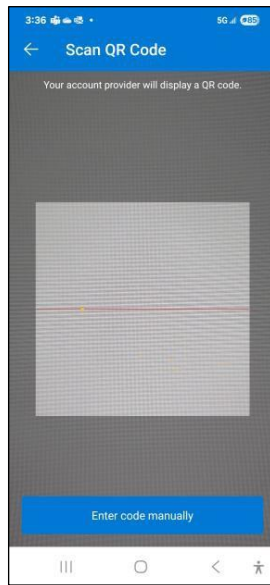
12. Open Microsoft Authenticator on your mobile phone.
13. Tap **Verified IDs** at the bottom of the page. The Microsoft Authenticator Verified IDs page is displayed.



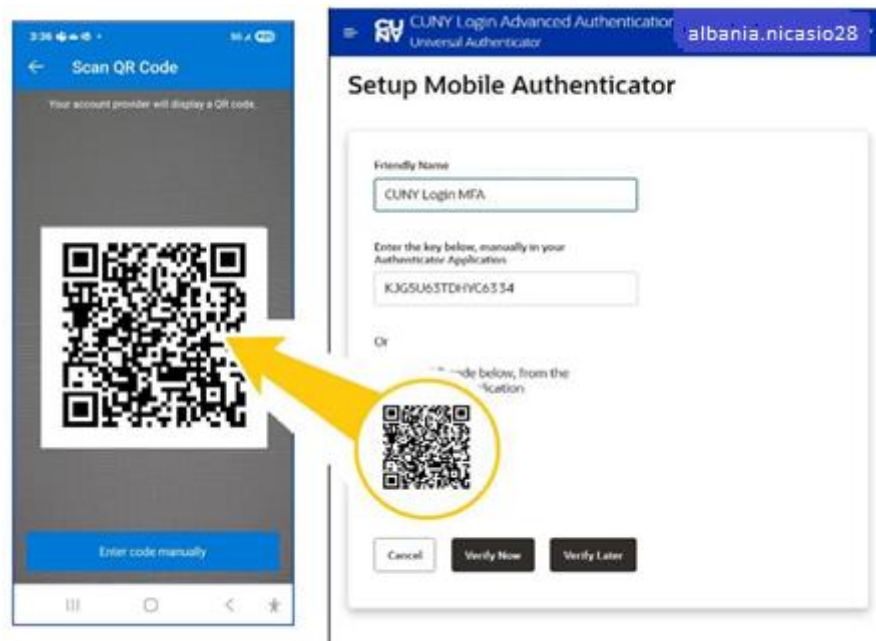
14. Tap **Scan a QR code**.



15. The Microsoft Authenticator Scan QR Code page is displayed.



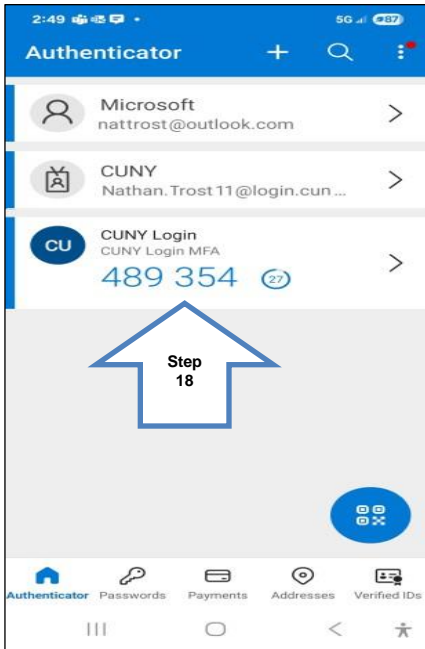
16. At this point, use the camera window on the Scan QR Code page on your desktop to capture the QR code displayed on the CUNY Login Advanced Authentication - Setup Mobile Authenticator page on the computer.



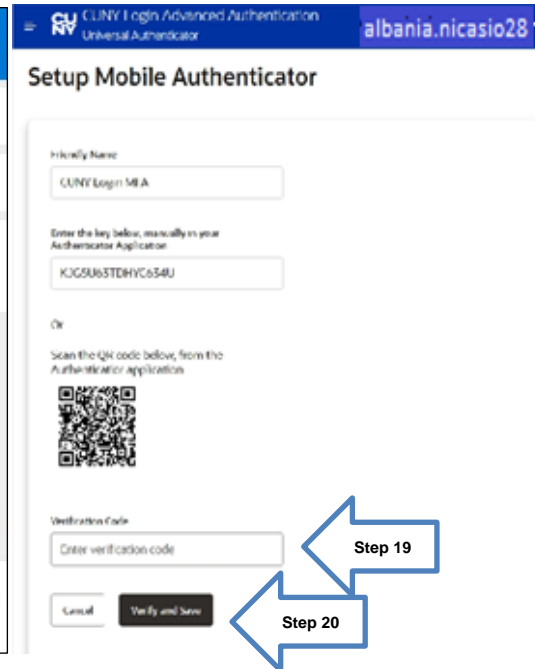
This sets up a new MFA account in Microsoft Authenticator, having the friendly name you entered, with a time-based one-time password (TOTP) code that changes every 30 seconds. A countdown timer indicates how much longer the password code remains valid for authentication.

17. On the CUNY Login Advanced Authentication - Setup Mobile Authenticator page on the computer, click **Verify and Safe**.

Picture 1: Mobile Phone



Picture 2: Your desktop



18. **Picture 1:** A Verification Code field is added to the **CUNY Login Advanced Authentication - Setup Mobile Authenticator** page.

19. **Picture 2:** From your desktop, in the Verification Code field, type the password code (6-digit *number*) from the Microsoft Authenticator app on your phone.

20. Click **Verify and Save**.

The My Authentication Factors page displays the Mobile Authenticator - TOTP MFA account just added.



21. Click on your CUNY Login username in the top right corner of the page, choose **Log out** and close your browser.

Your CUNY Login MFA TOTP method has been set up, and the corresponding MFA account is now in your mobile phone's Microsoft Authenticator app.

If you don't have a smartphone, please follow the instructions below to set up the MFA.

Please note: if you have more than one computer, these instructions are to be followed for every device.

1. In a new browser window, open [CUNY MFA Self-Service](https://ssologin.cuny.edu/oa/rui) (<https://ssologin.cuny.edu/oa/rui>). The CUNY Login page displays.

2. Enter your CUNY Login username and password. An Oracle Identity Management page is displayed asking you to grant access to continue.
3. Click **Allow** to continue. The CUNY Login Advanced Authentication - Manage your authentication page is displayed.
4. Click on **Add Authentication Factor** to display the list of authentication factor methods.
5. Choose **Mobile Authenticator – TOTP** (Time-based One-Time Password). The CUNY Login Advanced Authentication - Setup Mobile Authenticator page is displayed.
6. In the **Friendly Name** field, type a name (such as “CUNY_Login_MFA”) to easily distinguish CUNY Login MFA from any other accounts. Keep this browser window open.
7. Open a new browser window and navigate to Oracle Mobile Authenticator (<https://apps.microsoft.com/detail/oracle-mobile-authenticator/9NBLGGH4NSH8?hl=en-us&gl=US>). Click Install and wait while the app installs. Click Open.
8. In the Oracle Mobile Authenticator app, click the plus sign to add an account.
9. Click the **Enter Key Manually** link.
10. In the **Select Account Type** window, select **Oracle**.
11. Type in the friendly name from step 6 into the **Account** field. Type in the key from step 6 in the **Key** field. Click the **Save** button.
12. A password will appear in the Oracle Mobile Authenticator. Switch back to the CUNY Login Advanced Authentication - Setup Mobile Authentication page and click **Verify Now**. A Verification Code field is added to the CUNY Login Advanced Authentication - Setup Mobile Authenticator page.
13. In the **Verification Code** field on the CUNY Login Advanced Authentication - Setup Mobile Authenticator page, type the one-time password code from your Oracle Mobile Authentication app and click **Verify and Save**. The CUNY Login Advanced Authentication - Manage your authentication page is displayed with an Authentication Factors window showing the Mobile Authenticator - TOTP MFA account just added.

If you need assistance or have any questions:

- Contact the BCC [help desk](#) for assistance if:
 - You lost or are replacing the mobile phone used for CUNY Login MFA
 - Having issues with your CUNY Login
 - Having issues setting up or using CUNY Login MFA
- a. BCC help Desk Contact information
 - **Phone Number:** 718-289-5969
 - **Hours of operation:** Mon-Fri 8 am to 7 pm, Sat 9 am to 1 pm
 - Email: TSC@bcc.cuny.edu