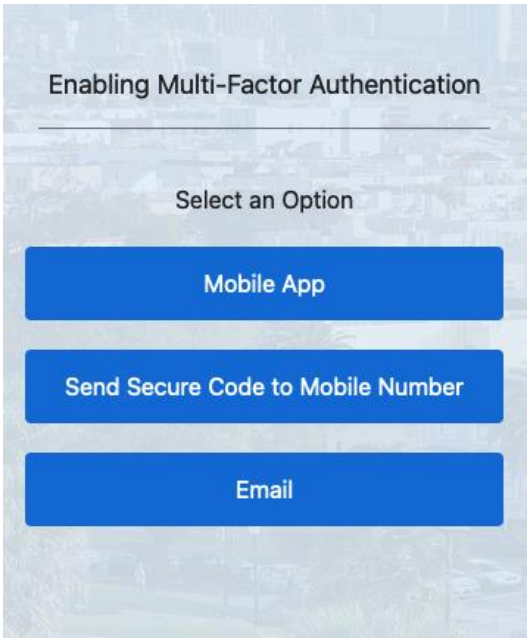
User Guide: Register Multi-Factor Authentication (MFA)

Table of Contents

User Guide: Register Multi-Factor Authentication (MFA)

The MyApps Portal requires users to set up at least two multi-factor authentication (MFA) methods after validating their login credentials to access their account.

1. Enroll first MFA factor



Go to https://myapps.sfgov.org/.

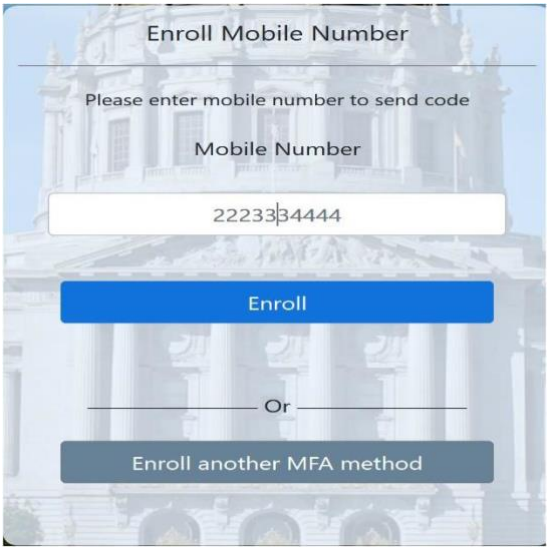
Enter username:
(Employees use DSW number,
POIs use POI number,
Contractors use loginID,
Suppliers use supplierID number)
and password.

Click “Agree & Sign in”.

After validating login credentials, the user will see a window that asks to enroll in at least one MFA factor such as Mobile App, SMS to Mobile Number and Email.

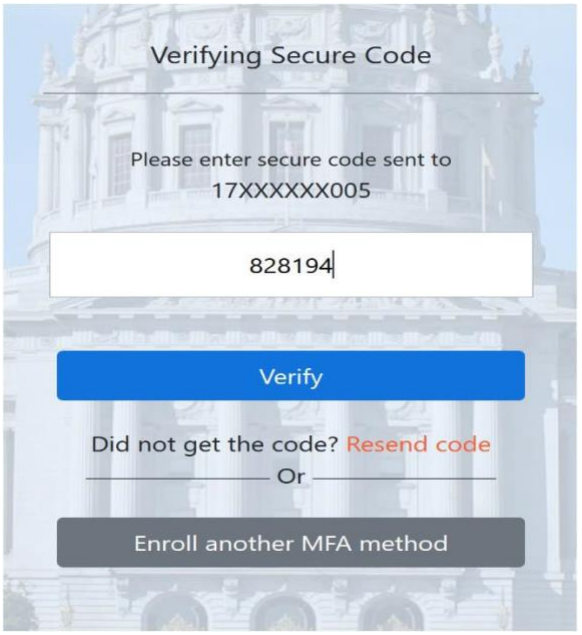
1.1 Enroll Mobile Number

- Click “**Send Secure Code to Mobile Number**” button.



- Then, it will open a new window where a user must **enter** a mobile number and click “**Enroll**” button to receive a mobile message with a secure code.

- Enter the secure code that you received on your mobile number and click the "**Verify**" button to complete the enrollment of mobile number as shown in the image:



- Click the "**Done**" button to get access to the account or click "**enroll other factors**" to setup others such as email or mobile app.

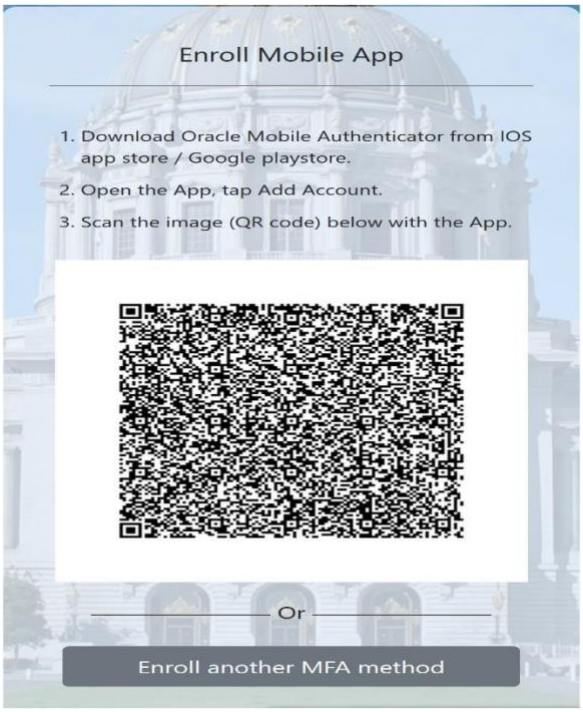
1.2 Enroll Mobile App

- Click the "**Mobile App Notification**" button.

  Note: **Download** the Oracle Authentication Mobile App from the iOS App Store or Google Play Store.

- After clicking "mobile app notification", a user will see a screen with **QR code to scan** as shown:

- Once the app is installed on your phone, open the camera from the Oracle Authenticator app and **scan** or hover the camera over the QR code as showing in the below image.



- After the QR code has been scanned, you will be asked to add a new device or overwrite an existing one. If this is your first time setting up the app, please select add a new device.

- After the mobile application has been installed and configured on your mobile device, you will see the following screen on your computer:

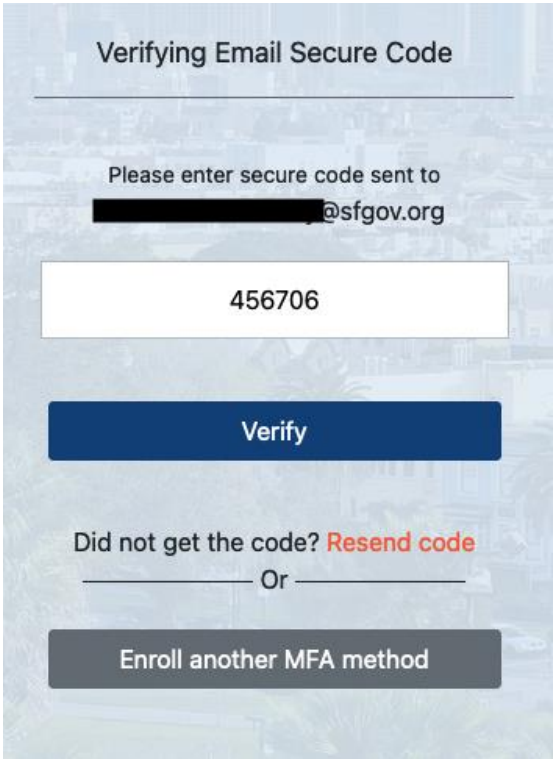
- Click the "**Done**" button to get access to the account or click "**enroll other factors**" to setup email or a mobile phone.

1.3 Enroll Email

- Click "**Email**" button.

- A new window opens and asks the user to enter the One Time Passcode (OTP) sent to their email.

- Enter the One Time Passcode (OTP) that you received on your email and click the "**Verify**" button to complete the enrollment of email as shown in the image.



- Click the "**Done**" button to get access to the account or click "**enroll other factors**" to setup others such as email or mobile app.

2. Enroll second MFA factor

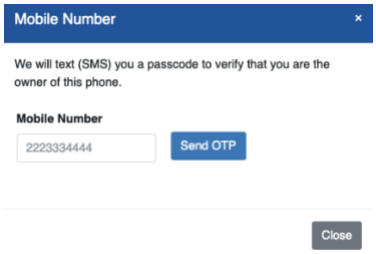
Users are allowed to add multiple Mobile App, SMS, and FIDO authentication factors; however, they can add only one email factor.

To add a new MFA factor, click “Configure” on the tile or click the arrow on the MFA menu  and choose one of ‘Add FIDO Authenticator’, ‘Add Mobile App’, ‘Add Mobile Number’.

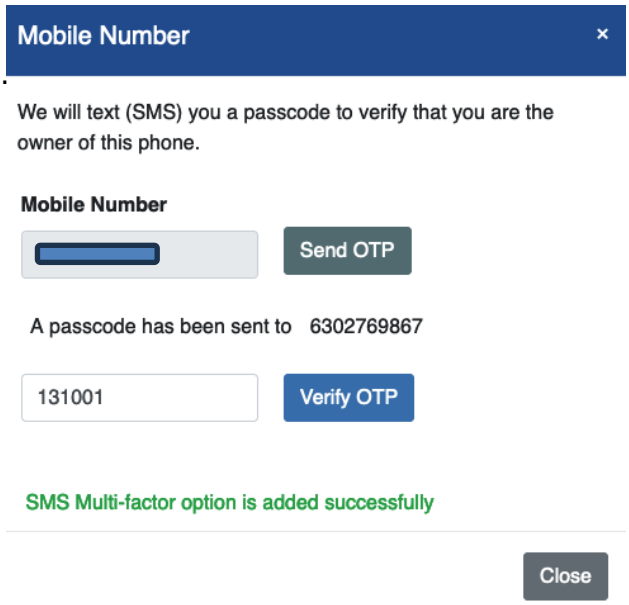
2.1 Enroll Mobile Number

To add a new Mobile Number (SMS Factor)

- Click ‘Configure’ on the Mobile Number tile or click ‘Add Mobile Number’ menu from the MFA menu (burger)
- On the pop-up window enter the mobile number you wish to enroll, then click **Send OTP** button.



- On the next page, enter the One Time Passcode received on your mobile and click **Verify OTP** button. The message “SMS Multi-factor option is added successfully” will be displayed.



2.2 Enroll FIDO Factor

You can enroll for FIDO authentication in the **MyApps Portal** after your first successful login using any of the above MFA options. Different FIDO options are explained below.

2.2a Windows Hello

In the Windows operating system, navigate to “Sign-in options” using search or by pressing the Windows key and typing “sign-in”. Windows Hello sign-in options include Windows Hello Face, Windows Hello Fingerprint and Windows Hello Pin.

Additional help:
Windows Hello for Business documentation
Windows sign-in options and account protection
Should any questions about this event or the need for immediate assistance arise, contact your department’s service desk, or the DT Service Desk at (628) 652-5000, or email dtis.helpdesk@sfgov.org.

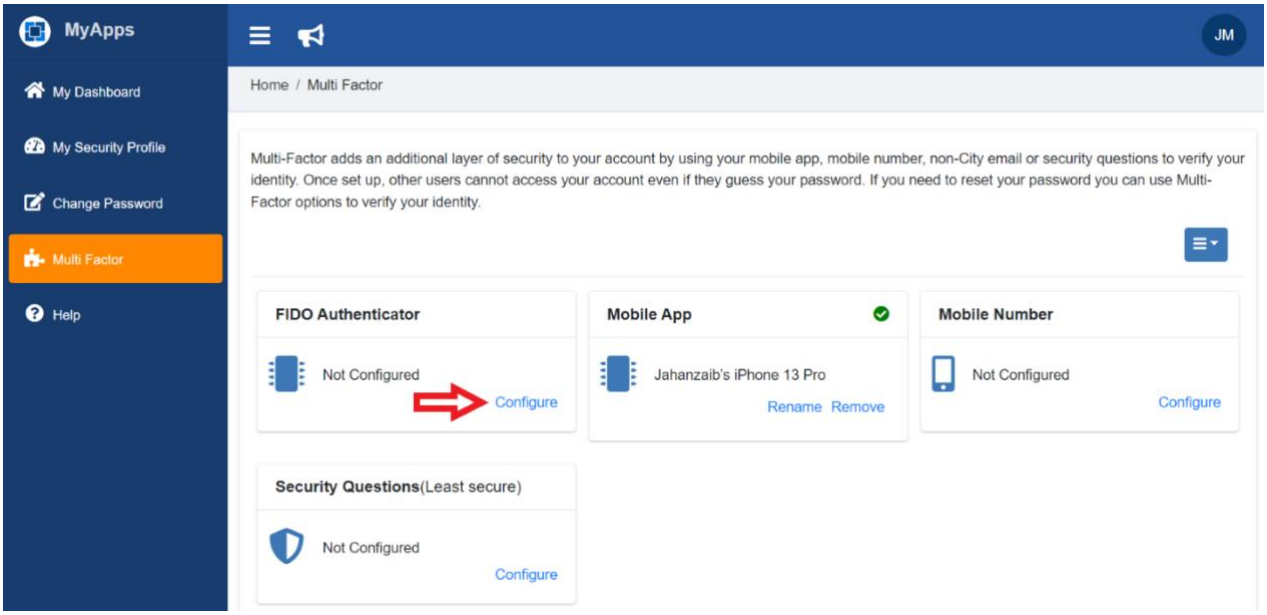
2.2b Mac Touch ID (Chrome Browser only)

See the Apple support page here for guidance.

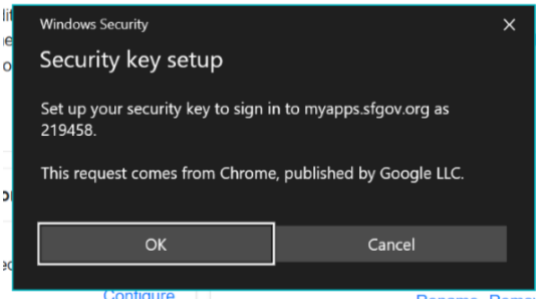
2.2c YubiKey USB device

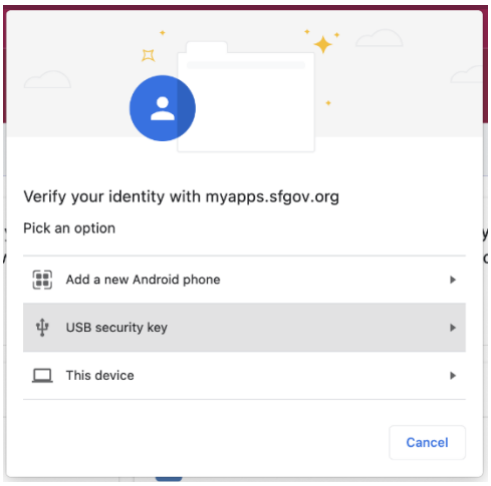
Note: Before enrolling for the FIDO MFA, you should have a **YubiKey** Security Key that is initially setup with PIN and Fingerprint(s). For detailed information on how to setup a YubiKey in **Windows** or **Mac/Chrome** refer to the FIDO User Guide.

- Assuming you have an already setup **YubiKey** we can move on and enroll it into MyApps.
- Look for the **FIDO Authenticator** Tile and click on **Configure.** If you already have a **FIDO Authenticator** added and wish to register another **FIDO Authenticator** device, go to the dropdown menu in the top right and click **Add FIDO Authenticator**.



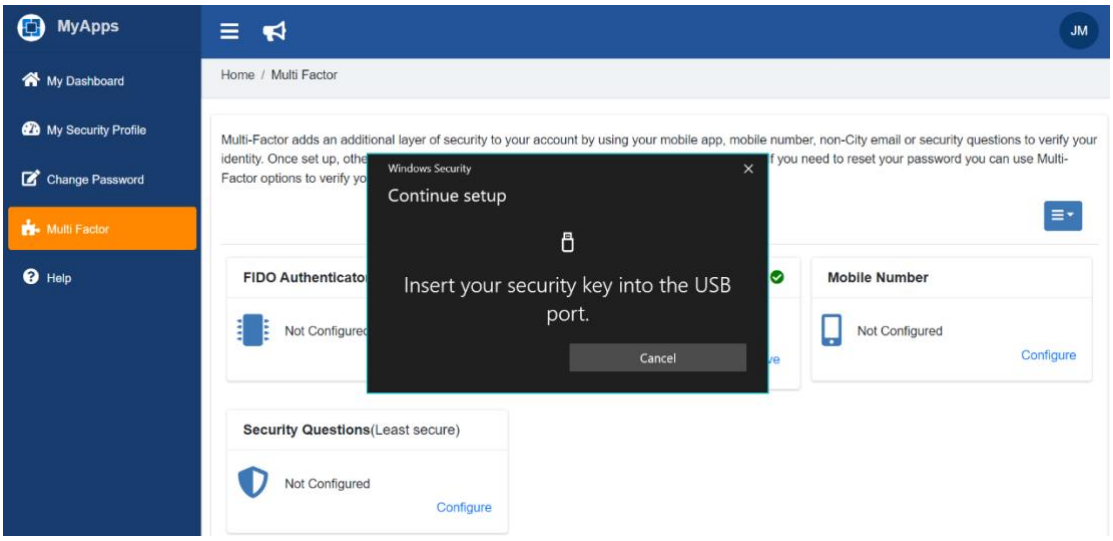
- You will now see a **Windows Security** pop-up prompting for a **Security Key Setup**. Click **OK.** In case of **Mac or Chrome** a dialogue should pop-up asking you to choose how to "Verify your identity." Select "**USB security key**." (You may also use one of the other options to use other multi-factor authentication methods; these will not use your YubiKey.

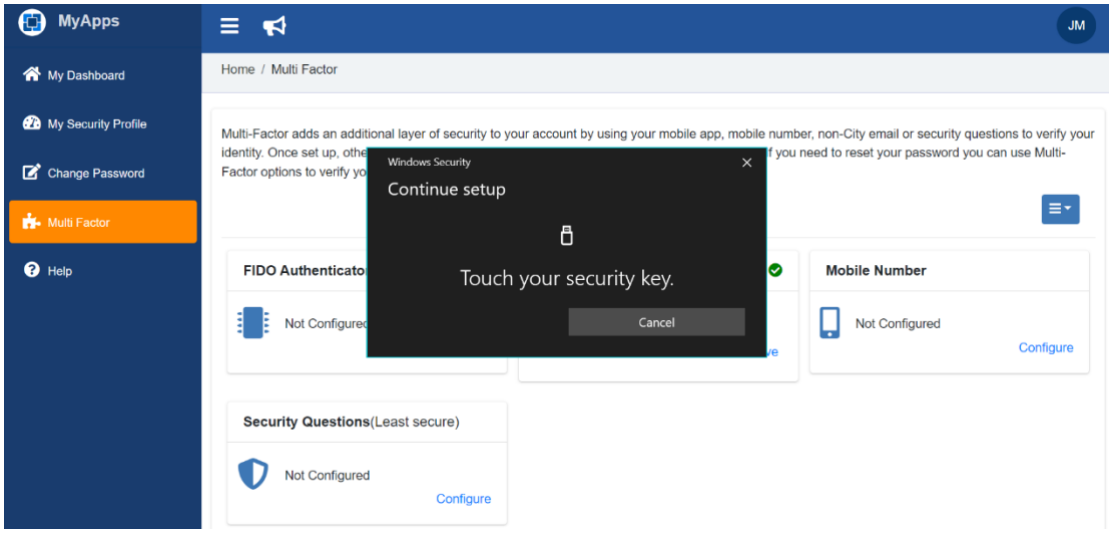




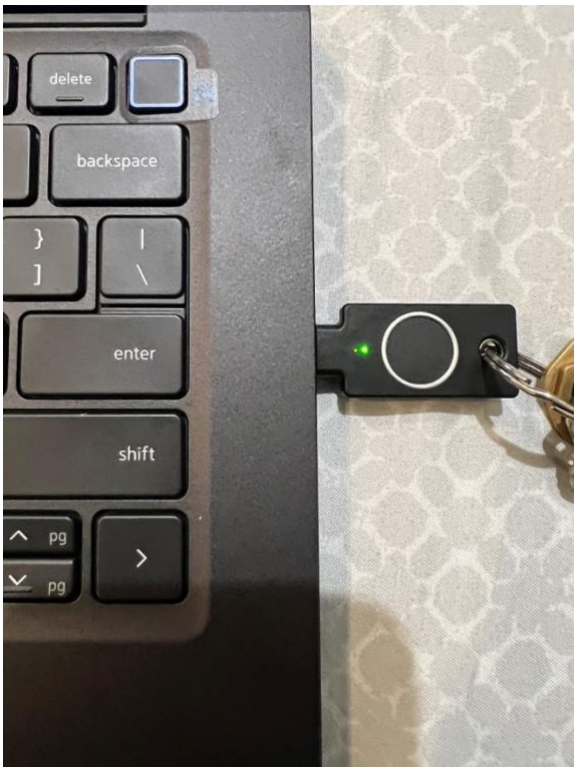
Windows **Mac/Chrome**

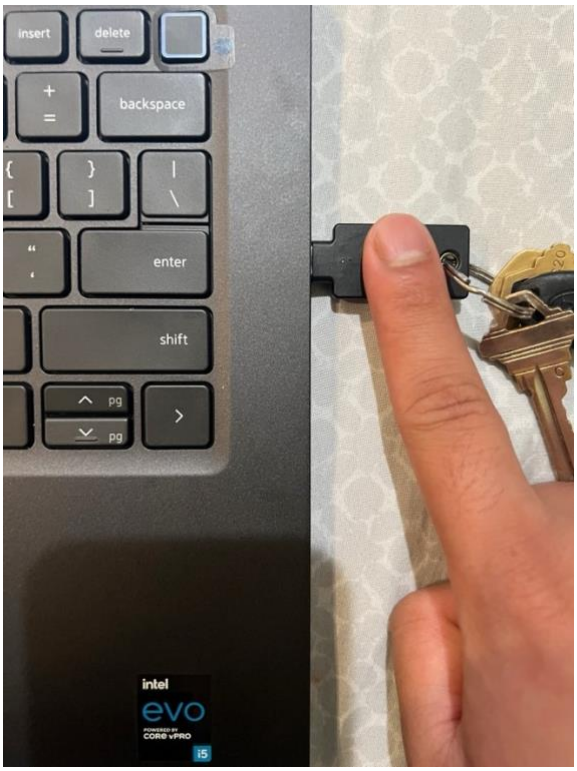
- You will now be prompted to **Insert your security key into the USB port** (if not already inserted) and **Touch your security key.**



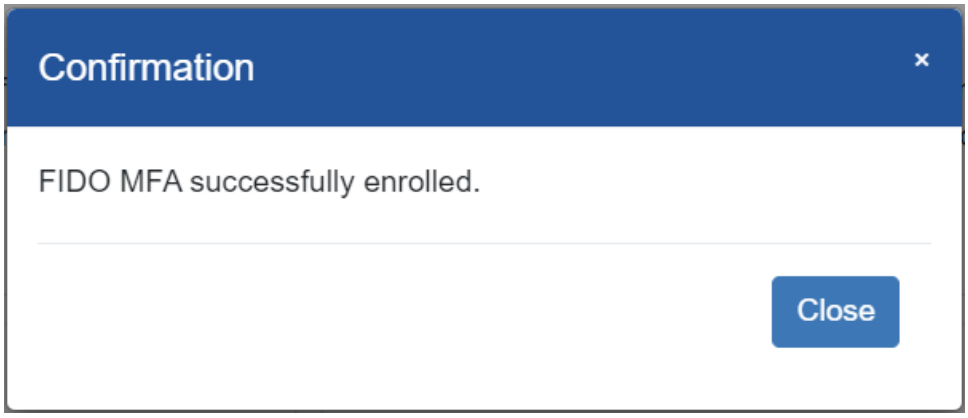


- Go ahead and touch the **YubiKey Bio** sensor while the **Green LED** is still flashing, making sure to touch the ring-bezel as well. It should look something like this.





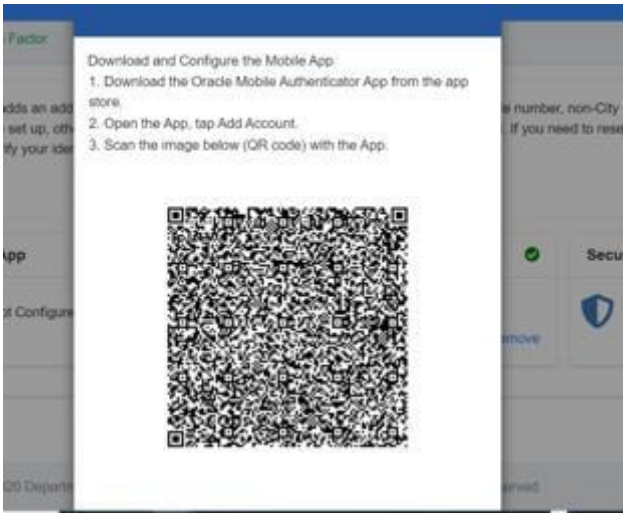
- If the fingerprint matches any of the fingerprints registered in that YubiKey, you should see a confirmation saying **FIDO MFA successfully enrolled.** Otherwise, **Red LED** will blink which means the fingerprint was not recognized and you may want to try again.



- You can now use your YubiKey to sign in. You will be prompted to insert the key and tap the fingerprint reader when signing in, if you choose YubiKey as your MFA factor. You can make YubiKey your default authenticator by following the steps in the next section.

2.3 Enroll Mobile App

- Click ‘Configure’ on the Mobile App tile or click ‘Add Mobile App’ from the MFA menu (burger)
- Note: Users can download the Oracle Authentication mobile app from the mobile iOS App Store or Google Play Store.



- A pop-up box will appear in the middle of the screen as shown below:

- Once the app is installed on their phone, users can open the camera from the Oracle Authenticator app and scan or hover the camera over the QR code (shown in the image below).

- Once users scan the QR code, a pop-up box will appear on their mobile screen, asking them to add a new device or overwrite the existing one. If using the authenticator app for the first time, users should select “add new.” Otherwise, users can select “overwrite.”

- Once the QR code has been canned in the authenticator app and configuration is done, select “close” to see the enrolled device info in the mobile app section.

3. Authenticate using MFA to access the MyApps Portal

After enrolling in MFA users will need to authenticate using MFA to gain access to the MyApps Portal.

- If a user has set **email** authentication as their default, they will see the following screen.

- The user should follow the instructions on screen to enter the secure passcode received by email.

- Click the "**Verify**" button. The user will be redirected to the MyApps Portal dashboard.

- If a user has set **mobile number** authentication as their default, they will see the following screen.

- The user should follow the instructions on screen to enter the secure passcode received by their mobile device.

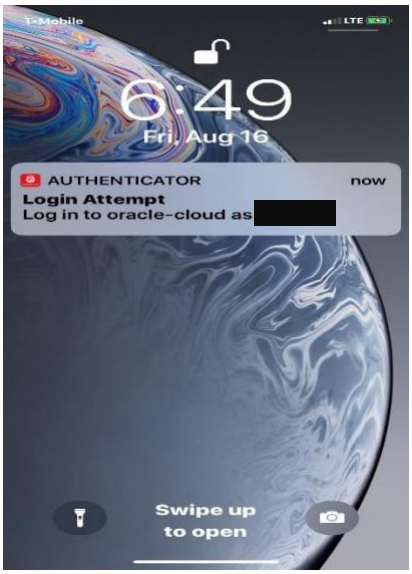
- Click the "**Verify**" button. The user will be redirected to the MyApps Portal dashboard.

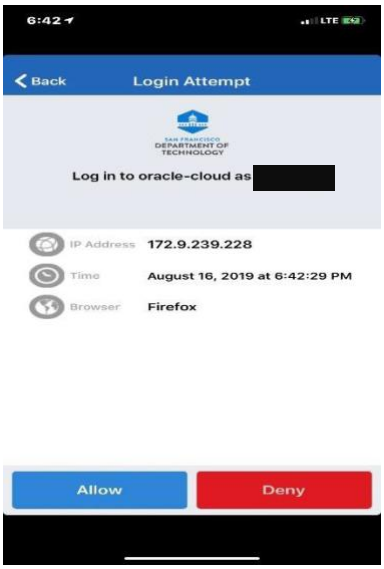
- If a user has set **mobile app** authentication as their default, they will see the following screen.

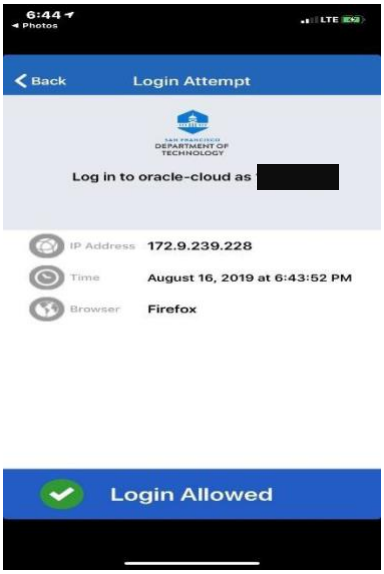
- The user should follow the instructions on screen to approve the push notification received by their mobile device.

- Open the push notification in the "**Oracle Authentication App**" on the user's mobile device.

- Tap the "**Allow**" button on the mobile device. After few seconds, the user will be redirected to the MyApps Portal dashboard.

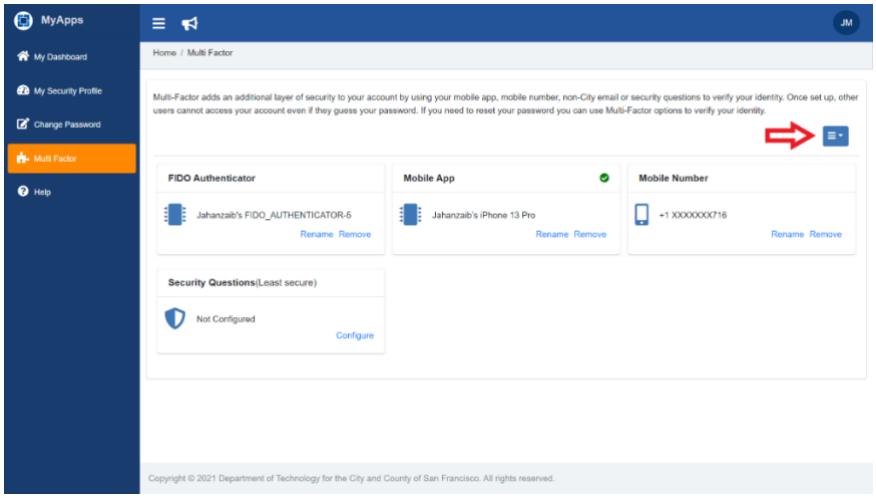


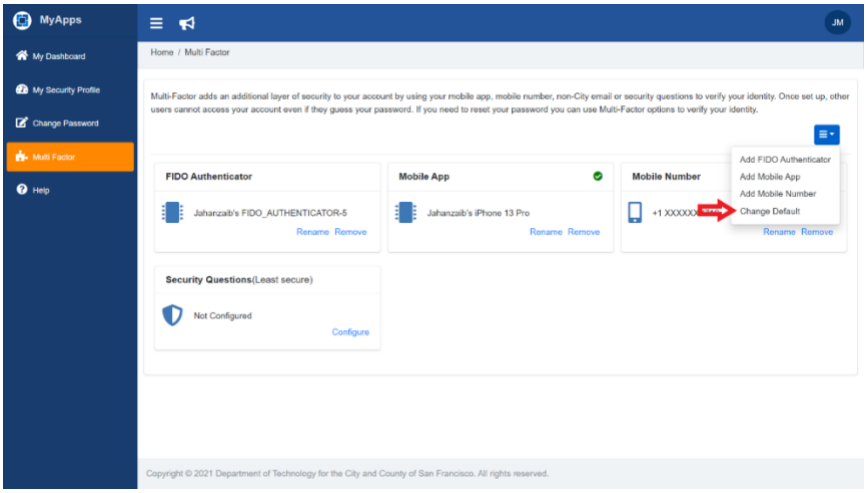




- A user can also check the box **"Trust this device for 30 days"** to prevent MFA verification each time a user access MyApps portal.

4. Set default MFA Factors

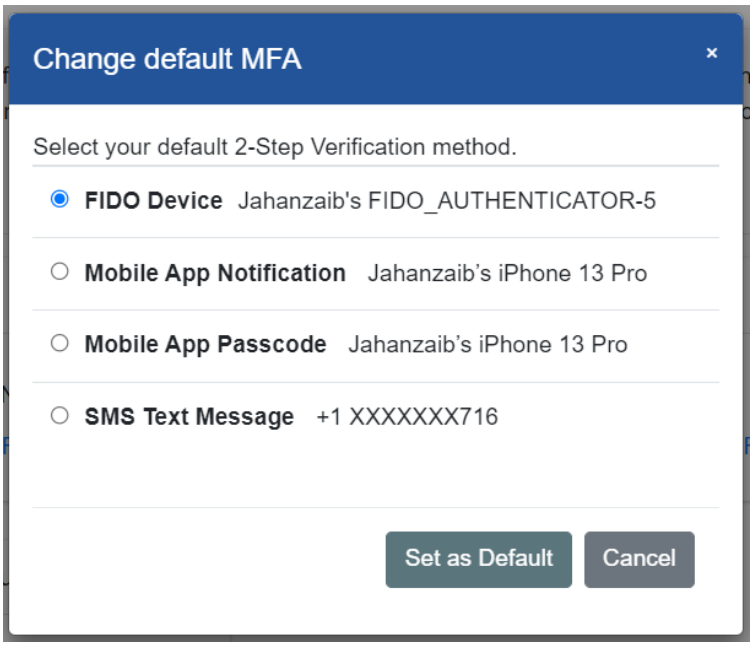




- This feature helps a user to choose which MFA factor they want to use for authentication when accessing the MyApps Portal from an external network.

- Click the "**Change Default**" button.

- After clicking the "Change Default" button, a new pop-up screen will appear as shown:

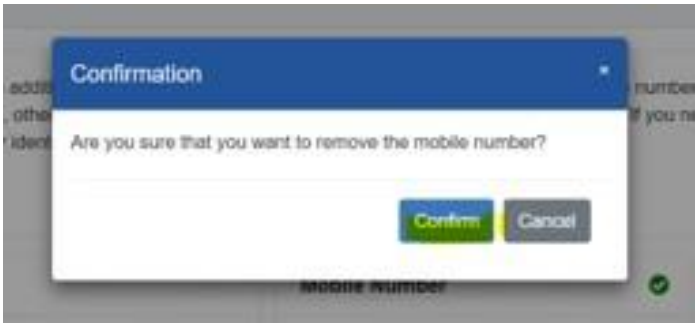


- Users can select an MFA factor such as Email, Mobile Number, Mobile App or FIDO Device by choosing a radio button from the list.

- Once a radio button is selected, click the "**Set as Default**" button.

5. Remove MFA Factors such as Security Questions, Mobile Number and Mobile App

- Users should select the MFA factor they want to remove such as Email, Mobile Number or Mobile App. For example, if they want to remove an email MFA factor, they can go to the email section and click the **"Remove"** button on the right side of the pane as shown in the image.



- After clicking "remove", you will see a pop-up box that will ask you to confirm your selection again.