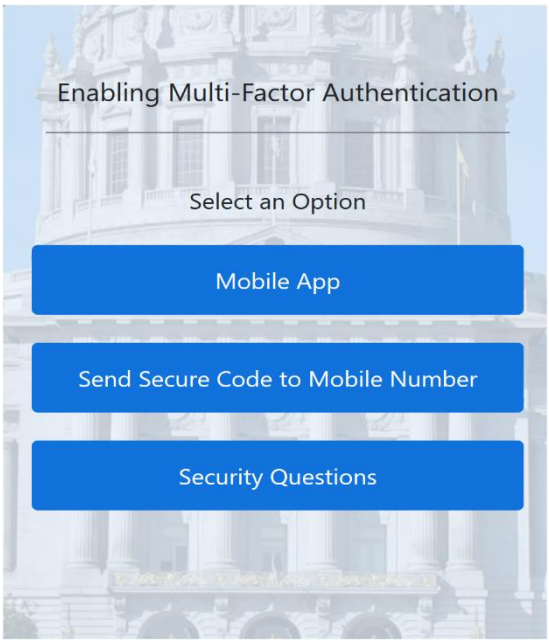
User Guide: Register Multi-Factor Authentication (MFA)

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

1. Enroll MFA Factors



Go to “myapps.sfgov.org”.

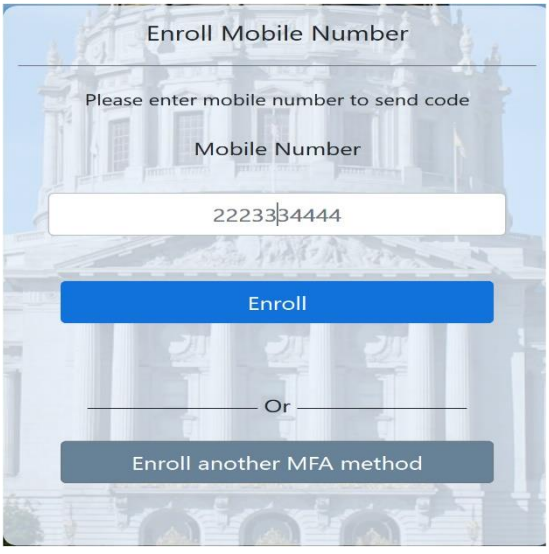
Enter username (for employees #DSW, POI’s - #POI number, contractor’s- loginID, Suppliers- #supplierID) and password

Click “Agree & Sign in”.

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

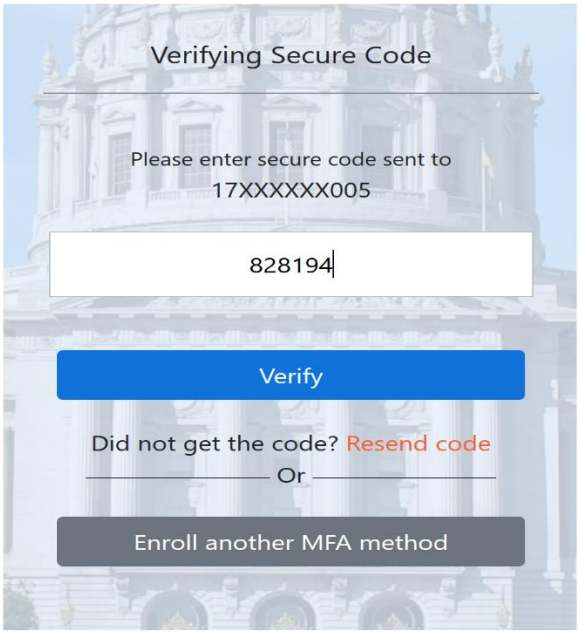
1.1 Enroll Mobile Number

- 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:



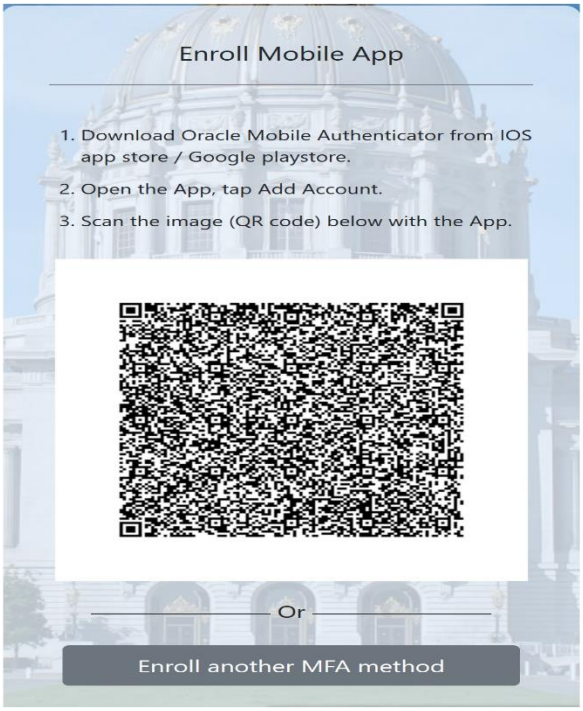
- Click the "**Done**" button to get access to the account or click "**enroll other factors**" to setup others such as email or mobile app.

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.

2. 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.

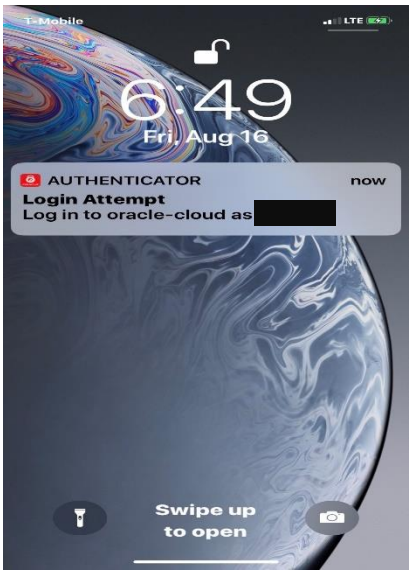
- Click the "**Verify**" button. The user will be redirected to the MyApps Portal dashboard.

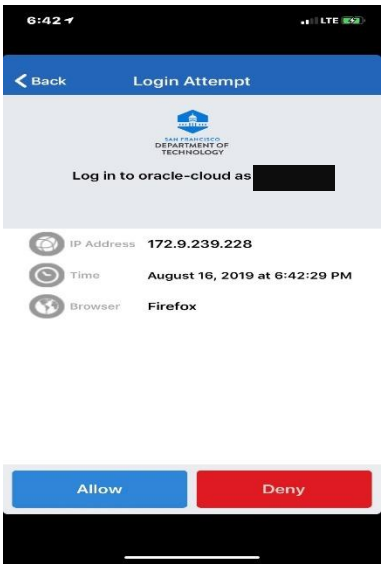
- If a user has set **mobile app** authentication as their default, they will see the following screen.

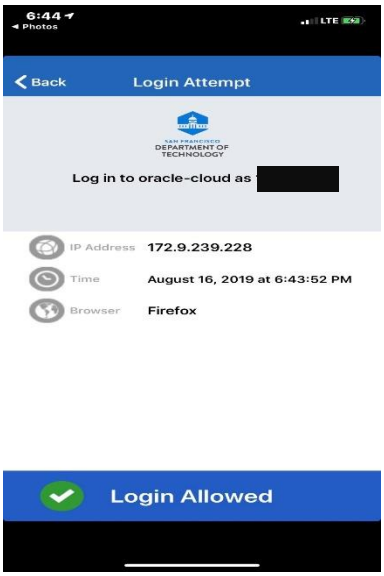
- The user should follow the instructions on screen to approve the push notification received by their mobile device.

- 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.





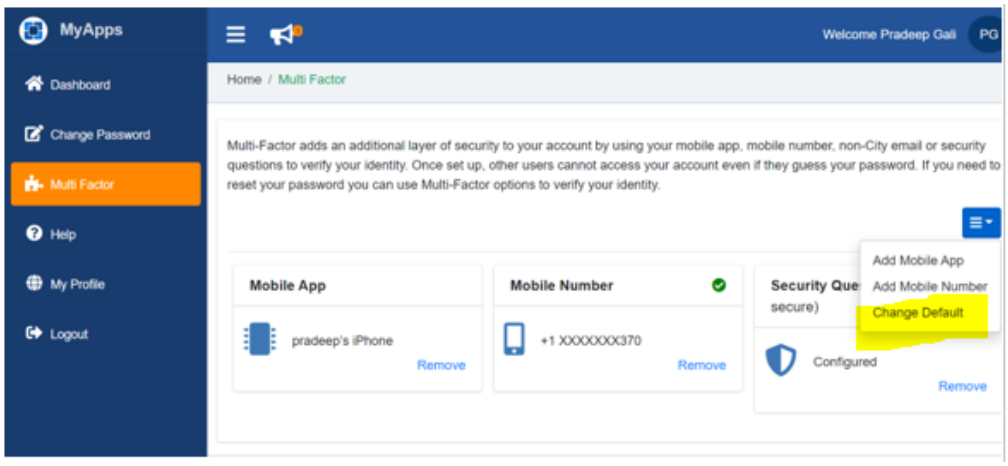


- A user can also check the box **"Trust this device for 30 days"** to prevent MFA verification each time a user access MyApps portal.

Choosing the Default MFA Settings

To enhance the security of user accounts and City services, the MyApps Portal requires users to set up Multi-Factor Authentication (MFA) for their account.

1. Click "Multi Factor" from the portal



- On the Multi-Factor verification page, you can see all the enrolled MFA Factors.

2. Click on “Change Default”

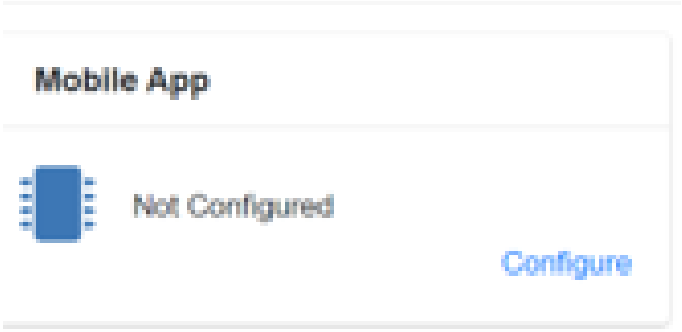
Users can **Enroll** into MFA through Email, a mobile phone, and the Oracle Mobile Authenticator App**.**

- Use the “**Set as Default**” feature to change the default method.

All the functionalities mentioned above are explained below in detail.

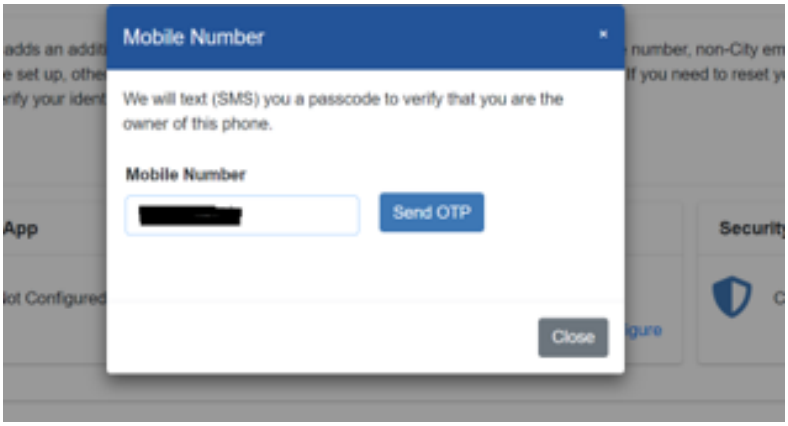
2.1 Enroll Authentication Factor

1.a.1 Enroll Mobile Number

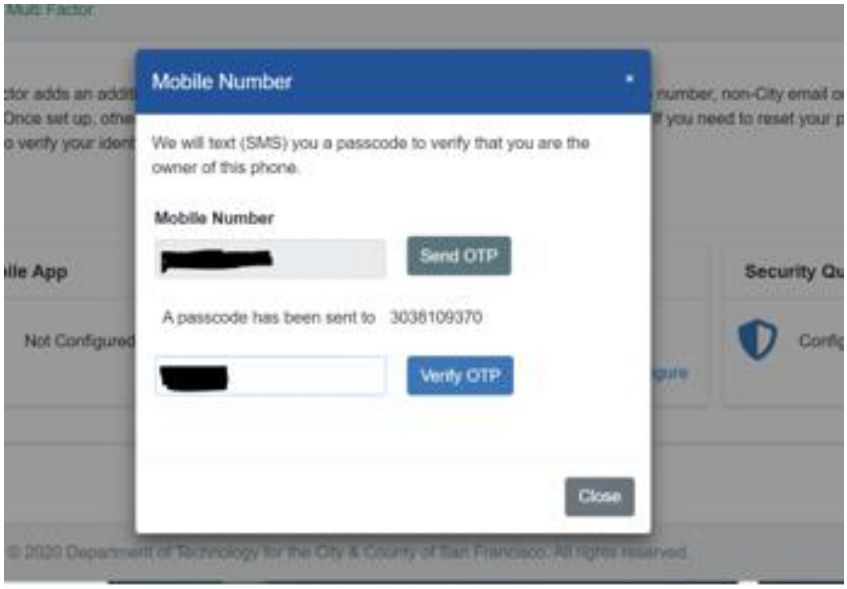


- Click the “Configure” button in the mobile number section.

Note: Users have the option of adding more than one contact number.

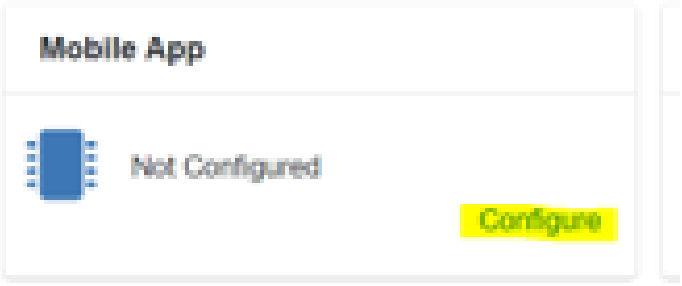


- After clicking the “Configure” button, a pop-up window will appear where users must enter their mobile number. Users can then click “Send OTP” to get a message sent to their device as shown in the image:

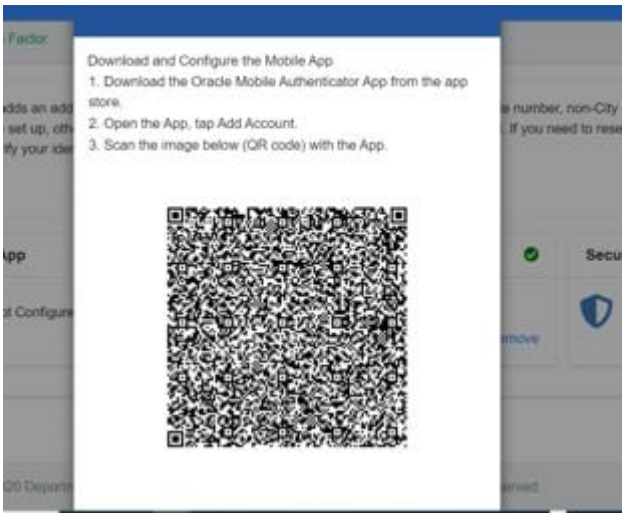


- Users can enter the code received on their mobile number and click “Verify OTP” to complete the enrollment of a mobile number as shown in the image:

1.a.2 Enroll Mobile App



- Click the “Configure” button in the mobile app section.
- Note: Users can download the Oracle Authentication mobile app from the mobile iOS App Store or Google Play Store.

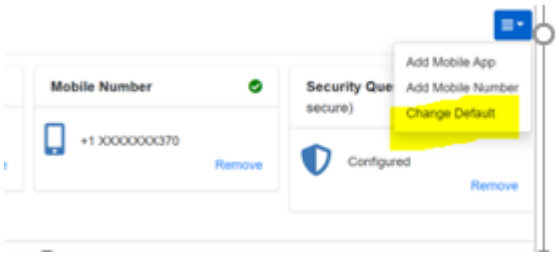


- A pop-up box will appear in the middle of the screen as shown below:
- Once the app is installed on their phone, users can open the camera from the Oracle Authenticator app and scan or hover the camera over the QR code (shown in the image below).

- 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.

2.2 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.

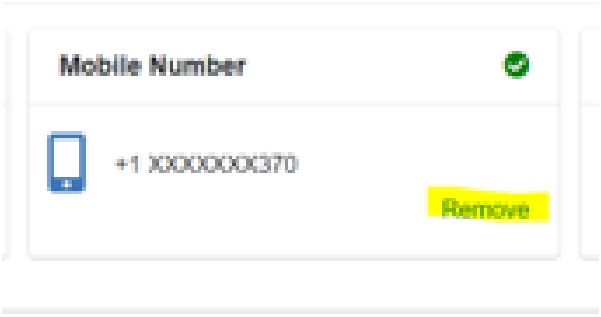
- Click the “**Change Default**” button.

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

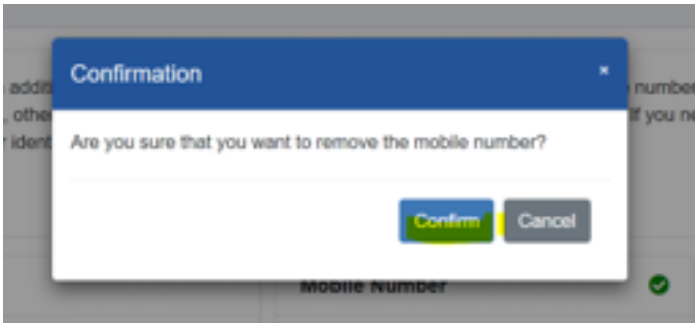
- Users can select an MFA factor such as Email, Mobile Number, or Mobile App by choosing a radio button from the list.

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

2.3 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.