Indiana Office of Technology
Powering a State that Works

# Multi-Factor Authentication (MFA) / PhoneFactor Mobile App Registration for existing users currently using Phone call or Text verification

## Requirements before starting:

In order to successfully register your smart phone with the State of Indiana MFA service you will need access to a computer with internet access and a modern internet browser such as Microsoft Edge, Google Chrome, Firefox or Safari. Additionally, you will need your Apple iOS or Android smartphone and access to its respective app store (Apple App Store or Google Play Store. For state issued iPhones you can obtain the app from the current MDM store or have it pushed to your device).

Additionally, these instructions assume you already have registered your account with the State of Indiana MFA service and are not currently using the MFA app method for your default verification. If you have not already registered your account with the State of Indiana MFA service, please reference the instructions for first time registration. If you already have setup your MFA application and are adding a new account and need assistance, contact the IOT Helpdesk for additional support options.

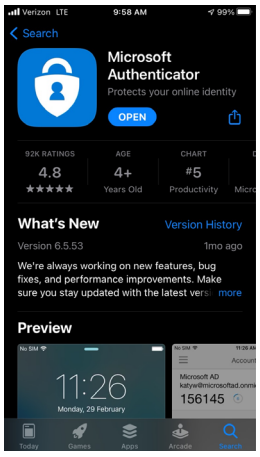
## Instructions:

1. Download the Microsoft Authenticator application. The only supported application that works with the State of Indiana Multi-Factor Authentication (MFA) service is the Microsoft Authenticator app. Third party authenticator applications are not supported at this time.

   For Apple iOS devices:

   https://apps.apple.com/us/app/microsoft-authenticator/id983156458

   or manually search for “Microsoft Authenticator” published by Microsoft Corporation in the Apple App Store.

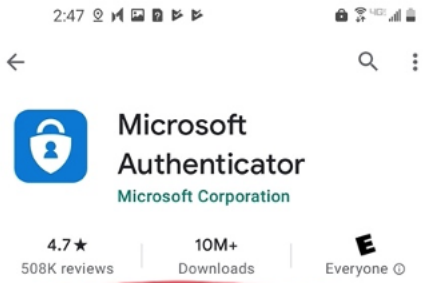



(Continued, Step 1. Download the Microsoft Authenticator application)

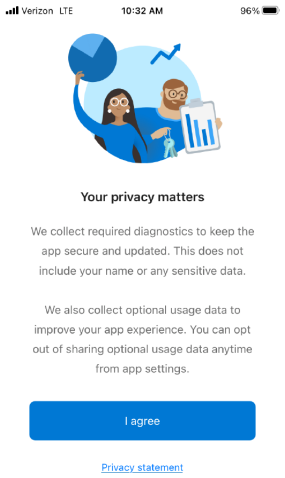
For Android devices:

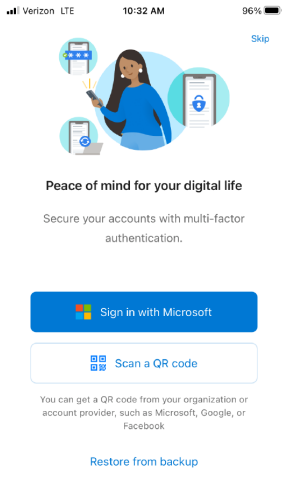
https://play.google.com/store/apps/details?id=com.azure.authenticator

or manually search for “Microsoft Authenticator” published by Microsoft Corporation in the Google Play Store.

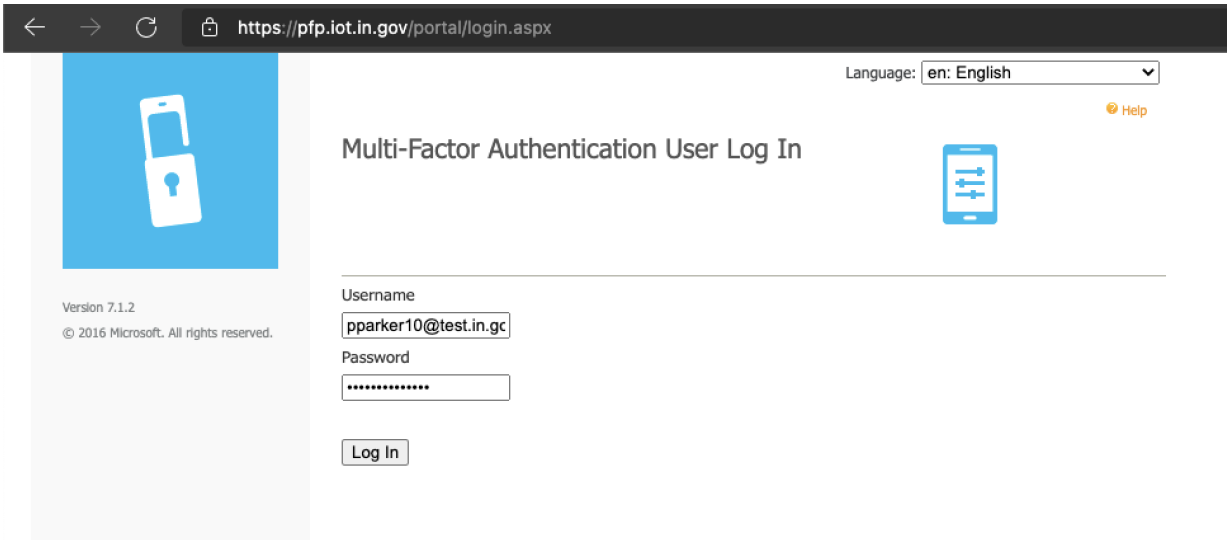


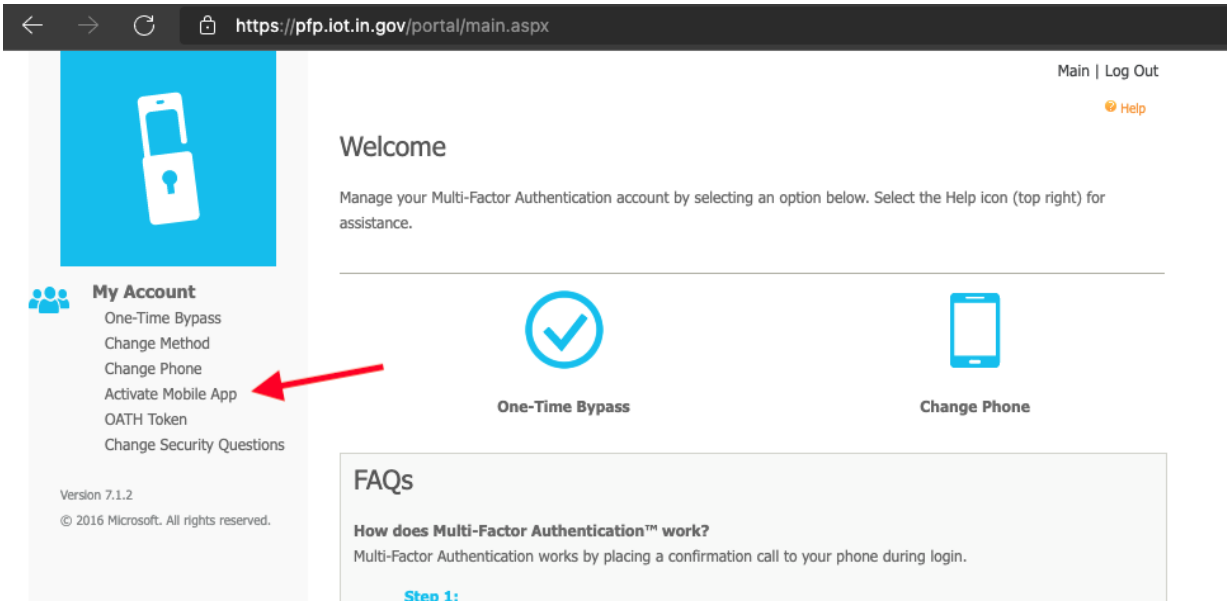

2. Follow any prompts necessary to download the Microsoft Authenticator application to your smart phone. Open the application and review the user and privacy agreements that you approve (you must agree in order to use the application). After accepting the agreement stop at the add account/scan QR code screen and proceed to the next step (Step 3, sign into MFA User Portal).



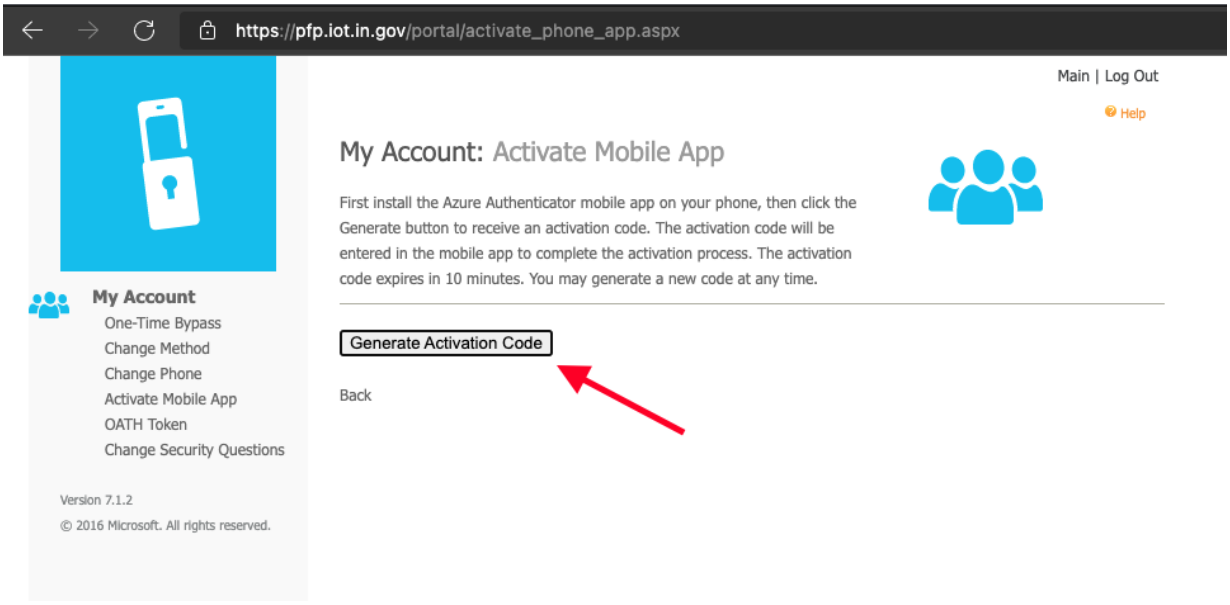



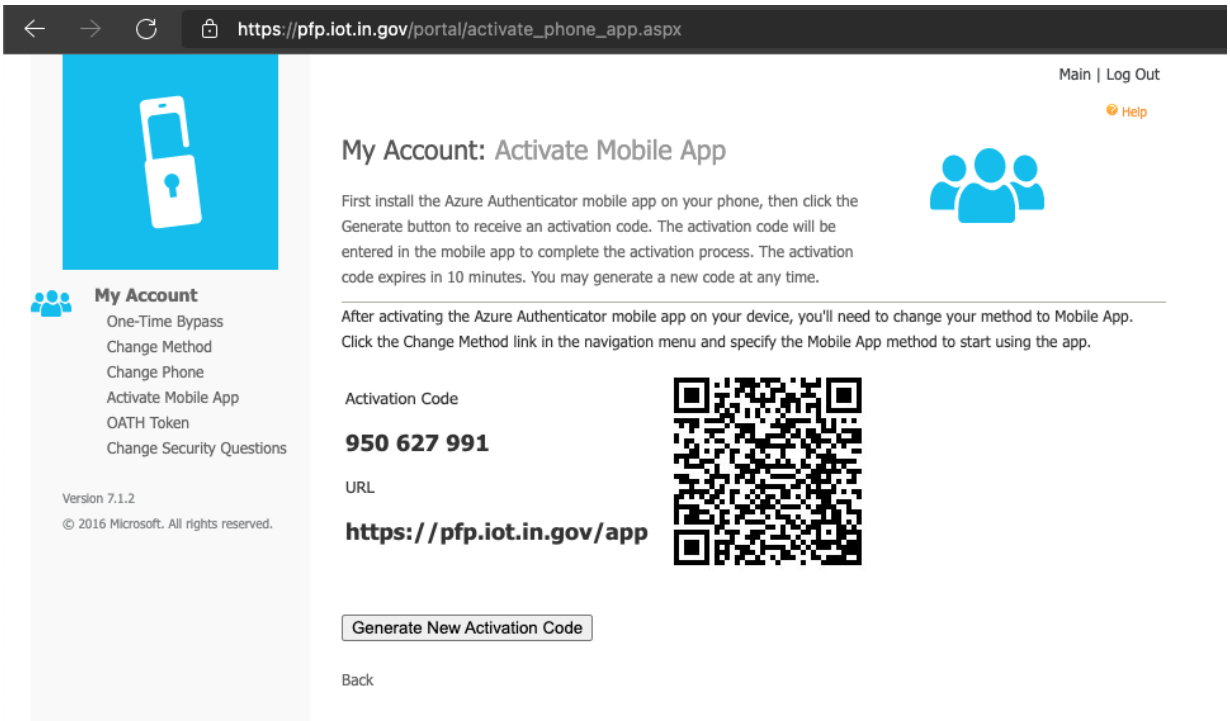
3. Log into MFA User Portal, https://pfp.iot.in.gov with your State of Indiana user account credentials. Your user name should be your email address (contractor accounts that do not have a state issued email account should use your UPN (User Principal Name) value). You are prompted by your current MFA method (phone call or text) to sign in to the portal:



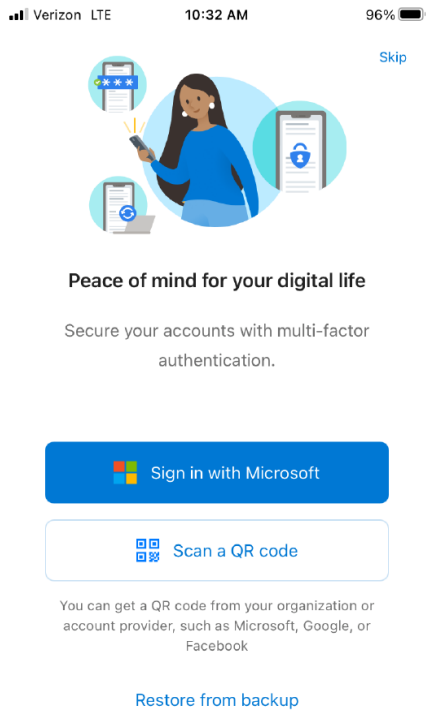



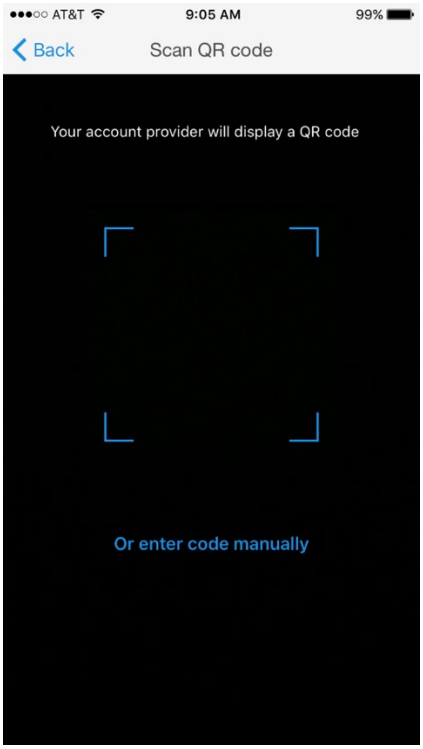
4. Select “Active Mobile App” from the “My Account” section in the left-hand menu, then click the “Generate Activation Code” button as shown below;



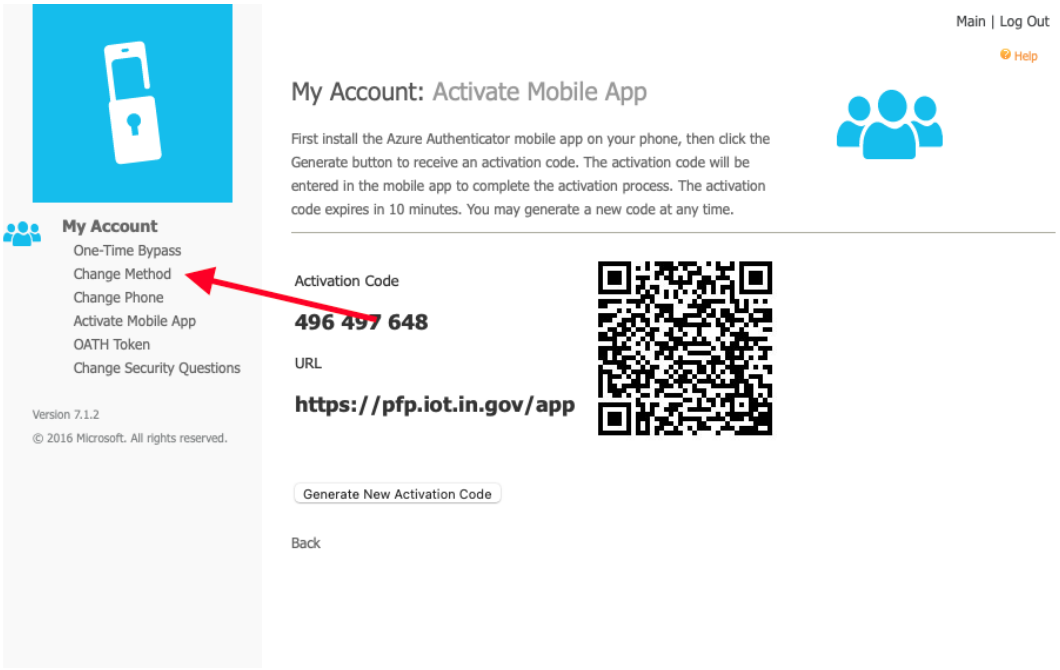
5. On your mobile phone click the “Scan QR code” button from within the Microsoft Authenticator app as shown from step 2 (you may need to allow permissions to the camera on your device, as well as permission to allow notifications, both are necessary to register and use the Authenticator app):



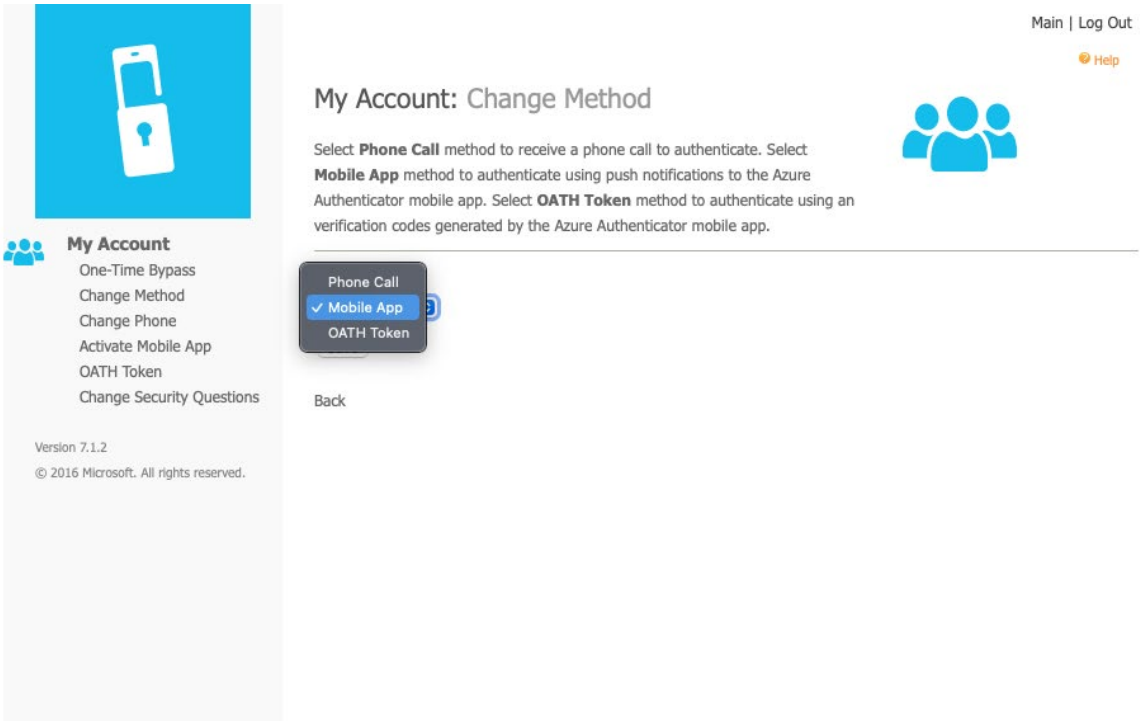




Once completing the scan, you will be returned to the account screen in the mobile app. Return to your computer and complete the registration process as shown in the next step (proceed to step 6).

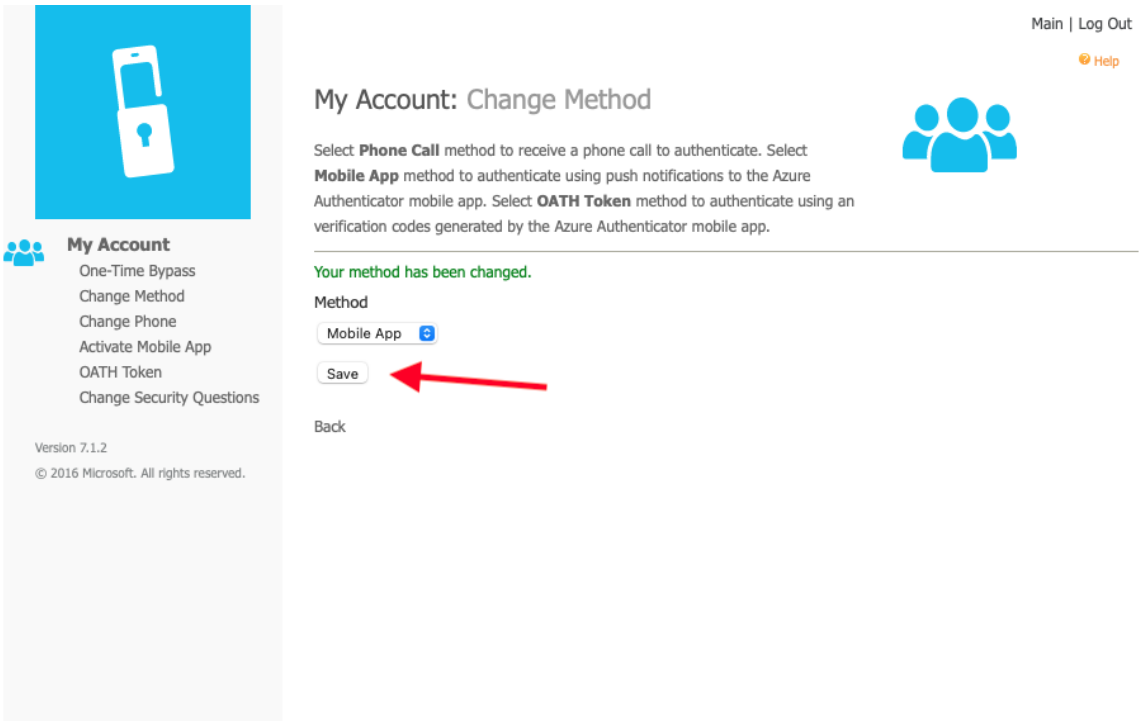
6. Back from within the user portal select “Change Method” from the left-hand menu:




From the “Change Method” screen, select “Mobile App” from the drop down menu;



When “Mobile App” has been selected be sure to click the “Save” button and verify the portal says method has saved.




Congratulations, you have successfully registered and switched your MFA method to the Microsoft Authenticator app. You can test by signing out of the MFA user portal and then signing back in.