



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.

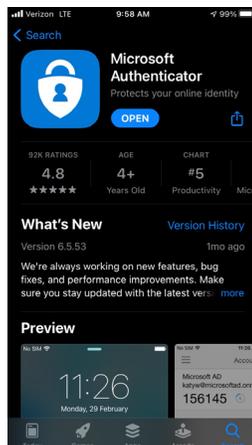
Instructions:

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)

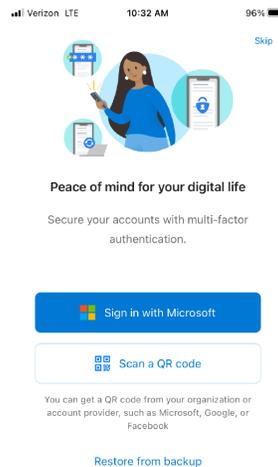
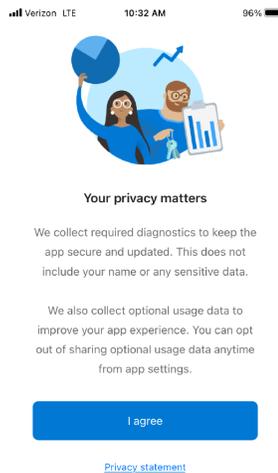
For Android devices:

<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:

The screenshot shows the login page for the Multi-Factor Authentication User Portal. The browser address bar displays <https://pfp.iot.in.gov/portal/login.aspx>. The page title is "Multi-Factor Authentication User Log In". On the left, there is a blue icon of a smartphone with a lock symbol. Below it, the text reads "Version 7.1.2" and "© 2016 Microsoft. All rights reserved.". On the right, there is a language dropdown menu set to "en: English" and a "Help" icon. The main content area contains a "Username" field with the value "pparker10@test.in.gc", a "Password" field with masked characters, and a "Log In" button.

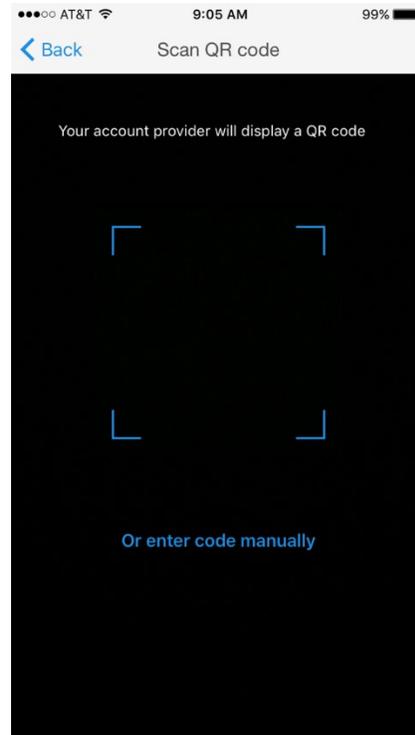
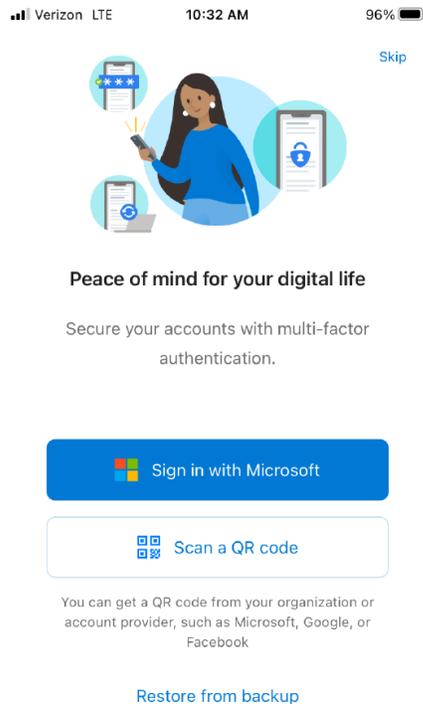
The screenshot shows the "Welcome" page of the Multi-Factor Authentication User Portal. The browser address bar displays <https://pfp.iot.in.gov/portal/main.aspx>. The page title is "Welcome". On the left, there is a blue icon of a smartphone with a lock symbol. Below it, the text reads "Version 7.1.2" and "© 2016 Microsoft. All rights reserved.". On the right, there is a "Main | Log Out" link and a "Help" icon. The main content area contains a "Welcome" heading and a paragraph: "Manage your Multi-Factor Authentication account by selecting an option below. Select the Help icon (top right) for assistance." Below this, there are two large buttons: "One-Time Bypass" (with a checkmark icon) and "Change Phone" (with a smartphone icon). A red arrow points to the "One-Time Bypass" button. At the bottom, there is a "FAQs" section with the heading "How does Multi-Factor Authentication™ work?" and the text: "Multi-Factor Authentication works by placing a confirmation call to your phone during login." Below this, the text "Step 1:" is visible.

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;

The screenshot shows a web browser at the URL https://pfp.iot.in.gov/portal/activate_phone_app.aspx. The page title is "My Account: Activate Mobile App". On the left, there is a "My Account" menu with options: One-Time Bypass, Change Method, Change Phone, Activate Mobile App, OATH Token, and Change Security Questions. The "Activate Mobile App" option is selected. Below the menu, it says "Version 7.1.2" and "© 2016 Microsoft. All rights reserved." On the right, there is a "Main | Log Out" link and a "Help" icon. The main content area contains the following text: "First install the Azure Authenticator mobile app on your phone, then click the Generate button to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes. You may generate a new code at any time." Below this text is a button labeled "Generate Activation Code" which is highlighted with a red arrow. There is also a "Back" link.

The screenshot shows the same web browser at the URL https://pfp.iot.in.gov/portal/activate_phone_app.aspx. The page title is "My Account: Activate Mobile App". On the left, the "My Account" menu is the same as in the previous screenshot. The main content area contains the following text: "First install the Azure Authenticator mobile app on your phone, then click the Generate button to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes. You may generate a new code at any time." Below this text is a new paragraph: "After activating the Azure Authenticator mobile app on your device, you'll need to change your method to Mobile App. Click the Change Method link in the navigation menu and specify the Mobile App method to start using the app." Below this paragraph, there is an "Activation Code" section with the code "950 627 991". Below the code is a "URL" section with the URL "https://pfp.iot.in.gov/app". To the right of the URL is a QR code. Below the QR code is a button labeled "Generate New Activation Code". There is also a "Back" link.

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:

Main | Log Out
Help

My Account: Activate Mobile App

First install the Azure Authenticator mobile app on your phone, then click the Generate button to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes. You may generate a new code at any time.

Activation Code
496 497 648

URL
https://pfp.iot.in.gov/app

Generate New Activation Code

Back

My Account
One-Time Bypass
Change Method
Change Phone
Activate Mobile App
OATH Token
Change Security Questions

Version 7.1.2
© 2016 Microsoft. All rights reserved.

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

Main | Log Out
Help

My Account: Change Method

Select **Phone Call** method to receive a phone call to authenticate. Select **Mobile App** method to authenticate using push notifications to the Azure Authenticator mobile app. Select **OATH Token** method to authenticate using an verification codes generated by the Azure Authenticator mobile app.

Phone Call
✓ Mobile App
OATH Token

Back

My Account
One-Time Bypass
Change Method
Change Phone
Activate Mobile App
OATH Token
Change Security Questions

Version 7.1.2
© 2016 Microsoft. All rights reserved.

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

The screenshot displays the 'My Account: Change Method' interface. On the left, a navigation menu includes 'My Account' with sub-options: 'One-Time Bypass', 'Change Method', 'Change Phone', 'Activate Mobile App', 'OATH Token', and 'Change Security Questions'. The main content area features a blue header with a mobile phone icon, followed by the title 'My Account: Change Method'. Below the title, instructions state: 'Select **Phone Call** method to receive a phone call to authenticate. Select **Mobile App** method to authenticate using push notifications to the Azure Authenticator mobile app. Select **OATH Token** method to authenticate using an verification codes generated by the Azure Authenticator mobile app.' A green message reads 'Your method has been changed.' The 'Method' dropdown is set to 'Mobile App', and a red arrow points to the 'Save' button. A 'Back' link is visible at the bottom. The top right corner contains 'Main | Log Out' and a 'Help' icon. The footer includes 'Version 7.1.2' and '© 2016 Microsoft. All rights reserved.'

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.