Popular Business Access

Token User Guide

POPULAR®

POPULAR®

Introduction

This Guide provides instructions for the registration, activation, and use of the Soft Token authentication solution. It explains how Soft Tokens function within Popular Business Access (PBA), the steps required for their enrollment and activation, and the authentication process used to securely access the system and authorize transactions. In addition, it provides information to help customers assign Soft Tokens to their authorized users, obtain additional support, and understand how the authentication mechanism works.

Prerequisites

Before activating a Soft Token, make sure that:

- A Soft Token license has been assigned to the user.
- The user has been granted access to Popular Business Access (PBA).
- The Popular Business Access mobile application is installed on the user's mobile device.
- The user has received the activation email containing instructions to complete the enrollment process.
- The user's email address and mobile phone number are current and available for authentication and activation purposes.

POPULAR®

Soft Token Registration

Follow the registration steps to activate Soft Token using QR code or activation password, then create PIN and enable biometrics.

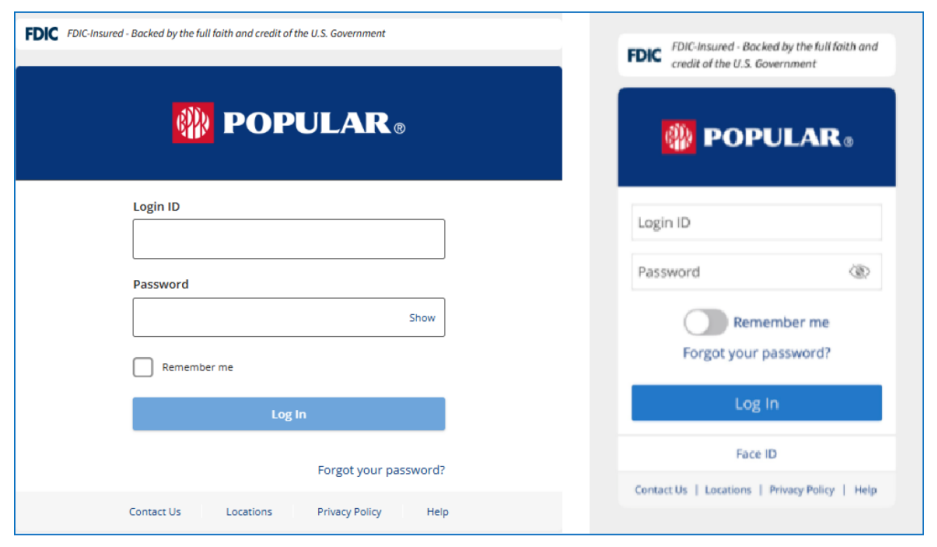
Soft Token Registration with Biometrics

1. To begin the registration process, the Users must have been assigned a Soft Token license. Once the license has been assigned, the Users will receive an email notifying them that the process has started, along with the credentials required to access Popular Business Access (PBA).

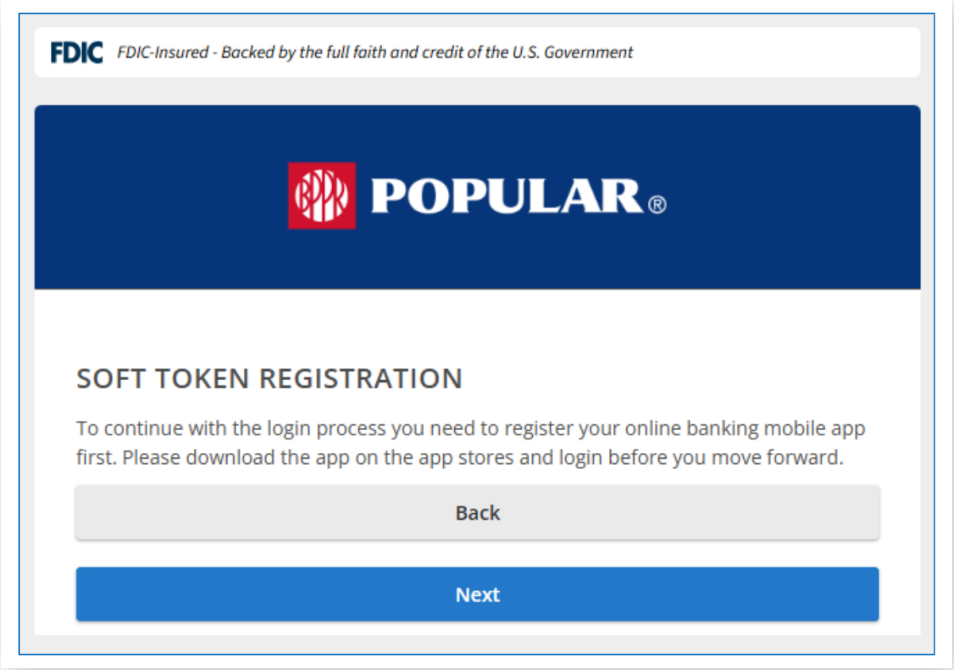
   This email will provide a link to Popular Business Access online banking platform and initial instructions for registering and activating the Soft Token.



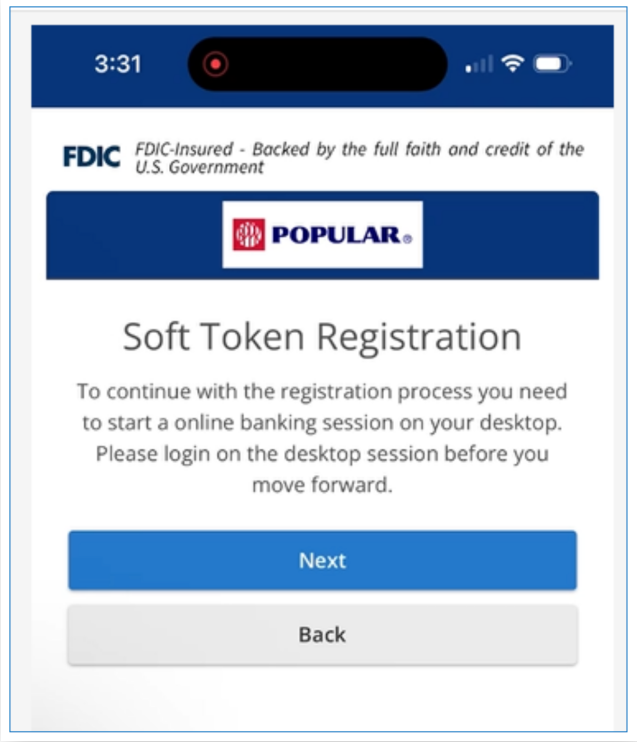
2. Before continuing, you have to access the Popular Business Access online banking website and download and configure the mobile application.



3. When login into the Desktop, the platform will require you to ensure to have logged into the mobile app.

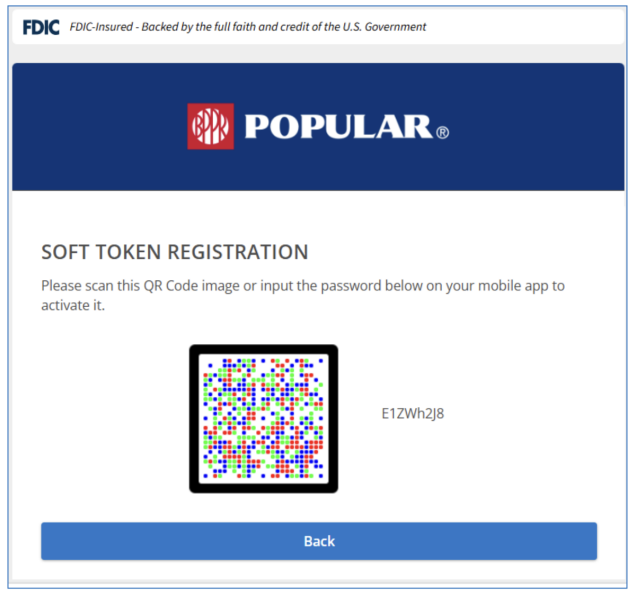


4. Log in through the Mobile Application. When logging in into the Mobile Application, the platform will require you to ensure you have logged into the Desktop app.

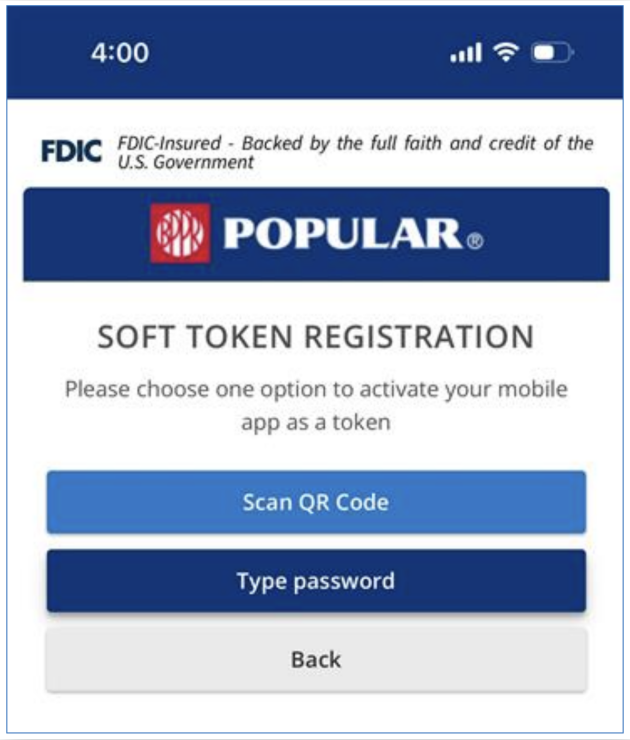


5. In both versions, click **Next**.

    a. The Desktop platform will display the QR Code screen. This screen will also display a unique password.

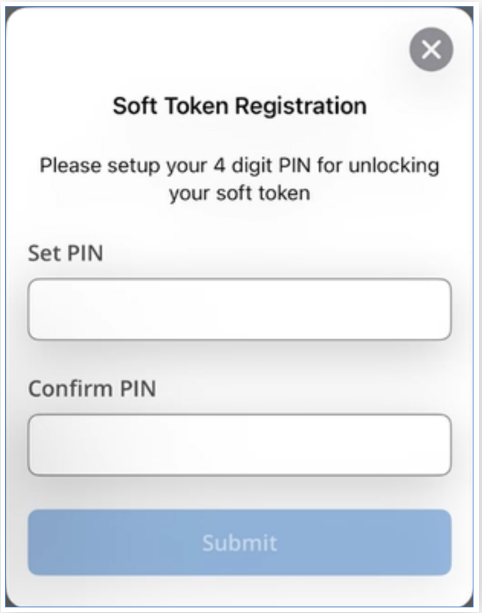


b. In the Mobile App, the platform will display the options to **Scan QR Code**, **Type password** and **Back**.

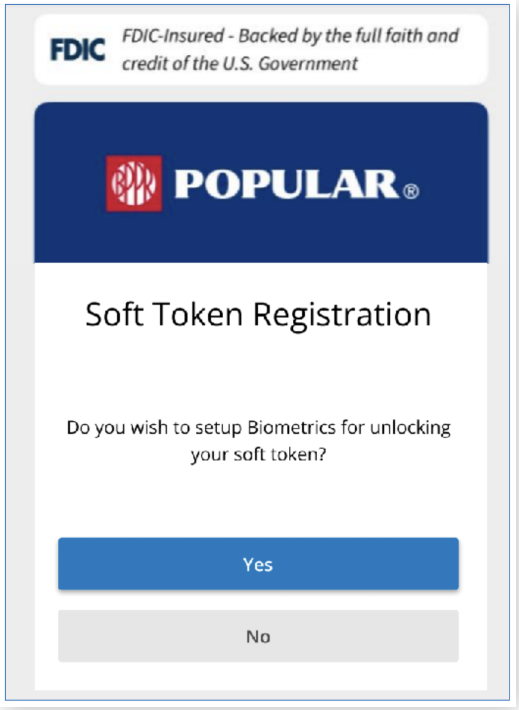


6. Press the **Scan QR Code** button in the Mobile Application to continue registration. This will enable the camera to scan the QR Code displayed on the Desktop.

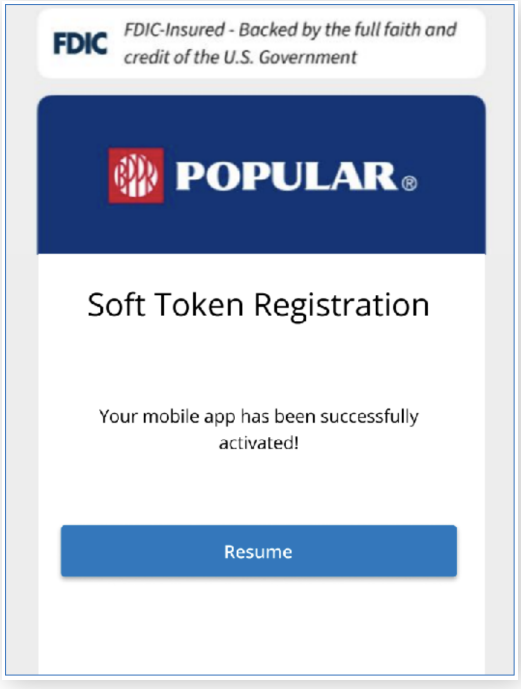
7. Once the scanning of the QR Code is successful, the platform provide a field to complete a 4-digit PIN in Mobile Application. This PIN is unique only for Soft Token Authentication.



8. Once the PIN is entered and registered successfully, the platform will require you to use the device's native biometrics such as fingerprint or facial recognition.



9. Upon confirmation, the platform will successfully register the device as a Soft Token registered device.



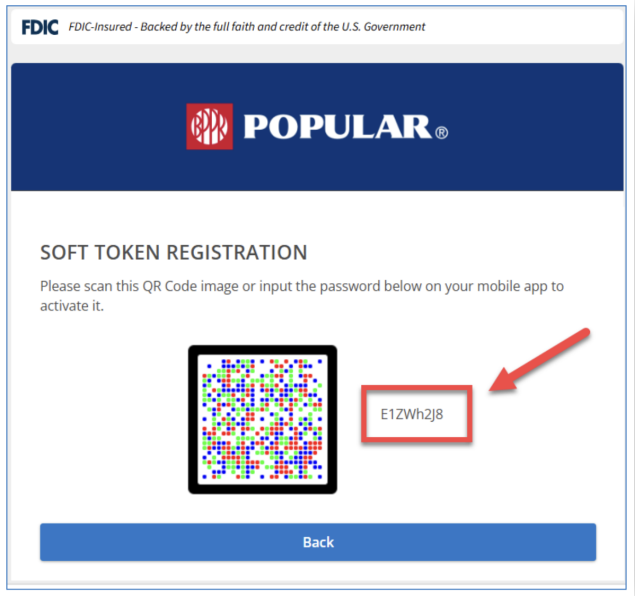
10. Upon successful registration, the platform will request to Authenticate as a first time login validation.

Soft Token Registration with Password

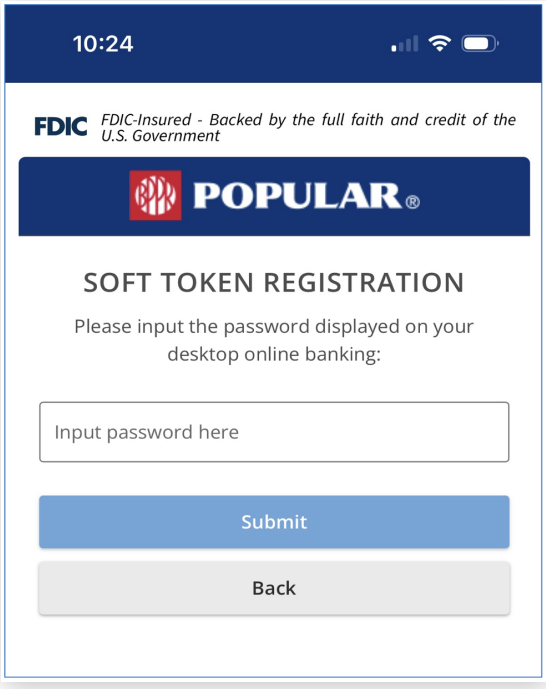
Should you encounter difficulties with the camera, the platform will allow you to register the device with a unique password.

Complete previous steps 1 to 5 from the Soft Token Registration with Biometrics.

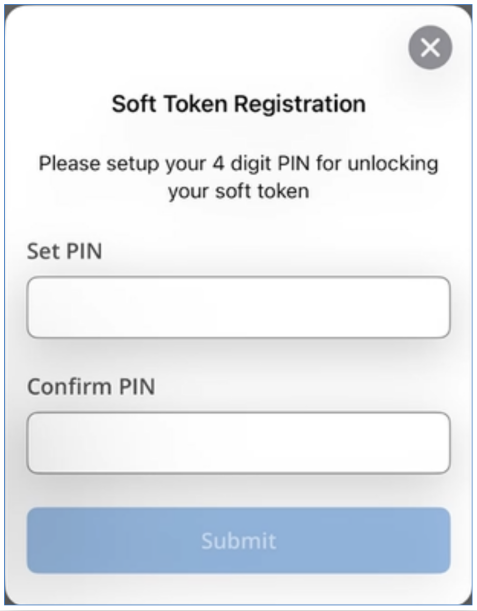
6. In Desktop, the screen displaying the QR Code will also display a password. This password is unique for the users' Soft Token registration.



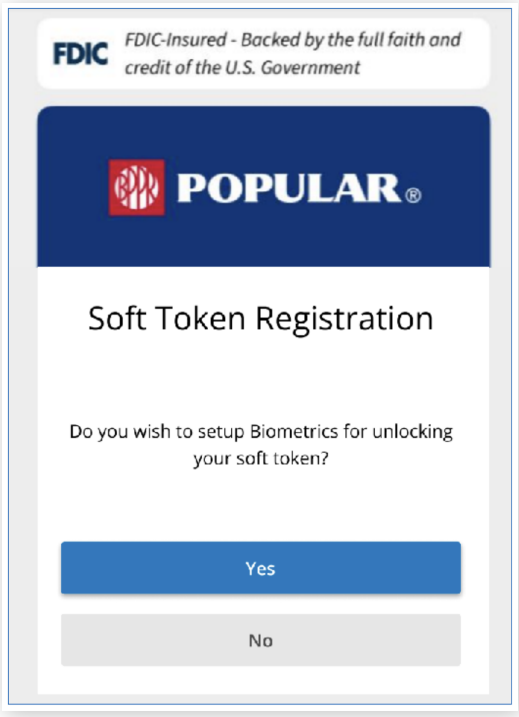
7. Press the **Type password** button in the Mobile App to continue registration. A screen will be displayed in the Mobile App to input the password.



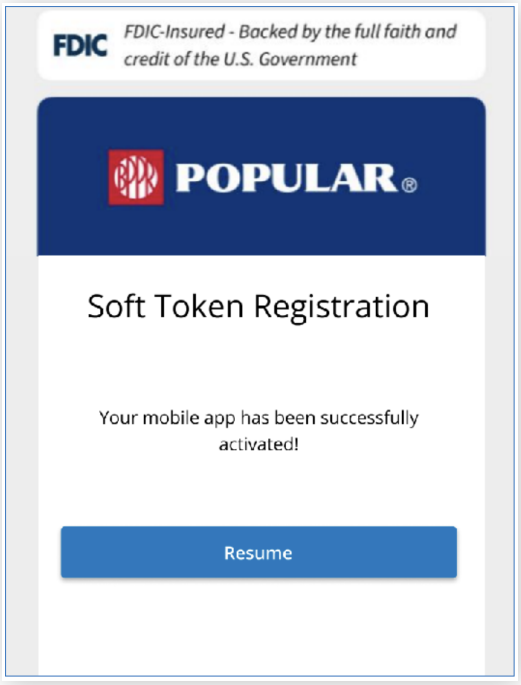
8. Once the password entered is successful, the platform will prompt you to complete a 4-digit PIN in Mobile Application. This PIN is unique only for Soft Token Authentication.



9. Once the PIN is entered and registered successfully, the platform will require you to use the device's native Biometrics.



10. Upon confirmation, the platform will successfully register the device as a Soft Token registered device.

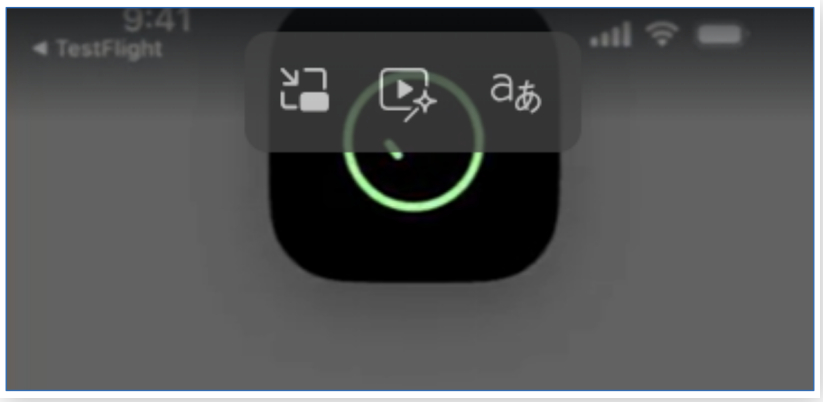


11. Upon successful registration, platform will request to Authenticate as a first-time login validation.

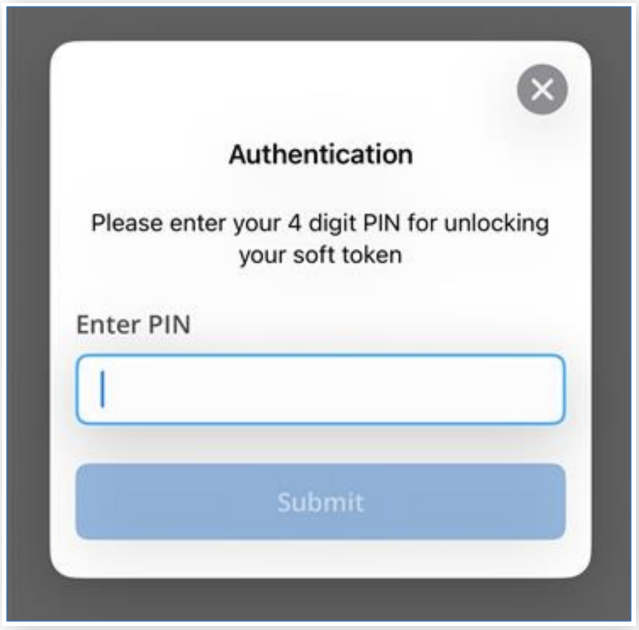
Mobile Application Authentication

Authenticate with biometrics or PIN to access the Mobile App.

1. Once logged into the mobile app, it will ask for authentication. It will automatically scan Biometrics, if you have enabled the functionality.



2. If you have not configured the device for Biometrics, the Mobile App will prompt you to enter the PIN.

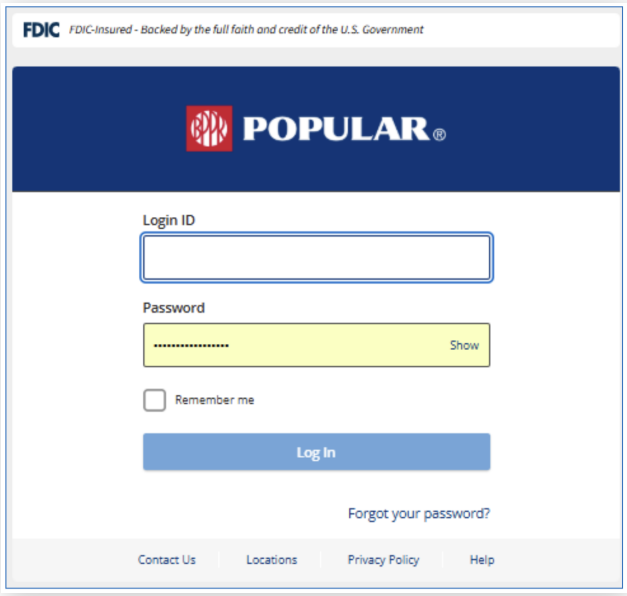


3. Once the information is registered successfully, the system will authenticate and allow you to continue to Popular Business Access.

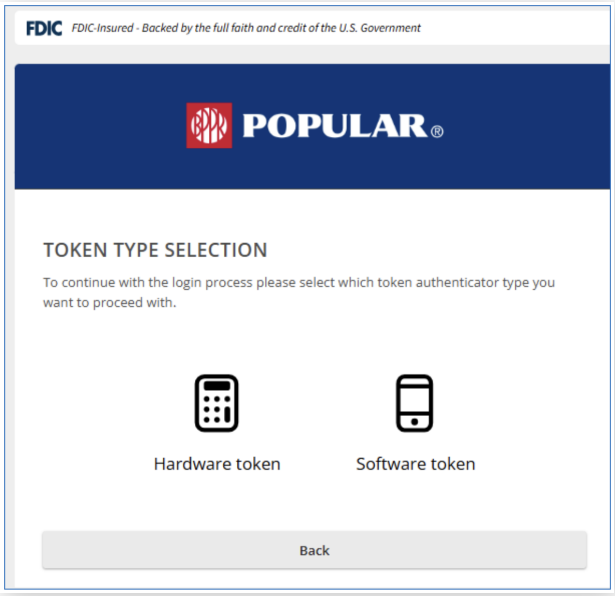
Desktop Application Authentication

Sign in and approve authentication requests using the Soft Token Mobile App.

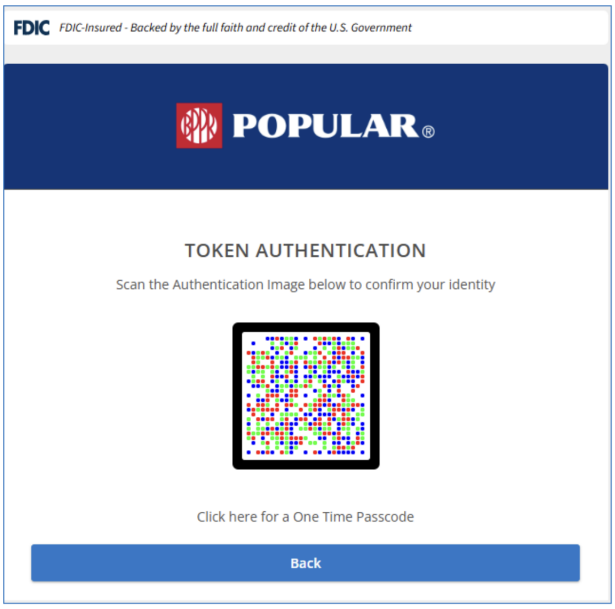
1. Enter the credentials into Desktop.



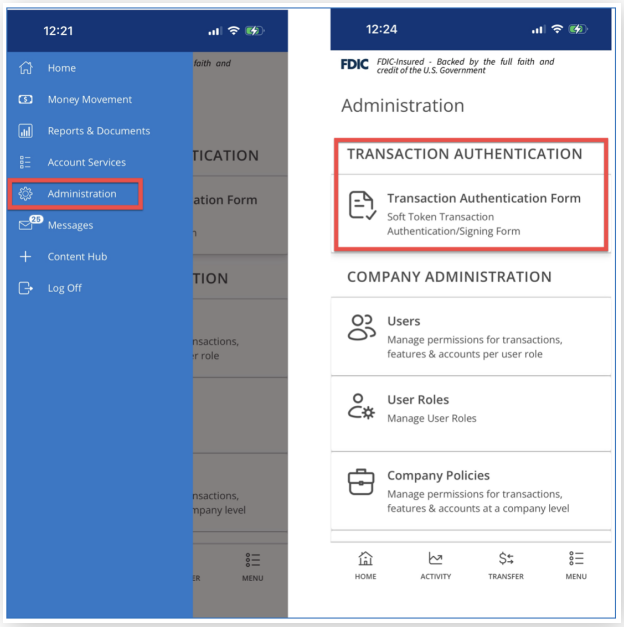
2. If you have a Hard Token and Soft Token, the platform will ask you to select which option to proceed with.



3. With Soft Token, the platform will present the QR Code to scan.

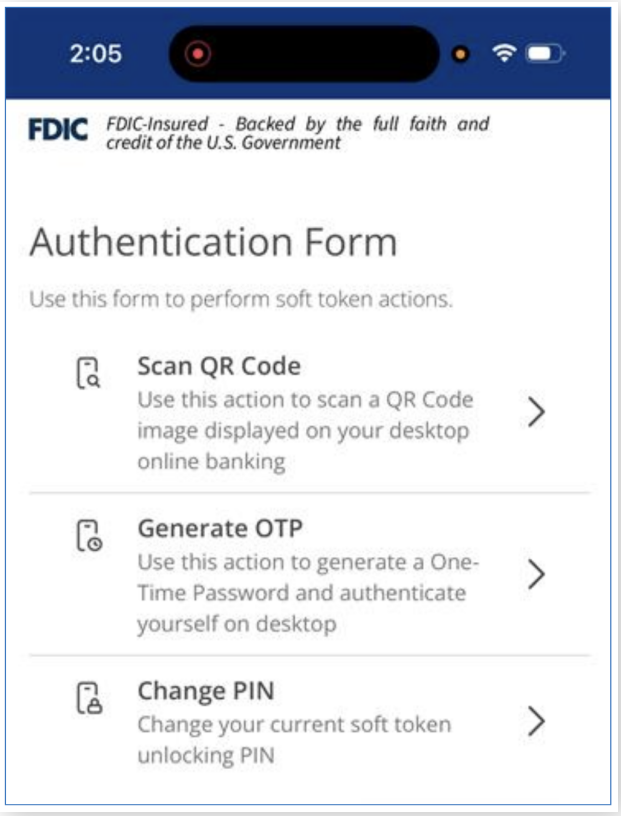


4. In the Mobile App, navigate to the **Menu** and upon selecting the **Administration** menu option, on top of the screen you will see the **Transaction Authentication** section.



5. Select the **Transaction Authentication Form**.

6. The **Transaction Authentication** will provide you with three options:
   - Scan QR Code.
   - Generate OTP.
   - Change PIN.



7. Select **Scan QR Code** and the Mobile App will automatically enable the camera to scan the QR Code and, once successful, it will then request you to add Biometrics or PIN for Authentication.

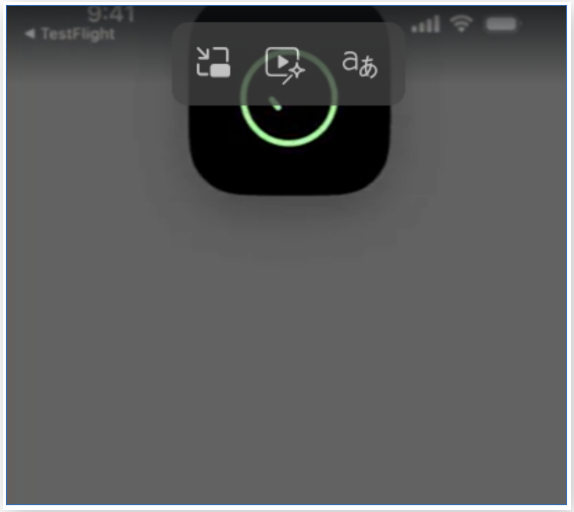
8. Upon successful Authentication, you can navigate Popular Business Access.

Transaction Authentication

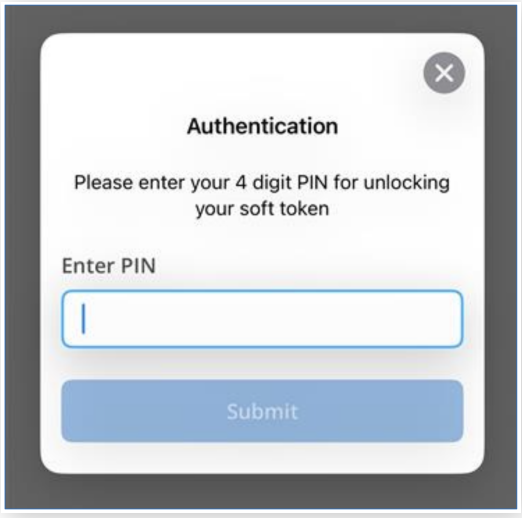
Approve transactions securely using the Soft Token.

Transaction Authentication in Mobile

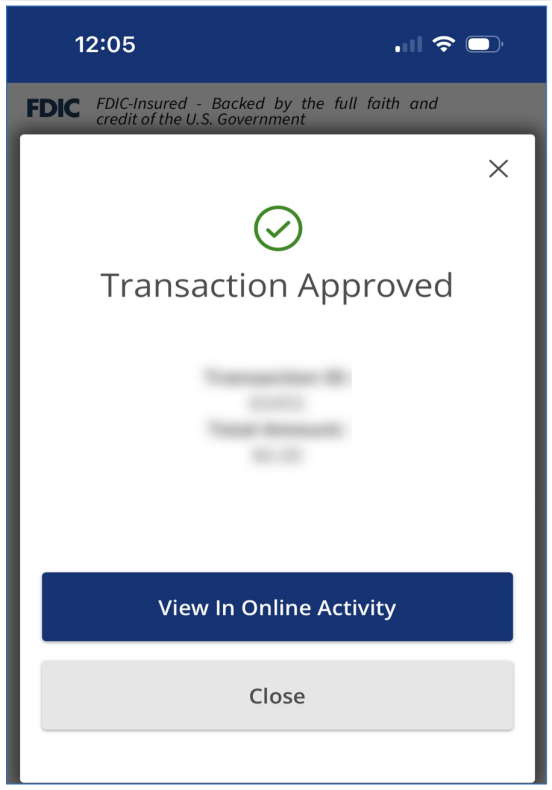
1. Once completed and ready to submit transaction, Mobile App will prompt to scan Biometrics for transaction authentication.



2. If you have not configured the device for Biometrics, the Mobile App will prompt you to enter the configured PIN.



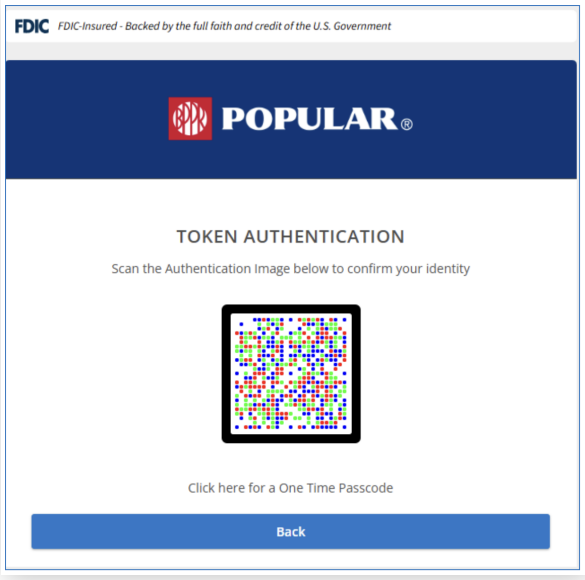
3. Once successful, the transaction is authenticated and approved.



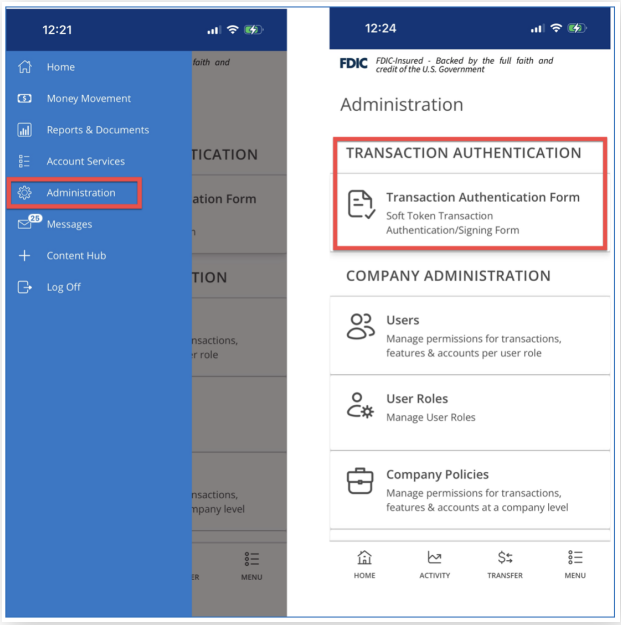
Transaction Authentication in Desktop

1. You will need to log into the Mobile App to perform the transaction authentication in Desktop.

2. In Desktop, once completed the transaction, a pop-up screen will present the QR Code to scan when submitting the transaction in the Desktop version.

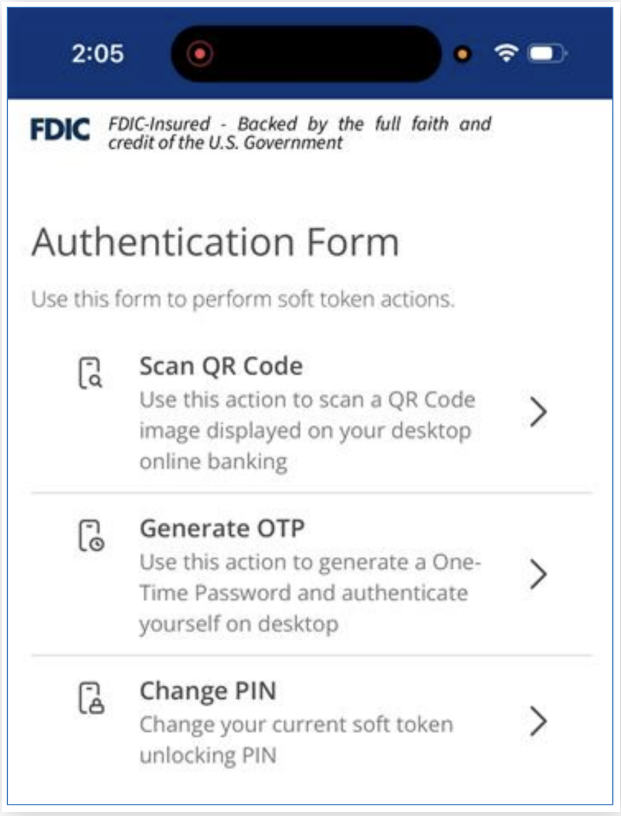


3. In the Mobile App, navigate to the **Menu** and select the **Administration** menu option, on top of the screen you will see the **Transaction Authentication** section.

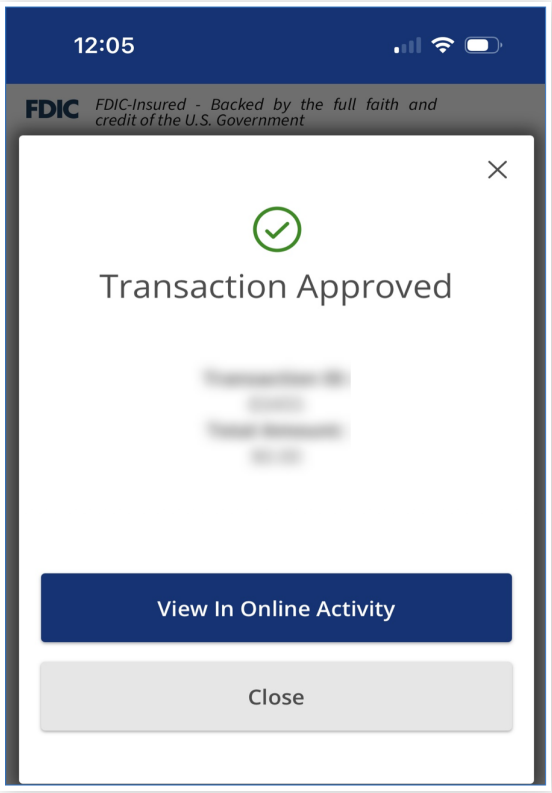


4. Select the **Transaction Authentication Form**.

5. The **Transaction Authentication** Form will provide you with three options:
   - Scan QR Code.
   - Generate OTP.
   - Change PIN.



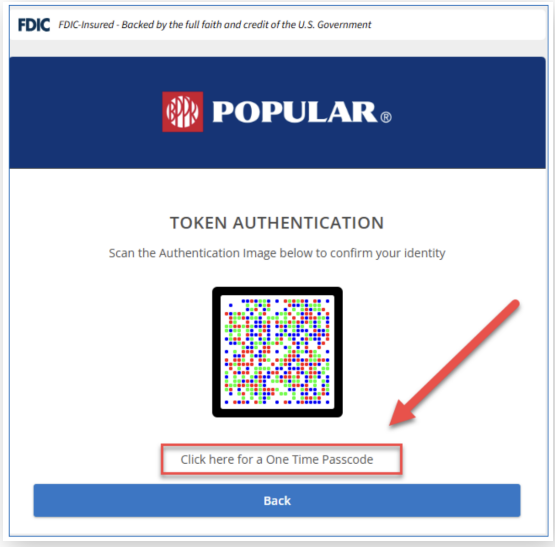
6. Select **Scan QR Code** and the Mobile App will automatically enable the camera to scan the QR Code and, once successful, it will then request you for the Biometrics or PIN for authentication. After the authentication, the transaction will be authorized and completed.



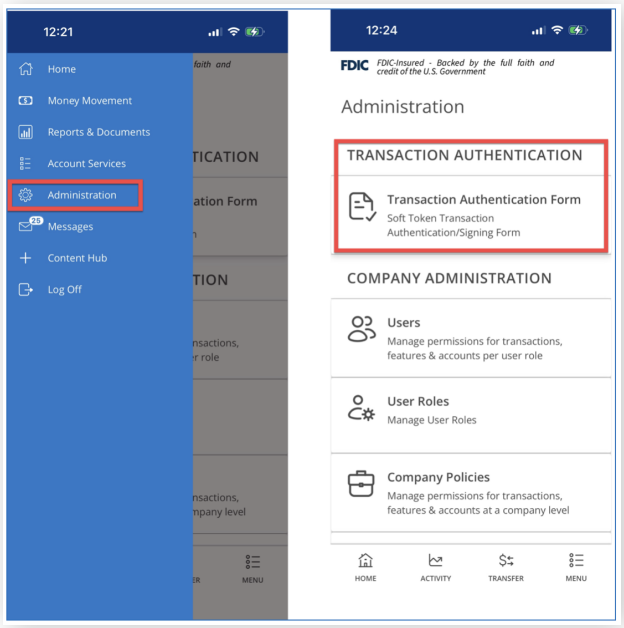
Transaction Authentication in Desktop using OTP

If you are confronting difficulties with the camera on their devices, you can enable the One-Time Password.

1. In the Desktop version, when authenticating a transaction or authorizing a functionality, the Token Authentication screen will display a link Click here for a One-Time Password.

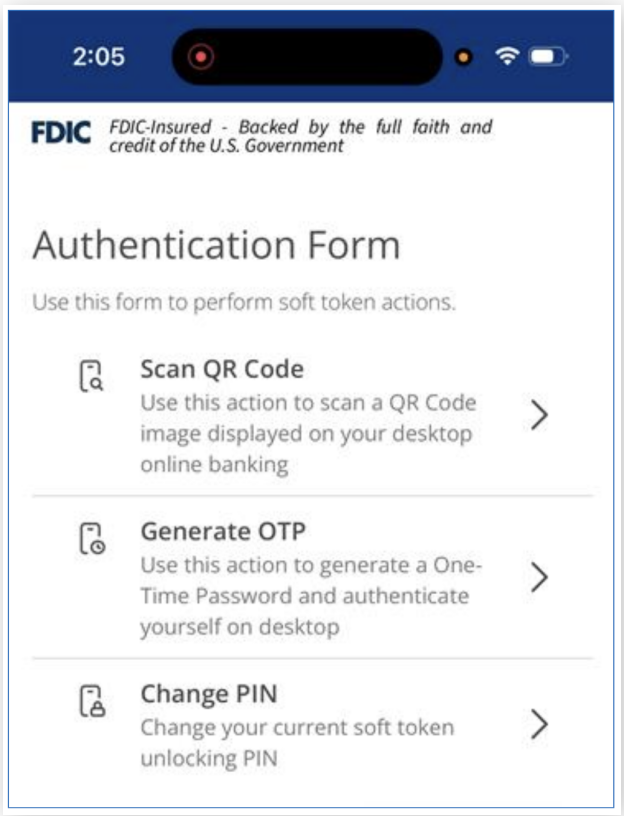


2. In the Mobile App, navigate to the **Menu** and select the **Administration** menu option, on top of the screen you will see the **Transaction Authentication** section.

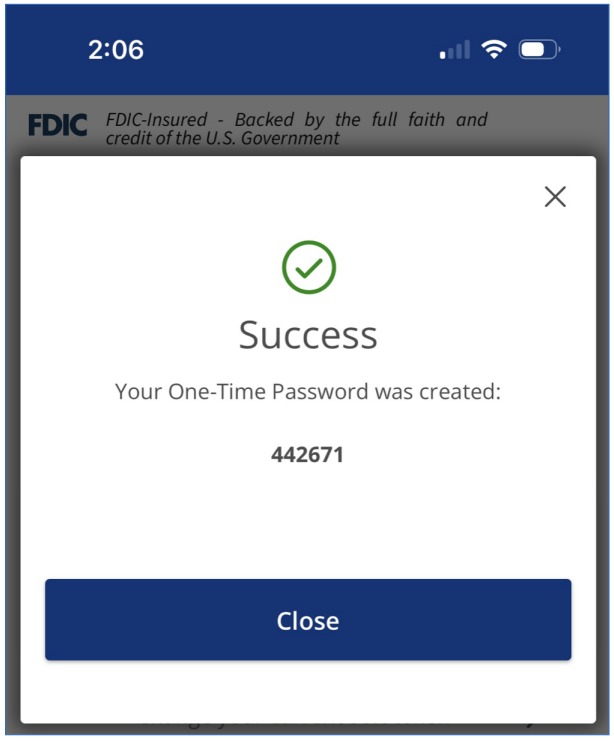


3. Select the **Transaction Authentication Form**.

4. The **Transaction Authentication** Form will provide you with three options:
   - Scan QR Code.
   - Generate OTP.
   - Change PIN.



5. Select **Generate OTP** and the Mobile App will automatically request the Biometrics or PIN for authentication.
6. Upon successful authentication, the Mobile App will successfully display the OTP code.



POPULAR®

Frequently Asked Questions

Refer to common questions regarding activation, PIN resets, new devices, and lost devices.

Can I register more than device?
Yes, you may register up to 3 devices in total per user registered for Soft Token. You may make the request to the CSR. The Admin User may be able to also perform this request.

What if my device gets reset or if I delete the Mobile Application?
You may request to register the device again. Ensure that you have not reached the 3 Device Limit. If the Limit is reached, a previous registered device must be removed prior to proceeding.

May I use a Hard Token and a Soft Token at the same time?
You may have a Soft Token and Hard Token registered. However, the system will only allow the user to use one authentications mechanism at a time.

If I remove the Hard Token will I lose the Soft Token as well?
No. The Soft Token and Hard Token are separate items assigned to a user.

Is there a limit of Soft Tokens I can use?
While you can have multiple users with Soft Tokens, each user is assigned only one license that may be used with up to 3 Devices.

What if I bought a new device and needed to remove an old one?
You can manage the devices registered as Soft Tokens. In this section you may remove previous devices that you will not use.

POPULAR®

Troubleshooting

Resolve common issues such as QR scanning failures, invalid activation codes, or connectivity problems.

- If there is an issue registering a device, the platform will allow you to continue from the previous point that was saved. If necessary, you can request to register the same device again.
- If the authentication fails upon scanning the QR Code, you may use the OTP as an alternative.
- If the authentication fails, you may retry the authentication process.
- If you attempt to authenticate at the same time in two versions, the platform will only approve the first transaction entered and will require you to resend the authentication for the second transaction.

Security Best Practices

Protect your personal identification number (PIN), always keep your device secure, and carefully review every authentication request before approving it. Never share your credentials with others and report any suspicious or unexpected activity immediately to help safeguard your account and company information.

Support & Assistance

For additional assistance, you may contact the Commercial Support Center at **787-756-3939** or **1-855-756-3939**, available Monday through Friday, from 8:00 a.m. to 5:00 p.m.