



INFORMATION SECURITY

Profile Manager Quick Reference Guide

Published 02/06/2024

Member FDIC



Table of Contents

Overview	3
Profile Manager Log In Methods	3
First Method:	3
Second Method:	5
Third Method:	6
Welcome Message	6
Profile Manager Pages	6
Profile Info	7
Security	9
Okta Verify Enrollment	11
Google Authenticator Enrollment	13
Text Message Authentication (SMS) Enrollment	15
Voice Call Authentication Enrollment	17
Additional Information for Remove and Reset Options:	19
Single Sign-On	21

Overview

The Profile Manager application is a self-service application where customers can update the following information:

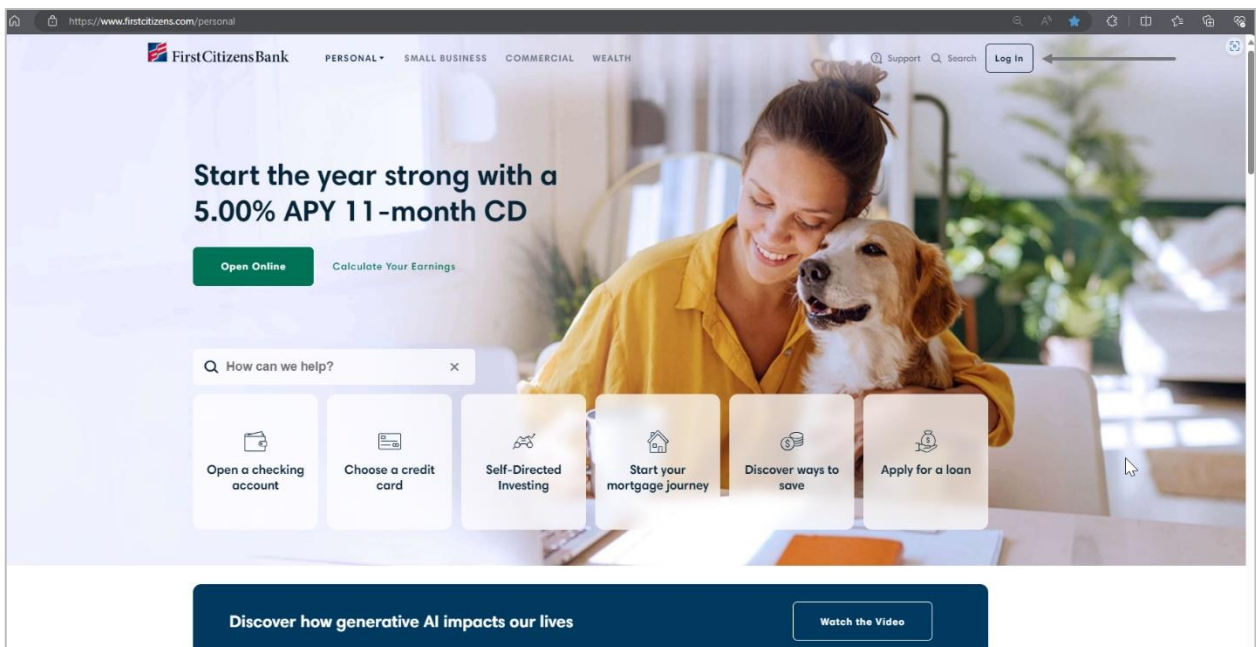
- First Name
- Last Name
- Email
- Mobile Number
- Multi-Factor Authentication Factor
- Activate Single Sign On (SSO) to log into one or more applications with the same credentials

Profile Manager Log In Methods

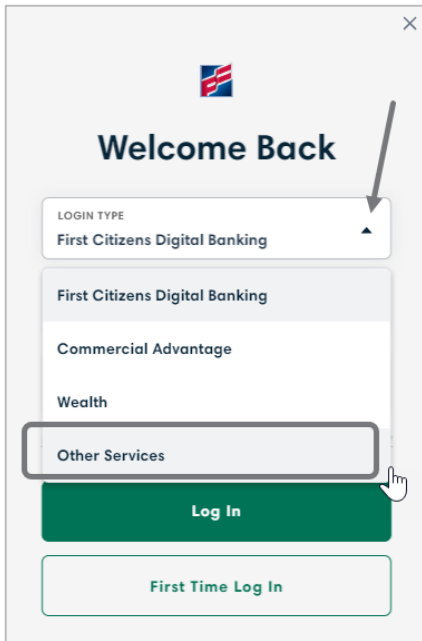
There are several methods to log into Profile Manager:

First Method:

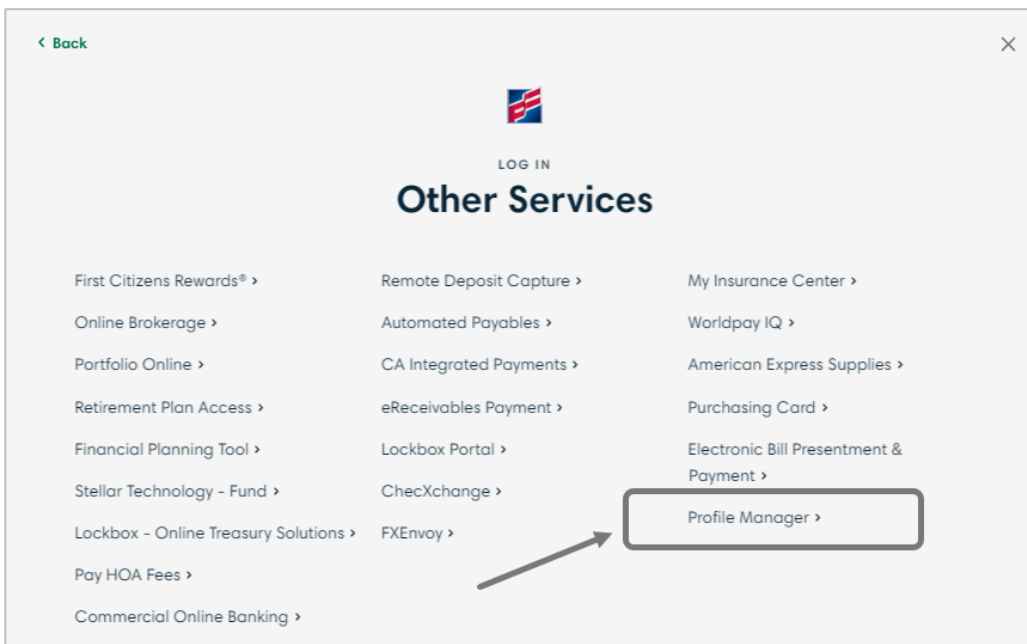
1. Navigate to www.firstcitizens.com home page, click on the **Log In** button at the top right-hand corner.



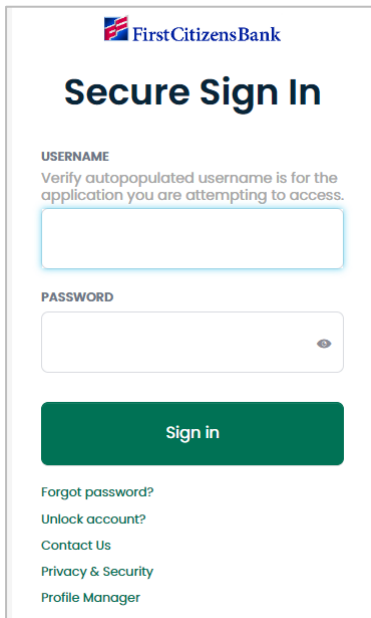
- You will be directed to the **Welcome Back** page. Select the drop-down caret, then select **Other Services** from the list of options.



- Click on the **Profile Manager** link.



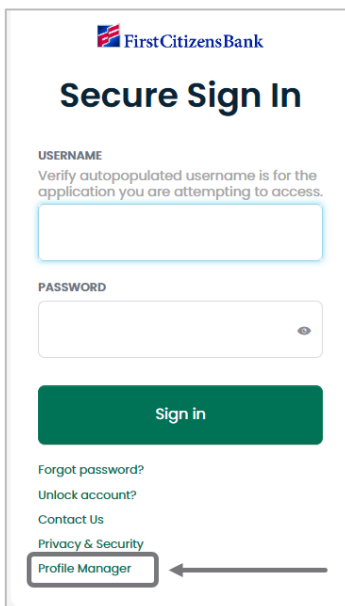
4. Log in using your credentials.



The image shows a screenshot of the First Citizens Bank 'Secure Sign In' page. At the top is the First Citizens Bank logo. Below it is the title 'Secure Sign In'. Underneath is the 'USERNAME' section with a prompt to verify the autopopulated username. There is a text input field for the username. Below that is the 'PASSWORD' section with a text input field and an eye icon for toggling visibility. A green 'Sign in' button is positioned below the password field. At the bottom of the form are several links: 'Forgot password?', 'Unlock account?', 'Contact Us', 'Privacy & Security', and 'Profile Manager'.

Second Method:

1. Navigate to the application you are accessing, select the **Profile Manager** link below the **Sign in** button.



This image is identical to the one above, showing the 'Secure Sign In' form. However, in this version, the 'Profile Manager' link at the bottom is highlighted with a black rectangular box. A grey arrow points from the right side of this box towards the left, indicating the user should click on this link.

Third Method:

If the application page does not include a link to Profile Manager, please proceed to the login screen to access it.

Welcome Message

When you access Profile Manager for the first time, a window will open with a welcome message. Select the **OK** button or click on the **X** on the top-right corner to continue your session.



Profile Manager Pages

There are three tabs (or pages) in Profile Manager:



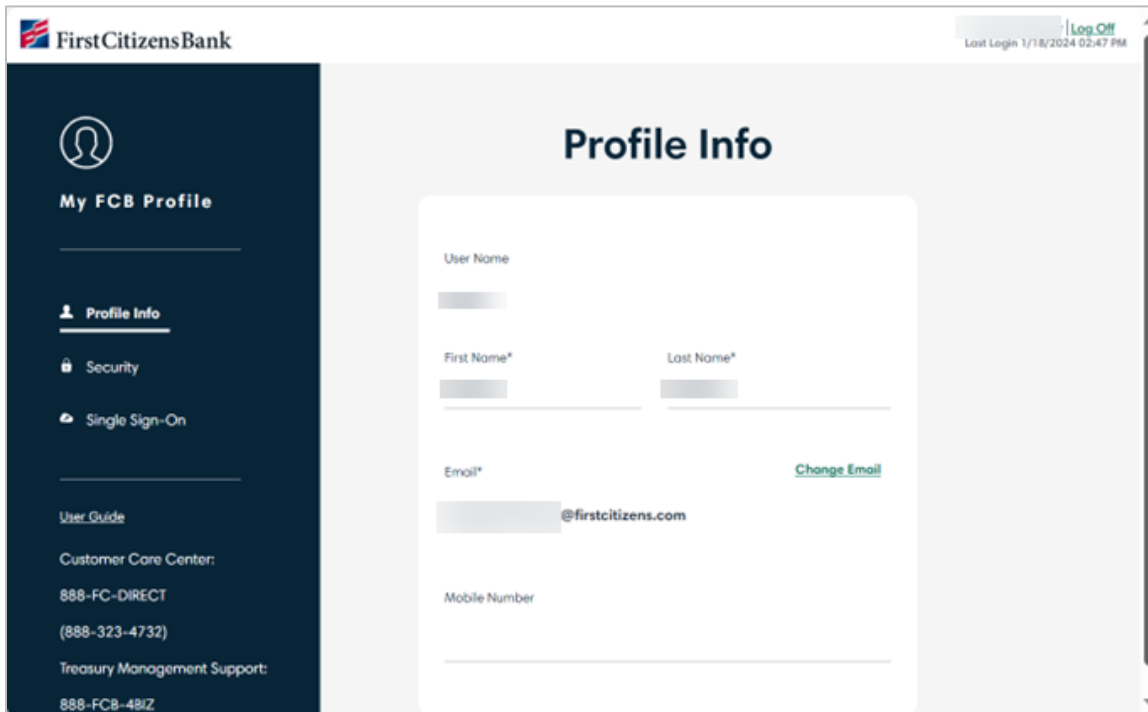
- Profile Info
- Security
- Single Sign-On

The Profile Manager user guide is now accessible once you are logged in to Profile Manager. You can also find customer service information for Customer Care Center and Treasury Management Support.

Profile Info

You can self-service **First Name**, **Last Name**, **Email** address, and **Mobile Number**.

Note: **User Name** is not an editable field.

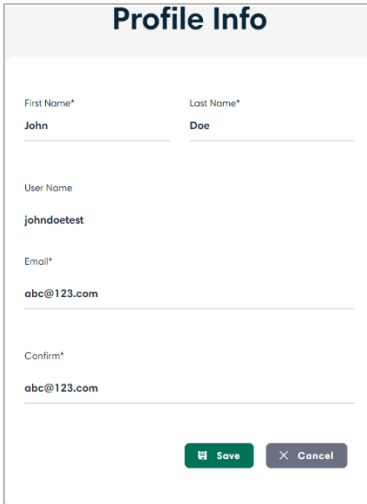


The screenshot shows the First Citizens Bank Profile Manager interface. On the left is a dark blue sidebar with the bank's logo and navigation links: 'My FCB Profile' (with a user icon), 'Profile Info' (selected), 'Security', and 'Single Sign-On'. Below these are links for 'User Guide', 'Customer Care Center: 888-FC-DIRECT (888-323-4732)', and 'Treasury Management Support: 888-FCB-48IZ'. The main content area is titled 'Profile Info' and contains a form with the following fields: 'User Name' (disabled), 'First Name*' and 'Last Name*' (both with input boxes), 'Email*' (with a 'Change Email' link) and 'Mobile Number' (with an input box). The top right of the page shows a 'Log Off' link and the text 'Last Login 1/18/2024 02:47 PM'.

- To update first name, click on the blank space under the field name and above the line, make the necessary change and tab to the next field. **First Name Successfully Updated** success message will display.
- To update last name, click on the blank space under the field name and above the line, make the necessary change and tab to the next field. **Last Name Successfully Updated** success message will display.
- To update the email address, click on **Change Email** link. Enter the new email address in the **Email*** field. Re-enter the same email address on the **Confirm*** email. Click on **Save**.

- A confirmation window will display, click **Confirm. Email Successfully Updated** success message will display.

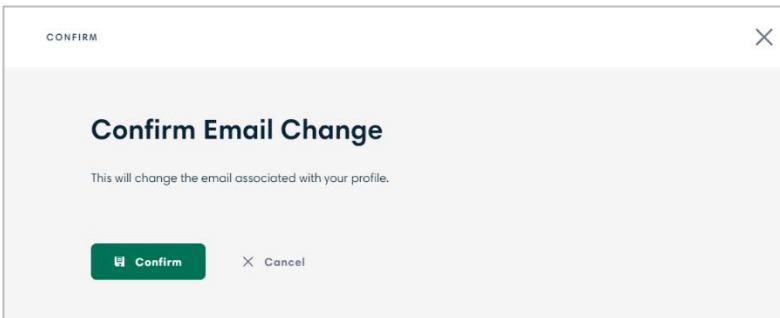
Note: The email address must be in abc@xyz.com format.



The 'Profile Info' form contains the following fields and values:

Field	Value
First Name*	John
Last Name*	Doe
User Name	johndoetest
Email*	abc@123.com
Confirm*	abc@123.com

At the bottom right, there are two buttons: a green 'Save' button and a grey 'Cancel' button.



The 'CONFIRM' dialog box has a title bar with a close button (X). The main content area displays:

Confirm Email Change

This will change the email associated with your profile.

At the bottom, there are two buttons: a green 'Confirm' button and a grey 'Cancel' button.

- To update **Mobile Number**, click on the blank space under the field name and above the line, make the necessary change and tab to the next field. **Mobile Number Successfully Updated** success message will display.

Profile Info

User Name
John

First Name*
John

Last Name*
Doe

Email Address*
abc@1234.com

Confirm*


Save
Cancel


Mobile Number

123-123-1234

Security

You can enroll in Multi Factor Authentication (MFA) method by selecting **Use This** button. You can also **Remove** or **Reset** an established method.


First Citizens Bank



My FCB Profile

Settings

Profile Info

Security

Single Sign-On

[User Guide](#)

Customer Care Center:


888-FC-DIRECT
(888-323-4732)

Treasury Management Support:

888-FCB-4BIZ
(866-322-4249)

Security


These are the methods you can use to verify your identity whenever you try to log in. You always need at least one. The **Okta Verify App** is the easiest and most secure.



Best
Okta Verify


→

✓ Use This




Best
Google Authenticator

✓ Use This



Best
SMS & Text

✕ Remove
↺ Reset





Best
Voice Call

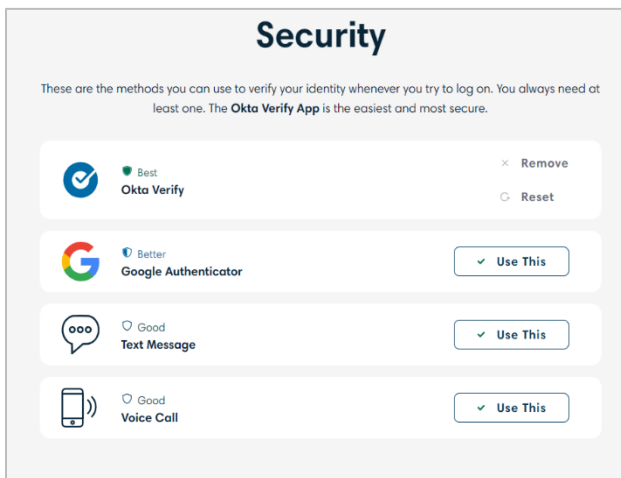
✓ Use This

Disclosures ▼

The Multi-Factor Authentication (MFA) options rating of Best, Better and Good are based on Industry Standards and are only recommendations of The Bank. The Bank is not responsible for any adverse effects the MFA option may incur if these factors are compromised.

NEW MFA users will have four options available; we recommend registering for more than one MFA. Please refer to the chart below in determining the best fit based on your company policies.

	Voice Call Authentication	Text Message Authentication	Google Authenticator	Okta Verify
Enhanced security	Good	Good	Better	Best
Mobile device required		✓	✓	✓
Landline compatible	✓			
App download			 App Store (iPhone) / Google Play Store (Android)	 App Store (iPhone) / Google Play Store (Android)
Access to camera (recommended)			✓	✓
Push notification enabled				✓



Okta Verify

- Uses a push notification sent to the mobile app (requires download).

Google Authenticator

- Enter a single-use code from the mobile app (requires download).

Text Message Authentication

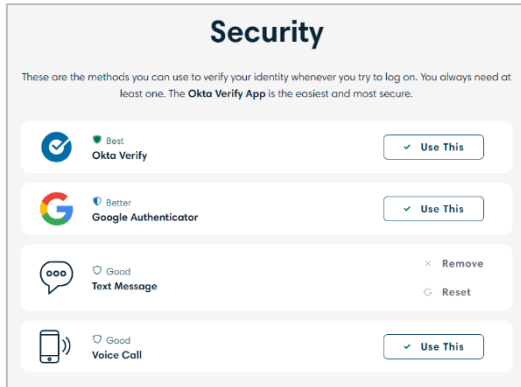
- Enter a single-use code sent to your mobile phone.

Voice Call Authentication

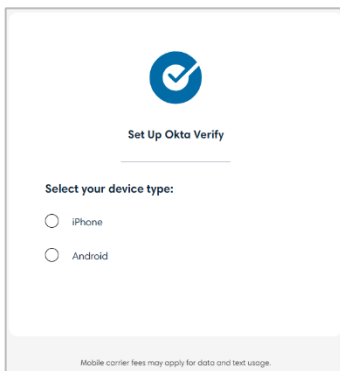
- Use a phone to authenticate by following voice instructions.

Okta Verify Enrollment

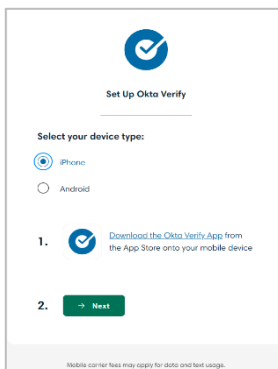
1. Click **Use This** next to Okta Verify.



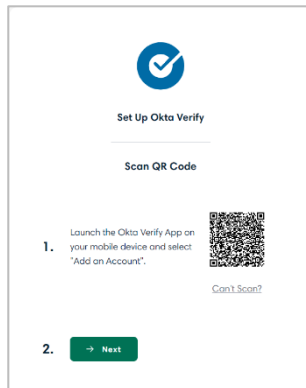
2. Select your device type.



3. Download **Okta Verify** app from Apple App Store (iPhone) or Google Play (Android) first, then click **Next**.



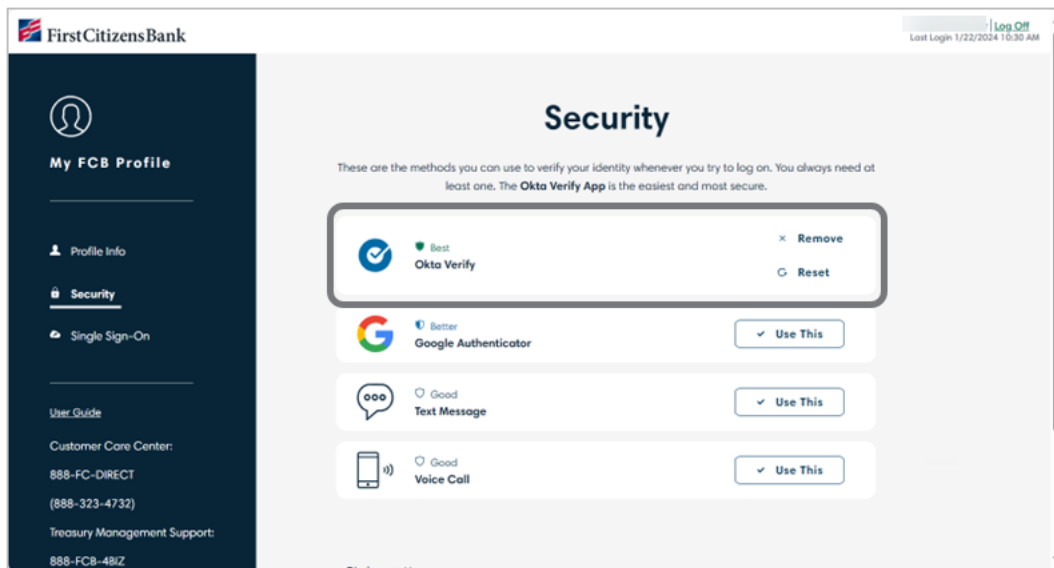
- Launch **Okta Verify** app on your mobile device and select **Add An Account**.



- Scan the QR code using your mobile device.

Note: If you do not wish to allow access to your mobile device camera, click the **Can't scan?** link and follow the instructions provided in the FAQ.

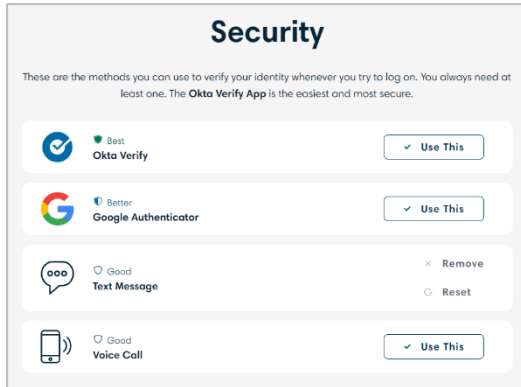
- Success 2 step verification complete** success message will display.
- The **Use This** button will be replaced with a **Remove** and a **Reset** button.



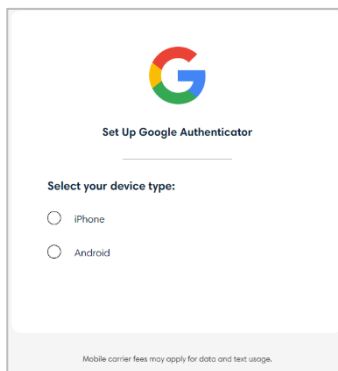
- The client will receive an email confirming that a multifactor authenticator has been set up.

Google Authenticator Enrollment

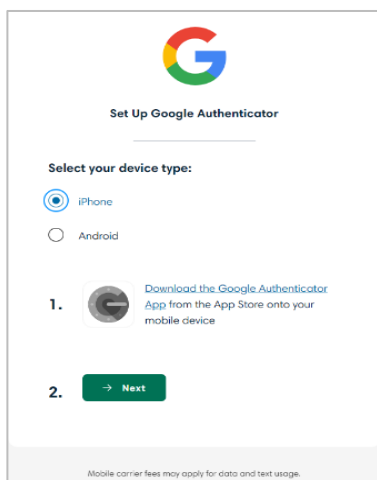
1. Click **Use This** next to Google Authenticator.



2. Select your mobile device.

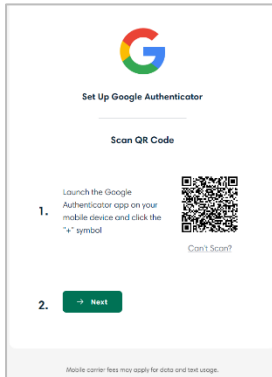


3. Download Google Authenticator from the App Store (iPhone) or Google Play (Android) first, then click **Next**.

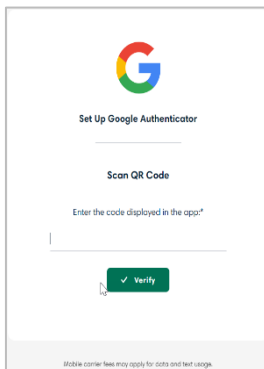


4. Launch Google Authenticator app on your mobile device and tap the **+** icon.
5. Scan the QR code using your mobile device.

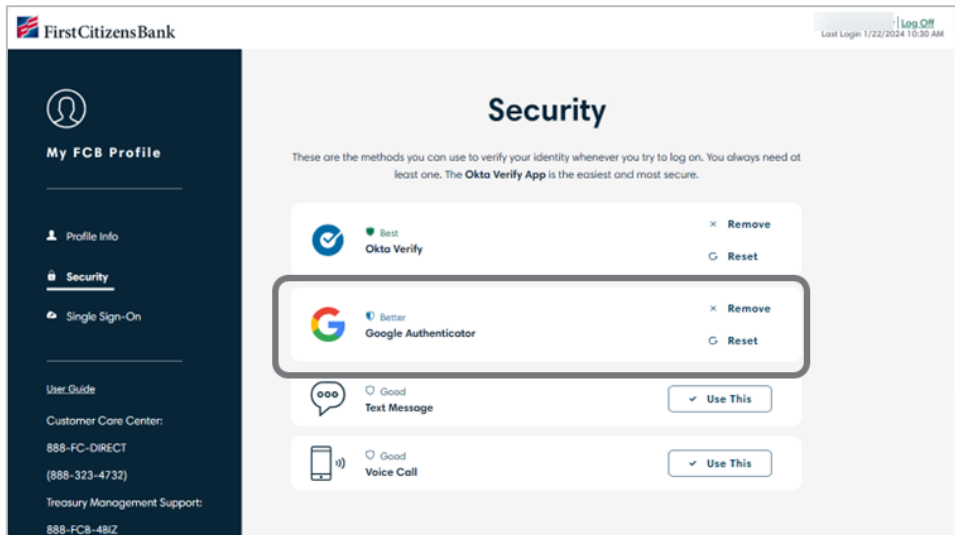
Note: If you do not wish to allow access to your mobile device camera, click the Can't scan? link and follow the instructions provided in the FAQ.



6. Enter code sent to Google Authenticator app in the **Enter code** field and click **Verify**.



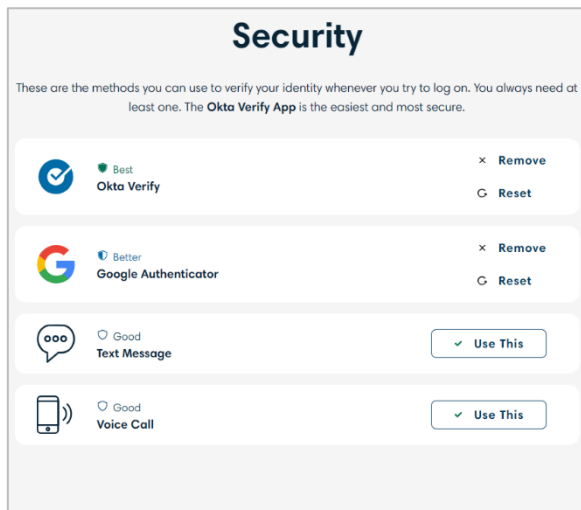
7. **Success 2 step verification complete** success message will display.
8. The **Use This** button will be replaced with a **Remove** and a **Reset** button.



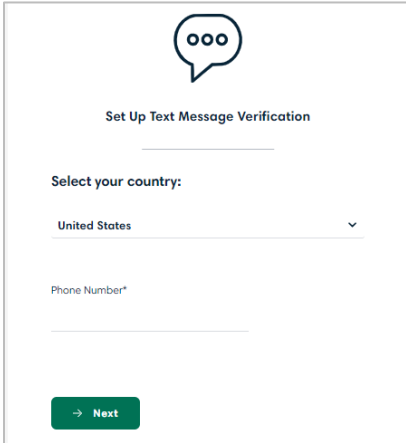
9. The client will receive an email confirming that a multifactor authenticator has been set up.

Text Message Authentication (SMS) Enrollment

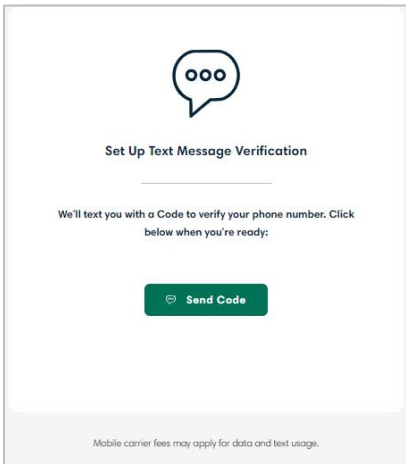
1. Click **Use This** next to Text Message Authentication.



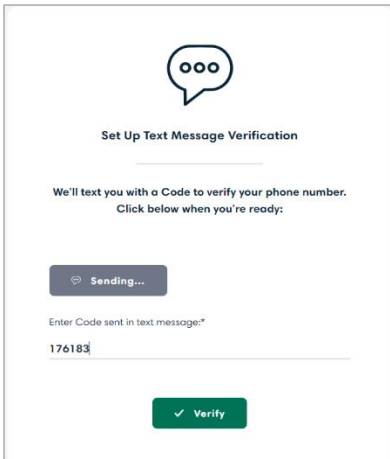
2. Enter the phone number for your mobile device and click **Next**.



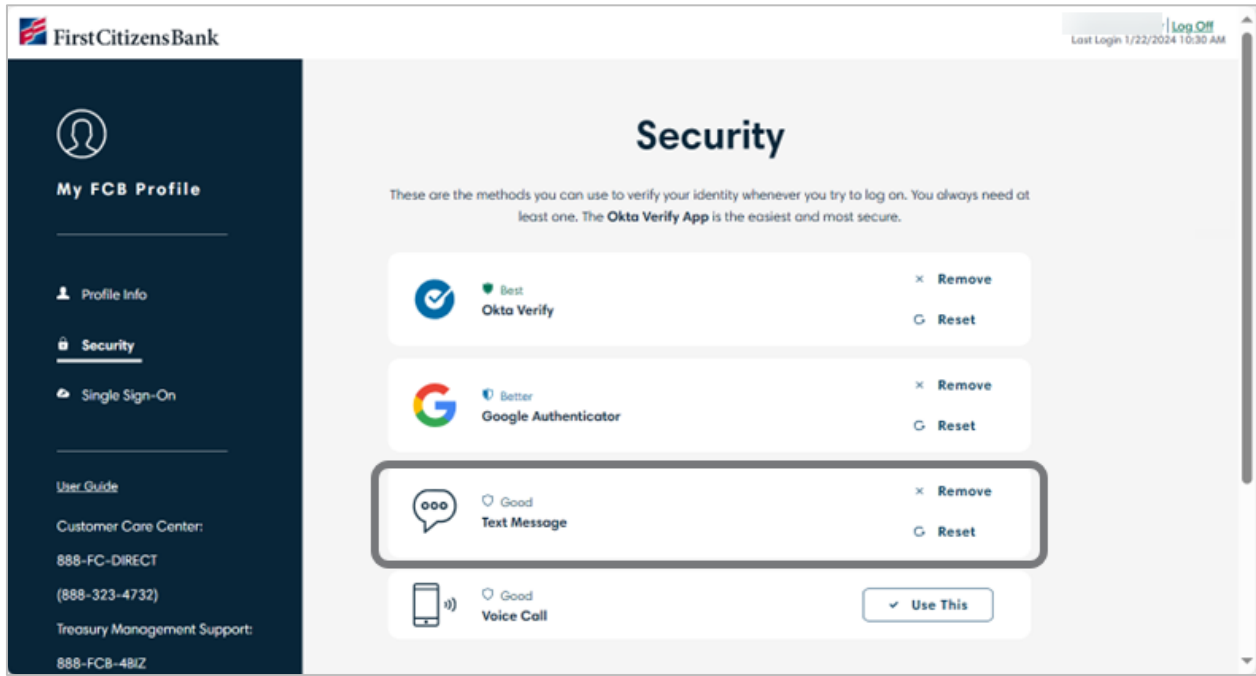
3. Click **Send Code**.



4. Enter code sent to mobile device in **Enter code** field and click on **Verify**.



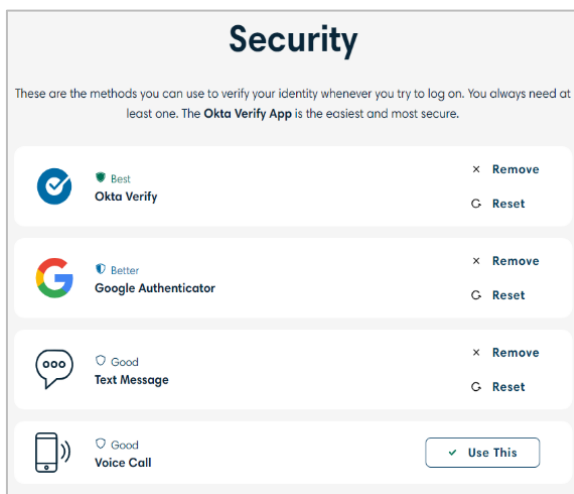
5. **Success 2 step verification complete** success message will display.
6. The **Use This** button will be replaced with a **Remove** and a **Reset** button.



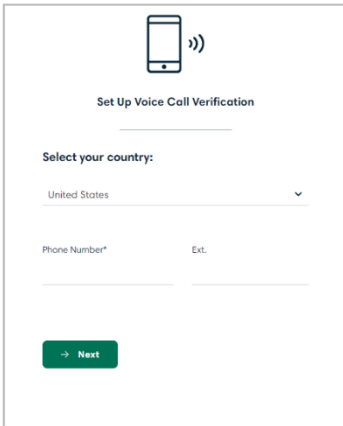
7. The client will receive an email confirming that a multifactor authenticator has been set up.

Voice Call Authentication Enrollment

1. Click **Use This** next to Voice Call Authentication.

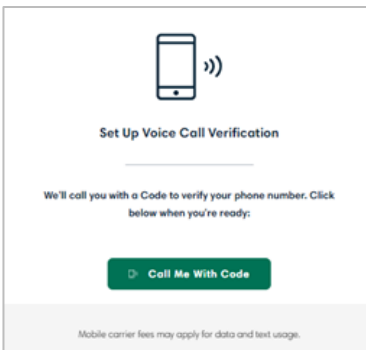


2. Enter the phone number you wish to receive a call on (can be a landline or a mobile device) and click **Next**.



The screen displays a mobile phone icon with signal waves. Below it, the title "Set Up Voice Call Verification" is centered. A horizontal line separates the title from the "Select your country:" label. A dropdown menu shows "United States" with a downward arrow. Below this are two input fields: "Phone Number*" and "Ext.". At the bottom is a green button with a right arrow and the text "Next".

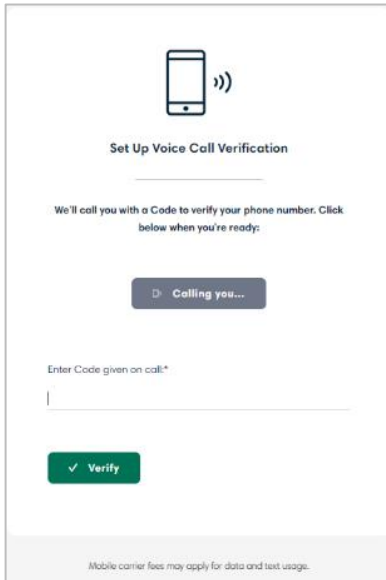
3. Click **Call Me With Code**. Answer the phone call and listen for the code.



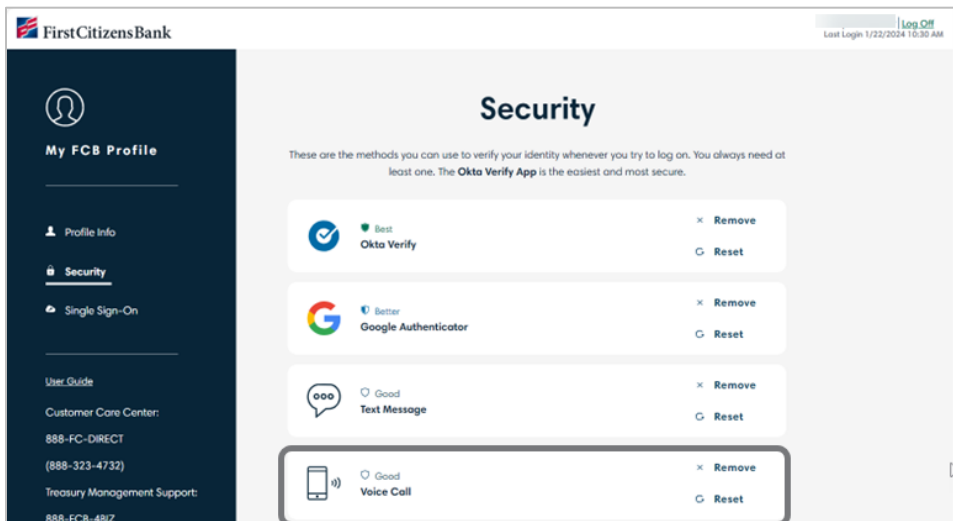
This screen is identical to the previous one but includes an additional line of text: "We'll call you with a Code to verify your phone number. Click below when you're ready:". Below this text is a green button with a phone icon and the text "Call Me With Code". At the very bottom, in small text, it says "Mobile carrier fees may apply for data and text usage."

"Hello, thank you for using
our phone verification
system. Your code is..."

4. Enter code in the **Enter code** field and click **Verify**. **Success 2 step verification complete** success message will display.



5. The **Use This** button will be replaced with a **Remove** and a **Reset** button.



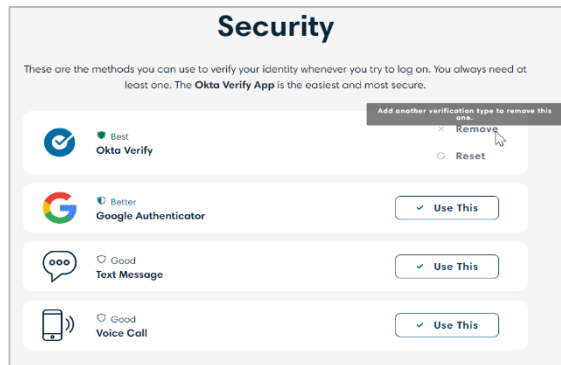
6. The client will receive an email confirming that a multifactor authenticator has been set up.

Additional Information for Remove and Reset Options:

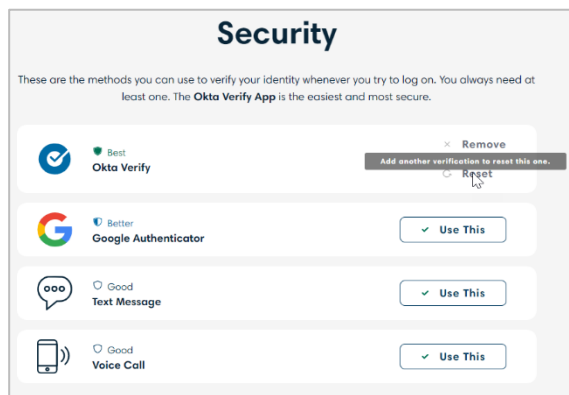
1. If you choose to remove a factor, then you will receive an email to confirm that one or more multifactor authenticators have been removed from your First Citizens account.

2. You must have at least 2 MFA factors before removing or resetting one of the factors. If you only have one factor enrolled, then you will get the following messages:

- Remove: **Add another verification type to remove this one.**



- Reset: **Add another verification type to reset this one.**



When to use reset and why:

1. For Reset, the process is the same as a new enrollment (refer to the new enrollment section of this guide).
2. For Okta Verify and Google Authenticator, the Reset button is used if you have a new mobile device. The account on Okta Verify or Google Authenticator on the old mobile device will not transfer to the new mobile device. You will need to re-enroll so that a new account can be added to log in using that factor on the new mobile device.
3. For SMS and Voice, the Reset button is used if you have a new phone number that needs to be updated.
4. If you choose to Reset a factor, then you will receive two emails:
 - The first email will confirm removal of one or more multifactor authenticators for your First Citizens Bank Account.

- The second email will confirm that a multifactor authenticator has been set up for your First Citizens Account.

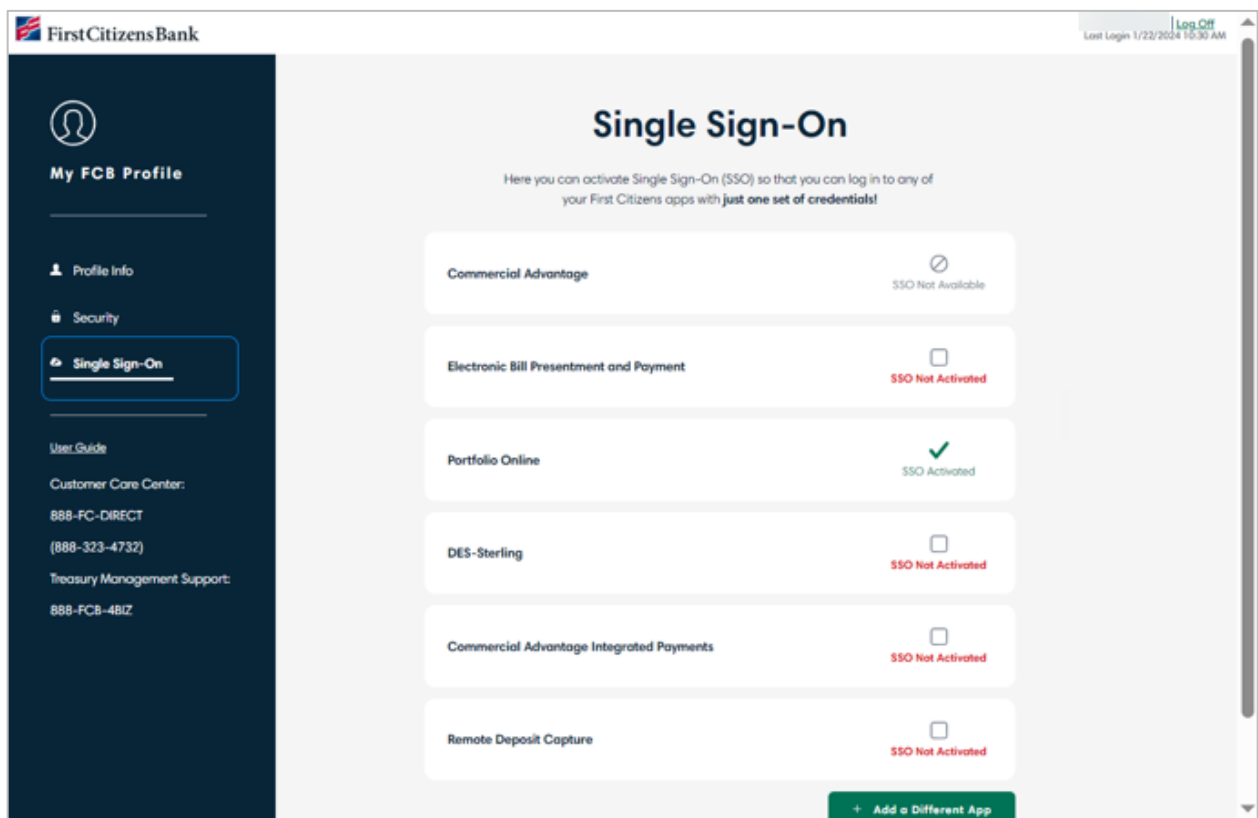
Single Sign-On

You can merge your existing First Citizens Bank applications, so that you only have one digital identity (Username & Password) to use as a Single Sign-On (SSO) for all your First Citizens Bank applications.

Note: You must be provisioned to more than one First Citizens Bank application to be eligible for SSO.

1. Choose the application you wish to merge with by clicking the **+Add a Different App**.

Note: The application that displays as SSO Activated is the application you logged in with to access Profile Manager. This will become the digital identity that you use to log in to your merged accounts (SSO Not Activated).



2. Choose the application you want to merge from the Single Sign-On Setup.

SINGLE SIGN-ON SETUP

×

Set up an App for SSO

We'll permanently merge your old profile into this profile so that you can log in with just one set of credentials! Just select which app you'd like to setup to get started:

[Electronic Bill Presentment and Payment >](#)[DES-Sterling >](#)[Commercial Advantage Integrated Payments >](#)[Remote Deposit Capture >](#)

3. Enter your existing login credentials for the application that was chosen and click **Next**.

SINGLE SIGN-ON SETUP

×

Remote Deposit Capture

Enter your login info for this app below:

Username*

Janedoetest

Password*

.....

[Forgot Password](#)[Unlock Account](#)[Trouble Logging In?](#)

→ Next

- If you are not required to enroll in MFA for this application, then click **Confirm Single Sign-On Setup**.

SINGLE SIGN-ON SETUP

Confirm


We'll permanently merge this app's profile into your FCB profile so that you can log in with just one set of credentials!

After this process is completed, use as your Username to log in to **Remote Deposit Capture**

Note: If you have multiple FCB profiles, make sure you are logged in to the correct profile that you want to merge with this app's profile.


✓ Confirm Single Sign-On Setup

- Both applications have been SSO Activated, which means you will now be able to log into both applications using the same Username and Password. If you are required to choose an MFA factor, then all the factors that you are enrolled in for that application will display.


First Citizens Bank

[Log Off](#)

Last Login 1/22/2024 10:30 AM



My FCB Profile

Profile Info

Security

Single Sign-On

User Guide

Customer Care Center:

888-FC-DIRECT

(888-323-4732)

Treasury Management Support:

888-FCB-4BIZ

Single Sign-On


Here you can activate Single Sign-On (SSO) so that you can log in to any of your First Citizens apps with **just one set of credentials!**

Commercial Advantage	SSO Not Available
Electronic Bill Presentment and Payment	SSO Not Activated
Portfolio Online	SSO Activated
DES-Sterling	SSO Not Activated
Commercial Advantage Integrated Payments	SSO Not Activated
Remote Deposit Capture	SSO Activated

➕ Add a Different App

SINGLE SIGN-ON SETUP

Verify

 Okta Verify App

Click below to verify with the Okta App on your phone:

Send Push

[Or enter code](#)

6. Once you have gone through all the necessary MFA factor verification steps then click **Confirm Single Sign-On Setup**.

SINGLE SIGN-ON SETUP

Confirm

We'll permanently merge this app's profile into your FCB profile so that you can log in with just one set of credentials!

After this process is completed, use as your Username to log in to **Remote Deposit Capture**

Note: If you have multiple FCB profiles, make sure you are logged in to the correct profile that you want to merge with this app's profile.

Confirm Single Sign-On Setup

7. The applications that were chosen for the merge have been SSO Activated, which means you will now be able to log into these applications using the same Username and Password. If you have merged all available applications, then you will receive this message when you click on the **+ Add a Different App** button.

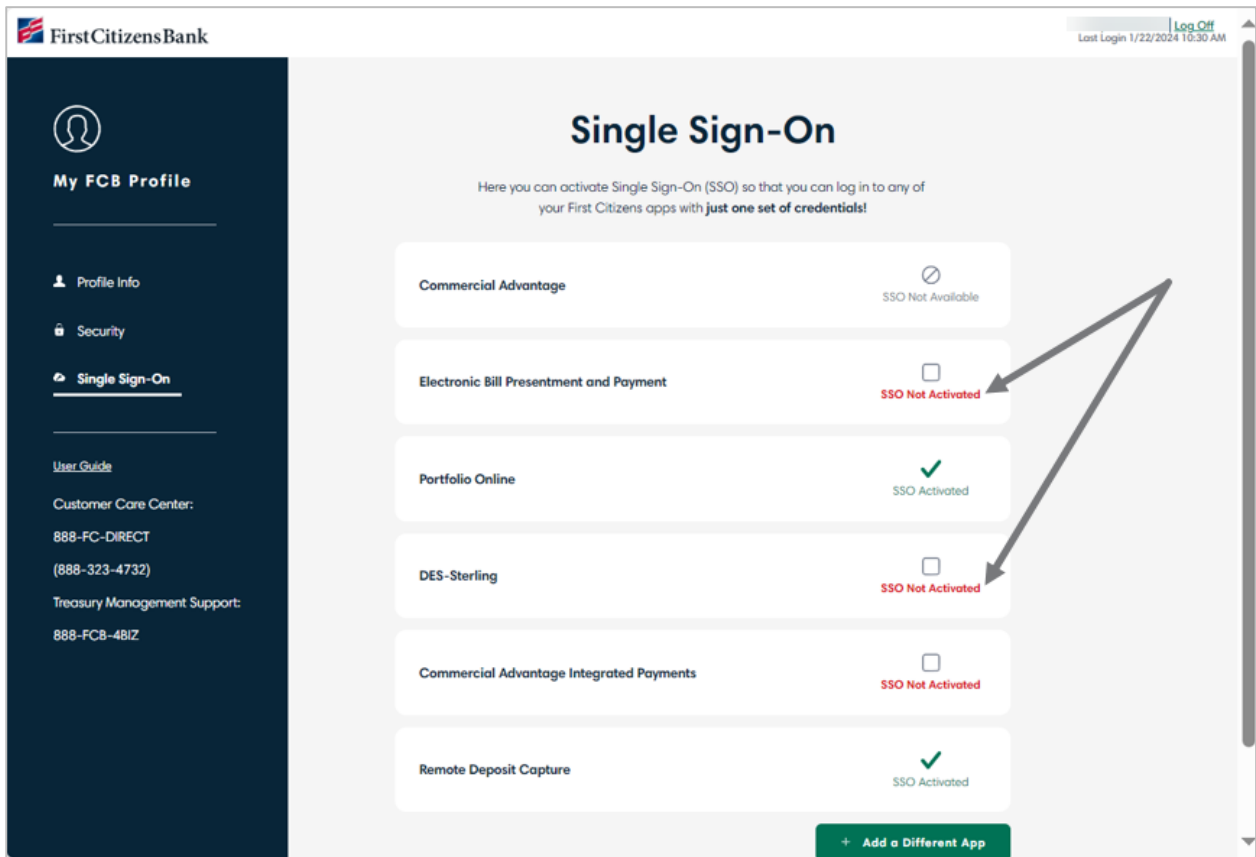
SINGLE SIGN-ON SETUP

Set up an App for SSO

You've already set up every available app for SSO!

We've got more app integrations coming soon, so keep an eye on your email and we'll let you know when they're available!

8. You will see **SSO Not Available** if an application is not available to undergo the merge process.



Disclosures:

Google and Google Docs are trademarks of Google LLC and this user guide is not endorsed by or affiliated with Google in any way.

Okta Content is the exclusive property of Okta and/or its licensor(s). Okta and/or licensor(s) own(s) all right, title and interest in the Okta Content, including but not limited to copyright, trademark, service mark, trade dress, and other applicable worldwide intellectual property rights.