Business Online Banking

DIGIPASS* User Guide

This document provides step-by-step instructions about how to download and use the DIGIPASS App to create "soft tokens" via your iOS or Android mobile device.

TABLE OF CONTENTS (click to jump to page)

DIGIPASS for Business Online Banking . . . . Page 3

Downloading the Application . . . . Page 3

Activating the Soft Token. . . . . Page 4

Using the Features and Functionality . . . . Page 7

Ongoing Login . . . . Page 7

Digital Signature . . . . Page 9

Add Another Token . . . . Page 9

Remove a Token . . . . Page 9

Working with Settings. . . . . Page 10

Manage Biometric Protection . . . . Page 11

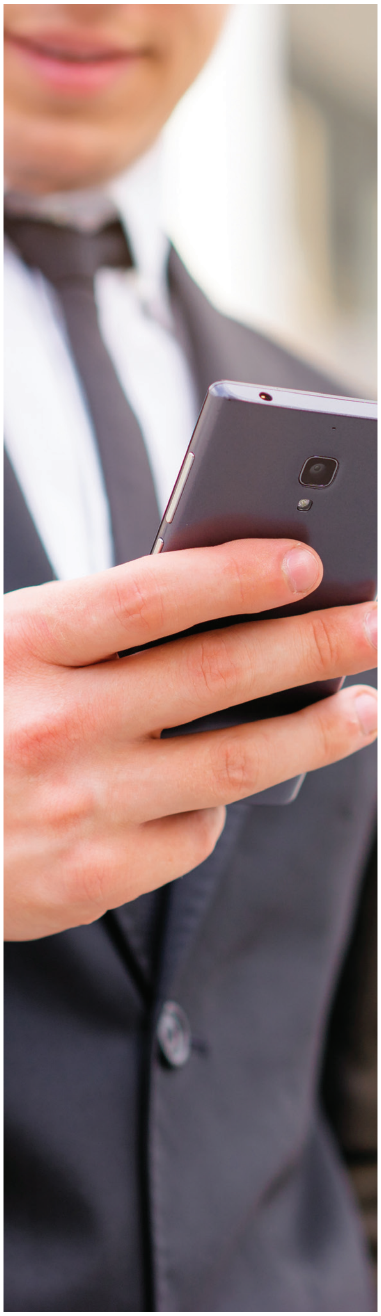
Change Password . . . . Page 12

Information . . . . Page 13

Provider Information . . . . Page 14

Rename the Token . . . . Page 14

Delete the Token . . . . Page 15



* DIGIPASS is a third-party application and is not developed or maintained by First National Bank. By utilizing the app, you agree to the terms and conditions set forth by DIGIPASS.

TREASURY MANAGEMENT

First National Bank

- Educate staff about password confidentiality and reinforce this regularly.
- Check that all requests for information are genuine – and ignore any requests for bank account details and passwords, whether by phone or email.
- Ignore suspicious emails, consider deleting them unread – **and be very wary of opening attachments or clicking on any links contained within an email, unless they are from a known source.** Always cut and paste URL information into a new browser window.
- Keep your web browser and anti-virus applications up to date with security patches.
- Ensure account transaction reconciliation functions are performed utilizing segregation of duties processes and performed and reviewed timely.
- Frequently check and review systems and processes with your 'security hat' on.
- Review transaction activity and account information on a daily basis. FNB has several Treasury Management services such as Positive Pay that can provide additional tools to assist with the review.

PLEASE NOTE: A Business Email Compromise (BEC) is a form of phishing attack where a cyber-criminal impersonates an executive (often the CEO), and attempts to get an employee, customer, or vendor to transfer funds or sensitive information to the phisher.

Unlike traditional phishing attacks, which target a large number of individuals across a company, BEC attacks are highly focused. Cyber criminals will scrape compromised email inboxes, study recent company news, and research employees on social media sites in order to make these email attacks look as convincing as possible. This high level of targeting helps these email scams to slip through spam filters and evade email whitelisting campaigns. It can also make it much, much harder for employees to recognize the email is not legitimate. An email message request for payment to be sent outside the company should ALWAYS be verified OUTSIDE of the email channel to ensure it is a legitimate request. Do not verify the request via email as the verification may be coming from the fraudster.

If you see anything unusual immediately contact Treasury Management Support at (866) 750-5298.

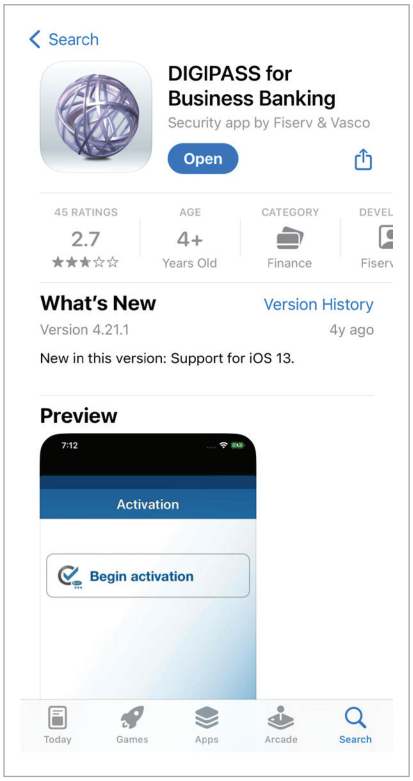
Everyone in your business needs to remember that skilled fraudsters will resort to all manners of subtlety and guile to trick people into disclosing valuable information.

For additional security updates and information, visit our website at www.fnb-online.com and click on the Security Center link at the bottom of the screen.

IMPORTANT

- For a successful soft token activation:
  - Download and launch the DIGIPASS for Business Banking application on a mobile device. This allows you to scan the QR code that displays in Business Online Banking on your desktop.
  - Log into your Business Online Banking account mobile app.
- Note: While DIGIPASS is available to iOS and Android mobile devices, this User Guide features screen images of iOS devices only. This is because the iOS and Android user experiences are virtually identical.

Log into Business Online Banking


DIGIPASS for Business Banking

Security app by Fiserv & Vasco

What's New

Version 4.21.1 4y ago

New in this version: Support for iOS 13.

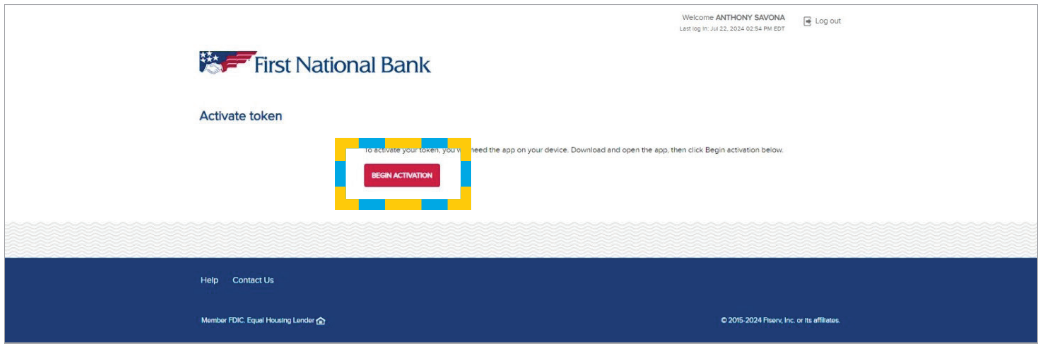
Downloading the Application

1. Go to the Google Play (Android users) or App Store (iOS users).
2. Search **DIGIPASS for Business Banking**.
3. **Install the App**.

Activating the Soft Token

After you download the application on your mobile device, you need to activate the soft token. Complete the following steps to activate the soft token on your mobile device.

1. Launch the DIGIPASS app.
2. Click **Begin Activation on Both Devices**.



Welcome **ANTHONY SAVONA**
Last log in: Jul 22, 2024 02:54 PM EDT

Log out

First National Bank

Activate token

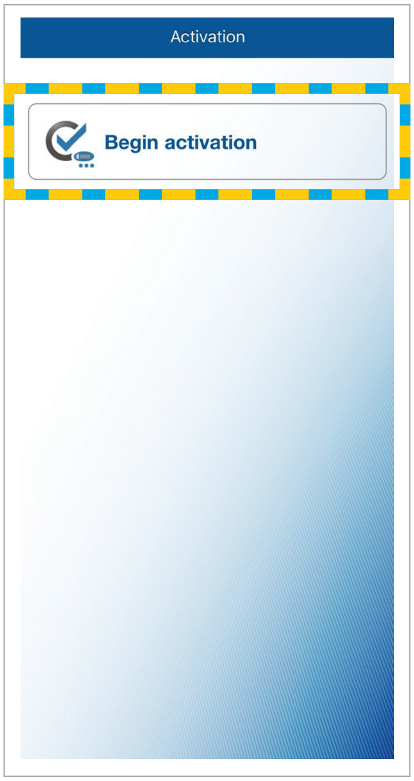
To activate your token, you w need the app on your device. Download and open the app, then click Begin activation below.

BEGIN ACTIVATION

Help Contact Us

Member FDIC. Equal Housing Lender

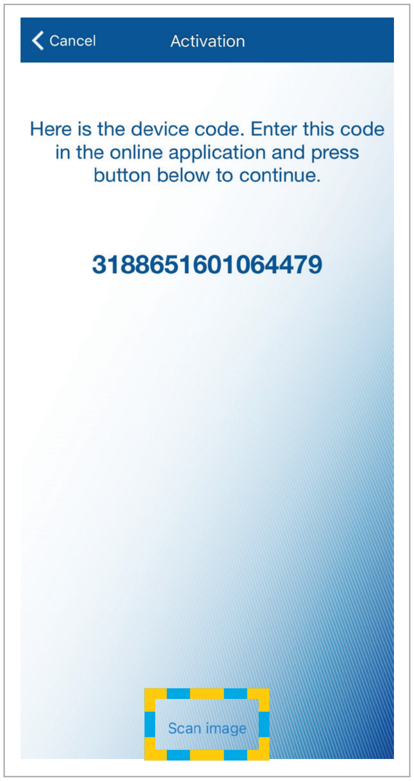
© 2015-2024 Fiserv, Inc. or its affiliates.



Activation

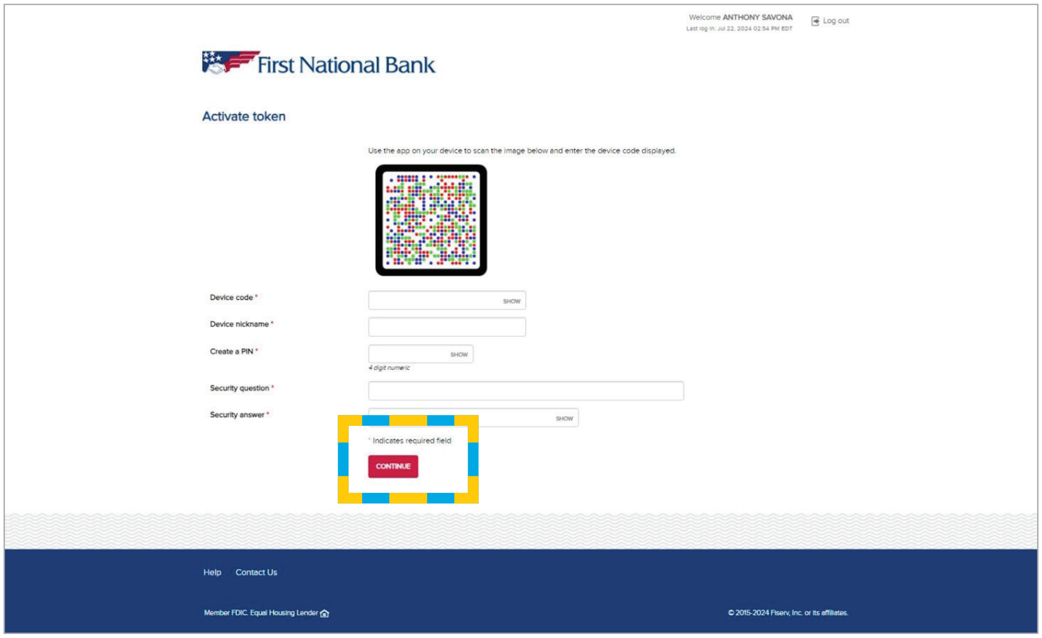
Begin activation

3. Clicking **Begin Activation** on your mobile device will automatically launch your camera functionality. Use the camera to scan the QR code that DIGIPASS displays on your Business Online Banking application. A device code then appears on your mobile device.
4. Enter the **Device Code** on your Business Online Banking application and complete all other fields. When creating a Personal Identification Number – or PIN – choose a four-digit number that's easy for you to remember but difficult for someone to guess. For example, the birthday of a friend or loved one… a street address of a neighbor…or the last four digits of a phone number you have memorized. Once you've completed all the fields, **Click Continue.**
5. Click **Scan image** to scan the second image that displays on your Business Online Banking application. The Complete activation screen appears.



Here is the device code. Enter this code in the online application and press button below to continue.

3188651601064479



Welcome ANTHONY SAVONA
Last log in: Jul 22, 2024 02:54 PM EDT
Log out
First National Bank

Activate token

Use the app on your device to scan the image below and enter the device code displayed.

Device code * SHOW

Device nickname *

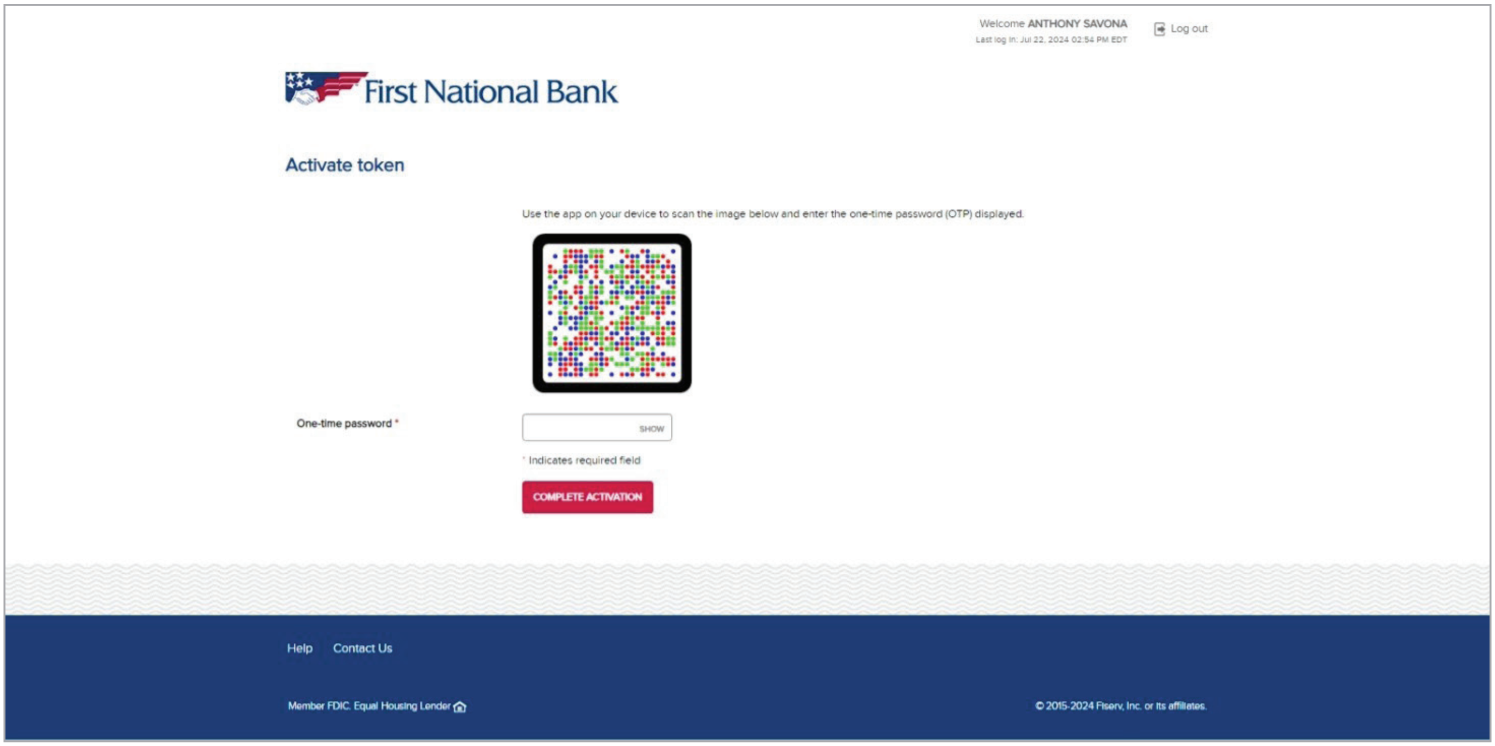
Create a PIN * SHOW
4 digit numeric

Security question *

Security answer * SHOW

* Indicates required field

CONTINUE
Help
Contact Us
Member FDIC. Equal Housing Lender
© 2015-2024 Fiserv, Inc. or its affiliates.



Welcome ANTHONY SAVONA
Last log in: Jul 22, 2024 02:54 PM EDT

Activate token

Use the app on your device to scan the image below and enter the one-time password (OTP) displayed.

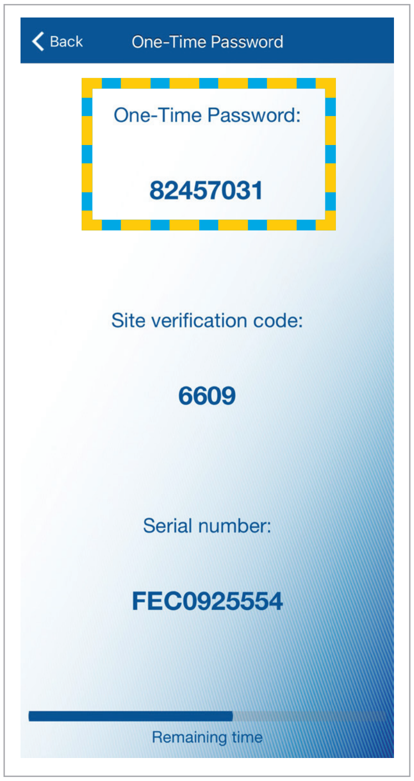
One-time password *

* Indicates required field

Member FDIC. Equal Housing Lender

© 2015-2024 Fiserv, Inc. or its affiliates.

6. Enter the first **One-Time Password** in the Business Online Banking application. The complete activation screen displays the soft token serial number assigned to you.



One-Time Password: 82457031

Site verification code: 6609

Serial number: FEC0925554

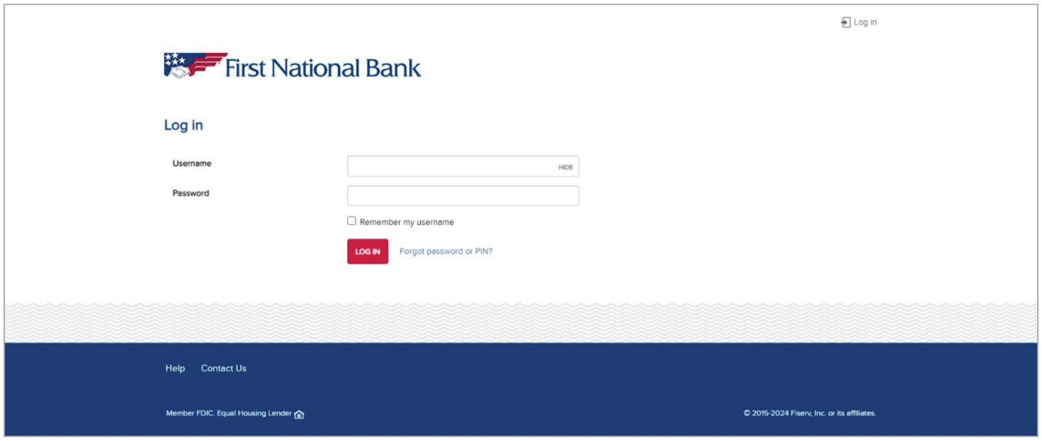
7. Click **Done**.

One-Time Password

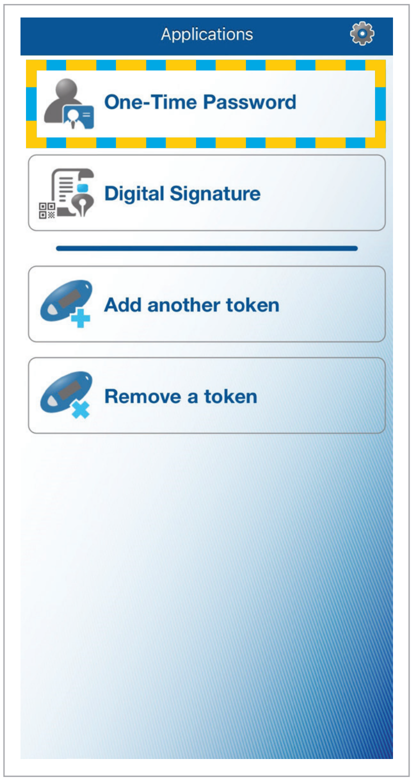
Use the **One-Time Password** feature for logging into the Business Online Banking application.

NOTE: If either the Change Password or Manage Biometric Protection feature is enabled in the Settings menu of your application, you need to provide the local password or fingerprint before the device generates a one-time password.

1. **Launch Business Online Banking** and enter your Username in the "Username" field.

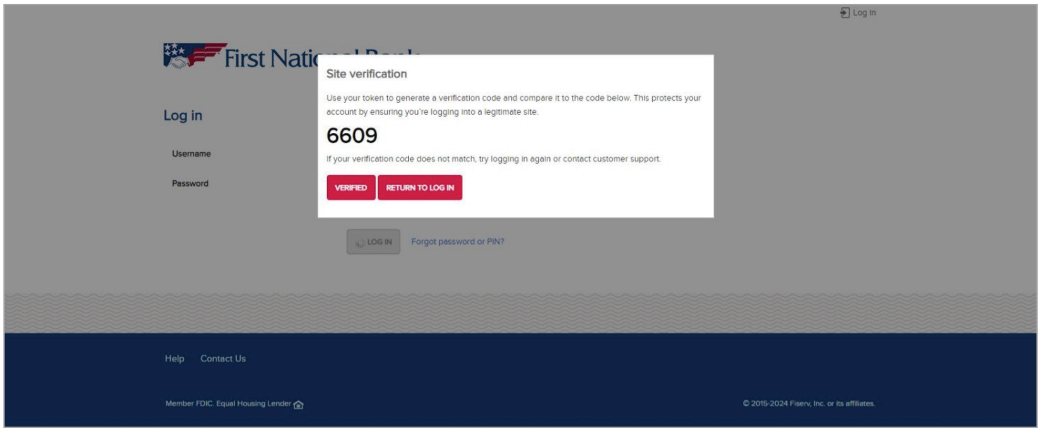


2. Launch DIGIPASS on your mobile device and **Select One-Time Password**



3. **Enter** your One-Time Password PLUS the 4-digit PIN (created during activation) in the "Password" field. For example: If your PIN is **1234** and your One-Time Password is **82457031**, then the Password to enter is **824570311234**.

4. Verify that the 4 digit Site Verification Code ‘6609’ displayed in Business Online Banking matches the Site Verification Code displayed on your DIGIPASS mobile app and **click ‘Verified’** in Business Online Banking.

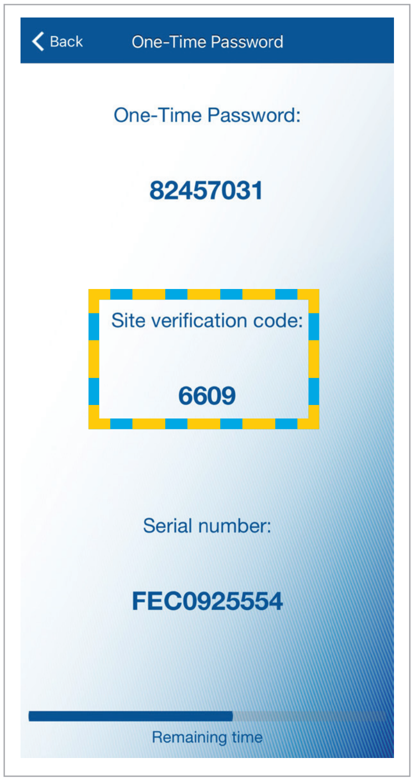


Site verification

Use your token to generate a verification code and compare it to the code below. This protects your account by ensuring you're logging into a legitimate site.

6609

If your verification code does not match, try logging in again or contact customer support.



One-Time Password:

82457031

Site verification code:

6609

Serial number:

FEC0925554

Digital Signature

Use the **Digital Signature** feature to scan the image that displays on your Business Online Banking application to generate a password at the time you perform a transaction.

Add Another Token

If you are associated with different companies, use the **Add another token** feature to add another soft token on your device.

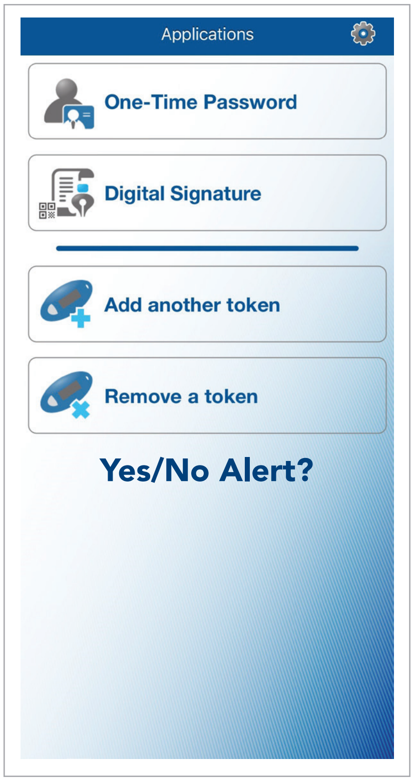
Follow steps 2 through 6 of Activating the Soft Tokens section to add multiple soft tokens.

NOTE: If a soft token serial number already exists, the device prompts for confirmation of whether you want to overwrite the existing soft token.

Remove a Token

Use the **Remove a token** feature to remove a token from the application. Complete the following steps to remove a token. NOTE: You should only remove a token if you are directed to do so by an FNB Customer Support Representative.

1. Scan the image that displays on your Business Online application to remove the soft token. A confirmation message to remove the token appears.

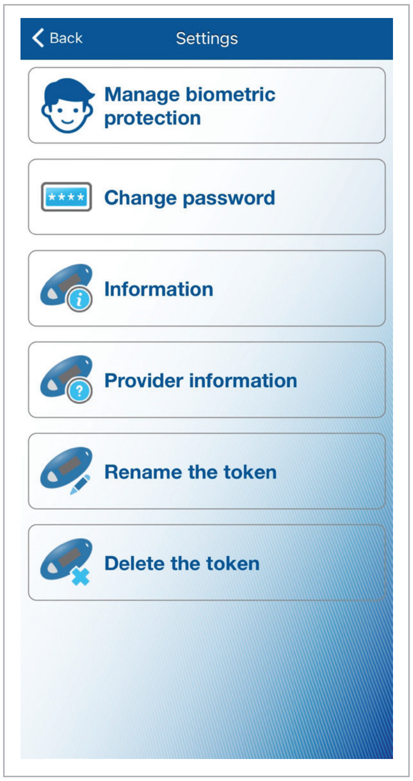


2. Click **Yes**.

Working with Settings

The **Settings** button displays on the top bar of the application. The following options are available:

- Manage Biometric Protection
- Change Password
- Information
- Provider Information
- Rename the Token
- Delete the Token

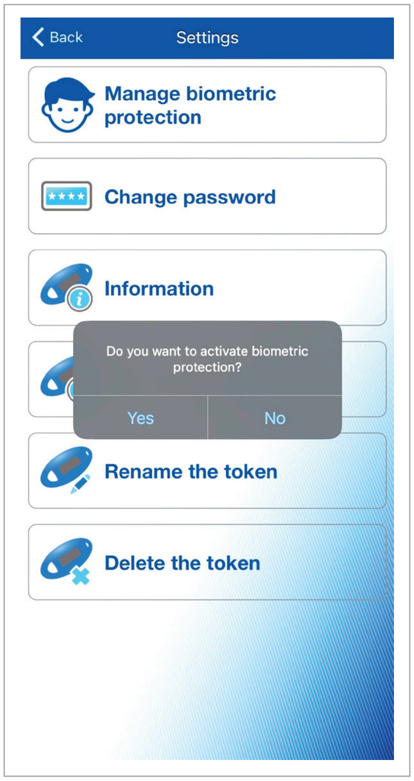


Manage Biometric Protection*

The Manage Biometric Protection option allows you to enable or disable biometric protection for the application. The option provides you with an extra level of security at the time of activation of the soft token, logon, or performing transactions.

NOTE: This option only displays on a device that supports the biometric protection feature and the feature is enabled.

You need to provide the local password to activate the Manage Biometric Protection option.

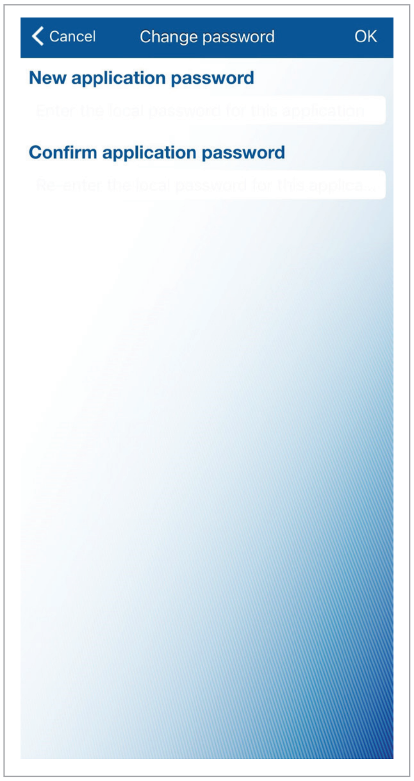

Do you want to activate biometric protection?

* FNB does not collect, use, process or retain your biometric data. By using biometric verification for secure log-in to DIGIPASS you agree to the terms and conditions set forth by DIGIPASS.

Change Password

The **Change password** option allows you to add or change the local password.

NOTE: This option does not display if the Manage Biometric Protection option is enabled.



New application password

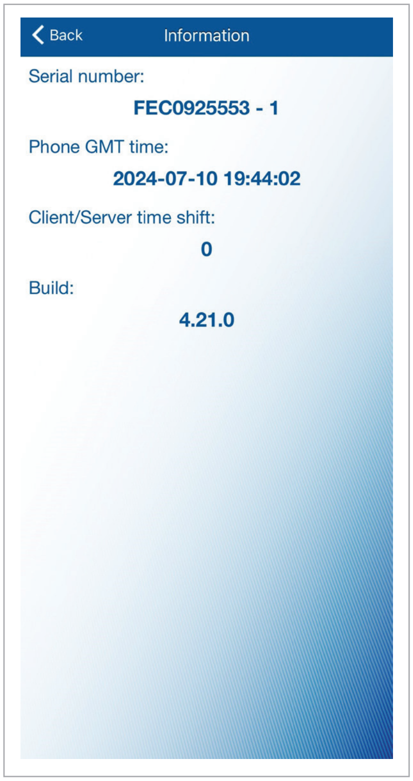
Enter the local password for this application

Confirm application password

Re-enter the local password for this applica ...

Information

The **Information** option displays the soft token serial numbers and other application details.



Serial number:
FEC0925553 - 1

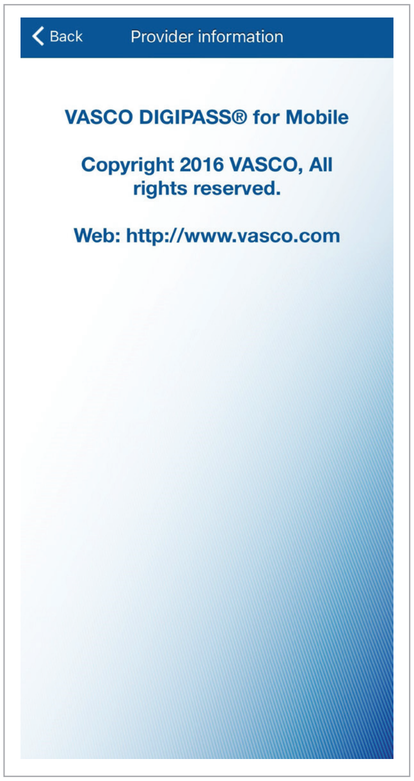
Phone GMT time:
2024-07-10 19:44:02

Client/Server time shift:
0

Build:
4.21.0

Provider Information

The **Provider information** option displays copyright information of the provider.



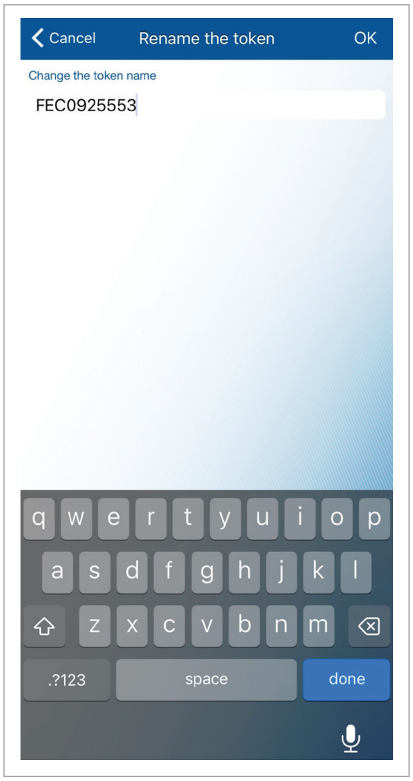
VASCO DIGIPASS® for Mobile

Copyright 2016 VASCO, All rights reserved.

Web: http://www.vasco.com

Rename the Token

The **Rename the token** option allows you to rename the available tokens.

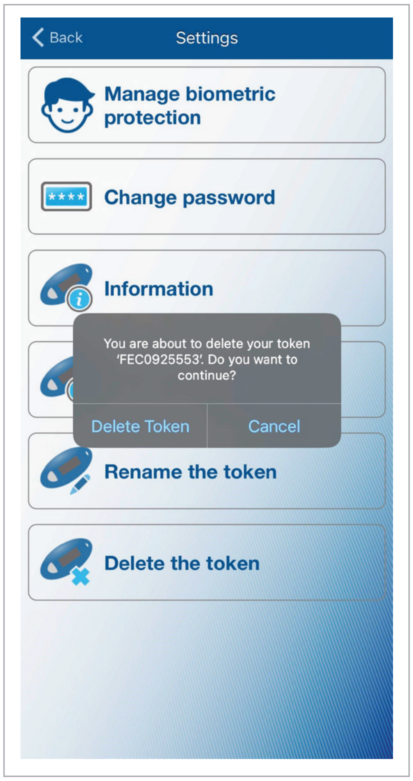


Change the token name

FEC0925553

Delete the Token

The **Delete the token** option allows you to delete the soft tokens without scanning the image



You are about to delete your token 'FEC0925553'. Do you want to continue?

For Assistance:

- For additional assistance, please call Treasury Management Support Toll-free at **(866) 750-5298** to speak to a support representative Monday - Friday between the hours of 8:00 AM and 5:30 PM EST.
- For technical assistance with tokens, please select the option for DIGIPASS.
- To contact Treasury Management Support via e-mail, the address is treasurymgmt@fnb-corp.com.