



ENROLLING A 3RD PARTY APP (2FA APP)

About

A 3rd party token – also known as a Two-Factor Authentication (2FA) app and a “Time-Based One-Time Password” (TOTP) – requires the installation of a third-party app on the user’s mobile device from their respective app store.

2FA apps may be used for both retail and business customers.

Step 1

Download one of the apps below on the user’s primary mobile device. Users may choose another 2FA app, but should be prepared to personally troubleshoot any issues that may arise.

Duo Mobile



(Twilio) Authy



Google Authenticator



Step 2

Sign in to Kennebec Savings Bank’s online banking platform on a desktop device. Navigate to Settings > Security. Under Two-Factor Authentication > 2FA App, select Enroll

Authenticate using a two-factor authentication application like Google Authenticator, Authy, or Duo.

☐ Set As Preferred Authentication Method ★

Enroll

Step 3

Scan a QR code using their 2FA app – see step 4 for the mobile app side



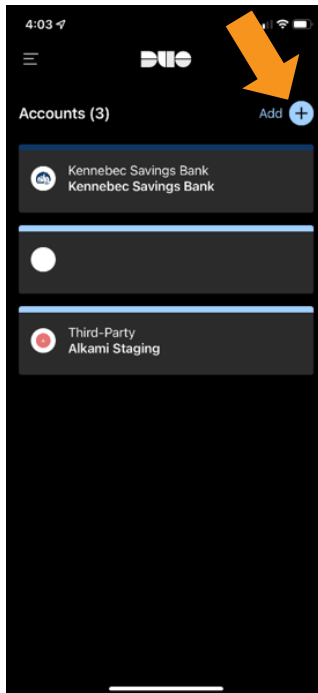
Enter code manually.

***this QR code is an example** use the QR code on your computer screen, once logged in.

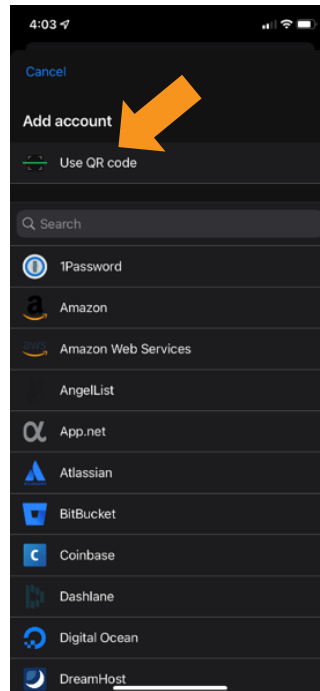


Step 4: In Duo, the process looks like this:

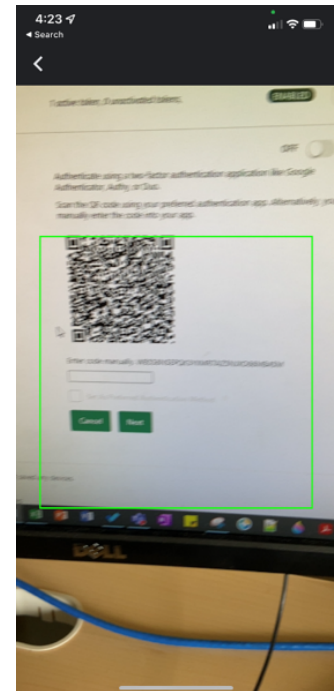
- 1 Open Duo and click Add in the top right.



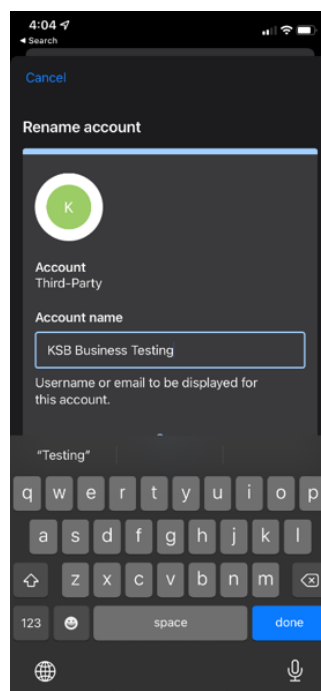
- 2 Click Use QR Code.



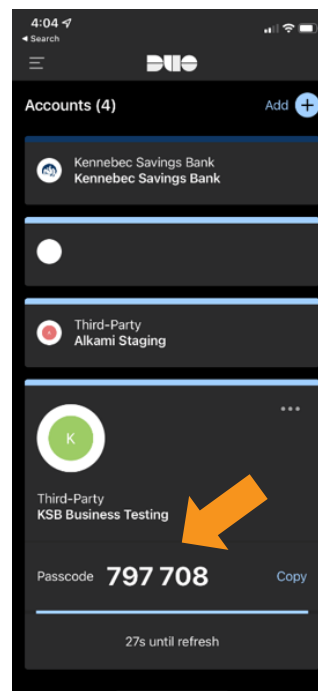
- 3 Use your camera to scan the QR code on your desktop.

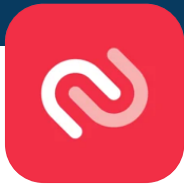


- 4 Name your account.



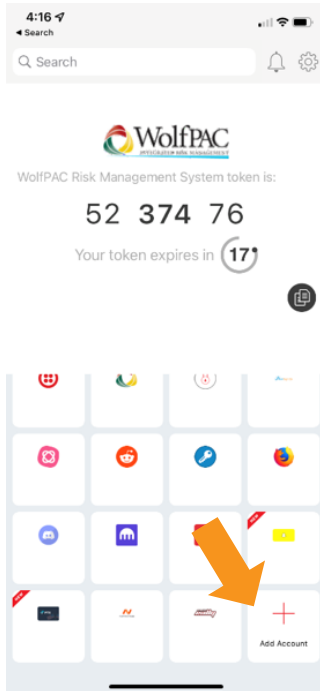
- 5 Use your passcode to finalize enrollment.





Step 4: In Authy, it looks like this:

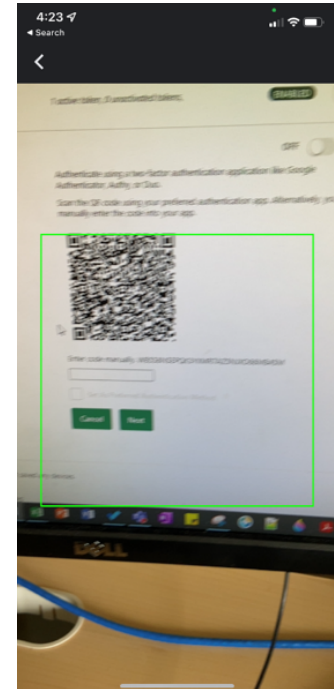
- 1 Open Authy and click the Add Account tile



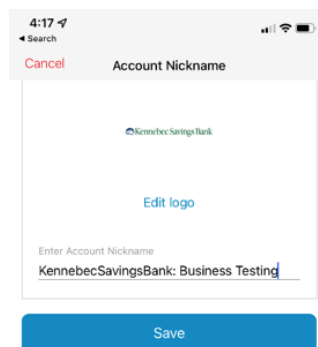
- 2 Click Scan QR Code.



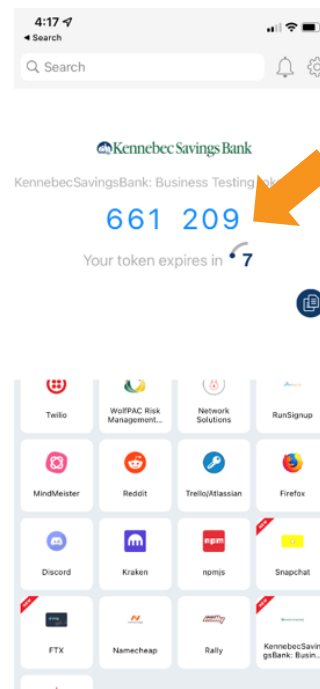
- 3 Use your camera to scan the QR code on your desktop.



- 4 Name your account.



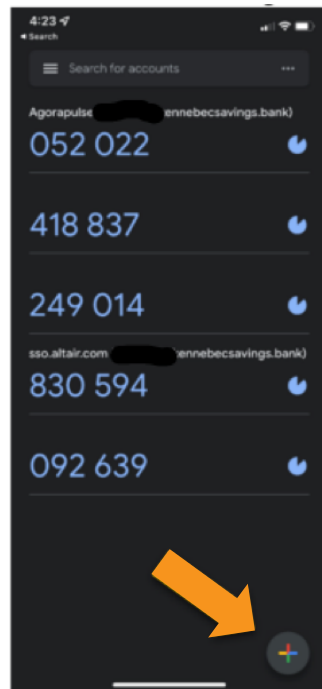
- 5 Use your token to finalize enrollment.



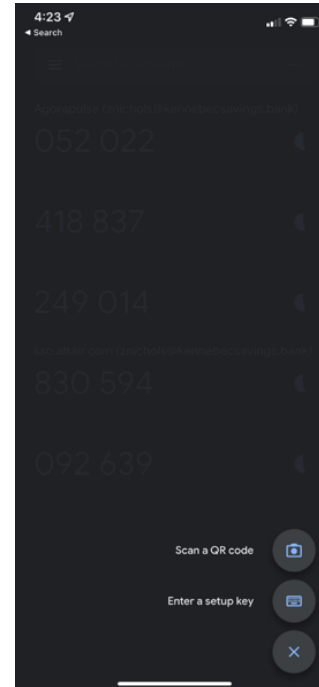


Step 4: In Google Authenticator, it looks like this:

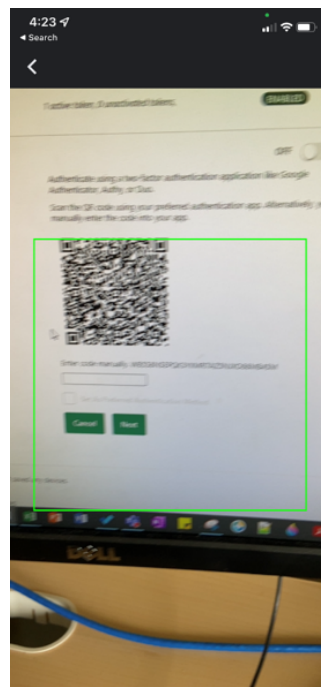
- 1** Open Authenticator and click the + in the bottom right.



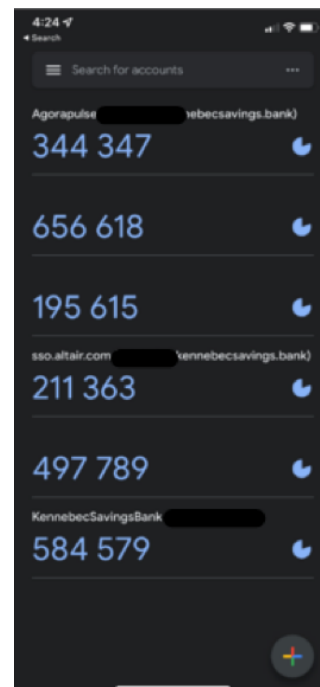
- 2** Click Scan QR Code.



- 3** Use your camera to scan the QR code on your desktop.



- 4** Use your code to finalize enrollment.

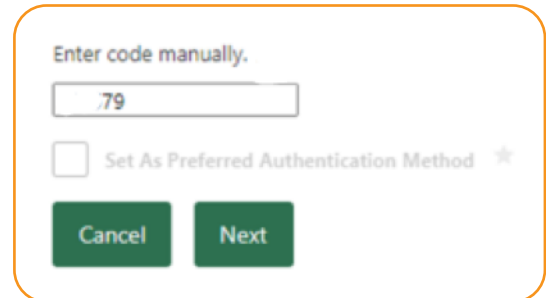


NOTE:

With Duo, Authy, and Google Authenticator, you may also be required to create a backup code or password, so that if you ever lose access to your mobile device, you can restore access to your 2FA app credentials. The bank should be able to assist users with re-accessing our platform and enrolling a new soft token if necessary, but will not be able to assist with restoring the original 2FA app if they use it for other services.

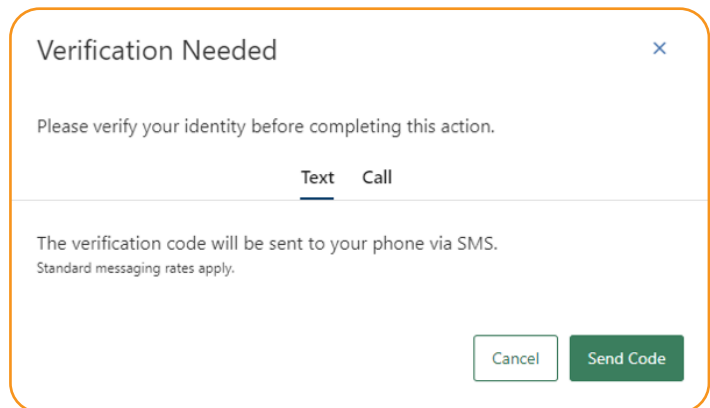
Step 5

Enter the six digit code displayed in your 2FA app and hit Next to complete enrollment:



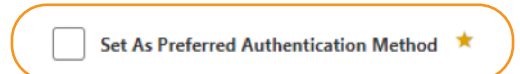
Step 6

You may be asked to verify your identity with an existing multifactor authentication method

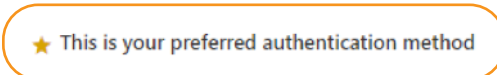


Step 7

Set as preferred authentication method by checking the box



Which will change it to this:



Step 8

Turn on the Require Two-Factor Authentication For Each Login at the top of the section



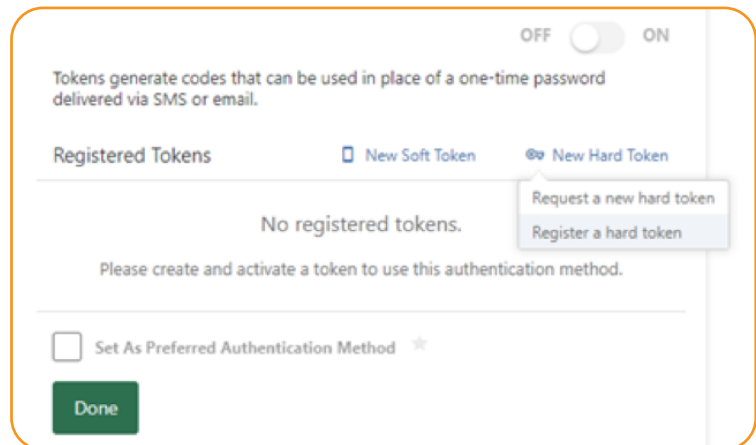
Note: To delete a token, you must first turn on another method and make primary, before you can delete a token.

ENROLLING A HARD TOKEN

Note: Hard tokens are only available for eligible business customers. You can speak with our Business Account Managers to discuss the use of hard tokens.

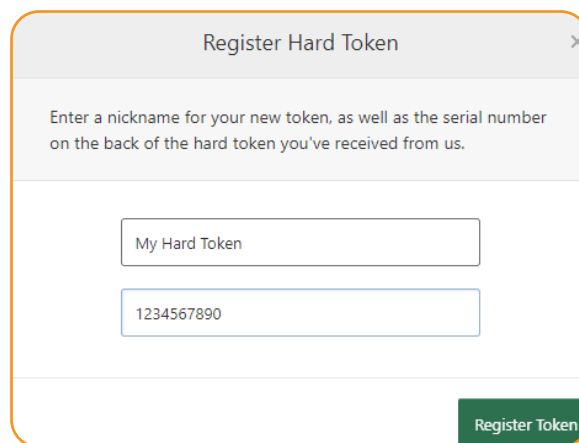
Step 1

Sign into Kennebec Savings Bank Online Banking platform on a desktop device, go to Settings > Security. Under Two-Factor Authentication, select New Hard Token > Register a hard token



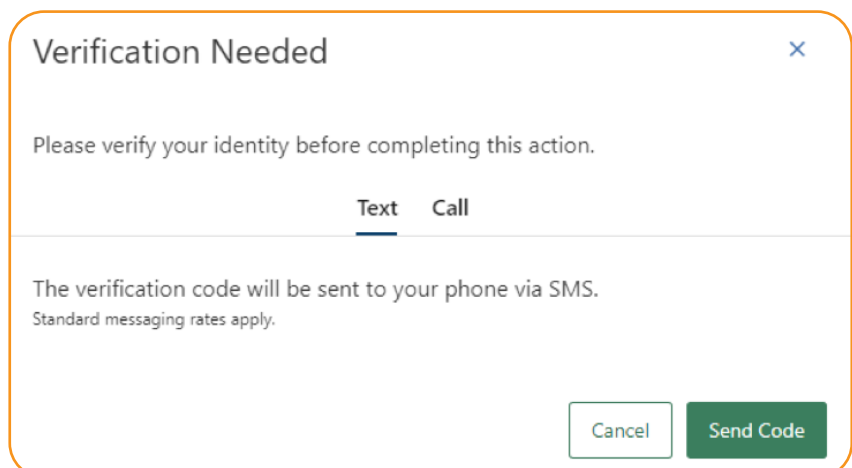
Step 2

Register a hard token by entering a nickname for the token, its serial number on the back, and selecting Register Token



Step 3

You will be required to verify using an existing MFA method



Step 4

For the two successive codes: Press the button on your token enter the number. Press and hold the button on the token and the token will display all 8's. Disregard this and press the token button again to receive a valid code. Enter that code on your desktop and click Sync

 The token was assigned successfully.

You will be entering two successive codes to complete the token registration process.

To begin, please press and hold the button on your token until the first code appears. Press and hold the button again to receive the second code

First Token Code

Second Token Code

Sync

Step 5

Set Token as your preferred method

OFF  ON

Tokens generate codes that can be used in place of a one-time password delivered via SMS or email.

Registered Tokens [New Soft Token](#) [New Hard Token](#)

 My Hard Token

Serial #: 1234567890 • Never used

ACTIVE 

☐ Set As Preferred Authentication Method ★

Done

Step 6

Click to turn on Require Two factor for each login

Require Two-Factor Authentication For Each Login ⓘ

OFF  ON

EMAIL CODE

1 email address on file

DISABLED 

CODE VIA SMS

OFF  ON

A one-time code will be sent to your phone number of choice. The phone numbers can be edited under the Contact tab.

HOME	(207) 662-5801
MOBILE	(207) 662-5801
Edit in contact settings >	

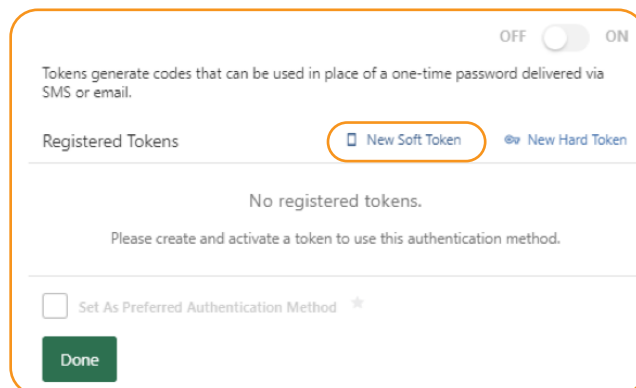
Note: Soft tokens are only available for eligible business customers.

Online Banking:

Step 1. Sign into Kennebec Savings Bank's Online Banking platform on a desktop device. Navigate to Settings > Security.

Step 2. Require two-factor authentication for each login, if desired

Step 3. Click edit for Token > New Soft Token



App Store/Google Play Store:

Step 4. Download the Entrust Identity app from App Store or Google Play

Step 5. Open the app on mobile device

Step 6. Read and acknowledge the terms and conditions of the app

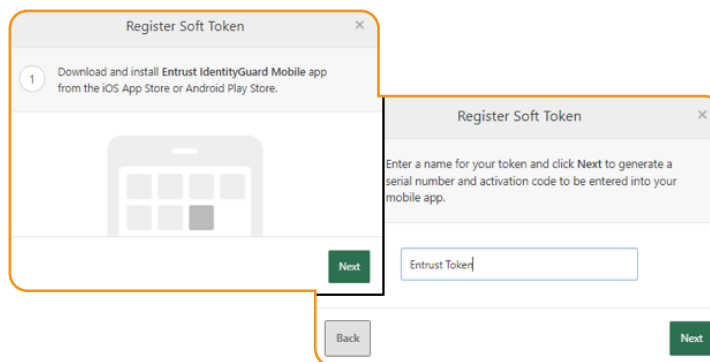
Step 7. On the "Let's get started", select "Add identity later"



Online Banking:

Step 8. Click Next

Step 9. Name your token and click next



Entrust Identity App:

Step 10. Click Add Identity > Manual

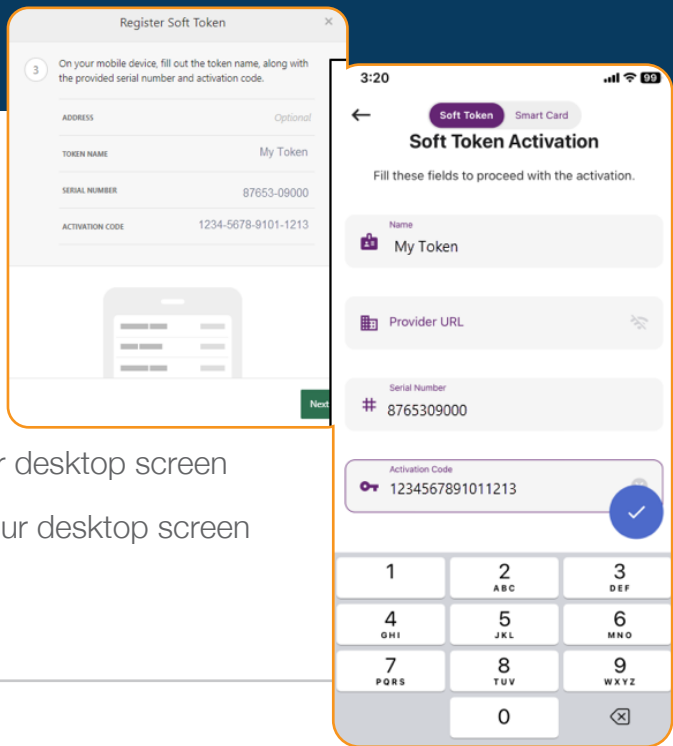
Step 11. Type the same token name again

Step 12. Skip provider URL

Step 13. Enter Serial Number (10 digits) from your desktop screen

Step 14. Enter Activation Code (16 digits) from your desktop screen

Step 15. Click Checkmark for next screen



Online Banking:

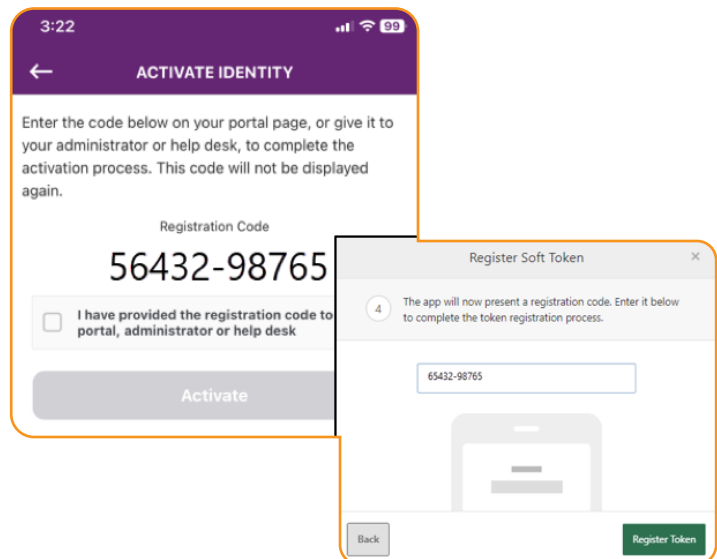
Step 16. Click Next

Step 17. Enter the Registration code from Identity app. Click register Entrust Identity App:

Step 18. Check "I have provided the registration code to the portal, administrator or help desk."

Step 19. Click Activate. Click OK on the pop up

Step 20. Set your identity pin by entering it twice and clicking confirm.



Online Banking:

Step 21. If preferred method, check "Set as Preferred Method"

Step 22. Click done.

With "Require Two-Factor Authentication For Each Login" enabled, each time online banking is accessed, open the Entrust Identity app to retrieve the 8-digit authentication code.

