

Associated Connect[®]

Multi-Factor Authentication and Password Management Guide



Table of Contents

Associated Connect Access	3
Available Services	3
Sign-In and Security	3
Multi-Factor Authentication	4
Text Message (SMS) Verification	4
Security Code Authentication.....	5
Mobile Token Installation and Activation.....	5
Renaming your OneSpan Account	10
Using your Mobile Token	11
Physical Token Registration.....	13
Using your Physical Token	14
Registering and Assigning Tokens (for Company Administrators)	16
De-Registering and un-assigning Tokens (Company Administrator)	18
Password Management.....	20
Associated Connect Password FAQ.....	21

Associated Connect Access

Associated Connect provides secure, single sign-on access to your business and commercial banking services through AssociatedBank.com/Business or AssociatedBank.com/Commercial.

Available Services

Once signed in, users can access a wide range of online banking functions:

Banking	Account Balances, ACH Origination Check Inquiry, Image Search, Positive Pay, Stop Payments, Transfers and Wire Transfers
Account Summary	View balances and transaction details
Cash Management	Bill Pay*, Cash Ordering, Checkview, FX Manager, Lockbox, Remote Deposit and Trade Services
Transmission and Reporting	Document Center, Export Tools and File Transfer

*Some services within the bill payment service have service charges. Please refer to the Business Fee Schedule or the applicable Checking Product Disclosure for details. (1276)

Sign-In and Security

Access to Associated Connect requires identity verification through one of two methods:

High-Risk Services	• Sign in with your username and password. • Verify identity using multi-factor authentication (MFA) with a unique access code from a mobile or physical token.
Low-Risk Services	• Sign in with your username and password. • Verify identity using a unique access code sent by text message (SMS) to your registered mobile number.

For help with tokens, see the Multi-Factor Authentication and Password Management Guide or contact Customer Care at 800-728-3501.

Associated Bank does not charge a fee to download our digital applications; however, transactional fees may apply. Carrier message and data rates may apply; check your carrier's plan for details. Visit AssociatedBank.com/disclosures for Terms and Conditions for your service. (1406)

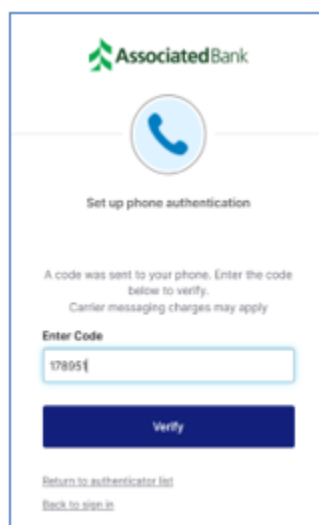
Multi-Factor Authentication

The Associated Connect platform is a fully integrated suite of cash and treasury management solutions for business clients that offers a wide array of services including ACH Origination, Account Transfers, Bill Pay, Cash Ordering, Document Center, Export, File Transfer, FX Manager, Lockbox, Positive Pay, Remote Deposit, Wire Transfer and Trade Services.

Associated Connect uses different types of multi-factor authentication depending on the services that the client is set up with. The type of authentication that'll be required will depend on the risk level of the client's accessible services. For high-risk services, multi-factor authentication is set up at the company level for all users.

Text Message (SMS) Verification

When signing in with low-risk services, you may receive a text message (SMS) containing a unique verification access code sent to your registered mobile number. Enter the code when prompted to securely complete the sign-in process.



The image shows a mobile app screen for Associated Bank. At the top is the Associated Bank logo. Below it is a blue circular icon with a white telephone handset. The text "Set up phone authentication" is centered. Below that, a message states: "A code was sent to your phone. Enter the code below to verify. Carrier messaging charges may apply." There is a text input field labeled "Enter Code" containing the number "17895". Below the input field is a dark blue button labeled "Verify". At the bottom, there are two links: "Return to authenticator list" and "Back to sign in".

Security Code Authentication

Clients with access to high-risk services will always be required to enter a security code when signing in to Associated Connect. Associated Bank offers two types of security tokens that can be used to authenticate a user's identity through a unique, randomly generated numeric code. Each Associated Connect user will need to determine which type of security token they prefer:

- A mobile token which is available by downloading a mobile application.
- A physical token.

Note: *Physical tokens will be provided upon request and may take up to 7 days to be delivered. Please contact your Company Administrator if you require a physical token. If you're a Company Administrator, please call our Customer Care team at 800-728-3501 to request physical tokens.*

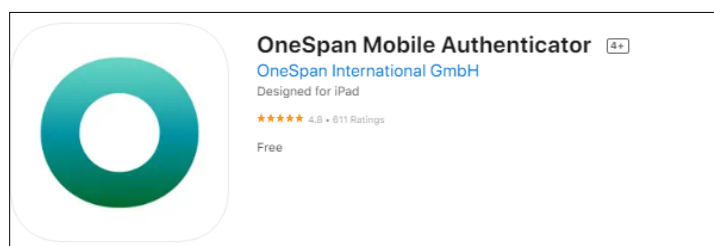
Mobile Token Installation and Activation

If you'd like to use a mobile token for authentication, you'll need to install the **OneSpan Mobile Authenticator**® application on your mobile device. This mobile token is supported on Apple and Android products that have:

- Android 4.1 and higher
- iOS 12.0 and higher

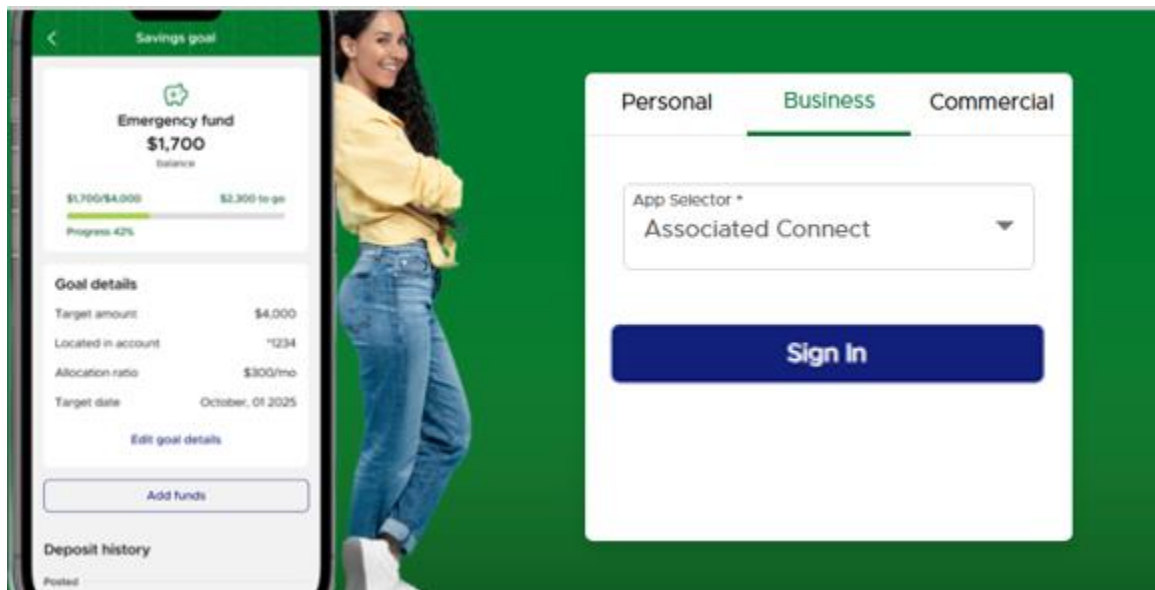
You'll need access to a mobile device and computer for this initial setup process.

From the App Store or Google Play Store, download the **OneSpan Mobile Authenticator** app on your mobile device.

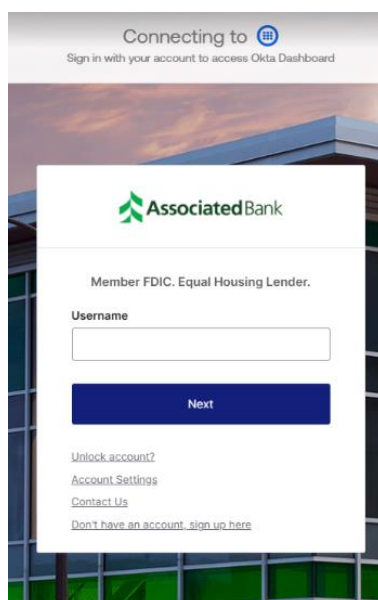


After the mobile app installs, complete the following steps on a computer to activate your mobile token:

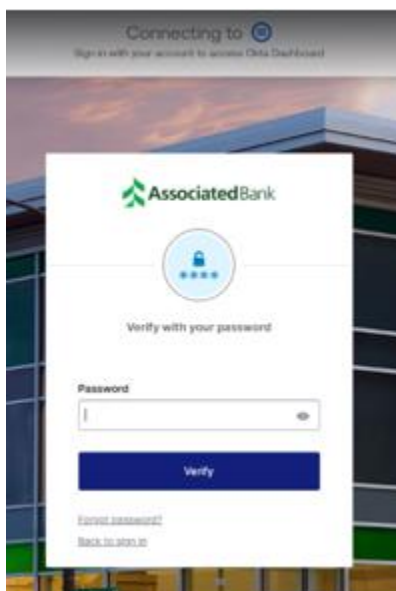
From the **AssociatedBank.com/Business** or **AssociatedBank.com/Commercial** website, sign in to Associated Connect:



1. Enter your Associated Connect Username and select **Next**.



2. Enter your Associated Connect password and select **Verify**.



3. Return to your mobile device, open the OneSpan Mobile Authenticator app.
4. On the mobile app's first screen, select **Activate Account**.
5. Allow the app to access your camera. Scan the provided image shown on your computer by selecting the camera icon on the bottom of your mobile device's screen.

Note: *You may have to adjust the angle of your phone to capture the image. An upward angle is recommended if the image does not immediately scan.*

The app will then require you to **Authenticate** yourself in order to move to the next step. For Android and Apple devices, your fingerprint or facial recognition will be utilized.

6. Once the authentication is successful and the image is captured, the app will provide a numeric code to secure the app. Enter the code into the **Device Code** box (see image below) on your computer and select **Continue**.



7. A second image will appear within the Associated Connect portal on your computer. Scan this with your mobile device by clicking  .

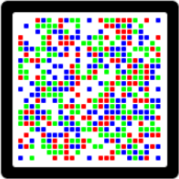
Activating MFA

[? Need help?](#)

Please click [here](#) for instructions on how to download the OneSpan app and active your mobile device for MFA

Step 2 - Confirmation Code

3. Scan this 2nd image using the OneSpan App on your mobile device.



4. Enter the Device Code shown in the OneSpan App on your mobile device and click "Continue".

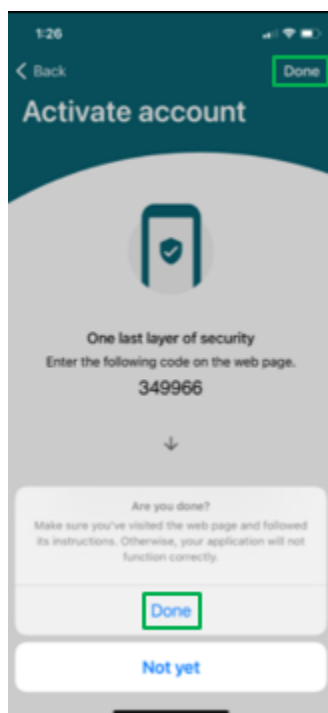
Confirmation Code

Activate

8. A second numeric code will be shown on your mobile device. Enter the code into the **Confirmation Code** box on your computer and select **Activate**.

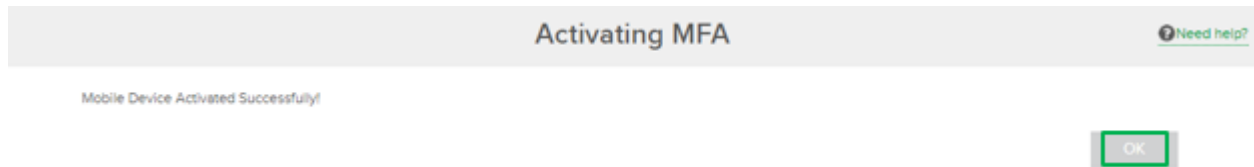


9. Once completed, select **Done** at the top right of the mobile app. A window will pop up at the bottom to confirm you're done with setup. Select **Done** again.



Note: If you don't select **Done** to confirm the activation within the app, you'll need to have your token de-activated and complete the setup process again. Please call our Customer Care team at 800-728-3501 to have your token de-activated.

10. You'll see that your mobile device has been successfully added. Select **OK** to begin your session.



Your OneSpan app is now activated and can be utilized on Associated Connect.

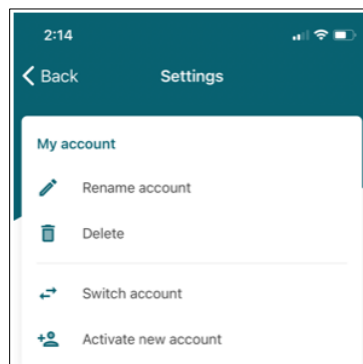
Renaming your OneSpan Account

Once your OneSpan app is set up, the account name can be changed.

1. Open your OneSpan app.
2. Select the gear icon at the top right of the application.



3. Select **Rename account** or **Switch account** to name a different account that's been previously set up.



Note: This is also the area where additional accounts can be set up, following the same setup steps as listed above by selecting **Activate new account**.

4. Enter the new name, then select **OK**.

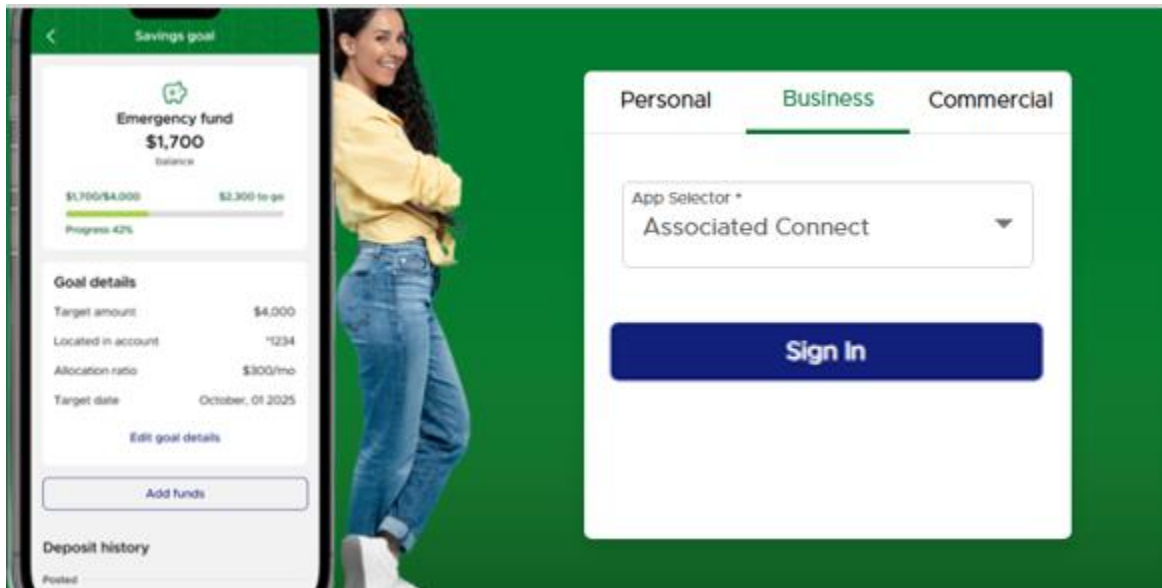
Change account name
Enter your account name

Demo

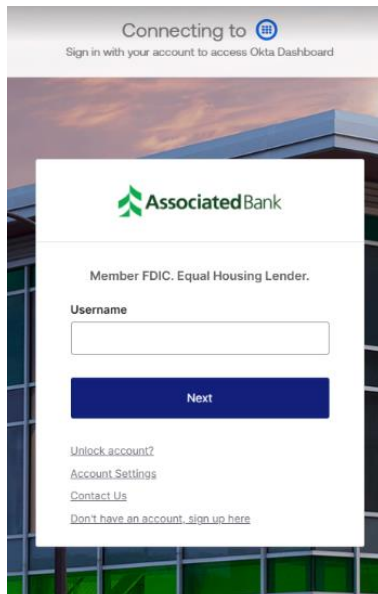
Cancel
OK

Using your Mobile Token

To use your mobile token to access Associated Connect, sign in to Associated Connect directly from Associated Bank's website at **AssociatedBank.com/Business** or **AssociatedBank.com/Commercial** by following the directions below.



1. Enter your Associated Connect Username and select **Next**.



Connecting to 
Sign in with your account to access Okta Dashboard

 Associated Bank

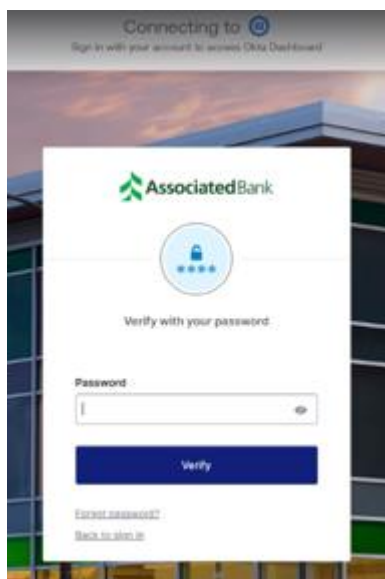
Member FDIC. Equal Housing Lender.

Username

Next

[Unlock account?](#)
[Account Settings](#)
[Contact Us](#)
[Don't have an account, sign up here](#)

2. Enter your Associated Connect password and select **Verify**.



Connecting to 
Sign in with your account to access Okta Dashboard

 Associated Bank



Verify with your password:

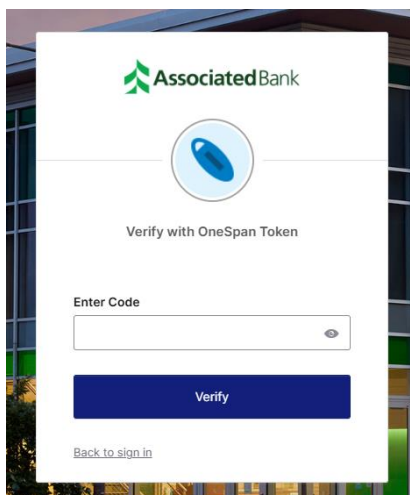
Password

Verify

[Forgot password?](#)
[Back to sign in](#)

3. You'll be prompted to enter a security code each time you sign in. To obtain the correct security code, open the OneSpan app on your mobile device and follow the instructions below. You'll need to enter your 6-digit OneSpan PIN, fingerprint or facial recognition that was established during the mobile token registration process.

4. Select the option to generate a One Time Password (OTP). OneSpan will then generate a security code. Enter the security code that appears on your mobile device into the **Enter Code** box on the Associated Connect screen and select **Verify**.



5. Once your security code is validated, you'll be able to access any service within Associated Connect.

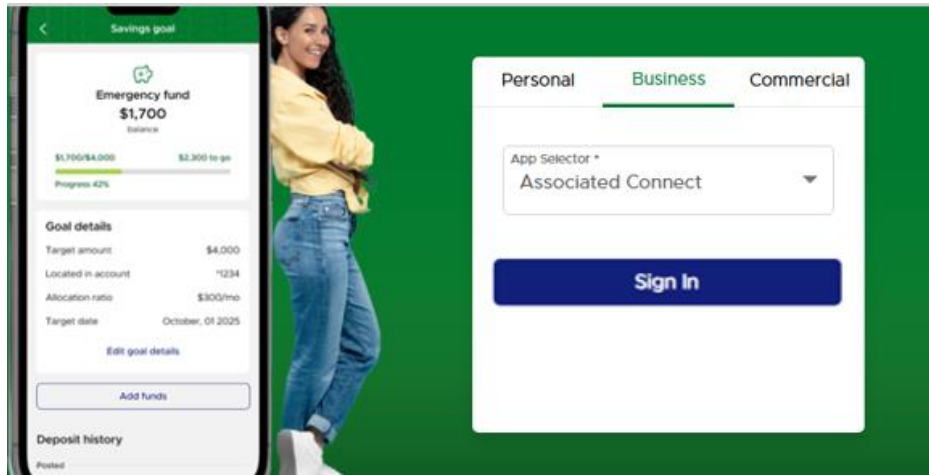
Physical Token Registration

Physical Tokens will be provided upon request and will need to be registered and assigned by your Company Administrator. Once you receive your physical token from your Company Administrator, you'll be able to use it immediately.

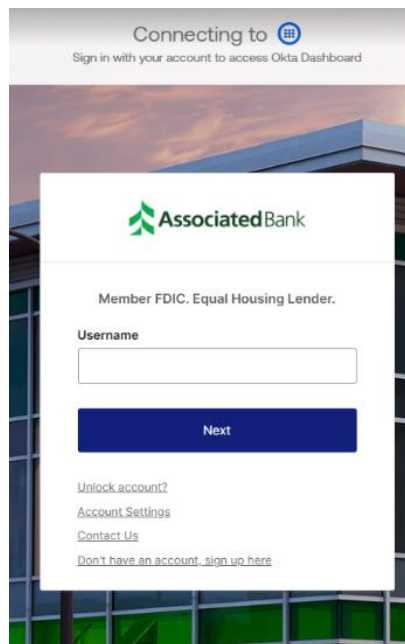
Note: *Physical tokens may take up to 7 days to be delivered. Please contact your Company Administrator if you require a physical token. If you're a Company Administrator, please call our Customer Care team at 800-728-3501 to request physical tokens.*

Using your Physical Token

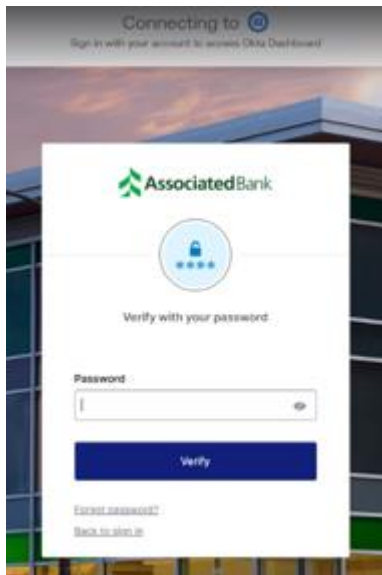
To use your Physical Token to access Associated Connect, sign in to Associated Connect directly from Associated Bank's website at **AssociatedBank.com/Business** or **AssociatedBank.com/Commercial** by following the directions below.



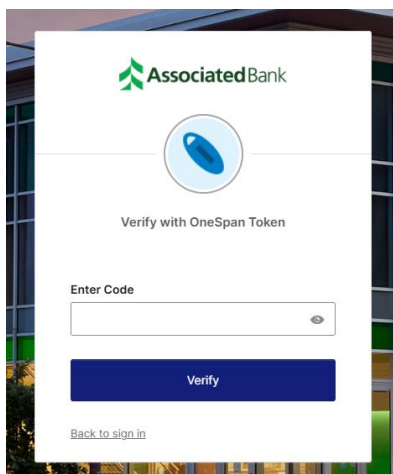
1. Enter your Associated Connect Username and select **Next**.



2. Enter your Associated Connect password and select **Verify**.



3. You'll be prompted to enter a security code. Refer to your physical token to obtain the correct security code and follow the steps below:

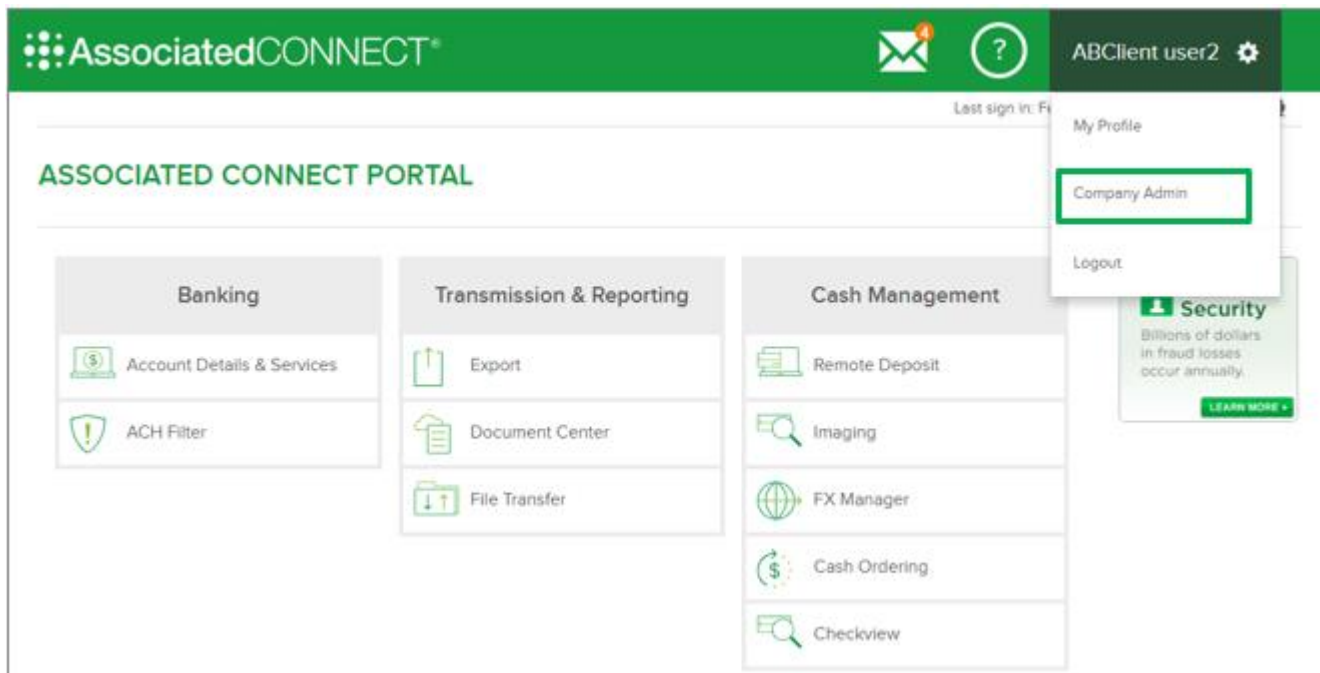


4. Press the button on your physical token and it'll generate a valid security code on its screen.
5. Enter the security code into the **Enter Code** box on the Associated Connect screen and select **Verify**.
6. Once your security code is validated, you'll be able to access any service within Associated Connect.

Registering and Assigning Tokens (for Company Administrators)

The Company Administrator will be required to register each user for either a physical or mobile token if the company profile has access to high-risk services.

1. From the Associated Connect portal, select your name in the upper right-hand corner and then select **Company Admin**.



2. The **Company Admin** screen will be displayed. Select the User Name you'd like to assign a token to.

Company Admin			
▼ Manage Users			
User Name	User ID	User Status	Security Admin
AB Training	ABTraining	Lockout - Inactive	True
April Spring	AprilSpring	Lockout - Inactive	True
August Summer	AugustSummer	Lockout - Inactive	True

3. Select the **MFA Token** link noted under the Manage User Profile Information section.

AssociatedCONNECT®

Last sign in: February 22, 2019 at 10:43 a.m.

User Preferences

▼ Manage User Profile Information

Display Name:	ABCClient user2	
Last sign in:	2/25/2019 10:49:21 AM	Usage Report
Email:	associatedbank.com	Change Email
Password Last Changed:	1/22/2019 11:00:40 AM	
User Status:	Active	Reactivate Delete
Company Admin:	True	MFA Token

▼ Manage User Services

Manage Services [Edit](#)

▼ Manage User Accounts

Account Number	Account Type	Account Nickname	
	Checking	account 1	Remove
	Checking	account 2	Remove
	Checking	account 3	Remove

[Add Account](#)

4. The **MFA – User Setup** screen will display. Select the type of token to be assigned to the user, either a **Physical Token** or a **Mobile Token**.

MFA - User Setup

Green, Ann

Client Id AnnGreen

-- Select One --

Physical Token

Mobile Token

Physical Token Code #

[De-Register](#) [Register](#)

Note: For physical tokens only, enter the **Token Code** serial number shown on the bottom of the physical token device to be assigned to the user. The number will be formatted as “99-9999999-9” and can be found beneath the bar code. Don’t include the dashes when registering your physical token.

5. Select **Register**.

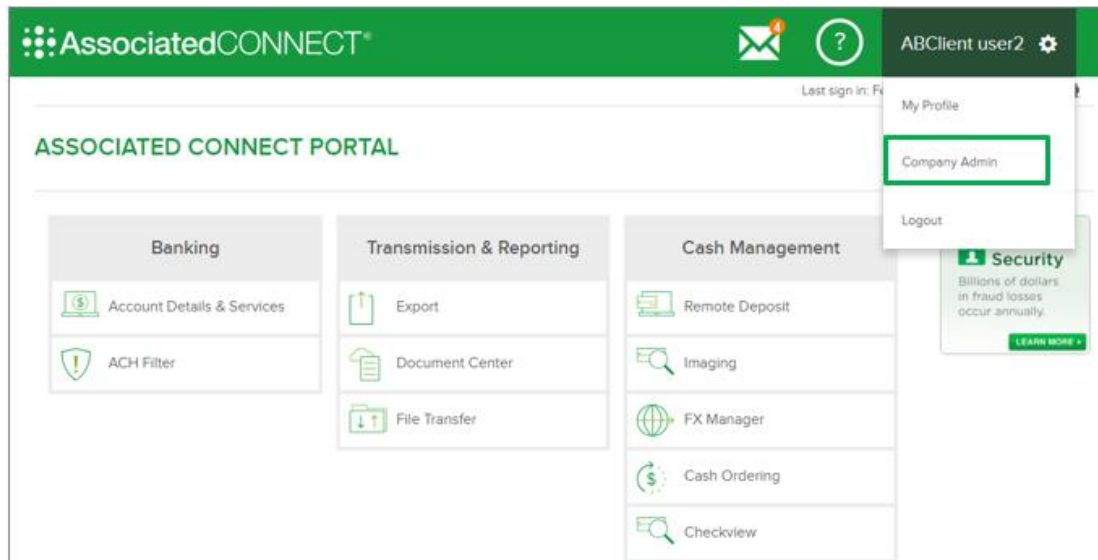
Note: If a user already has a token registered in the system, you must de-register that token before registering a new token or switching to a different token type. Directions on how to de-register a token can be found in the de-registering and un-registering tokens section of this guide.

6. A message indicating a successful registration should be displayed.

De-Registering and un-assigning Tokens (Company Administrator)

In the event that users require replacement tokens, change roles or leave the organization, Company Administrators will need to de-register their tokens.

1. From the Associated Connect portal, select your name in the upper right-hand corner and then select **Company Admin**.



2. The **Company Admin** screen will be displayed. Select the User Name you'd like to de-register a token for.

Company Admin			
▼ Manage Users			
User Name	User ID	User Status	Security Admin
AB Training	ABTraining	Lockout - Inactive	True
April Spring	AprilSpring	Lockout - Inactive	True
August Summer	AugustSummer	Lockout - Inactive	True

3. Select the **MFA Token** link under Manage User Profile Information.

AssociatedCONNECT®

Last sign in: February 22, 2019 at 10:43 a.m.

User Preferences

▼ Manage User Profile Information

Display Name:	ABClient user2	
Last sign in:	2/25/2019 10:49:21 AM	Usage Report
Email:	associatedbank.com	Change Email
Password Last Changed:	1/22/2019 11:00:40 AM	
User Status:	Active	Deactivate Delete
Company Admin:	True	MFA Token

▼ Manage User Services

Manage Services [Edit](#)

▼ Manage User Accounts

Account Number	Account Type	Account Nickname	
	Checking	account 1	Remove
	Checking	account 2	Remove
	Checking	account 3	Remove

[Add Account](#)

4. The **MFA – User Setup** screen will display. Select **De Register**.

MFA - User Setup

Green, Ann

Client Id AnnGreen

-- Select One --
Physical Token
Mobile Token

Physical Token Code #

[De-Register](#) [Register](#)

5. A message indicating a successful de-registration will be displayed.

Password Management

Associated Bank provides multi-factor authentication on accounts as an extra layer of security. However, protecting online banking passwords is also a critical component of preventing unauthorized access to your accounts. Cybercriminals use sophisticated software that can run millions of combinations of letters and symbols in a very short period of time. Establishing strong passwords and ensuring they remain secure is essential to protecting your financial assets and company information. This applies to all applications you may use, not just your bank accounts. Key recommendations for password security include:

- Make your passwords strong with at least 12 characters including capital letters, numbers and symbols. Alternatively, use a passphrase as they are harder for hackers to crack.
- Don't use the same password in multiple applications; use unique strong passwords and passphrases on each website or application.
- Never share your passwords with anyone.
- Change your passwords regularly.
- Don't fall for phishing attacks. Be very careful before clicking a link (even if it appears to be from a legitimate site) asking you to sign in, change your password or provide any other personal information. It could be a phishing scam where the information you enter goes to a hacker.
- Company Administrators should evaluate password lengths and composition requirements, incorrect sign in lockouts, password expiration, repeat password usage and encryption requirements.

Associated Connect Password FAQ

Does my sign in ID expire if I have not signed into Associated Connect for a while?

Yes, after 180 days of inactivity you'll receive an email alerting you that your ID will be disabled after 365 consecutive days of inactivity. Both physical and mobile tokens will also deactivate if not used within 720 days of inactivity. To enable your ID and/or reactivate your token, call our Customer Care team at 800-728-3501.

Will I get a reminder from Associated Bank that my sign in ID is about to be disabled?

Yes, you'll receive an email 10 days prior to the expiration of your sign-in ID, alerting you to sign in to Associated Connect to prevent your sign-in ID from being disabled.

How do I unlock my password if I have had too many failed sign-in attempts?

If you've locked yourself out of Associated Connect, please contact your company administrator to have your password unlocked.

Contact information

If you have any further questions regarding the Associated Connect multi-factor authentication or password management, please call our Customer Care team at 800-728-3501.