# Associated Connect®

Multi-Factor Authentication and Password Management Guide


# Table of Contents

# Portal Access

The Associated Connect portal allows users to access all Associated Connect services through an easy-to-use single sign-in. To access the portal, sign in to Associated Connect directly from Associated Bank's website at **AssociatedBank.com/Business** or **AssociatedBank.com/Commercial**. The portal has been divided into three sections:

| Category | Icon | Definition |
|---|---|---|
| Banking |  | Account Details and Services<br>(Includes Account Balances, Account Transfers, ACH Origination, Check Inquiry, Image Search Transaction Activity, Positive Pay, Stop Payments and Wire Transfers.) |
| |  | Account Summary Page<br>(Includes Ledger Balance, Available Balance, Collected Available Balance, Float Next Business Day, Float 2+ Days and Transactions and Details for each account) |
| |  | ACH Filter |
| |  | Bill Pay |
| Cash Management |  | Lockbox |
| |  | Remote Deposit |
| |  | Checkview |
| |  | FX Manager |
| |  | Cash Ordering |
| |  | Trade Services |
| Transmission and Reporting |  | Export |
| |  | Document Center |
| |  | File Transfer |

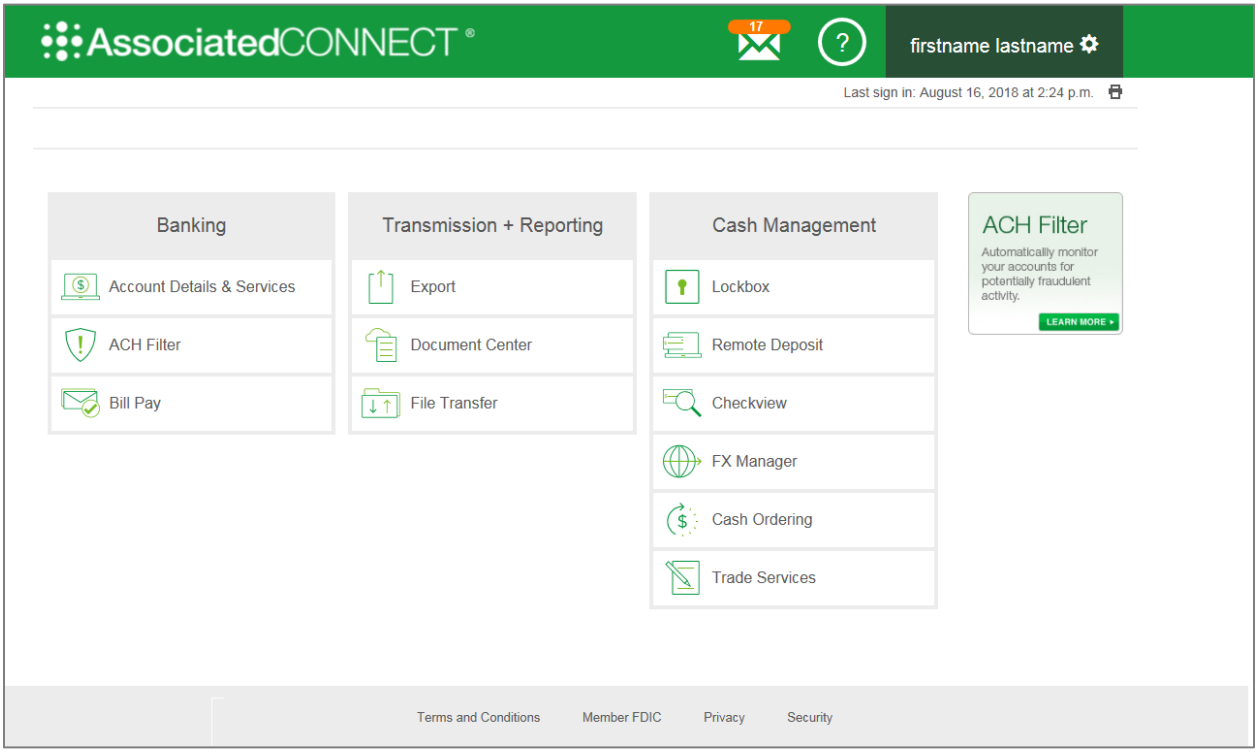
To access Associated Connect, you will be required to verify your identity through one of two methods:

1. For clients who have access to high-risk services such as Bill Pay, ACH and Wire Transfers, you will sign in with your username and password, and then will be required to verify your identity through multi-factor authentication. Associated Connect users will be required to enter a unique access code generated by either a mobile or physical token to gain access to the portal. Additional information about how to set up, use and obtain a token from Associated Bank can be found in this guide or by contacting Customer Care at 800-728-3501.

2. For clients who only have low-risk services, you will sign in with your username and password. Periodically, you will be asked a series of challenge questions to confirm your identity.

## Associated Connect Portal

The Associated Connect Portal is the first screen you will see after signing in. This provides access to all of your online banking services.



# Multi-Factor Authentication

The Associated Connect platform is a fully integrated suite of cash and treasury management solutions for business clients and offers a wide array of services including ACH Filter, 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 setup with. The type of authentication that will be required will depend on the risk level of the client's accessible services.

Multi-factor authentication is now at a company level and not a user level, meaning that if the company is setup with high risk services, no matter what service an individual user is setup for, all users of Associated Connect will have the same level of multi-factor authentication going forward.

## Knowledge Based Questions

Clients with access to low-risk services will be periodically required to answer a previously established knowledge-based question when signing in to Associated Connect.


## 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 are a company administrator, please call our Customer Care team at 800-728-3501 to request physical tokens.*

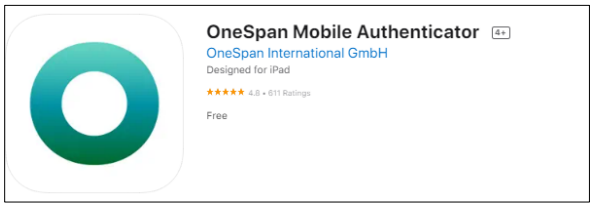
## Mobile Token Installation and Activation

Choosing to use a mobile token for authentication requires the installation and activation of the **OneSpan Mobile Authenticator®** application on your mobile device. The mobile token is supported on Apple and Android products that have:

- Android 4.1 and higher
- iOS 12.0 and higher

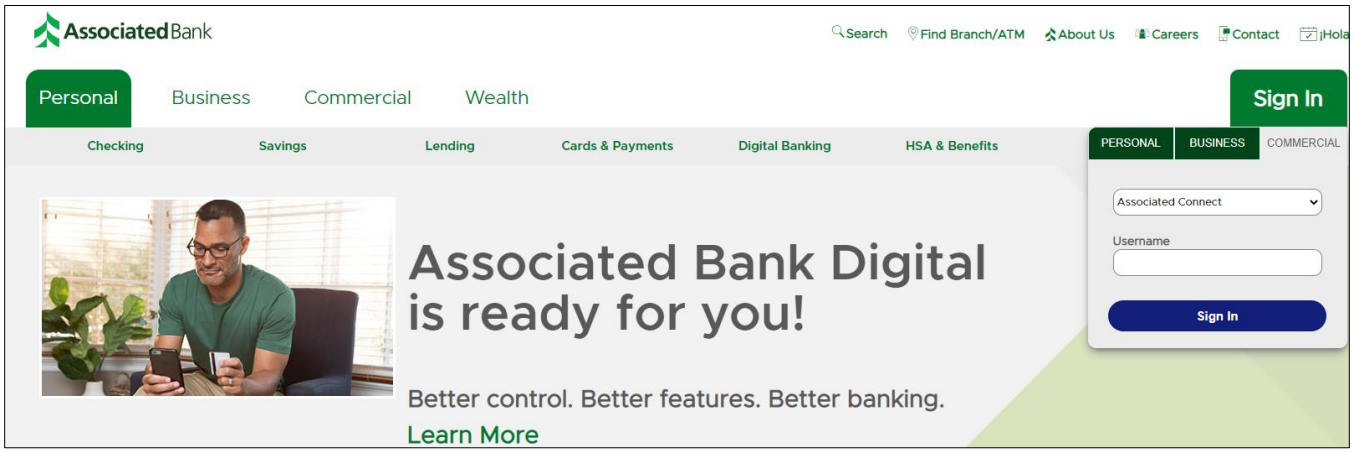
Access to both a mobile device and a computer is required for this initial setup process.

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

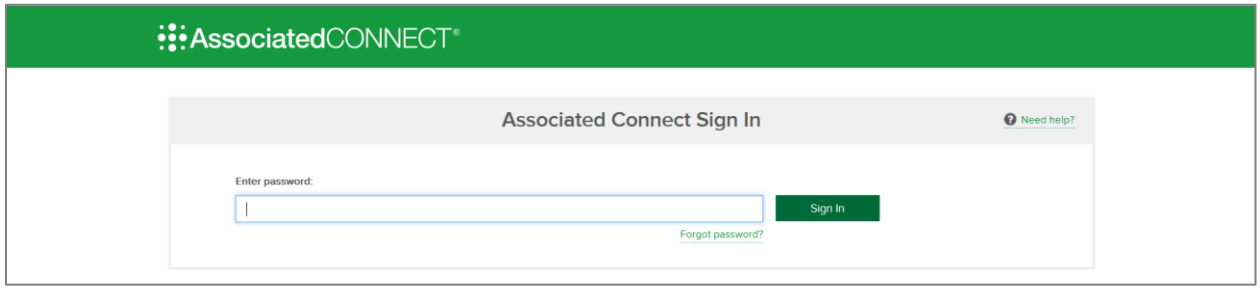



After the application installs, the following steps should be completed on a computer to activate your mobile token**:**

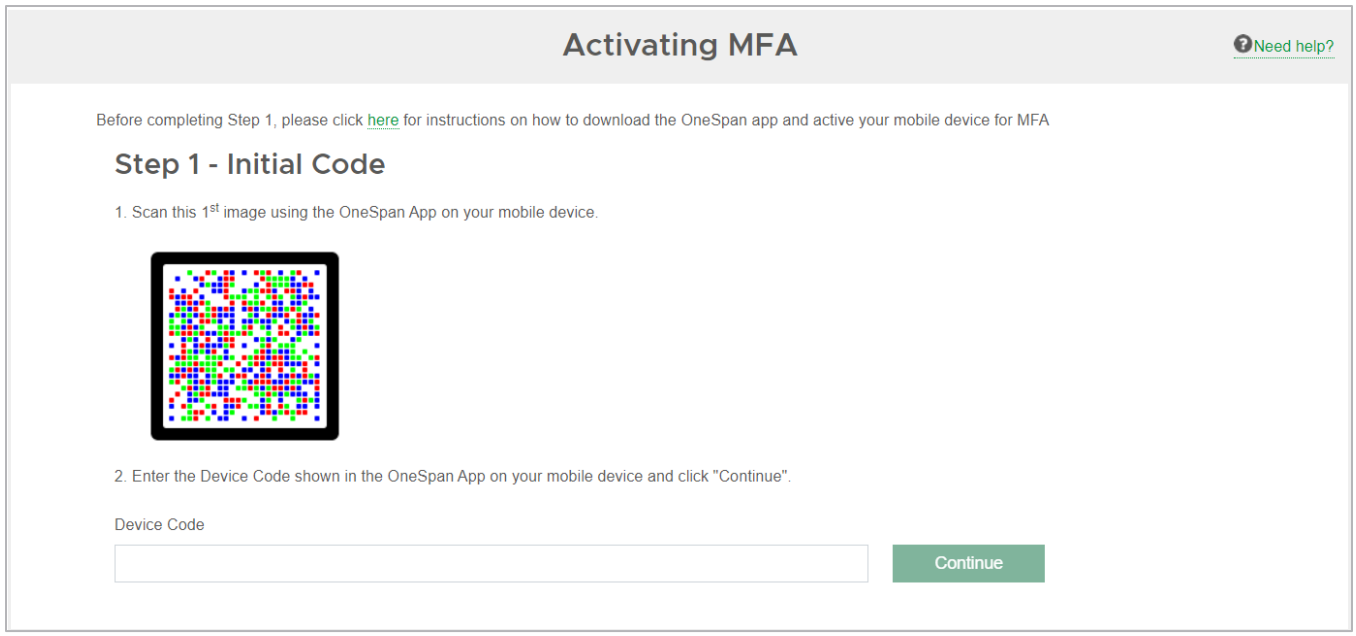
1. From the **AssociatedBank.com/Business** or **AssociatedBank.com/Commercial** website, sign in to Associated Connect (see screenshot references below).
2. Enter your Associated Connect Username and select the **Sign In** button.



3. Enter your Associated Connect password and select the **Sign In** button.




4. When activating the mobile token for the first time, the following screen will appear. Return to your mobile device.

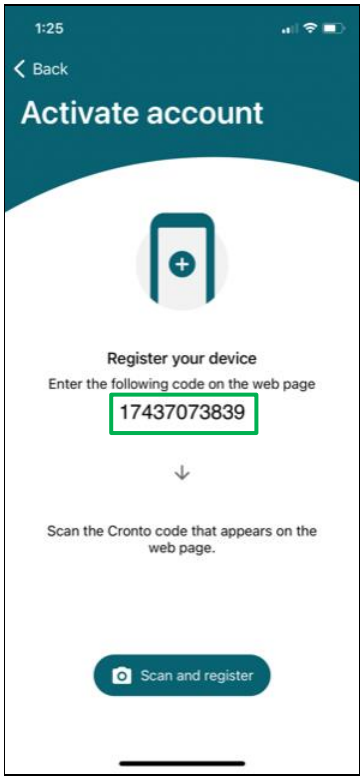


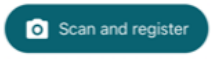

5. On your mobile device, open the OneSpan Mobile Authenticator Application.
6. On the mobile app's first screen, select **Activate Account**.
7. Allow the app to access your camera. Scan the provided image shown on your computer by selecting the camera icon on the bottom of your device's screen.

**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.*

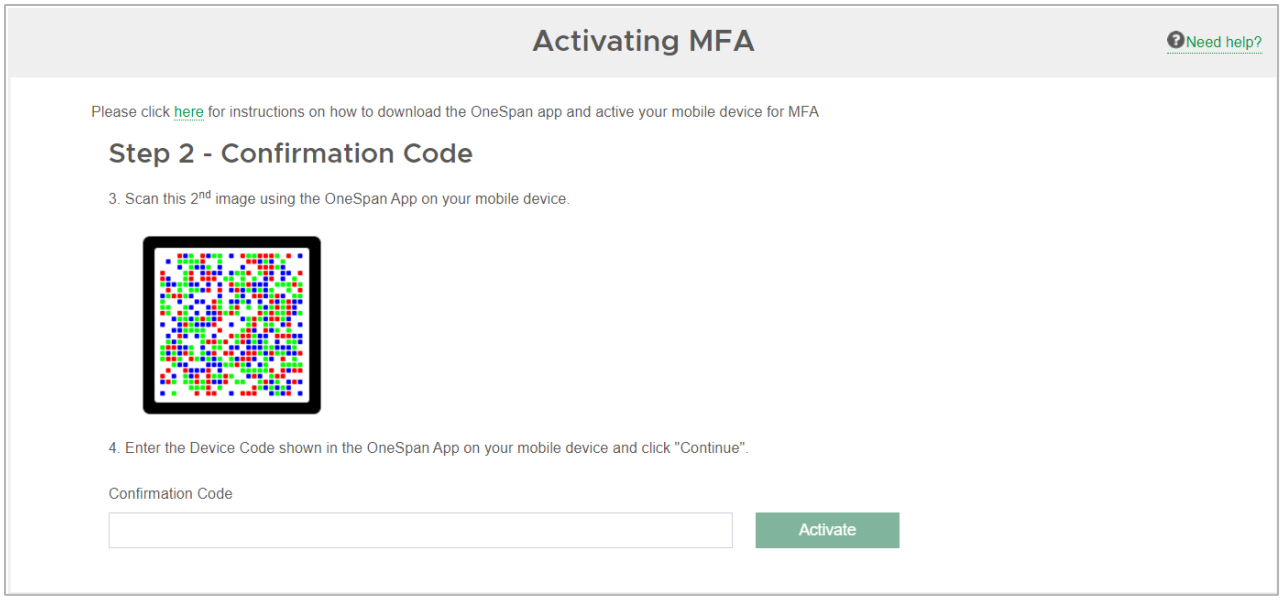
The app will then require you to **Authenticate** yourself in order to move to the next step. For Android and Apple devices, your fingerprint or facial recognition will be utilized.

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

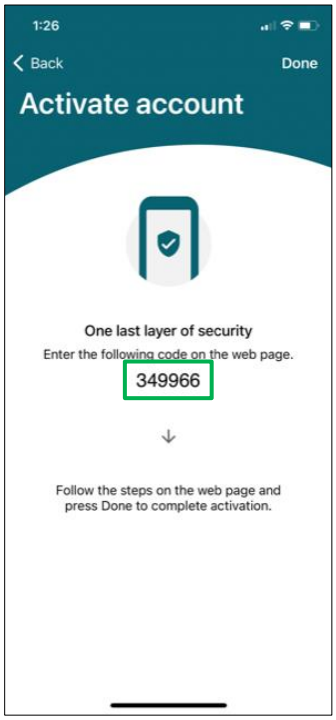



9. A second image will appear within the Associated Connect portal on your computer. Scan this with your mobile device by clicking on 

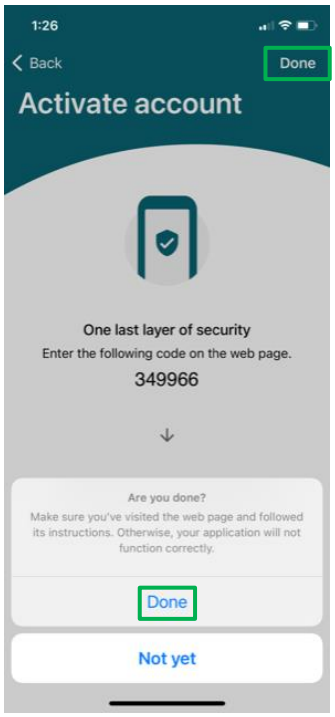
.




10. 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**.




11. Once completed, select **Done** at the top right of the mobile app. A window will pop-up at the bottom to confirm you are done with set-up. Select **Done** again.




**Note:** *If you do not select the **Done** to confirm the activation within the app, you will 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.*

12. You will now see that your mobile device has been successfully added. Select **OK** to begin your session.

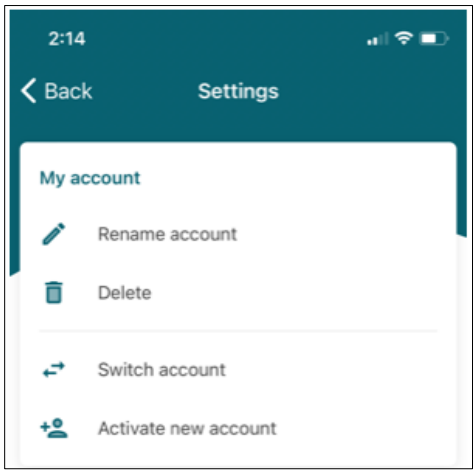

Your OneSpan Application is now activated and can be utilized on Associated Connect.

## Renaming your OneSpan Account

Once your OneSpan application is setup, the Account name can be changed.

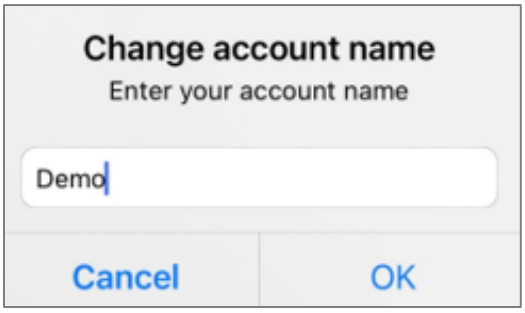
1. Open your OneSpan application.
2. Select the gear icon at the top right of the application.


3. Select **Rename account**, or **Switch account** to name a different account previously setup.




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

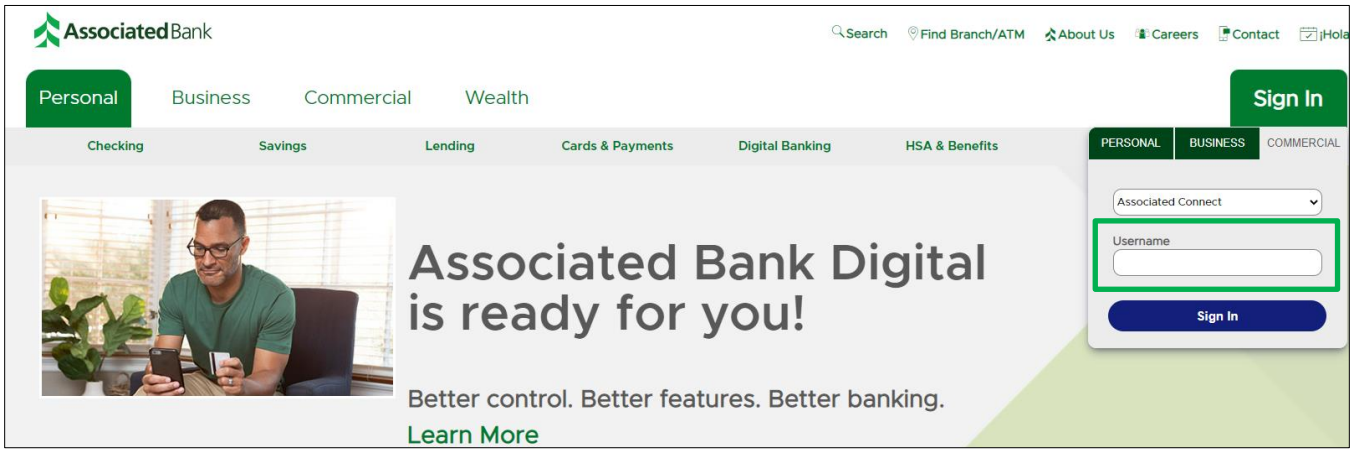
4. Enter the new name, then click OK.



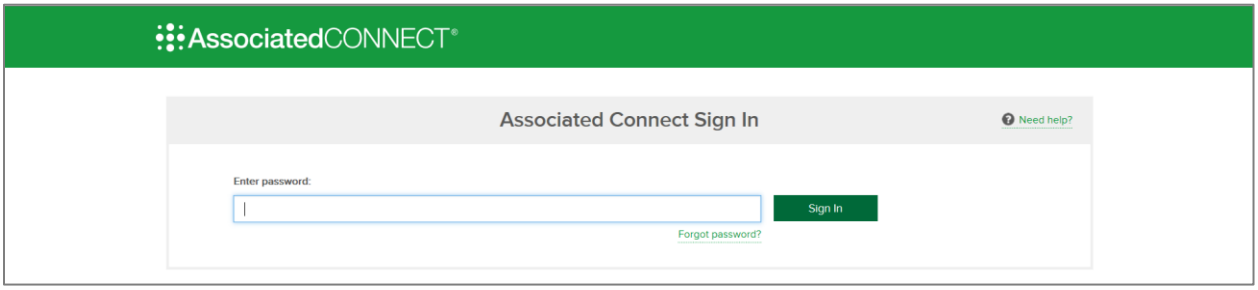

## Using your Mobile Token

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.

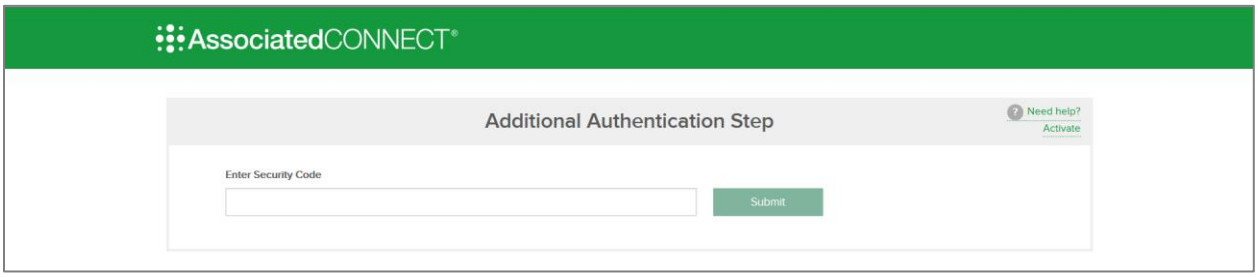
1. Enter your Associated Connect Username and select the **Sign In** button.




2. Enter your Associated Connect password and select the **Sign In** button.




3. You will be prompted to enter a security code each time you sign in. To obtain the correct security code, open OneSpan app on your mobile device and follow instructions below. You will need to enter your 6 digit OneSpan PIN, thumbprint 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 Security Code** box on the Associated Connect screen and select **Submit**.
5. Once your security code is validated, you will be able to access any service within Associated Connect.

## Physical Token Registration

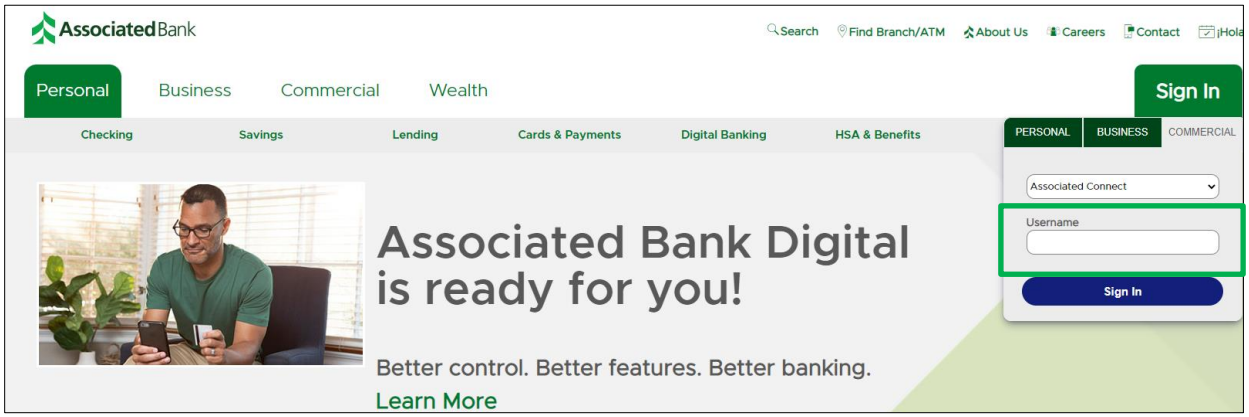
Physical Tokens will be provided upon request and will be registered and assigned by your company administrator. Once you receive your physical token from your company administrator, you will be able to use it immediately.

**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 are a company administrator, please call ourCustomer Care team at 800-728-3501 to request physical tokens.*

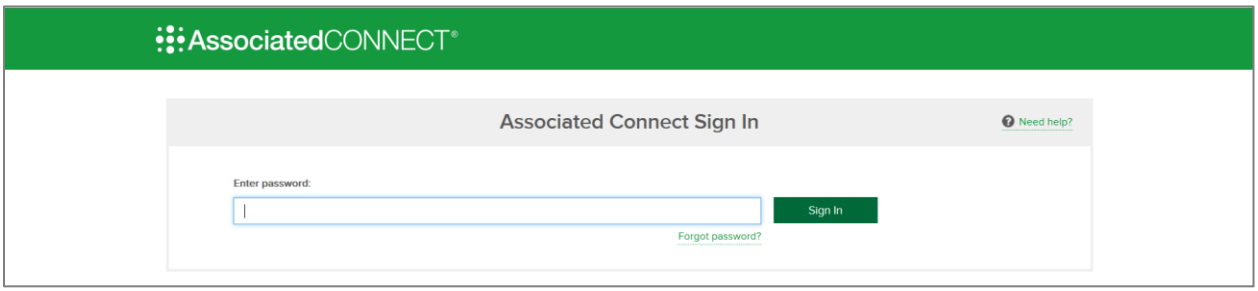
## Using your Physical Token

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.

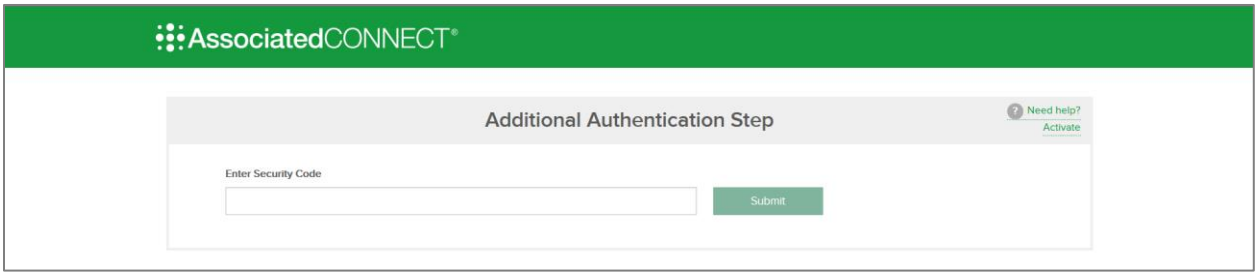
1. Enter your Associated Connect Username and select the **Sign In** button.




2. Enter your Associated Connect password and select the **Sign In** button.




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

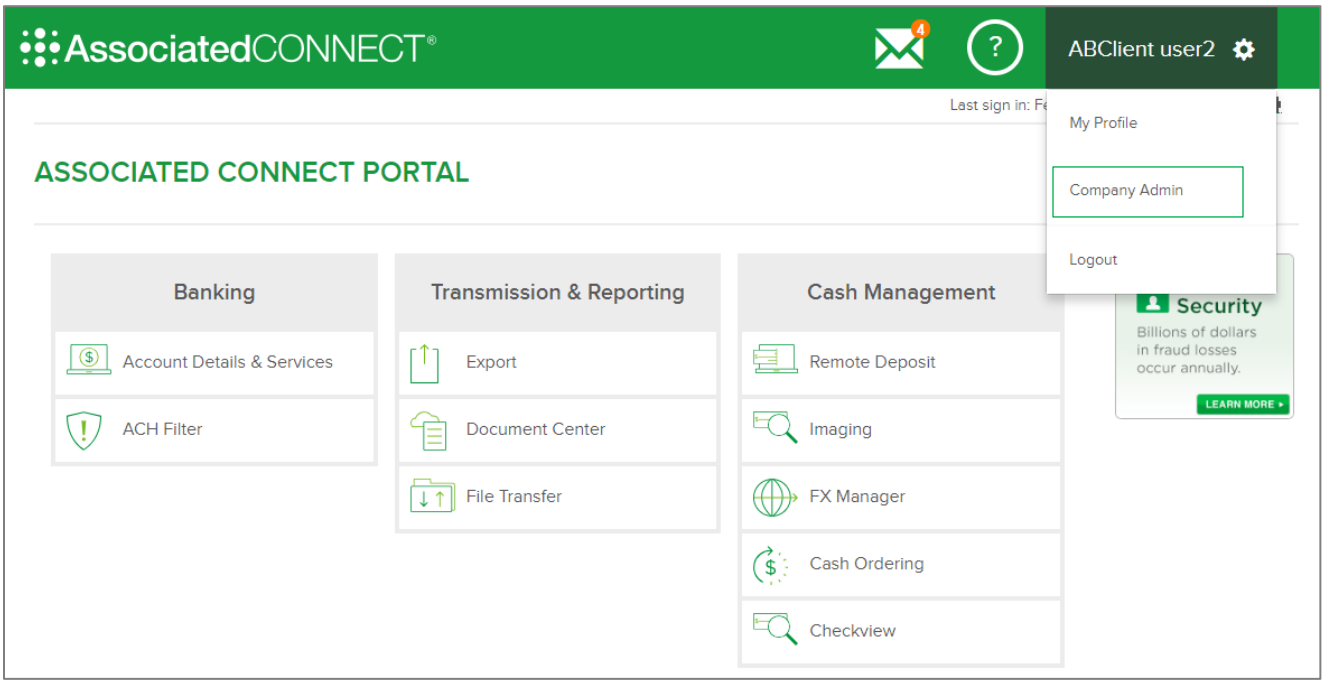



4. Press the button on your physical token and it will generate a valid security code on its screen.
5. Enter the security code into the Associated Connect **Enter Security Code** box on the Associated Connect screen and select **Submit**.
6. Once your security code is validated, you will be able to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

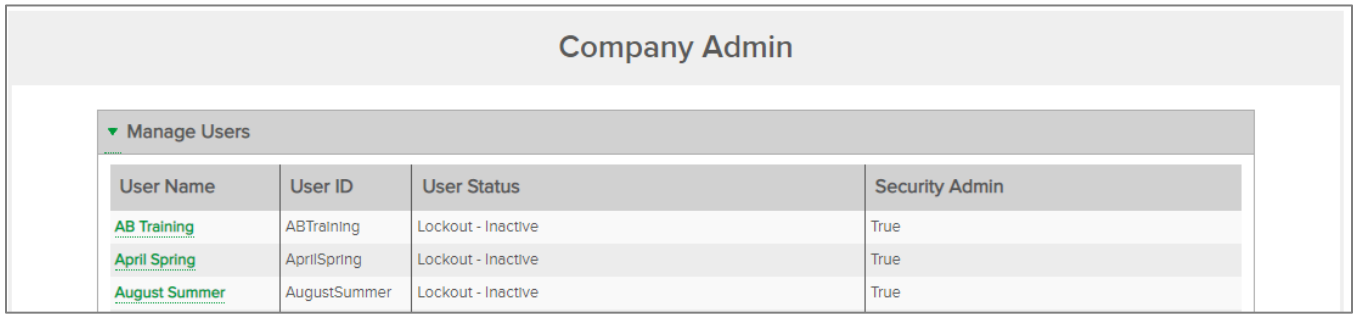
## Registering and Assigning Tokens (Company Administrator)

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.

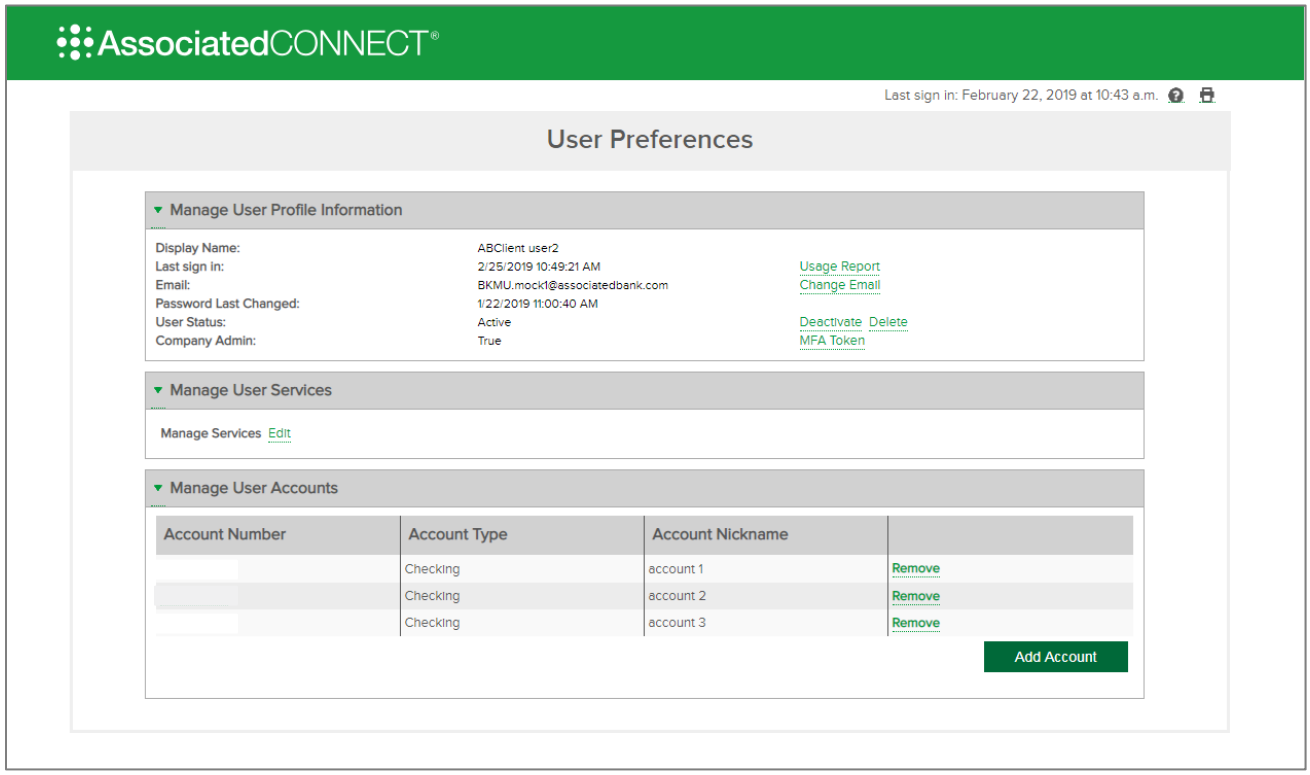
1. From the Associated Connect portal, select your name in the upper right-hand corner and then select **Company Admin.**



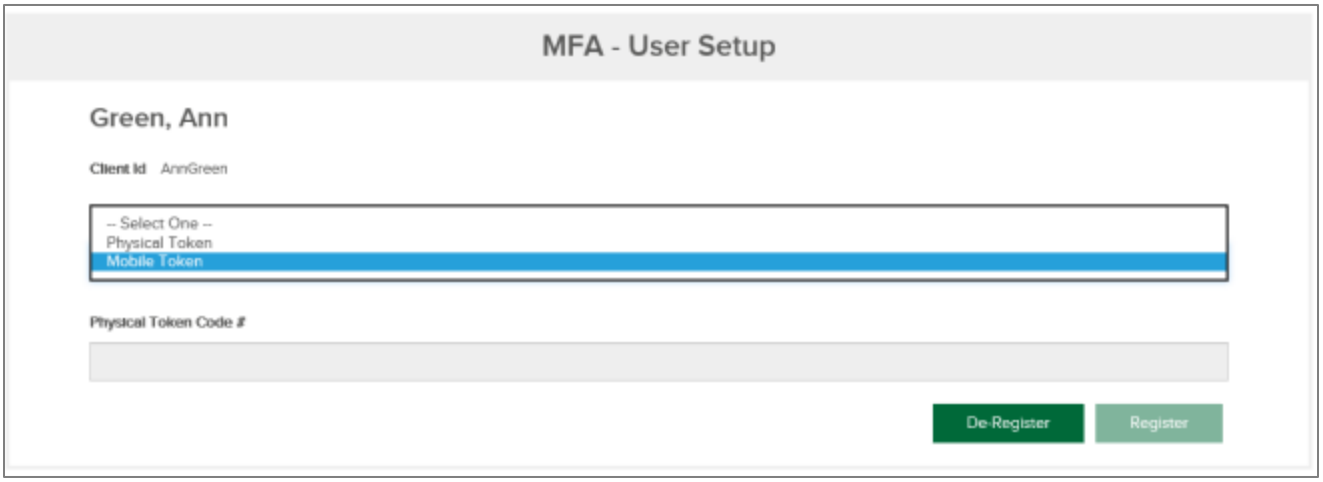

2. The **Company Admin** screen will be displayed. Select the User you would like to assign a token to.




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




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**.




**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. Do not include the dashes when registering your physical token.*

5. Select the **Register** button.

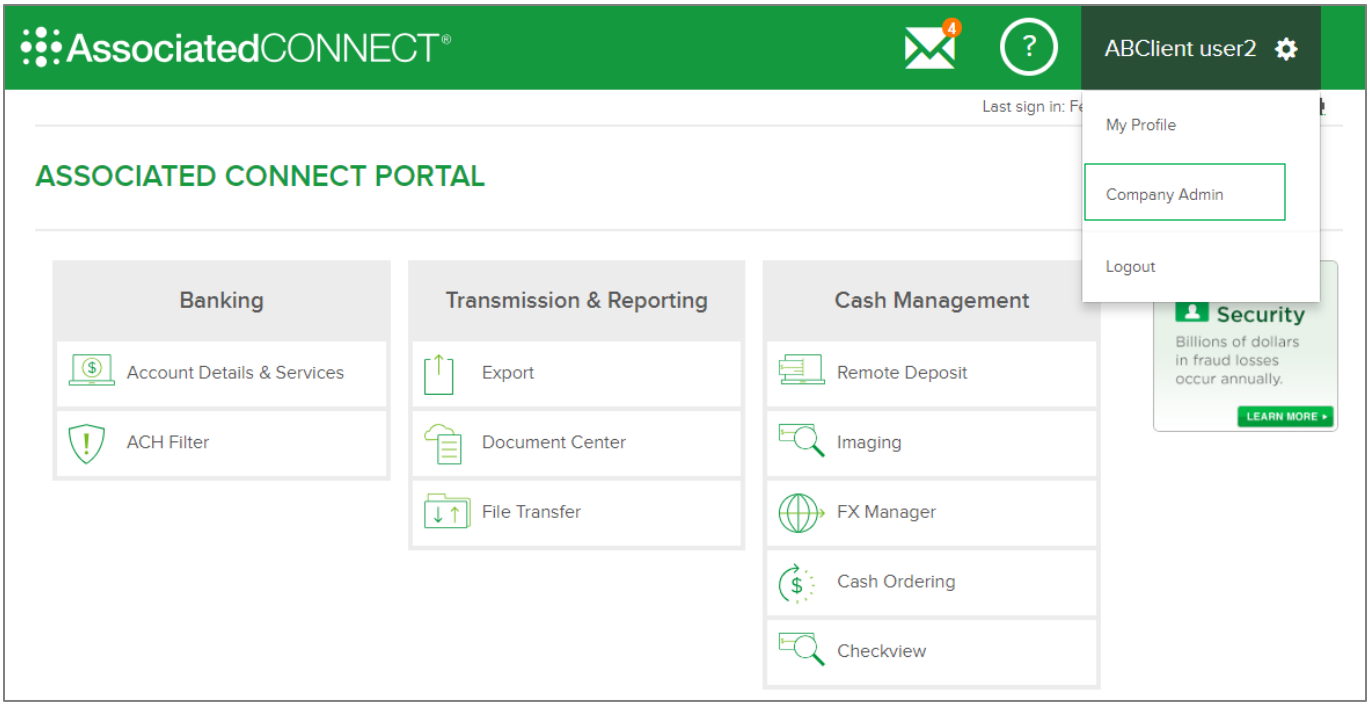
**Note:** *If a user already has a token registered in the system, you must de-register that token before registering a new token or switching to a different token type. Directions on how to de-register a token can be found in the de-registering and un-registering tokens section of this guide.*

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

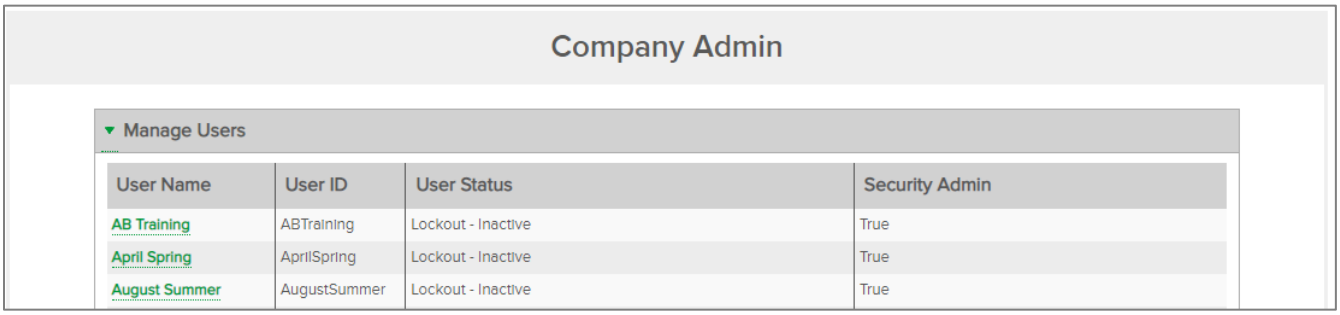
## De-Registering and un-assigning Tokens (Company Administrator)

Company administrators may need to de-register tokens in the event that users require replacement tokens, change roles or leave the organization.

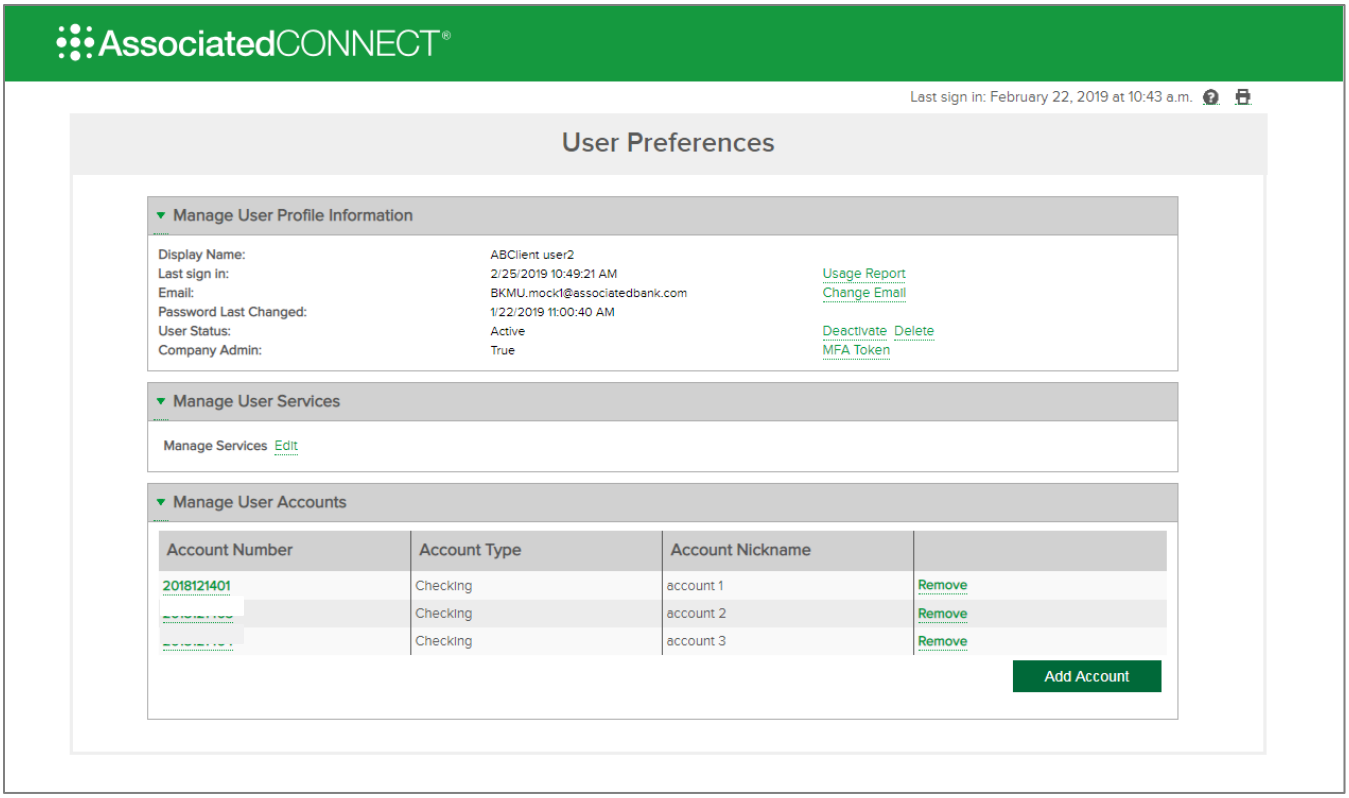
1. From the Associated Connect portal, select your name in the upper right-hand corner and then select **Company Admin.**



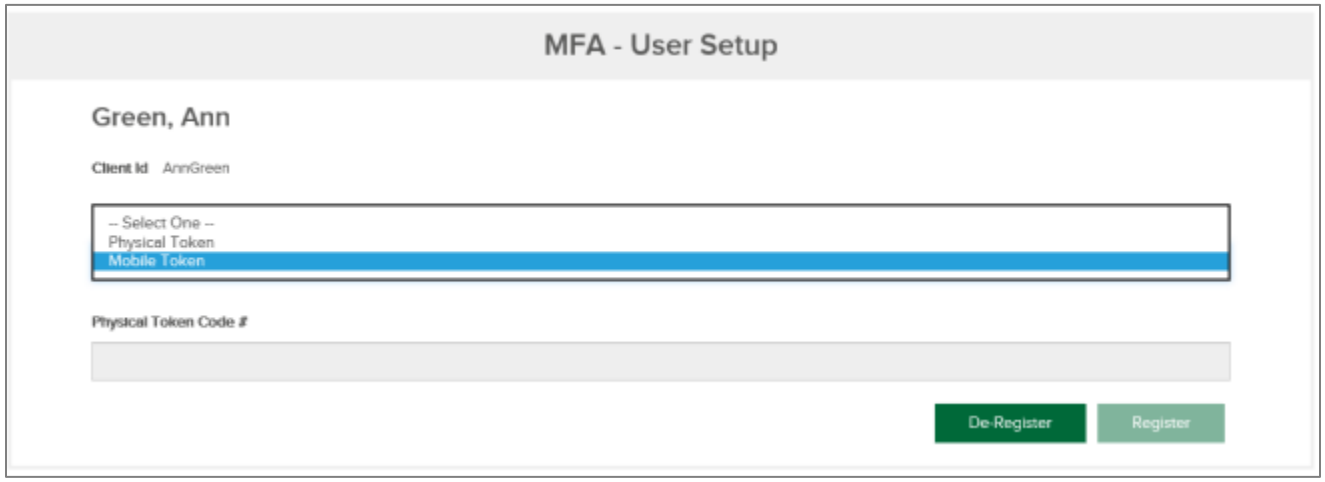

2. The **Company Admin** screen will be displayed. Select the username you would like to de-register a token for.




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




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




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.
- Do not 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 on a link (even if it appears to be from a legitimate site) asking you to log 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 log-on 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 will 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 will 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 often do I need to change my password?**
At Associated Bank, you are required to change your online password every 180 days in order to protect your accounts. If you do not sign in within a 365-day period, your password will be disabled.

**Will I get a reminder from Associated Bank that my Associated Connect password is about to expire?**
Yes, upon sign-in to Associated Connect, you will receive an alert notifying you that you password is about to expire.

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