Associated Connect® FAQs

Out-of-Band Authentication and Password Management

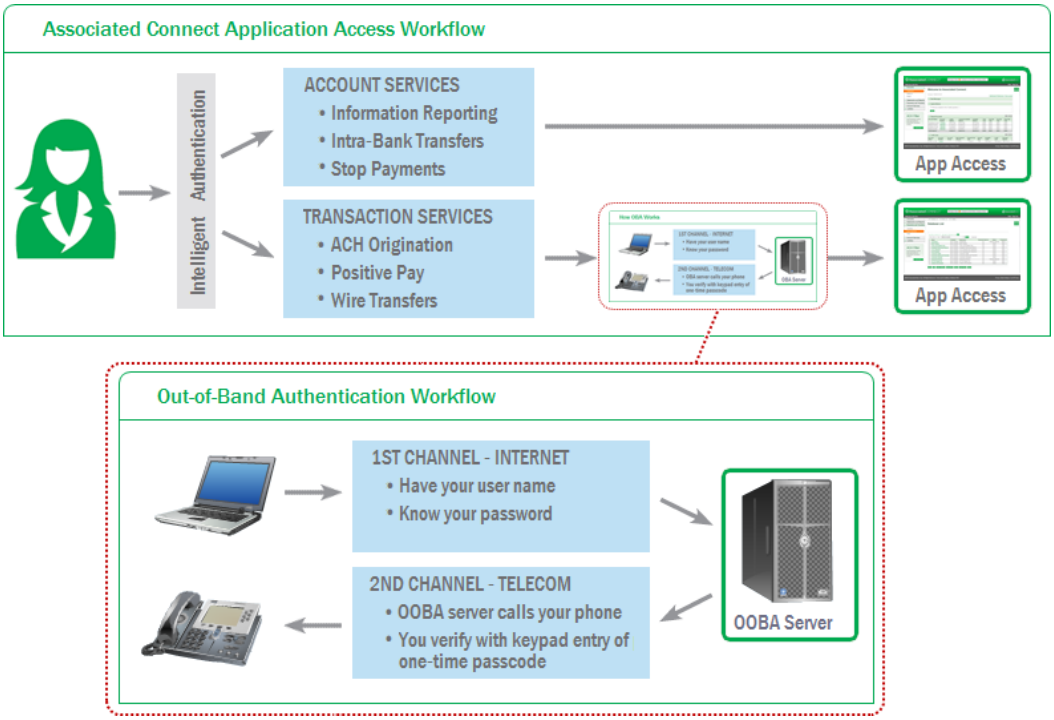
Out-of-Band Authentication

The Associated Connect electronic banking platform is a fully integrated suite of cash management solutions for business clients. Associated Connect offers a wide array of services including information reporting, funds transfer, fraud prevention and user access management. For general account services access, Associated Connect utilizes advanced multi-factor and intelligent authentication tools to verify a user's identity. For higher-risk services such as external funds transfer, fraud prevention and user access management, Associated Connect also utilizes Out-of-Band Authentication (OOBA) as an additional layer of identity verification.

OOBA Process Summary

As an added layer of protection against unauthorized access to higher-risk services, OOBA uses a second, separate communication channel to verify a user's identity. Once authorized, the OOBA verification is valid for the duration of the user session.

1. When a user signs into Associated Connect and selects an OOBA-protected service, the web page is refreshed to display a random, one-time passcode.
2. Simultaneously, Associated Connect initiates a phone call to the user's registered phone number.
3. After answering the phone, the user is prompted to enter the passcode on the phone's keypad.
4. Upon successful verification of the passcode, the user is navigated to the requested OOBA-protected service.



AssociatedBank

Member FDIC. (8/17) 10787

Frequently Asked Questions

How long does it take to access a protected service?

OOBA adds a minimal amount of time to the authentication process – just the amount of time for the phone call to connect and you to enter the one-time PIN followed by the # sign. The instant the correct information is entered, even before you disconnect the phone call, the authentication is completed and you are granted access. It is not necessary to listen to the entire telephone message; the one-time PIN followed by the # sign may be entered as soon as the OOBA call is answered.

Does OOBA work everywhere or just in the U.S.?

OOBA works with any United States or Canadian phone number. Upon request, OOBA can be made available for international phone numbers. Please contact your Commercial Deposits and Treasury Management representative or call Treasury Management Customer Care at 800-270-2707 for information on pricing and availability.

Can a user designate more than one phone to receive an OOBA call?

Yes, your company's Security Administrator can set up an unlimited number of phone numbers for each user. When you access a service protected by OOBA, you will be given a choice of which number to use for that particular OOBA call.

How are OOBA telephone numbers maintained after the initial activation?

Once OOBA has been activated, Security Administrators can add or delete telephone numbers for themselves and other users authorized to access services within Associated Connect. Just click Company Admin and select the user to make changes under the Manage User OOBA section.

Can users maintain their own OOBA telephone numbers?

No, only Security Administrators who are responsible for Associated Connect security procedures for their company can maintain the telephone numbers set up for OOBA calls. Each Security Administrator can maintain telephone numbers for themselves and other users, including other Security Administrators.

What if a user enters the one-time PIN incorrectly or presses the wrong button during the OOBA call?

Entering an incorrect passcode will result in the user not being granted access to the protected service. However, Associated Connect will present the user with a message suggesting that they retry the OOBA call or contact Treasury Management Customer Care. If another OOBA call is not attempted, the user will not be logged out of Associated Connect and will still have access to services not protected by OOBA.

What if a user can't answer the OOBA call?

Not answering an OOBA call has the same effect as entering a wrong passcode. Associated Connect will prompt the user to retry the OOBA call or contact Treasury Management Customer Care. If another OOBA call is not attempted, the user will not be logged out of Associated Connect and will still have access to services not protected by OOBA.

What if I receive an OOBA call when I'm not trying to access a protected service?
This would only occur if someone else has logged into Associated Connect with your ID and password, and then tried to access an OOBA-protected service. In such a situation, enter ***6** on your telephone key pad to instantly lock out your individual access to Associated Connect. After locking out your user access, call Treasury Management Customer Care immediately and report the incident.

Password Management

Cyber-crime research indicates that account takeover is among the top 10 banking fraud types. Online banking password protection is a crucial element in preventing unauthorized access to your bank accounts. Without proper control, content and structure, a password can serve as a gateway to data breaches affecting your company's information and financial assets.

Key Aspects of Password Security:

- Always keep passwords confidential
- Password length & complexity are important. An 8-character password using letters, numbers or symbols is recommended
- Company Administrators should evaluate password lengths and composition requirements, incorrect log-on lockout, password expiration, repeat password usage, and encryption requirements
- Regularly change your password

Frequently Asked Questions

Does my log in ID expire if I have not logged into Associated Connect for a while?
Yes, after 90 days of inactivity you will receive an email alerting you that your ID will be disabled after 180 consecutive days of inactivity. To enable your ID, call our Treasury Management Customer Care team at 800-270-2707, Option 2.

Will I get a reminder from Associated Bank that my log in ID is about to be disabled?
Yes, you will receive an email 10 days prior to your log in ID expiring, alerting you to log in to Associated Connect or your log in ID will be disabled.

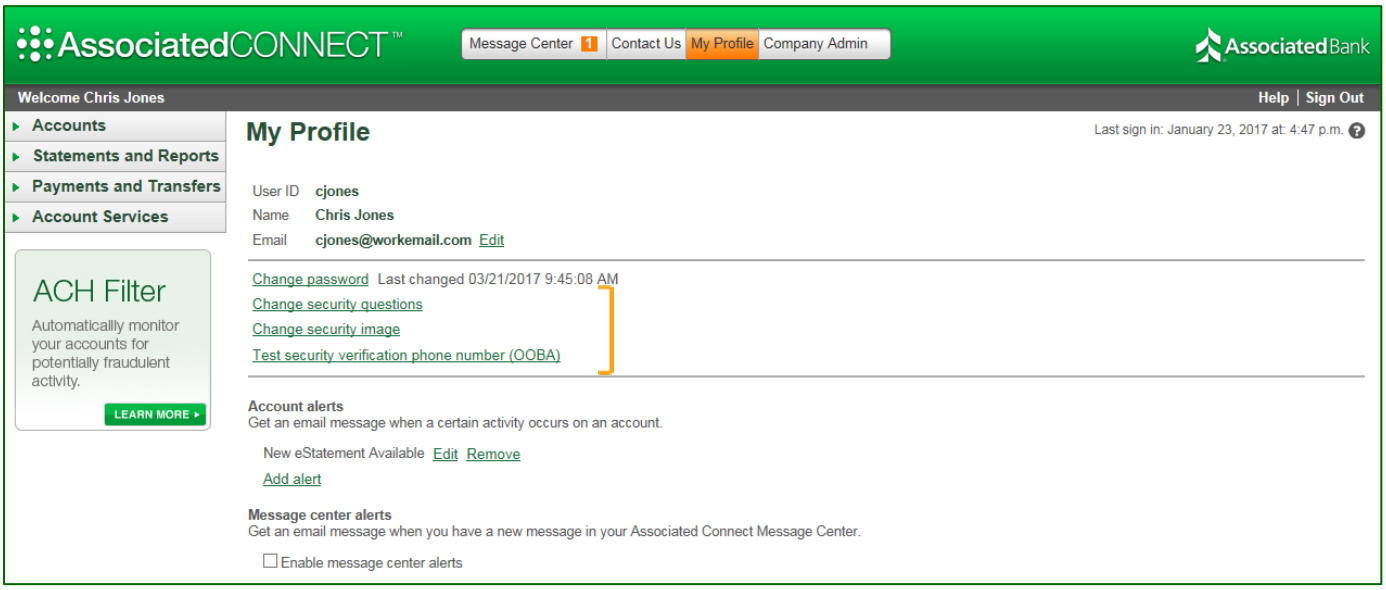
How often do I need to change my password?
At Associated Bank we require you to change your online password every 90 days in order to protect your accounts and help prevent you from becoming a statistic. If you do not sign in within a 180-day period, your password will be disabled.

Will I get a reminder from Associated Bank that my Associated Connect password is about to expire?

Yes, upon login to Associated Connect prior to password expiration, you will receive an alert notifying you that you password is about to expire.

Can I change my own password or security questions/image?

When logged into your Associated Connect, go to "My Profile". Here you will be able to change your password as well as edit your security questions, image and test your OOBA phone number.

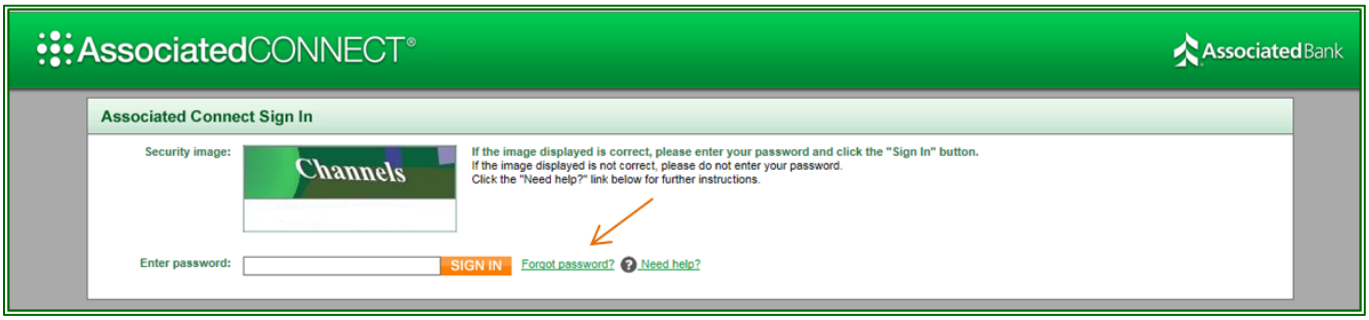


How do I unlock my password if I have had too many failed log in attempts?

If you have locked yourself out of the system, call our Treasury Management Customer Care team at 800-270-2707, Option 2, to have your User ID unlocked.

What happens if I forgot my password?

Log in using your User ID and click "Forgot Password?"



You will be prompted to provide your User ID, answer a security question, and successfully complete an OOBA confirmation. After your identity has been validated, you will be prompted to enter a temporary password. Once logged in you will be required to change your password again for security purposes.

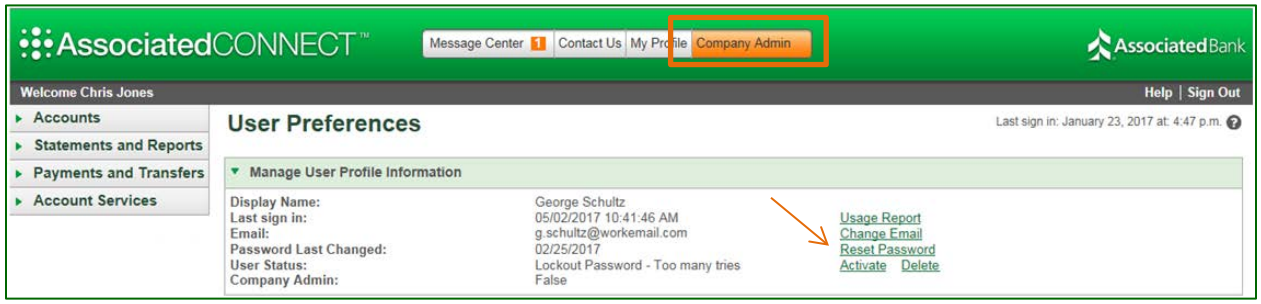
Password Resets and User Activation Reference

The chart below provides a quick reference to the required actions the Security Administrator must perform for each lockout scenario.

LOCK OUT REASON	RESET PASSWORD	REACTIVATE USER
Too Many Password Attempts	✔	✔
Inactive	✔	✔
OOBA Failure		✔

Can the Associated Connect Security Administrator reset passwords?

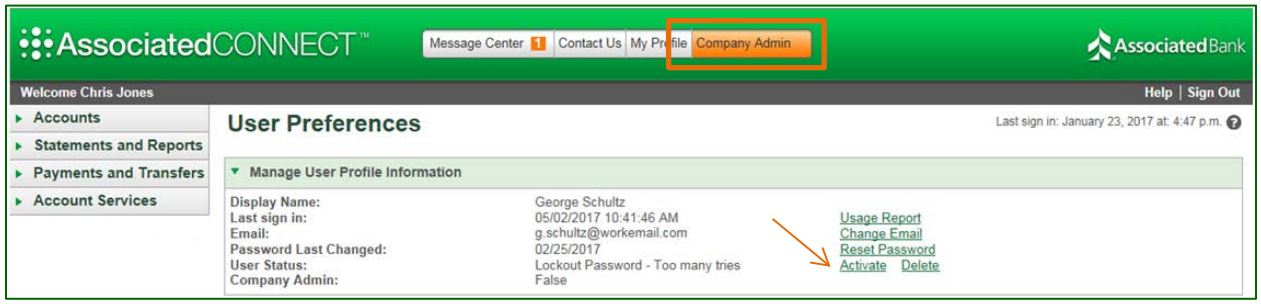
Yes, when a Security Administrator is logged in, go to "Company Admin".



Select the user requiring a password reset and click the "Reset Password" link. The Company Administrator will be able to enter a temporary password for the user.

Can the Associated Connect Security Administrator unlock users?

Yes, when a Security Administrator is logged in, go to "Company Admin". Select the user requiring a password reset or needing to be enabled and click "Activate". The Company Administrator will be able to enter a temporary password for the user.



Contact Information

If you have any further questions regarding the Associated Connect Out-of-Band Authentication service or Password Management, please call our Treasury Management Customer Care team at 800-270-2707, Option 2.