Exchange
Secure & OTP FAQs

Q: What is Exchange Secure?

A: Exchange Secure is BOK Financial's approach to authenticating users when using online services. While passwords serve as adequate protection in a variety of network scenarios, organizations and consumers now need more than passwords alone to protect against online fraud and identity theft.

Exchange Secure, also known as strong authentication, requires at least two forms of identity authentication for accessing Exchange or a particular service within the platform. This means, combining something a user "knows," such as a password, with something a user "has," such as a challenge code from a token or one-time passcode, to ensure secure online authentication.

Strong authentication is any combination of the above mentioned factors and perhaps other ones, also called two or three-factor authentication. By combining several independent authentication factors, much stronger security against intruding attacks is assured. For example, one factor may be something that the user knows such as a password or PIN, while the second factor may be something the user has, such as a token, or a smart card. If one of the factors is lost or stolen, the user's identity cannot be compromised.

Q: Why is there a need for strong authentication?

A: More and more businesses are utilizing the speed and economic advantages of the Internet to transact and exchange sensitive or confidential information. While expanding their e-business environments to employees, customers, and partners, businesses become exposed and vulnerable to many risks including unauthorized access, fraud, IP theft, information leaks, and malicious harm. If users' identities are not properly authenticated, an organization has no assurance that access to resources and services is properly controlled. Businesses with Internet presence can have a potentially large community of customers and partners in various diverse geographic locations, connected through only the browser. Therefore, strong authentication is of critical importance to positively identify such participants.

Q: What types of strong authentication exist today?

A: BOK Finanical has investigated many forms of strong authentication. These include hardware and software tokens, smart cards, SMS-based systems and biometrics. All of these systems offer strong authentication capabilities and are deployed within various organizations and vertical market segments around the world.

All financial institutions are required to use some form of Strong Authentication. We continue to evaluate solutions.

Q: As an Exchange company administrator or user, what type of strong authentication will be available to me?

A:
- All Exchange users, including company administrators, will use an SMS text and Voice.
- One-Time Passcode (OTP) solution that we refer to simply as One-Time Passcode.

Q: As a company administrator, how do I entitle One-Time Passcode functionality to new users?

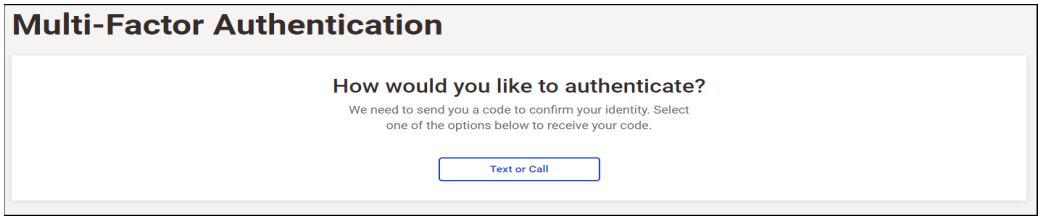
A: The bank's data security department will be automatically notified when a new user is added to the Exchange application and will automatically set the user to One-Time Passcode.

BOK FINANCIAL

Q: How does One-Time Passcode work?

A:

Before being granted access to Exchange or a challanged service, the user will be prompted to request a One-Time Passcode (OTP) be delivered to the user's pre-defined delivery channel for that session, as illustrated below. The user will then enter the code in the requested field to gain access to the service. Because the authentication code is delivered outside of the application it is considered an "out of band" delivery.



Q: What is the benefit of using One-Time Passcode versus other forms of strong authentication?

A:

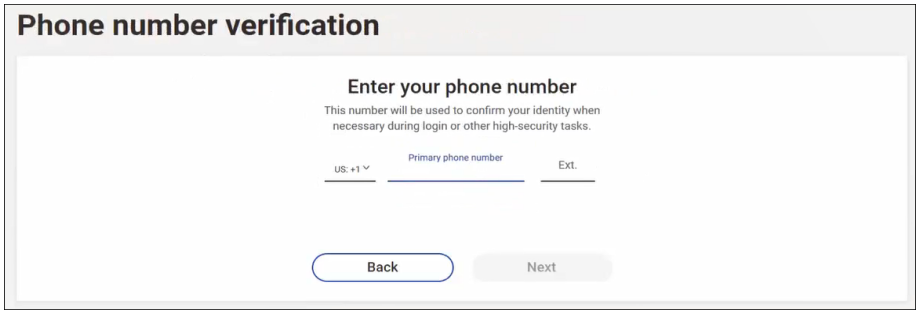
SMS and Voice One-Time Passcode (OTP):

- Allows continued access to the Exchange desktop application and mobile application without the burden of carrying an additional physical device, such as a token.
- Provides a high level of proven security against fraud.
- Is one of the more commonly used strong authentication solutions, along with tokens, being used by U.S. Banks for Cash Management web applications.

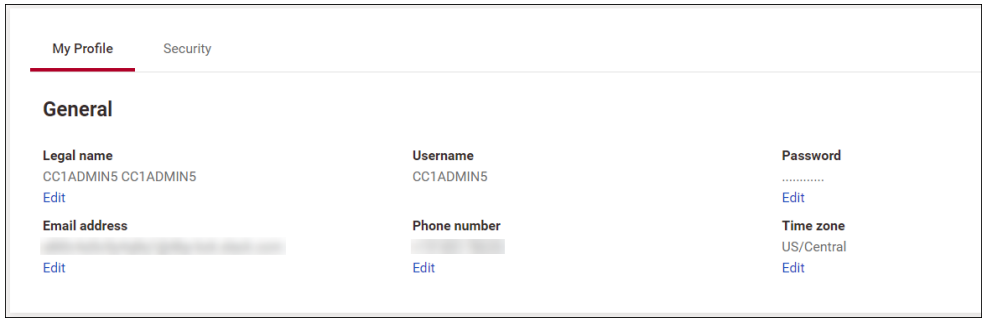
Q: How do I set up and manage contact points?

A:

Upon accessing the Exchange desktop application for the first time, all users will be prompted to set up voice/text contact point, also known as delivery channel.



After initial set up, phone number can be edited through "My Profile". Voice or Text delivery selection is made each time the challange is presented.



BOK FINANCIAL

Q: Will there be support for phone extensions or international phone numbers?

A: Domestic and International phone numbers are supported. However, phone extensions are not supported.

Q: What is a challenged service?

A: A challenged service within Exchange is a service that requires the use of One-Time Passcode before a function can be completed, including initial login.

Q: Which Exchange services will be challenged services?

A:
- Login
- Approving Wire Payments
- Approving ACH Payments
- Forgot Password
- Changes in User Profile
- Creating/editing a user
- Approving a user

Q: What is a challenge code entry window?

A: A challenge code entry window is a window that opens in the Exchange session for the user to enter information to confirm we are accepting instructions for high risk transactions from an authorized Exchange user.

Q: What do I type in the challenge entry window?

A: Enter the One-Time Passcode received via text or voice.

Q: What happens if I enter the value incorrectly in the Exchange challenge entry window? Will I be locked out of using Exchange after a certain number of attempts?

A: Entering an invalid code in the challenge entry window will not lock the user out of Exchange unless the user has exceeded the number of attempts allowed while trying to access the application. However, if this occurs while in the application when accessing any of the above mentioned high risk services, you will not be able to access it until the One-Time Passcode is entered correctly.

Q: How many times can I mistype my One-Time Passcode before I am locked out?

A: Currently, users may take three (3) attempts to enter a valid passcode before a new One-Time Passcode must be requested and utilized.

Q: How long do I need to wait until challenged services are accessible?

A: It will take up to two business days to complete the OTP set up process. Users will be prompted to set up contact points upon login once the set up process is complete. Users may utilize non-challenged services at any time, but will not be able to access challenged services until the OTP set up process is complete.

Q: What do I do if I need support for the One-Time Passcode service?

A: Please contact your Treasury Client Services Professional for assistance.

BOK FINANCIAL