

Quick Reference Guide

2FA at Login

JHA Treasury Management™

Last Updated: September 22, 2021

2FA at Login

Overview: Two-Factor Authentication (2FA) is a method that relies on a user providing their login credentials in addition to their password, as well as a second factor, which is usually a secure token or a one-time passcode verification. Integration of 2FA prevents Man in the Middle (MITM) attacks such as Sniffing Attackers, Packet Injection and Session Hacking.

This enhancement will provide Financial Institutions with the ability to activate 2FA at login using the desktop application. Users will be prompted with authentication via Secure Token or Out of Band – based on the selected authentication method setting for the Treasury Management customer.

With this enhancement there will be no changes to the mobile user’s experience. Mobile users will continue to be prompted to input their user credentials or utilize biometrics, and then they will be prompted with their established security questions.

Important: For QuickBooks Express Web Connect, if 2FA at Login is enabled for your customer and they utilize QuickBooks via Express Web Connect, an error message will be presented blocking their ability to log in. The reason is when QuickBooks Online attempts to establish a connection, the interface to bypass tokens during the login process is not available like it is for Web Connect or Direct Connect.

Benefits for the Banks?

- Enhancement activation control with a new feature configuration

Benefits for Customers?

- Enhanced security

2FA at Login

Back Office - Configuration - Company User Settings & Company Details

The screenshot displays the 'Company User Settings' interface. The top navigation bar includes 'Company', 'User', 'Configuration', and 'Reports'. The left sidebar lists 'Admin Settings', 'Account Settings', 'Authentication Settings', and 'Login Settings'. The main content area is titled 'Authentication Settings' and includes the following fields:

- Out-of-Band**: Number of Allowed Failed Attempts – Challenge Point (3)
- Secure Token**: ENABLED (marked with a red '1')
- Number of Allowed Failed Attempts – Challenge Point (3)
- Enable 2FA at Login**: ENABLED (marked with a red '1')

Buttons for 'Save' and 'Cancel' are located at the bottom left. A circular callout highlights the 'Company Details' section, which includes:

- Authentication Status**: ACTIVE (marked with a red '2')
- Authentication Method**: Out-of-Band (radio button), Secure Token (radio button, selected)
- Authentication Profile**: Default (with an edit icon)

1. Authentication Settings - Enable 2FA at Login

This new configuration will default to inactive

Until this configuration is activated, users will not be prompted to authenticate with their Secure Token or their One Time Passcode at login

2. Company Authentication Settings - Authentication Status

Authentication Status must be set to Active

Note: Both Enable 2FA at Login and Authentication Status must be active in order for 2FA at Login to function within the desktop application.

2FA at Login

Channel - User Login - Secure Token

Secure Token Registration ●—1

If you have received or installed your Secure Token/Credential, register it by entering the information requested below. If you do not wish to register your Secure Token/Credential at this time, or if you have not yet received or installed it, select Remind me later.

1. If you have a key fob, enter the Serial Number, which is located on the back of the fob after the letters "S/N". If you are using a virtual token, enter the Credential ID, which begins with 4 letters.
2. Enter your Credential/Token Code. This is the random, six-digit code that is displayed on your credential.
3. Create a 4-digit PIN and enter it twice to confirm it. You will use this PIN in conjunction with the random code generated by your Secure Token/Credential.

Serial Number / Credential ID:

Token / Credential Code:

PIN:

Confirm PIN:

●—2

Security Questions

Question 1: Which was the first foreign country you visited?

Answer:

Question 2:

Answer:

Question 3:

Answer:

Identity Verification ✕ ●—3

We need to verify your identity for the security of the account. Please enter your security code followed by your 4-digit PIN (no-space)

1. Registration

Users who have not previously registered will be prompted to register their secure token at login

2. Remind me later

Users have the option to select Remind me later for up to 5 days, and on the 6th day they will be required to register

Note: Customers who have already registered their secure token will not have to register again once this enhancement is implemented.

3. Authentication

After successful registration and upon a user's next login, they will be prompted to input their security code + their PIN they established at registration

Note: If the user inputs incorrect information and you would like to give them another attempt, please validate the Number of Allowed Failed Attempts within Back Office under Company User Authentication Settings. This parameter will continue to be utilized for challenge points as well. Screen capture on the previous page illustrates this setting.

2FA at Login

Channel - User Login - One Time Passcode

1—● Phone Numbers for Authentication

For additional authentication purposes, please provide phone numbers to receive text messages (SMS) and automated phone calls. You may be prompted to verify your identity by responding to a text message or automated phone call at login or when initiating transactions.

Text Message (SMS)

Get a prompt via text message and reply to verify your identity.

Add Phone Number

Automated Phone Call

Receive a prompt via automated phone call and reply to verify your identity.

Add Phone Number

You can only enter this information one time. You must contact your financial institution to change your security phone numbers.

2—● Remind Me Later

Add Phone Number

Receive a text message (SMS) and reply to verify your identity.

Phone Number: - -

Use same number for automated phone calls.

Verify Number **Cancel**

Automated Phone Call

Receive a prompt via automated phone call and reply to verify your identity.

Add Phone Number

You can only enter this information one time. You must contact your financial institution to change your security phone numbers.

3—● Identity Verification

We need to verify your identity for the security of the account please enter your One Time Password below.

Verify

1. Registration

Users who have not previously registered will be prompted to register their one-time passcode

2. Remind me later

Users have the option to select Remind me later for up to 5 days, and on the 6th day they will be required to register

Note: Customers who have already registered their one-time passcode will not have to register again once this enhancement is implemented.

3. Authentication

After successful registration and upon a user's next login, they will be prompted to input their one-time passcode received via text message or automated phone call.

Note: If the user inputs incorrect information, they will have an unlimited number of attempts to login. At this time, a configuration setting is not available.