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?

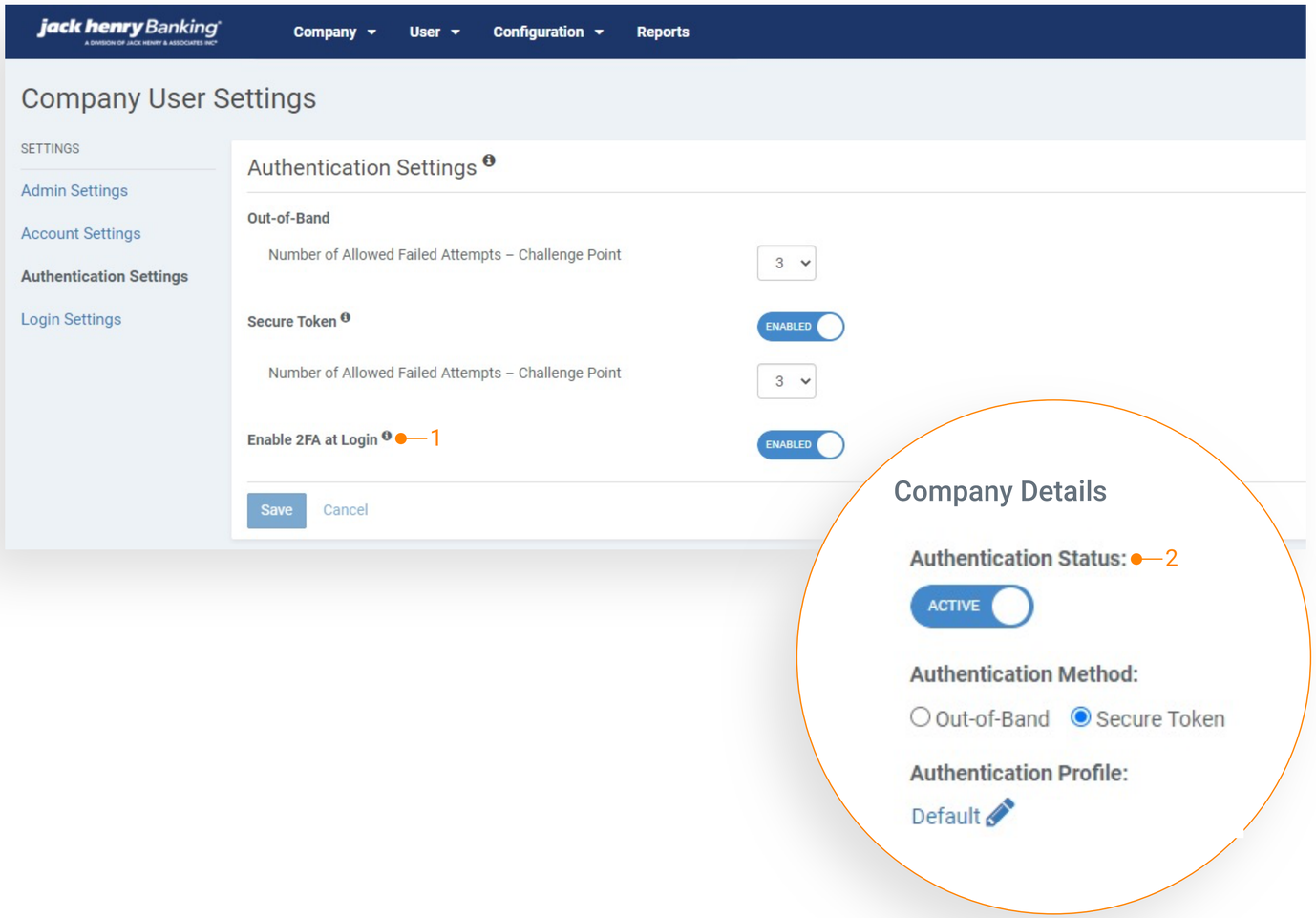
- Enhancement activation control with a new feature configuration

Benefits for Customers?

- Enhanced security

2FA at Login

Back Office - Configuration - Company User Settings & Company Details



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

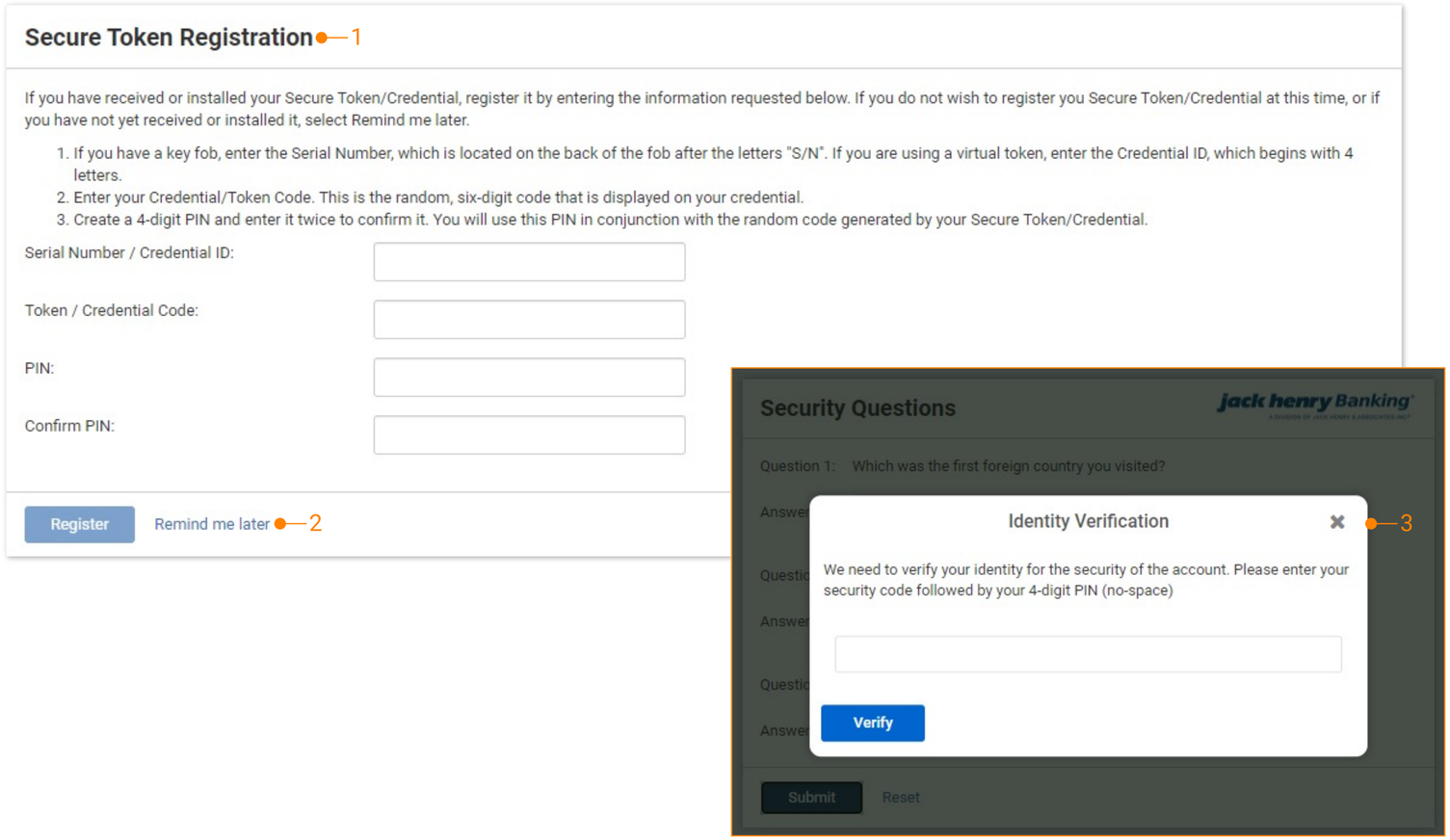
2. Company Authentication Settings - Authentication Status

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



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.

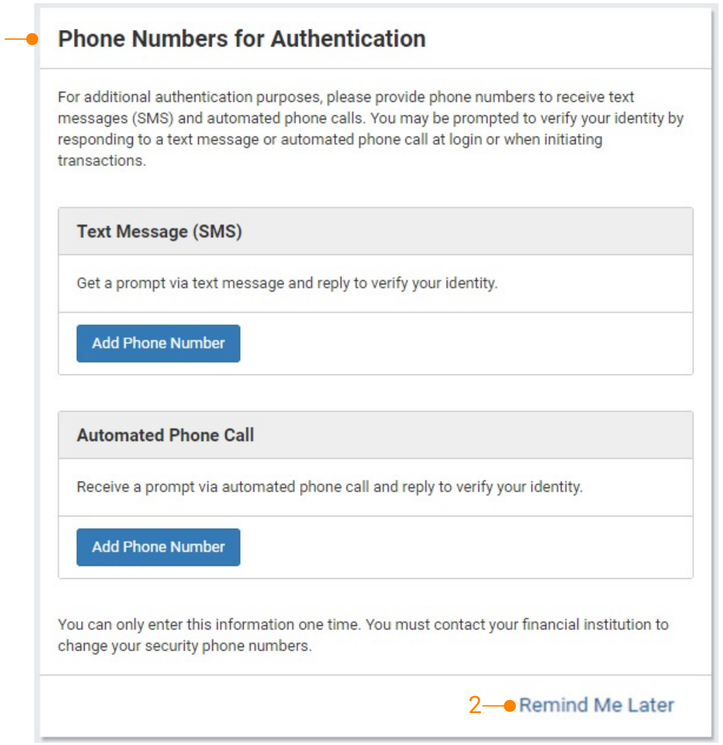
3. Authentication

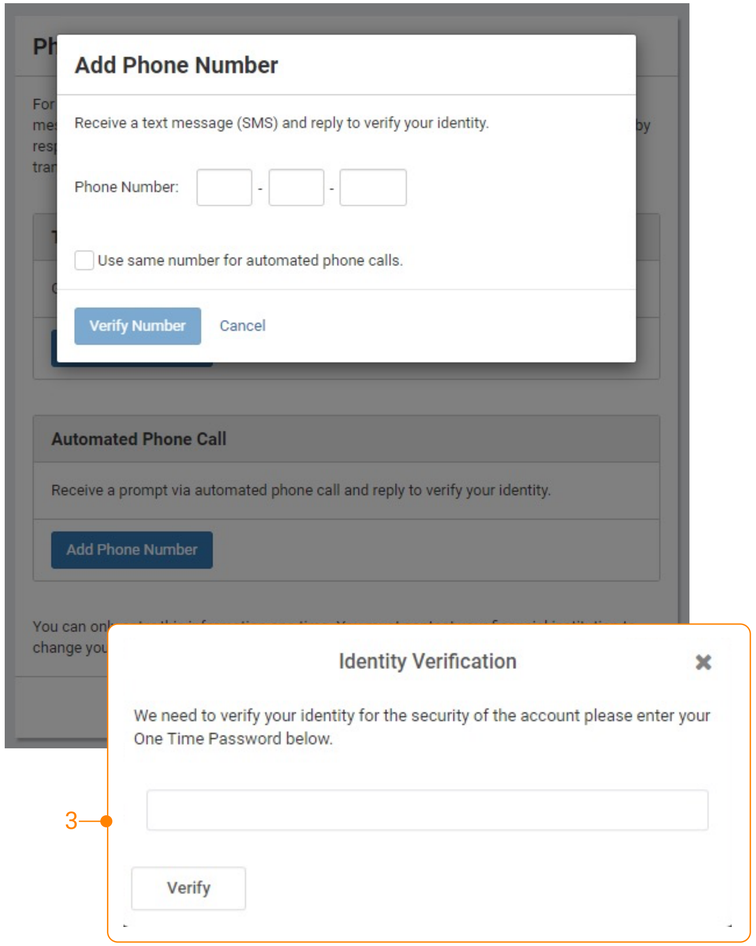
After successful registration and upon a user's next login, they will be prompted to input their security code + their PIN they established at registration

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. 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.