Quick Reference Guide

QRG Back Office Secure Token Authentication

JHA Treasury Management™

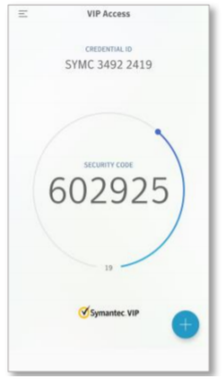
Last Updated: July 11, 2022

QRG Back Office Secure Token Authentication

Overview: The Secure Tokens feature within JHA Treasury Management coordinates with third-party software from Symantec. FI Users will need to log a case within jSource in order to complete set up and use. The option to enable secure tokens will be grayed out until this step is completed. Users can be instructed to download virtual tokens to their desktop or mobile device or be provided physical tokens before these steps are performed.

Note: To have this feature enabled, you will need to log a a support case via the For Clients Portal. The Secure Tokens feature within Treasury Management relies upon third-party software from Symantec

Preparing for Secure Token Enablement



Smartphone Access

Search VIP Access within the APP Store on your mobile device and download the Symantec application.

Hard Tokens

Physical keychain devices can be provided to all within your organization for VIP access.

Contact your JHA Inside Sales Rep to order physical tokens.

Desktop and Tablet Access

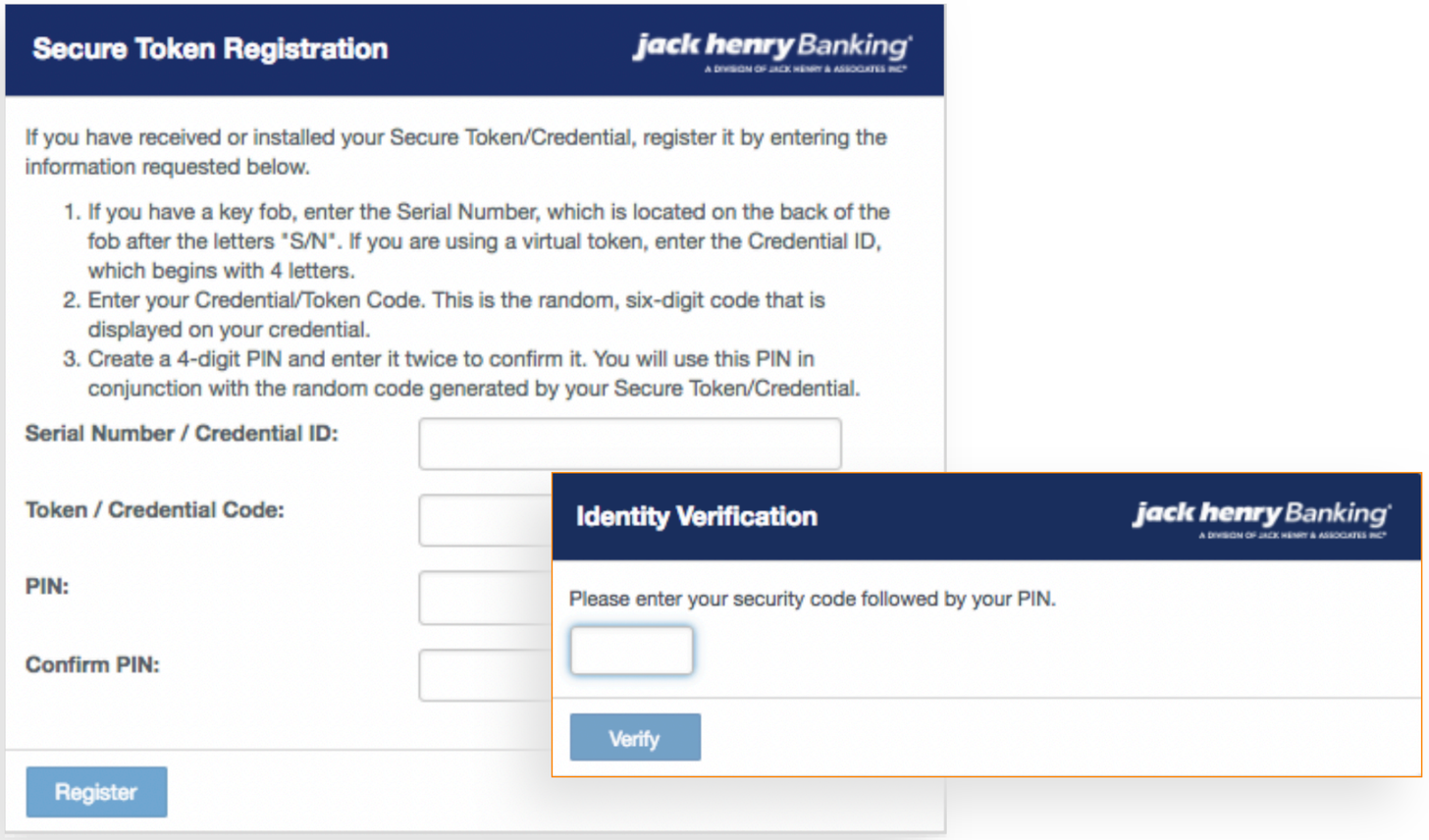
Vitural tokens can be downloaded to company workstations.

For instructions on how to download desktop or tablet tokens, go to http://idprotect.vip.symantec.com

- Prior to enabling this feature, Back Office users should be instructed to download virtual tokens to their desktop or mobile device or be provided physical tokens.
- To order physical tokens for your employees, visit the following site: https://www.kristopherjamescompany.com.
- To download a desktop token, visit https://vip.symantec.com.
- To download a mobile token, search for VIP Access within the applicable app store.

Note: Once this feature is enabled, all Back Office users will be required to register to proceed with login.

User Registration and Authentication



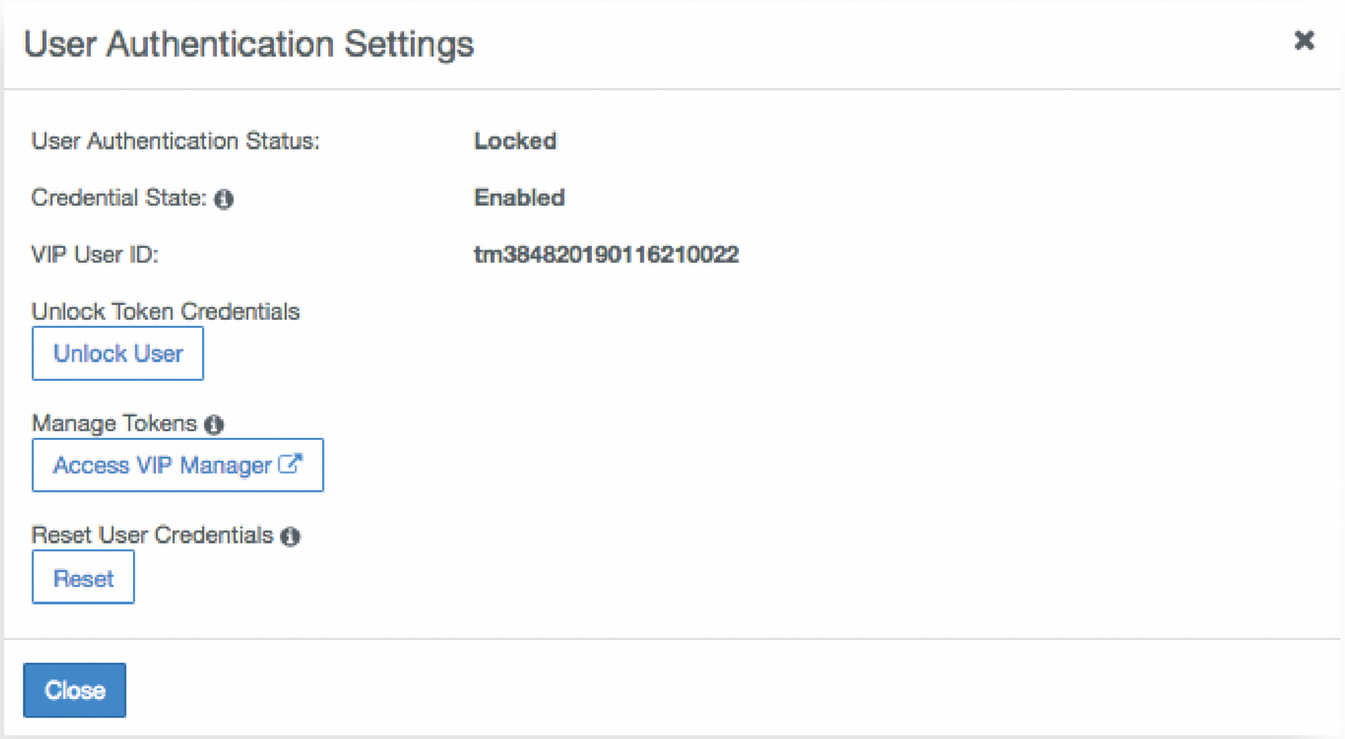
- After logging in with their user name and password, Back Office users will be prompted to register their credentials.
- Users must enter their Credential ID from their physical or virtual token (located on the bank of physical tokens), the six-digit security code displayed on the token, and a four-digit PIN of their choosing.

Note: Users who already have a Symantec VIP Access credential for other JHA products may use the same one to register for Treasury Management.

- At subsequent logins, users must enter the six-digit security code displayed on the token plus their PIN in order to proceed.

Note: Users can view an audit trail of failed Secure Token authentication attempts by hovering over the Last Login icon when it appears in the header.

User Authentication Settings



FI Administrators have the ability to manage Secure Token authentication settings for Back Office users. To view or modify a user's Secure Token authentication settings, locate the user within the FI User List, then select "Authentication Settings" from the "Actions" dropdown menu.

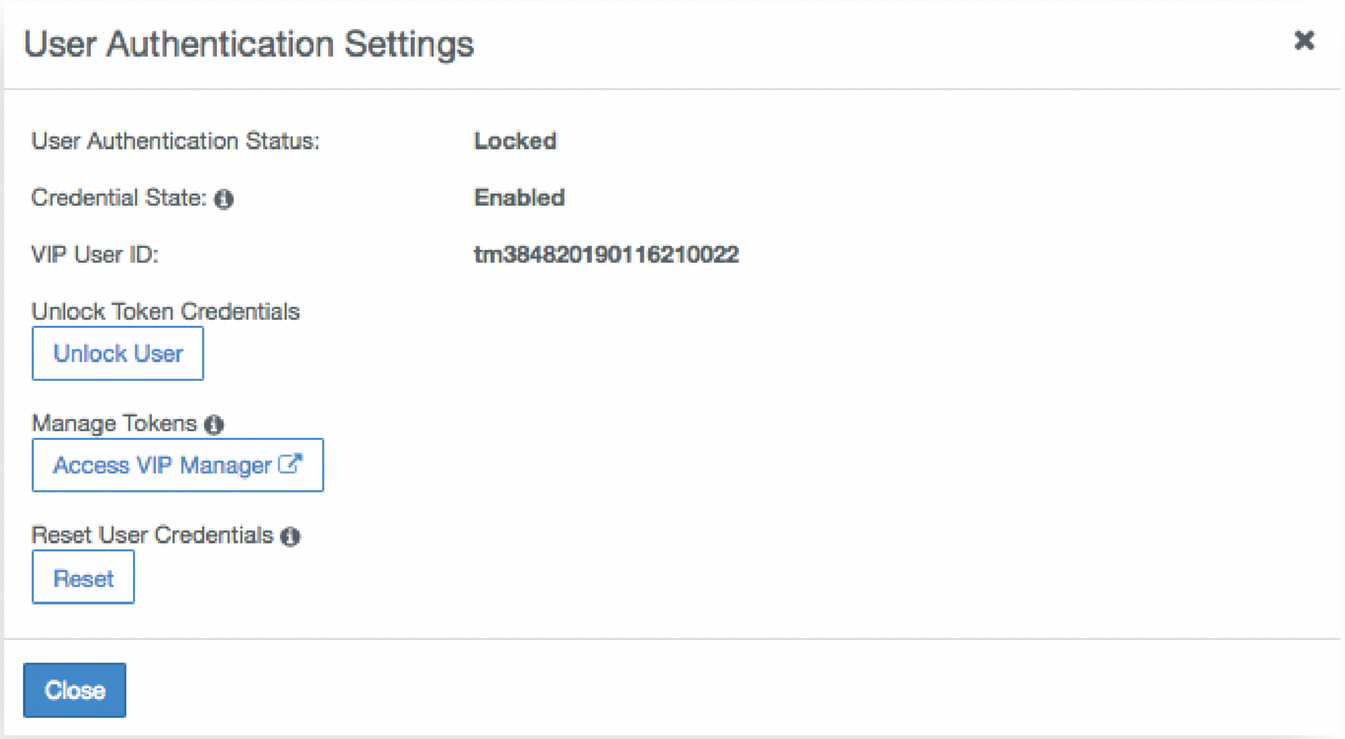
User Authentication Status: Indicates whether or not the user has registered a credential or if the user has been locked due to too many failed Secure Token authentication attempts.

Credential State: Indicates the state of the Symantec VIP Access credential.

VIP User ID: A unique identifier generated by TM. You may need it when performing certain tasks within VIP Manager

Note: If the User Authentication Status is "locked," the FI administrator can unlock the user within Back Office. If the Credential State is "locked" (or "disabled" or "inactive"), the FI administrator will have to access VIP Manager to resolve the issue.

Control Credential Access



To Unlock a User's Credential (Within Back Office)

- Select Unlock User. A confirmation window will appear.
- Click the checkbox if you would like to also reset the user's credential registration.
- Select Unlock Secure Token in the confirmation window.

To Reset a User's Credential

- Select Reset. A confirmation window will appear.
- Select Reset again in the confirmation window.
- The user will be prompted to register again at the next login. This action will also unlock the user.

To Access VIP Manager

You can access VIP Manager to view usage reports, provide users with temporary security codes, and perform other tasks related to users' credentials. You will need a Symantec account to log on.

- Select Access VIP Manager. A new browser window will open.
- Enter your email address and password.