



First-Time Secure Login for Treasury Management Users



800.974.3273 | ubmich.com





Let us be your guide. For good reason, First-Time login to our Treasury Management Software is a secure process.

Each user is empowered with the ability to customize their own unique User Login credentials. Administrators can determine when passwords expire and set deadlines for users to reset their passwords. In addition to these user friendly features, we have created a process to ensure first-time logins will be secure across your organization. This Guide will walk you through each step. From Enrollment to first-time credential settings, to establishing security questions, you'll be prepared to educate your team members as well as provide orientation for new associates.

Let us guide you through each of these 7 easy to follow steps:

Step 1 Enrollment email

Step 2 Credentials for first time login

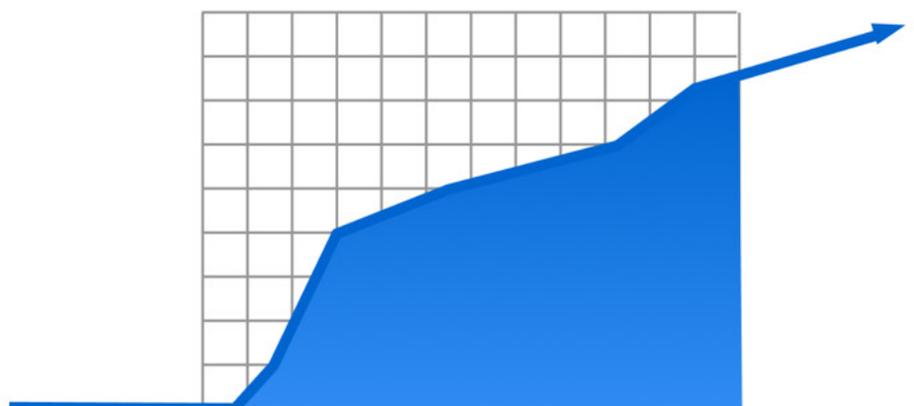
Step 3 Completing a first login

Step 4 Enroll SMS text or Token authentication

Step 5 Creating a new password

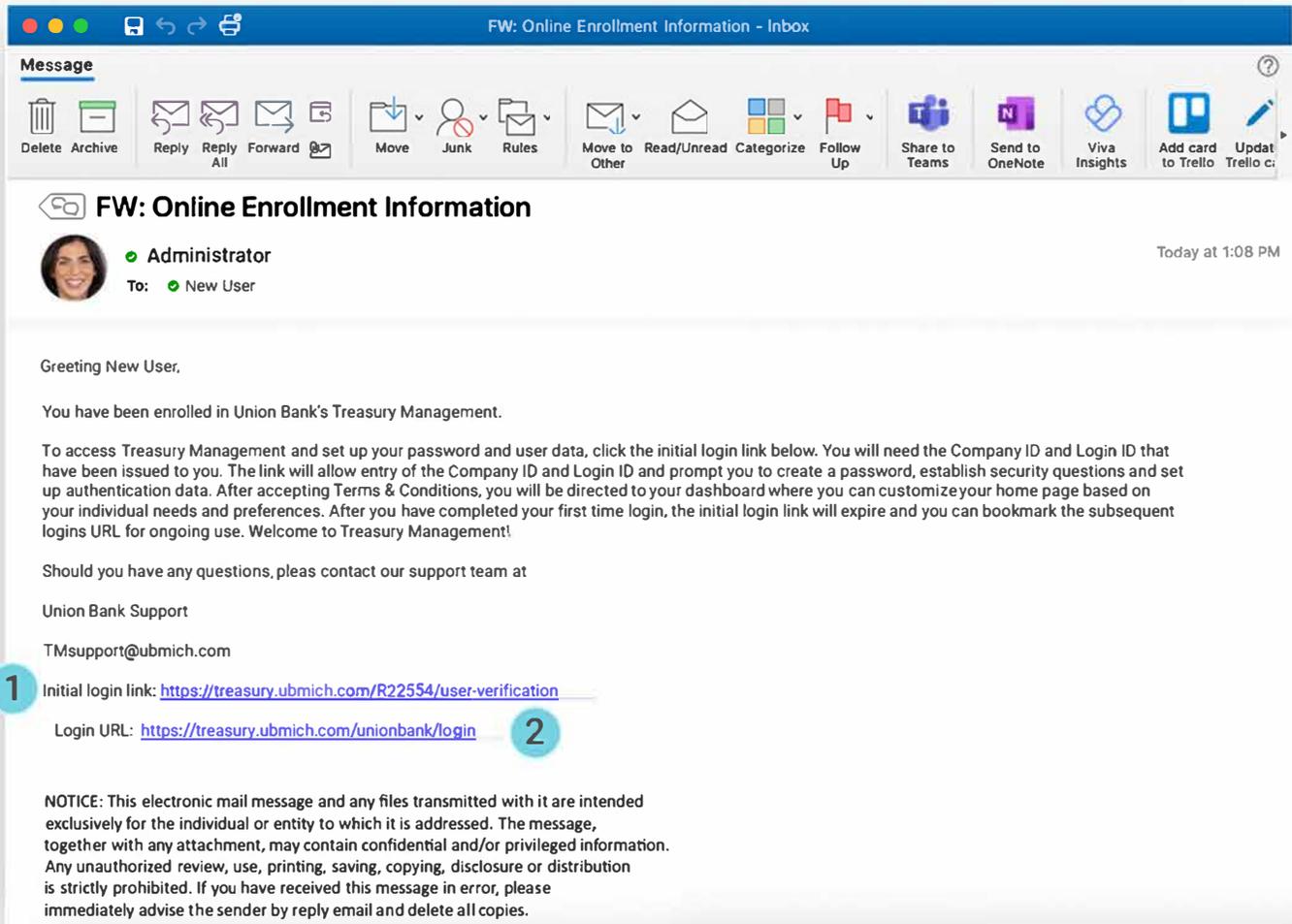
Step 6 Establishing security questions

Step 7 Accepting Terms and Conditions



Step 1: Enrollment Email

When a new user is created by an FI back office user or a company administrator, an email will be sent as soon as the enrollment is completed. The email will contain a link to be used for the first-time login. This link can only be used for the first login. After the user has successfully signed in, the link will no longer be valid. From the time the email has been delivered, the user will have no more than seven days to complete the initial login. After seven days, the link will expire.



1 Initial Login Link will take the user through several enrollment and authentications steps.

2 Login Link will be used for logins after the enrollment process. We recommend bookmarking it so it is always accessible.

Note: Enroll email for converted users.

During a conversion event from a different online banking system to Treasury Management, enrollment emails are handled differently. Companies and users will be set up via conversion scripts on the weekend of the conversion event. Enrollment emails will be sent at a time designated by the financial institution.

Step 2: Credentials for first time login

The initial login link in the enrollment email is the user's gateway to the platform. However, there is required information for a successful login that must be communicated to the user before the email is sent. The financial institution creates the company ID when onboarding the company in Back Office. This company ID is part of every login, including the initial login, and must be known to the user at that time.

Financial Institutions leverage many different options for communicating the company and login ID credentials. In orchestrated conversion events, many institutions prepare individualized mailings to users to communicate the company and login IDs. For ongoing business, methods such as secure email or personalized training (on-site or remote) are common practices for communicating the required credentials.

The screenshot shows a web browser window with the title "Treasury Management". The address bar contains the URL "qa.jha.treasury.jackhenry.com/R22554/user-verification?code=VM7VaxgbFs%2FGGjyRWs%2BZ69JM0Rba9E%2FRH%2B...". The page content is a "User Verification" form. The form has a title "User Verification" and a sub-header "To verify your identity and process with a password change, please enter your Company ID and Login ID and provide the answer(s) for your security question(s)". There are two input fields: "Company ID: *" with a button "Enter Company ID" and "Login ID: *" with a button "Enter Login ID". Below the fields are "Submit" and "Reset" buttons. The form is overlaid on a light blue background. The browser's navigation bar shows "Apps", "Getting Started", and "Imported From Fir...". There is also an "Update" button in the top right corner of the browser window.

1 Company ID is generated from the Financial Institution in the Back Office. The bank will need to provide this information to the selected admins at each company. Due to its secure nature, verbal disclosure or encrypted communication is recommended.

2 Login ID is specific to each individual user. This too must be communicated **before** the enrollment email is sent in order for a success login to be completed. Again due to its secure nature, verbal disclosure or encrypted communication is recommended.

Step 3: Completing a first login

Once a user is in possession of his or her credentials and the enrollment email has been sent, login can occur. There are several steps required during this process. The first time the user logs in, her or she will be guided through the procedures listed below.

Accessing Initial login

1 User Verification

To verify your identity and process with a password change, please enter your Company ID and Login ID and provide the answer(s) for your security question(s).

Company ID: *

Login ID: *

1. First Prompt

The initial login screen is accessed via the link on the enrollment email. On landing, the user will be prompted to enter the company ID and Login ID.

2 User Verification

 We could not process your login attempt. Please try again or contact your system administrator.

To verify your identity and process with a password change, please enter your Company ID and Login ID and provide the answer(s) for your security question(s).

Company ID: *

Login ID: *

2 Error Scenario

If the credentials entered are not valid, the user will receive an error. The user can re-attempt by correcting the invalid data and re-submitting.

The remainder of this guide will focus on these final steps.

-  Enrolling for SMS text or token authentication
-  Creating a new password
-  Establishing security questions and answers
-  Accepting Terms and Conditions

Step 4: Enrolling SMS Authentication

After the company ID and login ID are validated, the user will be guided through the collection process for Out of Band or Token authentication.

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.

[Remind me later](#)

2 Verify Phone Number

A text message (SMS) was sent to your phone. We need to verify your identity for the security of the account please enter your One Time Password below:

Phone Number: 9133413434

[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.

[Remind me later](#)

1. First Prompt For out of band (SMS text or phone call) the user will be prompted to add a number. When a number is added, a code will be sent to the mobile device in case of text or delivered via automated phone call.

2. Second Prompt The code must then be entered into the verification screen and it must be an exact match for the code that was delivered to the user's phone. The code will be valid for no more than 10 minutes.

Step 4: Enrolling SMS Authentication

3 **Verify Phone Number**

Success!

Phone Number: 7174758580

What is your preferred method of verification?

Text Message Automated Phone Call

Done

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.

Remind me later

4 **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) – Preferred

Phone Number: xxx-xxx-8580

Automated Phone Call

Phone Number: xxx-xxx-8580

Edit Phone Number Remove

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

Done

3. Third Prompt When the code is entered and validated, the user will then have option to use the same number for either text or automated phone call, and set the preferred method.

4. Fourth Prompt The final step allows the user to complete the authentication collection and continue, or continue to add / edit authentication data. After clicking Done, the user will continue to the next phase of the first time login.

Step 4: Token Authentication

For clients set up for token authentication, step four will collect the token data in lieu of a phone number for text authentication. Token authentication is completed in one simple step. The token, which can be a mobile application, PC desktop application, or physical device, will have a serial number. This serial number or device ID must be entered in the token registration screen, along with the one-time code currently displayed on the token. Each user will also personalize a four-digit PIN that will be included after the token code each time authentication is required.

Secure Token Registration

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.

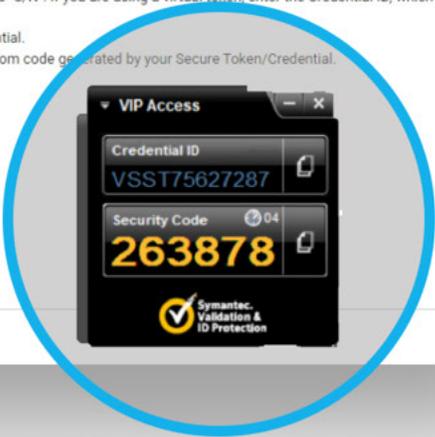
1. If you have a key fob, enter the Serial Number, which is located on the back of the fob after the letters "S/N". If you are using a virtual token, enter the Credential ID, which begins with 4 letters.
2. Enter your Credential/Token Code. This is the random, six-digit code that is displayed on your 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:



Note: If you have not yet downloaded a token, you can download an application to your PC by visiting <https://vip.symantec.com>. If you prefer to use a mobile device application, search for VIP Access (Symantec VIP) in your device application store.

Step 5: Creating a new password

During the initial login process, the user does not have or use a temporary password. For continued use, a password must be created. The password parameters are established by the financial institution in Back Office and each institution may set requirements differently.

Change Password

Please enter a new password following the password requirements listed below.

Password Requirements:

- Password maximum length : 25
- Password minimum length : 8
- Allow alpha characters in password : Yes
- Allow numbers in password : Yes
- Allow special characters in password : Yes
- Alpha characters in password are required : No
- Numbers in password are required : No
- Special characters in password are required : No
- Number of upper case required in password : 0
- Number of lower case required in password : 0
- Cannot be one of the previously used passwords : 3

Company ID: cbgp

Login ID: dtilton

New Password: *

Confirm Password: *

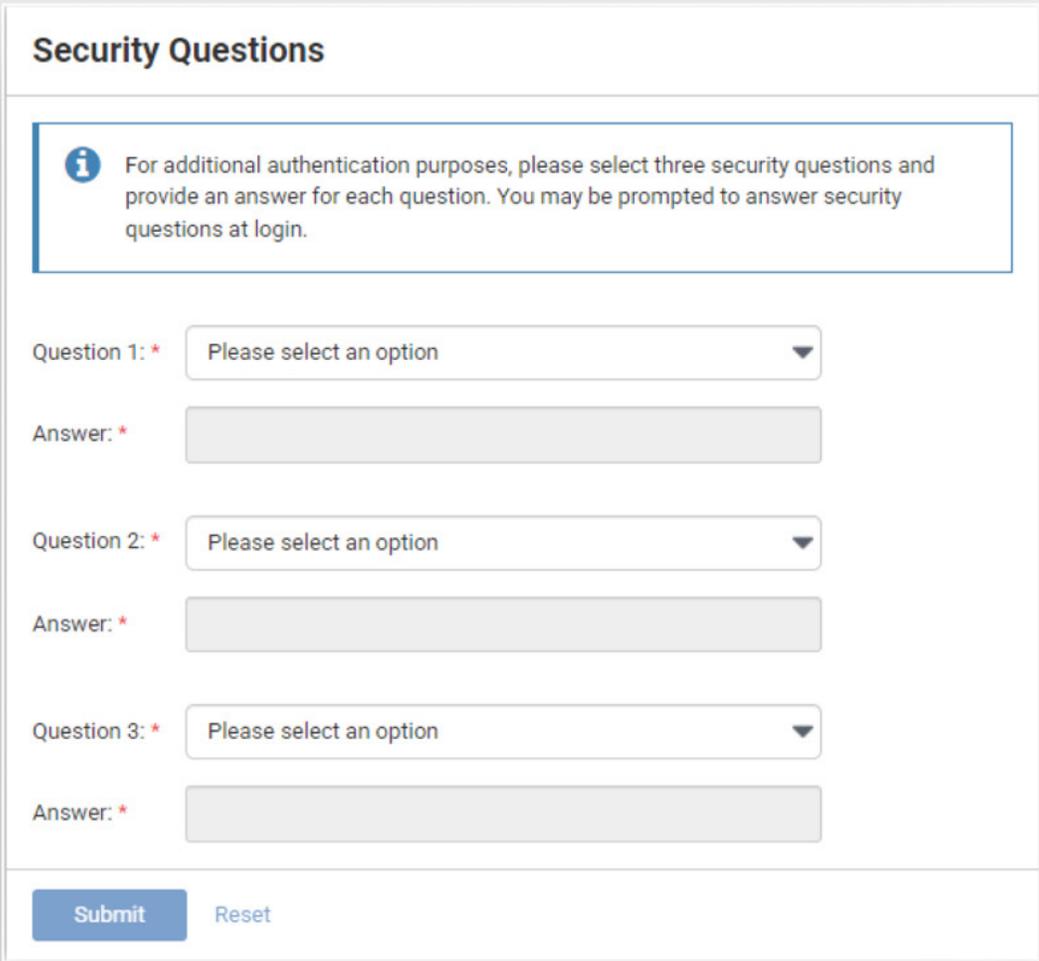
 Reset

Password Strength For password strength, the password should be no less than eight characters and should require combinations of alpha, numeric and special characters. Passwords are case sensitive so it is also advisable to require a specific number of uppercase alpha characters.

Note: The requirements will be displayed to the user on the screen and the user will not be able to save until the entered data satisfies the requirements. To ensure that the user has entered a string that he or she intended to, **it must be entered twice.**

Step 6: Security questions and answers

The Treasury Management platform users RSA to challenge users with security questions if anomalies are detected in a login session. Completing security question registration is part of the initial login process. Each user must select three questions and fill in the corresponding answer.



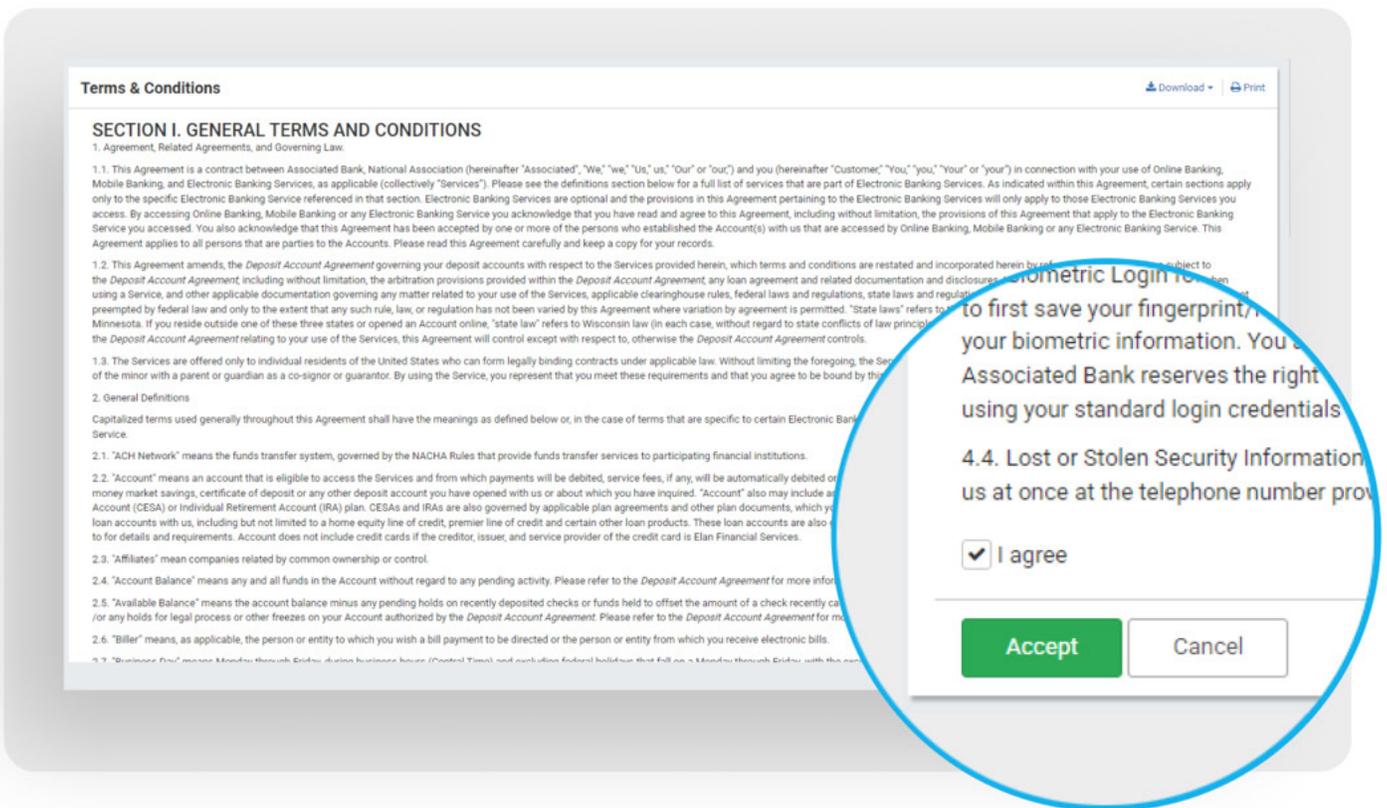
The screenshot shows a web form titled "Security Questions". At the top, there is an information icon and a message: "For additional authentication purposes, please select three security questions and provide an answer for each question. You may be prompted to answer security questions at login." Below this, there are three identical question sets. Each set consists of a dropdown menu labeled "Question 1:", "Question 2:", or "Question 3:" with a red asterisk, and a text input field labeled "Answer:" with a red asterisk. The dropdown menus currently display "Please select an option". At the bottom of the form, there are two buttons: "Submit" and "Reset".

Hint: The questions selected should be appropriate to the user and the answers should be information the user can easily recall for authentication at random times.

Note: A user cannot opt-out or bypass security question registration. This is a requirement to use the platform.

Step 7: Accepting Terms and Conditions

Terms & Conditions for the Treasury Management system are controlled by a financial institution back office user. The terms can be updated at any time and the FI can choose to have all users re-accept any time a change is made. All users signing into Treasury Management must accept the financial institutions Terms & Conditions. There are no options to defer or decline. If a user does not complete the acceptance, the session will be terminated. To accept Terms & Conditions, the user must scroll to the bottom of the document



Accept and Agree After scrolling to the bottom of the Terms & Conditions, there are two required actions to complete the acceptance. First, the user must check the I agree box. Second, the user must click Accept. This completes the first time login process.

During the subsequent logins, the user will access the institution's conventional login page and authenticate with

- **Company ID**
- **Login ID**
- **Password**

If the financial institution requires additional authentication at login (with token or SMS text) the challenge will occur after the company ID / Login ID / Password have been validated.

Additionally, if anomalies are detected such as logging in from a different location or a dynamic IP address, the user may be challenged with security questions.