

Treasury Management

unified identity service (UIS)

Unified Identity Service (UIS) for Treasury Management is a replacement solution to Outseer's (formerly RSA) Multifactor Authentication. UIS aligns with Jack Henry Digitals' strategic direction for platform security by employing modern OAuth 2.0 authentication protocol. We recognize that transitions like this can be difficult, and often bring about new challenges for you and your clients. We promise that we'll do everything we can to make this upcoming transition as seamless as possible, and work with you to resolve issues and provide guidance.

We've answered some of the most frequently asked questions here to get you started:

frequently asked questions

Treasury Management already has 2FA at login. Why this change?

There are several reasons why UIS takes Treasury Management in the right direction. While the existing two-factor login authentication provides the basic need for scrutinized access, UIS takes that to the next level, providing a more consistent and secure mechanism for login authentication.

With UIS, a unique identifier is generated and maintained for a single identity that links an end user with their credentials stored in Google Cloud Identity. Keep in mind that UIS does not impact end user permissions stored in products that utilize UIS; all permissions and ability to access still reside within the Treasury application.

What are the other benefits?

Security & Technology

UIS has substantial infrastructure to identify and block credential stuffing attacks before they lock a user out of their account, and contains preventions to make it difficult for phishing sites and other attach schemes to be possible. Neither of these protective measures are available within Treasury Management today.

Additionally, by moving to UIS, Treasury Management automatically reaps the benefits of changes made to the overall security of the Jack Henry Digital Banking Platform. As changes are made to benefit Banno or Banno Business, for example, Treasury inherits those foundational changes to improve security. We will no longer need to make security and authentication changes through separate Treasury Management development tools.

Functionality & Integration

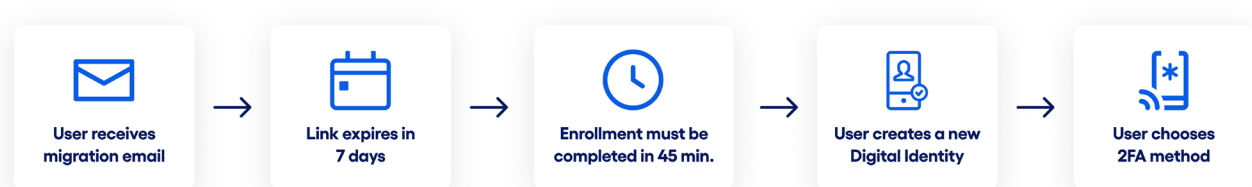
In order for Treasury Management to get to the next level of functionality needed to attract and retain business and grow deposits, we must align with the overall Jack Henry Digital Platform technology strategy. Integrations planned following the migration to UIS include Plaid, Finicity, Conversations for Business, and opportunities for other third-party providers.

user experience

What should users expect during the migration to UIS?

After you've chosen your UIS migration date, you'll want to make sure you include the following talking points in your communication:

- Users who are in an active status and have logged in 45 days prior to your migration date will receive an email with instructions and a link to create a new Digital Identity.
- Action must be taken before the link expires (within 7 days of being issued)
- Once the user accepts the invitation and clicks the link, enrollment must be completed within 45 minutes. Users who do not complete the enrollment process within 45 minutes of clicking the link will require intervention by the bank.
- Clicking the link will prompt the user to select a new username and create a new password that will be used during all subsequent logins.
- After successfully creating their new credentials, users will be prompted to establish their two-factor login method for login (SMS text, voice phone call, authenticator app, or secure token).



Users who do not fit the criteria listed above will be handled on an individual basis, with the bank issuing invitation emails on a per-request basis. Once invited, the same credential creation process outlined below applies.

1. Migrated or newly-created channel users will receive an enrollment email.

Greetings Jessica Kenney,

You have been enrolled in Business Banking.

With the FI ID and Login ID credentials you have been provided, please select the Initial Login link. The link below will allow entry of your FI ID and Login ID, and will prompt you to establish a password. In addition, you will then be prompted to establish security questions to which you will provide answers for. After selection and entry of your security questions and answers you will be directed to the FI Back Office Dashboard.

Should you have any questions, please contact us directly at:

FI Support
email@bank.com
(123) 555-5555

Initial login: <https://treasurybackoffice.dev.jackhenry.com/user-verification?code=Gy2wvrYeo0MnDG3h%2bAfbqXNI%2Fv1xNsSaEgh7aBLBPmQ%3d>

2. The Digital ID enrollment link will direct users to enter the Company and Login IDs provided.

The diagram illustrates the flow from a generic login form to a pre-filled one. On the left, a 'Login' form prompts the user to 'Input your Treasury Company ID and Treasury User ID to begin the enrollment process. You will be prompted to complete profile details, as well as select a user name and password.' It features two input fields: 'Company ID *' with the placeholder 'Enter Company ID' and 'Login ID *' with the placeholder 'Enter Login ID'. Below these are 'Submit' and 'Reset' buttons. A blue arrow points to the right, where the same 'Login' form is shown, but the 'Company ID *' field is pre-filled with 'Foxtrot' and the 'Login ID *' field is pre-filled with 'mjones'. The 'Submit' and 'Reset' buttons remain at the bottom.

3. Users will be prompted to create their Treasury profile and Digital ID.

The screen displays the Treasury Bank logo at the top, labeled 'PRIMARY LOGO'. Below the logo is a message: 'Create your Treasury Bank ID to establish your account access.' with an information icon. A button with a person icon and the text 'Create my Treasury Bank ID' is provided. Below this, a section titled 'ALREADY HAVE A TREASURY BANK ID?' asks the user to 'Login to link an additional account.' and includes a 'Username' input field. A 'Forgot?' link is positioned to the right of the input field. At the bottom, a green 'Continue' button is visible.

- Step 1 of User ID: Users will complete & verify profile information.
- Step 2 of User ID: Users will create their credentials. This Username/Digital ID and Password will be used for subsequent logins.

Treasury Bank
PRIMARY LOGO

Create your Treasury Bank ID to establish your account access.

Create your Treasury Bank ID

Verify your profile information

First name (Required)
Madelyn

Last name (Required)
Jones

Email
Email (Required)
jkenney@jackhenry.com

Phone Number

Country
+1 Home

Country
+1 Mobile

Country
+1 Work

Next

Treasury Bank
PRIMARY LOGO

Create your Treasury Bank ID credentials

Username
mjonesuis

Show rules

Password
.....

Show rules

Confirm password
.....

Next

4. Users will protect their accounts with 2-step verification and choose their preferred method.

Protect your Treasury Bank ID with 2-step verification

Each time you sign into your Treasury Bank ID on an unrecognized device, we require your password and a verification code. Never share your code with anyone.

Add an extra layer of security
Enter your password and a unique verification code.

Keep the bad people out
Even if someone else gets your password, it won't be enough to sign into your account.

Get started

Choose your Treasury Bank ID verification method

Voice or text message
Verification codes are sent to your phone.

Authenticator app
Using a different authenticator app? We support using any authenticator app using either a QR code scan or manual code entry.

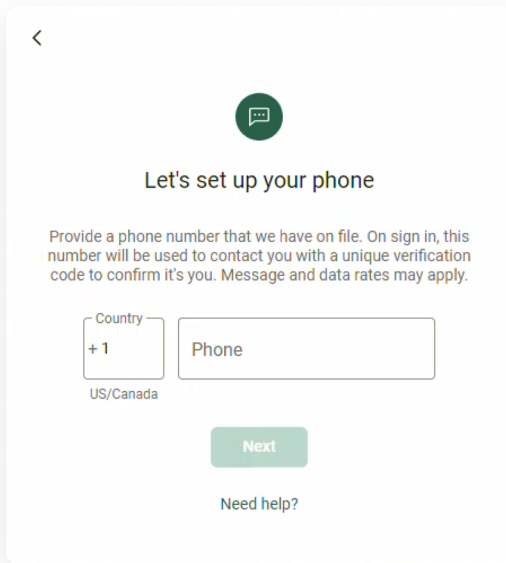
Symantec VIP
Use Symantec VIP authentication to sign into your account. We support digital and hard tokens.

Security key
Use a hardware token to authenticate.

2-Step Verification Methods

Users will have the option to choose from 4 different verification methods: voice or text message, authenticator app, Symantec VIP, or a security key.

Voice or text message



Let's set up your phone

Provide a phone number that we have on file. On sign in, this number will be used to contact you with a unique verification code to confirm it's you. Message and data rates may apply.

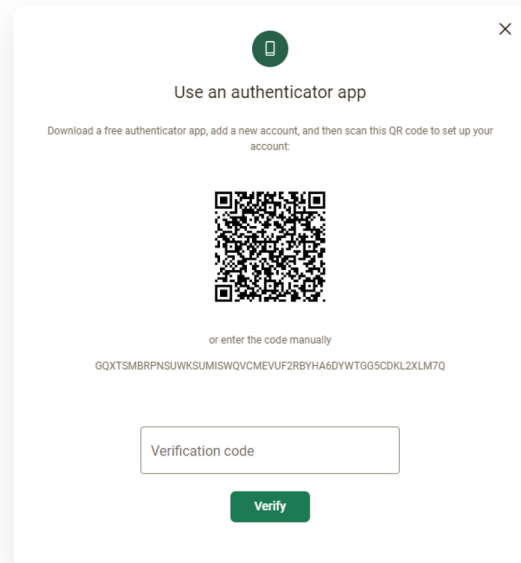
Country
+ 1
US/Canada

Phone

Next


[Need help?](#)

Authenticator app



Use an authenticator app

Download a free authenticator app, add a new account, and then scan this QR code to set up your account.



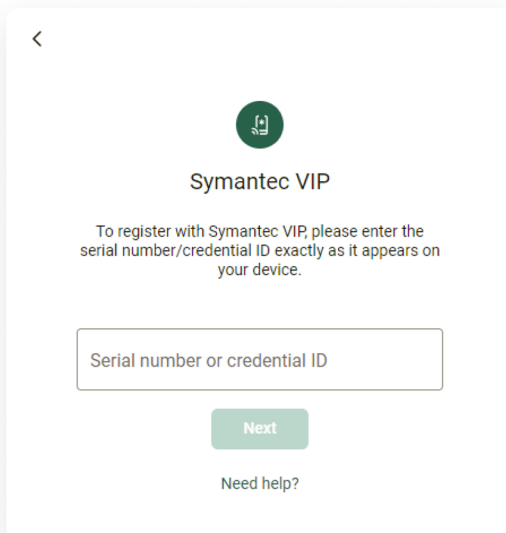
or enter the code manually

GQXTSMBRPNSUWKSUMISWQVCMFVUF2RBYHA6DYWTGG5CDKL2XLM7Q

Verification code

Verify

Symantec VIP



Symantec VIP

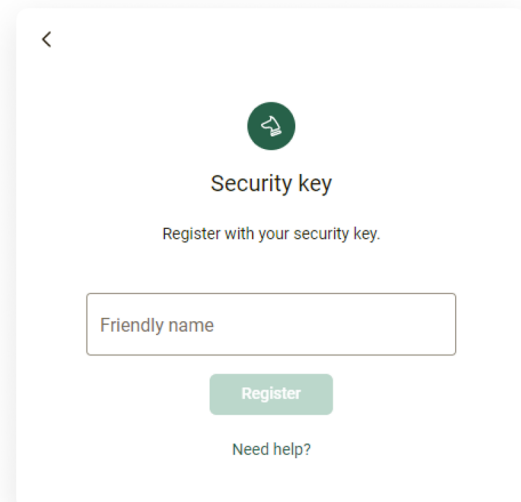
To register with Symantec VIP, please enter the serial number/credential ID exactly as it appears on your device.

Serial number or credential ID

Next

[Need help?](#)

Security key



Security key

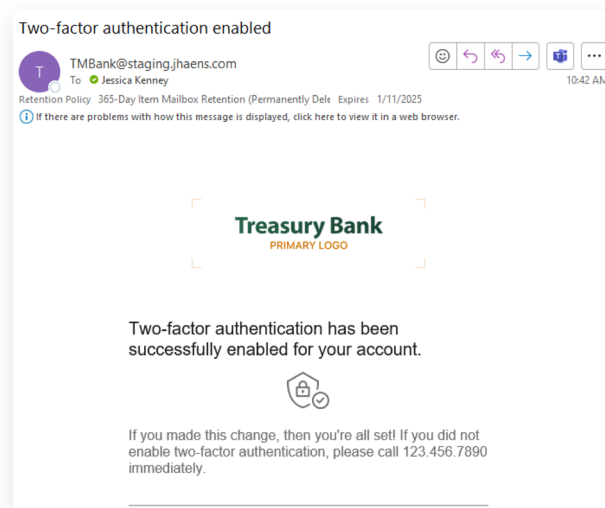
Register with your security key.

Friendly name

Register

[Need help?](#)

- When complete, user receives an email confirming 2FA verification setup.



See it in action! ★ New!

Click [here](#) to view a video of the enrollment process from receipt of the email to creation of the Digital Identity. You may need to authenticate into For Clients to view the video.

migration timeline

When should we expect the migration to UIS to occur?

Migrations to UIS can happen any time between now and May 30, 2025. To request a migration date, please open a Treasury Management case with the description of Treasury Management UIS migration date. Note that we will not be performing migrations between March 3rd and March 21st due to the ISO20022 migration on March 10th.

When determining your preferred date for migration, keep in mind that until you are migrated, any new features developed following the benefit of UIS may not be available to banks still on the current authentication method. For example, let's say Treasury Management develops and makes available a new single sign-on to a feature that your bank is interested in. If that feature should be available prior to your migration, it could not be enabled until your migration was complete.

Can company users be migrated in waves?

No, the migration of qualified users must happen all at once. The current authentication method and Unified Identity cannot be in place in your production environment at the same time.

Based on the active user migration process outlined above, now is a good time to perform any cleanup of user information so that the migration emails sent are as accurate as possible.

How are new users added after migrating to UIS?

New users will continue to be added via Treasury Management Back Office. Upon submitting the new user, they will be sent an email with instructions and a link to create their Digital Identity per the steps outlined in previous pages. Upon clicking the link in the email, the process is the same as the users receiving the migration email.

billing information ★ New!

How much will UIS cost? How will this affect our current contract?

While there will not be a new contract for Unified Identity Service, there is a flat-fee of \$250.00 per month. This cost will replace those currently being assessed for the Outseer MFA authentication product. Your MFA contract for use with Treasury Management will automatically be terminated with no action on your part.

additional frequently asked questions

Can my users keep their existing username?

It is possible that the user's existing Login ID can be used again, however usernames now need to be unique across your entire brand, including Banno usernames. In many cases a new username will have to be chosen, especially if you have many users with the Username of Admin. One way to promote choosing a username that will already be familiar is to use a combination of the existing Company ID plus the existing Login ID. For example, a Company ID of C102345 with a Login ID of janedoe could be a UIS ID of C102345janedoe.

What if an end user currently logs into multiple companies?

During migration, each user meeting the criteria outlined will receive an email to create their Digital ID. If the same email address is tied to more than one user, whether a different company or the same company, each will receive an individual email.

The first email link clicked on will take the user through the steps outlined above. When they click the link in the second (or third) email, they will be able to use the "Already have a Treasury Bank ID?" Login to link an additional account feature shown below. Upon entering their Digital ID their accounts will be linked together under that digital ID. Upon subsequent logins the user will get to choose which company they want to access.

How are password reset requests handled?

Bank Administrator Password reset requests will be handled through the Identity app via Banno People rather than Treasury Management Back Office and will only be available to bank employees. The ability to set a temporary password on the user's behalf will not be available with UIS. Users will be able to perform account recovery activities identical to those the bank can initiate for them via Banno People.

Company administrators will be able to send a password reset link to company users via the Treasury Management desktop application.

What are the new rules for creating a username?

Username must be between 4 and 64 characters in length.

Username can contain letters (a-z), numbers (0-9), dashes (-), underscores (_), apostrophes ('), and periods (.) and can begin or end with non-alphanumeric characters except periods (.) and spaces.

Username cannot contain more than one period (.) in a row, accents, accented letters, ampersands (&), equal signs (=), brackets (<,>), plus signs (+), at signs (@), or commas (,).

What are the new rules for creating a password?

Password must be between 8 and 64 characters in length.

All ASCII and Unicode characters (including spaces) are supported for passwords.

Password must not match or contain your username and must not begin or end with a space.

Passwords will not expire.

Can users lock themselves out with UIS at login?

Users can be temporarily locked with multiple failed 2FA verification attempts, with varying failed attempts based on the authentication method. Users cannot be locked out due to invalid password attempts.

Can the 'Don't ask for codes again while using this browser' feature be disabled for Treasury Management users?

No, it cannot be disabled. The 'remember this browser' feature is tied to the browser that is used during selection of the 2FA method. If a brute-force attack was attempted, or a login from a different browser was attempted, 2FA prompts would occur and access would not be granted until successfully validated using one of the established 2FA methods. Remember, post-authentication actions can still be challenged at the activity itself.

Do I have to allow all of the available authentication types?

No, you don't have to offer all of the available authentication methods. You have the choice between different security levels (standard, enhanced, or high) and each security level has corresponding authentication types it accepts.

The standard security level is the most flexible and it offers users the choice between a phone call, text, email, FIDO keys, Symantec tokens, or an authenticator app. The enhanced security level offers the same options as the standard level with the exception of phone-based delivery options. The high security level only accepts FIDO tokens, which prevents sim-swapping.

we're here for you every step of the way

We hope that you're as excited about this new journey as we are. If you have any additional questions or concerns, please reach out – we're happy to help in whatever way we can. As always, thank you for trusting us to serve you and your clients!

experience next-level login

Let's talk about this together. digitalexperience@jackhenry.com

For more information about Jack Henry, visit jackhenry.com.