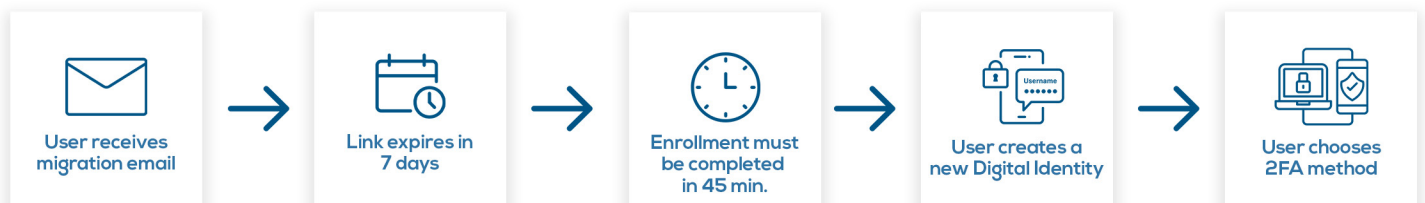


Treasury Management

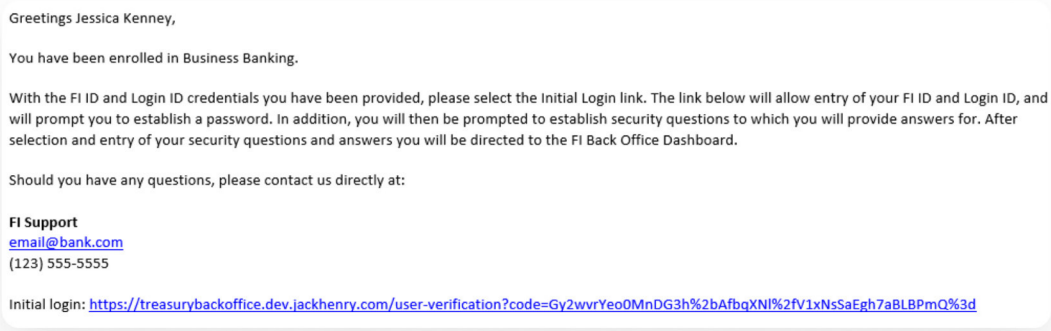
User Experience

What should users expect during the migration to UIS?

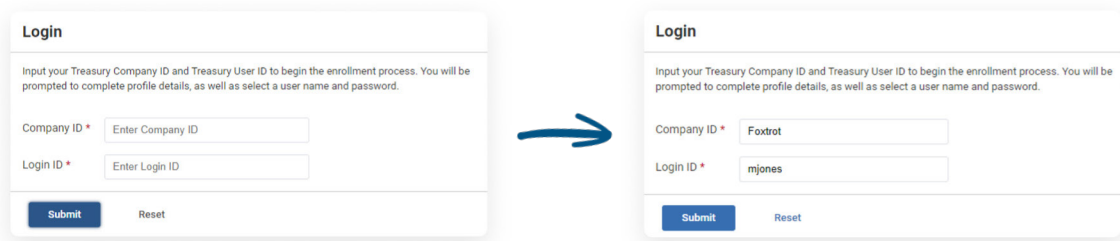
- Users who are in an active status and have logged in 45 days prior to your migration date will receive an email with instructions and a link to create a new Digital Identity.
- Action must be taken before the link expires (within 7 days of being issued)
- Once the user accepts the invitation and clicks 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, or authenticator app).



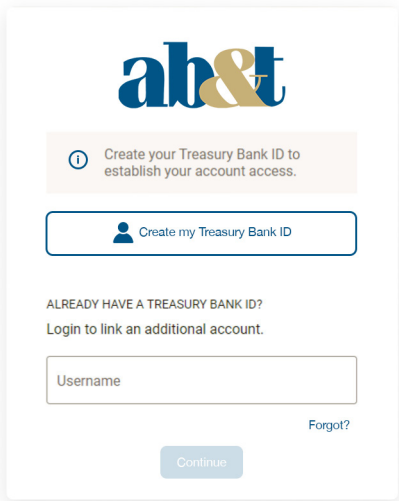
1. Active users that have logged in 45 days prior will receive an enrollment email.



2. The Digital ID enrollment link will direct users to enter the Company ID and Login IDs currently used for online access. Action must be taken with 7 days of being issued. Once the link is clicked, enrollment must be completed within 45 minutes.



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



- 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.

The first screenshot shows the 'Create your Treasury Bank ID' screen with the following fields:

- First name (Required):** Madison
- Last name (Required):** Jones
- Email (Required):** mjones@bank.com
- Phone Number:** Three fields for Country (+1), Home, Mobile, and Work, all with US/Canada as the default country.

The second screenshot shows the 'Create your Treasury Bank ID credentials' screen with the following fields:

- Username:** mjonesuis
- Password:** (masked with dots)
- Confirm password:** (masked with dots)

A blue arrow points from the first screen to the second.

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

The first screenshot shows the 'Protect your Treasury Bank ID with 2-step verification' screen with the following text:

- 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.

The second screenshot shows the 'Choose your Treasury Bank ID verification method' screen with the following options:

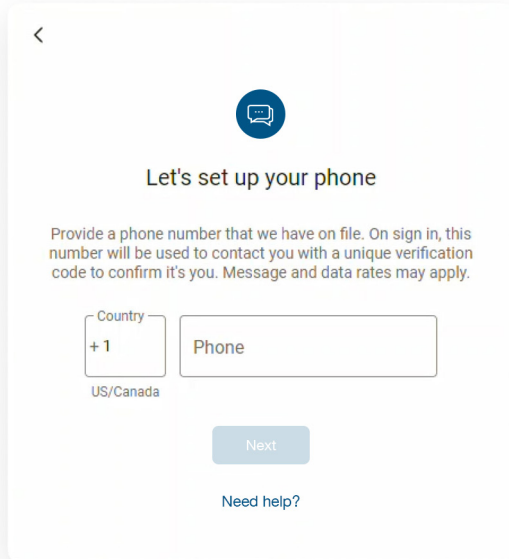
- Voice or text message**
Verification codes are sent to your phone.
- Authenticator app**
Using a different authenticator app? We support using any authenticator app using either a QR code scan or manual code entry.
- Symantec VIP**
Use Symantec VIP authentication to sign into your account. We support digital and hard tokens.

A blue arrow points from the first screen to the second.


2-Step Verification Methods

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

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.

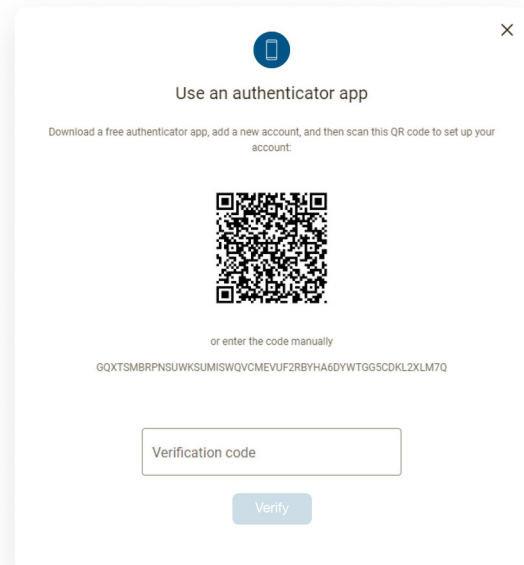
Country
+ 1
US/Canada

Phone


Next

[Need help?](#)

Authenticator app




< X



Use an authenticator app

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

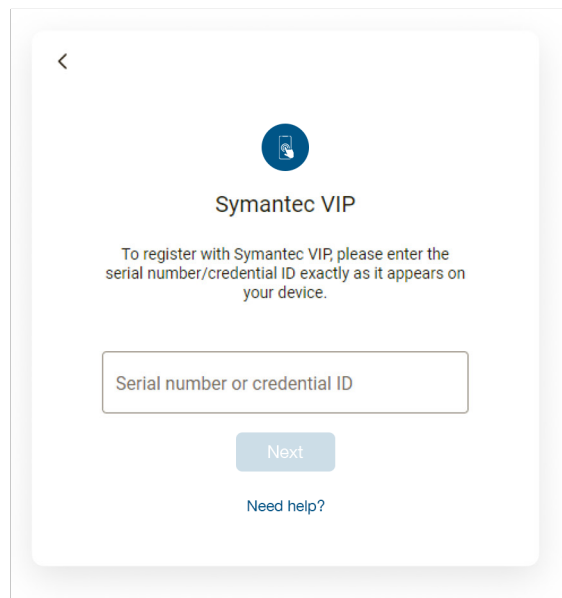


or enter the code manually
GQXTSMBRPN SUWKSUMISWQVCMEVUF2RBYHA6DYWTGG5CDKL2XLM7Q


Verification code

Verify

Symantec VIP



<



Symantec VIP

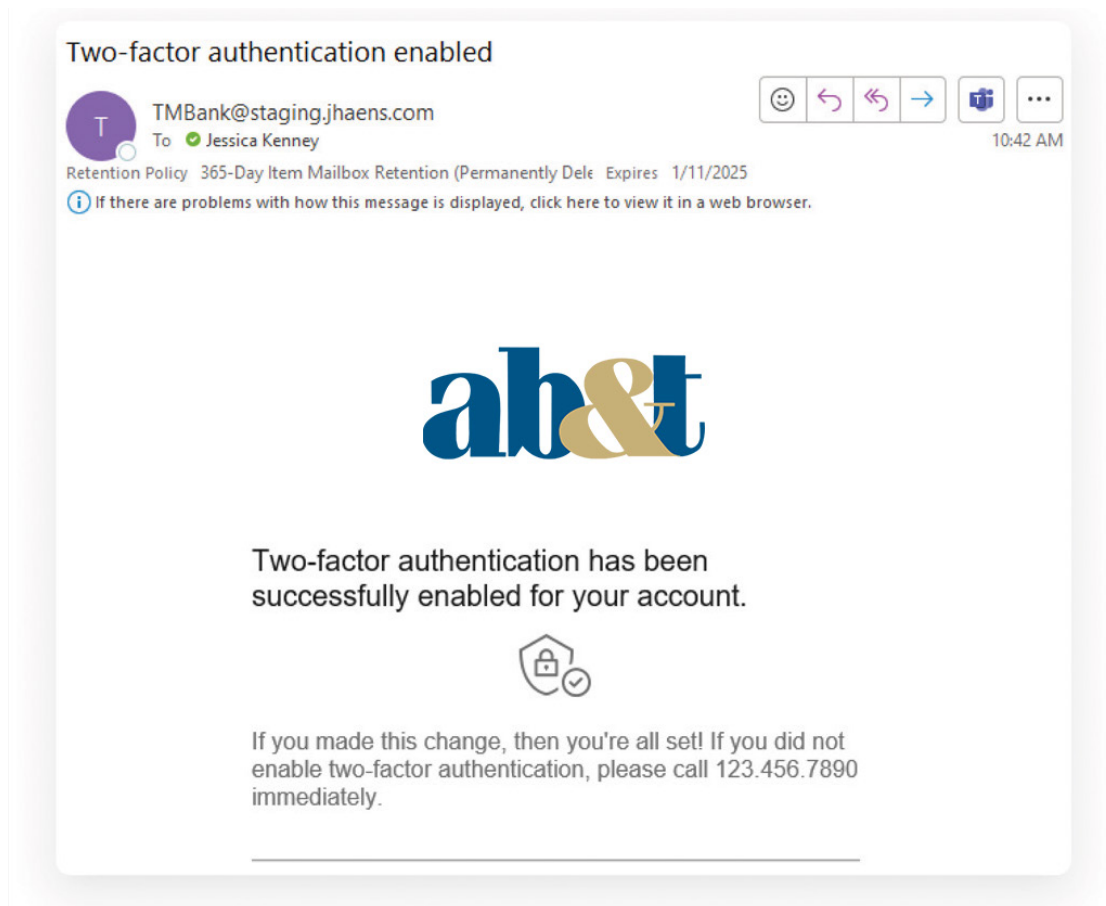
To register with Symantec VIP, please enter the serial number/credential ID exactly as it appears on your device.

Serial number or credential ID

Next

[Need help?](#)

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



See it in action!

For more information about the reenrollment process, including a brief video example of creating the Digital Identity, visit our Treasury Management resource page at [AB&T - Business Banking - Business Management Tools - Treasury Management](#).

Frequently Asked Questions

Can a user keep their existing username?

It is possible that the user's existing LoginID can be used again, however usernames now need to be unique across the entire database. In many cases a new username will have to be chosen.

What if the user logs into multiple companies?

During migration, each user 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 outline 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. Upon entering their Digital ID their accounts will be linked together under that Digital ID. Upon subsequent logins the user will get to chose which company they want to access.

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), 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, accented letters, ampersands (&), equal signs (=), brackets (<, >), plus signs (+), at signs (@), or commas (,).

What are the new rules for creating a password?

Passwords must be between 8 and 64 characters in length.

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

Passwords 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 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 enabled with the UIS login?

Yes, it can be enabled. 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. Additionally, users that integrate with Intuit services (Quickbooks Online/QBO/Express Web Connect) will need to elect this feature for the third-party service to work successfully.

We're here for you every step of the way!

We hope that you are 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.

Call us at **(229)405-7214** or email at **madison.chapman@abtgold.com**.

As always, thank you for trusting us to serve you!

