

Unified identity service (UIS)

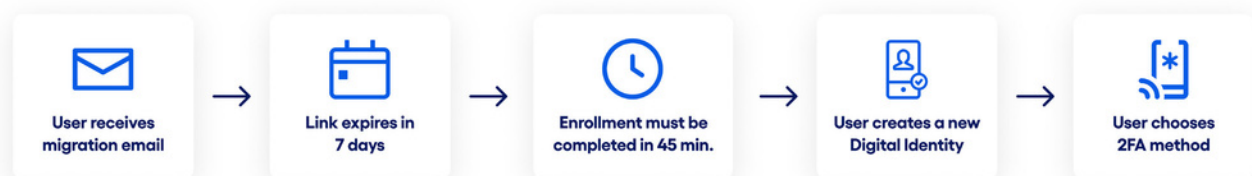
Unified Identity Service (UIS) for Treasury Management is a replacement solution to Outseer's (formerly RSA) Multifactor Authentication. UIS aligns with Bank of San Francisco's strategic direction for platform security by employing modern OAuth 2.0 authentication protocol. We recognize that transitions like this can be difficult, and often bring about new challenges. 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 provided a step-by-step guide to the user experience here to get you started:

User experience

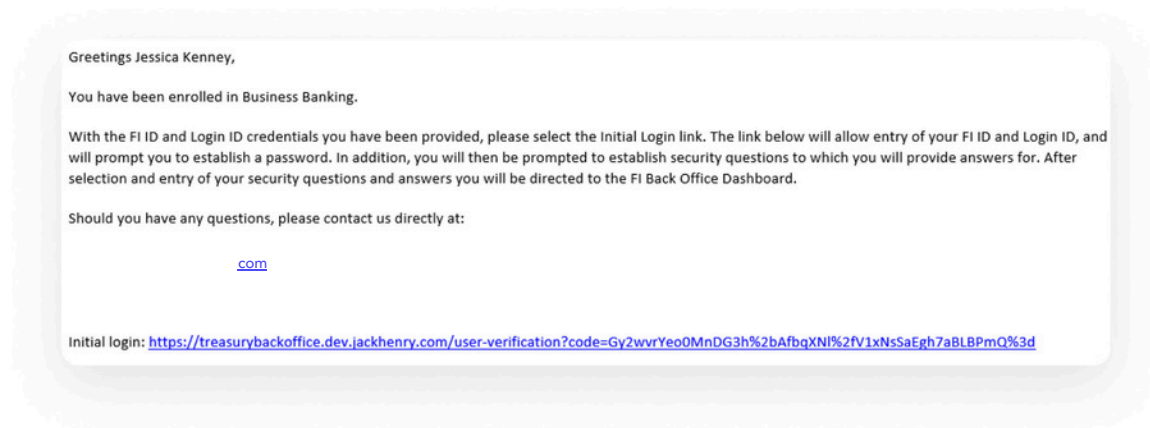
What should users expect during the migration to UIS?

- Users who are in an active status and have logged in 45 days prior to the 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 Bank of San Francisco.
- 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 Bank of San Francisco 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.



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

The diagram shows two 'Login' forms. The first form has input fields for 'Company ID' and 'Login ID', both with placeholder text 'Enter [ID]'. The second form, reached via a blue arrow, has the same fields but is pre-filled with 'Foxtrot' for Company ID and 'mjones' for Login ID. Both forms include 'Submit' and 'Reset' buttons.

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

The screen displays the Bank of San Francisco (BSF) logo and the text 'BANK OF SAN FRANCISCO'. Below this is a message: 'Create your Treasury Bank ID to establish your account access.' A green 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 users to 'Login to link an additional account.' It includes a 'Username' input field, a 'Forgot?' link, and a 'Continue' button.



- 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 screen, titled "Create your Treasury Bank ID" with the subtitle "Verify your profile information", features the BSF Bank of San Francisco logo and a green arrow icon. It includes a green box with a checkmark icon and the text "Create your Treasury Bank ID to establish your account access." Below this, there are input fields for "First name (Required)" (filled with "Madelyn"), "Last name (Required)" (filled with "Jones"), "Email (Required)" (filled with "jkenney@jackhenry.com"), and "Phone Number". The phone number section has three rows for "Home", "Mobile", and "Work", each with a country code dropdown (set to "+1") and a text input field. A green "Next" button is at the bottom.

A blue arrow points to the second screen, titled "Create your Treasury Bank ID credentials". It also features the BSF logo and a green arrow icon. It includes a green box with a checkmark icon and the text "Create your Treasury Bank ID credentials". Below this, there are input fields for "Username" (filled with "mjonesuts"), "Password" (filled with "*****"), and "Confirm password" (filled with "*****"). There are "Show rules" links between the password and confirm password fields. A green "Next" button is at the bottom.

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

The first screen, titled "Protect your Treasury Bank ID with 2-step verification", features a green shield icon. It includes a green box with a checkmark icon and the 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." Below this, there are two sections: "Add an extra layer of security" with a lock icon and the text "Enter your password and a unique verification code.", and "Keep the bad people out" with a person icon and the text "Even if someone else gets your password, it won't be enough to sign into your account." A green "Get started" button is at the bottom.

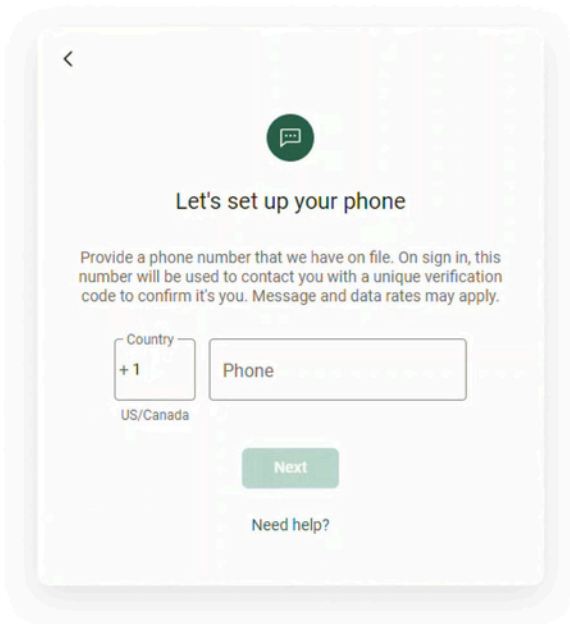
A blue arrow points to the second screen, titled "Choose your Treasury Bank ID verification method". It features a green shield icon. It includes a green box with a checkmark icon and the text "Choose your Treasury Bank ID verification method". Below this, there are four options, each with an icon and a description: "Voice or text message" (message icon) with "Verification codes are sent to your phone.", "Authenticator app" (phone icon) with "Using a different authenticator app? We support using any authenticator app using either a QR code scan or manual code entry.", "Symantec VIP" (VIP icon) with "Use Symantec VIP authentication to sign into your account. We support digital and hard tokens.", and "Security key" (key icon) with "Use a hardware token to authenticate." A green "Next" button is at the bottom.



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.

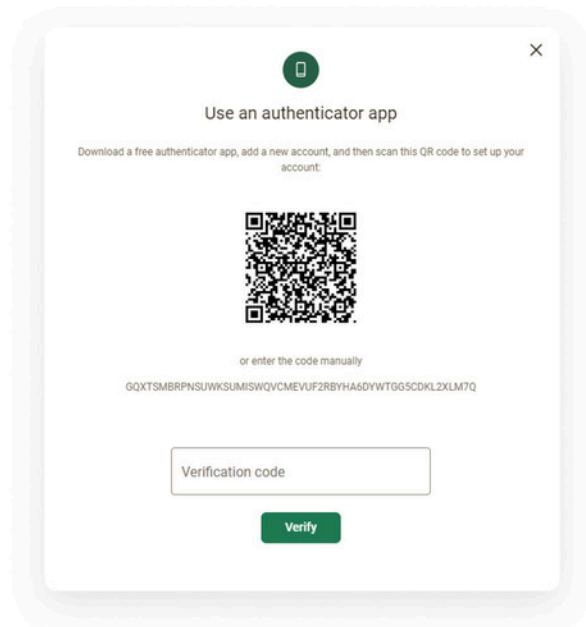
Country
+1
US/Canada

Phone

Next

Need help?

Authenticator app



Use an authenticator app

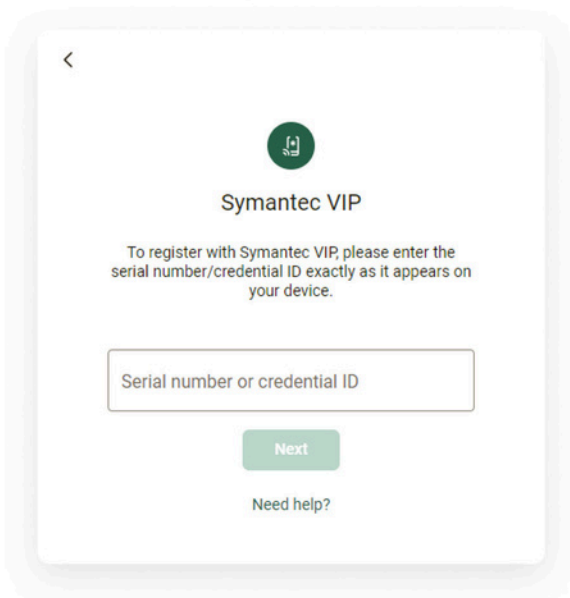
Download a free authenticator app, add a new account, and then scan this QR code to set up your account.

or enter the code manually
GQXTSMBRPN SUWKSUMISWQVCM EVUF2RBYHA6DYWTG65CDKL2XLM7Q

Verification code

Verify

Symantec VIP



Symantec VIP

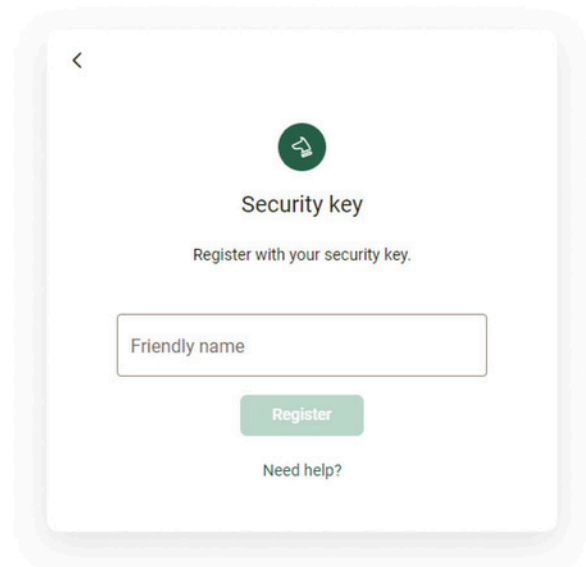
To register with Symantec VIP, please enter the serial number/credential ID exactly as it appears on your device.

Serial number or credential ID

Next

Need help?

Security key



Security key

Register with your security key.

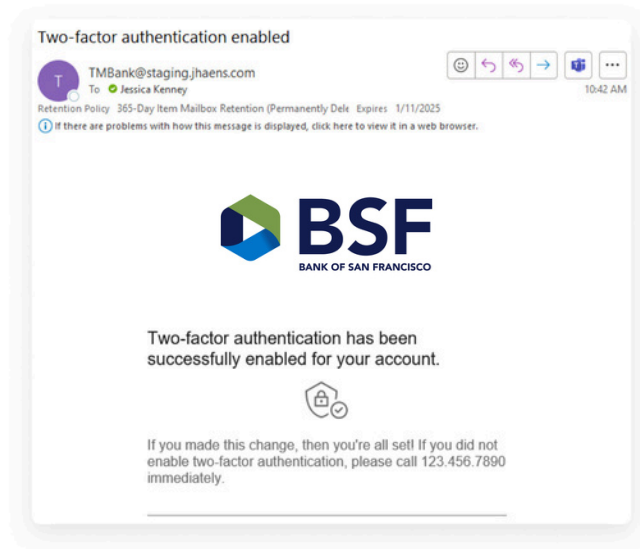
Friendly name

Register

Need help?



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



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. Call us at 415-744-6700 or email at digitalbanking@bankbsf.com. As always, thank you for trusting us to serve you!

