Digital Banking Platform

security enhancement frequently asked questions

In response to the many questions we received during our special-edition Digital Security Meetup with Ben Metz and Chad Killingsworth on January 24, 2025, we have prepared this extensive FAQ document to provide a more comprehensive understanding of the changes.

scope of document and related enhancements

Which security enhancements do these FAQs address?

As part of our initiative to continuously enhance security for Banno™, we have been working hard to release the following security-related features that help Banno customers fight fraud. These enhancements come at no additional cost to your financial institution.

- **Block high-risk actions on new devices**: This feature, which is available for all financial institutions today, enables your financial institution to restrict newly registered devices from performing high-risk actions (HRAs) on end users' accounts until the device is manually unblocked by an authorized employee of your financial institution.
  - » **Anchor device verification (Coming soon)**: When this feature becomes available, accountholders will be able to use an anchor device to unblock a new device they're using, thereby removing the need for your support staff to manually verify end users on the phone to unblock devices. This feature is coming very soon, so watch our Monthly Digital Statement for more information!
- **Enhanced Default 2FA methods**: This feature allows your financial institution's authorized personnel to configure which 2FA methods your financial institution requires. The improved configuration options are based on three levels of security – Standard, Enhanced, or High – that you can control based on user type. For example, you can configure one level of security for retail users and another level for business users.

- **2FA for high-risk actions**: This feature, which recently rolled out to all financial institutions on February 6th, gives your authorized administrators the option to require 2FA – rather than a password – for high risk actions. This means you can enforce an alternative security measure (e.g. tokens, passkeys) for adding external accounts, transferring funds, and other activities that could present a risk to your financial institution and end users. Please note, your institution must be on app version 3.19 or above to utilize 2FA for high-risk actions.

For more information, you can access the recording of our special Digital Security Meetup webinar in which we address these features via the For Clients Portal. In addition, remember to check out our Digital Monthly Statement for the latest status updates about upcoming features.

Which environments do these enhancements affect?

The security settings covered in this document affect the Banno Digital Platform™.

The following security settings also affect JHA Treasury Management™ – if your financial institution has already migrated to Unified Identity Service:

- **Enhanced Default 2FA:** This applies to Treasury Management users for enrollment, login, and account recovery.
- **Changing 2FA settings:** Any changes your financial institution makes to 2FA settings, including resetting 2FA for a user, apply to Treasury Management as well.
- ***Manage security settings* permission:** This setting for Users & Groups also gives your financial institution admins access to Treasury Management security settings.
- **2FA for high-risk actions:** Specific actions apply to Treasury Management users.
  - » Change username and password (end user actions)
  - » Change address, change email, remove device (end user actions)
  - » Edit username, edit user address, edit user email, edit user phone number, reset 2FA, remove device (these end user actions, which can be edited on Banno, also take effect in Treasury Management)

Your financial institution's authorized personnel can manage certain corresponding security settings in Banno People™ or the newly released Identity App. Note that adopting the baseline offering of Unified Identity Service starts to bridge the Banno and Treasury Management environments – letting Treasury Management leverage the security protocols that we have in place for the Banno Platform today.

high-risk actions

This section includes questions and answers related to high-risk actions.

What is considered a high-risk action?

Jack Henry defines a high-risk action as any method that allows an attacker to modify or add information in a way that enables the unauthorized transfer of funds from a financial institution. This includes any profile changes (e.g. email, phone number, contact details) as well as actions that enable external payments.

Is there reporting around high-risk actions?

Not yet; however, we are working on providing you with reports around high-risk action blocking and are currently aiming to make this reporting available later this quarter.

Are there plans to add to the index of high-risk actions?

We have had a lot of really great dialogue with customers as we have been communicating the release of the new enhancements. The potential risks associated with the actions listed below are becoming increasingly apparent.

Based on the feedback we received during the special Digital Security Meetup, we will commit to working toward making the following items high-risk actions:

- Member-to-member transfers
- Travel notices

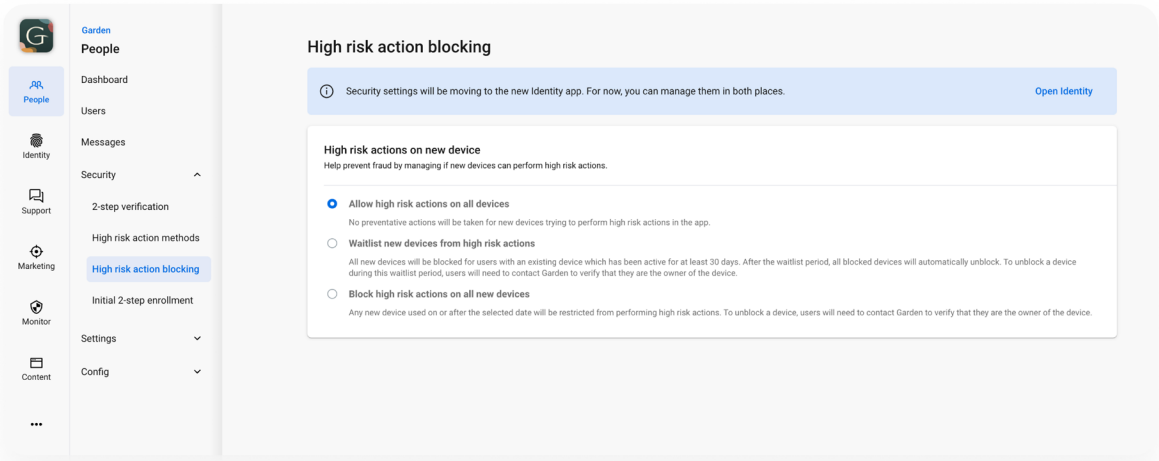
To view our index of high-risk actions, check out the Security page on the Knowledge Base.

high-risk action blocking

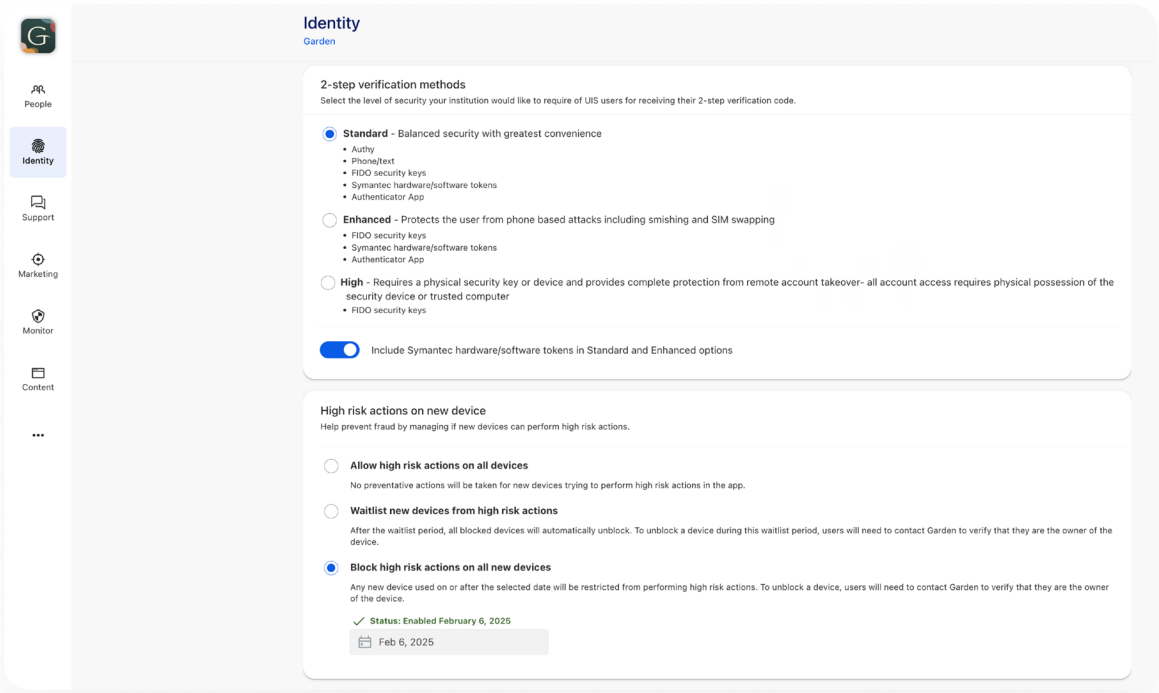
This section includes questions and answers related to high-risk action blocking on new devices.

How is high-risk action blocking enabled and managed?

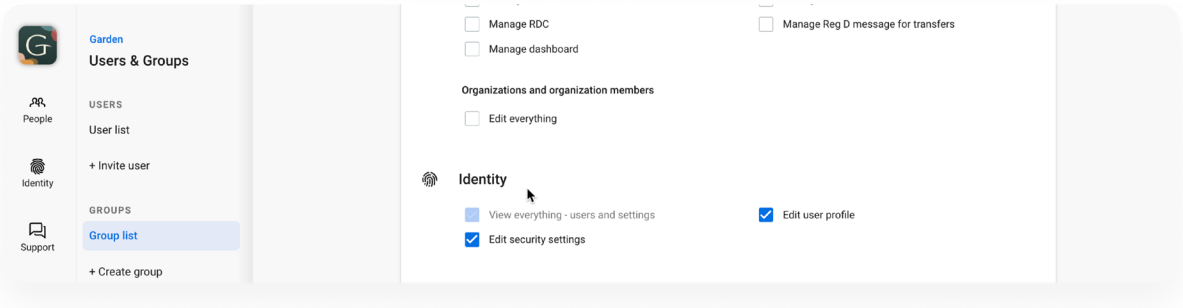
In Banno People, authorized admins (those with the *Manage security settings* permission) can manage this setting on the *high-risk action blocking* screen – accessed via the new *Security* menu.



In the Identity App, authorized admins (those belonging to a group with the *Edit security settings* permission*) can manage this setting on the *Settings* screen – accessed from the Identity App landing screen.



The *Edit security* settings permission required to manage Identity settings is located in the *Identity* section of Group permissions:



You can find documentation on high-risk action blocking on the Knowledge Base.

What about new end users who are self-enrolling?

The experience for net-new end users differs based on the option selected for the *high-risk actions on new device* setting:

- *Allow high-risk actions on all devices:* This option lets net-new end users self-enroll and then perform additional high-risk actions as well.
- *Waitlist new devices from high-risk actions for 7 days:* This option allows net-new end users to self-enroll and perform high-risk actions on their initial device. However, additional devices will be blocked from accessing the user profile unless the original device has already completed a high-risk action after the waitlist period.
  - » Additionally, when a new device is introduced for an existing user (i.e., one who already has a device registered for over 30 days), that new device is prevented from performing high-risk actions for a period of 7 days, unless the user contacts the financial institution to manually unblock it.
- *Block high-risk actions on all new devices:* This option blocks devices of net-new end users who self-enroll.

At what point is a new device no longer considered a new device?

With the waitlist mode of our high-risk device blocking feature, the default is set to seven days; however, your institution may configure this number up to thirty days.

Is blocking high-risk actions on new devices organization-wide or can it be segmented by user groups?

Currently, these settings are organization-wide. However, we will continually explore evolving the settings to give your financial institution more granular control. Stay tuned to our recurring Digital Banking Meetups and Monthly Digital Statements for any future updates.

How does blocking high-risk actions on new devices impact financial institutions using NuDetect?

NuDetect will continue operating as it does today. If an end user is on a new device and attempts a high-risk action, Banno will block the action until it has been unblocked by your financial institution.

In general, high-risk actions are sent to NuDetect for scoring and may be blocked based on the threshold your financial institution has configured.

How does high-risk blocking affect end users who utilize private browsers and clear cookies and/or cache?

When end users utilize private browsers (or clear their cookies and/or cache), they are removing all indicators Banno can use to 'trust' the device. End users who take any of these approaches will be blocked from high-risk actions on every login.

To mitigate this, we have rolled out a FIDO token capability that allows Jack Henry to trust devices that utilize FIDO keys as their 2FA method.

Will trusted devices be impacted by software updates?

A software update doesn't typically register as a new device. While there may be exceptions, it generally won't cause friction with high-risk actions.

Can a financial institution manually verify a device if needed?

Yes, an admin will be able to enable a device in Banno People. However, it's crucial to have proper verification measures in place to ensure customer identity before proceeding.

Can financial institutions use a predefined list to select which high-risk actions get blocked?

Enabling blocking of high-risk actions will block all high-risk actions; it's not possible to customize that list today. We will continue exploring enhancements to this process in the future.

Are there any plans to give financial institutions the ability to utilize geolocation blocking?

Yes! We are looking into located-based blocking. Stay tuned to our Monthly Digital Statements for more information on enhancements.

Is there an index that lists all the actions that are considered high-risk actions?

Yes! We have this documented on the *Security* page of the Knowledge Base under High-risk actions.

anchor device verification Coming Soon

What is the criteria that helps determine whether an anchor device is trustworthy?

While we can't disclose the specific methods used due to security reasons, we employ multiple factors to verify device trustworthiness. As fraud tactics evolve, we will continuously enhance our security measures to protect customer accounts and maintain trust at the device level.

Will notifications be sent in real-time to anchor devices?

Yes, if the user has push notifications enabled, the anchor device will receive a real-time notification – ensuring the user is promptly alerted.

Will financial institutions get a notification when a device has been deauthorized?

While your financial institution will record this activity in the user's account history, there is currently no real-time notification sent when a device is deauthorized.

What is the new device is a desktop and not a mobile device?

We also have other verification flows in place based on levels of trusts for devices. If the level of trust is high enough, simpler verification flows are in place to ensure two browsers are able to complete the verification flow.

initial 2-step enrollment

This section includes questions and answers related to initial 2-step enrollment.

How will email validation work during first time enrollment in 2-step verification?

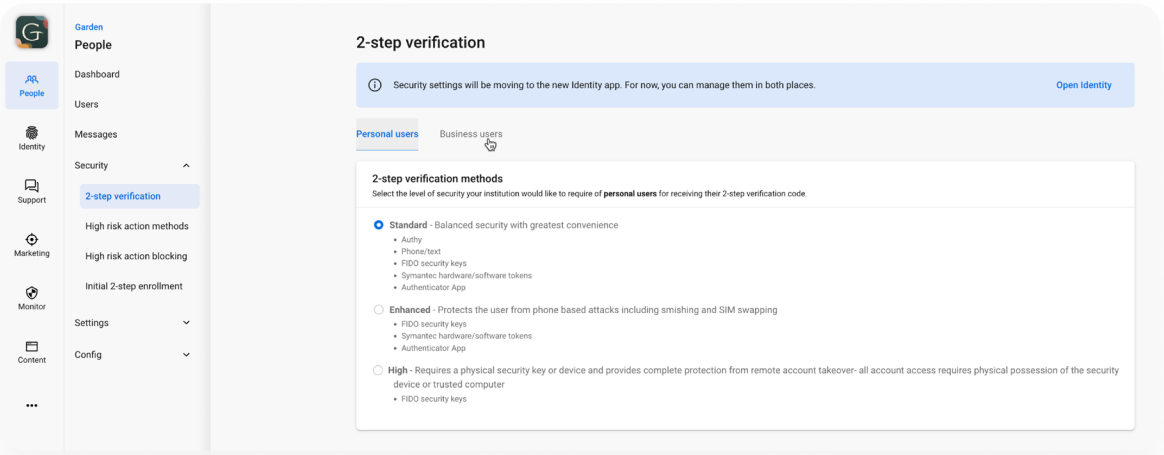
If your institution requires email validation during first-time enrollment in 2-step verification, end users will need to verify their identity with a single-use password sent to the email address on file. This applies only to the initial enrollment in 2-step verification and is unrelated to the email option in code delivery methods.

What about end users who do not have email?

Your financial institution will have a user-level override for this within your security settings. This setting can be managed on a user-by-user basis or kept in sync with your institution-level settings. For example, this can be turned "on" at the institution level, but turned "off" at the user level.

Enhanced Default 2FA

This section includes questions and answers related to the Enhanced Default 2FA functionality (i.e. 2-step verification).



What about the migration to ENS for sending 2FA codes?

Please see our updates to 2FA code delivery FAQ for details on the migration to ENS.

Does the new *Standard* security level auto-enable other 2FA methods for business users who were previously restricted to FIDO tokens?

No, the new *Standard* security level does not automatically enable additional 2FA methods for business users. At rollout, your financial institution's default 2FA was set at the *Standard* level, which includes more 2FA methods than the *Enhanced* and *High* levels. However, end users must actively choose to enroll in those additional methods.

The enrollment process does not auto-enable FIDO tokens (or any previously used methods, except for email and Symantec tokens for end users who were already enrolled in those). Instead, the method is presented as an option should the end user be prompted to re-enroll in 2FA – such as when their device is completely cleared – or if they are a new user enrolling for the first time. Additionally, end users can manually enroll in these new methods by navigating to their security settings.

Therefore, we recommend that your authorized admin do **one** of the following:

- Set institution-wide security levels: Configure the security level for *Business users* at the institution level, right away, to ensure the available methods meet your security requirements.
- Apply user-level overrides: Configure user-level overrides for specific end users (via the *Security* tab on their user profile in either Banno People or the Identity App).

How do the new default 2FA security levels impact business users who are currently restricted to using only Symantec tokens for 2FA?

Symantec tokens can remain an option for end users, so long as an authorized admin from your financial institution selects either the *Standard* or *Enhanced* security level on the *Business users* tab. Along with Symantec tokens, end users will also have the option to use the other 2FA methods included in the *Standard* or *Enhanced* level.

We have migrated user-specific overrides as a part of our rollout to include those currently enrolled in Symantec tokens. If you're looking for the highest level of security for business users, you will want to select *High* for that user type (on the *Business users* tab of *2-step verification* screen in Banno People) or for specific business users (on the *Security* tab of the individual end user's profile).

FIDO tokens vs. Symantec tokens

FIDO tokens are a more-secure level of 2FA security and are not shareable, unlike Symantec tokens. You'll want to coordinate with business users before enforcing the highest level of 2FA security, as the change would require the end user(s) to purchase a FIDO token that meets Banno's security requirements.

Before the new default 2FA rollout, restricting 2FA methods to Symantec tokens was necessary for certain business users – e.g. those with ACH origination, wires, or high bill pay limits – who required the highest level of security. However, *now* the highest level of security available is FIDO tokens, because unlike Symantec tokens, it is not possible to share FIDO tokens.

How do passkeys compare to FIDO tokens in terms of trust?

A FIDO token is a security key or device used for 2FA that you tap or plug in to verify your identity. A passkey is a FIDO authentication credential based on the FIDO2 standard, designed to provide secure, passwordless authentication for websites and apps. Passkeys are phishing-resistant, tied to the end user's device or cloud-synced keychain, and offer a high level of security similar to FIDO security keys.

Are passkeys available for Banno Mobile?

Passkeys are not yet available on the Mobile app, however, we are working to get it prioritized. Stay tuned to future announcements for updates on this.

Does default 2FA affect financial institution employees?

No, the Enhanced Default 2FA functionality does not apply to your authorized admins (financial institution employees).

Are there any safeguards for default 2FA to prevent members from sharing their authentication code with a bad actor?

The most effective way to prevent end users from sharing their 2FA codes – with *anyone* – is to enforce a higher security level. The *High* security level, which specifically requires FIDO security keys, is the only method that eliminates the risk of code sharing, as it does not rely on one-time passcodes that can be easily shared.

Was email enabled as a verification method for all financial institutions during the Enhanced Default 2FA rollout?

Financial institutions that were already enrolled in email verification will be seamlessly migrated during the rollout. Email 2FA remains a supported option; however, its use requires signing off on indemnification due to the associated risks.

transitioning from Authy

Will the Authy app still qualify as a 2FA method?

No, the third-party provider supporting Authy is phasing out the platform, requiring us to transition end users to alternative methods. The overwhelming majority of Banno end users already rely on SMS and voice for 2FA, and these methods will be seamlessly migrated to the ENS platform.

What is the approach for removing Authy?

The removal of Authy will occur in two phases:

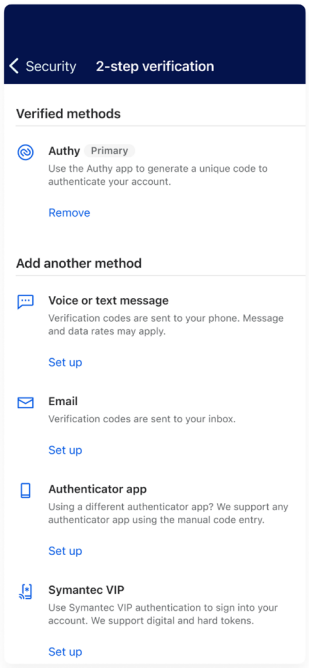
1. **Disabling new enrollments:** Authy will no longer be available as a new 2FA method, but existing enrollments will remain supported.
2. **Migrating existing Authy users:** Current Authy enrollments will be transitioned to the Banno OTP method, eliminating the need for end users to re-enroll.

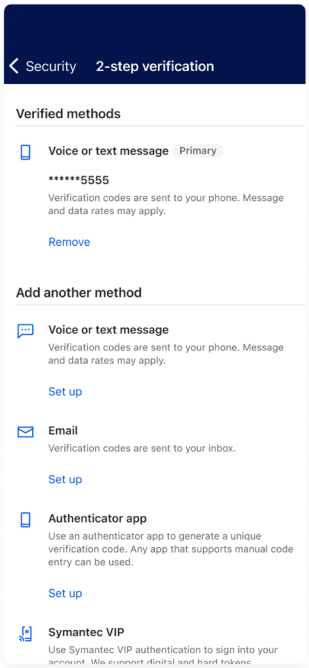
Will end users need to re-enroll in 2Fa on their next sign-on?

If the end user did not have Authy as an enrolled option, nothing changes for their experience. If the end user was enrolled in *only* Authy, that option will simply go away and by default, we will migrate this enrollment to the Banno OTP method. This method will be present with one or multiple numbers that are enrolled.

Please note that as part of this project, Jack Henry will handle the Authy-to-OTP migration for end users currently enrolled in Authy. This transition will have minimal user impact and will not disrupt authentication.

Before Removing Authy





After Removing Authy

Is it possible to identify which end users receive 2FA codes via the Authy app rather than SMS?

Unfortunately, no. The Digital team is unable to identify the specific end users who authenticate using the Authy Mobile Application; we only retain knowledge of the number of end users who have established Authy as a 2FA method. We have access to the number of end users who user Authy, but we do not know anything further about the individual end users themselves.

What about international phone numbers?

As of right now, the cores do not have a good way of supporting international phone numbers. So there will need to be a core-supported phone number (US format) for initial user enrollment and account recovery.

Does removing Authy have any impact on established account aggregator connections (Plaid, Finicity, Yodlee, etc.)?

There should be no impact whatsoever.

What authenticator apps can be recommended to replace Authy?

Your end users can continue using Authy; they just need to manually register is as their authenticator app. Google Authenticator is also a viable option. Additionally, end users on iOS can leverage the built-in authentication functionality on their iPhones.

Are there any options end users can use that lets them share login credentials and 2FA codes with a trusted family member?

There is no reason to share credentials, and we strongly recommend against any sharing of credentials. However, if they do, we recommend they set up multiple 2FA phone numbers which are supported today.

other customer questions from the January Digital Security Meetup

During the Digital Security Meetup, customers asked (some variation) of the following questions.

What about masking account numbers?

This is not possible today, due to a Dodd-Frank 1033 requirement that the account number for anything that is ACH enabled has to be shared via the APIs. Additionally, the account number will still be available via OFX downloads. However, we hear all your feedback and this is something we will take under advisement to give your institution more control.

Is there more information available for brand protection integrations?

For more information on our alliance with third-party brand protection integrations, check out the Additional Integrations page on the Knowledge Base.

Are business users for Banno defined as digital IDs that are Cash Management in SilverLake or customers with a TIN vs. SSN?

Banno Business users are digital-only users and represented by Cash Management useers in SilverLake. Banno does not collect or have a TIN or SSN for these end users.

we're here for you every step of the way

If you have any questions, please open a case via the ForClients Portal.

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