Digital Banking Platform

updates to 2FA code delivery

With so many great security improvements coming your way in the next few months, we have prepared this extensive FAQ document to provide a more-comprehensive understanding of the changes, including the upcoming migration to our ENS (Enterprise Notification System) platform.

2FA, ENS, and the pending migration

What is 2FA?

Two-Factor Authentication (2FA) provides an extra layer of security to authenticate users when logging into their account. 2FA requires something the person knows (like a password) and something the person has (like a code sent to their phone).

A 2FA code is a temporary code consisting of a short string of numbers or a token sent to the user's phone or generated by an authentication app. After entering their password, the user enters the temporary 2FA code as the second authentication step to prove that it's really them attempting to login.

The Banno Digital Platform™ requires 2FA for a few scenarios. To learn more about how 2FA protects your financial institution and your end users, check out this Knowledge Base article.

What is ENS?

The Enterprise Notification System (ENS) is our centralized platform designed to send critical notifications and communications across an organization. It is a contracted platform for Banno customers that ensures that the appropriate person or systems receive timely and relevant information about events, alerts, or updates.

What's changing?

Currently, Banno utilizes a third-party integration to send 2FA codes. We are migrating the method of delivery of these 2FA codes from this third-party integration to ENS. This migration, driven by the release of several security enhancements detailed below, reflects our ongoing commitment to delivering top-tier security features in a sustainable and efficient manner.

This migration will increase the number of SMS messages sent through ENS, and that will be reflected in the cumulative ENS fees for your financial institution, in accordance with your existing ENS contracts.

Which security enhancements are driving this migration?

As part of our initiative to further enhance security for Banno, we have been working hard to release the following security-related features to help Banno customers fight fraud at no additional cost to your financial institution:

- **Block high-risk actions on new devices**: This feature, which will be available for all financial institutions upon its release, will enable your financial institution to restrict newly registered devices from performing high-risk actions on user accounts until the device is manually unblocked by an authorized employee of your financial institution.
- **Enhanced default 2FA methods**: This feature will allow 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 will give your authorized administrators the option to require 2FA – rather than a password – for high-risk actions. This means that you can enforce an alternative security measure (e.g. tokens, SMS) for adding external accounts, transferring funds, and other activities that could present a risk to your financial institution and users.

How will this migration benefit financial institutions?

The migration of the delivery of 2FA codes from a third-party integration to ENS offers several key benefits:

- **Consolidation**: All Jack Henry notifications, including SMS messages, alerts, and 2FA codes, will be sent from a single dedicated phone number for each financial institution (or short code, if the financial institution has established a short code through ENS). For example, when a user receives a balance notification, it will come from the same phone number that their 2FA notifications come from, and that phone number will belong to your specific financial institution.
- **Additional security**: Because all alerts will originate from your dedicated phone number, end users can more easily differentiate the legitimate alerts you send from any fraudulent alerts sent from a bad actor's phone number.
- **ENS dedicated short code**: Your financial institution will have the option to contract for ENS dedicated short codes to establish a unique short code for your financial institution to deliver all alerts, including 2FA login codes.
- **Potential for branded messaging**: This migration paves a path to offer RCS (Rich Communication Services) messages at a later date.

  - RCS is an encrypted messaging protocol designed to provide a sleeker, more-engaging experience without leaving the messaging app built into the end user's smartphone.
  - Embracing ECS will let our team build ways to engage with your users in a more meaningful way. Depending on carrier support, RCS will position us to – eventually – offer adoption-driving capabilities such as branded sender IDs, rich media, and interactive content.
- **Enhanced visibility**: Jack Henry has better visibility into 2FA codes sent by ENS, which let us provide better customer support if an end user doesn't receive their 2FA code (i.e. finding the reason that the code wasn't received).

When will the migration occur?

We are targeting to begin sending 2FA codes through ENS in February 2025.

How should we prepare for the migration to ENS?

No action is *required* from your financial institution regarding this change. This migration will be seamless for the vast majority of users. You may, however, want to inform users that they might be prompted to set up a new 2FA method in Banno, as further detailed in the 'Authy' section directly below.

transitioning from Authy

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

The third-party provider supporting Authy is phasing out the platform, thereby requiring us to transition users to alternative methods. The overwhelming majority of Banno end users rely on SMS and voice for 2FA, and those methods will be seamlessly migrated to the ENS platform.

The small percentage of users (less than 1%) who rely on the Authy app will, however, need to set up a new 2FA method within Banno. If these users prefer to continue using the Authy app, they still can; they will simply need to manually register it as an Authenticator app in Banno which is available today.

Can we identify which end users receive 2FA codes via the Authy app rather than SMS?

Unfortunately, no. The Digital team is unable to identify the select users who authenticate using the Authy Mobile Application; we only retain knowledge that a user has established Authy as a 2FA method.

When will the migration away from Authy occur?

This migration from Authy will coincide with the (separate) move to ENS, in February 2025.

Should we enable authenticator apps as a 2FA method?

Yes. In fact, authenticator apps will be included in both the Standard and Enhanced security levels once we release the Default 2FA methods feature.

Does this affect our 2FA options for international users?

We will handle the identification of international numbers for your financial institution and default to Authy for the short term. We will then follow up with support for international numbers in ENS during the first few months of 2025.

impact on short codes

Will our existing short code work for sending 2FA codes?

Any existing short codes that are already working with ENS will continue to work. The simplest way to verify whether your financial institution has a short code that works with ENS is to check your ENS contract for "Enterprise Notifications System (ENS) Dedicated Short Code."

If you have an existing short code that is **not already working with ENS**, your financial institution will need to provide it to the ENS team (by opening a case via the For Clients Portal and selecting the *EI&S Shared Services provider* group), so we can add it to ENS. To order a net-new short code for ENS, please reach out to your account executive and request a proposal for "Enterprise Notifications System (ENS) Dedicated Short Code" so they can get the ball rolling.

Once your team reviews the proposal and returns the signed contract addendum, we, Jack Henry, will begin the process to submit and manage the short code campaign for you. Typically, new short code campaigns are approved within 6 to 8 weeks after submission.

Is our existing short code exclusive?

If your ENS contract includes the line item "Enterprise Notifications System (ENS) Dedicated Short Code," that code is unique to your financial institution. Note that short codes are not required, as your ENS contract includes a unique long code consisting of a 10-digit number.

additional questions

Will the new default 2FA methods work for high-risk actions?

Yes, the enhanced default 2FA methods will be made available as a configurable option for high-risk actions.

Will any of the upcoming changes to 2FA affect Banno Admin apps?

No, we aren't currently making any 2FA changes to Banno People™, Banno Support™, Banno Marketing™, Banno Monitor™, Banno Content™, or anything accessed via the ••• (More) menu in Banno Admin – all of which will still support sign in via the Authy app for now. We will, however, be updating the 2FA options for those applications in the future.

Does the blocking of new devices impact the ability to connect with third-party aggregators?

No. Device blocking only applies to high-risk actions. The release of the 2FA for high-risk actions feature will not impact a users' option to connect third-party aggregators.

we're here for you every step of the way

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

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