EXOSTAR
Together We Thrive

Secure OTP (SOTP)

Release Notes

Version 3.7.1 | August 27, 2026

Defects

- Fixed an issue where the name change page did not function correctly during the Identity Proofing process, preventing users from updating their name before completing proofing.
- Fixed an issue where Hardware OTP token binding failed intermittently due to tokens entering a suspended state in the SAS server. The system now automatically handles orphaned SAS bindings during token activation.
- Updated the support message displayed when a user has a Hardware OTP token as their only authenticator to accurately describe the replacement token process and account revocation requirements.
- Fixed an issue where SAML assertions returned through EAG contained an incorrect credential type. When a customer authenticates using a passkey, the assertion now correctly returns "passkey" instead of "password".

Version 3.7.0 | May 28, 2026

Features and Enhancements

- Stood up a dedicated Secure OTP (SOTP) environment to support MAG independently, enabling separate deployment and release cycles for each platform.

Version 3.6.0 | May 15, 2026

Features and Enhancements

- SOTP now supports the U.S. Person Verification (USPV) service, a webcam-based identity and citizenship verification capability. Applicants can complete the full verification journey online: review a service preamble, accept a consent form, upload an Employment Verification Letter (EVL), confirm their personal details, and schedule a live webcam session with an Exostar verification agent. Appointment confirmation and rescheduling instructions are delivered to the applicant by email.

- SOTP exposes a suite of USPV Service APIs allowing client systems to integrate directly with the service. Client systems can initiate a verification request, resubmit corrected applicant details before an appointment is scheduled, cancel a pending request, and retrieve proofing status and verification results. Clear error responses are returned for all failure conditions.
- The applicant-facing USPV workflow includes a license key entry page, consent form, EVL upload page, a details review and document-selection page, and an attestation form. Applicant data and attestation records are captured and stored for use during the webcam session and for audit purposes.
- Webcam proofers have access to a USPV request inbox within MAG, where they can search for and review incoming verification requests. From a request, proofers can review the applicant's submission, generate an activation code, approve or reject the request, and extend the request expiration date.
- Onboarding specialists have access to a USPV review inbox within MAG, where they can perform a final review of requests approved by a webcam proofer. Specialists can approve or reject the verification. On approval, the applicant's status is set to Verification Completed and the result is made available to the client system via API.
- MAG supports two separate USPV verification queues: Verify USPV MAG for MAG-originated requests and Verify USPV Other/Non-MAG for requests from non-MAG client systems. Onboarding specialists access their queue via the Approve USPV option in the MAG requests tab.
- EPCS signature computation and audit log persistence are now handled within the iam-mfa-mgmt component, maintaining compatibility with the existing EPCS client API contract.

Version 3.5.0 | February 23, 2026

Defects

- The Credential Management page now shows only credentials available under the user's current subscription. Credentials not included in the subscription (e.g., Authy, Mobile ID, FIDO, Hardware OTP) are no longer displayed.
- We have fixed an issue where invalid FIDO authenticators were correctly blocked, but no error message was displayed to the user. Users now see an "Authenticator Not Allowed" message with a link to supported authenticators when a non-approved FIDO device or synced passkey is presented.
- We have fixed a FIDO registration issue where passkey creation failed because the proofing ID was not populated when a credential was bound after proofing. The authenticator is now registered correctly when bound after proofing.
- We have fixed an issue where the FIDO passkey status was not displayed correctly. The "Manage Passkey" label showed a raw resource key string instead of the expected FIDO text due to a missing property file.
- We have fixed an issue where optional credentials (Hardware OTP, Authy) were displayed on the activation page even when not included in the user's subscription, resulting in "Invalid license key" errors when attempting activation.

Version 3.4.0 | October 10, 2025

Features and Enhancements

- FIDO Synced Passkey support.

Defects

- We have fixed an issue where users with active 2FA credentials were not seeing those credentials displayed on the View Details page, even though they were active.

Version 3.3.0 | March 15, 2025

Features and Enhancements

- The Header of all Angular-based SOTP screens has been updated to reflect the latest Exostar branding.
- The Footer of all Angular-based SOTP screens has been updated to reflect the latest Exostar branding.

Version 3.2.1 | April 9, 2025

Defects

- We have resolved the defect where the US citizenship status is not properly set by the application.

Version 3.2.0 | March 7, 2025

Features and Enhancements

- User accounts will be locked after 100 consecutive failed authentication attempts with a hardware token, and you will have to reach out to Exostar support to unlock the account.

Version 3.1.1 | December 12, 2024

Defects

- To prevent issues when binding the hardware token, we will temporarily disable the submit button after a user submits the hardware OTP codes needed to bind a hardware token. This will allow the UI to wait on the backend processes to complete.
- We have resolved the issues with Puerto Rico numbers not being properly set up with Authy.

- We have resolved the issue of the return to client button not being customized as expected with the EHR vendor name.

Version 3.0 | October 18, 2023

Features and Enhancements

- We have included support for an IAL2 compliant remote identity proofing process which we anticipate should have a better pass rate with our users making it easier to proof their identity.

Version 2.13 | July 13, 2023

Features and Enhancements

- To account for changes to Twilio's Authy setup process, we have enhanced the application to allow users to change their email address during Authy registration.
- As part of our continuous improvement to our security posture, we are releasing a minor update that includes retiring support for TLS 1.0 and 1.1 across all solutions. In addition, this release removes support for the ECDHE-RSA-CHACHA20-POLY1305 cipher to better align with security requirements.

Defects

- Resolved the issue where hardware tokens were not fully unassigned from user accounts upon revocation which prevented assigning a new hardware token.
- Fixed the issue that occurs when a user with an unexpired second factor subscription deactivates their subscription.

Version 2.12 | February 27, 2023

Features and Enhancements

- Created a new API that supports system calls from a client to sign a digest without requiring second-factor authentication.
- Updated the code given to a user after webcam proofing is complete or when the user goes through the snail mail option for Experian proofing from an 8-character numeric code to an 8-character alphanumeric code.
- Enhanced Exostar Portal Administrator role to be able to edit token serial for users who are still in the waiting proofing resume state.

- When an Exostar Portal Administrator is searching for users of a particular client who have OTP credentials, the admin is now required to specify the targeted client and is no longer given the option to search for all clients.
- Enhanced Exostar Portal Administrator role to be able to delete user hardware token so that the user can try activating it again.

Defects

- Fixed issue of suspended and deactivated users still having a pending webcam proofing active in the waiting queue.
- Fixed the issue of users being able to submit or accept Terms and Conditions showed during identity proofing multiple times. The button is disabled when an acceptance is in progress.
- Fixed the issue of MAG users with expired OTP identity proofing not being able to revoke their OTP account.
- Fixed issue of emails not being sent to a Google mail or Yahoo mail account.

Version 2.11 | June 2, 2022

Features and Enhancements

- Added the ability to choose to show SFCA terms when a client is configured to use the Register flow.

Defects

- Fixed the issue of when a new ProviderPass customer goes live, SOTP application in Production must be restarted because SOTP SecureForms does not load the new EPCS signing certificate on Soft reload.
- Fixed the error preventing deactivation of a user who never activated the HW Token.
- Fixed JAXBException issue occurring when a user's account has proof only flag set and a call to get the user's credentials is made to the API.
- Fixed issue when binding Authy, the UI does not validate the phone number for the given country selected by the user.
- Fixed issue of SOTP not throwing an error response when a hyphen is used in the first name of an Experian proofing.
- Fixed the issue of a system error being thrown on proofing start due to the proofing profile not being validated against the proof type.