

Shared One-Time Password Release Notes

Version 3.6.0: May 2026

Feature Updates

- 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/FedRAMP for MAG-originated requests and Verify USPV Other/Non-FedRAMP for requests from non-FedRAMP client systems. Onboarding specialists access their queue via the Approve USPV option in the MAG requests tab.

Version 3.5.0: March 2026

Feature Updates

- 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.

Resolved Issues

- 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: November 2025

Feature Updates

- FIDO Synced Passkey Support

Resolved Issues

- 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: July 2025

Feature Updates

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

Version 3.2.1: May 2025

Resolved Issues

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

Version 3.2.0: April 2025

Feature Updates

- 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 2024

Feature Updates

- To prevent issues when binding the Hardware Token, we have temporarily disabled the submit button after a user submits the Hardware OTP codes need to bind a Hardware Token. This will allow the UI to wait on the backend processes to complete.

Resolved Issues

- We have 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: November 2023

Feature Updates

- 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.