

Sign-in, MFA and sessions

DOCUMENT	VERSION	STATUS
SB-GD-141	1.0, October 2026	Public. Checked against the product, October 2026

Who this is for

Workspace owners, admins and security reviewers who want to know how people sign in to SynapBridge, which second factors exist, and how sessions behave.

Before you start

- This document describes behavior in the product code as of release 2.233.x. It is not an audit report.
- SynapBridge supports two identity back ends, Amazon Cognito and WorkOS AuthKit. Which one a deployment uses is a server setting. A few details below differ by back end, and each is called out.
- Sign-in and session handling run in server-side route handlers. Nothing about your sign-in is decided in the browser.

How sign-in works

- 1 You enter your email address on the sign-in page.
- 2 The page sends only the email domain to a lookup. If your domain belongs to a workspace with single sign-on enabled and verified, you are sent to your identity provider. Otherwise you continue with a password.
- 3 After the password step, you complete a second factor (see the next section).
- 4 On success the server creates a session and sets session cookies. You land in the product.

Passkey sign-in is a separate option. The sign-in page has a passkey link, and registered passkeys are managed under Security settings.

Passwords

SynapBridge application code does not store password hashes. Passwords are held by the identity provider, Amazon Cognito or WorkOS. When you create an account, you choose your own

password and it must be at least 12 characters.

On the WorkOS password path, repeated failures lock the account: 10 failed attempts in a 15 minute window lock that email address for 15 minutes.

MFA methods

Setting up a second factor is part of creating an account. A user cannot finish sign-up without enrolling one factor.

- **Authenticator app (TOTP).** The sign-up flow shows a QR code and a manual-entry key, and you confirm with a 6 digit code. Codes follow RFC 6238 (SHA-1, 6 digits, 30 second step). On the WorkOS path the server accepts codes within a window of plus or minus 60 seconds to allow for clock drift, and the TOTP secret is stored encrypted with an AWS KMS key.
- **Passkeys (WebAuthn).** You can register passkeys in Security settings and sign in with one from the sign-in page. You can remove a passkey there too.
- **Backup codes.** Users can generate ten one-time backup codes in Security settings, and regenerate them later. Codes are stored as SHA-256 hashes. Using a backup code resets MFA immediately so you can enroll again.
- **Text message (SMS).** The code path exists, but it is switched off by the `MFA_SMS_ENABLED` setting. Treat SMS as not available.

Rate limits on MFA

MFA verification is rate limited per enrollment session (5 attempts per 15 minutes) and per IP address.

Email codes

A 6 digit email code verifies a new account's email address. The code is stored hashed with a per-code salt and expires after 10 minutes. After 5 wrong attempts the code is locked for 15 minutes. Sends are limited to 1 per 30 seconds and 5 per hour per address.

Email codes are used for account verification at sign-up. Email-based MFA recovery is a separate flow (next section). Forgot-password does not use email codes: the email code endpoint returns "not implemented" for any purpose other than sign-up verification. Password reset is a separate flow from the forgot password page. On the WorkOS path it sends an emailed reset link, and completing a reset revokes the user's live sessions.

Lost authenticator: MFA recovery

- **With a backup code:** MFA is reset immediately.

- **With an email code only:** the reset is scheduled with a delay, and an email with a cancel link is sent to the account's address. A 24 hour cooldown blocks a second recovery for the same email.
- **After a reset,** the user's sessions are revoked, and the user must enroll a new factor at next sign-in.

Sessions

SynapBridge uses an opaque session id held in a cookie. The session record itself lives on the server, not in the browser.

- The main cookie is named `__Host-sb_session_id`. Related cookies are `__Host-sb_session`, `__Host-sb_access` and `__Host-sb_refresh`.
- The session cookie is HttpOnly, Secure and SameSite=Lax. The `__Host-` prefix means each cookie is bound to the exact host that set it and carries no Domain attribute.

Lifetime and idle timeout

Sessions have a sliding lifetime of 14 days: activity extends it. A session that has been idle for more than 7 days stops working, even inside the 14 days. These are the default values in code. The idle timeout can be changed by a server setting, and the lifetime is the same for every workspace. There is no per-workspace or per-plan session length setting.

Signing out and revoking sessions

- Signing out ends your session and clears the cookies on this domain. Sign-out also revokes issued tokens at the identity provider.
- A workspace admin can revoke a user's sessions from the user's page in the Admin center. The server records the action in the admin audit trail.

What an admin can set

- **Session revocation, MFA reset and password reset** for a user, from the Admin center user page. Those three actions ask the admin to re-enter their own password.
- **Single sign-on.** If your identity provider's sign-in shows that MFA was performed, SynapBridge accepts it. If the sign-in carries no proof of MFA, the user completes SynapBridge's own MFA step.
- **MFA policy page.** The Admin center has an MFA policy page (enforcement level, allowed methods, bypass groups, recovery codes). In the current code this page records settings but does not change sign-in, because MFA is already required for every user. Do not rely on it to loosen or tighten MFA.

Limits and notes

Note SMS MFA is not available while MFA_SMS_ENABLED is off.

- Session length and idle timeout are not configurable per workspace.
- This document gives no TOTP secret length and no used-code replay claim, because neither can be confirmed from application code.
- This document does not describe production network or infrastructure controls.
- Plan availability of single sign-on and the MFA policy page is not stated here. Check your plan page.