

Single sign-on setup

DOCUMENT	VERSION	STATUS
SB-GD-132	1.0, October 2026	Public. Checked against the product, October 2026

Single sign-on (SSO) lets people in your workspace sign in through your company identity provider. SynapBridge uses WorkOS to handle the connection with your provider. SSO is a beta feature.

Who this is for

Workspace owners, and the identity or IT administrator who will configure your identity provider.

Before you start

- You must be a workspace owner. The Identity provider page in the Admin center is limited to owners. An admin who is not an owner is sent back to the Admin center home page.
- Plan: check Pricing or your billing page to confirm SSO is included in your plan. Access is checked again on the server when you open the page.
- Your identity provider can speak SAML 2.0 or OpenID Connect (OIDC). Someone on your identity team needs permission to create or edit an application in that provider.
- You need an email domain you control, and access to its DNS records, so you can verify it. Free email providers such as gmail.com and outlook.com cannot be claimed.
- Sign-in only goes to your identity provider for email addresses on a verified domain. Without a verified domain, people continue to sign in with a password and multi-factor authentication (MFA).

Set up the connection

- 1 In the Admin center, open Identity, then Identity provider.
- 2 In the Provider configuration section, find the card titled "Set up SSO via WorkOS" and select "Open WorkOS setup". A WorkOS-hosted setup page opens in a new tab.
- 3 Your identity administrator completes the SAML or OIDC setup in that page. The page text states that SynapBridge does not see your identity provider credentials or certificates.

- 4 Return to the Identity provider page and select the button labeled "I finished · check status". If the connection is not active yet, the page tells you to finish setup in the WorkOS tab and check again.
- 5 Look at the status badge on the Provider configuration section. It shows one of Draft, Active, Needs attention, or Disabled. Continue when it shows Active.

Note If the page says your workspace does not have a WorkOS organization yet, contact support. SynapBridge cannot create the connection for you from this page in that case.

Alternative: metadata URL

Below the WorkOS card, the same page has a form for a provider type and a metadata URL.

- 1 Choose a provider type: "SAML 2.0" or "OpenID Connect (OIDC)".
- 2 Enter the "SAML metadata URL" or the "OIDC discovery URL". It must start with https and be shorter than 2048 characters.
- 3 Optionally enter a "Friendly label". It is shown to workspace members on the sign-in page.
- 4 Select "Test connection". For SAML the check looks for a reachable https URL, a 2xx response, and a SAML EntityDescriptor. For OIDC it looks for valid JSON that includes issuer, authorization_endpoint, and jwks_uri.
- 5 Select "Save configuration".

The test only checks the metadata document. It does not sign anyone in.

Verify your email domain

Sign-in routing depends on a verified domain.

- 1 On the same Identity provider page, find the "Verified domains" card.
- 2 Under "Add a domain", enter your domain (for example acme.com) and select "Claim domain".
- 3 Domain ownership is checked with a DNS TXT record. This card lists the claim and its status but does not display the record value. If you cannot find the record details to add at your DNS host, contact SynapBridge support before you continue.
- 4 After the record is in place, select "Check DNS" next to the claim. The claim status changes from Pending to Verified.
- 5 Each verified domain has a join policy, shown as either "Auto-join" or "Requires approval". People who sign up with a domain set to require approval appear in a "Pending members" card, where an owner or admin can approve or deny them.

If you do not see the Verified domains card, ask SynapBridge support whether domain verification is turned on for your workspace.

What happens at sign-in

- 1 A person types their work email on the sign-in page. When they leave the email field, the page checks the domain.
- 2 If the domain is verified and your workspace has an active SSO connection, the page shows "Redirecting to" your provider name (or "your company") and sends them to your identity provider.
- 3 If the domain is unknown, unverified, revoked, or its connection is disabled, the person sees the normal password sign-in. Personal email domains always use the password flow.
- 4 After the identity provider confirms the person, SynapBridge finds or creates their account and adds them to your workspace. No invite or password is needed.
- 5 MFA: if the sign-in carries proof that your identity provider performed MFA, SynapBridge accepts it. If it does not, including when your provider is connected but not set up to send that proof, SynapBridge asks the person to enroll in or complete its own MFA step.

SSO is not enforced. The router reports "enforced" as false, and password sign-in stays available next to SSO.

What is not configurable

- There is no attribute-mapping screen in SynapBridge. Email and name come from the profile that WorkOS returns.
- There is no just-in-time (JIT) provisioning switch. A successful SSO sign-in creates the account and workspace membership automatically.
- Role: a person gets the Member role unless a group-to-role mapping on the WorkOS connection says admin or viewer. The Owner role is never granted by an identity provider group.
- There is no test sign-in link and no separate "turn on" switch. The connection is live once its status is Active.
- SynapBridge does not display an ACS URL, entity ID, or service provider metadata file on this page. Look for those values in the WorkOS-hosted setup page.

What to ask your identity team

- Which protocol will you use, SAML 2.0 or OIDC?
- Who will complete the WorkOS-hosted setup page, and do they have rights to create an application in the provider?
- Can you add a DNS TXT record for the domain claim, and who owns that DNS zone?
- Does the provider send an MFA signal in the sign-in (for example the OIDC amr claim)? If not, expect SynapBridge to ask for its own MFA.

- Should group names map to Admin or Viewer roles? That mapping is set on the WorkOS connection, not in SynapBridge.

Turn SSO off in an emergency

On the Identity provider page, the "Emergency disable" section has a "Disable single sign-on" button. You can enter a reason, which is written to the audit log, and you confirm by typing a word. People then sign in with password and MFA. MFA is not turned off by this action. To use SSO again, save a new configuration.

If every admin is locked out, contact support@synapbridge.com with your tenant id and a description of the outage. Support verifies ownership out of band before it issues a one-time recovery link.

Limits and notes

- SSO is a beta feature. Expect changes.
- The page lists the last 100 successful SSO sign-ins in a "Recent sign-ins" section.
- The Identity provider page also contains a "Directory Sync" card. See the "User provisioning with SCIM" guide.
- SynapBridge does not publish a list of tested identity providers. The form hint text names Okta, Azure AD, Google Workspace, Ping, and OneLogin as providers that publish a metadata document. Ask your identity team to confirm against your own provider.
- Plan wording: this guide does not state which plan includes SSO. Check Pricing or your billing page.