

Onboard a new team

DOCUMENT	VERSION	STATUS
SB-GD-102	1.0, October 2026	Public. Checked against the product, October 2026

Who this is for

Owners and Admins who are bringing a team into an existing SynapBridge account.

Before you start

You need:

- The Owner or Admin role. The Admin center is not open to other roles.
- At least one AI provider connected. See the guide "Quickstart: your first hour".
- A list of the people to add, with the role each should have.
- A decision on whether the team needs a group, a spend cap, or both.

How the pieces fit

Read this section first. It prevents the most common wrong assumption.

- Your account is one tenant. The name at the top of the sidebar is the tenant name, and you edit it under Settings, then Workspace. In several screens, such as Cost caps, "Entire workspace" means the whole tenant.
- Users, roles, groups, provider connections, policies and spend caps belong to the tenant.
- A workspace, created from the sidebar switcher, is a named entry inside the tenant. It stores a name, who created it, and whether it is the default. Every tenant has one default workspace.
- A workspace has no members, no policy, no budget and no region of its own. Selecting a workspace does not change which data you see. No other part of the product filters by workspace today.

So "onboard a team" means: invite the people, group them, give them roles, and set caps and policies at the tenant level. Creating a workspace is optional and only gives you a named entry.

Step 1: Connect the providers the team will use

Look for the "Shared" pill on a connection. It marks a connection shared with your organization.

- 1 Open Settings, then "AI providers".
- 2 Choose "Connect" on each provider the team needs and complete the key or sign-in step.
- 3 Confirm each tile shows "Connected".

Step 2: Invite the team

- 1 Open Admin center, then Users, then "Add user".
- 2 Enter the email, choose a role (Viewer, Member or Admin), and choose "Send invite".
- 3 Repeat for each person. The email subject is "You've been invited to a SynapBridge workspace". The link expires after 7 days.
- 4 To add many people at once, use Admin center, then Users, then "Bulk import". Upload a CSV (up to 512 KiB and 1000 rows) with the columns email, role and display_name. The wizard steps are Upload, Preview, Dry run and Result. If the page says "Bulk import is not available for your workspace yet", invite people one at a time instead. Check the Users list afterwards to confirm who was invited.
- 5 The "Invited" filter on the Users list shows people who have not accepted yet.

Admins can invite Members and Viewers. Only an Owner can invite an Admin. Owners cannot be invited from this panel.

Step 3: Create a group (optional)

Use a group to treat a team as one unit, for example for a spend cap.

- 1 Open Admin center, then Groups, then "Create group".
- 2 Complete the steps Basics, Members and Roles.
- 3 Choose the group type. Security groups can hold role assignments. Distribution groups are for addressing and notifications only.
- 4 Every member of a group inherits the roles you assign to the group.

If the page says groups are not available for your workspace yet, contact SynapBridge support.

Step 4: Set a spend cap (optional)

- 1 Open Admin center, then Cost management, then "Cost caps". Choose "Create cap". Cost caps need the Business plan.

- 2 Under Scope, pick "Entire workspace", a user, or a group. For a user or group, enter the ID in the target box (the Users list row menu has "Copy user ID").
- 3 Pick the Period (Daily or Monthly) and enter the cap amount in US dollars.
- 4 Set the alert thresholds. The default is 50, 75, 90 percent.
- 5 Under "When cap is reached", pick Warn or Block. Warn sends alerts and calls keep flowing. Block sends alerts and refuses further calls through SynapBridge's checked paths once the cap is reached. A cap is a check, not a guarantee.
- 6 Add an alert email, and optionally a Slack or Teams webhook URL.

The scope and period of a cap cannot be changed after it is created. Create a new cap instead. The Admin center menu shows a plan badge next to Cost caps.

Step 5: Review policies and models

- Policies: open Governance, then Policies. Policies cover PII, Content, Access, Cost and Provider categories. Each has a status of Draft, Simulate, Live, Paused or Retired. You can start with "From template" or "Create policy". Policies belong to the tenant, not to one workspace. Policies need the Business plan or above. The register records a policy but does not by itself enforce it; see the guide "Policies and the policy simulator".
- Models: Admin center, then "Model entitlements", holds an allow-list of provider and model pairs. When the list is empty, all models are allowed. This page depends on a feature setting, so it may not be turned on for your account.

Step 6: Create a workspace (optional)

- 1 In the sidebar header, open the switcher with the chevron ("Switch workspace").
- 2 Under "Workspaces", choose "New workspace".
- 3 Type a name in "Workspace name" and choose "Create".

If your plan has a limit, the switcher shows "Upgrade your plan to create another workspace." The default workspace has a "Default" badge and cannot be deleted. Other workspaces have a Delete button.

Step 7: Check that it works

- 1 Ask one new member to accept the invite and sign in. They set a password and set up MFA.
- 2 Ask them to send a message in Chat.
- 3 Open Insights, then "Usage & spend" to see the usage.
- 4 Owners and Admins can check Governance, then "Audit trail" (Pro plan or above).

Limits and notes

- Do not promise the team workspace-level policy, budgets, members or region. They do not exist.
- Role changes reach a person after their session refreshes. They see a "Your role changed" prompt with a "Refresh session" button.
- Single sign-on (Identity provider) and SCIM provisioning pages are Owner-only. The pricing page lists SSO and SCIM under the Business plan.
- Groups, custom roles and some other admin features can show "not available for your workspace yet" until support enables them.
- Do not put protected health information into SynapBridge until a signed HIPAA agreement is in place. That program is planned.