

User provisioning with SCIM

DOCUMENT	VERSION	STATUS
SB-GD-133	1.0, October 2026	Public. Checked against the product, October 2026

SCIM lets your identity provider add, update, and deactivate people in your SynapBridge workspace without manual invites. SCIM provisioning is a beta feature.

Who this is for

Workspace owners and identity administrators who want people to be added and removed from SynapBridge from their directory.

Before you start

- You must be a workspace owner. The Directory sync pages and the SCIM provisioning page are limited to owners.
- Plan: check Pricing or your billing page to confirm SCIM is included in your plan. This guide does not state a plan.
- Your identity provider must support SCIM 2.0. The Directory sync wizard lists Microsoft Entra ID, Okta, Google Workspace, OneLogin, JumpCloud, Rippling, and Generic SCIM v2.0.
- Set up single sign-on first if you plan to use it. See the "Single sign-on setup" guide. SSO and Directory Sync are both offered on the same Identity provider page.
- If a SCIM page says "SCIM administration is not available yet", or that it is not available for your workspace, contact SynapBridge support to have it enabled.

Where to set it up

SCIM has three places in the product. Use the one that matches your task.

- Admin center, Identity, Identity provider: the "Directory Sync (automatic access)" card has an "Open Directory Sync setup" button. It opens a WorkOS-hosted setup page in a new tab, the same way SSO setup does. Return and select the button labeled "I finished · check status".
- Admin center, Identity, Directory sync: the "Connect IdP" button starts a five-step wizard. The steps are Choose provider, Create connection, Endpoint & token, Test connection, and Map groups & roles.

- Settings, SCIM provisioning: shows the SCIM 2.0 base URL for your workspace, a sync status card, an error log, a reconciliation table, group-to-role mapping, and a "Rotate token" button.

Connect your provider with the wizard

- 1 In the Admin center, open Identity, then Directory sync, and select "Connect IdP".
- 2 Choose your identity provider and enter a name for the connection.
- 3 On the Endpoint and token step, copy the SCIM endpoint URL and the bearer token. The token is shown once. Copy it into your identity provider before you leave this step.
- 4 In your identity provider, paste the endpoint and token into its SCIM provisioning settings. The wizard shows provider-specific steps and a link to setup instructions.
- 5 Run the Test connection step and check the initial user list.
- 6 On the last step, map groups and roles.

Note If you lose the token, you must rotate it. A rotated token cannot be shown again.

Where the token is created and rotated

- The wizard creates the endpoint and token when you create the connection, and shows the token once.
- On Settings, SCIM provisioning, "Rotate token" opens a dialog. Rotating invalidates the current token immediately, so your identity provider stops syncing until you paste the new value. The new token is shown once, and the action is audited.
- If no token has been provisioned for the workspace, "Rotate token" is disabled and the page tells you to contact support.
- Tokens used with the SynapBridge SCIM endpoint have the form `scim_workspace_random` and are sent as a Bearer token.

What SynapBridge supports

Directory sync events

When connected through Directory sync, SynapBridge acts on user events from your directory: user created, user updated, and user deleted.

- Active users are created (if needed) and added to your workspace. Name comes from the first and last name in the directory. Events without an email address are skipped.
- Roles: a directory user gets the Admin, Member, or Viewer role if the directory supplies one of those. Otherwise they get Member. The Owner role is never assigned by a directory event.

- Group-to-role mapping: the page maps an identity provider group id to a role id. A tenant can have up to 500 mappings.
- Group events are not used. The only directory events SynapBridge handles are the three user events above.

Native SCIM endpoint

SynapBridge also runs a SCIM 2.0 endpoint that accepts the workspace bearer token. These operations are supported:

- GET Users: list users in your workspace. Use the count query parameter to set a page size (default 100).
- POST Users: create a user. The request must include userName, which is used as the email address. The name comes from name.formatted, or displayName. A duplicate returns 409.
- GET Users by id: return one user from your workspace.
- PATCH Users by id: only two operations are handled. Replace active (false disables the user, true enables them) and replace displayName.
- DELETE Users by id: remove the user.
- GET ServiceProviderConfig: returns discovery information. It reports patch as supported and bulk, change password, sort, and etag as not supported.

These return something other than success:

- All calls to the Groups endpoints return 501 with the message "Groups: implementation pending". Group push from your identity provider does not work through this endpoint.
- PUT on Users is not handled and returns 404.
- GET ResourceTypes and GET Schemas return empty resource lists.
- A request with a missing or wrong bearer token returns 401.

Deprovisioning

When your directory marks a user inactive or deletes them, SynapBridge does two things: it removes the user's membership in your workspace, and it marks the user inactive (active is set to false). The user record is kept, not deleted. If the person becomes active again, they are added back as a normal update.

Through the native endpoint, PATCH with active set to false disables the user, and DELETE removes the user.

This guide does not describe what happens to sessions that are already open. Do not assume that a session ends at the moment of deprovisioning. If you need access to stop at a precise time, also remove the person at your identity provider and ask your SynapBridge owner to review active

access.

Limits and notes

- SCIM is a beta feature. Expect changes.
- Groups through the native endpoint return 501.
- The Settings, SCIM provisioning page has a "Trigger manual sync" action. Treat it as unfinished: the page itself notes that the sync consumer is pending, and queued runs expire after 24 hours.
- The error log keeps errors for 24 hours.
- SynapBridge reads email, first and last name, state, and role from directory user events. Group-to-role mapping is the mapping step the product offers.
- Verify with a test user before you roll SCIM out to the whole company.
- Plan wording: this guide does not state which plan includes SCIM. Check Pricing or your billing page.