

API keys and scopes

DOCUMENT	VERSION	STATUS
SB-GD-122	1.0, October 2026	Public. Checked against the product, October 2026

Who this is for

Admins and developers who create, hand out and retire SynapBridge API keys.

Before you start

- Workspace API keys carry scopes. They are used for the AI gateway and a few other surfaces.
- A key acts inside your workspace only. Keys are not limited to a project or a sub-workspace.
- Treat every key like a password. Keep it in a secrets store, never in source code or a browser.

Workspace API keys

Format

A workspace key looks like `sk_p_` followed by 43 characters. The letter after `sk_` names the environment, and `p` is used in production. The 43 characters are random. Keys have no expiry date.

The Prefix column in Admin shows the first 11 characters of the key, which is enough to tell keys apart. SynapBridge stores only a SHA-256 hash of the key and that prefix, not the key itself.

Scopes

A key has one or more of four scopes. A key created without scopes gets read.

- `read`: read access. Required by the MCP server tools available today and by the agent-to-agent task route.
- `write`: write-capable calls. Required by the outcomes events route.
- `admin`: intended for MCP admin tools and tenant-wide usage data. On the MCP server, `admin` ranks above `write` and `write` ranks above `read`, so a key with a higher scope also passes a lower scope check there.
- `gateway`: calling models through the AI gateway.

Who can create each scope

- read: any signed-in member of the workspace.
- write: owner, admin or member. Viewer and read-only roles cannot grant it.
- admin: owner or admin.
- gateway: owner or admin, on the Team plan or above.

A role that is not allowed to grant a scope gets a 403. The same rules are enforced in the key service as well as in the web app.

Create a key

- 1 Open Admin center, then Applications, then API keys.
- 2 Enter a name and, if the key stands for an AI assistant or connector, choose its AI provider. The provider lets the key use workspace memory tools. A key with no provider declared is blocked from them.
- 3 Choose Create key and copy the secret.

Keys made on this page get the read scope. To create a key with the write or admin scope, send POST `/api/v1/apikeys` from a signed-in session with a body such as `{"name": "ci", "scopes": ["write"]}`. Gateway keys are created on Admin center, Applications, AI gateway, which also sets their limits. See the AI gateway guide.

One-time secret

The secret is returned once, in the response to the create or rotate request, and the console shows it in a panel with a Copy button. It cannot be retrieved later. If you lose it, rotate the key.

Rotate and revoke

- Rotate. POST `/api/v1/apikeys/{keyId}/rotate` creates a new key with the same name, scopes and gateway limits, returns its secret once, and revokes the old key right away. There is no overlap in which both keys work. The AI provider you declared on the old key is not copied, so if the new key uses memory tools, send PATCH `/api/v1/apikeys/{keyId}/provider` from a signed-in session with a body such as `{"provider_id": "anthropic"}`. The console has no control for this after a key is created.
- Zero-downtime swap. Create a second key, deploy it, then revoke the first.
- Revoke. DELETE `/api/v1/apikeys/{keyId}` marks the key revoked. The row stays in the list for reference, and the key is refused from then on. A revoked key cannot be restored or rotated.
- Rotate, revoke, gateway limit changes and provider changes need the owner or admin role.

Audit of changes

These actions are written to the audit log: `apikey.create`, `apikey.rotate`, `apikey.revoke`, `apikey.policy.update` and `apikey.provider.update`. Refused attempts to create a gateway key are

recorded as well. Each key records when it was last used and who created it. For gateway keys, each call also appears in the request log and spend tracking under the key.

Where workspace keys work

- AI gateway: `/api/gateway/v1/chat/completions`, `/api/gateway/v1/messages` and `/api/gateway/v1/models`, with the gateway scope.
- MCP server: `POST /api/v1/mcp-server`. Each tool names the scope it needs, and the tools available today need read.
- Agent-to-agent tasks: `POST /api/v1/a2a/tasks`, with the read scope.
- Outcomes events: `POST /api/v1/outcomes/events`, with the write scope.

The key goes in the Authorization header as a Bearer token. The AI gateway also accepts it in the `x-api-key` header.

Where workspace keys do not work

The web console routes under `/api/v1`, such as admin users, workspaces, memory facts, audit and billing, are for a signed-in browser session. They refuse API keys. Managing keys themselves (create, rotate, revoke, limits) is also session-only.

Limits and notes

- Names are limited to 80 characters.
- The key list shows name, prefix, scopes, creator, creation time and status.
- There is no per-key expiry. Retire keys by rotating or revoking them.
- A role cannot create a key that is more powerful than the role itself allows. A missing or unknown role is treated as having no role.
- Compliance: SynapBridge is architected to align with the SOC 2 Trust Services Criteria, and with HIPAA and PCI-DSS requirements. The HIPAA BAA program is planned.