

SpaceApp team pilot

SpaceApp is a self-hosted workspace where each developer runs AI coding CLIs side by side in persistent rooms, on their own machine and their own API keys. OpenCode comes first; Claude Code, OpenAI Codex, Gemini CLI, Qwen, Kimi, Grok and DeepSeek are among the CLIs it installs. Up to 16 panes fit in a room.

It is open source under the MIT License (copyright INTRATRADER SINGLE MEMBER P.C.), with no licence fee. The current release is `run-spaceapp 1.1.7`, installed with `npx --yes run-spaceapp@latest install` on Linux, macOS or Windows 11 with Docker.

The pilot (2-4 weeks, from €1,500)

For software and AI teams of 3-15 developers who already use AI coding CLIs. It is provided and invoiced by INTRATRADER SINGLE MEMBER P.C. (oll4.com), Patras, Greece, the company that develops SpaceApp.

1. **One install per developer**, on their own machine. Each developer is the owner of their own SpaceApp.
2. **OpenCode and Claude Code on your own API keys**, with your MCP servers. Other CLIs are added when they pass a task on your install during setup.
3. **A nightly backup with a tested restore** on each install: a scheduled backup, a copy kept off the machine, and one restore tested with you.
4. **Two workflows or MCP integrations** built with you, for example a review room, a test-and-fix loop, or an internal tool exposed to the agents over MCP.
5. **Team training** and a short written runbook, then **30 days of support**.

Price: a fixed quote after a 30-minute scoping call, from €1,500. The quote depends on the number of installs, the integrations and your environment. 50% is paid at signing and 50% at handover. The install stays yours, with no lock-in.

Your AI accounts

The pilot uses only your own API keys and accounts with the model providers. Model requests go from your install to the providers you configure, under your agreements with them. SpaceApp does not host models.

What protects an install today (run-spaceapp 1.1.7)

- **Local by default:** the web app listens on `127.0.0.1:4911`. First launch uses a one-time, hashed, expiring setup token; there is no default password.
- **Sign-in:** a signed session cookie (HMAC), a CSRF header on every change, and login limited to 10 attempts per 15 minutes.
- **Keys:** API keys are read from masked input into restrictive secret files; they are not passed in command arguments, logs or database rows. Only the CLI container mounts provider keys and logins.
- **Containers:** no container gets the Docker socket, and the CLI container runs with `no-new-privileges`. SpaceApp's own images are pulled by the digest recorded in the npm package.
- **Telemetry:** off by default.
- **Backup and restore:**
 - backup pauses the containers, so the database, files, memory and workflow history are saved from one moment. Backups exclude provider API keys and logins.
 - If a database or the file swap fails during restore, it puts every database and file back as they were before.

What the pilot is not

- **Not a production security certification.** SpaceApp is actively developed software with a public list of open findings: `docs/quality/KNOWN_LIMITATIONS.md` in the repository.
- **Not tenant isolation.** Each install has one trusted owner, and rooms organise work rather than separating untrusted users.
- **Not a sandbox for the host.** Agents work with the folders and credentials an install is given. Scope them per machine.
- **Not hardened for the open Internet.** If you expose an install, TLS, proxy access, firewall and log retention are yours.
- **Production use** needs at least a threat model for your environment, monitoring of the nightly backups and a review of the logs against your requirements. These can be scoped as separate work.

Book a paid pilot: spaceapp.dev → «Team pilot» → «Book a paid pilot» · github.com/oll4com/spaceapp