Run sandboxes in CI

- Cleanup and exit codes
- Parse command output
  - Update scripts for v0.48.0

This page describes local sandboxes in CI. For cloud execution without local virtualization, see Run without attaching.

For CI environments and scripts where a browser isn't available, authenticate with a Docker Personal Access Token (PAT):

```
$ echo "$DOCKER_PAT" | sbx login --username <your-docker-id> --password-stdin
```

Generate a PAT from your Docker account settings with at least **Read** scope.

Sign in before running commands that require authentication. Read-only commands and commands run with `--force` do not open an interactive sign-in flow. Create workspace directories before calling `sbx create` or `sbx run`: without a terminal, these commands fail if a workspace directory does not exist.

Create the sandbox in the background with `sbx create`, run agent tasks with `sbx exec`, and remove the sandbox when finished:

```
$ sbx create --name ci-task --clone claude .
$ sbx exec ci-task -- claude --dangerously-skip-permissions -p "Review the code and commit
your changes"
$ git fetch sandbox-ci-task
$ sbx rm --force ci-task
```

Agent credentials (API keys, GitHub token) can be preconfigured as global secrets so they're available to any sandbox the CI runner creates. If the relevant environment variables are already set in the CI environment (see the built-in services table for which variables each service reads), import them all at once:

```
$ sbx secret import --all
```

To overwrite an existing stored entry, add `--force`. To pass a value from your CI provider's secret store, use `-t`. For example, in a GitHub Actions step:

```
- run: sbx secret set anthropic --force -t "${{ secrets.ANTHROPIC_API_KEY }}"
```

Cleanup and exit codes

`sbx exec` returns the exit status of the command it runs. A failure to run the command, such as a missing sandbox, returns 125. A missing executable inside a local sandbox returns 127. Check stderr for the cause before deciding whether to retry.

Confirmations require terminal input. Piping an answer, such as `echo y`, does not confirm an operation. Use `--force` on commands that provide it to skip confirmation in scripts. `sbx kit builder history rm` uses `--yes` or `-y` instead, because its `--force` flag is passed to Buildx.

A command that requires confirmation fails with exit status 1 when stdin is not a terminal. Declining a confirmation also returns a non-zero exit code. Treat this as an incomplete operation when deciding whether to continue a script.

For repeatable cleanup, check which resources exist before removing them. For example, use `sbx mcp ls` before `sbx mcp rm`, which fails for an unregistered server even with `--force`. Likewise, `sbx secret rm` fails if no secret matches the selector; check for matches with `sbx secret ls` before removing secrets.

Parse command output

Use `--format json` or `--format yaml` on commands that support structured output. Human-readable tables and messages can change between releases. Results go to stdout. Errors, warnings, hints, and progress go to stderr.

```
$ sbx ls --json | jq -r '.[].name'
$ sbx prune --dry-run --format yaml
```

`--json` is an alias for `--format json`. On commands with shared output flags, `--format`, `--json`, and `--quiet` (`-q`) are mutually exclusive, even when `--json` and `--format json` request the same format. Unsupported format values are rejected. `sbx events --json` emits newline-delimited JSON, and `sbx mcp auth --format text|json` uses command-specific formats.

For lists of identifiers without table headings, use `--quiet` or `-q`:

Command	Output
`sbx policy ls -q`	Local rule IDs. With `--cloud`, network patterns instead.
`sbx settings ls -q`	Setting keys.
`sbx policy approval ls -q`	Approval IDs.

Update scripts for v0.48.0

{{< copy-as-prompt instruction="Update this repository's Docker Sandboxes CLI usage for v0.48.0 using the migration reference below. Inspect scripts and documentation, update affected commands and output parsers, and verify the changes. Preserve unrelated behavior." >}}

Docker Sandboxes v0.48.0 changes flags and structured output. Update scripts that use the following flags:

Command	Previous flag	Replacement
`sbx run`, `sbx env run`	`--detached`	`--detach` or `-d`
`sbx logout`	`--yes`, `-y`	`--force` or `-f`
`sbx env create`, `sbx env run`	`--auto-approve`, `-y`	`--force` or `-f`
`sbx create`	`--quiet`, `-q`	`--no-progress` suppresses progress but still prints the creation summary
`sbx template save`	`-d` for a description	`--description`
`sbx diagnose`	`--output`, `-o`	`--format table`, `json`, `yaml`, or `github-issue`
`sbx policy log`	`--quiet`, `-q`	Removed without a replacement

`sbx settings ls` is the primary command spelling. `sbx settings list` remains an alias. Replace the deprecated `sbx mcp add --skip_auth` with `--skip-auth`. Secret commands that default to global scope still accept the deprecated `--global` flag but print a warning to stderr. Omit the flag for those commands.

JSON field names use `snake_case`. YAML uses the same representation. Update parsers for these commands:

Command	Structured output in v0.48.0
`sbx ls`	A sandbox array, replacing `{sandboxes: [...]}`. `created_at` and `last_used_at` use RFC 3339 timestamps. Rows include `detached`.
`sbx template ls`	An image array, replacing `{images: [...]}`.

Command	Structured output in v0.48.0
Local `sbx mcp ls`	A server array, replacing `{gateway: {...}, servers: [...]}`. Each row includes `gateway`. Cloud rows describe server usage across sandboxes and differ from local registration rows.
`sbx policy log`	`{updated_at, allowed: [...], blocked: [...]}` for local and cloud output. See Monitoring traffic.
`sbx --cloud policy ls`	Field names use `snake_case` instead of camelCase.
`sbx ports`	Local rows contain `host_ip`, `host_port`, `sandbox_port`, and `protocol`. Cloud rows contain `sandbox_port` and `url`, replacing `port`. Local publish and unpublish results include `action: published` or `action: unpublished`.
Cloud `sbx volume create`, `sbx volume ls`, `sbx volume inspect`	Fields such as `ID`, `Name`, and `CreatedAt` become `id`, `name`, and `created_at`. `volume inspect` defaults to human-readable details, so request a structured format explicitly.
`sbx rm`, `sbx stop`, `sbx template rm`, `sbx volume rm`	An array of results with `action`, `resource`, `name`, and optional `id` and `error`, including missing or failed targets. Actions are lowercase: `removed`, `stopped`, `removing`, `stopping`, or `failed`.

For example, replace the jq filter `.sandboxes[].name` with `.[].name` when extracting sandbox names from `sbx ls --json`.

{{< /copy-as-prompt >}}

□□□ #2
□ □□□ □□□ 2026-10-31 19:02:37 UTC
□ □□□ □□□ 2026-10-31 19:02:38 UTC