

**CLI commands**

Sandbox CLI

Manage Docker-based sandbox containers for isolated agent execution.

Overview

OpenClaw can run agents in isolated Docker containers for security. The `sandbox` commands help you manage these containers, especially after updates or configuration changes.

Commands

`openclaw sandbox explain`

Inspect the **effective** sandbox mode/scope/workspace access, sandbox tool policy, and elevated gates (with fix-it config key paths).

```
openclaw sandbox explain
openclaw sandbox explain --session agent:main:main
openclaw sandbox explain --agent work
openclaw sandbox explain --json
```

`openclaw sandbox list`

List all sandbox containers with their status and configuration.

```
openclaw sandbox list
openclaw sandbox list --browser # List only browser containers
openclaw sandbox list --json      # JSON output
>
```

Output includes:

Container name and status (running/stopped)

Docker image and whether it matches config

Age (time since creation)

Idle time (time since last use)

Associated session/agent

openclaw sandbox recreate

Remove sandbox containers to force recreation with updated images/config.

```
openclaw sandbox recreate --all          # Recreate all containers
openclaw sandbox recreate --session main # Specific session
openclaw sandbox recreate --agent mybot  # Specific agent
openclaw sandbox recreate --browser     # Only browser containers
openclaw sandbox recreate --all --force  # Skip confirmation
```

Options:

--all : Recreate all sandbox containers

--session <key> : Recreate container for specific session

--agent <id> : Recreate containers for specific agent

--browser : Only recreate browser containers

--force : Skip confirmation prompt

Important: Containers are automatically recreated when the agent is next used.

>

Use Cases

After updating Docker images

```
# Pull new image
docker pull openclaw-sandbox:latest
docker tag openclaw-sandbox:latest openclaw-sandbox:bookworm-slim

# Update config to use new image
# Edit config: agents.defaults.sandbox.docker.image (or agents.list[].sandbox.docker.image)

# Recreate containers
openclaw sandbox recreate --all
```

After changing sandbox configuration

```
# Edit config: agents.defaults.sandbox.* (or agents.list[].sandbox.*)

# Recreate to apply new config
openclaw sandbox recreate --all
```

After changing setupCommand

```
openclaw sandbox recreate --all
# or just one agent:
openclaw sandbox recreate --agent family
```

For a specific agent only

 # Update only one agent's containers
openclaw sandbox recreate --agent alfred

>

Why is this needed?

Problem: When you update sandbox Docker images or configuration:

Existing containers continue running with old settings

Containers are only pruned after 24h of inactivity

Regularly-used agents keep old containers running indefinitely

Solution: Use `openclaw sandbox recreate` to force removal of old containers. They'll be recreated automatically with current settings when next needed.

Tip: prefer `openclaw sandbox recreate` over manual `docker rm`. It uses the Gateway's container naming and avoids mismatches when scope/session keys change.

Configuration

Sandbox settings live in `~/.openclaw/openclaw.json` under `agents.defaults.sandbox` (per-agent overrides go in `agents.list[].sandbox`):



```
"agents": {  
    "defaults": {  
        "sandbox": {  
            "mode": "all", // off, non-main, all  
            "scope": "agent", // session, agent, shared  
            "docker": {  
                "image": "openclaw-sandbox:bookworm-slim",  
                "containerPrefix": "openclaw-sbx-",  
                // ... more Docker options  
            },  
            "prune": {  
                "idleHours": 24, // Auto-prune after 24h idle  
                "maxAgeDays": 7, // Auto-prune after 7 days  
            },  
        },  
    },  
},  
}
```

See Also

- Check sandbox setup

◀ [reset](#)

[security](#) ▶

Powered by [mintlify](#)