Protocols and APIs › Tools Invoke API

Protocols and APIs

# Tools Invoke API

OpenClaw's Gateway exposes a simple HTTP endpoint for invoking a single tool directly. It is always enabled, but gated by Gateway auth and tool policy.

- `POST /tools/invoke`
- Same port as the Gateway (WS + HTTP multiplex): `http://<gateway-host>:<port>/tools/invoke`

Default max payload size is 2 MB.

## Authentication

Uses the Gateway auth configuration. Send a bearer token:

- `Authorization: Bearer <token>`

Notes:

- When `gateway.auth.mode="token"` , use `gateway.auth.token` (or `OPENCLAW_GATEWAY_TOKEN` ).
- When `gateway.auth.mode="password"` , use `gateway.auth.password` (or `OPENCLAW_GATEWAY_PASSWORD` ).
- If `gateway.auth.rateLimit` is configured and too many auth failures occur, the endpoint returns `429` with `Retry-After` .

## Request body

```
{
  "tool": "sessions_list",
  "action": "json",
  "args": {},
  "sessionKey": "main",
  "dryRun": false
}
```

Fields:

- `tool` (string, required): tool name to invoke.
- `action` (string, optional): mapped into args if the tool schema supports `action` and the args payload omitted it.
- `args` (object, optional): tool-specific arguments.
- `sessionKey` (string, optional): target session key. If omitted or `"main"`, the Gateway uses the configured main session key (honors `session.mainKey` and default agent, or `global` in global scope).
- `dryRun` (boolean, optional): reserved for future use; currently ignored.

## Policy + routing behavior

Tool availability is filtered through the same policy chain used by Gateway agents:

- `tools.profile` / `tools.byProvider.profile`
- `tools.allow` / `tools.byProvider.allow`
- `agents.<id>.tools.allow` / `agents.<id>.tools.byProvider.allow`
- group policies (if the session key maps to a group or channel)
- subagent policy (when invoking with a subagent session key)

If a tool is not allowed by policy, the endpoint returns **404**.

Gateway HTTP also applies a hard deny list by default (even if session policy allows the tool):

- `sessions_spawn`
- `sessions_send`
- `gateway`
- `whatsapp_login`

You can customize this deny list via `gateway.tools` :

```
{
  gateway: {
    tools: {
      // Additional tools to block over HTTP /tools/invoke
      deny: ["browser"],
      // Remove tools from the default deny list
      allow: ["gateway"],
    },
  },
}
```

To help group policies resolve context, you can optionally set:

- `x-openclaw-message-channel: <channel>` (example: `slack` , `telegram` )
- `x-openclaw-account-id: <accountId>` (when multiple accounts exist)

## Responses

- `200` → `{ ok: true, result }`
- `400` → `{ ok: false, error: { type, message } }` (invalid request or tool input error)
- `401` → unauthorized

`429` → auth rate-limited ( `Retry-After` set)

`404` → tool not available (not found or not allowlisted)

`405` → method not allowed

`500` → `{ ok: false, error: { type, message } }` (unexpected tool execution error; sanitized message)

## Example

```
curl -sS http://127.0.0.1:18789/tools/invoke \
  -H 'Authorization: Bearer YOUR_TOKEN' \
  -H 'Content-Type: application/json' \
  -d '{
    "tool": "sessions_list",
    "action": "json",
    "args": {}
  }'
```

‹ OpenAI Chat Completions CLI Backends ›