Browser › Browser Login

Browser

Browser Login

Manual login (recommended)

When a site requires login, **sign in manually** in the **host** browser profile (the openclaw browser).

Do **not** give the model your credentials. Automated logins often trigger anti-bot defenses and can lock the account.

Back to the main browser docs: Browser.

Which Chrome profile is used?

OpenClaw controls a **dedicated Chrome profile** (named `openclaw` , orange-tinted UI). This is separate from your daily browser profile.

Two easy ways to access it:

1. **Ask the agent to open the browser** and then log in yourself.
2. **Open it via CLI**:

```
openclaw browser start
openclaw browser open https://x.com
```

If you have multiple profiles, pass `--browser-profile <name>` (the default is `openclaw`).

X/Twitter: recommended flow

- **Read/search/threads:** use the **host** browser (manual login).
- **Post updates:** use the **host** browser (manual login).

Sandboxing + host browser access

Sandboxed browser sessions are **more likely** to trigger bot detection. For X/Twitter (and other strict sites), prefer the **host** browser.

If the agent is sandboxed, the browser tool defaults to the sandbox. To allow host control:

```
{
  agents: {
    defaults: {
      sandbox: {
        mode: "non-main",
        browser: {
          allowHostControl: true,
        },
      },
    },
  },
}
```

Then target the host browser:

```
openclaw browser open https://x.com --browser-profile openclaw --targe
```

Or disable sandboxing for the agent that posts updates.

‹ Browser (OpenClaw-managed) Chrome Extension ›

›