



☰ Other install methods > Ansible

Other install methods

Ansible

The recommended way to deploy OpenClaw to production servers is via [openclaw-ansible](#) – an automated installer with security-first architecture.

Quick Start

One-command install:

```
curl -fsSL https://raw.githubusercontent.com/openclaw/openclaw-ansible/main/install.sh | sh
```

📦 Full guide:

The [openclaw-ansible](#) repo is the source of truth for Ansible deployment. This page is a quick overview.

What You Get

🔒 **Firewall-first security:** UFW + Docker isolation (only SSH + Tailscale accessible)

🔒 **Tailscale VPN:** Secure remote access without exposing services publicly

🐳 **Docker:** Isolated sandbox containers, localhost-only bindings

🛡️ **Defense in depth:** 4-layer security architecture



One-command setup: Complete deployment in minutes

Systemd integration: Auto-start on boot with hardening

>

Requirements

OS: Debian 11+ or Ubuntu 20.04+

Access: Root or sudo privileges

Network: Internet connection for package installation

Ansible: 2.14+ (installed automatically by quick-start script)

What Gets Installed

The Ansible playbook installs and configures:

1. **Tailscale** (mesh VPN for secure remote access)
2. **UFW firewall** (SSH + Tailscale ports only)
3. **Docker CE + Compose V2** (for agent sandboxes)
4. **Node.js 22.x + pnpm** (runtime dependencies)
5. **OpenClaw** (host-based, not containerized)
6. **Systemd service** (auto-start with security hardening)

Note: The gateway runs **directly on the host** (not in Docker), but agent sandboxes use Docker for isolation. See [Sandboxing](#) for details.

Post-Install Setup

After installation completes, switch to the openclaw user:

```
sudo -i -u openclaw
```

The post-install script will guide you through:



1. **Onboarding wizard:** Configure OpenClaw settings
2. **Provider login:** Connect WhatsApp/Telegram/Discord/Signal
3. **Gateway testing:** Verify the installation
4. **Tailscale setup:** Connect to your VPN mesh

Quick commands

```
# Check service status  
sudo systemctl status openclaw  
  
# View live logs  
sudo journalctl -u openclaw -f  
  
# Restart gateway  
sudo systemctl restart openclaw  
  
# Provider login (run as openclaw user)  
sudo -i -u openclaw  
openclaw channels login
```

Security Architecture

4-Layer Defense

1. **Firewall (UFW):** Only SSH (22) + Tailscale (41641/udp) exposed publicly
2. **VPN (Tailscale):** Gateway accessible only via VPN mesh
3. **Docker Isolation:** DOCKER-USER iptables chain prevents external port exposure
4. **Systemd Hardening:** NoNewPrivileges, PrivateTmp, unprivileged user

Verification



Test external attack surface:

```
nmap -p- YOUR_SERVER_IP
```

Should show **only port 22** (SSH) open. All other services (gateway, Docker) are locked down.

Docker Availability

Docker is installed for **agent sandboxes** (isolated tool execution), not for running the gateway itself. The gateway binds to localhost only and is accessible via Tailscale VPN.

See [for sandbox configuration.](#)

Manual Installation

If you prefer manual control over the automation:

```
# 1. Install prerequisites
sudo apt update && sudo apt install -y ansible git

# 2. Clone repository      ›
git clone https://github.com/openclaw/openclaw-ansible.git
cd openclaw-ansible

# 3. Install Ansible collections
ansible-galaxy collection install -r requirements.yml

# 4. Run playbook
./run-playbook.sh

# Or run directly (then manually execute /tmp/openclaw-setup.sh after)
# ansible-playbook playbook.yml --ask-become-pass
```

Updating OpenClaw

The Ansible installer sets up OpenClaw for manual updates. See [this page](#) for the standard update flow.

To re-run the Ansible playbook (e.g., for configuration changes):

```
cd openclaw-ansible
./run-playbook.sh
```

Note: This is idempotent and safe to run multiple times.

Troubleshooting

Firewall blocks my connection

If you're locked out:

Ensure you can access via Tailscale VPN first



SSH access (port 22) is always allowed

The gateway is **only** accessible via Tailscale by design

>

Service won't start

```
# Check logs
sudo journalctl -u openclaw -n 100

# Verify permissions
sudo ls -la /opt/openclaw

# Test manual start
sudo -i -u openclaw
cd ~/openclaw
pnpm start
```

Docker sandbox issues

```
# Verify Docker is running
sudo systemctl status docker

# Check sandbox image
sudo docker images | grep openclaw-sandbox

# Build sandbox image if missing
cd /opt/openclaw/openclaw
sudo -u openclaw ./scripts/sandbox-setup.sh
```

Provider login fails

Make sure you're running as the `openclaw` user:

```
sudo -i -u openclaw
openclaw channels login
```

>

Advanced Configuration

For detailed security architecture and troubleshooting:

Related

- full deployment guide
- containerized gateway setup
- agent sandbox configuration
 - per-agent isolation

< Nix

Bun (Experimental) >

Powered by [mintlify](#)