Contabo VPS + OpenClaw Setup Guide

Audience: non-technical PC users. Goal: buy a cheap VPS, secure it, install OpenClaw, and connect it to Telegram and Claude (subscription).

This guide is written for **Contabo VPS 10 (8 GB RAM)** on **Ubuntu 24.04**.

What you will achieve

- A private server (VPS) running Ubuntu 24.04.
- Secure access using **Tailscale** (no public admin ports).
- OpenClaw installed and running as a background service.
- Telegram bot connected.
- Claude connected via your subscription.
- Browser automation working on the VPS.

Preparation (do this first, on your own PC)

Complete these steps before buying the VPS. This way you can paste tokens directly during setup without switching context.

1. Create a Telegram bot and save the token

1. Open Telegram and find `@BotFather`.
2. Send `/newbot`.
3. Choose a name and a username.
4. BotFather will give you a **Bot Token** (looks like `123456:ABC...`).

Save the Bot Token somewhere safe.

2. Install Tailscale on your PC

Linux/macOS: Run in terminal:

```
curl -fsSL https://tailscale.com/install.sh | sh
```

Windows: Go to tailscale.com and download the app.

Then sign in and confirm Tailscale is running (you'll see its icon in your system tray/menu bar).

3. Ensure you have a Claude subscription

You need an active Claude subscription at claude.ai.

Part 1: Buy and Access VPS

Step 1. Buy the VPS on Contabo

1. Go to Contabo and choose **VPS 10 (8 GB RAM)**.
2. Choose:
3. **Operating system:** Ubuntu **24.04 LTS**
4. **Server location:** pick the closest region
5. Set the **root password** option.
6. Finish checkout.
7. After the VPS is ready, find **Server IP address** (looks like `123.45.67.89`) in your email.

Write it down.

Step 2. Connect to the server

1. Open Terminal (macOS/Linux) or Windows Terminal (Windows).
2. Type this command, replacing YOUR_SERVER_IP with your actual IP:

```
ssh root@YOUR_SERVER_IP
```

1. Type `yes` when asked about unknown host.
2. Paste the root password and press Enter.

If you see a prompt like `root@...`, you're connected.

Part 2: Secure the Server

Step 3. Update and create a user

Copy and paste each block. Wait for each to finish before running the next.

Update system and create user "remote":

```
apt update && apt upgrade -y
adduser remote
usermod -aG sudo remote
```

It will ask you to create a password. Save it. Then allow this user to login:

```
mkdir -p /home/remote/.ssh && cp -r /root/.ssh/* /home/remote/.ssh/ 2>/dev/null
```

Now disconnect and reconnect as the new user:

```
exit
```

Then:

```
ssh remote@YOUR_SERVER_IP
```

Step 4. Install Tailscale on the server

Tailscale creates a private network between your PC and the server.

```
curl -fsSL https://tailscale.com/install.sh | sh
sudo tailscale up
```

After running, it shows a login link. Copy it, open in your browser, and approve the server. Then get your server's Tailscale IP:

```
tailscale ip -4
```

It returns something like `100.x.y.z`. Write this down as **TS_IP**.

Step 5. Lock down the server

After this step, you'll only access the server through Tailscale (more secure).

First, test that Tailscale works. On your PC, open a new terminal and run:

```
ssh remote@TS_IP
```

(Replace TS_IP with the 100.x.y.z address from Step 4.)

If this works, continue. If not, check that Tailscale is running on both your PC and server.

Enable the firewall:

```
sudo apt install -y ufw && sudo ufw default deny incoming && sudo ufw default a
```

Type `y` when asked.

Disable root login:

```
sudo sed -i 's/^#*PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config &
```

From now on, always connect using `ssh remote@TS_IP`.

Part 3: Install OpenClaw

Step 6. Install Claude Code CLI

```
curl -fsSL https://claude.ai/install.sh | bash
echo 'export PATH="$HOME/.local/bin:$PATH"' >> ~/.bashrc && source ~/.bashrc
claude setup-token
```

It shows a URL. Copy it and open it in your PC's browser. Log in to Claude and approve. You'll get a short code.

Go back to the server terminal and paste the code. Press Enter.

You'll see a token like `sk-ant-xxxxxxxx`. This is saved automatically.

Step 7. Install OpenClaw

Install Node.js 22 and pnpm:

```
curl -fsSL https://deb.nodesource.com/setup_22.x | sudo -E bash -
sudo apt install -y nodejs
curl -fsSL https://get.pnpm.io/install.sh | sh - && source ~/.bashrc
```

Install Homebrew (interactive, follow the prompts):

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/H
```

Configure shell and install OpenClaw:

```
echo 'eval "$(/home/linuxbrew/.linuxbrew/bin/brew shellenv)"' >> ~/.bashrc && e
pnpm i -g openclaw
```

Step 8. Onboarding

Run the interactive setup wizard:

```
openclaw onboard --install-daemon
```

The wizard guides you through configuration. Follow each screen:

Screen	What to select
Security confirmation	**Yes**
Gateway configuration	**Local** (unless you need remote access)
Model / auth provider	**Anthropic**
Authentication	Paste your `sk-ant-...` token from Step 6
Channel selection	**Telegram** → paste your Telegram bot token
Daemon installation	**Yes** (runs as background service)
Security defaults	**Enable** pairing approvals

After onboarding, OpenClaw starts running automatically as a background service.

Step 9. Install browser support

This lets the bot browse websites.

```
sudo apt update && sudo apt install -y chromium xvfb fonts-liberation libnss3 l
```

Restart OpenClaw:

```
systemctl --user restart openclaw-gateway.service
```

Part 4: Connect and Verify

Step 10. Pair your Telegram account

1. Open your bot in Telegram.
2. Send `/start`.
3. The bot replies with a pairing code.
4. On the server, run (replace CODE with your actual code):

```
openclaw pairing approve telegram CODE
```

Note: Pairing codes expire after 1 hour. If the code doesn't work, send `/start` again to get a new one.

Step 11. Open the Dashboard

The dashboard lets you manage OpenClaw from your browser.

On your PC, open Terminal/Windows Terminal and run:

```
ssh -L 18789:127.0.0.1:18789 remote@TS_IP
```

Keep this window open.

On the server, run:

```
openclaw dashboard --no-open
```

It prints a link like `http://127.0.0.1:18789/?token=...`

Copy the full link and open it in your PC's browser.

Step 12. Test the bot

1. Open your bot in Telegram.
2. Send `hi`.
3. You should get a response.

Verify everything is healthy:

```
openclaw status
```

This shows if all services are running correctly.

Done! Your OpenClaw is running.

Troubleshooting

Bot doesn't respond

Check if OpenClaw is running:

```
systemctl --user status openclaw-gateway.service
```

View logs:

```
journalctl --user -u openclaw-gateway.service -n 100 --no-pager
```

Restart it:

```
systemctl --user restart openclaw-gateway.service
```

Can't open dashboard

Make sure the SSH tunnel command is still running on your PC.

Browser tool fails

Run the browser install command from Step 9 again, then restart OpenClaw.

Security notes

- Keep your tokens in a password manager.
- Always use Tailscale to connect to your server.
- Don't share your dashboard link.

Appendix A: WhatsApp setup

In the Dashboard:

1. Go to Channels
2. Add WhatsApp
3. Scan the QR code with your phone (WhatsApp → Settings → Linked Devices)

Appendix B: Skills and Gemini API

After the bot works, you can add extra features:

```
openclaw configure
```

Some skills need a Gemini API key. Get one at https://aistudio.google.com/app/api-keys, then:

```
echo 'export GEMINI_API_KEY="YOUR_KEY"' >> ~/.bashrc && source ~/.bashrc
```

Appendix C: Useful commands

```
# Check if OpenClaw is running
systemctl --user status openclaw-gateway.service

# Restart OpenClaw
systemctl --user restart openclaw-gateway.service

# View logs
journalctl --user -u openclaw-gateway.service -n 100 --no-pager

# Check Tailscale
tailscale status

# Reconfigure OpenClaw
openclaw configure
```

Get a VPS

Buy a VPS at Contabo