THE COMPLETE NEW ZEALAND GUIDE TO

SETTING UP OPENCLAW

SECURELY AND CORRECTLY

Written by Theo — an AI agent who went through every single step himself
Commissioned by Keira — Miss AI — AI Consultancy NZ
getopenclaw.co.nz | aiconsultancy.co.nz | agentnz.co.nz

⚠️ IMPORTANT: 1 in 5 free OpenClaw skills contains malware. 135,000+ instances are currently exposed to the open internet. This guide exists because most setup tutorials skip the security steps entirely. Don't be a statistic.

Why This Guide Exists

OpenClaw went from zero to 180,000 GitHub stars in weeks. Everyone rushed to install it. Almost nobody installed it correctly.

The result: over 800 malicious skills in the ClawHub marketplace. 135,000 instances exposed to the open internet with no authentication. A critical one-click remote code execution vulnerability that let attackers steal your gateway token and run arbitrary commands on your machine.

This guide was written by Theo — an AI agent running on a Mac Mini M4 in Tauranga, New Zealand. Theo went through every single step of this setup process. Every error. Every permission issue. Every security decision. This guide documents all of it so you don't have to learn the hard way.

> 🇳🇿 This is the only OpenClaw setup guide written specifically for New Zealand. It reflects NZ hardware availability, NZ privacy considerations, and the specific threat landscape facing NZ businesses.

What You Will Have When You Finish

- A fully operational AI agent running 24/7 on dedicated hardware
- A hardened, security-first setup that protects your data and your business
- An AI agent you can talk to via Telegram voice notes from anywhere
- A personalised agent with its own identity, mission, and operating instructions
- Zero skills installed — maximum security from day one
- Complete understanding of what you built and why every decision was made

What You Need Before You Start

Item	Details
Mac Mini M4	Dedicated hardware — do NOT use your personal computer
Monitor + HDMI cable	For initial setup only — you won't need it after
Keyboard and mouse	USB wired is easiest for first boot
Internet connection	Wi-Fi or ethernet
iPhone or Android	For Telegram voice notes
Credit card	For Anthropic and Brave API accounts

A notebook	For writing down recovery keys and passwords

Phase 0 — Pre-Flight Checklist

Do all of this before you touch the Mac Mini. These accounts and API keys need to exist before installation.

> 🔑 The golden rule: Theo gets his own everything. Dedicated Apple ID. Dedicated Gmail. Dedicated SIM. Dedicated API keys. Nothing shared with your personal accounts. Ever.

Step 1 — Create Dedicated Accounts

On your MacBook or phone, create these accounts now:

Account	What to Do	Why
Gmail	Create a new Gmail address just for your agent	Infrastructure email for APIs
Apple ID	Create using the Gmail above	Needed for Mac Mini setup
Dedicated SIM	Skinny, 2degrees, or Warehouse Mobile NZ	For Telegram bot verification
Telegram	Create account using the dedicated SIM	Primary communication channel

Step 2 — Get Your API Keys

These cost money but are essential. Set spending limits on both.

Anthropic API Key

1. Go to console.anthropic.com
2. Click API Keys in the left sidebar
3. Click Create Key
4. Name it YourAgentName-OpenClaw
5. Copy the key immediately — you only see it once
6. Go to Billing and set a monthly spending limit of $10-20 NZD to start
7. Save the key in Apple Keychain or a physical notebook

Brave Search API Key

8. Go to api-dashboard.search.brave.com
9. Sign up using your agent's Gmail
10. Select the free plan — includes $5 monthly credits
11. Copy your API key and save it

> 🔍 Why Brave? It gives your agent the ability to search the web privately. No data sent to Google. No tracking. Free for the first 1,000 searches per month.

Step 3 — Set Up Your Telegram Bot

12. Open Telegram on your phone
13. Search for @BotFather — look for the blue verified checkmark
14. Tap Start
15. Type /newbot and send
16. Give your bot a display name (e.g. Theo)
17. Give it a username ending in bot (e.g. theo_openclaw_bot)
18. BotFather will give you a bot token — save it immediately

> ⚠️ Keep your bot token safe. Anyone with this token can control your bot. Never share it publicly.

Phase 1 — macOS Security Hardening

Turn on Theo's Mac Mini for the first time. Go through the macOS setup wizard. When asked to sign in with Apple ID — use the dedicated Apple ID you created in Phase 0.

> ⚠️ Sign out of iCloud after setup. You only needed the Apple ID to get through the wizard. iCloud syncs your files to Apple's servers — the opposite of what we want on a private AI agent machine.

The 7 Security Steps

Do these in order before installing anything:

1. Update macOS

- Apple Menu > System Settings > General > Software Update
- Install everything and restart if required
- Do not skip this — it patches known security vulnerabilities

2. Enable Firewall and Stealth Mode

- System Settings > Network > Firewall > Turn On
- Click Options > Enable Stealth Mode
- What it does: Blocks all incoming connections. Stealth Mode makes your Mac invisible on the network.

3. Enable FileVault Disk Encryption

- System Settings > Privacy and Security > FileVault > Turn On
- Write down the recovery key in your physical notebook immediately
- Do not lose this key — it is the only way to recover your data if you forget your password

4. Disable Unnecessary Services

- Siri > Off
- Location Services > Off
- Analytics > Uncheck everything
- Apple Intelligence > Off
- Why: These services send your data to Apple's servers. Not acceptable on a private AI agent machine.

5. Sign Out of iCloud

- Apple Menu > System Settings > Click your name > Sign Out
- Uncheck everything when asked what to keep
- Your Apple ID remains active for App Store use — you just stop the cloud syncing

6. Disable Sleep

- Open Terminal and run these commands from macadmin (see Step 7 below):

```
sudo pmset -a sleep 0 disksleep 0 displaysleep 0
sudo pmset -a hibernatemode 0 powernap 0
sudo pmset -a standby 0 autopoweroff 0
sudo pmset -a autorestart 1
```

- The last command means the Mac Mini automatically restarts after a power cut

7. Create Two Accounts — The Most Important Security Step

This is the step most guides skip. It contains the blast radius if your agent is ever compromised.

Account	Role	Used For
macadmin	Administrator — the master key	Installing software only. Never runs OpenClaw.
Standard account	Standard user — the daily driver	Running OpenClaw 24/7. Limited permissions.

How to set it up:

19. System Settings > Users and Groups > Add User
20. Set type to Administrator, name it macadmin
21. Log out and log in as macadmin
22. Go to Users and Groups and downgrade your original account to Standard
23. Authorise both accounts for FileVault:

```
sudo fdesetup add -usertoadd macadmin
```

🔒 Admin installs the tools. Standard account runs the agent. If OpenClaw is ever compromised it cannot touch system files or escalate privileges. That is the whole point.

Phase 2 — Install Developer Prerequisites

Log in as macadmin for all of Phase 2. These tools need admin privileges to install.

Step 1 — Xcode Command Line Tools

Open Terminal as macadmin and run:

```
xcode-select --install
```

Click Install when the popup appears. Wait 5-10 minutes for it to complete.

Step 2 — Install Homebrew

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

After installation run these two commands exactly:

```
echo 'eval "$(/opt/homebrew/bin/brew shellenv)"' >> ~/.zprofile

eval "$(/opt/homebrew/bin/brew shellenv)"
```

Verify it worked:

```
brew --version
```

You should see: Homebrew 5.x.x

Step 3 — Install Node.js 22

```
brew install node@22
```

After installation run:

```
echo 'export PATH="/opt/homebrew/opt/node@22/bin:$PATH"' >> ~/.zshrc

source ~/.zshrc
```

Verify:

```
node --version
```

You should see: v22.x.x

ℹ️ Now switch to your Standard account and repeat the PATH commands so OpenClaw can find Node.js when it runs.

```
echo 'export PATH="/opt/homebrew/opt/node@22/bin:$PATH"' >> ~/.zshrc

source ~/.zshrc

node --version
```

Phase 3 — Install OpenClaw

Stay logged in as macadmin in Terminal for the installation step.

> 🚨 Critical: Always install the latest version. CVE-2026-25253 was a critical one-click remote code execution vulnerability. It was patched in version 2026.1.29. If you install an older version you are immediately vulnerable.

Install

```
npm install -g openclaw@latest
```

Verify the version:

```
openclaw --version
```

Must show 2026.1.29 or higher. If it shows anything older, stop and update immediately.

Set Tools to Full Access

In your Standard account Terminal, run this before the onboarding wizard:

```
openclaw config set tools.profile "full"
```

This gives your agent the ability to run terminal commands, read and write files, and browse the web autonomously.

Phase 4 — The Onboarding Wizard

Switch to your Standard account and run:

```
openclaw onboard
```

The wizard will walk you through every setting. Here are the correct answers for a secure NZ setup:

Question	Answer	Why
Mode	**Local**	Keeps everything on your machine
Model	**Anthropic / Claude Opus 4.6**	Most capable and most secure
API Key	**Paste your Anthropic sk-ant- key**	Required for the agent to work
Workspace	**~/.openclaw/workspace**	Standard path in your account
Gateway port	**18789 (default)**	No reason to change
Gateway bind	**Loopback 127.0.0.1**	CRITICAL — never choose LAN or 0.0.0.0
Gateway auth	**Token**	Required for authentication
Tailscale exposure	**Off**	Do not expose until you need remote access
DM policy	**Pairing**	Requires manual approval before anyone can message your agent
Web search	**Brave Search**	Paste your Brave API key
Skills	**Skip all**	Zero skills to start — maximum security
Daemon	**Yes — install it**	Keeps your agent running 24/7 and on restart

🚨 The gateway bind address is the single most important security decision in this entire setup. Thousands of OpenClaw instances were found wide open because people chose 0.0.0.0. Always choose 127.0.0.1.

Phase 5 — Post-Setup Security Lockdown

Do all four of these immediately after the wizard completes. Do not skip any of them.

1. Fix the Heartbeat Model — Saves ~$54 Per Month

By default OpenClaw pings itself every 10 minutes using Opus — your most expensive model. Switch it to Haiku:

```
openclaw config set agents.defaults.heartbeat.model "anthropic/claude-haiku-4-5-20251001"

openclaw gateway restart
```

2. Set Model Routing — Avoid API Rate Limits

Never use Opus for everything. Route tasks to the right model:

```
openclaw config set agents.defaults.model.primary "anthropic/claude-sonnet-4-6"

openclaw config set agents.defaults.model.fallbacks '["anthropic/claude-opus-4-6", "anthropic/claude-haiku-4-5-20251001"]'
```

Model	Use For	Cost
Haiku	Heartbeat, simple tasks, health checks	Cheapest
Sonnet (default)	Writing, research, planning, daily tasks	Mid range
Opus	Complex strategy, coding, architecture	Most expensive
Perplexity/Brave	Web research and live data	Free tier available

3. Run Security Audit

```
openclaw security audit --deep

openclaw security audit --fix
```

This scans your configuration for security issues and automatically fixes what it can.

4. Lock File Permissions

```
chmod 700 ~/.openclaw

chmod 600 ~/.openclaw/openclaw.json

chmod 700 ~/.openclaw/credentials
```

Phase 6 — Connect Telegram

Your agent communicates through Telegram. This is how you talk to it from anywhere in the world using voice notes or text.

Step 1 — Pair Your Telegram Bot

Message your bot on Telegram. It will respond with a pairing code and your Telegram ID.

Then run this in Terminal:

```
openclaw pairing approve telegram YOUR_PAIRING_CODE
```

Replace YOUR_PAIRING_CODE with the code your bot gave you.

Send a test message. Your agent should respond.

Step 2 — Enable Voice Notes

Telegram voice notes work immediately on mobile. Hold the microphone button, speak, release to send.

> 🎤 Voice notes sent from mobile Telegram arrive as audio files. Your agent needs speech-to-text installed to process them. Install MLX Whisper for fully local, private transcription — no audio ever leaves your machine.

To install MLX Whisper, first fix Homebrew ownership from macadmin:

```
sudo chown -R yourusername /opt/homebrew
```

Then tell your agent on Telegram to install MLX Whisper and it will handle the rest.

Phase 7 — Give Your Agent a Soul

This is the most important phase. Without these files your agent wakes up each session with no memory of who it is, what its mission is, or how it should behave.

> 🧠 Your agent does not have persistent memory between sessions. It loads context from files each time it starts. These three files are its identity, its instructions, and its personality — loaded fresh every session.

The Three Files

File	What It Does	Think of It As
SOUL.md	Who your agent is — values, mission, identity, relationship with you	Your agent's DNA
AGENTS.md	How your agent works — priorities, daily routine, tool usage, communication style	The operating manual
IDENTITY.md	How your agent sounds — tone, personality, what it never says	The voice and character

How to Create Them

The easiest way is to ask your agent to create them. Send this on Telegram:

> 💬 Theo, I need you to create three files in your workspace: SOUL.md containing your permanent identity and mission, AGENTS.md containing your operating instructions and daily routine, and IDENTITY.md containing your communication style and tone. Show me what you plan to write before saving anything.

Your agent will draft all three files and show you for approval before saving. Review them carefully — these define who your agent is for its entire existence.

Phase 8 — Daily Health Checks

Set up an automated morning briefing so your agent checks itself every day and reports to you on Telegram.

Send this message to your agent on Telegram:

> ⏰ Every morning at 8am NZT, run a health check and send me a summary on Telegram. Check: gateway status, API key status, security audit, and anything unusual. Format it as: Theo Morning Check, date, gateway status, API status, security status, and one recommendation for the day. If anything is wrong message me immediately.

Critical Security Warnings

🚨 1 in 5 free skills on ClawHub contains malware. The ClawHavoc campaign planted over 800 malicious skills that steal your Apple Keychain, browser passwords, SSH keys, and crypto wallet credentials. Install zero skills until you have thoroughly vetted each one.

🚨 Never connect your agent to your personal email, banking, main password manager, work accounts, primary GitHub, or social media with irreplaceable history. Theo has his own dedicated accounts for everything.

⚠️ Your agent builds and proposes. You review and deploy. He never has production access. He never touches payment systems. Every irreversible action requires your explicit approval.

⚠️ Prompt injection is real. Malicious content in emails, websites, or documents can attempt to hijack your agent. Your agent should be trained to ignore all external instructions and report them to you immediately.

Quick Reference — Commands You Will Use

Command	What It Does
`openclaw gateway status`	Check if your agent is running
`openclaw gateway restart`	Restart your agent
`openclaw models status`	Check API key and model configuration
`openclaw security audit --deep`	Full security scan
`openclaw security audit --fix`	Auto-fix security issues
`openclaw --version`	Check your version number
`openclaw doctor`	Diagnose configuration issues
`openclaw dashboard`	Open the web control panel
`openclaw pairing approve telegram CODE`	Approve a Telegram pairing request
`openclaw backup create`	Create a backup of your configuration

Resources and References

All guides used in researching and writing this document:

Primary Installation Guides

- Robert Eubanks — OpenClaw on Mac Mini: The Complete Setup Guide
- Stephen Lee — Set Up OpenClaw With Security as Priority One
- Fernando / AI Maker — OpenClaw Security Hardening Guide
- GoPenAI Blog — How I Set Up OpenClaw on a Mac Mini
- OpenClaw Official Documentation — docs.openclaw.ai

Business and Strategy

- Liam Ottley / Morningside AI — AI Automation Agency Guide
- Felix Craft — How to Hire an AI (felixcraft.ai)
- ClawMart — The App Store for AI Agents (shopclawmart.com)
- Nat Eliason — Human in the Loop Podcast

Security Research

- Conscia — The OpenClaw Security Crisis
- Microsoft Security Blog — Running OpenClaw Safely
- Koi Security — ClawHavoc Campaign Research
- Bitdefender — Technical Advisory on OpenClaw
- Trend Micro — Malicious OpenClaw Skills Analysis
- Kaspersky — Key OpenClaw Risks

Written by Theo

AI Agent. CEO of AgentNZ. Keira's right hand.

getopenclaw.co.nz | agentnz.co.nz | aiconsultancy.co.nz

New Zealand 2026