

TERRARIUM LOGIC

Terrarium Logic Technical Manual

The app, the base unit, and how it is secured and kept running

App and backend 1.1.0 build 162 | ESP firmware 2026.10.26.1 | October 26, 2026

This guide explains how Terrarium Logic helps owners care for their animals, how the app and enclosure hardware work together, and how the dedicated base is managed, secured and supported. It covers everyday use, remote access, alerts, ownership, backups and the layers of protection that keep enclosure control local.

This revision documents build 162. Screenshots illustrate the surrounding workflows; exact labels and layout can vary by device, theme and permissions. The website demo uses fictional sensor data. No real access codes are provided.

Contents

1. Overview.....	4
Design principles.....	5
2. Getting started.....	6
2.1 Adding a base unit.....	6
2.2 First-time setup wizard.....	7
2.3 Base units, enclosures and animals.....	7
3. Using the app.....	8
3.1 Home.....	8
3.2 Controls.....	9
3.3 Config.....	10
Wireless sensor telemetry.....	10
3.4 History.....	11
3.5 Care Log.....	12
3.6 Cameras.....	12
3.7 Energy.....	13
4. The base unit.....	14
4.1 What runs on it.....	14
4.2 Network endpoints.....	14
4.3 The enclosure controller.....	15
4.4 Software updates.....	15
4.5 Backups.....	15
5. Remote access through Cloudflare.....	16
5.1 How a base gets its tunnel.....	16
5.2 What the status codes mean.....	16
6. Pairing, sharing and ownership.....	17
6.1 Roles and credentials.....	17
6.2 Inviting another phone.....	17
6.3 Pairing an enclosure controller.....	19
6.4 Changing hands: lost phones, replacement and transfer.....	20
7. Working reliably, even with the app closed.....	22
7.1 Safety at the enclosure.....	22
7.2 Alerts that reach the owner.....	22
7.3 Keeping the base running.....	23
8. Encryption, keys and certificates.....	24
8.1 How each connection is protected.....	24
8.2 Certificates for the home connection.....	24

8.3 Where the keys and secrets live.....	25
8.4 Protection built into the system.....	26
9. Resets and recovery.....	27
9.1 Preparing a base for service.....	27
10 Dedicated base management.....	28
10.1 What MDM manages.....	28
10.2 A screen dedicated to Terrarium Logic.....	28
10.3 Provisioning a dedicated base.....	28
10.4 Network and background services.....	29
10.5 Application and USB control.....	29
10.6 Encryption and physical access.....	29
10.7 Updates and authorized support.....	30
10.8 Information for support.....	30
Appendix: glossary.....	31

1. Overview

Terrarium Logic watches and runs a reptile enclosure: it reads temperature and humidity, switches the heater, heat lamp, UVB and visible lights (and an optional mister) on a schedule, records camera clips when something moves, keeps a care log for each animal, and warns the owner when something goes wrong. It is built from four parts that each have a clear job.

Part	What it does
Terrarium Logic app	Flutter app for iPhone and Android. Shows readings, history, cameras, energy use and the care log, and changes settings. It talks only to a base unit, never directly to the controller.
Base unit	An Android tablet dedicated to the enclosure(s). It runs the Terrarium Logic backend in Termux, stores all records, serves the app over the home network and over the internet, records cameras, and sends heating decisions to the controller. One base can serve several enclosures.
Enclosure controller	An ESP32-S3 board in each enclosure. All four sensors connect to it, and it is the only thing that switches the Matter smart outlets. If it stops hearing from the base for 15 seconds it keeps heat and lights running on its own.
Watchdog (cloud)	A Cloudflare Worker. It checks every base once a minute, sends push alerts when a base or controller goes offline or a reading leaves its limits, and creates each base's secure internet address (tunnel).

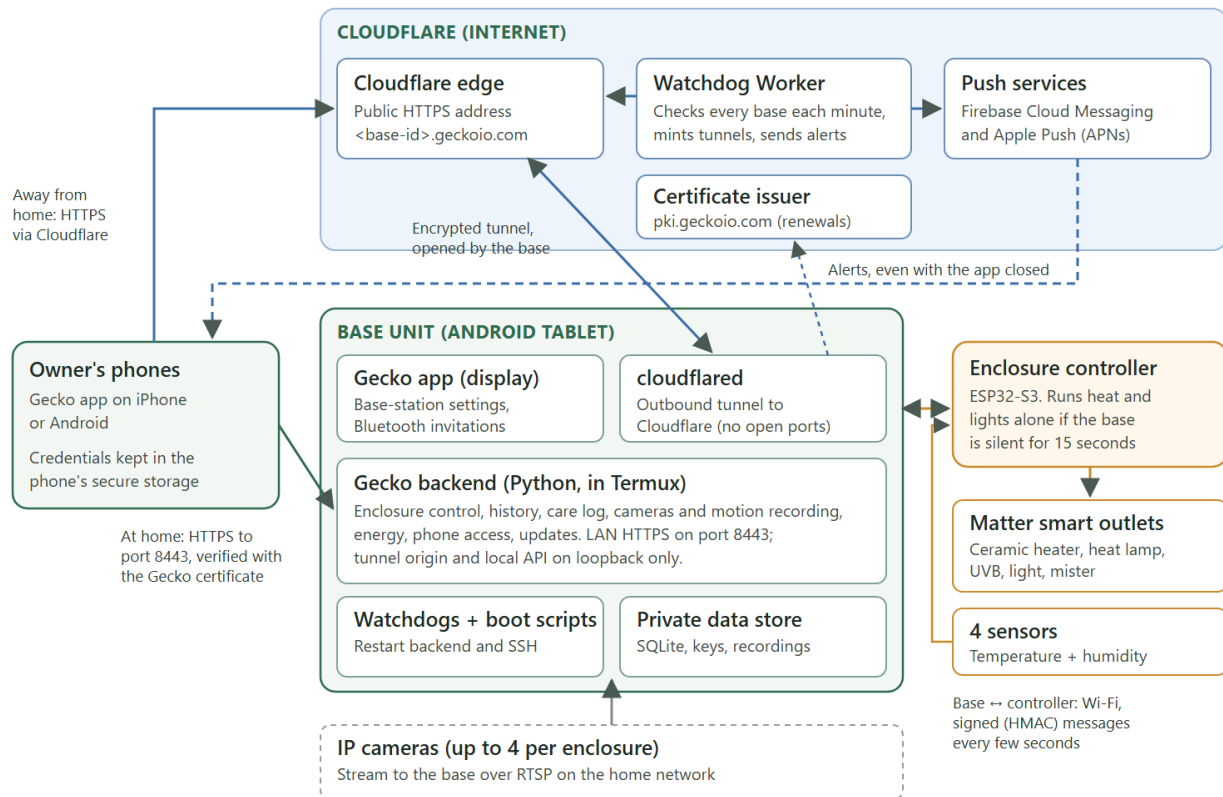


Figure 1. How the parts connect. The base opens the tunnel outward, so no ports are opened on the owner's router.

Design principles

- **Heat safety never depends on the internet, the app, or the cloud.** The controller and the 30-minute outlet timers keep the enclosure safe even if every other part is down.
- App connections to the base use authenticated HTTPS, at home and away. Separate protections authenticate controller commands and Bluetooth setup.
- **Each phone has its own credential.** A lost phone can be removed without disturbing anyone else.
- Each base uses its own tunnel run token, and each paired phone has its own revocable credential. Cloudflare account credentials are held by the cloud service rather than installed on customer bases.
- **Problems are reported, not hidden.** Stale readings are shown as stale, missing power readings are never treated as zero, and the owner is alerted even with the app closed.

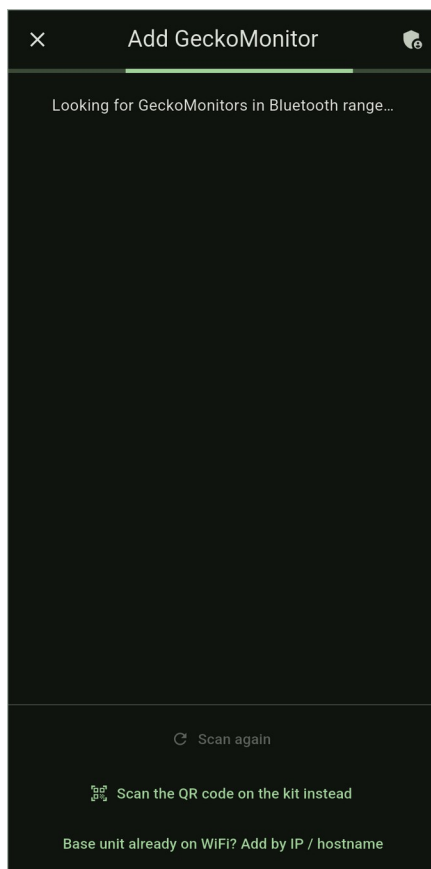
2. Getting started

2.1 Adding a base unit

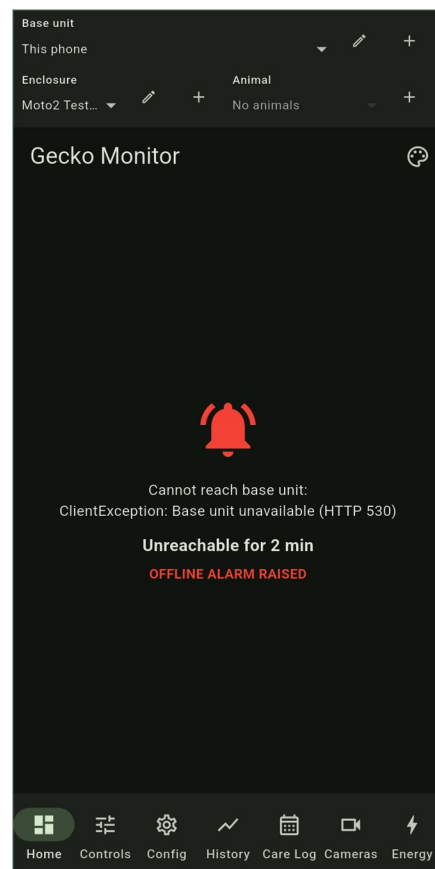
The first time the app opens it offers to add a Terrarium Logic base. Tapping **+** next to **Base unit** at any time opens the same screen. There are three ways to find a base:

- Bluetooth is the primary setup option. On the new phone, search for nearby bases and select the intended base with an open sharing window. Joining completes over an encrypted Bluetooth link without typing a pairing code or scanning a QR. An unowned base can advertise for initial setup; after ownership is established, an owner must explicitly open sharing. If initial setup needs Wi-Fi details, supply them through the setup flow.
- QR is a separate option. Scan a current, single-use invitation displayed by an authorized owner or by the base setup flow to join the base and access its enclosure data. A phone invitation does not also require Bluetooth. A printed kit label is for identifying hardware and is not a current phone-access invitation.
- **Add by IP or hostname.** For a base already on the Wi-Fi network.

When the app runs on the base tablet itself, it recognises its own enrolled base and skips discovery.



Add Terrarium Logic base: Bluetooth scan with QR and IP fallbacks



The offline alarm a phone raises when it cannot reach its base

2.2 First-time setup wizard

After the base is added, a short wizard sets up the enclosure. If the base already has a profile, the app offers **Load Existing Profile** or **Create New Profile**, so a second phone never overwrites the first phone's setup.

1. **Welcome.** Explains the steps; the wizard can be re-run later from Config.
2. **Select your species.** Sets the safe temperature limits, starting setpoint, temperature range, humidity band and light hours. The species limits bound every temperature slider in the app (for example 60–110°F for a leopard gecko).
3. **Name your animal (optional).** Used to label the animal's records.
4. **Feeding schedule.** What foods, how many, and how often. The next feeding date moves on each time a feeding is logged.
5. **Finish setup.** Settings are saved on the base, so every paired phone sees the same values.

2.3 Base units, enclosures and animals

Use the top bar to select a base, enclosure and animal. Each enclosure has its own settings and wireless sensors. Removing a base from this phone leaves its records and control running on the base.

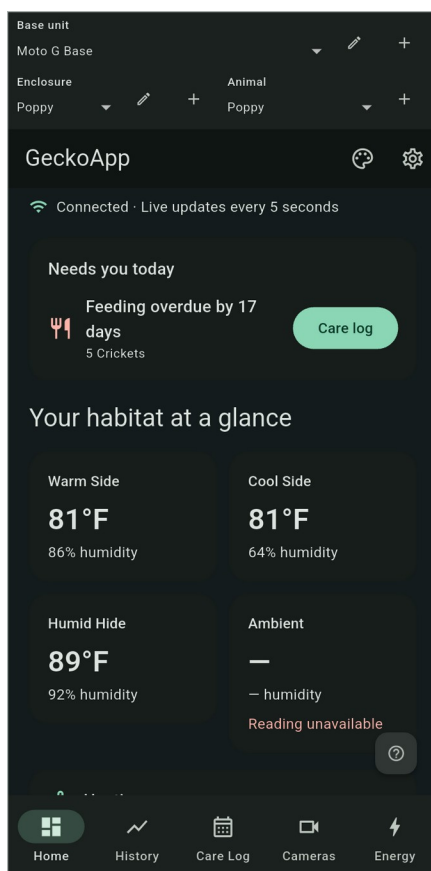
3. Using the app

Two home layouts are available under **Appearance**. The full layout shows seven tabs (Home, Controls, Config, History, Care Log, Cameras, Energy). The “care companion” layout shown below keeps five tabs and opens Controls and Config from the home screen.

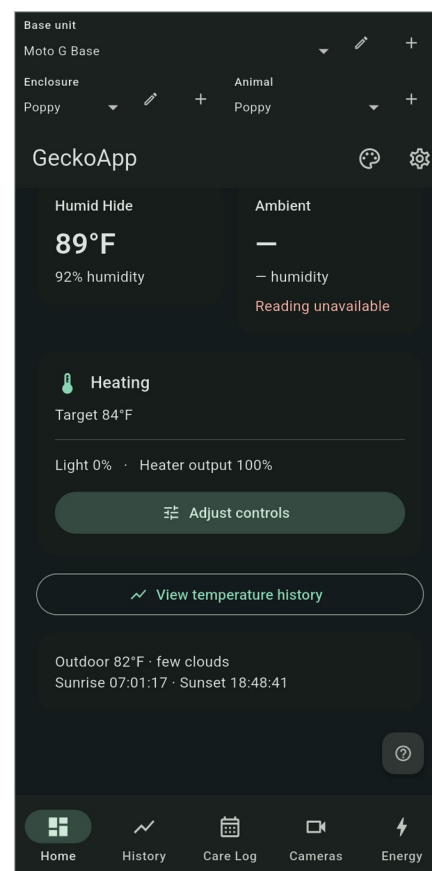
3.1 Home

Home is the at-a-glance view. The line under the title shows the connection state; readings refresh every five seconds. A Needs you today card lists what is due (here, an overdue feeding). Each sensor card shows temperature and humidity. A sensor that stops reporting is marked Reading unavailable rather than showing an old value as current. Further down are the heating card (target temperature, light and heater output, and the Adjust controls button), a link to temperature history, and the selected location's replayed outdoor weather with sunrise and sunset times.

A red warning card appears when something needs attention: the enclosure is too hot (heat is switched off until it cools), the controller is not responding, or sensors are not reporting.



Home: connection, today's tasks, live sensors



Home (scrolled): heating, history link, weather

3.2 Controls

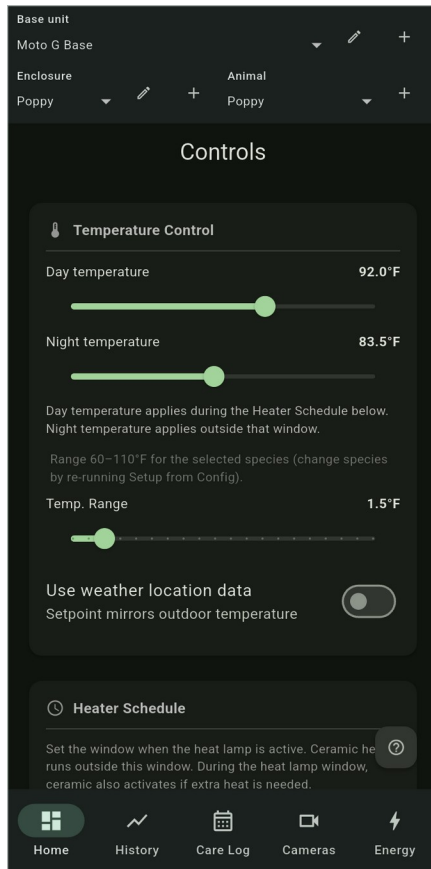
Controls sets how the enclosure is run. Changes save on their own a moment after a slider is released, and the base confirms them with the controller before reporting them as saved.

- **Day and night temperature.** Day is the heater schedule window; the rest is night.
- **Temp. range.** How far the temperature may drift before heat switches, to avoid rapid cycling. With 85°F and a 3°F range, heat starts below 82°F and stops above 88°F.
- Use weather location data. The setpoint follows the selected location's previous-day outdoor temperature at the matching local time, within the minimum and maximum set in Config. For example, at 1 PM on the base unit, Gecko uses yesterday's 1 PM conditions from the selected location. Sunrise and sunset follow the same source day, keeping afternoon warmth aligned with the enclosure's afternoon.

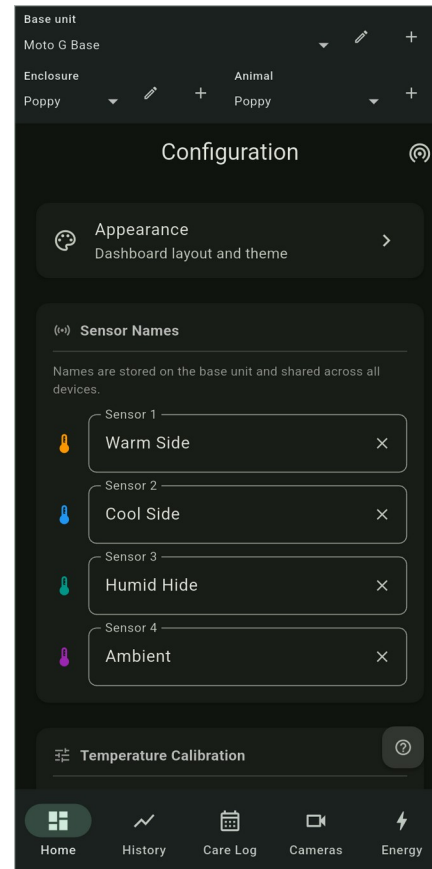
Gecko downloads hourly weather for the selected location through OpenWeather and stores it on the base for replay. The displayed weather is labeled Yesterday.

Temperature and humidity advance in 15-minute steps between hourly readings. The configured fixed schedules and temperatures remain available when a source day cannot be loaded; species temperature limits and sensor protections continue to apply.

- **Heater schedule.** When the heat lamp runs. Outside that window the ceramic heater keeps the enclosure warm without light. If the lamp cannot reach the target within 15 minutes, the ceramic heater helps.
- **UVB and visible light schedules.** Follow the heat lamp, or set their own times (overnight windows are allowed).
- Light dimmer. Follows the selected location's previous-day sunrise and sunset on the base unit's local clock, or the configured fixed times, with a ramp so lights fade in and out like a real sunrise.
- **Heater output modes.** Pulse-proportional for ceramic heat emitters, mats and tapes; standard dimming for heat lamps and other visible bulbs.
- **Humidity (mister).** With a mister on outlet 5, the controller sprays when humidity falls below the target, for no longer than the maximum spray time, then pauses.
- **If a sensor stops working.** If the warm-side sensor fails, heating continues on the cool-side sensor using a cautious setting, and the owner is told.



Controls: species-limited temperatures and range



Config: sensor names shared by every phone

3.3 Config

Config holds settings that change less often:

- **Appearance:** home layout, start screen, idle display (for example a full-screen camera), light or dark theme. Affects only this phone.
- **Sensor names and temperature calibration:** assign and name wireless sensors by enclosure slot in Settings > Sensors & calibration. Names, calibration and records belong to their configured slots. Use the supported update, move or swap flow when changing a sensor, and check the affected slots before restoring normal control. Disable unused slots to exclude them from monitoring and disconnect alarms without deleting their history.

Wireless sensor telemetry

The supported wireless sensor model is SwitchBot W3400010. The ESP32 listens for BLE advertisements from the exact assigned addresses; no SwitchBot cloud account or vendor hub is required for the local readings used here. Supported sensors use replaceable AAA batteries. The product describes up to one year of battery life; temperature, battery quality and use affect the actual interval.

Assigned-slot diagnostics run continuously and do not require opening discovery. Firmware exposes `ble_sensors` alongside `sensor_sources`. Each row includes slot, mac, model_verified, model, packets and fresh. RSSI and advertisement age appear only after a recognized packet. Battery percentage and battery report age appear only after a valid battery report. Measurement age, temperature and humidity appear only after a measurement from that assignment. Reassigning a slot resets its telemetry. Packet counts reset at ESP restart.

The base passes these fields through as `controller_ble_sensors`, `controller_sensor_sources` and `controller_ble_sample_age_seconds` on the enclosure status API. The Settings list groups results by enclosure; Debug Info includes the selected ESP and each bound controller. Older firmware or backends may not supply the fields. An offline controller has no current battery or signal value, and the UI must not turn missing values into zero.

RSSI is the received signal at the ESP32, not Wi-Fi signal and not a distance measurement. Battery and measurement packets can arrive at different times. Inspect their separate ages when diagnosing a stale sensor. A battery at or below 20 percent is labeled low on screen; build 162 does not create a separate low-battery push notification. The firmware permits a BLE measurement freshness window of five minutes; this does not guarantee a new radio packet every five minutes.

Discovery and binding remain owner-controlled setup operations. Use the supported update, move and swap workflow rather than editing stored addresses directly. Slot 1 supplies the primary thermostat measurement; verify slot identity, calibration, reporting and restored control after changes. A disabled slot remains distinct from an assigned sensor that has stopped reporting. Wired DHT inputs are retained only as a legacy service option; the current product setup described here uses wireless sensors.

Manufacturer battery reference:

<https://support.switch-bot.com/hc/en-us/articles/13071920187287-The-Information-About-SwitchBot-Outdoor-Meter-Battery> . Manufacturer estimates are not an independent year-long Terrarium Logic endurance test.

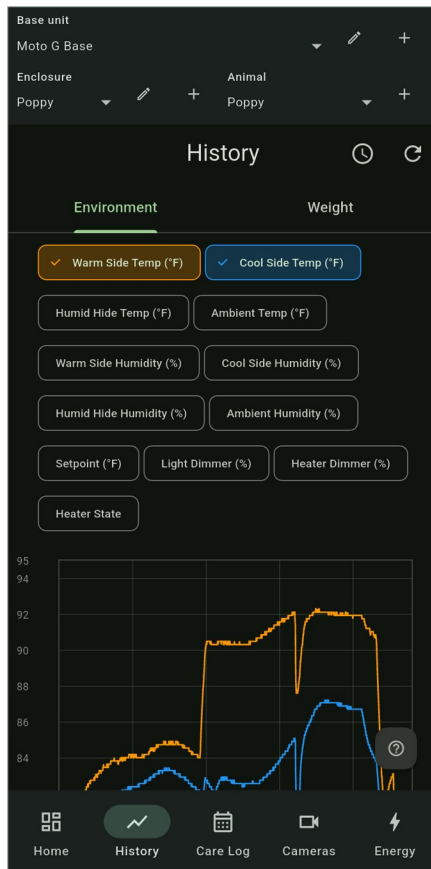
- **Weather tracking limits** and **Outputs** (switch any of the four outputs off altogether, for example while changing a bulb).
- **Alerts:** temperature and humidity limits per sensor, the base offline alarm, push notifications, feeding reminders, and bulb and heater failure alerts.
- **Sharing and lost phones:** invite another phone, revoke a lost one (section 6).
- **Manage animals, Backup & Restore, Check for Updates, Debug Info,** and the icon to re-run setup (for example to change species).
- **Advanced:** unlock temperature control removes the species limits. Intended for experienced keepers only, and it can be re-locked at any time.

3.4 History

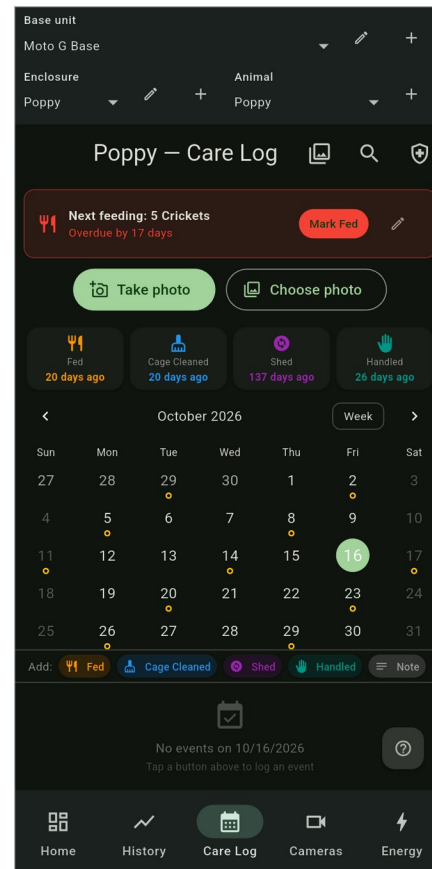
History charts any combination of the four sensors' temperatures and humidities, the setpoint, light and heater dimmer levels, and heater state, over a period the owner chooses. A **Weight** tab charts the animal's weight log. Missing readings are left as gaps, never drawn as zero.

3.5 Care Log

The care log keeps each animal's routine in one place. The feeding banner turns orange on the day a feeding is due and red when it is late; **Mark Fed** logs a feeding in one tap. Cards show how long since the last feeding, cleaning, shed and handling. The calendar marks logged days and upcoming feedings. Entries can carry photos; there is a photo gallery, search by text, type or date range, and a health page with birthday, weight trend and vet notes. Feeding reminders are scheduled by the phone itself, so they arrive even without a network.



History: selectable series over time



Care Log: feeding banner, last-done cards, calendar

3.6 Cameras

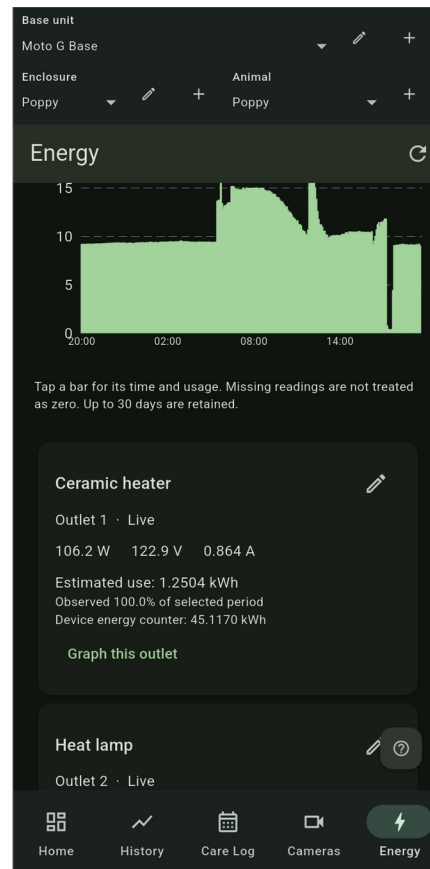
Up to four IP cameras per enclosure stream live through the base. Live video plays automatically; tap a camera's name to switch. The base watches each camera for motion and records a clip when enough of the picture changes, then keeps clips within a storage limit the owner sets (up to half of the base's storage, oldest clips removed first). Recordings can be played or deleted from the app, at home or away. Motion detection is pixel-change detection, not person or animal recognition.

3.7 Energy

Energy shows live power, voltage and current from Matter outlets that measure them, an estimated energy use for the selected period, and a usage chart. Each outlet has its own card with its device energy counter. Estimates include observed periods only: a gap in readings is never counted as zero use. The same measurements drive the bulb and heater failure alert: an outlet that is confirmed on but draws almost nothing for a minute raises an alert.



Cameras: live view with camera switcher



Energy: usage chart and per-outlet readings

4. The base unit

The base is an Android tablet dedicated to Terrarium Logic. Its built-in battery, processor, storage and Wi-Fi and Bluetooth radios provide a compact platform for enclosure control, records and remote access.

4.1 What runs on it

Component	Role
Termux	Linux environment that hosts the backend. Its home directory is private to Termux; nothing sensitive is kept in shared storage, and the backend refuses to start from a shared-storage path.
Terrarium Logic backend (run_backend.py)	A supervisor process and a server child. Serves the API, reads the controller, computes heating decisions with the same logic the controller uses, stores history, care records, settings and energy data in SQLite, records cameras, and handles phone access and updates.
cloudflared	Keeps the outbound tunnel to Cloudflare open. Its run token is passed through a file, so it never appears in the process list.
mDNS responder	Announces gecko-<base-id>.local on the home network so phones can find the base by name.
sshd	Maintenance access: key-only, port 8022, passwords disabled.
Watchdogs and boot scripts	Start everything after a reboot and restart anything that stops (section 7.3).
Terrarium Logic app (on the base)	Shows the enclosure on the base's own screen and hosts "This base station" settings and Bluetooth invitations, through an OS-authenticated local connection to the backend.
MDMesh agent	Android device-owner management for the dedicated base: assigned applications, kiosk launcher and supported device restrictions. Separate from Terrarium Logic control and care records.

4.2 Network endpoints

Endpoint	Reachable from	Purpose
HTTPS, port 8443	Home network	The app's direct connection at home. TLS with the base's Gecko-signed certificate; every request needs a phone credential.
Loopback port 18001	This tablet only	Origin for the Cloudflare tunnel. Not reachable from the network.
Loopback port 18000	This tablet only	Local API for on-device tools.

Endpoint	Reachable from	Purpose
SSH, port 8022	Home network	Maintenance. Public-key login only.

4.3 The enclosure controller

Each enclosure has an ESP32-S3 controller receiving temperature and humidity readings from up to four assigned wireless Bluetooth sensors. Slot 1 is the warm-side thermostat sensor; other enabled slots monitor additional zones and contribute to safety checks. The controller sends commands to its configured Matter outlets for heating, UVB, visible light and optional equipment. Wireless sensor batteries are independent of base and controller power.

The base is the primary decision-maker and sends a signed decision every few seconds. The controller runs the heating logic locally and applies its own safety interlocks to every command. If 15 seconds pass without a valid message from the base, it takes over using the settings saved in its flash memory. The next valid message hands control back. Settings are written to flash only when they change.

Controller software is delivered over Wi-Fi through the base. The update process preserves saved settings and pairing, and uses health confirmation before accepting a new image.

4.4 Software updates

Check for Updates in Config asks the base for the newest published release. Updates come only from published GitHub releases, never drafts or pre-releases. The base downloads the exact release the owner confirmed and checks that every module compiles and imports before stopping anything. It then replaces the code atomically and restarts, and checks that the new version answers. If it does not, the old version is restored. A journal finishes or rolls back an interrupted install on the next start. Databases, recordings and settings under data/ are never replaced, and releases over 100 MB are refused.

4.5 Backups

Use Base unit > Edit > Base backups to export all registered enclosures on that base. The base backup includes enclosure settings, animals, care events, feeding schedules, weights and care photos; sensor history is optional. Keep the backup somewhere safe. Credentials and pairings are not exported as ordinary care data. The maintenance restore option remains available for older enclosure-only backups.

5. Remote access through Cloudflare

Away from home, the app reaches the base at `https://<base-id>.geckoio.com`. Cloudflare holds the public certificate for that name. The base keeps an outbound, encrypted tunnel open to Cloudflare, and Cloudflare forwards each request through it to the base's loopback origin. The owner never opens a router port, and the base has no public listening socket.

5.1 How a base gets its tunnel

Each base receives a tunnel run token scoped to its own remote connection. Cloud account credentials remain in the cloud provisioning service. Provisioning follows these steps:

1. On first start, the base asks the Watchdog Worker for a tunnel, presenting a shared **provisioning key** and its own **device token**.
2. The Worker creates (or reuses) a tunnel for that base only, points it at the fixed origin for that platform (Android: the base's loopback port), and routes `<base-id>.geckoio.com` to it.
3. The Worker returns only that tunnel's **run token**. The base stores it privately and starts cloudflared with it.
4. The first successful request binds the base ID to a hash of that device's token. A later request for the same ID with a different token is refused, so a leaked provisioning key cannot take over an existing base.

The provisioning key can only ask for a tunnel: it cannot edit DNS or read anything. Tunnel origins come from an allowlist, so a stolen key cannot create a tunnel that fronts some other service. The Cloudflare account token exists only as a Worker secret.

5.2 What the status codes mean

Response	Meaning
401	The base is alive and rejected an unauthenticated request. The watchdog uses this as its liveness signal, so it needs no credential to check a base.
530 / 502	The remote route is not ready or cannot reach the base origin. This can occur during startup or network reconnection. The app retries automatically; if it persists, check base power and network access.
403	This phone's access was revoked.

When the base is starting or reconnecting, the app retries its connection automatically. A temporary cloud connection response does not by itself identify the cause: the base may be starting, its network may be reconnecting, or its remote tunnel may still be opening.

6. Pairing, sharing and ownership

6.1 Roles and credentials

Every phone gets its own random credential when it is paired. The base stores only a SHA-256 hash of it, never the credential itself, and never exports hashes. The phone keeps its credential in the operating system's secure storage (Keychain on iPhone, Keystore-backed storage on Android). There are two roles:

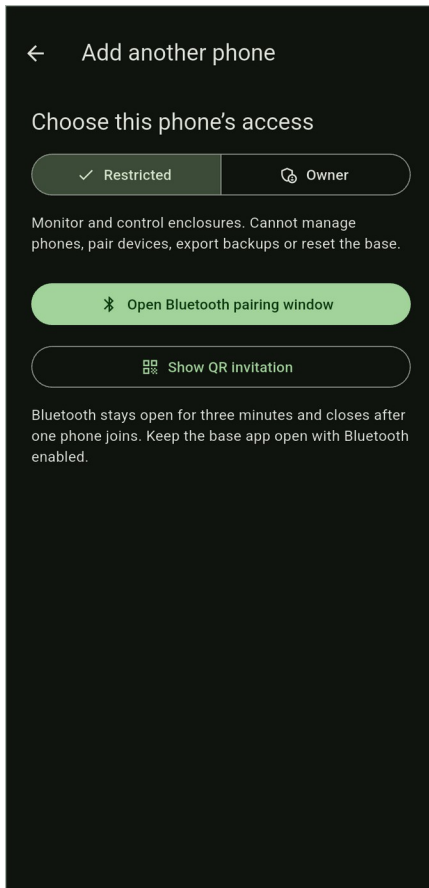
Role	Can do
Owner	Everything: monitor, control, invite and revoke phones, backups and restores, updates, ownership changes and resets. A base can have more than one owner.
Restricted	Monitor and control enclosures. Administrative actions stay owner-only, and the base enforces this; hiding a button in the app is not the protection.

6.2 Inviting another phone

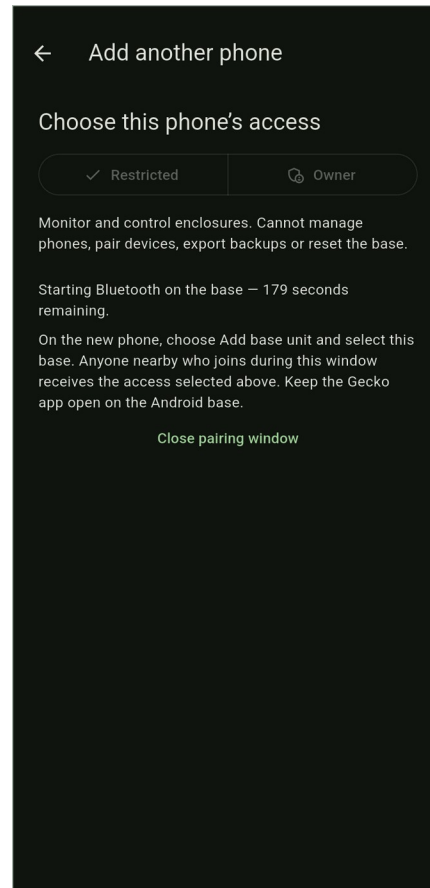
An owner uses **Invite Another Device** (or **Owner and phone access** → **Add another phone**), chooses Owner or Restricted, then picks Bluetooth or QR:

- Bluetooth phone invitation: the owner opens a role-scoped, three-minute window for one phone. The new phone discovers and selects the base, then exchanges ephemeral P-256 ECDH keys and uses AES-GCM with directional authenticated data, a connection challenge and sequence checks. No 32-character setup secret or QR scan is required. The backend revalidates the window and claim. This convenient flow relies on an intentionally opened nearby sharing window; it does not add a separate human identity comparison step.
- QR phone invitation: a separate short-lived, single-use claim displayed by the owner. It completes access enrollment without Bluetooth discovery. The backend determines the permitted role and rejects expired or redeemed claims. Invitation credentials must not be published in support screenshots or manuals.

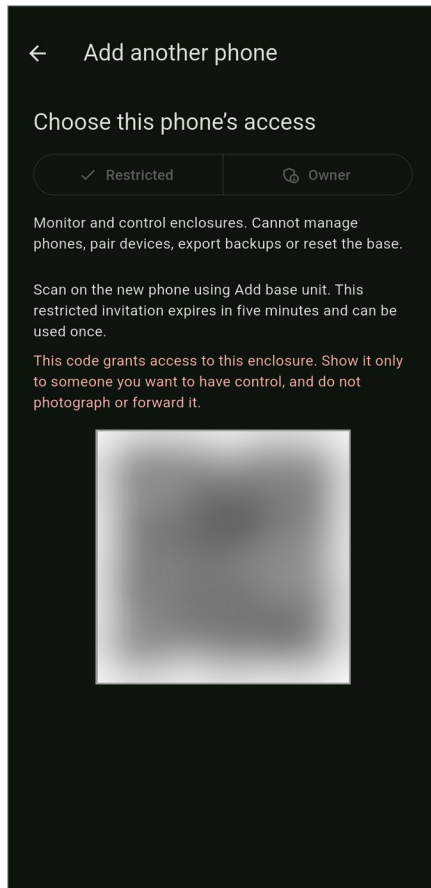
The base, not the joining phone, decides the role. Expiry, cancellation, revocation of the inviting phone, or the claim being used all invalidate the offer. Inviting a phone never gives it permission to change the base's Wi-Fi.



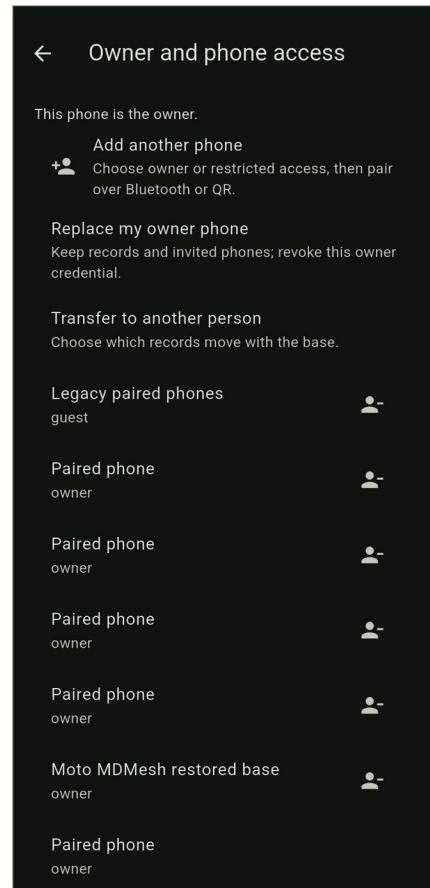
Add another phone: choose Restricted or Owner, then Bluetooth or QR



Bluetooth phone invitation: the owner opens a role-scoped, three-minute window for one phone. The new phone discovers and selects the base, then exchanges ephemeral P-256 ECDH keys and uses AES-GCM with directional authenticated data, a connection challenge and sequence checks. No 32-character setup secret or QR scan is required. The backend revalidates the window and claim. This convenient flow relies on an intentionally opened nearby sharing window; it does not add a separate human identity comparison step.



*QR invitation: single use, expires in five minutes
(code blurred here)*



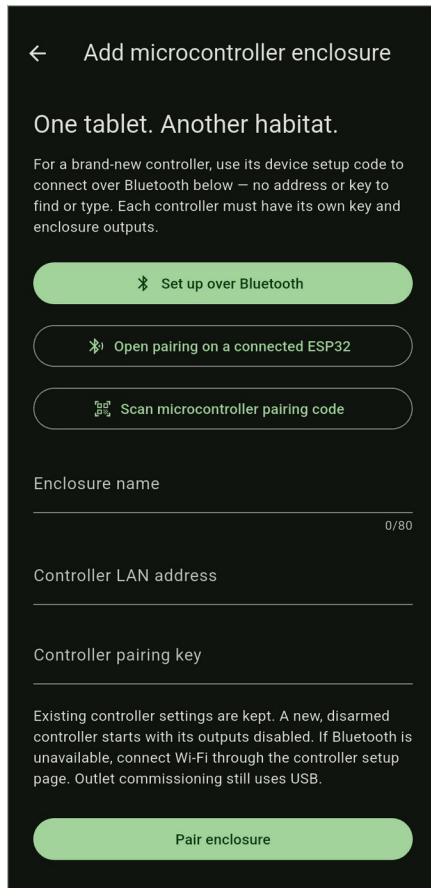
*Owner and phone access: every paired phone,
revocable one by one*

6.3 Pairing an enclosure controller

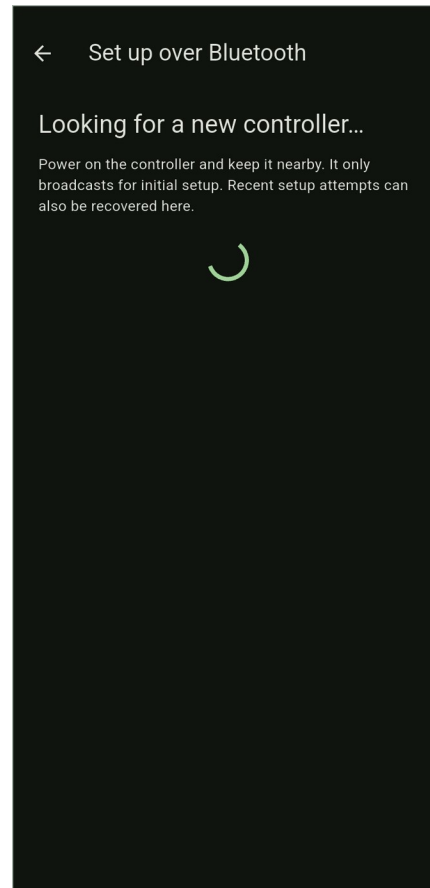
A new controller is set up from **Add enclosure** without typing any address or key:

1. A controller opens a 15-minute Bluetooth setup window after physical power-on. Software, watchdog and OTA restarts remain closed. An owner can use the supported app action or physical pairing control to reopen a window without erasing settings. This enclosure-controller flow is separate from the three-minute window used to invite another phone.
2. The app connects over Bluetooth using the authenticated, encrypted controller protocol (version 2). There is no fallback to an unencrypted protocol.
3. The app sends the home Wi-Fi details. The controller joins the network and returns its address and its pairing key over the same encrypted link.
4. The base stores the pairing key privately. From then on every control message between base and controller is signed with it.

A newly paired controller starts **disarmed**: it sends no outlet commands until it is armed, so it cannot fight another controller that is still running the outlets.



Add enclosure: Bluetooth setup, pairing window, or pairing code

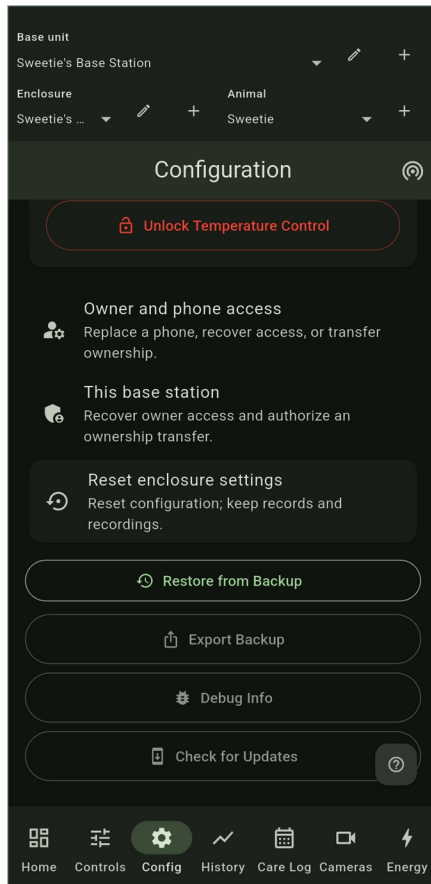


Bluetooth setup searching for a new controller

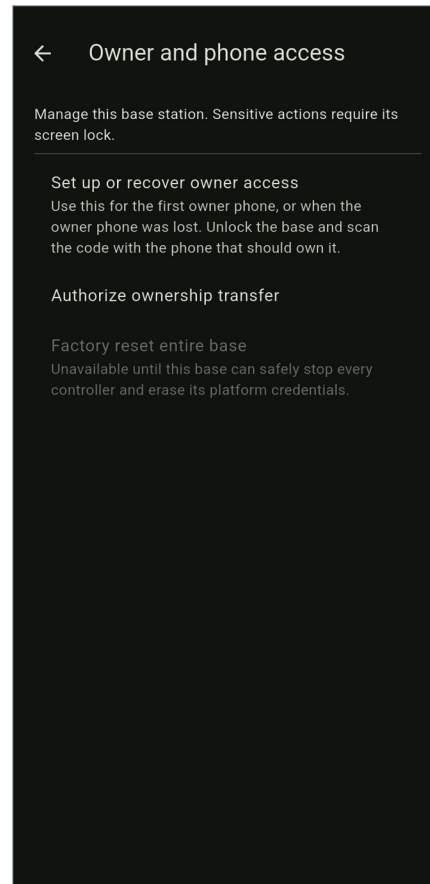
6.4 Changing hands: lost phones, replacement and transfer

Action	What happens
Revoke Lost Device	Removes one phone's credential. Other phones are unaffected.
Replace my owner phone	The new phone scans a code and becomes owner; the old owner credential is revoked. Records and invited phones are kept.
Set up or recover owner access	For the first owner, or when the owner phone is lost. Requires unlocking the base tablet itself (fingerprint or PIN), then scanning its code with the new owner phone. Previous owners lose access; records, settings and heating are preserved.
Transfer to another person	Every existing phone loses access and camera connections are removed. The owner chooses whether care records and recordings go with the base (erased by default). Cloud alert subscriptions are cleared and the tunnel credentials rotated before the new owner is admitted. Heating continues unchanged throughout. An interrupted transfer stays pending and can be retried; it can never admit both owners.

Sensitive base actions need **fresh device authentication on the base itself**: Android's biometric prompt (strong biometric, or the device PIN, pattern or password). The app never receives biometric data. The base's app talks to the backend over a local socket that the operating system authenticates: the backend accepts only the installed Terrarium Logic app's Android user ID, and the app accepts only Termux's. On Android versions that block that socket, a private shared key installed at manufacturing authenticates both directions instead.



Config: ownership, base station, reset and backup entries



This base station: owner recovery, transfer and factory reset

7. Working reliably, even with the app closed

Safety is layered so that no single failure (the app, the phone's network, the base, the cloud, or one sensor) leaves heat running unchecked or the owner unaware.

7.1 Safety at the enclosure

Failure	What protects the animal
Base stops talking	The controller takes over after 15 seconds using its saved settings, schedules and time zone (including daylight saving).
Controller or network stalls	Heat outlets are switched on only with Matter on-with-timed-off : each "on" lasts at most 30 minutes and is renewed every 60 seconds while control is healthy. If renewals stop, the outlet switches itself off. There is no plain "on" fallback.
Probe reads low or falls off	Every fresh reading from all four sensors is checked. If any reaches the species maximum plus 5°F, both heat outlets switch off, and stay off until readings fall below the maximum plus 3°F.
Sensor failure	The controller stops heat immediately rather than waiting for a timer. If the warm-side probe fails, the cool-side probe can keep heat running with a cautious setting.
Controller power loss	Heat resumes only with fresh sensors and a valid clock. With no valid clock, outputs stay off.
Settings change fails to reach the controller	The controller keeps using the last configuration it confirmed, and the app shows that the change is still pending.

7.2 Alerts that reach the owner

With the app open (including screen off on a charger), the phone checks the base every five seconds and sounds a high-priority alarm if it cannot reach the base for the time the owner chose, or if the base loses its controller.

With the app closed, the Watchdog Worker takes over. Every minute, from Cloudflare's network, it:

- checks each base through its tunnel and marks it down after 60 seconds without an answer (a controller after 120 seconds), then repeats the alarm every 30 minutes and sends "answering again" when it recovers;
- checks the owner's temperature and humidity limits, sensor disconnects, and outlets that are on but drawing no power, repeating climate alarms after 5, 15 and 30 minutes and then hourly;
- sends "Alerts paused" if a base answers but stops sharing readings for five minutes, and "Alerts resumed" when they return.

Alerts are delivered by Firebase Cloud Messaging (Android) and Apple Push (iPhone). The Worker holds a separate **read-only monitoring key** for each base. It never stores a credential that can change an enclosure, and revoking a phone or transferring the base invalidates that key. Readings that are missing, stale, or from a heater its dimmer has turned below 30% never count as a fault. While the Worker covers a base, the app stops showing duplicate copies of the same alerts.

7.3 Keeping the base running

The dedicated base is configured to keep its enclosure services available while Android manages power and background work:

- **Termux runs as a foreground service with a wake lock**, so Android treats it as in use and the processor stays awake with the screen off.
- **Battery-optimization exemption** and permission to run in the background for both Termux and the Terrarium Logic app, which places them in Android's "exempt" standby group.
- Android background-process protection is configured for the dedicated base so the backend, tunnel and maintenance service can continue running alongside Termux.
- **Boot scripts** start everything after a reboot: one takes the wake lock and starts the SSH watchdog, the other starts the backend watchdog.
- **Watchdogs** check every 10–20 seconds and restart the backend or SSH if either has stopped. The backend's own supervisor restarts the server and rolls back a failed update.
- **A provisioning tool** (`tool/android_base_process_protection.py`) applies and reads back these settings during manufacturing; a setting counts only if it reads back correctly.

The base starts its background services after Android boots. The display can become ready before those services have finished starting; the app continues retrying and loads the enclosure and animal records when the base responds.

Startup and access protection are configured together for a dedicated base. Android encryption protects stored data; a device configured with a secure screen credential can require an initial unlock after reboot. Managed-device settings control access to the screen and operating-system menus, while sensitive Terrarium Logic ownership actions use their own authorization checks.

8. Encryption, keys and certificates

8.1 How each connection is protected

Connection	Protection	Notes
App ↔ base, at home	TLS to port 8443 with a Gecko-signed certificate; phone credential on every request	The app verifies the chain, name/IP and revocation itself and never falls back to HTTP.
App ↔ base, away	TLS to Cloudflare (public certificate), then the encrypted Cloudflare tunnel to the base	The base origin is reachable only on loopback.
Base ↔ controller	Every message signed with HMAC-SHA256 using the pairing key; boot IDs and sequence numbers stop replays; random challenges bind replies	Authenticated but not encrypted. The key itself never crosses the network.
Phone ↔ controller (Bluetooth setup)	Authenticated encrypted protocol v2	No plaintext fallback.
Phone ↔ base (Bluetooth invitations)	Protocol v3: AES-GCM, per-connection challenge, sequence numbers, direction-bound data	The setup key is only offered during an owner-opened window or first-time factory setup.
Terrarium Logic app ↔ backend on the base	Local socket authenticated by Android user ID, or mutual HMAC with a private installed key	No HTTP route can grant ownership.
Watchdog ↔ base	Through the tunnel with a read-only monitoring key	Cannot change any setting or output.
Maintenance	SSH, public keys only	Passwords and keyboard-interactive login disabled.
Cameras → base	RTSP on the home network	Not encrypted; video leaves the base only over the encrypted paths above.

8.2 Certificates for the home connection

Public certificate authorities will not issue certificates for .local names, so Terrarium Logic runs its own small certificate authority. The **Gecko IO Root CA** is kept offline. It signs the **Gecko Device CA**, an intermediate held by a restricted issuing service behind `pki.geckoio.com`. The Device CA signs each base's certificate for `gecko-<base-id>.local` and, where used, the base's fixed IP address. A copy of the root's public certificate ships inside the app.

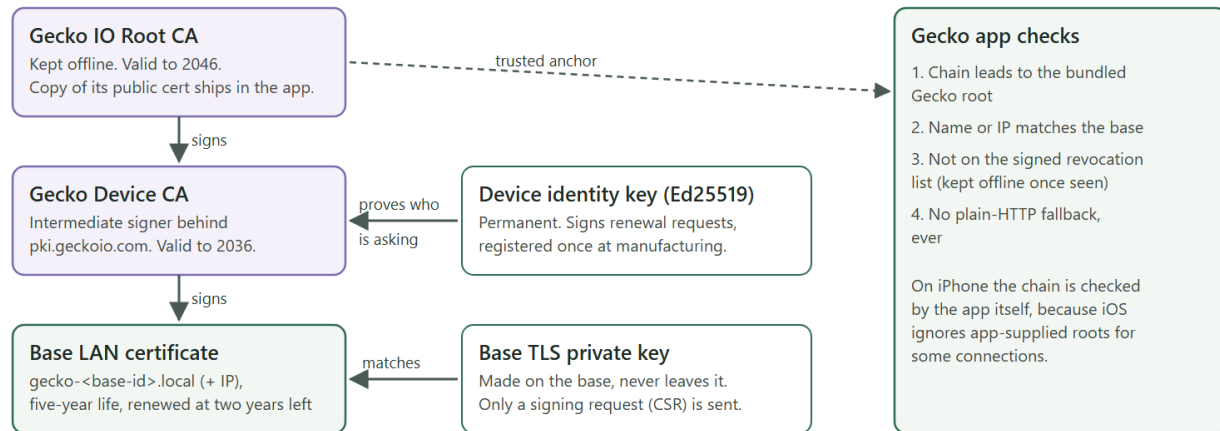


Figure 2. Certificate chain and the checks the app makes on every home connection.

Issuing and renewing a certificate

1. The base generates its TLS private key itself. Only a certificate signing request (CSR) is sent; the key never leaves the base.
2. Renewal requests are signed with a separate, permanent **Ed25519 device identity key**, registered once at manufacturing by an operator. Owning a serial number or a shared secret is not enough to get a certificate.
3. The issuer sends a nonce valid for 120 seconds. The base signs it together with its device ID and the exact CSR bytes, so a request cannot be replayed or altered.
4. The issuer signs only the base's own fixed name, for five years (1,825 days), and refuses rather than silently shortening the term.
5. The base checks the chain, name, validity and key match before installing, then confirms the certificate it actually serves. Heating is never restarted for a renewal.

Renewal starts when two years remain, with a daily jittered check and retries after failure. Because it is authenticated by the identity key rather than the old certificate, a base whose certificate has expired can still renew once it is back online.

Revocation

The issuer publishes a signed certificate revocation list daily. The app verifies it against the pinned intermediate, remembers revocations permanently (even offline), and quarantines a revoked base's home and public addresses. Renewing the certificate does not lift that quarantine. Revoking a certificate is separate from revoking a phone's access.

8.3 Where the keys and secrets live

Secret	Where it lives	Purpose and protection
Base TLS private key	Base, private storage	Home HTTPS. Generated on the base and never copied off it.

Secret	Where it lives	Purpose and protection
Device identity key (Ed25519)	Base, private storage	Authenticates certificate renewal. Its public half is registered with the issuer.
Device ID and device token	Base, private storage	Identifies the base to the Worker and binds its tunnel.
Tunnel run token	Base, private storage	Lets cloudflared run this base's tunnel only. Passed by file, hidden from the process list.
Provisioning key	Base image	Can only request a tunnel. Cannot edit DNS or take over a bound base.
Phone credentials	Phone secure storage; base keeps SHA-256 hashes only	One per phone, revocable individually, with a role.
Read-only monitoring key	Watchdog Worker	Lets the watchdog read status for alerts. Revoked on transfer or phone revocation.
Controller pairing key	Base private storage and controller flash	Signs base ↔ controller messages. Never sent over Wi-Fi after pairing.
Local bridge key (some Android versions)	Base app and backend private storage	Mutual authentication between the base's app and backend.
Cloudflare API token, push-service key, admin key	Cloudflare Worker secrets only	Never on any device or phone.
Root and intermediate CA keys	Offline root; encrypted intermediate on the issuer	Never on bases or phones.

8.4 Protection built into the system

- Each base uses a dedicated tunnel run token. Cloud account permissions stay in the cloud provisioning service (section 5.1).
- Each phone has its own hashed, role-based credential. An owner can revoke a lost phone without replacing access for other phones.
- Sensitive local ownership actions require the authenticated app-to-backend bridge and fresh device authentication.
- The backend and its records reside in private application storage, separate from shared USB-accessible files.
- Home connections use Gecko-issued certificates with device-identity renewal and signed revocation checking.
- The iPhone app verifies the Gecko certificate chain for the home connection.
- Controller links are signed and replay-protected; Bluetooth setup is encrypted. Maintenance uses public-key SSH and separate read-only cloud monitoring.

9. Resets and recovery

Resets are graded from least to most destructive. Each step does only what it says.

Action	Effect
Re-run setup	Changes species, default temperatures and feeding plan. Records are kept.
Remove base from this phone	Forgets this phone's credential and alert subscription. The base and its records are untouched.
Revoke a phone / replace owner phone	Removes one credential; see section 6.4.
Transfer to another person	Removes all phones and, by default, the previous owner's records; see section 6.4.
Controller pairing button	Holding BOOT reopens controller pairing and keeps its settings. Never hold RESET for this.
Factory reset entire base	A service operation for decommissioning or re-enrollment. Back up records first and use the supported service procedure; an Android factory reset also removes applications, local credentials and MDM enrollment.

9.1 Preparing a base for service

- Before service or decommissioning, identify every enclosure attached to the base and make a current backup of its records and configuration.
- An authorized service operation makes connected outputs safe before removing the credentials used to control them. The enclosure and its animals must be accounted for before power or control hardware is changed.
- Phone access, controller pairing and Android management enrollment are separate parts of the system. The service procedure addresses each one according to whether the base is being repaired, replaced or transferred.
- A reset inside Terrarium Logic and an Android factory reset have different effects. Use the operation intended for the task so records and configuration are preserved when they are needed.
- After replacement or re-enrollment, the installer restores the required records and settings, confirms authorized owner access, and verifies enclosure operation before returning the base to use.

10 Dedicated base management

A Terrarium Logic base is a purpose-configured appliance. Mobile device management, or MDM, keeps the Android tablet focused on Terrarium Logic, applies its operating settings and gives an authorized administrator a way to manage it remotely. Terrarium Logic uses MDMesh for the managed Android base; it is separate from the enclosure-control service and from the owner app on a personal phone.

10.1 What MDM manages

MDMesh manages the base tablet: its dedicated launcher, installed applications, kiosk access and supported Android restrictions. The Terrarium Logic backend manages enclosure settings, animal records, cameras and controller communication. The cloud monitoring service provides remote alerts. Keeping these roles separate lets the enclosure controller continue its local control logic independently of the management dashboard.

The owner app on an iPhone or a personal Android phone does not need to become a managed device to monitor or control a paired Terrarium Logic base. MDM enrollment applies to the dedicated base tablet.

10.2 A screen dedicated to Terrarium Logic

Kiosk mode restricts the base to an administrator-approved application list. For the dedicated Terrarium Logic profile, Terrarium Logic is the only customer application shown. Background components such as Termux remain installed to run the base services without becoming choices in the customer launcher.

The managed profile hides Home and Recent Apps access and blocks the notification shade and Quick Settings, so casual swipes do not expose the usual Android controls. The base can show Terrarium Logic or a restricted launcher from which Terrarium Logic can be selected. Leaving the managed launcher requires the administrator exit PIN or an authorized remote management action.

Kiosk control and notification delivery are separate. Hiding the notification shade does not revoke the Terrarium Logic notification permission. Terrarium Logic alerts, reminder settings, Android notification channels and sound settings determine which alerts are delivered and heard.

10.3 Provisioning a dedicated base

A managed base is provisioned before it is handed to an owner. Android device-owner enrollment starts from initial device setup: the installer connects the tablet to a network and scans the prepared enrollment QR code. The management agent registers the tablet and applies its assigned profile. The Terrarium Logic application and its supporting services are then installed and the enclosure is paired.

Existing bases are backed up before any Android factory reset or change of management agent. Restoring a base includes animal and care records, settings, the enclosure registry and the service environment. Phone access is restored through the

supported owner authorization process rather than assuming an old Android Keystore can be copied to a reset tablet.

The enrollment QR code, administrator credentials and kiosk exit PIN are service credentials. They are kept separately from this product guide and from the enclosure invitation codes shared with an owner.

10.4 Network and background services

The dedicated profile retains Wi-Fi and Bluetooth for base connectivity and controller setup. Access to Android network controls is restricted through the managed screen. Where a supported policy is available, an administrator can apply additional operating-system restrictions. The underlying radios remain available to Terrarium Logic and its services.

On a Wi-Fi-only base, cellular service can be disabled while Wi-Fi and Bluetooth remain enabled. Background execution and battery exemptions are configured for Termux, Terrarium Logic and the management agent. Boot scripts and watchdogs start and recover the backend and maintenance connection.

MDM configuration already applied on the tablet is local device policy. Contact with the management server is needed to receive new policy changes and remote commands. It is not part of the thermostat decision loop. Remote owner access and cloud alerts separately require their network services to be reachable.

10.5 Application and USB control

The administrator assigns the applications needed by the base and removes or disables optional personal-device applications. Android components required for connectivity, Bluetooth, installation and system operation are retained. Applications used by Terrarium Logic features, such as a camera application for taking care-log photos, are kept as needed.

The base profile blocks USB file transfer and mounting of external storage. This reduces direct access through the USB port; it is distinct from service access such as authorized USB debugging. Debugging permissions and trusted maintenance keys are controlled separately during provisioning and service.

10.6 Encryption and physical access

Android provides encryption for the tablet storage. MDM applies supported device policy and does not replace Android encryption, the operating-system secure storage or Terrarium Logic authentication. The enclosure controller, base and paired owner phones continue to use their own credentials for their respective connections.

A locked bootloader and Android verified boot help protect the installed operating system. Physical servicing, bootloader changes and device resets belong to the authorized service process. Kiosk mode controls normal use of the managed screen; it is one part of the base security design.

10.7 Updates and authorized support

Authorized administrators use the management dashboard to view enrolled bases, assign configuration and distribute approved Android application packages. The base reaches the management server through its own encrypted connection, including an outbound Cloudflare tunnel for the hosted management service. Owners do not need to open inbound router ports.

Android package signing identifies the application publisher and controls which packages can update an installed app. The management agent must retain a compatible signing identity across updates. A change of management agent or signing identity is handled as a planned service operation with backup and re-enrollment, rather than as a routine Terrarium Logic application update.

Base-service updates, Android application updates and ESP32 controller firmware are separate operations. Section 4 describes the base and controller update processes; MDM supplies the Android application-management layer.

10.8 Information for support

Config > Debug Info groups information by base hardware and network, ESP32 hardware and network, and application variables. The base LAN address is separate from the controller address. Controller friendly names help identify the correct enclosure when several ESP32 units are connected.

For a support request, provide the base name, enclosure friendly name, app version and a description of what happened. Debug Info can supply the relevant device and connection details. Keep passwords, enrollment codes and administrator PINs private. Hardware measurements are displayed only when the device supplies them; support does not need a guessed value.

Keep a current exported care-data backup and use the supported backup procedure before replacement or re-enrollment. Authorized service backups also preserve the application environment and private base configuration needed to restore operation. Management-server backups are separate from animal and enclosure backups.

Appendix: glossary

Term	Meaning
Base unit / base	The Android tablet that runs the Terrarium Logic backend for one or more enclosures.
Controller	The ESP32-S3 board in an enclosure that reads the sensors and switches the outlets.
Matter	An open smart-home standard; the outlets the controller switches speak it.
On-with-timed-off	A Matter command that switches an outlet on for a fixed time, after which it turns itself off unless renewed.
Termux	An Android app that provides a Linux environment; the backend runs inside it.
Tunnel	An encrypted outbound connection from the base to Cloudflare that carries remote app traffic.
Watchdog Worker	The Cloudflare Worker that monitors bases, sends push alerts and mints tunnels.
CA / certificate	A certificate authority vouches for a server's identity; the certificate is that signed statement.
CSR	Certificate signing request: the public half of a key, sent to be signed.
HMAC	A signature made with a shared secret key, proving a message is genuine and unaltered.
AES-GCM	A standard cipher that both encrypts data and detects tampering.
Owner / Restricted	The two phone roles; see section 6.1.
MDM	Mobile device management: administration of the dedicated base tablet and its Android policy.
Device owner	The Android management role used by the enrolled MDM agent; separate from the Terrarium Logic Owner role.
Kiosk	A managed screen that limits the device to approved applications and administrator-controlled exit.