



AETOS
TECHLABS

GATE ACCESS · MDM
VISITOR & DEVICE CONTROL



AETOS ONE · GATE ACCESS

The phone follows the badge. Enter to exit.

Badge-issued, profile-based restrictions on every phone that walks through your gate — camera, calls, hotspot, USB, apps — armed the moment the card taps the turnstile, and released only when security scans it back in. Not by GPS. Not by walking out.



Badge-driven

The card tap arms it, the card return releases it. GPS and Wi-Fi are back-up layers, never the trigger.

Human approval

Nothing is enforced and no card exists until the officer checks physical ID and confirms the host.

Honest per OS

Android enforces everything. iOS enforces most. The brochure says which — so does the demo.



Eleven steps.

Not one of them is automatic trust.

From the QR poster on the turnstile to full access restored at the exit desk
— each step as it happens in the working demo.

01

Scan QR

A QR poster on the turnstile is the only entry point. It opens the store listing for the gate app — no manual search, no wrong app.

02

Install the app

The app is the policy agent. On company Android it enrolls as Device Owner; on iOS it installs the supervised profile. Permissions declared up front.

03

Sign up

Name, ID, employer, host and purpose. The requested profile decides which restriction set will be armed later.

04

Request sent

Nothing is enforced yet and no card exists. The visitor waits at the desk while the officer works the queue.

05

Security review

The officer checks submitted details against physical ID and confirms the host. Approval is a human decision, not an automatic one.

06

Card issued

A physical card is bound to this person and device. The badge ID is the key that links the turnstile to the device policy.

07

Tap gate

The badge event fires a webhook; the device is added to the restricted group for its profile. Gate opens, policy arms.

08

Inside

Blocked apps grey out and launches are refused. Policy is cached on-device, so it holds even without signal inside the building.

09

Hand back

Exit is card-driven, not GPS-driven. Restrictions do not lift by walking out — the officer must scan the card back in.

10

Full access

Device removed from the restricted group, every restriction lifted, the app's runtime permissions revoked until next visit.

11

Next visit

Profile already verified and stored. Identity confirmed, card re-issued in seconds; the same policy re-arms on tap.



Audit log

Every request, approval, tap, policy push and release is timestamped against the officer and the badge — retained a year.

PROFILE

Employee

Camera, gallery, screenshots, USB, hotspot and app store blocked. Calls, microphone, Bluetooth and personal apps allowed. Corporate Wi-Fi only.

PROFILE

Contractor

Everything the employee loses, plus calls, messages, mail, microphone and Bluetooth blocked. Guest Wi-Fi. Four-app kiosk.

PROFILE

Public visitor

Single-app kiosk. Emergency calls only. Portal Wi-Fi. No call-log capture — the least data the site needs to hold.

WHAT IS CONTROLLED



Aetos One

Fourteen features, three profiles, and what each OS can actually enforce.

The right-hand columns are the honest part. A brochure that promises dialer blocking on iPhone is selling something Apple does not allow.

FEATURE	EMPLOYEE	CONTRACTOR	VISITOR	ANDROID	IOS
Rear & front camera	Blocked	Blocked	Blocked	Yes	Yes
Gallery / photos	Blocked	Blocked	Blocked	Yes	Hidden
Voice calls (dialer)	Allowed	Blocked	Emergency	Yes	No
Video calls	Blocked	Blocked	Blocked	Yes	Yes
Screenshot & recording	Blocked	Blocked	Blocked	Yes	Yes
Wi-Fi network	Corp only	Guest	Portal	Yes	Yes
Mobile hotspot	Blocked	Blocked	Blocked	Yes	Partial
Bluetooth	Allowed	Blocked	Blocked	Yes	Partial
USB file transfer	Blocked	Blocked	Blocked	Yes	Yes
Microphone	Allowed	Blocked	Blocked	Yes	No
App install / store	Blocked	Blocked	Blocked	Yes	Yes
Personal apps	Allowed	Kiosk 4	Kiosk 1	Yes	Yes
Location shared	On-site	On-site	On-site	Yes	App-level
Call-log capture	Metadata	Metadata	None	Yes	No

Android — full enforcement DEVICE OWNER

- + Every feature in the table is enforceable, including dialer blocking, microphone and call-log metadata.
- + Policy cached on device — holds through dead zones inside the building; the badge-out is what releases it.
- + Enforcement lands in 10–30 s. Geofencing can back up the badge trigger as a second layer.

iOS — supervised limits ABM + DEP

- + Camera, FaceTime, screenshots, USB, app install and Single App Mode are all enforceable on supervised devices.
- Apple exposes no API to block the dialer, read call logs or reach the camera roll. Those rows stay off for iPhone.
- ! No GPS or Wi-Fi trigger exists on iOS — the badge-swipe webhook is the only way to switch policy on entry and exit.



Room-level location, and alarms that fire on time.

Optional on top of the badge layer. Beacons tell you the room; rules turn "nothing happened by 09:30" into a message to the right owner.

RECOMMENDED

BLE beacons

Accuracy	1–3 m (room)
Indoor / outdoor	Yes / No
Phone battery	Low (~2 %/day)
Hardware	1 per 8–10 m

Room-level indoor path. Beacons are passive; the app ranges them and reports zone changes. Best cost-to-accuracy for an office or plant floor.

GPS path tracking

Accuracy	5–15 m
Indoor / outdoor	Unreliable / Yes
Phone battery	High (8–15 %/day)
Hardware	None

Campus geofence, vehicle and field-staff routes, off-route deviation. Useless for telling one room from the next.

Wi-Fi AP triangulation

Accuracy	3–8 m
Indoor / outdoor	Yes / No
Phone battery	Medium
Hardware	Existing APs

No new hardware if AP density is already high. Drifts as APs move or channels change — a fallback layer, not the primary.

Late arrival

No badge-in and no beacon by 09:30 on a workday → **manager** by email + SMS; attendance row flagged. Grace 15 min.

Early departure

Badge-out or last beacon before 17:00 with no approved leave → **security desk**; exception logged.

Overtime

Still ranged by any beacon after 20:00 → **manager** notified, taxi voucher offered, restriction session auto-extended.

Restricted-zone entry

Server room or lab beacon ranged outside 08:00–19:00 → **immediate security alert** + CCTV clip for that door, ±2 min.

No-movement

Lone worker in a hazard zone, no zone transition for 30 min → **safety team**; call the device; dispatch a floor marshal. Escalates in 2 min.

Off-route

Delivery driver deviates > 500 m from the planned GPS route → **dispatcher** with live map link and last heading.

UNDER THE HOOD

Rules are data, not code.

Add a rule as a row: trigger, window, zone, grace, severity, owner, channel.

Zone events every 5–10 s

Dwell derived server-side — a killed app can't fake it

Evaluator ticks every 60 s

Email · SMS · webhook per owner

Unacknowledged → next tier

Evidence kept one year



AETOS
TECHLABS

Watch the demo. Tap a card, watch a phone lock.

A working demo exists — visitor profile, device OS, security console and audit log. Thirty minutes shows the whole journey.



CALL

+91 99666 12678
+91 90309 03030



WEB

aetostechlabs.com



EMAIL

krishna@aetostechlabs.com
aetostechlabs@yahoo.com



OFFICE

Aetos Techlabs LLP
Hyderabad, Telangana