Tài liệu kết nối Hotel Admin với hệ thống TravelQ

Dành cho đội kỹ thuật Holitech · Phiên bản tài liệu 01/11/2026 · Gói nguồn: bản 8b4226bb

Công ty Cổ phần Hạ tầng Du lịch số Việt Nam (VDTI) · MST 4101683286

Tài liệu này tương thích với bản TravelQ ID đã gửi Holitech: cùng định dạng mã, cùng đường dẫn `/api/v1/partner/...`, cùng scope khoá. Không có giá trị bí mật nào trong tài liệu và trong gói.

1. Kiến trúc

Thành phần	Vai trò
Trình duyệt (Hotel Admin)	web tĩnh trong `site/`; không chứa khoá API; chỉ gọi `/api/tqid/*` cùng tên miền
Máy chủ Hotel Admin (Node 18+)	`server/server.mjs` phục vụ web tĩnh và proxy `/api/tqid/*`; giữ khoá TravelQ ID trong file env
nginx HTTPS	đứng trước máy chủ Node; mẫu cấu hình trong `deploy/nginx/`
Dịch vụ TravelQ ID	xác minh mã, hồ sơ có đồng ý, giao dịch nhận phòng, so khớp giấy tờ, so khớp khuôn mặt
App TravelQ cho khách	đặt phòng, thanh toán qua cổng Vietcombank, (dự kiến) order trong phòng
Hệ thống TravelQ trung tâm	nhập giá, duyệt quỹ hoà vốn, khớp giao dịch Vietcombank, đẩy kết quả sang Hotel Admin

Luồng chính: trình duyệt → nginx → Node (kiểm tra phiên, Origin, mã khách sạn) → TravelQ ID. Khoá chỉ đi ở chặng Node → TravelQ ID.

2. Triển khai trên máy chủ Holitech

- Holitech tự vận hành trên máy chủ riêng, không dùng đám mây. Hai cách: **Node + systemd** (khuyên dùng) hoặc **Docker Compose**. Chi tiết từng lệnh trong `docs/HUONG-DAN-TRIEN-KHAI-HOTEL-ADMIN-HOLITECH.md`.
- Chạy thử: `bash tools/verify.sh` → `PORT=3100 node server/server.mjs` → `BASE=http://127.0.0.1:3100 bash tools/smoke-test.sh`.
- Chưa đặt khoá TravelQ ID thì proxy tự chạy **chế độ mô phỏng** (`server/tqid-mock.mjs`), dùng để thử giao diện.
- Bản tham chiếu trên Cloudflare Pages dùng `cloudflare-pages/functions/api/tqid/[[path]].js` với cùng lõi proxy trong `cloudflare-pages/lib/`; Holitech không bắt buộc dùng.
- Mỗi khách sạn một bản (hoặc nhiều khách sạn trên một máy chủ qua `HOTELS`), dữ liệu tách theo mã khách sạn.

3. Bản đồ thư mục gói

Đường dẫn	Nội dung
`site/`	web Hotel Admin bản 8b4226bb (index.html, các file JS, CSS, assets, `data/data.js` dữ liệu mẫu)
`server/server.mjs`	máy chủ web tĩnh, Basic auth tuỳ chọn, access log, gắn proxy
`server/tqid-route.mjs`, `tqid-proxy.mjs`	định tuyến và xử lý `/api/tqid/*`
`server/tqid-format.mjs`	kiểm tra định dạng TravelQ ID và ký tự kiểm tra
`server/tqid-mock.mjs`	dữ liệu mô phỏng khi chưa có khoá

Đường dẫn	Nội dung
`cloudflare-pages/functions/`, `cloudflare-pages/lib/`	bản Cloudflare Pages Function tham chiếu
`deploy/nginx/`, `deploy/systemd/`	mẫu nginx và dịch vụ systemd
`Dockerfile`, `docker-compose.yml`	chạy bằng Docker
`tools/`	`verify.sh` (SHA256), `smoke-test.sh`, `gen-secrets.sh`, `backup.sh`
`.env.example`	danh sách biến, chỉ tên, không giá trị
`docs/`	hướng dẫn triển khai, 2 tài liệu PDF này và bản markdown nguồn
`src_draft/`	mã mức B (`rooms.js`, `inroom.js`) để tham khảo, **chưa nạp** vào `site/`

4. Biến môi trường (chỉ tên)

Biến	Ý nghĩa
`HOST`, `PORT`, `SITE_DIR`, `TRUST_PROXY`, `ACCESS_LOG`	cấu hình máy chủ Node
`HOTEL_ADMIN_BASIC_USER`, `HOTEL_ADMIN_BASIC_PASSWORD_SHA256`	đăng nhập HTTP Basic trước toàn trang (tuỳ chọn)
`HOTEL_ID`, `HOTEL_NAME`, `HOTELS`	mã và tên khách sạn; nhiều khách sạn dạng `MÃ|Tên;MÃ|Tên`
`TRAVELQ_ID_API_KEY`, `TRAVELQ_ID_API_KEY__<MÃ>`	khoá TravelQ ID cho khách sạn mặc định và cho từng khách sạn (dấu `-` đổi thành `_`)
`TRAVELQ_ID_SITE`, `TRAVELQ_ID_SITE__<MÃ>`	mã site để lọc giao dịch theo khách sạn
`TRAVELQ_ID_BASE_URL`	gốc dịch vụ TravelQ ID, https, không kèm `/api/v1`
`TRAVELQ_ID_APP_URL`	trang để khách cấp quyền (mặc định bằng gốc dịch vụ)
`HOTEL_SESSION_SECRET`	chuỗi ngẫu nhiên tối thiểu 32 ký tự để ký phiên
`HOTEL_STAFF_ACCOUNTS`	`MÃ KS|MÃ NV|Họ tên|sha256 PIN`, cách nhau bằng `;`

File `.env` đặt quyền 600, không commit, không gửi qua chat. Mật khẩu và chuỗi bí mật sinh bằng `tools/gen-secrets.sh` ngay trên máy chủ.

5. Proxy `/api/tqid/*`

5.1 Đường dẫn

Yêu cầu từ trình duyệt	Chuyển tới TravelQ ID	Mục đích
`GET /api/tqid/status?hotel=`	(nội bộ)	chế độ live hoặc mô phỏng; danh sách nhân viên của đúng khách sạn
`POST /api/tqid/session`	(nội bộ)	lễ tân đăng nhập mã NV và PIN, nhận phiên ký HMAC mang `hid`
`GET /api/tqid/verify/{tqid}`	`GET /api/v1/partner/ids/{tqid}/verify`	kiểm tra mã hợp lệ
`GET /api/tqid/profile/{tqid}`	`GET /api/v1/partner/ids/{tqid}`	hồ sơ khách, chỉ khi khách đã cấp quyền

Yêu cầu từ trình duyệt	Chuyển tới TravelQ ID	Mục đích
`GET /api/tqid/transactions/{tqid}`	`GET /api/v1/partner/ids/{tqid}/transactions`	giao dịch, lọc chỉ tại khách sạn của phiên
`POST /api/tqid/transactions/{tqid}`	`POST /api/v1/partner/ids/{tqid}/transactions`	ghi giao dịch nhận hoặc trả phòng theo mã booking
`POST /api/tqid/document-match/{sub}`	`POST /api/v1/partner/users/{sub}/document/match`	đối chiếu giấy tờ (`sub` dạng `u_…`)
`POST /api/tqid/face-verify`	`POST /api/v1/checkin/face-verify`	so khớp selfie (JPEG data URL, tối đa khoảng 1 MB), không lưu ảnh

Định dạng TravelQ ID: `TQ` + 9 chữ số, chữ số cuối là ký tự kiểm tra Luhn; vẫn nhận dạng cũ `TQ-YYYY-XXXXXXXC`. Tiền tố `TQID:` trong mã QR được bỏ qua.

5.2 Phiên và phạm vi khách sạn

- Mọi yêu cầu (trừ `status`, `session`) cần phiên lễ tân. Phạm vi khách sạn lấy từ `hid` trong phiên do máy chủ ký.
- Header `x-hotel-id` khác `hid` → `403 hotel_mismatch`. Sửa `hid` trong token → chữ ký sai → `401`.
- Khách sạn chưa có khoá riêng → `503 not_configured`, không dùng khoá khách sạn khác.

5.3 Quy tắc Origin và bảo mật

- Proxy không chuyển tiếp `Origin` của trình duyệt; từ chối Origin khác trang Hotel Admin (`403 origin_not_allowed`).
- Quản trị TravelQ ID phải đăng ký Origin của tên miền Hotel Admin mà Holitech dùng.
- Khoá không trả về trình duyệt, không ghi log. Không lưu và không ghi log ảnh selfie hay nội dung yêu cầu.
- Giới hạn tần suất theo IP, theo phiên và theo lượt so khớp khuôn mặt.

5.4 Mã lỗi

HTTP	code	Ý nghĩa
400	`invalid_tqid`, `invalid_sub`	sai định dạng mã
401	`invalid_login`, `staff_session_required`	sai PIN hoặc hết phiên
403	`origin_not_allowed`, `hotel_mismatch`	gọi từ trang khác hoặc phiên thuộc khách sạn khác
theo TravelQ ID	`consent_required` (chuyển tiếp)	khách chưa cấp quyền xem hồ sơ
404	`not_found`, `hotel_not_found`	không tìm thấy mã hoặc mã khách sạn
409	so khớp khuôn mặt	cần đối chiếu giấy tờ trước
413, 422	`payload_too_large`, `validation`	ảnh quá lớn, thiếu hoặc sai dữ liệu
423, 429	tạm khoá, `rate_limited`	khoá so khớp tạm thời, quá nhiều yêu cầu
503	`not_configured`	thiếu biến môi trường hoặc khách sạn chưa có khoá

6. Thanh toán Vietcombank và đối soát

- Khách thanh toán trong app TravelQ; nội dung chuyển khoản chứa mã booking `TQH-YYMMDD-NNNN`; phòng hoà vốn giữ chỗ 30 phút, không hoàn tiền.
- TravelQ nhận giao dịch từ Vietcombank theo kênh đã thống nhất trong hợp đồng (ngoài phạm vi Hotel Admin), khớp với booking và đẩy kết quả sang Hotel Admin. Hotel Admin chỉ đọc.
- Trường đề xuất (nội bộ TravelQ, không phải đặc tả Vietcombank): `txn_ref`, `received_at`, `amount`, `memo`, `booking_ref`, `due`, `result` (`matched`, `short`, `over`, `unmatched`, `after_expiry`), `channel` (`hv`, `ta`).
- Điểm nối **dự kiến**: `GET /api/hotel/payments?from=&to=` và webhook `POST /api/hotel/payments/sync` (TravelQ ký HMAC), lọc theo `hid`. Đối soát cuối tháng `GET /api/hotel/reconciliation/{YYYY-MM}`, xác nhận `POST .../confirm` bởi chủ khách sạn.

7. Mô hình dữ liệu (đề xuất cho API thật)

Đối tượng	Trường chính
`hotel`	`hid`, `name`, `features[]` (chức năng đang bật), giờ nhận 14:00, giờ trả 12:00
`room_type`	`code`, `name`, `total`, `price_hv`, `price_ta_net`, `price_sell` (chỉ đọc, TravelQ nhập)
`room`	`no` (ví dụ 102), `type`, `view`, `status` (`sach`, `ban`, `dang_o`)
`allotment`	`date`, `room_type`, `hv_quota` (TravelQ duyệt), `hv_sold`, `hv_locked`, `ta_open` (khách sạn đặt; 0 là ngừng TA), `ta_sold`, nhật ký thay đổi
`booking`	`ref` `TQH-YYMMDD-NNNN`, `channel` (`hv`, `ta`), `room_type`, `checkin`, `checkout`, `guests`, `pay_status`, `room_no` (dự kiến)
`guest`	`tqid` hoặc khối ghi tay: `cccd` (nếu có), `personal_id` của bé, `full_name`, `address`, `is_child`; danh sách và phiếu chỉ in `tqid`
`checkin`	`booking_ref`, `method` (`qr`, `face`, `manual`, `kiosk`), `staff`, `at`, `guests[]`, `early`, `extend_hours` (1–6), `receipt` (A4 ký hoặc biên nhận điện tử)
`reconciliation`	`month`, tổng hoà vốn, tổng TA net, hoa hồng, trạng thái xác nhận
`inroom_order` (dự kiến)	`id`, `room_no`, `booking_ref`, `items[]`, `dept` (`nha-hang`, `buong-phong`, `spa`, `ky-thuat`), `status`, `pay_status`, `open_from`, `lock_at`

8. Điểm nối dự kiến cho mức C

Tất cả lọc theo `hid` của phiên; tên đường dẫn là đề xuất, Holitech có thể đổi cho phù hợp backend.

Đường dẫn (dự kiến)	Mục đích
`GET /api/hotel/rooms`, `PATCH /api/hotel/rooms/{no}`	danh sách phòng và trạng thái sạch bẩn
`GET/PUT /api/hotel/allotments?date=`	quỹ hoà vốn (đọc, khoá, mở) và số TA theo ngày
`POST /api/hotel/bookings/{ref}/assign`	gán số phòng trước cho booking
`GET /api/hotel/bookings/by-tqid/{tqid}`	khách quét ID hoặc khuôn mặt thì hiện phòng đã gán
`POST /api/hotel/checkins`	ghi nhận phòng; chặn trước 14:00 trừ khi quản lý cho nhận sớm
`POST /api/hotel/stays/{ref}/extend`	gia hạn 1–6 giờ; quá hạn tính 1 đêm qua app TravelQ
`POST /api/hotel/keycards/encode`	ghi thẻ từ qua SDK khoá cửa của khách sạn (chưa chọn hãng)
`GET/PUT /api/hotel/features`	bật tắt chức năng theo khách sạn

Đường dẫn (dự kiến)	Mục đích
`GET /api/app/inroom/{room_no}/menu`, `POST /api/app/inroom/orders`	phía app TravelQ: chỉ mở khi khách đang ở đúng phòng, tự khoá ở `lock_at`
`GET/PATCH /api/hotel/orders`	lễ tân điều phối, bộ phận cập nhật trạng thái
Quản trị TravelQ nhiều cấp	app riêng: cả nước, tỉnh, trưởng phòng, nhân viên nhập liệu, nhân viên sales; chưa thiết kế API

9. Danh sách kiểm thử

1. `bash tools/verify.sh` khớp `SHA256SUMS`.
2. `smoke-test.sh`: trang chủ 200, `/api/tqid/status` trả chế độ mô phỏng khi chưa có khoá.
3. Đăng nhập lễ tân đúng PIN được, sai PIN `401`; nhân viên khách sạn A không vào được khách sạn B.
4. Gửi `x-hotel-id` khác phiên → `403 hotel_mismatch`; Origin lạ → `403 origin_not_allowed`.
5. Mã sai ký tự kiểm tra → `400 invalid_tqid`.
6. Với khoá thử nghiệm: verify, profile (trước và sau khi khách cấp quyền), transactions GET và POST, document-match, face-verify.
7. Kiểm tra log máy chủ và nginx không chứa khoá, ảnh, nội dung yêu cầu.
8. Giao diện: Quỹ phòng (khoá HV, đặt TA 0), nhận phòng đoàn (+ từng khách, quét mã, ghi tay), phiếu A4 chỉ in TravelQ ID, xuất khai báo lưu trú.
9. Thu hồi khoá: thu hồi trên TravelQ ID, xoá khỏi env, khởi động lại dịch vụ.

10. Vòng 3 · API mới (03/11/2026)

Các API dùng chung một lõi cho Cloudflare Pages Functions (`functions/api/hotel`, `functions/api/he-thong`) và máy chủ Node của Holitech (`server/tqid-route.mjs`). Mã nguồn nằm ở `server/hotel-ops.mjs`, `server/hotel-seed.mjs` và `server/he-thong.mjs`. Máy chủ giữ dữ liệu giả lập trong bộ nhớ, khi nối cơ sở dữ liệu thật thì thay lớp lưu trữ.

10.1 /api/hotel (phiên lễ tân, header `x-staff-session`)

Đường dẫn	Việc làm
`GET rooms`, `PUT rooms/:so/clean`	Lấy danh sách phòng và cập nhật tình trạng dọn phòng
`GET bookings`, `GET assignments`, `PUT assignments/:booking`	Lấy booking và gán phòng trước cho từng booking
`GET` và `PUT settings/times`	Đọc và đổi giờ nhận, trả phòng. Chỉ quản lý được đổi.
`POST early-checkin/:booking`	Quản lý cho nhận phòng sớm khi phòng đã sạch
`POST kiosk/lookup`, `POST checkin/:booking`	Tìm booking bằng khuôn mặt hoặc TravelQ ID rồi nhận phòng. Máy chủ trả mã lưu trú có hạn 48 giờ.
`POST extend/:booking`	Gia hạn từ 1 đến 6 giờ, quá 6 giờ thì tính 1 đêm
`POST checkout/:booking`	Trả phòng, đánh dấu phòng cần dọn và khoá màn order của khách
`POST keycard/:booking`	Ghi thẻ từ trắng cho phòng đã nhận
`GET orders`, `POST orders/:id/dispatch`, `advance`, `cancel`	Lấy order gộp, giao bộ phận, chuyển bước và huỷ order
`GET` và `PUT features`	Đọc và bật, tắt chức năng của từng khách sạn. Chỉ quản lý được đổi.
`POST guest/orders`	Đã bỏ. App khách gửi order qua `/api/app/inroom/orders` (mục 11).

10.2 /api/he-thong (phiên quản trị, header `x-admin-session`)

Đường dẫn	Việc làm
`POST session`, `GET me`	Đăng nhập bằng mã tài khoản và PIN, phiên có hạn 12 giờ. Sai 8 lần thì khoá 10 phút.
`GET stats`, `GET hotels`, `GET hotels/:id`	Lấy số liệu và khách sạn trong phạm vi vai trò
`PUT hotels/:id/status`	Bật hoặc tạm dừng bán phòng. Chỉ quản trị cả nước và cấp tỉnh được làm.
`POST hotels/:id/proposals`	Gửi đề xuất sửa hồ sơ. Trường giá hoặc phí bị từ chối với mã `price_not_here`.
`GET changes`, `POST changes/:id/approve`, `reject`	Lấy danh sách đề xuất, duyệt hoặc từ chối
`GET staff`, `POST leads`	Xem nhân sự trong phạm vi. Nhân viên kinh doanh thêm khách sạn đang tiếp cận.

10.3 Biến môi trường mới (chỉ tên)

Biến	Ý nghĩa
`HETHONG_ACCOUNTS`	Tài khoản quản trị hệ thống dạng `MÃ|sha256 của PIN;…`. Có thể thêm `|vai trò|phạm vi|họ tên`.
`HOTEL_SESSION_SECRET`	Dùng chung để ký phiên lễ tân, mã lưu trú và phiên quản trị. Chuỗi ngẫu nhiên dài từ 32 ký tự.

11. /api/app · kiosk sảnh và order trong phòng (03/11/2026)

Lõi chung `lib/app-guest.mjs` (Cloudflare Pages: `functions/api/app/[[path]].js`; máy chủ Node: `server/app-guest.mjs` qua `server.mjs`). Đường dẫn này không nhận phiên lễ tân và không gọi hệ thống nhà hàng bên ngoài.

11.1 /api/app/kiosk (header `x-kiosk-device`)

Đường dẫn	Việc làm
`POST enrol`	Chỉ bản xem trước (`HOTEL_PREVIEW_GUEST=1`): kích hoạt nhanh máy kiosk 12 giờ. Bản chính thức trả 403 `enrol_disabled`.
`GET info`	Tên khách sạn, giờ nhận, trả phòng
`POST lookup`, `POST face`	Tìm booking bằng TravelQ ID hoặc khuôn mặt. Trả phòng đã gán, TravelQ ID che bớt.
`POST checkin`, `POST keycard`	Nhận phòng (từ 14:00 hoặc khi quản lý cho phép nhận sớm), ghi thẻ trắng. Trả link order kèm mã lưu trú.
`POST call`	Gọi lễ tân hỗ trợ

Mã thiết bị kiosk ký bằng `HOTEL_SESSION_SECRET`, kiểu `kiosk`, gắn mã khách sạn và mã máy. Quản lý cấp mã qua `POST /api/hotel/kiosk-devices` (phiên lễ tân). Thu hồi bằng biến `HOTEL_KIOSK_REVOKED`. File tĩnh không chứa khoá API.

11.2 /api/app/inroom (header `x-stay-token`)

Đường dẫn	Việc làm
`POST demo-stay`	Chỉ bản xem trước: mở màn order của khách đang ở phòng 103
`GET session`, `GET menu`	Phòng, hạn lưu trú và menu theo chức năng khách sạn đang bật
`GET orders`, `POST orders`, `POST orders/:id/cancel`	Order của phòng này. Order mới vào hàng chờ `/api/hotel/orders`, mã từ OD-1101. Khách hỏi lại mỗi 5 giây để thấy trạng thái.

Mã lưu trú gắn với booking và phòng. Sau trả phòng (kể cả khi đã gia hạn) mọi lệnh trả 401/403 và màn order tự khoá.

11.3 Lưu ý triển khai

- Biến chỉ dùng cho bản xem trước, phải tắt trên bản chính thức: `HOTEL_PREVIEW_GUEST`, `HOTEL_STATE_DAILY`, `HOTEL_DEMO_CLOCK`, `HOTEL_DEMO_NOW`.
- Dữ liệu vận hành lưu trong D1 `HOTEL_STATE`. Bản xem trước dùng D1 riêng `travelq-hotel-admin-xam-state`.
- Máy chủ gửi `X-Frame-Options: DENY`. App TravelQ mở màn order bằng webview, không nhúng iframe.
- Kiosk tra cứu bằng TravelQ ID là điểm yếu: ai biết mã TravelQ ID có thể thấy số phòng. Nên bắt buộc khuôn mặt hoặc thêm mã xác nhận khi lên bản chính thức.
- Rủi ro cấu hình: D1 `DB` trỏ vào `benhvienso-live` ở cả hai môi trường. Bản xem trước đã bỏ ràng buộc này. Bản chính thức nên được rà lại trước lần triển khai sau.