

## QUICK 2 OODOO ONLINE BASIC FEATURES

**Feature List & configuration map (an enterprise production-polish build)**

### **1) Branding, domains, and TLS**

- **Brand:** Quick2Odoo Online (Q2O)
- **Primary domains:** app.quick2odoo.online (web), api.quick2odoo.online (API)
- **Cloud-managed TLS:** Azure Front Door / Ingress controller
- **Configure**
  - **DNS:** CNAME app. and api. to Front Door/ingress public host
  - **Helm values:** k8s/helm/q2o/values.yaml → ingress.hosts[\*].host, env.NEXT\_PUBLIC\_API\_URL, env.NEXTAUTH\_URL
  - **Terraform:** Front Door managed certs (already in prior infra; ensure hostnames bound)

### **2) Authentication & SSO**

- **API** expects **NextAuth JWT** (HS256 or RS256 via JWKS)  
File: api/app/auth.py
- **Web** now includes **NextAuth** route and providers (Okta, Entra/Azure AD, Google)  
Files: web/pages/api/auth/[...nextauth].ts, web/package.json includes next-auth
- **Configure**
  - **Web env:** NEXTAUTH\_SECRET, provider creds (GOOGLE\_ID/SECRET, OKTA\_ID/SECRET/ISSUER, AZURE\_AD\_ID/SECRET/TENANT)
  - **API env:** NEXTAUTH\_JWT\_ALG=HS256 (or RS256 with NEXTAUTH\_JWKS\_URL), NEXTAUTH\_SECRET
  - **CORS:** set Q2O\_ALLOWED\_ORIGINS to web origin in Helm values

### **3) Tenancy & billing (Stripe)**

- **Tiers:** Freebie (2 yrs), Starter (3), Half (5), Full (10)
- **Stripe webhook** updates tenant plan in DB  
File: api/app/billing.py

- **Configure**
  - **Secrets:** STRIPE\_SECRET, STRIPE\_WEBHOOK\_SECRET
  - **Plan map:** STRIPE\_PLAN\_MAP (JSON mapping Price IDs → Plan names)
  - **Success/Cancel URLs:** BILLING\_SUCCESS\_URL, BILLING\_CANCEL\_URL
  - **Postman** collection includes webhook, checkout examples

#### **4) QuickBooks Online (QBO) & Odoo v18 integrations**

- **QBO** OAuth refresh in API; **QBO client** in API & Worker  
Files: api/app/oauth\_qbo.py, api/app/clients/qbo.py, worker/qbo\_client.py
- **Odoo v18** JSON-RPC client in API & Worker  
Files: api/app/clients/odoo.py, worker/odoo\_client.py
- **Configure**
  - Save Odoo connection via **Onboarding** page or API (/connect/odoo/save)
  - **Secrets:** QBO\_CLIENT\_ID, QBO\_CLIENT\_SECRET; set tenant tokens via OAuth flow (already modeled)

#### **5) QBO Desktop (QBD) starter**

- **Web Connector** .QWC generator and ping stub  
File: api/app/qbd.py → GET /qbd/webconnector.qwc, GET /qbd/ping
- **CDC/SOAP** loop to be plugged next (placeholder preserved)
- **Configure**
  - .QWC params (company, appurl) via querystring; secure behind admin if desired

#### **6) Backfill, incremental & Temporal wiring (NEW)**

- **Temporal** workflow class **shared** for API+Worker  
File: shared/temporal\_defs/workflows/backfill.py
- **API /entities/backfill** now **starts Temporal** (and keeps Tier enforcement)  
File: api/app/entities.py (starts BackfillWorkflow.run)
- **Worker** registers activities and workflow; connects to Temporal  
File: worker/run\_worker.py

- **Activities scaffold per entity** (fetch from QBO; upsert to Odoo; **IdMap** persist; **ErrorLog** on failure)  
File: worker/temporal/activities/entities.py
- **Rate limiting** for QBO calls (token bucket + 429 retry)  
File: worker/ratelimit.py and used by worker/qbo\_client.py
- **Reconciliation strict mode**  
Env: RECONCILE\_STRICT=true|false (raises if required mapping missing)
- **Configure**
  - Temporal: TEMPORAL\_ADDRESS, TEMPORAL\_NAMESPACE, TEMPORAL\_TASK\_QUEUE
  - DB: DATABASE\_URL in both API & Worker
  - QBO limits: QBO\_RPS, QBO\_BURST
  - Recon: RECONCILE\_STRICT

## 7) Mappings & search (UI + API)

- **Rich Mapping UI** with live search (QBO + Odoo) and pair save  
File: web/pages/mappings.tsx
- **Search endpoints** for mapping UI  
File: api/app/search.py → /search/qbo, /search/odoo
- **Mappings save endpoint**  
File: api/app/mappings.py

## 8) Onboarding wizard + Theme

- **Onboarding wizard** with Test QBO, Save Odoo, Test Odoo  
File: web/pages/onboarding.tsx
- **Theme toggle** with persisted light/dark (banking look basis)  
File: web/components/ThemeToggle.tsx + Tailwind dark mode

## 9) Real-time jobs/errors (SSE)

- **Signed SSE** per-tenant; **token** endpoint and **stream** endpoint  
Files: api/app/sse\_sign.py, api/app/ops\_stream.py
- **Admin ops endpoints** for Jobs & Errors (for UI)  
File: api/app/ops\_admin.py → /ops/jobs, /ops/errors

- **UI:** web/pages/jobs.tsx, web/pages/errors.tsx subscribe to SSE
- **Configure**
  - SSE\_SIGNING\_SECRET

## 10) Observability & audit

- **App Insights + Log Analytics;** alerts on API 5xx spikes and WAF blocks  
Files: infra/terraform/azure/appinsights.tf
- **Audit logs** middleware writing to DB  
Files: api/app/audit.py, model in api/app/models.py
- **Dashboards:** foundation in place; can add Workbooks JSON next
- **Configure**
  - var.alert\_email in Terraform (default given)

## 11) Security & WAF

- **Azure Front Door WAF** with:
  - OWASP ruleset, **rate limit, bad bot block**
  - **Geo allowlist** (JM/US/CA/GB default), **path allow** for Stripe webhook
  - **IP allowlist** variable (defaults allow all)  
Files: infra/terraform/azure/waf.tf, variables.tf
- **Key Vault CSI** for secrets → K8s Secret sync  
File: k8s/helm/q2o/templates/secretpointerclass.yaml
- **Private Endpoint** template for Postgres  
File: infra/terraform/azure/private\_endpoint.tf
- **Configure**
  - Terraform vars: allowed\_countries, ip\_allowlist, Key Vault/PE inputs
  - Helm secrets via values or Key Vault CSI sync

## 12) Deployment: Helm + CI/CD

- **Helm** umbrella: API, Worker, Service, Ingress, Secrets  
Folder: k8s/helm/q2o/

- **GitHub Actions:** build → ACR → AKS → **helm upgrade**  
File: .github/workflows/api\_worker.yml
- **Dockerfiles:** both API & Worker copy **shared** workflow package
  - api/Dockerfile, worker/Dockerfile now COPY .../shared ./shared
- **Local dev:** docker-compose.yml (API + Web)

### 13) Data retention & compliance posture

- Policy (as set): **payloads 30 days, logs 90 days** — reflected in LAW & notes
- Compliance: SOC 2 / ISO 27001 track supported by WAF, KV, PE, logs, SSO hooks (auditing in place; needs policies + runbooks for full compliance)

### 14) Postman & docs

- **Postman** collection: health, connect/test, mappings, backfill, comparative, SSE, Stripe, search, QBD  
File: postman\_collection.json
  - **Docs:** docs/POLISH\_NOTES.md summary of polish items
- 

### Changes since last build (what was added or modified)

#### Added

- Temporal wiring end-to-end: shared workflow, API start, worker activities, rate limiter.
- Live comparative reports (QBO+Odoo) endpoint.
- Rich mapping UI and search endpoints (QBO/Odoo).
- Onboarding wizard and theme toggle (dark/light).
- QBO Desktop .QWC generator.
- Audit logging middleware and DB table.
- Key Vault CSI SecretProviderClass (K8s).
- Private Endpoint Terraform for Postgres.
- Ops admin endpoints for Jobs/Errors (to back Jobs/Errors UI).

- NextAuth route with Okta/Google/Entra providers (web).

### Preserved

- Branding/domain rename to **Quick2Odoo Online** and quick2odoo.online.
- Stripe-based tiering (Freebie/Starter/Half/Full) and enforcement in backfill.
- SSE with token signing and per-tenant channels.
- WAF w/ OWASP, rate limit, geo allowlist, webhook path allow.
- App Insights + alerts, Helm, CI/CD, Dockerfiles, Postman, docker-compose.

### Not removed

- Minimal placeholders (e.g., QBD SOAP/CDC) remain as stubs awaiting the next increment.
- 

### **Proceeded: Backfill → Temporal workflow wiring + activities + ID map**

I've already implemented the wiring and packaged it:

- **API starts Temporal:** api/app/entities.py now connects to Temporal and starts BackfillWorkflow.run, returning workflow\_id.
- **Shared workflow:** shared/temporal\_defs/workflows/backfill.py.
- **Worker:**
  - Activities for fetch\_qbo\_entities and upsert\_odoo\_entities in worker/temporal/activities/entities.py.
  - **IdMap** persistence and **ErrorLog** capture in worker datalayer.
  - **Rate limiter** for QBO calls; configurable via QBO\_RPS and QBO\_BURST.
  - **RECONCILE\_STRICT** guard (raise if mappings not found).
- **Dockerfiles** updated to include .../shared into images.
- **Ops admin endpoints** added for UI lists.

---

**Build file:** quick2odoo\_online\_scaffold\_ENTERPRISE\_WIRED.zip

## Final pre-launch checklist (config you should set)

- **Azure Terraform:** run with your RG/subscription; set allowed\_countries, ip\_allowlist, alert\_email, Key Vault/AKS vars; apply Front Door + WAF + AppInsights + AKS + KV.
- **Helm values:**
  - Domains in ingress.hosts, env.NEXT\_PUBLIC\_API\_URL, env.NEXTAUTH\_URL
  - Temporal envs; Key Vault URI if using API secret fetch; plan map; CORS origins
- **Secrets** (via Key Vault CSI or Helm secrets):
  - DATABASE\_URL, NEXTAUTH\_SECRET, SSE\_SIGNING\_SECRET
  - QBO: QBO\_CLIENT\_ID, QBO\_CLIENT\_SECRET
  - Stripe: STRIPE\_SECRET, STRIPE\_WEBHOOK\_SECRET, STRIPE\_PLAN\_MAP
  - SSO: GOOGLE\_\*, OKTA\_\*, AZURE\_AD\_\*
- **Web:** enable providers in NextAuth env; confirm web deploy target (AKS ingress or static hosting).
- **Temporal Cloud / Self-hosted:** set TEMPORAL\_ADDRESS, TEMPORAL\_NAMESPACE and open task queue q2o-sync; deploy **worker**.
- **Odoo v18:** ensure instance ready (modules installed, API key issued). Use **Onboarding** page to save & test.