

DOCUMENTO UFFICIALE DI ACCREDITAMENTO & PROCEDURE OPERATIVE

PureLabs VoiceCore

Manuale Operativo Tecnico–Amministrativo Enterprise

Specifiche Architetture, Configurazione Dual-Protocol :8090, Sicurezza M365 Entra ID, API Google
GBP & SOP Sistemistiche di Presidio.

● DUAL-PROTOCOL ENGINE :8090

Server nativo Windows con API REST asincrona e fallback multi-thread.

● SQLITE WAL & IMMUTABILITÀ

Write-Ahead Logging, thread-safety, integrity check e zero corruzione dati.

● M365 ENTRA ID & RBAC

Single Sign-On aziendale, token bearer sicuri e segregazione ruoli.

● GBP API & TAMPER GUARD

Sincronizzazione orari, recensioni e monitoraggio consistenza NAP 21 sedi.

MANUALE OPERATIVO TECNICO-AMMINISTRATIVO PURELABS VOICECORE

Specifiche Architettureali, Configurazione di Sistema, Sicurezza M365, API Google GBP & Procedure di Esercizio

Documento Tecnico di Riferimento per IT Engineering, DevOps, Cybersecurity & DPO

Versione 5.0.0 Enterprise / Infrastruttura & Connettività Sanitaria / Settembre 2026

1. ARCHITETTURA DI SISTEMA & TOPOLOGIA DI RETE

1.1 Panoramica dell'Infrastruttura

PureLabs VoiceCore è un sottosistema autonomo e disaccoppiato dell'ecosistema sanitario PureLabs. Risiede fisicamente sul server centrale di produzione `srvpurelabs` (IP Tailscale: `100.65.69.32` / LAN: `192.168.1.50`) e risponde sulla porta di servizio **8090**. Il sistema è pubblicato su internet con il dominio pubblico ufficiale `voicecore.purelabs.it` mediante terminazione TLS e routing gestito dal firewall hardware aziendale **OPNsense** (Sede Centrale PureLabs Milano, Viale Enrico Forlanini 23).



1.2 Dual-Protocol Sniffer & Sicurezza TLS

Il server web proprietario in `server.py` implementa un'architettura **Dual-Protocol** all'interno della classe `ThreadedHTTPServer(ThreadingMixIn, HTTPServer)`:

- Tramite la primitiva `socket.recv(2, socket.MSG_PEEK)`, il server ispeziona i primi 2 byte di ogni connessione in ingresso senza consumarli dal buffer di ricezione;
- Se i byte corrispondono al pattern `0x16 0x03` (inizio del record TLS `ClientHello`), la socket viene incapsulata a runtime nel contesto crittografico `ssl_context.wrap_socket(sock, server_side=True)`;

- In caso contrario (richieste plain HTTP provenienti da reverse proxy locali o LAN), la connessione prosegue in chiaro senza generare errori o handshake timeout.

1.3 Presidio h24/7 come Servizio Windows Nativo

In ottemperanza alle regole infrastrutturali di PureLabs S.p.A., VoiceCore gira stabilmente come **Servizio Windows nativo** (`PureLabs_VoiceCore`):

- Gestito dal Service Control Manager (`services.msc`);
- Host wrapper nativo: `PureLabs_VoiceCore_Service.exe` (compilato in C# .NET);
- Avvio automatico (`Auto-Start`) al boot della macchina fisica prima dell'accesso utente;
- Watchdog di auto-healing: riavvio istantaneo del processo entro 3 secondi in caso di crash o eccezione non gestita;
- Log operativi dedicati: `C:\NextCare\CustomerSatisfaction\voicecore_service.log` ;
- Monitoraggio proattivo del servizio `PureLabs_Heartbeat` su porta 8090 con alert automatici su canale **Microsoft Teams Dipartimento IT**, email M365 e notifiche Toast su desktop Windows 11.

• 2. MODELLAZIONE DATI & DATABASE ENGINE (SQLITE WAL)

2.1 Storage & Concorrenza

Il database risiede in `storage/voicecore.db`. È basato su SQLite 3.x configurato con:

- `PRAGMA journal_mode=WAL;` (Write-Ahead Logging per consentire letture concorrenti multiple senza blocco delle scritture);
- `PRAGMA foreign_keys=ON;` (integrità referenziale a cascata);
- Timeout busy handler impostato a `20.0s`.

2.2 Schema DDL & Principali Entità Relazionali

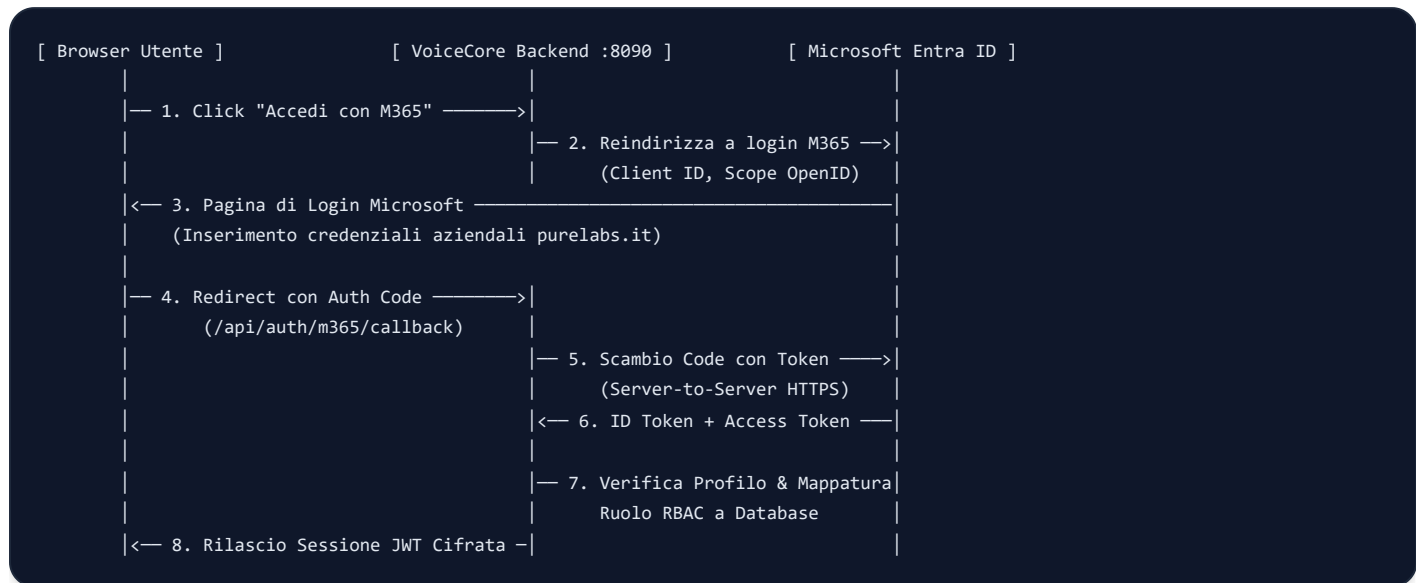
Lo schema relazionale comprende 15 tabelle normalizzate:

1. `companies` : Anagrafica delle 11 regioni sociali del gruppo (Codice, Nome, Partita IVA, Regione di appartenenza, Palette cromatica brand, Logo);
2. `clinics` : I 21 presidi sanitari territoriali collegati alle società (Indirizzo, Telefono, Email, Coordinate geografiche `latitude` / `longitude`, Orari di apertura, `google_place_id`, `google_review_url`);
3. `surveys` : Questionari compilati dai pazienti (`nps_score`, `nps_category`, canale marketing, canale prenotazione, `appointment_on_time`, `csat_acceptance`, `csat_medical`, `csat_reporting`, testo suggerimento, dati contatto, flag instradamento a Google);
4. `service_recovery_tickets` : Ticket di reclamo (`survey_id`, severità, stato lavorazione, categoria disservizio `issue_category`, azione correttiva `recovery_action`, operatore assegnato, tentativi di chiamata, timeline multi-step immutabile `timeline_json`);
5. `users` : Utenti amministrativi profilati con Microsoft Entra ID (`m365_oid`, email aziendale, ruolo `holding` / `regional` / `facility`, JSON sedi abilitate `allowed_clinics_json`, preferenze report);
6. `google_api_configs` : Parametri di connessione OAuth2 per Google Business Profile API (Client ID, Secret, Master Account ID, `location_group_id`);
7. `google_reviews` : Tutte le recensioni Google Maps sincronizzate (ID recensione univoco, nome e foto autore, rating 1–5, timestamp, risposta inviata con data, sentiment score, topic clinici);
8. `google_location_insights` : Metriche di rendimento Google Maps (visualizzazioni ricerca, visualizzazioni mappe, telefonate, richieste indicazioni stradali);
9. `google_auto_reply_policies` : Politiche per risposte automatiche intelligenti a recensioni positive a 5 stelle (disattivato di default per presidio umano);
10. `google_posts` & `google_posts_locations` : Post promozionali, eventi screening e aggiornamenti pubblicati sulle schede Google Maps con targeting geografico;
11. `tamper_guard_logs` : Log di audit anti-manomissione NAP (Name, Address, Phone) con confronto fra anagrafica certificata e dati live Google;
12. `report_subscriptions` & `report_delivery_logs` : Schedulazioni dei digest email settimanali/mensili e storico delle trasmissioni.

● 3. AUTENTICAZIONE & FEDERAZIONE MICROSOFT 365 (ENTRA ID)

3.1 Flusso OAuth2 Server-Side Authorization Code Flow

Per azzerare i rischi di vulnerabilità CORS ed eliminare la dipendenza da popup browser instabili, l'autenticazione è strutturata secondo il flusso **Server-Side Authorization Code**:



3.2 Parametri Tenant & Sicurezza

- **Tenant ID:** `1c047d49-9712-4ea5-80c4-0e702251c57f` (PureLabs Group Azure Tenant);
- **Client ID:** `db00d5ae-ce9d-4e5f-9f10-aedf9e62f4bc`;
- **Session TTL:** 24 ore con rinnovo automatico al refresh dell'interfaccia;
- **Zero PHI nei Token:** Il JWT contiene esclusivamente identità tecnica (`sub`, `email`, `role`, `allowed_clinics`) e nessuna informazione sanitaria.

● 4. GOOGLE BUSINESS PROFILE (GBP) API & SYNC ENGINE

4.1 Architettura del Connettore (`backend/google_reviews_engine.py`)

Il connettore interroga le Google Business Profile API v4.9:

- **Location Group ID:** gestione raggruppata delle 21 sedi tramite il contenitore aziendale accreditato `locationsGroups/purelabs-all-clinics`;
- **Mapping Strutture 1:1:** ogni sede ha associato il `google_place_id` ufficiale e l'endpoint di recensione verificato;
- **Normalizzazione Date:** conversione automatica di stringhe grezze Google (es. "un mese fa", timestamp RFC3339) in formati ISO 8601 standard (`YYYY-MM-DD HH:MM:SS`), garantendo filtri temporali perfetti;
- **Deduplicazione Record:** chiave primaria univoca basata su `google_review_id`, impedendo duplicazioni durante le sincronizzazioni incrementali;
- **Background Worker Schedulato:** worker asincrono configurato per il polling periodico ogni 6 ore (o forzabile manualmente dal cruscotto).

4.2 Calcolo Ponderato Metrologico NPS & Statistiche

Il motore applica il rigore matematico stabilito dalla metodologia internazionale **Bain & Company / Fred Reichheld**:

- Formula:
$$\text{NPS} = \frac{\text{Promotori} - \text{Detrattori}}{\text{Totale}} \times 100 \text{ in } [-100, +100]$$
;
- Nessun dato fittizio o arrotondamento improprio: i KPI card rispecchiano le recensioni reali censite a database.

● 5. SCHEDULATORE REPORT DIGEST SETTIMANALI (M365 & SMTP)

5.1 Motore `backend/reports_engine.py`

Lo schedulatore interno esegue una scansione oraria per verificare le sottoscrizioni in scadenza:

- **Spedizione Standard:** ogni **Lunedì mattina alle ore 08:00**;
- **Canali di Spedizione Supportati:**
 1. **Microsoft Graph API:** trasmissione nativa tramite account di servizio certificato `voicecore@purelabs.it`;
 2. **SMTP Relay Office 365:** fallback automatico su `smtp.office365.com:587` con TLS.
- **Template HTML Luxury:** impaginazione istituzionale PureLabs a larghezza fissa (600px), responsive, compatibile con Microsoft Outlook Desktop (VML/MSO tags), Apple Mail e dispositivi mobili;
- **Audit di Spedizione:** ogni invio genera un record in `report_delivery_logs` con stato (`INVIATO` / `FALLITO`) e dettagli tecnici per la verifica dell'IT.

● 6. PROCEDURE OPERATIVE STANDARD (SOP) PER SISTEMISTI

6.1 Gestione dei Servizi Windows

Tutte le operazioni sul server `srvpurelabs` devono essere eseguite tramite la console centralizzata `C:\NextCare\GESTIONE_SERVIZI_PURELABS.bat` oppure da PowerShell amministrativo:

```
# Verifica stato del servizio VoiceCore
Get-Service -Name PureLabs_VoiceCore

# Riavvio del servizio in caso di aggiornamento del codice
Restart-Service -Name PureLabs_VoiceCore

# Arresto e Avvio
Stop-Service -Name PureLabs_VoiceCore
Start-Service -Name PureLabs_VoiceCore
```

❗ AVVISO CRITICO

Divieto di Sessioni Terminale Orfane: È severamente vietato eseguire `python server.py` manualmente da terminale interattivo. Il servizio è attivo h24/7 nel Service Control Manager.

6.2 Procedura di Backup & Disaster Recovery

1. Backup Integrale Automatizzato:

- Eseguire lo script: `python C:\NextCare\CustomerSatisfaction\tools\make_voicecore_backup.py`;
- Lo script genera un archivio compresso e validato in `C:\NextCare\CustomerSatisfaction\backups\PureLabs_VoiceCore_PreSync_Backup_YYYYMMDD_HHMMSS.zip`;
- Esegue automaticamente `zf.testzip()` per certificare l'assenza di corruzione.

1. Ripristino del Database (Recovery):

- Arrestare il servizio: `net stop PureLabs_VoiceCore`;
- Sostituire `storage/voicecore.db` con lo snapshot certificato;
- Verificare l'integrità del file: `sqlite3 storage/voicecore.db "PRAGMA integrity_check;"`;
- Riavviare il servizio: `net start PureLabs_VoiceCore`.

6.3 Configurazione Firewall & Porte di Rete

- Porta locale di ascolto: `8090 TCP` (Dual Protocol HTTP/HTTPS);

- Regola Windows Defender Firewall: "PureLabs VoiceCore Service 8090" abilitata per subnet locale e Tailscale;
- Regola NAT OPNsense: Port Forwarding da WAN IP pubblico porta 443 a IP LAN 192.168.1.50:8090 .