DOCUMENT TECHNIQUE

Interfaces et prérequis techniques

Document de référence à destination des directions des systèmes d'information

Domaines à autoriser · Stack par application · Prérequis par device · Déploiement en parc géré · On-Prem et BYOC

Ce document décrit ce qu'il faut autoriser, installer et préparer pour utiliser Gilbert dans une organisation, ainsi que la composition technique de chaque application. Il s'adresse aux équipes informatiques, réseau et sécurité, ainsi qu'aux prestataires qui administrent le parc. Les sections 1 à 10 s'appliquent à tous les déploiements. La section 11 ne concerne que le déploiement de Gilbert dans votre propre environnement.

SOMMAIRE

01 Vue d'ensemble de l'architecture

02 Choisir le bon canal selon la réunion

03 Domaines à autoriser sur les postes

04 Stack technique par application

05 Prérequis techniques par device

06 Déploiement de l'application ordinateur en parc géré

07 Matériel de salle

08 Authentification et gestion des identités

09 Services tiers et localisation des données

10 Données, sécurité et conformité

11 Gilbert On-Prem / BYOC (Deploy)

12 Check-list pour la mise en service

1 Vue d'ensemble de l'architecture

Gilbert est un assistant de réunion : l'application cliente capture ou dépose un fichier audio, celui-ci est transcrit puis synthétisé, et le compte rendu est restitué à l'utilisateur dans l'application. La chaîne complète repose sur une API REST exposée en HTTPS, unique point d'entrée de la solution. Aucun bot ne rejoint vos réunions.

COMPOSANT	RÔLE ET COMPOSITION
Applications clientes	Web, iOS, Android et ordinateur. Capture ou dépôt de l'audio, consultation des transcriptions et des comptes rendus (section 4)
Backend	FastAPI, Python 3.14. API REST en HTTPS, point d'entrée unique de la solution
Traitements asynchrones	Celery et Redis. Transcription, génération et exports exécutés en file d'attente
Base de données	PostgreSQL avec l'extension pgvector. Utilisateurs, réunions, transcriptions, comptes rendus, métadonnées et index vectoriel
Chaîne de transcription	Voxtral en service prioritaire, OVH Whisper en repli automatique
Génération des résumés	Mistral
Agent (RAG)	Interrogation du corpus de réunions par recherche augmentée, adossée à l'index pgvector
Doc Engine	Moteur d'export des comptes rendus vers les formats bureautiques
Suggested actions	Actions proposées à l'issue de la réunion et poussées vers les outils métier : Slack, Notion, HubSpot et autres intégrations
Hébergement	OVHcloud, France

Deux modes de déploiement. Gilbert est opéré par défaut en service mutualisé par Lexia, hébergé en France. Il peut également être déployé dans votre environnement selon le modèle BYOC ou en on-prem air-gappé. Les sections 2 à 10 s'appliquent aux deux cas ; la section 11 ne concerne que le déploiement dans votre environnement.

2 Choisir le bon canal selon la réunion

Les quatre applications ne captent pas la même chose. Ce tableau évite l'erreur la plus fréquente en début d'usage.

SITUATION	APPLICATION À UTILISER	CE QUI EST CAPTÉ
Réunion en salle (conseil, commission, CVS)	Ordinateur ou mobile	Micro du poste ou micro de salle, toutes les voix présentes
Visioconférence (Teams, Zoom, Meet)	Ordinateur	Son du système et micro, sans bot dans la réunion
Réunion hybride	Ordinateur, sur le poste qui porte la visio	Son du système et micro de salle
Entretien individuel, déplacement	Mobile (iOS, Android)	Micro de l'appareil, y compris écran verrouillé
Enregistrement déjà réalisé	Web ou ordinateur	Dépôt du fichier audio

Point d'attention. L'application web ne capte pas le son d'une visioconférence : elle enregistre le micro du poste et permet le dépôt de fichiers. Pour une réunion Teams, Zoom ou Meet, l'application ordinateur est nécessaire.

3 Domaines à autoriser sur les postes

Côté poste utilisateur, seuls des flux HTTPS sortants sont nécessaires. Aucun flux entrant vers le poste n'est requis, aucun port autre que 443 n'est utilisé.

DOMAINE	FLUX	USAGE
gilbert-assistant.ovh	HTTPS 443	Application web et API de production : envoi de l'audio, consultation des transcriptions et des comptes rendus
gilbert-assistant.ovh (WebSocket)	WSS 443	Avancement de la transcription en direct. À autoriser explicitement sur les proxys qui filtrent l'upgrade WebSocket
gilbert-assistant.fr	HTTPS 443	Site, page de téléchargement et mises à jour automatiques de l'application ordinateur. Bloquer ce domaine désactive les mises à jour
login.microsoftonline.com	HTTPS 443	Uniquement si le SSO Microsoft Entra est activé
App Store, Google Play	HTTPS 443	Installation, mise à jour et notifications des applications mobiles

Ces domaines sont les seuls contactés par les applications clientes. Les services tiers listés en section 9 sont appelés par le backend, jamais par les postes : ils n'ont pas à être autorisés sur votre réseau, sauf si vous hébergez Gilbert vous-même (section 11).

4 Stack technique par application

Quatre applications clientes partagent le même backend. Dans tous les cas, la transcription et la génération du résumé sont réalisées côté backend : aucun modèle n'est embarqué sur le poste ou l'appareil. Les cinq langues d'interface, français, anglais, allemand, espagnol et italien, sont prises en charge sur les quatre plateformes.

4.1 Gilbert Web

ÉLÉMENT	DÉTAIL
Frontend	React 18, TypeScript, Vite
Backend	FastAPI, Python 3.14
Traitements asynchrones	Celery et Redis
Base de données	PostgreSQL avec pgvector
Transcription	Voxtral prioritaire, repli automatique sur OVH Whisper
Résumés	Mistral
Suggested actions	Actions proposées après la réunion, poussées vers Slack, Notion, HubSpot et autres intégrations
Agent	Interrogation du corpus de réunions en RAG
Doc Engine	Export des comptes rendus
Langues	FR, EN, DE, ES, IT
Interfaces	Séparation stricte entre l'interface utilisateur et l'interface d'administration
Statut	En production sur gilbert-assistant.ovh

4.2 Gilbert iOS

ÉLÉMENT	DÉTAIL
Technologies	Swift 5, SwiftUI
Cible minimale	iOS 16 et versions supérieures
Enregistrement	Capture en arrière-plan, écrite en segments .m4a successifs
Reprise après incident	Recovery après crash : les segments déjà écrits sont retrouvés et l'enregistrement est reconstitué
Envoi	Upload chunked vers le backend
Traitement IA	Transcription et résumé réalisés côté backend
Notifications	Push via APNs
Langues	FR, EN, DE, ES, IT, répartis sur 26 catalogues .xcstrings
Langue de transcription	Déterminée côté backend, indépendamment de la langue d'interface
Statut	Application de référence : elle fixe l'UX canonique pour les autres plateformes

4.3 Gilbert Android

ÉLÉMENT	DÉTAIL
Technologies	Kotlin 1.9.20, Jetpack Compose
Niveaux d'API	minSdk 26, targetSdk 36
Architecture	Hilt et ViewModels
Enregistrement	Foreground service, avec notification permanente pendant la capture
Reprise après incident	Recovery pendant et après l'enregistrement
Envoi	Upload chunked robuste, tolérant aux coupures réseau
Traitement IA	Transcription et résumé réalisés côté backend
Notifications	Push via FCM
Facturation	Billing Google Play
Observabilité	Sentry
Langues	FR, EN, DE, ES, IT
Statut	Refonte progressive vers la parité UX et fonctionnelle avec iOS. Cette parité est encore en cours

4.4 Gilbert Desktop

ÉLÉMENT	DÉTAIL
Socle	Tauri 2.11, cœur en Rust
Frontend	React 18 et TypeScript, exécutés dans la WebView
WebView	WebView2 sur Windows, WebKit sur macOS
Capture audio	Micro et son système : ScreenCaptureKit sur macOS, WASAPI en mode loopback sur Windows
Contrôle en réunion	Pilule flottante native, au-dessus des autres fenêtres
Fonctionnement hors ligne	Queue offline-first : l'enregistrement se poursuit sans réseau et part dès la connexion rétablie
Envoi	Upload chunked
Traitement IA	Transcription et résumé délégués au backend
Consultation	Accès aux comptes rendus depuis l'application
Langues	FR, EN, DE, ES, IT, via le moteur i18n hybride partagé entre desktop et web
Rôle dans la feuille de route	Terrain d'avancée pour le Doc Engine V2, l'éditeur TipTap et le Studio

5 Prérequis techniques par device

Côté poste utilisateur, un seul flux est nécessaire : HTTPS sortant vers les domaines de la section 3. Aucun flux entrant vers le poste n'est requis.

5.1 Web (navigateur)

CRITÈRE	REQUIS
Navigateurs	Chrome 90+, Firefox 88+, Safari 14+, Edge 90+
Protocole	HTTPS obligatoire, upgrade WebSocket autorisé
Microphone	Autorisation microphone accordée dans le navigateur
Réseau	1 Mbit/s sortant minimum vers les domaines de la section 3

5.2 iOS

CRITÈRE	REQUIS
Version minimale	iOS 16
Permissions	Microphone, notifications, exécution audio en arrière-plan
Distribution	App Store, déployable par MDM (Intune, Jamf)
Notifications	APNs joignable depuis le réseau des appareils

5.3 Android

CRITÈRE	REQUIS
Version minimale	Android 8.0 (API 26), cible API 36
Permissions	RECORD_AUDIO, POST_NOTIFICATIONS, FOREGROUND_SERVICE_MICROPHONE
Restrictions de batterie	Exclure l'application des politiques d'optimisation agressives, le foreground service devant vivre toute la réunion
Distribution	Google Play Store, déployable par MDM
Notifications	FCM joignable depuis le réseau des appareils

5.4 Ordinateur (Windows, macOS)

CRITÈRE	WINDOWS	MACOS
OS minimum	Windows 10 (1803+)	macOS 13 Ventura
Runtime WebView	WebView2 (présent par défaut sur Windows 11)	WebKit natif
Capture du micro	Autorisation système et application	Autorisation micro dans Confidentialité et sécurité
Capture du son système	WASAPI loopback, sans autorisation supplémentaire	ScreenCaptureKit : autorisation d'enregistrement de l'écran requise
Distribution	.msi (parc géré) ou .exe	.dmg, ou .pkg pour un déploiement MDM
Configuration du poste	4 Go de RAM, 500 Mo de disque	4 Go de RAM, 500 Mo de disque

L'application ordinateur est distribuée pour Windows et macOS. Sur un poste Linux, l'application web reste utilisable pour l'enregistrement du micro et le dépôt de fichiers.

6 Déploiement de l'application ordinateur en parc géré

SUJET	DÉTAIL
Installation silencieuse	Paquet .msi installable sans interaction : `msiexec /i Gilbert.msi /qn`
Télédistribution	GPO, Microsoft Intune ou tout outil acceptant un paquet MSI. Sur macOS, déploiement MDM (Intune, Jamf)
Droits requis	Installation par utilisateur possible sans élévation. L'installation pour tous les utilisateurs du poste nécessite des droits administrateur
Signature du binaire	Binaires signés Windows et notarisés Apple. Aucun avertissement SmartScreen ou Gatekeeper à la première exécution
Mises à jour	Vérification automatique au lancement, téléchargement depuis gilbert-assistant.fr. Désactivables par paramètre d'installation ou en bloquant ce domaine, la version étant alors gérée par vos propres campagnes de déploiement
Proxy d'entreprise	Le proxy système est respecté, y compris authentifié. En cas d'inspection TLS, autoriser les domaines de la section 3 et l'upgrade WebSocket
Antivirus	Aucune exclusion nécessaire dans le cas général. Avec un EDR strict, autoriser le binaire, l'accès au microphone et le répertoire de travail de l'application

7 Matériel de salle

La qualité de la captation détermine celle du compte rendu. Ces points concernent en particulier les instances délibérantes, conseils et commissions.

SUJET	RECOMMANDATION
Microphone	Micro du poste jusqu'à six participants. Au-delà, micro pieuvre USB de conférence
Placement	Appareil au centre de la table, à distance égale des participants, hors flux de ventilation
Alimentation	Poste branché sur secteur pour toute réunion de plus d'une heure
Réunions à enjeu	Second appareil en enregistrement de secours sur les séances dont le compte rendu est opposable
Réseau en salle	L'enregistrement fonctionne hors ligne, la queue offline-first prenant le relais. L'envoi nécessite 1 Mbit/s sortant, une fois la séance terminée

8 Authentification et gestion des identités

Par défaut, les utilisateurs se connectent par email et mot de passe : aucune intervention n'est nécessaire côté annuaire. Le SSO Microsoft Entra ID est proposé en option pour les organisations qui souhaitent centraliser les accès. Les sessions authentifiées sont portées par des jetons JWT.

ÉLÉMENT	DÉTAIL
Mode par défaut	Email et mot de passe, comptes créés depuis l'interface d'administration
Option SSO	Microsoft Entra ID, sur votre tenant, en OAuth 2.0
Sessions	Jetons JWT pour les sessions applicatives
Séparation des rôles	Interface utilisateur et interface d'administration strictement séparées
À préparer si SSO	Enregistrement de l'application dans votre tenant, consentement administrateur, URL de redirection, attributs transmis (nom, prénom, adresse email)

9 Services tiers et localisation des données

Les services ci-dessous sont appelés par le backend, jamais par les postes utilisateurs. Le tableau précise pour chacun la donnée transmise et sa localisation d'hébergement.

SERVICE	RÔLE	HÉBERGEMENT	DONNÉES TRANSMISES
OVHcloud	Hébergement du backend et de la base	France	Ensemble des données de la solution
Voxtral	Transcription, service prioritaire	France	Fichier audio et langue
OVH Whisper	Transcription, repli automatique	France	Fichier audio et langue
Mistral	Génération des résumés et Agent	France	Texte transcrit et prompt
Brevo	Emails transactionnels	Société française, hébergement UE	Nom, adresse email, lien vers le compte rendu
Slack, Notion, HubSpot	Intégrations des suggested actions	Selon l'éditeur, activation à votre initiative	Contenu de l'action poussée, uniquement pour les intégrations que vous activez
Prometheus	Métriques opérationnelles	Auto-hébergé, France	Compteurs et latences, aucun contenu métier
Sentry	Erreurs applicatives, backend et Android	Auto-hébergé, France	Stack trace et contexte technique, aucun contenu métier

Cloisonnement des données. Les fichiers audio ne sont transmis qu'aux seuls services de transcription. Aucun contenu métier, ni audio, ni transcription, ni compte rendu, n'est transmis aux services de supervision et de suivi des erreurs.

10 Données, sécurité et conformité

SUJET	RÈGLE APPLIQUÉE
Localisation	Hébergement en France chez OVHcloud, transcription et génération en France. Vos échanges ne quittent pas le territoire français
Rétention de l'audio	Suppression du fichier audio après transcription réussie. Suppression automatique après 24 heures en cas d'attente ou d'échec. Durée paramétrable
Transcriptions et comptes rendus	Conservés tant que la réunion existe dans le compte, supprimables à tout moment par l'utilisateur
Entraînement des modèles	Aucune donnée client utilisée pour entraîner des modèles
Réversibilité	Export des données en formats ouverts par le Doc Engine, sur demande et à tout moment
Transport	HTTPS et TLS 1.2 ou 1.3 sur l'ensemble des échanges client et serveur

Documents disponibles sur demande : document de sécurité et conformité Gilbert (réf. SC-2026-01), modèle de DPA, politique de sécurité des systèmes d'information, charte Frugalité IA.

11 Gilbert On-Prem / BYOC (Deploy)

Le modèle principal est le **BYOC, Bring Your Own Cloud** : vous possédez les données et l'infrastructure, l'éditeur pouvant opérer l'instance à distance. Une variante on-prem air-gappée, sans aucune liaison sortante, est également prévue. Dans les deux cas, la transcription et la génération des résumés restent dans votre environnement : aucune donnée de contenu ne transite par le SaaS mutualisé.

ÉLÉMENT	DÉTAIL
Infrastructure	Linux Ubuntu 22.04 LTS, Docker 24+, 2 vCPU et 4 Go de RAM minimum, 20 Go de stockage, PostgreSQL avec pgvector et Redis
Réseau	Port 443 en entrée via load balancer ou reverse proxy TLS, enregistrement DNS de type A, certificat Let's Encrypt ou équivalent
STT et LLM	Deux options : Azure OpenAI, ou vLLM auto-hébergé exposant une API compatible OpenAI
Control-plane	Gilbert Deploy, centralisé : suivi de santé, suivi d'usage et distribution des mises à jour
Modèle de distribution	Push ou pull selon votre politique réseau, avec payload allowlisté. Aucun accès au contenu par le control-plane
Statut	Étude et audit de faisabilité réalisés, plan arrêté en deux lots : backend, puis desktop. L'implémentation est à venir

12 Check-list pour la mise en service

Domaines autorisés sur les postes, le proxy et l'inspection TLS — SECTION 3

Mode d'installation de l'application ordinateur et politique de mises à jour — SECTION 6

Authentification : email et mot de passe, ou SSO Microsoft Entra — SECTION 8

Intégrations des suggested actions à activer : Slack, Notion, HubSpot — SECTION 9

Matériel des salles : micro pieuvre au-delà de six participants, alimentation secteur — SECTION 7

Mode de déploiement : SaaS mutualisé, BYOC ou on-prem air-gappé — SECTIONS 1, 11