

安全 · 2026 年 10 月

安全与隐私

除非另有说明，本文适用于默认的**本地部署**配置。

1. 部署方式

- 每个会议室一台 Windows 电脑运行所有环节：采集、语音检测、识别、翻译、语音合成和送达。
- 所有模型随安装包提供，从电脑磁盘读取。
- 安装、启动或开会均不需要互联网连接。
- 无许可证服务器、无遥测、不检查更新、无云账号。
- **已实测：**在启动、空闲和整场会议期间，均未连接电脑之外的任何地址。请参阅《网络行为声明》文档。

2. 网络暴露面

- 会议室网络上只有一个监听端口：TCP 8760（可配置），用于参会者页面、音频流、会议室屏幕和控制台。
- 每个内部服务（采集、翻译引擎、神经语音）都绑定到 `127.0.0.1`，无法从网络访问。
- 安装程序创建的防火墙规则只在**专用和域**网络上放行该端口 – 绝不在公用网络上放行。
- 推荐的会议室网络：独立 VLAN 上的专用 WiFi 接入点，连接会议室电脑，且没有更远的路由。

3. 数据生命周期

数据项	位置	保留时长	默认
采集的音频	电脑内存	数秒	从不写入磁盘。不存在可录音的设置。
识别文本	电脑内存	一句话	翻译并播报后即丢弃

数据项	位置	保留时长	默认
翻译文本和音频	电脑内存 → 会议室网络 → 所选手机	播放一次	电脑不保存
手机上的字幕	手机浏览器内存	直到关闭页面或会议结束	不写入设备
文字记录	电脑内存	由操作员设定	关闭
文字记录导出	—	—	关闭
日志中的会议文本	电脑磁盘	滚动覆盖	关闭 — 日志只记录句子长度和词数，从不记录内容
手机偏好设置	手机浏览器存储	直到清除	仅语言选择和浅色/深色

刻意不提供“保留音频”选项：处理流程中没有任何环节把采集的音频写入磁盘，提供这样的开关会暗示一种并不存在的能力 — 以及风险。

4. 访问控制

参会者。 参会者页面和音频流只能从会议室网络访问。可选的会议 PIN 把守入口；在 PIN 被接受前，页面不提供任何选项，音频流和文字记录流也会拒绝连接。每部手机只接收持有人所选的语言。

会议室屏幕。 仅用于显示。显示加入地址、PIN 和语言。其文字记录默认关闭，只显示开启后所说的内容，会议结束即清除。受同一 PIN 保护。

操作员控制台。

- 在会议室电脑的桌面窗口中，控制台使用发给该窗口的一次性本地令牌打开。
- 从任何其他机器访问都需要管理员密码（HTTP Basic 认证）。
- 密码在安装时生成，只保存在单独的凭据文件中 — 绝不保存在可共享的配置文件中，该配置文件可以放心交给支持团队。未设置密码时拒绝访问，绝不会因此放行。
- 只有当会议室屏幕和控制台在会议室电脑本机运行时才会显示 PIN；PIN 绝不会返回给其他机器。

会议。 会议之外不传译任何内容。结束会议会立即停止传译：排队中的句子被丢弃，每部手机放弃待播音频并提示会议已结束，会议室屏幕清除文字记录。

5. 软件供应链

- 一个离线安装包：应用、其全部依赖、所有模型和语音，以及所需的运行环境。
- 安装前会校验所含组件的完整性。
- 安装包中的每个语音都获得商用许可。
- 凭据绝不写入可共享的配置。

6. 运行环境

- Windows 更新、终端防护和电脑上的其他软件仍遵循客户的 IT 策略。
- 操作员窗口是 Microsoft Edge WebView2；Ovvo s Wasel 启动它时关闭了后台联网、组件更新和 SmartScreen。站点可通过自己的 WebView2 策略覆盖这些设置。
- 对于物理隔离的会议室，请将电脑及其接入点与任何对外路由隔离；产品本身不需要任何路由。

7. 支持模式

- 无常驻远程代理、电脑上无供应商账号、无入站端口。
- 远程支持仅在客户使用自己批准的工具开启的会话中进行，全程监督；客户关闭即结束。
- 支持从不需要会议音频或文字记录。
- 物理隔离的会议室：电话支持，由操作员操作键盘，或在陪同下现场支持。

8. 云端配置

可选，默认关闭。当操作员启用并输入 API 密钥后，音频和文本会按设计发送给所选服务商（Azure、Deepgram、DeepL、OpenAI、Anthropic、ElevenLabs）。凡是内容必须留在本地的场合，都应保持关闭。