

SECURITY · OCTOBER 2026

Security & Privacy

Applies to the default **on-premise** profile unless stated.

1. Deployment posture

- One Windows PC per room runs every stage: capture, speech detection, recognition, translation, voices and delivery.
- All models ship in the installer and are read from the PC's disk.
- No internet connection is needed to install, start or run a meeting.
- No licence server, no telemetry, no update check, no cloud account.
- **Measured:** no connection to any address outside the PC during start-up, idle or a full meeting. See the Network Behaviour Statement document.

2. Network exposure

- **One** listening port on the room network: TCP 8760 (configurable), serving the participant page, the audio stream, the room display and the console.
- Every internal service (capture, translation engine, neural voice) is bound to `127.0.0.1` and unreachable from the network.
- The installer's firewall rule allows the port on **Private and Domain** networks only – never Public.
- Recommended room network: a dedicated WiFi access point on an isolated VLAN with a link to the room PC and no route beyond it.

3. Data lifecycle

Artefact	Where	Lifetime	Default
Captured audio	PC memory	Seconds	Never written to disk. No setting exists to record it.
Recognised text	PC memory	One sentence	Discarded after it is translated and spoken

Artefact	Where	Lifetime	Default
Translated text and audio	PC memory → room network → the chosen phone	Played once	Not stored by the PC
Captions on a phone	Phone browser memory	Until the page closes or the meeting ends	Not written to the device
Transcript	PC memory	Operator-defined	Off
Transcript export	—	—	Off
Meeting text in logs	PC disk	Rotating	Off — logs record a sentence's length and word count, never its words
Phone preferences	Phone browser storage	Until cleared	Language choice and light/dark only

There is deliberately no "keep audio" option: nothing in the pipeline writes captured audio to disk, and offering a switch would imply a capability — and a risk — that does not exist.

4. Access control

Participants. The participant page and audio stream are reachable only from the room network. An optional meeting PIN gates them; until it is accepted the page offers nothing to choose and the audio and transcript streams refuse the connection. Each phone receives only the language its holder chose.

Room display. Output only. Shows the join address, PIN and languages. Its transcript is off by default, shows only what is said after it is switched on, and clears when the meeting ends. Protected by the same PIN.

Operator console.

- In the desktop window on the room PC, the console opens with a one-time local token issued to that window.
- From any other machine it requires the administrator password (HTTP Basic authentication).

- The password is generated at installation and stored only in a separate credentials file — never in the shareable configuration file, which is safe to hand to support. An unset password denies access; it never grants it.
- The PIN is shown to the room display and console only when they run on the room PC itself; it is never returned to another machine.

Meetings. Nothing is interpreted outside a meeting. Ending a meeting stops interpretation immediately: queued sentences are discarded, every phone drops the audio it was holding and shows that the meeting has ended, and the room display clears its transcript.

5. Software supply chain

- One offline installation package: the application, all its dependencies, all models and voices, and the runtime it needs.
- Bundled components are integrity-checked before they are installed.
- Every voice in the package is licensed for commercial use.
- Credentials are never written to the shareable configuration.

6. Operating environment

- Windows updates, endpoint protection and other software on the PC remain under the customer's IT policy.
- The operator window is Microsoft Edge WebView2; Ovvos Wasel starts it with background networking, component updates and SmartScreen switched off. A site can override these flags through its own WebView2 policy.
- For air-gapped rooms, isolate the PC and its access point from any outward route; the product needs none.

7. Support model

- No standing remote agent, no vendor account on the PC, no inbound port.
- Remote support only in a session the customer opens, with their own approved tool, attended throughout; it ends when they close it.
- Support never needs meeting audio or transcripts.
- Air-gapped rooms: telephone support with the operator at the keyboard, or an on-site visit under escort.

8. The cloud profile

Optional and off by default. When an operator enables it and enters API keys, audio and text are sent to the chosen providers by design (Azure, Deepgram, DeepL, OpenAI, Anthropic, ElevenLabs). It should remain off wherever content must stay on site.