

SECURITY · OCTOBER 2026

Network Behaviour Statement

Product: Ovvos Wasel 1.0 (on-premise profile, default configuration) **Measured:** 14 October 2026

This statement lists every network port Ovvos Wasel opens and every address it contacts. **The second list is empty.** It also records how that was measured, so an accreditation team can repeat it.

1. Ports the product opens

Port	Bound to	Process	Purpose	Reachable from
8760/TCP (configurable)	all interfaces	Ovvos Wasel server	Participant page, audio/caption stream (WebSocket), room display, operator console	The room network
8761/TCP	127.0.0.1	Audio capture service	Hands captured audio to the server	This PC only
ephemeral/TCP	127.0.0.1	Translation engine	Translation requests from the server	This PC only
ephemeral/TCP	127.0.0.1	Neural voice service	Speech synthesis requests from the server	This PC only

Only one port faces the network. The installer (run as Administrator) creates one inbound Windows Firewall rule for it, allowed on **Private and Domain** networks and never on Public ones.

2. Addresses the product contacts

None. No component of Ovvos Wasel initiates a connection to any address outside the PC — no licence server, no telemetry, no update check, no model download, no cloud service.

To show its own address in the QR code, the server asks Windows which network interface it would use. It does this with a UDP socket "connected" to `198.51.100.1` (a reserved documentation address, RFC 5737, never routed). A UDP connect sends no packet; it only makes Windows choose the interface. The server also resolves the PC's own hostname. Neither leaves the PC.

3. How this was measured

Two independent witnesses ran together, so a short-lived connection missed by one would be caught by the other.

Witness 1 — the operating system's TCP table. Every 150–200 ms, every TCP connection owned by an Ovvos Wasel process — the application, its capture service, translation engine, voice service, and the WebView2 processes hosting its window — was recorded if its remote address was not this PC.

Witness 2 — audit hooks inside every process. An audit handler loaded into every process the application starts fires inside the networking layer for *every* name lookup and connection attempt, however brief, so nothing can fall between polls. The handler was tested first against a known lookup.

Scenarios

1. Cold start to engines ready, then idle — 110 seconds.
2. A full meeting: start meeting, a phone connected listening in Arabic, 95 seconds of English speech played into the room, four target languages, end meeting — 230 seconds.
3. The neural voice service started on its own and asked to speak Arabic, English and German.
4. The application window.

4. Results

Scenario	Witness 1 (TCP)	Witness 2 (audit hooks)
Cold start + idle, 110 s	No connections outside the PC	No lookups or connections outside the PC (only the UDP interface probe and own-hostname lookup described above)
Full meeting, 230 s – 12 sentences, 48 deliveries in 4 languages, all 12 received by the phone	No connections from Ovvos Wasel processes	Nothing beyond the interface probe
Neural voice: start, then speak Arabic, English, German	—	No lookups or connections ; all three synthesised successfully
Application window	No connections	—

5. Scope and limits

- **Default on-premise profile.** The optional cloud profile, if an operator enables it and enters API keys, sends audio and text to the chosen provider by design. It is off by default.
- **The operating system is out of scope.** Windows Update, Defender, time sync and other software on the PC follow the customer's own IT policy. For an air-gapped room, isolate the PC and its access point from any route outward.
- **Installation.** The offline package installs with no internet connection.
- **Repeatability.** The measurement scripts can be supplied to an accreditation team. The simplest independent check is a span-port capture or host firewall log during an acceptance meeting: expect no outbound flow from the Ovvos Wasel processes.