

Deployment notes for IT

Installing without administrative rights, what the application writes and where, and what to allow through an endpoint agent.

1. Installation

Per-user. No administrative rights are required and no system services are installed. The application writes nothing outside the user's own profile and the folders the operator chooses.

2. Code signing

macOS is signed with a Developer ID Application certificate, with the hardened runtime enabled, notarised by Apple and stapled so Gatekeeper can verify it without network access.

Windows is signed as CHADURA TECH PRIVATE LIMITED and timestamped, including every nested binary and DLL inside the installer. SmartScreen builds reputation per certificate, so a download may still show a warning until that reputation accrues; the publisher shown will be the name above rather than "Unknown publisher".

The Linux .rpm is GPG-signed and can be verified against the published key before installation.

3. Network policy

The application requires no network access and makes no connections. It can be run on a host with all outbound traffic blocked, and doing so is a reasonable way for a customer to verify the claim independently. Every feature works in that state; the only visible effect is that the website links in the interface fail to open, since those are handed to the user's browser rather than fetched by the application. See the Network section of the security overview.

4. Filesystem access

The application reads the folders the operator selects and writes only into the output directories listed in the security overview, plus its own storage under the user profile. It never modifies an original document in place.

5. What to give it

- Read and write access to the engagement folders the operator works on.
- Nothing else. No shared service account, no database, no inbound ports.

6. Verifying the claims yourself

- Run it with the network disconnected; everything except nothing continues to work.
- Watch it with a network monitor; there is no traffic to see.
- Inspect resources/sidecar and confirm the process opens no sockets (`lsof -i`).
- The generated IPC and sidecar surfaces in the security overview are the complete list of operations the interface can trigger.

7. Known limitations

- No independent audit of the signing chain. All three platforms are signed — Windows as CHADURA TECH PRIVATE LIMITED and timestamped, macOS notarised and stapled, the .rpm GPG-signed — but a customer wanting assurance beyond checking the signatures themselves should ask for one.
- No independent penetration test.
- No SOC 2 or ISO 27001.
- **English is the only OCR language pack bundled.** The engine itself ships on all three platforms. Roman-script documents in other languages are recognised acceptably; a different script is not recognised at all, and the failure looks like a poor scan rather than a missing pack.
- The bundled Windows tesseract .exe is the upstream UB Mannheim build, unmodified. It shipped carrying a third-party signature whose issuing certificate had expired; it is now re-signed as CHADURA TECH PRIVATE LIMITED along with the rest of the installer, so it validates like everything else inside it.