

PLwC Softwarebeschreibung - Open Beta v0.2.0-rc18.dev9

Stand: 13. Juli 2026

Zweck

PLwC - Personality Layer with Conscience - ist ein gesteuertes lokales MCP-Gateway fuer MCP-faehige Assistenten. Es verhindert, dass eine KI unkontrolliert auf Dateien, Shell, Dokumente oder dauerhafte Profildaten zugreift.

Die Open Beta richtet sich an technisch versierte Nutzer, Tester und Pruefer. PLwC ist kein finaler oeffentlicher Release und nicht produktionszertifiziert.

Ziel-Clients

PLwC ist fuer Claude Desktop und kompatible lokale MCP-Clients ausgelegt. Das oeffentliche Repository beschreibt ausserdem lokale GPT-Clients und Odysseus als relevante Test- und Integrationsziele.

Gateway-Modell

PLwC stellt genau einen sichtbaren MCP-Server bereit:

- `plwc-gateway`

Alle wirksamen Operationen laufen ueber Policy- und Governance-Pruefungen. Fruehere Einzeltools sind nicht mehr als eigene oeffentliche Facade-Tools sichtbar.

Oeffentliche Facade-Tools

Die Open Beta v0.2 stellt acht oeffentliche Facade-Tools bereit:

- `plwc_status`
- `plwc_describe`
- `plwc_profile`
- `plwc_reflection`
- `plwc_governor`
- `plwc_sandbox_run`
- `plwc_workspace_operation`
- `plwc_document_operation`

Kontrollierte Faehigkeiten

PLwC kontrolliert insbesondere:

- Workspace-Operationen innerhalb konfigurierter Roots
- Dokumentoperationen fuer DOCX, XLSX, PPTX, PDF, ZIP und Bilder
- Docker-backed Python- und Shell-Ausfuehrung
- Profilaktivierung und Profilkompilierung
- gesteuerte Reflection-Eintraege
- Memory- und Persona-Governance ueber Plan-/Apply-Flows
- strukturierte lokale Audit-Events

Sicherheitsmodell

PLwC folgt einem fail-closed Modell:

- Ein sichtbarer Gateway-Server, keine Bypass-MCPs.
- Geschuetzte Profil- und Governance-Dateien koennen nicht direkt ueber Workspace-Operationen editiert werden.
- Parent Traversal, absolute Host-Pfade, UNC-Pfade und geschuetzte Segmente werden abgelehnt.
- Python- und Shell-Snippets laufen ueber Docker.
- Es gibt keinen stillen Rueckfall auf eine Host-Shell.
- Fehlende Engines, fehlende Docker-Images und Policy-Denials scheitern geschlossen.
- Dokument-Assets muessen workspace-relativ sein.

Bewusste Grenzen

Nicht im Open-Beta-Scope:

- OCR
- PDF-Redaktion
- digitale Signaturen
- Formularerstellung
- PDF/A-Claim
- LibreOffice- oder Pandoc-Konvertierung
- Makroausfuehrung
- Netzwerkzugriff zur Laufzeit
- JavaScript in PDFs
- HTML/CSS-Rendering-Pipeline

Status

- Status: Open Beta
- Version: `v0.2.0-rc18.dev9`

- Readiness: [RC_READY_WITH_NOTES](#)
- Paket-, Desktop- und Odysseus-Smoke-Test: [PASS](#)
- Paketierte Builds koennen unsigned sein.

Quellen

- Repository: <https://github.com/mhoedt-ai/PLwC>
- Installation: <https://github.com/mhoedt-ai/PLwC/blob/main/docs/INSTALLATION.md>
- Open Beta Testing: https://github.com/mhoedt-ai/PLwC/blob/main/BETA_TESTING.md
- Security Model: https://github.com/mhoedt-ai/PLwC/blob/main/docs/SECURITY_MODEL.md