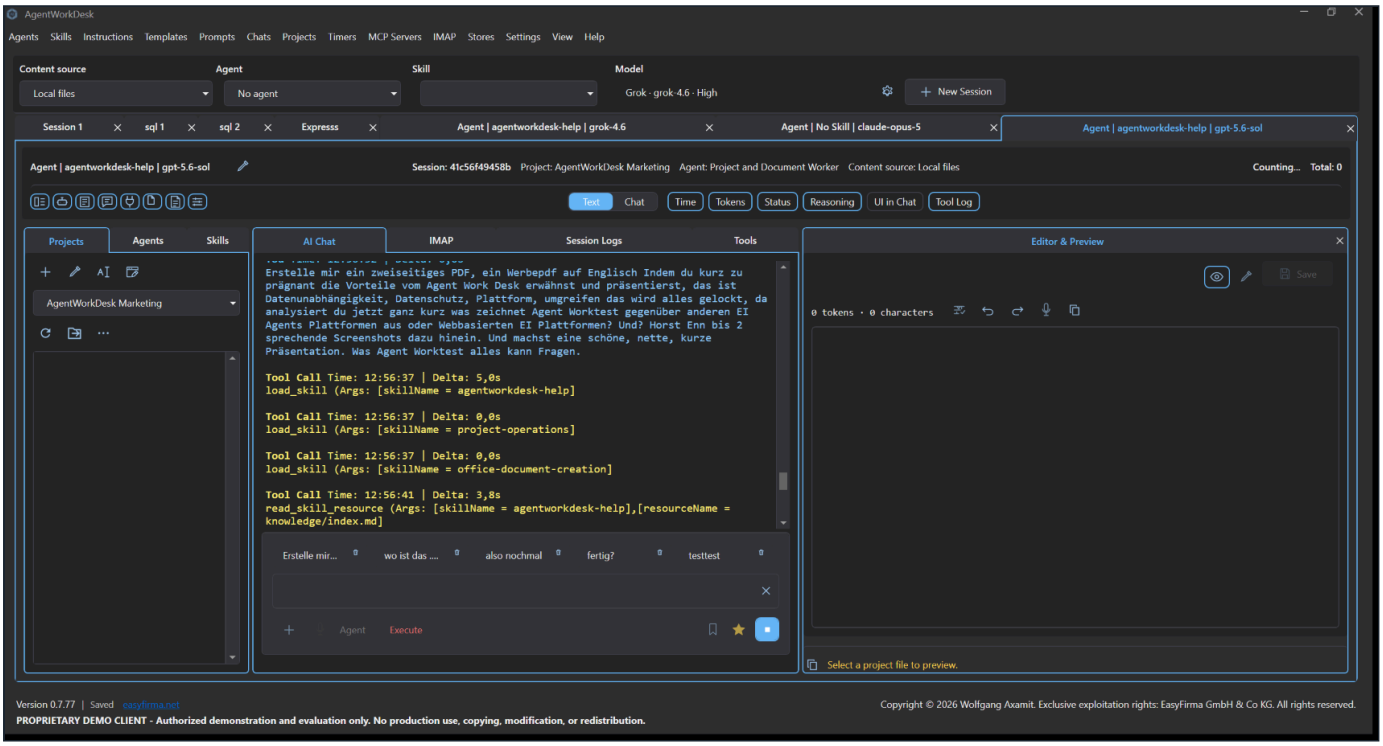
WINDOWS DESKTOP · UNTERNEHMEN · UNABHÄNGIGKEIT ALS PRINZIP

AgentWorkDesk

KI auf eigener Infrastruktur.

Native Windows-Anwendung für KI-Chats und Agent-Workflows. Die KI plant und schreibt Skripte, Ihr PC führt sie nach Freigabe aus. Eigene Datenspeicher, freie Modellwahl, verschlüsselte Zugänge und ausdrücklich freigegebene Tools.



Ihr Arbeitsplatz. Projekte, parallele Sessions, KI-Chat und Editor direkt im Zugriff.

ANBIETER FREI WÄHLBAR

Grok · OpenAI · Anthropic · Gemini · DeepSeek · Mistral · Groq · OpenRouter · Perplexity · Azure OpenAI · Ollama

01 / IHRE DATEN
Unabhängigkeit
Lokale Dateien, Netzlaufwerke oder eigene SQL-Server; mehrere Speicher gleichzeitig.

02 / IHRE ZUGÄNGE
Datenschutz
API-, SQL-, IMAP- und MCP-Schlüssel verschlüsselt in eigenen Speichern.

03 / IHRE TOOLS
Kontrolle
Read, Write, Manage, Execute; Erhöhungen nur bestätigt und nur je Session.

04 / IHRE LOGS
Nachweise
Tokens, Tool Calls und HTTP in eigenen Session-, App- und Audit-Dateien.

Professionelle KI. Für die Praxis.

Einfach per Drag-and-drop. Ihr PC. Ihre Regeln. Ihre Nachweise.

INHALT

Inhalt und Überblick.

01 **Prinzip und Bedienung** 03
Die KI plant, der PC führt aus; Oberfläche und Ausstattung

02 **Arbeitsabläufe** 04
Dokumente, parallele Sessions, Timer und E-Mail-Workflow

03 **Agents und Skills** 05
Wiederverwendbare Spezialisten aus Instructions, Skills und Tools

04 **Modelle, APIs und Tools** 06
Anbieter, Laufzeit, Tool-Rechte, MCP und Settings

05 **Datenschutz und Kontrolle** 07
Speicher, Zugänge, Logs, Betriebsformen und Anbieterwechsel

06 **Leistung und Kosten** 08
Cloud und lokal im Vergleich mit belegten Anbieterwerten

07 **Altanlagen und Hardware** 09
Unbetreute Steuerungen am angeschlossenen PC analysieren

08 **Technische Architektur** 10
Schichten, Chat, Session und Run, Oberfläche, Fehlergrenzen und Logs

09 **Daten, Owner und Tools** 11
Architekturbild, Stores, Datenablage und Tool-Katalog

10 **Entwicklung, Qualität und Grenzen** 12
Konzept, Prüfungen, UI-Test und klar benannte Grenzen

11 **Quellen und Kontakt** 13
Anbieterangaben, Kostenbeispiele und Grundlage

Sechs Vorteile auf einen Blick

1 · DATEN

Kein Upload nötig

Das Skript arbeitet dort, wo die Daten liegen; Rohdaten bleiben im Haus.

2 · DATEIGRÖSSE

512 GB statt 512 MB

Ein Büro-PC hat 512 GB SSD; Cloud-Chats nehmen 40 bis 512 MB je Datei an.

3 · RECHENLEISTUNG

4 Kerne, 16 GB RAM

Schon ein Büro-PC übertrifft Sandboxen mit 1 CPU, 5 GiB RAM oder 30 s Laufzeit.

4 · KOSTEN

Keine Tokens fürs Rechnen

Lokale Rechenschritte erzeugen keine Tokens und keine Sitzungsgebühr.

5 · UNABHÄNGIGKEIT

Anbieter frei wählbar

Anbieter wechseln, Ablauf prüfen, weiterarbeiten; der Bestand bleibt.

6 · VERLÄSSLICHKEIT

Skript rechnet, Mensch gibt frei

Verbindliche Zahlen kommen aus geprüften Skripten, nicht aus KI-Antworten.

01 / PRINZIP UND BEDIENUNG

Die KI plant. Ihr PC führt aus.

Entscheidend ist der Ausführungsort des Skripts, nicht allein der Standort des Modells. An ein Cloud-Modell geht nur der tatsächlich gesendete Kontext.

Eigene Speicher

Dateien, Netzlaufwerke und eigene SQL-Server statt Anbieter-Cloudspeicher.

Freie Modellwahl

Cloud oder lokal. Anbieter wechseln, Daten und Arbeitsabläufe behalten.

Lokale Tools

Dokumente, E-Mail, SQL, MCP und Skripte mit kontrollierten Freigaben.

Profi-Code

Native Windows-App auf C#/.NET und WPF. KI-gestützt entwickelt, professionell geführt.



Produktiv ohne Kommandozeile

Windows-Oberfläche

Setup installiert die App. Projekte, Chats, Dateien und Einstellungen per Menü, Button und Drag-and-drop; Slash-Commands bleiben optional.

Vorbereitete Spezialisten

Default Settings, Agents und Skills: Agency Coordinator, Skill Architect, Project and Document Worker und Mail Assistant.

Profil je Aufgabe

Instructions, Antwortumfang, Reasoning, Verlauf, Laufzeiten, Logging; Templates und gespeicherte Prompts bewahren erprobte Konfigurationen.

Mehrere Monitore

Tabs lassen sich auf weitere Bildschirme ziehen; parallele Arbeit bleibt im Blick.

Was der lokale Ansatz leistet

Rohdaten bleiben am Speicherort

Lokale Rechenschritte erzeugen keine Modell-Tokens und brauchen keinen Cloud-Container.

Verbindliche Zahlen aus Skripten

KI-Antworten sind selbst bei Temperature=0 nicht garantiert reproduzierbar; geprüfte Skripte rechnen.

Bestand ohne KI nutzbar

Geprüfte Skripte bleiben im eigenen Bestand und laufen später auch ohne KI.

Keine Automatik-Konformität

Der Ansatz ersetzt weder fachliche Prüfung noch Freigaben und macht Cloud-Nutzung nicht automatisch datenschutzkonform.

Ergebnis: Sie nutzen KI, ohne Rohdaten hochzuladen, ohne Uploadgrenze und ohne Bindung an einen Anbieter.

02 / ARBEITSABLÄUFE

Vom Auftrag zum nutzbaren Ergebnis.

Wiederverwendbare Spezialisten verbinden Modelle, Fachwissen und Tools. Die Oberfläche hält Auftrag, Bearbeitung und Ergebnis zusammen.

Dokumente und Projekte

Word, PDF, Excel und PowerPoint erzeugen und im Projekt ablegen. Dateiverwaltung, Vorschau, Bearbeitung, Anhänge und Suche sind integriert.

Fortsetzen und zuordnen

Gespeicherte Chats und kompatible Agentenzustände lassen sich später fortsetzen. Jeder Lauf bleibt seinem gewählten Datenspeicher zugeordnet.

Parallel und delegiert

Mehrere Sessions und Modelle arbeiten gleichzeitig, auch im selben Projekt. Delegation und Todo-Listen koordinieren Teilaufgaben.

Timer für wiederkehrende Aufgaben

Auftrag, Anbieter, Modell, Skill und Zeitplan nach Intervall oder Kalender bei laufender App; neue oder weiterverwendete Session; Starts und Ergebnisse protokolliert.

Beispiel: Kundenanfragen im IMAP-Postfach

1 · Lesen
Ordner und Nachrichten auflisten, E-Mails lesen und durchsuchen.

→

2 · Einordnen
Produktwissen, Tonfall und Rückfrageregeln per Agent und Skill anwenden.

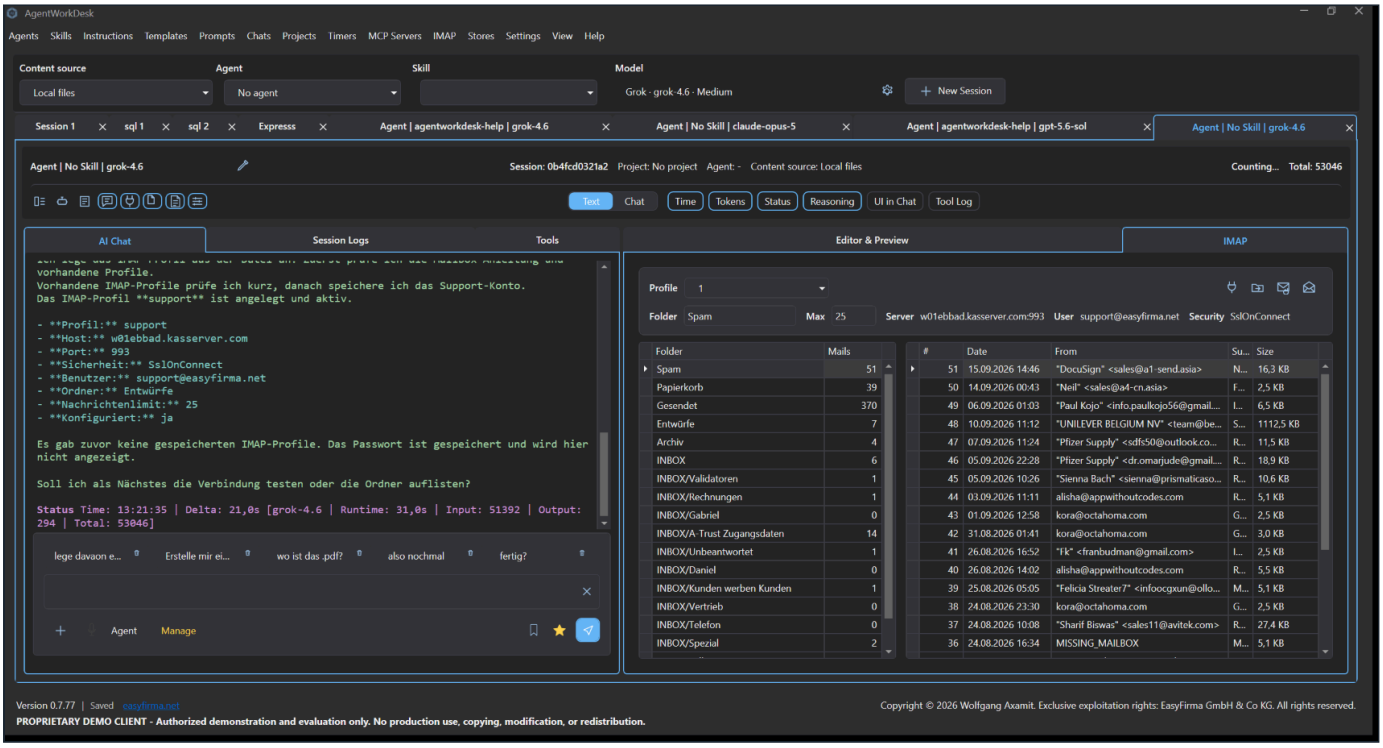
→

3 · Entwurf
Antwort mit Schreibfreigabe im Postfach ablegen; verschieben oder kopieren.

→

4 · Prüfen
Mensch prüft den Entwurf und schärft die Regeln nach.

IMAP ist integriert; ein zusätzlicher MCP-Server ist nicht nötig.



E-Mail-Workflow. KI-Chat und verbundenes IMAP-Postfach direkt in AgentWorkDesk.

03 / AGENTS UND SKILLS

Aufgabenwissen und Werkzeuge verbinden.

Spezialisten

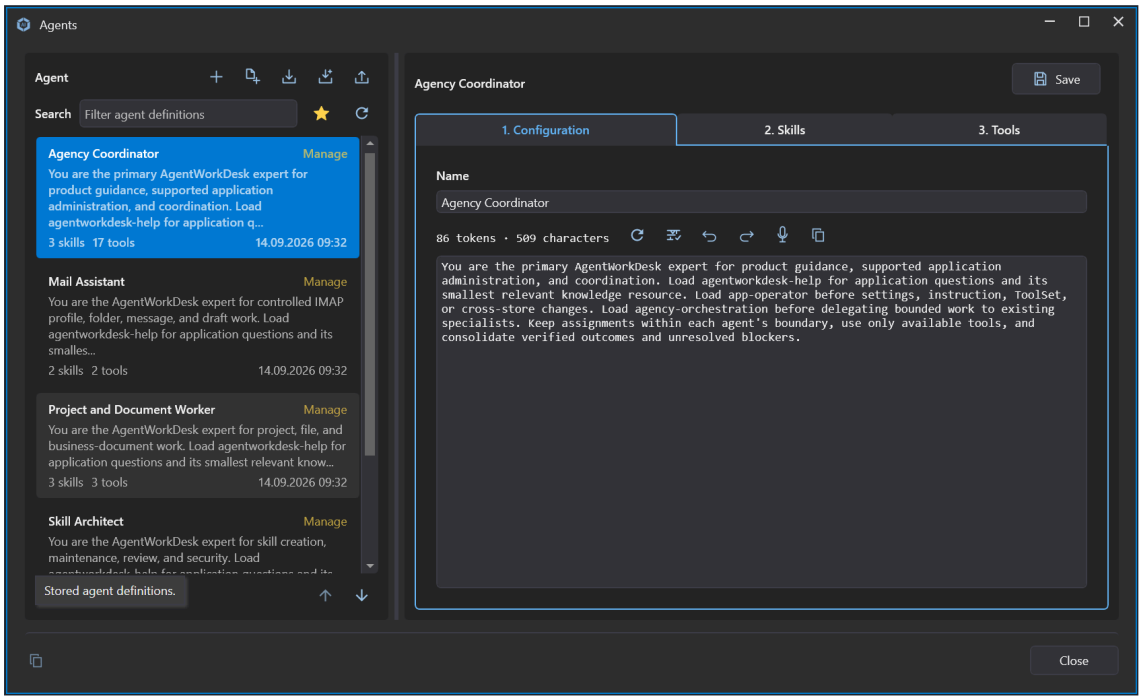
Systemprompt, Instructions, Skills und Tool-Auswahl legen das Verhalten fest; im Agent-Modus stehen nur die gewählten Tools bereit.

Skills

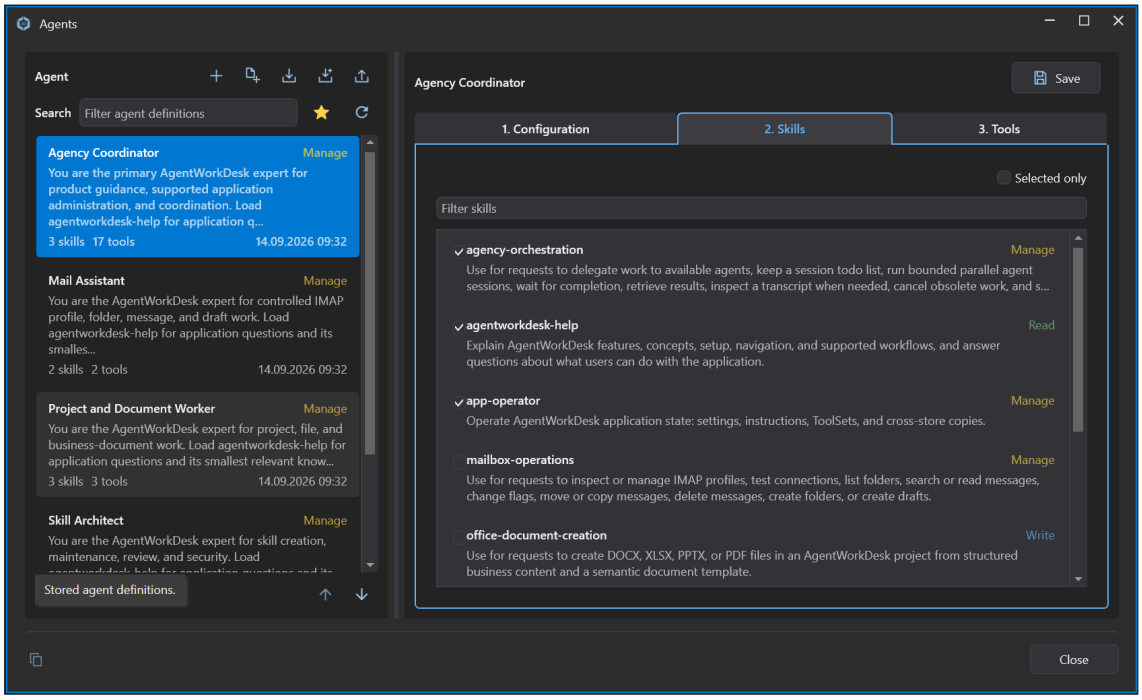
SKILL.md, Ressourcen und Skripte liefern wiederverwendbare Arbeitsanleitungen und Fachwissen.

Selbstverbesserung

Mit Freigabe erstellt, startet und verbessert die KI weitere Agents und Skills, auch anbieterübergreifend.



Agents. Vorbereitete Agents links, Instructions des gewählten Agents rechts; Configuration, Skills und Tools sind getrennte Bereiche.



Skills. Wiederverwendbare Skills werden gezielt zugeordnet; Beschreibung und Berechtigungsstufe zeigen ihren Aufgabenbereich.

04 / MODELLE, APIS UND TOOLS

Die Konfiguration bleibt bei Ihnen.

Grok OpenAI Anthropic Gemini DeepSeek Mistral Groq OpenRouter Perplexity Azure OpenAI Ollama

API-Zugänge, Endpunkte und Modelllisten konfigurierbar; lokales Ollama ohne Anbieter-API-Schlüssel. Auswahl nach Qualität, Preis, Geschwindigkeit und Datenschutz.

Microsoft Agent Framework

Microsoft.Extensions.AI mit gemeinsamer IChatClient-Schnittstelle; Antworten gestreamt. Auto, Chat- und Responses-API wählbar; Anthropic mit eigener Anbindung.

Rund 100 integrierte Tools

Projekte, Dokumente, IMAP, Agents, Skills, Settings und Session-Koordination; jedes Tool einzeln wählbar, Zugriffe technisch kontrolliert.

MCP gezielt anbinden

Lokale und entfernte Server über HTTP/HTTPS; Beschreibungen und Parameterschemata werden ausgelesen, jedes Tool ausdrücklich freigegeben.

Tool-Rechte gelten technisch

Read	Write	Manage	Execute
Startstufe	Schreiben	Verwalten	Ausführen

Neue Tabs beginnen mit Read. Erhöhungen nur nach Bestätigung und **nur für die Session**; Zustimmung wird nicht gespeichert, Reduktionen wirken sofort, Windows-Rechte bleiben maßgeblich.

Verhalten je Aufgabe

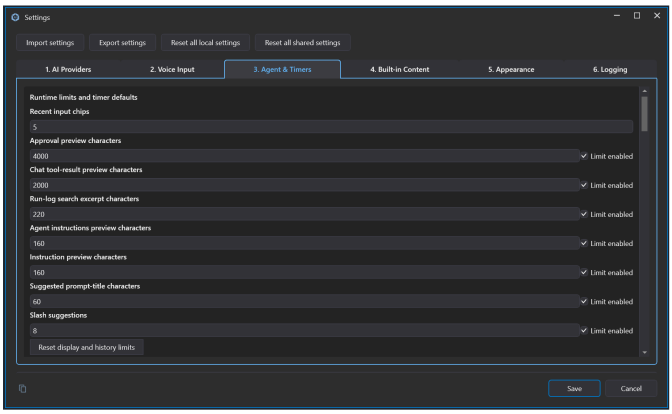
Systemprompt, Instructions, Aufgabenprompts und Skills bestimmen, was ein Agent tut.

Feineinstellung

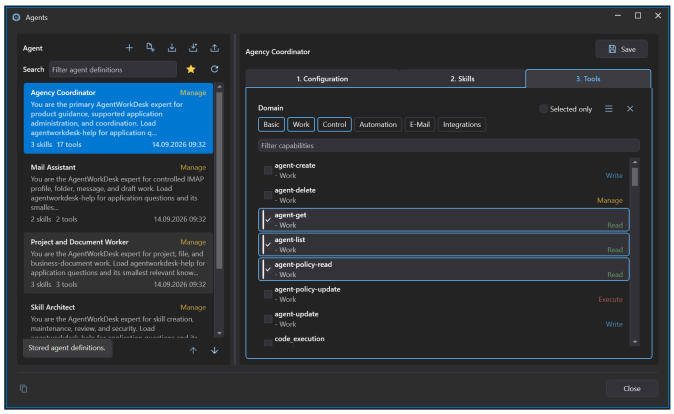
Antwortprofil, Ausgabelänge, Reasoning, Verlauf, Laufzeiten und Logging, soweit der Anbieter es unterstützt.

Wiederverwendung

Agents, Templates und gespeicherte Prompts bewahren bewährte Konfigurationen.



Settings. Nach Aufgabenbereichen gegliedert: Provider, Spracheingabe, Agents & Timer, Inhalte, Darstellung, Logging.



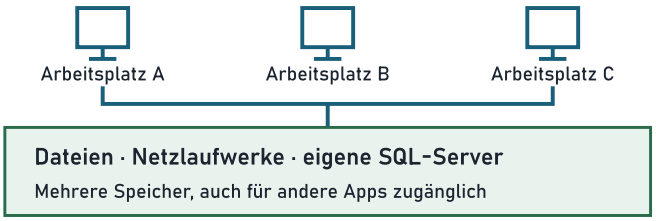
Tool-Auswahl. Read, Write, Manage und Execute je Tool; aktivierte und nicht freigegebene Tools direkt unterscheidbar.

05 / DATENSCHUTZ UND KONTROLLE

Datenschutz. Rechte. Unabhängigkeit.

Eigene Speicher, verschlüsselte Zugänge und kontrollierte Tools. In die Cloud geht nur der gesendete Kontext.

Bestände gemeinsam nutzen



Gemeinsam pflegen, wiederherstellen

Projekte, Agents und Skills mit Transaktionen und Änderungskontrolle. Import/Export, Kopieren, Desktop-Checkout und Papierkorb.

Inhalte bei Bedarf laden

SQL-Dateilisten laden zuerst Metadaten, Inhalte erst beim Zugriff. SQL Server implementiert; PostgreSQL und MariaDB vorgesehen, ohne Zusage.

Zugänge und Nachweise

API, SQL, IMAP, MCP: Zugänge bleiben verschlüsselt in eigenen Speichern; Entschlüsselung erst bei Nutzung auf dem PC.

Tool Call
Argumente, Ergebnis, Tokens, Laufzeit, HTTP-Logs

→

Eigene Logs
Session, App, append-only Audit mit Benutzer und Objekt

→

Auswerten
Ansehen, Kopieren, ZIP; optionale SQL-Replikation

Umfang und Darstellung des Loggings sind konfigurierbar; Aufbewahrung und Bereinigung bleiben eine bewusste Betriebsentscheidung.

Cloud, lokal oder ohne KI

Cloud-Modell

Anbieter nach Qualität, Preis und Datenschutz wählen. Die Ausführung bleibt lokal; gesendeter Kontext und Tool-Ergebnisse gehen an den Anbieter.

Lokales Modell

Ohne Anbieter-Key und Modellgebühr. Offlinefähig, wenn Modell, Daten und Tools lokal vorliegen; eigene Betriebskosten.

Ohne KI

Vorbereitete, geprüfte Skripte direkt unter Windows starten. Keine automatische Fortsetzung unterbrochener KI-Läufe.

Eigener Arbeitsplatz statt Cloud-Zugang

Bereich	Gehostete KI	AgentWorkDesk
Arbeitsplatz	Browser-Zugang	Windows-App
Daten	Anbieter-Cloud	Eigene Dateien und SQL
Modellwahl	Plattformangebot	Cloud oder lokal
Freigaben	Kontorichtlinien	Je Tool und Session
Zugänge	Kontogebundener Tresor	Verschlüsselt im eigenen Speicher
Audit	Plattformkonsole	Eigene Logs, ZIP / SQL

Typische gehostete Umgebung; einzelne Dienste weichen ab.

Bei Anbieterausfall wechseln

Anderen konfigurierten Anbieter oder lokales Modell wählen, ohne Datenumzug. Modellfähigkeiten, Tools und Ablauf vor Produktiveinsatz prüfen.

Verbindliche Zahlen aus Skripten

KI-Antworten sind nicht garantiert reproduzierbar. **KI entwirft, geprüftes Skript rechnet, Fachkraft gibt frei.** Prüfpflicht und Haftung bleiben.

DSGVO: Technische Grundlage, keine automatische Konformität. Gesendeter Kontext und Anbieterbedingungen bleiben bei Cloud-Modellen entscheidend.

06 / LEISTUNG UND KOSTEN

Lokal rechnen statt Rohdaten hochladen.

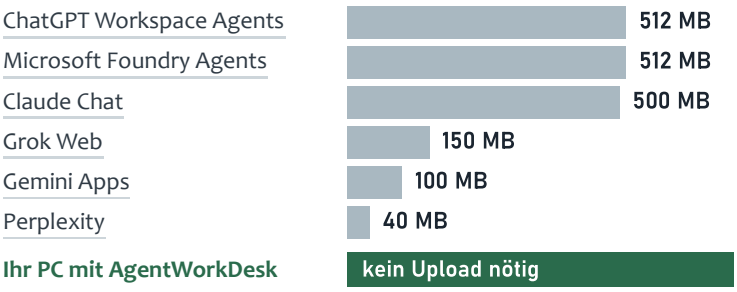
Drei Wege, dieselbe Auswertung

Beispiel: 100 MB Protokolldaten auswerten.

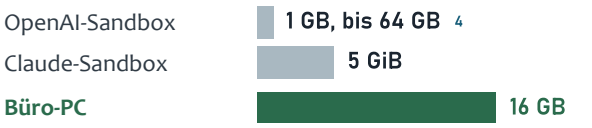
	Rohdaten im Prompt Chat ohne Skript	Cloud-Sandbox Skript beim KI-Anbieter	Ihr PC Lokal mit AgentWorkDesk
UPLOAD	**Ja** alle Rohdaten als Text	**Ja** Datei in den Container	**Nein** Daten bleiben am Speicherort
EINGABE-TOKENS	**rund 25 Mio.** durch Kontext begrenzt	**Skript und Ergebnis** Rohdaten zählen nicht	**Skript und Ergebnis** Rohdaten zählen nicht
GEBÜHR	**Modellabhängig** Tokenpreis des Anbieters	**0 bis 1,92 $** je 20-Min.-Sitzung, nach RAM und Anbieter[4]	**Keine Containergebühr** eigene Hardware, eigener Strom
GRENZEN	**Kontextfenster** größere Dateien passen nicht	**Sandbox** z. B. 1 CPU, 5 GiB RAM oder 30 s Laufzeit[1,3]	**Ihr PC** alle Kerne, RAM, SSD, Programme
ROHDATEN	**Beim Anbieter**	**Beim Anbieter** Anthropic: bis 30 Tage gespeichert[1]	**Bleiben bei Ihnen**

Skript und Ergebnis verursachen lokal ähnliche Tokenkosten wie in der Cloud-Sandbox. **Lokal entfallen Upload, Sitzungsgebühr und Sandbox-Grenzen.** Stückweise auswerten, nur Treffer und Summen ans Modell.

Uploadgrenze je Datei[2]



Arbeitsspeicher fürs Skript[1,3]



Zugriffszeit je Schritt



Typische Größenordnungen, keine garantierten Grenzen; kein Aufgaben-Benchmark.

Die KI ist austauschbar. Ihr Bestand bleibt.



Quellen 1 bis 4 auf Seite 13. Sandbox-Werte gelten für Anbieter-APIs und sind veränderlich; Tokenmenge mit rund 4 Zeichen je Token geschätzt. Hardware, Strom und Betrieb sind nicht kostenlos.

07 / ALTANLAGEN UND HARDWARE

Altanlagen wieder in den Griff bekommen.

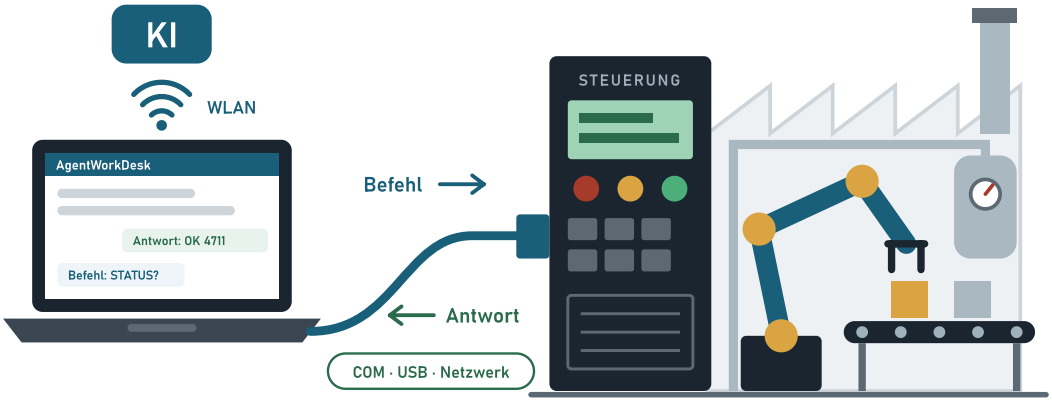
Steuerungen und Geräte sind unverzichtbar, aber oft unbetreut. AgentWorkDesk bringt die KI an den PC, an dem die Anlage hängt.

Unverzichtbar
Der Betrieb hängt an Steuerung, Prüfstand oder Messgerät.

Unbetreut
Hersteller nicht greifbar, Dokumentation lückenhaft.

Unverstanden
Wer das System kannte, ist nicht mehr im Haus.

Die KI arbeitet am PC der Anlage



Laptop mit AgentWorkDesk — Industrieanlage, seit Jahren ohne Betreuung

ERREICHBAR ÜBER WINDOWS: COM, RS-232, RS-485 · USB · Netzwerk (TCP/IP) · Registry · Dienste, Treiber · Dateien

Der Arbeitsablauf vor Ort

1 Lesen
Konfiguration, Registry, Dokumentation und alten Code auswerten.

2 Sprechen
Ein freigegebenes Skript öffnet die Schnittstelle und fragt das Gerät ab.

3 Programmieren
Die KI schreibt Hilfsprogramme für diese Hardware und dokumentiert.

4 Testen
Sofort am Gerät: Antwort lesen und korrigieren; Fachkraft prüft.

Ihr Nutzen

- **Wissen kommt zurück ins Haus:** dokumentiert und wiederverwendbar.
- **Kurze Wege:** schreiben, ausführen und Antwort lesen an einem Ort.
- **Lösung für den Einzelfall:** gebaut für Ihre Anlage; Skripte laufen später auch ohne KI.

Grenzen

- Freigaben begrenzen die Ausführung; Windows-Rechte gelten unverändert.
- Erreichbar ist, was Windows, Treiber und Schnittstellen bieten. Kein Echtzeit- oder Kernel-Zugriff.
- Eingriffe in Steuerungen prüft und verantwortet eine Fachkraft.

Analyse, Programmierung und Test direkt am PC der Anlage. Aus der Cloud allein geht das nicht.

Cloud-Sandboxen wie das Anthropic Code Execution Tool laufen ohne Internet und vom Host isoliert (Quelle 1, Stand 16.11.2026).

08 / TECHNISCHE ARCHITEKTUR

Klare Schichten, gemeinsame Fachlogik.

Oberfläche und KI-Tools nutzen dieselben fachlichen Operationen. Abhängigkeiten fließen nur in eine Richtung.

Anwendung
C# 14, .NET 10, WPF und DevExpress 26.1.3.

Agenten-Laufzeit
Microsoft Agent Framework, Extensions.AI und AgentFrameworkToolkit.

Speicher
FileSystem oder SQL Server inkl. Express über SqlClient.

Integrationen
ModelContextProtocol, MailKit für IMAP, NAudio für Sprache.

Schichten

Ui / Tools	Fenster, Chat-Ansicht, Tool-Schemas, Markdown-Ausgabe
▼	
Ops	Fachliche Abläufe, Validierung, Transfer, Laufsteuerung
▼	
Services	KI-Provider, Dokumente, IMAP, MCP, Prozesse, Sprache
Repository	Index, Ids und eindeutige Namen je Domain
▼	
Storage	FileSystem oder SQL Server über eine Schnittstelle

Chat, Session und Run

Chat
Dauerhafter Arbeitskontext mit Projekt, Stores, Anhängen, Todos und Sessions.

Session
Gespräch mit fester Konfiguration ab Anlage: Agent, Modell, Instructions, Skills, Tools. Status Idle, Running, WaitingForApproval, Cancelling oder Failed.

Run
Ein Durchlauf; Oberfläche, Timer und Session-Tools starten ihn über denselben Pfad mit denselben Freigaben.

Agent-Ebene
Liest nur die Laufanfrage, ruft den Provider und liefert den Stream zurück; ApiKey und Endpoint werden nie gespeichert.

Oberfläche

Hauptfenster
Jeder offene Chat als Tab mit dockbaren Bereichen für Chat, IMAP, Vorschau, Logs und Werkzeuge; Drag-and-drop mit dem Explorer in beide Richtungen.

Workbench-Kern
Zehn Verwaltungsfenster mit Liste, Suche, Favoriten und Editor; ungespeicherte Änderungen werden mit Speichern, Verwerfen oder Abbrechen aufgelöst.

Fehlergrenzen

Zentraler Einstieg
Jede Benutzeraktion mit Audit, Busy-Sperre und einheitlicher Meldung; fachliche Ablehnung als Warnung, unerwartete Fehler mit kopierbarem Stack.

Stabiler Betrieb
Die App beendet sich bei Fehlern nie selbst. Ein Store-Wechsel stoppt Runs, speichert Chats und baut die Dienste neu auf.

Vier getrennte Log-Kanäle

App-Log
Technik, Betrieb und vollständige Fehler; lokal.

Audit-Log
Benutzeraktionen mit Ergebnis und Dauer; lokal.

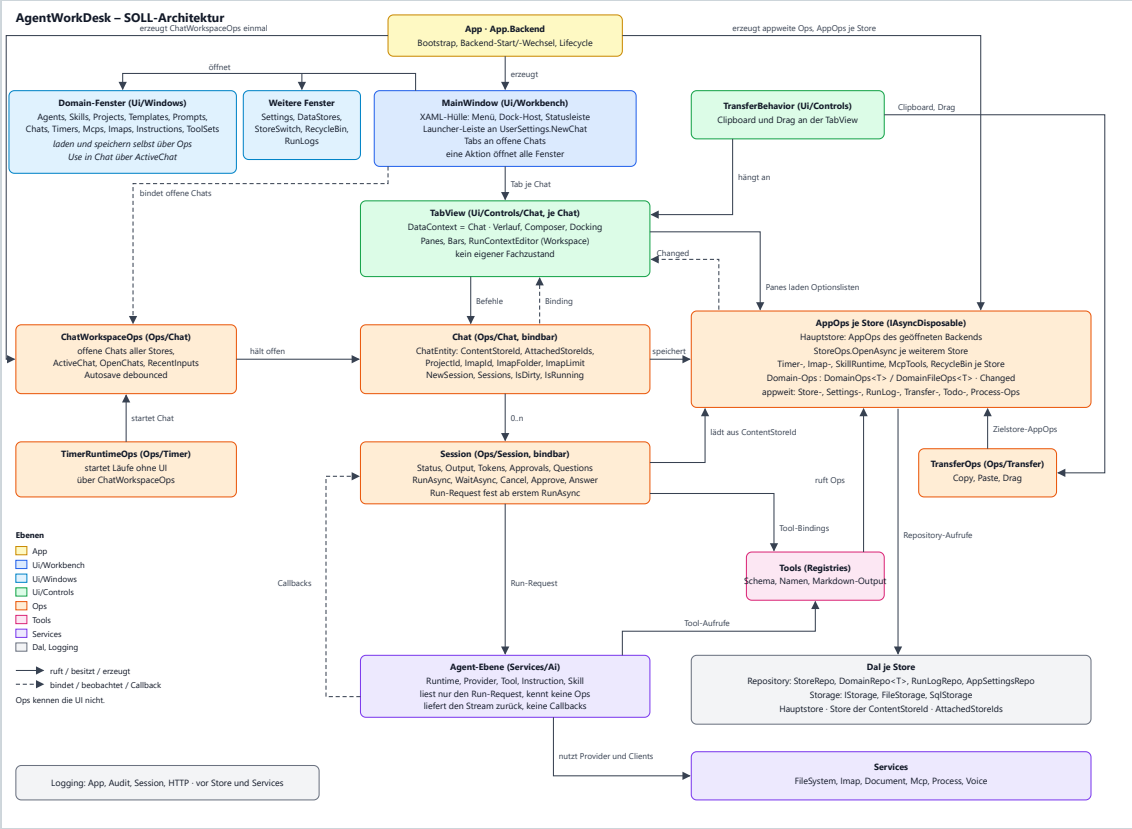
Session-Log
Nachrichten, Tools und Ergebnisse je Run; im Hauptstore.

HTTP-Log
Provider-Verkehr roh, gestreamt, Geheimnisse maskiert.

09 / DATEN, OWNER UND TOOLS

Ein Speichervertrag, klare Owner.

Owner, Aufrufe und Bindungen



Stores und Datenhaltung

Hauptstore

Genau einer ist geöffnet: Chats, Inhalte, App-Einstellungen und Run-Logs. Ein Chat liest Agents und Skills aus seinem Content-Store und Projekte aus weiteren angebundenen Stores.

Markdown und Originalformat

Fachobjekte als Markdown, Dateien im Original; je Domain ein Index mit Ids, Namen und Zeitstempeln. Benutzereinstellungen und Layouts bleiben lokal.

Transfer und Seed

Objekte zwischen Stores kopieren; Referenzen über Namen auflösen. Mitgelieferte Agents, Skills und MCPs beim ersten Start mit leerem Store.

```
Data/
├─ agents/, instructions/, templates/,
│  timers/, tool-sets/, mcps/, imaps/,
│  prompts/, chats/
│     index.md + entities/{Id}.md
├─ projects/, skills/
│     index.md + entities/{Id}/
│        project.md bzw. skill.md
│        files/
└─ run-logs/{yyyy-MM-dd}/
      {SessionId}_{RunId}.md

Speicher  FileSystem · SQL Server
Vertrag   ein IStorage für beide
Zugriff   Ui/Tool → Ops → Repo → Storage
```

Tool-Katalog

basic · work · control · automation · email · integrations · standard · agent · skill · project · session · instruction · timer · imap · mcp · provider · process · log · settings · store · toolset · todo · document

Standard-ToolSets Default und Domains; ToolSets ändern keine Sicherheitsstufe. Native Skill-Tools, Provider-Tools wie Websuche und Code-Interpreter sowie dynamische MCP-Tools ergänzen den Katalog. Jeder Aufruf läuft durch ein zentrales Gate mit Audit.

10 / ENTWICKLUNG, QUALITÄT UND GRENZEN

Professionell entwickelt, ehrlich begrenzt.

KI-gestützte Umsetzung unter Leitung eines Softwareentwicklers mit 33 Jahren Praxiserfahrung. Architektur, technische Entscheidungen und Qualität bleiben in Expertenhand.

Konzept zuerst

Ein Gesamtkonzept in neun Kapiteln beschreibt das Zielsystem; daraus abgeleitete Instructions je Bereich steuern die Umsetzung.

Genehmigte Pläne

Größere Änderungen laufen in Phasen mit Build-Prüfung und Commit je Phase.

Strenge Prüfungen

Analyzer-Warnungen sind Build-Fehler; Namen, Async, Collections, Dateigröße und Fehlerbehandlung werden per Build, ReSharper und Audit-Skripten geprüft.

Black-Box-UI-Test je Verwaltungsfenster

xUnit und FlaUI starten die gebaute App mit isoliertem Datenordner und bedienen sie ausschließlich über UI Automation.

1 Open
Fenster öffnen, Ausgangsanzahl erfassen.

2 Create
Neu anlegen; Anzahl plus eins.

3 Update
Namen ändern, speichern, Liste prüfen.

4 Read
Schließen, erneut öffnen, Eintrag vorhanden.

5 Copy
Duplizieren; Anzahl plus zwei.

6 Pending
Auswahlwechsel abbrechen; Entwurf bleibt.

7 Discard
Änderung verwerfen; gespeicherter Name.

8 Close
Beim Schließen verwerfen; Stand bleibt.

9 Delete
Beide löschen; Ausgangsanzahl erreicht.

Grenzen, klar benannt

- Technische Grundlage für DSGVO-konforme Abläufe, keine automatische Konformität.
- KI-Antworten sind nicht garantiert reproduzierbar; verbindliche Zahlen brauchen geprüfte Skripte.
- Tool-Freigaben ersetzen keine fachliche Prüfung; Verantwortung bleibt beim Anwender.
- Kein Echtzeit- oder Kernel-Zugriff; Eingriffe in Steuerungen verantwortet eine Fachkraft.

Betrieb

- Anbieterwechsel erfordert erneute Prüfung von Modellfähigkeiten, Tools und Ablauf.
- Timer starten nur bei laufender Anwendung.
- Lokaler Betrieb ist nicht kostenlos: Hardware, Strom und Betrieb bleiben.
- Preise, Limits und Verfügbarkeit der Anbieter können sich ändern.

Dauerhafte Chats, wiederverwendbare Spezialisten, eigene Daten, kontrollierte Tools und nachvollziehbare Ausführung in einer Windows-Anwendung.

11 / QUELLEN UND KONTAKT

Belege, Kosten und Geltungsbereich.

Externe Vergleichswerte aus Anbieterangaben, abgerufen am 16.11.2026; für diese Fassung nicht erneut extern verifiziert.

Kostenbeispiele

Cloud-Container

OpenAI: 0,03 US-Dollar bei 1 GB bis 1,92 US-Dollar bei 64 GB je 20-Minuten-Sitzung. Anthropic: 1.550 Freistunden pro Monat, danach 0,05 US-Dollar je Stunde. Modellgebühren kommen hinzu.

Tokenschätzung

25 Mio. Tokens für 100 MB Text bei rund vier Zeichen je Token; Kontextfenster beispielhaft 1 Mio. Tokens. Rechenbeispiele, keine Preis- oder Modellzusage.

Externe Quellen

[1] Anthropic, Code Execution Tool: Container, Aufbewahrung bis 30 Tage, 1 CPU, 5 GiB RAM, kein Internet, vom Host isoliert. Pricing: Laufzeit- und Modellkosten.

[2] Uploadgrenzen: ChatGPT Workspace Agents, Microsoft Foundry Agents, Claude, Grok, Gemini Apps (Videos bis 2 GB), Perplexity.

[3] Google, Gemini Code Execution: 30 s Laufzeit. OpenAI, Code Interpreter: 1 GB Standard. Büro-PC: Lenovo ThinkCentre M70t Gen 5 mit 4 Kernen, 16 GB RAM, 512 GB SSD; Beispiel, kein Mindeststandard.

[4] OpenAI Pricing: 0,03–1,92 $ je 20-Min.-Container (1–64 GB). Anthropic Pricing: 1.550 Freistunden/Monat, danach 0,05 $/h.

Grundlage und Abgrenzung

Zusammengeführt aus Product Overview DE v014, Technology and Benefits Guide DE v006, Local Performance DE v005, Legacy Hardware DE v001, AWD-Vorstand DE v016, Gesamtdokument DE v001 und dem technischen Gesamtkonzept.

Gehostete KI-Dienste unterscheiden sich in Modellen, Werkzeugen, Speicher, Freigaben und Audit. Verglichen wird der lokale Ausführungsansatz, nicht pauschal die Leistung aller Cloud-Produkte. Zugriffszeiten sind Größenordnungen einzelner Zugriffe, kein Aufgaben-Benchmark.

Professionelle KI. Für die Praxis.

Einfach per Drag-and-drop. Ihr PC. Ihre Regeln. Ihre Nachweise. · easyfirma.net

© 2026 Wolfgang Axamit · Ausschließliche Verwertungsrechte: EasyFirma GmbH & Co KG