

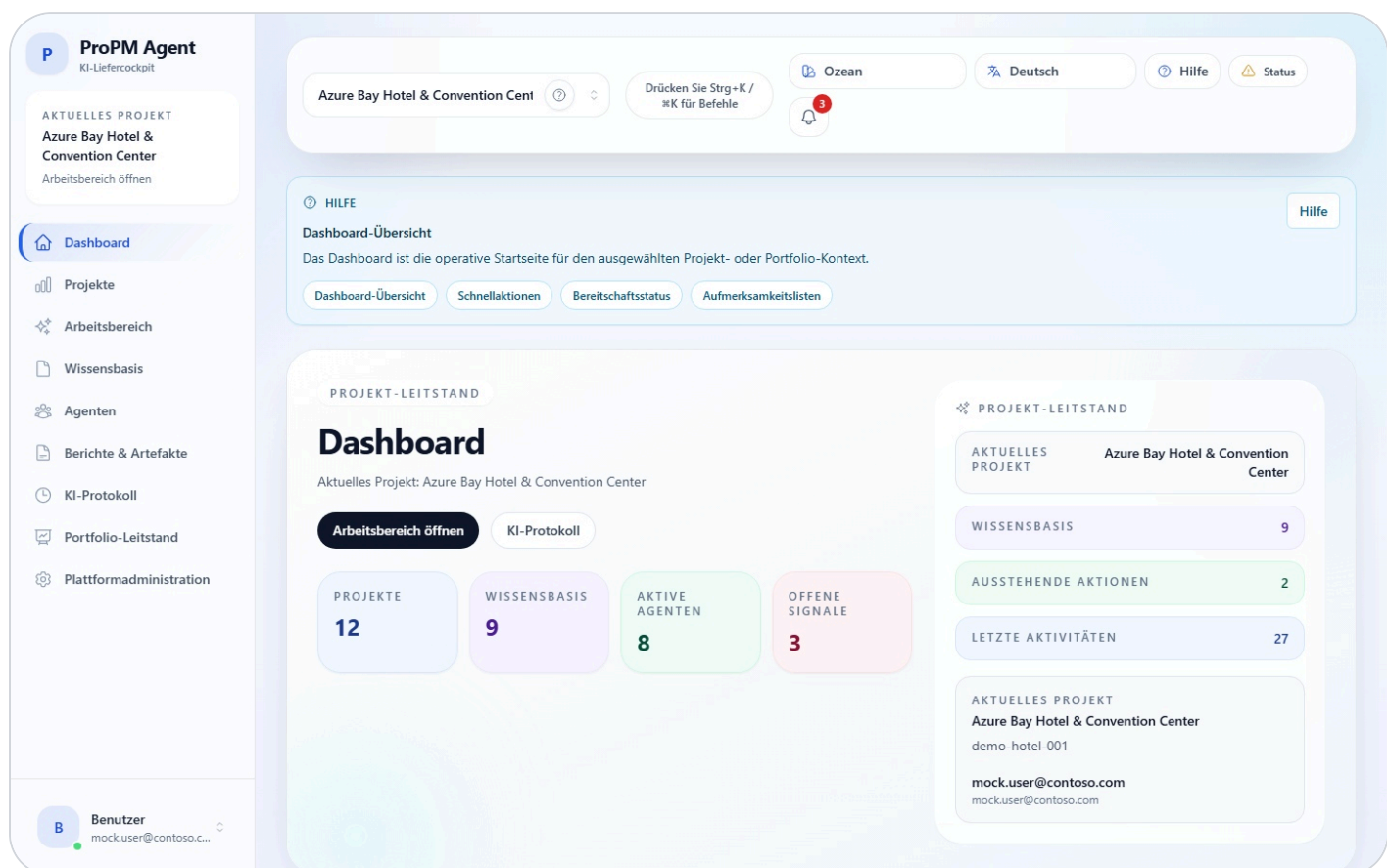
Benutzerhandbuch ProPM Agent

Lesen wird dringend empfohlen

Um die Einführung von ProPM Agent im Unternehmen erfolgreich zu gestalten und die Anwendung voll auszuschöpfen, wird dringend empfohlen, diesen Leitfaden bereits zu Beginn des Projekts zu lesen und während der Bereitstellung, der Einrichtung von Connectoren, der Governance und des täglichen Betriebs darauf zurückzugreifen.

Diese Dokumentation hilft Ihnen, ProPM Agent im Alltag zu nutzen: Navigation, Projekte, Wissen, Agenten, Governance, Berichte, Administration und Bereitstellung. Sie ist für zwei Zielgruppen strukturiert:

- **Geschäftsanwender**, die in einem Projekt arbeiten;
- **Technische Administratoren**, die Zugriff, Integrationen, den KI-Anbieter, das Abonnement und die Überwachung verwalten.



PDF exportieren

Deutsches PDF herunterladen

Ich suche die richtige Seite schnell

ANGETROFFENE SITUATION	ÖFFNEN SIE ZUERST	DANN
Ich kann mich nicht anmelden	Start	Wartung, Support und FAQ , um Tenant, redirect URI , Lizenzplatz oder Gesundheitszustand zu unterscheiden
Kein Projekt erscheint	Start	Projekte und Arbeitsbereich , dann Wartung, Support und FAQ , falls die Projektzuordnung oder Rolle unklar bleibt
Eine Seite bleibt leer, solange kein aktives Projekt definiert ist	Start	Projekte und Arbeitsbereich , um den Projektkontext zu bestätigen, dann Wartung, Support und FAQ , falls der leere Zustand weiter unnormal wirkt
Eine Aktion ist sichtbar, aber blockiert	Governance, Entscheidungen und Aktionen	Connectoren und Integrationen , dann KI-Anbieter und Plattformintegrationen für Connector, Binding, Konfiguration, Policy oder Health, oder Tenant-Plan, lizenzierte Benutzer und App-Updates für verfügbare verbleibende Lizenzen
Der KI-Anbieter scheint nicht funktionsfähig zu sein	KI-Anbieter und Plattformintegrationen	Wartung, Support und FAQ und Berichte, KI-Log und Nachvollziehbarkeit , um den tatsächlich verwendeten Anbieter zu bestätigen

Wenn Sie direkt nach einer Prüfprozedur oder einem Betriebshaken suchen, öffnen Sie [Wartung, Support und FAQ](#).

Empfohlener Leseweg

WENN SIE SUCHEN...	BEGINNEN SIE HIER
Eine neue Instanz in Azure bereitstellen	Azure Marketplace Deployment
Sich anmelden, die Authentifizierung prüfen und Ihr erstes Projekt erstellen	Start
Die Oberfläche, die Palette, Benachrichtigungen und den Gesundheitszustand verstehen	Oberfläche und Navigation
Den Projektkontext und die Einstellungen des Arbeitsbereichs verwalten	Projekte und Arbeitsbereich
Mitglieder, Rollen, Delegationen und RBAC-Grenzen des Projekts verwalten	Zugriffskontrolle und Projektrollen

WENN SIE SUCHEN...	BEGINNEN SIE HIER
Dokumente importieren, Beweise suchen und mit Agenten arbeiten	Wissen und Agenten
Eine strukturierte Ausgabe korrekt lesen, ihre Beweise und Frische prüfen	Strukturierte Ausgaben, Beweise und Frische
Signale, Governance und Aktionen mit Genehmigung verarbeiten	Governance, Entscheidungen und Aktionen
Ein Artefakt überprüfen, ein PM-Dokument veröffentlichen und im KI-Log nachforschen	Berichte, KI-Log und Nachvollziehbarkeit
Unterstützte Connectoren und Integrationen verstehen	Connectoren und Integrationen
Projekte vergleichen, Integrationen, KI und Lizenzen verwalten	Portfolio · KI-Anbieter und Plattformintegrationen · Tenant-Plan, lizenzierte Benutzer und App-Updates
Support- und Prüfverfahren konsultieren	Wartung, Support und FAQ
Produktthemen klären	Glossar

Schneller Weg nach Profil

PROFIL	PRIORITÄRE SEITEN
Geschäftsanwender / Mitwirkender	Start → Oberfläche und Navigation → Projekte und Arbeitsbereich → Wissen und Agenten → Strukturierte Ausgaben, Beweise und Frische
Projekthinhaber	Start → Projekte und Arbeitsbereich → Zugriffskontrolle und Projektrollen → Governance, Entscheidungen und Aktionen → Connectoren und Integrationen → Berichte, KI-Log und Nachvollziehbarkeit
Technischer Administrator	Azure Marketplace Deployment → Start → KI-Anbieter und Plattformintegrationen → Tenant-Plan, lizenzierte Benutzer und App-Updates → Wartung, Support und FAQ
Support / Audit	Start → Strukturierte Ausgaben, Beweise und Frische → Berichte, KI-Log und Nachvollziehbarkeit → Governance, Entscheidungen und Aktionen → Glossar

Empfohlener End-to-End-Weg

In einer realen Nutzung ist der häufigste Ablauf:

1. Die veröffentlichte URL bereitstellen oder abrufen;

2. Mit einem autorisierten Microsoft Entra ID-Konto anmelden;
3. Ein **aktives Projekt** erstellen oder auswählen;
4. Den **Projektersteller** die ersten nützlichen Rollen delegieren lassen;
5. Das **Wissen** des Projekts laden;
6. Einen Austausch in **Agenten** starten;
7. Die **strukturierte Ausgabe**, ihre Beweise, Frische und Vertrauenswürdigkeit erneut prüfen;
8. Das Ergebnis in ein **Artefakt** oder ein **PM-Dokument** umwandeln, dann vor dem Download als **DOCX / XLSX**, Veröffentlichung oder Hinzufügen zum Wissen überprüfen;
9. **Proaktive Signale, Aktionen & Genehmigungen** und bei Bedarf externe Integrationsflüsse verarbeiten;
0. Auf Plattformebene verwalten, wenn das Thema das Projekt übersteigt.

Beschriftungskonvention

Wenn die Plattform eine passende deutsche Beschriftung bereitstellt, bevorzugt diese Dokumentation diese Form:

- **Arbeitsbereich;**
- **Wissen;**
- **PM-Dokumente;**
- **KI-Log;**
- **Zugriffskontrolle;**
- **Governance-Richtlinien;**
- **Projektintegrationen;**
- **Plattformintegrationen;**
- **Einstellungen des KI-Anbieters;**
- **Aktionen & Genehmigungen.**

Wenn ein englischer Begriff zur Auflösung einer Mehrdeutigkeit nützlich ist, wird er gelegentlich in Code gesetzt, z. B. `Trace ID` oder `OpenAI-compatible`.

Was ProPM Agent abdeckt

Basierend auf den überprüften Verhaltensweisen organisiert ProPM Agent die Arbeit um den **Projektkontext**:

1. Sie öffnen oder erstellen ein Projekt;

2. Sie füttern das **Wissen**;
3. Sie fragen die **Agenten** ab;
4. Sie lesen die **strukturierte Ausgabe** erneut;
5. Sie wandeln diese Ergebnisse in **PM-Dokumente** und Artefakte um;
6. Sie prüfen die **Nachvollziehbarkeit** im **KI-Log**;
7. Sie verarbeiten **Signale, Digests, Entwürfe** und **governance-gesteuerte Aktionen**;
8. Sie nutzen **Connectoren** und **Integrationen** nur, wenn sie validiert und an das Projekt gebunden sind;
9. Administratoren steuern die technische Schicht in **Plattformadministration**.

Funktionsarchitektur

BEREICH	WAS ES ERMÖGLICHT
Dashboard	Den allgemeinen Zustand, Metriken, Aufmerksamkeitspunkte und nächste Schritte anzeigen
Projekte	Projekte erstellen, öffnen und den Projektkontext speichern
Arbeitsbereich	Projektzusammenfassung, operative Transparenz, Signale, Shortcuts und Projekt-Einstellungen bündeln
Zugriffskontrolle	Mitglieder, Standardrollen, benutzerdefinierte Rollen und Projektberechtigungen verwalten
Wissen	Nachschlagen, hochladen, importieren, Metadaten lesen und Ingestionsverlauf verfolgen
Agenten	Einen Agenten auswählen, einen Austausch starten, Sprachaufnahme in Agenten nutzen, falls die Umgebung dies noch unterstützt, und benutzerdefinierte Agenten je nach Berechtigung verwalten
Strukturierte Ausgaben	Zusammenfassung, Beweise, Frische, Vertrauen, Artefaktvorschläge und weitere Schritte lesen
PM-Dokumente / Berichte & Artefakte	Überprüfen, vergleichen, genehmigen, veröffentlichen, herunterladen und Liefergegenstände wieder in das Wissen einfügen
KI-Log	Läufe, Aktivitäten, technische IDs und Transparenz der KI-Laufzeit untersuchen
Connectoren und Integrationen	Plattformdefinitionen, Projektbindungen, Aktionsrichtlinien und governance-gesteuerte Ausführung trennen

BEREICH	WAS ES ERMÖGLICHT
Portfolio-Befehlszentrale	Mehrere Projekte mit Signalen, Gewichtungen, Schwellenwerten und gespeicherten Kohorten vergleichen
Plattformadministration	Integrationen, KI-Anbieter, Abonnement, Lizenzplätze und Plattformaktivität verwalten

Was die Anwendung unterscheidet

Folgende Elemente sind explizit in der Oberfläche, den Seed-Daten oder den Tests sichtbar:

- **strukturierte Ausgaben** mit Abschnitten, Beweisen, Frische, Vertrauen und zu treffenden Entscheidungen;
- **Lineage / Nachvollziehbarkeitskette** zwischen einem Run, einer strukturierten Ausgabe, einem Artefakt, einer Artefaktversion und einem PM-Dokument;
- **proaktive Signale** für Widersprüche, Frische, Blockierungen, Nachverfolgungen und bestimmte Portfolioprasse;
- **governance-gesteuerte Dokumentenketten** von einem Agenten-Ergebnis zu den Downloads **DOCX / XLSX**, zur Veröffentlichung und zur erneuten Einfügung in das Wissen;
- **governance-gesteuerte Connectoren** getrennt zwischen **Plattformintegrationen, Projektintegrationen** und **Aktionen & Genehmigungen**;
- **Transparenz der KI-Laufzeit** mit tatsächlich verwendetem Anbieter, beim Deployment ausgewähltem Anbieter und Modellfamilie.

Zielgruppen und Verantwortlichkeiten

PROFIL	HAUPTBEDÜRFNISSE
Projektleiter / PMO	Projektkontext, Agenten, Liefergegenstände, Signale, Governance und Nachvollziehbarkeit
Mitwirkender	Wissen durchsuchen, Inhalte generieren, Ausgaben prüfen und Läufe verfolgen
Projekthinhaber	Projektparameter, Rollendelegation, Dokumentkategorien, Projektintegrationen und Governance-Richtlinien

PROFIL	HAUPTBEDÜRFNISSE
Technischer Administrator / Abonnement	Bereitstellung, Authentifizierung, Plattformintegrationen, KI-Anbieter, Abonnement, Lizenzplätze und Überwachung

Screenshots und Diagramme

Screenshots und Diagramme dienen als visuelle Orientierung. Sie zeigen die wichtigsten Bildschirme und können je nach Daten, Berechtigungen und Umgebungskonfiguration leicht variieren.

Demo-Inhalte können zudem je nach Umgebung variieren: Manche Projekte zeigen nicht immer dieselben Seed-Dokumente, Seed-Berichte oder Beispielinhalte wie in der Dokumentation.

Was lokal im Browser bleibt und was geteilt ist

Im Produkt existieren zwei Logiken nebeneinander:

- einige Komfortfunktionen, etwa das gemerkte aktuelle Projekt oder die gespeicherte Chat-Kontinuität, bleiben lokal im Browser;
- Projektdaten, Dokumente, Artefakte, Genehmigungen und Veröffentlichungen gehören zum gemeinsamen Plattformzustand.

Ein in einem Browser sichtbarer Chatverlauf ist daher kein zentrales Archiv, das automatisch mit allen Benutzern geteilt wird.

Support und Kontakt

Verwenden Sie den richtigen Kanal je nach Art der Anfrage:

ANFRAGETYP	PRIORITÄT
Technischer Support	URL der Bereitstellung, betroffenes Projekt, angetroffene Situation, ungefähre Uhrzeit, Trace ID falls sichtbar
Zugangs-, Tenant- oder Identitätsfrage	Erwarteter Tenant, verwendetes Konto, tatsächlich geöffnete URL, Microsoft-Nachricht oder Screenshot
Kommerzielle oder Abonnementfrage	Kontokontext, aktueller Plan, bestellte Sitze, Zusatzlizenzen, genutzte Sitze und Lizenzbedarf

Alle diese Anfragen können an den folgenden Kontakt gesendet werden:

- **NovaBiz**
- 131 Continental Dr, Suite 305
- Newark, DE 19713 · USA
- support@navabiz.pro

Weiter

- [Start](#)
- [Projekte und Arbeitsbereich](#)
- [Connectoren und Integrationen](#)
- [Glossar](#)

Start

Startseite · Start

ProPM Agent
KI-Liefercockpit

AKTUELLES PROJEKT
Alle Projekte
Projekt auswählen

Dashboard
Projekte
Arbeitsbereich
Wissensbasis
Agenten
Berichte & Artefakte
KI-Protokoll
Portfolio-Leitstand
Plattformadministration

Benutzer
mockuser@contoso.c...

Alle Projekte

Drücken Sie Strg+K / ⌘K für Befehle

Ozean

Deutsch

Hilfe

Status

Projekte
Projektarbeitsbereiche durchsuchen und verwalten.

Standard-Demoprojekte installiert + Projekt erstellen

HILFE

Projektverzeichnis

Die Projektseite listet alle zugänglichen Projekte auf und erlaubt das erneute Öffnen im Arbeitsbereich.

Projektverzeichnis Projektformular Project ID Project name Project description Demo-Projektimport

Suchen...

Zuletzt verwendet

Ansicht speichern

Exportieren

NAME	ERSTELLER	MEINE ROLLE	STATUS	ERSTELLT	AKTIONEN
Azure Bay Hotel & Convention Center demo-hotel-001 Demo construction program: 220-room upscale hotel, conference center, and wellness facilities in Tunis. Standard-Demoprojekt	Michael Carter michael.carter@NovaBizLLC.onmicrosoft.com	Project Admin	active	21/04/2026 15:08:08	Arbeitsbereich Demo löschen
North Delta Gas Compression & Export Upgrade demo-energy-001 Demo oil & gas capital program: brownfield compression upgrade, shutdown execution, and export reliability improvements. Standard-Demoprojekt	Jennifer Walker jennifer.walker@NovaBizLLC.onmicrosoft.com	Project Admin	active	20/04/2026 15:08:08	Arbeitsbereich Demo löschen

Ziel

Diese Seite erklärt, wie Sie den Zugriff auf ProPM Agent vorbereiten, die erste Anmeldung erfolgreich durchführen, das richtige Projekt auswählen und die unverzichtbaren technischen Punkte unmittelbar nach einer Bereitstellung prüfen.

Wer kann diese Seite nutzen

- **Geschäftsanwender**, der eine URL erhält und sich ohne umfangreiche Unterstützung anmelden muss;
- **Projekthinhaber**, der den ersten Projektkontext erstellen oder auswählen muss;
- **Technischer Administrator**, der die Authentifizierung, die Laufzeit und den ersten Zugriff validieren muss.

Wenn Sie noch keine Anwendungs-URL haben

Wenn Ihre Instanz noch nicht bereitgestellt wurde, beginnen Sie mit [Azure Marketplace-Bereitstellung](#). Dieser Schritt ermöglicht es, die Web-URL, die API und die erforderlichen Laufzeitparameter vor jeder Benutzeranmeldung zu erhalten.

Vor dem Start

Voraussetzungen für den Benutzer

Für die normale Nutzung benötigen Sie:

- die **URL der Bereitstellung** von ProPM Agent;
- ein **Microsoft Entra ID-Konto**, das im betreffenden Mandanten autorisiert ist;
- Zugriff auf mindestens ein Projekt oder das Recht, ein Projekt zu erstellen;
- einen modernen Browser, der aktuelle Web-Anwendungen unterstützt;
- wenn Sie Sprache nutzen, einen Browser, der die Spracherkennungs-APIs unterstützt.

Voraussetzungen für den technischen Administrator

Die folgenden Elemente müssen korrekt konfiguriert sein:

ELEMENT	ROLLE
<code>clientId</code>	Identifiziert die Entra-Anwendung, die im Web verwendet wird
<code>authority</code>	Legt die Microsoft Entra-Authentifizierungs-Authority fest
<code>scopes</code>	Definiert die bei der Authentifizierung angeforderten Berechtigungen
<code>redirectUri</code> und <code>postLogoutRedirectUri</code>	Steuern die Rückkehr nach Anmeldung und Abmeldung
<code>allowedTenantId</code>	Beschränkt, falls konfiguriert, den autorisierten Mandanten
<code>/runtime-config.json</code>	Dynamisches Überschreiben von URLs und Authentifizierungsparametern zur Laufzeit
API-URL	Ermöglicht der Web-Oberfläche, die Plattform-Services zu erreichen

ELEMENT	ROLLE
Abonnement / Sitzplätze	Bedingt den Zugriff in Bereitstellungen, die eine Lizenz pro Benutzer erzwingen

Erstanmelde-Pfad

1. Öffnen Sie die veröffentlichte URL Ihrer Bereitstellung;
2. Lassen Sie die Anwendung Sie zur Microsoft-Anmeldeseite umleiten;
3. Melden Sie sich mit dem autorisierten Konto an;
4. Kehren Sie zur Anwendung zurück, in der Regel zum **Dashboard**;
5. Prüfen Sie die Interface-Sprache, das aktuelle Projekt und eventuelle sichtbare Nachrichten in der oberen Leiste;
6. Öffnen Sie **Projekte**, um Ihr erstes Projekt auszuwählen oder zu erstellen.

Erste Anmeldung in 5 Minuten

Für einen sehr einfachen ersten Ablauf gehen Sie in dieser Reihenfolge vor:

1. melden Sie sich an;
2. bestätigen Sie das **aktive Projekt** in der oberen Leiste oder öffnen Sie **Projekte**;
3. erstellen oder öffnen Sie ein Projekt;
4. öffnen Sie **Agenten**, um eine erste einfache Frage zu stellen, zum Beispiel zu Status oder Prioritätsrisiko;
5. lesen Sie die **strukturierte Ausgabe**;
6. öffnen Sie danach **KI-Journal**, wenn Sie die Run-Spur wiederfinden müssen, oder **Berichte & Artefakte**, wenn Sie das Ergebnis in ein gesteuertes Dokument umwandeln möchten.

Dieser Ablauf genügt, um die Kernlogik der Anwendung zu verstehen, ohne zuerst alle Administrationsoberflächen zu öffnen.

Zu kennende Zugriffs-Zustände

In der Oberfläche gibt es zwei Zustände:

- **Nur-Lesen**: Sie können eine Oberfläche ansehen, aber nicht ihre Einstellungen ändern;
- **Zugriff verweigert**: Die Route oder Aktion ist für Ihr Konto nicht verfügbar.

Diese Unterscheidung ist wichtig für Verwaltungsbereiche: Manchmal kann eine technische Seite nur zur Ansicht geöffnet werden, ohne Änderungen speichern zu können.

Erwartetes Ergebnis nach der ersten Anmeldung

Wenn alles korrekt konfiguriert ist, sollten Sie:

- das **Dashboard** in guten Bedingungen erreichen;
- **Projekte** öffnen;
- ein Projekt auswählen oder erstellen;
- anschließend auf **Arbeitsbereich, Wissen, Agenten, Berichte & Artefakte** und **KI-Journal** je nach Ihren Rechten zugreifen.

Erstes Projekt erstellen

Das Anwendungsformular bietet die folgenden Felder:

- **Projekt-ID;**
- **Name;**
- **Beschreibung;**
- **Standard-Datensprache;**
- **Zusätzliche Datensprachen.**

Projekt erstellen

Jeder authentifizierte Benutzer kann ein Projekt erstellen. Der Ersteller wird zum primären Administrator des Projekts.

Projekt-ID ⓘ

proj-011

Verwenden Sie Kleinbuchstaben, Zahlen und Bindestriche. Lassen Sie das Feld leer, damit ProPM Agent eine lesbare Projekt-ID erzeugen kann.

Name ⓘ

Beschreibung ⓘ

Default data language

English ▼

This controls seeded document categories, default agent prompts, and other project data defaults. It does not change the app language.

Additional data languages

☒ English Default	☐ Français
☐ Deutsch	☐ Español
☐ हिन्दी	

Additional languages stay available for project data when you explicitly ask agents to

Abbrechen Erstellen

Wichtiger Punkt

Die **Datensprache des Projekts** ist nicht dasselbe wie die **Interface-Sprache**.

Die Datensprache beeinflusst insbesondere:

- die standardmäßig vorgeschlagenen Dokumentkategorien;
- bestimmte Agenten-System-Prompts;

- die projektspezifischen Anfangswerte.

Wenn kein Projekt angezeigt wird

Mehrere Bildschirme zeigen einen expliziten leeren Zustand, wenn kein Projekt ausgewählt ist. Das ist normal.

Um fortzufahren:

1. Verwenden Sie den **Projekt-Auswahl-Filter** in der oberen Leiste;
2. Öffnen Sie **Projekte**, um ein zugängliches Projekt auszuwählen;
3. Wenn Sie Erstellungsrechte haben, erstellen Sie ein Projekt;
4. Wenn die Liste weiterhin leer bleibt, prüfen Sie mit Ihrem Administrator, ob Ihr Konto dem richtigen Projekt hinzugefügt wurde.

Checkliste nach der Bereitstellung für den technischen Administrator

Nach einer neuen Bereitstellung prüfen Sie mindestens:

1. die tatsächlich veröffentlichte **Web-URL**;
2. die Verfügbarkeit der Datei `/runtime-config.json` ;
3. die Konsistenz zwischen der veröffentlichten URL und den in Entra konfigurierten **Redirect-URLs**;
4. das Vorhandensein eines gültigen **client ID**;
5. den korrekten Wert von **authority** und, falls verwendet, von **allowedTenantId**;
6. die erwarteten **scopes** für Frontend und API;
7. die **API-URL**;
8. den Verbrauch oder die Verfügbarkeit von **Sitzplätzen**, falls der Plan dies verlangt;
9. einen ersten Verbindungstest mit einem Standard-Benutzerkonto und einem Administratorkonto.

Häufige Prüfungen bei der ersten Anmeldung

Der Microsoft-Account authentifiziert sich, aber der Zugriff funktioniert noch nicht wie erwartet

Prüfen Sie in dieser Reihenfolge:

1. den **Mandanten**, der während der Anmeldung verwendet wird;
2. ob das Konto im Mandanten autorisiert ist;
3. die Verfügbarkeit eines **Sitzplatzes**, falls der Plan eine Lizenz pro Benutzer verlangt;
4. die Existenz mindestens eines zugänglichen Projekts für dieses Konto.

Mandanten- oder externes / Gast-Konto

Wenn Microsoft angibt, dass Ihr Konto im Ziel-Mandanten nicht existiert, bedeutet dies in der Regel, dass es als **externer / Gast-Benutzer** in den Mandanten eingeladen werden muss, der die Anwendung hostet, und dann auf die Unternehmens-Anwendung oder über eine Gruppe autorisiert werden muss.

redirect URI mismatch

Wenn die Anmeldung einen Weiterleitungsfehler zurückgibt, vergleichen Sie die tatsächlich veröffentlichte URL mit den **Redirect-URIs** der Entra-Anwendungs-Registrierung. Jede veröffentlichte Umgebung muss exakt gelistet sein, ohne Tippfehler.

unauthorized_client oder Entra-Anwendung im falschen Mandanten

Dieses Symptom weist in der Regel darauf hin, dass die Anwendungs-Registrierung nicht im richtigen Mandanten liegt oder die Bereitstellung eine inkompatible Authority für eine **single-tenant**-Anwendung nutzt.

Erfolgreicher Zugriff, aber Admin-Ansicht im Nur-Lesen-Modus

Das bedeutet häufig, dass das Konto authentifiziert ist, aber nicht als modifizierbarer Plattform-Administrator aufgelöst wurde. Prüfen Sie die Admin-Gruppen, den Token-Mandanten und die von Ihrer Umgebung verwendete Admin-Auflösungsmethode.

Anmeldung OK, Dashboard geladen, aber zusätzliche Prüfung sinnvoll

Dieses Szenario weist oft darauf hin, dass die Authentifizierung erfolgreich war, aber eine zusätzliche Prüfung der Laufzeit oder Konnektivität sinnvoll ist. Öffnen Sie den **Gesundheitsindikator**, notieren Sie den Zustand **API**, **auth**, die **Latenz** und das

aktuelle Projekt, dann fahren Sie mit [Benutzeroberfläche und Navigation](#) fort, um das Panel zu lesen, und mit [Wartung, Support und FAQ](#) für Prüfpunkte.

Schnelle Referenzen - zu bestätigender Zugriff

AUSGANGSSITUATION	ZUERST PRÜFEN	DANN
Microsoft gibt einen Fehler vor der Rückkehr in die Anwendung	authority , verwendeter Mandant, clientId , redirectUri , postLogoutRedirectUri , allowedTenantId	Vergleichen Sie die Laufzeit-Konfiguration und die Entra-Registrierung, dann führen Sie einen Test mit dem richtigen Konto durch
Microsoft-Anmeldung funktioniert, aber die Anwendung bleibt blockiert	Verfügbarkeit eines Sitzplatzes , Gesundheitsindikator, API-URL	Prüfen Sie anschließend den Zugriff auf ein Projekt und die tatsächlichen Rechte des Kontos
Anmeldung funktioniert, Dashboard lädt, aber Verfügbarkeit prüfen empfohlen	Zustände auth , API , Latenz und aktives Projekt	Öffnen Sie Benutzeroberfläche und Navigation , dann Wartung, Support und FAQ , um Auth, Laufzeit und Projektkontext zu unterscheiden
Anwendung öffnet sich, aber kein Projekt erscheint	Projekt-Auswahl-Filter, Liste Projekte , Projektzugehörigkeit, Erstellungsrecht	Bitten Sie den Projekthinhaber , das Konto bei Bedarf dem richtigen Projekt hinzuzufügen
Eine Seite ist sichtbar, aber nicht bearbeitbar	Projekt-Rolle oder Admin-Rolle, Zustand Nur-Lesen vs Zugriff verweigert	Prüfen Sie anschließend die Admin-Gruppe oder die betreffenden Projekt-Berechtigungen

Situation, zu erfassende Elemente und nächste Seite

ANGETROFFENE SITUATION	ZU ERFASSENDE ELEMENTE	NÄCHSTE ZU ÖFFNENDE SEITE
Microsoft-Fehler vor Rückkehr in die Anwendung	genaue Fehlermeldung, Screenshot, verwendetes Konto, tatsächlich geöffnete URL	Start , dann Wartung, Support und FAQ , falls Zweifel bestehen
Dashboard geladen, aber Verfügbarkeit prüfen sinnvoll	Zustände API , realtime , auth , Latenz, Testzeit, aktuelles Projekt	Benutzeroberfläche und Navigation , dann Wartung, Support und FAQ

ANGETROFFENE SITUATION	ZU ERFASSENDE ELEMENTE	NÄCHSTE ZU ÖFFNENDE SEITE
Kein Projekt sichtbar	Screenshot des Projekt-Auswahl-Filters, E-Mail des Kontos, erwartetes Projekt	Projekte und Arbeitsbereich
Seite sichtbar, aber Kontrollen ausgegraut	Seitennamen, erwartete Rolle, Screenshot der deaktivierten Buttons	Zugriffskontrolle und Projekt-Rollen oder Portefeuille und technische Administration je nach Oberfläche
Anmeldung OK, aber Runs starten nicht	Trace ID falls vorhanden, aktives Projekt, Gesundheitsindikator, erwarteter KI-Provider	Wartung, Support und FAQ , dann Berichte, KI-Journal und Nachverfolgbarkeit

Für eine Situation, die Authentifizierung, Laufzeit, Projekt, Sitzplatz oder KI-Provider mischt, nutzen Sie anschließend [Wartung, Support und FAQ](#) als übergreifende Prüfpunkte.

Gute Praktiken von Anfang an

- wählen Sie das richtige Projekt **vor** das Starten von Agenten;
- definieren Sie die Datensprache des Projekts korrekt bei der Erstellung;
- prüfen Sie Ihr Rechte-Level, bevor Sie Governance oder technische Administration ändern;
- wenn Ihre Bereitstellung ein Sitzplatzmodell nutzt, vergewissern Sie sich, dass Ihr Zugriff ordnungsgemäß zugewiesen wurde;
- behalten Sie die Bereitstellungs-URL und, falls nötig, die angezeigte **Trace ID** für den Support.

Weiter

- [Azure Marketplace-Bereitstellung](#)
- [Benutzeroberfläche und Navigation](#)
- [Projekte und Arbeitsbereich](#)
- [Wartung, Support und FAQ](#)

Azure Marketplace-Bereitstellung

[Startseite](#) · Azure Marketplace-Bereitstellung

Ziel

Diese Seite beschreibt die Bereitstellung von **ProPM Agent** aus **Azure Marketplace**. Sie erklärt die beiden wichtigsten Azure-Formularseiten, den Zweck jedes sichtbaren Felds und die Prüfungen vor **Review + create**.

Die Screenshots zeigen das Formular **Create ProPM-50**. Der angezeigte Name kann je nach ausgewähltem Marketplace-Plan abweichen, zum Beispiel ProPM-50, ProPM-100 oder ein anderer verfügbarer Plan.

Zielgruppe

PROFIL	NUTZUNG DIESER SEITE
Azure-Administrator	Managed Application aus Azure Marketplace erstellen
Tenant-Administrator	Entra-Gruppen und ersten Administratorzugriff vorbereiten
Plattformadministrator	Verstehen, welche Einstellungen nach der Installation abzuschließen sind
Support	Ablauf prüfen, ohne Secrets oder interne Variablen anzufordern
Fachlicher Benutzer	Nein, dafür Erste Schritte verwenden

Vor dem Start

Bereiten Sie diese Informationen vor, bevor Sie das Marketplace-Formular öffnen.

INFORMATION	WARUM SIE BENÖTIGT WIRD
Ziel-Azure-Abonnement	Trägt die Marketplace-Transaktion und die bereitgestellten Ressourcen
Ziel-Ressourcengruppe	Organisiert das kundenseitige Managed-Application-Objekt
Ziel-Azure-Region	Definiert den primären Bereitstellungsort
Anwendungsname	Identifiziert die ProPM-Agent-Instanz in Azure

INFORMATION	WARUM SIE BENÖTIGT WIRD
Managed Resource Group	Nimmt die internen, von der Anwendung verwalteten Ressourcen auf
Entra Group Object IDs	Gewähren Zugriff auf die Plattformadministration
Optionale Bootstrap-Benutzer	Helfen beim ersten Zugriff oder bei kontrollierter Wiederherstellung
Initialer KI-Anbieter	Gibt die KI-Anbieterfamilie an, die für diese Instanz vorbereitet wird
Optionale CORS Origins	Erlauben zusätzliche Web-Domains, falls erforderlich
VNet-CIDR-Plan	Verhindert Konflikte mit dem Organisationsnetzwerk
Initiales Passwort	Muss generiert und als Secret gespeichert werden

Kopieren Sie niemals Passwort, Secret, API-Schlüssel, Token oder vertrauliche Werte in die Dokumentation oder in eine ungesicherte Support-Anfrage.

Bereitstellungsablauf

1. Öffnen Sie das ProPM-Agent-Angebot in Azure Marketplace.
2. Wählen Sie den gewünschten Marketplace-Plan.
3. Füllen Sie den Tab **Basics** aus.
4. Wählen Sie **Next**.
5. Füllen Sie den Tab **Application Settings** aus.
6. Wählen Sie **Review + create**.
7. Beheben Sie mögliche Validierungsfehler.
8. Starten Sie die Erstellung.
9. Warten Sie, bis die Azure-Bereitstellung abgeschlossen ist.
0. Öffnen Sie die veröffentlichte URL und schließen Sie die Administration in ProPM Agent ab.

Bildschirm 1 - Basics

Der Tab **Basics** definiert den Azure-Bereich der Bereitstellung: Abonnement, Ressourcengruppe, Region und Azure-Namen der Managed Application.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

AmineSMAOUI@NovaBi...
NOVABIZ LLC (NOVABIZLLC.ONL...)

Home > ProPM Agent

Create ProPM-50

BasicsApplication SettingsReview + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘMicrosoft Azure Sponsorship (39d01e96-f8d1-47a4-9adf-c6e6715fa... ⓘ

Resource group * ⓘgroupress11 ⓘ
[Create new](#)

Instance details

Region * ⓘ(US) East US ⓘ

Managed Application Details

Provide a name for your managed application, and its managed resource group. Your application's managed resource group holds all the resources that are required by the managed application which the consumer has limited access to.

Application Name * ⓘ

Managed Resource Group * ⓘmrg-propm-agentx-20260525113909 ⓘ

PreviousNextReview + create

[Give feedback](#)

Felder im Tab Basics

FELD	PFLICHTFELD	EINGABE	AUSWIRKUNGEN UND EMPFEHLUNGEN
Subscription	Ja	Das Azure-Abonnement, das die Managed Application und Marketplace-Abrechnung trägt.	Verwenden Sie ein Abonnement, in dem Sie eine Managed Application bereitstellen und Ressourcengruppen erstellen oder auswählen dürfen. Prüfen Sie auch interne Kosten- und Governance-Regeln.
Resource group	Ja	Die kundenseitige Ressourcengruppe, die das Managed-Application-Objekt enthält.	Wählen Sie eine vorhandene Gruppe oder Create new . Dies ist nicht die interne Managed Resource Group mit den technischen ProPM-Agent-Ressourcen.
Create new	Nein	Azure-Aktion zum Erstellen einer neuen Ressourcengruppe, wenn keine passende Gruppe existiert.	Verwenden Sie einen klaren Namen mit Bezug auf Umgebung und Region. Vermeiden Sie temporäre Namen für produktive Instanzen.
Region	Ja	Die primäre Azure-Region der Bereitstellung.	Wählen Sie eine von Ihrer Organisation zugelassene Region, nahe an den Benutzern und passend zu Datenresidenz-Anforderungen. Halten Sie sie konsistent mit geplanten Netzwerk- und KI-Ressourcen.

FELD	PFLICHTFELD	EINGABE	AUSWIRKUNGEN UND EMPFEHLUNGEN
Application Name	Ja	Der sichtbare Name der ProPM-Agent-Managed-Application-Instanz.	Verwenden Sie einen stabilen, lesbaren Namen wie <code>propm-prod-eus</code> . Der Name hilft beim Erkennen der Instanz in Azure. Keine Secrets oder sensiblen Kundendaten verwenden.
Managed Resource Group	Ja	Die verwaltete Ressourcengruppe, die interne von der Anwendung bereitgestellte Ressourcen erhält.	Azure schlägt oft einen generierten Namen vor. Halten Sie ihn eindeutig und erkennbar. Diese Gruppe wird von der Anwendung verwaltet; direkter Zugriff kann durch das Managed-Application-Modell eingeschränkt sein.
Previous	Nein	Kehrt zum vorherigen Formularschritt zurück.	Dieser Button startet keine Bereitstellung.
Next	Nein	Wechselt zum nächsten Tab, wenn Pflichtfelder ausreichend gefüllt sind.	Verwenden Sie ihn für Application Settings . Wenn Azure blockiert, prüfen Sie Pflichtfelder mit  .
Review + create	Nein	Startet die finale Azure-Validierung vor der Erstellung.	Erst nach Abschluss der Anwendungseinstellungen verwenden. Azure zeigt danach Fehler oder Warnungen, die vor der echten Erstellung behoben werden müssen.

Bildschirm 2 - Application Settings

Der Tab **Application Settings** konfiguriert die ProPM-Agent-Umgebung selbst: Administrationsidentität, Installationsmodus, initialen KI-Anbieter, CORS, Monitoring, Logging, initiales Passwort und Netzwerk.

Microsoft Azure

Search resources, services, and docs (G+7)

Copilot

AmineSMAOUI@NovaBi...
NOVABIZ LLC (NOVABIZLLC.ON...

Home > ProPM Agent

Create ProPM-50

Environment Name * ⓘ

prod

Installation mode ⓘ

New installation - create new resources

Platform Administration Entra Group Object IDs * ⓘ

Platform Administration Bootstrap Users (optional) ⓘ

Allow Azure RBAC admin recovery ⓘ

☒

LLM Provider ⓘ

CORS Allowed Origins ⓘ

Enable alerting (Azure Monitor) ⓘ

☒

Enable debug logging ⓘ

☐

Password * ⓘ

Confirm password * ⓘ

VNet CIDR * ⓘ

10.0.0.0/16

Previous

Next

Review + create

Give feedback

Felder im Tab Application Settings

FELD	PFLICHTFELD	EINGABE	AUSWIRKUNGEN UND EMPFEHLUNGEN
Environment Name	Ja	Kurzer Umgebungsname, zum Beispiel <code>dev</code> , <code>test</code> , <code>uat</code> oder <code>prod</code> .	Hilft beim Erkennen der Umgebung in Ressourcen, Konfiguration und Support-Austausch. Verwenden Sie einen kurzen, stabilen, nicht geheimen Wert nach interner Konvention.
Installation mode	Szenarioabhängig	Der Installationsmodus. Für eine Erstinstallation New installation - create new resources beibehalten.	Erstellt eine neue Instanz mit neuen Ressourcen. Einen Attach-Modus für vorhandene Ressourcen nur für vorbereitete Planwechsel, größere Updates oder Recovery-Szenarien verwenden.
Platform Administration Entra Group Object IDs	Ja	Object IDs der Entra-Gruppen, die die Plattform administrieren dürfen.	Tragen Sie die Object IDs der Gruppen ein, nicht nur Anzeigenamen. Diese Gruppen bestimmen den Zugriff auf Platform Administration nach der Bereitstellung. Dedizierte Gruppen sind besser als zu breite Gruppen.

FELD	PFLICHTFELD	EINGABE	AUSWIRKUNGEN UND EMPFEHLUNGEN
Platform Administration Bootstrap Users (optional)	Nein	Bootstrap- oder Recovery-Benutzer, falls Ihre Betriebsprozedur dies verlangt.	Nützlich für den ersten Zugriff, wenn Entra-Gruppen noch nicht vollständig greifen. Liste minimal und kontrolliert halten.
Allow Azure RBAC admin recovery	Nein	Checkbox für Administrator-Wiederherstellung über Azure RBAC.	Aktiviert lassen, wenn Ihr Betriebsmodell einem autorisierten Azure-Administrator die Wiederherstellung des Plattformzugriffs erlaubt. Nur deaktivieren, wenn Governance eine strikte dokumentierte Trennung verlangt.
LLM Provider	Empfohlen	Initiale KI-Anbieterfamilie: Azure OpenAI, OpenAI, OpenRouter oder OpenAI-compatible, je nach verfügbaren Optionen.	Dies ist eine initiale Bereitstellungsabsicht. Es beweist nicht, dass der Anbieter betriebsbereit ist. Nach der Installation den Anbieter in Platform Administration > AI Provider Settings mit Save , Validate , Test und Activate abschließen.
CORS Allowed Origins	Szenarioabhängig	Zusätzliche erlaubte Web-Origins, zum Beispiel <code>https://portal.contoso.com</code> .	Leer lassen, wenn keine zusätzliche Origin benötigt wird. Zu breite Wildcards vermeiden. Werte sollten vollständige Origins mit <code>https://</code> , Domain und bei Bedarf Port sein.
Enable alerting (Azure Monitor)	Nein	Aktiviert oder deaktiviert Azure-Monitor-Alarme für die Umgebung.	Für Produktion empfohlen, damit Vorfälle erkannt werden. Anschließend Empfänger, Action Rules und Kostenregeln in Azure Monitor prüfen.
Enable debug logging	Nein	Aktiviert detailliertere Logs.	In Produktion deaktiviert lassen, außer bei Support-Diagnose. Debug Logging kann Log-Volumen erhöhen und mehr technische Details für berechnigte Administratoren sichtbar machen.

FELD	PFLICHTFELD	EINGABE	AUSWIRKUNGEN UND EMPFEHLUNGEN
Password	Ja	Das initiale Passwort, das vom Bereitstellungsformular verlangt wird.	Starkes Passwort generieren und in einem genehmigten Vault oder Secret Manager speichern. Nicht per E-Mail, Chat oder ungesichertem Ticket senden.
Confirm password	Ja	Derselbe Wert wie Password .	Azure prüft, dass beide Felder übereinstimmen. Bei Fehler beide Werte erneut aus der sicheren Quelle eingeben.
VNet CIDR	Ja	Der private Netzwerkbereich für die Bereitstellung, zum Beispiel <code>10.0.0.0/16</code> .	Bereich wählen, der nicht mit bestehenden Netzwerken, Peerings, VPNs oder geplanten Bereichen kollidiert. Vor Erstellung vom Netzwerkteam validieren lassen, da Änderungen nach der Bereitstellung schwierig sind.
Previous	Nein	Kehrt zum Tab Basics zurück.	Nützlich, um Abonnement, Gruppe, Region oder Namen vor finaler Validierung zu korrigieren.
Next	Nein	Wechselt zum nächsten Formularschritt.	Verwenden, wenn Sie der Tab-Reihenfolge folgen möchten.
Review + create	Nein	Führt die finale Validierung aller Parameter aus.	Azure erstellt Ressourcen erst, wenn Sie nach der Validierung die Erstellung bestätigen. Alle Fehler vorher beheben.

LLM Provider auswählen

Das Feld **LLM Provider** wählt die KI-Familie, die die Umgebung zunächst verwenden soll. Es beendet die KI-Konfiguration nicht.

AUSWAHL	WANN WÄHLEN	NACH DER INSTALLATION NOCH ERFORDERLICH
Azure OpenAI	Die Organisation möchte im Azure-, Entra- und Microsoft-Governance-Ökosystem bleiben.	Endpoint, Region oder verfügbares Modell, Azure-OpenAI-Einstellungen, Tests und Aktivierung bestätigen.

AUSWAHL	WANN WÄHLEN	NACH DER INSTALLATION NOCH ERFORDERLICH
OpenAI	Die Organisation nutzt OpenAI APIs direkt.	URL, Modell, Schlüssel oder Secret-Referenz eingeben, dann Save, Validate, Test, Activate ausführen.
OpenRouter	Die Organisation möchte mehrere Modelle über einen Einstiegspunkt nutzen.	Base URL, Schlüssel oder Secret-Referenz, Standardmodell eingeben, dann validieren und aktivieren.
OpenAI-compatible	Die Organisation nutzt ein OpenAI-kompatibles Gateway oder Endpoint.	Exakten Endpoint, Authentifizierungsmodus, erwartetes Modell oder Deployment eingeben und echte Kompatibilität testen.

Einfache Regel: Die Bereitstellung **wählt** den KI-Anbieter aus; die ProPM-Agent-Administration macht ihn **betriebsbereit**.

Validierung vor Review + create

Prüfen Sie diese Punkte vor der Erstellung.

PRÜFUNG	ERWARTETES ERGEBNIS
Abonnement und Ressourcengruppe	Passen zur Zielumgebung und zu Governance-Regeln
Region	Erfüllt Datenresidenz, Verfügbarkeit und Netzwerkstrategie
Application Name	Name ist klar, stabil und nicht vertraulich
Managed Resource Group	Name ist eindeutig und erkennbar
Entra Group Object IDs	IDs gehören zu den Gruppen für Plattformadministration
Bootstrap Users	Liste ist leer oder streng auf vorgesehene Konten begrenzt
RBAC recovery	Auswahl passt zur Wiederherstellungsprozedur
LLM Provider	Initialer Anbieter passt zur KI-Strategie
CORS	Nur erforderliche Origins sind erlaubt
Alerting	Für zu überwachende Umgebungen aktiviert
Debug logging	Außerhalb kontrollierter Diagnose deaktiviert

PRÜFUNG	ERWARTETES ERGEBNIS
Password	Im Vault gespeichert und nie im Klartext geteilt
VNet CIDR	Vom Netzwerkteam validiert und ohne bekannte Überschneidung

Nach der Bereitstellung

1. Warten Sie, bis Azure-Provisioning abgeschlossen ist.
2. Öffnen Sie die veröffentlichte ProPM-Agent-URL.
3. Melden Sie sich mit einem Konto an, das durch Entra-Gruppen oder Bootstrap-Prozedur autorisiert ist.
4. Prüfen Sie Zugriff auf **Plattform Administration**.
5. Öffnen Sie die KI-Anbieter-Einstellungen.
6. Führen Sie **Save, Validate, Test** und **Activate** für den gewählten Anbieter aus.
7. Prüfen Sie Lizenzen und Marketplace-Plan.
8. Führen Sie einen ersten Funktionstest mit einem Standardbenutzer aus.
9. Prüfen Sie nach einem Run das [Journal IA](#), um den tatsächlich verwendeten Anbieter zu bestätigen.

Häufige Blocker

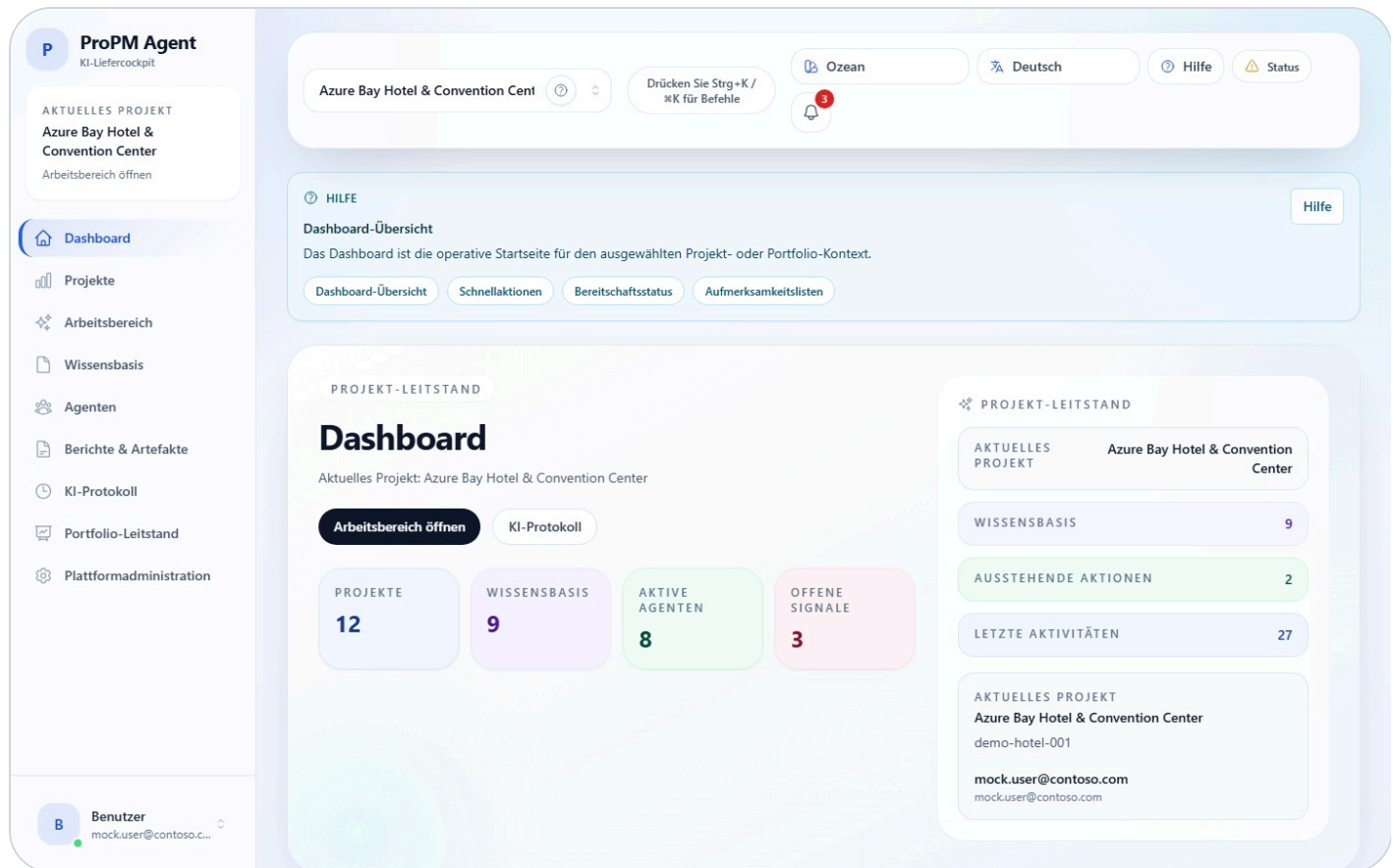
SYMPTOM	WAHRSCHEINLICHE URSACHE	EMPFOHLENE AKTION
Azure wechselt nicht zum nächsten Schritt	Pflichtfeld leer oder ungültig	Alle mit  markierten Felder und Meldungen unter den Feldern prüfen
Administrator sieht Plattform Administration nicht	Falsche Entra Object ID oder Gruppenmitgliedschaft noch nicht propagiert	Object ID der Gruppe und Kontomitgliedschaft prüfen
Netzwerkkonflikt bei Validierung	VNet CIDR bereits verwendet oder überlappend	Mit dem Netzwerkteam anderen Bereich wählen
KI-Anbieter nach Erstellung nicht nutzbar	Bereitstellung hat nur die Anbieterfamilie ausgewählt	Anbieter in Administration mit Save, Validate, Test, Activate abschließen
Zu viele Logs oder unerwartete Kosten	Debug Logging oder Alerting ohne Governance aktiviert	Azure-Monitor-Einstellungen anpassen und Debug außerhalb Diagnose deaktivieren

Weiter

- Für Entra-Zugriff öffnen Sie [Azure- und Entra-Administration](#).
- Für den KI-Anbieter öffnen Sie [KI-Anbieter](#).
- Für Lizenzen, Pläne und Updates öffnen Sie [Lizenzen, Pläne und Updates](#).
- Für Benutzer senden Sie [Erste Schritte](#).

Schnittstelle und Navigation

[Startseite](#) · Schnittstelle und Navigation



Ziel

Diese Seite erklärt, wie man sich in der ProPM Agent-Shell zurechtfindet, das **Dashboard** liest, die **Command Palette** nutzt, die **Benachrichtigungen** interpretiert und das **Health Panel** bei Bedarf für eine schnelle Überprüfung verwendet.

Überblick

Die Oberfläche folgt einer einfachen Logik:

1. die **Sidebar** öffnet die großen Funktionsbereiche;
2. die **Top bar** ändert das aktuelle Projekt und öffnet die Schnellwerkzeuge;
3. die zentrale Fläche zeigt den **aktuellen Kontext**;
4. mehrere Bildschirme ändern ihren Zustand je nach **aktivem Projekt** und Ihren **Rechten**.

Hauptnavigation

EINTRAG	HAUPTVERWENDUNG
Dashboard	Lesen Sie den allgemeinen Status und die empfohlenen nächsten Schritte
Projects	Erstellen, öffnen und wechseln Sie den Projektkontext
Workspace	Projektzusammenfassung, Signale, Readiness und Projekteinrichtungen
Knowledge	Suchen, hochladen und importieren Sie Referenzdokumente
Agents	Interagieren Sie mit verfügbaren Agenten und lesen Sie strukturierte Ausgaben
Reports & artifacts	Überprüfen, vergleichen, veröffentlichen oder herunterladen Sie PM-Dokumente
AI Log	Untersuchen Sie Runs, Ereignisse und Metadaten der Nachvollziehbarkeit
Portfolio	Vergleichen Sie mehrere Projekte über konfigurierbare Signale
Platform Administration	Verwalten Sie Integrationen, KI-Anbieter, Abonnement und Plattformaktivität

Dashboard

Das **Dashboard** ist der nützlichste Bildschirm direkt nach dem Einloggen.

Es konsolidiert:

- Situation-Metriken;
- Aufmerksamkeitspunkte;
- empfohlene nächste Schritte;
- Shortcuts zu den Bereichen, in denen gehandelt werden muss;
- einen Überblick über offene Signale und geprüfte Elemente.

Nutzen Sie es als **Orientierungsseite**: wenn kein Projekt aktiv ist, bleiben einige Blöcke leer; wenn ein Projekt ausgewählt ist, passen sich die Indikatoren an.

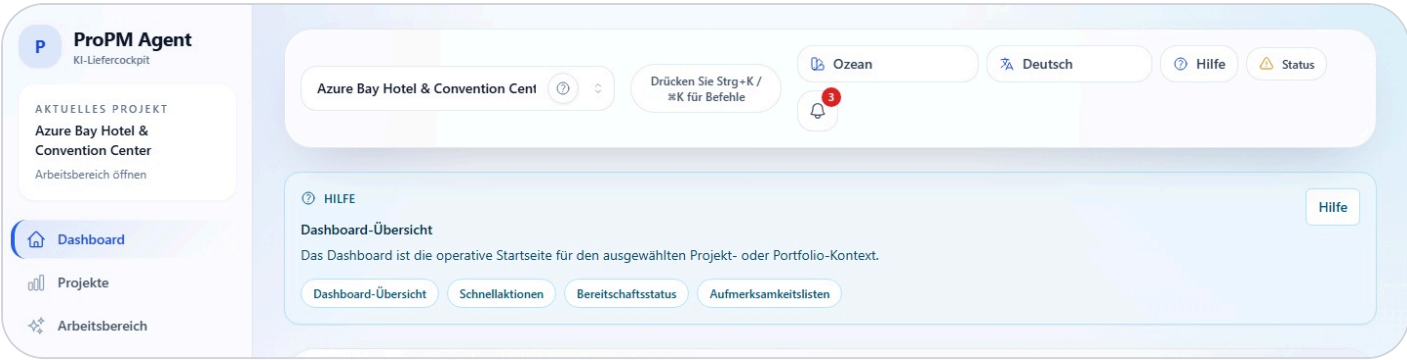
Wie man die großen Bereiche des Dashboards liest

BEREICH	WAS SIE ZUSAMMENFASST	NÜTZLICHER REFLEX
Summary tiles	Zähler für Projekte, Wissen, aktive Agenten, offene Signale, Entwürfe von Benachrichtigungen und ausstehende Aktionen	Erkennen Sie sofort, ob das Thema ein Kontextmangel, eine Verzögerung bei der Überprüfung oder eine verwaltete Warteschlange ist
Score cards	Allgemeiner Zustand der Lieferung, des Ausführungstakt, der Governance-Abdeckung und der Wissenstiefe	Lesen Sie diese Karten als Orientierungshilfen, bevor Sie einen Detailbildschirm öffnen
Readiness blocks	Wissensbasis, Automatisierungsabdeckung, Governance-Posture und Lieferfluss	Identifizieren Sie, welcher Pfeiler die normale Nutzung des Projekts blockiert
Attention panel	Signale, verwaltete Aktionen und Watchlist-Connectoren	Gehen Sie zum Workspace , um aktive Blockaden zu behandeln
Pulse panel	Letzter Digest, aktuelle Benachrichtigungen, jüngste Aktivitäten und Connector-Status	Überprüfen Sie, was sich geändert hat, ohne die gesamte Projektgeschichte erneut zu lesen
Quick links	Verknüpfungen zu Workspace , Knowledge , Agents , Reports & artifacts , AI Log und Portfolio	Öffnen Sie direkt die richtige Oberfläche anstatt Bildschirme zu navigieren

Die Scores und Indikatoren des Dashboards sollten als **Priorisierungsreferenz** gelesen werden, nicht als alleinige Schlussfolgerung.

Was tun, wenn das Dashboard widersprüchlich erscheint?

1. Bestätigen Sie zuerst das **aktive Projekt** in der oberen Leiste.
2. Behandeln Sie die Karten anschließend als **Orientierungs-Signale**, nicht als einzige Wahrheit.
3. Öffnen Sie den **Workspace**, um Signale, Readiness und Projektblockaden zu prüfen.
4. Öffnen Sie das **AI Log**, wenn der Zweifel auf einen Run, eine Ausgabe oder einen tatsächlich genutzten Anbieter gerichtet ist.
5. Wenn das Dashboard lädt, aber eine zusätzliche Überprüfung anfordert, öffnen Sie den **Health indicator** bevor Sie zu den angezeigten Daten schließen.



Top bar

ELEMENT	FUNKTION
Project selector	Ändert das aktuelle Projekt ohne die vollständige Liste zu durchlaufen
Command palette	Schnelle Suche nach Seiten und häufigen Aktionen
Notifications	Zeigt die vom Produkt gemeldeten Aufmerksamkeitspunkte an
Health indicator	Öffnet eine schnelle Ansicht des API-, Echtzeit- und Auth-Status
Language	Ändert die Sprache der Oberfläche
Theme	Schaltet zwischen hell/dunkel aus
Help	Öffnet die integrierten Hilfemeldungen

Wie Sie das aktive Projekt in der oberen Leiste lesen

Der Projektselektor in der oberen Leiste definiert das **aktive Projekt**. Dieses Projekt wird anschließend als Kontext von projektbezogenen Seiten verwendet.

In der Praxis:

- **Knowledge** sucht innerhalb des aktiven Projekts;
- **Agents** startet Runs im aktiven Projekt;
- **Reports & artifacts** prüft PM-Dokumente und Artefakte des aktiven Projekts;
- **AI Log** zeigt Runs und Aktivität des aktiven Projekts;
- **Workspace** zeigt Signale, Einstellungen und Integrationen des aktiven Projekts.

Das ausgewählte Projekt kann lokal im Browser gemerkt werden. Diese Navigationshilfe ist keine plattformweit geteilte Einstellung.

Wenn eine projektbezogene Seite leer oder widersprüchlich wirkt, lesen Sie daher zuerst den im Projektselektor angezeigten Namen.

Command palette

Die Command Palette ist für die schnelle Navigation konzipiert.

- **Windows / Linux:** 
- **macOS:** 

Sie filtert die verfügbaren Seiten und Einträge nach **Name** und **Beschreibung**.

Verwenden Sie sie, um schnell zum **AI Log**, zur **Platform Administration** oder zu jeder selten geöffneten Route zurückzukehren.

Benachrichtigungen

Der Benachrichtigungsbereich ist über das Glocken-Symbol in der oberen Leiste zugänglich.

Verfügbare Funktionen:

- Zähler für ungelesene Elemente;
- Dropdown-Paneel;
- **Mark all as read;**
- **Clear all;**
- Klick auf eine Benachrichtigung, um die zugehörige Oberfläche zu öffnen, wenn eine Navigation bereitgestellt wird.

Benachrichtigungen stammen nicht nur aus einer einzigen Ereignisfamilie. In ProPM Agent können sie unter anderem bündeln:

- Statusänderungen von Agenten oder Runs;
- Ereignisse zu Berichten, Artefakten oder Dokumenten;
- serverseitig gelesene Projektbenachrichtigungen;
- Governance- oder Genehmigungsfolgen;
- Integrations-, Marketplace-, Abonnement- oder kostenbezogene Aktualisierungen.

Das Zentrum in der oberen Leiste kann daher nahezu Echtzeit-Ereignisse und serverseitig gelesene Projektbenachrichtigungen in derselben Liste mischen.

Health indicator

Der Health indicator öffnet ein Quick-Read-Panel. Es ermöglicht die Anzeige von:

- API-Status;

- Echtzeit-Status;
 - Auth-Status;
 - angezeigte Latenz;
 - eine Meldung, falls die Oberfläche eine hat;
 - dem aktuellen Projekt, wenn der Kontext bei der Statusauswertung wichtig ist.
- Öffnen Sie ihn, wenn ein Agent offline erscheint, wenn Benachrichtigungen nicht mehr aktualisiert werden oder wenn eine Verfügbarkeitsprüfung sinnvoll ist.

Wenn das Panel einen degradierenden Zustand anzeigt, während die Oberfläche noch lädt, folgen Sie dieser Lesereihenfolge:

WENN DAS SIGNAL HAUPTSÄCHLICH BETRIFFT...	ÖFFNEN SIE ANSCHLIESSEND	WARUM
authentication	Start	um Tenant, Konto, redirect URI , Admin-Gruppe oder Lizenzplatz zu unterscheiden
runtime , API oder Konnektivität	Wartung, Support und FAQ	um den Prüfpfad zwischen Health, KI-Anbieter, Integrationen und Ausführung zu verfolgen
project context , ein leerer Bildschirm oder fehlende Aktion	Projekte und Arbeitsbereich	um aktives Projekt, Binding, Readiness und Projektrechte zu prüfen

Bevor Sie eskalieren, notieren Sie den angezeigten Status für **API**, **realtime**, **auth**, **latency**, **current project** und die ungefähre Testzeit. Diese Angaben erleichtern die Bearbeitung durch das zuständige Team erheblich.

Projektkontext und leere Zustände

Mehrere Bildschirme von ProPM Agent hängen vom aktiven Projekt ab. In der Praxis:

- **ohne Projekt ausgewählt**, zeigen einige Seiten einen normalen leeren Zustand;
- **mit Projekt ausgewählt**, lädt dieselbe Seite Daten und Aktionen dieses Projekts;
- das Projektwechseln ändert den Inhalt von **Knowledge**, **Agents**, **Reports & artifacts** und **AI Log**.

Diese Kontextabhängigkeit verhindert das Vermischen von Beweisen, Gesprächen und Lieferungen mehrerer Projekte.

Was Navigation nicht bedeutet

Einige Missverständnisse treten häufig auf:

- das Öffnen von **Portfolio** ändert nicht automatisch das aktive Projekt projektbezogener Seiten;
- **All projects** ist kein im oberen Balken auswählbares Projekt;
- eine leere Seite ist kein Beweis für einen Fehler: sie kann einfach bedeuten, dass kein aktives Projekt gesetzt ist oder dass für dieses Projekt noch keine Daten existieren;
- ein im Browser sichtbarer Chatverlauf bedeutet nicht, dass er mit allen Benutzern geteilt ist.

Sprache, Thema und Hilfe

Die Sprache der Oberfläche kann über die obere Leiste geändert werden. Das Thema verbessert den Lesekomfort, hat jedoch keine Auswirkungen auf Projektdaten. Die integrierten Hilfekataloge decken die allgemeine Navigation, Projektseiten, das AI Log und Governance-Erinnerungen ab.

Was in der Navigation lokal im Browser bleibt

Neben der Chat-Kontinuität und dem gemerkten aktuellen Projekt bleiben auch folgende Hilfen browserlokal:

- Sprache und Thema der Oberfläche;
- Liste der zuletzt verwendeten Projekte;
- gelesen/gelöscht-Status des Benachrichtigungszentrums;
- einige lokal gespeicherte Tabellen- oder Ansichtsvoreinstellungen.

Projektbenachrichtigungen, Signale, Digests, Benachrichtigungsentwürfe, governierte Aktionen, Dokumente und Artefakte gehören dagegen zum geteilten Plattformzustand. Ein lokal sichtbarer Verlauf oder ein lokal als gelesen markiertes Element bedeutet deshalb nicht automatisch, dass der gemeinsame Plattformzustand geändert wurde.

Navigations-Tipps

- Wechseln Sie das Projekt **vor** dem Öffnen eines Agenten oder eines Berichts;
- Nutzen Sie die **Command Palette**, um schnell eine selten genutzte Oberfläche zu finden;
- Kehren Sie zum **Dashboard** zurück, wenn Sie den Überblick verlieren;

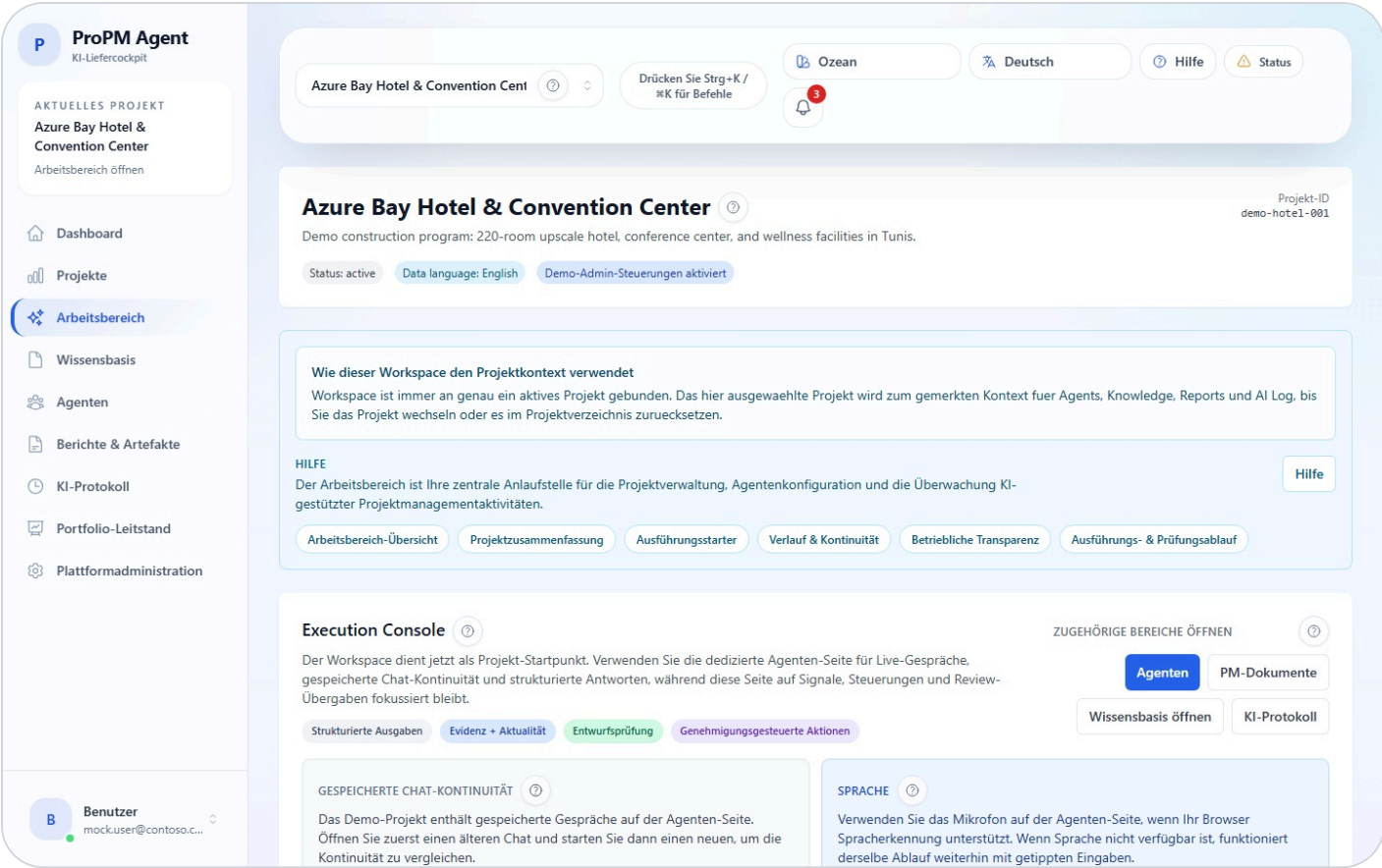
- Wenn eine Aktion fehlt, unterscheiden Sie klar zwischen **Read-Only** und **Zugriff verweigert**;
- Öffnen Sie den **Health indicator**, bevor Sie zu einer Service-Verfügbarkeitsfrage kommen.

Weiter

- [Projekte und Arbeitsbereich](#)
- [Wissen und Agenten](#)
- [Strukturierte Ausgaben, Beweise und Frische](#)
- [Berichte, KI-Log und Nachvollziehbarkeit](#)

Projekte und Arbeitsbereich

Startseite · Projekte und Arbeitsbereich



Ziel

Diese Seite erklärt den Unterschied zwischen **Projekte**, **Arbeitsbereich** und **Agenten**, und beschreibt die tatsächlich in der Anwendung sichtbaren Projekteinstellungen.

Drei zu unterscheidende Oberflächen

OBERFLÄCHE	WANN MAN SIE NUTZT
Projekte	Erstellen eines Projekts, Öffnen eines bestehenden Projekts, Wechseln des Kontexts
Arbeitsbereich	Lesen der Projektzusammenfassung, operativen Transparenz, Signale und Projekteinstellungen
Agenten	Starten eines Live-Austauschs mit einem Agenten und Lesen der strukturierten Ausgabe des Runs

In der Praxis dient **Projekte** dazu, in den richtigen Kontext zu gelangen, **Arbeitsbereich** zur Konfiguration und **Agenten** zur Ausnutzung.

Die genaue Rolle des aktiven Projekts

Das **aktive Projekt** ist der Kontext, der aktuell auf projektbezogene Arbeitsseiten angewendet wird.

Konkret bestimmt es:

- welche Dokumente in **Knowledge** sichtbar sind;
- welche Runs in **Agents** gestartet werden;
- welche PM-Dokumente, Artefakte und Diffs in **Reports & artifacts** sichtbar sind;
- welche Runs und Ereignisse in **AI Log** erscheinen;
- welche Signale, Integrationen und Richtlinien im **Workspace** erscheinen.

Verwechseln Sie es deshalb nicht mit:

- **Portfolio**, einer Mehrprojekt-Vergleichsfläche;
- **All projects**, einem optionalen Sichtbarkeitsbereich benutzerdefinierter Agenten über mehrere Projekte desselben Kontos hinweg.

Projekt erstellen

Das Formular enthält die folgenden Felder:

- **ID Projekt**;
- **Name**;
- **Beschreibung**;
- **Standard-Datensprache**;
- **Zusätzliche Datensprachen**.

Eingabeempfehlungen:

- wählen Sie eine lesbare und dauerhafte ID;
- verwechseln Sie nicht **Projekt-Datensprache** und **Interface-Sprache**;
- definieren Sie den Umfang korrekt, bevor Sie Wissen oder Agenten öffnen.

Projektersteller: Anfangsrechte und Delegation

Beim Erstellen übernimmt der **Projektersteller** die Rolle **Projektbesitzer** und alle verfügbaren Projektberechtigungen. In der Praxis ist er also derjenige, der das Projekt öffnen, die anfängliche Konfiguration prüfen und anschließend die Rollen an das restliche Team delegieren kann.

Empfohlene Delegation unmittelbar nach der Erstellung

1. Öffnen Sie **Zugriffskontrolle**;
2. Fügen Sie mindestens einen weiteren **Projektbesitzer** oder einen vertrauenswürdigen **Projektleiter** hinzu;
3. Erstellen Sie bei Bedarf gezielte benutzerdefinierte Rollen statt mehrere Besitzer zu haben;
4. Weisen Sie anschließend Rollen an Mitwirkende, Leser und Auditoren zu;
5. Lesen Sie abschließend die **Governance-Richtlinien** und die **Projektintegrationen**, um Rechte, Connectoren und Validierungen abzustimmen.

Was die Plattform weiterhin schützt

- Der **Ersteller** bleibt geschützt;
- Die Rolle des Erstellers bleibt in der Oberfläche fest;
- Die Delegation erfolgt durch Zuweisung zusätzlicher Rollen, nicht durch Abschaffung des Erstellerschutzes;
- Für detailliertes RBAC siehe [Zugriffskontrolle und Rollen Projekt](#).

Projekt öffnen und wechseln

Ein Projekt kann von folgenden Orten aus geöffnet werden:

- der Seite **Projekte**;
- dem **Projektselektor** in der oberen Leiste;
- dem zuletzt im Browser gespeicherten Kontext.

Wenn Sie das Projekt wechseln, werden die folgenden Oberflächen synchronisiert:

Wissen, Agenten, PM-Dokumente / Berichte & Artefakte, KI-Log, Signale und Projekteinstellungen.

Der Projektwechsel ändert damit tatsächlich den **aktiven Kontext**, der für Dokumentensuche, Agentengespräche, Berichte und die zugehörige Nachvollziehbarkeit verwendet wird.

Das zuletzt gemerkte Projekt kann lokal im Browser gespeichert werden, um die Wiederaufnahme zu erleichtern; diese lokale Erinnerung ist jedoch keine plattformweit geteilte Einstellung.

Der Arbeitsbereich: Steuerzentrale des Projekts

Der **Arbeitsbereich** bündelt in einer Oberfläche:

- die **Projektzusammenfassung**;
- Verknüpfungen zu **Agenten**, **PM-Dokumenten** und **KI-Log**;
- eine Sicht auf **operative Transparenz**;
- die **Signale** des Projekts;
- Registerkarten für Projekteinstellungen.

Der **Arbeitsbereich** zeigt keinen eigenen Einstiegspunkt für **Spracheingabe** mehr. Wenn Spracheingabe in einigen Umgebungen noch vorhanden ist, ist sie in **Agenten** verfügbar, nicht als separater Einstiegspunkt im Arbeitsbereich.

Operative Transparenz und Vorbereitung

Der Arbeitsbereich dient nicht nur der Zusammenfassung des Projekts. Er ermöglicht auch zu sehen, ob das Projekt bereit ist zu handeln:

- Vorhandensein oder Fehlen von Signalen;
- Aktuelle Aktivität;
- Verknüpfungen zu Entwürfen oder zugehörigen Lieferungen;
- Vorbereitung der Projektintegrationen, falls vorhanden;
- Anzeige des tatsächlich verwendeten KI-Anbieters ohne Öffnen der Tenant-Konfiguration.

Nutzen Sie diesen Bereich, um zu verstehen **warum** eine Aktion oder ein Import verfügbar, bestätigt oder blockiert sein könnte.

Mittel

Offen

Suggest

Entwurf erstellen

Contradictory status signals detected

24h zurückstellen

Verwerfen

A narrative source and an operational source disagree on the current dependency posture.

Warum es erzeugt wurde: Generated because the current narrative implies the dependency is stable while another source still reports an active watchpoint.

1 Evidenzverweise

3-mal ausgelöst

EMPFOHLENE NÄCHSTE SCHRITTE

- Capture the contradiction explicitly in the next briefing artifact.

knowledge: Aktuell

connector:primavera-primary: Widersprüchlich

Zuletzt erkannt: 21/04/2026 14:12:20

Mittel

Zurückgestellt

Draft

Entwurf erstellen

Approved publication follow-up pending

24h zurückstellen

Verwerfen

1 Evidenzverweise

artifacts: Alternd

actions: Alternd

LETZTER DIGEST

?

Hotel proactive digest

Erzeugt 21/04/2026 14:37:20

2 zusammengefasste Signale

1 vorbereitete Entwürfe

[Hoch] Schedule freshness degraded

Schedule evidence is older than the latest project narrative and should be reviewed before publication.

[Mittel] Contradictory status signals detected

A narrative source and an operational source disagree on the current dependency posture.

Wie Signale, Digests und Entwürfe eintreffen

In der Oberfläche liest das Signale-Panel des Projekts drei geteilte Plattformflüsse für das **aktive Projekt** erneut:

- aktuelle **Signale**;
- aktuelle **Digests**;
- **Benachrichtigungsentwürfe**, die mit diesen Signalen verbunden sind.

Nützliche Lesart:

- das Öffnen des Arbeitsbereichs lädt den bereits bekannten gemeinsamen Zustand dieses Projekts;
- **Refresh** fordert das System ausdrücklich auf, das Projekt erneut auszuwerten und die neuesten proaktiven Signale zu ziehen;

- **Generate digest draft** erstellt eine neue gruppierte Zusammenfassung und kann `in_app`-Benachrichtigungsentwürfe vorbereiten;
- diese Elemente sind daher nicht nur lokale Browser-Notizen.

Registerkarten auf Projektebene

REGISTERKARTE	ZWECK
Agentenkonfiguration	Agenten für dieses Projekt konfigurieren
Zugriffskontrolle	Mitglieder, Rollen und Projekteinstellungen verwalten
Dokumentenkategorien	Dokumenten-Taxonomie des Projekts anpassen und auf projektbezogene Oberflächen übertragen
Governance-Richtlinien	Connectoren, Ziele, Aktionsrichtlinien, Renderprofile und Benachrichtigungspräferenzen auf Projektebene festlegen
Projektintegrationen	Projektbezogene, bereitgestellte und autorisierte Integrationen verbinden
Aktionen & Genehmigungen	Aktionsanfragen, Validierungen und gesteuerte Ausführung verwalten

Agentenkonfiguration

Die auf Projektebene bestätigten Parameter sind:

- `status` ;
- `temperature` ;
- `max tokens` .

Sichtbare Einschränkungen

- `temperature` wird zwischen **0** und **2** erwartet;
- `max tokens` muss eine ganze Zahl ≥ 1 sein.

Konfigurationsverlauf

Die Oberfläche zeigt auch einen Versionsverlauf mit mindestens:

- Versionsnummer;
- Status;
- Temperatur;

- Max Tokens;
- Erstellungsdatum;
- Autor;
- zugehörige Trace ID.

Projekt-Agentenkonfiguration

Agenten pro Projekt aktivieren/deaktivieren und Parameter anpassen.
Prüfen Sie die effektive Laufzeitkonfiguration für jeden Agenten, bearbeiten Sie jeweils nur eine Zeile und verwenden Sie den Verlauf, um Änderungen nachzuvollziehen.

STATUS

8

8 aktiviert

DEAKTIVIERT

0

0 deaktiviert

BEARBEITEN

0

0 Zeilen bearbeitet

Speichern Sie Änderungen zeilenweise, damit jede Anpassung nachvollziehbar bleibt. Verwenden Sie Zurücksetzen, um ungespeicherte Änderungen vor dem Speichern zu verwerfen.

Agent	Version	Status	Temperatur	Max. Tokens	Aktionen
Virtual Project Manager default Routes your request to the right performance-domain specialist agents, then synthesizes a single value-focused answer. Principles: Adopt a Holistic View; Focus on Value; Embed Quality; Be an Accountable Leader; Integrate Sustainability; Build an Empowered Culture.	Erste Speicherung ausstehend	aktiviert	0.2 Aktuell: 0.2	1024 Aktuell: Nicht festgelegt	Speichern Zurücksetzen Verlauf
Governance Lead default Ensures appropriate oversight, decision making, compliance, and alignment with organizational policies. Principles: Adopt a Holistic View; Focus on Value; Embed Quality; Be an Accountable Leader; Integrate Sustainability; Build an Empowered Culture.	Erste Speicherung ausstehend	aktiviert	0.2 Aktuell: 0.2	1024 Aktuell: Nicht festgelegt	Speichern Zurücksetzen Verlauf
Scope Lead default Defines and manages the boundaries of the project, including quality expectations. Principles: Adopt a Holistic View; Focus on Value; Embed Quality; Be an Accountable Leader; Integrate Sustainability; Build an Empowered Culture.	Erste Speicherung ausstehend	aktiviert	0.2 Aktuell: 0.2	1024 Aktuell: Nicht festgelegt	Speichern Zurücksetzen Verlauf
Schedule Lead default Establishes timelines, sequences work, and supports the coordination of activities. Principles:	Erste Speicherung ausstehend	aktiviert	0.2 Aktuell: 0.2	1024 Aktuell: Nicht festgelegt	Speichern Zurücksetzen Verlauf

Zugriffskontrolle

Die Registerkarte **Zugriffskontrolle** verwaltet Mitglieder und Projektrollen. Sie unterstützt:

- Standardrollen;
- Benutzerdefinierte Rollen;
- RBAC-Schutzmechanismen;
- Nur-Lese-Zugriff für nicht autorisierte Profile.

Siehe die zugehörige Seite: [Zugriffskontrolle und Rollen Projekt](#).

Dokumentenkategorien

Diese Registerkarte dient dazu, die Dokumentenklassifizierung mit dem Projekt abzugleichen. In der Praxis beeinflusst die Projekt-Taxonomie die vorgeschlagenen Kategorien bei Uploads und einige Dokumentenauswahl-Filter, die später in Projektoberflächen verwendet werden.

Konkreter Effekt einer Aktualisierung

Wenn die Kategorienliste erfolgreich geändert wird:

- Der Kategorieauswahl-Filter beim Upload in **Wissen** wird aktualisiert;
- Die Kategoriefilter in **PM-Dokumenten** passen sich an, wenn sie diese geteilte Taxonomie nutzen;
- Die Änderung bleibt auf das **aktuelle Projekt** beschränkt.

Praktische Beispiele

Halten Sie eine kurze und stabile Taxonomie. Zum Beispiel, anstatt Varianten zu multiplizieren, bevorzugen Sie ein paar konsistente Kategorien wie:

- Projektcharte;
- Risikoregister;
- Statusbericht;
- Einkaufsplan;
- Kommunikationsplan.

Das Ziel ist nicht, die Dokumentenversion in der Kategorie zu kodieren, sondern eine wiederverwendbare Klassifizierung zwischen **Wissen** und **PM-Dokumenten** zu behalten.

Dokumentkategorien

Konfigurieren Sie die im gesamten Projekt verwendete Kategorielliste (Knowledge-Uploads + PM-Doc-Kategorien).

Neue Kategorie

Status / SteerCo x

RAID x

Architecture x

Requirements x

Design x

Test Plan x

Release Notes x

Meeting Notes x

Vendor x

Finance x

Security x

Operations x

Business Case x

Benefits Management Plan x

Project Charter x

Change Management Plan x

Communications Management Plan x

Procurement Management Plan x

Quality Management Plan x

Resource Management Plan x

Risk Management Plan x

Schedule Management Plan x

Scope Management Plan x

Stakeholder Engagement Plan x

Assumption Log x

Issue Log x

Lessons Learned Register x

Milestone List x

Risk Register x

Stakeholder Register x

Status Report x

Tip: Halten Sie die Liste kurz und stabil. Sie können Uploads später weiterhin über Metadaten mit einer benutzerdefinierten Kategorie versehen.

Governance-Richtlinien

Diese Registerkarte legt die Regeln fest, die Entscheidungen, Validierungen und Governance-Verhalten des Projekts umrahmen. Nutzen Sie sie vor der Veröffentlichung eines Lieferobjekts oder der Genehmigung einer externen Aktion.

Unteroberflächen in Governance-Richtlinien

UNTEROBERFLÄCHE	WAS SIE REGELT
Ausführungs-Connectoren	Typ des Connectors, Status, Ausführungsmodus, Umgebung, Scopes und Kontextparameter
Artefaktziele	Ziel des Artefakts, zugehöriger Connector, Aktivität oder Standard
Aktionsrichtlinien	Betroffene Rolle, Ziel-Connector, Aktionsniveau (<code>observe</code> , <code>draft</code> , <code>propose</code> , <code>execute</code>), Wirkung (<code>allow</code> , <code>require_approval</code> , <code>deny</code>) und erlaubte Scopes
Renderprofile	Renderprofile und Ausgabeformate, die bei gesteuerten Veröffentlichungen verwendet werden
Benachrichtigungspräferenzen	Kanal, Benachrichtigungstyp, Digest-Modus, Schweregrenzwert und Aktivierung der Präferenz

Nützliche Einstellungsexemplare

- Erfordern Sie eine explizite Genehmigung vor einer Veröffentlichung zu **SharePoint**;
- Erlauben Sie die Erstellung von **Jira**-Tickets nur auf `propose`-Ebene für bestimmte Rollen;
- Bereiten Sie `signal_digest` in `in_app` für interne Nachverfolgung vor;
- Lassen Sie externe Benachrichtigungen `email` , `teams` oder `webhook` in einem genehmigten Pfad nur, wenn der Connector gesund ist;
- Wählen Sie getrennte Renderprofile für **DOCX** und **XLSX** Veröffentlichungen.

Glaubwürdiges Szenario - sensibles Projekt / gesteuerte Veröffentlichung

Für ein Projekt, bei dem jede externe Veröffentlichung kontrolliert werden muss, sieht eine konsistente Einstellung oft so aus:

1. **Artefaktziele:** SharePoint-Ziel aktiv mit bekanntem Renderprofil;

- Aktionsrichtlinien:** `allow` für `observe` und `draft`, aber `require_approval` für `execute` bei Veröffentlichungen und externen Benachrichtigungen;
- Ausführungs-Connectoren:** Externe Connectoren nur für tatsächlich autorisierte Rollen sichtbar;
- Benachrichtigungspräferenzen:** `signal_digest` in `daily` für das Team, `signal_alert` nur für die sensibelsten Fälle;
- Projektintegrationen:** Bindings aktiviert nur für bereits validierte Connectoren auf Plattformebene.

Diese Kombination verhindert, dass ein Entwurf, ein Digest oder eine Aktion als direkt veröffentlichbar erscheint, während das Projekt noch eine menschliche Genehmigung benötigt.

Governance-Richtlinien

Konfigurieren Sie gesteuerte Connectoren, Ziele, Aktionsrichtlinien, Rendering-Profil, Aktualitätsgrenzen und Benachrichtigungs-Digests.

CONNECTOREN 3	ZIELE 2	AKTIONSRICHTLINIEN 2	RENDERING-PROFILE 2	BENACHRICHTIGUNGSEINSTELLUNGEN 1
------------------	------------	-------------------------	------------------------	-------------------------------------

Review and save each governance object independently so connector posture, routing destinations, action boundaries, rendering behavior, and notification rules stay easy to audit.

GESTEUERTE AKTIONSTYPEN

Artefakt in SharePoint veröffentlichen Teams-Nachricht senden Outlook-Nachricht senden Jira-Ticket erstellen Azure-DevOps-Ticket erstellen Kalender-Follow-up erstellen

Connectoren

3 konfiguriert

Status, Ausführungsmodus, Umgebung und Geltungsbereich für connector-gestützte Aktionen.

Microsoft Graph / SharePoint

graph-sharepoint-primary • Microsoft Graph / SharePoint

Aktiviert Mock Aktualität: Fresh

Name Connector-Typ

Microsoft Graph / SharePoint Microsoft Graph / SharePoint

Beschreibung

Status Ausführungsmodus

Aktiviert Mock

Environment Fixture-Referenz

Jira

jira-primary • Jira

Aktiviert Mock Aktualität: Alternd

Name Connector-Typ

Jira Jira

Beschreibung

Status Ausführungsmodus

Aktiviert Mock

Environment Fixture-Referenz

Custom environment delivery-board

Projektintegrationen

Diese Registerkarte trennt technisch definierte **Plattformintegrationen** von denen, die tatsächlich vom Projekt nutzbar sind.

Wie Sie diese Registerkarte lesen

Projektintegrationen ist nicht der Ort, an dem die vollständige technische Konfiguration des gesamten Tenants vorgenommen wird. Die Registerkarte dient vor allem dazu, die operative Einsatzbereitschaft des Projekts zu lesen: was dieses Projekt sehen kann, was bereit ist und was mit expliziter Ursache blockiert bleibt.

Sie können dort typischerweise mehrere Informationsfamilien ablesen:

- **Ausführungs-Connectoren**: gesteuerte Ausführungsoptionen zu externen Systemen;
- **Ingestionsanbieter**: Importquellen, die anschließend von **Wissen** genutzt werden;
- **Transparenz der KI-Laufzeit**: effektiver KI-Anbieter und der beim Deployment ausgewählte Anbieter;
- **Lizenz- und Sitzplatzstatus**: sichtbarer aktiver Plan, gekaufte Lizenzen, genutzte Lizenzen und verfügbare Sitzplätze.

Was der Bildschirm „Projektintegrationen“ zeigt

Der Bildschirm trennt technische Readiness von Projektverfügbarkeit:

- Plattform-Setup, Projektbindung, Policy, Permission, Health und Lizenzverfügbarkeit für den App-Zugriff sind **getrennte Ursachen**. Ein Connector kann schreibgeschützt sichtbar bleiben, damit das Projektteam versteht, warum er blockiert ist, statt anzunehmen, dass er fehlt;
- die technische Konfiguration bleibt in **Plattformadministration**. Projektverantwortliche können aktivierte und bereite Integrationen binden, während Tenant-URLs, Authentifizierungsstrategie, API-Schlüssel und Secret-Referenzen zentral kontrolliert bleiben.

BEREICH	WAS SICHTBAR SEIN KANN	WIE HANDELN
Ausführungs-Connectoren	eine aktuelle Liste, die auch leer sein kann, plus ein Katalog Available to bind mit Asta Powerproject schedule sync, Azure DevOps delivery project, Jira delivery workspace, Microsoft Project schedule sync, Microsoft Teams collaboration, Outlook executive notifications, SharePoint publication library, Smartsheet portfolio workspace, Webhook event delivery und Wrike delivery workspace	Bind to project nur für Connectoren verwenden, die auf Plattformebene bereits aktiviert und bereit sind
Ingestionsanbieter	Anbieter wie Smartsheet sheet import und Azure Data Factory evidence pipeline mit Status Healthy , plus verfügbare Anbieter wie SharePoint knowledge import, Azure Blob document ingest, Confluence knowledge import, Jira issue import, SFTP document intake, Microsoft Project schedule import, Wrike task import und Asta Powerproject schedule import	Validate binding zur erneuten Prüfung eines gebundenen Anbieters, Disable zum Schließen auf Projektebene oder Bind to project für einen genehmigten Anbieter verwenden

Anbieterkarten können **Ready**, **Healthy** oder **Not configured** anzeigen. **Not configured** bedeutet, dass der Anbieter im Plattformkatalog existiert, aber Quelle, Zugangsdaten oder Readiness-Prüfung noch fehlen, bevor das Projekt ihn nutzen kann. Für Pflichtfelder, Probes, Aktions-Mapping und Grenzen der Live-Ausführung nutzen Sie [Connectoren und Integrationen](#). **Ready** oder **Healthy** bedeutet kohärente Vorbereitung, beweist aber für sich allein nicht, dass ein vollständiges externes Ticket, eine Nachricht oder ein Import bereits ausgeführt wurde.

Angezeigte Blockierungsgründe

Eine Projektintegration oder eine Importoption kann aus folgenden Gründen blockiert sein:

- Policy;
- Permission;
- zu prüfender Gesundheitszustand;
- fehlende oder deaktivierte Plattformdefinition;
- fehlende oder nicht konfigurierte Projektbindung;
- unvollständige anbieterspezifische Konfiguration oder Validierung.

Wie man eine Bindungsblockade interpretiert

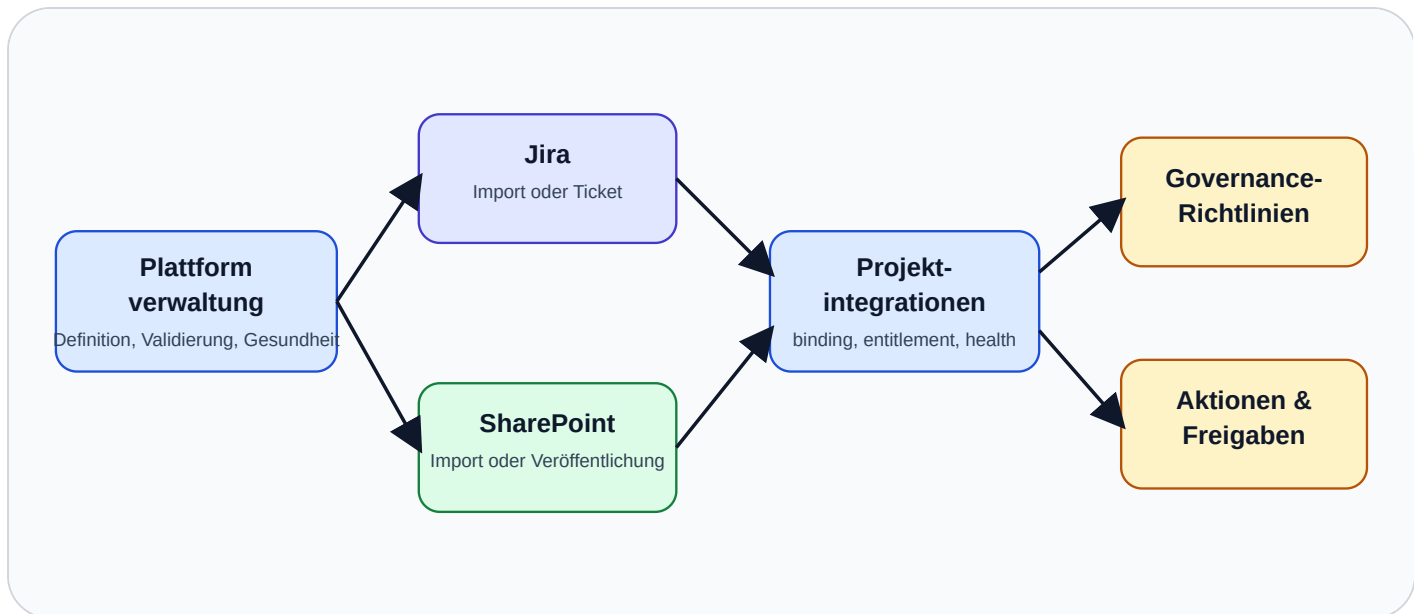
SICHTBARE URSACHE	PRAKTISCHE LESUNG	EMPFOHLENE REFLEXION
entitlement	Legacy-Bezeichnung für eine blockierte Integration, kein Funktionsunterschied zwischen Marketplace-Plänen	Konfiguration, Validierung, Health, Binding, Policy, Rolle und Lizenzverfügbarkeit bei Zugriffsproblemen prüfen
policy	Die Projektgovernance verbietet oder limitiert diesen Fluss	Lesen Sie Governance-Richtlinien vor der Änderung der Bindung
permission	Der Connector existiert, aber Ihre Rolle erlaubt es nicht, ihn zu aktivieren oder zu nutzen	Prüfen Sie die Projektkontrolle in Zugriffskontrolle und Rollen Projekt
health	Die Plattformdefinition existiert, aber ihre Vorbereitung oder Verfügbarkeit erfordert Prüfung	Öffnen Sie die Plattformadministration zur Bestätigung der technischen Definition
fehlende oder deaktivierte Definition	Nichts ist auf Tenant-Ebene wirklich bereit	Bitten Sie zunächst um Einrichtung oder Reaktivierung der Plattform
fehlende oder nicht konfigurierte Projektbindung	Die Plattform ist bereit, aber das Projekt nutzt die Integration noch nicht	Aktivieren Sie die Bindung explizit auf Projektebene

Praktische Bedeutung von **binding** und Lizenzierung

- **binding** bedeutet, dass der Connector oder Anbieter auf Plattformebene existiert, aber erst noch mit dem Projekt verknüpft und für dieses Projekt freigegeben werden muss, bevor das Projekt ihn nutzen kann;
- **Lizenzierung** bestimmt, ob ein Benutzer einen verfügbaren Sitzplatz für den App-Zugriff hat. Marketplace-Pläne schalten keine unterschiedlichen Connector-Familien frei oder aus;
- ein sichtbarer, aber blockierter Connector ist daher nicht automatisch defekt: Die Oberfläche kann ihn gerade deshalb sichtbar lassen, um die Blockierungsursache zu erklären.

Wenn eine Blockade anhält, öffnen Sie anschließend **Plattformadministration**, um die technische Definition zu prüfen, und kehren Sie zum Projekt zurück, um die Bindung und Vorbereitung zu bestätigen.

Jira, SharePoint und Connector-Kette



Halten Sie diese Logik einfach:

1. **Plattformintegrationen** definieren den Connector oder den Ingestionsanbieter;
2. **Projektintegrationen** zeigen nur die genehmigten und bereitgestellten Bindungen;
3. **Governance-Richtlinien** entscheiden, welche Rolle beobachten, vorbereiten, vorschlagen oder ausführen kann;
4. **Aktionen & Genehmigungen** wenden diese Regeln bei der tatsächlichen Anfrage an;
5. **PM-Dokumente** und **KI-Log** behalten die Spur des Flusses.

Siehe die zugehörige Seite: [Connectoren und Integrationen](#).

Aktionen & Genehmigungen

Diese Registerkarte wandelt eine Empfehlung in eine kontrollierte Operation um. Eine Aktion kann **sichtbar** aber nicht **ausführbar** sein, wenn:

- Sie haben nicht die richtige Berechtigung;
- Der kompatible Connector ist nicht bereit;
- Die Projektbindung begrenzt die Aktion;
- Die erforderliche Genehmigung wurde noch nicht erteilt.

Die zentralen Zustände, die Sie unterscheiden sollten

In der Oberfläche unterscheiden Warteschlange und Übersichtskarten vor allem vier kanonische Lesarten:

SICHTBARER ZUSTAND	PRAKTISCHE LESART
Execution prerequisites	kompatible Connectoren können existieren, aber die Ausführung bleibt durch Health, Konfiguration, Binding, Permission, Policy, Genehmigung oder fehlende Readiness blockiert
Pending approval	die Anfrage wurde vorgeschlagen und wartet noch auf eine Governance-Entscheidung
Ready to execute	die Anfrage ist bereits approved , die eigentliche Ausführung bleibt aber ein eigener Schritt
Executed history	die Aktion wurde tatsächlich ausgeführt und bleibt als Verlauf bzw. Audit-Nachweis sichtbar

Eine Anfrage kann also **approved** sein, ohne bereits **executed** zu sein.

Wie Sie eine Registerkarte lesen, die leer oder unvollständig wirkt

Die bloße Sichtbarkeit der Registerkarte bedeutet nicht, dass bereits eine Aktion ausführbar ist. Wenn nichts Konkretes sichtbar wird, ist die nützlichste Lesart oft:

1. kein **kompatibler und gesunder Ausführungs-Connector** ist für diesen Aktionstyp bereit;
2. die **Projektbindung** macht die Option im Projekt noch nicht sichtbar;
3. eine **Policy** erlaubt die Ansicht, aber nicht Vorschlag oder Ausführung;
4. Ihre **Permission** erlaubt das Anzeigen der Warteschlange, nicht aber das Handeln;
5. eine Genehmigung ist erforderlich und es wurde noch keine Entscheidung getroffen.

Wenn alles korrekt vorbereitet ist, sollte mindestens Folgendes sichtbar oder erfüllbar sein:

- ein kompatibler Aktionstyp;
- mindestens eine gesunde Ausführungsoption;
- eine gültige Projektbindung;
- eine kohärente Policy;
- ein Benutzer, der je nach Fall vorschlagen, genehmigen oder ausführen darf.

Nur-Lese oder Zugriff verweigert

- **Nur-Lese:** Die Registerkarte bleibt sichtbar, aber das Speichern ist blockiert;
- **Zugriff verweigert:** Die Route oder Aktion ist für Ihr Konto nicht verfügbar.

Dieser Unterschied ist besonders wichtig für **Zugriffskontrolle**, **Projektintegrationen** und die Governance-Einstellungen.

Empfohlener Ablauf nach Projekterstellung

1. Öffnen Sie den **Arbeitsbereich**;
2. Prüfen Sie zunächst den **Ersteller**, die **Mitglieder** und die **Rollen**, wenn das Projekt kollaborativ ist;
3. Passen Sie anschließend die **Dokumentenkategorien** an;
4. Lesen Sie die **Governance-Richtlinien** vor jeder externen Veröffentlichung;
5. Verbinden Sie ausschließlich die tatsächlich bereitgestellten **Projektintegrationen**;
6. Laden Sie anschließend die **Wissen**;
7. Gehen Sie schließlich zu **Agenten**, **PM-Dokumenten** und **Aktionen & Genehmigungen**.

Zwei nützliche Konfigurationsszenarien

Szenario 1 – neues Projekt minimal

Für ein Projekt, das startet, behalten Sie eine einfache Reihenfolge:

1. Fügen Sie die notwendigen Mitglieder hinzu und prüfen Sie deren Rollen;
2. Erstellen Sie eine kurze Dokumenten-Taxonomie in **Dokumentenkategorien**;
3. Aktivieren Sie nur die bereits validierten und wirklich notwendigen Integrationen;
4. Bereiten Sie eine minimale Governance vor, z. B. einen internen Digest und ein Standard-Artefaktziel;
5. Laden Sie anschließend die **Wissen** vor dem Öffnen der Agenten.

Dieses Szenario verhindert, dass zu früh Connectoren oder Verteilungsregeln verwendet werden, die sofort nicht genutzt werden.

Szenario 2 - sensibles Projekt / gesteuerte Veröffentlichung

Für ein Projekt, das externe Benachrichtigungen oder eine formelle Dokumentenveröffentlichung ausgesetzt ist:

1. Beschränken Sie Rollen, die Zugriff auf externe Connectoren haben;
2. Bereiten Sie ein SharePoint- oder Äquivalentziel in **Artefaktziele** vor;
3. Wenden Sie `require_approval` auf die Aktionsstufen an, die externe Veröffentlichung erzeugen können;
4. Bevorzugen Sie `signal_digest` für die aktuelle Nachverfolgung und reservieren Sie sofortige Alarmer für kritische Fälle;
5. Machen Sie in **Projektintegrationen** nur die Bindungen sichtbar, deren Vorbereitung und Politik bereits konform sind.

Dieses zweite Szenario richtet die Signalüberwachung, Veröffentlichung, Genehmigung und reale Ausführung aufeinander ab, anstatt das Team jede Oberfläche als unabhängige Fläche zu behandeln.

Weiter

- [Zugriffskontrolle und Rollen Projekt](#)
- [Wissen und Agenten](#)
- [Governance, Entscheidungen und Aktionen](#)
- [Connectoren und Integrationen](#)
- [Portfolio und technische Administration](#)

Zugriffskontrolle und Projektrollen

[Startseite](#) · Zugriffskontrolle und Projektrollen

Projektzugriff steuern

Weisen Sie zuerst Rollen zu und verengen Sie den Umfang nur bei begründetem Bedarf.

1

Mitglieder

Fügen Sie Benutzer oder Gruppen zum aktiven Projekt hinzu.

2

Standardrollen

Beginnen Sie mit Owner, Manager, Contributor, Reader oder Auditor.

3

Benutzerdefinierte Rollen

Nutzen Sie sie nur, wenn Standardrollen nicht passend sind.

4

RBAC-Garde-fous

Verhindern Sie Selbstsperre, unerwartete Erhöhung und Policy-Umgehung.

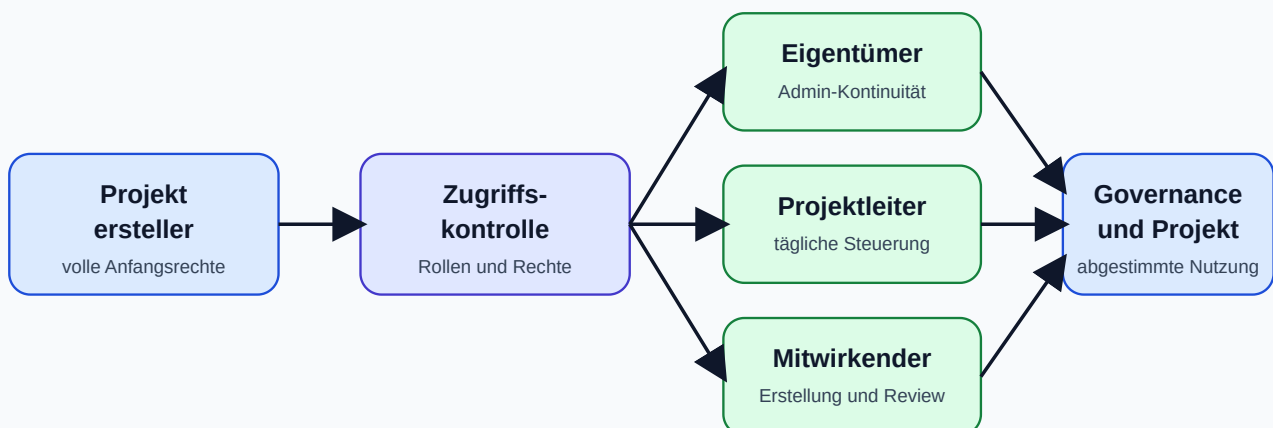
5

Audit-Spur

Speichern Sie, wer Zugriff geändert hat, wann und warum.

Wenn ein Button deaktiviert ist, prüfen Sie Rolle, Policy und Integration

Blockaden kommen meist von Projektrolle, RBAC-Regel oder Integrationsbindung.



Ziel

Die **Zugriffskontrolle** ist der RBAC-Bereich auf Projektebene. Sie ermöglicht es, zu entscheiden:

- wer in das Projekt eintritt;
- welche Rolle jedes Mitglied erhält;
- welche benutzerdefinierten Rollen in diesem Projekt existieren;
- welche Berechtigungen diese Rollen gewähren.

Warum ist das wichtig

Die Rechte bestimmen einen großen Teil der Erfahrung: Ausführung von Agenten, Verwaltung von Mitgliedern, Generierung von Lieferobjekten, Konfiguration von Integrationen, Governance von Veröffentlichungen und Audit-Lesen. Eine korrekte Rollen-Lesung verhindert, dass ein funktionaler Block als fehlende Autorisierung missverstanden wird.

Wer kann diese Seite nutzen

- **Mitglieder und Rollen einsehen:** jedes Mitglied, das auf den Arbeitsbereich zugreifen kann;
- **Mitglieder verwalten:** Benutzer mit `members:manage` ;
- **Benutzerdefinierte Rollen verwalten:** Benutzer mit `roles:manage` .

Ersteller des Projekts: Anfangsrolle und Delegation

Bei der Projekterstellung startet der Ersteller mit der Rolle **Projektinhaber** und allen verfügbaren Projekt-Berechtigungen. Er dient somit als administrativer Ausgangspunkt: Er öffnet das Projekt, prüft die Anfangskonfiguration und delegiert anschließend die nützlichen Rollen an andere Mitglieder.

Empfohlene Delegation

1. behalten Sie den Ersteller als ersten administrativen Wächter;
2. vergeben Sie einen zweiten **Projektinhaber**, falls das Projekt nicht von einer einzigen Person abhängig sein soll;
3. nutzen Sie **Projektleiter** für die tägliche Steuerung;

4. reservieren Sie benutzerdefinierte Rollen für echte Bedarfsschwankungen;
5. prüfen Sie anschließend **Governance-Politiken** und **Projekt-Integrationen**, damit die Rechte den externen Nutzungen entsprechen.

Was diese Seite bestätigt

- der Ersteller kann nicht von diesem Bildschirm entfernt werden;
- die Rolle des Erstellers bleibt fest;
- ein Benutzer kann sich nicht selbst zurückstufen oder selbst löschen von dieser Oberfläche;
- die Rollen-Delegation ist bestätigt;
- der freie Transfer des **Ersteller-Status** ist in den Administrationsbildschirmen nicht direkt angeboten.

Standardrollen

Jedes Projekt startet mit integrierten, geschützten Rollen:

ROLLE	TYPISCHE NUTZUNG
Projekthinhaber	Vollständige Projekt-Administration
Projektleiter	Tägliche operative Steuerung
Mitwirkender	Inhaltserstellung, Nutzung von Agenten und Lieferobjekten je nach Berechtigungen
Leser	Nur-Lesen-Zugriff
Auditor	Audit-orientierter Zugriff und Nachverfolgbarkeit

Diese integrierten Rollen sind serverseitig geschützt und können von der Oberfläche nicht gelöscht werden.

Schnelle Rollen-Matrix

Benutzerdefinierte Rollen können dieses Schema erweitern oder reduzieren. Die folgende Tabelle beschreibt das **typische Verhalten** der Standardrollen.

HÄUFIGE AKTION	PROJEKTINHABER	PROJEKTLEITER	MITWIRKENDER	LESER
Zugriff auf Projekt, Arbeitsbereich und Leseseiten	Ja	Ja	Ja	Ja
Suchen in Wissen, PM-Dokumente und KI-Journal erneut lesen	Ja	Ja	Ja	Ja
Einen Run in Agenten starten	Ja	Ja	Ja	Standardmäßig nein
Arbeitsinhalte und Entwürfe von Lieferobjekten ändern	Ja	Ja	Ja	Nein
Mitglieder, Rollen und Hauptprojekt-Einstellungen verwalten	Ja	Nein	Nein	Nein
Audit-orientierte Durchsicht	Ja	Ja	Ja	Nur-Lesen

Benutzerdefinierte Rollen

Das Produkt unterstützt die Erstellung, Bearbeitung und Löschung von **benutzerdefinierten Rollen** auf Projektebene.

Verfügbare Berechtigungen

Die exponierten Berechtigungen umfassen unter anderem:

- project:read
- project:update
- agent:run
- agent:configure
- documents:read
- documents:upload
- documents:delete
- report:generate
- history:read
- members:read

- `members:manage`
- `roles:manage`
- `settings:manage`

Berechtigung → konkreter Einfluss

BERECHTIGUNG	BETROFFENE OBERFLÄCHE	SYMPTOM BEI FEHLENDER BERECHTIGUNG
<code>agent:configure</code>	Tab Agenten-Konfiguration im Arbeitsbereich	Die Seite bleibt nur lesbar oder die Speichern-Kontrollen sind deaktiviert
<code>report:generate</code>	Erstellung von Entwürfen, Artefakten und PM-Dokumenten	Der Benutzer kann lesen, aber nicht das erwartete Lieferobjekt generieren
<code>history:read</code>	KI-Journal und detaillierte Run-Lesung	Die Nachverfolgbarkeit bleibt unzugänglich oder stark eingeschränkt
<code>settings:manage</code>	Projekt-Einstellungen, Governance und einige Integrationen	Die Parameter sind sichtbar, aber nicht veränderbar
<code>members:manage</code>	Bereich Mitglieder in Zugriffskontrolle	Hinzufügen, Entfernen oder Ändern eines Mitglieds ist unmöglich
<code>roles:manage</code>	Benutzerdefinierte Rollen und deren Berechtigungen	Erstellen, Anpassen oder Löschen einer benutzerdefinierten Rolle ist unmöglich

Diese Tabelle dient vor allem dazu, das Verhalten der Oberfläche korrekt zu lesen: Eine fehlende oder ausgegraute Aktion deutet oft auf eine nicht gewährte Berechtigung hin.

Projektbesitzer Integriert

Vollzugriff auf das Projekt.

Projekt anzeigen
Projekt bearbeiten
Dokumente anzeigen
Dokumente hochladen
Dokumente löschen
Dokumente suchen
PM-Dokumente anzeigen
PM-Dokumente bearbeiten

+6 weitere

☒ Projekt anzeigen Projektarbeitsbereich und Metadaten anzeigen.	☒ Projekt bearbeiten Projektdaten und -konfiguration bearbeiten.
☒ Dokumente anzeigen Projektdokumente und Wissen anzeigen.	☒ Dokumente hochladen Projektdokumente hochladen.
☒ Dokumente löschen Projektdokumente löschen.	☒ Dokumente suchen Projektdokumente und Wissen durchsuchen.
☒ PM-Dokumente anzeigen Projektmanagement-Dokumente anzeigen.	☒ PM-Dokumente bearbeiten Projektmanagement-Dokumente bearbeiten.
☒ PM-Dokumente exportieren Projektmanagement-Dokumente exportieren.	☒ Agenten ausführen Projektagenten und Assistenten-Workflows ausführen.
☒ Agenten konfigurieren Agenten und Projektparameter konfigurieren.	☒ RBAC anzeigen Rollenbasierte Zugriffskontrolleinstellungen anzeigen.
☒ RBAC verwalten Rollenbasierte Zugriffskontrolleinstellungen verwalten.	☒ Manage project settings Manage project-level settings (categories, configs).

Integrierte Rollen sind schreibgeschützt. Erstellen Sie eine benutzerdefinierte Rolle, wenn Sie andere Berechtigungen benötigen.

Was Sie auf der Seite sehen

Die Seite ist in zwei Arbeitsbereiche unterteilt:

1. Rollen und Berechtigungen

- Überprüfung der integrierten Rollen;
- Erstellung von benutzerdefinierten Rollen;
- Inspektion oder Bearbeitung der Berechtigungen einer benutzerdefinierten Rolle;

2. Mitglieder

- Hinzufügen eines Mitglieds per E-Mail;
- Zuweisung einer integrierten oder benutzerdefinierten Rolle;
- Rollenwechsel;
- Löschen eines Mitglieds, wenn dies noch erlaubt ist.

Die Seite kann auch Ihre aktuelle Identität anzeigen und, wenn sie exponiert ist, den geschützten Eintrag des **Erstellers** des Projekts.

Empfohlener Ablauf

Rollen vor dem Hinzufügen eines Mitglieds prüfen

1. öffnen Sie **Arbeitsbereich**;
2. wählen Sie den Tab **Zugriffskontrolle**;

3. lesen Sie die vorhandenen Rollen erneut;
4. prüfen Sie, ob eine Standard-Rolle ausreicht oder ob eine benutzerdefinierte Rolle nötig ist.

Eine benutzerdefinierte Rolle erstellen

1. öffnen Sie **Rollen und Berechtigungen**;
2. geben Sie einen **Namen** ein;
3. fügen Sie ggf. eine **Beschreibung** hinzu;
4. erstellen Sie die Rolle;
5. aktivieren oder deaktivieren Sie die gewünschten Berechtigungen;
6. prüfen Sie die angezeigten Badges oder Berechtigungen vor echter Nutzung.

Ein Mitglied hinzufügen oder aktualisieren

1. öffnen Sie **Mitglieder**;
2. geben Sie die **E-Mail** ein;
3. wählen Sie die gewünschte Rolle;
4. speichern;
5. prüfen Sie, ob die Zeile des Mitglieds die erwartete Rolle widerspiegelt.

Wenn der Benutzer zu einem anderen Mandanten gehört, denken Sie daran, dass ein **externer / Gast-Benutzer** zuerst in der Identität eingeladen werden muss, bevor das Projekt-RBAC ihm eine nützliche Rolle zuweisen kann.

Die Rolle eines bestehenden Mitglieds ändern

1. finden Sie die Zeile des Mitglieds in **Mitglieder**;
2. benutzen Sie den Rollen-Auswahl-Filter dieser Zeile;
3. wählen Sie die neue Rolle;
4. bestätigen Sie, dass die Zeile die aktualisierte Rolle anzeigt.

Ein Mitglied entfernen

1. finden Sie die Zeile des zu entfernenden Mitglieds;
2. benutzen Sie die Lösch-Aktion, falls verfügbar;
3. bestätigen Sie, dass das Mitglied aus der Liste verschwindet;

4. wenn die Aktion weiterhin blockiert, prüfen Sie zuerst, ob es sich nicht um Ihr eigenes Konto oder um den geschützten Eintrag des Erstellers handelt.

Bestätigte RBAC-Sicherheitsmechanismen

Die Oberfläche und die Plattform-Services setzen mehrere wichtige Schutzmaßnahmen um:

- Sie können **nicht** Ihr eigenes Zugangs-Token von diesem Bildschirm entfernen;
- Sie können **nicht** Ihre eigene Rolle von diesem Bildschirm ändern;
- Der Eintrag des **Erstellers** des Projekts bleibt geschützt;
- Eine **System-Rolle** kann nicht gelöscht werden;
- Eine **benutzerdefinierte Rolle**, die noch zugewiesen ist, kann nicht gelöscht werden;
- Benutzer ohne Verwaltungsrechte sehen eine **lesbare** Seite mit deaktivierten Kontrollen.

Nur-Lesen vs Zugriff verweigert

Diese beiden Zustände bedeuten nicht dasselbe:

- **Nur-Lesen:** Die Seite bleibt sichtbar, aber die Kontrollen zum Hinzufügen, Bearbeiten oder Löschen sind deaktiviert;
- **Zugriff verweigert:** Die Route oder Aktion ist für Ihr Konto nicht verfügbar.

In der Praxis ermöglicht dies, dass einige Profile die RBAC-Konfiguration erneut lesen können, ohne sie zu ändern.

Wie ein Verweis gelesen wird

WAS SIE BEOBACHTEN	WAHRSCHEINLICHSTE INTERPRETATION	EMPFOHLENE REAKTION
ein sichtbarer, aber ausgegrauter Kontroll	Oberfläche in Nur-Lesen	Prüfen Sie zuerst, ob Ihre Rolle die erwartete Berechtigung enthält
eine Aktion fehlt, obwohl sie für andere vorhanden ist	Berechtigung oder Rolle fehlt	Vergleichen Sie Ihre Standard- oder benutzerdefinierte Rolle mit der erwarteten Aktion

WAS SIE BEOBACHTEN	WAHRSCHEINLICHSTE INTERPRETATION	EMPFOHLENE REAKTION
eine Aktion ist sichtbar, aber unmöglich trotz UI	RBAC-Sicherheit auf Server-Seite oder Schutz-Beschränkung	Prüfen Sie, ob es sich um eine System-Rolle, Ihr eigenes Konto oder einen geschützten Eintrag handelt

Was der Ersteller praktisch delegiert

BEDARF	ROLLE ZUERST ZU VERGEBEN	WARUM
administrative Kontinuität	Projekthinhaber	Vermeiden, dass ein einzelner Account die gesamte Administration konzentriert
tägliche Steuerung	Projektleiter	Verwalten der laufenden Arbeit ohne die gesamte Administration zu öffnen
Inhaltserstellung und Agenten-Nutzung	Mitwirkender	Ausführen von Agenten und Vorbereitung von Lieferobjekten
breite Lesbarkeit	Leser	Nur-Lesen-Zugriff ohne Änderungsrisiko
Audit und Nachverfolgbarkeit	Auditor	Historie und Beweise erneut lesen ohne das Projekt zu beeinflussen

Häufige Probleme

Nicht möglich, eine benutzerdefinierte Rolle zu löschen

Prüfen Sie zuerst, ob diese Rolle noch einem Mitglied zugewiesen ist. Solange sie verwendet wird, bleibt die Löschung blockiert.

Nicht möglich, meine eigene Rolle zu ändern

Dieses Verhalten ist beabsichtigt, um einen versehentlichen Zugriffverlust zu verhindern. Bitten Sie einen anderen Projekt-Administrator, die Änderung durchzuführen.

Tab ist sichtbar, aber alles ausgegraut

Sie befinden sich wahrscheinlich in **Nur-Lesen** auf dieser Oberfläche. Prüfen Sie, ob Ihre Rolle `members:manage` oder `roles:manage` enthält.

Tipps

- nutzen Sie **Projektinhaber** nur für echte Projekt-Administratoren;
- halten Sie benutzerdefinierte Rollen gezielt und begrenzt auf einen konkreten Bedarf;
- lesen Sie die Berechtigungen vor der Delegation von Mitglieder-Verwaltung;
- dokumentieren Sie benutzerdefinierte Rollen in den Team-Praktiken, um Duplikate zu vermeiden.

Weiter

- [Projekte und Arbeitsbereich](#)
- [Governance, Entscheidungen und Aktionen](#)
- [Connectoren und Integrationen](#)
- [Wartung, Support und FAQ](#)

Wissen und Agenten

[Startseite](#) · Wissen und Agenten

ProPM Agent
KI-Liefercockpit

AKTUELLES PROJEKT
Azure Bay Hotel & Convention Center
Arbeitsbereich öffnen

Dashboard
Projekte
Arbeitsbereich
Wissensbasis
Agenten
Berichte & Artefakte
KI-Protokoll
Portfolio-Leitstand
Plattformadministration

Benutzer
mockuser@contoso.c...

Azure Bay Hotel & Convention Cent ⓘ ⌵ Drücken Sie Strg+K / ⌘K für Befehle Ozean Deutsch Hilfe Status

Wissensbasis

Vorbereitete Projektnachweise, Demo-Verarbeitungsstände und kontextbezogene Suche für Azure Bay Hotel & Convention Center

HILFE Hilfe

Wissens-Übersicht
Auf der Wissensseite laden Benutzer Dateien hoch, importieren Quellen, durchsuchen Inhalte und suchen nach Evidenz.

Wissens-Übersicht Dokument-Upload Upload a local file Importquellen Import from an approved source Wissenssuche

Wie Knowledge-Status und Metadaten zu lesen sind
Indexed bedeutet durchsuchbar, Ingesting bedeutet, dass das Element existiert, die Suchbarkeit aber noch nachziehen kann, und Failed bedeutet, dass Support oder ein neuer Versuch noetig ist. Source label und source system helfen bei der Herkunftsbewertung, waehrend Trace ID vor allem ein Support- und Audit-Schlüssel und kein alltaeglicher Funktionsschlüssel ist.

Auch im Demo-Modus bleibt Knowledge projektspezifisch. Nutzen Sie die vorbereiteten Dokumente, simulieren Sie einen Upload und suchen Sie dann nach evidenzgestützten Snippets, bevor Sie Inhalte anderweitig verwenden.

Vorbereitete Projekt-Wissensbasis durchsuchen ⓘ

Prüfen Sie Snippets, Quellverweise und Frischehinweise, bevor Sie Evidenz in Artefakte überführen.

Nach Dateinamen, Kategorien oder Status suchen... Suchen

Noch keine Ergebnisse.

Dokumente suchen... General 6 angezeigt Demo-Dokument hochladen Bibliothek aktualisieren

Dateiname	Kategorie	Quelle	Status	Aktualisiert	Aktionen
-----------	-----------	--------	--------	--------------	----------

Ziel

Diese Seite erklärt, wie man Dokumente hochlädt oder importiert, die in **Wissen** sichtbaren Metadaten erneut liest und den Projektkontext in **Agenten** nutzt.

Wissen: Was Sie tun können

Verfügbare Fähigkeiten:

- Suche in den Projektinhalten;
- Manuelles Hochladen;
- Aktualisierung der Daten;
- Import aus genehmigten Quellen;
- Durchsicht des Importverlaufes;
- Sortieren, Filtern und Paginieren der Ergebnisse.

Unterstützte Dateitypen

Die explizit akzeptierten Dateitypen in der Oberfläche umfassen unter anderem:

- **PDF;**
- **DOCX, ODT, RTF, TXT, Markdown;**
- **CSV, XLSX, XLSM, ODS;**
- **JSON, XML;**
- **PPTX, ODP;**
- **HTML / HTM;**
- **EML, EPUB;**
- **PNG, JPG, JPEG, BMP, TIFF, HEIF.**

Import aus genehmigten Quellen

Der Importmechanismus hängt von den auf Plattformebene validierten **Ingestionsanbietern** ab, die anschließend dem Projekt zur Verfügung gestellt werden.

Was der Importauswahl-Dialog zeigt

Je nach Quelle kann die Oberfläche Folgendes anzeigen:

- den Namen der Quelle;
- ein lesbares **Source Label**;
- das Datum des letzten Imports;
- einen Frische- oder Gesundheitsstatus;
- eine Blockierungsbeschreibung, wenn die Quelle nicht nutzbar ist.

Wann ein Import blockiert ist

Eine Importoption kann aus folgenden Gründen nicht verfügbar sein:

- fehlende Rechte;
- restriktive Richtlinie;
- zu prüfender Verfügbarkeits- oder Gesundheitszustand;
- fehlende oder nicht bereite Projektbindung;
- unvollständige Anbieterkonfiguration.

Importverlauf

Der Importverlauf ermöglicht es, mindestens Folgendes zu überprüfen:

- den angezeigten Namen des Anbieters;
- den Status des Runs;
- die Frische nach dem Import;
- die [Trace ID](#);
- die entdeckten, importierten, ignorierten oder als fehlgeschlagen gemeldeten Volumen;
- das Abschlussdatum, falls verfügbar.

Dokumentenliste und Suche

Sichtbare Dokumentenstatus

Die Dokumententabelle zeigt mindestens die folgenden Status:

- **Indexed**;
- **Ingesting**;
- **Failed**.

Ein sichtbares Dokument, das noch nicht in der Suche gefunden werden kann, befindet sich oft noch in der Phase **Ingesting**.

Sichtbare Metadaten in Suchergebnissen

Suchergebnisse können Folgendes anzeigen:

- Titel;
- Auszug;
- Score;
- Abschnitt;
- Frische-Badge;
- Badge **source system**;
- Badge **source label**;
- Link **Open source**;
- [Trace ID](#) der Suche.

Praktische Lesart:

- **source label** bezeichnet meist den sichtbaren Provider oder die Herkunft der Ingestion, z. B. **manual**, **SharePoint**, **ADF**, **Blob**, **Confluence** oder **Jira**;
- **source system** hilft dabei, das lesbare System oder den fachlichen Strom hinter diesem Beleg zu erkennen, z. B. **Knowledge**, **Schedule**, **Finance** oder **Operations**;
- die Such- **Trace ID** ist vor allem ein Diagnose-, Support- und Audit-Hinweis, nicht der übliche fachliche Schlüssel des Alltags.

Verwenden Sie **source label** und **source system** zusammen, wenn Sie die Herkunft eines Auszugs schnell vor seiner Wiederverwendung einschätzen müssen.

Vorbereitete Projekt-Wissensbasis durchsuchen

Suchen

Prüfen Sie Snippets, Quellverweise und Frischehinweise, bevor Sie Evidenz in Artefakte überführen.

Trace-ID: trace-demo-search-1776779552502

Trace ID is mainly for diagnosis and support, not for everyday business interpretation.

ABH-Risk-Register-v1.2.xlsx

Aktuell

ADF managed pipeline

ADF

Risk Register

Score: 0.95

ABH-Risk-Register-v1.2.xlsx ist unter Risk Register abgelegt. Der aktuelle Verarbeitungsstatus ist Indexiert, und die letzte Demo-Aktualisierung wurde am 21/04/2026 14:28:30 erfasst.

Risk Register Aktualisiert 21/04/2026 14:28:30

/documents?projectId=demo-hotel-001#doc-002 [Quelle öffnen](#)

ProPM Agent

KI-Liefercockpit

AKTUELLES PROJEKT

Azure Bay Hotel & Convention Center

Arbeitsbereich öffnen

Dashboard

Projekte

Arbeitsbereich

Wissensbasis

Agenten

Berichte & Artefakte

KI-Protokoll

Portfolio-Leitstand

Plattformadministration

Benutzer

mockuser@contoso.c...

selected project, and keep transverse or custom agents for cases where the domain coverage really fits.

SEARCH ROSTER

Agenten suchen...

default

all-projects

aktiviert

Schedule Lead

Establishes timelines, sequences work, and supports the coordination of activities...

default

all-projects

aktiviert

Finance Steward

Manages budgeting, cost performance, financial stewardship, and investment...

default

all-projects

aktiviert

Stakeholder Engagement Lead

Engages individuals and groups to support shared understanding, collaboration, and...

default

all-projects

aktiviert

Resource Manager

Plans and manages people, materials, tools, and facilities required for project...

default

all-projects

aktiviert

Risk Manager

Addresses uncertainty, threats, and opportunities through proactive planning...

default

all-projects

aktiviert

Holistic View: Focus on Value; Embed Quality; Be an Accountable Leader; Integrate Sustainability; Build an Empowered Culture.

AKTUELLES PROJEKT

Azure Bay Hotel & Convention Center

Art: default

Geltungsbereich: all-projects

Status: aktiviert

Domänen: Risk

Kind tells you whether the card is standard or custom, scope tells you where it can be used, status tells you whether it is currently available, and domains tell you what work it is meant to cover.

Chats

Neu

Chats suchen...

Construction risk review

21 apr, 2026, 13:33

2 Nachrichten

Umbenennen

Löschen

Risk Manager Nicht verfügbar

Die Sprachengabe ist in diesem Browser bereit.

Verwenden Sie das Mikrofon, um Sprachangaben an den Composer anzuhängen, und senden Sie erst, wenn der Prompt passend aussieht.

Update top 5 construction risks for the next two weeks with owners and mitigations.

13:29

Risk Manager

Top risks (2-week horizon):

1) Utility relocation delays (Owner: Construction Manager)

2) Chiller delivery slippage (Owner: Procurement Lead)

3) Skilled labor shortage (Owner: Contractor PM)

4) Late authority inspections (Owner: Permitting Lead)

5) Access road conflict (Owner: Site Logistics Lead)

Mitigation cadence: daily site sync + weekly RAID review.

Tokens: 562

Trace-ID: trace-demo-hotel-risk-001

Unified run flow

Chat -> Run -> Structured output -> Artifact -> PM Doc -> Knowledge

Open Knowledge

Agenten: Rolle der Seite

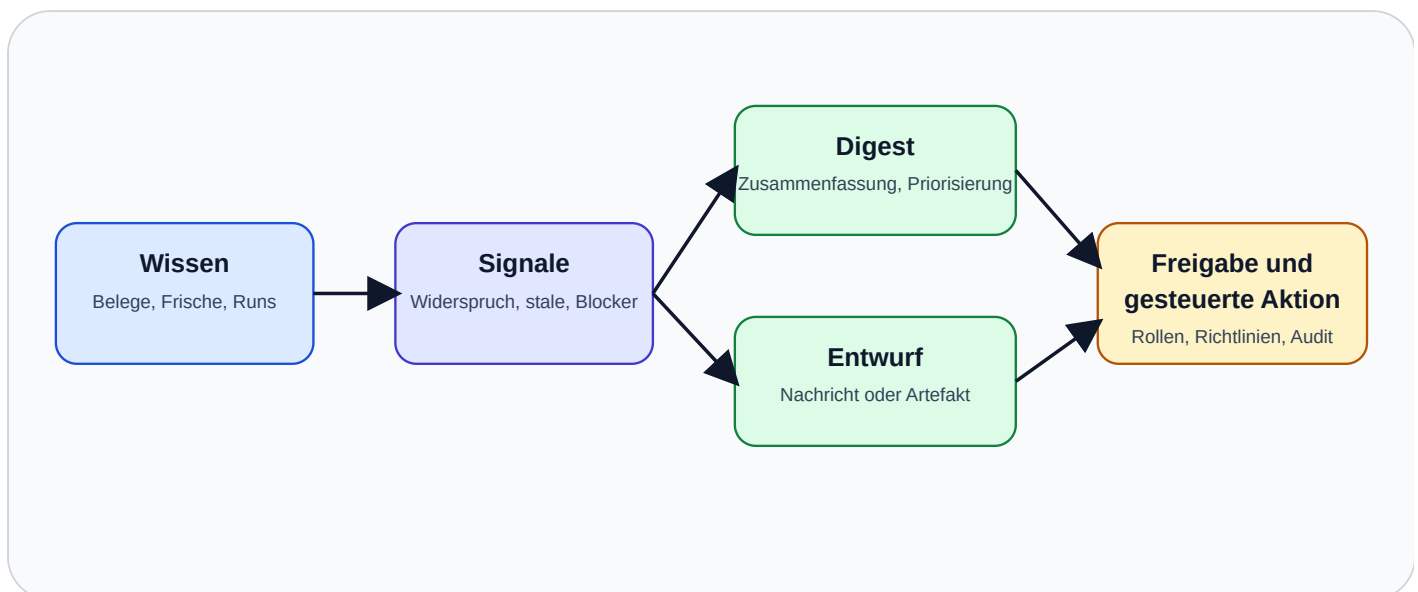
Die Seite **Agenten** nutzt den Projektkontext in einer geführten Konversation.

Bestätigte Funktionen:

- Liste der verfügbaren Agenten;
- Zusammenfassende Karte des ausgewählten Agenten mit **kind**, **scope**, **status** und abgedeckten Bereichen;
- Konversationsbereich;
- Strukturierte Ausgaben und Beweismittel;
- Gespeicherte Sitzungen im Browser;
- Erstellen und Löschen von benutzerdefinierten Agenten je nach Berechtigungen;
- Sprachsteuerung in **Agenten**, falls die Umgebung sie noch unterstützt.

Proaktivität von ProPM Agent

Proaktivität in ProPM Agent bedeutet nicht, dass ein Agent außerhalb des Projekts allein handelt. Das Verhalten ist stärker geregelt: die Plattform erkennt zu überwachende Situationen, meldet sie als **Signale**, kann einen **Digest** vorbereiten, einen **Entwurf** oder eine **gesteuerte Aktion** vorschlagen und lässt den Benutzer oder Genehmiger die weitere Vorgehensweise entscheiden.



Verfügbare Auslöser

Proaktivität kann durch folgende Faktoren ausgelöst werden:

- unzureichende **Frische**;
- **Widersprüchlichkeit** zwischen Beweisen;
- ein **Block** im Betrieb;
- **Planungsdruck** oder **Kosten** im Portfolio;
- **nicht abgeschlossene Ausführungen**;

- ein Folgebedarf, der Verteilung, Validierung oder erneute Ausführung erfordert.

Wo Proaktivität sichtbar wird

- **Arbeitsbereich:** Signal- und zu überprüfende Elemente;
- **Governance, Entscheidungen und Aktionen:** Digests, Benachrichtigungsentwürfe, Aktionsanfragen;
- **Portfolio-Befehlszentrum:** Vergleich von Projekten anhand von Indikatoren;
- **KI-Log:** Nachvollziehbarkeit der Entscheidungsfolge.

Was Proaktivität nicht allein tut

- Sie umgeht keine Rollen;
- Sie umgeht keine Richtlinien;
- Sie veröffentlicht nicht automatisch außerhalb der Anwendung ohne einen geregelten Pfad;
- Sie bleibt durch Beweise, Frische und sichtbare Status erklärbar.

Wie Sie einen Agenten schnell auswählen

Merken Sie sich diese Reihenfolge: **Fachbereich** -> **scope** -> **status**. Beginnen Sie mit dem abgedeckten Domänenbereich und prüfen Sie erst danach Sichtbarkeit und praktische Verfügbarkeit.

FELD	WAS SIE ZUERST PRÜFEN SOLLTEN	NÜTZLICHER REFLEX
abgedeckte Domänen	auf der Karte angekündigte Themen	gleichen Sie die Anfrage mit dem Agenten ab, dessen fachliche Abdeckung wirklich zur erwarteten Arbeit passt
scope	Sichtbarkeitsbereich des Agenten	prüfen Sie, ob der Agent auf das aktuelle Projekt begrenzt ist oder breiter sichtbar bleibt
status	praktische Verfügbarkeit des Agenten	bevorzugen Sie aktive Agenten für das ausgewählte Projekt, bevor Sie eskalieren
kind	ob die Karte standardmäßig oder benutzerdefiniert ist	behandeln Sie kind als beschreibenden Kontext, nicht als erstes Auswahlkriterium

In der Praxis suchen Sie im Roster zuerst nach Name oder Domäne. Bevorzugen Sie einen aktiven Agenten für das ausgewählte Projekt und nutzen Sie transversale oder

benutzerdefinierte Agenten nur dann, wenn ihre Fachabdeckung wirklich passt.

Mit Agenten arbeiten

1. **Überprüfen Sie das aktive Projekt;**
2. **Wählen Sie den passenden Agenten;**
3. Formulieren Sie eine nutzbare Anfrage mit Ziel, Umfang und erwartetem Format;
4. Lesen Sie die **strukturierte Ausgabe** erneut, bevor Sie sie wiederverwenden.

Die Oberfläche ermöglicht auch die Suche im Agenten-Roster, um schneller den richtigen Spezialisten zu finden.

Empfohlener Pfad

Für eine erste Nutzung ohne Mehrdeutigkeit:

1. stellen Sie in **Agenten** eine einfache Frage;
2. lesen Sie zuerst die Zusammenfassung der **strukturierten Ausgabe**;
3. prüfen Sie danach Belege, Frische und Vertrauen, falls die Antwort wiederverwendet werden soll;
4. öffnen Sie **Berichte & Artefakte** nur dann, wenn Sie dieses Ergebnis in ein gesteuertes, prüfbares oder veröffentlichbares Dokument umwandeln möchten.

Was **All projects** in Agenten wirklich bedeutet

Wenn der Dialog zum Erstellen benutzerdefinierter Agenten **All projects** anzeigt, bedeutet dies:

- der Agent wird weiterhin aus dem aktuellen Projekt erzeugt;
- er kann **in allen Projekten sichtbar sein, auf die dasselbe Konto Zugriff hat**;
- er folgt Ihrem Konto von einem Projekt zum anderen;
- er erzeugt keinen zusammengeführten Mehrprojekt-Datenraum;
- er ersetzt zur Laufzeit nicht das **aktive Projekt**.

Auch ein Agent mit **All projects** läuft weiterhin im **aktiven Projekt**, sobald Sie die Chat-Nachricht absenden.

Vom browserlokalen Chat zu PM-Dokumenten, DOCX und XLSX

Agenten springen nicht direkt zu einer final verteilten Datei. Der Ablauf ist stufenweise:

1. der aktuelle Chat bleibt zunächst **lokal im Browser**;
2. das Senden der Nachricht startet einen **Run** im aktiven Projekt;
3. der Run erzeugt eine **strukturierte Ausgabe**;
4. je nach Fluss und Ihren Rechten kann diese Ausgabe **Lineage**-Links, ein **Artefakt** oder ein **PM-Dokument** zeigen;
5. die Prüfung geht dann in **Berichte & Artefakte / PM-Dokumente** weiter;
6. das geprüfte Dokument kann anschließend je nach Governance **Add to knowledge**, **Download** oder **Publish** werden.

Ein Agenten-Chat erzeugt also nicht für sich allein ein gemeinsam genutztes Abschlussdokument.

Was **structured output** bedeutet

Eine **structured output** ist die strukturierte Ausgabe, die ein Agenten-Run erzeugt.

Sie kann enthalten:

- eine Zusammenfassung;
- Abschnitte;
- Belege oder Zitate;
- Frische- und Vertrauensinformationen;
- Nachvollziehbarkeits-IDs.

Für sich allein ist sie noch kein final veröffentlichtes Dokument.

Was **lineage** bedeutet

Lineage verbindet miteinander:

- den **Run**;
- die **structured output ID**;
- die **context snapshot ID**;
- das **Artefakt** und seine Version;
- das **PM-Dokument**, wenn ein gesteuertes Dokument existiert.

Diese Lineage hilft zu verstehen, woher ein Liefergegenstand kommt und welcher Kontext verwendet wurde.

Sitzungen und lokale Erinnerung

Der Chatverlauf ist lokal im Browser. In der Praxis gilt:

- Die gespeicherte Kontinuität ist an das Paar **Projekt + Agent** im aktuellen Browser gebunden;
- Eine Sitzung wird lokal auf dem verwendeten Gerät gespeichert;
- Wechseln Sie Browser, Profil oder Maschine oder löschen Sie den lokalen Speicher, kann ein gespeicherter Thread verschwinden;
- Der erste Prompt dient in der Regel als Sitzungsname, was die Wiederaufnahme erleichtert;
- Der Browser sollte nicht als gemeinsames zentrales Archiv betrachtet werden.

Browserlokal vs. geteilte Plattform

Merken Sie sich diese Trennung:

- **Chat-Kontinuität** und das **gemerkte Projekt** sind browserlokale Komfortfunktionen;
- **Dokumente, Importe, Artefakte, Genehmigungen** und **Veröffentlichungen** gehören zum gemeinsamen Plattformzustand.

Ein in einem Browser sichtbarer Verlauf ist daher nicht automatisch für alle Benutzer verfügbar.

Benutzerdefinierte Agenten

Die Erstellung von benutzerdefinierten Agenten hängt vom Berechtigungsniveau ab.

Zu beachten ist:

- Nicht alle Benutzer können einen Agenten erstellen;
- Der Erstellungsdialog erinnert an den aktiven **Projektkontext** vor dem Speichern;
- Sichtbare Felder umfassen mindestens **Name, Rolle / Anweisungen** und **Scope**;
- Wählen Sie standardmäßig **Nur Projekt**, es sei denn, die Umgebung zeigt explizit einen breiteren Scope;
- Wenn die Option **All projects** verfügbar ist, wird der Agent aus dem aktuellen Projekt erstellt, kann aber in anderen Projekten desselben Kontos sichtbar bleiben;
- Wenn ein Multi-Projekt-Agent nicht anderswo erscheint, prüfen Sie zunächst dasselbe Konto und den Zugriff auf das Zielprojekt;
- Das Löschen eines benutzerdefinierten Agenten bleibt kontrolliert;

- Ein benutzerdefinierter Agent bleibt durch die Regeln des Projekts und der Plattform geregelt.

Schnelles Auswahlbeispiel

BEDARF	EMPFOHLENE WAHL
Nominale Nutzung, großes Team, vorhersehbares Verhalten	Standard-Agent
Spezifische Anweisungen, Team-Ton, spezialisierter Workflow	Benutzerdefinierter Agent
Nutzung auf ein einzelnes Projekt beschränkt	Nur Projekt
Derselbe Agent in mehreren Projekten desselben Kontos wiederverwendbar	All projects , falls die Option tatsächlich exponiert ist

Benutzerdefinierten Agenten erstellen

Benutzerdefinierte Agenten erscheinen in Ihrer Liste und können pro Projekt oder für alle Projekte verwendet werden.

PROJEKTKONTEXT

Azure Bay Hotel & Convention Center

Projektspezifische Agenten bleiben innerhalb dieses Projekts. Agenten für alle Projekte folgen Ihrem Konto projektübergreifend.

Name

Stakeholder-Kommunikation

Rolle / Anweisungen

Sie sind ein Kommunikationsagent. Verfassen Sie Stakeholder-Updates in einem managementtauglichen Ton...

Geltungsbereich

Nur Projekt

Dieser Agent ist für Azure Bay Hotel & Convention Center sichtbar.

Abbrechen

Erstellen

Sprachsteuerung in Agenten

Diese Seite beschreibt keinen separaten **Sprach**-Eingangspunkt im **Arbeitsbereich**. Wenn eine Sprachsteuerung noch verfügbar ist, ist sie auf die **Agenten** beschränkt und hängt explizit von der Browserunterstützung der Spracherkennungs-APIs ab.

Wenn die Sprachsteuerung nicht verfügbar ist:

- Verwenden Sie die Texteingabe;
- Prüfen Sie die Mikrofonberechtigungen des Browsers;
- Unterscheiden Sie eine Browserbeschränkung von einer lokalen Umgebungsbeschränkung;
- Lesen Sie den hinzugefügten Text im Composer immer vor dem **Send** durch;
- Wenn der Mikrofonknopf nicht verfügbar ist oder eine Inkompatibilitätsmeldung erscheint, wechseln Sie sofort zur Texteingabe.

Praktische Hinweise zur Sprachsteuerung

SYMPTOM	ZUERST PRÜFEN	NÜTZLICHE REFLEXION
Mikrofonknopf fehlt oder inaktiv	Unterstützung von <code>SpeechRecognition</code> / <code>webkitSpeechRecognition</code>	Wechseln Sie sofort zur Texteingabe
Mikrofonberechtigung verweigert	Mikrofonberechtigung des Browsers oder OS	Erneuern Sie die Berechtigung und starten Sie die Aufnahme erneut
Unvollständige Transkription	Text im Composer	Lesen Sie, korrigieren und ergänzen Sie vor dem Send
Einzelne Fehler während der Aufnahme	Browserzustand oder aktuelle Sitzung	Stoppen Sie die Aufnahme, wechseln Sie zur Tastatur und versuchen Sie es später erneut

Die Texteingabe bleibt der nominale Backup-Pfad. Sie ermöglicht die Fortsetzung der Arbeit ohne Unterbrechung des Runs wegen einer lokalen Browserbeschränkung.

Gute Praktiken

- Laden Sie zuverlässige und aktuelle Quellen in die **Wissen**-Bibliothek, bevor Sie eine wichtige Analyse durchführen;
- Lesen Sie den Importverlauf, wenn eine verwaltete Quelle fehlt;
- Fordern Sie explizit **Beweise** oder **Zitate** an, wenn die Entscheidung damit begründet werden muss;

- Wenn eine Antwort die Zustände `stale`, `conflicting` oder `unavailable` enthält, öffnen Sie die Seite [Strukturierte Ausgaben, Beweise und Frische](#) vor der Veröffentlichung.

Weiter

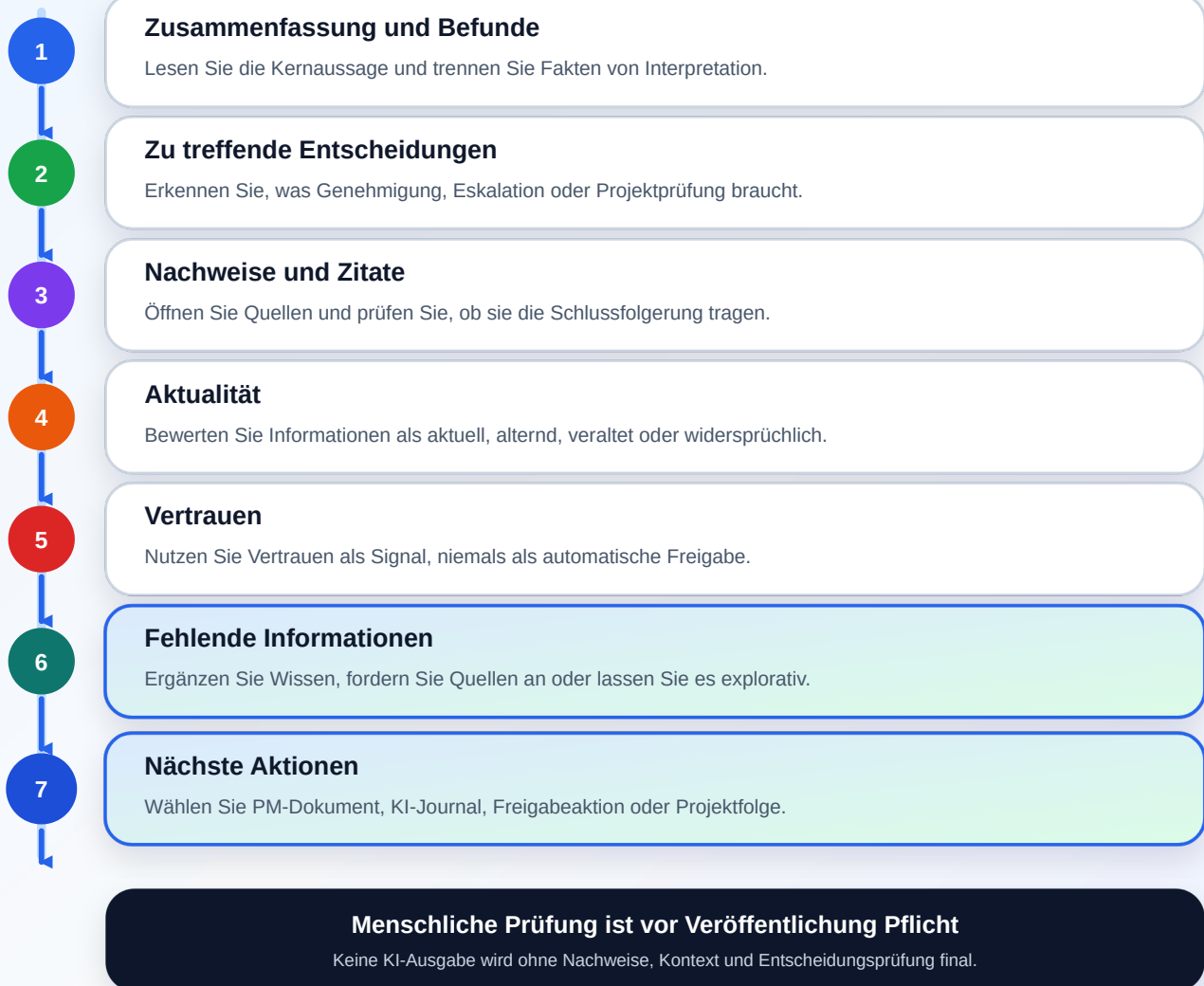
- [Strukturierte Ausgaben, Beweise und Frische](#)
- [Governance, Entscheidungen und Aktionen](#)
- [Berichte, KI-Log und Nachvollziehbarkeit](#)
- [Wartung, Support und FAQ](#)

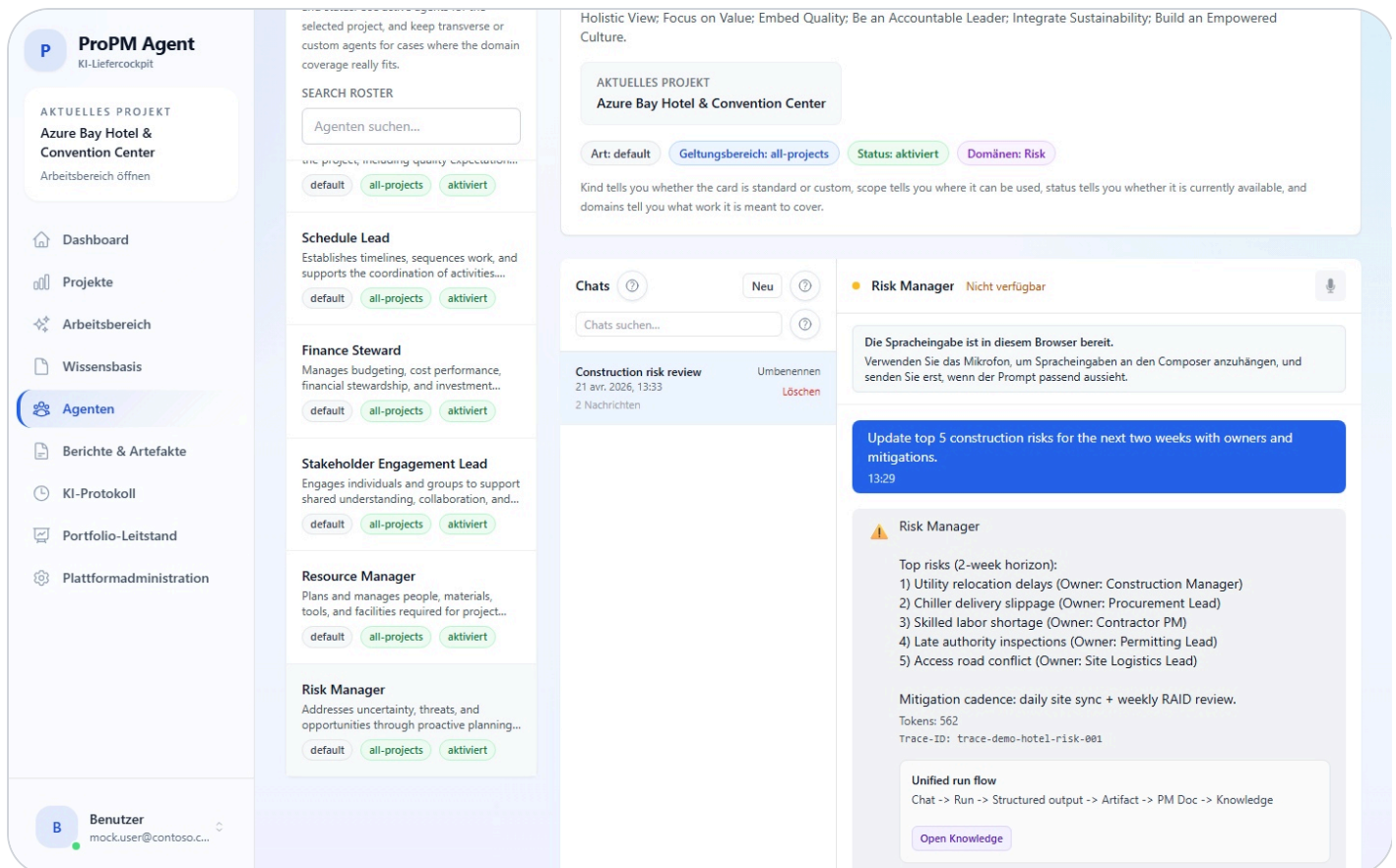
Strukturierte Ausgaben, Nachweise und Aktualität

[Startseite](#) · Strukturierte Ausgaben, Nachweise und Aktualität

Strukturierte Ausgabe vor Wiederverwendung prüfen

Jede KI-Antwort bleibt ein Entwurf, bis die menschliche Prüfung abgeschlossen ist.





Ziel

Diese Seite erklärt, wie eine **strukturierte Ausgabe** in ProPM Agent zu interpretieren ist, um zu entscheiden, ob das Ergebnis direkt nutzbar ist, überprüft werden muss oder in ein verwaltetes Artefakt umgewandelt werden sollte.

Warum das wichtig ist

ProPM Agent liefert nicht nur Freitext. Runs können zusätzlich Folgendes enthalten:

- eine **Zusammenfassung**;
- **Findings**;
- **zu treffende Entscheidungen**;
- **Aktionen**;
- **Annahmen**;
- **fehlende Informationen**;
- **Watchpoints**;
- **Nachweise**;
- Metadaten zur **Aktualität** und **Vertrauenswürdigkeit**;
- **Artefaktvorschläge, Follow-ups** und **Benachrichtigungen**.

Wo diese Informationen erscheinen

Strukturierte Ausgaben und ihre Metadaten sind auf mehreren Oberflächen sichtbar:

- **Agenten**, direkt nach einem Run;
- **KI-Protokoll**, in den Details eines Runs;
- **Berichte & Artefakte**, über die Abstammungslinie zwischen Run, Artefakt und PM Doc.

make procurement and schedule owners explicit before the first controls review.

Verantwortlich: Procurement Lead Stufe: program Fällig: 2026-01-13

Annahmen

- Authority inspection slots remain available through the planned enabling-works window.

Fehlende Informationen

- Confirm final sponsor attendance and decision authority for the kickoff SteerCo.

Beobachtungspunkte

- Long-lead equipment exposure should remain visible until procurement awards are contractually locked.

Evidenz

Project Charter

blob://demo/demo-hotel-001/01-project-charter.md

Aktuell

Autorität 5

Authorize and govern the delivery of a 220-room upscale urban hotel, conference center, and wellness facilities.

System: Knowledge

Master Schedule

blob://demo/demo-hotel-001/04-master-schedule.md

Alternnd

Autorität 4

Commissioning complete remains targeted for 2028-03-15 with a recovery trigger when SPI < 0.95.

System: Schedule

Wie man eine strukturierte Ausgabe liest

Empfohlene Lesereihenfolge

1. Lesen Sie die **Zusammenfassung**;
2. Öffnen Sie dann **Benötigte Entscheidungen** oder **Aktionen**;
3. Überprüfen Sie den Abschnitt **Nachweise**;
4. Lesen Sie **Vertrauenswürdigkeit** und **Quellenaktualität** erneut;
5. Entscheiden Sie dann, ob die Antwort im Chat bleiben, ein Artefaktentwurf werden oder eine menschliche Überprüfung erfordern kann.

Bedeutung der Abschnitte

ABSCHNITT	WOZU DIENT ER
Summary	Kürzeste Version des Ergebnisses, bereit für schnelle Überprüfung
Findings	Vom Run hervorgehobene Fakten, Motive oder Feststellungen
Decisions needed	Punkte, die eine menschliche Entscheidung erfordern
Actions	Empfohlene Folgeaktionen zur Ausführung oder Planung
Assumptions	Implizite Bedingungen, von denen die Antwort abhängt
Missing information	Fehlende Informationen, die die Robustheit des Ergebnisses verringern
Watchpoints	Risiken, Widersprüche oder zu beobachtende Themen
Evidence	Referenzen, die als Nachweis oder Begründung dienen
Artifact status / Artifact proposals	Hinweise auf mögliche Umwandlung des Ergebnisses in ein verwaltetes Artefakt
Follow-ups	Vorgeschlagene Fortsetzungsschritte
Notifications	Vom Flow vorgeschlagene Entwürfe oder Benachrichtigungen

Vereinfachtes Lesebeispiel

Das folgende Beispiel ist **illustrativ**. Es dient dazu zu zeigen, wie man eine strukturierte Karte vor der Wiederverwendung überprüft:

- **Summary:** Das kritische Paket scheint zwei Wochen im Verzug zu sein.
- **Findings:** Die letzte Planungsnotiz ist aktueller als der verwaltete Kalender-Connector.
- **Decisions needed:** Soll der Sponsor-Meilenstein neu gebaselined oder eine Planungsrevalidierung angefordert werden?
- **Evidence:** Planungsnotiz, Auszug aus dem wöchentlichen Bericht, Status des Quell-Connectors.
- **Source freshness:** Wissen **fresh**, Planungs-Connector **stale**.
- **Watchpoints:** Möglicher Widerspruch zwischen der Projektkommunikation und den letzten synchronisierten Daten.

Empfohlene Lesart in diesem Fall:

1. Die **Zusammenfassung** sagt Ihnen, was Sie zuerst überprüfen sollten;
2. Die Kombination **Nachweise** + **Quellenaktualität** verhindert, dass Sie zu schnell veröffentlichen;
3. Das Vorhandensein eines **Watchpoints** und einer zu treffenden Entscheidung drängt zu einer menschlichen Überprüfung, dann zu einem Artefakt, wenn das Thema formal wird.

Zwei häufige Fälle zu unterscheiden

FALL	PRAKTISCHE LESART	EMPFOHLENE ENTSCHEIDUNG
Vertrauenswürdigkeit korrekt, aber Aktualität unzureichend	Die Argumentation scheint kohärent, aber ein Teil der Quellen ist stale oder aging	Verbreiten Sie nicht ohne Revalidierung oder dokumentarische Aktualisierung
Geringe Vertrauenswürdigkeit, aber aktuelle Quellen	Die Quellen sind aktuell, aber der Run meldet noch Lücken, Widersprüche oder zu starke Annahmen	Behalten Sie die Ausgabe als explorative Arbeit, dann starten Sie die Überprüfung oder den Run neu, bevor Sie formalisieren

Diese Unterscheidung vermeidet es, die **Vertrauenswürdigkeit** als einzige Note zu behandeln. Eine Antwort kann solide erscheinen, während sie sich auf zu alte Quellen stützt, oder umgekehrt.

Wie man Nachweise liest

Jeder Nachweis oder jedes Zitat kann mehrere nützliche Elemente enthalten:

- einen **Titel** oder Quellennamen;
- einen **Quellen-URI** oder einen dokumentarischen Namen;
- einen **Auszug**;
- eine **Seite** oder einen **Abschnitt**, wenn verfügbar;
- ein **Synchronisationsdatum**;
- ein **Quellsystem**;
- ein **Aktualitäts-Badge**;
- einen **Autoritätsrang**, wenn angezeigt.

Was vor der Wiederverwendung eines Nachweises zu prüfen ist

1. Stützt der Auszug die angezeigte Aussage gut?
2. Ist die Quelle identifizierbar und wieder öffnbar?
3. Ist die Aktualität für das erwartete Entscheidungsniveau akzeptabel?
4. Erzählen mehrere Nachweise dasselbe, oder gibt es einen Widerspruch?

Aktualitätszustände

ZUSTAND	PRAKTISCHE BEDEUTUNG	EMPFOHLENE REAKTION
fresh	Quelle aktuell genug für normale Nutzung	Kann nach normaler Überprüfung wiederverwendet werden
aging	Quelle noch nutzbar, nähert sich aber einem Revalidierungsbedarf	Vor breiter Verteilung schnell überprüfen
stale	Quelle zu alt, um ohne zusätzliche Kontrolle als zuverlässig angesehen zu werden	Vor Entscheidung aktualisieren, neu importieren oder bestätigen
conflicting	Die Quelle widerspricht einer anderen relevanten Quelle	Nicht automatisch entscheiden; Nachweise erneut lesen
unavailable	Die Quelle konnte nicht bestätigt oder abgerufen werden	Als Warnung behandeln, nicht als nutzbaren Nachweis

Vertrauenswürdigkeit

Die **Vertrauenswürdigkeit** ist ein globales Signal für die Robustheit des Ergebnisses. Sie muss zusammen mit Aktualität und Nachweisen interpretiert werden, niemals isoliert.

Planen Sie eine zusätzliche menschliche Überprüfung ein, wenn Sie sehen:

- geringe Vertrauenswürdigkeit;
- fehlende oder unspezifische Nachweise;
- Zustände `stale`, `conflicting` oder `unavailable`;
- wichtigen Abschnitt **Fehlende Informationen**;
- Entscheidung oder Aktion mit externer Auswirkung.

Überprüfungsniveau je nach Auswirkung

AUSWIRKUNGSNIVEAU	MINIMALE ÜBERPRÜFUNG	EMPFOHLENE ESKALATION
Interner Arbeitsentwurf	<code>Summary</code> , <code>Findings</code> und mindestens einen wieder öffenbaren Nachweis prüfen	Ausgabe im Chat belassen, wenn sie explorativ bleibt
Teamkoordination oder interne Projektaktion	Nachweise, Aktualität, fehlende Informationen und vorgeschlagene Aktionen prüfen	Artefakt erstellen, wenn das Ergebnis geteilt oder historisiert werden muss
Sponsor-Entscheidung, Veröffentlichung, externe Benachrichtigung oder verwaltete Aktion	Alle Nachweise überprüfen, <code>conflicting</code> / <code>stale</code> Zustände entscheiden, technische IDs behalten	Über Berichte & Artefakte , Diff , Abstammungslinie und KI-Protokoll gehen, bevor verbreitet wird

Zu bewahrende Trace-IDs

FELD	VERWENDUNG
<code>Trace ID</code>	Run oder Ereignis genau beim Support wiederfinden
<code>Structured output ID</code>	Die tatsächlich produzierte strukturierte Ausgabe identifizieren
<code>Context snapshot ID</code>	Verstehen, in welchem dokumentarischen oder Projektkontext der Run lief

Diese Felder sind besonders nützlich, wenn Sie einen Run, ein Artefakt und ein Ereignis aus dem **KI-Protokoll** abgleichen müssen.

Wann die Ausgabe in ein Artefakt umwandeln

Der normale Weg ist:

1. Projektfrage;
2. Strukturierte Antwort;
3. Erstellung eines **Artefaktentwurfs**;
4. Überprüfung des **Diffs** und der **Abstammungslinie**;
5. Genehmigung oder Veröffentlichung.

Wandeln Sie eine Ausgabe in ein Artefakt um, wenn:

- sie ein formelles Lieferobjekt werden soll;
- sie eine Validierung oder Veröffentlichung durchlaufen muss;
- Sie eine explizite Abstammungslinie zu einem Run und seinen Nachweisen bewahren müssen;
- der Inhalt den Chat für externe Verbreitung, Genehmigung oder dauerhafte Nachverfolgbarkeit verlassen muss.

Einfache Regel: Solange Sie explorieren, kann der Chat ausreichen; sobald ein Ergebnis **geteilt, genehmigt, veröffentlicht oder als Spur bewahrt** werden muss, gehen Sie über **Berichte & Artefakte**.

Checkliste vor Wiederverwendung in einem Lieferobjekt

1. Entspricht die Zusammenfassung den detaillierten Findings?
2. Sind die vorgeschlagenen Aktionen mit der Projektsituation konsistent?
3. Sind die Nachweise präzise genug, um die Entscheidung zu rechtfertigen?
4. Sind die Aktualitätszustände akzeptabel?
5. Muss ein Artefakt erstellt werden, oder reicht es, die Ausgabe im Chat zu behalten?

Häufige Probleme

Die Antwort scheint sauber, aber es erscheint kein Nachweis

Behandeln Sie das Ergebnis als ein Element, das vor externer Nutzung überprüft werden muss. Das Fehlen sichtbarer Nachweise verringert die Fähigkeit, den Inhalt zu rechtfertigen.

Ein Nachweis ist **conflicting**

Veröffentlichen Sie nicht direkt. Öffnen Sie die Quelle, vergleichen Sie die widersprüchlichen Referenzen und dokumentieren Sie die Entscheidung im Artefakt oder in der Governance. Wenn das Thema eine formalisierte Entscheidung erfordert, gehen Sie zu [Governance, Entscheidungen und Aktionen](#), anstatt den Konflikt nur im Chat zu belassen.

Ein Nachweis ist **unavailable**

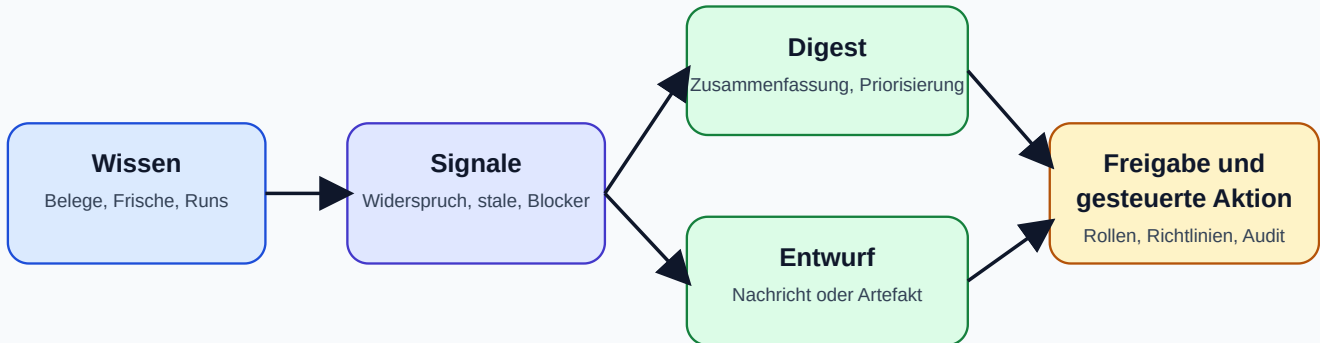
Gehen Sie davon aus, dass die Begründung nicht stabilisiert ist. Überprüfen Sie die Quelle in **Wissen**, dem Import oder den Run-Details im **KI-Protokoll**.

Weiterführend

- [Wissen und Agenten](#)
- [Berichte, KI-Protokoll und Nachverfolgbarkeit](#)
- [Wartung, Support und FAQ](#)

Governance, Entscheidungen und Aktionen

[Startseite](#) · Governance, Entscheidungen und Aktionen



Ziel

Diese Seite erklärt auf einfache Weise, wie ProPM Agent vorgeht:

1. ein **Signal** wird erkannt;
2. eine **Entscheidung** wird getroffen;
3. dann eine **gouvernierte Aktion**;
4. ggf. einer **Genehmigung** unterzogen;
5. bevor sie **ausgeführt** und **verfolgt** wird.

Diese Seite hilft Ihnen, klar zu verstehen:

- was eine **Governance-Richtlinie** ist;
- was `allow`, `require_approval` und `deny` bedeuten;
- was `observe`, `draft`, `propose` und `execute` bedeuten;
- wie man **Aktionen & Genehmigungen** Schritt für Schritt nutzt;
- warum eine Aktion sichtbar, aber blockiert sein kann.

Sehr einfacher Überblick des Flusses

Im ProPM Agent ist der übliche Weg:

1. ein **Signal** zieht die Aufmerksamkeit auf sich;
2. das Team liest es erneut;

3. die **Governance** entscheidet, was jede Rolle tun darf;
4. wenn ein externer Output nötig ist, wird eine **Aktion** erstellt;
5. wenn das Projekt es verlangt, geht die Aktion in die **Genehmigung**;
6. die Aktion wird dann **ausgeführt** oder **abgelehnt**;
7. die Spur bleibt im **Aktivitätsbereich** und im **Journal IA** sichtbar.

Teil 1 — Signale verstehen

Ein **Signal** ist eine strukturierte Warnung, die sagt: „**Dieses Thema verdient Aufmerksamkeit**“.

Signalbeispiele

Ein Signal kann auftreten:

- bei **Mangel an Frische** der Quellen;
- bei einer **Widersprüchlichkeit** mehrerer Beweise;
- bei einem **Projektblocker**;
- bei einer Folge, die eine **Benachrichtigung**, eine **Entscheidung** oder eine **externe Aktion** verdient.

Was der Benutzer typischerweise auf einer Signalkarte sieht

Eine Signalkarte kann anzeigen:

- einen **Titel**;
- eine **Zusammenfassung**;
- eine **Erklärung**;
- eine **Schwere**;
- einen **Status**;
- einen **Modus**;
- eine Anzahl von **Beweisen** oder erneuten Auslösungen;
- Aktionen wie **Create draft**, **Snooze 24h** oder **Dismiss** je nach Rolle.

Empfohlener Schritt-für-Schritt-Ansatz zur Signalbearbeitung

Wenn Sie ein Signal öffnen, halten Sie sich an diese Reihenfolge:

1. lesen Sie die **Zusammenfassung**;

2. lesen Sie anschließend die **Erklärung**;
3. prüfen Sie die **Beweise** und die **Frische**;
4. entscheiden Sie, ob das Thema nur **Beobachtung**, einen **Entwurf** oder eine echte **Aktion** erfordert;
5. wenn ein externer Output nötig wird, gehen Sie zu **Aktionen & Genehmigungen**.

Nützliche Signalstatus

STATUS	WAS ES BEDEUTET
open	Das Thema bleibt aktiv und erfordert weitere Aufmerksamkeit
snoozed	Das Thema wird vorübergehend pausiert
dismissed	Das Thema wird aus der aktiven Warteschlange entfernt
resolved	Das Thema gilt als bearbeitet

Nützliche Signalmodi

MODUS	EINFACHE INTERPRETATION
inform	Das Signal informiert, ohne sofortige Aktion zu verlangen
suggest	Das Signal schlägt einen nächsten Schritt vor
draft	Das Signal ist bereits auf einen Entwurf oder eine Vorbereitung ausgerichtet
request_approval	Das Signal ruft eine geregelte Überprüfung oder Genehmigung an

Teil 2 — Governance-Richtlinien

Was ist eine Governance-Richtlinie?

Eine **Governance-Richtlinie** ist eine Regel, die die Frage beantwortet:

„Wer darf was tun, auf welchem Connector, und mit welchem Kontrollniveau?“

Anders ausgedrückt verhindert Governance, dass eine externe Aktion ohne klaren Rahmen ausgeht.

Was eine Richtlinie entscheidet

Eine Richtlinie beantwortet im Allgemeinen vier Fragen:

1. **Wer?** – welche Rolle ist betroffen;
2. **Was?** – welcher Connector, welche Art von Aktion oder welches Ziel ist betroffen;
3. **Wie weit?** – einfache Beobachtung, Entwurf, Vorschlag oder Ausführung;
4. **Mit welchem Effekt?** – erlaubt, erlaubt mit Genehmigung oder verweigert.

Sehr einfaches Beispiel

Eine Richtlinie könnte bedeuten:

- der **Contributor** kann einen Teams-Entwurf vorbereiten;
- der **Projektleiter** kann eine SharePoint-Veröffentlichung vorschlagen;
- der **Projektbesitzer** muss vor der Ausführung genehmigen;
- niemand sonst darf diese Veröffentlichung direkt ausführen.

Die Ebenen verstehen: **observe**, **draft**, **propose**, **execute**

Die **Ebene** beschreibt, wie weit eine Rolle im Fluss gehen kann.

EBENE	WAS DER BENUTZER TUN KANN	WAS ER NOCH NICHT TUN KANN	EINFACHES BEISPIEL
observe	Informationen sehen, Thema verfolgen, Warteschlange prüfen	Aktion oder Entwurf erstellen	Ein Leser verfolgt Signale, ohne einen Output vorzubereiten
draft	Einen Entwurf, Text oder eine Aktionsabsicht vorbereiten	Die Aktion offiziell in die Warteschlange einreichen	Ein Contributor bereitet eine Teams-Nachricht vor, reicht sie aber nicht vor
propose	Eine echte Aktionsanfrage in die geregelte Warteschlange einreichen	Direkt ausführen	Ein Projektleiter schlägt ein Jira-Ticket vor
execute	Die reale Ausführung starten, wenn andere Bedingungen erfüllt sind	Die Richtlinie oder Genehmigungen umgehen	Ein Projektbesitzer veröffentlicht ein Artefakt zu SharePoint

Sehr einfache Interpretation

- **observe** = ich schaue zu;
- **draft** = ich bereite vor;

- **propose** = ich fordere offiziell an;
- **execute** = ich starte tatsächlich.

Die Effekte verstehen: **allow**, **require_approval**, **deny**

Der **Effekt** beschreibt, was die Plattform tut, wenn eine Rolle diese Ebene erreicht.

EFFEKT	WAS ES BEDEUTET	PRAKTISCHE KONSEQUENZ
allow	Die Aktion ist auf dieser Ebene erlaubt	Der Fluss kann ohne zusätzliche Genehmigungsschritte fortschreiten, wenn der Rest bereit ist
require_approval	Die Aktion ist möglich, muss aber genehmigt werden	Der Genehmigungs-Queue wird obligatorisch vor der Ausführung
deny	Die Aktion ist für diese Rolle oder diesen Bereich verboten	Der Benutzer kann in diesem Fluss nicht weitergehen

Sehr einfache Interpretation

- **allow** = ja;
- **require_approval** = ja, aber nach menschlicher Validierung;
- **deny** = nein.

Wie man eine Richtlinienzeile liest

Nehmen wir diese Lesung:

- **Rolle:** Projektleiter
- **Connector:** SharePoint publish
- **Ebene:** **execute**
- **Effekt:** **require_approval**

Das bedeutet:

- Der Projektleiter kann bis zur Ausführungsanfrage gehen;
- Die Veröffentlichung geht jedoch nicht sofort los;
- Eine Genehmigung ist vor der realen Ausführung nötig.

Konkrete Richtlinienbeispiele

GESCHÄFTSSZENARIO	ROLLE	EMPFOHLENE EBENE	EMPFOHLENER EFFEKT	WARUM
Veröffentlichung eines Protokolls zu SharePoint	Projektleiter	execute	require_approval	Der Output ist extern und muss noch einmal gelesen werden
Erstellung eines Jira-Tickets aus einem Blocker	Projektleiter	propose	allow oder require_approval	Das Projekt kann ein Ticket anfordern, ohne es automatisch zu öffnen
Interne Teams-Nachricht mit geringem Risiko	Contributor	execute oder propose	allow	Schnelle Kommunikation mit geringem Einfluss
Outlook-E-Mail an Sponsoren	Contributor	propose	require_approval	Sensiblere und formellere Kommunikation
Webhook zu einem Drittanbieter-Tool	Projektbesitzer	execute	require_approval	Technischer Output, der sehr kontrolliert bleiben soll
Connector nicht bereit oder nicht autorisiert	alle außer Admin	observe oder kein Gebrauch	deny	Wir vermeiden einen versehentlichen Start

Schritt-für-Schritt zur Konfiguration einer Governance-Richtlinie

Folgen Sie dieser einfachen Reihenfolge.

Schritt 1 — Öffnen der richtigen Oberfläche

Öffnen Sie im **Workspace** des Projekts **Governance-Richtlinien**.

Schritt 2 — Wählen Sie den zu kontrollierenden Fluss

Fragen Sie sich zuerst:

- Handelt es sich um eine **Veröffentlichung**;
- um ein **Ticket**;
- um eine **Nachricht**;
- um einen **Webhook**;
- um eine andere externe Aktion?

Schritt 3 — Wählen Sie die betroffene Rolle

Definieren Sie dann, welche Rolle handeln darf:

- **Contributor**;
- **Projektleiter**;
- **Projektbesitzer**;
- oder eine andere Rolle in Ihrer Konfiguration.

Schritt 4 — Wählen Sie die Aktionsstufe

Entscheiden Sie, ob diese Rolle nur:

- beobachten;
- einen Entwurf vorbereiten;
- vorschlagen;
- oder ausführen soll.

Schritt 5 — Wählen Sie den Effekt

Entscheiden Sie, ob diese Ebene:

- direkt erlaubt (`allow`);
- mit Genehmigung erlaubt (`require_approval`);
- oder verweigert (`deny`) sein soll.

Schritt 6 — Prüfen Sie den betroffenen Connector oder das Ziel

Eine gute Richtlinie reicht nicht aus, wenn der Connector:

- technisch nicht bereit ist;
- dem Projekt nicht offensteht;

- oder das richtige Ziel für Artefakte nicht hat.

Schritt 7 — Testen mit einer Nicht-Administrator-Rolle

Die beste Kontrolle ist praktisch:

1. melden Sie sich mit einer realistischen Geschäftsrolle an;
2. öffnen Sie **Actions & approvals**;
3. prüfen Sie, was sichtbar, erlaubt oder blockiert ist;
4. passen Sie die Richtlinie an, wenn das Verhalten nicht das erwartete ist.

Governance-Richtlinien

Konfigurieren Sie gesteuerte Connectoren, Ziele, Aktionsrichtlinien, Rendering-Profile, Aktualitätsgrenzen und Benachrichtigungs-Digests.

CONNECTOREN
3

ZIELE
2

AKTIONSRICHTLINIEN
2

RENDERING-PROFILE
2

BENACHRICHTIGUNGSEINSTELLUNGEN
1

Review and save each governance object independently so connector posture, routing destinations, action boundaries, rendering behavior, and notification rules stay easy to audit.

GESTEUERTE AKTIONSTYPEN

Artefakt in SharePoint veröffentlichen Teams-Nachricht senden Outlook-Nachricht senden Jira-Ticket erstellen Azure-DevOps-Ticket erstellen Kalender-Follow-up erstellen

Connectoren

Status, Ausführungsmodus, Umgebung und Geltungsbereich für connector-gestützte Aktionen.

3 konfiguriert

Microsoft Graph / SharePoint

graph-sharepoint-primary • Microsoft Graph / SharePoint

Aktiviert Mock Aktualität: Fresh

Name Connector-Typ

Microsoft Graph / SharePoint Microsoft Graph / SharePoint

Beschreibung

Status Ausführungsmodus

Aktiviert Mock

Environment Fixture-Referenz

Jira

jira-primary • Jira

Aktiviert Mock Aktualität: Alternd

Name Connector-Typ

Jira Jira

Beschreibung

Status Ausführungsmodus

Aktiviert Mock

Environment Fixture-Referenz

Custom environment delivery-board

Einfache Regeln für eine gute Governance-Konfiguration

- Verwenden Sie **allow** auf **execute** nur für Flüsse mit geringem Risiko;
- Verwenden Sie **require_approval** sobald ein Inhalt das Projekt verlässt oder ein externes System verändert;
- Verwenden Sie **deny**, wenn der Connector nicht bereit, nicht autorisiert oder zu sensibel ist;
- Halten Sie die Regeln konsistent mit den tatsächlich zugewiesenen Rollen;
- Testen Sie immer einen realen Fall, bevor Sie die Richtlinie als fertig betrachten.

Häufige Fehler zu vermeiden

FEHLER	RICHTIGE INTERPRETATION
„Ich sehe den Connector, also kann ich ihn benutzen“	falsch: Sichtbarkeit garantiert weder Berechtigung noch technische Gesundheit
„ propose bedeutet, dass die Aktion ausgeht“	falsch: propose bedeutet, dass der Antrag in die geregelte Warteschlange eintritt
„ execute bedeutet ohne Kontrolle“	falsch: execute kann noch mit require_approval kombiniert werden
„ deny bedeutet Ausfall“	falsch: deny ist oft eine normale Governance-Entscheidung

Teil 3 — Aktionen & Genehmigungen

Die Oberfläche **Actions & approvals** dient dazu, eine Absicht in eine echte **gouvernierte Aktion** umzuwandeln.

Wie diese Queue zu lesen ist

Keine Einträge können normal sein, wenn noch nichts vorgeschlagen wurde. Lesen Sie blockierte Voraussetzungen, Freigabe-Wartezustände, ausführbare Requests und den Ausführungsverlauf als unterschiedliche Zustände statt als eine generische leere Queue.

Aktionen & Genehmigungen

Schlagen Sie gesteuerte connector-gestützte Aktionen vor, halten Sie sie zur Genehmigung zurück und führen Sie sie erst nach Prüfung aus.

Form draft

Ausstehende Genehmigung

Ready to execute

Ausgeführt

Rejected / failed

EXECUTION PREREQUISITES

Clear

At least one compatible execution option is operational, so the proposal path is open.

PENDING APPROVAL

1

Requests proposed but still waiting for governance approval.

READY TO EXECUTE

1

Approved requests that are waiting for controlled execution.

EXECUTED HISTORY

0

Completed governed actions retained as execution history and audit evidence.

Gesteuerte Aktion vorschlagen

Unterstützte Aktionstypen bleiben richtlinienbewusst, aktualitätsbewusst und connector-begrenzt. Externe Ausführung umgeht in dieser Oberfläche niemals die Genehmigung.

Execution readiness

1 available • 0 blocked

Only enterprise-approved execution options appear here. Technical connector setup remains in Platform Administration.

Open Platform Administration

Review project integrations

Aktionstyp

Artefakt in SharePoint veröffentlichen

Execution option

Microsoft Graph / SharePoint — Microsoft Graph / SharePoint

Mode: Mock

Titel

SharePoint-Veröffentlichung für den Wochenbericht genehmigen

Begründung

Erläutern Sie, warum diese externe Aktion erforderlich ist und welche Evidenz sie unterstützt.

Vier kanonische Lesarten, die Sie im Kopf behalten sollten

In der Oberfläche lässt sich diese Fläche am einfachsten über vier unterschiedliche Zustände lesen:

KANONISCHE LESART	WAS SIE BEDEUTET
Execution prerequisites	kompatible Ausführungsoptionen können existieren, aber die operative Nutzung bleibt blockiert oder nicht verfügbar
Pending approval	eine governierte Anfrage wurde vorgeschlagen und wartet noch auf Genehmigung
Ready to execute	eine Anfrage ist bereits approved , die kontrollierte Ausführung bleibt aber ein separater Schritt

Governance, Entscheidungen und Aktionen

10/20

KANONISCHE LESART	WAS SIE BEDEUTET
Executed history	die Aktion wurde tatsächlich ausgeführt und bleibt als Audit-Verlauf sichtbar

Eine **approved**-Anfrage ist also noch keine **executed**-Anfrage.

Wenn alles korrekt vorbereitet ist, was sollte ich sehen?

In einem nominalen Fall findet der autorisierte Benutzer in der Regel:

- mindestens einen relevanten **Aktionstyp**;
- mindestens eine **kompatible und gesunde Ausführungsoption**;
- eine tatsächlich aktive **Projektbindung**;
- eine **Richtlinie**, die das Vorschlagen erlaubt oder sauber in die Genehmigung leitet;
- eine Warteschlange, in der Anfragen je nach Fall in **pending approval**, **approved**, **executed** oder **rejected** übergehen.

Wenn eines dieser Glieder fehlt, kann der Bildschirm leer, unvollständig oder rein informativ wirken, ohne dass dies automatisch eine Störung bedeutet.

Was der Benutzer auf diesem Bildschirm sieht

Ein Benutzer findet dort typischerweise:

- ein Formular zum **Vorschlagen einer governierten Aktion**;
- die Auswahl des **Aktionstyps**;
- die Auswahl des **Ausführungs-Connectors** oder der **Ausführungsoption**;
- eine Zusammenfassung der **Readiness**, die anzeigt, was verfügbar oder blockiert ist;
- Felder wie **Titel**, **Begründung**, **Ziel**, **Nachricht** oder **Ticketbeschreibung**;
- eine **Genehmigungs- und Ausführungswarteschlange** mit bereits eingereichten Anfragen.

Schritt-für-Schritt - eine gouvernierte Aktion erstellen

Schritt 1 - Öffnen des Bildschirms

Im **Workspace** öffnen Sie **Actions & approvals**.

Schritt 2 - Wählen Sie den Aktionstyp

Wählen Sie zunächst die geschäftliche Absicht. Die sichtbaren Aktionstypen umfassen unter anderem:

- **Publish artifact to SharePoint;**
- **Send Teams message;**
- **Send Outlook message;**
- **Create Jira ticket;**
- **Create Azure DevOps ticket;**
- **Webhook** je nach Tenant-Konfiguration.

Schritt 3 - Prüfen Sie die kompatible Ausführungsoption

Die Oberfläche sucht dann nach **kompatiblen Ausführungsoptionen**.

Wählen Sie eine Option:

- **gesund;**
- **autorisiert;**
- tatsächlich für Ihr Projekt geöffnet.

Wenn keine gesunde Option erscheint, betrifft die Prüfung meist:

- den Connector selbst;
- seinen Gesundheitszustand;
- die Projektbindung;
- die Richtlinie;
- oder Ihre Berechtigung.

Schritt 4 - Lesen Sie die Readiness

Der Bereich **Execution readiness** dient dazu, zu prüfen, ob Sie nicht nur eine theoretische Aktion vorbereiten.

In der Praxis:

- **available / healthy** = Option nutzbar;
- **blocked by health** = Connector auf Plattformseite prüfen;
- **blocked by entitlement** = Legacy-Bezeichnung für eine Blockierung ohne Planbezug; prüfen Sie Konfiguration, Binding, Policy, Berechtigung, Genehmigung oder Health;
- **blocked by policy** = restriktive Projekt-Governance;
- **blocked by permission** = Ihre Rolle reicht nicht aus;
- keine sichtbare Option = kompatibler Connector fehlt, die Projektbindung fehlt oder die Option ist für Ihre Rolle nicht geöffnet.

Nüchterne Lesart eines Bildschirms, der leer wirkt

Wenn **Actions & approvals** nichts Ausführbares zeigt, unterscheiden Sie zunächst drei Fälle, bevor Sie von einer Störung ausgehen:

1. die Verfügbarkeit der Ausführungsoptionen konnte nicht geladen werden;
2. kompatible Optionen existieren, bleiben aber blockiert oder nicht gesund;
3. für den aktuellen gouvernierten Aktionstyp ist noch keine kompatible Option konfiguriert.

In allen drei Fällen ist dies etwas anderes als eine Warteschlange, die einfach leer ist, weil noch niemand eine Aktion vorgeschlagen hat.

WAS SIE SEHEN	WAHRSCHEINLICH DOMINIERENDE URSACHE	NÜTZLICHER REFLEX
kein auswählbarer Connector	kein kompatibler und gesunder Connector ist bereit	zuerst Projektintegrationen , dann Plattformverwaltung prüfen
sichtbare Aktion, aber blockierter Button	Berechtigung, Richtlinie oder Genehmigung erforderlich	zuerst die Rolle, dann die Governance prüfen
sichtbare Warteschlange, aber nichts geht raus	die Anfrage wartet noch auf Genehmigung oder nachgelagerte Ausführung	den tatsächlichen Warteschlangenstatus erneut lesen
Connector vorhanden, aber nicht nutzbar	Binding, Health, Konfiguration, Policy oder Berechtigung reichen nicht aus	die gesamte Kette Plattform -> Projekt -> Richtlinie prüfen

Beachten Sie außerdem: Hier erscheinen nur Ausführungsoptionen, die unternehmensseitig freigegeben sind. Die technische Vorbereitung des Connectors erfolgt in **Plattformverwaltung**, die Projektexponierung lesen Sie über **Projektintegrationen**.

Schritt 5 - Füllen Sie Titel und Begründung aus

Geben Sie anschließend ein:

- einen **klaren Titel**;
- eine **kurze, aber nützliche Begründung**;
- die spezifischen Felder für den gewählten Aktionstyp.

Die Begründung muss zwei Fragen beantworten:

1. **Warum ist diese Aktion notwendig?**
2. **Auf welchen Beweisen oder Entscheidungen basiert sie?**

Schritt 6 - Füllen Sie die geschäftlichen Felder aus

Die Felder ändern sich je nach Aktionstyp.

AKTIONSTYP	HÄUFIG ERWARTETE FELDER
SharePoint-Veröffentlichung	Titel, Begründung, <code>artifact ID</code> , Ziel, Renderprofil, Format
Teams-Nachricht	Titel, Begründung, Nachrichtentext
Outlook-Nachricht	Titel, Begründung, Empfänger, Betreff, Nachrichtentext
Jira-Ticket	Titel, Begründung, Ticketbeschreibung, ggf. Projekt-/Board-Schlüssel
Azure DevOps Ticket	Titel, Begründung, Beschreibung, Tickettyp je nach Connector
Webhook	Titel, Begründung und Daten für das Zielsystem

Schritt 7 - Vorschlagen der Aktion

Sobald die Felder ausgefüllt sind, reichen Sie die Anfrage ein.

An diesem Punkt ist die Aktion noch nicht unbedingt ausgeführt. Sie kann zuerst in die **Genehmigungs-Queue** einsteigen.

Schritt 8 - Überprüfung durch den Genehmiger

Wenn die Richtlinie `require_approval` verlangt, muss ein Genehmiger prüfen:

- den Titel;
- die Begründung;
- den verwendeten Connector;
- das Nutzlast- oder geschäftliche Detail;
- das eventuell verknüpfte Artefakt oder den Entwurf.

Schritt 9 – Genehmigung, Ablehnung oder Ausführung

Je nach Richtlinie und Rolle des Genehmigers kann die Anfrage:

- **genehmigt**;
- **abgelehnt**;
- dann **ausgeführt** werden, wenn alles bereit ist.

Schritt 10 – Prüfen der endgültigen Spur

Nach Ausführung prüfen Sie:

- die Aktionswarteschlange;
- die Projektaktivität;
- die **Trace ID**, falls angezeigt;
- das **Journal IA**, falls der Fluss dort reflektiert wird;
- das Vorhandensein des Artefakts, Tickets oder der Nachricht im Zieltool.

Wie man die Aktionsstatus liest

STATUS	WAS ES BEDEUTET
draft	Die Anfrage ist noch vorbereitend
pending approval	Genehmigung wird vor echter Fortsetzung erwartet
approved	Die Anfrage wurde akzeptiert
executed	Die Aktion wurde tatsächlich gestartet
rejected	Die Anfrage wurde abgelehnt
failed	Die Aktion wurde gestartet, aber nicht korrekt abgeschlossen
cancelled	Die Anfrage wurde abgebrochen

Schritt-für-Schritt-Beispiel - Veröffentlichung eines Artefakts zu SharePoint

Situation

Das Team hat ein **wöchentliches Briefing** gelesen und möchte es in SharePoint veröffentlichen.

Ablauf

1. öffnen Sie **Actions & approvals**;
2. wählen Sie **Publish artifact to SharePoint**;
3. wählen Sie eine gesunde **SharePoint publish**-Option;
4. geben Sie den **Titel** der Aktion ein;
5. fügen Sie eine **Begründung** hinzu, z. B.: „Version geprüft und für wöchentliche Verbreitung freigegeben“;
6. geben Sie die **artifact ID** ein;
7. wählen Sie das **SharePoint-Ziel**;
8. wählen Sie das **Renderprofil** oder das **Format**, falls verlangt;
9. schlagen Sie die Aktion vor;
0. falls die Richtlinie es verlangt, warten Sie auf Genehmigung;
1. führen Sie aus;
2. prüfen Sie, dass das Artefakt tatsächlich in SharePoint veröffentlicht und in ProPM Agent verfolgt wird.

Schritt-für-Schritt-Beispiel - ein Jira-Ticket erstellen

Situation

Ein Signal meldet einen wiederkehrenden Blocker mit Planungsimpact.

Ablauf

1. öffnen Sie **Actions & approvals**;

2. wählen Sie **Create Jira ticket**;
3. wählen Sie einen verfügbaren Jira-Connector;
4. geben Sie einen klaren Titel ein, z. B.: „Lieferantenblocker bei kritischem Los“;
5. ergänzen Sie die **Ticketbeschreibung**;
6. fügen Sie die **Begründung** und nützliche Beweise hinzu;
7. schlagen Sie die Anfrage vor;
8. lassen Sie den Genehmiger prüfen, falls die Richtlinie `require_approval` verlangt;
9. führen Sie aus;
0. prüfen Sie anschließend die externe Referenz oder das erstellte Ticket.

Schritt-für-Schritt-Beispiel - Teams- oder Outlook-Nachricht senden

Situation

Das Projekt muss eine interne Gruppe oder einen Sponsor über eine abgeschlossene Überprüfung informieren.

Teams-Ablauf

1. wählen Sie **Send Teams message**;
2. wählen Sie den autorisierten Teams-Connector;
3. verfassen Sie eine kurze und verständliche Nachricht;
4. fügen Sie die Begründung hinzu, falls der Fluss geregelt ist;
5. schlagen Sie vor, lassen Sie ggf. genehmigen, dann ausführen.

Outlook-Ablauf

1. wählen Sie **Send Outlook message**;
2. wählen Sie den Outlook-Connector;
3. geben Sie die **Empfänger** ein;
4. ergänzen Sie **Betreff** und **Nachrichtentext**;
5. schlagen Sie vor, lassen Sie ggf. genehmigen, dann ausführen.

Praktischer Unterschied

- **Teams** eignet sich gut für kollaborative interne Kommunikation;

- **Outlook** eignet sich besser für formellere und gezieltere Kommunikation.

Schritt-für-Schritt-Beispiel – Webhook zu einem Drittanbieter

Situation

Das Unternehmen möchte einen internen Fluss zu einem eigenen Tool auslösen.

Ablauf

1. wählen Sie den Aktionstyp oder den mit dem **Webhook** verbundenen Fluss;
2. wählen Sie die kompatible Webhook-Ausführungsoption;
3. geben Sie Titel und Begründung ein;
4. ergänzen Sie die Daten für das Zielsystem;
5. schlagen Sie die Anfrage vor;
6. lassen Sie genehmigen, falls die Richtlinie es verlangt;
7. führen Sie aus;
8. prüfen Sie das Ergebnis im Zielsystem und im ProPM Agent Audit.

Warum eine Aktion sichtbar, aber nicht ausführbar sein kann

Eine Aktion kann in der Oberfläche sichtbar sein, aber blockiert bleiben, wenn:

- der kompatible Connector nicht gesund ist;
- das Projekt nicht das richtige Binding hat;
- die Projekt-Richtlinie dieses Aktionsniveau verbietet;
- Ihre Rolle nicht erlaubt, vorzuschlagen oder auszuführen;
- eine Genehmigung noch aussteht;
- Connector, Binding, Policy, Berechtigung, Genehmigung oder Health-Zustand den Fluss blockiert.

Was tun, wenn keine Ausführungsoption angezeigt wird

Folgen Sie dieser Reihenfolge:

1. prüfen Sie zuerst **Governance-Richtlinien**;
2. prüfen Sie dann **Projektintegrationen**;
3. öffnen Sie anschließend **Plattformverwaltung**;
4. prüfen Sie schließlich **Konfiguration, Binding, Berechtigung** und den Gesundheitszustand des Connectors.

Vollständiges Szenario - vom Signal zur ausgeführten Aktion

Einfaches Beispiel

1. ein `open`-Signal meldet einen Blocker;
2. das Team liest Zusammenfassung, Erklärung und Beweise;
3. es entscheidet, dass ein Jira-Ticket nötig ist;
4. die Richtlinie erlaubt dem **Projektleiter** zu `propose`, verlangt aber `require_approval`;
5. der Projektleiter erstellt die Anfrage in **Actions & approvals**;
6. der **Projektbesitzer** genehmigt;
7. die Aktion wird zu **executed**;
8. das externe Ticket und die interne Spur bleiben ausgerichtet.

Dieses Szenario fasst die Produktlogik gut zusammen: **sehen, entscheiden, kontrollieren, ausführen, verfolgen**.

Best Practices

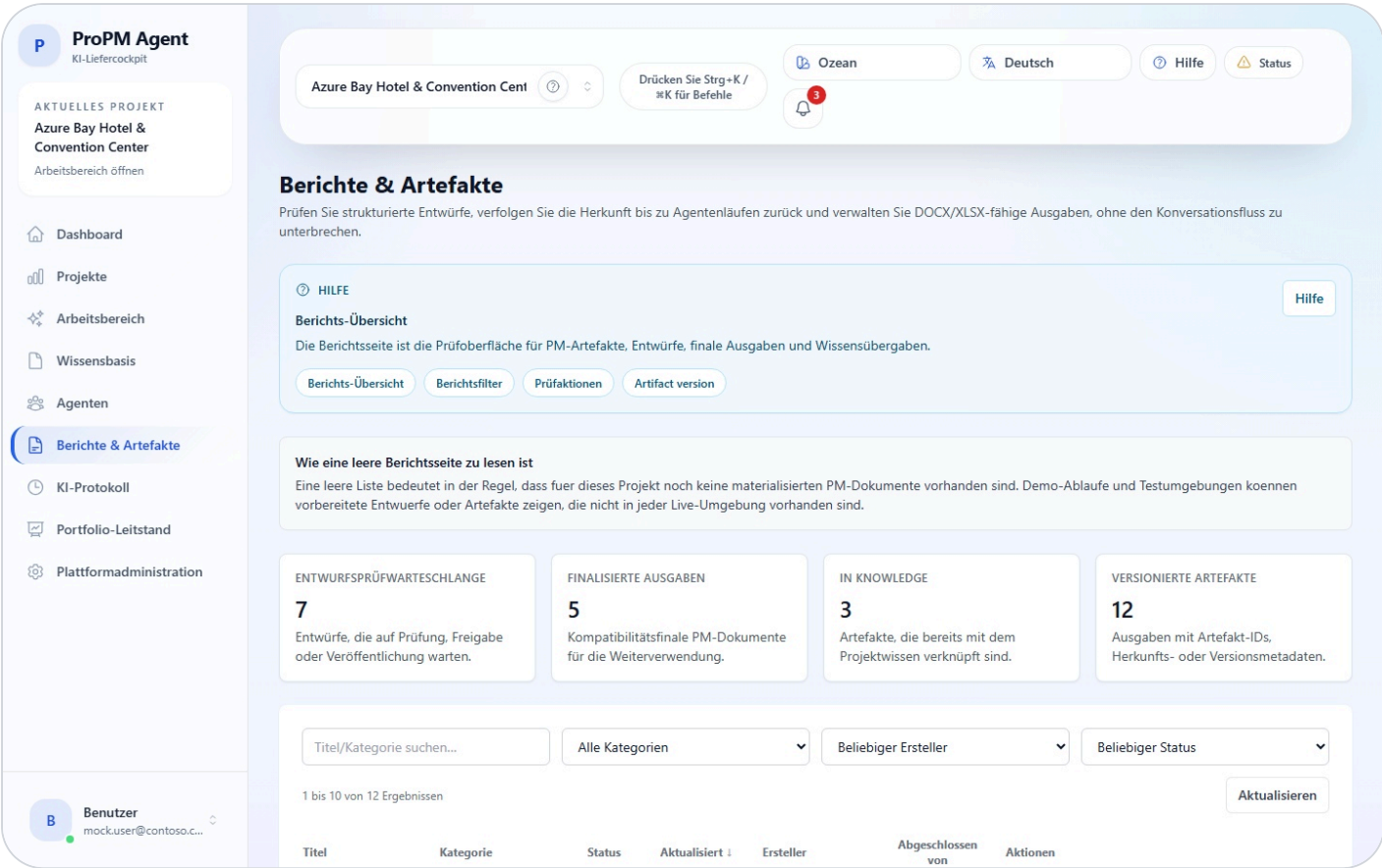
- verwechseln Sie niemals **Entwurf** und **tatsächliche Ausführung**;
- nutzen Sie Richtlinien, um sensible Ausgaben zu begrenzen;
- fordern Sie eine Genehmigung an, sobald ein Inhalt das Projekt verlässt oder ein externes System verändert;
- prüfen Sie immer die Beweise, bevor Sie eine Aktion vorschlagen;
- nutzen Sie das **Journal IA** und die Aktionswarteschlange als gemeinsame Auditquelle.

Weiter

- [Connectoren und Integrationen](#)
- [Berichte, KI-Protokoll und Nachverfolgbarkeit](#)
- [Portfolio und technische Administration](#)
- [Wartung, Support und FAQ](#)

Berichte, KI-Protokoll und Nachverfolgbarkeit

Startseite · Berichte, KI-Protokoll und Nachverfolgbarkeit



Ziel

Diese Seite erklärt den Unterschied zwischen **Artefakt**, **Artefaktversion** und **PM Doc** und erläutert dann die Rolle des **KI-Protokolls** für Audit und Support.

Drei zu unterscheidende Begriffe

BEGRIFF	ROLLE
Artefakt	Veraltetes Objekt, das aus einem Run oder einer Überprüfungsarbeit hervorgeht
Artefaktversion	Genaues Stadium eines Artefakts, mit Historie, Diff und Linie
PM Doc	Überprüftes, bearbeitetes, heruntergeladenes, veröffentlichtes oder in das Wissen zurückinjiziertes Projektdokument

Lebenszyklus

Der häufigste Fluss ist:

1. ein Agent erzeugt eine **strukturierte Ausgabe**;
2. diese Ausgabe wird zu einem **draft artifact**;
3. der Benutzer öffnet **Berichte & Artefakte**;
4. er liest den Inhalt erneut, prüft den **Diff** und die **Linie**;
5. er genehmigt, veröffentlicht, lädt herunter oder fügt das Dokument dem **Wissen** hinzu.

Sichtbare Status

Artefakt

Die auf Artefakt-/Versionsebene bestätigten Status sind:

- draft
- approved
- published
- superseded

PM Doc

PM Docs zeigen mindestens die folgenden Kompatibilitätszustände:

- draft
- final

Wenn Berichte & Artefakte leer wirken

Ein Projekt kann aus mehreren normalen Gründen eine leere Oberfläche zeigen:

- es wurde noch kein **Artefakt** oder **PM-Dokument** erstellt;
- der Run blieb auf der Stufe der **strukturierten Ausgabe** ohne nachgelagerte Umwandlung;
- das falsche Projekt oder ein Filter verbirgt die erwarteten Zeilen;
- die Umgebung enthält nicht dieselben Demo-Seed-Daten wie andere Screenshots oder Tests.

Beginnen Sie in diesem Fall wieder bei **Agenten** oder **KI-Log** und kehren Sie zu **Berichte & Artefakte** zurück, wenn ein gesteuertes Objekt tatsächlich existiert.

Verfügbare Aktionen in Berichte & Artefakte

Der Hub bietet Aktionen wie:

- **review / preview;**
- **diff;**
- **lineage;**
- **edit;**
- **download;**
- **add to knowledge;**
- **publish;**
- **delete.**

Diff, Linie und Versionierung

Diff

Der **Diff** vergleicht Artefaktversionen. Er ist besonders nützlich für:

- das erneute Prüfen von Abweichungen vor der Veröffentlichung;
- das Unterscheiden eines Agentenvorschlags von einer tatsächlich validierten Version;
- das Verstehen, warum sich ein finales Dokument von einem vorherigen Entwurf unterscheidet.

Linie

Die **Linie** verbindet:

- die `source run ID`;
- die `context snapshot ID`;
- die `structured output ID`;
- das Artefakt und seine Version;
- die verknüpften Veröffentlichungen und Nachweise.

Versionierung

Die Oberfläche ermöglicht auch die Auswahl einer Version anhand ihrer Nummer und die Identifizierung der vorherigen Version, der Vergleichsbasis oder einer ersetzten

Version.

Genehmigung und Veröffentlichung

Merken Sie sich folgende Regeln:

- **Approve** für eine Version im Status `draft` verfügbar ist;
- **Publish** verfügbar wird, wenn die Version `approved` oder bereits `published` ist;
- die Veröffentlichung verwaltete Formate und Ziele versendet;
- das Hinzufügen zum Wissen eine vom Herunterladen und Veröffentlichen getrennte Aktion bleibt.

Verfügbare Editoren

Das Produkt enthält mehrere Bearbeitungsoberflächen:

- einen Rich-/Markdown-Editor für dokumentorientierte Ausgaben;
- einen Tabellen-/Grid-Editor für tabellenorientierte Ausgaben;
- einen Review-/Source-Modus im Lesemodus, wenn das Format nicht auf gleiche Weise bearbeitbar ist.

Bestätigte Downloads: **DOCX** und **XLSX**.

Praktische Grenzen, die zu beachten sind

FALL	NÜTZLICHE LEKTÜRE
tatsächlich bearbeitbarer Inhalt	Verwenden Sie den Editor für die Überprüfung und kontrollierten Anpassungen vor der Genehmigung
Inhalt hauptsächlich im Review-Modus	Behandeln Sie den Bildschirm als Validierungsoberfläche, nicht als Hauptort für Neufassungen
Bedarf an einer Referenzdarstellung zur Weitergabe	Der verwaltete Download bleibt die zuverlässigste Ausgabe für die Weitergabe außerhalb der Anwendung

[Zurück zum Reports-Hub](#)

DOCX herunterladen

Zu Knowledge hinzufügen

Markdown kopieren

Löschen

Procurement Plan

Procurement Management Plan

Entwurf

v1

artifact-dem

Lauf run-001

HILFE

Hilfe

Berichtseditor-Übersicht

Der Editor erlaubt Änderungen an einem PM-Dokument, während Artefaktkontext und Prüfsicht sichtbar bleiben.

Berichtseditor-Übersicht

Metadatenfelder

Document title

Document status

Document category

Quell-Markdown

Save changes

Verwenden Sie den Rich-Text-Editor für DOCX-fähige Entwürfe. Die grundlegende Formatierung wird automatisch zurück in das Quell-Markdown gespeichert.

Diff-Zusammenfassung: Draft created for Procurement Plan. Review generated deltas before publication.

Titel

?

Procurement Plan

Status

?

Entwurf

Kategorie

?

Procurement Management Plan

Inhalt (Rich Text für DOCX)

?

Erstellt: 2026-04-21 11:24:45 • Aktualisiert: 2026-04-21 12:29:45

Visuell

HTML

Markdown

B

I

U

S

</>

Link einfügen

Absatz

"

.

1.

--

Tbl

Rückgängig

Wiederholen

Artefaktkontext

Kompatibilitätsmetadaten, die diesen bearbeitbaren Entwurf mit dem Artefakt-Lebenszyklus verknüpfen.

ARTEFAKT-ID

artifact-demo-hotel-001-pm-doc-012

ARTEFAKTVERSION

artifact-demo-hotel-001-pm-doc-012-v1

QUELLLAUF

run-001

RENDERING-PROFIL

docx-default

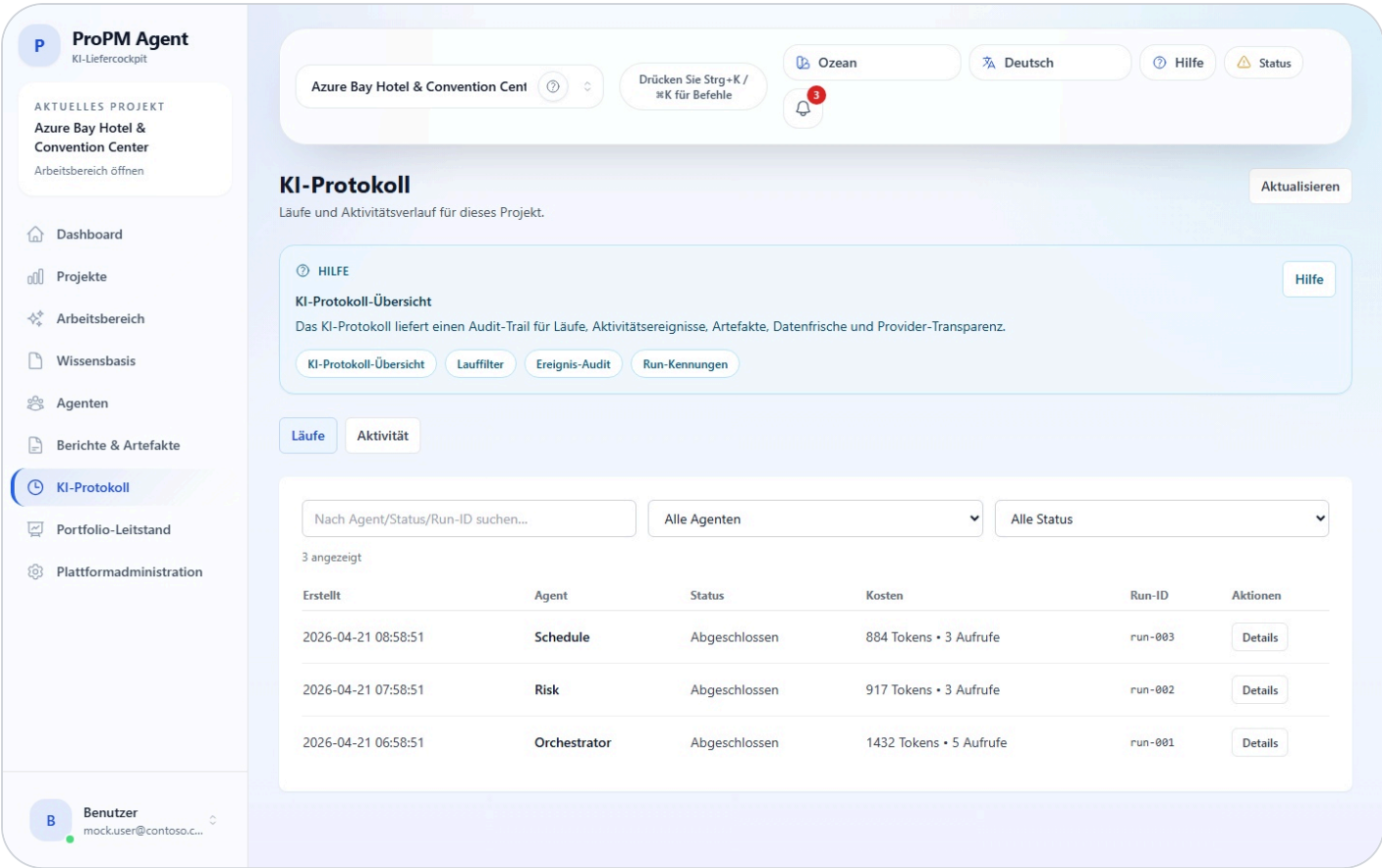
Artefaktprüfung

Prüfen Sie die Vorschauinhalte, vergleichen Sie Entwurfsunterschiede und inspizieren Sie die Herkunft vor der Veröffentlichung.

Status: Entwurf

Version: v1

artifact_oc-012



KI-Protokoll: Was die Seite abdeckt

Das **KI-Protokoll** hat zwei separate Tabs:

- **Runs;**
- **Activity.**

Runs vs. Activity

TAB	WOZU ER DIENT
Runs	Eine Agentenausführung, ihre Nachverfolgungs-Metadaten und ihre verknüpften Artefakte überprüfen
Activity	Eine Projekt-Zeitleiste überprüfen und die Rohdaten eines Ereignisses inspizieren

Wann Runs öffnen

Öffnen Sie **Runs**, um:

- zu verstehen, warum ein Ergebnis erzeugt wurde;
- den tatsächlich verwendeten Provider wiederzufinden;
- Aktualität, Vertrauen und Zitate erneut zu prüfen;
- einen Run mit einem Artefakt oder einem PM Doc zu verknüpfen.

Wann Activity öffnen

Öffnen Sie **Activity**, um:

- eine Chronologie zu rekonstruieren;
- zu überprüfen, ob ein Entwurf, eine Genehmigung oder eine Veröffentlichung ein Ereignis hinterlassen hat;
- die Rohdaten zu inspizieren, wenn Sie Support oder Audit durchführen.

Beispiele nützlicher Ereignisse, die in Activity zu bestätigen sind

Je nach Fluss kann **Activity** Ihnen helfen zu bestätigen, dass ein nachgelagertes Ereignis aufgezeichnet wurde, z.B.:

- Erstellung eines Entwurfs;
- Genehmigung eines Artefakts;
- Veröffentlichung;
- Vorbereitung einer Benachrichtigung;
- Entscheidung über Genehmigung, Ablehnung oder verwaltete Ausführung.

Konkrete Beispiele für **Type** / **Kind**

Die folgenden Werte dienen als Orientierung für häufige Ereignisse.

TYPE	KIND	PRAKTISCHE LESART
agent_execution	completed / failed	ein Agenten-Run wurde erfolgreich oder mit Fehler beendet
document_upload	started / completed / failed	ein Dokument begann seine Verarbeitung, beendete sie oder schlug fehl
report_generated	completed	ein PM Doc oder Bericht wurde generiert und protokolliert
marketplace_update	completed	eine Systembenachrichtigung oder -aktualisierung wurde im Verlauf aufgezeichnet

Sichtbare Filter und Spalten

Runs

Verfügbare Filter:

- Suche nach Agent / Status / Run ID;

- Agentenfilter;
- Statusfilter.

Sichtbare Spalten: **Created**, **Agent**, **Status**, **Cost**, **Run ID**, **Actions**.

Das Feld **Cost** zeigt, wenn verfügbar, mindestens die **Tokens** und die Anzahl der **Calls** an.

Praktische Lesart von **Trace ID**, **Cost**, **Confidence** und **Source freshness**

Behalten Sie für Support und Prüfung diese einfache Lesart im Kopf:

- **Run ID** ist der praktischste Anker, um eine sichtbare Zeile in **Runs** wiederzufinden;
- **Trace ID** ist die wichtigste Kennung für Support, Audit und serviceübergreifende Diagnose. Geben Sie sie bei Eskalationen immer mit weiter;
- **Cost** (**tokens** / **calls**) zeigt den Laufzeitverbrauch zur Transparenz und Untersuchung. Der Wert ist allein kein fachliches Freigabesignal;
- **Confidence** ist ein Prüfhinweis, keine eigenständige Beweisführung. Bei niedrigen Werten lesen Sie Antwort, Zitate und Artefakt erneut;
- **Source freshness** zeigt, wie aktuell die zitierten Nachweise noch sind. Bei **aging**, **stale**, **conflicting** oder **unavailable** prüfen Sie die Quellen vor externer Weitergabe erneut.

Wenn Sie einen portfolioweiten Hinweis auf Budget- oder Nutzungsdruck suchen, ist **cost_pressure** im **Portfolio** aussagekräftiger als die rohe **Cost**-Anzeige eines einzelnen Runs.

Activity

Verfügbare Filter:

- Suche nach Type / Kind / Actor;
- Type-Filter;
- Kind-Filter.

Sichtbare Spalten: **Created**, **Type**, **Kind**, **Actor**, **ID**, **Actions**.

In einem Run sichtbare technische Details

Die Detailansicht eines Runs kann zeigen:

- **Trace ID** ;
- **Context snapshot ID** ;

- **Structured output ID** ;
- Zitate;
- **Effective AI Provider** ;
- **Deployment-selected AI Provider** ;
- **Model family** ;
- **Confidence** ;
- **Source freshness** ;
- verknüpfte Artefakte.

Laufzeit-Transparenz der KI

Die folgende Unterscheidung ist wichtig:

- **für die Bereitstellung ausgewählter KI-Provider**: anfängliche Wahl der Umgebung;
- **effektiver KI-Provider**: tatsächlich für diesen Run verwendeter Provider.

Diese beiden Werte können abweichen. Im Zweifelsfall ist das **KI-Protokoll** für den betreffenden Run maßgeblich.

Praktische Lesart von **Effective AI Provider**

Effective AI Provider beantwortet die Frage: „**Welcher Anbieter hat diesen konkreten Run tatsächlich bedient?**“

Für Support und Ursachenanalyse ist dieser Wert verlässlicher als eine Annahme aus der Administrationskonfiguration, weil er den zur Laufzeit tatsächlich aufgelösten Anbieter zeigt. Wenn **Deployment-selected AI Provider** und Laufzeitwert voneinander abweichen, orientieren Sie sich für diesen Vorfall immer am **Effective AI Provider** im Run.

Je nach Symptom zuerst zu öffnende Oberfläche

SYMPTOM	ZUERST ZU ÖFFNENDE OBERFLÄCHE	WARUM
Inhaltsabweichung zwischen Entwurf und finaler Version	Diff	um zu sehen, was sich tatsächlich geändert hat

SYMPTOM	ZUERST ZU ÖFFNENDE OBERFLÄCHE	WARUM
Zweifel am Nachweis oder der Herkunft	Linie	um Run, strukturierte Ausgabe, Artefakt und Quellen zu verknüpfen
Zweifel an der Laufzeit, dem Provider oder der KI-Ausführung	Runs	um Trace ID , effektiven Provider, Aktualität und Vertrauen erneut zu prüfen
Zweifel an der Veröffentlichung, Genehmigung oder nachgelagerten Folge	Activity	um die Chronologie und die Rohdaten zu bestätigen

Empfohlener Untersuchungs-Workflow

Wenn ein Liefergegenstand, eine Veröffentlichung oder eine Benachrichtigung zweifelhaft erscheint, gehen Sie vom Sichtbarsten zum Technischsten:

1. öffnen Sie das betreffende **PM Doc** oder Artefakt;
2. prüfen Sie den **Diff**, um zu sehen, was sich tatsächlich geändert hat;
3. öffnen Sie die **Linie**, um **source run ID**, **Context snapshot ID** und **Structured output ID** zu notieren;
4. wechseln Sie zu **Runs**, um Aktualität, Vertrauen, Zitate, effektiven KI-Provider und verknüpfte Artefakte erneut zu prüfen;
5. verwenden Sie **Activity**, um den weiteren Fluss zu bestätigen: Entwurf, Genehmigung, Veröffentlichung, Benachrichtigung oder verwaltete Aktion;
6. behalten Sie schließlich die **Trace ID**, falls die Untersuchung vom Support oder Audit wiederaufgenommen werden muss.

Fall 1 — ein finales PM Doc scheint falsch

1. öffnen Sie das finale **PM Doc** und bestätigen Sie die tatsächlich veröffentlichte Version;
2. verwenden Sie **Diff**, um zu erkennen, was hinzugefügt, entfernt oder umformuliert wurde;
3. öffnen Sie **Linie**, um die **source run ID** und **Structured output ID** wiederzufinden;
4. prüfen Sie in **Runs** die Nachweise, die Aktualität und den effektiven Provider;
5. wenn der finale Inhalt nicht den erwarteten Fluss widerspiegelt, beenden Sie in **Activity**, um die Genehmigung, Veröffentlichung und den Akteur zu überprüfen, der

die Version vorangetrieben hat.

Fall 2 — eine vorbereitete Aktion oder Benachrichtigung ist nicht erfolgt

1. gehen Sie vom sichtbaren Entwurf, der Aktionswarteschlange oder der Benachrichtigung aus;
2. notieren Sie `relatedArtifactId` oder `relatedNotificationId`, falls vorhanden;
3. verwenden Sie **Activity**, um zu bestätigen, ob eine Genehmigung, Ablehnung oder Ausführung protokolliert wurde;
4. wenn die Folge unklar bleibt, kehren Sie zu **Runs** zurück, um den Quell-Run und die Logik zu überprüfen, die die Empfehlung erzeugt hat;
5. dokumentieren Sie schließlich die **Trace ID** und die verknüpften IDs, bevor Sie eskalieren.

Welche IDs vorrangig zu behalten sind

ART DES VORFALLS	VORRANGIG ZU BEHALTENDE IDS
zweifelhaftes Run-Ergebnis	<code>Trace ID</code> , <code>Context snapshot ID</code> , <code>Structured output ID</code>
verdächtiges finales Artefakt oder PM Doc	<code>source run ID</code> , <code>Structured output ID</code> , betreffende Artefaktversion
Aktion oder Benachrichtigung ohne klare Folge	<code>Trace ID</code> , <code>relatedArtifactId</code> , <code>relatedNotificationId</code>
übergreifende Support-Untersuchung	alle oben genannten IDs, plus ungefähre Uhrzeit und betreffendes Projekt

Best Practices für Nachverfolgbarkeit

- behalten Sie die **Trace ID**, wenn ein Ergebnis wichtig ist;
- prüfen Sie vor der Veröffentlichung die Linie zwischen Liefergegenstand und Nachweis;
- verwenden Sie bei Abweichungen zwischen zwei Versionen den **Diff** vor der Entscheidung;
- fügen Sie dem **Wissen** nur tatsächlich überprüfte Liefergegenstände hinzu;

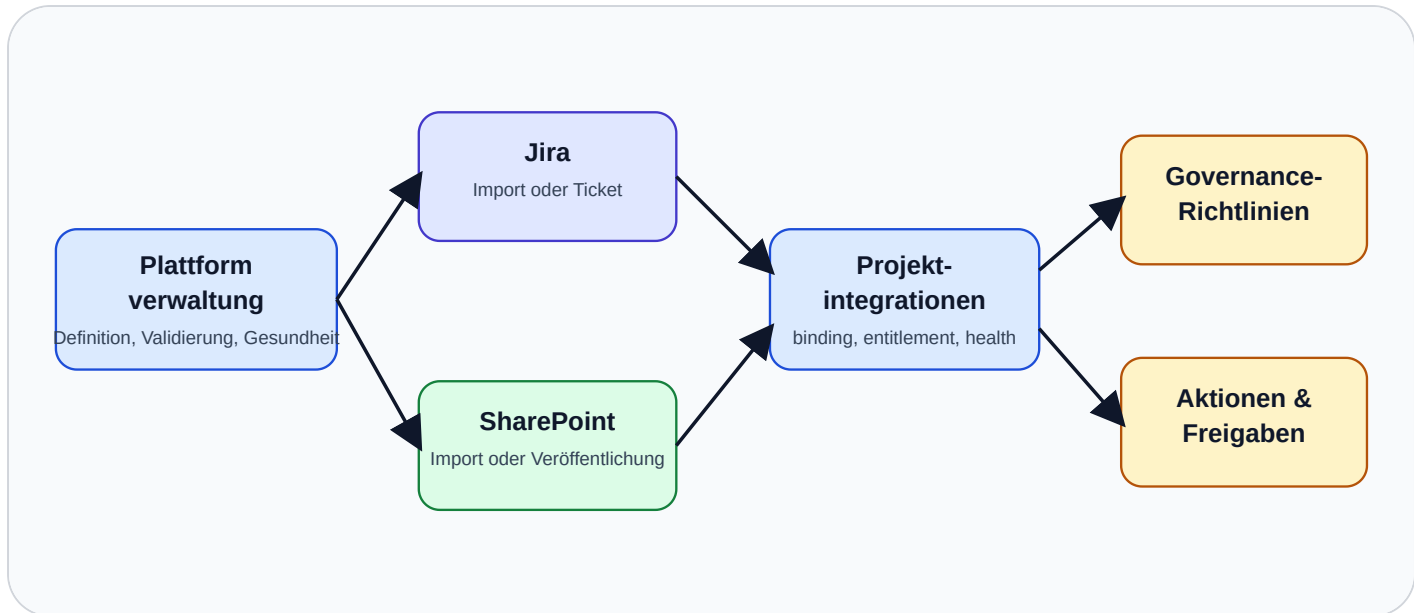
- verwenden Sie **Activity**, um die Untersuchung zu vervollständigen, wenn **Runs** nicht ausreicht.

Weiterführend

- [Strukturierte Ausgaben, Nachweise und Aktualität](#)
- [Portfolio und technische Administration](#)
- [Wartung, Support und FAQ](#)
- [Glossar](#)

Connectoren und Integrationen

[Startseite](#) · Connectoren und Integrationen



Ziel

Diese Seite erklärt den **operativen Katalog der in ProPM Agent unterstützten Connectoren und Ingestionsanbieter**, ihre Vorteile, ihre geschäftliche Nützlichkeit und wie sie in das Produkt integriert werden. Einige Verwaltungsverzeichnisse können zusätzlich erweiterbare oder kundenspezifische Familien anzeigen, die vor realer Nutzung weitere Konfiguration und Validierung benötigen.

Das Ziel ist es, drei einfache Fragen zu beantworten:

1. **Wozu dient dieser Connector?**
2. **Wo sieht man ihn in ProPM Agent?**
3. **Wie geht man von einem deklarierten Connector zu einem tatsächlich nutzbaren Connector über?**

Einen Connector in ProPM Agent verstehen

Ein Connector ist eine **kontrollierte Brücke** zwischen ProPM Agent und einem anderen Unternehmenswerkzeug.

Im Produkt kann ein Connector drei verschiedene Dinge tun:

TYP	ZWECK	BEISPIEL
Ausführungs-Connector	eine Aktion an ein externes Tool senden	ein Jira-Ticket erstellen, eine Teams-Nachricht senden, in SharePoint veröffentlichen
Ingestionsanbieter	Inhalt in das Wissen importieren	SharePoint-Dokumente, Confluence-Seiten, Azure DevOps Work Items importieren
Artefaktziel	ein überarbeitetes Deliverable in ein Ziel veröffentlichen	ein PM-Dokument in SharePoint veröffentlichen

Einfache Regel zum Behalten

- **Importieren** ist nicht dasselbe wie **Veröffentlichen**.
- **Ein Connector sehen** ist nicht dasselbe wie ihn **ausführen** zu können.
- Ein Connector kann auf **Plattformebene** existieren, ohne noch für ein Projekt geöffnet zu sein.

Wie ein Connector in ProPM Agent integriert wird

Unabhängig vom Connector ist der logische Ablauf immer gleich:

1. Der Administrator bereitet ihn in **Plattform Administration** vor;
2. Er validiert die Konfiguration und, wenn aktiviert, die reale Konnektivität;
3. Der Connector wird in **Project Integrations** verfügbar gemacht;
4. Die **Governance Policies** bestimmen, wer ihn nutzen kann und auf welcher Ebene;
5. Das Team nutzt ihn anschließend in **Knowledge, PM Documents** oder **Actions & approvals**;
6. Die endgültige Spur bleibt in der **Project Activity** und im **Journal IA** sichtbar.

Wo der Benutzer die Connectoren im Produkt sieht

OBERFLÄCHE	WAS DORT GEMACHT WIRD
Plattform Administration	technische Definition erstellen, Authentifizierung angeben, validieren, je Anbieter testen und bei Bedarf Probes aktivieren

OBERFLÄCHE	WAS DORT GEMACHT WIRD
Project Integrations	prüfen, welche Connectoren tatsächlich für das aktuelle Projekt geöffnet sind
Knowledge	Dokumente, Seiten, Tickets, Work Items oder andere Quellen je verfügbarem Anbieter importieren
Governance Policies	entscheiden, welche Rollen Aktionen beobachten, vorschlagen oder ausführen dürfen
Actions & approvals	eine Aktionsanfrage vorbereiten, genehmigen lassen und ausführen, wenn der Connector-Modus dies erlaubt
Journal IA / activity	den Fluss und die Ausführungen nachvollziehen

Drei Ebenen, die nicht verwechselt werden sollten

EBENE	WAS DAS BEDEUTET	RICHTIGES LESEN
Platform	Der Connector existiert technisch	er ist definiert, authentifiziert und global kontrolliert
Project	Der Connector ist für ein bestimmtes Projekt geöffnet	das Projekt kann ihn als potenzielle Option sehen
Governed usage	Der Connector kann in einem realen Fluss verwendet werden	der Benutzer hat die richtige Rolle, die richtige Politik und eine gesunde Ausführungsoption

Sichtbare Ausführungs-Connectoren

Ausführungs-Connectoren dienen dazu, **eine Aktion** von ProPM Agent an ein externes Tool zu senden.

Der Bildschirm **Projektintegrationen** zeigt diese aktivierten Ausführungs-Connectoren als bindbar, wenn sie noch nicht mit dem Projekt verknüpft sind.

Aktueller Katalog der Ausführungs-Connectoren

CONNECTOR IN DER OBERFLÄCHE	HAUPTNUTZEN	TYPISCHE PROJEKTAKTION
Asta Powerproject schedule sync	Unternehmenspläne und Baselines synchronisieren	binden, wenn Terminplanänderungen über einen governierten Projektkanal laufen müssen
Azure DevOps delivery project	Work Items erstellen oder aktualisieren und Delivery nachverfolgen	binden für Teams mit Boards, Sprints oder Delivery-Backlogs
Jira delivery workspace	Issues und Delivery-Follow-up erstellen oder aktualisieren	binden, wenn Risiken, Blockaden oder Entscheidungen zu governierten Jira-Tickets werden sollen
Microsoft Project schedule sync	Microsoft-Project-Terminpläne synchronisieren	binden, wenn der Masterplan in Microsoft Project gepflegt wird
Microsoft Teams collaboration	governierte Kollaborationsnachrichten und Genehmigungsbenachrichtigungen senden	binden für kontrollierte Team-Benachrichtigungen
Outlook executive notifications	governierte E-Mails oder Stakeholder-Updates senden	binden für formelle Kommunikation an benannte Empfänger
SharePoint publication library	geprüfte Artefakte in eine SharePoint-Bibliothek veröffentlichen	binden, wenn genehmigte PM-Lieferobjekte über SharePoint verteilt werden
Smartsheet portfolio workspace	Portfolio-Sheets und Workspace-Daten aktualisieren	binden, wenn Portfolio-Tracking in Smartsheet erfolgt
Webhook event delivery	einen bestimmten Enterprise- oder internen Endpoint aufrufen	binden für kundenspezifische nachgelagerte Automatisierung
Wrike delivery workspace	Aufgaben, Verantwortliche und Delivery-Koordination aktualisieren	binden, wenn Wrike die operative Delivery-Arbeit trägt

Sichtbare Ingestionsanbieter

Ingestionsanbieter dienen dazu, **Inhalt in ProPM Agent zu bringen**, um das **Wissen** zu bereichern.

Der Projektbildschirm trennt bereits gebundene Anbieter von Anbietern **Available to bind**. Zähler variieren je Tenant, aber die Oberfläche unterscheidet gesunde Bindings von Katalogeinträgen, die noch Projektbindung oder Plattformkonfiguration benötigen.

Aktueller Katalog der Ingestionsanbieter

ANBIETER IN DER OBERFLÄCHE	ANGEZEIGTER MODUS ODER QUELLE	HAUPTNUTZEN	READINESS-HINWEIS
Smartsheet sheet import	Smartsheet · Scheduled	Portfolio-Sheets in Wissen aktualisieren	kann als gebunden und Healthy erscheinen
Azure Data Factory evidence pipeline	ADF · Pipeline	Nachweise, RAID und Reporting-Refreshes importieren	kann als gebunden und Healthy erscheinen
Asta Powerproject schedule import	Asta Powerproject Import · Manual	Terminplan-Snapshots und Baselines importieren	bindbar, wenn Ready
Azure Blob document ingest	Blob Storage · Scheduled	gouvernierte Dokumentablagen und Archiv-Refreshes ingestieren	bindbar, wenn Ready
Confluence knowledge import	Confluence · Manual	Wiki-Seiten und Prozesswissen importieren	kann Not configured anzeigen, bis die Quelle vollständig ist
Jira issue import	Jira · Scheduled	Issues, Blockaden und Follow-up-Nachweise importieren	kann Not configured anzeigen, bis die Quelle vollständig ist
Microsoft Project schedule import	MS Project Import · Manual	Terminplan-Baselines und Aktualisierungen importieren	bindbar, wenn Ready
SFTP document intake	SFTP · Scheduled	Dokumentablagen von Dritten importieren	kann Not configured anzeigen, bis Host, Ordner und Zugangsdaten vollständig sind
SharePoint knowledge import	SharePoint · Manual	Wissensbibliotheken und Reporting-Artefakte importieren	bindbar nach Einrichtung von Site und Bibliothek
Wrike task import	Wrike · Scheduled	Aufgaben, Verantwortliche und Workflow-Nachweise importieren	bindbar nach Workspace-Einrichtung

Connectoren, die in mehreren Rollen vorkommen

Einige Namen erscheinen an mehreren Stellen im Produkt. Das ist normal: Importanbieter und Ausführungs-Connector bleiben getrennte Bindings.

FAMILIE	IMPORTROLLE	AUSFÜHRUNGSROLLE	RICHTIGES LESEN
SharePoint	SharePoint knowledge import	SharePoint publication library	kann Dokumente lesen und ein geprüftes Artefakt veröffentlichen, aber jede Rolle hat eigenes Setup und Binding
Jira	Jira issue import	Jira delivery workspace	kann Jira-Kontext importieren und anschließend ein governiertes Ticket erstellen, wenn auch der Ausführungs-Connector gebunden ist
Microsoft Project	Microsoft Project schedule import	Microsoft Project schedule sync	kann Terminplan-Nachweise in Wissen bringen und governierte Planänderungen synchronisieren
Smartsheet	Smartsheet sheet import	Smartsheet portfolio workspace	kann Portfolio-Nachweise aktualisieren und Smartsheet als Ausführungsziel aktualisieren
Wrike	Wrike task import	Wrike delivery workspace	kann operative Aufgaben-Nachweise importieren und Wrike-Aufgaben über governierte Aktionen aktualisieren
Asta Powerproject	Asta Powerproject schedule import	Asta Powerproject schedule sync	kann Terminplan-Snapshots importieren und kontrollierte Planänderungen synchronisieren
Azure DevOps	—	Azure DevOps delivery project	als Ausführungs-Connector verfügbar; ein Importpfad sollte separat validiert werden, wenn er verfügbar ist
ADF / Blob / Confluence / SFTP	nur Ingestionsanbieter	—	sie bereichern Wissen und werden nicht automatisch zu Aktionszielen

FAMILIE	IMPORTROLLE	AUSFÜHRUNGSROLLE	RICHTIGES LESEN
Teams / Outlook / Webhook	—	nur Ausführungs-Connector	sie senden governierte Nachrichten oder Ereignisse und importieren nicht automatisch Wissen

Unterstützter Katalog vs. erweiterbare Optionen

Der obige Katalog ist der operative Katalog, der aktuell initialisiert, geprüft und in **Project Integrations** angezeigt wird. **Platform Administration** kann zusätzlich weitere oder kundenspezifische Familien wie GitHub, GitLab, ServiceNow, Slack, Notion, Google Drive, OneDrive, Box oder Dropbox anzeigen.

Behandeln Sie diese zusätzlichen Einträge als Erweiterungen, bis ein Administrator technische Definition, Pflichtfelder, Authentifizierungsstrategie, Validierung, Projekt-Binding und passende Governance-Policy bestätigt hat.

Mindestkonfiguration je Ausführungs-Connector

Die folgenden Felder sind vor einer Nutzung in **test** oder **live** mindestens auszufüllen. Die Feldnamen können je Formular leicht variieren, aber das Prinzip bleibt gleich: ein Ziel, eine Authentifizierungsidentität und ein explizites Projektziel.

CONNECTOR	MINDESTFELDER VOR TEST/LIVE-NUTZUNG	TYPISCHE AUTHENTIFIZIERUNG	CONNECTIVITY-PROBE, WENN AKTIVIERT
Jira delivery workspace	<code>base_url</code> oder <code>site_url</code> , <code>project_key</code>	API key, basic, PAT, bearer token oder OAuth	liest das Zielprojekt in Jira
Azure DevOps delivery project	<code>organization_url</code> oder <code>organization</code> , <code>project</code> , <code>work_item_type</code>	PAT, bearer token oder OAuth	prüft den Work-Item-Typ im Projekt
Microsoft Teams collaboration	<code>team_id</code> , <code>channel_id</code>	Microsoft Graph mit bearer token, OAuth, client credentials oder managed identity	liest den Zielkanal in Teams

CONNECTOR	MINDESTFELDER VOR TEST/LIVE-NUTZUNG	TYPISCHE AUTHENTIFIZIERUNG	CONNECTIVITY-PROBE, WENN AKTIVIERT
Outlook executive notifications	<code>mailbox</code> , <code>user_id</code> oder <code>user_principal_name</code>	Microsoft Graph mit bearer token, OAuth, client credentials oder managed identity	prüft Mailbox oder Graph-Benutzer
SharePoint publication library	<code>site_id</code> oder <code>site_url</code> , <code>drive_id</code> oder <code>library</code>	Microsoft Graph mit bearer token, OAuth, client credentials oder managed identity	prüft Site und Bibliothek
Webhook event delivery	<code>webhook_url</code> oder <code>endpoint_url</code> über HTTPS	keine Auth, API key, bearer token, basic oder OAuth	sendet <code>HEAD</code> , danach bei Bedarf <code>GET</code>
Microsoft Project schedule sync	<code>project_id</code> , <code>portfolio</code> oder <code>workspace</code>	Microsoft Graph mit bearer token, OAuth, client credentials oder managed identity	nutzt den konfigurierten Probe-Endpoint oder Pfad
Smartsheet portfolio workspace	<code>sheet_id</code> oder <code>workspace_id</code>	API key, bearer token, OAuth oder PAT	liest Sheet oder Workspace in Smartsheet
Wrike delivery workspace	<code>folder_id</code> , <code>space_id</code> oder <code>task_id</code>	bearer token oder OAuth	liest Aufgabe oder Ordner in Wrike
Asta Powerproject schedule sync	<code>base_url</code> oder <code>endpoint_url</code> , danach <code>project_id</code> , <code>portfolio</code> oder <code>schedule_id</code>	API key, bearer token, OAuth oder basic	nutzt den konfigurierten Probe-Endpoint oder Pfad

Mindestkonfiguration je Ingestionsanbieter

Ein Ingestionsanbieter muss Quelle, Importmodus und die Identität zum Lesen dieser Quelle benennen. Geplante Importe benötigen außerdem eine kompatible Kadenz oder Orchestrierung.

ANBIETER	MINDESTFELDER VOR REALER NUTZUNG	TYPISCHE AUTHENTIFIZIERUNG	CONNECTIVITY-PROBE, WENN AKTIVIERT
SharePoint knowledge import	<code>site_id</code> oder <code>site_url</code> , <code>drive_id</code> oder <code>library</code>	Microsoft Graph mit bearer token, OAuth, client credentials oder managed identity	prüft Bibliothek und Root-Kinder

ANBIETER	MINDESTFELDER VOR REALER NUTZUNG	TYPISCHE AUTHENTIFIZIERUNG	CONNECTIVITY-PROBE, WENN AKTIVIERT
Azure Data Factory evidence pipeline	subscription_id , resource_group_name , factory oder factory_name , pipeline oder pipeline_name	managed identity, client credentials oder bearer token	liest die Pipeline-Definition
Azure Blob document ingest	account_url , storage_account oder account_name , danach container	managed identity, SAS, bearer token oder client credentials	listet einige Blobs aus dem Container
Confluence knowledge import	base_url , space , space_key oder space_id	basic, bearer token oder OAuth	prüft den Confluence-Space
Jira issue import	base_url oder site_url , danach project , project_key oder jql	API key, basic, PAT, bearer token oder OAuth	führt eine begrenzte Jira-Suche aus
SFTP document intake	host oder base_url , username oder user , folder oder path , gültiger Port falls angegeben	basic, password oder privater SSH-Schlüssel	prüft TCP-Erreichbarkeit des SFTP-Servers
Microsoft Project schedule import	project_id , portfolio oder workspace	Microsoft Graph mit bearer token, OAuth, client credentials oder managed identity	nutzt den konfigurierten Probe-Endpoint oder Pfad
Smartsheet sheet import	sheet_id oder workspace_id	API key, bearer token, OAuth oder PAT	liest Sheet oder Workspace in Smartsheet
Wrike task import	folder_id oder space_id	bearer token oder OAuth	liest Aufgaben aus Ordner oder Space
Asta Powerproject schedule import	base_url oder endpoint_url , danach project_id , portfolio oder schedule_id	API key, bearer token, OAuth oder basic	nutzt den konfigurierten Probe-Endpoint oder Pfad

Validierung, Probes und Runtime-Grenzen

SCHRITT	WAS BESTÄTIGT WIRD	WAS NICHT GARANTIERT WIRD
Save	die Definition ist auf Plattformebene gespeichert	die externe Quelle wurde nicht unbedingt kontaktiert
Validate	Pflichtfelder, Modus, Authentifizierung und HTTPS-URLs sind kohärent	ein echter Netzwerkaufruf erfolgt nur, wenn Probes aktiviert sind
Connectivity probe	ProPM Agent erreicht einen nicht destruktiven Provider-Endpoint	Ticket-Erstellung, Nachrichtenversand oder Vollimport werden nicht ausgelöst
Bind to project	das Projekt kann die Plattformdefinition konsumieren	Policy, Benutzerrolle, Health, Validierung und Binding-Readiness können die Nutzung weiter blockieren
Validate binding	das Projekt-Binding bleibt mit der Plattformdefinition ausgerichtet	es ersetzt keine reale Business-Aktion und keinen realen Import

Connectivity-Probes sind absichtlich opt-in. Ein Administrator kann sie mit

`connectivity_probe_enabled`, `run_connectivity_probe`,
`live_connectivity_check`, äquivalenten Metadaten oder einer Plattform-

Umgebungsvariable aktivieren. Ohne diese Aktivierung bleibt die Validierung eine Konsistenz- und Readiness-Prüfung.

Wenn ein Connector im Modus `mock` oder `test` bleibt, kann ProPM Agent Anfrage, Governance, Genehmigung und Spur verwalten, ohne den finalen Aufruf zwingend an das externe System zu senden. Reale Vendor-Ausführung erfordert einen kompatiblen Connector-Modus, vollständige Konfiguration, eine erlaubende Policy und eine Umgebung, die diesen Pfad aktiviert.

Gouvernierte Aktionen und erforderlicher Connector

BENUTZERAKTION	INTERNER AKTIONSTYP	ERFORDERLICHER CONNECTOR	MINDESTFELDER IM PAYLOAD
Artefakt nach SharePoint veröffentlichen	<code>publish_artifact_to_sharepoint</code>	<code>sharepoint_publish</code>	<code>artifact_id</code> , <code>destination_id</code>
Teams-Nachricht senden	<code>send_teams_message</code>	<code>teams</code>	<code>body</code>

BENUTZERAKTION	INTERNER AKTIONSTYP	ERFORDERLICHER CONNECTOR	MINDESTFELDER IM PAYLOAD
Outlook-Nachricht senden	send_outlook_message	outlook	body , recipients
Jira-Ticket erstellen	create_jira_ticket	jira	title
Azure-DevOps-Work-Item erstellen	create_azure_devops_ticket	azure_devops	title

Einige ältere Bezeichnungen werden automatisch normalisiert. Zum Beispiel wird `send_message` zu `send_teams_message` , `send_email` zu `send_outlook_message` , `create_work_item` zu `create_azure_devops_ticket` und `publish_sharepoint_artifact` zu `publish_artifact_to_sharepoint` .

Status, Blocker und Diagnose-Reihenfolge

SICHTBARER STATUS ODER BLOCKER	PRAKTISCHE BEDEUTUNG	ERSTE EMPFOHLENE AKTION
Ready oder available	die Definition kann gebunden oder genutzt werden, wenn der Rest der Kette offen ist	Projekt-Binding und Policy prüfen
Healthy	die letzte bekannte Validierung ist positiv	bestätigen, dass das Projekt gebunden ist
Not configured	Felder, Quelle, Ziel oder Zugangsdaten fehlen	Definition in Platform Administration vervollständigen
Not validated oder not_tested	die Definition existiert, hat aber die erwartete Validierung oder Prüfung noch nicht bestanden	Validate oder passenden Probe ausführen
Blocked by health	Plattform-Health ist degradiert oder ungültig	Endpoint, Auth, Scopes und Netzwerk prüfen
Blocked by entitlement	Legacy-Bezeichnung für eine blockierte Integration; in Marketplace-Plänen ist dies kein Funktionsunterschied	Konfiguration, Health, Binding, Policy, Rolle und Lizenzverfügbarkeit bei Zugriffsproblemen prüfen

SICHTBARER STATUS ODER BLOCKER	PRAKTISCHE BEDEUTUNG	ERSTE EMPFOHLENE AKTION
Blocked by policy	Projekt-Governance verbietet diese Aktion oder Nutzungsart	Policy oder Rolle anpassen
Binding disabled	das Projekt-Binding existiert, ist aber deaktiviert	Binding erneut aktivieren oder neu erstellen, falls erlaubt
Missing platform definition	das Projekt referenziert eine fehlende oder gelöschte Definition	Plattformdefinition neu erstellen oder korrigieren

Die nützlichste Diagnose-Reihenfolge lautet: Plattformdefinition, Pflichtkonfiguration, Validierung oder Probe, Projekt-Binding, Policy, Benutzerberechtigung, Aktions- oder Import-Payload und danach Lizenzverfügbarkeit, falls der Benutzer nicht auf die App zugreifen kann.

Import, externe Ausgabe und Audit

THEMA	WAS PROPM AGENT NACHVERFOLGT	WAS IM EXTERNEN TOOL ZU PRÜFEN IST
Knowledge-Import	Ingestion-Run, Anbieter, Binding, Source Label, Frische, Zähler und Trace ID	verfügbares Volumen, Quellrechte, Filter, übersprungene Dateien und Deduplizierung
SharePoint-Veröffentlichung	Aktionsanfrage, Genehmigung, Connector, Ziel und Trace ID	finale URL, Bibliothek, Schreibrechte und veröffentlichte Version
Jira oder Azure DevOps	Aktion, Begründung, Business-Payload und Trace ID	Schlüssel des erstellten Tickets oder Work Items, Zielprojekt und Item-Typ
Teams oder Outlook	Anfrage, logische Empfänger oder Kanal, Genehmigung und Trace ID	tatsächliche Zustellung, Kanal, Mailbox und mögliche Graph-Ablehnungen
Webhook	logischer Endpoint, Versuchstatus, Antwort oder Fehler und Trace ID	HTTP-Code, gekürzte Antwort, Signaturvalidierung und nachgelagerte Wiederholung

Legen Sie niemals ein Secret in den Business-Payload einer Aktion oder in eine Benutzernotiz. Secrets, Schlüssel und sensible Referenzen müssen in der dafür vorgesehenen Plattformkonfiguration bleiben.

Sicherheit und Authentifizierung

FAMILIE	ÜBLICHERWEISE AKZEPTIERTE AUTHENTIFIZIERUNG	AUFMERKSAMKEITSPUNKT
Microsoft Graph, Teams, Outlook, SharePoint und Microsoft Project	bearer token, OAuth, client credentials oder managed identity	Scopes auf notwendige Sites, Mailboxen, Kanäle oder Projekte begrenzen
Jira und Confluence	API key, basic, PAT, bearer token oder OAuth je Produkt	technische Konten mit geringstmöglichen Rechten verwenden
Azure DevOps	PAT, bearer token oder OAuth	Rechte auf Projekt und erwartete Work-Item-Typen begrenzen
Azure Data Factory und Blob Storage	managed identity, client credentials, SAS oder bearer token je Service	verwaltete Identitäten bevorzugen und zugängliche Container oder Pipelines begrenzen
SFTP	basic, password oder privater SSH-Schlüssel	Schlüsselrotation, Port und erlaubten Root-Ordner prüfen
Webhook	keine Auth, API key, bearer token, basic oder OAuth	HTTPS, Signatur oder Endpoint-Secret verlangen, wenn das Risiko es rechtfertigt

Beispiel 1 — SharePoint von Anfang bis Ende

SharePoint ist eines der besten Beispiele, um die komplette Logik zu verstehen.

Was SharePoint tun kann

- Dokumente in **Knowledge** importieren;
- als **Artefaktziel** dienen;
- eine **gouvernierte Veröffentlichung** über **SharePoint publish** empfangen.

Schritt-für-Schritt-Prozess

1. Der Administrator bereitet SharePoint in **Platform Administration** vor;
2. Das Projekt holt das SharePoint-Binding in **Project Integrations**;
3. Das Team importiert vorhandene Dokumente in **Knowledge**;
4. Ein PM-Dokument wird verfasst oder überarbeitet;

5. Eine Governance-Politik entscheidet, wer eine Veröffentlichung vorschlagen oder ausführen darf;
6. Die Veröffentlichung passiert über **Actions & approvals**, falls eine Validierung erforderlich ist;
7. Die endgültige Spur bleibt in der Projektaktivität und im **Journal IA** sichtbar.

Vorteile von SharePoint in ProPM Agent

- nutzt ein bereits bekanntes Dokumentenrepository der Teams;
- ermöglicht Import, Dokumentenprüfung und finale Veröffentlichung;
- eignet sich gut für formale Validierungsabläufe.

Beispiel 2 — Jira von Anfang bis Ende

Was Jira tun kann

- Issues und Kommentare als Kontext importieren;
- ein genehmigtes Ticket aus einer Entscheidung oder einem Signal erhalten;
- ein Blockieren in einem externen Tracking-System materialisieren.

Schritt-für-Schritt-Prozess

1. Jira wird in **Plattform Administration** vorbereitet;
2. Es wird im Projekt in **Project Integrations** geöffnet;
3. Das Team prüft ein Signal oder eine Entscheidung;
4. Es erstellt eine Aktion **Create a Jira ticket**;
5. Die Governance entscheidet, ob die Aktion direkt oder genehmigungsabhängig ist;
6. Das Ticket wird erstellt, wenn die Live-Ausführung des Vendors aktiviert ist; in jedem Fall bleiben Anfrage und Entscheidung im Produkt nachvollziehbar.

Vorteile von Jira in ProPM Agent

- wandelt ein Projektbeobachtung in ein formelles Ticket um;
- behält eine klare Spur zwischen Signal, Begründung und erstelltem Ticket;
- vermeidet ungetrackte manuelle Aktionen.

Beispiel 3 — Teams oder Outlook für die Verbreitung

Nutzen

- **Teams** dient zur Verbreitung einer Benachrichtigung im kollaborativen Tool;
- **Outlook** dient zum Versand einer formelleren Kommunikation per E-Mail.

Integration mit ProPM Agent

1. Der Connector wird auf Plattformebene vorbereitet;
2. Das Projekt sieht ihn als Ausführungsoption;
3. Eine Politik definiert, welche Rollen eine Nachricht senden dürfen;
4. Das Team bereitet die Nachricht in **Actions & approvals** vor;
5. Je nach Risiko wird die Aktion genehmigt und ausgeführt, wenn der Connector-Modus dies erlaubt;
6. Die Nachricht bleibt historisiert, auch wenn die externe Zustellung blockiert oder verzögert ist.

Hauptvorteil

Die Verbreitung erfolgt nicht als freie Nachricht, sondern bleibt **gouverniert, geprüft und nachvollziehbar**.

Beispiel 4 — Webhook event delivery

Wann verwenden

Verwenden Sie **Webhook event delivery**, wenn ProPM Agent nach einer governierten Entscheidung einen bestimmten internen oder Drittanbieter-Endpoint aufrufen soll.

Integration mit ProPM Agent

- Im aktuellen Katalog ist Webhook ein **Ausführungs-Connector**;
- binden Sie ihn erst an ein Projekt, nachdem Plattform-Endpoint und Health validiert wurden;

- falls später eine eingehende Webhook-Ingestion ergänzt wird, behandeln Sie sie als separaten Ingestionsanbieter mit eigener Validierung und eigenem Projekt-Binding.

Hauptvorteil

Webhook delivery bietet Flexibilität für kundenspezifische Automatisierung, ohne den Fluss zu einer unkontrollierten Ausgabe zu machen.

Wie man erkennt, ob ein Connector wirklich bereit ist

Um den Connector-Status richtig zu lesen, unterscheiden Sie drei einfache Zustände:

SITUATION	WAS DAS BEDEUTET
Der Connector ist in Platform Administration sichtbar	er existiert technisch
Der Connector ist in Project Integrations sichtbar	das Projekt kann ihn potenziell nutzen
Der Connector erscheint in Actions & approvals als gesunde und autorisierte Option	die Aktion kann tatsächlich vorgeschlagen oder ausgeführt werden

Warum ein sichtbarer Connector blockiert bleiben kann

Ein Connector kann sichtbar, aber nicht nutzbar sein, wenn:

- sein **Health** eine Überprüfung erfordert;
- das Projekt-Binding nicht geöffnet, gesund oder konfiguriert ist;
- die **Policy** des Projekts die Nutzung blockiert;
- der Benutzer nicht die richtige **Permission** hat;
- das Projekt-Binding noch nicht geöffnet wurde;
- das erwartete Artefaktziel nicht konfiguriert ist.

Einfache Lesung

WENN SIE BEOBACHTEN...	ÜBERPRÜFEN SIE ZUERST...
Der Connector existiert auf Plattformebene, erscheint aber nicht im Projekt	Project Integrations

WENN SIE BEOBACHTEN...	ÜBERPRÜFEN SIE ZUERST...
Er erscheint im Projekt, aber keine Aktion wird ausgelöst	Governance Policies und Rollenberechtigungen
Die Aktion ist sichtbar, aber keine gesunde Option erscheint	Health des Connectors, Projekt-Binding und kompatible Ausführungsoption
Der Import wird vorgeschlagen, liefert aber nichts	Ingestionsanbieter, tatsächlich zugängliche Quelle und Datenfrische
Die SharePoint-Veröffentlichung ist noch nicht abgeschlossen	Artefaktziel, Politik, Genehmigung und SharePoint publish

Empfohlener Workflow für Ihr Team

1. Identifizieren Sie die wirklich nützlichen Tools für das Projekt;
2. Bereiten Sie die Connectoren in **Platform Administration** vor;
3. Öffnen Sie nur die Connectoren, die bereit sind, im Projekt;
4. Richten Sie die **Governance Policies** nach Rollen ein;
5. Testen Sie einen ersten Import oder eine erste Aktion und unterscheiden Sie Readiness, Probe und reale Vendor-Ausführung;
6. Prüfen Sie die endgültige Spur im **Journal IA**.

Zu behalten

- ProPM Agent unterscheidet klar zwischen **Import**, **Veröffentlichung** und **externer Aktion**;
- ein gleicher Name, wie **SharePoint** oder **Jira**, kann in mehreren Rollen erscheinen;
- die richtige Lesung eines Connectors beruht immer auf drei Fragen: **ist er definiert? ist er im Projekt geöffnet? ist er durch Governance autorisiert?**

Weiter

- [Governance, Entscheidungen und Aktionen](#)
- [Projekte und Arbeitsbereich](#)
- [Portfolio und technische Verwaltung](#)
- [Berichte, Journal IA und Nachverfolgbarkeit](#)

Portfolio

[Startseite](#) · Portfolio

Portfolio-Review-Workflow

Vergleichen Sie Projekte erst nach Prüfung von Umfang, Signalprofil, Schwelle und Nachweisen.

1

Projektauswahl

Wählen Sie Portfolio, Umfang und Projekte aus, bevor Sie Kennzahlen lesen.

2

Signalprofil

Wählen Sie relevante Signale: Risiko, Zeitplan, Nachweise und Blocker.

3

Kohorten

Gruppieren Sie vergleichbare Projekte, damit Kontexte nicht vermischt werden.

4

Ausreißer-Schwelle

Setzen Sie die Sensitivität, bevor Abweichungen priorisiert werden.

5

Ausreißer und Nachweise

Prüfen Sie starke Abweichungen immer mit den zugehörigen Nachweisen.

6

Folgeentscheidung

Öffnen Sie Details, erstellen Sie eine Review-Aktion oder ein PM-Dokument.

Ein Ausreißer ist eine Review-Priorität, keine automatische Schlussfolgerung

Die Entscheidung hängt von Nachweisen, Projektkontext und menschlicher Validierung ab.

ProPM Agent
KI-Liefercockpit

AKTUELLES PROJEKT
Azure Bay Hotel & Convention Center
Arbeitsbereich öffnen

Dashboard
Projekte
Arbeitsbereich
Wissensbasis
Agenten
Berichte & Artefakte
KI-Protokoll
Portfolio-Leitstand
Plattformadministration

Benutzer
mock.user@contoso.C...

Azure Bay Hotel & Convention Cent

Drücken Sie Strg+K / ⌘K für Befehle

Ozean

Deutsch

Hilfe

Status

Portfolio-Steuerzentrale

Vergleichen Sie ausgewählte Projekte mit konfigurierbaren Signalen, narrativen Erklärungen und Drilldown-Evidenz statt mit einer starren Rot-Gelb-Grün-Scorecard.

Projekte verwalten

Vergleich aktualisieren

HILFE

Portfolio-Übersicht

Der Portfolio-Vergleich hilft beim Gegenüberstellen mehrerer Projekte anhand eines konfigurierbaren Signalmodells.

Portfolio-Übersicht

Gespeicherte Kohorten

Projektauswahl

Signalprofil

Mindestschweregrad

Gesamt-Schwelle für Ausreißer

Vergleichsergebnisse

Vergleichsbereitschaft

Wie Portfolio zu interpretieren ist

Portfolio ist eine querschnittliche Vergleichsfläche fuer PMO-artige Reviews. Leere oder ruhige Ergebnisse koennen eine restriktive Auswahl, begrenzte Evidenz oder tatsaechlich stabile Projekte bedeuten. Lesen Sie die Ansicht daher als vergleichende Entscheidungshilfe und nicht als universelles Gesundheitsurteil.

Use this page for cross-project comparison and PMO-style triage. Use a project workspace when you need one project's documents, approvals, or execution context.

Kohorten

Speichern Sie wiederverwendbare Projektgruppen mit einem Vergleichsprofil.

Gespeicherte Kohorte

Ad-hoc-Vergleich

Kohortenname

Kohorte Lieferreview

Comparison ready

12 von 12 ausgewählt • 7 signals selected • Mindestschweregrad: Alle Schweregrade anzeigen

PROJECTS COMPARED

12

Accessible projects in the current comparison

OUTLIERS

4

Projects exceeding the active signal profile

SIGNALS ENABLED

7

Comparative indicators currently applied

EVIDENCE GAPS

46

Signal / project combinations reported as unavailable

Ziel

Die Seite **Portfolio** ist eine projektübergreifende PMO-Prüffläche. Sie vergleicht mehrere Projekte mit demselben Signalmodell, bevor eine detaillierte Projektansicht geöffnet wird.

Nutzen Sie sie für die Frage: **welche Projekte brauchen jetzt vorrangige Aufmerksamkeit?**

Verwenden Sie sie vor allem, um:

- zu priorisieren, welches Projekt zuerst Aufmerksamkeit braucht;
- konsistente Signale über mehrere Projekte hinweg zu vergleichen;
- zu entscheiden, welches Projekt danach einen genaueren Drill-down verdient.

Behandeln Sie die Seite nicht als reine Sponsor-Zusammenfassung und nicht als Ersatz für den detaillierten **Arbeitsbereich** eines Projekts.

Wofür Portfolio gedacht ist

Die Seite vergleicht mehrere Projekte mit **konfigurierbaren Signalen**, nicht mit einer festen Rot-/Orange-/Grün-Tabelle.

Sie ermöglicht:

- mehrere Projekte auszuwählen;

- die zu vergleichenden Signale auszuwählen;
- für jedes Signal **Gewicht** und **Schwelle** zu setzen;
- die **Mindestschwere** zu filtern;
- eine wiederverwendbare **Kohorte** zu speichern;
- **Ausreißer** oder auffällige Werte zu erkennen;
- ein Projektdetail zu öffnen, um zu verstehen, warum es heraussticht.

Was der Benutzer sieht

BEREICH	WAS DORT GETAN WIRD
Projektauswahl	auswählen, welche Projekte in den Vergleich eingehen
Signalprofil	Signale, Gewichte, Schwellen und Mindestschwere wählen
Kohorten	eine wiederverwendbare Vergleichskonfiguration speichern oder laden
Vergleichsergebnisse	Zusammenfassung, Ausreißer und Unterschiede zwischen Projekten lesen
Projekt-Drill-down	Nachweise, aktuelle Aktivität und Signaldetails für ein Projekt öffnen

Schlüsselbegriffe

BEGRIFF	EINFACHE ERKLÄRUNG
Projekt	ein Projekt, das in den Vergleich einbezogen wird
Signal	ein vergleichender Indikator, zum Beispiel Blockaden, Aktualität oder Terminspannung
Gewicht	die Bedeutung eines Signals im Gesamtscore
Schwelle	das Niveau, ab dem ein Signal auffällig wird
Mindestschwere	ein Filter, der schwache Signale ausblendet
Kohorte	eine Projektgruppe mit gespeichertem Vergleichsprofil
Ausreißer	ein Projekt, das nach der aktiven Konfiguration stärker heraussticht als andere
Narrativer Vergleich	eine textliche Zusammenfassung des laufenden Vergleichs

BEGRIFF	EINFACHE ERKLÄRUNG
Projekt-Drill-down	projektweises Detail mit Nachweisen und Aktivität

Geführtes Beispiel

Ein PMO möchte drei Projekte vor einer wöchentlichen Review vergleichen.

1. Wählen Sie in **Projects** die Projekte aus, die zur gleichen Steuerungsdiskussion gehören.
2. Aktivieren Sie in **Signal profile** die relevanten Signale, zum Beispiel `blocker_density`, `freshness_issues`, `failed_runs` und `schedule_pressure`.
3. Setzen Sie Gewichte, um auszudrücken, was in dieser Review am wichtigsten ist.
4. Setzen Sie Schwellen, um zu entscheiden, ab wann ein Signal Aufmerksamkeit verdient.
5. Wählen Sie die Mindestschwelle, um bei Bedarf schwaches Rauschen auszublenden.
6. Setzen Sie den **Overall outlier threshold**, um die Selektivität des Vergleichs zu steuern.
7. Speichern Sie die Konfiguration als **Kohorte**, wenn sie wiederverwendet werden soll.
8. Klicken Sie auf **Refresh comparison**, um die Ansicht neu zu berechnen.
9. Lesen Sie die **Narrative comparison** und prüfen Sie dann die **Outliers**.
0. Öffnen Sie **Project drill-down**, um Nachweise, aktuelle Aktivität und Links zu Workspace, Knowledge, Reports oder AI Log zu prüfen.

Kohorten?

Speichern Sie wiederverwendbare Projektgruppen mit einem Vergleichsprofil.

Gespeicherte Kohorte?

Ad-hoc-Vergleich

Kohortenname?

Kohorte Lieferreview

Beschreibung?

Projekte, die derzeit gemeinsam im Portfolio hinsichtlich der Lieferleistung geprüft werden.

Kohorte speichern

Kohorte löschen

Standard-Signalprofil

Die Seite startet nicht mit einem leeren Blatt. Die Standardwerte sind ein sicherer Startpunkt, kein verpflichtendes Modell.

SIGNAL	STANDARDGEWICHT	STANDARDSCHWELLE
activity_change	1.0	45
blocker_density	1.2	35
freshness_issues	1.0	35
contradiction_count	1.1	35
failed_runs	1.3	40
schedule_pressure	1.2	40
cost_pressure	1.2	40
overall_outlier_score	-	55

Nützliche Ergänzungen:

- die **Mindestschwere** startet ohne restriktiven Filter;
- **Reset defaults** stellt diese Startwerte wieder her;
- gespeicherte **Kohorten** bewahren wiederverwendbare Profile;
- manche Umgebungen können zusätzlich eine vorkonfigurierte Kohorte anzeigen, deren Inhalt von den verfügbaren Einstellungen abhängt.

Portfolio-Signale

SIGNAL	WELCHE FRAGE BEANTWORTET ES?	WIE WIRD ES INTERPRETIERT?
activity_change	Ist die aktuelle Aktivität stark anders als im vorherigen Zeitraum?	hoch = ungewöhnliche Veränderung, die erklärt werden muss
blocker_density	Zeigt das Projekt viele Blockaden oder Eskalationen?	hoch = häufige oder konzentrierte Blockaden
freshness_issues	Sind Nachweise und Quellen zu alt oder nicht verfügbar?	hoch = die Projektansicht wird weniger zuverlässig
contradiction_count	Widersprechen sich Quellen?	hoch = Klärung oder Entscheidung erforderlich
failed_runs	Scheitern Automatisierungen oder Runs häufig?	hoch = technische oder operative Reibung
schedule_pressure	Zeigt der Terminplan Spannungen?	hoch = Termindruck oder Kalenderdrift
cost_pressure	Zeigen Budget oder Verbrauch Spannungen?	hoch = Budget- oder Kostenrisiko

Einen Ausreißer lesen

Ein **Ausreißer** ist kein magischer Score und kein endgültiges Urteil.

Ein Projekt ist ein Ausreißer, wenn:

- ein oder mehrere Signale hoch sind;
- diese Signale ein relevantes Gewicht haben;
- die aktiven Schwellen überschritten werden;
- der kombinierte Score über der globalen Ausreißer-Schwelle liegt.

Korrekte Lesart:

- **Ausreißer** bedeutet, dass das Projekt nach den aktuellen Regeln stärker auffällt als andere;
- **kein Ausreißer** bedeutet, dass das Projekt im Normalbereich der aktuellen Gruppe bleibt.

Warum ein Signal nicht verfügbar sein kann

Ein Signal kann **nicht verfügbar** sein, wenn der erforderliche Nachweis fehlt.

Beispiele:

- fehlen Planungsquellen, kann `schedule_pressure` nicht verfügbar bleiben;
- fehlen Budgetquellen, kann `cost_pressure` nicht verfügbar bleiben.

Ein nicht verfügbares Signal bedeutet nicht Null Risiko. Es bedeutet, dass das Portfolio nicht genügend zuverlässige Nachweise hat, um diesen Indikator zu berechnen.

Wenn Portfolio leer oder ruhig wirkt

Mehrere Lesarten können normal sein:

- kein zugängliches Projekt wurde geladen;
- kein Projekt oder kein Signal ist ausgewählt;
- der Vergleich lieferte keine verwendbaren Projektzusammenfassungen;
- manche Signale sind mangels Nachweisen nicht verfügbar;
- kein Projekt überschreitet die aktive globale Ausreißer-Schwelle.

Ein ruhiges Ergebnis kann daher an enger Auswahl, begrenzten Nachweisen oder wirklich stabilen Projekten liegen.

Wie der Vergleich berechnet wird

Erwartetes Verhalten:

1. die Seite lädt zugängliche Projekte;
2. sie wählt eine erste verwendbare Menge vor, wenn noch kein Projekt gewählt wurde;
3. sobald die Projekt- und Signalkonfiguration gültig ist, wird der Vergleich bei einem Service angefordert;
4. **Refresh comparison** löst eine asynchrone Neuberechnung aus und aktualisiert den sichtbaren **Snapshot**;
5. der Snapshot-Zeitstempel zeigt, wann diese Portfolioansicht neu berechnet wurde.

Gespeicherte **Kohorten** bewahren ein wiederverwendbares Vergleichsprofil, ersetzen aber nicht die Live-Vergleichsanfrage selbst.

Merkmale

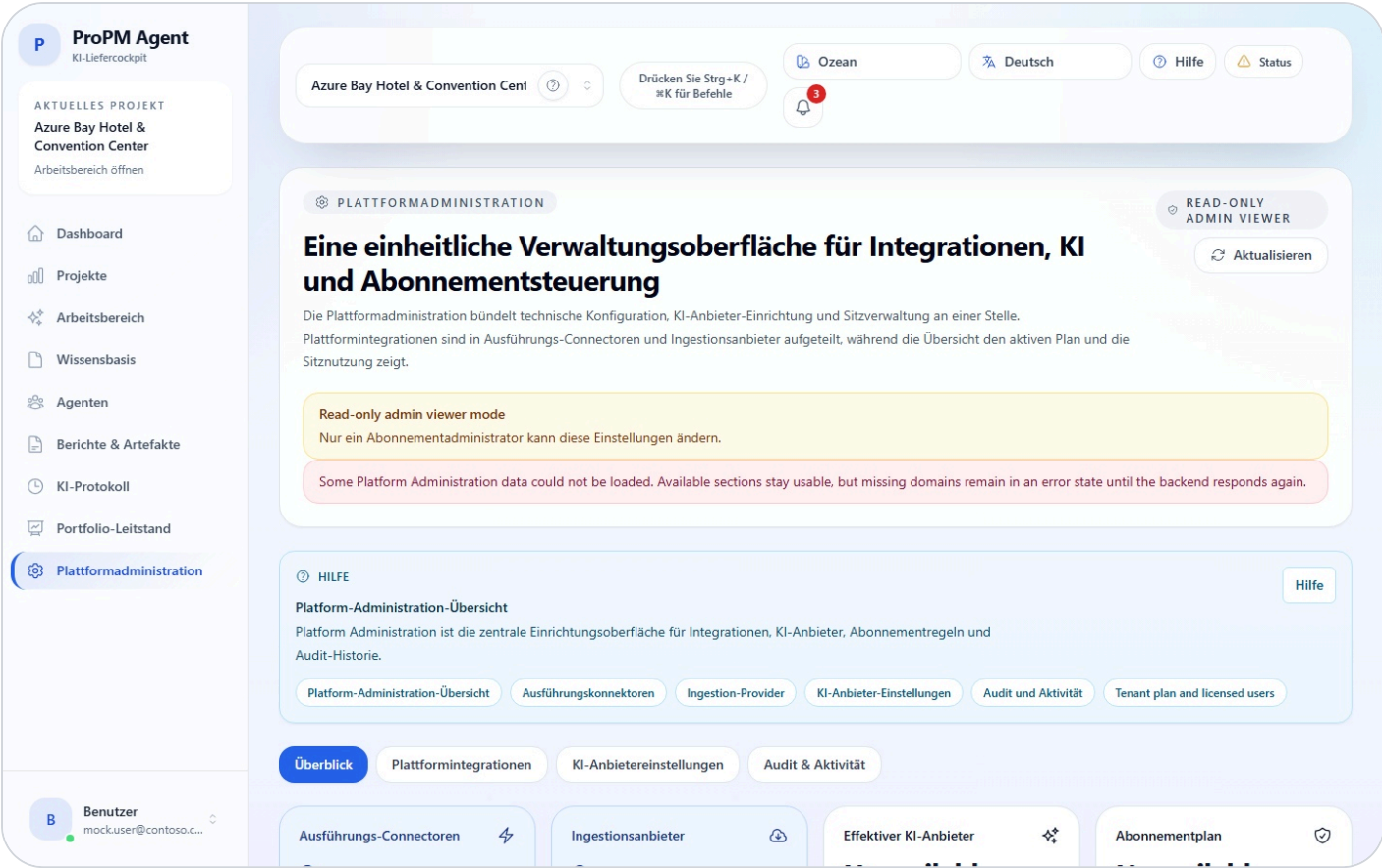
- beginnen Sie mit der Auswahl der richtigen Projekte;
- aktivieren Sie nur die für die Review nützlichen Signale;
- setzen Sie Gewichte, Schwellen und Schweregrade bewusst;
- nutzen Sie **Ausreißer** als Startpunkt der Untersuchung, nicht als endgültiges Urteil;
- öffnen Sie **Project drill-down**, um das Ergebnis zu verstehen.

Weiter

- [KI-Anbieter und Plattformintegrationen](#)
- [Tenant-Plan, lizenzierte Benutzer und App-Updates](#)
- [Berichte, KI-Log und Nachvollziehbarkeit](#)
- [Wartung, Support und FAQ](#)

KI-Anbieter und Plattformintegrationen

Startseite · KI-Anbieter und Plattformintegrationen



Ziel

Diese Seite behandelt die technische Vorbereitung von ProPM Agent auf Plattformebene:

- **Plattformintegrationen** für Konnektoren und Ingestion-Anbieter;
 - **KI-Anbieter-Einstellungen** für Laufzeit-Modellanbieter;
 - Readiness, Validierung, Tests, Health und Regeln für Projektbindungen.
- Nutzen Sie sie für die Frage: **ist die Plattform für die Organisation richtig vorbereitet, bevor Projekte sie verwenden?**

Sichtbare Administrationsbereiche

BEREICH	ROLLE
Overview	Zusammenfassung des allgemeinen Vorbereitungsstands
Platform integrations	technische Definitionen von Konnektoren und Ingestion-Anbietern

BEREICH	ROLLE
AI provider settings	Konfiguration, Validierung, Test und Aktivierung des KI-Anbieters
Tenant plan and licensed users	Marketplace-Plan, bestellte Sitze, Zusatzlizenzen und lizenzierte Benutzer
Audit / activity	Verlauf administrativer Aktionen

Für Marketplace-Plan, Lizenzen und Rollout von Anwendungsimages verwenden Sie [Tenant-Plan](#), [lizenzierte Benutzer](#) und [App-Updates](#).

Plattformintegrationen vs Projektintegrationen

Eine zentrale Produktregel lautet:

- die **Plattformebene** entscheidet, was technisch existiert;
- die **Projektebene** entscheidet, was in einem konkreten Projekt tatsächlich verwendet wird;
- die **Governance** entscheidet, wer mit dem Tool handeln darf.

VERANTWORTUNG	IN PLATTFORMADMINISTRATION GEPFLEGT	IN PROJEKTINTEGRATIONEN SICHTBAR
Technisches Setup	Tenant-URLs, Authentifizierungsstrategie, API-Schlüssel, Secret-Referenzen, Scopes und Quell- oder Zieldefinitionen	Readiness, Health und Blockierungsgründe schreibgeschützt
Operative Bindung	Enterprise-Konnektor/-Anbieter aktivieren oder deaktivieren und technische Health validieren	Bind to project , Validate binding und Disable für Projektverfügbarkeit
Benutzerführung	Admin-Audit, Validierungshistorie und tenantbezogene Konfiguration	Kontextlinks wie Open Platform Administration und Open Knowledge imports

Für Details je Konnektorfamilie siehe [Konnektoren und Integrationen](#).

Validierungs- und Sicherheitsregeln

Plattformvalidierungen wenden anbieterspezifische Anforderungen an:

- Pflichtfelder;
- kompatible Authentifizierungsstrategie;
- HTTPS-URLs, wenn erforderlich;

- gültiger SFTP-Port;
- explizite Quelle oder explizites Ziel;
- Konnektivitätsprobe nur, wenn sie durch Administrator oder Plattformkonfiguration aktiviert ist.

Secrets, Schlüssel und sensible Referenzen müssen in der dafür vorgesehenen Plattformkonfiguration bleiben. Legen Sie sie nicht in Notizen, Aktionspayloads oder Beschreibungen ab, die für Projektbenutzer sichtbar sind.

Vorbereitung und Blockierungsursachen

Eine Integration kann blockiert sein durch:

- **policy**;
- **permission**;
- zu prüfende **health**;
- fehlende Plattformdefinition;
- unvollständige anbieterspezifische Konfiguration oder Validierung;
- nicht geöffnete Projektbindung.

Empfohlener Prüfpfad:

1. lesen Sie die projektseitige Blockierung erneut;
2. öffnen Sie **Platform Administration**;
3. prüfen Sie die technische Definition des Konnektors oder Anbieters;
4. kehren Sie zum Projekt zurück, um Bindung und autorisierte Nutzung zu bestätigen.

KI-Anbieterfamilien

Zu den im Produkt sichtbaren Anbieterfamilien gehören unter anderem:

- **OpenRouter**;
- **OpenAI-compatible**;
- **OpenAI**;
- **Azure OpenAI**.

ANBIETER	WANN WÄHLEN?	WAS NORMALERWEISE AUSGEFÜLLT WIRD
OpenRouter	wenn mehrere Modellfamilien über eine Verbindung verglichen werden sollen	Base URL, Schlüssel, Standardmodell

ANBIETER	WANN WÄHLEN?	WAS NORMALERWEISE AUSGEFÜLLT WIRD
OpenAI-compatible	wenn die Organisation ein Gateway oder kompatibles Endpoint nutzt	exaktes Endpoint, Auth, Schlüssel oder Secret, erwartetes Modell
OpenAI	wenn die Organisation OpenAI direkt nutzt	URL, Schlüssel oder Secret, Standardmodell
Azure OpenAI	wenn die Organisation Azure-zentriert ist und Azure-OpenAI-Deployments wählen möchte	Endpoint, API-Version, Auth-Modus, Name des LLM-Deployments

Readiness des KI-Anbieters

STATUS	BEDEUTUNG
Configuration	Felder sind gespeichert
Validation	die Konfiguration hat die erwarteten Prüfungen bestanden
Test	echte Konnektivität wurde geprüft
Activate	der Anbieter ist in der Admin-Konfiguration aktiviert
Operational	der Anbieter kann als nutzbar gelten

Einfacher Vorbereitungsfluss:

1. öffnen Sie **AI provider settings**;
2. wählen Sie den gewünschten Anbieter;
3. füllen Sie die angeforderten Felder aus;
4. klicken Sie auf **Save**;
5. klicken Sie auf **Validate**;
6. klicken Sie auf **Test**;
7. klicken Sie auf **Activate**;
8. prüfen Sie das Ergebnis im **AI Log**.

Besonderheiten von Azure OpenAI

Bei **Azure OpenAI** müssen häufig ergänzt werden:

- der **Endpoint**;
- die **API version**;

- der **authentication mode**;
- der **LLM deployment name**;
- optional der **Embeddings deployment name**.

Details zur Auswahl eines KI-Anbieters während der Marketplace-Bereitstellung finden Sie unter [Azure Marketplace Deployment](#).

Effektiver Anbieter vs im Deployment gewählter Anbieter

Unterscheiden Sie zwei Begriffe:

- **Deployment-selected AI Provider**: Anbieter, der in der anfänglichen Umgebungskonfiguration gewählt wurde;
- **Effective AI Provider**: Anbieter, der zur Laufzeit für einen konkreten Run tatsächlich verwendet wird.

Der effektive Wert ist die zuverlässigste Referenz bei der Untersuchung eines konkreten Runs. Er erscheint im **AI Log** und kann vom im Deployment gewählten Wert abweichen.

Merkmale

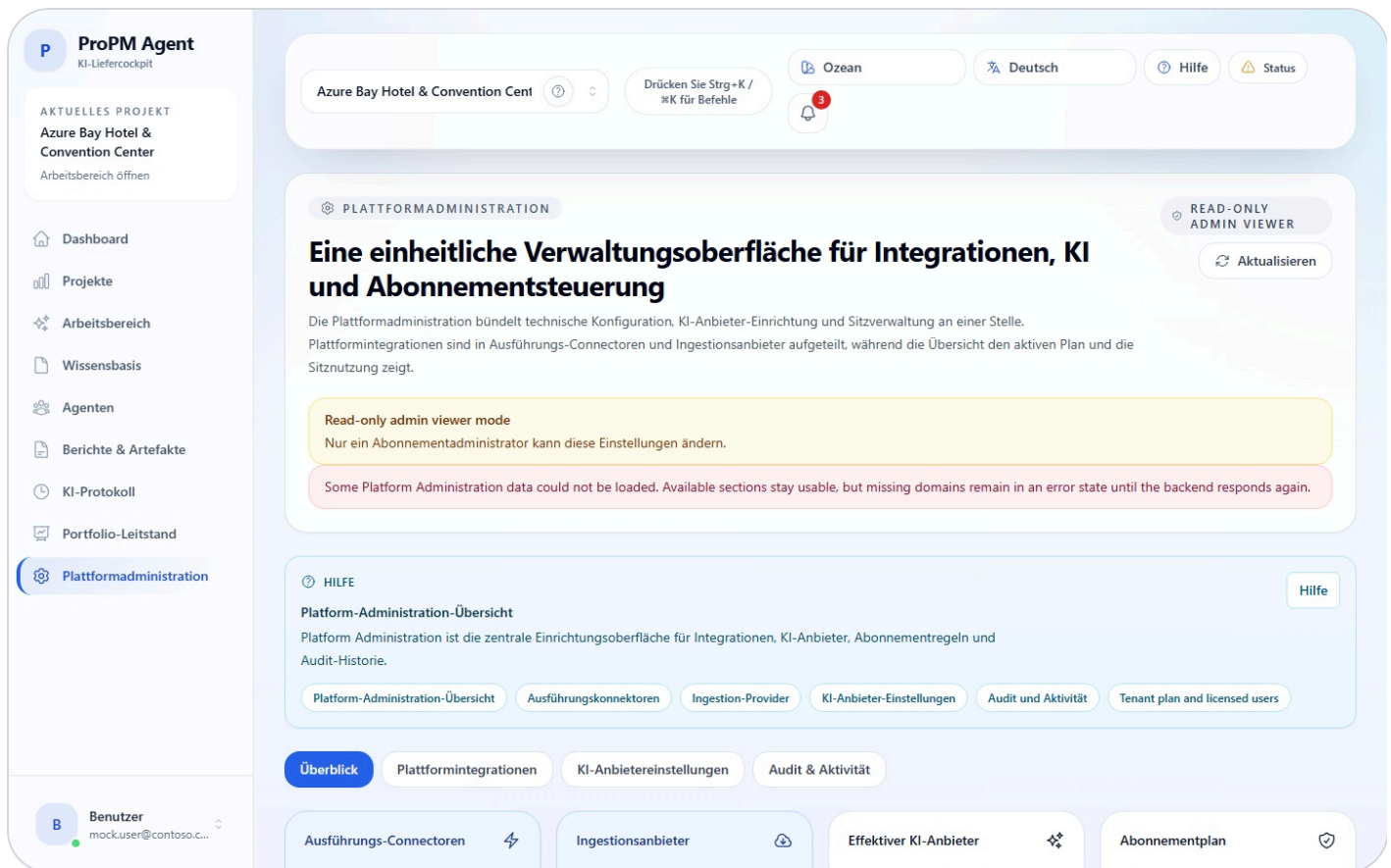
- die Plattformebene bereitet Konnektoren und Anbieter vor;
- die Projektebene öffnet deren reale Nutzung;
- Governance entscheidet, wer handeln darf;
- ein KI-Anbieter ist erst bereit, wenn er registriert, validiert, getestet und aktiviert ist;
- **AI Log** bleibt die Referenz zur Bestätigung des tatsächlich verwendeten Anbieters.

Weiter

- [Portfolio](#)
- [Tenant-Plan, lizenzierte Benutzer und App-Updates](#)
- [Konnektoren und Integrationen](#)
- [Berichte, KI-Log und Nachvollziehbarkeit](#)

Tenant-Plan, lizenzierte Benutzer und App-Updates

[Startseite](#) · Tenant-Plan, lizenzierte Benutzer und App-Updates



Ziel

Diese Seite erklärt den Benutzerablauf für **Platform Administration > Overview > Tenant plan and licensed users** und den empfohlenen Ablauf, wenn ein Kunde einen Azure-Marketplace-Plan ändern oder ein größeres Update ohne Verlust vorhandener Daten durchführen möchte.

Sie erklärt:

- welcher Marketplace-Plan aktuell für den Tenant erkannt wird;
- wie viele Lizenzen bestellt, enthalten, zusätzlich, genutzt und verbleibend sind;
- warum Azure Marketplace die offizielle Quelle für Pläne, Preise und Abrechnung bleibt;
- wie Zusatzlizenzen über Azure Marketplace mit der Abrechnungsdimension **seats** verwaltet werden;
- wie Sie eine neue ProPM-Bereitstellung aus Azure Marketplace im Modus **Attach existing ProPM data resources** erstellen;

- wie sich ein in-place App-Update von einer Planänderung oder einem größeren Update unterscheidet.

Die wichtigste Botschaft ist einfach: Um den Plan zu ändern oder ein größeres Update ohne Datenverlust durchzuführen, erstellen Sie eine **neue ProPM-Bereitstellung aus Azure Marketplace**, wählen **Attach existing ProPM data resources** und hängen die vorhandenen Datenressourcen der vorherigen Bereitstellung an. Dies ist keine manuelle Datenbankmigration.

Wo Sie die Seite finden

1. Öffnen Sie **Platform Administration**.
2. Bleiben Sie auf **Overview**.
3. Öffnen Sie **Tenant plan and licensed users**.

In ProPM zeigt dieser Bereich den aktuell erkannten Plan an und ermöglicht das Aktualisieren der Marketplace-Informationen. Er ersetzt Azure Marketplace nicht für Planauswahl, Preisprüfung, Abrechnungsänderungen oder den Abschluss einer kommerziellen Transaktion.

Marketplace-Pläne, Preise und Abrechnung

Azure Marketplace ist die offizielle Quelle für:

- die Liste der verfügbaren ProPM-Pläne;
- den Preis jedes Plans;
- die Planabrechnung;
- kommerzielle Planänderungen;
- Zusatzlizenzen, die mit der Dimension **seats** abgerechnet werden.

ProPM zeigt den aktuellen Plan an, damit Administratoren den Tenant-Status verstehen können. Planänderungen werden aber nicht mehr direkt in der ProPM-Administration durchgeführt. Ändern Sie den ARM-Plan der Managed Application nicht manuell. Zur Orientierung sind die bekannten ProPM-Marketplace-Pläne:

PLAN-ID	ANZEIGENAME	ENTHALTENE SITZE
free	Free	4
propm-20	ProPM-20	20

PLAN-ID	ANZEIGENAME	ENTHALTENE SITZE
propm-50	ProPM-50	50
propm-100	ProPM-100	100
propm-300	ProPM-300	300
propm-500	ProPM-500	500
propm-1000	ProPM-1000	1000

Prüfen Sie Plan, Preis und Abrechnungsbedingungen immer in Azure Marketplace, bevor Sie eine neue Bereitstellung starten.

Verwenden Sie für jede neue Bereitstellung oder jedes Upgrade nur die ProPM-Pläne, die aktuell in Azure Marketplace verfügbar sind.

Marketplace-Pläne steuern Lizenzkapazität. Sie schalten keine Konnektoren, KI-Anbieter oder Produktfunktionen frei oder aus.

Plan- und Lizenzfelder lesen

FELD	BEDEUTUNG
Current plan	Marketplace-Plan, der aktuell für den Tenant erkannt wird.
Ordered seats	Gesamtzahl der für den Tenant bestellten Lizenzen.
Included seats	Lizenzen, die im Marketplace-Basisplan enthalten sind.
Supplemental licenses	Zusätzliche Lizenzen, die über Marketplace-Abrechnung hinzugefügt wurden.
Used seats	Lizenzen, die aktuell von verbundenen oder lizenzierten Benutzern verbraucht werden.
Remaining seats	Noch verfügbare Lizenzen.

Wenn die angezeigten Informationen nicht zu einer kürzlich ausgeführten Azure-Marketplace-Aktion passen, nutzen Sie **Refresh Marketplace plan**, um ProPM mit den erkannten Marketplace-Informationen zu synchronisieren.

Zusatzlizenzen

Zusatzlizenzen werden über Azure Marketplace mit der Abrechnungsdimension **seats** verwaltet.

Nutzen Sie diesen Ablauf, wenn der Tenant mehr Kapazität benötigt, als der Basisplan enthält:

1. Prüfen Sie **Ordered seats**, **Included seats**, **Supplemental licenses**, **Used seats** und **Remaining seats** in ProPM.
2. Verwalten Sie zusätzliche Kapazität in Azure Marketplace oder über die ProPM-Aktion zur Abrechnung von Lizenzen in Azure, sofern sie in Ihrer Umgebung verfügbar ist.
3. Lassen Sie Azure Marketplace die Anfrage mit der Dimension **seats** akzeptieren und abrechnen.
4. Kehren Sie zu ProPM zurück.
5. Wählen Sie **Refresh Marketplace plan**, wenn die Zähler noch nicht aktuell sind.
6. Prüfen Sie **Ordered seats**, **Supplemental licenses** und **Remaining seats** nach der Synchronisierung.

Das Hinzufügen von Zusatzlizenzen ändert den Basisplan nicht. Das Entfernen oder Reduzieren von Zusatzlizenzen storniert oder erstattet die Abrechnung in Azure Marketplace nicht automatisch.

ProPM-Plan aktualisieren, ohne Daten zu verlieren

Um einen Azure-Marketplace-Plan zu ändern oder ein größeres Update durchzuführen, erstellen Sie eine neue ProPM-Bereitstellung und hängen diese an die vorhandenen Datenressourcen der vorherigen Bereitstellung an.

Die neue Bereitstellung erstellt eine neue Anwendungsschicht für den ausgewählten Plan, verwendet aber vorhandene Daten weiter. Benutzer, Dokumente, Konfigurationen, Agenten, Berichte und Geschäftsdaten sollten daher nach der Validierung weiterhin verfügbar sein.

Wann Sie diesen Ablauf nutzen

Nutzen Sie diesen Ablauf, wenn:

- Sie zu einem anderen ProPM-Plan in Azure Marketplace wechseln möchten;
- Sie ein größeres Update benötigen, das eine neue Marketplace-Bereitstellung erfordert;

- Sie die ProPM-Anwendungsschicht neu erstellen möchten, ohne vorhandene Daten zu verlieren;
- der ProPM-Support Sie bittet, im Modus zum Anhängen vorhandener Datenressourcen neu bereitzustellen.

Nutzen Sie diesen Ablauf nicht für ein einfaches in-place App-Image-Update.

Verwenden Sie dafür **Deployment & Updates** in ProPM, wenn diese Funktion verfügbar ist und die Release Notes keine neue Marketplace-Bereitstellung verlangen.

Bevor Sie beginnen

Bereiten Sie Folgendes vor:

- Azure-Zugriff auf die vorherige ProPM-Bereitstellung;
- die Berechtigung, eine neue ProPM Managed Application aus Azure Marketplace zu erstellen;
- den Zielplan für ProPM, ausgewählt in Azure Marketplace;
- die vollständige **Resource ID** der vorherigen ProPM Managed Application;
- ein Cutover-Zeitfenster, in dem Administratoren die neue Bereitstellung prüfen können;
- eine Prüfliste für Benutzer, Dokumente, Konfigurationen, Agenten, Berichte und Daten.

Beachten Sie vor jeder Aktion diese Vorsichtsmaßnahmen:

- löschen Sie die vorherige Managed Resource Group nicht, bevor die neue Bereitstellung validiert wurde;
- löschen Sie keine vorhandenen Datenressourcen, da sie von der neuen Bereitstellung wiederverwendet werden;
- ändern Sie den ARM-Plan der Managed Application nicht manuell;
- füllen Sie erweiterte Override-Optionen nur aus, wenn die vorherige Installation benutzerdefinierte Ressourcennamen verwendet hat oder ProPM-Support Sie dazu auffordert.

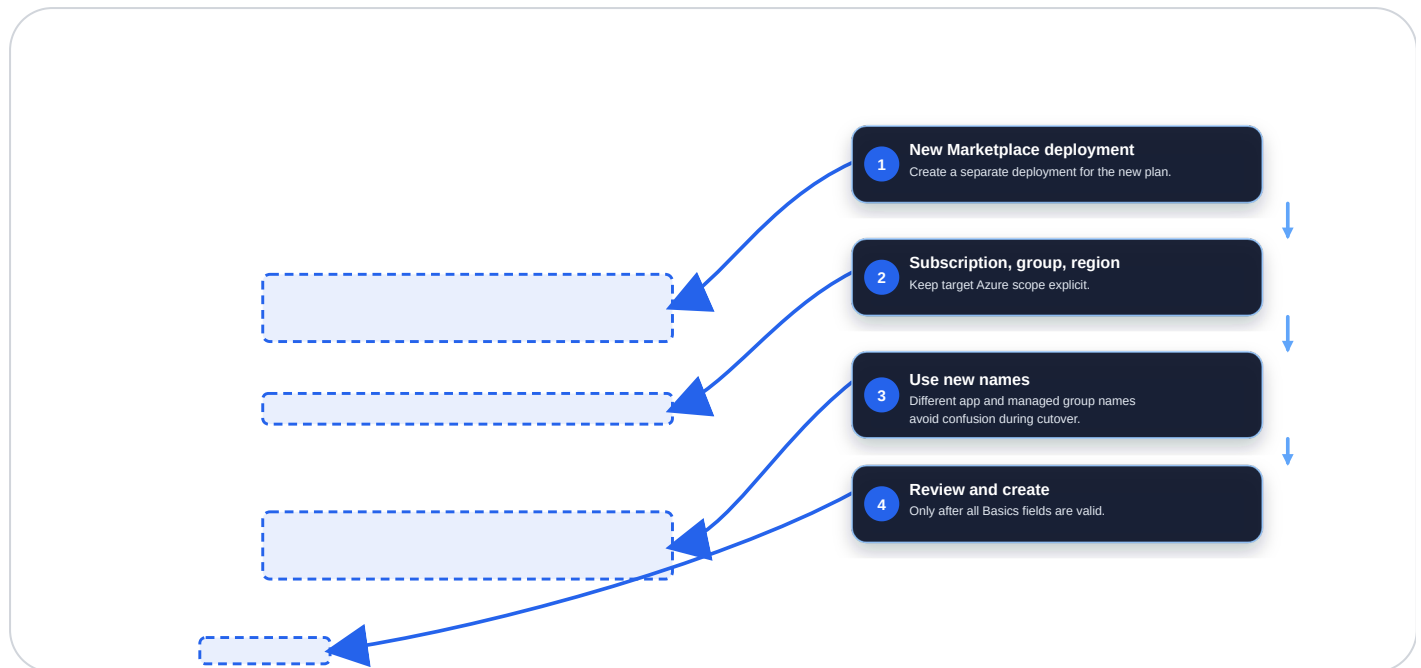
Schritt 1 - Neuen Plan in Azure Marketplace auswählen

Öffnen Sie Azure Marketplace und wählen Sie den gewünschten neuen ProPM-Plan. Planauswahl, Preise und Abrechnung werden in Azure Marketplace verwaltet. ProPM kann den aktuellen Plan anzeigen und erkannte Informationen aktualisieren, ist aber nicht die offizielle Quelle für die kommerzielle Transaktion.

Schritt 2 - Neue ProPM-Bereitstellung erstellen

Erstellen Sie in Azure Marketplace eine neue ProPM-Bereitstellung, anstatt die vorherige Bereitstellung direkt zu ändern.

Wählen Sie auf der Registerkarte **Basics** Abonnement, Ressourcengruppe, Region, Namen der neuen Managed Application und die neue Managed Resource Group.



Verwenden Sie einen anderen Namen für die neue Managed Application, damit vorherige und neue Umgebung während des Cutovers klar unterscheidbar sind.

Schritt 3 - Attach existing ProPM data resources auswählen

Wählen Sie auf der Registerkarte **Application Settings** im Feld **Installation mode** die Option **Attach existing ProPM data resources**. Dieser Modus erstellt eine neue Marketplace Managed Application und einen neuen Anwendungstier, verbindet diese aber mit den Datenressourcen der vorherigen ProPM-Bereitstellung.

Home > ProPM Agent

Create ProPM Agent ...

Environment Name * ⓘ

prod

Installation mode ⓘ

Attach existing ProPM data resources

Attach mode creates a new Marketplace Managed Application and application tier for the selected plan, but connects it to the resources used by an existing ProPM deployment. Enter the previous Managed Application resource ID so ProPM can read its recorded deployment outputs and discover the actual data resources, including when the previous deployment is also an attach deployment. Keep the previous deployment stopped or read-only during cutover to avoid two app tiers writing to the same data.

Previous ProPM Managed Application resource ID * ⓘ

Advanced overrides: leave the resource IDs below empty to auto-discover the ProPM resources from the previous deployment outputs. Fill a field only if the previous deployment outputs are unavailable or the data resources are externally managed.

Existing Storage account resource ID (optional override) ⓘ

Existing Azure AI Search service resource ID (optional override) ⓘ

Existing SQL server resource ID (optional override) ⓘ

Existing SQL database name (optional override) ⓘ

Existing Cosmos DB account resource ID (optional override) ⓘ

Existing Document Intelligence account resource ID (optional override) ⓘ

Existing Service Bus namespace resource ID (optional override) ⓘ

Previous

Next

Review + create

Felder für vorhandene Datenressourcen

FELD	PFLICHT	WAS EINTRAGEN	EMPFEHLUNG
Environment Name	Ja	Kurzer Umgebungsname, z. B. <code>prod</code> , <code>uat</code> oder <code>test</code> .	Stabilen, nicht geheimen Namen für den neuen Anwendungstier verwenden.
Installation mode	Ja	Attach existing ProPM data resources.	Nur für Planwechsel, größere Updates oder Wiederaufnahme mit vorhandenen Daten verwenden.
Previous ProPM Managed Application resource ID	Ja	Vollständige Azure Resource ID der vorherigen ProPM Managed Application.	Das Feld Id aus Properties der vorherigen Managed Application kopieren. Nicht nur Namen oder Managed Resource Group eintragen.

Tenant-Plan, lizenzierte Benutzer und App-Updates

7/15

FELD	PFLICHT	WAS EINTRAGEN	EMPFEHLUNG
Existing Storage account resource ID (optional override)	Nein	Resource ID des vorhandenen Storage Accounts.	Standardmäßig leer lassen. Nur ausfüllen, wenn automatische Erkennung nicht möglich ist oder Support es verlangt.
Existing Azure AI Search service resource ID (optional override)	Nein	Resource ID des vorhandenen Azure AI Search-Dienstes.	Leer lassen, sofern der Dienst aus der vorherigen Bereitstellung erkannt werden kann.
Existing SQL server resource ID (optional override)	Nein	Resource ID des vorhandenen SQL Servers.	Identifiziert den SQL Server, nicht den Datenbanknamen. Nur bei Sondertopologie verwenden.
Existing SQL database name (optional override)	Nein	Name der vorhandenen SQL-Datenbank.	Nur ausfüllen, wenn der Datenbankname nicht aus den vorherigen Outputs ermittelt werden kann.
Existing Cosmos DB account resource ID (optional override)	Nein	Resource ID des vorhandenen Cosmos DB Accounts.	Leer lassen, außer ein bestimmter vorhandener Account muss erzwungen werden.
Existing Document Intelligence account resource ID (optional override)	Nein	Resource ID des vorhandenen Document Intelligence Accounts.	Nur bei extern verwalteter oder benutzerdefinierter Ressource verwenden.
Existing Service Bus namespace resource ID (optional override)	Nein	Resource ID des vorhandenen Service Bus Namespace.	Standardmäßig leer lassen, damit der Namespace automatisch erkannt wird.

Lassen Sie erweiterte Override-Felder in den meisten Fällen leer. Füllen Sie diese Felder nur aus, wenn die vorherige Installation benutzerdefinierte Ressourcennamen genutzt hat, die Outputs nicht verfügbar sind oder ProPM-Support Sie dazu auffordert.

Schritt 4 - Cutover- und Plattformparameter prüfen

Die zweite Hälfte der Seite steuert Cutover-Sicherheit, Administrationszugriff, Wiederverwendung der KI-Konfiguration, CORS, Monitoring, SQL-Passwort und Netzwerk.

Microsoft Azure

Search resources, services, and docs (G+)

Home > ProPM Agent

Create ProPM Agent ...

Existing Event Grid topic resource ID (optional override) ⓘ

Block previous deployment during cutover ⓘ

☒

Platform Administration Entra Group Object IDs * ⓘ

Platform Administration Bootstrap Users (optional) ⓘ

Allow Azure RBAC admin recovery ⓘ

☒

Reuse previous AI provider configuration ⓘ

☒

AI provider fields are hidden for this update. ProPM will reuse the previous deployment's AI provider metadata and the existing Platform Administration configuration stored with your attached data. You can change AI settings after deployment from Platform Administration.

CORS Allowed Origins ⓘ

Enable alerting (Azure Monitor) ⓘ

☒

Enable debug logging ⓘ

☐

One secure SQL input is still required for attach updates: enter the existing ProPM SQL admin password so the new application tier can connect to the reused database. This password is not exposed by ARM outputs and cannot be read from the previous Managed Application because the managed resource group is protected by Azure deny assignments.

Password * ⓘ

Confirm password * ⓘ

VNet CIDR * ⓘ

10.0.0.0/16

Previous

Next

Review + create

Felder für Cutover und Plattform

FELD	PFLICHT	WAS EINTRAGEN	EMPFEHLUNG
Existing Event Grid topic resource ID (optional override)	Nein	Resource ID des vorhandenen Event Grid Topics.	Leer lassen, außer automatische Erkennung findet das Topic nicht oder Support verlangt den Wert.
Block previous deployment during cutover	Nein, empfohlen	Aktivieren, wenn die vorherige Umgebung während der Validierung blockiert werden soll.	Verhindert, dass zwei Anwendungstiers gleichzeitig in dieselben Daten schreiben. Alternativ vorherige Umgebung stoppen oder auf read-only setzen.

FELD	PFLICHT	WAS EINTRAGEN	EMPFEHLUNG
Platform Administration Entra Group Object IDs	Ja	Object IDs der Entra-Gruppen für Plattformadministration.	Object IDs eintragen, nicht Anzeigenamen.
Platform Administration Bootstrap Users (optional)	Nein	Bootstrap- oder Recovery-Benutzer.	Nur für ersten Zugriff oder kontrollierte Wiederherstellung nutzen.
Allow Azure RBAC admin recovery	Nein	Checkbox für Wiederherstellung über Azure RBAC.	Aktiv lassen, wenn das Betriebsmodell dies erlaubt.
Reuse previous AI provider configuration	Empfohlen	Aktivieren, wenn die vorherige KI-Konfiguration übernommen werden soll.	KI-Felder werden dann ausgeblendet. Änderungen sind später in Platform Administration möglich.
CORS Allowed Origins	Szenarioabhängig	Zusätzliche erlaubte Web-Origins.	Leer lassen, wenn keine zusätzlichen Origins benötigt werden.
Enable alerting (Azure Monitor)	Nein	Azure Monitor Alerts aktivieren oder deaktivieren.	Für Produktion empfohlen.
Enable debug logging	Nein	Detailliertere Logs aktivieren.	Außerhalb kontrollierter Diagnose deaktiviert lassen.
Password	Ja	Vorhandenes ProPM SQL-Admin-Passwort.	Für Attach-Updates weiterhin erforderlich, damit der neue Anwendungstier die wiederverwendete Datenbank erreicht. Sicher behandeln.
Confirm password	Ja	Derselbe Wert wie Password .	Beide Werte müssen übereinstimmen.
VNet CIDR	Ja	Privater Netzwerkbereich, z. B. <code>10.0.0.0/16</code> .	Vor Erstellung mit dem Netzwerkteam validieren und Überschneidungen vermeiden.

Nachdem Sie die weiteren vom Assistenten geforderten Parameter eingegeben haben, wählen Sie **Review + create**, prüfen die Konfiguration und starten die Bereitstellung.

Schritt 5 - Neue Bereitstellung prüfen

Nach Abschluss der neuen Bereitstellung öffnen Sie die neue ProPM-Instanz und prüfen die wesentlichen Punkte, bevor Benutzer dauerhaft umgestellt werden.

Prüfen Sie mindestens:

- Benutzer und ihre Zugriffe;
- Dokumente und Wissensbereiche;
- Plattformkonfiguration;
- Agenten und ihre Einstellungen;
- Berichte;
- Projekte, Portfolios und Geschäftsdaten;
- erwartete Konnektoren und Integrationen;
- den KI-Anbieter und erforderliche Einstellungen;
- Plan- und Lizenzzähler nach Marketplace-Synchronisierung.

Wenn der in ProPM angezeigte Plan nach der Azure-Marketplace-Aktion noch nicht aktuell ist, nutzen Sie **Refresh Marketplace plan**. Diese Schaltfläche synchronisiert nur den erkannten Zustand; sie ändert keinen Plan und löst keinen Kauf aus.

Schritt 6 - Cutover abschließen

Leiten Sie die Benutzer nach vollständiger Validierung zur neuen ProPM-Bereitstellung. Behalten Sie die vorherige Bereitstellung bei Bedarf vorübergehend als Sicherheit. Löschen Sie die vorherige Managed Application erst, wenn Sie sicher sind, dass der Cutover abgeschlossen ist und das gewählte Löschverfahren keine wiederverwendeten Datenressourcen entfernt.

Löschen Sie vorhandene Datenressourcen niemals manuell, solange sie von der neuen Bereitstellung verwendet werden.

Best Practices und Vorsichtsmaßnahmen

Tun Sie Folgendes:

- wählen Sie den neuen Plan in Azure Marketplace;
- erstellen Sie eine neue ProPM-Bereitstellung;
- wählen Sie **Attach existing ProPM data resources**;
- tragen Sie die vollständige Resource ID der vorherigen ProPM Managed Application ein;
- blockieren Sie die vorherige Bereitstellung während des Cutovers oder setzen Sie sie auf Nur-Lesen, falls erforderlich;

- validieren Sie die neue Bereitstellung, bevor Sie etwas löschen;
- nutzen Sie **Refresh Marketplace plan** nach einer Marketplace-Aktion, um ProPM erneut zu synchronisieren.

Vermeiden Sie Folgendes:

- löschen Sie die vorherige Managed Resource Group nicht vor Validierung der neuen Bereitstellung;
- löschen Sie keine vorhandenen Datenkonten, Datenbanken oder Datendienste;
- ändern Sie den ARM-Plan der Managed Application nicht manuell;
- stellen Sie diesen Ablauf nicht als manuelle Datenbankmigration dar;
- füllen Sie erweiterte Overrides nicht ohne bekannten Bedarf aus.

FAQ

Kann ich den Plan direkt in ProPM ändern?

Nein. ProPM zeigt den aktuellen Plan an und kann Marketplace-Informationen aktualisieren. Planänderungen, Preise und Abrechnung werden aber in Azure Marketplace verwaltet.

Was macht Refresh Marketplace plan?

Refresh Marketplace plan synchronisiert ProPM mit Marketplace-Informationen, die nach einer Azure-seitigen Aktion erkannt wurden. Es ändert keinen Plan, kauft keine Lizenzen und entfernt keine Lizenzen.

Ist dies eine manuelle Datenbankmigration?

Nein. Die neue ProPM-Bereitstellung verbindet sich automatisch mit vorhandenen Datenressourcen, wenn Sie **Attach existing ProPM data resources** auswählen und die vorherige Managed Application angeben.

Welche Resource ID muss ich eintragen?

Tragen Sie die vollständige Resource ID der vorherigen **ProPM Managed Application** ein. Tragen Sie nicht nur den Anwendungsnamen, Ressourcengruppenamen oder die Managed Resource Group ein.

Wann sollte ich erweiterte Override-Optionen nutzen?

Nutzen Sie sie nur, wenn die vorherige Installation benutzerdefinierte Ressourcennamen hat oder ProPM-Support Sie dazu auffordert. Im Standardfall lassen Sie diese Felder leer.

Kann ich die vorherige Managed Resource Group nach der neuen Bereitstellung löschen?

Löschen Sie sie nicht, bevor die neue Bereitstellung validiert wurde. Löschen Sie keine vorhandenen Datenressourcen, wenn die neue Bereitstellung sie wiederverwendet.

Wenn Zweifel bestehen, behalten Sie die vorherige Bereitstellung vorübergehend und fragen Sie ProPM-Support nach dem richtigen Lösungsverfahren.

Wie werden Zusatzlizenzen verwaltet?

Zusatzlizenzen werden über Azure Marketplace mit der Abrechnungsdimension **seats** verwaltet. ProPM kann Zähler anzeigen und synchronisieren, aber Azure Marketplace bleibt die Abrechnungsreferenz.

Refresh Marketplace plan

Nutzen Sie **Refresh Marketplace plan**, um ProPM mit dem erkannten Marketplace-Zustand des Tenants zu synchronisieren.

Diese Aktion:

- aktualisiert Plan- und Lizenzinformationen nach einer Marketplace-Aktion;
- führt selbst kein Plan-Upgrade aus;
- kauft keine Zusatzlizenzen;
- entfernt oder storniert keine Lizenzen;
- ändert keine Azure-Bereitstellungsressourcen.

Lizenzierte verbundene Benutzer

Die Liste **Licensed connected users** zeigt Benutzer, die aktuell Lizenzen verbrauchen.

Das Entfernen eines lizenzierten Benutzers gibt Anwendungskapazität für spätere Nutzung frei, abhängig von den Lizenzregeln des Tenants. Es ändert den Marketplace-Plan nicht und storniert keine über Azure Marketplace abgerechnete Nutzung.

App-Updates ohne Marketplace-Neubereitstellung

Der Bereich **Deployment & Updates** aktualisiert eine bestehende Installation in place, wenn das Update mit der aktuellen Bereitstellung kompatibel ist.

Er führt nicht aus:

- das Azure-Marketplace-Angebot erneut starten;
- eine neue Ressourcengruppe erstellen;
- bereits vorhandene Azure-Ressourcen neu erstellen;
- ein Marketplace-Plan-Upgrade anwenden;

- ein größeres Update durchführen, das eine neue Marketplace-Bereitstellung erfordert.

Praktisch liest die Administration das Image-Inventar der vorhandenen **Azure Container Apps** über Azure Resource Manager, vergleicht aktuelle Images mit genehmigten Zielimages in ACR und erstellt neue Revisionen auf den vorhandenen Container Apps.

Verfügbare Update-Aktionen

AKTION	ZWECK
Check for updates	Aktuelle Images, Zielimages, Kandidaten für Mutable-Tag-Refresh und optionale Manifestversion prüfen.
Apply update	Neue Images auf ausgewählte Services anwenden, indem neue Container-Apps-Revisionen erstellt werden.
Rollback last update	Zu vorherigen Images zurückkehren, wenn die letzte Operation die erforderlichen Referenzen erfasst hat.
Container App image inventory	Verwaltete Ressourcengruppe, verfolgte Services, aktuelle Images, Zielimages und Revisionsstatus prüfen.

Grenzen des Umfangs

Der Rollout von Anwendungsimagen ist von Marketplace-Planadministration getrennt. Die Update-Schaltflächen decken nicht ab:

- Datenbankschema-Migrationen;
- Erstellung neuer Azure-Ressourcen;
- Architekturänderungen;
- Marketplace-Plan-Upgrades;
- Cutovers zu einer neuen Bereitstellung mit vorhandenen Datenressourcen.

Merkmale

- Azure Marketplace ist die offizielle Quelle für Pläne, Preise und Abrechnung.
- ProPM zeigt den aktuellen Plan und Lizenzzähler, ersetzt Azure Marketplace aber nicht für Planänderungen.
- Um den Plan zu ändern oder ein größeres Update ohne Datenverlust durchzuführen, erstellen Sie eine neue ProPM-Bereitstellung aus Azure Marketplace.

- Wählen Sie im Bereitstellungsassistenten **Attach existing ProPM data resources**.
- Tragen Sie die vollständige Resource ID der vorherigen ProPM Managed Application ein.
- Löschen Sie die vorherige Managed Resource Group oder Datenressourcen nicht vor vollständiger Validierung der neuen Bereitstellung.
- Nutzen Sie **Refresh Marketplace plan** nur zur Synchronisierung des erkannten Marketplace-Zustands.
- Nutzen Sie **Deployment & Updates** für in-place App-Image-Rollout, nicht für kommerzielle Planänderungen.

Weiter

- [Azure Marketplace Deployment](#)
- [KI-Anbieter und Plattformintegrationen](#)
- [Wartung, Support und FAQ](#)

Wartung, Support und FAQ

[Startseite](#) · Wartung, Support und FAQ

NovaBiz Kontakt

Für den NovaBiz Support:

- E-Mail: support@navabiz.pro
- Adresse: NovaBiz, 131 Continental Dr, Suite 305, Newark, DE 19713, United States

Nützliche Oberflächen für den Betrieb

Die folgenden Beobachtungspunkte sind in der Anwendung bestätigt:

- **Benachrichtigungen** in der oberen Leiste;
- **Gesundheitsindikator** in der oberen Leiste;
- **Signale** im Projektarbeitsbereich;
- **KI-Protokoll** für Runs und Aktivitäten;
- **Audit / Activity** in der Plattformverwaltung.

Schnelle Prüfungsprozedur

1. prüfen Sie, ob das richtige **Projekt** aktiv ist;
2. unterscheiden Sie **leere Ansicht**, **schreibgeschützt**, **Zugriff verweigert** oder **angezeigte Meldung**;
3. öffnen Sie das **KI-Protokoll**, wenn das Thema einen Agenten, ein Ergebnis oder ein Artefakt betrifft;
4. behalten Sie die **Trace ID** bei und, falls sichtbar, die [Context snapshot ID](#) oder die [Structured output ID](#);
5. prüfen Sie Rechte, Integrationen, Projekt-Bindings, Health und Sitzverfügbarkeit, falls Zugriff oder Ausführung blockiert sind.

Schnelle Referenzen nach Situation

ANGETROFFENE SITUATION	OBERFLÄCHE ERSTER EBENE	NÄCHSTER SCHRITT
Anmelde- oder Microsoft-Rückkehr abnormal	Start	prüfen Entra, Mandant, redirectUri und Sitzplätze
Kein Projekt sichtbar nach Anmeldung	Projekte / Projekt-Auswahl	Zugriffskontrolle oder Hinzufügen des Kontos zum Projekt
Agentenantwort, Artefakt oder zweifelhafte Veröffentlichung	KI-Protokoll → Runs	Activity , dann Berichte & Artefakte
Import oder inkonsistente Suche	Wissen und Importhistorie	Projektintegration , dann Plattformverwaltung
Externe Aktion sichtbar, aber blockiert	Aktionen & Genehmigungen	Projektintegration , dann Plattformverwaltung

Schnelle Prüflisten

Zugriff zu bestätigen

Prüfen Sie die URL, den Mandanten, das Gastkonto bei Guest-Nutzung, die tatsächlich konfigurierte [redirectUri](#) und die Verfügbarkeit eines Sitzplatzes, wenn der Anwendungszugriff eine Lizenz verbraucht.

Seite sichtbar, aber nicht bearbeitbar

Sie befinden sich wahrscheinlich im **schreibgeschützten** Modus. Prüfen Sie Ihre Rolle, bevor Sie auf eine Berechtigungsbeschränkung schließen.

Dokument sichtbar, aber nicht suchbar

Beginnen Sie damit, den Dokumentstatus ([Indexed](#) , [Ingesting](#) , [Failed](#)) zu prüfen, die Importhistorie, das Seiten-Refresh und die Such- [Trace ID](#) , falls ein Aufruf fehlgeschlagen ist.

Import aus einer ausgegrauten oder fehlenden Quelle

Die nützlichsten Prüfungen sind: nicht validierter Anbieter, fehlendes Projekt-Binding, unzureichende Berechtigung, restriktive Richtlinie, unvollständige Konfiguration oder ein noch zu bestätigender Gesundheitsstatus.

Aktion sichtbar, aber nicht ausführbar

Prüfen Sie den kompatiblen Connector, das Projekt-Binding, die erforderliche Genehmigung, die Benutzerrolle und die geltende Richtlinie.

Spracheingabe nicht verfügbar

Die Spracheingabe hängt vom Browser ab. Versuchen Sie einen anderen Browser, prüfen Sie die Mikrofonberechtigungen und nutzen Sie die Texteingabe, falls die Spracherkennung nicht unterstützt wird.

Daten, die an den Support weitergegeben werden

ELEMENT	WARUM ES NÜTZLICH IST
URL der Bereitstellung	Identifiziert die betroffene Umgebung
Betroffenes Projekt	Reproduziert den Kontext
Trace ID	Findet den Run oder das Ereignis exakt
Context snapshot ID / Structured output ID	Verknüpft einen Run, eine Ausgabe und ein Artefakt
Screenshot	Versteht den sichtbaren Zustand zum Zeitpunkt der Blockierung
Ungefährer Zeitpunkt	Verknüpft das Ereignis mit den Logs

FAQ — Zugriff und Sicherheit

Warum kann ich eine Administrationsseite sehen, aber nicht bearbeiten?

Weil das Produkt **schreibgeschützt** und **Zugriff verweigert** unterscheidet. Eine Seite kann zur Inspektion angezeigt werden, ohne die Bearbeitung zu erlauben.

Warum gelingt meine Microsoft-Anmeldung, aber der Zugriff ist noch nicht wie erwartet?

Prüfen Sie den Mandanten, die Kontoberechtigung, die Existenz eines zugänglichen Projekts und die Verfügbarkeit eines Sitzplatzes, wenn der Anwendungszugriff eine Lizenz erfordert.

Warum gelingt meine Anmeldung, aber kein Projekt erscheint?

Diese Situation bedeutet nicht unbedingt ein Authentifizierungsproblem. Prüfen Sie zuerst den **Projekt-Auswahl** und dann die Seite **Projekte**. Wenn die Liste leer bleibt, wurde das Konto wahrscheinlich noch nicht dem richtigen Projekt hinzugefügt oder verfügt nicht über das Erstellungsrecht.

Wann muss ich ein externes Konto als **guest** einladen?

Wenn das Konto zu einem anderen Mandanten gehört als der, der die Anwendung hostet. Das Konto muss dann im Zielmandanten eingeladen und anschließend auf die Anwendung oder über die erwartete Gruppe autorisiert werden.

Wie unterscheiden sich schnell Mandant, **redirect URI**, Entra-Client oder Sitzplatz?

Folgen Sie dieser Reihenfolge:

1. Wenn Microsoft **vor** dem Rückkehr in die Anwendung fehlschlägt, vermuten Sie zuerst Mandant, **clientId** oder **redirect URI** ;
2. Wenn die Anmeldung gelingt, die Anwendung jedoch blockiert bleibt, prüfen Sie anschließend die **Sitzplätze** und den Projektzugriff;

3. Wenn nur eine bestimmte Oberfläche gesperrt bleibt, liegt das Thema oft bei **Rolle** oder **Berechtigung** statt bei Authentifizierung.

FAQ — Verfügbarkeit, Laufzeit und Konnektivität

Wie lese ich das Gesundheitspanel, wenn einige Seiten noch laden?

Weil die Authentifizierung weiterhin gültig sein kann, während eine **API** oder ein Anbieter noch eine Verfügbarkeitsprüfung verlangt. Notieren Sie zuerst den im Gesundheitsindikator gezeigten Status und gehen Sie dann zu [Interface und Navigation](#) für die Einordnung des Panels und zu [Portfolio und technische Administration](#), wenn der Verdacht auf den Anbieter oder die Admin-Integration fällt.

Was tun, wenn die Anmeldung gelingt, ein Projekt sichtbar ist, aber die Runs nicht starten?

Prüfen Sie in dieser Reihenfolge: aktives Projekt, Gesundheitsindikator, vermeintlich betriebsbereiter KI-Anbieter, Anbieter-Readiness, dann **KI-Protokoll**, um zu sehen, ob ein Run zumindest erstellt wurde. Wenn der Anbieter weiterhin verdächtig ist, gehen Sie zu [Portfolio und technische Administration](#).

FAQ — Projekt, Arbeitsbereich und Agenten

Wann sollte ich den Arbeitsbereich statt Agenten verwenden?

Verwenden Sie **Arbeitsbereich**, um das Projekt einzustellen und zu steuern; verwenden Sie **Agenten**, um mit einem Agenten zu chatten und eine strukturierte Ausgabe zu erzeugen.

Wo wird der Chatverlauf gespeichert?

Der sichtbare Verlauf ist lokal im Browser. Es ist keine zentrale, geteilte Archivierung.

Was ist lokal im Browser und was wird in der Plattform geteilt?

Im aktuellen Zustand gilt:

- die **Chat-Kontinuität** wird lokal gespeichert, pro Paar **Projekt + Agent**, im aktuellen Browser;
- das **gemerkte aktive Projekt** hängt ebenfalls vom Browser und manchmal von der lokalen Sitzung ab;
- weitere browserlokale Bequemlichkeiten sind die **Sprache der Oberfläche**, das **Theme**, die Liste der **zuletzt verwendeten Projekte**, der Lese-/Löschstatus des **Benachrichtigungszentrums** und einige gespeicherte **Tabellen- oder Ansichtspräferenzen**;
- **Dokumente, Importe, Artefakte, Genehmigungen, veröffentlichte Berichte, Projektbenachrichtigungen, Signale, Digests, Entwürfe** und **gesteuerte Aktionen** gehören zur **gemeinsam genutzten Plattform**.

Es ist daher normal, dass ein Chatverlauf beim Wechsel des Browsers oder Geräts verschwindet, während gesteuerte Projektobjekte für andere berechtigte Nutzer sichtbar bleiben.

Was bedeutet **All projects** genau?

All projects ist ein **Geltungsbereich für benutzerdefinierte Agenten**, kein einzelnes Projekt und keine Portfolio-Ansicht. Das bedeutet, dass ein benutzerdefinierter Agent in allen Projekten sichtbar bleiben kann, auf die **dasselbe Konto** Zugriff hat. Jeder Run wird dennoch im **aktiven Projekt** ausgeführt, das zum Zeitpunkt des Chats gewählt ist.

Warum erscheint ein benutzerdefinierter Agent nicht in einem anderen Projekt?

Prüfen Sie zuerst seinen **Geltungsbereich**. Ein Agent mit **Project only** bleibt auf das aktuelle Projekt beschränkt. Wenn die Umgebung einen Agenten mit **All projects** bereitstellt, muss er zusätzlich mit **demselben Konto** in einem Projekt geöffnet werden, auf das dieses Konto Zugriff hat.

Wird der Chatverlauf pro Projekt, pro Agent oder nur im Browser beibehalten?

Die Kontinuität ist **lokal im Browser** und an das Paar **Projekt + Agent** gebunden. Sie ist weder global für den gesamten Mandanten noch automatisch zwischen Browsern

geteilt.

Welche Browser oder Berechtigungen sollten für die Spracheingabe zuerst geprüft werden?

Beginnen Sie mit der Browserunterstützung für `SpeechRecognition` / `webkitSpeechRecognition`, dann prüfen Sie die Mikrofonzugriffsberechtigung. Wenn der Button nicht verfügbar bleibt oder die Erkennung fehlschlägt, kehren Sie zur Texteingabe zurück, ohne den Projektpfad zu blockieren.

Warum ist die Spracheingabe nicht in jeder Umgebung sichtbar?

Weil diese Funktion vom Browser und seiner Unterstützung für Spracherkennung abhängt. Die Spracheingabe ist optional: Wenn sie nicht eingeblendet wird oder nicht funktioniert, bleibt die Texteingabe in **Agents** der normale Arbeitsweg.

FAQ — Wissen und Suche

Warum wirken Arbeitsbereich, Wissen oder KI-Protokoll leer?

Prüfen Sie zuerst, ob ein **aktives Projekt** vorhanden ist. In der aktuellen Anwendung können diese Oberflächen einen **normalen leeren Zustand** anzeigen, solange kein Projekt ausgewählt ist.

Wenn bereits ein Projekt aktiv ist, unterscheiden Sie danach zwischen einem normalen leeren Zustand und einem tatsächlichen Fehlen von Daten: neues Projekt, kein Run, kein Dokument, kein Artefakt oder aktiver Filter.

Warum ist Berichte & Artefakte leer?

Die häufigsten Ursachen sind:

- es wurde noch kein **Artefakt** oder **PM-Dokument** erstellt;
- der Run blieb auf der Stufe der **strukturierten Ausgabe**;
- das falsche Projekt oder ein Filter verbirgt die Zeilen;
- die Umgebung enthält nicht dieselben Beispieldaten wie andere Screenshots oder Tests.

Warum ist ein Dokument in der Liste sichtbar, aber noch nicht auffindbar?

Weil es noch im Zustand **Ingesting** sein kann oder auf das Ende der Indexierungs-Pipeline wartet.

Was bedeuten **source label** und **source system**?

Dies sind Herkunftsindikatoren. Sie helfen, zu erkennen, woher ein Dokument oder Import stammt, ohne die gesamte detaillierte Konfiguration erneut zu lesen.

Warum kann ein Import als abgeschlossen erscheinen, während einige Dokumente noch nicht auffindbar sind?

Weil die sichtbare Ingestion nicht immer bedeutet, dass die gesamte Indexierung abgeschlossen ist. Prüfen Sie den Dokumentstatus (**Indexed** , **Ingesting** , **Failed**) und starten Sie die Suche erneut, wenn das Dokument tatsächlich indexiert ist.

Warum ist ein Dokument **Indexed**, aber ein Beweis bleibt **unavailable** in einer strukturierten Ausgabe?

Das Dokument kann in **Wissen** vorhanden sein, während der zugehörige Beweis zum Run nicht bestätigt, neu geöffnet oder stabilisiert werden konnte, als die Ausgabe generiert wurde. Lesen Sie weiter in [Ausgaben, Beweise und Frische](#), dann prüfen Sie den Run in [Berichte, KI-Protokoll und Nachverfolgbarkeit](#), falls nötig.

Was bedeuten die Frische-Badges in der Suche und in Beweisen?

Sie zeigen den zeitlichen Vertrauensstatus der Quelle an: **fresh** , **aging** , **stale** , **conflicting** oder **unavailable** . Nutzen Sie sie als Signal für eine erneute Durchsicht vor der Veröffentlichung, nicht als kosmetisches Detail.

Was ist der Unterschied zwischen **Trace ID** , **Context snapshot ID** und **Structured output ID** ?

- **Trace ID**: Hauptverfolgungs-ID, um einen Run oder ein Ereignis exakt zu finden;
- **Context snapshot ID**: Aufnahme des dokumentalen/Projektkontexts, der während des Runs verwendet wurde;
- **Structured output ID**: ID der tatsächlich erzeugten strukturierten Ausgabe.

Im Alltag ist die **Run ID** der praktischste Anker auf dem Bildschirm. Die **Trace ID** wird besonders wichtig, wenn Support, Audit oder eine serviceübergreifende Diagnose eingebunden sind.

FAQ — KI-Ausgaben und KI-Protokoll

Was ist der Unterschied zwischen Runs und Activity?

Runs zeigt die Ausführungen von Agenten und deren Metadaten; **Activity** zeigt eine Zeitleiste von Projektereignissen und das zugehörige Rohpayload.

Wie erkenne ich, welcher KI-Anbieter tatsächlich verwendet wurde?

Öffnen Sie die Run-Details im **KI-Protokoll** und lesen Sie **Effective AI Provider**. Das ist der Referenzwert für diesen Run.

Warum garantieren **Validate** und **Test** nicht immer, dass genau dieser Anbieter tatsächlich verwendet wird?

Weil **Validate** und **Test** vor allem die administrative Konsistenz und die Konnektivität der Konfiguration prüfen. Welcher Anbieter für einen konkreten Run tatsächlich verwendet wurde, entscheidet sich erst zur Laufzeit und ist im **KI-Protokoll** sichtbar.

Ein Run ist in **Runs** sichtbar, aber keine klare Folge erscheint in **Activity**. Was tun?

Dieser Fall bedeutet oft, dass der Run tatsächlich existiert, aber noch kein Entwurf, Artefakt, Benachrichtigung oder nachgelagerte Aktion erstellt wurde, oder Sie öffnen nicht das richtige Projekt bzw. den richtigen Filter in **Activity**. Führen Sie die Untersuchung über [Berichte](#), [KI-Protokoll](#) und [Nachverfolgbarkeit](#) durch und folgen Sie der Reihenfolge **Diff / Linie / Runs / Activity**.

Wie lese ich das Feld **Cost** ?

Verstehen Sie **Cost** als Transparenzsignal zur Laufzeit: **tokens** und **calls** helfen vor allem bei Untersuchung, Support und Nutzungsverständnis, sind aber für sich allein

kein fachliches Freigabesignal. Wenn Sie einen projektübergreifenden Hinweis auf Budget- oder Nutzungsdruck brauchen, öffnen Sie stattdessen **cost_pressure** im **Portfolio**.

Was soll ich mit **Confidence** und **Source freshness** konkret anfangen?

- **Confidence** ist ein Prüfhinweis, kein eigenständiger Beweis;
- **Source freshness** zeigt den Grad der Aktualität der zitierten Nachweise;
- wenn einer der beiden Werte schwach, alt, **conflicting** oder **unavailable** wirkt, gehen Sie vor einer externen Weitergabe zu Nachweisen, Run und Linie zurück.

FAQ — Berichte, Artefakte und Governance

Was ist der Unterschied zwischen PM Doc, Artefakt und Artefaktversion?

Das Artefakt ist das verwaltete Objekt, die Artefaktversion ist sein historisiertes Stadium, und der PM Doc ist das Projektdokument, das aus diesem Objekt überarbeitet, bearbeitet oder veröffentlicht wurde.

Warum ist eine Aktion sichtbar, aber nicht ausführbar?

Prüfen Sie Rechte, Connector, Projekt-Binding, Governance-Richtlinie und erforderliche Genehmigung. Siehe auch [Governance, Entscheidungen und Aktionen](#).

Wann muss ich Approve, Publish oder Add to knowledge?

- **Approve** validiert eine Artefaktversion, die noch im **draft** ist;
- **Publish** löst die verwaltete Verbreitung zu einem Ziel oder Format aus;
- **Add to knowledge** injiziert ein erneut gelesenes Dokument in die Projekt-Suche.

Diese drei Aktionen sind nicht austauschbar.

Wie wähle ich einen **conflicting** Beweis vor der Veröffentlichung aus?

Öffnen Sie die widersprüchlichen Quellen, vergleichen Sie den Ausschnitt, das Datum, die Herkunft und die Frische, dann dokumentieren Sie die Entscheidung im Artefakt, in der Review-Notiz oder im Governance-Workflow. Falls nötig, verknüpfen Sie anschließend alles mit dem **KI-Protokoll**.

Warum bleibt ein Benachrichtigungsentwurf **held** oder geht nie zu einem externen Kanal?

In der Oberfläche ist **in_app** der direkteste Pfad. Externe Kanäle können in der **held / draft** Haltung bleiben, bis die verwaltete Verbreitung, die Richtlinie, der Connector oder die Genehmigung erfüllt sind. Folgen Sie der Kette in **Governance, Entscheidungen und Aktionen**: Signal, möglicher Digest, Entwurf, Richtlinie, Connector, dann Genehmigung.

Warum bleibt eine Aktion **pending approval** oder **approved** ohne sichtbare Ausführung?

- **pending approval** bedeutet, dass die Zustimmung noch nicht erteilt wurde;
- **approved** bedeutet, dass die Zustimmung existiert, aber nicht unbedingt, dass die Ausführung bereits stattgefunden hat.

Bestätigen Sie anschließend die nachgelagerte Phase in **Aktionen & Genehmigungen**, dann in **Activity**. Falls nötig, nutzen Sie die Methode in **Berichte, KI-Protokoll und Nachverfolgbarkeit**.

Warum ist eine Integration in der Plattform verfügbar, aber in meinem Projekt gesperrt?

Eine technische Plattformdefinition reicht nicht aus. Es müssen noch ein gültiges **Projekt-Binding**, passende Berechtigungen, eine kompatible Richtlinie, ein akzeptabler Gesundheitsstatus und eine vollständige anbieterspezifische Konfiguration vorhanden sein.

Warum beweist **Validate** nicht immer, dass ein vollständiger externer Aufruf erfolgreich war?

Für Connectoren und Ingestionsanbieter bestätigt **Validate** zuerst die Konsistenz der Konfiguration: Pflichtfelder, Modus, Auth, URL und Quelle oder Ziel. Ein echter

Netzwerkaufruf erfolgt nur, wenn ein Connectivity-Probe aktiviert ist. Auch dann bleibt der Probe nicht destruktiv: Er erstellt nicht zwingend ein Ticket, sendet keine Nachricht und führt keinen Vollimport aus.

Wenn eine Aktion oder ein Import bereit wirkt, aber kein externes Ergebnis sichtbar ist, prüfen Sie in dieser Reihenfolge: Plattformdefinition, anbieterspezifische Konfiguration, Validierung oder Probe, Projekt-Binding, Policy, Benutzerberechtigung, Health-Zustand, danach Aktions- oder Import-Payload. Siehe auch [Connectors und Integrationen](#).

FAQ — Portfolio und Verwaltung

Warum stimmen Beispieldaten nicht immer exakt mit der Dokumentation überein?

Live-Umgebungen können sich unterscheiden. Manche Projekte zeigen nicht immer dieselben vorab geladenen Dokumente, Berichte oder Suchbeispiele wie in den Referenz-Screenshots.

Warum zeigt das Portfolio keine Projekte oder Ausreißer an?

Mehrere Lesarten sind normal:

- es wurde noch kein zugängliches Projekt geladen;
- aktuell ist kein Projekt oder kein Signal ausgewählt;
- der Vergleich hat keine verwertbaren Projektzusammenfassungen geliefert;
- einzelne Signale sind mangels Nachweisen nicht verfügbar;
- kein Projekt überschreitet mit der aktiven Konfiguration den globalen Ausreißer-Schwellenwert.

Ein ruhiges Portfolio kann daher aus einer restriktiven Auswahl, fehlenden Nachweisen oder einer tatsächlich stabilen Lage resultieren.

Gibt es implizite Standardwerte im Portfolio?

Nein. Die Oberfläche bietet vor allem **Standardwerte**, die Aktion **Reset defaults** und gespeicherte **Kohorten**. Die Standardwerte sind ein sicherer Startpunkt, aber kein verpflichtendes Modell. Einige Umgebungen zeigen zusätzlich eine vorkonfigurierte Kohorte; auch das variiert je nach Umgebung.

Wie löse ich einen Sitzplatz oder weise ihn neu zu?

Dies geschieht über **Plattformverwaltung** durch ein autorisiertes Profil. Die Rücknahme gibt den Sitz für eine spätere Neuzuweisung frei, vorbehaltlich der Abonnement-/Lizenzregeln und eines möglichen Rücknahmefensters.

Was bedeutet es, wenn **Validate** erfolgreich ist, **Test** aber in den KI-Anbieter-Einstellungen fehlschlägt?

Die administrative Konfiguration wirkt konsistent, aber die reale Konnektivität oder der entfernte Zugriff funktionieren noch nicht. Prüfen Sie Endpoint, Secret oder die tatsächliche Authentifizierung, die Erreichbarkeit des Anbieters und mögliche Netzwerkbeschränkungen. Folgen Sie danach der Sequenz in [Portfolio und technische Administration](#).

Warum ist mein Anbieter sichtbar, aber nie **Operational**?

Ein Anbieter kann konfiguriert oder sogar validiert sein, ohne die gesamte Kette **Configuration → Validation → Test → Activate** durchlaufen zu haben. Prüfen Sie auch Aktivierungsstatus, Laufzeitauswahl, Health und allgemeine Readiness, bevor Sie ihn als nutzbar betrachten.

Was tun, wenn in den KI-Anbieter-Einstellungen kein Azure OpenAI Deployment erscheint?

Das bedeutet in der Regel, dass in der konfigurierten Azure-OpenAI-Ressource kein Deployment sichtbar ist oder die Erkennung mit den aktuellen Parametern nicht gelingt. Prüfen Sie Endpoint, Auth, API-Version und die tatsächliche Existenz der Deployments in Azure. Führen Sie anschließend die Detailprüfung in [Portfolio und technische Administration](#) durch.

Warum ist der KI-Anbieter sichtbar, aber nicht editierbar oder nutzbar?

Der Anbieter kann lesbar sein, während seine Änderung einer Admin-Rolle vorbehalten ist. Seine tatsächliche Nutzung hängt auch von Readiness, Health-Zustand, Berechtigungen und der Laufzeitauflösung des tatsächlichen Anbieters ab.

Weiter

- [Glossar](#)
- [Start](#)
- [Portfolio und technische Administration](#)

Glossar

[Startseite](#) · Glossar

A

Verwaltete Aktion

Operation, die in der Anwendung vorbereitet und dann zur Genehmigung vor Ausführung eingereicht wird, z. B. eine SharePoint-Veröffentlichung oder die Erstellung eines Tickets.

Agent

Spezialisierte konversationelle Komponente, die im Kontext des aktuellen Projekts arbeitet und strukturierte Ausgaben, Zitate und Empfehlungen erzeugen kann.

Genehmigungen / approvals

Validierungsschritt, der verwendet wird, um eine Aktion vor ihrer Ausführung zu akzeptieren, abzulehnen oder zu rahmen.

Artefakt

Zwischen- oder Endprodukt, das in **Rapports & artefacts** nutzbar ist.

Artefaktziel / destination d'artefact

Verwaltetes Ziel, das bei einer Veröffentlichung oder Dokumentenverbreitung verwendet wird, z. B. SharePoint.

B

Projektbindung

Projektbezogener Bindeglied, das eine Plattformintegration tatsächlich in einem bestimmten Projekt nutzbar macht.

C

Portfolio-Befehlszentrum

Mehrprojektvergleichsfläche, basierend auf Signalen, Gewichten, Schwellenwerten und gespeicherten Kohorten.

Zitate

Referenzen, die mit bestimmten Agenten- oder Lauf-Ergebnissen angezeigt werden, um die verwendeten Beweise oder Quellen zu zeigen.

Kohorte

Gespeicherte Gruppe von Projekten und Portfolioberechnungsparametern.

Vertrauen

Indikator, der einer strukturierten Ausgabe beigelegt ist, um die Zuverlässigkeit des Ergebnisses zu beurteilen.

Wissen

Bereich, in dem Referenzdokumente des Projekts gesucht, hochgeladen, importiert und gefiltert werden.

Kontext-Snapshot

Erfassung des Kontexts, die einem Lauf im Journal IA zugeordnet ist.

D

Deployment-selected AI Provider / ausgewählter KI-Anbieter bei der Bereitstellung

Anbieter, der bei der Installation oder Bereitstellung der Umgebung ausgewählt wird.

Diff

Vergleich zweier Artefaktversionen, um Abweichungen vor Genehmigung oder Veröffentlichung zu überprüfen.

Digest

Geleitete Zusammenfassung mehrerer Signale, sichtbar im Arbeitsbereich und als Grundlage für einen Benachrichtigungsentwurf nutzbar. Siehe auch die Seite [Governance, Entscheidungen und Aktionen](#).

Dokumentkategorien / catégories documentaires

Klassifizierung, die verwendet wird, um die Inhalte des Projekts zu organisieren und deren Nutzung zu verbessern.

E

Effective AI Provider / tatsächlich genutzter KI-Anbieter

Anbieter, der tatsächlich für einen bestimmten Lauf verwendet wird. Dies ist der Referenzwert im Journal IA.

Berechtigung

Legacy-technische Bezeichnung für eine Zugriffs- oder Ausführungsblockierung. Marketplace-Pläne nutzen sie nicht, um unterschiedliche Produktfunktionen freizuschalten; prüfen Sie stattdessen Lizenz-/Sitzverfügbarkeit, Binding, Rolle, Policy, Konfiguration und Health-Zustand.

Aktivitätsereignis

Eintrag in der **Activity**-Zeitleiste im Journal IA, mit Typ, Art, Akteur und rohem Payload.

Arbeitsbereich

Zentrale Projektseite, die Zusammenfassung, operative Transparenz, Signale und Projekteinstellungen bündelt.

Execution connector / Ausführungs-Connector

Verwalteter Connector, der verwendet wird, um eine externe Aktion zu starten, z. B. Teams, Jira oder SharePoint-Veröffentlichung.

Executed / ausgeführt

Status, der anzeigt, dass eine verwaltete Aktion tatsächlich gestartet und protokolliert wurde, über die reine Genehmigung hinaus.

F

Modellfamilie

Transparenzinformation, die im Journal IA sichtbar ist und den tatsächlich verwendeten Modellentyp angibt.

Frisch / alternd / veraltet / widersprüchlich / nicht verfügbar

Frischezustände, die verwendet werden, um einen Beweis oder eine Quelle zu qualifizieren: frisch, alternd, veraltet, widersprüchlich oder nicht verfügbar.

Ingest-Anbieter

Technische Quelle, die das Importieren von Inhalten in das Wissenssystem ermöglicht.

H

Health / Gesundheitszustand

Indikator für Verfügbarkeit oder zu prüfenden Zustand, der auf einen Connector, einen Anbieter oder das globale Gesundheitsdashboard angewendet wird.

Held

Status, der einen Entwurf oder einen Veröffentlichungsfluss zurückhält, der noch nicht an seinen Zielkanal gesendet werden soll.

J

Journal IA

Seite, die die Läufe und die damit verbundenen Aktivitäten der KI-Verarbeitung anzeigt, mit Trace ID, Kontext, Zitate und zugehörigen Artefakten.

L

Nur-Lesezugriff

Status, in dem eine Seite oder ein Tab sichtbar, aber nicht bearbeitbar bleibt.

Nachverfolgung

Verfolgungskette, die einen Lauf, eine strukturierte Ausgabe, ein Artefakt, ein PM Doc und die zugehörigen Beweise verbindet.

LLM deployment name

Genauer Name der LLM-Bereitstellung, die von bestimmten Anbietern, insbesondere Azure OpenAI, in der Plattformverwaltung erwartet wird.

O

Operational

Status, der anzeigt, dass ein Anbieter nach erfolgreicher Konfiguration, Validierung und Test als betriebsbereit gilt.

P

Palette de commandes

Mechanismus für schnellen Zugriff auf häufige Seiten und Aktionen über die obere Leiste.

Pending approval

Status eines Antrags oder einer verwalteten Aktion, die noch eine menschliche Genehmigung vor Ausführung erfordert.

PM Doc

Überarbeitete Projektmanagementdokumentation, die bearbeitet, hochgeladen, veröffentlicht oder aus **Rapports & artefacts** wieder in das Wissen injiziert wurde.

Renderprofil

Parameter, der verwendet wird, um das Format oder das Renderverhalten eines generierten Dokuments zu bestimmen.

R

Rapports & artefacts

Bereich, der verwendet wird, um Projektlieferungen zu überprüfen, zu vergleichen, zu bearbeiten, zu veröffentlichen und herunterzuladen.

Readiness

Bereitschaftsgrad eines Projekts, einer Integration oder eines verwalteten Flows, um ohne operative Blockierung zu funktionieren. Siehe auch [Portfolio und technische Administration](#).

Run

Aufgezeichnete Ausführung eines KI-Processing oder Agentenaustauschs, die anschließend im Journal IA einsehbar ist.

S

Lizenzstelle

Lizenzeinheit, die von einem Benutzer in Deployments verbraucht wird, bei denen der Zugriff durch ein Abonnement begrenzt ist.

Signal

Proaktives Element, das ein Thema zur Aufmerksamkeit hervorhebt, z. B. eine Widerspruch, ein Block, geringe Frische oder eine weitere Handlung.

Source label

Quellenlabel, das hilft, lesbar zu identifizieren, woher ein Dokument oder ein Import stammt.

Source system

Quellsystem, das zusammen mit einem Beweis oder Suchergebnis angezeigt wird.

Structured output / strukturierte Ausgabe

Formatierte Ausgabe eines Agenten oder eines Laufs, die Zusammenfassung, Entscheidungen, Zitate, Vertrauen und Metadaten enthalten kann.

T

Dashboard

Orientierungsseite, die den allgemeinen Zustand, Metriken und vorgeschlagene nächste Aktionen anzeigt.

Test

Verbindungsprüfung, die nach der Validierung eines Anbieters ausgeführt wird, um zu bestätigen, dass die Plattform ihn tatsächlich nutzen kann.

Trace ID

Technische Kennung eines Laufs oder Ereignisses, unverzichtbar für Untersuchung und Support.

V

Validate / validation

Administrative Phase, die die Konsistenz einer Konfiguration vor der Verbindungsprüfung oder der Aktivierung eines Anbieters überprüft.

Version d'artefact

Historisierte Version eines Artefakts, die für Diff, Nachverfolgung, Genehmigung und Veröffentlichung verwendet wird. Siehe auch [Berichte](#), [KI-Protokoll](#) und [Nachverfolgbarkeit](#).

W

Watchpoint

Expliziter Aufmerksamkeitspunkt in einer strukturierten Ausgabe, der häufig verwendet wird, um ein Risiko, einen Widerspruch oder einen zu beobachtenden Bereich anzuzeigen.

Suite

- [Wartung, Support und FAQ](#)
- [Startseite](#)
- [Einführung](#)

Aktionen und Freigaben

Eine gesteuerte Aktion kann aus einem Signal, Dokument oder Connector-Fluss entstehen und je nach Richtlinie eine Genehmigung benötigen.

Aktion vorschlagen

1. Öffnen Sie Signal, PM-Dokument oder die Seite mit der Aktion.
2. Wählen Sie die Aktion, zum Beispiel SharePoint-Veröffentlichung oder Jira-Ticket.
3. Prüfen Sie Inhalt, Ziel und Begründung.
4. Senden Sie die Aktion.
5. Prüfen Sie den Status.

Genehmigen oder ablehnen

1. Öffnen Sie **Actions & approvals**.
2. Filtern Sie wartende Aktionen.
3. Öffnen Sie die Details.
4. Prüfen Sie Nachweise, Ziel, Wirkung und Antragsteller.
5. Wählen Sie **Approve** oder **Reject**.

Approved ist nicht executed

Approved bedeutet genehmigt. **Executed** bedeutet tatsächlich ausgeführt. Externe Aktionen benötigen Connector, Projektbindung, passende Richtlinie, Rolle, Gesundheit und gegebenenfalls Live-Modus.

Blocker

BLOCKER	BEDEUTUNG
Rolle fehlt	Nutzer darf nicht vorschlagen oder genehmigen
require approval	Genehmigung erforderlich
deny	Richtlinie verbietet die Aktion
Not bound	Projekt ist nicht angebunden

BLOCKER	BEDEUTUNG
Not healthy	Connector/Fournisseur ist nicht einsatzbereit

Azure- und Entra-Administration

Diese Seite richtet sich an Azure- und Tenant-Administratoren.

Bereitstellen

1. Öffnen Sie das ProPM-Agent-Angebot in Azure Marketplace.
2. Wählen Sie Plan, Abonnement, Region und Ressourcengruppe.
3. Geben Sie die im Assistenten verlangten Werte ein.
4. Wählen Sie die initiale KI-Anbieterfamilie.
5. Starten Sie die Bereitstellung.
6. Öffnen Sie die veröffentlichte URL.
7. Schließen Sie Entra-Zugriff und erste Administratoren ab.

Nach der Bereitstellung

THEMA	SEITE	
KI-Anbieter konfigurieren	KI-Anbieter	
Plattformintegrationen	Plattformintegrationen	
Lizenzen und Updates	Lizenzen	
Supportdiagnose	Supportdiagnose	

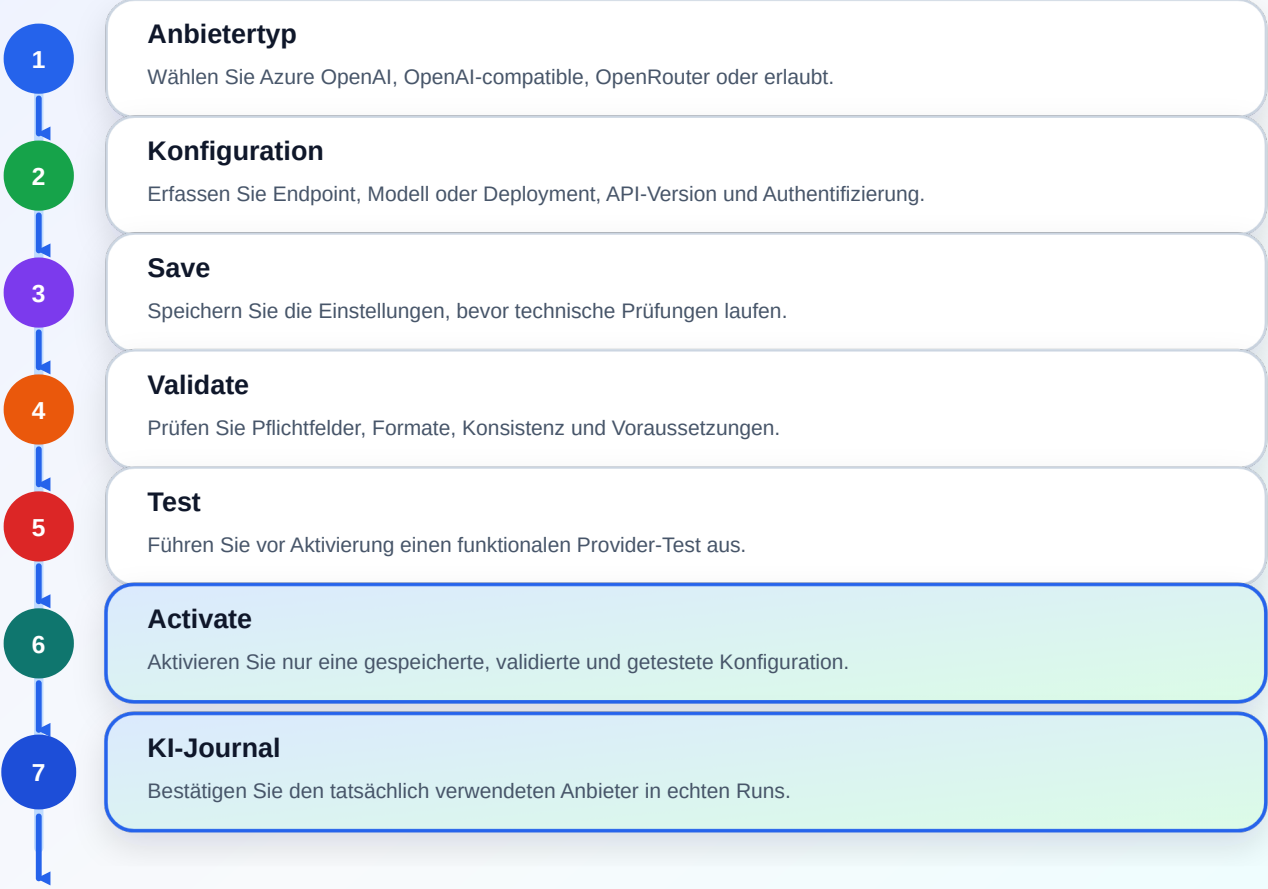
Hinweise

Der im Marketplace gewählte Anbieter ist nur die initiale Absicht. Der tatsächlich genutzte Anbieter wird im [KI-Journal](#) geprüft.

KI-Anbieter

KI-Anbieter-Einstellungen

Eine KI-Konfiguration ist erst nach Validierung, Test und kontrollierter Aktivierung belastbar.



Kopieren Sie niemals Secrets, API-Schlüssel oder Tokens in Tickets
Nutzen Sie sichere Referenzen und teilen Sie nur nicht sensible Informationen.

Diese Seite erklärt die Administration des KI-Anbieters auf Plattformebene.

Aktionen

AKTION	ZWECK
Save	Konfiguration speichern
Validate	Kohärenz prüfen
Test	Funktionalen Test ausführen

AKTION	ZWECK
Activate	Anbieter für Runs aktivieren

Konfiguration

1. Öffnen Sie **Platform Administration**.
2. Öffnen Sie **AI Provider Settings**.
3. Wählen Sie den Anbietertyp.
4. Füllen Sie die Felder der Oberfläche aus.
5. Wählen Sie **Save**.
6. Führen Sie **Validate** aus.
7. Führen Sie **Test** aus.
8. Wählen Sie **Activate**.
9. Prüfen Sie einen echten Run im [KI-Journal](#).

Wichtig

Secrets bleiben in sicheren Administrationswerkzeugen. Der effektive Anbieter eines Runs ist im KI-Journal maßgeblich.

Plattformintegrationen

Integrationen werden auf Plattformebene definiert und auf Projektebene nutzbar gemacht.

Vier Ebenen

EBENE	FRAGE
Plattform	Ist die Integration definiert und validiert?
Projekt	Ist sie an das aktive Projekt gebunden?
Governance	Erlaubt die Richtlinie die Aktion?
Ausführung	Sind Gesundheit, Rolle und Live-Modus ausreichend?

Integration definieren

1. Öffnen Sie **Platform Administration**.
2. Öffnen Sie **Platform Integrations**.
3. Wählen Sie Connector oder Ingestion Provider.
4. Erstellen oder öffnen Sie die Definition.
5. Speichern und validieren Sie.
6. Prüfen Sie den Validierungsverlauf.

Projektbindung

1. Öffnen Sie das Projekt.
2. Öffnen Sie Projektintegrationen.
3. Wählen Sie die validierte Integration.
4. Nutzen Sie **Bind to project**.
5. Prüfen Sie Readiness und Health.

Weiter

- [Connectors](#)
- [Aktionen und Freigaben](#)

Lizenzen, Pläne und Updates

Azure Marketplace bleibt die Quelle für Kauf, Preis und Abrechnung. ProPM Agent zeigt die erkannten Kapazitäten und Nutzer.

Für ein in-place App-Image-Update nutzen Sie **Deployment & Updates**. Für einen Planwechsel oder ein größeres Update mit bestehenden Daten erstellen Sie eine neue Marketplace-Bereitstellung und wählen **Attach existing ProPM data resources**.

Zähler

ZÄHLER	BEDEUTUNG
Ordered seats	Bestellte Kapazität
Included seats	Im Plan enthalten
Supplemental seats	Zusätzlich gekauft
Used seats	Verwendete Nutzerlizenzen
Remaining seats	Verbleibende Lizenzen

Nutzer verwalten

1. Öffnen Sie **Platform Administration**.
2. Öffnen Sie **Tenant plan and licensed users**.
3. Prüfen Sie die Nutzerliste.
4. Nutzen Sie **Release user** nur, wenn der Nutzer keinen Zugriff mehr braucht.

Marketplace-Plan aktualisieren

Refresh Marketplace plan synchronisiert bekannte Informationen. Es kauft nichts, ändert keinen Plan und keine Abrechnung.

Planwechsel oder größeres Update mit vorhandenen Daten

Nutzen Sie diesen Ablauf, wenn eine neue Marketplace Managed Application erforderlich ist, vorhandene ProPM-Daten aber erhalten bleiben müssen.

1. Öffnen Sie Azure Marketplace.
2. Wählen Sie den Zielplan.
3. Erstellen Sie eine neue ProPM-Bereitstellung.
4. Wählen Sie **Attach existing ProPM data resources**.
5. Tragen Sie die vollständige Resource ID der vorherigen ProPM Managed Application ein.
6. Lassen Sie Overrides leer, außer Support oder Architektur erfordern sie.
7. Prüfen Sie Cutover, Administration, CORS, Monitoring, SQL-Passwort und VNet CIDR.
8. Wählen Sie **Review + create**.

Update-Bildschirm 1 - Vorhandene Daten anhängen

[Home](#) > [ProPM Agent](#)

Create ProPM Agent ...

Environment Name * ⓘ

prod

Installation mode ⓘ

Attach existing ProPM data resources ▼

Attach mode creates a new Marketplace Managed Application and application tier for the selected plan, but connects it to the resources used by an existing ProPM deployment. Enter the previous Managed Application resource ID so ProPM can read its recorded deployment outputs and discover the actual data resources, including when the previous deployment is also an attach deployment. Keep the previous deployment stopped or read-only during cutover to avoid two app tiers writing to the same data.

Previous ProPM Managed Application resource ID * ⓘ

Advanced overrides: leave the resource IDs below empty to auto-discover the ProPM resources from the previous deployment outputs. Fill a field only if the previous deployment outputs are unavailable or the data resources are externally managed.

Existing Storage account resource ID (optional override) ⓘ

Existing Azure AI Search service resource ID (optional override) ⓘ

Existing SQL server resource ID (optional override) ⓘ

Existing SQL database name (optional override) ⓘ

Existing Cosmos DB account resource ID (optional override) ⓘ

Existing Document Intelligence account resource ID (optional override) ⓘ

Existing Service Bus namespace resource ID (optional override) ⓘ

Previous

Next

Review + create

FELD	PFLICHT	WAS EINTRAGEN	EMPFEHLUNG
Environment Name	Ja	Kurzer Umgebungsname, z. B. <code>prod</code> , <code>uat</code> oder <code>test</code> .	Stabilen, nicht geheimen Namen verwenden.
Installation mode	Ja	Attach existing ProPM data resources.	Erstellt neuen Anwendungstier und nutzt vorhandene Datenressourcen.
Previous ProPM Managed Application resource ID	Ja	Vollständige Azure Resource ID der vorherigen ProPM Managed Application.	Id aus Properties kopieren, nicht nur Namen eintragen.
Existing Storage account resource ID (optional override)	Nein	Resource ID des vorhandenen Storage Accounts.	Standardmäßig leer lassen.
Existing Azure AI Search service resource ID (optional override)	Nein	Resource ID des vorhandenen Azure AI Search-Dienstes.	Nur bei fehlender Auto-Erkennung ausfüllen.
Existing SQL server resource ID (optional override)	Nein	Resource ID des vorhandenen SQL Servers.	Identifiziert den Server, nicht die Datenbank.
Existing SQL database name (optional override)	Nein	Name der vorhandenen SQL-Datenbank.	Nur nutzen, wenn nicht automatisch erkannt.
Existing Cosmos DB account resource ID (optional override)	Nein	Resource ID des vorhandenen Cosmos DB Accounts.	Nur bei explizitem Bedarf ausfüllen.
Existing Document Intelligence account resource ID (optional override)	Nein	Resource ID des vorhandenen Document Intelligence Accounts.	Nur für externe oder benutzerdefinierte Ressource.
Existing Service Bus namespace resource ID (optional override)	Nein	Resource ID des vorhandenen Service Bus Namespace.	Standardmäßig leer lassen.
Previous	Nein	Zurück zum vorherigen Schritt.	Startet keine Bereitstellung.
Next	Nein	Weiter zum nächsten Schritt.	Nach Pflichtfeldern verwenden.
Review + create	Nein	Azure-Validierung vor Erstellung.	Erst nach Abschluss aller Parameter verwenden.

Update-Bildschirm 2 - Cutover und Plattform

Microsoft Azure

Search resources, services, and docs (G+)

Home > ProPM Agent

Create ProPM Agent ...

Existing Event Grid topic resource ID (optional override) ⓘ

Block previous deployment during cutover ⓘ

☒

Platform Administration Entra Group Object IDs * ⓘ

Platform Administration Bootstrap Users (optional) ⓘ

Allow Azure RBAC admin recovery ⓘ

☒

Reuse previous AI provider configuration ⓘ

☒

AI provider fields are hidden for this update. ProPM will reuse the previous deployment's AI provider metadata and the existing Platform Administration configuration stored with your attached data. You can change AI settings after deployment from Platform Administration.

CORS Allowed Origins ⓘ

Enable alerting (Azure Monitor) ⓘ

☒

Enable debug logging ⓘ

☐

One secure SQL input is still required for attach updates: enter the existing ProPM SQL admin password so the new application tier can connect to the reused database. This password is not exposed by ARM outputs and cannot be read from the previous Managed Application because the managed resource group is protected by Azure deny assignments.

Password * ⓘ

Confirm password * ⓘ

VNet CIDR * ⓘ

10.0.0.0/16

Previous

Next

Review + create

FELD	PFLICHT	WAS EINTRAGEN	EMPFEHLUNG
Existing Event Grid topic resource ID (optional override)	Nein	Resource ID des vorhandenen Event Grid Topics.	Leer lassen, außer Auto-Erkennung scheitert.
Block previous deployment during cutover	Nein, empfohlen	Aktivieren, um die vorherige Umgebung während der Validierung zu blockieren.	Verhindert parallele Schreibzugriffe auf dieselben Daten.

FELD	PFLICHT	WAS EINTRAGEN	EMPFEHLUNG
Platform Administration Entra Group Object IDs	Ja	Object IDs der Entra-Gruppen für Plattformadministration.	Object IDs verwenden, nicht Anzeigenamen.
Platform Administration Bootstrap Users (optional)	Nein	Bootstrap- oder Recovery-Benutzer.	Minimal halten.
Allow Azure RBAC admin recovery	Nein	Wiederherstellung über Azure RBAC.	Aktiv lassen, wenn Governance es erlaubt.
Reuse previous AI provider configuration	Empfohlen	Vorherige KI-Konfiguration übernehmen.	KI-Felder werden ausgeblendet; Änderungen später in Plattform Administration.
CORS Allowed Origins	Szenarioabhängig	Zusätzliche Web-Origins.	Leer lassen, wenn nicht benötigt.
Enable alerting (Azure Monitor)	Nein	Azure Monitor Alerts aktivieren.	Für Produktion empfohlen.
Enable debug logging	Nein	Detaillierte Logs aktivieren.	Nur für kontrollierte Diagnose.
Password	Ja	Vorhandenes ProPM SQL-Admin-Passwort.	Erforderlich, damit der neue Anwendungstier die wiederverwendete Datenbank erreicht. Als Secret behandeln.
Confirm password	Ja	Derselbe Wert wie Password .	Beide Werte müssen übereinstimmen.
VNet CIDR	Ja	Privater Netzwerkbereich, z. B. <code>10.0.0.0/16</code> .	Mit Netzwerkteam validieren und Überschneidungen vermeiden.

Updates

Prüfen Sie **Deployment & Updates** während eines kontrollierten Wartungsfensters und behalten Sie Supportinformationen für Rollback-Fälle. Nutzen Sie diese Funktion nicht für Planwechsel oder Cutover zu vorhandenen Datenressourcen.

Agenten

Agenten arbeiten im aktiven Projektkontext und können strukturierte Ausgaben mit Nachweisen erzeugen.

Standardagenten

BEDARF	AGENT
Übergreifende Analyse	Orchestrator
Richtlinien und Freigaben	Governance
Umfang und Anforderungen	Scope
Planung und Abhängigkeiten	Schedule
Budget und Kosten	Finance
Stakeholder und Kommunikation	Stakeholders
Kapazität und Ressourcen	Resources
Risiken und Probleme	Risk

Run starten

1. Öffnen Sie **Agents**.
2. Prüfen Sie das aktive Projekt.
3. Wählen Sie den Agenten.
4. Schreiben Sie eine präzise Anfrage mit Ziel und Kontext.
5. Fügen Sie relevante Dokumente hinzu, falls möglich.
6. Starten Sie den Run.
7. Lesen Sie Antwort, Zitate, Frische und Vertrauen.
8. Öffnen Sie bei Bedarf das [KI-Journal](#).

Eigene Agenten

Erstellen Sie einen eigenen Agenten nur mit passender Rolle. Wählen Sie Name, Zweck, Projektbereich oder **All projects**, speichern Sie und testen Sie mit einer einfachen Anfrage.

Hinweise

Eine Agentenantwort ist kein finales PM-Dokument. Chatverlauf kann browserlokal sein.

Wissen, Dokumente und Importe

Diese Seite erklärt, wie Sie Projektwissen pflegen und als Nachweis für Agenten und PM-Dokumente nutzen.

Dokument hochladen

1. Öffnen Sie **Knowledge**.
2. Wählen Sie **Upload**.
3. Wählen Sie die Datei.
4. Ergänzen Sie Kategorie oder Metadaten.
5. Starten Sie den Upload.
6. Warten Sie auf den Status **Indexed**.

Aus genehmigter Quelle importieren

1. Öffnen Sie **Knowledge**.
2. Wählen Sie die Importaktion.
3. Wählen Sie die verfügbare Quelle.
4. Starten Sie den Import.
5. Prüfen Sie den Importverlauf.
6. Verwenden Sie Dokumente erst nach **Indexed**.

Status

STATUS	BEDEUTUNG	AKTION
Indexed	Bereit für Suche und Agenten	Verwenden
Ingesting	Verarbeitung läuft	Warten und aktualisieren
Failed	Verarbeitung fehlgeschlagen	Format/Quelle prüfen
Nicht sichtbar	Falsches Projekt, Filter oder Rolle	Projekt und Filter prüfen

Suche

Suchen Sie nach Fachbegriffen, Dokumentnamen oder Fragen. Lesen Sie Snippet, Zitat, Source Label, Source System und Frische, bevor Sie eine Aussage verwenden.

Weiter

- [Agenten](#)
- [Strukturierte Ausgaben](#)
- [Supportdiagnose](#)

PM-Dokumente und Artefakte

Diese Seite beschreibt den Dokumentenfluss von einem Run bis zu einem geprüften PM-Dokument.

Lebenszyklus

Run → strukturierte Ausgabe → Artefakt → Version → PM-Dokument → Download / Publish / Add to knowledge.

BEGRIFF	BEDEUTUNG
Strukturierte Ausgabe	Agentenergebnis, noch zu prüfen
Artefakt	Governed Objekt aus Run oder Review
Version	Historisierter Zustand mit Diff
PM-Dokument	Geprüfter, versionierter Projektliefergegenstand

Dokument prüfen

1. Öffnen Sie **PM Docs** oder **Reports & artifacts**.
2. Prüfen Sie das aktive Projekt.
3. Filtern Sie nach Status, Typ oder Datum.
4. Öffnen Sie das Dokument.
5. Prüfen Sie Inhalt, Nachweise, Diff und Lineage.
6. Speichern Sie Änderungen, falls erlaubt.
7. Verwenden Sie **Download**, **Publish** oder **Add to knowledge** nach Review.

Aktionen

AKTION	WIRKUNG
Download	Lokale Kopie erzeugen
Publish	An eine gesteuerte Zielablage veröffentlichen
Add to knowledge	Geprüftes Dokument in Projektwissen aufnehmen

Weiter

- [KI-Journal](#)
- [Aktionen und Freigaben](#)

KI-Journal

Das KI-Journal zeigt, was bei einer Ausführung tatsächlich passiert ist: Run, Status, Zeit, Nutzer, Projekt, effektiver KI-Anbieter und Support-IDs.

Run finden

1. Öffnen Sie **AI Log**.
2. Wechseln Sie zu **Runs**.
3. Filtern Sie nach Projekt, Agent, Status oder Zeitraum.
4. Öffnen Sie den Run.
5. Prüfen Sie Status, Zeit, effektiven Anbieter und Links zu Artefakten.

Effektiven Anbieter prüfen

1. Öffnen Sie die Run-Details.
2. Suchen Sie **Effective AI Provider**.
3. Vergleichen Sie ihn mit dem erwarteten Anbieter.
4. Notieren Sie Abweichungen.
5. Bei wiederholter Abweichung öffnen Sie [KI-Anbieter](#).

Supporthinweis

Sammeln Sie Run ID, Trace ID, Artifact ID oder Action ID, wenn sichtbar. Kopieren Sie keine sensiblen Payloads.

Bekannte Einschränkungen

Nutzergrenzen

THEMA	EINSCHRÄNKUNG	EMPFEHLUNG
Chatverlauf	Kann browserlokal sein	PM-Dokumente und KI-Journal für gemeinsame Spuren nutzen
Aktives Projekt	Seiten hängen vom Projekt ab	Obere Leiste prüfen
All projects	Kein Zugriff auf alle Tenant-Projekte	Projektzugriff prüfen
Agentenantwort	Kein finales Dokument	Prüfen und bei Bedarf PM-Dokument erstellen
Vertrauen	Keine Freigabe	Nachweise und Frische prüfen

Integrationen

Ein sichtbarer Connector ist nicht automatisch nutzbar. Plattformdefinition, Projektbindung, Richtlinie, Rolle, Gesundheit und gegebenenfalls Live-Modus müssen passen.

Azure-Administration

Der im Deployment gewählte Anbieter beweist nicht den Anbieter eines Runs. **Refresh Marketplace plan** synchronisiert nur Informationen.

Portfolio- und Administrationsleitfaden

[Startseite](#) · Portfolio- und Administrationsleitfaden

Diese Seite wurde neu organisiert

Diese URL bleibt als Orientierungsseite erhalten, damit bestehende Links zu **Portfolio und technische Administration** nicht brechen.

Der Inhalt ist jetzt in drei klarere Administrationsbereiche aufgeteilt.

BEDARF	ZIELSEITE
Projekte vergleichen, Portfolio-Signale konfigurieren, Kohorten, Ausreißer und Projekt-Drill-downs lesen	Portfolio
KI-Anbieter konfigurieren, Readiness validieren, Plattformintegrationen, Bindings, Health und technische Blockierungsursachen verstehen	KI-Anbieter und Plattformintegrationen
Tenant-Plan, lizenzierte Benutzer, Zusatzlizenzen, App-Updates, Image-Inventar und Rollback auf bestehenden Azure Container Apps verwalten	Tenant-Plan, lizenzierte Benutzer und App-Updates

Produktregel zu Marketplace-Plänen

Alle Marketplace-Pläne stellen dieselben Produktfunktionen bereit. Nur die bestellte Lizenzkapazität unterscheidet sich.

Wenn ein Benutzer blockiert ist, prüfen Sie verbleibende Lizenzen, Rollen, Projektzugriff, Bindings, Policy, Konfiguration oder Health. Interpretieren Sie den Plan nicht als Funktionsstufe.

Empfohlene Lesereihenfolge

1. Beginnen Sie mit [Portfolio](#), wenn es um den Vergleich von Projekten geht.
2. Fahren Sie mit [KI-Anbieter und Plattformintegrationen](#) fort, wenn es um technische Vorbereitung, Anbieter, Konnektoren oder Bindings geht.
3. Nutzen Sie [Tenant-Plan, lizenzierte Benutzer und App-Updates](#), wenn es um Zugriffszuweisung, Tenant-Lizenzen, Zusatzlizenzen oder das Aktualisieren einer vorhandenen Installation geht.

Verwandte Seiten

- [Konnektoren und Integrationen](#)

- [Berichte, KI-Log und Nachvollziehbarkeit](#)
- [Wartung, Support und FAQ](#)

Aktives Projekt und Projekterstellung

Das aktive Projekt bestimmt, welche Daten in Knowledge, Agents, PM Documents, Signals und AI Log sichtbar sind.

Projekt auswählen

- 1. Öffnen Sie den Projektumschalter in der oberen Leiste.
- 2. Suchen Sie das gewünschte Projekt.
- 3. Wählen Sie es aus.
- 4. Prüfen Sie den Projektnamen in der oberen Leiste.
- 5. Öffnen Sie das Dashboard und bestätigen Sie die Daten.

Projekt erstellen

- 1. Öffnen Sie **Projects**.
- 2. Wählen Sie **Create project**, falls verfügbar.
- 3. Geben Sie Name, Beschreibung und erforderliche Einstellungen ein.
- 4. Wählen Sie die Standardsprache der Projektdaten, falls angeboten.
- 5. Speichern Sie.
- 6. Prüfen Sie, ob das Projekt auswählbar ist.

Wichtige Begriffe

BEGRIFF	BEDEUTUNG	
Aktives Projekt	Aktueller Arbeitskontext	
All projects	Nur Projekte, auf die dasselbe Konto bereits Zugriff hat	
Lokal gemerktes Projekt	Browserpräferenz, nicht globale Plattformregel	

Häufige Probleme

SYMPTOM	URSACHE	AKTION
Schaltfläche fehlt	Rolle reicht nicht aus	Project Owner kontaktieren

SYMPTOM	URSACHE	AKTION
Projekt fehlt	Sie sind kein Mitglied	Hinzufügen lassen
Daten passen nicht	Falsches aktives Projekt	Projekt wechseln und neu laden

Zielgruppen, Rollen und Geltungsbereiche

Diese Seite hilft, die richtige Dokumentation je nach Verantwortung in ProPM Agent zu öffnen.

Für wen

PROFIL	NUTZEN
Business-Nutzer	Tägliche Arbeit ohne Azure-Details verstehen
Project Owner	Mitglieder, Rollen, Governance und Projektintegrationen steuern
Azure-/Tenant-Administrator	Bereitstellung, Entra, KI-Anbieter, Lizenzen und Updates verwalten
Support/Audit	Runs, Trace IDs und Diagnoseinformationen finden

Dokumentationsebenen

EBENE	ENTHÄLT	ENTHÄLT NICHT
Endnutzer	Schritte, Rollen, erwartete Ergebnisse	Secrets, Roh-Payloads, Infrastrukturdetails
Project Owner	Projekttrollen, Richtlinien, Integrationen	Connector-Secrets und Low-Level-Auth
Azure/Admin	Marketplace, Entra, KI-Anbieter, Lizenzen	Tägliche Fachabläufe
Support/Audit	Run ID, Trace ID, effektiver Anbieter	Passwörter, Tokens oder vertrauliche Daten

Empfohlene Pfade

ROLLE	START	DANACH
Neuer Nutzer	Start	Navigation, Dashboard
Contributor	Wissen	Agenten, PM-Dokumente
Project Owner	Zugriffskontrolle	Governance
Tenant-Admin	Azure und Entra	KI-Anbieter, Lizenzen

ROLLE	START	DANACH
Support	Supportdiagnose	KI-Journal , FAQ

Sicherheitsregel

Geben Sie niemals Secrets, Kennwörter, Tokens oder vollständige sensible Payloads in Support-Anfragen weiter.

Sicherheit und Compliance

Identität und Zugriff

Die Anmeldung erfolgt in Azure-Umgebungen über Microsoft Entra ID. Projektzugriff hängt von Mitgliedschaft und Rolle ab.

Tenant- und Projektisolation

Der Tenant bildet den Organisationsrahmen. Das aktive Projekt begrenzt Dokumente, Runs, Signale, Aktionen und PM-Dokumente. **All projects** umgeht keine Berechtigungen.

Daten und Datenschutz

Laden Sie nur genehmigte Dokumente hoch. Maskieren Sie Support-Screenshots. Kopieren Sie niemals Secrets, Schlüssel, Tokens oder Passwörter in Prompts, Notizen, Aktionen oder Tickets.

Nachvollziehbarkeit

ELEMENT	WO
Run	KI-Journal
Effektiver KI-Anbieter	KI-Journal
PM-Dokument	PM-Dokumente
Gesteuerte Aktion	Aktionen
Trace ID	Supportdiagnose

Responsible AI

Prüfen Sie KI-Ausgaben vor Entscheidungen oder Veröffentlichungen. Vertrauen ersetzt keine Freigabe.

Signale und Benachrichtigungen

Signale lenken Aufmerksamkeit auf Risiken, Blocker, fehlende Nachweise oder Aktionen.

Signal lesen

1. Öffnen Sie **Signals**, **Inbox** oder den Signalbereich im Workspace.
2. Prüfen Sie Schweregrad, Status, Modus und Datum.
3. Öffnen Sie die Details.
4. Lesen Sie Nachweise und Empfehlungen.
5. Entscheiden Sie: behandeln, zurückstellen, schließen, Entwurf oder Aktion erstellen.

Aktionen

AKTION	WIRKUNG
Refresh	Signale neu laden oder berechnen
Generate digest draft	Digest-Entwurf vorbereiten
Create draft	Verwertbaren Entwurf erzeugen
Snooze 24h	Vorübergehend zurückstellen
Dismiss	Signal schließen

Benachrichtigungen

Öffnen Sie die Glocke, lesen Sie Einträge, folgen Sie Links, markieren Sie alles als gelesen oder löschen Sie die lokale Liste, wenn sie nicht mehr benötigt wird.

Weiter

- [Aktionen und Freigaben](#)
- [Supportdiagnose](#)

Support, Audit und Diagnose

Diese Seite erklärt, welche Informationen bei einem Incident nützlich sind.

NovaBiz Kontakt

Für den NovaBiz Support:

- E-Mail: support@navabiz.pro
- Adresse: NovaBiz, 131 Continental Dr, Suite 305, Newark, DE 19713, United States

Zu liefern

INFORMATION	BEISPIEL
Seiten-URL	Seite beim Fehler
Aktives Projekt	Projektname
Nutzer	Konto oder Gruppe, kein Passwort
Zeitpunkt	Datum, Uhrzeit, Zeitzone
Aktion	Upload, Run, Publish, Approve
Meldung	Exakter Text oder maskierter Screenshot
IDs	Run ID, Trace ID, Action ID falls sichtbar

Niemals liefern

- Passwörter, Secrets, Tokens oder Schlüssel.
- Vollständige sensible Payloads.
- Unmaskierte Kundendaten.

Schnelldiagnose

SYMPTOM	ERSTE PRÜFUNG
Anmeldung scheitert	Konto, Tenant, URL

SYMPTOM	ERSTE PRÜFUNG
Kein Projekt	Mitgliedschaft und Rolle
Dokument nicht indexiert	Status in Knowledge
Agent antwortet nicht	Run im KI-Journal
Aktion wartet	Freigabe, Richtlinie, Connector
Lizenz blockiert	Verbleibende Seats

Dashboard

Dashboard-Lesereihenfolge

Beginnen Sie mit dem Projektkontext, dann lesen Sie Status, Aktivität und Schnellzugriffe.

1

Aktives Projekt

Alle Kennzahlen, Runs und Dokumente hängen vom ausgewählten Projekt ab.

2

Projektkennzahlen

Prüfen Sie Fortschritt, Blocker, Risiken und fehlende Nachweise.

3

Zustand und Warnungen

Prüfen Sie Plattformzustand und Warnungen vor der Diagnose.

4

Letzte Aktivität

Lesen Sie Runs, Importe, Dokumente und Aktionen, um Änderungen zu verstehen.

5

Aktionsabkürzungen

Öffnen Sie Wissen, Agents, PM-Dokumente oder Aktionen im Kontext.

Wenn die Seite leer wirkt, prüfen Sie zuerst aktives Projekt und Rolle

Ein fehlender Projektkontext oder eine Rolle erklärt die meisten leeren Zustände.

Das Dashboard fasst den aktiven Projektkontext zusammen: Aktivität, Wissen, Agenten, PM-Dokumente, Signale, Aktionen und Schnellzugriffe.

Voraussetzungen

- Sie sind angemeldet.
- Ein aktives Projekt ist ausgewählt.
- Ihre Rolle erlaubt den Zugriff.

Dashboard lesen

1. Öffnen Sie **Dashboard**.
2. Prüfen Sie das aktive Projekt in der oberen Leiste.
3. Lesen Sie Karten für Dokumente, Runs, PM-Dokumente, Signale und Aktionen.
4. Prüfen Sie die jüngste Aktivität.

5. Öffnen Sie den passenden Schnellzugriff: **Workspace, Knowledge, Agents, PM Docs** oder **AI Log**.

Leere Zustände

ZUSTAND	BEDEUTUNG	AKTION
Kein aktives Projekt	Seiten haben keinen Projektkontext	Projekt auswählen
Kein Projekt verfügbar	Ihr Konto hat keinen Projektzugriff	Project Owner kontaktieren
Zugriff verweigert	Rolle reicht nicht aus	Rolle prüfen lassen
Veraltete Zahlen	Verarbeitung läuft noch	Seite aktualisieren oder später erneut prüfen

Weiter

- [Aktives Projekt](#)
- [Wissen](#)
- [Signale](#)