Voraussetzungen für Copilot Studio

Ein Agent in Microsoft Copilot Studio läuft in der Microsoft-Cloud, nicht auf einem Rechner in Ihrem Haus. Er erreicht FINN.AI MCP deshalb nur über den Zugang von außen — eine Adresse im Internet, verschlüsselt über HTTPS. Diese Seite ist die Checkliste dafür: was vor dem Einrichtungstermin bei Ihnen stehen muss und was wir dann auf dem Server einrichten.

> Die meisten Punkte brauchen Ihre IT oder Ihren IT-Dienstleister: Domain, Firewall und die Verwaltung von Microsoft 365. Fehlt einer davon, kommt keine Verbindung zustande — und Copilot Studio meldet dann selten, woran es liegt.

So sieht die Verbindung aus

```
Copilot Studio (Microsoft-Cloud)
        │  https://mcp.ihre-firma.de/mcp
        ▼
Ihre Firewall: Ports 80 und 443 weitergeleitet
        ▼
Webserver auf dem FINN.ghost-Server (Caddy): Zertifikat, Weiterleitung
        ▼
FINN.AI MCP
```

Der Webserver bezieht das Zertifikat für die Adresse selbst und erneuert es selbst. Nach außen liegt damit nur er — weder die Oberfläche von FINN.ghost noch die SelectLine sind aus dem Internet erreichbar.

Internetanschluss, Domain und Firewall

Voraussetzung	Worauf es ankommt
Feste öffentliche IPv4-Adresse	Bei einer wechselnden Adresse zeigt der DNS-Eintrag nach dem nächsten Wechsel ins Leere.
Eigene IPv4-Adresse am Anschluss	Anschlüsse ohne eigene IPv4-Adresse (DS-Lite, Carrier-Grade-NAT, häufig bei Kabelanbietern) erlauben keine Weiterleitung von außen. Dann geht es nur mit einem anderen Anschluss oder einer zusätzlichen festen Adresse vom Anbieter.
DNS-Eintrag	Eine eigene Subdomain, etwa `mcp.ihre-firma.de`, als A-Eintrag auf die öffentliche Adresse. Einen AAAA-Eintrag (IPv6) nur, wenn er ebenfalls auf diesen Server führt — ein falscher AAAA-Eintrag kann die Ausstellung des Zertifikats scheitern lassen.
Port 443 von außen frei	Auf 443 liegen oft schon Exchange/Outlook im Web, ein Remotedesktop-Gateway, ein SSL-VPN oder die Anmeldeseite der Firewall. Ist der Port belegt, braucht es eine zweite öffentliche Adresse oder eine Verteilung nach Adressnamen auf dem vorhandenen System — das vorher klären.
Weiterleitung 80 und 443	Beide Ports in der Firewall auf den FINN.ghost-Server weiterleiten, auf zwei freie Ports dort. Welche das sind, legen wir beim Termin gemeinsam fest.
Port 80 dauerhaft	Nicht nur zur Einrichtung: Das Zertifikat wird regelmäßig erneuert, und dafür muss der Webserver über Port 80 erreichbar bleiben.
Windows-Firewall	Auf dem Server eingehend die beiden Ports freigeben, auf die weitergeleitet wird.
Kein Filter, der Microsoft aussperrt	Die Anfragen kommen aus den Rechenzentren von Microsoft, nicht vom Rechner des Anwenders. Eine Länder- oder Adresssperre in der Firewall darf diese nicht abweisen.

> „Nur im Firmennetz" ist mit Copilot Studio nicht möglich: Auch wenn alle Anwender im Büro sitzen, stellt Microsoft die Verbindung her.

Wer den Zugang nicht ins Internet stellen möchte, nutzt stattdessen einen Assistenten auf dem Arbeitsplatz, siehe Zugang im eigenen Netz.

Server und FINN.ghost

- **Der Server läuft dauerhaft.** Der Agent antwortet nur, solange FINN.ghost läuft — ist der Server nachts aus, ist es der Agent auch.

- **FINN.AI MCP ist lizenziert.** Das Rechnungswesen ist nicht Teil des Standardumfangs und wird auf Wunsch zusätzlich freigeschaltet.
- **SelectLine ab Version 24.2** mit lizenzierter SelectLine-API. Wer FINN.ghost schon für ein anderes Modul einsetzt, hat beides bereits.
- **Fernzugriff mit Administratorrechten** auf den Server für den Einrichtungstermin — wir installieren den Webserver dort als Dienst.

Microsoft 365 und Copilot Studio

Voraussetzung	Worauf es ankommt
Zugang zu Copilot Studio	Wer den Agenten anlegt, muss unter https://copilotstudio.microsoft.com Agenten erstellen dürfen, also in einer Power-Platform-Umgebung die Berechtigung dazu haben. Welche Umgebung dafür vorgesehen ist, entscheidet der Power-Platform-Administrator.
Kontingent	Copilot Studio rechnet über Copilot Credits ab — als Kapazitätspaket oder nutzungsabhängig über ein Azure-Abonnement. Der Verbrauch hängt davon ab, wie viel mit dem Agenten gearbeitet wird.
Datenrichtlinie lässt den Connector zu	Copilot Studio verbindet MCP-Server über einen Power-Platform-Connector. Eine Datenrichtlinie (DLP) im Power Platform Admin Center gilt deshalb auch für FINN.AI MCP. Sind eigene Connectoren dort gesperrt, funktioniert der Agent nicht.
Anmeldung je Anwender	Jeder Anwender meldet sich beim ersten Gebrauch des Agenten selbst an, mit seinem eigenen SelectLine-Benutzer. Mit den Anmeldeinformationen des Erstellers liefe jeder Anwender unter dessen Benutzer — mit dessen Rechten und dessen Kürzel an jeder Änderung. Das hebt den Sinn der Anmeldung auf.
SelectLine-Benutzer für jeden Anwender	Jeder, der den Agenten nutzt, braucht einen SelectLine-Benutzer mit dem Recht auf die SelectLine-API für den Mandanten.
Freigabe in Teams	Soll der Agent in Microsoft Teams oder Microsoft 365 Copilot bereitstehen, muss die Veröffentlichung dort gegebenenfalls vom Administrator freigegeben werden.

> Die Datenrichtlinie ist der häufigste Stolperstein, und sie kann nur der Power-Platform-Administrator ändern. Am besten vorab klären, ob in der gewählten Umgebung eigene Connectoren erlaubt sind.

Im Haus zu klären

Frage	Warum sie zählt
Ist der Datenschutz geklärt?	Die Antworten des Agenten entstehen in der Microsoft-Cloud. Dorthin fließen die Daten, die er für eine Antwort abfragt — auch Adressen und Ansprechpartner. Das gehört vorher mit dem Datenschutzbeauftragten besprochen.
Mit wem wird der Agent geteilt?	Jeder, mit dem der Agent geteilt ist, meldet sich mit seinem eigenen SelectLine-Benutzer an. Was über die SelectLine-API läuft — Belege, Geschäftspartner, Lagerbuchungen —, unterliegt dessen Rechten; lesen kann jeder angemeldete Benutzer den gesamten Mandanten.
Darf geschrieben werden?	Bei Belegen, Geschäftspartnern und Lagerbuchungen entscheiden die Rechte des Benutzers in der SelectLine. Artikel, Projekte, freie Adressen und Journaleinträge schreibt der Agent ohne Rechteprüfung. Einzelne Werkzeuge lassen sich im Agenten abschalten, etwa alle, die löschen.
Wer ist Ansprechpartner?	Für den Termin braucht es jemanden mit Zugriff auf DNS, Firewall und die Verwaltung von Microsoft 365 — oder den jeweiligen Dienstleister.

Siehe Sicherheit und Verantwortung.

Was wir einrichten

1. Den **Webserver** auf dem FINN.ghost-Server: Er bezieht das Zertifikat für Ihre Adresse, erneuert es selbst und leitet die Anfragen an FINN.AI MCP weiter — die Verbindung, die Anmeldung und die Download-Links für Beleg-PDFs.
2. Unter **FINN.MCP → Einstellungen** die **Öffentliche Adresse**, etwa `https://mcp.ihre-firma.de`. Ohne sie gibt es keine Download-Links. Siehe Einstellungen.
3. Den **Agenten in Copilot Studio**, gemeinsam mit Ihnen:
   - Unter **Tools → Tool hinzufügen → Neues Tool → Model Context Protocol** (in der deutschen Oberfläche *Modellkontextprotokoll*) den Zugang eintragen: **Server-URL** `https://mcp.ihre-firma.de/mcp`, als Authentifizierung **OAuth 2.0** mit dynamischer Erkennung — die Adressen für Anmeldung und Token holt sich Copilot Studio dann selbst vom Zugang.
   - Für das Tool **nicht** die Anmeldeinformationen des Erstellers wählen, sondern die jedes Anwenders: Beim ersten Gebrauch öffnet sich für jeden Anwender die Anmeldeseite, und er meldet sich mit seinem SelectLine-Benutzer an.
   - Die generative Orchestrierung des Agenten muss eingeschaltet sein — ohne sie nutzt Copilot Studio keine MCP-Werkzeuge.

4. Eine **Probeverbindung**: drei Fragen, deren Antwort Sie kennen. Siehe Erstinbetriebnahme.

> Ein Agent, der bis 10/2026 mit dem API-Schlüssel (Typ **Header**, Name `x-api-key`) eingerichtet wurde, läuft nach dem Update weiter, solange der Schlüssel in den Einstellungen eingeschaltet ist — dann unter dem Benutzer, mit dem FINN.ghost selbst angemeldet ist, für alle Anwender gleich. Für die Anmeldung je Anwender das Tool neu anlegen, mit OAuth 2.0 und den Anmeldeinformationen jedes Anwenders. Der Webserver davor braucht dafür zusätzliche Weiterleitungen, siehe Zugang von außen.

> Der Zugang bringt 23 Werkzeuge mit. Das freie Lesen bringt zwei dazu und ein freigeschaltetes Rechnungswesen mit ihm noch einmal zwei, das freie Schreiben per SQL drei. Microsoft empfiehlt für einen Agenten höchstens 25 bis 30, erlaubt aber bis zu 128. Werden die Antworten unzuverlässig, lassen sich Werkzeuge, die im Alltag nicht gebraucht werden, im Agenten einzeln abschalten.

> Seltener gebrauchte Funktionen wie Lieferadressen, Ansprechpartner oder Verträge stehen nicht einzeln in der Liste. Der Agent findet sie über das Werkzeug *fachfunktionen* und führt sie über *fachfunktion_lesen*, *fachfunktion_anlegen* bzw. *fachfunktion_aendern* aus. Abschalten lassen sie sich deshalb nur gemeinsam, getrennt danach, ob sie lesen, anlegen oder ändern. Die löschenden Werkzeuge stehen weiter einzeln in der Liste.

Weiter

Erstinbetriebnahme

Created 2026-09-28 14:06:39 UTC by FINN
Updated 2026-10-31 00:55:08 UTC by FINN