

Einstellungen

Unter **FINN.MCP** → **Einstellungen** stehen drei Angaben. Mehr braucht der Zugang nicht.

The screenshot shows the 'FINN.MCP' settings page within the SelectLine application. The page has a dark red header with the 'SelectLine' logo and a settings gear icon. The main content area is white and contains the following fields and information:

- FINN.MCP** (Title) with a help icon (?)
- Text: 'Zugang für KI-Clients (z. B. Claude) auf die Daten des Mandanten. Änderungen an Port und öffentlicher Adresse werden erst nach einem Neustart der Anwendung wirksam – der wird beim Speichern angestoßen.'
- API-Schlüssel** field with a masked value '.....' and icons for visibility (eye) and copying (document).
- Text: 'Gilt als Header x-api-key bzw. Authorization: Bearer und als Kennwort auf der OAuth-Anmeldeseite.'
- Port** field with the value '3000'.
- Öffentliche Adresse** field with the value 'https://vpn.buchenblick.de'.
- Text: 'Port, auf dem der MCP-Server lauscht' and 'Adresse des Reverse-Proxy, nicht die des lokalen Ports. Gesetzt = OAuth aktiv (Connector-Dialoge ohne Header-Feld); leer = nur API-Schlüssel.'
- A blue bar at the bottom left shows an information icon and the text 'Endpoint: https://vpn.buchenblick.de/mcp'.
- A red 'SPEICHERN' button is at the bottom right.

API-Schlüssel

Das Geheimnis, mit dem sich eine Verbindung ausweist. Es wird beim ersten Start der Anwendung selbst erzeugt — steht das Feld leer, ist die Anwendung noch nicht neu gestartet.

Der Schlüssel lässt sich über das Augensymbol anzeigen und über das Kopiersymbol in die Zwischenablage legen. Ändern lässt er sich hier nicht.

Es gibt **einen** Schlüssel für beide Zugangswege: Programme im eigenen Netz senden ihn mit, und auf der Anmeldeseite des Zugangs von außen wird derselbe Wert als Kennwort eingegeben. Beide Wege öffnen denselben Werkzeugkasten, deshalb gibt es auch nur ein Geheimnis.

Der Schlüssel gehört behandelt wie ein Administratorkennwort: nicht per E-Mail versenden, nicht in einem Ticket hinterlegen, nicht in einer Konfigurationsdatei auf einem geteilten Laufwerk ablegen. Wer ihn hat, hat vollen Zugriff auf den Mandanten.

Port

Der Port, auf dem der Zugang lauscht. Vorbelegt ist 3000.

Zu ändern ist er nur, wenn der Port auf dem Server schon belegt ist.

Öffentliche Adresse

Das Feld entscheidet, **welcher der beiden Zugangswege** aktiv ist:

Feld	Wirkung
leer	Nur der Zugang im eigenen Netz über den Schlüssel. Siehe Zugang im eigenen Netz .
gefüllt	Zusätzlich der Zugang von außen mit Anmeldeseite. Siehe Zugang von außen .

Einzutragen ist die Adresse, unter der der Zugang **von außen** erreichbar ist — also die des vorgeschalteten Webservers, nicht die des lokalen Ports. Beispiel: `https://mcp.kunde.de`.

Die Adresse muss über HTTPS erreichbar sein. Eine unverschlüsselte Adresse wird abgelehnt — über diese Verbindung laufen Mandantendaten.

Der Endpoint

Unterhalb der Felder zeigt die Oberfläche die Adresse an, die in den Assistenten eingetragen wird. Sie endet immer auf `/mcp`:

- mit öffentlicher Adresse: `https://mcp.kunde.de/mcp`
- ohne: die lokale Adresse samt Port, nur im eigenen Netz erreichbar

Speichern startet die Anwendung neu

Port und öffentliche Adresse werden beim Start der Anwendung festgelegt. Beim Speichern wird deshalb ein Neustart angestoßen — für einige Sekunden sind alle Module von FINN.ghost nicht erreichbar.

Das gehört also nicht in die Mittagspause der Kommissionierer. Für alles andere gilt: Der Schlüssel bleibt über den Neustart erhalten, bestehende Verbindungen melden sich von selbst neu an.

Weiter

[Zugang im eigenen Netz](#)

Created 2026-09-01 11:36:37 UTC by API
Updated 2026-09-01 13:29:49 UTC by API