

Einstellungen

Datenbank, SelectLine-API, Lizenz, Server, E-Mail-Versand und EU-Auslands-Kontengruppen.

- [SelectLine - Einstellungen](#)
- [Datenbank](#)
- [SelectLine-API](#)
- [Lizenz und Module](#)
- [Server und Oberfläche](#)
- [E-Mail-Versand](#)
- [E-Mail über Microsoft 365](#)
- [EU-Auslands-Kontengruppen](#)

SelectLine - Einstellungen

Unter **SelectLine → Einstellungen** liegen alle Angaben, mit denen sich FINN.ghost in Ihre Datenstruktur einfügt. Jede Karte hat hier eine eigene Seite.

SelectLine SOFTWARE

SelectLine

Einstellungen

Shopify

Einstellungen

Zeitsteuerung

Datenbank

Name: SL_MGURKEN

Host: SQL02\SQLSRV17

Nutzer: sa

Passwort:

SPEICHERN

API

SL_MGURKEN

URL: https://sql02/slmobileAPI/

AppKey (FÜR SHOPIFY NICHT NOTWENDIG!)

Nutzer: aplShopify

Passwort:

SPEICHERN

FINN.ghost

Port: 8086

Bildformat: webp

☐ Nutzeranmeldung

Zeitsteuerung

Version: 22.1.0.230814 — ©2023 SelectLine Software GmbH Powered by DAKO-IT GmbH

Die Karten

Karte	Inhalt
Datenbank	Verbindung zur MSSQL-Datenbank des Mandanten
SelectLine-API	Adresse, AppKey und Benutzer der SelectLine-API
Lizenz und Module	der Lizenzschlüssel und was er freischaltet
Server und Oberfläche	Port, Bildformat, Bildqualität, Benutzeranmeldung
SSL mit Let's Encrypt	Zertifikat automatisch beantragen und erneuern
E-Mail-Versand	SMTP für Fehlermeldungen
E-Mail über Microsoft 365	OAuth und App-Only statt Kennwort

Karte	Inhalt
EU-Auslands-Kontengruppen	Kontengruppen je Land für das OSS-Verfahren

Die Karten erscheinen nacheinander: ohne Datenbankverbindung keine API-Karte, ohne API keine Lizenz, ohne Lizenz keine Modulkarten. Eine fehlende Karte heißt also, dass der Schritt davor noch offen ist.

Wann die Anwendung neu startet

Manche Änderungen wirken erst nach einem Neustart des Dienstes — den löst FINN.ghost selbst aus:

Geändert	Was passiert
Lizenz	Neustart, damit die Module geladen werden
Port, Bildformat, Anmeldung	Neustart, danach ist die Oberfläche unter dem neuen Port erreichbar
Zertifikat geholt oder importiert	Neustart, damit es der Webserver verwendet
Datenbank, API, E-Mail	kein Neustart

Wird der Port geändert, ist die Oberfläche unter der alten Adresse nicht mehr erreichbar. Der Browser wird auf die neue Adresse geschickt — Lesezeichen und Verknüpfungen gehören danach angepasst.

Wo die Angaben landen

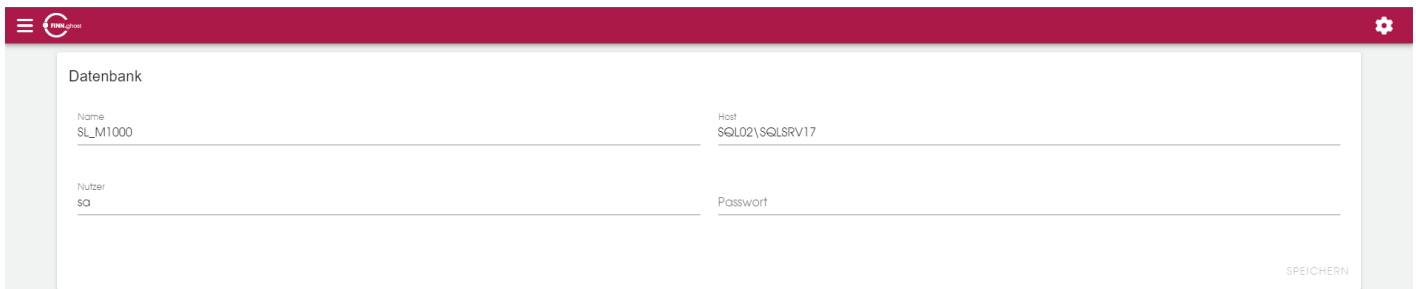
In der `config.json` im Installationsordner. Felder mit Kennwörtern werden dabei verschlüsselt. Siehe [Anpassungen über die config.json](#).

Nächster Schritt

[Datenbank](#)

Datenbank

Die Verbindung zur MSSQL-Datenbank des SelectLine-Mandanten. Sie ist die erste Einstellung — ohne sie erscheinen die weiteren Karten nicht.



The screenshot shows a web interface with a dark red header containing the 'FINN.ghost' logo and a settings icon. Below the header is a form titled 'Datenbank'. The form has four input fields: 'Name' with the value 'SL_M1000', 'Host' with the value 'SQL02\SQLSRV17', 'Nutzer' with the value 'sa', and 'Passwort' which is empty. A 'SPEICHERN' button is located at the bottom right of the form.

Die Felder

Feld	Inhalt	Beispiel
Name	Datenbank des gewünschten Mandanten	SL_M1000
Host	SQL-Server und Instanz	SQL02\SQLSRV17
Nutzer	SQL-Benutzer	sa
Passwort	dessen Kennwort	

Der Benutzer braucht Rechte auf die Tabellen dieser Datenbank **und** das Recht, Tabellen anzulegen — FINN.ghost legt eigene Tabellen im Mandanten an. Ein reines Leserecht genügt nicht.

Der Datenbankname bestimmt, in **welchem Mandanten** gearbeitet wird. Bei mehreren Mandanten lohnt der doppelte Blick: Alles, was FINN.ghost später schreibt, landet in diesem.

Wozu der direkte Zugriff dient

Gelesen wird direkt aus der Datenbank, geschrieben über die SelectLine-API.

Der Grund ist Tempo: Ein Artiklexport prüft zehntausende Datensätze auf Änderungen. Über die API wäre das um ein Vielfaches langsamer. Geschäftslogik — Nummernkreise, Preisfindung, Buchungen — bleibt trotzdem der SelectLine überlassen.

Siehe [SelectLine-API](#).

Wenn die Verbindung nicht zustande kommt

Meldung oder Symptom	Ursache
Anmeldung fehlgeschlagen	Benutzer oder Kennwort falsch
Server nicht erreichbar	Instanzname falsch, oder der SQL-Browser-Dienst läuft nicht
Zeitüberschreitung	Firewall zwischen FINN.ghost und SQL-Server
Verbindung steht, Module bleiben leer	falsche Datenbank — ein anderer Mandant

Bei einer benannten Instanz muss der Dienst **SQL Server Browser** laufen, sonst lässt sich `Server\Instanz` nicht auflösen. Alternativ den Port direkt angeben.

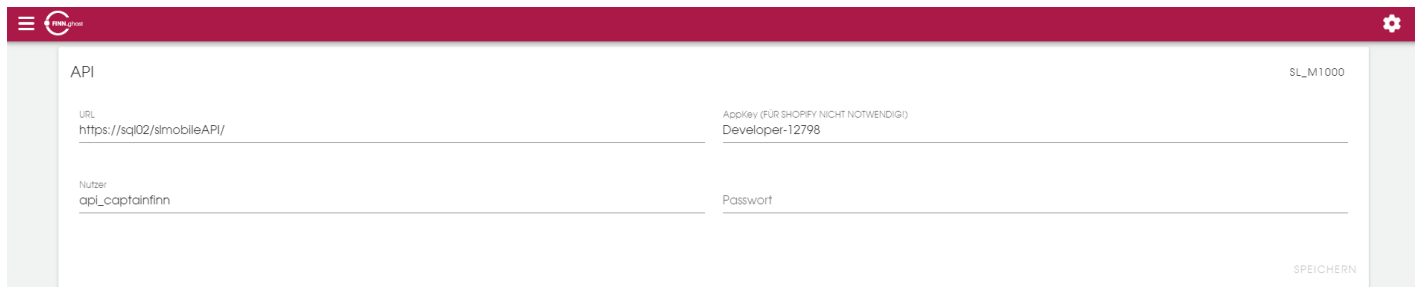
Die genaue Meldung steht im Protokoll. Siehe [Log Informationen](#).

Nächster Schritt

[SelectLine-API](#)

SelectLine-API

Über die SelectLine-API schreibt FINN.ghost in den Mandanten — Belege, Adressen, Artikel, Journale, Buchungen. Sie gehört zu sl.mobile.



The screenshot shows a web interface for configuring the SelectLine API. At the top is a red header bar with the FINN.ghost logo on the left and a settings gear icon on the right. Below the header, the page title 'API' is on the left, and 'SL_M1000' is on the right. The main form area contains four input fields: 'URL' with the value 'https://sql02/slmobileAPI/', 'AppKey (FÜR SHOPPY NICHT NOTWENDIG)' with the value 'Developer-12798', 'Nutzer' with the value 'apl_captainfinn', and 'Passwort' which is empty. A 'SPEICHERN' button is located at the bottom right of the form.

Die Felder

Feld	Inhalt
URL	Adresse der API
AppKey	der bei SelectLine hinterlegte AppKey
Nutzer	in der SelectLine angelegter API-Benutzer
Passwort	dessen Kennwort

URL

Die Adresse von sl.mobile, mit `slmobileApi` statt `slmobile`:

```
https://localhost/slmobileApi
```

Läuft FINN.ghost auf demselben Server wie sl.mobile, ist `localhost` die zuverlässigste Angabe — sie ist unabhängig von Rechnernamen und DNS.

AppKey

Der AppKey wurde beim Kauf der API bei SelectLine angegeben. Einzusehen in der SelectLine unter **Hilfe → Lizenzierung → AppKeys**.

Weicht der Eintrag hier vom AppKey in der SelectLine ab, meldet die API die Anmeldung ab. In diesem Fall den Wert aus der SelectLine übernehmen — nicht umgekehrt.

Bei der Lizenz **SelectLine Shopify-Anbindung** ist die API in der Lizenz enthalten; das Feld bleibt dann leer. In der Oberfläche steht deshalb *für Shopify nicht notwendig*.

Nutzer und Passwort

Der in der API-Konfiguration von sl.mobile eingerichtete API-Benutzer.

Dieser Benutzer arbeitet mit seinen SelectLine-Rechten. Er braucht Rechte auf den Mandanten und auf die Bereiche, die die eingesetzten Module berühren — Artikel, Adressen, Belege, Journale. Fehlt ein Recht, scheitert genau die Übertragung, die es braucht.

Ob die Verbindung steht

Steht sie, zeigt die Karte oben rechts den **Namen des Mandanten**. Ein Klick darauf öffnet die Angaben zum angemeldeten Benutzer.

Das ist die verlässlichste Einzelprüfung der Einrichtung: Der Name kommt aus der SelectLine — er erscheint nur, wenn Adresse, Benutzer, Kennwort und API-Lizenz zusammenpassen.

Wenn die Anmeldung scheitert

Symptom	Ursache
kein Mandantenname, Fehler im Protokoll	Benutzer, Kennwort oder AppKey falsch
Adresse nicht erreichbar	sl.mobile läuft nicht, oder die URL zeigt auf <code>slmobile</code> statt <code>slmobileApi</code>
Zertifikatsfehler	das Zertifikat von sl.mobile wird nicht anerkannt
Anmeldung geht, Schreiben scheitert	dem SelectLine-Benutzer fehlen Rechte

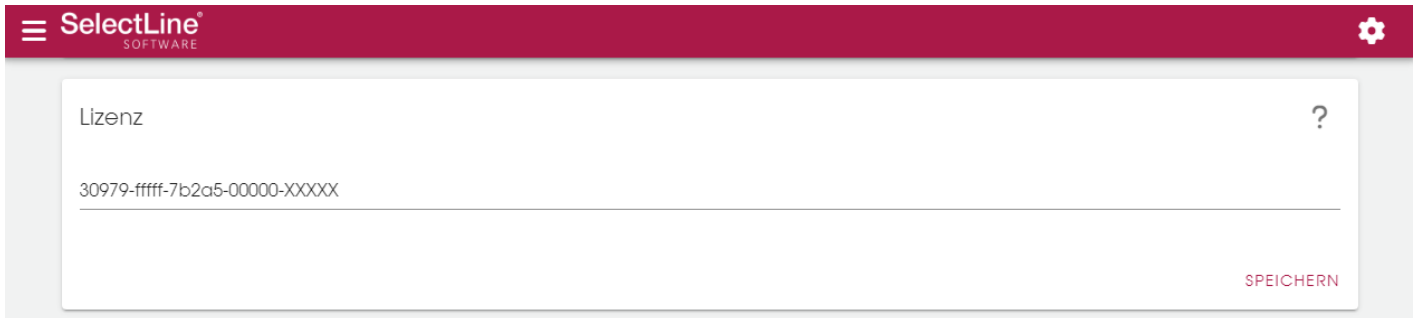
Siehe [Log Informationen](#).

Nächster Schritt

[Lizenz und Module](#)

Lizenz und Module

Die Lizenz entscheidet, welche Module FINN.ghost lädt. Was nicht lizenziert ist, erscheint nicht — weder im Menü noch in der Zeitsteuerung.



The screenshot shows the 'SelectLine SOFTWARE' interface. At the top is a red header bar with the logo on the left and a gear icon on the right. Below the header is a white form area. The form has a title 'Lizenz' in the top left and a question mark icon in the top right. Inside the form, there is a text input field containing the placeholder '30979-ffff-7b2a5-00000-XXXXX'. At the bottom right of the form is a red button labeled 'SPEICHERN'.

Der Schlüssel

Ein Feld, in das der Lizenzschlüssel eingetragen wird. Er kommt vom Fachhändler oder von DAKO-IT.

Nach dem Speichern startet die Anwendung neu, damit die freigeschalteten Module geladen werden. Das dauert einige Sekunden; danach die Seite neu laden.

Was danach im Menü steht

Je Modul ein Menüpunkt.

-  **SelectLine** 
-  **Merkmale / Varianten** 
-  **FINN.mail2sl** 
-  **GetMyInvoices** 
-  **FINN.webshop | B2B** 
-  **Shopware6** 

Modul	Was es macht
Shopware6	Anbindung an Shopware 6
Shopify	Anbindung an Shopify
FINN.webshop B2B	eigener Webshop
FINN.lager	Lagermodul mit Boards und Kommissionierung
Merkmale / Varianten	Sachmerkmale pflegen, Varianten erzeugen
FINN.mail2sl	E-Mails automatisch als Journal ablegen
GetMyInvoices	Eingangsrechnungen aus dem Portal
FINN.AI MCP	Zugriff für KI-Anwendungen
Pipedrive	Abgleich mit dem CRM
Übersetzungen	Artikeltexte übersetzen

Zu jedem Modul gibt es ein eigenes Handbuch. Die Liste steht im Überblick.

Siehe [Überblick](#).

Wenn ein Modul fehlt

Prüfung	
Ist der Schlüssel vollständig eingetragen?	Karte <i>Lizenz</i>
Wurde nach dem Speichern neu gestartet?	Seite neu laden
Ist das Modul überhaupt lizenziert?	beim Fachhändler erfragen
Steht im Protokoll ein Fehler zur Lizenz?	Log Informationen

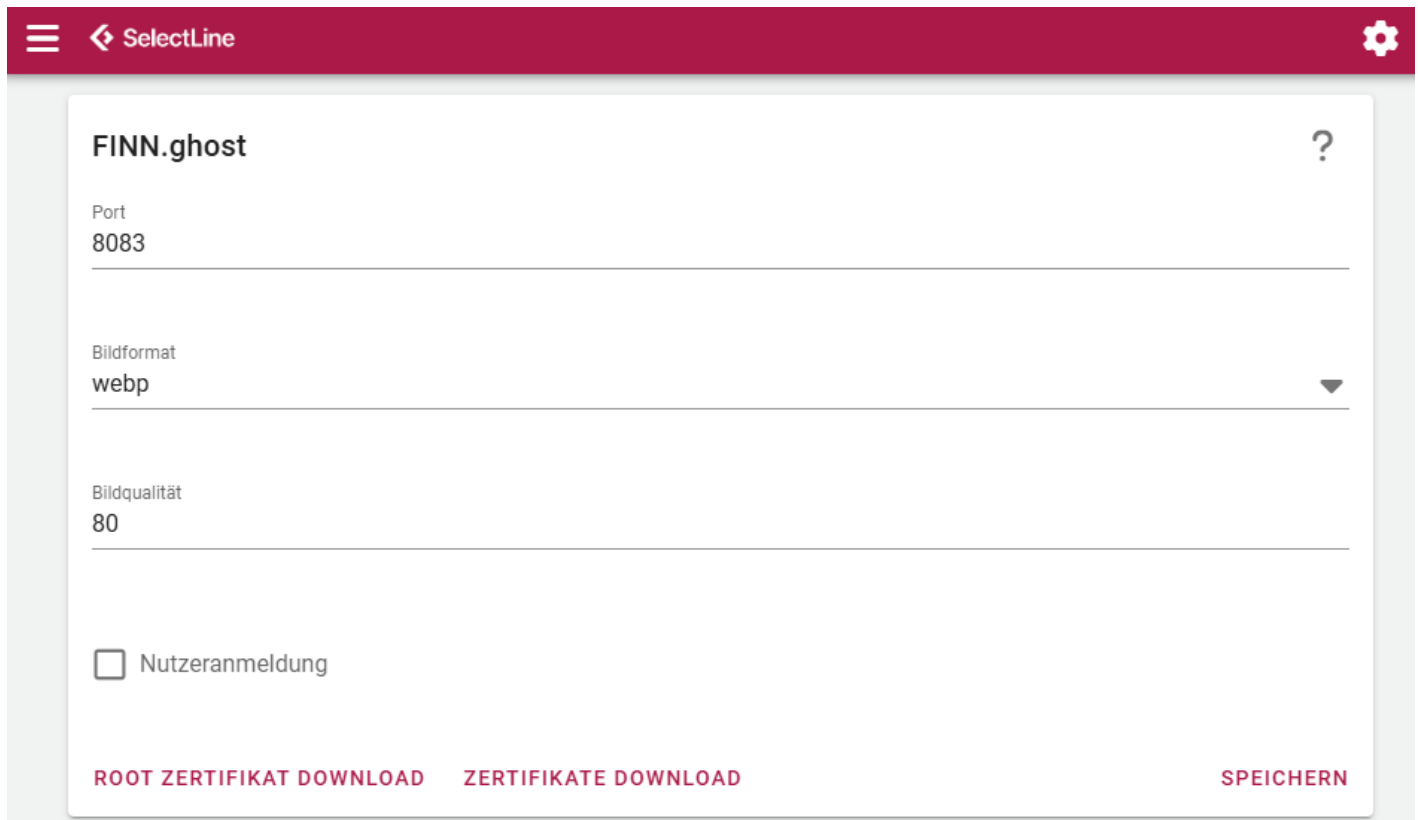
Die Lizenz wird gegen einen Dienst von DAKO-IT geprüft. Ohne ausgehende Internetverbindung kann diese Prüfung fehlschlagen — dann fehlen die Module, obwohl der Schlüssel richtig ist.

Nächster Schritt

[Server und Oberfläche](#)

Server und Oberfläche

Die Karte **FINN.ghost** regelt, unter welchem Port die Oberfläche läuft, wie Bilder an die Drittsysteme übertragen werden und ob eine Anmeldung nötig ist.



The screenshot shows the SelectLine dashboard with a maroon header. The main content area is a white card titled "FINN.ghost" with a question mark icon in the top right corner. Inside the card, there are three input fields: "Port" with the value "8083", "Bildformat" with the value "webp" and a dropdown arrow, and "Bildqualität" with the value "80". Below these fields is a checkbox labeled "Nutzeranmeldung" which is currently unchecked. At the bottom of the card, there are three buttons: "ROOT ZERTIFIKAT DOWNLOAD", "ZERTIFIKATE DOWNLOAD", and "SPEICHERN".

Port

Der Port, unter dem die Oberfläche erreichbar ist. Standard ist **8083**.

Laufen mehrere FINN.ghost-Installationen auf einem Server, braucht jede einen eigenen Port. Sonst startet die zweite nicht — im Protokoll steht dann, dass der Port belegt ist.

Nach dem Speichern startet die Anwendung neu und der Browser wird auf die neue Adresse geschickt. Lesezeichen, Verknüpfungen und die Einbindung in die SelectLine-Dashboards gehören danach angepasst.

Bildformat

In welchem Format Bilder aus der SelectLine an das angeschlossene System übertragen werden — unabhängig davon, wie sie in der SelectLine abgelegt sind.

Wert	Wann
webp	moderne Shops; kleinste Dateien bei gleicher Qualität
jpg	breiteste Verträglichkeit, für Fotos
png	wenn Transparenz gebraucht wird
original	keine Umwandlung; überträgt, was in der SelectLine liegt

Umgewandelt wird beim Übertragen. Eine Änderung wirkt deshalb erst auf Bilder, die danach übertragen werden — für die bereits übertragenen braucht es einen Lauf, der die Bilder erneut schickt.

Bildqualität

Ein Wert von 1 bis 100, Vorgabe **80**. Gilt für die verlustbehafteten Formate.

80 ist ein bewusst gewählter Kompromiss: Unterschiede zum Original sind im Shop kaum zu sehen, die Dateien aber deutlich kleiner. Höhere Werte lohnen selten, niedrigere werden bei Produktbildern sichtbar.

Bei *original* hat die Angabe keine Wirkung.

Nutzeranmeldung

Ist der Haken gesetzt, verlangt die Oberfläche eine Anmeldung. Angemeldet wird sich mit den **API-Benutzern aus sl.mobile**.

Ohne diesen Haken kann jeder, der den Server im Netz erreicht, die Oberfläche öffnen — und damit Einstellungen ändern und Übertragungen starten. Für jede Installation, die über `localhost` hinaus erreichbar ist, gehört die Anmeldung eingeschaltet.

Vor dem Einschalten prüfen, dass ein passender API-Benutzer existiert und das Kennwort bekannt ist — sonst sperrt man sich aus. Wieder hinein kommt man dann nur über die `config.json` auf dem Server.

Siehe [Anpassungen über die config.json](#).

Zertifikate herunterladen

Zwei Schaltflächen in derselben Karte:

Schaltfläche	Was sie liefert
ROOT ZERTIFIKAT DOWNLOAD	das Stammzertifikat für den Arbeitsplatz
ZERTIFIKATE DOWNLOAD	Zertifikat und Schlüssel für diese Installation

Das ist der ältere Weg zu einer sicheren Verbindung. Siehe [Zertifikat einrichten](#).

Für Installationen mit einer öffentlich erreichbaren Domain ist Let's Encrypt einfacher — dort entfällt das Verteilen von Zertifikaten an die Arbeitsplätze.

Siehe [SSL mit Let's Encrypt](#).

Nächster Schritt

[SSL mit Let's Encrypt](#)

E-Mail-Versand

FINN.ghost verschickt Fehlermeldungen und Zusammenfassungen per E-Mail. Der Versand ist technisch optional — praktisch ist er das Frühwarnsystem der Installation.

 SelectLine 

E-Mail 

?

STANDARD

M365-OAUTH

M365-APP-ONLY

Host

Port

☐ Verschlüsselte Verbindung

☐ Outlook365

Nutzer

Passwort

Absender

Absender Name

Empfänger

Betreff

Interval

SPEICHERN

Ohne Mailversand merkt niemand, dass eine Übertragung seit Tagen scheitert — die Meldung steht nur im Protokoll, und dort sieht niemand von selbst hinein. Diese Karte gehört deshalb zur Grundeinrichtung.

Ein- und ausschalten

Der Schalter in der Kartenüberschrift. Ausgeschaltet werden keine Mails verschickt und die Felder sind ausgeblendet.

Drei Wege

Die Karte hat drei Reiter:

Reiter	Wann
Standard	ein SMTP-Konto mit Benutzer und Kennwort
M365-OAuth	Microsoft 365, Versand über ein angemeldetes Konto
M365-App-Only	Microsoft 365, Versand ohne Benutzeranmeldung

Die beiden Microsoft-Wege stehen auf einer eigenen Seite. Siehe [E-Mail über Microsoft 365](#).

Reiter Standard

Feld	Inhalt
Host	SMTP-Server des Kontos
Port	üblich 465 (SSL) oder 587 (STARTTLS)
Verschlüsselte Verbindung	Verschlüsselung einschalten
Outlook365	Besonderheiten von Microsoft-365-Postfächern
Nutzer, Passwort	Zugang zum Postfach
Absender	abweichende Absenderadresse
Absender Name	Anzeigename
Empfänger	Ziele, mehrere mit Komma getrennt
Betreff	Betreff der Meldungsmails
Interval	Zeitspanne in Minuten

Beim Speichern wird sofort eine **Testmail** verschickt. Kommt sie nicht an, stimmt etwas an den Angaben — dann lohnt der Blick ins Protokoll, dort steht die Antwort des Mailservers.

Was das Intervall bedeutet

Meldungen werden gesammelt und im eingestellten Abstand verschickt — nicht einzeln.

Das ist Absicht: Bei einer Störung entstehen viele gleichartige Fehler. Gesammelt ergibt das eine Mail, einzeln hunderte.

10 Minuten sind ein guter Startwert. Wer nur die Tagesübersicht braucht, kann höher gehen; unter 5 Minuten wird es unruhig.

Ein sinnvoller Betreff

Der Betreff steht in jeder Mail. Bei mehreren Installationen gehört hinein, um **welche** es sich handelt — etwa `FINN.ghost Shop` und `FINN.ghost Lager`.

Sonst sind die Mails nicht auseinanderzuhalten, sobald der zweite Ghost dazukommt.

Wenn keine Mails ankommen

Ursache	Abhilfe
Schalter aus	einschalten
Empfänger leer	Adresse eintragen
Anmeldung abgelehnt	Kennwort prüfen; bei Microsoft 365 einen der M365-Reiter nutzen
Port blockiert	Firewall für ausgehendes SMTP öffnen
Mails im Spam	Absenderadresse zur eigenen Domain passend wählen

Microsoft hat die Anmeldung per Benutzer und Kennwort für SMTP abgeschaltet. Für Microsoft 365 führt der Reiter *Standard* deshalb in der Regel nicht mehr zum Ziel.

Siehe [E-Mail über Microsoft 365](#).

Nächster Schritt

E-Mail über Microsoft 365

Microsoft hat die Anmeldung mit Benutzer und Kennwort für SMTP abgeschaltet. Für Postfächer in Microsoft 365 führt deshalb einer der beiden folgenden Wege zum Ziel. Beide brauchen einmalig eine **App-Registrierung** im Azure-Portal.

Welchen Weg wählen

	OAuth	App-Only
Versand als	ein angemeldetes Benutzerkonto	die Anwendung selbst
Anmeldung	einmalig im Browser	keine
Absender	das angemeldete Postfach	ein frei angegebenes Postfach
Nötige Rechte	Delegiert: <code>SMTP.Send</code> , <code>offline_access</code>	Anwendung: <code>Mail.Send</code>

Für einen Server, der jahrelang unbeaufsichtigt läuft, ist **App-Only** der robustere Weg: Es hängt kein Benutzerkonto daran, das gesperrt werden oder das Kennwort wechseln könnte.

App-Only mit `Mail.Send` als Anwendungsberechtigung erlaubt der Registrierung, als **jedes** Postfach der Organisation zu senden. Wer das eng ziehen will, beschränkt die Registrierung in Exchange Online über eine Anwendungszugriffsrichtlinie auf das eine Absenderpostfach. Das gehört mit der Microsoft-365-Administration abgestimmt.

Weg 1 — OAuth

E-Mail ☒

?

STANDARD

M365-OAUTH

Tenant ID

Redirect URI

/api/settings/oauth/redirect

Client ID

Client Secret

Empfänger

Betreff

Interval

VERBINDEN

1. App registrieren

Im Azure-Portal eine neue App-Registrierung anlegen, mit einem eindeutigen Namen. Als **Umleitungs-URI** wird die Adresse dieser FINN.ghost-Installation eingetragen, endend auf `/api/mail/oauth/redirect`:

`https://finn.kunde.de:8083/api/mail/oauth/redirect`

[Home](#) > [App-Registrierungen](#) >

Anwendung registrieren

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

FINN.ghost ✓

Unterstützte Kontotypen

Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- ☒ Nur Konten in diesem Organisationsverzeichnis (nur "DAKO-IT GmbH" – einzelner Mandant)
- ☐ Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig)
- ☐ Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)
- ☐ Nur persönliche Microsoft-Konten

[Entscheidungshilfe...](#)

Umleitungs-URI (optional)

Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.

Web

`https://192.168.2.35:8083/api/settings/oauth/redirect` ✓

Registrieren Sie eine App, an der Sie gerade arbeiten. Integrieren Sie Katalog-Apps und andere Apps von außerhalb Ihrer Organisation, indem Sie sie aus [Unternehmensanwendungen](#) hinzufügen.

Die Umleitungs-URI muss **zeichengenau** mit der Adresse übereinstimmen, unter der FINN.ghost erreichbar ist — samt Port. Weicht sie ab, bricht Microsoft die Anmeldung mit einer Meldung zur Redirect-URI ab. Das ist der häufigste Stolperstein.

In älteren Fassungen dieser Anleitung endete die Adresse auf `/api/settings/oauth/redirect`. Das gilt nicht mehr — der Pfad lautet `/api/mail/oauth/redirect`.

2. Clientschlüssel erstellen

Unter **Zertifikate & Geheimnisse** einen neuen Clientschlüssel anlegen und den **Wert** sofort notieren.

Suche

Haben Sie Feedback für uns?

Übersicht

Schnellstart

Integrations-Assistent

Diagnose und Problembehandlung

Verwalten

Branding und Eigenschaften

Authentifizierung

Zertifikate & Geheimnisse

Tokenkonfiguration

API-Berechtigungen

Eine API verfügbar machen

App-Rollen

Besitzer

Rollen und Administratoren

Manifest

Support + Problembehandlung

Haben Sie einen Moment, um uns Feedback zu geben? →

Anhand von Anmeldeinformationen können vertrauliche Anwendungen sich beim Authentifizierungsdienst identifizieren, wenn sie Token (über ein HTTPS-Schema) an einem adressierbaren Webspeicherort erhalten. Für eine höhere Sicherheitsstufe wird empfohlen, ein Zertifikat (anstelle eines Clientgeheimnisses) als Anmeldeinformation zu verwenden.

Anwendungsregistrierungszertifikate, Geheimnisse und Verbundanmeldeinformationen finden Sie auf den Registerkarten unten.

Zertifikate (0)

Geheime Clientschlüssel (1)

Verbundanmeldeinformationen (0)

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert	Geheime ID
ClientSecret	2.11.2025	mXq8Q~95Q1r-JVbb5D5G_0avETfKvPt...	b274505b-4e72-4328-a261-6a102e3897...

Der Wert wird nur einmal angezeigt. Wer ihn nicht notiert, muss einen neuen Schlüssel anlegen. Clientschlüssel laufen außerdem ab — das Ablaufdatum gehört notiert, sonst bleibt der Mailversand irgendwann ohne Vorwarnung stehen.

3. Berechtigungen setzen

Unter **API-Berechtigungen** zwei delegierte Berechtigungen von **Microsoft Graph** hinzufügen und die Zustimmung erteilen:

Berechtigung	Wofür
SMTP.Send	Mails über SMTP AUTH senden
offline_access	Zugriff behalten, ohne erneute Anmeldung

Suche

Aktualisieren

Haben Sie Feedback für uns?

Übersicht

Schnellstart

Integrations-Assistent

Diagnose und Problembehandlung

Verwalten

Branding und Eigenschaften

Authentifizierung

Zertifikate & Geheimnisse

Tokenkonfiguration

API-Berechtigungen

Eine API verfügbar machen

App-Rollen

Besitzer

Rollen und Administratoren

Manifest

Support + Problembehandlung

Die Administratoreinwilligung wurde für die angeforderten Berechtigungen erfolgreich erteilt.

Durch das Erteilen einer mandantenweiten Einwilligung können Berechtigungen widerrufen werden, die bereits mandantenweit für diese Anwendung erteilt wurden. Berechtigungen, die

In der Spalte "Administratoreinwilligung erforderlich." wird der Standardwert für eine Organisation angezeigt. Die Benutzereinwilligung kann jedoch pro Berechtigung, Benutzer oder App

Konfigurierte Berechtigungen

Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. [Weitere Informationen zu Berechtigungen und Zustimmung](#)

Berechtigung hinzufügen

Administratorzustimmung für "DAKO-IT GmbH" erteilen

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status
Microsoft Graph (3)				
offline_access	Delegiert	Zugriff auf Daten beibehalten, für die Sie Zugriff erteilt ha...	Nein	Gewährt für "DAKO-IT G..."
SMTP.Send	Delegiert	Send emails from mailboxes using SMTP AUTH.	Nein	Gewährt für "DAKO-IT G..."
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein	Gewährt für "DAKO-IT G..."

Um die genehmigten Berechtigungen für einzelne Apps sowie die Einwilligungseinstellungen Ihres Mandanten anzuzeigen und zu verwalten, testen Sie [Unternehmensanwendung](#).

`User.Read` steht dort in der Regel schon — es wird beim Anlegen der Registrierung mitgegeben und kann bleiben. Wichtig ist der grüne Haken bei *Status*: ohne erteilte Zustimmung greifen die Berechtigungen nicht.

4. Werte übertragen

Aus dem Reiter **Übersicht** der Registrierung:

Feld in Azure	Feld in FINN.ghost
Anwendungs-ID (Client)	Client ID
Verzeichnis-ID (Mandant)	Tenant ID
beim Anlegen hinterlegte Umleitungs-URI	Redirect URI
notierter Wert des Clientschlüssels	Client Secret

E-Mail

?

STANDARD

M365-OAUTH

Tenant ID

Redirect URI

https://192.168.2.35:8083

/api/settings/oauth/redirect

Client ID

6f54d764-cf17-4137-94eb-53537a0eff3d

Client Secret

mXq8Q~95Q1r-JVbb5D5G_0avETfkVdPtWx9HhaYG

Empfänger

info@dako-it.com

Betreff

FINN.ghost

Interval

10

VERBINDEN

5. Verbinden

Nach dem Klick auf **Verbinden** fragt Microsoft nach der Anmeldung. Danach steht die Verbindung, und in der Karte erscheint die Adresse des verbundenen Kontos.

Angemeldet wird das Postfach, aus dem gesendet wird. Es muss ein Postfach in derselben Organisation sein.

Weg 2 — App-Only

E-Mail 

?

STANDARD M365-OAUTH **M365-APP-ONLY**

Tenant ID

Absender-E-Mail

Client ID

Client Secret

Empfänger

Betreff

Interval

VERBINDEN

1. App registrieren

Wie oben eine neue App-Registrierung mit eindeutigem Namen. Eine Umleitungs-URI wird hier **nicht** gebraucht.

Anwendung registrieren ...

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

Unterstützte Kontotypen

Kontotypen auswählen, die diese Anwendung verwenden oder auf diese API zugreifen können

[Entscheidungshilfe](#)

Umleitungs-URI (optional)

Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.

Plattform auswählen 

Beispiel: <https://example.com/auth>

Registrieren Sie eine App, an der Sie gerade arbeiten. Integrieren Sie Katalog-Apps und andere Apps von außerhalb Ihrer Organisation, indem Sie sie aus [Unternehmensanwendungen](#) hinzufügen.

2. Clientschlüssel erstellen

Unter **Zertifikate & Geheimnisse**, Wert notieren.

Zertifikate (0)

Geheime Clientschlüssel (0)

Verbundanmeldeinformationen (0)

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

+

 Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert ⓘ	Geheime ID
Für diese Anwendung wurden keine Clientgeheimnisse erstellt.			

3. Berechtigung setzen

Unter **API-Berechtigungen** eine **Anwendungsberechtigung** von Microsoft Graph hinzufügen und die Zustimmung erteilen:

Berechtigung			Typ	
Mail.Send			Anwendung	

Alle der benötigten Berechtigungen muss die Berechtigungen erteilen, die die Anwendung benötigt. Mehrere Berechtigungen erfordern eine Zustimmung.

+

 Berechtigung hinzufügen

✓

 Administratorzustimmung für "DAKO-IT GmbH" erteilen

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status
Microsoft Graph (2)				
Mail.Send	Anwendung	Send mail as any user	Ja	⚠ Für "DAKO-IT GmbH" ni...
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein	

Anwendungsberechtigungen brauchen immer die **Administratorzustimmung**. Ohne sie schlägt der Versand mit einer Rechtemeldung fehl, obwohl alle Werte richtig eingetragen sind.

4. Werte übertragen

Feld in Azure	Feld in FINN.ghost
Anwendungs-ID (Client)	Client ID
Verzeichnis-ID (Mandant)	Tenant ID
Wert des Clientschlüssels	Client Secret
—	Absender-E-Mail

STANDARD M365-OAUTH **M365-APP-ONLY**Tenant ID
4232457f-dc03-493d-8193-ae7ebb12913eAbsender-E-Mail
l.ruhle@dako-it.comClient ID
865e8837-4d64-41e9-a6b4-839a69a4c495Client Secret
*****Empfänger
l.ruhle@dako-it.comBetreff
FINN.ghostIntervall
0

TRENKEN

SPEICHERN

Die **Absender-E-Mail** ist das Postfach, aus dem gesendet wird.

Nach dem Speichern verschickt FINN.ghost eine Testmail an die eingetragenen Empfänger und bestätigt das in der Karte. Kommt sie nicht an, fehlt meist die Administratorzustimmung.

Über **Trennen** wird die Verbindung wieder gelöst.

Wenn der Versand nicht geht

Meldung oder Symptom	Ursache
Fehler zur Redirect-URI beim Verbinden	Umleitungs-URI weicht ab
Anmeldung geht, Versand scheitert	Berechtigung fehlt oder ohne Zustimmung
lief monatelang, jetzt nicht mehr	Clientschlüssel abgelaufen
App-Only meldet fehlende Rechte	Administratorzustimmung nicht erteilt
Absender wird abgelehnt	Postfach gehört nicht zur Organisation

Die Antwort von Microsoft steht im Protokoll. Siehe [Log Informationen](#).

Nächster Schritt

[EU-Auslands-Kontengruppen](#)

EU-Auslands-Kontengruppen

Beim Import von Bestellungen aus einem Shop entscheidet die **Kontengruppe** des Kunden, mit welchen Erlöskonten gebucht wird. Für Lieferungen in andere EU-Länder ist das je Land unterschiedlich — das ist das **OSS-Verfahren**.

Land (ISO)	Kontengruppe ohne VAT	Kontengruppe mit VAT
DE	Inlandskunde (Deutschland)	Inlandskunde (Deutschland)
default	Drittland	Drittland

Was eingestellt wird

Je Land eine Zeile:

Spalte	Inhalt
Land (ISO)	Länderkennzeichen mit zwei Zeichen, etwa AT
Kontengruppe ohne VAT	für Kunden ohne gültige Umsatzsteuer-Identnummer
Kontengruppe mit VAT	für Kunden mit gültiger Umsatzsteuer-Identnummer

Hinzugefügt wird ein Land über das Feld **Land hinzufügen (ISO2)**; die Kontengruppen kommen aus der Auswahl der im Mandanten vorhandenen Gruppen.

Es gibt zusätzlich eine **Vorgabe** für alle Länder ohne eigene Zeile. Damit genügt es, die Länder einzutragen, die abweichend behandelt werden.

Welche Adresse zählt

Maßgeblich ist das Land der **Lieferadresse** der Bestellung, nicht das der Rechnungsadresse.

Das entspricht dem OSS-Verfahren: Besteuert wird dort, wo die Ware ankommt.

Wann es wirkt

Beim Anlegen oder Aktualisieren eines Kunden im Rahmen des Bestellimports. Bestehende Kunden und bereits importierte Bestellungen werden nicht nachträglich geändert.

Diese Einstellung gehört **vor** dem ersten Bestellimport gesetzt. Sonst liegen die ersten Bestellungen mit der falschen Kontengruppe im Mandanten und müssen von Hand korrigiert werden.

Wer das entscheidet

Welche Kontengruppe für welches Land richtig ist, ist eine steuerliche Frage. Sie gehört mit der Buchhaltung oder dem Steuerberater geklärt — nicht in der Schnittstelle geraten.

Zurück zur Übersicht

[SelectLine - Einstellungen](#)