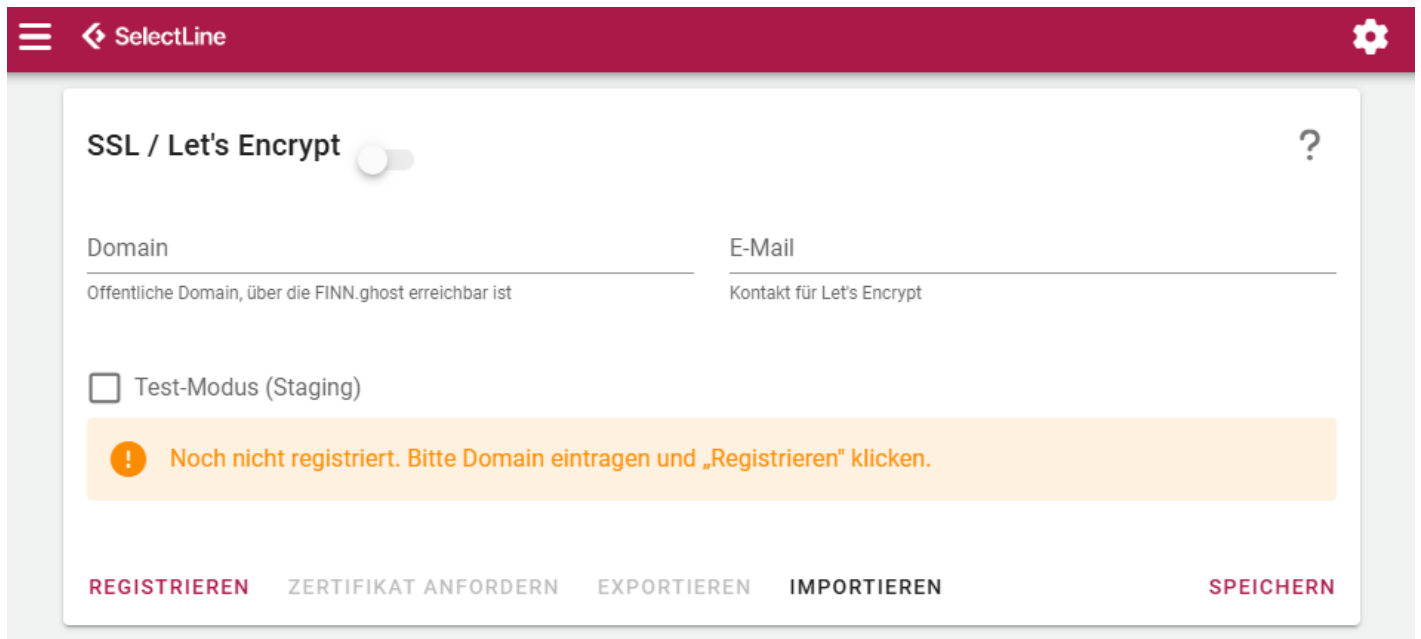


SSL mit Let's Encrypt

FINN.ghost kann sein Zertifikat selbst bei Let's Encrypt beantragen und automatisch erneuern. Das ist der empfohlene Weg — er ersetzt das Erstellen und Verteilen eigener Zertifikate.



The screenshot shows the 'SSL / Let's Encrypt' configuration page in the SelectLine control panel. At the top, there's a header bar with the SelectLine logo and a settings gear icon. Below the header, the page title 'SSL / Let's Encrypt' is followed by a toggle switch (currently off) and a help icon (?). The main form area contains two input fields: 'Domain' with a placeholder 'Öffentliche Domain, über die FINN.ghost erreichbar ist' and 'E-Mail' with a placeholder 'Kontakt für Let's Encrypt'. Below these fields is a checkbox labeled 'Test-Modus (Staging)'. A prominent orange warning box with an exclamation mark icon contains the text: 'Noch nicht registriert. Bitte Domain eintragen und „Registrieren“ klicken.' At the bottom of the form, there are five buttons: 'REGISTRIEREN' (highlighted in red), 'ZERTIFIKAT ANFORDERN', 'EXPORTIEREN', 'IMPORTIEREN', and 'SPEICHERN' (highlighted in red).

Warum das die einfachere Lösung ist

	eigenes Zertifikat	Let's Encrypt
Am Arbeitsplatz	Stammzertifikat installieren, je Rechner	nichts zu tun
Gültigkeit	von Hand erneuern	erneuert sich selbst
Vom Browser anerkannt	erst nach Installation	sofort
Voraussetzung	keine	eine öffentliche Domain

Der entscheidende Unterschied liegt beim Anwender: Ein selbst erstelltes Zertifikat muss auf jedem Rechner installiert werden, der die Oberfläche aufruft — und auf jedem neuen wieder. Mit Let's Encrypt entfällt das vollständig.

Voraussetzungen

Lizenzmodul SSL	ohne dieses Modul lässt sich der Schalter nicht setzen
Eine Domain	etwa <code>finn.kunde.de</code>
Zugriff auf das DNS der Domain	für einen einmaligen CNAME-Eintrag
Ausgehende Internetverbindung	für den Abruf des Zertifikats

FINN.ghost muss dafür **nicht** aus dem Internet erreichbar sein. Der Nachweis läuft über einen DNS-Eintrag, nicht über eine eingehende Verbindung — es muss also kein Port ins Internet geöffnet werden.

Einrichten

1. Domain und E-Mail eintragen

Feld	Inhalt
Domain	die öffentliche Domain, unter der FINN.ghost erreichbar sein soll
E-Mail	Kontaktadresse für Let's Encrypt

Die Domain muss auf die Installation zeigen, damit der Aufruf im Browser funktioniert — für die Ausstellung des Zertifikats selbst genügt der CNAME aus Schritt 2.

2. Registrieren

Die Schaltfläche **Registrieren** meldet die Installation einmalig an. Danach zeigt die Karte einen **CNAME-Eintrag**, der im öffentlichen DNS der Domain angelegt werden muss:

```
_acme-challenge.finn.kunde.de. CNAME <von FINN.ghost angezeigter Wert>.
```

Dieser Eintrag ist der Kern des Verfahrens: Über ihn weist FINN.ghost bei jeder Ausstellung nach, dass es zur Domain gehört. Er muss **dauerhaft** bestehen bleiben — wird er gelöscht, scheitert die nächste Erneuerung.

Angelegt wird er einmal. Danach ist am DNS nichts mehr zu tun, auch nicht bei jeder Erneuerung.

3. Zertifikat anfordern

Zertifikat anfordern holt das Zertifikat. Anschließend startet die Anwendung neu, damit der Webserver es verwendet.

Danach zeigt die Karte, bis wann es gültig ist und wie viele Tage bleiben.

Der Vorgang dauert bis zu zwei Minuten — der DNS-Eintrag muss sich erst verbreiten. Solange bitte nichts erneut anklicken.

Test-Modus

Der Haken **Test-Modus (Staging)** arbeitet gegen die Übungsumgebung von Let's Encrypt.

Sinnvoll beim Einrichten: Let's Encrypt begrenzt die Zahl der Ausstellungen je Domain und Woche. In der Übungsumgebung gilt diese Grenze nicht — Fehlversuche kosten dort nichts.

Ein Zertifikat aus dem Test-Modus wird von **keinem** Browser anerkannt. Nach dem erfolgreichen Test den Haken entfernen und das Zertifikat erneut anfordern.

Mehrere Installationen, eine Domain

Exportieren erzeugt einen Code, der auf einer weiteren FINN.ghost-Installation unter **Importieren** eingefügt wird. Die zweite Installation übernimmt damit Domain und Zugang, holt sich ihr Zertifikat selbst und startet neu.

Damit braucht der CNAME-Eintrag nur einmal angelegt zu werden, auch wenn mehrere Installationen dieselbe Domain nutzen.

Der Exportcode enthält den Zugang zur Zertifikatsverwaltung dieser Domain. Er gehört nicht in eine E-Mail an Dritte und nicht in ein Ticketsystem.

Erneuerung

Läuft von selbst:

Prüfung	alle 12 Stunden, Aufgabe <i>SSL Zertifikat erneuern</i>
Erneuert wird	wenn weniger als 30 Tage Restlaufzeit bleiben
Zusätzlich	bei jedem Start der Anwendung

Nach einer Erneuerung startet die Anwendung neu, damit das neue Zertifikat verwendet wird. Das dauert wenige Sekunden und fällt im Betrieb kaum auf — laufende Übertragungen brechen dabei aber ab.

Siehe [Zeitsteuerung der Module \(allgemein\)](#).

Wo die Dateien liegen

Im Installationsordner unter `data\ssl`:

Datei	Inhalt
<code>server.cert</code>	das Zertifikat
<code>server.key</code>	der zugehörige Schlüssel
<code>acme-account.key</code>	der Zugang zu Let's Encrypt

Diese Dateien gehören in die Datensicherung des Servers — und ansonsten in keine fremden Hände.

Wenn es nicht klappt

Symptom	Ursache
Schalter lässt sich nicht setzen	Lizenzmodul SSL fehlt

Symptom	Ursache
Meldung, es sei nicht vollständig konfiguriert	Domain, E-Mail oder Registrierung fehlt
Ausstellung bricht ab	CNAME nicht angelegt oder noch nicht verbreitet
Browser warnt weiter	Test-Modus noch aktiv, oder die Domain wird nicht aufgerufen
lief, jetzt abgelaufen	CNAME wurde entfernt, oder keine Internetverbindung

Wird die Oberfläche über `localhost` oder eine IP-Adresse aufgerufen, warnt der Browser trotz gültigem Zertifikat — es gilt für die Domain. Der Aufruf muss über die Domain gehen.

Die Meldungen stehen im Protokoll. Siehe [Log Informationen](#).

Nächster Schritt

[Zertifikat einrichten](#)

Created 2026-09-02 07:21:28 UTC by API
Updated 2026-09-02 10:39:44 UTC by API