ADMINISTRATORANLEITUNG

HTTPS aktivieren

Zertifikate einrichten und automatisch erneuern
.snap Stationär unter Windows

Eine verschlüsselte Verbindung.
Ein Zertifikat für Frontend und Backend.

Diese Anleitung führt Systemadministratoren von der Netzwerkvorbereitung bis zur Prüfung der HTTPS-Verbindungen. Sie können ein vorhandenes Zertifikat importieren oder die Ausstellung und Erneuerung über eine ACME-Zertifizierungsstelle einrichten.

> **Zuerst das passende Verfahren wählen**
> **Nur im Kundennetz erreichbar:** vorhandenes Zertifikat importieren oder interne ACME-CA verwenden.
> **Öffentliche ACME-CA:** der HTTP-Prüfpfad muss aus dem Internet über Port 80 erreichbar sein.

Ihr Weg durch die Einrichtung

Voraussetzungen und Zertifikatsverfahren 02

Netzwerk, DNS und benötigte Ports 03

Windows-Firewall und vorgeschaltete Firewalls 04

Variante A: vorhandenes Zertifikat importieren 05

Variante B: ACME-Zugang konfigurieren 06

ACME einrichten und erstmals ausstellen 07

Server starten, Clients umstellen und Betrieb prüfen 08

Fehler erkennen und gezielt beheben 09

HTTPS deaktivieren und weitere Informationen 10

Alle Servernamen, E-Mail-Adressen und Anwendungsports in den Beispielen sind Musterwerte. Verwenden Sie die Werte Ihrer eigenen Installation.

01 / VORBEREITUNG

Voraussetzungen festlegen

Planen Sie für die erstmalige Aktivierung ein Wartungsfenster ein. Die Einrichtung erfolgt auf dem Windows-Server, auf dem Frontend und Backend installiert sind.

Begriffe: CA steht für Zertifizierungsstelle. ACME ist ein Verfahren zur automatischen Ausstellung und Erneuerung von Zertifikaten. PEM bezeichnet das hier verwendete textbasierte Dateiformat.

Verfahren	Was Sie benötigen	Zusätzliche ACME-Freigabe
Zertifikatsimport	Serverzertifikat mit Zwischenzertifikaten und passender privater Schlüssel als PEM.	Keine. Die Erneuerung erfolgt durch Ihre IT und erneuten Import.
Interne ACME-CA	Interner ACME-Endpunkt, erreichbarer Prüfpfad und bei Bedarf CA-Zertifikat / EAB-Daten.	CA erreicht Server auf TCP 80; Server erreicht ACME-Endpunkt.
Öffentliche ACME-CA	Öffentlicher DNS-Name, öffentlicher HTTP-Prüfpfad und ACME-Konfiguration.	Eingehend TCP 80; ausgehend HTTPS zur CA, üblicherweise TCP 443.

Vor Beginn prüfen

- Aktuelle .snap-Installation vollständig installiert; Admin Tool mit Administratorrechten auf dem Installationsserver starten.
- Frontend- und Backend-Port im Admin Tool notieren. Für die Ersteinrichtung beide Server **und ihre Windows-Dienste stoppen**.
- Einen stabilen DNS-Namen festlegen. Dieser muss im Zertifikat als gültiger Servername enthalten sein; alle Clients verwenden diesen Namen.
- Die Windows-Dienste laufen unter **LocalSystem / SYSTEM**. Abweichende Dienstkonten vorab mit dem zuständigen Support abstimmen.
- Systemzeit synchronisieren, Administrationszugang sicherstellen und die Installation gemäß Ihrem Sicherungskonzept sichern.

> **Durchgängiges Beispiel**
> **Servername:** stationaer.kunde.de
> **Frontend:** https://stationaer.kunde.de:8091/
> **Backend:** https://stationaer.kunde.de:8090/
> 8091 und 8090 sind Beispielports, keine Vorgabe. Der Zertifikatsname enthält weder Protokoll noch Port.

02 / NETZWERK

DNS und Ports vorbereiten

HTTPS verwendet die bereits im Admin Tool konfigurierten Anwendungsports. Ein Wechsel auf Port 443 ist dafür nicht erforderlich.

Verbindung	Port / Richtung am Server	Freigabe und Zweck
Clients zum Frontend	TCP, eingehend z. B. **8091**	Nur aus den vorgesehenen Clientnetzen / VPN. Liefert die Benutzeroberfläche.
Clients zum Backend	TCP, eingehend z. B. **8090**	Nur aus den vorgesehenen Clientnetzen / VPN. Liefert die Anwendungs-API.
ACME-CA zum Prüfserver	TCP **80**, eingehend nur bei ACME	Öffentliche CA: aus dem Internet erreichbar. Interne CA: Zugriff aus deren Validierungsnetz.
Server zur ACME-CA	HTTPS, ausgehend üblicherweise TCP **443**	ACME-Verzeichnis und die dort angegebenen Dienst-Endpunkte; bei interner CA ggf. abweichender Port.
Server / Clients zum DNS	Bestehender DNS-Zugang typisch UDP / TCP 53	Namensauflösung über die vorgesehenen DNS-Server. Keine öffentliche DNS-Serverfreigabe am .snap-Server nötig.

Bei öffentlicher ACME-CA zusätzlich

- Öffentlichen DNS-Eintrag auf die öffentliche Server- oder Firewall-Adresse setzen. Bei NAT: extern TCP 80 auf **TCP 80 des Installationsservers** weiterleiten.
- Der Pfad `/.well-known/acme-challenge/` muss ohne Anmeldung, VPN-Zwang oder vorgeschaltete Zugriffssperre erreichbar sein. [1]
- Alle veröffentlichten A- und AAAA-Einträge müssen auf einen erreichbaren Prüfpfad zeigen. Fehlerhafte oder nicht bediente Einträge korrigieren.
- Port 80 muss lokal frei sein. Das Admin Tool startet dort während der Ausstellung einen eigenen temporären Prüfserver; z. B. IIS darf ihn nicht belegen.

> **Für jede Erneuerung erforderlich**
> Die ACME-Netzfreigaben und NAT-Zuordnung dauerhaft vorhalten. Außerhalb einer Prüfung muss auf Port 80 kein Dienst antworten. Die Anwendungsports müssen für die Zertifikatsprüfung nicht öffentlich erreichbar sein. DNS-01 und TLS-ALPN-01 werden durch diese Funktion derzeit nicht unterstützt.

03 / FIREWALL

Portfreigaben einrichten

Freigaben müssen auf allen beteiligten Ebenen passen: Windows-Firewall, Netzwerk-Firewall, Router / NAT und gegebenenfalls Cloud-Netzwerkregeln.

01 **Windows-Firewall öffnen**
Auf dem Installationsserver **Windows Defender Firewall mit erweiterter Sicherheit** öffnen (Startmenü oder `wf.msc`).

02 **Anwendungsports freigeben**
Unter **Eingehende Regeln** → **Neue Regel** → **Port** → **TCP** die beiden konfigurierten Ports angeben. Verbindung zulassen und passende Netzwerkprofile wählen. In den Regeleigenschaften unter **Bereich** die Remote-IP-Adressen auf Ihre Clientnetze / VPN beschränken.

03 **ACME-Port nur bei ACME ergänzen**
Separate eingehende TCP-Regel für lokalen Port **80** erstellen. Öffentliche CA: Remote-Adressen nicht auf das Kundennetz begrenzen. Let's Encrypt veröffentlicht keine feste Liste von Validierungs-IP-Adressen. [2] Interne CA: auf die von Ihrer IT benannten Validierungsadressen begrenzen.

Alternative: PowerShell als Administrator [4]

Beispiel für ein Clientnetz **10.20.0.0/16** und die Ports **8090 / 8091**. Diese Werte vor der Ausführung anpassen. Die Befehle legen neue Regeln an.

```
# Nur die vorgesehenen Clientnetze freigeben.
New-NetFirewallRule -DisplayName 'snap HTTPS Clients' `
  -Direction Inbound -Action Allow -Protocol TCP `
  -LocalPort 8090,8091 -RemoteAddress '10.20.0.0/16' `
  -Profile Any

# Nur bei ACME mit einer öffentlichen CA erforderlich.
New-NetFirewallRule -DisplayName 'snap ACME HTTP-01' `
  -Direction Inbound -Action Allow -Protocol TCP `
  -LocalPort 80 -RemoteAddress Any -Profile Any
```

Vorgeschaltete Regeln nicht vergessen
Dieselben Verbindungen gegebenenfalls in Azure-NSGs oder anderen Cloud-/Netzwerk-Firewalls zulassen und die NAT-Weiterleitung einrichten. Bei eingeschränktem Ausgangsverkehr HTTPS zur CA erlauben. Gruppenrichtlinien können lokale Windows-Regeln übersteuern. Eine globale Abschaltung der Firewall ist nicht erforderlich.

04 / VARIANTE A

Vorhandenes Zertifikat importieren

Verwenden Sie diesen Weg für ein von Ihrer IT oder einem Zertifikatsanbieter bereitgestelltes Zertifikat. Eine ACME-Konfiguration ist dafür nicht erforderlich.



Abbildung 1: Servername und Zertifikatsimport im Bereich „HTTPS-Zertifikate" (Bildausschnitt).

01 **Server stoppen und Servernamen eingeben**
Backend, Frontend und deren Windows-Dienste stoppen. Im Admin Tool **HTTPS-Zertifikate** öffnen. Den Namen ohne `https://` und ohne Port eintragen, z. B. stationaer.kunde.de.

02 **Zertifikat und privaten Schlüssel auswählen**
Bei **Zertifikat und Zwischenzertifikate** die PEM-Kette auswählen: zuerst Serverzertifikat, danach Zwischenzertifikate in Ausstellerreihenfolge. Darunter den passenden **unverschlüsselten privaten PEM-Schlüssel** auswählen.

03 **Übernehmen und fortfahren**
Zertifikat übernehmen anklicken und die Erfolgsmeldung abwarten. Anschließend mit Seite 8 fortfahren.

Dateiformat und Speicherung
PFX / PKCS#12, DER-Dateien und verschlüsselte Schlüssel können nicht direkt importiert werden. Die Dateiendung allein sagt nichts über das Format aus. Lassen Sie die erforderlichen PEM-Dateien von Ihrer IT bereitstellen. Das Admin Tool speichert die übernommenen Daten unter `C:\Users\All Users\euregon\tls\`. Originaldateien werden für den Betrieb nicht mehr benötigt; Schlüssel gemäß Ihrem Sicherungskonzept schützen.

05 / VARIANTE B

ACME-Zugang konfigurieren

Bei ACME übernimmt das Admin Tool die Ausstellung und spätere Erneuerung. Ein vorheriger manueller Zertifikatsimport ist nicht nötig. Beide Server und ihre Dienste bleiben zunächst gestoppt.



Abbildung 2: ACME-Adresse, Kontakt und optionale Vertrauens- / Kontobindungsdaten (Bildausschnitt).

Feld	Was Sie eintragen
Servername	Vollständiger DNS-Name oben im Dialog; für die aktuelle ACME-Funktion ein einzelner Name ohne Wildcard.
ACME-Verzeichnisadresse	HTTPS-Verzeichnisadresse Ihrer CA. Beispiele stehen unten. Das Feld hat keinen vorausgewählten Anbieter.
Kontakt-E-Mail	Betreute administrative E-Mail-Adresse Ihrer Organisation.
CA-Zertifikat für interne ACME-Verbindung	Nur bei internem ACME-Endpunkt mit eigener CA: CA-Zertifikat als PEM. Für Let's Encrypt / ZeroSSL leer lassen.
Kontobindung: Schlüssel-ID und HMAC-Schlüssel	Nur wenn die CA EAB verlangt. Beide Werte gemeinsam eintragen. Bei ZeroSSL sind diese Daten erforderlich. [3]

Beispieladressen
Let's Encrypt: https://acme-v02.api.letsencrypt.org/directory
ZeroSSL: https://acme.zerossl.com/v2/DV90

06 / ACME AKTIVIEREN

Einrichten und erstmals ausstellen

Vor dem Start müssen DNS, Portfreigaben und ACME-Zugang vollständig vorbereitet sein. Für die erstmalige HTTPS-Aktivierung bleiben Frontend, Backend und deren Dienste gestoppt.

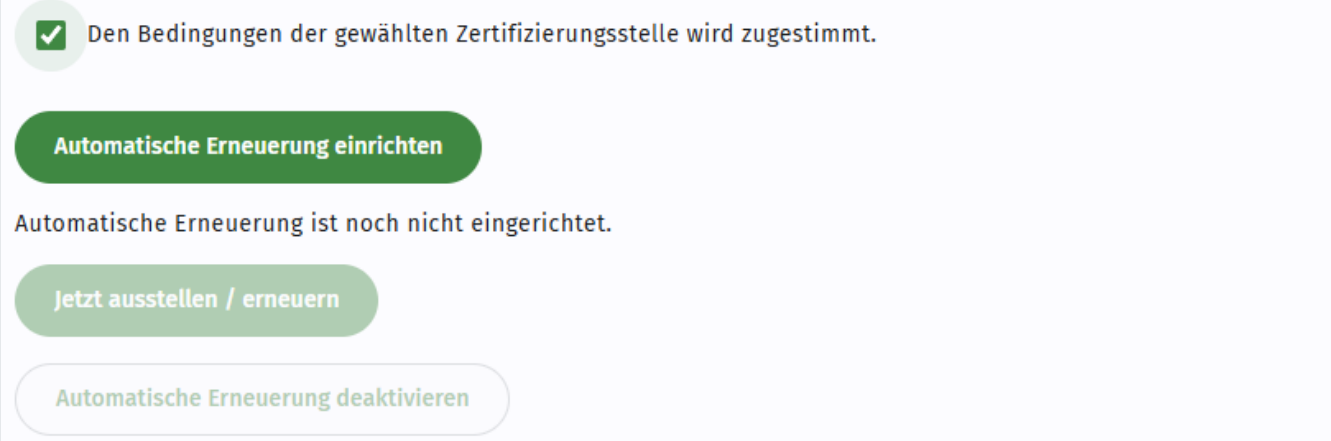


Abbildung 3: Zustimmung und ACME-Aktionen. „Jetzt ausstellen / erneuern“ wird nach der Einrichtung freigegeben.

01 **Bedingungen bestätigen**
Die Bedingungen der gewählten Zertifizierungsstelle prüfen und das Kontrollkästchen **Den Bedingungen der gewählten Zertifizierungsstelle wird zugestimmt.** aktivieren.

02 **Automatische Erneuerung einrichten**
Die gleichnamige Schaltfläche anklicken. Dadurch werden Konfiguration und Windows-Aufgabe gespeichert. Das Einrichten allein ist noch keine Bestätigung, dass ein Zertifikat ausgestellt wurde.

03 **Erste Ausstellung starten**
Jetzt ausstellen / erneuern anklicken. Die Fortschrittsanzeige bis zur Erfolgs- oder Fehlermeldung abwarten. Währenddessen keine Server starten und keine weitere Ausstellung auslösen.

04 **Erfolg kontrollieren**
Bei Erfolg sind Zertifikat und privater Schlüssel für beide Server übernommen. Der Dialog zeigt Servernamen und Gültigkeitsende. Danach mit Seite 8 fortfahren.

EAB und internes CA-Vertrauen
Bei ZeroSSL unter „Developer“ die **EAB Credentials for ACME Clients** erzeugen: **EAB KID → Schlüssel-ID**, **EAB HMAC Key → HMAC-Schlüssel**. Der REST-API-Key gehört nicht in diese Felder. [3]
Das optionale CA-Zertifikat schafft Vertrauen ausschließlich für **Admin Tool → interner ACME-Server**. Es verteilt kein Vertrauen an Browser oder andere Clients.

07 / ABSCHLUSS UND BETRIEB

HTTPS prüfen und überwachen

Nach erfolgreichem Import oder erfolgreicher ACME-Ausstellung werden dieselben Anwendungsports mit HTTPS betrieben. Eine automatische HTTP-Weiterleitung ist dafür nicht vorausgesetzt.

01 **Backend und Frontend starten**
Die zuvor gestoppten Windows-Dienste bzw. Server über das Admin Tool wieder starten und deren Status prüfen.

02 **Alle Client-Adressen umstellen**
In den eingesetzten Clients Frontend- und Backend-Adresse auf **https://** ändern. DNS-Name und konfigurierte Ports verwenden. Bestehende Integrationen mit fest eingetragenen HTTP-Adressen ebenfalls prüfen.

```
Frontend: https://stationaer.kunde.de:8091/
Backend:  https://stationaer.kunde.de:8090/

# Optionale Erreichbarkeitsprüfung mit TLS-Prüfung:
curl.exe https://stationaer.kunde.de:8091/frontendversion
curl.exe https://stationaer.kunde.de:8090/api/v1/version/server
```

03 **Vom tatsächlichen Arbeitsplatz aus prüfen**
Frontend öffnen, anmelden und eine normale Anwendungsfunktion ausführen. In den Zertifikatsdetails Servername, Aussteller und Gültigkeit für beide Ports kontrollieren. Zertifikatswarnungen nicht übergehen und die TLS-Prüfung nicht abschalten.

> **Bei einer internen Zertifizierungsstelle**
> Die vertrauenswürdige Stamm-CA muss auf allen vorgesehenen Endgeräten vorhanden sein. Ihre IT verteilt sie nach den Vorgaben für Windows, Browser und gegebenenfalls Mobilgeräte. Die konkrete Vertrauenskonfiguration ist vom eingesetzten Client abhängig.

Automatische Erneuerung im Betrieb

In der Windows-Aufgabenplanung die Aufgabe **StationaerCertificateRenewal** prüfen: aktiviert, Ausführung als **SYSTEM**, Wiederholung alle **5 Minuten**. Das Admin Tool muss nicht geöffnet sein.

Eine CA-Anfrage erfolgt ab Beginn des **letzten Drittels der tatsächlichen Zertifikatslaufzeit**; bei 90 Tagen also etwa 30 Tage vor Ablauf. Bei einem Fehler folgt ein weiterer Versuch beim nächsten Lauf. Bereits aktives HTTPS kann im laufenden Betrieb erneuert werden; Frontend und Backend laden das Zertifikat neu.

Gültigkeitsende und letzten Erneuerungsstatus regelmäßig kontrollieren. Bei rein manuellem Import muss Ihre IT rechtzeitig ein neues Zertifikat bereitstellen und importieren.

08 / FEHLERBEHEBUNG

Gezielt prüfen statt erneut bestellen

Prüfen Sie zuerst den angezeigten Schritt. Wiederholtes Klicken auf „Jetzt ausstellen / erneuern" kann zusätzliche Zertifikatsbestellungen auslösen und Anfragelimits erreichen.

Symptom	Prüfung / Maßnahme
Feld oder Schaltfläche ist deaktiviert	Mauszeiger auf das Element bewegen: Der Tooltip nennt den Grund. Für Konfigurationsänderungen beide Server und Dienste stoppen; laufende Vorgänge / Dateieinlesen abwarten.
Port 80 bereits belegt	Belegenden Dienst ermitteln, z. B. IIS. ACME benötigt den lokalen Port 80; eine externe Freigabe allein genügt nicht.
HTTP-01-Domainprüfung scheitert	Öffentlichen DNS-Eintrag, alle A-/AAAA-Ziele, NAT, Windows-Firewall und Netzwerk-/Cloud-Firewall prüfen. Zugriff muss von der CA aus ohne VPN und Anmeldung möglich sein.
Timeout, DNS- oder TLS-Fehler zur CA	Ausgehende Erreichbarkeit der ACME-Endpunkte, DNS, Proxy-/Firewall-Vorgaben und Systemzeit prüfen. Für interne CA gegebenenfalls das richtige CA-Zertifikat hinterlegen.
Kontobindung wird abgelehnt	CA-Adresse sowie EAB KID und HMAC-Schlüssel gemeinsam prüfen. Nicht den REST-API-Key verwenden. Die konkrete CA-Fehlerbeschreibung im Log auswerten.
Zertifikatswarnung im Client	Richtigen DNS-Namen, Gültigkeit, vollständige Zwischenzertifikatskette und Vertrauen zur ausstellenden Stamm-CA prüfen. Eine IP-Adresse ersetzt keinen DNS-Namen im Zertifikat.
Anfragelimit erreicht	Weitere Bestellungen vermeiden; ggf. „Automatische Erneuerung deaktivieren". Hinweise / Retry-After der CA im Log beachten. Wiederholte Tests nur in getrennter Staging-Umgebung. [5]
Erneuerung / Übernahme fehlgeschlagen	Status beider Server, Windows-Dienstkonten, Aufgabenplanung und Log prüfen. Bei unklarem aktivem Zertifikat oder Rollback-Fehler Betrieb mit dem zuständigen Support abstimmen.

Diese Informationen für die Fehleranalyse bereithalten
Zeitpunkt, angezeigten ACME-Schritt, Servername, CA-Adresse und die passenden Zeilen mit **[ACME] Diagnose:** aus **admin.tool.log**. Die Logdatei liegt im installierten Ordner **admintool**, beispielsweise unter `C:\Program Files (x86)\euregon\stationaer\admintool\`. Keine privaten Schlüssel, EAB-Geheimnisse oder Passwörter weitergeben.

09 / VERWALTUNG UND REFERENZ

Erneuerung oder HTTPS abschalten

Die beiden Aktionen haben unterschiedliche Auswirkungen. Für eine Rückkehr zu HTTP sind keine manuellen Dateilöschungen erforderlich.

Aktion im Admin Tool	Auswirkung
Automatische Erneuerung deaktivieren	Entfernt die automatische Erneuerung. Das aktive Zertifikat bleibt erhalten und HTTPS bleibt aktiv. Rechtzeitige Erneuerung anschließend selbst organisieren.
HTTPS deaktivieren	Entfernt die aktive HTTPS-Konfiguration samt Zertifikat und privatem Schlüssel sowie die automatische Erneuerung. Beide Server verwenden nach dem Start wieder HTTP.

Zu HTTP zurückkehren

Beide Server und deren Windows-Dienste stoppen. Unter **HTTPS-Zertifikate → Zu HTTP zurückkehren** auf **HTTPS deaktivieren** klicken und den Dialog bestätigen. Erfolgsmeldung abwarten, Server wieder starten und alle betroffenen Client-Adressen auf **http://** zurückstellen. Die Ports bleiben gleich. HTTP überträgt Anwendungsdaten unverschlüsselt.

Browser können zuvor gespeicherte HSTS-Vorgaben weiterhin anwenden. Bei automatischer Umleitung auf HTTPS die Browserrichtlinien mit Ihrer IT prüfen; das Abschalten am Server entfernt keine gespeicherten Regeln auf Endgeräten.

Abschlusskontrolle

Für den produktiven HTTPS-Betrieb dokumentieren: verwendeter DNS-Name, beide Anwendungsports, Zertifikatsaussteller und Gültigkeit, verantwortliche Kontaktstelle, Firewall-/NAT-Regeln sowie bei ACME den Status der Windows-Aufgabe. Den Zugriff über alle tatsächlich eingesetzten Clients prüfen.

Weiterführende Dokumentation

[1] Let’s Encrypt: HTTP-01 und weitere Prüfverfahren
https://letsencrypt.org/docs/challenge-types/

[2] Let’s Encrypt: Integrationshinweise / Firewall
https://letsencrypt.org/docs/integration-guide/

[3] ZeroSSL: ACME und EAB-Kontobindung
https://zerossl.com/documentation/acme

[4] Microsoft: New-NetFirewallRule
https://learn.microsoft.com/powershell/module/netsecurity/new-netfirewallrule

[5] Let’s Encrypt: Staging für Tests
https://letsencrypt.org/docs/staging-environment/

Staging-Zertifikate sind für Tests bestimmt und werden von üblichen Browsern nicht als vertrauenswürdig akzeptiert. Für den Produktivbetrieb die Produktions-CA verwenden. [5]
Dokumentationsstand: 29.10.2026. Screenshots zeigen Beispielwerte; Darstellung und Beschriftung können je nach installiertem Softwarestand abweichen.