



6. Mai 2026

Automatische Erneuerung von SSL/TLS-Zertifikaten mit Certbot und DigiCert

Schritt-für-Schritt-Anleitung zur Einrichtung der automatischen Zertifikatserneuerung.
Alle Platzhalter in <> müssen durch Ihre eigenen Werte ersetzt werden.

Version: 1.5

Betriebssystem: Linux (SUSE)

Webserver: Apache

Inhaltsverzeichnis

1. Zweck dieser Anleitung	3
Mit dieser Anleitung lernen Sie:	3
2. Technische Voraussetzungen	3
2.1 Certbot installieren	4
SUSE Linux:	4
Debian / Ubuntu:	4
RHEL / CentOS / Rocky Linux:	4
2.2 Apache-Status prüfen	5
3. DigiCert-Zugangsdaten (EAB)	6
4. Netzwerkkonfiguration (Proxy)	7
4.1 Proxy temporär setzen	7
4.2 Proxy dauerhaft konfigurieren (empfohlen)	7
Schritt 1 – Datei öffnen:	7
Schritt 3 – Zeilen am Ende der Datei einfügen:	7
5. Erstmalige Zertifikatserneuerung mit Certbot	8
5.1 Certbot-Befehl ausführen	8
6. Webserver neu starten	9
7. Funktionsprüfung	9
7.1 Browser-Test	9
7.2 Technischer Test	9
8. Automatische Erneuerung einrichten (Cronjob)	10
9. CAA Records (in Absprache)	11

1. Zweck dieser Anleitung

Diese Anleitung führt Sie Schritt für Schritt durch die Einrichtung der automatischen SSL/TLS-Zertifikatserneuerung. Ziel ist es, sicherzustellen, dass Ihre Website dauerhaft über HTTPS erreichbar ist und die Zertifikate rechtzeitig ohne manuellen Eingriff erneuert werden.

Mit dieser Anleitung lernen Sie:

- Certbot auf Ihrem Linux-Server zu installieren und zu konfigurieren
- SSL/TLS-Zertifikate von DigiCert über das ACME-Protokoll zu beantragen und zu erneuern
- die Zertifikatserneuerung vollständig zu automatisieren
- sicherzustellen, dass der Apache-Webserver nach der Erneuerung korrekt funktioniert

2. Technische Voraussetzungen

Bitte stellen Sie sicher, dass alle folgenden Voraussetzungen erfüllt sind, bevor Sie mit der Einrichtung beginnen:

- Linux-Server (z. B. SUSE, Debian/Ubuntu, RHEL/CentOS/Rocky Linux)
- Apache-Webserver installiert und aktiv
- Administratorrechte (sudo) vorhanden
- SSH-Zugriff auf den Server
- Domain ist über Port 80 aus dem Internet erreichbar
- Certbot ist installiert (siehe Abschnitt 2.1)



Empfehlung: Führen Sie alle Befehle als Root aus. Wechseln Sie mit folgendem Befehl in die Root-Umgebung:

```
sudo su -
```

2.1 Certbot installieren

Certbot ist ein Open-Source-Tool zur automatischen Beantragung und Erneuerung von SSL/TLS-Zertifikaten. Falls Certbot noch nicht installiert ist,

verwenden Sie den passenden Befehl für Ihr Betriebssystem:

SUSE Linux:

```
zypper search certbot  
sudo zypper install certbot python311-certbot-apache
```

Prüfen Sie anschliessend die installierte Version (muss > 2.1 sein):

```
certbot --version
```

Debian / Ubuntu:

```
sudo apt update  
sudo apt install certbot python3-certbot-apache -y
```

RHEL / CentOS / Rocky Linux:

```
sudo dnf install certbot python3-certbot-apache -y
```

2.2 Apache-Status prüfen

Stellen Sie sicher, dass der Apache-Webserver aktiv läuft, bevor Sie mit der Zertifikatserneuerung beginnen:

```
sudo systemctl status apache2
```



Erwartetes Ergebnis: Der Status muss active (running) anzeigen. Falls Apache nicht läuft, starten Sie den Dienst mit:

```
sudo systemctl start apache2
```

3. DigiCert-Zugangsdaten (EAB)

Für die Nutzung von DigiCert mit Certbot werden einmalig spezielle Zugangsdaten zur Kontobindung benötigt. Diese sogenannten External Account Binding (EAB)-Zugangsdaten verknüpfen Certbot eindeutig mit Ihrem DigiCert-Konto.

Zugangsdaten	Beschreibung
EAB-KID (Key ID)	Kennung zur Identifikation Ihres DigiCert-Kontos
EAB-HMAC-Key	Geheimer Schlüssel zur sicheren Authentifizierung bei DigiCert



Wichtig: Diese Zugangsdaten werden einmalig von DigiCert bereitgestellt und sind für jede Zertifikatsumgebung eindeutig. Bewahren Sie die Zugangsdaten sicher auf. Bei Verlust müssen neue EAB-Daten bei DigiCert angefordert werden.

4. Netzwerkkonfiguration (Proxy)

Falls Ihr Server für externe Internetverbindungen einen Proxy verwendet, muss Certbot diesen Proxy nutzen können, um die DigiCert-Server zu erreichen. Lokale und interne Ziele sollen dabei weiterhin direkt erreichbar bleiben.

4.1 Proxy temporär setzen

Diese Einstellungen gelten nur für die aktuelle Sitzung und müssen nach einem Neustart erneut gesetzt werden:

```
export https_proxy=http://prxp01.admin.ch:8080/  
export http_proxy=http://prxp01.admin.ch:8080/  
export no_proxy=localhost,127.0.0.1,.admin.ch
```

4.2 Proxy dauerhaft konfigurieren (empfohlen)

Um den Proxy permanent zu konfigurieren, bearbeiten Sie die Datei ~/.bashrc:

Schritt 1 – Datei öffnen:

```
vim ~/.bashrc
```

Schritt 2 – In den Bearbeitungsmodus wechseln:

Drücken Sie die Taste `i`, um in den Insert-Modus zu wechseln.

Schritt 3 – Zeilen am Ende der Datei einfügen:

```
export https_proxy=http://prxp01.admin.ch:8080/  
export http_proxy=http://prxp01.admin.ch:8080/  
export no_proxy=localhost,127.0.0.1,.admin.ch
```

Schritt 4 – Datei speichern und schliessen:

Drücken Sie `Esc`, geben Sie `:wq` ein und bestätigen Sie mit `Enter`.

Schritt 5 – Änderungen aktivieren:

```
source ~/.bashrc
```

5. Erstmalige Zertifikatserneuerung mit Certbot

Die Zertifikatserneuerung erfolgt über Certbot im non-interactive Modus, sodass der Vorgang vollständig automatisiert werden kann.

5.1 Certbot-Befehl ausführen

! **Wichtig:** Passen Sie alle Platzhalter in <> vor der Ausführung an Ihre Umgebung an.

```
sudo -E certbot certonly \  
  --apache \  
  --non-interactive \  
  --agree-tos \  
  --server https://one.digicert.com/mpki/api/v1/acme/v2/directory \  
  --email <IHRE_EMAIL_ADRESSE> \  
  --eab-kid "<IHRE_EAB_KID>" \  
  --eab-hmac-key "<IHRE_EAB_HMAC_KEY>" \  
  -d <IHRE_DOMAIN> \  
  --cert-name <ZERTIFIKATS_NAME>
```

Empfehlungen zum Zertifikatsnamen:

- Verwenden Sie die Hauptdomain ohne Protokoll (z. B. example.com)
- Optional: Präfix wie ssl- oder cert- voranstellen
- Beispiel: /etc/letsencrypt/live/example.com/



Tipp: Ein eindeutiger Zertifikatsname erleichtert die spätere Wartung, Zuordnung und Fehleranalyse - insbesondere wenn mehrere Zertifikate auf einem Server vorhanden sind.

6. Webserver neu starten

Damit Apache das neue Zertifikat lädt und verwendet, muss der Webserver nach der Erneuerung neu gestartet werden:

```
sudo systemctl restart apache2
```

7. Funktionsprüfung

Überprüfen Sie nach dem Neustart, ob das neue Zertifikat korrekt eingebunden ist und der Webserver ordnungsgemäss funktioniert.

7.1 Browser-Test

Rufen Sie Ihre Website im Browser auf:

```
https://<IHRE_DOMAIN>
```

Erwartetes Ergebnis: Das Zertifikat wird als gültig und vertrauenswürdig angezeigt. Im Browser erscheint ein Schloss-Symbol in der Adresszeile.

7.2 Technischer Test

Führen Sie einen curl-Test durch, um den HTTP-Statuscode zu prüfen:

```
curl -I https://<IHRE_DOMAIN>
```

Erwartetes Ergebnis: Die Antwort enthält **HTTP/1.1 200 OK**

8. Automatische Erneuerung einrichten (Cronjob)

Damit die Zertifikate zukünftig automatisch erneuert werden, wird ein Cronjob eingerichtet. Certbot erneuert Zertifikate automatisch rechtzeitig vor deren Ablauf.

Cronjob-Konfiguration öffnen:

```
sudo crontab -e
```

Fügen Sie folgende Zeile hinzu:

```
30 15 * * * HTTP_PROXY=http://prxc01.admin.ch:8080 HTTPS_PROXY=http://prxc01.ad-  
min.ch:8080 /usr/bin/certbot renew >> /var/log/certbot-cron.log 2>&1 && systemctl  
reload apache2
```

Element	Bedeutung
<code>30 15 * * *</code>	Tägliche Ausführung um 15:30 Uhr
<code>certbot renew</code>	Prüft und erneuert ablaufende Zertifikate automatisch
<code>>> /var/log/cert- bot-cron.log</code>	Protokollierung aller Aktionen in eine Logdatei
<code>systemctl reload apache2</code>	Apache lädt das neue Zertifikat nach der Erneuerung

9. CAA Records (in Absprache)



Wichtig: Es fehlt aktuell ein 0 issuevmc-Eintrag für digicert.com in den DNS CAA Records. Dies sollte mit dem DNS-Team abgesprochen werden, damit der Eintrag hinzugefügt werden kann.

CAA (Certification Authority Authorization) Records legen fest, welche Zertifizierungsstellen für Ihre Domain Zertifikate ausstellen dürfen. Der fehlende Eintrag sollte zeitnah ergänzt werden, um zukünftige Zertifikatsprobleme zu vermeiden.

CAA records for **admin.ch**

An authoritative DNS server (ins3.admin.ch) responded with these DNS records when we queried it for the domain admin.ch.

Data	Revalidate in
0 iodef "mailto:hostmaster@admin.ch" <input type="checkbox"/>	1h
0 issue "swissign.com"	1h
0 issue "letsencrypt.org"	1h
0 issue "digicert.com"	1h
0 issue "comodoca.com"	1h
0 issue "awstrust.com"	1h

Question and response

QUESTION

dig @ins3.admin.ch admin.ch. CAA

ANSWER

```
admin.ch. 3600 CAA 0 iodef "mailto:hostmaster@admin.ch"
admin.ch. 3600 CAA 0 issue "swissign.com"
admin.ch. 3600 CAA 0 issue "letsencrypt.org"
admin.ch. 3600 CAA 0 issue "digicert.com"
admin.ch. 3600 CAA 0 issue "comodoca.com"
admin.ch. 3600 CAA 0 issue "awstrust.com"
```

AUTHORITY

ADDITIONAL