

# SSL/TLS-Check

[tools.ngosu-corp.de/ssl](https://tools.ngosu-corp.de/ssl) prüft das Zertifikat und die Verschlüsselung eines Servers. Das geht für Webserver und für Mailserver per STARTTLS.

## Eingabe

- `example.de` prüft Port 443.
- `mail.example.de:25` prüft SMTP mit STARTTLS.
- `mail.example.de:993` prüft IMAPS (TLS direkt).

Unter **Verbindung** steht standardmäßig *automatisch*: Bei den Ports 25, 587, 143 und 110 wird STARTTLS benutzt, sonst TLS direkt. Du kannst die Verbindungsart auch fest wählen.

## Was geprüft wird

- **Zertifikat:** für wen ausgestellt (inklusive aller Namen/SANs), Aussteller, Ablaufdatum, Schlüssel, Fingerabdruck
- **Kette:** ob alle Zwischenzertifikate mitgeschickt werden und die Kette vertrauenswürdig ist
- **Protokolle:** TLS 1.0 bis 1.3 einzeln. Gut ist: 1.2 und 1.3 an, 1.0 und 1.1 aus
- **Schwache Cipher, HSTS und OCSP-Stapling**

## Häufige Befunde

- **„Kette unvollständig“:** Der Server schickt nur sein Zertifikat ohne Zwischenzertifikat. Browser verzeihen das manchmal, Apps und Mailserver oft nicht. In nginx `fullchain.pem` statt `cert.pem` angeben.
- **„Name passt nicht“:** Der geprüfte Name steht nicht im Zertifikat. Zertifikat mit allen Namen neu ausstellen.
- **„Läuft bald ab“:** Automatische Erneuerung prüfen, z. B. `certbot renew --dry-run`. Mit Premium kann das [Monitoring](#) rechtzeitig warnen.

# Im Terminal

```
curl tools.ngosu-corp.de/ssl/example.de  
curl tools.ngosu-corp.de/ssl/mail.example.de:25  
curl "tools.ngosu-corp.de/ssl/example.de?json"
```

---

Erstellt: 2026-10-16 11:50:01 CEST von cherry

Zuletzt aktualisiert: 2026-10-17 22:53:48 CEST von cherry