SSO-Zertifikat erneuern in Salesforce

CHEAT SHEET

Zwei Methoden, fünf häufige Fehler und eine Checkliste für den reibungslosen Wechsel.

A Self-Signed Zertifikat

Wenn Sie keinen eigenen CA-Prozess haben

1. Setup → **Certificate and Key Management**
2. Bestehendes Zertifikat öffnen → **„Edit“**
3. Neues Ablaufdatum setzen (mind. 2 Jahre) → **„Save“**
4. **Neues Zertifikat exportieren** und an IdP übermitteln
5. In **Identity Provider** das neue Zertifikat aktivieren

B CA-signiertes Zertifikat

Wenn Ihre IT eine eigene Certificate Authority nutzt

1. Setup → Cert. Mgmt → **„Create CA-Signed Certificate“**
2. **CSR herunterladen** und an IT/CA zur Signierung senden
3. Signiertes Zertifikat in Salesforce **importieren** (Upload Signed Certificate)
4. **SSO-Konfiguration** auf neues Zertifikat umstellen
5. Login mit einem Test-User **verifizieren**, bevor Sie das alte Zertifikat deaktivieren

Praxistipp: Downtime vermeiden

Erneuern Sie das Zertifikat mindestens 2 Wochen vor Ablauf. Aktivieren Sie das neue Zertifikat parallel zum alten, testen Sie den Login, und deaktivieren Sie erst dann das alte.

Achtung: Altes Zertifikat nie löschen

Löschen Sie das alte Zertifikat erst, wenn das neue in der SSO-Konfiguration aktiv und getestet ist. Sonst sperren Sie alle SSO-User aus. Im Notfall: SSO-Konfiguration komplett neu erstellen.

HÄUFIGE FEHLER & LÖSUNGEN

Fehler	Lösung
Invalid Certificate Zertifikat abgelaufen oder falscher Key-Type gewählt.	Ablaufdatum prüfen. Key-Type muss mit IdP-Anforderung übereinstimmen (Standard: RSA 2048 Bit).
Login Loop User wird endlos zwischen SF und IdP hin- und hergeschickt.	IdP-Login-URL, Entity-ID und ACS-URL in der SSO-Konfiguration gegenchecken. Alle drei müssen exakt stimmen.
Attribute Mismatch Federation ID stimmt nicht mit dem IdP-Claim überein.	Federation ID im User-Profil mit dem NameID-Claim des IdP abgleichen. Case-Sensitivity beachten.
Clock Skew Error Zeitdifferenz >5 Minuten zwischen Salesforce und IdP.	NTP-Synchronisierung auf dem IdP-Server sicherstellen. Salesforce nutzt UTC als Referenz.
Certificate Not Found SSO-Konfiguration verweist noch auf das alte, gelöschte Zertifikat.	Altes Zertifikat nie löschen, bevor das neue aktiv ist. Im Notfall: SSO-Konfiguration neu erstellen.

CHECKLISTE ZERTIFIKATSWECHSEL

- ☐ Ablaufdatum des aktuellen Zertifikats geprüft
- ☐ Neues Zertifikat erstellt (Self-Signed oder CA)
- ☐ Neues Zertifikat an IdP übermittelt
- ☐ SSO-Konfiguration auf neues Zertifikat umgestellt
- ☐ Test-Login mit einem User erfolgreich
- ☐ Altes Zertifikat deaktiviert (nicht gelöscht!)