SSO-Zertifikat erneuern

VORAUSSETZUNGEN Systemadmin-Profil | Zugriff auf Identity Provider | Neues Zertifikat bereit | Wartungsfenster abgestimmt

1 Ablaufdatum prüfen

Setup → **Certificate and Key Management** → Ablaufdatum im Überblick prüfen. Setzen Sie sich einen Kalender-Reminder 30 Tage vor Ablauf.

2 Neues Zertifikat vorbereiten

CSR generieren oder ein neues **Self-Signed Certificate** erstellen. Schlüssellänge: mindestens 2048 Bit (4096 empfohlen). Laufzeit: maximal 1 Jahr.

3 IdP informieren & Zeitfenster abstimmen

IT-Team oder IdP-Admin benachrichtigen. Wartungsfenster außerhalb der Kernarbeitszeit planen. Beide Seiten müssen gleichzeitig umschalten – sonst bricht der Login.

4 Zertifikat in Salesforce importieren

Setup → **Certificate and Key Management** → Upload oder Edit → neues Zertifikat zuweisen. **Label-Name** muss eindeutig sein. Format: PEM oder JKS.

5 SSO-Konfiguration aktualisieren

Setup → **Single Sign-On Settings** → aktive Konfiguration öffnen → Zertifikat auf das neue wechseln → speichern. Mehrere Konfigurationen? Jede einzeln prüfen.

6 Test in Sandbox

Neuen SSO-Login in der **Sandbox** testen. Login- und Logout-Fluss komplett durchspielen. SP-initiated und IdP-initiated Login separat testen.

7 Go-Live + Monitoring

Altes Zertifikat deaktivieren (nicht löschen!). Login-Logs **mindestens 24 Stunden beobachten**. Erst nach fehlerfreiem Betrieb das alte Zertifikat entfernen. Pfad: Setup → Login History.

WARNUNG Niemals das alte Zertifikat löschen, bevor das neue verifiziert ist – sonst kompletter SSO-Ausfall. Halten Sie für den Notfall einen Admin-Account mit direktem Login (ohne SSO) bereit.

PRAXIS Dokumentieren Sie jeden Zertifikatswechsel mit Datum, Beteiligten und IdP-Version in einem internen Wiki. Beim nächsten Mal sparen Sie sich die Hälfte der Abstimmung.