

Entra Connect nach Server-Wiederherstellung reparieren

Der Lösungsweg, der funktioniert hat – Schritt für Schritt (Stand 30.08.2026)

Wofür diese Anleitung ist: Der Entra-Connect-Server wurde nach einem Absturz aus der Sicherung wiederhergestellt. Danach synchronisierte er nicht mehr, im Ereignisprotokoll erschien der Fehler AADSTS700027 (das Anmeldezertifikat des Servers war in der Cloud nicht mehr registriert). Die folgenden Schritte haben das Problem behoben – die Zertifikatsrotation in Schritt 4 ist der eigentliche Fix.

Schritt 1: Festplatten wieder in Hyper-V einbinden

Nach dem Serverabsturz und dem Wiederherstellen der Datenträger müssen die (neuen bzw. wiederhergestellten) virtuellen Festplatten der VM wieder zugeordnet werden. Das geschieht auf dem Hyper-V-Host:

- Auf dem Hyper-V-Host den „Hyper-V-Manager“ öffnen.
- Rechtsklick auf die betroffene VM (den Entra-Connect-Server) → „Einstellungen...“.
- Links den Speichercontroller wählen (z. B. „SCSI-Controller“) → rechts „Festplatte“ → „Hinzufügen“.
- Bei „Virtuelle Festplatte“ auf „Durchsuchen“ klicken und die wiederhergestellte VHDX-Datei auswählen. Für jede Platte wiederholen.
- Mit „Übernehmen“ / „OK“ bestätigen. Falls nötig, unter „Firmware/BIOS“ die Startreihenfolge so setzen, dass die Systemplatte zuerst startet.

Schritt 2: Server starten und aktualisieren

- Die VM im Hyper-V-Manager starten und am Server anmelden.
- Windows-Updates einspielen: „Einstellungen → Update & Sicherheit → Windows Update → Nach Updates suchen“, Updates installieren und den Server bei Bedarf neu starten.
- Kurz prüfen, dass Netzwerk und Verbindung zum lokalen AD wieder funktionieren (z. B. Anmeldung mit einem Domänenkonto).
- Snapshot vom Server

Schritt 3: Entra-Connect (AD-Sync-Tool) aktualisieren

Die aktuelle Version des Sync-Tools besorgen und installieren. Fundstelle:

- **Im Microsoft Entra Admin Center:** entra.microsoft.com öffnen, oben in der Suchleiste „Connect“ eingeben und „Microsoft Entra Connect“ öffnen – dort ist der Downloadlink.
- **Alternativ direkt im Microsoft Download Center:** nach „Microsoft Entra Connect“ suchen (Download-ID 47594).
- Die heruntergeladene Datei auf dem Server starten.
- Der Installer erkennt die vorhandene Installation und bietet ein Upgrade an. Den Anweisungen folgen und bei Aufforderung mit dem Administrator-Konto anmelden.
- Das Upgrade abschließen lassen.

Hinweis: Das Update allein behebt den Zertifikatsfehler noch nicht – es stellt nur sicher, dass die aktuelle Version läuft. Der eigentliche Fix folgt in Schritt 4.

Schritt 4: Anwendungszertifikat rotieren (der eigentliche Fix)

Dabei erzeugt der Server ein neues Anmeldezertifikat und registriert es frisch in der Cloud. Damit passt der „digitale Ausweis“ des Servers wieder zu Entra ID, und der Fehler AADSTS700027 ist behoben.

Benötigt: ein Cloud-Administrator-Konto mit der Rolle „Administrator für Hybrididentität“ (oder Globaler Administrator), inkl. Passwort und ggf. zweitem Faktor.

- Auf dem Server den Assistenten öffnen: Symbol „Microsoft Entra Connect“ (Desktop/Startmenü) doppelklicken.
- Auf der Startseite auf „Weiter“ / „Configure“ klicken, bis die Liste „Weitere Aufgaben“ erscheint.
- In der Liste „Rotieren des Anwendungszertifikats“ (Rotate application certificate) auswählen und auf „Weiter“ klicken.
- Mit dem Cloud-Administrator-Konto anmelden (ggf. zweiten Faktor bestätigen).
- Den Anweisungen des Assistenten folgen – der Assistent erstellt das neue Zertifikat und registriert es automatisch in Entra ID.
- Den Vorgang bis „Konfiguration abgeschlossen“ durchlaufen lassen und den Assistenten schließen.

Ergebnis: Die Anmeldung des Servers an der Cloud funktioniert wieder, die Synchronisierung nimmt ihren Betrieb wieder auf. Der aufgestaute Rückstand (neue/geänderte Benutzer seit dem Ausfall) wird beim nächsten Lauf automatisch übertragen.

Schritt 5: Ergebnis kontrollieren

- Microsoft-365-Admincenter → „Status der Verzeichnissynchronisierung“: bei „Letzte Verzeichnissynchronisierung“ steht wieder eine aktuelle Uhrzeit.
- Neu im lokalen AD angelegte Benutzer erscheinen in Entra/Microsoft 365 und können sich online anmelden (bester Praxistest).
- Ereignisanzeige → Anwendung: es kommen keine Fehler 906 (AADSTS700027) und 662 mehr nach.

Nacharbeiten / Empfehlungen

- Wenn einige Tage alles stabil läuft: den Hyper-V-Prüfpunkt (Snapshot) löschen, damit die VM schlank bleibt.
- Optionale Absicherung: einen zweiten Pass-through-Authentifizierungs-Agent auf einem anderen Server installieren (aktuell nur 1 Agent = einziger Login-Weg).
- Zur Erinnerung: Microsoft unterstützt das Wiederherstellen eines Entra-Connect-Servers aus Backup/Snapshot offiziell nicht – nach einem Restore ist mit genau diesem Zertifikatsproblem zu rechnen. Der Fix ist dann wieder Schritt 4.

Quellen (Microsoft Learn)

[Authenticate to Microsoft Entra ID by Using Application Identity \(Zertifikat rotieren\)](#)

[Troubleshoot Microsoft Entra Connect Sync application-based authentication](#)

Umgebung: Tenant msshg.at, Domäne SCHULE.APS, Sync-App-ID edc94985-7b2b-422f-944f-0f70e2e37fad.