Einrichtung Schritt für Schritt – AzureAD und Gateway

Diese Anleitung richtet die Microsoft-Anmeldung der ERP Remote Console und das lokale Gateway-Passwort ein. Sie richtet sich an den Administrator; die Techniker benötigen anschließend ihr persönliches Console-Profil und ihr ERP-Austria-Microsoft-Konto. Stand: 09.10.2026.

Die Schritte beschreiben die neue Programmversion mit Entra-Unterstützung. Die produktive Entra-Einrichtung und die Umstellung des Servers müssen noch durchgeführt werden. Fehlen die unten genannten Felder, ist zunächst eine passende Gateway-/Console-Version bereitzustellen.

1. Vorbereiten

1. Gateway-Konfiguration und Technikerprofile sichern und für die Umstellung ein Wartungsfenster vorsehen.
2. Ein Administratorkonto im eigenen Microsoft-Entra-Tenant bereithalten, das App-Registrierungen verwalten und Administratorzustimmung für die eigene API erteilen darf. Für diese Schritte ist beispielsweise die Rolle **Cloudanwendungsadministrator** geeignet.
3. Lokalen Administratorzugriff auf den Gateway-Rechner und Zugriff auf euren Passwortmanager sicherstellen.
4. Den verwendeten Gateway-HTTPS-Namen notieren. Sein Zertifikat muss gültig sein, zum Hostnamen passen und auf Console- und Agent-Rechnern eine vertrauenswürdige Zertifikatskette besitzen.
5. Gateway und Console in einer Version mit der neuen Anmeldung bereitstellen. Die Entra-Registrierungen in Schritt 3–7 zuerst vorbereiten; die neue Gateway-Version sperrt Console-Zugriffe bei fehlender Konfiguration.

Die Gateway-Verwaltung verwendet ein **lokales Passwort**. Die Console verwendet zusätzlich zum Technikerprofil **Microsoft Entra ID (AzureAD)**. Agent und QuickSupport benötigen keine interaktive Microsoft-Anmeldung des Kunden. RoyalTS bleibt parallel im Einsatz.

2. Werteblatt anlegen

Die folgenden Werte während der Einrichtung in euren administrativen Unterlagen notieren. IDs sind keine Passwörter. Profilpasswörter und das Gateway-Passwort gehören in den Passwortmanager.

Bezeichnung	Woher kommt der Wert?	Verwendung

Tenant-ID	App-Registrierung → Übersicht → Verzeichnis-ID (Mandant)	Gateway: Entra Tenant-ID
API-App-ID	ERP Remote Gateway API → Übersicht → Anwendungs-ID (Client)	Gateway: Gateway API-App-ID
Console-App-ID	ERP Remote Console → Übersicht → Anwendungs-ID (Client)	Gateway: Console App-/Client-ID
API-Kennung	`api://<API-App-ID>`	Entra: Eine API verfügbar machen
Vollständiger Scope	`api://<API-App-ID>/access_as_user`	Entra: delegierte Console-Berechtigung
Benutzer-Objekt-ID je Techniker	Entra ID → Benutzer → Alle Benutzer → Person → Übersicht → Objekt-ID	Gateway: Entra Benutzer-Objekt-ID (oid)
Anmeldedomain	`erpaustria.com`	Gateway: Erlaubte Anmeldedomain

IDs nicht verwechseln: Bei den beiden Apps die *Anwendungs-ID (Client)* verwenden. Beim Techniker die *Objekt-ID des Benutzers* verwenden. Die Objekt-ID einer App gehört in keines dieser Gateway-Felder. Platzhalter in spitzen Klammern immer durch die eigene ID ersetzen.

3. Gateway-API in Entra registrieren

1. Microsoft Entra Admin Center öffnen und im ERP-Austria-Tenant anmelden.
2. **Entra ID → App-Registrierungen → Neue Registrierung** öffnen.
3. Name: **ERP Remote Gateway API**.
4. Unter unterstützten Kontotypen **Nur Konten in diesem Organisationsverzeichnis** wählen (Single Tenant).
5. Die Umleitungs-URI leer lassen und **Registrieren** wählen.
6. Aus der Übersicht die **Anwendungs-ID (Client)** als API-App-ID und die **Verzeichnis-ID (Mandant)** als Tenant-ID ins Werteblatt übernehmen.
7. Unter **Besitzer** einen verantwortlichen Administrator hinzufügen. Bei der Console-Registrierung später ebenfalls einen Besitzer hinterlegen.

Kontrolle: Die Registrierung heißt ERP Remote Gateway API und gehört ausschließlich zum eigenen Tenant.

4. Zugriffsscope der Gateway-API anlegen

1. In **ERP Remote Gateway API → Eine API verfügbar machen** wechseln.
2. Die Anwendungs-ID-URI auf `api://<API-App-ID>` setzen und speichern. Keinen abschließenden Schrägstrich ergänzen.
3. **Bereich hinzufügen / Add a scope** wählen und die folgende Tabelle übernehmen.

Feld	Eintrag
Bereichsname / Scope name	`access_as_user`
Wer darf zustimmen?	Nur Administratoren
Anzeigename für Administratorzustimmung	ERP Remote als angemeldeter Techniker verwenden
Beschreibung für Administratorzustimmung	Erlaubt der ERP Remote Console den Zugriff auf den Gateway im Namen des angemeldeten Technikers.
Status	Aktiviert

Bereich hinzufügen bestätigen. Ergebnis: `api://<API-App-ID>/access_as_user`. Für diese Einrichtung sind keine zusätzlichen Anwendungsrollen erforderlich. Microsoft beschreibt die betreffenden Portal-Felder unter API verfügbar machen.

5. Zugriffstoken der API einstellen

1. Weiterhin die Registrierung **ERP Remote Gateway API** geöffnet lassen.
2. **Manifest** öffnen. Im Microsoft-Graph-Format innerhalb des vorhandenen Abschnitts `api` den Wert `requestedAccessTokenVersion` auf die Zahl **2** setzen und speichern. Die übrigen Manifest-Einträge beibehalten. Es geht um die API-Registrierung, nicht die Console.
3. **Tokenkonfiguration → Optionalen Anspruch hinzufügen** öffnen.
4. Tokentyp **Zugriff / Access** wählen, **upn** markieren und hinzufügen.

Kontrolle: Die API fordert Version 2 an; `upn` steht bei den optionalen Zugriffstoken-Ansprüchen. ERP Remote benötigt diese Angaben für die Prüfung des API-Tokens und der Anmeldedomain. Die Einstellungen müssen in der API liegen, weil diese das angeforderte Zugriffstoken bestimmt.

Quellen: Microsoft-Graph-App-Manifest und optionale Ansprüche.

6. Console als Desktop-App registrieren

1. **Entra ID → App-Registrierungen → Neue Registrierung** öffnen.
2. Name: **ERP Remote Console**.
3. Kontotyp: **Nur Konten in diesem Organisationsverzeichnis**. Registrieren.

4. Die **Anwendungs-ID (Client)** als Console-App-ID ins Werteblatt übernehmen. Der Tenant muss derselbe wie bei der Gateway-API sein.
5. Unter **Besitzer** den verantwortlichen Administrator hinzufügen.
6. **Authentifizierung → Plattform hinzufügen → Mobile und Desktopanwendungen** wählen.
7. Die Umleitungs-URI `http://localhost` eintragen bzw. auswählen und die Plattform speichern.

Kontrolle: `http://localhost` steht unter der Desktop-Plattform. Diese Adresse ist die lokale Rückkehr aus dem Microsoft-Systembrowser, nicht die Gateway-Adresse. Der Gateway bleibt über HTTPS erreichbar. Für ERP Remote keine Client-Secrets erzeugen und keine impliziten Token-Flows aktivieren. Die Einstellung für zusätzliche öffentliche Client-Flows ist für den hier verwendeten Browserablauf nicht erforderlich. Quelle: Microsoft: Desktop-App konfigurieren.

7. Console für die eigene API berechtigen

1. In **ERP Remote Console → API-Berechtigungen → Berechtigung hinzufügen** wechseln.
2. **Meine APIs** öffnen und **ERP Remote Gateway API** auswählen. Falls die API nicht erscheint, den richtigen Tenant und die Besitzer beider Registrierungen prüfen.
3. **Delegierte Berechtigungen** wählen, `access_as_user` markieren und hinzufügen.
4. **Administratorzustimmung für den eigenen Tenant erteilen** wählen und bestätigen. Danach muss die Berechtigung als erteilt angezeigt werden.

Ergebnis: Die Console darf eure Gateway-API mit dem delegierten Scope aufrufen. Für ERP Remote ist keine zusätzliche Microsoft-Graph-Berechtigung erforderlich. Quelle: Microsoft: Zugriff auf die eigene API konfigurieren.

Optional: Unter **ERP Remote Gateway API → Eine API verfügbar machen → Autorisierte Clientanwendungen** die Console-App-ID hinzufügen und `access_as_user` auswählen. Dadurch wird diese Console für den Scope vorab autorisiert. Die personenbezogene Freigabe erfolgt zusätzlich im Gateway in Schritt 9.

8. Gateway lokal öffnen und konfigurieren

1. Die neue Gateway-Verwaltung auf dem Gateway-Rechner mit den erforderlichen Windows-Administratorrechten öffnen.
2. Beim ersten Start ein **lokales Gateway-Passwort mit mindestens 12 Zeichen** vergeben und bestätigen. Im Passwortmanager ablegen. Bei späteren Starts dieses Passwort eingeben.
3. **Gateway-Einstellungen** öffnen und zum Abschnitt **Console-Anmeldung · AzureAD / Entra ID** scrollen.
4. Die Werte aus dem Werteblatt wie folgt eintragen und speichern.

Gateway-Feld	Einzutragender Wert
Entra Tenant-ID	Verzeichnis-ID des eigenen ERP-Austria-Tenants
Console App-/Client-ID	Anwendungs-ID der Registrierung ERP Remote Console
Gateway API-App-ID	Anwendungs-ID der Registrierung ERP Remote Gateway API; nur die GUID, ohne `api://` oder Scope
Erlaubte Anmeldedomain	`erpaustria.com`, ohne `@` und ohne URL

Der Gateway unterstützt hier genau eine Anmeldedomain. Der Benutzer muss mit einem Anmeldenamen dieser Domain angemeldet sein; eine abweichende Mail-Alias-Adresse genügt nicht. Die Domainprüfung ergänzt die feste Technikerzuordnung.

Das lokale Gateway-Passwort schützt die Verwaltung. Nach der ersten Einrichtung kann der Windows-Dienst ohne interaktive Passwortabfrage starten. Ein Dienststart vor der erstmaligen Passwortvergabe wird abgewiesen.

9. Jeden Techniker mit seinem Entra-Benutzer verbinden

1. Im Entra-Portal **Entra ID → Benutzer → Alle Benutzer** öffnen.
2. Den tatsächlichen Microsoft-Benutzer des Technikers auswählen; seinen Anmeldenamen mit Domain kontrollieren.
3. In der Benutzerübersicht die **Objekt-ID** kopieren.
4. In der Gateway-Verwaltung **Benutzerverwaltung** öffnen und den zugehörigen Techniker bearbeiten.
5. Die kopierte ID in **Entra Benutzer-Objekt-ID (oid)** eintragen und speichern.
6. Für jeden weiteren Techniker wiederholen. Jeder Techniker benötigt seine eigene Zuordnung und sein persönliches Console-Profil.

Bestehende Benutzer: Die Zuordnung wird nicht automatisch ergänzt. **Neue Benutzer:** Den Techniker mit dem bestehenden Profilverfahren anlegen und die Objekt-ID vor der ersten Verwendung hinterlegen. Eine Objekt-ID darf nicht mehreren Technikern zugeordnet werden. Das

Passwort der exportierten Profildatei bleibt erforderlich.

10. Gateway starten und Konfiguration kontrollieren

1. Alle Gateway-Einstellungen speichern.
2. Den **Gateway-Windows-Dienst neu starten**. Die Entra-Einstellungen werden beim Start des Gateway-Prozesses eingelesen.
3. Auf einem Console-Rechner die tatsächliche Gateway-URL mit `/api/auth/config` im Browser öffnen, zum Beispiel `https://<euer-gateway-host>/api/auth/config`.
4. Erwartet wird eine JSON-Antwort mit den eingerichteten öffentlichen Anmeldedaten. Die Tenant-/App-IDs und Domain mit dem Werteblatt vergleichen. Dieser Endpunkt enthält keine Techniker-Zugangsdaten.

Kontrolle: Der Browser zeigt keinen Zertifikatsfehler. HTTP 503 bedeutet eine fehlende oder ungültige Entra-Konfiguration. Bei HTTP 404 die installierte Gateway-Version und die Weiterleitung des API-Pfads prüfen. Bei einer HTML-Anmeldeseite oder Umleitung prüfen, ob die Anfrage tatsächlich den ERP-Remote-Gateway erreicht.

11. Erste Anmeldung an der Console

1. Die passende neue Console-Version starten.
2. Falls noch kein persönliches Profil vorhanden ist, die eigene `.erpremote`-Profildatei mit dem zugehörigen Profilpasswort importieren. Ein neu angelegtes oder importiertes Profil benötigt ebenfalls die Microsoft-Anmeldung.
3. Wenn die Anmeldung nicht bereits beim Start bzw. Import geöffnet wird: In den Gateway-Einstellungen **Mit Microsoft anmelden / Geräte laden** wählen.
4. Im Microsoft-Anmeldefenster das eigene ERP-Austria-Konto wählen und die von eurer Organisation verlangte Anmeldung bzw. MFA abschließen.
5. Zur Console zurückkehren und warten, bis Geräte und Verbindungen geladen sind.
6. Eine ausdrücklich für diesen Techniker freigegebene Testverbindung öffnen.

Erst nach erfolgreicher Anmeldung und Gateway-Prüfung werden Daten synchronisiert und gespeicherte Verbindungen freigegeben. Bei jedem neuen Console-Prozess erfolgt eine interaktive Kontowahl; ein schon angemeldetes Browserkonto kann den Ablauf verkürzen. Ob erneut MFA verlangt wird, bestimmen eure Entra-Richtlinien.

12. Abnahme vor Freigabe an alle Techniker

- Ein korrekt zugeordneter Techniker kann sich anmelden, Geräte laden und eine erlaubte Verbindung öffnen.
- Die Anmeldung mit einem anderen Microsoft-Konto wird für das persönliche Technikerprofil abgewiesen.
- Ein Benutzer ohne hinterlegte Entra-Objekt-ID erhält keinen Console-Zugriff.
- Ein frisch importiertes Profil lädt vor erfolgreicher Anmeldung keine Geräte oder Zugangsdaten.
- Nach abgebrochener Anmeldung können auch gespeicherte direkte Verbindungen nicht gestartet werden.
- Eine externe Verbindung aus RoyalTS durchläuft die erforderliche Console-Anmeldung.
- Gateway-Verwaltung schließen und erneut öffnen: Das lokale Passwort wird verlangt.
- Agent und QuickSupport mit gültigem Gateway-Zertifikat testen. Windows und, falls eingesetzt, macOS separat prüfen.

Zertifikate: Ungültige Gateway-Zertifikate können bei Console und Agent nicht mehr zugelassen werden. Bei einer internen Zertifizierungsstelle deren Vertrauenskette korrekt auf den beteiligten Rechnern bereitstellen. Für die eigentliche RDP-Verbindung bleiben die bisherigen Entscheidungen zum Vertrauen in RDP-Zertifikate verfügbar.

Fehlerhilfe

Problem	Nächster Schritt
Kein Microsoft-Fenster erscheint	Persönliches Profil und Gateway-Adresse prüfen; `/api/auth/config` kontrollieren. Bei Zertifikats- oder Gateway-Fehlern zuerst diese beheben.
Microsoft meldet einen Umleitungsfehler	In der Console-App die Desktop-Plattform und exakt `http://localhost` prüfen.
Administratorgenehmigung erforderlich	Delegierten Scope `access_as_user` in der Console-App und erteilte Administratorzustimmung prüfen.
HTTP 401 / Token abgewiesen	Tenant-/App-IDs, API-Tokenversion 2, Systemzeit und Neustart des Gateways prüfen; Console schließen und neu anmelden.
Microsoft-Anmeldung erfolgreich, Gateway verweigert Zugriff	Technikerprofil, Benutzer-Objekt-ID, genaue Anmeldedomain, Console-App-ID und Scope prüfen. Kontrollieren, ob `upn` bei den Zugriffstoken der API eingerichtet ist.

Problem	Nächster Schritt
HTTP 503	Alle vier Gateway-Entra-Felder prüfen, speichern und Gateway-Dienst neu starten.
Ein anderer Techniker sieht eine Verbindung nicht	Privat/Öffentlich, Eigentümer und Ordnerberechtigungen prüfen. Anmeldung allein erteilt keine zusätzlichen Verbindungsrechte.
Gateway-Passwort vergessen	Passwortmanager prüfen. Eine Wiederherstellung muss durch den zuständigen lokalen Administrator nach Sicherung der Gateway-Daten erfolgen.

Nach erfolgreichem Ersttest können eure Entra-Administratoren zusätzliche MFA-/Conditional-Access-Regeln und gegebenenfalls Benutzerzuweisungen für die Anwendungen festlegen. Änderungen zunächst mit einem vorgesehenen Techniker prüfen.

Später einen Techniker hinzufügen

1. Microsoft-Benutzer mit erlaubtem Anmeldenamen bereitstellen.
2. Persönlichen Gateway-Techniker anlegen und dessen Entra-Benutzer-Objekt-ID speichern.
3. Benötigte Verbindungs-/Ordnerrechte vergeben; bei verwendeter Entra-Benutzerzuweisung auch dort zuweisen.
4. Persönliche Profildatei über den vorgesehenen Weg bereitstellen; Profilpasswort getrennt übermitteln.
5. Profil importieren, mit dem eigenen Microsoft-Konto anmelden und eine erlaubte Verbindung testen.

Die beiden App-Registrierungen werden pro Tenant und Installation eingerichtet. Für jeden Techniker wird anschließend nur seine persönliche Zuordnung und Berechtigung ergänzt.

Sicherung vor dem Update und Rückkehr zum bisherigen Stand

Die Sicherung der Ausgabeprogramme im Entwicklungsprojekt ersetzt keine Sicherung des produktiven Gateway-Rechners. Vor dem Austausch der installierten Programme die folgenden Daten sichern. Die Sicherung enthält sensible Verbindungsdaten und muss geschützt abgelegt werden.

A. Was muss gesichert werden?

Ort	Was sichern?
Gateway-Rechner	Den gesamten Ordner `C:\ProgramData\Phoenix Data Systems\ERP Austria Remote Gateway` einschließlich aller Unterordner und des Markers `migration.complete`. Darin liegen insbesondere Gateway-Einstellungen, Zertifikatsdaten, Techniker-/Gerätezuordnungen, gespeicherte Zugangsdaten und persönliche Verbindungen. Im Unterordner `Gateway` liegen auch der Verlauf `remote-history.sqlite` samt gegebenenfalls vorhandenen `-wal`/`-shm`-Dateien und nach Erstkonfiguration das lokale Passwortprüfdatum `admin-password.json`.
Ältere Gateway-Installation vor Datenmigration	Im Windows-Profil des Benutzers, unter dem der Gateway eingerichtet wurde: `%LOCALAPPDATA%\ERPRemote\Gateway`, `GatewayRegistrations`, `GatewayCredentials` und `GatewayPersonalConnections`. Wenn vorhanden, zusätzlich zum ProgramData-Ordner sichern.
Installierte Programme	Die bisherigen kompletten Programmordner einschließlich `appsettings*.json` sichern. Bei der Standardinstallation: `C:\Program Files\Phoenix Data Systems\ERP Austria Remote Gateway` und auf den Kundenrechnern `C:\Program Files\Phoenix Data Systems\ERP Austria Remote Agent`. Bei abweichender Installation deren tatsächlichen Ordner verwenden. Console-Programmordner bzw. macOS-App ebenfalls sichern.
Agent-Rechner, wenn der Agent aktualisiert wird	Gesamten Ordner `C:\ProgramData\Phoenix Data Systems\ERP Austria Remote Agent` sichern. Insbesondere `settings.bin` enthält die Geräteidentität und Registrierung; nicht löschen oder durch fremde Daten ersetzen.
Windows-Technikerrechner	Console schließen. `%APPDATA%\ERPRemote\Console` und `%LOCALAPPDATA%\ERPRemote\Console` sichern sowie die persönlichen exportierten `.erpremote`-Profile. Die Profilpasswörter separat im Passwortmanager bereithalten.
macOS-Technikerrechner	Die bisherige Console-App, die persönlichen `.erpremote`-Profile und deren Importpasswörter sichern. Die Console speichert Technikerzugangsdaten zusätzlich im macOS-Schlüsselbund; eine Kopie der App allein sichert diese nicht. Für einen neuen Rechner das persönliche Profil erneut importieren; für eine vollständige Mac-Wiederherstellung die eigene Systemsicherung verwenden.
Zertifikate und Betriebskonfiguration	Bei einem extern hinterlegten TLS-Zertifikat die PFX-Datei samt sicher verwahrtem Passwort beziehungsweise eine exportierbare Zertifikatssicherung mit privatem Schlüssel sichern. Reverse-Proxy-Konfiguration, Zertifikatsbindung, tatsächliche Dienstpfade, Starttyp und Dienstkonto dokumentieren. Bei Änderungen an RoyalTS auch dessen Konfiguration sichern.

Ort	Was sichern?
Entra und Passwortmanager	Tenant-/App-IDs, Scope, Redirect-URI, Benutzer-Objekt-IDs und erteilte Berechtigungen dokumentieren. Lokales Gateway-Passwort sowie Profil- und Zertifikatspasswörter im Passwortmanager ablegen. Microsoft-Zugriffstokens müssen nicht gesichert werden.

Maschinenbindung beachten: Gateway- und Agent-Einstellungen sind mit Windows-DPAPI an den Rechner gebunden; ältere benutzerbezogene Daten zusätzlich an das Windows-Benutzerprofil. Eine Ordnerkopie ermöglicht daher vor allem die Wiederherstellung auf demselben Rechner mit dem passenden Sicherheitskontext. Für den Ausfall des gesamten Servers zusätzlich eine geeignete System-/VM-Sicherung verwenden und deren Wiederherstellung prüfen. Eine Kopie der verschlüsselten Dateien auf einen anderen Windows-Rechner allein reicht nicht.

B. Sicherung ohne laufende Änderungen erstellen

1. Wartungsfenster beginnen, Console-Verbindungen beenden und Gateway-Verwaltung schließen.
2. Den Dienst **ERPRemote.Gateway** stoppen. Dadurch werden bestehende Fernwartungsverbindungen unterbrochen. Den Stillstand prüfen.
3. Jetzt Programmordner und die vollständigen Gateway-Datenordner in einen datierten, geschützten Sicherungsordner kopieren. Nicht nur die SQLite-Hauptdatei kopieren; den ganzen Datenordner sichern.
4. Bei einem Agent-Update dessen Dienst **ERPRemote.Agent** stoppen und Programm-/Datenordner sichern. Für Console-Sicherungen die Console schließen.
5. Kontrollieren, dass die Sicherung vollständig lesbar ist. Vorherige Versionen und Zeitpunkt notieren; bei einer VM-Sicherung auch deren Abschluss prüfen.
6. Erst danach die neuen Programme übernehmen. Vorhandene produktive `appsettings*.json`, Profile und Daten beibehalten; Beispielkonfigurationen aus der Ausgabe nicht darüberkopieren.
7. Gateway lokal öffnen, neues lokales Passwort vergeben und Entra-Einstellungen/Technikerzuordnungen ergänzen. Anschließend Dienst starten und die Abnahme aus Schritt 12 durchführen.
8. Nach erfolgreicher Einrichtung erneut sichern, damit die neue Passwortdatei und die Entra-Zuordnungen ebenfalls enthalten sind.

C. Wenn die Umstellung nicht funktioniert

1. Zunächst Fehlerhilfe dieser Seite prüfen. Fehlende Entra-Zustimmung, eine falsche Benutzer-ID oder ein nicht vertrauenswürdiges Gateway-Zertifikat sind Konfigurationsprobleme.

2. Falls eine Rückkehr erforderlich ist: Console schließen und betroffene Gateway-/Agent-Dienste stoppen.
3. Den fehlgeschlagenen aktuellen Stand separat sichern. Dann auf demselben Rechner die bisherigen Programmordner und die dazugehörigen Datenordner aus derselben Vor-Update-Sicherung wiederherstellen. Den Datenstand vollständig zurücksetzen, statt neue und alte Dateien zu mischen; auch die Ordnerberechtigungen beibehalten bzw. wiederherstellen.
4. Wenn die Sicherung vor der ProgramData-Migration erstellt wurde, den ursprünglichen Speicherort und Benutzerkontext wiederherstellen. Für einen Rechnerwechsel die System-/VM-Wiederherstellung verwenden.
5. Die zueinander passenden alten Gateway-/Console-Versionen starten; einen ebenfalls aktualisierten Agent bei Bedarf auf seinen gesicherten Stand zurücksetzen. Dienststatus, Anmeldung, Geräteanzeige und eine Testverbindung kontrollieren.

Eine Rückkehr zur alten Programmversion entfernt auch deren neue Entra- und Freigabeschutzfunktionen. Deshalb die alte Version nur mit dem passenden alten Datenstand betreiben und den Rückschritt als vorübergehende Maßnahme behandeln. Änderungen seit dem Sicherungszeitpunkt gehen bei der Wiederherstellung dieses Datenstands verloren.

Gateway-Startfehler nach der Passwortabfrage

Die Gateway-Ausgabe 1.00.237 konnte nach erfolgreicher Passworteingabe mit „Gateway-Einrichtung fehlgeschlagen: InvalidOperationException“ abbrechen. Dieser Startfehler ist in der korrigierten Ausgabe **1.00.243** behoben.

1. Gateway-Verwaltung schließen; falls das installierte Programm ersetzt wird, den Gateway-Dienst stoppen.
2. Die korrigierte `ERPRemote.Gateway.exe` aus dem Ausgabeordner bzw. dem neuen versionsbezogenen ZIP verwenden. Die bestehende `appsettings.json` und die Datenordner beibehalten.
3. Gateway-Verwaltung erneut öffnen und das bereits vergebene lokale Passwort eingeben. Die Passwortdatei `admin-password.json` nicht löschen.
4. Einstellungen kontrollieren und den Dienst nach abgeschlossener Entra-Einrichtung starten.

Console: Kein Microsoft-Anmeldefenster erscheint

Die Console lädt zuerst die öffentliche Anmeldekonfiguration vom Gateway. Erst wenn HTTPS und diese Konfiguration funktionieren, kann das Microsoft-Anmeldefenster geöffnet werden. Ab Console **1.00.326** gibt es oben im Fenster einen sichtbaren Knopf **Mit Microsoft anmelden** sowie eine konkrete Fehlermeldung. Die frühere Ausgabe 1.00.319 zeigte teilweise nur „HttpRequestException“ im Protokoll.

1. Unter **Gateway-Einstellungen** die tatsächliche HTTPS-Adresse einschließlich eines gegebenenfalls verwendeten Ports prüfen. Eine Adresse ohne Port verwendet 443.
2. Genau diese Adresse im Browser mit `/api/auth/config` öffnen. Beispiel bei bewusst eingerichteter externer Freigabe von Port 7443: `https://erpservice.erpaustria.com:7443/api/auth/config`. Gateway-Adresse und Port müssen zum persönlichen Profil und zur Firewall-/Proxy-Konfiguration passen.
3. Bei einem Zertifikatsfehler: Der Browser und die Console müssen ein gültiges Zertifikat für den eingetragenen Hostnamen mit vertrauenswürdiger Kette erhalten. Bei einem falschen Servernamen die NAT-/Portweiterleitung bzw. die TLS-Bindung am Reverse Proxy prüfen. Die Zertifikatsprüfung nicht abschalten.
4. Bei HTTP 503: Die vier Entra-Felder im Gateway vollständig und korrekt eintragen, speichern und den Gateway-Dienst neu starten.
5. Erwartet wird HTTP 200 mit einer JSON-Anmeldekonfiguration und ohne Zertifikatswarnung. Danach in der Console erneut **Mit Microsoft anmelden** wählen.
6. Falls nach der Microsoft-Anmeldung der Zugriff verweigert wird: Benutzer-Objekt-ID und persönliches Technikerprofil entsprechend Schritt 9 prüfen.

Ein automatisch erzeugtes, selbstsigniertes Gateway-Zertifikat wird durch die Erstellung allein auf den Clients nicht vertrauenswürdig. Entweder ein geeignetes vertrauenswürdiges TLS-Zertifikat als PFX im Gateway hinterlegen oder eine interne Zertifikatslösung mit korrekt bereitgestellter Vertrauenskette verwenden. Wenn TLS am Reverse Proxy endet, muss dort das passende externe Zertifikat gebunden sein. Das Vertrauen in RDP-Zertifikate ist davon getrennt.

Native Microsoft-Anmeldung unter Windows und macOS einrichten

Ab Version **1.00.332** verwendet die Console standardmäßig einen Microsoft-Broker: Windows WAM bzw. Company Portal auf verwalteten Macs. Vor dem ersten Einsatz die zusätzlichen Umleitungsadressen in der Console-App registrieren. Die Gateway-API-App bleibt dabei unverändert.

Entra-App ergänzen

1. Entra Admin Center öffnen und **App-Registrierungen → ERP Remote Console → Authentifizierung → Mobile und Desktopanwendungen** auswählen.

2. Diese zusätzlichen Umleitungsadressen hinzufügen und speichern:

Plattform	Zusätzliche Umleitungsadresse
Windows / WAM	`ms-appx-web://Microsoft.AAD.BrokerPlugin/a4c2f1c0-8f96-4c05-9683-40c39381d01b`
Verwalteter Mac / Company Portal	`msauth.com.erpaustria.erpremote.console://auth`

Die Windows-Adresse enthält die Console-Client-ID. Die Mac-Adresse ist fest an die Bundle-ID der ERP-Remote-Console gebunden. Die bereits vorhandene Umleitung `http://localhost` für die Browser-Alternative beibehalten. Keine Client-Secrets anlegen und keine impliziten Token-Flows aktivieren.

Windows testen

1. Die aktuelle Console-Ausgabe übernehmen. Persönliches Profil und bestehende Konfiguration beibehalten.
2. Als normal angemeldeter Windows-Benutzer starten. WAM benötigt eine interaktive Sitzung; nicht als Dienst oder unter einem fremden `runas`-Konto anmelden.
3. **Mit Microsoft anmelden** bzw. unter Gateway-Einstellungen **Microsoft-Anmeldefenster / Geräte laden** wählen.
4. Das Microsoft-Fenster wird der Console zugeordnet. Eigenes ERP-Austria-Konto wählen und erforderliche MFA abschließen.
5. Geräteanzeige und eine erlaubte Verbindung prüfen. Auch mit einem anderen Microsoft-Konto kontrollieren, dass die persönliche Technikerzuordnung weiterhin den Zugriff sperrt.

WAM benötigt Windows 10 bzw. Windows Server 2019 oder neuer. Wenn der Betriebssystem-Broker nicht verfügbar ist, kann MSAL auf die Browser-Anmeldung zurückfallen. Quelle: Microsoft: Windows WAM.

Verwalteten Mac testen

1. Im **Company Portal / Unternehmensportal** prüfen, dass der Mac registriert ist und die Microsoft-SSO-Erweiterung durch die Geräteverwaltung eingerichtet wurde. Eine Anmeldung in einer Microsoft-App über Company Portal als Vorprüfung verwenden.
2. Die aktuelle Console mit dem **macOS-App-Setup** installieren. Die App-Bundle-ID muss `com.erpaustria.erpremote.console` sein; das Setup registriert das zugehörige `msauth`-URL-Schema. Den Broker-Test aus der installierten App durchführen, nicht aus einer einzeln kopierten Programmdatei.
3. Console öffnen, persönliches Profil bei Bedarf importieren und **Mit Microsoft anmelden** wählen.
4. Der Company-Portal-Broker zeigt den Microsoft-Dialog im Vordergrund. Auf macOS unterstützt MSAL keine Windows-artige Zuordnung des Dialogs als Unterfenster der

Console.
5. Eigenes Konto wählen, MFA abschließen und eine erlaubte Testverbindung öffnen.

Ein verwalteter Mac allein genügt nicht: Company Portal und Microsoft-SSO müssen funktionieren. Der Broker ist für Apple Silicon und Intel vorgesehen. Die Ausgabe wurde auf Windows gebaut; die tatsächliche Anmeldung, SSO-Richtlinien und App-Zuordnung müssen auf dem verwalteten Mac geprüft werden. Quelle: Microsoft: macOS-Broker.

Browser-Alternative und Fehlerhilfe

Unter **Gateway-Einstellungen → Alternativ im Standardbrowser anmelden** kann ausdrücklich der bisherige Ablauf gewählt werden, beispielsweise während die zusätzlichen Entra-Umleitungen noch eingerichtet werden. Die Gerätefreigabe erfolgt auch dabei erst nach der serverseitigen Prüfung von Microsoft-Anmeldung und persönlichem Technikerprofil.

Problem	Prüfen
Native Anmeldung wird von Microsoft abgewiesen	Zusätzliche Umleitungsadresse in der richtigen Console-App, Tenant, delegierte API-Berechtigung und Administratorzustimmung prüfen.
Mac zeigt keinen Broker-Dialog	Company Portal, Registrierung und funktionierende SSO-Erweiterung prüfen; die installierte App mit passender Bundle-ID verwenden.
Microsoft-Anmeldung erfolgreich, Zugriff verweigert	Persönliches Technikerprofil, Entra-Benutzer-Objekt-ID und genaue Anmeldedomain prüfen. Der Broker ersetzt diese Gateway-Prüfungen nicht.
Kein Dialog wegen Gateway-Fehler	Gateway-Adresse einschließlich LAN-/VPN-Port, HTTPS-Zertifikat und `/api/auth/config` kontrollieren. Ohne gültige Anmeldekonfiguration wird auch der Broker nicht geöffnet.

Die Console schreibt ihren eigenen Microsoft-Token-Cache weiterhin nicht auf Platte. Windows WAM und Company Portal verwalten ihre Konten und Token-Caches selbst. Eine erneute Kontowahl bedeutet deshalb nicht zwangsläufig eine erneute Passwort- oder MFA-Abfrage; dies bestimmen Microsoft und eure Entra-Richtlinien.

AADSTS50011 nach dem Öffnen des Microsoft-Fensters

Diese Meldung bedeutet, dass die angeforderte Umleitungsadresse in der Entra-App fehlt oder nicht exakt übereinstimmt. In der Console-App mit Client-ID `a4c2f1c0-8f96-4c05-9683-40c39381d01b` unter **Authentifizierung → Mobile und Desktopanwendungen → URI hinzufügen** genau `ms-appx-web://Microsoft.AAD.BrokerPlugin/a4c2f1c0-8f96-4c05-9683-40c39381d01b` eintragen und

speichern. Die vorhandene Adresse `http://localhost` beibehalten. Danach 3–5 Minuten warten, das Fehlermeldungsfenster schließen und in der Console eine neue Anmeldung starten. Quelle: Microsoft: AADSTS50011 beheben.

Console 1.00.333: Port-Fallback und Mac-Fehlerkennung

Die Console versucht jetzt schon vor der Microsoft-Anmeldung den anderen Gateway-Port (7443/443), wenn der konfigurierte Port nicht erreichbar ist. Das hilft bei externem Zugriff über 443 und LAN-/VPN-Zugriff über 7443. Beide Ports werden mit strenger HTTPS-Zertifikatsprüfung geprüft. Die gespeicherte Adresse bleibt erhalten. Eine unvollständige Entra-Konfiguration und verweigerter Zugriff werden nicht durch einen Portwechsel verdeckt.

Bei einem Fehler der nativen Mac-Anmeldung wird zusätzlich eine **Fehlerkennung** angezeigt. Wenn die Browser-Anmeldung funktioniert, die native Anmeldung aber trotz Neustart nicht, diese Kennung für die Diagnose verwenden. Der Status „kompatibel“ im Unternehmensportal und eine normale Word-Anmeldung bestätigen noch nicht die Broker-Funktion. Company Portal/SSO und die installierte Console-App auf dem Mac prüfen; die Browser-Alternative kann bis zur Klärung verwendet werden.

Aktuelle Einrichtung und Navigation · 24.11.2026

Die folgenden Hinweise ergänzen die bestehende Einrichtungsanleitung. Sie ersetzen ältere Versionsangaben und die frühere breite Reiterleiste. Hersteller ist Phoenix Data Systems. Die dargestellten ERP-Austria-Tenant- und Appwerte sind Beispiele der bisherigen Installation; bei einem eigenen Partner-Gateway die eigenen registrierten Werte verwenden. Technische Bestandskennungen und Datenpfade nicht allein wegen der Herstellerumstellung umbenennen.

Bereich links	Einrichtung
Betrieb	Dienstübersicht, Netzwerk & Zertifikat, Geräte, laufende Fernwartungen und Protokoll
Benutzer & Anmeldung	Benutzerverwaltung, Zugriffsrollen, Anmeldung & Entra, Profilversand (SMTP)
Fernwartung	Gateway-Verbindungen für RDP/SSH/Web sowie QuickSupport/WebRTC

Bereich links	Einrichtung
Integration & Wartung	Leistungserfassung und Textprüfung, Lizenz, Tracker/Royal TS, Partner & Darstellung, Updates

Entra-Benutzer suchen statt Objekt-ID abschreiben

1. In der **bestehenden Console-App-Registrierung** unter API-Berechtigungen **Microsoft Graph → Delegierte Berechtigungen → User.ReadBasic.All** ergänzen und Administratorzustimmung erteilen. Gemeint ist nicht die Gateway-API-App und nicht eine Anwendungsberechtigung.
2. Für die Browseranmeldung derselben Console-App die Desktop-Umleitung **http://localhost** unter Mobile Anwendungen und Desktopanwendungen beibehalten beziehungsweise ergänzen. Kein neues Client-Secret nötig.
3. Im Gateway **Benutzer & Anmeldung → Anmeldung & Entra** die vorhandene Tenant-ID und Console-App-/Client-ID prüfen und Änderungen speichern.
4. **Benutzerverwaltung → Benutzer bearbeiten → Microsoft Entra → In Entra suchen…** öffnen.
5. Mindestens zwei Zeichen vom Anfang eines Namens oder einer E-Mail-Adresse eingeben, suchen und im Systembrowser mit einem passenden Microsoft-Konto anmelden. Bei zu vielen Treffern genauer suchen.
6. Anzeigename, Anmeldename und E-Mail kontrollieren, **Benutzer übernehmen** und danach den Benutzerdialog **Speichern**.

Es wird nur die Objekt-ID übernommen. Gateway-Rolle, Zugriffsrollen, Anzeigename, E-Mail und TANSS-Zuordnung werden nicht automatisch geändert. Bereits anderweitig zugeordnete Benutzer können nicht doppelt übernommen werden. Es ist kein neuer Connector und keine weitere App erforderlich.

Lizenzprüfung gehört zur Benutzerfreigabe

Zusätzlich zu Entra-Zuordnung und Rollen muss das Technikerkonto lizenziert sein: Im Volltest höchstens zehn feste Konten, nach dem Test ein Gratis-Techniker, im aktiven Server-Abo alle aktiven Konten. Die Lizenzseite übernimmt Freischaltungen im laufenden Dienst. Ein Lizenzfehler verlangt keine erneute Microsoft-Anmeldung. Lizenz und Leistungserfassung einrichten.

Gatewayports, Mac und Updates

Console und Tracker prüfen bei einem Fehler auf 443 auch 7443 beziehungsweise umgekehrt, solange dort kein echter ERP-Remote-Gateway erkannt wurde. Ein fremder Webserver gilt nicht als Gateway. Eine echte Zugriffsverweigerung und eine unvollständige Gateway-Anmeldekonfiguration werden nicht durch blindes Portwechseln übergangen. HTTPS-Zertifikate müssen gültig bleiben.

Neue Mac-Pakete werden ausschließlich für **Apple Silicon / ARM64** bereitgestellt; die früheren Intel-Hinweise betreffen Altinstallationen. Für die aktuelle integrierte Console das vollständige ARM64-Paket verwenden; das enthaltene RDP-Bundle benötigt macOS 27.2 oder neuer.

Die Dienstanzeige lautet **ERP Remote Gateway Server**. EXE-Dateiname und technische Dienstkennung bleiben unverändert. Für den Austausch des Programmcodes ein Wartungsfenster mit Sicherung und geordnetem Dienstneustart einplanen. Spätere Lizenzänderungen benötigen keinen weiteren Neustart.

Den vollständigen Gateway-Datenordner sichern. Eine ältere Gateway-EXE nicht auf den bereits aktualisierten Datenbestand setzen; für eine Rückkehr die zusammengehörige Vor-Update-Sicherung von Programm und Daten verwenden. Bestehende Einstellungen, Partneridentität und Lizenzdaten erhalten. Eigene Partnerdarstellung und zentrale Updates.

Created 2026-10-09 12:54:09 CEST by Access System API
Updated 2026-11-24 11:07:08 CET by Access MCP API