

Fehler bei der Benutzeranmeldung “Fehler bei der Benutzerauthentifizierung mit Active Directory, da das Benutzerkonto gesperrt ist”

Inhalt

[Problem](#)

[Umwelt](#)

[Auflösung](#)

[Ursache](#)

[Verwandte Inhalte](#)

- [Problem](#)
 - [Umwelt](#)
 - [Auflösung](#)
 - [Ursache](#)
 - [Verwandte Inhalte](#)
-

Problem

Active Directory generiert diesen Fehler, wenn ein Benutzer den Active Directory-Kontosperrungsschwellenwert auf dem Windows Server durch mehrmaliges Eingeben eines falschen Kennworts überschreitet:

“24408 User authentication against Active Directory failed since user has entered the wrong password”

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.2.0 und höher
- Active Directory-Integration für die Benutzerauthentifizierung

- Sowohl kabelgebundene als auch drahtlose Authentifizierungsumgebungen
- RADIUS-basierte Authentifizierung mit Network Access Devices (NADs)

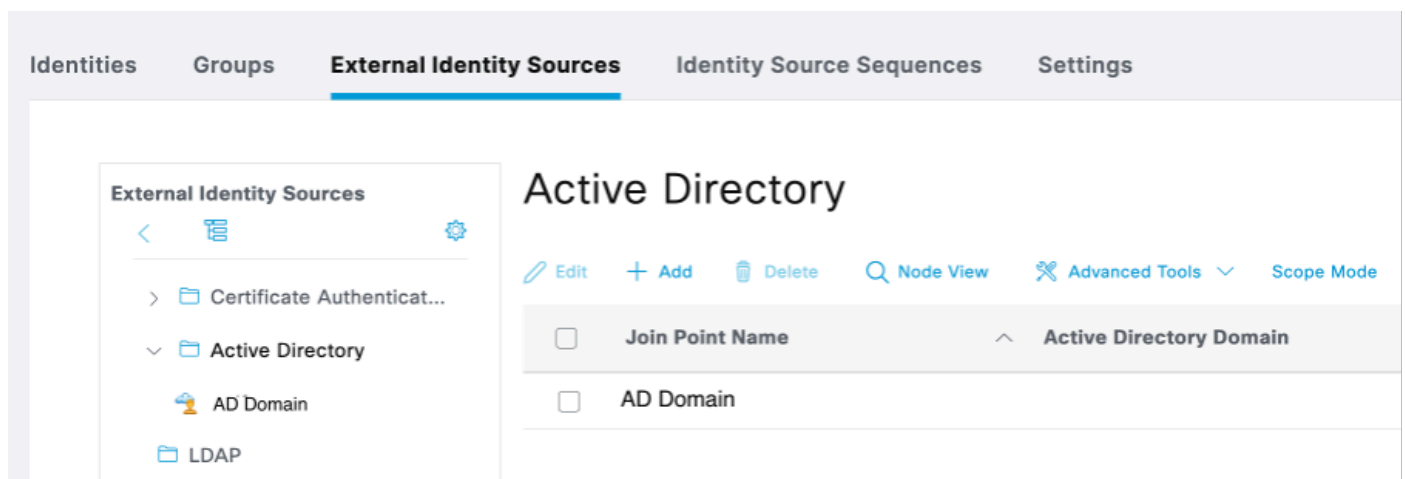
Auflösung

Schritt 1: Aktivieren Sie die Funktion "Verhindert die Sperrung von Active Directory-Benutzern" in Ihrer ISE-Bereitstellung:

Diese Funktion würde das Senden der Benutzerauthentifizierungen an das Active Directory beenden, um zu verhindern, dass sich das Benutzerkonto sperrt. Hierzu werden die maximal zulässigen Versuche mit ungültigen Kennwörtern konfiguriert und dieser Grenzwert mit der aktuellen Anzahl ungültiger Kennwörter (badPwdCount-Attribut) in AD verglichen, bevor eine Authentifizierungsanforderung gesendet wird.

1. Melden Sie sich bei der ISE-GUI an.

2. Navigieren Sie zu Administration > Identity Management > External Identity Sources > Active Directory. Wählen Sie die AD-Domäne aus, und aktivieren Sie die Funktion.



3. Wechseln Sie zur Registerkarte Erweiterte Einstellungen.

* Join Point Name

AD Domain



4. Aktivieren Sie im Abschnitt Active Directory-Benutzersperre verhindern das Kontrollkästchen Fehler-Authentifizierungsschutz aktivieren.

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum attempts

☒ Wireless

☒ Wired

5. Geben Sie die maximal zulässige Anzahl ungültiger Kennwortversuche ein.

- Diese Zahl muss kleiner als die maximale Anzahl ungültiger Kennwortversuche sein, die als Wert des badPwdCount-Attributs in Active Directory konfiguriert wurden.
- Aktivieren Sie das Kontrollkästchen Kabelgebunden oder drahtlos oder beide je nach Authentifizierungs-Verbindungstyp.

6. Klicken Sie auf Speichern.



Anmerkung: Die ISE lehnt Benutzerauthentifizierungsanforderungen so lange ab, bis das Active Directory-Attribut badPwdCount auf 0 zurückgesetzt wird.

Ursache

Dies kann aus folgenden Gründen geschehen:

- Der Benutzer gibt bei der Authentifizierung am Endgerät ein falsches Kennwort ein.
- Der Benutzer ändert die AD-Anmeldeinformationen und vergisst, die AD-Anmeldeinformationen in seinem Wireless-Endpunkt zu aktualisieren, der eine EAP-PEAP-Authentifizierung durchführt.

Verwandte Inhalte

- [Maximale Kennwortversuche für Active Directory-Konto konfigurieren](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.