

Problemen oplossen met de fout bij het inloggen van de gebruiker “gebruikersverificatie met Active Directory is mislukt omdat de gebruikersaccount is vergrendeld”

Inhoud

[uitgifte](#)

[milieu](#)

[resolutie](#)

[Oorzaak](#)

[Gerelateerde inhoud](#)

- [uitgifte](#)
 - [milieu](#)
 - [resolutie](#)
 - [Oorzaak](#)
 - [Gerelateerde inhoud](#)
-

uitgifte

Active Directory genereert deze fout wanneer een gebruiker de Active Directory Account Lockout Threshold op de Windows Server overschrijdt door meerdere keren een onjuist wachtwoord in te voeren:

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

milieu

- Cisco Identity Services Engine (ISE) versie 3.2.0 en hoger

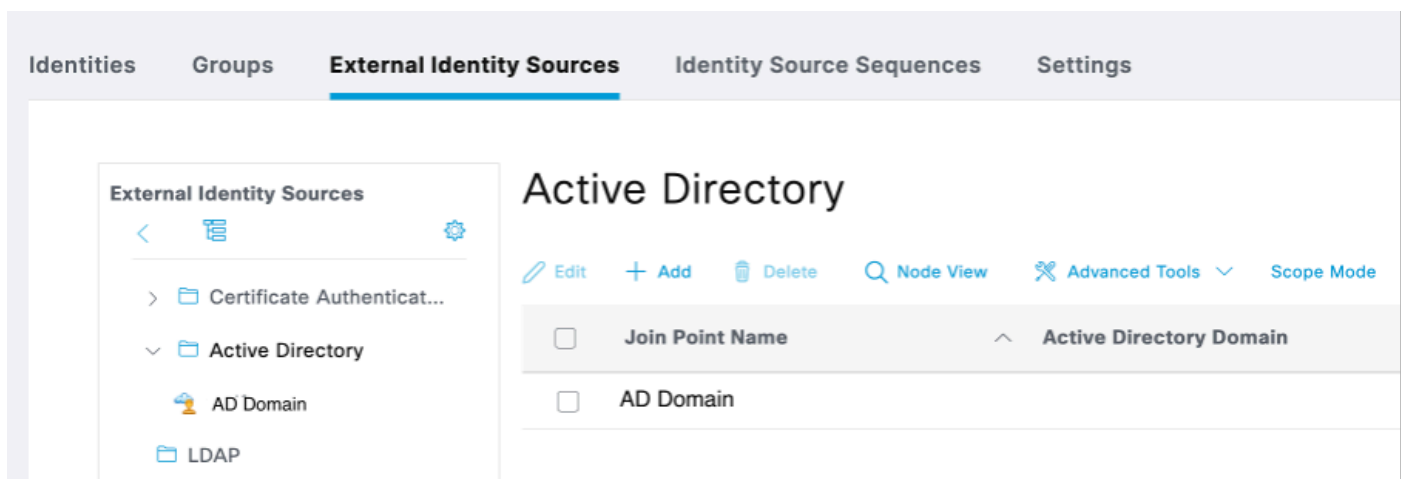
- Active Directory-integratie voor gebruikersverificatie
- Zowel bekabelde als draadloze verificatieomgevingen
- Op RADIUS gebaseerde verificatie met Network Access Devices (NAD's)

resolutie

Stap 1: Schakel de "Prevent Active Directory User Lockout"-functie in op uw ISE-implementatie:

Deze functie stopt met het verzenden van de gebruikersverificaties naar de Active Directory om te voorkomen dat de gebruikersaccount wordt vergrendeld door de maximaal toegestane slechte wachtwoordpogingen te configureren en deze limiet te vergelijken met de huidige slechte wachtwoordtelling (badPwdCount-kenmerk) in AD voordat een verificatieverzoek wordt verzonden.

1. Log in op de ISE GUI.
2. Navigeer naar Beheer > Identiteitsbeheer > Externe identiteitsbronnen > Active Directory. Selecteer het AD-domein, u wilt de functie inschakelen.



3. Ga naar het tabblad Geavanceerde instellingen.

* Join Point Name

AD Domain



4. Schakel in het gedeelte Gebruikersuitsluiting in Active Directory voorkomen het selectievakje in voor Bescherming tegen mislukte verificatie inschakelen.

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum 2 attempts

☒ Wireless

☒ Wired

5. Voer het maximum aantal toegestane pogingen tot een slecht wachtwoord in.

- Dit aantal moet lager zijn dan de maximale pogingen tot het invoeren van een slecht wachtwoord die zijn geconfigureerd als de waarde van het kenmerk badPwdCount in Active Directory.
- Schakel het selectievakje Bedraad of Draadloos of Beide in op basis van het type verificatieverbinding.

6. Klik op Opslaan.



Opmerking: ISE blijft verzoeken om gebruikersverificatie weigeren totdat het kenmerk Active Directory badPwdCount is gereset naar nul.

Oorzaak

Dit kan gebeuren om de volgende redenen:

- De gebruiker voert een onjuist wachtwoord in tijdens het uitvoeren van de verificatie op het eindpunt.
- De gebruiker wijzigt de AD-referenties en vergeet de AD-referenties bij te werken in het draadloze eindpunt dat EAP-PEAP-verificatie uitvoert.

Gerelateerde inhoud

- [Maximale wachtwoordpogingen voor Active Directory-account configureren](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.