

Troubleshooting the User Login Failure Error “User authentication against Active Directory failed since user's account is locked out”

Contents

[Issue](#)

[Environment](#)

[Resolution](#)

[Cause](#)

[Related Content](#)

- [Issue](#)
 - [Environment](#)
 - [Resolution](#)
 - [Cause](#)
 - [Related Content](#)
-

Issue

Active Directory generates this error when a user exceeds the Active Directory Account Lockout Threshold on the Windows Server by entering an incorrect password multiple times:

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

Environment

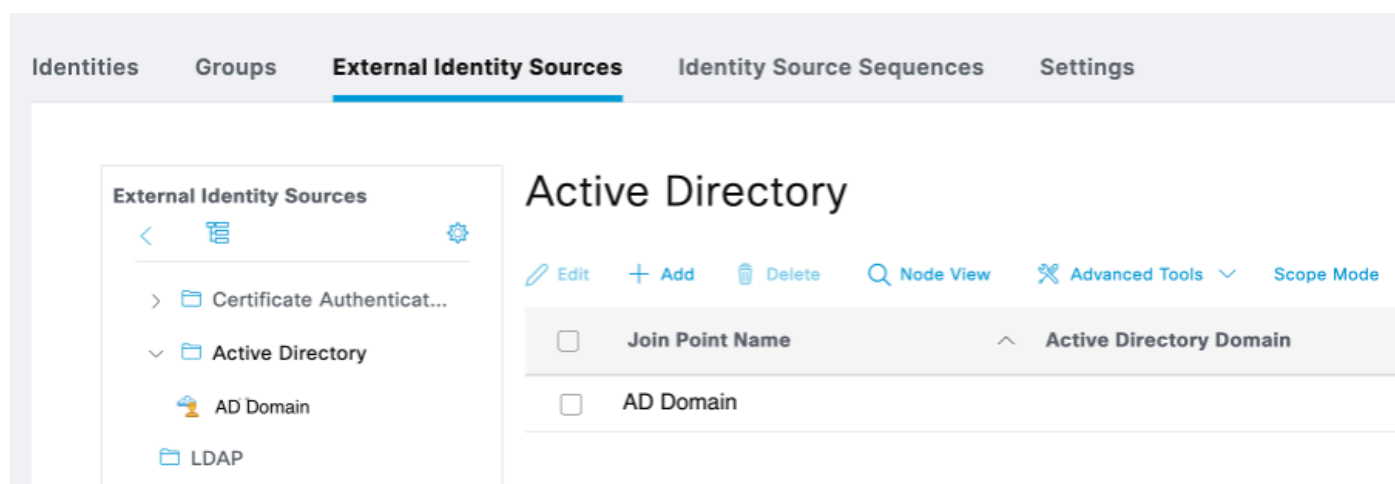
- Cisco Identity Services Engine (ISE) version 3.2.0 and later
- Active Directory integration for user authentication
- Both wired and wireless authentication environments
- RADIUS-based authentication with Network Access Devices (NADs)

Resolution

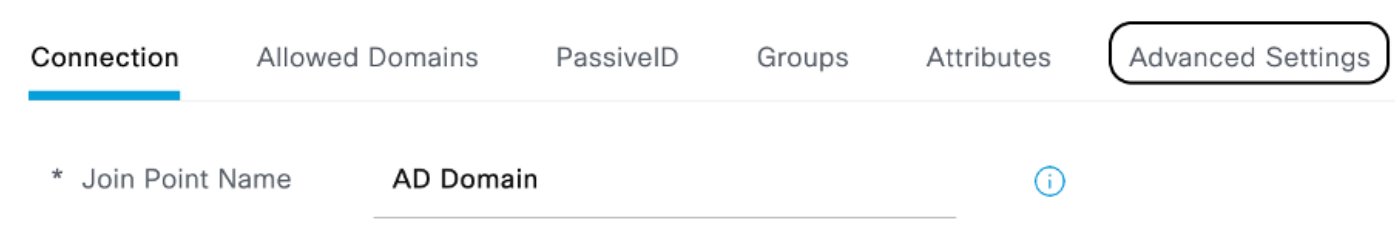
Step 1: Enable the “Prevent Active Directory User Lockout” feature on your ISE deployment :

This feature would stop sending the user authentications to the Active Directory to prevent the user account from locking out by configuring the maximum allowed bad password attempts and comparing this limit with the current bad password count (badPwdCount attribute) in AD before sending an authentication request.

1. Log into the ISE GUI.
2. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**. Select the **AD Domain**, you want to enable the feature.



3. Go to the **Advanced Settings** tab.



4. In the **Prevent Active Directory User Lockout** section, check the box for **Enable Failed Authentication Protection**.

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum attempts

☒ Wireless

☒ Wired

5. Enter the maximum number of bad password attempts allowed.

- This number must be less than the maximum bad password attempts configured as the value of the badPwdCount attribute in Active Directory.
- Make sure to enable either **Wired** or **Wireless** or **Both** check box according to your authentication connection type.

6. Click **Save**.



Note: ISE would continue to reject user authentication requests until the Active Directory badPwdCount attribute is reset to zero.

Cause

This can happen for the reasons:

- The user enters incorrect password while performing the authentication on the endpoint.
- The user changes the AD credentials and forget to update the AD credentials in their Wireless endpoint which perform EAP-PEAP authentication.

Related Content

- [Configure Maximum Password Attempts for Active Directory Account](#)