

# 用户登录失败错误故障排除“；由于用户帐户被锁定”，针对Active Directory的用户身份验证失败

## 目录

---

[问题](#)

[环境](#)

[分辨率](#)

[原因](#)

[相关内容](#)

---

- [问题](#)
  - [环境](#)
  - [分辨率](#)
  - [原因](#)
  - [相关内容](#)
- 

## 问题

当用户多次输入不正确的密码超过Windows Server上的Active Directory帐户锁定阈值时，Active Directory会生成此错误：

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

## 环境

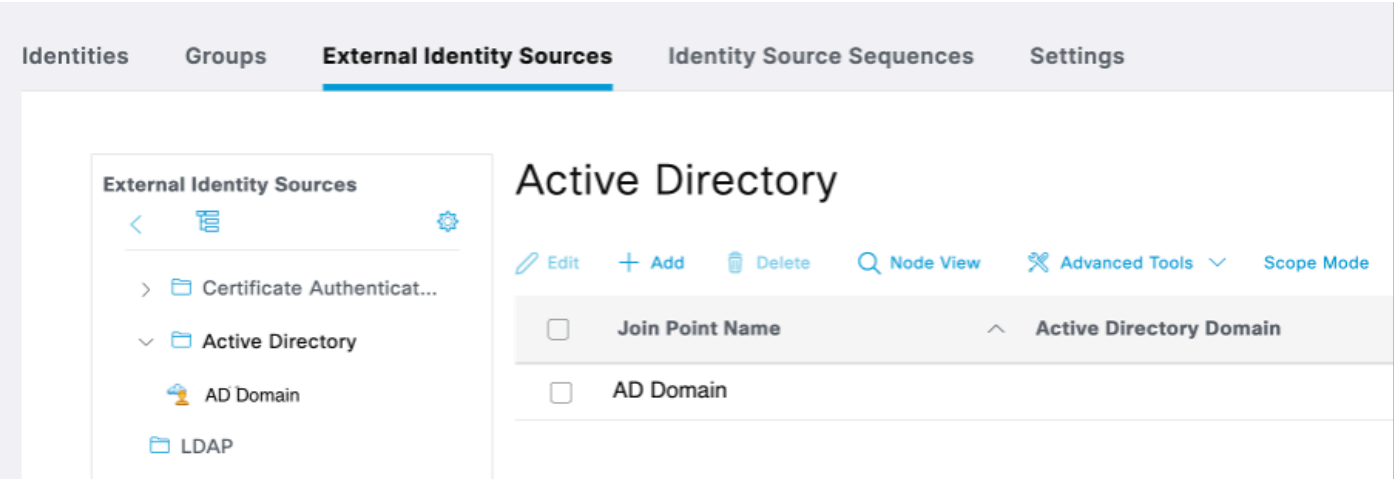
- 思科身份服务引擎(ISE)3.2.0版及更高版本
- 用于用户身份验证的Active Directory集成
- 有线和无线身份验证环境
- 使用网络接入设备(NAD)进行基于RADIUS的身份验证

# 分辨率

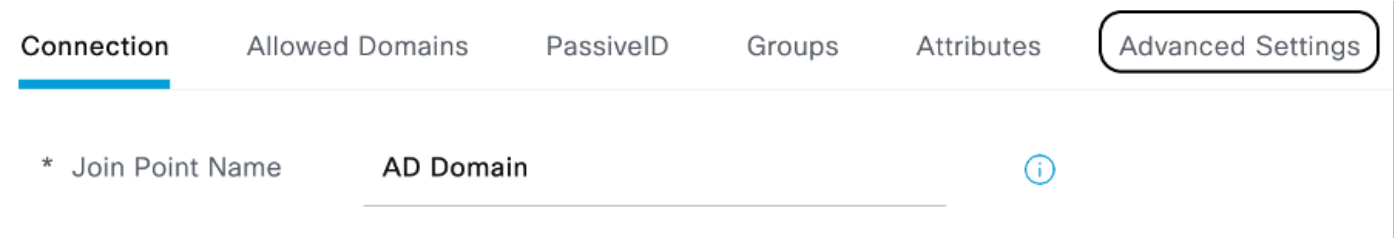
步骤 1：在ISE部署上启用“阻止Active Directory用户锁定”功能：

此功能将停止向Active Directory发送用户身份验证，以防止用户帐户锁定，方法是配置允许的最大错误密码尝试次数并将此限制与AD中的当前错误密码计数（badPwdCount属性）进行比较，然后发送身份验证请求。

- 1.登录ISE GUI。
- 2.导航到管理>身份管理>外部身份源> Active Directory。选择AD域，您要启用此功能。



3.转到Advanced Settings选项卡。



4.在阻止Active Directory用户锁定部分，选中启用失败的身份验证保护复选框。

## ▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum  attempts

☒ Wireless

☒ Wired

5.输入允许的最大错误密码尝试次数。

- 此数字必须小于配置为Active Directory中badPwdCount属性值的最大错误密码尝试次数。
- 确保根据身份验证连接类型启用Wired或Wireless或Both复选框。

6.单击保存。



注意：ISE将继续拒绝用户身份验证请求，直到Active Directory badPwdCount属性重置为零。

## 原因

发生这种情况的原因包括：

- 用户在终端上执行身份验证时输入了不正确的密码。
- 用户更改AD凭证，并忘记更新其无线终端中执行EAP-PEAP身份验证的AD凭证。

## 相关内容

- [配置Active Directory帐户的最大密码尝试次数](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。