

# ISE 3.5 EntraID外部组查询性能问题和Microsoft Graph API权限解析

## 目录

---

## 问题

查询EntraID.ExternalGroups时，具有EntraID REST ID存储配置的思科ISE 3.5 patch2在EAP-TLS身份验证期间遇到严重的身份验证延迟。Queried PIP - EntraID.ExternalGroups阶段需要超过30秒才能完成，导致EAP客户端超时并重新启动身份验证，从而阻止会话成功完成。

此外，尝试在EntraID REST ID存储配置中保存组属性时，会出现以下错误消息：

```
java.rmi.RemoteException: null; nested exception is: java.lang.NullPointerException
```

身份验证日志显示在外部组查找过程中出现异步PIP错误和策略引擎挂起。此问题显示为身份验证失败的工作流程，其中客户端由于查询时间延长而无法完成EAP会话。

## 环境

- 思科身份服务引擎(ISE)版本3.5.0.527，带补丁2
- 通过REST ID存储实现Microsoft EntraID(Azure Active Directory)集成
- 已配置EAP-TLS身份验证
- 为EntraID配置的REST源具有组属性检索
- 在ISE 3.4 patch4/patch5和ISE 3.5 patch2/patch3上观察到的问题

## 分辨率

解决方案涉及向ISE EntraID REST ID存储集成使用的Azure应用程序授予正确的Microsoft Graph API权限。

## 步骤 1：授予所需的Microsoft Graph API权限

导航到Azure门户并找到用于ISE集成的应用注册。授予此应用类型API权限：

Directory.Read.All

确保为此权限授予管理员同意。

## 步骤 2：重新启动ISE服务

授予Directory.Read.All权限后，在所有ISE节点上执行服务重新启动以确保新权限生效。

## 步骤 3：检验分辨率

测试身份验证过程，以确认Queried PIP - EntraID.ExternalGroups阶段在可接受的时间范围内完成，并且Group属性可以无错误地保存。

解析日志必须显示成功完成，而不显示AsynchronousPIPEError:

```
2026-05-26 14:21:47,981 DEBUG [I/O dispatcher 1][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::--
```

## 原因

此问题是由思科Bug ID CSCwu13703引起的，它影响ISE 3.5补丁3和相关版本。此漏洞与Microsoft Graph API权限不足，无法进行EntraID集成有关。如果没有正确的Directory.Read.All权限，ISE无

法从EntraID有效查询外部组，导致超时条件和策略引擎通过AsynchronousPIPErError异常挂起。

身份验证过程失败，因为每次失败的评估都会导致策略引擎抛出AsynchronousPIPErError并挂起身份验证工作流程，从而导致延长的查询时间和最终的客户端超时。

## 相关内容

- [思科漏洞ID CSCwu13703](#)
- [带Microsoft Active Directory Entra ID和Intune的思科ISE配置指南](#)

## 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）。