

ISE 3.5 EntraID External Groups Query Performance Issues and Microsoft Graph API Permission Resolution

Contents

Issue

Cisco ISE 3.5 patch2 with EntraID REST ID Store configuration experiences significant authentication delays during EAP-TLS authentication when querying EntraID.ExternalGroups. The **Queried PIP - EntraID.ExternalGroups** phase takes more than 30 seconds to complete, causing EAP clients to timeout and restart authentication, preventing successful session completion.

Additionally, when attempting to save Group attributes in the EntraID REST ID Store configuration, the following error message appears:

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

The authentication logs show asynchronous PIP errors and policy engine suspension during the external groups lookup process. The issue manifests as failed authentication workflows where clients cannot complete EAP sessions due to the extended query times.

Environment

- Cisco Identity Services Engine (ISE) Version 3.5.0.527 with Patch 2
- Microsoft EntraID (Azure Active Directory) integration via REST ID Store
- EAP-TLS authentication configured
- REST source configured for EntraID with group attribute retrieval
- Issue observed on ISE 3.4 patch4/patch5 and ISE 3.5 patch2/patch3

Resolution

The resolution involves granting the correct Microsoft Graph API permissions to the Azure application used by the ISE EntraID REST ID Store integration.

Step 1: Grant Required Microsoft Graph API Permissions

Navigate to the Azure portal and locate the application registration used for ISE integration. Grant this Application-type API permission:

Directory.Read.All

Ensure that admin consent is granted for this permission.

Step 2: Restart ISE Services

After granting the Directory.Read.All permission, perform a restart of the services on all ISE nodes to ensure the new permissions take effect.

Step 3: Verify Resolution

Test the authentication process to confirm that the **Queried PIP - EntraID.ExternalGroups** phase completes within acceptable timeframes and that Group attributes can be saved without errors.

The resolution logs must show successful completion without the AsynchronousPIPErrors:

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

Cause

The issue is caused by Cisco bug ID CSCwu13703, which affects ISE 3.5 patch 3 and related versions. The bug is related to insufficient Microsoft Graph API permissions for the EntraID integration. Without the proper Directory.Read.All permission, ISE cannot efficiently query external groups from EntraID, resulting in timeout conditions and policy engine suspension through AsynchronousPIPErro exceptions.

The authentication process fails because each unsuccessful evaluation causes the policy engine to throw AsynchronousPIPErro and suspend the authentication workflow, leading to the extended query times and eventual client timeout.

Related Content

- [Cisco bug ID CSCwu13703](#)
- [Cisco ISE with Microsoft Active Directory Entra ID and Intune Configuration Guide](#)