The End of the memberOf Operator in Entra ID Dynamic Groups: Find and Remediate Impacted Objects

Microsoft has announced the retirement of the `memberOf` **rule operator** for dynamic groups in **Microsoft Entra ID**. Organizations using this feature should begin assessing their environment immediately and identify all dependent configurations across **Entra ID**, **Microsoft Intune**, and related services.

What is changing?

The `memberOf` operator was introduced as a public preview feature that allowed administrators to create dynamic user or device groups based on the direct membership of other groups.

```
user.memberOf -any (group.objectId -in ['GroupID'])
```

This enabled scenarios such as:

- License assignment based on consolidated groups
- Conditional Access targeting
- Intune app and policy assignments
- Access package automation
- Applications that cannot evaluate nested group memberships

Microsoft has now confirmed that the **public preview is ending**. After **3 November 2026**, dynamic groups, dynamic administrative units, and entitlement management auto-assignment policies using the `memberOf` operator will **stop updating** and remain in their last known state. This can result in stale memberships, outdated access permissions, licensing inconsistencies, and incorrect policy targeting.

According to Microsoft, the underlying reason is that the `memberOf` operator can negatively affect the scalability and performance of dynamic membership processing across a tenant.

Why this matters

Many organizations use Entra ID groups as the foundation for:

- Intune application assignments
- Compliance policies
- Configuration profiles
- Conditional Access policies
- Group-based licensing
- Identity Governance and Access Packages

Once `memberOf` processing stops, memberships will no longer reflect changes in the source groups. Users may retain access they should have lost, while new users may never receive the access, licenses, or policies they require.

Finding Affected Objects and Dependencies

Identifying the dynamic groups using the `memberOf` operator is only the first step. In most environments, these groups are referenced throughout Microsoft Entra ID and Microsoft Intune, making it difficult to understand the full impact of the retirement.

To simplify this analysis, I created the **Check-EntraMemberOfUsage.ps1** script, available on GitHub:

GitHub Repository: Check-EntraMemberOfUsage.ps1

The script automatically discovers dynamic groups using the `memberOf` operator and maps where they are being used across Entra ID and Intune workloads. This helps administrators quickly identify dependencies and prioritize remediation efforts before Microsoft stops processing these groups.

What Does the Script Check?

The script identifies affected dynamic groups and searches for assignments and references in:

Entra ID workload that defines a memberOf rule:

- Dynamic groups
- Administrative units (incl. restricted management)
- Entitlement management policies

Entra ID workload that uses an affected group:

- Conditional Access policies
- Enterprise app assignments

Intune workload that uses an affected group:

- Device configuration, settings catalog & admin template profiles
- Compliance policies
- Enrollment configs & Autopilot profiles
- Scripts (PowerShell, shell, custom attribute, remediation)
- Windows update profiles
- Endpoint Security policies
- App assignments, app config & app protection policies

The resulting report provides a consolidated view of where these groups are currently used, helping to avoid overlooked dependencies during migration.

How to Use the Script

1. Download the script from the GitHub repository.
2. Connect to Microsoft Graph with the required permissions.
3. Execute the script in PowerShell.
4. Review the generated output and exported report.
5. Identify affected groups and dependent workloads.
6. Plan and validate replacement solutions before the retirement deadline.

This approach provides significantly more visibility than simply querying Entra ID for affected dynamic groups.

Extend the Analysis Further

The script focuses on Microsoft Entra ID and Microsoft Intune workloads, which are typically the most common areas where dynamic groups are assigned.

However, every environment is different. Additional workloads such as:

- Exchange Online
- SharePoint Online

- Microsoft Teams
- Power Platform
- Azure RBAC
- Enterprise Applications

can also depend on these groups.

Because the solution is built on Microsoft Graph and PowerShell, it can easily be extended to include further services. Modern AI-assisted development tools can significantly accelerate the creation of additional checks and reporting logic tailored to your environment.

AI Disclosure

This script was initially generated with the assistance of Claude Code (Anthropic) and subsequently reviewed and adapted for Microsoft Entra ID and Intune environments. As with any AI-generated code, validate and test it in a non-production environment before use.

References

- Microsoft Learn: Configure dynamic membership groups with the memberOf operator
- Our Cloud Network: The memberOf rule operator is ending for dynamic Groups in Entra
- LNC Docs: Microsoft Entra ID
- GitHub: Check-EntraMemberOfUsage.ps1

Revision #4
Created 2026-08-19 08:20:05 UTC by Luca Noah Caprez
Updated 2026-08-19 10:18:22 UTC by Luca Noah Caprez