Azure Permissions for VBO Cross-User Mailbox Restores

(Following Microsoft's Deprecation of '**ApplicationImpersonation' role)**

Date: 06/08/2025

Prepared by:

Paul Finn, Managed Services Consultant

Covenco Ltd.

Unit 4, MXL Centre

Lombard Way

Banbury

Oxfordshire

OX16 4TJ

www.covenco.com

Contents

Introduction

Microsoft has deprecated the ApplicationImpersonation RBAC role in Exchange Online, marking a major shift in how cross-mailbox operations (such as restores) are performed.

This change affects third-party backup and restore tools, including Veeam Backup for Microsoft 365, that previously relied on impersonation for mailbox access during restores.

Timeline of Deprecation

- **February 20, 2024**
  Microsoft announced the upcoming deprecation, stating that new role assignments would be blocked starting **September 2024**, with full removal no later than **February 2025**.

- **May–July 2024**
  Vendors began confirming that new assignments were already being blocked.

- **March 13, 2025**
  Deprecation was completed, and the role was fully removed from Exchange Online.

As a result, any attempt to use **ApplicationImpersonation** for restores or cross-mailbox access will now fail, regardless of whether it was previously assigned.

What This Means for You

- **ApplicationImpersonation can no longer be used** for mailbox restores or migrations in Exchange Online.

- The new supported approach for restore operations is to **grant explicit FullAccess permissions** on the target mailboxes to the restore account.

- Interactive authentication with delegated permissions is required for tools like **Veeam Explorer for Exchange**, as app-only authentication does not support cross-mailbox restores.

Updated Process Overview

With impersonation deprecated, the supported restore method involves granting FullAccess permission to the restore operator (or group) on the target mailboxes.

Step 1: Connect to Exchange Online PowerShell
```
Connect-ExchangeOnline
```

Step 2: Grant FullAccess to Target Mailboxes
For example, granting bob@bob.com access to user-to-restore-to@bob.com:

```
Add-MailboxPermission -Identity "user-to-restore-to@bob.com" `
        -User "bob@bob.com" `
        -AccessRights FullAccess `
        -AutoMapping:$false
```
Repeat for each mailbox you need to restore into.

(Optional) Use a Security Group for Bulk Assignments
If restoring to multiple mailboxes, assign FullAccess via a security group:

```
# Add restore user to a security group (e.g., RestoreOperators)
Add-DistributionGroupMember -Identity "RestoreOperators" -Member "bob@bob.com"
```

```
# Grant group FullAccess to a mailbox
Add-MailboxPermission -Identity "target.user@domain.com" `
        -User "RestoreOperators@domain.com" `
        -AccessRights FullAccess `
        -AutoMapping:$false
```

Important Notes
- Do not use ApplicationImpersonation
- Removing FullAccess - To revoke a previously granted FullAccess permission:
  ```
  Remove-MailboxPermission -Identity "user-to-restore-to@bob.com" `
          -User "bob@bob.com" `
          -AccessRights FullAccess `
          -InheritanceType All
  ```

Behaviour of FullAccess
- Grants the ability to open and manage mailbox content (does not allow Send As or Send on Behalf).
- Inherits permissions by default unless specified otherwise.
- When removing, always include -InheritanceType All to match the original grant.

FAQ

Q: Can I still use app-only authentication for Veeam Explorer restores?
No. Cross-mailbox restores require delegated permissions and an interactive sign-in.

Q: Does granting FullAccess allow sending emails as the mailbox owner?
No. FullAccess only allows opening and reading mailbox content. Send permissions require separate configuration.

Q: Is there an easier way for large restores?
Yes, create a **security group** and grant that group FullAccess to multiple mailboxes for simplified management.