Customer Action Plan for EWS retirement

Last Modified on 09/08/2026 10:13 am EDT

You can ensure EWS retirement will not affect your instance of PoliteMail with the following six steps.

Step 1 — Determine how your PoliteMail environment expands lists

Check **Settings > App Settings > List Expansion Methods Enabled** in PoliteMail. It is a Client/Server grid with rows for EWS, Graph, and MAPI. If you have server access, the same values live in the User Expansion Modes preference in user_preferences_tbl, with admin locks in override_user_preferences_tbl; stored values are some combination of GraphServer, GraphClient, EWSServer, EWSClient, and MAPI.

- **Graph configured and no DDLs in use:** No action beyond Step 4.
- **Graph configured but DDLs in use:** Go to Step 2.
- **EWS only, no Graph:** Go to Step 3. This is the highest-urgency case.

Step 2 — Migrate Exchange Dynamic Distribution Lists

For each DDL PoliteMail sends to, recreate the equivalent membership as an **Entra/Microsoft 365 Dynamic Group**. The underlying recipient filter usually translates directly into a dynamic membership rule. Once the group exists, Graph can enumerate membership and PoliteMail can expand it without EWS.

Alternatives if a DDL cannot be converted:

- Import the list into PoliteMail as a PoliteMail list.
- Use Syncronym to source membership from your directory or data warehouse.
- Where the source of truth is an HR or identity system, sync into a static group on a schedule.

Contact PoliteMail Support if you would like help identifying which of your lists are DDLs.

Step 3 — Configure Microsoft Graph

If your environment has never had Graph configured, this is the long-term fix and should be scheduled now. PoliteMail Support can walk your Exchange/Entra admin through the app registration and permission grant. Reference: PoliteMail Graph permissions.

Step 4 — Decide whether you need a short-term EWS allow list

If you cannot complete DDL migration before your tenant is disabled, you can buy time using the tenant-level allow list. In Exchange Online PowerShell:

```
# Inspect current state (the app ID list is only returned with this switch)
Get-OrganizationConfig -RetrieveEwsOperationAccessPolicy | Format-List EwsEnabled, EwsAllowedAppIDs
```

```
# Enable EWS and scope it to approved application IDs (comma-separated string)
Set-OrganizationConfig -EwsEnabled $true -EwsAllowedAppIDs "<PoliteMail application (client) ID>"
```

```
# To allow more than one app, list every ID in one string; the value replaces the previous list
Set-OrganizationConfig -EwsAllowedAppIDs "<app id 1>,<app id 2>"
```

Important caveats:

- The allow list is a bridge, not an exemption. It stops working on **April 1, 2027**.
- After October 1, 2026, EWSEnabled=True **without** an allow list blocks all EWS traffic. Setting the flag alone is not enough.
- EwsAllowedAppIDs is a single comma-separated string, not a multi-valued property, so @{Add=...} syntax does not work and each call replaces the whole list. Pass $null to clear it.
- Changes to the allow list can take up to 24 hours to take effect.
- EwsAllowList and EwsBlockList are the older user-agent based lists and are unrelated to EwsAllowedAppIDs.
- Confirm the exact application ID with PoliteMail Support before adding it; it is the client ID of the app registration your PoliteMail server uses.
- Microsoft states the allow list can also be maintained through Baseline Security Mode in the Microsoft 365 admin center.

Step 5 — Check your app registration for a shared-permission trap

We have seen SSO break for customers when EWS was disabled, because Microsoft Graph and EWS API permissions were configured on the **same** Azure app registration. The correct remediation is to remove the unnecessary EWS API permission from the registration, not to disable the shared app. Verify this before your tenant hits enforcement so you do not lose sign-in at the same time you lose list expansion.

Step 6 — Test before October

Ask your Exchange admin to run a controlled test in a non-production or pilot tenant:

Set-OrganizationConfig -EwsEnabled:$false

Then attempt a PoliteMail send to each of your major lists. Anything that fails to expand is a dependency you need to remediate. Re-enable afterward.

Separate licensing enforcement
Since March 1, 2026 Microsoft has enforced EWS licensing terms that were previously unenforced (message center MC1191578). Mailboxes licensed exclusively with Exchange Online Kiosk, Microsoft 365/Office 365 F1, or Microsoft 365/Office 365 F3 receive HTTP 403 responses on EWS calls, regardless of the allow list. If the mailbox PoliteMail accesses over EWS sits on a frontline SKU, verify licensing before assuming a configuration problem.