Restricting Application Permissions to Specific Mailboxes

The Graph API only allows all or no mailboxes. However, Microsoft released documentation to limit registered applications to specific mailboxes listed [here](https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access).

To help assist implementing least privileged access, we have provided guidance for setting up a new mail-enabled security group listed below.

**Note:** You will need the Exchange Online module in PowerShell. [See here](https://www.powershellgallery.com/packages/ExchangeOnlineManagement/3.0.0) to add the module to PowerShell and [here](https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps) on how to connect.

1. Navigate to the **App Registrations** page within Azure and click on the Meter Email Parser registration. Identify the Application Client ID in Azure.
2. Log in to **Microsoft Office 365 Exchange Admin Center** and navigate to Groups.
3. Create a new mail-enabled security group or use an existing one and identify the email addresses to be included.



* 1. Select Mail-Enabled Security group



* 1. Give it a name, preferably one that would help identify that group later. Assign an owner to the group.



* 1. Add the mailbox(es) which requires access.



* 1. Give the group an address.

 

1. Connect to **Exchange Online** via Powershell.
2. Run New-ApplicationAccessPolicy -AppId XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXX -PolicyScopeGroupId AllowCJAccess@Domain.com -AccessRight RestrictAccess -Description "Restrict this app to members of distribution group AllowCJAccess" (Replace AppID with Application Client ID / Security Group email address).



1. Test Application Permissions.
Test-ApplicationAccessPolicy -Identity XXXX@Domain.com -AppId XXXXXXXX-XXXX-XXXX-XXXX- XXXXXXX
	1. **Note:** AccessCheckResult will show Granted for mailboxes available to the application.

