Restrict App Registration application permission to certain mailboxes

> Requirements: Active Exchange Administrator Role and App Registration with application permissions granted.

Application Access Polices

Generally Application Permissions allow an Azure App Registration to access a certain type of data within the whole tenant.

For example the Application Permission Calendars.ReadWrite grants access to every calendar in every mailbox in the Exchange Online environment.

Use case

If, for example, you want to grant an App Registration the Read and Write permission on just 15 calendars, you can do so with an Application Access Policy.

Creating an Application Access Policy

To create an Application Access Policy, you first have to create your App Registration and grant the any Application permission (e.g. Mail.Send).

After that you need to create a Mail Enabled Security Group in the Exchange Admin Center and add the Mailboxes, on which the App Registration' permission shall be activated.

Now you can create the Application Access Policy with the following Command. First you have to log in to Exchange Online.

```
Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline
```

```
New-ApplicationAccessPolicy -AppId "<appregistrationid>" -PolicyScopeGroupId
"<PrimarySMTPAddressofMESG>" -Description "<yourcustomdescription>" -AccessRight Restrict
```

View existing Application Access Policies

If you want to view all existing Application Access Policies in your Tenant, you can do so with this command.

```
Get-ApplicationAccessPolicy
```

For more readability you can view this output in a gridview.

```
Get-ApplicationAccessPolicy | Out-GridView
```

Revision #14
Created 8 December 2022 16:06:04
Updated 21 July 2024 15:10:58