

Guide: How to Control Access to Calendars

deskbird Workplace Platform

Last updated: **March 2023**

Granting consent during the onboarding process allows Graph API access to all calendars in a Microsoft 365 tenant. We recommend applying an Application Access Policy and Management Scope to restrict access to specific calendars only. The Application Access Policy can either restrict or deny Graph API access to members of a mail-enabled security group.

There are two types of permissions that can be applied to the Application Access Policy, depending on whether you wish to allow or deny access to the mailboxes added to the mail-enabled security group.

- a) Use **DenyAccess** to deny access to mailboxes in the group and allow access to all other mailboxes.
- b) Use **RestrictAccess** to allow access to mailboxes in the group and restrict access to all other mailboxes.

Learn more about `New-ApplicationAccessPolicy` at Microsoft <https://docs.microsoft.com/en-us/powershell/module/exchange/new-applicationaccesspolicy?view=exchange-ps/>

How to set up an Application Access Policy:

Use the following PowerShell scripts to create a new mail-enabled security group, create an Application Access Policy and create the Management Scope, to restrict access to specific mailboxes.

1. Login with your Microsoft 365 admin account and then run the following scripts to create the session.

```

1 1. Set-ExecutionPolicy RemoteSigned
2 2. $UserCredential = Get-Credential
3 3. Connect-ExchangeOnline -Credential $UserCredential
4 4. $Session = New-PSSession -ConfigurationName Microsoft.Exchange -
   ConnectionUri https://outlook.office365.com/powershell-

```

```
5 | liveid/ -Credential $UserCredential -Authentication Basic -  
AllowRedirection  
5. Import-PSSession $Session -AllowClobber
```

2. Check your Microsoft 365 Service account does not have full impersonation rights.

```
1 | Get-ManagementRoleAssignment -RoleAssignee "Enter service account name"
```

3. Create a new mail-enabled security group to manage the mailboxes that you will either allow or deny access to.

```
1 | New-DistributionGroup -Name "Enter the name of new security group" -  
Alias "Enter the Alias" -Type security
```

4. Create an Application Access Policy on the mail-enabled security group.

```
1 | New-ApplicationAccessPolicy -AccessRight RestrictAccess -AppId "Enter  
Token Provider AD App ID" -PolicyScopeGroupId "Enter Email Enabled  
Security Group Mailbox ID" -Description "Restricted Access Group Policy"
```



-AccessRight: Replace "RestrictAccess" with "DenyAccess" to deny access to the calendars in the security group and allow access to all other calendars.

-Appld: 60e10e49-86e8-4755-ac34-2804c82237c6

5. Request the group identity (needed when mailboxes are added to the security group)

```
1 | $DG = Get-DistributionGroup -Identity "Enter Group Mailbox ID"
```