

How to Grant Application Impersonation Rights in Office 365?

Application Impersonation is an Exchange Online feature. With the help of this feature, the Administrator can set permissions for a software application. Many Administrators use this option for CRM integration, scheduled local backups, data migration to Office 365, etc.

Configure Impersonation in Office 365 using Exchange admin center

1. Go to <https://outlook.office365.com/ecp>
2. Log in with your Office 365 credentials.
3. Select the Permissions option from the screen.
4. Click on the "+" icon to add a new role group.
5. Provide a Name, Description, and click on the "+" icon from the Roles.
6. Select the ApplicationImpersonation option from the list.
7. Click on the Add and OK button.
8. Click on the "+" icon from the Members.
9. Select Administrator, click on Add, and OK button.
10. Finally, click on the Save button.

Note: If you are importing all user's mailboxes at once, then you need to provide a few more permissions.

Grant Full Access to Admin Mailbox

1. Select Recipients from the Exchange Admin Center.
2. Double click on the mailbox.
3. Select the Mailbox Delegation option from the Edit User Mailbox screen.
4. Click on the "+" icon from Full Access.
5. Select the Admin mailbox from Select Send on Behalf screen.
6. Click on the Add and OK button.
7. Finally, Click on Save.

Note: We have given permission for one mailbox. To provide permission for more mailboxes, you have to repeat these steps for each mailbox.

Application Impersonation Rights in Office 365 using PowerShell

To configure the ApplicationImpersonation role, you need:

1. Administrative credentials for the Exchange server.
2. Domain Administrator credentials to create and assign roles and scopes.
3. Exchange management tools. These are installed on the computer from which you will run the commands.

Configure impersonation for all users in an organization

1. Open Exchange Management Shell.
2. Go to the Start and choose All Programs.
3. Select Microsoft Exchange Server 2013.
4. Run the New-ManagementRoleAssignment cmdlet.

Example:

```
New-ManagementRoleAssignment -name:impersonationAssignmentName  
-Role:ApplicationImpersonation -User:serviceAccount
```

Configure impersonation for specific users or groups of users

1. Open Exchange Management Shell.
2. Go to the Start and choose the All Programs.
3. Select Microsoft Exchange Server 2013.
4. Run the New-ManagementScope cmdlet to create a scope. (If the existing scope is available, then skip this step.)

Example:

Creating a management scope for a specific group.

```
New-ManagementScope -Name:scopeName -RecipientRestrictionFilter:recipientFilter
```

Run the New-ManagementRoleAssignment cmdlet to set the permission to impersonate the members of the specified scope

```
New-ManagementRoleAssignment -Name:impersonationAssignmentName  
-Role:ApplicationImpersonation -User:serviceAccount -CustomRecipientWriteScope:scopeName
```