(/kb/)

Search our Knowledge Base:

How to set impersonation rights manually

Problem:

How to manually manage impersonation rights for an administrator account.

Solution:

Use the links below to learn how to add impersonation rights to your admin account via:

Windows PowerShell

Exchange admin center (applies to Exchange 2013, 2016 and Office 365 only).

Add impersonation rights in PowerShell

1. Run Windows PowerShell.
2. Check your PowerShell version by typing the following cmdlet:

```
$PSVersionTable
```

An empty response means that you are using version 1.0.

For versions 2.0 and newer, you should see a detailed answer.

We recommend that you keep PowerShell updated to avoid compatibility problems. To download the newest version of PowerShell, please visit this Microsoft website (http://technet.microsoft.com/en-us/library/hh847837.aspx).

3. If your Exchange server is in a remote location (for example, it is hosted) or you are connecting to Office 365 (Exchange Online), learn how to connect to remote Exchange via PowerShell (https://www.codetwo.com/kb/how-to-connect-to-exchange-server-via-powershell/). To manage permissions locally (if you have an on-premises Exchange server or if you are logged on to a remote Exchange server via Remote Desktop, etc.) execute the commands below in Exchange Management Shell.
4. Check if the account in question already has impersonation rights assigned by executing this cmdlet:

```
Get-ManagementRoleAssignment -RoleAssignee "<account name>" -Role ApplicationImpersonation -RoleAssigneeType user
```

where `<account name>` is the name of the administrator account (on the target server) that you want to check.

5. Add impersonation rights:

```
New-ManagementRoleAssignment –Name:<impersonation Assignment Name> –Role:ApplicationImpersonation –User: "<account
```

where `<impersonation Assignment Name>` is the name of your choice for this assignment. Be aware that each assignment should have a unique name. You can omit the `Name` switch, and a unique assignment name will be created automatically.

6. If necessary, you can also restrict these impersonation rights so that they apply to a specific group of users. To do so, you first need to define a management scope that includes your AD group:

```
$ADGroup = Get-DistributionGroup -Identity "<group name>"
New-ManagementScope "<scope name>" -RecipientRestrictionFilter "MemberOfGroup -eq '$($ADGroup.DistinguishedName)'"
```

where `<group name>` is the name of your AD group object, and `<scope name>` is the name of your choice for the new management scope.

Now, modify the existing assignment by using the following cmdlet:

```
Set-ManagementRoleAssignment "<impersonation Assignment Name>" -CustomRecipientWriteScope "<scope name>"
```

7. You can remove impersonation rights with this command, if necessary:

```
Get-ManagementRoleAssignment -RoleAssignee "<account name>" -Role ApplicationImpersonation -RoleAssigneeType user
```

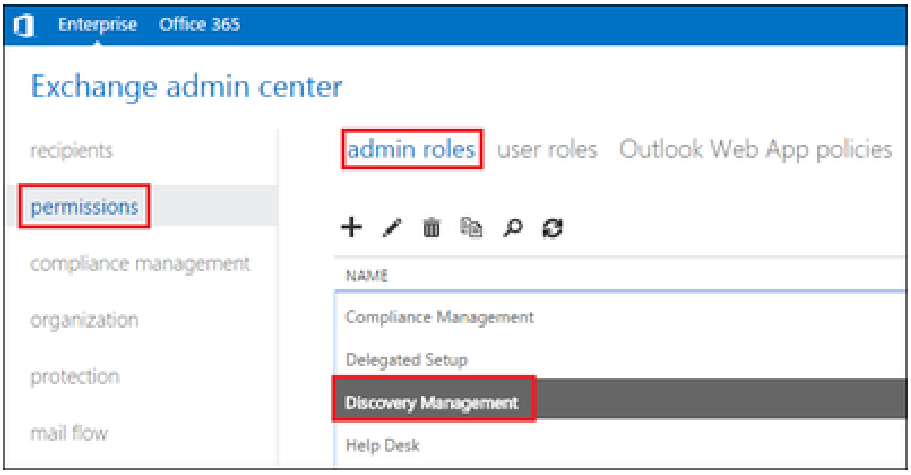
Add impersonation rights in Exchange admin center (EAC)

1. Open **Exchange admin center**:

    in Office 365: log in to your Microsoft Office 365 admin center (Office 365 admin center) as an admin and choose **Admin centers** > **Exchange** from the menu on the left.

    in Exchange 2013 and 2016: log in to **Exchange admin center** (`https://localhost/ecp`).

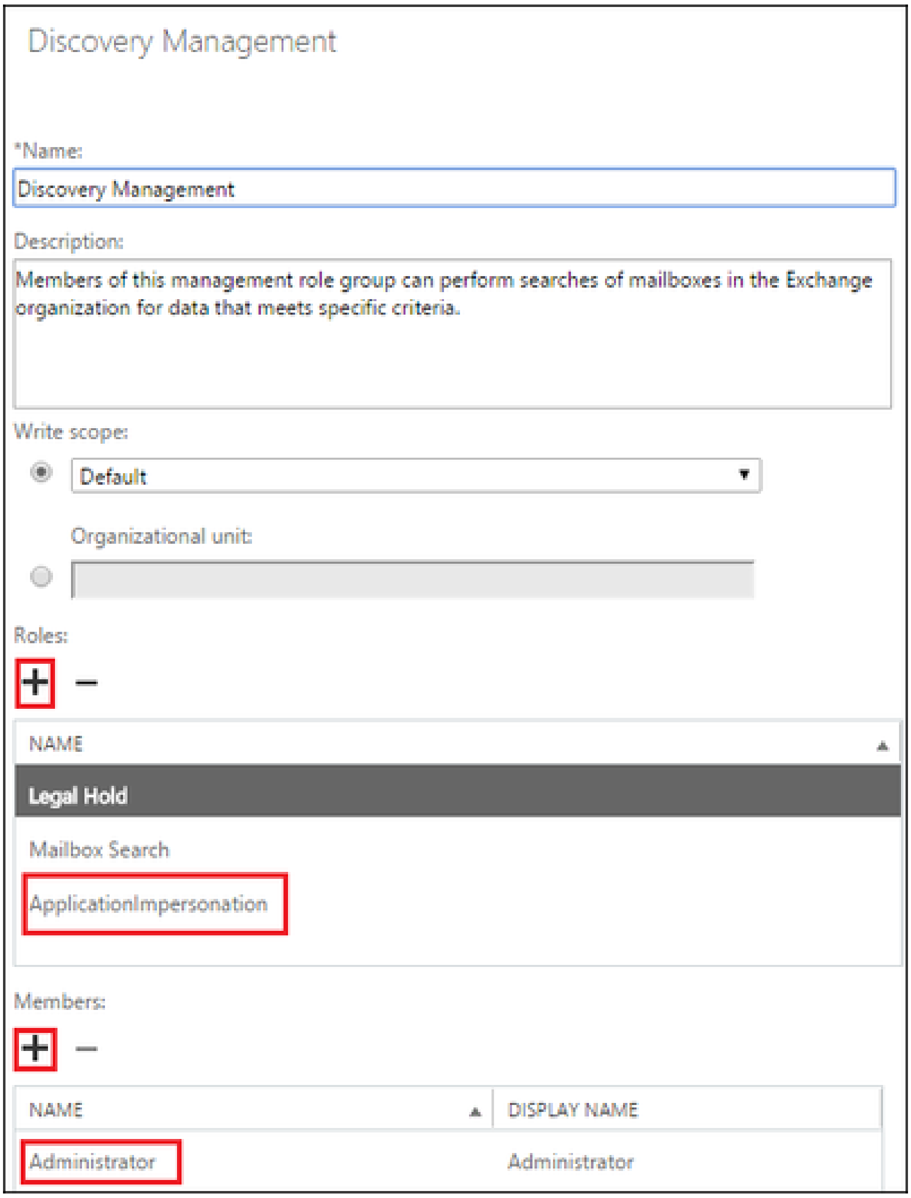
2. Go to **Permissions** > **admin roles** (**Fig. 1.**) and edit the **Discovery Management** role by double-clicking it:



(/media/images/2-37.png)

Fig. 1. The Discovery Management role in EAC.

3. Add the role **ApplicationImpersonation** and add your admin user as the group member (**Fig. 2.**).



Discovery Management

*Name: Discovery Management

Description: Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Write scope:

● Default

○ Organizational unit:

Roles:

NAME
Legal Hold
Mailbox Search
ApplicationImpersonation

Members:

NAME	DISPLAY NAME
Administrator	Administrator

(/media/images/3-25.png)

Fig. 2. How to add the right roles and users.

Note that according to Microsoft (http://community.office365.com/en-us/f/148/t/192823.aspx), in the Office 365 Small Business plans impersonation rights cannot be assigned manually. The default built-in admin account is the only one who can hold such permissions.

See also:

MS Technet on New-ManagementRoleAssignment cmdlet in Exchange Server (https://technet.microsoft.com/en-us/library/dd335193%28v=exchg.141%29.aspx)

How to allow PowerShell to connect to Exchange Server over IP address (https://www.codetwo.com/kb/powershell-over-ip/)

G+ Tweet Share Like 1 Share 1

Applies to:
CodeTwo Backup for Exchange (https://www.codetwo.com/backup-for-exchange/)
CodeTwo Backup for Office 365 (https://www.codetwo.com/backup-for-office-365/)
CodeTwo Email Signatures for Email Clients (https://www.codetwo.com/email-signatures-for-email-clients/)
CodeTwo Exchange Migration (https://www.codetwo.com/exchange-migration/)
CodeTwo Office 365 Migration (https://www.codetwo.com/office-365-migration/)

Categories: How-To

Last modified: 2018-07-16

Created: 2013-08-26

ID: 285

Keywords: impersonation, rights, permissions, exchange, migration