Required Permissions

This section describes required permissions for user accounts that are going to be used to back up and restore organizations data.

For Backup

Required Permissions for Veeam Backup for Microsoft Office 365

By default, Veeam Backup for Microsoft Office 365 (Veeam Backup for Microsoft Office 365 Service) uses the Local System account. This account has administrative rights on the local machine and should not be changed for Veeam services.

Required Permissions for SharePoint and OneDrive for Business Organizations

The account that is used to connect to Microsoft SharePoint organizations (On-Premises or Online) must belong to that organization and must conform to the following:

- **For SharePoint On-Premises.**

The account must be a member of the Farm Administrator group and must have the Site Collection Administrator role. This role can be assigned either automatically, when adding a new SharePoint organization, or manually. For more information on adding new organizations, see Adding Microsoft Organizations.

- **For SharePoint Online.**

The account must have either the Global Administrator role, or the SharePoint Administrator role.

If you prefer to use PowerShell to assign the SharePoint Administrator role for SharePoint Online organizations, you can use the following code snippet.

```
Connect-MsolService

$role=Get-MsolRole -RoleName "SharePoint Service Administrator"

$accountname=UPN

Add-MsolRoleMember -RoleMemberEmailAddress $accountname -RoleName $role.Name
```

The MSOL module can be downloaded here.

The $accountname parameter must be a user's UPN (for example, user.name@domain.com).

Required Permissions for Exchange Organizations:

The account that is used to connect to Microsoft Exchange organizations (On-Premises or Online) must belong to that organization, having a mailbox in that organization is optional.

This account must have the following Exchange roles assigned:

- The Role Management role. To grant **ApplicationImpersonation** role.
- The **ApplicationImpersonation** role. To assign this role, the account must be a member of the **Organization Management** group. This role can be assigned by using any of the following methods:
    - Automatically, when adding Exchange organizations.
    - Manually, by using Exchange Management PowerShell cmdlets.
    - Using the Microsoft Exchange control panel. For more information, see this Microsoft article.
- The **Organizations Configuration role**. To manage role assignments.
- The **View-Only Configuration role**. To obtain necessary organization configuration parameters.
- The **View-Only Recipients role**. To view mailbox recipients (required for back job creation).
- **MailboxSearch** or **MailRecipients**. To back up groups.

Assigning ApplicationImpersonation Role via PowerShell

For Microsoft On-Premises Organizations:

To assign the ApplicationImpersonation role for On-Premises organizations using PowerShell, do the following:

1. *Connect to the Exchange server.*

- $UserCredential = Get-Credential

  $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri http://exchangeServerName/PowerShell/ -Authentication Kerberos -Credential $UserCredential

  Import-PSSession $Session

2. Use the following cmdlet to grant the role.
- New-ManagementRoleAssignment –Role ApplicationImpersonation –User "Administrator"

For Microsoft Online Organizations

To assign the ApplicationImpersonation role for Online organizations using PowerShell, do the following:

1. *Connect to the Exchange server.*
- $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri

  https://outlook.office365.com/powershell-liveid/ -Credential $Credential -Authentication Basic -AllowRedirection

Import-PSSession $Session

2. *Use the following cmdlet to grant the role.*
- New-ManagementRoleAssignment –Role ApplicationImpersonation –User user.name@domain.com

To obtain the list of users whom the ApplicationImpersonation role has already been granted, use the following cmdlet (for both On-Premises and Online organizations).

- Get-ManagementRoleAssignment -Role "ApplicationImpersonation"

To remove the role, use the following cmdlet (for both On-Premises and Online organizations).

- Get-ManagementRoleAssignment -RoleAssignee "Administrator" -Role ApplicationImpersonation -RoleAssigneeType user | Remove-ManagementRoleAssignment

For Restore:

- To connect to the Veeam Backup for Microsoft Office 365 server from Veeam Explorers, the account you are using must be a member of the **local Administrator group**.
- To resolve mailboxes in Veeam Explorer for Microsoft Exchange and filter Exchange System Mailboxes, the account you are using must be configured according to the following:
    - The account is a member of the **Administrators** or **Organization Management** group.
    - The account has been granted the **Read** permission for the **objectClass** attribute of the Microsoft Exchange System Object container.

      *Make sure to select the **Apply these permissions to objects and/or containers within this container only** option. If the Read permission was not granted for the account that is a member of the Authenticated users group, Veeam Explorer will not be able to recover Exchange system mailboxes.*

- The account you are using to restore data to a public folder must own a mailbox on a target Microsoft Exchange server.
- To restore folders/items back to Exchange Online organizations, the account you are using in the restore wizard requires sufficient privileges to access the target production server.
- To restore to On-Premise Microsoft Exchange organizations, the account you are using in the restore wizard requires the following:
    - When using the account that owns a mailbox on a target server, make sure it has Full Access, which can be granted, for example, through impersonation or via rights assignment with the following cmdlet.
        - *Add-MailboxPermission –Identity "<target_mailbox>" -User "<user_account>" -AccessRights FullAccess –InheritanceType All*

When using the account that does not own a mailbox on a target server (for example, a service account), then access rights for the target mailbox must be granted through Exchange impersonation. For example, by running the following cmdlet.

New-ManagementRoleAssignment -Name "<role_name>" -Role ApplicationImpersonation -User "<user_account>" [-CustomRecipientScope "<scope>"]

The following cmdlet demonstrates how to narrow the group of users whom appropriate roles will be assigned to access the target mailbox. The CustomRecipientScope parameter is used with sample Organizational Unit specified as the scope.

New-ManagementRoleAssignment -Name "Exchange Test" -Role ApplicationImpersonation -User "Test User" -CustomRecipientScope "spain.local/TargetUsers"

Recalling Privileges Granted Through Impersonation:

To recall given privileges, run the following cmdlet.

Remove-ManagementRoleAssignment -Name "<role_name>"