

VEEAM



How to start with modern authentication in Veeam Backup *for Microsoft Office 365 v3*

Revision #2, June 2019

Polina Vasileva

Analyst, Veeam Software



Contents

Modern authentication in Veeam Backup <i>for Microsoft Office 365</i>	2
How to register a custom application in the Azure Active Directory portal	2
How to get your Application ID	7
How to get your Application secret	8
How to configure an MFA-enabled service account.....	10
How to grant a service account required roles and permissions	10
How to get an app password for an MFA-enabled service account	12
For a newly created service account:	12
For an existing service account:	13
How to add to the Veeam <i>Backup for Microsoft Office 365</i> scope, an Office 365 organization using modern authentication..	14
About Veeam Software.....	16

Modern authentication in Veeam Backup *for Microsoft Office 365*

Veeam® Backup *for Microsoft Office 365 v3* supports connecting to Office 365 using modern authentication and this paper will guide you through the pre-configuration steps to take for a seamless setup.

When adding an organization to the Veeam Backup *for Microsoft Office 365* scope with modern authentication, you need to provide two sets of credentials: custom Azure application credentials and MFA-enabled service account credentials.

A custom application to be used by Veeam Backup *for Microsoft Office 365* must be registered in your Azure Active Directory portal in advance. Veeam will utilize this application to access the Microsoft Graph API and retrieve your Microsoft Office 365 organization's data.

A service account must be enabled for multi-factor authentication (MFA) and granted the required roles and permissions. Note that when adding an organization, you will need to provide a username and app password for the service account.

Important note: While fully supporting modern authentication and MFA-enabled accounts, Veeam Backup *for Microsoft Office 365* must fill in the existing gaps in API support with the following requirements for basic protocols usage:

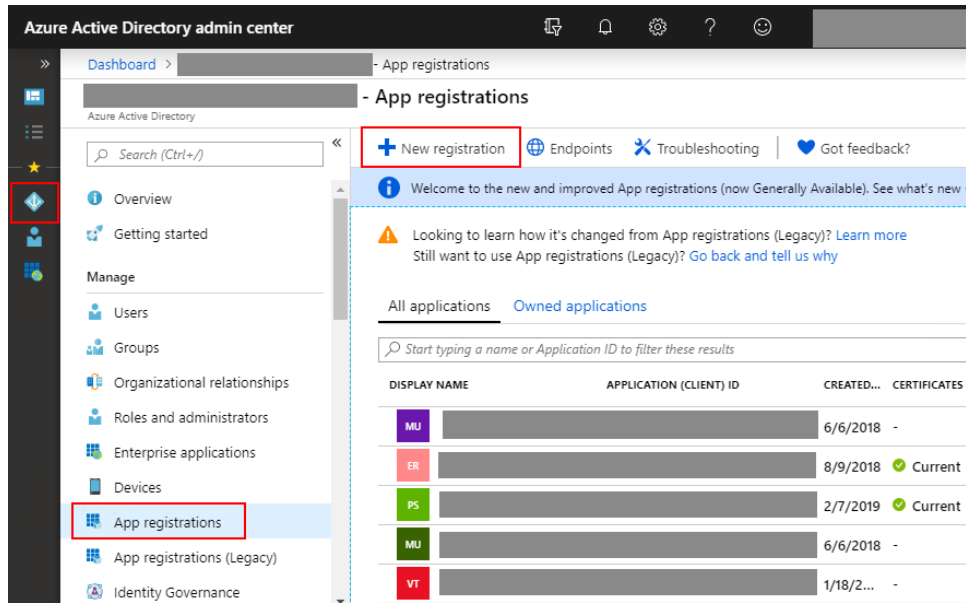
- Basic authentication for Exchange Online PowerShell
 - *AllowBasicAuthPowershell* must be enabled (set to True) for a service account used by Veeam Backup *for Microsoft Office 365*. It is required to get the correct information on licensed users, users' mailboxes, etc. Note that to minimize the footprint for a possible security breach, you can enable this authentication protocol for a single service account used by Veeam Backup *for Microsoft Office 365* and disable it for all other users in your Office 365 organization. For more information, see this [Microsoft article](#).
 - *AllowBasicAuthWebServices* can be disabled within your Office 365 organization for all users, including a service account used by Veeam Backup *for Microsoft Office 365*. In this case, you will need to use the Application certificate when connecting to Office 365 with a modern authentication.
- Basic authentication for SharePoint Online
 - *LegacyAuthProtocolsEnabled* must be set to \$True in your Office 365 organization. This authentication protocol is required for Veeam Backup *for Microsoft Office 365* to be able to work with specific SharePoint services, including (but not limited to) ASMX services. ASMX services allow you to access the customized Web Parts, which are the building blocks of modern site pages. Providing Veeam Backup *for Microsoft Office 365* an access to web parts, you can protect text, images, files, video, dynamic content and more added to your SharePoint site page.

How to register a custom application in the Azure Active Directory portal

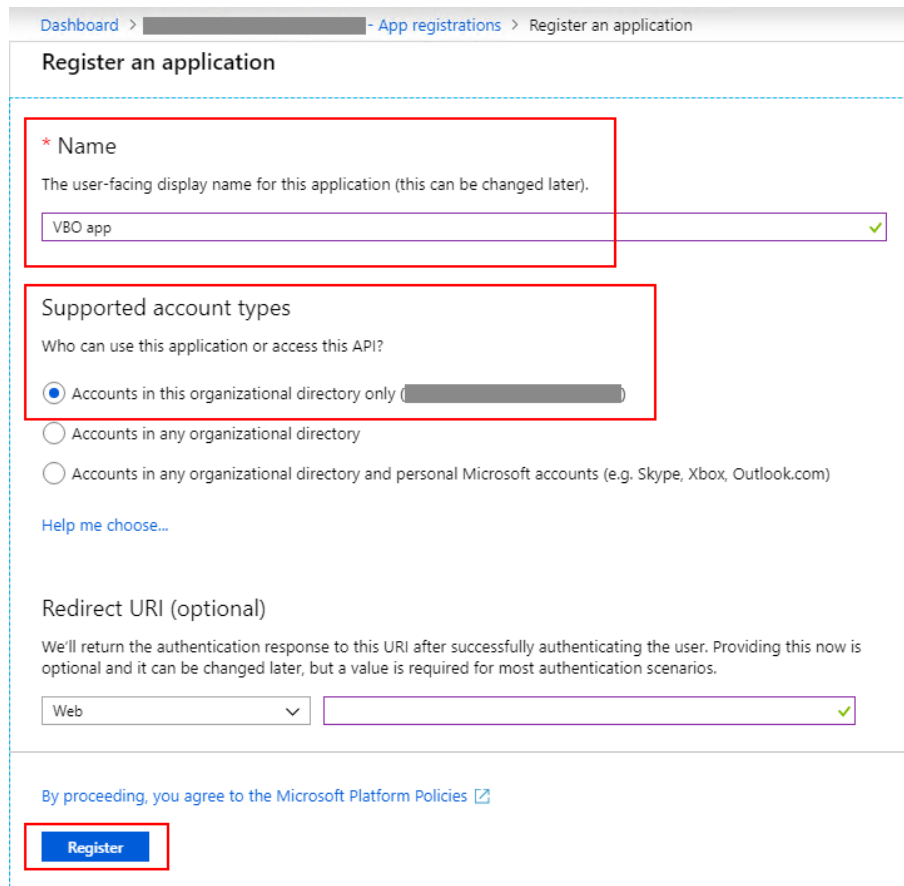
When using modern authentication, Veeam Backup *for Microsoft Office 365* requires Azure application credentials, such as application ID and application secret or application certificate. You can get these credentials on the Office 365 Azure Active Directory portal upon registering a new application in the Azure Active Directory.

To be able to register a new application, your Office 365 account must have one of the following roles: Global Administrator, Application Administrator or Cloud Application Administrator.

1. Sign into the Microsoft 365 Admin Center and navigate to Admin centers -> Azure Active Directory -> App registrations. Select New registration to add a custom application to the list of registered applications:



2. Add the app name, select Accounts in this organizational directory only as the supported account type. Application redirect URI is optional, so you can leave it blank on this step. Click Register:



- To grant your new application the required permissions, select View API Permissions in the app Overview section or navigate to the API permissions section:

Dashboard > [redacted] - App registrations > VBO app

VBO app

- Overview
- Quickstart
- Manage
 - Branding
 - Authentication
 - Certificates & secrets
 - API permissions
 - Expose an API
 - Owners
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Delete Endpoints

Display name: VBO app
Application (client) ID: [redacted]
Directory (tenant) ID: [redacted]
Object ID: [redacted]

Supported account types: My organization only
Redirect URIs: Add a Redirect URI
Managed application in local directory: VBO app

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API Permissions](#)

Documentation

- Microsoft identity platform
- Authentication scenarios
- Authentication libraries
- Code samples
- Microsoft Graph
- Glossary
- Help and Support

Dashboard > [redacted] - App registrations > VBO app

VBO app

- Overview
- Quickstart
- Manage
 - Branding
 - Authentication
 - Certificates & secrets
 - API permissions
 - Expose an API
 - Owners
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Delete Endpoints

Display name: VBO app
Application (client) ID: [redacted]
Directory (tenant) ID: [redacted]
Object ID: [redacted]

Supported account types: My organization only
Redirect URIs: Add a Redirect URI
Managed application in local directory: VBO app

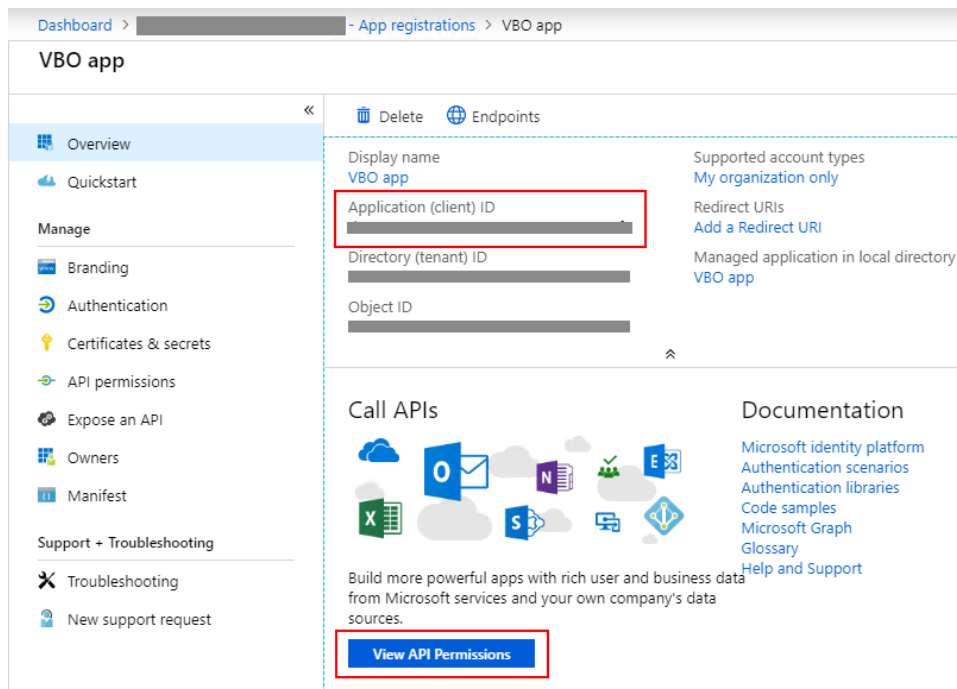
Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API Permissions](#)

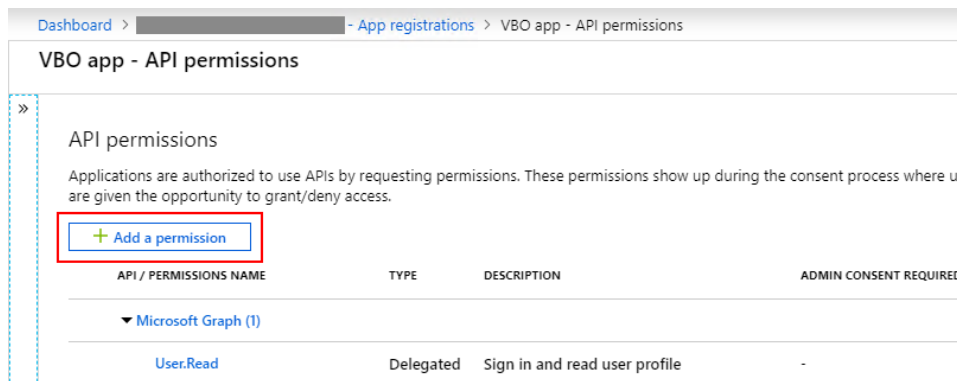
Documentation

- Microsoft identity platform
- Authentication scenarios
- Authentication libraries
- Code samples
- Microsoft Graph
- Glossary
- Help and Support

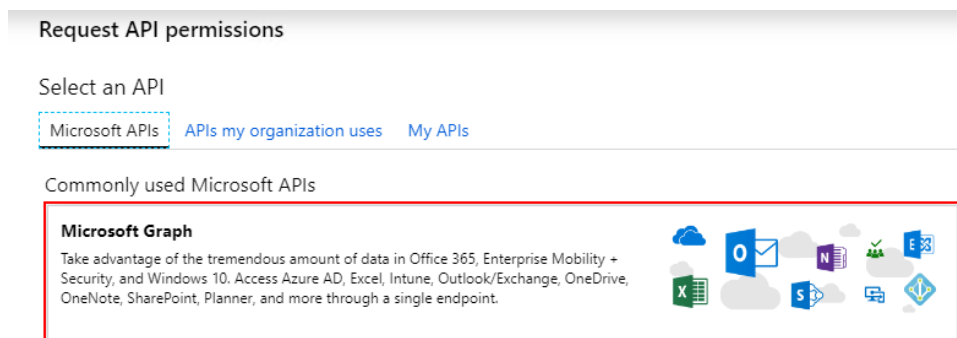


By default, the new application is granted with a *User.Read* delegated permission for Microsoft Graph. This permission is not required for Veeam Backup for Microsoft Office 365 and can be removed if you like.

4. Click **Add a permission:**



5. Select **Microsoft Graph** from the list of commonly used Microsoft APIs:



- Grant your new application the required permissions. Azure AD applications can have either Delegated or Application permissions. Delegated permissions require a signed-in user present, who consents to the permissions every time an API call is sent, while Application permissions are consented by an administrator once granted. Veeam Backup for Microsoft Office 365 acts as a service and requires Application permissions. Select **Directory.Read.All** (Read directory data) and **Group.Read.All** (Read all groups) from the list of available permissions, and click **Add permissions**:

Request API permissions

[← All APIs](#)
 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

PERMISSION	ADMIN CONSENT REQUIRED
▶ AccessReview	
▶ AdministrativeUnit	
▶ Application	
▶ AuditLog	
▶ Calendars	
▶ Calls	
▶ ChannelMessage	
▶ Chat	
▶ Contacts	
▶ Device	
▼ Directory (1)	
<input checked="" type="checkbox"/> Directory.Read.All Read directory data	Yes
<input type="checkbox"/> Directory.ReadWrite.All Read and write directory data	Yes

Add permissions
Discard

- If you want to add your tenant organization to the Veeam Backup for Microsoft Office 365 scope using a certificate, you must additionally select the following API and corresponding Application permissions when registering a new application:

- **Exchange** with **full_access_as_app** (Use Exchange Web Services with full access to all mailboxes) permissions;
- **SharePoint** with **Sites.FullControl.All** (Have full control of all site collections) permissions.

- Application permissions will allow your client application to access the Microsoft Graph web API directly as itself (no user context). This type of permission requires administrator consent. To grant administrator consent, click **Grant admin consent for <tenant name>**. Click **Yes** to confirm granting permissions:

Dashboard > [Organization] > App registrations > VBO app - API permissions

VBO app - API permissions

Do you want to grant consent for the requested permissions for all accounts in Veeam Software Group GmbH? This will update any existing admin consent records this application already has to match what is listed below.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (2)			
Directory.Read.All	Application	Read directory data	Yes ⚠ Not granted for [redacted] ...
Group.Read.All	Application	Read all groups	Yes ⚠ Not granted for [redacted] ...

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. [See best practices for requesting permissions](#)

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

✓ Successfully granted admin consent for the requested permissions.

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (2)			
Directory.Read.All	Application	Read directory data	Yes ✓ Granted for [redacted] ...
Group.Read.All	Application	Read all groups	Yes ✓ Granted for [redacted] ...

How to get your Application ID

Once your application is registered in the Azure Active Directory, there are several ways to get its Application ID.

1. Select **Azure Active Directory** -> **App registrations** and navigate to your app listed among the owned or all registered applications:

Dashboard > [Organization] > App registrations

[Organization] - App registrations

Azure Active Directory

Search (Ctrl+/)

- Roles and administrators
- Enterprise applications
- Devices
- App registrations**
- App registrations (Legacy)
- Identity Governance
- Application proxy
- Licenses

+ New registration | Endpoints | Troubleshooting | Got feedback?

Welcome to the new and improved App registrations (now Generally Available). See what's new →

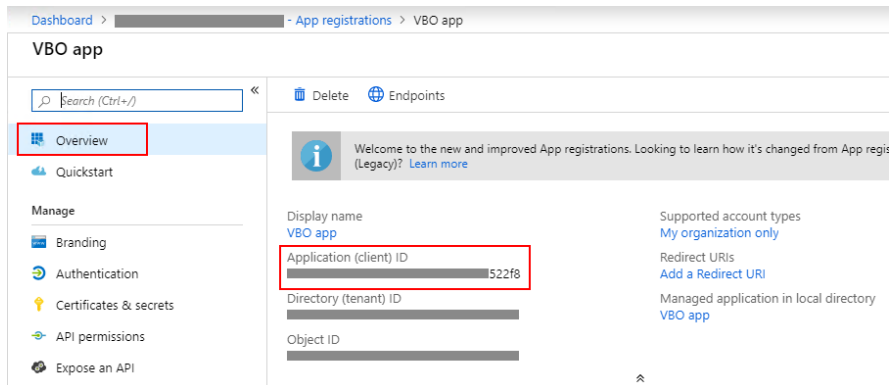
Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
Still want to use App registrations (Legacy)? [Go back and tell us why](#)

All applications | Owned applications

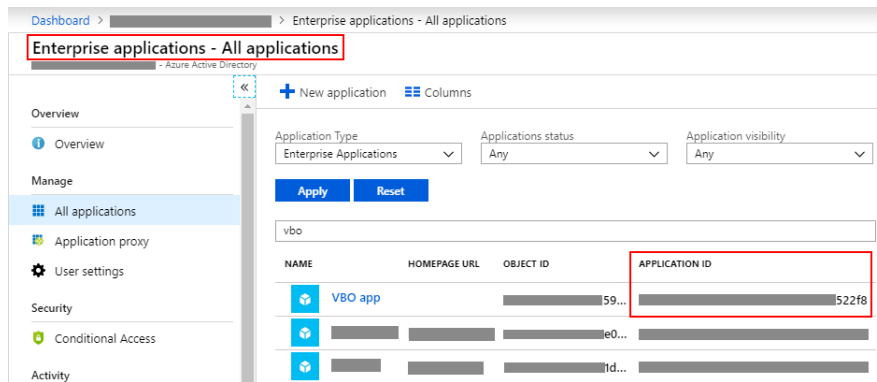
Start typing a name or Application ID to filter these results

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON
VBO app	[redacted] 522f8	6/3/2019

2. On your application's overview page:



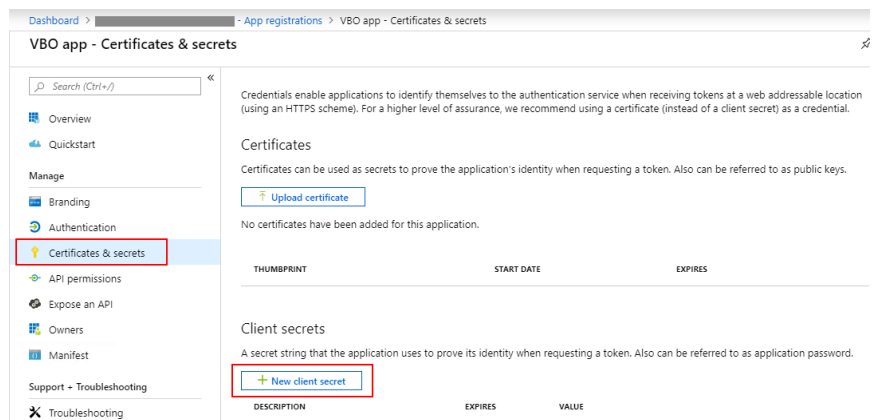
3. Select **Enterprise applications** -> **All applications** and navigate to your app:



How to get your Application secret

To get your Application secret (or Client secret), navigate to **Azure Active Directory** in the Azure Active Directory portal -> **App registrations** and select your app from the list.

On the app overview page, select **Certificates & secrets** -> select **New client secret**. Note that if you want to authenticate via Application certificate instead of Application secret, you can upload it on the same page, as shown on the image below.



Add secret description, its expiration period and select **Add**:

Add a client secret

Description
VBO app secret

Expires
 In 1 year
 In 2 years
 Never

Add Cancel

Copy your new Application secret (Client secret):

Dashboard > App registrations > VBO app - Certificates & secrets

VBO app - Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

THUMBPRINT	START DATE	EXPIRES
No certificates have been added for this application.		

Client secrets

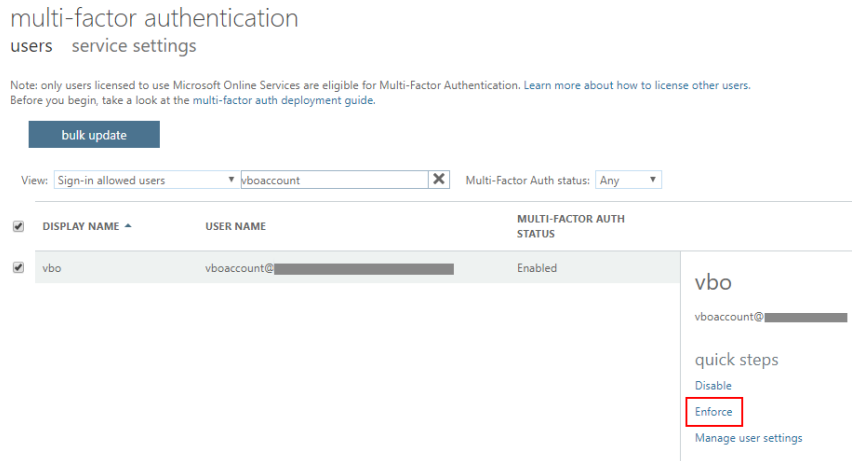
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
VBO app	6/3/2020	[REDACTED]

How to configure an MFA-enabled service account

1. In the Office 365 Admin Center, create a new user without a product license (in our examples below, we'll use the sample username, **vboaccount**).
2. In the user settings, click **Manage multi-factor authentication**, select the user from the list, click **Enable** and confirm the action in the pop-up window. Next, select the user again and click **Enforce** to allow the user create app passwords for non-browser applications, such as Veeam Backup *for Microsoft Office 365*.



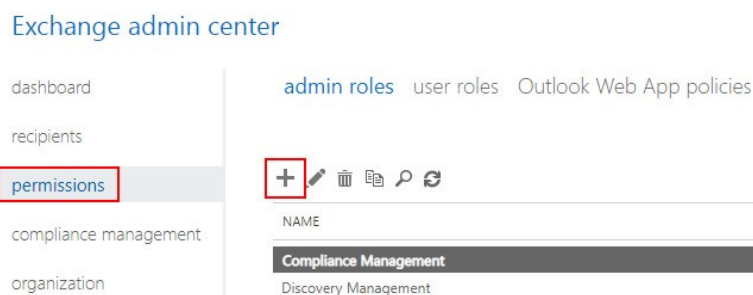
How to grant a service account required roles and permissions

To grant this account required roles and permissions, you can either select them via the Admin Center or assign directly via PowerShell.

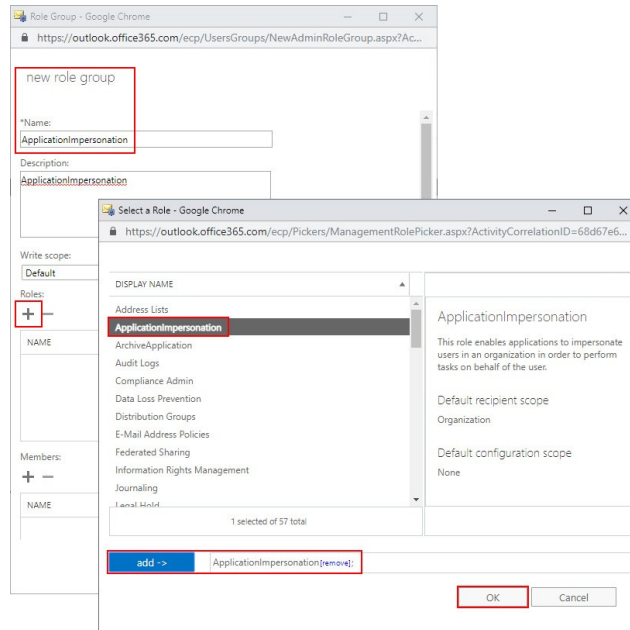
Assigning roles via the Admin Center

To assign roles via the Admin Center, navigate to the user properties, select **Customized administrator** and choose roles corresponding to the services you're going to protect with Veeam:

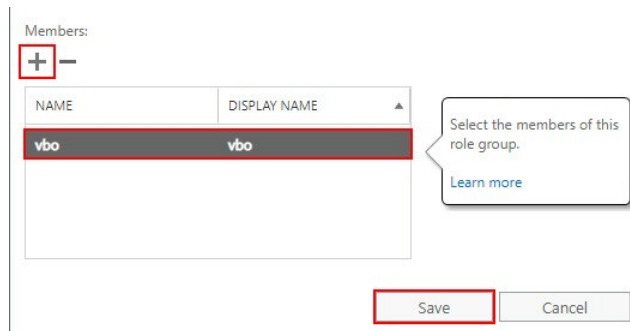
- **For Exchange Online**, Global Administrator or Exchange Administrator. In addition, you need to assign your service account the *ApplicationImpersonation* role as follows:
 - In the Exchange Admin Center, select **permissions** and create a new admin role group:



- Add role group name and description (optional), set the write scope to default and click add roles. Select the **ApplicationImpersonation** role from the list and click **Add**:



- Add your service account to the role group members and click **Save**:



- **For SharePoint Online**, Global Administrator or SharePoint Administrator.

Assigning roles directly via PowerShell

- Run PowerShell as administrator

```
Run Install-Module MSOnline
```

- Connect to Office 365 with your administrator account:

```
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential
$UserCredential -Authentication Basic -AllowRedirection Import-PSSession $Session -
DisableNameChecking
```

- Run the following to assign roles required to work with Exchange Online:

```
New-ManagementRoleAssignment -Role:ApplicationImpersonation
-User: vboaccount@domain.onmicrosoft.com
```

```
New-ManagementRoleAssignment -Role: "View-Only Configuration"  
-User: vboaccount@domain.onmicrosoft.com
```

```
New-ManagementRoleAssignment -Role: "View-Only Recipients"  
-User: vboaccount@domain.onmicrosoft.com
```

```
New-ManagementRoleAssignment -Role: "Mailbox Search"  
-User: vboaccount@domain.onmicrosoft.com
```

- To review roles and permissions assigned to the service account for Exchange Online, run:

```
Get-ManagementRoleAssignment -RoleAssigneeType:User  
-RoleAssignee:vboaccount@domain.onmicrosoft.com
```

- Run the following to assign roles required to work with SharePoint Online and OneDrive for Business:

```
Connect-MsolService  
Add-MsolRoleMember -RoleName "SharePoint Service Administrator"  
-RoleMemberEmailAddress "vboaccount@domain.onmicrosoft.com"
```

How to get an app password for an MFA-enabled service account

For a newly created service account:

Sign into Office 365 with your service account credentials. You will be prompted to provide additional security verification methods for this account:

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone

Select your country or region

Method

Send me a code by text message

Call me

Next

Upon a verification, you will be provided with a new app password. It's recommended to use an app password one time only on a per-application basis. A new unique app password can be created once needed.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 3: Keep using your existing applications

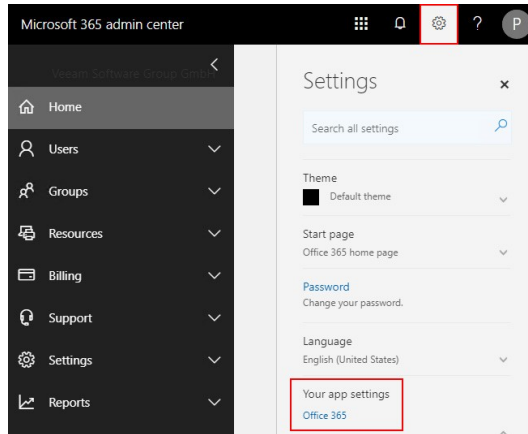
In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. [Learn more](#)

Get started with this app password:

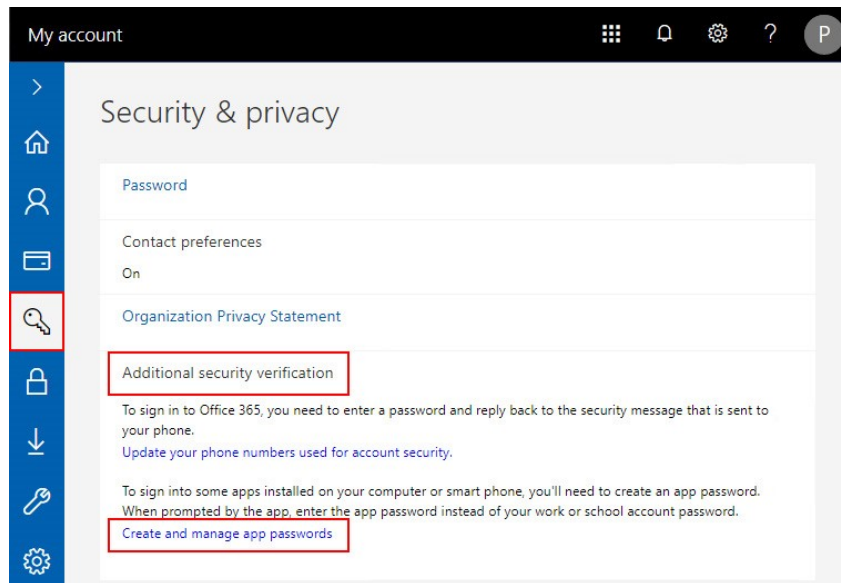
Done

For an existing service account:

1. Sign into Office 365 with your Veeam Backup *for Microsoft Office 365* service account. Note that you must pass additional verification.
2. Go to user's **Settings** -> **Your app settings**:



3. You will be redirected to <https://portal.office.com/account>. Select **Security & privacy** -> **Additional security verification** -> **Create and manage app passwords**:



4. Select **Create** to create a new app password. The same app password can be used for multiple apps or a new unique app password can be created for each app.

Microsoft

additional security verification app passwords


To sign into Outlook, Lync or other apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.

You can use the same app password with multiple apps or create a new app password for each app. [How do I get my apps working with app passwords?](#)

Note: If you are an admin of a Microsoft service, we recommend not using app passwords.

[Bookmark this page](#)

[create](#)




Create app password

Enter a name to help you remember where you use this password.

Name:

[next](#) [Cancel](#)



Your app password

Name: VBO

Password:

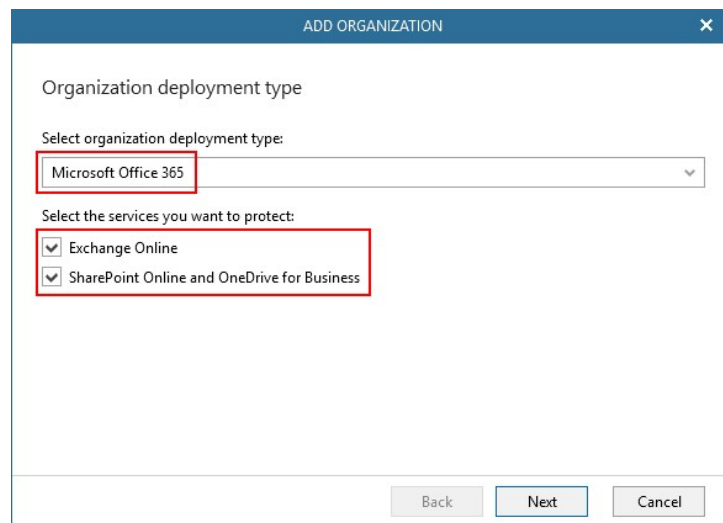
Note: This password will not be displayed again.

[copy password to clipboard](#)

[close](#)

How to add to the Veeam *Backup for Microsoft Office 365* scope, an Office 365 organization using modern authentication

1. In the Veeam Backup *for Microsoft Office 365* console, click **Add Org**, select **Microsoft Office 365** deployment type and specify the services you want to protect within this organization:



Organization deployment type

Select organization deployment type:

Microsoft Office 365

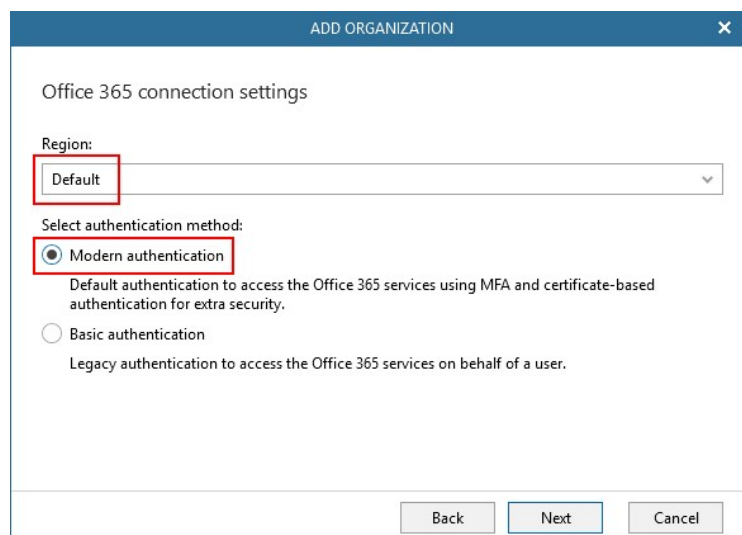
Select the services you want to protect:

Exchange Online

SharePoint Online and OneDrive for Business

Back Next Cancel

2. Select the **Region** where your Office 365 data center is located. Choose the **Default** for all global regions or specify the sovereign region, including Germany, China, U.S. Government or U.S. Government DOD. Select **Modern authentication** if you want to use an account enabled for MFA:



Office 365 connection settings

Region:

Default

Select authentication method:

Modern authentication

Default authentication to access the Office 365 services using MFA and certificate-based authentication for extra security.

Basic authentication

Legacy authentication to access the Office 365 services on behalf of a user.

Back Next Cancel

Important note: Modern authentication is not available for the China region.

3. On the next steps of the wizard, you need to provide for the selected services (Exchange Online and/or SharePoint Online and OneDrive for Business) your **Application ID** (or **Client ID**), **Application secret** (or **Client secret**) (or you can use application certificate instead), account username and its app password:

The screenshot shows a dialog box titled "ADD ORGANIZATION" with a close button in the top right corner. The main heading is "Exchange Online credentials". A red box highlights the following fields: "Application ID:" (text input), "Application secret:" (radio button selected, text input with "[Click here to change the password]"), "Application certificate:" (radio button unselected, text input with "Browse..." button), "Username:" (text input), and "App password:" (text input with "[Click here to change the password]"). Below these fields are two checked checkboxes: "Grant this account required roles and permissions" and "Use the same credentials for SharePoint Online and OneDrive for Business". At the bottom of the dialog are three buttons: "Back", "Next", and "Cancel".

Select **Grant this account required roles and permissions** to let Veeam Backup *for Microsoft Office 365* automatically assign the Application Impersonation role to the specified account.

You can choose to use the same or different credentials for Exchange Online and SharePoint Online.

About Veeam Software

Veeam® is the leader in backup solutions that deliver Cloud Data Management™. Veeam Availability Platform™ is the most complete backup solution for helping customers on the journey to achieving success in the 5 Stages of Cloud Data Management. Veeam has 343,000+ customers worldwide, including 82% of the Fortune 500 and 67% of the Global 2,000, with customer satisfaction scores at 3.5x the industry average, the highest in the industry. Veeam's global ecosystem includes 64,000 channel partners; Cisco, HPE, NetApp and Lenovo as exclusive resellers; and 22,500+ cloud and service providers. Headquartered in Baar, Switzerland, Veeam has offices in more than 30 countries. To learn more, visit <https://www.veeam.com> or follow Veeam on Twitter @veeam.

VEEAM

Cloud Data

Backup
for what's next

