

Veeam Backup for Microsoft Office 365 Modern authentication

AUCloud Veeam Backup for M365

Overview

This guide outlines the steps required to configure and implement your Office 365 Backup with AUCloud using the modern authentication method. You will be allocated a Customer Success Manager (CSM) who will assist you with the onboarding process, provide advice and act as a conduit to deeper technical support when required.

Prerequisites

- A Microsoft Office 365 account that has an active subscription.
- The Microsoft Office 365 account must have permission to manage applications in Azure Active Directory (Azure AD). Any of the following Azure AD roles include the required permissions:
 - [Application administrator](#)
 - [Application developer](#)
 - [Cloud application administrator](#)
- Completion of the [Set up a tenant](#) quick start.
- AUCloud provided certificate (public key) to be used in application registration.
- **Create a backup service account** in Azure AD with Exchange, Sharepoint and Teams [admin rights](#)

Azure AD Application permissions

Register an application

- In the Microsoft Office 365 Admin Centre, navigate to **Azure Active Directory**.
- Under **Manage**, select **App registrations** > **New registration**.
- Enter a display **Name** and select the **'Accounts in this organizational directory only'**.

The Redirect URI can be left blank.

- Select **Register** to complete the initial app registration.

Register an application

* Name
The user-facing display name for this application (this can be changed later).

TEST- Veeam Office 365 APP

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

By proceeding, you agree to the Microsoft Platform Policies

Register

Configure Application permissions

- Select the newly registered application, select **API permissions**, and add permissions for:

- Microsoft Graph
- Office 365 Exchange Online
- SharePoint

*Note: To search for other API, select **APIs my organisation uses**.*

TEST- Veeam Office 365 APP | API permissions

Search (Ctrl+F) Refresh Got feedback?

Overview Quickstart Integration assistant Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

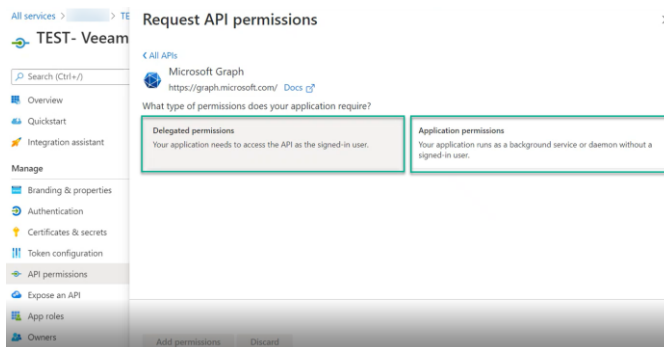
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user pr...	No	

- b. For each API e.g., Microsoft graph, add the appropriate delegated (restore) and application (backup) type permissions as per below:



i. **Delegated (restore) permissions.**

Note:

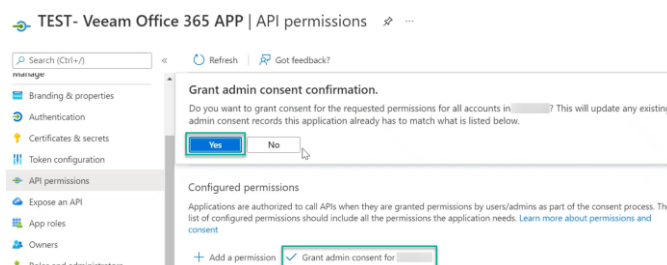
- *All listed permissions are required for data restore using Veeam Explorers.*

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Microsoft Graph	Directory.Read.All	✓	✓	✓	Querying Azure AD for organization properties, the list of users and groups and their properties.
	Group.ReadWrite.All			✓	Recreating in Azure AD an associated group in case of teams restore.
	Sites.Read.All		✓	✓	Accessing sites of the applications that are installed from the SharePoint store.
	Directory.ReadWrite.All			✓	Setting the preferred data location when creating a new M365 group for a multi-geo tenant in case of teams restore.
	offline_access	✓	✓	✓	Obtaining a refresh token from Azure AD.
Office 365 Exchange Online ¹	EWS.AccessAsUser.All	✓			Accessing mailboxes as the signed-in user (impersonation) through EWS.
SharePoint	AllSites.FullControl		✓	✓	Reading the current state and restoring SharePoint sites and OneDrive accounts content.
	User.Read.All		✓		Resolving OneDrive accounts (getting site IDs). Note: This permission is not required to restore SharePoint Online data.

ii. Application (backup) permissions.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Microsoft Graph	Directory.Read.All	✓	✓	✓	Querying Azure AD for organization properties, the list of users and groups and their properties.
	Group.Read.All	✓	✓	✓	Querying Azure AD for the list of groups and group sites.
	Group.ReadWrite.All		✓	✓	Recreating in Azure AD an associated group in case of a deleted team site restore. Note: This permission is only required for restore of SharePoint site data through REST API and PowerShell.
	Sites.Read.All		✓	✓	Querying Azure AD for the list of sites and getting download URLs for files and their versions.
	TeamSettings.ReadWrite.All			✓	Accessing archived teams.
Office 365 Exchange Online ¹	full_access_as_app	✓		✓	Reading mailboxes content.
SharePoint	Sites.FullControl.All		✓	✓	Reading SharePoint sites and OneDrive accounts content.
	User.Read.All		✓	✓	Reading OneDrive accounts (getting site IDs). Note: This permission is not used to back up Microsoft Teams data, but you must grant it along with SharePoint Online and OneDrive for Business permission to add Microsoft 365 organization successfully.

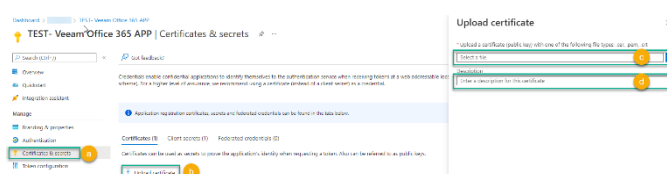
- c. After all APIs are added, you will need to **grant admin consent**.



Add a certificate (public key)

- Select **Certificates & secrets > Certificates**.
- Select **Upload certificate**.
- Browse for the certificate to be uploaded.

Note: AUCloud will provide this certificate.



- Enter a description.
- Select **Add**.

Join secure meeting with AUCloud

A joint session with the AUCloud technical team is required for you to enter the necessary credentials to finalise the configuration of the Veeam Backup for Office 365 application. This can be organised via Webex, Zoom, Teams chat or face-to-face meeting. Please advise your CSM on what suits best.

- Username
- Application ID

The screenshot shows a window titled "Edit Organization" with a close button (X) in the top right corner. The main heading is "Microsoft 365 connection settings". Below this, there are three sections:

- Specify a user account to use for impersonation in Exchange Online Web Services:** This section has a "Username:" label followed by a text input field.
- Specify Azure AD application credentials to connect to Microsoft Graph:** This section has an "Application ID:" label followed by a text input field, and an "Application certificate:" label followed by a text input field. To the right of the "Application certificate" field is an "Install..." button.
- Below these sections are two checkboxes:
 - ☐ Grant this application required permissions and register its certificate in Azure AD.
 - ☒ Allow this application to enable export mode for SharePoint Web Parts. Enabling export mode is required to back up customized content of SharePoint Online sites.

At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

Restore Portal Access Requirements

To access the Veeam restore portal, you must add an Enterprise Application in Azure AD

Prerequisite: For the below, you need to use a Service Account with enough rights to perform an Enterprise Application install on Azure AD. In order to perform these steps, we will need the AzureAD PowerShell cmdlet. To install this, open PowerShell and run the following command:

Install-Module -Name AzureAD

Next, type the following to store service account credentials:

```
$Credential = Get-Credential
```

This will open a traditional User and password Microsoft Popup:
Please enter your service account username and password in this popup.

The screenshot shows a "Windows PowerShell credential request" dialog box. It has a title bar with a question mark and a close button (X). The background is blue with a key icon. The text "Enter your credentials." is displayed. Below this are two input fields: "User name:" and "Password:". The "User name" field contains the text "admin@M365x73145060.c" and has a dropdown arrow on the right. The "Password" field is filled with dots. At the bottom right are two buttons: a blue button with a mouse cursor icon and a "Cancel" button.

The next command will connect your PowerShell to AzureAD using the credentials we introduced before:

```
Connect-AzureAD -Credential $Credential
```

We should see something like this if everything worked smoothly:

```
PS Cert:\CurrentUser\Root> Connect-AzureAD -Credential $Credential

Account Environment TenantId TenantDomain AccountType
-----
admin@M365x73145060.onmicrosoft.com AzureCloud c43ec543-63b7-459d-bbed-84a25448b313 M365x73145060.onmicrosoft.com User
```

And the final step which brings everything together:

```
New-AzureADServicePrincipal -AppId "33831092-5ae1-4b51-9eb2-a90033803540"
```

If everything works as expected, the output should show something similar to this:

```
PS Cert:\CurrentUser\Root> New-AzureADServicePrincipal -AppId "115c7c8c-627c-4ae6-b304-cfb0e9a01d67"

ObjectID AppId DisplayName
-----
7f81cd64-e7cf-4d01-b61d-a3f530867f90 115c7c8c-627c-4ae6-b304-cfb0e9a01d67 Veeam Restore Portal 365
```

Last-Step - Give permission to the new Application on Azure AD

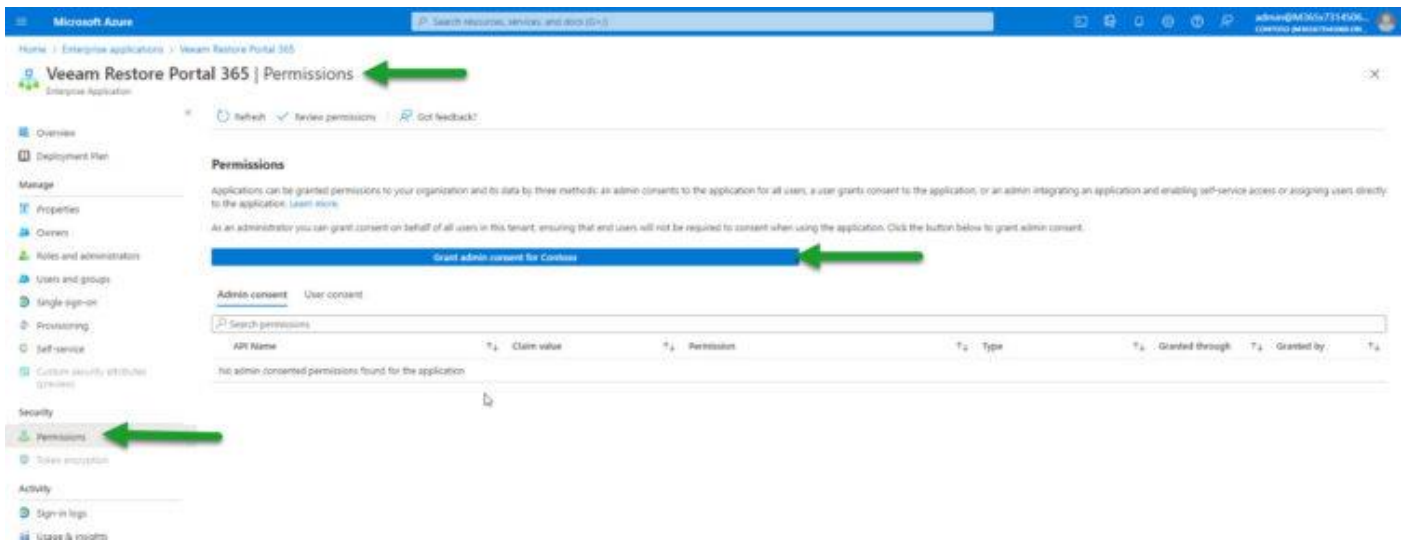
- Under Enterprise Applications, remove the enterprise applications filter, and order them by date.

You should see a new Veeam VBO application (the name of the Restore Portal).

The screenshot shows the 'Enterprise applications' page in the Azure portal. The left sidebar has 'Enterprise applications | All applications' selected. The main area shows a list of 402 applications. The 'Veeam Restore Portal 365' application is highlighted in the list. The table columns are Name, Object ID, Application ID, Homepage URL, and Created on.

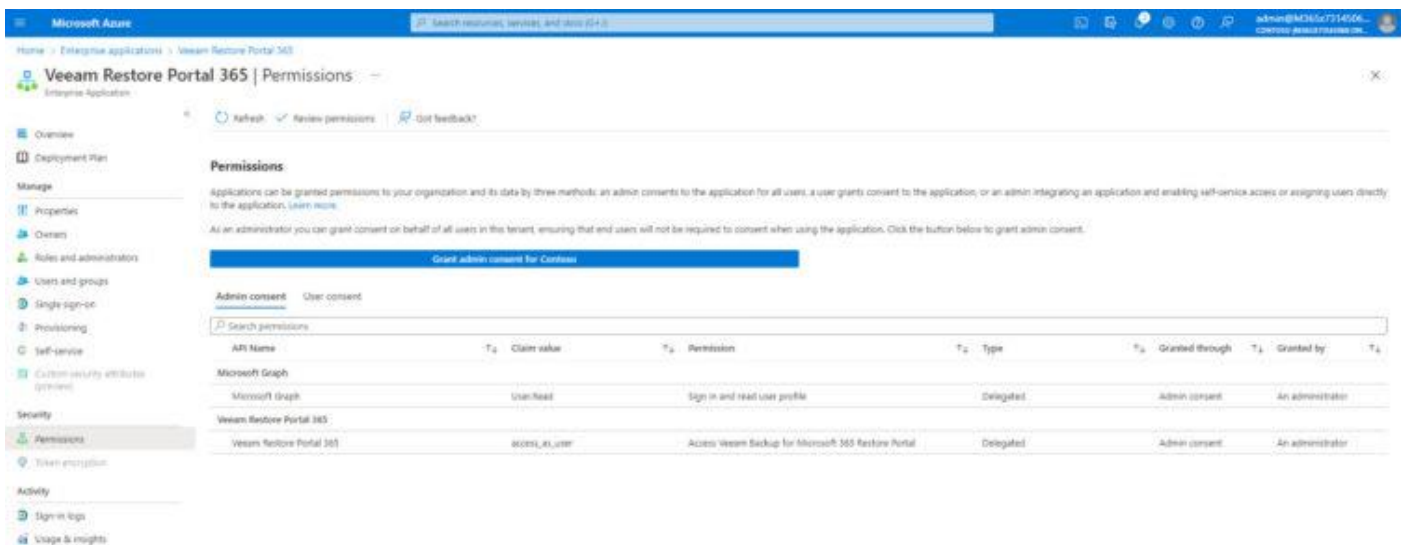
Name	Object ID	Application ID	Homepage URL	Created on
Veeam Restore Portal 365	115c7c8c-627c-4ae6-b304-cfb0e9a01d67	115c7c8c-627c-4ae6-b304-cfb0e9a01d67		3/16/2022
Veeam Microsoft 365	4063b0f6-60de-47fa-929e-e417b04a4d40	362ab073-efec-4689-bc3d-ae17a26d60f8		3/16/2022
Office 365 Reports	8c3b4dcb-1f2f-4368-b0da-171ad5c88adb	537bc9da-c4d2-4009-9647-ae304f52483e		3/16/2022
CDK.M3.Cloud App Security Demo	ed3a4e08-423d-4f32-92a3-757a1a05da1	64a79c37-4e1a-4e10-6780-08c23a08a05		3/16/2022
AADReporting	3b259d05-14f5-4a5b-99a9-739f1d145eb3	1b912e03-893d-4a8c-253e-76aa7ad02807		6/15/2022
ONEE LinkedIn Connection	6510568c-7d98-451b-bc77-60e34011f10a	16668c7-8a15-4a67-8a67-87040002090b		6/15/2022
Azure AD Identity Protection	25b07f21-110e-4d05-a683-0326ca8060	7c68d9e5-157d-43ef-96ae-214805818498		6/15/2022
CDK Graph Resolver Service and CAD	af6b6470-3061-4759-a77c-9c0b7f60396	288a381a-0488-4271-e13f-af307f0599c2		6/15/2022
Skyline for Business	ae4994d7-5b16-4871-648a-3013bc178bad	7557ab47-c889-433a-afcf-ae76b75733e1		3/15/2022
Provisioning worker app	6c0b4055-4741-4a1a-af08-0303b0f05e2	28570e03-d003-4891-b64a-1b48895e678		3/15/2022
Microsoft AppFlow ERM	9b0ea02f-6254-4a4e-9e83-0c060c04caad	8ee73ad0-6a25-4710-ab0c-746a8231ae49		3/15/2022
M365 App Management Service	07ba009d-d17d-4f0d-b07f-d01290002d6f	0117f1ae-825d-4aff-899e-3f23380a006		3/15/2022

On the Enterprise Application, go to Permissions, and press **"Grant admin consent"**



That process will ask us again for an authorized account.

We should see something like this:



Configuration is completed. You can then proceed to test connectivity to the Restore Portal.

Restore Portal URL:

- **OFFICIAL:** <https://vbo-csz.australiacloud.com.au/>
- **PROTECTED:** <https://evbo-csz.australiacloud.com.au/>