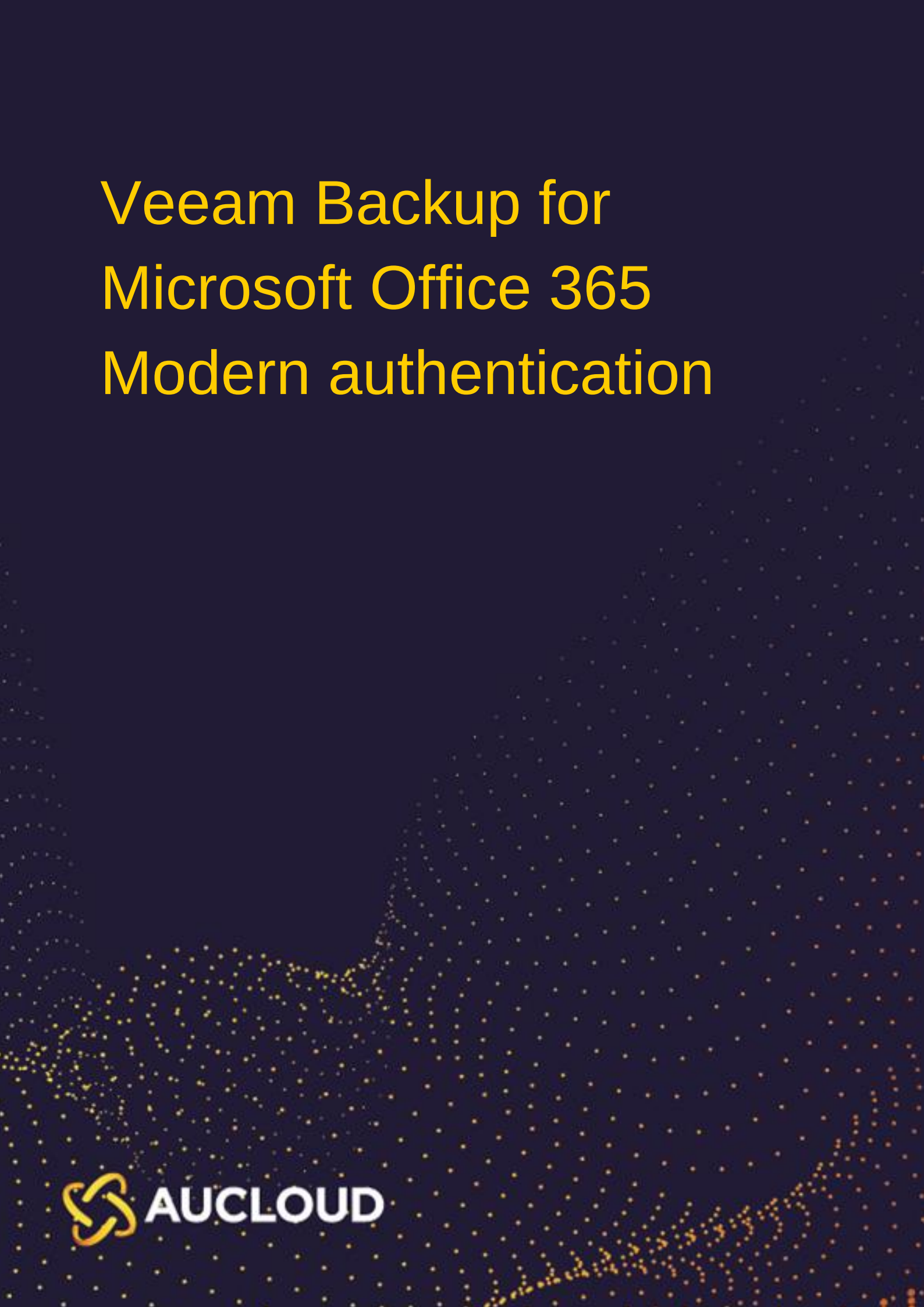
Veeam Backup for Microsoft Office 365 Modern authentication



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

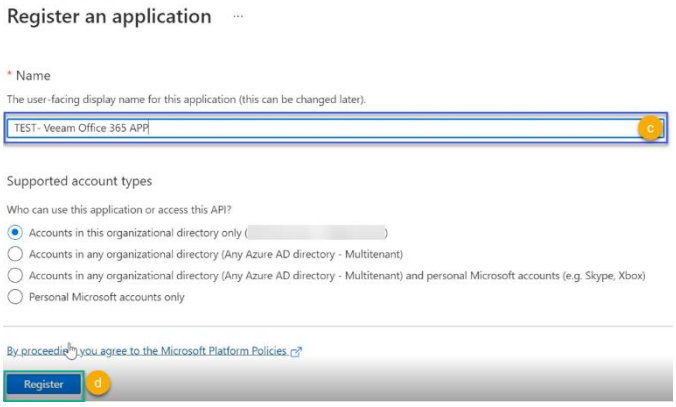
Azure AD Application permissions

Register an application

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

   The Redirect URI can be left blank.

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

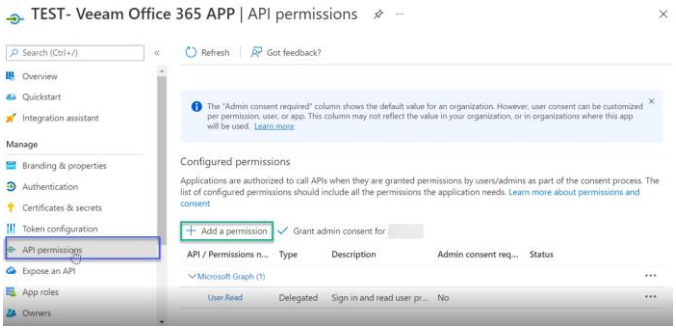


Configure Application permissions

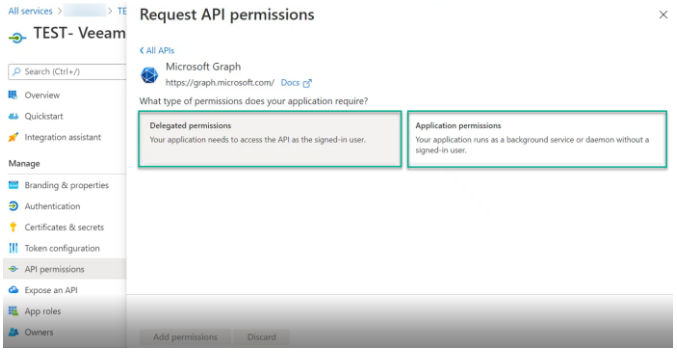
a. Select the newly registered application, select **API permissions**, and add permissions for:

   - Microsoft Graph
   - Office 365 Exchange Online
   - SharePoint

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



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



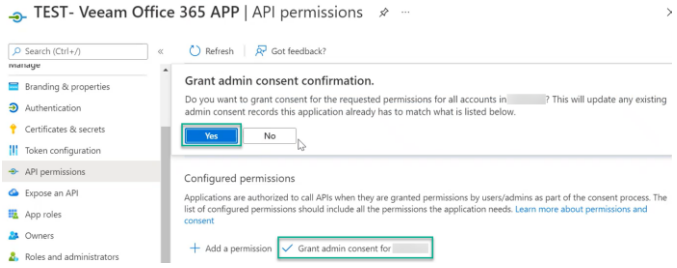
i. **Delegated (restore) permissions.**
Note:
- *All listed permissions are required for data restore using Veeam Explorers.*

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.**

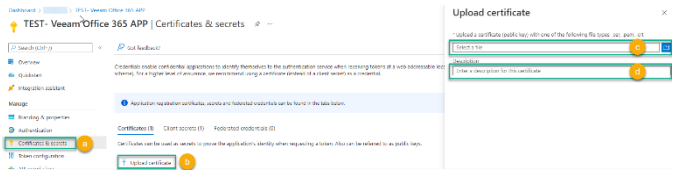


Add a certificate (public key)

a. Select **Certificates & secrets > Certificates.**
b. Select **Upload certificate.**
c. Browse for the certificate to be uploaded.

Note: AUCloud will provide this certificate.

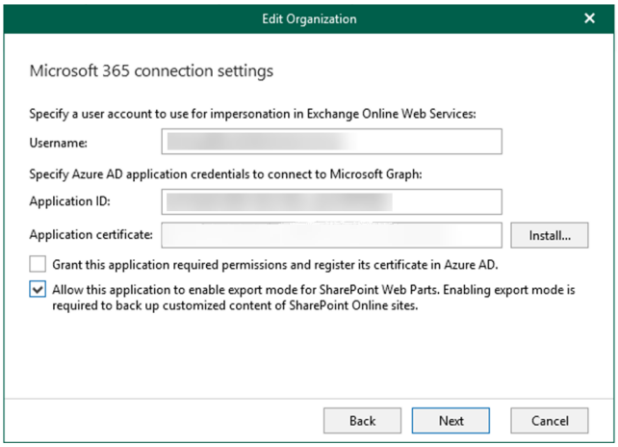
d. Enter a description.
e. Select **Add**.



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



Restore Portal Access Requirements

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

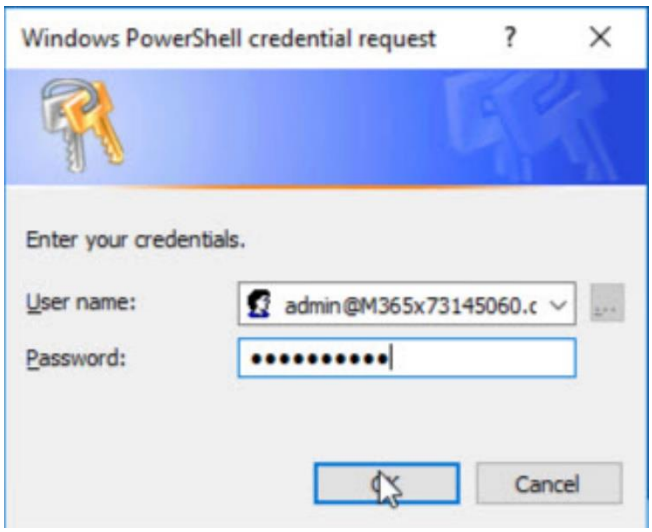
Prerequisite: For the below, you need to use a Service Account with enough rights to perform an Enterprise Application install on Azure AD. In order to perform these steps, we will need the AzureAD PowerShell cmdlet. To install this, open PowerShell and run the following command:

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 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:

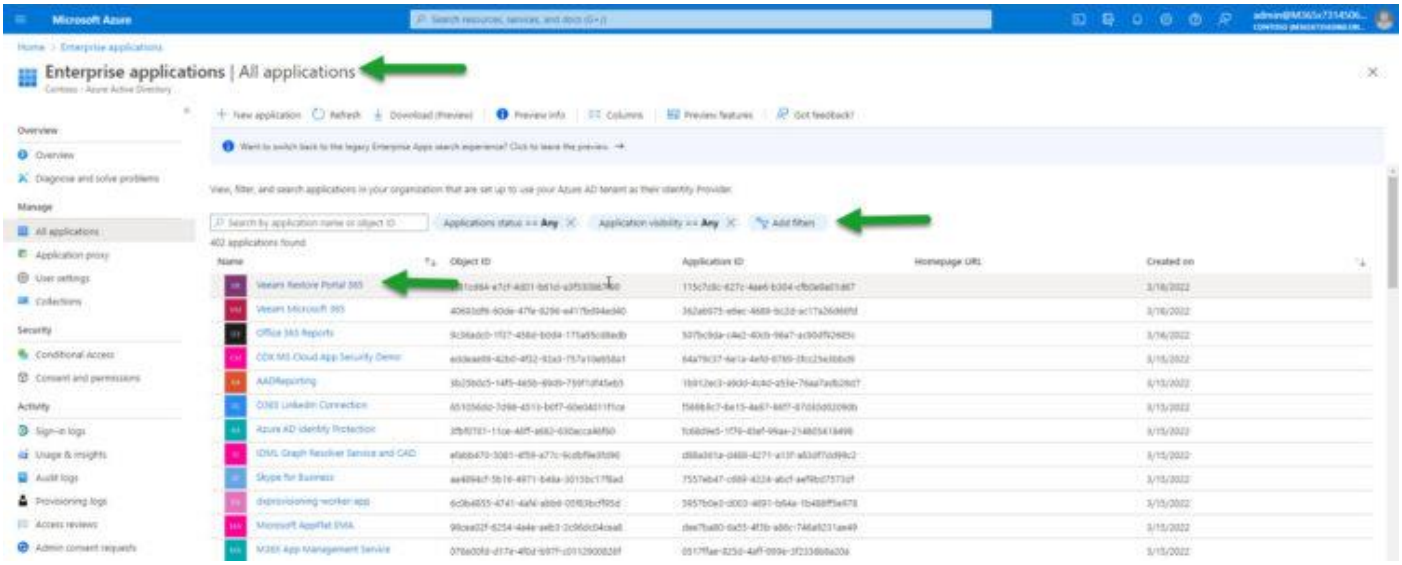
```
PS Cert:\CurrentUser\Root> New-AzureADServicePrincipal -AppId "115c7c8c-627c-4ae6-b304-cfb0e9a01d67"

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

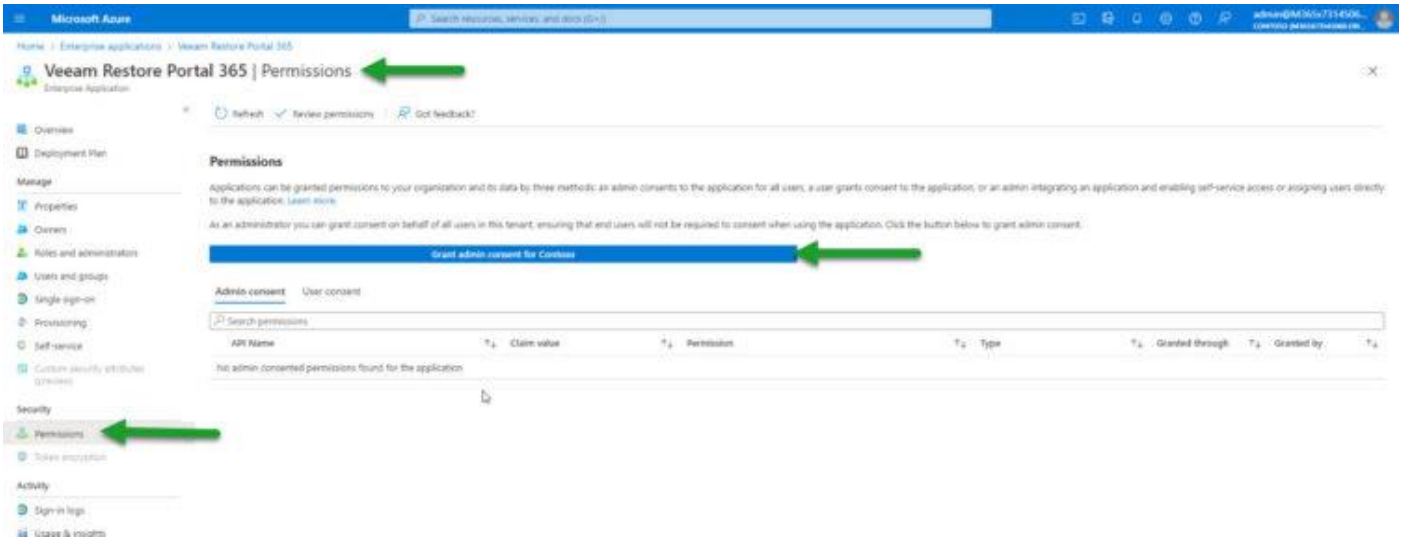
Last-Step - Give permission to the new Application on Azure AD

- 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).

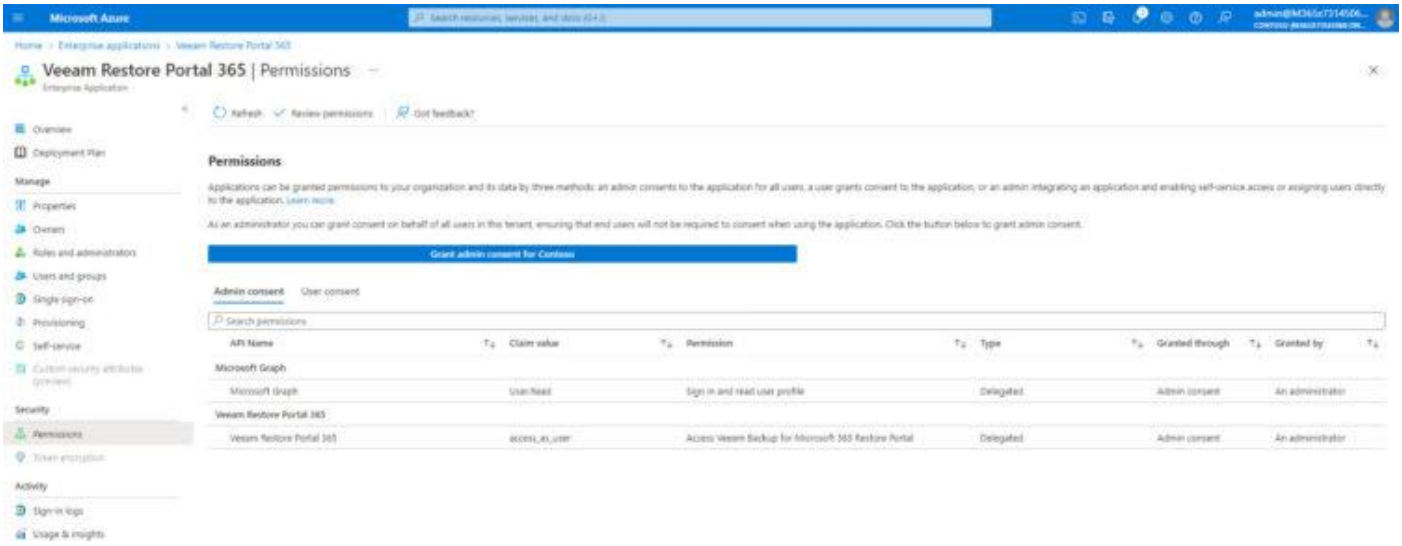


On the Enterprise Application, go to Permissions, and press "**Grant admin consent**"



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/