



USER GUIDE DOCUMENT FOR

PRIVATE CHAT BACKUP SERVICE

Version 4.0.0
2023 October



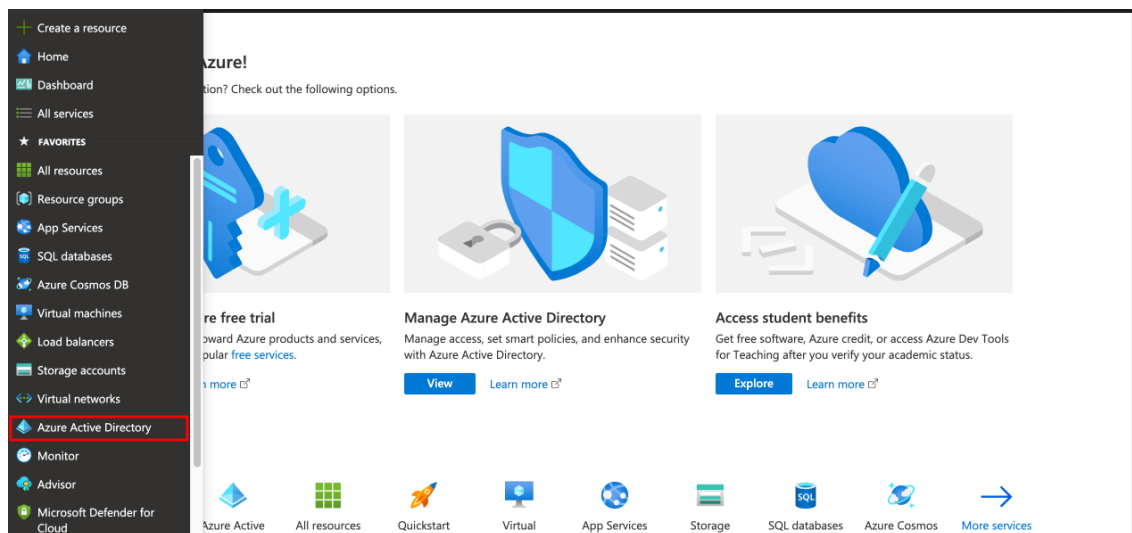
Overview

Due to Microsoft's new billing regulation regarding private chats and the Teams Export API, there are additional steps required to enable access to your private chat for the backup service. First, you will need to register a new application using Microsoft Azure Portal. After that, you will need to setup the new registered application as it relates to certificates and API permissions.

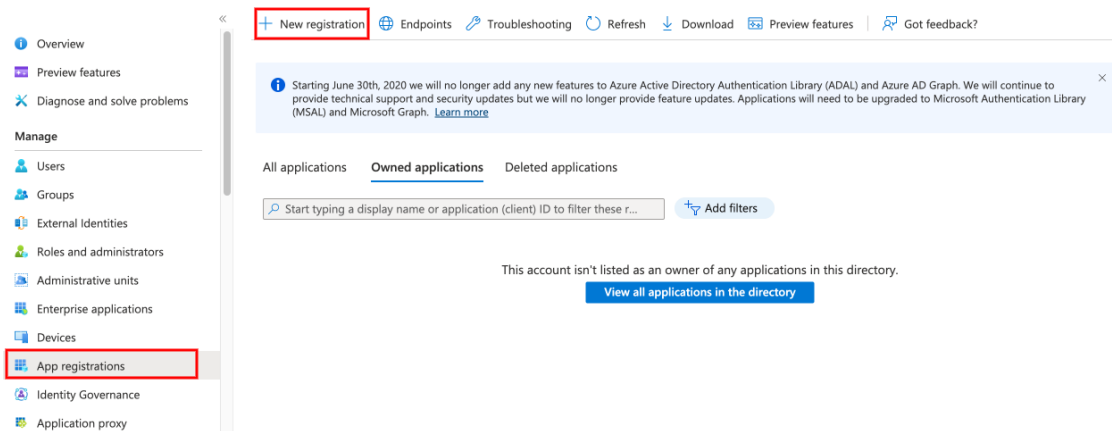
Please be advised, once you have completed the creation of this below application it must be associated with an azure billing resource. Please follow the guide from Microsoft linked here: <https://learn.microsoft.com/en-us/graph/metered-api-setup?tabs=azurecloudshell>

Register A New Application Using Microsoft Azure

1. Go to <https://portal.azure.com> and log in using your tenant admin credentials.
2. Select **Azure Active Directory** in the left navigation bar.



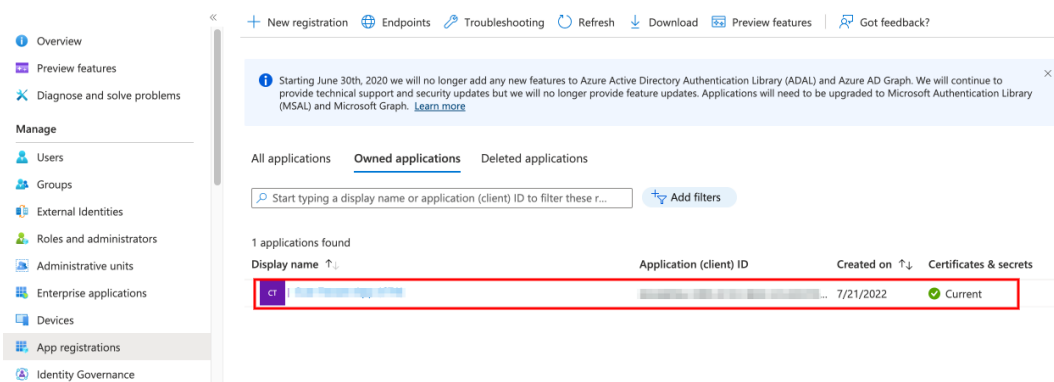
3. Select **App registrations**, then select **+ New registration**.



4. Complete the form. Then select the **Register** button. There are 2 sections that you will need to fill in:
- Name → It is required. Do not leave this space empty.
 - Account types → We recommend choosing the first option (single tenant). It is easier to comply with Microsoft's Access Policies.

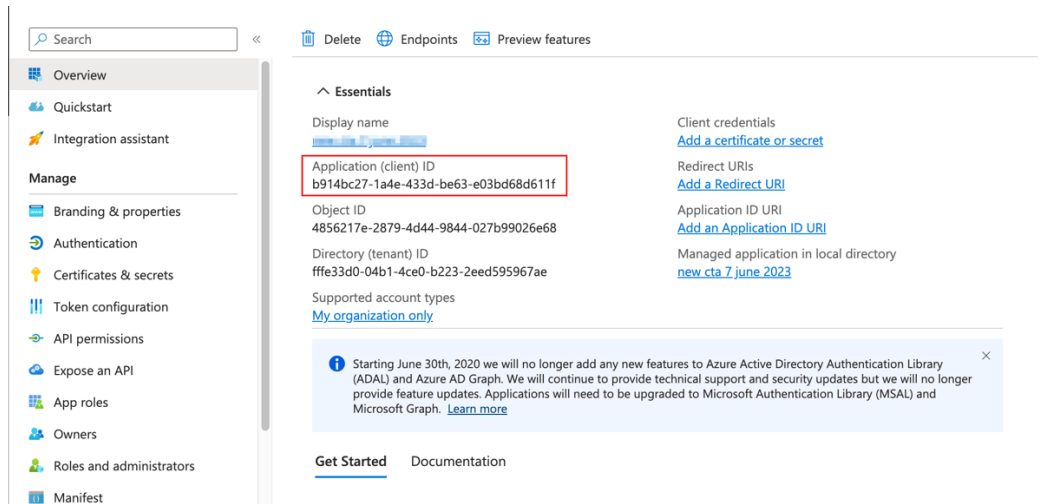
The screenshot shows the 'Register an application' form. The 'Name' field is highlighted with a red box. Below it, the 'Supported account types' section is shown, with the first option, 'Accounts in this organizational directory only (dropmyserver.com only - Single tenant)', selected and highlighted with a red box. The other options are '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)', and 'Personal Microsoft accounts only'.

5. Once completed, your application will display in the list.



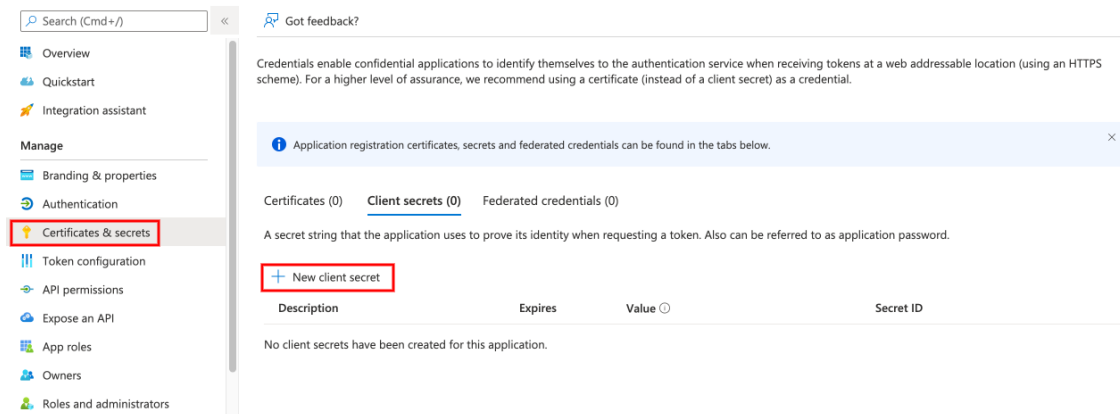
Private and Confidential

6. Select the newly registered application. Copy the Application (client) ID by hovering the cursor over the items. The system will display a copy button. Paste it to our portal as the Application ID.



Setup The Registered Application

1. Select the registered application.
2. Select **Certificates & secrets**, then select **+ New client secret**.



Private and Confidential

3. Input the description, set it to 24 months, and then select **Add**.

Home > [Application Name] > Certificates & secrets

Search (Cmd+/)

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Got feedback?

Credentials enable confidential applications to identify themselves to the scheme). For a higher level of assurance, we recommend using a certificate.

Application registration certificates, secrets and federated credentials

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token.

+ New client secret

Description Expires

No client secrets have been created for this application.

Add Cancel

Add a client secret

Description: Enter a description for this client secret

Expires: Recommended: 6 months (selected)
Recommended: 6 months
3 months
12 months
18 months
24 months (highlighted)
Custom

4. Once added, immediately copy the value, and paste it to our portal as the application secret code. **Please note:** Microsoft Azure will only allow you to copy value immediately after creation. Once you leave the page, it cannot be copied, and the full value will be hidden.

Search (Cmd+/)

Got feedback?

Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (2) Federated credentials (0)

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	Secret ID
CTA certificates	7/21/2024	8Su*****	bf6d5f4c-1409-4dbf-a92d-18abee0bd...
New certificates	7/27/2024	UzO8Q~IPW2HeDRG331sb.e7v18Ky-5...	5f2edfe7-71b7-4bb3-bcf9-bd3d9f065...

5. Select **API permissions**, then select **+ Add a permission**.

Search (Cmd+/)

Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators

Configured permissions

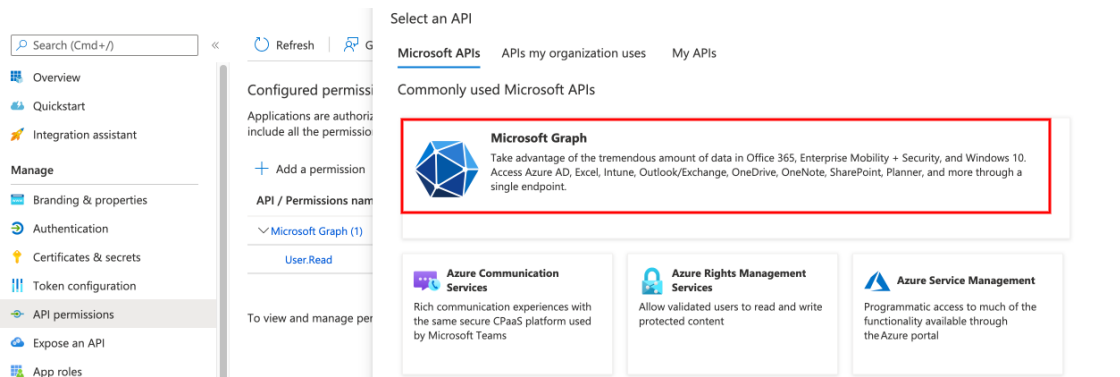
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for dropmyserver.com

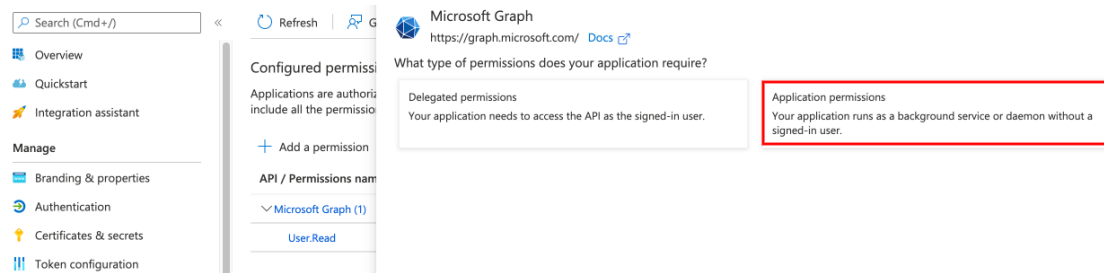
API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	Granted for dropmyserv...

To view and manage permissions and user consent, try [Enterprise applications](#).

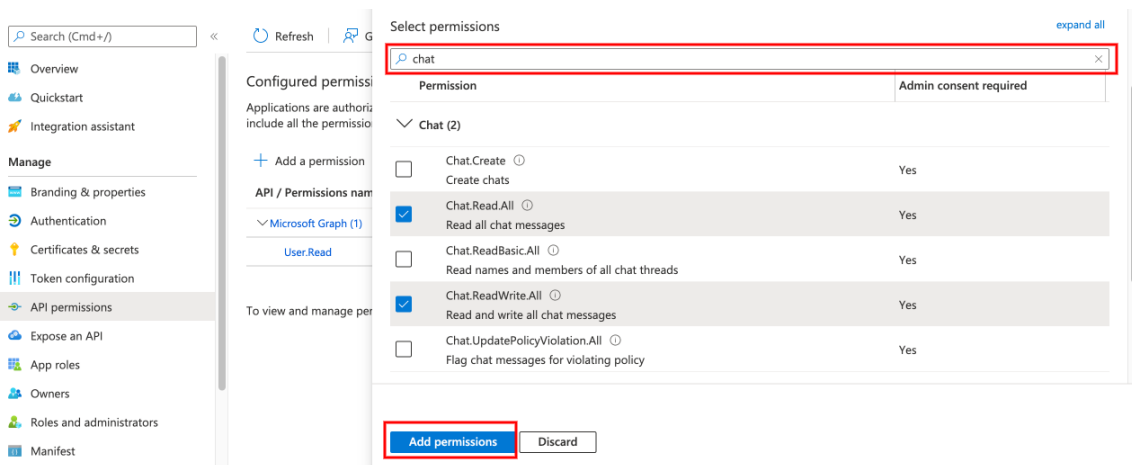
6. Select Microsoft Graph.



7. Select Application permissions.



8. Input 'chat' in search, then select Chat.Read.All and Chat.ReadWrite.All, then select Add permissions.



9. Do not forget to select **Grant admin consent for <domain>**.

Search (Cmd+//)

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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 dropmyserver.com

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
Chat.Read.All	Application	Read all chat messages	Yes	⚠ Not granted for dropmy... ***
Chat.ReadWrite.All	Application	Read and write all chat messages	Yes	⚠ Not granted for dropmy... ***
User.Read	Delegated	Sign in and read user profile	No	✅ Granted for dropmyserv... ***