



# **HYCU R-Cloud for Microsoft 365**

---

**Private Chat Backup**

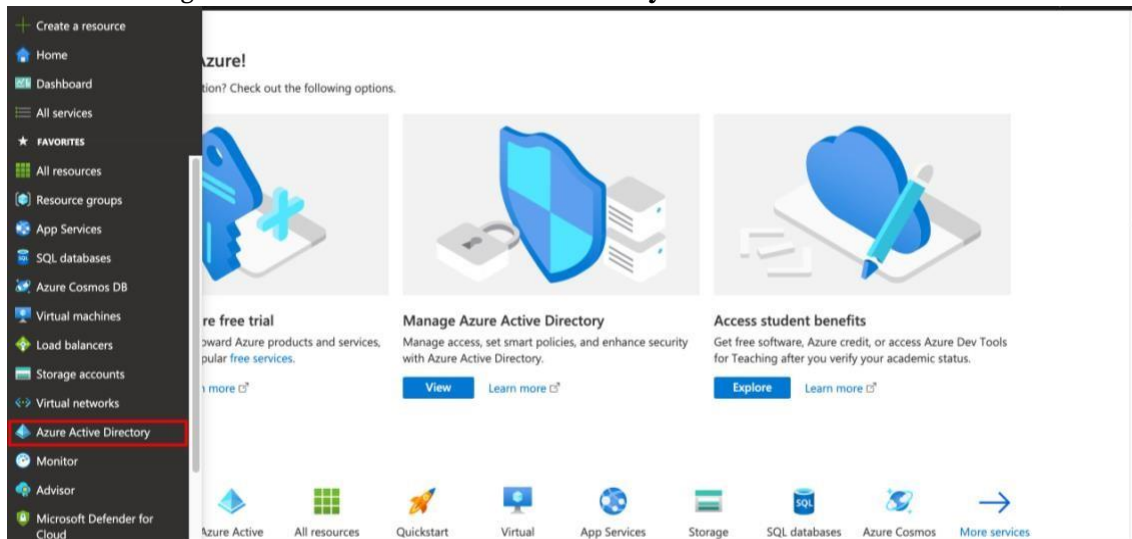
## Overview

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 chats for the HYCU R-Cloud for Microsoft 365 backup service:

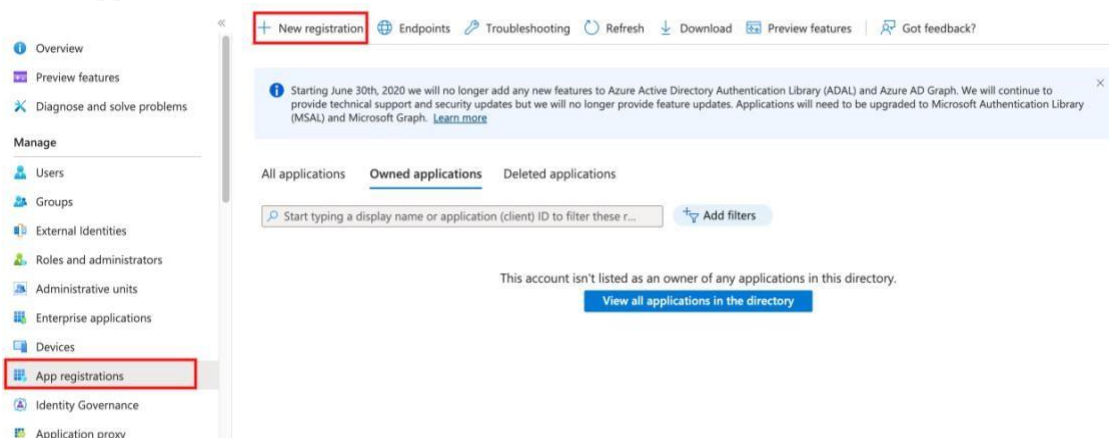
1. Register a new application using Microsoft Azure Portal.
2. Set up the new registered application as it relates to certificates and API permissions.
3. Associate the created application with the Azure billing resource.

## Register a new application using Microsoft Azure

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



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



4. Complete the form. You need to fill in two sections:
  - a. Name  
Required. Do not leave this space empty.
  - b. Supported account types  
We recommend choosing the first option (Single tenant), which makes it easier to comply with Microsoft's Access Policies.

c. Click **Register**.

[Home](#) > [DemoHYCU | App registrations](#) >

## Register an application ...

## \* Name

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

Private chat backup EUC

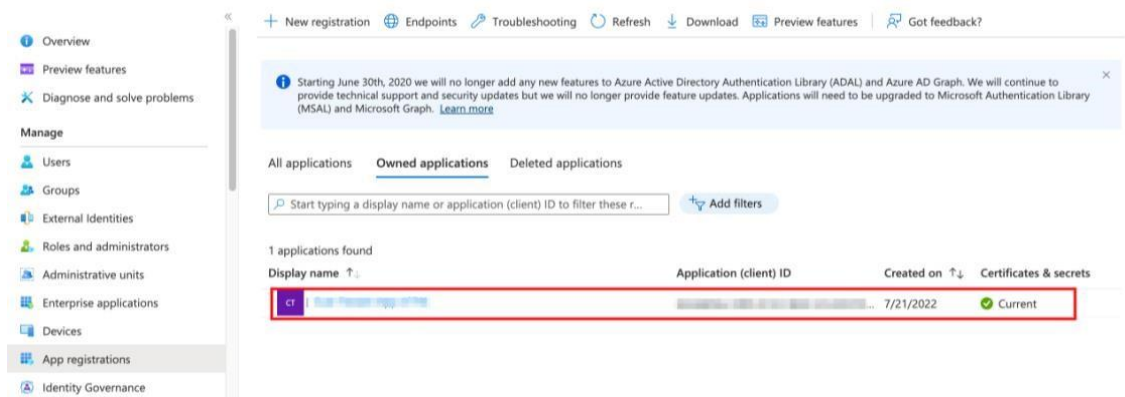
## Supported account types

Who can use this application or access this API?

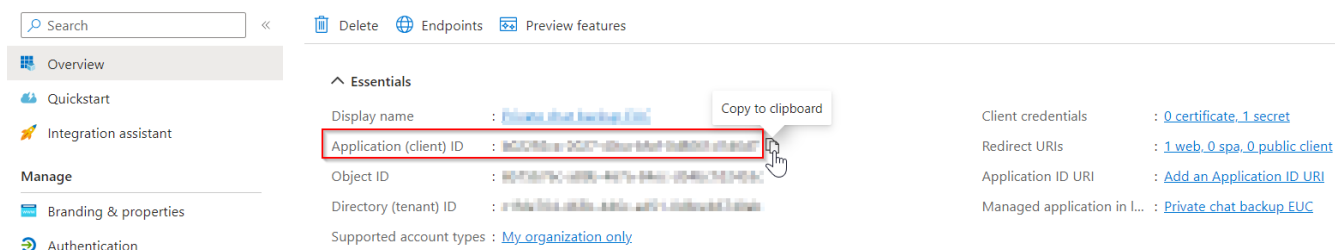
- ☒ Accounts in this organizational directory only (DemoHYCU only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

## 5. When the registration is completed, your application is displayed in the list.



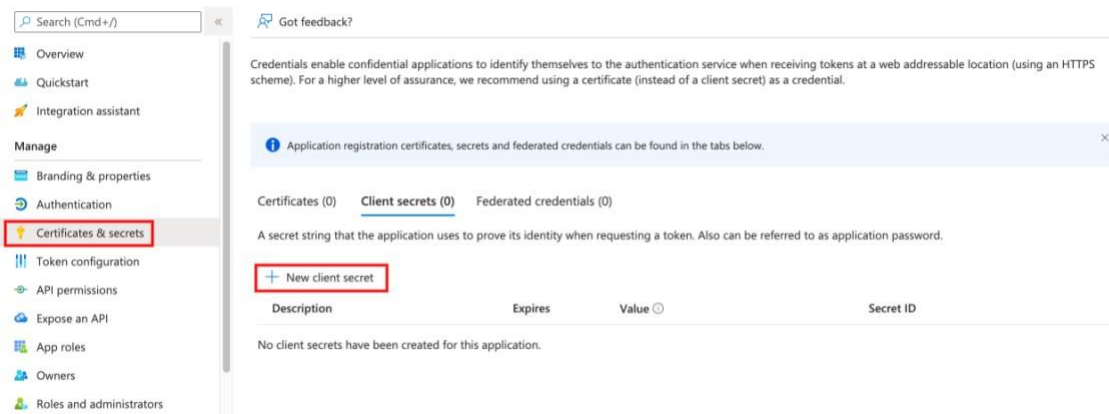
## 6. Select the newly registered application. Copy the Application (client) ID by hovering the cursor over the items to display a copy button to save it or paste it to our portal as the Application ID.



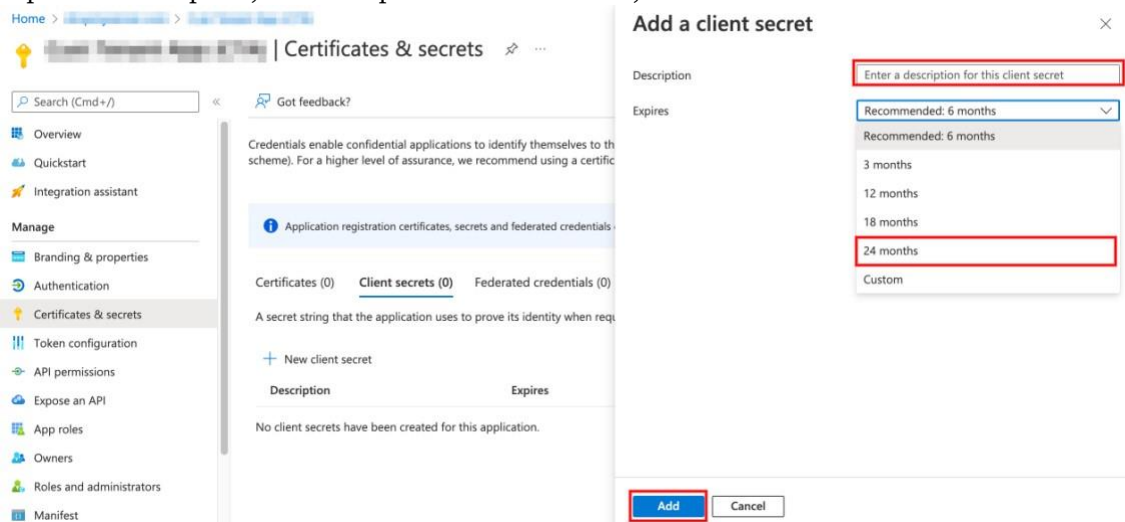
## Set up the registered application

## 1. Select the registered application.

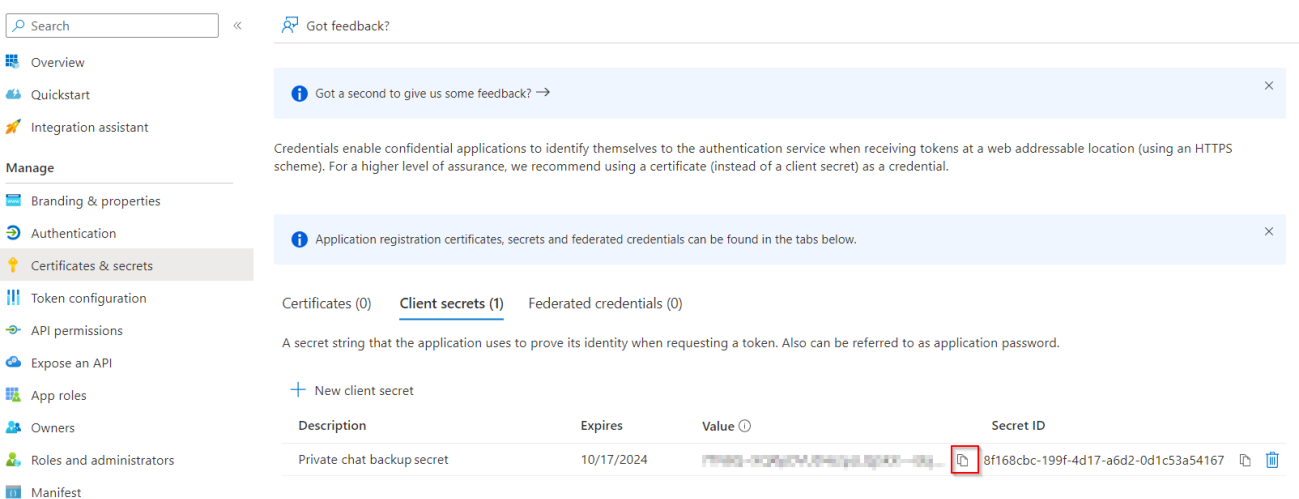
2. Select **Certificates & secrets**, and then select **+ New client secret**.



3. Input the description, set the expiration to 24 months, and then click **Add**.



4. Once added, immediately copy the value, and save it or paste it to our portal as the application secret code.  
**Note** Microsoft Azure will only allow you to copy the value immediately after creation. After you leave the page, it can no longer be copied, and the full value is hidden. You can however create a new secret later.



## 5. Select **API permissions**, and then click **+ Add a permission**.

Search

Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

**API permissions**

Expose an API

App roles

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 **Microsoft Graph**

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

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

## 6. Select **Microsoft Graph**.

Search (Cmd+/)

Refresh G

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

**API permissions**

Expose an API

App roles

Select an API

Microsoft APIs APIs my organization uses My APIs

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 **Microsoft Graph**

API / Permissions name

Microsoft Graph (1)

User.Read

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Commonly used Microsoft APIs

**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Communication Services**

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

**Azure Rights Management Services**

Allow validated users to read and write protected content

**Azure Service Management**

Programmatic access to much of the functionality available through the Azure portal

## 7. Select **Application permissions**.

Search (Cmd+/)

Refresh G

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

**API permissions**

Expose an API

App roles

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.

## 8. In the search field, type 'chat', and then select **Chat.Read.All** and **Chat.ReadWrite.All**. Click **Add permissions**.

Search (Cmd+/)

Refresh G

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

**API permissions**

Expose an API

App roles

Owners

Roles and administrators

Manifest

Select permissions

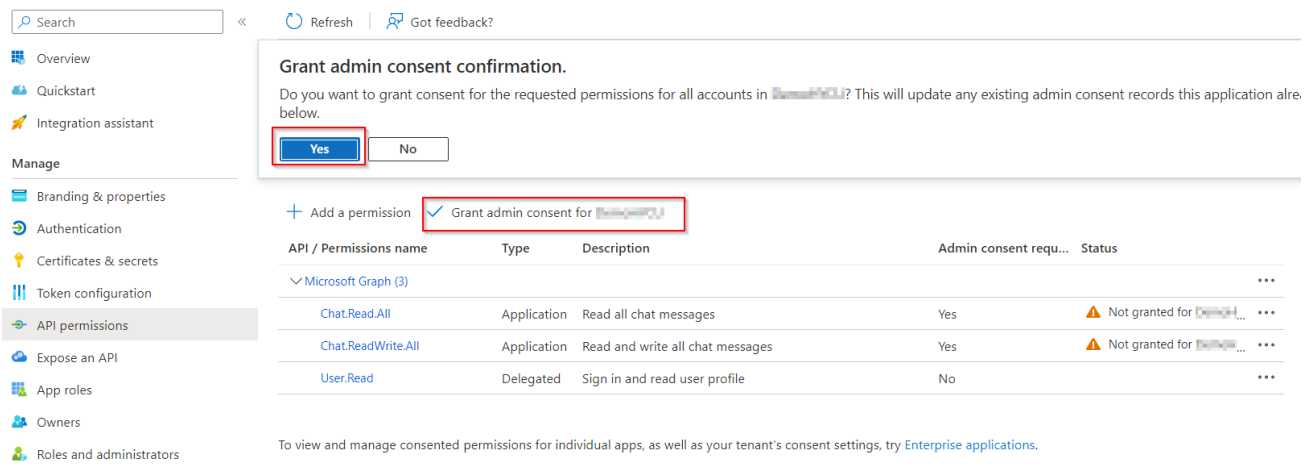
expand all

chat

Permission	Admin consent required
Chat (2)	
Chat.Create	Yes
<b>Chat.Read.All</b>	Yes
Chat.ReadBasic.All	Yes
<b>Chat.ReadWrite.All</b>	Yes
Chat.UpdatePolicyViolation.All	Yes

**Add permissions** Discard

9. Select **Grant admin consent for <domain>**, and then click **Yes** to confirm.



The screenshot shows the Microsoft Graph admin consent interface. A modal dialog titled "Grant admin consent confirmation." is displayed, asking for consent for the requested permissions for all accounts in the domain. The "Yes" button is highlighted with a red box. Below the dialog, the "Add a permission" section shows a checked checkbox for "Grant admin consent for [domain]". The main table lists permissions for Microsoft Graph (3):

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3)				
Chat.Read.All	Application	Read all chat messages	Yes	⚠ Not granted for [domain] ...
Chat.ReadWrite.All	Application	Read and write all chat messages	Yes	⚠ Not granted for [domain] ...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

## Associate the application with Azure billing

To associate the created application with the Azure billing resource, please follow the Microsoft instructions. See [Enable metered APIs and services in Microsoft Graph - Microsoft Graph | Microsoft Learn](#).

## Configure Private Chat backup in HYCU R-Cloud for Microsoft 365

1. Sign in to HYCU R-Cloud for Microsoft 365, go to **Account Settings**, select the **Credentials** tab, and expand the **Customer Tenant App**.

**ACCOUNT SETTINGS**  
DASHBOARD

Personal Details Notifications AutoDiscover Partner of Record **Credentials** 2

**Credential Settings**  
The setting is for Global Admin & Single Account credential update. To add new credential, please go to [Add Backup](#).

Search Email Account

**demohycu.onmicrosoft.com**  
Used for 8 Accounts & 26 Sites

**Credential Information**  
Global Admin (Backup):  
Credential Status: **Authentication Success**

**Device Authorization** **Active** ?  
With this step, you are authorizing Microsoft Exchange Online Remote PowerShell access using OAuth Token-based authentication.  
Status: **Verified**

**Customer Tenant App** **Inactive**  
Tenant application needs to be connected in order to enable private chat backup. [Learn more](#).

**Connect to Tenant Application**  
Please follow these steps below to connect your tenant application. The backup process will use this application to backup once it has been successfully tested.  
[See How to Connect](#) 3

2. Do the following:

- Enter the Application ID and the value for the application client secret.
- Optional.* Set the monthly limit for the number of the messages to be backed up.
- Select the check box to confirm that you understand the incurred costs and the limits set, and then click **Test & Save Connection**.

**Customer Tenant App** **Inactive**  
Tenant application needs to be connected in order to enable private chat backup. [Learn more](#).

**Connect to Tenant Application**  
Please follow these steps below to connect your tenant application. The backup process will use this application to backup once it has been successfully tested.

**Step 1:** Setup an application in your tenant **demohycu.onmicrosoft.com** using this user guide ([Download Here](#)).

**Step 2:** Enter following details about the application in the form below.

Application ID

App Secret Code

Max. Limit of Message per Month  ☐ Set to unlimited

Usage in current month: 0 messages x USD 0.00075 = **USD 0.0**

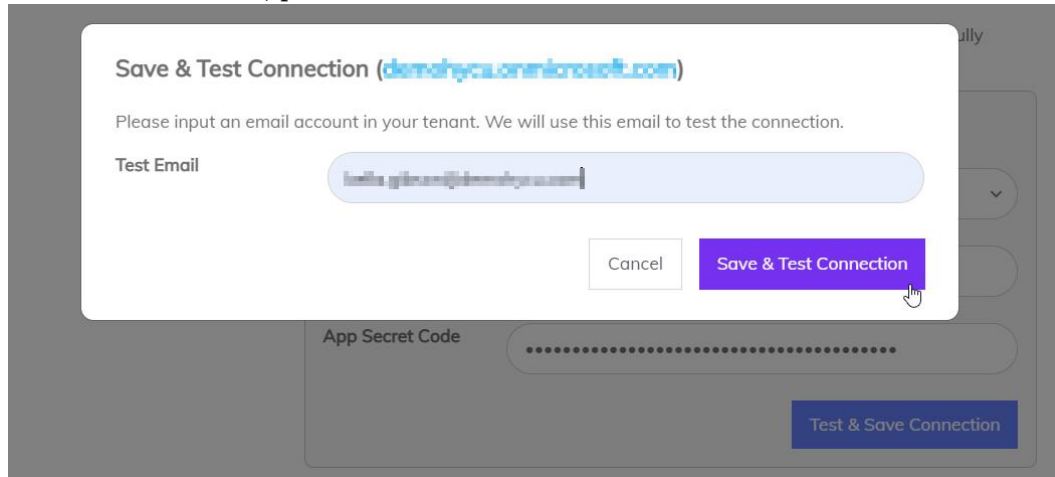
☐ I confirm that I understand the following aspects of Teams Private Chat Backup:

- The cost of message retrieval will be incurred by the owner of the tenant and the billing will be direct from Microsoft based on messages retrieved.
- If the number of messages retrieved per month exceeds the max limit set, then the backup of messages will be suspended for the rest of the month.

**Test & Save Connection**

[Show less](#)

3. To test the connection, provide an email account in the tenant and click **Save & Test Connection**.



The screenshot shows a modal dialog box titled "Save & Test Connection (demo@hycloud.com)". The dialog contains the instruction: "Please input an email account in your tenant. We will use this email to test the connection." Below this, there is a "Test Email" label and a text input field containing "demo@hycloud.com". At the bottom of the dialog are two buttons: "Cancel" and "Save & Test Connection". A mouse cursor is hovering over the "Save & Test Connection" button. In the background, a portion of the main interface is visible, showing an "App Secret Code" field with a masked input and a "Test & Save Connection" button.



