



HYCU R-Cloud for Microsoft 365

Private Chat Backup

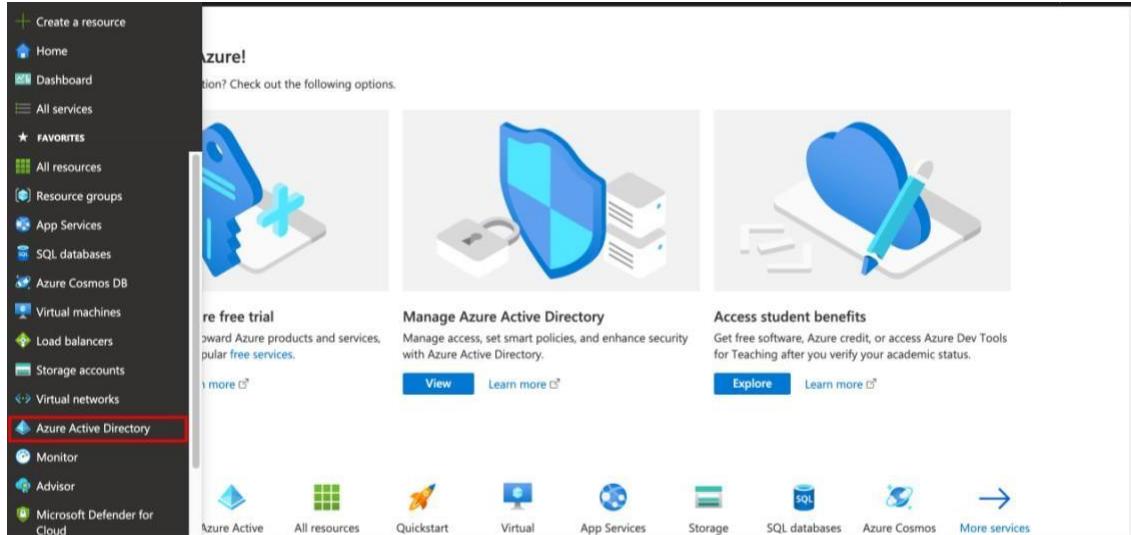
Overview

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:

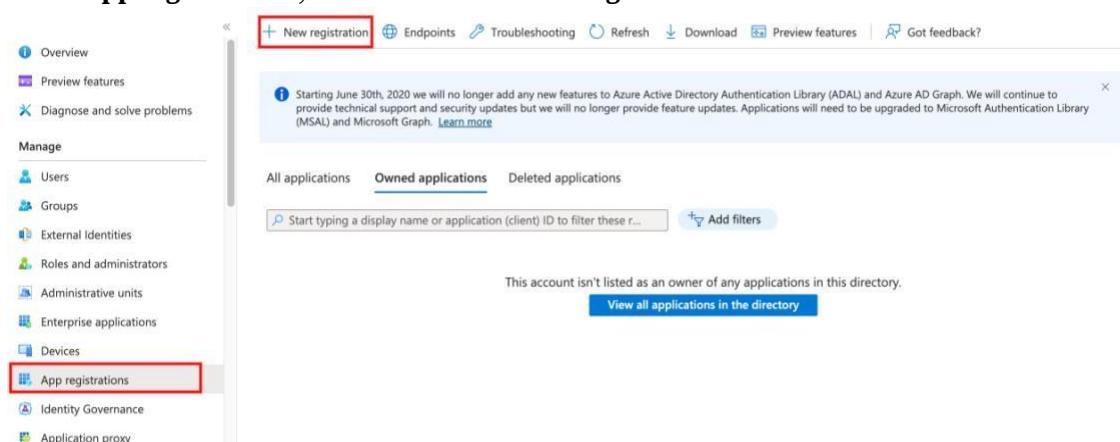
1. Register a new application using Microsoft Azure Portal.
2. Set up the new registered application as it relates to certificates and API permissions.
3. Associate the created application with the Azure billing resource.

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

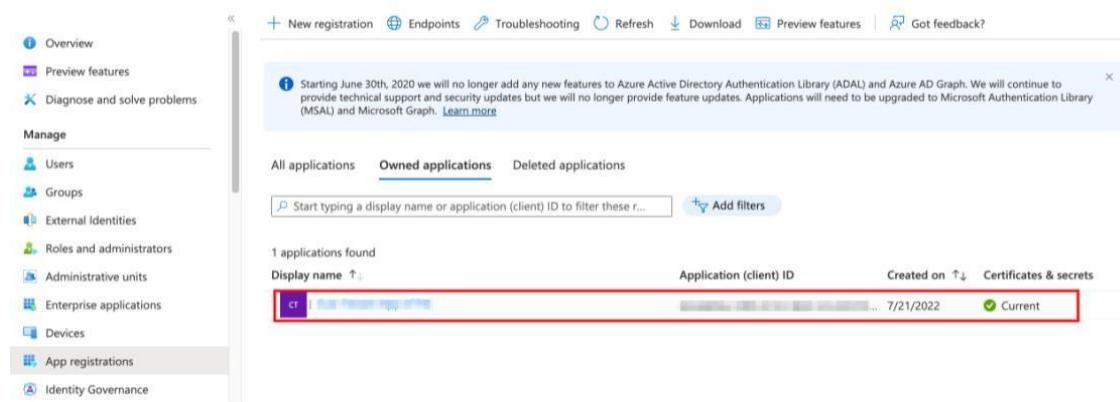


Supported account types

Who can use this application or access this API?

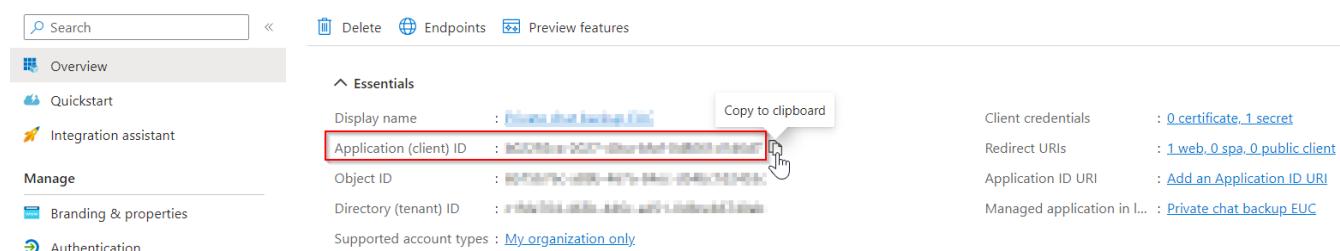
 Accounts in this organizational directory only (DemoHYCU only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only[Help me choose...](#)

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



The screenshot shows the 'Owned applications' section of the Azure portal. On the left, a sidebar lists 'Overview', 'Preview features', and 'Diagnose and solve problems'. Under 'Manage', 'App registrations' is selected. The main area shows a table with one application listed. The application details are: Display name: 'Private chat backup EUC', Application (client) ID: '00000000-0000-0000-0000-000000000000', Created on: '7/21/2022', and Certificates & secrets: 'Current'. A red box highlights the application name 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.

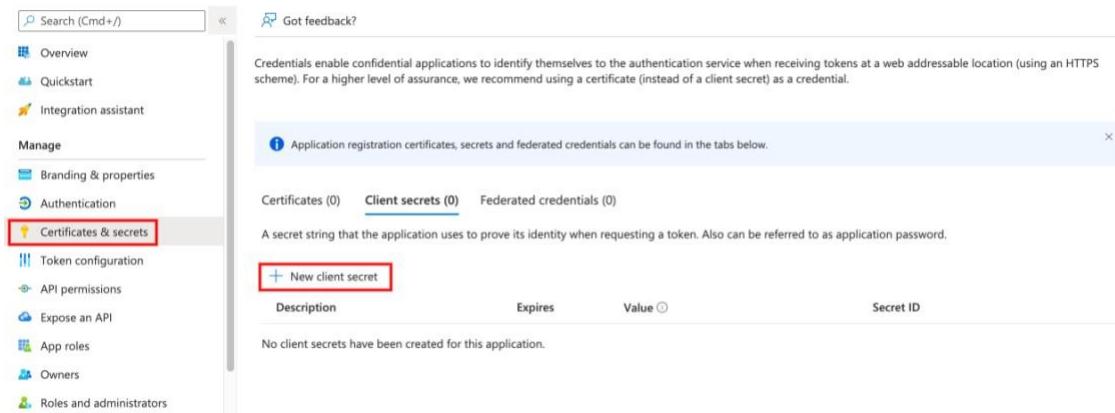


The screenshot shows the application details for 'Private chat backup EUC'. Under the 'Essentials' section, the 'Application (client) ID' field is highlighted with a red box. A cursor is hovering over the field, and a 'Copy to clipboard' button is visible. To the right, there are sections for 'Client credentials', 'Redirect URIs', 'Application ID URI', and 'Managed application in l...'. The 'Application (client) ID' value is '00000000-0000-0000-0000-000000000000'.

Set up the registered application

1. Select the registered application.

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



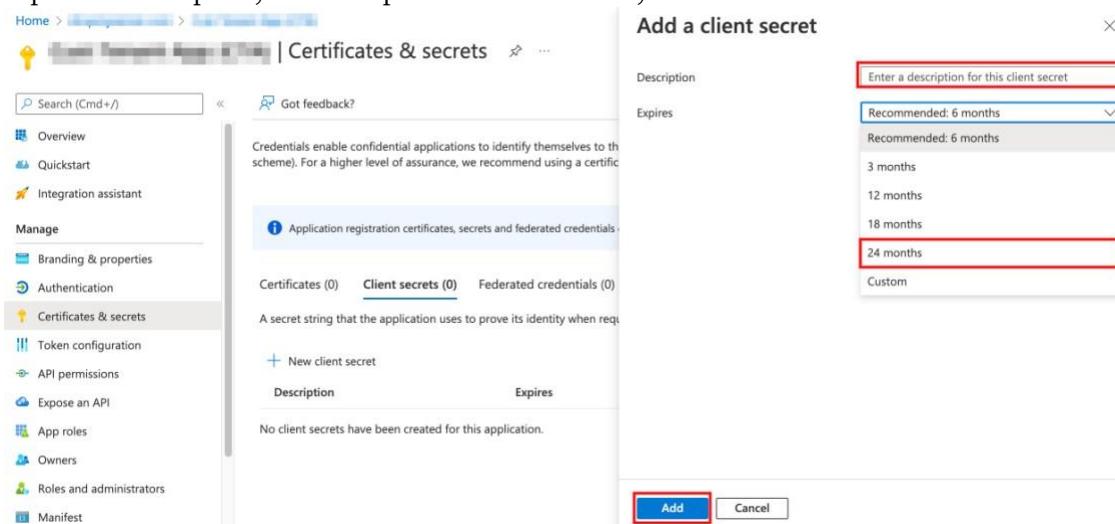
Certificates (0) Client secrets (0) Federated credentials (0)

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
No client secrets have been created for this application.			

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



Enter a description for this client secret

Recommended: 6 months

Recommended: 6 months

3 months

12 months

18 months

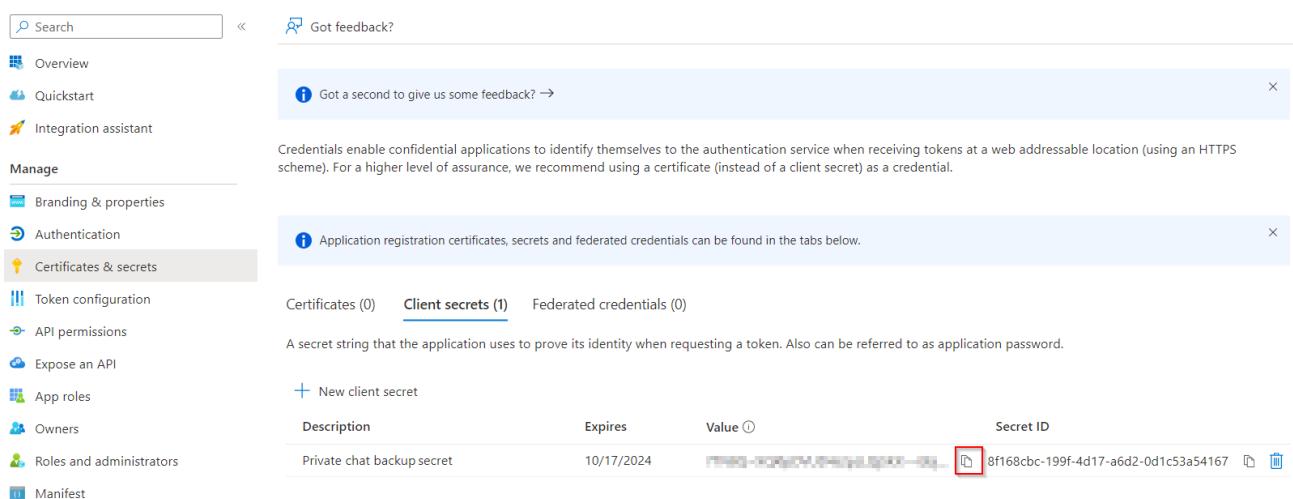
24 months

Custom

Add Cancel

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.



Got a second to give us some feedback? →

Credentials enable confidential 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.

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

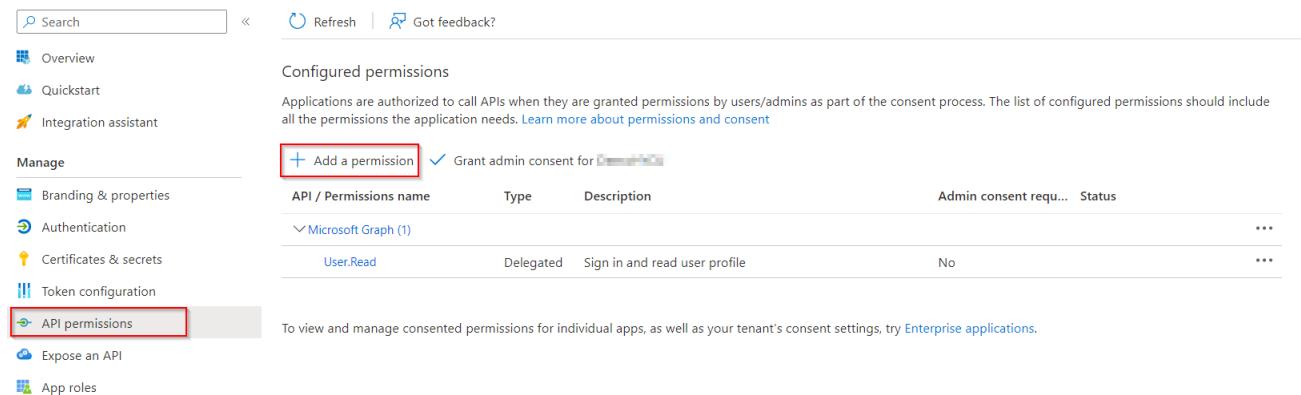
Certificates (0) Client secrets (1) Federated credentials (0)

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
Private chat backup secret	10/17/2024	8f168cbc-199f-4d17-a6d2-0d1c53a54167	

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



Configured permissions

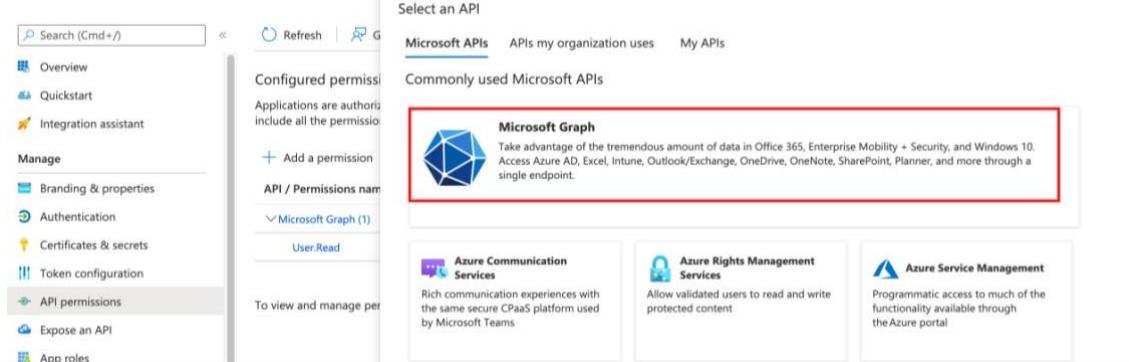
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for [\[redacted\]](#)

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**.



Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

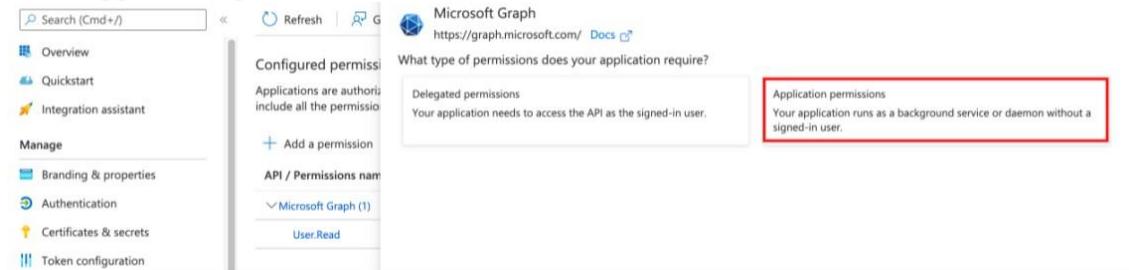
Microsoft Graph Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

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**.



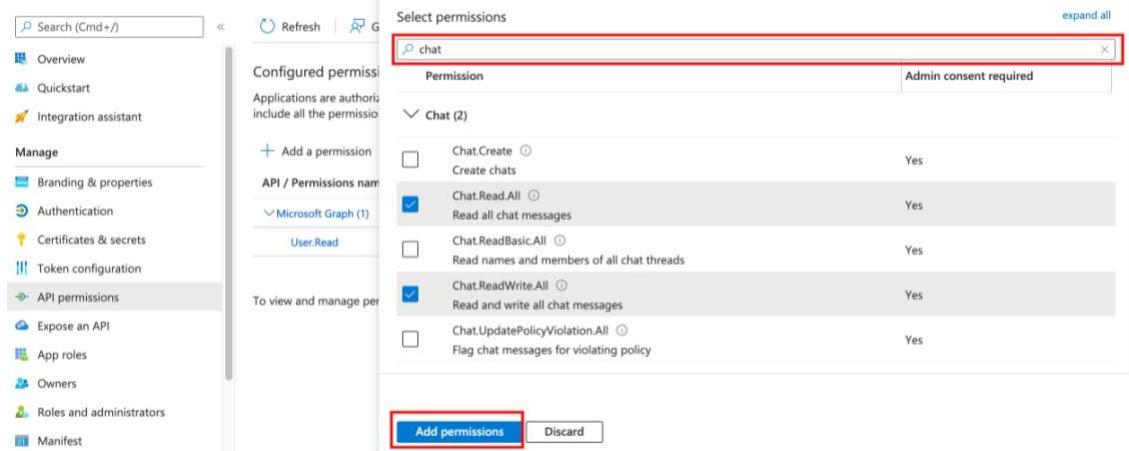
Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

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**.



Select permissions

chat

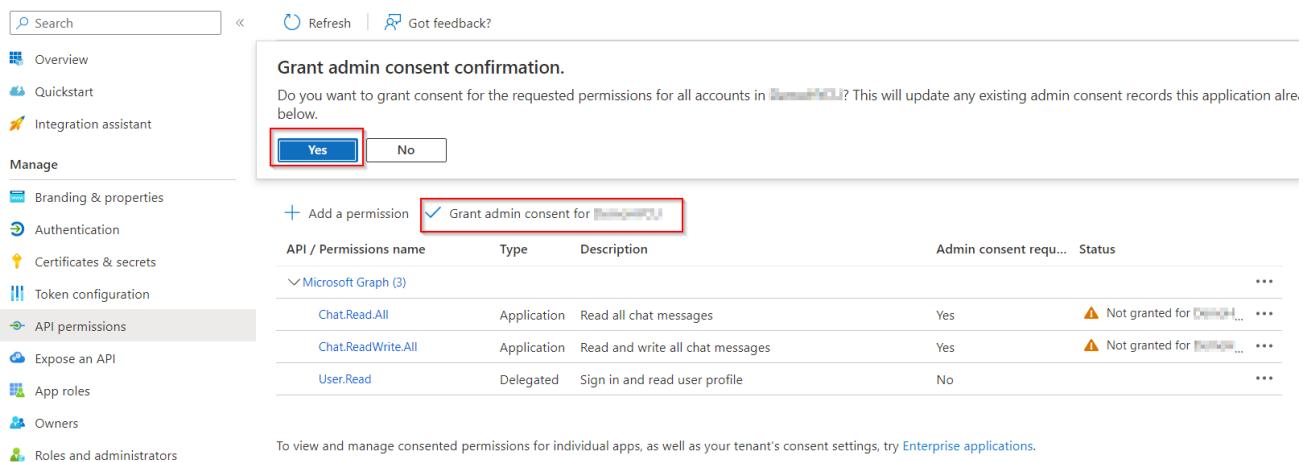
Permission Admin consent required

Chat (2)

<input type="checkbox"/> Chat.Create	Yes
<input checked="" type="checkbox"/> Chat.Read.All	Yes
<input type="checkbox"/> Chat.ReadBasic.All	Yes
<input checked="" type="checkbox"/> Chat.ReadWrite.All	Yes
<input type="checkbox"/> Chat.UpdatePolicyViolation.All	Yes

Add permissions **Discard**

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



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in **[REDACTED]**? This will update any existing admin consent records this application already has.

Yes **No**

+ Add a permission **Grant admin consent for [REDACTED]**

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

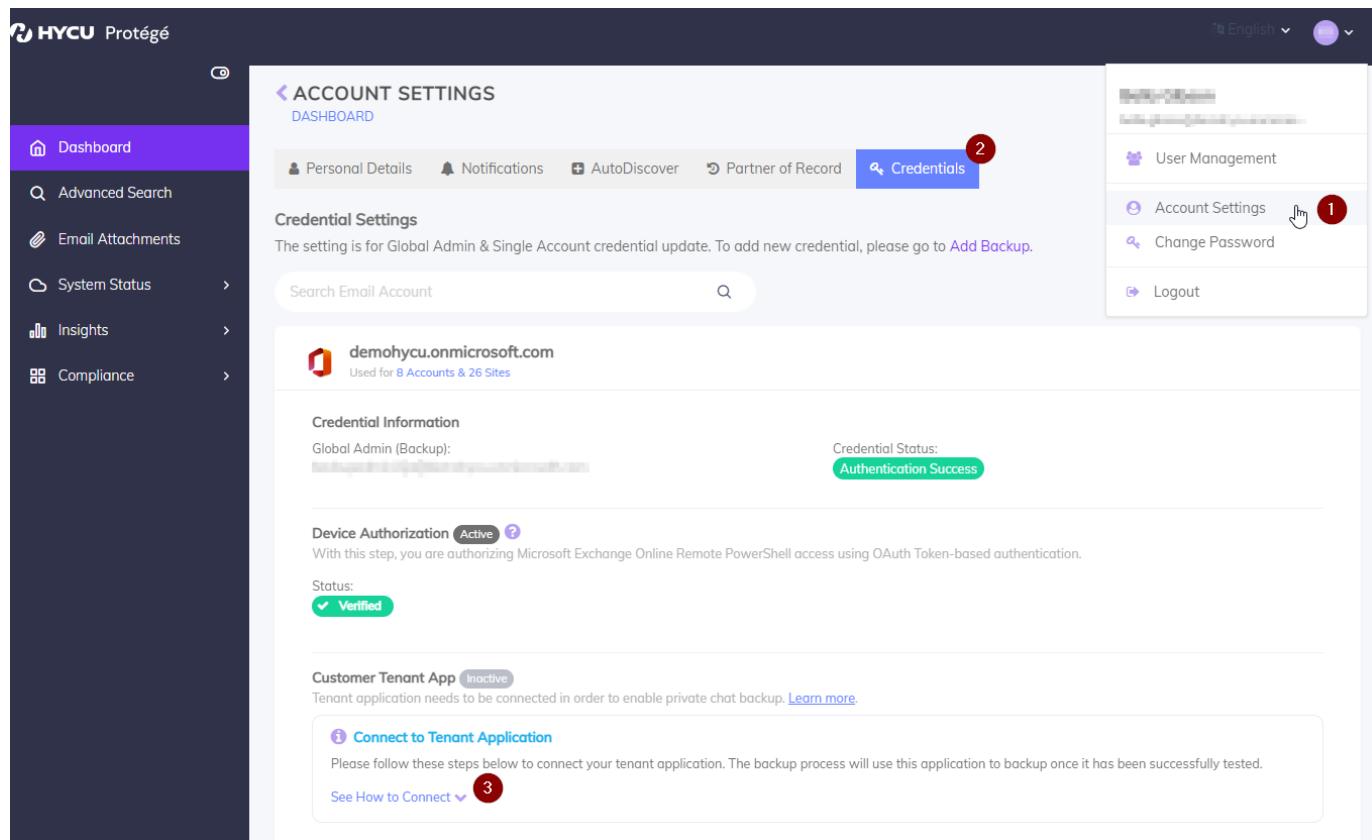
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

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**.



The screenshot shows the HYCU Protégé interface. The left sidebar has a purple header with the HYCU logo and 'Protégé'. The main menu items are: Dashboard, Advanced Search, Email Attachments, System Status, Insights, and Compliance. The 'Credentials' tab is highlighted with a red circle containing the number '2'. The top navigation bar includes: Personal Details, Notifications, AutoDiscover, Partner of Record, and a search bar for 'Credentials'. The right sidebar has a 'Logout' button. The main content area is titled 'ACCOUNT SETTINGS DASHBOARD' and shows 'Credential Settings' for 'demohycu.onmicrosoft.com' (Used for 8 Accounts & 26 Sites). It shows 'Global Admin (Backup)' with a redacted value and 'Credential Status: Authentication Success'. It also shows 'Device Authorization' (Active) with a redacted value and 'Customer Tenant App' (Inactive) with a redacted value. A 'Connect to Tenant Application' section with a red circle containing the number '3' is present.

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	<input type="text" value="Application ID"/>
App Secret Code	<input type="text" value="App Secret Code"/>
Max. Limit of Message per Month	<input type="text" value="Max. Limit of Message per Month"/> <input type="checkbox"/> Set to unlimited

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

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

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

