



USER GUIDE DOCUMENT FOR

PRIVATE CHAT BACKUP SERVICE

Version 6.0.0
2026 April

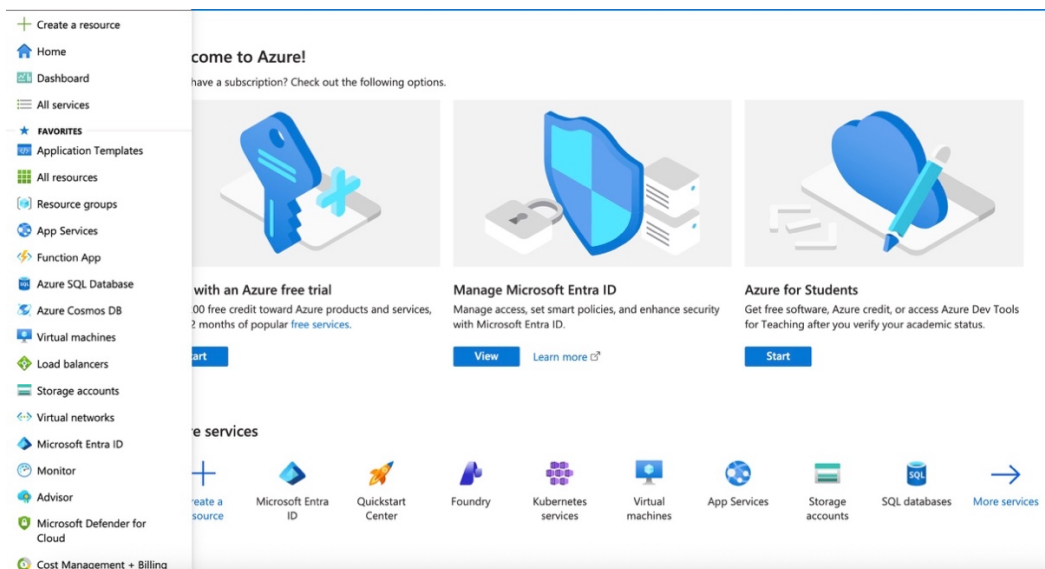


Overview

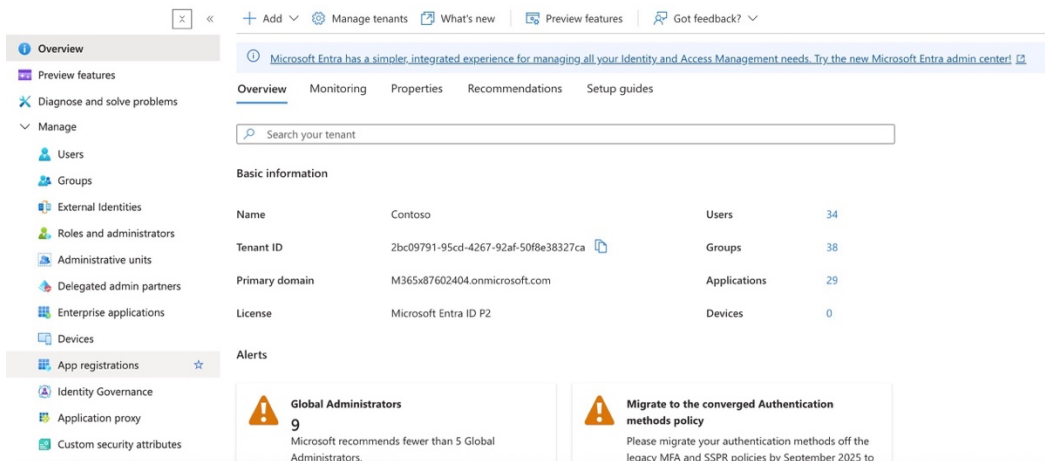
Once you decide to begin backing up Microsoft private chat to the system, you'll need to complete some setup on the Microsoft side. The process is straightforward. First, register a new application in the Microsoft Azure Portal. After that, configure the registered application by setting up its certificates and API permissions.

Register A New Application

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



3. Select **App registrations**, then select **+ Add > App registration**



Private and Confidential

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

Register an application ...

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

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Contoso only - Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

5. Once completed, the system will display detail info. Copy the Application (client) ID and paste it to our portal as the Application ID.

The screenshot shows the 'Overview' page for an application named 'created 13 feb'. The page includes a navigation sidebar with options like 'Quickstart', 'Integration assistant', 'Diagnose and solve problems', 'Manage', and 'Support + Troubleshooting'. The main content area displays 'Essentials' information:

Display name	: created 13 feb	Client credentials	: Add a certificate or secret
Application (client) ID	: d0ef0cef-578e-411c-9c3d-3bf4ae424cb7	Redirect URIs	: Add a Redirect URI
Object ID	: a359261c-cd02-4ef4-a1e2-95590ab6dca2	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 2bc09791-95cd-4267-92af-50f8e38327ca	Managed application in L...	: created 13 feb
Supported account types	: My organization only		

Below the essentials, there are two informational messages:

- Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).
- Welcome to the new and improved App registrations. Looking to learn how to change from App Registrations (Legacy)? [Learn more](#)
- Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

At the bottom, there is a section titled 'Build your application with the Microsoft identity platform' with a brief description and a 'Learn' link.

Private and Confidential

The screenshot shows the 'ACCOUNT SETTINGS' dashboard with the 'Credentials' tab selected. The page title is 'Credential Settings' and it includes a search bar for email accounts and filters for 'Type' and 'Status'. The main content area displays information for the tenant 'M365x87602404.onmicrosoft.com'. Under 'Credential Information', the status is 'Authentication Success'. Under 'Service Authorization', it states that the Exchange Online Management App is authorized to create a custom RBAC role. Under 'Custom Role Status', the status is 'Connected'. A 'Customer Tenant App' section is marked as 'Inactive' and includes a 'Connect to Tenant Application' instruction. Below this, there are two steps: 'Step 1: Setup an application in your tenant M365x87602404.onmicrosoft.com.' and 'Step 2: Enter the following application details in the form below.' The form contains two input fields: 'Application ID' and 'App Secret Code', both with placeholder text. A 'Test & Save Connection' button is located at the bottom right of the form.

ACCOUNT SETTINGS
DASHBOARD

Personal Details Notifications AutoDiscover Credentials

Credential Settings

The setting is for updating Domains & Single Accounts credentials. To add a new credential, please navigate to [Add Backup](#).

Search Email Account Q Type: All Status: All

M365x87602404.onmicrosoft.com
Used for 1 Accounts

Credential Information

Credential Status:
Authentication Success

Service Authorization ?
The Exchange Online Management App is authorized to create a custom RBAC role, incorporating only the minimum required PowerShell cmdlets.

Custom Role Status:
Connected

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 the steps below to connect your tenant application. The backup process will use this application to begin the backup once it has been successfully tested.

Step 1: Setup an application in your tenant M365x87602404.onmicrosoft.com.

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

Application ID

App Secret Code

Test & Save Connection

Setup The Registered Application

1. Go to <https://portal.azure.com> and log in using your tenant admin credentials.
2. Select **Microsoft Entra ID** (formerly Azure Active Directory) in the left navigation bar.
3. Select App Registrations, and select All applications tab.

Display name	Application (client) ID	Created on	Certificates & secrets
2nd attemp	7bcfbcb6-8fb3-4db2-9f00-7f9334f556d7	2/13/2026	-
Backup Application 3UmZ	9fcf14cb-625c-46c0-8cf0-b98daaf9512d	1/21/2026	Current
Backup Application 6cnL	df741642-8041-48d1-972a-c8c071762673	1/6/2026	Current
Backup Application C05Z	ee221f9f-d835-449a-9542-98541c2c24f6	1/6/2026	Current
Backup Application dEao	627f764b-f63d-440f-acb5-e201cec8d8e7	1/6/2026	Current
Backup Application fdUl	08aab7f7-da1c-43ac-a20a-c8c491fe865b	1/6/2026	Current
Backup Application fgjb	2332e74f-6db8-4e26-9fc4-dbd8ae8962d1b	1/6/2026	Current
Backup Application G1pq	eadfe219-205c-4d51-9963-217b8d6bed62	1/6/2026	Current

4. Select the registered application you've created on the above section.
5. Expand Manage then select **Certificates & secrets**. Click **+ New client secret**.

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

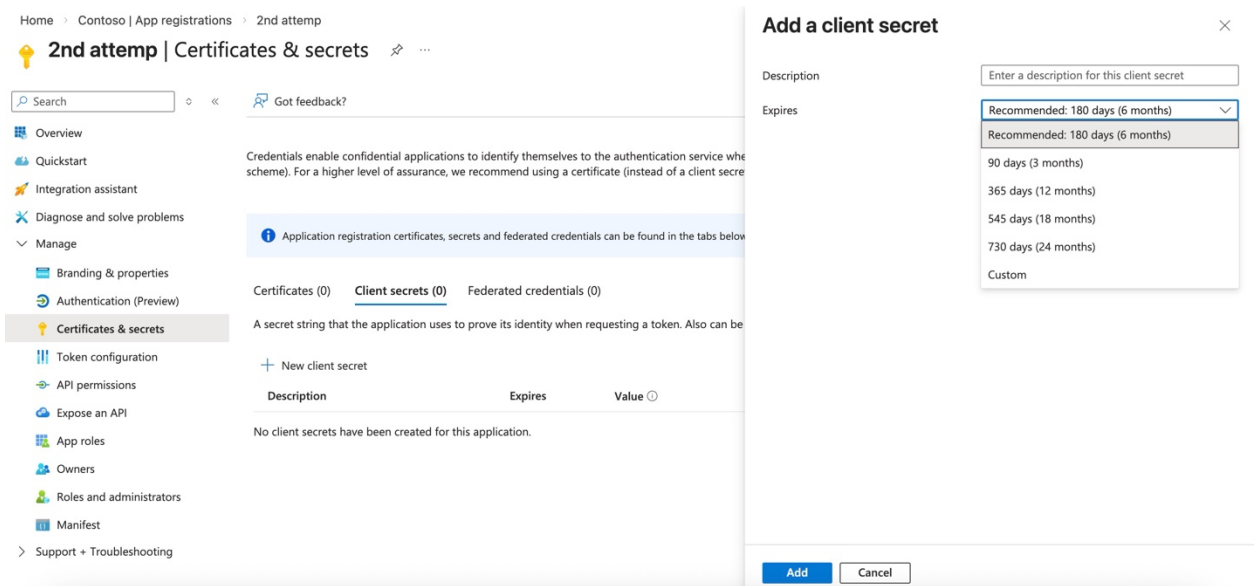
Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

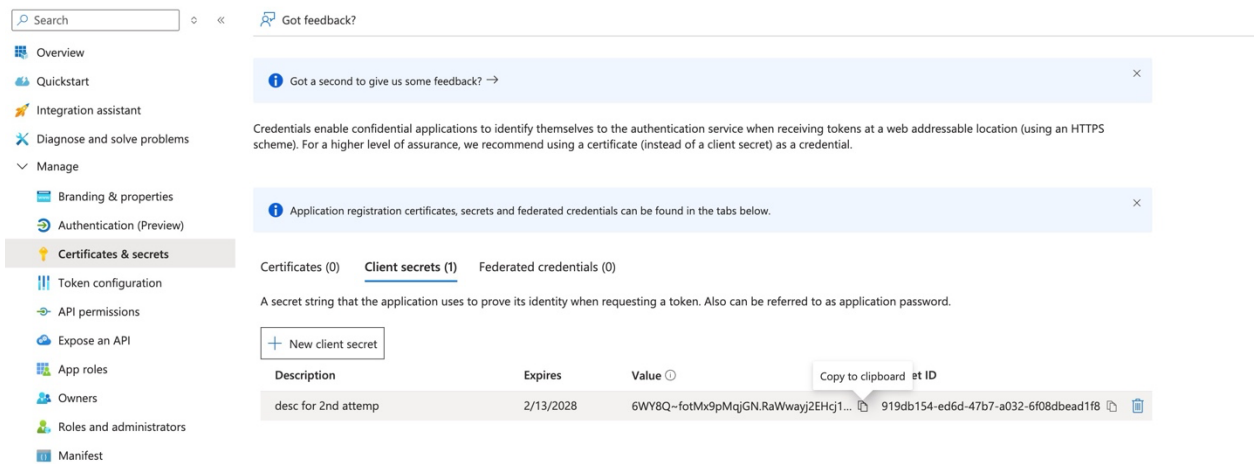
+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

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



7. Once added, immediately copy the value, and paste it to our portal as the application secret code. **Please note:** Microsoft 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.



Private and Confidential

ACCOUNT SETTINGS
DASHBOARD

Personal Details Notifications AutoDiscover **Credentials**

Credential Settings
The setting is for updating Domains & Single Accounts credentials. To add a new credential, please navigate to [Add Backup](#).

Search Email Account Q Type: All Status: All

M365x87602404.onmicrosoft.com
Used for 1 Accounts

Credential Information
Credential Status: **Authentication Success**

Service Authorization
The Exchange Online Management App is authorized to create a custom RBAC role, incorporating only the minimum required PowerShell cmdlets.
Custom Role Status: **Connected**

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 the steps below to connect your tenant application. The backup process will use this application to begin the backup once it has been successfully tested.

Step 1: Setup an application in your tenant **M365x87602404.onmicrosoft.com**.

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

Application ID

App Secret Code

Test & Save Connection

8. Select API permissions, then select + Add a permission.

Search Refresh Got feedback?

Overview Quickstart Integration assistant Diagnose and solve problems Manage Branding & properties Authentication (Preview) Certificates & secrets Token configuration **API permissions** Expose an API App roles Owners Roles and administrators Manifest Support + Troubleshooting

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

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 Contoso

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](#).

9. Select Microsoft Graph.

Request API permissions

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 Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.
- 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
- Dynamics CRM**
Access the capabilities of CRM business software and ERP systems
- Intune**
Programmatic access to Intune data
- Office 365 Management APIs**
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs
- OneNote**
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

10. Select Application permissions.

Request API permissions

< All APIs

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.

Application permissions Your application runs as a background service or daemon without a signed-in user.

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

Request API permissions

Select permissions expand all

Search: chat

Permission	Admin consent required
<input type="checkbox"/> Chat.Create Create chats	Yes
<input type="checkbox"/> Chat.ManageDeletion.All Delete and recover deleted chats	Yes
<input checked="" type="checkbox"/> Chat.Read.All Read all chat messages	Yes
<input type="checkbox"/> Chat.Read.WhereInstalled Read all chat messages for chats where the associated Teams application is installed.	Yes
<input type="checkbox"/> Chat.ReadBasic.All Read names and members of all chat threads	Yes
<input type="checkbox"/> Chat.ReadBasic.WhereInstalled Read names and members of all chat threads where the associated Teams application is	Yes
<input checked="" type="checkbox"/> Chat.ReadWrite.All Read and write all chat messages	Yes

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

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](#)

API / Permissions name	Type	Admin consent required	Status
Microsoft Graph (3)			
Chat.Read.All	Application	Yes	⚠ Not granted for Contoso
Chat.ReadWrite.All	Application	Yes	⚠ Not granted for Contoso
User.Read	Delegated	No	