



# Application Manager Portal Authentication

Last Modified on 01.09.24

Application Manager Portal authentication relies on the Microsoft Authentication Library (MSAL). In order for ADAL to work, you must approve the **Recast Application Manager Portal** Azure AD enterprise application in your environment. MSAL requires a Microsoft Organization Account or Microsoft Account. You can read more about Microsoft Accounts and their differences [here](#).

If your organization is not using Azure AD, skip to **Scenario 4**.

## Scenario 1: Request without admin consent workflow

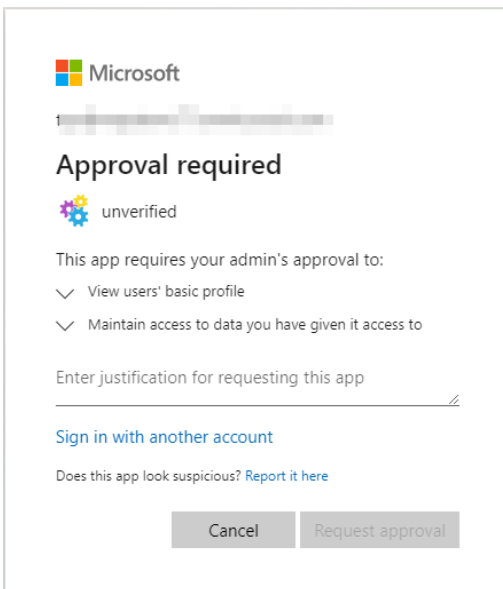
If your organization doesn't have an admin consent workflow configured, you can approve the enterprise app yourself. Select **Consent on behalf of your organization** and click **Accept** to continue to the Application Manager Portal.

The screenshot shows a Microsoft permissions request dialog. At the top is the Microsoft logo. Below it is a blurred header. The main heading is "Permissions requested". Underneath, there is a gear icon followed by "Recast Application Manager Portal" and "unverified" in blue. A warning message states: "This application is not published by Microsoft or your organization." Below this, it says "This app would like to:" followed by three items: "View your basic profile" (checked), "Maintain access to data you have given it access to" (checked), and "Consent on behalf of your organization" (unchecked). A paragraph of text explains that accepting permissions allows the app to use user data as specified in its terms of service and privacy statement, and notes that the publisher has not provided links to their terms for review. It provides a link to "https://myapps.microsoft.com" and a "Show details" link. At the bottom, there is a question "Does this app look suspicious?" with a "Report it here" link. Two buttons are at the bottom: "Cancel" and "Accept".

## Scenario 2: Request with admin consent workflow

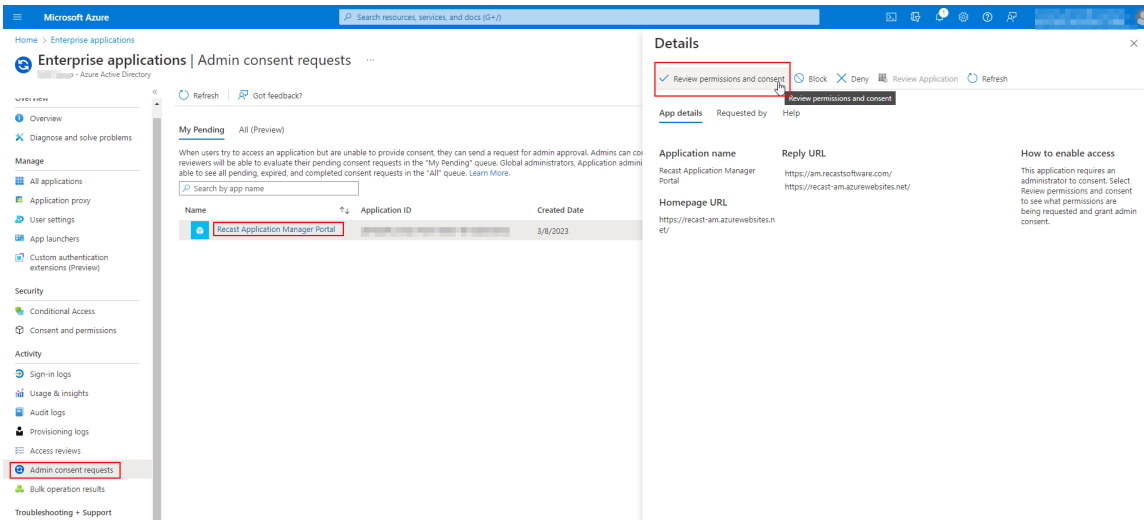
### Requester point of view

Some organizations have [admin consent workflow](#) enabled, which means that the consent request must be forwarded to the Azure administrator. In this case, log into our Portal and try to sign in. Enter the reason for the request and click **Request approval**. Your Azure administrator will receive a notification to approve the app.



## Admin point of view

The Azure administrator can approve the enterprise app from **Azure Portal > Enterprise Applications > Admin consent requests**. Select the app and click **Review permissions and consent** to open the consent window and approve the application.



After consent, make sure the **Assignment required** setting in the enterprise application properties is set to 'No'. If assignment required is set to 'Yes', you need to grant access to Portal users from the **Users and groups** tab:

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Recast Application Manager Portal

## Recast Application Manager Portal | Properties

Enterprise Application

Save Discard Delete Got feedback?


View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

Some of the displayed properties that are not editable are managed on the application registration in the application's home tenant.

Enabled for users to sign-in?  Yes  No

Name

Homepage URL

Logo 

Application ID

Object ID

Assignment required?  Yes  No

Visible to users?  Yes  No

To learn more, see Microsoft's documentation about [admin consent](#).

## Scenario 3: Need admin approval

### Requester point of view

Some organizations have disabled the ability to send enterprise application consent request. You are unable to login until global administrator has accepted the application.



### Need admin approval



needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

[Have an admin account? Sign in with that account](#)



[Return to the application without granting consent](#)

### Admin point of view

1. Open the following link with Azure AD global administrator account:


[https://login.microsoftonline.com/common/adminconsent?client\\_id=d04d6842-6082-40d4-b455-49136b959a7d](https://login.microsoftonline.com/common/adminconsent?client_id=d04d6842-6082-40d4-b455-49136b959a7d)

2. Select **Accept**

## Permissions requested

Review for your organization



Recast Application Manager Portal  
**unverified**

**This application is not published by Microsoft or your organization.**

This app would like to:

- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

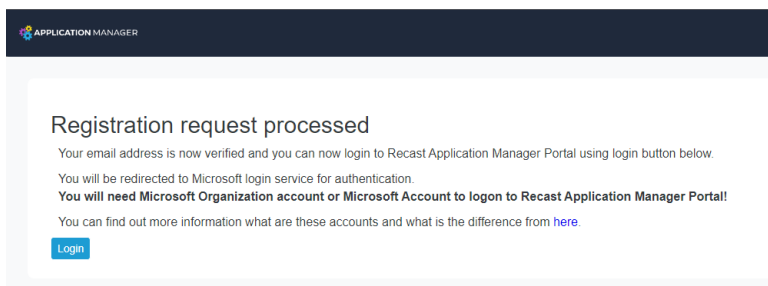
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

## Scenario 4: Register without Azure AD

To register without Azure AD:

1. Open the verification link in the Application Manager Portal registration email.
2. On the registration page, click **Login**.



APPLICATION MANAGER

### Registration request processed

Your email address is now verified and you can now login to Recast Application Manager Portal using login button below.  
You will be redirected to Microsoft login service for authentication.  
**You will need Microsoft Organization account or Microsoft Account to logon to Recast Application Manager Portal!**  
You can find out more information what are these accounts and what is the difference from [here](#).

3. On the Application Manager portal sign-in page, create a Microsoft account by clicking **Create one**. If you already have a Microsoft account with your organizational email address, skip to Step 6.
4. Enter your organizational email address, and click **Next**.
5. Follow prompts to create a password and verify your email address.
6. Once you've created your new Microsoft account, click **Yes** to let the app access your information.



## Let this app access your info?

unverified

Recast Application Manager Portal needs your permission to:



### View your basic profile

Recast Application Manager Portal will be able to see your basic profile (name, picture, user name).



### Maintain access to data you have given Recast Application Manager Portal access to

Allows Recast Application Manager Portal to see and update the data you gave it access to, even when you are not currently using the app. This does not give Recast Application Manager Portal any additional permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://microsoft.com/consent>. [Show details](#)

No

Yes