

Application Manager Legacy Portal Authentication

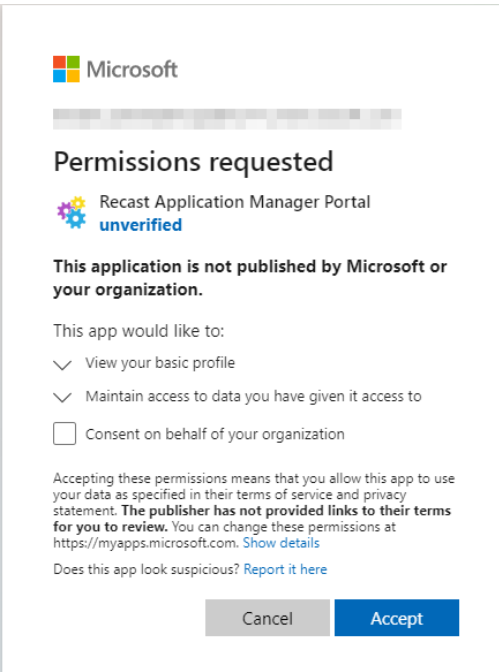
Last Modified on 11.20.25

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.



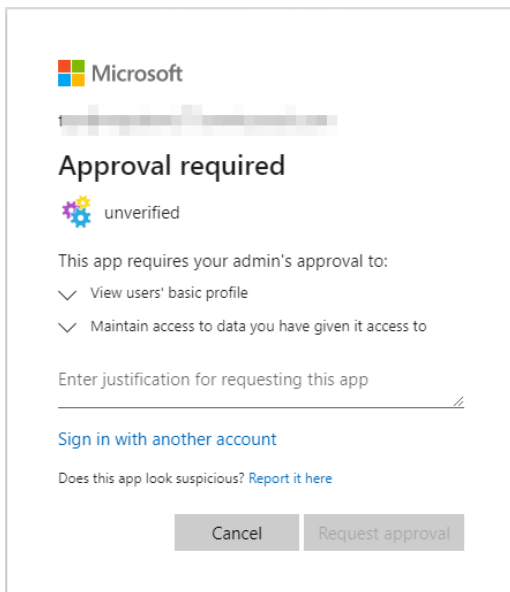
The screenshot shows a Microsoft permissions request dialog. At the top is the Microsoft logo. Below it is a blurred header. The main heading is "Permissions requested". Underneath, there is a gear icon and the text "Recast Application Manager Portal" with "unverified" in blue below it. A warning message 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 disclaimer follows: "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". At the bottom, it asks "Does this app look suspicious? Report it here" and has "Cancel" and "Accept" buttons.

Scenario 2: Request with admin consent workflow

Requester point of view

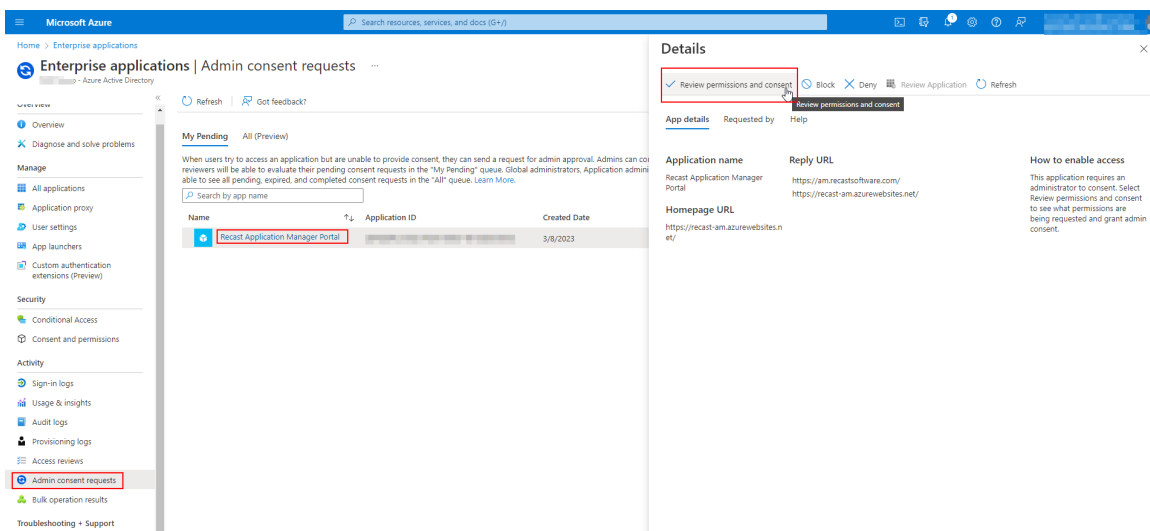
Some organizations have [admin consent workflow](#) enabled, which means that the consent request must be forwarded to the Azure administrator. In this case, log into our Portal and try to sign in. Enter the reason for the request and click **Request approval**. Your Azure administrator will receive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

Recast



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:

The screenshot shows the Microsoft Azure portal interface for the 'Recast Application Manager Portal'. The left sidebar contains navigation options like Overview, Deployment Plan, and Manage. The main content area shows the application's properties, including Name, Homepage URL, Application ID, and Object ID. The 'Assignment required?' toggle is currently set to 'No', and a mouse cursor is hovering over it.

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.

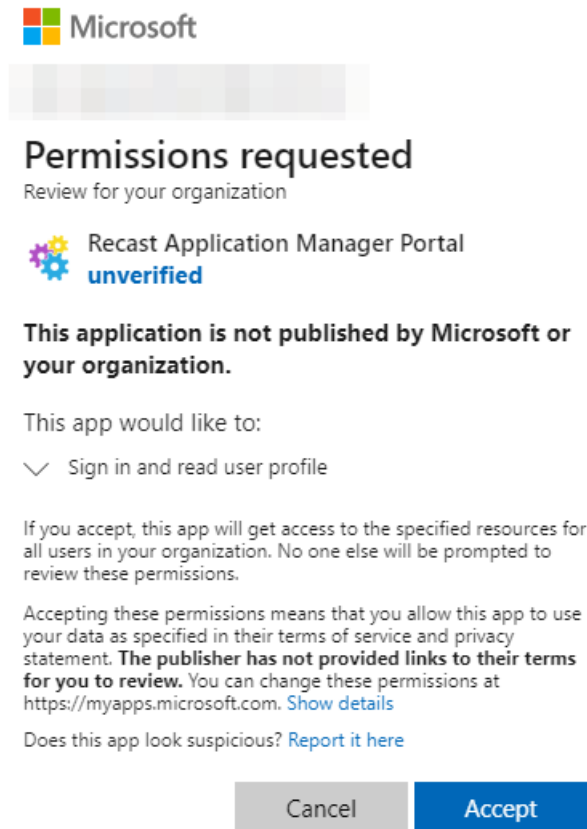
[Have an admin account? Sign in with that account](#)

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

Admin point of view

Recast

1. Open the following link with Azure AD global administrator account:
https://login.microsoftonline.com/common/adminconsent?client_id=d04d6842-6082-40d4-b455-49136b959a7d
2. Select **Accept**

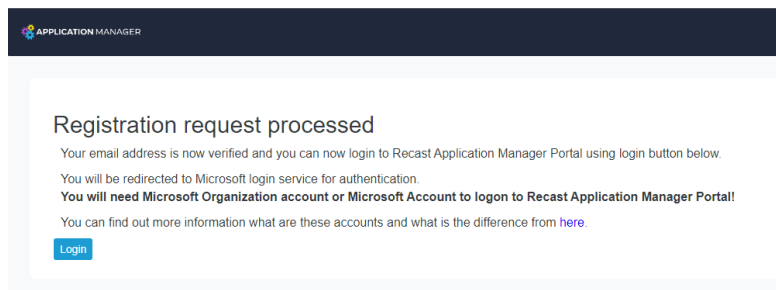


The screenshot shows a Microsoft permissions dialog box. At the top is the Microsoft logo. Below it is a blurred header. The main heading is "Permissions requested" with the subtitle "Review for your organization". The application name is "Recast Application Manager Portal" with a status of "unverified". 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 a checkmark and "Sign in and read user profile". A paragraph explains that accepting grants access to resources for all users and that the publisher has not provided links to their terms. A link to "Show details" is provided. At the bottom, there are "Cancel" and "Accept" buttons.

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**.



The screenshot shows the "Registration request processed" page in the Application Manager Portal. The header includes the "APPLICATION MANAGER" logo. The main heading is "Registration request processed". The text below states: "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." A blue "Login" button is visible at the bottom.

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.

Recast

6. Once you've created your new Microsoft account, click **Yes** to let the app access your information.

