

## Viewing and Changing Consent Policies in the Azure Portal

<https://campus.barracuda.com/doc/100368461/>

Note that this article refers only to the new end user interface in Email Gateway Defense made available to customers over the course of 2023-2024.

For more information on the new end user interface, see [Email Gateway Defense New User Interface User Guide](#).

With recent changes made to the Email Gateway Defense SSO login flow for the new user interface, an administrator may need to grant consent to the Email Gateway Defense app for your organization. End users may also see a consent screen based on the security consent policies set in Microsoft Entra ID by the administrator.

Note that either a user or a global administrator must establish consent between the Email Gateway Defense app and your organization's Microsoft Entra ID in order for login to proceed. The consent method, either by a global administrator or a user, is determined by the consent policy selected for your organization. The most restrictive policy requires an administrator to grant consent for the entire organization. The Microsoft recommended policy and the least restrictive policy allow end users to consent to use the app on an individual basis. A description of the consent policies and how to view and change them are provided in this article.

### Manage Access to Email Gateway Defense Application

To view or change the consent policies for users:

1. Log into the [Microsoft Entra admin center](#) (formerly Azure Active Directory) as a global administrator for the directory.
2. Select **Microsoft Entra ID** under Azure services.
3. Select **Enterprise applications** in the left-hand menu.
4. On the **Enterprise applications - All applications** page, go to **Security > Consent and permissions**.
5. Under **User consent settings**, select one of the options:
  - **Do not allow user consent** - Users cannot grant permissions to any application. Users can sign into applications that administrators have granted consent to on their behalf, but they cannot consent to new permissions to applications on their own.
  - **Allow user consent for apps from verified publishers, for selected permissions (Recommended)** - Users can consent only to applications that were published by a verified publisher or applications added to your tenant.
  - **Allow user consent for apps** - Users can consent to any permissions for any application without administrator consent.

6. Click **Save**.

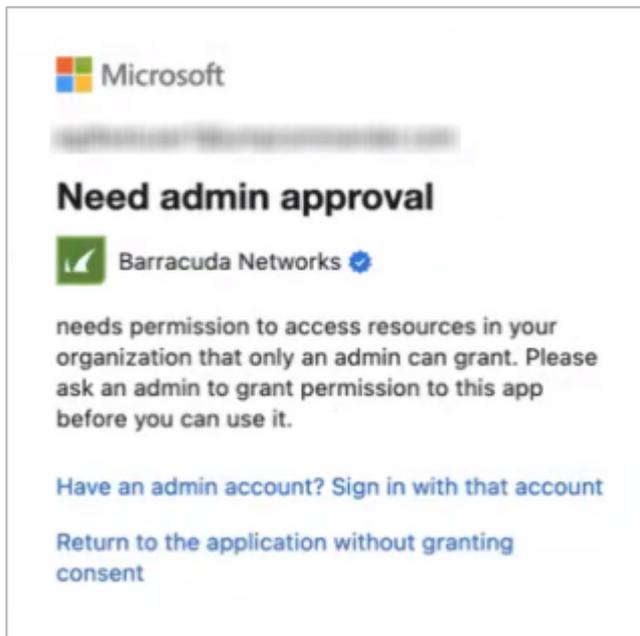
## User Consent Flows

When the end user logs into Email Gateway Defense, they will see one of the below user consent flows based on the selected policies above.

### Do not allow user consent

Users will be blocked from granting consent to any application. Users can sign into applications that administrators have granted consent to on their behalf, but they cannot consent to new permissions to applications on their own.

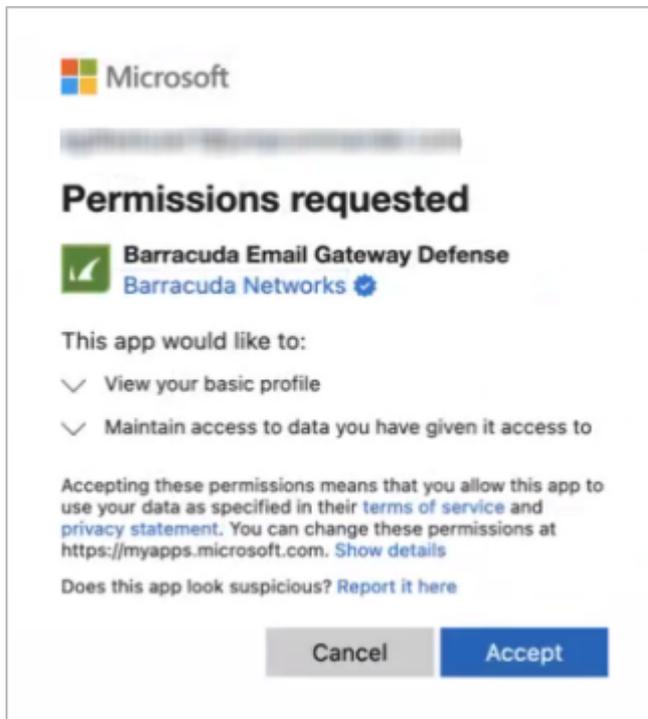
As a user, you will need to contact your administrator to grant access. You will not be able to access the application until your administrator grants consent.



### Allow user consent for apps from verified publishers, for selected permissions (Recommended)

Users will see the consent prompt to accept the permissions only for an application from a verified publisher or an application added to your tenant.

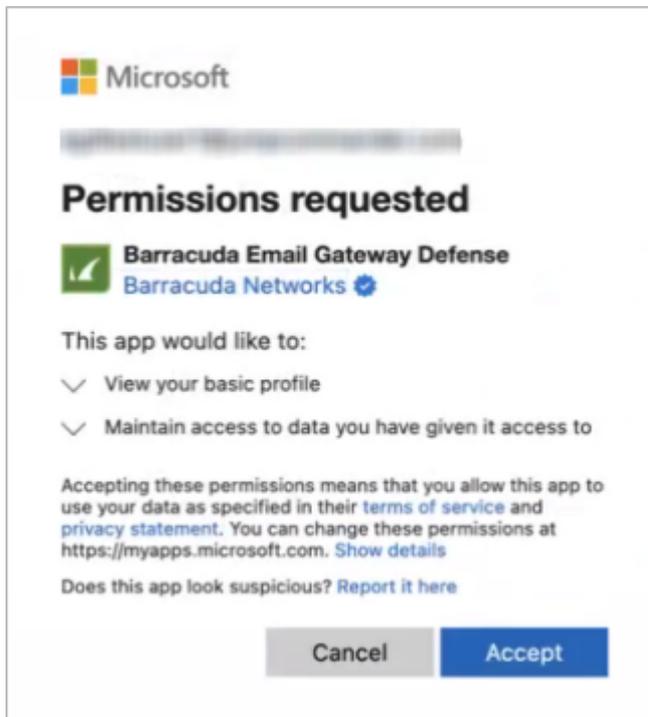
As a user, it is safe to click **Accept** to gain access to the application.



## Allow user consent for apps

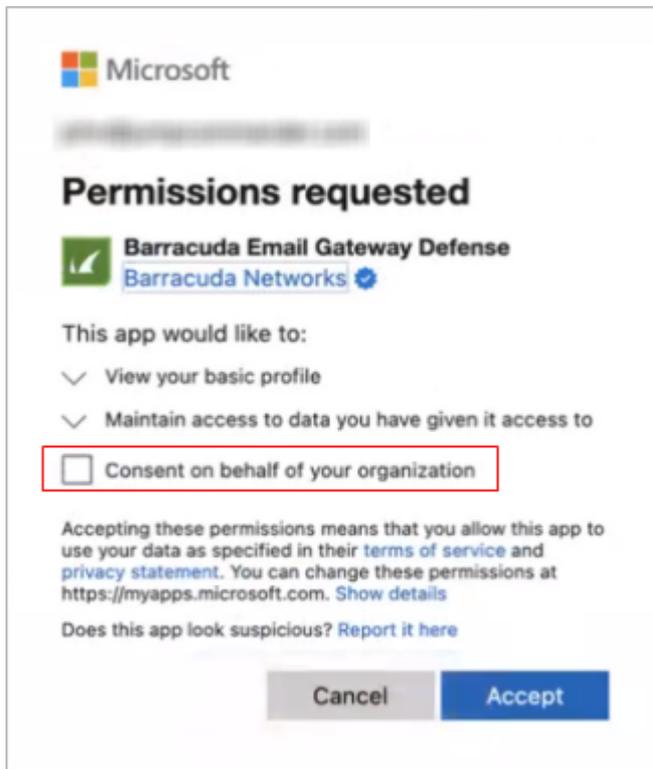
Users will see the consent prompt to accept the permissions for any application.

Users can consent to any permissions for any application, regardless of publisher or status (verified or unverified).



## Admin Consent Flow

In addition to the above scenarios, as an administrator, you can grant consent for the application on behalf of all users in the organization. When you log into Email Gateway Defense for the first time, select **Consent on behalf of the organization**.



The screenshot shows a Microsoft permissions dialog box. At the top left is the Microsoft logo. Below it is a blurred URL. The main heading is "Permissions requested". Underneath, there is a green checkmark icon followed by the text "Barracuda Email Gateway Defense" and "Barracuda Networks" with a verified badge. The text "This app would like to:" is followed by a list of permissions: "View your basic profile" and "Maintain access to data you have given it access to", both with checkmarks. A third option, "Consent on behalf of your organization", is highlighted with a red rectangular box and has an unchecked checkbox. Below the permissions list, there is a paragraph of text explaining that accepting permissions allows the app to use data as specified in their terms of service and privacy statement, with a link to "https://myapps.microsoft.com" and a "Show details" link. At the bottom, there is a link "Does this app look suspicious? Report it here" and two buttons: "Cancel" and "Accept".

## Figures

1. userConsentAdminApproval.png
2. userConsentVerified.png
3. userConsentVerified.png
4. adminConsent.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.