

How to Configure the New Email Gateway Defense App in Microsoft Entra ID

<https://campus.barracuda.com/doc/100369328/>

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

With Microsoft Entra ID (formerly Azure Active Directory) Single Sign-On (SSO), users sign in once using their primary organizational account to securely access web and SaaS applications. SSO enables users to authenticate to applications using their single organizational account.

The SSO environment protects defined resources (websites and applications) by requiring the following steps before granting access:

1. Authentication: Authentication verifies the identity of a user using login credentials.
2. Authorization: Authorization applies permissions to determine if this user may access the requested resource.

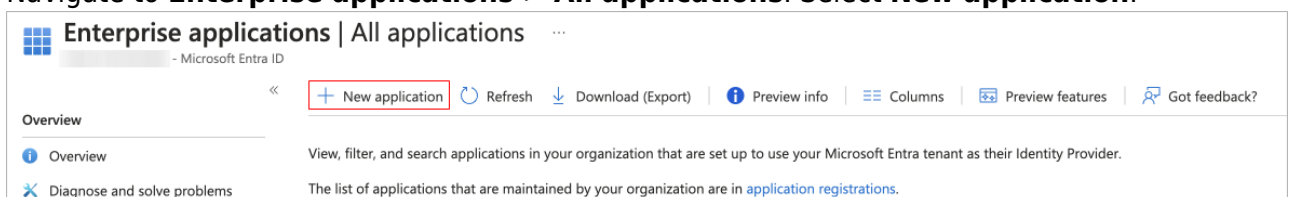
Adding the Email Gateway Defense app to your enterprise applications list in the Azure Portal allows end users to sign in using their Microsoft Entra ID credentials. This will also avoid consent screens appearing for users during the login process.

Once logged in, users can view their quarantine messages.

Add the Email Gateway Defense App to Your Enterprise Apps in the Azure Portal

Adding the Email Gateway Defense App to your enterprise applications list in the Azure Portal allows you to grant consent for the entire organization. This will also avoid consent screens appearing for users during the login process. For more information, see [User Consent Flows](#).

1. Log into the [Microsoft Entra admin center](#) (formerly Azure Active Directory) as a global administrator for the directory.
2. Navigate to **Enterprise applications > All applications**. Select **New application**.



3. On the **Browse Microsoft Entra Gallery** pane, type in "Email Gateway Defense" in the search box. Select **Barracuda Email Gateway Defense**.

Browse Microsoft Entra Gallery ...

[+ Create your own application](#) | [Got feedback?](#)

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning for their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for

Single Sign-on : **All**

User Account Management : **All**

Categories : **All**

 Federated SSO  Provisioning

Showing 1 of 1 results




**Barracuda Email
Gateway Defense**
Barracuda Networks




4. Click **Sign up for Barracuda Email Gateway Defense**.

Barracuda Email Gateway Defense

×

 Got feedback?

Logo ⓘ



Name * ⓘ

Barracuda Email Gateway Defense

Publisher ⓘ

Barracuda Networks

Provisioning ⓘ

Automatic provisioning is not supported

Single Sign-On Mode ⓘ

Linked Sign-on
OpenID Connect-based Sign-on

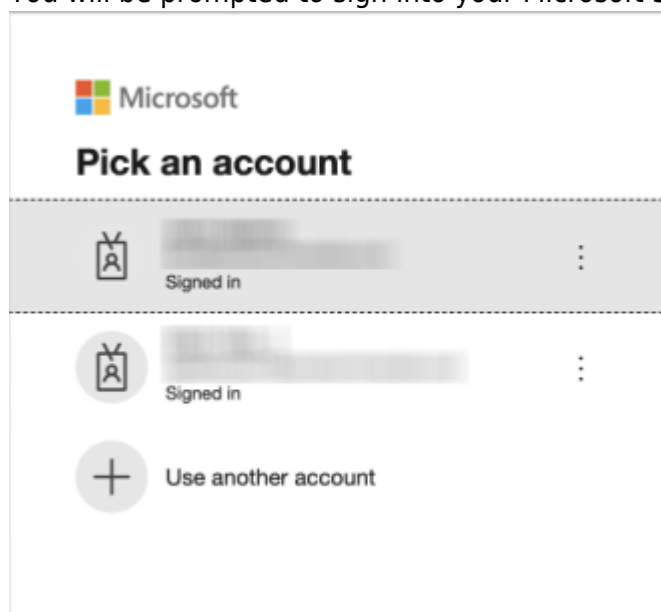
URL ⓘ

<https://www.barracuda.com/products/email-protection>

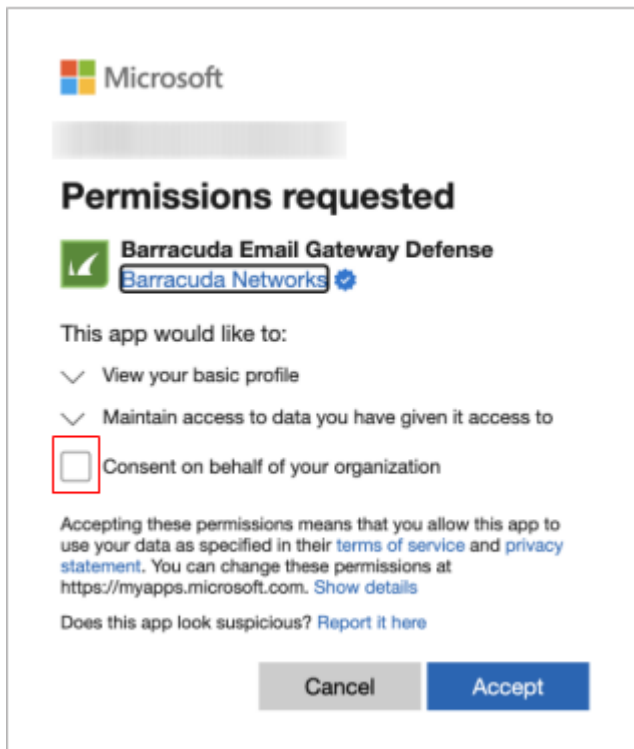
Single sign on for Barracuda Email Gateway Defense.

[Sign up for Barracuda Email Gateway Defense](#)

5. You will be prompted to sign into your Microsoft 365 account.



6. Check the **Consent on behalf of your organization** box. Click **Accept**.



You are redirected to the Email Gateway Defense end user page where you are logged into Email Gateway Defense.

Errors such as "Unable to log in. Domain does not exist." and "Invalid client" might appear if your domain does not yet exist on Email Gateway Defense. The Email Gateway Defense app is still added successfully into your enterprise applications.

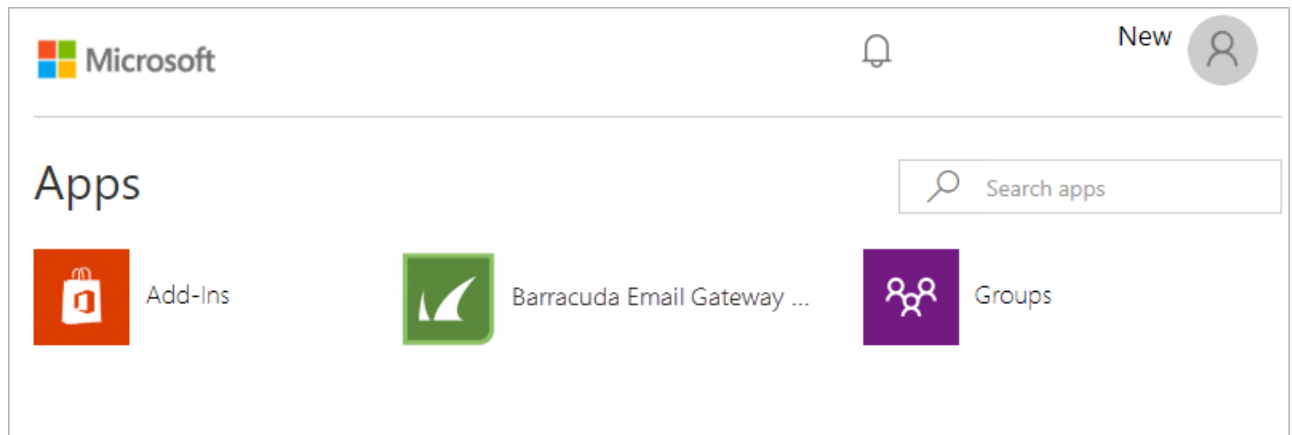
7. To check that the app is added to your enterprise applications, go back to the **Enterprise applications > All applications** page and refresh the page. You should now see the app in the list.

Access the Email Gateway Defense App in the My Apps Portal

By adding the Email Gateway Defense app to the My Apps portal, users can access the app via the My Apps portal with a single click once authenticated with their Azure credentials. *Note* that only the applications to which a user has access to will appear in the My Apps portal. Access to apps in the portal is subject to the access permissions established by your organization. For more information on the My Apps portal, see

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/myapps-overview>.

1. Log into <https://myapps.microsoft.com> with Microsoft Entra ID credentials.
The **Apps** page appears with the apps available for your account, including the app.



2. Click the Barracuda Email Gateway Defense app.

Remove the Email Gateway Defense App

To remove the Barracuda Networks app in Microsoft Entra ID:

1. Log into the [Microsoft Entra admin center](#) (formerly Azure Active Directory) as a global administrator for the directory.
2. Navigate to **Enterprise applications > All applications**.
3. On the **Enterprise applications - All applications** pane, you see a list of the apps you can manage. Select Email Gateway Defense.
4. Select **Manage > Properties** in the left menu.
5. At the top of the **Properties** pane, select **Delete**, and then select **Yes** to confirm you want to delete the application from your Microsoft Entra tenant.

User Consent Flows

Recommendation

Depending on the consent policy your organization has selected, users may be able to grant consent for themselves for a given application. As a global administrator, you can preemptively consent on behalf of the organization by adding the Email Gateway Defense app from the Microsoft Entra app gallery to your Microsoft portal as described in this article. This ensures that users will not be presented with a consent screen when logging into the new Email Gateway Defense interface. Alternatively, a global administrator can also log in directly to Email Gateway Defense and grant consent for the organization during the login process.

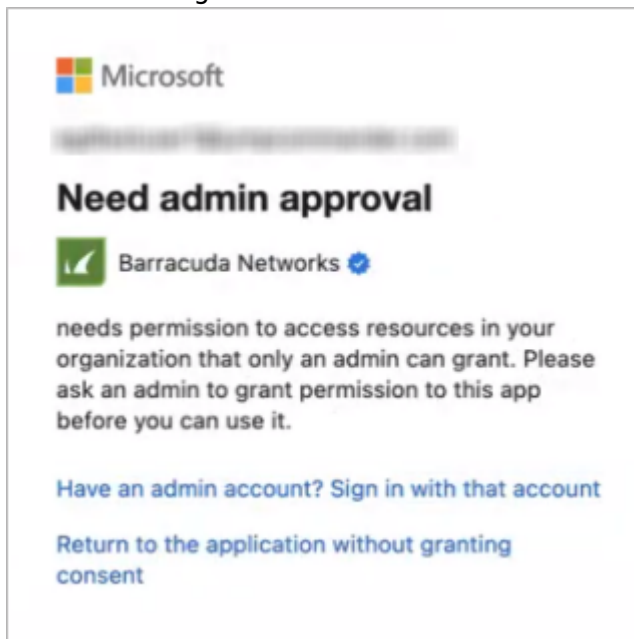
Note that in both cases, the Email Gateway Defense app will appear in the list of enterprise applications in the Azure Portal. However, Barracuda Networks recommends adding the app from the Microsoft Entra app gallery as described in this article for greater control with consent

screens.

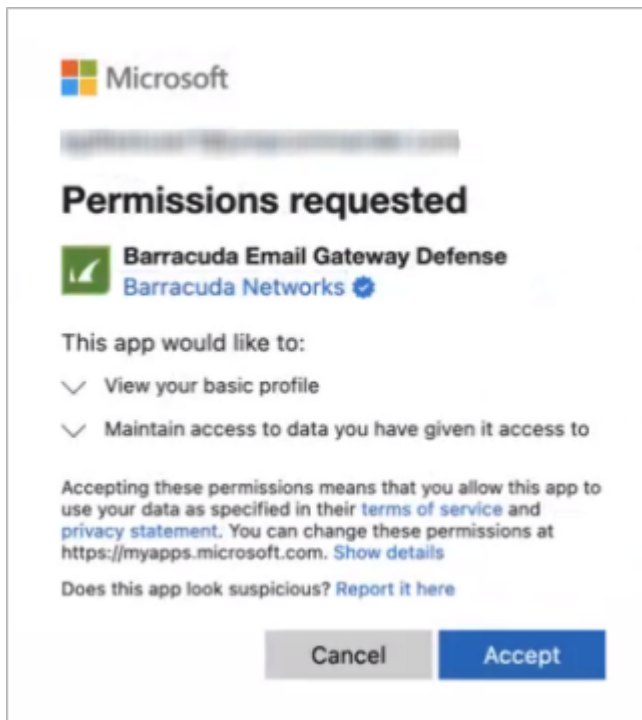
Also see [Viewing and Changing Consent Policies in the Azure Portal](#) for more information.

End users will see one of the below user consent flows based on the security consent policies set in the Azure Portal by the administrator. For more information, see [Viewing and Changing Consent Policies in the Azure Portal](#).

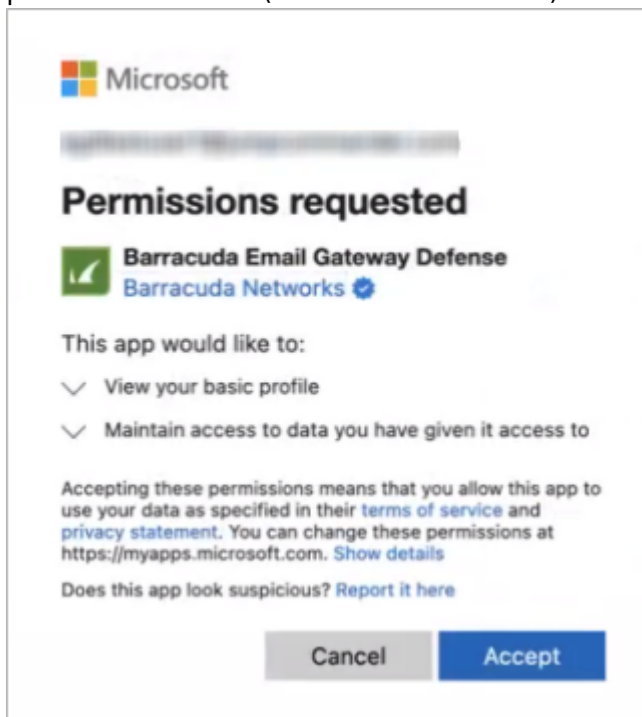
- **Do not allow user consent** – Users will be blocked from granting consent to any application. Users can sign into applications that administrators have granted consent to on their behalf, but they cannot consent to new permissions to applications on their own. Users will need to contact their administrator to grant access. They will not be able to access the application until the 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. 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).



End users are now logged into Email Gateway Defense and can see their Message Log page.

Figures

1. msAddNewApp1.png
2. egdApp.png
3. egdAppAdd.png
4. msSignIn.png
5. msConsent.png
6. egdMSApp.png
7. userConsentAdminApproval.png
8. userConsentVerified.png
9. userConsentVerified.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.