How to Configure the Outgoing Mail Using OAuth 2.0

The **From** field in MSPbots emails, notifications, and reports is customizable to use your company email instead of the default support@mspbots.ai. This article shows how to change the sender's email address using the OAuth2 method for more secure authorization.

What's on this page:

- Background information
- Prerequisites for editing the Outgoing Mail settings
- Gathering the MS OAuth 2.0 credentials for authorization
- Setting up OAuth 2.0 in MSPbots
- Verifying if the authentication is successful
- Related Topics

Background information

OAuth (Open Authorization) 2.0 is the modern standard to allow a website or application to access resources hosted by other web apps on behalf of a user. It adds security by providing consented access and restricting client actions performed on resources without sharing the user's credentials.

Now that basic authentication will be disabled and OAuth 2.0 is the new de facto industry standard for online authorization, MSPbots offers an option to add an extra authentication step in setting up the SMTP configuration for modifying the **From** field address for outgoing emails and sending reports. Users now have the option to use OAuth 2.0 in the Outgoing Mail settings.

If you prefer using only the basic authentication to modify the Outgoing Mail settings, refer to the article How to Configure the Outgoing Mail Using Basic Authentication.

Prerequisites for editing the Outgoing Mail settings

You must have the following to perform the procedure below:

- Admin permissions
- Inclusion in the Azure Active Directory (AAD)
- Outlook 365 license
- Application and developer roles for configuring the AAD

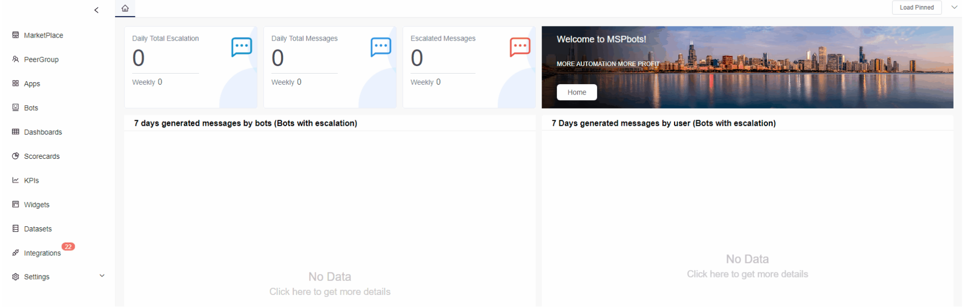
Gathering the MS OAuth 2.0 credentials for authorization

Follow these steps to generate the required information:

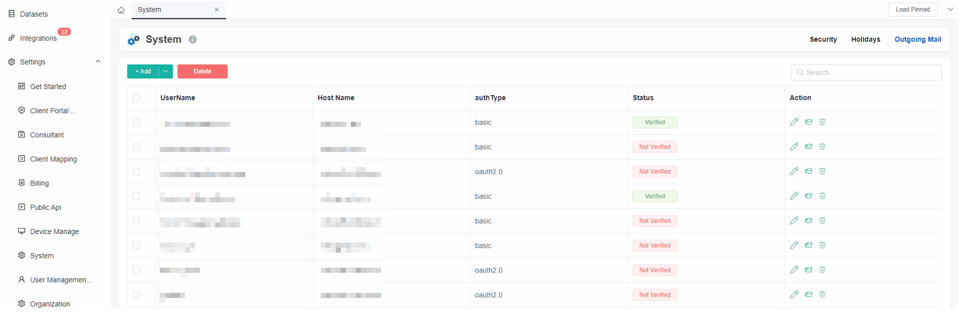
1. Prepare the redirect uniform resource identifier (URI) which is https://app.mspbots.ai/web/um/smtp/redirect. Once the authorization is successful, Microsoft will use this URI to notify MSPbots about the authentication result.

   You can find this information with the following steps:

   a. Go to **Settings** > **System** > **Outgoing Mail** in MSPbots.

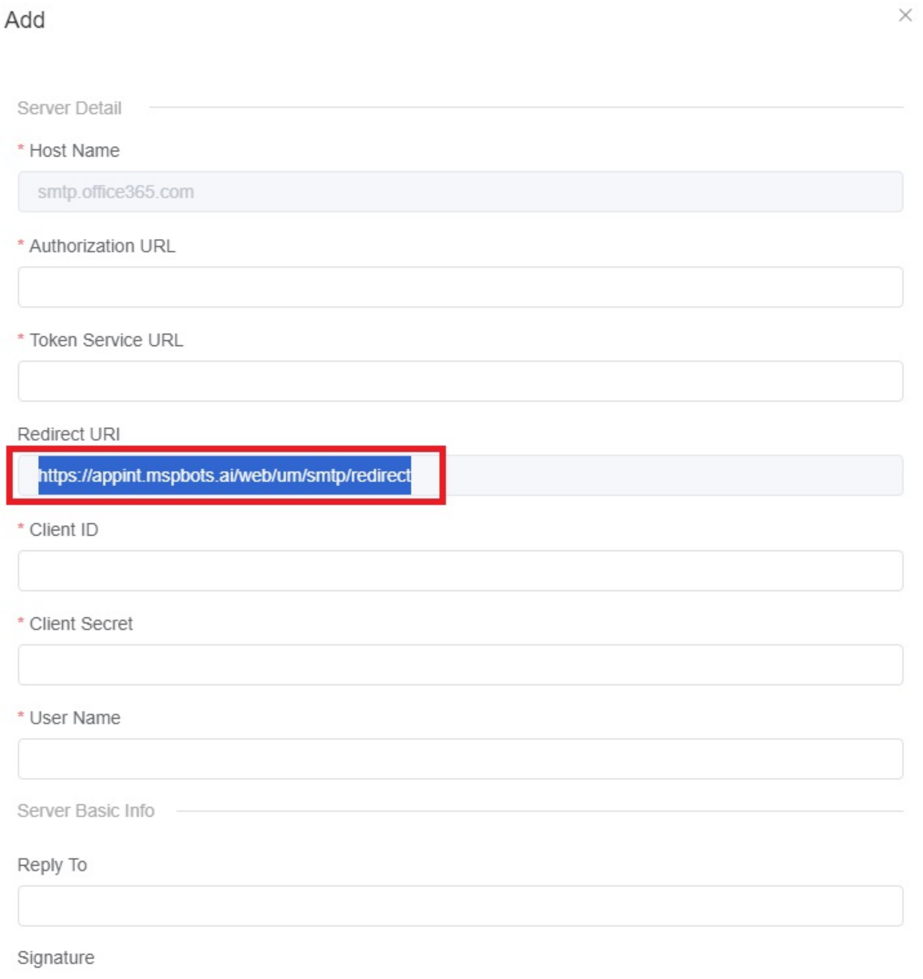


b. Click **v** icon beside the **+Add** button and select **OAuth2**.



□	UserName	Host Name	authType	Status	Action
□	[redacted]	[redacted]	basic	Verified	
□	[redacted]	[redacted]	basic	Not Verified	
□	[redacted]	[redacted]	oauth2.0	Not Verified	
□	[redacted]	[redacted]	basic	Verified	
□	[redacted]	[redacted]	basic	Not Verified	
□	[redacted]	[redacted]	basic	Not Verified	
□	[redacted]	[redacted]	oauth2.0	Not Verified	
□	[redacted]	[redacted]	oauth2.0	Not Verified	

c. When the Add window opens, go to the **Redirect URI** field, copy the given URL to Notepad, and save it on your Desktop. You will need this later when adding a New registration.



Add

Server Detail

* Host Name: smtp.office365.com

* Authorization URL

* Token Service URL

Redirect URI: https://appint.mspbots.ai/web/um/smtp/redirect

* Client ID

* Client Secret

* User Name

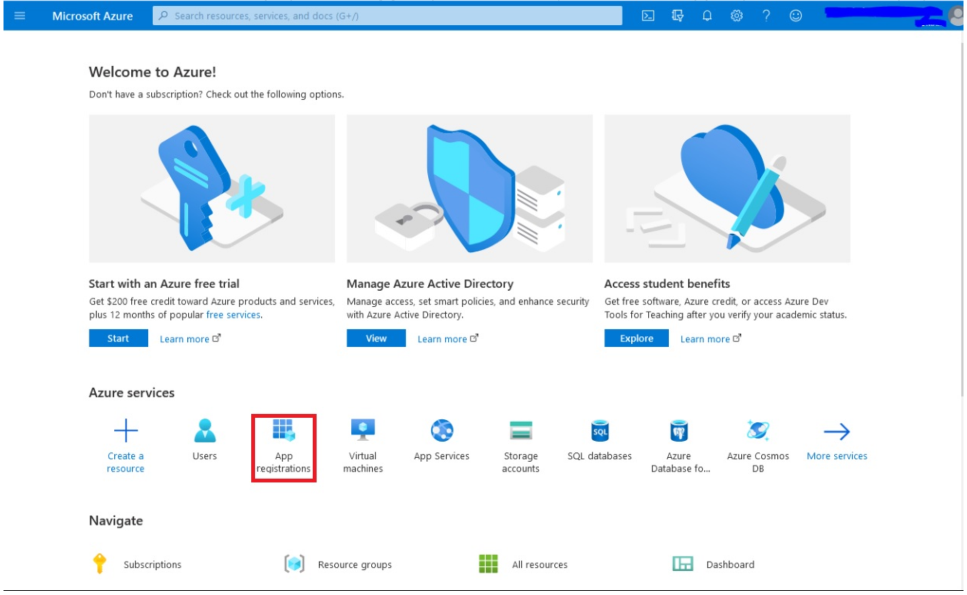
Server Basic Info

Reply To

Signature

2. Sign in to the Microsoft Azure portal and secure the credentials needed for the OAuth 2.0 authorization.
3. Create a new app registration.

a. On the Microsoft Azure homepage, click **App registrations**. If you can't find App registrations on the page, search for it in the search bar.



[redacted]

Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

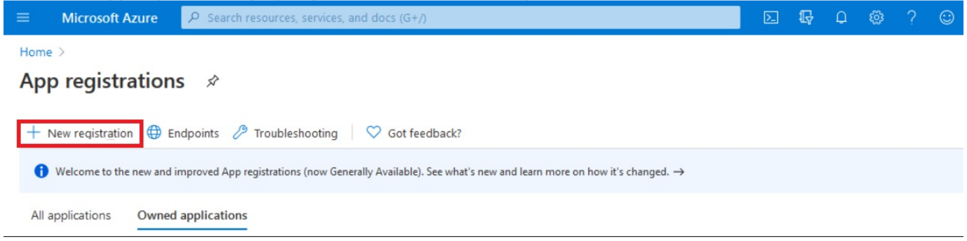
Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

b. When the App registrations page opens, click the **+New registration** tab.

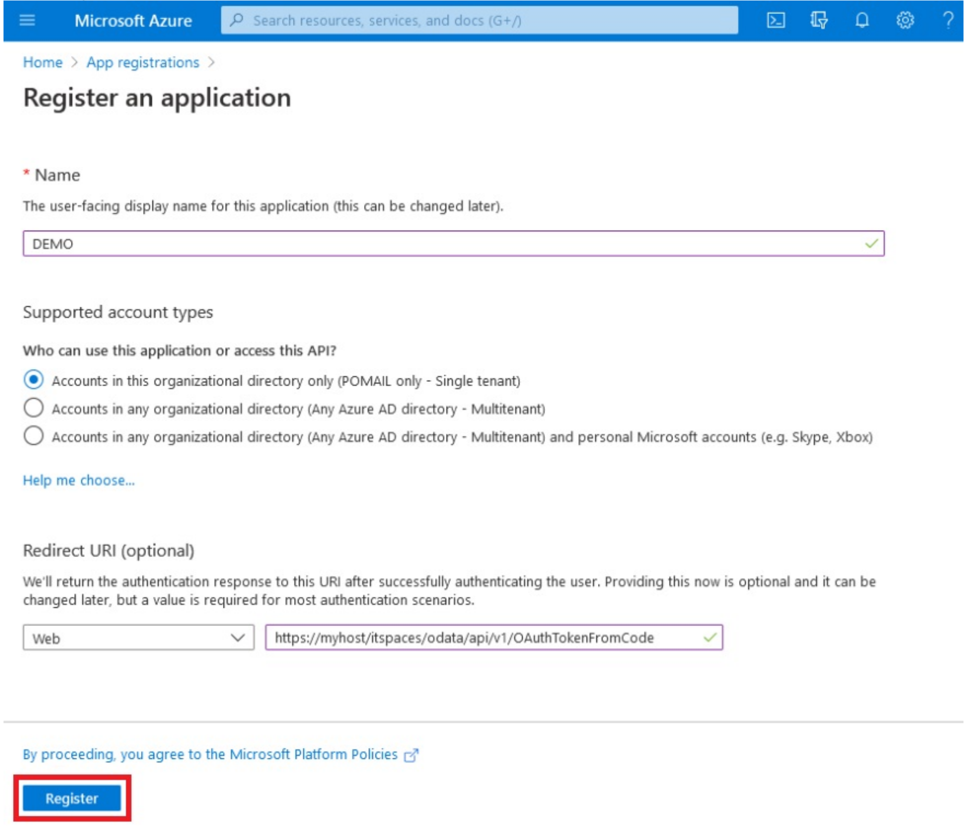


Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

c. In the Register an application form:

   i. **Name** - Enter a unique name for your application.
   ii. **Supported account types** - Select **Account in this organizational directory only (MSPbots.ai only - Single tenant)** from the options.
   iii. **Redirect URI (optional)** - In the first box, select **Web,** and in th**e second box**, enter the Redirect URI copied from Step 1.c.

iv. Click **Register**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > App registrations >

Register an application

* Name

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

DEMO

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (POMAIL only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

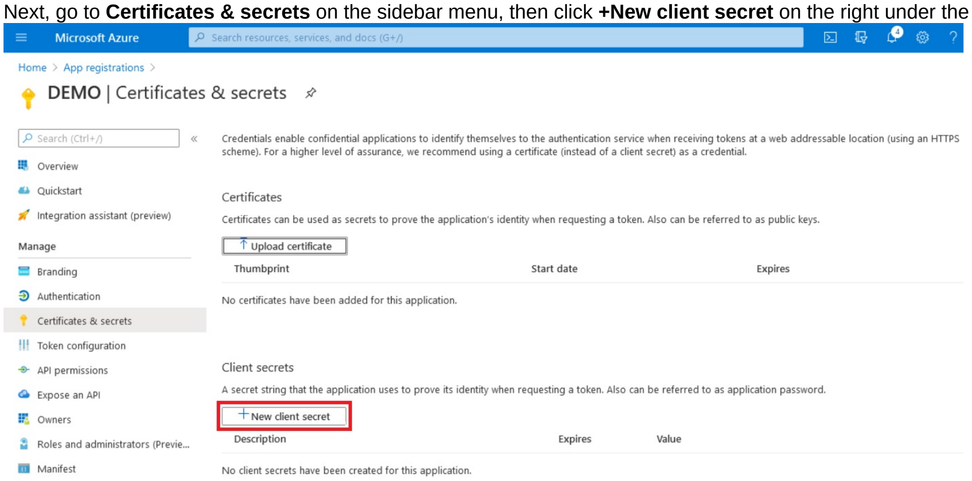
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://myhost/itspaces/odata/api/v1/OAuthTokenFromCode

By proceeding, you agree to the Microsoft Platform Policies

.

4. Next, go to **Certificates & secrets** on the sidebar menu, then click **+New client secret** on the right under the Client secrets tab.



DEMO | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

No certificates have been added for this application.

Client secrets

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

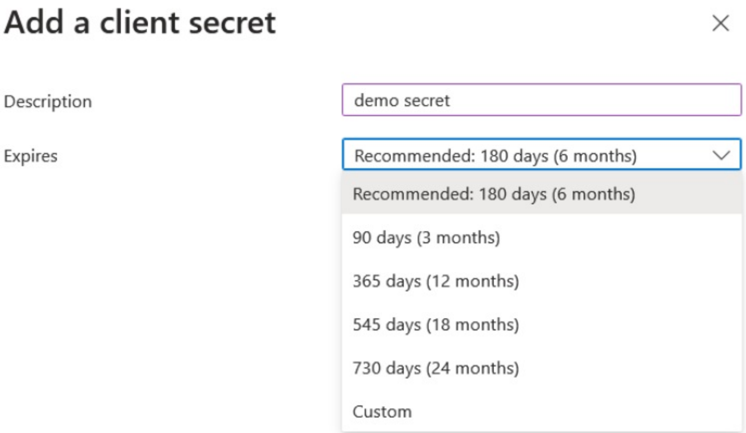
Description	Expires	Value

No client secrets have been created for this application.

a. In the Add a client secret window:

i. **Description** - Add a description.

ii. **Expires** - Select an expiry date from the dropdown menu.



Add a client secret

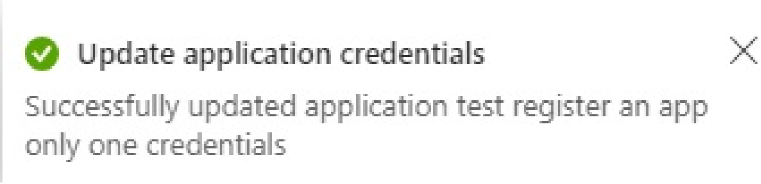
Description: demo secret

Expires: Recommended: 180 days (6 months)

Before the secret expires you must create a new secret and apply it to the MSPbots Outgoing Mail settings.

iii. Click **Add** located at the bottom of the Add a client secret window.

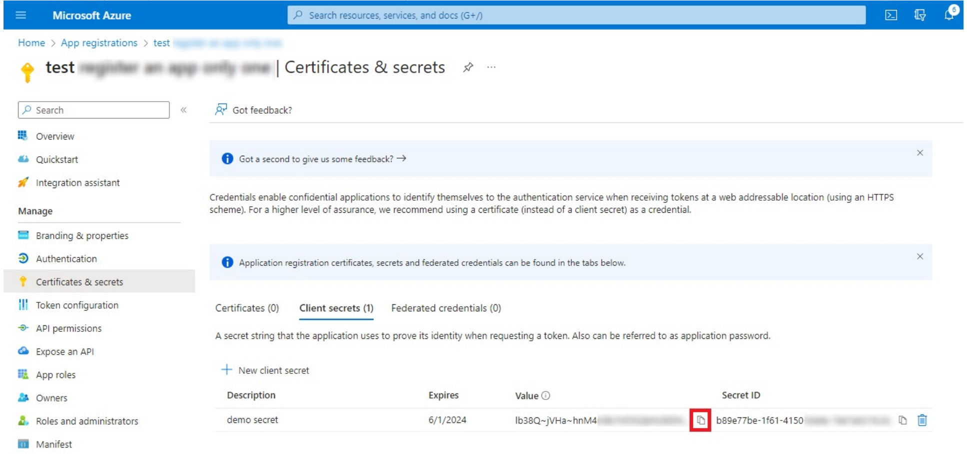
b. The addition is successful once the Update application credentials pop-up window appears.



Update application credentials

Successfully updated application test register an app only one credentials

c. Click the **copy** ⧉ icon in the Value column to copy the value to Notepad and save it on your Desktop. You will need this value later when configuring OAuth 2.0 in the mail settings.



test [redacted] | Certificates & secrets

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

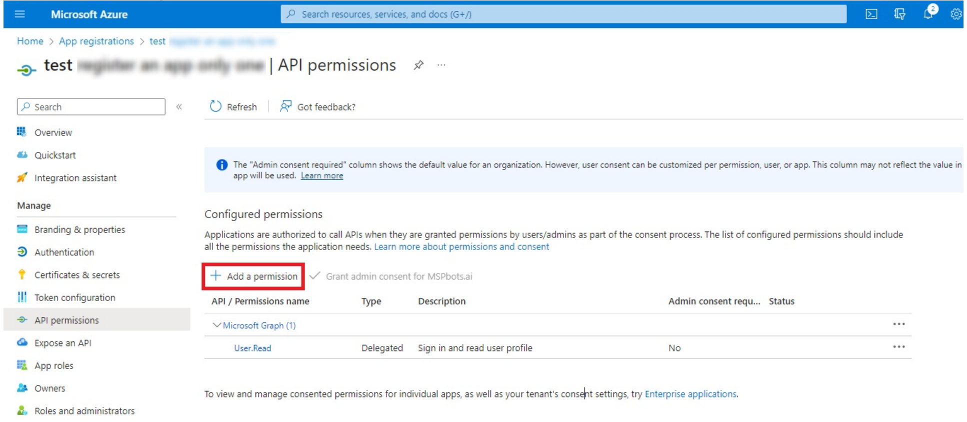
Application registration certificates, secrets and federated credentials can be found in the tabs below.

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

Description	Expires	Value	Secret ID
demo secret	6/1/2024	lb38Q~jVHa~hnM4[redacted]	b89e77be-1f61-4150[redacted]

5. Next, go to **API Permissions** on the sidebar menu.

a. Click the **+Add a permission** button.



test [redacted] | API permissions

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 app will be used. Learn more

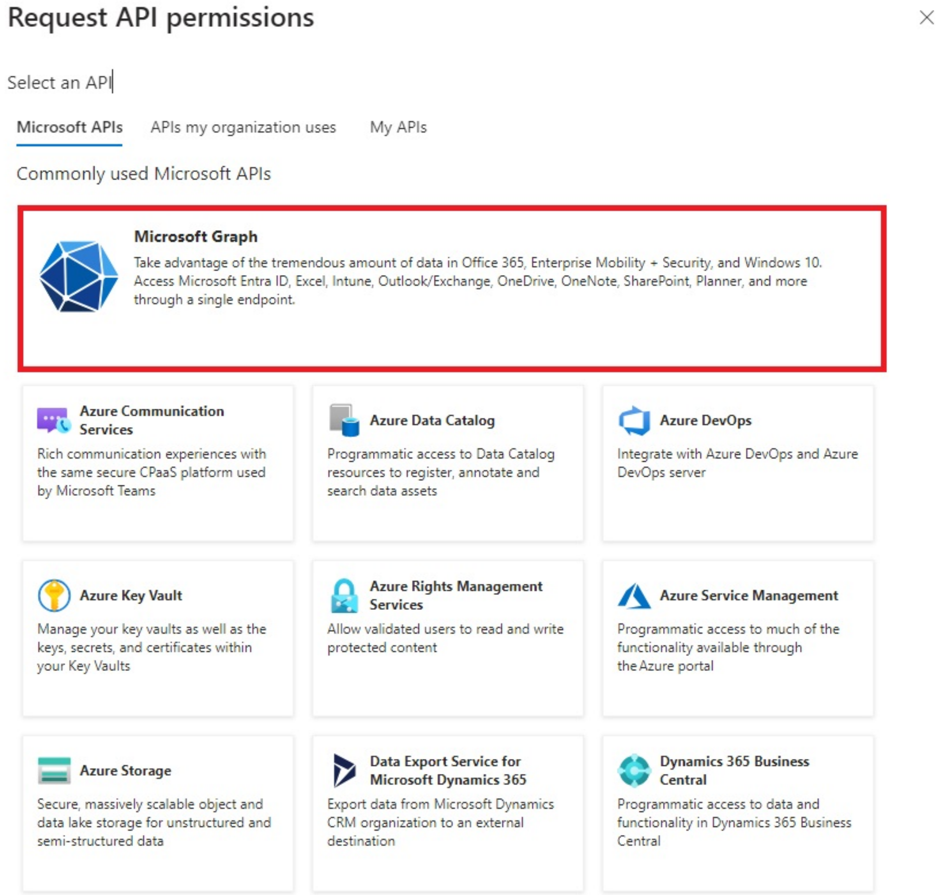
Configured permissions

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	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.

b. In requesting API permissions window, go to the Microsoft APIs tab and select **Microsoft Graph**.



Request API permissions

Select an API

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 Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

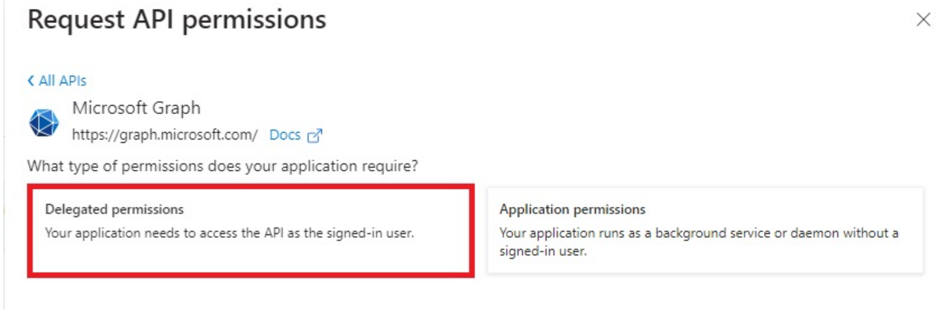
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

c. Next, select **Delegated permissions**.



Request API permissions

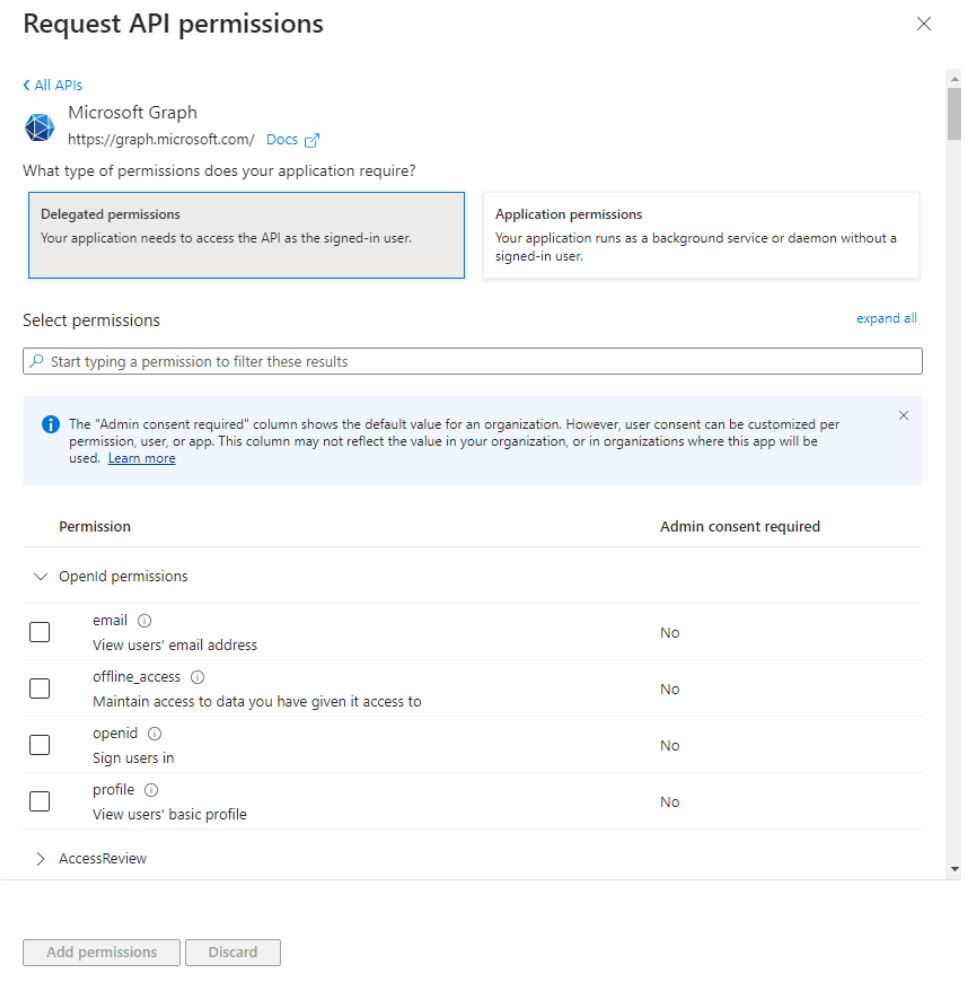
Microsoft Graph
https://graph.microsoft.com/ Docs

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.

d. Enter **SMTP** in the search bar under Select permissions, then click **SMTP** and select **SMTP.Send**.



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.

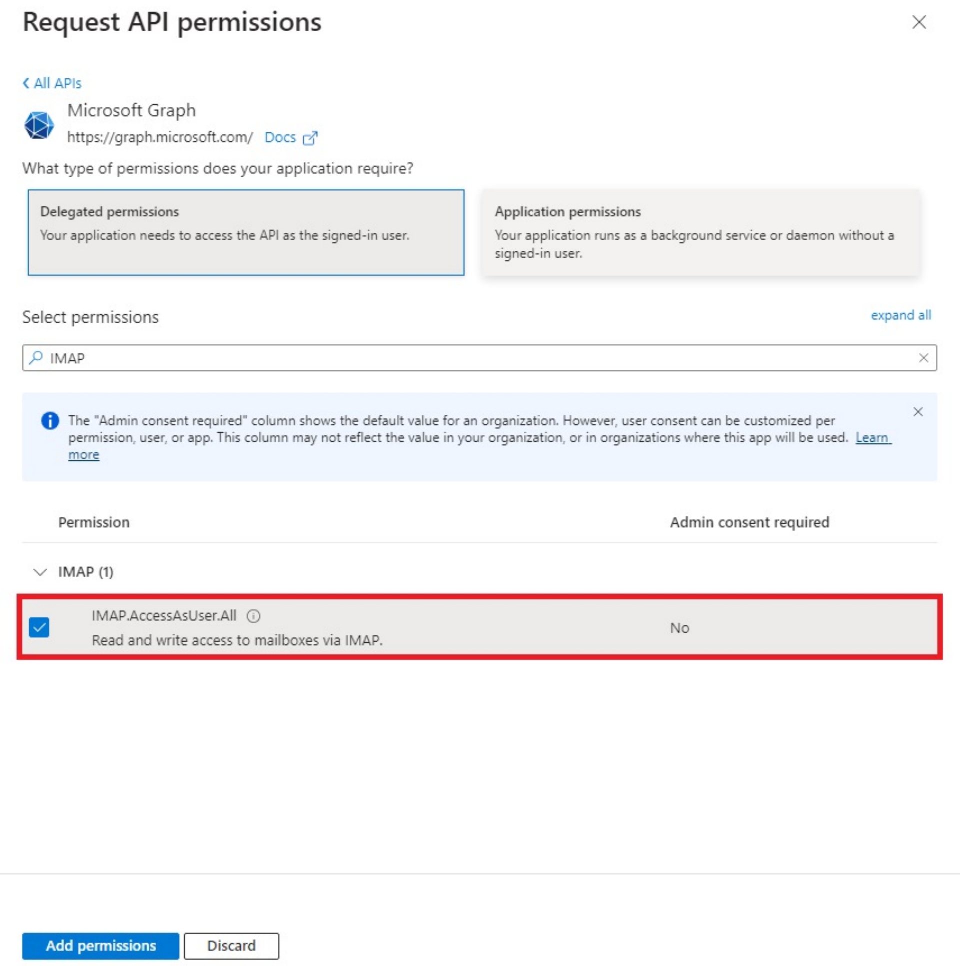
Select permissions

Start typing a permission to filter these results

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

	Permission	Admin consent required
	OpenId permissions	
□	email View users' email address	No
□	offline_access Maintain access to data you have given it access to	No
□	openid Sign users in	No
□	profile View users' basic profile	No
	AccessReview	

e. Enter **IMAP** in the search bar under Select permissions, then click **IMAP** and put a checkmark **IMAP.AccessAsUser.All**.



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.

Select permissions — expand all

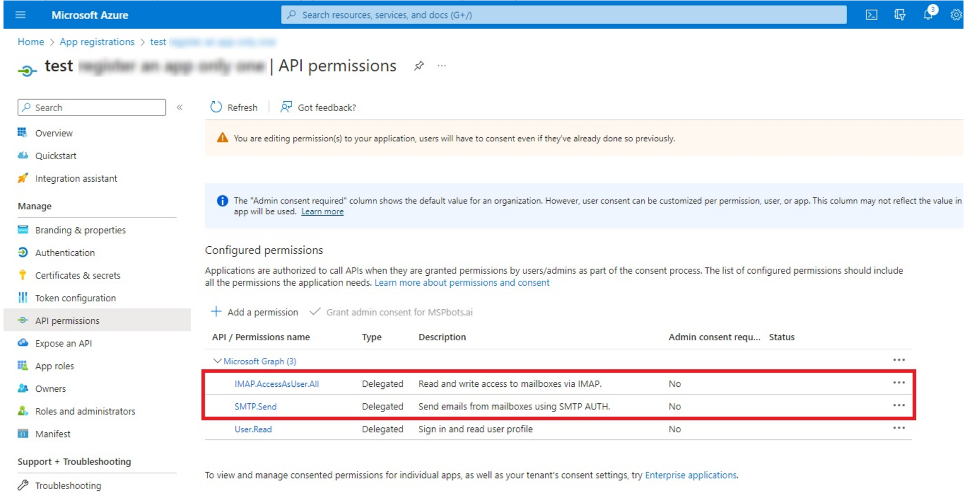
IMAP

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

Permission	Admin consent required
IMAP (1)	
☑ IMAP.AccessAsUser.All Read and write access to mailboxes via IMAP.	No

f. Click the **Add permissions** button.

g. The permissions you added will appear in the Configured permissions list.



Home > App registrations > test [redacted]

test [redacted] | API permissions

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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 app will be used. Learn more

Configured permissions

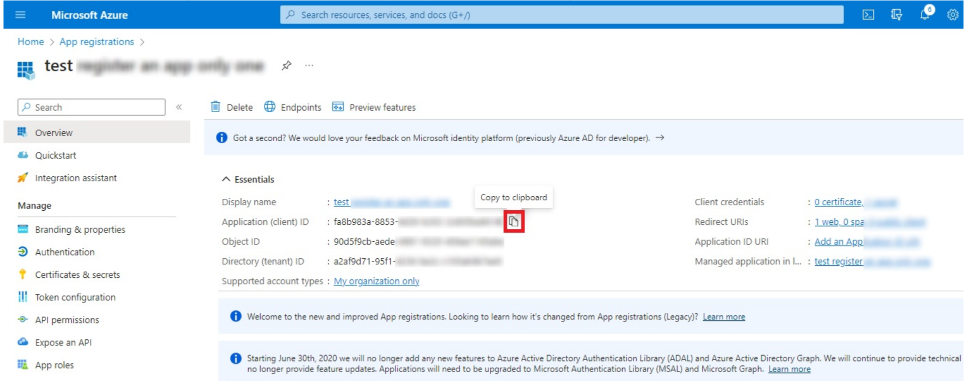
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	
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.

6. Next, go to the **Overview.**

a. Click the **copy** ⧉ icon next to the **Application (client) ID** to copy the value to Notepad and save it on your Desktop. You will also use this value for creating the OAuth 2.0 credential in the mail settings.



test [redacted]

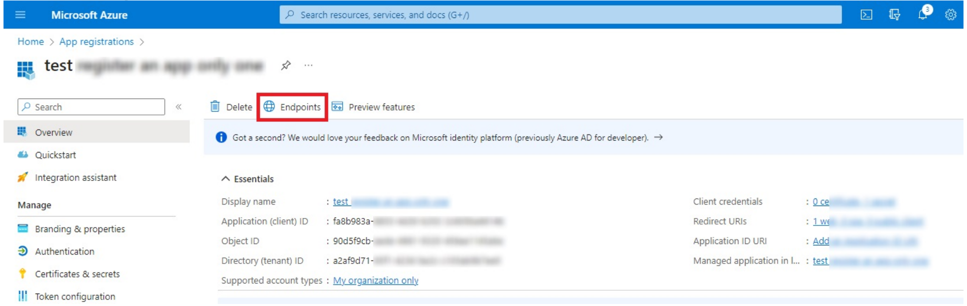
Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : test [redacted]
Application (client) ID : fa8b983a-8853-[redacted]
Object ID : 90d5f9cb-aede-[redacted]
Directory (tenant) ID : a2af9d71-95f1-[redacted]
Supported account types : My organization only
Client credentials : 0 certificate, [redacted]
Redirect URIs : 1 web, 0 spa, [redacted]
Application ID URI : Add an App[redacted]
Managed application in l... : test register [redacted]

Welcome to the new and improved App registrations. Looking to learn how it's changed 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 no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

b. Click the **Endpoints** tab.

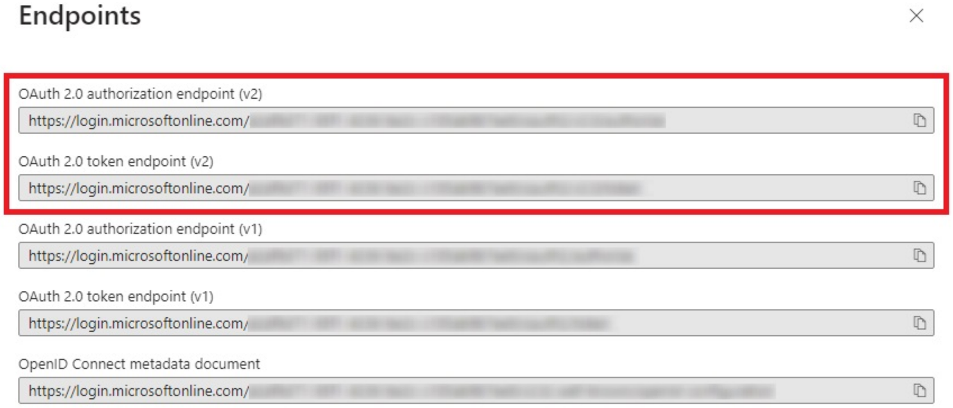


test [redacted]

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : test [redacted]
Application (client) ID : fa8b983a-[redacted]
Object ID : 90d5f9cb-[redacted]
Directory (tenant) ID : a2af9d71-[redacted]
Supported account types : My organization only
Client credentials : 0 ce[redacted]
Redirect URIs : 1 we[redacted]
Application ID URI : Add [redacted]
Managed application in l... : test [redacted]

c. Copy the **OAuth 2.0 authorization endpoint (v2)** and the **OAuth 2.0 token endpoint (v2)** to Notepad and save it on your Desktop, such as Notepad. You will also use these values for creating the OAuth 2.0 credential in the mail settings.



Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/[redacted]

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/[redacted]

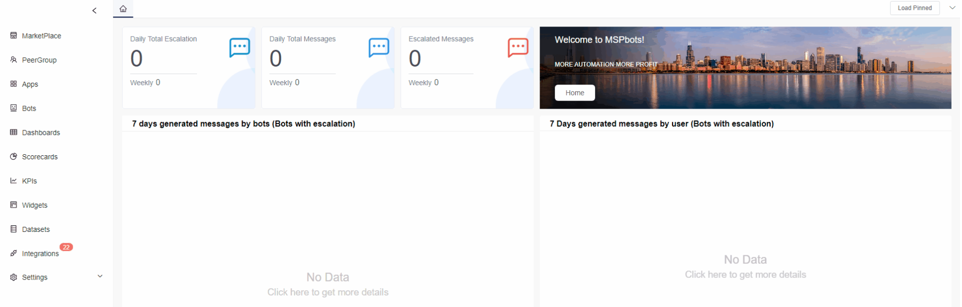
OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/[redacted]

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/[redacted]

OpenID Connect metadata document
https://login.microsoftonline.com/[redacted]

Setting up OAuth 2.0 in MSPbots

1. Open the MSPbots app.
2. Go to **Settings > System**, and click **Outgoing Mail** in the upper right corner of the System page.

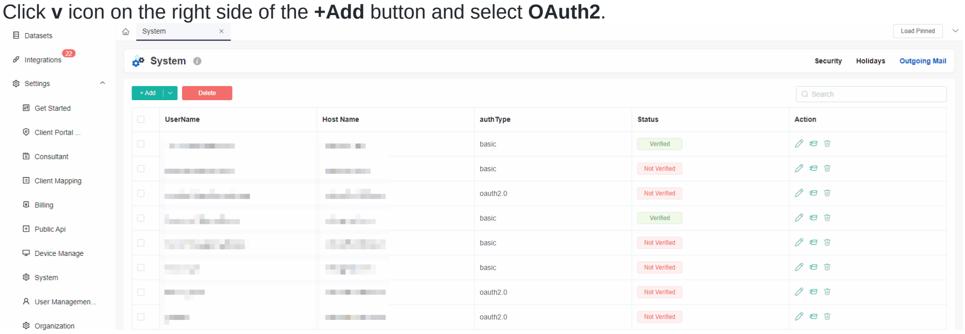


Daily Total Escalation 0 Weekly 0
Daily Total Messages 0 Weekly 0
Escalated Messages 0 Weekly 0

7 days generated messages by bots (Bots with escalation)
No Data
Click here to get more details

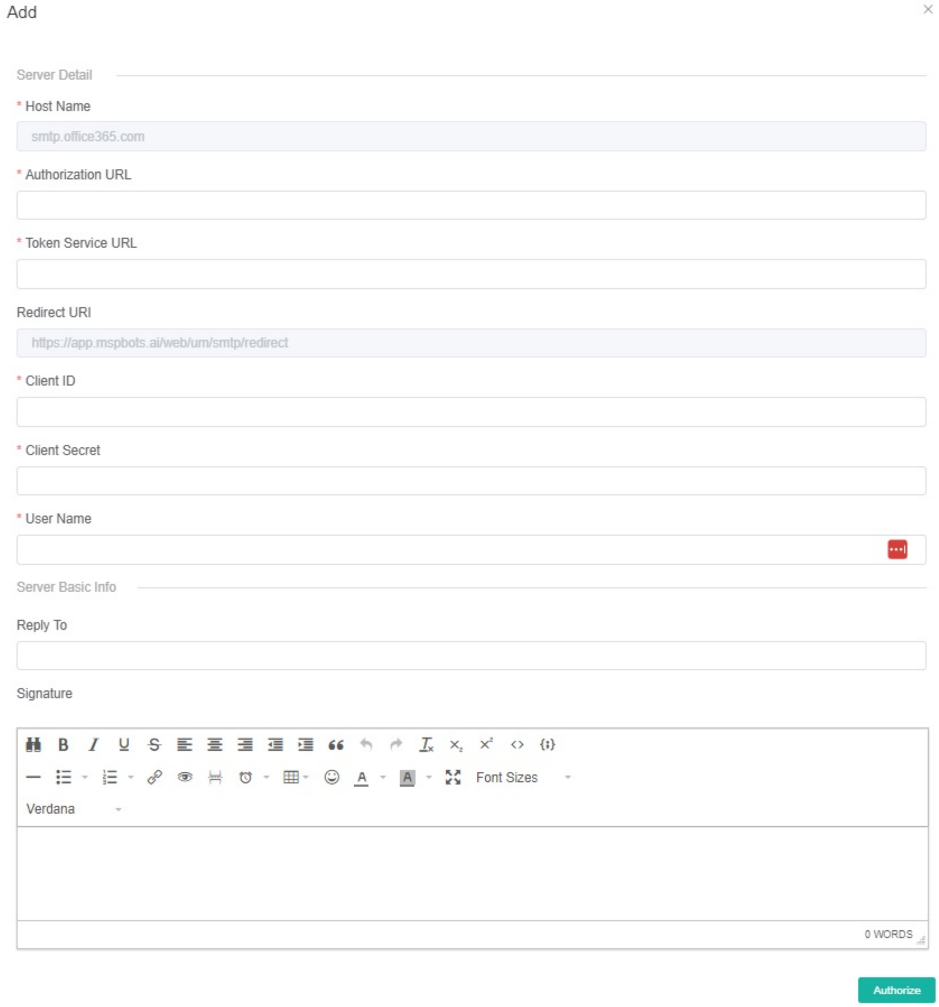
7 Days generated messages by user (Bots with escalation)
No Data
Click here to get more details

3. Click **v** icon on the right side of the **+Add** button and select **OAuth2**.



□	UserName	Host Name	authType	Status	Action
□	[redacted]	[redacted]	basic	Verified	
□	[redacted]	[redacted]	basic	Not Verified	
□	[redacted]	[redacted]	oauth2.0	Not Verified	
□	[redacted]	[redacted]	basic	Verified	
□	[redacted]	[redacted]	basic	Not Verified	
□	[redacted]	[redacted]	basic	Not Verified	
□	[redacted]	[redacted]	oauth2.0	Not Verified	
□	[redacted]	[redacted]	oauth2.0	Not Verified	

4. Fill in the following fields in the Add window.
   a. **Host Name** - This value is pre-filled.
   b. **Authorization URL** and **Token URL** - Use the values from Step 6.c of the previous section.
   c. **Redirect URI** - This value is pre-filled.
   d. **Client ID** - Use the values from Step 6.a of the previous section.
   e. **Client Secret** - Use the values generated in Step 4.c of the previous section.
   f. **Username** - Enter your username.
   g. **Reply to** - Enter your preferred email.
   h. **Signature** - Input your signature.



* Host Name: smtp.office365.com

* Authorization URL

* Token Service URL

Redirect URI: https://app.mspbots.ai/web/um/smtp/redirect

* Client ID

* Client Secret

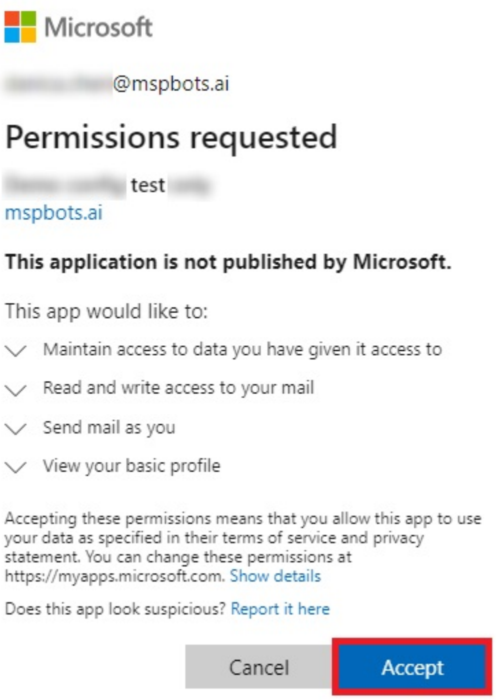
* User Name

Reply To

Signature

5. Click **Authorize**.
6. On the Microsoft login screen, enter the user password you provided in the OAuth 2.0 credential and click **Sign in**.

7. Click **Accept** in the Microsoft pop-up window requesting permissions for MSPbots.



Microsoft

[redacted]@mspbots.ai

Permissions requested

[redacted] test [redacted]
mspbots.ai

This application is not published by Microsoft.

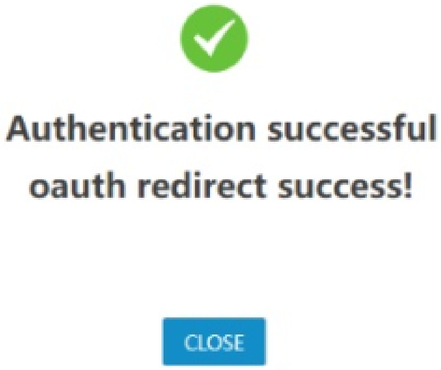
This app would like to:

- Maintain access to data you have given it access to
- Read and write access to your mail
- Send mail as you
- View your basic profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

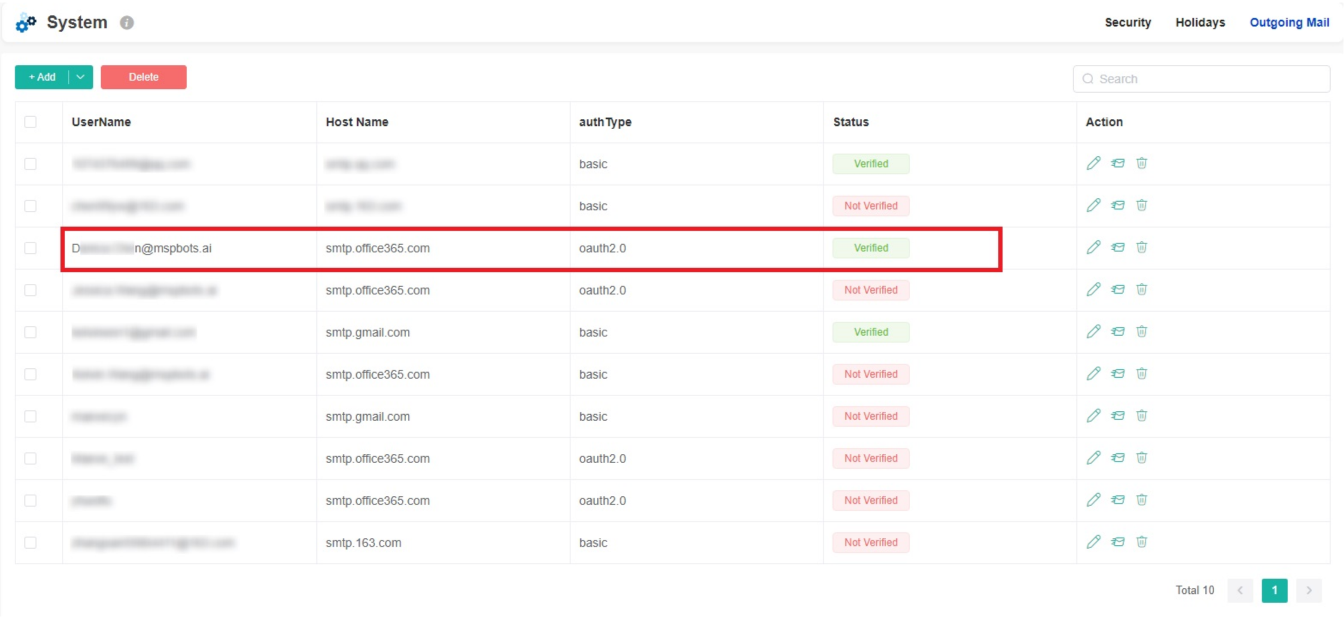
8. The message *Authentication successful oauth redirect success* appears.



Authentication successful
oauth redirect success!

Verifying if the authentication is successful

Go back to MSPbots and refresh the Outgoing Mail page to verify if the configuration works. The mailbox status should show **Verified** for a successful authentication. If the status is **Not Verified**, repeat Setting up OAuth 2.0 in MSPbots until the authorization is successful.



□	UserName	Host Name	authType	Status	Action
□	[redacted]	[redacted]	basic	Verified	✎
□	[redacted]	[redacted]	basic	Not Verified	✎
□	D[redacted]n@mspbots.ai	smtp.office365.com	oauth2.0	Verified	✎
□	[redacted]	smtp.office365.com	oauth2.0	Not Verified	✎
□	[redacted]	smtp.gmail.com	basic	Verified	✎
□	[redacted]	smtp.office365.com	basic	Not Verified	✎
□	[redacted]	smtp.gmail.com	basic	Not Verified	✎
□	[redacted]	smtp.office365.com	oauth2.0	Not Verified	✎
□	[redacted]	smtp.office365.com	oauth2.0	Not Verified	✎
□	[redacted]	smtp.163.com	basic	Not Verified	✎

Total 10 ‹ 1 ›

Related Topics

- How to Configure the Outgoing Mail Using Basic Authentication
- Configure the Outgoing Mail - Mailjet