3

DOCU13517

OAuth Registration for Microsoft 365 / Azure AD

[TOC]

Background

This Document describes the process of adding and configuring OAuth for Microsoft 365 within Azure

Introduction

This document describes a way of settings up an App registration for use with Highstage. However, this might not be the only way of doing this. There might also be special constraints within the tenant or for a specific server that influence how this should be set up. So this guide should only be seen as guidance.

Prerequisites

- To make this work, you need to have access to your organisations Azure Tenant and have priviligies to make changes to the Azure AD. If you don't have an account there yet, create it. You also have to set up a tenant that represents your company.
- Log into Azure Portal, and select the tenant that fits the organization that has the mail-address for Highstage. If you administer more than one tenant, use Directories + subscriptions filter to select the tenant for whom to register an application.

Guides

Register your application

In Azure Portal ⇒ expand the left menu ⇒ select Azure Active Directory ⇒ select App registrations ⇒ click + New registration. (Azure Portal is constantly evolving, so if you cannot find this page, use the search bar.)



 Name your application, choose which kind of accounts are going to use it, and click [Register]. Note: This guide is suitable for single tenant account types. For other types, further steps might be different.

\equiv Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)	🕘
Home > App registratio	ns >	
Register an application		×
* Name		i i i
The user-facing display name for this applica	tion (this can be changed later).	
Imap/Pop OAuth Service		\checkmark
Supported account types		
Who can use this application or access this A	PI?	
• Accounts in this organizational directory	only (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 account	nts (e.g. Skype, Xbox)
Personal Microsoft accounts only		
Help me choose		
By proceeding, you agree to the Missacoft Di	atform Balicias #7	
by proceeding, you agree to the Microsoft Pi	arionin koncies (3.	
Register		

3. You successfully registered your application and you can view its associated IDs. Some of them will be needed later to obtain an OAuth 2.0 token.



Set up client secret (application password)

4. In the left menu, select Certificates & secrets \Rightarrow click + New client secret.

\equiv Microsoft Azure	℅ Search resources, services, and docs (G+/)	🙆
Home > App registrati	ons > Imap/Pop OAuth Service	
💡 Imap/Pop OAuth Se	ervice Certificates & secrets 👒 …	\times
✓ Search (Ctrl+/) «	₽ Got feedback?	
Sverview	Credentials enable confidential applications to identify themselves to the authentication service when rece	iving 🔺
📣 Quickstart	tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommusion a certificate (instead of a client sceret) as a credential	nend
🚀 Integration assistant	using a certificate (instead of a ciefic secret) as a ciccertial.	
Manage	Application registration certificates, secrets and federated credentials can be found in the tabs below.	×
🚍 Branding & properties		
Authentication	Certificates (0) Client secrets (0) Federated credentials (0)	
📍 Certificates & secrets	A correct string that the application uses to prove its identity when requesting a taken. Also can be referred	ad to
Token configuration	as application password.	ato
➔ API permissions	+ New client secret	
Expose an API	Description Expires Value O Secret ID	
🔽 App roles		-1.
A Owners	No client secrets have been created for this application.	
👃 Roles and administrators 🖕		*

5. Provide some description for this secret, choose expiration period, and click Add.

\equiv Microsoft Azure	𝒫 Search resou	rces, services, and docs (G+/)		🕒
Home > App registr	ations > Imap/Pop	Add a client secret		×
Search (Ctrl+/)	Got feedb	Description	Secret 1	
 Overview Quickstart Integration assistant 	Credentials ena tokens at a wek using a certifica	Expires	Recommended, 6 months	
Manage Branding & properties	í Applicati			
 Authentication Certificates & secrets 	Certificates ((
III Token configuration	A secret string as application			
 API permissions Expose an API 	+ New clie			
App roles	No client seco			
 Owners Roles and administrators 	•	Add Cancel		

6. Immediately copy and save the newly created client secret's Value (not Secret ID). You will not be able to view the Value later anymore.

\equiv Microsoft Azure	$\mathcal P$ Search resources, se	rvices, and docs (G+/)		🚇
Home > App registrati	ons > Imap/Pop OAuth S	ervice		
💡 Imap/Pop OAuth S	ervice Certifica	ates & secret	S ☆ …	×
✓ Search (Ctrl+/) «	🖗 Got feedback?			
Soverview	Credentials enable confi	dential applications to id	dentify themselves to the authe	ntication service when receiving
🗳 Quickstart	tokens at a web address using a certificate (instea	able location (using an H ad of a client secret) as a	HTTPS scheme). For a higher lev a credential.	el of assurance, we recommend
💉 Integration assistant				
Manage	Certificates (0) Cli	ient secrets (1) Fed	erated credentials (0)	
🔤 Branding & properties	A secret string that the	application uses to prov	ve its identity when requesting	a token. Also can be referred to as
Authentication	application password.			
📍 Certificates & secrets	+ New client secret			
Token configuration	Description	Expires	Value 🛈	Secret ID
API permissions	Secret 1	3/9/2023	LH38Q~t8kYqNWL.D	c9da889f-5a25-4993 🗅 📋
🙆 Expose an API				_
🔣 App roles				
🌆 Owners				
👃 Roles and administrators 🗸				

Add app permissions

7. In the left menu, select API permissions \Rightarrow click + Add a permission.



8. Navigate to APIs my organization uses tab \Rightarrow type Office/Microsoft 365 Exchange in the search bar \Rightarrow click Office/Microsoft 365 Exchange Online entry.

≡ Micro	soft Azure		🧕
Home >	Request API p	permissions	×
ᢖ Imaj			
	Select an API		
Search (Ct	Microsoft APIs API	s my organization uses My APIs	
🕔 Overview	Apps in your directory th	nat expose APIs are shown below	
🗳 Quickstart	O Office 265 Evebange		
💉 Integratioi	- Office 365 Exchange		
	Name	Application (client) ID	_
Manage	Office 365 Exchange O	online 0000002-0000-0ff1-ce00-00000000	000
🔤 Branding (-		

9. Click Application permissions ⇒ type AccessAsApp ⇒ check IMAP.AccessAsApp and/or POP.AccessAsApp ⇒ click [Add permissions].

≡ Micros	soft Azure \mathcal{P} Search resources, services, and doc	s (G+/) 💽
Home >	Request API permissions	×
ᢖ Imaj		
🔎 Search (Ct	Office 365 Exchange Online https://ps.outlook.com	
4 Overview	What type of permissions does your application require?	
Quickstart	Delegated permissions	Application permissions
💉 Integration	Your application needs to access the API as the signed-in user.	Your application runs as a background service or daemon without a signed-in user.
Manage		
🗮 Branding (Select permissions	expand all
Authentica	P AccessAsApp	×
📍 Certificate	Permission	Admin consent required
Token con	V IMAP (1)	
API permi:		
Expose an	IMAP.AccessAsApp	Ves
App roles	✓ POP (1)	
A Owners	DOB Assess As Ann.	
Roles and	POP.AccessAsApp ()	Ves
0 Manifest		
Support + Tro		
🦉 Troublesh		
New supp	Add permissions Discard	

10. The newly-added IMAP.AccessAsApp and POP.AccessAsApp permissions have to be approved by your organization's administrator. Ask them to grant consent to your application by clicking Grant admin consent for [organization].

≡	Microsoft Azure	٩	Search resources, services, ar	nd docs (G+/)		🤇	
Hom	e > App r	registrations	> Imap/Pop OAuth Service				
-	Imap/Pop OAu	ıth Serv	ice API permissi	ons 🖈 …		\times	
»	🕐 Refresh 🕴 🔗 Got fe	eedback?					
	▲ You are editing permiss	sion(s) to your a	pplication, users will have to cons	ent even if they've already done so previously	л.		
	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 + Add a permission Grant admin consent for						
	API / Permissions name	Туре	Description	Admin consent req	Status		
	∽ Microsoft Graph (1)					•••	
	User.Read	Delegated	Sign in and read user profile	No		•••	
	✓ Office 365 Exchange Onlin	1					
	IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes	▲ Not granted for REBEX		1
	POP.AccessAsApp	Application	POP.AccessAsApp	Yes	▲ Not granted for REBEX		•

11. Application permissions have been granted. Optionally, you can remove the delegated User.Read permission which is not needed for app-only application - click the context menu on the right side of the permission and select [Remove permission].

≡	Microsoft Azure	م	Search resources, services, and o	locs (G+/)		🧕
Hom	ie > App r	egistrations	> Imap/Pop OAuth Service			
-- -	Imap/Pop OAu	ith Serv	ice API permissio	ns 🖈 …		\times
»	🕐 Refresh 🛛 🔊 Got fe	edback?				
	 Successfully granted ac 	lmin consent fo	r the requested permissions.			
	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	Туре	Description	Admin consent req	Status	
	∽ Microsoft Graph (1)					
	User.Read	Delegated	Sign in and read user profile	No	Remove permission	
	✓ Office 365 Exchange Onlin				Revoke admin consent	
	IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes		
	POP.AccessAsApp	Application	POP.AccessAsApp	Yes	🔮 Granted for	

Add mailbox access permissions

12. Now, you have to assign access permissions for your mailboxes. There is no web UI for this yet - you have to use PowerShell.

DOCU13517.md

13. Install the required PowerShell modules. Note: You can skip this step if you have already installed AzureAD and ExchangeOnlineManagement modules. Open your PowerShell as Administrator, and run:

```
Install-Module -Name AzureAD
Install-Module -Name ExchangeOnlineManagement
```

Confirm installation from PSGallery by typing Y + Enter.



(Wondering why these modules install from an untrusted repository? See this answer to Azure-PowerShell issue.)

• Get the service principal ID associated with your application. Note: You will be asked to log into your Azure account.

```
$AppId = "YOUR_APP_ID_HERE"
$TenantId = "YOUR_TENANT_ID_HERE"
Import-module AzureAD
Connect-AzureAd -Tenant $TenantId
($Principal = Get-AzureADServicePrincipal -filter "AppId eq '$AppId'")
$PrincipalId = $Principal.ObjectId
```



14. Register the service principal for your application. Note: You will be asked to log into your Exchange Online account.

```
$DisplayName = "Some principal name for IMAP/POP3 here"
Import-module ExchangeOnlineManagement
Connect-ExchangeOnline -Organization $TenantId
New-ServicePrincipal -AppId $AppId -ServiceId $PrincipalId -DisplayName
$DisplayName
```

🔀 Windows PowerShell				_	- 🗆	×
PS C:\> \$DisplayName = "Principal for PS C:\> PS C:\> Import-module ExchangeOnline PS C:\> Connect-ExchangeOnline -Organ	r IMAP/POP3" Management nization \$TenantId					^
The module allows access to all exist ble cmdlets.	ting remote PowerShell (V1	.) cmdlets in addi	tion to the 9 new,	, faster, a	and more	relia
Old Cmdlets	New/Reliable/Faster C					
Get-CASMailbox Get-Mailbox Get-MailboxFolderPermission Get-MailboxFolderStatistics Get-MailboxFolderStatistics Get-MailboxStatistics Get-MobileDeviceStatistics Get-Recipient Get-RecipientPermission To get additional information, run: Get Send your product improvement sugges the module, contact Microsoft suppor	Get-EXOCASMailbox Get-EXOMailboxFolderF Get-EXOMailboxFolderF Get-EXOMailboxFolderS Get-EXOMailboxFolderS Get-EXOMailboxStatist Get-EXOMobileDeviceSt Get-EXORecipient Get-EXORecipient Get-Help Connect-ExchangeO tions and feedback to exoc	Permission tatistics ion ics atistics ssion online or check ht mdletpreview@serv alias for problem	tps://aka.ms/exops ice.microsoft.com, s or support issue	;-docs . For issu 25.	es relate	d to
PS C:\> PS C:\> New-ServicePrincipal -AppId :	\$AppId -ServiceId \$Princip	alId -DisplayName	\$DisplayName			
DisplayName	ServiceId		AppId			
Principal for IMAP/POP3	45f1383b-	-3021c83b9357	4f5a9f88-	-bi	dca9a88c0	89
PS C:\>						~

15. Add FullAccess mailbox permissions to all mailboxes you want to access from your application.

```
Add-MailboxPermission -User $PrincipalId -AccessRights FullAccess -Identity

"mailbox.1@example.org"

Add-MailboxPermission -User $PrincipalId -AccessRights FullAccess -Identity

"mailbox.2@example.org"

Add-MailboxPermission -User $PrincipalId -AccessRights FullAccess -Identity

"mailbox.3@example.org"
```

 Congratulations! Now you have registered an application for accessing Office/Microsoft 365 mailboxes via IMAP or POP3 protocol and received its Application (client) ID, Client secret and Directory (tenant) ID. These strings are going to be used by your application to authenticate to Microsoft 365 via OAuth 2.0 and receive an OAuth token. This token is then used to authenticate to Exchange Online using IMAP or POP3 protocols.

Common Issues

- Make sure you used correct IDs in PowerShell cmdlets. If the IDs are mismatched, your app will be able to request an access token, but won't be able to use it to access mailboxes.
- Use an up-to-date version of Rebex IMAP or POP3. Old versions have not been tested with contemporary Exchange Online. They might still work, but if you encounter any issues, please try the latest release.
- This guide is only suitable for IMAP and POP3. For Exchange Web Services guide, This guide dont apply
- Microsoft 365 does not support app-only authentication for SMTP yet. However, it will still be possible to enable username/password authentication for SMTP after fall 2022.

