

Microsoft OAuth2 Authentication for email sending

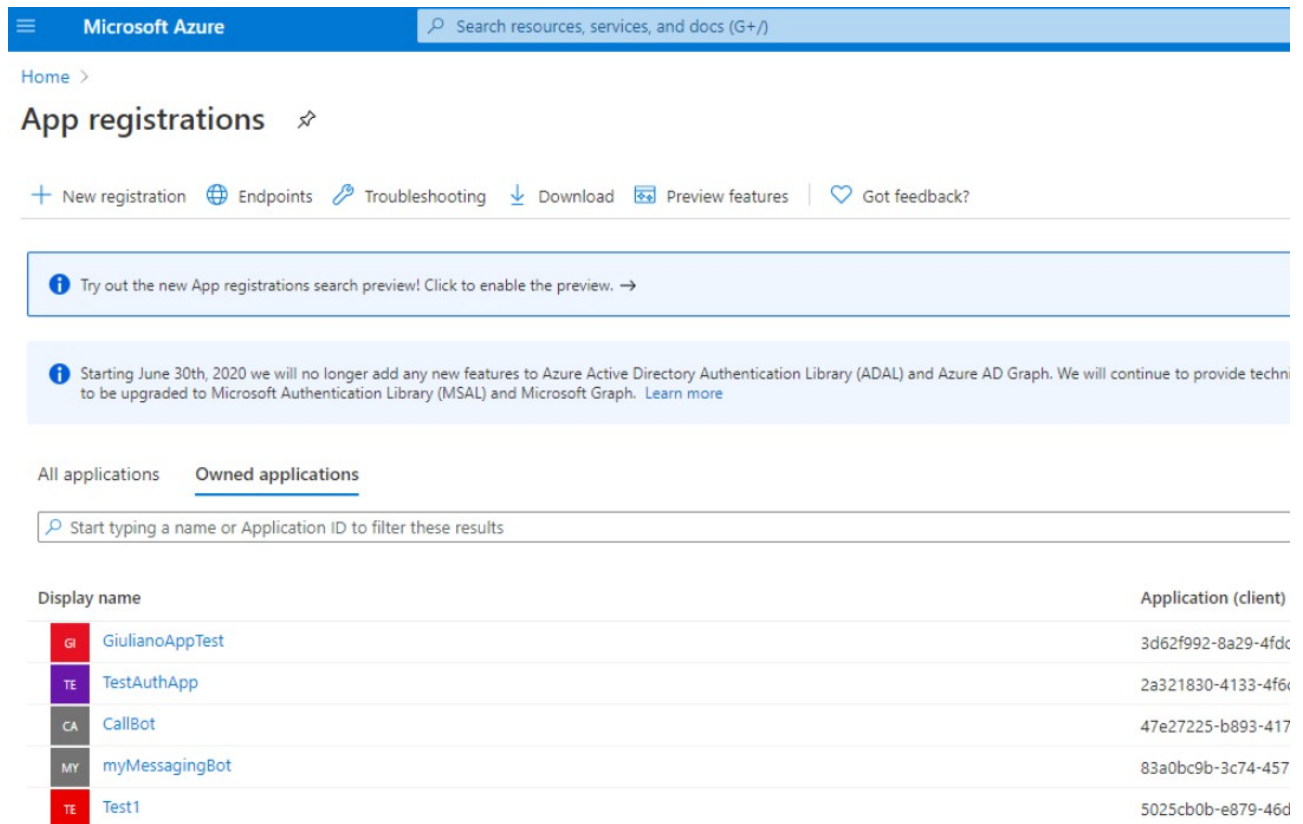
This authentication method is supported by Imagicle UC Suite, starting from 2021.Winter.2 release, and it relays on advanced OAuth2 authentication available for cloud-based Office 365 email service. Previous Imagicle releases are supporting OAuth2 basic authentication, which is dismissed by Microsoft starting from July 2021.

Requirements

In order to enable Imagicle UCX Suite to send email notifications and to handle email-to-fax service, leveraging Microsoft Office 365 cloud service and OAuth2 authentication, you must configure an application on [Azure Web Portal](#), taking note of Application ID, Directory ID and Client Secret data, needed later on while configuring this authentication method on Imagicle UCX Suite. Please read the following procedure to create a new application on Azure portal.

Azure web portal configurations

Please access to Azure portal and go to "App Registrations"



The screenshot shows the Microsoft Azure portal interface for App Registrations. The top navigation bar includes the Microsoft Azure logo and a search bar. Below the navigation bar, the page title is "App registrations". There are several links: "New registration", "Endpoints", "Troubleshooting", "Download", "Preview features", and "Got feedback?". A message box indicates that the new App registrations search preview is available. Another message box states that starting June 30th, 2020, new features for Azure Active Directory Authentication Library (ADAL) and Azure AD Graph will no longer be added, and they will be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Below the messages, there are tabs for "All applications" and "Owned applications". A search bar is present with the placeholder text "Start typing a name or Application ID to filter these results". The main content area displays a table of owned applications.

Display name	Application (client)
GI GiulianoAppTest	3d62f992-8a29-4fdc
TE TestAuthApp	2a321830-4133-4f6e
CA CallBot	47e27225-b893-417
MY myMessagingBot	83a0bc9b-3c74-457
TE Test1	5025cb0b-e879-46d

Click on "New registration" and choose a name like "MyOAuth2App". Then select "Accounts in this organizational directory only" and hit "Register"



Home > App registrations >

Register an application

Name

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



Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Imagicle spa 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)
- ☐ Personal Microsoft accounts only

[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.



By proceeding, you agree to the [Microsoft Platform Policies](#)

[Register](#)

The following window appears, including Application ID and Directory ID. Please copy both data, for later usage.

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations >

MyOAuth2App

Search (Ctrl+)

<<

Delete

Endpoints

Preview features

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Essentials

Display name : MyOAuth2App

Application (client) ID : 1cb8b5d2-8724-4f32-8152-a16a230b682b

Directory (tenant) ID : 969d5b92-bc05-403f-b576-97201b665e65

Object ID : 2c6bb16d-26b0-4910-8f6a-cff87b64bb2e

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL). We will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and

Now please click on "Certificates & secrets" option, included in left pane, and add a new "client secret" with the name of your choice and a long expiration period.

«

- Manage

- 🔑 Certificates & secrets

- ## Support + Troubleshooting

Description

Expires

- Add

Cancel

A secret string that the application uses to prove its identity when requesting a tok

+

No client secrets have been created for this application.

Microsoft OAuth2 Authentication for email sending

Request API permissions

< All APIs

Office 365 Exchange Online
https://outlook-tdf-2.office.com/

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.

Your application runs as a background service or daemon without a signed-in user.

From the list of available permission levels, please select "full_access_as_app" from "Other permissions" category.

Search resources, services, and docs (G+/)

!DigitalFax

Fax | API permissions

Refresh | Got feedback?

onfigured permissions

pplications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co
l the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Imagicle spa

API / Permissions name	Type	Description	Admin consent req...
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

> view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

< All APIs

Office 365 Exchange Online
https://outlook-tdf-2.office.com/

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 reply url to filter these results

Permission	Admin consent required
full_access_as_app ⓘ	Yes
Use Exchange Web Services with full access to all mailboxes	
Calendars	
Contacts	

Once permission has been assigned, you must authorize it for your organization, by clicking on "Grant admin consent for <company_name>".

Search resources, services, and docs (G+/I)

Mail2DigitalFax

MailFax | API permissions

Refresh | Got feedback?

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

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 Imagicle spa

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	-	...
Office 365 Exchange Online (1)				...
full_access_as_app	Application	Use Exchange Web Services with full access to all mailb...	Yes	Not granted for Imagicl... ...

To view and manage permissions and user consent, try [Enterprise applications](#).

This is the resulting page.

Search resources, services, and docs (G+/I)

Mail2DigitalFax

MailFax | API permissions

Refresh | Got feedback?

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 Imagicle spa

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	-	Granted for Imagicle spa ...
Office 365 Exchange Online (1)				...
full_access_as_app	Application	Use Exchange Web Services with full access to all mailb...	Yes	Granted for Imagicle spa ...

To view and manage permissions and user consent, try [Enterprise applications](#).

Optional configurations to restrict EWS Application to a mailbox set (Imagicle Digital Fax only)

Above described API Permission level privileges allows the application to access all EWS API on all organization mailboxes.

However, it's possible to optionally apply an advanced configuration on Microsoft Office 365 to restrict the application to access only a specific mailbox.

This is accomplished by accessing Exchange Online Administration Portal and create a new mail-enabled security group: Go to **Recipients** → **Groups** → **New mail-enabled security group**

Admin

Exchange admin center

dashboard recipients permissions compliance management organization protection advanced threats mail flow mobile public folders unified messaging hybrid

mailboxes **groups** resources contacts shared migration

Manage your Distribution Lists, Groups and more in New Exchange Admin Center.

GROUPS
IN OUTLOOK

More than a DL—even new members get all prior conversations and attachments.

Create a group

+ New Microsoft 365 group

- Distribution list
- Mail-enabled security group**
- Dynamic distribution list

DISPLAY NAME	STATUS
All Company	Active
imagicleucdev	Active

New Exchange admin center

Fill the form with a name and an alias. Those will be used later as a target of an Application Policy.

New Mail-enabled security group - Lavoro - Microsoft Edge

https://outlook.office365.com/ecp/UsersGroups/NewSecurity...

new mail-enabled security group

Mail-enabled security groups can be used to distribute messages and to assign access permissions to Active Directory resources. [Learn more](#)

*Display name:

*Alias:

*Email address:

 @

Notes:

*Owners:

+
-

Save
Cancel

Save form and edit the newly created group, go to **membership**, add a member, search for the mailbox to be granted to Digital Fax and add it:

Imagicle Digital Fax

general
ownership
+ membership
membership approval
delivery management
message approval
email options
MailTip
group delegation

Members:

+ -

Select Members - Lavoro - Microsoft Edge

https://outlook.office365.com/ecp/Pickers/MemberPi...

DISPLAY NAME	EMAIL ADDRESS
Adele Vance	AdeleV@imagicleucdev.onmicrosoft.com
Alex Wilber	AlexW@imagicleucdev.onmicrosoft.com
Diego Siciliani	DiegoS@imagicleucdev.onmicrosoft.com
Digital Fax	fax@imagicleucdev.onmicrosoft.com
Grady Archie	GradyA@imagicleucdev.onmicrosoft.com
Henrietta Mueller	HenriettaM@imagicleucdev.onmicrosoft.com
Imagicle Digital Fax	imagicle.digital.fax@imagicleucdev.onmicrosoft.com
Isaiah Langer	IsaiahL@imagicleucdev.onmicrosoft.com
Johanna Lorenz	JohannaL@imagicleucdev.onmicrosoft.com
Joni Sherman	JoniS@imagicleucdev.onmicrosoft.com
Lee Gu	LeeG@imagicleucdev.onmicrosoft.com
Lidia Holloway	LidiaH@imagicleucdev.onmicrosoft.com

1 selected of 20 total

add -> Digital Fax[remove];

OK Cancel

Connect to [Exchange Online PowerShell](#) and create an [Application Access Policy](#) to allow Digital Fax application to only access the newly created mail security group, by executing the following command, where:

- **AppId** value corresponds to the application "Client ID" value created within Azure app registration portal
- **PolicySecurityGroupId** corresponds to "Display Name" of the previously create security group

```
New-ApplicationAccessPolicy -AccessRight RestrictAccess -AppId <AppId> -PolicyScopeGroupId "Imagicle Digital Fax" -D
```



Output should be:

```
RunspaceId      : 2d08b315-81dd-4140-8a28-4a49431fb44d
ScopeName       : Imagicle Digital Fax
ScopeIdentity   : Imagicle Digital Fax
Identity        :
8f8ccdec-23bd-4452-bdb3-becc0c415a99\da34af4b-b01f-47e4-bfac-2f9fc3f1383e:S-1-5-21-2724517575-989
AppId           : da34aq4b-b01f-47e4-bfac-2f9fc3f1383e
ScopeIdentityRaw :
S-1-5-21-2724537575-989916663-4003715733-16076635;697c48d2-f812-4072-a10f-4455db66025e
Description     : Restrict Imagicle Digital Fax accessible mailboxes
AccessRight     : RestrictAccess
ShardType       : All
IsValid         : True
ObjectState     : Unchanged
```

Verify the rule, to check if the application can properly access the needed mailbox by executing the following command:

```
Test-ApplicationAccessPolicy -Identity <mail2fax address> -AppId <clientId>
```

Output should be:

```
RunspaceId : 2e08b315-81dd-4143-8a28-4a49431fa44d AppId :
da34ee4b-b01f-44e4-bfac-2f9fc3f1383e Mailbox : fax MailboxId :
c82eee91-a3e0-43f0-9a43-03e7ec7b1e96 MailboxSid :
S-1-5-21-2722357575-989916663-4003711733-159675946 AccessCheckResult : Granted
```

Then please verify the application can't access any other mailbox, by executing the following command:

```
Test-ApplicationAccessPolicy -Identity <any other mail address> -AppId <clientId>
```

In this case, output should be similar to below sample:

```
RunspaceId : 2d08b235-81dd-4140-8a28-4a49431fa44d AppId :
da34af4e-b01f-47e4-beec-2f9fc3f1383e Mailbox : fax MailboxId :
c82eee91-a3e0-43f0-9a43-03c7ec7b1e96 MailboxSid :
S-1-5-21-272451125-989916663-4003715733-15450946 AccessCheckResult : Denied
```