

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"

Microsoft Azure Search resources, services, and docs (G+)

Home >

App registrations

+ New registration | Endpoints | Troubleshooting | Download | Preview features | Got feedback?

Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support for these libraries until they are upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications Owned applications

Start typing a name or Application ID to filter these results

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).

MyOAuth2App ✓

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.

Public client/native (mobile ... e.g. myapp://auth ✓

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 (ADA) 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.

MyOAuth2App | Certificates & secrets

Search (Ctrl+/)

Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

Add a client secret

Description

DigitalFaxMailServiceSecret

Expires

- In 1 year
- In 2 years

Add

Cancel

Client secrets

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

+ New client secret

Description	Expires	Value
-------------	---------	-------

No client secrets have been created for this application.

Once added, you'll get some data associated to it. Please copy "Value" field for later usage. Copy the field immediately after having created the client secret, because it will be automatically hidden after few minutes, for security reasons.

Microsoft Azure Search resources, services, and docs (G+)

Home > App registrations > MyOAuth2App

MyOAuth2App | Certificates & secrets

Search (Ctrl+/) Got feedback?

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Certificates

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

Upload certificate

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 applicati

New client secret

Description	Expires	Value
DigitalFaxMailServiceSecret	12/31/2299	wJO9k3_x03-d-7cF~TptM9YDAEV84QJNv6

Now click on "Add permissions" and select "API's my organization users". Then search for "Office 365 Exchange online".

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below


Office 365

Name	Application (client)
Office 365 Enterprise Insights	f9d02341-e7aa-456c
Office 365 Exchange Online	00000002-0000-0ff1
Office 365 Information Protection	2f3f02c9-5679-4a5c
Office 365 Management APIs	c5393580-f805-4401
Office 365 Search Service	66a88757-258c-4c7:
Office 365 SharePoint Online	00000003-0000-0ff1

Select "Office 365 Exchange online" and then select "Application Permissions"

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

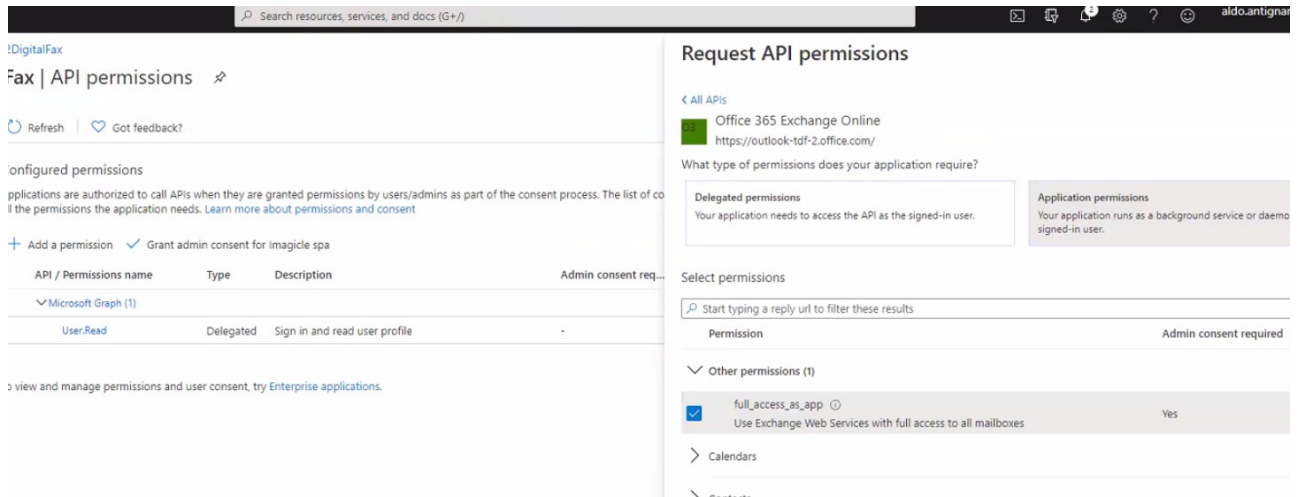
Your application needs to access the API as the signed-in user.

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.



!DigitalFax

Fax | 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 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...
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
Other permissions (1)	
<input checked="" type="checkbox"/> full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes
Calendars	
Contacts	

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

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.

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	-	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 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**

The screenshot shows the Exchange Admin Center interface. On the left is a navigation pane with 'recipients' selected. The main area is titled 'Exchange admin center' and contains a 'Groups' section. A blue banner at the top of the Groups section reads 'Manage your Distribution Lists, Groups and more in New Exchange Admin Center.' Below this is a 'GROUPS IN OUTLOOK' card with a 'Create a group' button. A '+ New Microsoft 365 group' button has a dropdown menu open, showing three options: 'Distribution list', 'Mail-enabled security group' (which is highlighted), and 'Dynamic distribution list'. Below the menu is a table of existing groups.

DISPLAY NAME	STATUS
All Company	Active
imagicleucdev	Active

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

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

*Display name:

Imagicle Digital Fax

*Alias:

imagicle.digital.fax

*Email address:

imagicle.digital.fax @ imagicleucdev.onmicro

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:

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
```