# Azure App Registration for Active Directory User Import

In order to be able to import users into Novus from an Azure Active Directory an Application must be created in Azure.

# App creation in Azure portal

Go to your Active Directory in the Azure portal and follow the steps below.

## Step 1. Register an App

Click App registrations, New registration.

### Azure Screenshot

# **Register an application**

#### \* Name

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

AdUserImport

### Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Bo Christian Skjøtt only - Single tenant)

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

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

O 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.

Web Ve.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies 🕝

Register

### Click the Register button

Home 🗦 Bo Christian Skjøtt				
Bo Christian Skjø	øtt   App registrations 🛛 🖈		×	
Manage	<ul> <li>Hew registration  Endpoints </li> </ul>	🦻 Troubleshooting 🛓 Download 💀 Preview feat	ures 🛛 💙 Got feedback?	
🚨 Users	Users All applications <b>Owned applications</b> Applications from personal account			
🚨 Groups	$\sim$ Start typing a name or Application ID to filter these results			
External Identities	Display name	Application (client) ID Created on	Certificates & secrets	
🚨 Roles and administrators	An Adliserimport	67bd1625-2b66-454b-00 10/12/2020	Current	
Administrative units		07501023-2500-4345-35 10/12/2020	Current	
Enterprise applications				
Devices				
App registrations				
Identity Governance				

# Step 2. Add API permissions

# Select **API permissions** and click on **Add a permission**.

## Select Microsoft Graph and then Application permissions.

Add these permissions:

- Group.Read.All
- GroupMember.Read.All
- User.Read.All

 $\times$ 

# Azure Screenshot

# **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.

Selec	Select permissions expa			
₽ us	P user ×			
F	Permission	Admin consent required		
> 1	> IdentityRiskyUser			
> 1	> IdentityUserFlow			
ד <	> TeamsAppInstallation			
> u	> UserAuthenticationMethod			
> ı	> UserNotification			
> UserShiftPreferences				
$\sim$ (	User (1)			
	User.Export.All ① Export user's data	Yes		
	User.Invite.All (i) Invite guest users to the organization	Yes		
	User.ManageIdentities.All () Manage all users' identities	Yes		
	User.Read.All ① Read all users' full profiles	Yes		
	User.ReadWrite.All ① Read and write all users' full profiles	Yes		

Add permissions

Discard

### Click on the "Grant admin consent for ..." button.

The permissions are then as shown below

- AdUserImport   API permissions 🖉						
ρ	Search (Ctrl+/) «	🖒 Refresh 📔 🗢 Got feedback?				
10	Overview	W     Image: Successfully granted admin consent for the requested permissions.       art     configured permissions				
<b>4</b> 23	Quickstart					
×	Integration assistant   Preview					
Ma	Manage Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of config include all the permissions the application needs. Learn more about permissions and consent					
-	Branding	+ Add a nermission V Grant admin consent for Bo Christian Skiett				
Э	Authentication					
Ŷ	Certificates & secrets	API / Permissions name	Туре	Description	Admin consent required	Status
11	Token configuration	✓Microsoft Graph (4)				
	API permissions	Group.Read.All	Application	Read all groups	Yes	🥑 Granted for I
		GroupMember.Read.All	Application	Read all group memberships	Yes	🥑 Granted for I
	Expose an API	User.Read	Delegated	Sign in and read user profile	-	🥑 Granted for I
-	Owners	User.Read.All	Application	Read all users' full profiles	Yes	🕑 Granted for I
9	Roles and administrators   Preview					-

# Step 3. Add a Client Secret

Home > Bo Christian Skjøtt > AdUserImport			
	♡ Got feedback?		
Soverview	Add a client secret		
🗳 Quickstart	Description MySecret		
💉 Integration assistant   Preview			
Manage	Expires		
🧮 Branding	O In 2 years		
Authentication	Never		
📍 Certificates & secrets			
Token configuration	Add Cancel		
API permissions			
🙆 Expose an API	Client secrets		
R Owners	A secret string that the application uses to prove its identity when		
Roles and administrators   Preview	A sedee saming that the application uses to prove its identity inter		
0 Manifest	+ New client secret		
Support + Troubleshooting	Description		
P Troubleshooting	No client secrets have been created for this application.		

Take a copy of the generated secret. It is only shown during creation.

Home > AdUserImport					
🔶 AdUserImport   Cert	tificates & se	crets 🖈			$\times$
✓ Search (Ctrl+/) «	♡ Got feedback?				
Overview     Quickstart	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.				
Manage	Certificates				
<ul> <li>Branding</li> <li>Authentication</li> </ul>	Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.				
📍 Certificates & secrets	↑ Upload certific	ate			
Token configuration	Thumbprint		Start date	Expires	
API permissions	No certificates have	been added for	this application.		
🙆 Expose an API	the contractor have been added for this application.				
Numers					
Roles and administrators   Preview	Client secrets				
III Manifest	A secret string that t can be referred to as	he application u application pas	ses to prove its iden sword.	tity when requesting a toker	n. Also
Support + Troubleshooting	+ New client cod	t			
Troubleshooting	Preventient sect		Mahar		
New support request	Description	Expires	value		
	MySecret	12/31/2299	R ***********	*****	

# Step 4. Get the Client and Tenant IDs for the application

Go to the Application Overview page and copy the Client ID and Tenant ID. You need to enter these in the Novus Configuration UI along with the Client Secret.

Azure Screenshot	
🔣 AdUserImport 🖉	
	📋 Delete 🌐 Endpoints 💀 Preview features
Overview	∧ Essentials
🗳 Quickstart	Display name : AdUserImport
🚀 Integration assistant   Preview	Application (client) ID : 67bd1625-2b66-454b-9969-73de9ccb98e3
	Directory (tenant) ID : e7c8b393-6866-475b-a45b-49cef97e4409
Manage	Object ID : bff7c3e1-ae54-42e3-8a31-2d39898bdb76

# App creation using Azure CLI commands

The steps above can also be done with the Azure CLI commands below.

Copy the **requiredResourceAccess.json** file to the Azure storage (clouddrive) used by Azure CLI.

If you are using the **Cloud Shell** in the Azure Portal then you can click on the Upload File button in its menubar as shown below



Create an application with this command

```
az ad app create \
--display-name AdUserImport \
--password VerySecretWord#1234 \
--end-date 2100-12-31 \
--required-resource-accesses requiredResourceAccess.json
```

Replace the password with your choice.

Grant admin consent for the requested API permissions with this command

where 00000000-0000-0000-000000000000 must be replaced with the actual ID of the application created above.

(Note: the az ad app permission admin-consent fails with an exception)