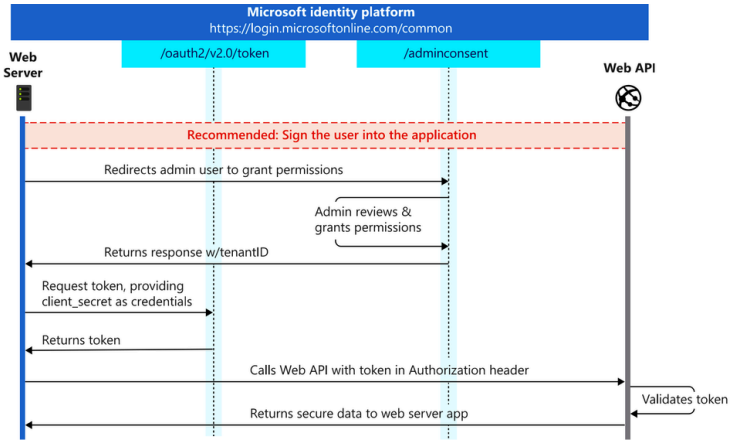
Copy of OAuth2.0 Email Integration Between Genesys and Microsoft (Client Credentials Flow)

1. Introduction

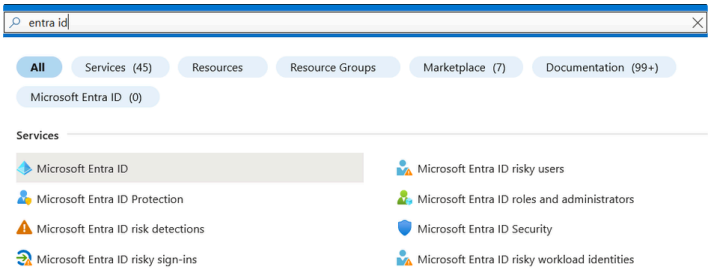
Since Genesys revealed the types of OAuth flows used for Microsoft 365 integration, now is the time to setup EMail integration using new type of flow - **Client Credential Grant Flow**. More on the subject can be seen in the official Microsoft document OAuth 2.0 client credentials flow on the Microsoft identity platform - Microsoft identity platform



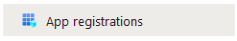
2. Creating application on the Azure portal

First step in the process is to create application on the Azure portal and give appropriate permissions.

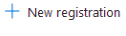
1. With appropriate login credentials, login to Microsoft Azure
2. When logged in, in the search bar, type “entra id” and from the list of results, click on the “Microsoft Entra ID“.



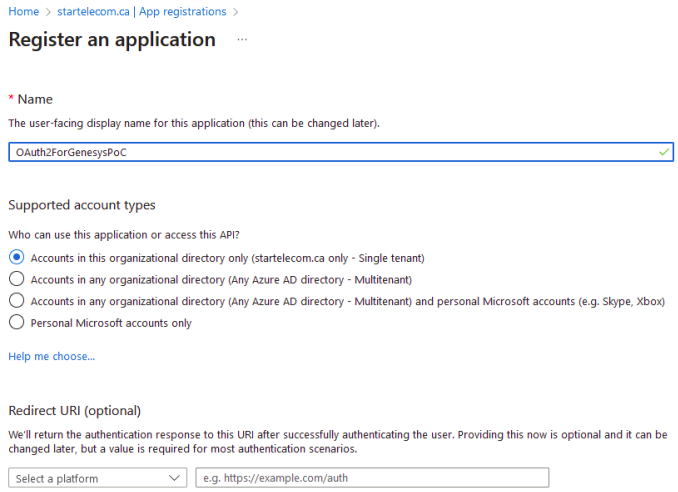
3. From the left menu, under the **Manage** submenu, choose “App registrations”.



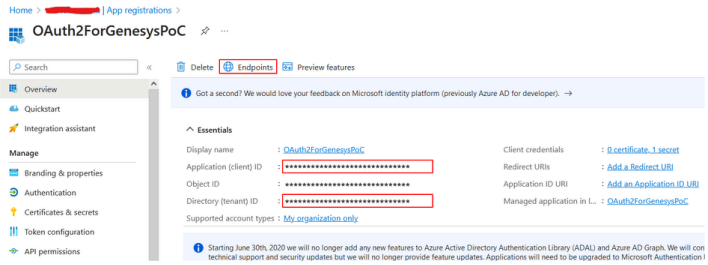
4. Now we can create new application, by clicking on the “New registration” option on the top menu.



5. All you have to do here is type the application name, in our example we will be creating application named OAuth2ForGenesysPoC. After entering application name, click on the Register button at the bottom of the page.



6. After registering the application, you will be taken to the application itself. Please copy values for the fields:
   * Application (client) ID,
   * Directory (tenant) ID
   as those will be needed later on for creating Custom SMTP Integration on the Genesys side.



7. Please note the “Endpoints” button in the image 2.3. We will need one more information from there, so please click the “Endpoints” button and copy the value from the OAuth 2.0 token endpoint (v2) field. This endpoint we will need later on in the process.

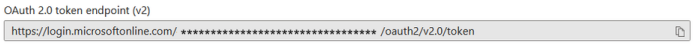
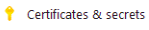


Image 2.4. OAuth 2.0 token endpoint

8. Next step would be creating a secret which will be used for authentication. To generate one, click on the “Certificates & secrets” options from the left menu.



9. In the window that got opened, click on the “New client secret”, add a description and the expiration period. Click add to save. After saving, please **copy the Value** of the newly created secret, as it will be needed later on.

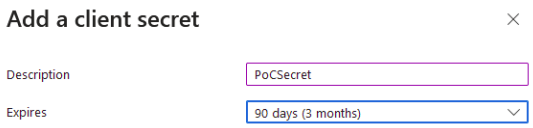
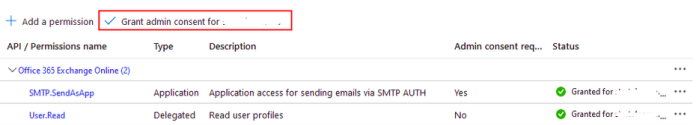


Image 2.5. - Creating the client secret

Please note that the secret's value is shown only once (on creation). If you fail to save it, you must recreate a new secret.

10. Next, we have to add appropriate API permissions. Click on the “API permission” button in the left menu and add the permissions given in the following image:



> Do not forget to grant admin consent after adding needed permissions. Failing to do so can produce an error in result returned from Microsoft Exchange Online - 535 5.7.3. Authentication unsuccessful.

3. Creating new Microsoft user

The second step is to create a valid Microsoft user and mailbox, assign it appropriate licenses, and update it with the allowed email applications, which are needed for this implementation to work.

1. With appropriate login credentials, login to https://admin.microsoft.com
2. Add a new user and assign it at least **Microsoft 365 Standard** license.
3. When you're done creating a mailbox and assign appropriate licenses, most important step is to turn on SMTP AUTH on the mailbox, since by default, this option is turned off. This option can be found by selecting the mailbox itself and when you do that, a new window on right side is opened. Select the "Mail" tab and from there, click on the "Manage email apps" option.

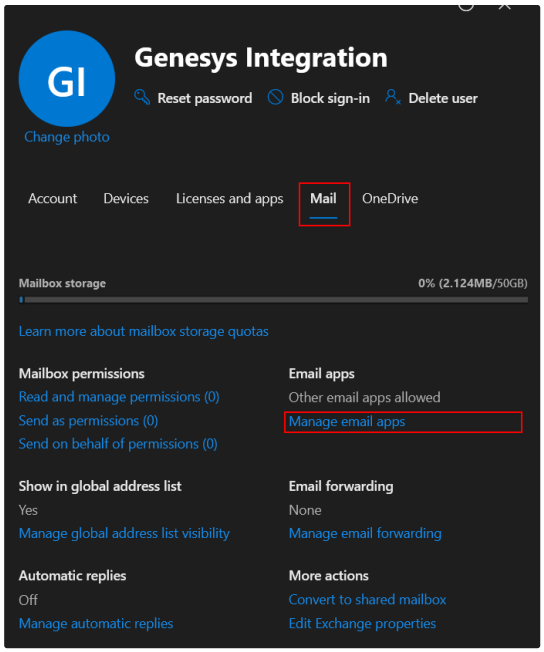


Image 3.1. - User settings

4. On the newly opened window, you will be presented with the application user has access to. If unchecked, please check the option next to "Authenticated SMTP" as this method of authentication is used by Client Credential Grant Flow.

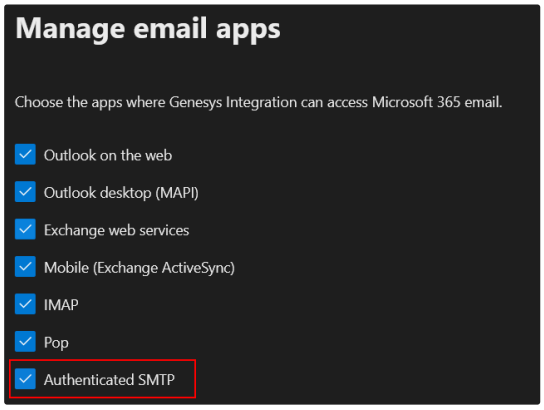


Image 3.2. Enabling Authenticated SMTP

4. Register service principal in Exchange

When the application is registered on the Azure portal and all admin consents are in place, it is time to register the application's service principal in Exchange using the Exchange Online Powershell.

4.1. Installing the AzureAD and Exchange Powershell module

In order to continue, we must install EXO (Exchange Online) powershell module. When installed, we must connect and login by using admin credentials.

```
Install-Module -Name ExchangeOnlineManagement -allowprerelease
Import-module ExchangeOnlineManagement
```

```
Connect-ExchangeOnline -Organization <tenantId>
```

Also, to continue to the next step, we must install the AzureAD PowerShell module. After the installation, we should connect current powershell session to the EntraID.

```
Install-Module -Name AzureAD -allowprerelease
Import-module AzureAD
Connect-AzureAD
```

4.2. Register service principal in Exchange

Assuming the previous step is successfully completed, we can try using the New-ServicePrincipal cmdlet in order to register the Entra AD application's service principal in Exchange.

```
$AADServicePrincipalDetails = Get-AzureADServicePrincipal -SearchString OAuth2ForGenesysPoC
New-ServicePrincipal -AppId $AADServicePrincipalDetails.AppId -ObjectId $AADServicePrincipalDetails.ObjectId -DisplayName "EXO Serviceprincipal for EntraAD App $($AAD
$EXOServicePrincipal = Get-ServicePrincipal -Identity "EXO Serviceprincipal for EntraAD App OAuth2ForGenesysPoC"
Add-MailboxPermission -Identity "genesysintegration_cf@YOUR_DOMAIN" -User $EXOServicePrincipal.Identity -AccessRights FullAccess
```

Please note that "OAuth2ForGenesysPoC" is the application name registered on Entra ID.

By doing this, we conclude the settings which are needed to be done on the Microsoft side. If successfully completed, you should leave Microsoft portal(s) with these information at hand:

- Client ID
- Client secret
- OAuth 2.0 Token Endpoint URL
- Email (username)

5. Configuring custom SMTP integration in Genesys

Next step in this PoC is to create and configure a custom SMTP integration and input all the information we got from Microsoft.

1. In the properties tab of the SMTP integration, we have to enter basic SMTP settings. Since we're using Microsoft Exchange, please will those fields with the information given in the image 5.1.

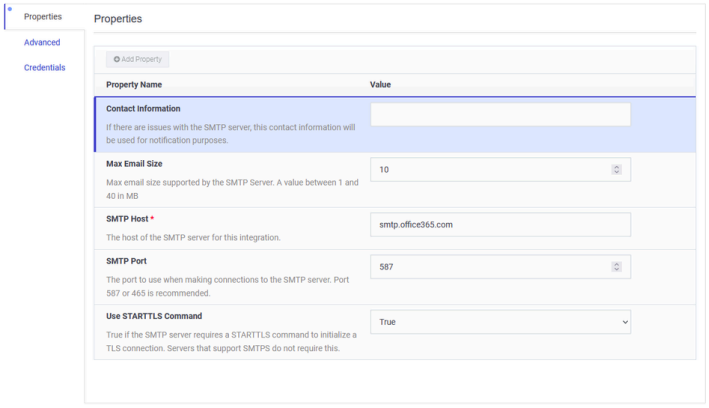


Image 5.1. Basic SMTP settings

2. Next step is to enter credentials, so let's open that tab and click on Configure (if you already have previous settings, you'll have Change button). In this window you can enter all the credentials brought from Microsoft. One field which value is missing is "Scopes". In this field, for this type of integration please type "https://outlook.office.com/.default". What does this mean? In Client Credential Grant Flow, we cannot use more specific scope. At the moment, .default scope is the only one which is being accepted by the Microsoft API.

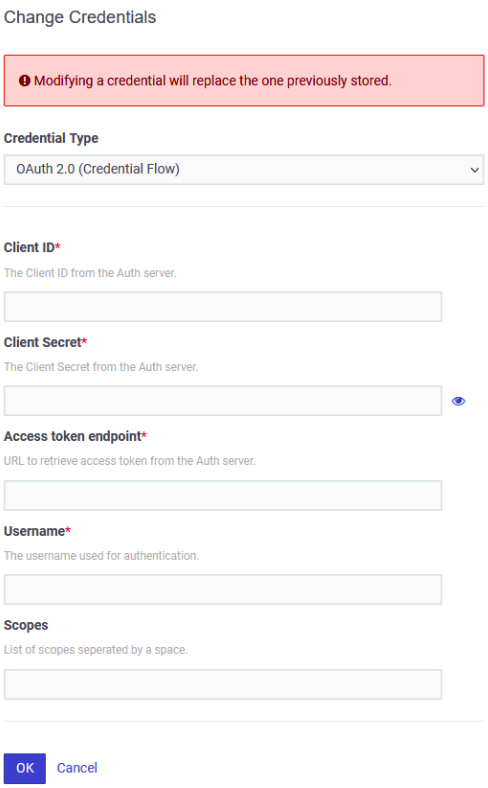


Image 5.2. Entering the data

3. Next you may try activating the custom SMTP integration. If everything is all right, you will get status Active.

6. Known error codes

Since Genesys does not return any usable error information, all the debugging can be done using either curl commands or checking the Sign-in logs on the Azure portal.

6.1. Error 535 5.7.3.

This error can be shown in several cases:

- If case of getting this error from the Microsoft Exchange Online on the Sign-In Logs page of the Azure portal, please re-check the permissions given to the application. As told, please confirm these permissions are in place:

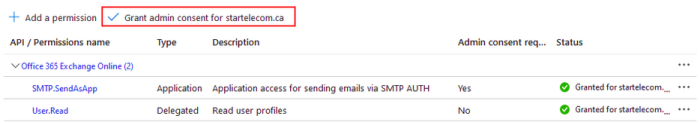


Image 6.1. - Configuring API permission set

- Please check if the scope is valid: "https://outlook.office.com/.default"
- Please check whether the Entra AD application's service principal in Exchange is registered.

6.2. Error 535 5.7.139.

If case of getting this error from the Microsoft Exchange Online on the Sign-In Logs page of the Azure portal, please re-check if the "Authenticated SMTP" option is set on the mailbox used for OAuth2.0 integration.

⚠ Please note, that if tenant policies are in place which prohibit SMTP authentication, then this option would not be enough for resolving the given error.

Related articles

If you are interested in other types of flows available for integration, please refer to pages down below.

OAuth2.0 SMTP Integration Between Genesys and Microsoft (ROPC Flow)