Reference:

Configure BC Oauth /w Application/Client/Service-To-Service Authorization):

* <https://yzhums.com/20690/>
* <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/automation-apis-using-s2s-authentication>
* <https://meetings.lm-ag.de/JoinCertain/Lobby?e=3a2adb7b-b4b9-46d8-876a-8ef0cf006994>

Configure BC Oauth /w Delegated authorization:

* <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/webservices/authenticate-web-services-using-oauth>
* <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/developer/devenv-develop-connect-apps#exploring-the-apis-with-postman-and-aad-authentication>

Business Central API reference: <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/api-reference/v2.0/endpoints-apis-for-dynamics>

Two types of Oauth Authentication Flows:

* **Delegated authorization**: access the Business Central Web Service API using a user credential. This authentication requires user’s interactive (i.e., user will be prompted to enter username and password – similar to how you login to Business Central website). This should work for one-time access to get data out, or when you want to retrieve/process data based on logged-in user. For example: an application to list all Sale Quotes created by the logged-in users, this is when we use Delegated authorization.
* **Application authorization (aka *service-to-service*, or *client credentials* authentication)**: this flow allows unattended access to Business Central without user credential (hence the name client/application authorization). The external service/server accesses Business Central by itself automatically, without user’s interactive, to perform its operation – such as pull data out or push data into Business Central.

For traditional Web Service Authentication (Basic Authentication), we will use the username and its corresponding Web Service Access Key. This basically the same with Delegated authorization, where the application accesses Business Central API through a user credential.

To configure OAuth Authentication for Business Central Online, we need to

1. **Create an App Registration** on the Azure Active Directory, where the Business Central tenant resides on.
2. Then **we will configure Business Central environment**, accordingly, based on which Authentication Flows we want to go with.
3. Finally, we will **configure our application/service to acquire Access Token and use the Token to access Business Central API**.

In the example below, we will setup an App Registration that supports both Delegated and Application authorization flows. Then we will configure Business Central accordingly. After that, we use Postman to retrieve data from Business Central API through both authorization flows.

# Create Azure App Registration

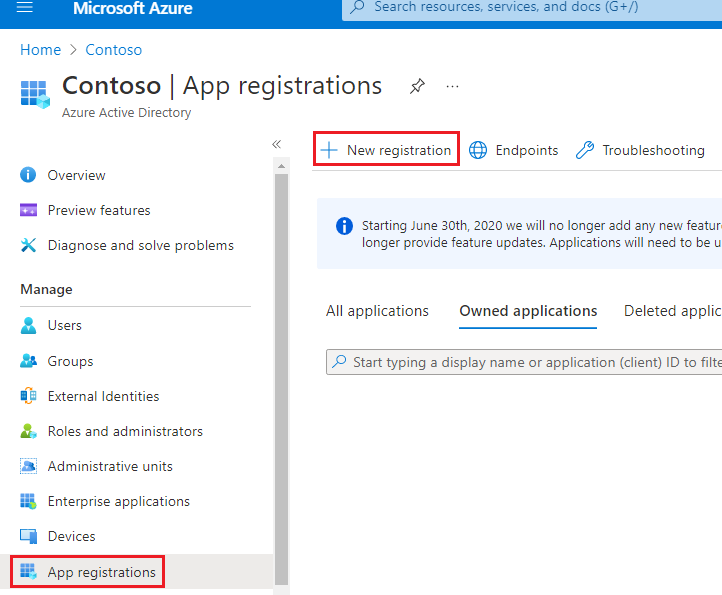
Each external service/app should have their own App Registration on Azure.

Example: there are three partners: Open Door, Sana and ChargeLogic. They both wants to access to the customer’s Business Central environment. We will need to create three Azure App Registration and give each partner the information of their own App Registration and access information.

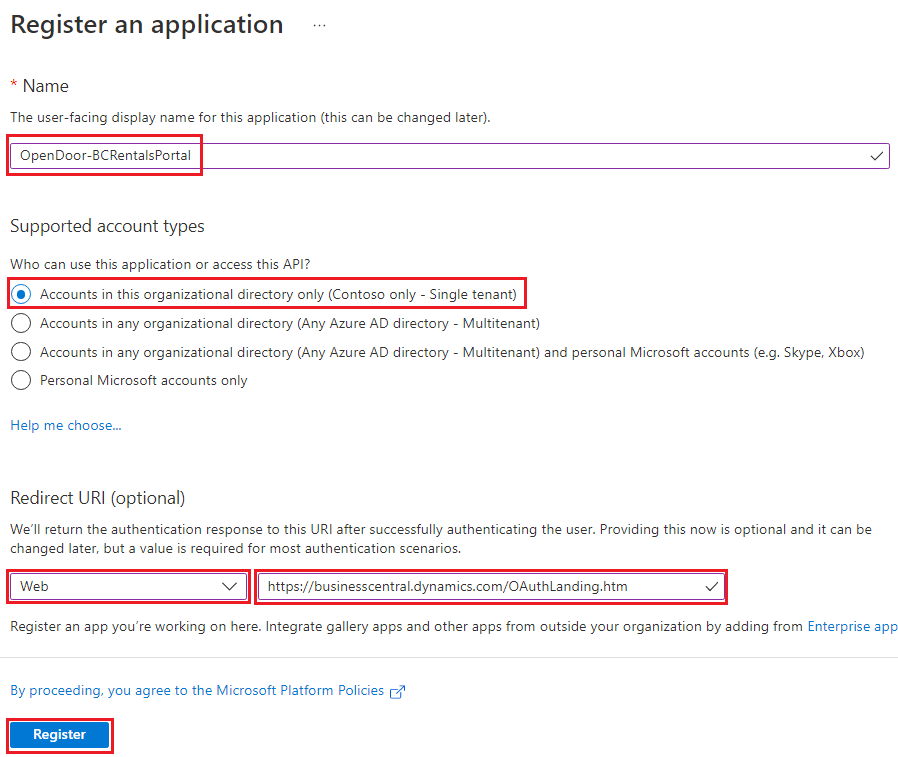
In this example, we will create an App Registration for Open Door, so that their Rentals portal server can access into the Business Central server to manage Rentals Quotes or Items (a total fiction scenario – we do not have such Portal)

This task can be done by IT team, or any personnel who has Global Admin right to the environment.

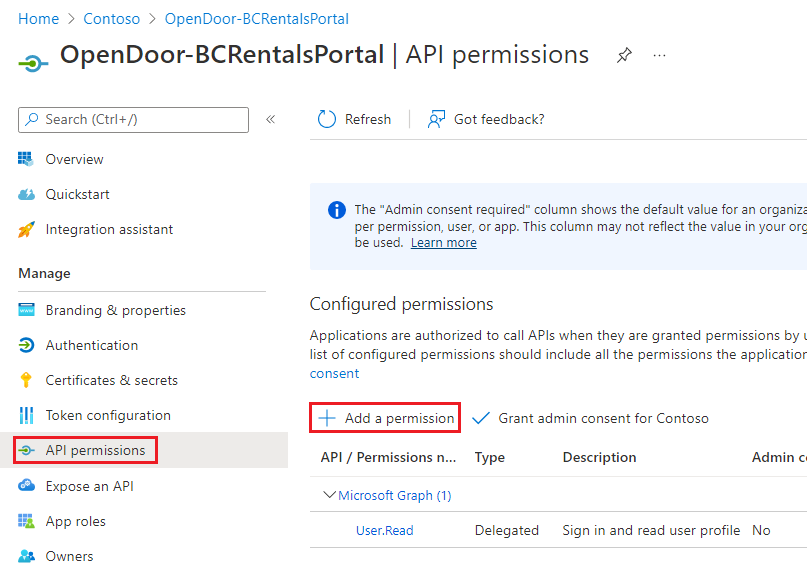
1. Login to **Azure Active Directory Portal of the Business Central tenant**, using the **Global Admin account**: <https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview>
2. In the Portal, go to **App Registration** pane and click **New registration**.



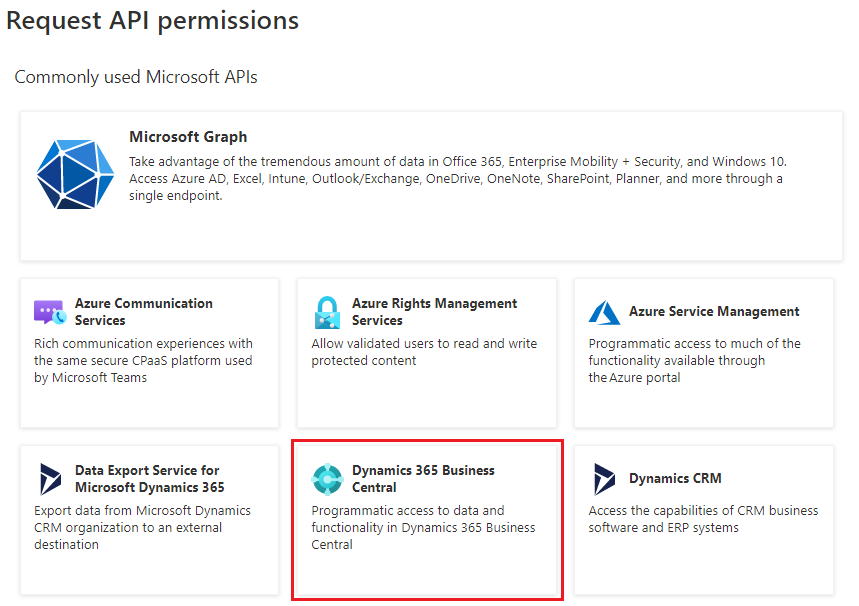
1. Name the application as descriptive as possible. It should preferably have the partner’s name and even the solution name (in case same partner has multiple services connect to the BC environment – each of them should have their own application)
2. Supported account types should be **Accounts in this organizational directory only** unless you know you need other option.
3. Redirect URI should be of type **Web** with following value [**https://businesscentral.dynamics.com/OAuthLanding.htm**](https://businesscentral.dynamics.com/OAuthLanding.htm)
4. Then click on **Register** to create the App Registration.



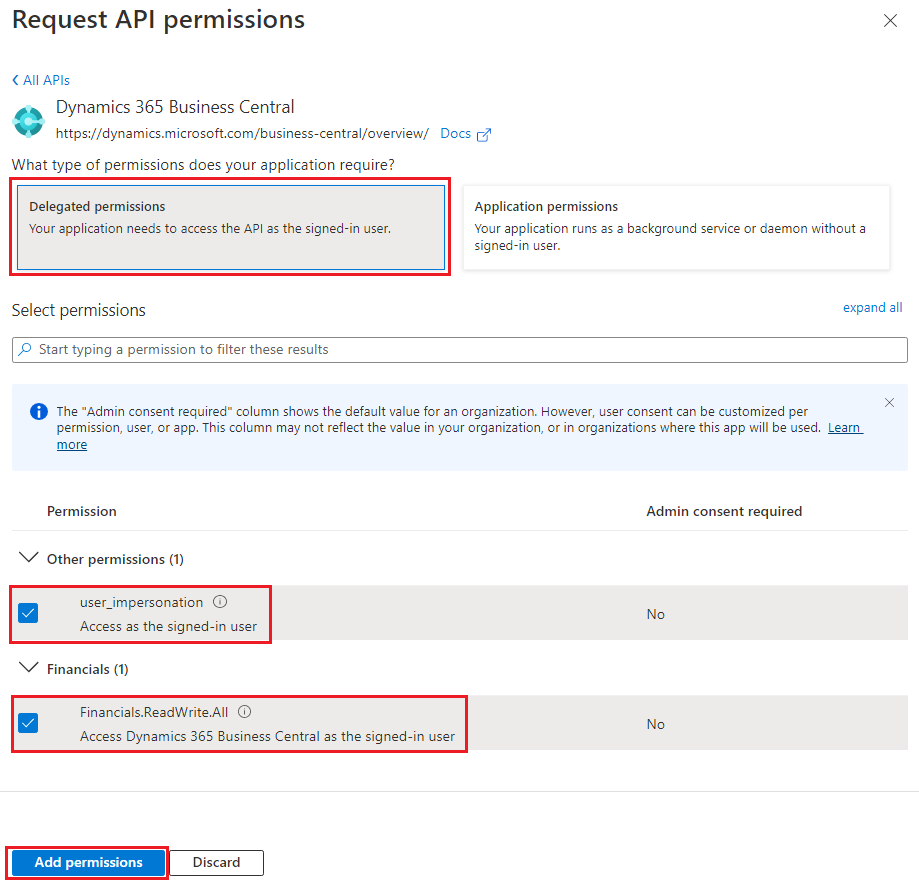
1. Once the App registration is created, you will be redirected to the app’s page. From there, go to **API permissions** tab and click **Add a permission**.



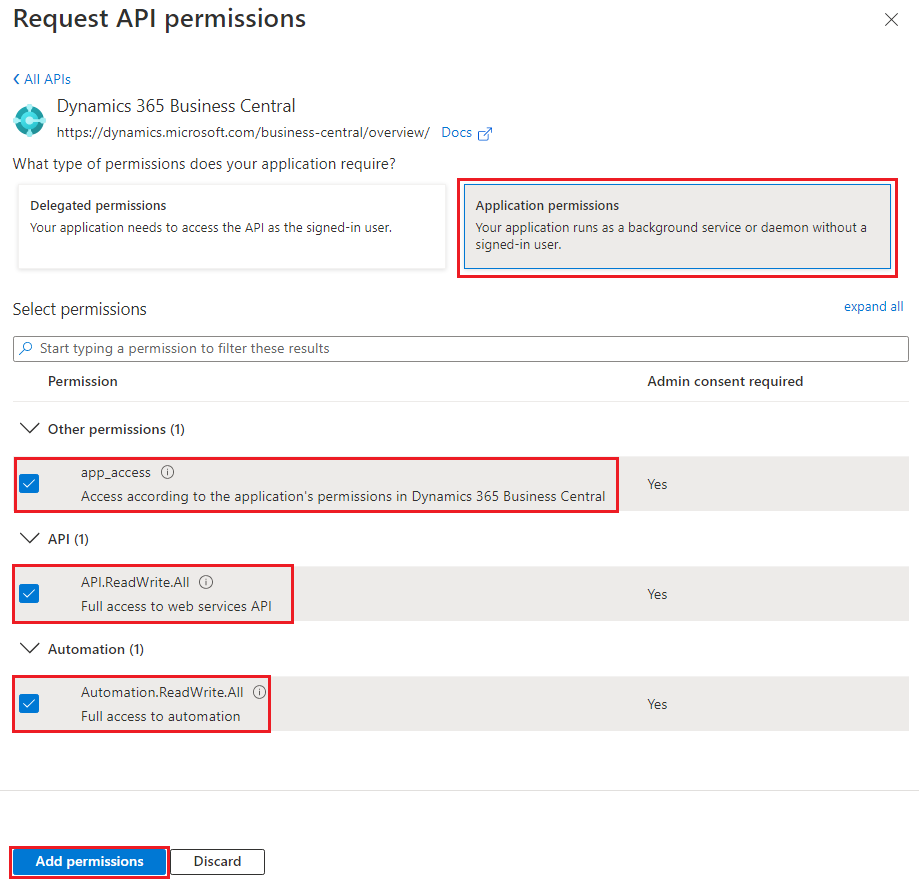
1. Select **Dynamics 365 Business Central** from the list.



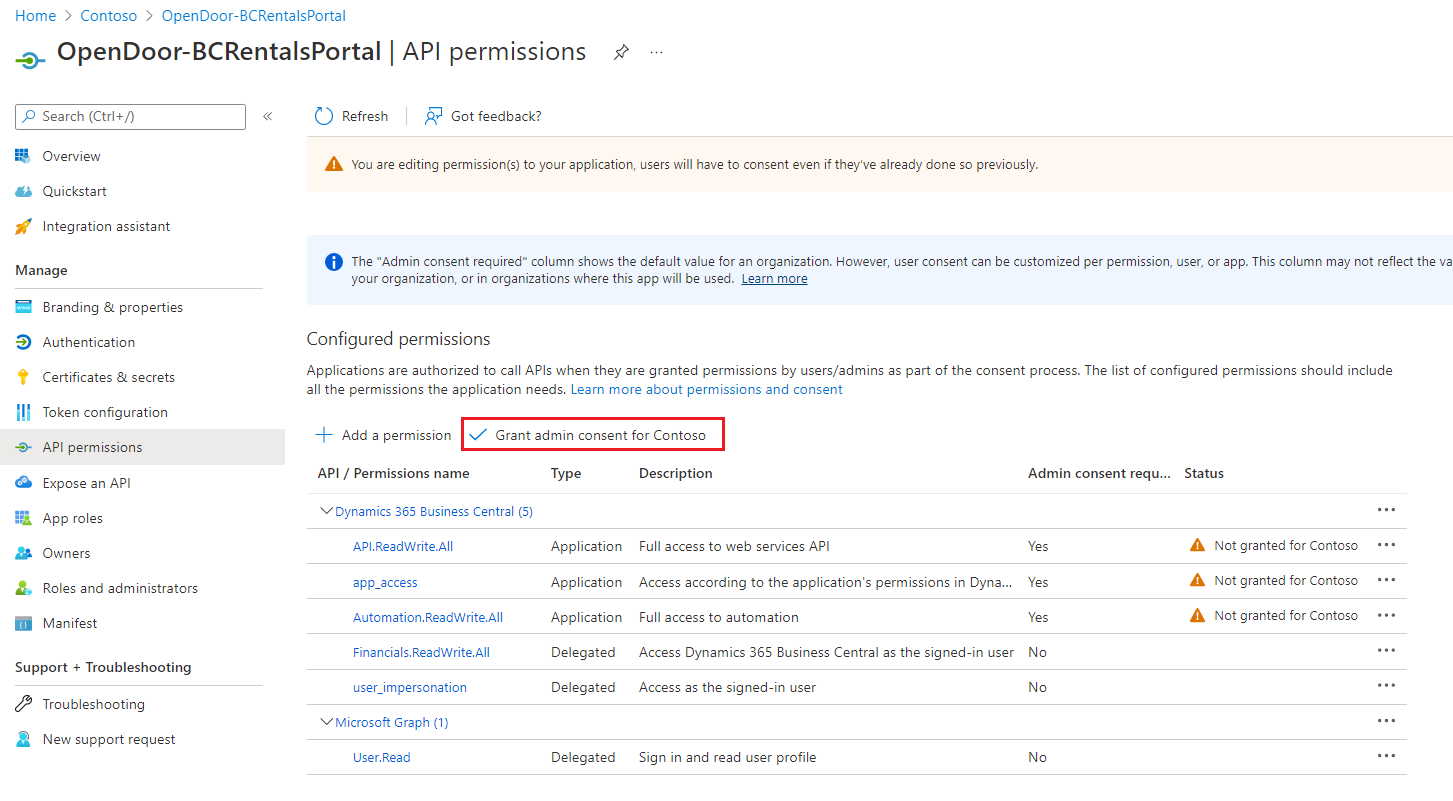
1. Select **Delegated permission** and tick both **user\_impersonation** and **Financials.ReadWrite.All** permissions, then click **Add permissions**.



1. Repeat step 7-8, this time select **Application permissions** and select all listed permission (**app\_access**, **API.ReadWrite.All** and **Automation.ReadWrite.All**) and click **Register**.



1. Back to the permission list, click on Grant admin consent button.



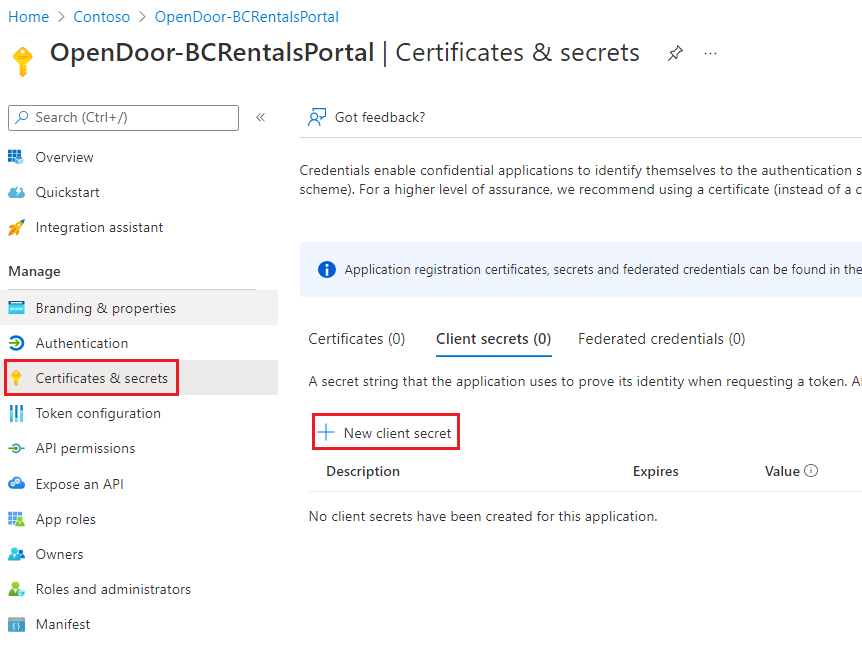
After this action, all the permissions should have green checkmark next to them.

Note: All those permissions are needed to ensure the App Registration supports both **Delegated Authorization** and **Application/Client/Service-to-Service** authentication. If you know your app only needs one or another, configure the permission accordingly for better security.

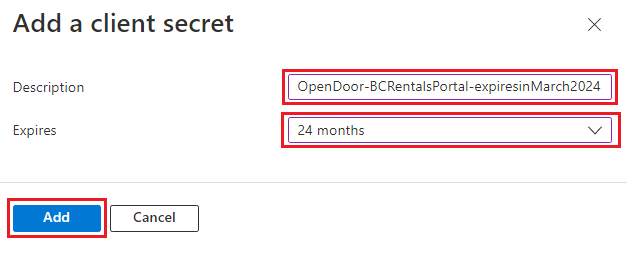
Graphical user interface, text, application, email

Description automatically generated

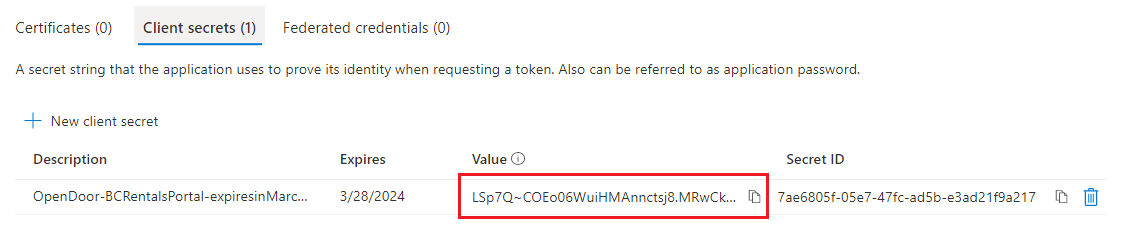
1. Go to **Certificates & secrets** section and click **New client secret**.



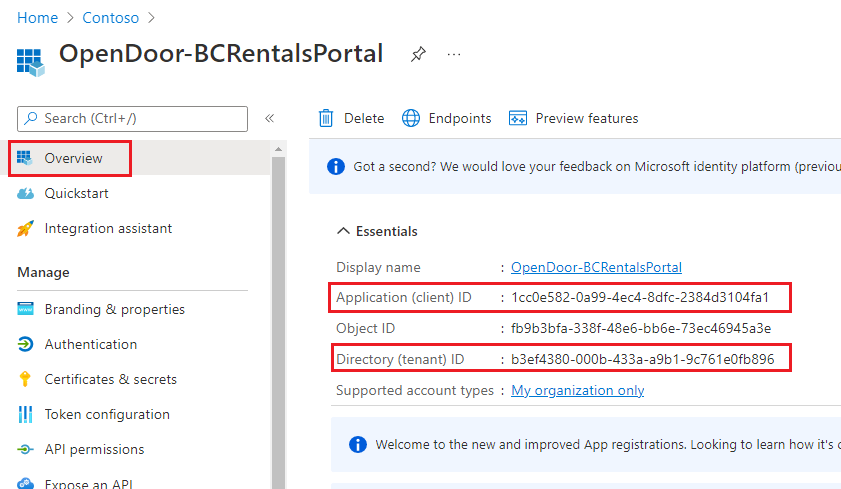
1. Put a description and configure expiry date of the secrets (maximum is 24 months) then click **Add**.



1. Take note of the secret value. It will disappear when you leave the page.



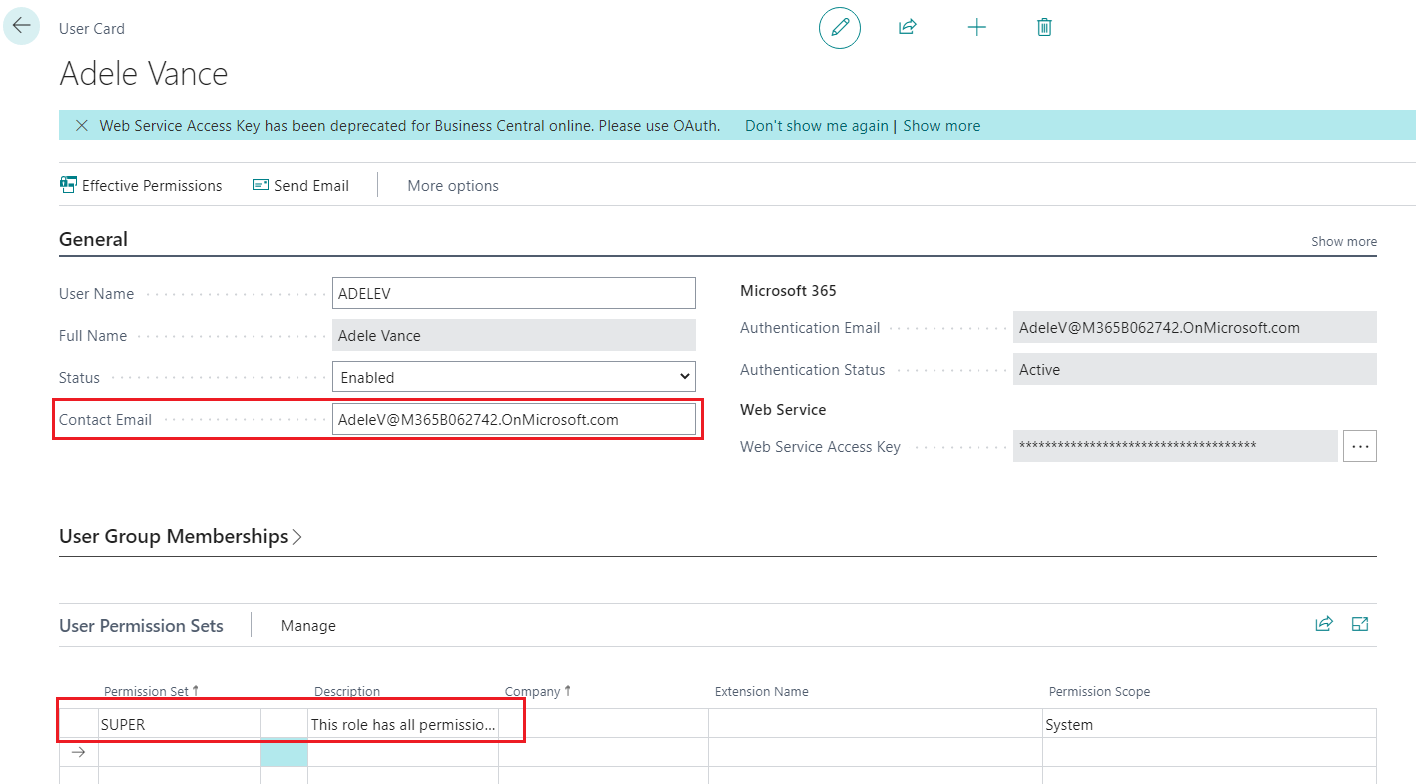
1. Go to **Overview** tab and take note of **Application (Client) ID** and **Directory (tenant) ID** values.



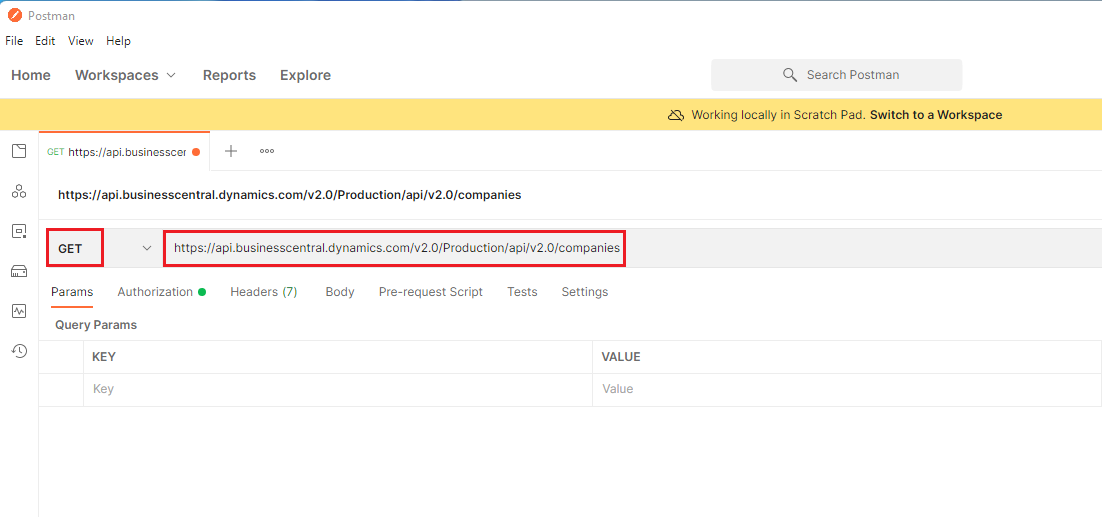
# Connect to Business Central’s API using Delegated Authorization (using Postman)

With Delegated authorization, we authenticate and access Business Central’s API using a user credential. Therefore, the very first step is to configure the user in Business Central with designated permission.

1. Prepare a Business Central user with sufficient permissions (e.g., if you want to access Sales Quotes/Orders, the user must have such permissions). For the sake of simplicity, the user in this example ([AdeleV@M365B062742.OnMicrosoft.com](mailto:AdeleV@M365B062742.OnMicrosoft.com)) has SUPER permission to the Business Central environment



1. Open Postman application, and use GET command for the following API endpoint: [https://api.businesscentral.dynamics.com/v2.0/**Production**/api/v2.0/**companies**](https://api.businesscentral.dynamics.com/v2.0/Production/api/v2.0/companies). This endpoint gets list of **companies** in the **Production** environment. More information about Business Central API: <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/api-reference/v2.0/endpoints-apis-for-dynamics>



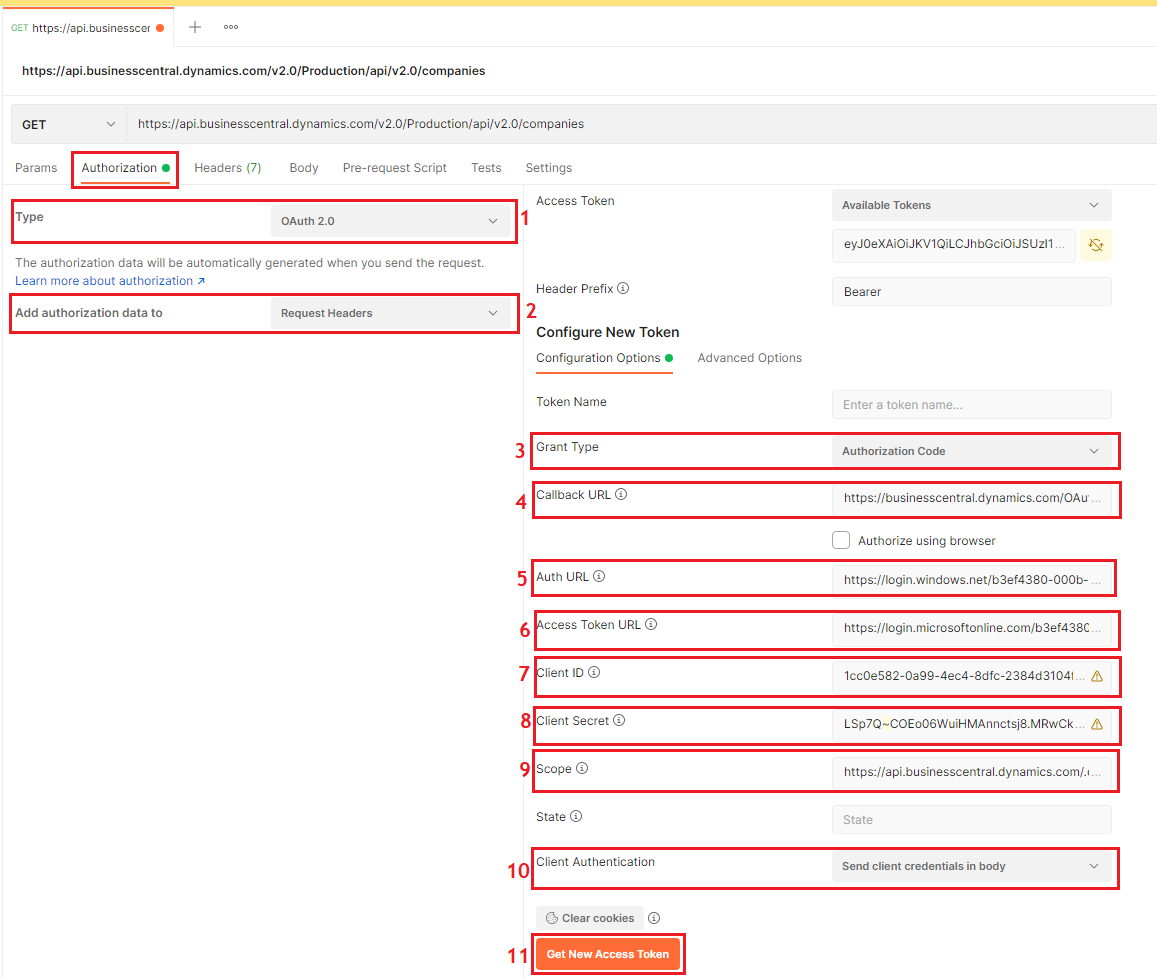
1. Go to Authorization tab, then enter the following information:
   1. **Type**: OAuth 2.0
   2. **Add authorization data to**: Request Headers
   3. **Grant Type**: Authorization Code
   4. **Callback URL**: https://businesscentral.dynamics.com/OAuthLanding.htm
   5. **Auth URL**: [https://login.windows.net/**DirectoryID**/oauth2/authorize?resource=https://api.businesscentral.dynamics.com](https://login.windows.net/DirectoryID/oauth2/authorize?resource=https://api.businesscentral.dynamics.com), where the **DirectoryID** is the corresponding you get from **Step #15 in Create Azure App Registration** above.

Example: <https://login.windows.net/b3ef4380-000b-433a-a9b1-9c761e0fb896/oauth2/authorize?resource=https://api.businesscentral.dynamics.com>

* 1. **Access Token URL**: [https://login.microsoftonline.com/**DirectoryID**/oauth2/v2.0/token](https://login.microsoftonline.com/DirectoryID/oauth2/v2.0/token), where the **DirectoryID** is the corresponding you get from **Step #15 in Create Azure App Registration** above.

Example: <https://login.microsoftonline.com/b3ef4380-000b-433a-a9b1-9c761e0fb896/oauth2/v2.0/token>

* 1. **Client ID**: you get this corresponding information **Step #15 in Create Azure App Registration** above. For example: 1cc0e582-0a99-4ec4-8dfc-2384d3104fa1
  2. **Client Secret**: this is from **Step #14 in Create Azure App Registration** above. Example: LSp7Q~COEo06WuiHMAnnctsj8.MRwCkkyBGhd.
  3. **Scope**: <https://api.businesscentral.dynamics.com/.default>
  4. **Client Authentication**: Send client credentials in body
  5. Click on **Get New Access Token**.



* 1. Login with the Business Central User above:

Graphical user interface, application

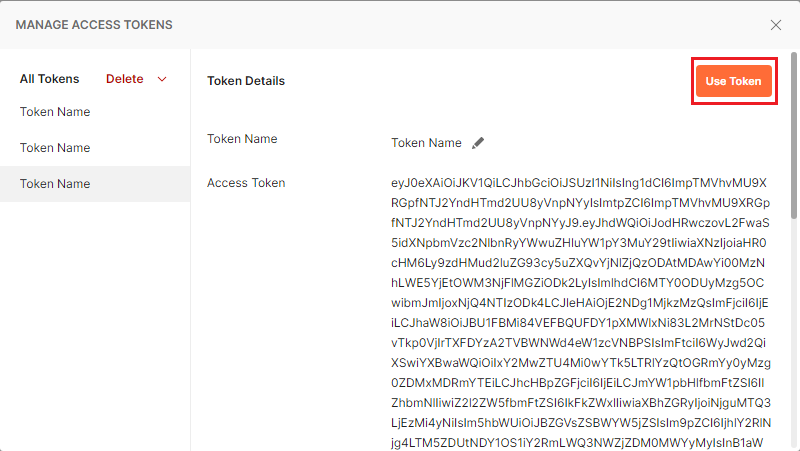
Description automatically generated

* 1. The authentication succeeds with the following message:

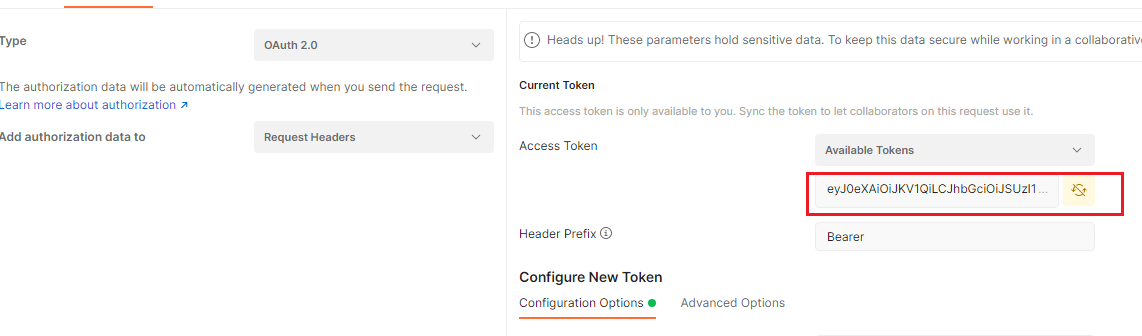
Graphical user interface, text, application

Description automatically generated

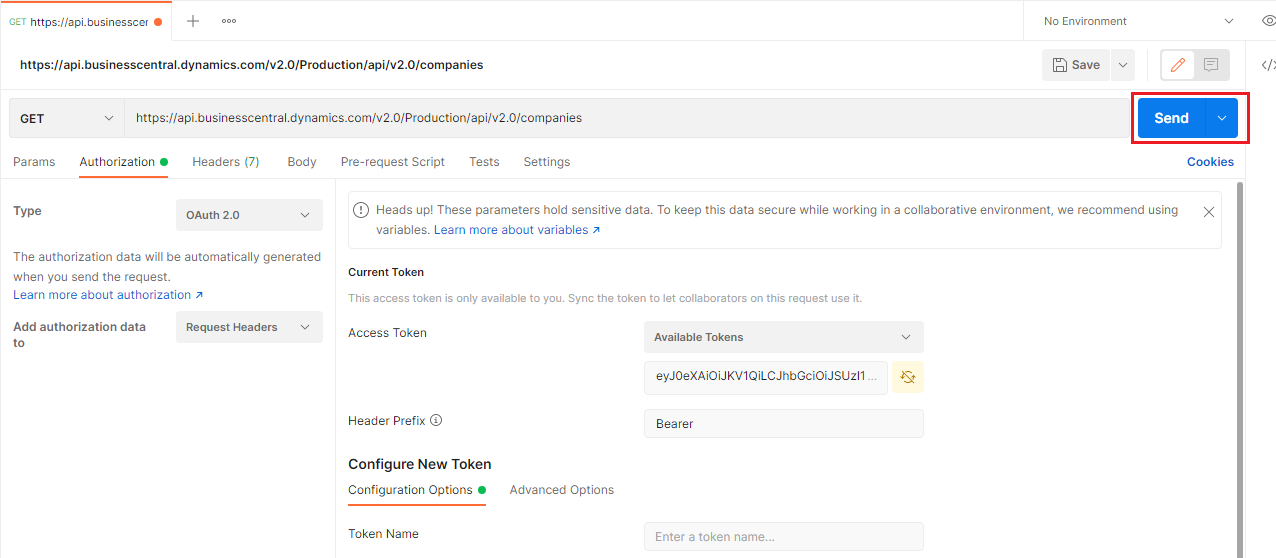
* 1. After this, an Access Token has been generated. Click on Use Token button.



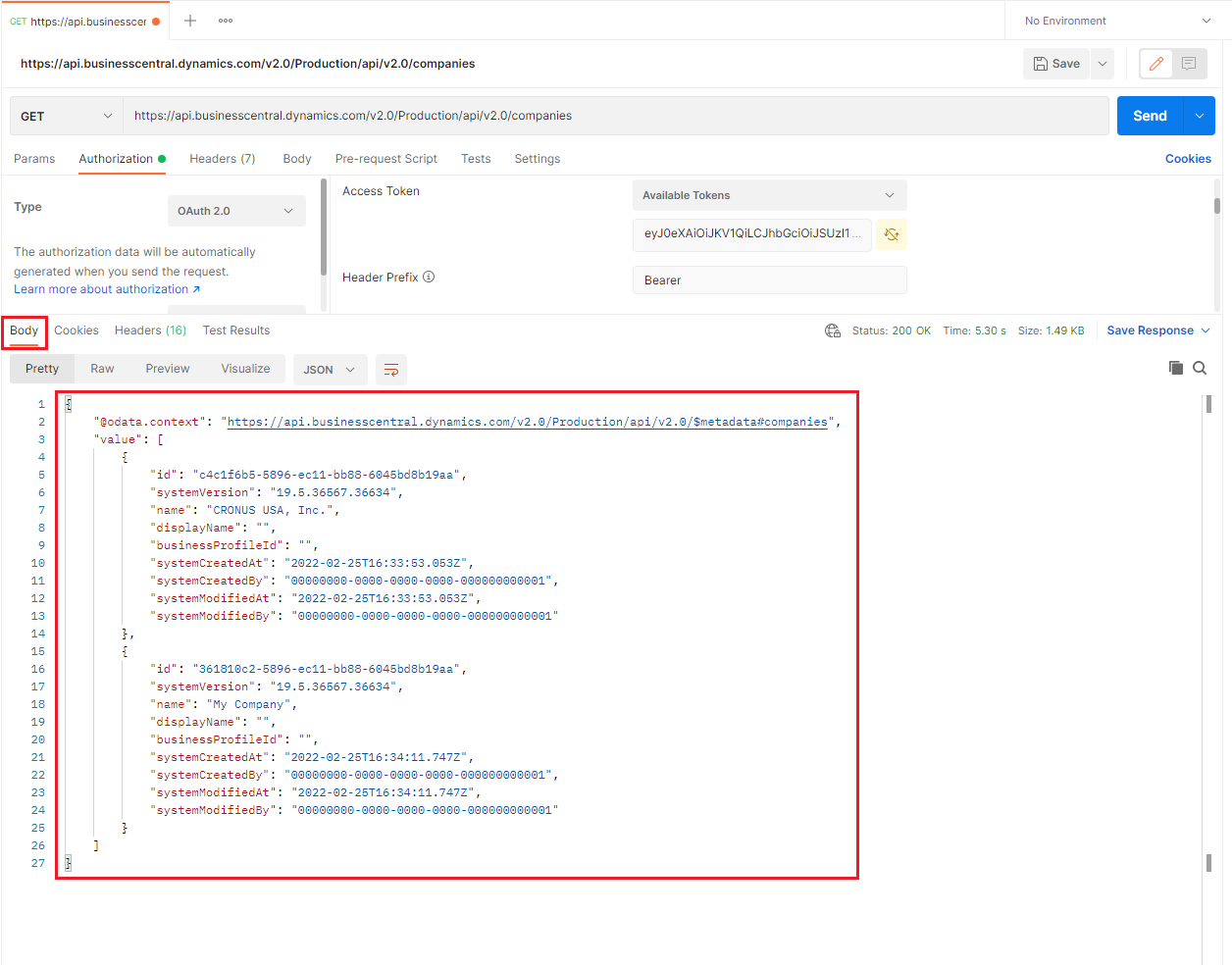
* 1. The token has been automatically filled in the **Access Token** field in Postman



1. Once we have the token in Access Token field, click on **Send** button. In this example, Postman will try to **GET** from [**https://api.businesscentral.dynamics.com/v2.0/Production/api/v2.0/companies**](https://api.businesscentral.dynamics.com/v2.0/Production/api/v2.0/companies) endpoint using the credential of [AdeleV@M365B062742.OnMicrosoft.com](mailto:AdeleV@M365B062742.OnMicrosoft.com) user through the acquired Access Token.



1. The result is displayed in the Body tab. This confirms the authorization and access have completed successfully.

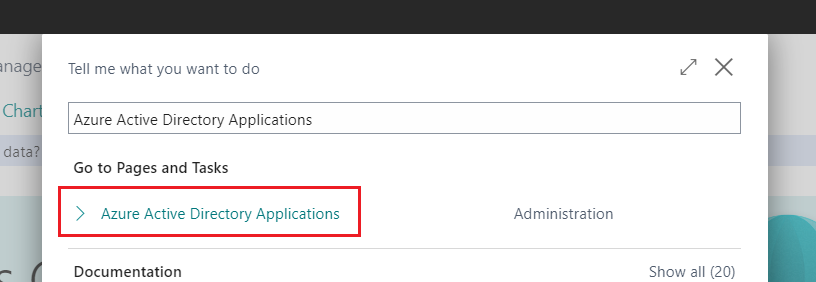


# Connect to Business Central’s API using Application/Client/Service-To-Service Authorization (using Postman)

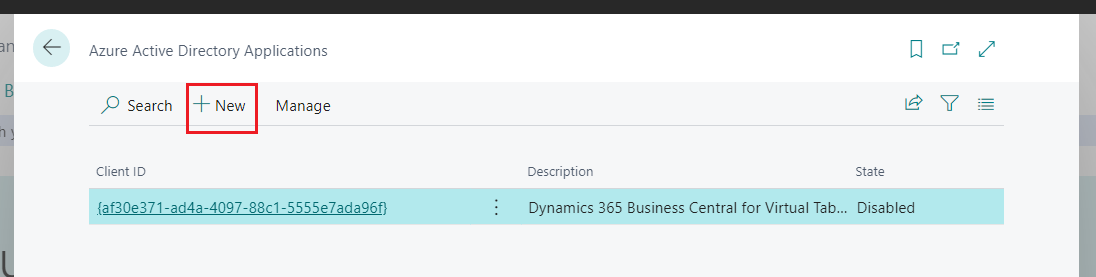
With Application/Client/Service-To-Service authorization, we authenticate and access Business Central’s API using the Application Credential, which is created in **Create Azure App Registration** above.

While the Delegated Authorization requires a user to login to generate corresponding Access Token, the Application/Client/Service-To-Service authorization does not require such “user interactive” step. This allows us to run unattended application/service, as well as automation on Business Central. The first step is to configure the Application in Business Central environment:

1. In Business Central, search and run the **Azure Active Directory Applications** page.

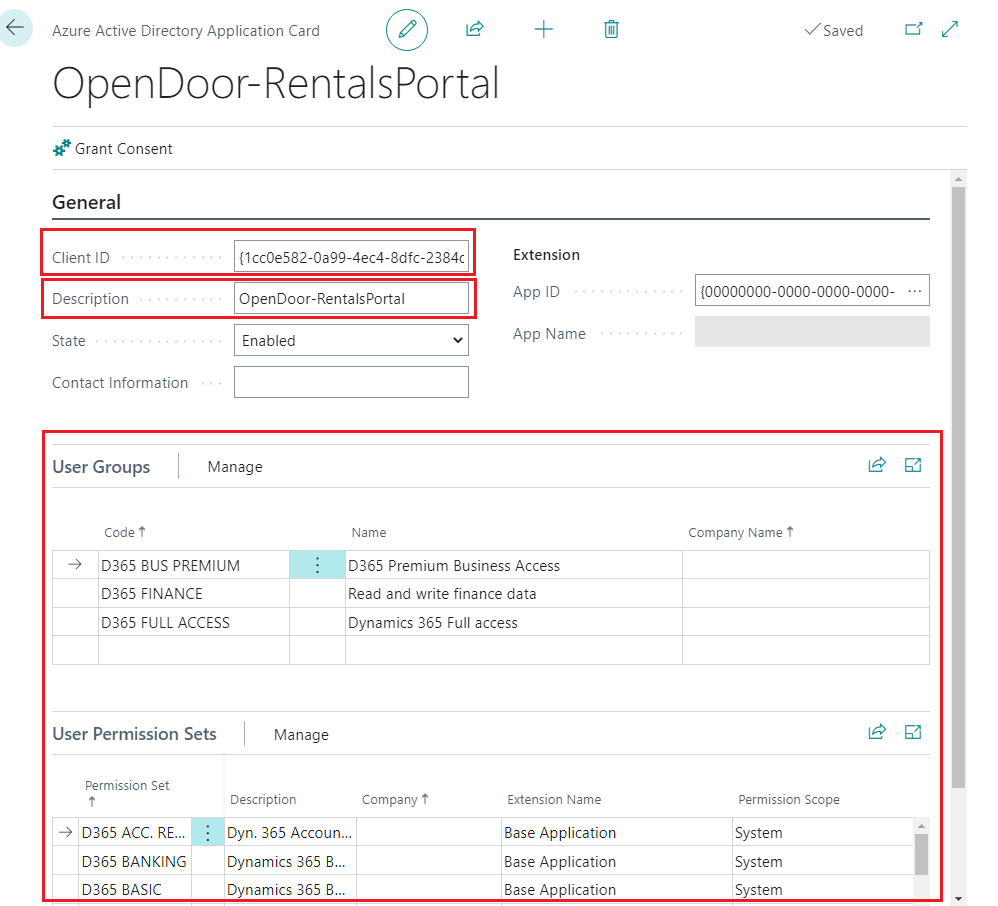


1. Click on **New** button.



1. Enter the following information:
   * **Client ID**: you get this information from **Step #15 in** **Create Azure App Registration**
   * **Description:** Use the name of the application here (e.g., OpenDoor-RentalsPortal) so that we know this relates to such application in Azure App Registration.
   * **Permission:** setup sufficient permissions (e.g., if you want to access Sales Quotes/Orders, the user must have such permissions)

Note: Application is not allowed to have SUPER permission. This is by design.

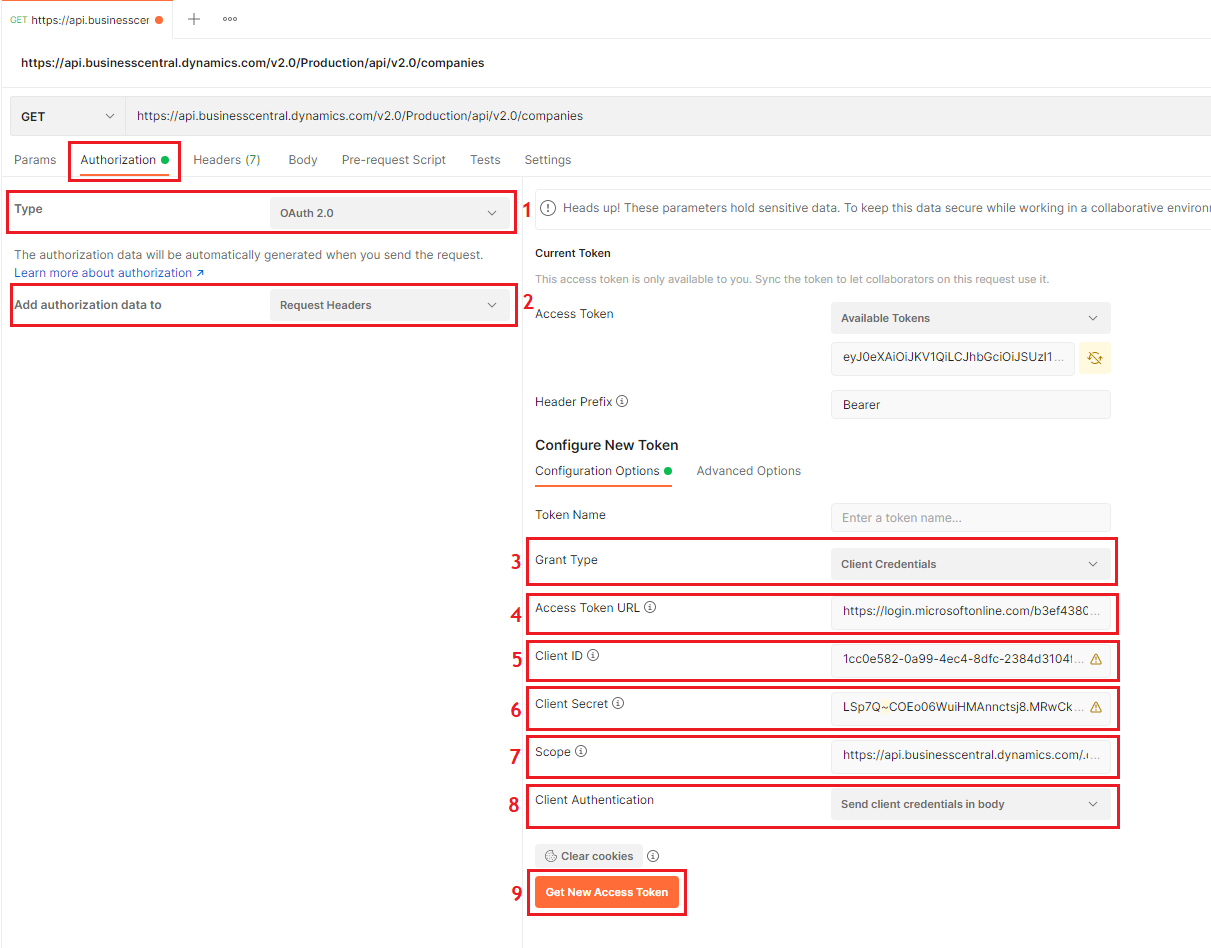


That is it for Business Central. Now we can use Postman to test.

1. Open Postman application, and use GET command for the following API endpoint: [https://api.businesscentral.dynamics.com/v2.0/**Production**/api/v2.0/**companies**](https://api.businesscentral.dynamics.com/v2.0/Production/api/v2.0/companies). This endpoint gets list of **companies** in the **Production** environment. More information about Business Central API: <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/api-reference/v2.0/endpoints-apis-for-dynamics>
2. Go to **Authorization** tab, then enter the following information:
   1. **Type**: OAuth 2.0
   2. **Add authorization data to**: Request Headers
   3. **Grant type**: Client Credentials
   4. **Access Token URL**: [https://login.microsoftonline.com/**DirectoryID**/oauth2/v2.0/token](https://login.microsoftonline.com/DirectoryID/oauth2/v2.0/token), where the **DirectoryID** is the corresponding you get from **Step #15 in Create Azure App Registration** above.

Example: <https://login.microsoftonline.com/b3ef4380-000b-433a-a9b1-9c761e0fb896/oauth2/v2.0/token>

* 1. **Client ID**: you get this corresponding information **Step #15 in Create Azure App Registration** above. For example: 1cc0e582-0a99-4ec4-8dfc-2384d3104fa1
  2. **Client Secret**: this is from **Step #14 in Create Azure App Registration** above. Example: LSp7Q~COEo06WuiHMAnnctsj8.MRwCkkyBGhd.
  3. **Scope**: <https://api.businesscentral.dynamics.com/.default>
  4. **Client Authentication**: Send client credentials in body
  5. Finally, click on **Get New Access Token**.

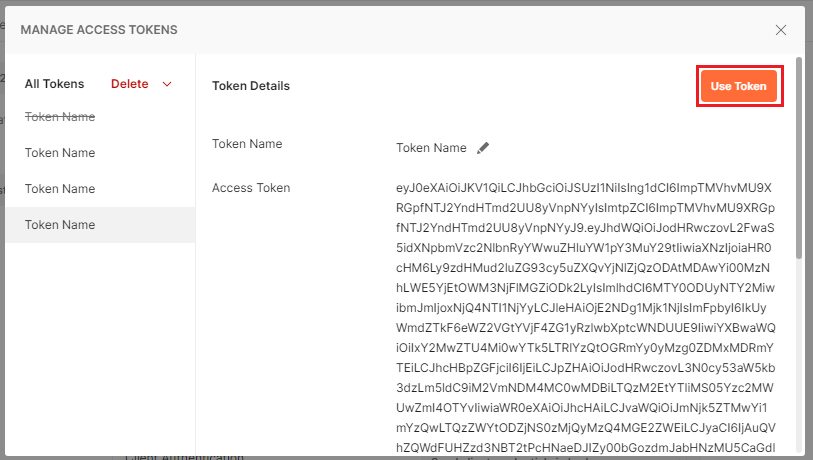
****

1. This time, we are not prompted to enter any user credential. Postman just authenticates straightaway.

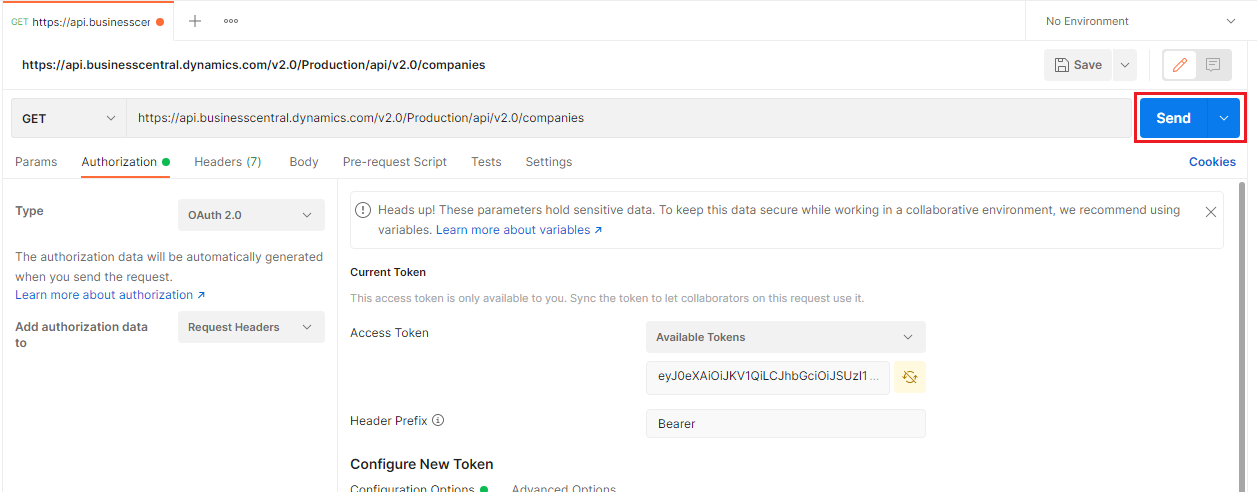
Graphical user interface, text, application

Description automatically generated

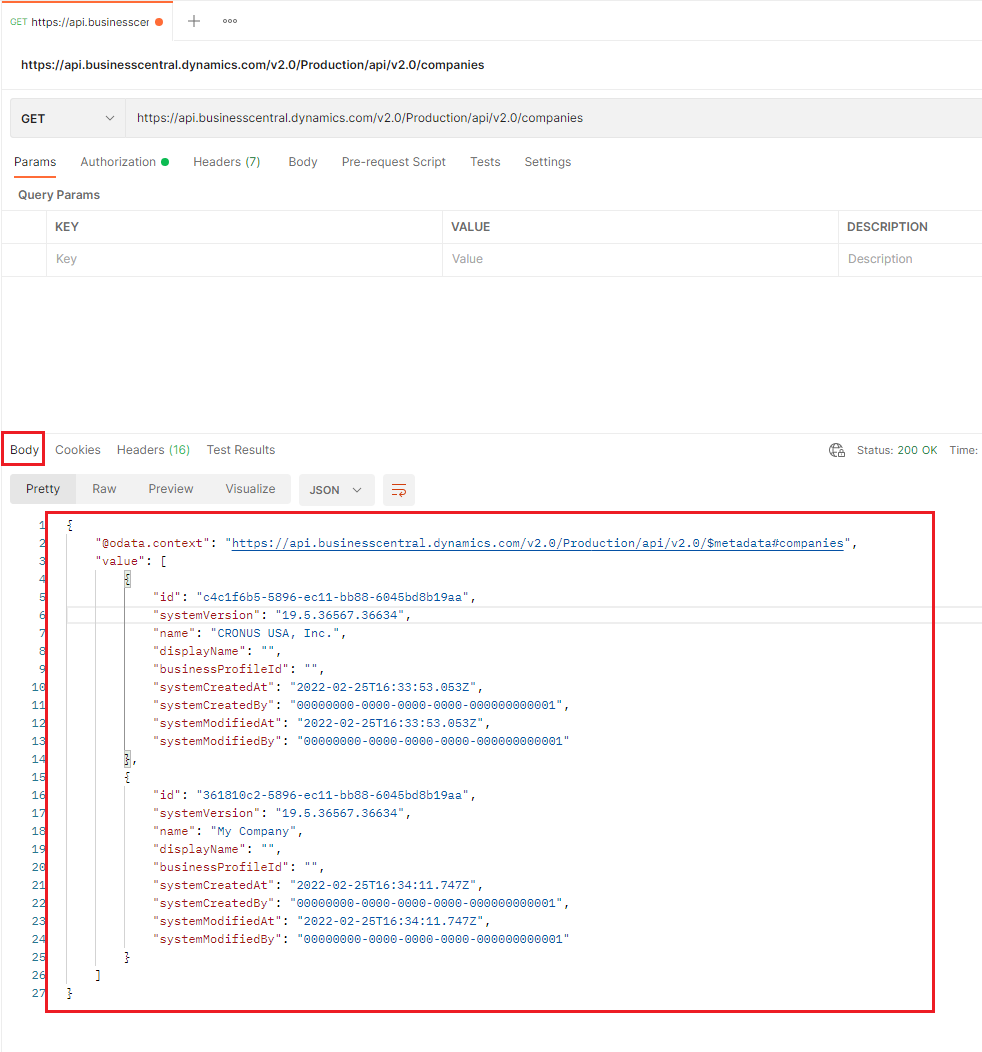
1. Click on **Use Token** button

****

1. Then click on Send button.

****

1. Result is displayed in **Body** tab

****