



WHITE PAPER

OAuth AUTHENTICATION IN CONNECTION SETUP

This document contains information about the OAuth authentication functionality in TRIMIT 23.1 for Microsoft Dynamics 365 Business Central 2023, Wave 1 (W1).

Version: 23.1
Date: 13-07-2023

CONTENTS

Introduction.....	1
Setup.....	2
Using OAuth when communication with TRIMIT.....	2
OAuth 2.0 S2S with Remote Replication.....	4
App Registration.....	5
BC connection Setup in Modelyn Admin	11
Connection setup.....	11
Important note.....	13
Further reading.....	14

INTRODUCTION

Using OAuth 2.0 (Service-to-Service) for communicating with TRIMIT for Business Central from our TRIMIT Portals or with the remote **Replication** functionality.

This new Authentication Type is demanded when working in Cloud environments, and can be used, but is not demanded in On-premises environments, where no changes to authentication methods are necessary at this time.

Service-to-Service means that the login occurs silently without any user intervention (no pop-ups), only using the **Client ID** and the **Client Secret**.

The functionality described is the functionality as of **TRIMIT 23.1 for Business Central W1 BC22.X**.

The pictures in this White Paper are based on the database for **TRIMIT 23.1**, which is based on Microsoft Dynamics 365 Business Central 2023 Release Wave 1, in the demo company **CRONUS TRIMIT W1 Ltd.** (based on CRONUS International Ltd. of Microsoft Dynamics 365 Business Central).

SETUP

TRIMIT Modelyn supports authentication with OAuth which is a standard BC connection method from April 2022. This user guide describes the method of connection TRIMIT Portals to TRIMIT for Business Central which is configured for Azure Active Directory authentication.

USING OAUTH WHEN COMMUNICATION WITH TRIMIT

In this white paper we will assume that you have already created the application in your tenants active directory.

Information on how to do as per standard Business Central documentation can be found here:

[Using Service to Service Authentication - Business Central | Microsoft Docs](#)

And here are a few blogs, which also contain guidelines for that process:

[Service to service authentication in Business Central 18.3 – How to set up – Kauffmann @ Dynamics 365 Business Central](#)

or

[Using OAuth to connect Business Central APIs and Web Service in Postman | Dynamics 365 Lab \(yzhums.com\)](#)

The first step in TRIMIT is to register an application in BCs **Azure Active Directory Application** List which can be found via **Tell me** and click **+ New**.

NOTE

This is a standard Business Central functionality, but we want to mention it regarding the **Permission Sets** you need.

Azure Active Directory Applications: All ▾ Search + New Delete				
Client ID	Description	State		
{af30e371-ad4a-4097-88c1-5555e7ada96f}	Dynamics 365 Business Central for Virtual Tables	Disabled		
	OAuth for TRIMIT Portals	Enabled		

Create a Card for your application that needs to login to BC using OAuth 2.0 (S2S).

Azure Active Directory Application Card

OAuth for TRIMIT Portals

Grant Consent

General

Client ID: [Redacted] Extension: [Redacted]
 Description: OAuth for TRIMIT Portals App ID: {00000000-0000-0000-0000-000000000000}
 State: Enabled App Name: [Redacted]
 Contact Information: [Redacted]

User Groups

User Permission Sets Manage

Permission Set ↑	Description	Company ↑	Extension Name	Permission Scope
→ D365 BASIC ISV	Dyn. 365 Basic ISV Acc.		Base Application	System
D365 FULL ACCESS	Dynamics 365 Full access		Base Application	System
TRIMIT-BASIC	TRIMIT Basic User		TRIMIT	Tenant
TRIMIT-POR-ADMIN	TRIMIT Portals Administrator		TRIMIT	Tenant
TRIMIT-POR-BASIC	TRIMIT Portals Basic User		TRIMIT	Tenant
TRIMIT-POR-PORTALS	TRIMIT Portals User		TRIMIT	Tenant

In the **Client ID** field, enter the **Application (Client) ID** for the registered application in Azure AD. Go to section **App Registration** in this document for more details.

You can choose if you want to add **User Groups** – with their applicable Permission Sets, which might have to be updated/extended - or **User Permission Sets** that are needed to run the application and be aware that the *SUPER* Permission Set is not allowed.

We recommend however, to use the **User Permission Sets**, because you don't want to give the **User Groups** the Basic ISV and Full Access Permissions, but they are needed for the connection to our Portals by using OAuth 2.0.

Based on the Release of TRIMIT that you installed, besides the **Permission Sets** *D365 BASIC ISV* and *D365 FULL ACCESS*, it should include the following Permission Sets:

TRIMIT-BASIC, *TRIMIT-POR-BASIC*, *TRIMIT-POR-PORTALS* and *TRIMIT-POR-ADMIN*

Or

As of TRIMIT 22.2 (based on Microsoft Dynamics 365 2022, wave 2 – BC21): *TRM-POR-BASIC* and *TRM-POR-ADMIN*

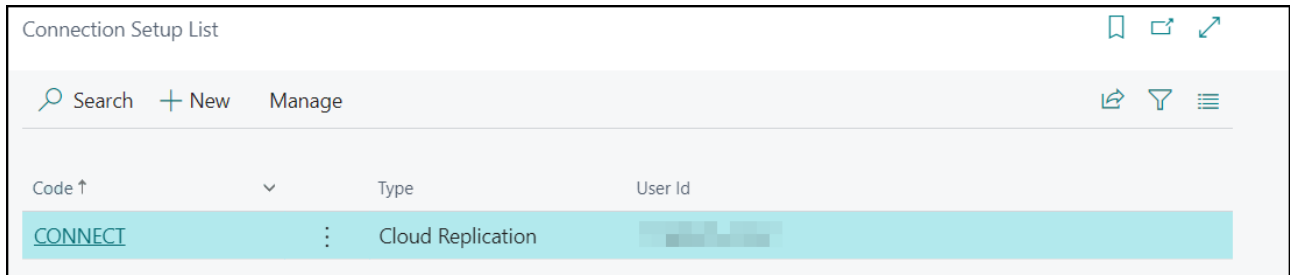
Finally click **Grant Consent**, which will show a webpage with permission information, which you will need to allow the application to be used. This is a onetime process.

Keep in mind that you also need to fill the necessary settings in Modelyn itself.

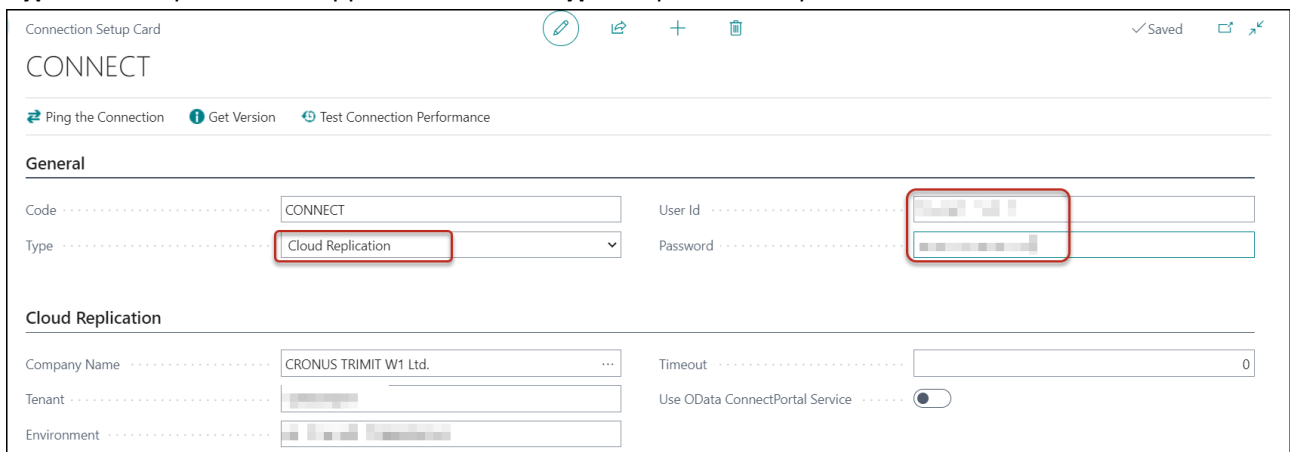
OAUTH 2.0 S2S WITH REMOTE REPLICATION

We added specific functionality regarding our Replication functionality; especially if you want to replicate data from one database to another database.

In the **Connection Setup** List (via **Tell me**), click **+ New** to create a new Connection with the appropriate settings.



For use with the remote Replication, you will also need to fill the **Connection Setup** Card, with the new **Type Cloud Replication** as opposed to the old **Type On-premises Replication**.

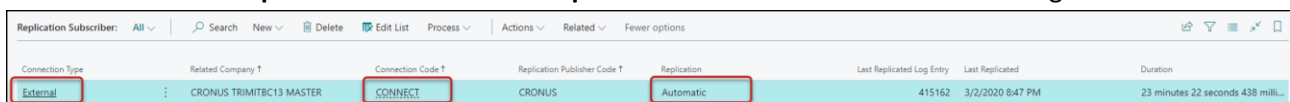


Fill the **Connection Setup** with the correct information of the other tenant, which participates in the remote replication.

You need to enter your new **Client Id** and **Client Secret** in the fields **User Id** and **Password**.

This Connection will then use an **Azure Active Directory Application** registration to login on the other tenant (see above on how to create this on the other tenant).

This **Connection Setup** can now be used in a **Replication Subscriber** for external exchange of data. I.e.:



Connection Type	Related Company	Connection Code	Replication Publisher Code	Replication	Last Replicated Log Entry	Last Replicated	Duration
External	CRONUS TRIMITBC13 MASTER	CONNECT	CRONUS	Automatic	415162	3/2/2020 8:47 PM	23 minutes 22 seconds 438 milli...

If you have any question or need help: ask partnersupport@trimit.com (previously known as service@trimit.com)

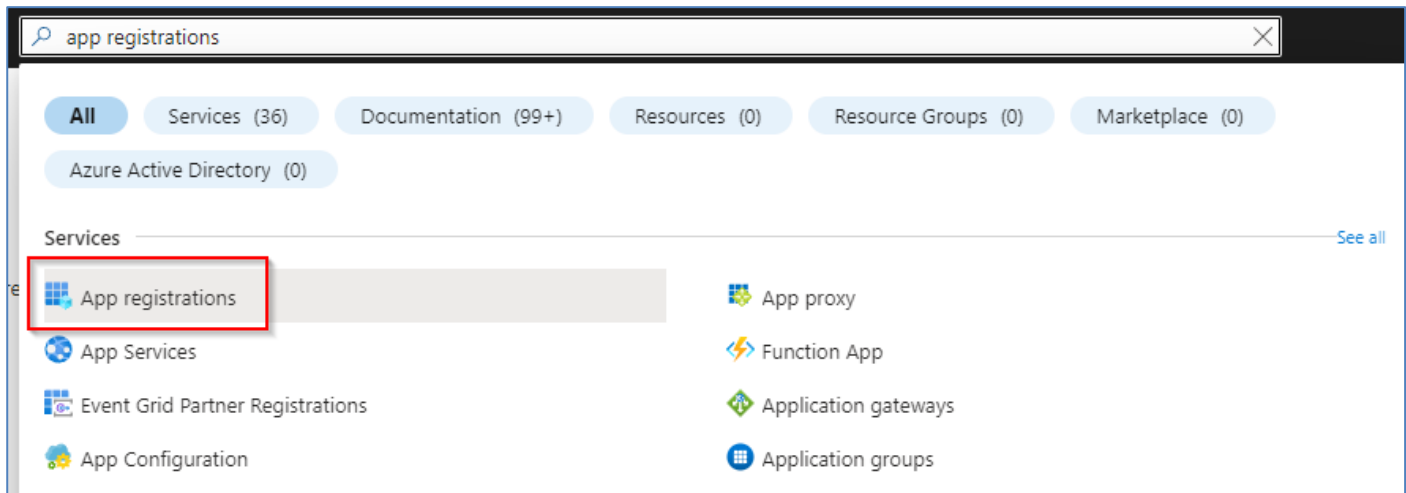
APP REGISTRATION

Prerequisites:

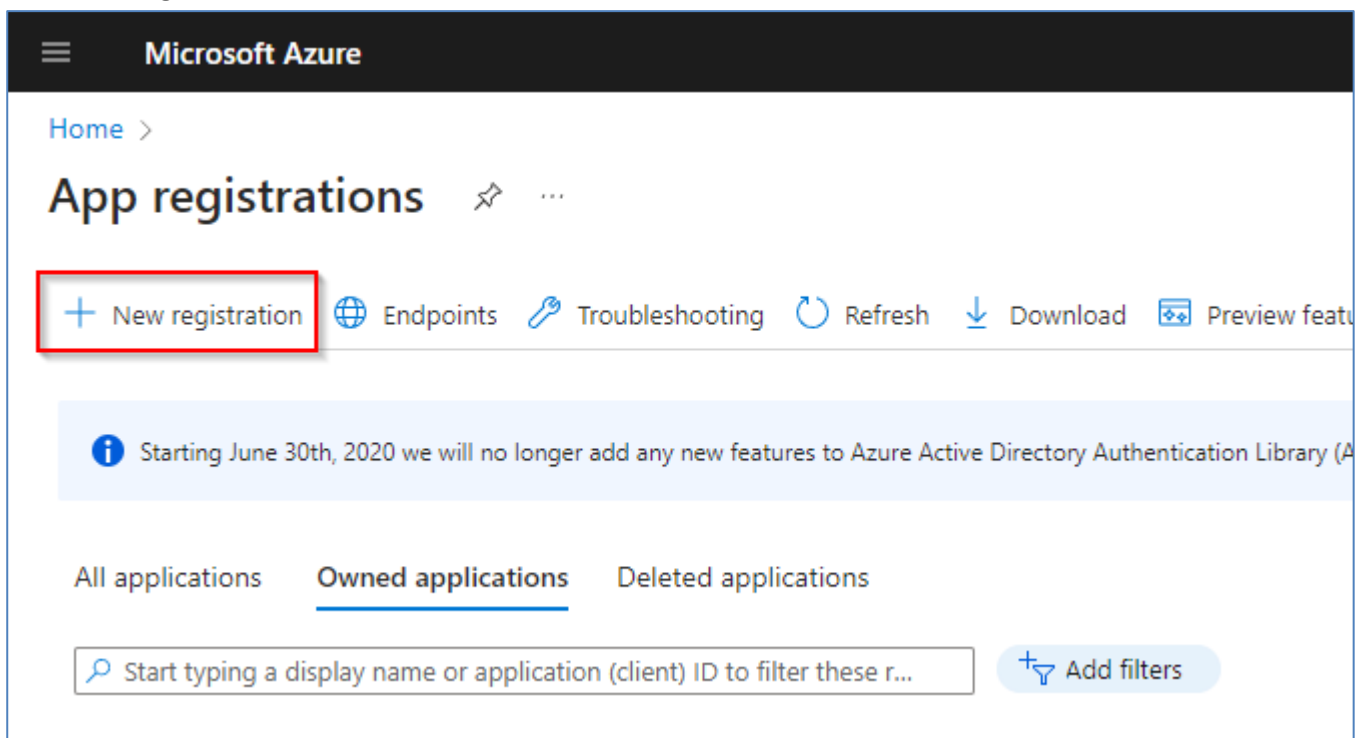
- Account in customers Azure Active Directory that has the Application Administrator Role (not partner/CSP user)
- Existing running Business Central tenant

Go to <https://portal.azure.com/>, log in using the account with the above role.

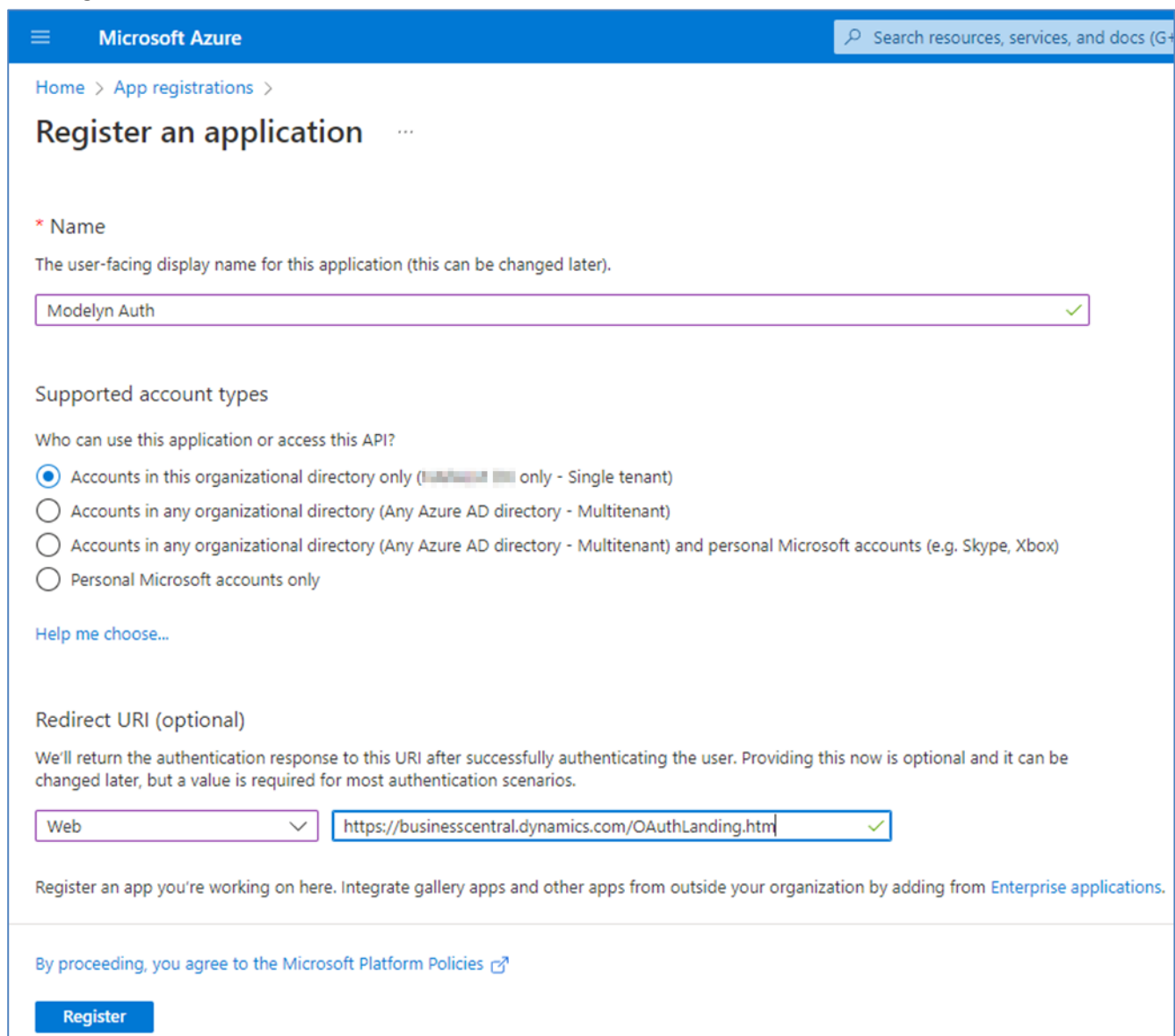
In the search box at the very top of the page, put in *App Registration* and select it in the results.



Click **New Registration**



Put in a name for the registration and set Redirect URI to <https://businesscentral.dynamics.com/OAuthLanding.htm>
Click register.



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

Home > App registrations >

Register an application

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

Modelyn Auth ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory 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.

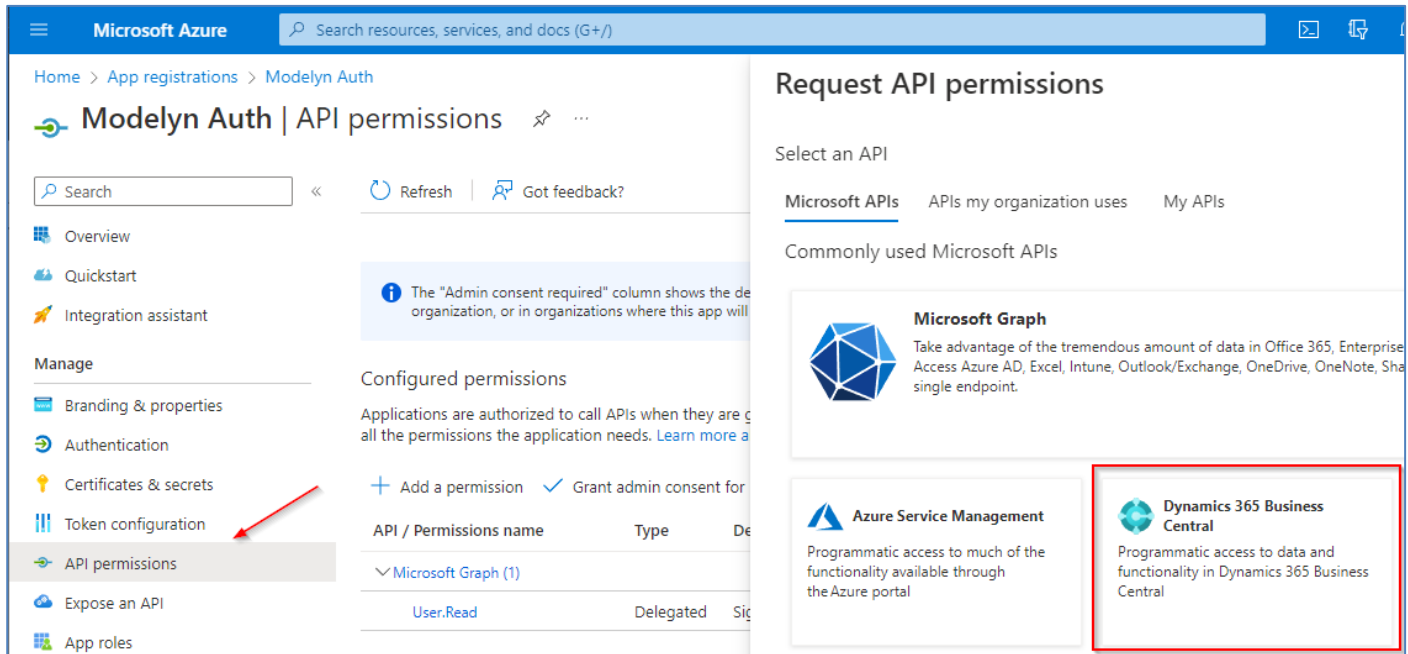
Web ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

Register

On the next page, go to API permissions, select Dynamics 365 Business Central under Microsoft APIs.



Microsoft Azure

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

Home > App registrations > Modelyn Auth

Modelyn Auth | API permissions

Search « Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

The "Admin consent required" column shows the de organization, or in organizations where this app will

Configured permissions

Applications are authorized to call APIs when they are g all the permissions the application needs. [Learn more a](#)

+ Add a permission ✓ Grant admin consent for

API / Permissions name	Type	De
Microsoft Graph (1)		
User.Read	Delegated	Sig

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, Sha single endpoint.



Azure Service Management

Programmatic access to much of the functionality available through the Azure portal



Dynamics 365 Business Central

Programmatic access to data and functionality in Dynamics 365 Business Central

Select **Application permissions** and tick **app_access** and **API.ReadWrite.All**. Click **Add permissions**.

[All APIs](#)



Dynamics 365 Business Central
<https://dynamics.microsoft.com/business-central/overview/>
[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.

Select permissions
expand all

Permission	Admin consent required
Other permissions (1) ☒ app_access ⓘ Access according to the application's permissions in Dynamics 365 Business Central	Yes
AdminCenter ☐ AdminCenter.ReadWrite.All ⓘ Full access to Admin Center API	Yes
API (1) ☒ API.ReadWrite.All ⓘ Full access to web services API	Yes
Automation ☐ Automation.ReadWrite.All ⓘ Full access to automation	Yes

Add permissions

Discard

You will be brought back to the permissions overview, click **Grant admin for [CUSTOMER NAME]**.

If the Grant option is greyed out, the user account is missing the *Application Administrator* role in Azure Active Directory.

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](#)

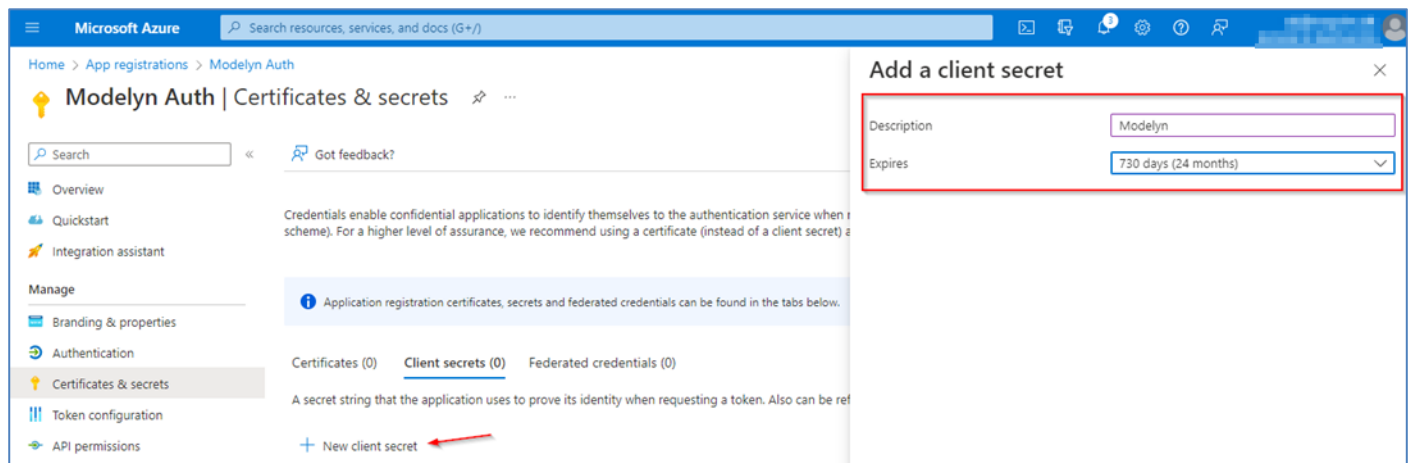
+ Add a permission ✓ Grant admin consent for [redacted]

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Dynamics 365 Business Central (2)				...
API.ReadWrite.All	Application	Full access to web services API	Yes	⚠ Not granted for [redacted] ...
app_access	Application	Access according to the application's permissions in Dyna...	Yes	⚠ Not granted for [redacted] ...
▼ Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...

To set up the *Client Secret*, go to **Certificates and secrets**, click **New client secret** in the **Client secrets** section. Give it a description and select an appropriate lifetime for the secret.

NOTE

When client secret expires, it will no longer work, so some sort of renewal process will have to be handled manually.



Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations > Modelyn Auth

Modelyn Auth | Certificates & secrets

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be ref

+ New client secret

Add a client secret

Description: Modelyn

Expires: 730 days (24 months)

After adding the client secret, it will be shown in the **Client secrets** overview for a short time, click the **copy to clipboard** icon to get the whole value. It is then used by the connecting party, for example Modelyn/Portals (**User Password/Client Secret** field in *System/Setup/Connections* in Modelyn admin).

Certificates (0)
Client secrets (1)
Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
Modelyn	1/18/2025		

The last pieces of information needed is shown at the **Overview**. **Application ID** and **Directory ID** are needed for Service to Service communication.

Microsoft Azure

Home > App registrations >


Modelyn Auth

Delete
Endpoints
Preview features

Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication

Essentials
Display name : [Modelyn Auth](#)
Application (client) ID : [11f30041-2-c104-4f22-8d0f-af980041-1c04](#)
Object ID : [228104f6-2d91-46c2-b0d1-288807914741](#)
Directory (tenant) ID : [11f30041-2189-4171-8a22-440432764114](#)
Supported account types : [My organization only](#)

To use this new App registration, we need to give it permissions in Business Central. Search for **Azure** in the BC webclient, and select **Azure Active Directory Application**.

In **Client ID**, put in the **Application ID** from above, select **Enabled** in **State** and confirm you want to add a user. In the example below is the permissions needed for CPO integration, here you need to either create a custom permission set for the integration, or select premade permissions.

When done, click **Grant Consent**. It will ask for which user to grant consent with, select the user used to create the App registration in Azure Active Directory.

Directory (tenant) ID is used by the connecting party, for example Modelyn/Portals (**Tenant Id** field in **System/Setup/Connections** in Modelyn admin).

Azure Active Directory Application Card

CPO Auth

Grant Consent | More options

General

Client ID	[REDACTED]	Extension	
Description	CPO Auth	App ID	{00000000-0000-0000-0000-000000000000}
State	Enabled ▾	App Name	
Contact Information		User information	
		User ID	{5ffd1fc5-59ba-4d55-90d2-c2702ce added}
		User Name	CPO AUTH 1

You must set the State field to Disabled before you can make changes to this app.

User Groups >

User Permission Sets | Manage

Permission Set ↑	Description	Company ↑	Extension Name	Permission Scope
→ D365 BASIC	Dynamics 365 Basic access		Base Application	System
D365 CUSTOMER, ED...	Dynamics 365 Create cus...		Base Application	System
D365 ITEM, EDIT	Dynamics 365 Create items		Base Application	System
D365 PURCH DOC, E...	Dyn. 365 Create purch. d...		Base Application	System
D365 SALES DOC, ED...	Dynamics 365 Create sale...		Base Application	System
TRM-API	TRIMIT API Tables		TRIMIT	System
TRM-POR-BASIC	TRIMIT Portal Basic		TRIMIT	System
TRM-PRODUCTION	TRIMIT Production		TRIMIT	System

BC CONNECTION SETUP IN MODELYN ADMIN

This chapter contains information about filling out the BC connection section in Modelyn admin when OAuth authentication type should be used. Available from portals version **TRIMIT BC Portals-JAN22-004-2022-06-22** and Modelyn version **7.1.335** and TRIMIT 21.2.

CONNECTION SETUP

Example of the OAuth BC connection in Modelyn:

External Data	
Interface Dynamics NAV: Web Service	Server Name api.businesscentral.dynamics.com
Security Method Azure AD	Instance Name SandboxPortal
Server Port 443	Tenant Id 57bc045c-94e4-4942-b850-
User/Client Id da8bd13b-5daf-4b70-9381-5	User Password / Client Secret CHr7Q~.qCdSg04JgaH1CY~tW1r
Company Name CRONUS TRIMIT Portal Test	Timeout 30

GET COMPANIES

DESCRIPTION OF THE FIELDS

Interface

Dynamics NAV: Web service

Server Name

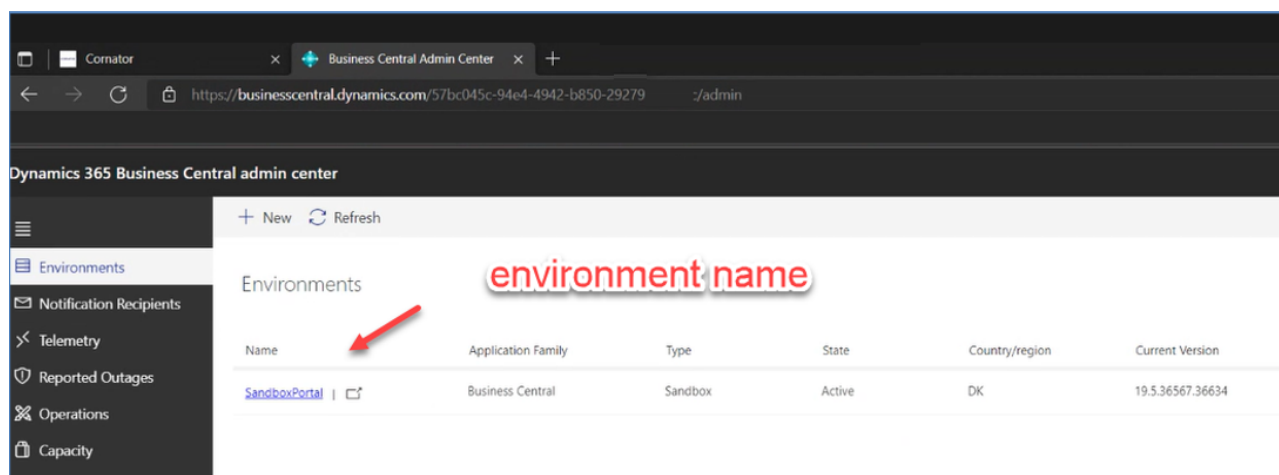
Always the same value, i.e. "api.businesscentral.dynamics.com"

Security Method

Use value "Azure AD" for OAuth authentication type

Instance Name

Also known as "environment name", can be seen inside Dynamics 365 Business Central admin center, under Environments



Server Port

443 for OAuth (7047 for webservice key, will be deprecated)

Tenant ID

Is a GUID value. Use the value from **Directory (tenant) ID** field on the Overview page in the App Registration section, see image above on page 10

User/Client ID

Is a GUID value. Use the value from **Directory (client) ID** field on the Overview page in the App Registration section, see image above on page 10

User Password/Client Secret

Use the value from **Value** field on the **Certificates & Secrets** page in the App Registration section, see image above on page 10

Company Name

Company name in TRIMIT Business Central

IMPORTANT NOTE

Regional setting (language, culture) should be the same on the user and on the service. Though there can be differences in setup of the Business Central On-Premises and in Cloud.

FURTHER READING

1. Microsoft documentation:
<https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/webservices/authenticate-web-services-using-oauth>
2. Here are a guide on how to do OAuth setup in AAD and BC from a third party blog:
[Service to service authentication in Business Central 18.3 – How to set up – Kauffmann @ Dynamics 365 Business Central](#)