DYNAVISION

Documentation:
Advanced Sync

Document version: 23.0.11

Date: 13/05/2024

Author: Dynavision Product Team

info@dynavision.be

T. +32 9 329 93 06

1 Introduction

Welcome to the official manual of the Dynavision Advanced Sync module.

This extension provides functionalities for syncing information between Business Central and another endpoint.

This manual is currently a work in progress and will be made available soon.

2 Installation

2.1 Extension

The Dynavision Advanced Sync module is a separate Business Central extension.

1. Choose the search icon, enter **Extension Management**, and then choose the related link.
2. Choose **Manage** in the Action bar on the page and choose action **Extension Marketplace**.
3. In the search bar, enter **Dynavision Advanced Sync** and install this app.

2.1.1 Dependencies (dependencies)

The Dynavision Advanced Sync module has dependencies to other modules. Those modules are automatically installed when the Dynavision Advanced Sync extension is installed.

3 Configuration

3.1 Setup Service-to-Service Authentication

Service-to-Service authentication is used in scenarios where there is no user interaction required. This authentication enables access to API's using the identity of an application instead of a user.
In order to set up this authentication, the following steps need to be performed:

1. Create an App Registration in Azure.
2. Create an AAD Application in Business Central and grant consent.

When it comes to licensing, this authentication method also requires an additional license:

If an application connects to Business Central with a single account, then that's considered multiplexing. In itself, this is not prohibited. However, it does not reduce the number of required licenses. All users accessing Business Central need to be properly licensed. No matter if they access Business Central with their own credentials or by sharing a single user.

See the following blog for more info about licensing.

3.1.1 Create App Registration

1. Navigate to the Azure portal.
2. Search and open the **App Registrations** page.
3. Choose the action **New Registration**.
4. Choose one of the following supported account types:
    a. Accounts in this organizational directory only ([organization] – Single tenant) : Select if the external application will only be used inside your organization.
    b. Accounts in any organizational directory (Any Azure AD directory – Multitenant) : Select if other organizations should access the external application.
5. Enter the following **Redirect URL**:
   https://businesscentral.dynamics.com/OAuthLanding.htm and select type **web**.
6. Choose the action **Register** to create the application.
7. Assign the correct permissions to the application.
    a. Open the created application and navigate to **API Permissions**, in the navigation pane.
    b. Choose the action **Add a permission** and select the **Dynamics 365 Business Central** API.
    c. Select **Application Permissions** (not delegated permissions) when asked for the type of permissions to configure.
    d. Check the **API.ReadWrite.All** permission.
    e. Choose the action **Add permissions**.
    f. Select the **API.Readwrite.All** permission and choose **Grant admin consent for [organization]**.

8. Create a client secret.
    a. Navigate to **Certification & secrets** in the app registration.
    b. Choose the action **New client secret**.
    c. Enter a **Description** and select an **Expiration period**.
    d. Choose **Add**.
    e. Copy the Value and store somewhere safely. This will be needed later to perform the API calls.

3.1.2 Create an AAD application in Business Central and grant consent

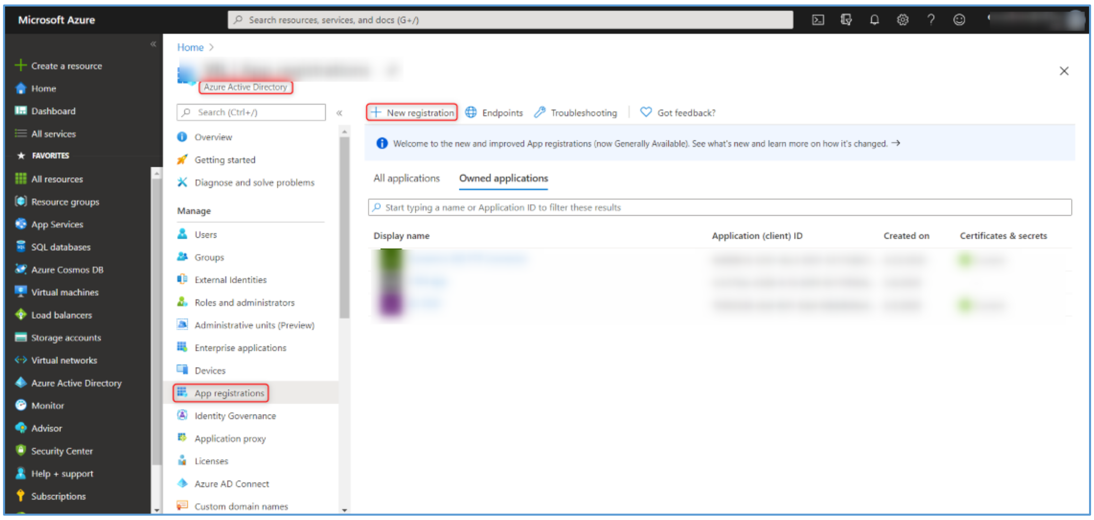
1. Navigate to the page **Microsoft Entra Applications** in Business Central.
2. Choose the action **New**.
3. Fill in the **Client ID**. This can be found on the Overview page of the Azure App Registration, in the field Application (Client) ID.
4. Choose the action **Grant Consent**.
5. Enter the **Login Credentials** in the login page that is shown. Only users with the following permissions will be able to login to grant consent.
    a. Global Administrator,
    b. Application Administrator, and
    c. Cloud Application Administrator.
6. **Accept** the request permissions.
7. Add the system permission **D365 Automation**. This permission set included the necessary rights for the table and table data.
8. Add a permission set that exposes the required API pages. *Example given: in case of the Dynavision Message API, add the ESCA CORE, EDIT permission set.*
   ***Remark**: it is important to add the **minimum permissions required for the scenario to work**. See the following resources for more info:*
    a. *https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/automation-apis-using-s2s-authentication#task-2-set-up-the-azure-ad-application-in-*
    b. *https://www.kauffmann.nl/2021/07/02/service-to-service-authentication-in-business-central-18-3-usage-and-license-terms/*

3.2 Authentication – User used for access to API

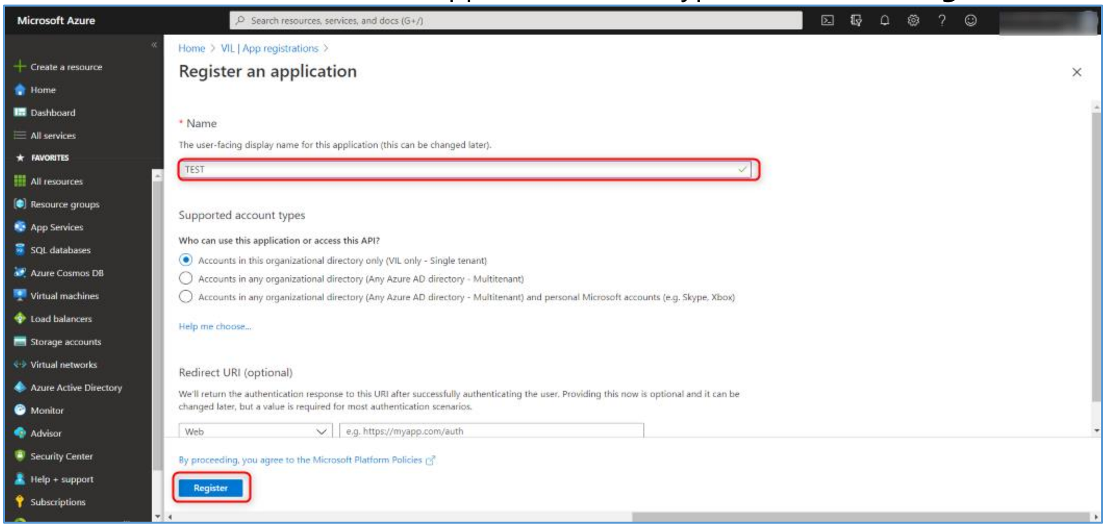
3.2.1 Access Token

For the OAuth authentication, an Access Token needs to be generated. This can be done by running through the following steps.

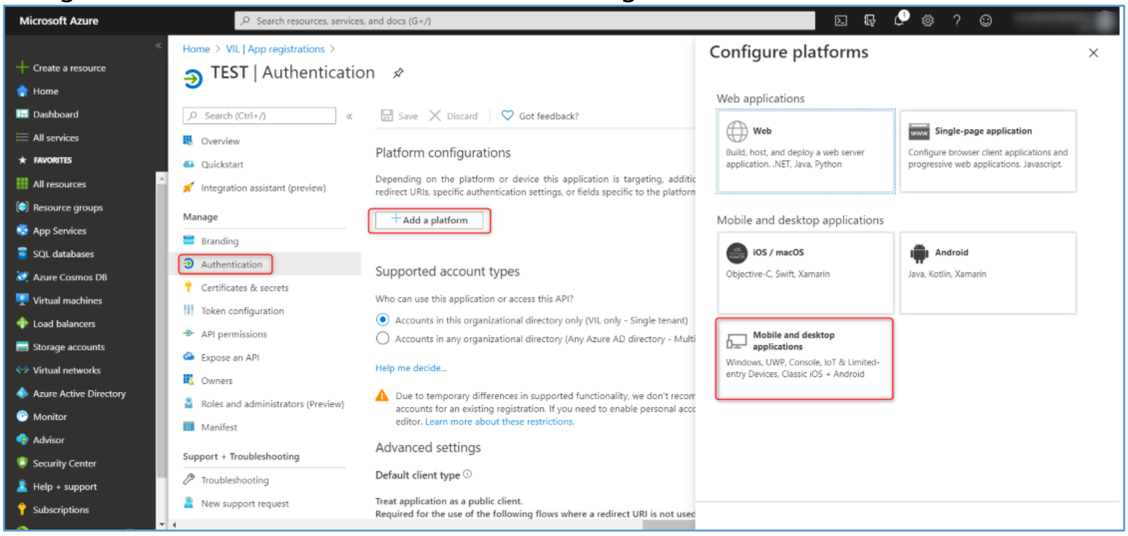
1. Navigate to the [Azure Portal]() with an AD-user.
2. Register a new application in the **App Registrations** page, which can be found in the navigation pane.



3. Fill in the Name and choose the supported account types and choose **Register**.

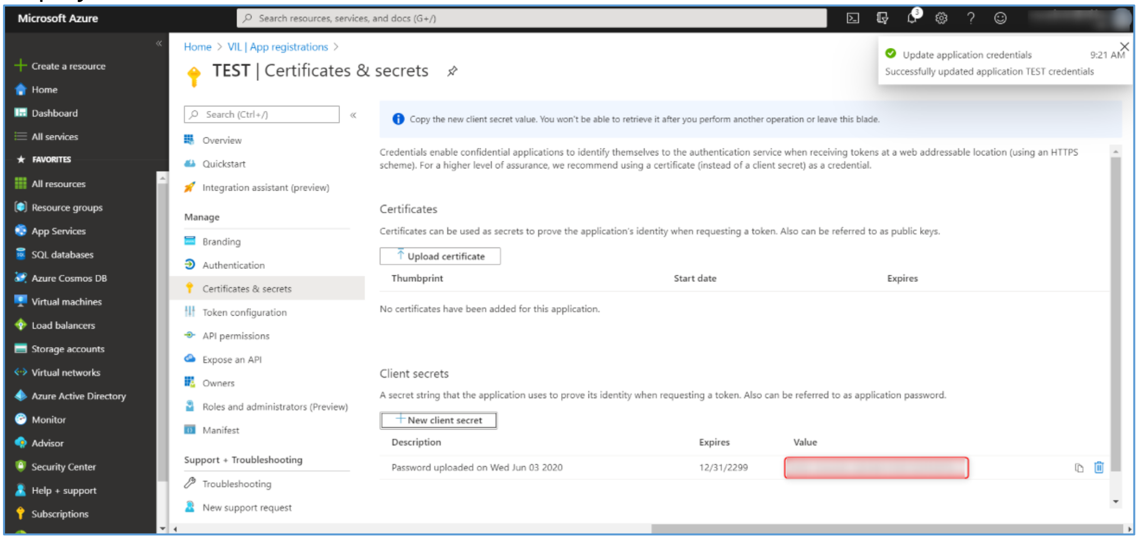


4. Copy the **Application (Client) ID**, and save this information for later use.
5. Navigate to the Tab **Authentication**, in the navigation menu and add a Platform.



6. Copy the **Redirect URL** and save this information for later use.
7. Navigate to the Tab **Certificates & secrets**.
8. Create a **New Client Secret**. This is not needed when a *mobile and desktop application* is created as platform, but for other platforms, it can be possible that this

Client Secret is needed. Save the secret immediately, because this will only be displayed once.



3.2.2 Authentication Setup

1. Choose the search icon, enter **Authentication Setup**, and then choose the related link.
2. Choose the action **New**, to create a new Authentication Setup.
3. Fill in the information needed according to the **Authorization Type**.
   a. **Authorization Type: Basic**
      i. **Web Service Username**
         Specifies the Web Service Username.
      ii. **Web Service Access Key**
         Specifies the Web Service Access Key.
   b. **Authorization Type: OAuth2 & Business Central OAuth2**
      i. **OAuth2 Grant Type**
         Specifies the OAuth2 Grant Type.
         The options are:
         01. Client Credentials, and
         02. Authorization Code.
      ii. **Tenant**
         Specifies the tenant for which the Authentication is set up.
      iii. **Client Id**
         Specifies the Client ID. This is the ID that is copied from the Access Token Setup.
      iv. **Client Secret**
         Specifies the Client Secret. This is the Secret that is copied from the Access Token Setup.
      v. **Authentication Provider URL**
         Specifies the Authentication Provider URL. This is the URL that will be used to authenticate the communication.

vi. **Redirect URL**
Specifies the Redirect URL. This is the Redirect URL that was copied from the Azure App when creating the Access Token.

vii. **Scope**
Specifies the Scope. This is the scope that contains the API's that will be used to communicate, using the authenticated connection.

viii. **Access Token**
Specifies the Access Token. This token can be obtained by choosing the action **Get Authentication String**.

ix. **Access Token expires at**
Shows when the Access Token expires. If this is blank, a new token is requested each time. This can be updated using the action **Get authentication String**.

x. **Initialized**
Indicates if additional steps (grant consent,...) are required before the authentication setup can be used.

c. For the **Authentication Type OAuth2 and Business Central OAuth2**, the supplied information can be checked by using the action **Test Connection**.

3.3 API URL

Set up the API URL's that will be needed to fetch the correct information in the communication between Business Central and the other endpoint.

1. Choose the search icon, enter **API URL**, and then choose the related link.
2. Either add the line for the API URL manually, or choose the action **Create API URL...** to start up the wizard to create the API URL.
3. Fill in the information requested on the list page or the wizard. Below is described what is asked for in the wizard.
    a. **API Code**
    Specifies the code that will be used to identify the API URL.
    b. **Authentication Code**
    Specifies the Authentication code, used to authenticate the communication that is executed with the API URL. This has been set up in the previous section, Authentication Setup.
    c. **TenantId**
    Specifies the Tenant ID of the Business Central Tenant that will communicate with the set up API URL. The current tenant ID will be filled in by default, but can be edited if the API points to another tenant.
    d. **Environment**
    Specifies the environment in the tenant. (*Sandbox, Production, ...)*
    e. **Company Name**
    Specifies the name of the company in the tenant environment. Using the lookup function, all companies in the environment are displayed to choose from.
    f. **Page Id**
    Specifies the API Page ID. *Attention: the presumption here is that the API pages*

on both environments are the same. It is also possible to view all API pages that can be selected using the lookup functionality in the field.

g. **Page Name**
   Displays the name of the selected API Page ID.
h. **API URL**
   Displays the API URL that will be created based on the entered parameters in the setup wizard.
   Remark: if this API URL is filled in, the process has been completed successfully.

4. After filling in the information in the wizard and choosing **Finish**, the line is created for the API URL.
   a. **Source Table No.**
      Specifies the source table of the API page.
   b. **CultureInfo**
      Specifies the culture that is used to format the date values. This will be filled in with the set **Region** on the tenant.
5. Once this information is set up, this can be used in the synchronization setup.

3.4 Synchronization Setup

The setup of the tables that need to be synced and the API URL that needs to be used in order to sync the information needs to be specified in the **Synchronization setup**.

1. Choose the search icon, enter **Synchronization Setup**, and then choose the related link.
2. Fill in the information for the Synchronization.
   a. **Code**
      Specifies the code of the Synchronization Setup.
   b. **Table Caption**
      Specifies the table that is being Synchronized.
   c. **Enabled**
      Specifies if the Synchronization Setup is enabled.
   d. **Requires Context**
      Specifies if the Synchronization setup is executed via code and cannot be executed individually.
   e. **API URL Code**
      Specifies the Code of the API URL used for synchronization.
   f. **API URL**
      Specifies the API URL used for synchronization.
   g. **Operation**
      Specifies the type of operation for the synchronization.
      The options are:
      i. **Post & update**
         Information will be posted from the current environment to the other endpoint. This will create or update records.
      ii. **Post**
         Information will be posted from the current environment to the other endpoint. This will create records.

iii. **Update**
Information will be posted from the current environment to the other endpoint. This will update records.

iv. **Get: Filter**
Will fetch information from the other endpoint, using the specified **Filter** in the field **Filer**. Using the fetched information, records will be created, updated or deleted in the current environment, based on the values set in the next three columns.

h. **Insert**
Specifies if new external records are inserted locally.

i. **Modify**
Specifies if external modified records are modified locally.

j. **Delete**
Specifies if external deleted records are deleted locally.

k. **Last Synchronization On**
Specifies when the last synchronization occurred.

l. **Only Process Modified Data**
Specifies that only modified records will be processed. This requires the Modified At field to be included in the mappings when data is imported. When exporting data, the value of the Source Date Field No. is used.

m. **Skip Token**
Specifies the Skip Token, that is used for server side paging.

n. **Filter**
Specifies the filter applied to local records before sending, or applied to records when fetching information.

o. **Pre-processor**
Specifies how the records are pre-processed before they are synchronized.

p. **No. Of Templates**
Specifies the number of linked templates. These templates are applied before the post-processor is executed.

q. **Post-Processor**
Specifies how the records are pre-processed after they are synchronized.

r. **Error Message**
Specifies the error message when an error has occurred during processing.

info@dynavision.be
T. +32 9 329 93 06

3.5 Synchronization Mappings

The synchronization mappings need to be set up for the **Synchronization Setup**, in order to map the fields that are synchronized between the two endpoints.

1. Choose the action **Synchronization Mappings** on the page **Synchronization Setup**. This will open the **Synchronization Mappings** page for the selected **Synchronization Setup.**
2. Add all API Fields that need to be mapped.
    a. **API Field Name**
    Specifies the name of the field in the external API.
    b. **Enabled**
    Specifies if the mapping is enabled.
    c. **Is Master System Id**
    If enabled, this field will be used as OData key field instead of the primary key fields. This also needs to be activated when delete actions are used.
    d. **Skip field Validation**
    Specifies if the validation of the field should be skipped.
    e. **Field Caption**
    Specifies the field that needs to be mapped with the API Field.
    f. **Update Field From Response**
    Specifies if the field should be updated with the corresponding value in the API response.
    g. **Calculated Value**
    Specifies a calculated value that will be used to fill the field.
    The options are:
        i. Street,
        ii. House No.,
        iii. VAT No.,
        iv. ISO Language Code,
        v. Contact Account ID,
        vi. Feature Property Type,
        vii. Opportunity Account ID,
        viii. Opportunity Contact ID,
        ix. Opportunity Property ID,
        x. Customer default Contact ID,
        xi. Next Quotation Number,
        xii. Contact Last Name,
        xiii. Production BOM Description,
        xiv. Production BOM Unit of Measure,
        xv. Production BOM Sales Price,
        xvi. Quotation Property Value,
        xvii. Property Value,
        xviii. Ship-To Address Customer No.,
        xix. Ship-To Address Code.
    h. **Fix Value**
    Specifies a fix value that will be used to fill the field.

i. **Example Data**
   Specifies example data for the mapping.
j. **Validation Failed**
   Specifies if the example data was correctly validated. The example data validation can be triggered by choosing the action **Validate Example Data**.

info@dynavision.be
T. +32 9 329 93 06