Shipping Connector

for Microsoft Dynamics 365 Business Central

Business Central Web Services
OAuth 2.0 Configuration Guide

I. Purpose of this document

This guide will assist with configuration of Shipping Connector for use with Business Central OAuth 2.0 authentication.

OAuth 2.0 authentication is a protocol employed by the Entra/Azure Active Directory to enforce secure identification of entities that seek to interact with resources under its governance.

A complete description of OAuth 2.0 is beyond the scope of this document. (But, if you really want to geek-out here is a link for further reading).

Note: We will make an effort to keep this guide up to date however the dynamic nature of the web makes it difficult to stay in sync – so if you run into any discrepancies with this guide please point them out to us via our Support Page.

II. Prerequisites

To follow this guide, you will need administrative access to your Entra/Azure Active Directory.

III. Parts

There are two parts to this guide:

- Guide for Business Central Cloud
- Guide for Business Central OnPrem with Active Directory

Please skip to the part that is pertinent to your environment.

Guide for use with Business Central Cloud

If you use Business Central Cloud and you are reading this guide, then it is likely that web services authentication in the Shipping Connector Configuration tool is failing.

Follow these instructions to address that issue.
Please note: We are happy to help – please contact us should you need assistance.

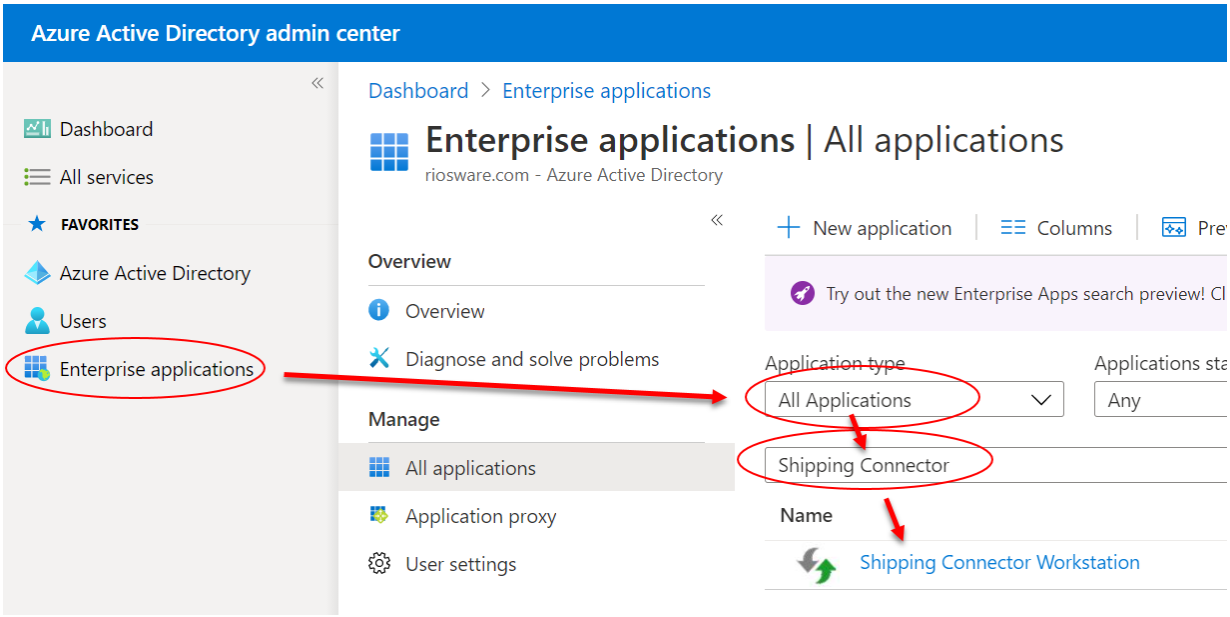
Step 1 – Add Permissions for Shipping Connector Workstation

The Shipping Connector Workstation application (running on your shipping PC) needs to synchronize shipping data with your Business Central system in the Microsoft Cloud.

To do that, a Microsoft Entra/Azure "Enterprise Application" is required.
We have already created and deployed the Enterprise Application – it is named "Shipping Connector Workstation" in the Entra/Azure Enterprise Applications directory.
(We'll use the term "Shipping Connector EA" for this going forward)

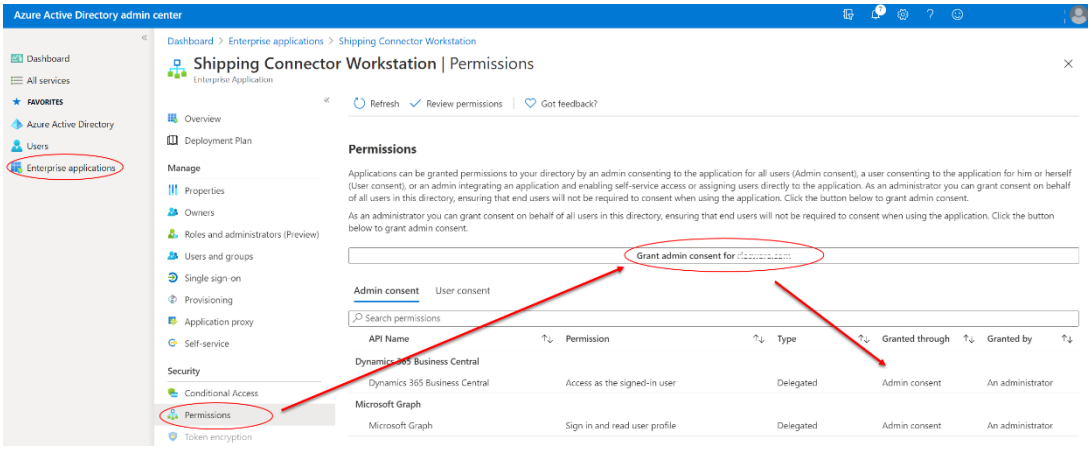
To communicate with your Business Central system, the Shipping Connector Workstation application (running on your shipping PC) uses the identity of the Shipping Connector EA. You must authorize the Shipping Connector EA to make the connection.

In the AAD console click on the Enterprise applications link, change the filter to All Applications, and search for Shipping Connector Workstation.



Click the Shipping Connector Workstation link, then select the Permissions link

Grant consent for user impersonation



That's it – you have successfully configured Active Directory to allow Shipping Connector Workstation to interact with your Business Central app.

Guide for use with Business Central OnPrem

In the case of Business Central OnPrem, configuring Azure Active Directory to allow Shipping Connector to interact with your Business Central OnPrem instance is a bit more involved.

You will need to complete these steps:

- Create a registered app entry for Business Central in Aad
- Expose an API/scope for the Business Central registered app to enable user impersonation
- Add the Shipping Connector Workstation registered app as a client app to the API/scope

Once complete, you will need to copy the following information for later use:

- The registered Application ID for the Business Central app (App ID)
- The URI given to the exposed API/scope (Scope)

Step 1 – Create an Azure Active Directory App Registration for Business Central OnPrem

Note: The intimate details of Business Central app registration in the Azure Active Directory is outside the scope of this guide. If you are a Business Central Azure Active Directory administrator this concept should be familiar to you. If you are not familiar with this concept, then you should probably defer to someone who knows this stuff…

The definitive guide for registering Business Central OnPrem in Azure Active Directory is located here: Registering Business Central On-Premises in Azure AD for Integrating with Other Services.

Please follow that guide to configure Business Central properly in Azure Active Directory.

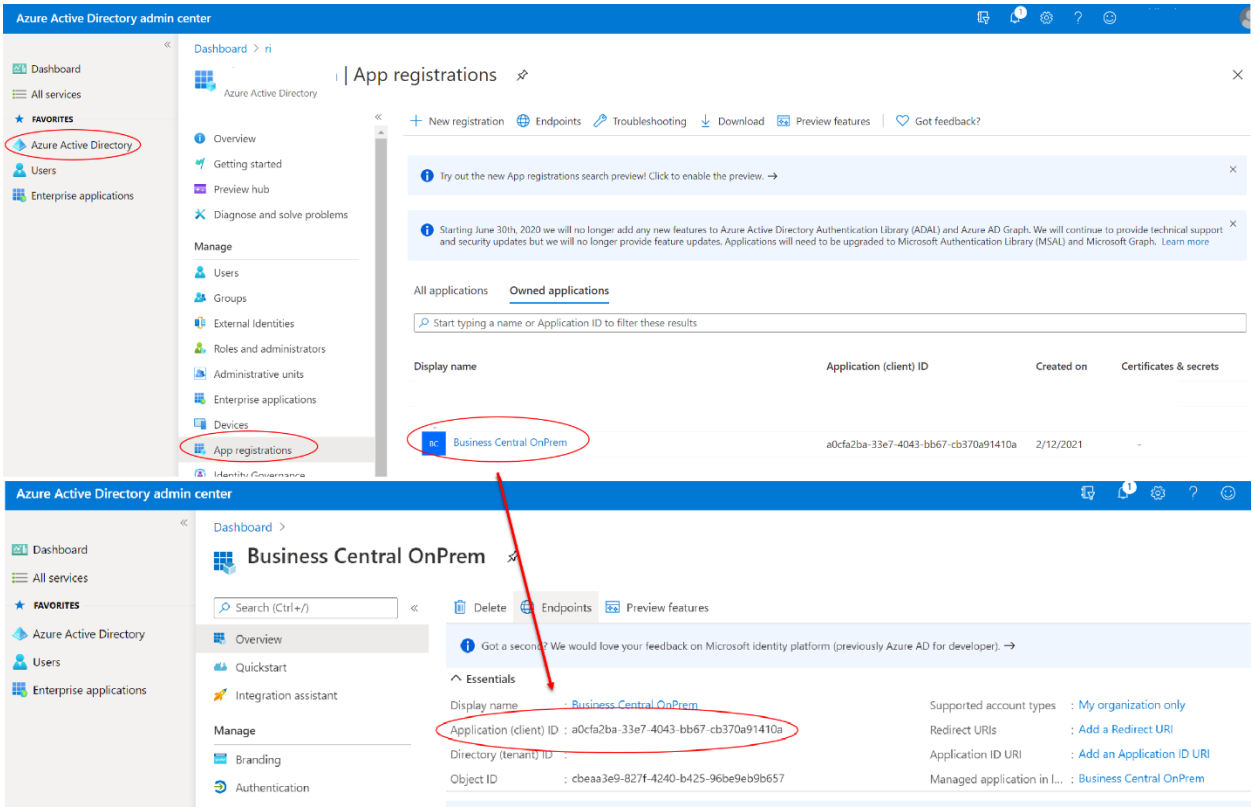
A well described example is available here:

Authenticating Business Central Users with Azure Active Directory (Sign in to Business Central On-Premises with Office 365 account) | Dynamics 365 Lab (yzhums.com)

It also provides an example of exposing an API/scope.

We will not step through the details of Business Central app registration here – we'll just assume you completed that step correctly (since if you didn't pretty much nothing else is going to work…)

Once completed you will need to retrieve the Application ID from the Aad console.



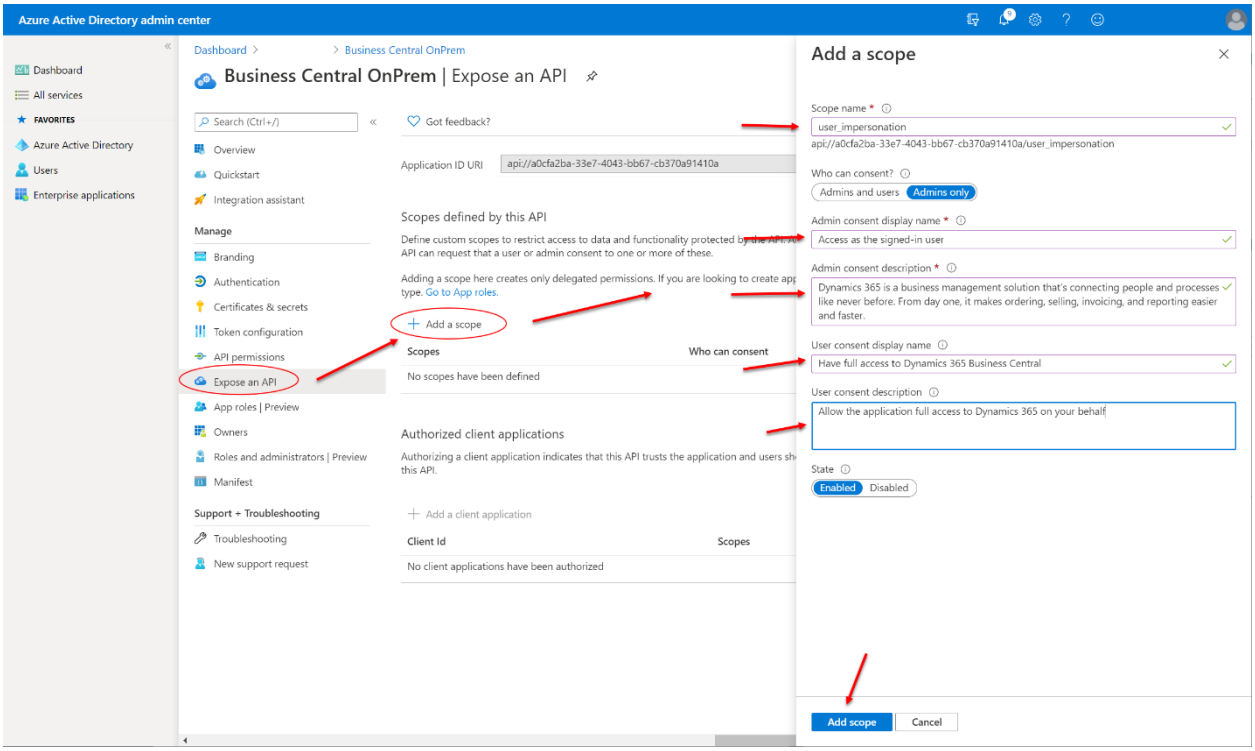
Copy the registered Application Id – we'll need it when configuring Shipping Connector Workstation.

Step 2 – Expose an API/Scope for user impersonation

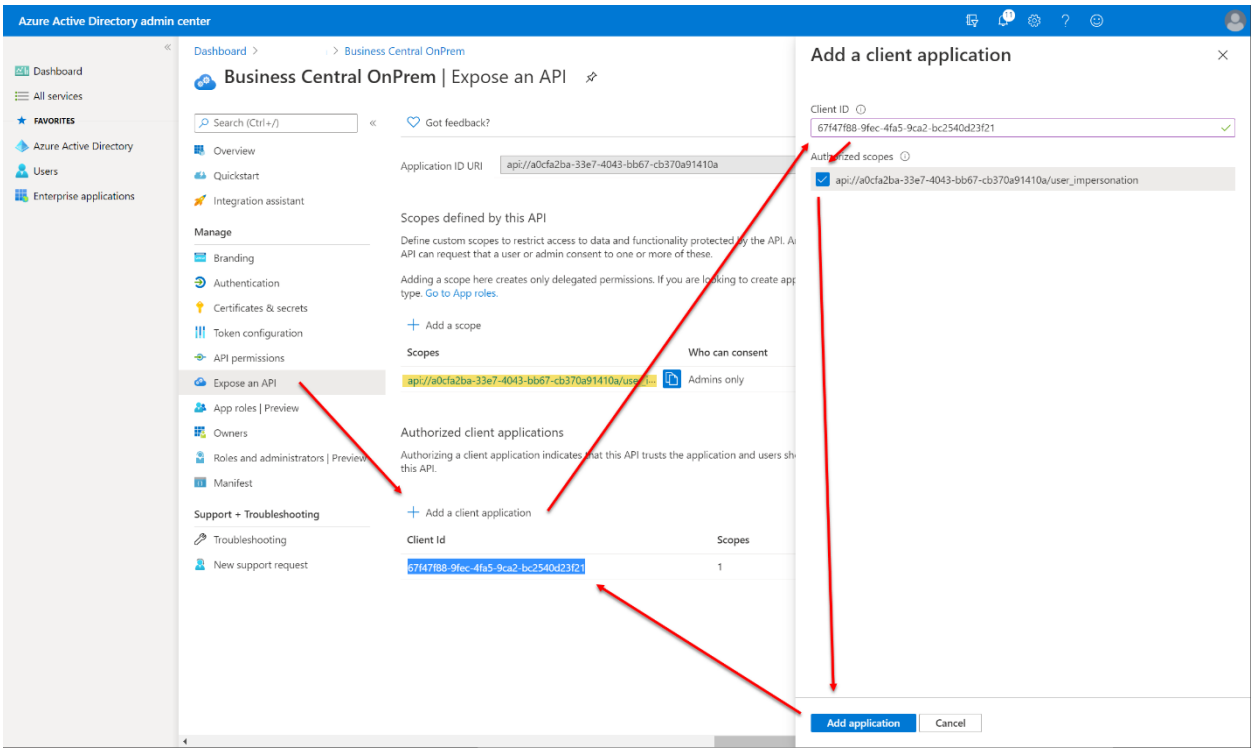
Now we need to expose an API/Scope for user impersonation (so the Shipping Connector app can access the web service as a Business Central user).

Back on the register app screen select the "Expose an API" link.

Then configure as in the following screen shot – here I have used the verbiage from the registered app for Microsoft Dynamics 365 Business Central (SaaS).



Now we will give the Shipping Connector Workstation app access to the scope.
Click the “Add a client application” link – the client application screen will display.
Enter the App ID for Shipping Connector Workstation: 67f47f88-9fec-4fa5-9ca2-bc2540d23f21



The Shipping Connector Workstation app is already defined in Azure Active Directory.
If you wish to locate it, open the Enterprize Apps list, then search All applications for “Shipping Connector Workstation”.

Now check off the user_impersonation scope – this grants access to the scope.

After clicking the “Add application” link the client registration will display.

Copy the Scope URI (the yellow highlighted value in the screen shot) – we will need it when configuring Shipping Connector Workstation.

You’re done configuring Shipping Connector in Azure Active Directory.

Note: There are many variants of the above that can be implemented to achieve the same goal. We have described a simple configuration. Experienced Aad administrators may wish to deviate from this guide per their own security considerations.

-- End of Document --