

Integration of Azure Active Directory



1. Introduction

This documentation is for administrators who want to synchronise an Azure Active Directory with DoubleClue.

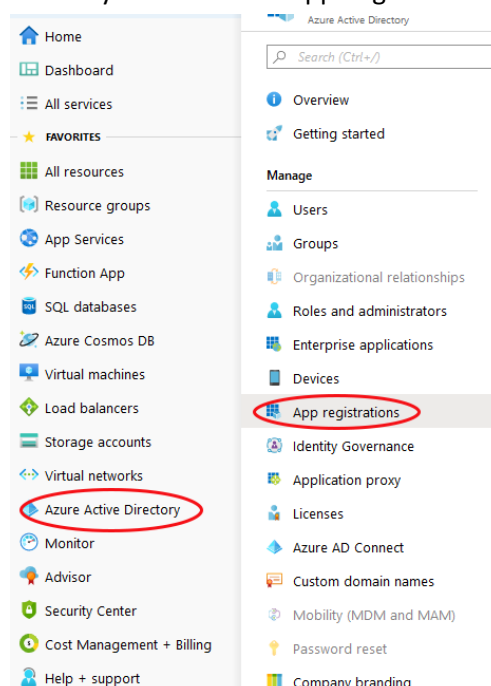
Requirements:

- DoubleClue Installation
- Azure Account

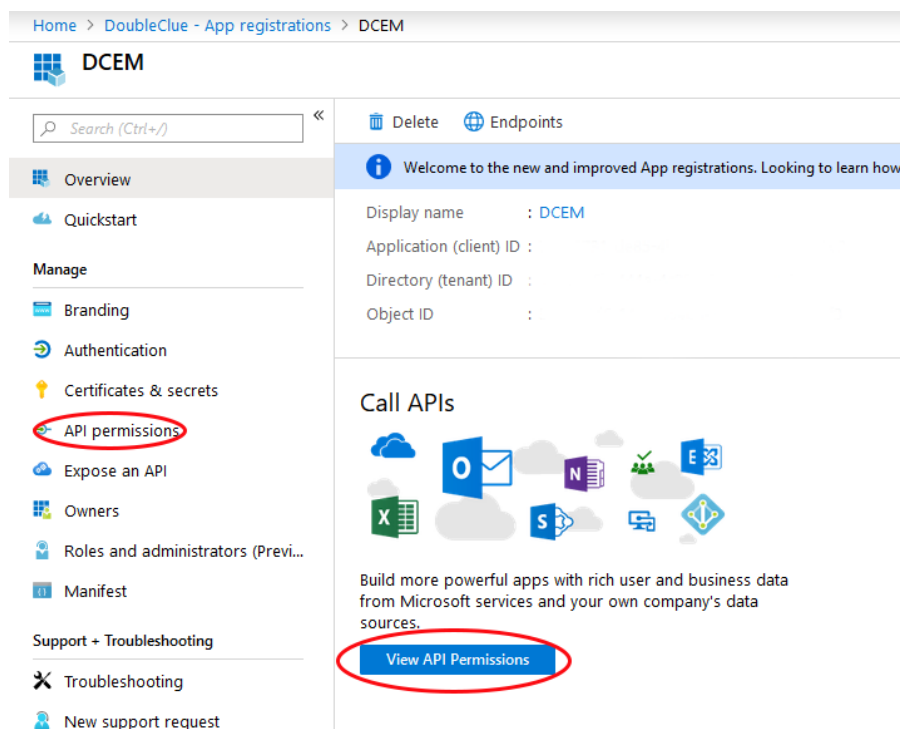
2. Setting up an Azure Application

2.1 App Registration & Configuration

1. Log into your Global Administrator account on <https://portal.azure.com>
2. Go to “Azure Active Directory” and choose “App Registrations” in the submenu.



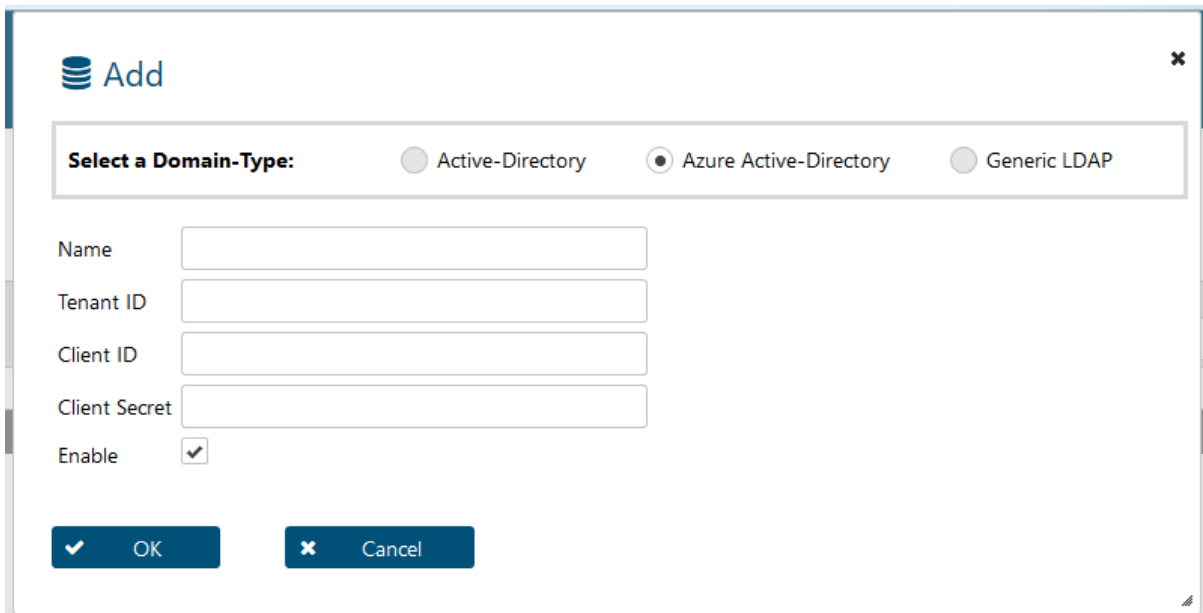
3. Click on “New registration”. If you have already registered an app you wish to use, select it instead and skip directly to step 5.
4. Give your application an easily recognisable name, eg. “DoubleClue”. Then choose the account type you want to support and click “Register”.
5. Copy the “Application (client) ID” and “Directory (tenant) ID” from the application side. Store them in a safe location – you will need them later.
6. Click on “View API Permissions” or “API Permissions” from the submenu on the left side of the app registration page.



7. Choose “Add a permission” and select “Microsoft Graph” then “Application permissions”. This will open the menu to select permissions.
8. Open the menu item “Directory” and enable “Directory.Read.All”. Then open the item “Users” and enable “User.Read.All”. Confirm the selection with the “Add Permission”-Button at the bottom of the menu.
9. Go to “Certificates & Secrets” in the submenu on the left.
10. Add a “New Client Secret” and choose an expiration time.
11. Copy the value of the client secret. Be aware that the secret is only shown once! Should it be lost, it can’t be restored and a new secret has to be defined.

2.2 Connecting with DCEM

1. Log into DCEM as an administrator.
2. Go to “Administration” in the main menu and then to the “Domain” in the sub menu.
3. Add a new Domain.
4. Choose “Azure Active-Directory” as Domain-Type.



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. Below the title bar, there is a section labeled "Select a Domain-Type:" with three radio button options: "Active-Directory", "Azure Active-Directory" (which is selected), and "Generic LDAP". Below this section are four text input fields labeled "Name", "Tenant ID", "Client ID", and "Client Secret". Below the input fields is an "Enable" checkbox, which is checked. At the bottom of the dialog, there are two buttons: "OK" with a checkmark icon and "Cancel" with an X icon.

5. Select a meaningful and easily memorable name, like the company name. Note that this name will be the prefix users will need to add to their User ID to identify themselves with DoubleClue.
6. Paste the Tenant ID and Client ID from the value you copied in step 2.1.5 in the respective fields.
7. Paste in the Client Secret from the value you copied in step 2.1.11 in the respective field.
8. Confirm the input. You now have a successfully connected your DCEM to the Azure app.