

Register TimeLog PSA with the Microsoft identity platform

This document guides you through the workflow on adding the TimeLog PSA app in your Azure Active Directory and creating the TimeLog integration credentials.

In short is the installation done in five steps

1. Add/register the TimeLog PSA app in your Azure portal.
When adding the TimeLog PSA is it important to copy the **Client secret** and **Application (client) ID** (page 6 in the attached PDF)
Both codes are to be used when establishing the connection between TimeLog and you BC installation.
2. Install the TimeLog PSA app from BC Extension Marketplace
3. Run the TimeLog PSA setup in your BC installation via Assisted setup.
Copy the **Tenant ID** and **Environment** name to be used when establishing the connection.
See page 7 in the attached PDF.
4. Enable the TimeLog PSA application in your BC installation.
5. Establish the connection between TimeLog and the BC installation.
Here, the four copied pieces of information must be used.

Bullet 1 needs access to your Azure portal

Bullet 2, 3 & 4 needs system admin. rights in the BC installation

Bullet 5 needs system admin rights in the TimeLog installation

Prerequisites:

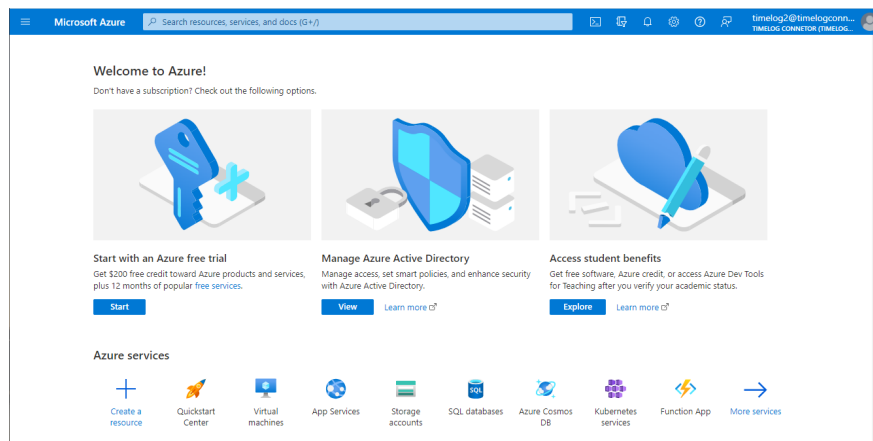
Installed MSAL .PS Powershell module.

User access need to be Global Administrator or Privileged Role Administrator

This workflow description is based on Microsoft [Quickstart: Register an application with the Microsoft identity platform](#)

1. Azure AD Application registration

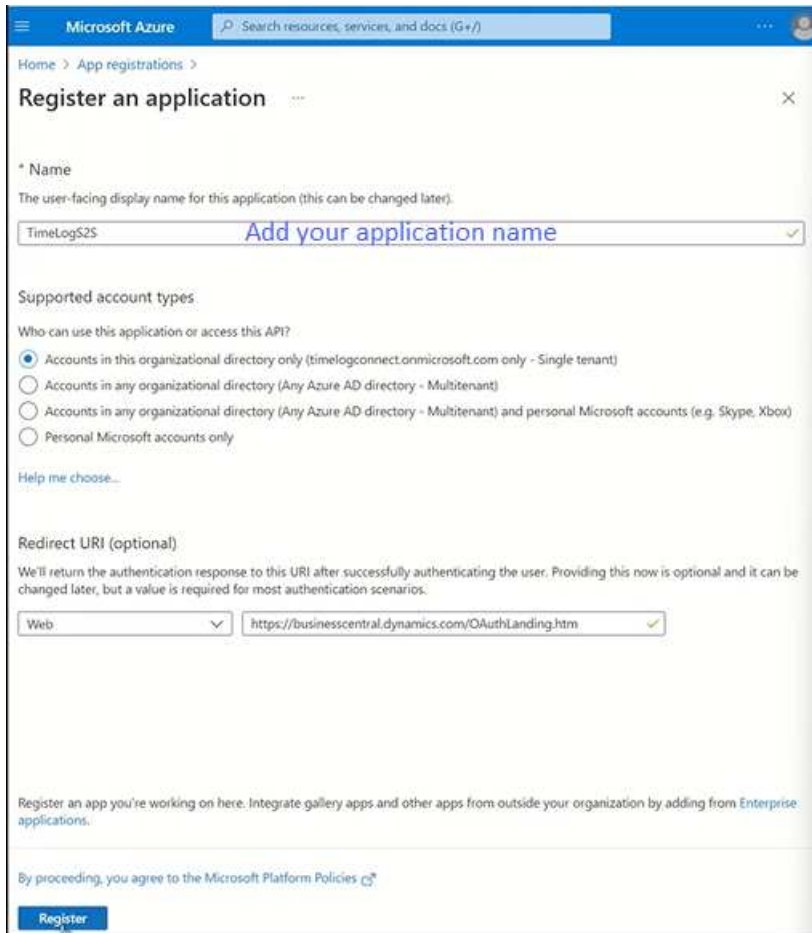
Sign into azure portal (<https://portal.azure.com>) and search on 'App registrations'



2. Register an application

Click '+ **New registration**'. Provide a '**Name**' for application, set '**Supported account types**' to "**Accounts in this organizational directory only**".

In **Redirect URI** you select **Web** and add the URL for your Business Central on-premises browser client and click '**Register**' button to add the TimeLog integration application.



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).

TimeLogS2S [Add your application name](#)

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

- Accounts in this organizational directory only (timelogconnect.onmicrosoft.com 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.

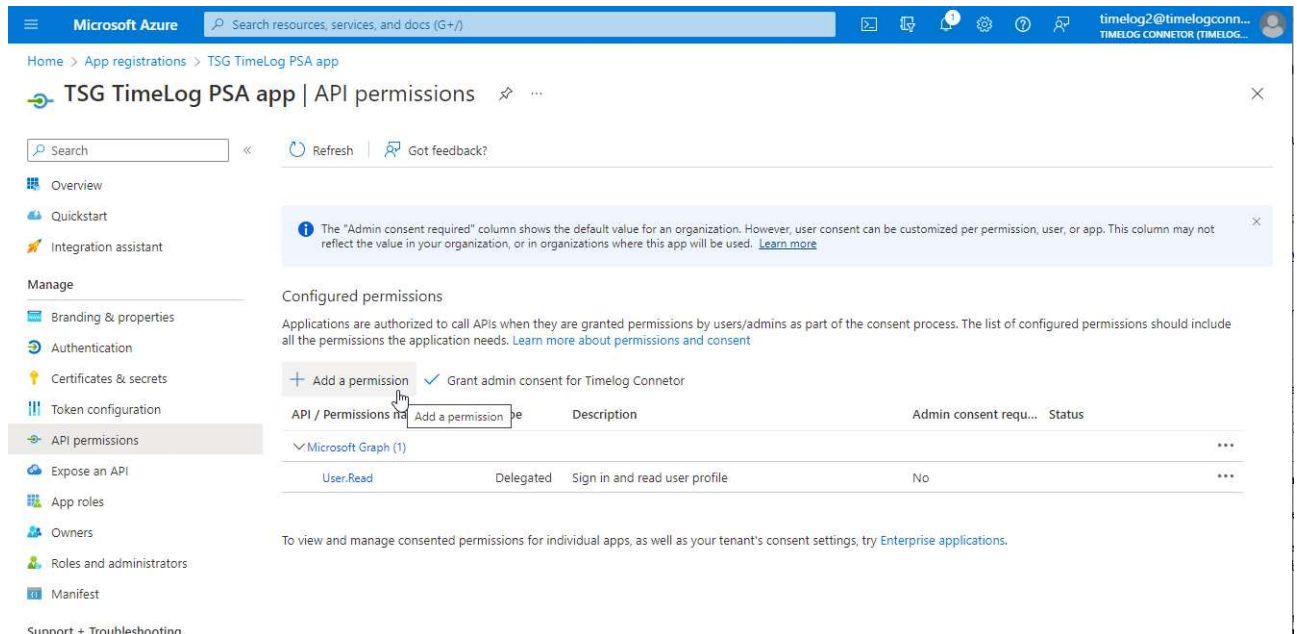
By proceeding, you agree to the [Microsoft Platform Policies](#)

[Register](#)



3. API permissions

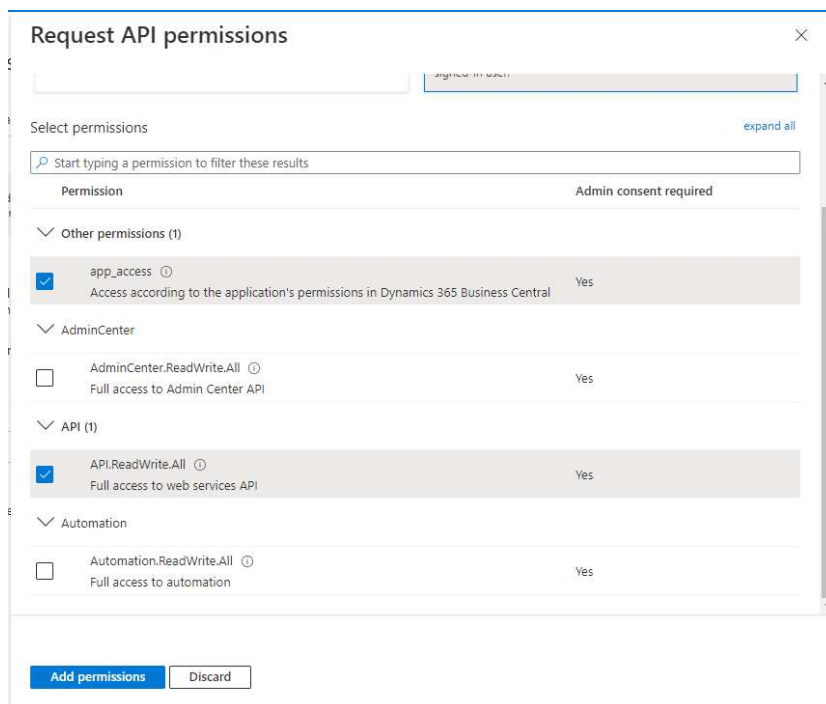
Setup API permissions for the newly created application, go to 'API permissions' and click **Add an application**:



The screenshot shows the 'API permissions' page for the 'TSG TimeLog PSA app' in the Microsoft Azure portal. The left-hand navigation pane includes sections for 'Manage' (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest) and 'Support + Troubleshooting'. The main content area is titled 'Configured permissions' and contains a table of permissions. A tooltip explains that the 'Admin consent required' column shows the default value for an organization, but user consent can be customized. The table lists one permission: 'User.Read' (Delegated) with the description 'Sign in and read user profile' and 'Admin consent required' set to 'No'. There are 'Add a permission' buttons above the table and a 'Grant admin consent for Timelog Connector' button.

In order to acquire tokens as application (used for automation APIs), click: 'Dynamics 365 Business Central' - 'Application permissions' and mark "app_access" and "API.ReadWrite.All"

Click **Add permission**



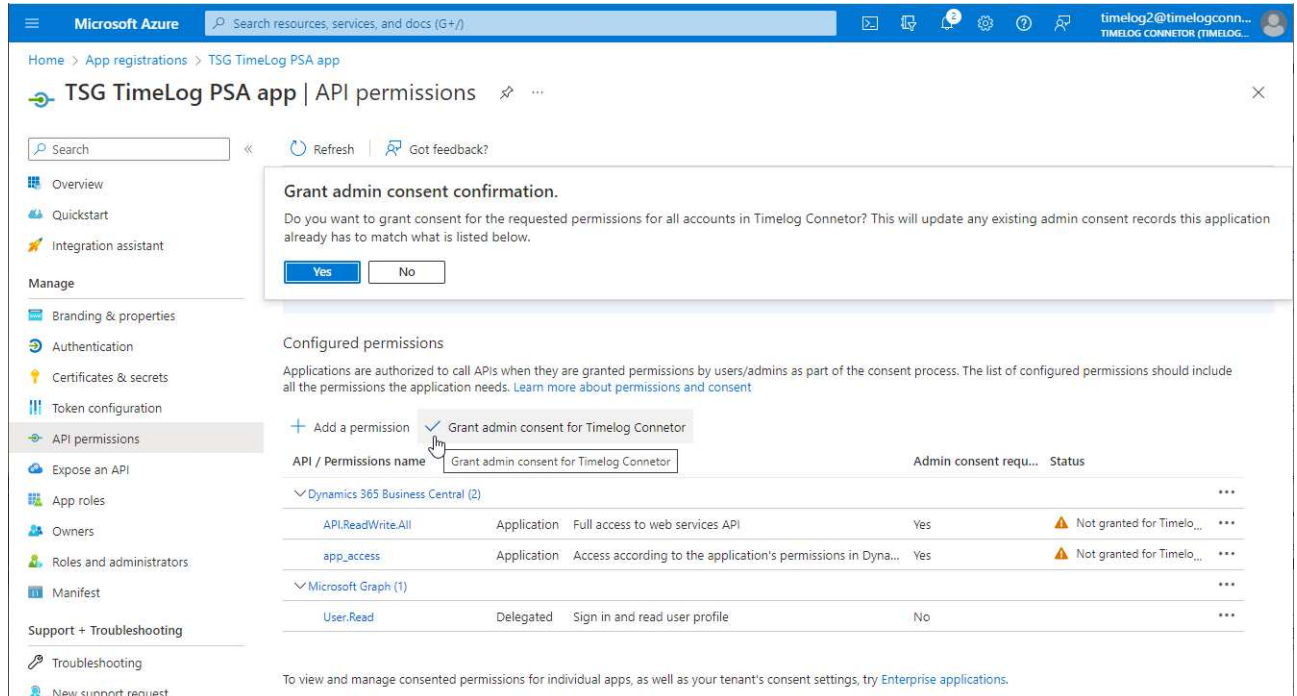
The screenshot shows the 'Request API permissions' dialog box. It has a search bar at the top with the text 'Start typing a permission to filter these results'. Below the search bar is a table with columns for 'Permission' and 'Admin consent required'. The table is organized into sections: 'Other permissions (1)', 'AdminCenter', 'API (1)', and 'Automation'. In the 'Other permissions (1)' section, the 'app_access' permission is selected with a blue checkmark. In the 'API (1)' section, the 'API.ReadWrite.All' permission is also selected with a blue checkmark. At the bottom of the dialog, there are two buttons: 'Add permissions' (highlighted in blue) and 'Discard'.



4. Grand admin consent confirmation

After permissions are added, click **'Grant admin consent for ...'**.
Click **Yes** button to grant consent for the requested permissions.

Status in the table of permissions should change to **'Granted'**



The screenshot shows the Microsoft Azure portal interface for the 'TSG TimeLog PSA app | API permissions' page. A modal dialog titled 'Grant admin consent confirmation.' is displayed, asking 'Do you want to grant consent for the requested permissions for all accounts in TimeLog Connector? This will update any existing admin consent records this application already has to match what is listed below.' with 'Yes' and 'No' buttons. Below the dialog, the 'Configured permissions' section is visible, showing a table of permissions. A dropdown menu is open over the 'Grant admin consent for TimeLog Connector' button, and a mouse cursor is pointing at it. The table lists permissions for Dynamics 365 Business Central and Microsoft Graph.

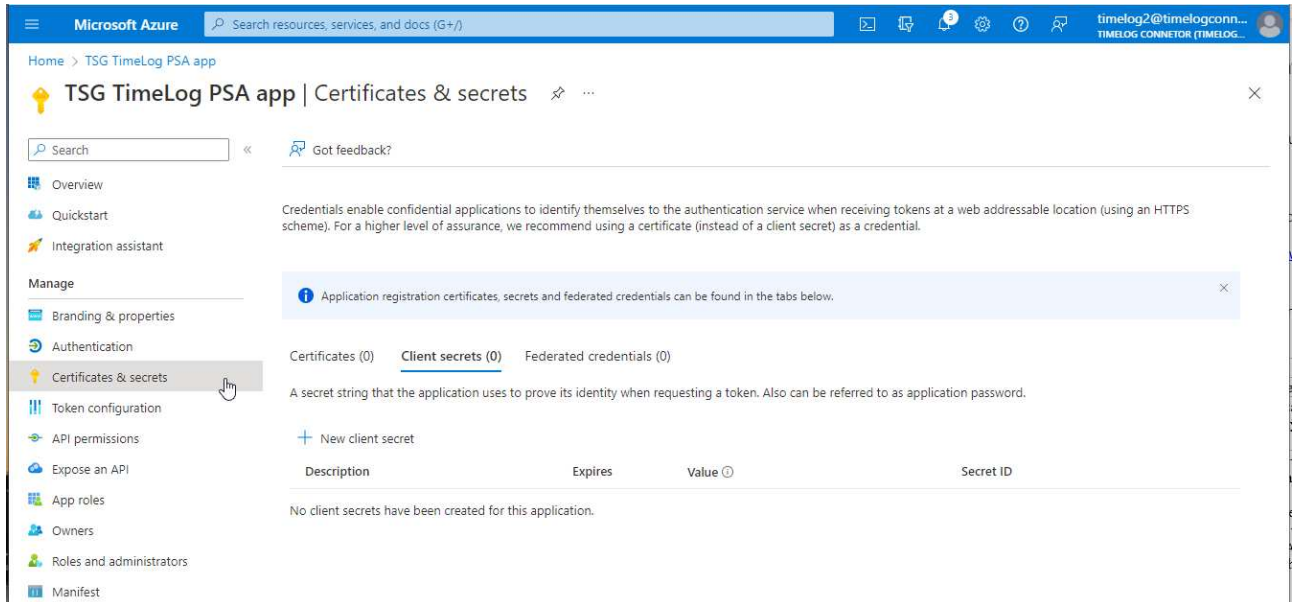
API / Permissions name	Admin consent requ...	Status
Dynamics 365 Business Central (2)		
API.ReadWrite.All	Application	Full access to web services API
app_access	Application	Access according to the application's permissions in Dyna...
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile



5. Certificates and secrets

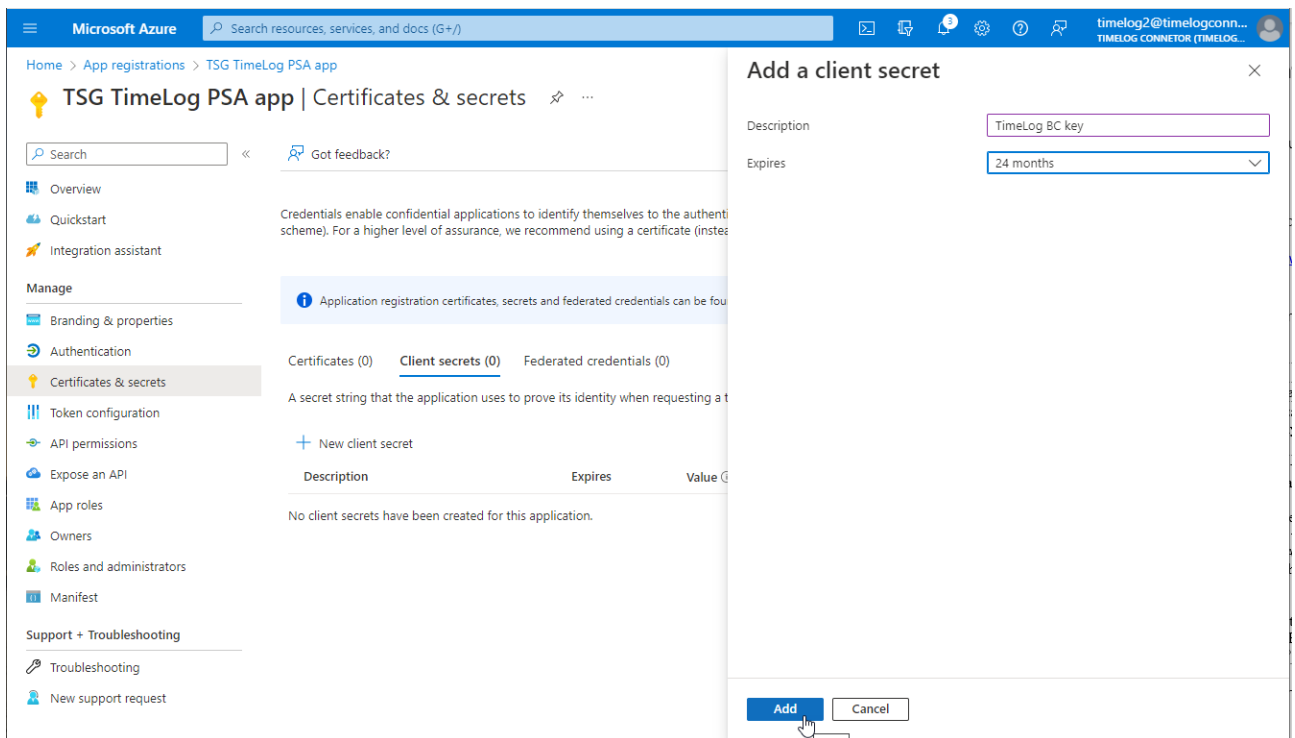
Setup client secret (used in authorization code flow scenario and application scenario):

Go to '**Certificates & secrets**' - '**Client secrets**', click '**+ New client secret**'



The screenshot shows the Microsoft Azure portal interface for the 'TSG TimeLog PSA app'. The left-hand navigation pane is open, with 'Certificates & secrets' selected. The main content area shows the 'Client secrets' tab, which is currently empty. A '+ New client secret' button is located above a table that would list existing client secrets. The table has columns for 'Description', 'Expires', 'Value', and 'Secret ID'. A message at the top of the content area states: 'Application registration certificates, secrets and federated credentials can be found in the tabs below.'

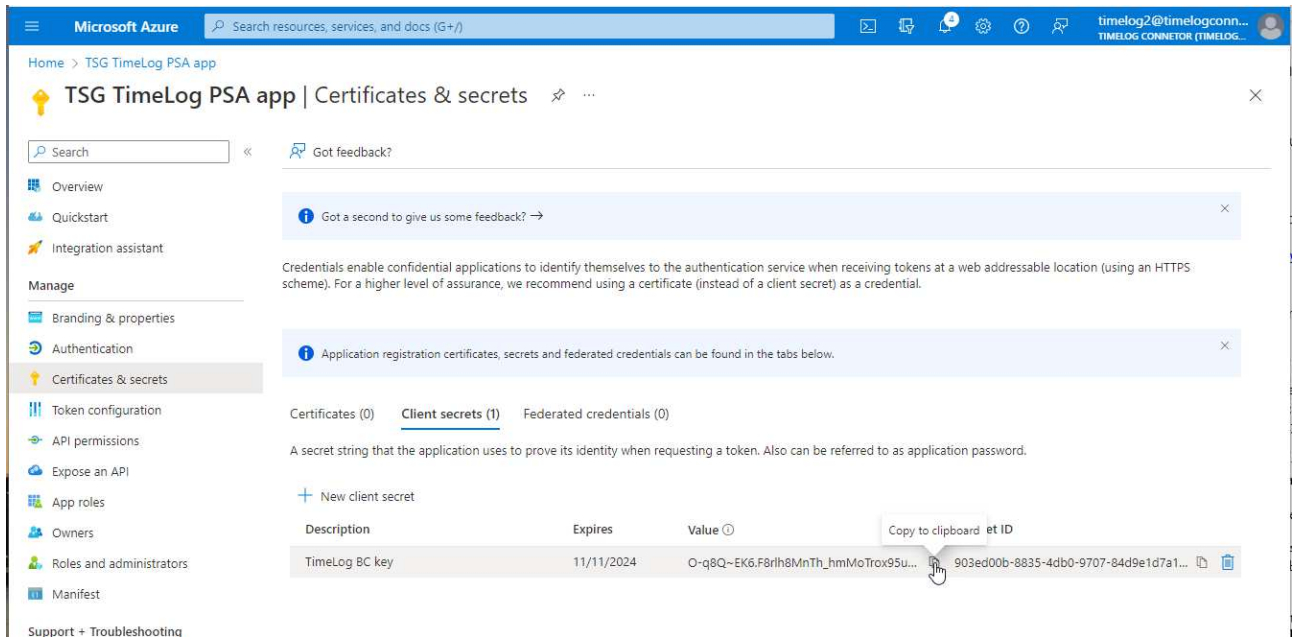
Add some **Description**, choose '**Expires**' setting to 24 months and click '**Add**'



The screenshot shows the 'Add a client secret' dialog box in the Microsoft Azure portal. The 'Description' field contains the text 'TimeLog BC key'. The 'Expires' dropdown menu is set to '24 months'. At the bottom of the dialog, there are two buttons: 'Add' and 'Cancel'. A mouse cursor is pointing at the 'Add' button.



After secret is created, copy secret '**Value**' and save for later when setting up the TimeLog to BC-integration.

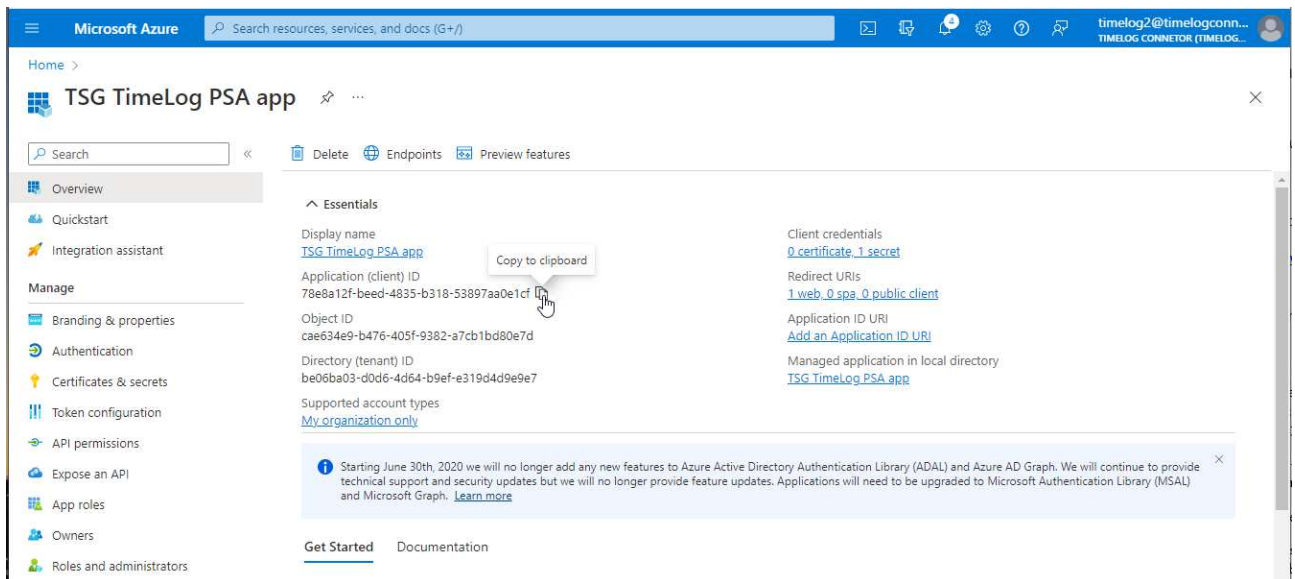


Copy the **Client secret** of the registered application. You will need this later when setting up the TimeLog to BC-integration.

6. Copy client ID

Select **Overview**

Copy the **Application (client) ID** from the App registrations – Overview. You will need it when adding the new client into your Business Central Microsoft Entra Applications



Copy the **Application (client) ID** of the registered application. You will need in the Business Central Microsoft Entra application setup.

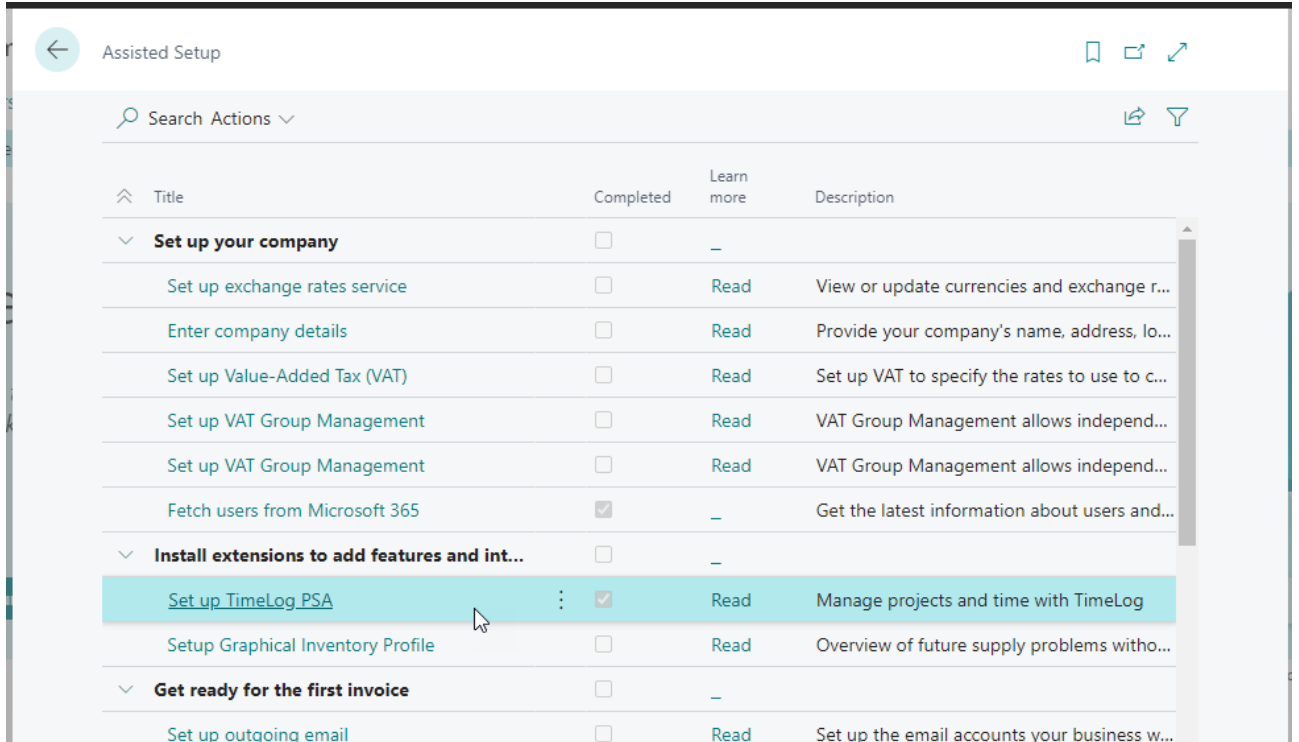


7. Install the TimeLog PSA app in your Business Central

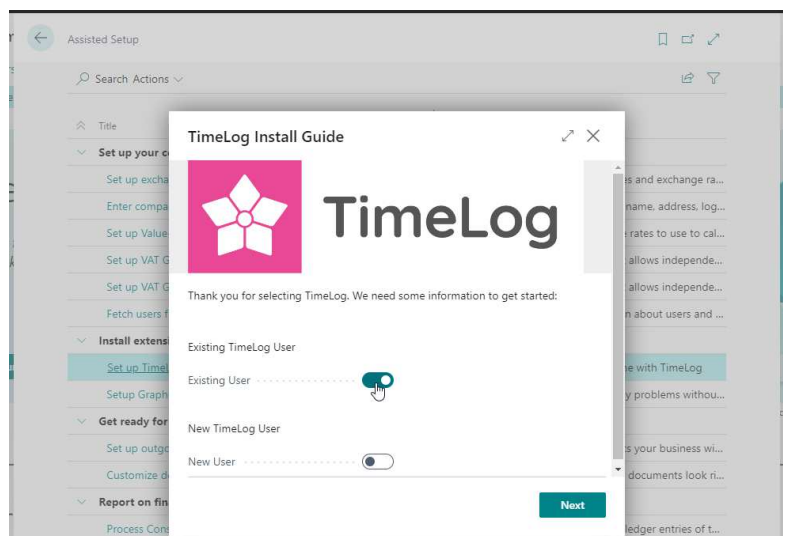
Open **Extension Marketplace** from within your Business Central installation and search for **TimeLog PSA**. Please be aware that you have the user rights to buy new applications to your Business Central.

Click **Free trial** and accept Microsoft license agreements and follow the guidelines.

When the TimeLog PSA app have been installed are you to run **Setup TimeLog PSA** in Assisted setup.



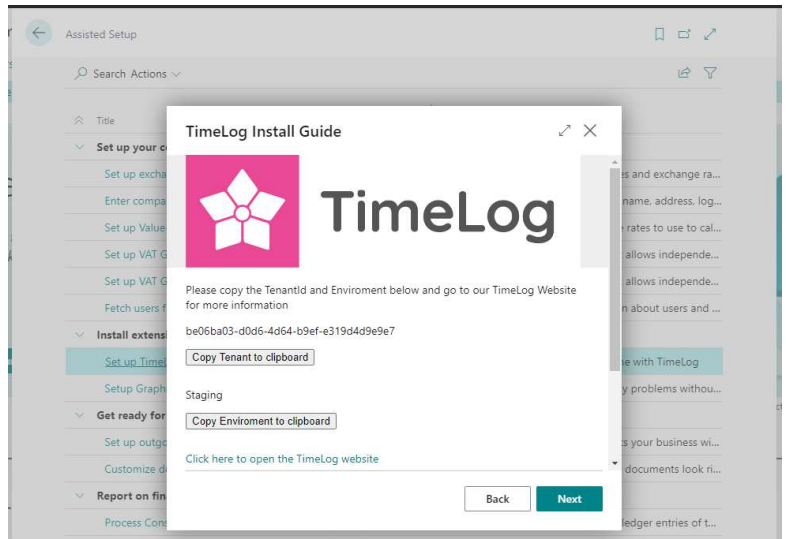
Click on **Setup TimeLog PSA** and click the slider next to Existing User, and click **Next**.



Copy the **Tenant ID key** and save it for later when setting up the integration connection.

Copy the **Environment name** and save it for later when setting up the integration connection.

Click **Next** and **Finish** on the next window to close the TimeLog PSA configuration.

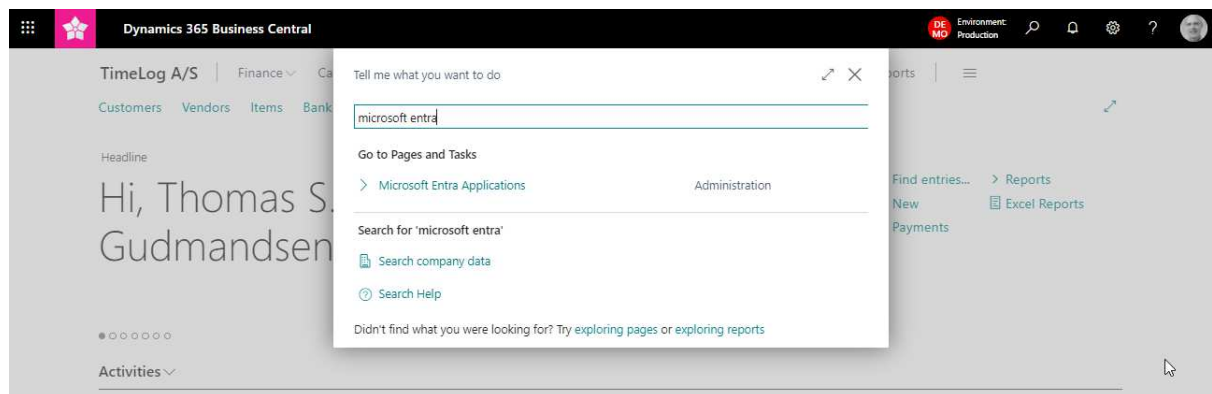


If your TimeLog installation is having multi legal entities activated, are you to run the **Setup TimeLog PSA** on each Business Central company that is to get connected to your TimeLog installation and use the unique Tenant ID and Environment name when setting up the connection.

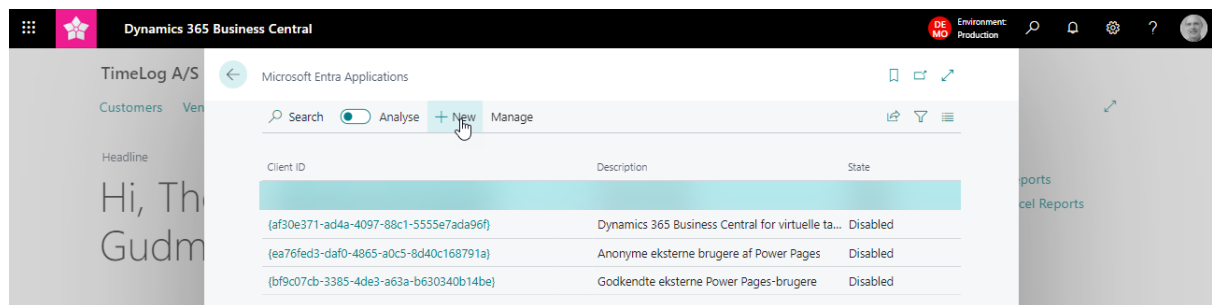
8. Setup of Microsoft Entra Application in Business Central

Complete these steps to set up the Microsoft Entra application for service-to-service authentication in Business Central.

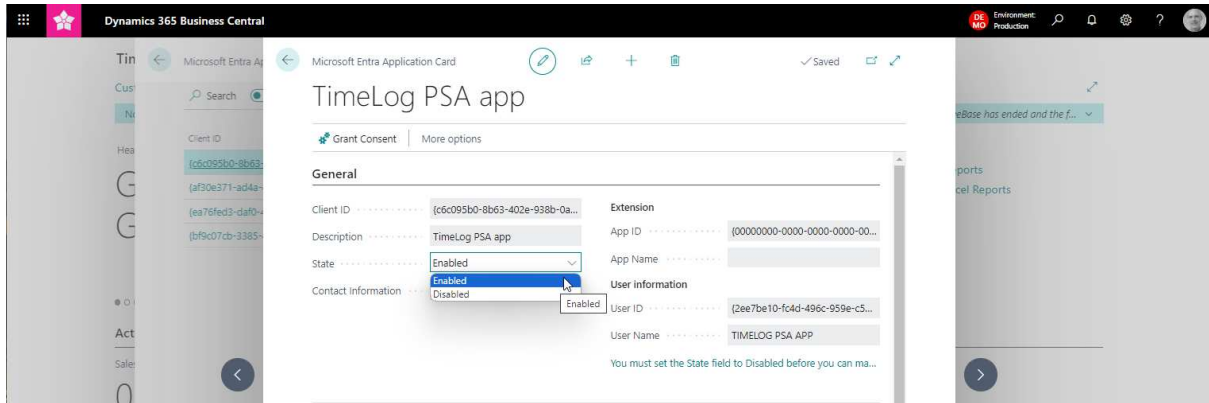
In your Business Central client, search for **Microsoft Entra Applications**



Click **New**,



Past the copied Application (client) ID into **Client ID**, add a description name and change State to **Enable** and click **Yes** to the new created user.

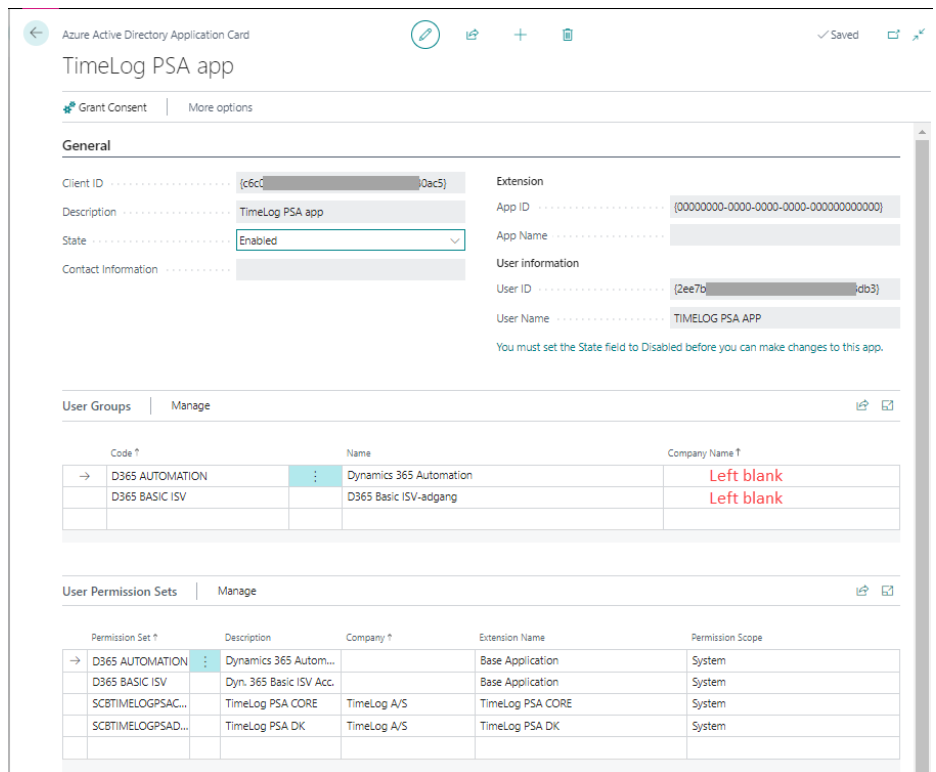


Add the **User Group**

- D365 AUTOMATION
- D365 BASIC ISV

Do not add a company name to the added user groups.

This is selected when configuring the BC integration in TimeLog system administration.



and **User Permission Sets**

- D365 BASIC ISV
- D365 AUTOMATION
- SCBTIMELOGPSACORESET
- SCBTIMELOGPSADKSET

If you have other apps installed in your Business Central installation, will you perhaps be needing to add additional permissions or the superuser permission **SUPER (DATA)** to your User Permissions Sets.

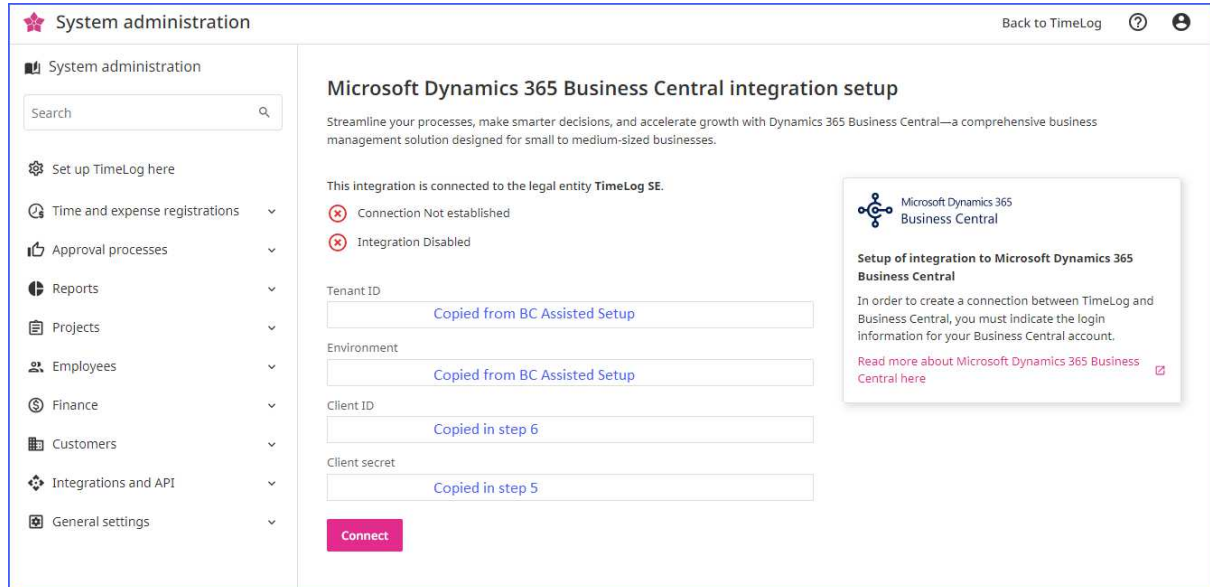
The added TimeLog PSA is now added in your Business Central Active Directory and you are now ready to install the TimeLog PSA app and run the setup



9. TimeLog – BC integration connection configuration

Add the Business central integration in TimeLog System administration >> Integrations and API >> Integrations and click **Configure Business Central**.

Add the copied credentials into the related fields in the user interface.



System administration Back to TimeLog ?

Microsoft Dynamics 365 Business Central integration setup

Streamline your processes, make smarter decisions, and accelerate growth with Dynamics 365 Business Central—a comprehensive business management solution designed for small to medium-sized businesses.

This integration is connected to the legal entity **TimeLog SE**.

- Connection Not established
- Integration Disabled

Tenant ID:

Environment:

Client ID:

Client secret:

Connect


Microsoft Dynamics 365 Business Central

Setup of integration to Microsoft Dynamics 365 Business Central

In order to create a connection between TimeLog and Business Central, you must indicate the login information for your Business Central account.

[Read more about Microsoft Dynamics 365 Business Central here](#)

When you have added the credentials information in the four fields are you to click **Connect** to establish the connection to your Business Central and you get access to the Business Central integration configuration.

Click the question icon  in the top right corner to open the integration configuration guide in our Help Center.

