

Office365: HOW TO GET TenantId, ClientId and ClientSecret

If you use Microsoft office 365 for email sending. Your company Microsoft admin need to get following settings from **Azure AD Application**

- **Directory (Tenant) ID**
- **Application (Client) ID**
- **Client Secret Value**

These three values are required for integrating CLOUDEX TMS with Microsoft Graph using OAuth2.

1 Sign in to Azure Portal

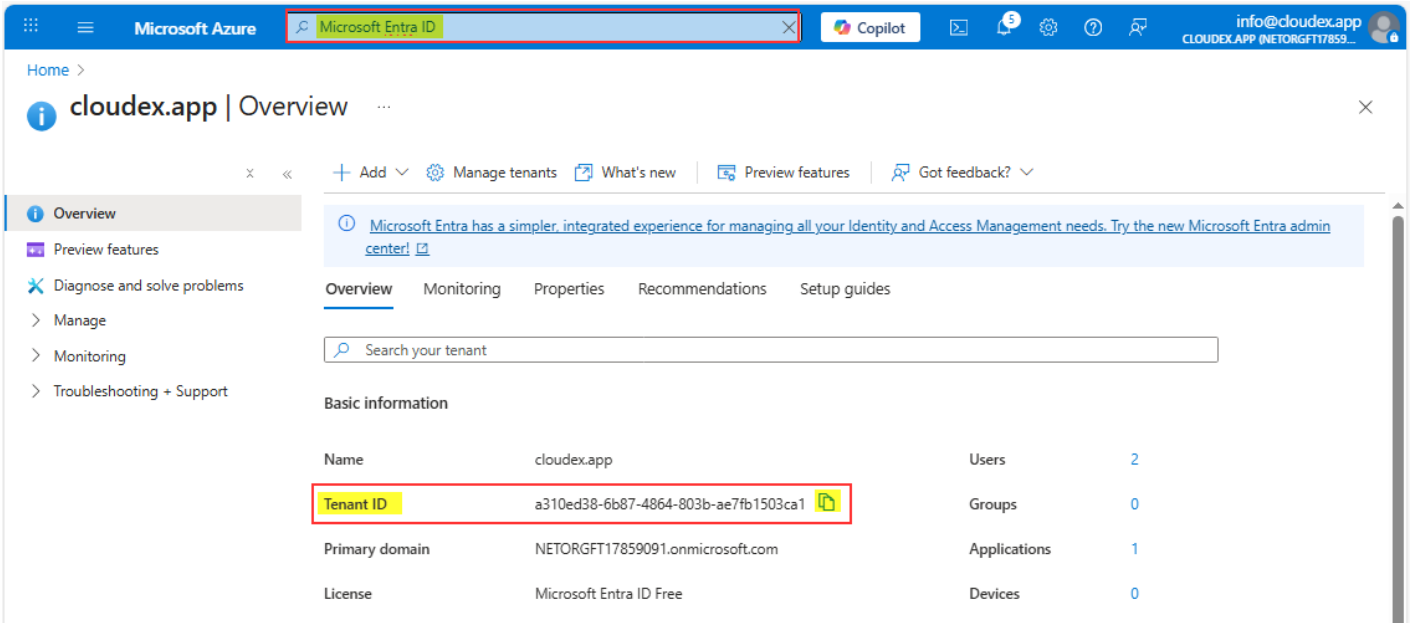
Open: <https://portal.azure.com>

Sign in with a Microsoft 365 **Global Admin** or **Application Administrator** account.

2 Open “Microsoft Entra ID” (Azure AD)

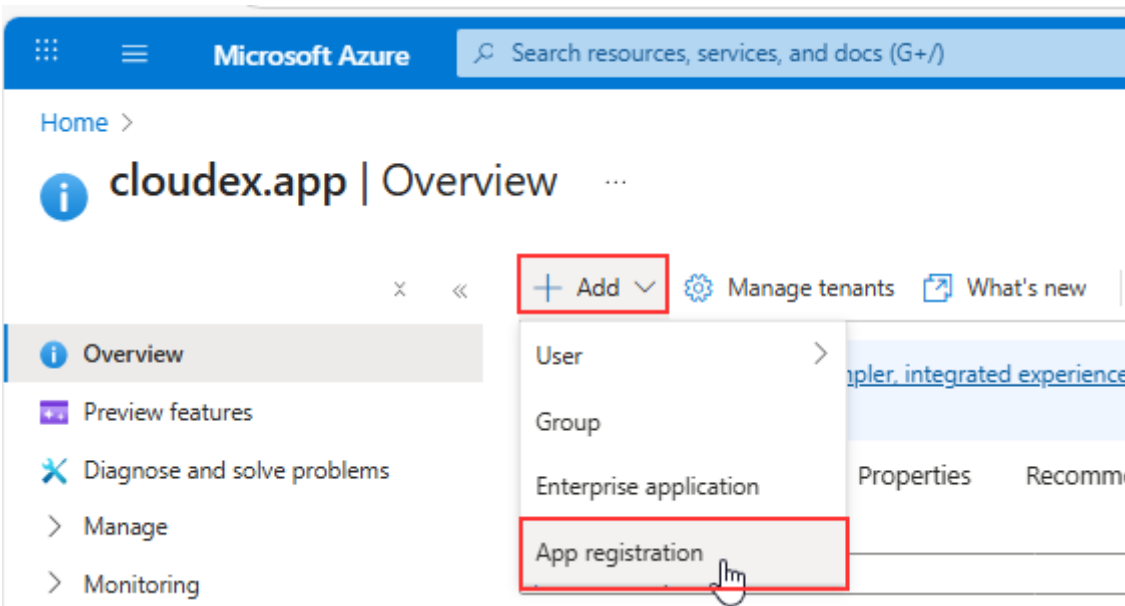
Left menu → **Microsoft Entra ID**

(or search “Entra ID” in the top search bar)



3 Create a new App Registration

1. Left menu: **App registrations**
2. Click **New registration**



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

Home > clouDEX.app | Overview >

Register an application

* Name

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

CLOUDEX TMS ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (clouDEX.app only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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 | <https://my.clouDEX.app/YourCompanyCode/Services/Office365Callb...> ✓

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

URL type must be "Web" NOT "Single page application"

Looks like better to register as Single tenant. If you register as multi tenant then can be so than you need to enter CLOUDEX MpnId 7086574

Fill the form:

Field	Value
Name	CLOUDEX TMS Email Integration (or any name)
Supported account types	✓ Accounts in any organizational directory (multitenant)
Redirect URI	Select Web → Enter your redirect: https://my.clouDEX.app/YourCompanyCode/Services/Office365Callback.aspx 1) Replace YourCompanyCode with your web app CompanyCode 2) Redirect URL is case-sensitive

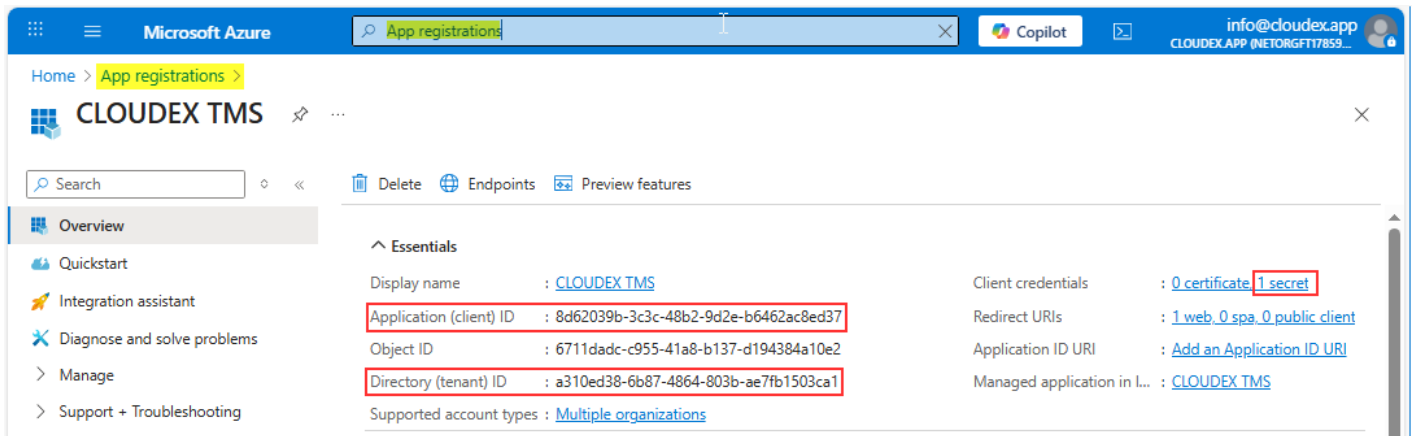
Click **Register**.

4 Get the Tenant ID and Client ID

After creation, you will be redirected to the app's **Overview** page.

Here you will see:

- ✓ **Directory (Tenant) ID**
- ✓ **Application (Client) ID**



Copy them and save.

You already have **2/3** values.

5 Create Client Secret

Side menu → **Certificates & secrets**

1. Click **New client secret**
2. Enter a name:
3. Choose expiration:
 - 6 months (not recommended)
 - 12 months
 - **24 months** (recommended)
 - Or "Custom"
4. Click **Add**

Add a client secret ✕

Description

Expires

Certificates (0) Client secrets (2) 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
CLOUDEX TMS Secret	5/30/2026	fw_*****	56b30de6-e8a1-4945-9448-7675ea2d02... 📄 🗑️
CLOUDEX TMS	12/1/2027	Oc6dd0eb [REDACTED] 7ee13 📄	rb8... 📄 🗑️

IMPORTANT ⚠️

Copy the Client Secret VALUE immediately.

You will never be able to see it again later.

Store it securely (Azure Key Vault, password manager, etc).

Now you have:

- **ClientId**
- **TenantId**
- **ClientSecret Value**

6 📄 Add Required API Permissions

Side menu → **API permissions**

Click:

- **Add a permission**
- **Microsoft Graph**
- **Delegated permissions**

Search + select:

- ✓
- ✓
- ✓

✓ `offline_access`

Then click **Add permissions**.

Then click **Grant admin consent**.

The screenshot shows the Microsoft Azure portal interface for configuring API permissions for an application named 'CLOUDEX TMS'. The 'Request API permissions' dialog is open, showing the 'Microsoft Graph' API selected. The 'Mail.ReadWrite' permission is chosen, and the 'Grant admin consent' checkbox is checked. The 'Add permissions' button is highlighted with a red box and a red circle containing the number 5. Other elements are marked with red circles: 1 on the 'API permissions' menu item, 2 on the '+ Add a permission' button, 3 on the search input containing 'Mail.ReadWrite', 4 on the 'Mail.ReadWrite' permission row, and 5 on the 'Add permissions' button.

API / Permissions name	Type
Mail.ReadWrite	Delegated
Mail.Send	Delegated
Mail.Send.Shared	Delegated
offline_access	Delegated
User.Read	Delegated

Permission	Admin consent required
Mail (2)	
<input checked="" type="checkbox"/> Mail.ReadWrite Read and write access to user mail	No

Can be in new interface need to choose Microsoft Graph API

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 Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Rights Management Services

Allow validated users to read and write protected content



Azure Service Management

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



Dynamics CRM

Access the capabilities of CRM business software and ERP systems

7▣ Final Check: Authentication Settings

Side menu → **Authentication**

Ensure:

- ✓ Your redirect URI is correct
- ✓ “Allow public client flows” is **OFF**
- ✓ “Access tokens” and “ID tokens” are **ON**

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

Home > App registrations > CLOUDEX TMS

CLOUDEX TMS | Authentication

Search Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication**
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

Warning: This app has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL.js 2.0, you should migrate URIs. →

Add URI

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (cloudex.app only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

[Help me decide...](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock

Configure the application instance modification lock. [Learn more](#) [Configure](#)

[Save](#) [Discard](#)

☑️ DONE — Values ready to use

You now have everything:

Parameter	Where to find it
TenantId	App → Overview → Directory (tenant) ID

Parameter	Where to find it
ClientId	App → Overview → Application (client) ID
ClientSecret	App → Certificates & Secrets → Value

Problem solution

In case you have any problems sending out emails from CLOUDEX TMS or Ozols you can run **"Diagnose and solve problems"** tool

The screenshot shows the Azure portal interface for the 'Diagnose and solve problems' tool. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant, **Diagnose and solve problems** (highlighted), Manage, and Support + Troubleshooting. The main content area is titled 'Sign-in Diagnostic: Review Sign-ins' and shows a table of flagged sign-in events. Below the table, a progress bar indicates 'Running diagnosis ...' with a 'Cancel' button.

createdDateTime	userDisplayName	userPrincipalName	appDisplayName	status	errorCode	flaggedForReview
2026-01-20T10:11:00Z	Jekaterina Pavkštello	doc.████████@e.lv	CLOUDEX TMS	Failure	900971	false

Revision #16

Created Mon, Dec 1, 2025 1:02 PM by [Janis Veldre](#)

Updated Tue, May 26, 2026 1:11 PM by [Janis Veldre](#)