

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)

The screenshot shows the Microsoft Entra ID Overview page. The 'Tenant ID' is highlighted with a red box. The page includes a left-hand navigation menu with options like 'Overview', 'Preview features', 'Diagnose and solve problems', 'Manage', 'Monitoring', and 'Troubleshooting + Support'. The main content area displays basic information about the tenant, including its name, ID, primary domain, and license.

Basic information	
Name	clouDEX.app
Tenant ID	a310ed38-6b87-4864-803b-ae7fb1503ca1
Primary domain	NETORGFT17859091.onmicrosoft.com
License	Microsoft Entra ID Free

3 Create a new App Registration

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

The screenshot shows the Microsoft Azure portal interface. The 'Add' button is highlighted with a red box, and the 'App registration' option in the dropdown menu is also highlighted with a red box. The page shows the 'clouDEX.app | Overview' section with a left-hand navigation menu.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

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 beter 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

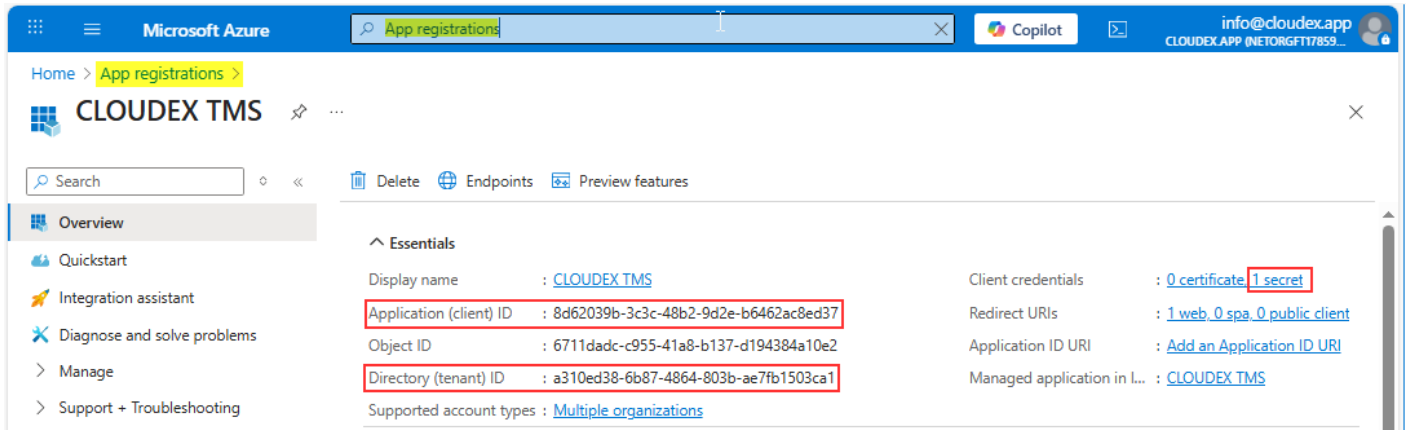
Click **Register**.

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

CLOUDEX TMS

Expires

730 days (24 months)

Add

Cancel

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	0c6dd0eb-*****7ee13 	rb8*****u...  

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:

- ✓ Mail.ReadWrite
- ✓ Mail.Send
- ✓ Mail.SendShared
- ✓ offline_access
- ✓ User.Read

!!! If email sending does not work, then add also following permissions

- ✓ email
- ✓ openid
- ✓ profile

Then click **Add permissions.**

Then click **Grant admin consent.**

Microsoft Azure | Search resources, services, and docs (G+/J) | Copilot | info@cloudex.app | CLOUDEXTMS

Home > cloudex.app | App registrations > CLOUDEXTMS

CLOUDEXTMS | API permissions

Search | Refresh | Got feedback?

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

Granting tenant-wide consent may revoke permissions for all the applications in your organization. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they have all the permissions the application needs. [Learn more](#)

2 + Add a permission **✓** Grant admin consent

API / Permissions name	Type
Microsoft Graph (5)	
Mail.ReadWrite	Delegated
Mail.Send	Delegated
Mail.Send.Shared	Delegated
offline_access	Delegated
User.Read	Delegated

Other permissions granted for cloudex.app

These permissions have been granted for cloudex.app. [Learn more](#)

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

3 Mail.ReadWrite

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
Mail (2)	
☒ Mail.ReadWrite Read and write access to user mail	No

4

5 **Add permissions** Discard

Add or remove favorites by pressing Ctrl+Shift+F

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**

The screenshot shows the Microsoft Azure portal interface for configuring an application named "CLOUDEX TMS". The left sidebar contains a navigation menu with options like Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, Branding & properties, Authentication (highlighted), 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 "Authentication" and includes a search bar and a "Got feedback?" link. The "Platform configurations" section explains that additional configuration may be required based on the target platform or device. Below this, there is a section for "Web" configurations, specifically "Redirect URIs". It states that the URLs accepted as destinations for authentication responses (tokens) must match one listed here. A warning message indicates that the app has implicit grant settings enabled and suggests migrating URLs if using a SPA with MSAL.js 2.0. A single redirect URI is listed: "https://my2.cloudex.eu/dev/Services/Office365Callback.aspx". Below the "Web" section, the "Implicit grant and hybrid flows" section explains how to request a token directly from the authorization endpoint. It provides instructions for SPA and ASP.NET Core web apps. A selection box allows choosing the tokens to be issued: "Access tokens (used for implicit flows)" and "ID tokens (used for implicit and hybrid flows)". The "Supported account types" section asks "Who can use this application or access this API?" and offers two options: "Accounts in this organizational directory only (cloudex.app only - Single tenant)" and "Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)". The "Advanced settings" section includes "Allow public client flows" (set to "No") and "App instance property lock" (set to "Configure"). At the bottom, there are "Save" and "Discard" buttons.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

info@cloudex.app
CLOUDEX.APP (NETORGFT17859...

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](#)

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 URLs. →

https://my2.cloudex.eu/dev/Services/Office365Callback.aspx

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
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

Home - Microsoft 365 admin center

CLOUDEX TMS - Microsoft Azure

Office365: HOW TO GET ... | OZOL

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/troubleshoot/appld/62ae9078-f60e-48f4-ac4e-f683418544fe/isMSAApp~/false

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Tempusline SIA | App registrations > CLOUDEX TMS

CLOUDEX TMS | Diagnose and solve problems

Search

Start Over

New Support Request

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Sign-in Diagnostic: Review Sign-ins

Flagged Sign-In Events

All Sign-In Events

Authentication summary

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

Running diagnosis ...

Please wait while we scan multiple data sources...

Cancel

Revision #4
Created 2026-06-25 06:22:16 UTC by Admin
Updated 2026-07-17 12:18:13 UTC by Admin