

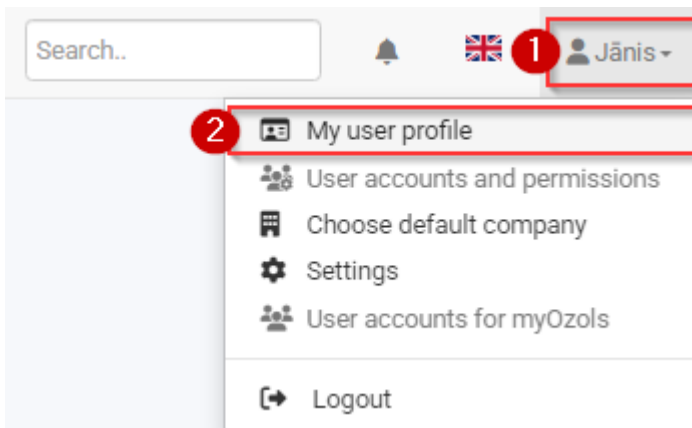
1. Settings

- [E-mail settings](#)
- [Create google email password](#)
- [Office365: HOW TO GET TenantId, ClientId and ClientSecret](#)
- [Microsoft email configuration](#)
- [Order conditions update](#)
- [Set up Office365 e-mail](#)
- [HOW TO CHANGE APPLICATION Callback URL in Azure Portal](#)

E-mail settings

To send emails from Cloudex TMS:

- 1) Click on the Your User Name icon
- 2) Select the "My Profile" menu



In the "Email password" field:

- 1) Enter your email password
- 2) Click the "Save" button

A screenshot of the 'My user profile' form. The form has a title bar with a close button (X). It contains several input fields: 'Name' (Jānis), 'Surname' (Veldre), 'Position' (Position), 'GSM' (+37129489925), 'Phone' (+37163050199), 'Email' (info@cloudex.lv), and 'Email password' (masked with dots). A red circle with the number '1' is placed over the 'Email password' field. At the bottom of the form, there is a status bar showing 'Saved: 20.03.2025 11:22 webuser'. To the right of the status bar, there is a 'Save' button (blue) and a 'Cancel' button (white). A red circle with the number '2' is placed over the 'Save' button.

Create google email password

1) Open google account and login:

<https://myaccount.google.com/>

2) Open **Drošība/Security**

If 2-step verification is not available in the section, your company's email administrator must first enable it: [instrukction how to do it read here](#)

3) Ieslēgt "2-pakāpju verifikāciju / 2-Step verification"

← 2-Step Verification

Turn on 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#) 



[Turn on 2-Step Verification](#)

4) Create a password/key for emails

If there is no "App passwords" section in the Two-step verification / 2-step verification section, you must exit the page and re-enter it. Or use the link

<https://myaccount.google.com/apppasswords>

← 2-Step Verification

Your account is protected with 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#) ↗



[Turn off 2-Step Verification](#)

Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options



Passkeys and security keys



Add a security key



Google prompt



2 devices



Authenticator



Add authenticator app



Phone number



29 489 925



Backup codes



Get backup codes



App passwords

App Passwords aren't recommended and are unnecessary in most cases. To help keep your account secure, use "Sign in with Google" to connect apps to your Google Account.

App passwords

1 App password



5) Create password

← App passwords

App passwords help you sign into your Google Account on older apps and services that don't support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.

[Learn more](#)

Your app passwords

OZOLS

Created on Mar 26



To create a new app specific password, type a name for it below...

App name

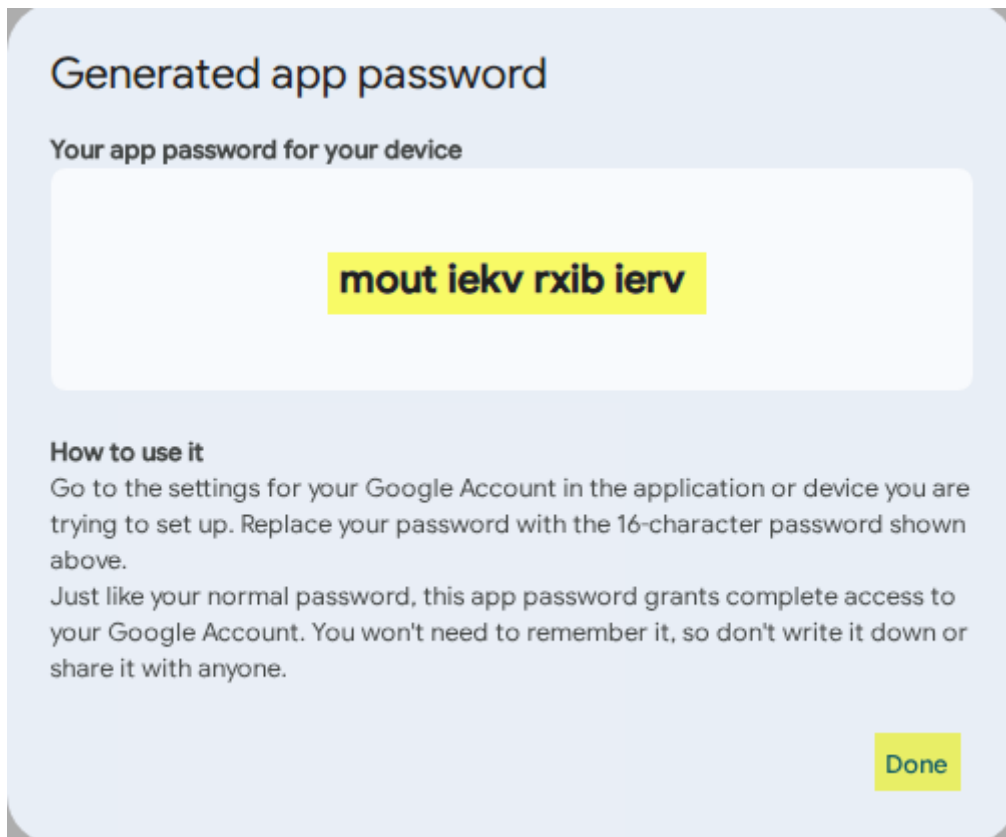
CLOUDEX TMS

Create

6) Copy new password and enter it in OZOLS or CLOUDEX TMS

Instructions for entering your email password in Ozols: <https://doc.ozols.lv/books/ozols-tms-english/page/5-e-mail-settings>

Instructions for entering your email password in CLOUDEX TMS: <https://doc.ozols.lv/books/cloudex-tms-english/page/e-mail-settings>



Companies must have the option enabled that is available

[Instrukction from google](#)

Showing settings for users in clouDEX.lv

Organizational Units

Search for organizational units

▼ clouDEX.lv

Groups

Customize settings for a group within an organizational unit. One group per organizational unit. [Learn more](#)

Search for a group

Authentication
Locally applied

Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. [Learn more](#)

☒ Allow users to turn on 2-Step Verification

Enforcement

☐ Off☒ On

☐ On from Date

New user enrollment period

New user enrollment period
Allows new users some time to enroll before enforcement is applied

None

Frequency

Users can avoid repeated 2-Step Verification at login on their trusted devices. [Learn more](#)

☒ Allow user to trust the device

Methods

Select the method to enforce. [Learn more](#)

☒ Any

☐ Any except verification codes via text, phone call

☐ Only security key

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 Azure portal interface. At the top, the search bar contains 'Microsoft Entra ID'. The left sidebar shows the 'Overview' page selected. The main content area displays the 'Basic information' for the tenant 'clouDEX.app'. A red box highlights the 'Tenant ID' field, which contains the value 'a310ed38-6b87-4864-803b-ae7fb1503ca1'.

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 its dropdown menu is open. The 'App registration' option is selected and highlighted with a red box. A hand cursor is pointing at the 'App registration' option.

Search resources, services, and docs (G+)

Home > clouDEX.app | Overview

+ Add Manage tenants What's new

- User
- Group
- Enterprise application
- App registration

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)

Field	Value
Supported account types	✓ Accounts organizational directory (multitenant)
Redirect URI	Select Web → Enter your redirect: https://my.cloudex.app/ Your CompanyCode /Services/Office365Callback.aspx 1) Replace Your CompanyCode with your web app CompanyCode 2) Redirect URL is case- sensitive

Click **Register**.

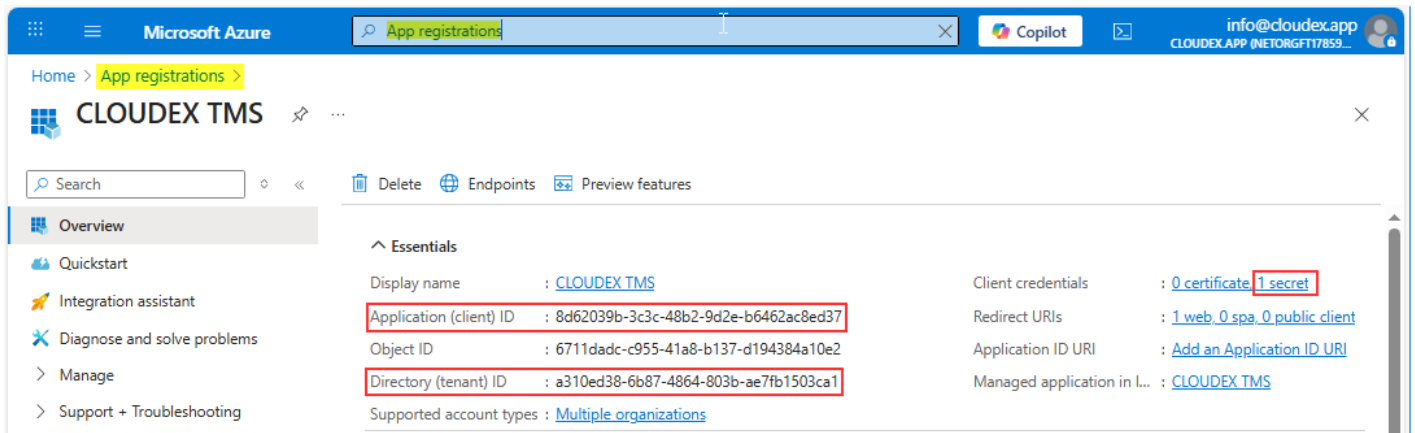
4 Get the Tenant ID and Client ID

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

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	0c6dd0eb *****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:

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

Then click **Add permissions**.

Then click **Grant admin consent**.

The screenshot shows the Microsoft Azure portal interface for managing API permissions for an application named 'CLODEX TMS'. The left sidebar shows the 'API permissions' section selected. The main area displays the 'Request API permissions' dialog for the 'Microsoft Graph' API. The 'Delegated permissions' tab is active, showing a list of permissions under the 'Mail' category. The 'Mail.ReadWrite' permission is selected, and the 'Admin consent required' column shows 'No'. The 'Add permissions' button is highlighted with a red box and a red circle with the number 5.

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)	
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+/) 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

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 URIs. →

<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
ClientSecretValue	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 cent...CLOUDEX TMS - Microsoft AzureOffice365: HOW TO GET ... | OZOL... | +

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

Microsoft AzureSearch resources, services, and docs (G+/)Copilot

Home > Tempusline SIA | App registrations > CLOUDEX TMS

CLOUDEX TMS | Diagnose and solve problems

Search

Start OverNew Support RequestGot feedback? ▾

OverviewQuickstartIntegration assistantDiagnose and solve problemsManageSupport + Troubleshooting

Sign-in Diagnostic: Review Sign-ins

Flagged Sign-In EventsAll Sign-In Events

Authentication summary

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

Running diagnosis ...

Please wait while we scan multiple data sources...

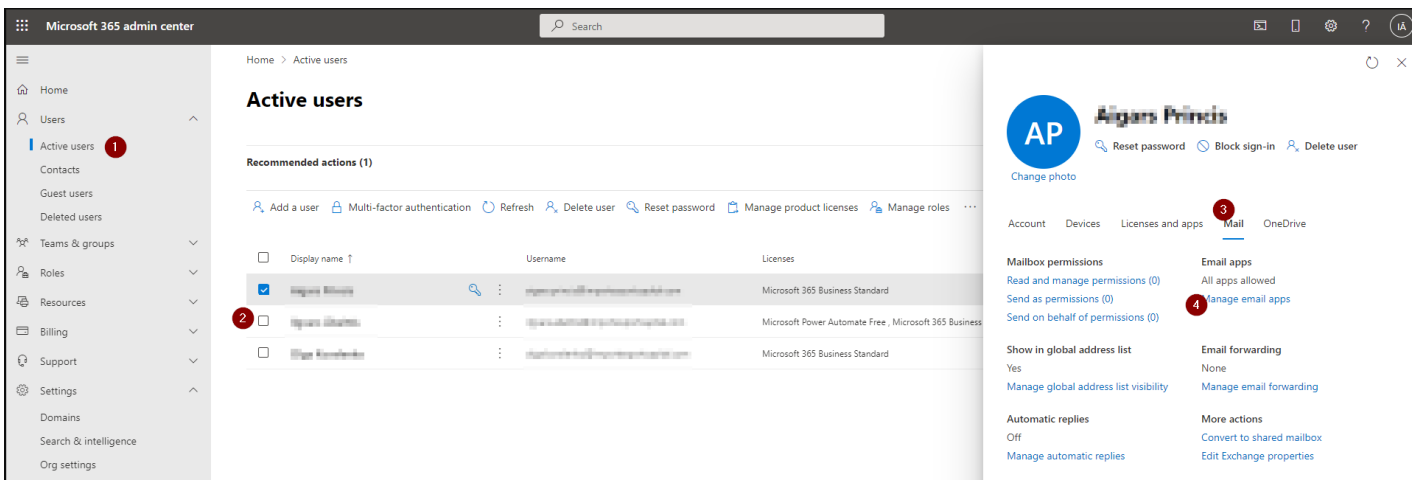
Cancel

Microsoft email configuration

1. Enable “Authenticated SMTP” for the mailbox

Open the Microsoft 365 Admin Center: <https://admin.microsoft.com>

Steps to enable Authenticated SMTP



1. In the left menu, click **Users → Active users**.
2. Click on the user/mailbox you will use for CLOUDEX TMS.
3. In the user details pane, go to the **Mail** tab.
4. Click **Manage email apps** (or *Email apps*).
5. In the list of email apps, find **Authenticated SMTP** and make sure the checkbox or toggle is **ON / enabled**.
6. Click **Save**.



2. Create an app password (if MFA is enabled)

If Multi-Factor Authentication (MFA) is enabled for the mailbox you use (recommended), SMTP cannot use your normal password. In that case you must create a special **app password** and use it in CLOUDEX TMS.

If MFA is **not** enabled for this user, you can use the normal account password instead of an app password. However, using MFA + app password is more secure and recommended.

Instruction to generate an app password

<https://doc.ozols.lv/books/ozols-tms-english/page/8-e-mail-server-configuration-for-work-with-ozols-tms>

What to do if “Authenticated SMTP” switch does NOT appear

1. Turn off Checkbox "Turn off SMTP AUTH protocol for your organization"
2. Turn on use of old legacy TLS clients.
3. After enabling, wait **3-5 minutes**, then check the user mailbox again.

The screenshot shows the Exchange Admin Center (EAC) interface. The left sidebar contains navigation links: Home, Recipients, Mailboxes, Groups, Resources, Contacts, Mail flow, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, Settings (highlighted with a red circle and number 2), Troubleshoot, and Other features. The main content area is titled 'Settings' and contains a table with the following data:

Name	Description
List view preference	Select normal view or compact view as your preference
Mail flow (highlighted with a red circle and number 3)	Manage your organization's settings for sending and receiving messages
Hybrid setup	Connect and manage both your on-premises and cloud mailboxes

The 'Mail flow settings' panel is open on the right, showing the following configuration:

- General**
 - ☐ Turn off plus addressing for your organization. [Learn more](#)
 - ☐ Turn on sending from aliases
- Security**
 - ☐ Turn off SMTP AUTH protocol for your organization
 - ☒ Turn on use of legacy TLS clients. [Learn more](#)
- Reply-all Storm Protection**
 - ☒ Enable reply-all storm protection
 - Minimum number of recipients (1000 to 5000): 2500
 - Minimum number of reply-alls (2 to 20): 10
 - Block duration (1 to 24 hours): 6
- Message Recall**
 - ☒ Enable cloud-based message recall
 - ☒ Allow users to recall messages read by the recipient
 - ☐ Enable recall alerts for recipients
 - ☐ For all recalled messages

A red circle with the number 4 highlights the 'Security' section, and a red circle with the number 5 highlights the 'Save' button at the bottom right of the panel.

Confirm the mailbox type (SMTP is NOT available for some accounts)

The **Authenticated SMTP** switch is available ONLY for:

- User mailboxes with Exchange Online Plan 1 or 2
- Shared mailboxes
- Microsoft 365 E3/E5 Business Standard/Business Premium accounts

It will **NOT appear** for:

- ☐ Mailboxes with no Exchange license
- ☐ Accounts converted to *Microsoft 365 Groups*
- ☐ Mailboxes that were soft-deleted or recently restored
- ☐ Resource mailboxes (Room / Equipment)

How to check:

In Microsoft 365 Admin Center:

Users → Active users → Select user → Licenses and Apps

Make sure:

✓ **Exchange Online** is enabled

If Exchange Online is missing → SMTP will NOT be available.

Ensure modern authentication SMTP is not forced

Microsoft sometimes blocks SMTP for users with strict conditional access.

Check these items:

- Conditional Access policy requiring MFA for all protocols
- Legacy auth blocked at the tenant level
- Security defaults enabled (this disables SMTP)

To check Security Defaults:

1. Go to Azure Portal
<https://portal.azure.com>
2. Search for **Azure Active Directory**
3. Open **Properties**
4. Click **Manage Security Defaults**
5. If **Security defaults = Enabled**, you must turn it **OFF** to allow SMTP.

“After disabling, wait up to 15 minutes, then check Manage Email Apps again.

If none of the above works - your tenant may have SMTP permanently disabled

Microsoft has been turning off SMTP AUTH for security reasons.

Admins must manually re-enable it per mailbox.

To force-enable for a specific mailbox (Admin only):

1. Go to:
<https://admin.exchange.microsoft.com>
2. Navigate to:
Users → Active Users → select user → Mail → Email apps → Manage
3. If still missing, enable via PowerShell:

```
Set-CASMailbox -Identity user@domain.com -SmtpClientAuthenticationEnabled $true
```

(Admins only — if customer cannot run PowerShell, you can give them this line to pass to their IT provider.)

Summary: Why SMTP may not appear

Reason	Solution
Tenant wide SMTP disabled	Enable under Exchange Admin Center → Settings → Mail flow
New UI hides the option	Use Classic Exchange Admin Center (ECP)
No Exchange Online license	Add a license
Security Defaults enabled	Disable Security Defaults
Legacy auth blocked by Conditional Access	Update policies

Reason	Solution
Mailbox type unsupported	Use a licensed user or shared mailbox
Needs Powershell	Run Set-CASMailbox

Order conditions update

In order to edit Order for carrier rules or Order for Client rules Click on Your name > Settings > Classifications > Agreement rules > Edit

The screenshot shows the CLOUDEX web application interface. The top navigation bar includes the CLOUDEX logo, a search bar, and a user profile dropdown labeled 'Jānis' (marked with a red circle 1). The left sidebar contains a 'Company settings' section with sub-items: 'Configurations', 'Company settings', and 'Classifications' (marked with a red circle 3). The 'Classifications' section is further divided into 'Logistics' and 'Agreement rules' (marked with a red circle 4). The 'Agreement rules' section is highlighted with a red box. The main content area displays a table with columns 'Name' and 'Translation'. The table contains two rows: 'Carrier rules for Road' and 'Client rules for Road'. The 'Carrier rules for Road' row has an edit icon (pencil) next to it (marked with a red circle 5). The 'Client rules for Road' row also has an edit icon. The table is titled 'Search in list' and has a 'Column visibility' button. The bottom right corner shows a settings menu (marked with a red circle 2) with options: 'My user profile', 'User accounts and permissions', 'Change password', 'Settings', 'Choose default company', 'User accounts for myOzols', 'Compact mode', 'Dark theme', and 'Logout'.

CLOUDEX New ▾ Operational work ▾ Finances ▾ Reports ▾ Emails ▾ Lists ▾ Search...

Company settings

Configurations Company settings **Classifications**

Package type ▾

Logistics

- Term type
- Other classifier
- Department
- Client category
- Text template
- Agreement rules**
- Price list

Search in list

Name	Translation
Carrier rules for Road	ENG; RUS; LV; LT;
Client rules for Road	ENG; LT;

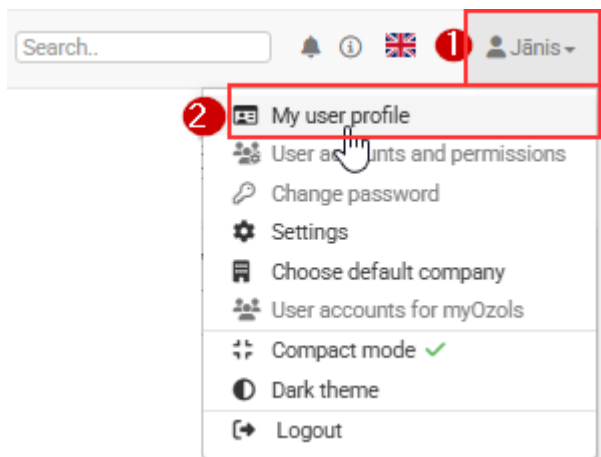
Settings

- My user profile
- User accounts and permissions
- Change password
- Settings
- Choose default company
- User accounts for myOzols
- Compact mode ✓
- Dark theme
- Logout

Set up Office365 e-mail

If your email provider is Microsoft Office365 You need o set up email sending following this instruction

- 1) Click on your name
- 2) Choose My user profile



Press comand button [Office365 setup]

My user profile ×

Name	Jānis	Surname	Veldre
Position	Transport Manager		
GSM	+371 29489925	Phone	Phone
Email	info@cloudex.lv		
Email password	Office365 setup		

Saved: 09.12.2025 14:19 webuserSaveCancel

Then press command button [Connect to Microsoft]

Microsoft Email Authorization

Office365 Status: Not connected

Connect to Microsoft

Login with your email and follow further instructions

HOW TO CHANGE APPLICATION Callback URL in Azure Portal

1 Open Azure Portal

Go to: <https://portal.azure.com>

Sign in using a **Global Administrator** or **Application Administrator** account.

2 Open Microsoft Entra ID

- 1) In the left menu, click: **Microsoft Entra ID or Search for App registrations**
- 2) Open All Applications
- 3) Open CLODEX TMS application

The screenshot shows the Microsoft Azure portal interface. At the top, the 'App registrations' link is highlighted with a red box and a red circle labeled '1'. Below the navigation bar, the 'App registrations' page is displayed. A red box labeled '2' highlights the 'All applications' tab. Below the tabs, there is a search bar and a table of applications. The table has columns for 'Display name', 'Application (client) ID', 'Created on', and 'Certificates & secrets'. One application, 'CLODEX TMS', is listed and highlighted with a red box and a red circle labeled '3'.

Display name	Application (client) ID	Created on	Certificates & secrets
CLODEX TMS	8d6203...	12/1/2025	Current

Choose Redirect URLs

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header with the 'Microsoft Azure' logo and a search bar containing 'App registrations'. Below the header, the 'Home' link is visible. The main content area is titled 'CLOUDEX TMS'. On the left, there's a sidebar with navigation links: 'Overview' (selected), 'Quickstart', 'Integration assistant', 'Diagnose and solve problems', 'Manage', and 'Support + Troubleshooting'. The 'Overview' page displays various application details under the 'Essentials' section, including 'Display name' (CLOUDEX TMS), 'Application (client) ID', 'Object ID', 'Directory (tenant) ID', and 'Supported account types'. On the right, there are links for 'Client credentials' (0 certificate, 1 secret), 'Redirect URIs' (1 web, 0 spa, 0 public client), 'Application ID URI' (Add an Application ID URI), and 'Managed application in local directory' (CLOUDEX TMS). The 'Redirect URIs' link is highlighted with a red box.

Press edit button and set correct URL

!!!! In **YourCompanyCode** you should place your company code `https://my.cloudex.app/YourCompanyCode/Services/Office365Callback.aspx`

Redirect URI configuration Settings

A redirect URI, or reply URL, is the location where the Entra authorization server sends the user and delivers tokens once the user has successfully signed in or signed out. [Learn more about what is a redirect URI](#)

[+ Add Redirect URI](#) [Delete](#)

i If you want to view or change implicit grant and hybrid flows settings or front-channel logout URL, please visit the settings tab.

⚠ 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. →

Start typing a reply url to filter these results		Platform Type : All
☐ Platform Type ↑↓	Redirect URI ↑↓	
☐ Web	Edit	...
☐ Web	https://my.cloudex.app/YourCompanyCode/Services/Office365Callback.aspx	

Redirect URL should be under Web NOT under Single-application