



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Intelligent Workload Distribution Administrator's Guide

Prepare for Office 365 integration

Contents

- 1 Authorization using client credentials grant flow
- 2 Authorization on behalf of the user

Prepare to set up Office 365 mailboxes by adding a new Enterprise Application in the Azure Active Directory (AD) portal. This one-time authorization procedure is a prerequisite for setting up Office 365 mailboxes.

Related documentation:

-

Authorization using client credentials grant flow

In order to avoid manual re-login for mailboxes that do not have a valid token, Genesys recommends using Client Credentials grant authentication for accessing Office365 using Graph API.

Provisioning procedure is described below:

Important

You must follow Steps 1 - 4 only if you do not have a registered application. You can skip to Step 5 if you already have an application.

1. Sign in to Azure AD portal, go to **Application Registrations** and click on **New Registration**.
2. Enter a name for your application, for example *Engage cloud Email Single Tenant*.
3. Select **Accounts in this organizational directory only (Single tenant)**, unless you have multiple tenants that must use this app. Click **Register**.

Register an application ...

* Name

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

Engage cloud Email Single Tenant ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (engageiwd 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.

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

[Register](#)

- Navigate to **API Permissions** and add the **Mail.ReadWrite** and **Mail.Send** API permissions for Microsoft Graph.

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|------------------------|-------------|--------------------------------------|-----------------------|-----------------------|
| Microsoft Graph (2) | | | | |
| Mail.ReadWrite | Application | Read and write mail in all mailboxes | Yes | Granted for engageiwd |
| Mail.Send | Application | Send mail as any user | Yes | Granted for engageiwd |

- In Workload Manager, configure a mailbox with Account Type **Office365** and Access Type **Without a User**.

The screenshot shows a 'New Mailbox' configuration window. At the top, there is a title bar with 'New Mailbox' and a close button. Below the title bar, there is a 'Name' field containing 'Department mailbox' and an 'Enabled' checkbox which is checked. Underneath, there are two dropdown menus: 'Account Type' set to 'Office365' and 'Access Type' set to 'Without a user'. Below these are five text input fields: 'Email Address', 'App ID', 'App Secret', and 'App Tenant'. A blue 'Save' button is located at the bottom right of the form.

6. Enter the application ID, tenant ID, and secret for the application that you configure in the Azure portal, and click **Save**.

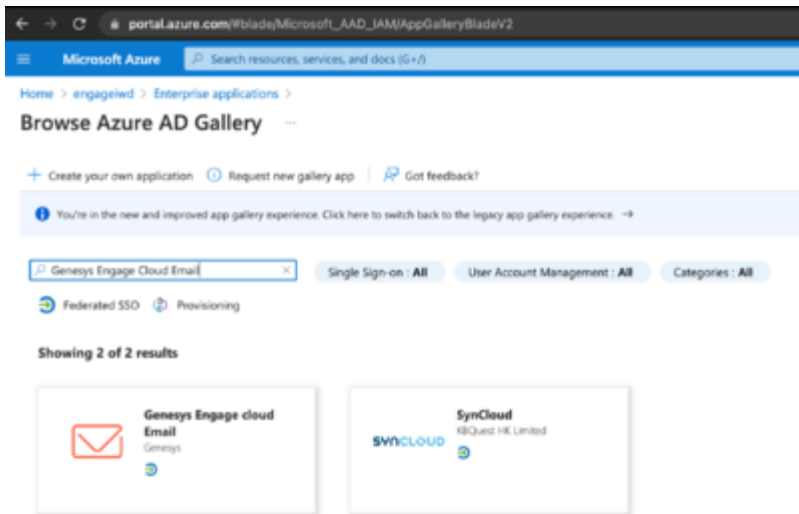
It is recommended that you follow the Microsoft documentation to limit application access to only specific mailboxes: Limiting application permissions to specific Exchange Online mailboxes.

For instructions on how to configure the Office 365 mailbox, see View, edit, and create Genesys Multicloud CX Email boxes. If you are already logged in to Office365 (for example, to access your own corporate mailbox), open Workload Manager in an *Incognito* browser window for mailbox configuration sign-in with Microsoft.

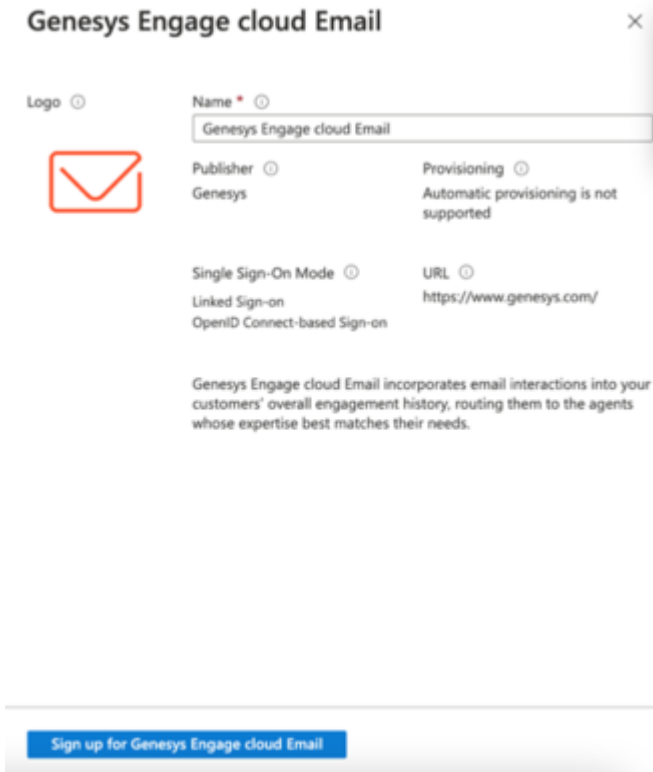
Authorization on behalf of the user

Azure AD administrators who manage the customer's Office 365 account must add the required Enterprise Application using the following steps:

1. Sign in to Azure AD portal and search for *Genesys Multicloud CX Email*.
2. Select the **Genesys Multicloud CX Email** app.



3. Click **Sign up for Genesys Multicloud CX Email.**



4. Select **Consent on behalf of your organization** and click **Accept** after reviewing the permissions requested.



Permissions requested



This app would like to:

- Read user mail
- Sign in and read user profile
- Read and write access to user mail
- Send mail as a user
- Read and write access to mailboxes via IMAP.
- Send emails from mailboxes using SMTP AUTH.
- Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)



You will be redirected to the Workload Manager login page. Close the login page as it is not required at this stage.

For instructions on how to configure the Office 365 mailbox, see View, edit, and create Genesys Multicloud CX Email boxes.