



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.

E-mail Server Administration Guide

Setting up Microsoft Azure mailboxes for OAuth 2.0 authorization

Setting up Microsoft Azure mailboxes for OAuth 2.0 authorization

Starting with version 8.5.107.06, E-mail Server supports the OAuth 2.0 authorization access to Microsoft Exchange Online API for Office 365 with the IMAP and EWS protocols. Starting with version 8.5.202.02, OAuth 2.0 support is extended to POP3 and SMTP protocols.

To set up Microsoft Azure mailboxes using the OAuth 2.0 authorization access:

1. [Create a Microsoft Azure application.](#)
2. [Configure Genesys E-mail Server.](#)
3. [Configure Proxy.](#)

Important

E-mail Server (classic) only supports EWS, POP3, and IMAP protocols and does not support the Graph API protocol. The Graph API protocol is supported by Advanced Email (powered by our IWD solution). Refer to the topic [View, edit and create Genesys Engage cloud Email boxes.](#)

Creating a Microsoft Azure application

OAuth defines the following grant types: authorization code, implicit, resource owner password credentials, and client credentials. The Genesys solution uses resource owner password credentials.

1. Follow Steps 1-8 as described in [this documentation](#) to register an Azure public client application for the mailbox(es) that will be accessed by Genesys E-mail Server. Note that a single Azure application can support all mailboxes for the same company.
2. In step 6, for entering the name in Supported account types:
 - Select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.
Note: Single-tenant accounts, **Accounts in this organizational directory only**, are also supported.
 - Leave the **Redirect URI** empty (as well as in Step 7).
3. Copy and paste the Application (client) ID and the Directory (tenant) ID into a text document for insertion during the E-mail Server configuration.

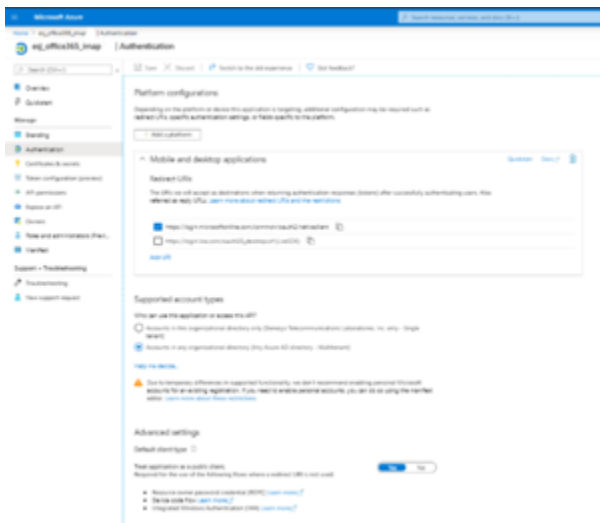
After the application is created, it should look similar to this (click to expand it):

Setting up Microsoft Azure mailboxes for OAuth 2.0 authorization



Where **esj_office365_imap** is the Azure application name.

If you open the **Supported account types** and **Redirect URIs**, it should look similar to this:



The **Application ID URI** should be empty:



Adding Application Permissions

Read through the article [Permissions and consent in the Microsoft identity platform endpoint](#) to learn about permissions and consent.

You might want to consult this document, [Configure permissions for Microsoft Graph](#), although it focuses on getting permissions for the Graph API and you must configure application permissions for Office 365 Exchange Online.

For IMAP, POP3, and EWS, the application must have the following permissions granted by the company's administrator, depending on the email protocols used:



(Click to expand)

Important

- For the EWS protocol, the Azure application must have the following permissions:
User.Read
EWS.AccessAsUser.All
- For the IMAP protocol, the Azure application must have the following permissions:
User.Read
IMAP.AccessAsUser.All
- For the POP3 protocol, the Azure application must have the following permissions:
User.Read
POP3.AccessAsUser.All
- For the SMTP protocol, the Azure application must have the following permissions:
SMTP.Send

Setting up a mailbox

The mailbox has the following special settings in the company's system:

- Multifactor authentication is disabled on the mailbox.
- The IMAP protocol is enabled (if IMAP is used).
- The POP3 protocol is enabled (if POP3 is used).
- Nothing is needed for the EWS protocol.

Configuring Genesys E-mail Server

To configure E-mail Server:

- Set the JavaMail property **mail.<type>.auth.mechanisms** (where <type> can be **ews**, **imap**, **pop3**, or **smtp**) to XOAuth2. (To disable OAuth 2.0, remove the JavaMail property.)
- Add this JavaMail property for a Microsoft Office 365/Outlook POP3 mailbox pop-client:

```
mail.pop3.auth.xoauth2.two.line.authentication.format=true
```

- [Configure options in the **smtp-client** section.](#)
- [Configure options in the **pop-client** section.](#)

Configuring the **smtp-client** section

Configure the following configuration options:

- **directory-id**—Specify the Directory (tenant) ID of the registered Microsoft Azure application for the Office 365 mailbox.
- **tenant-authority**—Specify the authority server of the registered Microsoft Azure application for the Office 365 mailbox. For Office 365, the default configuration value is `https://login.microsoftonline.com/`.
- **client-id**—Specify the Client ID of the registered Microsoft Azure application for the Office 365 mailbox.
- **scope**—Specify the access token scope. For Office 365, the default configuration value is `https://outlook.office.com/.default`.
- **token-expiry-margin-time**— Specify the amount of time an SMTP connection for the EWS/SMTP type remains connected before its access token expires and the server closes the connection.

Configuring the **pop-client** section

Configure the following configuration options:

- **directory-id**—Specify the Directory (tenant) ID of the registered Microsoft Azure application for the Office 365 mailbox in the corresponding POP client.
- **tenant-authority**—Specify the authority server of the registered Microsoft Azure application for the Office 365 mailbox in the corresponding POP client. For Office 365, the default configuration value is `https://login.microsoftonline.com/`.
- **client-id**—Specify the Client ID of the registered Microsoft Azure application for the Office 365 mailbox in the corresponding POP client.
- **scope**—Specify the access token scope. For Office 365, the default configuration value is `https://outlook.office.com/.default`.

Configuring Proxy

E-mail Server implements **Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials**. It sends the client identification and user's credentials to the Microsoft Identity Platform (IDP) to request an access token. If a proxy has been used to access Office 365, you must have additional access to the Microsoft IDP (<https://login.microsoftonline.com/>, default https port is 443) and keep the same credentials if they were created previously.

To comply with **RFC 6749**, the Microsoft IDP validates the resource owner credentials by accessing the resource owner.