

Create an Azure AD App with Graph permissions for Mail

Introduction

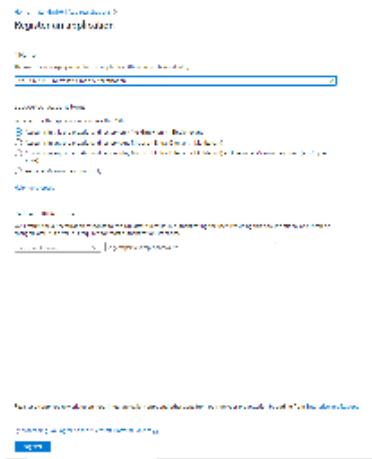
To allow applications to send e-mails as a given user or service account in Microsoft Entra, we need to configure an Microsoft Entra Active Directory application registration with the appropriate permissions.

Create an Azure AD App with Graph permissions

You can execute these steps using Azure PowerShell, the Azure CLI, or the Azure Portal. The steps required to enable Microsoft Graph SMTP authentication using the Azure Portal are described below.

Create App Registration

In the Azure Active Directory of your Tenant, navigate to App registrations and create a New registration. Choose a name and select "Register".



Create a User with permissions to use the Application

Navigate to Azure Active Directory Users and create a new User

If you already have a user which is used for the Microsoft Graph Teams Presence API App registration, you can use that user for this purpose again!

Assign the User to the Application

Navigate to the registered App configuration and into the tab "Owners" and add the User.

Home > [redacted] > jtel ACD SMTP Microsoft Graph Authentication

jtel ACD SMTP Microsoft Graph Authentication | Owners

Search

+ Add owners | Remove owners | Got feedback?

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners**
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got a second to give us some feedback? →

The users listed here can view and edit this application registration. Additionally, any user (may not be listed here) with administrative privileges to manage any application (e.g. Global Administrator, Cloud App Administrator etc.) can view and edit the application registrations. Currently, only individual users are supported as owners of applications. Assignment of groups as owners is not yet supported. If the user setting "Restrict access to Microsoft Entra ID administration portal" is set to Yes, non-admin users will not be able to use the Azure portal to manage the applications they own. [Learn more](#)

Name	Email	User name	Job Title	Type
<input type="checkbox"/>	[redacted]	[redacted]	[redacted]	Member

Grant Permissions

The Microsoft Graph SMTP Authentication requires permissions to send emails. Configure the following permissions with "Add a permission" and grant the permssions by clicking on "Grant admin consent for <Tenant Name>". The permission "User.Read" is added by default and should not be removed.

Microsoft Azure

Home > jtel GmbH | App registrations > jtel ACD SMTP Microsoft Graph Authentication

jtel ACD SMTP Microsoft Graph Authentication | API permissions

Search

Refresh | Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission | Grant admin consent for jtel GmbH

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				...
Mail.Send	Application	Send mail as any user	Yes	Granted for jtel GmbH ...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Create a Client Secret

Navigate to Certificates and Secrets and click on "New client secret" to add a new secret.

Expiry



As this secret will expire after the configured amount of time, please make note of this because it must be changed in the Client Master Data settings in your jtel ACD after being renewed in the Microsoft Entra Active Directory.

Configuring Client Master Data

The newly **Tenant ID**, as well as the Application ID (**Client ID**) and Client Secret (**Secret Hash Value**) are now configured in the jtel portal. The E-Mail Server and user also have to be changed, if you are switching to Office 365.

The configuration is added as Client Administrator in the Menu [Client Master Data](#) in the email tab.

E-Mail Sender	The E-Mail address which should be displayed as the sender
E-Mail Server	smtp.office365.com :587
Tenant ID	The Tenant ID of your Microsoft Entra AD
Client ID	The Client ID of the new registered Application
E-Mail User	The new user which is the owner of the registered Application
E-Mail Password	The Secret Hash Value