

Teams - jtel Microsoft Azure Login

Introduction

This page explains the required configuration prior to using the jtel Microsoft Azure Login feature. Creation of the app registration as well as configuration in your jtel portal.

Configuration

Create Registered Application in Azure

Login as Administrator in Azure portal and go to Azure Entra ID. Open the page App registrations and press 'New registration'

Choose a name and set the redirect URL. We will use 'myjtelportal' in the example.

<https://myjtelportal.jtel.de/CarrierPortal/azurelogin>

Afterwards press 'Register'.

Home > jtel GmbH | App registrations >

Register an application ...

* Name

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

jtel Login ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (jtel GmbH 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://myjtelportal.jtel.de/CarrierPortal/azurelogin> ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

Register

<https://portal.azure.com/#>

Generate secret key and save information

Copy the **<Application (client) ID>**, as well as the **<Directory (tenant) ID>** and save that information for later.

Go to 'Certificates & Secrets' and press 'New client secret'. Add a description and your desired expiry date. Make note of this expiry date as you will have to generate a new Secret Key and change the jtel configuration before it runs out. If you do not, the feature will stop working immediately after expiry.

After pressing 'Add' to create the secret, make note of the **<Secret Value>** for later.

The secret value can only be accessed once after creation in azure. If you do not save it but need it again later, you will have to create a new secret.

Create configuration in jtel

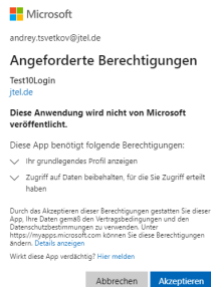
We will now create the configuration in jtel. In your jtel portal as a client administrator, go to 'Menu User Data Client Master Data Parameters'.

Press 'Add' to create a new parameter, add the parameter Name and Value and press 'Save'. The following three parameters are created:

Parameter Name	Value
User.Authentication.Azure.Authority	<a href="https://login.microsoftonline.com/<Directory (tenant) ID>">https://login.microsoftonline.com/<Directory (tenant) ID>
User.Authentication.Azure.ClientsID	<Application (client) ID>
User.Authentication.Azure.Secret	<Secret Value>

Prevent First Login Dialogue

To prevent the following dialog at first login



the following API permissions must be set. Go to 'API permissions' and press 'Add a permission'. Click on Microsoft Graph and Delegated permissions. Use the filter and checkbox, as well as the button 'Add permission' to add the permissions to your registered application.

Afterwards, press 'Grant admin consent for <Your company name>' and 'Yes' to consent to the configured permissions.

+ Add a permission		✓ Grant admin consent for jtel GmbH		
API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3)				...
Group.Read.All	Delegated	Read all groups	Yes	✓ Granted for jtel GmbH ...
openid	Delegated	Sign users in	No	✓ Granted for jtel GmbH ...
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for jtel GmbH ...

See also: <https://learn.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience>

Force Azure Login

If required for your organization, the login via Azure can be set to mandatory in your jtel ACD. To ensure that all logins to your jtel ACD are done via jtel Microsoft Azure Login, configure the following parameter

In your jtel portal as a client administrator, go to 'Menu User Data Client Master Data Parameters'.

Press 'Add' to create a new parameter, add the parameter Name and Value and press 'Save'. With Value 1 jtel Microsoft Azure Login will be mandatory for all users within the client. Value 0 or leaving the parameter unconfigured in the system will allow other methods of authentication.

Parameter Name	Value
User.Authentication.Azure.Force	1