Teams - Presence Status Connector

Introduction

This page provides a guide to the required configuration to activate the jtel Teams Presence API in your jtel system.

The API functions are described in detail at this page.

Azure Configuration - Prerequisites

The configuration should be done by a Azure AD Tenant Administrator. The configuring user must have access to the following:

- Active Directory Administration
- User Administration
- Role Administration
- API permission Administration

Azure Configuration - Step by Step Guide

Microsoft Documentation

Information on this page was extracted from Microsoft and is subject to changes from Microsoft. Please refer to the following Microsoft documentation page if you are having any issues with the described steps:

https://learn.microsoft.com/en-us/graph/auth-register-app-v2

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".

Home > jtel GmbH | App registrations >

Register an application

* Name

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

jtel Teams Presence API registration

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 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.

Select a platform | e.g. https://example.com/auth

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

Create a User with permissions to use the Application

Navigate to Azure Active Directory Users and create a new User

Additional User Configuration

The users default password must be changed during first login. Log into the account on for example a different browser to complete a first-login and set a new password.

Make sure the users password does not contain any of the following special characters:

[]

<>

?

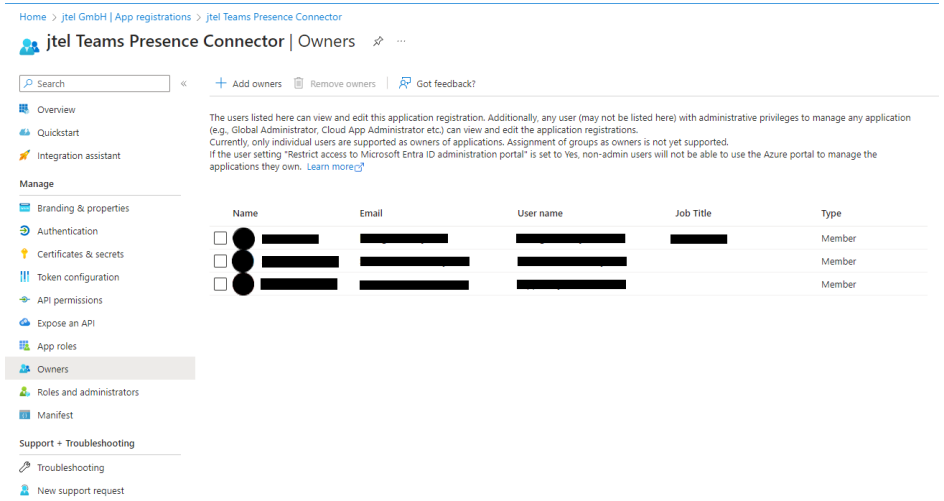
#

&

Depending on your Azure AD configuration and security, the users password might reset by default after a defined amount of time has passed. If you do not wish to disable this for this User, make sure to keep track of the date, as the configuration in the jtel Teams Presence Aggregator contains the password of the user and must be changed accordingly.

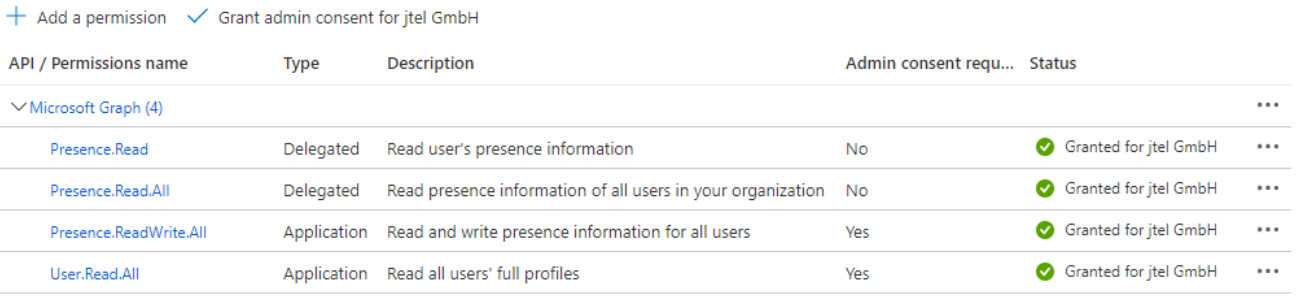
Assign the User to the Application

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



Grant Permissions

The Presence Connector requires permissions to read the users presence status. Configure the following permissions with "Add a permission" and grant the permssions by clicking on "Grant admin consent for <Tenant Name>".

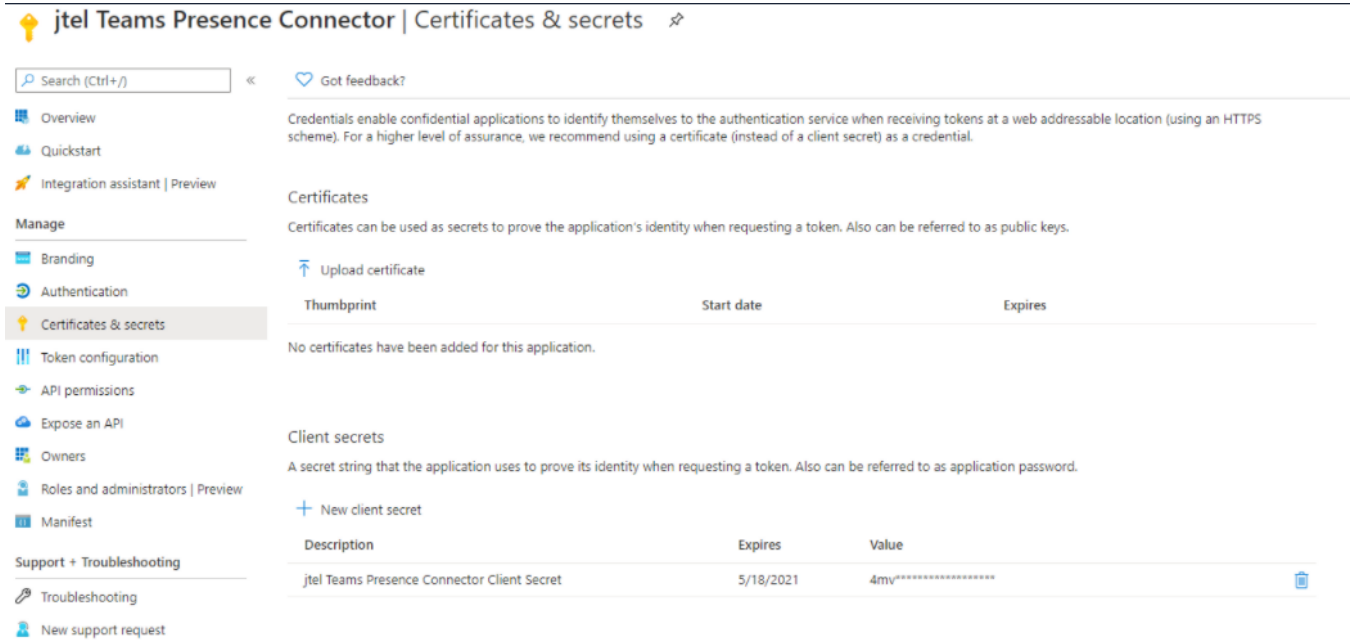


Create a Client Secret

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 jtel Teams Presence Aggregator after being renewed in the Azure AD.



Gather all Information

Please provide all information on the following table to the contact who will be configuring the jtel Teams Presence Connector in your jtel ACD:

Note: The Secret Value is required, not the Secret ID.

Data	Value
Application (client) ID	
Directory (tenant) ID	
Secret Value	
User email address	
User password	