# up2talk OIDC Setup
# Microsoft

Setup Guide

October 2023

Your audio. Our solution.

2wcom

# Contents


1 About this guide ..... 3

2 Registering up2talk ..... 3

3 Configuring platform settings ..... 4

4 Configuring API permissions ..... 4

5 Configuring claims and tokens ..... 5

6 Adding a client secret ..... 6

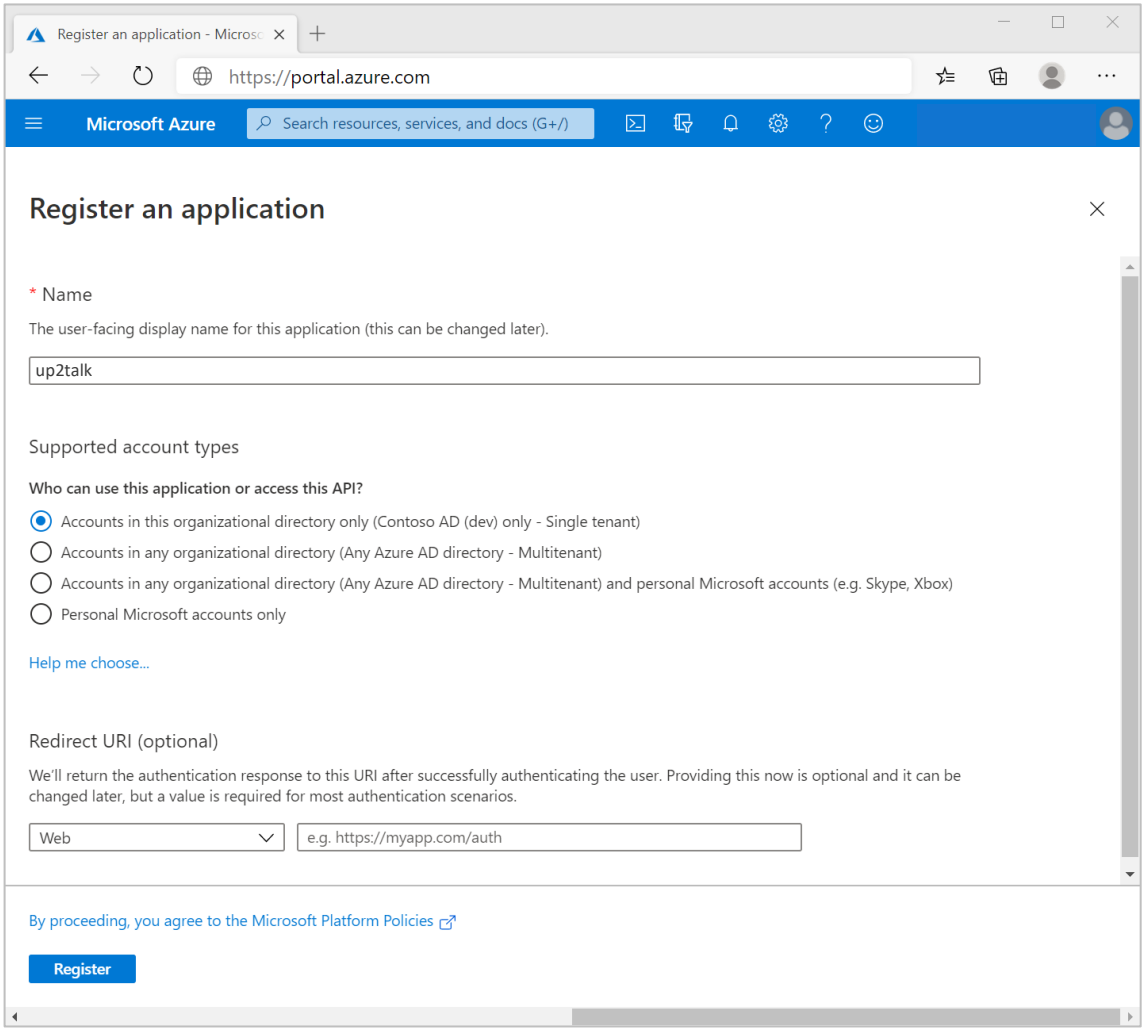
7 Configuring users and groups ..... 7

# 1 About this guide

To log in to the up2talk app and ensure that the OIDC token contains groups with their cloud name, you must configure Microsoft Azure as an OpenID Connect provider. This guide shows you how to register up2talk with the Microsoft identity platform and which settings you must configure.

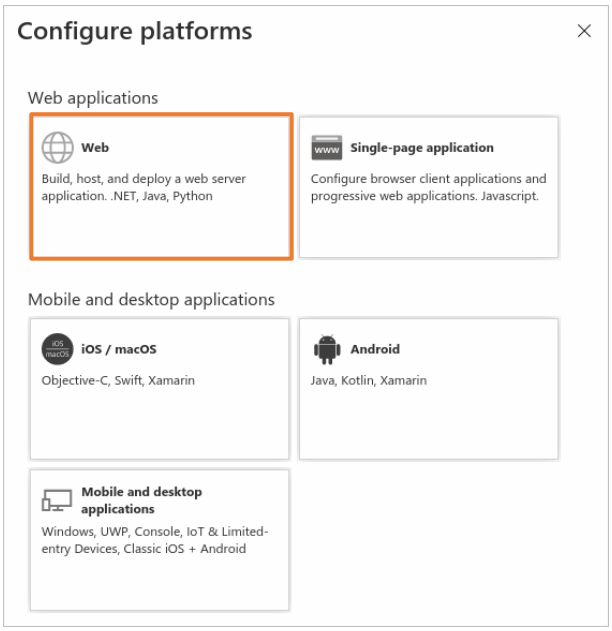
# 2 Registering up2talk

1. Log in to your Microsoft Azure Company as at least a Cloud Application Administrator.
2. Navigate to **Identity → Applications → App registrations** and select **New registration**.
3. Enter a display **Name** for your application. We recommend the Name “up2talk”.
4. Click **Register**.



# 3 Configuring platform settings

1. Navigate to **Authentification** and click **Add a platform**.
2. Select the **Web** tile.




3. Enter the following **Redirect URI**:
   https://<customer_namespace>.up2talk.de/auth/self-service/methods/oidc/callback/microsoft
   Make sure to insert your customer namespace in the URI that you have received from 2wcom.
4. Make sure that the checkboxes for **Acces token** and **ID token** are selected.
5. Click **Cofigure** to save the settings.

# 4 Configuring API permissions

You must grant the up2talk app a set of API permissions to operate correctly.

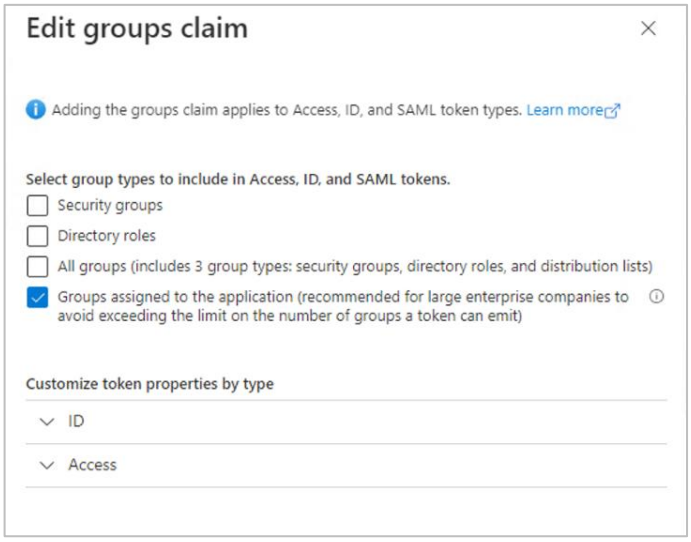
1. Navigate to **API permissions → Add a permission → Microsoft Graph**.
2. Select **Delegated permissions**.
3. Under **Select permissions**, select the following permissions:

| | |
|---|---|
| email | View user's email address |
| Group.Read.All | Read all groups |
| offline_access | Maintain access to data you have given it access to |
| openID | Sign users in |
| profile | View user's basic profile |
| User.Read | Sign in and read user profile |

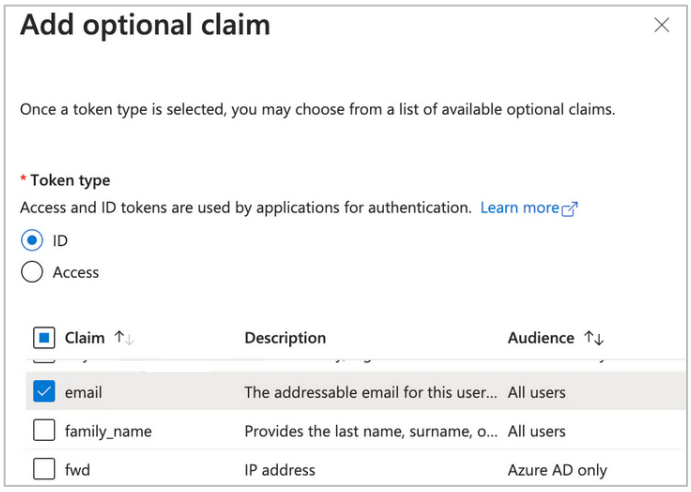
4. Click **Add permissions** to save the settings.
5. Under Configured permissions, grand admin consent for the **Group.Read.All** permission.

# 5 Configuring claims and tokens

1. Navigate to **Token configuration**.
2. Click **Add groups claim**.
3. Under **Select group types to include in Access, ID, and SAML tokens**, activate the **Groups assigned to the application** checkbox.




4. Click **Add**.
5. Click **Add optional claim**.
6. Under **Token type**, select **ID**.
7. In the **Claim** list, select **email**, **family_name**, **given_name**, **preferred_username**, and **upn**.




8. Click **Add**.
9. Navigate to **Manifest**.

10. In the `optionalClaims` section, add `cloud_displayname` to `additonalProperties` of `groups`:

```
{
   ...
   "optionalClaims": {
      "idToken": [
         ...
         {
            "name": "groups",
            "source": null,
            "essential": false,
            "additionalProperties": [
               "cloud_displayname"
            ]
         }
      ]
      ...
   }
}
```

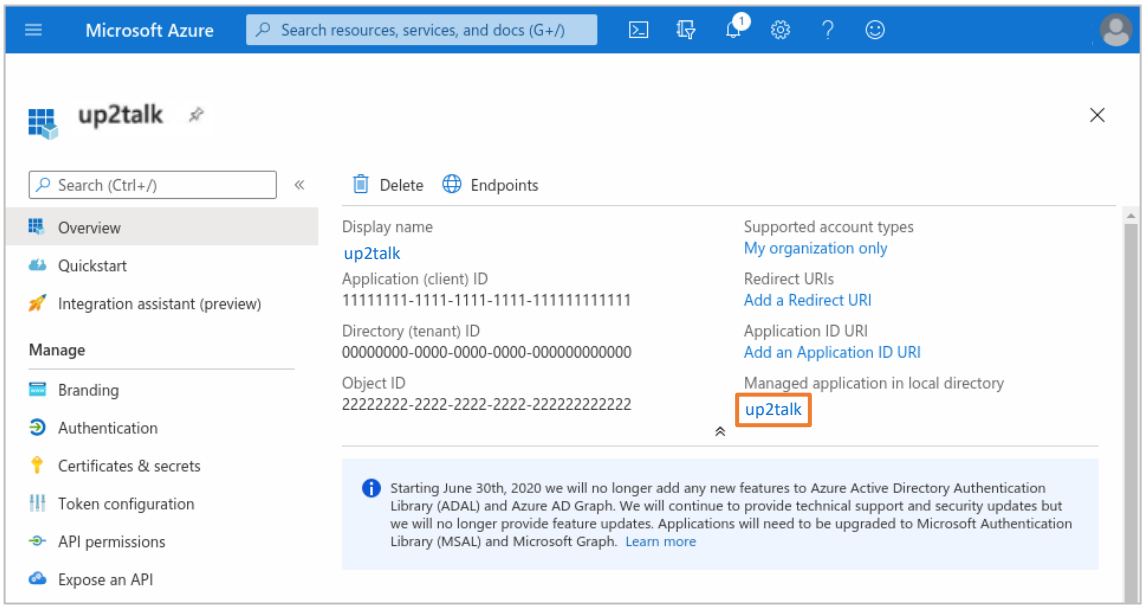
11. Click **Save**.

# 6 Adding a client secret

1. Navigate to **Certificates & secrets**.
2. Under **Client secrets**, click **Add client secret**.
3. Enter any name for the secret, for example “up2talk_oidc_secret”.
4. Select an expiration for the secret or specify a custom lifetime.
5. Click **Add**.
6. Record the secret *value*.
7. Navigate to **Overview**. Record the *Client ID* and the *Tenant ID*.
8. Send the *Client ID*, the *Tenant ID*, and the generated secret value to the up2talk administrator of 2wcom.

# 7 Configuring users and groups

1. Navigate to **Overview**.
2. Click on the **Managed application in local directory** link.




3. Navigate to **Users and groups → Add user/group**.
4. Add all groups that should be mapped to roles in up2talk. Note that there are separate groups for Microsoft Teams and email distribution lists.
5. Click **Select** to save the settings.

⇒ You have configured Microsoft Azure as an OpenID Connect provider. You can now log in to up2talk with a Microsoft account and configure the group settings for your up2talk instance.