CANDI

ADVANCED BUSINESS AND DIGITAL SOLUTIONS

Configure AAD for your portal

INCIDENT MANAGEMENT

TEAM CANDI

Contents

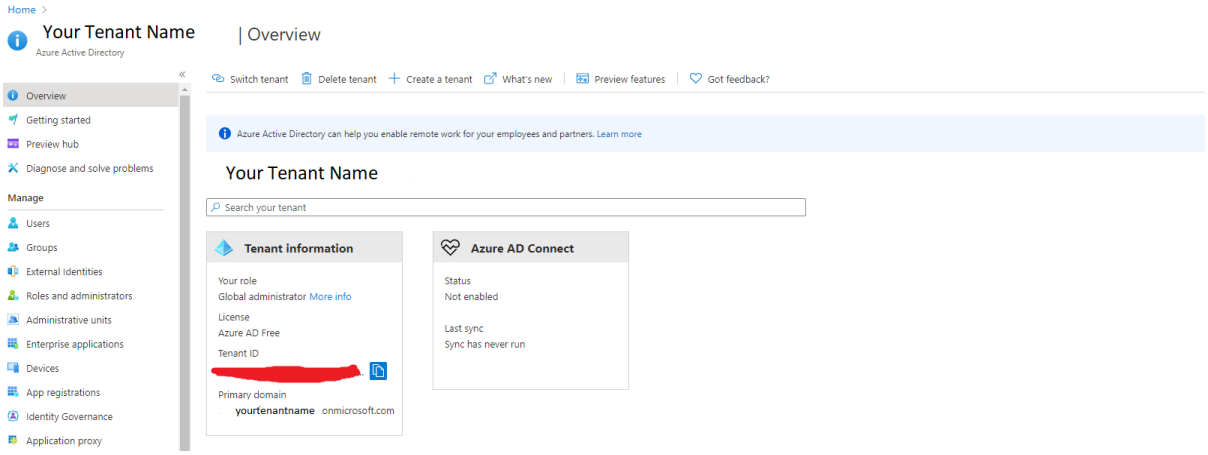
Follow these steps to successfully enable Azure Active Directory with Incident Management Application.

1. Steps before Application Creation

1.1. Create an Azure Active Directory B2B Tenant

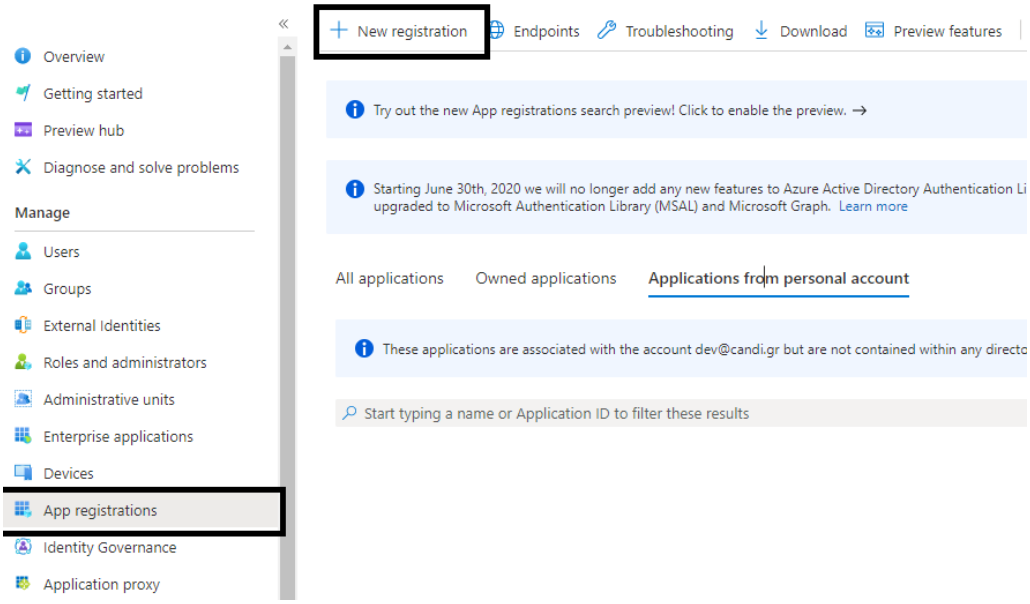
Our portal provides **Azure Active Directory B2B** as an External Login Provider.
Your Azure Subscription gives you by default an Azure Active Directory Tenant. If you want, you can use this subscription to connect with our portal. In case you need another tenant follow the instructions in the link down below and create an **Azure Active Directory B2B** tenant.
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant

Go to your AAD overview page. Looks like this:

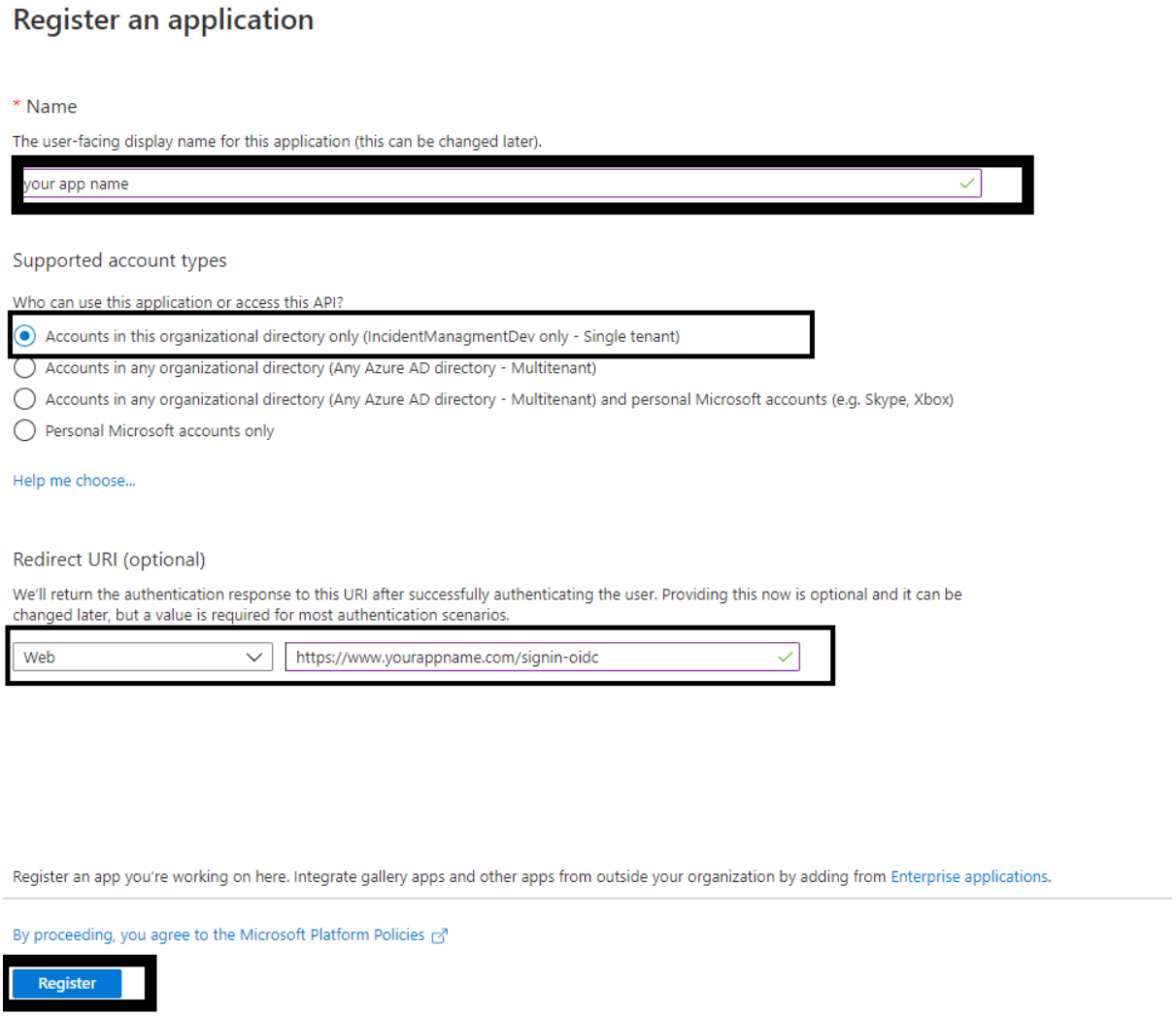


Copy **Primary Domain** and **Tenant ID** and insert them to the application creation wizard.
After that, you must go to **App Registration** and add **New Registration.**

1.2. Create New App Registration



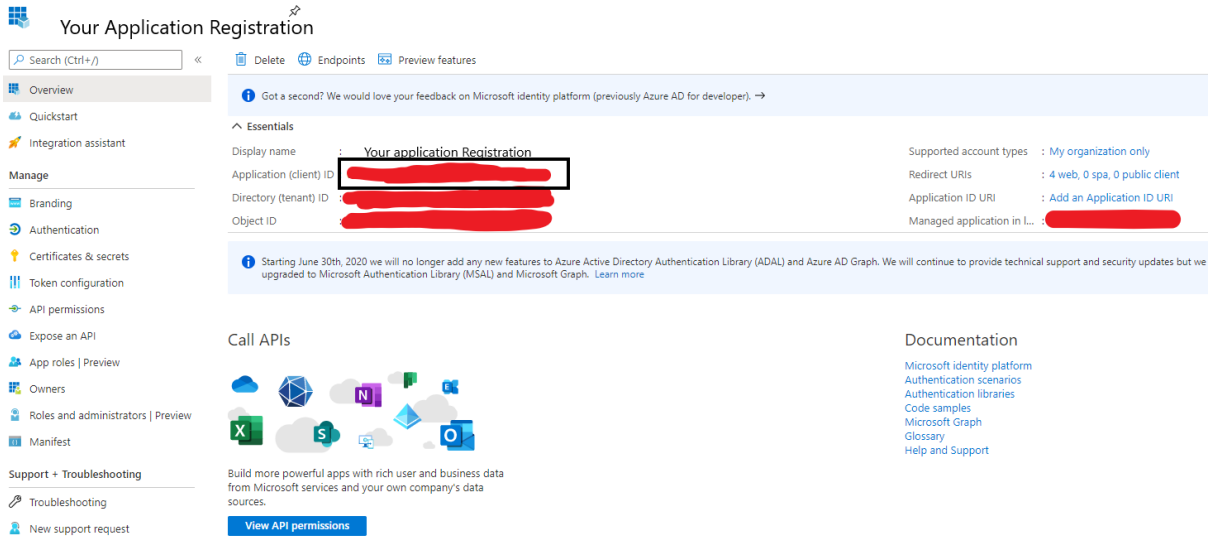
Click on **New Registration** and fill the form like this image down bellow



Name your application as you wish. Choose **Accounts in this organizational directory only (IncidentManagmentDev only - Single tenant)** and add **https://<www.yourappname.com>/signin-oidc** in redirect url. Finally **Register** your application

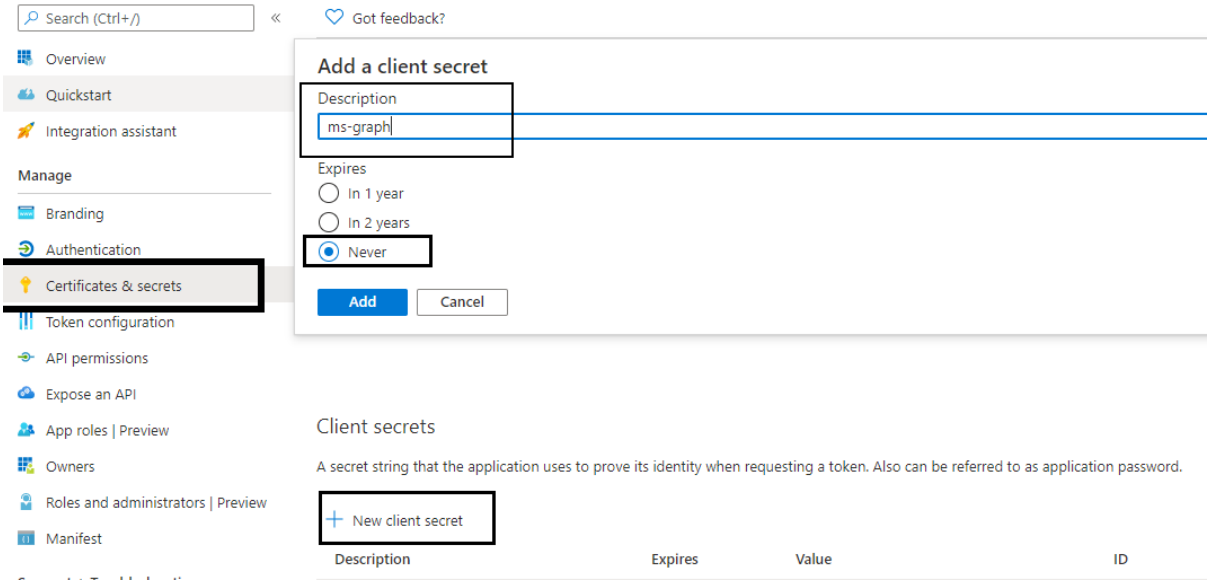
**Note: After the first initialization, your application url will look like <yourappname>.azurewebsites.net. Follow this documentation if you want to create a custom DNS*
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain

After application registration go to overview of this app registration.



Copy **Application Id** and insert it to the application creation wizard.
The final step you will need for the application wizard creation, is to generate a **Client Secret**

1.3. Create New Secret



- Go to **Certificates & secrets.**
- Click **New Client Secret.**
- Name **Description** “ms-graph”.
- Select **Never** for the Expiration.
- Click **Add**

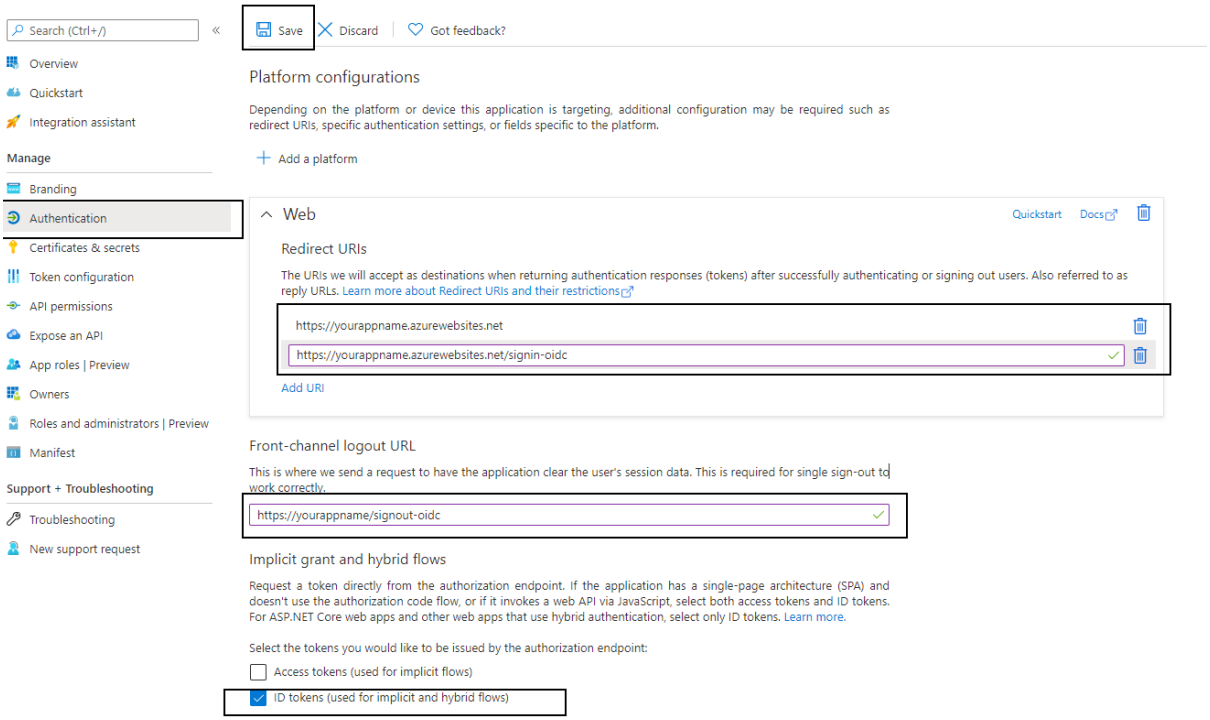
Copy and store somewhere safely client **Value.** If you lose it, you can’t retrieve it after!!
Also insert it to the application creation wizard.
Finish the application creation wizard and follow post-creation steps.

2. Post-Creation Application Steps

2.1. Authorization

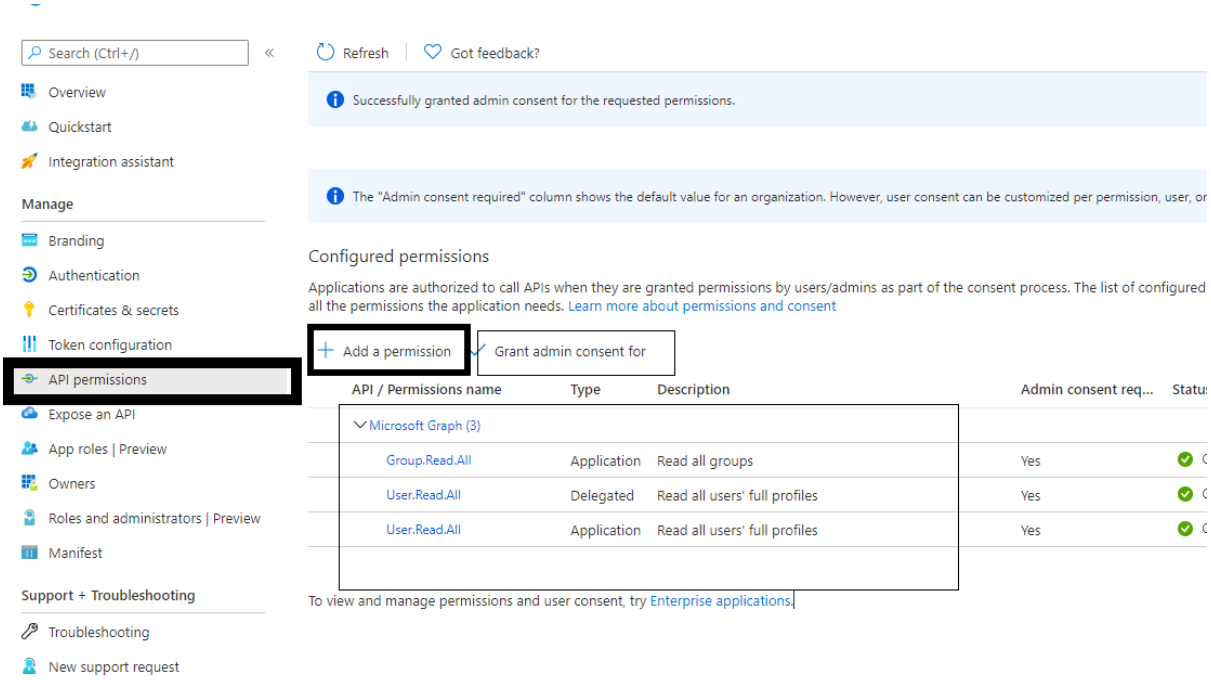
Congratulations for creating your application. We have some few things to do, to be ready to use Azure Active Directory as an external provider.

- Go to the app registration of our application and click on **Authentication.**
- Add **Redirect Urls** (check the image down below)
- Add **Front-channel logout URL**
- Select **ID tokens (used for implicit and hybrid flows)**
- Set **Allow public client flows** to **NO**
- Click Save



2.2. API Permissions

After that you must go to **API permissions** and give the following Permissions to the application (check the image down below). Add them and grand access to enable them (You must be the administrator of this tenant)

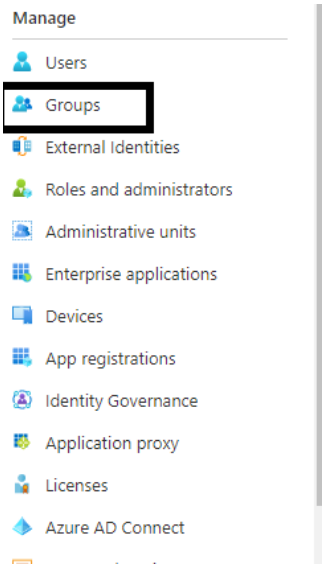


The mandatory API permissions are:

- **Microsoft Graph: Application Permissions -> Group -> Read All**
- **Microsoft Graph: Application Permissions -> User -> Read All**
- **Microsoft Graph: Delegated Permissions -> User -> Read All**

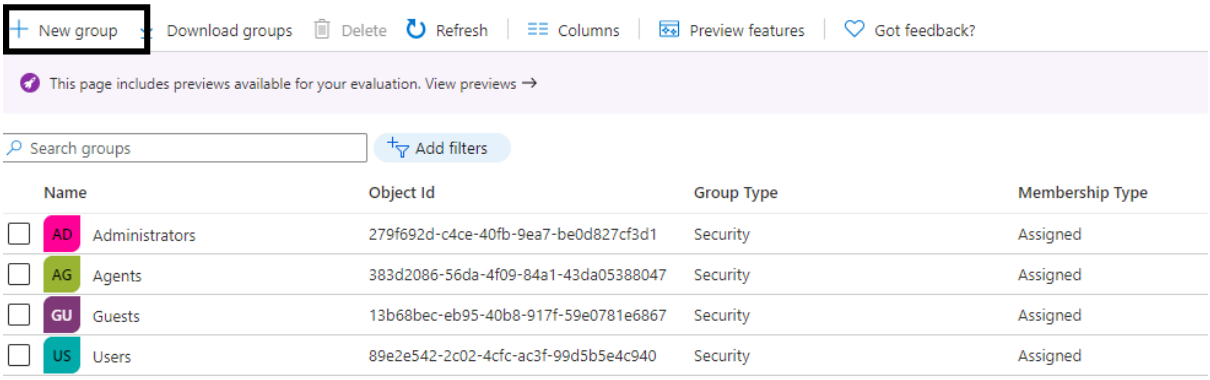
2.3. Users Configuration

Go to the Azure Active Directory Manage -> Groups



Create the following 4 groups as Group Type **Security :**

- **Administrators**
- **Agents**
- **Guests**
- **Users**



Finally, you must populate your band new Azure Active Directory with your users. Go to application documentation for more information about User's Tab fields.

Portal initial set up

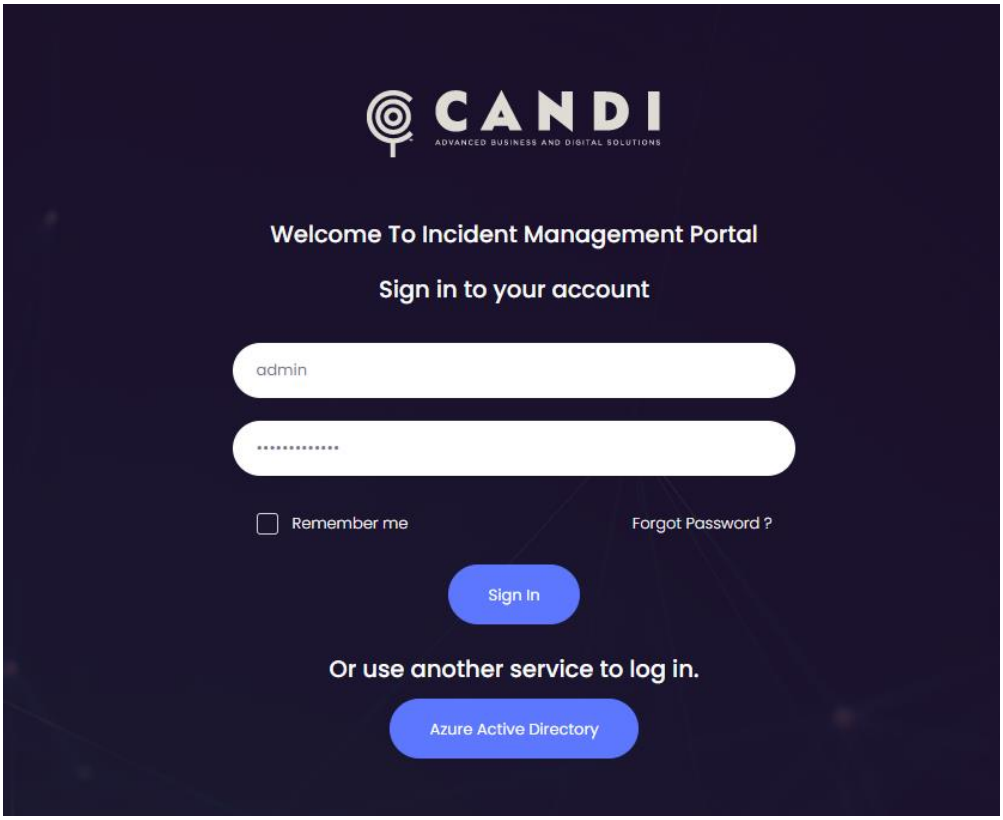
Follow these steps to successfully configure your Incident Management Application.

3. Steps before using the Application

3.1. Log in with default admin

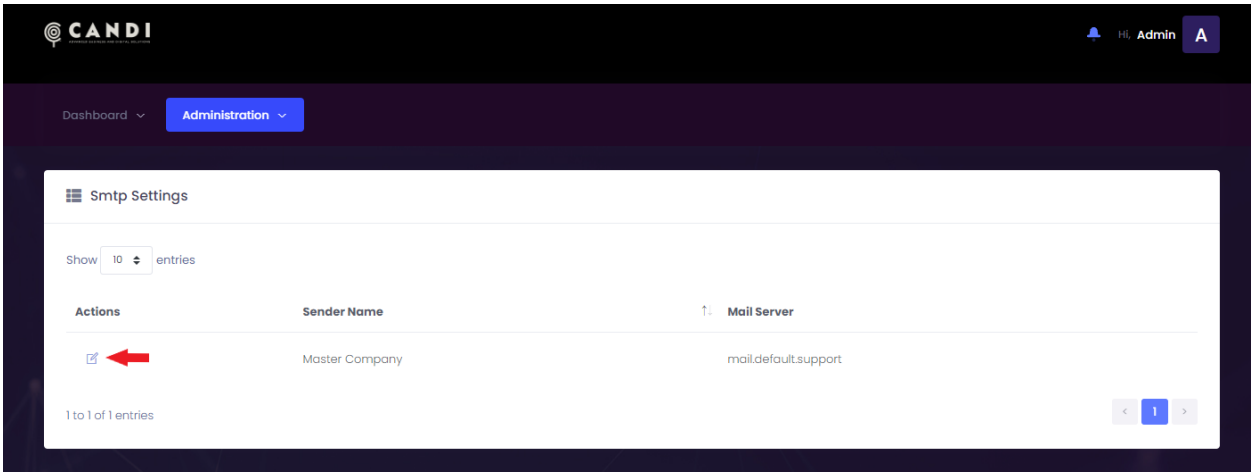
On your log in screen fill the username and the password and hit ‘Sign in’ button.

Username: admin
Password: Administr@t0r

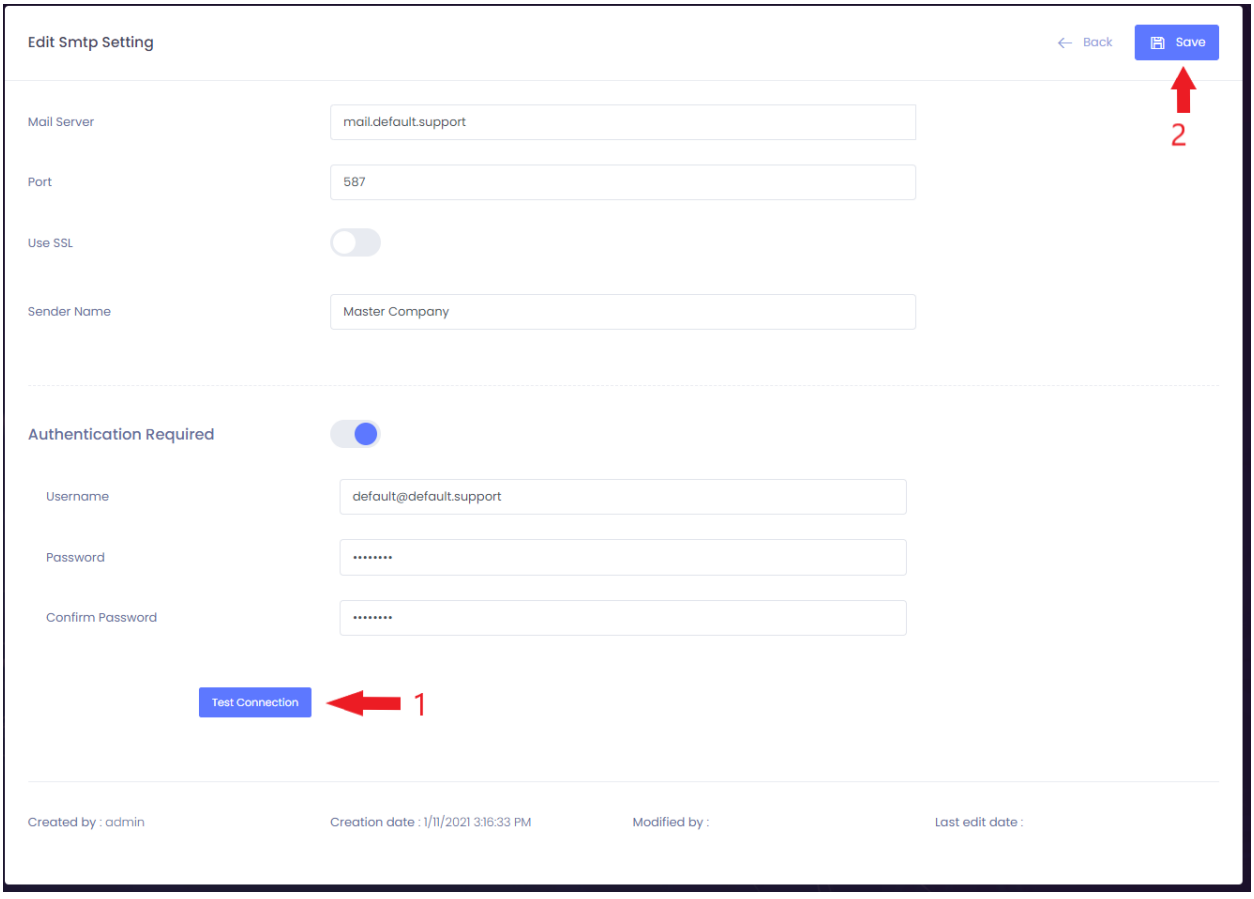


3.2. Set up your Smtp Settings

At Administration -> Portal Settings -> Smtp Settings, press the edit button.

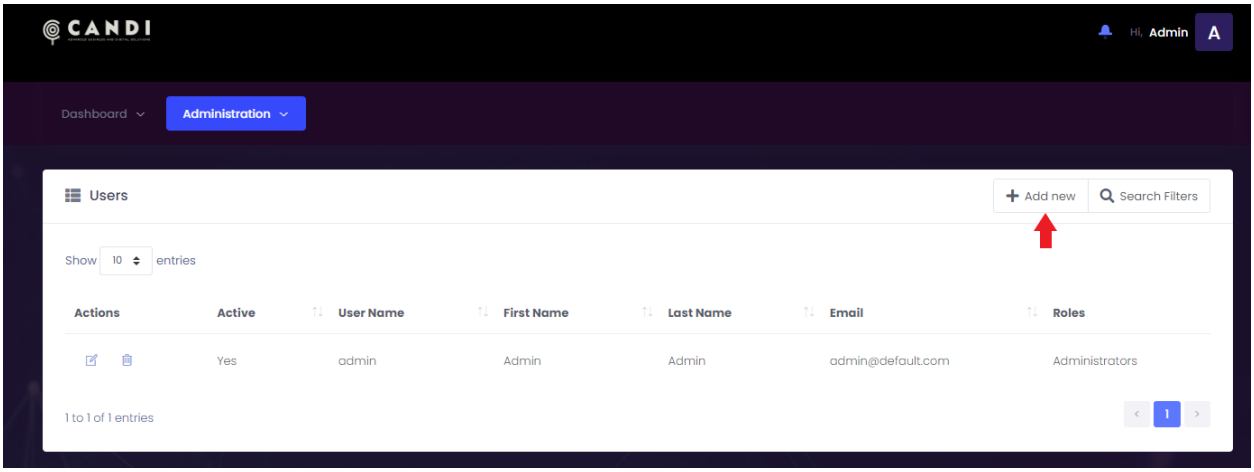


Change the settings and add your smtp that will send the appropriate emails to users, Test Connection (Button 1) if the test was successful press Save (Button 2).

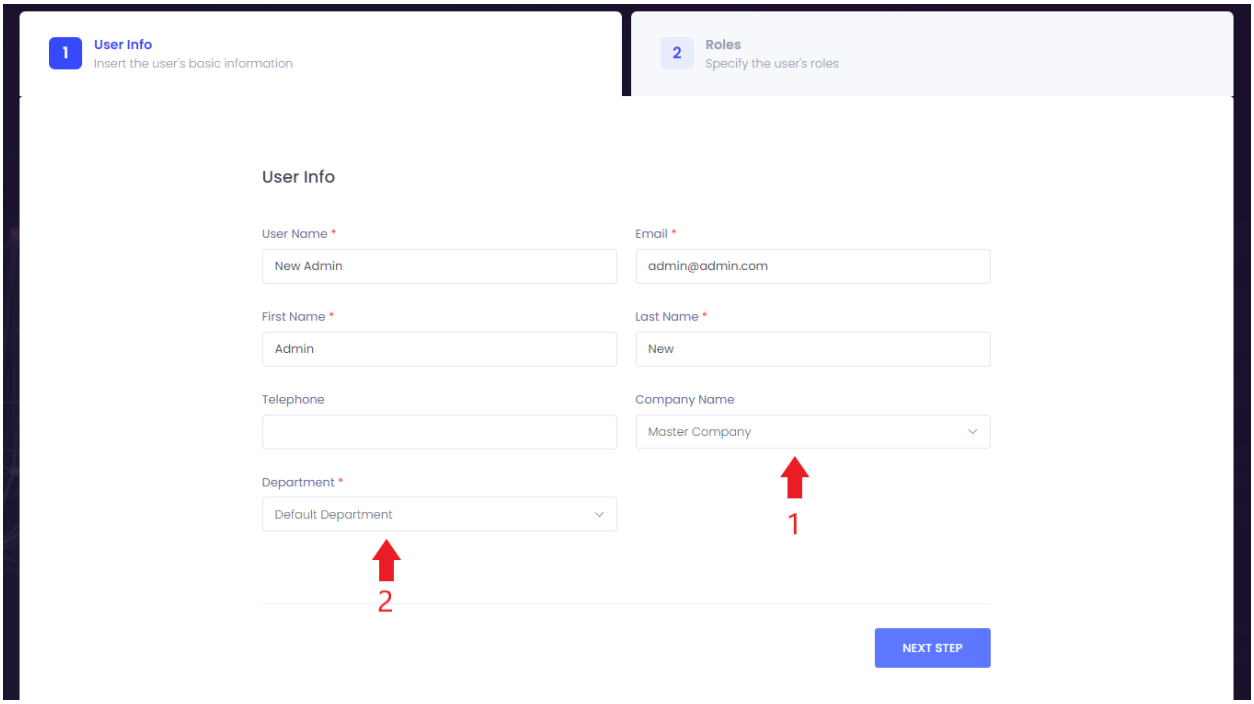


3.3. Create your Portal Administrator

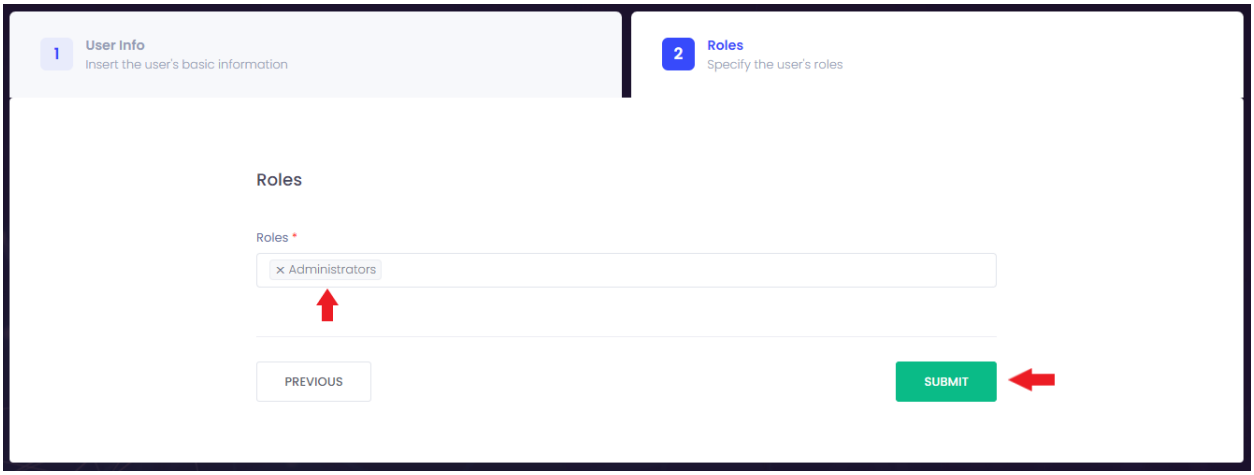
At Administration -> User click the '+ Add new' button



Fill the form with administrator's information, as Company Name select the 'Master Company' and as Department select the 'Default Department' and press Next.

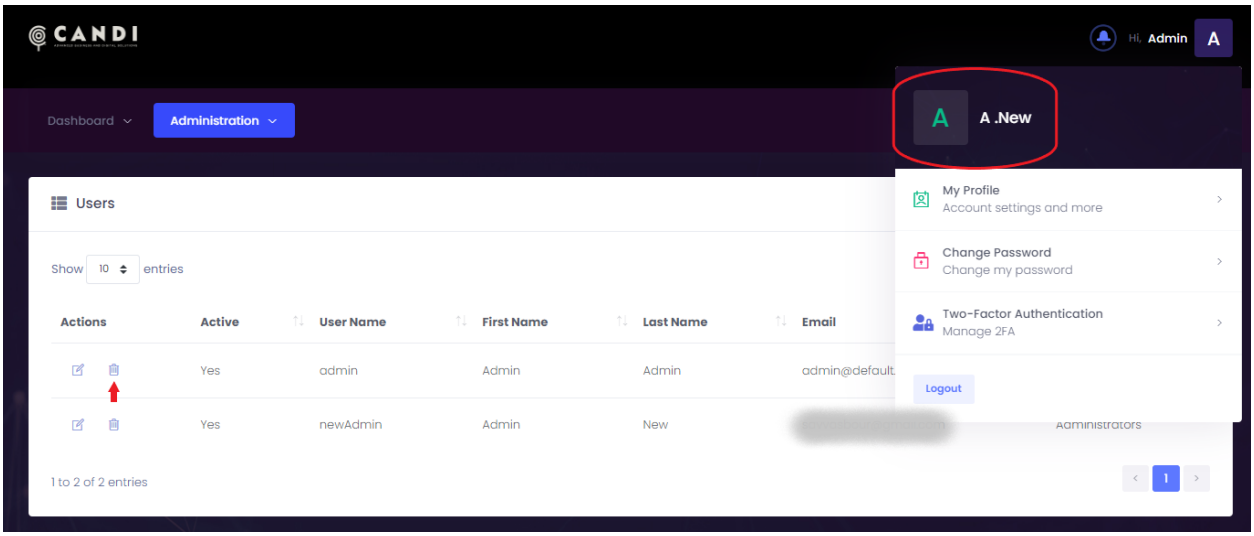


At the Roles section select ‘Administrators’ role and click submit.



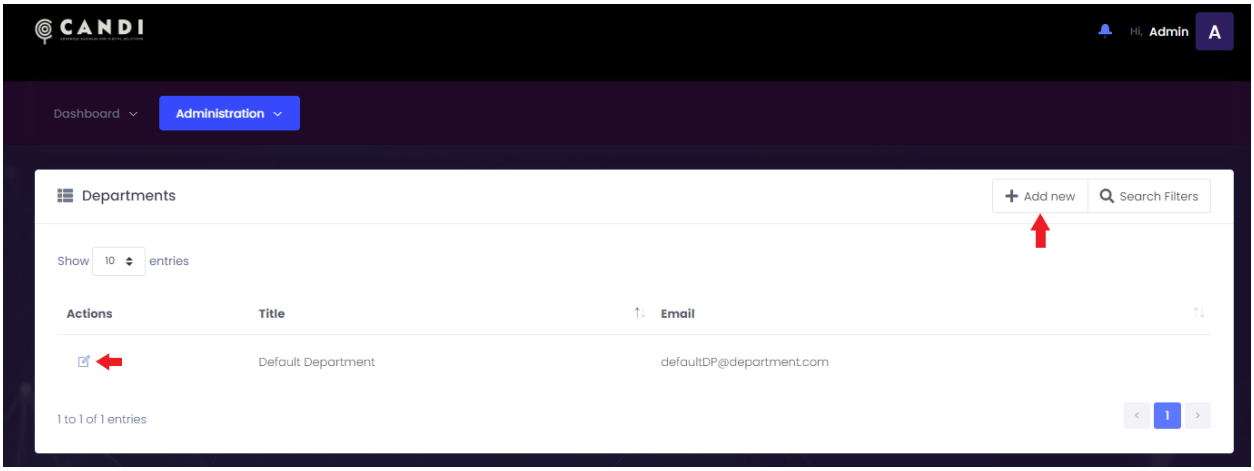
After the success of creation an email will be send to the email that was filled to complete the invitation.

After the completion of the invitation (your admin is created successfully) log in with the new account you created and delete the default admin before you move to next step.



3.4. Edit the Default Department

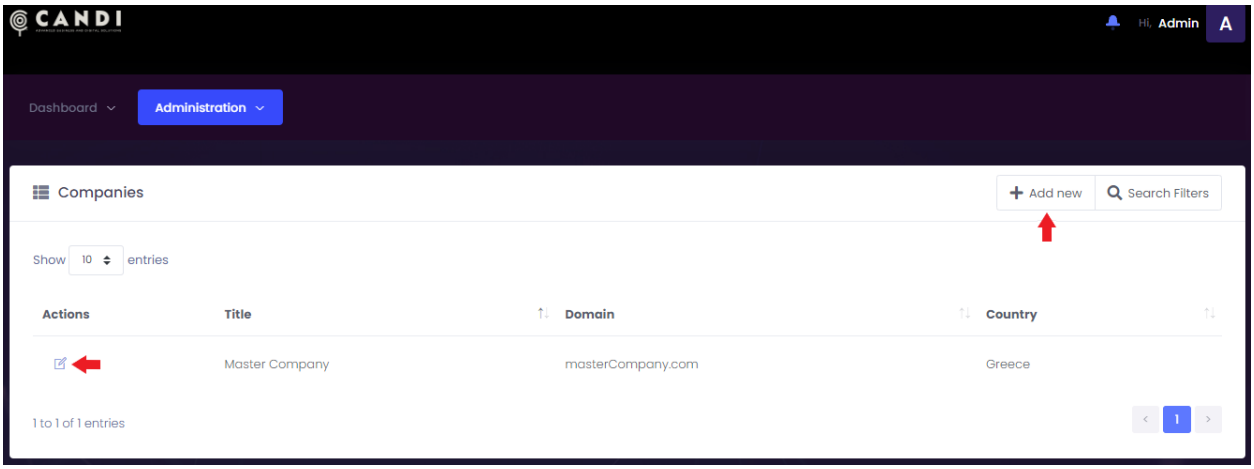
At Administration -> Department click the edit button of ‘Default Department’



Edit the 'Default Department' to match with your Department in Azure AD and add more if you have.

3.5. Edit the Default Company

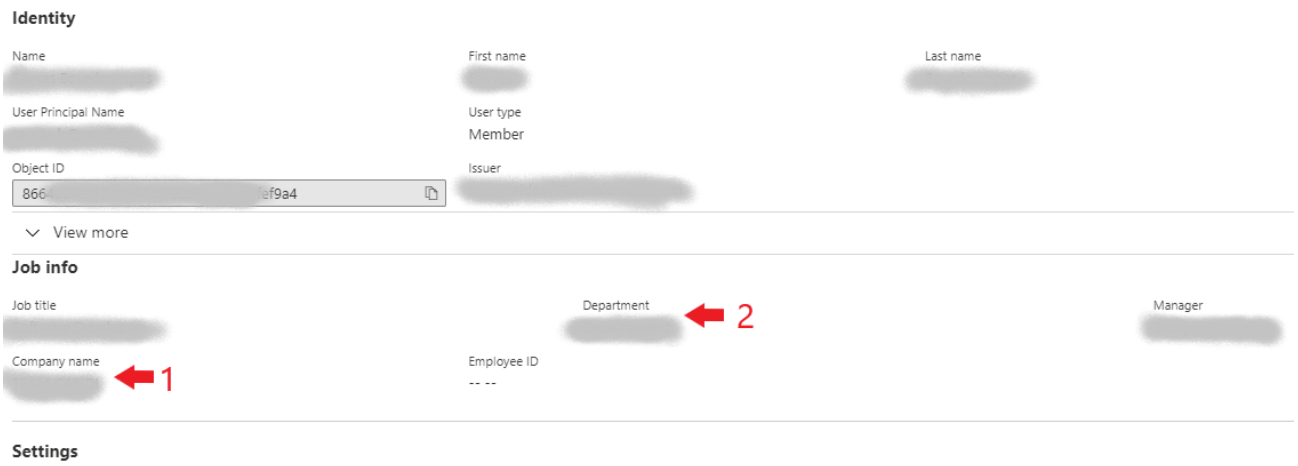
At Administration -> Company click the edit button of ‘Master Company



As Title of ‘Master Company’ you should write the exact name of the Company that Azure AD users have in company name. Then you can add more Companies that will be your 'Client Companies'.

This picture is from the Azure Active Directory.

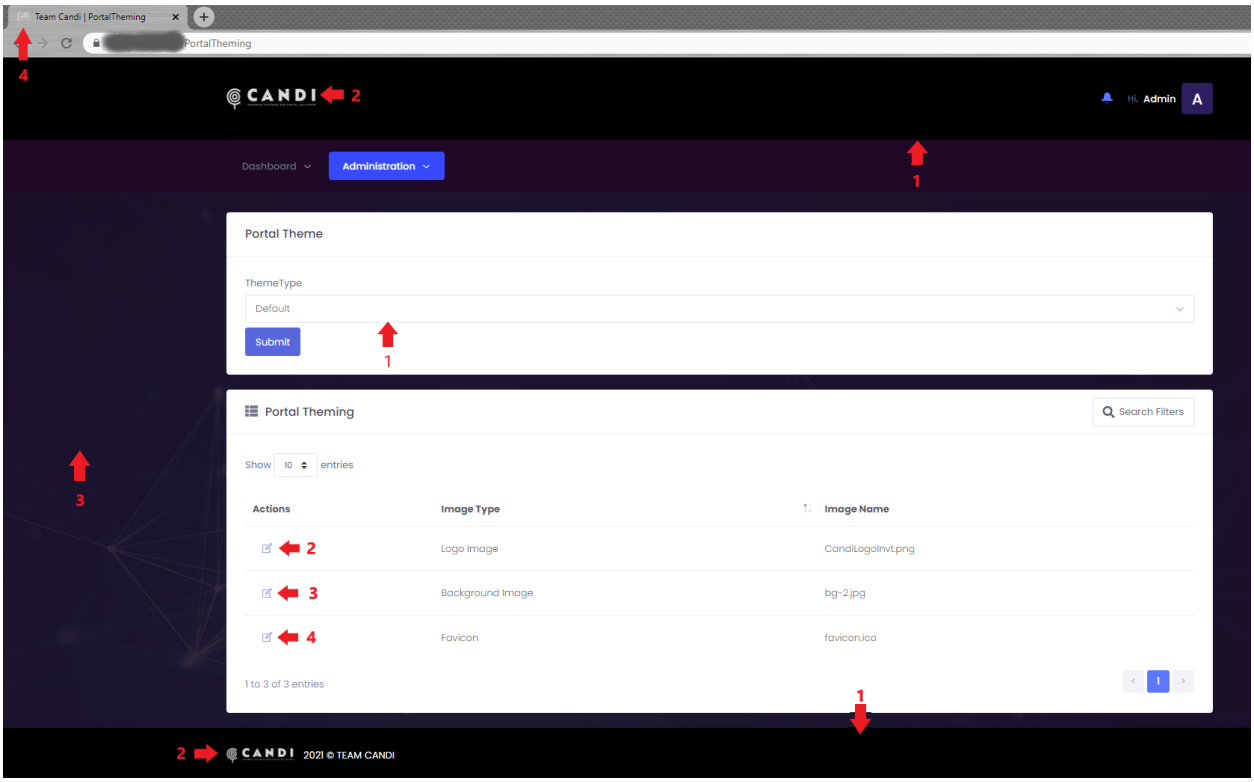
The ‘Master Company’ Title should be the same as the users have in the Company name field (1) in Azure AD and the department should be the same with the Department field (2). (only ‘Master Company’ Users can have Department).



3.6. Edit the Theme and Style of Portal

At Administration -> Portal Settings -> Portal Theme.

Number 1: you can change the Theme (Dark Light),
Number 2: you can change the Logo,
Number 3: you can change the Background of the entire Portal,
Number 4: you can change the favicon of the browser tab.



3.7. Edit the Meta Tags and Metadata

At Administration -> Portal Settings -> MetaTags you can change the Meta Tags and Metadata of the portal.

CANDI

ADVANCED BUSINESS AND DIGITAL SOLUTIONS

Custom Development & Business Solutions

Cross Platform Mobile Applications

AI & IoT

Collaboration & Reporting

TEAM CANDI | 2A Argiroupoleos Str. Kallithea, 17676 Greece | +30 211 999 4800 | https://candi.gr | info@candi.gr