



# CANDI

ADVANCED BUSINESS AND DIGITAL SOLUTIONS



Custom Development &  
Business Solutions



Cross Platform  
Mobile Applications



AI & IoT



Collaboration &  
Reporting

## Configure AAD for your portal

INCIDENT MANAGEMENT

TEAM CANDI



Contents

1.	Steps before Application Creation .....	3
1.1.	Create an Azure Active Directory B2B Tenant .....	3
1.2.	Create New App Registration.....	3
1.3.	Create New Secret .....	5
2.	Post-Creation Application Steps .....	6
2.1.	Authorization .....	6
2.2.	API Permissions.....	7
2.3.	Users Configuration .....	7
3.	Steps before using the Application .....	9
3.1.	Log in with default admin .....	9
3.2.	Set up your Smtip Settings.....	10
3.3.	Create your Portal Administrator .....	11
3.4.	Edit the Default Department .....	13
3.5.	Edit the Default Company.....	13
3.6.	Edit the Theme and Style of Portal .....	14
3.7.	Edit the Meta Tags and Metadata .....	14

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

## 1. Steps before Application Creation

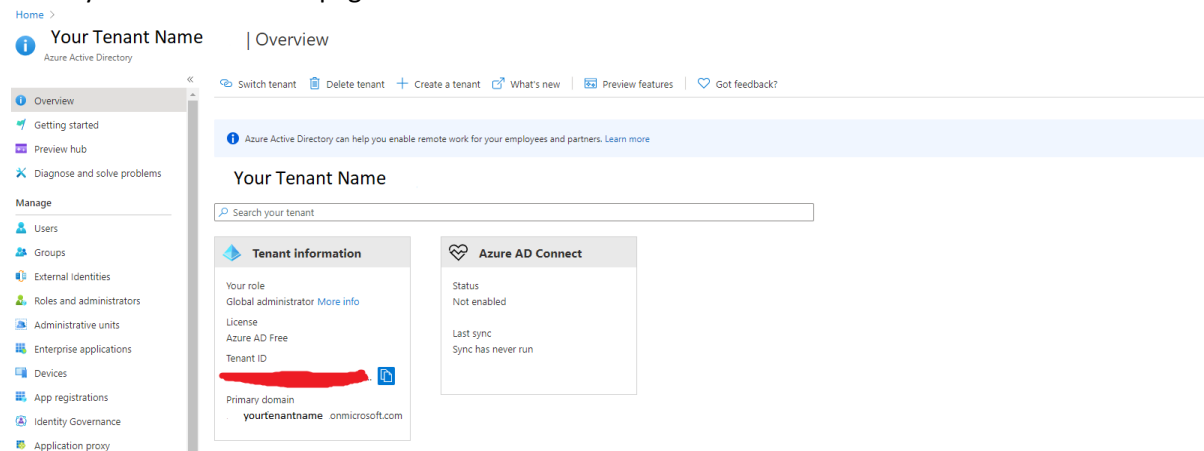
### 1.1. Create an Azure Active Directory B2B Tenant

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>

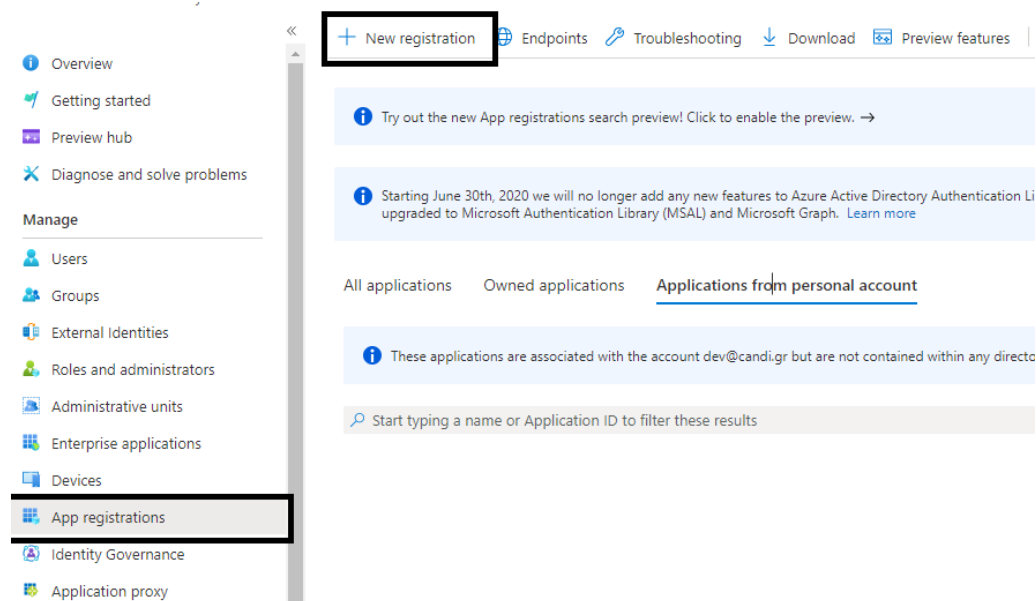
Go to your AAD overview page. Looks like this:



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

### Register an application

\* Name

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

your app name ✓

#### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (IncidentManagementDev 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.

Web

https://www.yourappname.com/signin-oidc ✓

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

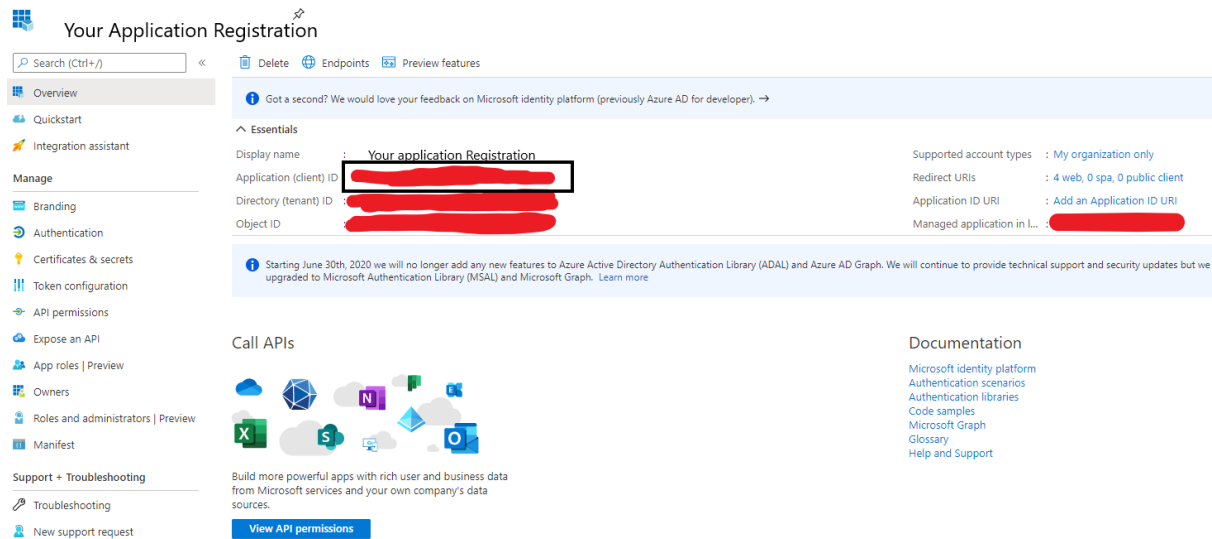
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Name your application as you wish. Choose **Accounts in this organizational directory only (IncidentManagementDev 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>

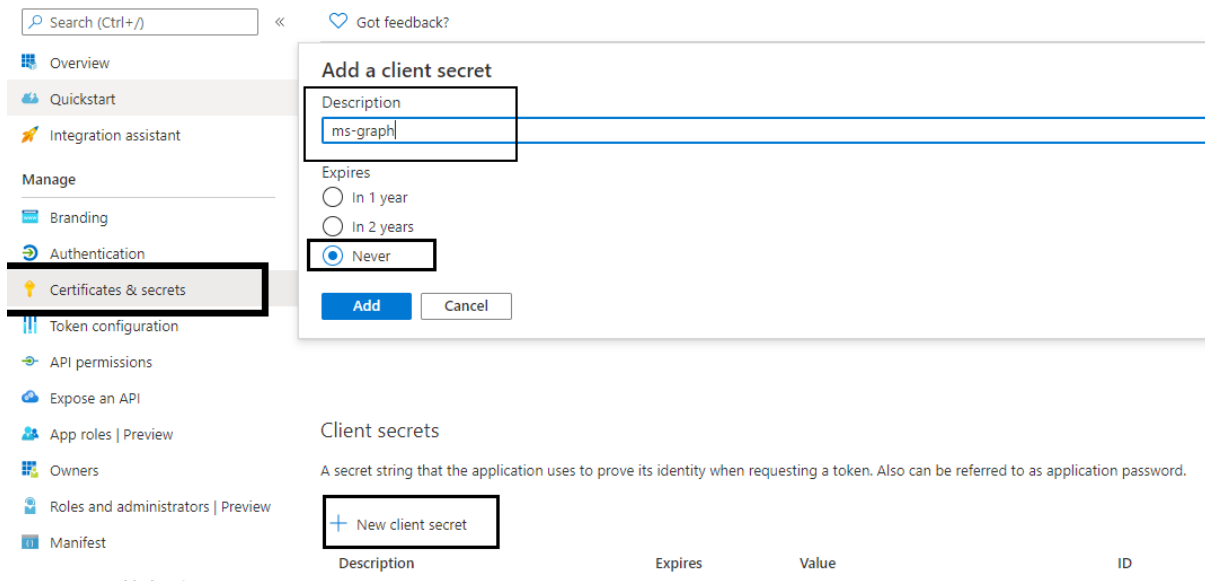
After application registration go to overview of this app registration.



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.

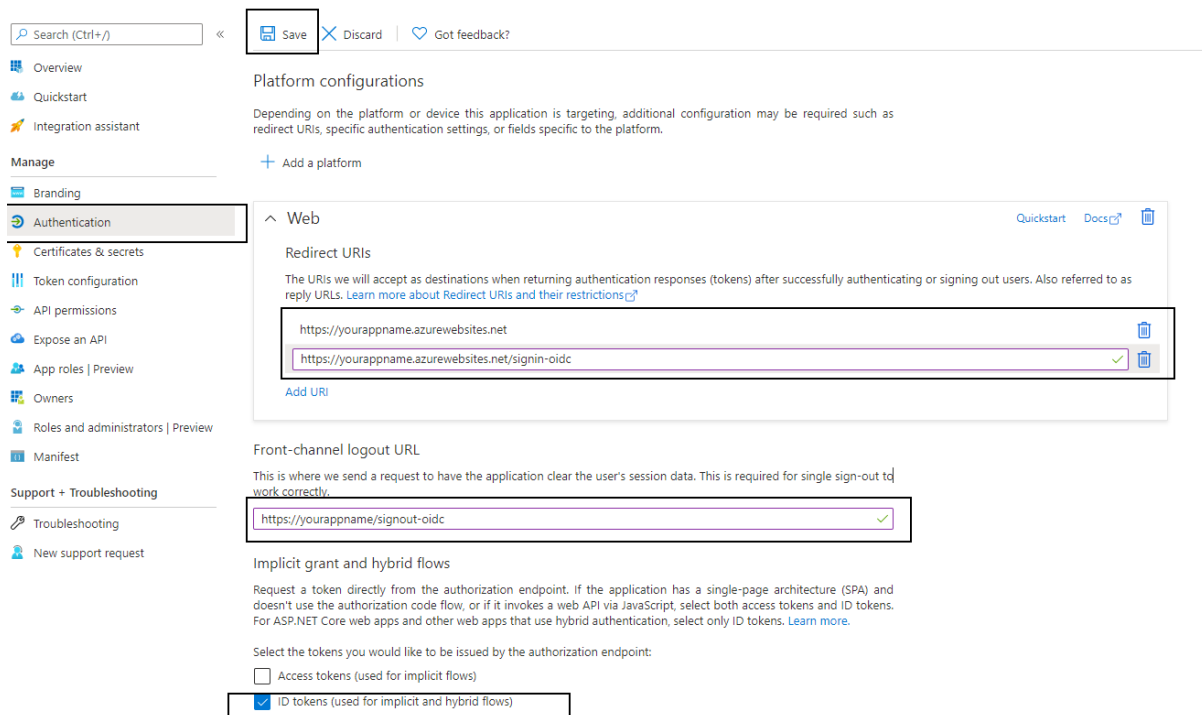
Finish the application creation wizard and follow post-creation steps.

## 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



Search (Ctrl+/) < Save Discard Got feedback?

Overview  
Quickstart  
Integration assistant  
Manage  
Branding  
Authentication  
Certificates & secrets  
Token configuration  
API permissions  
Expose an API  
App roles | Preview  
Owners  
Roles and administrators | Preview  
Manifest  
Support + Troubleshooting  
Troubleshooting  
New support request

### Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

#### Web

Quickstart Docs

##### Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://yourappname.azurewebsites.net  
https://yourappname.azurewebsites.net/signin-oidc

Add URI

##### Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://yourappname/signout-oidc

##### Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more](#).

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)  
☒ ID tokens (used for implicit and hybrid flows)

## 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 grant access to enable them (You must be the administrator of this tenant)

Search (Ctrl+/) « Refresh Got feedback?

Overview  
Quickstart  
Integration assistant

Manage

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

Support + Troubleshooting  
Troubleshooting  
New support request

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app role.

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 all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✓
User.Read.All	Delegated	Read all users' full profiles	Yes	✓
User.Read.All	Application	Read all users' full profiles	Yes	✓

To view and manage permissions and user consent, try [Enterprise applications](#).

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

Manage

Users  
**Groups**  
External Identities  
Roles and administrators  
Administrative units  
Enterprise applications  
Devices  
App registrations  
Identity Governance  
Application proxy  
Licenses  
Azure AD Connect

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

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



<div><div>+ New group</div><div>Download groups</div><div>Delete</div><div>Refresh</div><div>Columns</div><div>Preview features</div><div>Got feedback?</div></div>				
This page includes previews available for your evaluation. View previews →				
<div><div>Search groups</div><div>Add filters</div></div>				
	Name	Object Id	Group Type	Membership Type
<input type="checkbox"/>	<div>AD</div> Administrators	279f692d-c4ce-40fb-9ea7-be0d827cf3d1	Security	Assigned
<input type="checkbox"/>	<div>AG</div> Agents	383d2086-56da-4f09-84a1-43da05388047	Security	Assigned
<input type="checkbox"/>	<div>GU</div> Guests	13b68bec-eb95-40b8-917f-59e0781e6867	Security	Assigned
<input type="checkbox"/>	<div>US</div> Users	89e2e542-2c02-4cfc-ac3f-99d5b5e4c940	Security	Assigned

Finally, you must populate your brand 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.

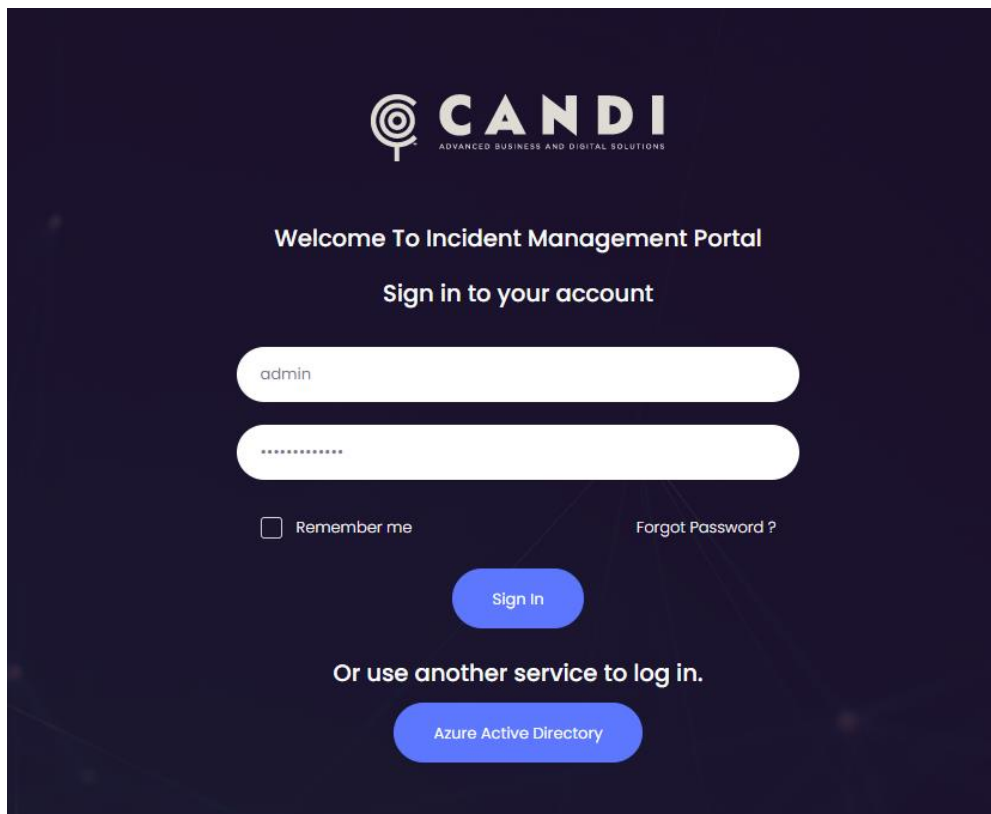
## 3. Steps before using the Application


### 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](#)



 **CANDI**  
ADVANCED BUSINESS AND DIGITAL SOLUTIONS

Welcome To Incident Management Portal

Sign in to your account

admin

\*\*\*\*\*

☐ Remember me [Forgot Password ?](#)

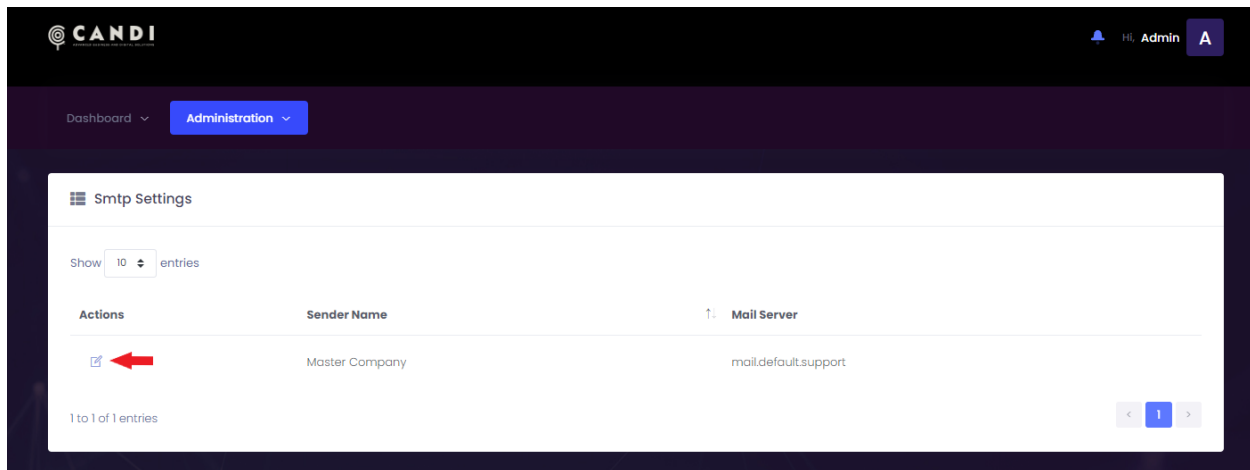
Sign in

Or use another service to log in.

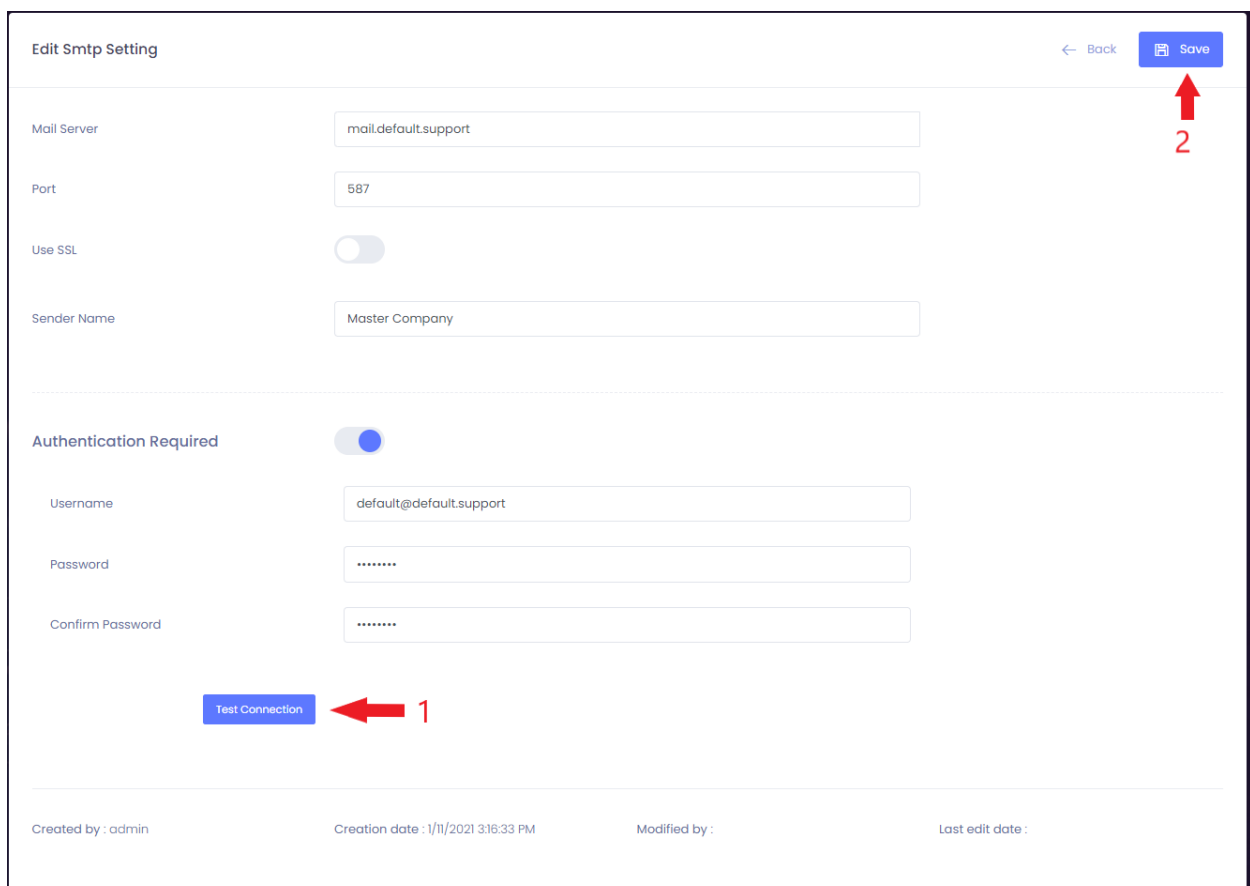
Azure Active Directory

### 3.2. Set up your Smtip Settings

At Administration -> Portal Settings -> Smtip 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).



← Back **Save**

Mail Server: mail.default.support

Port: 587

Use SSL: ☐

Sender Name: Master Company

Authentication Required: ☒

Username: default@default.support

Password: .....

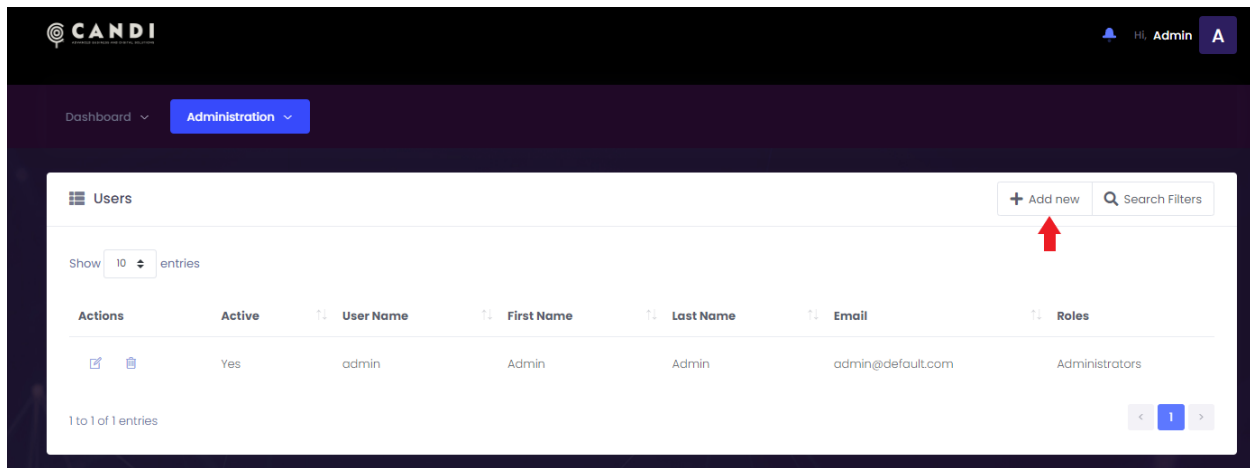
Confirm Password: .....

**Test Connection** **Save**

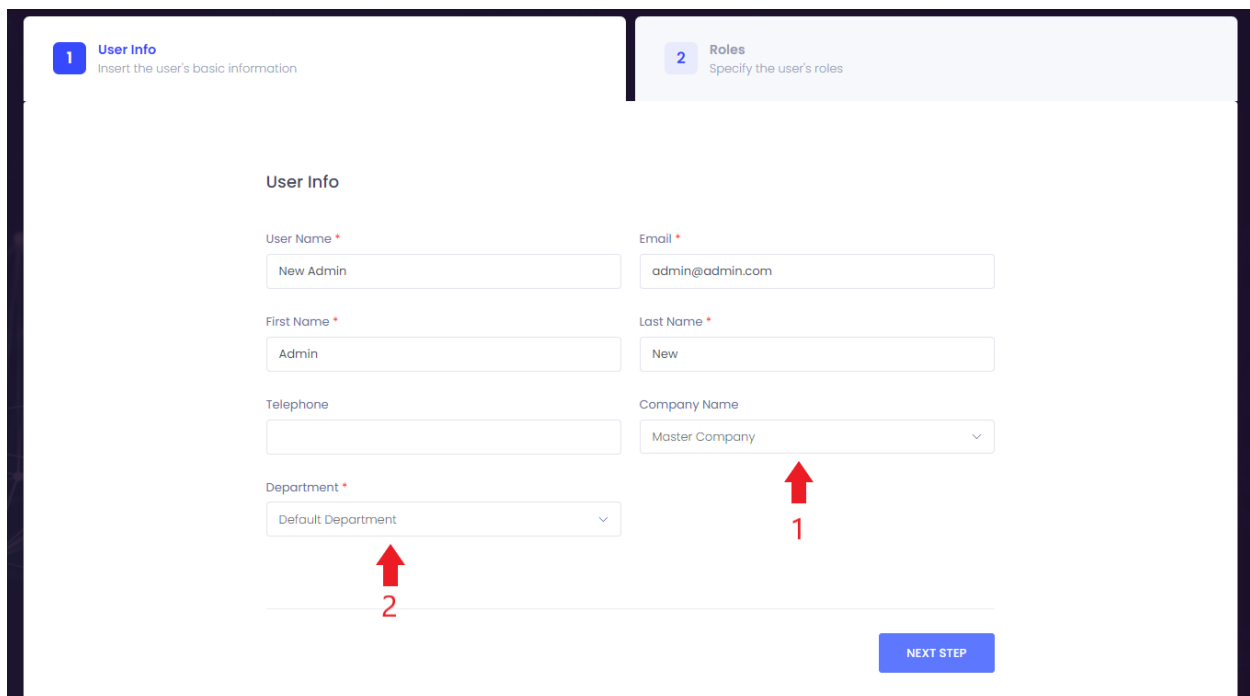
Created by : admin      Creation date : 1/11/2021 3:16:33 PM      Modified by :      Last edit date :

### 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.



**1 User Info**  
Insert the user's basic information

**2 Roles**  
Specify the user's roles

**User Info**

User Name \*  
New Admin

Email \*  
admin@admin.com

First Name \*  
Admin

Last Name \*  
New

Telephone

Company Name  
Master Company

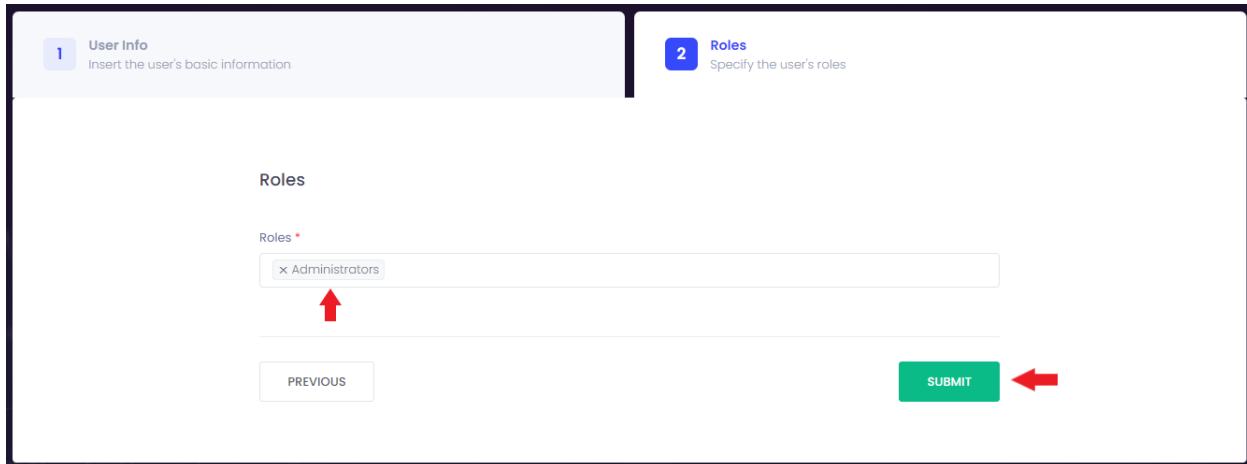
Department \*  
Default Department

**2**

**1**

**NEXT STEP**

At the Roles section select 'Administrators' role and click submit.



1 User Info  
Insert the user's basic information

2 Roles  
Specify the user's roles

Roles

Roles \*

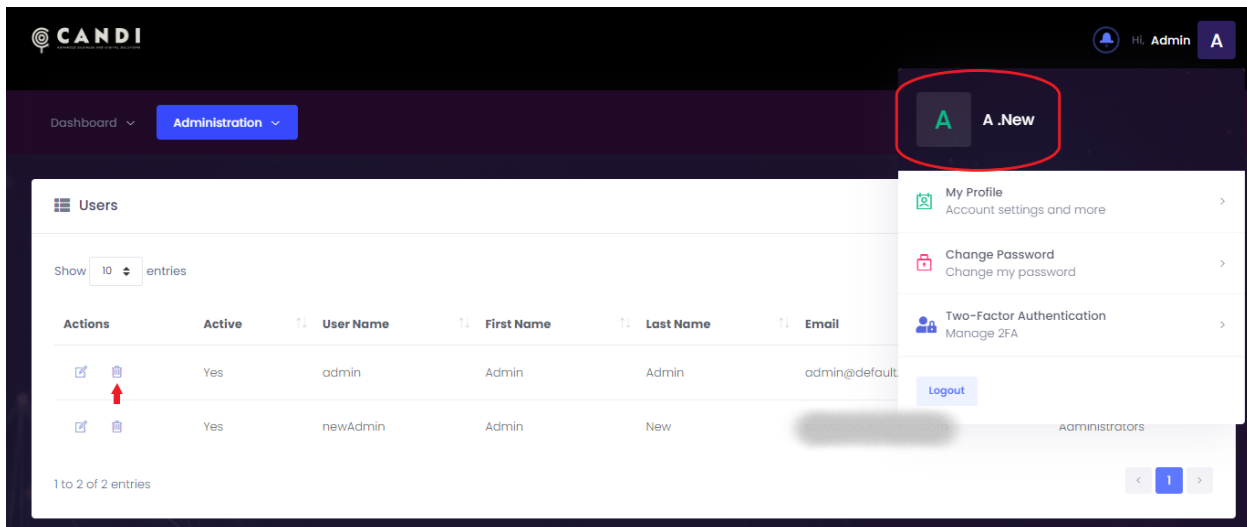
x Administrators

PREVIOUS

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.



CANDI

Dashboard Administration

A .New

My Profile  
Account settings and more





Change Password  
Change my password

Two-Factor Authentication  
Manage 2FA

Logout

Users

Show 10 entries

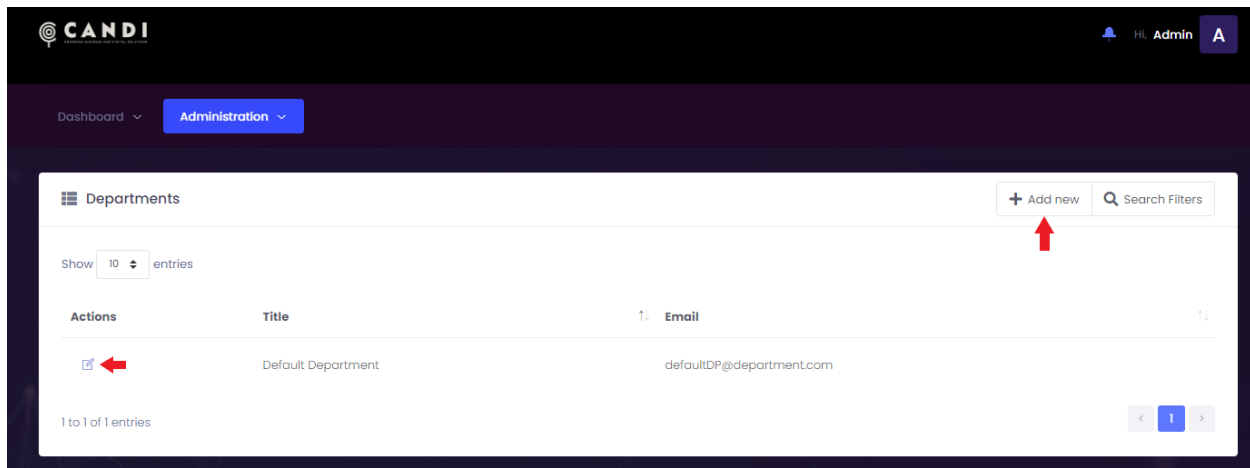
Actions	Active	User Name	First Name	Last Name	Email
 	Yes	admin	Admin	Admin	admin@default
 	Yes	newAdmin	Admin	New	

1 to 2 of 2 entries

Administrators

### 3.4. Edit the Default Department

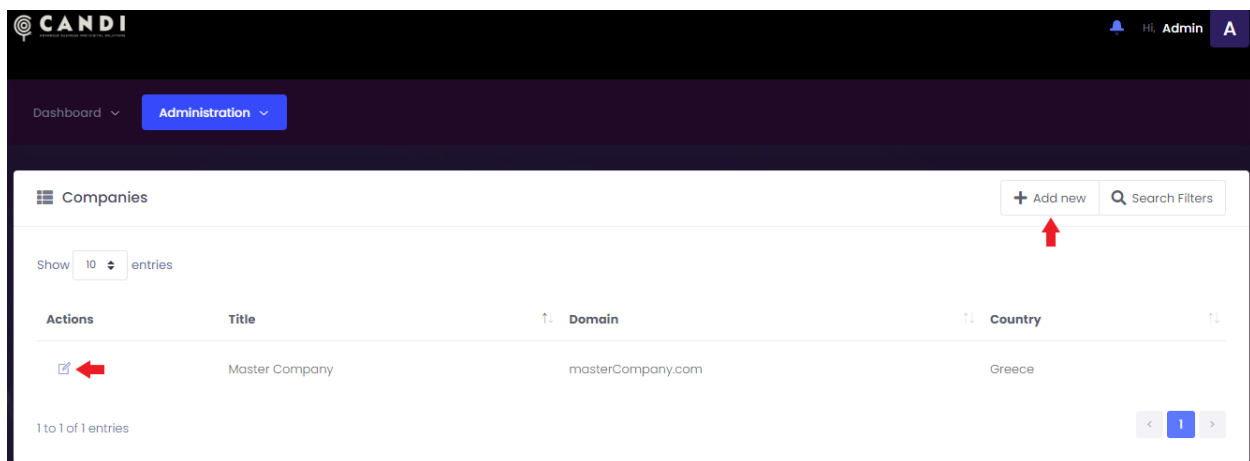
At Administration -> Department click the edit button of 'Default Department'



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).

**Identity**

Name	First name	Last name
User Principal Name	User type	
	Member	
Object ID	Issuer	
866	ef9a4	
View more		

**Job info**

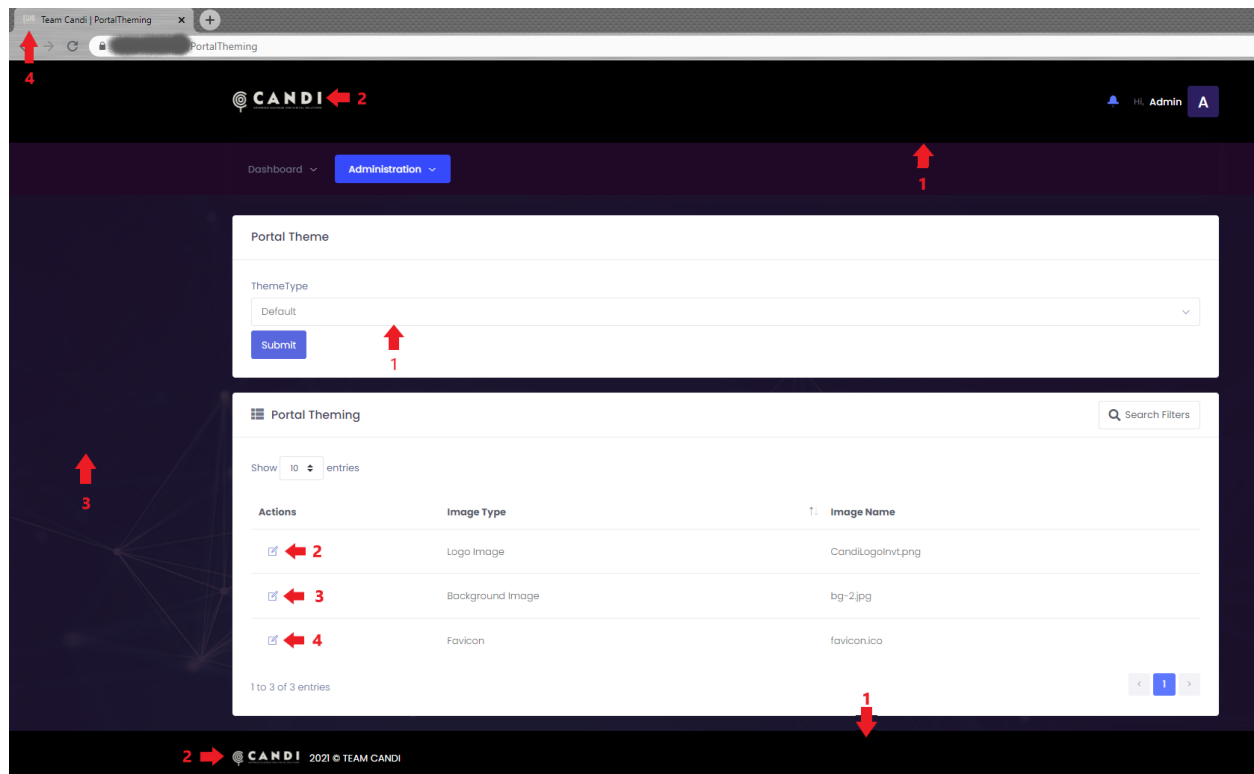
Job title	Department	Manager
Company name	Employee ID	
	-- --	

**Settings**

### 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