alcatraz ai

Alcatraz AI Admin Portal

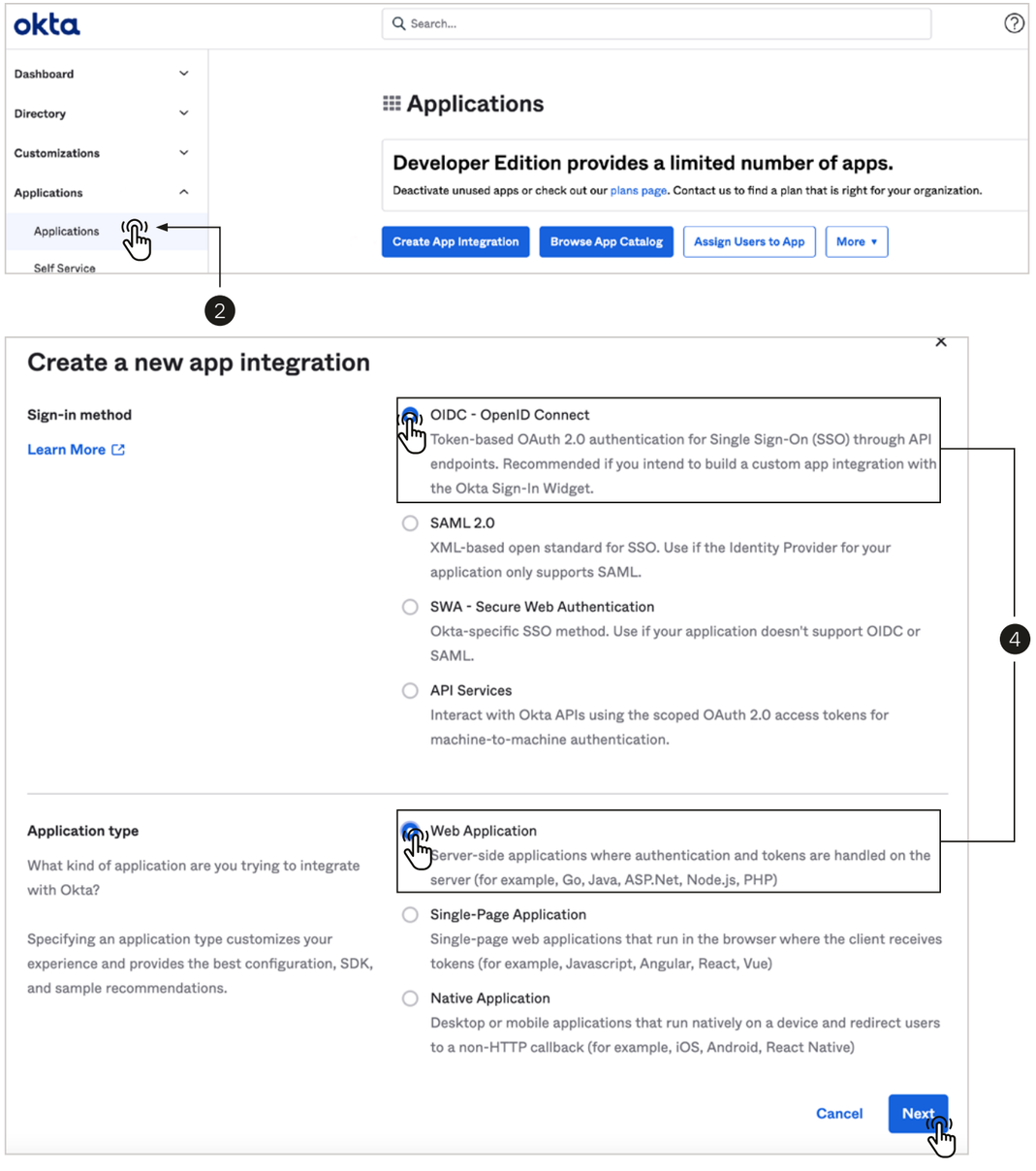
SSO Configuration

Table of Contents

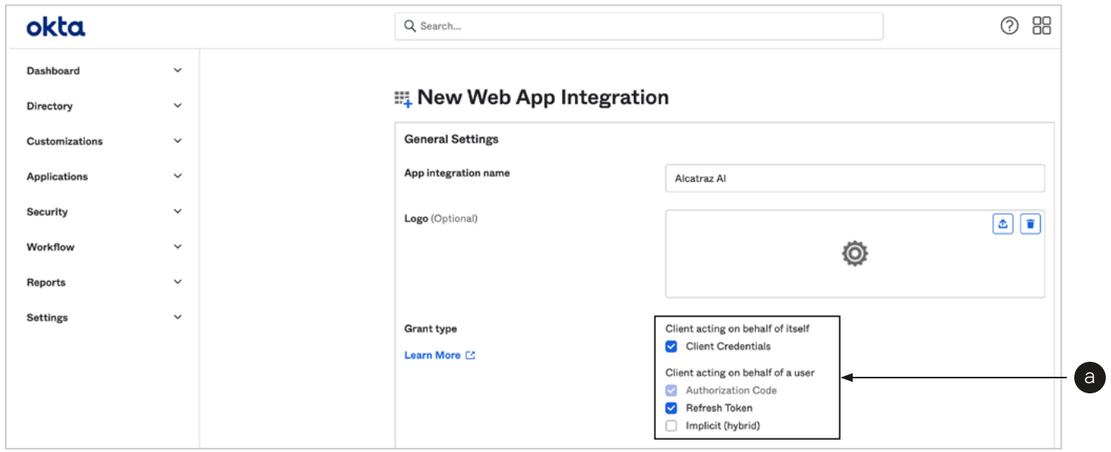
1—SSO with Okta

Before a user can sign in Alcatraz Platform using Okta as an identity provider, it is necessary to create an Okta app integration that represents Alcatraz in the provider's system – from where the required configuration will be fetched.

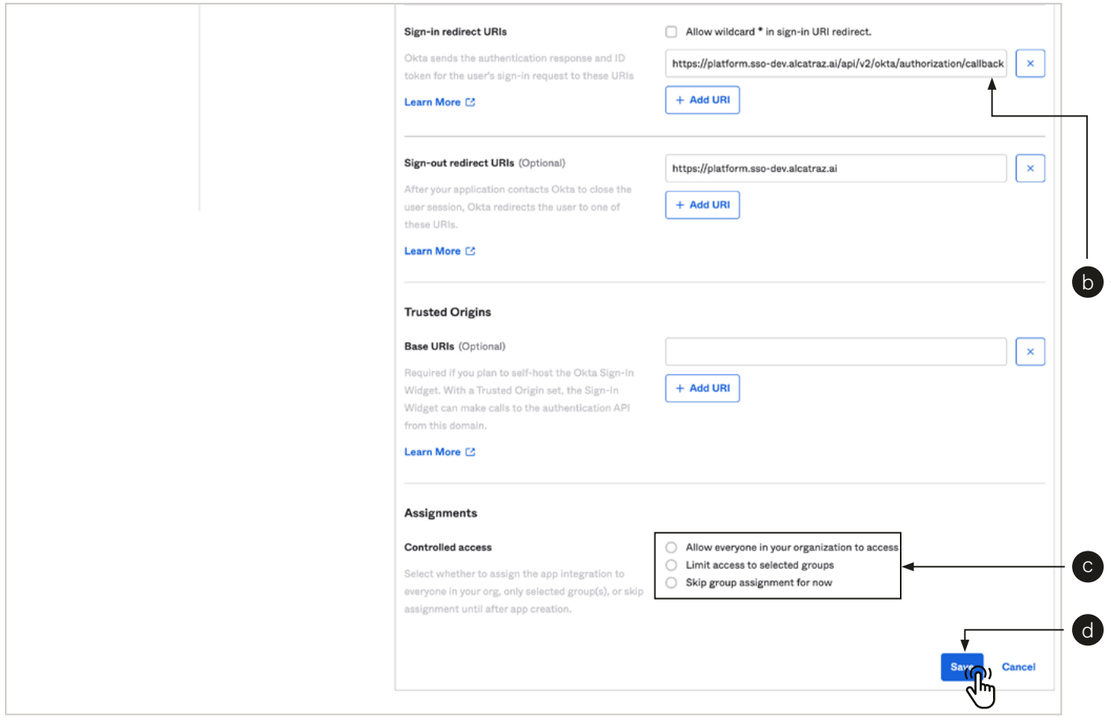
1. Sign in to your **Okta** organization with an administrator account.
2. In the Admin Console, go to **Applications —> Applications**.
3. Click **Create App Integration**.
4. Select **OIDC - OpenID Connect** as the Sign-in method and **Web Application** as the Application type and click **Next**.
   Our system supports only OIDC, and do not support SAML, Single Page or Workers.

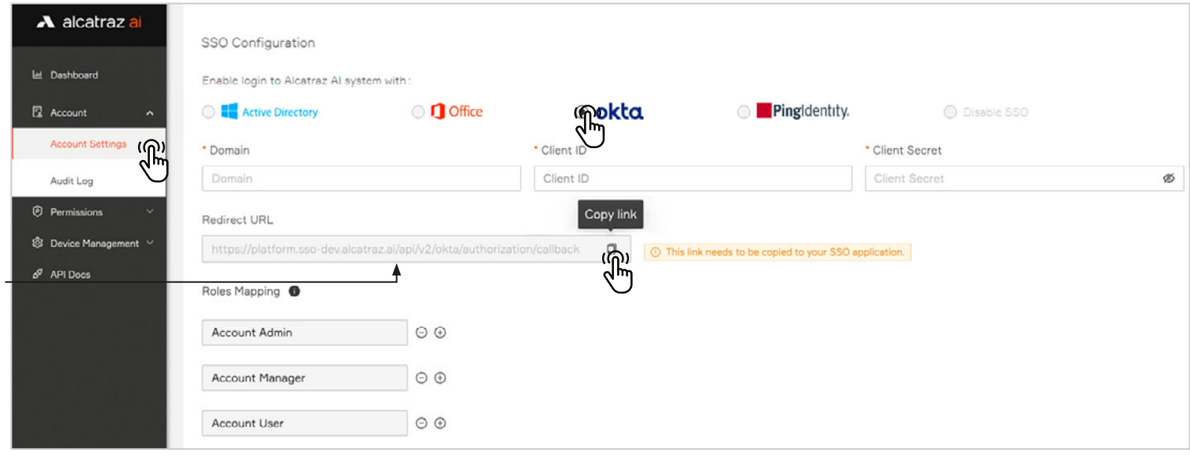


5. **New Web App** Integration screen will load. Configure the app as follow:
   a. Select **Client Credentials** and **Refresh Token** options.

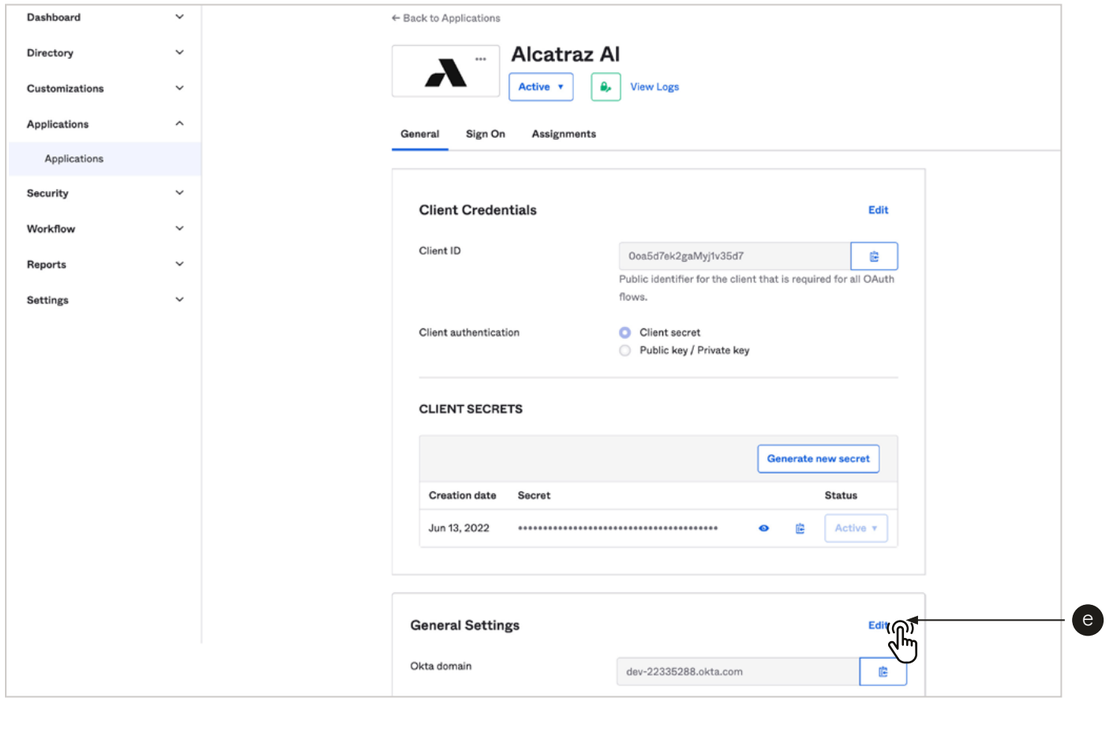


   b. Alcatraz AI Platform redirect credentials need to be entered to the **Sign-in/Sign-out redirect URIs** values.
   — Open the Alcatraz Admin Portal, go to **Account –> Account settings**, scroll down to the **SSO Configuration** section and click to open it. Select **Okta** of the displayed SSO provider options.
   — For **Sign-in redirect URIs** enter the **Redirect URL** copied from the Alcatraz AI **SSO Configuration** UI.
   — For **Sign-out redirect URIs** use the base url (of the **Redirect URL** ex. **https://platform.sso-dev.aclatraz.ai**).
   c. For **Controlled access** section choose option by your organization preferences.
   d. Click **Save**.

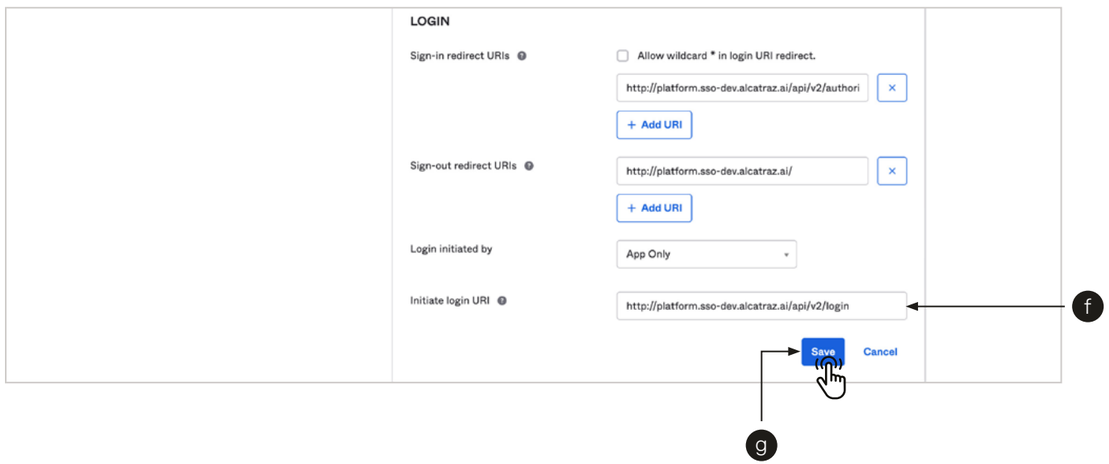




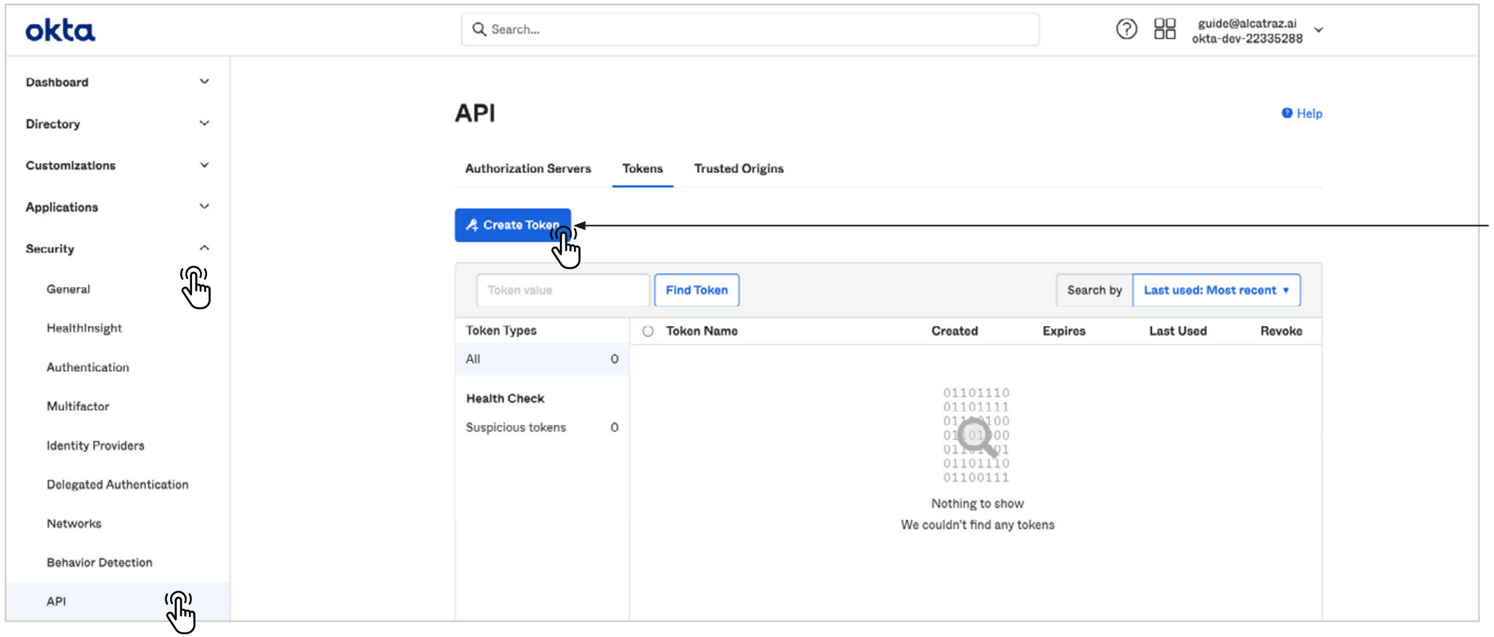
e. After saving – the system will open display the settings of the already created integration app.
In **General** tab scroll down and click **Edit** button of the **General Setting** section.



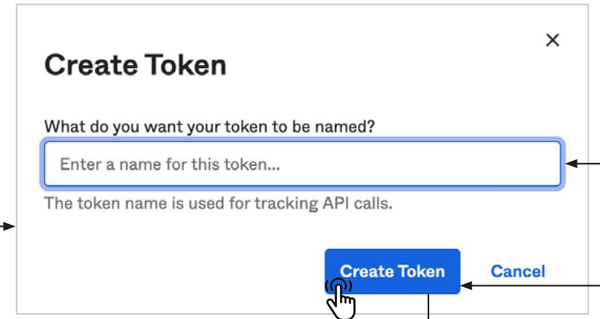
f. Scroll down to the **LOGIN** credentials and fill the **Initiate login URI** (base URL + /api/v2/okta/login ex. https://platform.sso-dev.aclatraz.ai/api/v2/okta/login).
Note: all of the URIs of the LOGIN section need to be filled properly to enable the SSO integration.
g. Click **Save**.



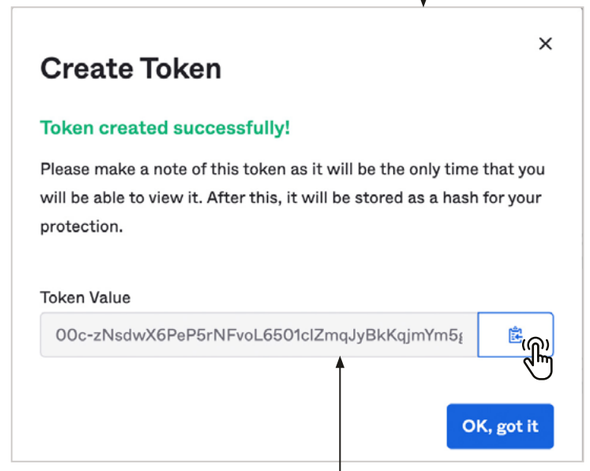
6. Create an Okta API token, go to **Security —> API**, click **Tokens** tab. Okta API tokens are utilized to authenticate and synchronize the Okta user groups with the groups configured in the Alcatraz AI Admin Portal.
   a. Click **Create Token**. A pop-up will be displayed.
   b. Add token name and click **Create Token** to continue. A successful message with the token value will be displayed.



a



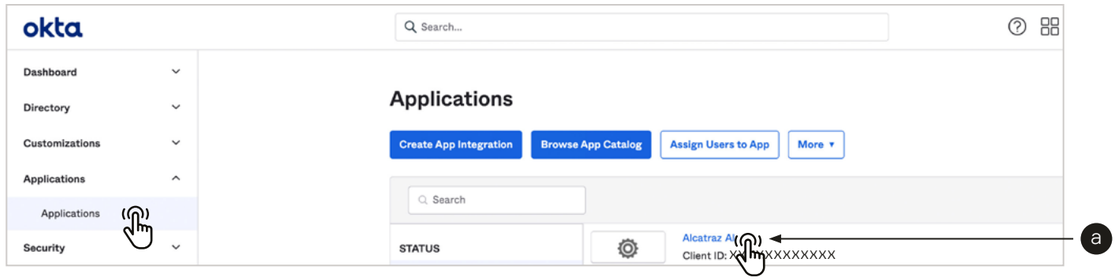
b



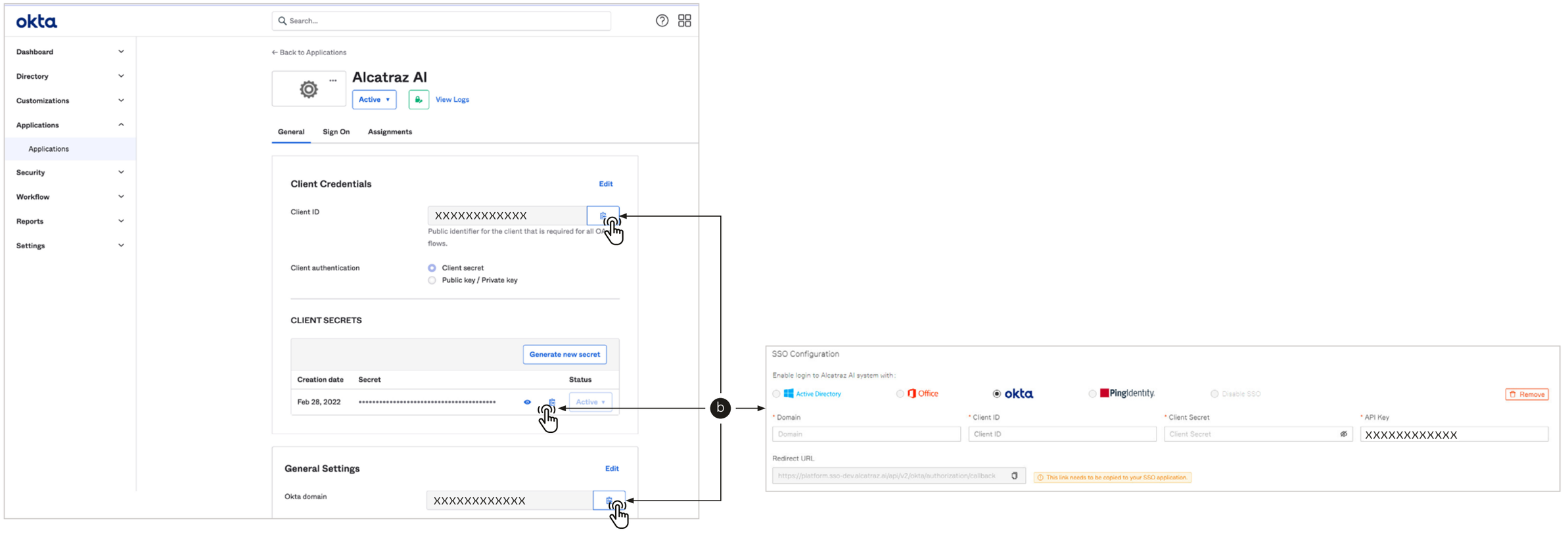
c. Copy the token value and add it to the API key field (in the Alcatraz AI UI).
   Copy the token value right after creating the token. By security policies the value is visible only while creating it. Note: tokens expire automatically after a certain period and can also be deactivated at any time. Once a token is expired it should be regenerated and updated in the Alcatraz AI SSO configuration.

C

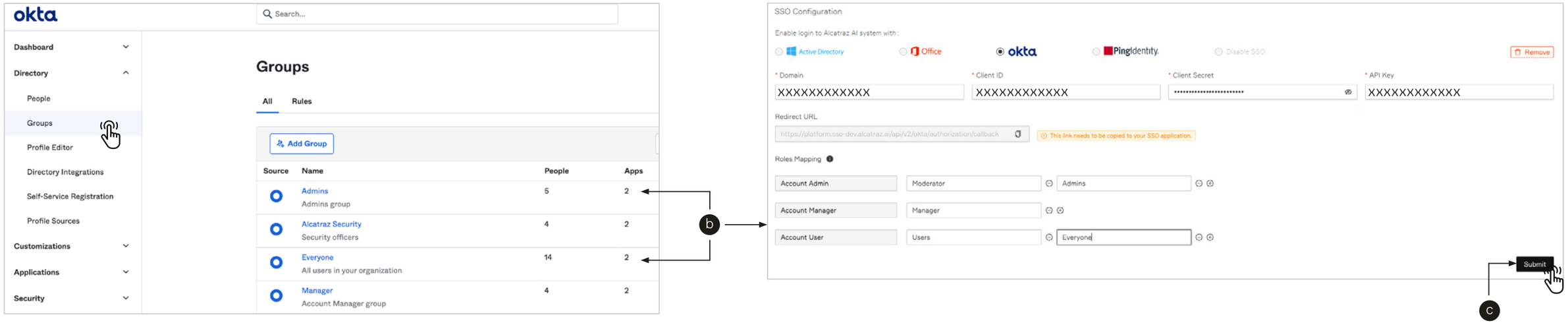
7. Configure the Alcatraz Admin Portal, with the required credentials from the new created Okta integration app.
   a. In Okta Admin Console, go to **Applications –> Applications** and click on the created integration app.



   b. Copy the **Client ID, Secret** and **Okta domain** credentials (from the **General** tab) and add them to the required fields of the **SSO Configuration** section.



8. Map the Okta groups to the **Alcatraz roles**.
   Note: At least one Okta group must be mapped to Alcatraz role.
   a. In Okta Admin Console, go to **Directory —> Groups.**
   b. Copy the names of the groups that will be mapped in Alcatraz AI system. Assign a selected group to preferred user role. The mapping allows more than one group to be assigned to a role.
   c. Click **Submit** when ready.



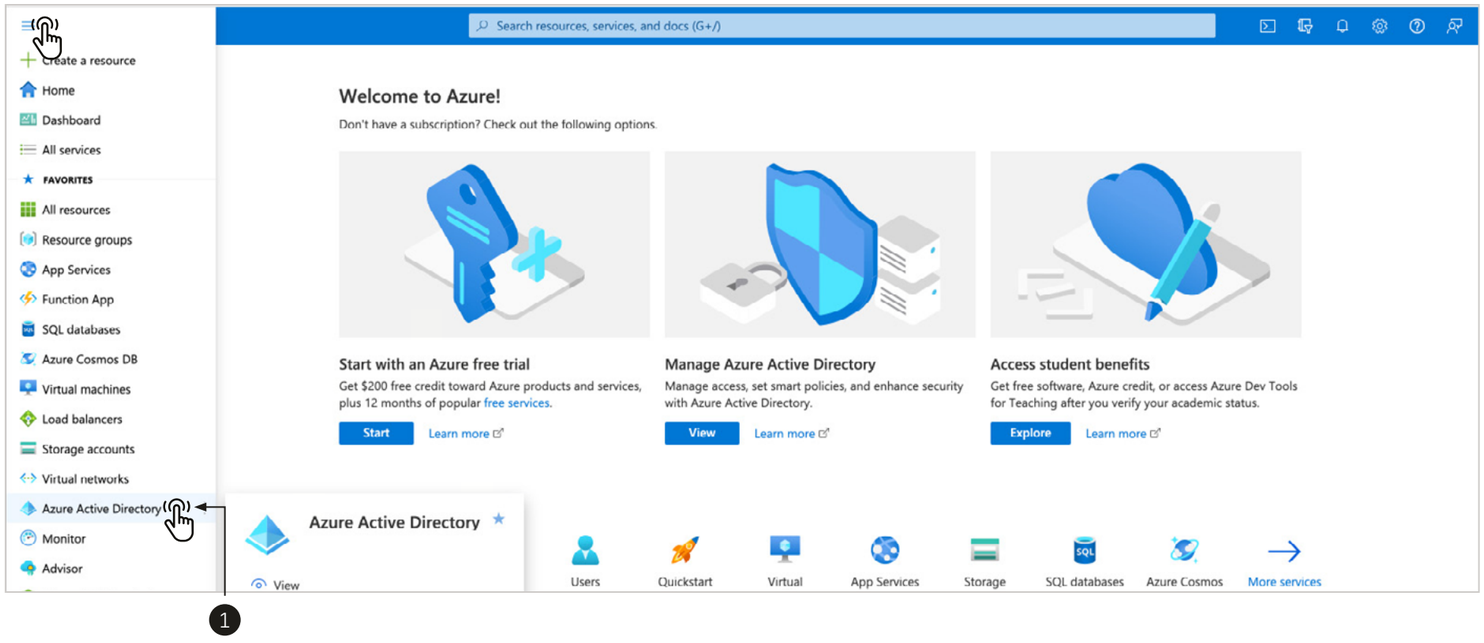
9. Log out and a new login screen will be available, allowing to use Okta as identity provider to log to the Alcatraz platform.

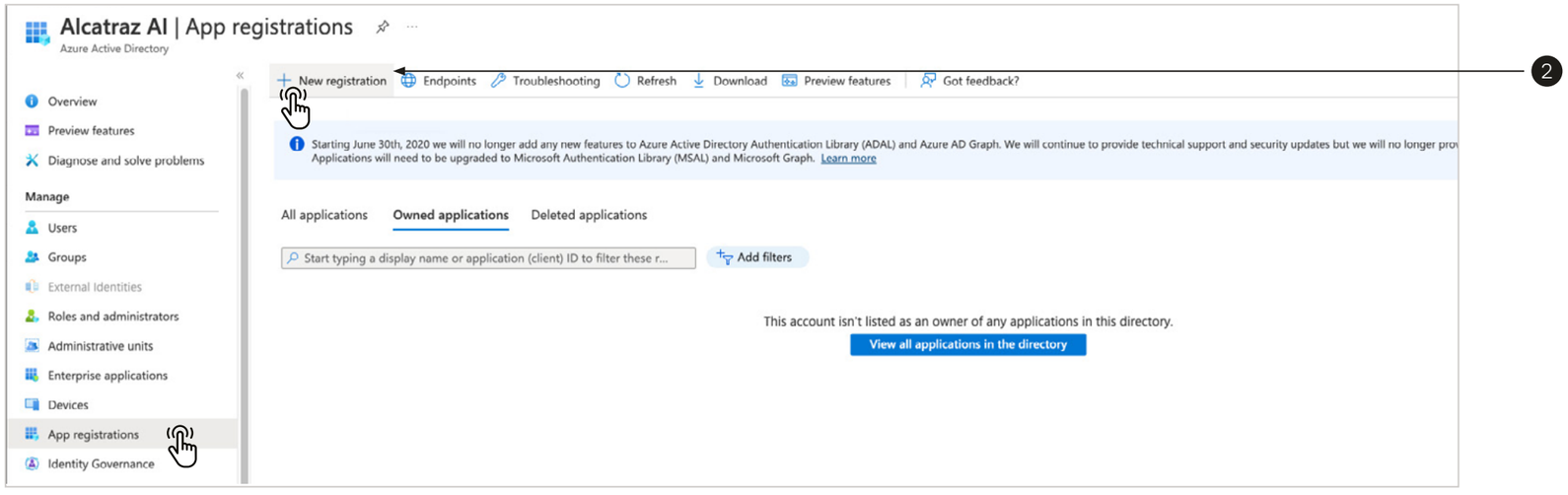
2—SSO with Azure

Before you can sign a user in Alcatraz Platform using Microsoft as an identity provider, you need to create an Azure account that has an active subscription. The Azure account must have permission to manage applications in Azure Active Directory (Azure AD). Any of the following Azure AD roles include the required permissions:

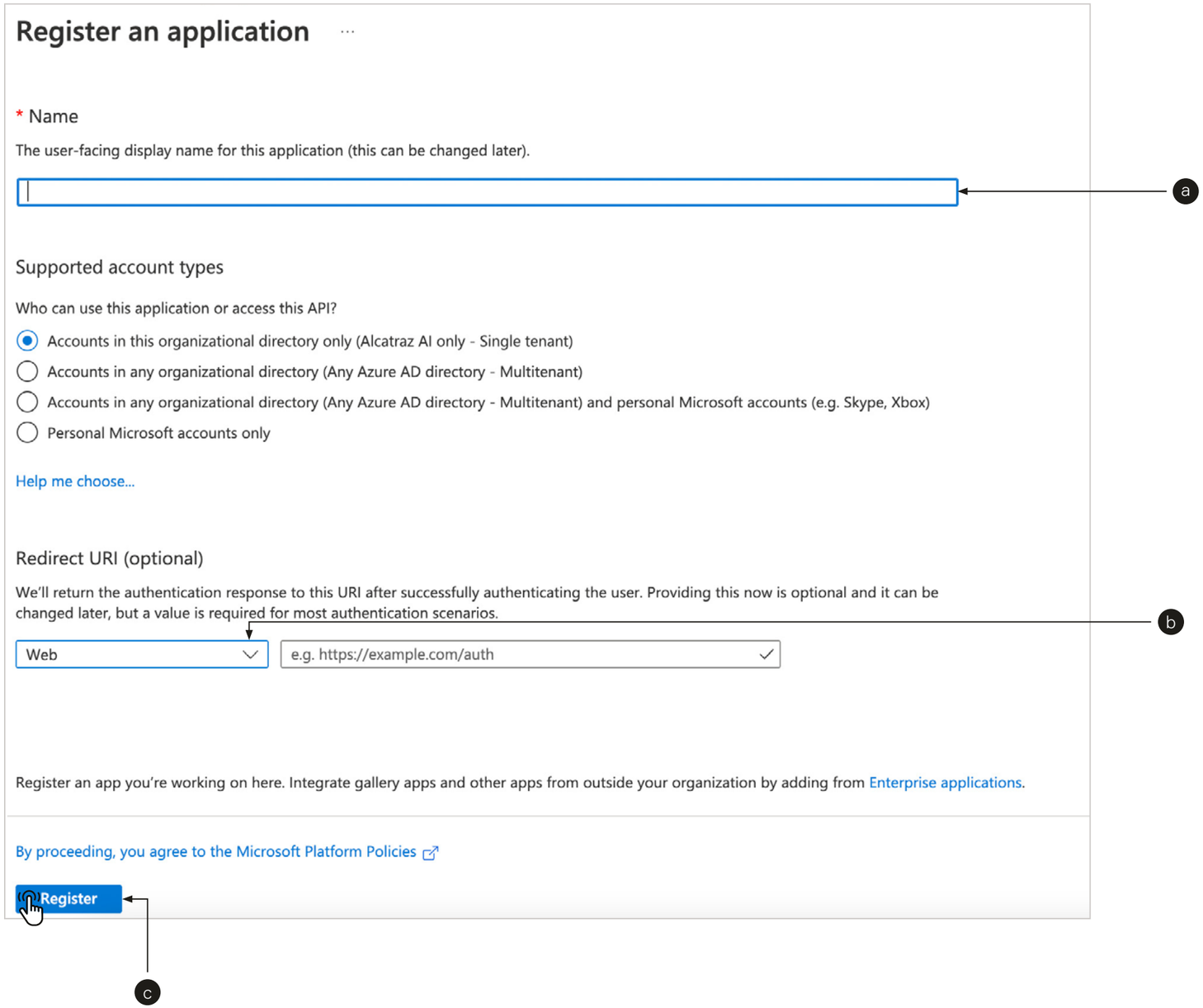
—Application Administrator
—Application Developer
—Cloud Application Administrator

1. Sign in to your account. Click on top left menu and select **Azure Active Directory**.
2. Under **Manage,** select **App registrations** and click **New registration**.





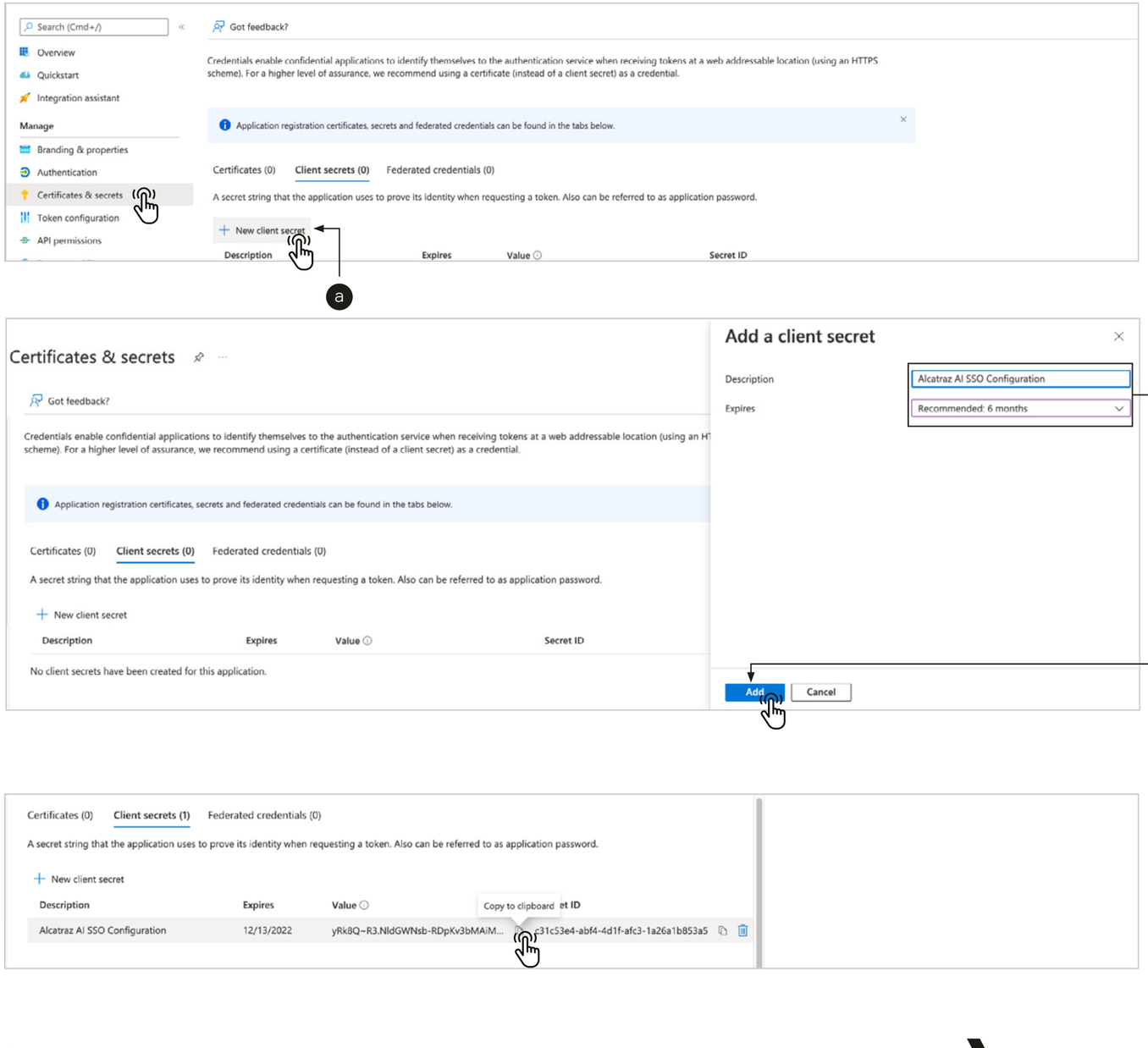
3. **Register an application** screen will load. Configure the app as follow:
   a. In the **Name** section, enter a meaningful application name that will be displayed to the users.
   b. Select **Web**, without entering anything for Redirect URI.
      Note that the redirect URI will be configured in further steps. (Step 8)
   c. Click **Register** to create the application.



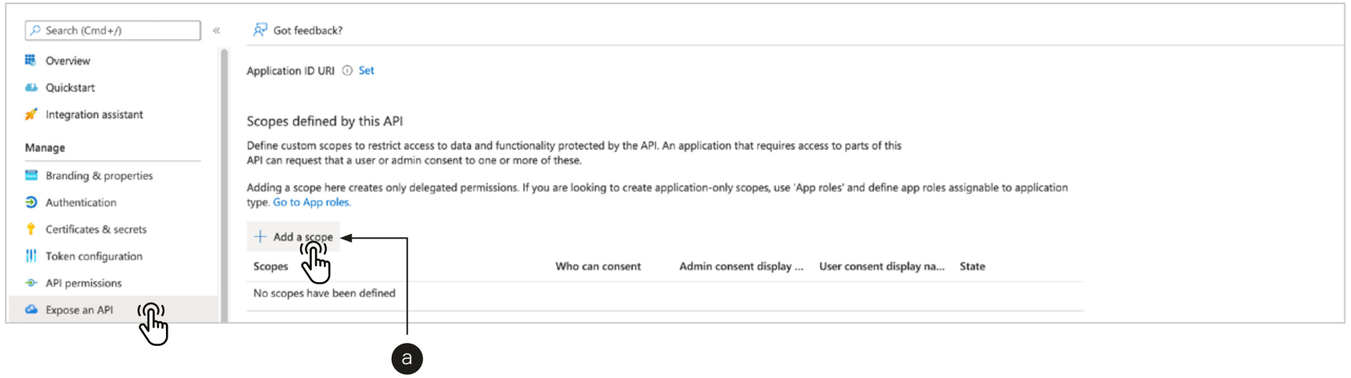
4. Create **Client Secret**.
   a. Go to **Certificates & secrets** and click **New client secret**.
   b. Add **Description** and select or configure expiration time by your preferences.
   c. Click **Add** to continue.

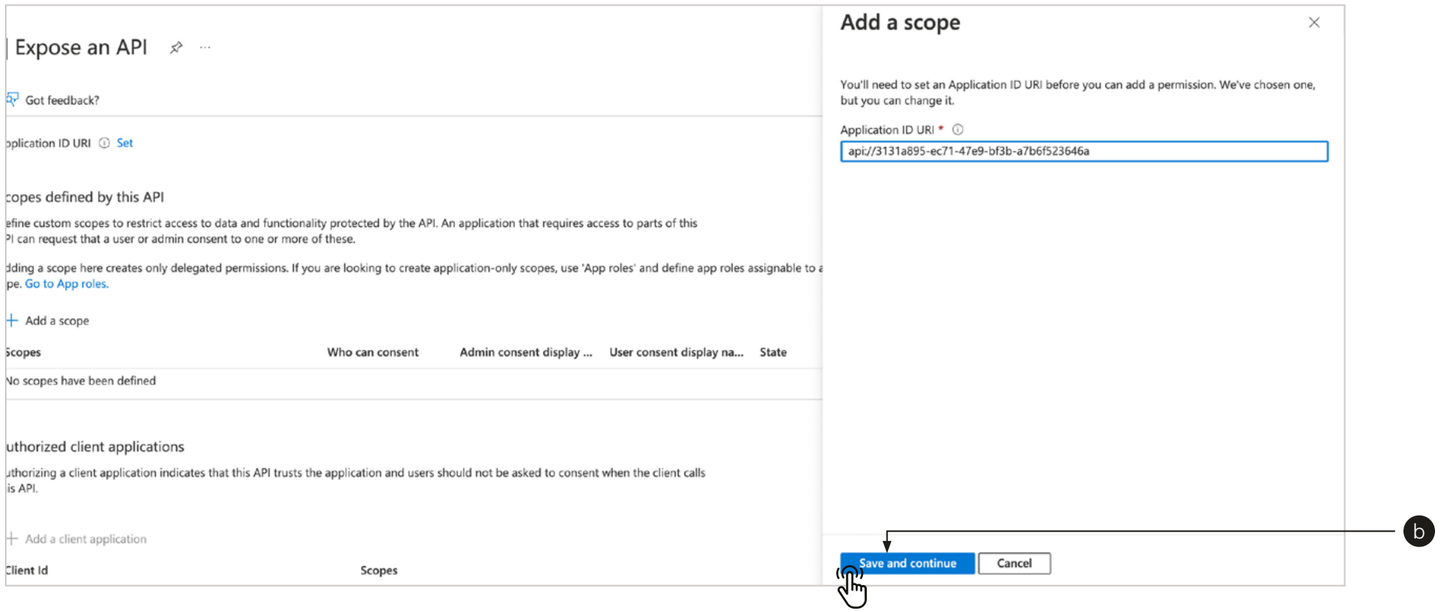
   Note: copy and record the secret's value for use in your client application code. The secret value might not displayed again after you leave the page.

   Client secret credentials expire automatically after the selected expiration period. Once a secret credential is expired it should be regenerated and updated in the Alcatraz AI SSO configuration.

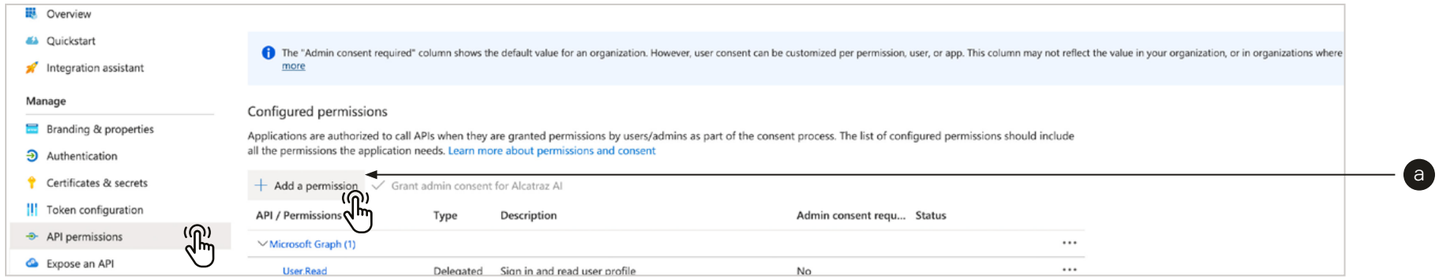


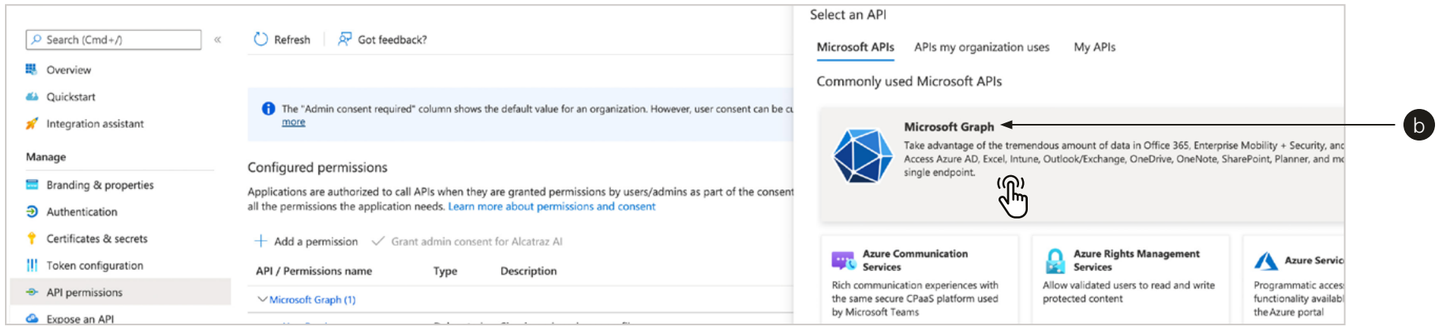
5. Expose an API
   a. Under **Manage,** select **Expose an API click Add a scope**.
   b. Accept the proposed **Application ID URI** (api://{clientId}) by selecting **Save and continue**.

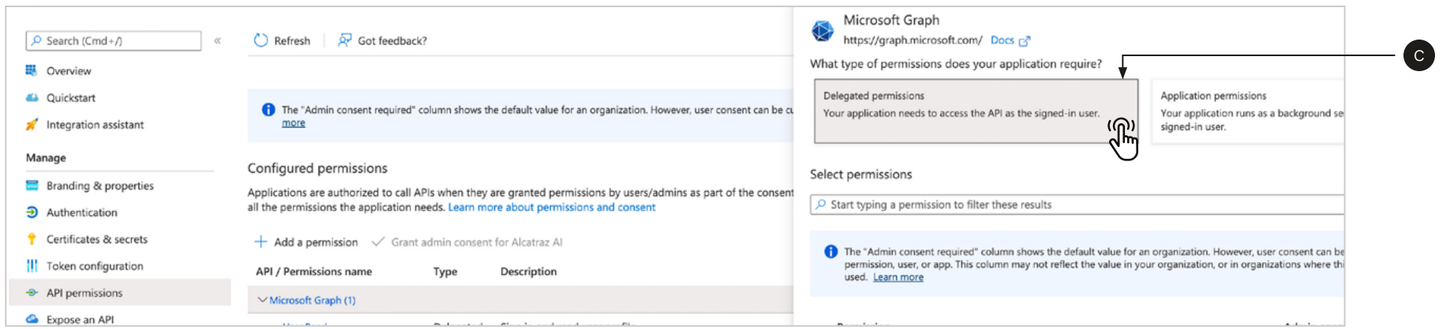




6. **Set API Permissions**
   a. Under **Manage,** select **API permissions** and click **Add a permission**.
   b. Select **Microsoft Graph**.
   c. And click **Delegated permissions**.







d. Set the following API Permissions to be able to create user sessions and sync user groups:
—Under **OpenId permissions: email, offline_access, openid,** and **profile**.
Our system supports only Open ID connect, and do not support SAML, Single Page or Workers.

Permission	Admin consent required
OpenId permissions (4)	
email View users' email address	No
offline_access Maintain access to data you have given it access to	No
openid Sign users in	No
profile View users' basic profile	No

—Under **Group: Group.Read.All**
—Under **GroupMember: GroupMember.Read.All**

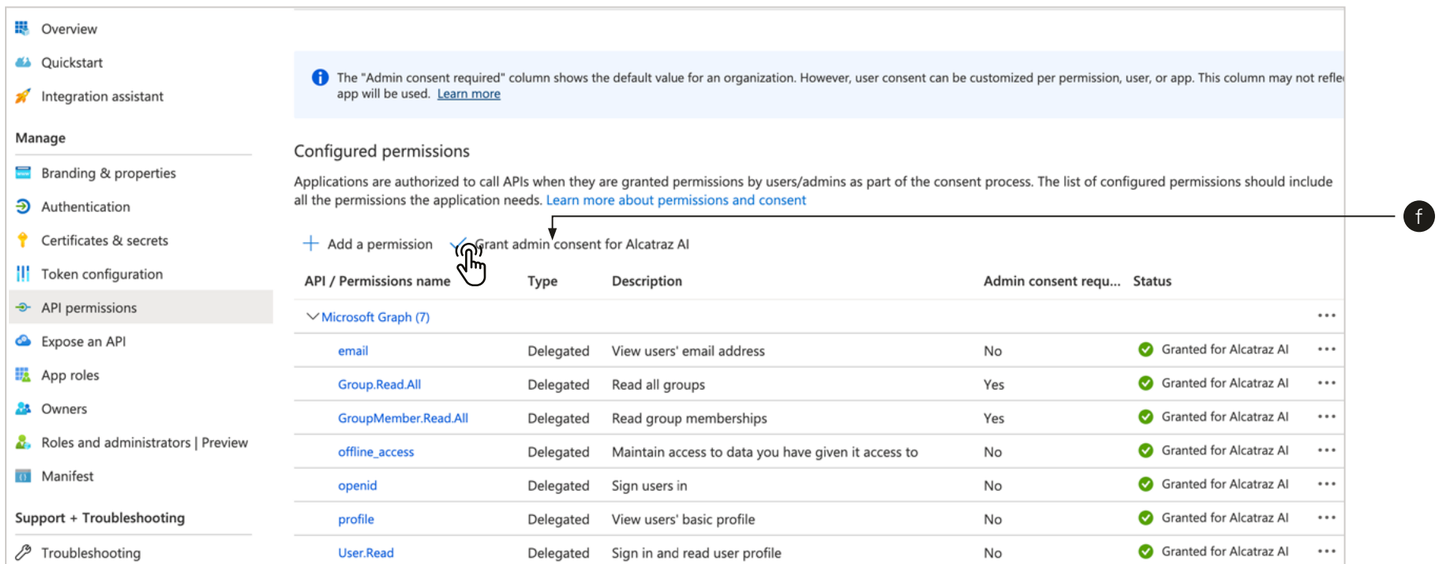
Group (1)	
Group.Read.All Read all groups	Yes
Group.ReadWrite.All Read and write all groups	Yes
GroupMember (1)	
GroupMember.Read.All Read group memberships	Yes

—Under **User: User.Read**

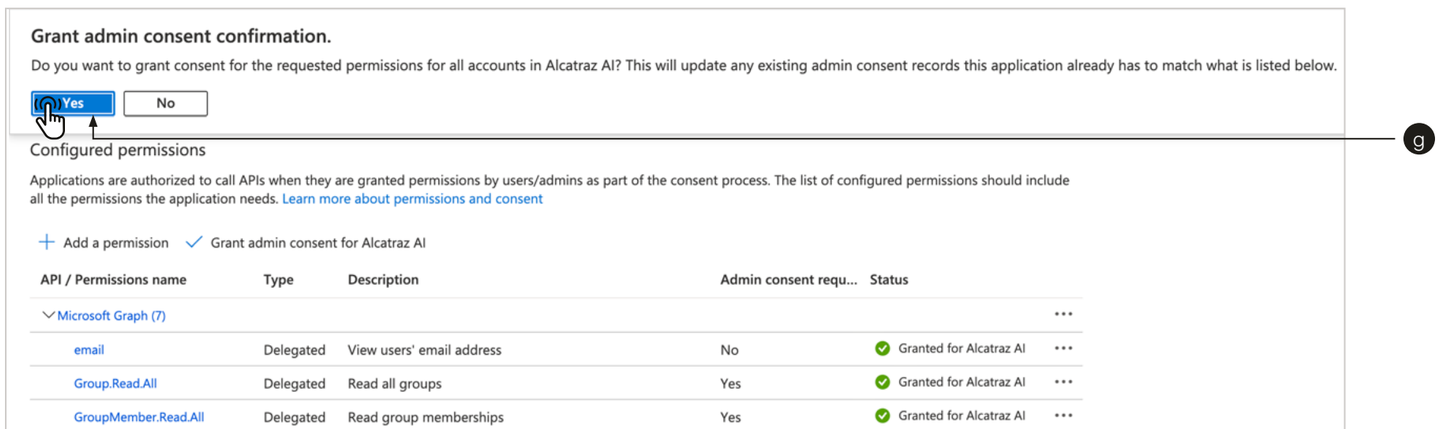
User (1)	
User.Export.All Export user's data	Yes
User.Invite.All Invite guest users to the organization	Yes
User.ManageIdentities.All Manage user identities	Yes
User.Read Sign in and read user profile	No

e. Click **Update permissions** when ready. And verify if they are displayed as followed list (refer to the image below).

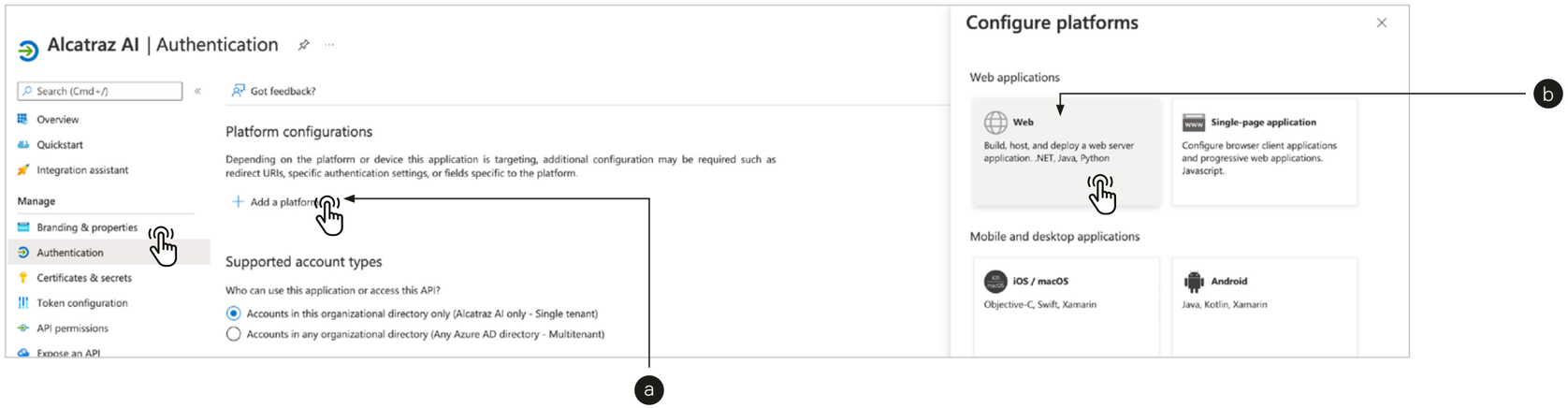
f. After verifying the permissions list click **Grant admin consent for "App Name"** button.



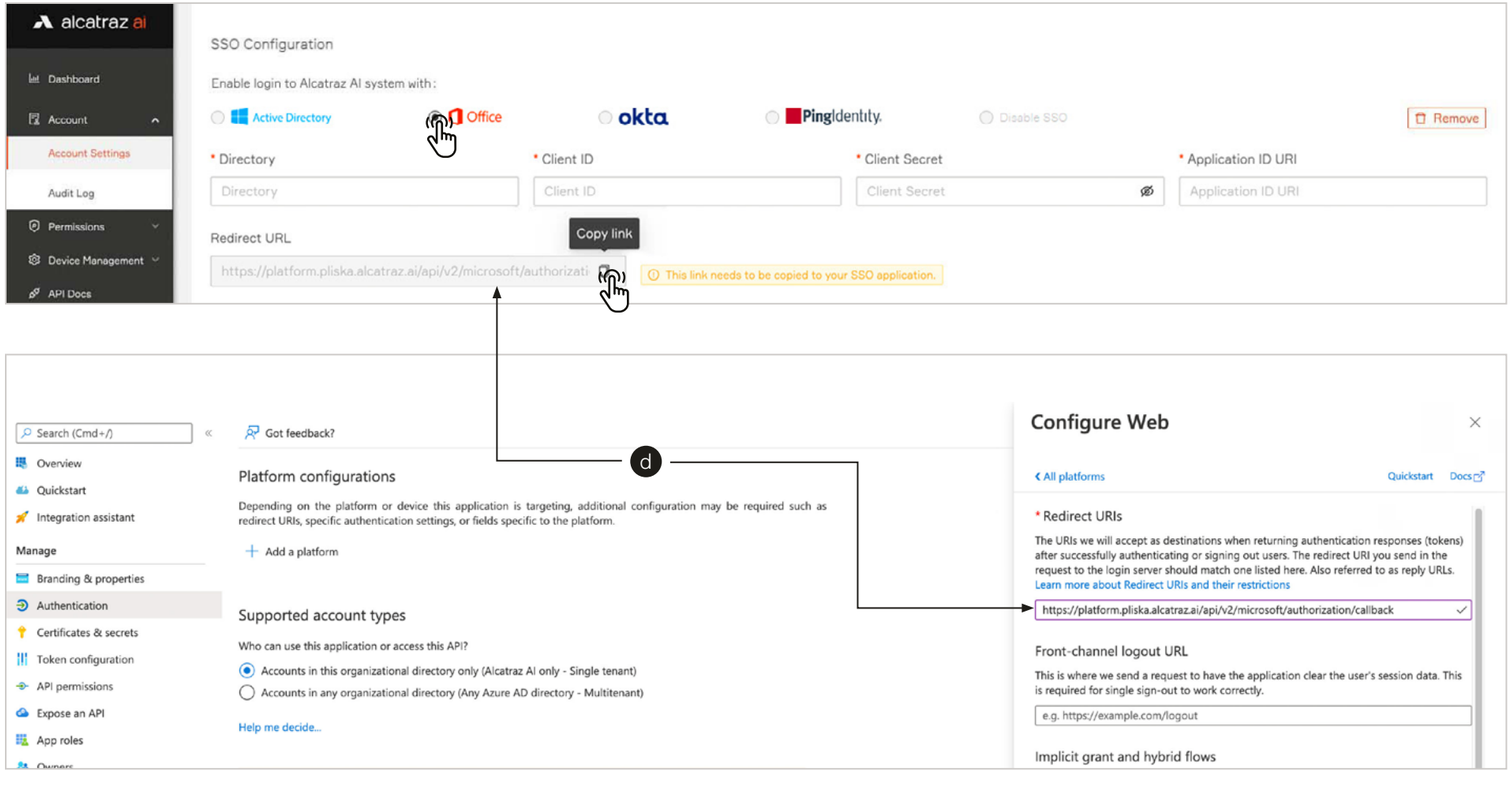
g. Click **Yes** on the displayed dialog.



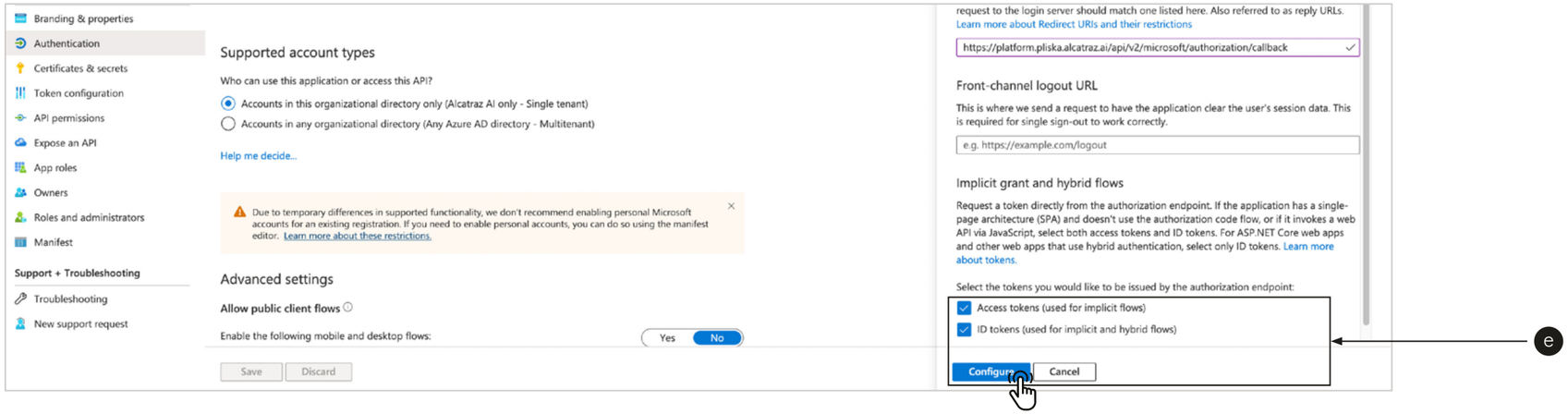
8. Configure the Redirect URI.
   a. Go to **Authentication** and click **Add a platform**.
   b. Click on **Web** option.



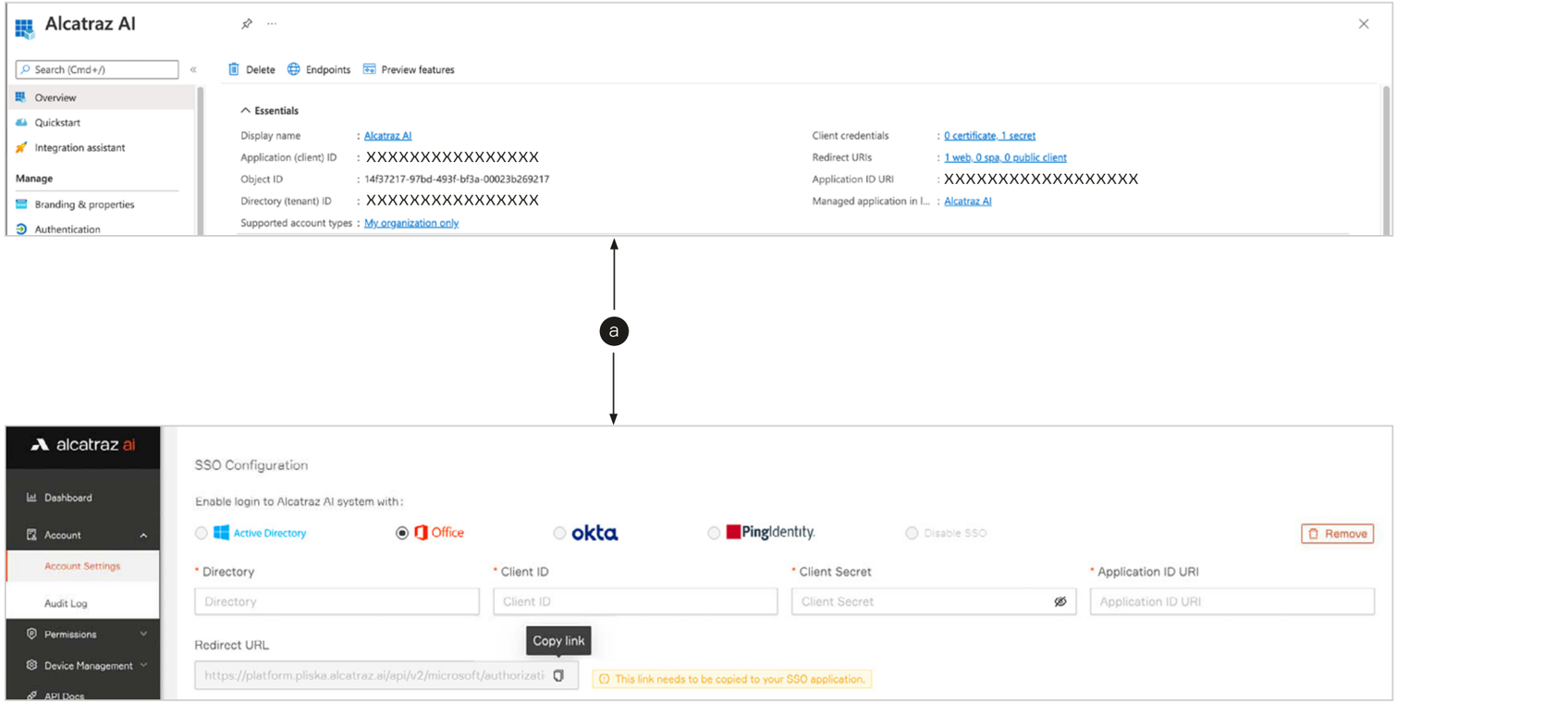
   c. Open the Alcatraz Admin Portal, go to **Account —> Account settings,** scroll down to the **SSO Configuration** section and click to open it. Select **Office** of the displayed SSO provider options.
   d. Copy the **Redirect URL** of the Alcatraz Admin Portal and place it to the **Redirect URI** of the **Configure Web** section.



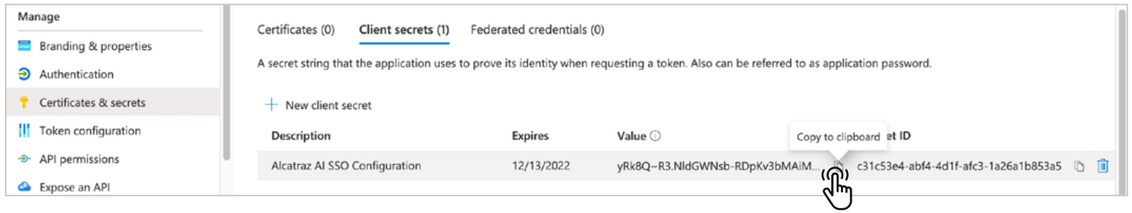
e. Select the **Access tokens** and **ID tokens** options and click **Configure.**



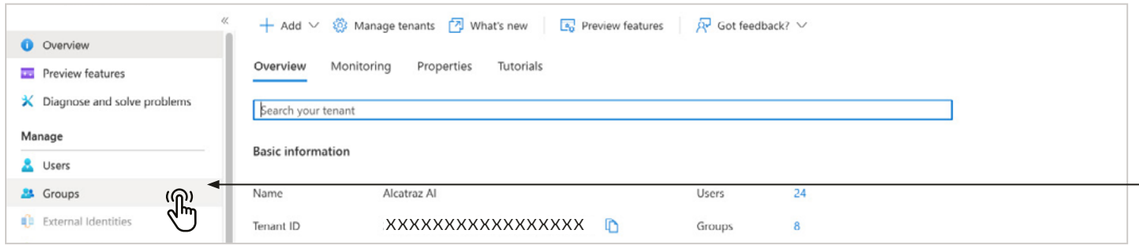
9. Configure the Alcatraz Admin Portal
   a. Couple of credentials need to be copied from the new registered a Microsoft Azure. Click **Overview** and copy the following credentials and place it to Alcatraz AI SSO section:
   —**Application (client) ID** to **Client ID**
   —**Directory (tenant) ID** to **Directory**
   —**Application ID URI** to **Application ID URI**



b. For **Client Secret** field place the value of the client secret that was created earlier. (Step 4)

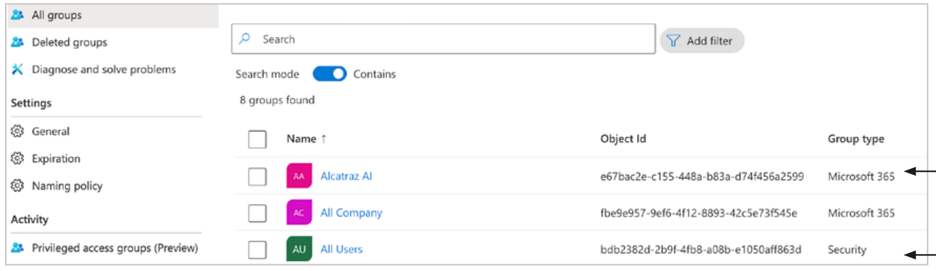


10. Map the Microsoft Azure groups to the **Alcatraz roles.**
    Note: At least one group must be mapped to Alcatraz role.
    a. Under **Manage** select **Groups.**
    b. Copy the names of the groups that will be mapped in Alcatraz AI system. Assign a selected group to

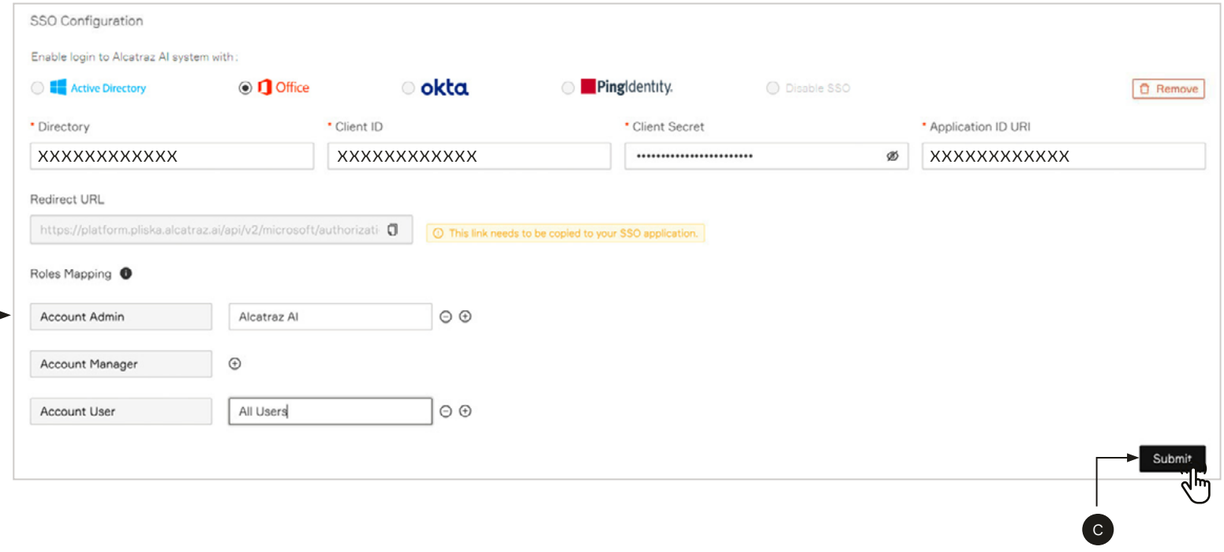


a

preferred user role. The mapping allows more than one group to be assigned to a role.
c. Click **Submit** when ready.

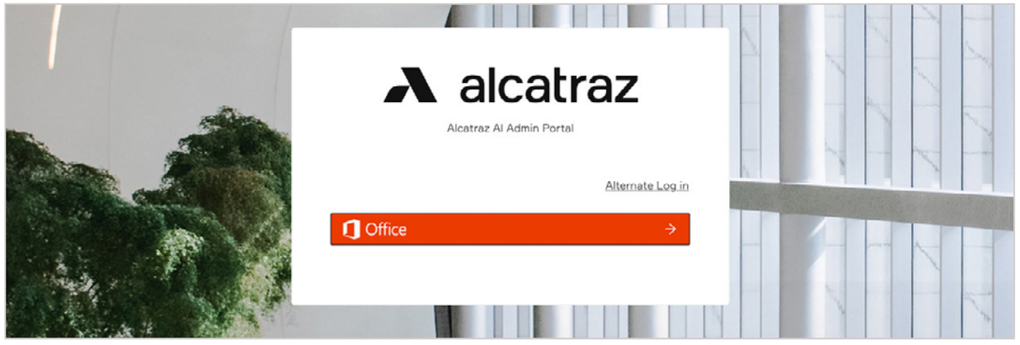


b



c

11. Log out and a new login screen will be available, allowing to use Office as identity provider to log to the platform.

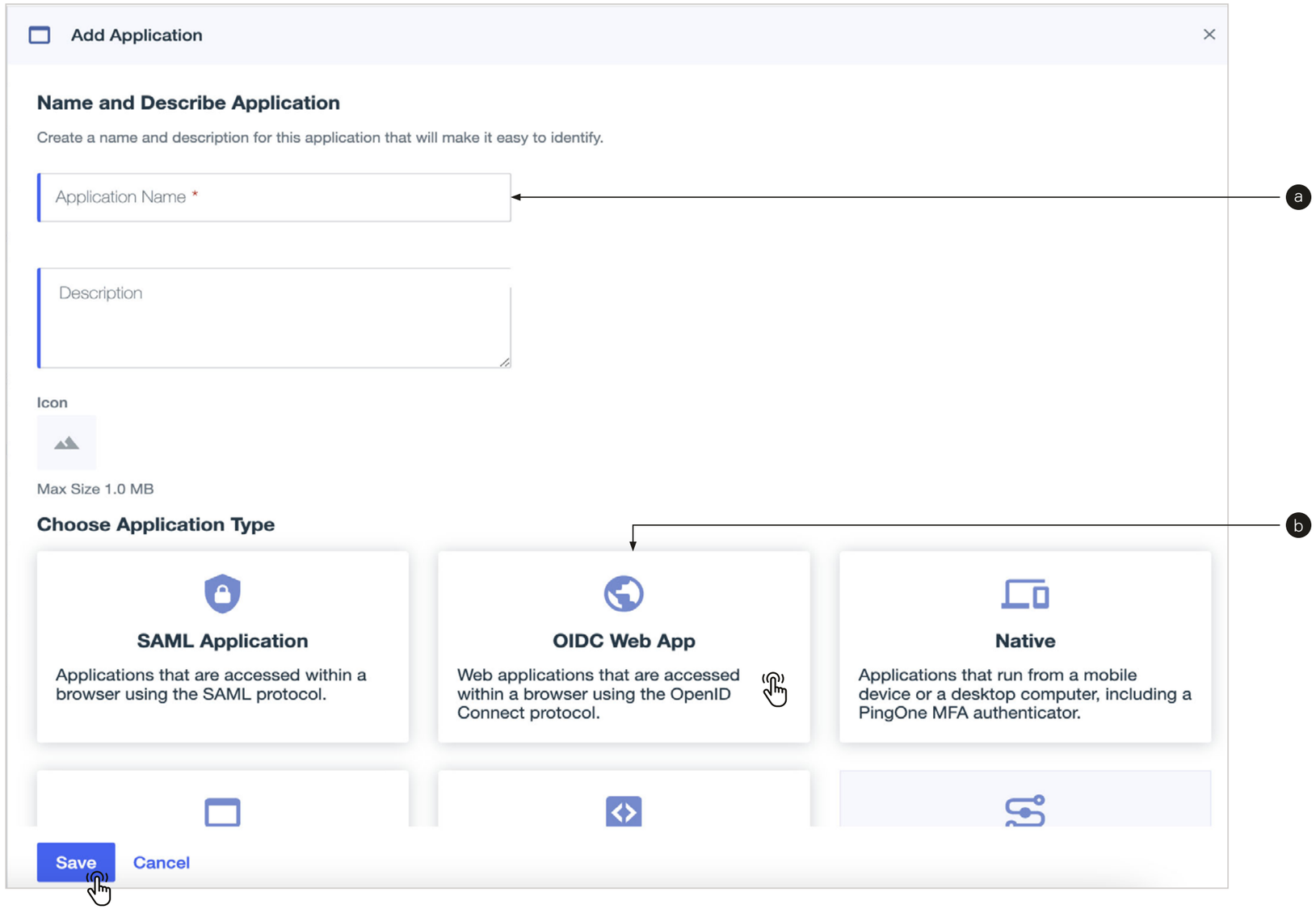


3—SSO with Ping Identity

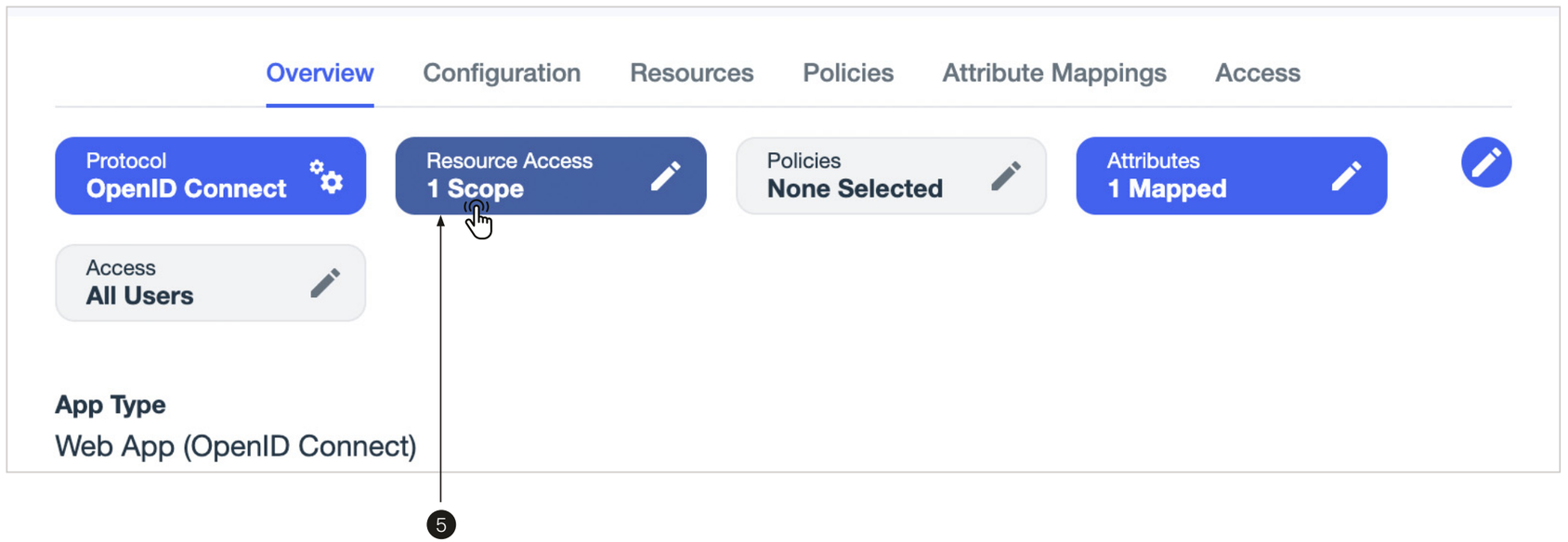
Before you can sign a user in Alcatraz AI Platform using Ping as an identity provider, you need to create a Ping application integration that represents Alcatraz AI system in Ping and from where the required configuration will be fetched.

1. Sign in to your **Ping** organization with an account with sufficient permissions.
2. In the Admin Console, go to **Connections —> Applications.**
3. Click on the **plus (+)** icon to create a new application.

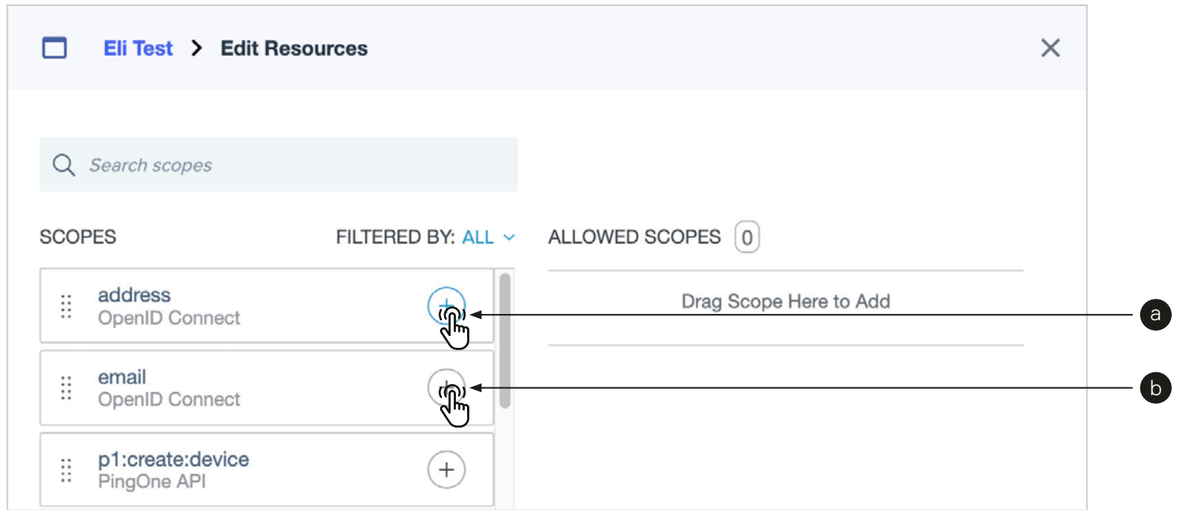
4. **Add Application** screen will load. Configure the app as follow:
   a. Enter an **Application Name.**
   b. For **Application type** choose **OIDC Web App** and select the **Save** button.
   Our system supports only OIDC, and do not support SAML, Single Page or Workers.



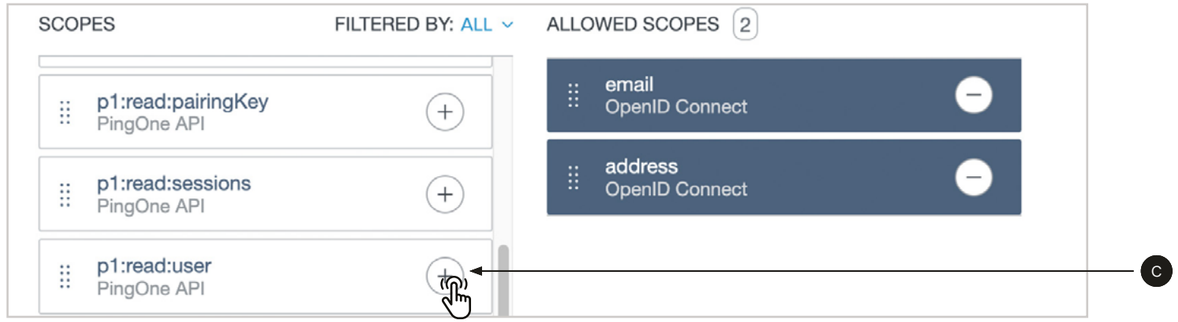
5. On the new application view panel select the **Resource Access** panel.



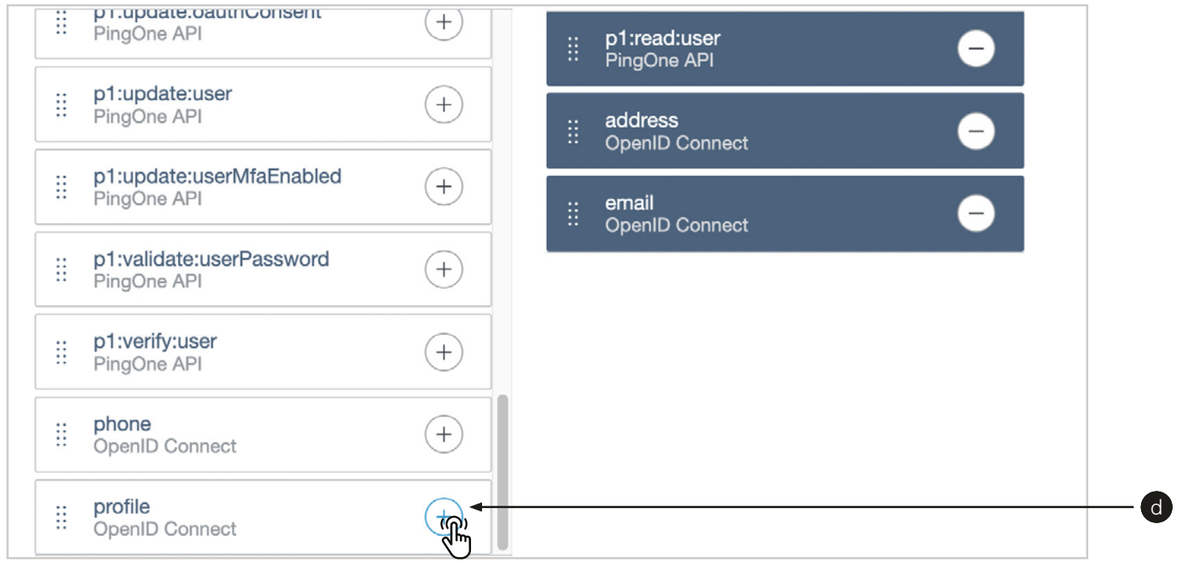
6. Configure the system by select the following **Scopes.** Click the **plus (+)** button, or drag the Scope to the right column to select it.
   a. **address**
   b. **email**



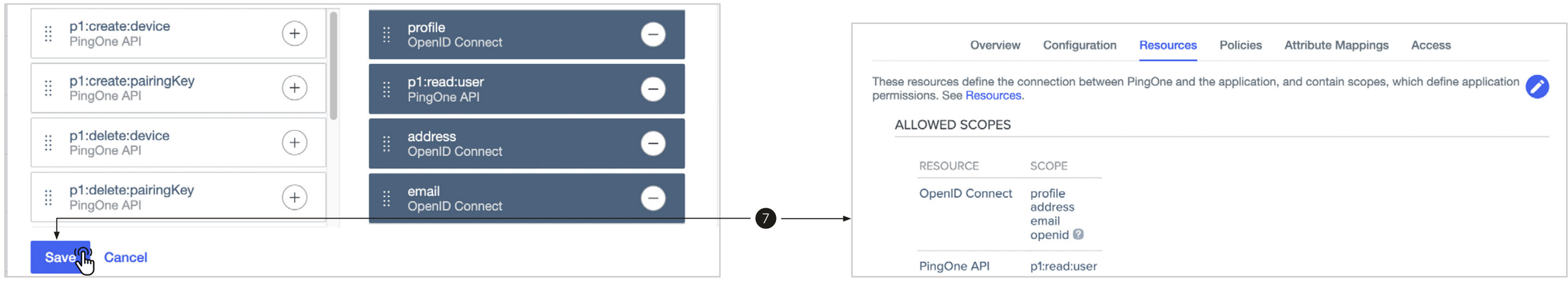
c. **p1:read:user**



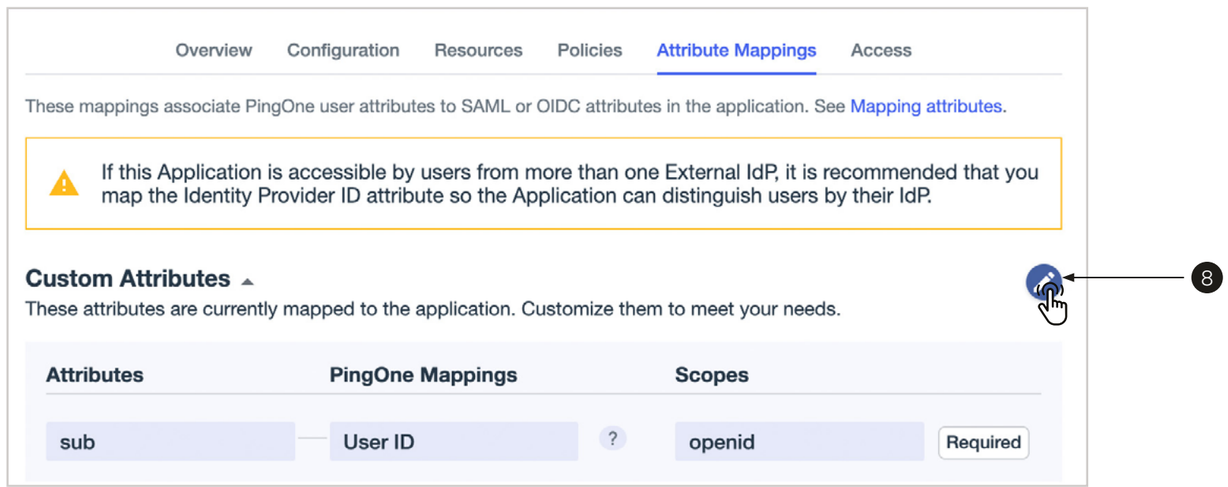
d. **profile**



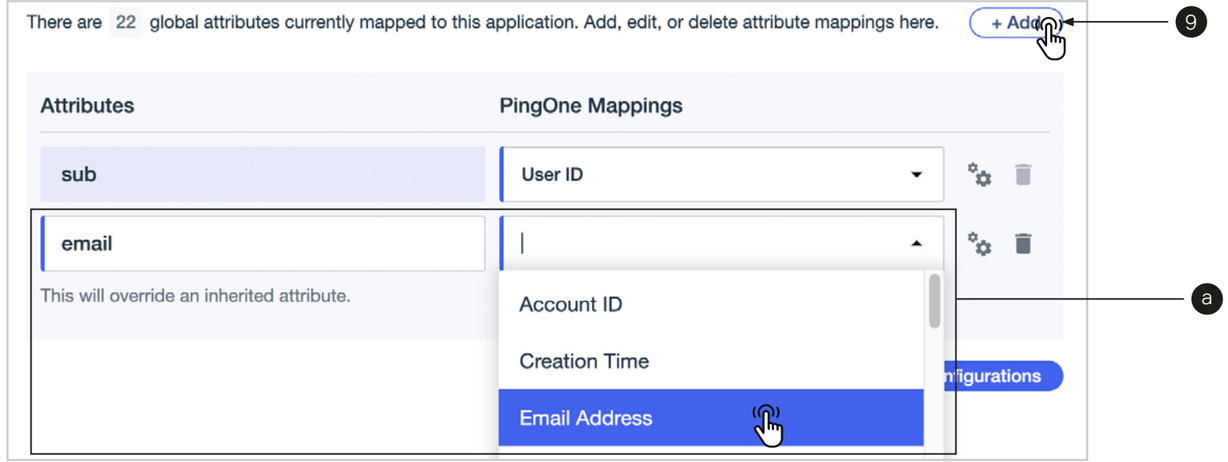
7. After adding the last **Scope** click **Save** and a list of the selected resources will be displayed.



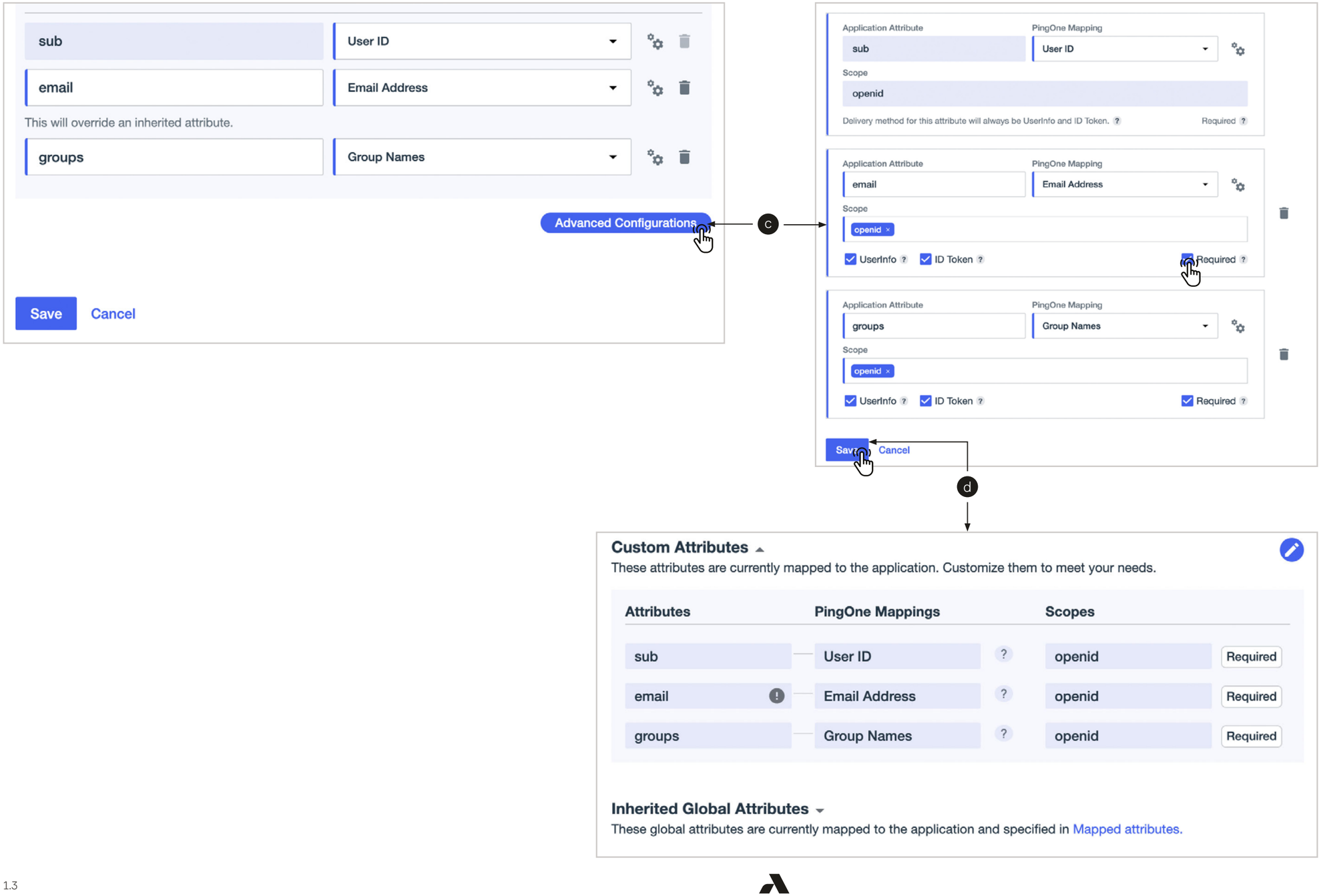
8. Go to the **Attribute Mappings.** Click on the edit icon.



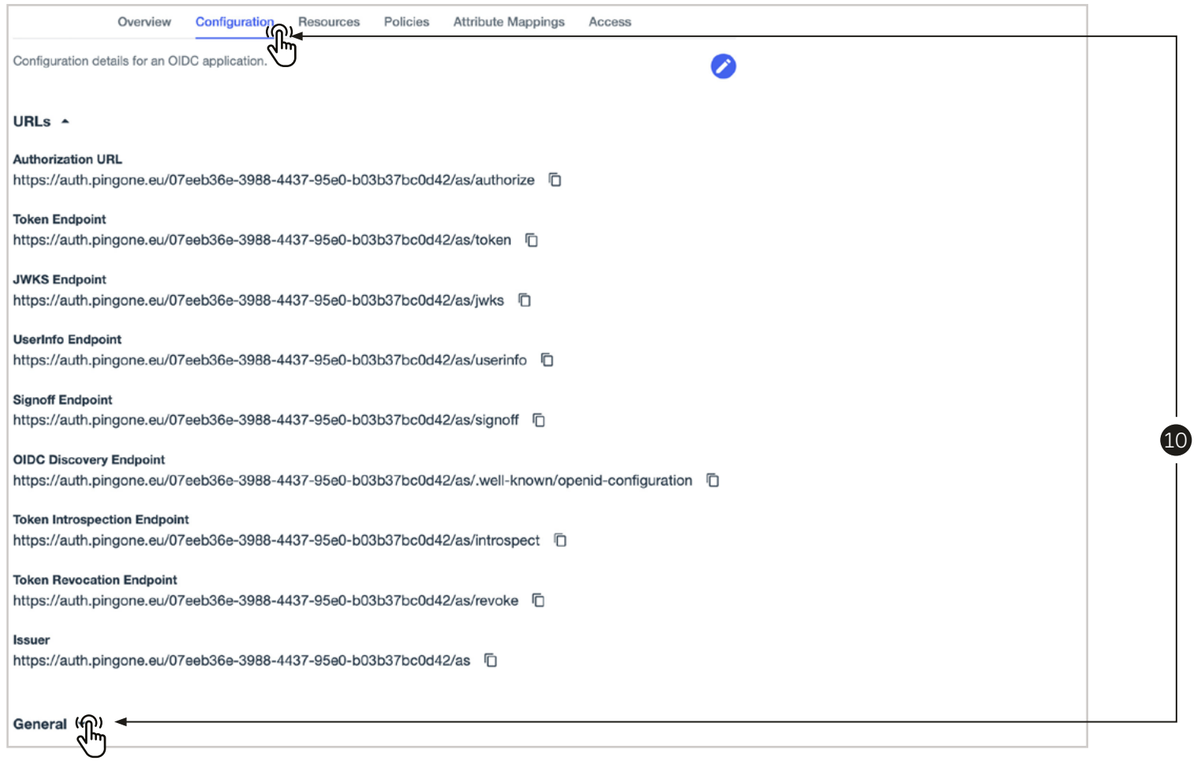
9. Click on the on the **+ Add** button to create the following mappings.
   a. Write **email** in the first field and then select **Email Address** from the drop down list.



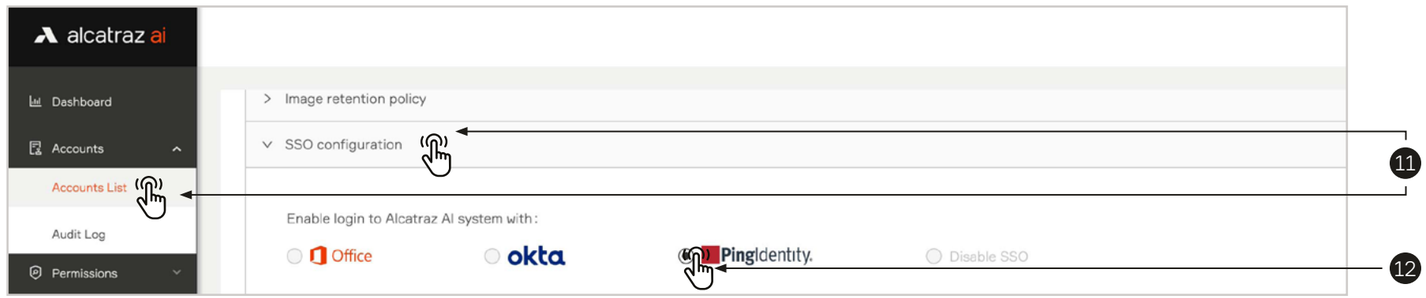
b. Click on the **+ Add** button again. Write **groups** in the first field and then select **Group Name** from the drop down list.
Note that the application attribute names should match exactly.
c. Click on **Advanced Configuration a**nd select the **Required** checkbox on both application attributes (**email** and **groups**).
d. Click **Save** and the attributes will be added.



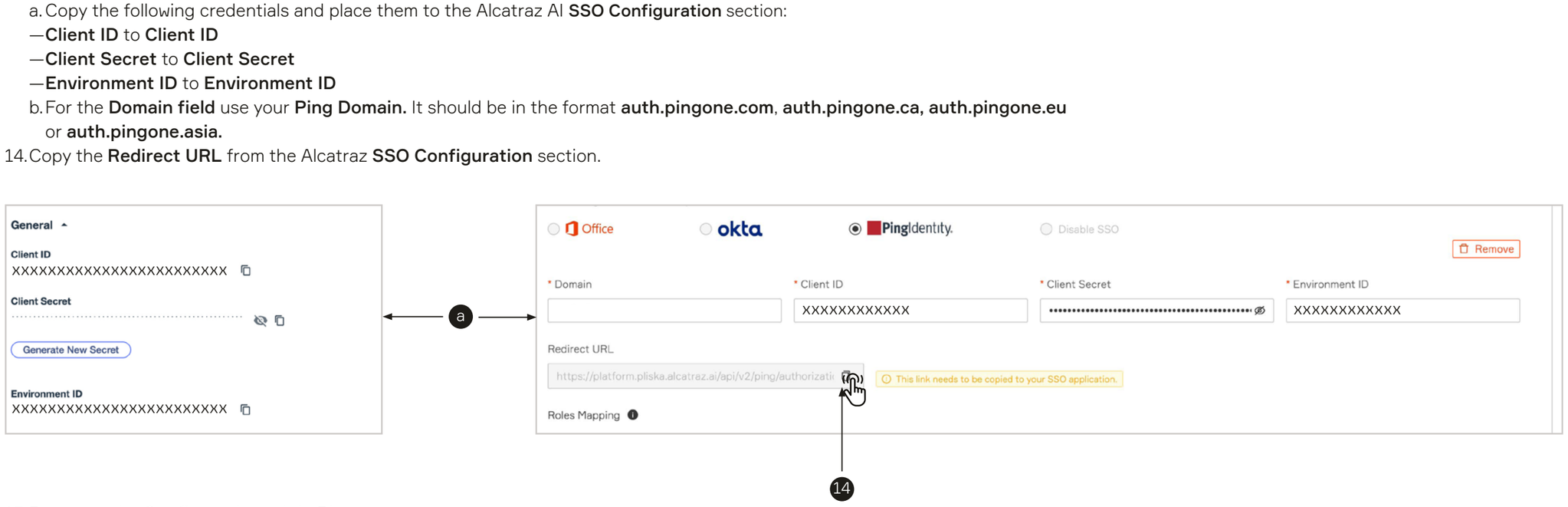
10. Select the **Configuration** tab and then select **General** button from where we will get the required configuration that will be needed by the Alcatraz Admin Portal.



11. Open the Alcatraz Admin Portal, go to **Account –> Account settings,** scroll down to the **SSO Configuration** section and click to open it.
12. Select **Ping Identity** of the displayed identity provider options.

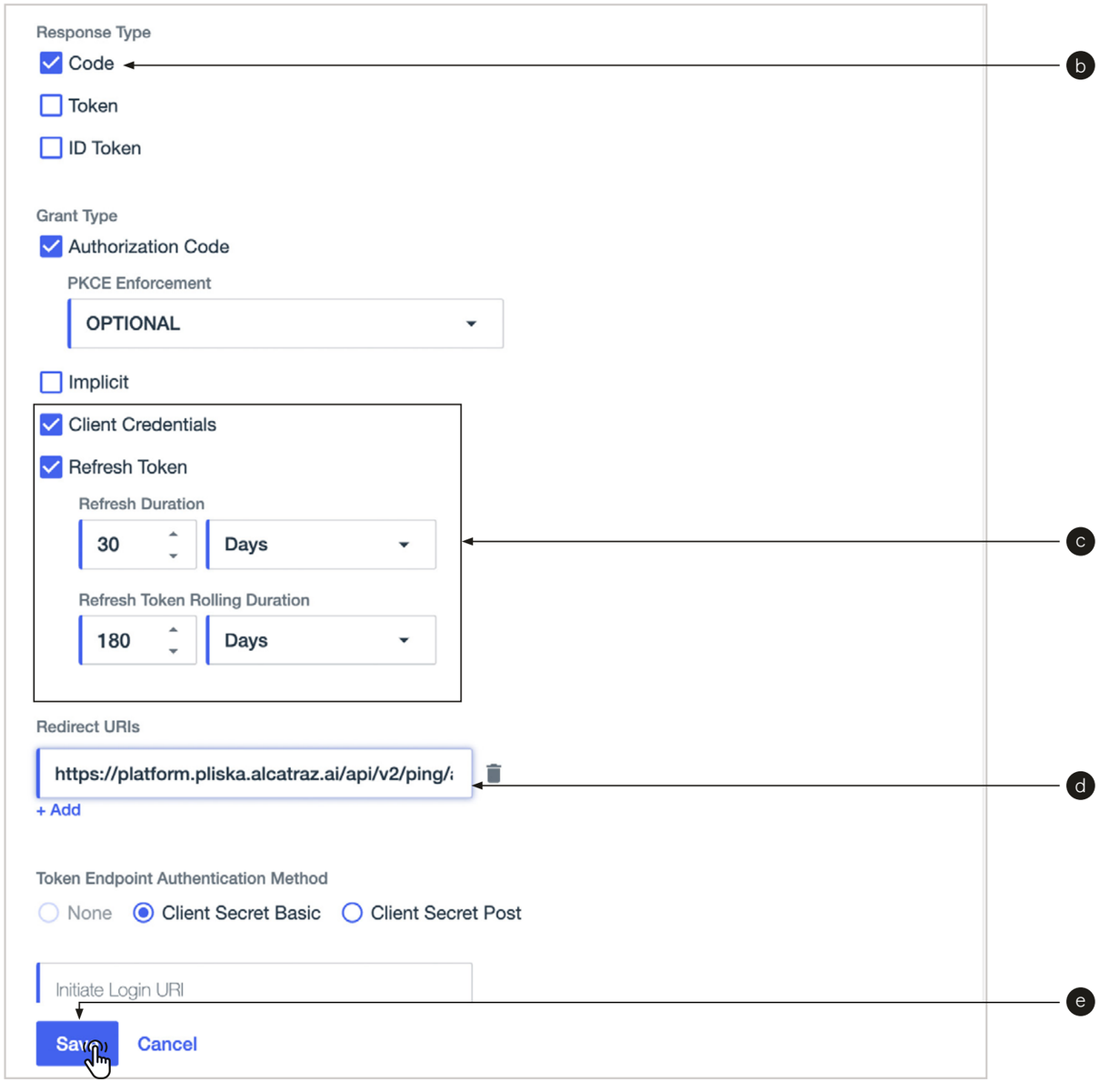


13. Return to the **Ping Admin** console, **Configuration** tab, **General** section.
    a. Copy the following credentials and place them to the Alcatraz AI **SSO Configuration** section:
    —**Client ID** to **Client ID**
    —**Client Secret** to **Client Secret**
    —**Environment ID** to **Environment ID**
    b. For the **Domain field** use your **Ping Domain.** It should be in the format **auth.pingone.com**, **auth.pingone.ca, auth.pingone.eu** or **auth.pingone.asia.**
14. Copy the **Redirect URL** from the Alcatraz **SSO Configuration** section.

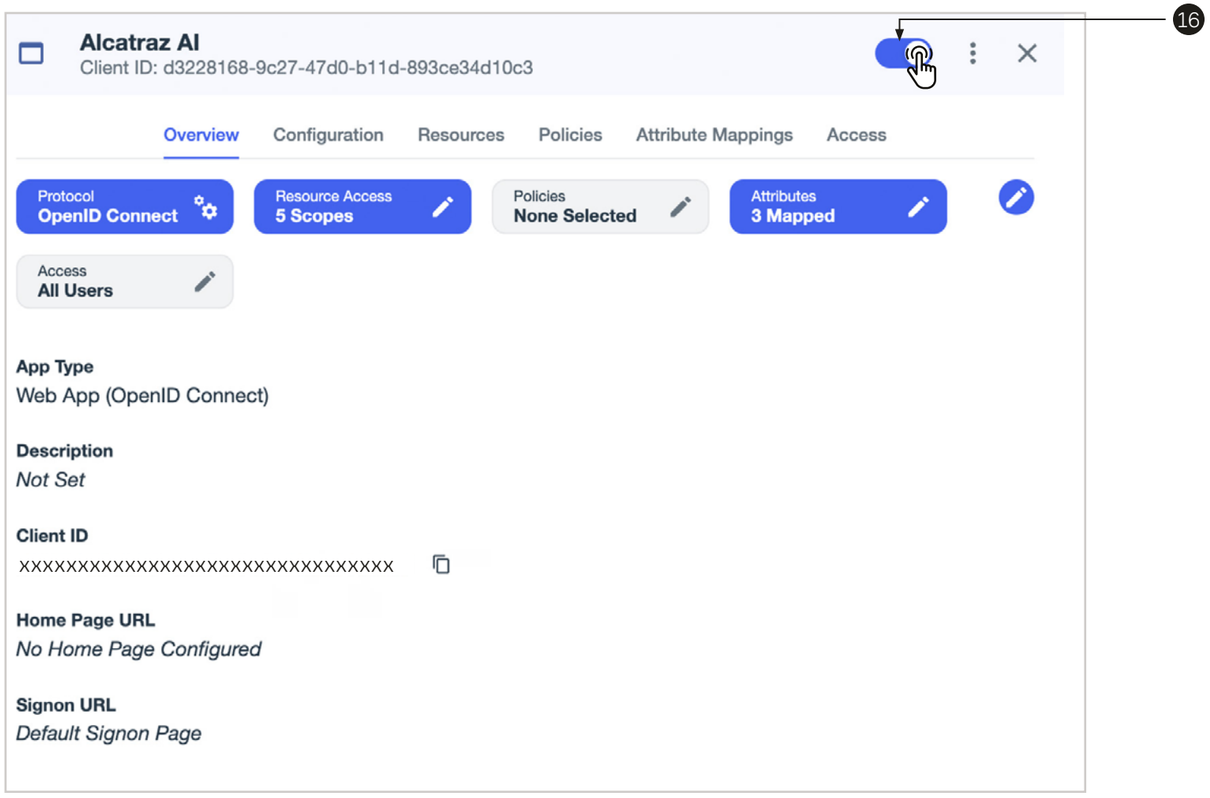


15. Return to the **Configuration** tab in Ping.
    a. Click the edit button.
    Edit Configuration section will be displayed.

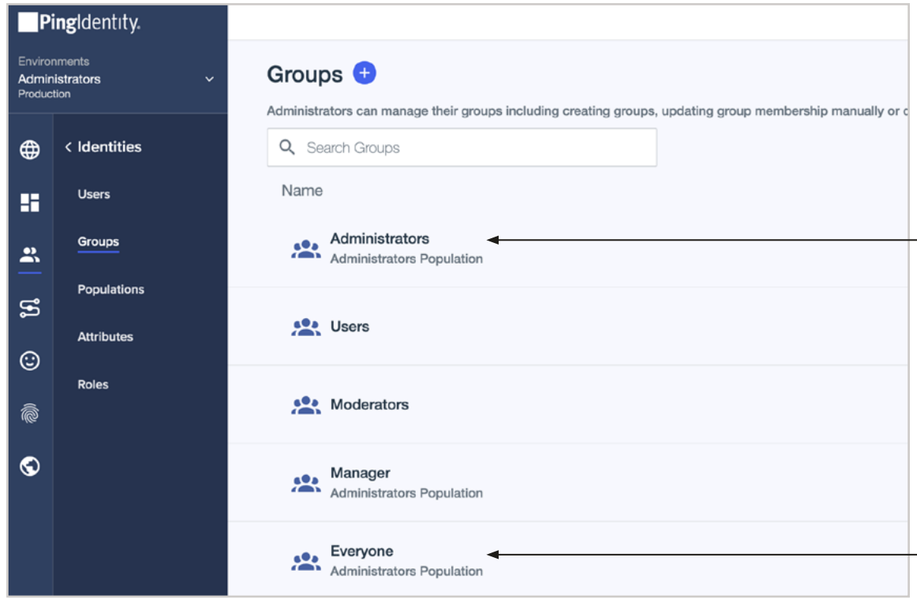
b. For **Response Type** our system supports: **Code. (Token and Token ID are not supported)**
c. For **Response Type** select **Client Credentials** and **Refresh Token.**
d. In he **Redirect URIs** field paste the **Redirect URL** (of the Alcatraz Platform).
e. Click **Save.**



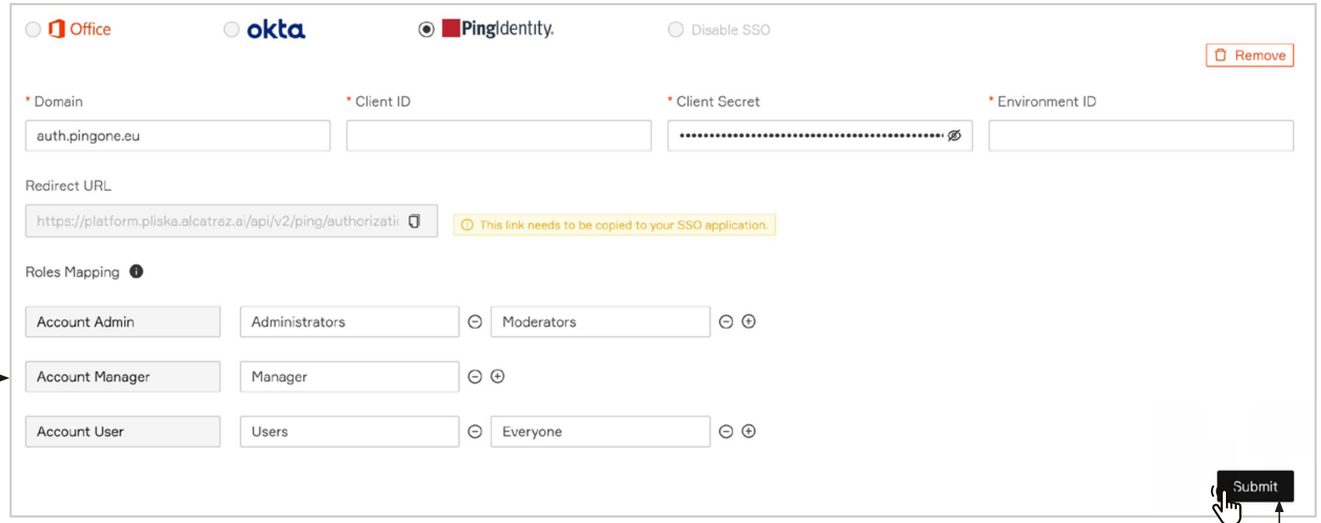
16. Enable the application by turning on the toggle.



17. Map Ping Identity Groups to **Alcatraz roles.**
    a. Go to **Identities —> Groups.**
    b. Copy the names of the groups that will be mapped in Alcatraz AI system. Assign a selected group to preferred user role.
    The mapping allows more than one group to be assigned to a role.
    Note: At least one group must be mapped to Alcatraz role.
    c. Click **Submit** when ready.

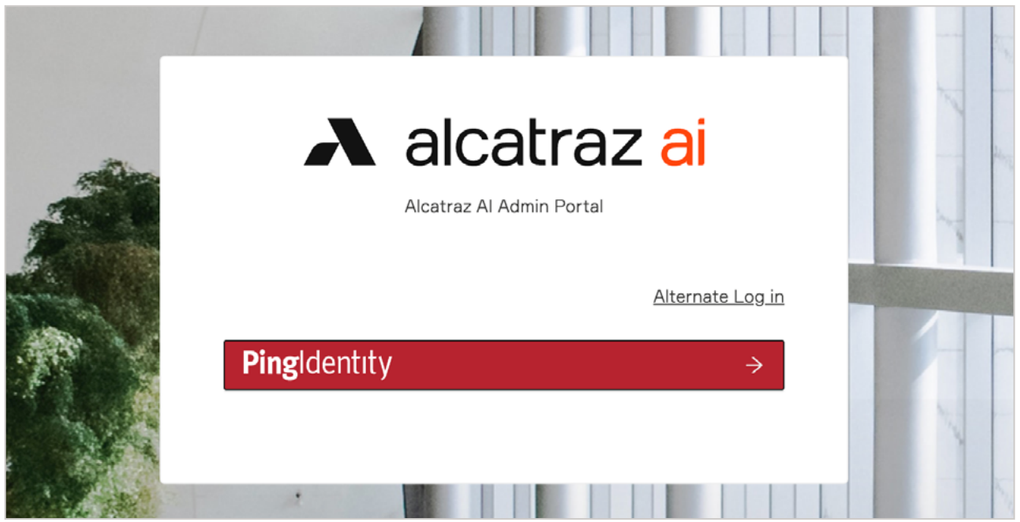


b



c

18. Log out and a new login screen will be available, allowing to use **Ping Identity** as identity provider to log to the Alcatraz AI platform.



alcatraz ai