

Alcatraz AI Admin Portal SSO Configuration

Table of Contents

1—SSO with Okta. 3

2—SSO with Azure 9

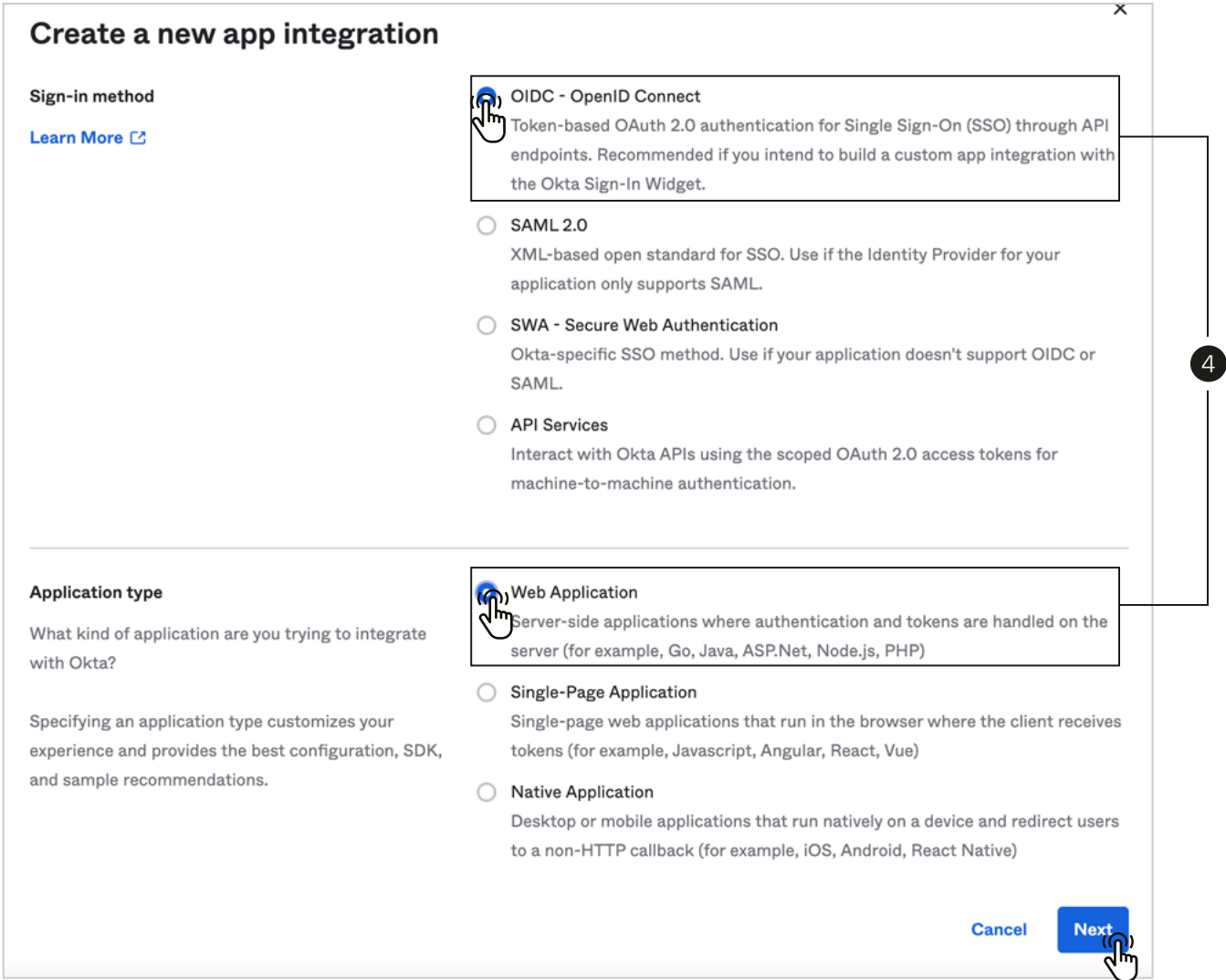
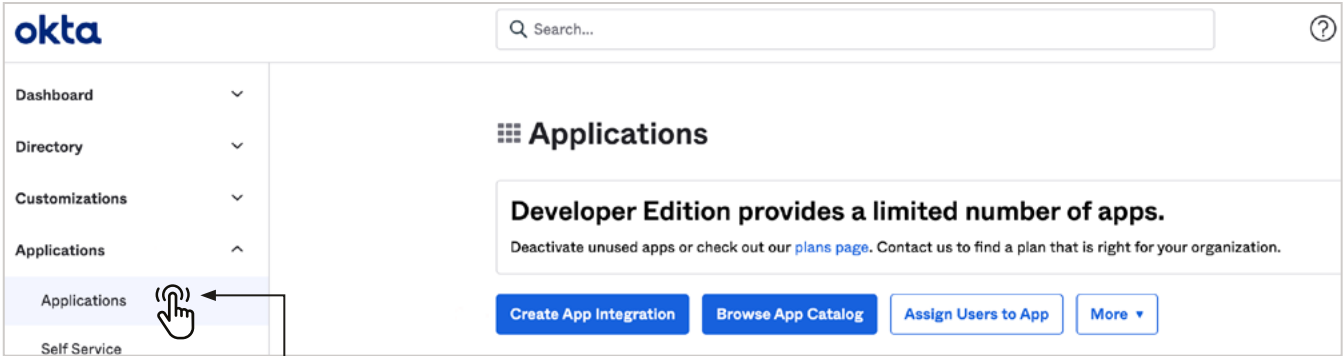
3—SSO with Ping Identity 19



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.

Okta

Search...

New Web App Integration

General Settings

App integration name: Alcatraz AI

Logo (Optional)

Grant type

- ☒ Client acting on behalf of itself
 - ☒ Client Credentials
 - ☒ Authorization Code
 - ☒ Refresh Token
 - ☐ Implicit (hybrid)

[Learn More](#)

- 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.alcatraz.ai>).
- c. For **Controlled access** section choose option by your organization preferences.
- d. Click **Save**.

Okta - New Web App Integration

Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs.

[Learn More](#)

☐ Allow wildcard * in sign-in URI redirect.

<https://platform.sso-dev.alcatraz.ai/api/v2/okta/authorization/callback> [x]

[+ Add URI](#)

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

[Learn More](#)

<https://platform.sso-dev.alcatraz.ai> [x]

[+ Add URI](#)

Trusted Origins

Base URIs (Optional)

Required if you plan to self-host the Okta Sign-in Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

[Learn More](#)

[+ Add URI](#)

Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

- ☐ Allow everyone in your organization to access
- ☐ Limit access to selected groups
- ☐ Skip group assignment for now

[Save](#) [Cancel](#)

Alcatraz AI - SSO Configuration

Enable login to Alcatraz AI system with:

- ☒ Active Directory
- ☐ Office
- ☒ Okta
- ☐ Pingidentity
- ☐ Disable SSO

Domain

Domain

Client ID

Client ID

Client Secret

Client Secret

Redirect URL

<https://platform.sso-dev.alcatraz.ai/api/v2/okta/authorization/callback> [Copy link](#)

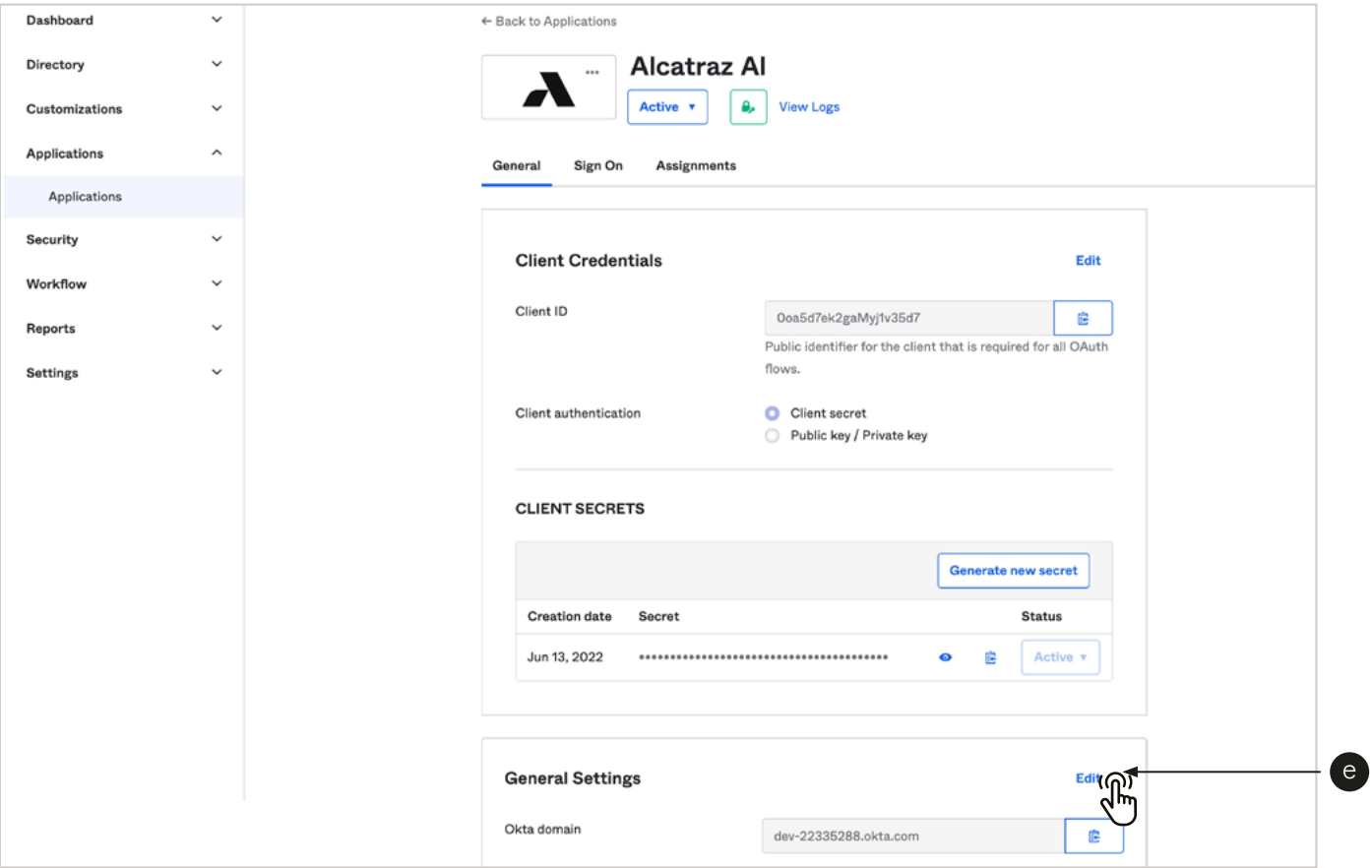
This link needs to be copied to your SSO application.

Roles Mapping

- Account Admin
- Account Manager
- Account User



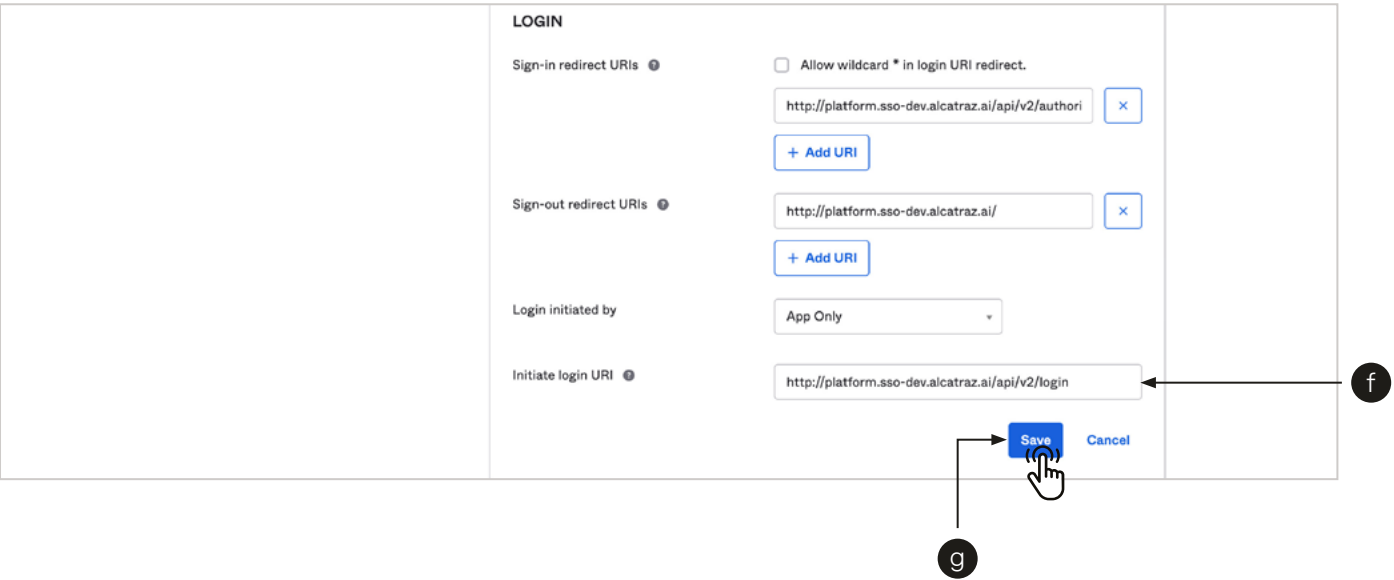
e. After saving – the system will open display the settings of the already created integration app.
In **General** tab scroll down and click **Edit** button of the **General Setting** section.



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.

okta

Search...

guide@alcatraz.ai
okta-dev-22335288

Dashboard

Directory

Customizations

Applications

Security

General

HealthInsight

Authentication

Multifactor

Identity Providers

Delegated Authentication

Networks

Behavior Detection

API

API

Authorization Servers

Tokens

Trusted Origins

Create Token

Token value

Find Token

Search by

Last used: Most recent

Token Types

All

0

Health Check

Suspicious tokens

0

Token Name

Created

Expires

Last Used

Revoke

01101110

01101111

01101100

01101100

01101101

01101110

01100111

Nothing to show

We couldn't find any tokens

Create Token

What do you want your token to be named?

Enter a name for this token...

The token name is used for tracking API calls.

Create Token

Cancel

Create Token

Token created successfully!

Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.

Token Value

00c-zNsdwX6PeP5rNFvoL6501clZmqJyBkKqjmYm5f

OK, got it

alcatraz ai

SSO Configuration

Enable login to Alcatraz AI system with:

Active Directory

Office

okta

Pingidentity

Disable SSO

Domain

Client ID

Client Secret

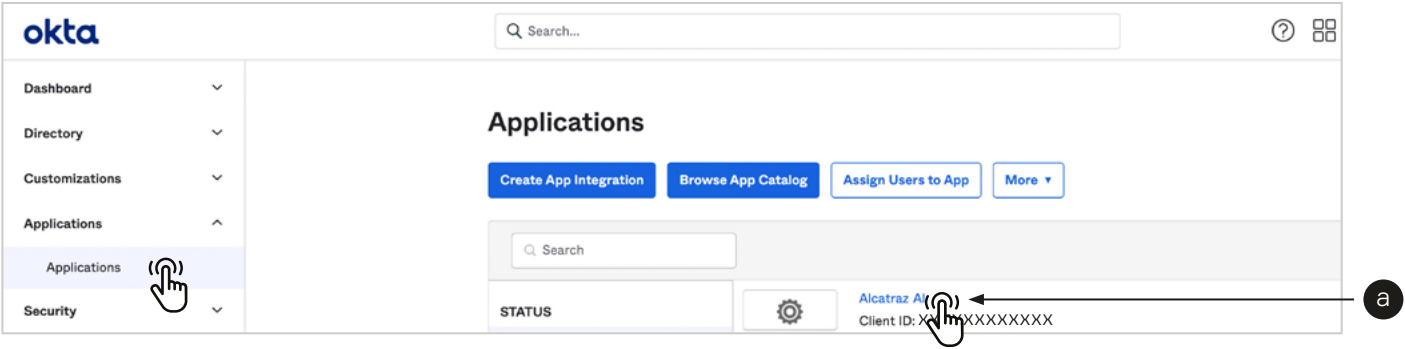
API Key

Remove

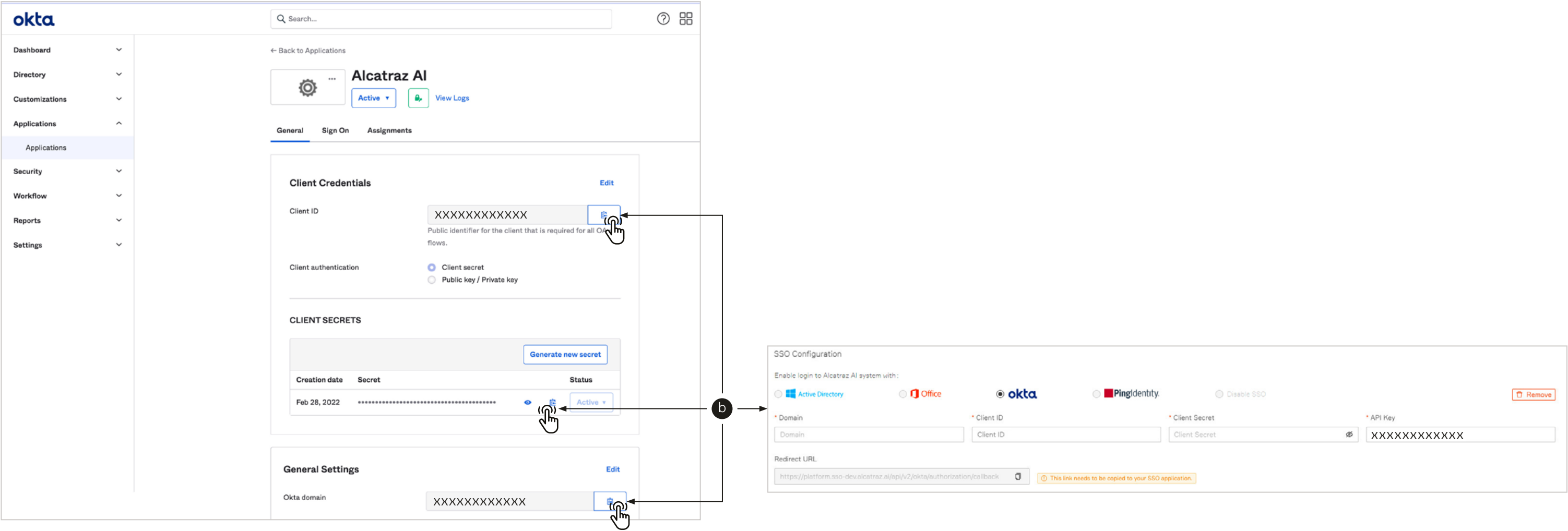
- c. Copy the token value and add it to the API key field (in the Alcatraz AI UI).
Copy the token value right after creating the token. By security policies the value is visible only while creating it.
Note: tokens expire automatically after a certain period and can also be deactivated at any time. Once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



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.

okta

Search...

Dashboard

Directory

People

Groups

Profile Editor

Directory Integrations

Self-Service Registration

Profile Sources

Customizations

Applications

Security

Groups

All Rules

Add Group

Source	Name	People	Apps
	Admins Admins group	5	2
	Alcatraz Security Security officers	4	2
	Everyone All users in your organization	14	2
	Manager Account Manager group	4	2

SSO Configuration

Enable login to Alcatraz AI system with:

Active Directory

Office

okta

Pingidentity

Disable SSO

Remove

* Domain

XXXXXXXXXXXX

* Client ID

XXXXXXXXXXXX

* Client Secret

XXXXXXXXXXXX

* API Key

XXXXXXXXXXXX

Redirect URL

https://platform.sso-dev.alcatraz.ai/api/v2/okta/authorization/callback

This link needs to be copied to your SSO application.

Roles Mapping

Account Admin

Moderator

Admins

Account Manager

Manager

Account User

Users

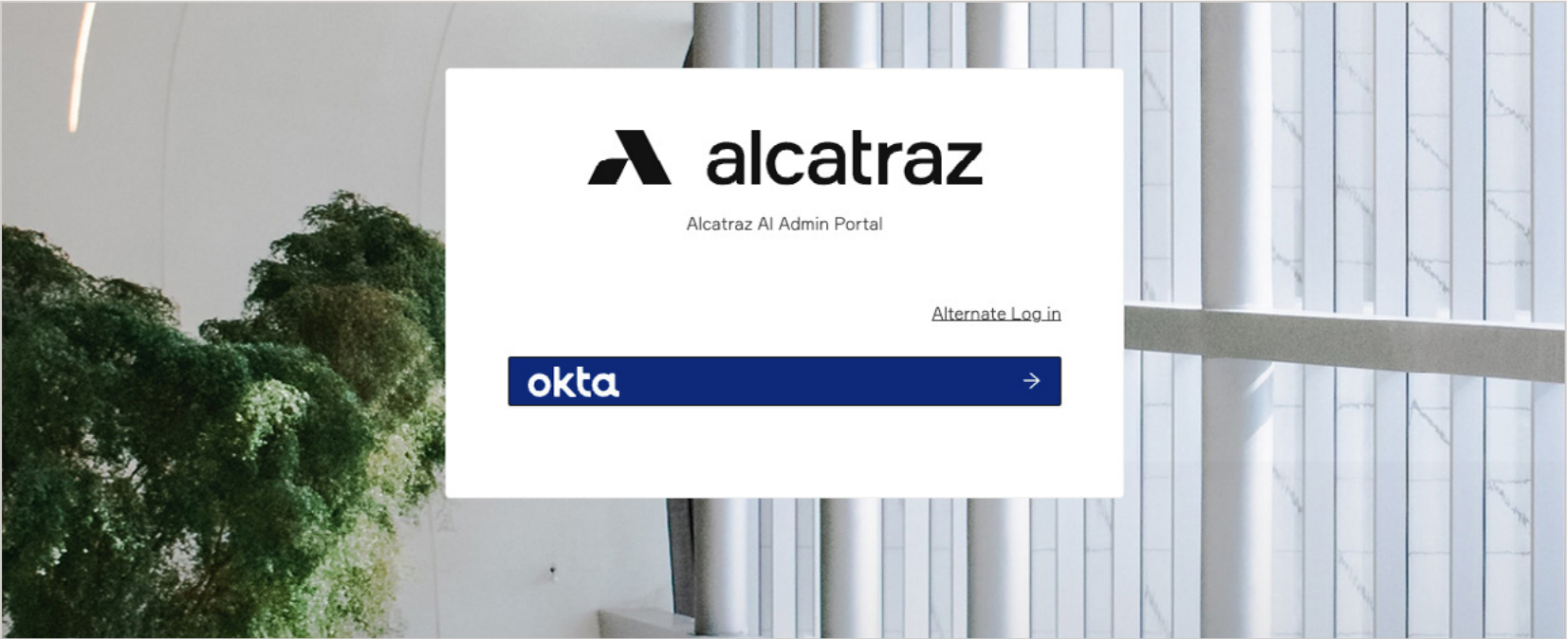
Everyone

Submit

b

c

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

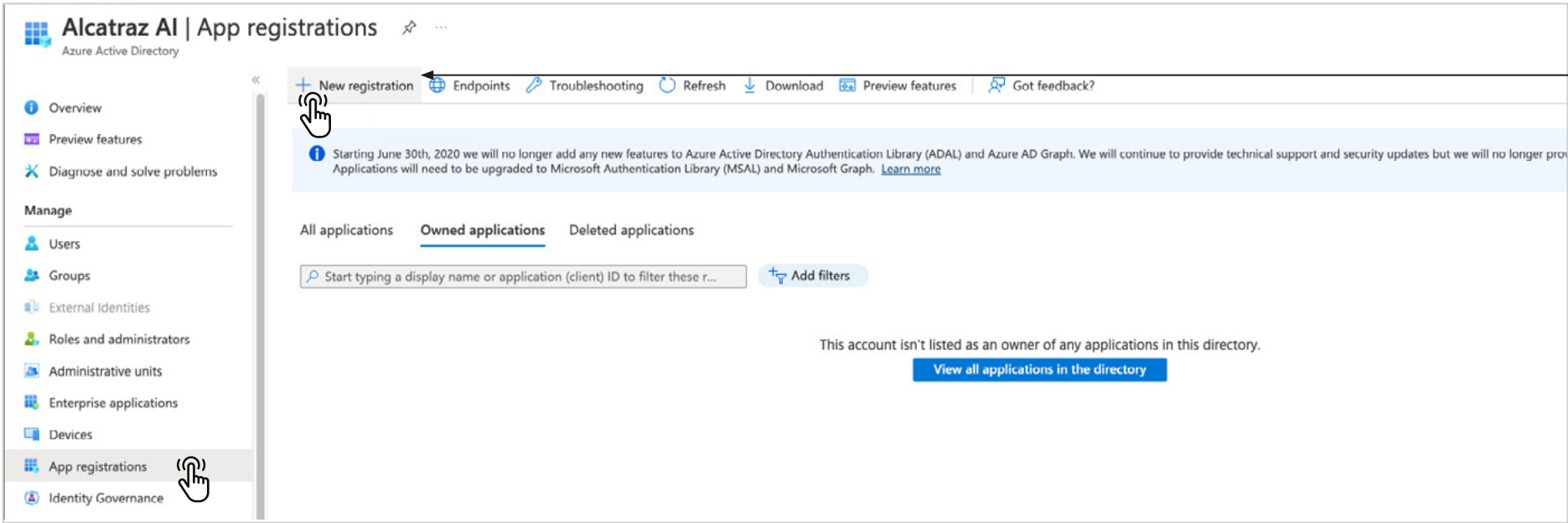
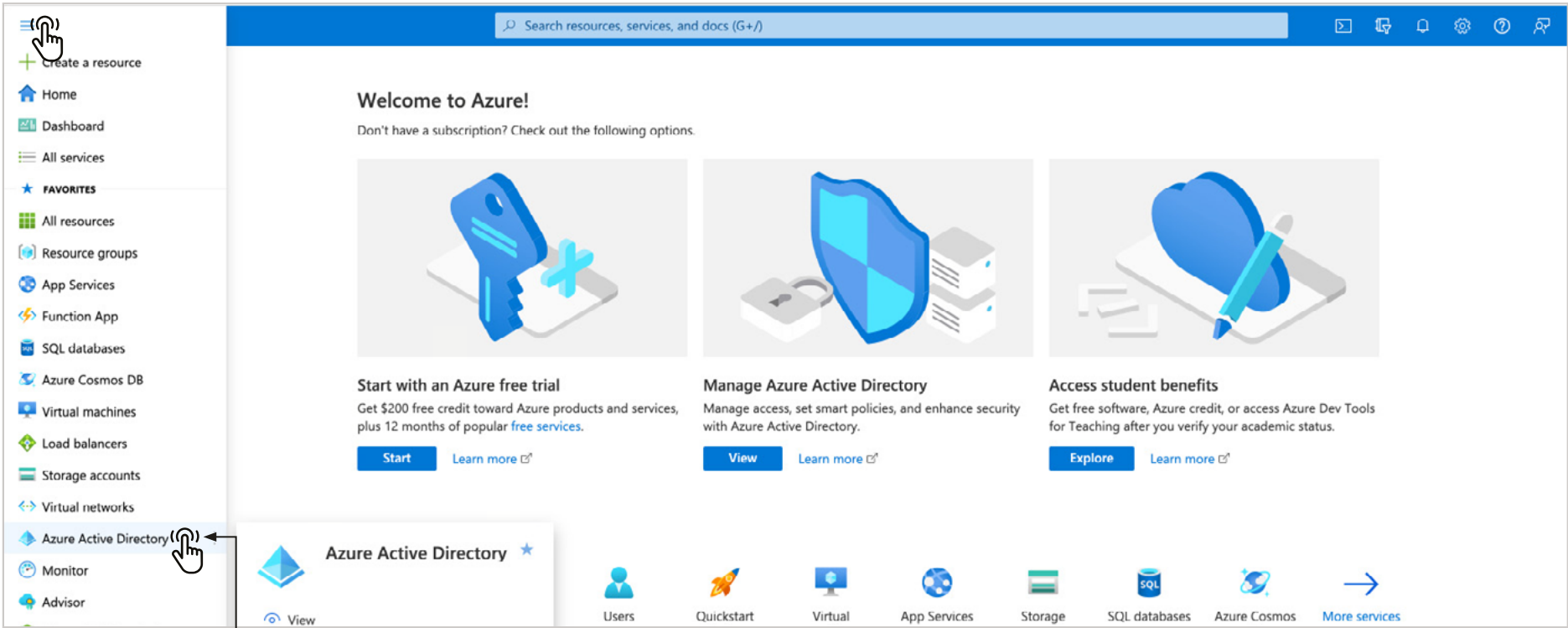


2—SSO with Azure

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.

Register an application

*** Name**

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

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Alcatraz AI 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.

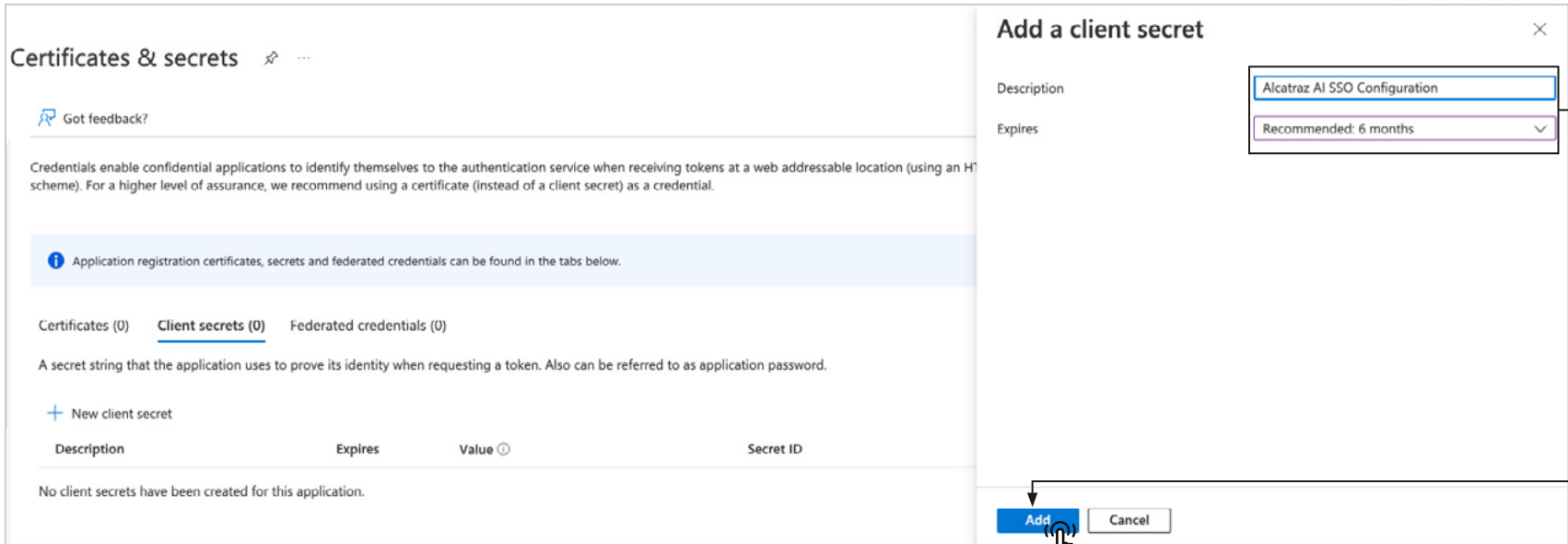
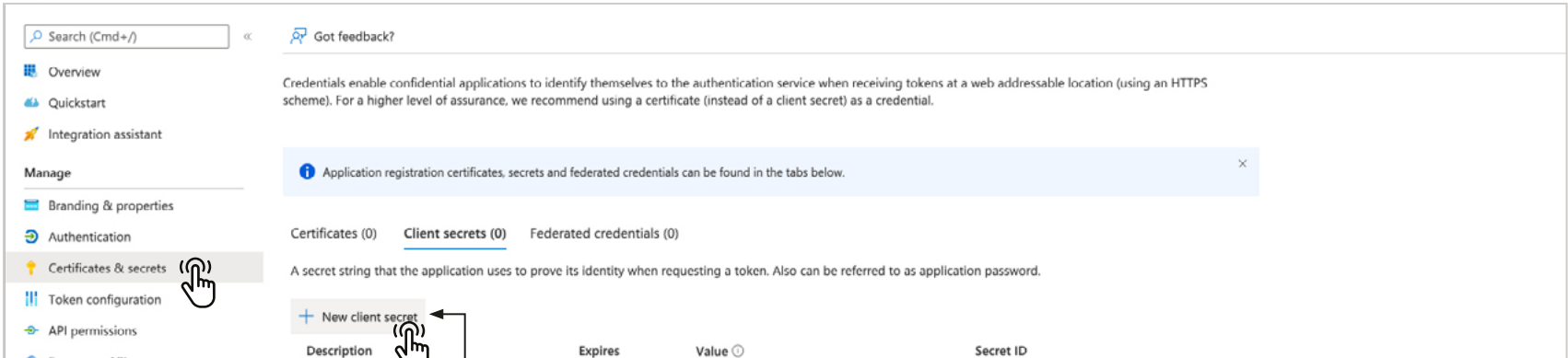
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

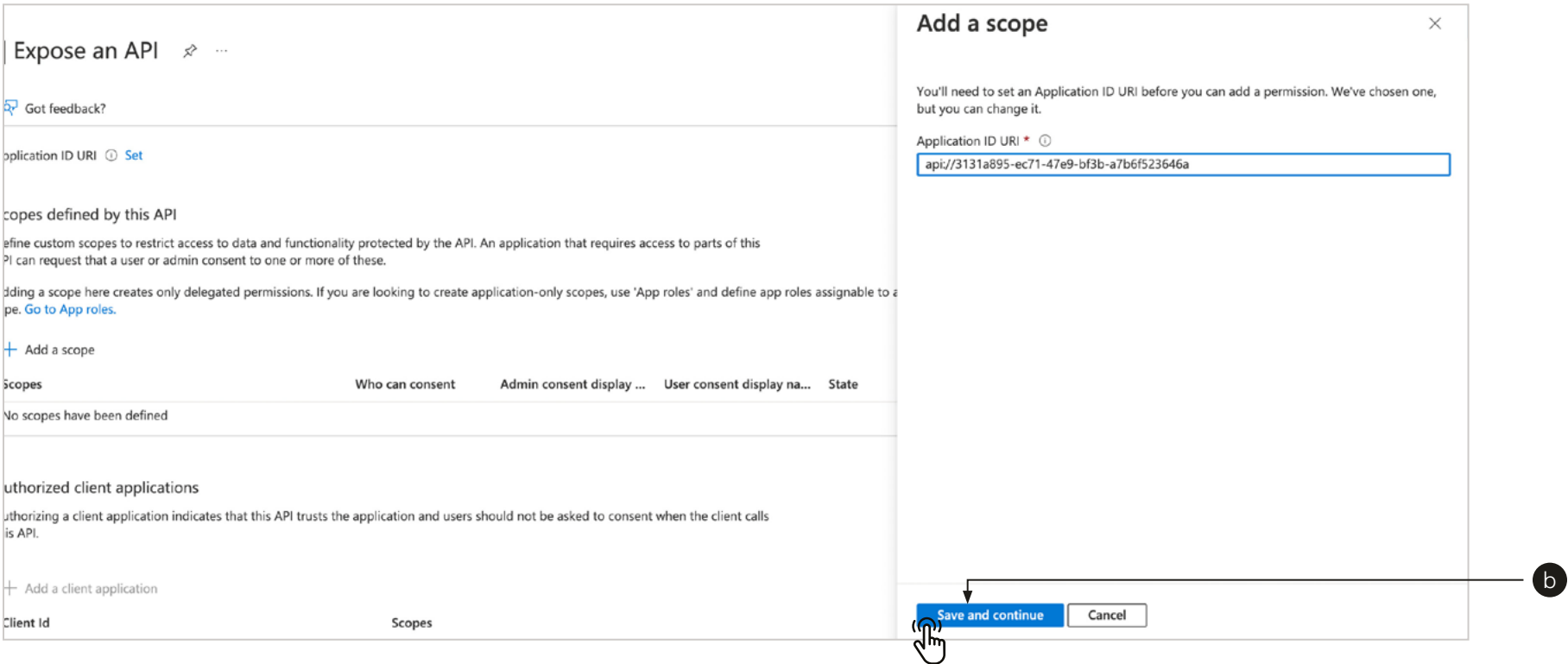
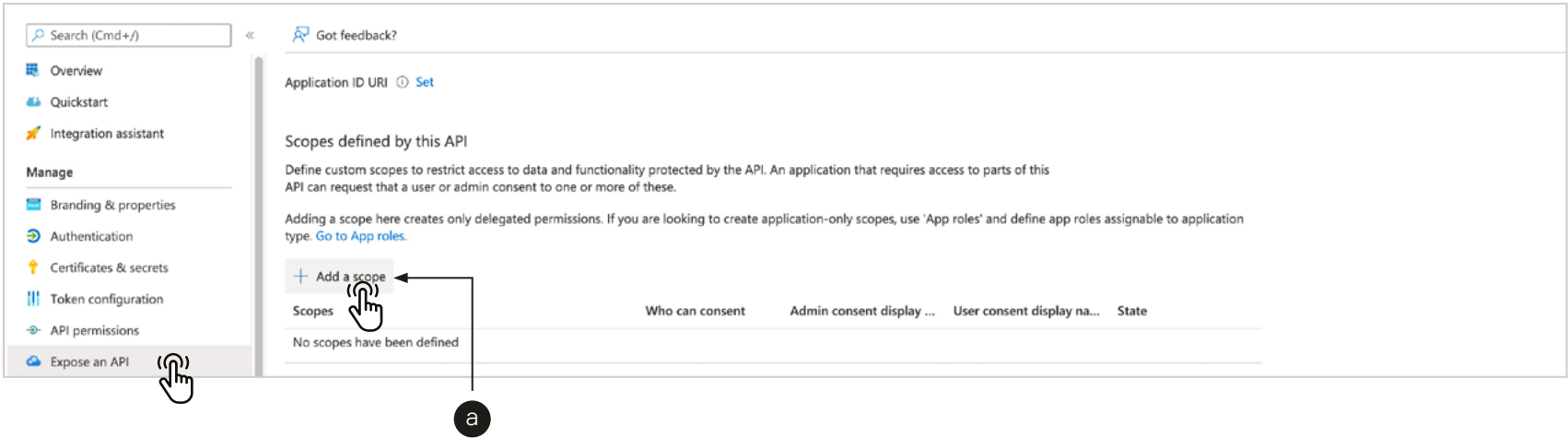
4. Create **Client Secret**.
- a. Go to **Certificates & secrets** and click **New client secret**.
 - b. Add **Description** and select or configure expiration time by your preferences.
 - c. Click **Add** to continue.

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.

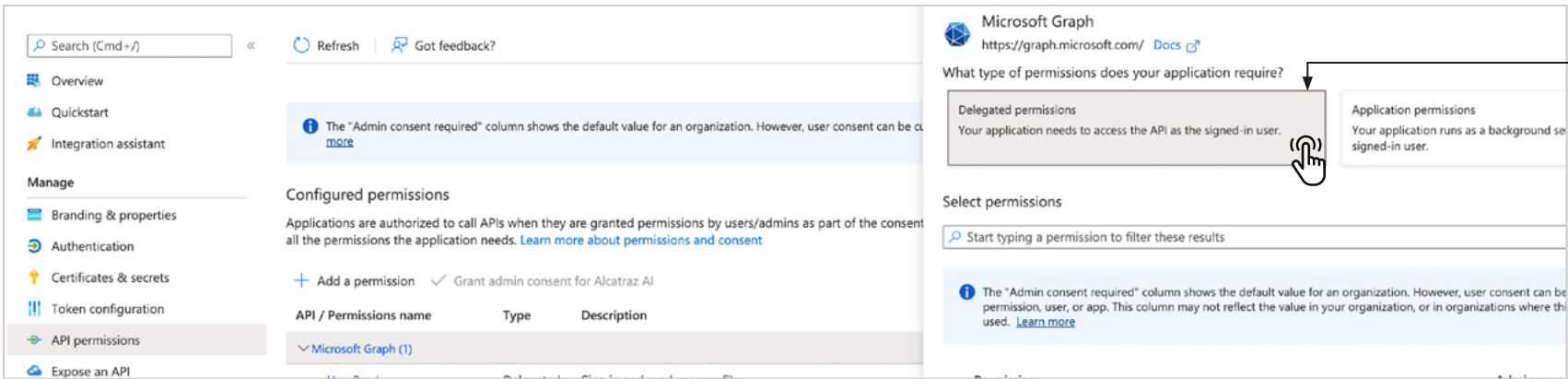
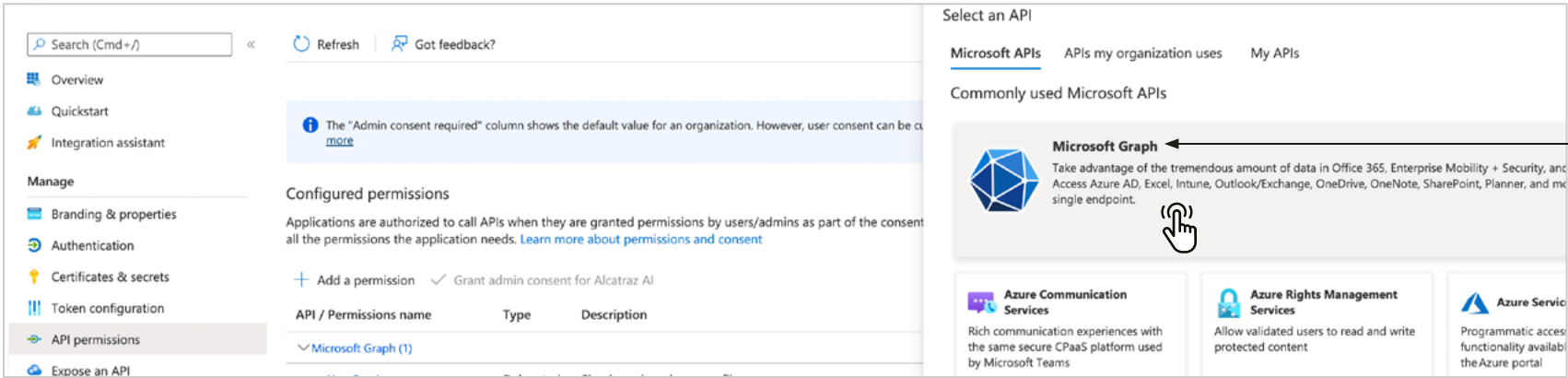
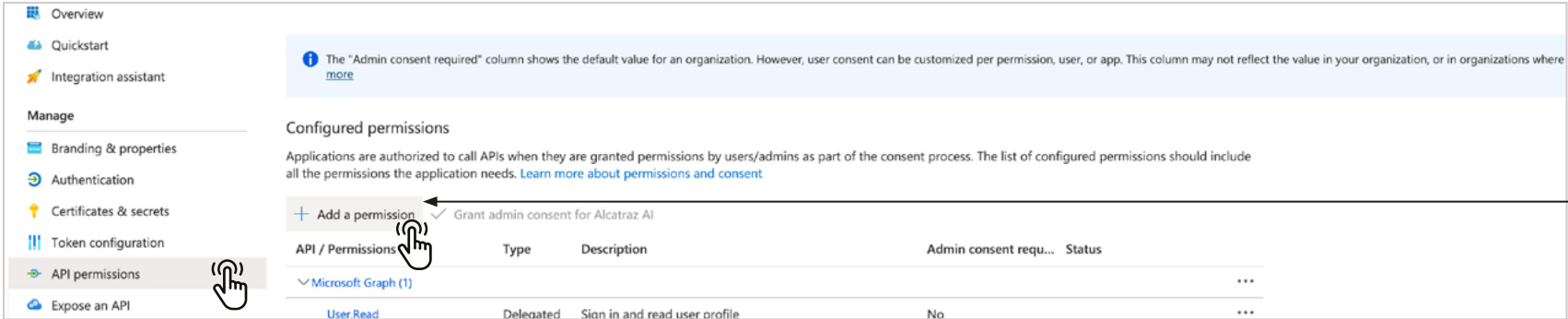
Client secret credentials expire automatically after the selected expiration period. Once a secret credential is expired it should be regenerated and updated in the Alcatraz AI SSO configuration.



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)	
<input checked="" type="checkbox"/> email ⓘ View users' email address	No
<input checked="" type="checkbox"/> offline_access ⓘ Maintain access to data you have given it access to	No
<input checked="" type="checkbox"/> openid ⓘ Sign users in	No
<input checked="" type="checkbox"/> profile ⓘ View users' basic profile	No

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

Group (1)	
<input checked="" type="checkbox"/> Group.Read.All ⓘ Read all groups	Yes
<input type="checkbox"/> Group.ReadWrite.All ⓘ Read and write all groups	Yes
GroupMember (1)	
<input checked="" type="checkbox"/> GroupMember.Read.All ⓘ Read group memberships	Yes

- Under **User: User.Read**

User (1)	
<input type="checkbox"/> User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/> User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/> User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/> 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.

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect what will be used. [Learn more](#)

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

+ Add a permission

✓ Grant admin consent for Alcatraz AI

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (7)				
email	Delegated	View users' email address	No	✓ Granted for Alcatraz AI
Group.Read.All	Delegated	Read all groups	Yes	✓ Granted for Alcatraz AI
GroupMember.Read.All	Delegated	Read group memberships	Yes	✓ Granted for Alcatraz AI
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for Alcatraz AI
openid	Delegated	Sign users in	No	✓ Granted for Alcatraz AI
profile	Delegated	View users' basic profile	No	✓ Granted for Alcatraz AI
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Alcatraz AI

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

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Alcatraz AI? This will update any existing admin consent records this application already has to match what is listed below.

Yes

No

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

+ Add a permission

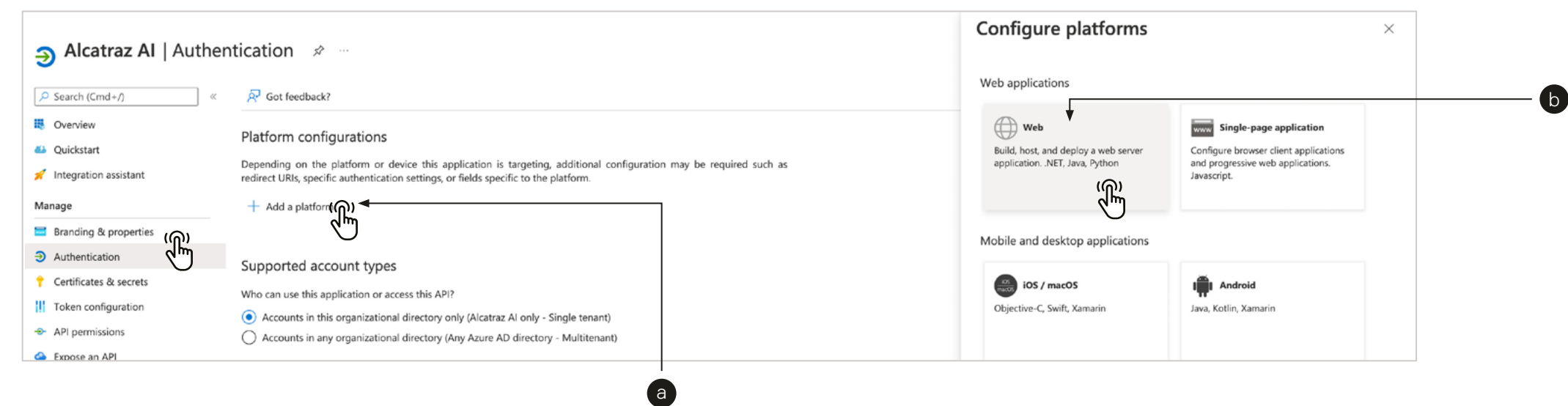
✓ Grant admin consent for Alcatraz AI

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (7)				
email	Delegated	View users' email address	No	✓ Granted for Alcatraz AI
Group.Read.All	Delegated	Read all groups	Yes	✓ Granted for Alcatraz AI
GroupMember.Read.All	Delegated	Read group memberships	Yes	✓ Granted for Alcatraz AI

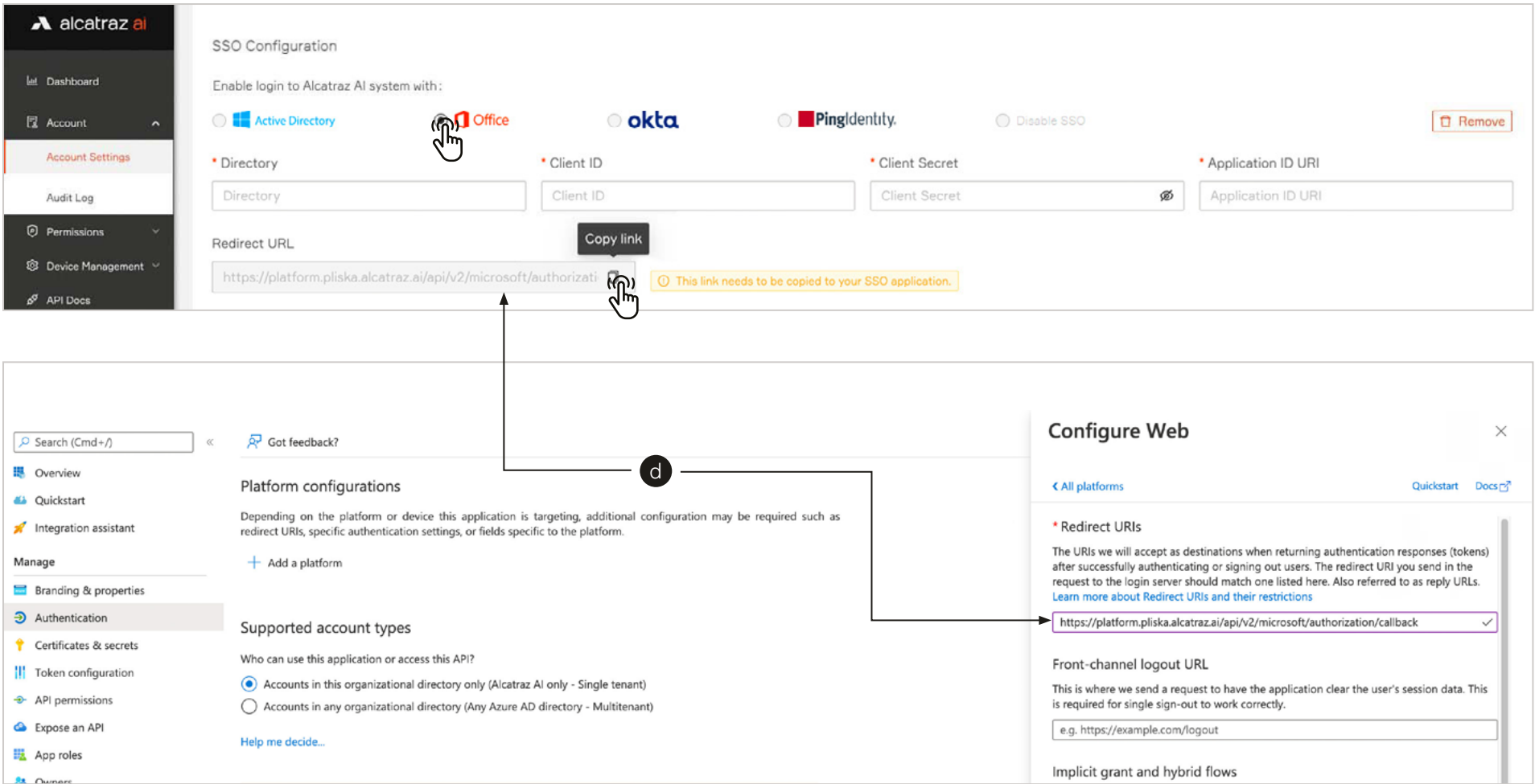
Ver. 1.3

15

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**.

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Alcatraz AI only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows ☐

Enable the following mobile and desktop flows:

Yes No

Save Discard

request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

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.

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 about tokens.](#)

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)

Configure Cancel

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**

The screenshot displays the Alcatraz AI SSO Configuration interface. The top panel, titled 'Alcatraz AI', shows the 'Essentials' tab with the following configuration details:

- Display name: [Alcatraz AI](#)
- Application (client) ID: XXXXXXXXXXXXXXXXXXXX
- Object ID: 14f37217-97bd-493f-bf3a-00023b269217
- Directory (tenant) ID: XXXXXXXXXXXXXXXXXXXX
- Supported account types: [My organization only](#)
- Client credentials: [0 certificate, 1 secret](#)
- Redirect URIs: [1 web, 0 spa, 0 public client](#)
- Application ID URI: XXXXXXXXXXXXXXXXXXXX
- Managed application in I...: [Alcatraz AI](#)

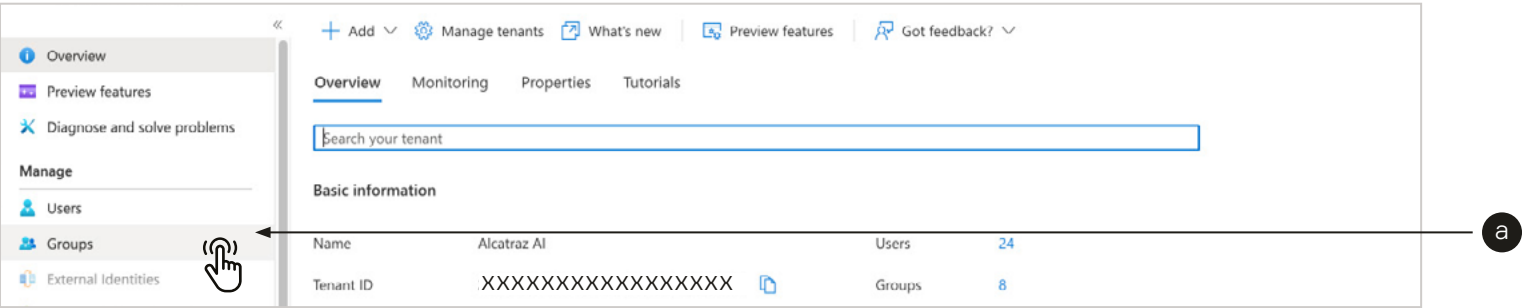
The bottom panel, titled 'SSO Configuration', shows the 'Enable login to Alcatraz AI system with:' section. The 'Office' option is selected. Below this, there are fields for 'Directory', 'Client ID', 'Client Secret', and 'Application ID URI'. The 'Redirect URL' field contains the link <https://platform.pliska.alcatraz.ai/api/v2/microsoft/authorize>, with a 'Copy link' button and a warning: 'This link needs to be copied to your SSO application.'

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

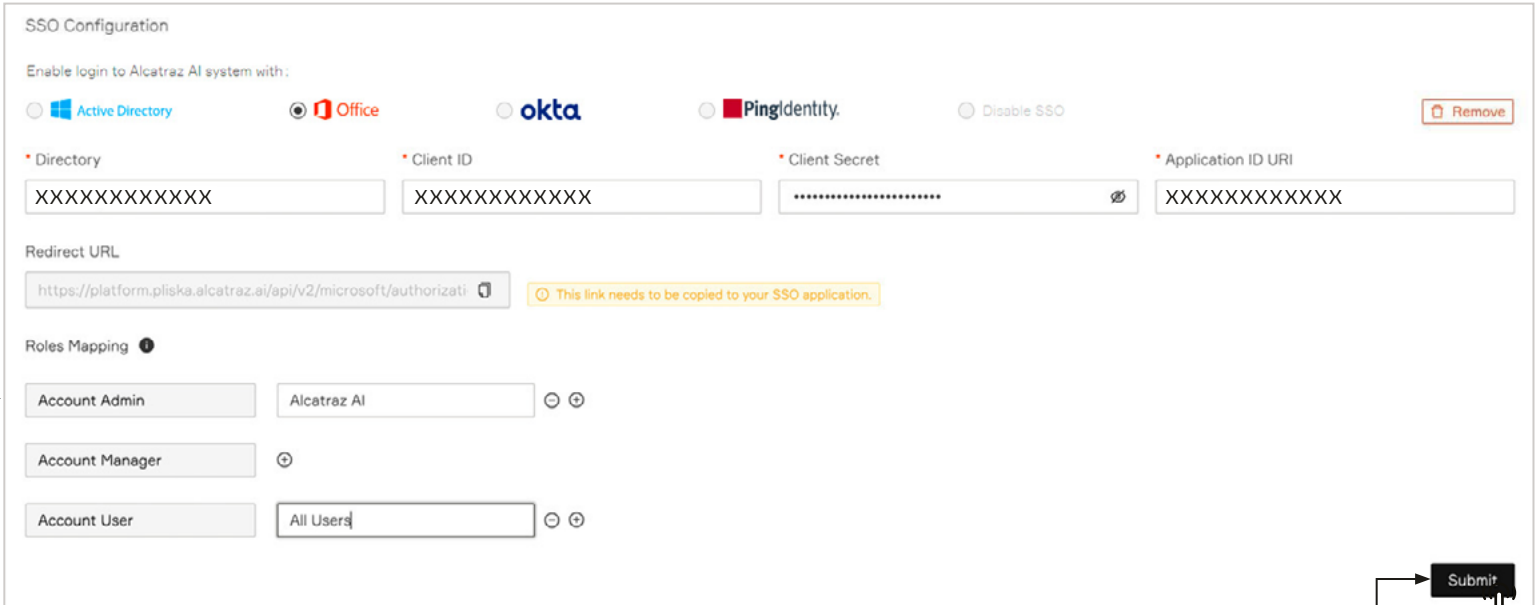
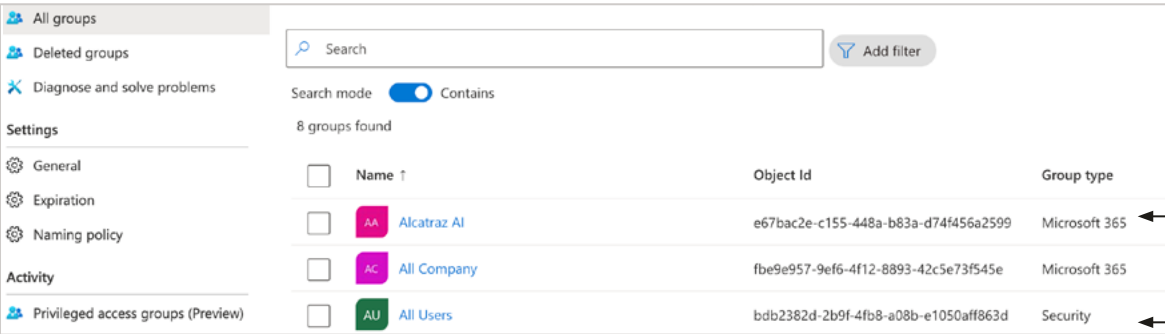


10. Map the Microsoft Azure groups to the **Alcatraz roles**.
Note: At least one group must be mapped to Alcatraz role.

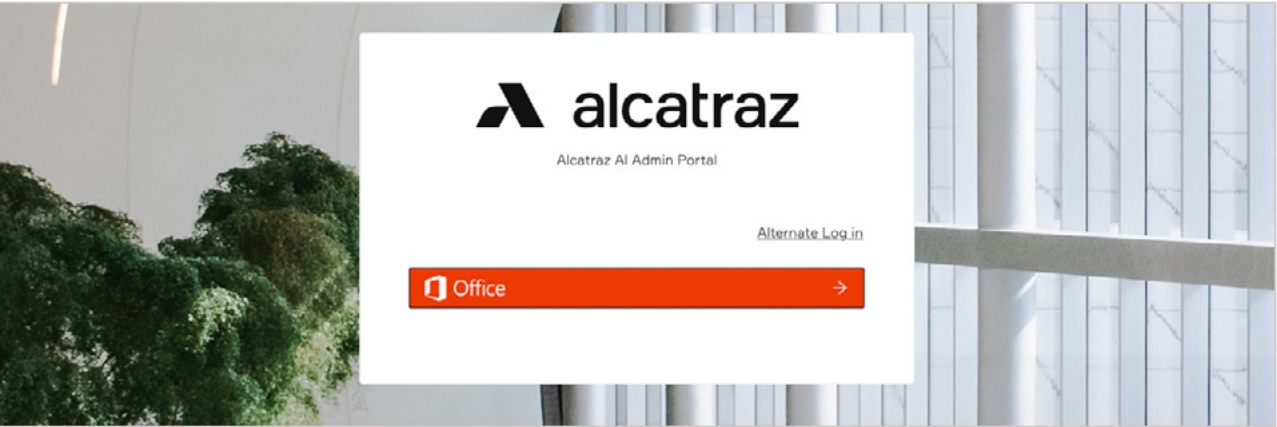
- a. Under **Manage** select **Groups**.
- b. Copy the names of the groups that will be mapped in Alcatraz AI system. Assign a selected group to



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



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



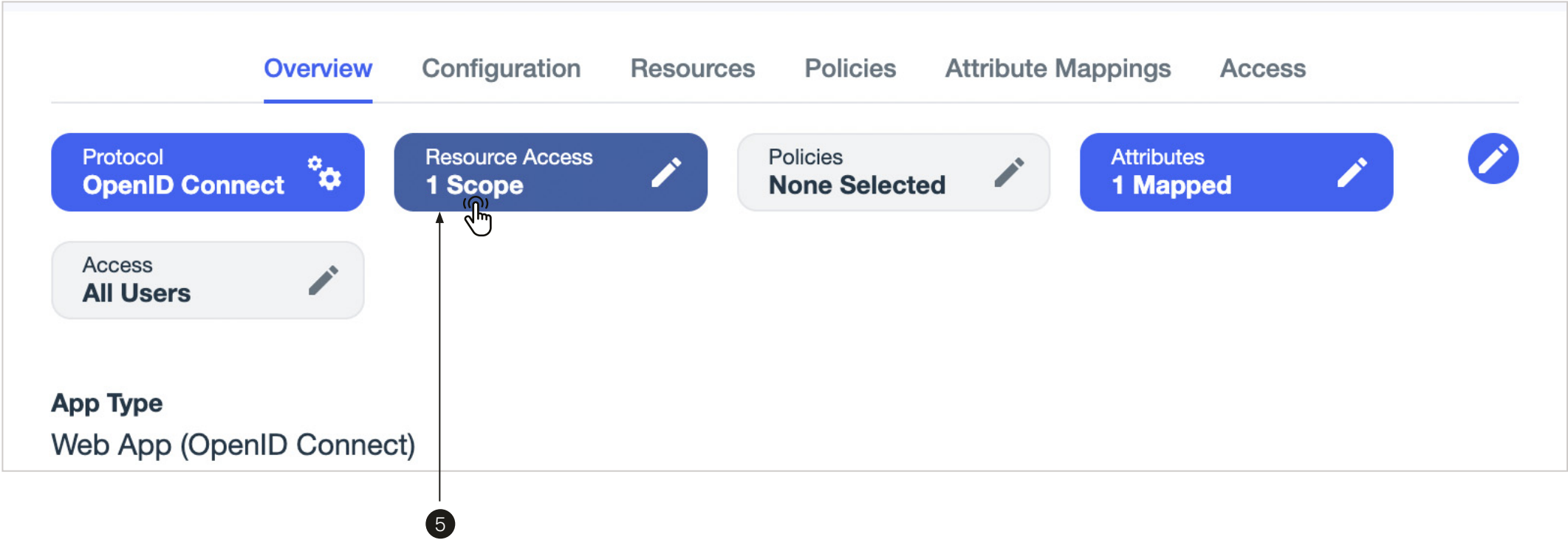
3—SSO with Ping Identity

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.

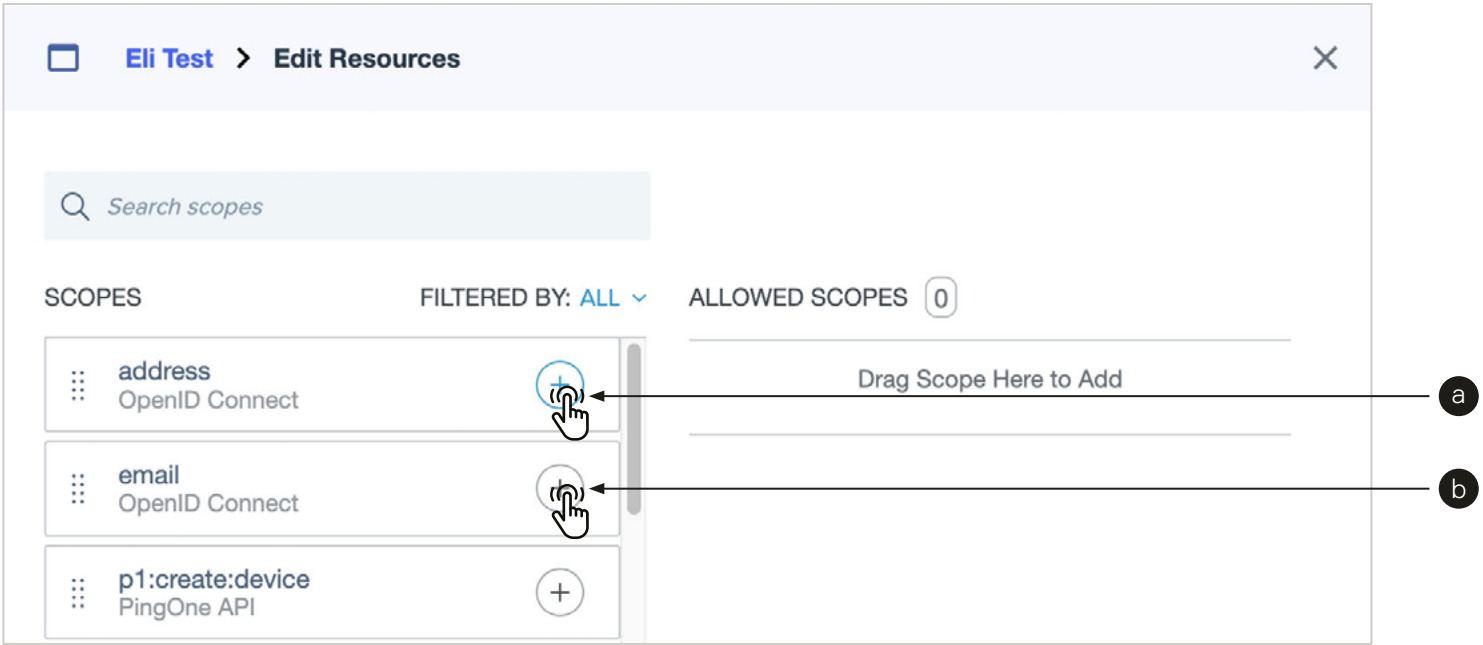


5. On the new application view panel select the **Resource Access** panel.



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**

SCOPES

FILTERED BY: ALL

ALLOWED SCOPES 2

p1:read:pairingKey

PingOne API

+

p1:read:sessions

PingOne API

+

p1:read:user

PingOne API

+

email

OpenID Connect

-

address

OpenID Connect

-

d. **profile**

p1:update:badmConsent

PingOne API

+

p1:update:user

PingOne API

+

p1:update:userMfaEnabled

PingOne API

+

p1:validate:userPassword

PingOne API

+

p1:verify:user

PingOne API

+

phone

OpenID Connect

+

profile

OpenID Connect

+

p1:read:user

PingOne API

-

address

OpenID Connect

-

email

OpenID Connect

-

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

p1:create:device

PingOne API

+

p1:create:pairingKey

PingOne API

+

p1:delete:device

PingOne API

+

p1:delete:pairingKey

PingOne API

+

profile

OpenID Connect

-

p1:read:user

PingOne API

-

address

OpenID Connect

-

email

OpenID Connect

-

Save

Cancel

Overview

Configuration

Resources

Policies

Attribute Mappings

Access

These resources define the connection between PingOne and the application, and contain scopes, which define application permissions. See [Resources](#).

ALLOWED SCOPES

RESOURCE	SCOPE
OpenID Connect	profile address email openid
PingOne API	p1:read:user



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

OverviewConfigurationResourcesPoliciesAttribute MappingsAccess

These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See [Mapping attributes](#).

⚠️ If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

Custom Attributes ▲

These attributes are currently mapped to the application. Customize them to meet your needs.

Attributes	PingOne Mappings	Scopes
sub	User ID ?	openid Required

8

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.

There are 22 global attributes currently mapped to this application. Add, edit, or delete attribute mappings here.

+ Add

AttributesPingOne Mappings

sub	User ID	<div><div>⚙️</div><div>🗑️</div></div>
email		<div><div>⚙️</div><div>🗑️</div></div>

This will override an inherited attribute.

Account ID

Creation Time

Email Address

Configurations

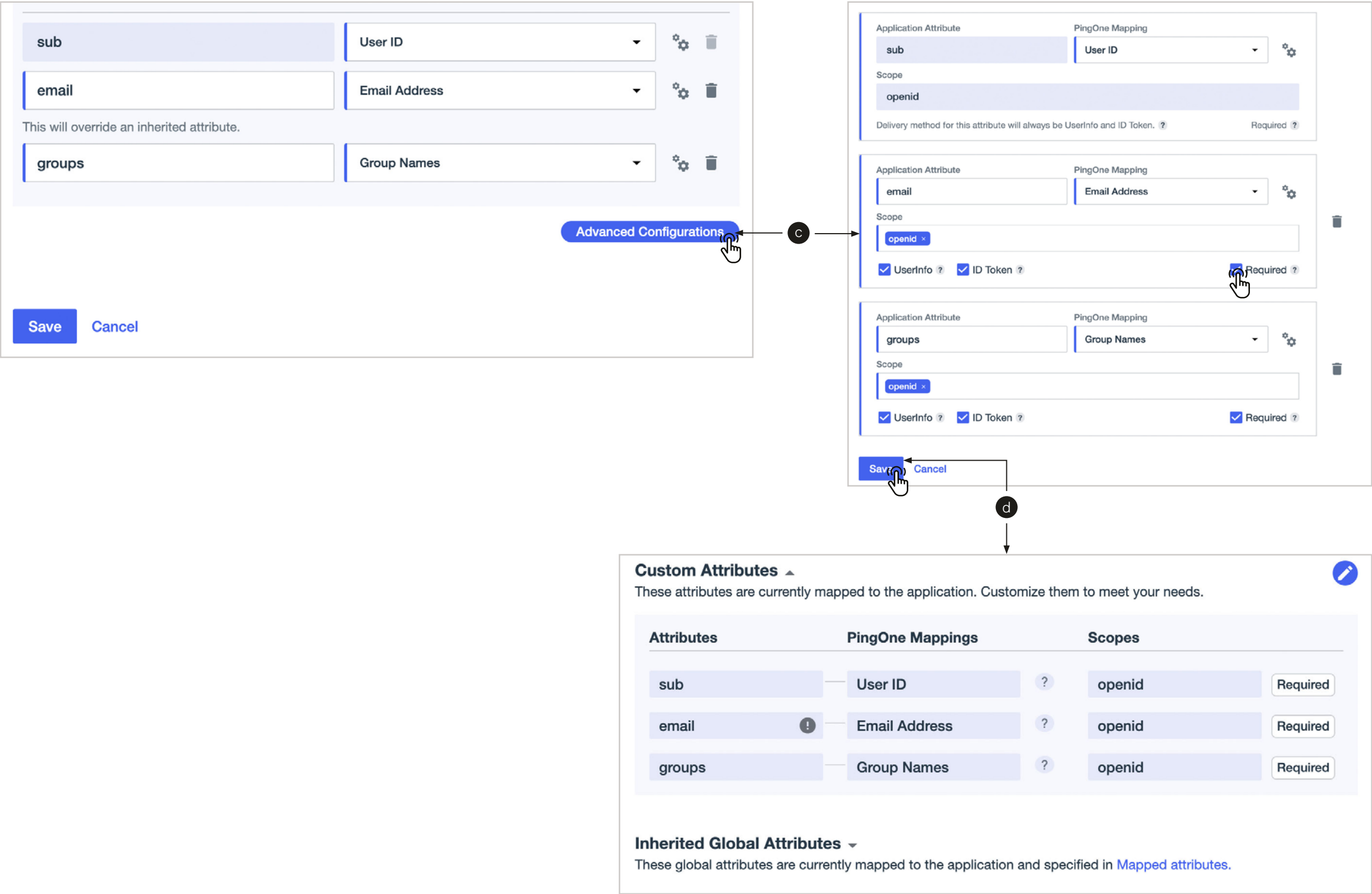
9

a

Ver. 1.3

23

- 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** and 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.

OverviewConfigurationResourcesPoliciesAttribute MappingsAccess

Configuration details for an OIDC application.

URLs

Authorization URL

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/authorize

Token Endpoint

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/token

JWKS Endpoint

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/jwks

Userinfo Endpoint

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/userinfo

Signoff Endpoint

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/signoff

OIDC Discovery Endpoint

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/.well-known/openid-configuration

Token Introspection Endpoint

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/introspect

Token Revocation Endpoint

https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as/revoke

Issuer

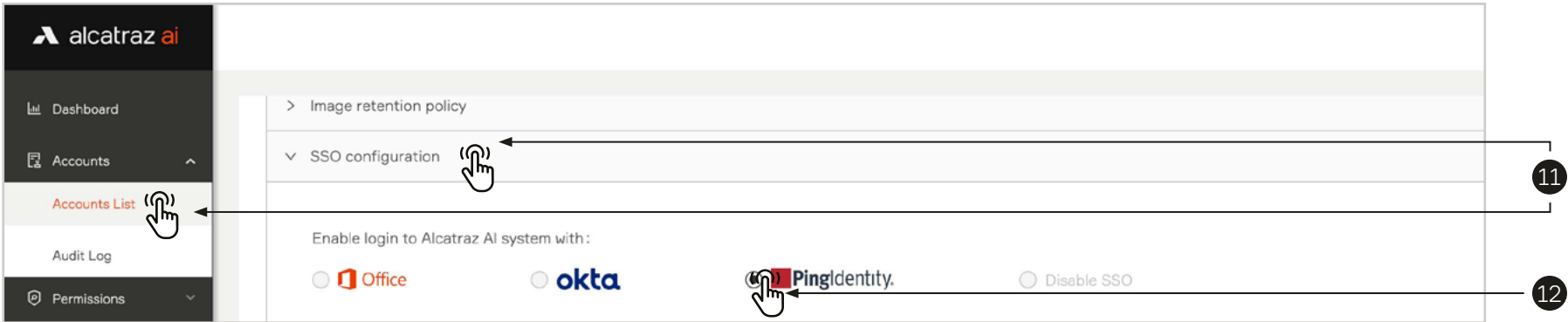
https://auth.pingone.eu/07eeb36e-3988-4437-95e0-b03b37bc0d42/as

General

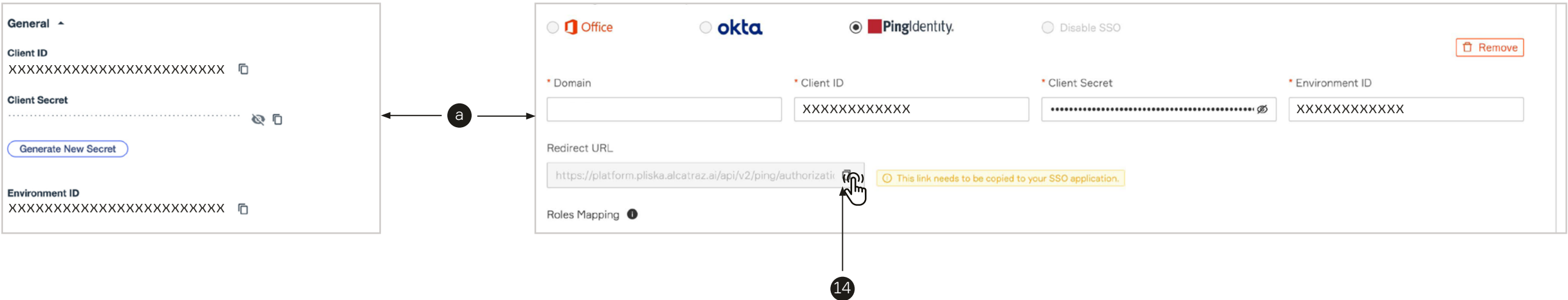
10



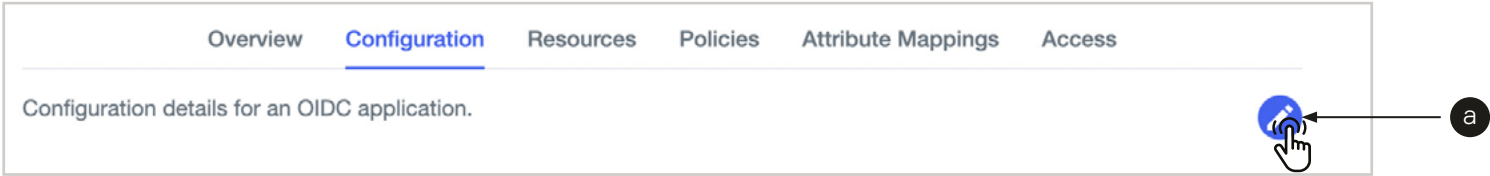
11. Open the Alcatraz Admin Portal, go to **Account** → **Account settings**, scroll down to the **SSO Configuration** section and click to open it.
12. Select **Ping Identity** of the displayed identity provider options.



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**.

Response Type

☒ Code

☐ Token

☐ ID Token

Grant Type

☒ Authorization Code

PKCE Enforcement

OPTIONAL

☐ Implicit

☒ Client Credentials

☒ Refresh Token

Refresh Duration

30

Days

Refresh Token Rolling Duration

180

Days

Redirect URIs

https://platform.pliska.alcatraz.ai/api/v2/ping/i

+ Add

Token Endpoint Authentication Method

☐ None

☒ Client Secret Basic

☐ Client Secret Post

Initiate Login URI

Save Cancel

b

c

d

e



16.Enable the application by turning on the toggle.

Alcatraz AI

Client ID: d3228168-9c27-47d0-b11d-893ce34d10c3

Overview

Configuration

Resources

Policies

Attribute Mappings

Access

Protocol

OpenID Connect

Resource Access

5 Scopes

Policies

None Selected

Attributes

3 Mapped

Access

All Users

App Type

Web App (OpenID Connect)

Description

Not Set

Client ID

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Home Page URL

No Home Page Configured

Signon URL

Default Signon Page

16



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.

The image shows two side-by-side screenshots from a web application. The left screenshot is the 'Groups' page in Ping Identity, showing a list of groups: Administrators, Users, Moderators, Manager, and Everyone. Arrows point from the 'Administrators' and 'Everyone' groups to the right screenshot. The right screenshot is the 'Roles Mapping' page in the Alcatraz AI system. It shows a form for mapping roles to groups. The 'Roles Mapping' section has three rows: 'Account Admin' mapped to 'Administrators' and 'Moderators', 'Account Manager' mapped to 'Manager', and 'Account User' mapped to 'Users' and 'Everyone'. A 'Submit' button is at the bottom right, with a circled 'c' and an arrow pointing to it. A circled 'b' is also present on the left screenshot, pointing to the group names.

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.

