

Alcatraz Al Admin Portal SSO Configuration

Table of Contents

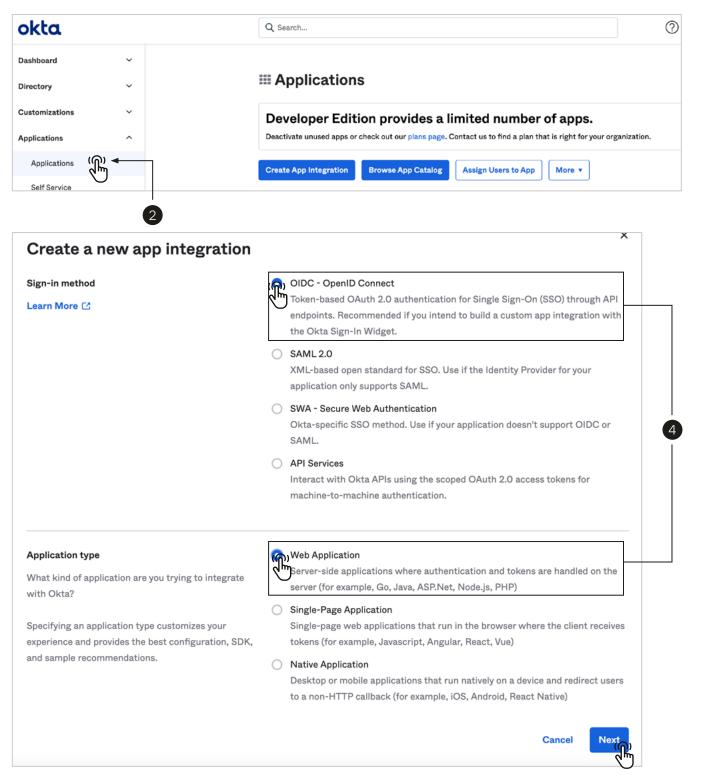
| 1— | SSO with | Okta. | | | | | • | • | • | • | • | • | • | • | • | • | • • | • | • | • | • | | | | • | |
|----|-----------|---------|--------|---|--|--|---|---|-------|---|---|-------|---|---|-------|---|-----|---|---|---|---|---|-------|---|---|--|
| 2— | -SSO with | Azure | | | | | • | • | • | | | • | | • | | | | | | • | • | • | • | • | • | |
| 3— | SSO with | Ping lo | dentit | у | | | • | | | | | | | • | | | | • | | | | • | | • | | |

| • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | .3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|
| | | • | • | • | • | • | | • | • | • | • | • | • | • | | .9 |
| | | | | | | | | | | | | | | | | 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 | | Q Search | 0 88 |
|----------------|---|---|------|
| Dashboard | Ý | | |
| Directory | ~ | 👯 New Web App Integration | |
| Customizations | ~ | General Settings | |
| Applications | ~ | App integration name Alcatraz Al | |
| Security | ~ | Logo (Optional) | ۵ (|
| Workflow | ~ | | Ô |
| Reports | ~ | | |
| Settings | ~ | Grant type Client acting on behalf of itself Learn More C2 Client Credentials | |
| | | Client acting on behalf of a user Authorization Code Refresh Token Implicit (hybrid) | 4 |

b. Alcatraz Al 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 Al **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.

| 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 × + Add URI | | A alcatraz ai | SSO Configuration Enable login to Alcatraz AI system w | with : | (finekta | PingIdentity. | Disable SSO | |
|---|---|----------------------|------------------|---|-----------------------------|---|-------------------------------------|---------------|---|
| 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 C | https://platform.sso-dev.alcatraz.ai | D | Account Settings | Domain Domain Redirect URL https://platform.sso-dev.alcatraz.c Roles Mapping | ai/api/v2/okta/authorizatio | Client ID Copy link on/callback One This line | nk needs to be copied to your SSO a | Client Secret | ø |
| 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 🖸 | × | | | Account Admin Account Manager Account User | | | | | |
| 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 | C d | | | | | | | |

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.

| Dashboard | ~ | ← Back to Applications |
|----------------|---|---|
| Directory | ~ | Alcatraz Al |
| Customizations | ~ | Active T & View Logs |
| Applications | ^ | General Sign On Assignments |
| Applications | | |
| Security | ~ | Client Credentials Edit |
| Workflow | ~ | |
| Reports | ~ | Client ID Ooa5d7ek2gaMyj1v35d7 |
| Settings | ~ | Public identifier for the client that is required for all OAuth flows. |
| | | Client authentication Client secret Public key / Private key |
| | | CLIENT SECRETS |
| | | Generate new secret |
| | | Creation date Secret Status |
| | | Jun 13, 2022 •••••• 💿 😰 🗛 |
| | | General Settings |
| | | Okta domain dev-22335288.okta.com |

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).

λ

Note: all of the URIs of the LOGIN section need to be filled properly to enable the SSO integration. g.Click **Save**.

| LOGIN | |
|------------------------|--|
| Sign-in redirect URIs | Allow wildcard * in login URI redirect. |
| | http://platform.sso-dev.alcatraz.ai/api/v2/authori |
| | + Add URI |
| Sign-out redirect URIs | http://platform.sso-dev.alcatraz.ai/ |
| | + Add URI |
| Login initiated by | App Only * |
| Initiate login URI | http://platform.sso-dev.alcatraz.ai/api/v2/login |
| | Save Cancel |
| | |
| | 9 |

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 Al Admin Portal.

a. Click **Create Token**. A pop-up will be displayed.

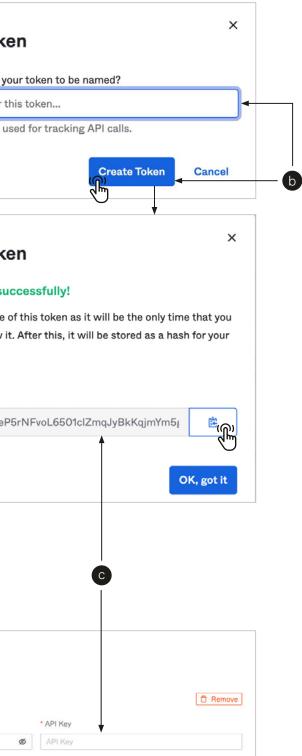
b. Add token name and click **Create Token** to continue. A successful message with the token value will be displayed.

| okta | Q Search | | guide@alcatraz.ai okta-dev-22335288 | |
|--------------------------|----------------------|---------------------------|---|-------------------------------------|
| Dashboard ~ | | | | Create To |
| Directory ~ | API | | Hei | P What do you wan |
| Customizations ~ | Authorization Server | rs Tokens Trusted Origins | | Enter a name fo |
| Applications 🗸 | A Create Token | | | a The token name is |
| Security ^ | | - | | |
| General | Token value | Find Token | Search by Last used: Most recent V | |
| HealthInsight | Token Types | O Token Name C | eated Expires Last Used Revoke | |
| Authentication | All | 0 | | |
| Multifactor | Health Check | | 01101110 | Create To |
| Identity Providers | Suspicious tokens | 0 | | |
| Delegated Authentication | | | 01101110 01100111 | Token created |
| Networks | | | thing to show dn't find any tokens | Please make a no |
| Behavior Detection | | | | will be able to view protection. |
| | | | | |
| | | | | Token Value |
| | | | | 00c-zNsdwX6F |
| | | | | |

c. Copy the token value and add it to the API key field (in the Alcatraz Al 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.

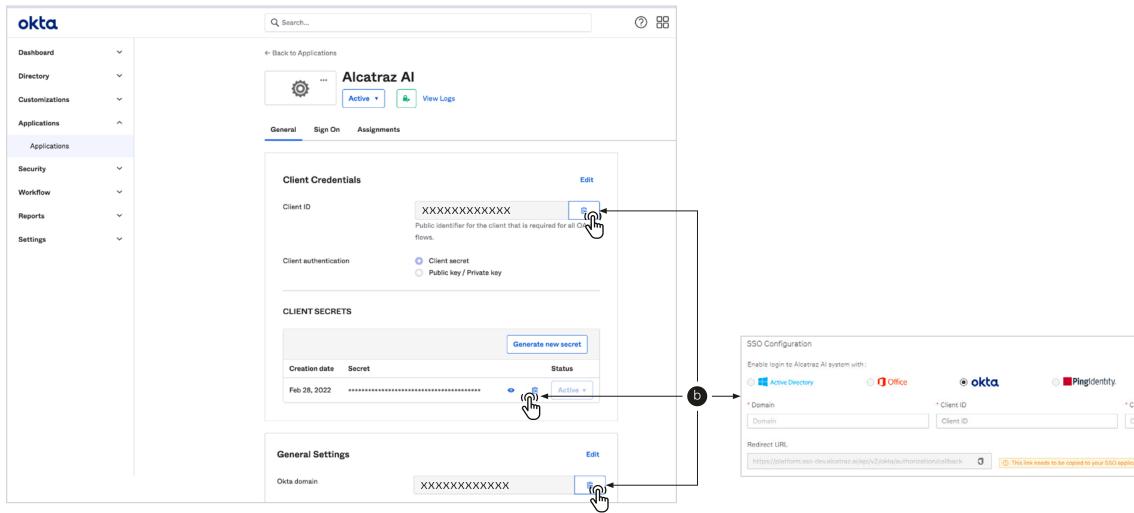
| \Lambda alcatraz ai | | | | | |
|---------------------|----------------------------------|----------|-----------|---------------|-----------------|
| | SSO Configuration | | | | |
| 네 Dashboard | Enable login to Alcatraz Al syst | em with: | | | |
| 🖾 Account 🔷 | Active Directory | Office | okta | Pingldentity. | Disable SSO |
| Account Settings | * Domain | | Client ID | | * Client Secret |
| Audit Log | Domain | | Client ID | | Client Secret |
| | | | | | |



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.

| okta | | Q Search | 0 8 |
|------------------|---|--|-----|
| Dashboard | ~ | | |
| Directory | ~ | Applications | |
| Customizations | ~ | Create App Integration Browse App Catalog Assign Users to App More V | |
| Applications | ^ | | |
| Applications (႐) | | Q Search | |
| Security | × | STATUS | |

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.



| XXXXXXXXX |
|-----------|
| 2 |

8. Map the Okta groups to the **Alcatraz roles**.

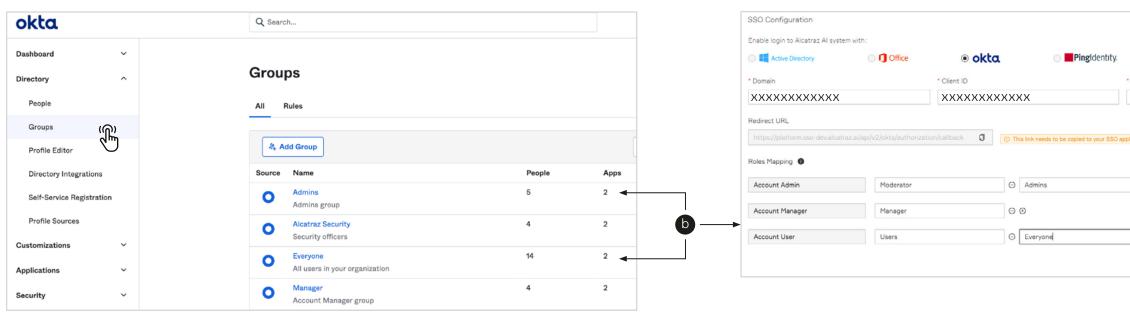
Note: At least one Okta group must be mapped to Alcatraz role.

a. In Okta Admin Console, go to **Directory --> Groups.**

b. Copy the names of the groups that will be mapped in Alcatraz Al system. Assign a selected

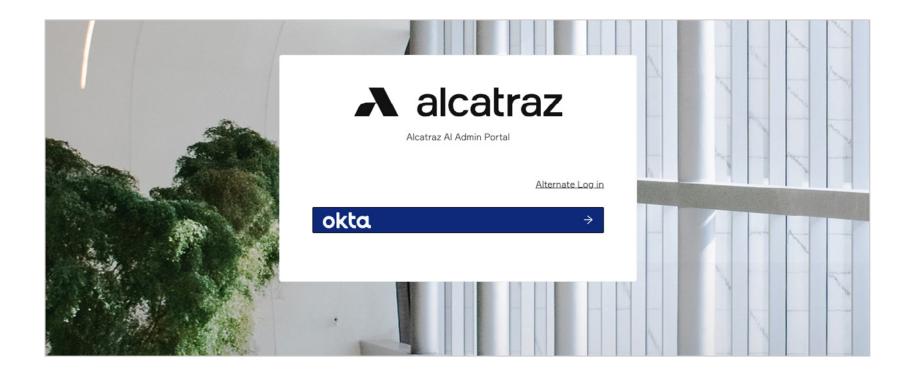
group to preferred user role. The mapping allows more than one group to be assigned to a role.

c. Click **Submit** when ready.



λ

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



| Disable SSO | | | 🕆 Remove |
|---------------|---|---------------------------|----------|
| Client Secret | ø | * API Key XXXXXXXXXXXXXXX | |
| ication. | | | |
| 00 | | | |
| 0 0 | | | |
| | | | Submit |
| | | | С |

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:

- -<u>Application Administrator</u>
- -Application Developer
- -<u>Cloud Application Administrator</u>

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

+ create a resource D 🗗 🗘 🕸 🛈 🖄 ♀ Search resources, services, and docs (G+/) 合 Home Welcome to Azure! Z Dashboard Don't have a subscription? Check out the following options. = All services * FAVORITES All resources () Resource groups App Services Function App SQL databases S Azure Cosmos DB Start with an Azure free trial Manage Azure Active Directory Access student benefits Virtual machines Get \$200 free credit toward Azure products and services, Manage access, set smart policies, and enhance security Get free software, Azure credit, or access Azure Dev Tools with Azure Active Directory. for Teaching after you verify your academic status. plus 12 months of popular free services. 4 Load balancers Start Learn more View Learn more d Learn more d Storage accounts Virtual networks ا الم Azure Active Directory Azure Active Directory Monitor . ۲ \rightarrow 🗛 Advisor Users Quickstart SQL databases Azure Cosmos More services View Virtual App Services Storage (1 Alcatraz Al | App registrations 🔗 Azure Active Directo + New registration the Endpoints <a>? Troubleshooting C Refresh <a>U Download <a>Device Preview features Got feedback? Overview Preview features 1 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer prov ✗ Diagnose and solve problems ations will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more Manage All applications **Owned applications** Deleted applications Users 🚨 Groups P Start typing a display name or application (client) ID to filter these r... External Identities Roles and administrators This account isn't listed as an owner of any applications in this directory. Administrative units View all applications in the directory Enterprise applications

2

 \mathbf{A}

Devices

App registrations

Identity Governance

F

| 3. Register an application screen will load. Configur | e the app a | 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 Al only - Single tenant) |
| O 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 V e.g. https://example.com/auth V |
| |
| |
| |
| 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 🔁 |
| (^Ω Register ◄ |
| |
| |

λ

С

- 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 Al SSO configuration.

| ,O Search (Cmd+/) « | 🔗 Got feedback? | | | | | |
|---|---|---|---|--|-------------------------------|---|
| Overview Quickstart Integration assistant | | | he authentication service when receiving tokens a cate (instead of a client secret) as a credential. | t a web addressable location (using an HTTPS | | |
| Manage | Application registration certificates, | secrets and federated credential: | can be found in the tabs below. | | × | |
| Branding & properties Authentication | Certificates (0) Client secrets (0) | Federated credentials (0) | | | | |
| r Certificates & secrets (۲) | A secret string that the application use | s to prove its identity when rec | uesting a token. Also can be referred to as application | ation password. | | |
| API permissions | + New client secret | | | | | |
| | Description | Expires | Value 🛈 | Secret ID | | |
| | a | | | | | |
| | | | | Add a client secret | | × |
| ertificates & secrets | \$ ··· | | | Description | Alcatraz Al SSO Configuration | |
| 🖗 Got feedback? | | | | Description | | |
| | | | | Evoiror | Recommended: 6 months | |
| | tions to identify themselves to the authent e, we recommend using a certificate (inste | | g tokens at a web addressable location (using a lential. | Expires | Recommended: 6 months | ~ |
| scheme). For a higher level of assurance | | ad of a client secret) as a cred | | | Recommended: 6 months | |
| scheme). For a higher level of assurance | e, we recommend using a certificate (inste | ad of a client secret) as a cred | | | Recommended: 6 months | ~ |
| Certificates (0) | e, we recommend using a certificate (inste | ad of a client secret) as a crec | lential. | | Recommended: 6 months | ~ |
| Certificates (0) | e, we recommend using a certificate (inste s, secrets and federated credentials can be fou D) Federated credentials (0) | ad of a client secret) as a crec | lential. | | Recommended: 6 months | ~ |
| Certificates (0) Client secrets (0 A secret string that the application use | e, we recommend using a certificate (inste s, secrets and federated credentials can be fou D) Federated credentials (0) | ad of a client secret) as a cred nd in the tabs below. token. Also can be referred to | lential. | | Recommended: 6 months | |
| Application registration certificates Application registration certificates Certificates (0) Client secrets (0 A secret string that the application use + New client secret | e, we recommend using a certificate (instead s, secrets and federated credentials can be fou D) Federated credentials (0) ses to prove its identity when requesting a Expires Value ① | ad of a client secret) as a cred nd in the tabs below. token. Also can be referred to | ential. | | Recommended: 6 months | |

| (| Certificates (0) Clien | t secrets (1) Fed | lerated credentials (0 |)) | |
|---|-----------------------------|-----------------------|--------------------------|--------------------------|---|
| , | A secret string that the ap | plication uses to pro | ove its identity when re | questing a token. Also c | can be referred to as application password. |
| | + New client secret | | | | |
| | Description | | Expires | Value 🕕 | Copy to clipboard et ID |
| | Alcatraz Al SSO Configu | uration | 12/13/2022 | yRk8Q~R3.NIdGWNs | sb-RDpKv3bMAiM 🖓 🛱 📋 |
| | | | | | ₹ F |

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**.

| ♀ Search (Cmd+/) « | 🔊 Got feedback? |
|-------------------------------------|---|
| Overview | Application ID URI ① Set |
| 🍊 Quickstart | |
| 🚀 Integration assistant | Scopes defined by this API |
| Manage | Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these. |
| Branding & properties | Are can request that a user or admin consent to one or more of these. Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application |
| Authentication | type. Go to App roles. |
| 📍 Certificates & secrets | + Add a scope |
| Token configuration | Scopes Im Who can consent Admin consent display User consent display na State |
| API permissions | No scopes have been defined |
| 🔺 Expose an API 🛛 🕧 | |
| 4 | |
| | a |

| Expose an API 🛷 … | Add a scope × |
|---|---|
| रुरे Got feedback? | You'll need to set an Application ID URI before you can add a permission. We've chosen one, but you can change it. |
| oplication ID URI ③ Set | Application ID URI * ① api://3131a895-ec71-47e9-bf3b-a7b6f523646a |
| copes defined by this API | |
| efine custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this PI can request that a user or admin consent to one or more of these. | |
| dding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to a pe. Go to App roles. | |
| + Add a scope | |
| Scopes Who can consent Admin consent display User consent display na State | |
| No scopes have been defined | |
| | |
| uthorized client applications | |
| uthorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls is API. | |
| + Add a client application | • |
| Client Id Scopes | Save and continue Cancel |
| | |

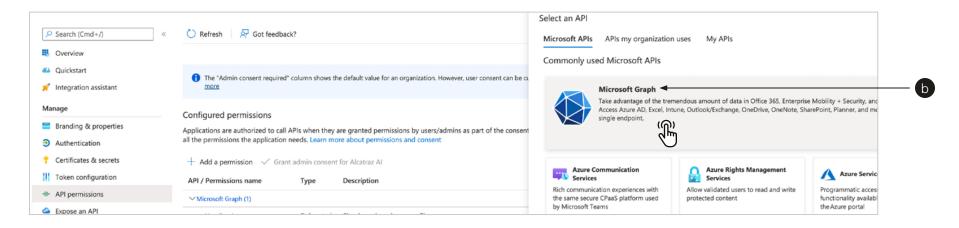
6. Set API Permissions

a. Under Manage, select API permissions and click Add a permission.

b. Select Microsoft Graph.

c. And click **Delegated permissions**.

| Overview | |
|--|---|
| QuickstartIntegration assistant | 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 the value in your organization, or in organizations where more |
| Manage Branding & properties Authentication | 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 |
| Certificates & secrets Token configuration | + Add a permission Grant admin consent for Alcatraz Al API / Permissions Type Description Admin consent requ Status |
| → API permissions ((()) | API / Permissions Type Description Admin consent requ Status VMicrosoft Graph (1) *** |
| Expose an API | User Read Delegated Sign in and read user profile No … |



| Search (Cmd+/) | 🕐 Refresh 🔰 🖗 Got feedback? | Microsoft Graph https://graph.microsoft.com/ Docs 27 |
|---|--|--|
| Overview | | What type of permissions does your application require? |
| Quickstart Integration assistant | The "Admin consent required" column shows the default value for an organization. However, user consent can be comore | Delegated permissions Your application needs to access the API as the signed-in user. Your application runs as a background se signed-in user. |
| Manage | Configured permissions | \bigcirc |
| Branding & properties | Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent | Select permissions |
| Authentication | all the permissions the application needs. Learn more about permissions and consent | Start typing a permission to filter these results |
| 📍 Certificates & secrets | + Add a permission 🗸 Grant admin consent for Alcatraz Al | The "Admin consent required" column shows the default value for an organization. However, user consent can be |
| Token configuration | API / Permissions name Type Description | The Admin Consent required column shows the default value for an organization, However, user consent can be permission, user, or app. This column may not reflect the value in your organization, or in organizations where the used. Learn more |
| API permissions | ✓ Microsoft Graph (1) | |
| Expose an API | the Red Red Red and an arrest | A state of the second stat |

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.**

| P€ | ermission | Admin consent required |
|----------|---|------------------------|
| \sim o | penId permissions (4) | |
| | email 🛈 View users' email address | No |
| | offline_access ① Maintain access to data you have given it access to | No |
| | openid 🛈 Sign users in | No |
| | profile ① View users' basic profile | No |

-Under GroupMember: GroupMember.Read.All

| \checkmark Gr | oup (1) | |
|-----------------|--|-----|
| | Group.Read.All ① Read all groups | Yes |
| | Group.ReadWrite.All ① Read and write all groups | Yes |
| \checkmark Gr | oupMember (1) | |
| | GroupMember.Read.All ① Read group memberships | Yes |

| ∨ Us | ser (1) | |
|------|---|-----|
| | User.Export.All ① Export user's data | Yes |
| | User.Invite.All ① Invite guest users to the organization | Yes |
| | User.Manageldentities.All ① Manage user identities | Yes |
| | User.Read (i) 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.

| Sverview | | | | | | |
|--------------------------------------|-------------------------------------|-------------------|--|-----------------------------------|---------------------------------|----------|
| Quickstart | The "Admin consent required | " column shows th | ne default value for an organization. However, user consent | can be customized per permission | user or ann This column may n | ot refle |
| 🚀 Integration assistant | app will be used. Learn more | | in default value for all organization. However, aser consent | can be customized per permission, | user, or upp. This column may h | Je rene |
| Manage | Configured permissions | | | | | |
| Branding & properties | U | APIs when they | are granted permissions by users/admins as part of the | consent process. The list of conf | figured permissions should inc | lude |
| Authentication | all the permissions the application | | | | 5 | |
| 📍 Certificates & secrets | + Add a permission | nt admin consent | for Alcatraz Al | | | |
| Token configuration | API / Permissions name | Туре | Description | Admin consent requ | Status | |
| - API permissions | Microsoft Graph (7) | | | | | |
| Expose an API | email | Delegated | View users' email address | No | 📀 Granted for Alcatraz Al | ••• |
| App roles | Group.Read.All | Delegated | Read all groups | Yes | 📀 Granted for Alcatraz Al | ••• |
| A Owners | GroupMember.Read.All | Delegated | Read group memberships | Yes | 📀 Granted for Alcatraz Al | ••• |
| & Roles and administrators Preview | offline_access | Delegated | Maintain access to data you have given it access to | No | 🤡 Granted for Alcatraz Al | ••• |
| 10 Manifest | openid | Delegated | Sign users in | No | 📀 Granted for Alcatraz Al | ••• |
| Support + Troubleshooting | profile | Delegated | View users' basic profile | No | 📀 Granted for Alcatraz Al | ••• |
| Troubleshooting | User.Read | Delegated | Sign in and read user profile | No | 📀 Granted for Alcatraz Al | ••• |
| | | | | | | |

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

| Grant admin consent co | onfirmation. | | | | |
|---|---------------------------|---|---|-----------------------------------|--|
| Do you want to grant consent | for the requested | d permissions for all accounts in Alcatraz A | I? This will update any existing admin | consent records this applica | tion already has to match what is listed below |
| No No | | | | | |
| Configured permissions | | | | | |
| | , | are granted permissions by users/admins as p ore about permissions and consent | art of the consent process. The list of con | figured permissions should in | clude |
| | | | | | |
| + Add a permission 🗸 Gra | ant admin consent | for Alcatraz Al | | | |
| + Add a permission \checkmark Gra API / Permissions name | ant admin consent Type | for Alcatraz Al Description | Admin consent requ | Status | |
| | | | Admin consent requ | Status | |
| API / Permissions name | | | Admin consent requ No | Status Granted for Alcatraz Al | ••• |
| API / Permissions name Microsoft Graph (7) | Туре | Description | · | | |

8. Configure the Redirect URI.

a. Go to Authentication and click Add a platform.

b. Click on **Web** option.

| ∋ Alcatraz AI Auther | ntication 💉 | | Configure platforms | | × | |
|--|---|---------------------------|---|--|---|---|
| Search (Cmd+/) « | R Got feedback? | | Web applications | | | b |
| Overview Quickstart Integration assistant Manage Branding & properties Authentication | Platform configurations Depending on the platform or device this application is targeting, additional configuration redirect URIs, specific authentication settings, or fields specific to the platform. + Add a platform | n may be required such as | Web Build, host, and deploy a web server applicationNET, Java, Python | Single-page application Configure browser client applications and progressive web applications. Javascript. | | |
| Certificates & secrets III Token configuration API permissions Expose an API | Supported account types Who can use this application or access this API? Accounts in this organizational directory only (Alcatraz Al only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) | | iOS / macOS Objective-C, Swift, Xamarin | Java, Kotlin, Xamarin | | |

- 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.

| Account Active Directory | |
|--|-------------------------------------|
| Account Settings | |
| Audit Log Directory Client ID Client Secret Ø Application ID URI | |
| Permissions Redirect URL Copy link | |
| Device Management Attps://platform.pliska.alcatraz.ai/api/v2/microsoft/authorizati O This link needs to be copied to your SSO application. | |
| API Docs | |
| Search (Cmd+/) Search (Cmd+/) Got feedback? Configure Web All platforms | X Quickstart Docs 2 ⁷ |
| 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. | |
| Manage + Add a platform The URIs we will accept as destinations when returning authentica after successfully authenticating or signing out users. The redirect | URI you send in the |
| E Branding & properties request to the login server should match one listed here. Also refe | |
| Authentication Supported account types https://platform.pliska.alcatraz.ai/api/v2/microsoft/authorization. | ′callback 🗸 |
| Certificates & secrets Who can use this application or access this API? Front-channel logout URL | |
| Construction Accounts in this organizational directory only (Alcatraz Al only - Single tenant) Accounts in this organizational directory only (Alcatraz Al only - Single tenant) Accounts in this organizational directory only (Alcatraz Al only - Single tenant) Accounts in this organizational directory only (Alcatraz Al only - Single tenant) | er's session data. This |
| API permissions Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) e.g. https://example.com/logout | |
| Help me decide | |

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

| Branding & properties | | request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions |
|---|---|---|
| Authentication | Supported account types | https://platform.pliska.alcatraz.ai/api/v2/microsoft/authorization/callback |
| ↑ Certificates & secrets 11 Token configuration ◆ API permissions ▲ Expose an API ▲ App roles | Who can use this application or access this API? Accounts in this organizational directory only (Alcatraz Al only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Help me decide | 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. e.g. https://example.com/logout |
| Owners Roles and administrators Manifest | 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. | 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. |
| Support + Troubleshooting | Advanced settings | Select the tokens you would like to be issued by the authorization endpoint: |
| Troubleshooting | Allow public client flows \odot | Access tokens (used for implicit flows) |
| New support request | Enable the following mobile and desktop flows: Yes No | ID tokens (used for implicit and hybrid flows) |
| | Save Discard | |
| | | - <i>A</i> μ |

- 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

| 💦 Alcatraz Al | \$ | | | | × |
|---|--|---------------------------------------|---|--|--------------------|
| Search (Cmd+/) | « 🚺 Delete 🌐 Endpoints 💀 Preview fe | atures | | | |
| 👯 Overview | | | | | |
| Quickstart Integration assistant | Display name : <u>Alcatraz Al</u> | | Client credentials Redirect URIs | : <u>0 certificate, 1 secret</u> : <u>1 web, 0 spa, 0 public client</u> | |
| Manage | · · · | d-493f-bf3a-00023b269217 | Application ID URI | : XXXXXXXXXXXXXXXXXXX | xxx |
| Branding & properties Authentication | Directory (tenant) ID : XXXXXX Supported account types : <u>My organizati</u> | XXXXXXXXXXX an only | Managed application in | I : <u>Alcatraz Al</u> | |
| | | a | | | |
| A alcatraz ai | SSO Configuration | | | | |
| 님 Dashboard | Enable login to Alcatraz Al system with: | | | | |
| 🖾 Account 🔷 🗠 | Active Directory | Office Okta | Pingldentity. | Disable SSO | C Remove |
| Account Settings | * Directory | Client ID | Client Secret | - A | pplication ID URI |
| Audit Log | Directory | Client ID | Client Secret | ø | Application ID URI |
| Permissions | Redirect URL | Copy link | | | |
| I Device Management ∨ API Docs | https://platform.pliska.alcatraz.ai/api/v2/ | microsoft/authorizati 0 O This link r | needs to be copied to your SSO application. | | |

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

| Manage Branding & properties Authentication | Certificates (0) Client secrets (1) A secret string that the application uses to | Federated credentials (prove its identity when r | , | be referred to as application password. |
|---|---|--|---------------------|--|
| 📍 Certificates & secrets | + New client secret | | | |
| Token configuration | Description | Expires | Value 🛈 | Copy to clipboard et ID |
| API permissions | Alcatraz AI SSO Configuration | 12/13/2022 | yRk8Q~R3.NIdGWNsb-R | ت 1c53e4-abf4-4d1f-afc3-1a26a1b853a5 🗅 🧃 |
| Expose an API | | | | |

10. Map the Microsoft Azure groups to the **Alcatraz roles.**

Note: At least one group must be mapped to Alcatraz role.

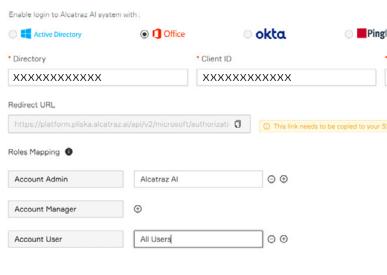
a. Under Manage select Groups.

b. Copy the names of the groups that will be mapped in Alcatraz Al 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.

| All groups | | | |
|------------------------------------|----------------------|--------------------------------------|---------------|
| Deleted groups | 𝒫 Search | Y Add filter | |
| X Diagnose and solve problems | Search mode Contains | | |
| Settings | 8 groups found | | |
| 袋 General | Name î | Object Id | Group type |
| Expiration Naming policy | AA Alcatraz Al | e67bac2e-c155-448a-b83a-d74f456a2599 | Microsoft 365 |
| Activity | All Company | fbe9e957-9ef6-4f12-8893-42c5e73f545e | Microsoft 365 |
| Privileged access groups (Preview) | AU All Users | bdb2382d-2b9f-4fb8-a08b-e1050aff863d | Security |



SSO Configuration

λ

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



| Identity. | | emove |
|-----------------|-------------------|-------------|
| | | emove |
| Client Secret | cation ID URI | |
| SO application. | | |
| | | |
| | Su | ubmit Im |

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.

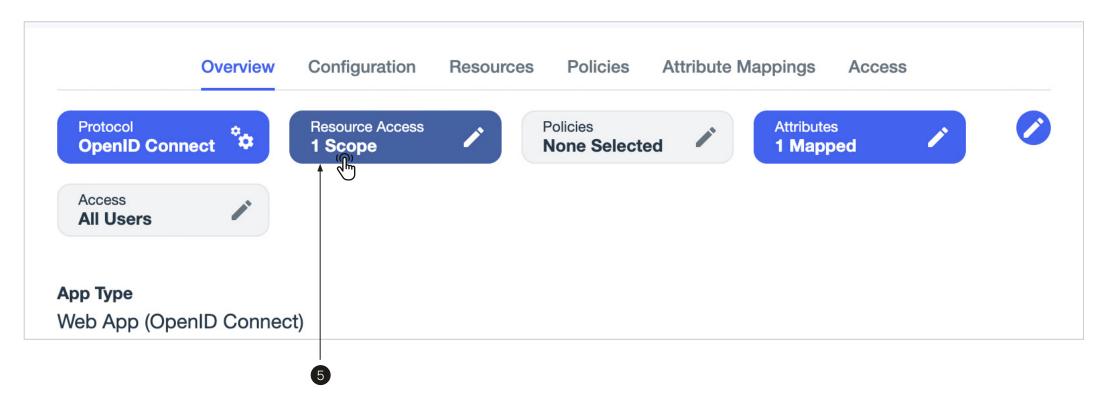
| Pi | ngldentity. | | | ? • S Explore • Toshko |
|-----------------------------|--------------------|---|---------------------|--|
| Enviror Admin Product | istrators 🗸 🗸 | Applications 🚓 | | |
| ⊕ | | Q. Search 7 Applications by Application Name - | Filter | |
| * | Applications | Demo Login Client ID:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | Avg daily sign-ons: | Past 7 days No data yet % |
| ព | Application Portal | Ping Integration Client ID:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | Avg daily sign-ons: | 1 _/ % Past 7 days 12 wk trend % |
| ٢ | IDENTITY PROVIDERS | PingOne Admin Console Client ID:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | Avg daily sign-ons: | 3 ~ % Past 7 days 12 wk trend |
| Ô | External IDPs | | | |
| | 2 | | 3 | |

- 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.

| Add Application | | × |
|--|--|--|
| Name and Describe Application Create a name and description for this application that w | vill make it easy to identify. | |
| Application Name * | | |
| Description | | |
| lcon | | |
| Max Size 1.0 MB | | |
| Choose Application Type | • | |
| • | | <u></u> 0 |
| SAML Application | OIDC Web App | Native |
| Applications that are accessed within a browser using the SAML protocol. | Web applications that are accessed within a browser using the OpenID Connect protocol. | Applications that run from a mobile device or a desktop computer, including a PingOne MFA authenticator. |
| | <> | S |
| Save Cancel | | |

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



λ

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

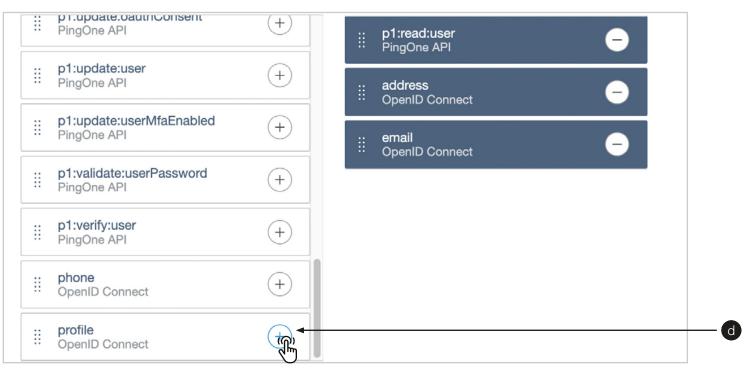
b. email

| | Eli Test > Edit Reso | urces | | × |
|------|---------------------------------|--------------------|------------------------|---|
| Q | Search scopes | | | |
| SCOF | | FILTERED BY: ALL V | ALLOWED SCOPES | |
| | address OpenID Connect | | Drag Scope Here to Add | |
| | email OpenID Connect | | | |
| :: | p1:create:device PingOne API | + | | |

c. p1:read:user

| SCOPES | FILTERED BY: ALL 🗸 | ALLC | OWED SCOPES 2 | | |
|---|--------------------|------|--------------------------------|---|-----|
| :: p1:read:pairingKey :: PingOne API | + | # | email OpenID Connect | - | |
| p1:read:sessions PingOne API | + | : | address OpenID Connect | • | |
| :: p1:read:user :: PingOne API | | | | | — C |

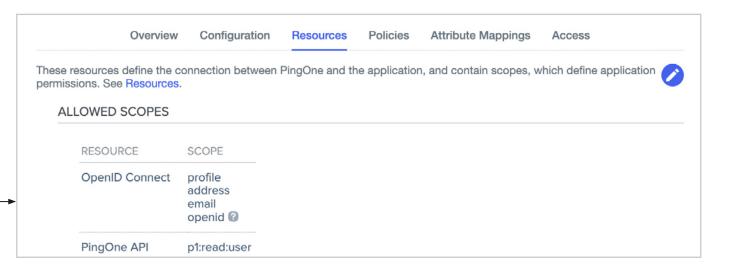
d.**profile**



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

| p1:create:device PingOne API | + | :: profile :: OpenID Connect | e |
|---|---|--|---|
| p1:create:pairingKey PingOne API | + | :: p1:read:user :: PingOne API | - |
| p1:delete:device PingOne API | + | :: address :: OpenID Connect | e |
| p1:delete:pairingKey PingOne API | + | :: email :: OpenID Connect | - |

(7)



| Overview | Configuration Res | sources Policies | Attribute Mappings | Access |
|-------------------------|--|----------------------|---------------------------------|------------------------|
| se mappings associate P | PingOne user attributes to S | SAML or OIDC attribu | tes in the application. Se | ee Mapping attributes. |
| | n is accessible by users Provider ID attribute so | | | |
| | | | | |
| istom Attributes 🔺 | ntly mapped to the applic | cation. Customize th | em to meet your needs | s. 💦 |
| | | | em to meet your needs Scopes | s. 🥳 |

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 a | application. Add, edit, or delete attribute mappings here. | + Add |
|---|--|--------------|
| Attributes | PingOne Mappings | |
| sub | User ID 🗸 | ت م |
| email | | °o 🗐 |
| This will override an inherited attribute. | Account ID | a |
| | Creation Time | n'igurations |
| | Email Address | |

- 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.

| | | | | | - | | | |
|--|---------------|---------------|----------|---|--------------------------------------|--|------------|---|
| sub | User ID | ° ↓ | I | | Application Attribute sub | PingOne Mapping User ID | • °¢ | |
| email | Email Address | • °¢ | 1 | | Scope openid | | | |
| This will override an inherited attribute. | | | | | Delivery method for this attribute w | ill always be UserInfo and ID Token. ? | Required ? | |
| groups | Group Names | • °0 | Î | | Application Attribute | PingOne Mapping | | |
| | • | | | | email | Email Address | • °o | |
| | | | | | Scope | | | î |
| | Advan | ced Configura | | C | openid × | | | - |
| | | | 4™ | | UserInfo ? VID Token | 2 | Required ? | |
| Save Cancel | | | | | Application Attribute | PingOne Mapping | | |
| | | | | | groups | Group Names | • °o | |
| | | | | | Scope | | | Î |
| | | | | | openid × | | | |
| | | | | | ✓ UserInfo ? ✓ ID Token | 2 | Required ? | |
| | | | | | Sav() Cancel | | | |
| | | | | L | d | | | |
| | | | | | ↓ | | | |
| | | | | | | | | |

Custom Attributes 🔺

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

| Attributes | PingOne Mappings | | Scopes | |
|------------|------------------|---|--------|--|
| sub | User ID | ? | openid | |
| email | Email Address | ? | openid | |
| groups | Group Names | ? | openid | |

Inherited Global Attributes -

λ

These global attributes are currently mapped to the application and specified in Mapped attributes.

| Requ | ired | |
|------|------|--|
| Requ | ired | |
| Requ | ired | |

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.

| Overview Configuration Resources Policies Attribute Mappings Access | |
|--|----|
| Configuration details for an OIDC application. | |
| URLs A | |
| 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 | 10 |
| 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 Image: Comparison of Compari | |
| 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 (| |

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.

| A alcatraz ai | | |
|---------------|--|-----|
| 네 Dashboard | > Image retention policy | |
| Accounts | ✓ SSO configuration | 1 |
| Audit Log | Enable login to Alcatraz Al system with: | |
| Permissions Y | Office Okta Office Disable SSO | -12 |

13. Return to the **Ping Admin** console, **Configuration** tab, **General** section.

a. Copy the following credentials and place them to the Alcatraz Al 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.

| General A | Office Okta | Pingldentity. | O Disable SSO | |
|--|--|-------------------------------------|----------------------|----------------|
| Client ID XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | * Domain | * Client ID | * Client Secret | Environment ID |
| Client Secret | | XXXXXXXXXXX | Ø | XXXXXXXXXXX |
| Generate New Secret | Redirect URL | | | |
| Environment ID XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | https://platform.pliska.alcatraz.ai/api/v2/ping/au | O This link needs to be copied to y | our SSO application. | |
| 15.Return to the Configuration tab in Ping. a.Click the edit button. Edit Configuration section will be displayed. | | 4 | | |
| Overview Configuration Resources Policies Attribute | e Mappings Access | _ | | |
| Configuration details for an OIDC application. | - | , a | | |

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 | |
| Code | b |
| Token | |
| ID Token | |
| | |
| Grant Type | |
| Authorization Code | |
| PKCE Enforcement | |
| OPTIONAL - | |
| Implicit | |
| Client Credentials | |
| Refresh Token | |
| Refresh Duration | |
| 30 🗘 Days 🗸 | C |
| Refresh Token Rolling Duration | |
| 180 _ Days - | |
| | |
| Redirect URIs | |
| https://platform.pliska.alcatraz.ai/api/v2/ping/; | |
| + Add | d |
| | |
| Token Endpoint Authentication Method | |
| None O Client Secret Basic O Client Secret Post | |
| | |
| Initiate Login URI | e |
| | • |

 \mathbf{A}

| | ew Configuration | Resources | Policies A | ttribute Ma | appings Acce | SS | |
|--------------|-----------------------------|-----------|---------------------------|-------------|------------------------|----|--|
| D Connect | Resource Access 5 Scopes | | Policies None Selected | | Attributes 3 Mapped | 1 | |
| rs 🖊 | | | | | | | |
| • | | | | | | | |
| p (OpenID Co | nnect) | | | | | | |
| ion | | | | | | | |
| | | | | | | | |
| **** | | ē | | | | | |
| | | .0 | | | | | |
| | | | | | | | |

17. Map Ping Identity Groups to Alcatraz roles.

a. Go to **Identities** -> Groups.

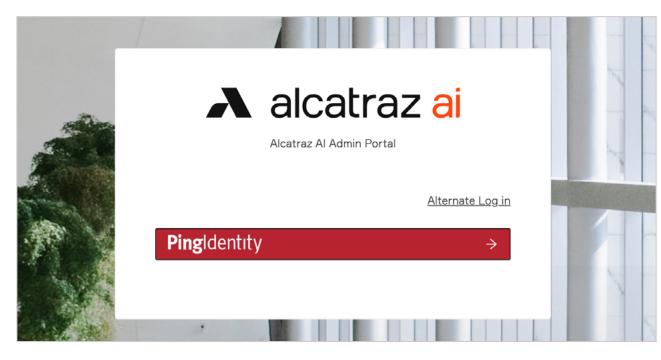
b. Copy the names of the groups that will be mapped in Alcatraz Al system. Assign a selected group to preferred user role.

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.

| Environ Admini Product | strators ~ | Groups 🛨 Administrators can manage their groups including creating groups, updating group membership manually or c | | | | | | |
|------------------------------|---------------------------|---|--|----------------|---|-----------------------|------------------|----------|
| ⊕ | < Identities Users | Q Search Groups Name | Office Okta | ۲ | PingIdentity. | O Disable SSO | | D Remove |
| * | Groups | Administrators Administrators Population | * Domain auth.pingone.eu | * Client ID | | * Client Secret | * Environment ID | |
| H © | Populations Attributes | Users | Redirect URL https://platform.pliska.alcatraz.ai/api/v2/pi | | This link needs to be copied to | | | |
| 0 (| Roles | Moderators | Roles Mapping | graderenzaer g | U This link needs to be copied to | your SSO application. | | |
| S | | Manager Administrators Population | Account Admin Administ | itors | Moderators | $\odot \oplus$ | | |
| | | Everyone Administrators Population | Account Manager Manager | | ⊙ ⊕Everyone | \odot \oplus | | |
| | | | | | | | | Submit |
| 18.Lo | og out and a new | login screen will be available, allowing to use Ping Identity as identity provi | ler to log to the Alcatraz Al platfo | rm. | | | | |





© 2022 Alcatraz Al Inc. All Rights Reserved