# SSO Okta - How to configure?

SSO - Configuring Okta for Single Sign-On

Gathid user authentication has been designed to work with your existing identity authentication processes wherever possible.

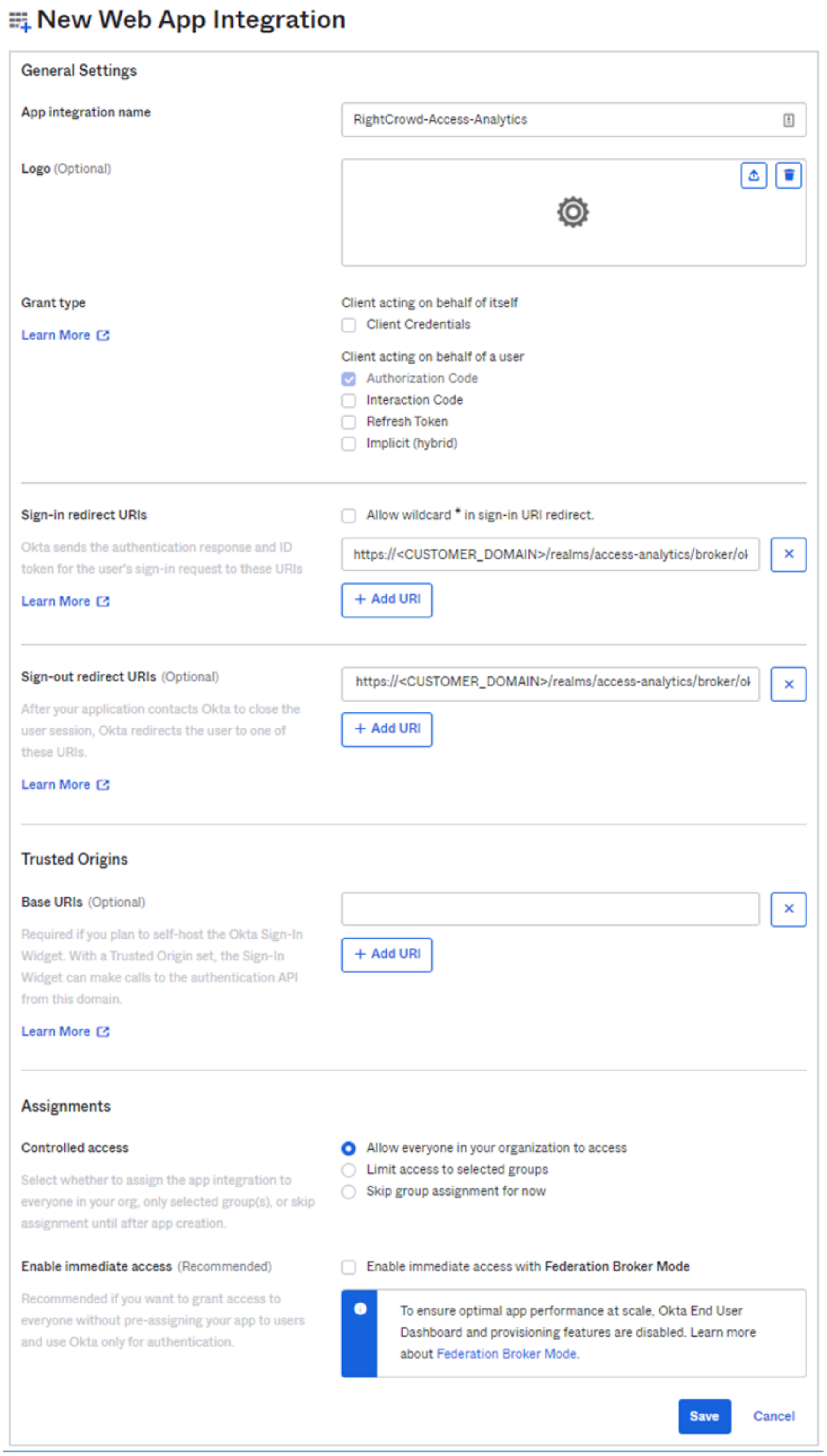
The following guide has been developed to assist you with configuring your Gathid instance within your existing Okta identity store.

Throughout the process, you will:

1. Configure an Okta Application for Gathid Single Sign-On
2. Provide the required information to your Gathid representative

**Register an Okta Application for Gathid Single Sign-On**

1. Browse to Okta Portal and log in to your organization.
2. Select **Create a new app integration**
3. Select **Sign-in method** → **OIDC - OpenID Connect**
4. Select **Application type** → **Web Application**
5. In **General Application Settings**, configure
6. **App integration name**, for example: e.g. “Gathid”
7. **Grant type** → Client acting on behalf of a user → Authorization Code
8. **Sign-in redirect URLs** → https://<CUSTOMER_DOMAIN>/realms/access-analytics/broker/okta-oidc/endpoint
9. **Sign-out redirect URLs** → https://<CUSTOMER_DOMAIN>/realms/access-analytics/broker/okta-oidc/endpoint/logout_reponse <CUSTOMER_DOMAIN> will be provided by your Gathid representative. Click to Register the application. You will be redirected to an overview of your new application.



New Web App Integration

General Settings

App integration name: RightCrowd-Access-Analytics

Logo (Optional)

Grant type

Learn More

Client acting on behalf of itself

□ Client Credentials

Client acting on behalf of a user

☑ Authorization Code

□ Interaction Code

□ Refresh Token

□ Implicit (hybrid)

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://<CUSTOMER_DOMAIN>/realms/access-analytics/broker/ok

+ 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://<CUSTOMER_DOMAIN>/realms/access-analytics/broker/ok

+ 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

Enable immediate access (Recommended)

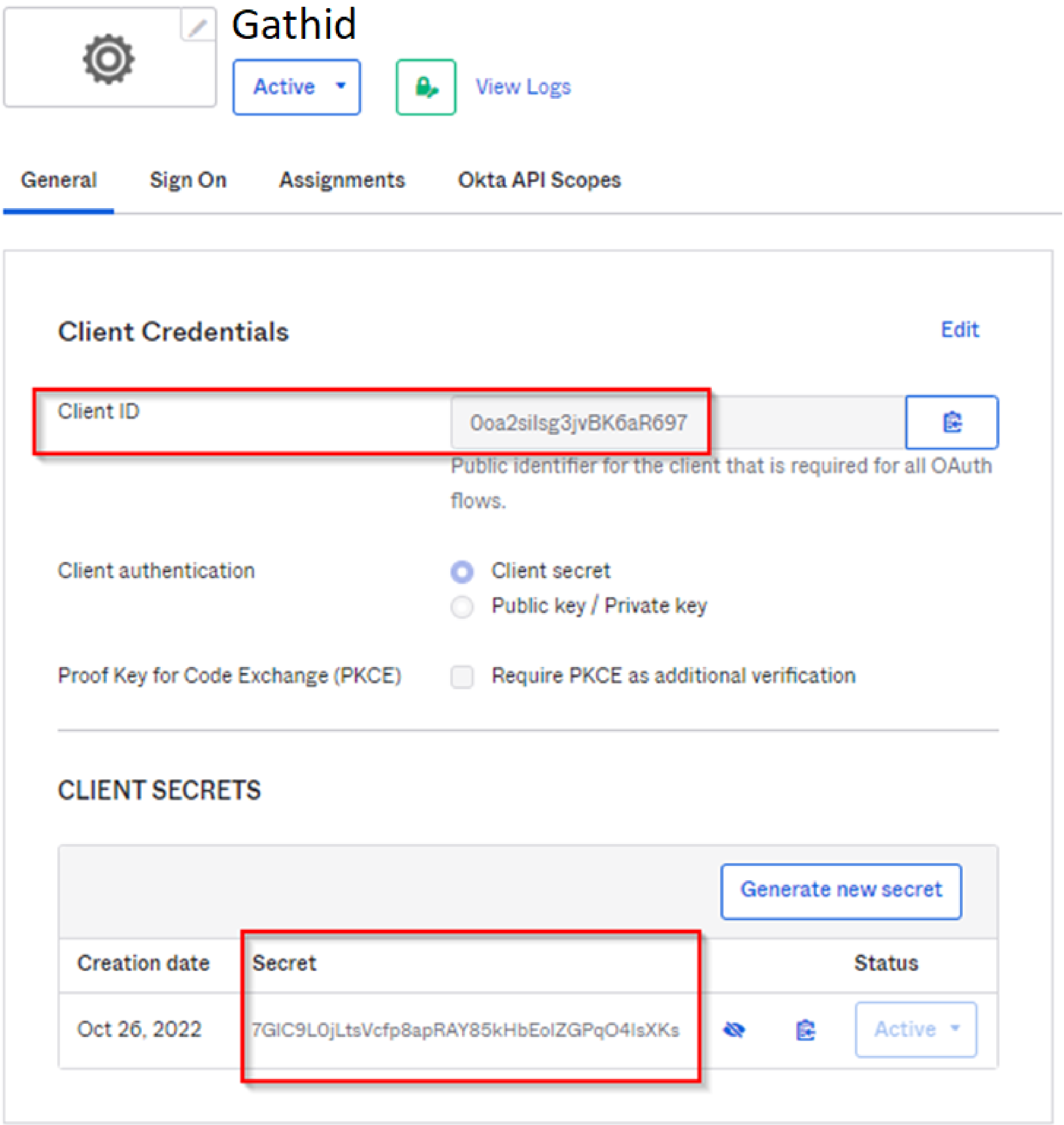
Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.

□ Enable immediate access with **Federation Broker Mode**

To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. Learn more about Federation Broker Mode.

Save Cancel

10. **Assignments** → Controlled access → Allow everyone in your organization to access
    NOTE: depending on your organizational policy, you may want to Limit access to selected groups.
11. Select **Save**
12. Once the application is created, on the **General** tab
13. Copy **Client ID**
14. Copy **Secret**



Client Credentials

Client ID: 0oa2silsg3jvBK6aR697

Public identifier for the client that is required for all OAuth flows.

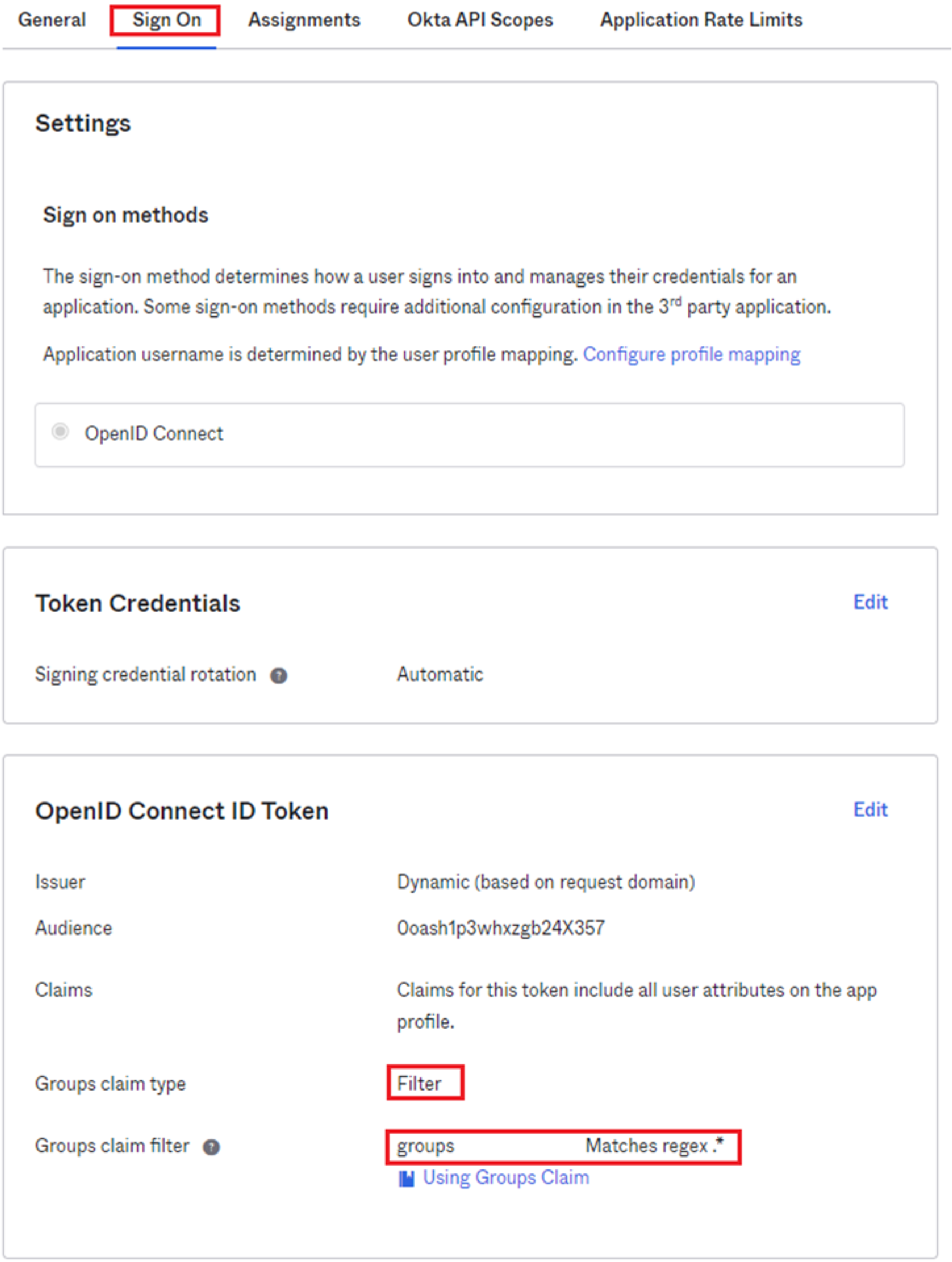
Client authentication: ● Client secret ○ Public key / Private key

Proof Key for Code Exchange (PKCE): □ Require PKCE as additional verification

CLIENT SECRETS

| Creation date | Secret | Status |
|---|---|---|
| Oct 26, 2022 | 7GlC9L0jLtsVcfp8apRAY85kHbEolZGPqO4lsXKs | Active |

15. Select **Sign On** tab to configure Okta group inclusion in the OpenID Connect Token



**Settings**

**Sign on methods**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ OpenID Connect

**Token Credentials** Edit

Signing credential rotation: Automatic

**OpenID Connect ID Token** Edit

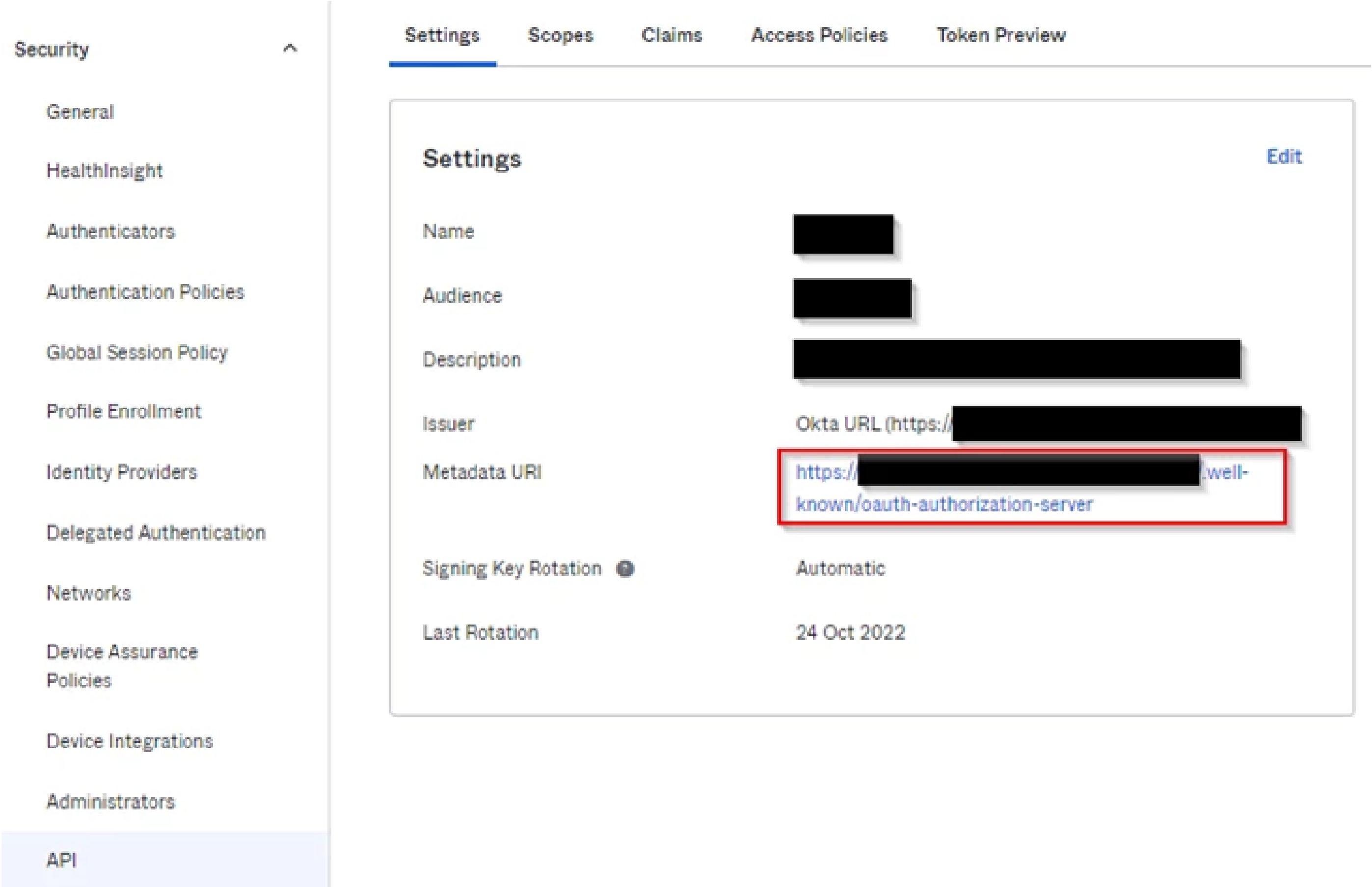
| | |
|---|---|
| Issuer | Dynamic (based on request domain) |
| Audience | 0oash1p3whxzgb24X357 |
| Claims | Claims for this token include all user attributes on the app profile. |
| Groups claim type | Filter |
| Groups claim filter | groups Matches regex .*<br>Using Groups Claim |

16. Add Claim with the following configuration:
    - Issuer-> Dynamic (based on request domain)
    - Groups claim type → Filter
    - Group claim filter → groups - Matches regex .*
    - The proposed regex filter will send all Okta groups to Gathid. To avoid an extensive list of groups, you may update the regex

filter to narrow down the list.
NOTE: For large enterprise companies to avoid exceeding the limit on the number of groups a token can emit, adjust matching regex to select only a subset of groups relevant only to access to Gathid

17. Depending on the Okta licence your organization has, you need to provide Metadata URI or your Okta Organization URL. If you are able to see the API option on the left side menu, please proceed to the next step and get a copy of the Metadata URI. If you do not have access to the API option, please provide your Okta Organization URL, which is the URL that your employees use to log into Okta.
For more information, you can find https://developer.okta.com/docs/concepts/auth-servers/#org-authorization-server-discovery-endpoints

18. Select **API** from the left side menu, and select **default** Authorization server. Copy Metadata URL:



Settings

Name [redacted]

Audience [redacted]

Description [redacted]

Issuer Okta URL (https:/[redacted]

Metadata URI https:/[redacted].well-known/oauth-authorization-server

Signing Key Rotation Automatic

Last Rotation 24 Oct 2022

19. Open the **Claims** tab from the same page and adjust the **groups** claim to have the **Value**:
isEmpty(Arrays.toCsvString(Groups.startsWith("active_directory","",100))) ? Groups.startsWith("OKTA","",100) : Arrays.flatten(Groups.startsWith("OKTA","",50),Groups.startsWith("active_directory","",50))

Note: This will ensure that any Active Directory groups synced with Okta are also displayed.

**Selecting Okta Groups to be used for Gathid Roles**

Once a user is authenticated to Gathid, authorization to specific functionality or data set is enforced by Role Base Access Control (RBAC). By default, Access Analytics has three roles defined: ADMINISTRATOR, USER, AND RESPONDER.

Initially, we recommend that you define at least one ADMINISTRATOR, other accounts can be added to the other roles that are suitable for your organization over time.

Okta Groups are used to map a Gathid role to people from your organization. You can use existing Okta groups or create specific groups for your Gathid Roles. Once you determine the group(s), please provide the group’s Object ID to your Gathid representative.

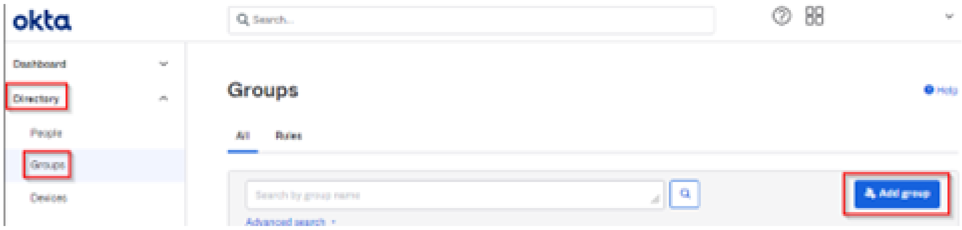
To find available group names, follow the steps below:

1. Browse to Okta Portal and log in to your organization.
2. Select: **Groups**
3. Copy the Group Names to be used for Access Analytics Roles.

**Creating new Gathid Groups in Okta**

The following steps describe the group creation:

1. Browse to your Okta Portal and log in to your organization.
2. Select: **Groups**
3. Select **Add group**



4. Define your new group name and description
5. Press **Save** to save the group.
6. Copy the **Name** and share it with your Gathid representative.

**Provide required information**

Make sure you have a copy of the following and provide it to your Gathid representative:

- ✓ Client ID
- ✓ Secret
- ✓ Metadata URL or your Okta Org name
- ✓ Group Names for mapping to Gathid Roles