ICI OKTA OIDC App

Configuration Guide for OIDC Integration

February 2021

Icertis

Table of Contents

1. Overview

Icertis has launched app integration in the Okta Integration Network (OIN). With help of this integration, clients will be able to use Single Sign On through OIDC and gain access to ICI API's through token generated through Okta.

2. OAuth

What is OAuth?

OAuth, which stands for "Open Authorization," allows third-party services to exchange your information without you having to give away your password. Basically, OAuth is an authorization protocol that allows you to approve one application interacting with another on your behalf without giving away your password.

How does ICI use OAuth?

ICI uses OAuth for providing access to ICI API to customers using Okta as a third party, which has been authorized by ICI to issue and validate authorization requests to access the API.

How does the authorization flow look like?

- Client Application requests Access token for ICI API from Okta Authorization Server.
- Okta token issuance endpoint validates the credentials and issues the JWT Access Token for ICI API.
- Over HTTPS, client application uses the returned JWT access token to add the JWT string with a "Bearer" designation in the Authorization header of the request to the ICI API.
- ICI's Token Validation handler will validate the Access token with the Okta Authorization server.
- If the token validation is successful, ICI will set up the user context based on a particular claim type value mapped against a User in ICI repository (user can be a service or an application user) and will return the desired resource accordingly.

1.1. Supported Features

- SSO in ICI using OIDC
- Access to ICI API using OAuth

1.2. Requirements

- Valid license or subscription of ICI platform
- Valid license or subscription of Okta

1.3. Configuration Steps

Configure OAuth

1. **Log on** to Okta with your administrator account.
2. **Navigate** to “Applications”.
3. **Click** “Add Application”.

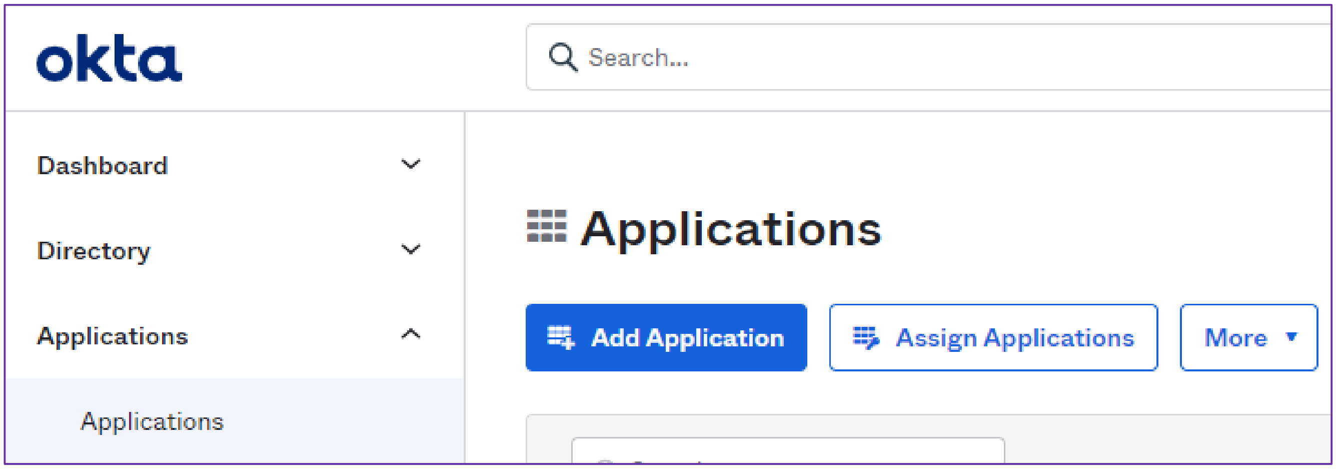
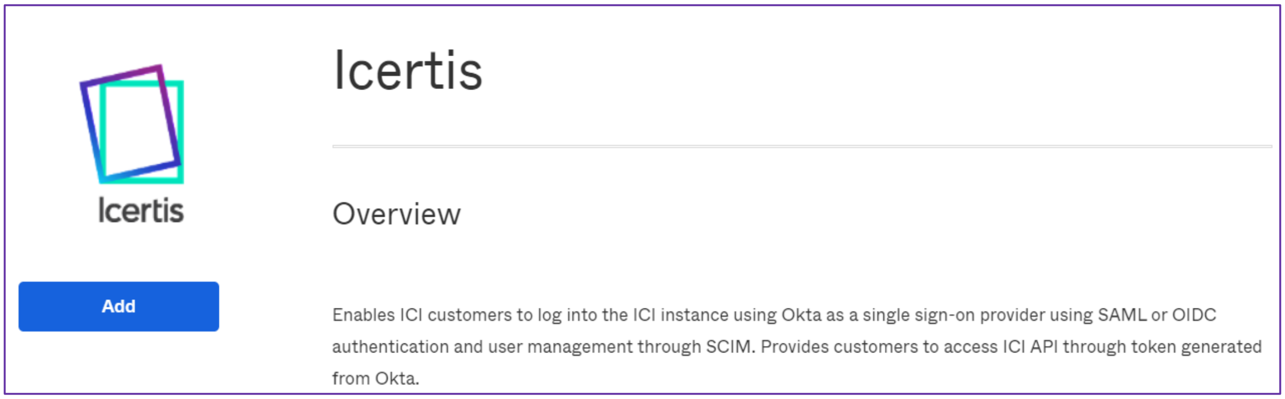


Figure 1 - Okta dashboard screen

4. **Search** for “Icertis” and **click** the App to select it.
5. **Click** “Add” on the left to continue.



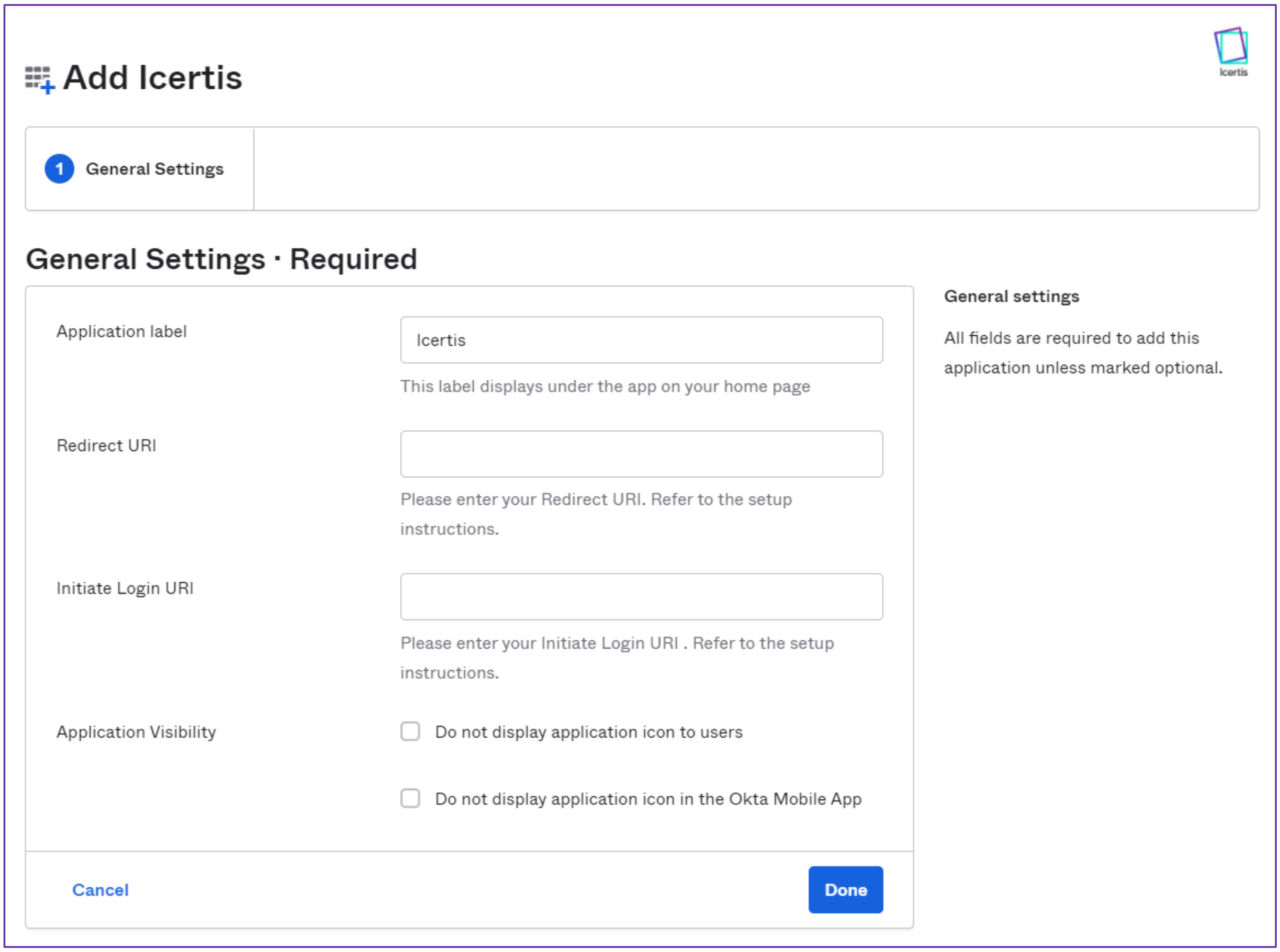
Icertis

Overview

Enables ICI customers to log into the ICI instance using Okta as a single sign-on provider using SAML or OIDC authentication and user management through SCIM. Provides customers to access ICI API through token generated from Okta.

Figure 2 – Add Icertis screen

6. **Enter** the "Redirect URI and Initiate Login URI" of your Icertis instance.



Add Icertis

1 General Settings

General Settings · Required

Application label	Icertis This label displays under the app on your home page
Redirect URI	Please enter your Redirect URI. Refer to the setup instructions.
Initiate Login URI	Please enter your Initiate Login URI . Refer to the setup instructions.
Application Visibility	□ Do not display application icon to users □ Do not display application icon in the Okta Mobile App

General settings

All fields are required to add this application unless marked optional.

Figure 3 – Add General Settings.

7. **Click** “Done” to add the App.
8. After the app is added, users must be assigned to it. This will allow them to use the Okta credentials.
9. **Open** the newly added App under “Applications” and navigate to the “Assignments” tab.

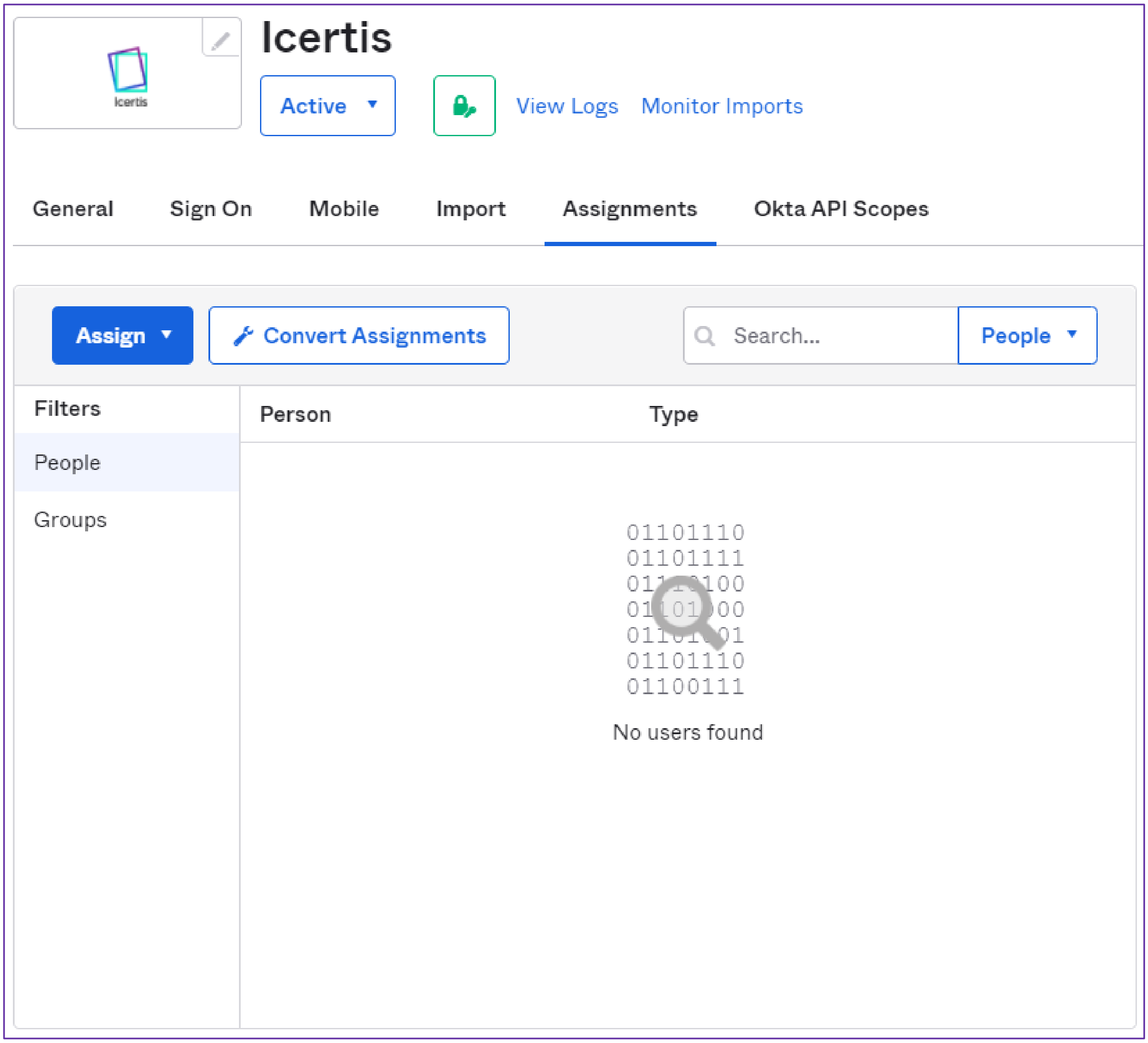


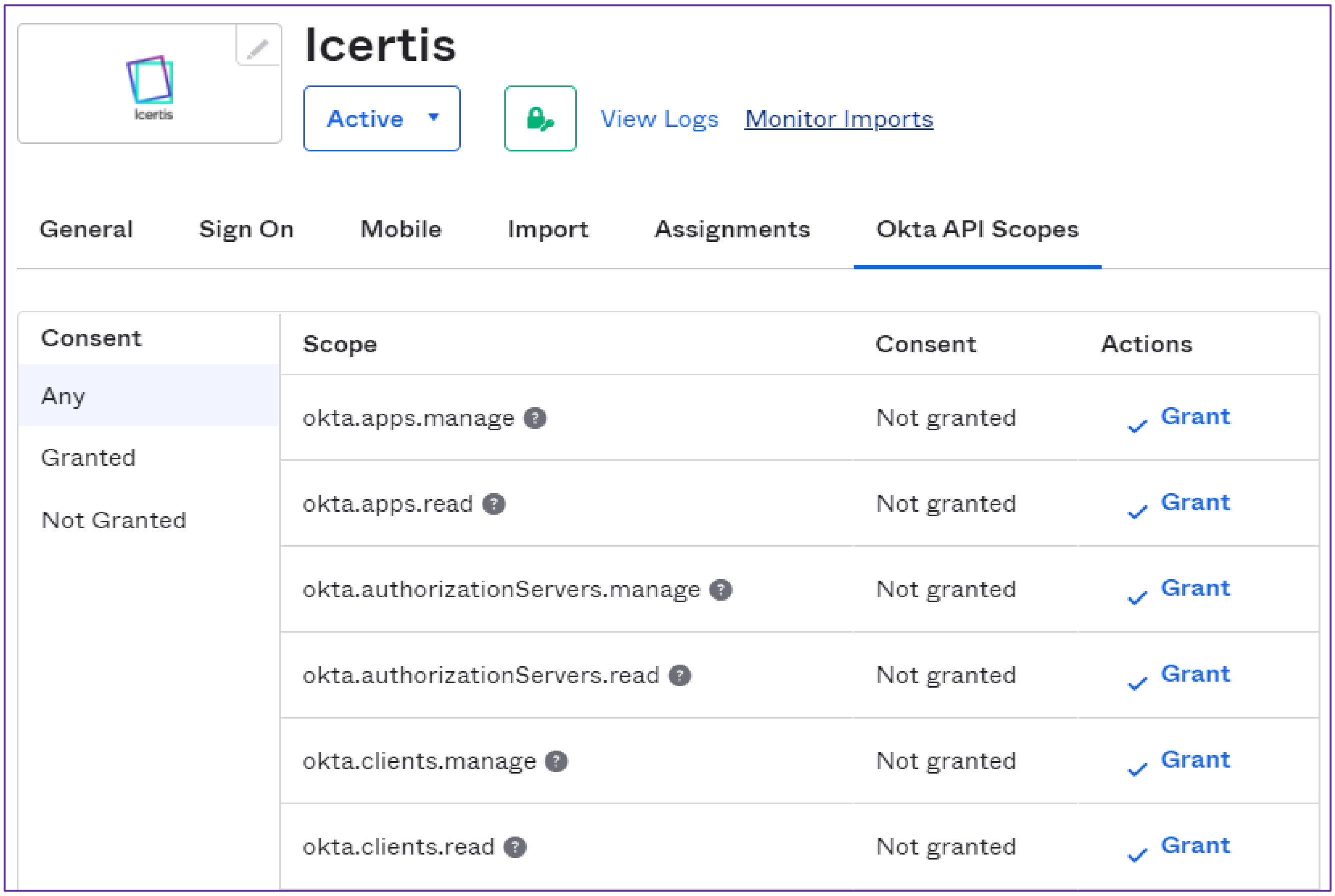
Figure 4 – OAuth App assignment section

10. **Click** on “Assign” and pick the appropriate principal type you want to assign (person or group).

11. **Modify** the assignment fields as needed (defaults should suffice) and **click** “Save and Go Back”.

12. **Click** “Done” to close the dialog.

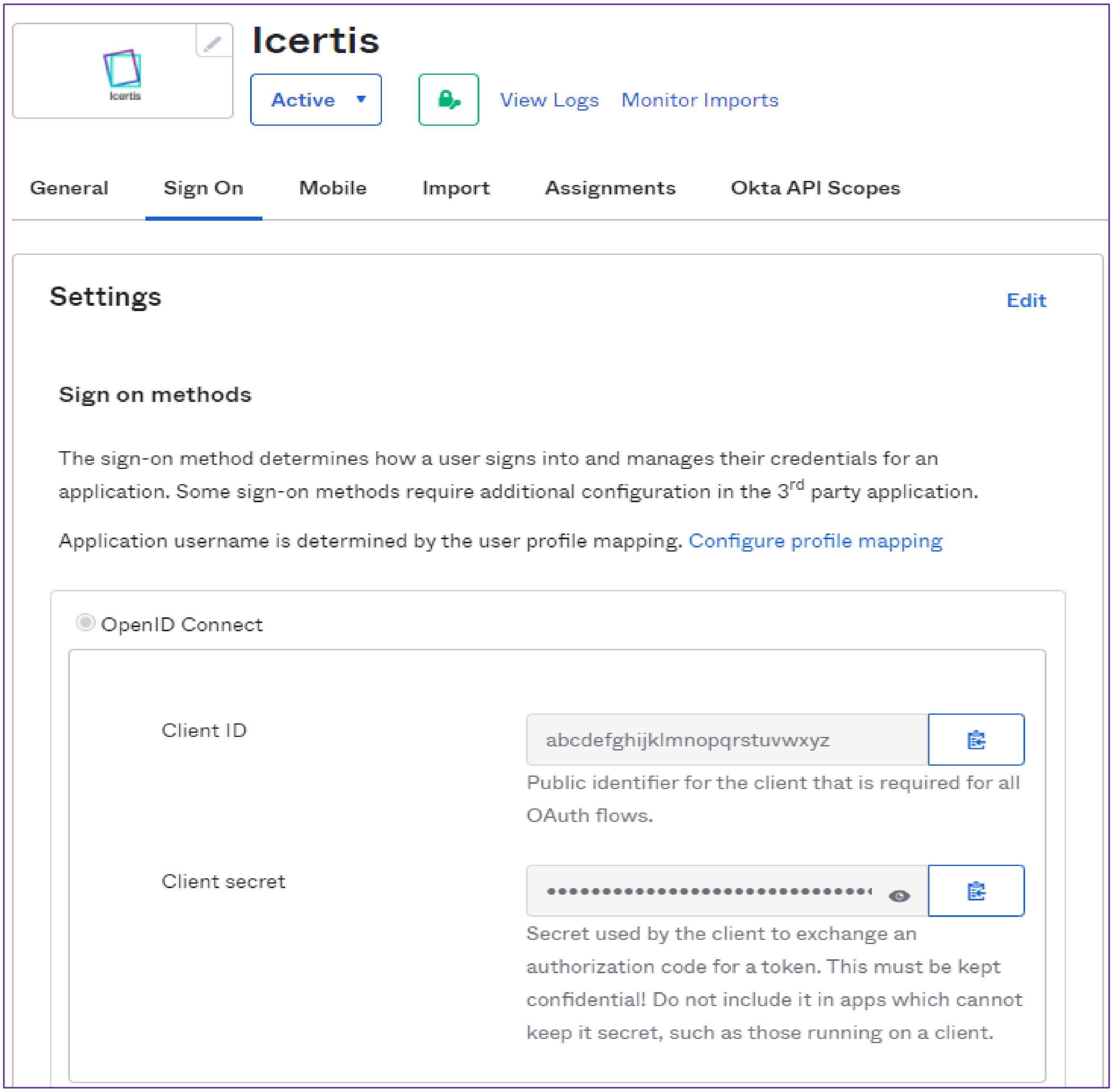
13. **Navigate** to the “Okta API Scopes” tab and grant/revoke scope consent as needed. This is shown in Figure - 5 below. ICI expects atleast 2 scopes – openid, custom scope (to denote use with client credentials flow). Custom scope can be created as shown in Figure 9, 10.



Scope	Consent	Actions
okta.apps.manage ?	Not granted	✓ Grant
okta.apps.read ?	Not granted	✓ Grant
okta.authorizationServers.manage ?	Not granted	✓ Grant
okta.authorizationServers.read ?	Not granted	✓ Grant
okta.clients.manage ?	Not granted	✓ Grant
okta.clients.read ?	Not granted	✓ Grant

Figure 5 – Okta Scopes section

14. **Navigate** to the “Sign On” tab and note the “Client ID” and “Client secret” values. These will be used for setting up API integration.



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

Client ID: abcdefghijklmnopqrstuvwxyz

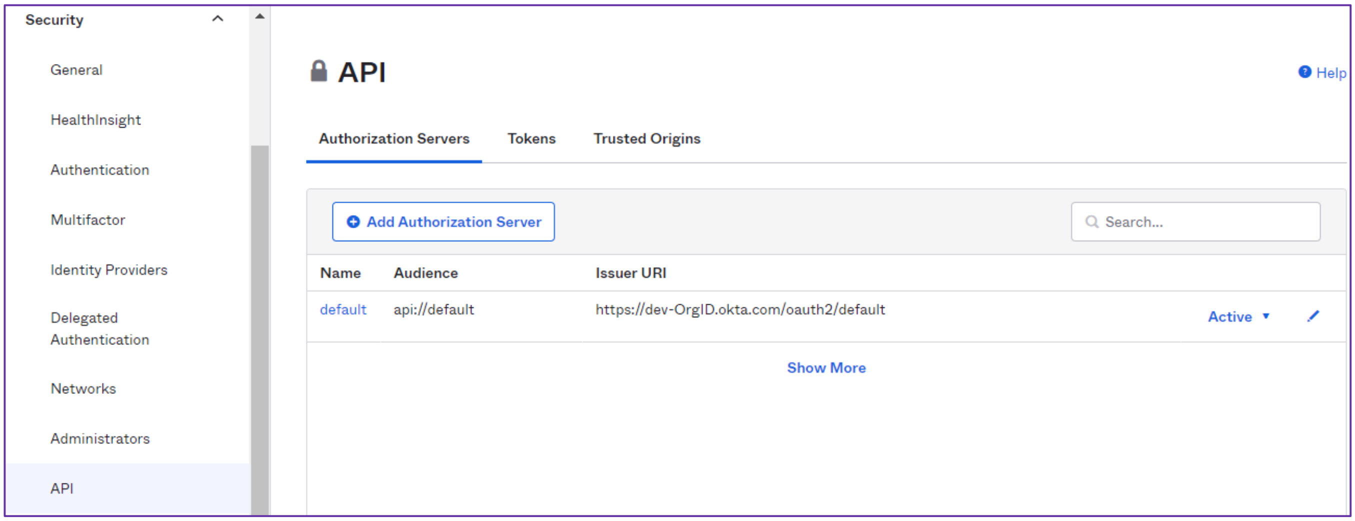
Public identifier for the client that is required for all OAuth flows.

Client secret: ••••••••••••••••••••••••••••••

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

Figure 6 – Client Credentials

15. **Navigate** to “API” tab and **select** “Authorization Servers” which enlists all servers configured in Okta.



Name	Audience	Issuer URI
default	api://default	https://dev-OrgID.okta.com/oauth2/default

Figure 7 – Authorization Servers

16. **Add** a new Authorization Server (if it's not already present) by clicking on "Add Authorization Server" button and fill required details (Name and Audience) and Save it. ICI expects audience to be: "*api://default".*

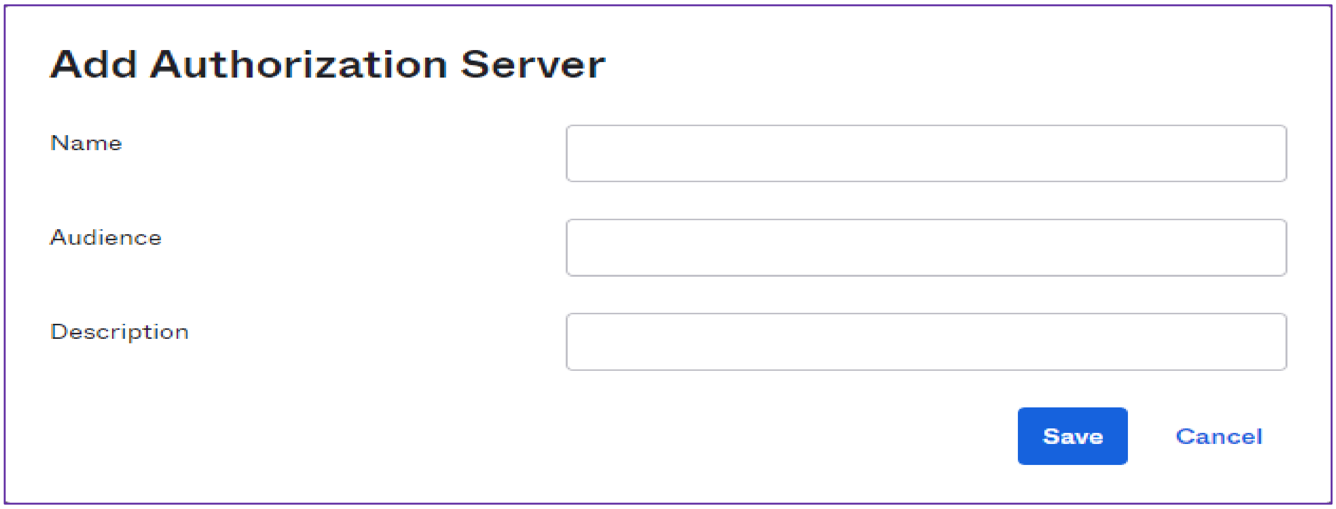


Figure 8 – Add Authorization Server Form.

17. Once the server has been created, we can create custom scopes by clicking *Add Scope* as shown in Figure – 9. For example – We will create oauth_custom_scope to be used in authorization flow as show in Figure – 10.

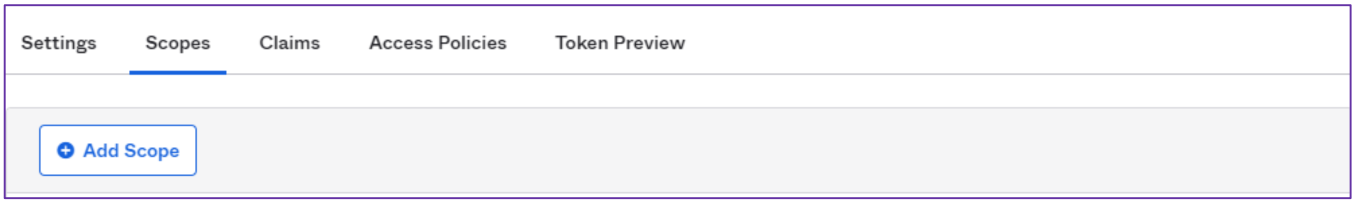
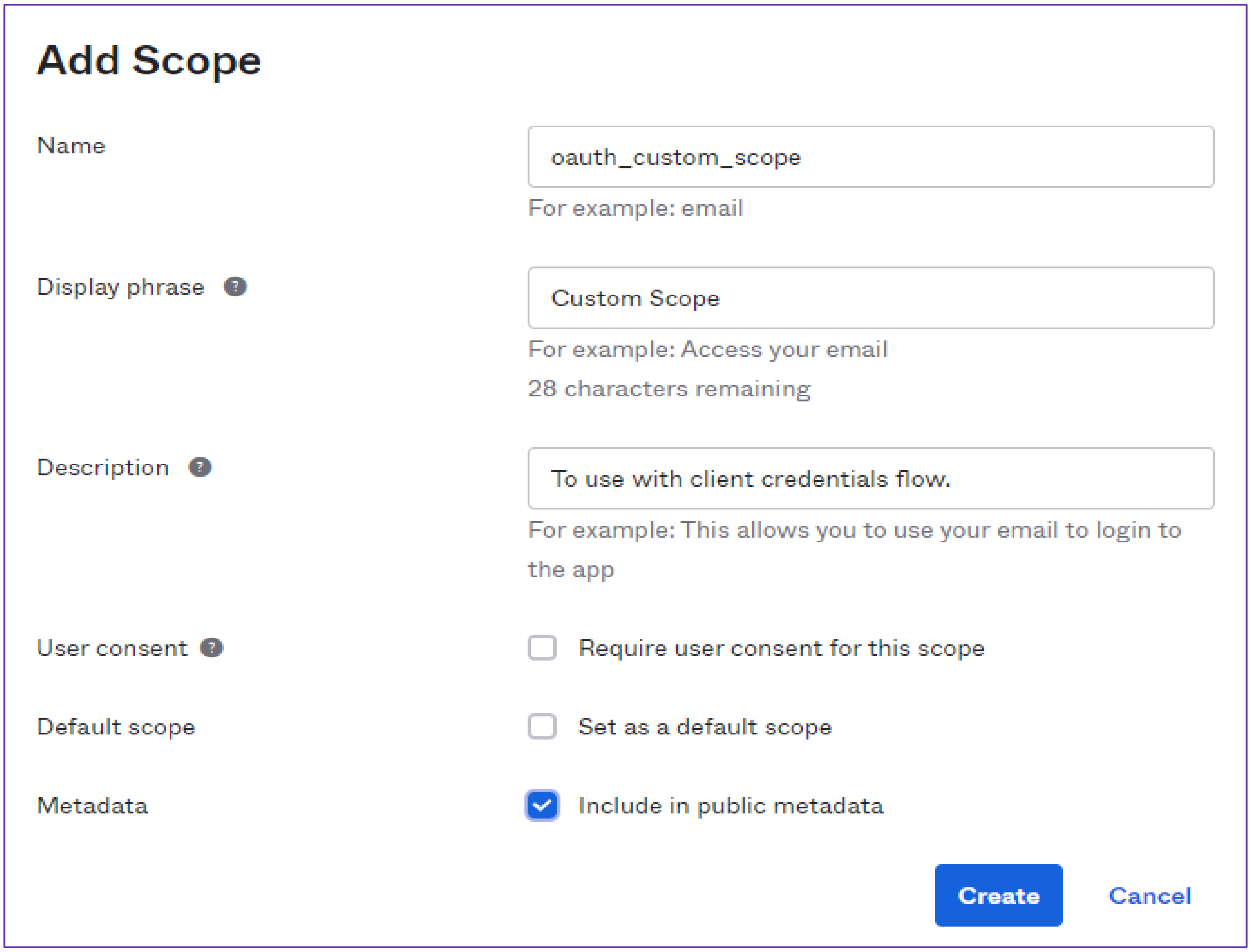


Figure 9 – Create Custom Scope



Add Scope

Name: oauth_custom_scope
For example: email

Display phrase: Custom Scope
For example: Access your email
28 characters remaining

Description: To use with client credentials flow.
For example: This allows you to use your email to login to the app

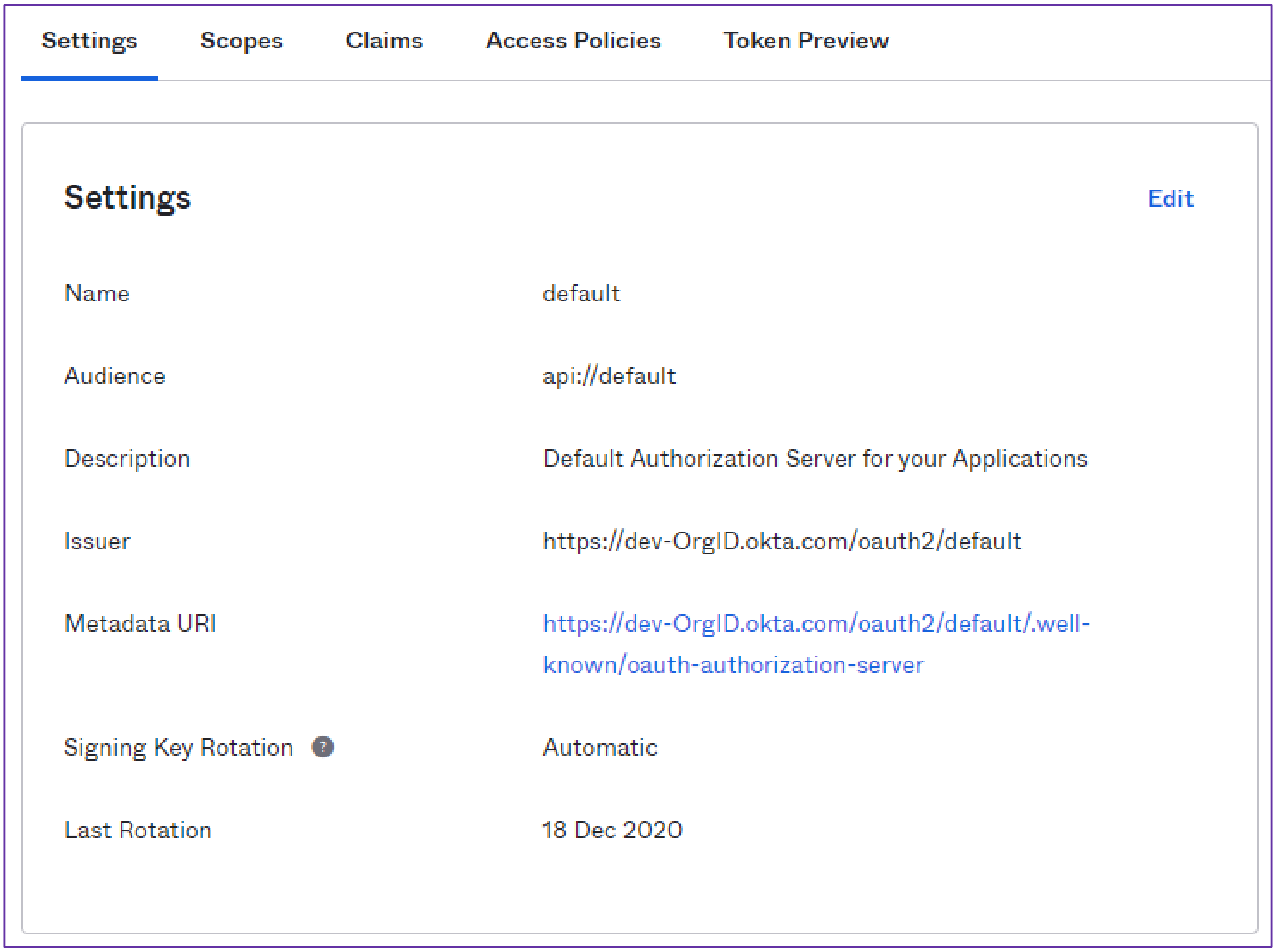
User consent: □ Require user consent for this scope

Default scope: □ Set as a default scope

Metadata: ☑ Include in public metadata

Figure 10 – Create Custom Scope Fields.

18. **Select** one of the authorization servers listed in the server list (Refer Figure 7). Use these details to configure your ICI instance.



Settings

Name	default
Audience	api://default
Description	Default Authorization Server for your Applications
Issuer	https://dev-OrgID.okta.com/oauth2/default
Metadata URI	https://dev-OrgID.okta.com/oauth2/default/.well-known/oauth-authorization-server
Signing Key Rotation	Automatic
Last Rotation	18 Dec 2020

Figure 11 – Authorization Server Details.

19. Use Client Credentials (Refer Figure 6) and Authorization Server Details (Refer Figure 11) to setup OIDC and OAuth in ICI.

1.4. Notes

1. To begin using OAuth flow, log on to your ICI instance. For example, *.icertis.com. The Okta Login page opens.
2. Enter your credentials and if authentication is successful, you will be redirected back to your ICI instance.