innovar healthcare

OIDC Plugin

Created: Jan 2, 2026
Updated:

Introduction

OIDC is an **open, industry-standard identity protocol** built on OAuth 2.0. By adopting OIDC, the integration engine can seamlessly integrate with leading Identity Providers (IdPs) such as **Google Auth Platform and Okta,** avoiding vendor lock-in and ensuring long-term compatibility.

Why OIDC?

Centralized Identity Management

The OIDC plugin enables **centralized user authentication** through an external IdP rather than local user stores. This allows organizations to:

- Manage users, roles, and credentials in one place
- Enforce consistent authentication policies across systems
- Reduce administrative overhead within the integration engine

Enhanced Security Posture

- Eliminating local password storage within Mirth Connect / BridgeLink
- Supporting strong authentication mechanisms such as **Multi-Factor Authentication (MFA)**
- Using **short-lived tokens** and cryptographic signing (JWT) to **prevent credential leakage**

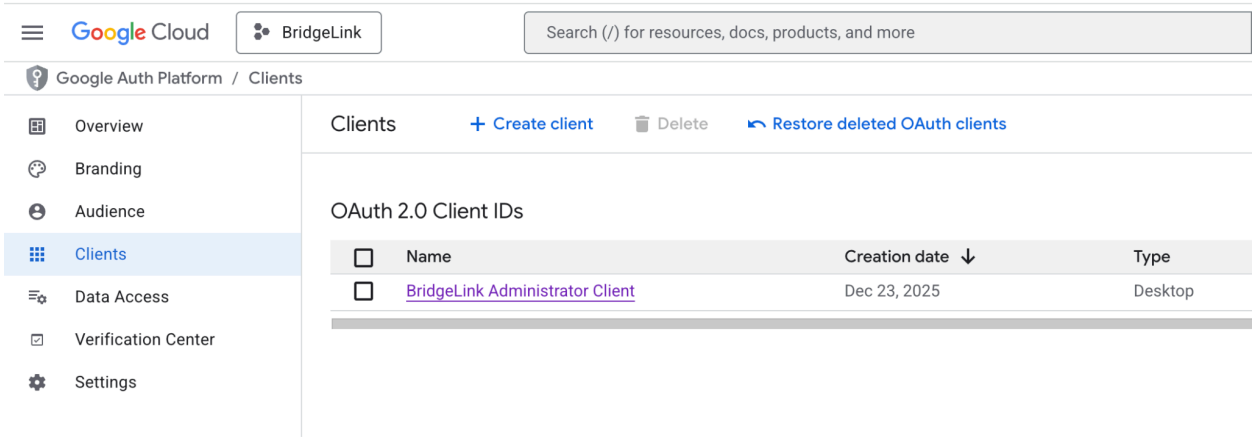
Improved User and Administrator Experience

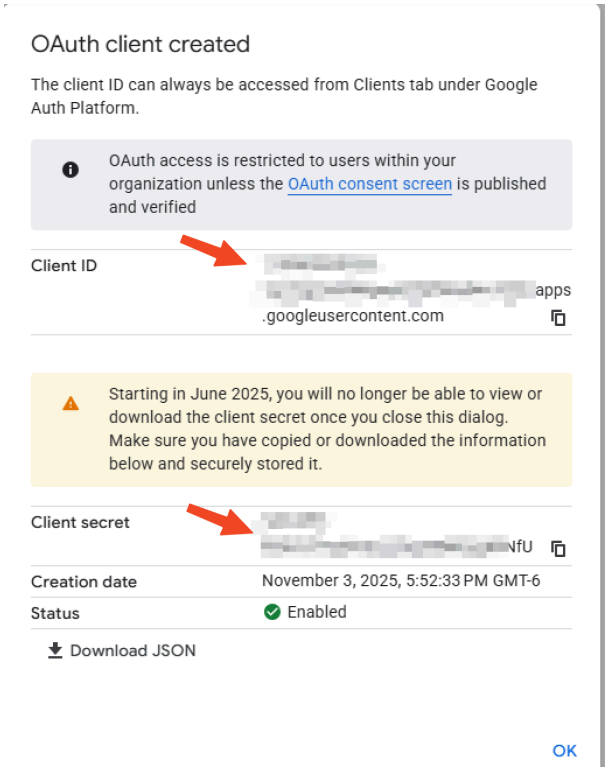
- Users benefit from familiar enterprise login experiences
- Administrators gain simplified onboarding and offboarding

Configure with Google Auth Platform

Prerequisite

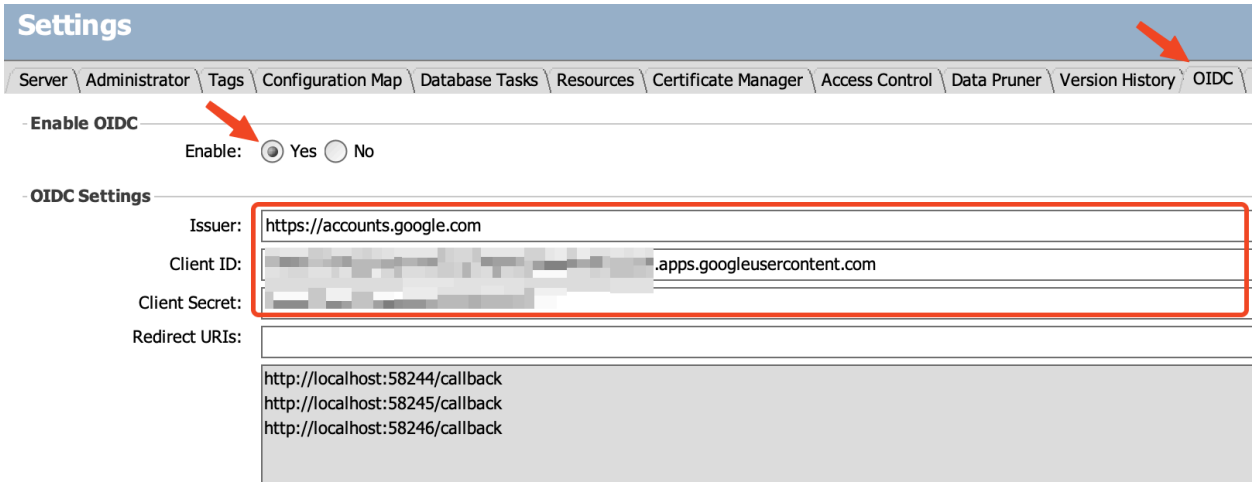
- Create an OAuth 2.0 Client ID and select the **Desktop** application type.
- Securely save the Client ID and Secret obtained from your Google Cloud Platform (GCP) account.





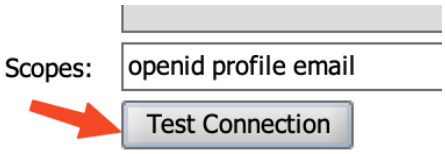
Step 1: Configure OIDC Settings

- Open the **BridgeLink Administrator Console** and navigate to **Settings** > **OIDC**.
- Enable the OIDC feature.
- Enter the Issuer URL: `https://accounts.google.com`
- Enter the Client ID and Secret.
- Add at least 3 **Callback URLs**. You can enter idle ports on your local machine.

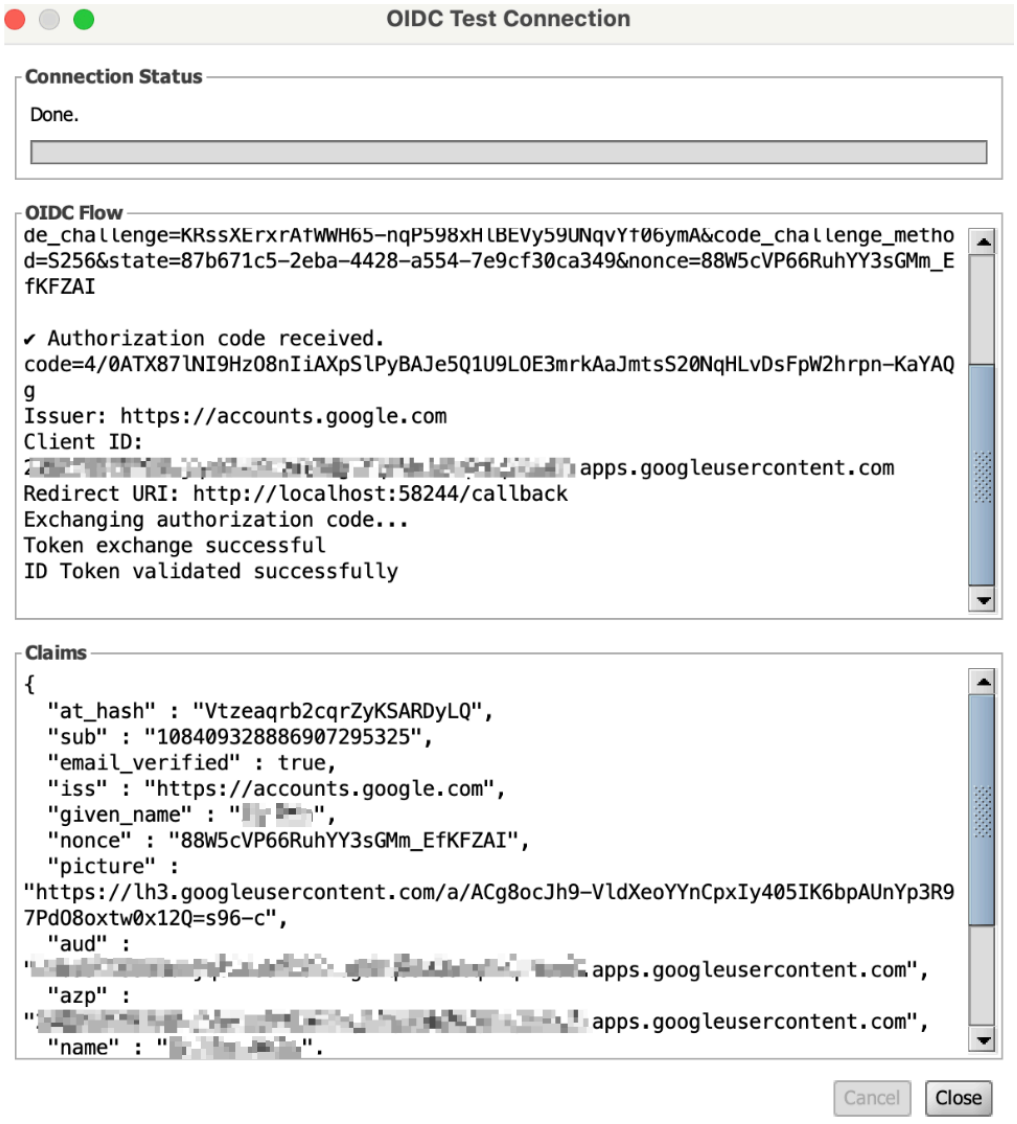


Test Connection

Click “Test Connection” to run a test with your OIDC server



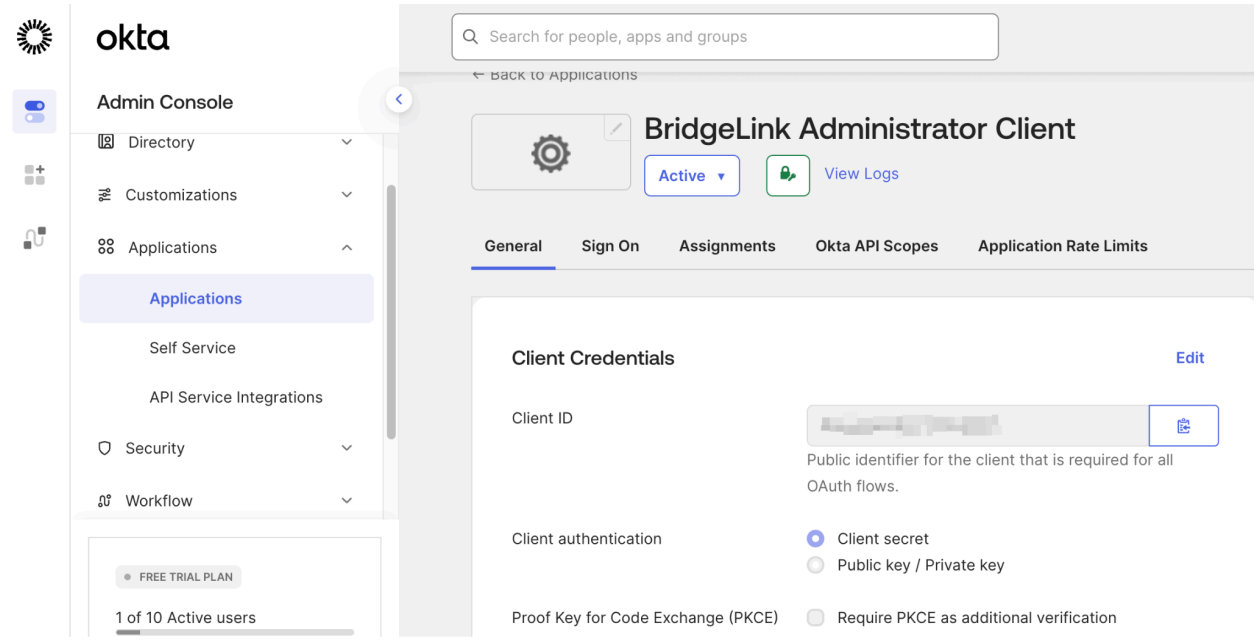
You can see the claims response from OIDC server in the prompt dialog window



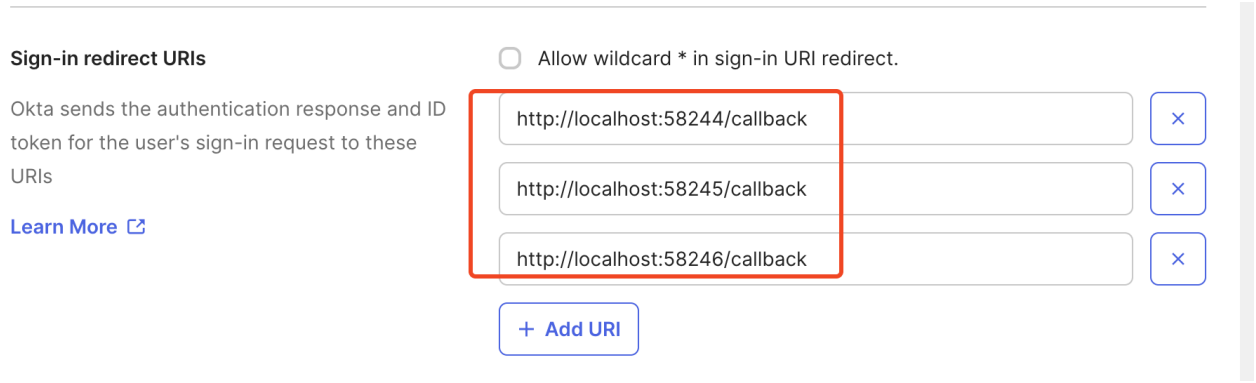
Configure with Okta

Prerequisite:
Please create an App Integration in your Okta account.

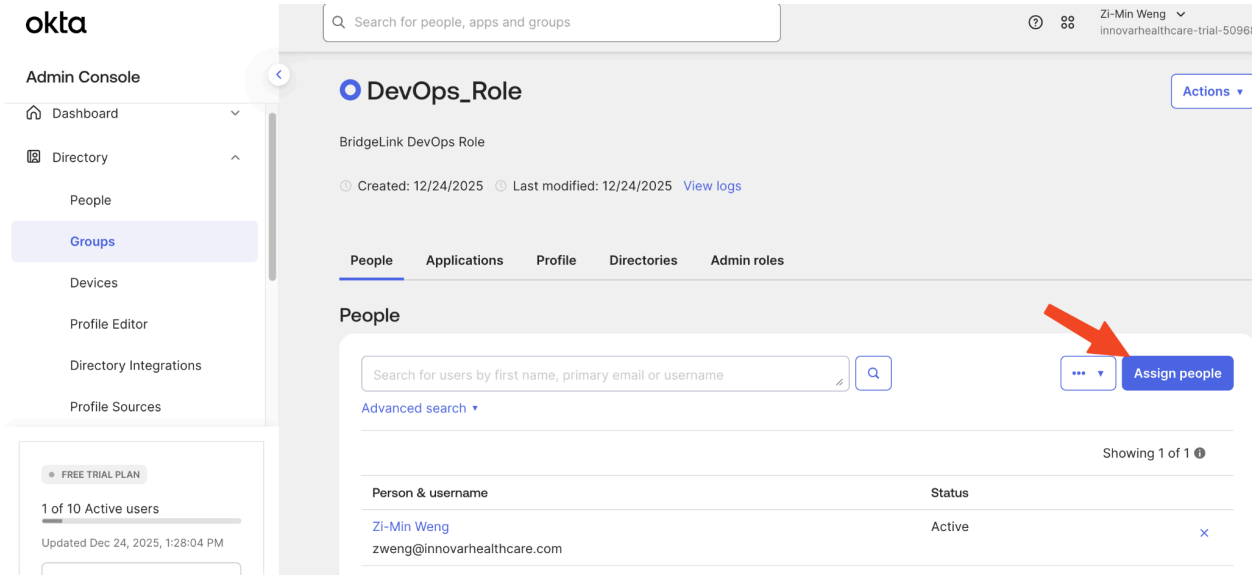
EX:



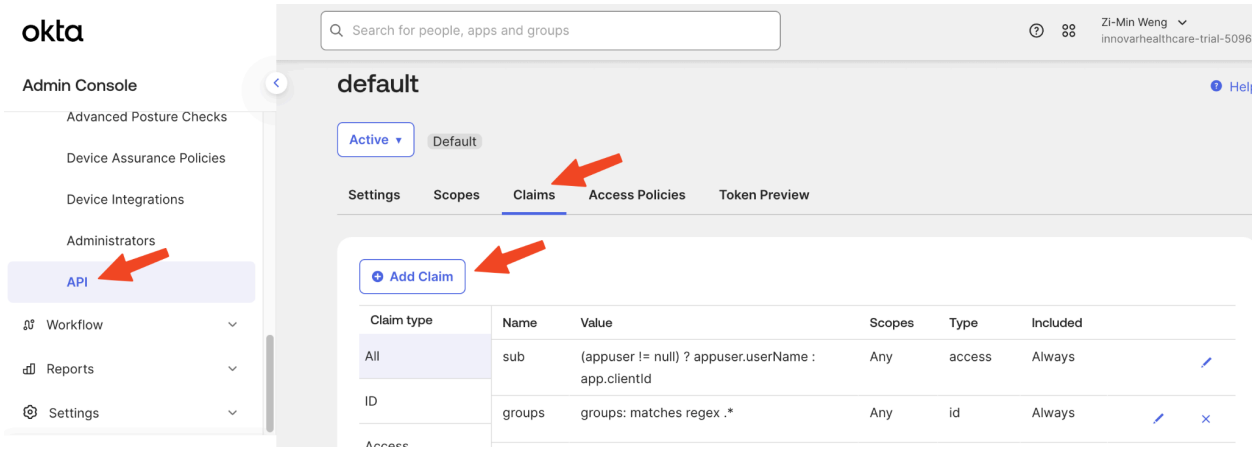
Make sure you enter at least 3 callback urls, these will be used in the BridgeLink OIDC setting.



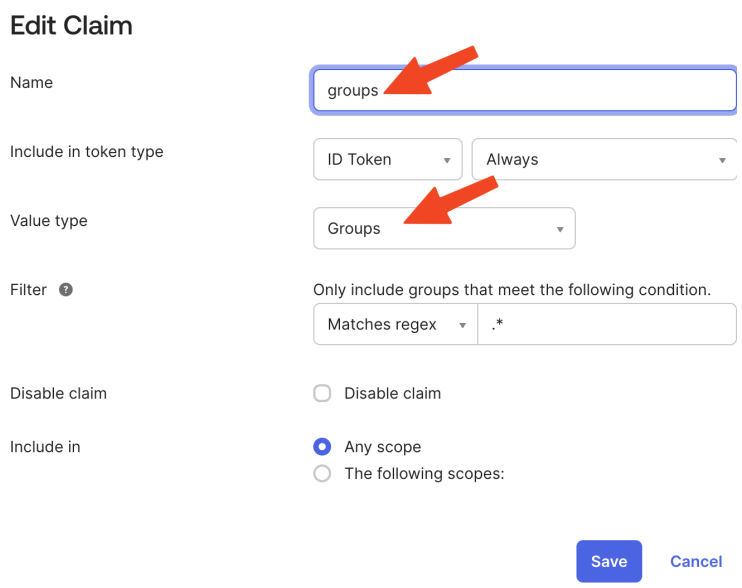
Navigate to **Okta -> Directory -> Groups -> “Add group”, and add user to the group**
EX:



Navigate to **Okta -> Security -> API -> Select the Authorizer server -> Claims -> Add Claim**

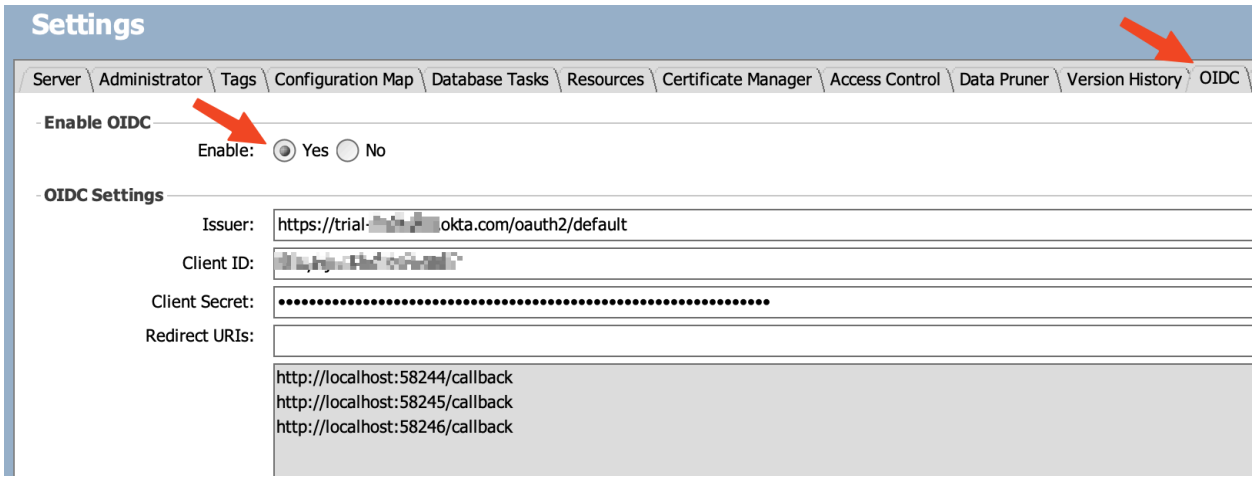


In the Claim edit window, please enter “groups”, select the ID Token for token type, Groups for Value type. And save.



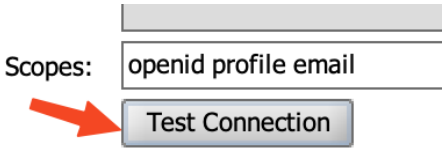
Step 1: Configure OIDC Settings

- Open the **BridgeLink Administrator Console** and navigate to **Settings** > **OIDC**.
- Enable the OIDC feature.
- Enter the Issuer URL: `https://{yourOktaDomain}/oauth2/default`
- Enter the Client ID and Secret.
- Add the same **Callback URLs as on Okta**. You can enter idle ports on your local machine.

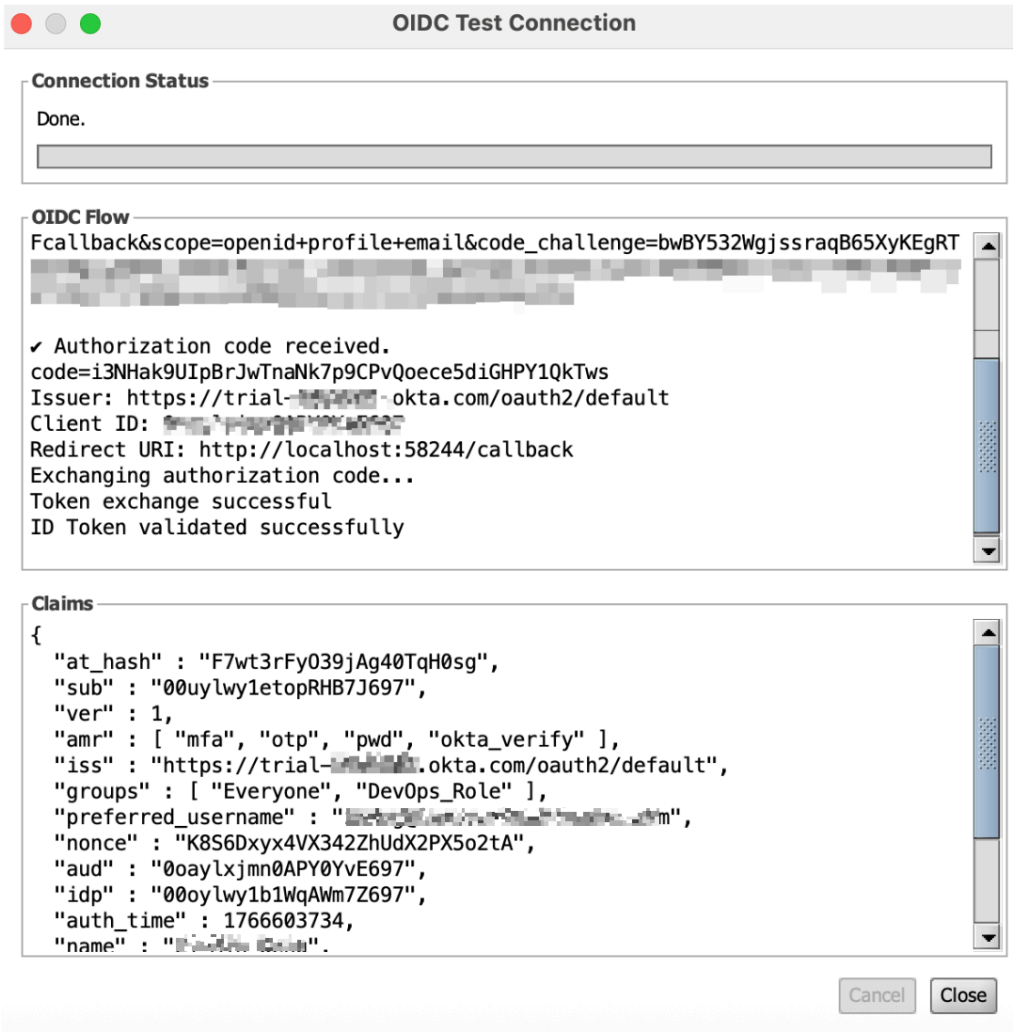


Test Connection

Click “Test Connection” to run a test with your OIDC server



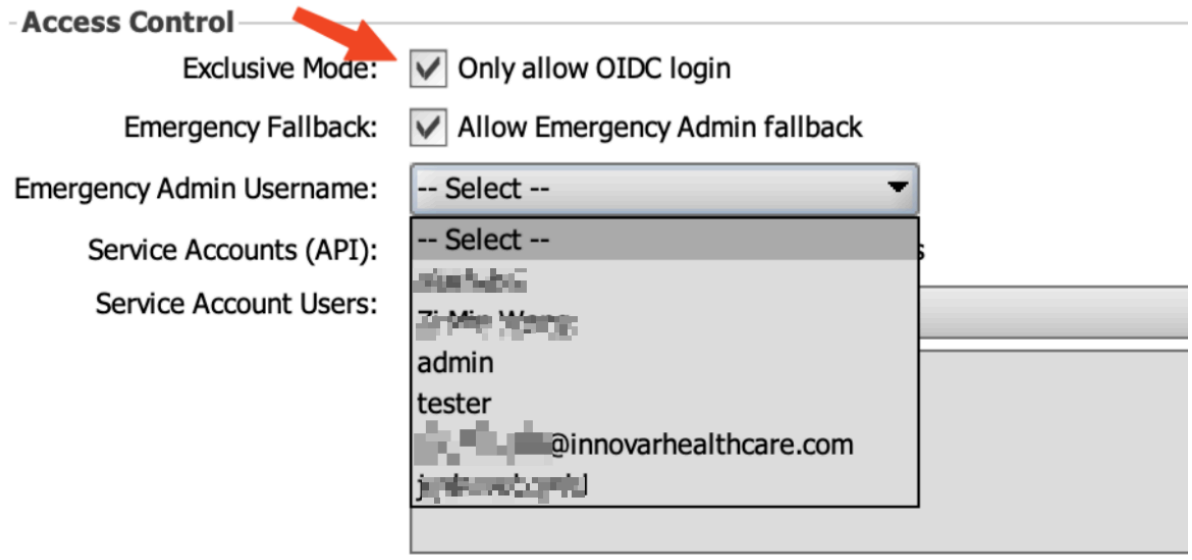
You can see the claims response from OIDC server in the prompt dialog window
EX:



After Issuer Configuration:

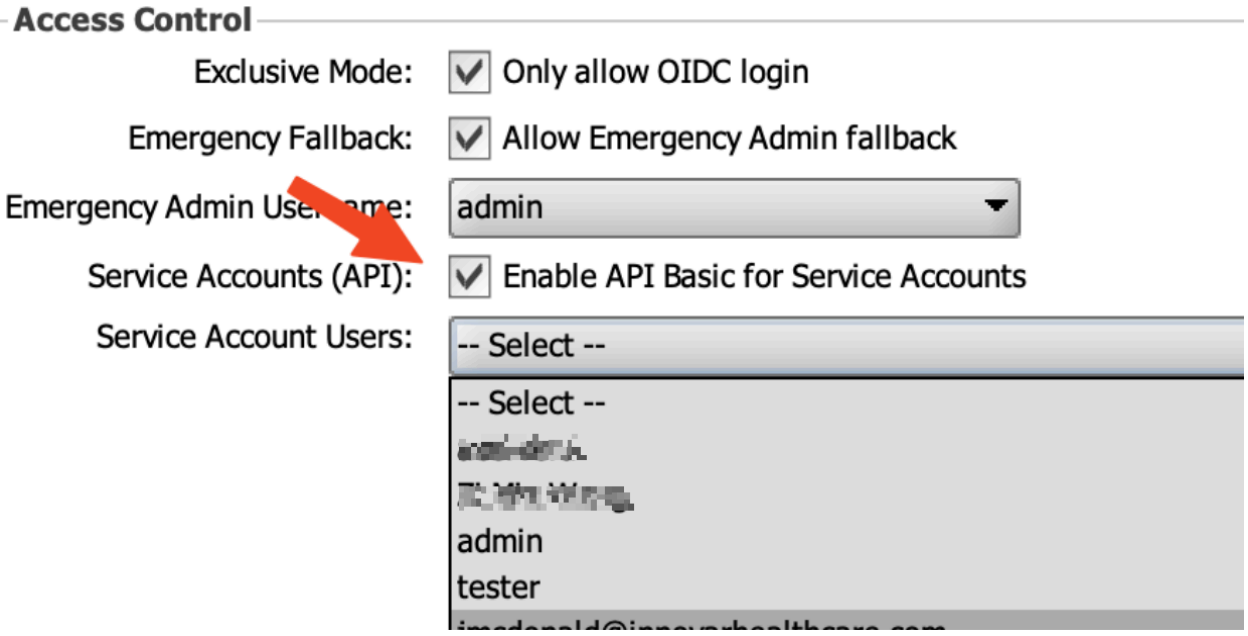
Configure Only Allow OIDC Login

If "Only allow OIDC login" is selected, all BridgeLink users **must** sign in through the OIDC server. An exception user can be added to bypass OIDC authentication for emergency fallback.



Enable API Basic for Service Accounts

When "Enable API Basic for Service Accounts" is enabled and a user is chosen, only the selected user can access and utilize the BridgeLink APIs (https://<BridgeLink IP>:8443/api).

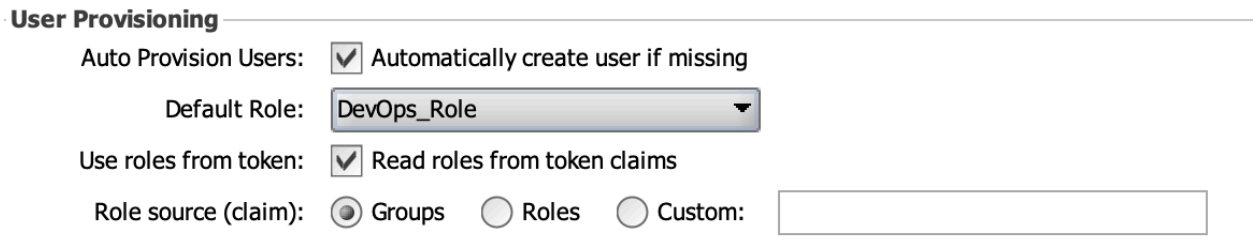


Configure Auto Provision User

This feature creates a new user in BridgeLink if the username from the OIDC login does not exist. The new user will be assigned the role defined in the Innovar Role-Based Control plugin.

Role Source from OIDC Claims

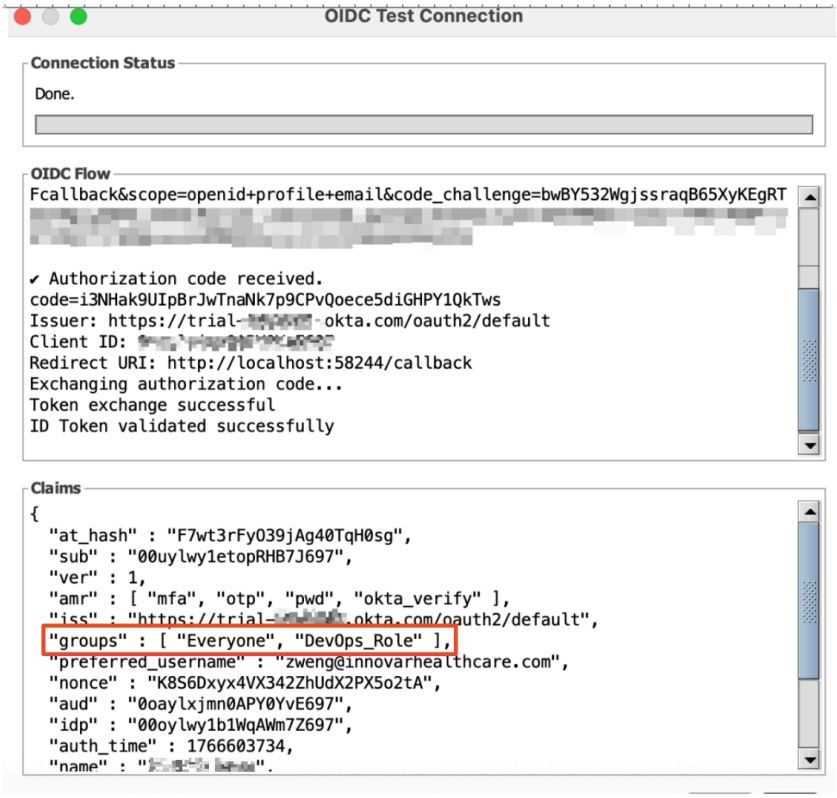
If you check "**Read roles from token claims,**" the OIDC plugin reads the role name from the claim payload and assigns the matched role name in the Innovar Role-Based Control plugin. You must define the corresponding role privilege in the Innovar Role-Based plugin first.



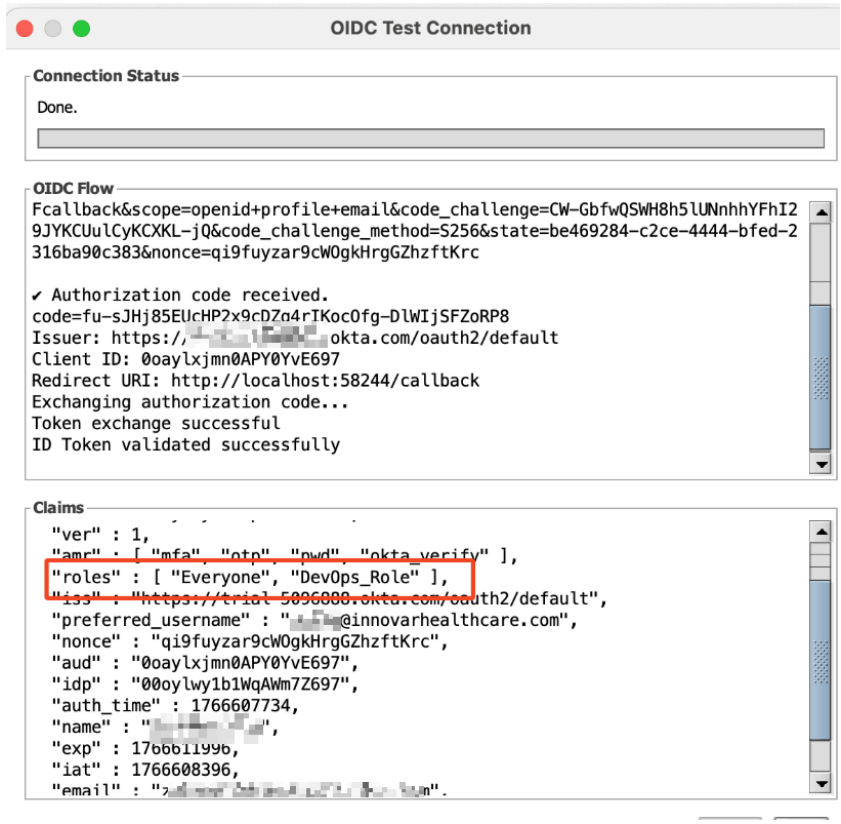
Role source from OIDC claims

EX: the claim payload from Okta with group name “DevOps_Role”, please select the role source based on the OIDC claim response. For example, select “Groups” if you see the claims like the

below picture:



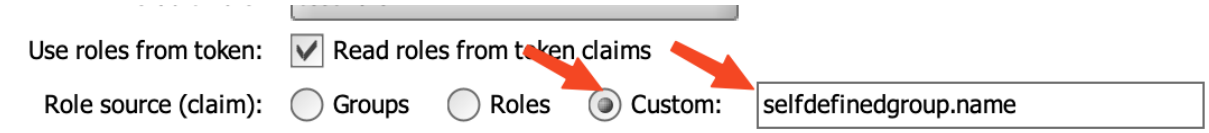
Select “Roles” if you see the claim like the below picture:



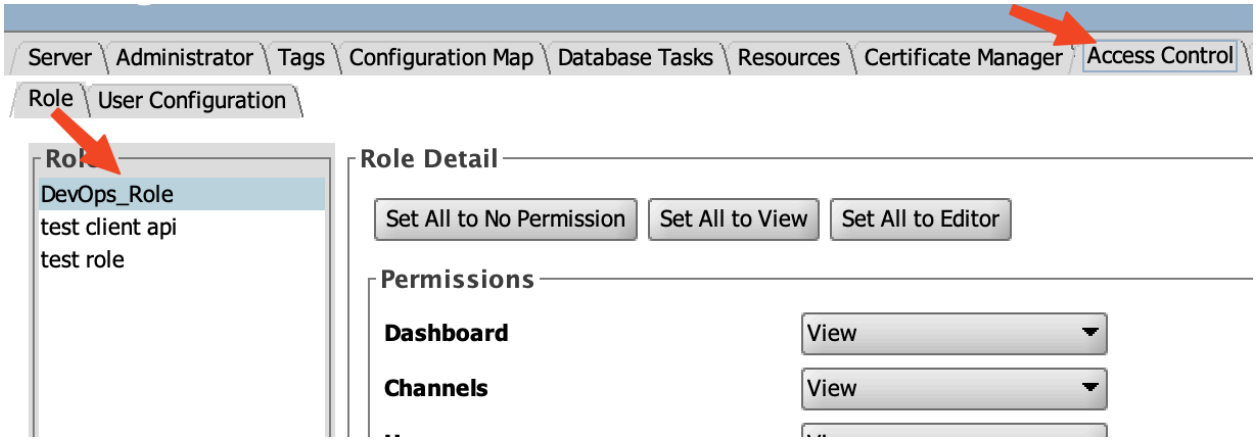
Select “custom” and enter the custom pattern in claim
EX: claim response

```
{
  "selfdefinedgroup": {
    "name": "DevOps_Role"
  }
}
```

Custom Role source claim:



Make sure you have the same role name in the Innovar Role-based Control setting.



This configuration **will automatically create a new user** in BridgeLink—if they do not already exist—upon sign-in with OIDC, assigning them the **DevOps_Role** privilege.

Now you are all set!