

OIDC Plugin

Created: Jan 2, 2026
Updated:

Introduction.....	3
Why OIDC?.....	3
Configure with Google Auth Platform.....	4
Test Connection.....	5
Configure with Okta.....	6
Test Connection.....	9
After Issuer Configuration:.....	10
Configure Only Allow OIDC Login.....	10
Enable API Basic for Service Accounts.....	11
Configure Auto Provision User.....	12
Role source from OIDC claims.....	12

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.

Google Cloud

BridgeLink

Search (/) for resources, docs, products, and more

Google Auth Platform / Clients

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Clients

+ Create client

Delete

Restore deleted OAuth clients







OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type
<input type="checkbox"/>	BridgeLink Administrator Client	Dec 23, 2025	Desktop

OAuth client created

The client ID can always be accessed from Clients tab under Google Auth Platform.

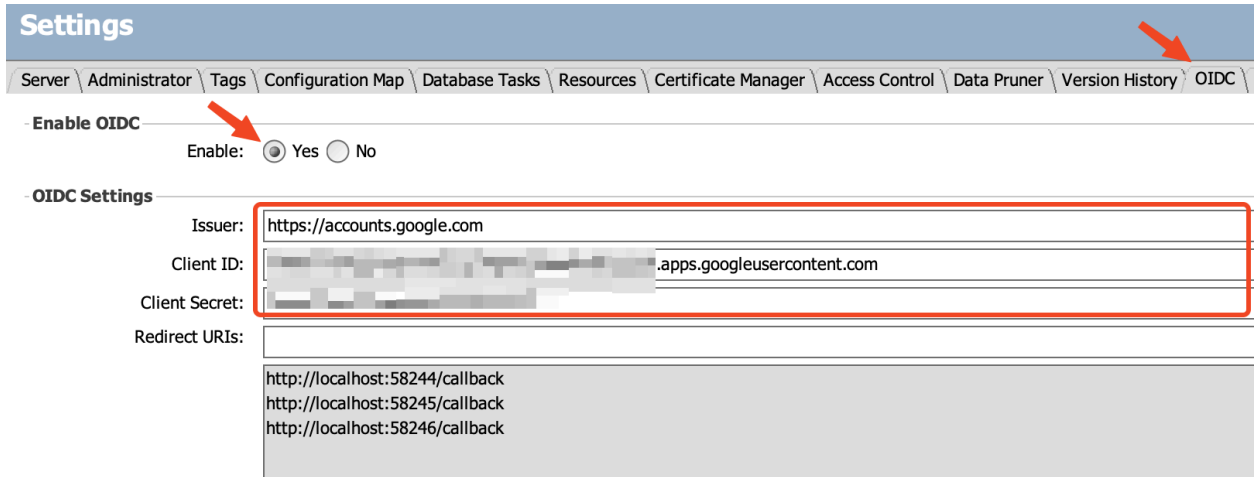
i OAuth access is restricted to users within your organization unless the [OAuth consent screen](#) is published and verified

Client ID	 [Redacted] apps .googleusercontent.com 
Client secret	 [Redacted] nFU 
Creation date	November 3, 2025, 5:52:33 PM GMT-6
Status	 Enabled
 Download JSON	

OK

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.



Settings

Server | Administrator | Tags | Configuration Map | Database Tasks | Resources | Certificate Manager | Access Control | Data Pruner | Version History | **OIDC**

- Enable OIDC

Enable: ☒ Yes ☐ No

- OIDC Settings

Issuer:

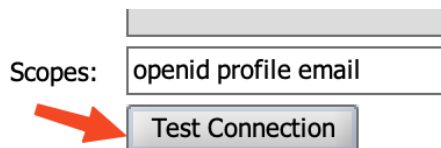
Client ID:

Client Secret:

Redirect URIs:

Test Connection

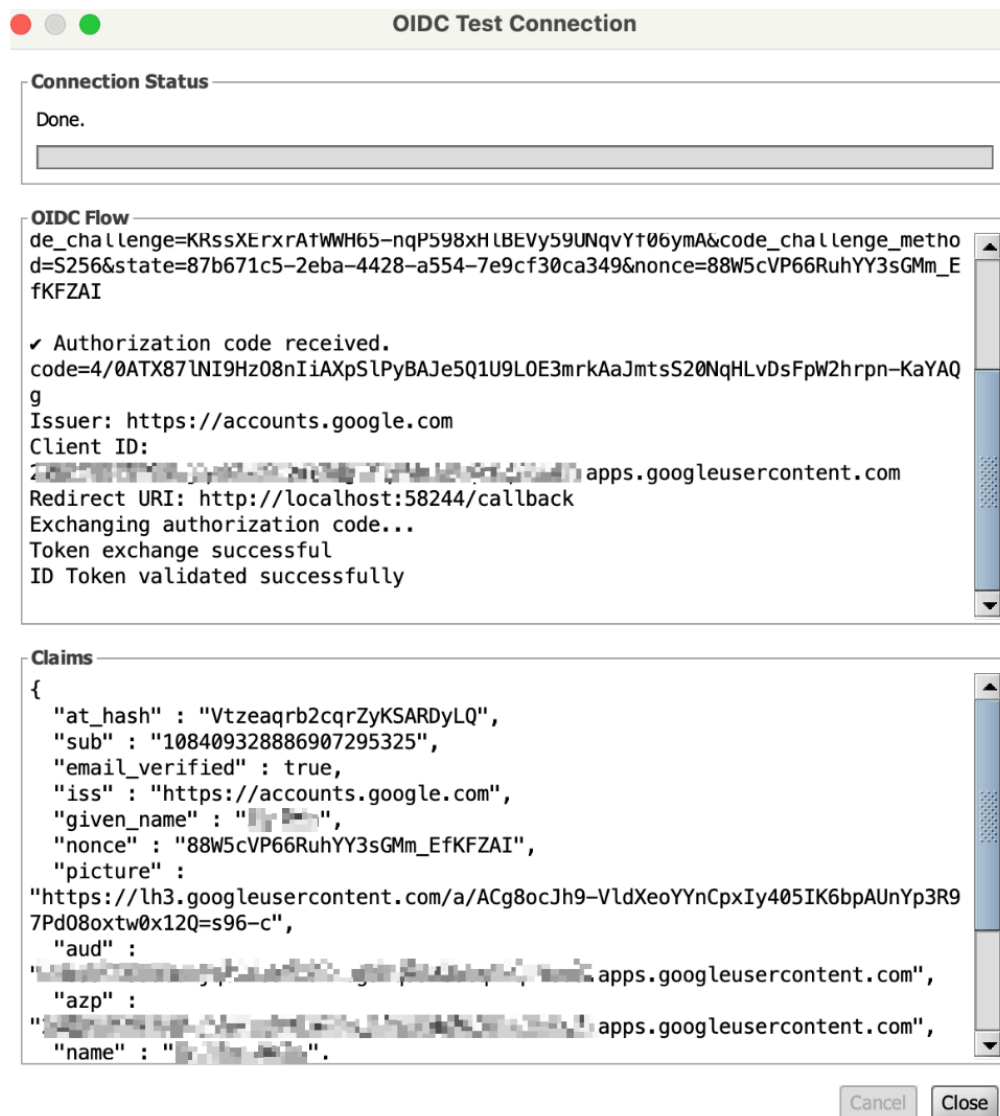
Click “Test Connection” to run a test with your OIDC server



Scopes:

Test Connection

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

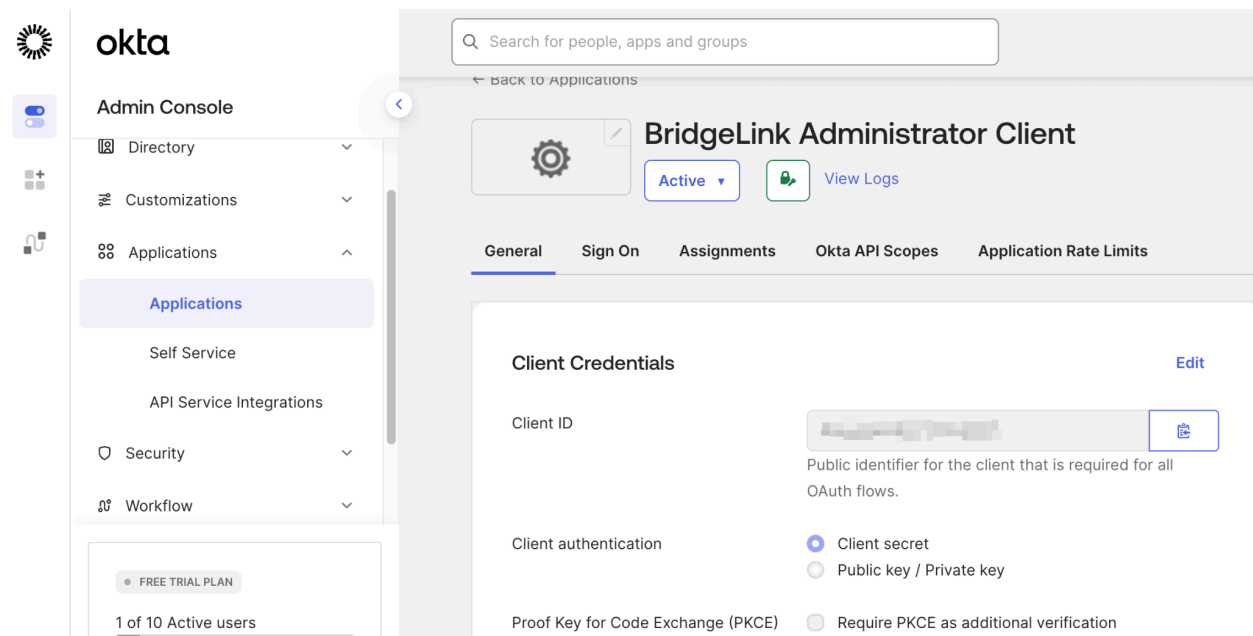


Configure with Okta

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.

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.

http://localhost:58244/callback

X

http://localhost:58245/callback

X

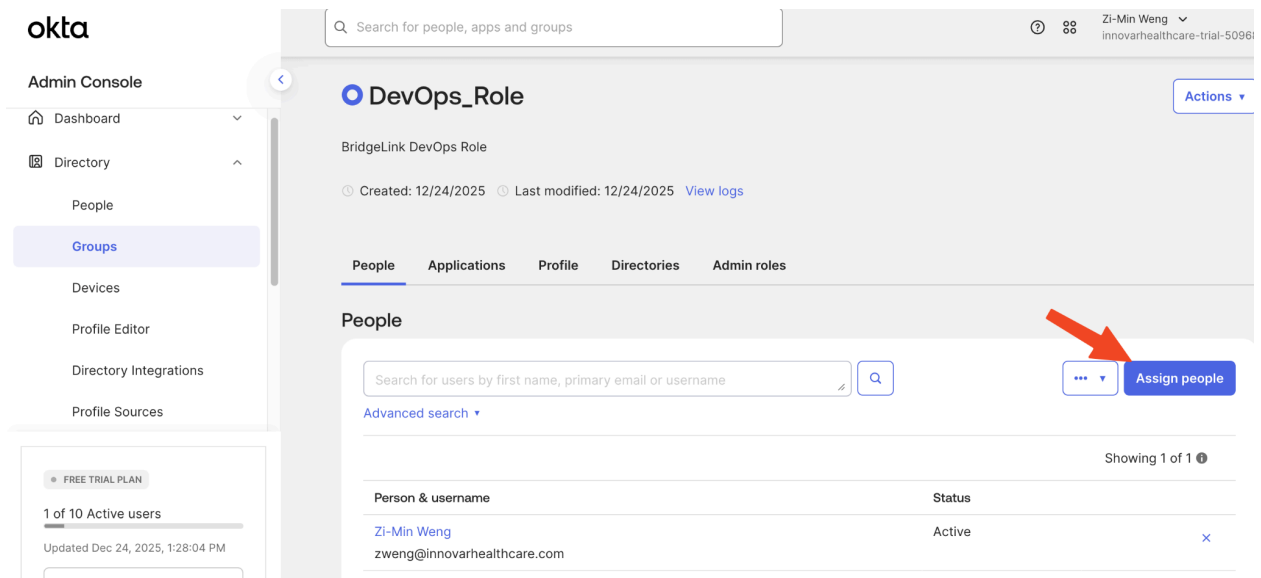
http://localhost:58246/callback

X

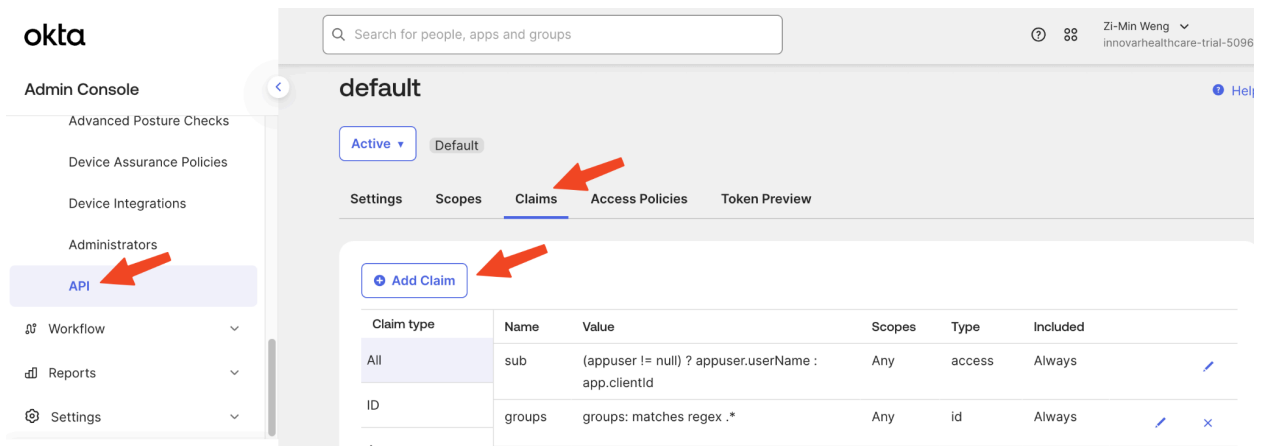
+ Add URI

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.

Edit Claim

Name

Include in token type

Value type

Filter ⓘ Only include groups that meet the following condition.

Disable claim ☐ Disable claim

Include in ☒ Any scope ☐ The following scopes:

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.

Settings

Server Administrator Tags Configuration Map Database Tasks Resources Certificate Manager Access Control Data Pruner Version History **OIDC**

Enable OIDC

Enable: ☒ Yes ☐ No

OIDC Settings

Issuer:

Client ID:


Client Secret:

Redirect URIs:

Test Connection

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

Scopes:



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

OIDC Test Connection

Connection Status

Done.

OIDC Flow

Fcallback&scope=openid+profile+email&code_challenge=bwBY532WgjssraqB65XyKEgRT

✓ Authorization code received.

code=i3NHak9UIpBrJwTnaNk7p9CPvQoece5diGHPY1QkTws

Issuer: https://trial-~~XXXXXXXXXX~~.okta.com/oauth2/default

Client ID: ~~XXXXXXXXXX~~

Redirect URI: http://localhost:58244/callback

Exchanging authorization code...

Token exchange successful

ID Token validated successfully

Claims

{
"at_hash" : "F7wt3rFy039jAg40TqH0sg",
"sub" : "00uylwy1etopRHB7J697",
"ver" : 1,
"amr" : ["mfa", "otp", "pwd", "okta_verify"],
"iss" : "https://trial-~~XXXXXXXXXX~~.okta.com/oauth2/default",
"groups" : ["Everyone", "DevOps_Role"],
"preferred_username" : "~~XXXXXXXXXX~~",
"nonce" : "K8S6Dxyx4VX342ZhUdX2PXSo2tA",
"aud" : "0oaylxjmn0APY0YvE697",
"idp" : "00oylwy1b1WqAwM7Z697",
"auth_time" : 1766603734,
"name" : "~~XXXXXXXXXX~~".
}

Cancel

Close

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.

- Access Control

Exclusive Mode: ☒ Only allow OIDC login

Emergency Fallback: ☒ Allow Emergency Admin fallback

Emergency Admin Username: -- Select --

Service Accounts (API): -- Select --

Service Account Users:

admin
tester
jane.doe@innovarhealthcare.com

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>).

- Access Control

Exclusive Mode: ☒ Only allow OIDC login

Emergency Fallback: ☒ Allow Emergency Admin fallback

Emergency Admin Username: admin

Service Accounts (API): ☒ Enable API Basic for Service Accounts

Service Account Users:

-- Select --

-- Select --

admin

tester

jane.doe@innovarhealthcare.com

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.

User Provisioning

Auto Provision Users: ☒ Automatically create user if missing

Default Role: DevOps_Role ▼

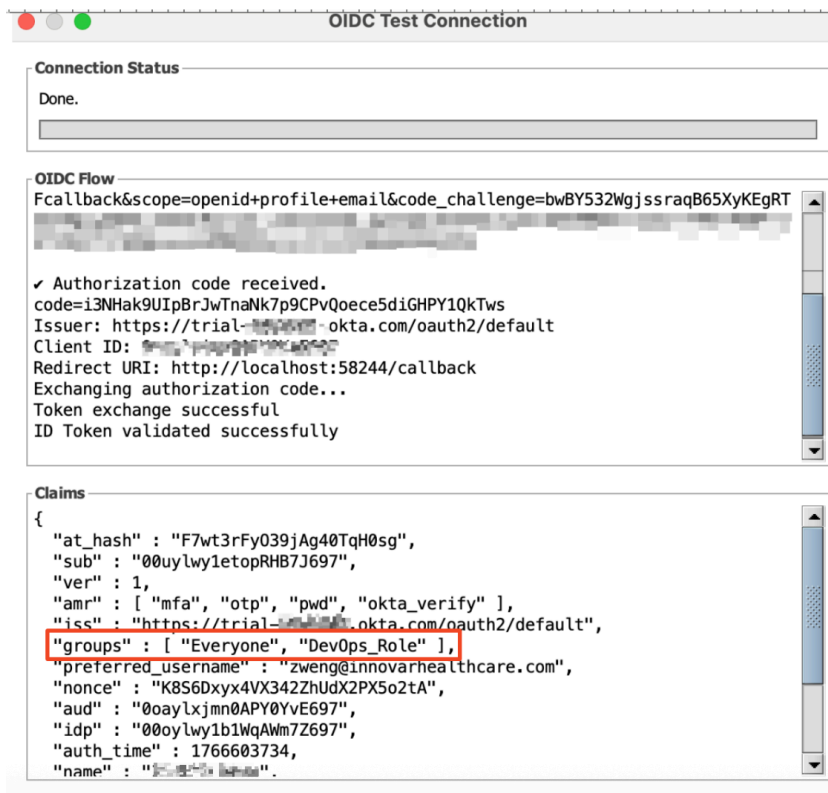
Use roles from token: ☒ Read roles from token claims

Role source (claim): ☒ Groups ☐ Roles ☐ Custom:

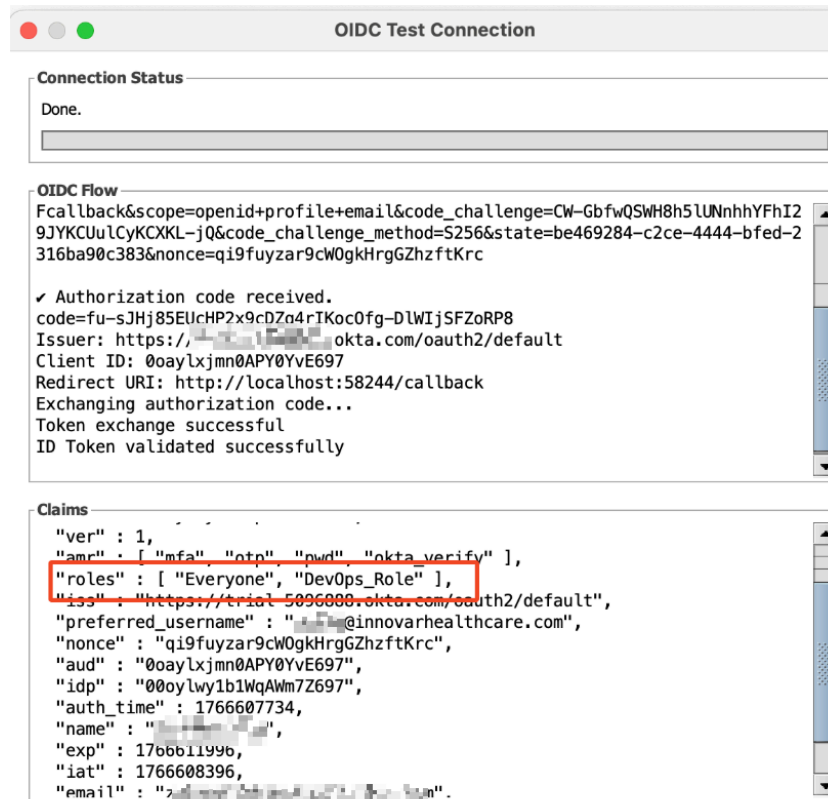
Role source from OIDC claims

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

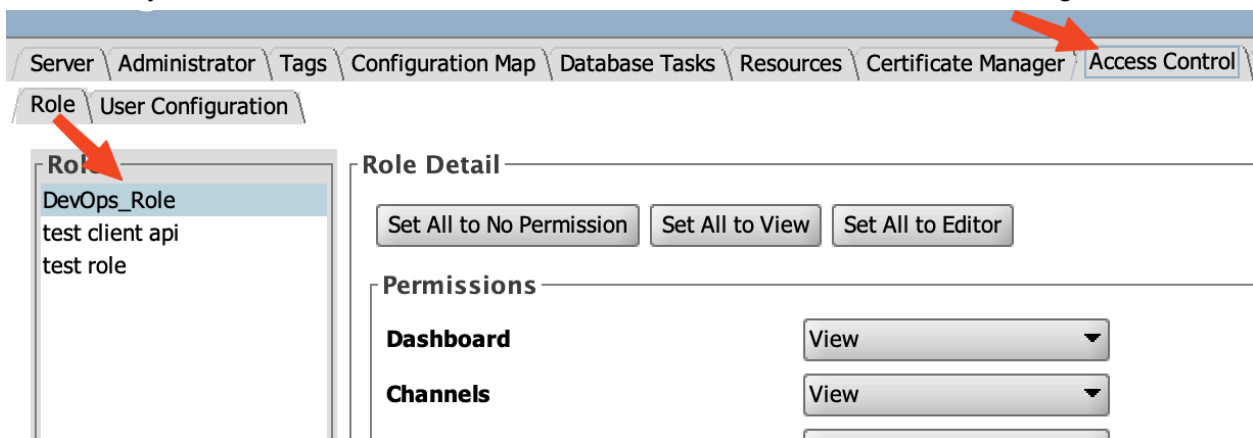
```
{
  "selfdefinedgroup": {
    "name": "DevOps_Role"
  }
}
```

Custom Role source claim:

Use roles from token: ☒ Read roles from token claims

Role source (claim): ☐ Groups ☐ Roles ☒ Custom:

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!