OIDC Plugin for BridgeLink

User Manual

Table of Contents

1 Introduction

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

2 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

3 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.

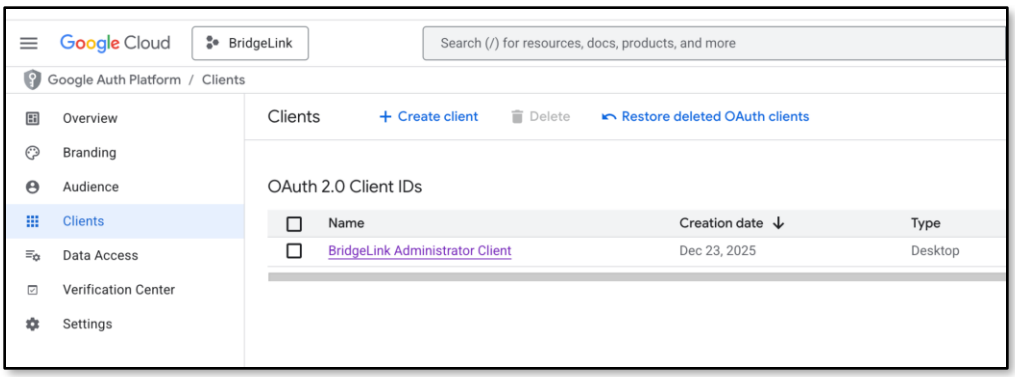

Figure 1: *Google Cloud Platform OAuth 2.0 Client IDs*

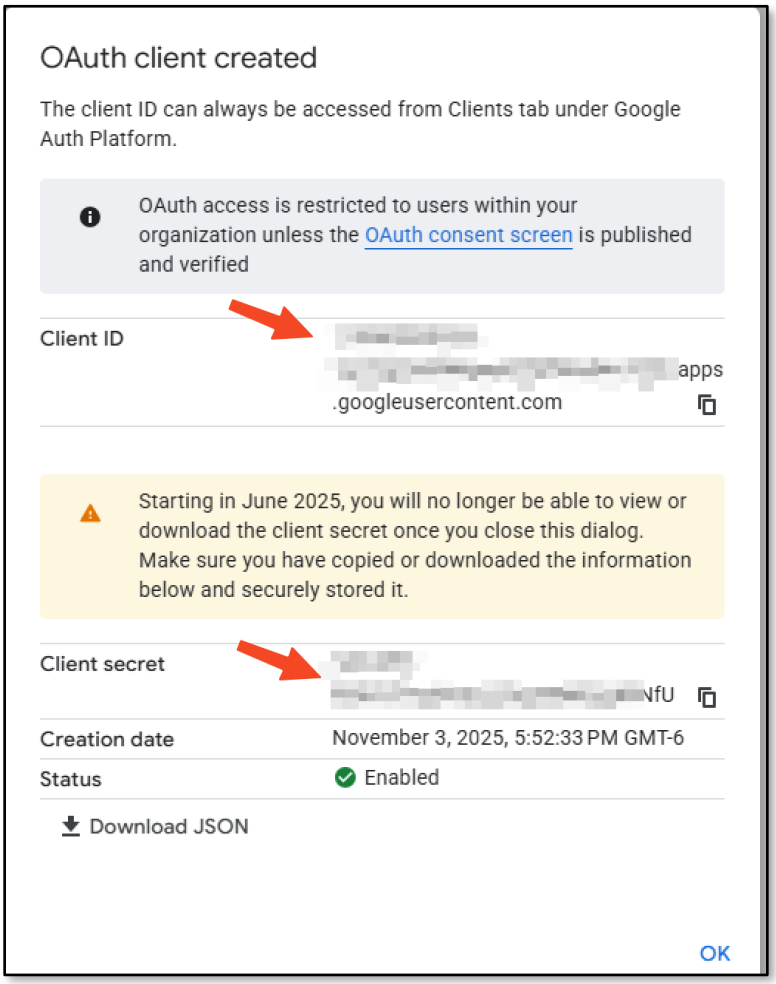

Figure 2: *OAuth client created dialog showing Client ID and Client Secret*

3.1 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.

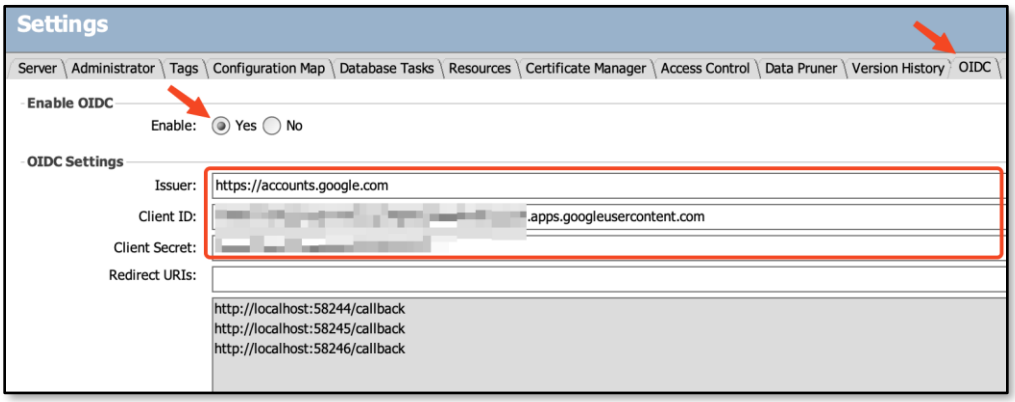

Figure 3: *BridgeLink OIDC Settings configured for Google*

3.2 Test Connection

Click "Test Connection" to run a test with your OIDC server.

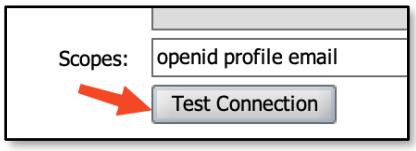

Figure 4: *Test Connection button with scopes*

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

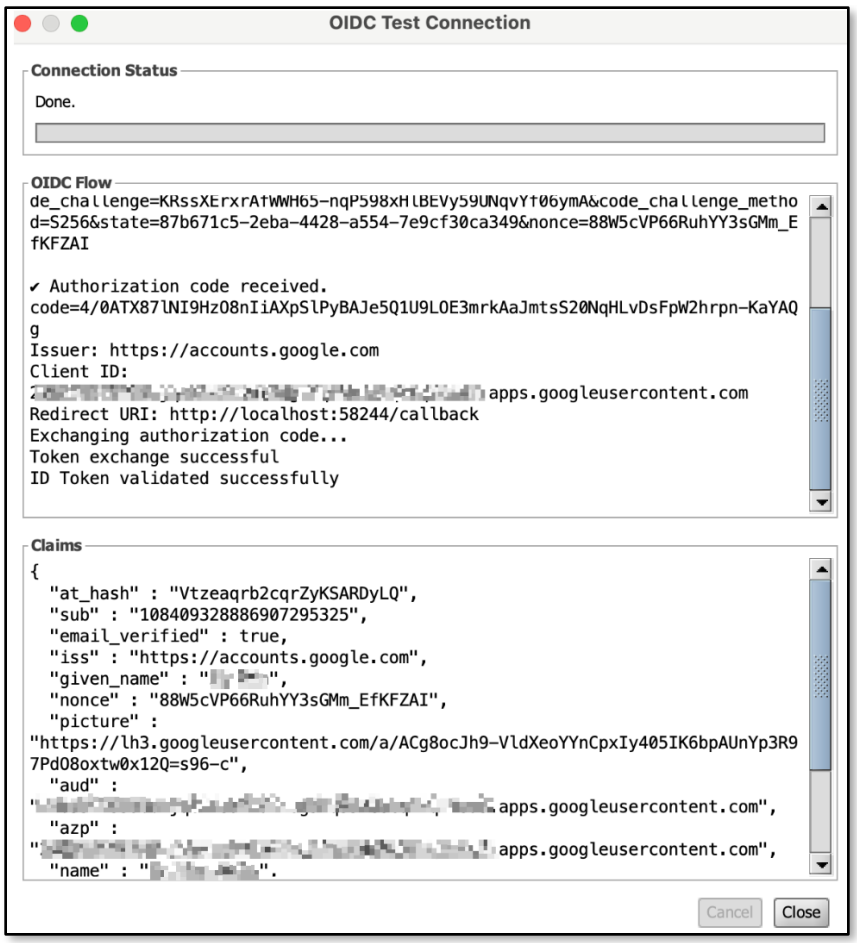

Figure 5: *OIDC Test Connection results showing claims from Google*

4 Configure with Okta

Prerequisite

Please create an App Integration in your Okta account.

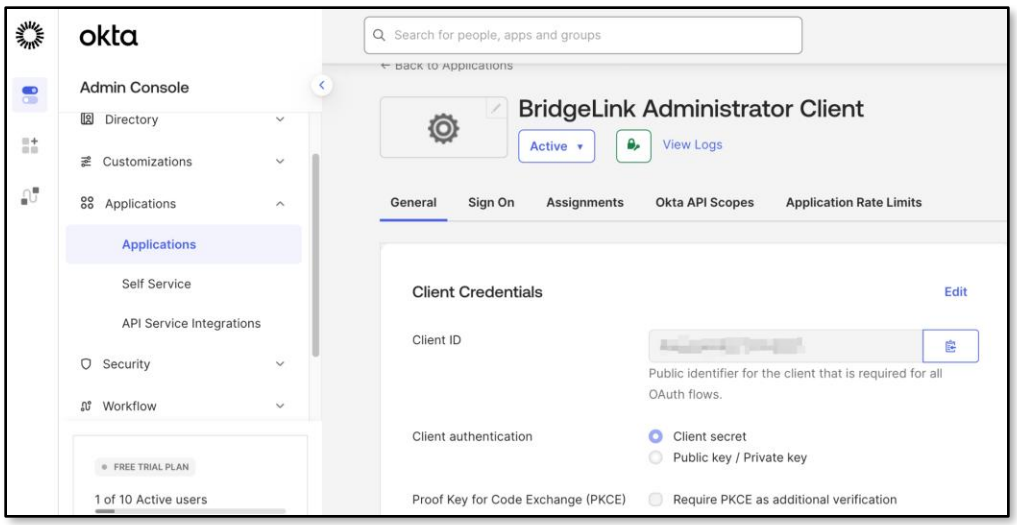

Figure 6: *Okta Admin Console showing BridgeLink Administrator Client*

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

Figure 7: *Okta Sign-in redirect URIs configuration*

Navigate to **Okta > Directory > Groups > "Add group"**, and add user to the group.

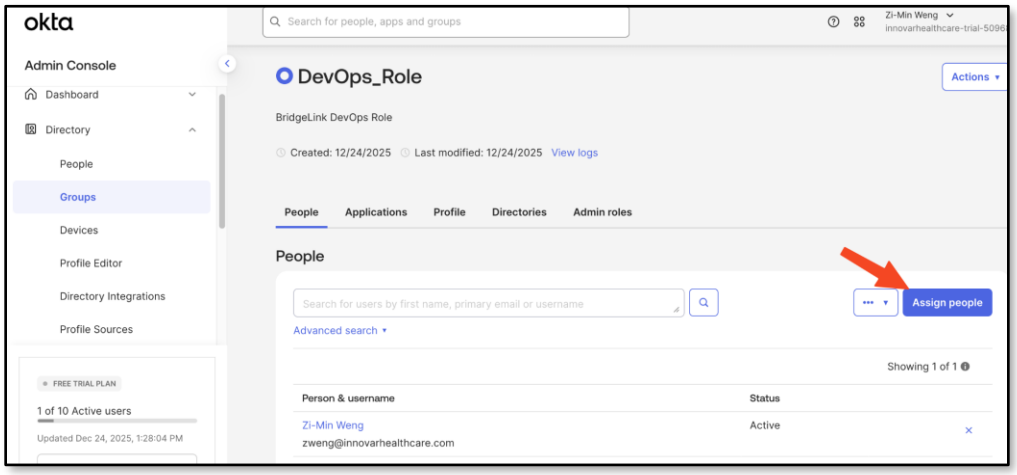

Figure 8: *Okta DevOps_Role group with assigned people*

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.

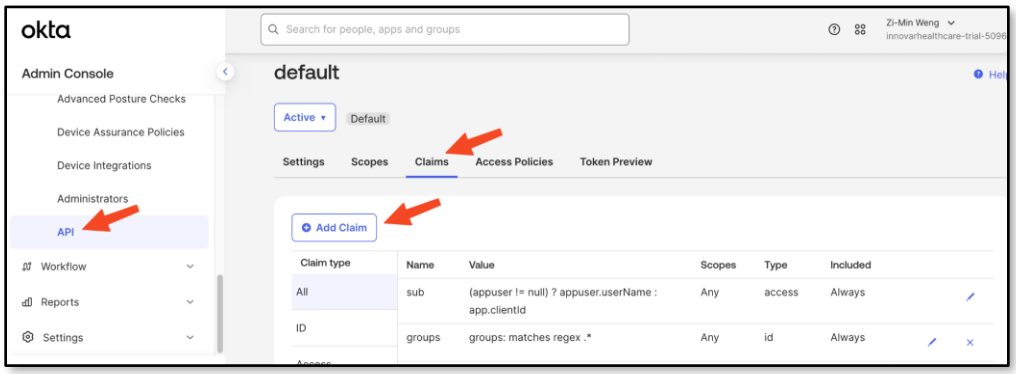

Figure 9: *Okta API Claims configuration*

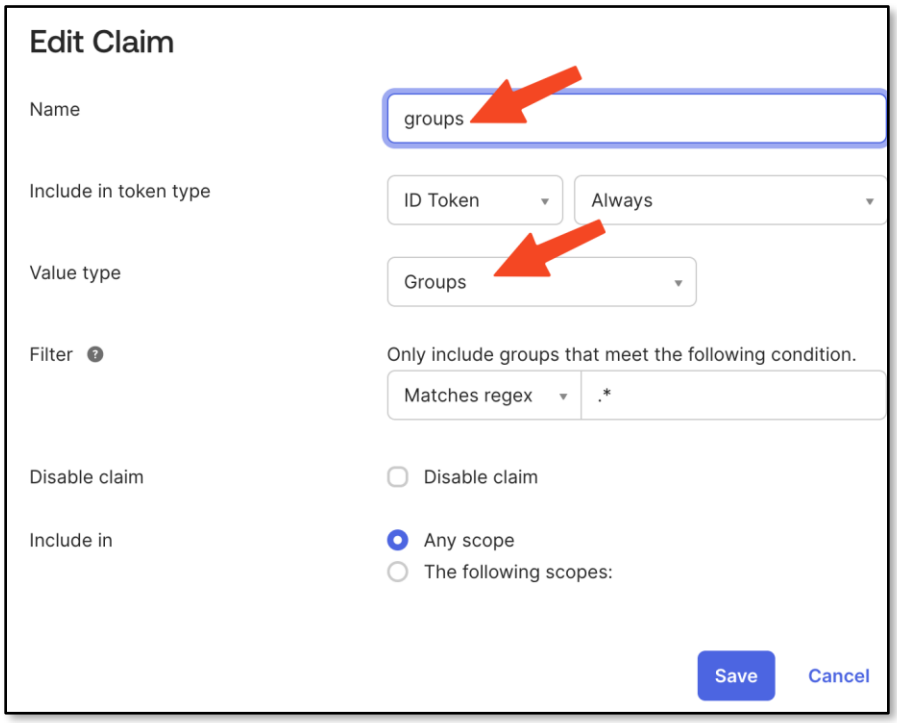

Figure 10: *Okta Edit Claim dialog for groups*

4.1 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.

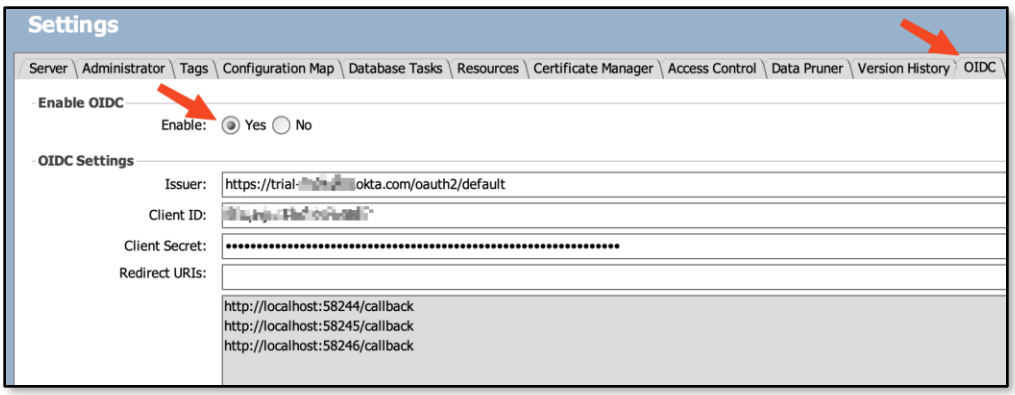

Figure 11: *BridgeLink OIDC Settings configured for Okta*

4.2 Test Connection

Click "Test Connection" to run a test with your OIDC server.

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

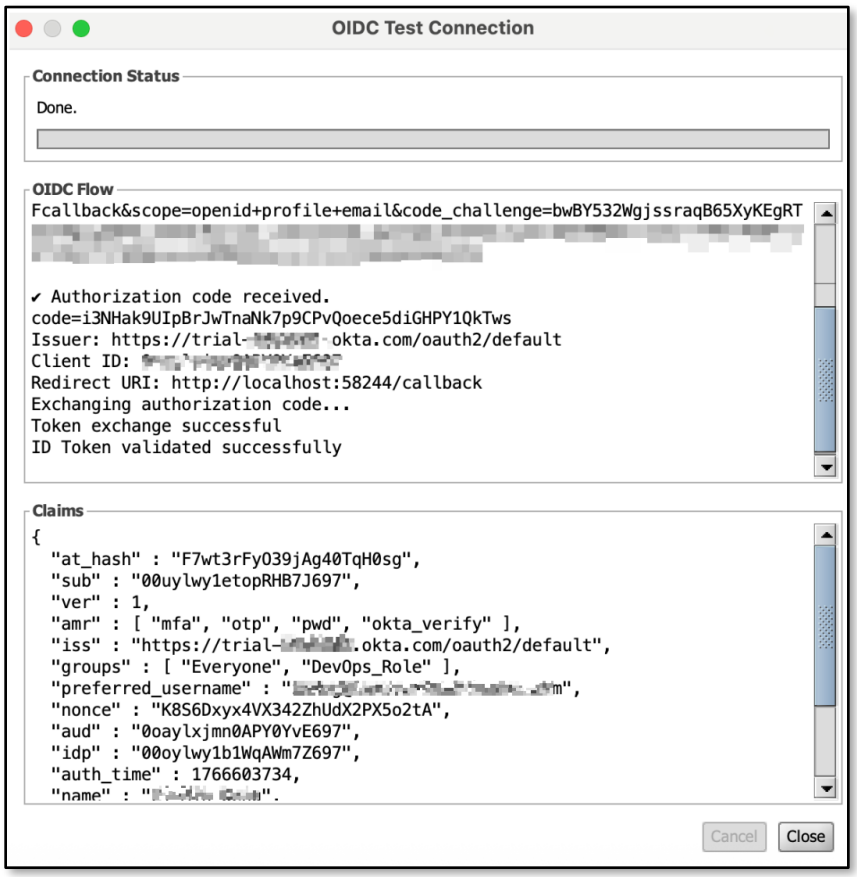

Figure 12: *OIDC Test Connection results showing claims from Okta*

5 After Issuer Configuration

5.1 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.

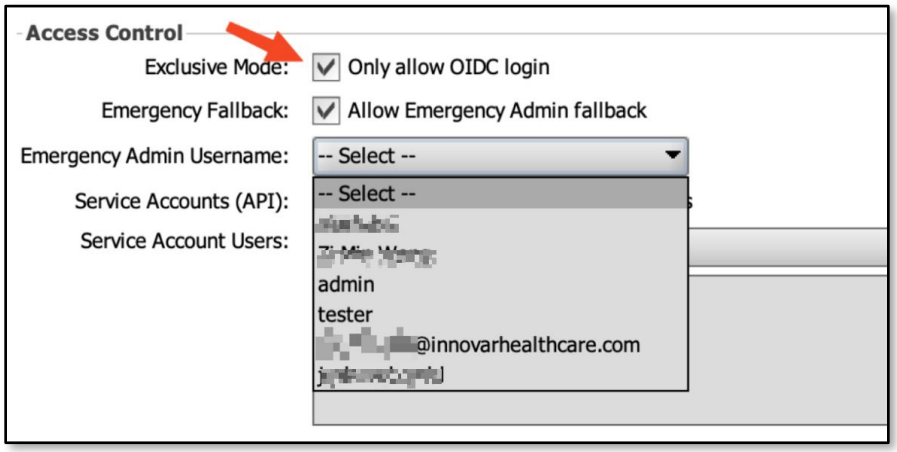

Figure 13: *Access Control settings with Only Allow OIDC Login enabled*

5.2 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).

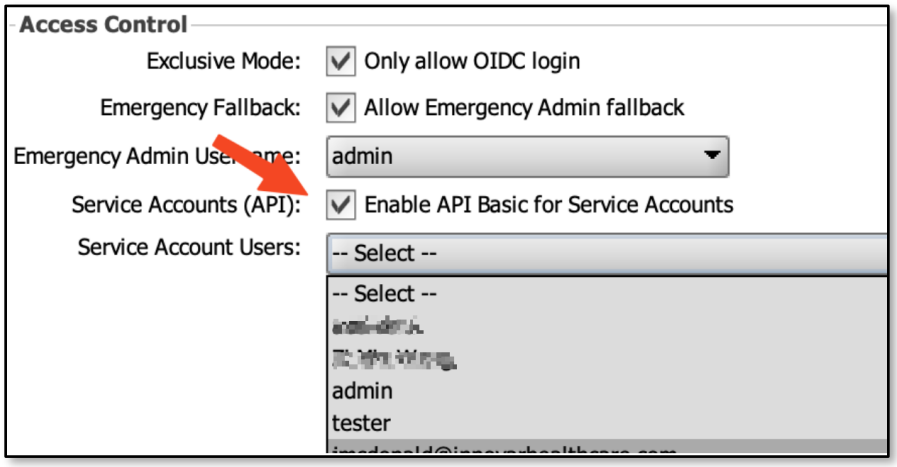

Figure 14: *Service Accounts API configuration*

5.3 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.

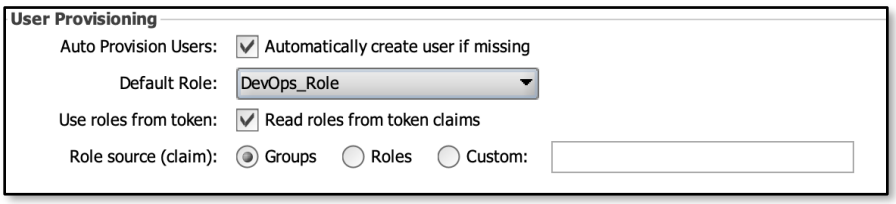

Figure 15: *User Provisioning settings with role source from claims*

Select the role source based on the OIDC claim response. For example, select "Groups" if you see the claims like the following:

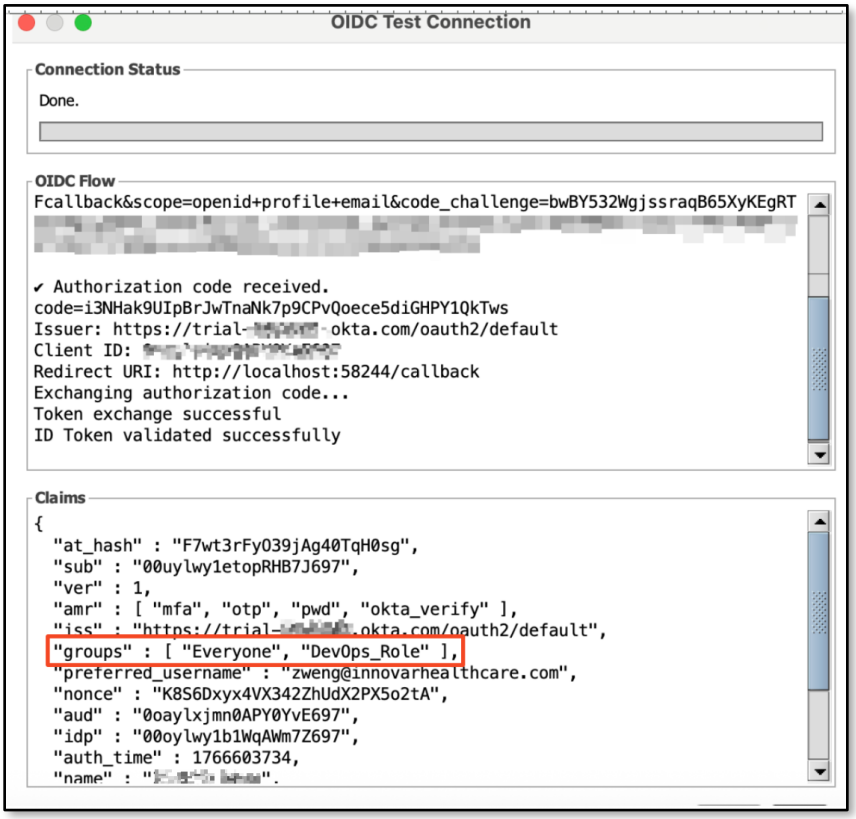

Figure 16: *Claims response showing groups array*

Select "Roles" if you see the claim like the following:

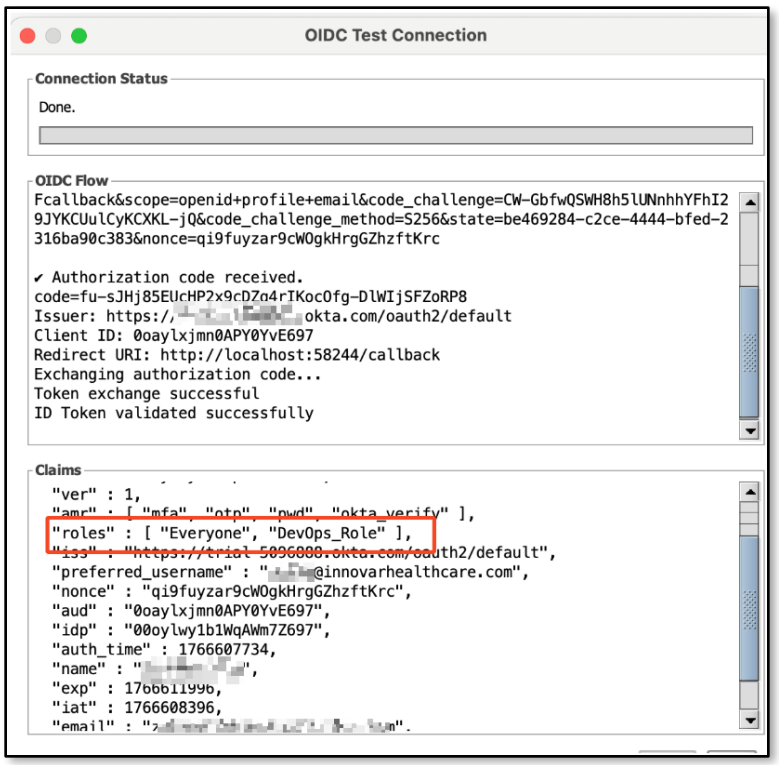

Figure 17: *Claims response showing roles array*

Select "Custom" and enter the custom pattern in the claim. For example, with a claim response containing a nested object:

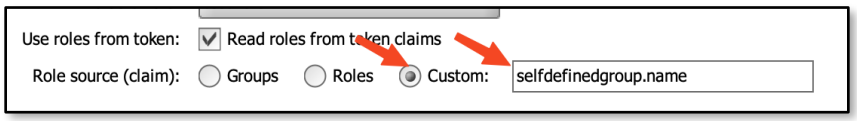

Figure 18: *Custom role source claim configuration*

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

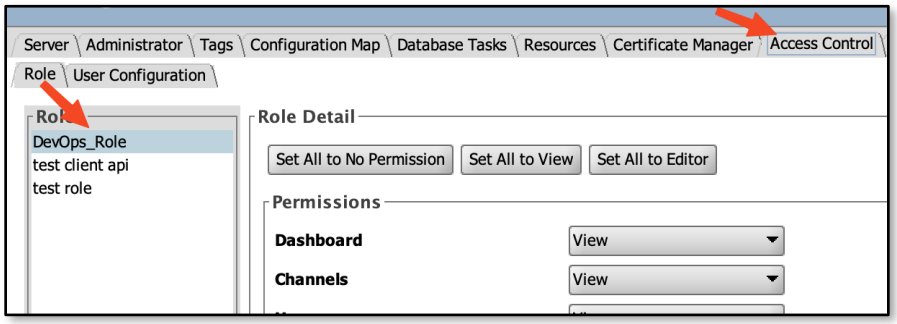

Figure 19: *Access Control role configuration matching the OIDC role name*

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.

6 Document Control

Revision History:

Version	Date	Author	Description
1.0.0	April 21, 2026	Calvin Redding	Initial branded release for OIDC Plugin

Document Information:

Property	Value
Document Title	OIDC Plugin for BridgeLink: User Manual
Classification	External
Owner	Innovar Healthcare Systems Group