BridgeLink OpenID Connect (OIDC) Plugin: User Guide

For BridgeLink WebAdmin

Table of Contents

About This Guide

The OpenID Connect (OIDC) plugin lets BridgeLink users sign in through an external identity provider, such as Google Auth Platform or Okta, instead of a local BridgeLink password. It centralizes user authentication, lets your identity provider enforce multi-factor authentication and password policy, and can automatically create BridgeLink users and assign their roles based on the claims your identity provider returns at sign-in. This guide is for BridgeLink administrators configuring single sign-on. By the end, you will be able to register BridgeLink as a client application with your identity provider, enable and test OIDC in WebAdmin, control who can bypass OIDC in an emergency, and map identity provider roles to BridgeLink roles.

Requirements

- BridgeLink 26.6.0 or later.
- A valid OIDC plugin license, installed on the **License Manager** tab under **Settings** (see Installation and Activation).
- An OpenID Connect identity provider (IdP) account with administrative access to register a client application. This guide uses Google Auth Platform and Okta as examples. Any standards-compliant OIDC provider works.
- To assign BridgeLink roles automatically from identity provider claims, the Access Control plugin, licensed and configured with role names that match the groups or roles your identity provider returns.

Installation and Activation

1. Sign in to **WebAdmin** as an administrator.
2. In the left navigation, under **ADMINISTRATION**, click **Settings**.
3. Click the **License Manager** tab, then the **Installed Licenses** sub-tab.
4. Click **Install License** and choose the OIDC plugin license file, a `.json` file supplied by Innovar Healthcare.
5. Review the **Install License** dialog, which previews the license's **Customer**, **Products**, **Issued**, **Expires**, and **Server match**, then click **Install**. A confirmation toast reads "License installed."
6. Restart BridgeLink when prompted; a banner reads "License changes will take effect after restarting BridgeLink."
7. Click the **License Status** sub-tab and confirm the **OIDC Authentication** row shows **Active** under **Status**.
8. Click the **OIDC** tab to confirm the plugin is available.

Configuration

Configure with Google Auth Platform

Before you configure BridgeLink, register BridgeLink as a client application in Google Auth Platform.

1. In Google Auth Platform, create an OAuth 2.0 Client ID and select **Desktop** as the application type.
2. Save the **Client ID** and **Client Secret** shown after creation. Google Cloud Platform (GCP) does not let you view the client secret again after you close this dialog.

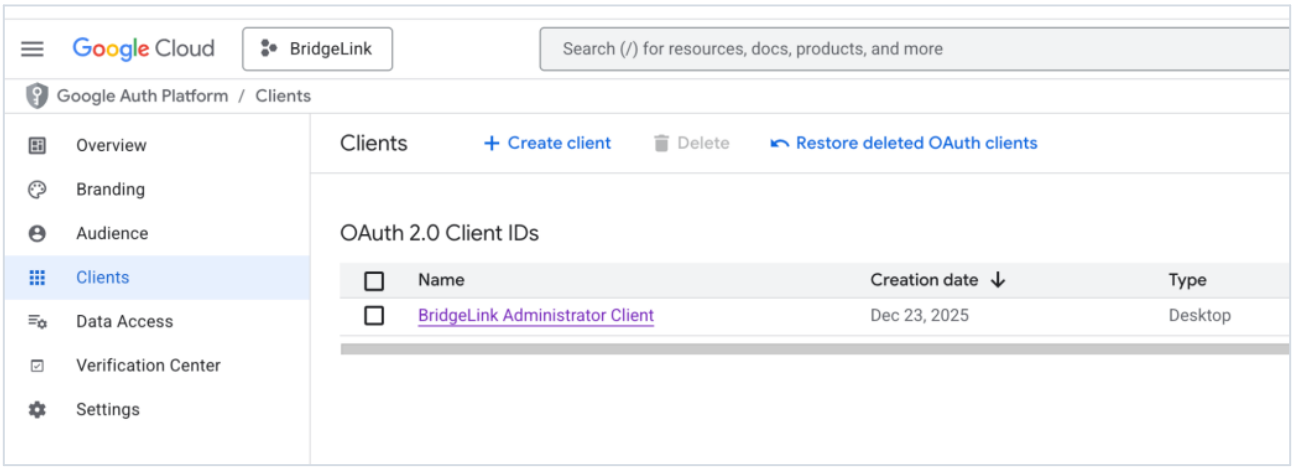

Figure 1: Google Cloud Platform OAuth 2.0 Client IDs

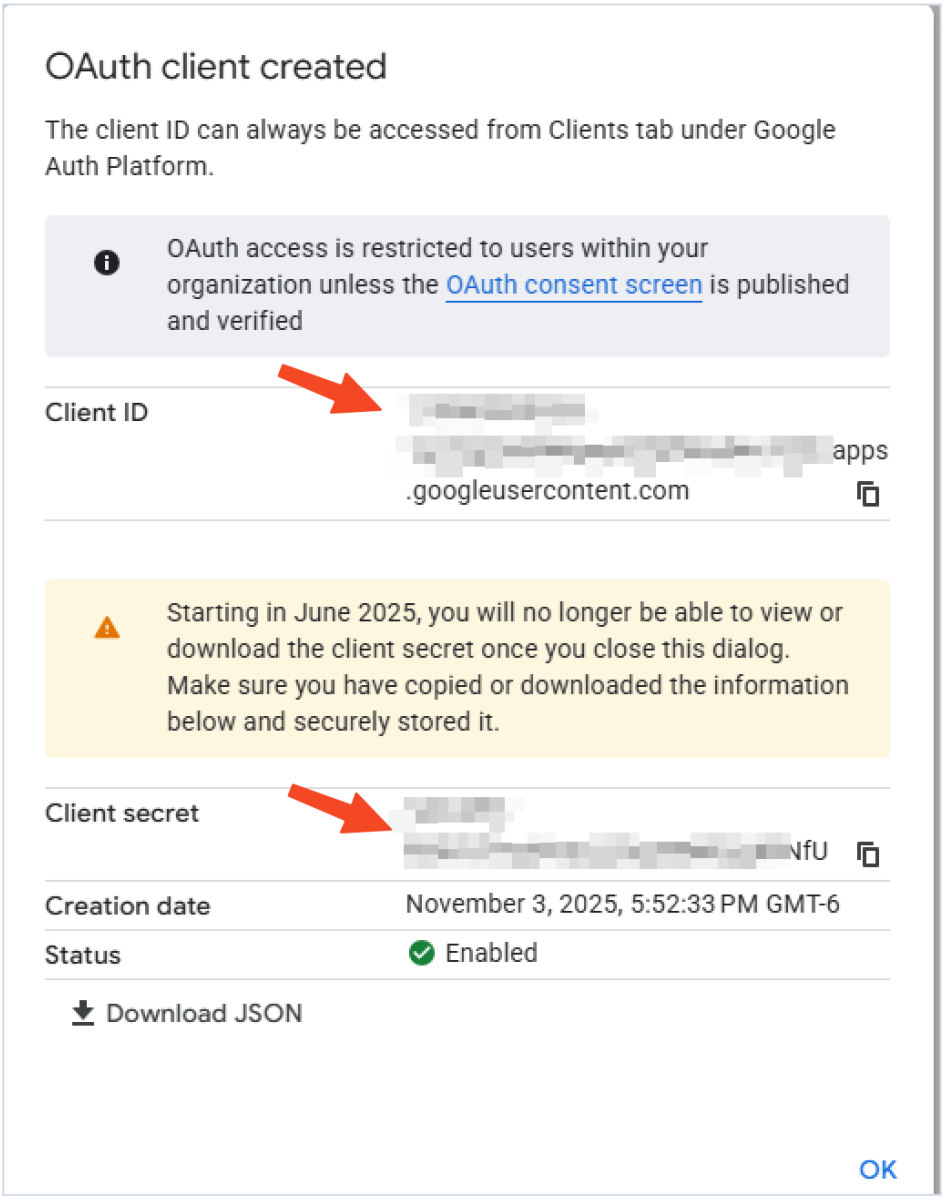

Figure 2: OAuth client created dialog showing Client ID and Client Secret

With the client application registered, configure the OIDC Settings in WebAdmin:

1. In WebAdmin, click **Settings**, then click the **OIDC** tab.
2. Under **Enable OIDC**, set **Enable** to **Yes**.
3. Under **OIDC Settings**, enter `https://accounts.google.com` in **Issuer**.
4. Enter the **Client ID** from Google Auth Platform.
5. Enter the **Client Secret** from Google Auth Platform. Leave this field blank if you registered a public client and want BridgeLink to use PKCE without a secret.
6. Enter a callback URL in the field next to **Redirect URIs** and click **Add**. Repeat to add at least three callback URLs, each using a different local port. BridgeLink tries each configured URL in turn until it finds one it can use, so having several reduces the

chance of a port conflict during sign-in.

7. Enter the OAuth scopes to request in **Scopes**, or keep the default `openid profile email`.
8. Click **Save**.

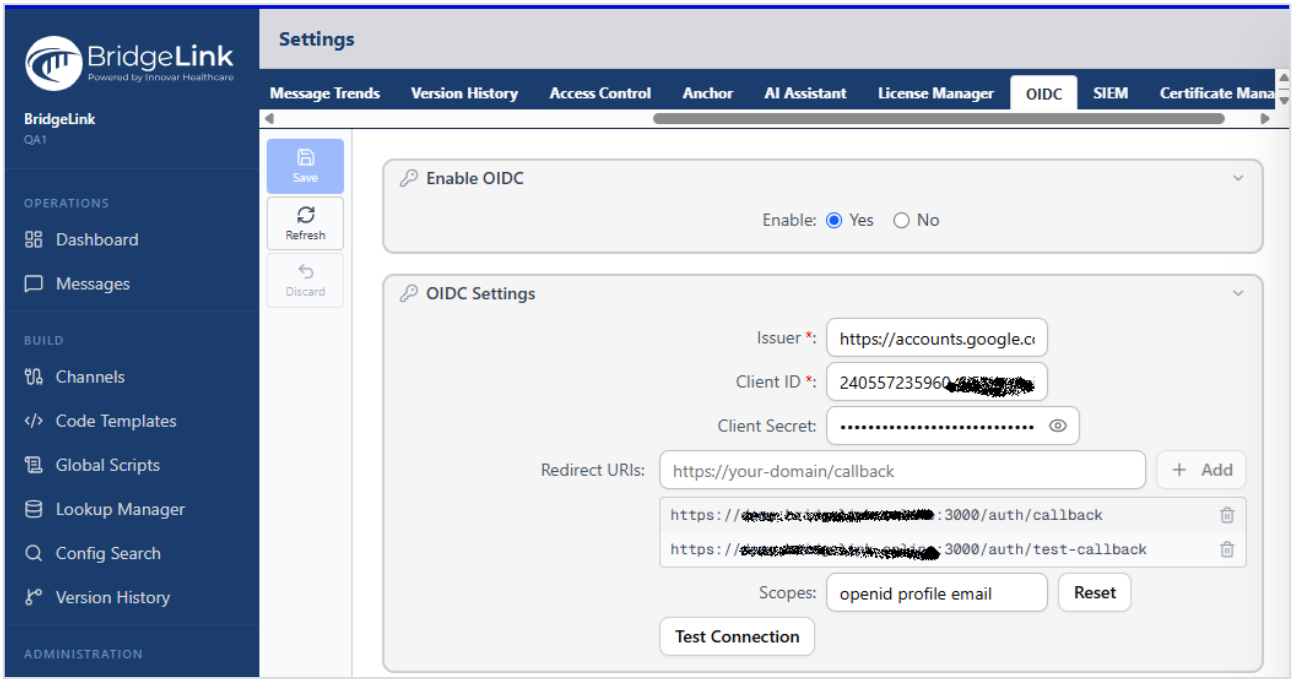

Figure 3: BridgeLink OIDC Settings configured for Google

Setting	What it does	Default
Enable	Turns the OIDC plugin on or off.	No
Issuer	The identity provider's issuer URL, used to discover its OIDC endpoints.	(none)
Client ID	The client identifier registered with your identity provider.	(none)
Client Secret	The client secret registered with your identity provider. Leave blank for a public client using PKCE.	(none)
Redirect URIs	Local callback URLs the sign-in flow can bind to. Add several to avoid port conflicts.	(none)
Scopes	The OAuth scopes requested during sign-in.	`openid profile email`

To confirm the connection works before you rely on it:

1. Click **Test Connection**.
2. Review the **OIDC Flow** section for a successful token exchange.
3. Review the **Claims** section for the claims your identity provider returned.

4. Click **Close**.

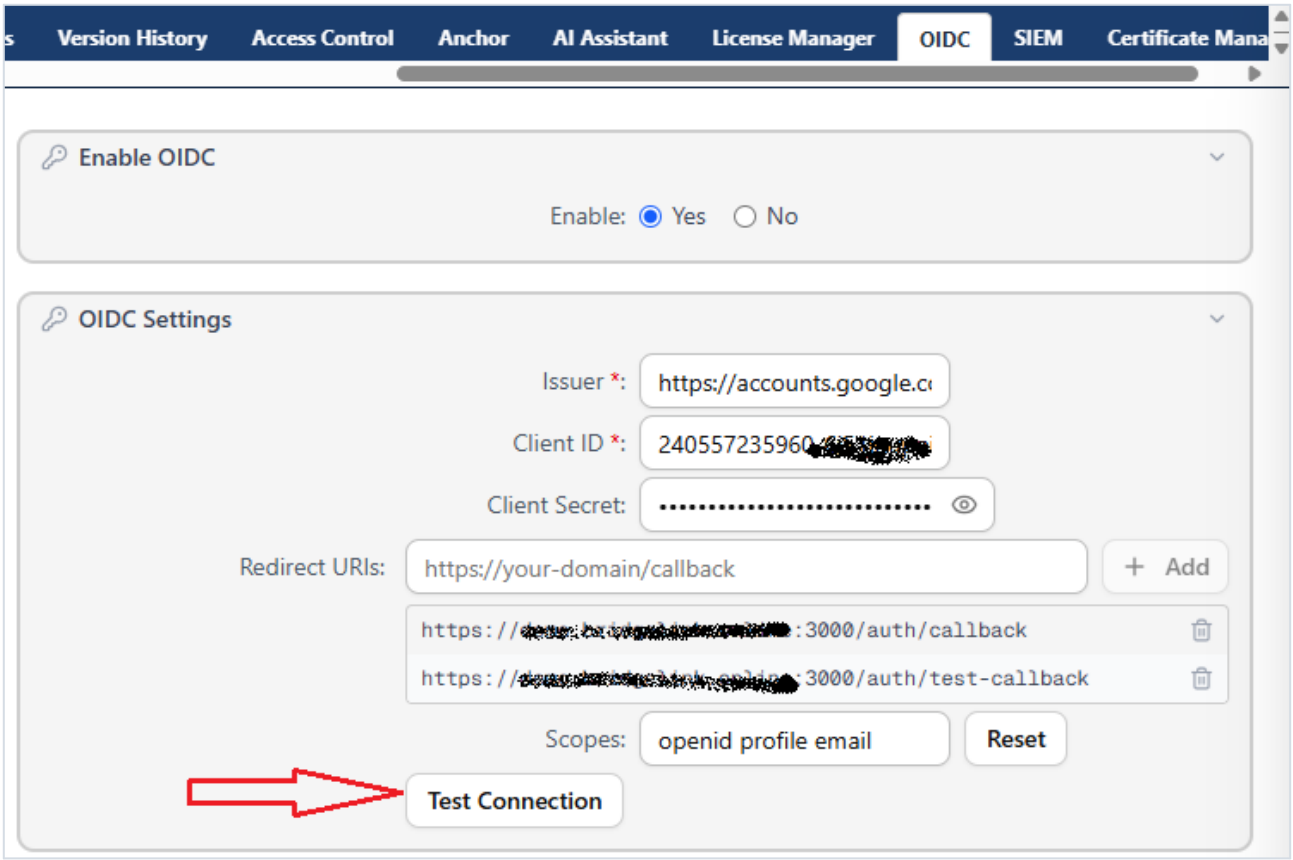

Figure 4: Test Connection button with scopes

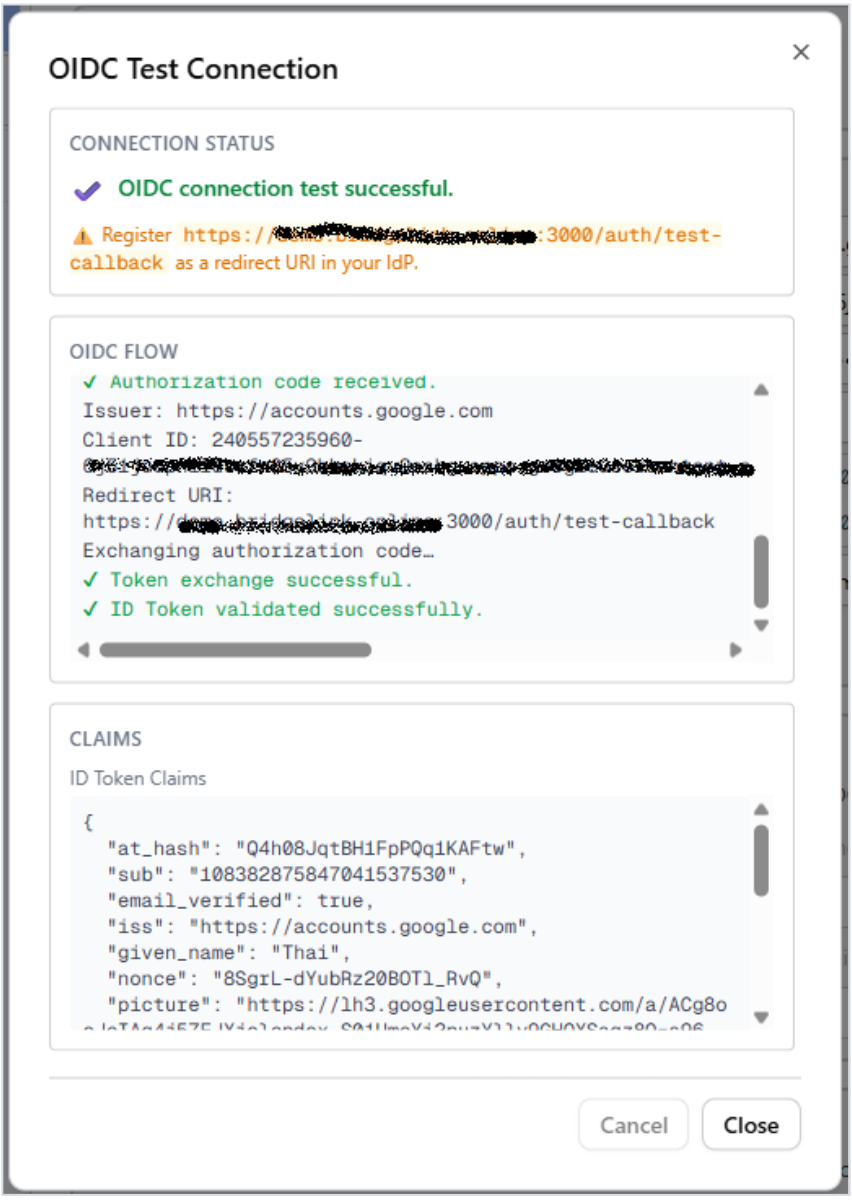

Figure 5: OIDC Test Connection results showing claims from Google

If **Test Connection** shows a warning about a callback URL, register that exact URL as a redirect URI in Google Auth Platform and try again.

Configure with Okta

Before you configure BridgeLink, create an App Integration in your Okta account.

1. In Okta, create an App Integration for BridgeLink.
2. Under **Sign-in redirect URIs**, add at least three callback URLs, each using a different local port. Use the same URLs you plan to enter in BridgeLink's **Redirect URIs**.
3. Under **Okta > Directory > Groups**, click **Add group**, then add the users who need BridgeLink access to the group.

4. Under **Okta > Security > API**, select your authorization server, click the **Claims** tab, then click **Add Claim**.
5. In the claim editor, enter `groups` as the name, select **ID Token** as the token type, and select **Groups** as the value type. Save the claim.

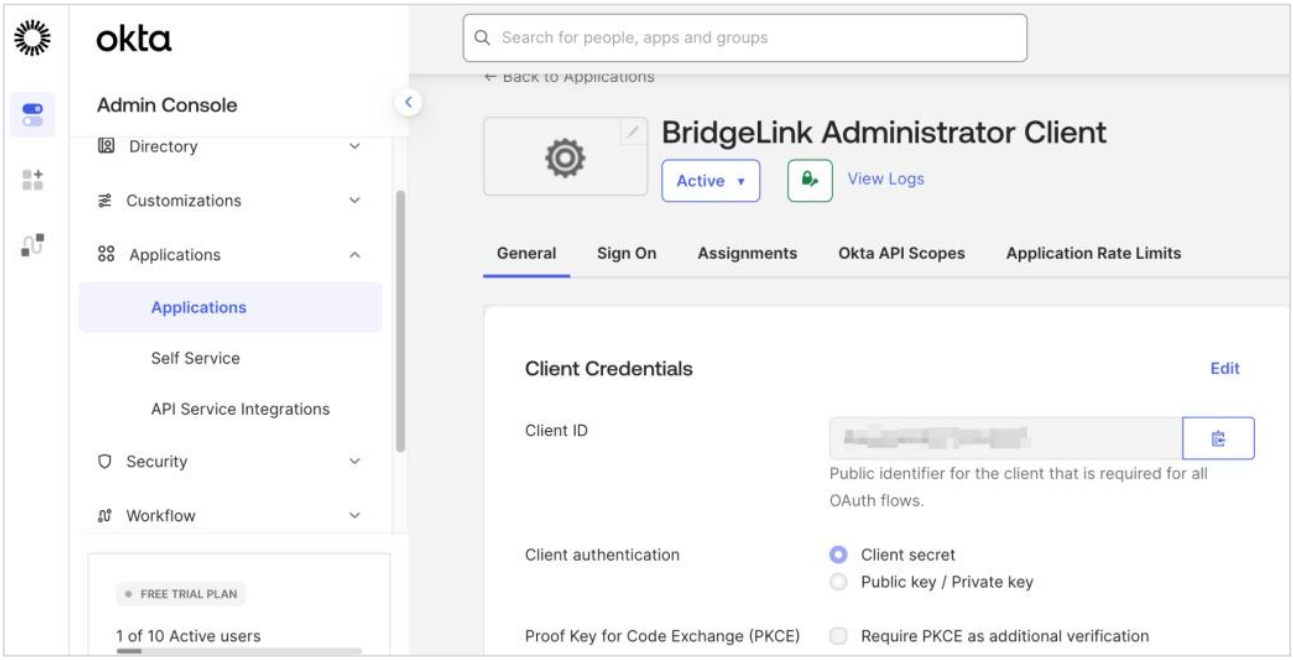

Figure 6: Okta Admin Console showing BridgeLink Administrator Client

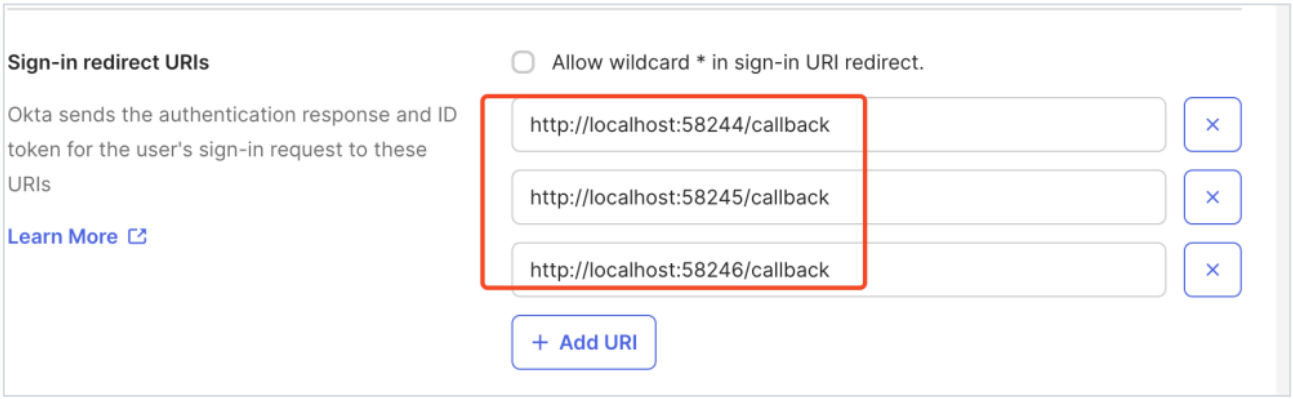

Figure 7: Okta Sign-in redirect URIs configuration

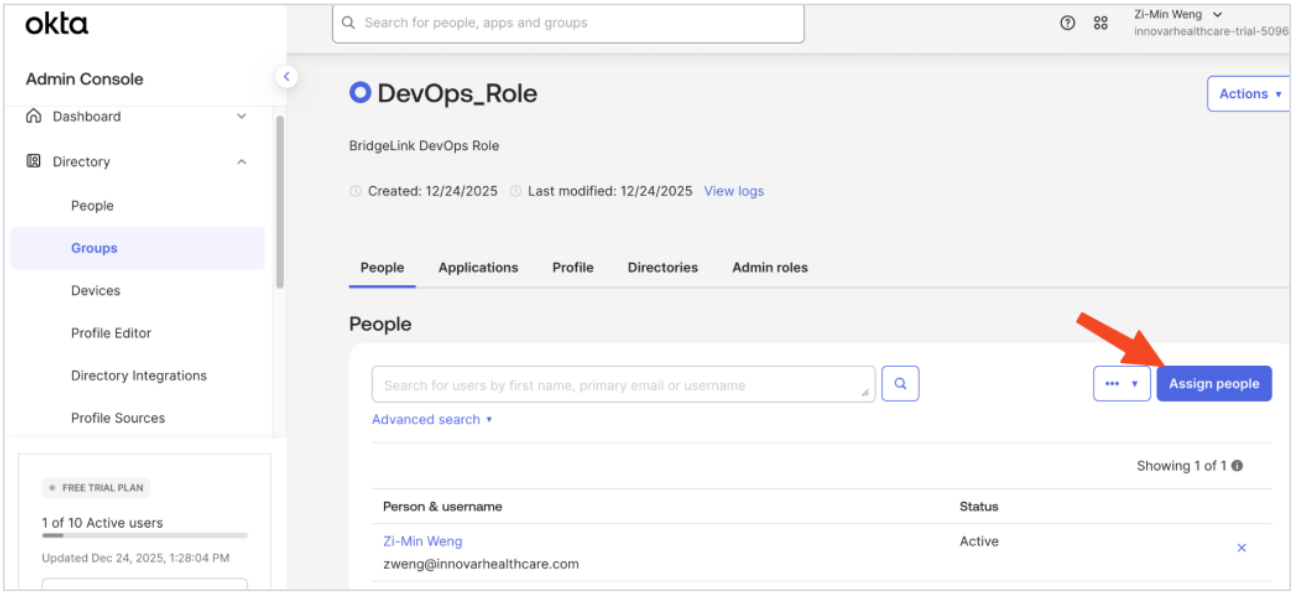

Figure 8: Okta group with assigned people

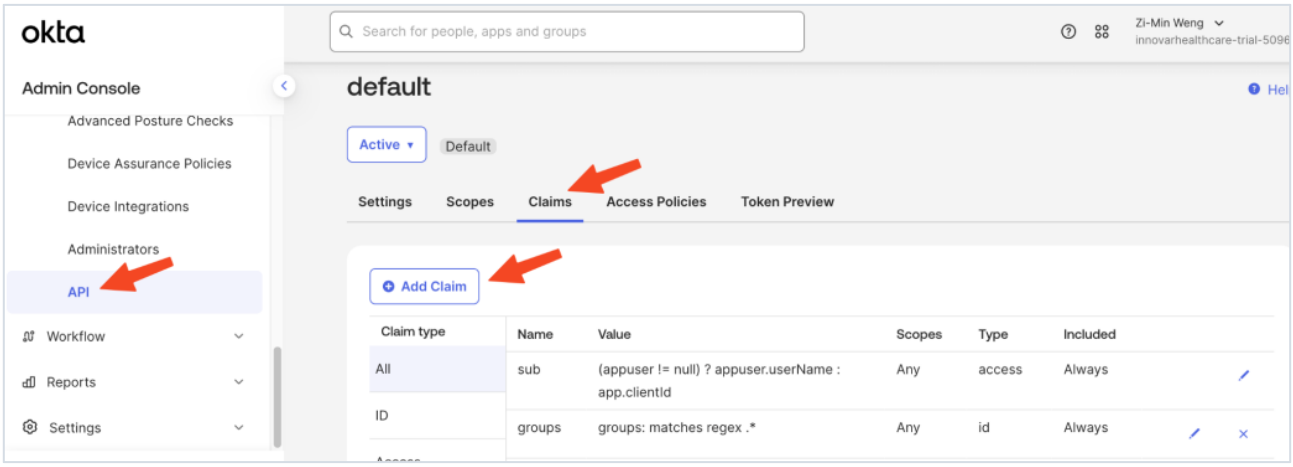

Figure 9: Okta API Claims configuration

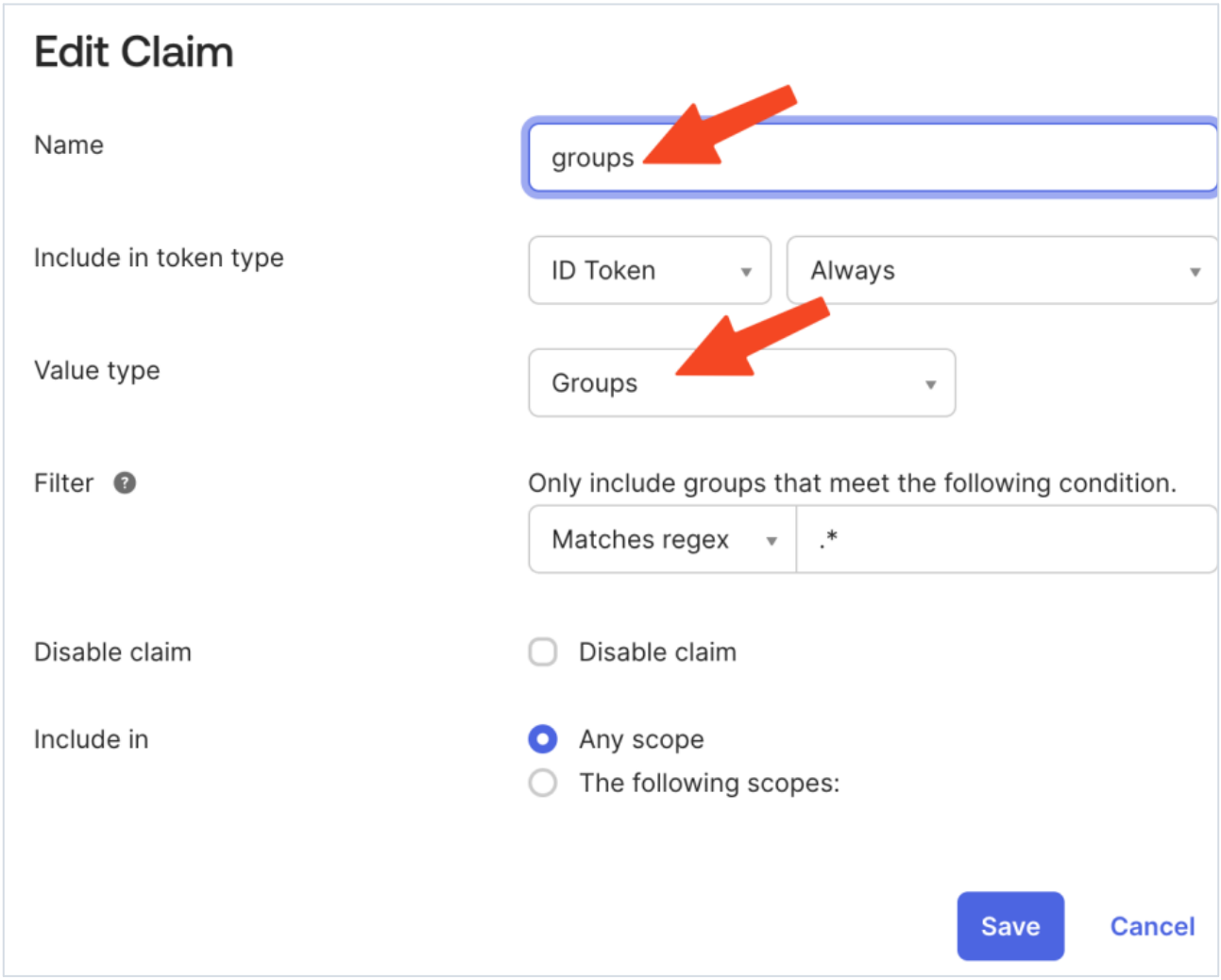

Figure 10: Okta Edit Claim dialog for groups

With the App Integration registered, configure the OIDC Settings in WebAdmin. The fields are the same as described under **Configure with Google Auth Platform**; only the values differ.

1. In WebAdmin, click **Settings**, then click the **OIDC** tab.
2. Under **Enable OIDC**, set **Enable** to **Yes**.
3. Under **OIDC Settings**, enter `https://{yourOktaDomain}/oauth2/default` in **Issuer**, replacing `{yourOktaDomain}` with your Okta domain.
4. Enter the **Client ID** and **Client Secret** from your Okta App Integration.
5. Add the same callback URLs you configured in Okta's **Sign-in redirect URIs** to **Redirect URIs**.
6. Click **Save**.

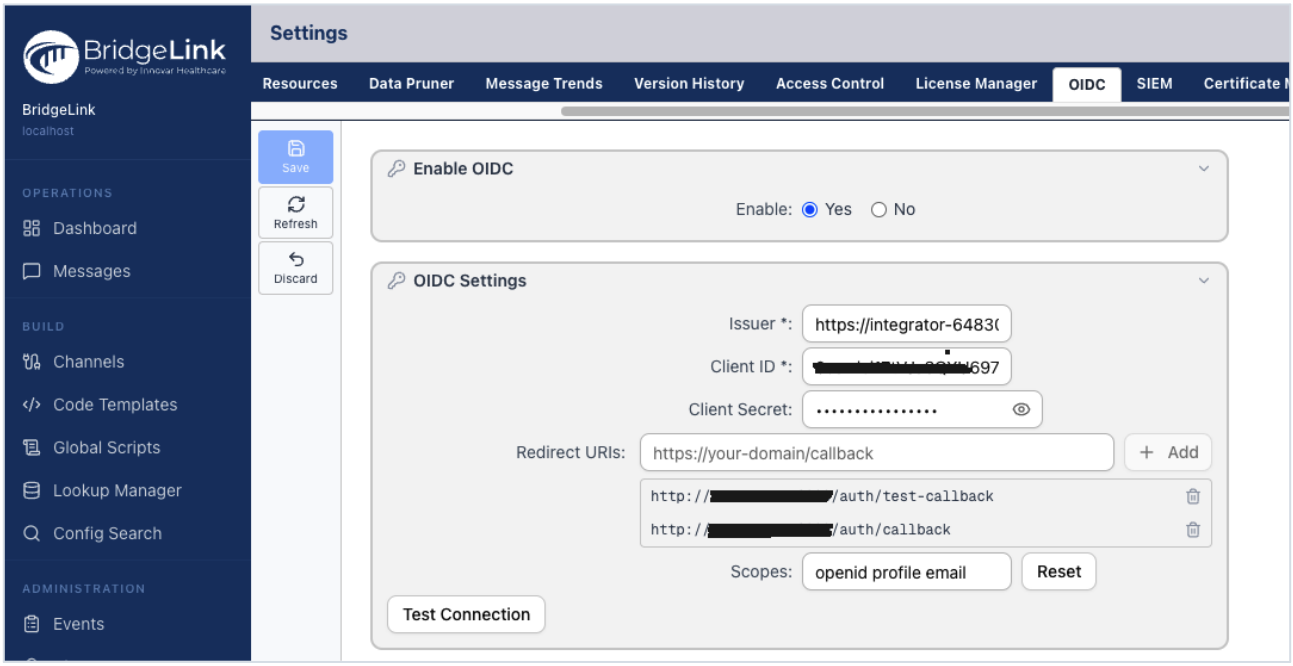

Figure 11: BridgeLink OIDC Settings configured for Okta

To confirm the connection works, click **Test Connection** and review the **OIDC Flow** and **Claims** sections, the same way as described under **Configure with Google Auth Platform**.

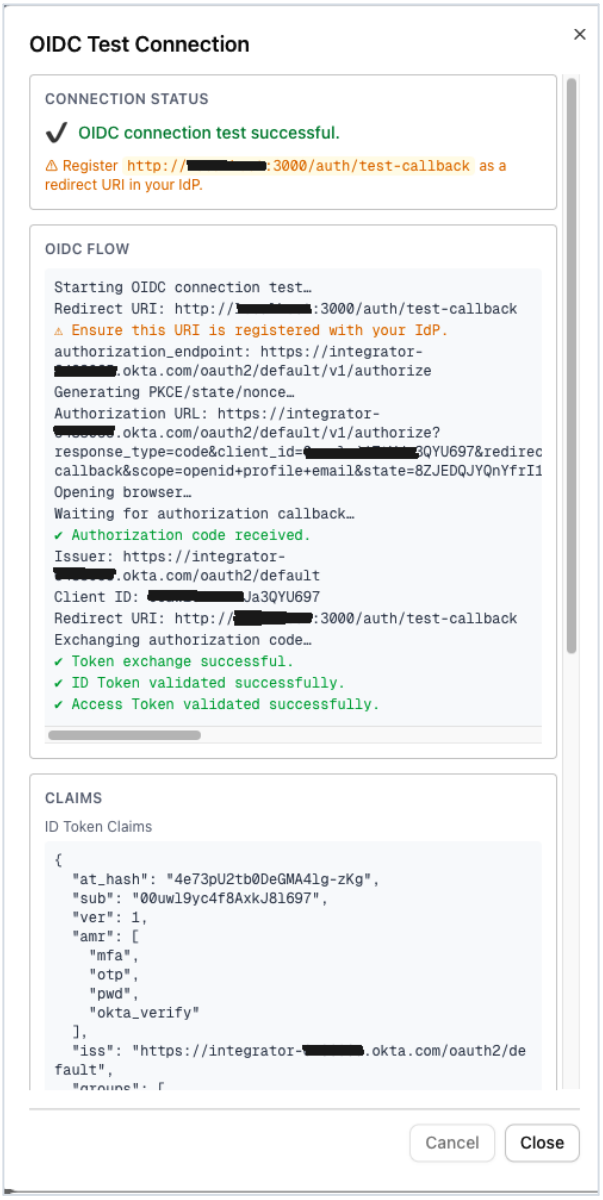

Figure 12: OIDC Test Connection results showing claims from Okta

If **Test Connection** shows a warning about a callback URL, register that exact URL as a redirect URI in your Okta App Integration and try again.

Access Control

After your issuer is configured and tested, use **Access Control** to decide whether OIDC is required for every user and who can bypass it.

1. In WebAdmin, click **Settings**, then click the **OIDC** tab, then scroll to **Access Control**.
2. Before you require OIDC login, check **Allow Emergency Admin fallback** under **Emergency Fallback**, then choose an account from **Emergency Admin Username**. This account can still sign in with its local BridgeLink password if your identity provider is unavailable.

3. To restrict BridgeLink API basic authentication to specific accounts, check **Enable API Basic for Service Accounts** under **Service Accounts (API)**.
4. Select a user from **Service Account Users** and click **Add**. Repeat for each account that needs API access. Only the users you add here can authenticate to the BridgeLink API (`https://<BridgeLink IP>:8443/api`) with basic authentication.
5. To require every BridgeLink user to sign in through your identity provider, check **Only allow OIDC login** under **Exclusive Mode**.
6. Click **Save**.

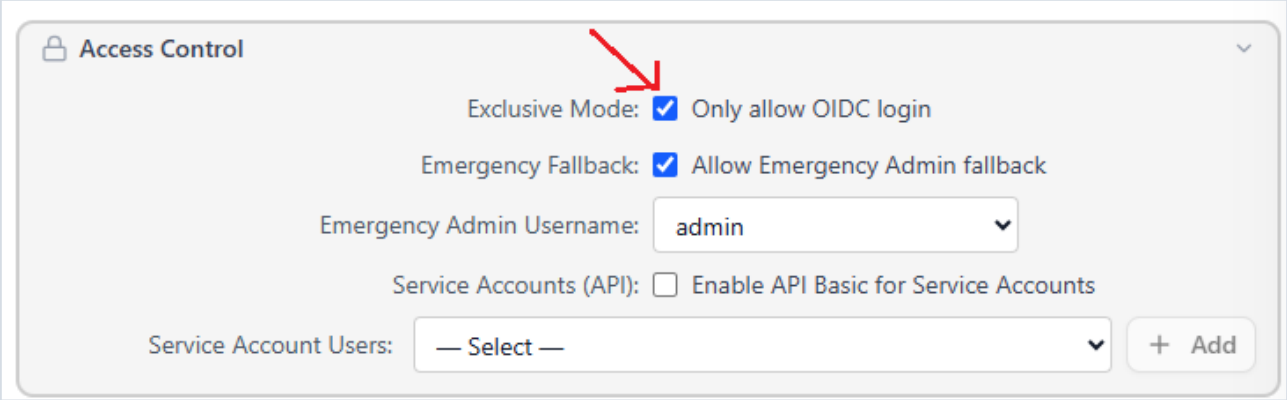

Figure 13: Access Control settings with Only Allow OIDC Login enabled

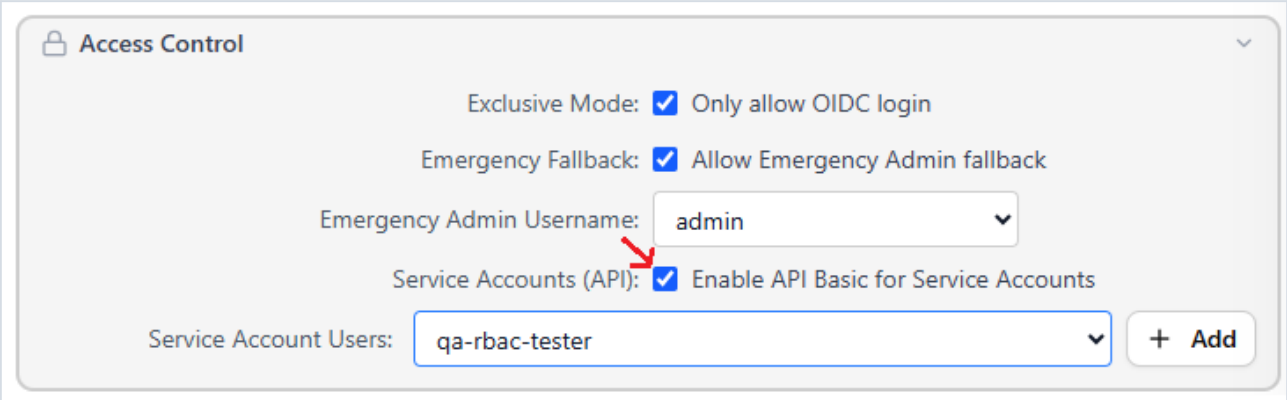

Figure 14: Service Accounts API configuration

Setting	What it does	Default
Exclusive Mode: Only allow OIDC login	Requires every user to sign in through the OIDC identity provider.	Unchecked
Emergency Fallback: Allow Emergency Admin fallback	Lets one designated account sign in with its local BridgeLink password even when Exclusive Mode is on.	Unchecked
Emergency Admin Username	The account exempted from Exclusive Mode.	(none selected)

Setting	What it does	Default
Service Accounts (API): Enable API Basic for Service Accounts	Restricts BridgeLink API basic authentication to the accounts listed in Service Account Users.	Unchecked
Service Account Users	The accounts allowed to use API basic authentication when the setting above is enabled.	(none)

Exclusive Mode always continues to allow the emergency admin account and any configured service account users, even when **Only allow OIDC login** is checked. Configure **Emergency Fallback** and **Service Accounts (API)** before you enable **Only allow OIDC login**, so you cannot lock yourself out if your identity provider becomes unreachable.

User Provisioning and Role Mapping

User Provisioning controls whether BridgeLink creates new users automatically when someone signs in with OIDC for the first time, and how it decides which role to assign them.

1. Under **User Provisioning**, check **Automatically create user if missing** next to **Auto Provision Users** to have BridgeLink create a new user the first time someone signs in with OIDC.
2. Select a role from **Default Role**. BridgeLink assigns this role when it cannot resolve a role from the claims, or when role mapping is turned off.
3. To assign roles from your identity provider's claims instead of always using the default role, check **Read roles from token claims** next to **Use roles from token**.
4. Under **Role source (claim)**, select where BridgeLink should look for the role name:
   - **Groups**: reads the role name from a `groups` claim in the token
   - **Roles**: reads the role name from a `roles` claim in the token
   - **Custom**: reveals a text field where you enter the dot notation path to the claim, for example `access.roles`
5. Click **Save**.

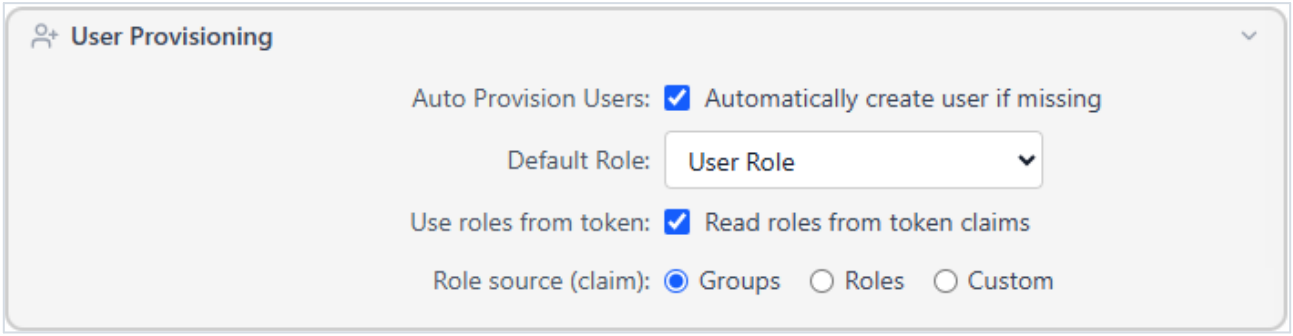

Figure 15: User Provisioning settings with role source from claims

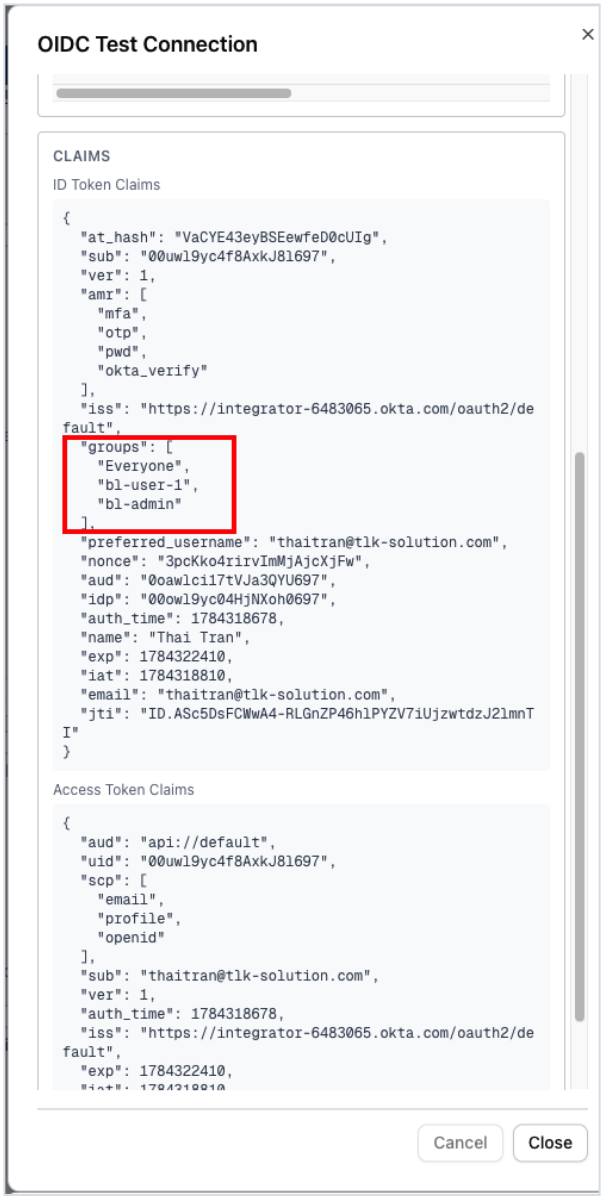

Figure 16: Claims response showing a groups array

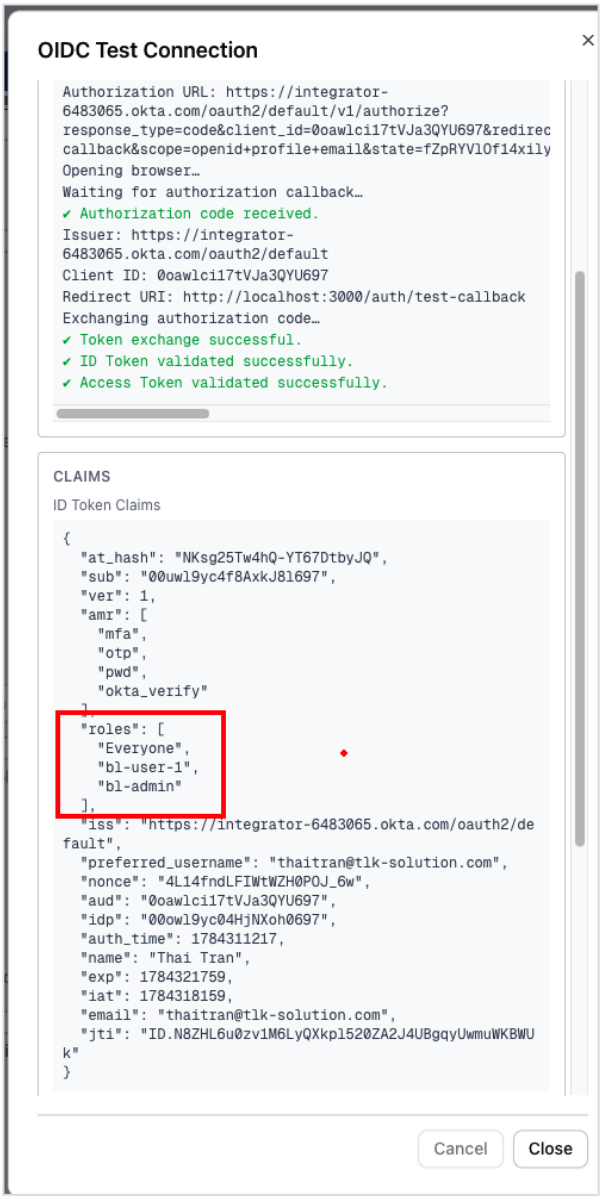

Figure 17: Claims response showing a roles array

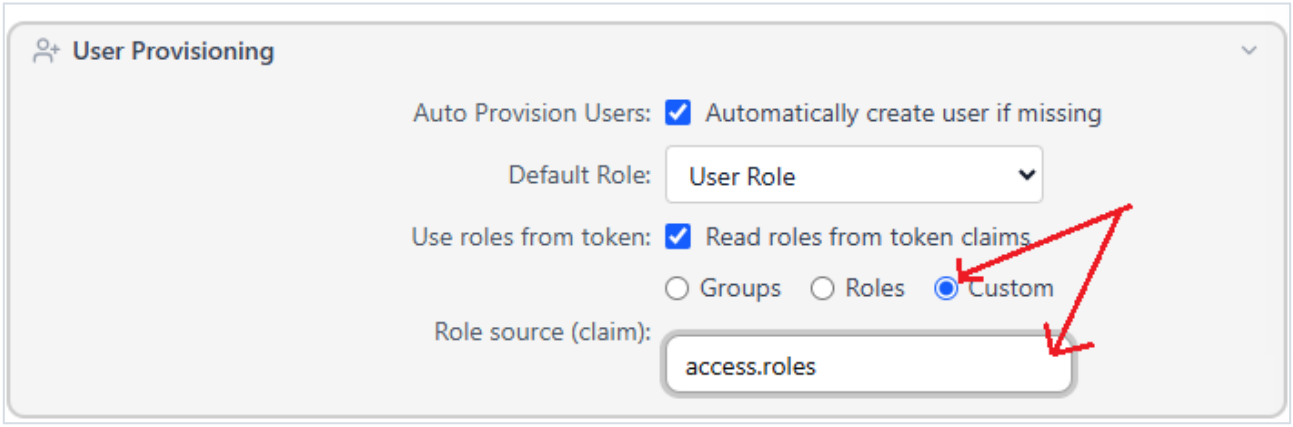

Figure 18: Custom role source claim configuration

Setting	What it does	Default
Auto Provision Users: Automatically create user if missing	Creates a new BridgeLink user the first time someone signs in with OIDC and no matching user exists.	Unchecked
Default Role	The role assigned to an auto-provisioned user when no role can be resolved from claims.	(none selected)
Use roles from token: Read roles from token claims	Turns on role mapping from the OIDC claims instead of always using Default Role.	Unchecked
Role source (claim)	Where BridgeLink looks for the role name: `Groups`, `Roles`, or a `Custom` claim path.	`Groups`

Every role name BridgeLink resolves, whether from **Default Role** or from an OIDC claim, must already exist with the same spelling in **Access Control > Role**. Add or rename BridgeLink roles there first, then match the names your identity provider returns.

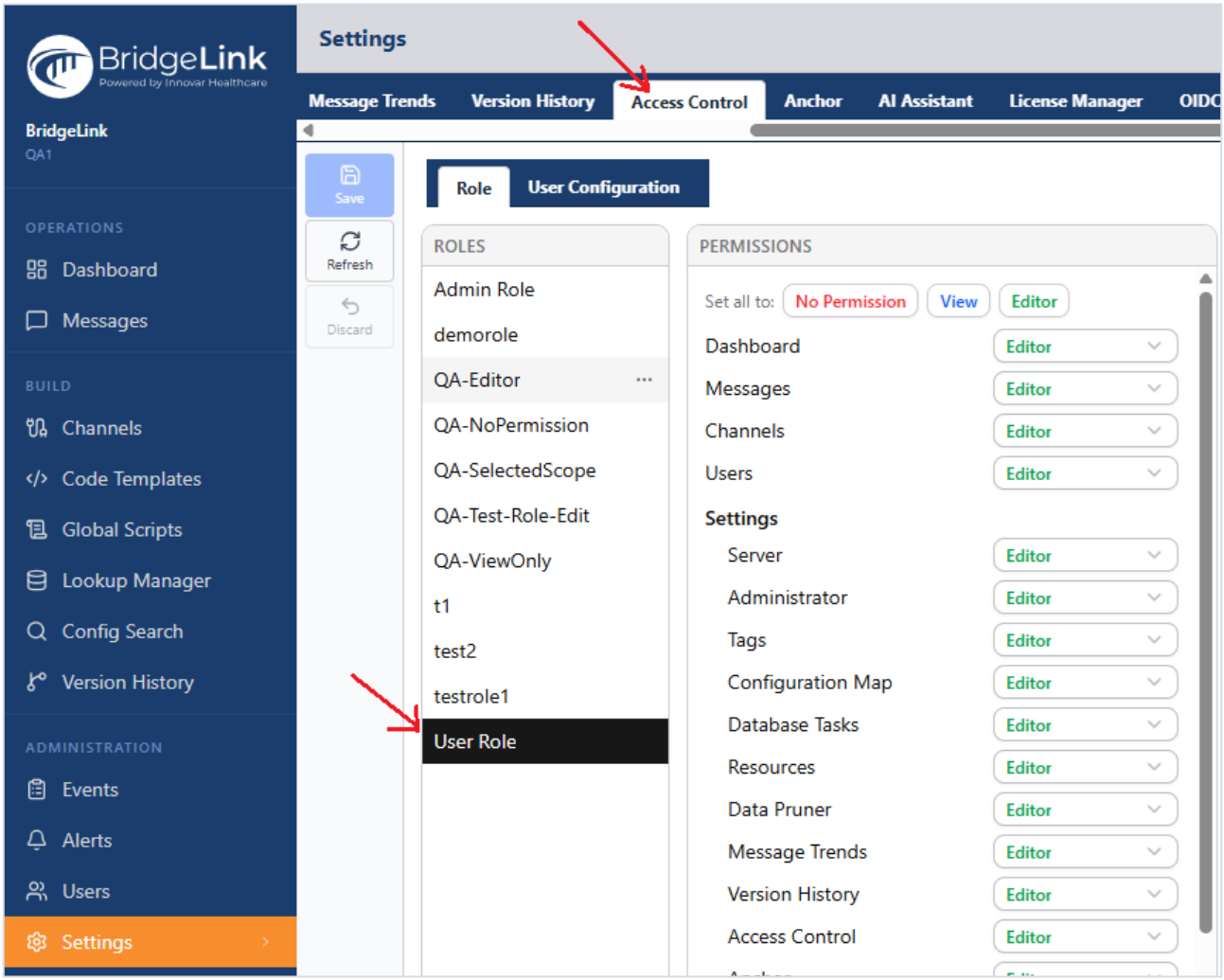

Figure 19: Access Control role configuration matching the OIDC role name

If a BridgeLink user already exists, signing in with OIDC updates their name and email but does not change their assigned role. To change an existing user's role, do it directly in **Access Control**.

Using OIDC

Signing In

Once your identity provider is configured and OIDC is enabled, users sign in through WebAdmin's own login page instead of a separate client.

1. Open the WebAdmin login page.
2. Enter your BridgeLink server address in **Server**.
3. Wait for the **Sign in with SSO** button to appear below **Login**. It appears automatically once WebAdmin confirms OIDC is enabled for that server.
4. Click **Sign in with SSO**. You do not need to enter **Username** or **Password**.
5. Your browser redirects to your identity provider. Sign in there, completing multi-factor authentication if your identity provider requires it.
6. After your identity provider approves the sign-in, your browser returns to BridgeLink and signs you in automatically.

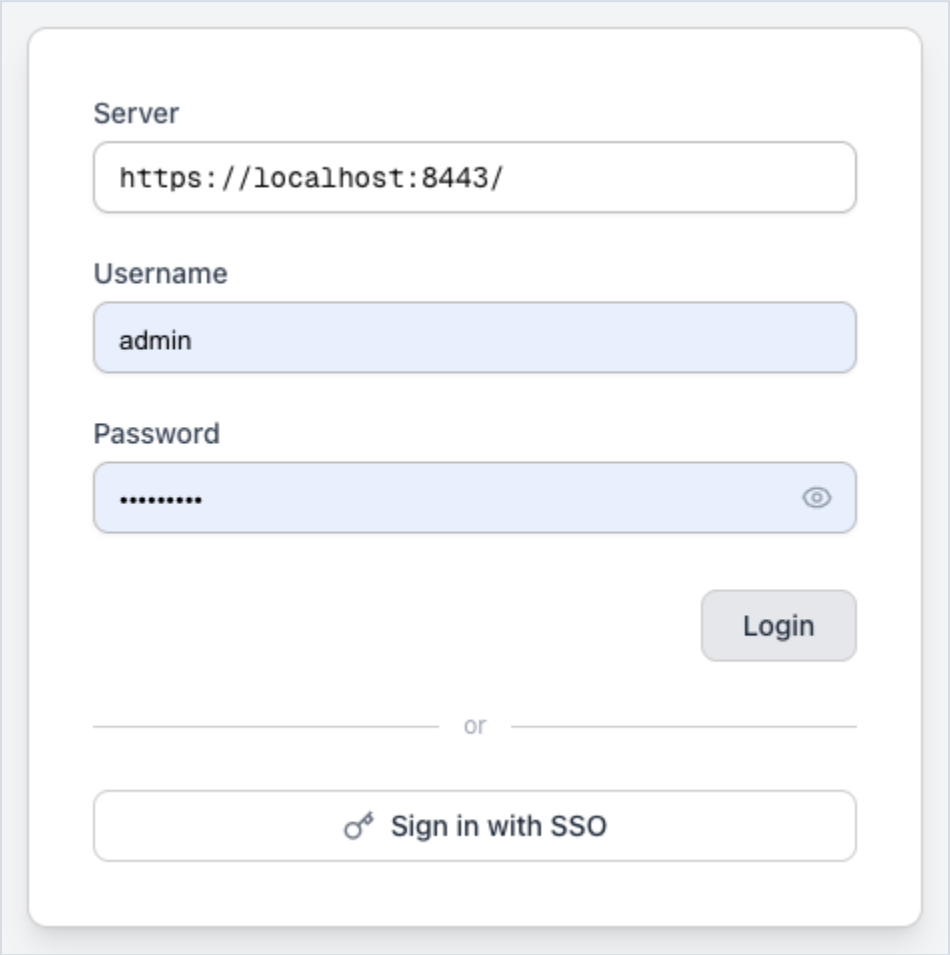

Figure 20: WebAdmin login page with the Sign in with SSO option

Testing the Connection Again

Run **Test Connection** any time you change the **Issuer**, **Client ID**, **Client Secret**, or **Redirect URIs**, or after your identity provider rotates a secret or changes its claim structure.

1. In WebAdmin, click **Settings**, then click the **OIDC** tab.
2. Click **Test Connection**.
3. Review the **Claims** returned to confirm your identity provider is reachable and returning the claims your role mapping expects.
4. Click **Close**.

Troubleshooting

Symptom	Likely cause	What to do
Test Connection fails or shows an error before returning claims	The **Issuer**, **Client ID**, or **Client Secret** does not match your identity provider's application, or the callback URL used during the test is not registered with your identity provider	Confirm each value against your identity provider's application settings. If the dialog shows a callback URL warning, register that exact URL as a redirect URI in your identity provider.
A user signs in with OIDC but no BridgeLink account is created	**Automatically create user if missing** is turned off	Under **User Provisioning**, check **Automatically create user if missing**.
Sign-in fails with an ambiguous role error	The token's claim contains more than one value that matches an existing Access Control role name	Confirm only one claim value matches a role name in **Access Control > Role**, or adjust your identity provider's claim to return a single matching value.
An existing user's role does not change after signing in with OIDC	BridgeLink only updates name and email for existing users; it does not reassign roles automatically	Change the user's role directly in **Access Control**.
Administrators are locked out after enabling **Only allow OIDC login**	**Emergency Fallback** was not configured before Exclusive Mode was enabled, or the identity provider is unreachable	Sign in with the **Emergency Admin Username** configured under **Emergency Fallback**, or with a configured **Service Account User**.

Support

Contact Innovar Healthcare support at `support@innovarhealthcare.com` if you cannot resolve an issue with this guide. Include your BridgeLink version, the OIDC plugin version, and, if the issue involves a failed sign-in or Test Connection, the relevant Server Log entries. For help planning a more complex identity provider integration, Innovar Healthcare's professional services team is also available.