

Testing ID Everywhere OIDC with Postman

Overview

Postman can be used to test an ID Everywhere OpenID Connect integration before connecting a production application.

This guide demonstrates the **Authorization Code flow with PKCE**, using a confidential test client.

This configuration has been successfully tested against ID Everywhere, including token retrieval and a UserInfo request.

Prerequisites

You will need:

- Access to ID Everywhere.
- An account permitted to create OIDC applications.
- Postman with OAuth 2.0 authorization support.
- An active ID Everywhere user for testing.

Never use production client secrets in screenshots or publicly shared Postman collections.

Step 1 — Register an OIDC test application

Sign in at:

<https://app.ideverywhere.com>

Open your tenant's OIDC Applications management page.

Create an application with:

Application Name: Postman OIDC Test

Application Type: Web / Server Application (Confidential)

Authorized Redirect URL:

`https://oauth.pstmn.io/v1/browser-callback`

Save the application and securely record its Client ID and Client Secret.

Important: The Postman browser callback URL ends in `/v1/browser-callback`, not `/v1/callback`.

Step 2 — Open Postman's authorization settings

In Postman, create or open an HTTP request.

Select the **Authorization** tab.

Set the authorization type to **OAuth 2.0**.

Choose the option to configure a new token.

Step 3 — Configure OAuth 2.0

Enter the following settings:

Setting	Value
Grant Type	Authorization Code (With PKCE)
Callback URL	<code>https://oauth.pstmn.io/v1/browser-callback</code>
Authorization URL	<code>https://app.ideverywhere.com/oauth2/authorize</code>
Access Token URL	<code>https://app.ideverywhere.com/oauth2/token</code>

Client ID	Your IDE application's Client ID
Client Secret	Your IDE application's Client Secret
Scope	<code>openid profile email</code>
Code Challenge Method	SHA-256 / S256
Client Authentication	Send as Basic Auth header

The exact names of settings may vary slightly between Postman versions.

Why these settings matter

Authorization Code: The supported OIDC grant type.

PKCE S256: Protects the authorization-code exchange.

Client Secret: Authenticates the confidential client to the token endpoint.

Scope: Requests OIDC authentication and identity information.

Basic Auth Header: Sends the confidential client's credentials using the supported `client_secret_basic` method.

Step 4 — Request an access token

Click **Get New Access Token** or the equivalent action in Postman.

Postman should open the ID Everywhere authorization page.

Sign in using your ID Everywhere account.

After authentication, Postman should receive the authorization response and exchange the code for tokens.

If successful, Postman displays the resulting token information.

Do not share these tokens publicly.

Step 5 — Test the UserInfo endpoint

Create a new HTTP request in Postman.

Method: GET

URL:

```
https://app.ideverywhere.com/oauth2/userinfo
```

Under Authorization, select **Bearer Token** and use the access token returned by the successful authorization flow.

Alternatively, configure the request to use the OAuth 2.0 token already obtained in Postman.

Send the request.

Step 6 — Review the response

A successful UserInfo response may contain information similar to:

```
{
  "sub": "example-unique-user-id",
  "name": "Example User",
  "given_name": "Example",
  "family_name": "User",
  "tenant_id": 2,
  "role": "domain_admin",
  "email": "user@example.com",
  "email_verified": true
}
```

This is illustrative data. Actual values depend on the authenticated user and the granted scopes.

A successful response confirms that the access token was accepted by the UserInfo endpoint and that identity information was returned.

It does not, by itself, prove that a third-party application correctly validates ID tokens.

Common Postman errors

invalid_request

Verify that the Scope includes:

openid

This is required for OIDC authentication.

Also confirm the grant type, callback URL, and other required authorization parameters.

Redirect URL mismatch

Ensure the callback URL registered in ID Everywhere exactly matches the one used in Postman.

invalid_client

Verify the Client ID, Client Secret, and client authentication method.

For this confidential-client example, use **Basic Auth header**.

invalid_grant

Start a new authorization flow.

Authorization codes cannot be reused. Also confirm the PKCE verifier and redirect URI are consistent across the authorization and token requests.

No UserInfo response

Confirm that the request uses the **access token**, not the ID token or Client Secret.

Check whether the token is expired.

Testing public applications

For a public-client test:

1. Create a Public Application (PKCE) registration in ID Everywhere.
2. Register Postman's exact callback URL.
3. Select Authorization Code with PKCE S256.
4. Supply the Client ID.
5. Do not supply a Client Secret.
6. Use a client authentication method of None, where available.
7. Complete the authorization flow.

Security reminders

- Do not publish Client Secrets.
- Do not paste live tokens into support tickets.
- Use dedicated test applications where possible.
- Revoke or rotate exposed credentials.
- Remove unused test registrations.

Related articles

- [Connecting an Application Using OIDC](#)
- [Understanding OIDC Settings and Security Terms](#)
- [Troubleshooting OIDC Connections](#)

Revision #1

Created 2026-10-10 22:11:54 UTC by Administrator

Updated 2026-10-10 22:12:05 UTC by Administrator