Configuring Auth0 as an OAuth Provider in PHPKB

👤 Palwinder Singh

How to configure Auth0 as an OAuth provider in PHPKB knowledge base software? In this tutorial, you will learn how to configure **Auth0** as **OAuth Provider** with **PHPKB OAuth plugin**.

> **PHPKB OAuth Authentication Plugin**
>
> The OAuth 2.0 authentication plugin enables users to log in using their Google, Microsoft, Facebook, or any other account via buttons on the login page of your knowledge base.
>
> **Interested to buy this plugin?** Contact Us for Licensing & Pricing.

PHP Requirements:

- PHP 7.0 or later
- CURL extension
- JSON extension
- OpenSSL extension

Download & Installation:

Extract the package (that you received after purchasing this plugin), copy all the files & folders, and paste them at their respective locations under the installation directory of PHPKB Knowledge Management Software on your server. There is a new folder, called '**add-ons**' (applicable to PHPKB v9.0), copy that and put it directly under the root folder (i.e. outside **/admin/** folder) of the PHPKB package.

Steps:

1. Log in to the **Administrator Control Panel** of PHPKB as a **Superuser**, go to **Tools** > **OAuth / OpenID-Connect** plugin.
2. After successfully logging in to PHPKB (at Step 1), open a new tab/window and log in to Auth0 Dashboard, as we are going to configure some of the settings parallel.
3. Click **Applications** > **Applications** (which is available in the Left-Sidebar menu) and then click **Create Application** button.
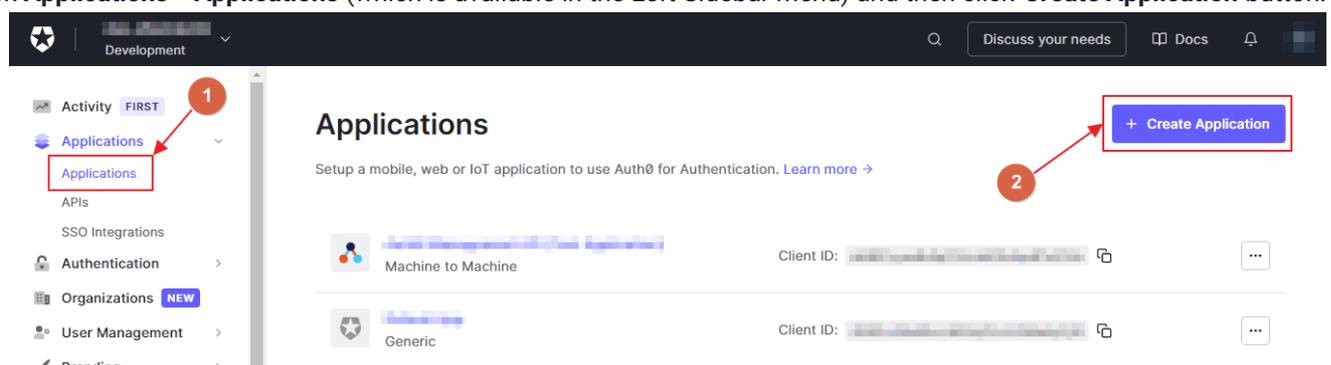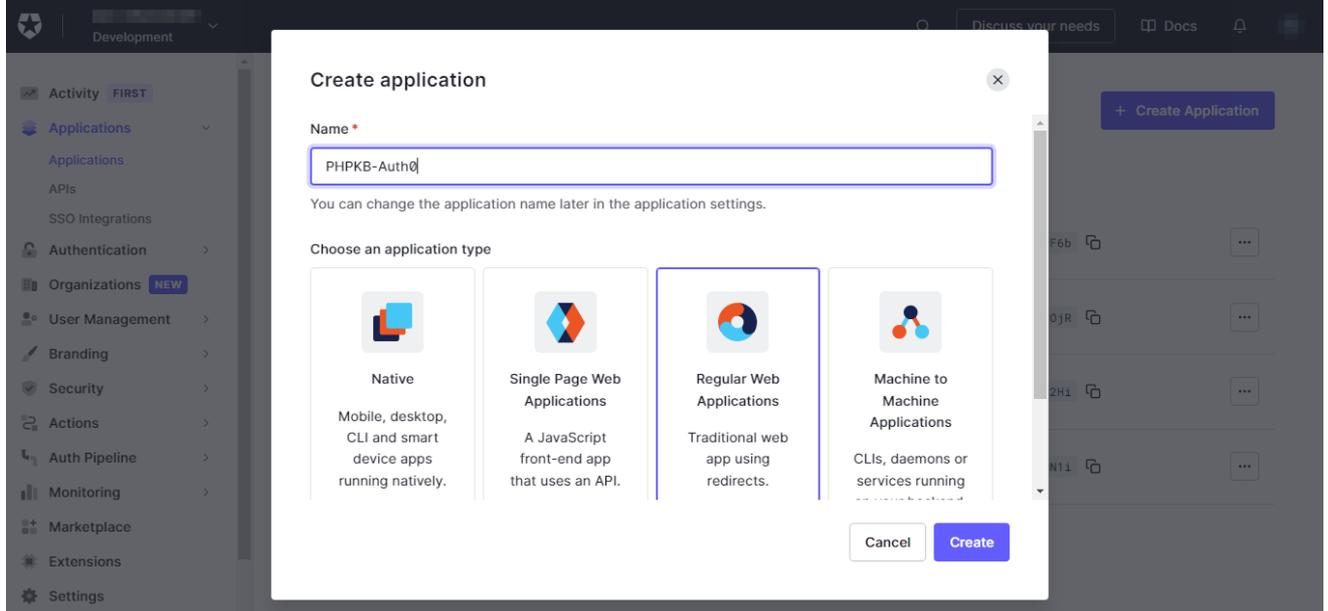

4. Enter the **Name** of your application and select **Choose an application type** as **Regular Web Applications** and click on the **Create** button.

¹²Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

5. Once your application has been created, it will be opened by default, select the **Settings** tab (next to the "**Quick Start**" tab), you will see the Basic Information section, and since you have already logged in to the Administrator Control Panel of PHPKB, copy the **Client ID** and **Client Secret** from this screen (Auth0 Settings), and paste them, one by one, in the **Tools** > **OAuth** > **Client ID** and **Client Secret** input boxes.

6. Then scroll down to the **Application URIs** section, paste the **Redirect URL** (by copying from **Tools** > **OAuth** > **Basic Configuration** section > **Redirect URL**) in the **Application Login URI** & **Allowed Callback URL** input boxes.

Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

Application URIs

Application Login URI

https://█████████add-ons/oauth/index.php

In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. Learn more

Allowed Callback URLs

https://█████████add-ons/oauth/index.php

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://` . You can use Organization URL parameters in these URLs.

7. Now, scroll down further, click on the **Advanced Settings** section, click on the **Grant Types** and make sure these are selected (especially the **Authorization Code** option), and update it in the **Tools** > **OAuth** > **Grant Type** option. (Default: **Authorization Code**)

Advanced Settings

| Application Metadata | Device Settings | OAuth | Grant Types | WS-Federation | Certificates | Endpoints |

Grants

☑ Implicit   ☑ Authorization Code   ☑ Refresh Token   ☑ Client Credentials   ☐ Password
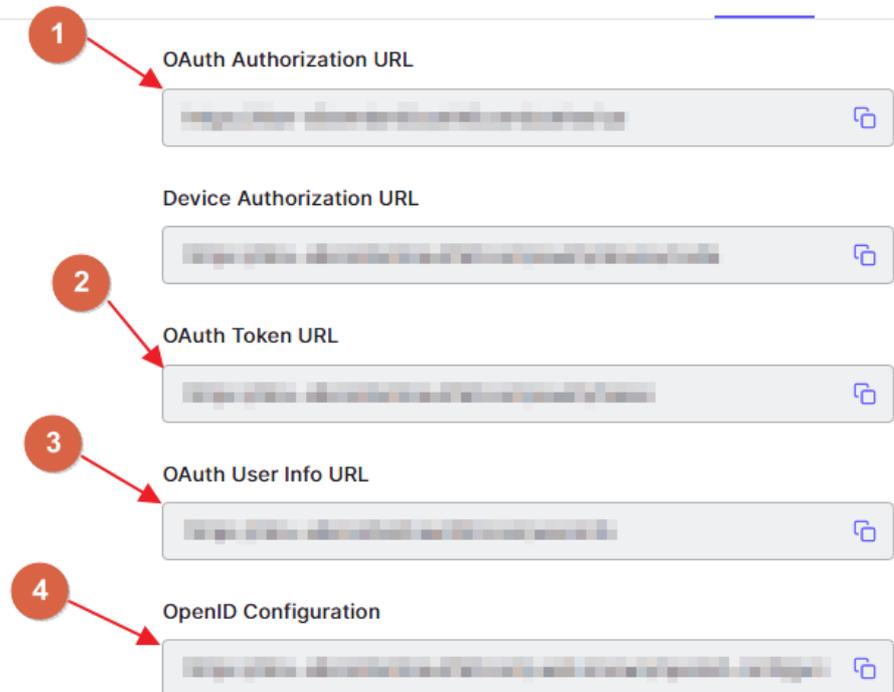
☐ MFA   ☐ Passwordless OTP

8. After enabling the desired Grant Types, expand **Endpoints**, copy the values in fields 1, 2 & 3 (as shown in the screenshot below), and paste them in the **Tools** > **OAuth** > **Authorize Endpoint**, **Access Token Endpoint** & **Get User Info Endpoint** input boxes respectively.
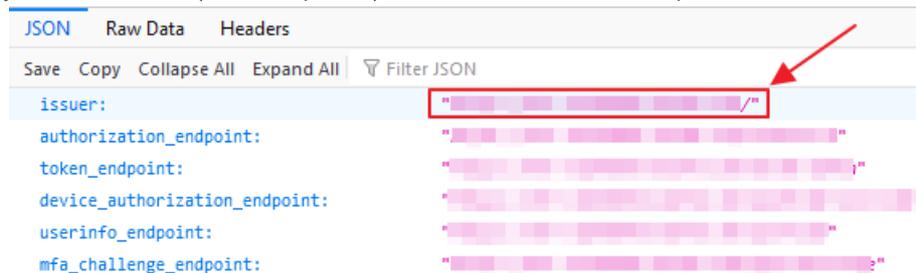
Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

Advanced Settings

Application Metadata   Device Settings   OAuth   Grant Types   WS-Federation   Certificates   **Endpoints**

OAuth

OAuth Authorization URL

Device Authorization URL

OAuth Token URL

OAuth User Info URL

OpenID Configuration

9. Thereafter, copy the last URL (i.e. #4 as shown in the screenshot at **Step 8**), open a new tab/window, and at this point, copy the **issuer** URL (without quotes) from the JSON data, and paste it into the **Tools** > **OAuth** > **Issuer URL** box.

JSON   Raw Data   Headers

Save   Copy   Collapse All   Expand All   ▽ Filter JSON

issuer:

authorization_endpoint:

token_endpoint:

device_authorization_endpoint:

userinfo_endpoint:

mfa_challenge_endpoint:

Note: If you have installed any JSON Viewer extension in your browser then it would output the JSON data in a friendly & readable format, otherwise, you would see it as raw output (unformatted).

10. Let us configure the other settings.

> **Tip**: To make the configuration task easier, helpful notes/tips are added under the fields/options where it is necessary.

⁴Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

BASIC CONFIGURATION

Configure basic settings, like Enable OAuth, Redirect URL, App Name, Client ID, Client Secret, Scope, Authorize Endpoint, Access Token Endpoint, etc.

Enable OAuth? ☑ Yes

Whether you want to enable & show OAuth on Login page to users or not.

Issuer URL *

The initial endpoint that is contacted by the relying party to begin a flow (must be a valid Base URL for Discovery configuration and PHPKB will fetch Authorization URL, Issuer URL, etc. using this Base URL). It must start with HTTPS for production and it may start with HTTP on localhost.

For example: If the Discovery Document URL is https://login.example.com/.well-known/openid-configuration then just enter https://login.example.com

Redirect URL   oauth/index.php

This is where user will be redirected after a successful authentication. You should add this URL in your OAuth Server as OAuth Redirect or Callback URL.

App Name (Optional)

You can enter the App Name, like Google. Default: OAuth

Display Name (Optional)   Login with Auth0

Please enter what you want to show on Login button. Default: Login with <App Name>

Client ID *

A publicly exposed string that is used by the service API to identify the application. It is also used to build authorization.

Client Secret *

Secret is used to authenticate the identity of the application to the service API when the application requests to access a user account. It must be kept private between the application and the API.

Scope   openid email

The scopes that are associated with access tokens determine what resources are available when they are used to access OpenID connect protected endpoints. For example: openid profile name email phone

Note: This is fetched automatically if the Discovery configuration is found.

Authorize Endpoint *

Access Token Endpoint *

Get User Info Endpoint *

Grant Type   Authorization Code ▾

11. Now configure the **Advanced Settings** section.

ADVANCED SETTINGS

You can configure more options, like Create user if not exists, Keep existing users, Update user data, Default group(s) assignment, and Default Role.

Create user if not exists? ☑ Yes

Auto-provisioning. If user does not exist, PHPKB will create a new user with the data provided by the Identity Provider.

Auto-linking existing users? ☑ Yes

If a PHPKB account already exists with the same identity as a newly-authenticated user over OpenID Connect, login as that user instead of generating an error.

Update User Data? ☑ Yes

Auto-update. PHPKB will update the account details of user with the data provided by the server.

Match PHPKB account by   email ▾

Select what field will be used in order to find the user account. If "email", the plugin will prevent the user from changing his/her email address in My Profile page.

Default Group(s) Assignment   Choose default group(s) assignment ▾

The default group(s) that will be assigned to Member users when they would log in to PHPKB via OAuth.

⁵⁷Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

12. Then configure the **Attribute Mapping** section.

> 🚩 **Tip**: To create users as Member users, you can set the '**Default Role**' as '**Member**', otherwise, change it accordingly.

ATTRIBUTE MAPPING

Sometimes the names of the attributes sent by the identity provider do not match the names used by PHPKB for the user accounts. In this section you can set the mapping between provider fields and PHPKB fields. Note: This mapping may also be set at identity provider's side (if supported).

Username *	email
Email *	email
First Name	name
Last Name	
Role	

The attribute that contains the role of the user, for example 'memberOf'.

Default Role	Writer

Default role assignment to all users.

13. The next is the **Role Mapping** section where you can map the roles returned by your IdP with the roles that are available in PHPKB.

> 🚩 If your IdP does not return any roles then you can skip this section.

ROLE MAPPING

The Identity Provider can use its own roles. In this section, you can set the mapping between IdP and PHPKB roles. Accepts comma separated values. Example: admin,owner,superuser

Member	
Writer	
Writer-Trusted	
Editor	
Superuser	

14. Then you can set **Role Precedence** for different roles.

> 🚩 If your IdP does not return any roles then you can skip this section.

⁶Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

ROLE PRECEDENCE

In some cases, the IdP returns more than one role. In this secion, you can set the precedence of the different roles. The smallest integer will be the role chosen.

Member [0-99]

Writer [0-99]

Writer-Trusted [0-99]

Editor [0-99]

Superuser [0-99]

15. Finally, set up **Security Settings** accordingly (if needed).

SECURITY SETTINGS

Configure Proxy and `cert` (certificate) path.

Configure Proxy?

Configure a proxy. For example: http://my.proxy.com:80

Configure Cert Path?

Configure a cert. For example: /path/to/my.cert

16. Test the configuration by going to the **Login** page (either in the Public area or Admin area, if Default Role is not set to Member).

That's all!

⁷Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.