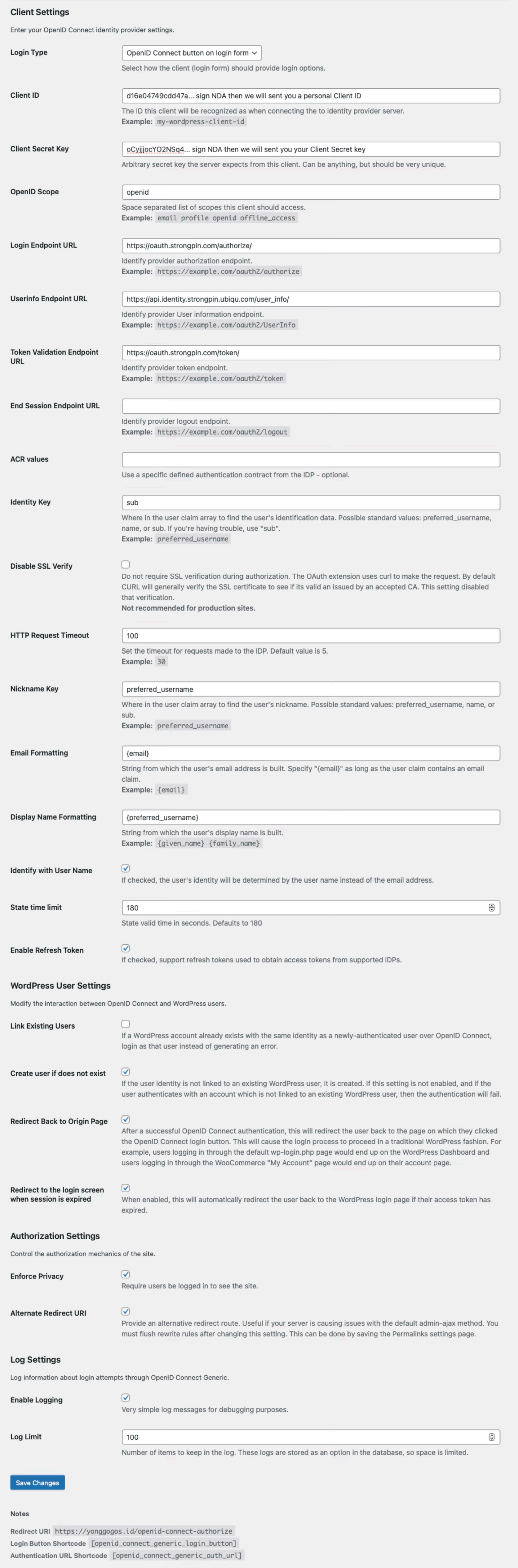

Client Settings

Enter your OpenID Connect identity provider settings.

Login Type

OpenID Connect button on login form

Select how the client (login form) should provide login options.

Client ID

d16e04749cdd47a... sign NDA then we will sent you a personal Client ID

The ID this client will be recognized as when connecting the to Identity provider server.
Example: `my-wordpress-client-id`

Client Secret Key

oCyjjjocYO2NSq4... sign NDA then we will sent you your Client Secret key

Arbitrary secret key the server expects from this client. Can be anything, but should be very unique.

OpenID Scope

openid

Space separated list of scopes this client should access.
Example: `email profile openid offline_access`

Login Endpoint URL

https://oauth.strongpin.com/authorize/

Identify provider authorization endpoint.
Example: `https://example.com/oauth2/authorize`

Userinfo Endpoint URL

https://api.identity.strongpin.ubiqu.com/user_info/

Identify provider User information endpoint.
Example: `https://example.com/oauth2/UserInfo`

Token Validation Endpoint URL

https://oauth.strongpin.com/token/

Identify provider token endpoint.
Example: `https://example.com/oauth2/token`

End Session Endpoint URL

Identify provider logout endpoint.
Example: `https://example.com/oauth2/logout`

ACR values

Use a specific defined authentication contract from the IDP - optional.

Identity Key

sub

Where in the user claim array to find the user's identification data. Possible standard values: preferred_username, name, or sub. If you're having trouble, use "sub".
Example: `preferred_username`

Disable SSL Verify

☐ Do not require SSL verification during authorization. The OAuth extension uses curl to make the request. By default CURL will generally verify the SSL certificate to see if its valid an issued by an accepted CA. This setting disabled that verification.
Not recommended for production sites.

HTTP Request Timeout

100

Set the timeout for requests made to the IDP. Default value is 5.
Example: `30`

Nickname Key

preferred_username

Where in the user claim array to find the user's nickname. Possible standard values: preferred_username, name, or sub.
Example: `preferred_username`

Email Formatting

{email}

String from which the user's email address is built. Specify "{email}" as long as the user claim contains an email claim.
Example: `{email}`

Display Name Formatting

{preferred_username}

String from which the user's display name is built.
Example: `{given_name} {family_name}`

Identify with User Name

☑ If checked, the user's identity will be determined by the user name instead of the email address.

State time limit

180

State valid time in seconds. Defaults to 180

Enable Refresh Token

☑ If checked, support refresh tokens used to obtain access tokens from supported IDPs.

WordPress User Settings

Modify the interaction between OpenID Connect and WordPress users.

Link Existing Users

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

Create user if does not exist

☑ If the user identity is not linked to an existing WordPress user, it is created. If this setting is not enabled, and if the user authenticates with an account which is not linked to an existing WordPress user, then the authentication will fail.

Redirect Back to Origin Page

☑ After a successful OpenID Connect authentication, this will redirect the user back to the page on which they clicked the OpenID Connect login button. This will cause the login process to proceed in a traditional WordPress fashion. For example, users logging in through the default wp-login.php page would end up on the WordPress Dashboard and users logging in through the WooCommerce "My Account" page would end up on their account page.

Redirect to the login screen when session is expired

☑ When enabled, this will automatically redirect the user back to the WordPress login page if their access token has expired.

Authorization Settings

Control the authorization mechanics of the site.

Enforce Privacy

☑ Require users be logged in to see the site.

Alternate Redirect URI

☑ Provide an alternative redirect route. Useful if your server is causing issues with the default admin-ajax method. You must flush rewrite rules after changing this setting. This can be done by saving the Permalinks settings page.

Log Settings

Log information about login attempts through OpenID Connect Generic.

Enable Logging

☑ Very simple log messages for debugging purposes.

Log Limit

100

Number of items to keep in the log. These logs are stored as an option in the database, so space is limited.

Notes

Redirect URI `https://yonggogos.id/openid-connect-authorize`
Login Button Shortcode `[openid_connect_generic_login_button]`
Authentication URL Shortcode `[openid_connect_generic_auth_url]`