

OpenID Connect is an authentication layer on top of OAuth 2.0, an authorization framework. The standard is controlled by the OpenID Foundation.

New in [Tiki23](#). The library used is <https://packagist.org/packages/stevehoades/oauth2-openid-connect-client>

To enable OpenID Connect

Select Tiki and OpenID Connect from tiki-admin.php?page=login -> General preferences -> Authentication method.

Visit the OpenID Connect tab and fill the preferences page.

Tiki uses OpenID Connect with Authorization Code, after a successful login, the user is redirected to Tiki Login page, and a code is passed as query argument. Tiki will contact the OpenID auth endpoint to exchange the code for the Access Tokens.

The redirect URL should point to tiki-login.php.

OKTA OpenID Connect (example)

To use OKTA services you need to create an account at <https://www.okta.com>. Okta offer trial account once your email validated you will be redirected to your Okta Dashboard.

<SERVER_DOMAIN>: <https://my.okta.com>

| pref | value |
|--------------------------------|---|
| Issuer URL | <SERVER_DOMAIN>/oauth2/default |
| Provider URL Authorization | <SERVER_DOMAIN>/oauth2/default/v1/authorize |
| Provider URL user access token | <SERVER_DOMAIN>/oauth2/default/v1/token |
| JKWS URL | <SERVER_DOMAIN>/oauth2/default/v1/keys |

Keycloak OpenID Connect (example)

<SERVER_DOMAIN>: <https://my.server.com>

Realm: master

| pref | value |
|--------------------------------|--|
| Issuer URL | <SERVER_DOMAIN>/auth/realms/master |
| Provider URL Authorization | <SERVER_DOMAIN>/auth/realms/master/protocol/openid-connect/auth |
| Provider URL user access token | <SERVER_DOMAIN>/auth/realms/master/protocol/openid-connect/token |
| JKWS URL | <SERVER_DOMAIN>/auth/realms/master/protocol/openid-connect/certs |

Client ID and Client Secret are provided by the service.

How user is linked

After a successful login and access token retrieved, Tiki will use the user email to match against the existing users.

How user is created

If no user is matched and the preference "Create user if not registered in Tiki" is enabled, Tiki will use the preferred_username or the name, returned in the access_token, to create a new user and login the user right after.

If the username or name, are already in use, Tiki will return an error.

Alias: [OIDC](#)