Single Sign On (SSO) - OpenID connect in translate5

If you wish, you can set up the same translate5 instance on different domains and configure for different clients different domains and different OpenID servers.

- Use different IPDs with the same translate5 / Mapping of client via domain
- Examples how to use translate5 as OpenID client with different OpenID servers for Single-Sign-On (SSO) usage
- Configuration within translate5
- Creation of a user through OpenId Connect / Matching with an existing user
- Create and map a translate5 client to a client on IDP side via custom claims

Use different IPDs with the same translate5 / Mapping of client via domain

The main domain, under which translate5 runs, is configured in the system configuration under the id runtimeOptions.server.name

By default it is associated to the translate5 client "defaultcustomer" and it is also used for all other clients, users and logins.

Yet, it is possible to run one and the same translate5 instance under multiple different domains and associate different clients to different domains.

If you want to do this, you have to enter the domain you want to use for the client in the field "translate5 domain" in the tab "General" of a client in the client management of translate5. In addition you have to create an Apache vhost for this domain, that points to the same document_root as the main translate5 domain of your instance.

If you have done this and a user accesses translate5 via the domain associated to a client,

- the OpenID IDP configured for this client will be asked to authenticate the user
- if a user will be created via the SSO, he/she will automatically be associated with this client

This way it is possible to use different OpenID IPDs with different clients in the same translate5 instance.

Alternatively, you can use one OpenID IDP and map users to different clients via a custom field of your IDP.

Examples how to use translate5 as OpenID client with different OpenID servers for Single-Sign-On (SSO) usage

- Google as OpenID server for translate5
- MS Azure ActiveDirectory as OpenID server for translate5
- MS ActiveDirectory Federation Services

Configuration within translate5

To configure translate5 to work with OpenId connect is very simple. Navigate to the clients tab in your translate5 instance, and under the OpenId sub-tab there are OpenId configuration fields that need to be set.

Fill in the fields with the data as explained below. How to obtain the data of the OpenId Connect server is explained by the Google example further below.

translate5 domain (in the General tab of the edited client): the used translate5 instance url/domain. (Google configuration example: translate5.net). Note: do not define the domain with protocol included. Valid definition will be translate5.net, test.translate5.net, translate5.net . Invalid: http://translate5.net

For more information on how the translate5 domain is used and why it is important, please see above.

All other fields exist in the OpenId tab of the edited client)

OpenId server: OpenId authentication server url. This is the URL translate5 redirects users for authentication at the OpenId connect server (Google configuration example: https://accounts.google.com)

OpenId issuer: OpenId issuer url. In many cases this url is identical with the OPenId server url.

OpenId user name: OpenId authentication server username (Google configuration example: "Client ID" see image3)
(the user name that allows the openId client application to connect to the API of the openId server; do NOT mix this up with the username of the user, that wants to authenticate!)

OpenId password: OpenId authentication server password (Google configuration example: "Client secret" see image3)
(the password that allows the openId client application to connect to the API of the openId server; do NOT mix this up with the password of the user, that wants to authenticate!)

OpenId OAuth URL: OpenId authentication server OAuth url. This is the URL translate5 uses in the background to do the server to server authentication mechanism (Google configuration example: https://accounts.google.com/o/oauth2/auth). Also used to fetch the openid server properties (ex: https://accounts.google.com/o/oauth2/auth/.well-known/openid-configuration)

System Roles: translate5 internal user system roles.

- If the OpenID connect server is configured and able to pass roles along with the authentication, the translate5 system roles passed by the OpenID server will be set for this user in translate5.
- If the roles in the OpenID server change, on the next login they will also change in translate5.
- The OpenID server will only be able to set roles, that are checked in the OpenID Connect configuration of the corresponding client in translate5. Other roles will be ignored by translate5, even if the OpenID server claims them.
- If the OpenID Connect server is not able to or configured to claim roles, the roles checked in the OpenID Connect configuration of the corresponding client in translate5 will always automatically be set for users of this client.

Link text on login page: Label text on the login page of translate5. A click on it redirects the user to the configured openid server for authentication, instead of using translate5 for authentication. If the checbox "Do not show login page" below the field "Link text on login page" is checked, the user will directly be redirected to the openid server for authentication/authorization and will never see the translate5 login page.

Checkbox "Do not show login page: Automatically redirect to OpenID Connect server": Redirect directly to the SSO authentication provider.

Creation of a user through OpenId Connect / Matching with an existing user

If a user authenticates, the following steps are done:

1. Translate5 tries to find an existing translate5 user by issuing authority and openid identity/subject of the user claims. If for those values, there is an existing user in transalte5, this translate5 user will be used and updated with potential new rights and user attributes (like name, e-mail, etc.)
2. If in the above case there is no matching user found in translate5, translate5 tries to find a valid e-mail address in the information, the OpenId Connect IPD provides about the connecting user:
    a. First it looks in the email field requested of the userinfo_endpoint (if configured)
    b. If not found there, translate5 tries to find it in the 'upn' claim.
    c. If not found there, translate5 tries to find it in the preferred_username claim
    d. If it is not found there, translate5 will throw an exception
3. If a user exists, that has the e-mail address as login name as the one coming from OpenId Connect IDP, but with different OpenId specific issues and sub values, we will create new user with "OID-" as login prefix but with same email address.
4. If a user exists, that has the e-mail address as login name as the one coming from OpenId Connect IDP, but with no OpenId specific issues and sub values (so a manually created one), translate5 updates this user with the info coming from the OpenId Connect IDP.

Create and map a translate5 client to a client on IDP side via custom claims

By default to what a client a user belongs to, that authenticates via SSO is defined by the URL he/she uses to access translate5.

Yet, you can also configure one OpenID IDP together with translate5, so that one IDP can authenticate users for different clients within translate5.

To do this:

- Go to the system configuration and look up the field `runtimeOptions.customers.openid.claimsFieldName`. Set it to the name of the attribute in your IDP, that contains the client number in the OpenID token claims. How translate5 will handle values in this config:
    - no value: the currently authenticated user will be mapped to the client in translate5 via URL (see above)
    - defined value: translate5 will check if there exists an attribute in the OpenId token claims with this value. In case there is value, translate5 will try to find a client with the number in the token claims value.
        - If there is a client with this number, this client will be used for the current user.
        - If no client is found, a new client will be created with number and name as the value provided in the claims