Configure OIDC entities

Now that you are logged in, you can go and register your service on the SURFconext platform. Note that at this moment it's possible to independently register and test entities on the test environment of SURFconext. Although it is possible to add and edit production connections here, the SURFconext team will submit the changes and additions to the production environment on your request.

In this stage we assume that you:

- Have an account at a connected Identity Provider. This can be at one of the to SURFconext connected institutions or a eduID guest account.
- Are member of the SURFconext Team associated with the service in the SP Dashboard
- Are logged in successfully at https://sp.surfconext.nl

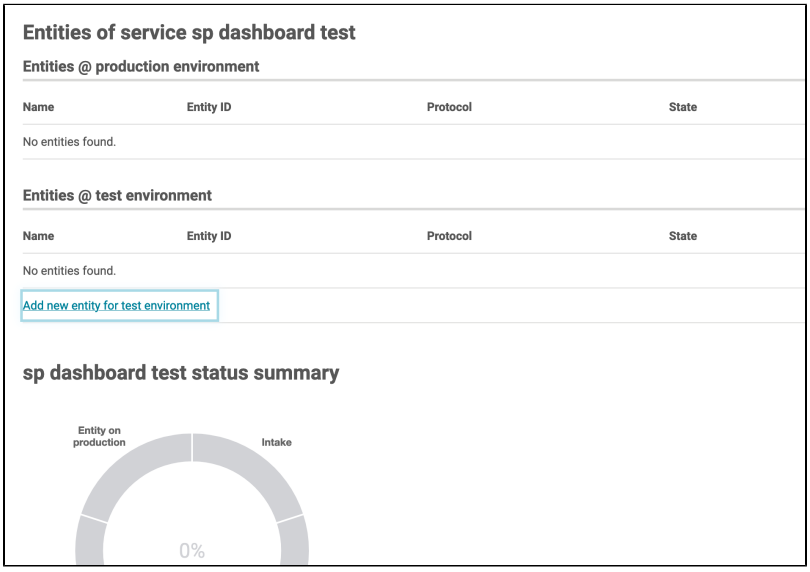
Getting your service published on the Production Environment of SURFconext, the following needs to be taken care of:

- First you will **add an entity**.
- **Fill out all the forms** of that entity in the SP Dashboard. This is generally known as the metadata of your service in SURFconext.
- If your done with all the metadata, you can **publish the entity** to the test environment to start testing.
- You can **manage your entities** from here as well: add another one, remove an entity and promote, entity to production and more.
- If you are done, you can **promote the entity to production.**

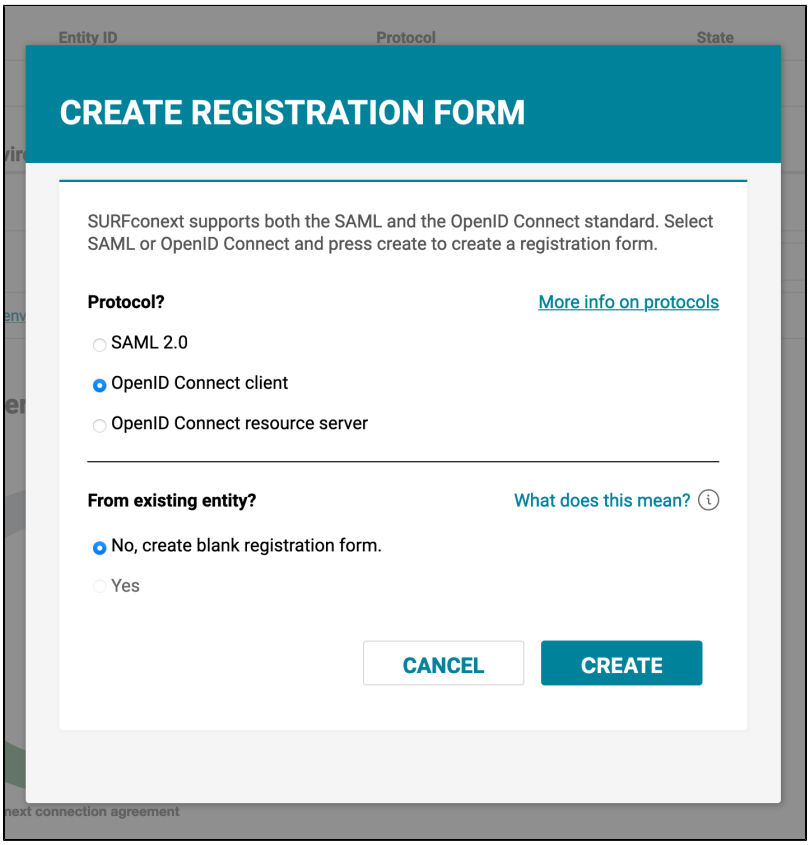
Add entity

An entity on SURFconext is the least you need to get going. Select 'Add new entity for test environment'.

If you see nothing familiar, start by selecting a service from the pull down at the top right of the window.



You will be prompted to select SAML 2.0 client, OpenID Connect client, or an OpenID Connect resource server.



You can choose either an OpenID Connect client, or an OpenID Connect resource server. For most cases, an OpenID Connect client is sufficient. If you want to protect an API using SURFconext, you can add a resource server for this purpose. Please note that resource servers need to be connected to an OpenID Connect client. Only a connected resource server can validate access_tokens of that client.

Fill out the form

Assuming you got acquainted with OpenID Connect by now, most of the form is self explanatory. Extra information about fields can be found under the question mark. It is important to consider the claims you need to receive via SURFconext so set the claims accordingly. More information on claims can be found on this page. Take your time to experiment with claims whilst in the test environment.

> SURFconext has a **data minimisation** policy, which means you only receive those claims that are **strictly needed** to make your service work.

Configure your client

You have received a client ID and a secret, with which you can configure your client. The minimal configuration needed is:

client ID: The client ID you received

client secret: The secret shown to you

The .well-known URL: https://connect.test.surfconext.nl/.well-known/openid-configuration (production is https://connect.surfconext.nl/.well-known/openid-configuration)

scope: openid

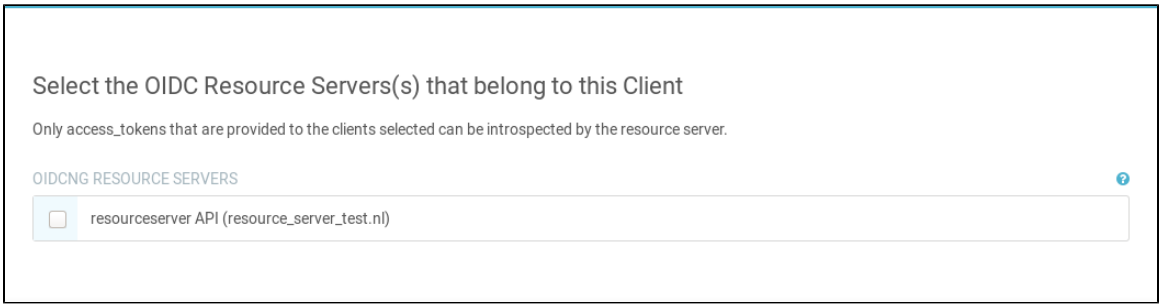
If you need other URL's in your application you can find these in the aforementioned . well-known configuration URL

Playground

A playground application is available for your convenience. It's a pre-configured OpenID Connect client that is shows the technical details of the features supported by the OIDC gateway. When you tick "Enable playground" in the SP Dashboard, the redirect URL of the playground is added to your configuration. If you add your client details in authorization tab the OpenID Connect test Playground or the OpenID Connect production Playground for production entities, you can test your own Client, and view all the reponses and claims that the OpenID connect server can supply.

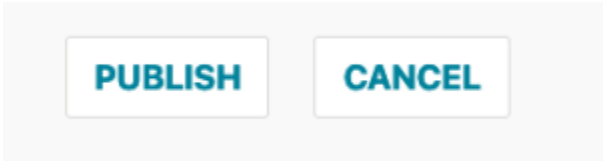
Resource server

You can use SURFconext to protect your API (also known as resource server). For a more technical background see this page. Adding a resource server requires less information as connecting an OIDC client. You don't need to enter the subject type (transient or persistent) and you don't need to request the claims you want. The subject type and claims requested are configured in the Client configuration. The resource server receives the same subject and claims as the Client. After adding a resource server, you need to configure the Client to allow resource server access. You can do so by editing the client, see the screenshot below.



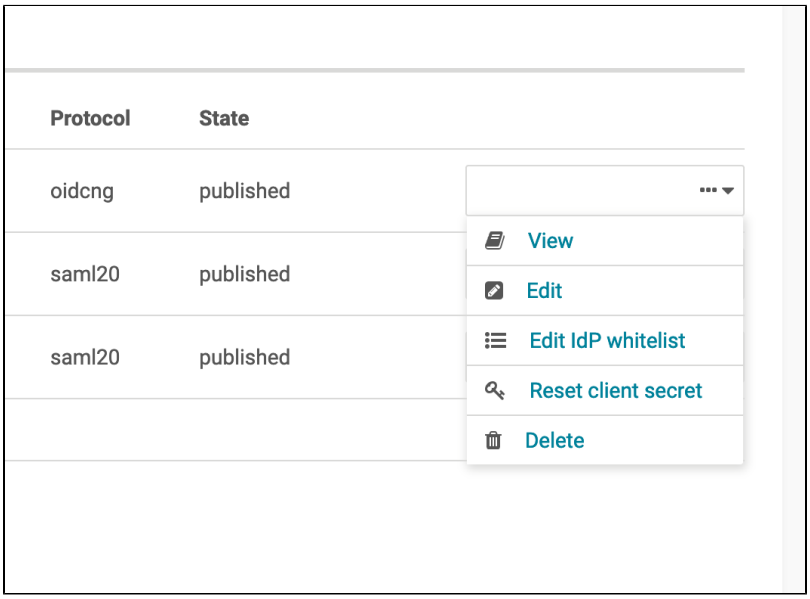
Publish your entity

Satisfied with your filled out form? Press the 'publish' button to push your entity to the test environment of SURFconext. Your service will be connected automatically to the all available IdPs, ready to be tested. Please see below if you want to limit the access to your client



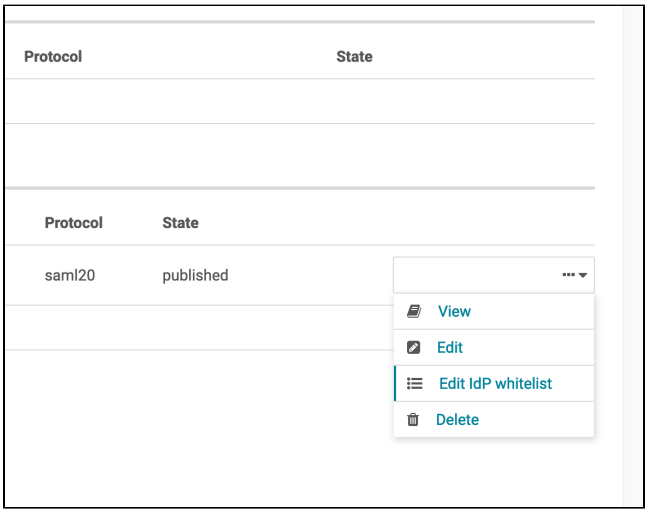
Manage your entities

The three dots at the end of each row shows all options for that entity. OpenID connect clients are the type "oidcng", resource servers are named "oidcng_rs"



Limit access to your entity

By default, **all** IdP's that are connected to the **test environment** are able to log in to your service. If you want to limit that access, you can do so. Select 'Edit IdP whitelist' from the dropdown: there you can choose which IdP's are allowed to connect to your service.



Production

If you have sorted everything out and all is working as aspected you can promote your entity to production.

When you promote your entity to production we will run through some technical checks together and see if the contracts are in place. Besides this we need you to provide us with the institution(s) you want to connect with as well as a contact at the institution. The latter is important because institutions don't simply connect to a service not knowing who initiated it.

Navigate