Connect to the Test environment

The Test Environment is the playground for testing new services with SURFconext. It is in no way connected to the production environment of SURFconext and thus not connected to real identity providers and real users. In the Test environment test-IP's and test-accounts are available. Connecting to it is simple and a contract at this point is **not** necessary so you can start testing immediately. At this point you should have **pre pared** your application so it supports **SAML** or **OpenID Connect**. This page will show you how you can define your test instance on our test environment. Both SAML and OpenID Connect will be depicted.

On this page you will find the steps necessary to define your service in SURFconext. You will need to do the following:

1. Configure your service for SURFconext using SAML or OpenID Connect
2. Register your SAML/OpenID Connect enabled service in the SP dashboard
3. Test your connection with fictional IdP's, fictional users and fictional attribute values

If you have succeeded to go through these steps you have successfully connected your service to the test environment of SURFconext!

1. Configure your service for SURFconext

To start you will need to configure your service with SURFconext specific parameters.

SAML

For your service, you need to import the Entity Descriptor of the SURFconext IdP Proxy of our test environment in your Service Provider. Depending on the software you use, you must import the metadata-URL or place a file with this information on a location that is accessible by the service.

> ⊗ The Public SAML metadata or the 'Entity Descriptor' of the SURFconext IdP proxy for the test environment differs from the production environment. The following applies:
>
> - **Test Environment: https://metadata.test.surfconext.nl/idp-metadata.xml**
> - **Production Environment: https://metadata.surfconext.nl/idp-metadata.xml**
>
> Service Providers that are connected to the 'Test Environment' of SURFconext can not and will not be connected to both identity providers on the production environment and the test environment. The user profiles from IdP's on the test environment are fictional or unverified. Real users, with their profiles can only connect to your service through the production environment of SURFconext. Once verified that you are connected to the production environment you must use the entity descriptor of the production environment as mentioned above.

OpenID Connect

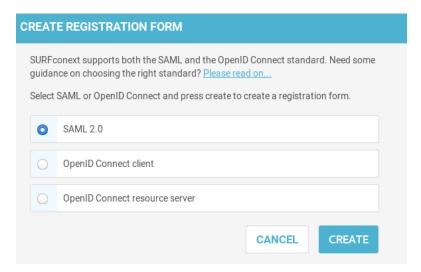Via the SP Dashboard you'll get the necessary data for OpenID Connect, which are:

- A username and secret
- The .well-known URL has all the OpenID Connect configuration parameters. This URL can be used by your software to find all the configuration it needs. The test URL is https://connect.test.surfconext.nl/.well-known/openid-configuration

Configure your service with these data to enable access through OpenID Connect. The scope "openid" is sufficient to get all configured claims.

⊗

As you might expect the OpenID Connect configuration as found in the **.well-known URL differs from test to production**. A small but essential difference:

- Test Environment: **https://connect.test.surfconext.nl/.well-known/openid-configuration**
- Production Environment: **https://connect.surfconext.nl/.well-known/openid-configuration**

2. Register your SAML/OpenID Connect enabled service in the SP dashboard

After the intake by telephone, the SURFconext team will add you to a team. If you have confirmed the membership of this team, members have access to designated services in the SP Dashboard. You can manage entities of the service you have been granted accesses to. If you are a member of multiple teams you will see the according services.

CREATE REGISTRATION FORM

SURFconext supports both the SAML and the OpenID Connect standard. Need some guidance on choosing the right standard? Please read on...

Select SAML or OpenID Connect and press create to create a registration form.

- ● SAML 2.0
- ○ OpenID Connect client
- ○ OpenID Connect resource server

CANCEL   CREATE

User Attributes

Not provided by the import URL but necessary to promote a service to production is a solid motivation of each attribute used. Read our wiki 'Attribute best practice' to get to know more. In short, we want you to use as **few attributes as possible and as privacy preserving as possible**. If you use too many, SURFconext can decline promotion of the service to production and ultimately an institution can decline your request to connect to the service.

3. Test your connection with fictional IdP's, fictional users and fictional attribute values

After logging in to your service, you will see the WAYF-screen with the available test Identity Providers. SURFconext supplies two test IdP's:

- SURFconext Test IdP
- SURFconext Mujina IdP

SURFconext Test IdP
This test IdP allows you to test **various login and attribute scenarios**, common when dealing with SAML Identity Providers. Several fictitious user accounts are available with attributes matching real world scenarios. The users are also members of groups that you can use to test retrieval of group information.

The 'SURFconext Test IdP' is not available in the Production environment.
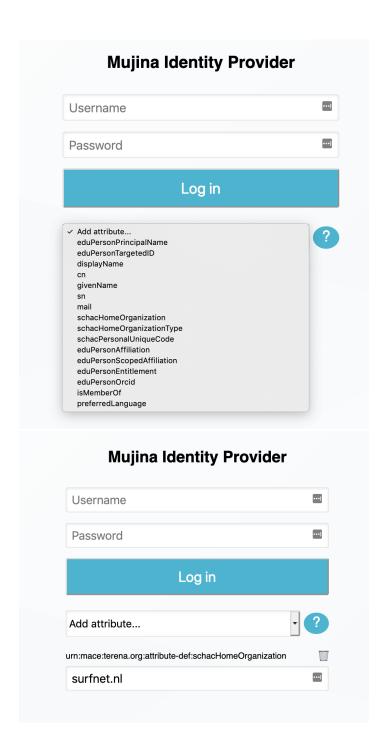
SURFconext Mujina Identity Provider
This test IdP lets you impersonate every possible user. **You are able to select attributes and values of your choice.** This is a great way of testing all attributes available to SURFconext. You can add the attributes as shown in the pull-down on the login page of Mujina. The attributes you can use are described in detail on our attributes page.

> ⓘ   Take the following into account when using our Mujina Identity Provider:
>
>   - **Username** will be used as the value for the attribute **'urn:mace:dir: attribute-def:uid'**
>   - Password is **not** necessary
>   - The attribute 'urn:mace:dir:attribute-def:eduPersonOrcid' is currently not available for use with Mujina.
>   - **An IdP will never be connected to SURFconext without the attributes 'urn:mace:dir:attribute-def:uid' and 'urn:mace:terena. org:attribute-def:schacHomeOrganization'** so it is advised to always test with both these used.

Mujina Identity Provider

Username

Password

Log in

✓ Add attribute...
eduPersonPrincipalName
eduPersonTargetedID
displayName
cn
givenName
sn
mail
schacHomeOrganization
schacHomeOrganizationType
schacPersonalUniqueCode
eduPersonAffiliation
eduPersonScopedAffiliation
eduPersonEntitlement
eduPersonOrcid
isMemberOf
preferredLanguage

?

Mujina Identity Provider

Username

Password

Log in

Add attribute...

?

urn:mace:terena.org:attribute-def:schacHomeOrganization

surfnet.nl

Back to start

Return our step by step guide to continue to connect your service.

Navigate