

Sluit een test IdP aan op de testomgeving van SURFconext

SURFconext heeft een **test-** en **productieomgeving** beschikbaar. Op beide kun je een service provider (SP) en een identity provider (IdP) aansluiten. De testomgeving wordt meestal gebruikt om een dienst te definiëren, te testen en te controleren of deze werkt zoals verwacht. Deze omgeving sluit nauw aan bij de productieomgeving. Op onze testomgeving kun je direct gebruik maken van de volgende IdP's:

- **SURFconext Test IdP**
De SURFconext Test IdP bevat een aantal fictieve gebruikersaccounts met bijpassende attributen welke overeenkomen met reële scenario's. We hebben [een lijst met gebruikers, wachtwoorden en attributen waarvan je gebruik kunt maken](#).
- **SURFconext Mujina IdP (Mock-IdP)**
Met de "Mujina IdP" kan voor de duur van een login-sessie een willekeurig account worden aangemaakt waarvoor elk van de door SURFconext ondersteunde attributen een willekeurige waarde opgegeven kan worden.
- **SURFconext gast IdP (eduID)**
Onze gast-IdP heeft de volgende kenmerken:
 - Iedereen kan op eduID (<https://eduid.nl>) een account aanmaken.
 - eduID heeft ook een testomgeving: <https://test.eduid.nl>.
 - Op de test-omgeving van SURFconext is de testomgeving van eduID automatisch aan elke dienst gekoppeld (op de productie-omgeving staat dat standaard uit en moet je expliciet vragen om een koppeling met eduID).
 - Het attribuut "urn:mace:terena.org:attribute-def:schacHomeOrganization" wordt door eduID vrijgegeven en kent slechts 2 waarden: "eduid.nl" of "surfguest.nl". (Gebruikers met de waarde surfguest.nl maakten vroeger gebruik van een andere gast-IdP en hebben hun oude account gemigreerd naar eduID).
 - Bij een koppeling met deze IdP moet je als dienstleverancier goed nadenken over hoe je bepaalt of een gebruiker op je dienst mag en wat hij of zij mag doen: iedereen in de wereld kan tenslotte een account aanmaken op de gast-IdP. Op [deze pagina](#) vind je informatie over hoe SURFconext kan helpen bij autorisatie.

Met bovenstaande IdP's kun je diensten uitgebreid testen. Soms kan het de voorkeur hebben te testen met een IdP van jouw instelling. Je kunt eenvoudig een test-IdP aansluiten op onze test-omgeving. Daarover vind je hier meer.

Wat kan ik met mijn test-IdP op de testomgeving van SURFconext?

Het opvoeren van een test-IdP gaat op een vergelijkbare manier als op productie maar de eisen die we stellen zijn niet zo streng, zodat je meer ruimte hebt om dingen te testen en te doen die op productie niet mogen. Denk aan het volgende:

- Je kunt parameters, bijvoorbeeld [attributen](#), in je IdP testen zonder dat eindgebruikers op productie hier ooit iets van merken. Denk hierbij aan een attribuut met (meerdere) waarden in een multi-valued attribuut als `urn:mace:dir:attribute-def:eduPersonEntitlement`. Als je klaar bent met testen kun je de wijzigingen met vertrouwen toepassen op de productieomgeving van je IdP of SP.
- Probeer eens iets anders uit dan wat je al op productie hebt draaien. Alle op productie bestaande technieken kun je ook op onze testomgeving gebruiken: SimpleSAMLphp, Microsoft ADFS, Microsoft Azure, of NetIQ Access Manager. Dit zijn dezelfde technieken als in gebruik op productie.
- Als je zelf wel eens diensten opvoert in SURFconext, kun je deze met je eigen test-IdP met representatieve test-accounts testen.



Het is belangrijk op te merken dat als je een test-IdP aansluit op onze testomgeving je er voor moet zorgen dat de identiteiten van gebruikers op deze omgeving niet herleidbaar zijn naar natuurlijke personen. Een test-IdP heeft alleen test-accounts!

Wat zijn de verschillen tussen test en productie op SURFconext?

De configuratie van je IdP is technisch gezien gelijk aan die op de productieomgeving maar je zult de metadata van onze testomgeving moeten laden op je IdP om correct met de test omgeving te verbinden. De endpoints zijn anders. Volg de handleidingen voor het opzetten van een IdP zoals [hier omschreven](#) en gebruik in plaats van de metadata van productie de metadata die je vindt op <https://metadata.test.surfconext.nl/> en in het bijzonder de metadata van SURFconext als Service Provider die je op [deze pagina vindt](#). SURFconext gedraagt zich namelijk als Service Provider voor jouw test-IdP!

Hoe sluit ik mijn test-IdP aan?

Om gebruik te maken van de testomgeving is geen contract of aansluitovereenkomst nodig; je kunt direct met de techniek aan de slag. Raadpleeg onze pagina's over het aansluiten van [een IdP om je voor te bereiden](#). Stuur vervolgens een mail naar support@surfconext.nl en wij helpen je op weg. Zorg dat je de URL van de metadata van het Identity Management systeem, je IdP, gereed hebt als je snel wilt aansluiten.

Test je IdP

We hebben ook op test een dienst beschikbaar die je de mogelijkheid biedt jouw IdP te testen. Dit stelt je in staat vast te stellen of het aanmelden met SURFconext goed werkt en of SURFconext de attributen goed ontvangt van jouw IdP. Ga naar de volgende site om te zien of je IdP doet wat hij moet doen:

- <https://engine.test.surfconext.nl/authentication/sp/debug>
 - Dit is onze debugpagina en deze dienst is op elke IdP in SURFconext aangesloten, zowel op test als productie. De productieinstantie van deze dienst [vind je hier](#). Op deze pagina kun je zien of de authenticatie succesvol is en of de attributen correct worden ontvangen door SURFconext. Je ziet hier de gegevens van jouw Identity Provider zoals geregistreerd in SURFconext, het SAML2 Subject en de attributen die SURFconext ontvangt. De dienst doet een validatie op de attributen aangegeven met een groen vinkje uiterst rechts (scroll naar rechts indien nodig).
 - En een succesvolle authenticatie ziet er als volgt uit:

Show response from Identity Provider

✓ Authentication success

Retry

Identity Provider

	
Logo	
Name	SURFnet bv
Entity ID	https://idp.surfnet.nl
Workflow Status	testaccepted

Dit is alles wat je nodig hebt om te weten of je IdP werkt met SURFconext! Als je succesvol aanmeldt op bovenstaande dienst (met meerdere test-accounts) gaat de authenticatie goed en ontvangt SURFconext de benodigde attributen om te functioneren en dus te koppelen met diensten. Je zult dan kunnen aanmelden op de meeste diensten. Raadpleeg [onze pagina over attributen](#) om de attributen set zo volledig mogelijk te vullen. Niet alle diensten maken gebruik van dezelfde attributen. Je kunt als voorbeeld de productieinstanties van de debugpagina gebruiken in combinatie met de productieinstantie van jouw IdP om te zien hoe en welke je de attributen moeten vullen (voor jouw IdP).

Als bovenstaande werkt, kun je aan de slag met je eigen diensten of die van service providers met wie je samenwerkt!

Richtlijnen voor gebruik

Op de test-omgeving zijn alle partijen aan het testen zijn en hier kunnen er dingen 'fout' gaan, anders dan verwacht. Het is dus verstandig geen persoonsgegevens van echte personen te gebruiken op deze test-omgeving. Onze test-IdP kan [als voorbeeld dienen](#) om fictieve gebruikers aan te maken. We stellen geen technische eisen aan je IdP, zoals bijvoorbeeld de technische veiligheid zoals TLS. Het is desondanks wel verstandig je hiermee bekend te maken en te zorgen dat je een hoge rating krijgt. Wij vragen hier zeker wel om als je naar productie gaat. Raadpleeg [onze pagina over SSL/TLS configuraties](#) om een rating A of hoger te krijgen. En aangezien het een testomgeving is, kun je dus ook testen wat je kunt doen (en vooral moet laten) om een rating F of T te krijgen!