

# SAML-tracer

- [Inleiding](#)
- [Installatie](#)
- [Single sign-on](#)
- [Attribute statement](#)
- [Single logout](#)

# Inleiding

SAML-tracer is een tool voor het bekijken van SAML- (en WS-Federation-)berichten die via de browser worden verzonden bij single sign-on en single logout.

# Installatie

Firefox: installeer de browser extensie via deze [pagina](#).

Chrome: installeer de browser extensie via deze [pagina](#).

Meer uitleg over het installeren en algemeen gebruik van de SAML-tracer kun je vinden op deze [pagina](#) van SURFconext.

# Single sign-on

Deze pagina beschrijft hoe je kunt controleren of single sign-on succesvol heeft plaatsgevonden.

1. Open de SAML-tracer plugin en navigeer naar de login URL van de service provider, bij voorkeur in een incognito/private venster.
2. Log in op de identity provider met je gebruikersnaam en wachtwoord en ga terug naar de SAML-tracer plugin.

Hier zie je twee regels met het SAML label:

Een AuthnRequest bericht van de service provider naar de identity provider:

GET https://login.acc.uu.nl/nidp/saml2/sso?RelayState=https%3A%2F%2Flogin.acc.uu.nl%2Fnidp%2Fsaml2%2Fmetadata%2Burn%2F... SAML

Een Response bericht van de identity provider naar de service provider.

POST	https://demo.serviceprovider.nl/acs	SAML
------	-------------------------------------	------

3. Selecteer het Response bericht van de identity provider.
4. Ga naar de tab 'SAML' in de onderste helft van het venster.
5. Zoek naar het <samlp:Status> element in de SAML response (je kunt scrollen of ctrl + f gebruiken om te zoeken).
6. Controleer de status code.

Een succes ziet er zo uit:

```
<saml:Issuer>https://login.acc.uu.nl/nidp/saml2/metadata</saml:Issuer>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
```

# Attribute statement

Deze pagina beschrijft hoe je de attribute statement kunt controleren.

1. Open de SAML-tracer plugin en navigeer naar de login URL van de service provider, bij voorkeur in een incognito/private venster.
2. Log in op de identity provider met je gebruikersnaam en wachtwoord en ga terug naar de SAML-tracer plugin.

*In de bovenste helft van het venster zie je twee regels met het SAML label:*

Een AuthnRequest bericht van de service provider naar de identity provider:

```
GET https://login.acc.uu.nl/nidp/saml2/sso?RelayState=https%3A%2F%2Flogin.acc.uu.nl%2Fnidp%2Fsaml2%2Fmetadata%2Burn%2F SAML
```

Een Response bericht van de identity provider naar de service provider.

```
POST https://demo.serviceprovider.nl/acs SAML
```

3. Selecteer het Response bericht van de identity provider.
4. Ga naar de tab 'Summary' in de onderste helft van het venster.

*De attribute statement ziet er zo uit\*:*

AttributeStatement:	
* mail	= j.doe@acc.uu.nl
* name	= Doe, J. (John)
* preferred_username	= Doe00001
* given_name	= John
* family_name	= Doe

\* Dit is een voorbeeld. De daadwerkelijke attributen zullen overeenkomen met de instellingen voor de specifieke service provider.

# Single logout

Deze pagina beschrijft hoe je kunt controleren of single logout (uitlog-verzoek) succesvol heeft plaatsgevonden. Een single logout kan op twee manieren worden geïnitieerd: door de service provider of door de identity provider. Per type logout dient er op een ander pad geantwoord te worden:

Type	Pad
Geïnitieerd door service provider (SP-initiated)	/nidp/saml2/slo
Geïnitieerd door identity provider (IDP-initiated)	/nidp/saml2/slo_return

## Geïnitieerd door service provider

1. Open de SAML-tracer plugin, log uit op een service provider en ga terug naar de SAML-tracer plugin.

*Hier zie je twee regels met het SAML label:*

Een LogoutRequest bericht van de service provider naar de identity provider:

```
GET https://login.acc.uu.nl/nidp/saml2/slo?SAMLRequest=IZLbatwwEIZfxejex3V8EGvDtkSt7sl7Yam9KZo7XEiaSAML
```

Een LogoutResponse bericht van de identity provider naar de service provider.

```
GET https://demo.serviceprovider.nl/simplesaml/module.php/saml/sp/saml2-logout.php/uu_prod?SAMLResponse=SAML
```

3. Selecteer het LogoutResponse bericht van de identity provider.

4. Ga naar de tab 'SAML' in de onderste helft van het venster.

5. Zoek naar het <samlp:Status> element in de SAML response (je kunt scrollen of ctrl + f gebruiken om te zoeken).

6. Controleer de status code.

*Een succes ziet er zo uit:*

```
<saml:Issuer>https://login.acc.uu.nl/nidp/saml2/metadata</saml:Issuer>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
```

## Geïnitieerd door identity provider

*Disclaimer: deze werkwijze geldt alleen voor POST en Redirect bindings.*

1. Open de SAML-tracer plugin, ga naar <https://login.acc.uu.nl/nidp/app/logout> en ga terug naar de SAML-tracer plugin.

*Hier zie je twee regels met het SAML label:*

Een LogoutRequest bericht van de identity provider naar de service provider.

```
GET https://demo.serviceprovider.nl/simplesaml/module.php/saml/sp/saml2-logout.php/uu_preprod?SAMLRequest=I SAML
```

Een LogoutResponse bericht van de identity provider naar de service provider.

```
GET https://login.acc.uu.nl/nidp/saml2/slo_return?SAMLResponse=fZFNb8lwDib%2FSpV7m7SrShe1lbZxgcEOBXH SAML
```

3. Selecteer het LogoutResponse bericht van de service provider.

4. Ga naar de tab 'SAML' in de onderste helft van het venster.

5. Zoek naar het <samlp:Status> element in de SAML response (je kunt scrollen of ctrl + f gebruiken om te zoeken).

6. Controleer de status code.

*Een succes ziet er zo uit:*

```
<saml:Issuer>sp-p-test</saml:Issuer>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
```