

# Handleiding NetIQ Access Manager als IdP en SP aan SURFnet



Met jouw hulp kunnen we onze documentatie verder verbeteren. Kom je zaken tegen in deze handleiding die niet kloppen of verduidelijking behoeven? Laat het ons weten via [support@surfconext.nl](mailto:support@surfconext.nl)

## Inhoud

- Inhoud
- 1. Inleiding
- 2. Introductie NetIQ Access Manager
  - Identity Server
  - Access Gateway
  - SSL VPN
  - JAVA agents
  - Policies
- 3. Hoe gaat het koppelen globaal in zijn werk?
  - IdP
  - SP
- 4. NetIQ Access Manager als Idp
  - 4.1. User Store toevoegen
  - 4.2. SP toevoegen aan Identity Server
  - 4.3. Voeg het token signing certificate van SURFconext toe
  - 4.4. Communiceer de eigen IdP metadata URL aan SURFnet
  - 4.5. Maak een attributen set aan
  - 4.6. Compatibiliteitsproblemen met diensten
  - 4.7. Controle van de configuratie
- 5. NetIQ Access Manager als SP
  - 5.1. SURFconext als IdP toevoegen
  - 5.2. Een reverse proxy toevoegen
  - 5.3. Controle

## 1. Inleiding

Via de SURFconext-infrastructuur voor online samenwerking beschikken gebruikers over diensten van verschillende leveranciers, die ze in één omgeving kunnen toepassen. Dit biedt nieuwe samenwerkingsmogelijkheden, binnen instellingen en over instellingsgrenzen heen. Deze handleiding beschrijft hoe een instelling die op SURFnet is aangesloten, met behulp van NetIQ Access Manager (NAM) kan aansluiten op SURFconext. Voor het lezen van deze handleiding is enige kennis van federatief identity management een pre. Een lijst van nuttige documenten:

- De [SURFconext factsheet](#) voor een overzicht van SURFconext.
- De [dienstbeschrijving](#) van SURFconext.
- Een [uitleg over SAML 2.0](#), de techniek waar de aansluiting op is gebaseerd.

We beschrijven in deze handleiding twee gevallen:

1. Aansluiten als Identity Provider (IdP), zodat medewerkers en studenten van een instelling met hun instellingsaccount kunnen inloggen op de diensten die op SURFconext zijn aangesloten. Een lijst van [diensten](#) is hier te vinden. Een dergelijke aansluiting biedt tevens single sign-on voor alle diensten die via SURFconext worden gebruikt.
2. Aansluiten als Service Provider (SP), zodat medewerkers en studenten van andere instellingen kunnen inloggen bij een dienst van de instelling die als Service Provider fungeert. Bijvoorbeeld op Blackboard of een samenwerkingsomgeving. We beschrijven hier niet hoe groepenfunctionaliteit die de instelling heeft aan SURFconext beschikbaar gesteld kan worden. Om dit te doen dienen [andere technieken](#) te worden toegepast. Het voordeel van het beschikbaar stellen van instellingsgroepen aan SURFconext is dat deze groepen dan gebruikt kunnen worden in sommige van de op SURFconext aangesloten diensten, en dus niet opnieuw hoeven te worden aangemaakt.

### ! SURFconext Metadata

Houd er rekening mee dat de metadata en de metadata locaties die gebruikt worden voor de test- en productieomgevingen van SURFconext verschillen. Gebruik ze als volgt:

- **Test:** <https://metadata.test.surfconext.nl/idp-metadata.xml>
- **Productie:** <https://metadata.surfconext.nl/idp-metadata.xml>

## 2. Introductie NetIQ Access Manager

NetIQ Access Manager levert gebruikers veilige toegang tot interne en externe (web) applicaties. Algemene informatie over dit product vindt u hier . Technische informatie is [hier](#) te vinden.

Access Manager levert de functionaliteiten die te zijn is in de onderstaande figuur:



### Identity Server

De Identity Servers biedt centrale authenticatie- en identity informatie voor alle applicaties. Dit gebeurt op basis van één of meerdere directories (NetIQ eDirectory, Active Directory of een LDAP server) waarin deze informatie is opgeslagen. Verder kunnen aan een Identity Server IdPs en SPs worden gekoppeld. Voor SURFconext zijn dit een SAML 2.0 IdP en SP. Hierbij dienen ook attribute sets te worden aangemaakt, waarin gedefinieerd wordt welke gegevens (attributen) van de IdP naar de SP (of van SP naar IdP) worden overgestuurd in de SAML communicatie. Het gaat dan onder meer om naam en e-mailadres van de betreffende gebruiker die wil inloggen. De attributen moeten conform de afspraken binnen SURFconext worden aangeleverd, dat wil zeggen met de juiste attribuutnaam en de juiste afspraken voor de waarde. Deze zijn voor SURFconext gedefinieerd op [deze pagina](#). De hier gedefinieerde informatie moet passen op de attributen die NetIQ Access Manager kent. Dat is vaak niet vanzelf zo en daarom dient er voor de attribute sets ook een attribute mapping te worden gemaakt. Bij het aanmaken gebeurt dit tegelijk.

### Access Gateway

De Access Gateway is een zogenaamde 'reverse proxy', die tussen de gebruiker en de web applicatie staat en levert dan single sign-on en/of gedifferentieerde toegang (autorisatie). Toegang wordt geweigerd of verleend op basis van policies die gekoppeld zijn aan de web applicaties. Toegang kan worden verleend op basis van de rol die een gebruiker binnen de organisatie heeft. Bijvoorbeeld op basis van groepslidmaatschap of bepaalde attributen, die de Identity Server aanlevert.

De Access Gateway heeft als voordeel boven andere single sign-on en autorisatie-oplossingen dat er geen additionele software op de webserver hoeft te worden geïnstalleerd. Technisch gezien vertaalt de Access Gateway de authenticatie en autorisaties uit Identity Server naar standaard HTTP headers, waarmee de meeste web applicaties overweg kunnen. Het is tevens mogelijk om authenticatie naar achterliggende systemen op basis van web formulieren (naam en wachtwoord op de web pagina) te automatiseren.

### SSL VPN

SSL VPN biedt beveiligde toegang tot wel of niet webgebaseerde diensten op basis van HTTPS. Hierbij kan ook met een user certificaat worden gewerkt als extra authenticatiemiddel.

## JAVA agents

Access Manager biedt IBM WebSphere, BEA WebLogic en JBoss agents die autorisatie en toegang bieden tot servlets en Enterprise JavaBeans (EJBs). Deze agents gebruiken Java Authentication and Authorization Service (JAAS), Java Authorization Contract voor Containers (JACC) en interne Web-server APIs voor authenticatie. Tezamen leveren zij granulaire, policy- gebaseerde autorisatie en toegang tot servlets en EJBs.

## Policies

Policies worden gebruikt om de autorisaties voor gebruikers te bepalen. Ze bepalen bijvoorbeeld of iemand een web server mag bereiken op basis van IP-adres, de methode van authenticatie of de rol van de betreffende persoon.

In dit document beschrijven we hoe NetIQ Access Manager 3.2 als IdP of SP kan dienen voor SURFconext. Daarvoor hebben we de SSL-VPN en JAVA agent functionaliteiten niet nodig. De Access Gateway en Policies hebben we alleen nodig voor de configuratie van NetIQ Access Manager als SP, omdat we daarbij ook een achterliggende web service ontsluiten.

## 3. Hoe gaat het koppelen globaal in zijn werk?

### IdP

Om als IdP te koppelen moet in NetIQ Access Manager het volgende gebeuren:

1. Configureer een directory (User Store genoemd) aan de Identity Server. Deze wordt gebruikt voor de identiteiten waarmee ingelogd kan worden op diensten aan SURFconext.
2. Aan een Identity Server moet SURFconext als SAML 2.0 SP worden gekoppeld (en daarmee configureer je de Identity Server tevens als IdP). In feite wordt hierbij de SAML 2.0 metadata van SURFconext toegevoegd aan de NetIQ IdP configuratie.
3. Voeg het SURFconext 'token signing certificate' toe aan de 'Trusted Roots' van NetIQ Access Manager. Met deze certificaten worden straks SAML 2.0 berichten ondertekend, zodat we zeker weten ze van SURFconext komen en onderweg niet gewijzigd zijn.
4. Communiceer de eigen IdP metadata URL aan SURFnet, zodat deze in de configuratie van SURFconext kan worden opgenomen.
5. Er moet een attribute set en mapping worden aangemaakt voor de attributen die worden meegestuurd vanuit de IdP naar SURFconext.
6. Controle van de configuratie.

### SP

Om een applicatie te koppelen waarvoor NetIQ Access Manager als SP kan fungeren, zetten we eerst een test webapplicatie op.

Daarna zijn de volgende stappen nodig:

1. SURFconext als IdP toevoegen voor NetIQ Access Manager.
2. Een reverse proxy toevoegen voor de dienst die willen aanbieden.
3. Controle van de configuratie.

## 4. NetIQ Access Manager als Idp

### 4.1. User Store toevoegen

Ga naar 'Devices/Identity Servers/IDP-cluster' en ga naar de tab 'Local' en klik onder 'User Stores' op 'new'. Dat ziet er uit als in de onderstaande afbeelding:

Access Manager
Devices
Policies
Auditing
Security

Identity Servers > IDP-Cluster >

m7

Name: \* m7
Admin name: \* cn=admin,o=novell  
(Ex: cn=admin,o=novell)
Admin password: \* .....
Confirm password: \* .....
Directory type: eDirectory
☐ Install NMAS SAML method
☐ Enable Secret Store lock checking

**LDAP timeout settings**
LDAP Operation: 15 seconds
Idle Connection: 10 seconds

**Server replicas**
New | Delete | Validate 1 Item(s)

<input type="checkbox"/> Name	IP Address	Port	Use SSL	Max. Connections	Validation Status
<input type="checkbox"/> m7-directory	192.168.168.12	636	<input checked="" type="checkbox"/>	20	<input checked="" type="checkbox"/>

**Search Contexts**
New | Delete | 1 Item(s)

<input type="checkbox"/> Context	Scope
<input type="checkbox"/> o=m7	One Level

<< Back
Finish
Cancel

Vul de juiste gegevens in (in ons geval een eDirectory server van de organisatie 'm7') en klik op 'Finish'. Merk op dat we een eDirectory replica en een search context (de plek in de directory information tree waaronder iedereen zich bevindt die SURFconext moet kunnen gebruiken; hier kunnen er meerdere van worden opgegeven) hebben gedefinieerd.

Een belangrijke stap die niet vergeten mag worden is nu het updaten van de configuratie onder 'Devices/Identity Servers'. Zie de onderstaande afbeelding. Deze actie onderbreekt de services van Access Manager niet. Maar hij kan ook pas uitgevoerd worden nadat alle wijzigingen zijn aangebracht.

Access Manager
Devices
Policies
Auditing

Identity Servers

*i* Notice: Warning
Any changes to 'IDP-Cluster' will not take effect until the servers using this configuration are updated.

Servers
Shared Settings

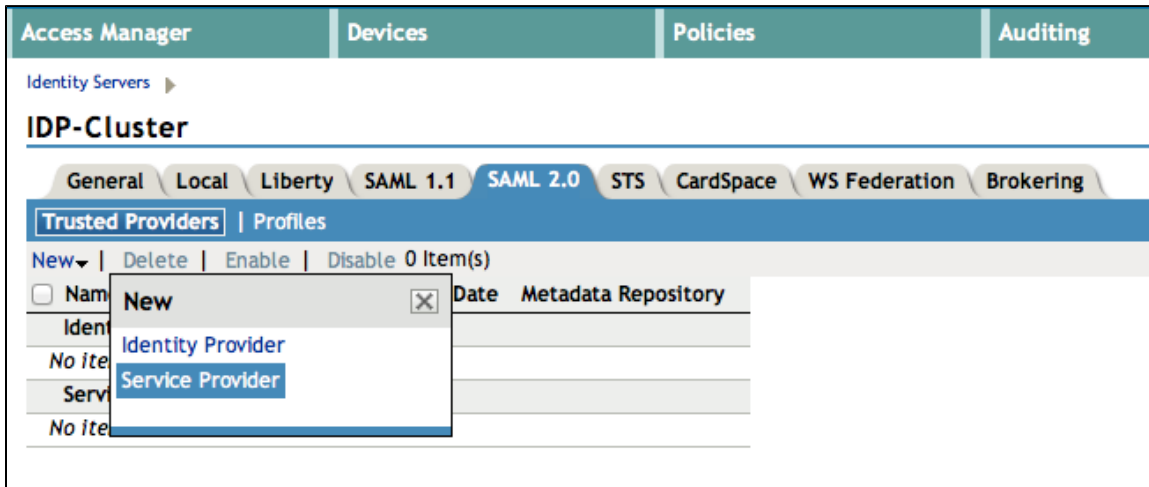
Start | Stop | Refresh | Actions 1 Item(s)

<input type="checkbox"/> Name	Status	Health	Alerts	Commands	Statistics	Type	Configuration
IDP-Cluster	Update All	<input checked="" type="checkbox"/>	0	<a href="#">View</a>	<a href="#">Edit</a>		<a href="#">Delete</a>
<input checked="" type="checkbox"/> 192.168.168.12	Update	<input checked="" type="checkbox"/>	0	<a href="#">Complete</a>	<a href="#">View</a>	Linux	

Update
☒ All Configuration (possible service interruption)  
- Configuration changed
☐ Logging Settings
☐ Policy Settings
OK
Cancel

## 4.2. SP toevoegen aan Identity Server

Ga naar 'Devices/Identity Servers/IDP-cluster'. Zorg dat in de tab 'General' onder 'Configuration' onderaan het vinkje bij SAML 2.0 is aangezet. Ga nu naar de tab 'SAML 2.0'. Kies nu 'new' en dan 'Service Provider' (zie onderstaande figuur).



Hiermee gaan we SURFconext als SP toevoegen door de metadata URL op te geven. Zie de figuur hieronder. De metadata URL is <https://metadata.surfconext.nl/idp-metadata.xml>.

Let op: controleer de URL eerst in een browser en controleer ook het SSL certificaat bij de URL (de browser geeft dit aan als u op het slotje klikt). Dit is belangrijk omdat in een later stadium u de metadata van SURFconext gaat gebruiken om een trust-relatie met SURFconext op te zetten.

The screenshot shows the 'Create Trusted Service Provider' form, Step 1 of 2: Specify name and metadata. The form has three main fields: 'Source' with a dropdown menu set to 'Metadata URL', 'Name' with a text input field containing 'SURFconext', and 'URL' with a text input field containing 'https://metadata.surfconext.nl/sp-metadata.xml'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Klik nu op 'Next'. Dan krijgen we (als het goed is) het volgende te zien:

Access Manager	Devices	Policies	Auditing	Sec
Identity Servers ► IDP-Cluster ►				
<b>Create Trusted Service Provider</b>				
<b>Step 2 of 2: Confirm certificates</b>				
<b>Signing Certificate</b>				
Subject: CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL				
Validity: 24 januari 2011 - 23 januari 2021				
Issuer DN: CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL				
Algorithm: SHA1withRSA				
Serial Number: cce2c6d5cc507d4d				
<input type="button" value=" &lt;&lt; Back"/> <input type="button" value=" Finish"/> <input type="button" value=" Cancel"/>				

Neem contact op met SURFnet als deze stap mislukt. Als het gelukt is, klik dan op 'Finish'.  
Daarna ziet u het volgende scherm:

Access Manager	Devices	Policies	Auditing
Identity Servers ►			
<b>IDP-Cluster</b>			
General   Local   Liberty   SAML 1.1   <b>SAML 2.0</b>   STS   CardSpace   WS Federation   Brokering			
<b>Trusted Providers</b>   Profiles			
New ▼   Delete   Enable   Disable 1 Item(s)			
<input type="checkbox"/>	Name	Enabled	Metadata Expiration Date Metadata Repository
<b>Identity Providers</b>			
No items			
<b>Service Providers</b>			
<input type="checkbox"/>	<a href="#">SURFconext</a>	✓	Not specified Not Applicable

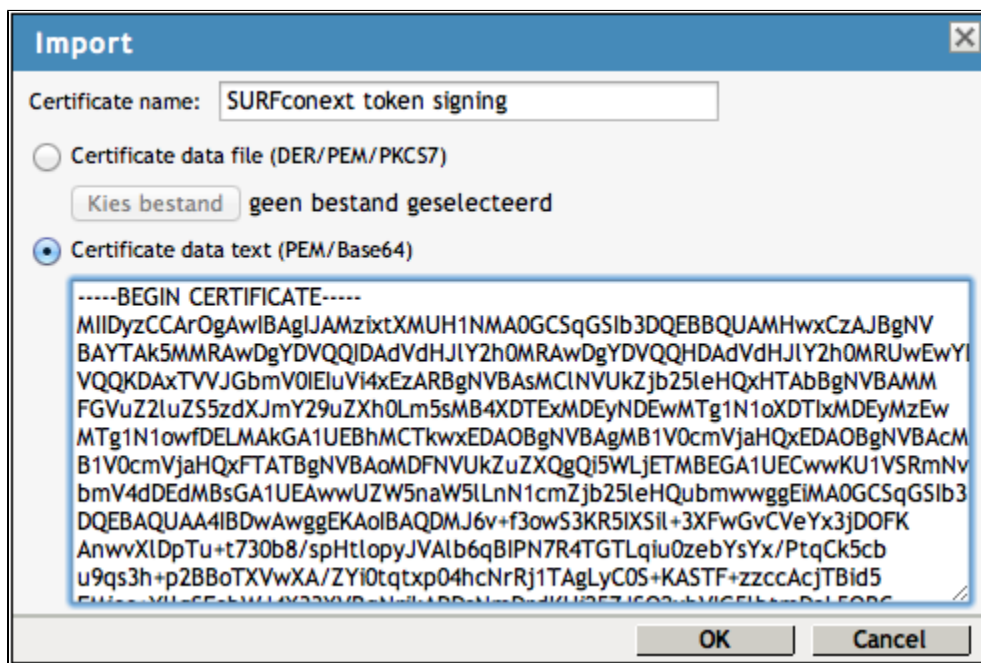
Update wederom de clusterconfiguratie zoals hierboven beschreven, of wacht daarmee tot de attributen geconfigureerd zijn (zie onder).

### 4.3. Voeg het token signing certificate van SURFconext toe

SURFnet gebruikt bij SURFconext zogenaamde self signed certificates voor het ondertekenen van de SAML 2.0 berichten. Self signed certificates bieden voldoende garantie omdat SURFconext geen publieke dienst is.

Ga naar 'Devices/Identity Servers/IDP-cluster'. Ga naar de tab 'SAML 2.0'. Klik op de zojuist aangemaakte SP (SURFconext genoemd in ons voorbeeld). Klik nu op de tab 'Metadata' en zoek het signing certificate. Zie de figuur hieronder.





Geef het certificaat een beschrijvende naam (hier dus 'SURFconext token signing') en selecteer 'Certificate data text' en plak hierin het gekopieerde certificaat. Let op: U bent niet klaar, want in de regel boven het certificaat moet staan '~~-----BEGIN CERTIFICATE-----~~' en in de regel onder het certificaat (niet in beeld in de figuur) '~~-----END CERTIFICATE-----~~'. Hiermee creëren we een geldig PEM certificaat, zoals NetIQ Access Manager het graag ziet.

Klik op 'OK'. Als alles goed is gegaan ziet u het onderstaande scherm:

Access Manager	Devices	Policies	Auditing	Security
<b>Certificates</b>				
Certificates   Trusted Roots   External Trusted Roots   Command Status				
Import...   Delete   Auto-Import From Server...				
<input type="checkbox"/> Name	Subject	Starting Date	Ending Date	
<input type="checkbox"/> configCA	O=netiqam_tree, OU=Organizational CA	12 november 2012	4 februari 2036	
<input checked="" type="checkbox"/> SURFconext token signing	CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL	24 januari 2011	23 januari 2021	

## 4.4. Communiceer de eigen IdP metadata URL aan SURFnet

Controleer of op de volgende URL inderdaad een geldige XML laat zien:

`https://<servernaam>/nidp/saml2/metadata`

Dit is metadata van de IdP en bevat alle informatie die nodig is om de IdP aan SURFconext toe te voegen.



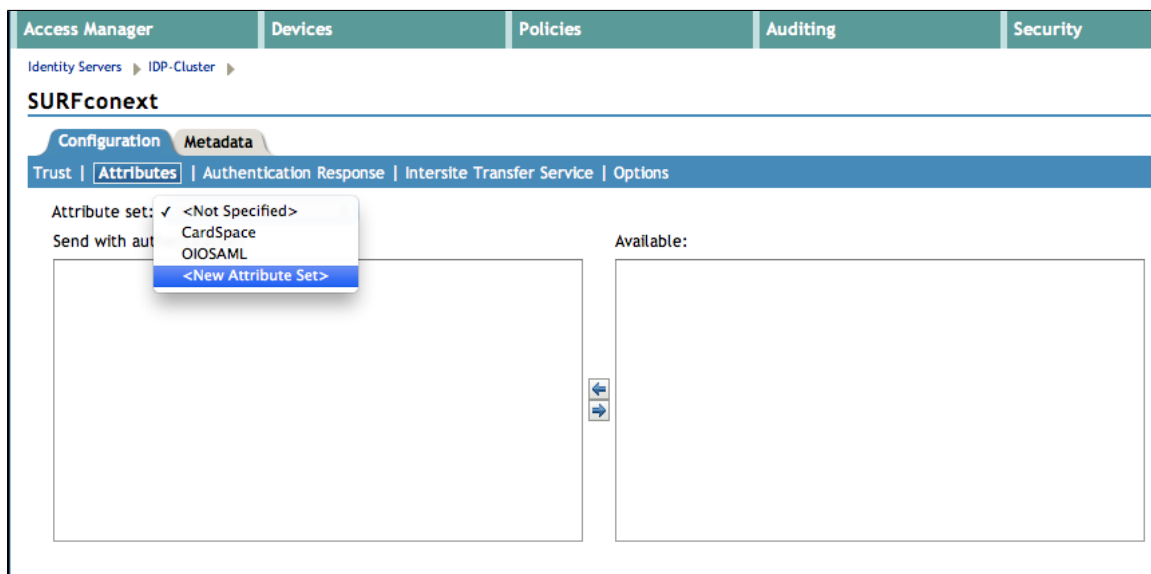
Deze URL dient ook voor SURFnet benaderbaar te zijn.

Geef deze URL aan SURFnet door (mail naar support@surfconext.nl) en wacht op bericht waarin SURFnet aangeeft dat de metadata is geconfigureerd. U kunt intussen wel verder met de overige stappen, behalve de laatste controle.

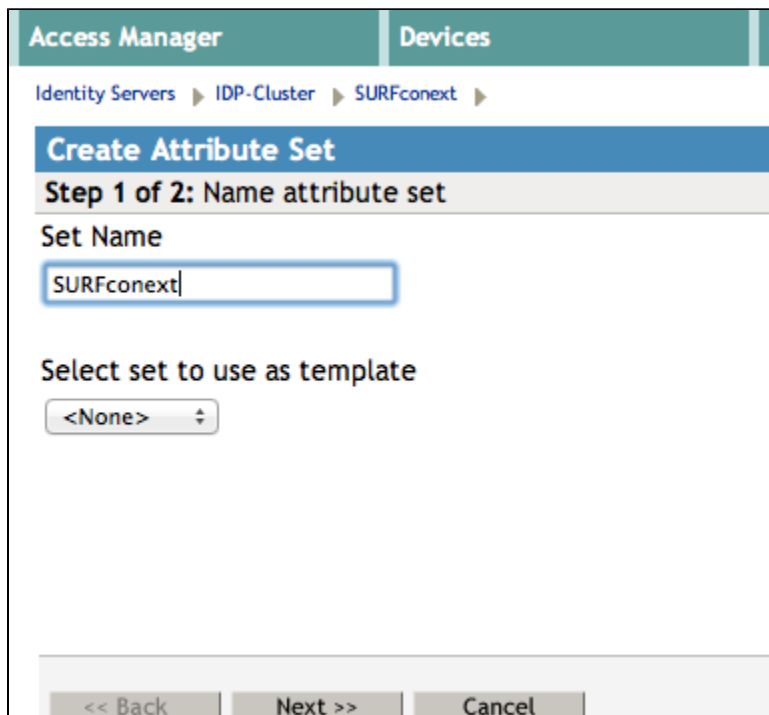
## 4.5. Maak een attributen set aan

Ga naar 'Devices/Identity Servers/IDP-cluster'. Ga naar de tab 'SAML 2.0'. Klik op de zojuist aangemaakte SP (SURFconext in ons voorbeeld). Klik onder de tab 'Configuration' op 'attributes' en kies bij het uittolmenu 'attribute set' voor '<New Attribute Set>'. Zie hieronder in de figuur:





Vervolgens gaan we een nieuwe attribute set aanmaken. Zie de volgende figuur:



Klik op 'Next' en vervolgens in het volgende scherm op 'New'.

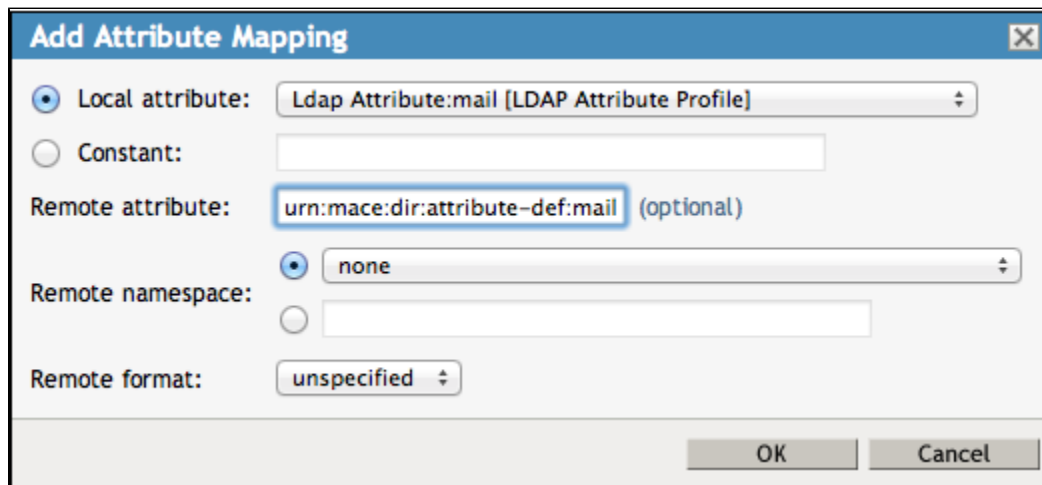
Voor SURFconext zijn conform de metadata de volgende attributen verplicht:

urn:mace:dir:attribute-def:mail  
 urn:mace:dir:attribute-def:displayName  
 urn:mace:dir:attribute-def:sn  
 urn:mace:dir:attribute-def:givenName  
 urn:mace:terena.org:attribute-def:schacHomeOrganization  
 urn:mace:dir:attribute-def:uid

De betekenis van deze attributen is te vinden op de attributenschema pagina van SURFnet: <https://wiki.surfnetlabs.nl/display/surfconextdev/Attributes+in+SURFconext>

We zullen in deze handleiding alleen de eerste mapping maken.

In het scherm dat we nu te zien krijgen (zie hieronder) kiezen we de local attribute waarde. Let op dat voor de meeste attributen een naam die in LDAP voorkomt gekozen moet worden (aangegeven met 'LDAP Attribute:').  
 Vul voor 'remote attribute' de volledige urn in zoals gespecificeerd op de SURFnet attributenschema pagina.



The 'Add Attribute Mapping' dialog box has the following fields:

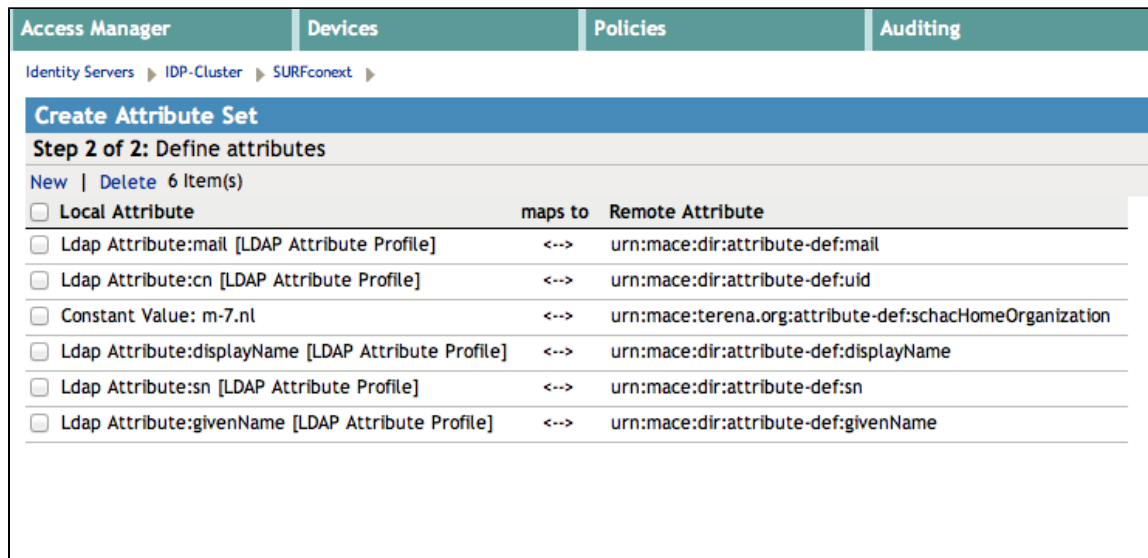
- Local attribute:** ☒ Local attribute:
- Constant:** ☐ Constant:
- Remote attribute:**
- Remote namespace:** ☒ none
- Remote format:**

Buttons: OK, Cancel

Klik op 'OK' en herhaal dit voor de overige attributen. Let erop dat u de attributen mapping zorgvuldig en correct kiest. Dus het locale attribuut bij 'urn:mace:dir:attribute-def:mail' moet voor iedereen daadwerkelijk wijzen naar een geldig e-mailadres. Verder merken we nog op dat voor schacHomeOrganization we een 'Constant' moeten kiezen met als waarde de domeinnaam van de IdP. In ons geval 'm-7.nl'.

Let er verder op dat bij een standaard installatie van eDirectory die wordt gebruikt als User Store meestal niet 'uid' wordt gebruikt als inlognaam maar 'cn'. Wij mappen dan ook het LDAP attribuut 'cn' op urn:mace:dir:attribute-def:uid.

In onze situatie krijgen we uiteindelijk het volgende te zien:



The 'Create Attribute Set' interface shows the following table of attribute mappings:

<input type="checkbox"/> Local Attribute	maps to	Remote Attribute
<input type="checkbox"/> Ldap Attribute:mail [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:mail
<input type="checkbox"/> Ldap Attribute:cn [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:uid
<input type="checkbox"/> Constant Value: m-7.nl	<-->	urn:mace:terena.org:attribute-def:schacHomeOrganization
<input type="checkbox"/> Ldap Attribute:displayName [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:displayName
<input type="checkbox"/> Ldap Attribute:sn [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:sn
<input type="checkbox"/> Ldap Attribute:givenName [LDAP Attribute Profile]	<-->	urn:mace:dir:attribute-def:givenName

Als we nu op 'Next' klikken, kunnen we kiezen welke attributen uit de set we willen gebruiken voor deze SURFconext SP. Zie de figuur hieronder:

Access Manager | Devices | Policies | Auditing | Security

Identity Servers > IDP-Cluster >

### SURFconext

Configuration | Metadata

Trust | **Attributes** | Authentication Response | Intersite Transfer Service | Options

Attribute set: SURFconext

Send with authentication:

Constant Value: m-7.nl

Available:

- Ldap Attribute:cn [LDAP Attribute Profile]
- Ldap Attribute:displayName [LDAP Attribute Profile]
- Ldap Attribute:givenName [LDAP Attribute Profile]
- Ldap Attribute:mail [LDAP Attribute Profile]
- Ldap Attribute:sn [LDAP Attribute Profile]

In bovenstaand voorbeeld moeten alle attributen links komen te staan (bij 'Send with authentication').

Uiteindelijk updaten we de clusterconfiguratie onder 'Devices/Identity Servers'. Vergeet deze stap niet!

## 4.6. Compatibiliteitsproblemen met diensten

Er is bekend dat er compatibiliteitsproblemen zijn tussen NetIQ AM als IdP en SPs welke werken met Microsoft (.Net). Deze problemen worden veroorzaakt door het anders interpreteren van de SAML2.0 specificatie. Volgens Microsoft kan een URI alleen een absolute URI (zie [wikipedia](https://en.wikipedia.org/wiki/URI) voor uitleg over URIs) zijn terwijl NetIQ AM ook gebruik maakt van URI verwijzingen (zoals ook mogelijk is volgens de SAML2.0 en XSD specificatie). Om deze problemen voor te zijn adviseren wij om het authenticatie contract van de NetIQ AM IdP aan te passen.

Het aanpassen van authenticatie contract voor het aanpassen van een URI-verwijzing naar een absolute URI kunnen de volgende stappen uitgevoerd worden:

Ga naar 'Devices/Identity Servers/IDP-cluster' en ga naar de tab 'Local' en klik onder 'Contracts' op 'new'.

Access Manager | Devices | Policies | Auditing | Security

Identity Servers >

### IDP-Cluster

General | **Local** | Liberty | SAML 1.1 | SAML 2.0 | STS | CardSpace | WS Federation | Brokering

User Stores | Classes | Methods | **Contracts** | Defaults

New | Delete

Name	URI	Level
<a href="#">Name/Password - Basic</a>	basic/name/password/uri	0
<a href="#">Name/Password - Form</a>	name/password/uri	0
<a href="#">Secure Name/Password - Basic</a>	secure/basic/name/password/uri	0
<a href="#">Secure Name/Password - Form</a>	secure/name/password/uri	0

OK Cancel Apply

Vul de gegevens in als onderstaand plaatje:

Access Manager | Devices | Policies | Auditing | Security

Identity Servers > IDP-Cluster >

### Create Authentication Contract ?

**Step 1 of 2: Configuration**

Display name:

URI:

Password expiration servlet:

☐ Allow user interaction

Authentication Level:

Authentication Timeout:  Minutes

Activity Realm(s):

☐ Satisfiable by a contract of equal or higher level

☐ Satisfiable by External Provider

Requested By:

Allowable Class:


If you add more than one X509 method, only the first one will be used and it will automatically be moved to the top of the list.

Methods:

Available methods:

- 
- 
- 

<< Back | Next >> | Cancel

Vergeet niet de Method 'Name/Password - Form' aan te klikken en vervolgens op de  te klikken.

Klik op 'Next'

Vul bij Text in: Name/Password - Form URI

Selecteer image: Form Auth Username Password

Access Manager | Devices | Policies | Auditing | Security

Identity Servers > IDP-Cluster >

### Create Trusted Identity Provider ?

**Step 2 of 2: Enter authentication card values**


ID:

Text:

Image:

☒ Show Card

☐ Passive Authentication Only



<< Back | Finish | Cancel

Klik op 'Finish'

Stel nu deze nieuwe Authenticatie Contract in als de Default Authenticatie Contract.

Ga naar tab: 'Defaults'

Selecteer bij Authentication Contract de nieuwe 'Name/Password - Form URI' contract.

Access Manager | Devices | Policies | Auditing | Security

Identity Servers ▸

### IDP-Cluster

General | Local | Liberty | SAML 1.1 | SAML 2.0 | STS | CardSpace | WS Federation | Brokering

User Stores | Classes | Methods | Contracts | **Defaults**

Defaults

User Store: SingleBoxUserStore ▾

Authentication Contract: Name/Password - Form URI ▾

Authentication Type	Default Contract
Name Password:	<None> ▾
Secure Name Password:	<None> ▾
X509:	<None> ▾
Smart Card:	<None> ▾
Smart Card PKI:	<None> ▾
Token:	<None> ▾

OK Cancel Apply

Klik op 'OK'

Uiteindelijk updaten we de clusterconfiguratie onder 'Devices/Identity Servers'. Vergeet deze stap niet!

## 4.7. Controle van de configuratie

Nadat u van SURFnet bevestiging heeft ontvangen dat uw metadata is toegevoegd, kunt u uw nieuwe IdP gaan testen op een test SP. Hiervoor heeft SURFnet de volgende URLs beschikbaar:

<https://engine.surfconext.nl/authentication/sp/debug>

U heeft een test-koppeling zolang u de bijlage bij het SURFnet contract voor SURFconext nog niet ondertekend terug gestuurd heeft naar SURFnet. Daarna heeft u automatisch een productiekoppeling.

## 5. NetIQ Access Manager als SP

Om als SP te kunnen koppelen hebben we een applicatie nodig die we gaan aanbieden op SURFconext. Deze applicatie moet vanaf NetIQ Access Manager via een URL bereikbaar zijn. In ons voorbeeld heeft de applicatie de URL <http://namsp/> en is bereikbaar op (private) IP-adres 192.168.168.5.

Let op dat de hier vermelde instructies zeer specifiek zijn voor een bepaalde (test)situatie. U zult dus zelf moeten nagaan waar uw situatie afwijkt. We raden u aan een expert in te schakelen als u denkt zelf onvoldoende ervaring te hebben.

### 5.1. SURFconext als IdP toevoegen

We gaan nu SURFconext als IdP toevoegen. Ga naar 'Devices/Identity Servers/IDP-cluster'. Ga naar de tab 'SAML 2.0'. Klik nu op 'New' en kies voor 'Identity Provider'. Zie de figuur hieronder:

Access Manager | Devices | Policies | Auditing

Identity Servers ▸

## IDP-Cluster

General | Local | Liberty | SAML 1.1 | SAML 2.0 | STS | CardSpace | WS Federation | Brokering

Trusted Providers | Profiles

New ▾ | Delete | Enable | Disable 1 Item(s)

	Expiration Date	Metadata Repository
<input type="checkbox"/> New		
<input type="checkbox"/> Identity Provider		
<input type="checkbox"/> Service Provider		
<input type="checkbox"/> ...	... November 2012	Not Applicable

Vervolgens vullen we een naam en de volgende metadata URL in:

<https://metadata.surfconext.nl/idp-metadata.xml>

Access Manager | Devices | Policies

Identity Servers ▸ IDP-Cluster ▸

## Create Trusted Identity Provider

### Step 1 of 3: Specify name and metadata

Source: Metadata URL ▾

Name: \* SURFconext

URL: \* <https://metadata.surfconext.nl/idp-metadata.xml>

Klik nu op 'Next'. U krijgt het volgende te zien als alles is goed gegaan:

Access Manager | Devices | Policies | Auditing

Identity Servers ▸ IDP-Cluster ▸

## Create Trusted Identity Provider

### Step 2 of 3: Confirm certificates

#### Signing Certificate

Subject: CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL

Validity: 24 januari 2011 - 23 januari 2021

Issuer DN: CN=engine.surfconext.nl, OU=SURFconext, O=SURFnet B.V., L=Utrecht, ST=Utrecht, C=NL

Algorithm: SHA1withRSA

Serial Number: cce2c6d5cc507d4d

Klik nu op 'Next'. Nu gaan we een inlog 'card' aanmaken. In het volgende scherm vullen we bij ID 'SURFconext' in en kiezen we een afbeelding bij 'Image'. Er zijn er een aantal standaard aanwezig en we kunnen er ook zelf één uploaden. We voegen geen 'Authentication contracts' aan 'Satisfies contract' toe vanuit de 'Available contracts'.

Nu klikken we op 'Finish'.

Klik nu op SURFconext onder Identity Provider in het IDP overzichtsscherm ('Devices/Identity Servers/IDP-cluster'). Klik op de tab 'Authentication Card' en kies vervolgens 'Authentication Request'. Selecteer hier onder 'Name Identifier Format' voor 'Transient'.

Ga nu terug naar de tab 'Configuration' en selecteer 'Attributes'. Kies de SURFconext attribute set die eerder is aangemaakt bij het toevoegen van NetIQ Access Manager als IdP hierboven. En kies daarna alle attributen om ze als beschikbaar toe te voegen (zie hierboven).

Ga nu naar 'User Identification' en zorg dat daar 'Attribute matching' **niet** is aangeklikt. Dit zorgt ervoor dat de federatief geauthenticeerde gebruiker niet tegen de lokale directory gematched zal worden.

## 5.2. Een reverse proxy toevoegen

Ga naar 'Devices/Access Gateways/AG-Cluster/NAM-RP'. Dan komen we op het volgende scherm:

Access Manager | Devices | Policies | Auditing | Security

Servers > Configuration >

### Reverse Proxy: AG-Cluster - NAM-RP

Cluster Member: 192.168.168.12

Listening Address(es): ☒ 192.168.168.12

[TCP Listen Options](#)

☒ Enable SSL with Embedded Service Provider  
☒ Enable SSL between Browser and Access Gateway  
☒ Redirect Requests from Non-Secure Port to Secure Port

Server Certificate:

[Auto-generate Key](#)

Non-Secure Port:  (Redirected to Secure Port)

Secure Port:  (Used for Trusted IDS Encryption, HTTPS Listening)

#### Proxy Service List

Name	Enabled	Multi-Homing	Published DNS Name	Web Server Addresses	HTML Rewriting
<input type="checkbox"/> NAM-Service	<input checked="" type="checkbox"/>		netiqam	192.168.168.12 : 8443	<a href="#">default</a>
<input type="checkbox"/> _namportal	<input checked="" type="checkbox"/>	Path-Based	netiqam	192.168.168.12 : 8443	<a href="#">default</a>
<input type="checkbox"/> _solvsn	<input checked="" type="checkbox"/>	Path-Based	netiqam	127.0.0.1 : 3443	<a href="#">default</a>

Klik op 'New' en vul de gegevens in zoals hieronder:

### New Proxy Service

Proxy Service Name:

Multi-Homing Type:

Published DNS Name:

Path:

Web Server IP Address:

Host Header:

Web Server Host Name:

(Alternate Host Name)

Geef de reverse proxy een naam (hier 'Test-SP'). Deze naam is alleen maar een beschrijving in de configuratie. Hier kiezen we voor een 'Path-Based' reverse proxy. Dat betekent dat de dienst onder dezelfde hostnaam als de NetIQ Access Manager beschikbaar is op internet. Als dat anders moet, dan kunt u hier ook voor 'Domain Based' kiezen.

De 'Published DNS Name' is hier de hostnaam van de NetIQ Access Manager en al voor ons ingevuld en kan niet aangepast worden.

Het 'Web Server IP Address' is het IP-adres waarop de NetIQ Access Manager reverse proxy de dienst die we gaan beschikbaar stellen kan bereiken.

Het 'Path' veld is in dit geval het pad in de URL waaronder de dienst beschikbaar wordt gemaakt. In ons geval wordt de URL daarmee <https://netiqam/namsp>.

De 'Host Header' wordt gebruikt om onderscheid te kunnen maken voor de achterliggende website (bijvoorbeeld 'vhost' in de Apache webserver). We kunnen hier kiezen voor het doorsturen van de hostnaam van de NetIQ Access Manager ('Forward Received Hostname') of voor het doorsturen van een zelf gekozen naam ('Web Server Host Name'). Dat doen we hier en de naam die we hier kiezen is 'namsp'.

Klik op 'OK'.

Aan de configuratie in het overzichtsscherm is nu de volgende regel toegevoegd:



Indien u nu in hier op Test-SP klikt kunt u nog specifieke instellingen aanbrengeen. Het is afhankelijk van de dienst welke nodig zijn.

Klik nu in het overzichtsscherm op 'NAM-Service' (de overkoepelende configuratie voor de nieuwe reverse proxy). Ga nu naar de tab 'Protected Resources'. Dan komen we in het volgende scherm:

Access Manager
Devices
Policies
Auditing
Security

Servers
Configuration
Reverse Proxy

### Protected Resources: AG-Cluster - NAM-RP - NAM-Service

Proxy Service
Web Servers
HTML Rewriting
Protected Resources
Logging

**Note:** Wildcard URL paths (/\*) for resources using form fill policy are performance intensive. To improve the performance, replace any high performance Web Server Resources being made Public or being Protected by an Authentication Procedure and/or Authorization Policies.

Select the Policy View to see which Protected Resources are using each Policy. Click the "Used By" link (on the Policy View) to assign a Policy to

Resource View

#### Protected Resource List

New...	Delete	Enable	Disable			
<input type="checkbox"/> Name		Enabled	URL Paths	Authentication Procedure	Authorization	Identity Injection
<input type="checkbox"/> nesp		✓	1 Paths	[None]	[None]	[None]
<input type="checkbox"/> nidp		✓	1 Paths	[None]	[None]	[None]
<input type="checkbox"/> portal		✓	2 Paths	Any Contract	[None]	basic_auth, ... (2)
<input type="checkbox"/> portal_public		✓	1 Paths	[None]	[None]	[None]
<input type="checkbox"/> sslvpn		✓	1 Paths	Any Contract	[None]	SSLVPN_Default
<input type="checkbox"/> sslvpn_public		✓	1 Paths	[None]	[None]	[None]

Klik in dit scherm op 'New'. En vul een naam in en klik op 'OK'.

New

Name:

OK
Cancel

In het volgende scherm vullen we een beschrijving in en een URL. dat moet hetzelfde zijn als we eerder hebben ingevuld, namelijk namsp. Hiermee gaan we authenticatie afdwingen voor alles wat zich achter dit pad bevindt.

Access Manager
Devices
Policies
Auditing

Servers
Configuration
Reverse Proxy
Protected Resources

Overview: AG-Cluster - NAM-RP - NAM-Service - Test-SP

Overview
Authorization
Identity Injection
Form Fill

Protected Resource: Test-SP  
Description: beveiliging van Test-SP  
Authentication Procedure: [None]

URL Path List
New... | Delete
1 item(s)

URL Path
<input type="checkbox"/> /namp/*

Server(s) must be updated before changes made on this panel will be used. See [Configuration](#) Panel for summary of changes.

OK
Cancel

Nu gaan we naar de tab 'Identity injection' en we vinken 'basic\_auth' aan en klikken op 'Enable'. Dit geldt alleen als de achterliggende applicatie basic authentication aan kan.

Access Manager
Devices
Policies

Servers
Configuration
Reverse Proxy
Protected Resources

Identity Injection: AG-Cluster - NAM-RP - NAM-Service - Test-SP

Overview
Authorization
Identity Injection
Form Fill

Identity Injection Policies enabled for this Resource definition.

Identity Injection Policy List
Manage Policies | Enable | Disable

Name	Enabled	Policy Container	Description
<input checked="" type="checkbox"/> <a href="#">basic_auth</a>	Enable	Master_Container	
<input type="checkbox"/> <a href="#">fillRole</a>		Master_Container	
<input type="checkbox"/> <a href="#">SSLVPN_Default</a>		Master_Container	

Klik op de link 'basic\_auth'. Dan verschijnt het volgende scherm:

Policies ▸

**Edit Policy: basic\_auth** ?

Type: Access Gateway: Identity Injection

Description:

Rule List					
New	Delete	Copy	Enable	Disable	1 item(s)
<input type="checkbox"/>	Rule	Priority	Enabled	Action	Description
<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>	Inject into Authentication Header	

Changes made on this panel must be applied from the [Policies](#) Panel.

We klikken nu op '1' onder 'Rule' en gaan daarmee de injection aanpassen.

We passen de configuratie aan zodat het LDAP attribuut 'cn' op de authentication header user name wordt afgebeeld. We hebben eerder namelijk in de attribute mapping (zie NetIQ Access Manager als IdP) aangegeven dat 'cn' voor SURFconext de gebruikersnaam (uid) is. We gebruiken hier een dummy password.

Policies ▸ Edit Policy ▸

**Edit Rule: basic\_auth - Rule 1**

Type: Access Gateway: Identity Injection

Description:

Priority:

Actions	
New ▾	
Do	Inject into Authentication Header
User Name:	LDAP Attribute ▾ : cn ▾ Refresh Data Every: Session ▾
Password:	String Constant ▾ : <input type="text" value="FooPass"/>
Multi-Value Separator:	, ▾
DN Format:	LDAP (ex, cn=jsmith,ou=Sales,o=Novell) ▾

Changes made on this panel must be applied from the [Policies](#) Panel.

Klik op 'OK', sluit alle schermen door op 'OK' of 'Close' knoppen te klikken (sluit nooit een scherm vanuit de browser). Update nu de configuratie.

## 5.3. Controle

Ga nu als gebruiker naar de URL die hoort bij de reverse proxy voor de dienst. In ons geval <https://netiqam/namsp>. We hebben hier de volgende PHP pagina achter gezet:

```
<?php
phpinfo();
?>
```

De output ziet er dan als volgt uit:

_SERVER["REMOTE_PORT"]	43160
_SERVER["GATEWAY_INTERFACE"]	CGI/1.1
_SERVER["SERVER_PROTOCOL"]	HTTP/1.1
_SERVER["REQUEST_METHOD"]	GET
_SERVER["QUERY_STRING"]	<i>no value</i>
_SERVER["REQUEST_URI"]	/
_SERVER["SCRIPT_NAME"]	/index.php
_SERVER["PHP_SELF"]	/index.php
_SERVER["PHP_AUTH_USER"]	joe
_SERVER["PHP_AUTH_PW"]	FooPass
_SERVER["REQUEST_TIME"]	1356103099

Hierin zijn de geauthenticerde gebruiker en het door ons aangebrachte dummy wachtwoord te herkennen in de PHP server variabelen: PHP\_AUTH\_USER en PHP\_AUTH\_PW.