SURFFEDERATIE HANDLEIDING AD FS 2.0

VOOR AANSLUITING ALS IDENTITY PROVIDER

versie 2.0, 15 juli 2010

SURFNET BV, RADBOUDKWARTIER 273, POSTBUS 19035, 3501 DA UTRECHT
T +31 302 305 305, F +31 302 305 329, WWW.SURFNET.NL

INHOUD

1. INLEIDING

Als organisatie kunt u aansluiten op de SURFfederatie met het protocol Active Directory Federation Services 2.0 (AD FS 2.0) van Microsoft. U kunt aansluiten op twee manieren:

- als Identity Provider (IDP), in AD FS-terminologie 'Account Partner' (AP) genoemd. Bent u IDP, dan is de Active Directory van uw organisatie ontsloten naar de SURFfederatie. Hierdoor kunnen gebruikers in uw Active Directory zich authenticeren voor diensten binnen de SURFfederatie.
- als Service Provider (SP), in AD FS-terminologie 'Resource Partner' (RP) genoemd. In deze rol kunt u als organisatie ook diensten aanbieden via de SURFfederatie.

In deze handleiding leest u hoe u uw organisatie aansluit in de rol van Identity Provider, de rol die voor de meeste instellingen van toepassing zal zijn.

De procedure voor het aansluiten als IDP bestaat uit de volgende onderdelen:

1. Een AD FS 2.0-serversysteem inrichten, o.a. Windows Server 2008 configureren en AD FS 2.0 installeren (hoofdstuk 2)
2. De AD FS 2.0-server configureren voor aansluiting als Identity Provider voor de SURFfederatie (hoofdstuk 3)
3. Een AD FS 2.0 proxy inrichten (hoofdstuk 4)
4. Attributen vrijgeven aan de SURFfederatie (hoofdstuk 5)

1.1 Meer informatie over AD FS 2.0

AD FS 2.0 (codenaam Geneva Server) is de opvolger van AD FS v1 zoals oorspronkelijk beschikbaar op Windows Server 2003 R2 en Windows Server 2008. De belangrijkste wijziging ten opzichte van AD FS v1 is de ondersteuning van het SAML 2.0 protocol. Meer informatie over AD FS 2.0 is hier te vinden:

http://www.microsoft.com/windowsserver2008/en/us/ad-fs-2-overview.aspx

Deze handleiding is gebaseerd op de release van AD FS 2.0 (5 mei 2010). Meer informatie over de installatie van AD FS 2.0 is hier te vinden:

http://technet.microsoft.com/en-us/library/adfs2(WS.10).aspx

Voor een step-by-step guide van Microsoft, wellicht handig als naslagwerk naast deze handleiding, zie:

http://technet.microsoft.com/en-us/library/ff631096(WS.10).aspx

1.2 Waarom server en proxy?

Naast het inrichten van een AD FS 2.0-server is het noodzakelijk om 'voor' de AD FS-server, buiten het Windows-domein, een AD FS-proxy in te richten die het verkeer van buitenaf doorstuurt naar de AD FS-server. Dit houdt in dat er 2 verschillende Windows Server 2008 machines geconfigureerd worden in deze setup.

Dit heeft de volgende reden: de AD FS-server moet in het Windows-domein worden opgenomen en daarom liever niet direct bereikbaar zijn van buitenaf. Door een AD FS-proxy in te richten en deze voor de AD FS-server te plaatsen, **buiten het Windows-domein**, is de AD FS-server minder kwetsbaar voor aanvallen van buitenaf.

Bijkomend voordeel is dat een proxy kan worden geconfigureerd om een loginpagina met de look-and-feel van de instelling te tonen aan de gebruiker, in plaats van de standaard popup-prompt die de AD FS-server laat zien. Dit verbetert de herkenbaarheid van de login voor de eindgebruiker en biedt de mogelijkheid extra informatie aan de gebruiker te tonen. Daarnaast kan phishing beter worden voorkomen door het door het toepassen van een geldig SSL-servercertificaat.

1.3 Auteurs

Deze handleiding is tot stand gekomen door bijdragen van Paul Lemmers (DevCon), Jan Michielsen (bureau Hendrikx Van der Spek), Remco Poortinga (SURFnet bv) en Hans Zandbelt (SURFnet bv).

2. AD FS 2.0-SERVER INRICHTEN

2.1 Inleiding

Voordat u de specifieke instellingen voor de SURFfederatie kunt invoeren, moet u een basisinstallatie op de AD FS 2.0-server uitvoeren. Dat gaat in de volgende stappen:

1. Windows Server 2008 installeren en configureren (paragraaf 2.1)
2. De AD FS 2.0-software installeren (paragraaf 2.2)
3. Basisinstellingen van AD FS 2.0 configureren (paragraaf 2.3)

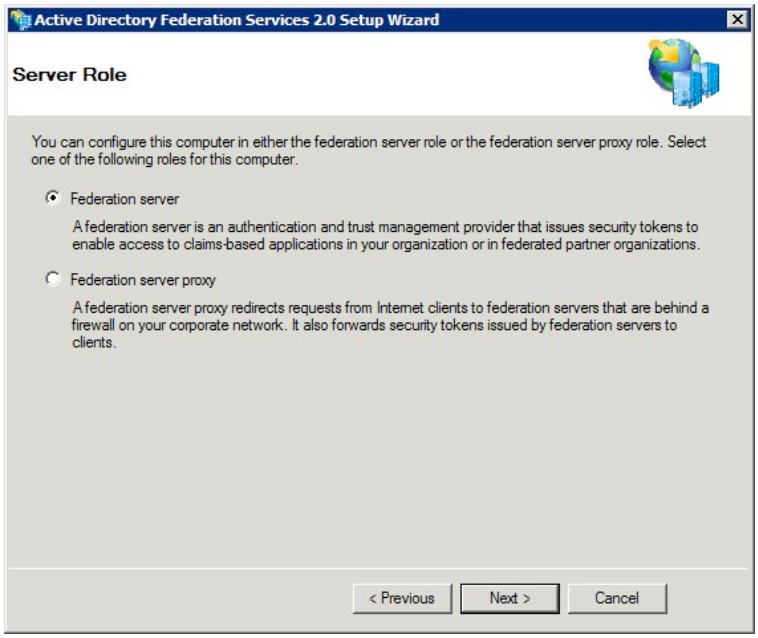
2.2 Windows Server 2008 installeren en configureren

Om een AD FS 2.0-server te kunnen inrichten, moet u eerst Windows Server 2008 installeren en configureren:

- Installeer de juiste versie van het besturingssysteem op de server: Windows Server 2008 SP2 of Windows Server 2008 R2 (standaard of enterprise).
- Stel de tijd op de server correct in zorg dat deze wordt gesynchroniseerd met een time server.
- Neem de server op in het domein van de Active Directory waaruit de accounts voor de federatie komen.
- Installeer Internet Information Services (IIS) en zorg dat deze een geldig SSL-servercertificaat heeft. U kunt servercertificaten (onder meer) verkrijgen via de SURFcertificaten-dienst van SURFnet: http://www.surfnet.nl/nl/diensten/authenticatie/Pages/certificaten.aspx

2.3 AD FS 2.0-software installeren

1. Download AD FS 2.0 Server via http://go.microsoft.com/fwlink/?linkid=151338 voor uw platform (Windows Server 2008 SP2 of 2008 R2, 32 of 64 bits) en start de executable.
2. Doorloop het begin van de procedure en accepteer de licentieovereenkomst.

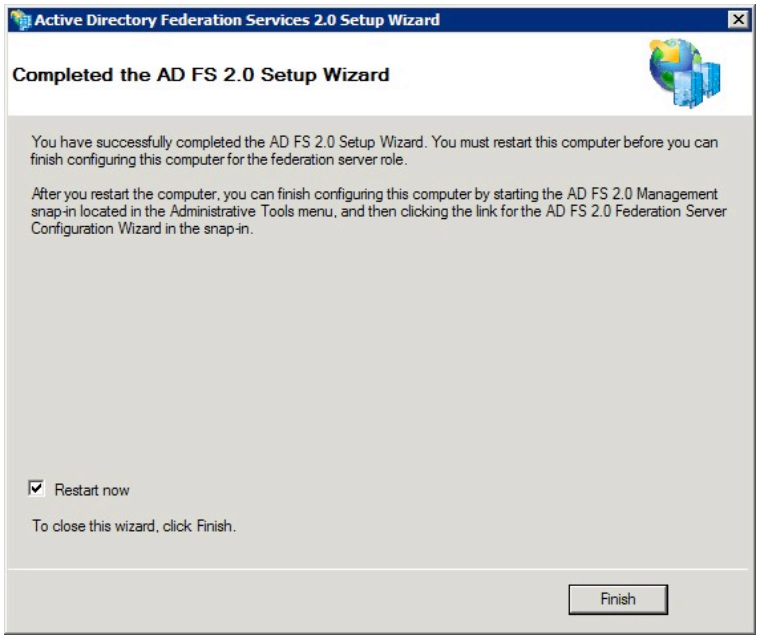


3. Selecteer **Federation server** en klik op **Next**.

   De eigenlijke installatie begint nu.

4. Volg de stappen in de wizard.

   Nadat de software is geïnstalleerd, verschijnt het volgende venster:

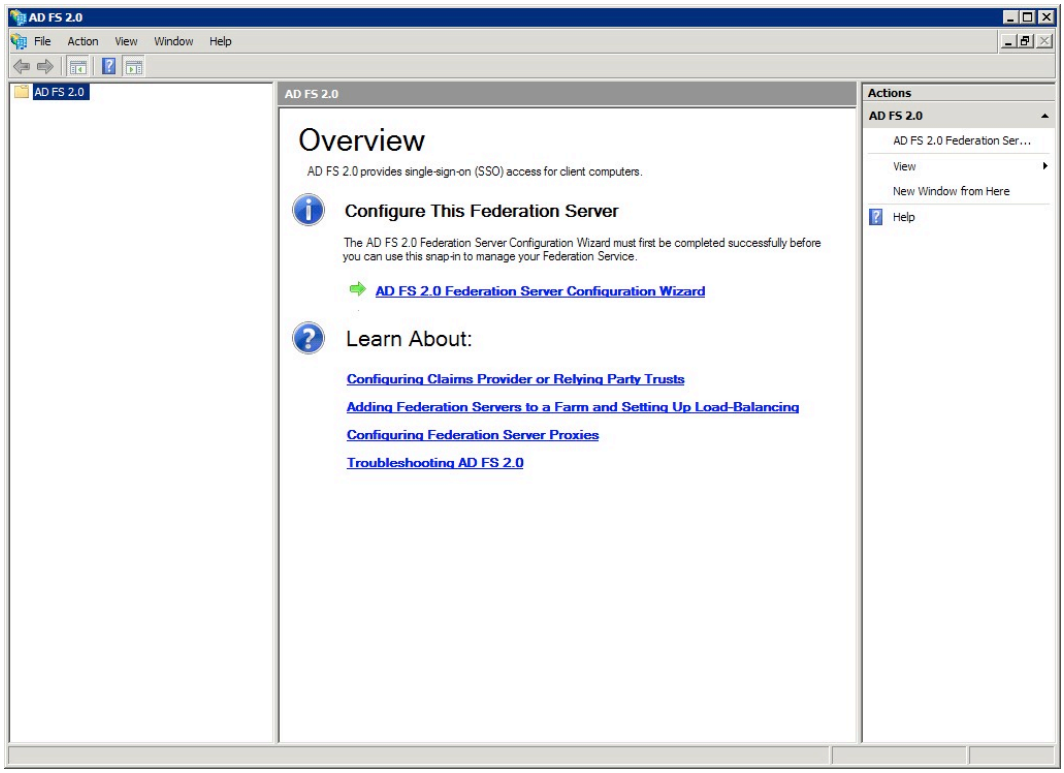


5. Zorg dat **Restart now** aangevinkt is en klik op **Finish**.

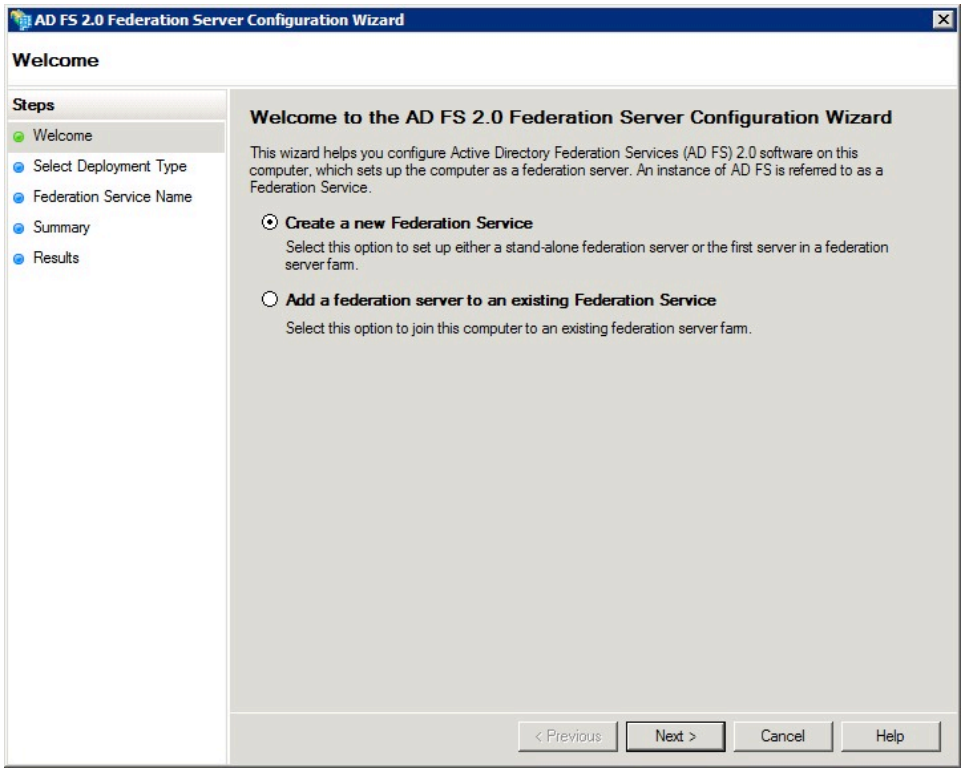
   De server start opnieuw op. Hiermee is de basisinstallatie van de AD FS 2.0-software afgerond.

2.4 Basisinstellingen AD FS 2.0 configureren

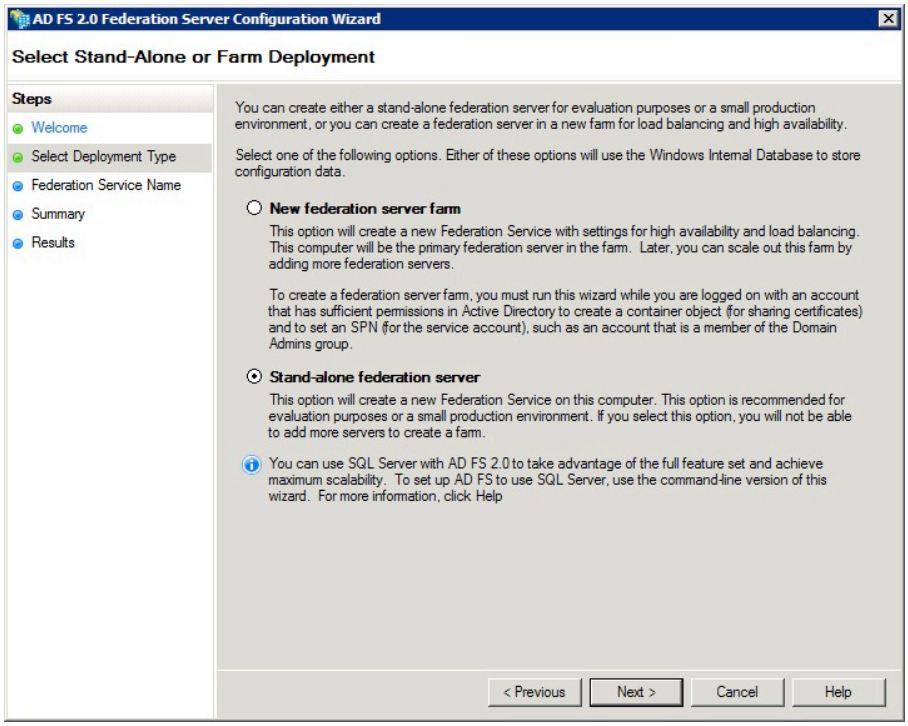
1. Kies **Start > All Programs > Administrative Tools > AD FS 2.0 Management** om de AD FS 2.0-configuratieapplicatie te starten.



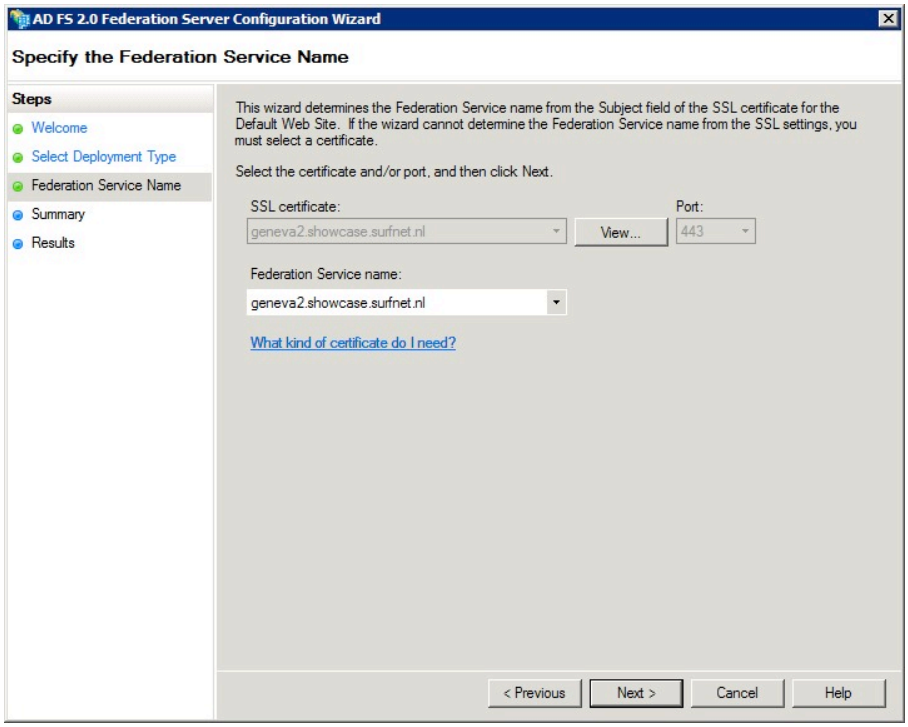
2. Klik op **AD FS 2.0 Federation Server Configuration Wizard**.



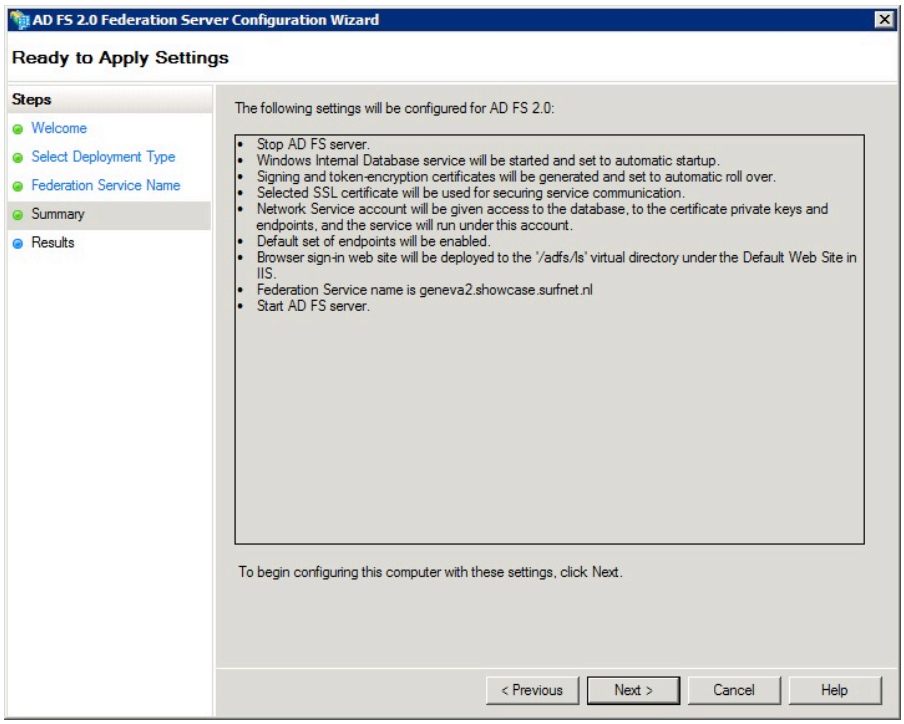
3. Selecteer **Create a new Federation Service** en klik op **Next**.



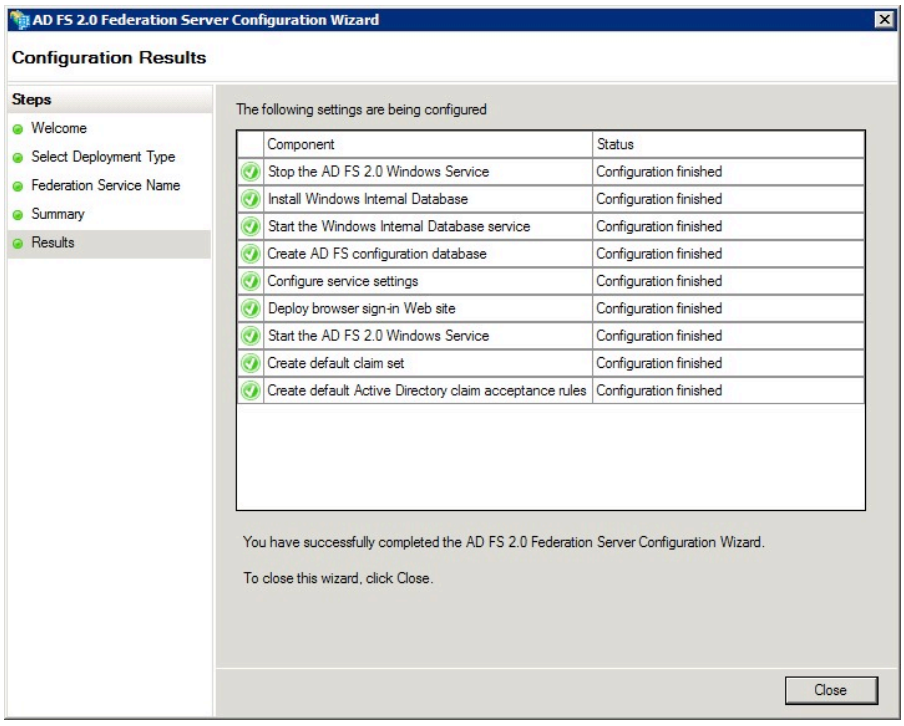
4. Selecteer **Stand-alone federation server** en klik op **Next**.



5. In het veld 'Federation Service name' is de hostnaam van uw server al ingevuld. Laat deze ongewijzigd en klik op **Next**.



6. Klik op **Next** om de ingestelde settings toe te passen.



7. Klik op **Close** als het configuratieproces is afgerond.

Hiermee is ook de basisinstallatie van de AD FS 2.0-server afgerond.

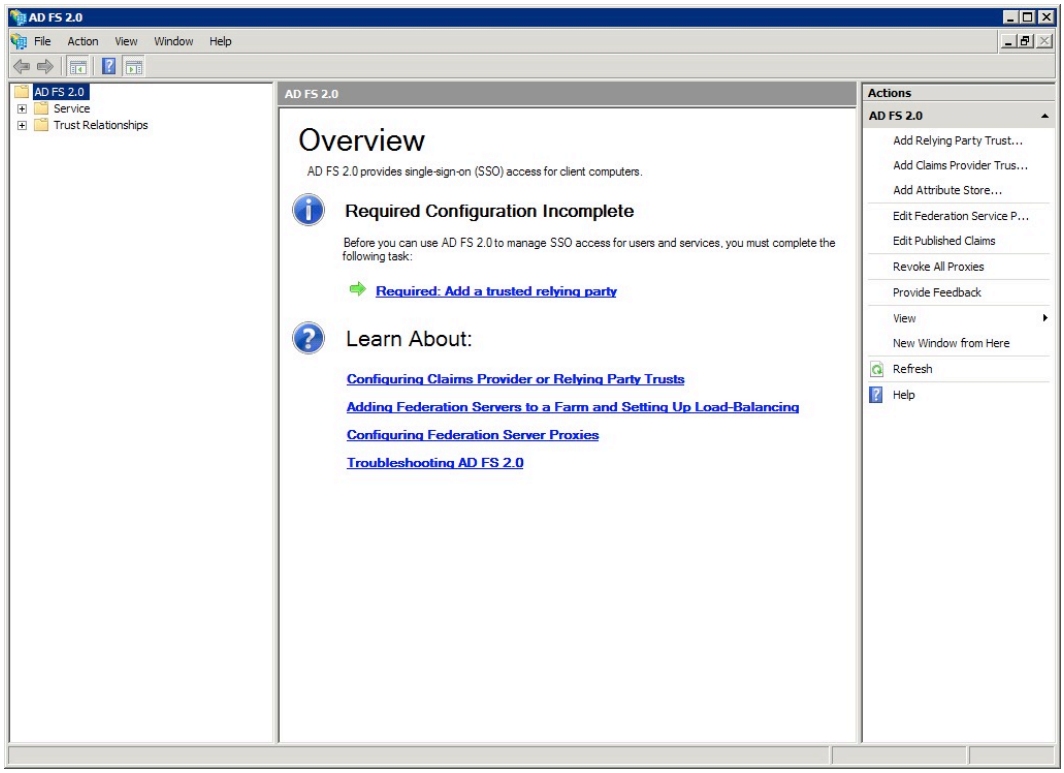
3. AD FS 2.0-SERVER CONFIGUREREN ALS IDENTITY PROVIDER

3.1 Inleiding

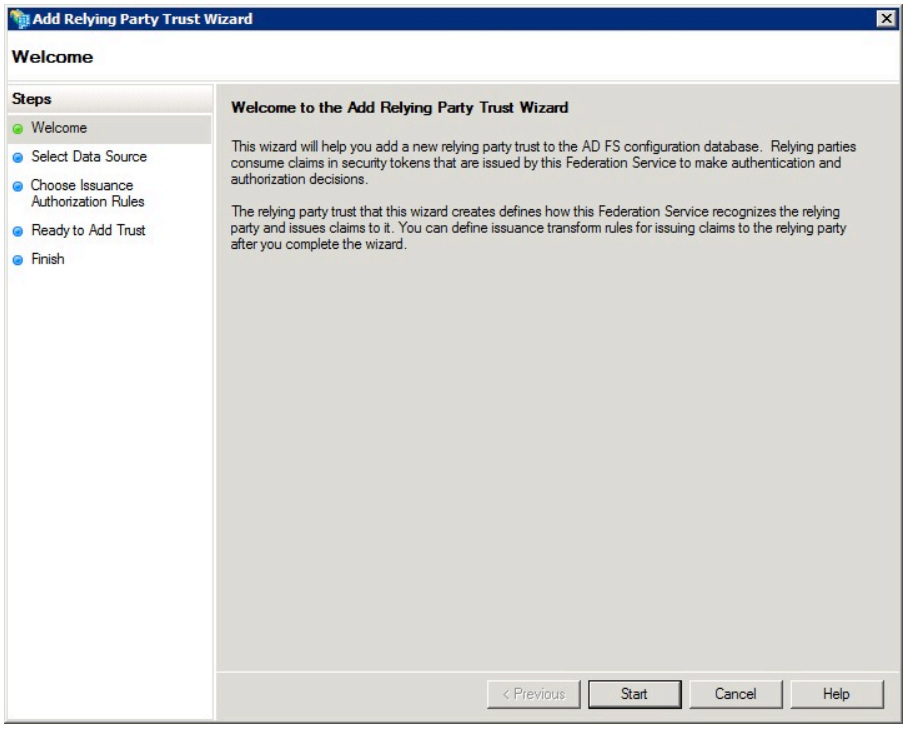
Om uw gebruikers met hun instellingsaccount toegang te kunnen geven tot diensten van de SURFfederatie, moet u uw AD FS 2.0-server configureren als Identity Provider.

3.2 Basisconfiguratie

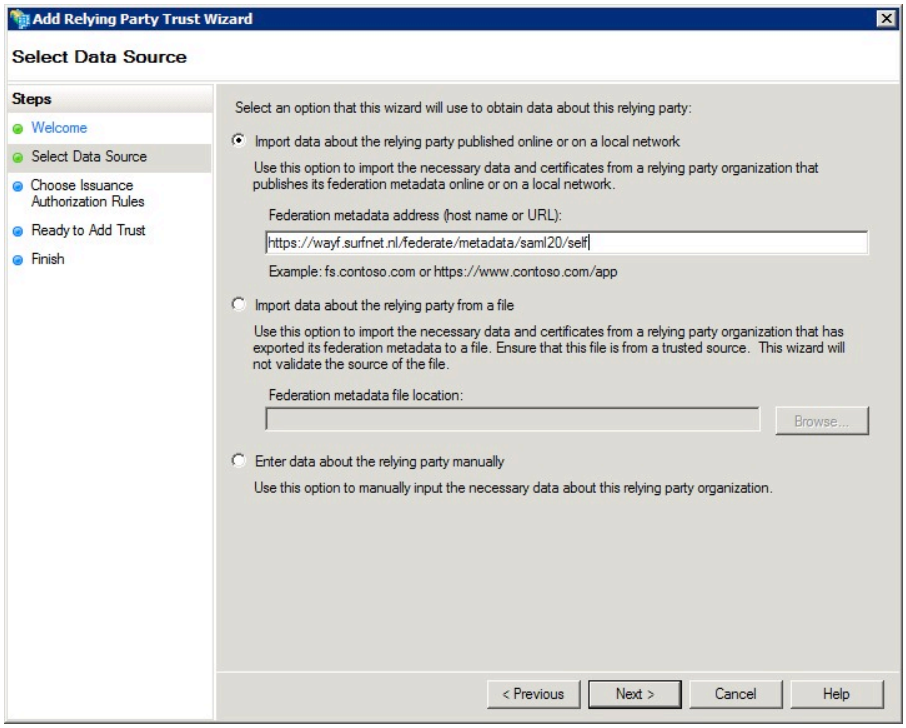
1. Kies **Start > All Programs > Administrative Tools > AD FS 2.0 Management** om de AD FS 2.0-configuratieapplicatie te starten.



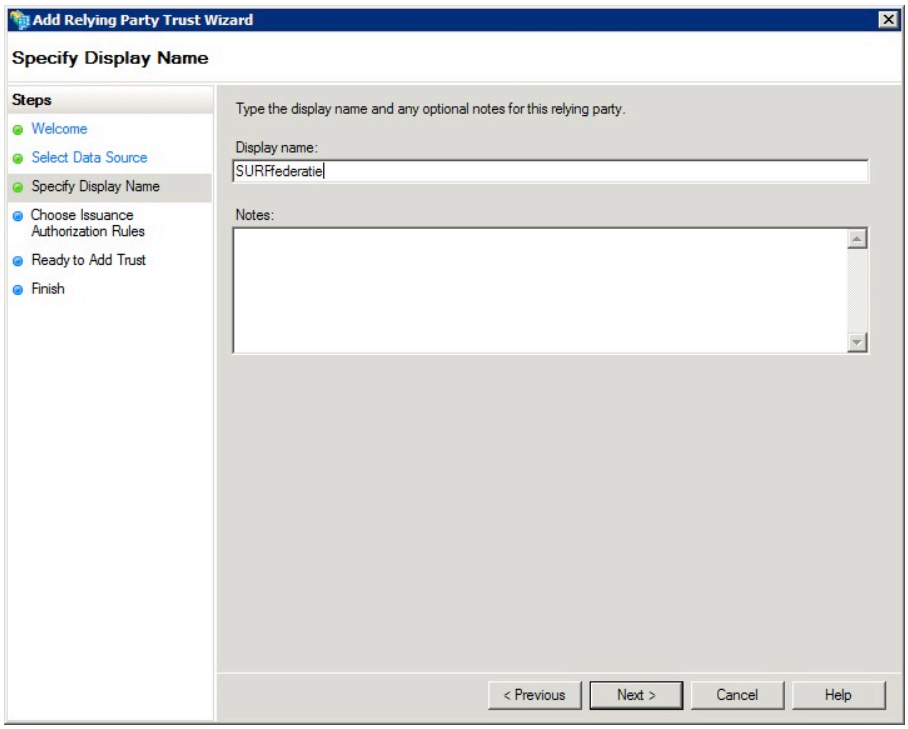
2. Klik op **Required: Add a trusted relying party**.



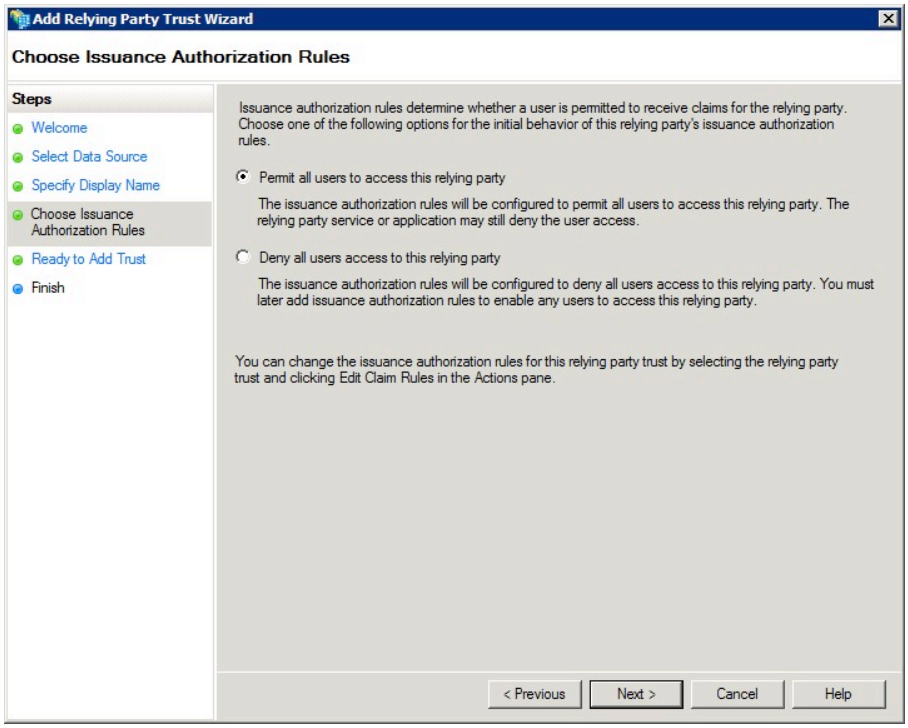
3. Klik op **Start**.



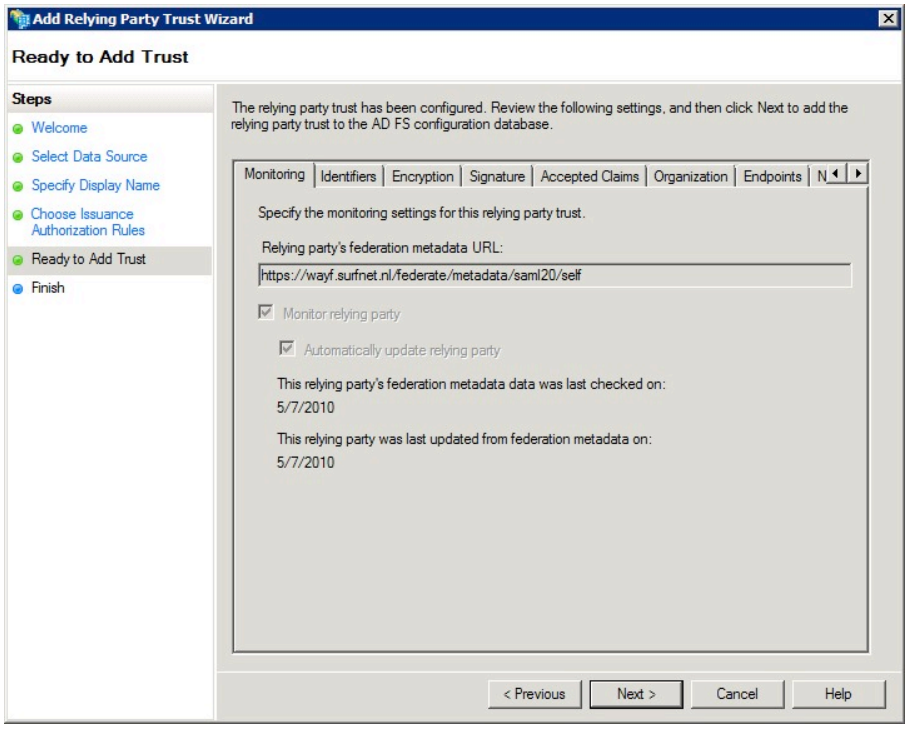
4. Vul in het veld 'Federation metadata address (host name or URL)' de volgende URL in: https://wayf.surfnet.nl/federate/metadata/saml20/self en klik op **Next**.



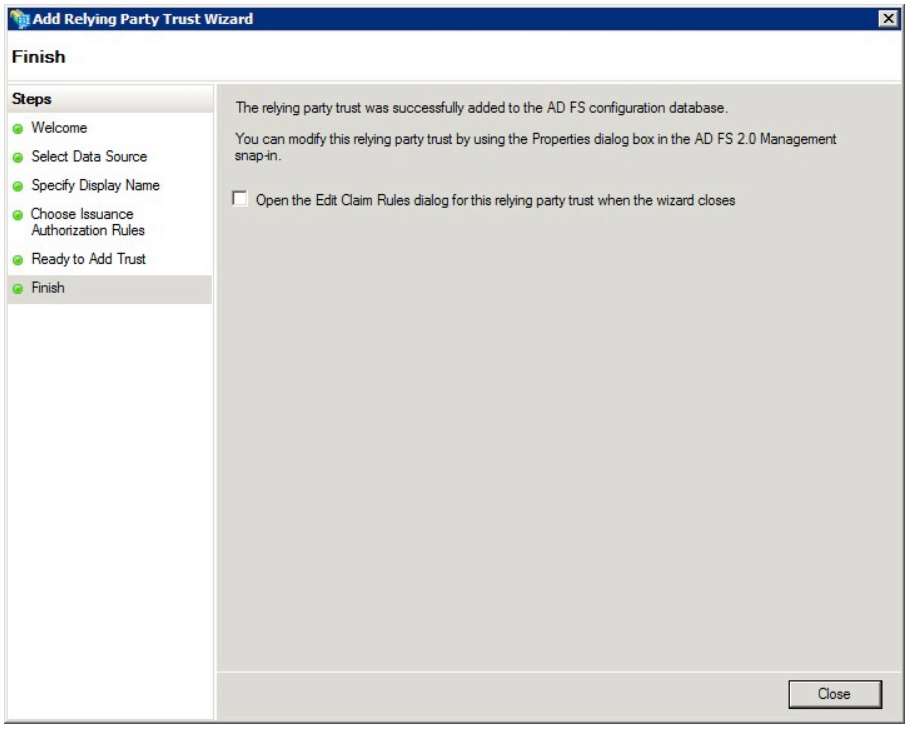
5. Vervang in het veld 'Display name' de default hostnaam (wayf.surfnet.nl) door de naam 'SURFfederatie' en klik op **Next**.



6. Selecteer **Permit all users to access this relying party** en klik op **Next**.



7. Klik in dit overzichtsvenster op **Next**.



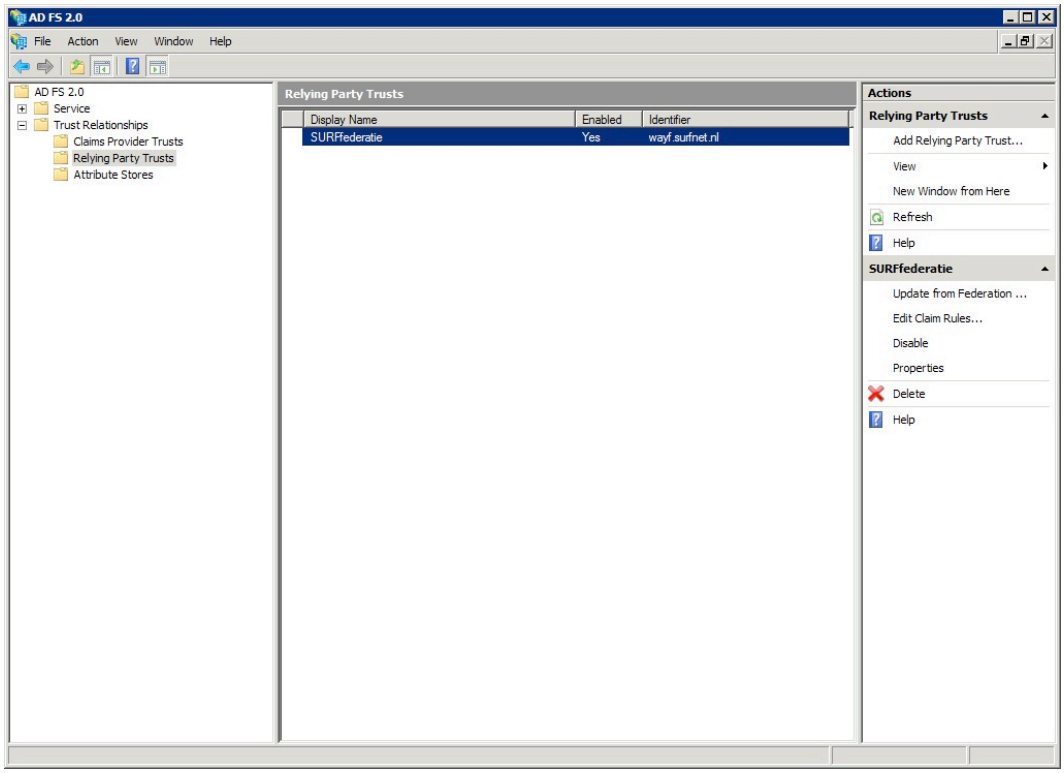
8. Deselecteer **Open the Edit Claim Rules dialog…** Met de 'Claims Rules dialog' worden de attributen geconfigureerd. Dit doet u later in het configuratieproces (zie hoofdstuk 5).

9. Klik op **Close** om deze configuratie af te ronden.

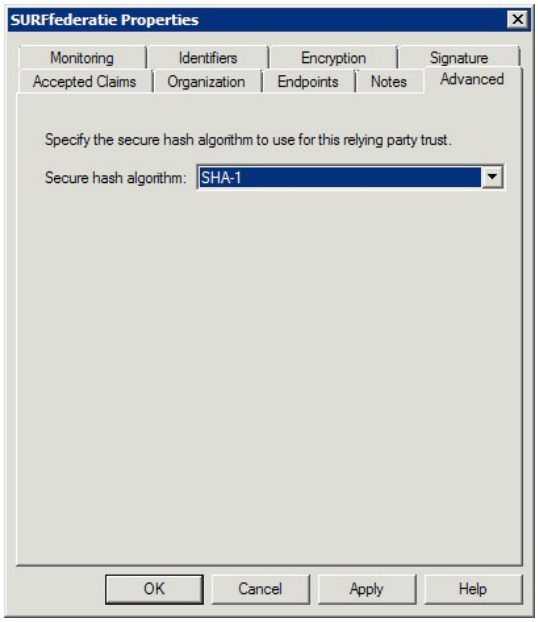
3.3 SHA1-algoritme inschakelen

In AD FS 2.0 worden handtekeningen standaard gezet met behulp van het SHA256-algoritme. Dit algoritme werkt niet goed samen met de SURFfederatie. Voor een goede werking moet dit vervangen worden door het SHA1-algoritme.

1. Kies in de linkerkolom van het overzichtsvenster **Trust Relationships > Relying Party Trusts**.



2. Dubbelklik in de middelste kolom op **SURFfederatie**.



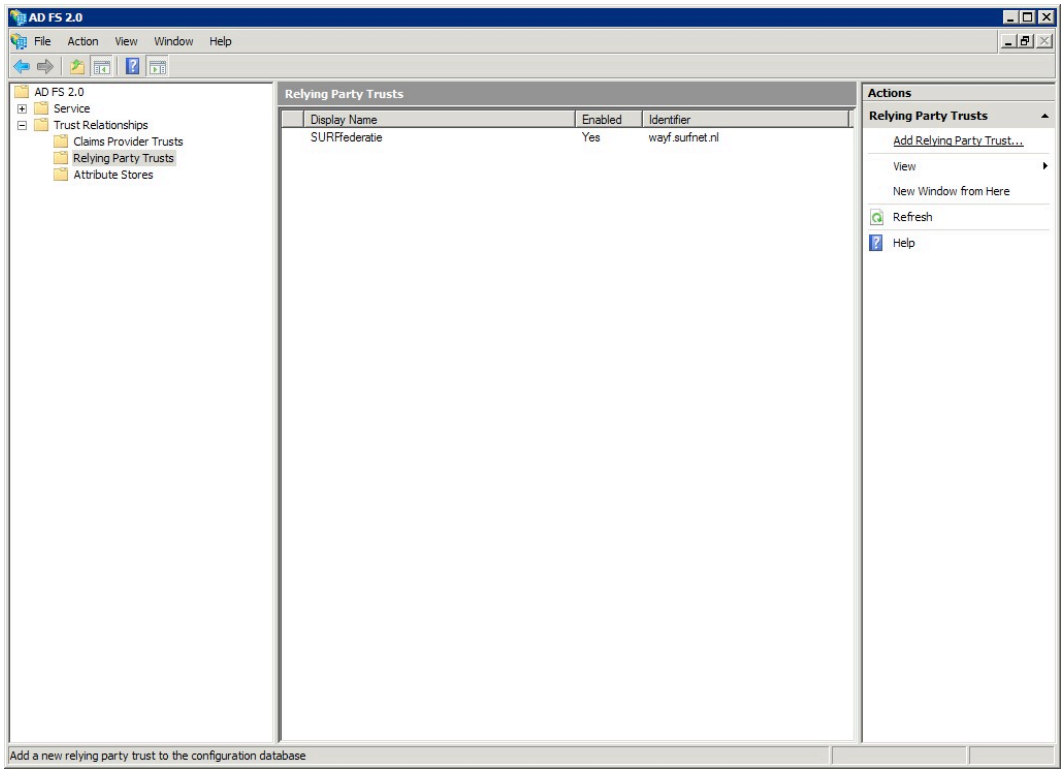
3. Selecteer het tabblad **Advanced** en kies in het veld 'Secure hash algorithm' de waarde **SHA-1**.

4. Klik op **OK** om de configuratie voor de SURFfederatie af te ronden.

3.4 Testen

Het is aan te bevelen om ook een aansluiting om de SURFfederatie testomgeving te configureren om uw installatie te kunnen testen in het geval van wijzigingen.

1. Kies links in het overzichtsvenster **Trust Relationships > Relying Party Trusts**.



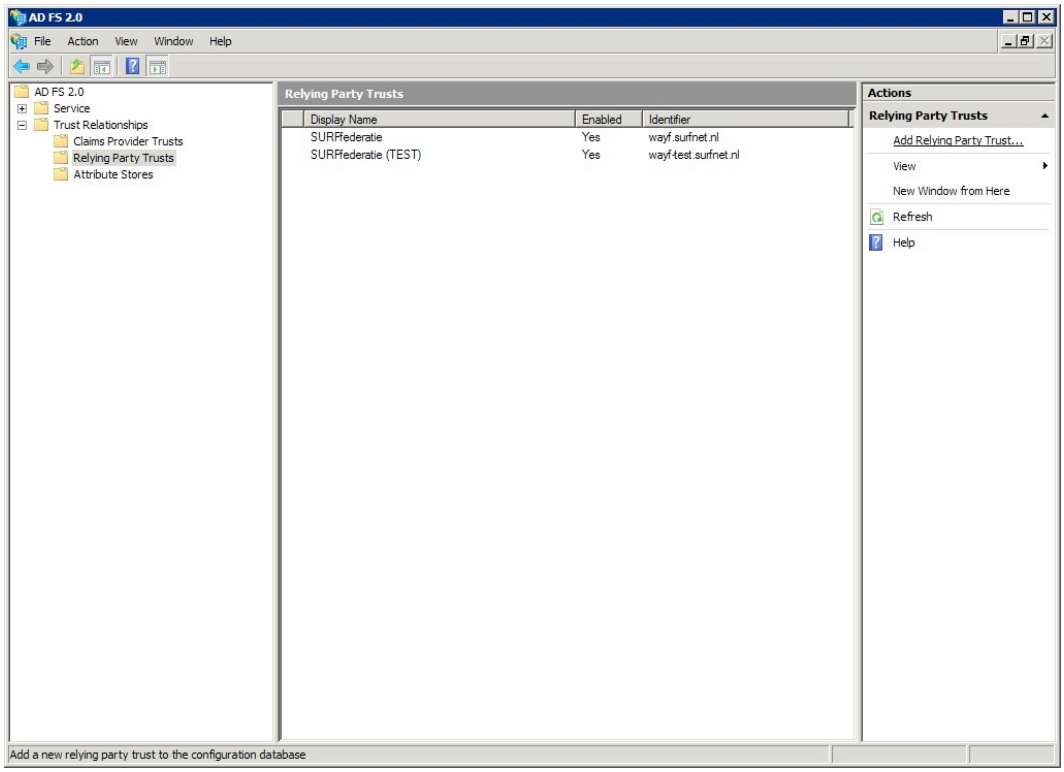
2. Klik in de rechterkolom onder 'Actions' op **Add Relying Party Trust…**.

3. Doorloop nu opnieuw de stappen uit paragraaf 3.2 en 3.3, met deze verschillen:

   - in paragraaf 3.2, stap 4 vult u de URL https://wayf-test.surfnet.nl/federate/metadata/saml20/self in.

   - in paragraaf 3.2, stap 5 vult u de 'Display name' de waarde 'SURFfederatie (TEST)' in.

Het overzichtsvenster bevat nu twee relying party entries, en ziet er als volgt uit:



4. Controleer of de SAML 2.0 metadata informatie van uw server beschikbaar is op de volgende URL:
   https://<hostnaam>/FederationMetadata/2007-06/FederationMetadata.xml (vul zelf de juiste hostnaam in).

4. AD FS 2.0-PROXY INRICHTEN

4.1 Inleiding

De AD FS-proxy hoeft niet op een aparte machine te worden geïnstalleerd, maar kan op een bestaande machine komen te staan die ook al voor andere doeleinden in gebruik is.

De installatie van een AD FS 2.0-proxy gaat in de volgende stappen:

1. Windows Server 2008 installeren en configureren (paragraaf 4.1)
2. AD FS 2.0-software installeren (paragraaf 4.2)
3. De instellingen van de AD FS 2.0-proxy configureren (paragraaf 4.3)

4.2 Windows Server 2008 installeren en configureren

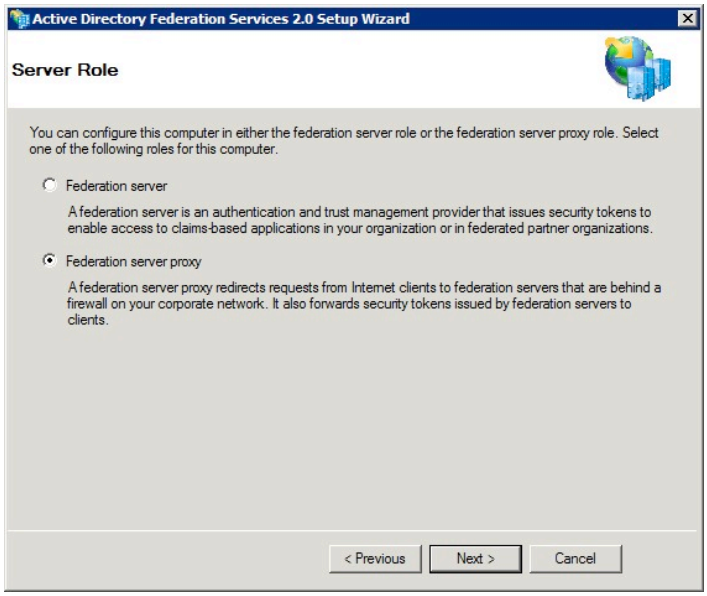
Om een AD FS 2.0-proxy te kunnen inrichten, moet u eerst Windows Server 2008 installeren en configureren:

- Installeer de juiste versie van het besturingssysteem op de server: Windows Server 2008 SP2 of Windows Server 2008 R2 (standaard of enterprise).
- Stel de tijd op de server correct in zorg dat deze wordt gesynchroniseerd met een time server.
- Zorg ervoor dat de server **niet** opgenomen is in het domein van de Active Directory waaruit de accounts voor de federatie komen.
- Installeer Internet Information Services (IIS) en zorg dat deze een geldig SSL-servercertificaat heeft. U kunt servercertificaten (onder meer) verkrijgen via de SURFcertificaten-dienst van SURFnet: http://www.surfnet.nl/nl/diensten/authenticatie/Pages/certificaten.aspx

4.3 AD FS 2.0-software installeren

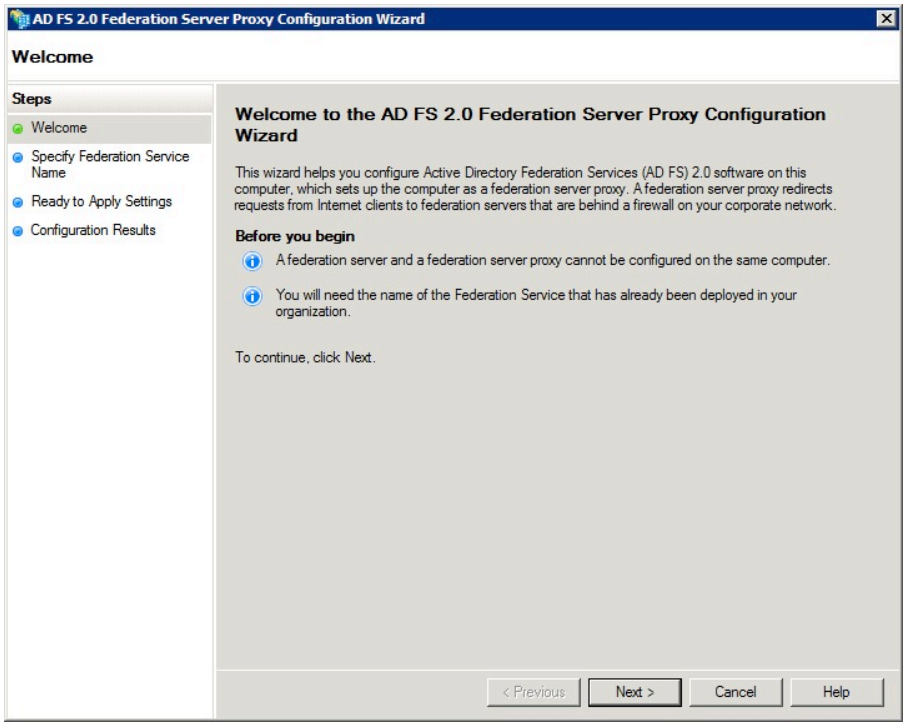
Zie paragraaf 2.3 voor het installeren van de AD FS 2.0-software, met dit verschil:

kies bij stap 3 voor **Federation server**.

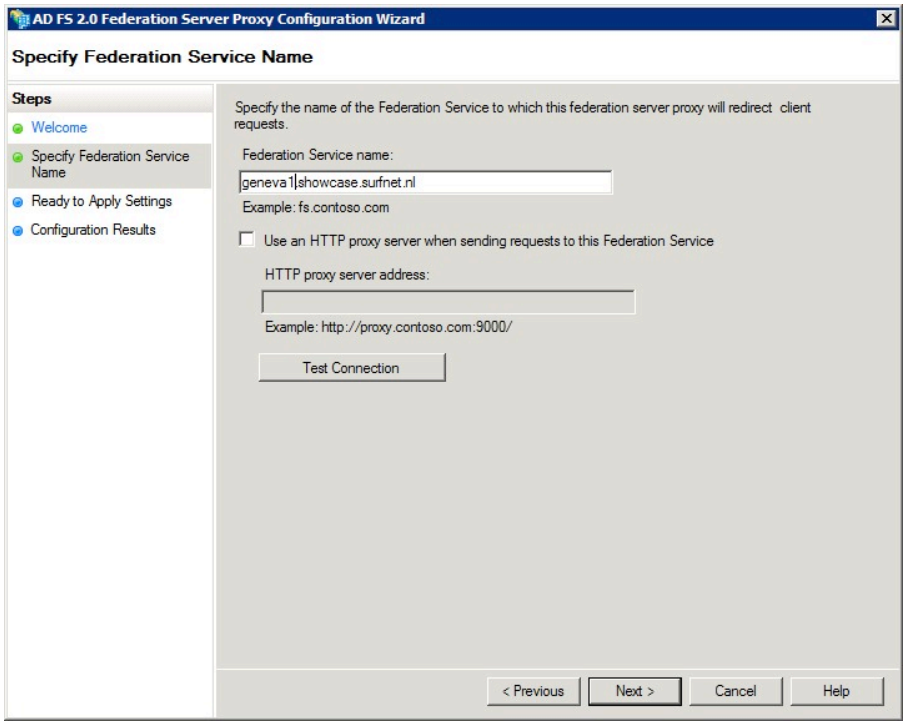


4.4 AD FS 2.0 Proxy Configuratie

1. Kies **Start > Programs > Administrative Tools > AD FS 2.0 Federation Server Proxy Configuration Wizard** om de AD FS 2.0-proxy configuratieapplicatie te starten.

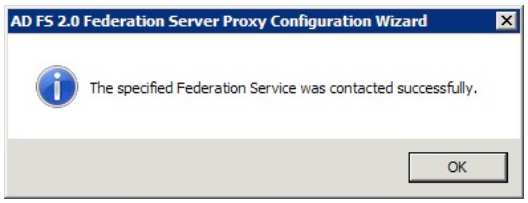


2. Klik op **Next**.



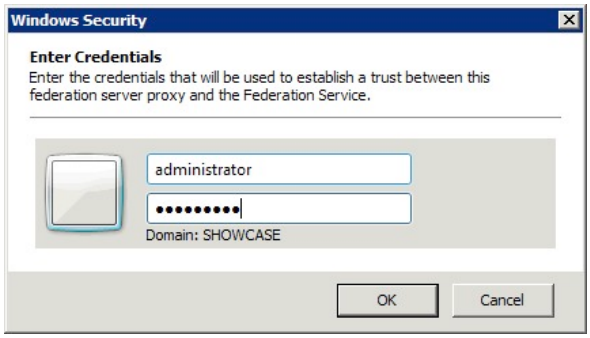
3. Vul in het veld 'Federation Service name' de naam in van uw AD FS 2.0-server die u in paragraaf 2.4 hebt gekozen. Normaal gesproken is dit de hostnaam van de AD FS 2.0-server.

4. Klik op **Next**.

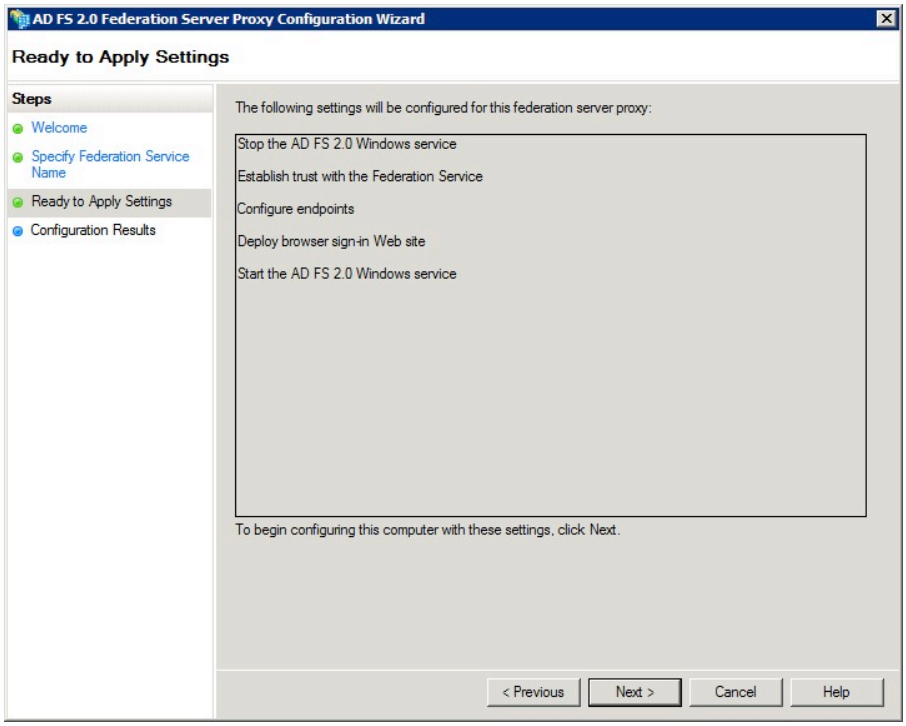


De popup geeft aan dat er een succesvolle verbinding van de proxy naar de server gelegd kon worden.

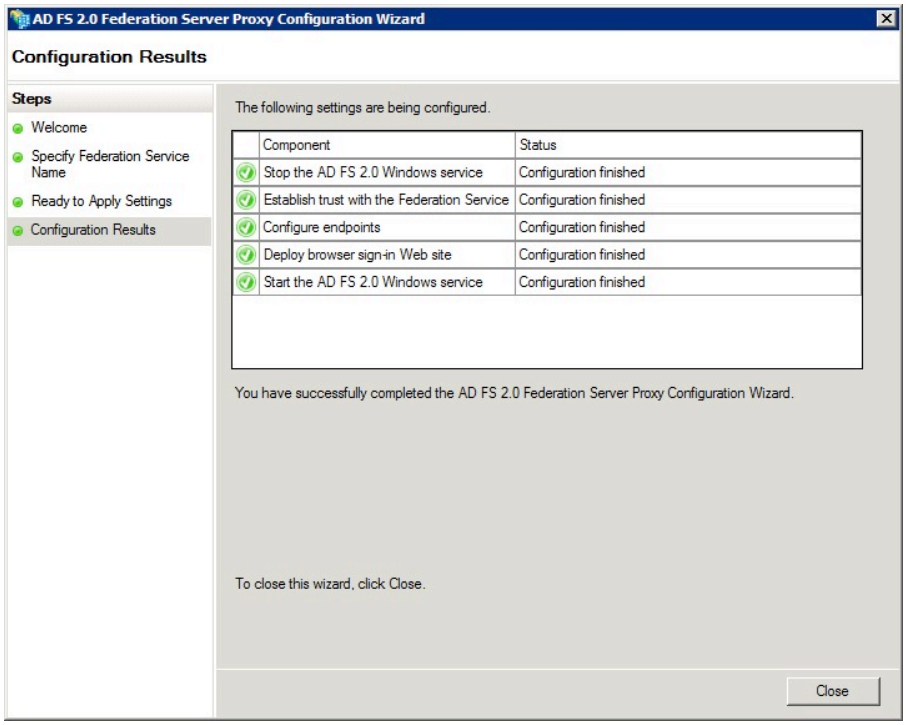
5. Klik op **OK**.



6. Voer gebruikersnaam en wachtwoord in van het adminstrator-account van de AD FS 2.0-server en klik op **OK**.



7. Klik op **Next**.



8. Klik op **Close** als de installatie voltooid is.

4.5 DNS configureren

Als de server en de proxy zijn ingericht, moet u de DNS-configuratie nog aanpassen. Interne verzoeken (van binnen het Windows-domein) moeten namelijk direct naar de server worden geleid, externe verzoeken moeten via de proxy lopen.

Registreer de IP-adressen van de AD FS 2.0-server en –proxy in het DNS als volgt:

- het adres 'adfs.mycampus.nl' moet voor verzoeken vanaf uw eigen domein resolven naar de AD FS 2.0-server.
- het adres 'adfs.mycampus.nl' moet voor verzoeken vanaf externe domeinen resolven naar de AD FS 2.0-proxy.

Het testen van de proxy kan verlopen door op een client machine tijdelijk de HOSTS-file aan te passen naar de nieuwe situatie.

4.6 Testen

1. Stuur een e-mail naar SURFfederatie Beheer (federatie-beheer@surfnet.nl), waarin u aangeeft dat u op de productie- en testomgeving van de SURFfederatie wilt aansluiten met uw AD FS 2.0-server. Geef daarbij de URL van uw AD FS 2.0-server door (adfs.mycampus.nl).
2. Wacht tot uw gegevens geconfigureerd zijn (u krijgt hiervan bericht) en test daarna via: https://wayf-test.surfnet.nl/attributes.

4.7 Login pagina aanpassen

De standaard login pagina op de ADFS proxy kan nu worden aangepast naar de look-and-feel van uw instelling, door de file:

```
C:\Program Files\Active Directory Federation Services
2.0\WSFederationPassive.Web\FormsSignIn.aspx
```

te wijzigen. Bij voorkeur dient hier tekst te worden opgenomen over:

- de manier waarop gebruikers moeten inloggen, bijv. in welk formaat de user identifier moet worden ingevoerd (bijv. "student nummers" of "NetID")
- een waarschuwing dat (bijv. bij gebruik op publieke terminals), uitloggen alleen voor gegarandeerd kan worden door de browser af te sluiten
- dat bij het inloggen moet worden gelet op een geldige HTTPS URL op de juiste server

5. ATTRIBUTEN VRIJGEVEN

5.1 Inleiding

Attributen zijn gebruikerkenmerken die de AD FS 2.0-server na een geslaagde authenticatie van een gebruiker kan toevoegen aan informatie die aan de SURFfederatie wordt doorgegeven. Voorbeelden van attributen zijn het e-mailadres van de gebruiker of de naam van een groep waar de gebruiker lid van is.

De set van gestandaardiseerde attributen die binnen de SURFfederatie kunnen worden gebruikt, vindt u hier:

http://www.surffederatie.nl/attributenschema

Voordat de SURFfederatie attributen kan gebruiken in het authenticatieproces, moet u ze vrijgeven aan de SURFfederatie. In dit hoofdstuk worden vier attributen als voorbeeld vrijgegeven:

- Name ID (loginnaam)
- urn:mace:dir:attribute-def:uid (loginnaam; kan verschillen van waarde bij User ID)
- urn:mace:dir:attribute-def:mail (e-mailadres)
- urn:mace:dir:attribute-def:displayName (weergavenaam)

Deze fungeren slechts als voorbeeld; overleg met SURFnet over de specifieke attributen die uw organisatie nodig heeft voor het benaderen van diensten in de SURFfederatie. Een overzicht daarvan vindt u hier:

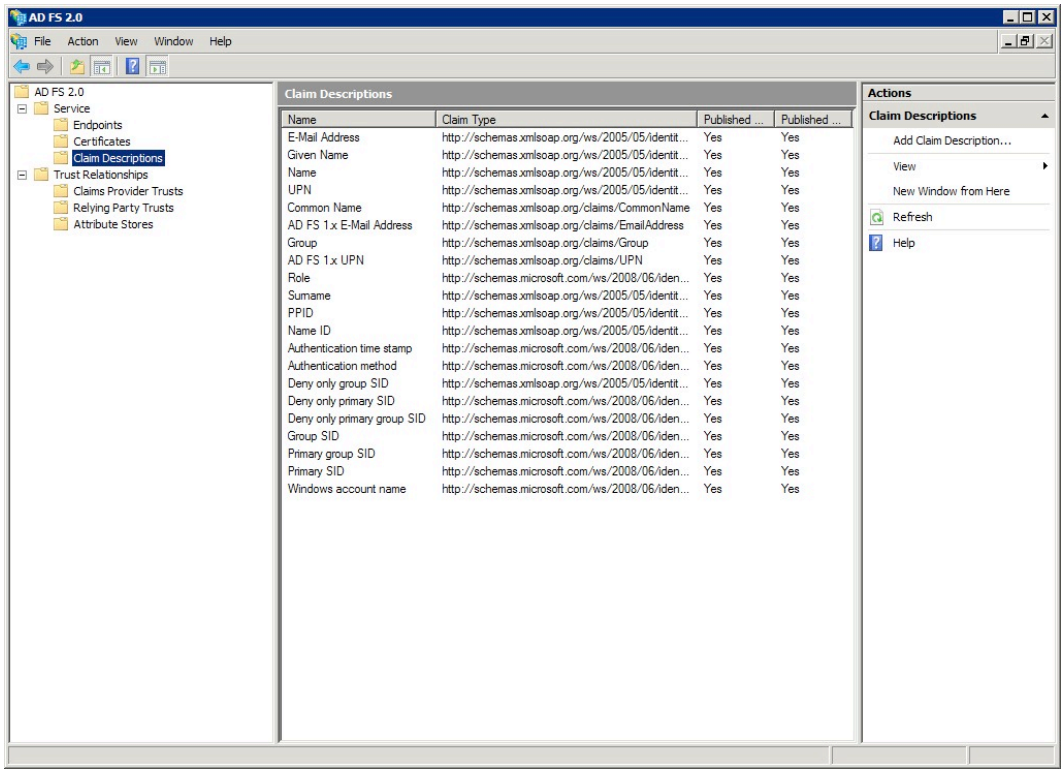
http://www.surffederatie.nl/attributen

Het vrijgeven van attributen bestaat uit twee stappen

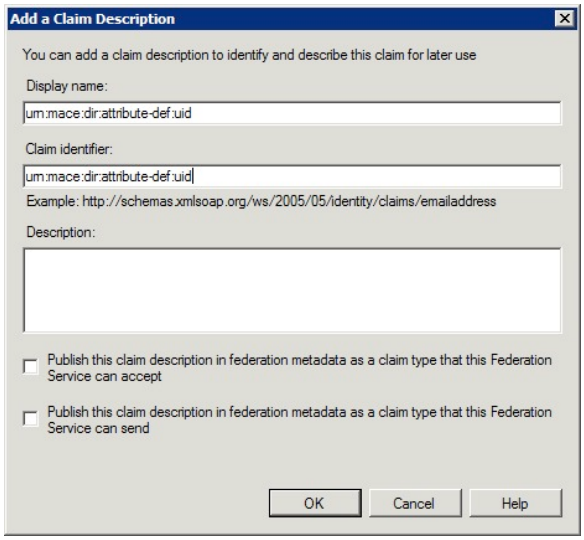
1. Attributen definiëren (paragraaf 5.2)
2. Attributen toewijzen aan de SURFfederatie (paragraaf 5.3)
3. Testen (paragraaf 5.4)

5.2 Attributen definiëren

1. Kies op de AD FS 2.0-server **Start > All programs > Administrative Tools > AD FS 2.0 Management** om de AD FS 2.0 configuratieapplicatie te starten.
2. Selecteer **Service > Claims Descriptions** in de linker kolom van het overzichtsvenster.



3. Klik in de rechterkolom onder 'Actions' op **Add Claim Description…**.



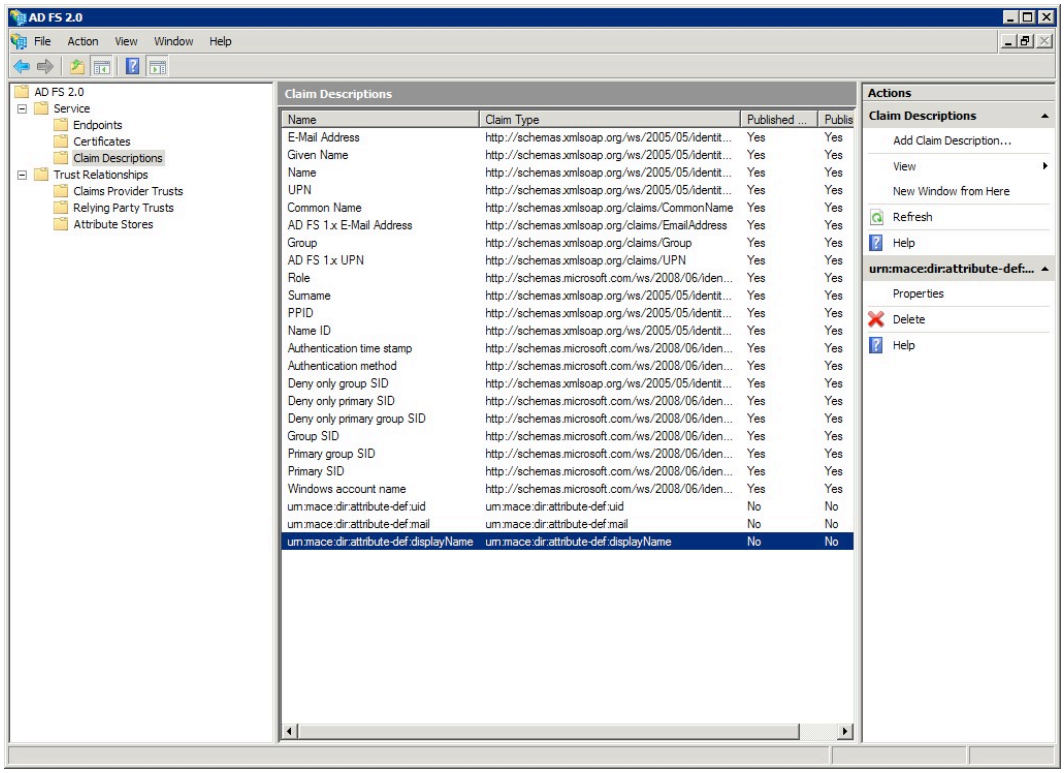
4. Vul in de velden 'Display name' en 'Claim identifier' de waarde in van het attribuut dat u wilt vrijgeven aan de SURFfederatie. Zie voor een overzicht van attributen: http://www.surffederatie.nl/attributenschema.

Vul voor elk attribuut in beide velden exact hetzelfde in.

5. Klik op **OK**.

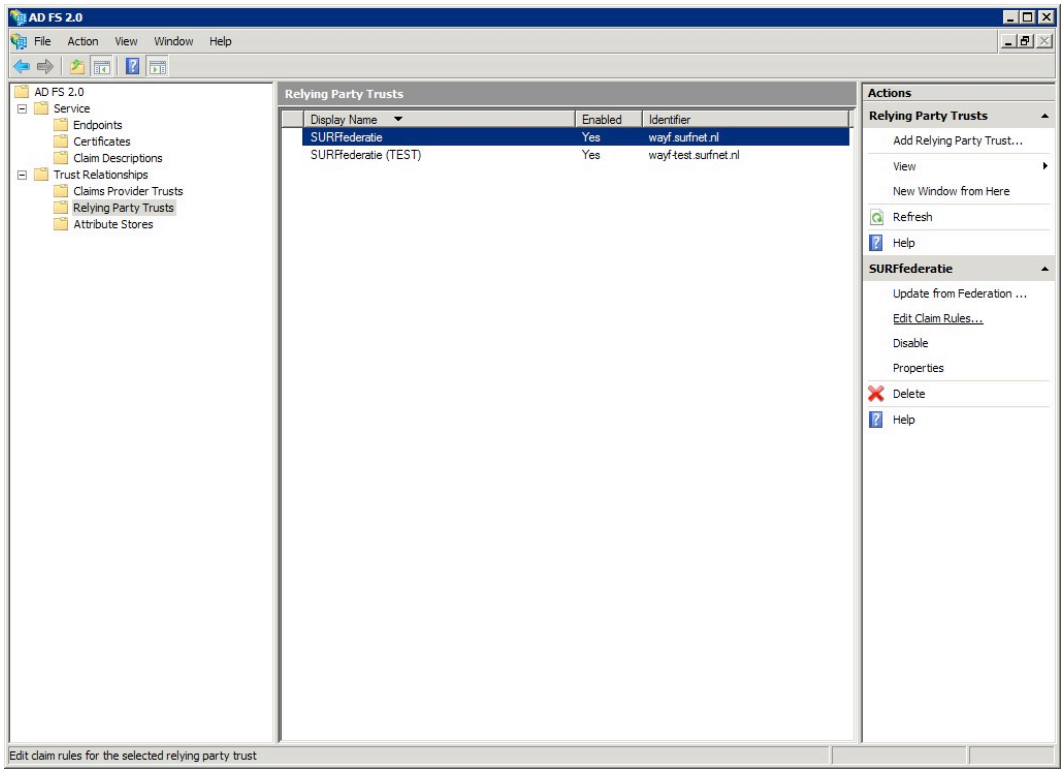
6. Herhaal de voorgaande stap voor alle attributen, zodat deze onderaan in de lijst van Claim Descriptions verschijnen.

Het attribuut 'Name ID' hoeft niet te worden gedefinieerd, omdat dit attribuut al bestaat.

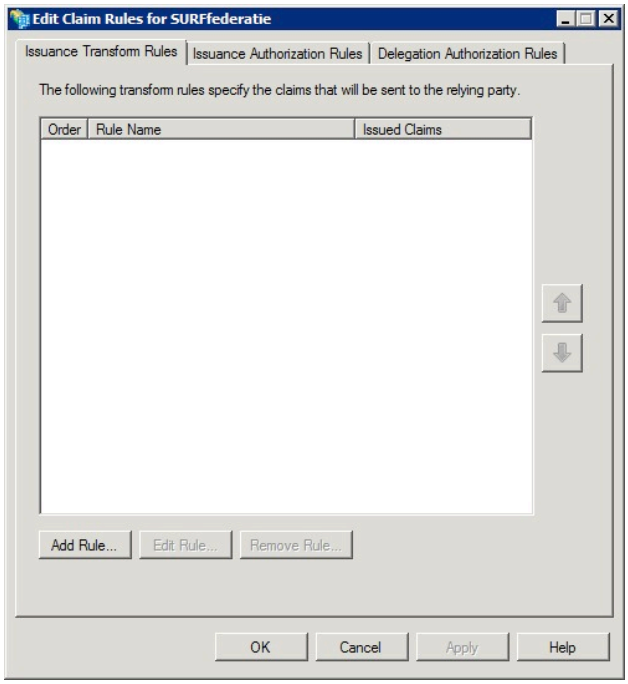


5.3 Attributen toewijzen aan SURFfederatie

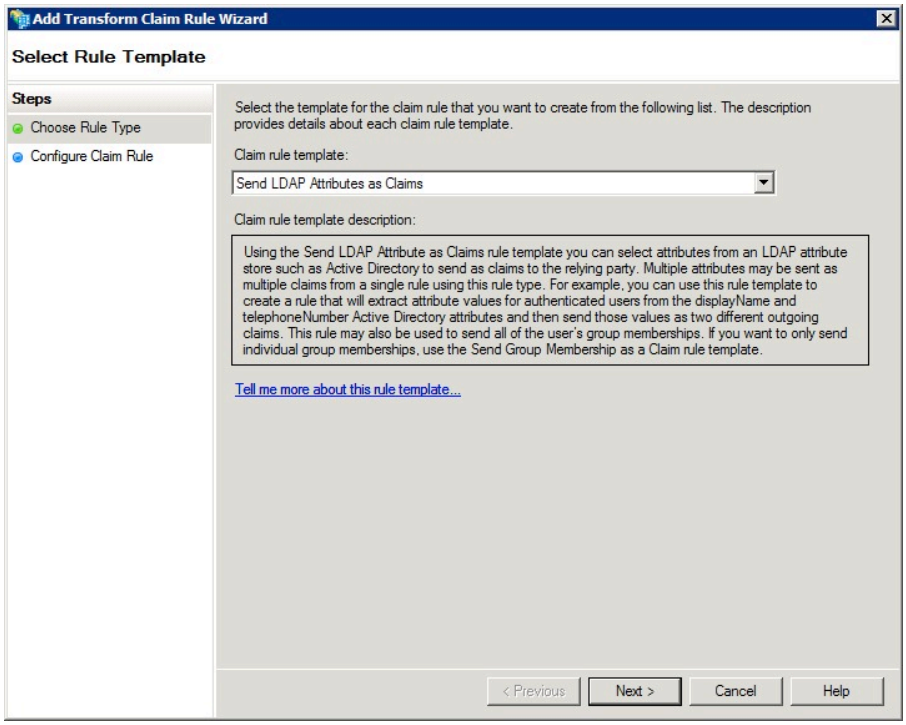
1. Kies in de linkerkolom **Trust Relationships > Relying Party Trusts**.



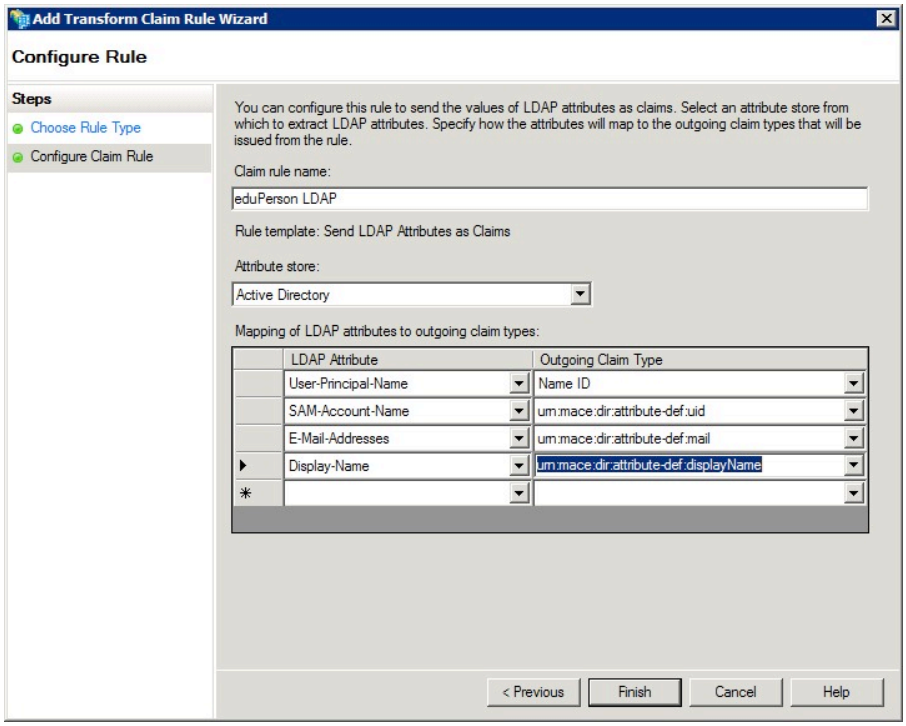
2. Klik in de middelste kolom op **SURFfederatie (TEST)**, en vervolgens in de rechterkolom op **Edit Claim Rules**.



3. Klik op **Add Rule…**.



4. Kies onder 'Claim rule template' voor **Send LDAP Attributes as Claims** klik op **Next**.



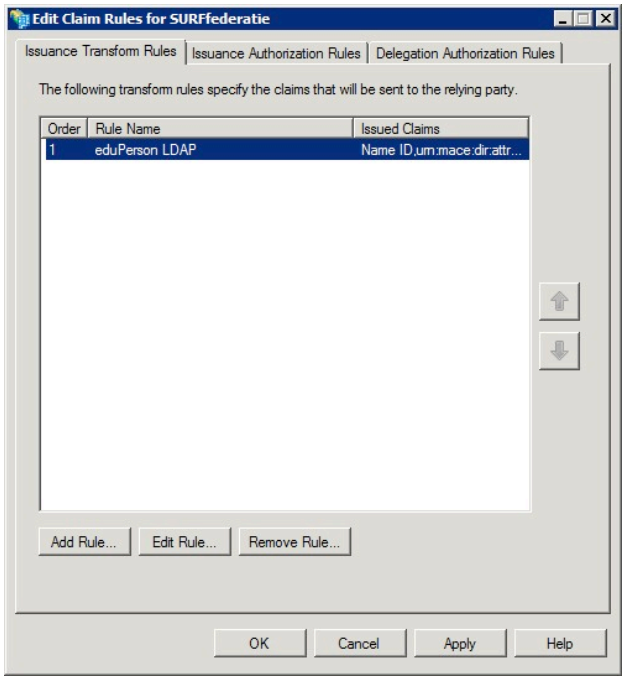
5. Vul een zinvolle naam in in het veld 'Claim rule name', bijvoorbeeld 'eduPerson LDAP'.

6. Selecteer onder 'Attribute store' de optie **Active Directory**.

7. Voeg de volgende attribuutmappings toe:

LDAP Attribute	Outgoing Claim Type
User Principal Name	Name ID
SAM-Account-Name	urn:mace:dir:attribute-def:uid
E-Mail-Addresses	urn:mace:dir:attribute-def:mail
Display-Name	urn:mace:dir:attribute-def:displayName

8. Klik op **Finish**.



9. Klik op **OK**.

5.4 Testen

U kunt testen of de vrijgave van de attributen is gelukt.

1. Ga naar https://wayf-test.surfnet.nl/attributes.
2. Selecteer uw instelling en log in.

U ziet nu een overzicht van de attributen die worden vrijgegeven aan uw instelling.