Melding einde support ADFS 2.0 (EOL)

Melding einde support ADFS 2.0 en Windows Server 2008 (EOL)

De support van Windows Server waarop ADFS 2.0 draait loopt af op 14-01-2020. Voor nieuwe identity providers raden we ten strengste af deze versie te gebruiken - zie in plaats daarvan onze Handleidingen en richtlijnen van nieuwere versies van ADFS. Gebruik deze pagina enkel ter referentie of voor vragen over providers die nog gebruiken maken van ADFS 2.0 en Windows Server 2008.

ADFS 2.0 en Windows Server 2008 (Legacy)

Inlog-problemen met een ADFS2.0 IdP bij her-authenticatie? Dit kan komen door een security patch van Microsoft 'MS13-066'

Inleiding

In deze handleiding lees je hoe je jouw organisatie kunt aansluiten op SURFconext als Identity Provider met behulp van ADFS2.0 (in ADFS-terminologie Account Partner (AP) genoemd).

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

1. een ADFS 2.0-serversysteem inrichten; waaronder Windows Server 2008 configureren en ADFS 2.0 installeren
2. de ADFS 2.0-server configureren voor aansluiting als Identity Provider voor SURFconext.
3. een ADFS 2.0 proxy inrichten indien toegang van buiten het lokale netwerk gewenst is.
4. attributen vrijgeven aan SURFconext

Meer informatie over ADFS 2.0

ADFS 2.0 (codenaam Geneva Server) is de opvolger van ADFS v1 zoals deze oorspronkelijk beschikbaar was op Windows Server 2003 R2 en Windows Server 2008. De belangrijkste wijziging ten opzichte van ADFS v1 is de ondersteuning van het SAML 2.0-protocol.

Deze handleiding is gebaseerd op de release van ADFS 2.0 (5 mei 2010). Meer informatie over de installatie van ADFS 2.0 vind je op http://technet.microsoft.com/en-us/library/adfs2(WS.10).aspx.

Voor een step-by-step guide van Microsoft, handig als naslagwerk naast deze handleiding, zie: http://technet.microsoft.com/en-us/library/ff631096(WS.10).aspx.

Waarom server en proxy?

Om de ADFS-server minder kwetsbaar te maken voor aanvallen van buitenaf, moet je naast een ADFS 2.0-server ook een ADFS-proxy inrichten buiten het Windows-domein. De ADFS-server moet namelijk bij voorkeur niet bereikbaar zijn van buitenaf. Je doet dit door een ADFS-proxy in te richten en deze 'voor' de ADFS-server te plaatsen Dit houdt in dat je twee verschillende Windows Server 2008 machines moet configureren in deze setup.

De proxy zorgt ervoor dat gebruikers die niet zijn ingelogd op het domain, via een username/ password formulier kunnen inloggen. Dit formulier kan aan de look-and-feel van jouw organisatie worden aangepast.

ADFS 2.0-Server inrichten

Inleiding

Voordat je de specifieke instellingen voor SURFconext kunt invoeren, moet je een basisinstallatie op de ADFS 2.0-server uitvoeren. Hiervoor moet je onderstaande stappen doorlopen:

1. Installeer en configureer Windows Server 2008.
2. Installeer de ADFS 2.0-software.
3. Configureer de basisinstellingen van ADFS 2.0.

Windows Server 2008 installeren en configureren

Om een ADFS 2.0-server te kunnen inrichten, moet je eerst Windows Server 2008 installeren en configureren.

Hiervoor moet je onderstaande stappen doorlopen:

1. Installeer de juiste versie van het besturingssysteem op de server: Windows Server 2008 SP2 of Windows Server 2008 R2 (standaard of enterprise).
2. Stel de tijd op de server correct in en zorg ervoor dat je deze synchroniseert met een time server.
3. Neem de server op in het domein van de Active Directory waaruit de accounts voor de SURFconext federatie komen.
4. Installeer Internet Information Services (IIS) en zorg dat deze een geldig SSL-servercertificaat heeft. Je kunt servercertificaten (onder meer) verkrijgen via de SURFcertificaten-dienst van SURFnet: http://www.surf.nl/diensten-en-producten/surfcertificaten/index.html of anders via een commerciële aanbieder.

ADFS 2.0-software installeren

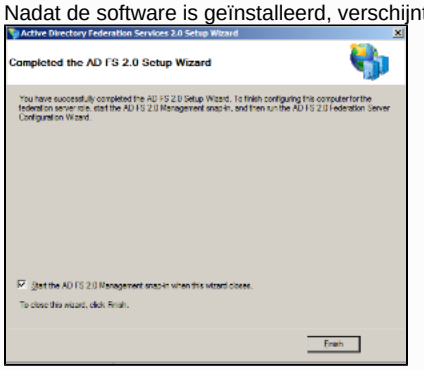
Voordat je met de eigenlijke installatie kunt beginnen, moet je de volgende stappen doorlopen:

1. Download ADFS 2.0 Server via http://go.microsoft.com/fwlink/?linkid=151338 voor jouw 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’.

Je kunt nu beginnen met de eigenlijke installatie. Doorloop de volgende stappen:

1. Volg de stappen in de wizard.
2. Nadat de software is geïnstalleerd, verschijnt het volgende venster:



3. Als de optie ‘Restart now’ aanwezig is, vink deze dan aan en klik op ´Finish´. De server start opnieuw op. Hiermee is de basisinstallatie van de ADFS 2.0-software afgerond.
4. Als de optie ´Start the ADFS 2.0 Management snap-in when this wizard closes´ aanwezig is, zorg er dan voor dat deze niet aangevinkt is en klik op ‘Finish’.

Verlengen geldigheidsduur van het token-signing certificaat

Tijdens de installatie van de ADFS/server is een self-signed tokencertificaat geïnstalleerd met een standaard geldigheidsduur van 1 jaar. Dit certificaat wordt automatisch vernieuwd voordat de geldigheidsduur is verstreken. Volgens de standaardinstellingen wordt 20 dagen voor het verstrijken van het oude certificaat een nieuw certificaat gegenereerd.

Wij raden je aan de geldigheidsduur van dit certificaat te verlengen tot bijvoorbeeld 5 jaar, omdat wij als Service Provider elke keer het nieuwe certificaat moeten vernieuwen als er een certificate rollover plaatsvindt.

Doorloop de onderstaande stappen om het automatisch gegenereerde token signingcertificaat te verlengen en te vervangen:

1. Start Windows PowerShell.
2. Laad de ADFS-plugin met het commando:

```
Add-PSSnapin Microsoft.Adfs.PowerShell
```

3. Zet de geldigheidsduur van certificaten op 5 jaar (1825 dagen) met:

```
Set-ADFSProperties -CertificateDuration 1825
```

NB: stap 4 alleen uitvoeren als je de server nog niet in productie hebt genomen! Voor productieservers kun je wachten tot het eerstvolgende moment waarop een certificate rollover plaatsvindt.

4. Activeer het nieuwe certificaat met:

```
Update-ADFSCertificate -CertificateType Token-Signing -Urgent
```

5. Controleer of het tokencertificaat nu inderdaad is verlengd met

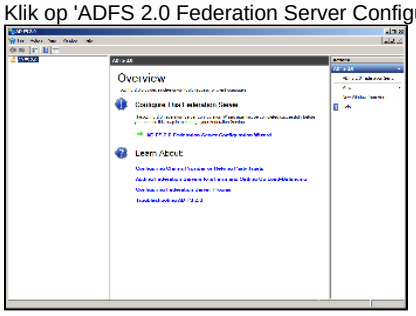
```
Get-ADFSCertificate -CertificateType Token-Signing
```

De verloopdatum van het certificaat staat vermeld onder ‘Not After’.

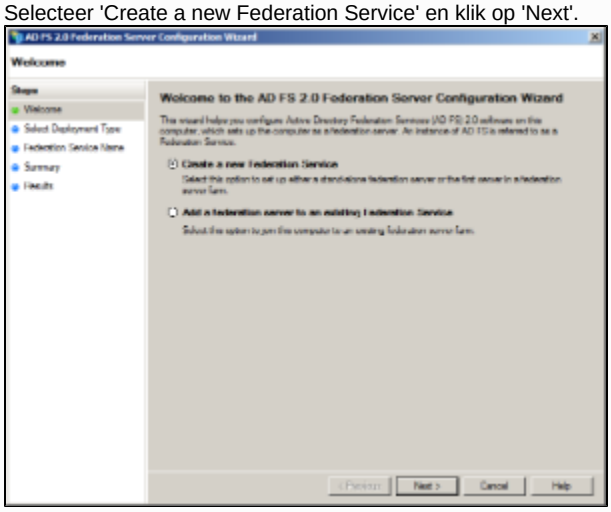
Basisinstellingen ADFS 2.0 configureren

Om de basisinstellingen van ADFS 2.0 te configureren moet je de volgende stappen doorlopen:

1. Kies 'Start' -> 'All Programs' -> 'Administrative Tools' -> 'ADFS 2.0 Management' om de ADFS 2.0-configuratieapplicatie te starten.
2. Klik op 'ADFS 2.0 Federation Server Configuration Wizard'.

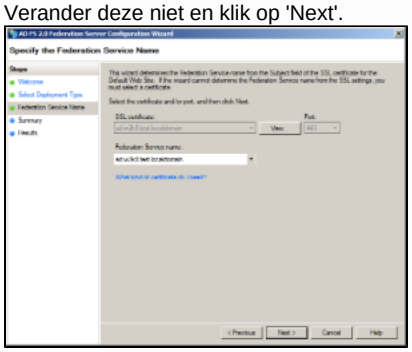


3. Selecteer 'Create a new Federation Service' en klik op 'Next'.

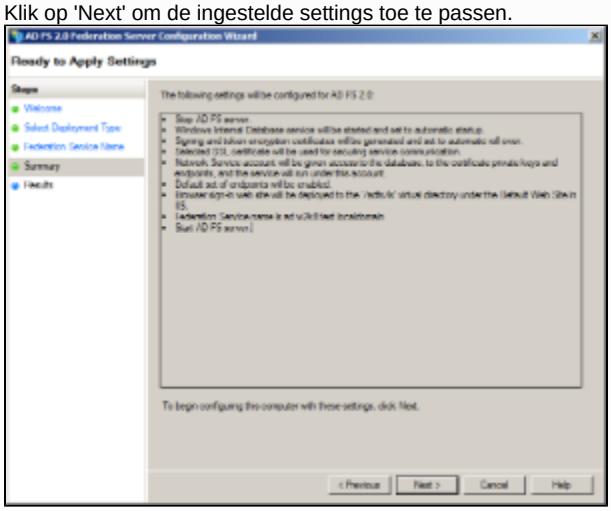


4. Selecteer afhankelijk van het gewenste service level 'Stand-alone federation server' of 'New federation server farm' en klik op 'Next'. (Deze handleiding gaat uit van een stand-alone server. Voor informatie over het opzetten van een farm verwijzen we naar de documentatie van Microsoft).

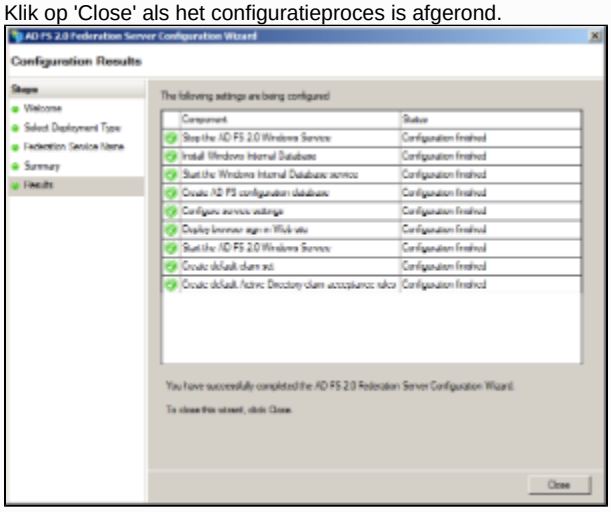
5. In het veld 'Federation Service name' is de hostnaam van jouw server en het bijbehorende SSL certificaat al ingevuld. Verander deze niet en klik op 'Next'.



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 ADFS 2.0-server afgerond.

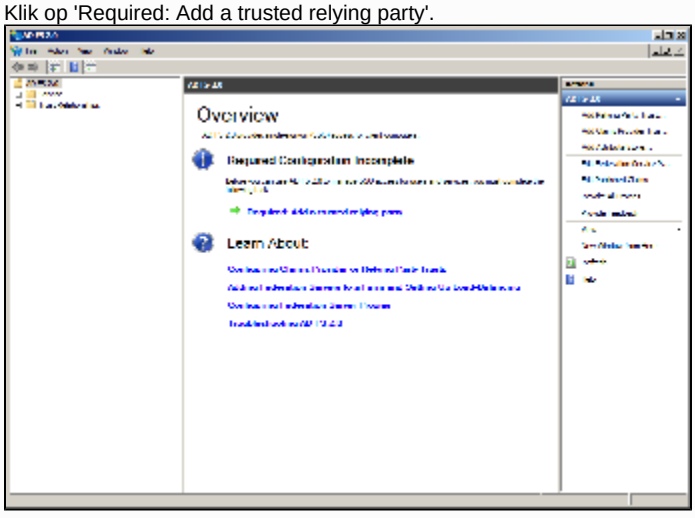
ADFS 2.0-server configureren als Identity Provider

Inleiding

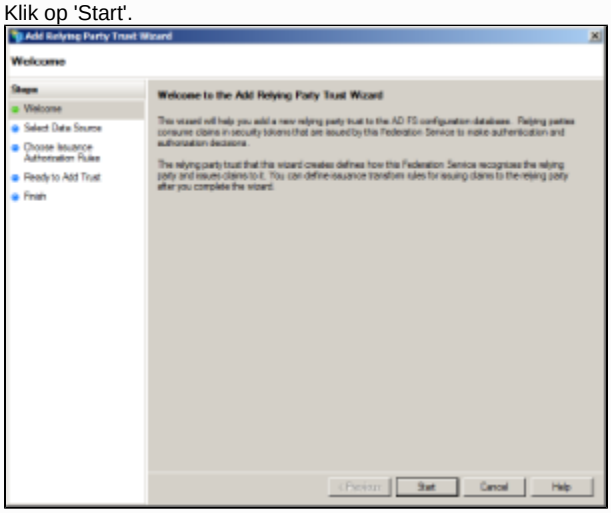
Om jullie gebruikers met hun instellingsaccount toegang te geven tot diensten van SURFconext, moet je de ADFS 2.0-server configureren als Identity Provider.

Basisconfiguratie

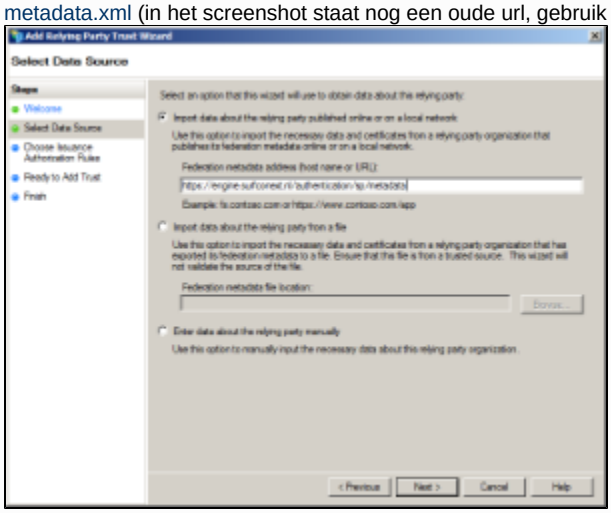
1. Kies 'Start' -> 'All Programs' -> 'Administrative Tools' -> 'ADFS 2.0 Management' om de ADFS 2.0-configuratieapplicatie te starten.
   Klik op 'Required: Add a trusted relying party'.



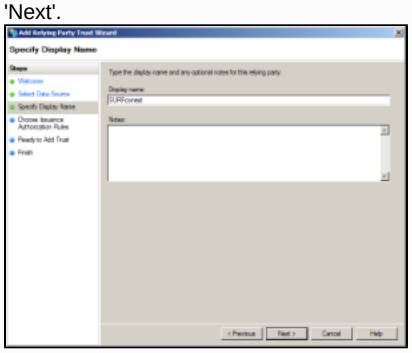
2. Klik op 'Start'.



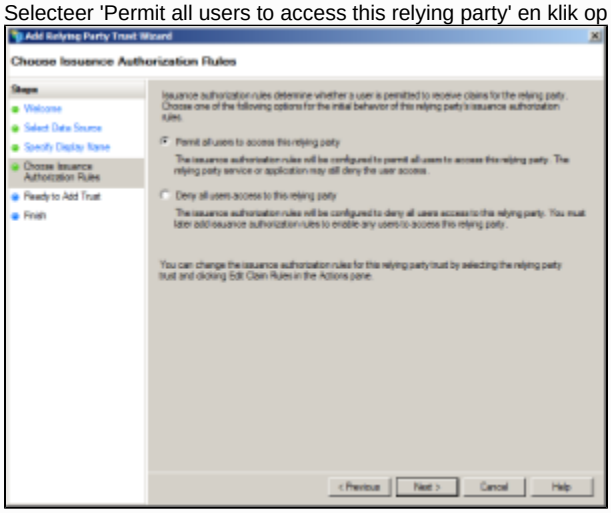
3. Vul in het veld 'Federation metadata address (host name or URL)' de volgende URL in: https://metadata.surfconext.nl/sp-metadata.xml (in het screenshot staat nog een oude url, gebruik die niet meer) en klik op 'Next'.



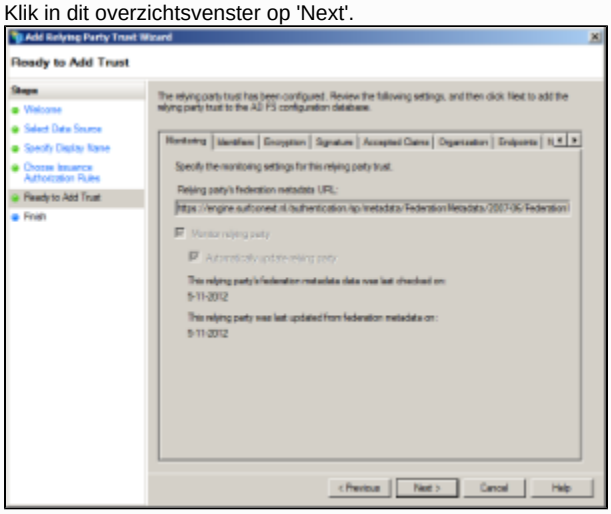
4. Vervang in het veld 'Display name' de default hostnaam (metadata.surfconext.nl) door de naam 'SURFconext' en klik op 'Next'.



5. Selecteer 'Permit all users to access this relying party' en klik op 'Next'.

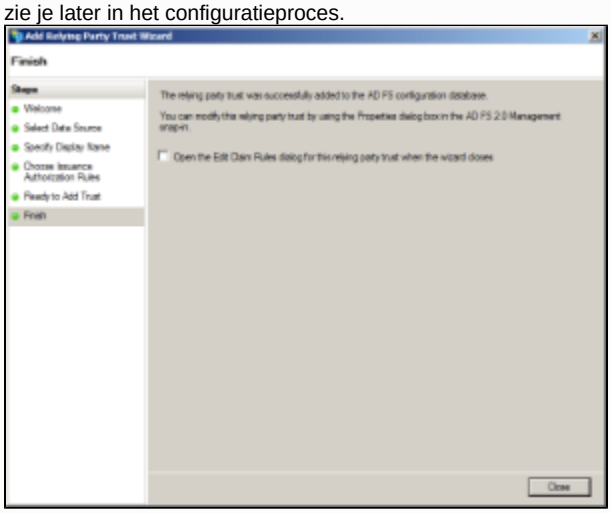


6. Klik in dit overzichtsvenster op 'Next'.



*Let op: De URL in bovenstaand screenshot is **niet** de correcte locatie van onze metadata.*
Gebruik https://metadata.surfconext.nl/sp-metadata.xml zoals hierboven beschreven.

7. Deselecteer 'Open the Edit Claim Rules dialog…' Met de 'Claims Rules dialog' worden de attributen geconfigureerd. Dit zie je later in het configuratieproces.



8. Klik op 'Close' om deze configuratie af te ronden.

ADFS 2.0-Proxy inrichten

Inleiding

Je hoeft de ADFS-proxy niet op een aparte machine te installeren. Je kunt een bestaande machine gebruiken die ook voor andere doeleinden wordt toegepast, zolang deze maar niet in het Domain opgenomen is en alleen via local-admin account beheerd wordt

Om een ADFS 2.0-proxy te installeren moet je de volgende stappen doorlopen:

1. Installeer en configureer Windows Server 2008.
2. Installeer ADFS 2.0-software.
3. Configureer de instellingen van de ADFS2.0-proxy.

Windows Server 2008 installeren en configureren voor ADFS 2.0-proxy

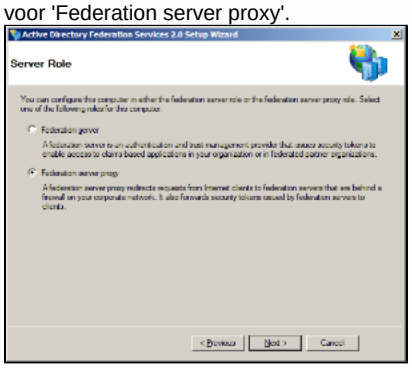
Om een ADFS 2.0-proxy in te richten, moet je eerst Windows Server 2008 installeren en configureren.

Hiervoor moet je de volgende stappen doorlopen:

1. Installeer de juiste versie van het besturingssysteem op de server: Windows Server 2008 SP2 of Windows Server 2008 R2 (standaard of enterprise).
2. Stel de tijd op de server correct in en zorg ervoor dat je deze synchroniseert met een time server.
3. Zorg ervoor dat de server niet is opgenomen in het domein van de Active Directory waaruit de accounts voor de SURFconext federatie komen.
4. Installeer Internet Information Services (IIS) en zorg dat deze een geldig SSL-servercertificaat heeft. Je moet hiervoor het certficaat dat gebruikt is op de server exporteren en op deze server importeren.
   Je kunt servercertificaten (onder meer) verkrijgen via de SURFcertificaten-dienst van SURFnet: http://www.surf.nl/diensten-en-producten/surfcertificaten/index.html
5. Zorg ervoor dat het certificaat van de IIS-installatie op de ADFS 2.0-server vertrouwd wordt door de ADFS 2.0 proxy-server. Als het certificaat van de ADFS2.0-server getekend is door een lokale Certificate Authority (zoals een Certificate Server in het Active Directory-domein), dan moet je het certificaat van de lokale Certificate Authority toevoegen in de ‘Trusted Root Certificate’-store van het ADFS2.0-server computeraccount.

ADFS 2.0 Proxy-software installeren

Zie ADFS 2.0-software installeren voor het installeren van de ADFS 2.0-software, met het verschil dat je bij stap 3 moet kiezen voor 'Federation server proxy'.

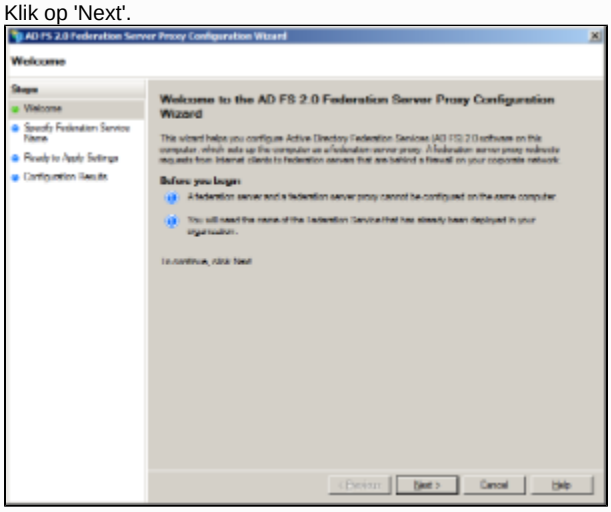


ADFS 2.0-proxyconfiguratie

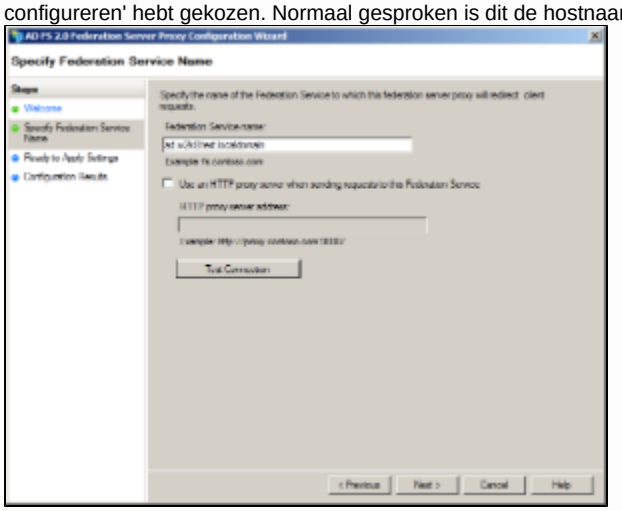
Doorloop voor het configueren van de ADFS 2.0-proxyconfiguratie de volgende stappen:

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

2. Klik op 'Next'.



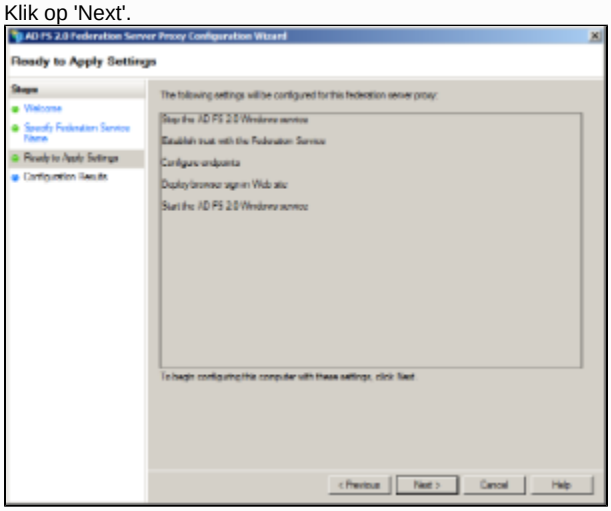
3. Vul in het veld 'Federation Service name' de naam in van de ADFS 2.0-server die je bij 'Basisinstellingen ADFS 2.0 configureren' hebt gekozen. Normaal gesproken is dit de hostnaam van de ADFS 2.0-server. Klik op 'Next'.



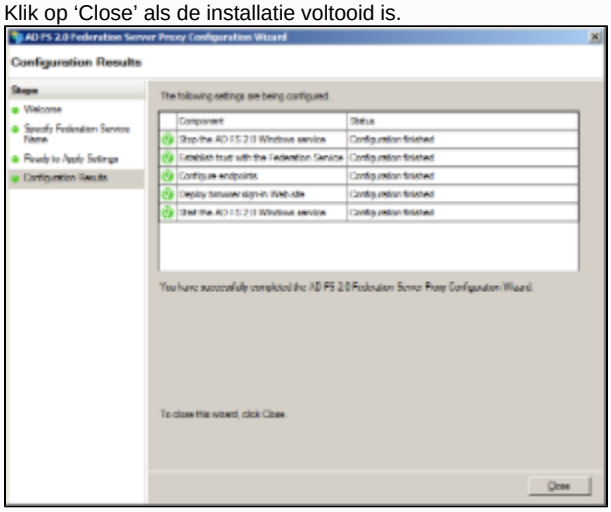
4. De pop-up geeft aan dat er een succesvolle verbinding van de proxy naar de server gelegd is. Klik op 'OK'.

5. Voer de gebruikersnaam en het wachtwoord in van het administrator account van de ADFS 2.0-server en klik op 'OK'.

6. Klik op 'Next'.



7. Klik op ‘Close’ als de installatie voltooid is.



DNS configureren

Als de server en de proxy zijn ingericht, moet je 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.

Om de IP-adressen van de ADFS 2.0-server en -proxy in het DNS te registreren, moet je de volgende stappen doorlopen:

- Het adres ‘adfs.example.nl’ moet voor verzoeken vanaf je eigen domein resolven naar de ADFS 2.0-server.
- Het adres ‘adfs.example.nl’ moet voor verzoeken vanaf externe domeinen resolven naar de ADFS 2.0-proxy.

Je kunt de proxy testen door op een clientmachine tijdelijk de HOSTS-file aan te passen naar de nieuwe situatie.

Testen installatie en configuratie

Om te testen of de installatie en configuratie goed is uitgevoerd en je op de juiste manier toegang hebt tot SURFconext, moet je de volgende stappen doorlopen:

1. Stuur een e-mail naar het SURFconext-team (support@surfconext.nl), waarin je aangeeft dat je als Identity Provider op SURFconext wilt aansluiten met je ADFS 2.0-server. Geef daarbij de URL van de ADFS 2.0-server door (adfs.mycampus.nl).
2. Wacht tot jouw gegevens geconfigureerd zijn (je krijgt hierover een e-mail) en test via de debug-pagina.

Loginpagina aanpassen

Je kunt nu de standaard login-pagina op de ADFS-proxy aanpassen naar de look-and-feel van jouw instelling. Dit doe je door onderstaande file te wijzigen:

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

Neem hier bij voorkeur tekst op over:

- de manier waarop gebruikers moeten inloggen; bijvoorbeeld in welk formaat de user identifier moet worden ingevoerd (bijvoorbeeld ‘student nummers’ of ‘NetID’)
- een waarschuwing dat (bijvoorbeeld bij gebruik op publieke terminals), uitloggen alleen gegarandeerd wordt als de browser wordt afgesloten
- dat de gebruiker bij het inloggen moet letten op een geldige HTTPS URL op de juiste server

Klik hier voor meer informatie over de richtlijnen voor het vormgeven van de loginpagina.

Attributen vrijgeven

Inleiding

Attributen zijn gebruikerskenmerken die de ADFS 2.0-server na een geslaagde authenticatie van een gebruiker kan toevoegen aan informatie die aan SURFconext wordt doorgegeven. Voorbeelden van attributen zijn het e-mailadres van de gebruiker of de naam van een groep waarvan de gebruiker lid is.

De set van gestandaardiseerde attributen die je binnen SURFconext kunt gebruiken, vind je hier:

https://wiki.surfnetlabs.nl/display/surfconextdev/Attributen+in+SURFconext

Voordat SURFconext attributen kan gebruiken in het authenticatieproces, moet je ze vrijgeven aan SURFconext. Hieronder vind je een voorbeeld van 4 attributen:

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

Deze attributen zijn slechts een voorbeeld. Als je wilt weten welke specifieke attributen jouw organisatie nodig heeft voor het benaderen van diensten via SURFconext, overleg hierover dan met SURFnet.

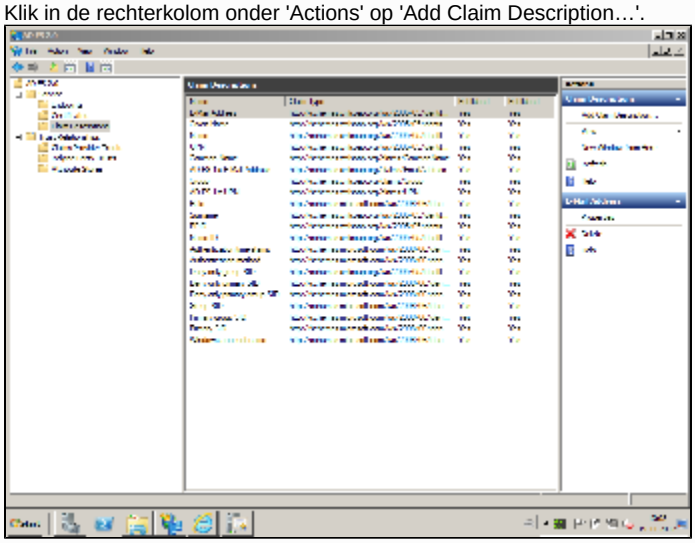
Verplichte attributen voor SURFconext zijn: het NameID, `urn:mace:dir:attribute-def:uid` en `urn:mace:terena.org:attribute-def:schacHomeOrganization`.

Bij het vrijgeven van attributen moet je de volgende stappen doorlopen:

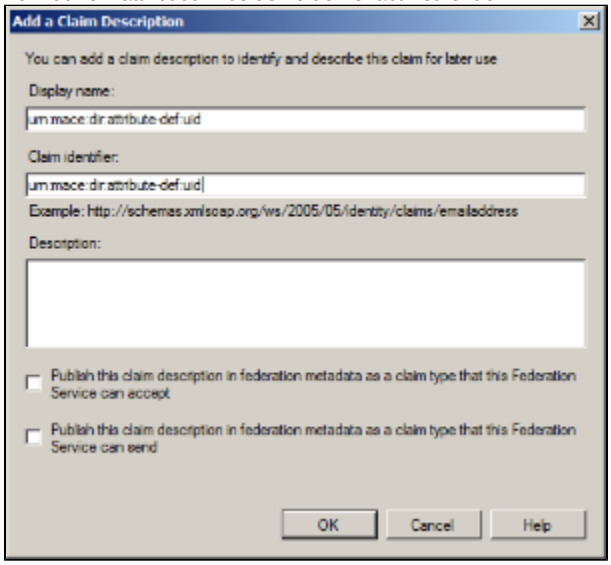
1. Definieer de attributen.
2. Wijs de attributen toe aan SURFconext.
3. Test of de attributen juist zijn vrijgegeven.

Attributen definiëren

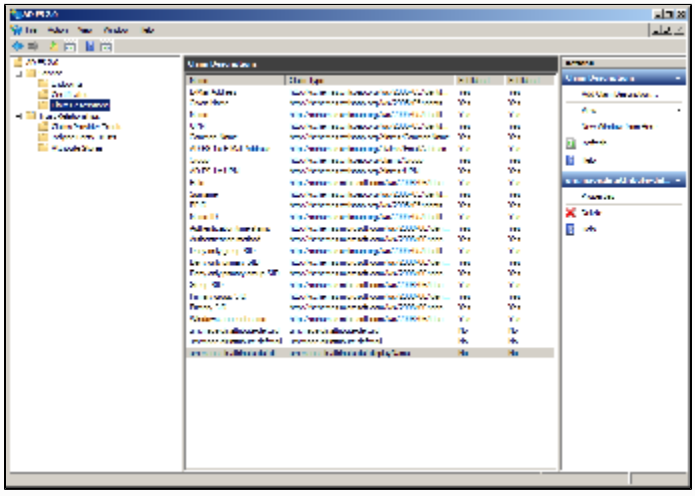
1. Kies op de 'ADFS 2.0-server Start' -> 'All programs' -> 'Administrative Tools' -> 'ADFS 2.0 Management' om de ADFS 2.0 configuratieapplicatie te starten.
2. 'Selecteer Service' -> 'Claims Descriptions' in de linker kolom van het overzichtsvenster.
3. Klik in de rechterkolom onder 'Actions' op 'Add Claim Description…'.



4. Vul in de velden 'Display name' en 'Claim identifier' de waarde in van het attribuut dat je wilt vrijgeven aan SURFconext. Zie voor een overzicht van attributen: Attributen in SURFconext
   Vul voor elk attribuut in beide velden exact hetzelfde in.



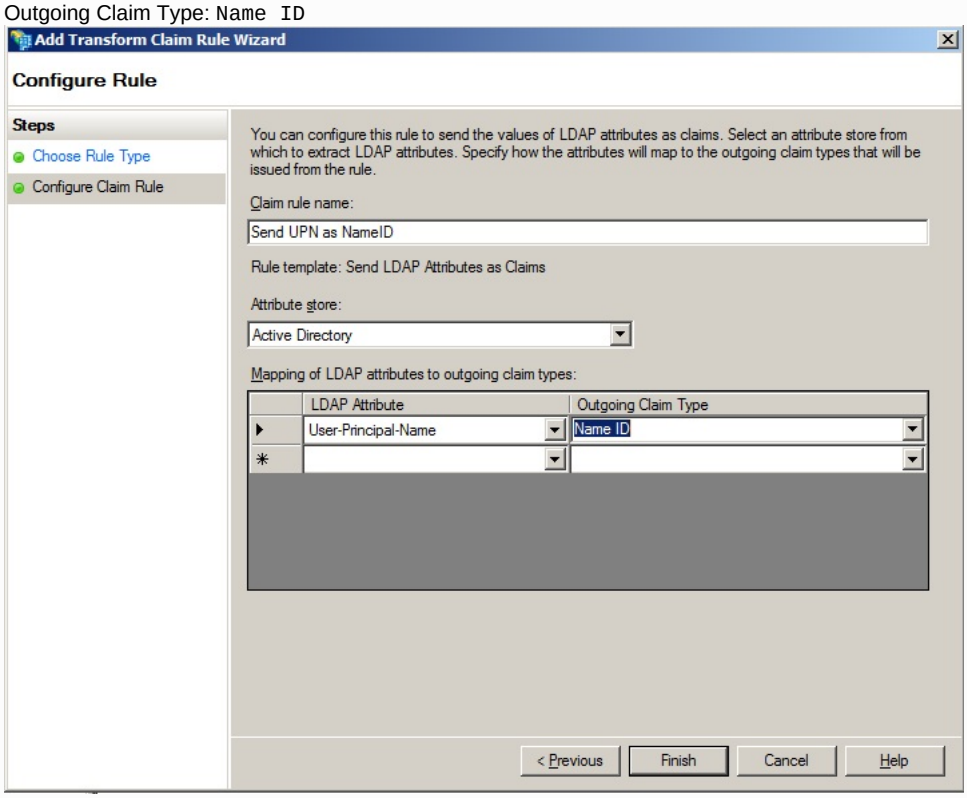
5. Klik op 'OK'.
6. Herhaal de voorgaande stap voor alle attributen, zodat deze onderaan in de lijst van Claim Descriptions verschijnen.



Toevoegen NameID

Het NameID in een SAML-bericht is feitelijk het onderwerp waarover attributen vrijgegeven worden en is verplicht in SURFconext. De exacte waarde maakt echter minder uit, omdat SURFconext richting Service Providers zelf een nieuw NameID genereert. Je kunt het vrijgeven met een waarde die de gebruiker uniek identificeert, zoals de User Principal Name, username/uid of een administratienummer. In ADFS kun je het als volgt aanpakken:

1. Claim Rule Template: Send LDAP Attributes as Claims
2. Claim Rule Name: Send UPN as NameID
3. LDAP Attribute: User-Principa- Name
4. Outgoing Claim Type: `Name ID`

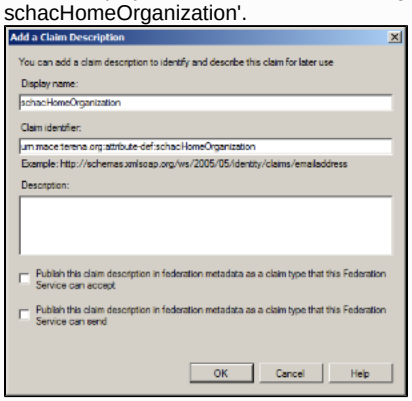


Toevoegen schacHomeOrganization

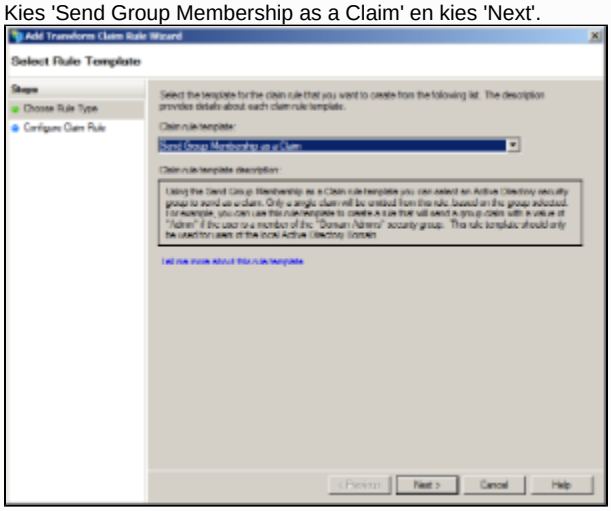
Het schacHomeOrgansation attribuut is verplicht voor gebruik van SURFconext. Dit attribuut moet voor alle gebruikers van de Identity Provider hetzelfde zijn. ADFS2 kent geen statische attributen of claims. De truc is dat je een 'Send Group Membership as a Claim' gebruikt, met als groep 'Domain Users'. Omdat dit altijd waar is, wordt het attribuut altijd toegevoegd.

Als je deze claim wilt toevoegen, moet je de volgende stappen doorlopen:

1. Kies op de 'ADFS 2.0-server Start' -> 'All programs' -> 'Administrative Tools' -> ADFS 2.0 Management om de ADFS 2.0 configuratieapplicatie te starten.
2. 'Selecteer Service' -> 'Claims Descriptions' in de linkerkolom van het overzichtsvenster.
3. Klik in de rechterkolom onder 'Actions' op 'Add Claim Description…'.
4. Vul de 'Display name' met 'schacHomeOrganization' en de 'Claim identifier' met 'urn:mace:terena.org:attribute-def:schacHomeOrganization'.

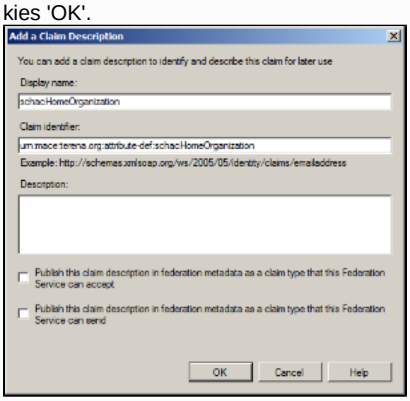


5. Plaats een vinkje voor onderstaande 2 opties:
    - 'Publish this claim ... Service can accept'.
    - 'Publish this claim ... Service can send'.
6. Kies 'OK'.
7. Selecteer 'ADFS 2.0' -> 'Trust Relationships' -> 'Relying Party Trusts'.
8. Selecteer 'SURFconext' en kies voor 'Edit Claim Rules...'.
9. Kies 'Add Rule...'.
10. Kies 'Send Group Membership as a Claim' en kies 'Next'.



11. Vul in:
    - 'Claim rule name' met 'schacHomeOrganization'.
    - 'User's group' met 'Domain Users'.
    - 'Outgoing claim type' met 'schacHomeOrganization'.
    - 'Outgoing claim value' met de gewenste waarde.

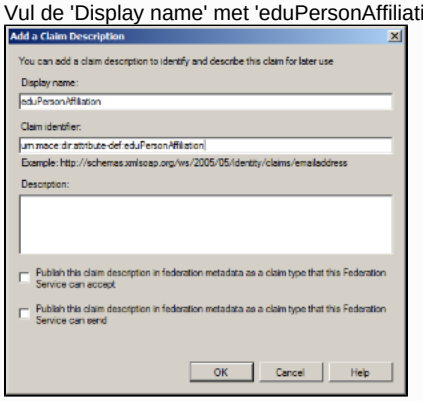
    kies 'OK'.

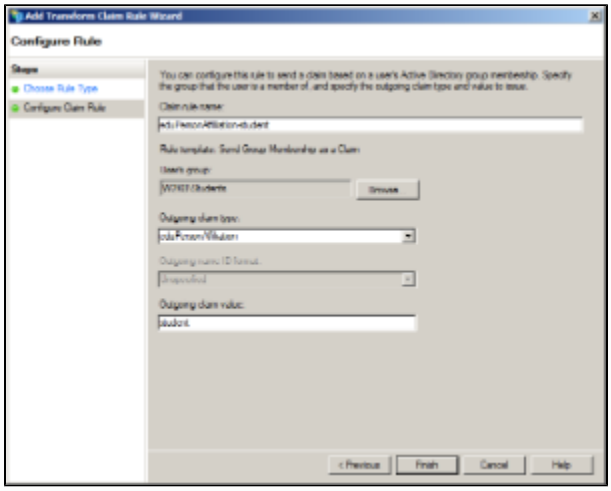


Toevoegen eduPersonAffiliation

Met het eduPersonAffiliation-attribuut kun je de relatie van de gebruiker met de instelling aangeven. Deze relatie wordt bepaald aan de hand van een groepslidmaatschap. Je kunt meerdere waarden als eduPersonAffiliation meegeven door meerdere eduPersonAffiliation claims toe te voegen. Ook kun je meerdere eduPersonAffiliation claims dezelfde waarde geven.

Voor het toevoegen van eduPersonAffiliation claim moet je de volgende stappen doorlopen:

1. Kies op de 'ADFS 2.0-server Start' -> 'All programs' -> 'Administrative Tools' -> 'ADFS 2.0 Management' om de ADFS 2.0 configuratieapplicatie te starten.
2. Selecteer 'Service' -> 'Claims Descriptions' in de linkerkolom van het overzichtsvenster.
3. Klik in de rechterkolom onder 'Actions' op 'Add Claim Description…'.
4. Vul de 'Display name' met 'eduPersonAffiliation' en de 'Claim identifier' met 'urn:mace:dir:attribute-def:eduPersonAffiliation'.


5. Plaats een vinkje voor onderstaande 2 opties:
    - 'Publish this claim ... Service can accept'.
    - 'Publish this claim ... Service can send'.
6. Kies 'OK'.
7. Selecteer 'ADFS 2.0' -> 'Trust Relationships' -> 'Relying Party Trusts'.
8. Selecteer SURFconext en kies voor 'Edit Claim Rules...'.
9. Kies 'Add Rule...'.
10. Kies 'Send Group Membership as a Claim' en kies 'Next'.
11. Vul in:
    - 'Claim rule name' met bijvoorbeeld 'eduPersonAffiliation-student'.
    - 'User's group' met bijvoorbeeld 'Students'.
    - 'Outgoing claim type' met 'eduPersonAffiliation'
    - 'Outgoing claim value' met de gewenste waarde (bijvoorbeeld 'student').
      Kies 'Finish'.


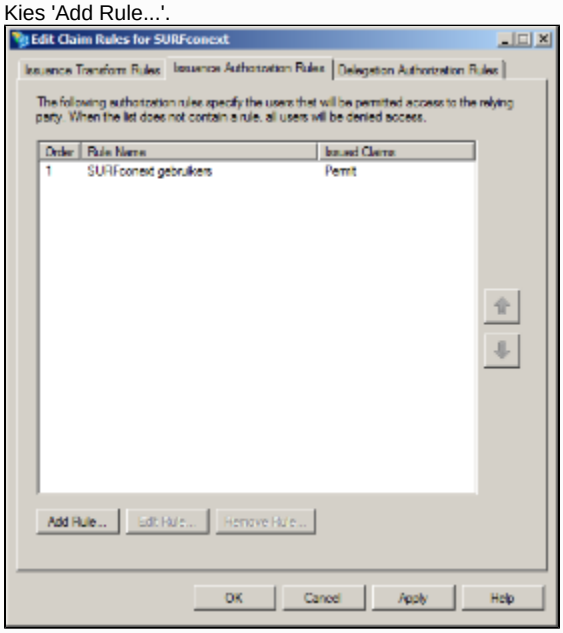
12. Herhaal stap 7 t/m 11 als je meerdere affiliations wilt toevoegen, zoals bijvoorbeeld 'employee'.

Beperken gebruik op basis van groepslidmaatschap

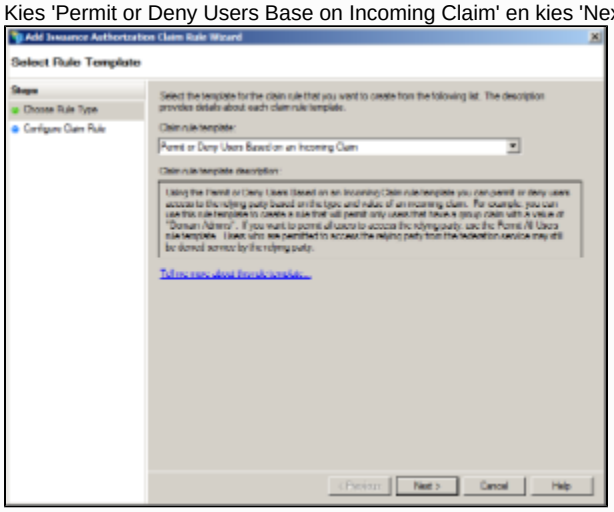
Met de standaardinstallatie van ADFS 2.0 kunnen alle gebruikers binnen de Active Directory gebruikmaken van de federatieve koppeling. Dit is dus inclusief alle Service Accounts. Als je 'Issuance Authorization Rules' instelt, kun je het gebruik beperken tot leden van 1 of meerdere groepen of op basis van attributen (claims) van de gebruikers.

Het volgend voorbeeld beperkt het gebruik tot leden van 1 bepaalde groep SURFconext-gebruikers.

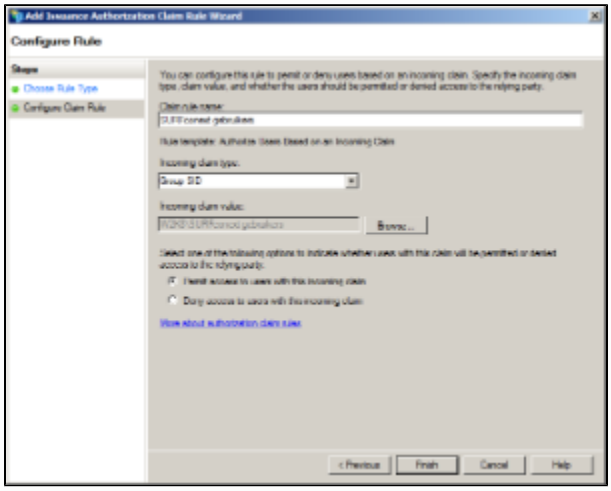
1. Kies op de ADFS 2.0-server 'Start' -> 'All programs' -> 'Administrative Tools' -> 'ADFS 2.0 Management' om de ADFS 2.0 configuratieapplicatie te starten.
2. Selecteer 'ADFS 2.0' -> 'Trust Relationships' -> 'Relying Party Trusts'.
3. Selecteer 'SURFconext' en kies voor 'Edit Claim Rules...'.
4. Ga naar het tabblad: 'Issuance Authorization Rules'.
5. Kies 'Add Rule...'.



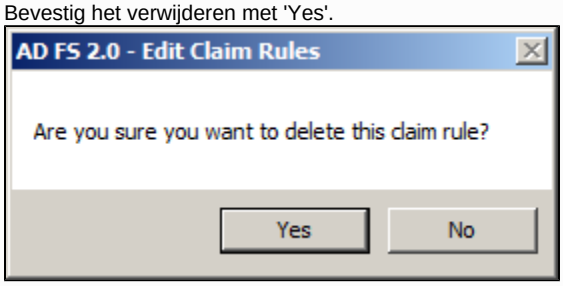
6. Kies 'Permit or Deny Users Base on Incoming Claim' en kies 'Next'.



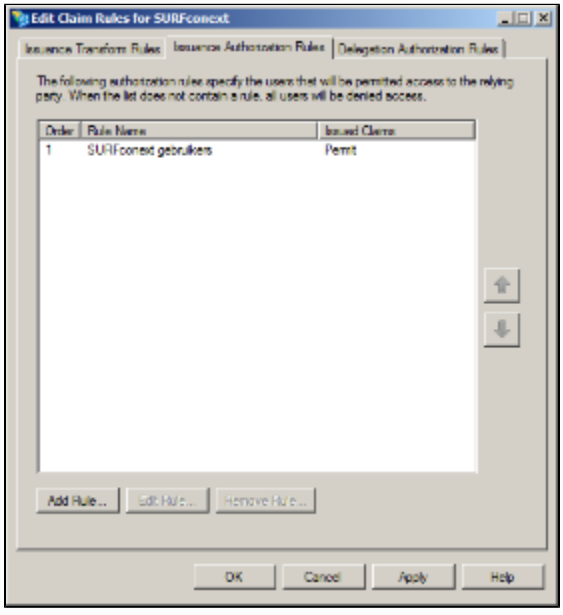
7. Vul in:
    - 'Claim rule name' met bijvoorbeeld 'SURFconext gebruikers'.
    - 'Incoming claim type' met bijvoorbeeld 'Group SID'.
    - 'Incoming claim value' browse naar de gebruikersgroep (bijvoorbeeld 'SURFconext gebruikers').
      Zorg dat je 'Permit access to users within this incoming claim' selecteert.
      Kies 'Finish'.



8. De standaard Rule 'Permit Access to All Users' kun je verwijderen door deze te selecteren en op 'Remove Rule...' te klikken.
9. Bevestig het verwijderen met 'Yes'.



10. Kies 'OK'.



Toevoegen eduPersonScopedAffiliation

Om eduPersonScopedAffiliation toe te voegen aan de ADFS claims kan de volgende Custom claims rule gebruikt worden, er vanuit gaande dat de claims "urn:mace:dir:attribute-def:eduPersonAffiliation" en "urn:mace:terena.org:attribute-def:schacHomeOrganization" zoals eerder in deze handleiding beschreven, correct gedefinieerd zijn.

Kies weer voor "Edit Claim rules" en "Add Rule". Kies in het volgende scherm voor "Send Claims Using a Custom Rule" en klik op "Next".

Geef de Rule een beschrijvende naam zoals "Create eduPersonScopedAffiliation" en plak de volgende code in het "Custom Rule" venster:

c1: [Type == "urn:mace:dir:attribute-def:eduPersonAffiliation"] && c2:[Type == "urn:mace:terena.org:attribute-def:schacHomeOrganization"] => issue(Type = "urn:mace:dir:attribute-def:eduPersonScopedAffiliation", Value = c1.Value + "@" + c2.Value);

Klik "Finish" en klik "Ok" in de "Edit Claims Rules" dialoog. Test hierna de uitgifte van het nieuwe attribuut.