ADFS-koppeling met Vaccinatieregister.nl t.b.v. Single Sign-on

Versie 1.0
27 juli 2018

Inhoudsopgave

1 Introductie

VR biedt organisaties de mogelijk voor zogenaamde ‘Single Sign-on’ (SSO) gebaseerde authenticatie via Windows ADFS (Active Directory Federation Services) en met gebruikmaking van het SAML2.0 protocol.

Hiermee kan een gebruiker, wanneer ingelogd op de eigen (CITRIX) werkplek automatisch doorloggen in VR. Dit maakt het gebruik van een apart login/wachtwoord of Two Factor Authenticatie (TFA) om in te loggen in VR overbodig.

Een belangrijk voordeel van ADFS naast het SSO, is dat gebruikers centraal in ADFS beheerd kunnen worden en bij een eventueel vertrek van een medewerker centraal de toegang tot de werkplek én automatisch ook tot VR geweigerd kan worden.

Doordat het middels de ADFS-koppeling vooralsnog niet mogelijk is autorisaties centraal te managen, zullen in VR altijd gebruikers met de juiste autorisaties opgevoerd en/of gewijzigd moeten blijven worden (bijv. Admin, Baliemedewerkers, Medisch personeel, beheerders, etc).

Dit document beschrijft de inrichting om de ADFS-koppeling met VR te realiseren.

2 Randvoorwaarden

Voor de SSO-koppeling tussen VR met de organisatie is het volgende nodig:

1. ADFS binnen de organisatie, geïnstalleerd en geconfigureerd middels KB artikel
2. Geldige gebruikers binnen Active Directory van de organisatie, elk met een geldig email adres.
3. De nodige SSL-certificaten voor secure communicatie naar ADFS en VR middels het HTTPS protocol.
4. Een ADFS-beheerder die de nodige setup voor VR in ADFS kan configureren en klaarzetten.
5. De specifieke 'SAML 2.0/W-Federation' URL in de ADFS Endpoints sectie
6. Communicatie tussen:
   a. de ID Provider (ADFS van de organisatie), hierna kortweg IDP genoemd,
   b. de Services Providers (VR acceptatie + productie), hierna kortweg SP genoemd.

3 Doorlooptijd

In de regel is het inrichten en configureren van ADFS in een dagdeel gerealiseerd (voor zowel VR-acceptatie als productie, mits aan de in paragraaf 2 vermelde randvoorwaarden zijn voldaan.

4 Stappenplan

4.1 Stap 1 – Aanmaken van ‘Relying Party Trust’ in ADFS

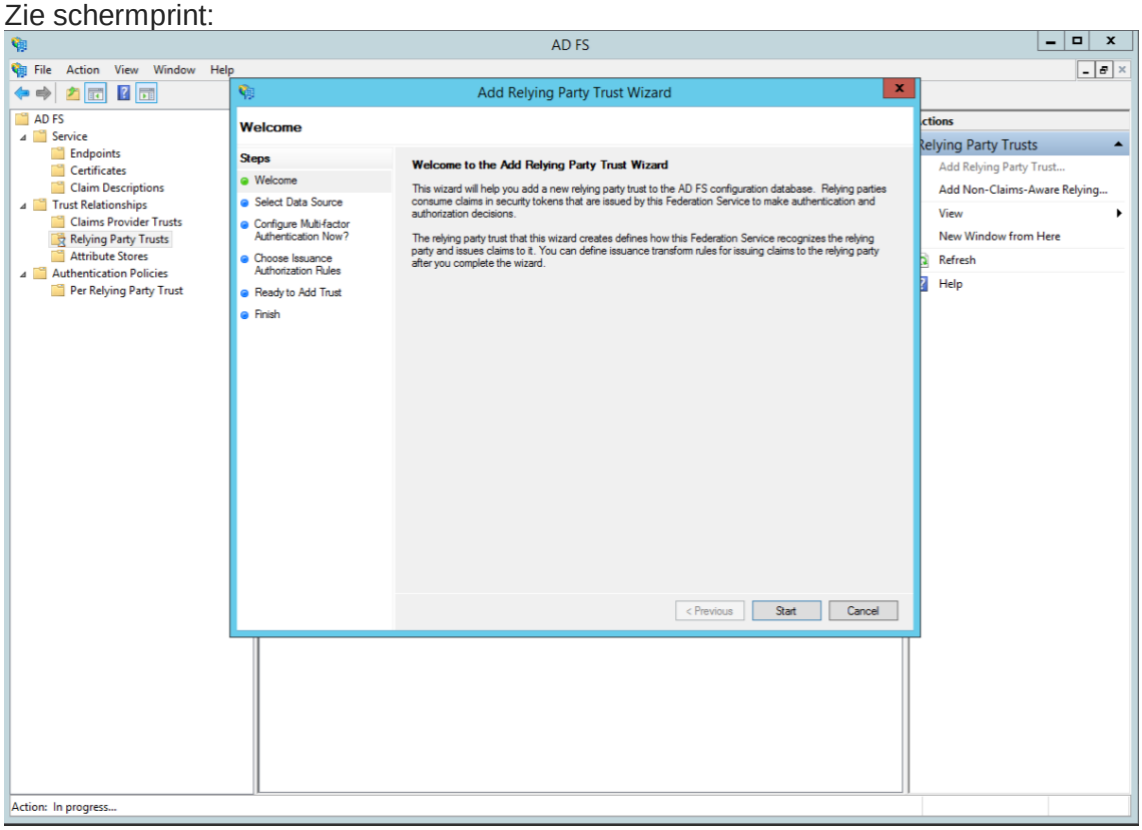
De connectie tussen ADFS en VR is gedefinieerd met gebruikmaking van een zogenaamde Relying Party Trust (RPT).

Een RPT bestaat uit een verscheidenheid aan identifiers, namen en regels die een externe web toepassing identificeren aan ADFS.

Ga als volgt te werk om deze RPT aan te maken:

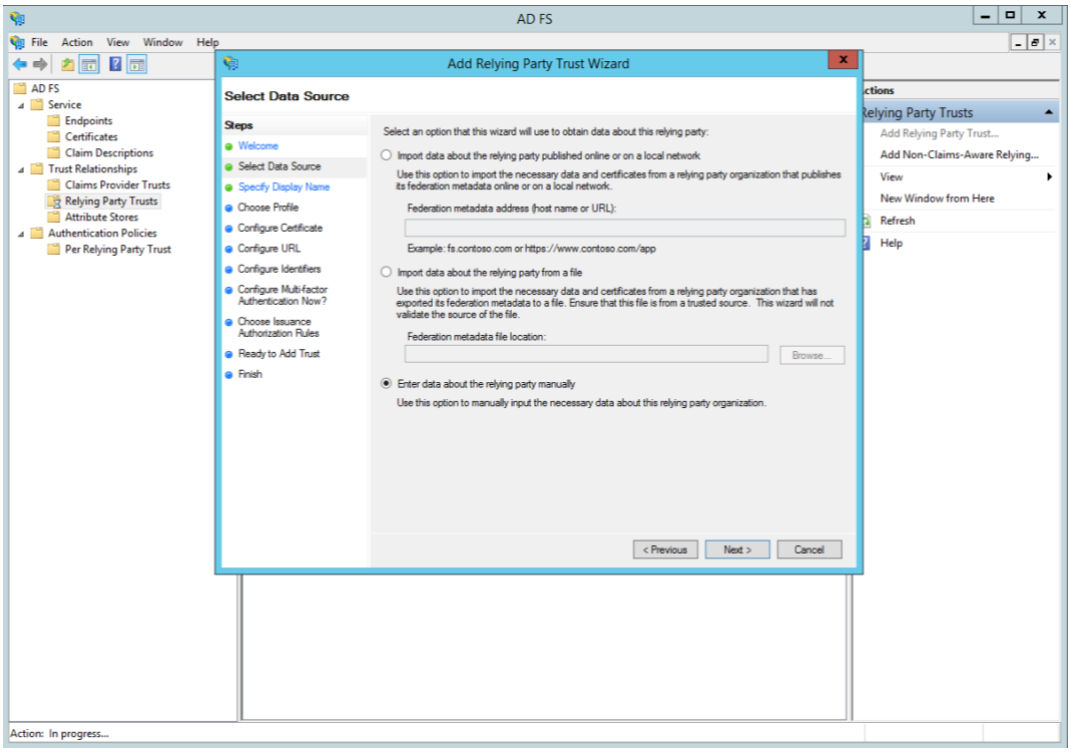
Ga naar de ‘Relying Party Trusts’ folder vanuit ADFS Management en selecteer ‘add a new Standard Relying Party Trust’ vanuit de ‘Actions’ sidebar. Vervolgens wordt de configuratie wizard voor een nieuwe trust gestart.

Zie schermprint:

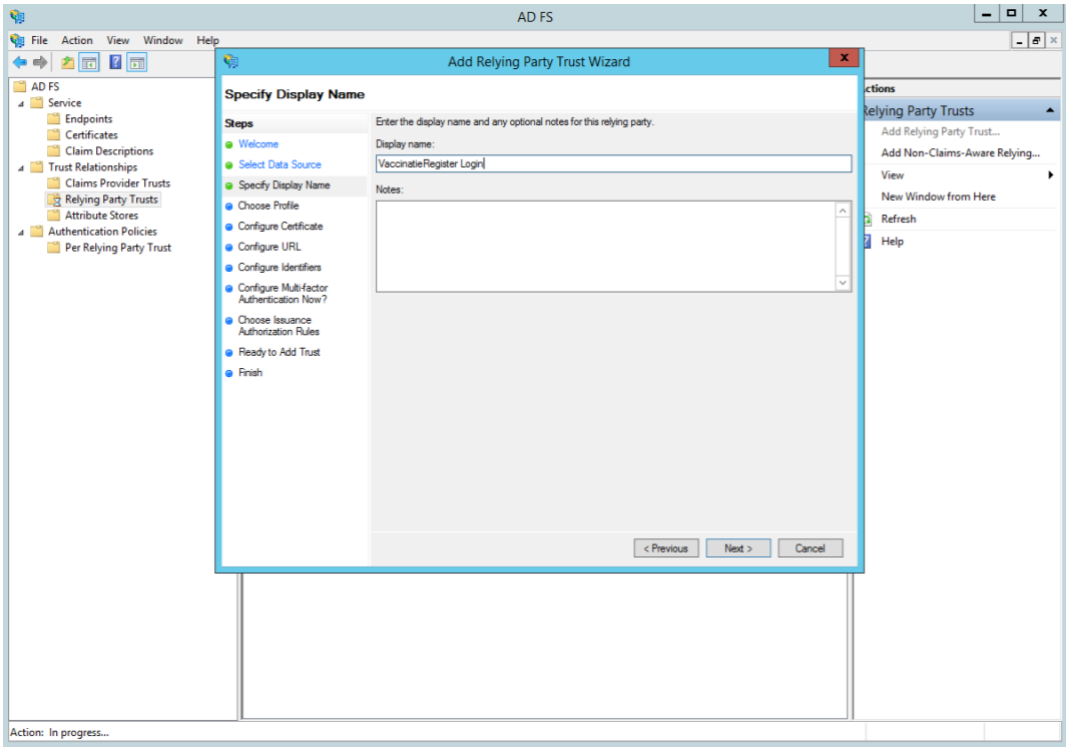


Voer vervolgens achter elkaar de volgende acties uit:

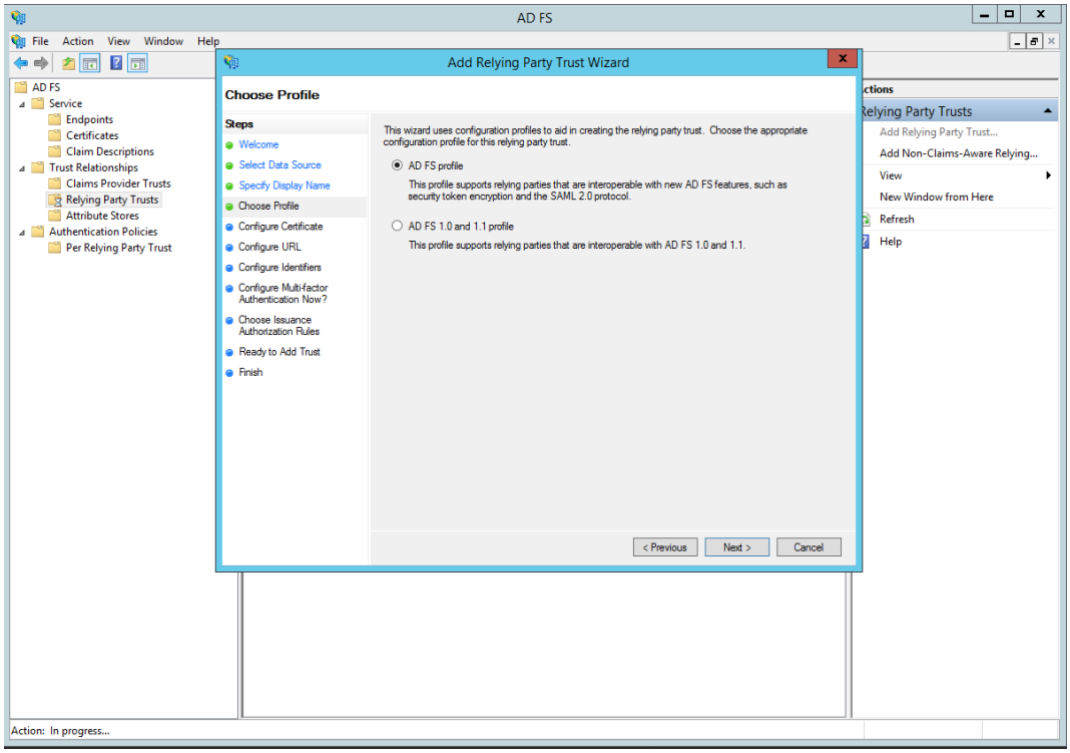
1. In het ‘Select Data Source’ scherm selecteer vervolgens de laatste optie: “Enter data about the relying party Manually”



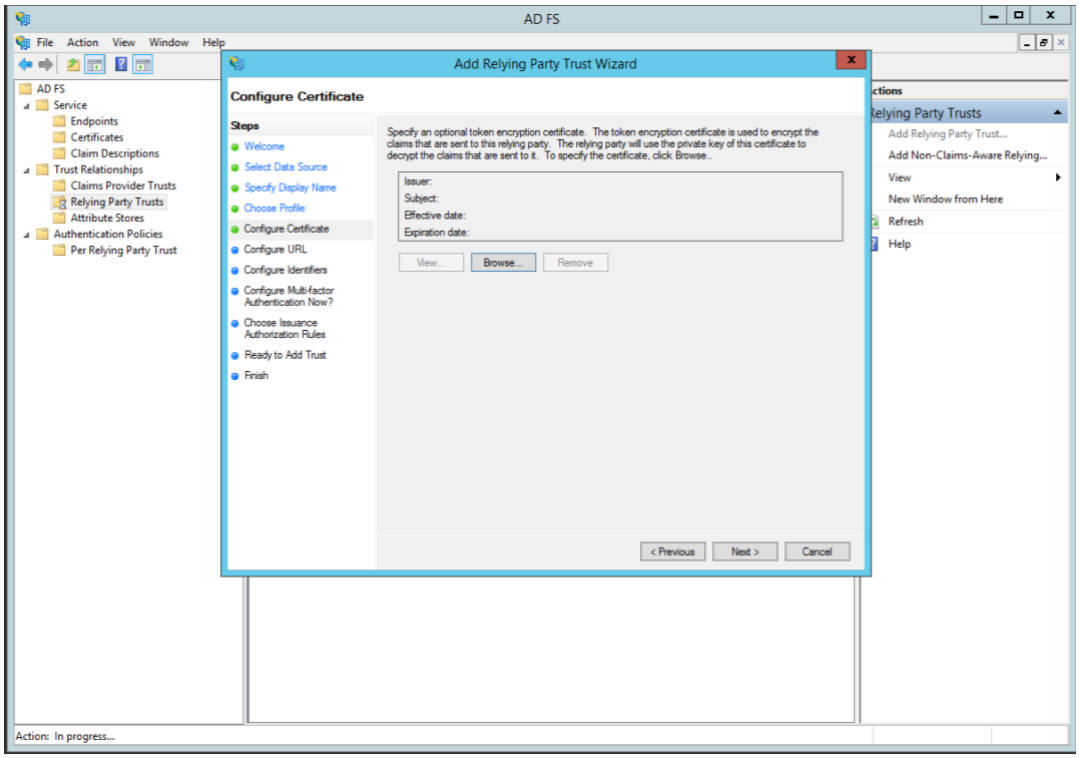
2. In het volgende scherm, voer een Display naam in die herkenbaar is inclusief eventuele van belang zijnde notities:



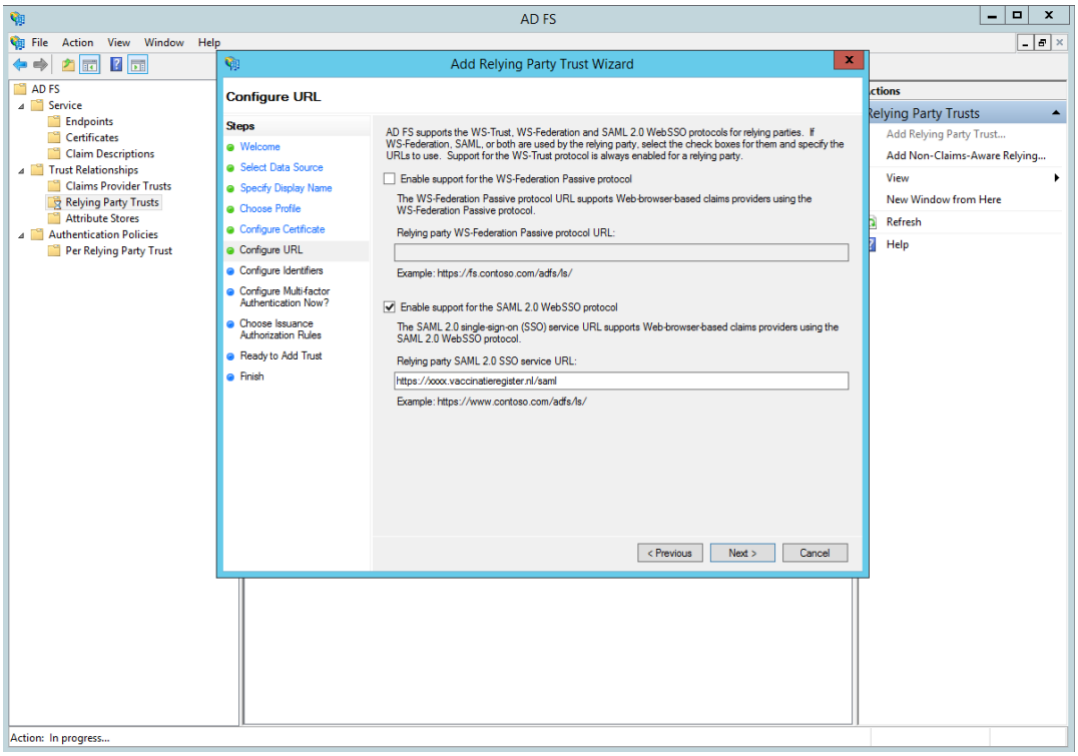
3. Op het volgende scherm, selecteer de radio button “ADFS FS profile”



4. Laat op het volgende scherm de certificaat details op ‘default’ staan



5. In het volgende scherm, selecteer de check box genaamd “Enable support for the SAML 2.0 WebSSO protocol”.



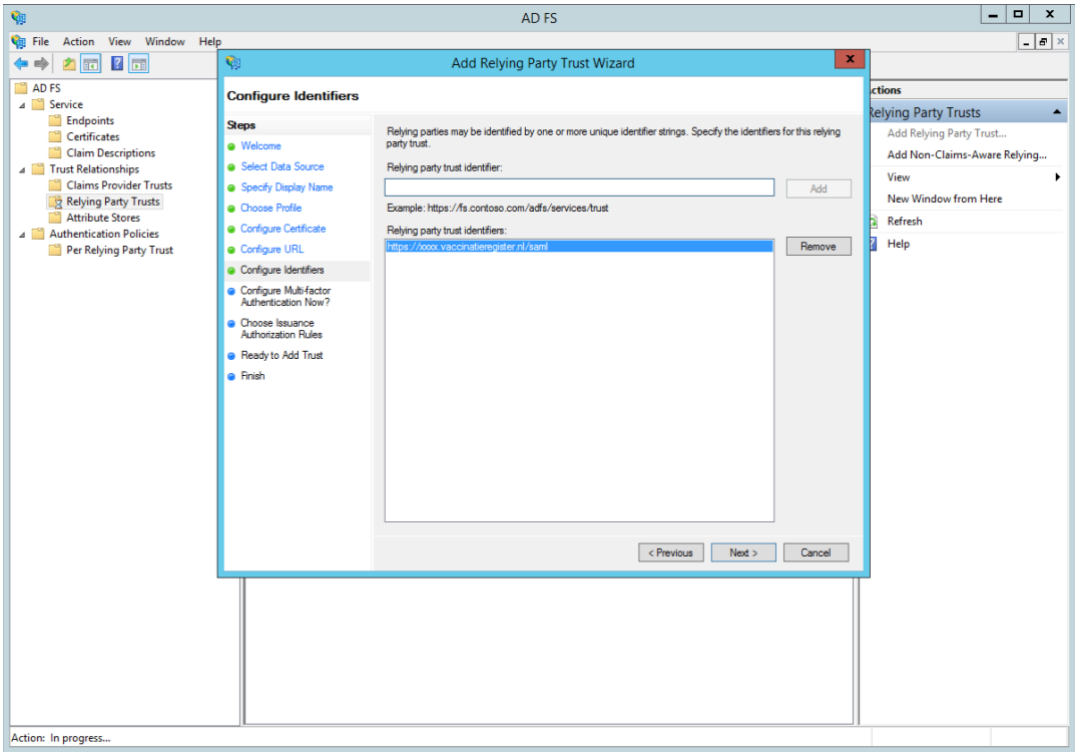
Het SAML service URL van Vaccinatieregister voor de betreffende organisatie dient hier ingevoerd te worden, als volgt:

https://<organisatie_id>.vaccinatieregister.nl/saml

In bovenstaand voorbeeld is https://xxxx.vacinatieregister.nl/saml ingevoerd.

LET OP:
- Protocol is HTTPS
- Aan het einde van het URL dient geen ‘/’ opgenomen te worden na het woord saml.

6. In het volgende scherm, voeg een ‘Reyling party trust identifier’ of subdomein van vaccinatieregister.nl toe

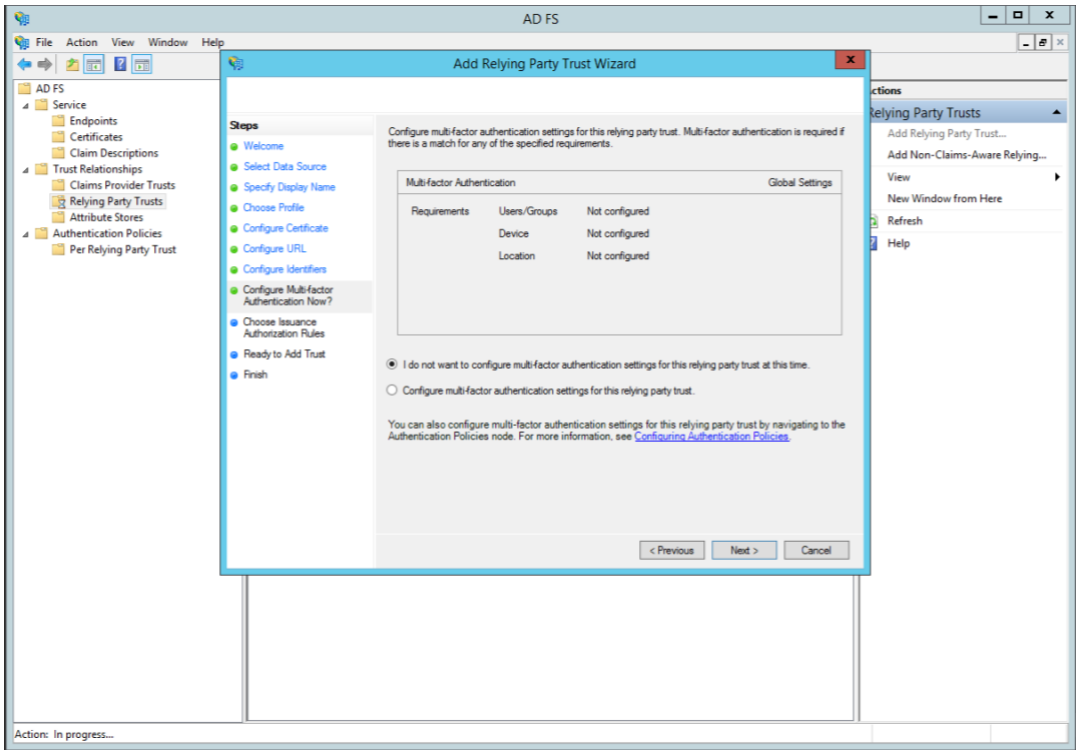


Nb: indien het subdomein.vaccinatieregister.nl een ‘request failure error’ geeft, voer dit domein dan in als URL inclusief https:// in, als volgt:

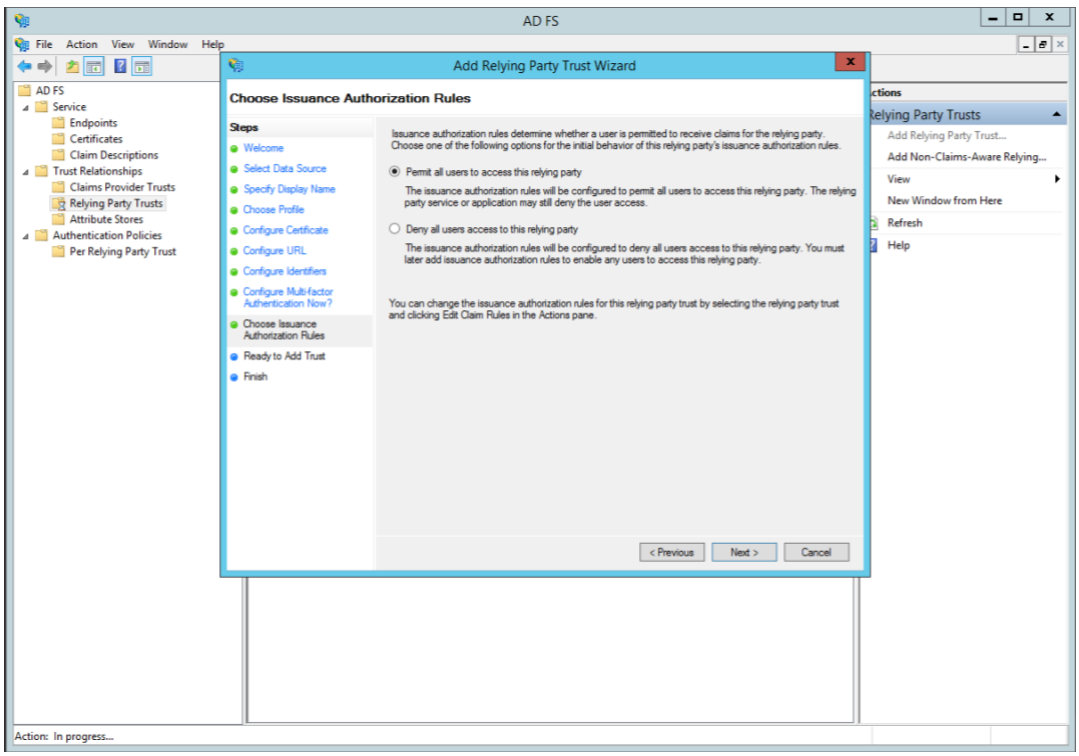
https://xxxx.vaccinatieregister.nl

Eventueel kan hier ook de Acceptatie-omgeving aan toegevoegd worden, bijv: https://xxxxdemo.vaccinatieregister.nl

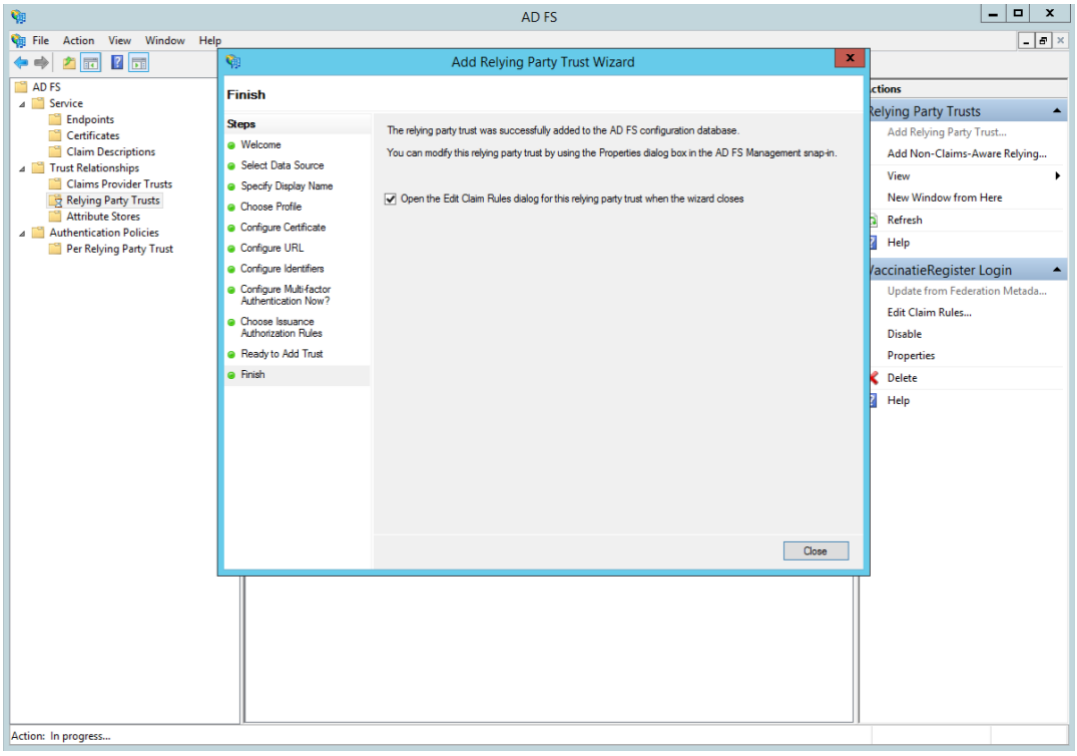
7. Op het volgende scherm zou multi-factor authenticatie geactiveerd kunnen worden, maar dit is buiten scope van deze handleiding.



8. Op het volgende scherm, selecteer “Permit all users to access this relying party”



9. Op de volgende twee schermen, zal de wizard een overzicht van de settings geven. Selecteer in het laatste scherm de ‘Close’ knop, waarna de “Claim Rules” editor wordt geopend. Ga vervolgens verder met de volgende stap (paragraaf 4.2).

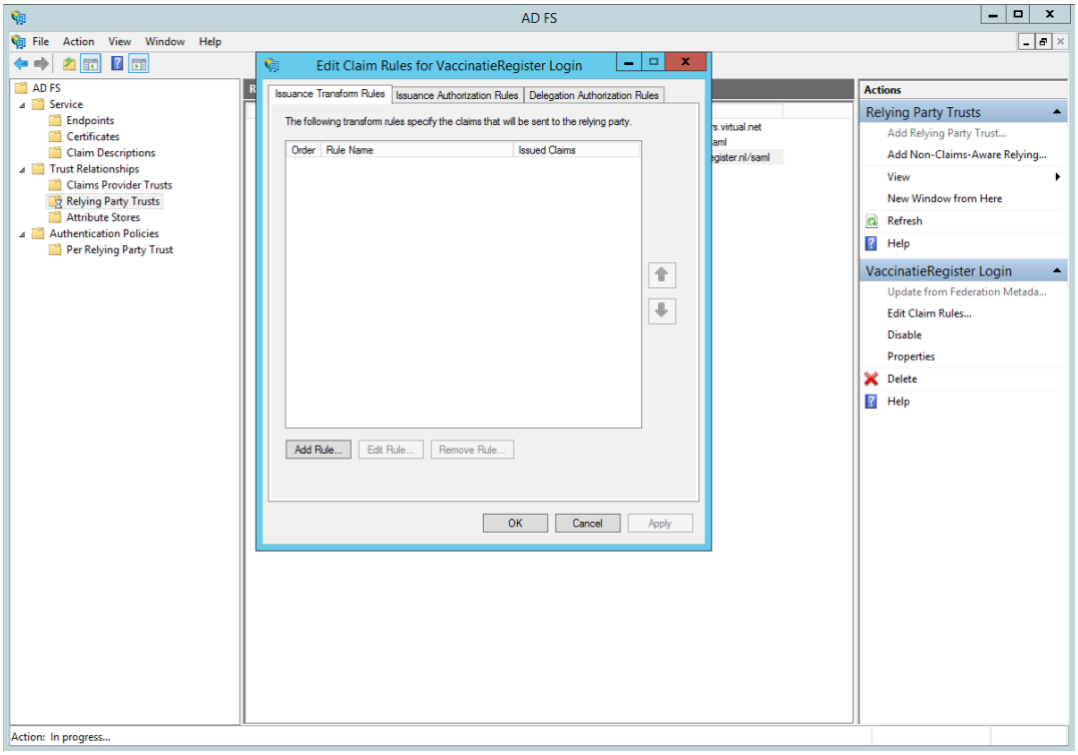


4.2 Stap 2 – Aanmaken ‘Claim’ regels in ADFS

Wanneer de “Relying Party Trust” is aangemaakt, moeten de zogenaamde ‘Claim’ regels aangemaakt worden en de RPT op enkele punten geüpdatet worden.

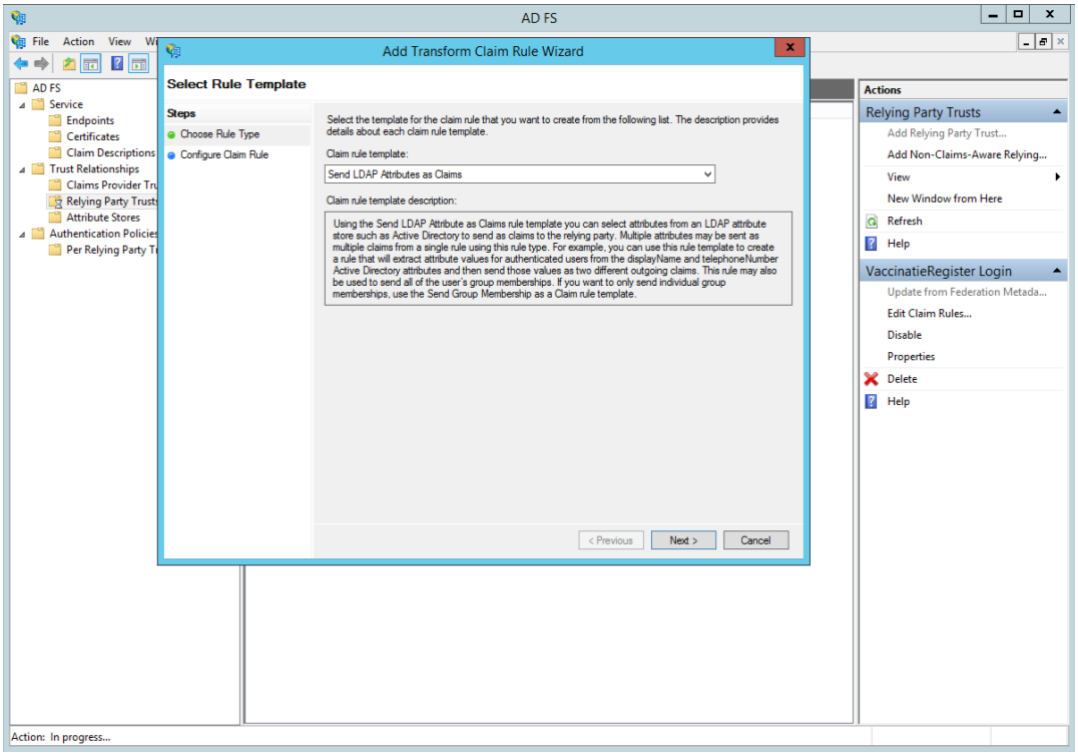
Na voorgaande stap zal automatisch de Claim regel editor worden geopend.

Zie voorbeeld:



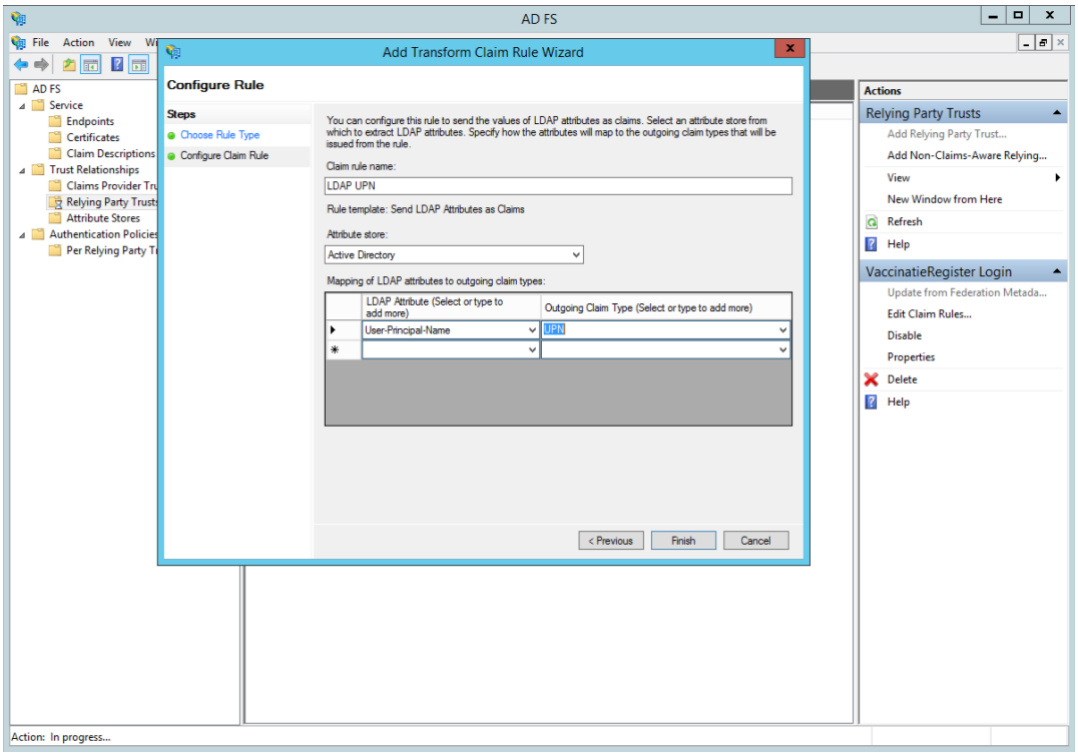
1. Om een nieuwe regel aan te maken, selecteer “Add Rule”.

Maak vervolgens een regel aan “Send LDAP Attributes as Claims”



2. Op het volgende scherm, selecteer Active Directory als Attribute store en doe het volgende:

   a. In de LDAP Attributen kolom, selecteer User-Principal-Name
   b. In de Outgoing Claim Type, selecteer UPN



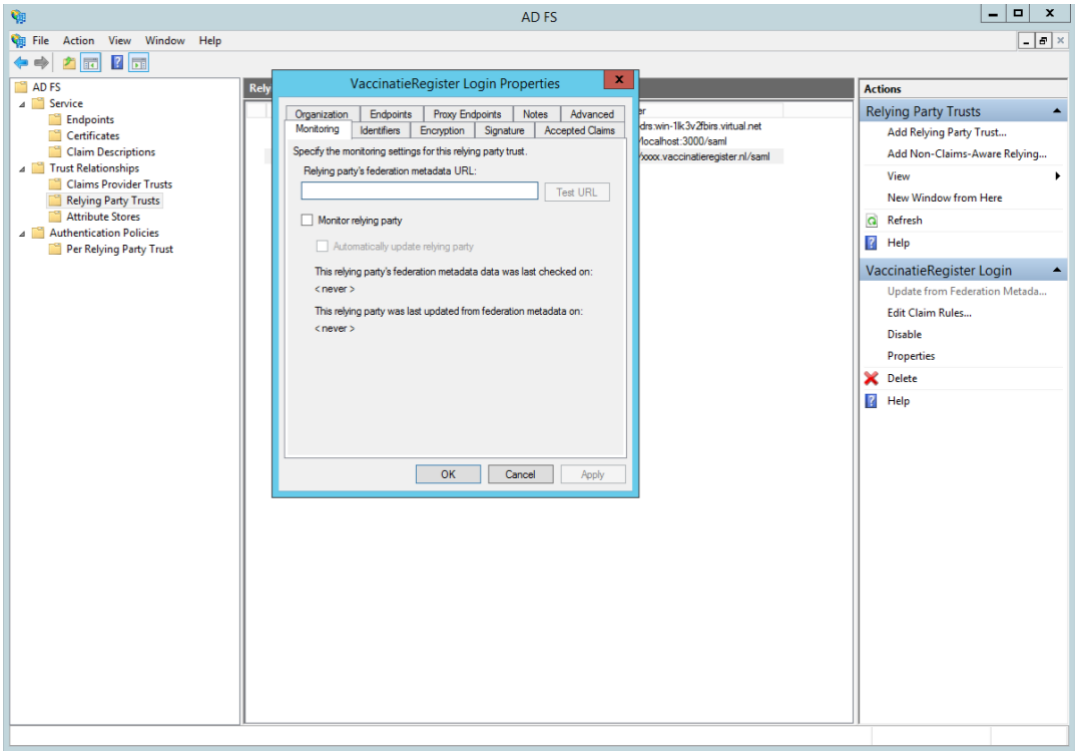
3. Click op Finish om deze nieuwe regel op te slaan.

Click vervolgens weer op OK en ga door met de volgende stap (paragraaf 4.3).

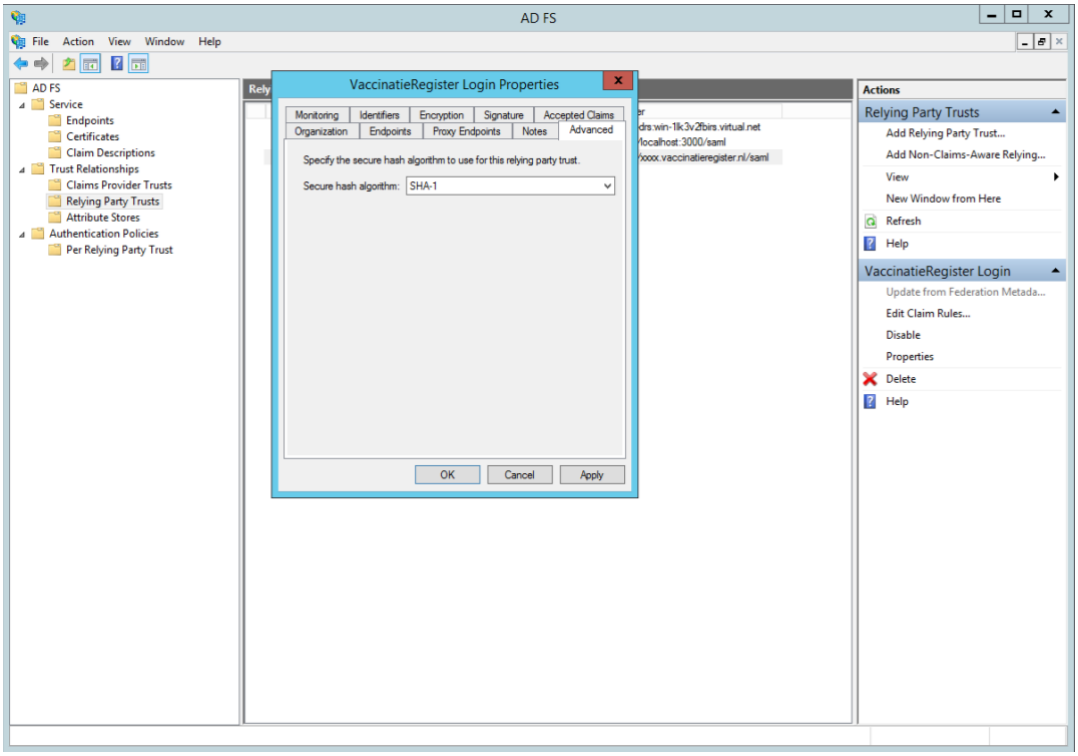
4.3 Stap 3 – Aanpassen van de ‘Trust’ settings in ADFS

Er moeten nog een aantal ‘Trust’ settings van de RPT worden aangepast. Selecteer hiervoor “Properties” vanuit de “Actions” navigatie kolom aan de zijkant van het ADFS-scherm.

1. Check dat de “Monitor relying party” uitgevinkt staat, als volgt:



2. In de Advanced tab, voer het Secure hash algoritme “SHA-1” in:



De beheerder van ADFS zal vervolgens een SAML logout Endpoint toevoegen met hieraan gekoppeld het Trusted ADFS url die er als voorbeeld als volgt uit ziet:

https://<fqdn van de adfs van organisatie>/adfs/ls/?wa=wsignout1.0

De binding is een zogenaamde ‘post’ binding:

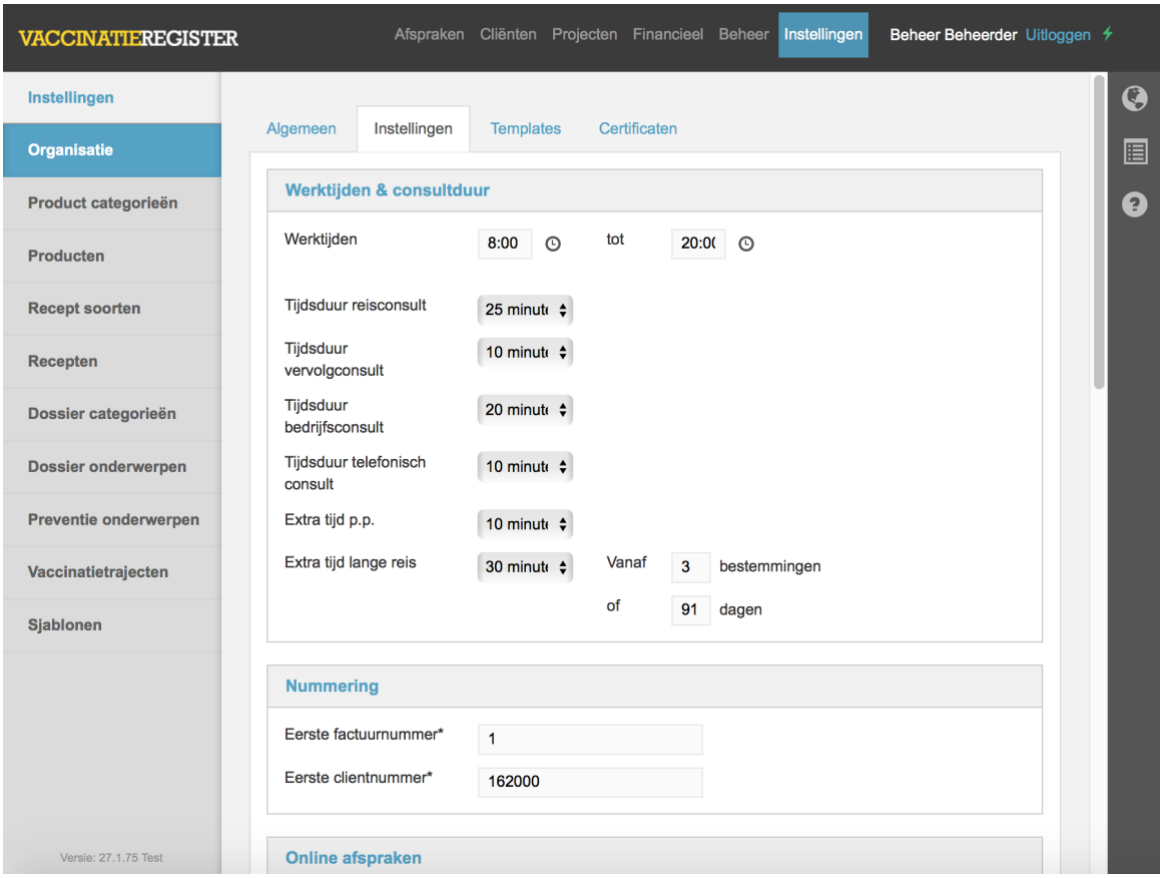
Waarbij:

<fqdn van de adfs van organisatie> = de fully qualified domain name van de adfs-server of adfs-proxy server

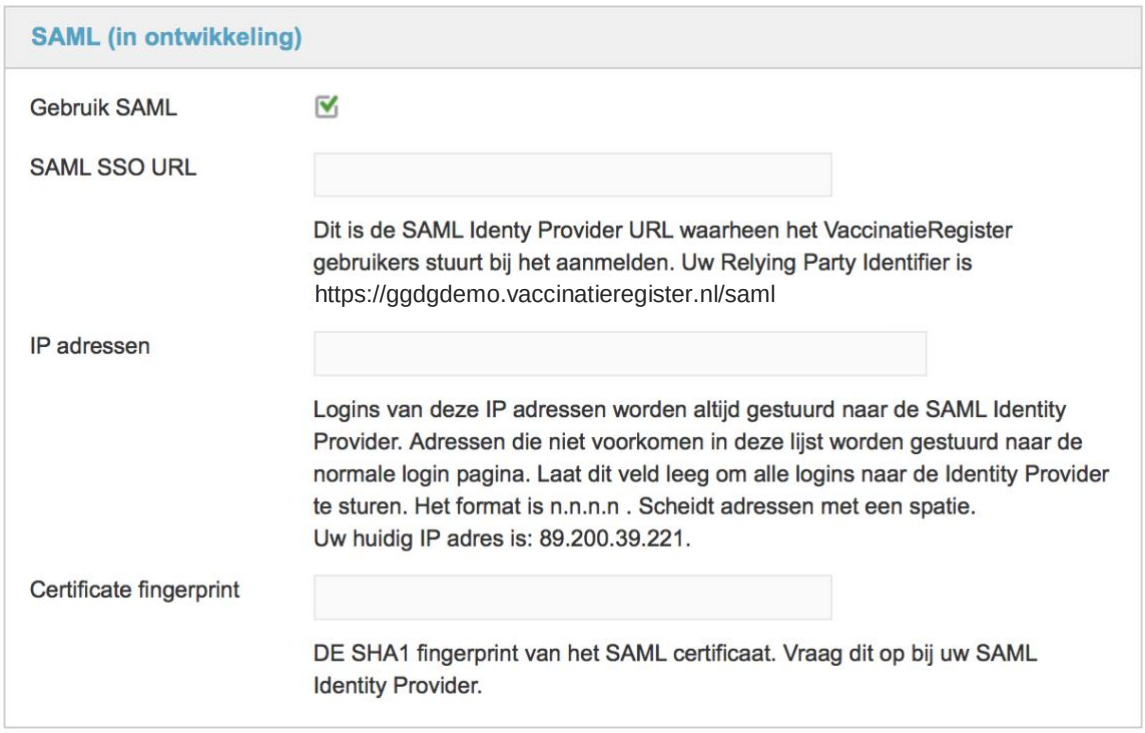
4.4 Stap 4 – Aanpassingen VR Acceptatie en Productie

Als laatste stap moet Vaccinatieregister geconfigureerd worden om middels SAML te authentiseren tegen de ADFS / ID Provider van de organisatie.

Log hiervoor in, in Vaccinatieregister als gebruiker met ‘beheer’ rechten. Selecteer vervolgens bovenin het hoofdmenu de keuze “Instellingen”, en in het “Organisatie” menu de sub optie “Instellingen”



Scroll naar beneden en voer vervolgens onderin dit scherm de “SAML” instellingen in, in nauw overleg met de ADFS-beheerder:



1. Vink de optie “Gebruik SAML”

2. Voer het SAML SSO URL in, als volgt:

   https://<fqdn van de adfs van organisatie>/adfs/ls

3. Voer hier (optioneel) de IP-adressen van waaruit middels SAML geauthentiseerd moet worden. Deze optie maakt het mogelijk om bijvoorbeeld alleen SAML mogelijk te maken indien de connectie naar VR wordt opgezet vanuit het kantoor van de organisatie, indien hier het IP-adres of adres range van de organisatie ingevoerd wordt. Alle niet ingevoerde IP-adressen maken gebruik van basic authenticatie (gebruikersnaam/wachtwoord) of Two Factor Authenticatie (TFA) zoals geconfigureerd in VR.

   Indien hier niets ingevuld wordt gaat alle communicatie over SAML.
4. Het certificate fingerprint is op te vragen bij de ADFS-beheerder. Deze is op een Windows ADFS server als volgt te verkrijgen:

   1. Start PowerShell op als Administrator
   2. Voer uit: Get-AdfsCertificate
   3. Kopieer de thumbprint van het Token Signing Certificate
   4. plak in het veld Certificate fingerprint van het SAML scherm

4.5 Stap 5 – Test vervolgens de connectie

De SAML-connectie kan vervolgens worden getest door herhaaldelijk in en uit te loggen door verschillende gebruikers, elk met een eigen rol en/of met gebruikmaking van specifiek voor dit doel opgezette test accounts.

Indien gebruik gemaakt wordt van SAML én van basic authenticatie of TFA test dit dan vanuit de verschillende locaties om vast te stellen dat dit ook werkt.

De koppeling tussen de gebruiker in Vaccinatieregister en de Windows gebruiker moet als volgt wordt gelegd: de username in Vaccinatieregister moet overeenkomen met de naam voor het '@' teken in de UPN, dwz

<VR gebruikersnaam>@<upn domain>