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

Versie 1.0 27 juli 2018

Inhoudsopgave

1	Ir	ntroductie	
2	R	andvoorwaarden	3
3	D)oorlooptijd	3
4	S	tappenplan	3
	4.1	Stap 1 – Aanmaken van 'Relying Party Trust' in ADFS	
	4.2	Stap 2 – Aanmaken 'Claim' regels in ADFS	
	4.3	Stap 3 – Aanpassen van de 'Trust' settings in ADFS	
	4.4	Stap 4 – Aanpassingen VR Acceptatie en Productie	
	4.5	Stap 5 – Test vervolgens de connectie	

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:			
%		AD FS	_ 🗆 X
输 File Action View Window Hel	P		_ 8 ×
🗢 🔿 🙍 🖬 👔	\$	Add Relying Party Trust Wizard	
AD FS	Welcome		ctions
Endpoints	Steps		Relying Party Trusts
Certificates	Welcome	Welcome to the Add Relying Party Trust Wizard	Add Relying Party Trust
▲ ☐ Trust Relationships	 Select Data Source 	This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and	Add Non-Claims-Aware Relying
Claims Provider Trusts	Configure Multi-factor	authorization decisions.	View
Attribute Stores	Authentication Now?	The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party	Refresh
A Carteria Authentication Policies	Authorization Rules	after you complete the wizard.	2 Help
Per Relying Party Trust	 Ready to Add Trust 		i nep
	 Finish 		
		< Previous Start Cancel	
Action: In progress			
Action: in progress			

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"

9		AD FS	_ 🗆 X
翰 File Action View Window He	P		_ 8 ×
🗢 🄿 🙇 📰 🛛 🖬	\$	Add Relying Party Trust Wizard	
AD FS	Select Data Source		ctions Relying Party Trusts
Certificates Claim Descriptions Truts Heltionships Claims Provider Truts Attribute Stores Attribute Stores Authentication Policies Per Relying Party Trust	Velicone Velicone Velicone Select Data Source Secoty Datalsy Name Configure Configure URL Configure Velice Configure Velice Configure Velice Configure Mathematic Ready to Add Truat Pinish	Select an option that this wixard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Lee this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (not name or URL): Example: fs contose com or hitps://www.contose.com/app Import data about the relying party from a life Use this option to import the necessary data and certificates from a relying party organization that has explored its federation metadata address (not certificates from a relying party organization that has explored its federation metadata file location: Federation metadata file location: Borwae Federation to metadata file location: Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization. 	Add Relying Party Trust Add Non-Claims-Aware Relying View New Window from Here Refresh Help

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

6 ⁶	AD FS	X
File Action View Window Help		_ #
	Add Relying Party Trust Wizard	<u>^</u>
AD FS Sp	pecify Display Name	ctions
a Service Service a Endpoints Service a Cartificates a a Trust Relationships a a Claims Provider Trusts a a Attribute Stores a a Attribute Stores a a Attribute Stores a a Authentication Policies a	pachage in the provided in the set of the se	telying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying View New Window from Here 2 Refresh 2 Help

%		AD FS	_ D X
Window He	lp		_ # ×
🗢 🔿 🖄 🗊	N	Add Relying Party Trust Wizard	
AD FS	Choose Profile		ctions
⊿ Gervice			Relying Party Trusts
Certificates	Steps	This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate	Add Relying Party Trust
Claim Descriptions	Welcome	configuration profile for this relying party trust.	Add Non-Claims-Aware Relying
⊿ Intrust Relationships	Select Data Source	AD FS profile	View
Claims Provider Trusts	Specify Display Name	This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.	New Window from Here
Attribute Stores	 Choose Profile 		B. Refresh
A Suthentication Policies	 Configure Certificate 	AD FS 1.0 and 1.1 profile	2 Help
Per Relying Party Trust	 Configure URL 	This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.	д пер
	 Configure Identifiers 		
	Configure Multi-factor Authentication Now?		
	Choose Issuance		
	Authorization Rules		
	 Ready to Add Trust 		
	 Finish 		
		< Previous Next > Cancel	
			_
Action: In progress			

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

9		AD FS	_ _ ×
Image: Window Hele Image: Provide the state of the	P (%)	Add Relying Party Trust Wizard	X
AD FS AD FS AD FS Catflicates Claim Descriptions Claim Service Claim Service Claim Service Trusts Relying Party Trusts Attribute Stores Attribute Stores Per Relying Party Trust	Configure Certificate Steps Welcome Select Data Source Sochy Daptay Name Croces Profile Configure Certificate Configure Matificator Authorization Now? Choose Nasance Authorization Rules Resdy to Add Trust Presh	Add Relying Party Trust Wizard Seadly an optional token encryption certificate. The token encryption certificate is used to encrypt the dama that are sent to 1. To specify the certificate. click Browse. Issue: Browse: Browse: Periove date: Cancel Cancel	ctions Lelying Party Trusts Add Reying Party Trust. Add Non-Claims-Aware Relying View New Window from Here Refresh Help
Action: In progress	, .		

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

%		AD FS	_ 🗆 X
翰 File Action View Window He	lp		_ 8 ×
🗢 🔿 🙍 📰 🚺 🖬	\$	Add Relying Party Trust Wizard	
AD FS	Configure Identifiers		ctions
Endpoints Certificates Clim Descriptions Trust Relationships Clims Provider Trusts Attribute Stores Per Relying Party Trusts Per Relying Party Trusts Per Relying Party Trust	Steps Velcome Sect Data Source Sect Data Source Cross Patie Conce Patie Configure Vente Configure Vente Configure Vente Configure Vente Configure Multifactor Authorization Nov? Crosse Susance Authorization Rules Ready to Add Trust Finish	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust. Relying party trust identifier: Cample: https://fs.contoso.com/adfs/services./trust. Relying party trust identifier: Interst //soccurationing party in the identifier in the identifier in the identifier in the identifier. Interst //soccurationing party in the identifier: Interst //soccurationing party in the identifier in the iden	Retying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying View New Window from Here Refresh Help
Action: In progress			

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.

Na AD FS	x
💱 File Action View Window Help	. 8 ×
💠 🔿 📶 🛐 🛐 Add Relying Party Trust Wizard	
AD 55 Service Configure multi-factor authentication entings for this relying party trutt. Multi-factor authentication is majured for this relying for this party for the special for any of the special for the relying party trut. Add Blore-Claims Aware Relying View In Add Field for Authentication Special for any of the special for t	ng

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

-		AD FS	_ 🗆 X
翰 File Action View Window H	ielp		_ # ×
(= =) 🖄 📰 🚺 🖬	%	Add Relying Party Trust Wizard	
AD FS	Choose Issuance Auth	norization Rules	ctions
Endpoints	0		Relying Party Trusts
Certificates	Steps	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.	Add Relying Party Trust
Claim Descriptions	Select Data Source		Add Non-Claims-Aware Relying
Claims Provider Trusts	Specify Display Name	Permit all users to access this reying party The issuance at thorization place will be configured to permit all users to access this reking party. The reking	View 🕨
Relying Party Trusts	Choose Profile	party service or application may still deny the user access.	New Window from Here
Attribute Stores	Configure Certificate	O Deny all users access to this relying party	Refresh
Per Relying Party Trust	Configure URL	The issuance authorization rules will be configured to deny all users access to this relying party. You must	2 Help
	Configure Identifiers	later add issuance authorization rules to enable any users to access this relying party.	
	Configure Multi-factor Authentication Now?	You can change the issuance authorization rules for this relying party trust by selecting the relying party trust	
	Choose Issuance Authorization Rules	and clicking Edit Claim Rules in the Actions pane.	
	Ready to Add Trust		
	e Frish	< Previous Next > Cancel	
Action: In progress			

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:		
\$	AD FS	_ 🗆 X
翰 File Action View Window Help		_ 6 ×
🗢 🔿 🙍 🖬 📓 🖬	🎨 🛛 Edit Claim Rules for VaccinatieRegister Login	
AD FS	Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules	Actions
△ Service	The following transform place energies the claime that will be east to the relation party	Relying Party Trusts
Certificates	s.vitual.net	Add Relying Party Trust
Claim Descriptions	Order Rule Name Issued Claims gister.nl/saml	Add Non-Claims-Aware Relying
Irust Relationships Claims Provider Trusts		View •
Relying Party Trusts		New Window from Here
Attribute Stores		Refresh
Per Relying Party Trust		🛛 Help
		VaccinatieRegister Login
		Update from Federation Metada
	•	Edit Claim Rules
		Disable
		Properties
		🗙 Delete
		P Help
	Add Rule Edt Rule Remove Rule	
	OK Cancel Apply	
Action: In progress		

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

Maak vervolgens een regel aan "Send LDAP Attributes as Claims"

%		AD FS	_ 🗆 X
📬 File Action View W	1	Add Transform Claim Rule Wizard	_ 8 ×
🗢 🔿 🖄 📰 📓 🗊	12		
AD FS	Select Rule Template		Actions
⊿ Service ☐ Endpoints	Steps	Select the template for the claim rule that you want to create from the following list. The description provides	Relying Party Trusts
Certificates	Choose Rule Type	details about each claim rule template.	Add Relying Party Trust
Claim Descriptions	Configure Claim Rule	Claim rule template:	Add Non-Claims-Aware Relying
I rust Relationships Claims Provider Tru		Send LDAP Attributes as Claims	View •
📑 Relying Party Trust		Claim rule template description:	New Window from Here
Attribute Stores		Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute	G Refresh
Per Relying Party T		subjections source blockowy to send as claims to the relying party, maliple autoutes may be send as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a single truling structure table to use for a theories of the send table to be table	Help
		A due that will extract atmost evalues for authenticated users from the displaying claims. This rule may also he was a strain of the user of the service of	VaccinatieRegister Login
		memberships, use the Send Group Membership as a Claim rule template.	Update from Federation Metada
			Edit Claim Rules
			Disable
			Properties
			🗙 Delete
			P Help
		< Previous Next > Cancel	
I			
Action: In progress][

- 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

%	AD FS	_ D X
Sile Action View W	Add Transform Claim Rule Wizard	_ 6 ×
AD FS Service		Actions
Seps Cathfactes Cathfactes Cathfactes Cath Descriptions Cath Descriptions Cathour Sproider Tra Relying Party Trutt Attribute Stores Per Relying Party Trutt	You can configure this rule to send the values of LDAP attributes so claims. Select an attribute store from which its entral LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be autorities will be attribute to the outgoing claim types that will be attribute store. Claim Le name:	Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying View New Window from Here Image: Refresh Help VaccinatieRegister Login Update from Federation Metada Edd Claim Rules Disable Properties Delete Help
Action: In progress		

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:

%	AD FS	_ 🗆 X
🙀 File Action View Window Help		_ 8 ×
💠 🔿 📶 🖬 🖬		
 File Action View Window Help File Action View Window Help AD FS AD FS Endpoints Chim Descriptions Claim Descriptions Claim Service Trusts Relying Party Trusts Attribute Stores Per Relying Party Trust 	AD FS	Actions Relying Party Trusts Add Relying Party Trust. Add Relying Party Trust. Add Non-Claims-Aware Relying View New Window from Here Refresh Heip VaccinatieRegister Login Update from Federation Metada Edit Claim Rules Disable Properties Delete Heip
		1

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 adfsserver 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"

VACCINATIEREGISTE	R Afspraken Cliënten Projecten Financieel Beheer Instellingen Beheer Beheerder Uitloggen 4	
Instellingen		
Organisatie	Algemeen Instellingen Templates Certificaten	
Product categorieën	Werktijden & consultduur	9
Producten	Werktijden 8:00 O tot 20:00 O	
Recept soorten	Tijdsduur reisconsult 25 minutr \$	
Recepten	Tijdsduur 10 minut 🗘	
Dossier categorieën	Tijdsduur 20 minuti \$	
Dossier onderwerpen	Tijdsduur telefonisch consult	
Preventie onderwerpen	Extra tijd p.p. 10 minutr 🗘	
Vaccinatietrajecten	Extra tijd lange reis 30 minute 🗘 Vanaf 3 bestemmingen	
Sjablonen	of 91 dagen	
	Nummering	
	Eerste factuurnummer* 1	
	Eerste clientnummer* 162000	
Versie: 27.1.75 Test	Online afspraken	

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

SAML (in ontwikkeling)		
Gebruik SAML		
SAML SSO URL		
	Dit is de SAML Identy Provider URL waarheen het VaccinatieRegister gebruikers stuurt bij het aanmelden. Uw Relying Party Identifier is https://ggdgdemo.vaccinatieregister.nl/saml	
IP adressen		
	Logins van deze IP adressen worden altijd gestuurd naar de SAML Identity Provider. Adressen die niet voorkomen in deze lijst worden gestuurd naar de normale login pagina. Laat dit veld leeg om alle logins naar de Identity Provider te sturen. Het format is n.n.n.n . Scheidt adressen met een spatie. Uw huidig IP adres is: 89.200.39.221.	
Certificate fingerprint		
	DE SHA1 fingerprint van het SAML certificaat. Vraag dit op bij uw SAML Identity Provider.	

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>