Single-sign-on met SAML 2.0 (Active Directory)

Inleiding

Het is vaak gewenst dat gebruikers niet op het portal nog een keer een wachtwoord in hoeven te vullen. Om te zorgen dat gebruikers gelijk ingelogd zijn kunt u gebruik maken van SAML 2.0. Dit wordt ondersteund door bijvoorbeeld ADFS en SimpleSAML. Het voordeel van deze methode is het gemak voor gebruikers en het feit dat het wachtwoord van de gebruiker niet in een extern systeem ingevuld hoeft te worden.

Op deze pagina

Zie ook

- Inloggen met LDAP (Active Directory)
- Veel gestelde vragen

Overzicht

Bij het gebruik van single-sign-on (SSO) via SAML 2.0 is er een externe server (van uw school) die de identiteit van de gebruiker vaststelt en daar voor instaat.

We gebruiken de volgende terminologie:

Term	Betekenis
SAML	Security Assertion Markup Language, een specificatie van berichten die servers naar elkaar kunnen sturen om de identiteit en rechten van een persoon vast te stellen.
Single-sign-on (SSO)	De gebruiker logt één keer in, op een server/systeem van de school, en hoeft daarna verder nergens meer een wachtwoord in te vullen.
Identity provider (IdP)	Het systeem wat de identiteit van de gebruiker vaststelt en aan andere systemen kan garanderen dat de gebruiker zegt wie hij is. Dat is bijvoorbeeld de ADFS server van de school.
Service provider (SP)	Het systeem wat de dienst aanbied waar de gebruiker gebruik van moet kunnen maken. Dat is bijvoorbeeld het portal.

Er zijn meerder methodes om gebruik te maken van single-sign-on met SAML:

Methode	Werking	Ondersteund door het portal	Benodigde instellingen
Identity provider initiated single-sign-on	1. De gebruiker gaat naar de identity provider en klikt daar op een knop om naar het portal te gaan. 2. De identity provider stuurt een SAML verzoek tot inloggen naar de service provider. 3. De gebruiker is ingelogd.	JA	• saml2.enabled • saml2.issuer_id • saml2.certificate
Redirect + Identity provider initiated single-sign-on	1. De gebruiker gaat naar de service provider (het portal) 2. De gebruiker wordt automatisch doorgestuurd naar de identity provider door middel van een HTTP GET. Dit kan ook via een link op de login pagina van het portal. 3. Aan de hand van de redirect bepaalt de service provider waar de gebruiker wil inloggen 4. De identity provider stuurt dit verzoek als SAML naar de service provider (het portal). 5. De gebruiker is ingelogd.	JA	• saml2.enabled • saml2.identity_provider_url • saml2.issuer_id • saml2.certificate Optioneel: • saml2.force_redirect
Service provider initiated single-sign-on (SP initiated SSO)	1. De gebruiker gaat naar de service provider (bijvoorbeeld het portal) 2. De service provider stuurt een SAML verzoek naar de identity provider om de identiteit vast te stellen. 3. De identity provider stuurt een SAML verzoek terug naar de service provider. 4. De gebruiker is ingelogd.	NEE	Niet ondersteund

Instellingen

Om gebruik te maken van single-sign-on door middel van SAML 2.0 gaat u naar de pagina **Beheer > Admin-paneel > Instellingen**. Hier vult u de volgende gegevens in:

Instelling	Voorbeeld	Toelichting
saml2.enabled	true	true als SAML2.0 authenticatie is ingeschakeld, false in andere gevallen. Als dit op true staat wordt er een tekst en een login link weergegeven op de loginpagina van het portal.
saml2.force_redirect	false	true als ALLE gebruikers direct naar de SAML login URL moeten worden geredirect bij het openen van schoolnaam.zportal.nl. Als u deze waarde op true heeft staan maar u wilt toch met een wachtwoord inloggen dan kunt u https://schoolnaam.zportal.nl?sso=false gebruiken.
saml2.identity_provider_url	https://adfs.example.com/adfs/ls/idpinitiatedsignon.aspx?SAMLRequest=&RelayState=https://schoolnaam.zportal.nl&RedirectTo=https://schoolnaam.zportal.nl/api/v3/oauth/saml	De URL waar de browser heen geredirect wordt voor de authenticatie. Let op dat dit afhankelijk van uw situatie behoorlijk kan verschillen van het voorbeeld.
saml2.issuer_id	http://adfs.example.com/adfs/services/trust	De naam van de server waar we response van krijgen. Staat bovenin de de FederationMetadata.xml. Let op: hoofdlettergevoelig!
saml2.certificate	EboteSTfsrBV... yT+z2yL8jscw==	Het x509 certificaat waarmee de SAML server zijn identiteit kan aantonen. Dit is een Base64 gecodeerde string, die zeer waarschijnlijk eindigt op =. In het FederationMetadata.xml bestand staat het certificaat tussen de <x509Certificate> en </x509Certificate> tags.

Als uw server een configuratie XML URL aanbiedt dan kunt u deze in de browser openen om de benodigde instellingen (waaronder het certificaat) te vinden. Dit bestand is in het geval van ADFS vaak te vinden op https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml

Extra help voor samenstellen saml2.identity_provider_url

De volgende artikelen kunnen hulp bieden bij het goed samenstellen van de saml2.identity_provider_url. Sommige scholen hebben ADFS in proxy modus staan en moeten dan met de optie LoginToRP aan de slag:

- https://techontip.wordpress.com/2013/01/11/logintorp-auto-select-relaying-party/
- https://blogs.technet.microsoft.com/askds/2012/09/27/ad-fs-2-0-relaystate/

De toevoeging wordt dan *&LoginToRP=https://{portalnaam}.zportal.nl*

U verder dient het volgende op uw eigen server in te stellen:

Instelling	Voorbeeld	Toelichting
AD FS profile	aan	U dient voor de algemene optie te kiezen, niet voor ADFS 1.0 and 1.1 profile
Enable support for the SAML 2.0 WebSSO protocol	aan	
Relying party SAML 2.0 SSO service URL	https://schoolnaam.zportal.nl/api/v3/oauth/saml	De URL waarnaartoe de gebruiker wordt terugverwezen als deze succesvol is ingelogd.
Relying party trust identifier	schoolnaam.zportal.nl	Dit is de naam waar het portal zich mee identificeert

Als laatste zet u voor alle gebruikers die via SAML moeten kunnen inloggen een vinkje bij "externe authenticatie".

Herkenning van gebruikers

Gebruikers worden herkend op basis van:

1. code
2. extra gebruikersnaam
3. mailadres

Als uw SAML identity provider als gebruikersnaam (Name ID) een van deze velden meegeeft wordt de gebruiker vanzelf ingelogd. Het portal ondersteunt het ook als het mailadres in de attribute "mail" of "email" wordt meegegeven.

U kunt zowel LDAP als SAML ingeschakeld hebben in de instellingen. In dat geval kan zowel direct via SAML worden ingelogd, maar als de gebruiker toch een wachtwoord invult wordt deze gecontroleerd via LDAP. Op deze manier kunt u soepel overstappen van de ene naar de andere methode. Wel is het in dat geval handig om de saml2.force_redirect optie nog niet in te schakelen.

Gebruik

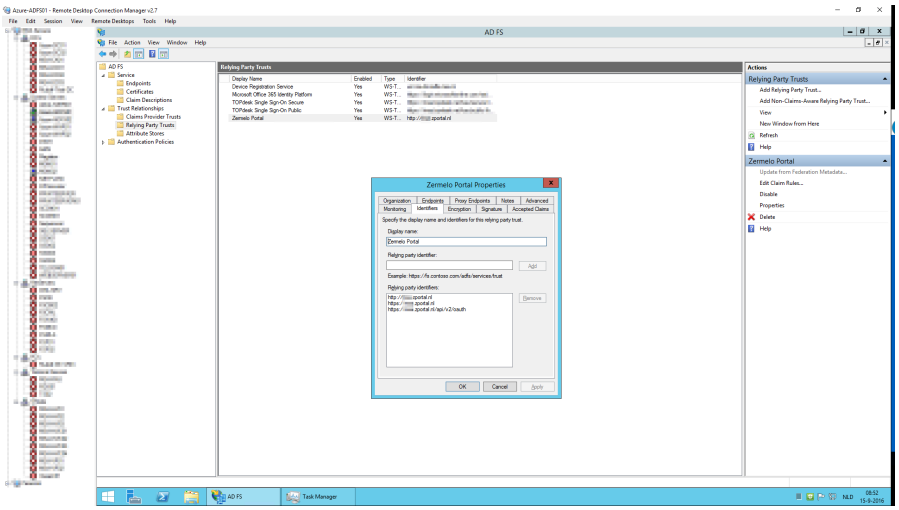
Het inloggen werkt als volgt. De gebruikers gaan naar schoolnaam.zportal.nl. Hierna wordt (als saml2.enabled en saml2.force_redirect true is) de gebruiker geredirect naar saml2.url. Dat is het adres van uw SAML server. Als force_redirect niet aanstaat dan kan de gebruiker klikken op de link *Login met single-sign-on*.

Alleen gebruikers waarbij "Externe authenticatie" (intern "ldap") aan staat kunnen inloggen via SAML of LDAP. Andere gebruikers loggen nog steeds in met hun wachtwoord.

> **Tip**
>
> Als inloggen niet meteen werkt, dan kunt u bij Beheer > Admin-paneel > Logs misschien een melding vinden die u verder helpt.

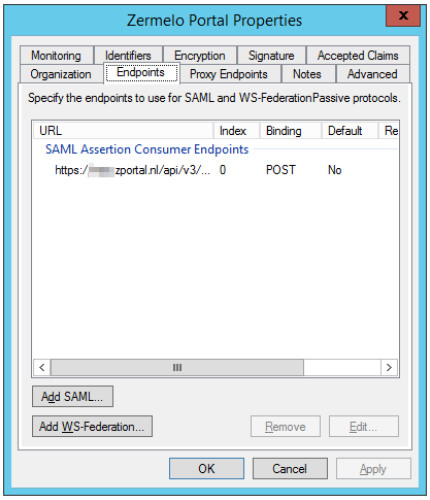
Handleiding AD

Maak een nieuwe Relying Party Trust met de volgende eigenschappen. Op de tabbladen die hier niet bij staan wordt niets ingevuld.

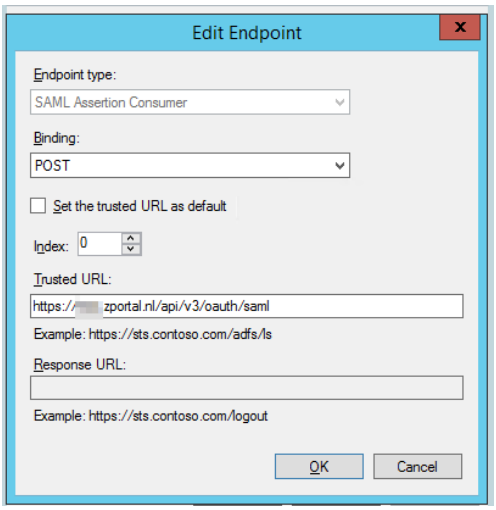


Deze zijn waarschijnlijk niet alle drie nodig.

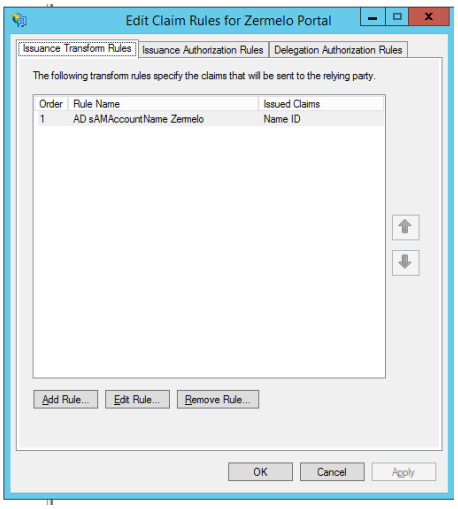
Nu gaan we naar het tabblad endpoints:



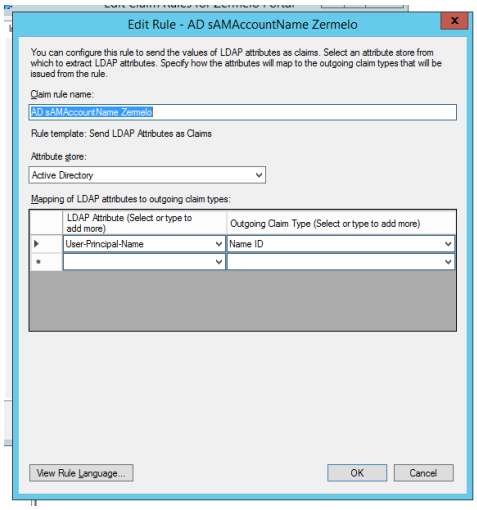
We selecteren het endpoint en klikken op Edit...



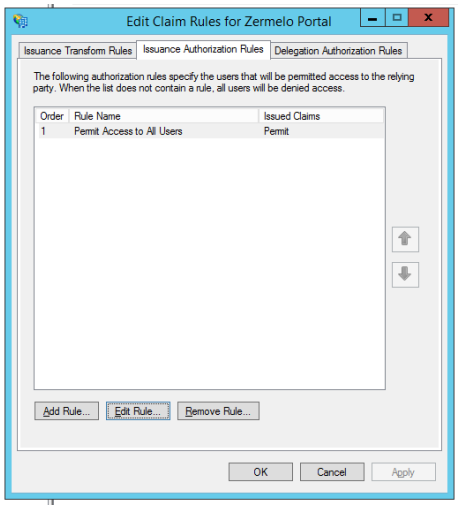
We sluiten dit scherm en bewerken dan de Claim Rules:



Als je nummer 1 edit:



En als laatste binnen ADFS:



En de settings binnen het Admin-paneel: