Handleiding Youforce Single Sign On

13-12-2023

VISMA | raet

Inhoudsopgave

Inleiding

Introductie

In deze handleiding vindt u de stappen die u moet doorlopen om de koppeling tussen Youforce en uw organisatie te realiseren. Deze koppeling faciliteert het gebruik van Single Sign-on (SSO) op basis van Security Assertion Markup Language (SAML) of OpenID Connect. Hierbij treedt uw eigen organisatie op als Identity Provider en Youforce als Service Provider.

Met andere woorden: u levert de identiteit van de gebruiker en Youforce levert de service.

Na het realiseren van deze Single Sign-on koppeling melden medewerkers zich alleen nog maar aan bij het netwerk van uw organisatie. De geautoriseerde medewerkers kunnen daarna gebruik maken van Youforce zonder zich nogmaals aan te melden met de Youforce gebruikersidentificatie en wachtwoord.

Doelgroep

Dit document is bestemd voor (systeem)beheerders die expertise hebben op het gebied van installeren en beheren van SAML / OpenID Connect / Single-Sign-on-koppelingen. Aanvullend is kennis nodig van Youforce gebruikersbeheer.

Opmerking: Het opzetten en configureren van een SAML of OpenID Connect verbinding is gespecialiseerd werk, waarop Visma|Raet geen support levert. U kunt hiervoor terecht bij uw ICT afdeling of een gespecialiseerd bedrijf in Active Directory en Active Directory Federation Services (ADFS) / Azure.

Randvoorwaarden

Als u gebruik wilt maken van een Single Sign-on koppeling moet uw organisatie beschikken over een eigen Identity Provider of Identity Service. Meestal wordt gebruik gemaakt van een ADFS Service of Azure in combinatie met Active Directory. Visma|Raet ondersteunt ook andere services, zolang SAML 2.0 of OpenID connect als standaard wordt gebruikt.

Configureren ADFS SAML koppeling

Uitwisselen gegevens (Systeembeheerder/Visma|Raet)

Om de SAML koppeling tot stand te brengen, hebben we van uw organisatie een aantal gegevens nodig:

Federation Metadata bestand
Dit is een link naar de federation metadata. U kunt ook het bestand via een request/mail naar ons toesturen.

Identificatie van de Identityprovider
Dit is meestal de waarde van een domein (bijvoorbeeld: organisatie.com).

Identificatie van het identity veld
Dit is de waarde waarin de identity van de gebruiker wordt geretourneerd. Standaard adviseren wij hiervoor de volgende waarde:

Voor ADFS: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn

Het logout adres (single logout)
Het advies is geen logout adres te configureren. Bij het uitloggen uit Youforce logt u ook uit bij de Identity provider. Als het wel wenselijk is deze configureren, kunt u deze ook aanleveren.

Inrichten connectie

Onze support medewerker gaat na of u alle gegevens geleverd heeft en zet de aanvraag intern door naar de consultant die de inrichtingswerkzaamheden tegen betaling uitvoert. Na de intake met de functioneel beheerder en ICT medewerker ontvangt u een inschatting van de benodigde uren. Na de inrichting ontvangt u van ons de Youforce-metadata url om de SAML configuratie in uw eigen omgeving in te richten.

Belangrijk: Naast het Identity veld is voor een succesvolle SAML koppeling ook de NameID nodig. Hoewel wij dit gegeven niet gebruiken, is het een vereiste dat de NameID in het SAML Subject wordt doorgegeven. ADFS geeft dit niet standaard door en het moet dan ook handmatig toegevoegd worden aan de SAML assertion.

Configureren Azure SAML koppeling

Inrichten connectie

Om de SAML koppeling tot stand te brengen, kan met de volgende gegevens een SAML applicatie in Azure aangemaakt worden:

EntityID:
https://raet-ib-prod.raet.com

Reply url:
https://identity.raet.com/sp/ACS.saml2

Sign on url:
https://mijn.youforce.com of https://mijn.youforce.com/sso/*klantnaam*/

Ons advies is om geen klant specifieke url aan te maken zie:
https://community.visma.com/t5/Kennisbank-Youforce-Portaal/Het-nieuwe-inloggen-Veel-gestelde-vragen-voor-beheerders/ta-p/471423#toc-hId-2091974859

Uitwisselen gegevens (Systeembeheerder/Visma|Raet)

Nadat de configuratie in Azure gedaan is ontvangen wij graag de volgende gegevens:

Federation Metadata bestand
Dit is een link naar de federation metadata xml.

Identificatie van de Identity Provider
Dit is meestal de waarde van een domein (bijvoorbeeld: organisatie.com)

Identificatie van het identity veld
Dit is de waarde waarin de identity van de gebruiker wordt geretourneerd. Standaard adviseren wij hiervoor de volgende waarde voor Azure: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Het logout adres (single logout)
Het advies is geen logout adres te configureren. Bij het uitloggen uit Youforce logt u ook uit bij de Identity provider. Als het wel wenselijk is deze configureren, kunt u deze ook aanleveren.

Onze support medewerker gaat na of u alle gegevens geleverd heeft en zet de aanvraag intern door naar de consultant die de inrichtingswerkzaamheden tegen betaling uitvoert. Na de intake met de functioneel beheerder en ICT medewerker ontvangt u een inschatting van de benodigde uren.

Belangrijk: Naast het Identity veld is voor een succesvolle SAML koppeling ook de NameID nodig. Hoewel wij dit gegeven niet gebruiken, is het een vereiste dat de NameID in het SAML Subject wordt doorgegeven. Azure geeft dit standaard door.

Configureren OpenID Connect koppeling

Inrichten connectie

Om een OpenID koppeling tot stand te brengen moet eerst een OpenID applicatie aangemaakt worden en ontvangen wij daarna de volgende gegevens:

Issuer URL:
Dit is een link naar de metagegevens document dat de meeste informatie bevat die vereist is voor een app om zich aan te melden. Dit omvat informatie zoals de URL's die moeten worden gebruikt en de locatie van de openbare ondertekeningssleutels van de service.

ClientID:
De toepassings-id (client) die is toegewezen aan uw app.

Client Secret:
De secret die is toegewezen aan uw app.

Identificatie van de het identity veld
Dit is de waarde waarin de identity van de gebruiker wordt geretourneerd. Voor OpenID Connect is dit vaak:

- upn
- preferred_username (Azure)

Identificatie van de Identityprovider
Dit is meestal de waarde van een domein (bijvoorbeeld: organisatie.com).

Uitwisselen gegevens (Systeembeheerder/Visma|Raet)

Onze support medewerker gaat na of u alle gegevens geleverd heeft en zet de aanvraag intern door naar de consultant die de inrichtingswerkzaamheden tegen betaling uitvoert. Na de intake met de functioneel beheerder en ICT medewerker ontvangt u een inschatting van de benodigde uren. Na inrichting ontvangt u van ons een Redirect-URI om de OpenID Connect configuratie in uw eigen omgeving in te richten.

Gebruikers identiteiten in Youforce (Youforce beheerder)

Identiteit individueel beheren

U kunt de identity via Individueel gebruikersbeheer toevoegen of aanpassen. Ga naar Beheer | Portaal Beheer | Individueel Gebruikersbeheer en pas voor de betreffende gebruiker de waarde van het Identity veld aan.

Identiteiten groepsgewijs beheren

De interne netwerknamen van de gebruikers (identiteiten) van uw organisatie moeten binnen Youforce gekoppeld worden aan een Youforce gebruiker. Hoe dit in zijn werk gaat, leest u hieronder.

1. Ga naar Beheer | Portaalbeheer | Single Sign On |Groepsgewijs Netwerknamen Opvoeren.
2. Klik op Voltooien en download het txt-bestand in een lokale directory naar keuze.
3. Het gedownloade bestand bevat de kolom Identity. Voor elke gebruiker vult u hier een waarde in. De waarde van het veld Identity is vrij te kiezen maar moet wel uniek zijn binnen uw organisatie.
4. Maak een kopie van het bewerkte bestand en stel deze veilig in een andere map. Als deze blijft staan in dezelfde map wordt deze ook verstuurd.
5. Ga naar Zenden en Ontvangen | Zenden en kies voor Gebruikersbeheer.
6. Geef de locatie in van het te zenden bestand en klik op Zenden. Als er dubbele Identities in het bestand aanwezig zijn, breekt de import af vanaf het punt dat er een dubbele waarde is gevonden. Wij adviseren u daarom om het bestand vooraf te controleren, te corrigeren en - indien nodig - opnieuw in te zenden.
7. Ga naar Beheer | Portaal Beheer | Rapportages via Logboek Groepsgewijs Gebruikersbeheer.
8. Controleer hier of de import succesvol is verlopen.

Opmerkingen

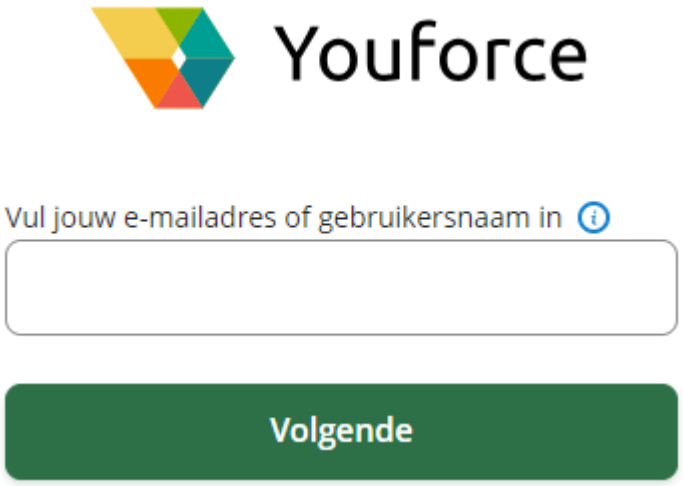
- Een nieuwe import moet altijd volledig zijn omdat het alle bestaande identities overschrijft. Download dus altijd de laatste versie van het bestand en werk deze bij. Vervolgens kunt u het totale bestand weer uploaden.
- Een identity moet uniek zijn binnen de organisatie. Als er twee of meer gebruikers zijn met dezelfde identity, worden deze gebruikers niet bijgewerkt en het importproces stopt. Dit wordt gemeld in het logboek: Portaalbeheer | Rapportages | Logboek Groepsgewijs Gebruikersbeheer.

  Indien gewenst kunt u het importbestand corrigeren voor een nieuwe volledige import/upload.
- U blijft zelf verantwoordelijk voor het koppelen van de juiste identiteit aan de juiste gebruiker. Wees hierbij zorgvuldig om te voorkomen dat medewerkers binnen uw organisatie elkaars gegevens zien.

Testen van de koppeling

Algemeen

Uw medewerkers kunnen inloggen via: https://mijn.youforce.com



Hier vult de gebruiker zijn gebruikersnaam en domein in (bijvoorbeeld gebruiker@organisatie.com).

Als de gebruiker al is geauthenticeerd binnen uw organisatie, ziet hij direct het bureaublad van Youforce. Zo niet, dan wordt hij doorverwezen naar de inlogpagina van uw eigen Identity Provider.