



SAML KOPPELING TUSSEN AZUREAD EN SURFCONEXT

SAML CLAIM MAPPING

14-JUN-2019

© 2017 InSpark, all rights reserved.

Alle rechten voorbehouden. U ontvangt dit document onder de uitdrukkelijke voorwaarde dat u dit document vertrouwelijk zal behandelen en dat, indien u niet wenst in te gaan op dit document, van de inhoud geen gebruik zal maken zonder voorafgaande schriftelijke toestemming van InSpark. Tevens is het niet toegestaan dit document op enigerlei wijze aan derden ter beschikking te stellen zonder voorafgaande schriftelijke toestemming van InSpark. InSpark behoudt zich alle rechten voor ter zake auteursrecht rustende op dit document. Alle genoemde handelsmerken in dit document zijn eigendom van de rechthebbenden.

Dit document is gebaseerd op informatie die is verstrekt door u en InSpark kan niet garanderen dat deze informatie correct en/of compleet is. Omdat InSpark de veranderingen in techniek en de wijzigingen in de computer- en netwerkomgevingen van klanten volgt, dient dit document niet te worden opgevat als een verbintenis of toezegging van InSpark. Prijswijzigingen onder voorbehoud.

Inhoudsopgave

1. Inleiding	1
2. AzureAD SAML Claims	2
2.1. SAML claim	2
2.2. Type Claim mapping	3
2.2.1. Vaste Single-value mapping	3
2.2.2. User Attribute Single-value mapping	4
2.2.3. Transformatie Single-value mapping	5
2.2.4. Mutli-value mapping	6
3. BuildGuide	8
3.1. Aanmaken SAML koppeling met SurfConext	8
3.2. Aanmaken van AssignedRoles	13
3.3. Aanmaken voor Groups - AssignedRoles	17
4. Validatie SAML Claims	19
5. Referenties	20

1. INLEIDING

Dit document is een technische handleiding om een SAML koppeling op te zetten tussen Azure Active Directory en SurfConext. Deze handleiding is geschreven voor technische personen die ervaring hebben met het implementeren van Identity Providers, User Provisioning en Federatieve systemen en koppelingen.

Note:

AzureAD gebruikers moeten minimaal een AzureAD Premium P1 of hoger licentie hebben om gebruik te maken van [federatieve SAML applicaties](#).

2. AZUREAD SAML CLAIMS

Dit hoofdstuk beschrijft kort de verschillende type SAML claims van AzureAD

2.1. SAML CLAIM

Een SAML koppeling gebruikt claims om kenmerken van een gebruiker naar een resource provider te sturen. Een SAML claim is een hash value. Een hash value bestaat uit een key/value pair.

Voorbeeld van een single-value SAML claim

Email = "jan.janssen@surfconext.nl"

displayName = "Jan Janssen"

Voorbeeld van multi-value SAML claim

urn:mace:dir:attribute-def:eduPersonEntitlement =

- **urn:mace:terena.org:tcs:personal-user**
- **urn:mace:terena.org:tcs:escience-user**
- **urn:mace:dir:entitlement:common-lib-terms**
- **urn:x-surfnet:surfxxxxxx.nl:surfdrive:quota:100**

Een multi-value SAML claim ziet er in SAML format als volgt uit:

```
<saml:Attribute Name="urn:mace:dir:attribute-def:eduPersonEntitlement"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">urn:mace:terena.org:tcs:personal-user</saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string">urn:mace:terena.org:tcs:escience-user</saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string">urn:mace:dir:entitlement:common-lib-terms</saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string">urn:x-surfnet:surfxxxxxx.nl:surfdrive:quota:100</saml:AttributeValue>
</saml:Attribute>
```

2.2. TYPE CLAIM MAPPING

AzureAD SAML koppeling biedt de volgende methoden voor het mappen van user attributes & claims.

2.2.1. VASTE SINGLE-VALUE MAPPING

Deze type mapping wijst één vaste waarde toe aan een SAML claim. Alle gebruikers krijgen dezelfde vaste waarde in de claim.

SAML Claim mapping	
Source	SAML koppeling
Type	Single-value
SAML claim name	Fixed claim name
SAML claim value	Fixed value
Claim value mapping	Claim value = “fixed value”

Voorbeelden

De SurfConext claim voor preferredLanguage heeft voor alle gebruikers dezelfde waarde “NL”

urn:mace:dir:attribute-def:preferredLanguage = “NL”

De SurfConext claim voor schacHomeOrganization heeft voor alle gebruikers dezelfde waarde “SurfConext.nl”

urn:mace:terena.org:attribute-def:schacHomeOrganization = “SurfConext.nl”

2.2.2. USER ATTRIBUTE SINGLE-VALUE MAPPING

Deze type mapping wijst één waarde toe aan één SAML claim. De claim waarde is gelijk aan het user account attribute.

SAML Claim mapping	
Source	Azure Active Directory - User Account Active Directory - User Account*
Type	Single-value
SAML claim name	Fixed claim name
SAML claim value	AAD User account attribute
Claim value mapping	Claim value = user.displayname

*) AADConnect synchroniseert Active Directory user accounts naar Azure Active Directory.

Voorbeeld

De SurfConext claim voor displayname is gelijk aan het AzureAD user attribute “Displayname”, maw elke gebruiker krijgt zijn eigen naam te zien als displayname.

urn:mace:dir:attribute-def:displayName = user.displayname

2.2.3. TRANSFORMATIE SINGLE-VALUE MAPPING

Deze type mapping wijst één dynamische waarde toe aan één SAML claim. De dynamische waarde is een bewerking van vaste waarde of van een of meerdere user attributen. De bewerking van de waarde is afhankelijk van de gekozen transformatie type.

SAML Claim mapping	
Source	Azure Active Directory - User Account Active Directory - User Account*
Type	Single-value
SAML claim name	Fixed claim name
SAML claim value	Dynamic value (transformation rule)
Claim value mapping	Claim value = <transformation rule>
Input transformation	Fixed values, user attributes

Voorbeeld

De SurfConext claim voor eduPersonPrincipalName wordt samengesteld van de Active Directory user attribute samaccountname en de domain suffix “@surfconext.nl”

**urn:mace:dir:attribute-def:eduPersonPrincipalName = Join
 (“user.onpremisesamaccountname”, ””, ”@surfcontext.nl”)**

2.2.4. MUTLI-VALUE MAPPING

Deze type mapping wijst één or meerdere waarden toe aan één SAML claim. Hiervoor wordt gebruik gemaakt van de user attribute assignedroles. De mapping wordt in twee logische stappen samengesteld. De eerste stap wordt de claim value ingesteld op het user attribute: user.assignedroles. In de tweede stap worden de assignedroles gekoppeld aan één of meerdere AD/AAD groepen.

De werking van deze mapping is te vergelijken met een checkbox-lijst van vaste waarden. De assignedroles zijn de vaste waarden die gekozen kunnen worden in de checkbox-lijst. De groep lidmaatschap bepaald of een check-box aan of uit gezet wordt voor één van de assignedroles.

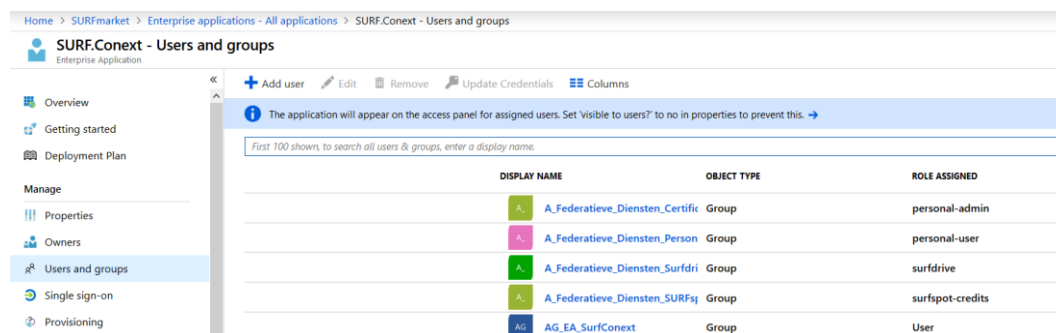
1: SAML Claim mapping

SAML Claim mapping	
Source	Azure Active Directory - User Account Active Directory - User Account*
Type	Multi-value
SAML claim name	Fixed claim name
SAML claim value	Fixed values (selected)
1: Mapping: Claim value mapping	Claim value = user.assignedroles
2: Mapping: assignedroles- groups	Group membership add one or more assignedroles Each assigned role adds a fixed value to the Claim

Note: Er kan maar 1 multi-value SAML claim per SAML koppeling worden aangemaakt.

2: Mapping AssignedRoles-Groups

In de configuratie “Users and groups” van een Enterprise applicatie kunnen een of meerdere groepen worden gekoppeld aan een assigned role. Zie voorbeeld hieronder.



DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
A_Federatieve_Diensten_Certific	Group	personal-admin
A_Federatieve_Diensten_Person	Group	personal-user
A_Federatieve_Diensten_Surfdri	Group	surfdri
A_Federatieve_Diensten_SURFsj	Group	surfsport-credits
AG_EA_SurfConext	Group	User

Standaard heeft een Enterprise applicatie één role: user. Normaal wordt deze role gebruikt als accesscontrol om gebruikers/groepen toegang te verlenen tot de Enterprise applicatie. Deze mapping zorgt dus voor de toegang tot de applicatie en voor toevoegen van meerdere waarden op multi-value Claim.

De assignedroles van een Enterprise Applicatie kunnen worden uitgebreid door de AzureAD te patchen. Elke toegevoegde assignedroles krijgt een fixed value. (zie paragraaf 3.3)

Voorbeeld

1: Claim mapping

urn:mace:dir:attribute-def:eduPersonEntitlement = user.assignedroles

De waarde van eduPersonEntitlement = user.assignedroles

2: Group - Assignedroles

Gebruiker is lid van 2 van de 4 groepen: A_Federatieve_Diensten_Surfspot_Credits en A_Federatieve_Diensten_Surfdrive

Deze twee groepen mappen respectievelijk de assignedroles: surfspot-credits en surfdrive

3: De fixed values van de assignedroles zijn als volgt:

Assignedrole	Value
Surfspot-credits	urn:x-surfnet:surfxxxxxx.nl:surfspot:Credits:7500
Surfdrive	urn:x-surfnet:surfxxxxxx.nl:surfdrive:quota:100

Resultaat: eduPersonEntitlement bevat twee waarden

urn:x-surfnet:surfxxxxxx.nl:surfspot:Credits:7500

urn:x-surfnet:surfxxxxxx.nl:surfdrive:quota:100

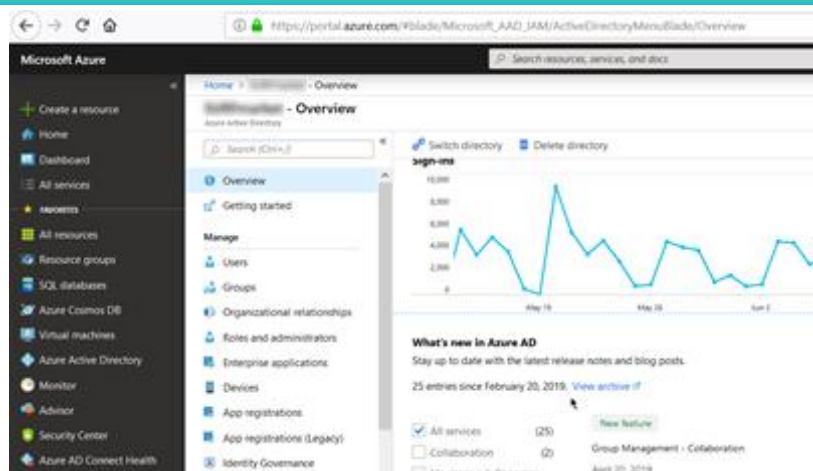
3. BUILDGUIDE

Instructie voor het maken van AzureAD SAML koppeling met SurfConext. Voor het maken van SAML configuratie heb je global admin rechten nodig in je AzureAD/Office365 tenant.

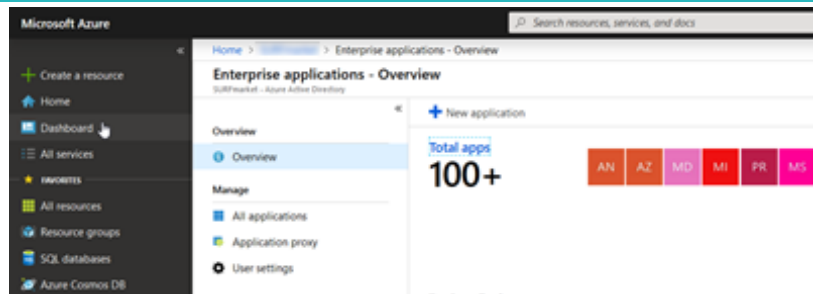
3.1. AANMAKEN SAML KOPPELING MET SURFCONEXT

Deze paragraaf beschrijft het maken van een SAML koppeling met SurfConext

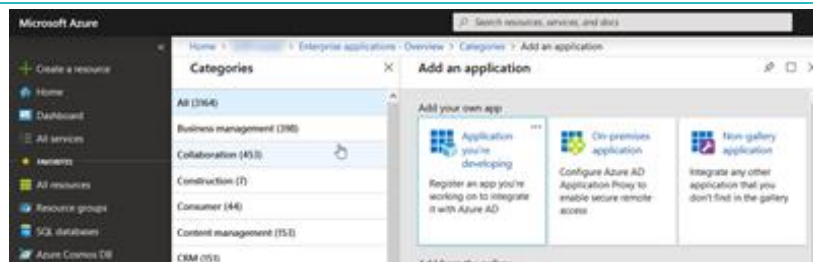
Login in op de Azure Portal en open de Azure Active Directory, Enterprise Applications



Druk op + New Application



Selecteer de tegel met Non-gallery application



Geef de Enterprise Application een naam: SURF.Conext en druk op Add

Add your own application

* Name

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports:
SAML-based single sign-on
[Learn more](#)

Automatic User Provisioning with SCIM
[Learn more](#)

Password-based single sign-on
[Learn more](#)

Add

In de properties pagina worden de basis instellingen van de applicatie ingesteld. De surfconext logo vind je [hier](#). De ObjectID heb je nodig voor aanmaken van AssignedRoles (3.2). De optie visible to users mag uitgeschakeld worden, deze heb je wel nodig als je koppeling wil testen.

SURF.Conext - Properties
Enterprise Application

Save Discard Delete

Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

Security
Conditional Access
Permissions
Token encryption (Preview)


Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Access reviews

Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request

Enabled for users to sign-in? Yes No

Name

Homepage URL

Logo 

User access URI

Application ID

Object ID

Terms of Service Uri

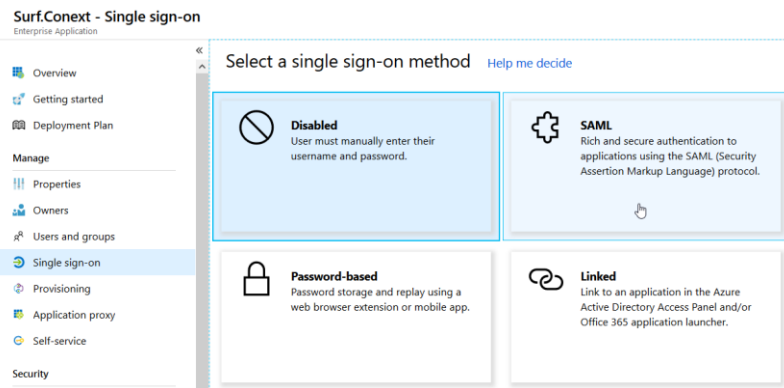
Privacy Statement Uri

Reply Uri

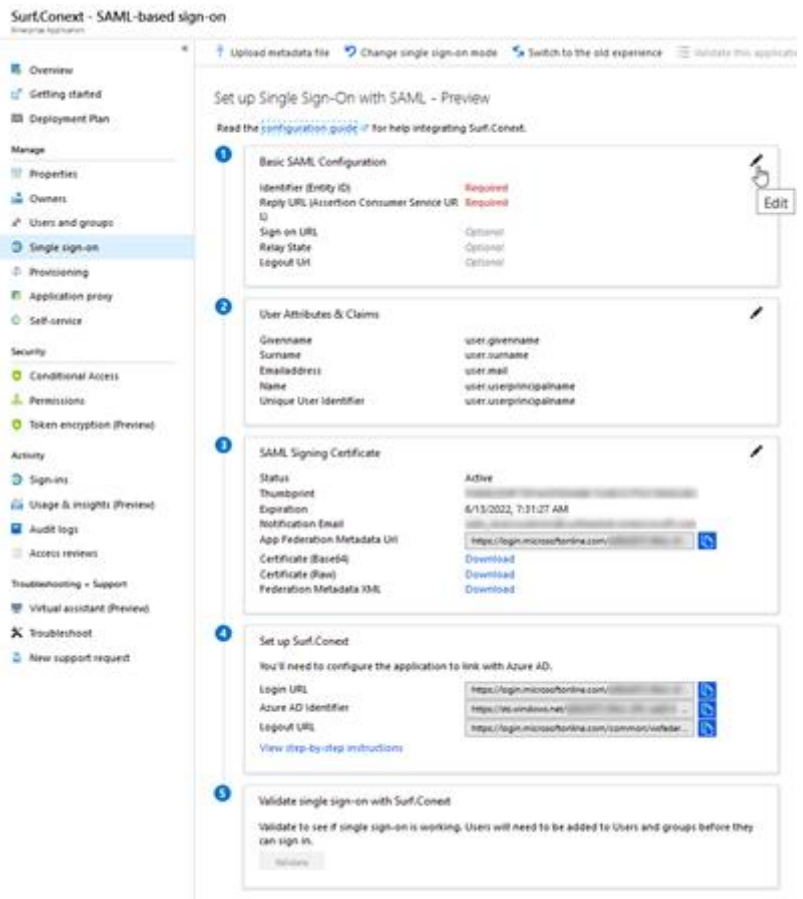
User assignment required? Yes No

Visible to users? Yes No

Selecteer in linker context menu Manage op Single sign-on en selecteer daarna de single sign-on methode: SAML



Begin met de SAML configuratie door uitvoeren van stap 1 en 2. Open de Basic SAML configuration door op pen in de linker bovenhoek te klikken



Vul de volgende gegevens in voor SAML configuratie.

Basic SAML Configuration

Save

* Identifier (Entity ID) ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

https://engine.surfconext.nl/authentication/sp/metadata

* Reply URL (Assertion Consumer Service URL) ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://engine.surfconext.nl/authentication/sp/consume-assertion

Sign on URL ⓘ
https://engine.surfconext.nl/authentication/sp/consume-assertion

Relay State ⓘ
Enter a relay state

Logout Url ⓘ
Enter a logout url

Open hierna in stap 2: User attributes & Claims en klik op Edit. Klik op + Add new claim om extra claims toe te voegen.

User Attributes & Claims

+ Add new claim

Name identifier principalname [nameid-format=emailAddress]

Groups returned from claims response

CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
urn:mace:dir:attribute-def:cn	user.displayName
urn:mace:dir:attribute-def:displayName	user.displayName
urn:mace:dir:attribute-def:eduPersonAffiliation	user.extensionattribute1
urn:mace:dir:attribute-def:eduPersonEntitlement	user.assignedroles

Vul bij Name de Claim naam in en voor de Claim value selecteer je user attribute of een constante waarde.

Manage user claims

* Name urn:mace:dir:attribute-def:displayName ✓

Namespace Enter a namespace URI

Source Attribute Transformation

* Source attribute Select from drop down or type a constant

- user.assignedroles
- user.city
- user.companyname
- user.country
- user.department
- user.displayName
- user.dnsdomainname
- user.employeeid

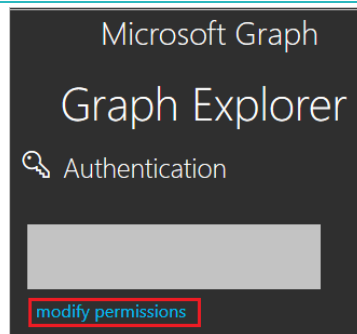
3.2. AANMAKEN VAN ASSIGNEDROLES

Dit deel beschrijft hoe assigned roles aangemaakt worden om een multi-value Claim op te bouwen. Elke assigned role krijgt zijn eigen “fixed value”. Om de assignedroles te bewerken wordt de graph explorer gebruikt om de Enterprise Application te patchen. De assignedroles worden in de Graph Explorer weergegeven als approles.

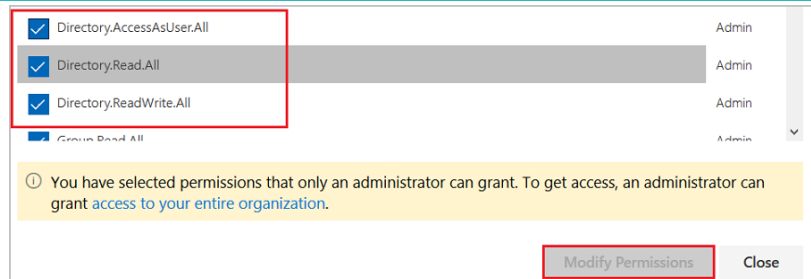
Login op de AzureAD portal en open daarna een tabblad voor de AAD Graph Explorer. Je logt nu automatisch aan op Graph Explorer

<https://developer.microsoft.com/graph/graph-explorer>

Begin met het instellen van de permissies voor Graph Explorer

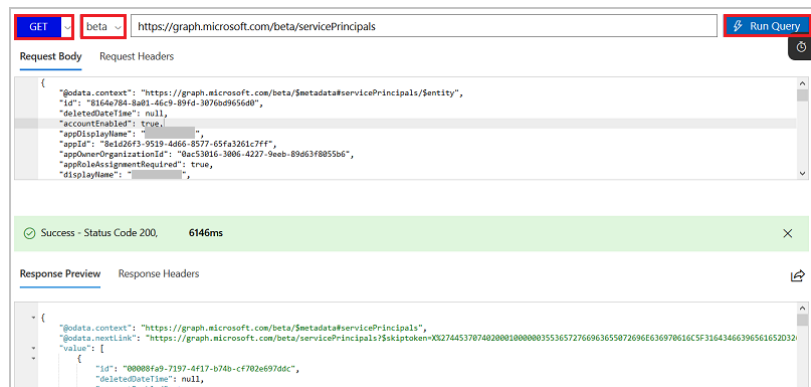


Selecteer de volgende permissies

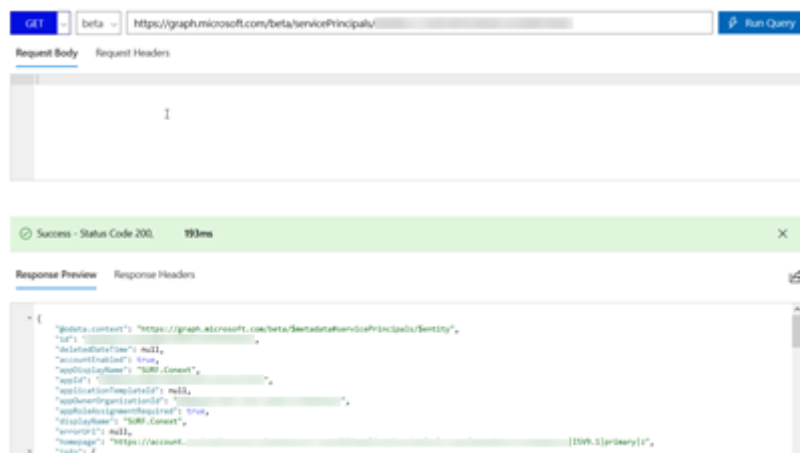


Open de volgende query en klik op Run Query. Response review laat een deel van alle resultaten zien.

<https://graph.microsoft.com/beta/servicePrincipals>



Pas the query aan met ObjectID



Kopieer de JSON stuk van de appRoles in een lokale editor (notepad)

Eerste regel
"appRoles":[

Laatste regel
,

```
"appRoles": [
  {
    "allowedMemberTypes": [
      "User"
    ],
    "description": "msiam_access",
    "displayName": "msiam_access",
    "id": "7dfd756e-8c27-4472-b2b7-38c17fc5de5e",
    "isEnabled": true,
    "origin": "Application",
    "value": null
  },
  ...
],
```

Breidt de approles uit met de gewenste claim values. Verwijder niet de user en msiam_access rollen.

```
"appRoles": [
  {
    "allowedMemberTypes": [
      "User"
    ],
    "description": "User",
    "displayName": "User",
    "id": "18d14569-c3bd-439b-9a66-3a2aee01d14f",
    "isEnabled": true,
    "origin": "Application",
    "value": null
  },
  {
    "allowedMemberTypes": [
      "User"
    ],
    "description": "msiam_access",
    "displayName": "msiam_access",
    "id": "b9632174-c057-4f7e-951b-be3adc52bfe6",
    "isEnabled": true,
    "origin": "Application",
    "value": null
  }
],
```

Een extra claim value ziet er als volgt uit
Wijzig de values van description, displayName en value voor de multi-value SAML claim. Geef elke approle een unieke id.

Zorg dat deze JSON formatering correct is. Let hierbij op de scheidingstekens “,” tussen de approles {}

```
{  
  "allowedMemberTypes": [  
    "User"  
  ],  
  "description": "eduPersonEntitlement personal-admin",  
  "displayName": "personal-admin",  
  "id": "d45c250a-ace0-4660-87fc-a1c33afdb282",  
  "isEnabled": true,  
  "origin": "ServicePrincipal",  
  "value": "urn:mace:terena.org:tcs:personal-admin"  
},
```

Voorbeeld van 4 extra approles

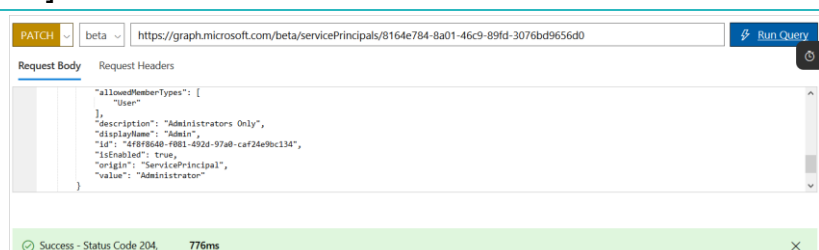
```
"appRoles": [  
  {  
    "allowedMemberTypes": [  
      "User"  
    ],  
    "description": "User",  
    "displayName": "User",  
    "id": "18d14569-c3bd-439b-9a66-3a2aee01d14f",  
    "isEnabled": true,  
    "origin": "Application",  
    "value": null  
  },  
  {  
    "allowedMemberTypes": [  
      "User"  
    ],  
    "description": "msiam_access",  
    "displayName": "msiam_access",  
    "id": "b9632174-c057-4f7e-951b-be3adc52bfe6",  
    "isEnabled": true,  
    "origin": "Application",  
    "value": null  
  },  
  {  
    "allowedMemberTypes": [  
      "User"  
    ],  
    "description": "eduPersonEntitlement personal-admin",  
    "displayName": "personal-admin",  
    "id": "d45c250a-ace0-4660-87fc-a1c33afdb282",  
    "isEnabled": true,  
    "origin": "ServicePrincipal",  
    "value": "urn:mace:terena.org:tcs:personal-admin"  
  }  
]
```

```

    },
    {
      "allowedMemberTypes": [
        "User"
      ],
      "description": "eduPersonEntitlement surfspot-credits",
      "displayName": "surfspot-credits",
      "id": "d45c250a-ace0-4660-87fc-a1c33afdb284",
      "isEnabled": true,
      "origin": "ServicePrincipal",
      "value": "urn:x-surfnet:xxxxxxx.nl:surfspot:Credits:7500"
    },
    {
      "allowedMemberTypes": [
        "User"
      ],
      "description": "eduPersonEntitlement surfdrive",
      "displayName": "surfdrive",
      "id": "d45c250a-ace0-4660-87fc-a1c33afdb283",
      "isEnabled": true,
      "origin": "ServicePrincipal",
      "value": "urn:x-surfconext:xxxxxxx.nl:surfdrive:quota:100"
    },
    {
      "allowedMemberTypes": [
        "User"
      ],
      "description": "eduPersonEntitlement personal-user",
      "displayName": "personal-user",
      "id": "d45c250a-ace0-4660-87fc-a1c33afdb281",
      "isEnabled": true,
      "origin": "ServicePrincipal",
      "value": "urn:mace:terena.org:tcs:personal-user"
    }
  ]
}

```

Kopieer de appRoles tekst naar de Request Body veld en wijzig de query commando van GET naar PATCH en klik op Run Query. Je krijgt onderin een success melding als dit gelukt is.



Het kan paar minuten duren voordat de nieuwe assignedroles zichtbaar worden in de Enterprise Application - Users & Groups. Deze afbeelding is inclusief groepen. Zie volgende paragraaf om groepen aan de assignedroles te koppelen.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
A_Federatieve_Diensten_Certific	Group	personal-admin
A_Federatieve_Diensten_Person	Group	personal-user
A_Federatieve_Diensten_Surfdriv	Group	surfdrive
A_Federatieve_Diensten_SURFsp	Group	surfspot-credits
AG_SA_SurfConext	Group	User

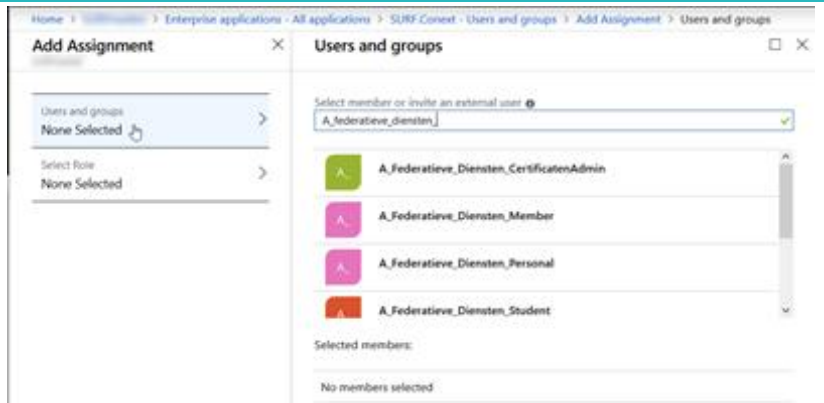
3.3. AANMAKEN VOOR GROEPS - ASSIGNEDROLES

Dit deel beschrijft hoe groepen aan de assignedroles worden gekoppeld.

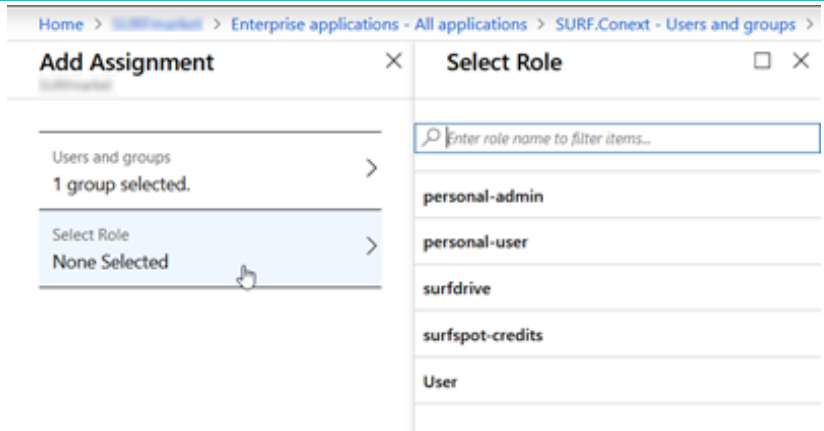
Open Users and Groups in de Enterprise Application - SURF.Conext, en druk op + Add User



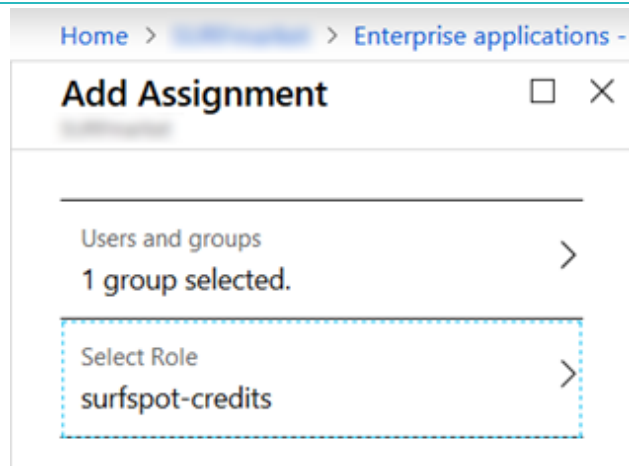
Voeg een of meerdere groepen toe voor een van de assigned roles.



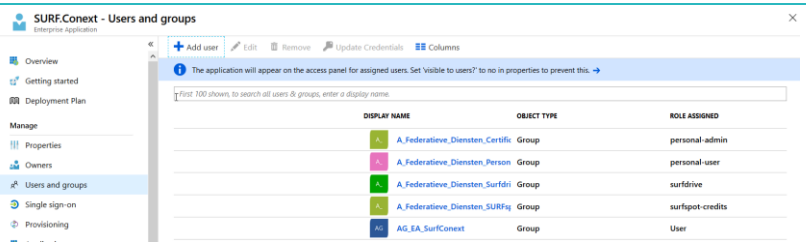
Selecteer 1 role



Druk op Assign knop om de mapping toe te voegen.



Afhankelijk van het aantal rollen (values) krijg je een lijst van groep en rollen.



Door een gebruiker lid te maken van een of meer van deze “role/value” groepen kan per gebruiker bepaald worden welke values toegekend worden aan de multi-value SAML claim.

4. VALIDATIE SAML CLAIMS


Nadat SurfConext de SAML koppeling met AzureAD heeft aangemaakt kun je de SAML claims controleren op de volgende URL: <https://profile.surfconext.nl/>

Op deze pagina selecteer je de nieuwe SAML koppeling van jouw organisatie. Hierna login je in met een account om de claims te controleren.

Show response from Identity Provider

✓ Authentication success

Identity Provider

	
Logo	
Name	SurfConext
Entity ID	http://auth.surfconext.nl/adfs/services/trust
Workflow Status	prodaccepted

SAML2 Subject

NameID	MVercoouteren@surfconext.nl
--------	-----------------------------

Attributes

SURFconext Display Name	Name	Value	Valid
User ID	um:mace:dir:attribute-def:uid	MVercoouteren	✓
Email address	um:mace:dir:attribute-def:mail	Maurice.Vercoouteren@surfconext.nl	✓
Display Name	um:mace:dir:attribute-def:displayName	Maurice Vercoouteren	✓
Surname	um:mace:dir:attribute-def:sn	Vercoouteren	✓
Full Name	um:mace:dir:attribute-def:cn	Maurice Vercoouteren	✓
First name	um:mace:dir:attribute-def:givenName	Maurice	✓
Affiliation	um:mace:dir:attribute-def:eduPersonAffiliation	employee	✓
Organization	um:mace:terena.org:attribute-def:schacHomeOrganization	surfconext.nl	✓
Entitlement	um:mace:dir:attribute-def:eduPersonEntitlement	<ul style="list-style-type: none">um:mace:terena.org:tcs:personal-userum:x-surfnet:surfdrive:quota:100um:x-surfnet:surfspot:Credits:7500	✓
Institution user ID	um:mace:dir:attribute-def:eduPersonPrincipalName	MVercoouteren@surfconext.nl	✓
Preferred Language	um:mace:dir:attribute-def:preferredLanguage	NL	✓

5. REFERENTIES

Configuratie van een non-gallery application in AzureAD

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-single-sign-on-non-gallery-applications>

Configuratie van role claims

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-enterprise-app-role-management>



INSPARK

Innovate to accelerate