SAML KOPPELING TUSSEN AZUREAD EN SURFCONEXT

SAML CLAIM MAPPING

14-JUN-2019

Maurice Vercouteren
19-06-2019

InSpark

Inhoudsopgave

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.

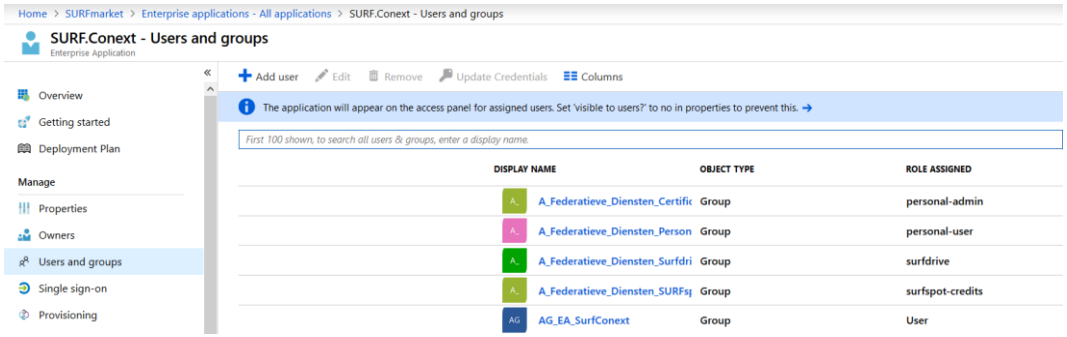
1: SAML Claim mapping

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.



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

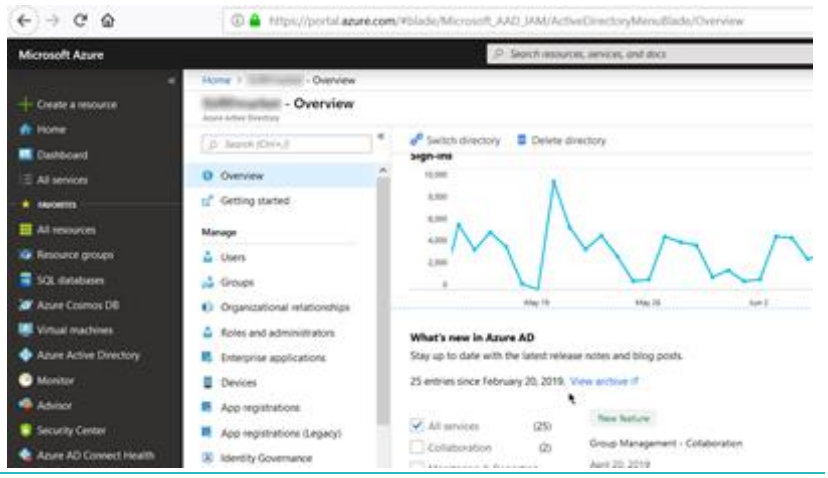
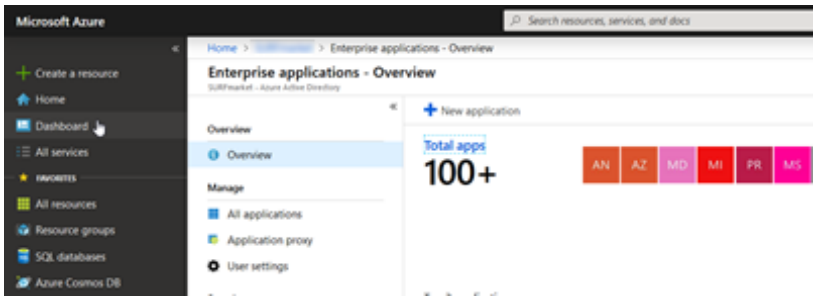
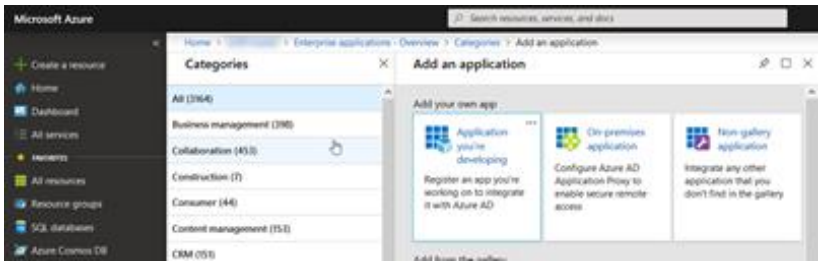
urn:x-surfnet:surfxxxxxx.nl:surfspot:Credits:7500
urn:x-surfnet:surfxxxxxx.nl:surfdrive:quota:100

3. BUILDGUIDE

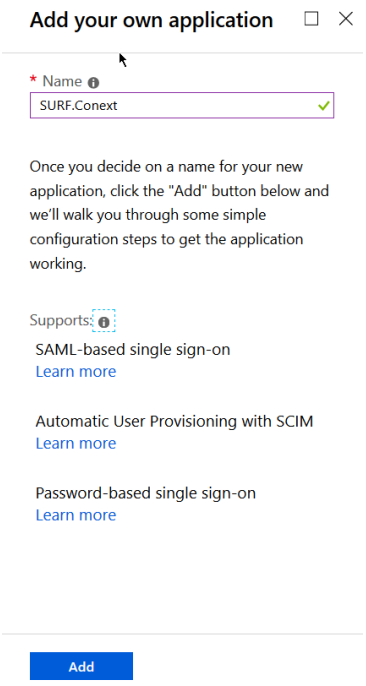
Instructie voor het maken van AzureAD SAML koppeling met SurfConext. Voor het maken van SAML configuratie heb je global admin rechten nodig in je AzureAD/Office365 tenant.

3.1. AANMAKEN SAML KOPPELING MET SURFCONEXT

Deze paragraaf beschrijft het maken van een SAML koppeling met SurfConext

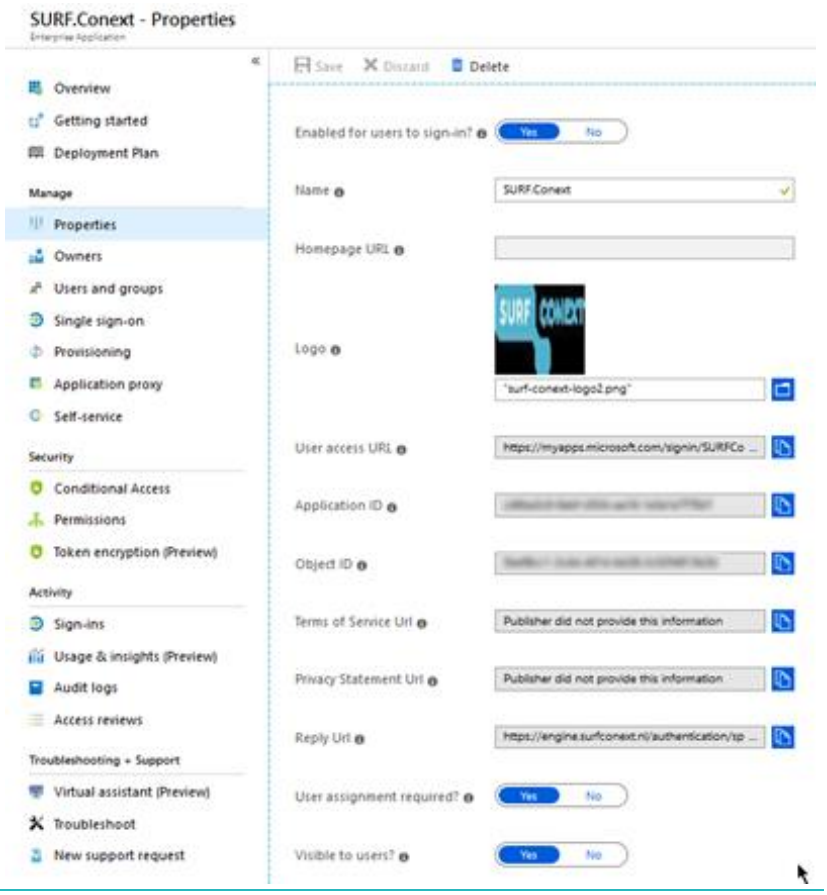
Login in op de Azure Portal en open de Azure Active Directory, Enterprise Applications	
Druk op + New Application	
Selecteer de tegel met Non-gallery application	

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

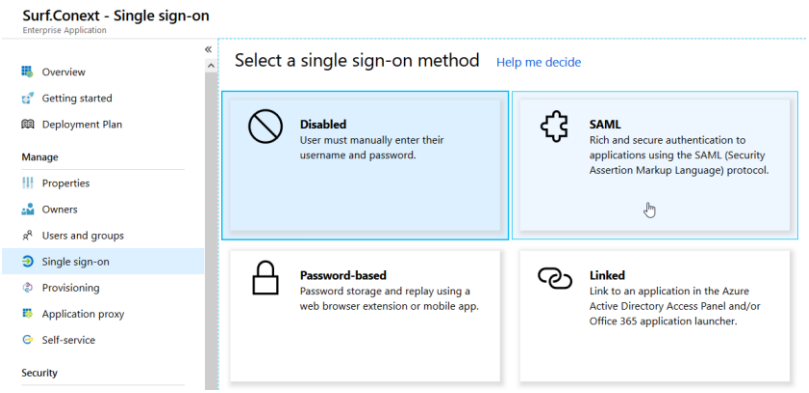


In de properties pagina worden de basis instellingen van de applicatie ingesteld.

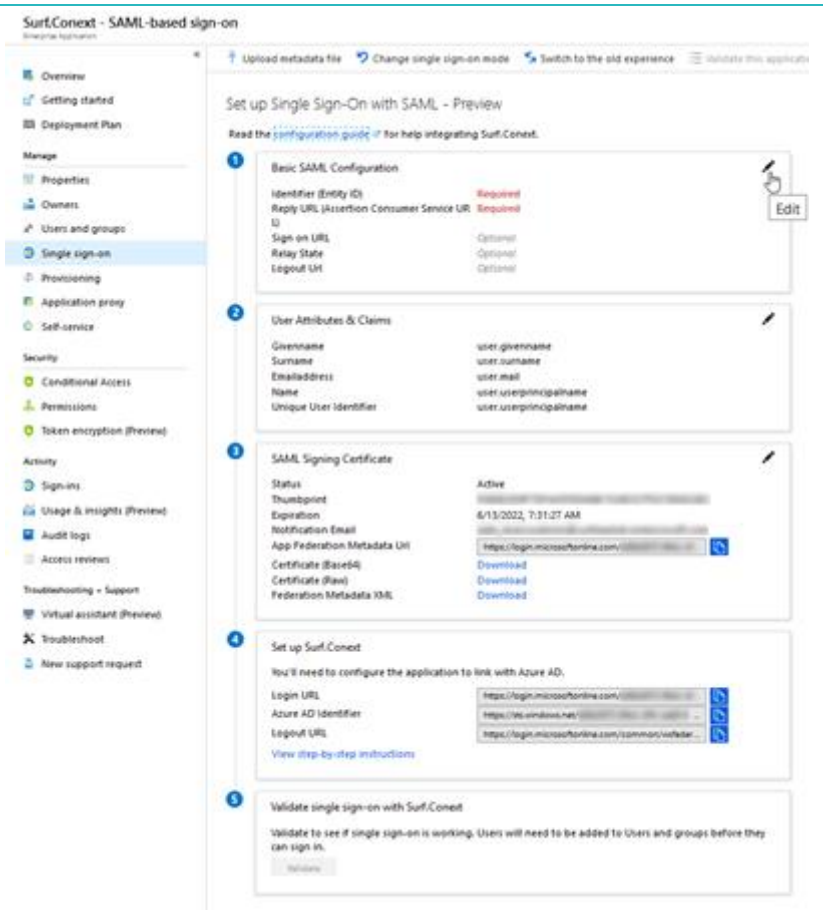
De surfconext logo vind je hier. De ObjectID heb je nodig voor aanmaken van AssignedRoles (3.2). De optie visiable to users mag uitgeschakeld worden, deze heb je wel nodig als je koppeling wil testen.



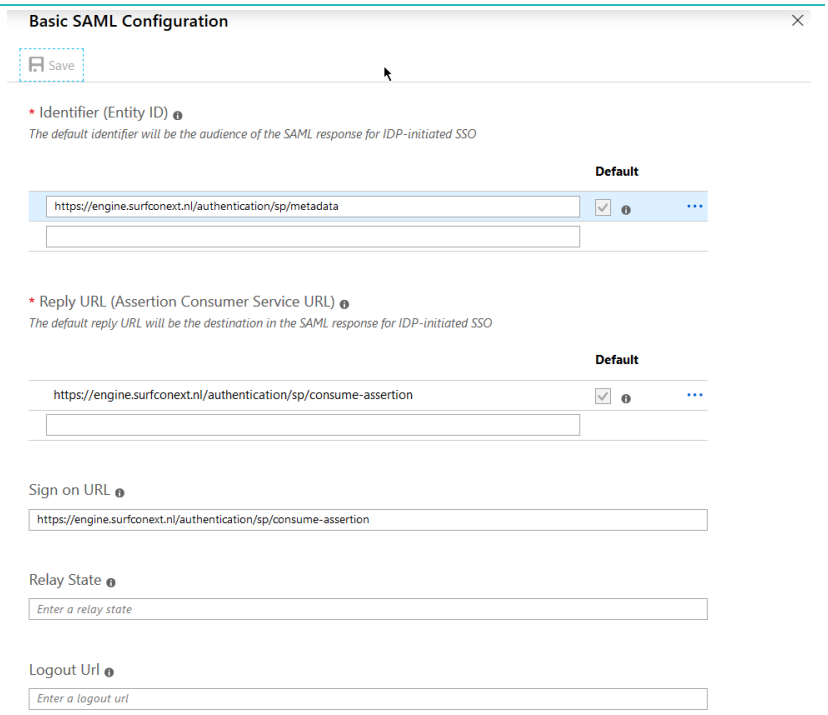
Selecteer in linker context menu Manage op Single sign-on en selecteer daarna de single sign-on methode: SAML



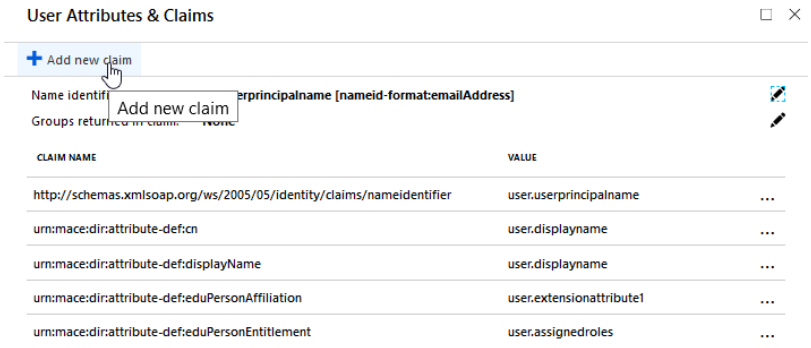
Begin met de SAML configuratie door uitvoeren van stap 1 en 2. Open de Basic SAML configuration door op pen in de linker bovenhoek te klikken



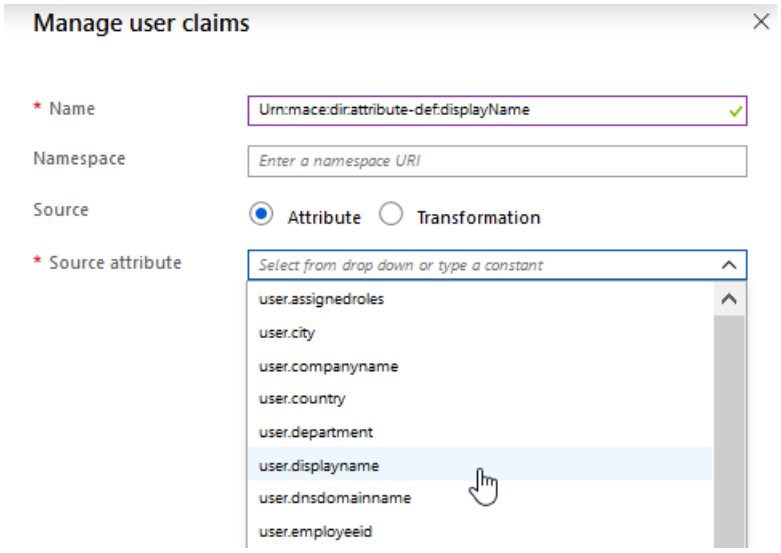
Vul de volgende gegevens in voor SAML configuratie.



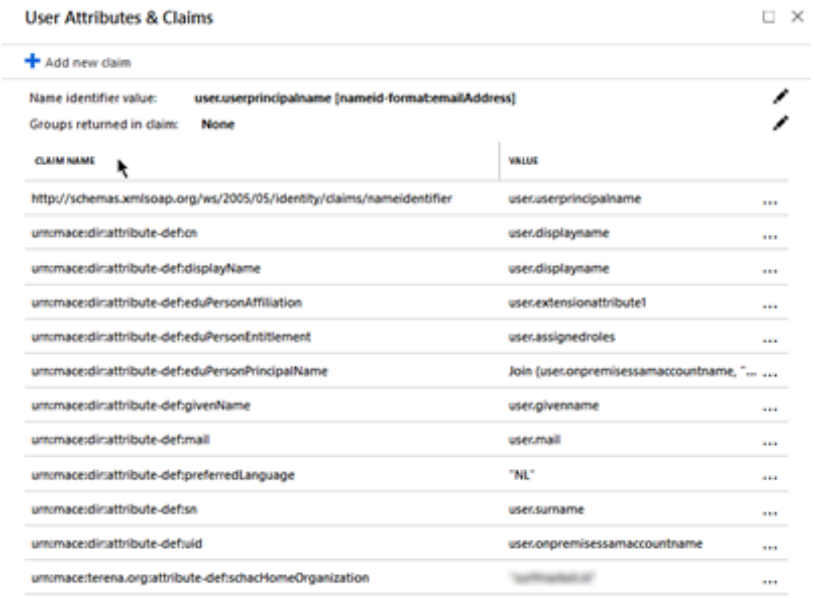
Open hierna in stap 2: User attributes & Claims en klik op Edit. Klik op + Add new claim om extra claims toe te voegen.



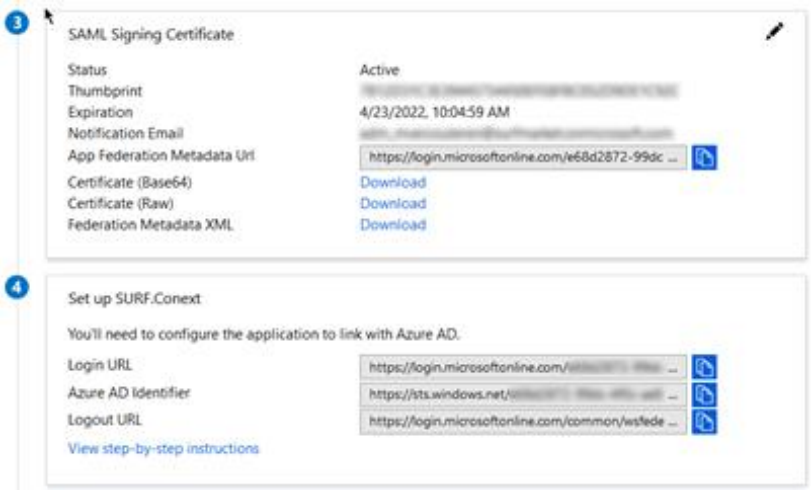
Vul bij Name de Claim naam in en voor de Claim value selecteer je user attribute of een constante waarde.



Maak alle SAML Claims aan die je nodig hebt voor SurfConext.

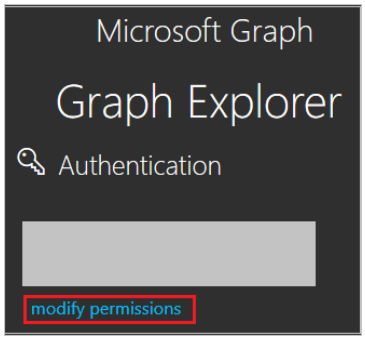
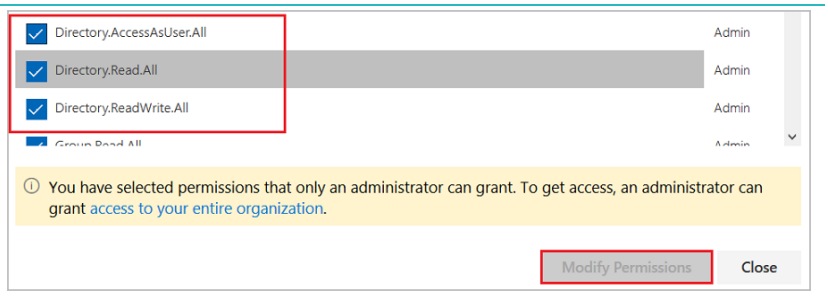
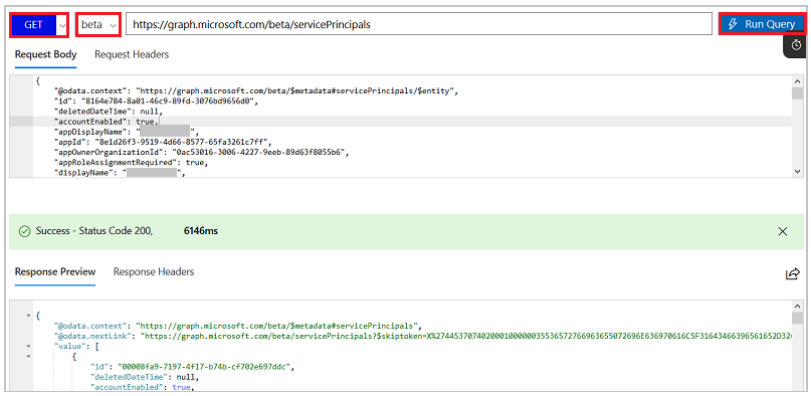


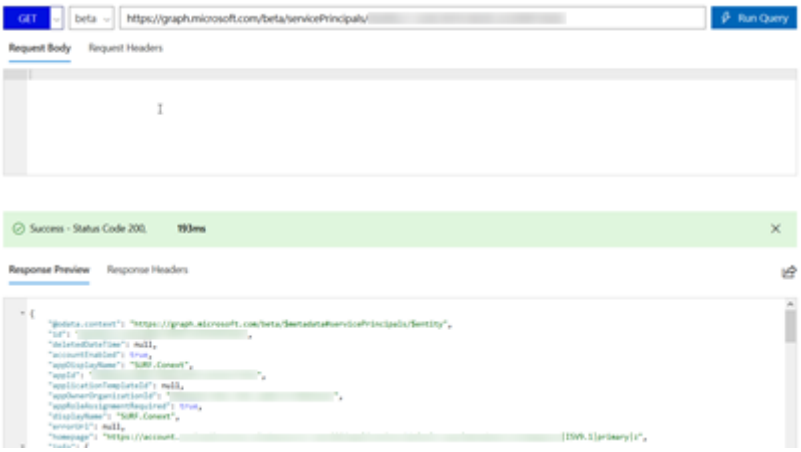
Kopieer de gegevens van stap 3 en 4 naar je computer en download de certificaten. Deze informatie heeft SurfConext nodig om de koppeling met jouw AzureAD te maken.



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],	

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 scheidingsteken “,” tussen de approles {}

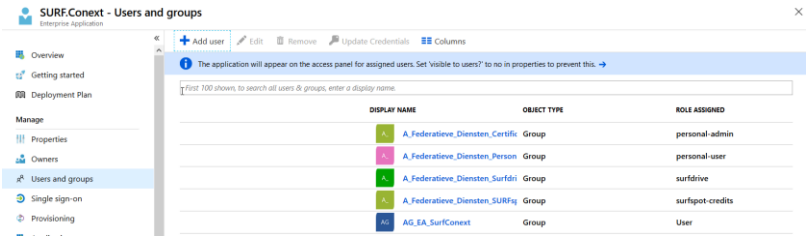

```
{
   "allowedMemberTypes": [
      "User"
   ],
   "description": "eduPersonEntitlement personal-admin",
   "displayName": "personal-admin",
   "id": "d45c250a-ace0-4660-87fc-a1c33afdb282",
   "isEnabled": true,
   "origin": "ServicePrincipal",
   "value": "urn:mace:terena.org:tcs:personal-admin"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


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"
```

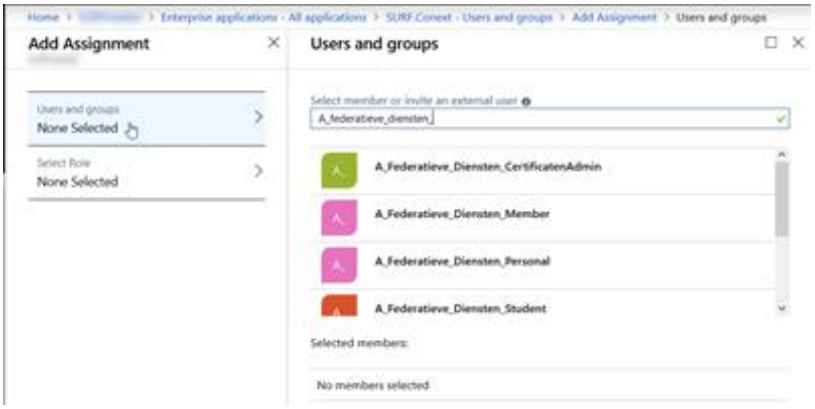
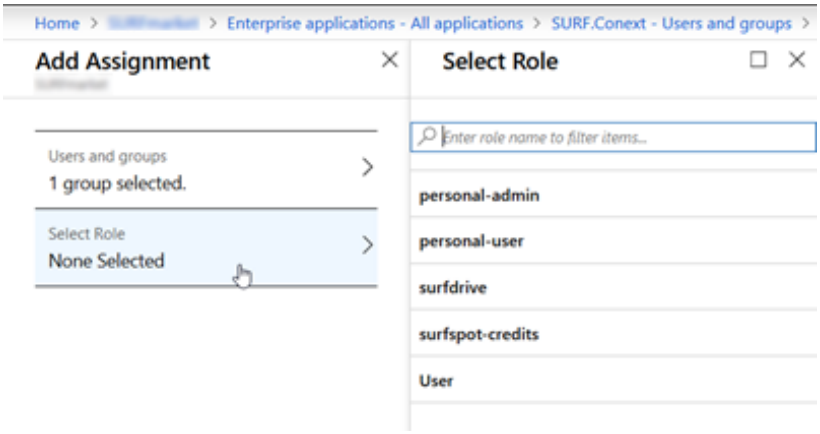
```
        },
        {
            "allowedMemberTypes": [
                "User"
            ],
            "description": "eduPersonEntitlement surfspot-
credits",
            "displayName": "surfspot-credits",
            "id": "d45c250a-ace0-4660-87fc-a1c33afdb284",
            "isEnabled": true,
            "origin": "ServicePrincipal",
            "value": "urn:x-
surfnet:xxxxxxxx.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"
        }
    ]
```

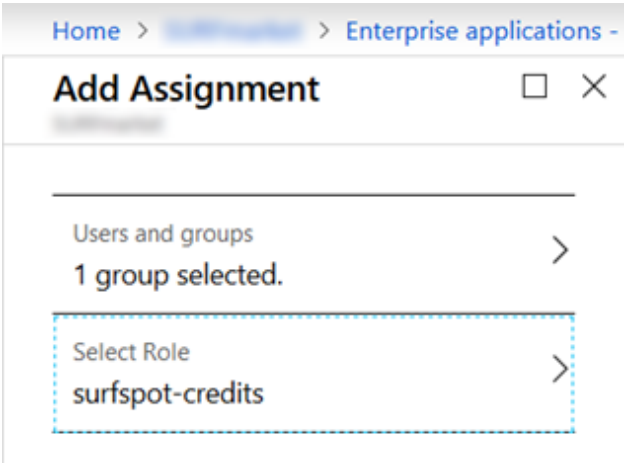
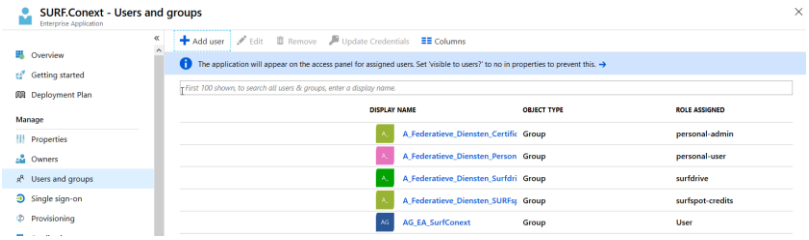

Kopieer de appRoles tekst naar de Request Body veld en wijzig de query commando van GET naar PATCH en klik op Run Query. Je krijgt onderin een success melding als dit gelukt is.

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.	

3.3. AANMAKEN VOOR GROUPS - 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	

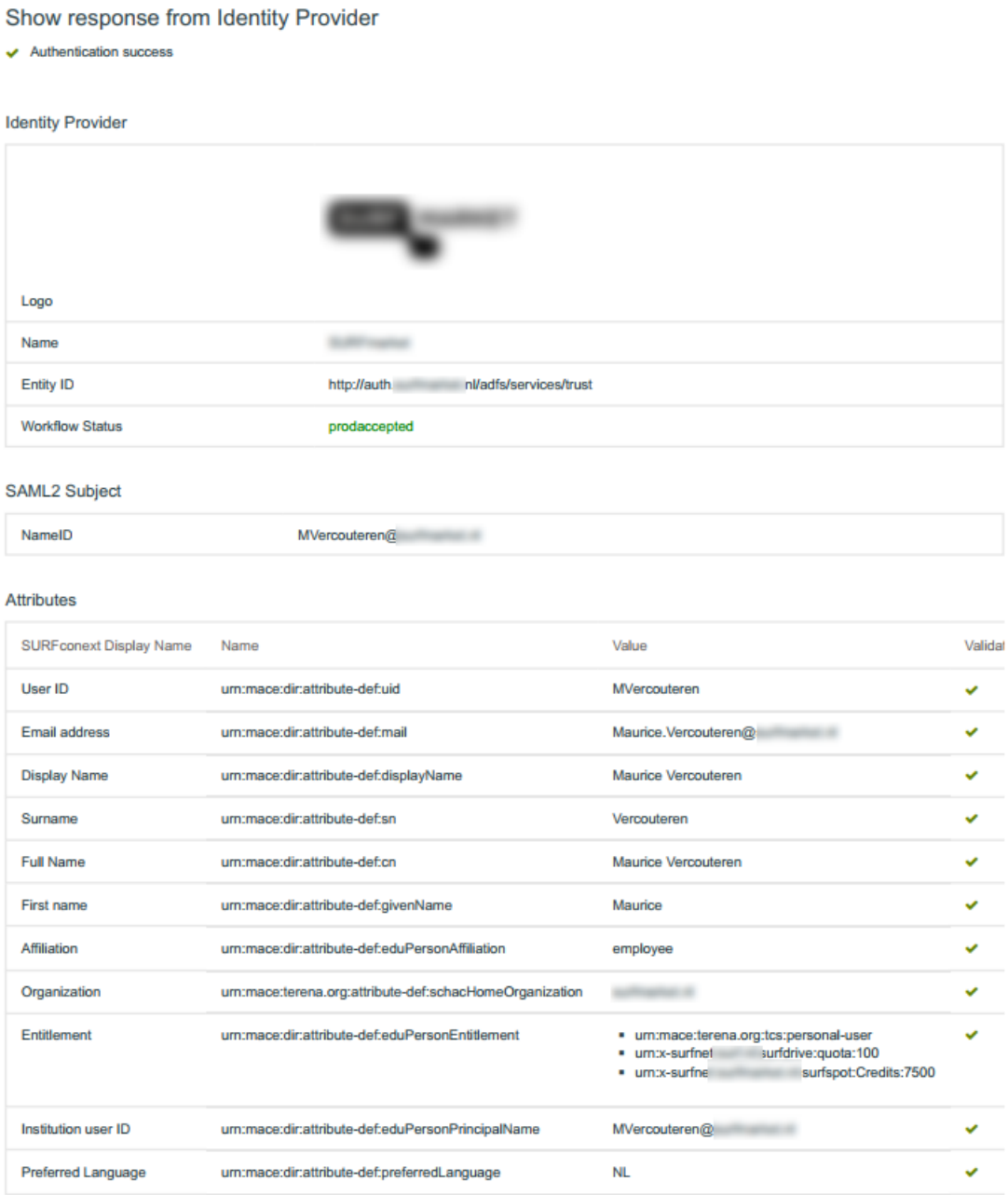
Druk op Assign knop om de mapping toe te voegen.	
Afhankelijk van het aantal rollen (values) krijg je een lijst van groep en rollen.	

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	
Entity ID	http://auth nl/adfs/services/trust
Workflow Status	prodaccepted

SAML2 Subject

NameID	MVercouteren@

Attributes

SURFconext Display Name	Name	Value	Validat
User ID	urn:mace:dir:attribute-def:uid	MVercouteren	✔
Email address	urn:mace:dir:attribute-def:mail	Maurice.Vercouteren@	✔
Display Name	urn:mace:dir:attribute-def:displayName	Maurice Vercouteren	✔
Surname	urn:mace:dir:attribute-def:sn	Vercouteren	✔
Full Name	urn:mace:dir:attribute-def:cn	Maurice Vercouteren	✔
First name	urn:mace:dir:attribute-def:givenName	Maurice	✔
Affiliation	urn:mace:dir:attribute-def:eduPersonAffiliation	employee	✔
Organization	urn:mace:terena.org:attribute-def:schacHomeOrganization		✔
Entitlement	urn:mace:dir:attribute-def:eduPersonEntitlement	▪ urn:mace:terena.org:tcs:personal-user ▪ urn:x-surfnet surfdrive:quota:100 ▪ urn:x-surfne surfspot:Credits:7500	✔
Institution user ID	urn:mace:dir:attribute-def:eduPersonPrincipalName	MVercouteren@	✔
Preferred Language	urn: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