Rollekataloget

SAML opsætning

**Version**: 1.2.0

**Date**: 22.11.2018

**Author**: BSG

Indhold

[1 Indledning 3](#_Toc530636251)

[1.1 Nødvendige oplysninger 3](#_Toc530636252)

[2 Opsætning af Relying Part i AD FS 3](#_Toc530636253)

[2.1 Opret Claim Rule for NameID 3](#_Toc530636254)

# Indledning

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens AD FS, så det er muligt for kommunens medarbejdere at logge på Rollekataloget.

Det forudsættes at læseren har kendskab til konfiguration af AD FS.

## Nødvendige oplysninger

Rollekataloget skal have følgende oplysninger om brugere når de logger på

* Brugerens identitet (kommer i audit-loggen når brugerens udfører handlinger der skal logges).

Identitet skal sendes i NameID feltet under Subject. Der er ikke andre krævede attributter. Et eksempel på en korrekt udfyldt Subject/NameID blok vises nedenfor.

<Subject>

<NameID>**bsg**</NameID>

</Subject>

# Opsætning af Relying Part i AD FS

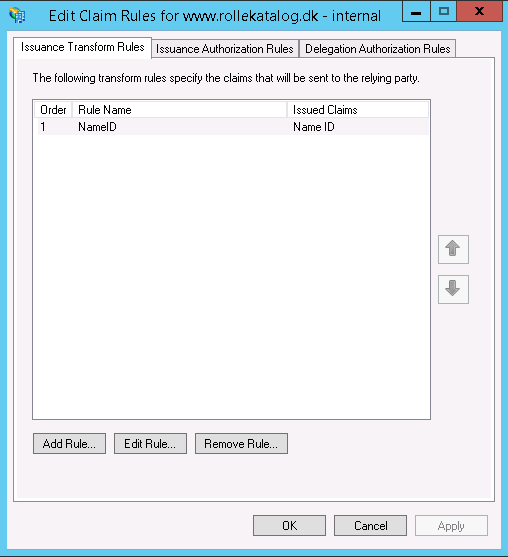
Der skal oprettes en ny ”Relying Party” i AD FS. Dette gøres på helt normal vis, og Rollekatalogets metadatafil kan hentes her (erstat <kommune> med dit kommunenavn)

https://<kommune>.rollekatalog.dk/saml/metadata

Når denne er oprettet, skal der opsættes relevante ”Claim Rules”, der sikrer at de relevante oplysninger om brugeren sendes til Rollekataloget på login tidspunkt.

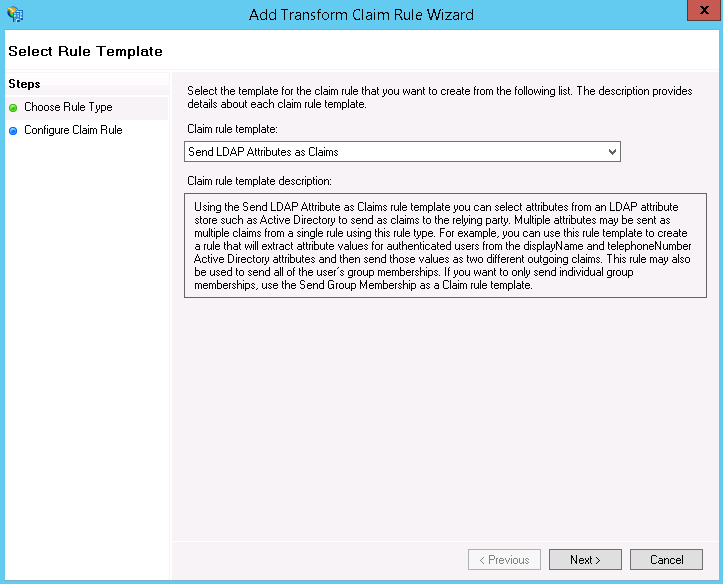
## Opret Claim Rule for NameID

Efter at en Relying Party oprettes i AD FS, åbnes skærmbilledet til Claim Rules automatisk, men man kan også få skærmbilledet frem ved at højreklikke på den Relying Party man har oprettet, og så vælge ”Edit Claim rules…”

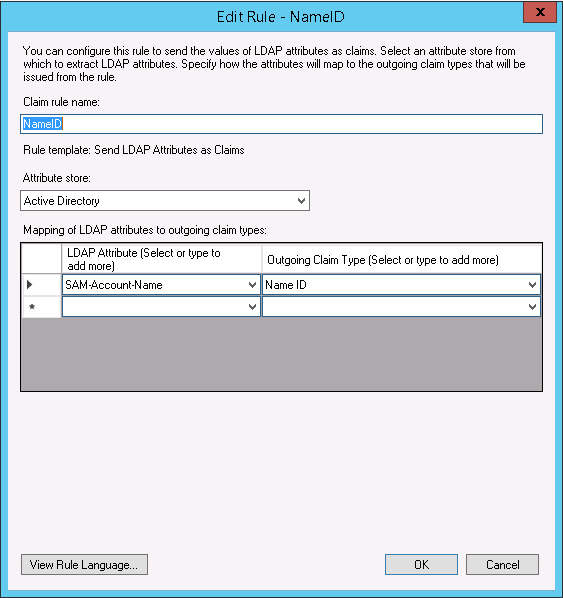


I dette skærmbillede trykker man på ”Add Rule” for at oprette en ny Claim Rule.

I efterfølgende skærmbillede vælges ”Send LDAP Attribute as Claims”.



Efterfølgende mappes SAM-Account-Name til de udgående claims, ved at udfylde skærmbilledet så det ligner nedenstående



Herefter er brugerens identitet mappet korrekt.