Danmarks Miljøportal (DMP)

Vejledning til ADFS 3.0-importapplikation:

Import af Safewhere\*Identify SP til AD FS 2019 IdP

Version 1.0

# Indledning

Denne vejledning beskriver brugen af importimportapplikationen til brug i forbindelse med AD FS 2019 i partnerorganisationer.

* Windows Server 2019 AD FS - Windows Server 2019[[6]](https://en.wikipedia.org/wiki/Active_Directory_Federation_Services#cite_note-AD_FS_Frequently_Asked_Questions_(FAQ)-6)

Vejledningen omhandler udelukkende brugen af importapplikationen, som benyttes op mod DMP's nye Safewhere\*Identify-baserede SP.

Der foreligger også en tilsvarende vejledning til importapplikationen, når denne skal benyttes op mod DMP's hidtidige ADFS 2.0 og ADFS 3.0 baserede SP.

Importapplikationen åbner mulighed for at indlæse en liste af henholdsvis claims-definitioner, attributter og roller (som er eksporteret fra Safewhere\*Identify-konfigurationen i DMP's centrale brugerstyring) og få disse oprettet i Active Directory og AD FS 2019-opsætningen hos den pågældende partnerorganisation. Dvs. sagt på en anden måde: Det er muligt for partnerorganisationer automatisk at få oprettet de basisinformationer og roller i ADFS såvel som Active Directory, der er nødvendige for at konfigurere partnerorganisationen til at optræde som fødationspartner i forhold til den opgraderede version af DMP's centrale brugerstyring.

Udover selve importapplikationen (som tager form af en .NET-applikation), så skal du råde over følgende filer for at gennemføre konfigureringen af AD FS 2019:

* ClaimDescriptionExport.xml – XML-fil med claims (claims descriptions), der finder anvendelse i DMP-løsningen. DefaultADPropertyMapping.xml – XML-fil med mappings mellem Active Directory-attributter og de claims, der er nødvendige for at kunne anvende DMP-løsningen.
* Speciel XML-fil genereret af DMP til partnerorganisationen – XML-fil med de grupper, der finder anvendelse op mod DMP-løsningen.

*Bemærk at importapplikationen udelukkende fungerer i partnerorganisationen, der anvender Active Directory og Microsoft AD FS 3.0 / ADFS 2019.*

# Indhold

[Indledning 2](#_Toc103009264)

[Indhold 3](#_Toc103009265)

[Introduktion til konfigurering til DMP hos partnerorganisationen 4](#_Toc103009266)

[Oprettelse af DMP som Relying Party 5](#_Toc103009267)

[Introduktion til importapplikationen 13](#_Toc103009268)

[Konfiguration af ADFS-importapplikationen 13](#_Toc103009269)

[Brug af ADFS-importapplikationen til import af claims 16](#_Toc103009270)

[Brug af ADFS-importapplikationen til import af attributter 18](#_Toc103009271)

[Brug af ADFS-importapplikationen til import af roller 20](#_Toc103009272)

[Tilretning af claims i overensstemmelse med organisationens behov 23](#_Toc103009273)

[Oprettelse af avancerede claims 23](#_Toc103009274)

[Tilpasning af claims, der er unikke for hver enkelt organisation 26](#_Toc103009275)

[Oprettelse af speciel claim 31](#_Toc103009276)

[Aktivering af SSO til web services login på organisationens AD FS 3.0 server 33](#_Toc103009277)

[Aktivering af endpoint til web services login 34](#_Toc103009278)

[Aktivering af kryptering på udstedte tokens 36](#_Toc103009279)

# Introduktion til konfigurering til DMP hos partnerorganisationen

Importapplikationen er bygget for at spare partnerorganisationsadministratoren for det manuelle og ensformige indtastningsarbejde, der er forbundet med den praktiske etablering af føderationsaftalen med DMP.

Når partnerorganisationen anvender importapplikationen skal der kun udføres følgende aktiviteter efter partnerorganisationen har installeret og konfigureret dets AD FS 2019-server (se "Introduktion til automatisk login mod Danmarks Miljøportal’s Safewhere Identify SP – AD FS 3.0" for yderligere information) for at få DMP tilsluttet til partnerorganisationen:

* Fremsendelse af informationer omkring AD FS 2019-installationen til DMP’s administrator (se evt. "Introduktion til automatisk login mod Danmarks Miljøportal’s Safewhere Identify SP" for yderligere information)
* Oprettelse af DMP som Relying Party
* Import af claims (oprettelse af de nødvendige claims descriptions) ved hjælp af importapplikationen
  + Med brug af den attributfil, der er fremsendt fra DMP
* Import af attributter (oprettelse af de nødvendige mapninger mellem claims og Active Directory-attributter) ved hjælp af importapplikationen
  + Med brug af den attributfil, der er fremsendt fra DMP
* Import (og evt. oprettelse i Active Directory) af grupper ved hjælp af importapplikationen
  + Med brug af den gruppefil, der er fremsendt fra DMP
* Tilretning af claims i overensstemmelse med organisationens behov
* Validering af at det er muligt at få kontakt fra en af partnerorganisationens egne pc-klienter til DMP’s ClaimApp-applikation samt validering af at claims bliver korrekt overført til samme. <https://administration.miljoeportal.dk/identifyclaimapp/>

Fra dette tidspunkt behøver partnerorganisationen ikke længere at bruge yderligere energi på AD FS 2019 for at føderationsløsningen til at fungere efter hensigten. Dvs. alt det efterfølgende arbejde består i at melde brugerne til og fra de ønskede Active Directory-grupper ovre i partnerorganisationens eget Active Directory.

*Hele installations- og konfigureringsforløbet for AD FS 2019 hos en partnerorganisation er beskrevet indgående i dokumentet "Introduktion til automatisk login mod Danmarks Miljøportal’s Safewhere Identify SP – AD FS 2019".*

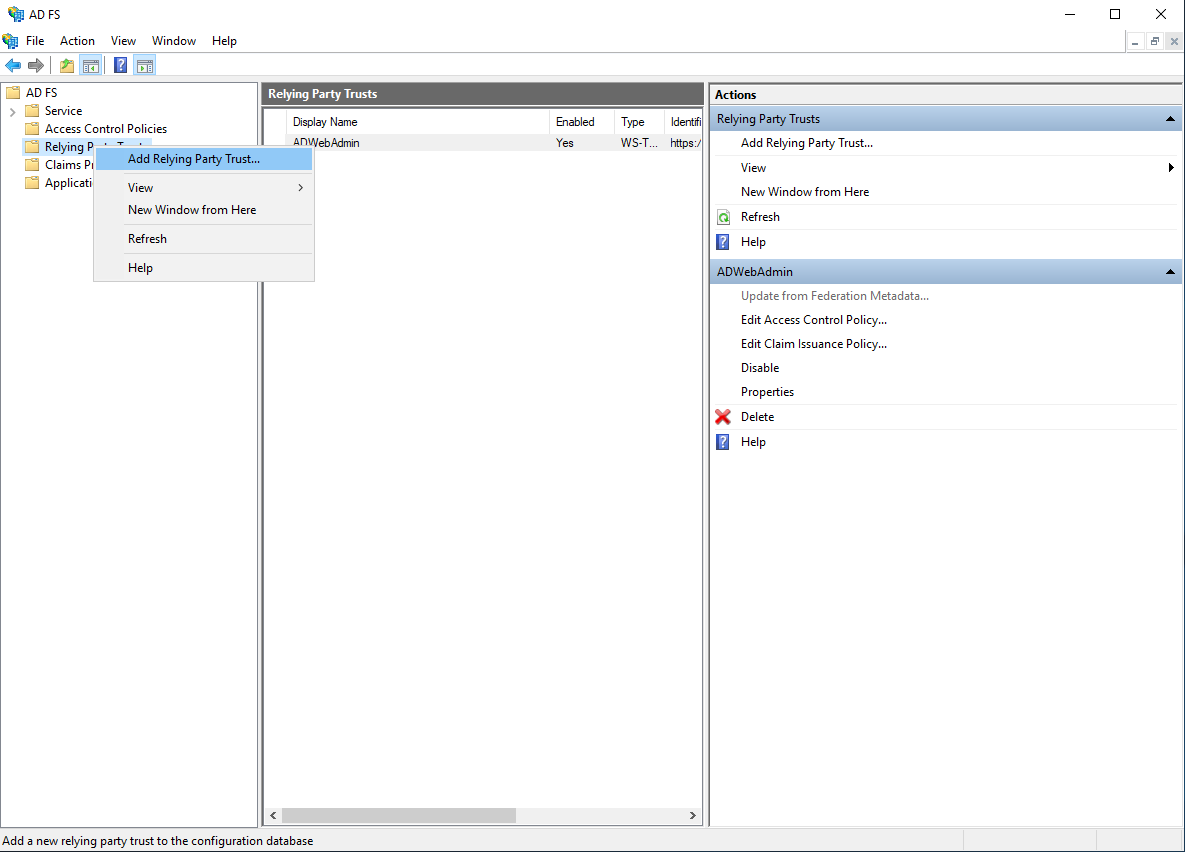
# Oprettelse af DMP som Relying Party

Før importapplikationen køres skal DMP's Safewhere\*Identify SP oprettes som Relying Party på partnerorganisationens AD FS 2019-server.

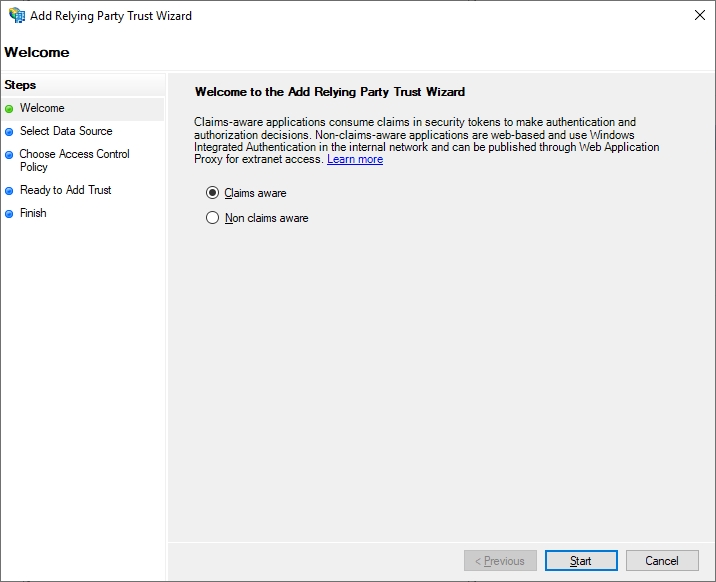
DMP's Safewhere\*Identify SP oprettes som RP på AD FS 2019 på følgende vis:

Log på AD FS 2019-serveren med administrator-rettigheder

Start AD FS 2019 Management-applikationen

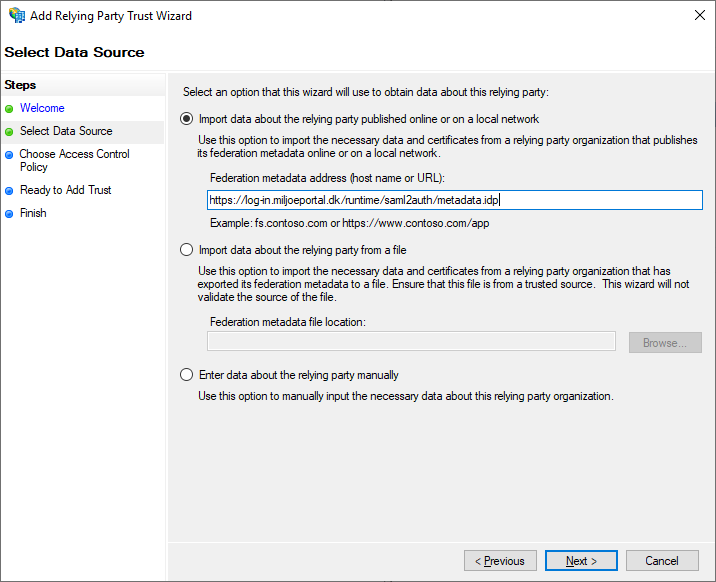
Højreklik på Relying Party Trusts og vælg Add Relying Party Trust..

Vælg ”Claims aware” og Tryk Start

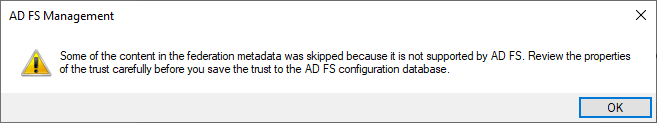


Indtast

<https://log-in.miljoeportal.dk/runtime/saml2auth/metadata.idp> i "Import data about the relying party published online or on a local network" og tryk Next.

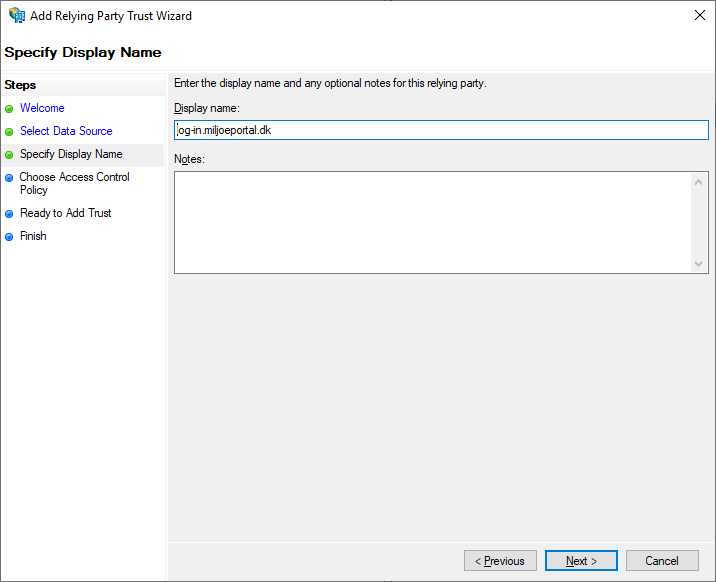


Denne dialog dukker evt. op.

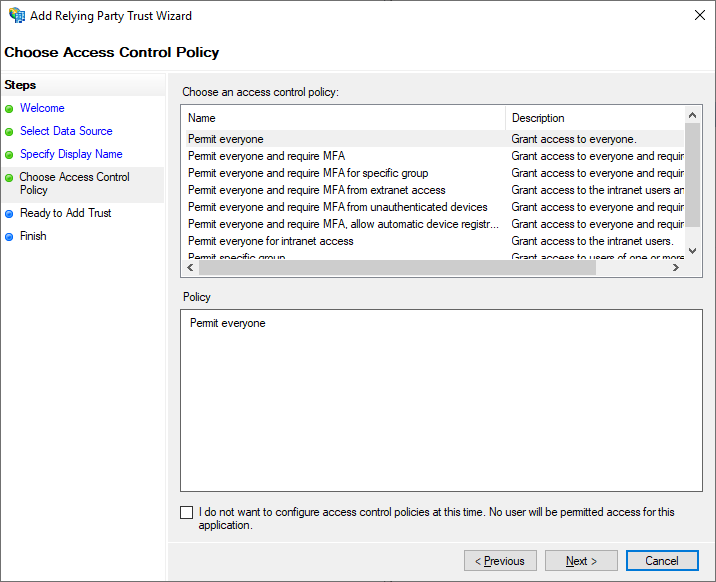


Tryk “OK”

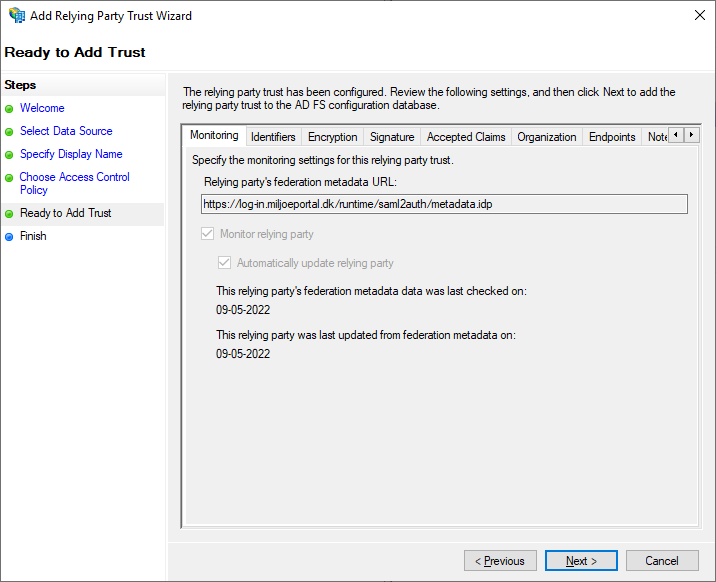
Tryk Next.

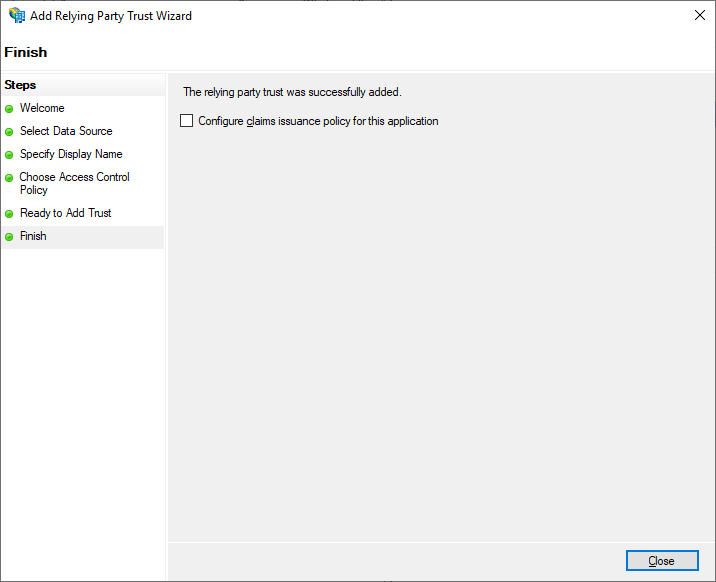


Tryk Next.



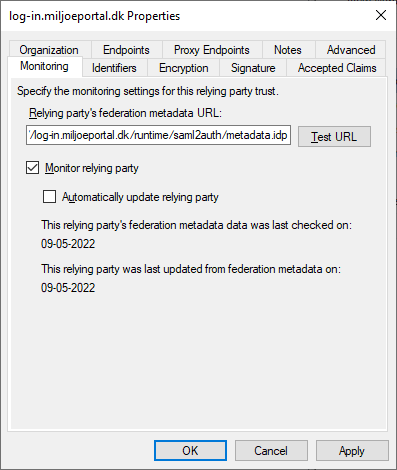
Tryk Next





Fjern afkrydsningen i "Configure claims issuance policy for this application" og tryk Close.

Det er desuden vitalt at fjerne afkrydsningen i ”Automatically update relying party” i Monitoring-fanebladet, da man ellers vil opleve at ændringen, der blev udført i sidste skridt, bliver fjernet og AD FS 2019-logins i de fleste tilfælde vil ophøre med at fungere.



*Hvis man har behov for at opdatere federation metadata vil det således være nødvendigt at genkøre PowerShell-ændringen som angivet i sidste skridt umiddelbart efter opdateringen.*

# Introduktion til importapplikationen

ADFS-importapplikationen automatiserer oprettelsen hos partnerorganisationen af de nødvendige claims, attributter og grupper i Active Directory samt de nødvendige claim-mapninger i ADFS 3.0. Dette sker på basis af filer, der indeholder en liste over de claims, attributter eller roller, der er relevante for partnerorganisationen. Dvs. du skal huske at rekvirere de relevante filer (dvs. XML-filer med en liste over de ønskede attributter eller roller) hos DMP.

Importapplikationen fungerer kun i partnerorganisationen, der anvender Active Directory og Microsoft AD FS 3.0.

Importapplikationen **skal** afvikles på den server i partnerorganisationen, som har AD FS 3.0 installeret. Hvis ADFS-installationen består af flere servere i et NLB-miljø skal applikationen kun afvikles en gang.

Applikationen skal afvikles i konteksten af en bruger, som har administratorrettigheder på AD FS 3.0-serveren og har ret til at læse og oprette grupper i Active Directory.

Hvis der måtte komme filer med opdateringer til claims, attributter eller roller er det muligt at køre importapplikationen igen. Importapplikationen er i stand til at ændre på de eksisterende mapninger for attributter eller roller, oprette claim descriptions samt tilføje Active Directory-grupper. Den kan imidlertid ikke slette eksisterende Active Directory-grupper.

Importapplikationen udfører følgende opgaver, når den anvendes til import af claims:

* Oprettelse af de relevante claims i form af Claim Descriptions i ADFS.

Importapplikationen udfører følgende opgaver, når den anvendes til import af attributter:

* Oprettelse af én LDAP-baseret Claim Rule i ADFS med navnet ”AD-attributmapninger”, som indeholder mappninger fra de relevante AD-attributter til de oprettede Claim Descriptions.
* Opdatering af IssuanceTransformRules på den relevante Relying Party i ADFS-opsætningen

Importapplikationen udfører følgende opgaver, når den anvendes til import af roller:

* Oprettelse af de relevante roller – i form af Security Groups – i Active Directory.
* Oprettelse af en Claim Rule i ADFS for hver enkelt Active Directory-gruppe. Hver af disse claim rules bærer gruppens navn .
* Opdatering af IssuanceTransformRules på den relevante Relying Party i ADFS-opsætningen.

# Konfiguration af ADFS-importapplikationen

Applikationen konfigureres i konfigurationsfilen ”AdfsGroupClaimImport.exe.config”, som ligger i samme folder som applikationen. Filen kan åbnes i notepad.exe eller en anden teksteditor.

Nedenfor er vist en konfigurationsfil, hvor de elementer, der skal ændres er angivet med fed skrift.

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<configSections>

<sectionGroup name="GAD">

<section name="ADToolBox"

type="GAD.ADToolBox.ADToolBoxConfigurationSectionHandler,   
 GAD.ADToolBox"/>

</sectionGroup>

</configSections>

<GAD>

<ADToolBox>

<LDAPPath>**LDAP://dc1.kommune.dk**</LDAPPath>

<DomainRoot>**dc=kommune,dc=dk**</DomainRoot>

<Authentication>

<Impersonate>**False**</Impersonate>

<UserName>kommuneadm</UserName>

<Password>megethemmeligt</Password>

</Authentication>

</ADToolBox>

</GAD>

<appSettings>

<!--Version-->

<add key="Version" value="IDENTIFY"/>

<!--ADFS Property Import-->

<add key="default\_federation\_partner" value="https://log-in.miljoeportal.dk/runtime/"/>

<add key="AD\_attribute\_mapping" value="AD-attributmapninger"/>

<add key="default\_role\_claim\_type" value="http://www.miljoeportal.dk/roles"/> </appSettings>

</configuration>

* LdapPath

Angiver LDAP-navnet i overensstemmelse med DNS-syntaksen til en Active Directory DC i det domæne, der skal oprettes grupper i. Såfremt man er ligeglad med hvilken DC, der vælges i det pågældende domæne kan man nøjes med at angive domænenavnet.

* DomainRoot

Angiver LDAP-stien i overensstemmelse med DN-syntaksen til Active Directory roddomænet (dvs. det første domæne i Active Directory forest’en).

* Impersonate

Skal sættes til True, hvis værktøjet skal køre i den nuværende brugers kontekst.

* UserName, Password og Domain skal være udfyldt, såfremt Impersonate er sat til False

Når Impersonate sættes til False skal der angives brugernavn, password og domain på en bruger med Domain Administrator-rettigheder.

* default\_federation\_partner i afsnittet appSettings

I ADFS-konfigurationen er denne sat til ’https://log-in.miljoeportal.dk/runtime/’, denne værdi angiver en Identifier på en Relying Party i ADFS konfigurationen.

* AD\_attribute\_mapping i afsnittet appSetting

I ADFS-konfigurationen er denne sat til ’AD-attributmapninger’,

Denne værdi benyttes til at navngive en LDAP Claim Rule på den som oprettes på

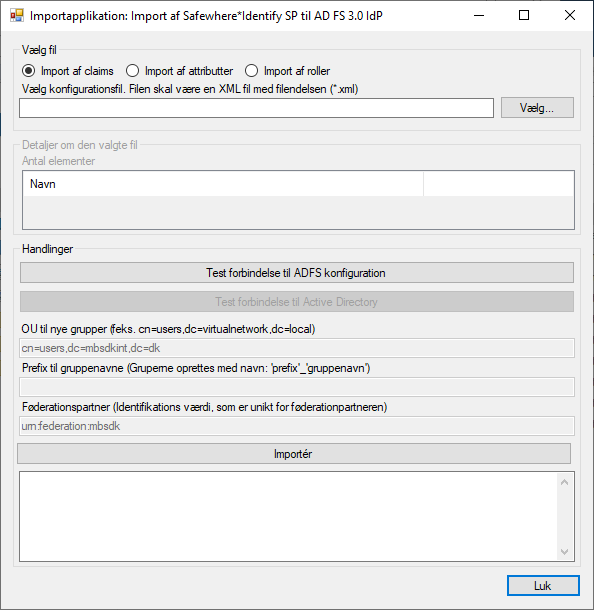
den specificerede Relying Party i forbindelse med imort af attributter.

* default\_role\_claim\_type i afsnittet appSettings

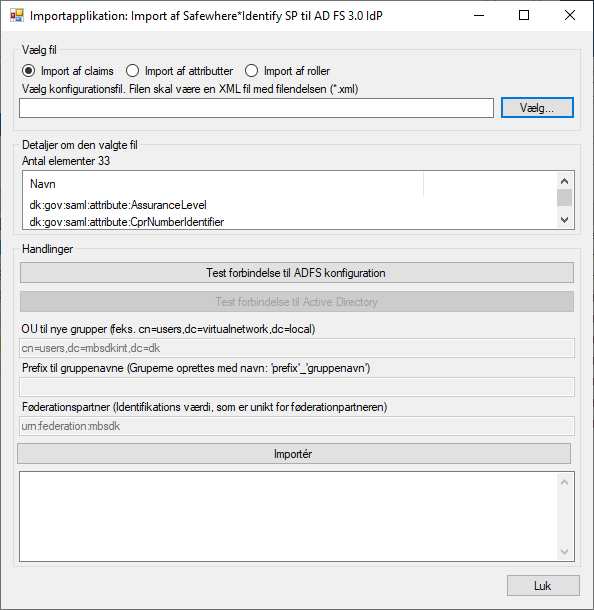
I ADFS-konfigurationen er denne sat som standard til ’http://www.miljoeportal.dk/roles’, Denne URL værdi anvendes i forbindelse med import af roller, når en gamle version af rollefilen anvendes. URL'en kan om nødvendigt tilrettes således at den peger på en Claim Description (ClaimType), som erstatter ’http://schemas.xmlsoap.org/claims/Group’ Claim Type'n, der ellers ville være blevet anvendt.

# Brug af ADFS-importapplikationen til import af claims

1. Start importapplikationen. Når applikationen er startet bør der vises dette programvindue:



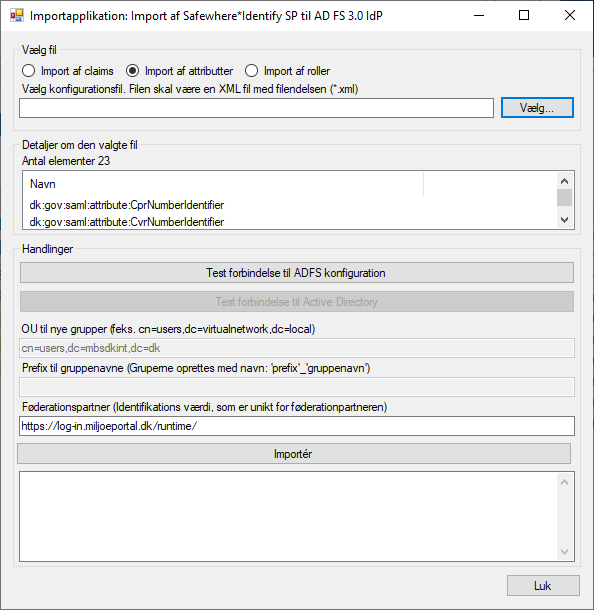
1. Vælg ”Import af claims” og tryk på ”Vælg…”-knappen ude til højre og udpeg den claimfil, som er rekvireret fra DMP central brugerstyring. Når filen er indlæst vil listen med claims blive populeret som vist på billedet nedenfor.



1. Brug testknappen til at validere at applikationen kan få kontakt med ADFS-konfigurationen.
2. Når testen er gennemført med succes trykkes der på ”Importér”-knappen”. Ved tryk på denne knap påbegyndes import-operationen mod ADFS-konfigurationen.
3. Under operationen vil applikationen løbende angive status i tekstfeltet i bunden af applikationen.
   1. Hvis applikationen melder om fejl eller ikke fortæller at den har oprettet de ønskede AD-attributmapninger og/eller ADFS Claim Rule, så bør du huske at klippe denne information ud og gemme den til brug for den efterfølgende fejlfinding.

# Brug af ADFS-importapplikationen til import af attributter

1. Redigér applikationens konfigurationsfil (se afsnittet ”Konfiguration af ADFS-importapplikationen”) således at den peger på partnerorganisationens Active Directory samt om nødvendigt angiver en bruger med Domain Administrator-rettigheder.
2. Start importapplikationen. Når applikationen er startet bør der vises dette programvindue:

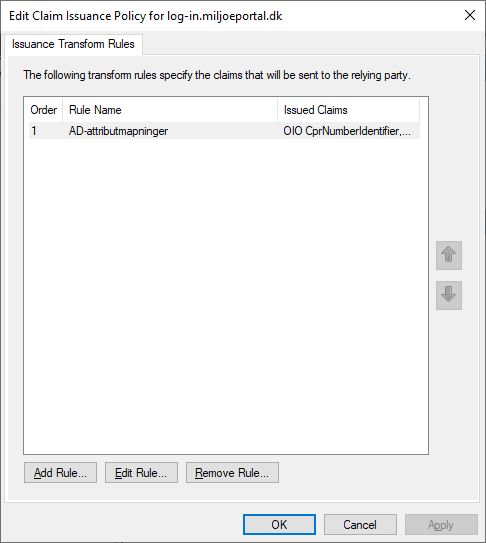


1. Vælg ”Import af attributter” og tryk på ”Vælg…”-knappen ude til højre og udpeg den attributfil, som er rekvireret fra DMP central brugerstyring. Når filen er indlæst vil listen med attributter blive populeret som vist på billedet nedenfor og ”Føderationspartner” feltet vil blive udfyldt med værdien fra ADFS-konfigurationen, der er autoudfyldt med identifikationsværdien på den relevante føderationspartner (hvilket i denne sammenhæng er DMP, som har det unikke identifikations værdi https://log-in.miljoeportal.dk/runtime/).

1. Brug testknappen til at validere at applikationen kan få kontakt med ADFS-konfigurationen.
2. Når testen er gennemført med succes trykkes der på ”Importér”-knappen”. Ved tryk på denne knap påbegyndes import-operationen mod ADFS-konfigurationen.
3. Under operationen vil applikationen løbende angive status i tekstfeltet i bunden af applikationen.
   1. Hvis applikationen melder om fejl eller ikke fortæller at den har oprettet de ønskede AD-attributmapninger og/eller ADFS Claim Rule, så bør du huske at klippe denne information ud og gemme den til brug for den efterfølgende fejlfinding.

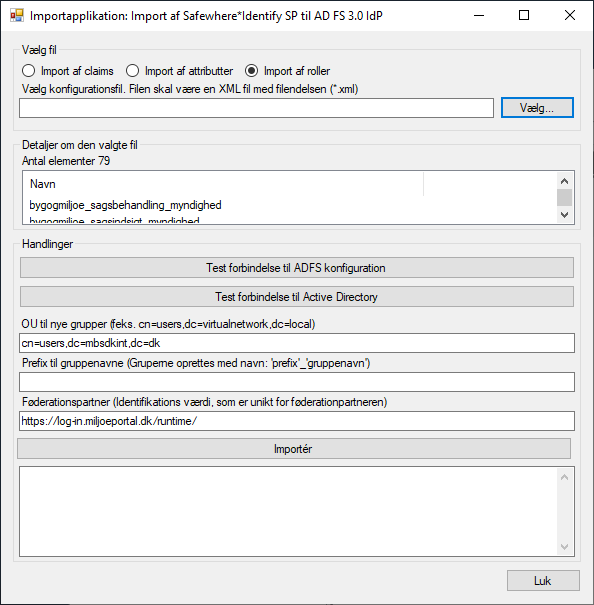
Bemærk at værktøjet overskriver indholdet af en evt. tidligere version af "AD-Attributmapninger" LDAP claim rule!

Hvis det er første gang du kører importapplikationen vil den første claims rule i ”Edit Claim Issuance Policy…” nu være oprettet på login.miljoeportal.dk Relying Party'en:



# Brug af ADFS-importapplikationen til import af roller

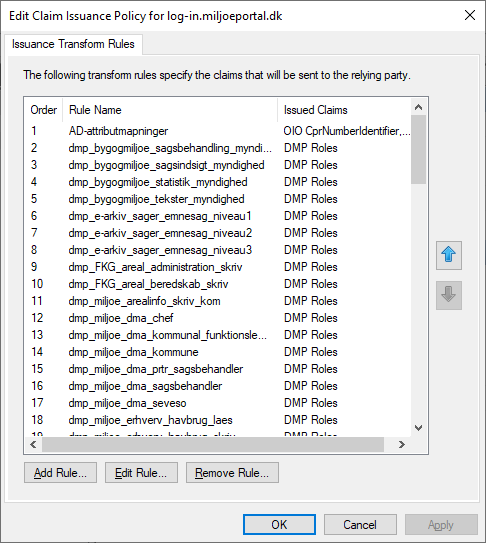
1. Det formodes at applikationens konfigurationsfil allerede er redigeret (se afsnittet ”Konfiguration af ADFS-importapplikationen”) således at den peger på partnerorganisationens Active Directory samt om nødvendigt angiver en bruger med Domain Administrator-rettigheder og importapplikationen er startet.
2. Vælg ”Import af roller” og tryk på ”Vælg…”-knappen ude til højre og udpeg den gruppefil, som er rekvireret fra DMP central brugerstyring. Når filen er indlæst vil listen med grupper blive populeret som vist på billedet nedenfor.



1. Indtast DN (distinguished name) på den OU, som brugerne skal oprettes i.
   1. Husk at egenoprettede OU’er altid adresseres OU=<*navn\_på\_OU*>, hvorimod Active Directory’s prædefinerede containers (Users, Computers og Builtin) skal adresseres CN=<*navn\_på\_container*>.
2. Indtast evt. et prefix til grupperne der oprettes i Active Directory.
3. Brug de to testknapper til at validere at applikationen kan få kontakt med både ADFS-konfigurationen og en Active Directory DC.
   1. Bemærk evt. at testen af forbindelsen til Active Directory fejler, hvis ikke ”OU til nye grupper”-feltet er udfyldt.
4. Når de to tests er gennemført med succes trykkes der på ”Importér”-knappen. Ved tryk på denne knap påbegyndes import-operationen mod Active Directory og ADFS-konfigurationen..
5. Under operationen vil applikationen løbende angive status i tekstfeltet i bunden af applikationen.
   1. Hvis applikationen melder om fejl eller ikke fortæller at den har oprettet de ønskede Active Directory-grupper og/eller ADFS claim rule, så bør du huske at klippe denne information ud og gemme den til brug for den efterfølgende fejlfinding.

Bemærk at værktøjet overskriver evt. ændringer af de claim rules for grupperne, som tidligere er blevet oprettet af importværktøjet!

Hvis det er første gang du kører importapplikationen vil der nu være oprettet væsentligt flere claims rules på login.miljoeportal.dk Relying Party'en:



# Tilretning af claims i overensstemmelse med organisationens behov

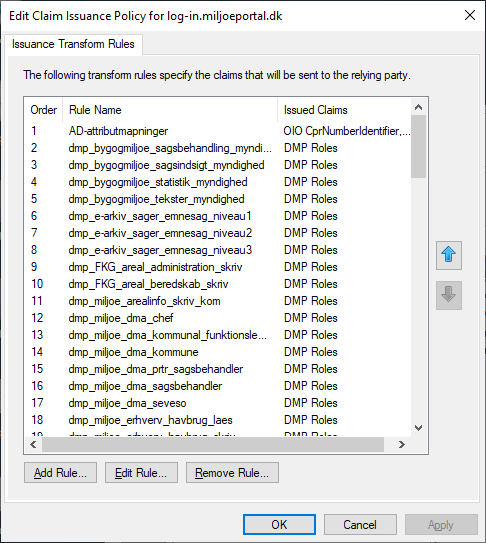
Det er nødvendigt at tilføje to håndfulde claims efter afviklingen af importapplikationen for at organisationens har fået etableret det komplette sæt af claims til brug for alle applikationerne i Danmarks Miljøportal.

## Oprettelse af avancerede claims

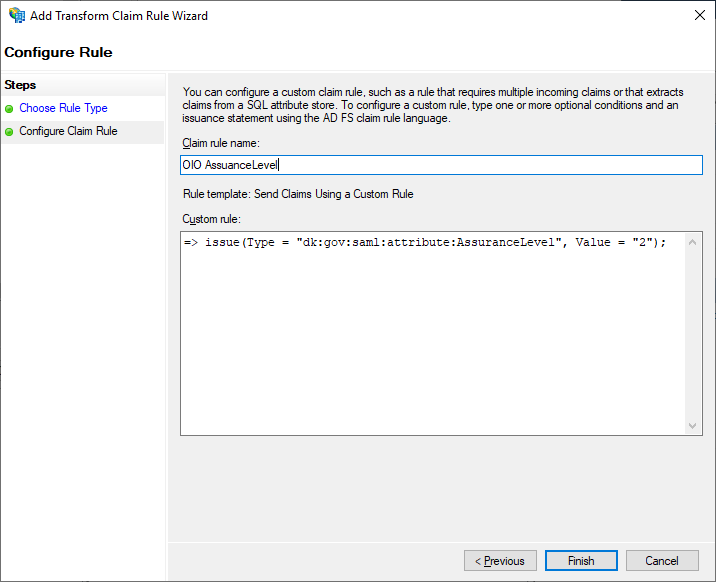
OIO SAML rummer fire claims (OIO AssuranceLevel, OIO SpecVer og OIO Postal Address), som nødvendigvis må håndteres separat på grund af deres egenart.

Det er vist nedenfor, hvordan disse fire claims skal oprettes samt hvor de skal placeres i rækkefølgen.

Bemærk i øvrigt at nogle af de fire claims-værdier kan vise sig at skulle justeres afhængig af organisationen.



Opret en custom claim rule kaldet OIO AssuanceLevel



Kopier følgende, så det ligner ovenstående billede:

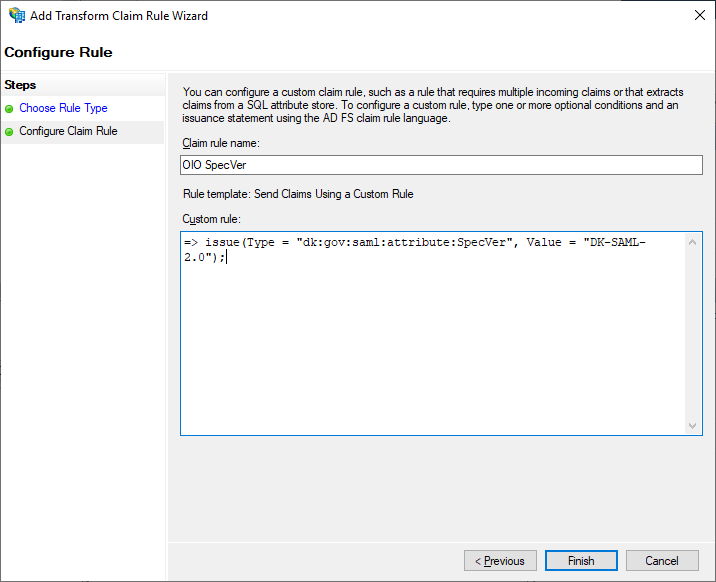
*Claim rule name:*

OIO AssuranceLevel

*Custom rule*:

=> issue(Type = "dk:gov:saml:attribute:AssuranceLevel", Value = "2");

Opret en custom claim rule kaldet OIO SpecVer



Kopier følgende, så det ligner ovenstående billede:

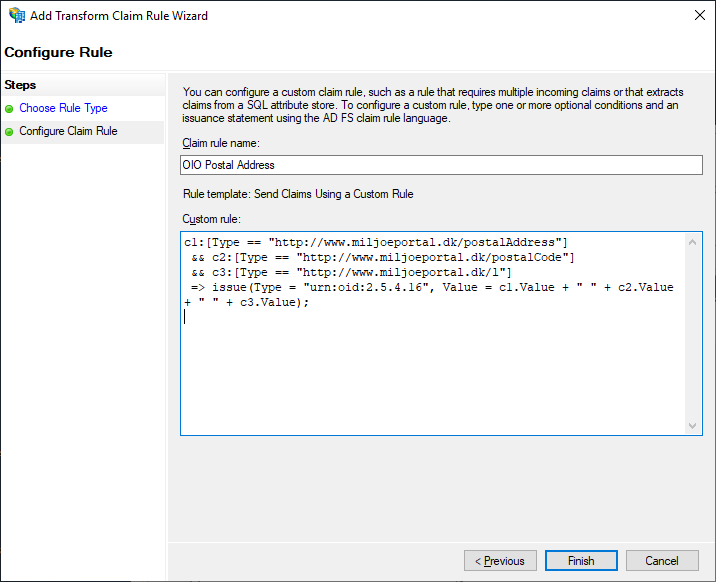
*Claim rule name:*

OIO SpecVer

*Custom rule*:

=> issue(Type = "dk:gov:saml:attribute:SpecVer", Value = "DK-SAML-2.0");

Opret en custom claim rule kaldet OIO Postal Address



Kopier følgende, så det ligner ovenstående billede:

*Claim rule name:*

OIO Postal Address

*Custom rule*:

c1:[Type == "http://www.miljoeportal.dk/postalAddress"]

&& c2:[Type == "http://www.miljoeportal.dk/postalCode"]

&& c3:[Type == "http://www.miljoeportal.dk/l"]

=> issue(Type = "urn:oid:2.5.4.16", Value = c1.Value + " " + c2.Value + " " + c3.Value);

## Tilpasning af claims, der er unikke for hver enkelt organisation

Løsningen opererer derudover med fem claims (cvrNumberIdentifier, organizationNumber, OrganizationName, PNumberIdentifier og sourceIPAddresses), som er unikke hos hver organisation.

Det er forskelligt hvor mange af disse fem claims, der skal være udfyldt (det afhænger dels af organisationen og dels af hvilke applikationer, der benyttes). DMP stiller dog som krav at de to førstnævnte claims skal være tildelt en værdi.

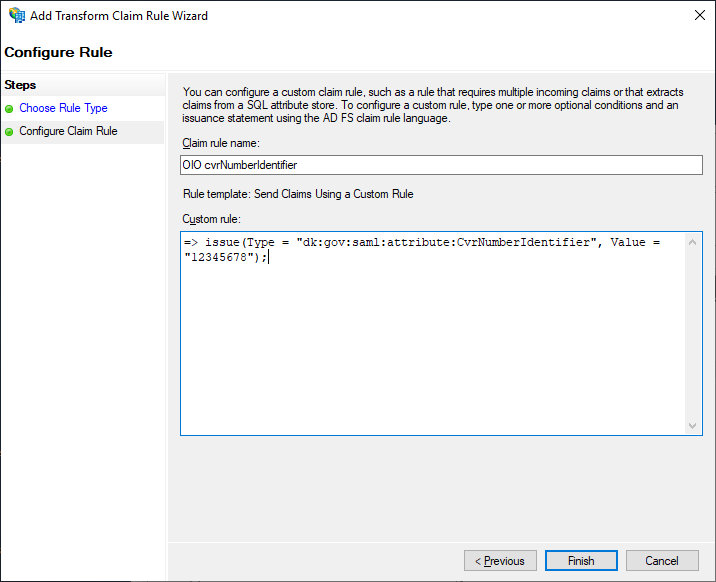
Tildelingen af en værdi til de relevante claims kan fx håndteres ved at lægge de relevante informationer ned i en AD-attribut og oprette de nødvendige LDAP claims rules eller placere informationerne andetsteds og oprette en custom attribute store. Disse to løsninger er nødvendige, hvis claims-værdierne kan være forskellige på tværs af brugerne i organisationens Active Directory.

Såfremt værdierne er de samme for alle Active Directory-brugere kan det håndteres ved at oprette nogle custom rules, der sætter en given claim til en fast værdi.

*Når du sætter en given attribut (fx cvrNumber, employeeNumber eller sourceIPAddresses) til en fast værdi ved brug af en custom rule på DMP Relying Party Trust'en skal du huske at checke om der findes en tilsvarende mapping i Attributmapninger til DMP. Denne skal i givet fald slettes. Ellers vil din custom rule ikke fungere.*

En løsning baseret på faste claims-værdier er eksemplificeret nedenfor i forbindelse med cvrNumberIdentifier, organizationNumber og sourceIPAddresses claims:

Opret en custom claim rule kaldet OIO cvrNumberIdentifier



Kopier følgende, så det ligner ovenstående billede(dog skal 12345678 erstattes med jeres egen værdi):

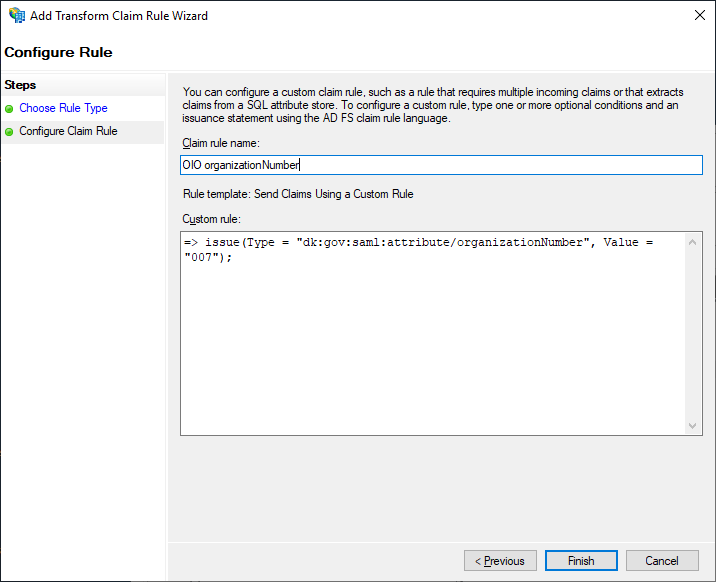
*Claim rule name:*

OIO cvrNumberIdentifier

*Custom rule*:

=> issue(Type = "dk:gov:saml:attribute:CvrNumberIdentifier", Value = "12345678");

Opret en custom claim rule kaldet OIO organizationNumber



Kopier følgende, så det ligner ovenstående billede(dog skal 007 erstattes med jeres egen værdi):

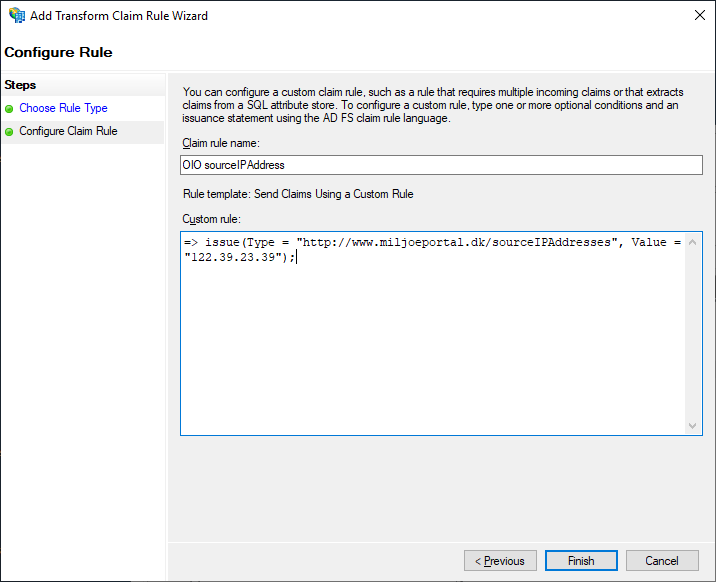
*Claim rule name:*

OIO organizationNumber

*Custom rule*:

=> issue(Type = "dk:gov:saml:attribute/organizationNumber", Value = "007");

Opret en custom claim rule kaldet OIO sourceIPAddress



Kopier følgende, så det ligner ovenstående billede(dog skal 122.39.23.39 erstattes med jeres egen værdi):

*Claim rule name:*

DMP sourceIPAddresses

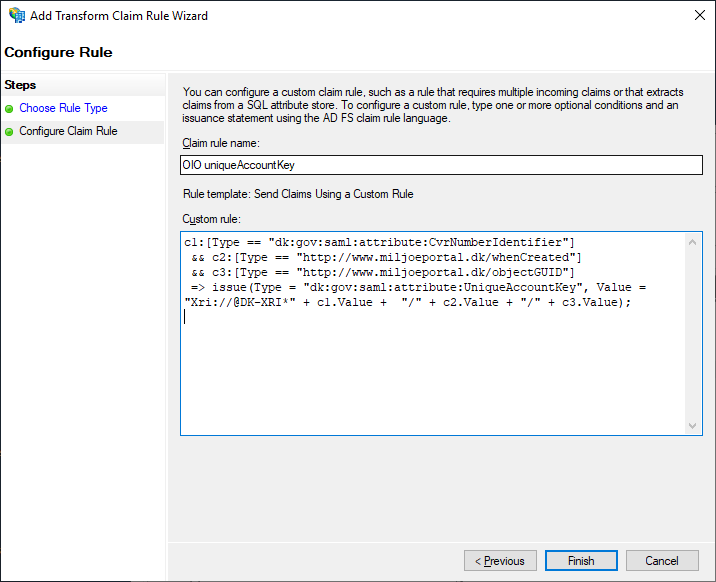
*Custom rule*:

=> issue(Type = "http://www.miljoeportal.dk/sourceIPAddresses", Value = "122.39.23.39");

## Oprettelse af speciel claim

Hvis der skal være sikkerhed for at single logout fungerer fra organisationens lokale føderationsserver vil det være nødvendigt at tilføje en UniqueAccountKey og derefter formatere den til en NameID claim rule:

Opret en custom claim rule kaldet OIO uniqueAccountKey



Kopier følgende, så det ligner ovenstående billede:

*Claim rule name:*

OIO uniqueAccountKey

*Custom rule*:

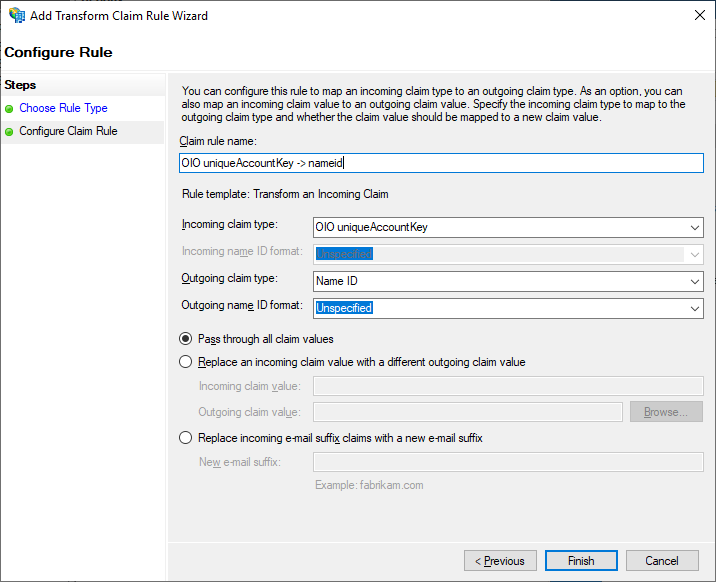
c1:[Type == "dk:gov:saml:attribute:CvrNumberIdentifier"]

&& c2:[Type == "http://www.miljoeportal.dk/whenCreated"]

&& c3:[Type == "http://www.miljoeportal.dk/objectGUID"]

=> issue(Type = "dk:gov:saml:attribute:UniqueAccountKey", Value = "Xri://@DK-XRI\*" + c1.Value + "/" + c2.Value + "/" + c3.Value);

Opret en **Transform** Claim Rule:



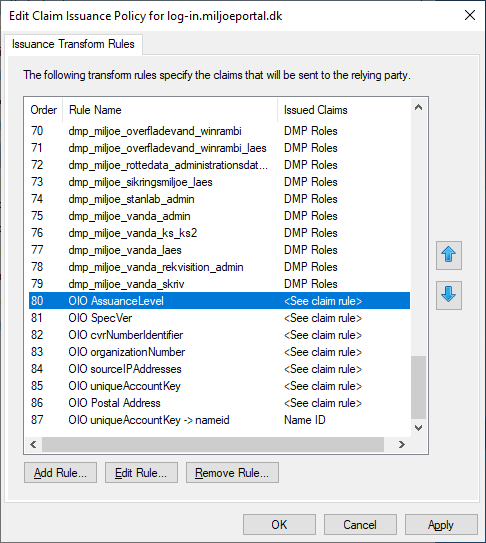
Opsæt følgende, så det ligner ovenstående billede:

*Claim rule name:*

OIO uniqueAccountKey -> nameid

NameID claim rule’n skal blot placeres efter den specielle OIO uniqueAccountKey claim.

Alle tilpassede claims skal indplaceres som vist i rækkefølgen i billedet herunder:



# Aktivering af SSO til web services login på organisationens AD FS 3.0 server

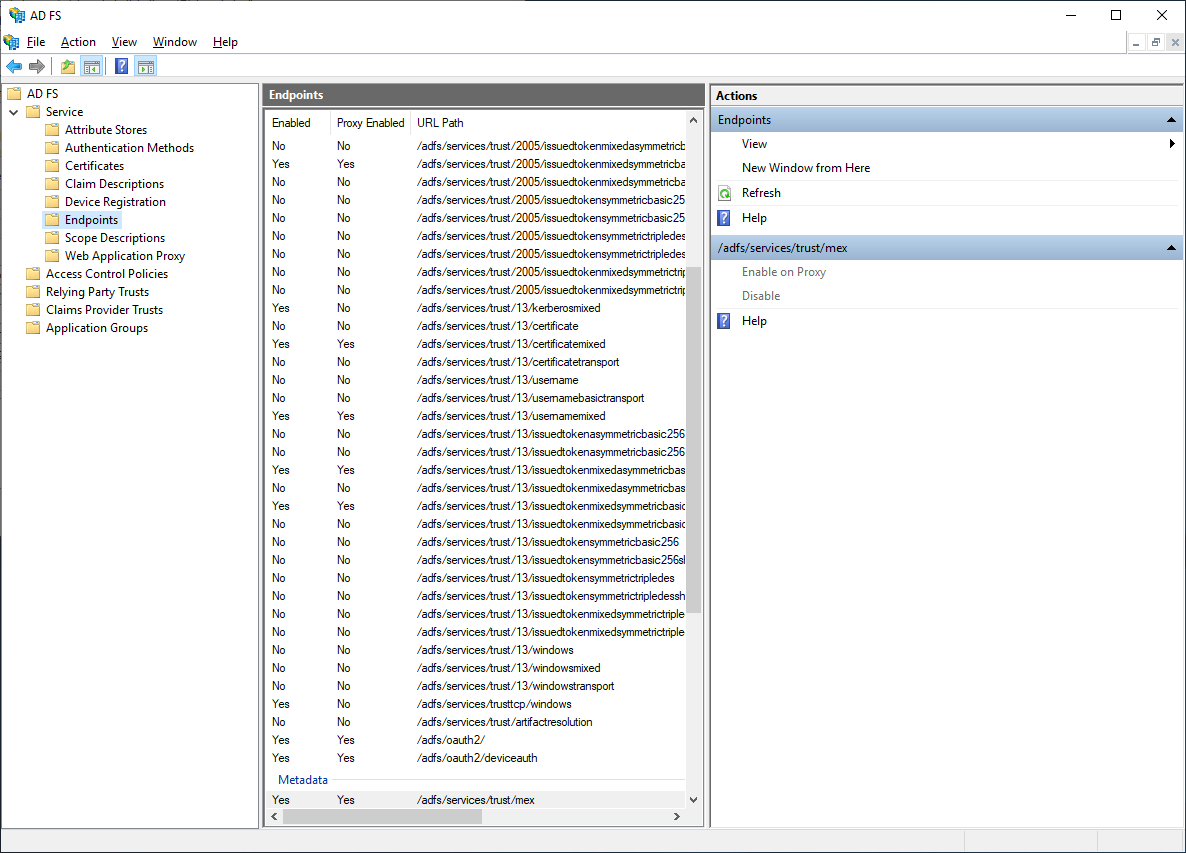
Brugen af SSO til web services kræver to ting på organisationens føderationsserver.

1. Aktivering af et konkret endpoint til web services login
2. Aktivering af kryptering på udstedte tokens

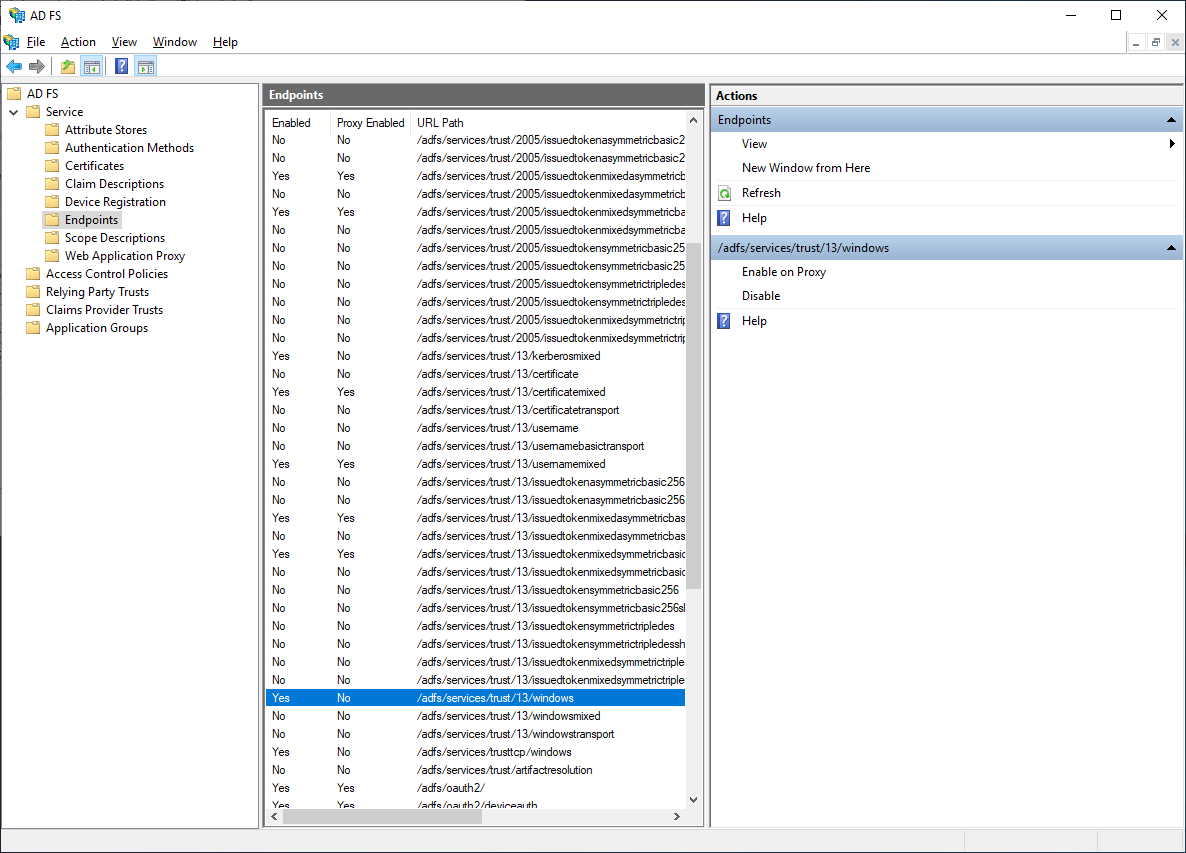
De følgende afsnit beskriver disse punkter i detaljer.

## Aktivering af endpoint til web services login

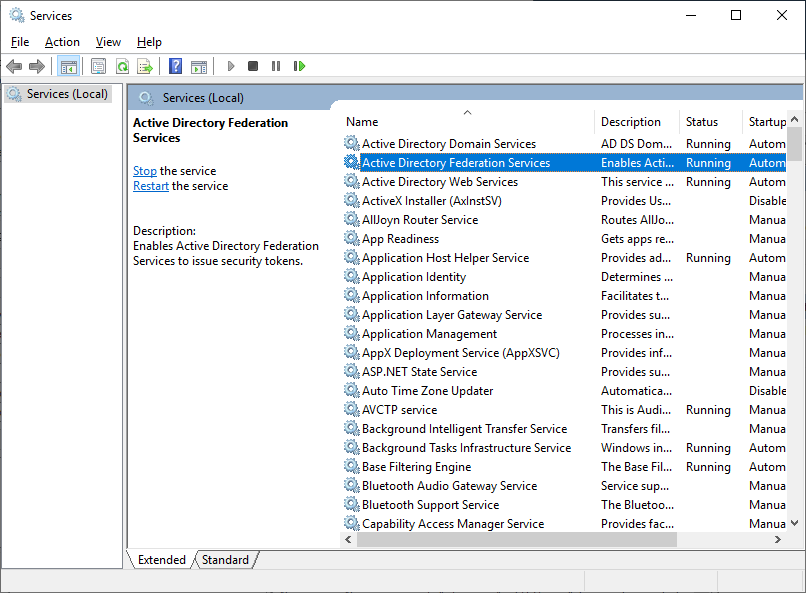
1. Fra AD FS 3.0 MMC’en markeres endpoints



1. Endpointet ”/adfs/services/trust/13/windows” findes i listen



1. Endpointet skal stå til “Enabled”: Yes og “Proxy Enabled”: No. Dette ændres ved at højreklikke på endpointet og vælge Enable.
2. Genstart AD FS 2019 servicen



## Aktivering af kryptering på udstedte tokens

1. Åbn en powershell kommandoboks som administrator på serveren
2. Skriv følgende kommandoer hver efterfulgt af enter.

set-adfsrelyingpartytrust -targetidentifier: "https://log-in.miljoeportal.dk/runtime/" -EncryptClaims:$true