Reindex

Kundevejledning

AD FS opsætning til Reindex

Version: 1.0

Dato: 19. april 2016

Forfatter: Lasse Balsvad (XPERION)

Revisionshistorik

Version	Dato	Initialer	Ændringer
1.0	19-04-2016	LBA	Dokument oprettet

Version	Dato	Initialer	Ændringer
1.1	09-05-2016	HEB	Specific path for customer entry

Reindex

Side

Indholdsfortegnelse

Reindex

Indledning

Dette dokument beskriver, hvordan Reindex oprettes som Relying Party Trust i Microsoft AD FS for, at I kan logge på Reindex systemet ved brug af føderation.

Vigtig information om opkobling til Reindex

Inden du begynder konfigurationen af AD FS ift. at blive koblet på Reindex systemet bør du læse dette afsnit, som sikre en nem opkobling og sparer unødig tid ift. fejlsøgning, hvis I på et tidspunkt udskifter jeres signeringscertifikat.

Send FederationMetadata til Reindex

For at I kan blive sat op i Reindex's systemer til føderation skal I sende jeres FederationMetadata.xml til Reindex. Brug evt. nedenstående procedure.

Alternativt kan I sende et link (URL), hvor jeres metadata-fil er offentligt tilgængelig fra.

Hent FederationMetadata:

1. Log på ADFS serveren
2. Åben en browser og hent filen FederationMetadata.xml fra jeres AD FS løsning.
   Eks: https://adfs.domain.dk/federationmetadata/2007-06/federationmetadata.xml

Kan metadata-filen ikke hentes, skal I kontrollere, at I har slået endpointet for jeres matadata til. Dette kontrolleres i AD FS Management under \AD FS\Service\ Endpoints\ i afsnittet "Metadata". Sørg for endpointet er "Enabled".

Udskiftning af signeringscertifikat

Hvis I planlægger at udskifte jeres signeringscertifikat, er det vigtigt at Reindex får besked på dette, så vi også kan opdatere/udskifte certifikatet i vores løsning. Hvis vi ikke får besked om certifikatskiftet vil login ikke være er muligt, når I udskifter jeres signeringscertifikat.

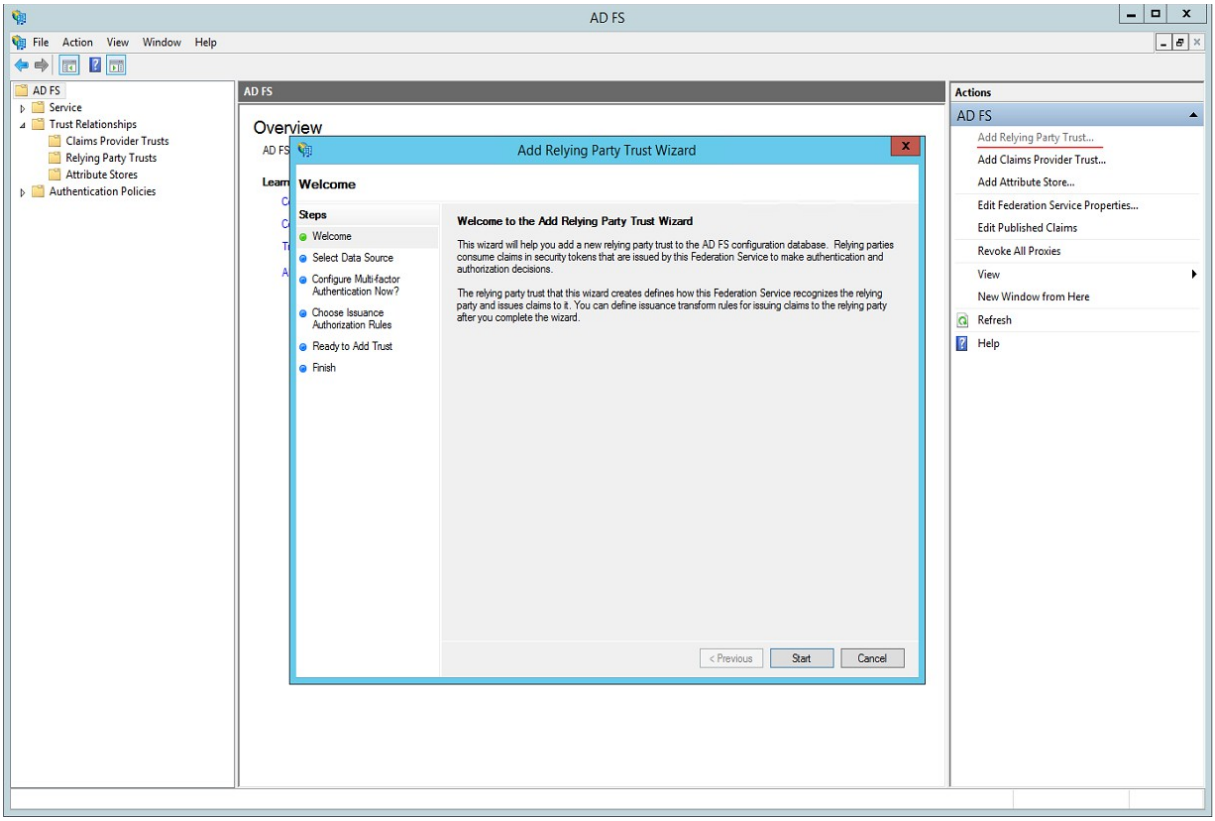
Reindex skal have jeres nye signeringscertifikat min. 5 dage før udskiftning.

Opsætning af Reindex som Relying Party Trust i AD FS

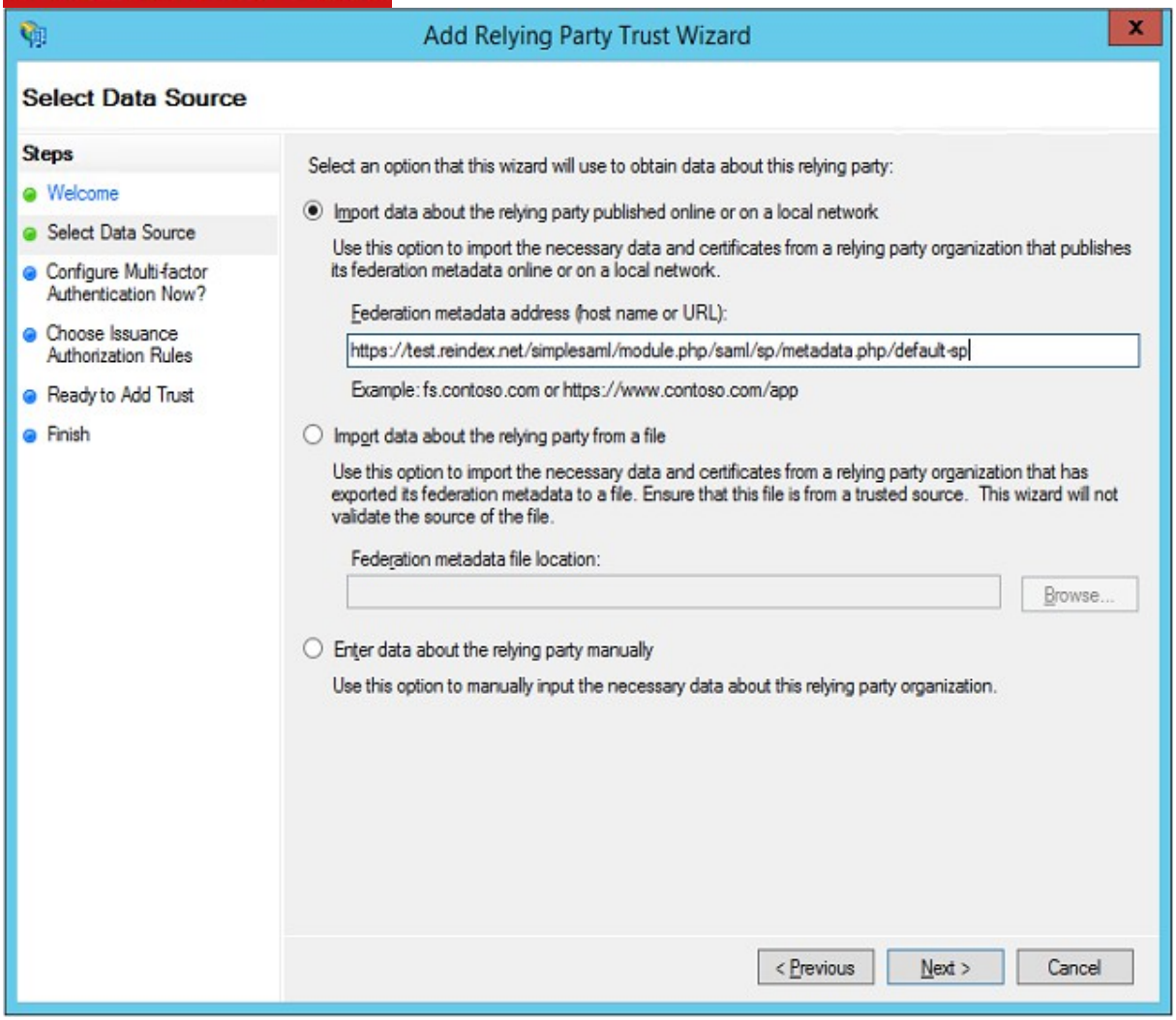
Følgende afsnit beskriver selve opsætningen af Reindex, som relying party trust i AD FS.

Generel opsætning

Åbn AD FS Management Add Relying Party Trust

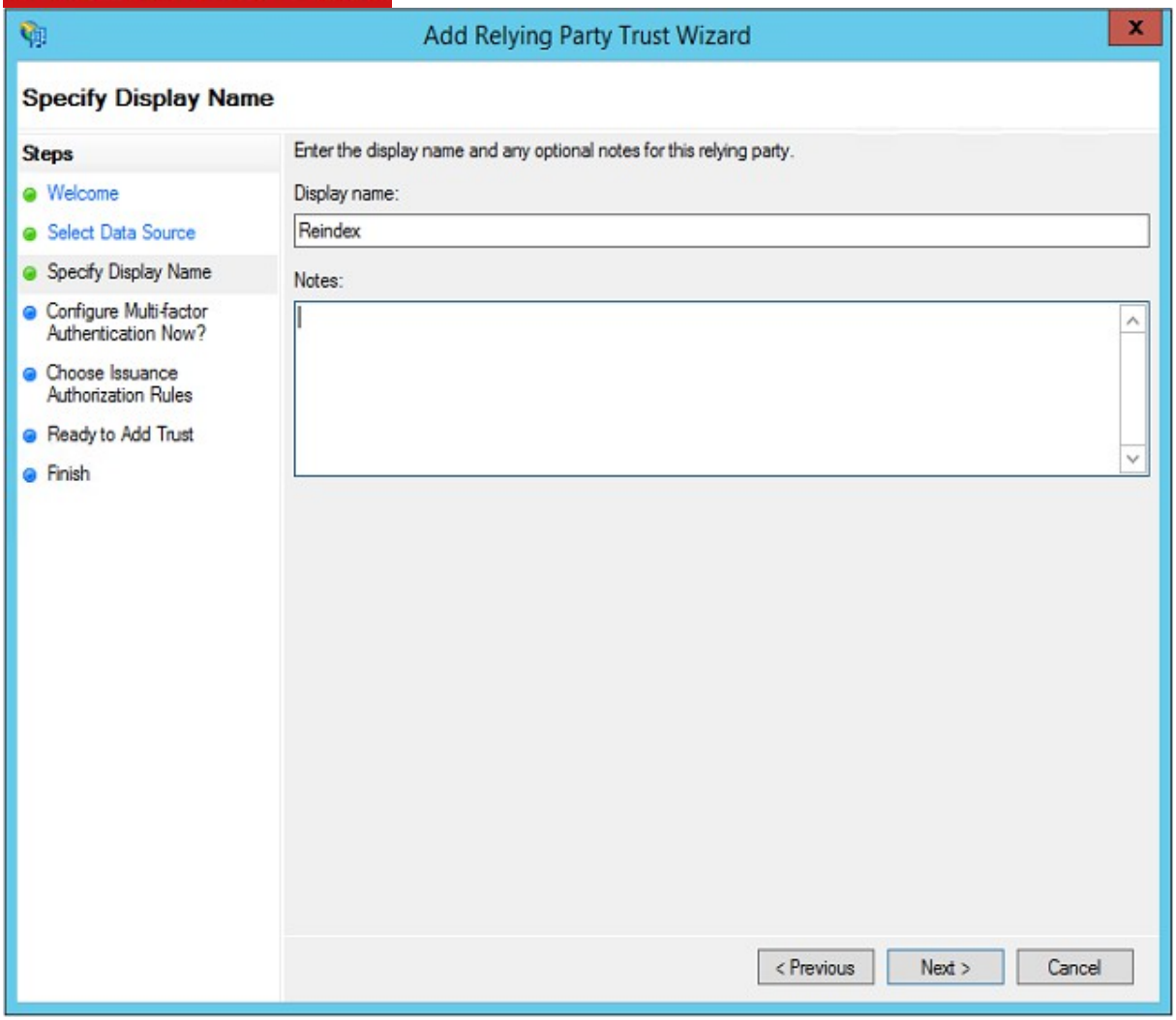


Klik på [**Start**]-knappen i vinduet.



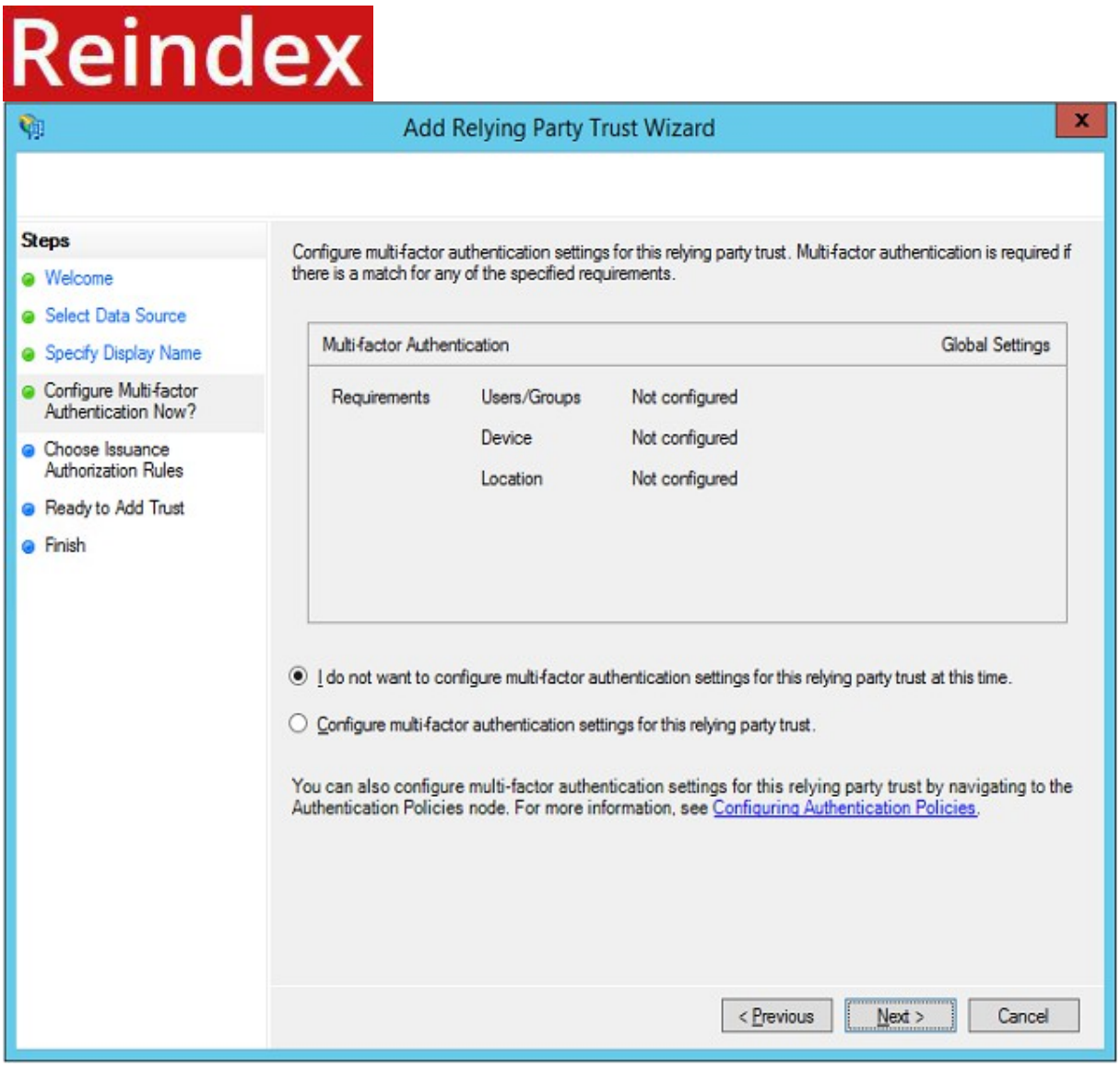
Vælg "**Import data about the relying party published online or on local network**" og indsæt følgende adresse:
https://saml.reindex.net/simplesaml/module.php/saml/sp/metadata.php/default-sp

Klik på [**Next**] -knappen

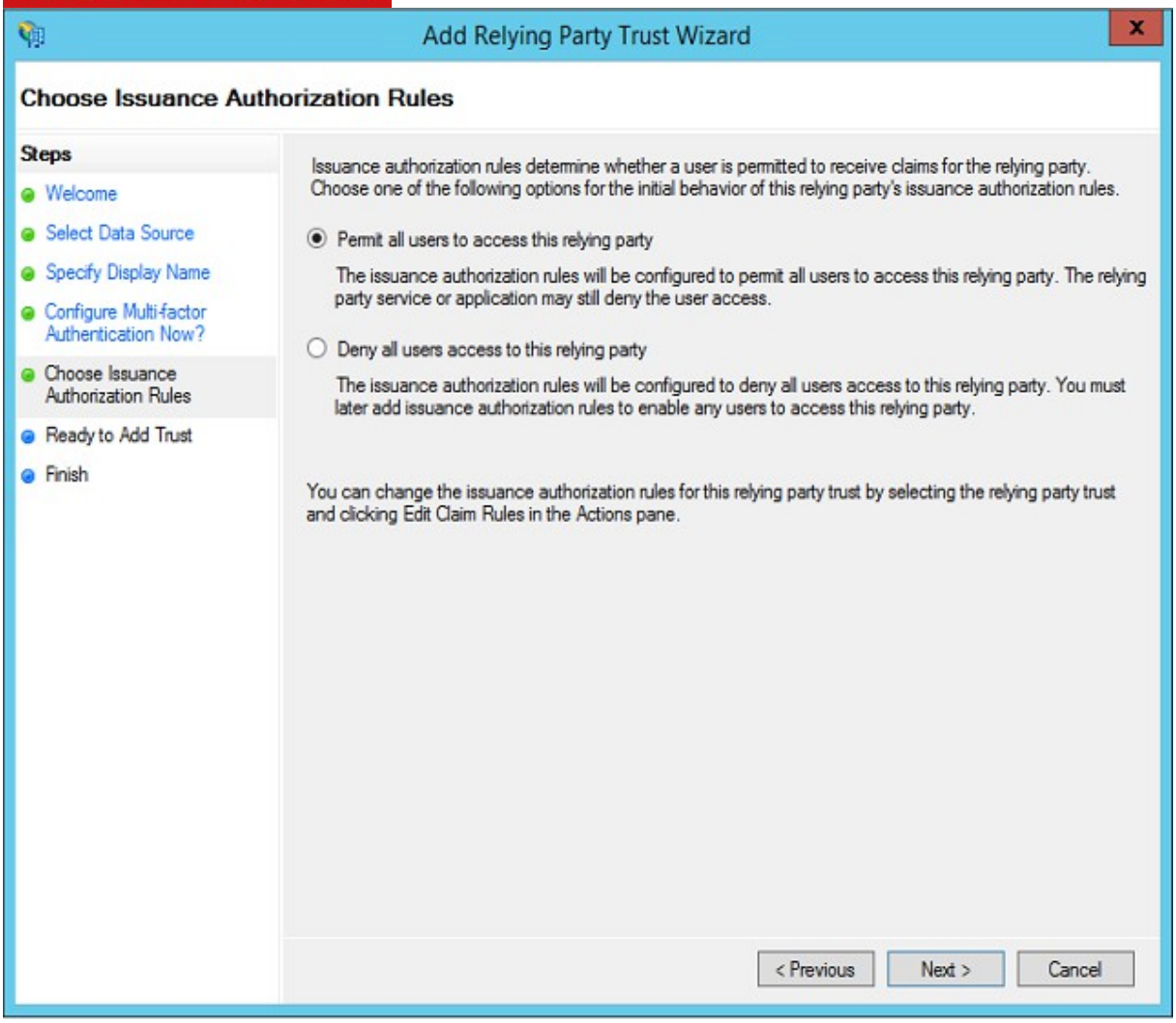


Indtast ”**Reindex**” i feltet for Display name.

Klik på [**Next**]-knappen

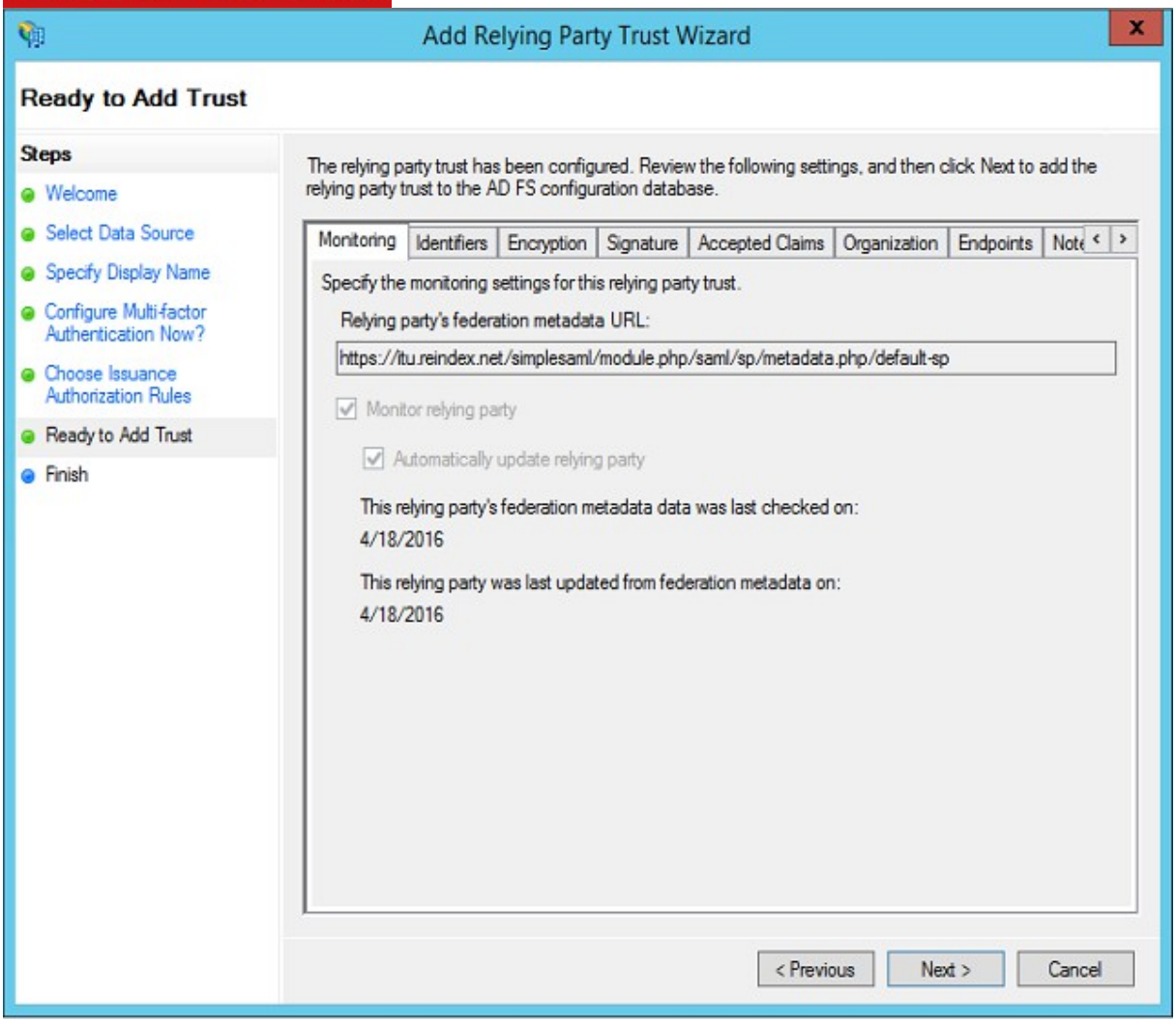


Klik på [**Next**]-knappen

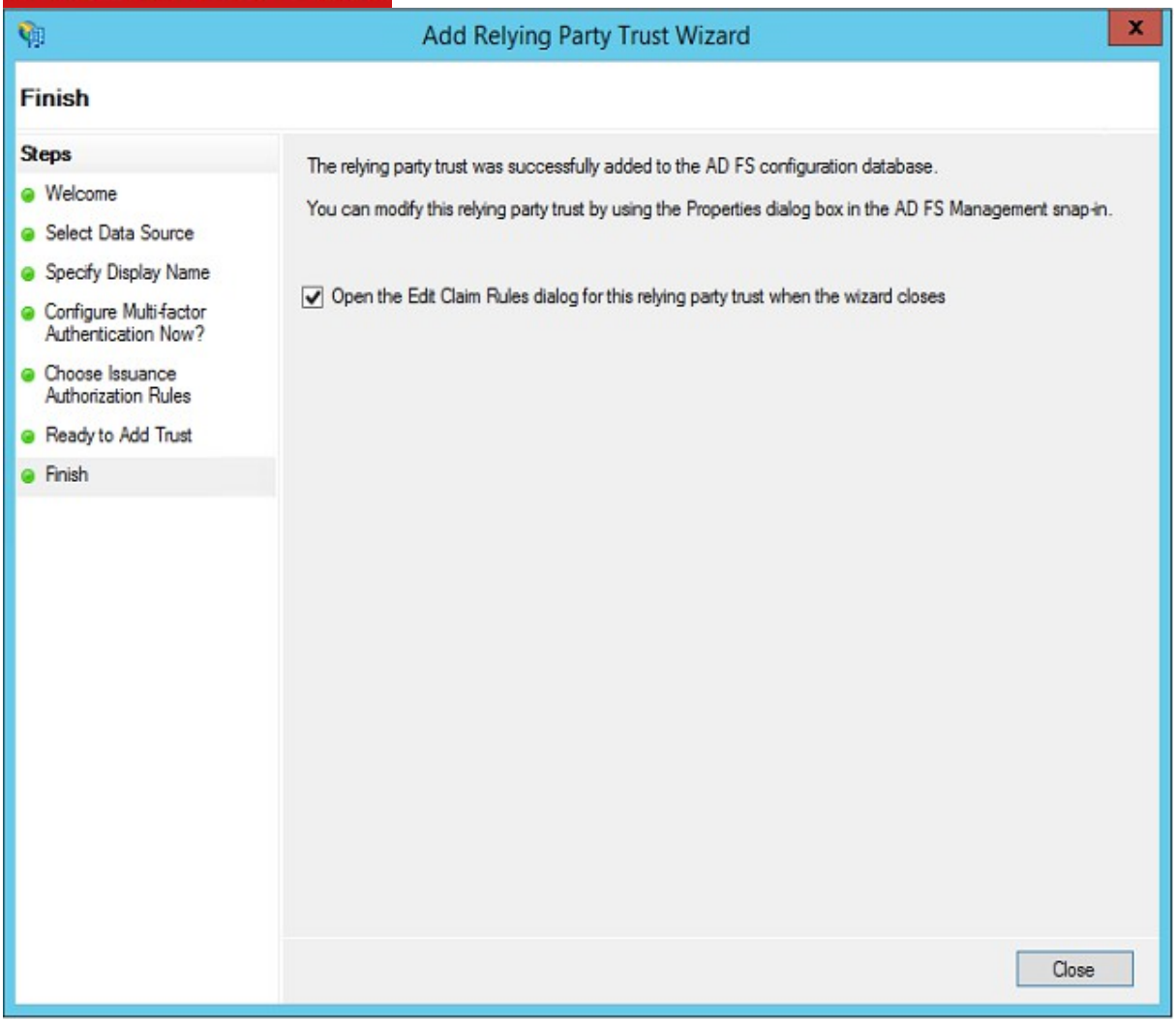


Klik på [**Next**]-knappen

Hvis du senere ønsker at begrænse adgang til forbindelsen for bestemte brugere kan dette opsættes i claim rule vinduet under fanen "Issuance Authorization Rules". Dette er dog ikke beskrevet i denne vejledning.



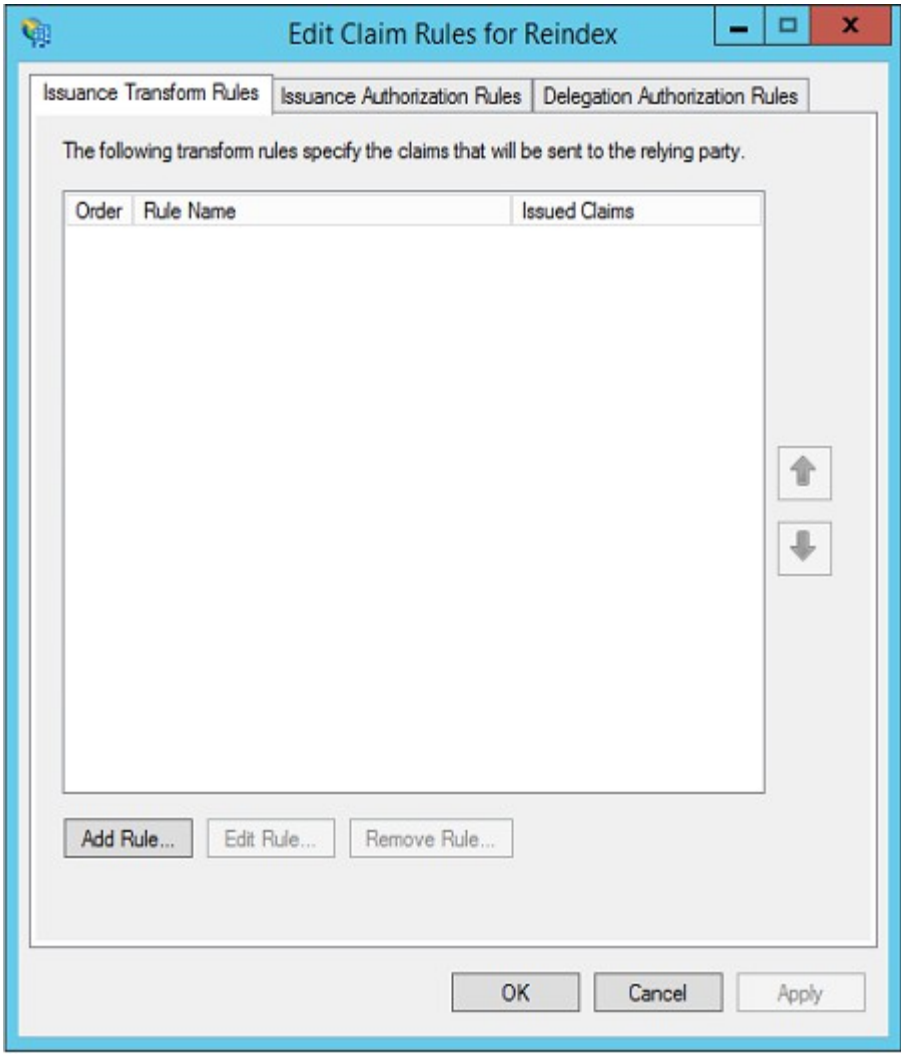
Klik på [**Next**]-knappen



Klik på [**Close**]-knappen

Opsætning af påkrævede Claim Rules

Følgende afsnit beskriver de Claim Rules der er påkrævede for at forbinde til Reindex.

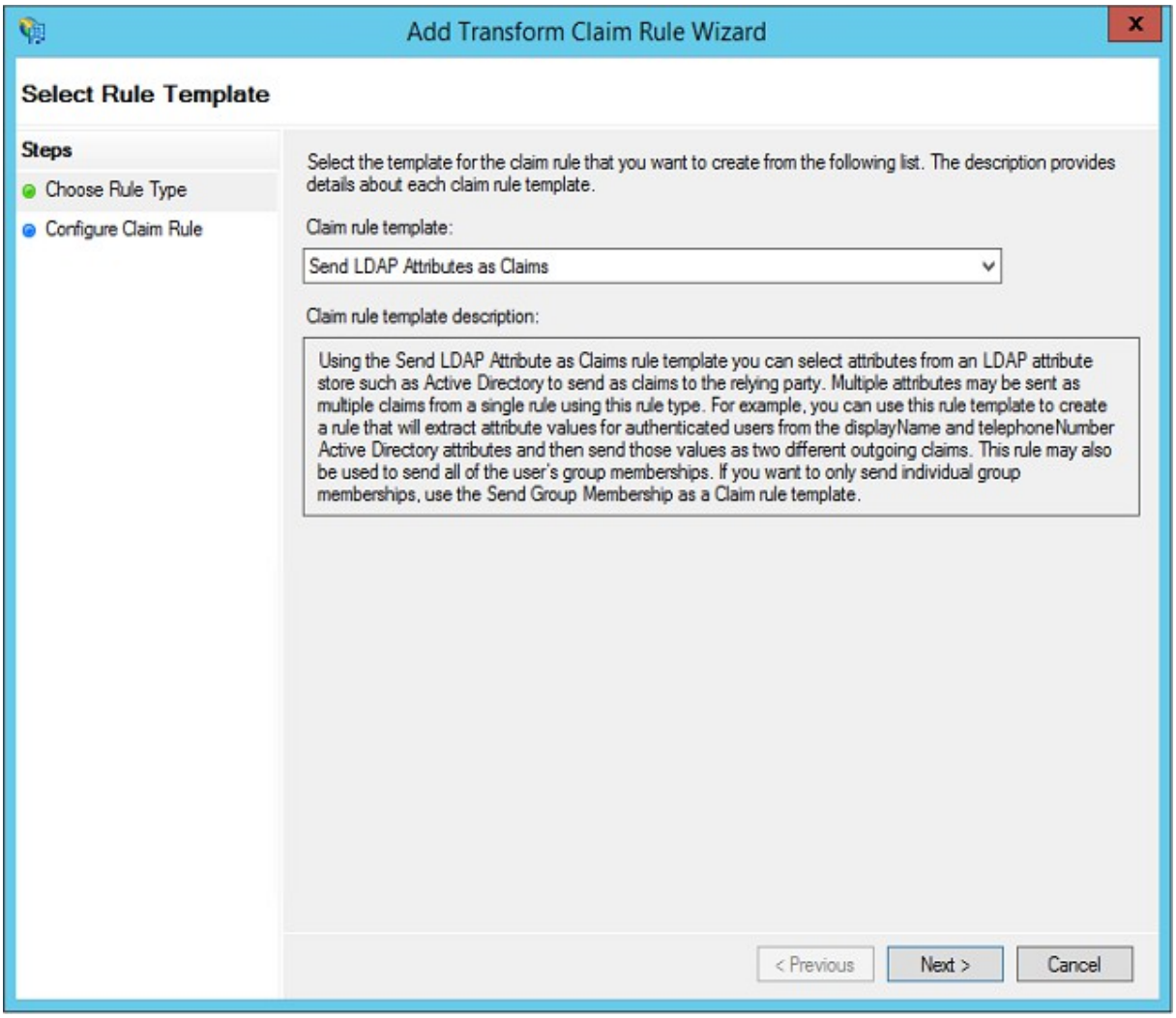


Klik på [**Add Rule…**]-knappen

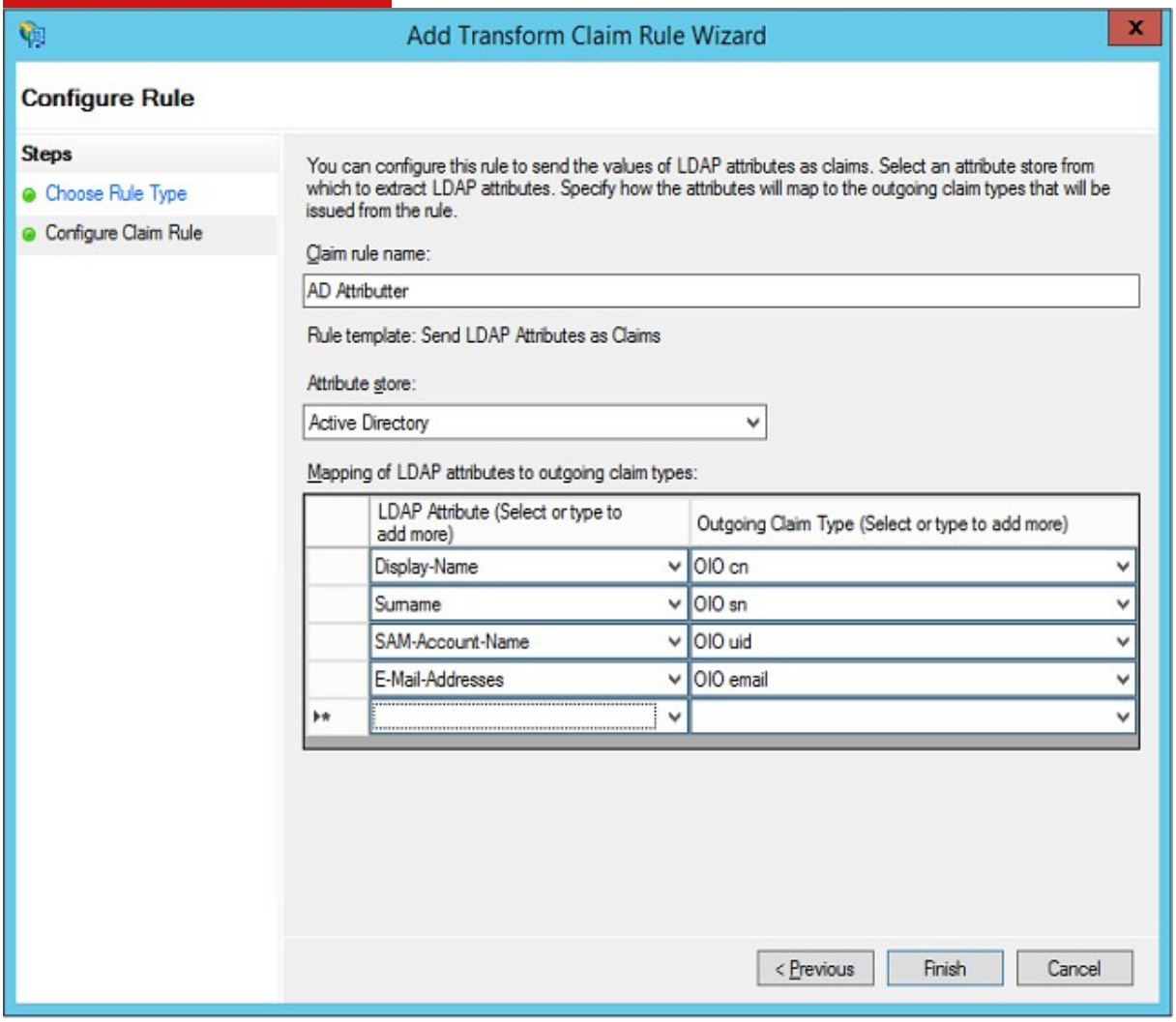
Reindex

Send AD Attributter

Her beskrives hvordan brugeres AD attributter mappes til de påkrævede claimtyper og sendes til Reindex.



Vælg "**Send LDAP Attributes as Claims**" og klik på [**Next**]-knappen.



Da Reindex overholder OIO Web SSO Profile V2.0.9 (OIOSAML 2.0.9) konfigureres LDAP Attribute Store til at levere værdier i nedenstående påkrævede claimtyper.

LDAP Attribut	Påkrævede udgående Claim Type (Navn)
Display-Name	urn:oid:2.5.4.3 (OIO cn)
Surname	urn:oid:2.5.4.4 (OIO sn)
SAM-Account-Name	urn:oid:0.9.2342.19200300.100.1.1 (OIO uid)
E-Mail-Addresses	urn:oid:0.9.2342.19200300.100.1.3 (OIO email)

Er ovenstående claimtyper ikke oprettet I jeres AD FS løsning, så se hvordan de kan indlæses i bilag 1.

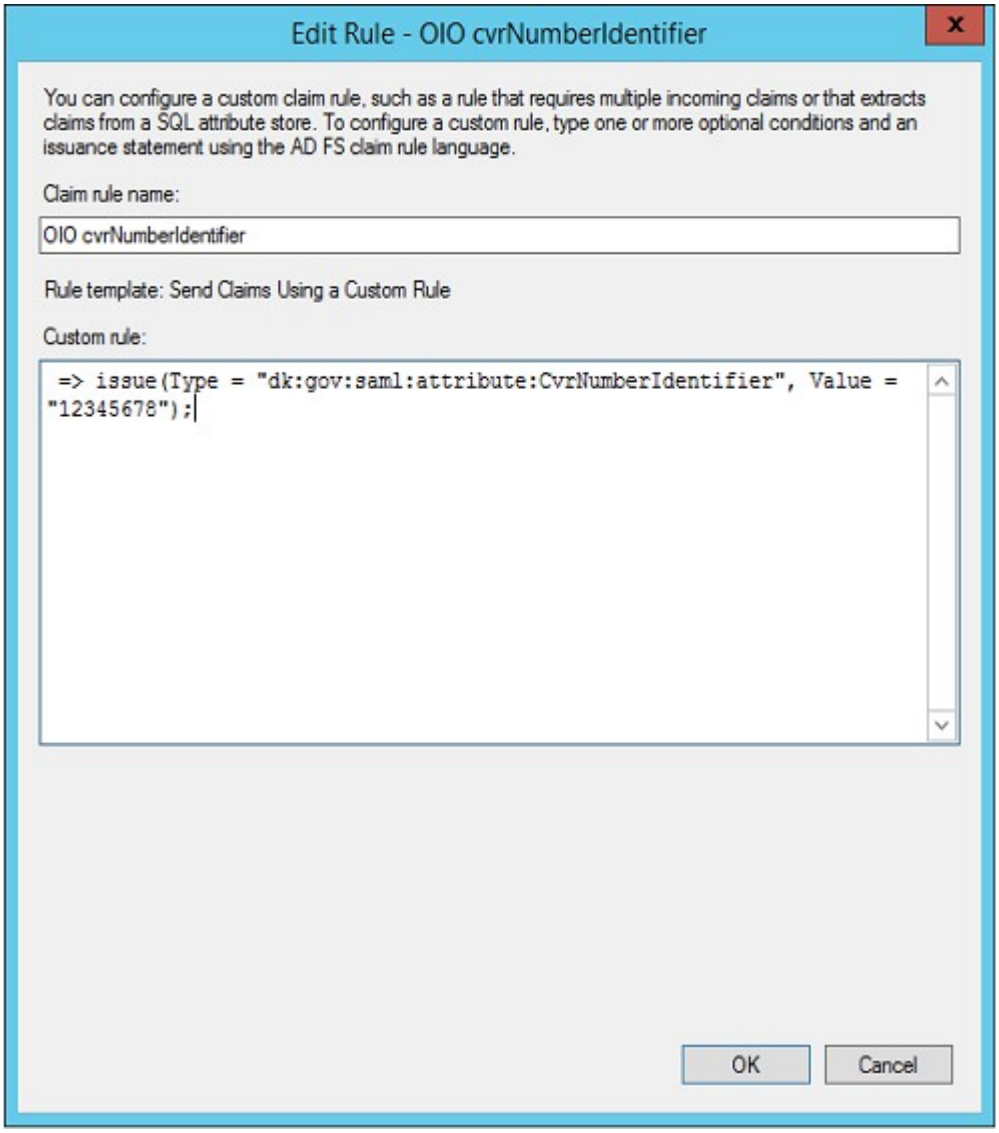
Klik på [**Finish**]-knappen

Reindex

Send CVR-nummer

Her opsættes en claim rule til at sende jeres CVR-nummer.

Klik på [**Add Rule…**]-knappen og vælg ”**Send Claims Using a Custom Rule**”. Klik herefter på [**Next**]-knappen og opsæt nedenstående claim rule.



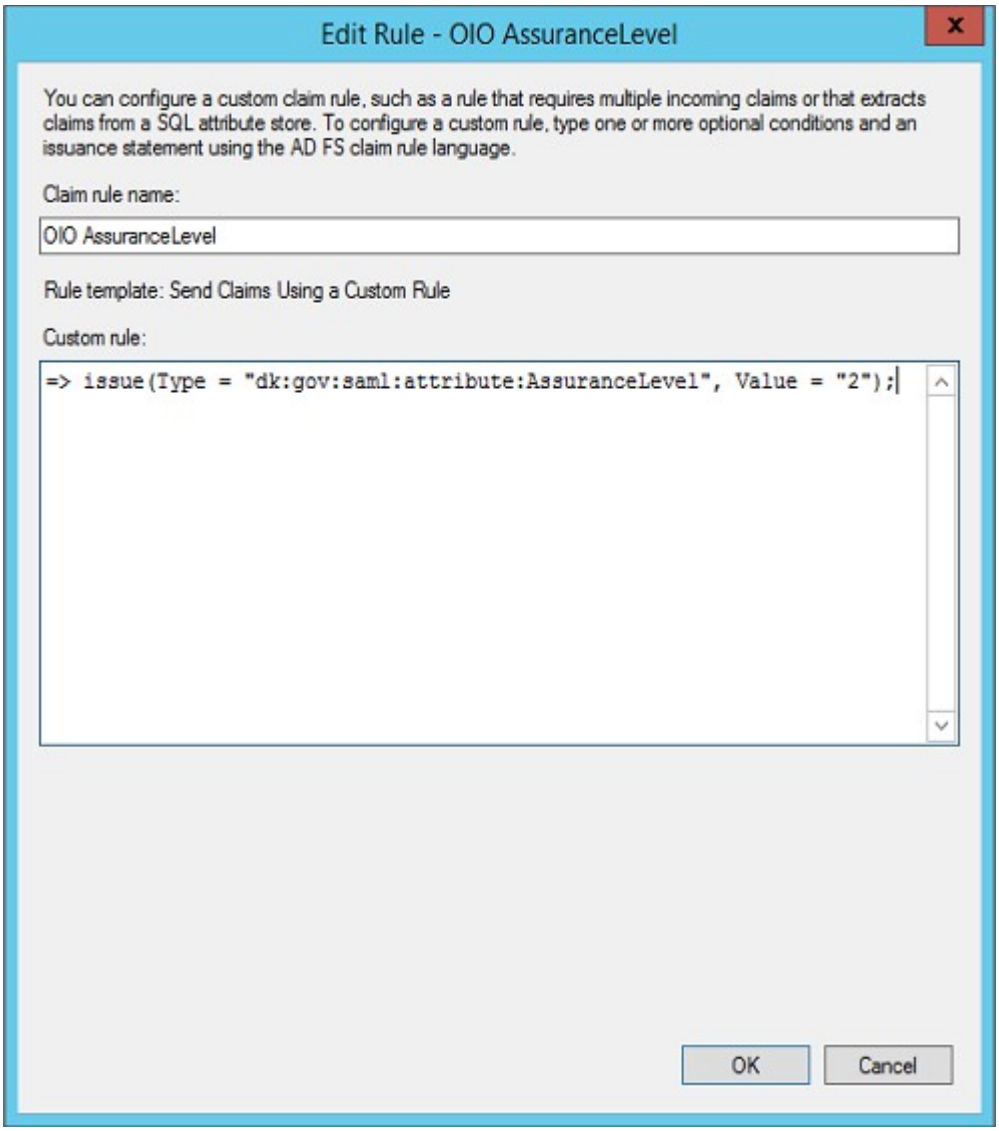
Indtast værdierne:

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

Klik på [**Finish**]-knappen

Send AssuranceLevel

Klik på [**Add Rule…**]-knappen og vælg ”**Send Claims Using a Custom Rule**”. Klik herefter på [**Next**]-knappen og opsæt nedenstående claim rule.



Indtast værdierne:

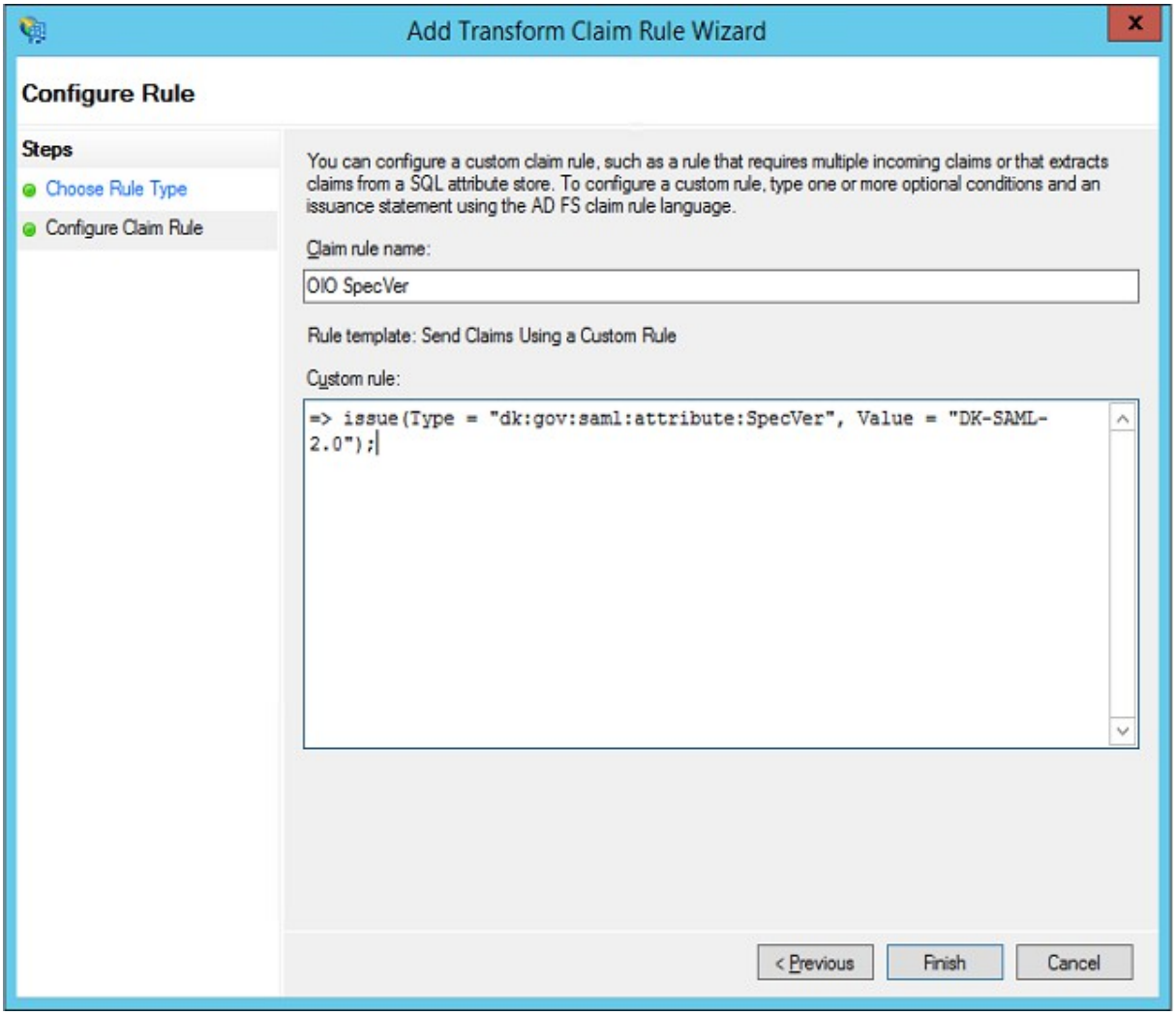
OIO AssuranceLevel
=> issue(Type = "dk:gov:saml:attribute:AssuranceLevel", Value = "2");

Klik på [**Finish**]-knappen

Reindex

Send SpecVer

Klik på [**Add Rule…**]-knappen og vælg "**Send Claims Using a Custom Rule**". Klik herefter på [**Next**]-knappen og opsæt nedenstående claim rule.



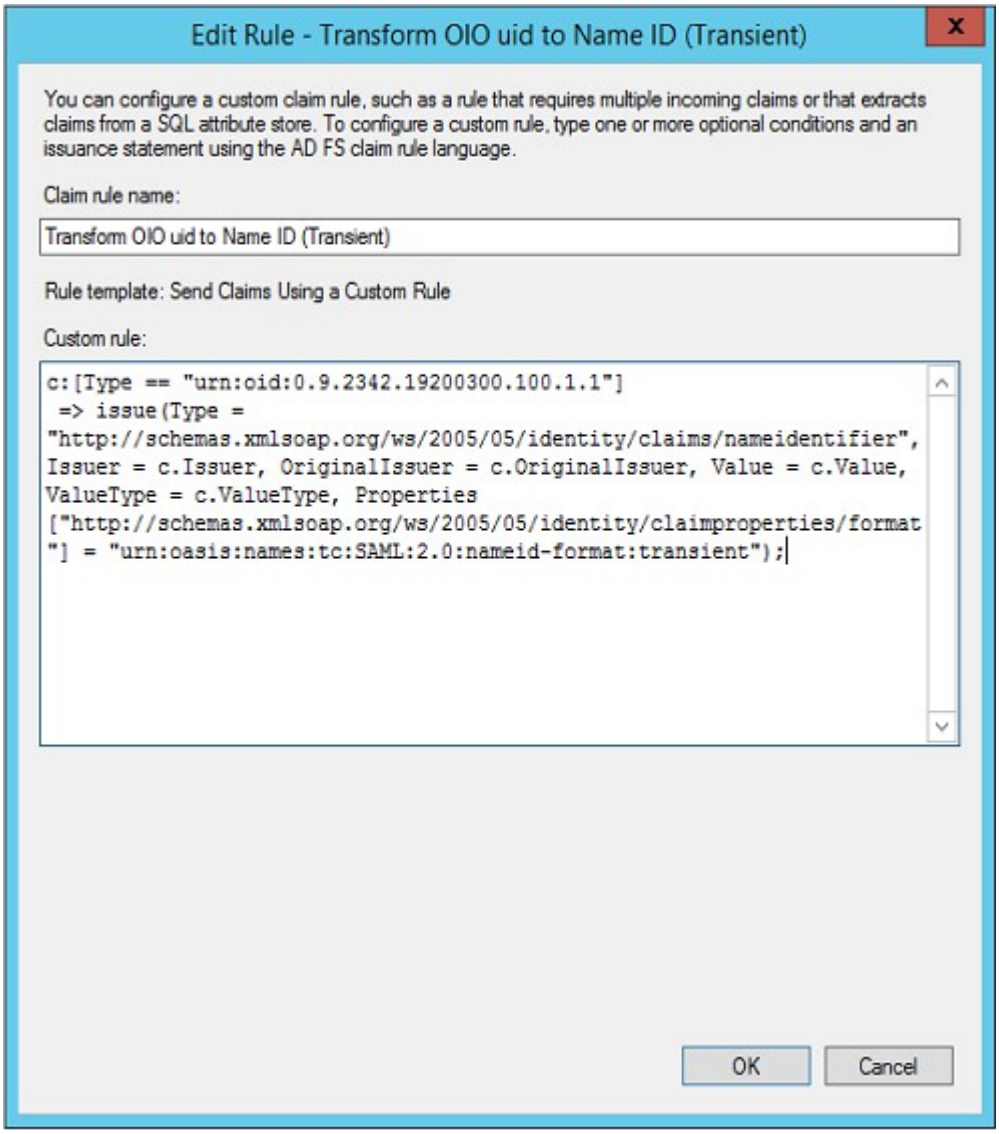
Indtast værdierne:

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

Klik på [**Finish**]-knappen

Send Name ID

Klik på [**Add Rule…**]-knappen og vælg "**Send Claims Using a Custom Rule**". Klik herefter på [**Next**]-knappen og opsæt nedenstående claim rule.



Indtast værdierne:

Transform OIO uid to Name ID (Transient)
c:[Type == "urn:oid:0.9.2342.19200300.100.1.1"] => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");

Klik på [**Finish**]-knappen

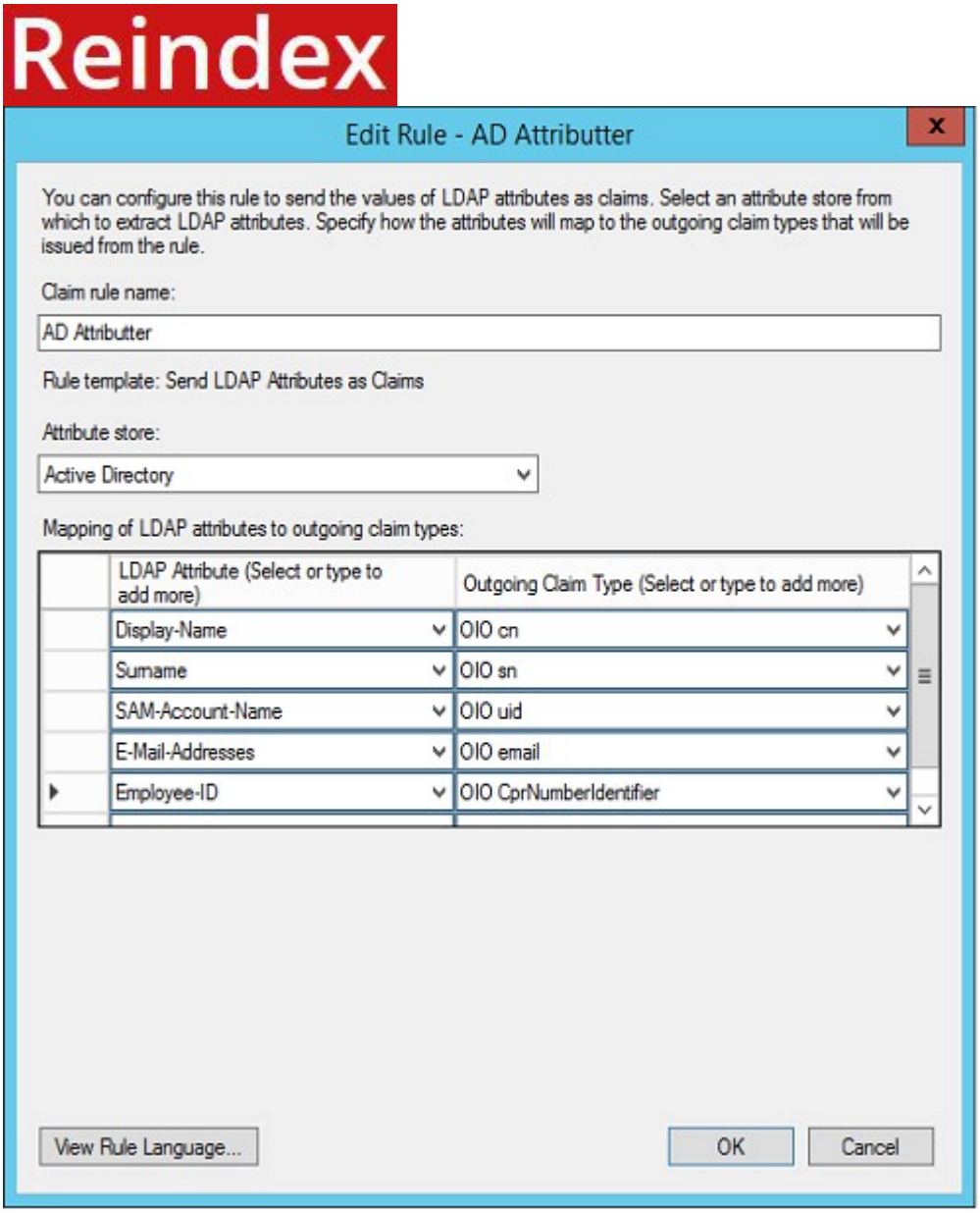
Opsætning af kundespecifikke claim rules

Opsætning af kundespecifikke claim rules afhænger af jeres aftale med Reindex. Der kan nemlig være krav til, at nogle kundetyper leverer CPR-nummer på deres brugere.

Send CPR-nummer

Redigér den eksisterende ”AD Attributter” claim rule og tilføj den AD Attribut, som indeholder brugerens CPR-nummer. Den udgående claim skal være:

Navn	Type
OIO CprNumberIdentifier	dk:gov:saml:attribute:CprNumberIdentifier



Bilag 1

Følgende kommandoer kan afvikles i en PowerShell prompt med administrative rettigheder for at tilføje Claim Typer beskrevet i OIOSAML 2.0.9 profilen.

```
Add-AdfsClaimDescription -ClaimType:"dk:gov:saml:attribute:AssuranceLevel"
-Name:"OIO AssuranceLevel"
Add-AdfsClaimDescription
-ClaimType:"dk:gov:saml:attribute:CprNumberIdentifier" -Name:"OIO
CprNumberIdentifier"
Add-AdfsClaimDescription
-ClaimType:"dk:gov:saml:attribute:CvrNumberIdentifier" -Name:"OIO
cvrNumberIdentifier"
```

```
Add-AdfsClaimDescription -ClaimType:"dk:gov:saml:attribute:IsYouthCert"
-Name:"OIO OCES Youth Certificate"
Add-AdfsClaimDescription
-ClaimType:"dk:gov:saml:attribute:PidNumberIdentifier" -Name:"OIO PID
Number Attribute"
Add-AdfsClaimDescription
-ClaimType:"dk:gov:saml:attribute:RidNumberIdentifier" -Name:"OIO Employee
Number/RID"
Add-AdfsClaimDescription -ClaimType:"dk:gov:saml:attribute:SpecVer"
-Name:"OIO SpecVer"
Add-AdfsClaimDescription
-ClaimType:"dk:gov:saml:attribute:UniqueAccountKey" -Name:"OIO
uniqueAccountKey"
Add-AdfsClaimDescription -ClaimType:"urn:oid:0.9.2342.19200300.100.1.1"
-Name:"OIO uid"
Add-AdfsClaimDescription -ClaimType:"urn:oid:0.9.2342.19200300.100.1.3"
-Name:"OIO email"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.10" -Name:"OIO
Organization Name"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.11" -Name:"OIO
Organization Unit"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.12" -Name:"OIO Title"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.16" -Name:"OIO Postal
Address"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.3" -Name:"OIO cn"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.4" -Name:"OIO sn"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.5" -Name:"OIO
Certificate Serial Number"
Add-AdfsClaimDescription -ClaimType:"urn:oid:2.5.4.65" -Name:"OIO OCES
Pseudonym"
```