

Reindex

Kundevejledning

AD FS opsætning til Reindex

Version: 1.0

Dato: 19. april 2016

Forfatter: Lasse Balsvad (XPERION)

Reindex

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

Indholdsfortegnelse

Indledning.....	4
Vigtig information om opkobling til Reindex.....	4
Send FederationMetadata til Reindex.....	4
Udskiftning af signeringscertifikat.....	4
Opsætning af Reindex som Relying Party Trust i AD FS.....	5
Generel opsætning.....	5
Opsætning af påkrævede Claim Rules.....	12
Send AD Attributter.....	13
Send CVR-nummer.....	15
Send AssuranceLevel.....	16
Send SpecVer.....	17
Send Name ID.....	18
Opsætning af kundespecifikke claim rules.....	19
Send CPR-nummer.....	19
Bilag 1.....	20



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 unødigt 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 metadata 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 muligt, når I udskifter jeres signeringscertifikat.

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

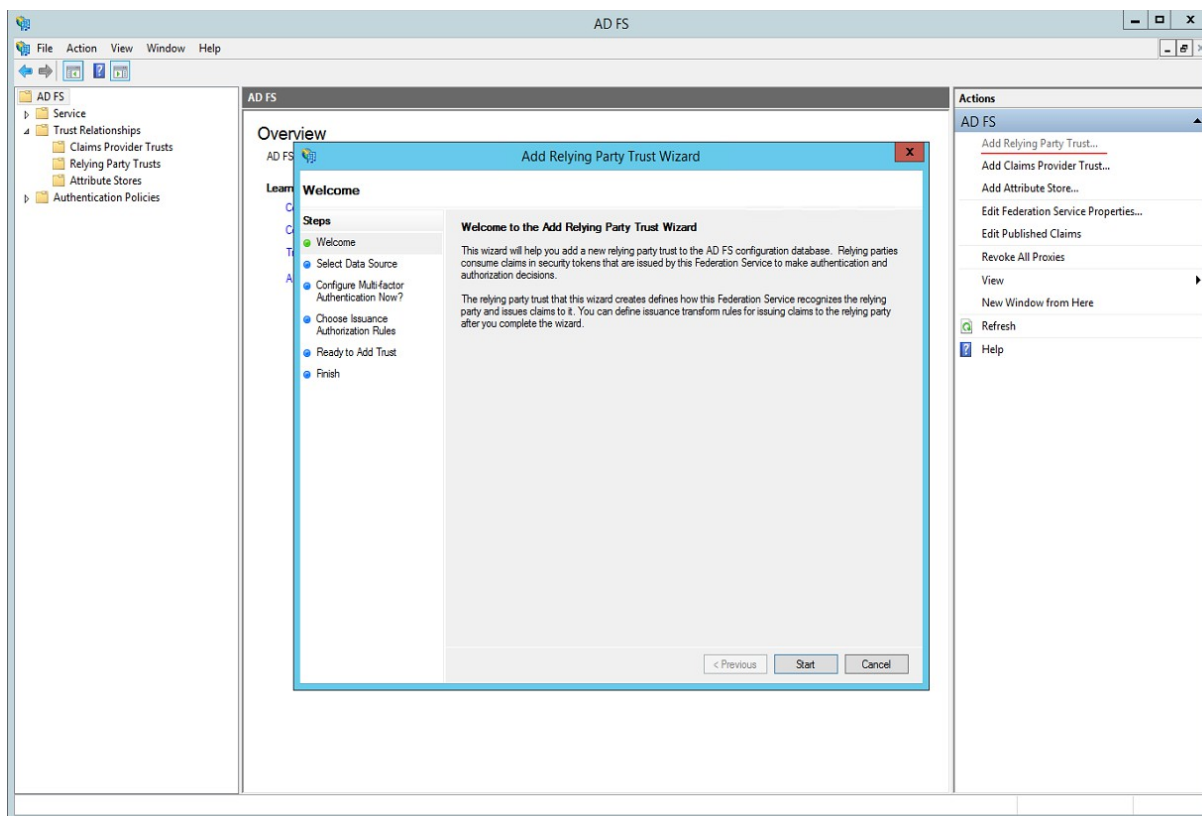
Reindex

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.

Reindex

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". On the left, a "Steps" pane lists: Welcome, Select Data Source (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled "Select Data Source" and contains the instruction: "Select an option that this wizard will use to obtain data about this relying party:". Three radio buttons are present: 1) "Import data about the relying party published online or on a local network" (selected), with a text box containing "https://test.reindex.net/simplesaml/module.php/saml/sp/metadata.php/default-sp" and an example "fs.contoso.com or https://www.contoso.com/app"; 2) "Import data about the relying party from a file", with a text box for "Federation metadata file location:" and a "Browse..." button; 3) "Enter data about the relying party manually". At the bottom are buttons for "< Previous", "Next >", and "Cancel".

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

Reindex

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". The current step is "Specify Display Name". On the left, a "Steps" pane lists the following steps: Welcome, Select Data Source, Specify Display Name (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction "Enter the display name and any optional notes for this relying party." Below this, there is a "Display name:" label followed by a text box containing the word "Reindex". Underneath is a "Notes:" label followed by a large, empty text area with a vertical scrollbar. At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

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

Klik på [**Next**]-knappen

Reindex

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?**
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

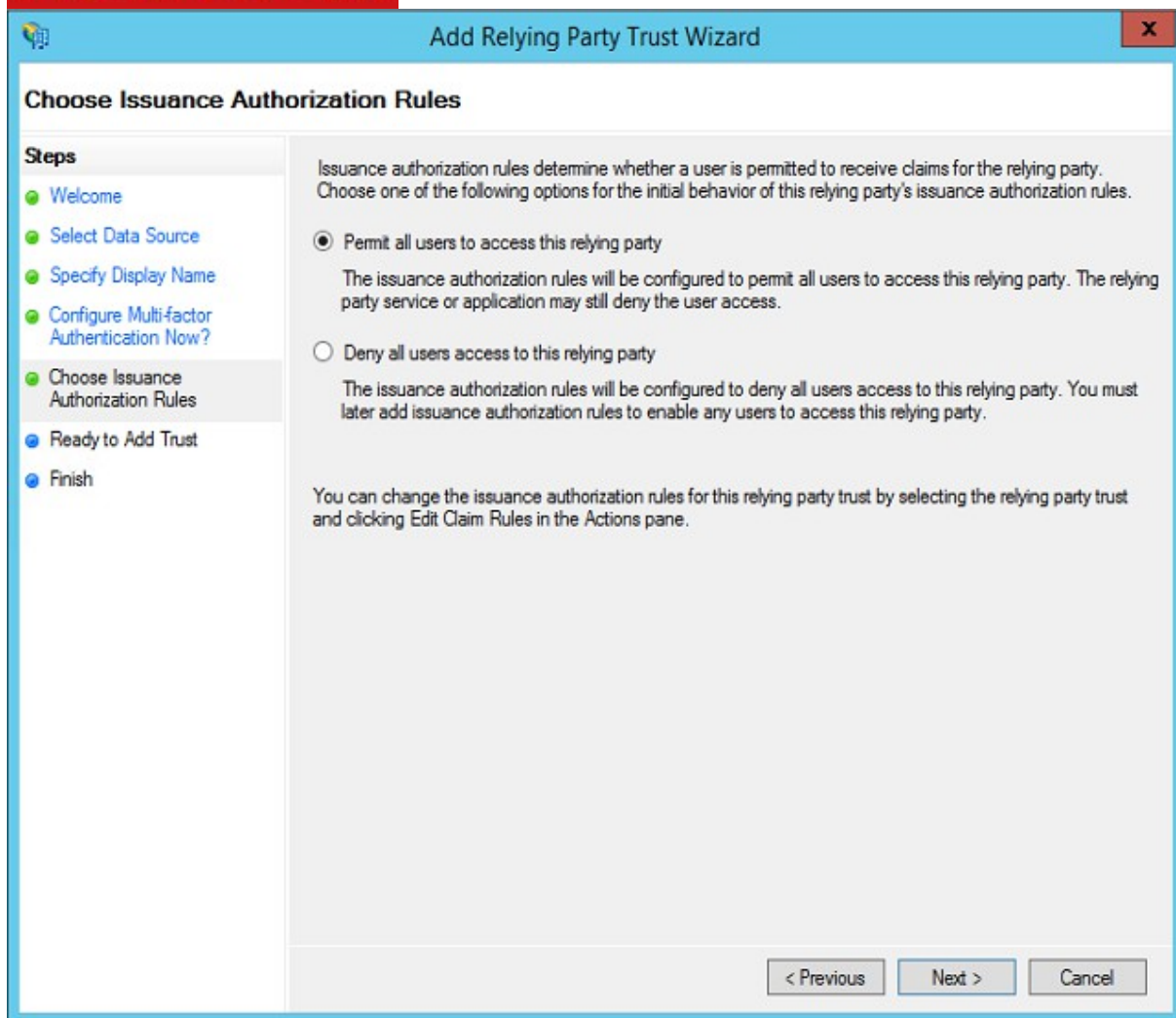
I do not want to configure multi-factor authentication settings for this relying party trust at this time.

Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

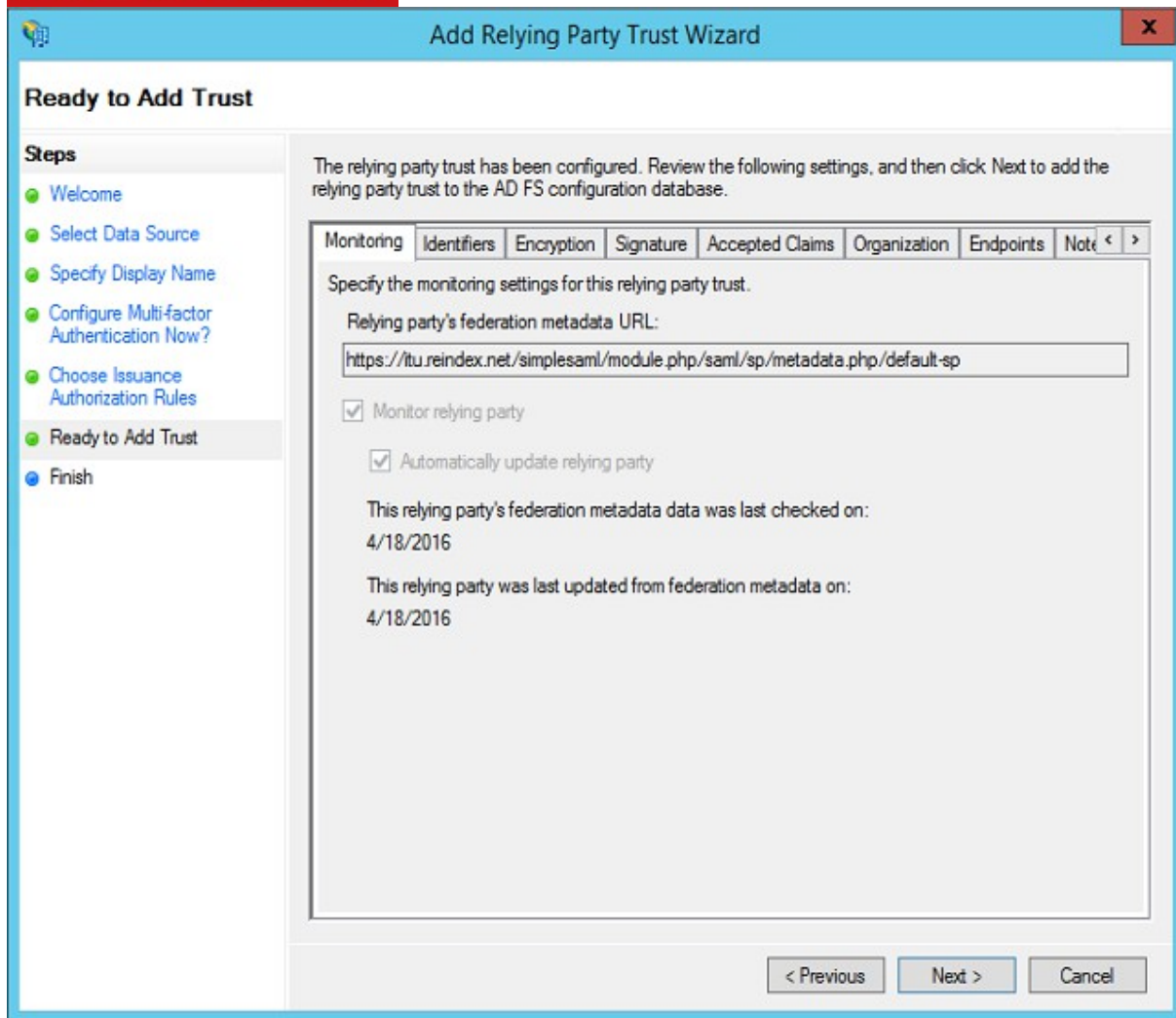
< Previous Next > Cancel

Klik på [Next]-knappen



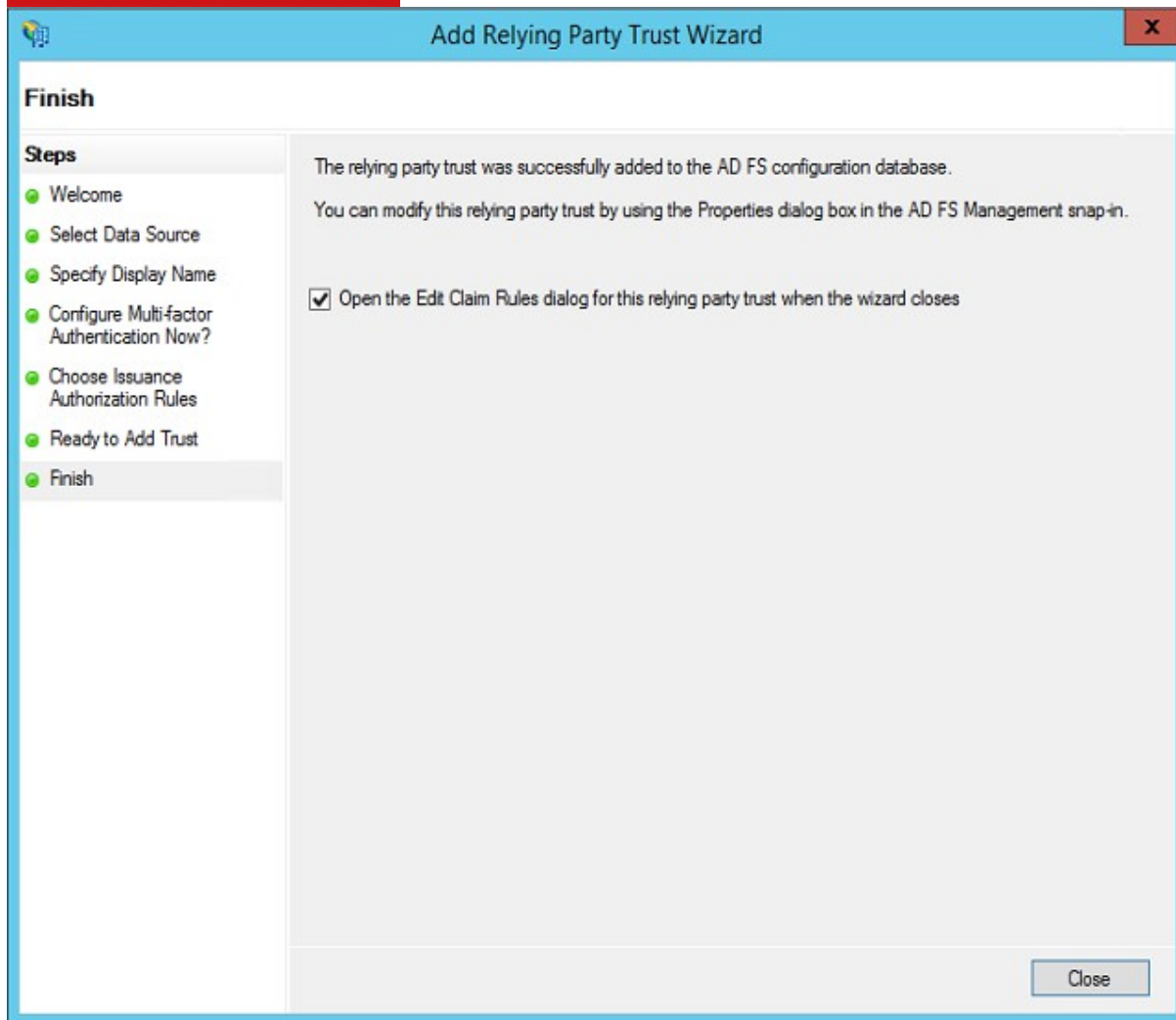
Klik på [Next]-knappen

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

Reindex

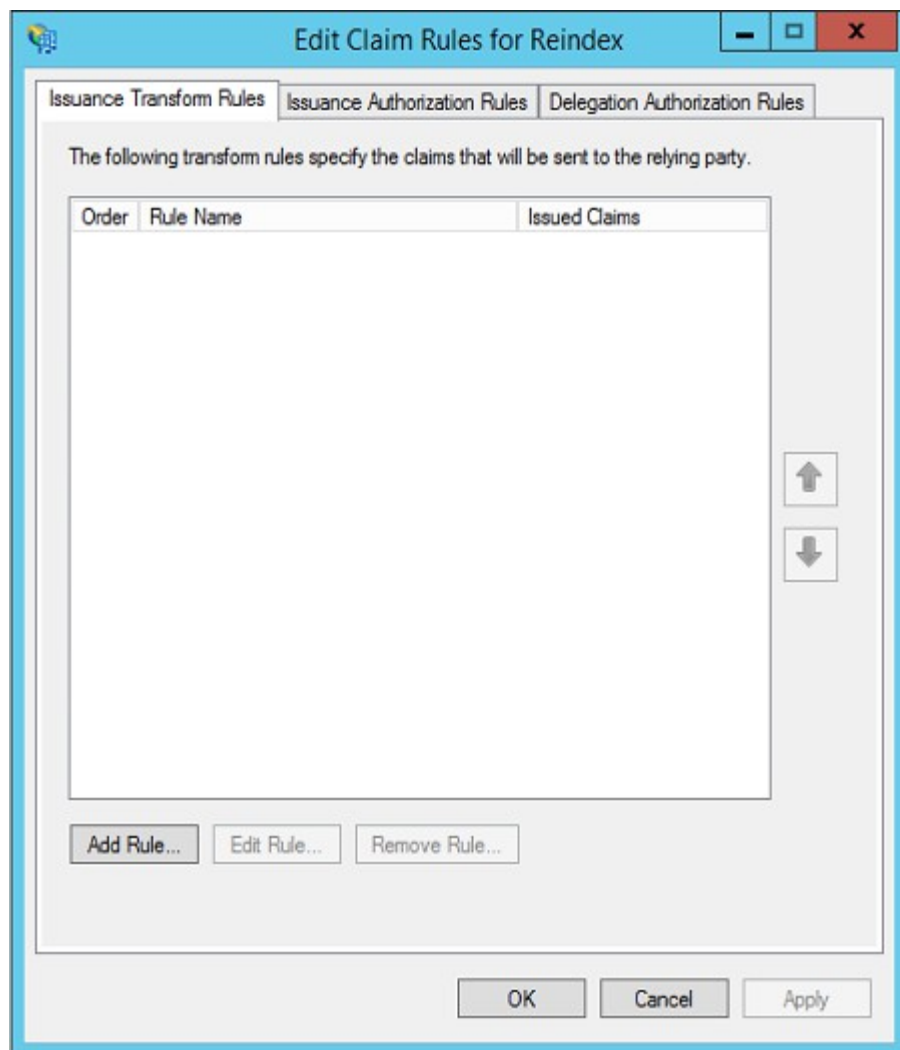


Klik på [**Close**]-knappen

Reindex

Opsætning af påkrævede Claim Rules

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

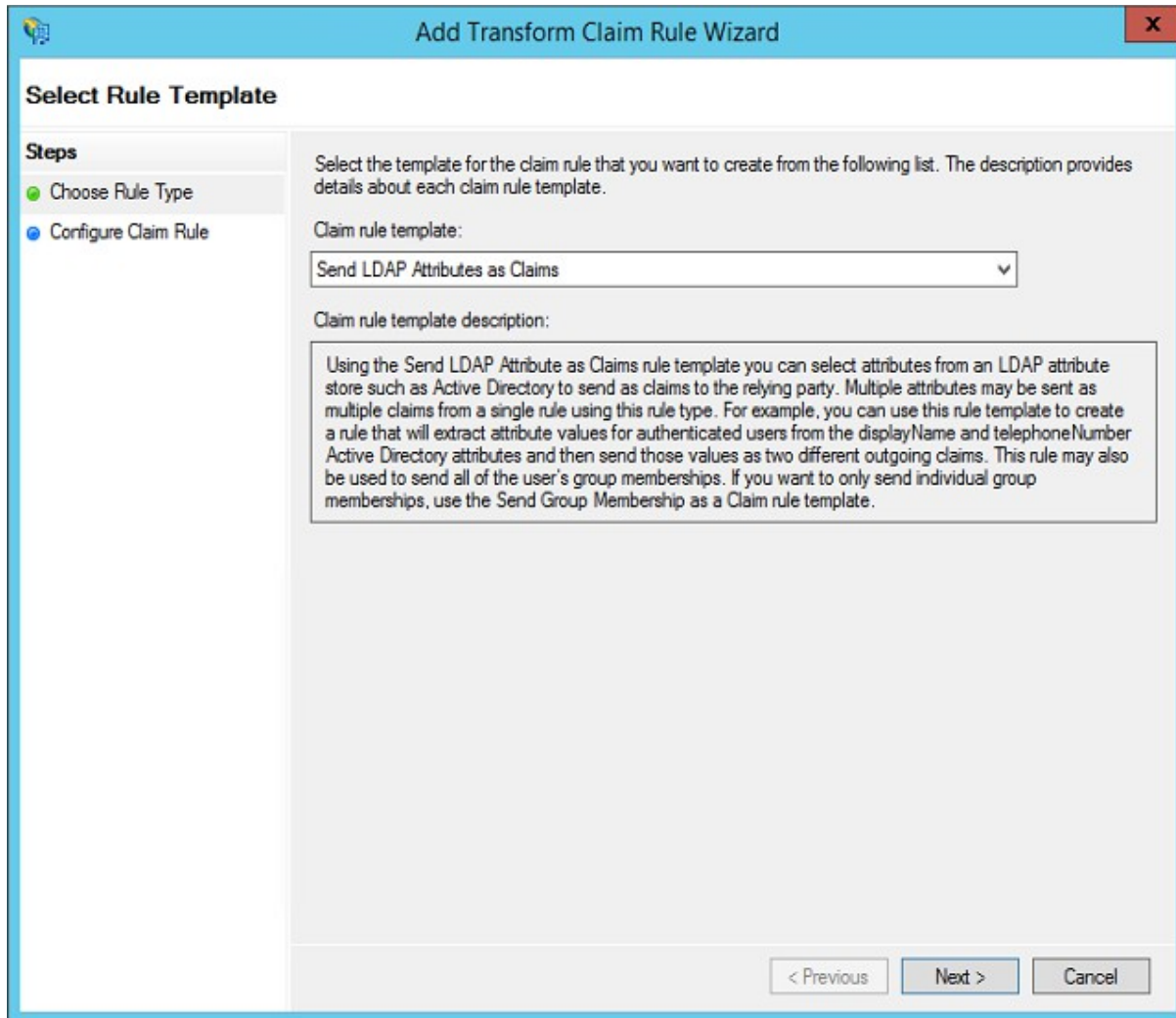


Klik på [**Add Rule...**]-knappen

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.

Reindex

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
AD Attributter

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
Display-Name	OIO cn
Surname	OIO sn
SAM-Account-Name	OIO uid
E-Mail-Addresses	OIO email
▶*	

< Previous Finish Cancel

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

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.

Edit Rule - OIO cvrNumberIdentifier

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
OIO cvrNumberIdentifier

Rule template: Send Claims Using a Custom Rule

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

OK Cancel

Indtast værdierne:

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

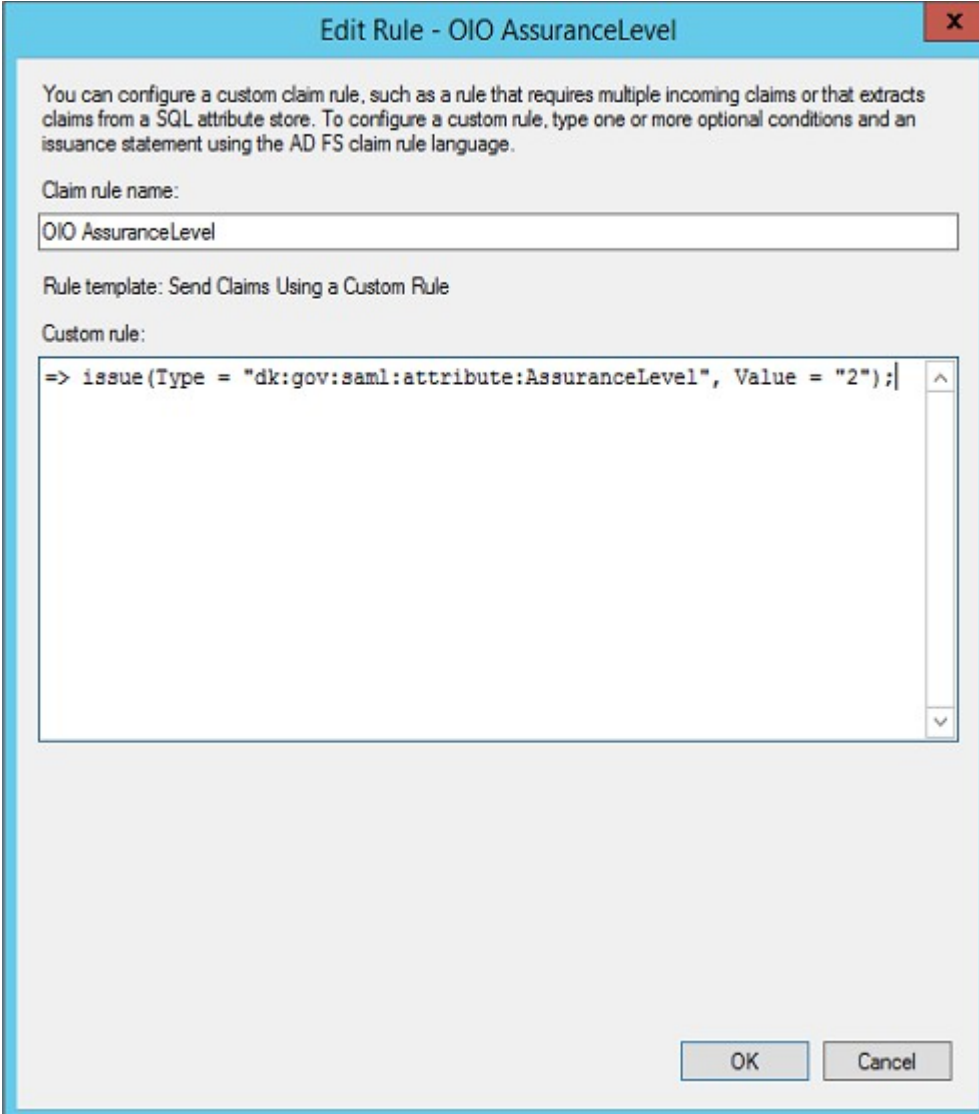
Reindex

Klik på **[Finish]**-knappen

Reindex

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.



Edit Rule - OIO AssuranceLevel

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
OIO AssuranceLevel

Rule template: Send Claims Using a Custom Rule

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

OK Cancel

Indtast værdierne:

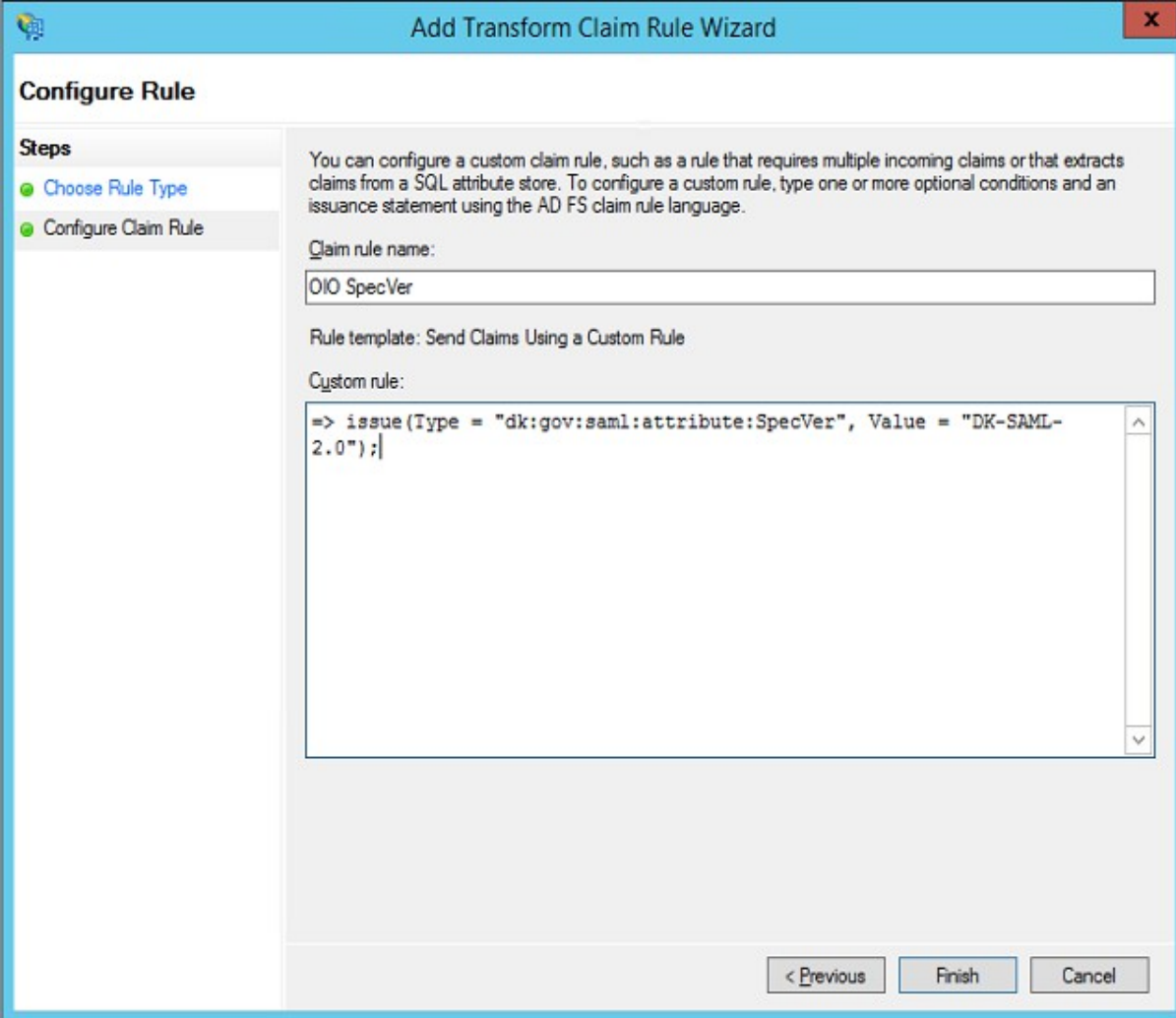
OIO AssuranceLevel
<code>=> issue(Type = "dk:gov:saml:attribute:AssuranceLevel", Value = "2");</code>

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.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
OIO SpecVer

Rule template: Send Claims Using a Custom Rule

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

< Previous Finish Cancel

Indtast værdierne:

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

Klik på **[Finish]**-knappen

Reindex

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.

Edit Rule - Transform OIO uid to Name ID (Transient)

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
Transform OIO uid to Name ID (Transient)

Rule template: Send Claims Using a Custom Rule

Custom rule:
`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");|`

OK Cancel

Indtast værdierne:

Transform OIO uid to Name ID (Transient)
<code>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");</code>



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

Reindex

Edit Rule - AD Attributter

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	Display-Name	OIO cn
	Surname	OIO sn
	SAM-Account-Name	OIO uid
	E-Mail-Addresses	OIO email
▶	Employee-ID	OIO 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"
```

Reindex

```
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"
```