

ADFS Opsætning til Statens SSO Økonomistyrelsen

Indholdsfortegnelse

ADFS Opsætning til Statens SSO Økonomistyrelsen	1
1. Intro og forudsætning.....	2
1.1 Federation Metadata.....	2
2. Opsætning af Trust på Microsoft ADFS Server	2
2.1 Opsætning af "Relying Party Trust"	2
2.3 Opsætning af LDAP claim rule.	5
2.4 Opsætning af Custom Claim rules.	7
2.5 Opsætning af Transform Name ID claim	9
3 Specifikationer og anbefalinger.....	11
3.1 Assurancelevel.....	11
3.2 Logonmethod	11
3.3 Eksempel på custom claims til logonmethod.....	12
3.4 Anbefalinger vedrørende certifikater.....	12

1. Intro og forudsætning

Denne vejledning er udført på en Windows 2019 Server med ADFS-rollen installeret og konfigureret.

ADFS-serveren benytter ikke MFA, men det **anbefales/krav** at der altid benyttes MFA, når login foretages fra internettet.

Indholdet i dette dokument er udarbejdet for at assistere institutionerne i den korrekte oprettelse af en "Relying Party Trust" med Økonomistyrelsens SSO-løsning.

1.1 Federation Metadata

Der skal bruges Metadata modtaget fra Økonomistyrelsen i form af URL (fremsendes sandsynligvis sammen med denne vejledning)

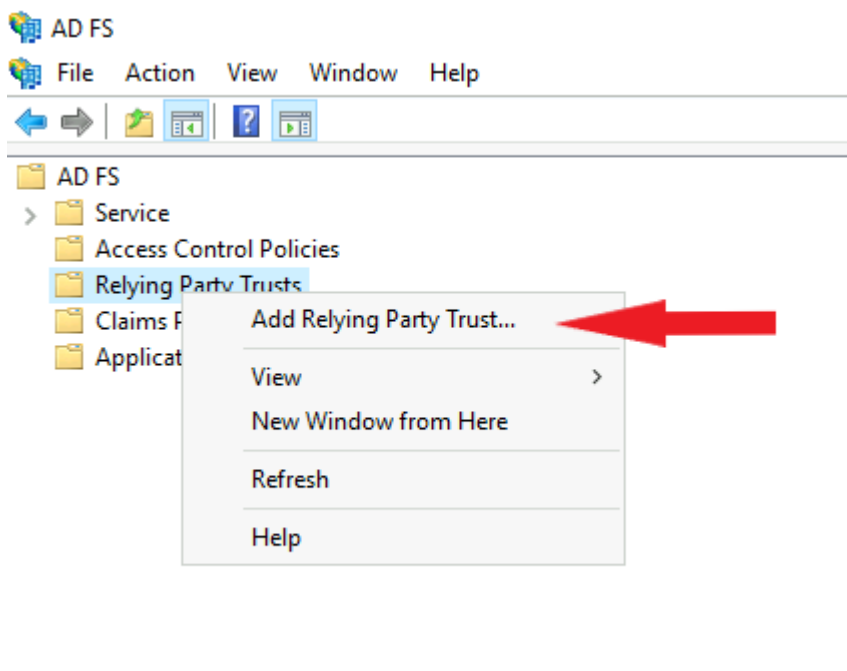
For institutioner som ikke har anvendt den eksisterende SSO løsning:

Metadata fra egen ADFS opsætning skal udleveres til Økonomistyrelsen som en Metadata fil eller URL

2. Opsætning af Trust på Microsoft ADFS Server

2.1 Opsætning af "Relying Party Trust"

1 I ADFS-Konsollen højre klikkes på "Relying Party Trust" og der trykkes på "Add Relying Party Trust"



2 I konfigurationswizard vælg "Claim Aware" og tryk "start"

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Welcome'. On the left, a 'Steps' pane lists: Welcome (selected), Select Data Source, Choose Access Control Policy, Ready to Add Trust, and Finish. The main content area is titled 'Welcome to the Add Relying Party Trust Wizard' and contains the following text: 'Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. [Learn more](#)'. Below this text are two radio buttons: 'Claims aware' (which is selected) and 'Non claims aware'.

3 Indsæt Federation metadata URL, som du har modtaget og tryk "Next"

The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Select Data Source' step. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Select Data Source'. On the left, the 'Steps' pane lists: Welcome, Select Data Source (selected), Choose Access Control Policy, Ready to Add Trust, and Finish. The main content area is titled 'Select an option that this wizard will use to obtain data about this relying party:'. It contains two radio buttons: 'Import data about the relying party published online or on a local network' (selected) and 'Import data about the relying party from a file'. The first option includes a text box for 'Federation metadata address (host name or URL):' containing the URL 'https://auth.prod.statens-ss0.dk/realms/Statens_SSO/broker/KUNDE SPECIFIK URL/endpoint/descrip'. Below this is an example: 'Example: fs.contoso.com or https://www.contoso.com/app'. The second option includes a text box for 'Federation metadata file location:' and a 'Browse...' button.

- Udfyld "Display name" eks. "MODST SSO (Produktion)" og "MODST SSO (PreProd)" – Det kan være en god idé at gemme kontaktoplysninger og Metadata URL i Notes. Og tryk "Next"

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Display name:
MODST SSO (Produktion)

Notes:
KontaktOplysninger@email.dk
Metadata URL: https://auth.prod.statens-ssso.dk/realms/Statens_SSO/broker/KUNDE
SPECIFIK URL/endpoint/descriptor

- Sæt en passende "Access Control Policy" der passer til jeres adgangs politikker og infrastruktur. Og tryk "Next"

Add Relying Party Trust Wizard

Choose Access Control Policy

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require multi-factor authentication.
Permit everyone and require MFA for specific group	Grant access to everyone and require multi-factor authentication for a specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require multi-factor authentication from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require multi-factor authentication from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require multi-factor authentication, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specific groups.

Policy

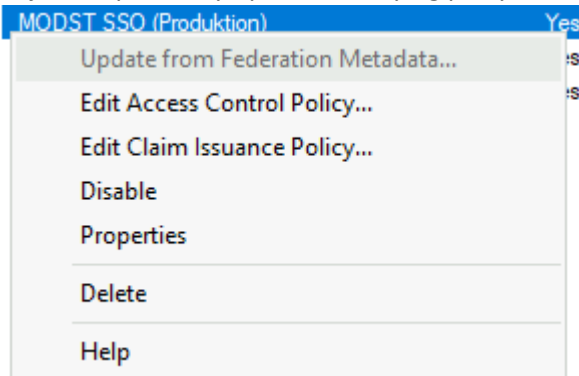
- Permit users from intranet network
- Permit users from internet network and require multi-factor authentication

- Tryk "Next" og "Close" for at afslutte konfigurationswizard.

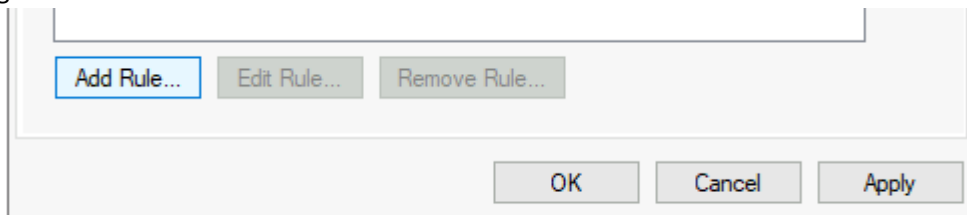
2.3 Opsætning af LDAP claim rule.

Følgende guide skal udføres pr. relying party trust. I dette afsnit lægges LDAP regler direkte på Relying Party trust. Bemærk, at disse regler kun aktiveres når brugerne logger på via Active Directory. Anvendes der andre claim providers på AD FS til autentificering, så kræver det at disse LDAP regler populeres på den oprindelige IdP/Claim Provider.

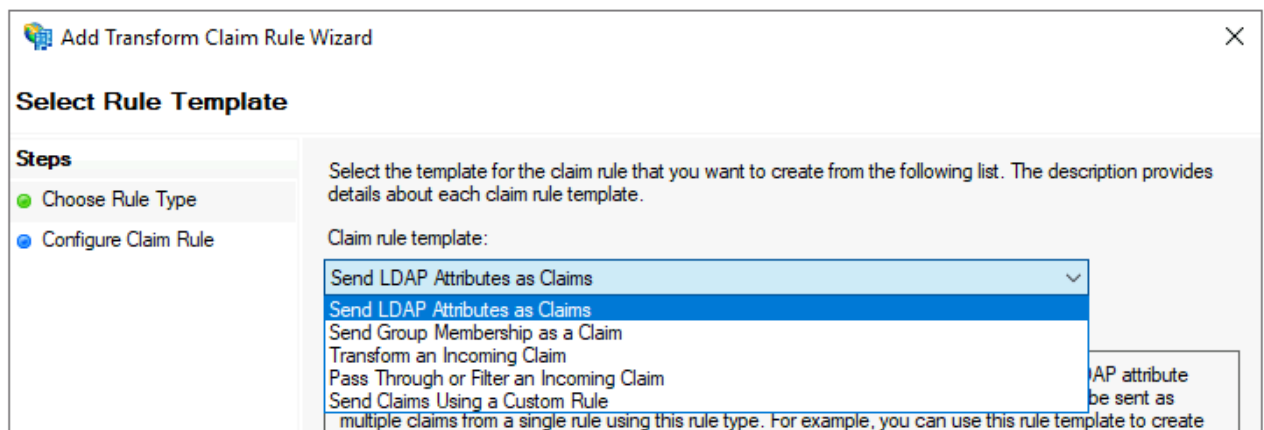
- 1 Højre klik på det ny oprettede relying party trust og vælg "Edit Claim Issuance Policy"



- 2 vælg "add rule"



- 3 Vælg "Send LDAP Attributes as Claims" i drop down og tryk næste



- 4 Giv reglen et navn "LDAP", vælg "Active directory" som "Attribute store" og udfyld felterne "LDAP Attribute" og "Outgoing Claim Type".

Det er vigtigt at udskifte Outgoing Claim Type med værdierne i tabellen og ikke vælge standardværdierne, som den kan tilbyde via drop down menuen. I nedenstående anvendes mail-attributten på brugerne som brugerid i fagsystemerne (user id og Name claims). Hvis I bruger UPN navn til brugerid, så skal LDAP attributten for user id og Name claim være User-Principal-Name attributten.

<u>LDAP Attribute</u>	<u>Outgoing Claim Type</u>
E-Mail-Addresses	https://modst.dk/sso/claims/email
E-Mail-Addresses	https://modst.dk/sso/claims/userid
objectGuid	https://modst.dk/sso/claims/uniqueid
Mobile	https://modst.dk/sso/claims/mobile
Surname	https://modst.dk/sso/claims/surname
Given-Name	https://modst.dk/sso/claims/givenname
E-Mail-Addresses	Name

Eksempel på "LDAP" claim rule:

Edit Rule - LDAP ✕

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)
▶	E-Mail-Addresses ▾	https://modst.dk/sso/claims/email ▾
	E-Mail-Addresses ▾	https://modst.dk/sso/claims/userid ▾
	objectGuid ▾	https://modst.dk/sso/claims/uniqueid ▾
	Telephone-Number ▾	https://modst.dk/sso/claims/mobile ▾
	Sumame ▾	https://modst.dk/sso/claims/sumame ▾

2.4 Opsætning af Custom Claim rules.

I dette afsnit vil der blive vist eksempel på hvordan der oprettes en "custom rule" på jeres ADFS Server for de attributter som ikke findes i jeres AD.

Syntaksen i hvert regel er følgende:

```
=> issue(type = "Claimtype", value = "value");
```

For CVR vil det se således ud:

```
=> issue(type = "https://modst.dk/sso/claims/cvr", value = "12345678");
```

Det vil være nødvendigt at rette både **CVR**, **assurancelevel** og **logonmethod** værdierne til, så de passer jeres setup.

Udfør guiden for hvert af følgende regler: **CVR**, **assurancelevel** og **logonmethod**. Bemærk, at logonmethod claimet skal matche brugerens logon metode.

Så hvis brugeren er logget på med tofaktor, så skal logonmethod attributten afspejle dette. Det samme gælder assurancelevel claimet. Se mere om dette i ØSs generelle tilslutningsvejledning, under afsnittet: "Information om hvilke attributter, institutionen skal medsende fra sin lokale IdP".

I AD FS kan man se en brugers logonmetode via følgende claim: <https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-rule-to-send-an-authentication-method-claim> Se mere her: <https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-claim-rules> .

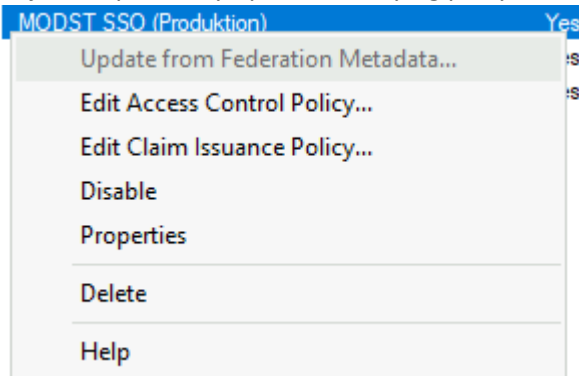
Denne guide er baseret på en AD FS, der anvender forms-login og enkeltfaktor. Derfor 2 i assurancelevel, og username-password-protectedtransport. Hvis jeres AD FS anvender kerberos og enkeltfaktor for alle brugere, så skal assurancelevel stå til 2 og logonmethod til kerberosspnego. Hvis AD FS anvendes både internt og eksternt fra, så skal AD FS' authenticationmethod claim oversættes til den tilsvarende logonmethod og assurancelevel claim til at afspejle dette korrekt for hvert login.

[Se værdier for assurancelevel og logonmethod claims HER.](#)

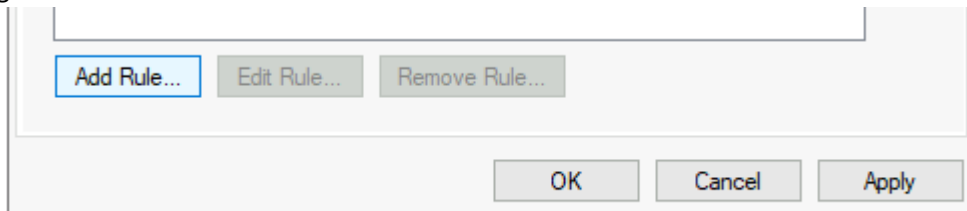
De 3 Custom Claim Rule til CVR, assurancelevel og logonmethod
<pre>=> issue(type = "https://modst.dk/sso/claims/cvr", value = "12345678");</pre>
<pre>=> issue(type = "https://modst.dk/sso/claims/assurancelevel", value = "2");</pre>
<pre>=> issue(type = "https://modst.dk/sso/claims/logonmethod", value = "username-password-protectedtransport");</pre>

Følgende guide skal udføres pr. relying party trust

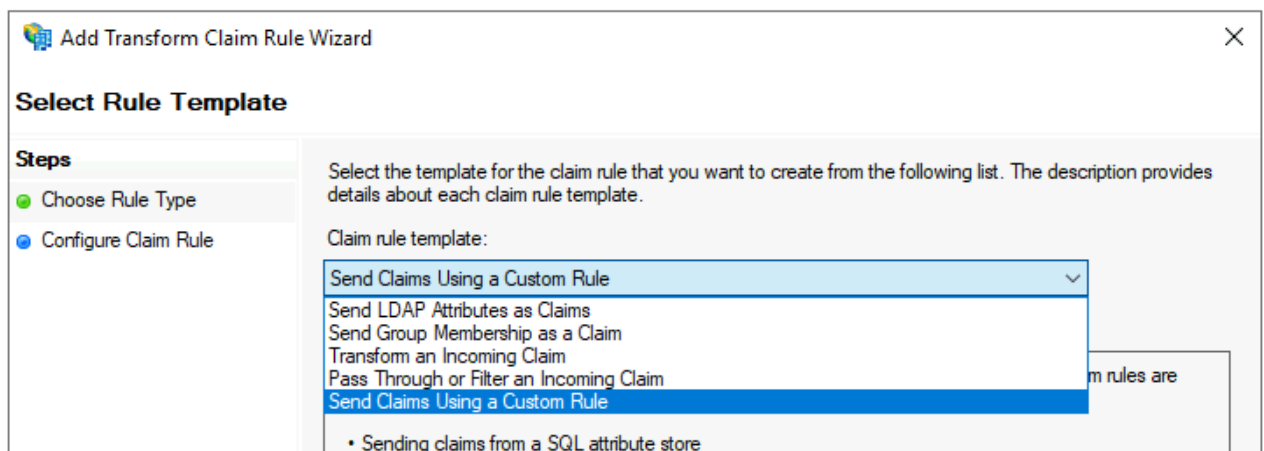
- 1 Højre klik på det ny oprettede relying party trust og vælg "Edit Claim Issuance Policy"



- 2 vælg "add rule"



- 3 Vælg "Send Claims Using a Custom Rule" i dropdown og tryk næste



- 4 Udfyld "Claim rule Name" og "Custom Rule" for **CVR** og gentag punkt 2 til 4 for henholdsvis **assurancelevel** og **logonmethod**. Eksempel på Custom Rule for CVR claim

Edit Rule - CVR

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:
CVR

Rule template: Send Claims Using a Custom Rule

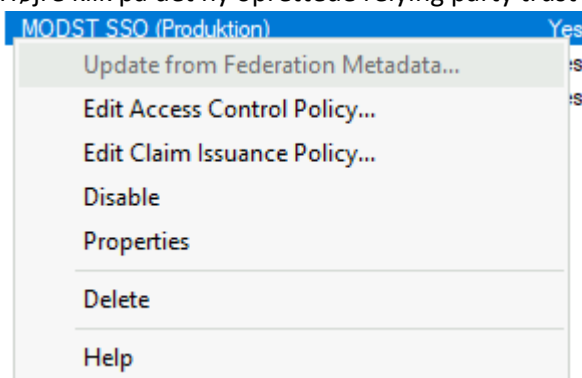
Custom rule:
`> issue (Type = "https://modst.dk/sso/claims/cvr", Value = "12345678");`

2.5 Opsætning af Transform Name ID claim

Følgende guide skal udføres pr. relying party trust

Name ID oversættes fra `https://modst.dk/sso/claims/userid` claimen som en Transform rule. Denne transform rule skal således transformere `userid` claimen til en ny claim af typen Name ID (persistent identifier).

- 1 Højre klik på det ny oprettede relying party trust og vælg "Edit Claim Issuance Policy"



- 2 vælg "add rule"
- 3 Vælg "Transform an incoming Claim" i dropdown og tryk næste

4 Udfyld

Claim rule Name: **Transform userid to Name ID**

Incoming claim type: <https://modst.dk/sso/claims/userid>

Incoming claim type: **Ved fejl prøv at indsætte denne værdi: UPN**

Outgoing claim type: **Name ID**

Outgoing name ID format: **Persistent Identifier**

Edit Rule - Transform userid to Name ID

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type: **Alternativt benyt: UPN**

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

Pass through all claim values

Du burde nu have 5 Claimrules, som vist på eksemplet:

Edit Claim Issuance Policy for MODST SSO (Produktion)

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	LDAP	https://modst.dk/sso/clai...
2	CVR	<See claim rule>
3	Assurancelevel	<See claim rule>
4	Logonmethod	<See claim rule>
5	Transform userid to Name ID	Name ID

Dette afslutter opsætningen. **HUSK at tilrette Logonmethod og Assurancelevel, så det matcher jeres setup.**

3 Specifikationer og anbefalinger

3.1 Assurancelevel.

<u>Værdi</u>	<u>Beskrivelse</u>
2	Der er foretaget enkeltfaktor validering, f.eks. brugernavn/adgangskode eller kerberos spnego i forbindelse med en domain joined device
3	Der er foretaget to-faktor validering af brugeren – f.eks. sms kode, nemid eller tilsvarende.

3.2 Logonmethod

<u>Værdi</u>	<u>Beskrivelse</u>
username-password-protectedtransport	Username/Password login
kerberos-spnego	Ægte SSO via “Windows Integrated Authentication” (WIA)
two-factor	To faktor login

3.3 Eksempler på custom claims til logonmethod

Her er et eksempel, på to custom claim rules, som i første regel kontrollerer om claimet

<http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod> har præcis værdien = "<http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows>"]

Hvis dette er et match udstedes claimet <https://modst.dk/sso/claims/logonmethod> med værdien "kerberos-spnego"

i anden regel kontrolleres om claimet

<http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod> har en værdi der adskiller sig fra =

"<http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows>"]

Hvis dette er et match udstedes claimet <https://modst.dk/sso/claims/logonmethod> med værdien "username-password-protectedtransport"

```
@RuleName = "1 Logonmethod = Windows Authentication"
```

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod", Value == "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows"]
```

```
=> issue(Type = "https://modst.dk/sso/claims/logonmethod", Value = "kerberos-spnego");
```

```
@RuleName = "2 Logonmethod = Any other authentication method"
```

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod", Value != "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows"]
```

```
=> issue(Type = "https://modst.dk/sso/claims/logonmethod", Value = "username-password-protectedtransport");
```

3.4 anbefalinger vedrørende certifikater

For at forhindre hyppige ændringer til federationsforbindelserne anbefaler vi at der bruges et selfsigned certifikat, udstedt lokalt fra jeres maskine til både signering og decryption med en længere levetid end den som ADFS opretter som standard.

Vi anbefaler følgende til jeres opsætning af certifikatet:

- SHA-256
- Levetid: 3-5 år
- RSA: 4096bits