

# AULA

## Opsætningsvejledning

**Version:** 1.0.0  
**Date:** 09.03.2019  
**Author:** BSG

## Indhold

|       |   |   |
|-------|---|---|
| 1     | Indledning .....                                    | 3 |
| 2     | Overblik over den tekniske opsætning .....          | 3 |
| 3     | Detaljer .....                                      | 3 |
| 3.1   | Tilslutte sig OS2faktor via OS2.....                | 3 |
| 3.2   | Modtage API nøgler til den tekniske opsætning ..... | 4 |
| 3.3   | Foretage den tekniske opsætning af AD FS .....      | 4 |
| 3.3.1 | Opsætte AULA som en Relying Party.....              | 4 |
| 3.3.2 | Opsætte Claim Rules .....                           | 4 |
| 3.4   | MFA konfiguration i AD FS .....                     | 6 |
| 3.5   | Sende AD FS metadata til AULA .....                 | 6 |

# 1 Indledning

Dette dokument er udarbejdet som en samlet vejledning til AD FS opsætningen til login til AULA. Der er taget udgangspunkt i den officielle vejledning, der kan hentes her

<https://aulainfo.dk/wp-content/uploads/Vejledning-til-Ops%C3%A6tning-af-kommunal-Identity-Provider.pdf>

Man bør under alle omstændigheder forholde sig til indholdet af den officielle vejledning. Dette dokument er alene tiltænkt en nem måde at danne sig overblik over alle opgaverne, og tilføje oplysninger der er relevante for OS2faktor opsætningen.

Efter gennemgang af denne vejledning, vil man kunne foretage login til AULA via AD FS, og vil kunne foretage step-up med OS2faktor når AULA er klar til at understøtte dette.

## 2 Overblik over den tekniske opsætning

Der skal udføres følgende opgaver for at være på plads med opsætningen af AD FS til AULA.

1. Tilslutte sig OS2faktor via OS2
2. Modtage API nøgler til den tekniske opsætning af driftoperatøren på OS2faktor
3. Foretage den tekniske opsætning af AD FS
4. Sendte AD FS metadata til AULA

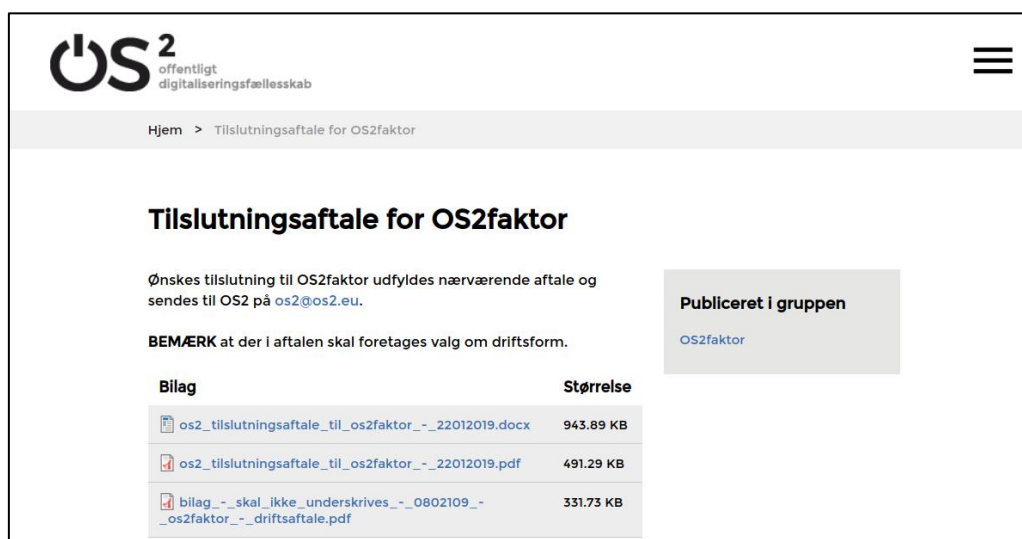
## 3 Detaljer




Ovenstående opgaver er beskrevet nedenfor i flere detaljer

### 3.1 Tilslutte sig OS2faktor via OS2

For at anvende OS2faktor skal man være tilsluttet infrastrukturen. Dette gøres ved at udfylde den tilslutningsaftale der findes her

<https://os2.eu/dokument/tilslutningsaftale-os2faktor>



| Bilag   | Størrelse |
|---|-----------|
|  os2_tilslutningsaftale_til_os2faktor_-_22012019.docx                    | 943.89 KB |
|  os2_tilslutningsaftale_til_os2faktor_-_22012019.pdf                     | 491.29 KB |
|  bilag_-_skal_ikke_underskrives_-_0802109_-_os2faktor_-_driftsaftale.pdf | 331.73 KB |

## 3.2 Modtage API nøgler til den tekniske opsætning

Når tilslutningsaftalen er modtaget af OS2, vil I blive kontaktet af driftoperatøren, der giver jer de API nøgler der skal anvendes til den tekniske opsætning.

Bemærk at man altid kan modtage flere API nøgler, så man har en nøgle per teknisk integration. Der er ingen yderligere omkostninger forbundet med at få flere API nøgler.

Til hver API nøgle er der bundet et navn, som er den tekst der vises til slutbrugeren når denne skal logge på (fx "Du er ved at logge på XYZ, vil du godkende login'et?").

## 3.3 Foretage den tekniske opsætning af AD FS

Først gennemføres opsætningen af OS2faktor på AD FS serveren/serverne. Her henvises til den generelle opsætningsguide for OS2faktor der kan findes her

<https://www.os2faktor.dk/download.html>

Når OS2faktor er installeret på AD FS serveren, gennemføres nedenstående trin for at konfigurere selve AULA integrationen

### 3.3.1 Opsætte AULA som en Relying Party

I den officielle vejledning til AD FS opsætningen for AULA (se link øverst i dette dokument) er metadata for AULA indlejret. For nemheds skyld er metadata trukket ud i en XML fil, og vedlagt denne vejledning (se aula.xml).

I AD FS vælges "Relying Party Trust" og herunder "Add Relying Party Trust". I den menu der kommer frem, vælges at indlæse metadata fra en fil, hvor ovennævnte aula.xml vælges.

Til alle andre valg i opsætningen vælges bare default værdien.

Efter endt opsætning åbnes "Claim Rules" dialogen, hvor nedenstående claim rules oprettes

### 3.3.2 Opsætte Claim Rules

AULA forventer at modtage 4 claims, de er

- Brugerens unikke identitet
- Brugerens UniLogin ID
- Kommunens CVR nummer
- Det AssuranceLevel som brugeren er logget på med (værdien 2 eller 3)

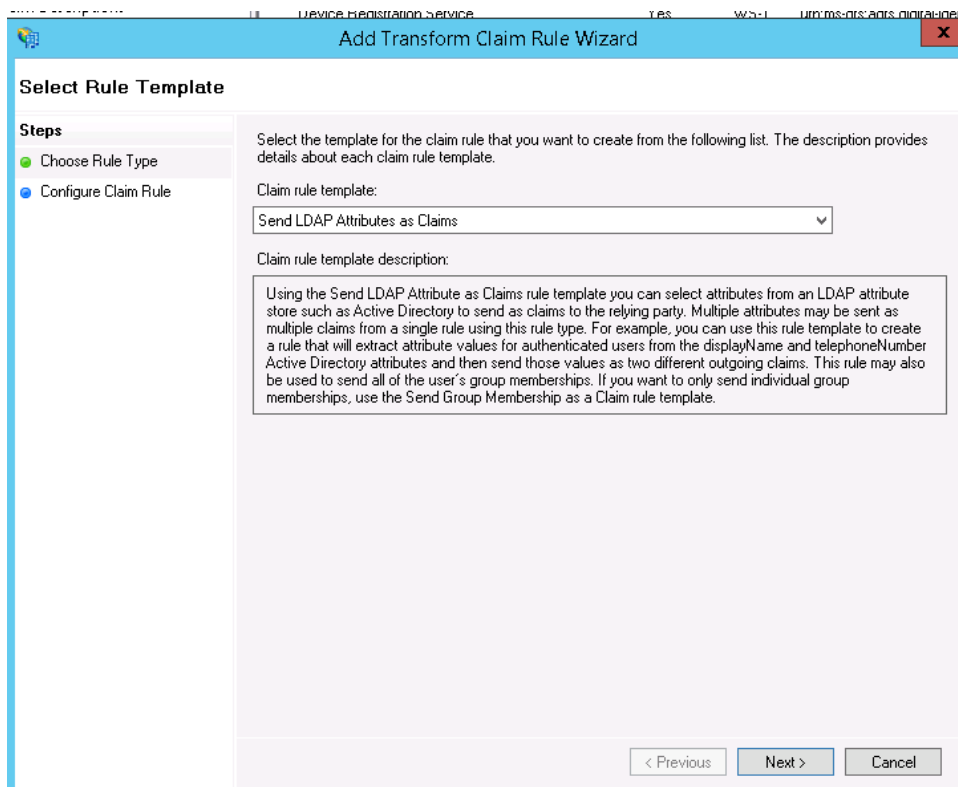
#### **Brugerens unikke ID**

I den officielle vejledning angives det at det unikke ID på brugeren blot skal være unikt og det samme ved hvert login, og de anbefaler at bruge SID'en på brugeren. Hvis dette ønskes, så kan man bruge denne claim rule, der oprettes som en "Custom Claim Rule"

For at understøtte nem copy/paste, er denne claim rule lagt i filen claim-rules.txt der følger med denne vejledning.

#### **Brugerens UniLogin ID**

I næsten alle kommuner er sAMAccount lig med brugernes UniLogin. Hvis det er tilfældet hos jer, kan I lave en almindelige mapning af AD attributten, ved at vælge "Send LDAP Attribute as Claims"



**Add Transform Claim Rule Wizard**

**Select Rule Template**

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

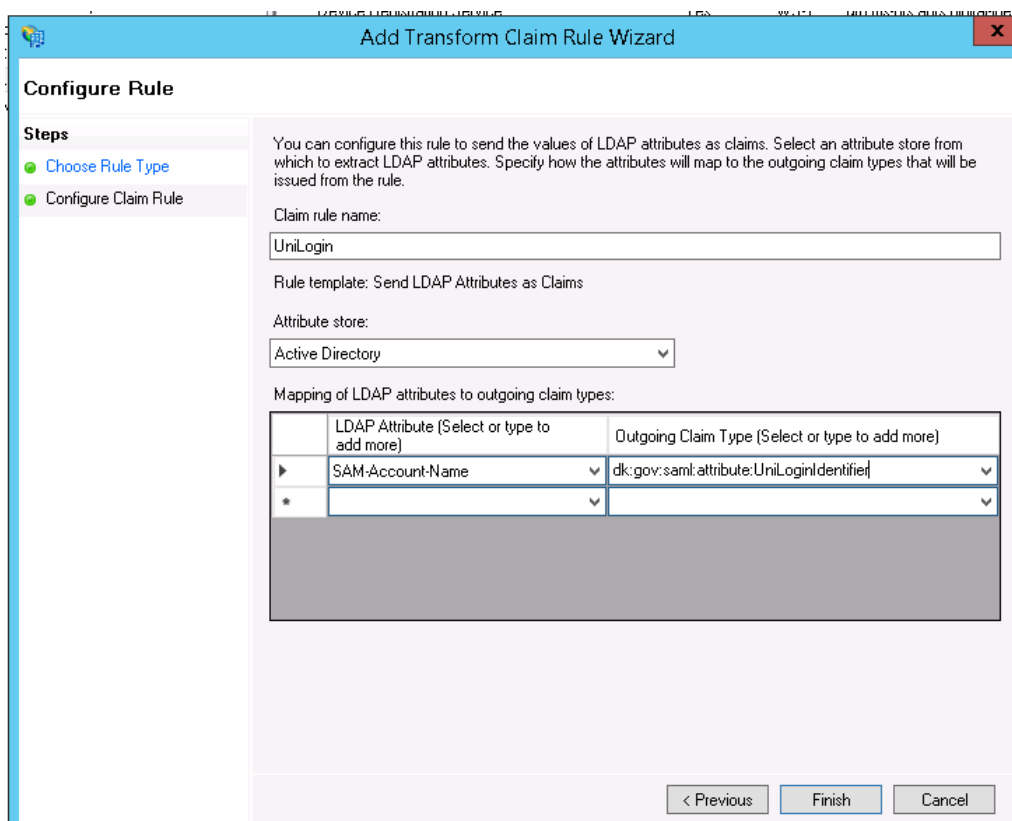
Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous   Next >   Cancel

Og dernæst mappe sAMAccountName til dk:gov:saml:attribute:UniLoginIdentifier som vist nedenfor



**Add Transform Claim Rule Wizard**

**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:

UniLogin

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) |
|---|---|--|
| ▶ | sAM-Account-Name                            | dk:gov:saml:attribute:UniLoginIdentifier         |
| * |   |  |

< Previous   Finish   Cancel

## Kommunens CVR nummer

Kommunens CVR nummer skal også medsendes som et claim, hvilket gøres via endnu et Custom Claim. Selve reglen ligger i claim-rules.txt filen, så den let kan kopieres inde i AD FS.

## AssuranceLevel

I den officielle vejledning til AULA står der at man skal medsende værdien 2 når en bruger logger på med brugernavn/kodeord, og værdien 3 når brugeren logger på med 2-faktor. Der står ikke hvordan dette gøres, da det vil være produktafhængigt.

Der ligger 2 claim rules, der skal opsættes i AD FS som Custom Claim Rules, i filen claims-rules.txt. Den første regel sender værdien 2 når brugeren ikke anvender OS2faktor, og værdien 3 når brugeren har anvendt OS2faktor i forbindelse med login.

## 3.4 MFA konfiguration i AD FS

Bemær at der IKKE skal laves en regel i AD FS om at brugeren skal anvende MFA (multi-factor authentication). Hvis man gør dette, så vil brugeren altid skulle anvende OS2faktor på login tidspunktet. Ved at undlade at sætte en sådan regel op, så er det AULA selv der bestemmer hvornår OS2faktor skal I spil.

## 3.5 Sende AD FS metadata til AULA

I har modtaget en KLIK opgave fra KOMBIT i forbindelse med implementeringen af AULA. I denne KLIK opgave bliver I bedt sende følgende oplysninger til AULA projektet

- Jeres AD FS metadata
- Jeres institutionskode
- Den metode I ønsker at anvende til step-up

Her skal I sende selve AD FS metadata filen, den institutionskode der repræsenterer jeres kommune, og angive at I anvender AD FS til step-up.

Når AULA har opsat jeres fremsendte metadata i deres ende, vil brugerne kunne gennemføre login til AULA via AD FS.