



ØKONOMISTYRELSEN

Opsætning af IdP i Azure AD Enterprise Application

Statens SSO

ISBN: 97887-7659-112-0

Publiceret/Opdateret: Oktober 2026

Indhold

1. Opsætning af IdP i Azure AD Enterprise Application	2
2. Opsætning af Enterprise Application	3
3. Konfiguration af SAML	4
4. Konfiguration af claims (attributter)	5
5. Fremsendelse af metadata URL og maildomæner	6
6. Test af tilkobling til Statens SSO	7
7. Yderligere hjælp	8

1. Opsætning af IdP i Azure AD Enterprise Application

Denne vejledning gennemgår, hvordan en teknisk administrator opretter og konfigurerer en Enterprise Application i Microsoft Entra ID (Azure AD) med henblik på at tilslutte institutionen til Statens SSO

Vejledningen henvender sig til institutioner, der anvender Microsoft Entra ID (Azure AD) som identitetsleverandør (IdP), og beskriver, hvordan institutionen tilsluttes Statens SSO.

Vejledningen er opdelt i følgende afsnit:

1. Opsætning og konfiguration af IdP (afsnit 2-4)
2. Fremsendelse af metadata-URL og maildomæner (afsnit 5)
3. Test af forbindelse til Statens SSO (afsnit 6)
4. Yderligere hjælp (afsnit 7)

2. Opsætning af Enterprise Application

Denne vejledning beskriver, hvordan en Enterprise Application oprettes i Microsoft Entra ID (Azure AD)

1. Log ind på <https://entra.microsoft.com/>.
2. Klik på **Enterprise Application**.
3. Klik på **New application**.
4. Klik på **Create your own application**.
5. Navngiv applikationen i feltet under *What's the name of your application?*

Tip: Navngiv evt. Applikationen Statens SSO.

6. Vælg **Integrate any other application you don't find in the gallery (Non-gallery)** under *What are you looking to do with your application?*
7. Klik på **Create** nederst på siden. Vent, mens applikationen oprettes. Det kan tage op til 30 sekunder.
8. Gå til Properties i sidemenuen under Manage.
9. Vælg **No** under *Assignment required?*

OBS: Når Assignment required? er sat til No, kræves der ikke en eksplicit tildeling af brugere eller grupper til Enterprise Application for at få adgang.

10. Klik på **Save**.
11. Klik på **Users and groups**.
12. Klik på **Add user/group** og tildel adgang til de relevante brugere eller grupper fra institutionens eget Microsoft Entra ID (Azure AD).

3. Konfiguration af SAML

Denne vejledning beskriver, hvordan SAML-forbindelsen konfigureres i Microsoft Entra ID ved hjælp af metadata og et krypteringscertifikat.

1. Klik på **Single sign-on** i sidemenuen under Manage.
2. Klik på **SAML**.
3. Hent den relevante metadata-fil:

SSO Miljø	Metadata
Test	https://statens-ss0-test.oes.dk/runtime/saml2auth/metadata.idp
Produktion	https://statens-ss0.oes.dk/runtime/saml2auth/metadata.idp

4. Klik på **Upload metadata file**, og upload metadata-filen.
5. Klik **Save**.

Tip: Kontrollér, at oplysningerne under *Basic SAML Configuration* stemmer overens med nedenstående:

- Identifier (Entity ID): <https://statens-ss0.oes.dk/runtime/>
- Reply URL (Assertion Consumer Service URL): <https://statens-ss0.oes.dk/runtime/saml2auth/consume.idp>
- Relay State: Optional
- Sign on URL: Optinal
- Logout URL (Optional): <https://statens-ss0.oes.dk/runtime/saml2auth/signoffrequest.idp>

6. Klik på **No I'll test later** i pop-up vindue.
7. Klik på **Token encryption** under Security i sidemenuen.
8. Hent det relevante encryption-certifikat (PROD eller TEST) fra Statens Single Sign-On på oes.dk.

Tip: certifikater findes under punkt 2. Institutioner – teknisk tilkobling (IdP)).

Højreklik på certifikatet, og vælg Gem link som. Vælg Alle filer (.) som filtype, og angiv et filnavn med filtypen .cer (fx certifikat.cer).

9. Klik på **Import Certificate**, og importer det hentede certifikat.
10. Klik **Add**.
11. Klik på de **tre prikker (...)** ud for certifikatet og vælg **Activate token encryption certificate**.
12. Klik **Yes**.

OBS: Kontrollér, at certifikatets status ændres til *Active*.

4. Konfiguration af claims (attributter)

Denne vejledning beskriver, hvordan de claims (attributter), der sendes til Statens SSO, konfigureres i Microsoft Entra ID.

1. Klik på **Single sign-on** i sidemenuen.
2. Klik på **SAML**.
3. Klik på **Edit** ud for Attributes & Claims.
4. Slet alle eksisterende Additional claims på listen. Klik på de **tre prikker (...)** ud for hvert claim, og vælg Slet.
5. Klik på **Unique User Identifier (Name ID)** under Required claims.
6. I feltet *Source attribute** angives *user.mail*.
7. Klik **Save**.
8. Klik på **Add new claim** for hvert claim (attribut), der skal oprettes. Udfyld claim-indstillingerne med værdierne fra nedenstående skema, og klik på **Save**. Gentag dette for hvert claim i skemaet.

OBS: For hvert claim angives værdierne fra kolonnerne Name, Namespace og Source attribute i de tilsvarende felter. Hvis Namespace-feltet er tomt i tabellen, skal feltet også være tomt i konfigurationen.

Name	Namespace	Source attribute
email	https://modst.dk/sso/claims	user.mail
userid	https://modst.dk/sso/claims	user.mail
uniqueid	https://modst.dk/sso/claims	user.objectid
mobile	https://modst.dk/sso/claims	user.mobilephone
surname	https://modst.dk/sso/claims	user.surname
givenname	https://modst.dk/sso/claims	user.givenname
Name		user.mail
cvr	https://modst.dk/sso/claims	<i>Indsat CVR nummer</i>
logonmethod	https://modst.dk/sso/claims	<i>Se særskilt beskrivelse nedenfor</i>
assurancelevel	https://modst.dk/sso/claims	<i>Se særskilt beskrivelse nedenfor</i>

Ved custom claims (assurancelevel og logonmethod) skal der angives den værdi i feltet *Source attribute*, som svarer til den valgte opsætning.

Tip: Hvis Azure-opsætningen allerede har to-faktorvalideret brugeren, skal følgende værdier vælges: Assurancelevel: "3" og Logonmethod: "username-password-protectedtransport".

Assurancelevel	
Source attribute	Beskrivelse
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.
Logonmethod	
Source attribute	Beskrivelse
username-password-protectedtransport	Username/Password login
kerberos-spnego	Ægte SSO via "Windows Integrated Authentication" (WIA)
two-factor	To faktor login

5. Fremsendelse af metadata URL og maildomæner

Denne vejledning beskriver, hvordan App Federation Metadata URL og maildomæner fremsendes til Økonomistyrelsen.

1. Log ind på <https://entra.microsoft.com/>.
2. Klik på **Single sign-on** i sidemenuen under Manage.
3. Klik på **SAML**.
4. Kopier **App Federation Metadata URL** under SAML certificates.
5. Fremsend App Federation Metadata URL og institutionens maildomæner til Økonomistyrelsen via Statens Administrations [Serviceportal](#) eller på sso@oes.dk.

Tip: Ved oprettelse sag via Statens Administrations Serviceportal vælges bestillingsblanket 'Øvrige', og herefter Single Sign On (SSO). Indsæt App Federation Metadata URL i feltet *Kort beskrivelse**.

6. Test af tilkobling til Statens SSO

Denne vejledning beskriver, hvordan tilkoblingen til Statens SSO testes.

Bemærk: Testen kan først gennemføres, når Økonomistyrelsen har færdigkonfigureret opsætningen og har givet besked om, at der kan testes. Beskeden gives via den valgte kommunikationskanal – enten via en sag på Statens Administrations Serviceportal eller pr. e-mail på sso@oes.dk.

1. Åbn Claimapp via linket til det relevante miljø nedenfor.

SSO Miljø	claimapp
Test	https://statens-sso-test.oes.dk/samlclaimapp1/MyPage.aspx
Produktion	https://statens-sso.oes.dk/samlclaimapp1/MyPage.aspx

2. Indtast **e-mailadresse**.
3. Opsæt 2-faktor (se evt. vejledning til opsætning af 2-faktor på oes.dk under punkt 1).
4. Kontrollér, at de modtagne claims er konfigureret korrekt i henhold til [afsnit 4](#).

Tip: Fremsend eventuelt et skærbillede af de modtagne claims til Økonomistyrelsen, hvis der er behov for hjælp til at kontrollere opsætningen.

7. Yderligere hjælp

Ved behov for yderligere hjælp kan du kontakte Serviceportalen.

Alle vejledninger til Statens SSO kan findes på oes.dk.

Hvis vejledningen ikke løser problemet, kan der oprettes en sag via Statens Administrations Serviceportal: <https://statens-adm.dk/support/serviceportalen/>

- For problemer med Statens SSO vælges bestillingsblanket 'Øvrige → Single Sign On (SSO)' på Serviceportalen.

Ved ingen adgang til Statens Administration serviceportal kan problem rapporteres til sso@oes.dk