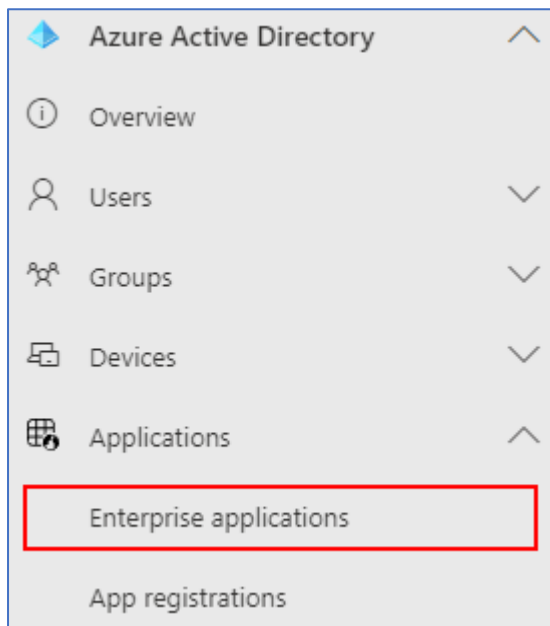
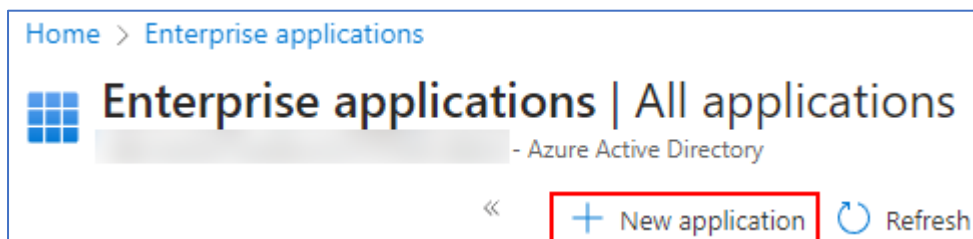


Statens SSO med Azure AD Enterprise Applications

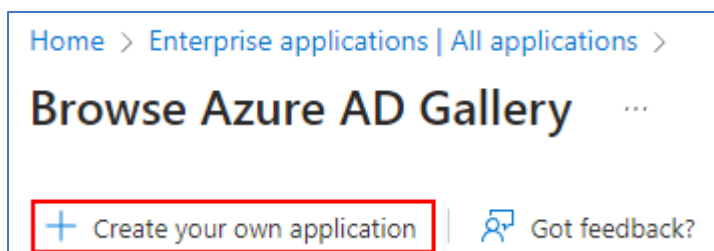
Log ind på <https://entra.microsoft.com/>



Klik på **Enterprise applications**



Klik på **New application**



Klik på **Create your own application**

Create your own application



Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Azure AD (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Giv din application et navn. F.eks. "Statens SSO"

Vælg **Integrate any other application you don't find in the gallery (Non-gallery)**

Klik på **Create** i bunden og vent på at applikationen er oprettet (op til 30 sekunder)

Statens SSO | Overview
Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Klik på **Single sign-on**

Statens SSO | Single sign-on ...
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

Klik på **SAML**

3 SAML Certificates

Token signing certificate Edit

Status Active

Thumbprint

Expiration

Notification Email

App Federation Metadata Url <https://login.microsoftonline.com/> ...

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Verification certificates (optional) Edit

Required	No
Active	0
Expired	0

Kopier **App Federation Metadata Url** og send denne til Økonomistyrelsen. Afvent metadata-fil og certifikat retur.

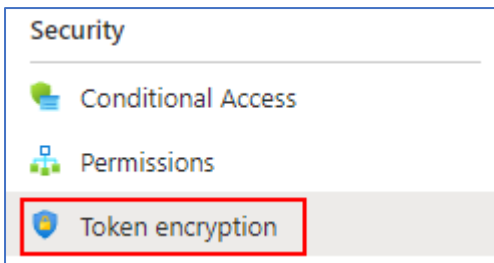
[Home](#) > [Enterprise applications | All applications](#) > [Statens SSO](#) >

Statens SSO | SAML-based Sign-on ...
Enterprise Application

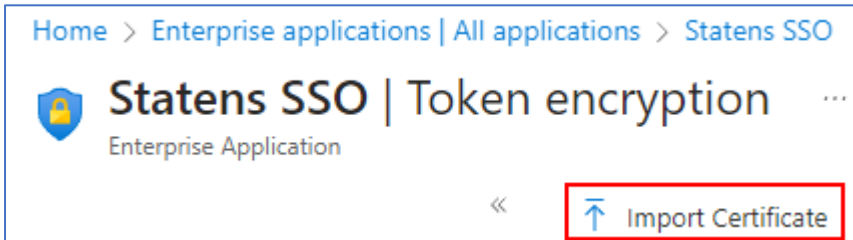
« [Upload metadata file](#) [Change single sign-on mode](#)

Klik på **Upload metadata file**, og upload Økonomistyrelsens metadata-fil:

Miljø	Metadata
Test:	https://statens-sso-test.oes.dk/runtime/saml2auth/metadata.idp
Prod:	https://statens-sso.oes.dk/runtime/saml2auth/metadata.idp



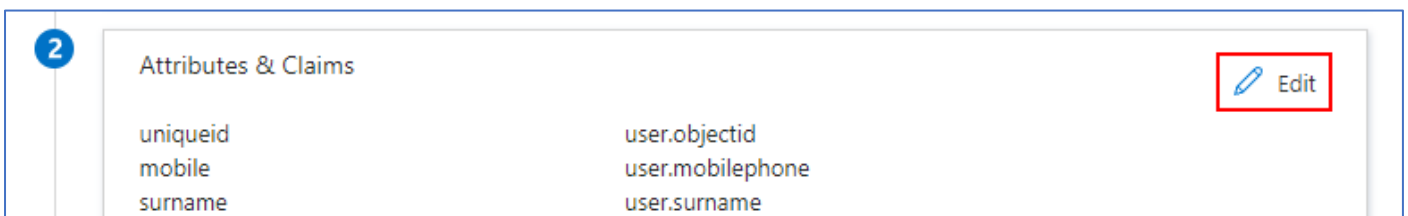
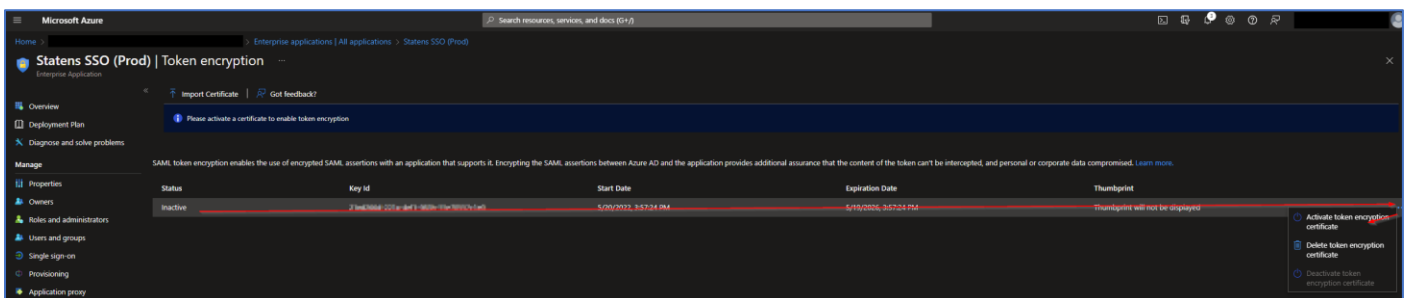
Klik på **Token encryption**



Klik på **Import Certificate** og importer det certifikat som findes på Økonomistyrelsen website.

<https://oes.dk/digitale-loesninger/statens-single-sign-on/den-kommende-sso-loesning/>

Sørg for at "Encryption certificate" er aktiveret



Klik på **Single sign-on** i sidemenuen og så på **Edit** ud for **Attributes & Claims**

Additional claims			
Claim name	Type	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname	...

Slet alle **Additional claims** på listen ved at klikke på prikkerne i højre side

Attributes & Claims ...

[+ Add new claim](#) [+ Add a group claim](#) [≡ Columns](#) | [Got feedback?](#)

Klik på **Add new claim**

Manage claim ...

[Save](#) [Discard changes](#) | [Got feedback?](#)

Name *	userid
Namespace	https://modst.dk/sso/claims
Choose name format	
Source *	☒ Attribute ☐ Transformation ☐ Directory schema extension (Preview)
Source attribute *	user.mail

Udfyld claim indstillingerne ud fra nedenstående skema fra Økonomistyrelsen.

Klik på **Save** for at gemme

Name	Source attribute
https://modst.dk/sso/claims/email	user.mail
https://modst.dk/sso/claims/userid	user.mail
https://modst.dk/sso/claims/uniqueid	user.objectid
https://modst.dk/sso/claims/mobile	user.mobilephone
https://modst.dk/sso/claims/surname	user.surname
https://modst.dk/sso/claims/givenname	user.givenname
Name	user.mail
https://modst.dk/sso/claims/cvr	Indsæt CVR nummer
https://modst.dk/sso/claims/logonmethod	Læs herunder
https://modst.dk/sso/claims/assurancelevel	Læs herunder

Ved custom claims (assurancelevel og logonmethod) skal du skrive de værdier under **"Source attribute"** som svarer til den opsætning du kører med.

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

I et Azure setup hvor man allerede har to-faktor valideret brugeren, skal følgende værdier vælges:

Assurancelevel: 3

Logonmethod: username-password-protectedtransport

Den færdige opsætning kan se ud som nedenstående:

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
https://modst.dk/sso/claims/assurancelevel	SAML	"3"
https://modst.dk/sso/claims/cvr	SAML	"54256123"
https://modst.dk/sso/claims/email	SAML	user.mail
https://modst.dk/sso/claims/givenname	SAML	user.givenname
https://modst.dk/sso/claims/logonmethod	SAML	"username-password-pr..."
https://modst.dk/sso/claims/mobile	SAML	user.mobilephone
https://modst.dk/sso/claims/surname	SAML	user.surname
https://modst.dk/sso/claims/uniqueid	SAML	user.objectid
https://modst.dk/sso/claims/userid	SAML	user.mail
Name	SAML	user.mail

Vælg properties på applikationen og sæt "Assignment required?" til "No".