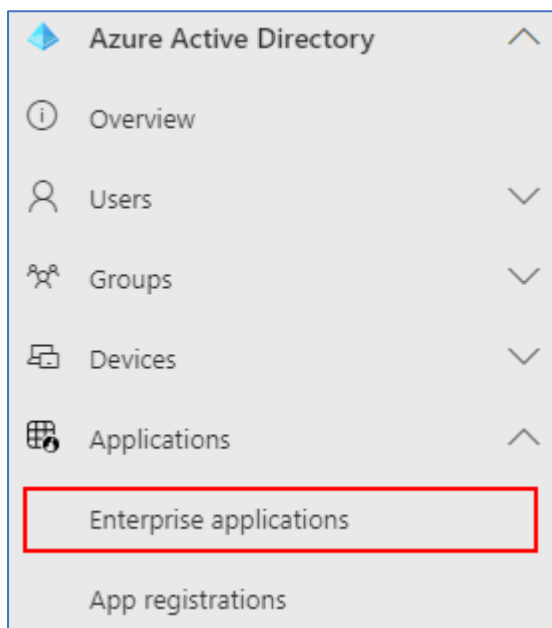
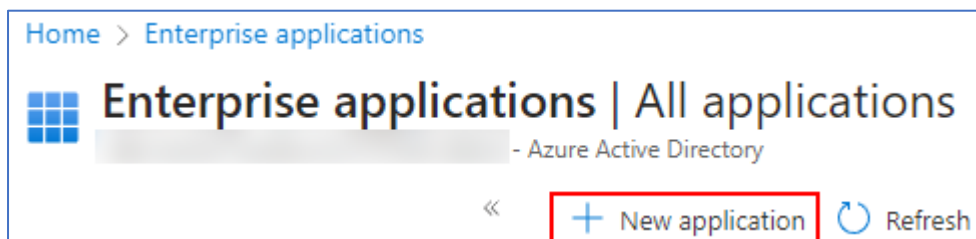


Statens SSO med Azure AD Enterprise Applications

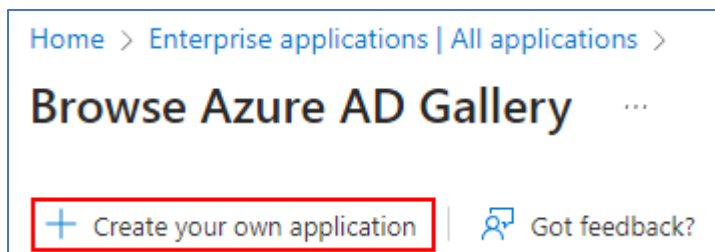
Log ind på <https://entra.microsoft.com/>



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?

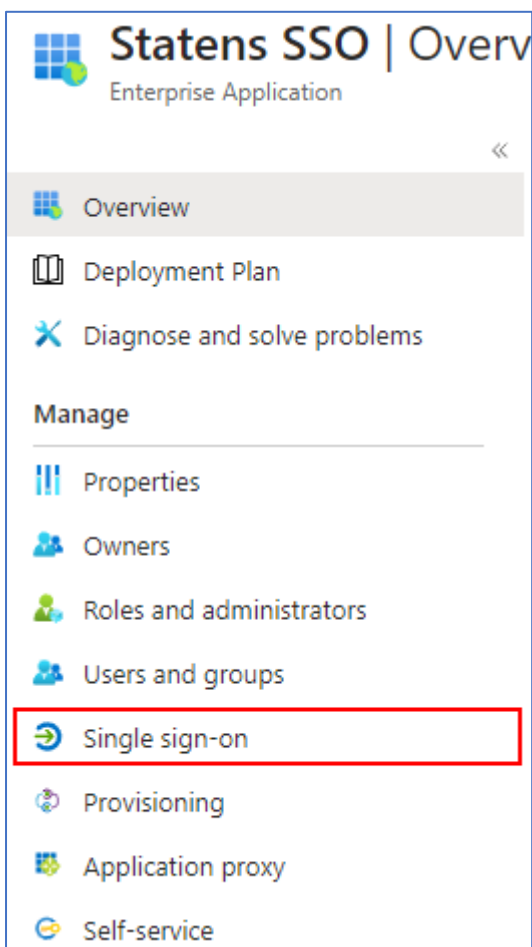
What are you looking to do with your application?

- 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)



The screenshot shows the Azure AD portal interface for an application named "Statens SSO | Overview". The page title is "Statens SSO | Overview" and the subtitle is "Enterprise Application". The left-hand navigation menu is visible, with the following items: Overview (selected), Deployment Plan, Diagnose and solve problems, Manage (header), Properties, Owners, Roles and administrators, Users and groups, Single sign-on (highlighted with a red box), Provisioning, Application proxy, and 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

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

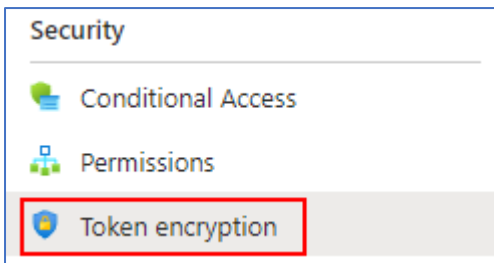
Kopier **App Federation Metadata Url** og send denne til Økonomistyrelsen. Afvent metadata-fil og certifikat retur.

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

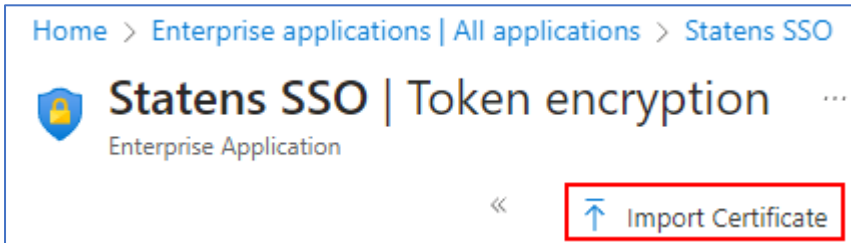
Statens SSO | SAML-based Sign-on ...
Enterprise Application

« ↑ Upload metadata file ↻ Change single sign-on mode »

Klik på **Upload metadata file**, og upload metadata-filen som Økonomistyrelsen har returneret.

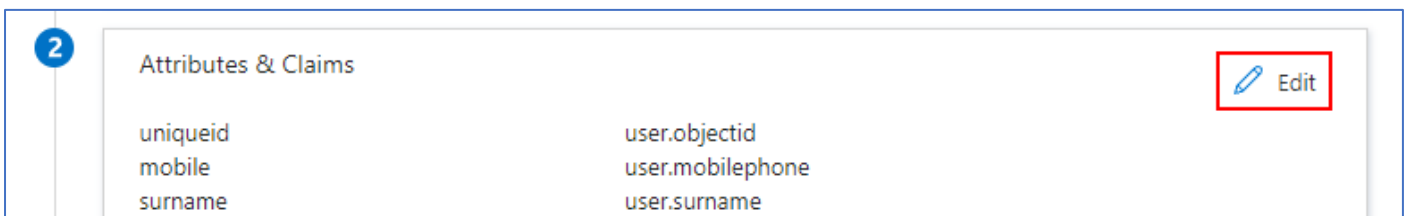
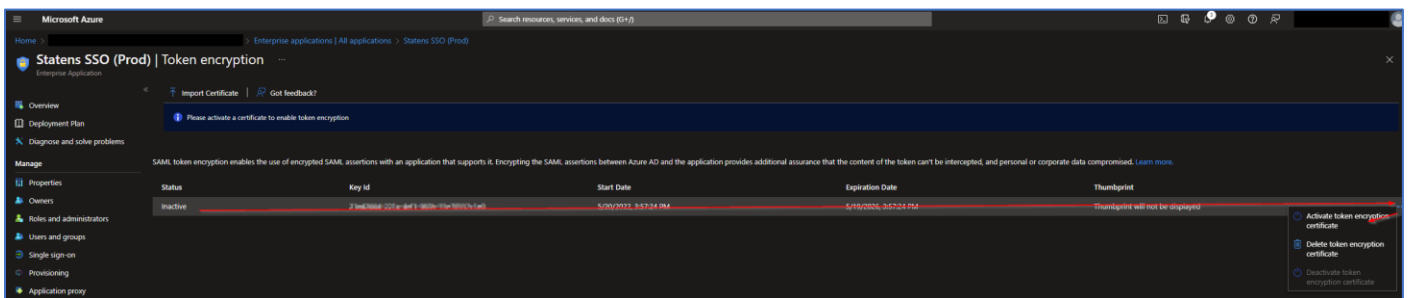


Klik på **Token encryption**



Klik på **Import Certificate** og importer det certifikat som Økonomistyrelsen har returneret.

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 *	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation <input type="radio"/> 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/assurancelevel	Læs herunder
https://modst.dk/sso/claims/logonmethod	Læs herunder
https://modst.dk/sso/claims/cvr	Læs herunder

Ved custom claims (assurancelevel, logonmethod og CVR) kan extensionattributes i on-premise AD bruges og synces til Azure via Azure AD Connect.

Vi har valgt at bruge henholdsvis extensionattributes 13, 14 og 15 til dette formål.

Assurancelevel

Værdi	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

Værdi	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, kan følgende værdier vælges:

Assurancelevel: 3

Logonmethod: username-password-protectedtransport

Følgende PowerShell script kan benyttes til at sætte extensionattributes for alle brugere i en given OU:

```
$OU = Get-ADUser -Filter * -SearchBase "OU=afdeling,DC=contoso,DC=local"

$assurancelevel = "indsæt assurancelevel her"
$logonmethod = "indsæt logonmethod her"
$cvr = "indsæt cvr-nummer her"

foreach ($user in $OU) {
    <#
    CLEAR ATTRIBUTES FIRST TO OVERWRITE EXISTING
    Set-ADUser -Identity $user -Clear "extensionAttribute13"
    Set-ADUser -Identity $user -Clear "extensionAttribute14"
    Set-ADUser -Identity $user -Clear "extensionAttribute15"
    #>

    Set-ADUser -Identity $user -Add @{extensionAttribute13 = $assurancelevel}
    Set-ADUser -Identity $user -Add @{extensionAttribute14 = $logonmethod}
    Set-ADUser -Identity $user -Add @{extensionAttribute15 = $cvr}
}
```

En scheduled task kan eventuelt oprettes med ovenstående script.

Den færdige opsætning kan se ud som nedenstående:

Required claim		
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [nameid-format:emailAddress]
Additional claims		
Claim name	Type	Value
https://modst.dk/sso/claims/assurancelevel	SAML	user.extensionattribute13
https://modst.dk/sso/claims/cvr	SAML	user.extensionattribute15
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	user.extensionattribute14
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".