

Guiden som viser **IT-**  
**avdelingen** hvordan dere  
får til **SSO** på Compendias  
løsninger



Denne korte guiden viser steg for steg hva som skal til for at dere kan komme i gang med SSO.

## Hva er SSO (Single Sign-On)?

SSO betyr at brukeren kan logge inn med samme brukernavn/passord på alle digitale tjenester. Altså kun én innlogging.

Det gjør administrasjonen enklere, og fjerner hindringer for brukeren. SSO gir tilgang til systemet fra hvor som helst, og dere kan sende lenker på e-post uten å bekymre dere for om de ansatte får til å åpne dem.

## Krav for å starte med SSO

En må benytte Azure AD eller annen standard som benytter SAML-protokollen.

Compendia støtter disse tjenestene:

- Azure AD
- Feide
- Microsoft ADFS
- Annen SAML federering(Pingfederate)

Er en av disse satt opp i din virksomhet? Da er dere klare 😊

## Attributter som må sendes

Vi trenger e-post, fornavn, etternavn og mobilnummer. Skal dere ha avvikssystem også, trenger vi i tillegg avdelings-attributtet.

## Det var det Våre konsulenter bistår i testingen

Vi i Compendia har flere SSO-eksperter som hjelper dere med testingen. Vi tar en kort gjennomgang med IT og sammen tester vi at løsningen virker.

## Trenger du å gjøre noen avklaringer?

Gjengen på support svarer deg på alle dine SSO-spørsmål. Ta kontakt på [support@compendia.no](mailto:support@compendia.no), 40 00 59 30 eller chat med oss på [compendia.no](https://compendia.no).

## Installasjonsveiledning: Azure AD

Configuring Azure Active Directory as a SAML Identity Provider for Compendia – Compublish WebApp







1. Connect to Azure tenant with Azure AD Global Administrator account rights. Navigate to Azure Active Directory.



Azure Active  
Directory

2. Under Manage, click Enterprise application.

## Manage

-  Users
-  Groups
-  Organizational relationships
-  Roles and administrators
-  Enterprise applications
-  Devices


3. Click New application and select Non-gallery application. Enter a Name and click Add.



## Enterprise applications - All applications



Standardmappe - Azure Active Directory



 New application

 Columns

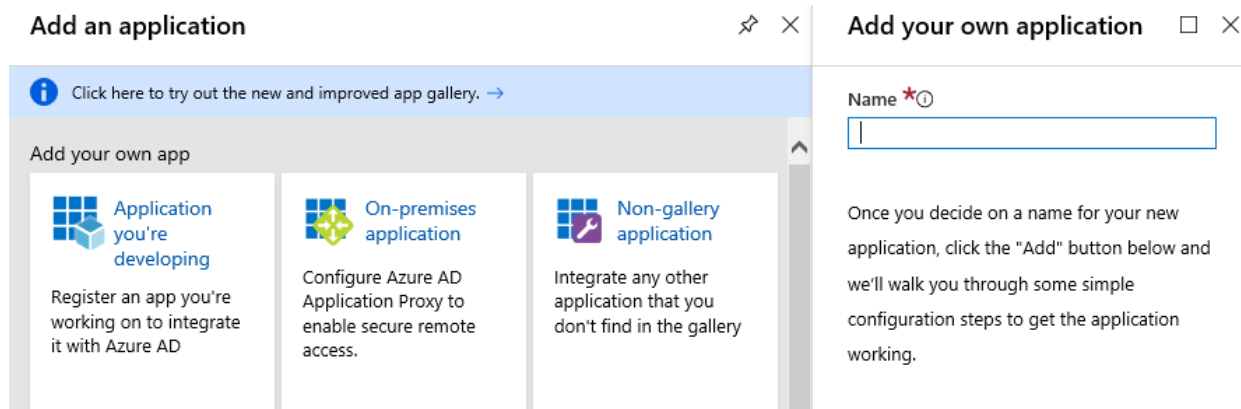
### Overview

-  Overview
-  Diagnose and solve problems

### Application Type

Enterprise Applications

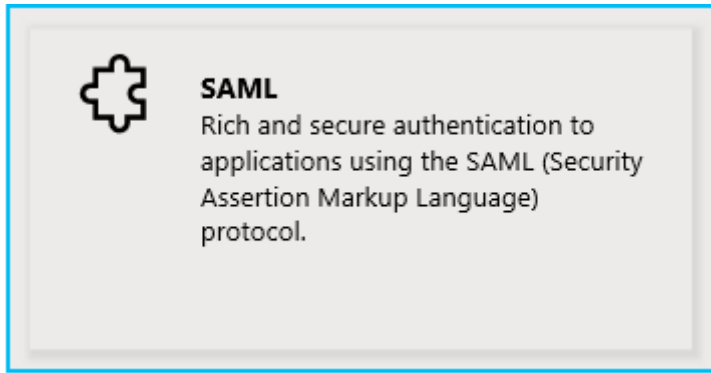




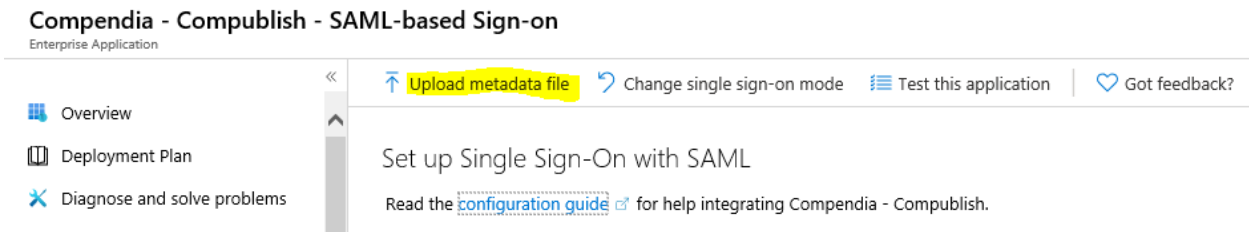
4. Click your new created application.




5. Under Select a single sign-on method, select SAML.




6. Under “your application name” - SAML-based Sing-on click Upload metadata file.



7. Navigate to xml file from Compendia and click add.This will fill Identifier and Reply URL provided by Compendia.

Basic SAML Configuration 	
Identifier (Entity ID)	https://saml.compendia.no/saml/g/13/metadata
Reply URL (Assertion Consumer Service URL)	https://saml.compendia.no/saml/g/13/consumer
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

User Attributes & Claims 	
Mobile	user.telephonenumber
Email	user.mail
FirstName	user.givenname
Name	user.userprincipalname
SecondName	user.surname
Unique User Identifier	user.userprincipalname

Click the pencil icon for **User Attributes & Claims**.

8. Add new claim.

### User Attributes & Claims

---

+ Add new claim
+ Add a group claim
☰ Columns

9. Set name to mobile and in Source attribute choose user.telephonenumber.

## Manage claim

 Save  Discard changes

Name \*  ✓

Namespace

Source \*  Attribute  Transformation

Source attribute \*  ▼

▼ Claim conditions

10. Click to others default created claims and remove Namespace “path” from all of them.

## Manage claim

 Save  Discard changes

Name \*  ✓



Namespace

Source \*  Attribute  Transformation

Source attribute \*  ▼



11. Click Download Federation Metadata XML.


SAML Signing Certificate 	
Status	Active
Thumbprint	BA97ED2FC1CF1115351C0D4ECCA208604933C72E
Expiration	11/14/2022 2:05:18 PM
Notification Email	robert.priczel@gmail.com
App Federation Metadata Url	<a href="https://login.microsoftonline.com/43b5d745-ef27-4...">https://login.microsoftonline.com/43b5d745-ef27-4...</a> 
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
<b>Federation Metadata XML</b>	<b><a href="#">Download</a></b>

12. This will download XML file to your computer. Send this file to Compendia.

13. Copy and sent Login URL, Azure AD Identifier and Logout URL to Compendia.

#### Set up Compendia - Compublish

You'll need to configure the application to link with Azure AD.

Login URL	<a href="https://login.microsoftonline.com/43b5d745-ef27-4...">https://login.microsoftonline.com/43b5d745-ef27-4...</a> 
Azure AD Identifier	<a href="https://sts.windows.net/43b5d745-ef27-498d-938d...">https://sts.windows.net/43b5d745-ef27-498d-938d...</a> 
Logout URL	<a href="https://login.microsoftonline.com/common/wsfede...">https://login.microsoftonline.com/common/wsfede...</a> 

[View step-by-step instructions](#)

14. Click Users and group and add access to application for users or groups of your choosing.



# Compendia - Compublish - Users and groups

Enterprise Application

<< **+ Add user** Edit Remove Update Credentials Columns

**i** The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in pro

First 100 shown, to search all users & groups, enter a display name.

Display Name



- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage**
- Properties
- Owners
- Users and groups**
- Single sign-on