

Opsætning af AD FS på SaaS-miljø

Formål

Dokumentet beskriver opsætningen af AD FS i forbindelse med XFlow som en SaaS-løsning.

Opsæt relying party trust

Du skal oprette SaaS AD FS serveren som relying party trust. Dette gør du ved at starte relying party trust guiden og indtaste AD FS serverens federation metadata URL.

<https://adfs.firstagenda.biz/FederationMetadata/2007-06/FederationMetada...>

Følg herefter guiden på skærmen.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

Import data about the relying party published online or on a local network
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

Import data about the relying party from a file
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

Enter data about the relying party manually
Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

Opsæt claims

Du skal opsætte claims, så de korrekte informationer kommer til XFlow.

XFlow forventer claimet "E-mail Address" til identifikation af brugeren.

Om claims

Opsætningen af claims er helt afhængig af din claims provider. Der er ingen endegyldig løsning, og de nødvendige oplysninger kan variere fra claims provider til claims provider.

Hvis der opstår problemer, er du velkommen til at kontakte supporten. Supporten kan hjælpe med Active Directory og Office 365.

Typiske eksempler

Active Directory

Hvis du benytter Active Directory som claims provider, skal du oprette en claim rule ud fra template "Send LDAP Attributes as Claims". "LDAP Attribute" skal sættes til den attribut i Active Directory, hvor brugernes e-mail adresse ligger. "Outgoing Claim Type" skal være "E-mail Address".

Office 365

Hvis du benytter Office 365, skal du oprette et pass through på "Name" claimet og benytte en transform rule, så udgående claim bliver af typen "E-mail Address".

Edit Rule - Name to E-Mail Address



You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Name to E-Mail Address

Rule template: Transform an Incoming Claim

Incoming claim type: Name

Incoming name ID format: Unspecified

Outgoing claim type: E-Mail Address

Outgoing name ID format: Unspecified

- Pass through all claim values
- Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

- Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com