

OS2MO ADFS Mini Guide

Indholdsfortegnelse

1 Opsætning af ADFS-serveren.....	2
1.1 Viborg.....	2
1.1.1 Opret en ny Claims Aware Relaying Party Trust.....	2
1.1.2 Indsæt Metadata URL for serveren.....	3
1.1.3 Giv forbindelsen et navn.....	4
1.1.4 Bonus info om opsætningen i Viborg Kommune.....	5
1.2 Bonus info om opsætningen i Holstebro Kommune.....	6

1 Opsætning af ADFS-serveren

1.1 Viborg

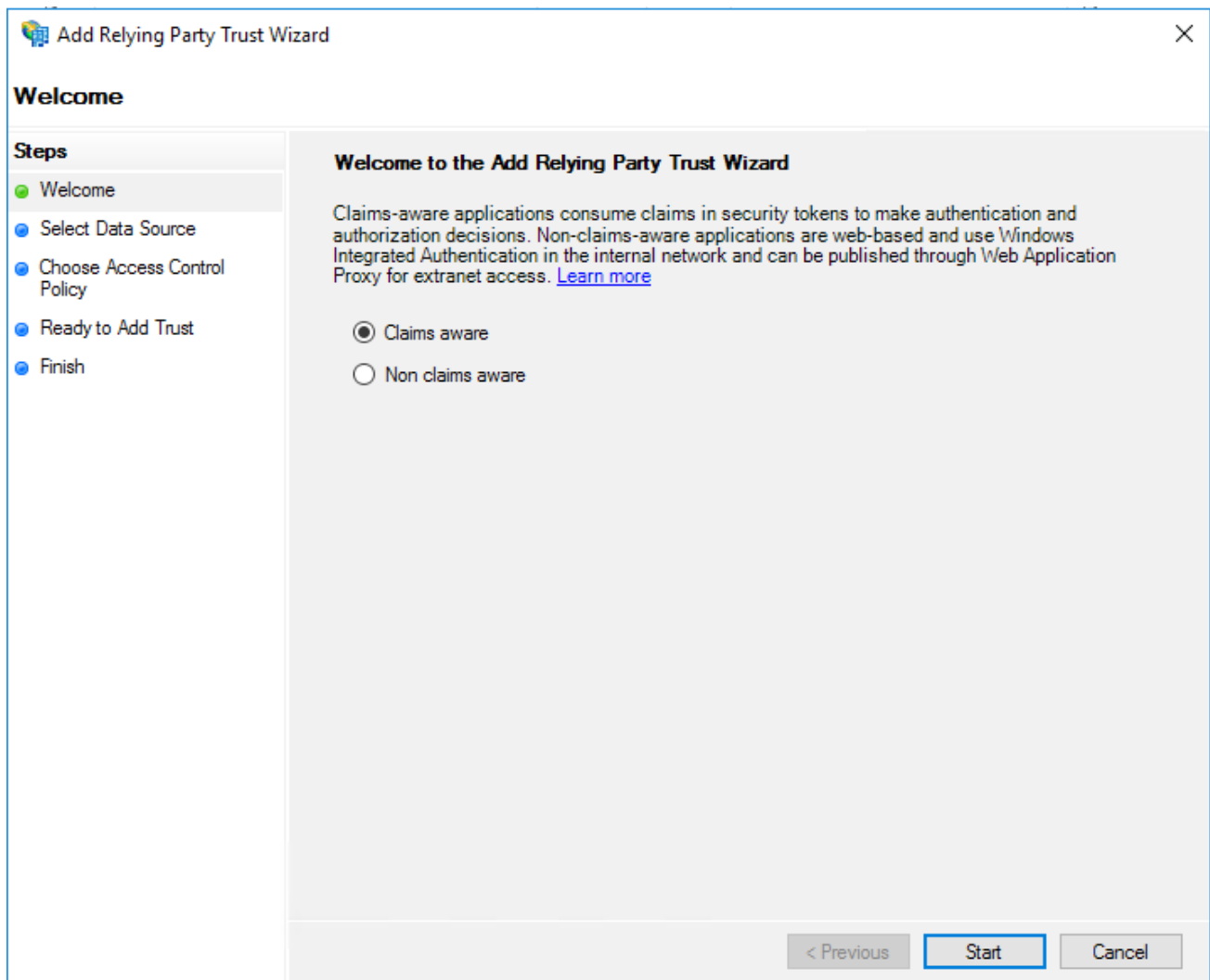
Selve opsætningen af ADFS serveren er relativt simpel.

I skal bruge en Metadata adresse på OS2MO Serveren.

I dette tilfælde er vores OS2MO server opsat til at køre SSL igennem vores Load Balancer.

I dette eksempel er adressen: <https://devos2mo.testdomian.dk/saml/metadata/>

1.1.1 Opret en ny Claims Aware Relaying Party Trust



Add Relying Party Trust Wizard

Welcome

Steps

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

Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. [Learn more](#)

☒ Claims aware

☐ Non claims aware

< Previous Start Cancel

1.1.2 Indsæt Metadata URL for serveren

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

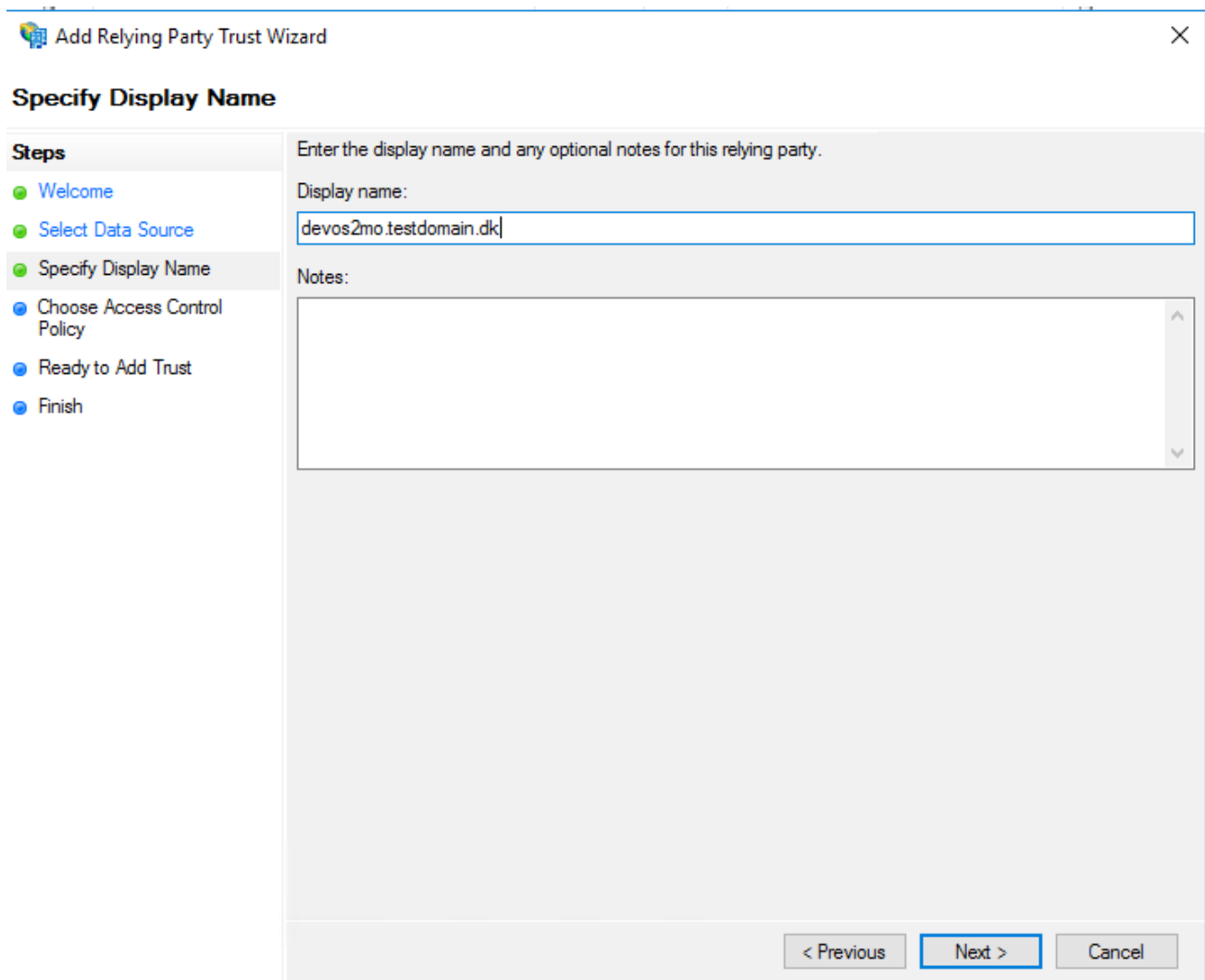
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

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.

1.1.3 Giv forbindelsen et navn

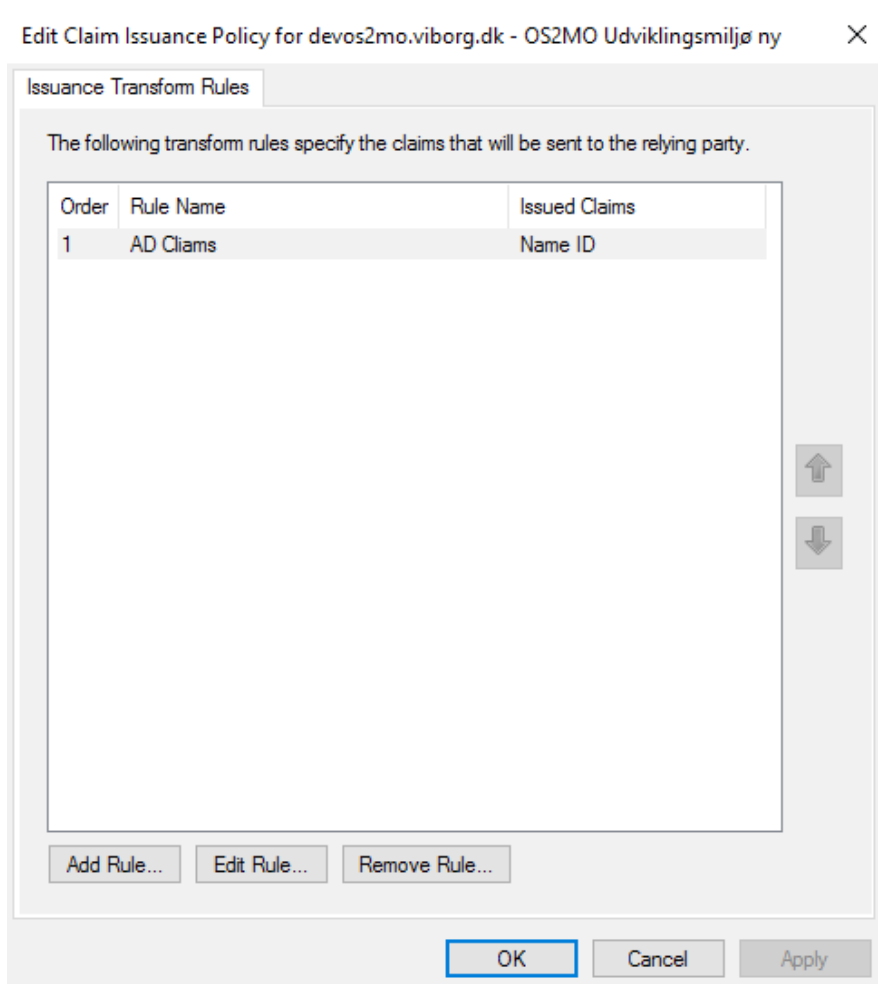


The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: 'Welcome' (green circle), 'Select Data Source' (green circle), 'Specify Display Name' (green circle and highlighted), 'Choose Access Control Policy' (blue circle), 'Ready to Add Trust' (blue circle), and 'Finish' (blue circle). The main area contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label and a text box containing 'devos2mo.testdomain.dk'. Underneath is a 'Notes:' label and a large, empty text area with a vertical scrollbar. At the bottom right, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Herefter vælges ønsket Access Control Policy og opsætningen færdiggøres.

Der skal nu opsættes et Claim på forbindelsen.

Dette Claim bruges p.t. kun til at vise brugerens Navn i toppen af OS2MO hjemmesiden.



1.1.4 Bonus info om opsætningen i Viborg Kommune

Vi havde i Viborg en del udfordringer med at få vores forbindelse til at virke korrekt.

Fra OS2MO blev der udgivet en Metadata der indeholdt forkerte informationer i forhold til forbindelsessikkerheden. (Endpoints blev angivet som http og ikke https som de skulle).

Ovenstående oplysning kan ses under Endpoints i Egenskaber for Relaying Party Trust for OS2MO ADFS forbindelsen.

Vores Netværk Team har opsat en Load Balancer foran Serveren der tager http forbindelsen fra OS2MO og laver den om til en HTTPS-forbindelse med et egnet certifikat.

Dette kan også gøres med et NGINX Reverse Proxy opsætning, jeg ved Magenta har implementeret noget NGINX Reverse Proxy i OS2MO udgivelsen fra midt i marts.

Vi havde i starten lidt udfordringer med at Secure Hash Algorithm for OS2MO ikke var sat til SHA-256 fra Magenta side, det kan måske være i skal høre Magenta om dette er tilfældet ved jer.

Secure Hash Algorithm kan ændres under Advanced i egenskaber for Relaying Party Trust for OS2MO ADFS forbindelsen.

1.2 Bonus info om opsætningen i Holstebro Kommune

Magenta installerede autentificerings komponenten på OS2MO serverne.

Vi afleverede vores ADFS metadata endpoint til Magenta, så Magenta kunne få peget OS2MO serverne på vores ADFS. Det findes her i ADFS:

- Udvid *Service*
- Vælg *Endpoints*
- Find et endpoint af typen: Federation Metadata
- Aflæs URL Path hertil
 - o Eksempel:
`https://adfs.testdomain.dk/FederationMetadata/2007-06/
FederationMetadata.xml`

Vi har begrænset adgangen til OS2MO, så det kun er brugere som er medlem af en bestemt AD gruppe som må tilgå siden. Dette gøres på følgende måde:

- Udvid *Trust Relationships*
- Vælg *Relying Party Trusts*
- Højreklik på det ønskede trust
- Klik *Edit Claim Rules*
- Vælg *Issuance Authorization Rules* fanen
- Slet "Permit Access To All Users" reglen
- Klik *Add Rule*
- Vælg *Permit or Deny Users Based on an Incoming Claim*
- Under *Incoming Claim Type*, vælg *Group SID*
- Klik *Browse* ved *Incoming claim value*
- Vælg den ønskede gruppe