Wolters Kluwer

ADFS Single Sign on (SSO)

Configuration Guide

Wolters Kluwer

About this guide

The purpose of this guide is to help technical users to configure XCM as relying party and enable Single Sign on (SSO) in Active Directory Federation Services (AD FS) and Azure.

This guide does not explain how to install and configure AD FS. Users of this guide should have an understanding about AD FS, SSO and SAML.

Related References

https://en.wikipedia.org/wiki/Active_Directory_Federation_Services

https://en.wikipedia.org/wiki/Single_sign-on

https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

https://en.wikipedia.org/wiki/SAML_2.0

Typographical Convention

This guide uses the following convention:

Convention	Meaning
Bold text	User interface elements that allow the user to control the interface.
Italic type	Important information to the user.

Introduction to Single Sign on and ADFS

Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers. A simple version of single sign-on can be achieved over IP networks using cookies but only if the sites share a common DNS parent domain.

Active Directory Federation Services (AD FS), a software component developed by Microsoft, can run on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access-control authorization model to maintain application security and to implement federated identity. Claims-based authentication involves authenticating a user based on a set of claims about that user's identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims-based authentication. It is part of the Active Directory Services.

Configuring SSO in AD FS

XCM Platform includes a Data Import-Export web application tool, using this tool the customer service representative team will be able to import CPA firm’s data into XCM.

Follow the procedure below to configure SSO in AD FS:

Prerequisites:

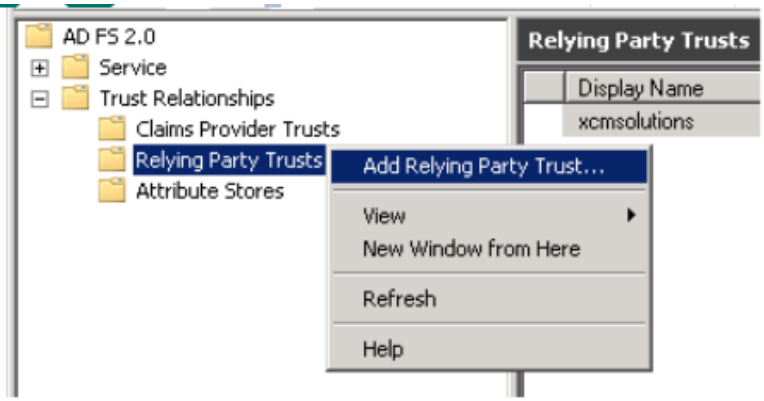
Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2 or Windows Server 2016 with Active directory and AD FS installed and running.

Procedure:

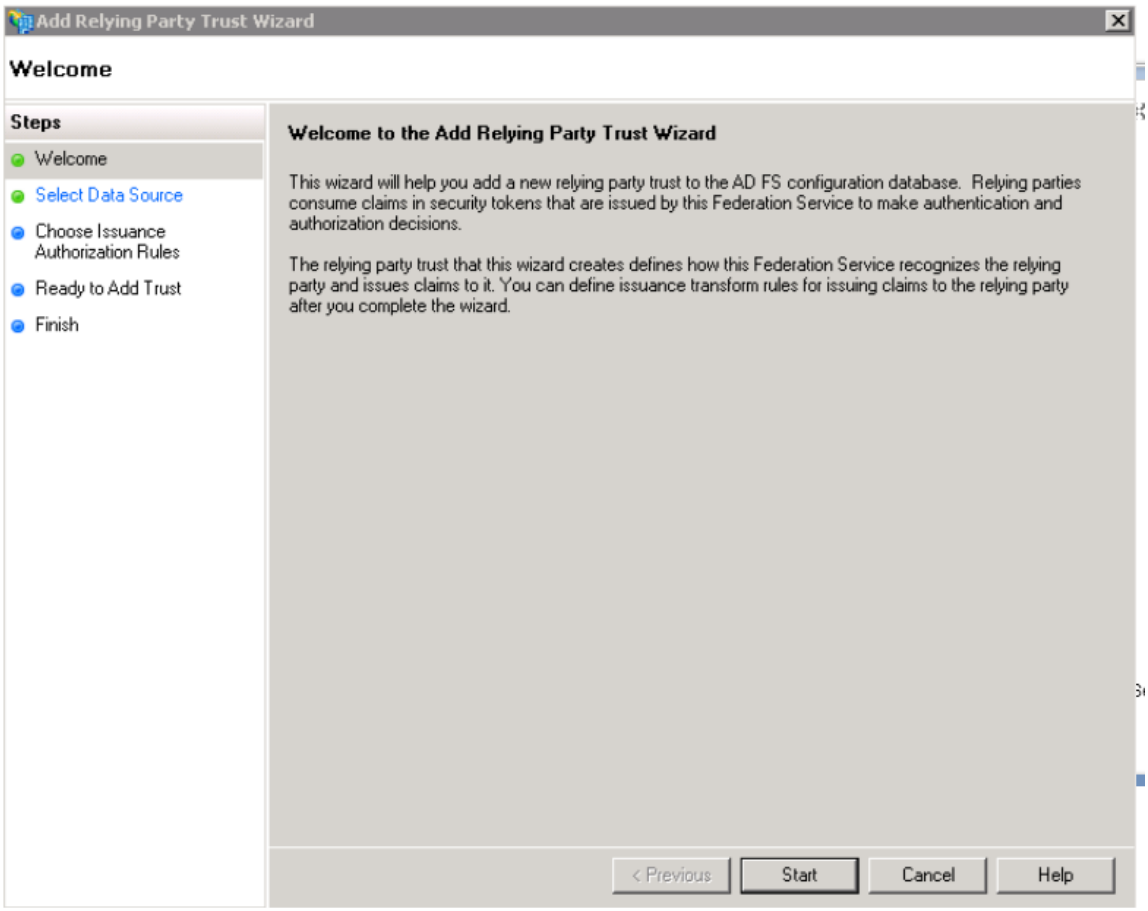
Click the **Start** button and select **AD FS 2.0 Management**. AD FS 2.0 window opens.

In the AD FS 2.0 window, click the plus sign next to **Trust Relationships** folder. The folder expands.

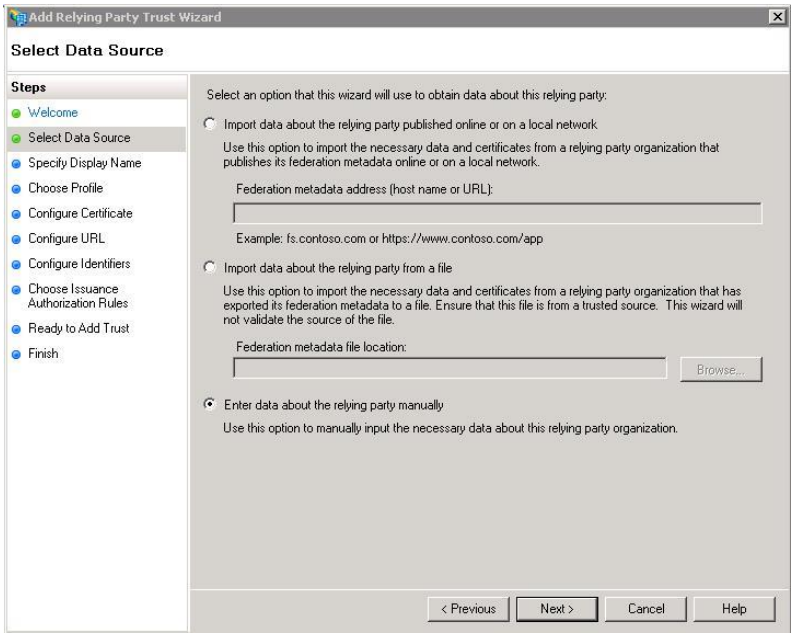
Right click **Relying Party Trusts** folder, click **Add Relying Party Trust.** The Add Relying Party Trust Wizard dialog box starts.



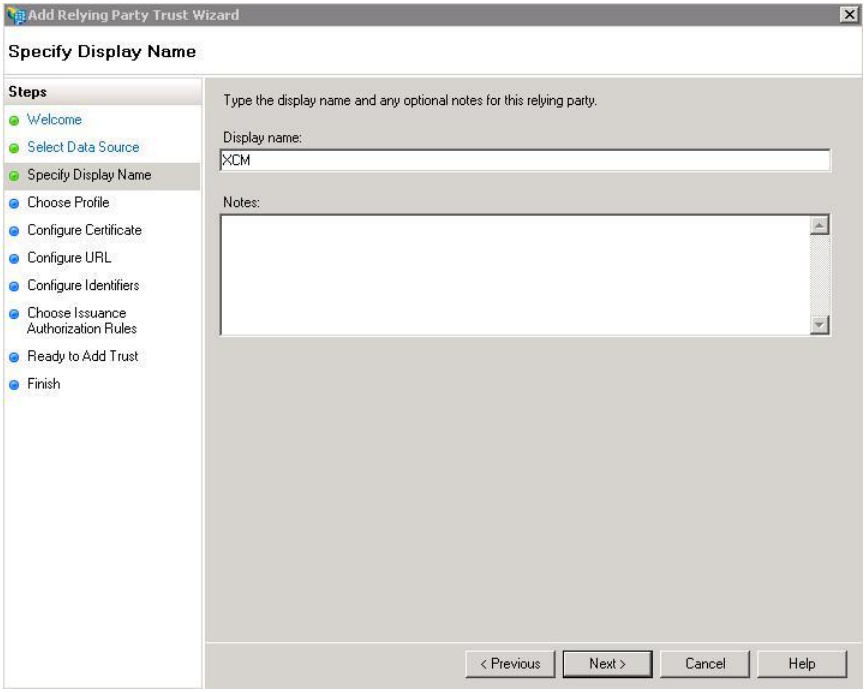
In the **Add Relying Party Trust Wizard**, click **Start**.



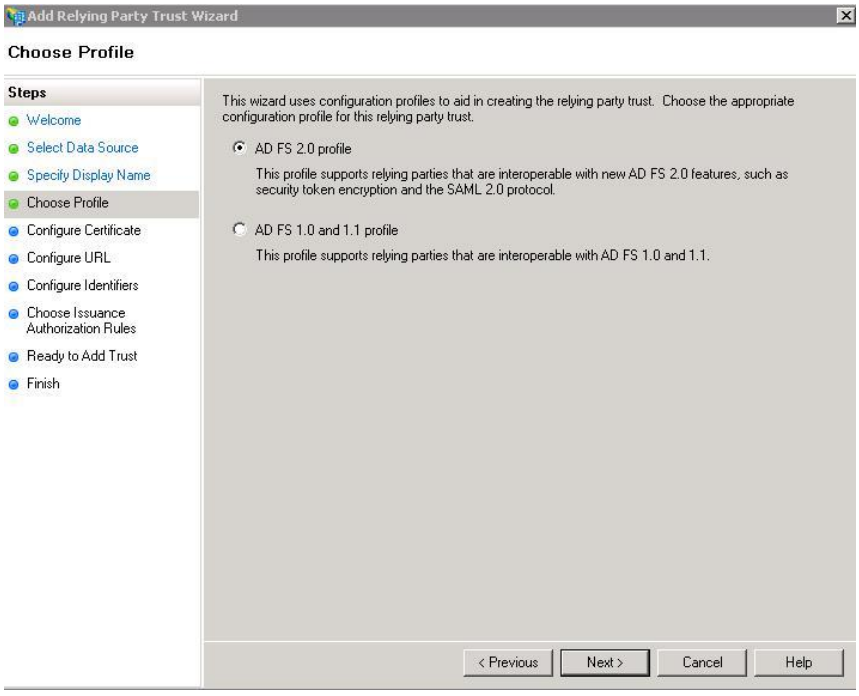
In the **Select Data Source** tab, select **Enter data about the relying party manually** and click **Next**.



6. Enter the **Display name** and **Notes** to identify the relying party, click **Next**.

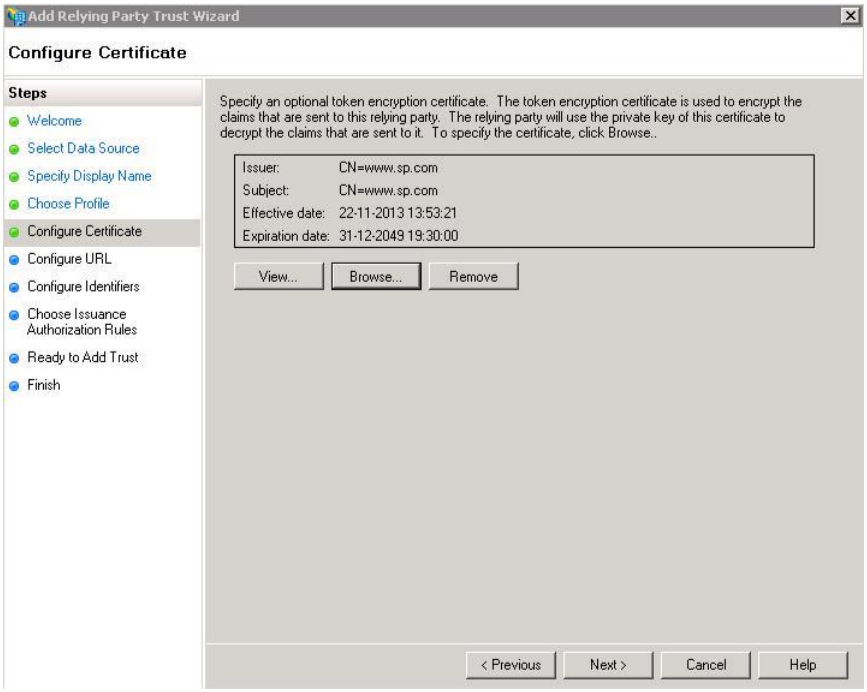


In the **Choose Profile** tab, select **AD FS 2.0 profile**, click **Next**. AD FS 2.0 profile is selected by default.

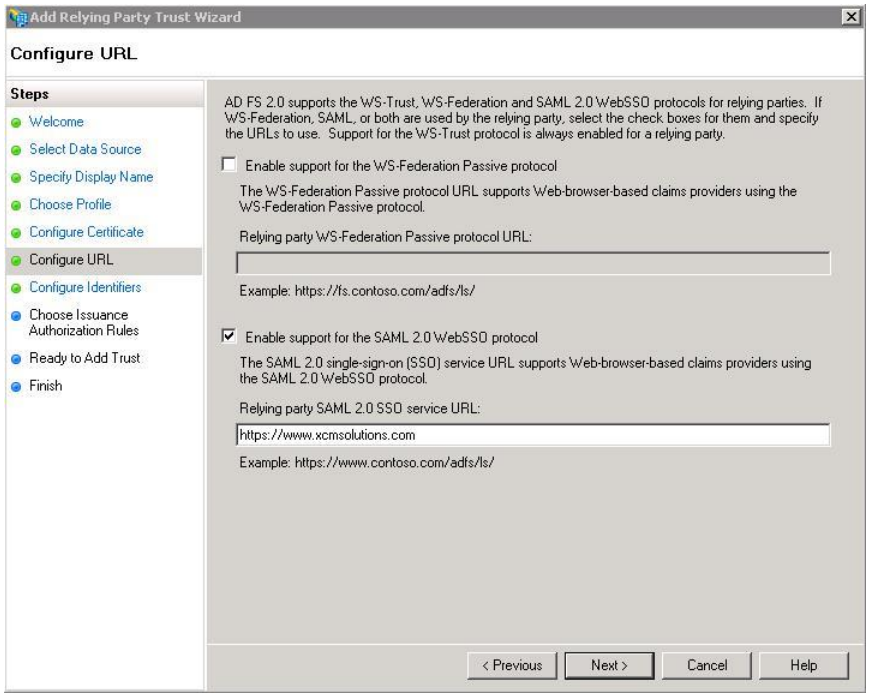


In the **Configure Certificate** tab, browse and open the token encryption certificate, click **Next**.

Note: XCM customer service representative or your point of contact will share the token encryption certificate.

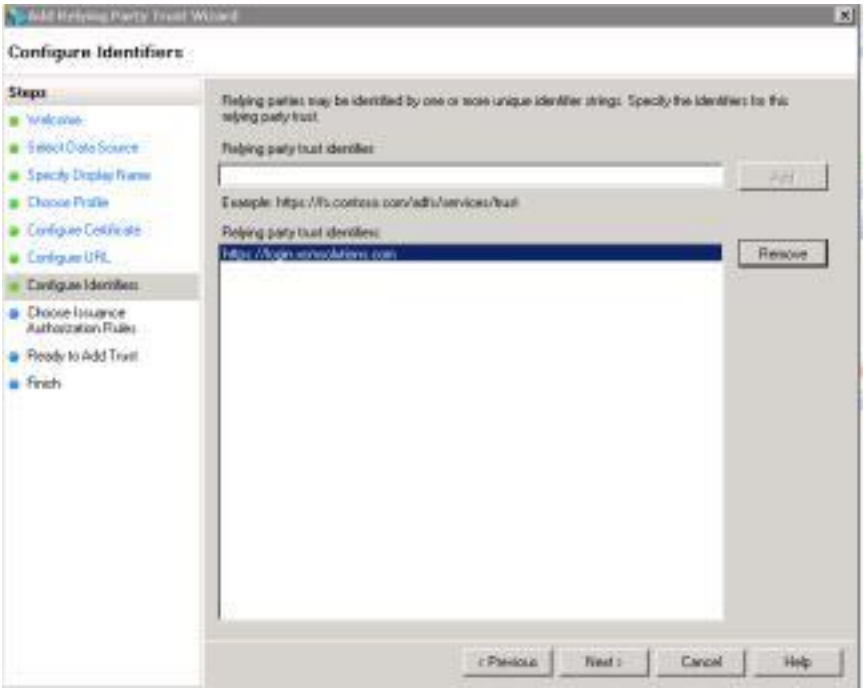


In the **Configure URL** tab, select **Enable support for the SAML 2.0 WebSSO protocol** and enter the **Relying party SAML 2.0 SSO service URL**, click **Next**.

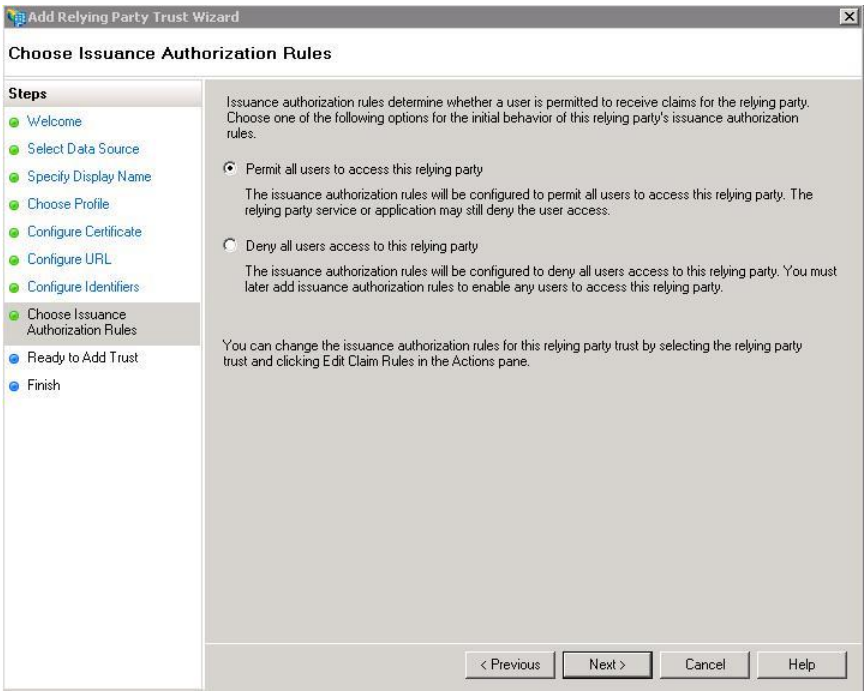


10. In the **Configure Identifiers** tab, enter the relying party trust identifier.
Click **Add** and click **Next**.

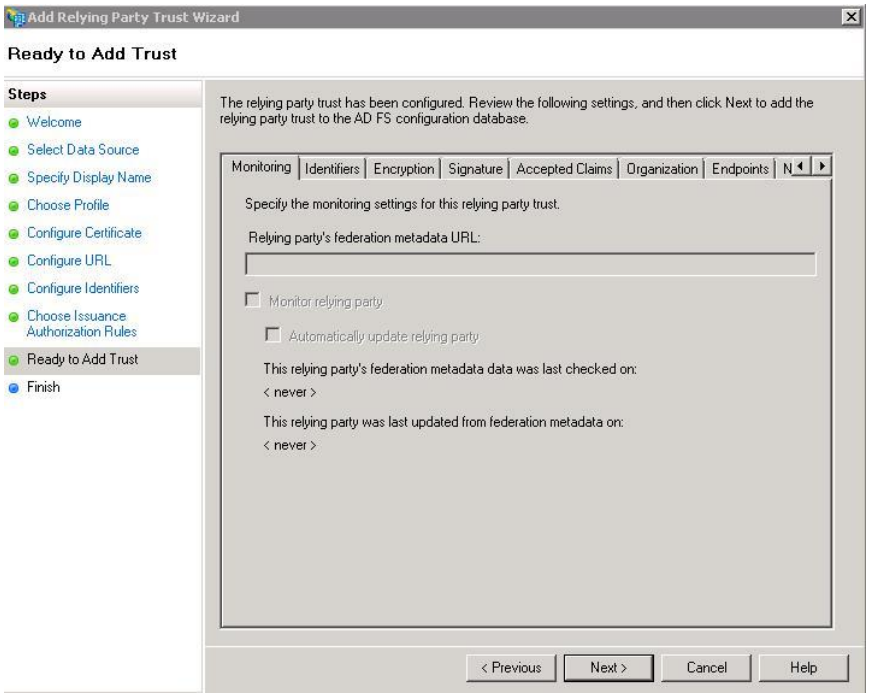
Note: XCM customer service representative or your point of contact will share the relying party trust identifier details.



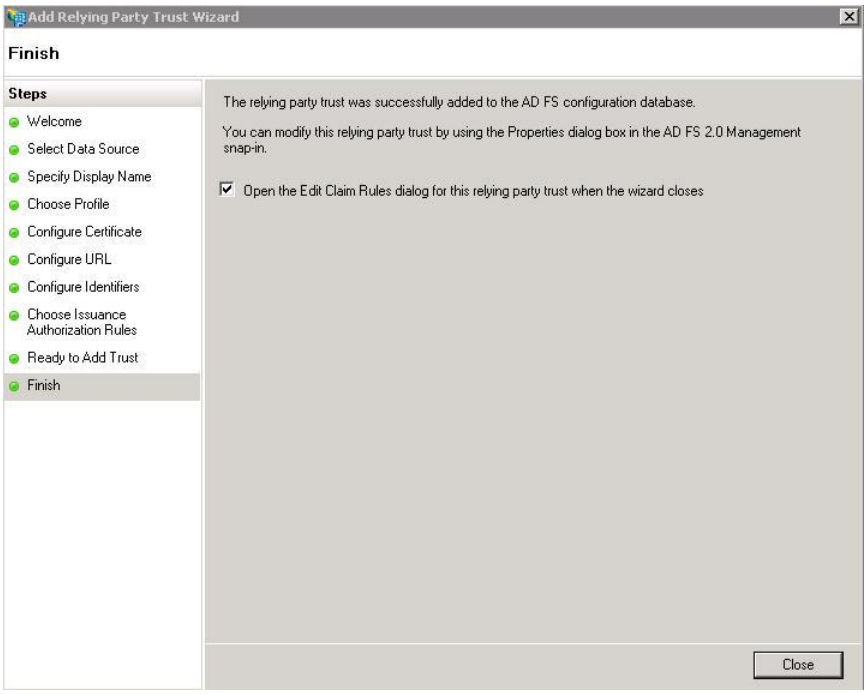
11. In the **Choose Issuance Authorization Rules** tab, select the authorization rule, click **Next**.



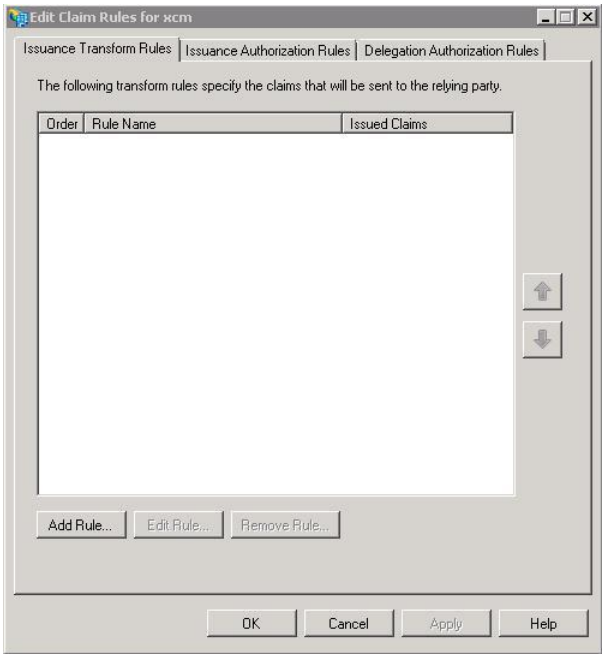
12. In the **Ready to Add Trust** tab, verify all information, click **Next**.



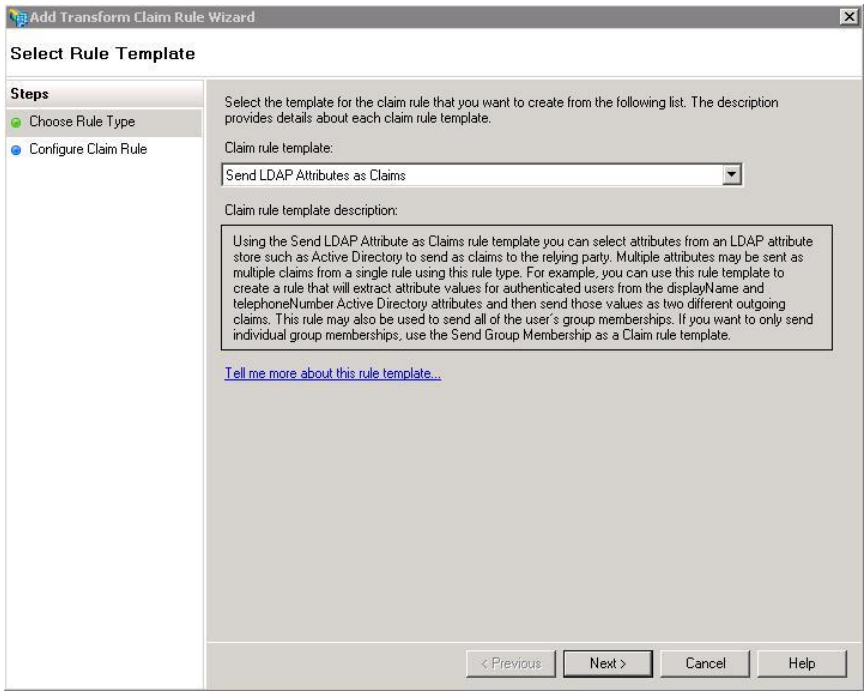
13. In the **Finish** tab, click **Close**.



14. The **Edit Claim Rules** dialog box automatically opens, click **Add Rule**.



15. In the **Choose Rule Type** tab, select **Send LDAP Attributes as Claims** as Claim rule template, click **Next**.



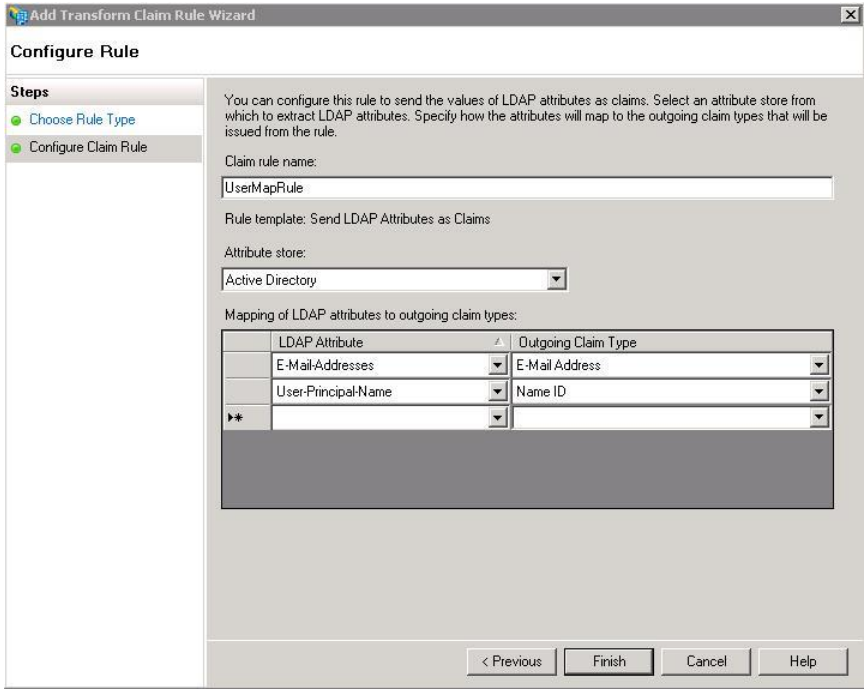
16. In the **Configure Claim Rule** tab:

Enter the **claim rule name**.

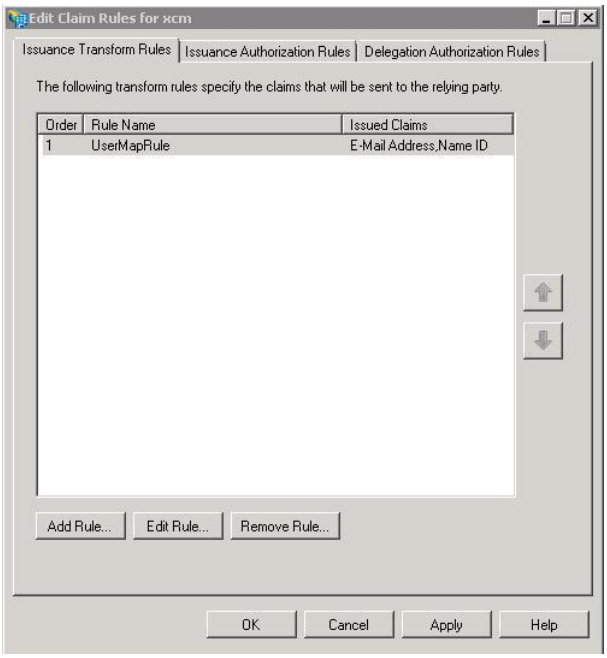
In the **Attribute store**, select **Active Directory**.

Configure **Mapping of LDAP attributes to outgoing claim types** with the settings in the image below**:**

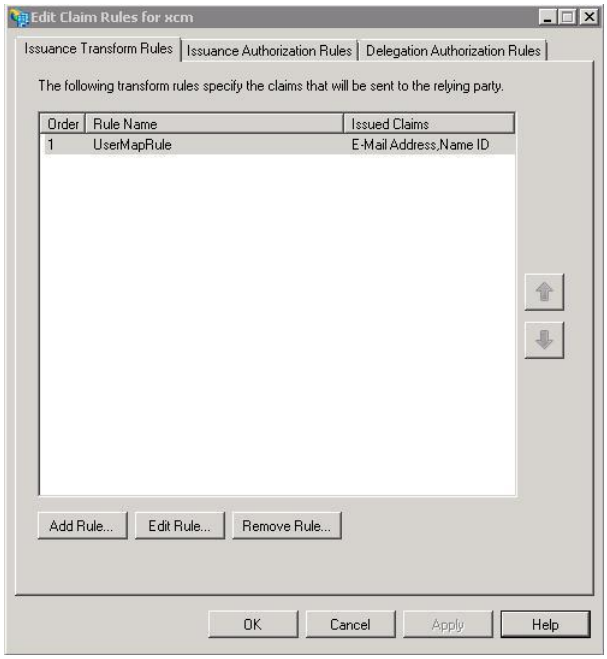
Click Finish.



17. Click **Apply**.



18. Click **Ok**.



You have successfully configured SSO in ADFS.