

ADFS Single Sign on (SSO)

Configuration Guide

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. |
| <i>Italic type</i> | 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:

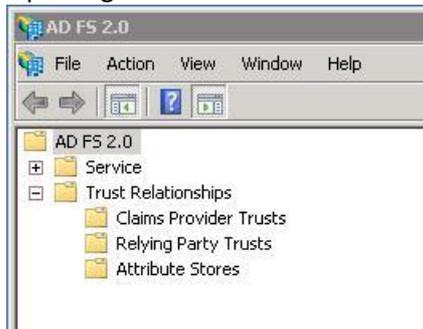
Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2 or Windows Server 2016 with Active directory and AD FS installed and running.

Procedure:

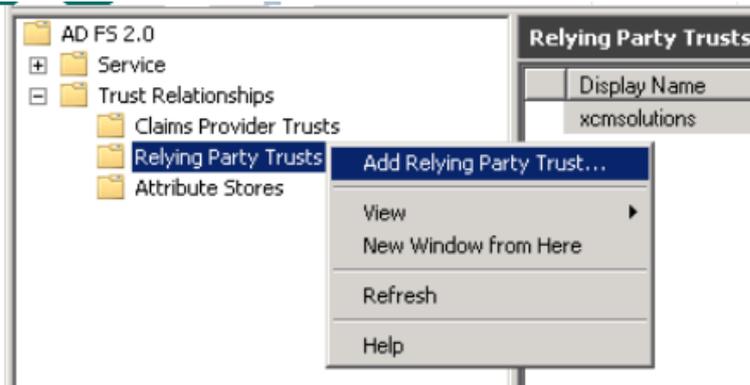
Click the **Start** button and select **AD FS 2.0 Management**. AD FS 2.0 window opens.



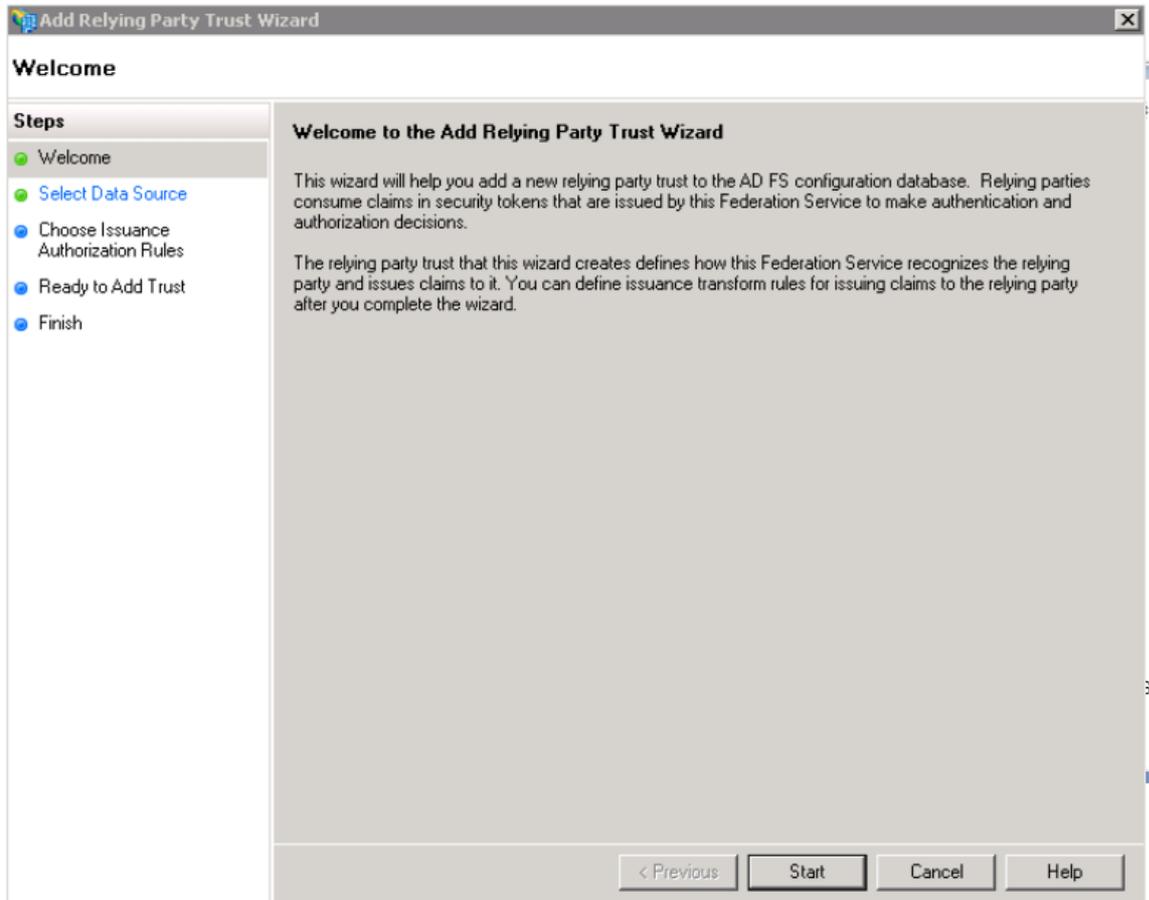
In the AD FS 2.0 window, click the plus sign next to **Trust Relationships** folder. The folder expands.



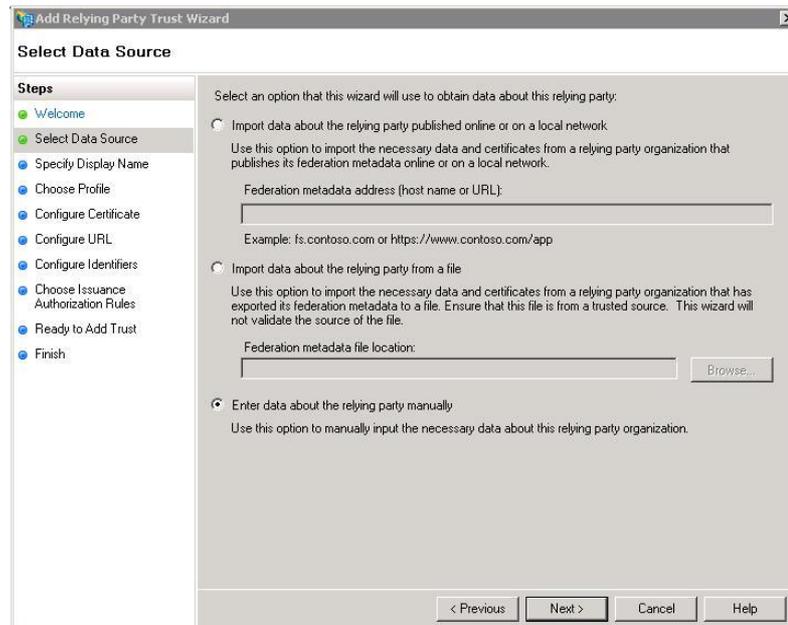
Right click **Relying Party Trusts** folder, click **Add Relying Party Trust**. The Add Relying Party Trust Wizard dialog box starts.



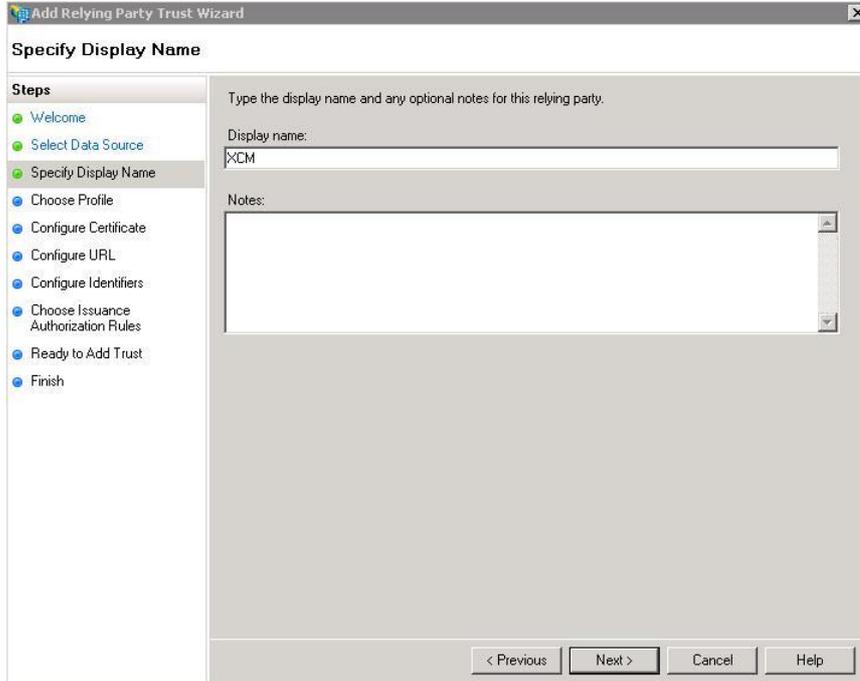
In the **Add Relying Party Trust Wizard**, click **Start**.



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

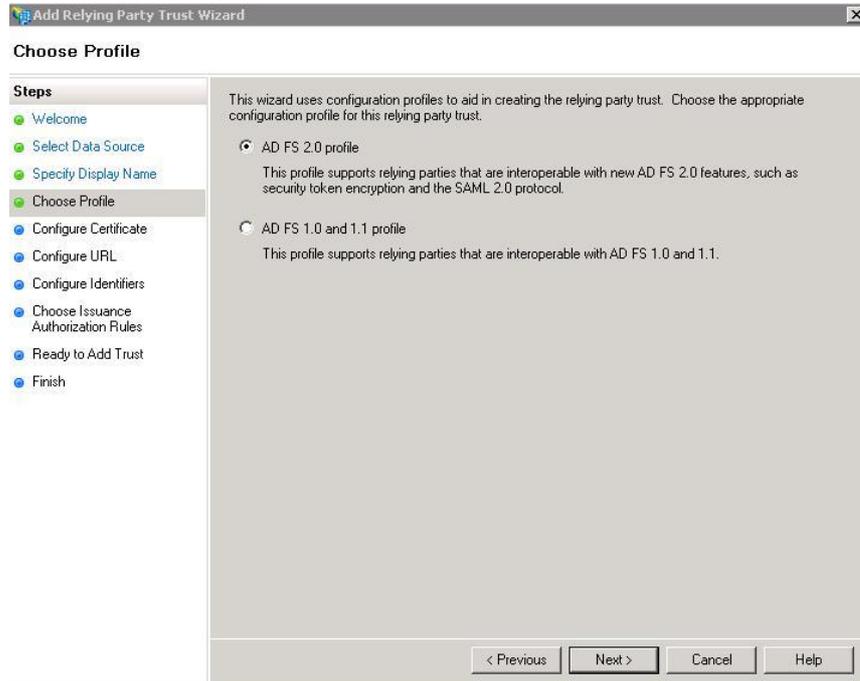


6. Enter the **Display name** and **Notes** to identify the relying party, click **Next**.



The screenshot shows the 'Specify Display Name' step of the 'Add Relying Party Trust Wizard'. The 'Steps' pane on the left lists the following steps: Welcome, Select Data Source, Specify Display Name (current), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the text 'Type the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' text box containing 'XCM' and a 'Notes:' text area which is currently empty. At the bottom, there are four buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

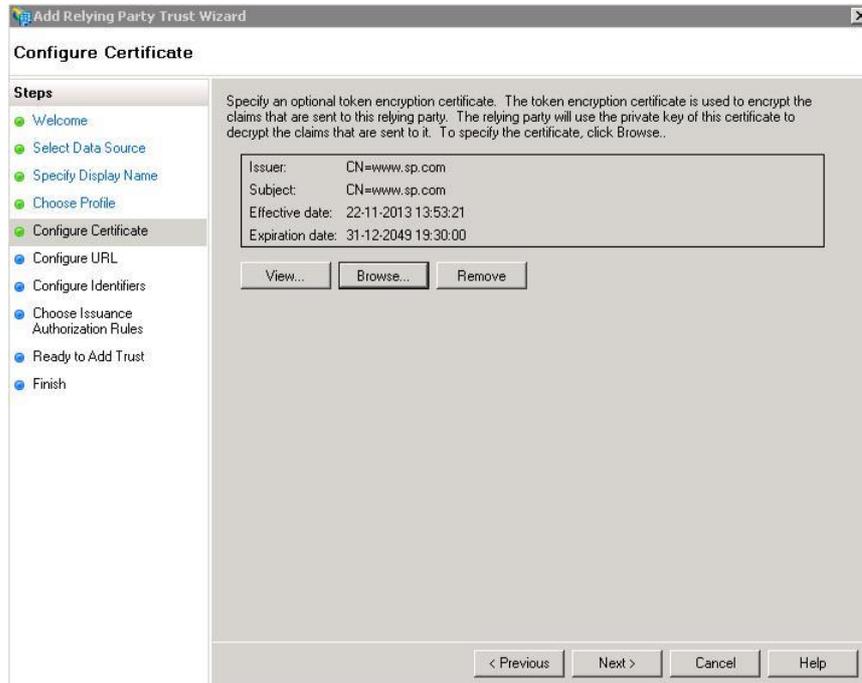
In the **Choose Profile** tab, select **AD FS 2.0 profile**, click **Next**. AD FS 2.0 profile is selected by default.



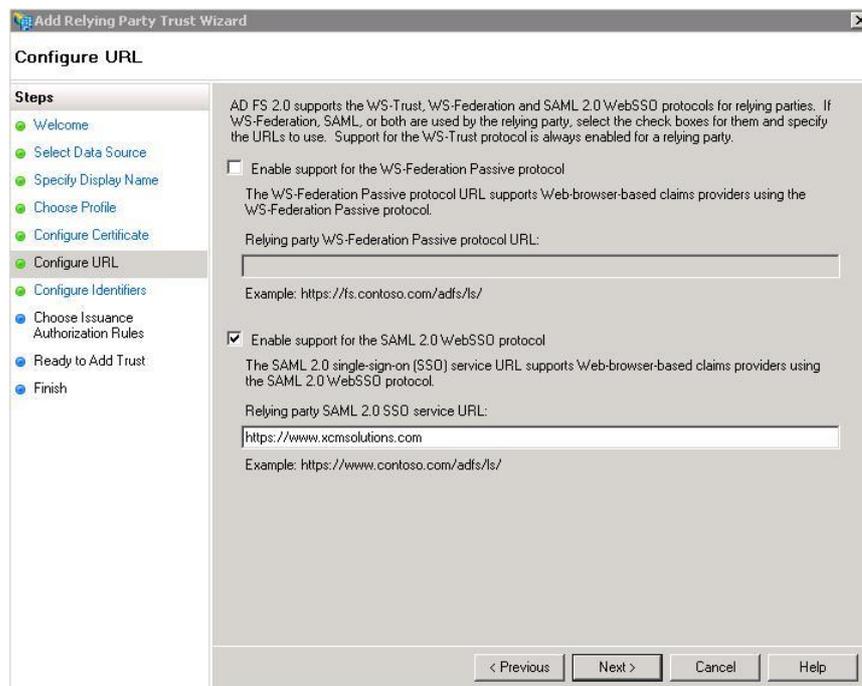
The screenshot shows the 'Choose Profile' step of the 'Add Relying Party Trust Wizard'. The 'Steps' pane on the left lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile (current), Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the text 'This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.' Below this, there are two radio button options: 'AD FS 2.0 profile' (which is selected) and 'AD FS 1.0 and 1.1 profile'. The 'AD FS 2.0 profile' option has a description: 'This profile supports relying parties that are interoperable with new AD FS 2.0 features, such as security token encryption and the SAML 2.0 protocol.' The 'AD FS 1.0 and 1.1 profile' option has a description: 'This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

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.

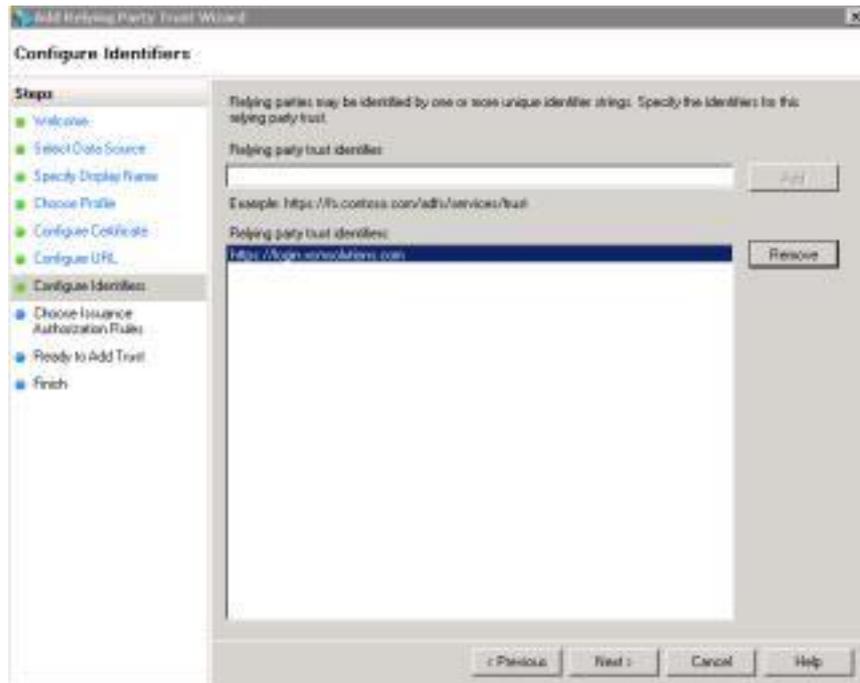


In the **Configure URL** tab, select **Enable support for the SAML 2.0 WebSSO protocol** and enter the **Relying party SAML 2.0 SSO service URL**, click **Next**.

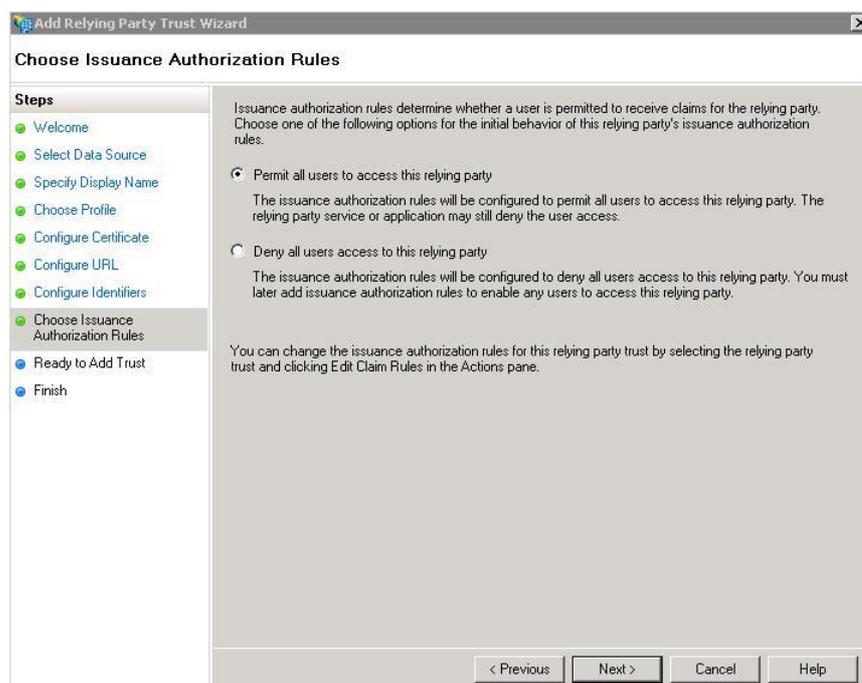


10. In the **Configure Identifiers** tab, enter the relying party trust identifier.
Click **Add** and click **Next**.

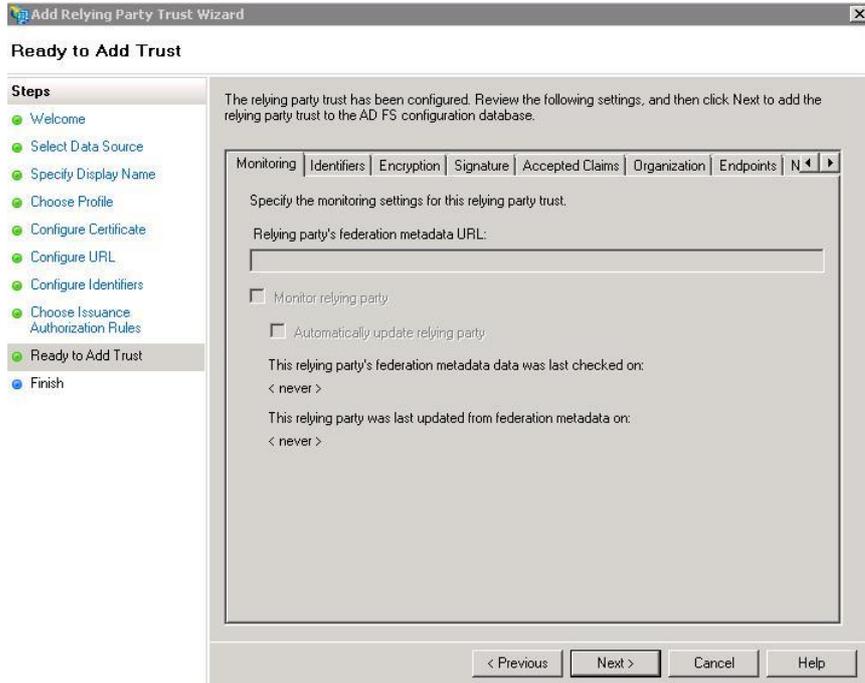
Note: XCM customer service representative or your point of contact will share the relying party trust identifier details.



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

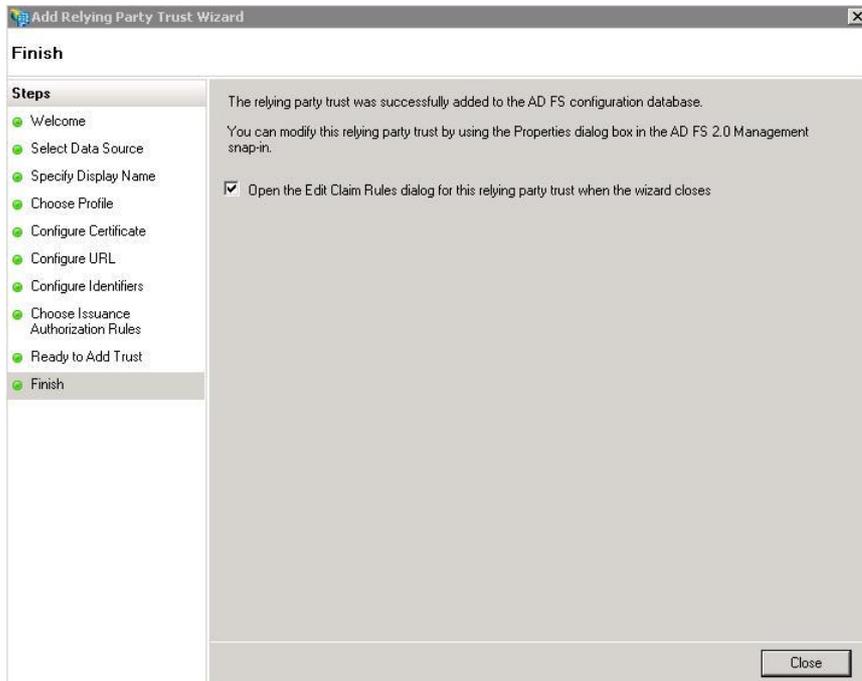


12. In the **Ready to Add Trust** tab, verify all information, click **Next**.



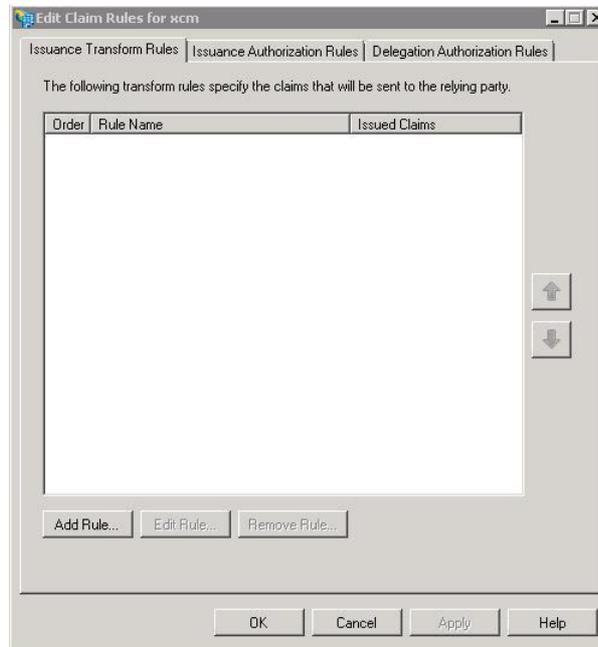
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Ready to Add Trust' step. The 'Steps' list on the left includes: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules, Ready to Add Trust (highlighted), and Finish. The main area contains the following text: 'The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.' Below this is a tabbed interface with 'Monitoring' selected. The 'Monitoring' tab contains: 'Specify the monitoring settings for this relying party trust.', 'Relying party's federation metadata URL:' followed by an empty text box, two unchecked checkboxes for 'Monitor relying party' and 'Automatically update relying party', and two labels with '< never >' values: 'This relying party's federation metadata data was last checked on:' and 'This relying party was last updated from federation metadata on:'. At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'Help'.

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

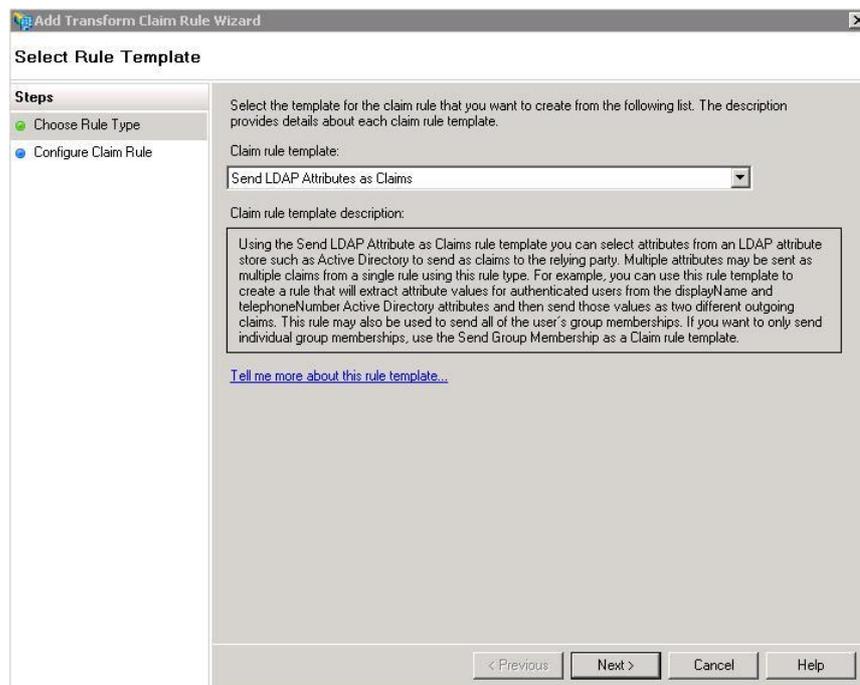


The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Finish' step. The 'Steps' list on the left includes: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish (highlighted). The main area contains the following text: 'The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snap-in.' Below this is a checked checkbox for 'Open the Edit Claim Rules dialog for this relying party trust when the wizard closes'. At the bottom right is a 'Close' button.

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**.



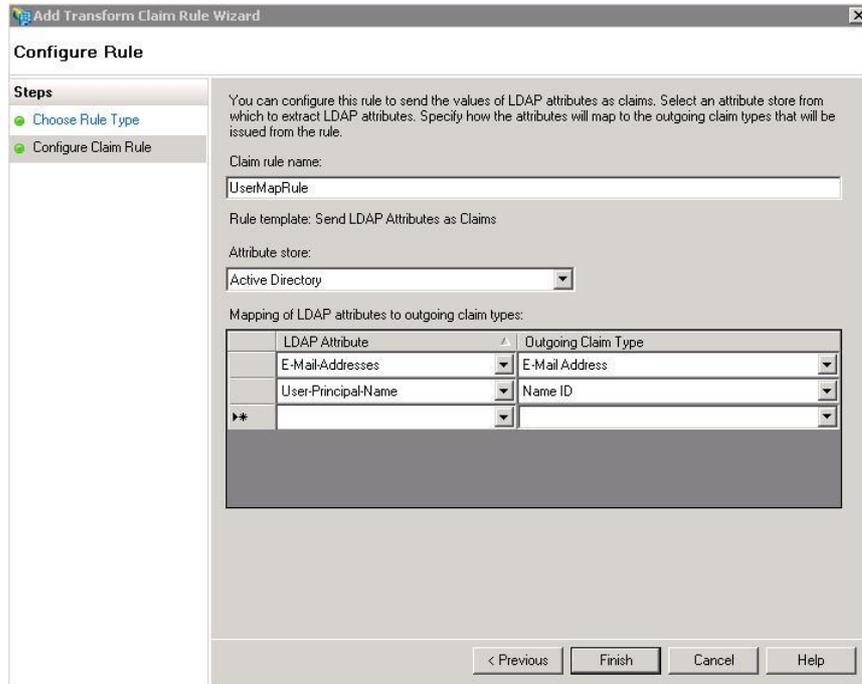
16. In the **Configure Claim Rule** tab:

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**.



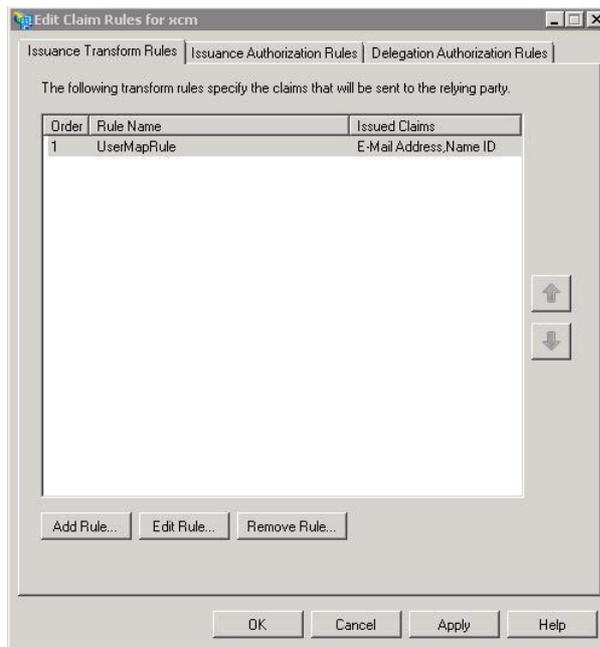
The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' tab. The 'Steps' pane on the left shows 'Configure Claim Rule' as the current step. The main area contains the following configuration options:

- Claim rule name:** UserMapRule
- Rule template:** Send LDAP Attributes as Claims
- Attribute store:** Active Directory
- Mapping of LDAP attributes to outgoing claim types:**

| LDAP Attribute | Outgoing Claim Type |
|---------------------|---------------------|
| E-Mail-Addresses | E-Mail Address |
| User-Principal-Name | Name ID |
| * * | |

Buttons at the bottom include '< Previous', 'Finish', 'Cancel', and 'Help'.

17. Click **Apply**.

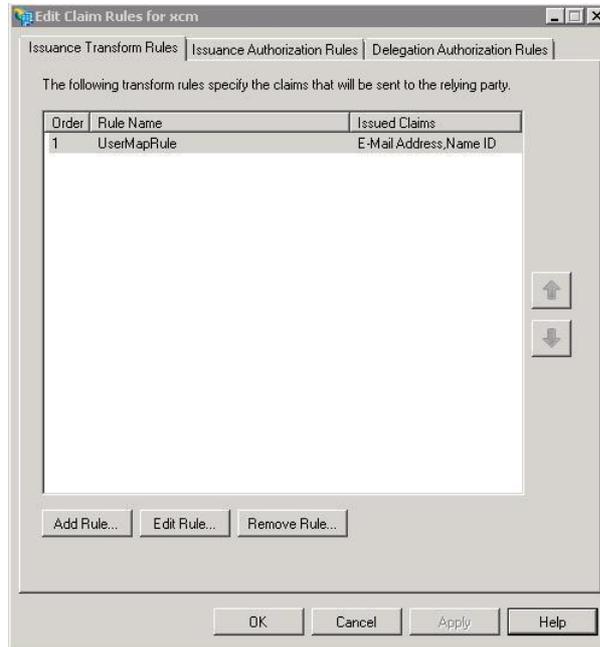


The screenshot shows the 'Edit Claim Rules for xcm' dialog box. It has three tabs: 'Issuance Transform Rules', 'Issuance Authorization Rules', and 'Delegation Authorization Rules'. The 'Issuance Transform Rules' tab is active, showing a list of rules:

| Order | Rule Name | Issued Claims |
|-------|-------------|-------------------------|
| 1 | UserMapRule | E-Mail Address, Name ID |

Below the table are buttons for 'Add Rule...', 'Edit Rule...', and 'Remove Rule...'. At the bottom of the dialog are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

18. Click **Ok**.



You have successfully configured SSO in ADFS.