Set Up Active Directory Federation Services (ADFS)

schoolwires®
a Blackboard solution

This guide covers all available Schoolwires features and functionality. Features included in your contract may vary.

Table of Contents

Introduction

Active Directory Federation Services (ADFS) is a software component developed by Microsoft. It can be installed on Windows Server operating systems so that users have single sign-on access to systems and applications.

ADFS is a standards-based service that provides for the secure sharing of identity information between trusted partners (a federation) across an *extranet* (an intranet that can be accessed by authorized outside users). When users access a Web application from a federation partner, their organization has the responsibility of authenticating them. It provides identity information in the form of *claims* to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which then uses the claims authorize the user.

This guide provides information on how to configure ADFS for SAML implementation. This configuration must be done prior to configuring SAML in Schoolwires.

Note that you need to obtain our Signature certificate prior to ADFS setup.

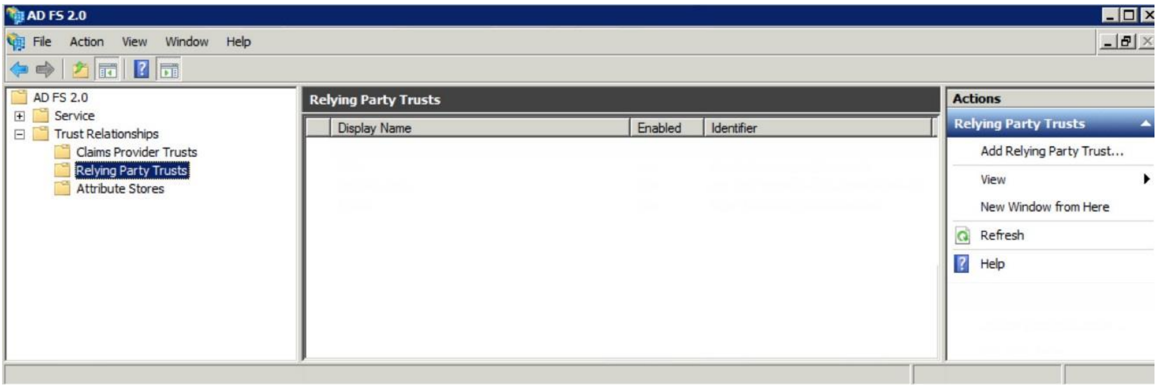
Signature Certificate

Before you begin to set up ADFS, you must obtain our Signature Certificate. Contact your Blackboard representative to obtain the certificate. You can also download the certificate from the Schoolwires Community and Support Network site.

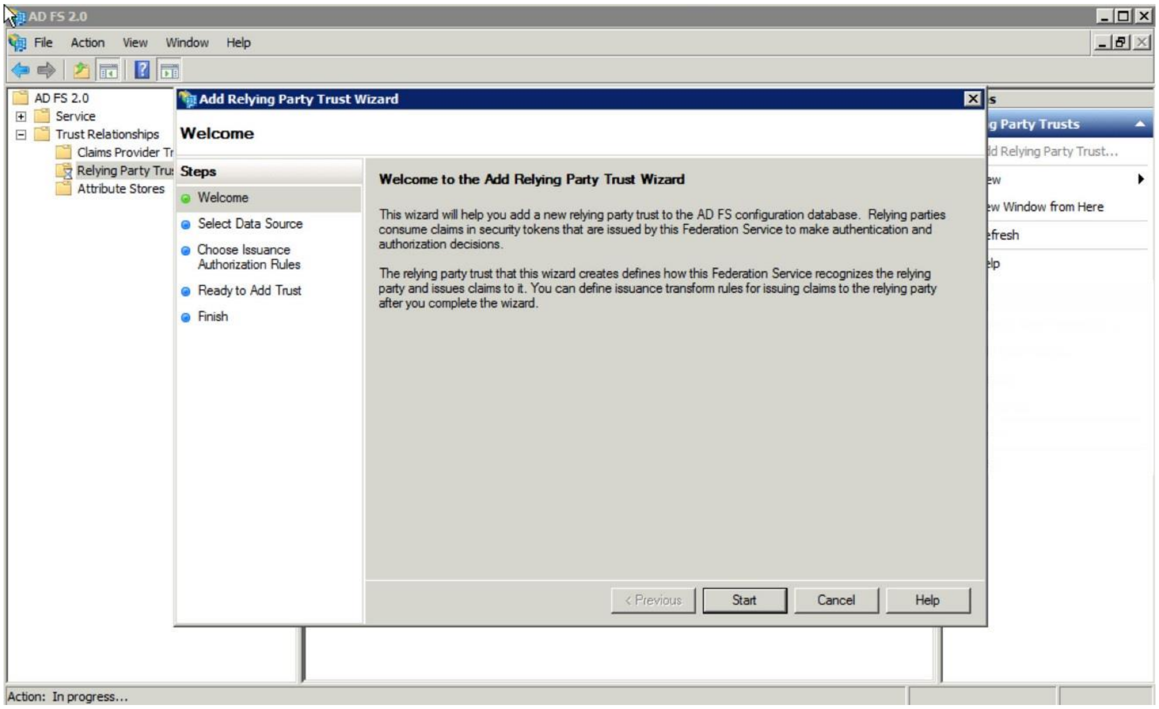
Configure ADFS 2.0

Here's how you configure ADFS 2.0. This must be completed before you configure SAML in Schoolwires.

1. Launch ADFS 2.0 Management on the ADFS server.



2. Under Trust Relationships, select and add *Relying Party Trusts*.

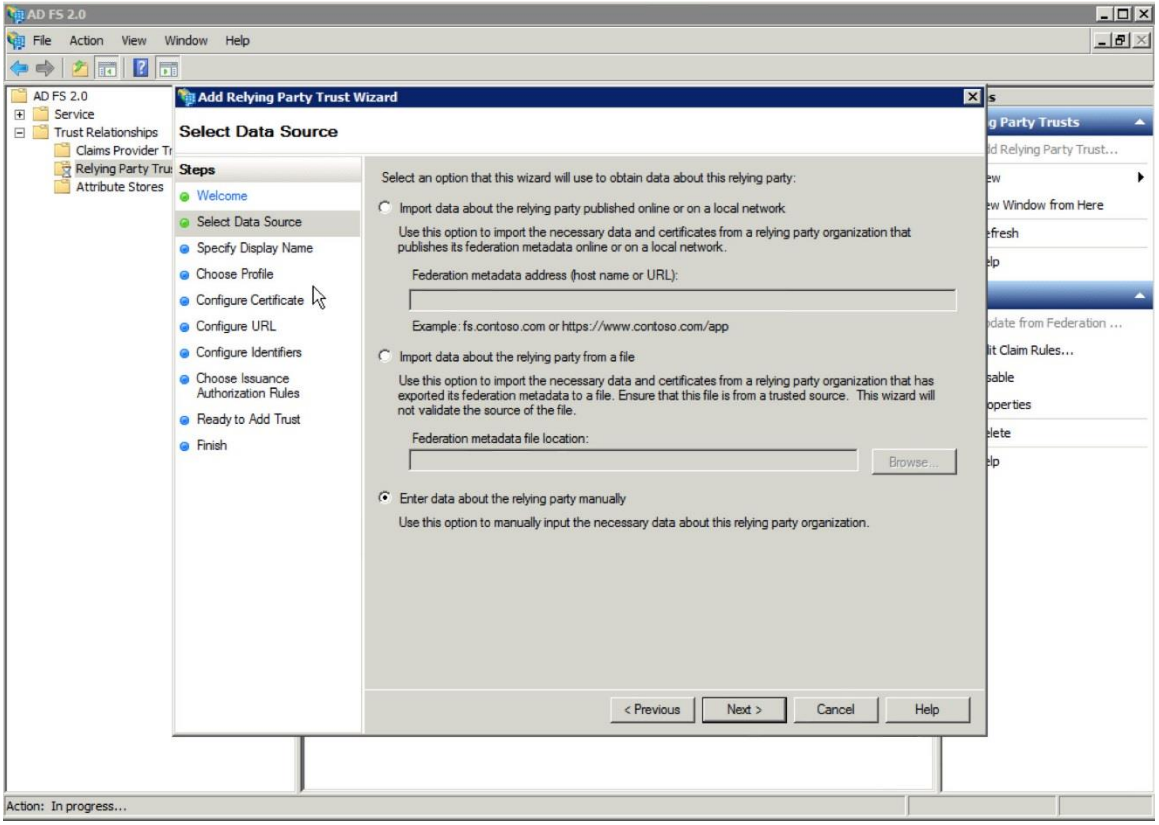


Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

3. Under Select Data Source, check *Enter data about relying party manually* and complete the wizard.



Select Data Source

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:

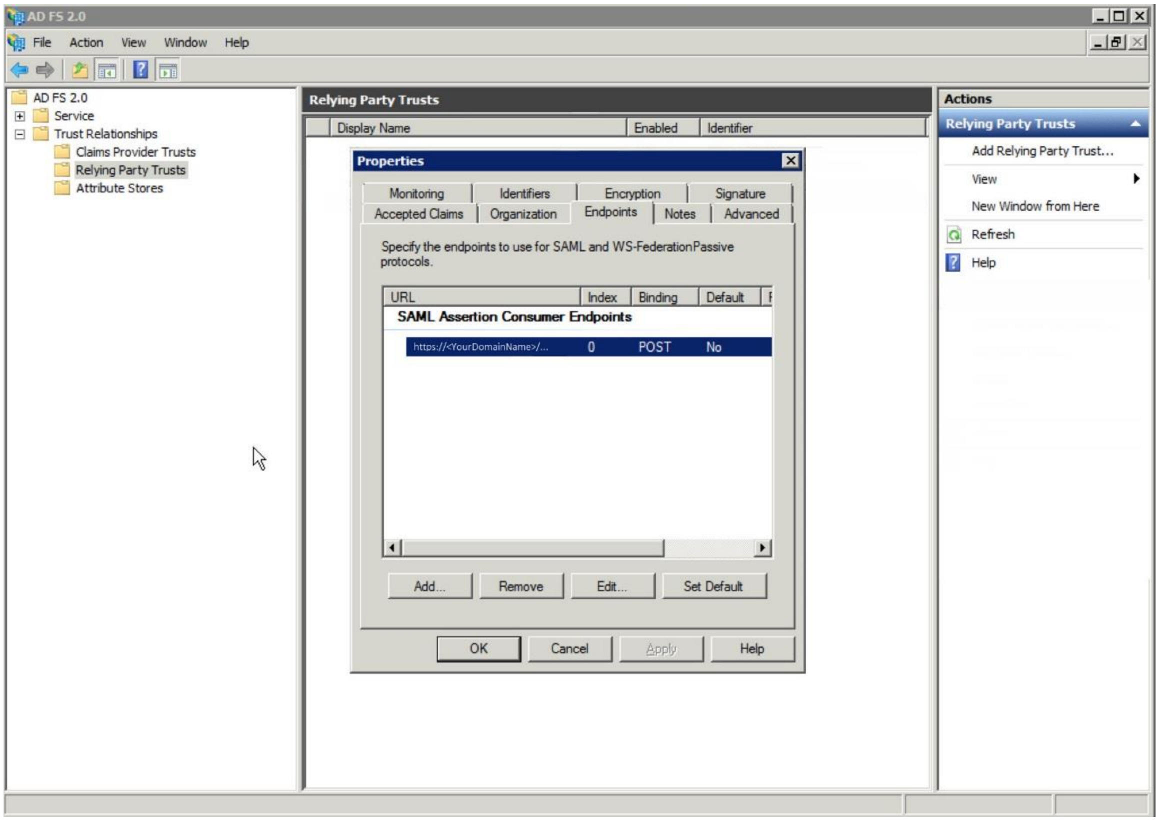
● Enter data about the relying party manually

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

- Under Specify Display Name, enter *Schoolwires* for Display Name.
- Under Choose Profile, check *ADFS 2.0.*
- Under Configure URL, check *Enable support for the SAML 2.0*
  Enter https://<ClientsDomain>/site/handlers/samlhandler.ashx/ProcessRequest as the Relying party SAML 2.0 SSO service URL.

- Under Choose Issuance Authorization Rules, check *Permit all users to access this relying party*.

4. Right click on the relying party in the list and select *Properties*. Select the Relying Party Properties **Endpoints** tab and ensure that the binding is *POST*.



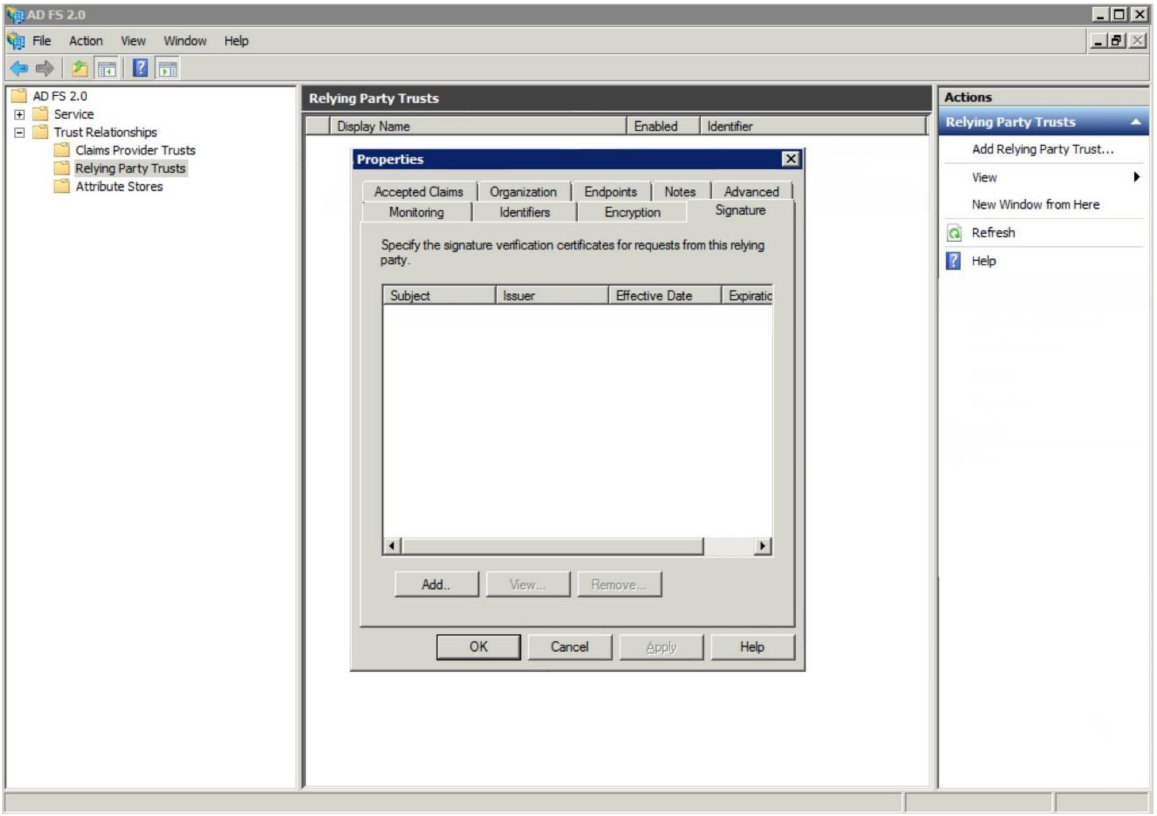
Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default
SAML Assertion Consumer Endpoints			
https://<YourDomainName>/...	0	POST	No

Enter *https://<YourDomainName>* for the Relying party trust identifier.

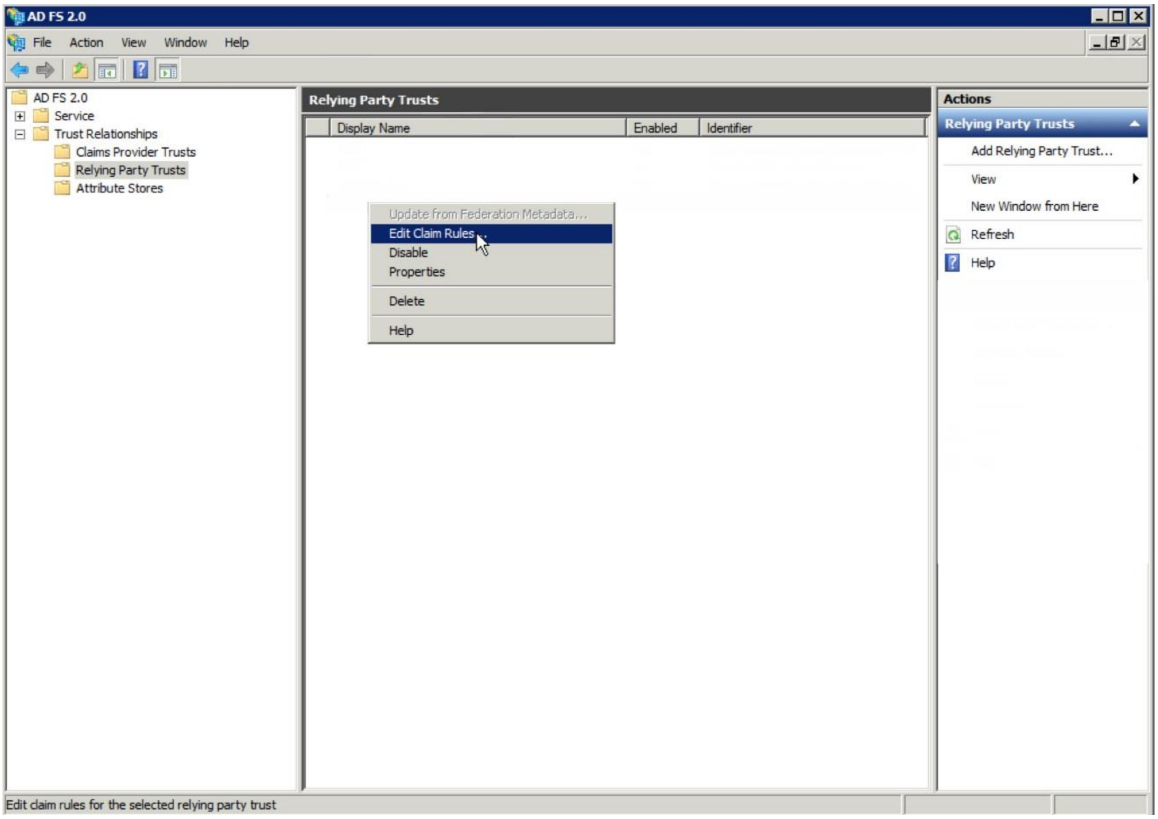
5. On the Relying Party Properties **Advanced** tab, set *SHA-1* as the Secure Hash Algorithm.

6. On the Relying Party Properties **Signature** tab, add the Signature Certificate (.cer). Contact your Blackboard representative to obtain a copy of the certificate or download it from the Schoolwires Community & Support Network Site.

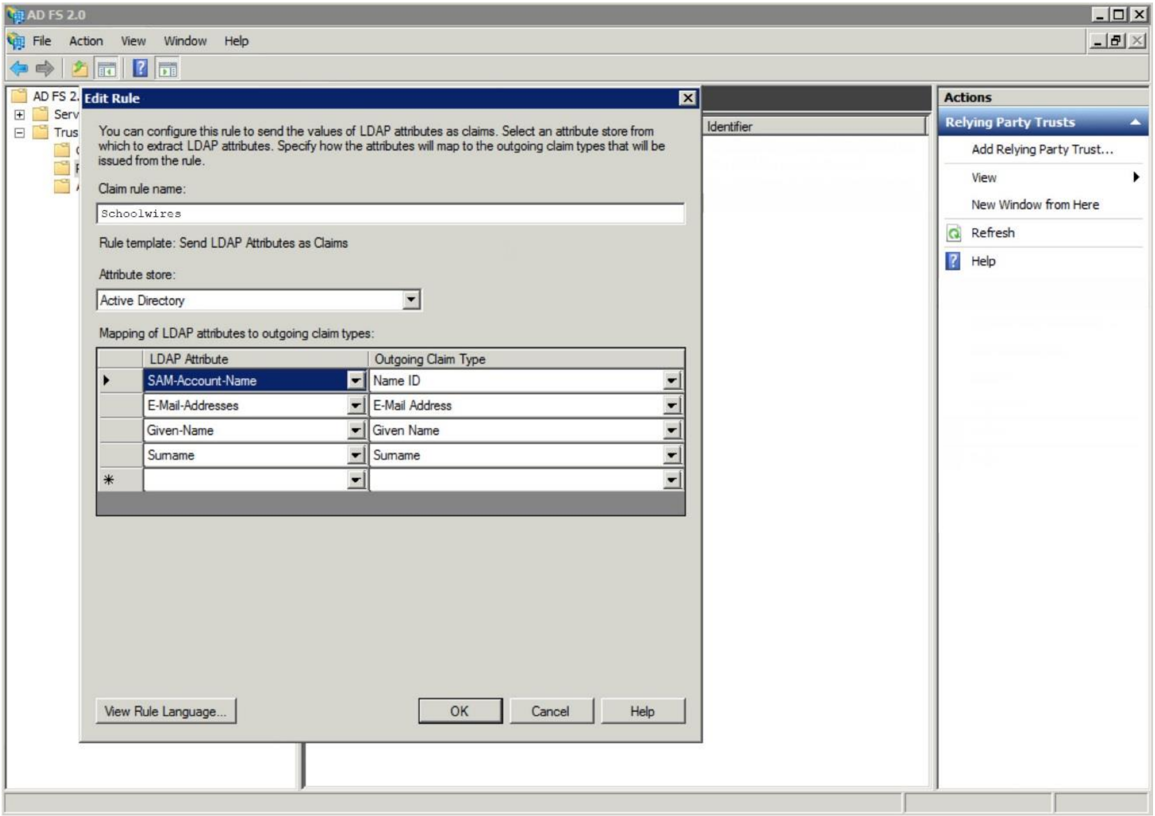


Specify the signature verification certificates for requests from this relying party.

7. Right click on the relying party in the list and select Edit Claim Rules…



8. Click **Add Rule** and select *Send LDAP Attributes as Claims* under Choose Rule Type.



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Schoolwires

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	SAM-Account-Name	Name ID
	E-Mail-Addresses	E-Mail Address
	Given-Name	Given Name
	Surname	Surname
*		

- Enter *Schoolwires* for Claim rule name under Configure Claim Rule.
- Select *Active Directory* as the Attribute Store.
- Map attribute *SAM-Account-Name* to Outgoing Name ID.
- Map attribute *E-Mail-Addresses* to Outgoing E-Mail Address.
- Map attribute *Given-Name* to Outgoing Given Name.
- Map attribute *Surname* to Outgoing Surname.