LAW MASTER®
Law Practice Technology

Setting up Windows Authentication

Administrator’s Instructions

A MASTRIN CREATION

About This Guide

This Guide contains the guidelines on how to configure Windows authentication with user's LawMaster login. Using Windows authentication makes sense when you want your users to be able to use their standard Windows user names and passwords when accessing LawMaster.

This document is intended for a technical audience, specifically the system administrator in charge of setting up users in LawMaster.

For details on the supported platforms, see the latest **Release Notes**.

Contents

Overview

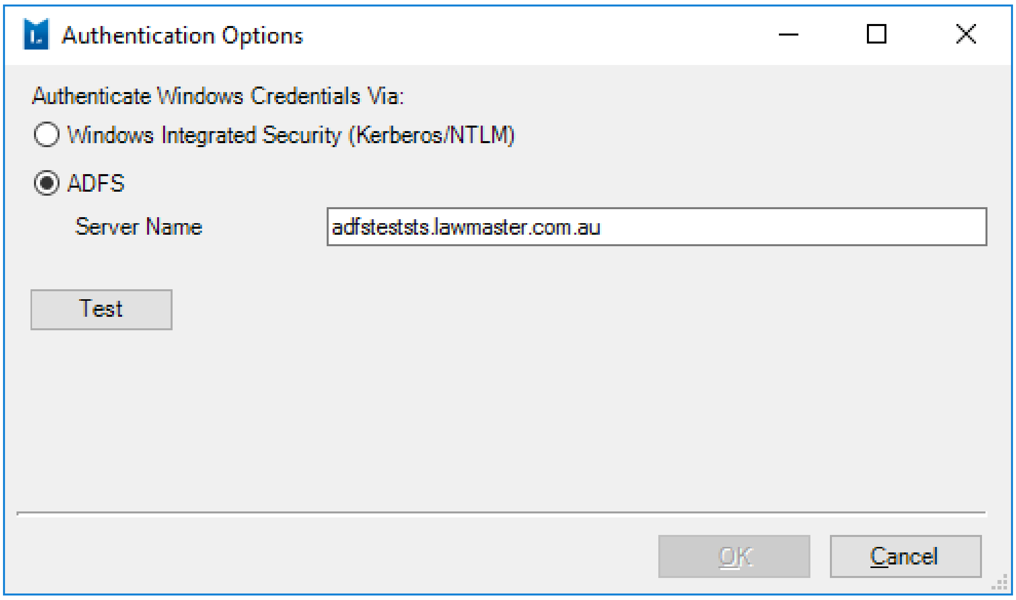
In order to use Windows authentication (single sign-on), you must either:

a) be hosting your own application server on a computer connected to your windows domain OR

b) have an Microsoft AD FS server contactable from your user's system.

Authentication Options Parameter

You can configure the authentication options from Parameters > Set Parameters > Miscellaneous > Authentication Options within LawMaster.



Authentication Options

Authenticate Windows Credentials Via:

○ Windows Integrated Security (Kerberos/NTLM)

● ADFS

Server Name: adfstests ts.lawmaster.com.au

Figure 1: Authentication Options parameter

This parameter allows you to test Windows Integrated Security, i.e. if your application server is on your domain or the connection to your AD FS server (from your current PC).

Your AD FS server must be configured to authenticate LawMaster clients – see instructions below. Regardless of which method you use to authenticate windows credentials, you must then configure your resources with their windows domain accounts. The user@fulldomainname.com.au format is preferred, but domainname\user will continue to work for older Microsoft Operating Systems.

Note: As of Monaco R2 product release, signing in with Windows authentication will be prevented in some scenarios where it previously would have allowed access.

Instructions to Setup AD FS

This section provides the external links to help you configure your AD FS server to authenticate LawMaster client.

Install and configure AD FS within your domain. Follow the links below for the help on the AD FS configuration.

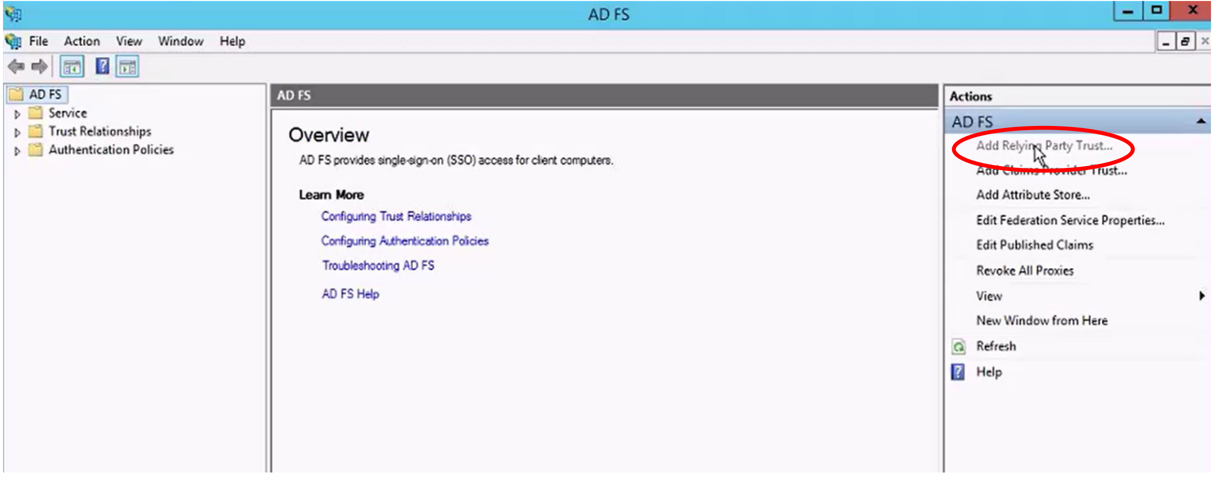
1. Deployment guide https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-deployment
2. Installation instructions https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/install-the-ad-fs-role-service
3. Configuration instructions for AD FS (in general, not LawMaster specific) https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-a-federation-server
4. Non-Microsoft screenshots and tips that may help - http://samirvaidya.blogspot.com.au/2015/03/set-up-and-install-active-directory.html

Configure AD FS for LawMaster

The AD FS server then needs to be configured to accept connections from LawMaster applications. Follow the instructions below:

1. Open the *AD FS Management* application.

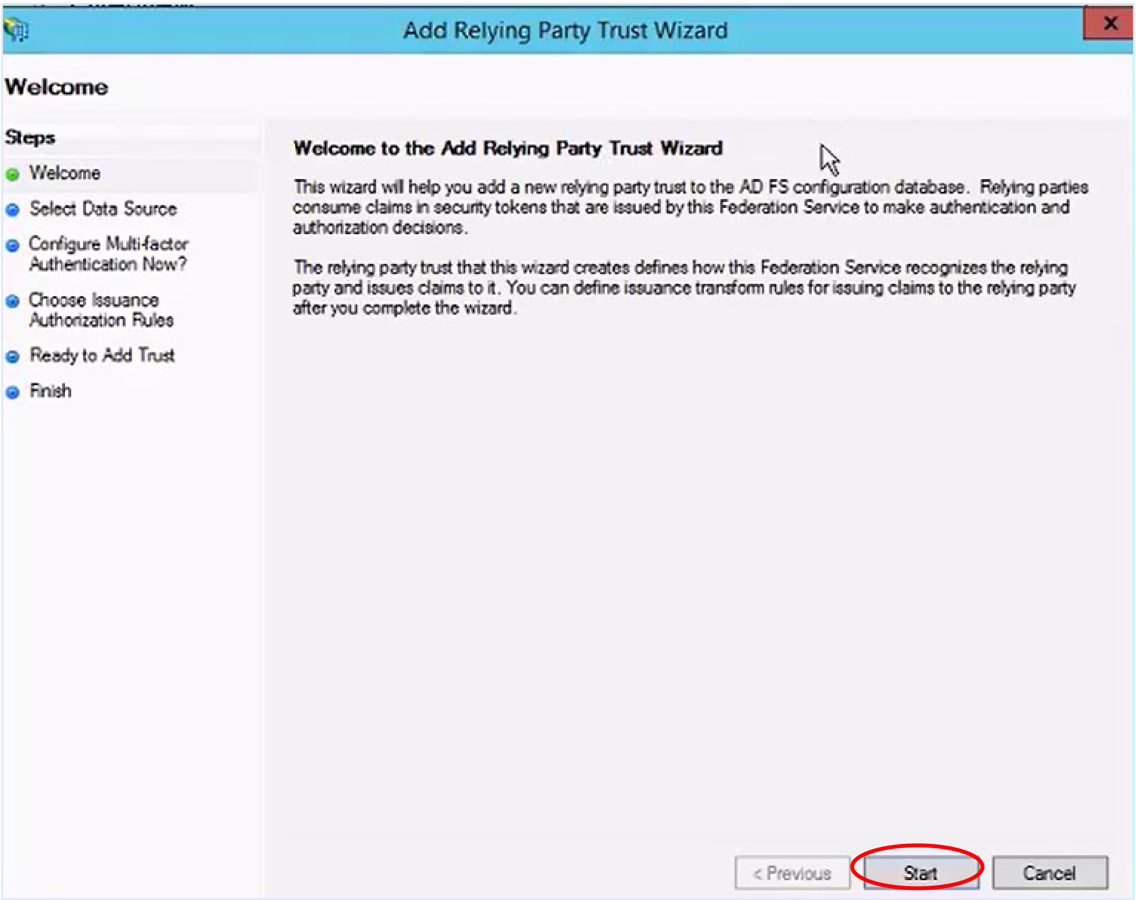
2. From the *Actions* panel on the right side, choose the *Add Relying Party Trust* option.



Overview

AD FS provides single-sign-on (SSO) access for client computers.

3. The system launches the *Add Relying Party Trust Wizard*. Click *Start* to initiate.



Add Relying Party Trust Wizard

Welcome

Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

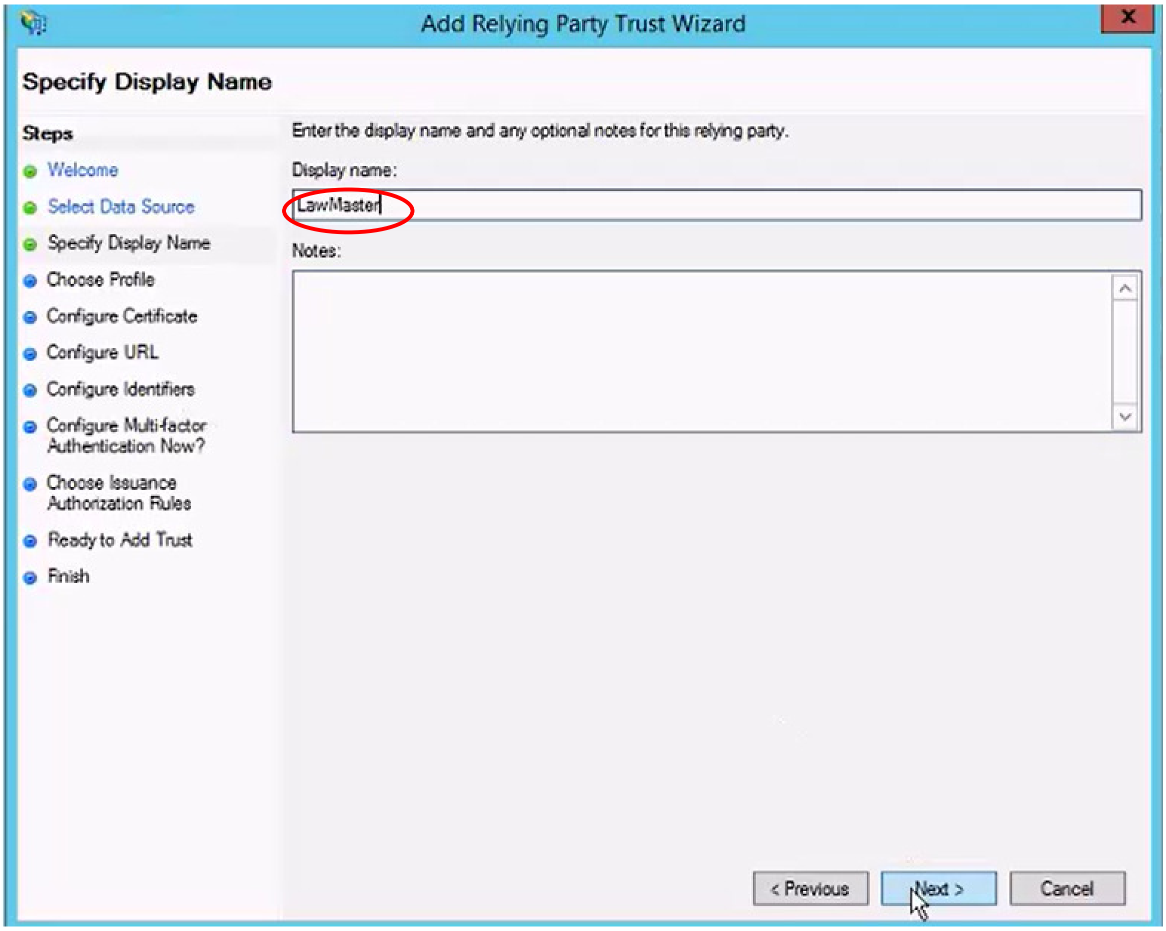
Welcome to the Add Relying Party Trust Wizard

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.

4. Select *Enter Data about the relying party manually* and click *Next*.

5. Enter the display name as *LawMaster* and click *Next*.



Add Relying Party Trust Wizard

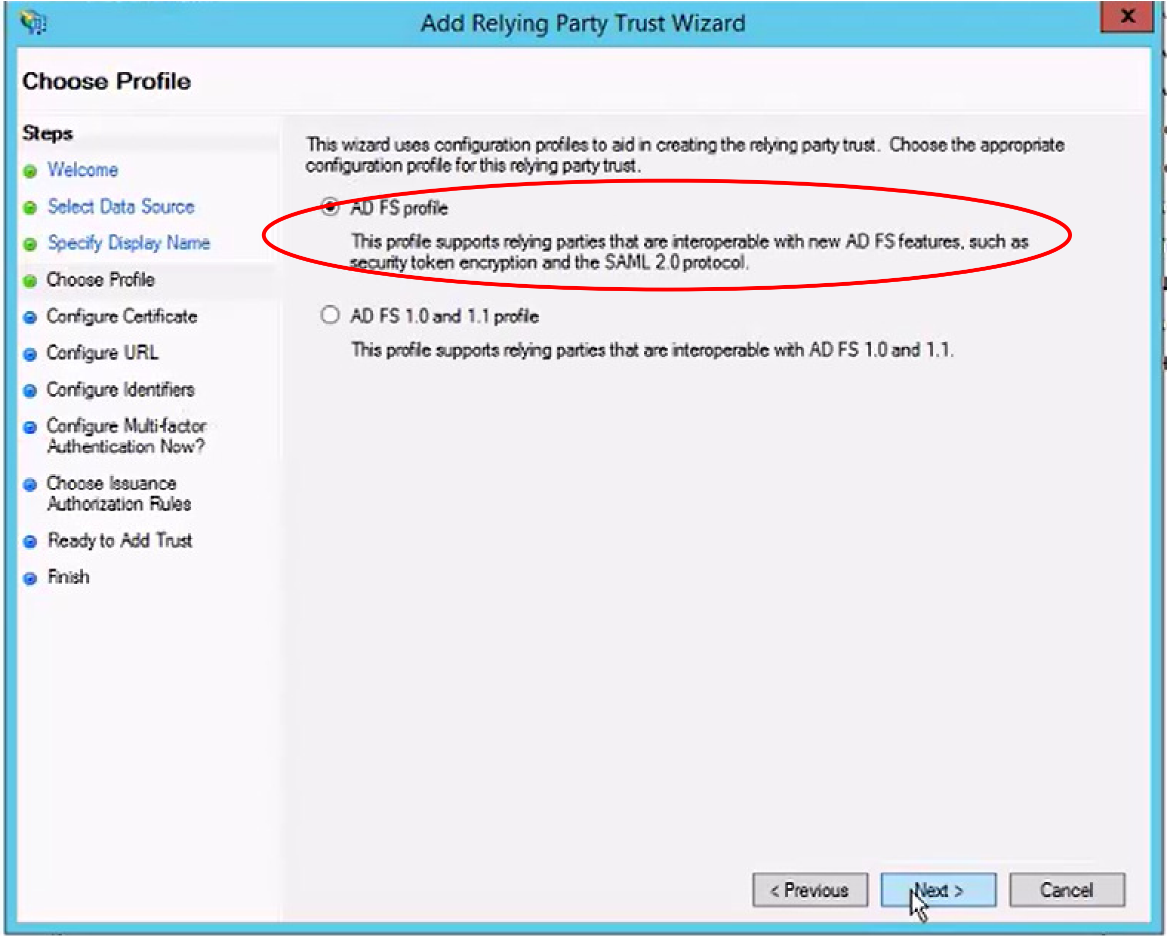
Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: LawMaster

Notes:

6. Choose the *AD FS profile* option and click *Next*.



Add Relying Party Trust Wizard

Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

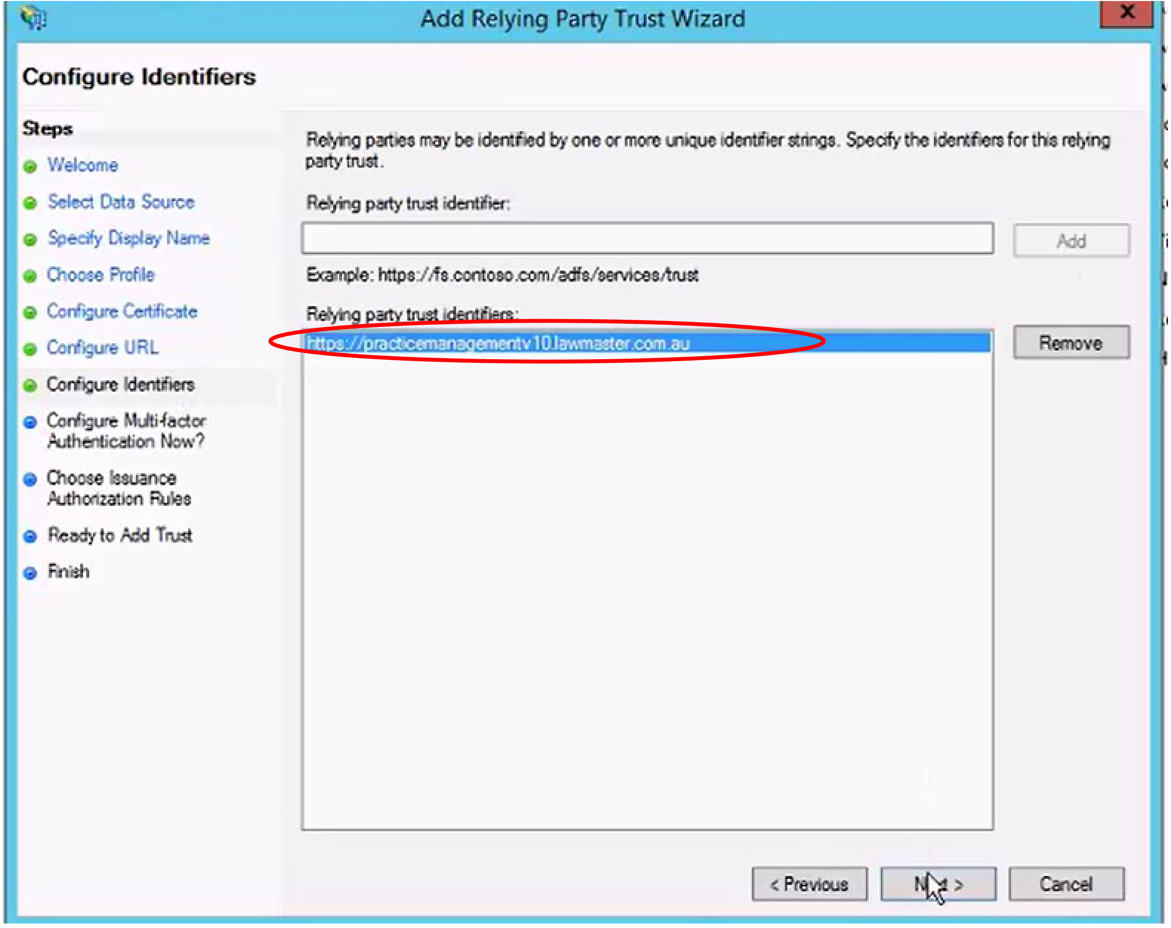
○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

7. In the following screen, do not configure a certificate, and press *Next*.

8. Similarly, do not add support for WS-Federation or SAML 2 Web SSO), and press *Next*.

9. Add an identifier of https://practicemanagementv10.lawmaster.com.au, and click *Next*.



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

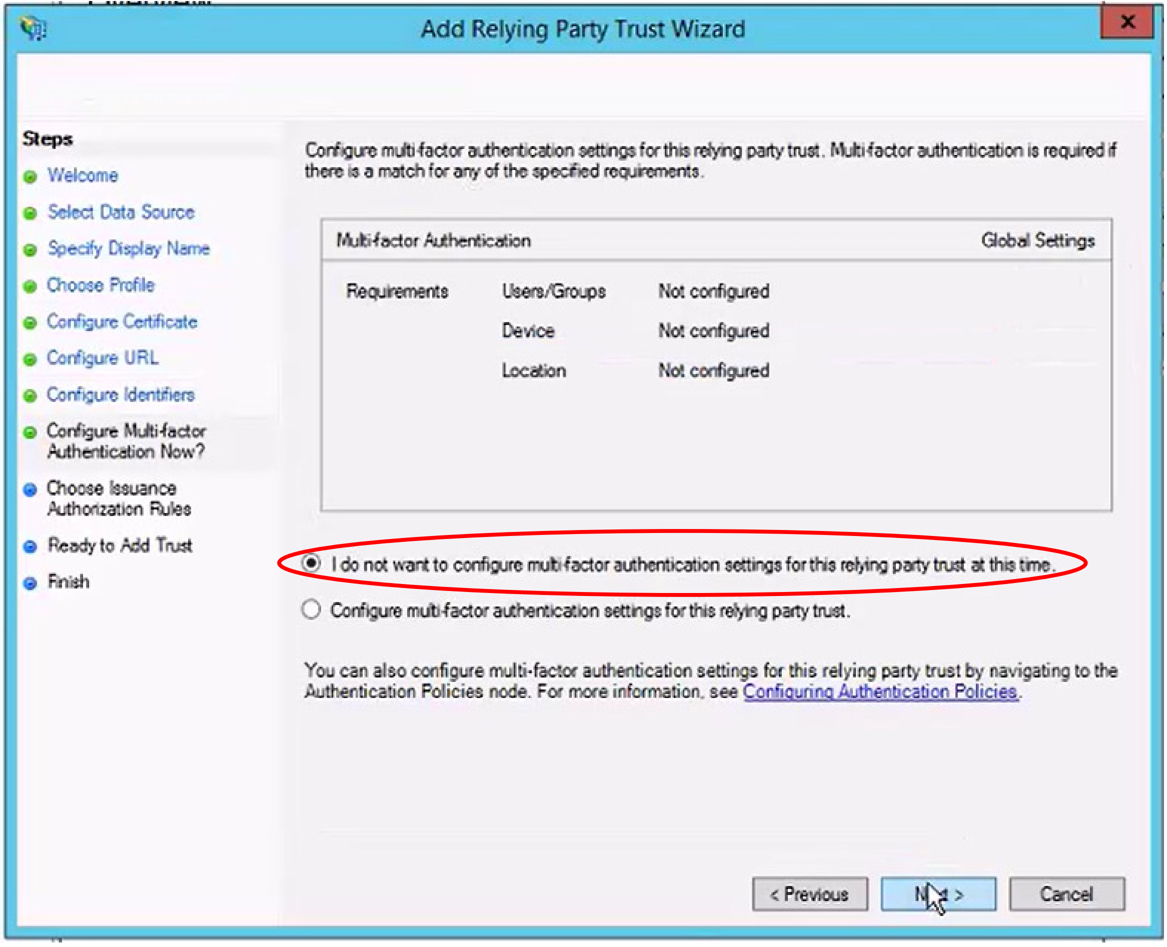
Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

https://practicemanagementv10.lawmaster.com.au

10. Choose not to configure multifactor authentication and click *Next*.



Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

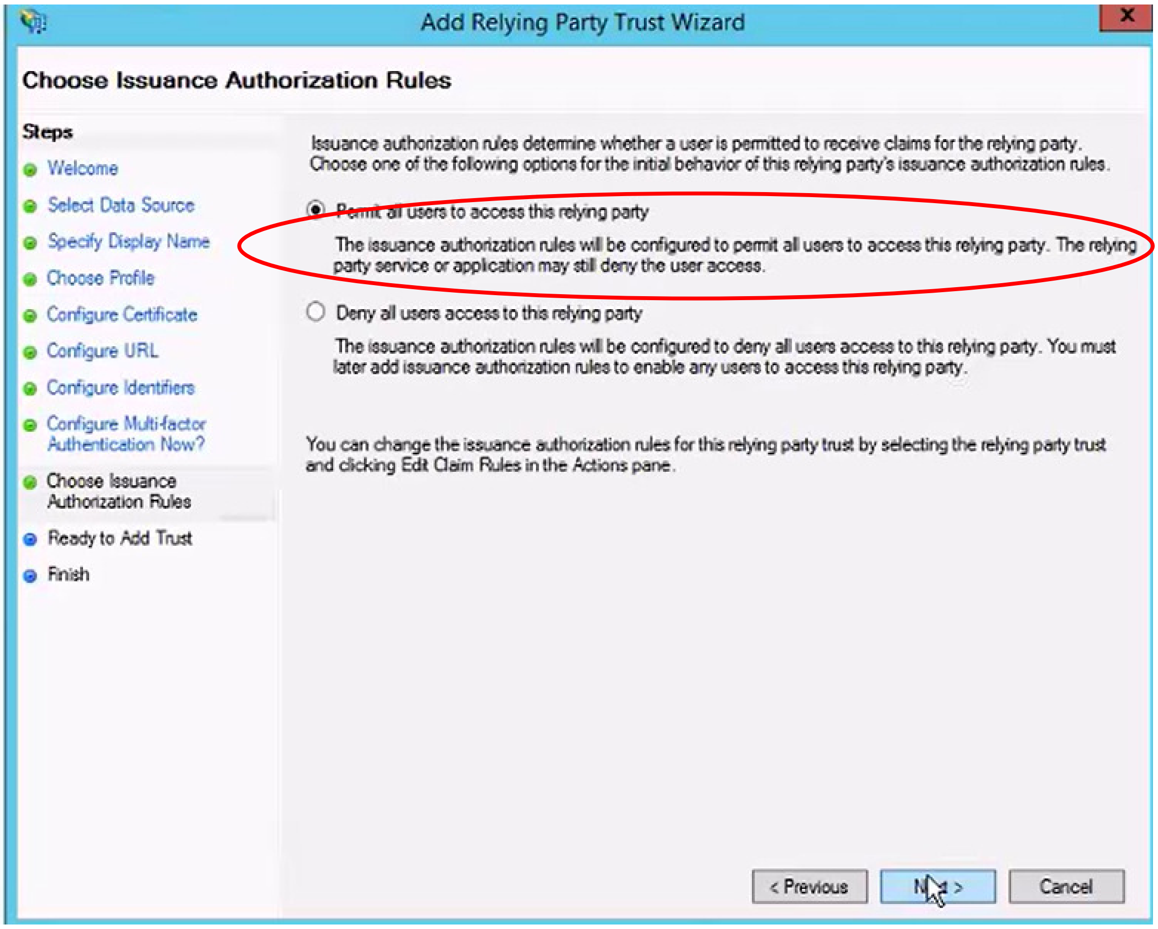
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

11. For authorisation rules, select to permit all users to access this relying party.



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

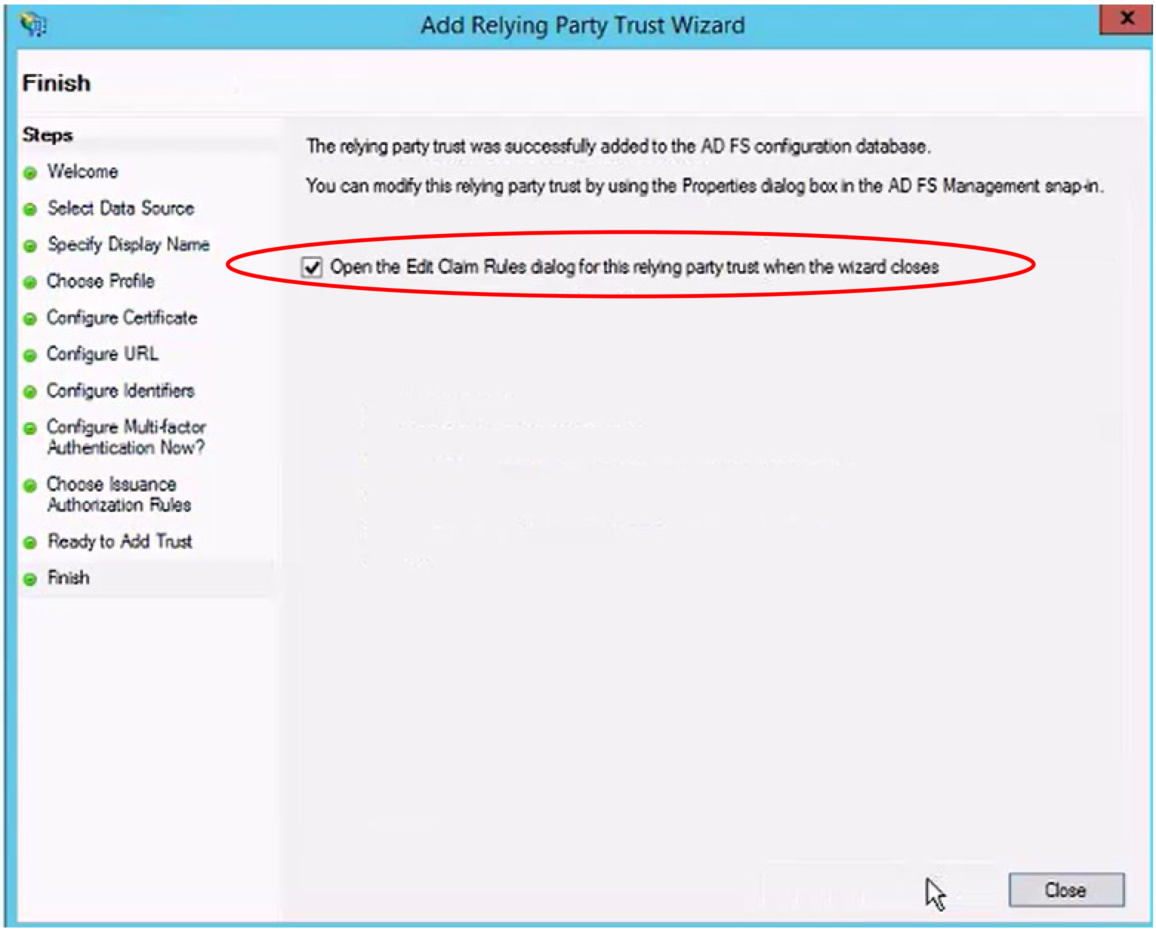
○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

12. Do not set any advanced settings and click *Next*.

13. Select the *Open the Edit Claim Rules* option for this relying party trust, and then click *Close* to exit the wizard.

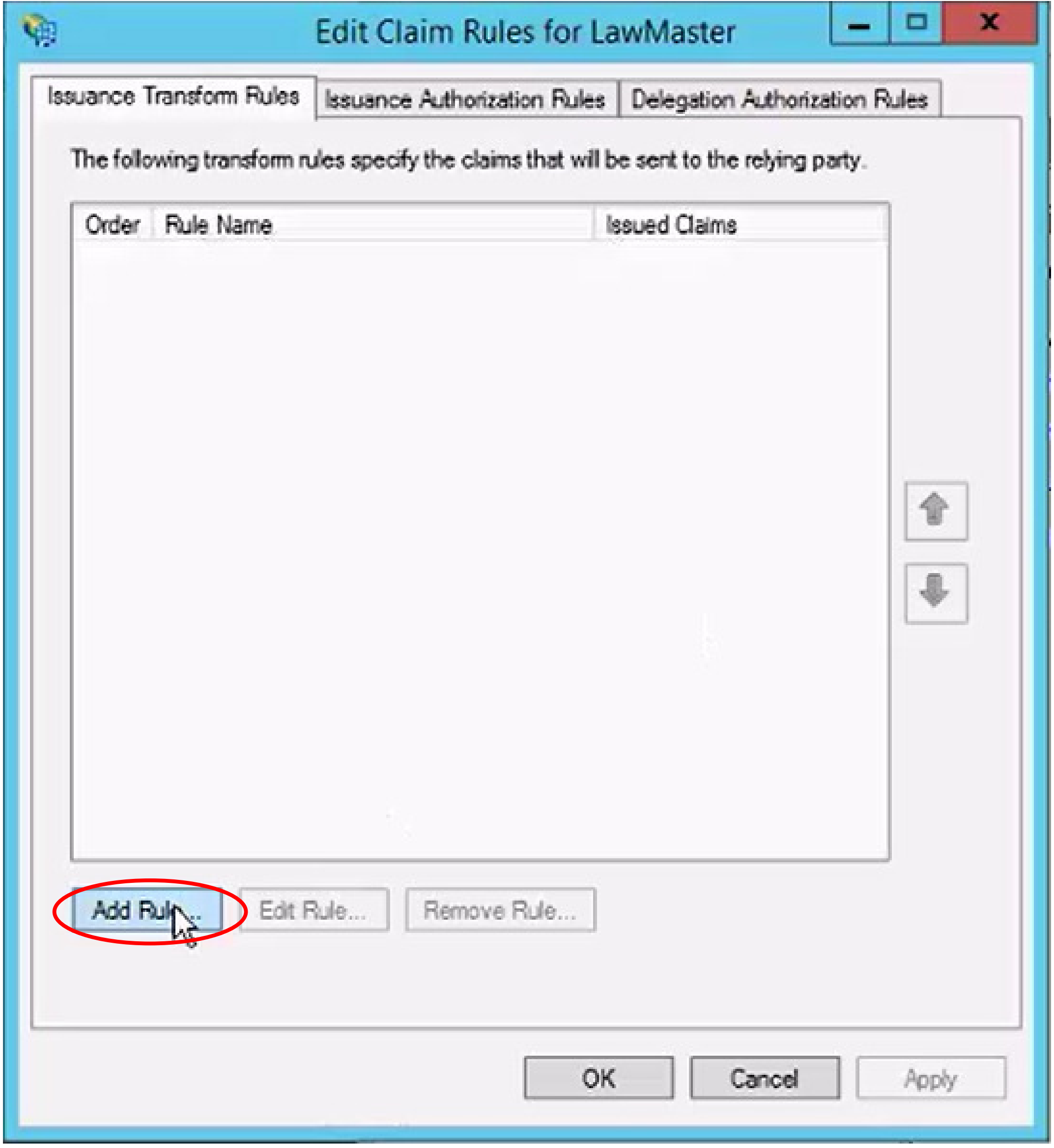


The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

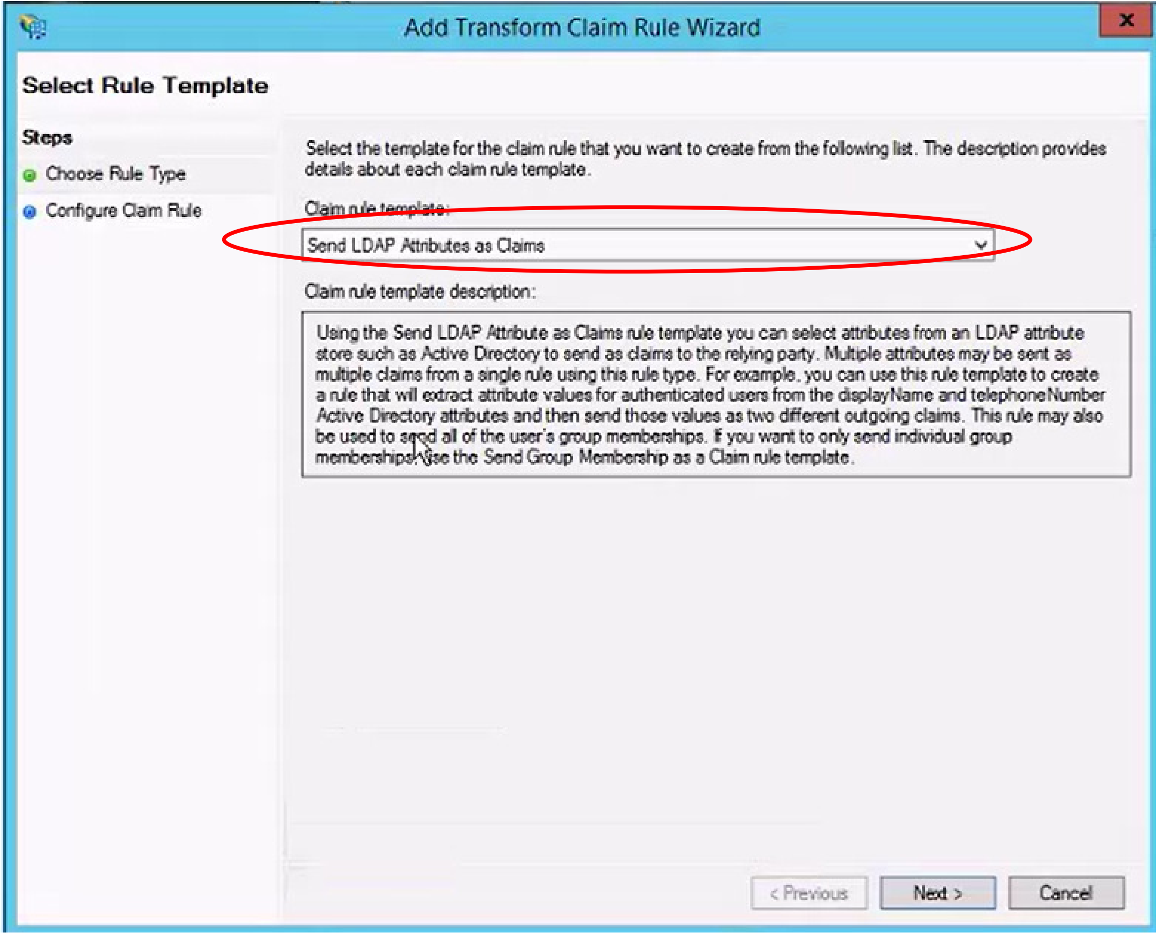
☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

14. Add a claim rule by clicking the *Add Rule* button.



The following transform rules specify the claims that will be sent to the relying party.

15. Choose claim rule template of *Send LDAP Attributes as Claims* and click *Next*.



Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

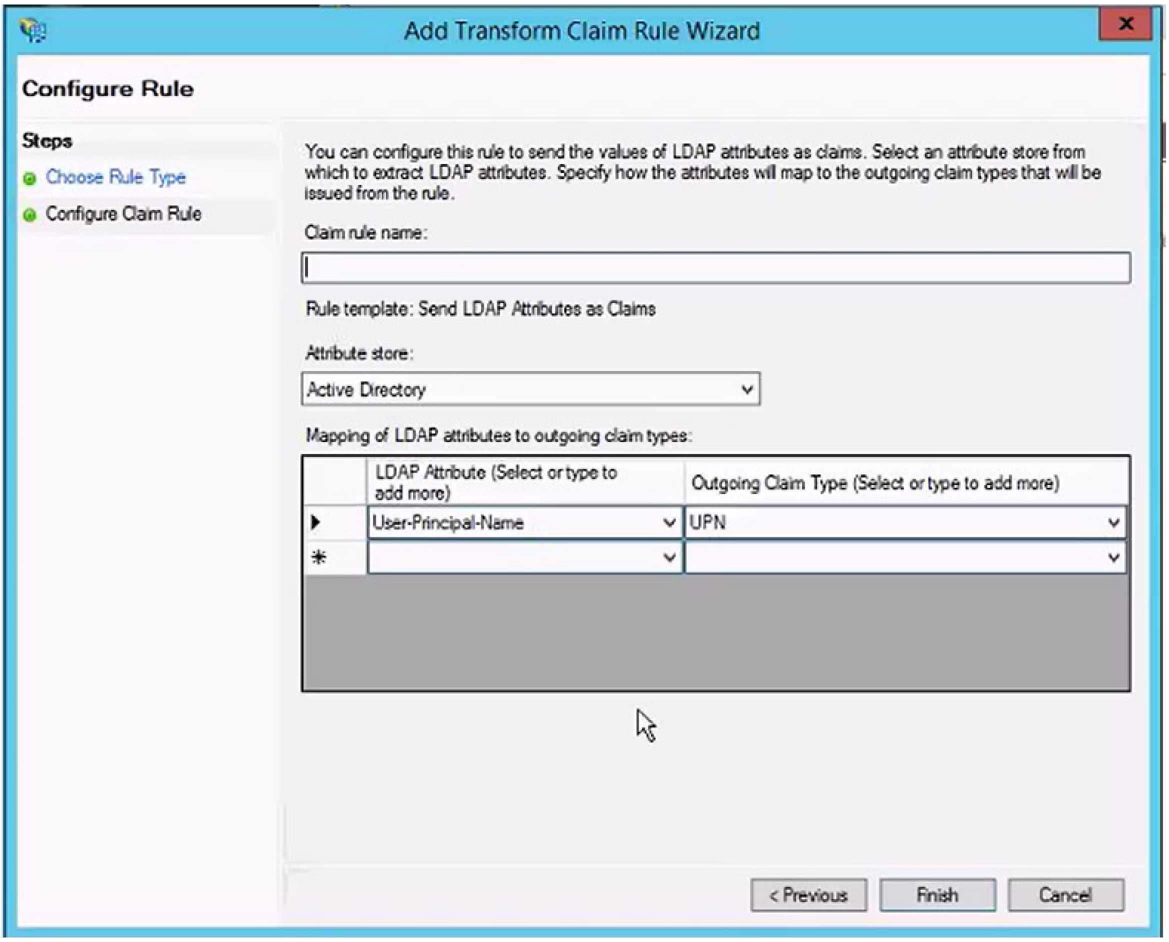
Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

16. Enter a rule name as *LawMaster Claims*, and select *Active Directory* as the Attribute Store. Choose to send *User-Principal-Name* as an outgoing claim of type *UPN*, and then click *Finish*.



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

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:

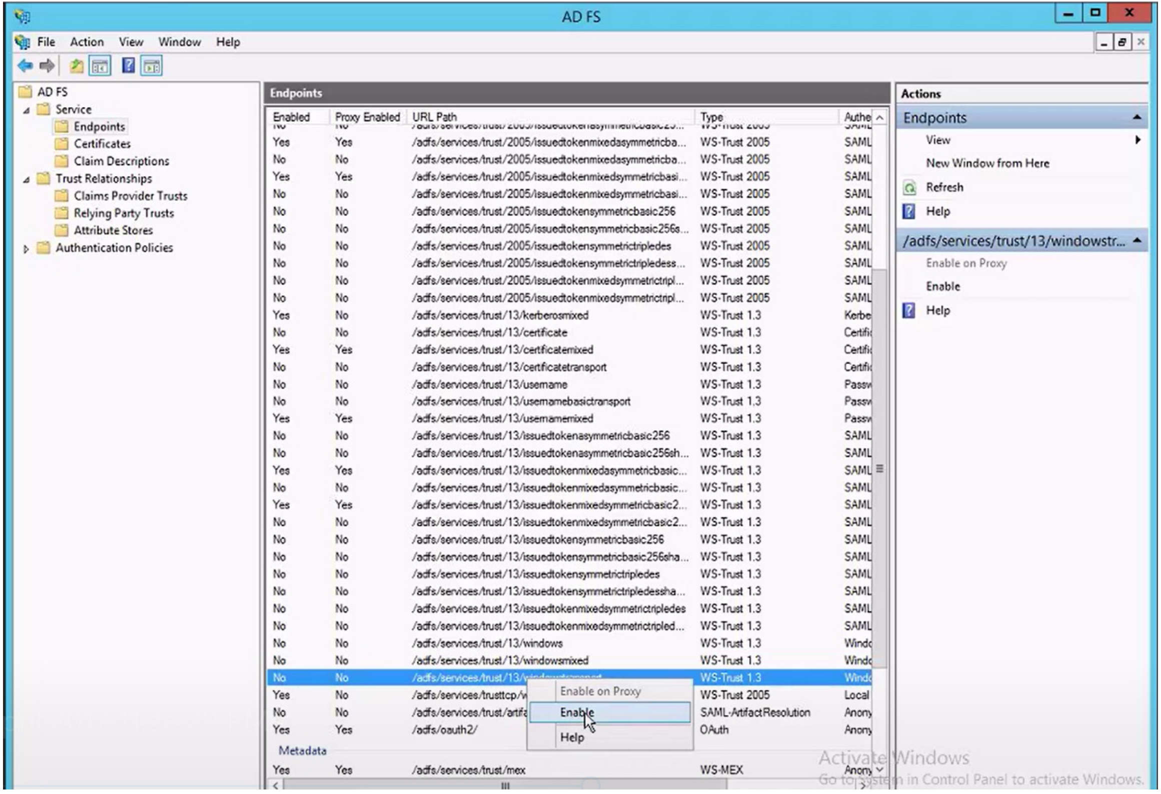
Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	UPN
*		

17. Back in the *AD FS* > *Service* > *Endpoints* configuration:
    a. Enable the endpoint for adfs/services/trust/13/windowstransport
    b. Enable the endpoint for /FederationMetaData/2007-06/FederationMetaData.xml



Endpoints

Enabled	Proxy Enabled	URL Path	Type	Authe
No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic25...	WS-Trust 2005	SAML
Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedasymmetricba...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokenmixedasymmetricba...	WS-Trust 2005	SAML
Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256s...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledes	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledess...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerbe
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certifi
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certifi
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certifi
No	No	/adfs/services/trust/13/usemame	WS-Trust 1.3	Passw
No	No	/adfs/services/trust/13/usemamebasictransport	WS-Trust 1.3	Passw
Yes	Yes	/adfs/services/trust/13/usemamemixed	WS-Trust 1.3	Passw
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sh...	WS-Trust 1.3	SAML
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3	SAML
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256sha...	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha...	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripled...	WS-Trust 1.3	SAML
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windo
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windo
No	No	/adfs/services/trust/13/	WS-Trust 1.3	Windo
Yes	No	/adfs/services/trusttcp/w	WS-Trust 2005	Local
No	No	/adfs/services/trust/artifa	SAML-ArtifactResolution	Anony
Yes	Yes	/adfs/oauth2/	OAuth	Anony
Metadata				
Yes	Yes	/adfs/services/trust/mex	WS-MEX	Anony

18. Refer to the notes below for the internet connectivity.

19. Restart the AD FS service if you are prompted to do so.

AD FS Meta Data Access

- Microsoft AD FS is designed to expose `FederationMetaData.xml` to the Internet.
- LawMaster's application service will attempt to connect to that endpoint to obtain certificate signing information.
- By default, AD FS will change the certificate it uses to sign claims every 12 months.
- If there is some reason you cannot or do not expose that endpoint to the application server, care must be taken to make sure the application service has the latest AD FS signing certificate details.
  a. You will receive a warning when using the authentication options test
  b. Performing that test (and pushing OK) will save the current AD FS certificate signing details with our application server.
  c. If no extra steps are taken, the system will work fine for a period of time until AD FS changes it's signing certificate. (At which point all users will have to login with LawMaster credentials)
  d. If you wish to use AD FS in this way, we recommend disabling the automatic certificate rollover.
  You can use this powershell command to do so:

```
Set-ADFSProperties -AutocertificateRollover $false
```

Single Sign On via Azure Active Directory Authentication

Single Sign On (SSO) can be accomplished through the use of Azure Active Directory authentication. To enable this, your Azure administrator must register your LawMaster installation and provide the Redirect URL, Application (Client) ID and Directory (Tenant) ID.

The Authentication Options Parameter (Set Parameters → Miscellaneous → Authentication Options) has been extended to allow users to select Azure SSO as an option and record the following:

1. Redirect URL for sending the authentication request
2. Application (Client) ID
3. Directory (Tenant) ID

Once the Authentication Options parameter has been configured, individual users must be enabled by ticking the Auto Login option in the Security → Maintain User Security → User Settings area, then adding their Microsoft Email address into the User Name field. When logging into LawMaster, the user will be prompted to select which Microsoft Account to use and will be prompted to provide their Microsoft Account password if they have not recently done so.