



# Implementing ADFS

---

Version 1.0

Last updated: 10th Nov 2017

Author: Sukhjinder Singh

E: [customerservices@peoplehr.com](mailto:customerservices@peoplehr.com)

## Table of Contents

INTRODUCTION .....	3
SETUP ON ADFS .....	4
SETUP ON PEOPLEHR .....	11

### 1. Introduction

People HR supports Single Sign-on (SSO) authentication in conjunction with identity provided by Active Directory Federation Services (ADFS).

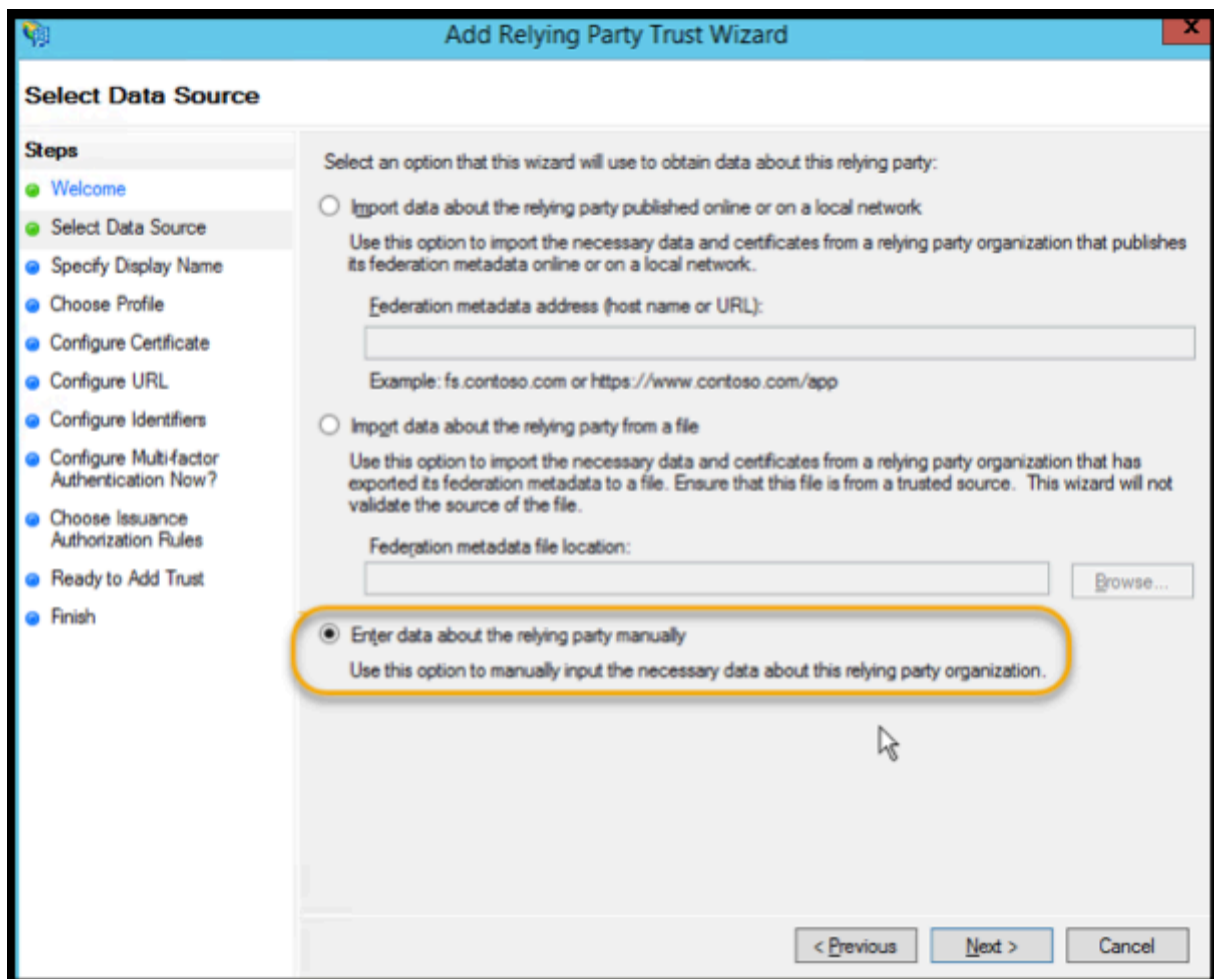
Please note all your users in your active directory will need to have an email address attribute.

## 2. Setup ADFS

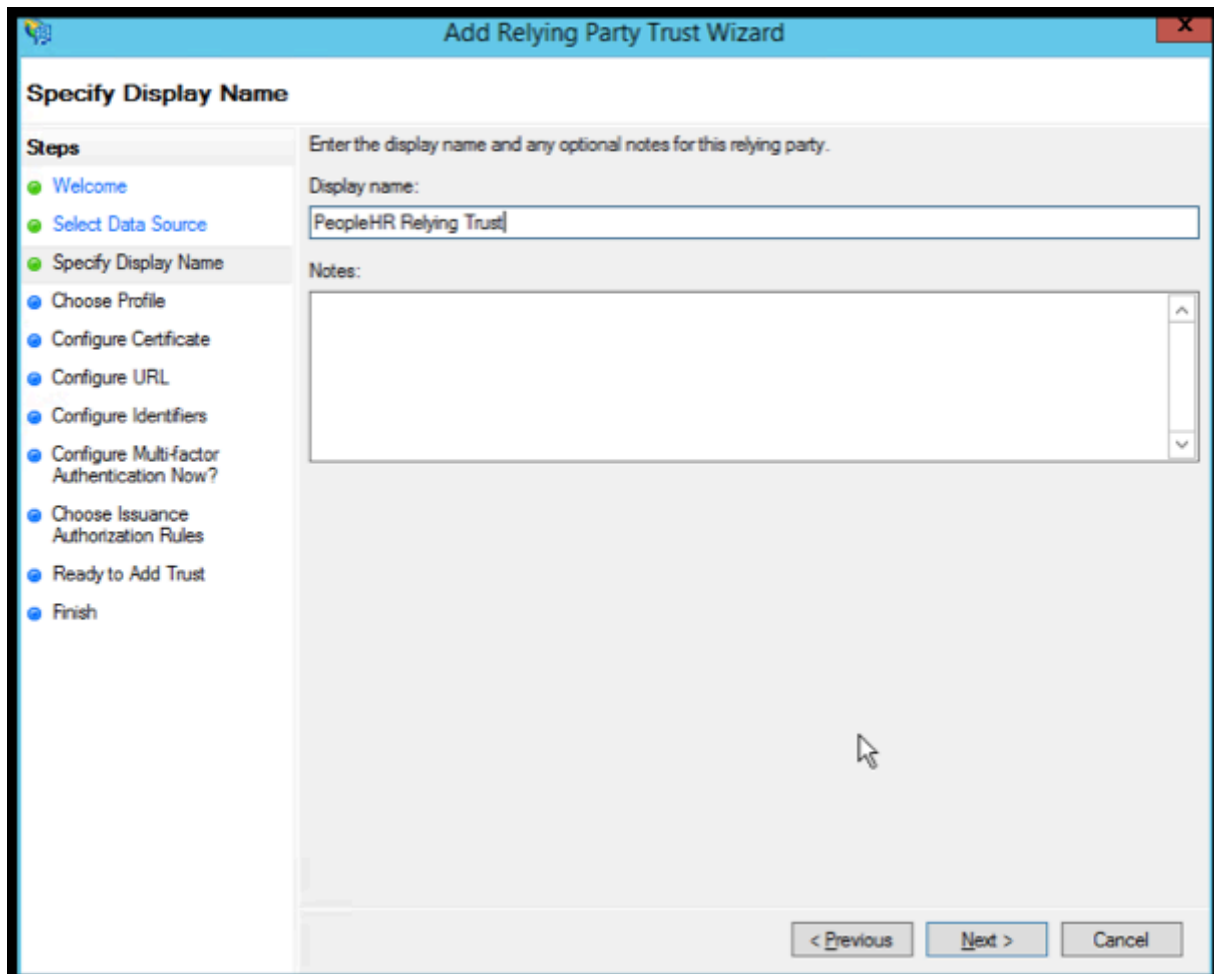
The steps below are for ADFS v3.0:

On the ADFS server, open the ADFS Management tool

1. Right click on Relying Party Trust and click 'Add Relying Party Trust'
2. On the welcome screen, click 'Start'
3. Select the option for 'Enter data about the relying party manually' and click 'Next'




4. Enter a Display name and any notes you may want to add, then click 'Next'



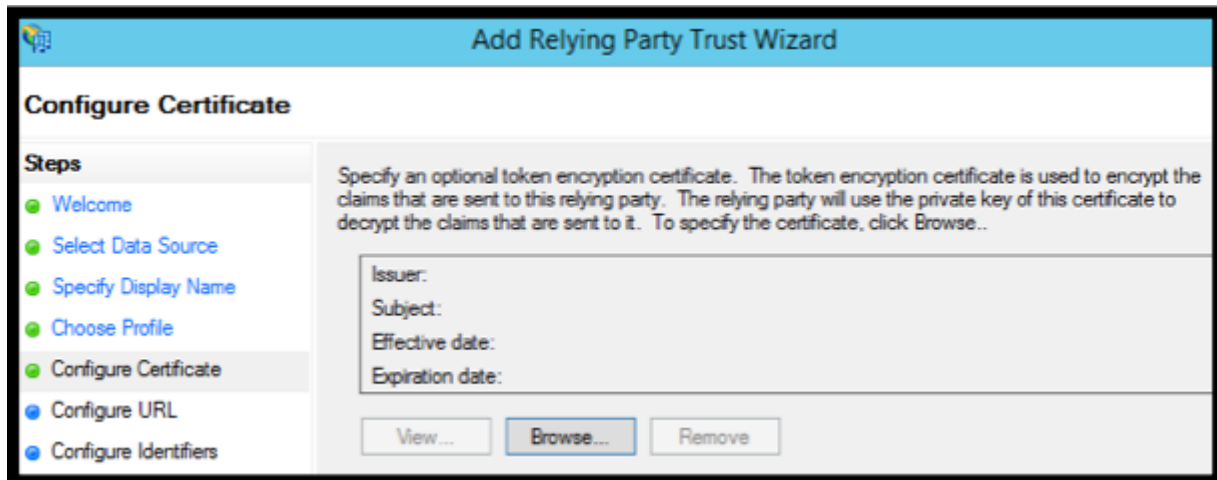
The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The window has a blue title bar with the text 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (current step), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the text '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 'PeopleHR Relying Trust'. Below the text box is a 'Notes:' label and a large text area. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

5. Make sure ADFS profile is selected, then click 'Next'



The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Choose Profile' step. The window has a blue title bar with the text 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile (current step), Configure Certificate, and Configure URL. 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 text, there are two radio button options. The first option is 'AD FS profile', which is selected (indicated by a filled radio button) and highlighted with a yellow rounded rectangle. Below it is a description: 'This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.' The second option is 'AD FS 1.0 and 1.1 profile', which is not selected (indicated by an empty radio button). Below it is a description: 'This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.'

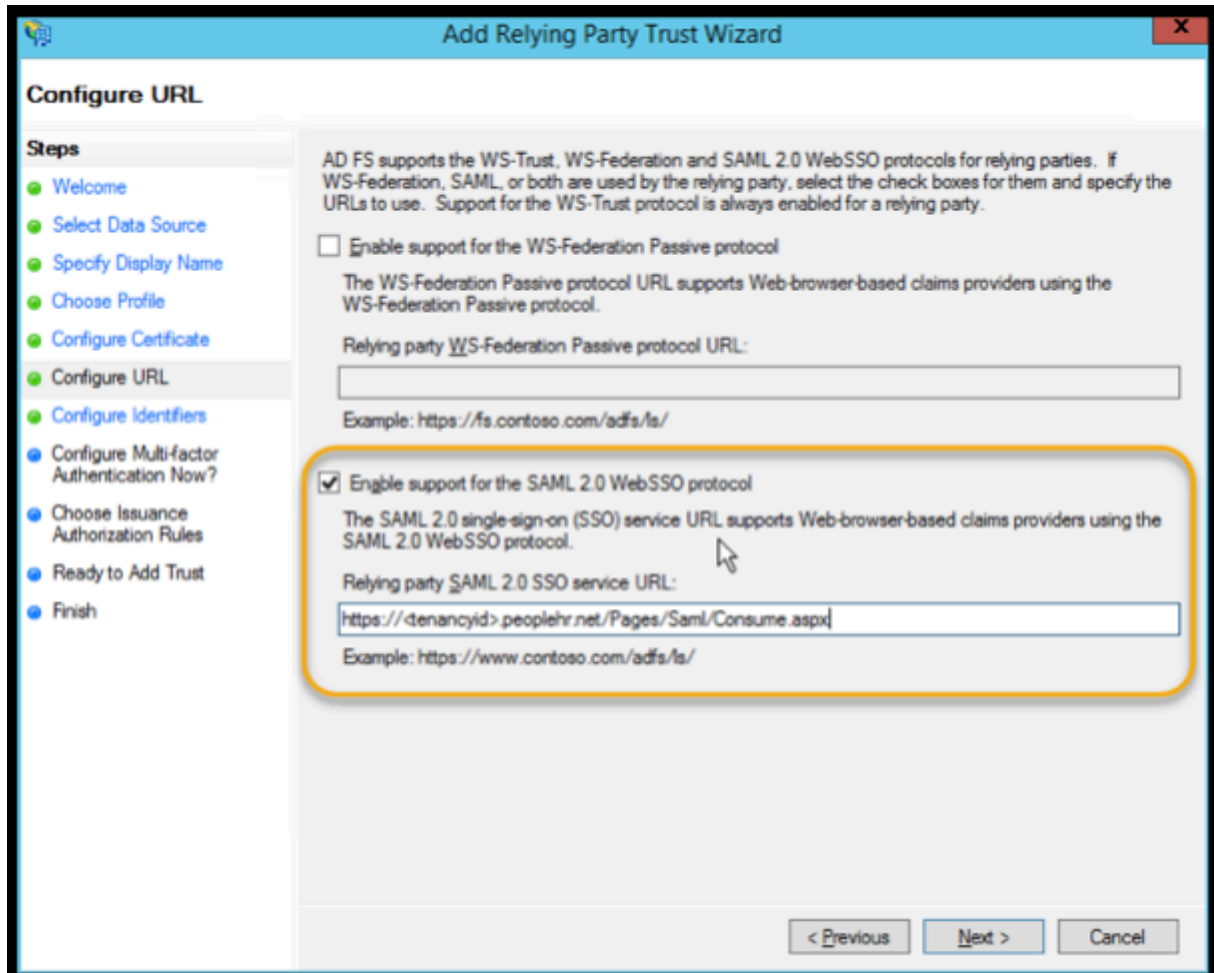
6. Under the Configure Certificate section, add a certificate if required, otherwise just click 'Next' to continue



The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Configure Certificate' step. The window has a blue title bar with the text 'Add Relying Party Trust Wizard'. Below the title bar, the main content area is titled 'Configure Certificate'. On the left side, there is a 'Steps' panel with a list of steps: 'Welcome', 'Select Data Source', 'Specify Display Name', 'Choose Profile', 'Configure Certificate' (which is highlighted with a green circle), 'Configure URL', and 'Configure Identifiers'. The main area on the right contains a text box with the following text: 'Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..'. Below this text box, there are four input fields: 'Issuer:', 'Subject:', 'Effective date:', and 'Expiration date:'. At the bottom of the main area, there are three buttons: 'View...', 'Browse...' (which is highlighted with a blue border), and 'Remove'.

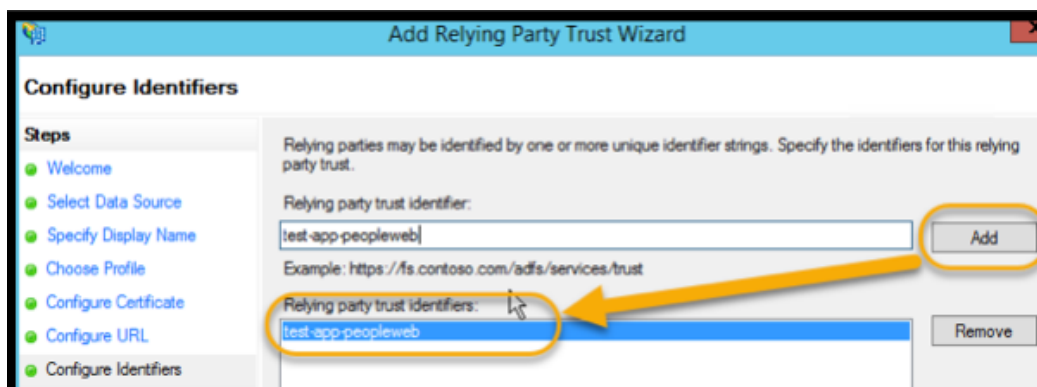
7. Under the section to Configure URL, tick the option to 'Enable support for the SAML 2.0 WebSSO protocol'

8. For the Relying party SAML 2.0 SSO service URL, enter:  
`https://<tenancyid>.peoplehr.net/Pages/Saml/Consume.aspx` (Make sure you enter the correct tenancy id – should match the link you use to access your company specific People HR portal).



9. Click 'Next' to configure the identifiers

10. For the Relying party trust identifier, enter 'test-app-peopleweb' and click on the 'Add' button



11. Click 'Next'

12. Ensure 'I do not want to configure multi-factor authentication settings for this relying party trust at this time' is selected and click 'Next'

The screenshot shows the 'Configure Multi-factor Authentication' wizard. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, **Configure Multi-factor Authentication Now?** (highlighted), Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main content area has a title bar with 'Multi-factor Authentication' and 'Global Settings'. Below the title bar is a table:

Requirements	Users/Groups	
		Not configured
	Device	Not configured
	Location	Not configured

Below the table, there are two radio button options. The first option, 'I do not want to configure multi-factor authentication settings for this relying party trust at this time.', is selected and highlighted with a yellow box. The second option is 'Configure multi-factor authentication settings for this relying party trust.' At the bottom, there is a note: '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](#).'

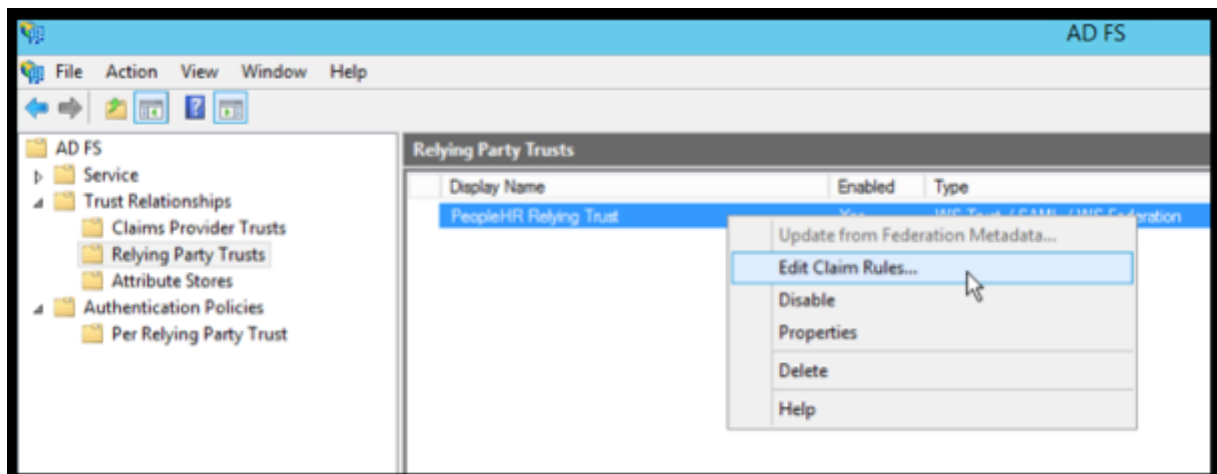
13. Under Choose Issuance Authorisation Rules, ensure 'Permit all users to access this relying party' is selected, and click 'Next'

The screenshot shows the 'Choose Issuance Authorization Rules' wizard. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, **Choose Issuance** (highlighted), Ready to Add Trust, and Finish. The main content area has a title bar with 'Choose Issuance Authorization Rules'. Below the title bar is a text box: '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.' Below this text box are two radio button options. The first option, 'Permit all users to access this relying party', is selected and highlighted with a yellow box. Below this option is a description: '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.' The second option is 'Deny all users access to this relying party', with a description: '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.' At the bottom, there is a note: '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.'

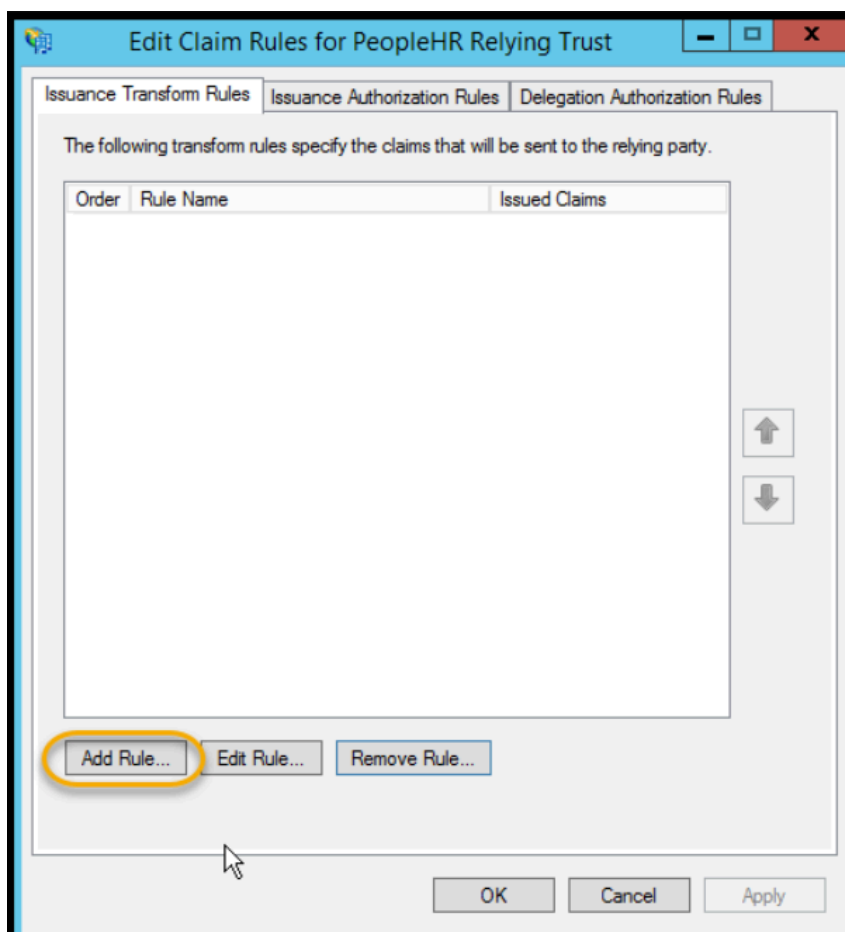
14. Under ready to Add Trust, click 'Next' and then Finish to complete the initial setup.



15. Under Relying Party Trusts, right click on the People HR Relying Trust that was just created, and click 'Edit Claim Rules'



16. Under the Issuance Transform Rules, click 'Add Rule'.



Please set up an LDAP rule and select the attribute E-Mail-Addresses and the outgoing claim Type to Name ID

17. Click 'Finish' to add the rule.

18. This is the ADFS config finished, close the ADFS Management console

**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: nameid

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)
E-Mail-Addresses	Name ID
*	

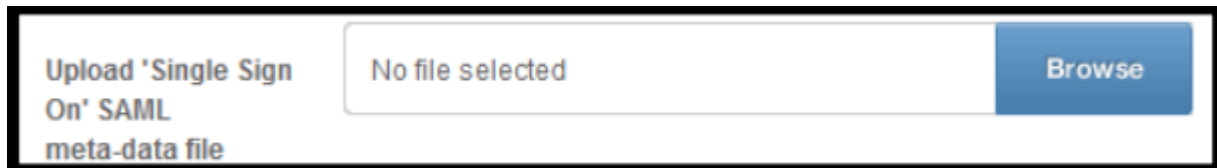
< Previous Finish Cancel

19. Download the metadata.xml file from the following link: <https://sts.YOURSERVER.com/FederationMetadata/2007-06/FederationMetadata.xml>

### 3. Setup on People HR

20. Log into the People HR portal using an account that has Full Admin access

21. Navigate to 'Settings' > 'Company' and under Upload 'Single Sign On' SAML meta-data file, click on 'browse' and upload the metadata.xml file downloaded earlier

A screenshot of a web interface for uploading a SAML meta-data file. On the left, the text 'Upload 'Single Sign On' SAML meta-data file' is displayed. To the right is a file selection area containing a light gray box with the text 'No file selected' and a blue button labeled 'Browse'.

Single Sign On should now be working.