

CAUSELINK ADFS CONFIGURATION

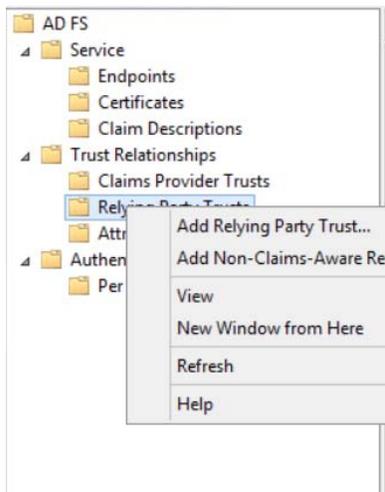
Updated: March 30th, 2017

Prerequisites / Caveats

- Self-signed certificates are **NOT** supported
- Your ADFS server or proxy must be accessible to the Causelink service
- An understanding that our implementation is a Service Provider (SP) initiated logon
- Users must log into the system before their name appears as a user within Causelink

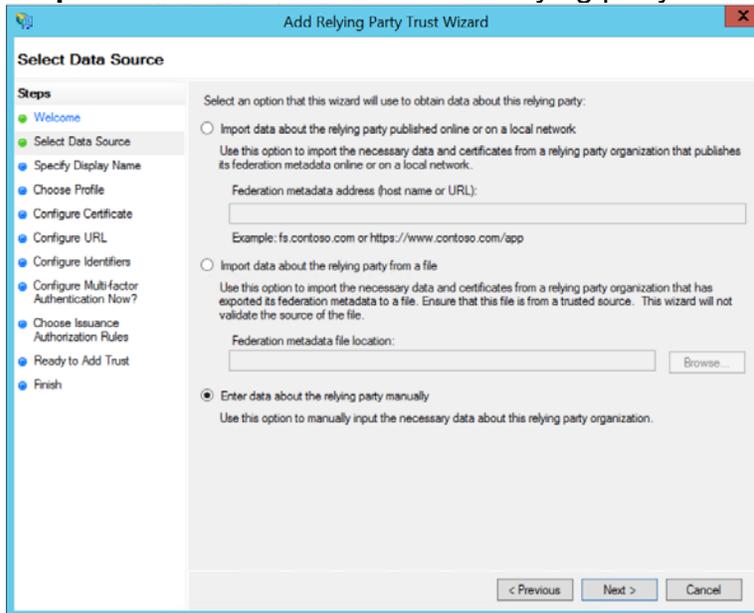
Configuration

Step 1. In the ADFS Management Console right click Relying Party Trusts then click on Add Relying Party Trust.



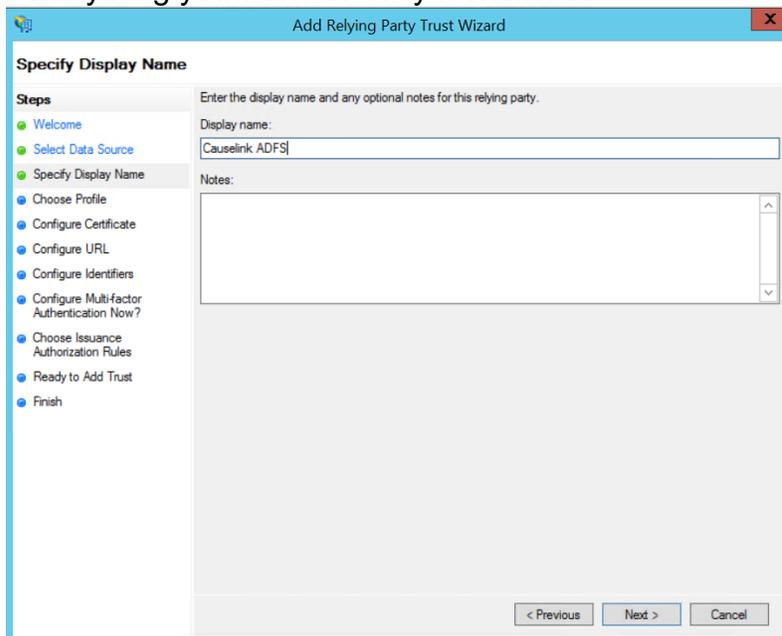
causelink® enterprise

Step 2. Choose Enter data about relying party manually then click Next



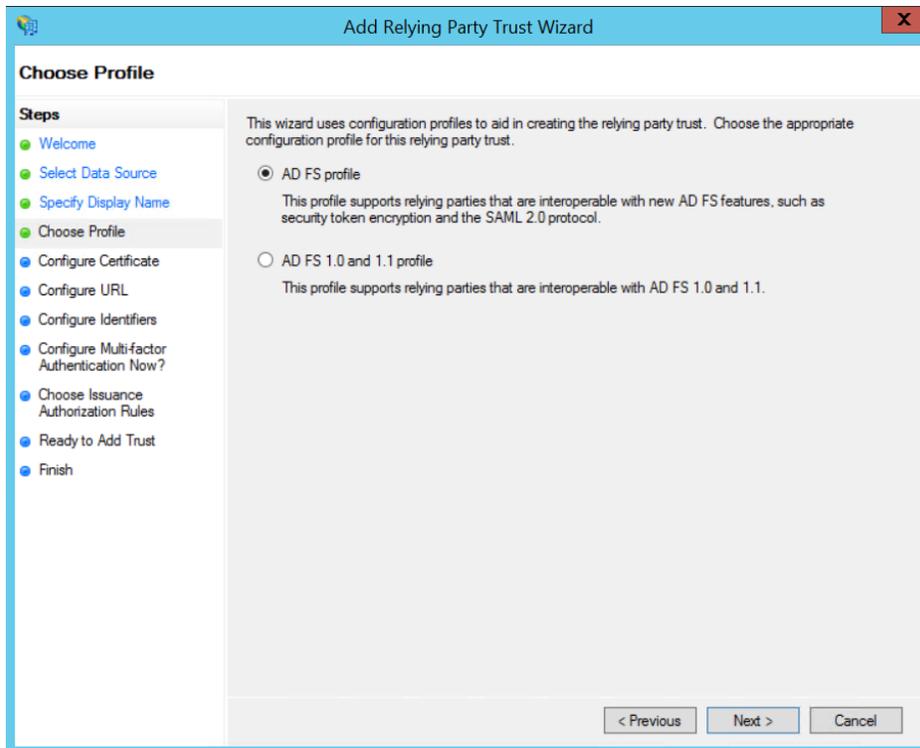
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Select Data Source' and contains the instruction: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' (unselected), with a sub-instruction to import data from a relying party organization and a text box for 'Federation metadata address (host name or URL)'. 2. 'Import data about the relying party from a file' (unselected), with a sub-instruction to import data from a file and a text box for 'Federation metadata file location' with a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected), with a sub-instruction to manually input the necessary data. At the bottom, there are '< Previous', 'Next >', and 'Cancel' buttons.

Step 3. Enter a display name and any notes that may be necessary then click Next. In the example below Causelink ADFS is entered as an example. It can be anything you want for easy identification.

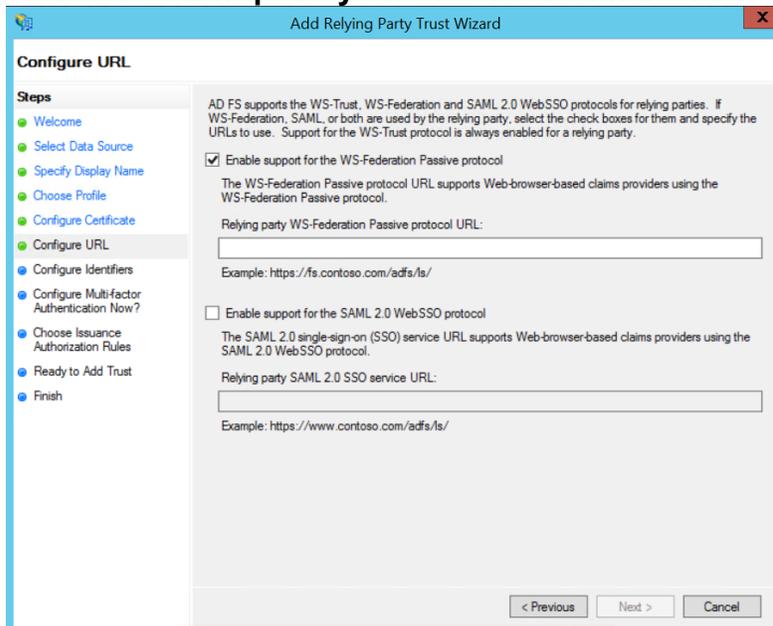


The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. On the left, the 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Specify Display Name' and contains the instruction: 'Enter the display name and any optional notes for this relying party.'. There is a text box for 'Display name:' containing the text 'Causelink ADFS'. Below it is a 'Notes:' text area. At the bottom, there are '< Previous', 'Next >', and 'Cancel' buttons.

Step 4. Choose AD FS profile then click Next

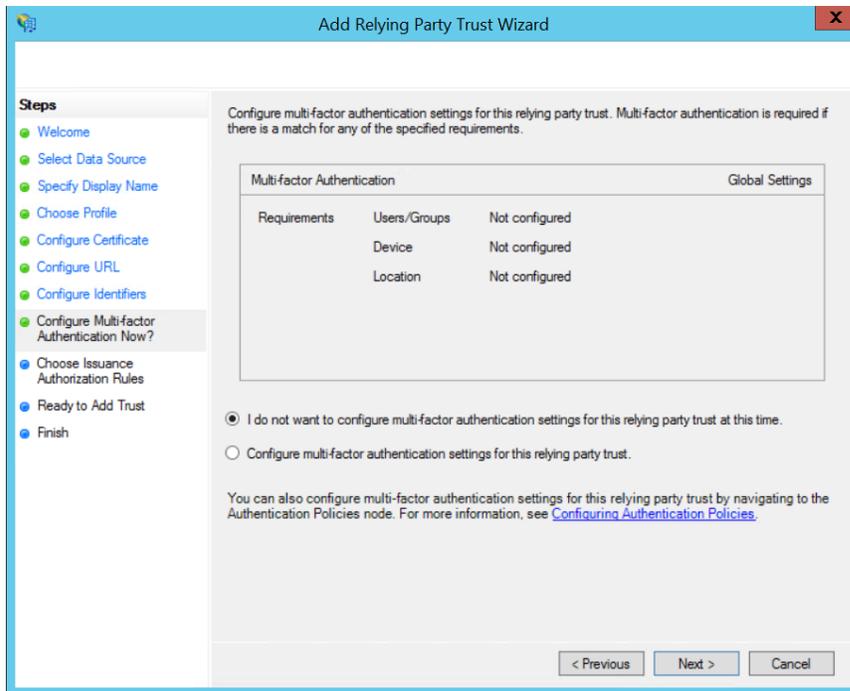


Step 5. Choose Enable support for the WS-Federation Passive Protocol and enter the URL **https://<your-site>.causelink.com/adfs** then click Next.

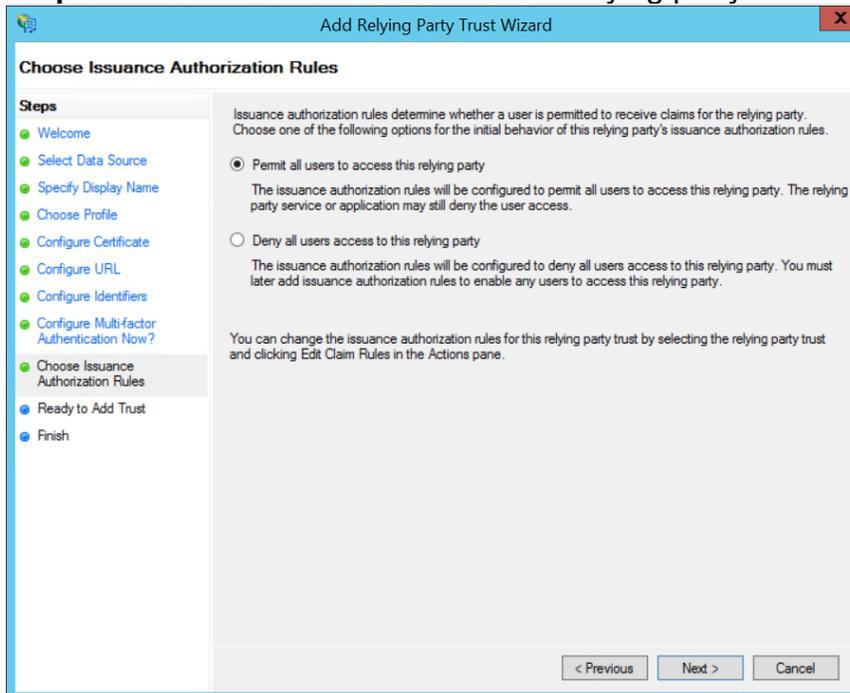


Step 6. On the next screen just click Next.

Step 7. Choose I do not want to configure multi-factor authentication then click Next



Step 8. Permit All users to access this relying party then Next



Step 9. At this point the trust has been configured click Next

causelink® enterprise

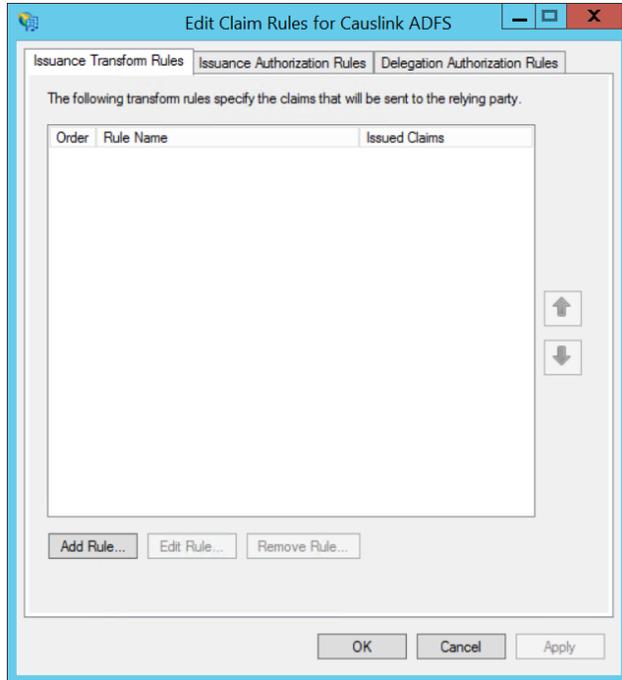
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main area is titled 'Ready to Add Trust'. On the left, a 'Steps' list includes: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust (highlighted), and Finish. The main content area contains the 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 tabs for Monitoring, Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Note. The 'Monitoring' tab is active. It contains the text: 'Specify the monitoring settings for this relying party trust.' followed by 'Relying party's federation metadata URL:' and an empty text box. Below the text box are two checkboxes: 'Monitor relying party' (checked) and 'Automatically update relying party' (unchecked). Further down, it says 'This relying party's federation metadata data was last checked on: < never >' and 'This relying party was last updated from federation metadata on: < never >'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Step 10. Leave the box checked and choose Close.

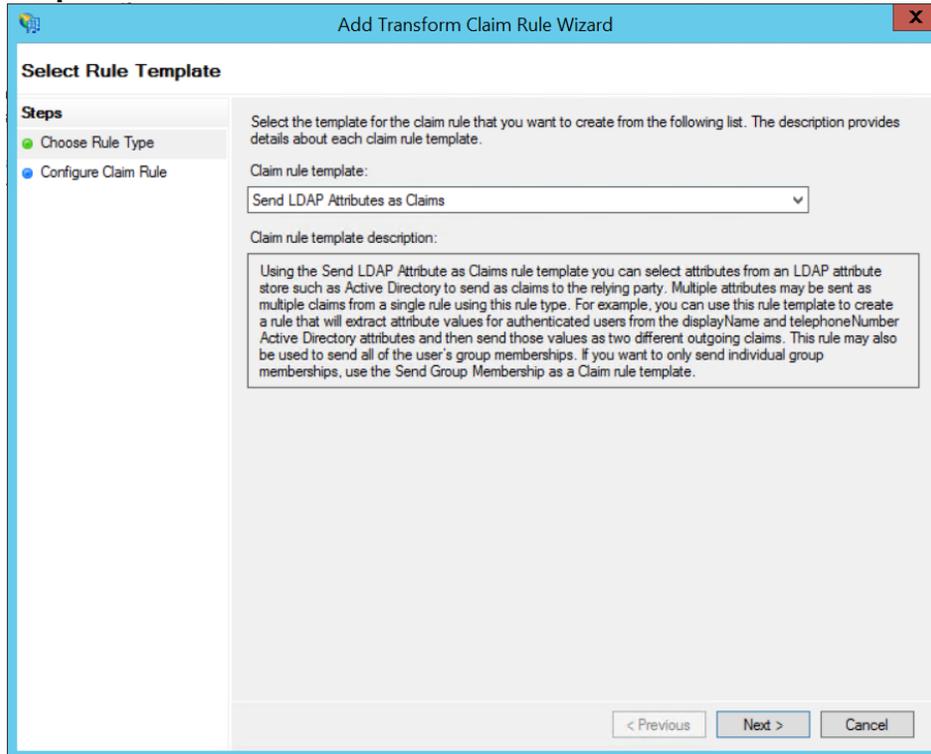
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main area is titled 'Finish'. On the left, a 'Steps' list includes: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish (highlighted). The main content area contains the 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 Management snap-in.' Below this is a checkbox labeled 'Open the Edit Claim Rules dialog for this relying party trust when the wizard closes', which is checked. At the bottom right, there is a 'Close' button.

Step 11. Click Add Rule

causelink® enterprise



Step 12. Choose Send LDAP Attributes as Claims then click Next



causelink® enterprise

Step 13. Enter a Claim rule name it can be anything. For Attribute store choose Active Directory. Below that enter the following claims. objectGUID is the only one that will need to be manually typed in, everything else is selectable from the lists that pop up. Once everything is entered choose OK.

E-Mail-Addresses -> E-Mail Address (sends Email listed in AD as Claim)
Surname -> Surname (sends Last Name in AD as Claim)
Given-Name -> Given Name (sends First Name in AD as Claim)
objectGUID -> PPID (send GUID in base64 for unique user identification as Claim)

Edit Rule - LDAP Claims

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:

Mapping of LDAP attributes to outgoing claim types:

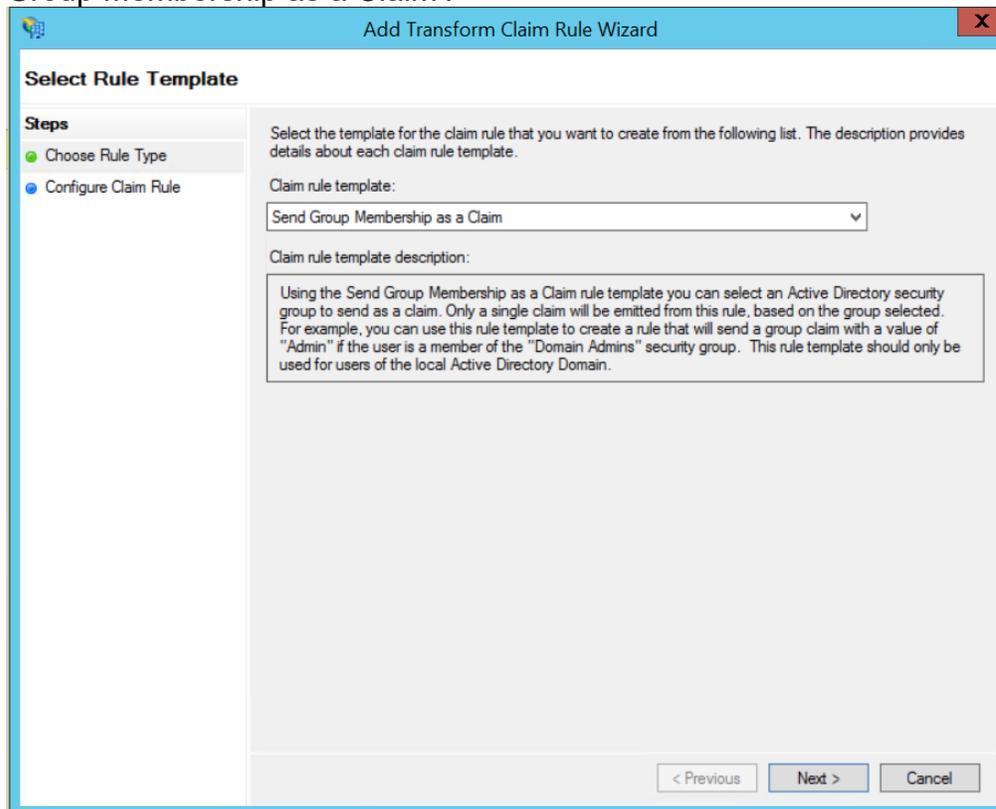
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Display-Name	Common Name
	User-Principal-Name	UPN
	E-Mail-Addresses	E-Mail Address
	Surname	Surname
	Given-Name	Given Name

Optional – Configure Additional Claims

Causelink can be configured to only allow users meeting certain criteria into the system. Your claim can be whatever you like, and ADFS allows for claim chaining meaning you can combine many claims into a single outbound value.

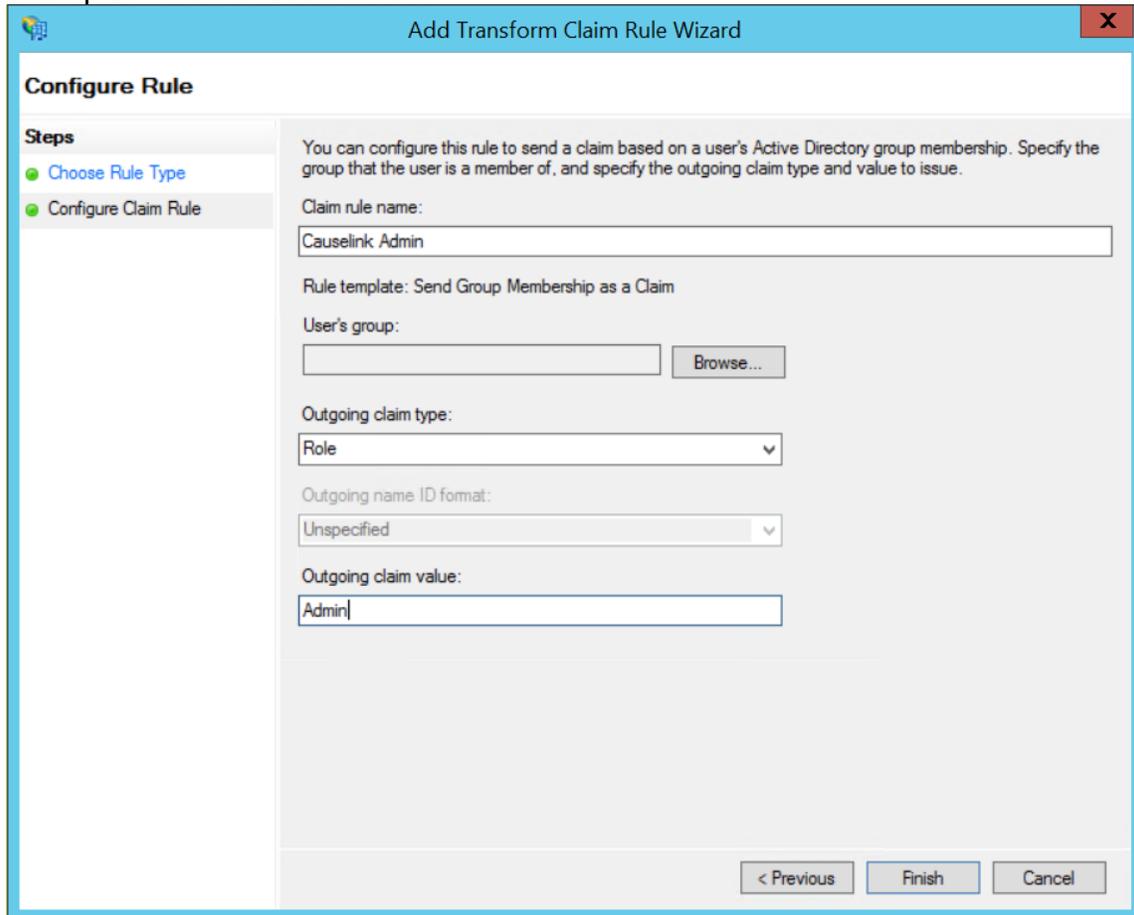
In our example we specify a group claim 'Role'.

Step 1. Click to add another rule, and this time choose the template 'Send Group Membership as a Claim'.



causelink® enterprise

Step 2. Give the claim rule a name and after that choose an internal AD group for the role to be mapped to. The outgoing claim type is set to 'Role' in our example. Then choose finish.



The screenshot shows a Windows-style dialog box titled "Add Transform Claim Rule Wizard" with a close button (X) in the top right corner. The main area is titled "Configure Rule". On the left, there is a "Steps" sidebar with two items: "Choose Rule Type" (highlighted with a green dot) and "Configure Claim Rule" (with a green dot). The main content area contains the following fields and instructions:

- Instruction: "You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue."
- Field: "Claim rule name:" with a text box containing "Causelink Admin".
- Text: "Rule template: Send Group Membership as a Claim".
- Field: "User's group:" with an empty text box and a "Browse..." button.
- Field: "Outgoing claim type:" with a dropdown menu set to "Role".
- Field: "Outgoing name ID format:" with a dropdown menu set to "Unspecified".
- Field: "Outgoing claim value:" with a text box containing "Admin".

At the bottom right, there are three buttons: "< Previous", "Finish", and "Cancel".

Step 3. Be sure to let Sologic know what your claim type name is, because the application must be configured to match this value, and the configuration is not available via the administrative interface.

Optional – Adjust user roles and group associations

User roles and group associations are defined within Causelink. All users are added to the system under the Analyst role (see the User Guide for a description of all role capabilities). Once a user has accessed the system, and their name appears in the People page, you can change their Role and/or Group association from that page.