causelink® enterprise

CAUSELINK ADFS CONFIGURATION

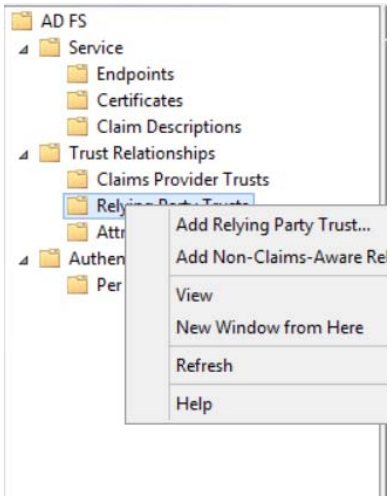
Updated: March 30th, 2017

Prerequisites / Caveats

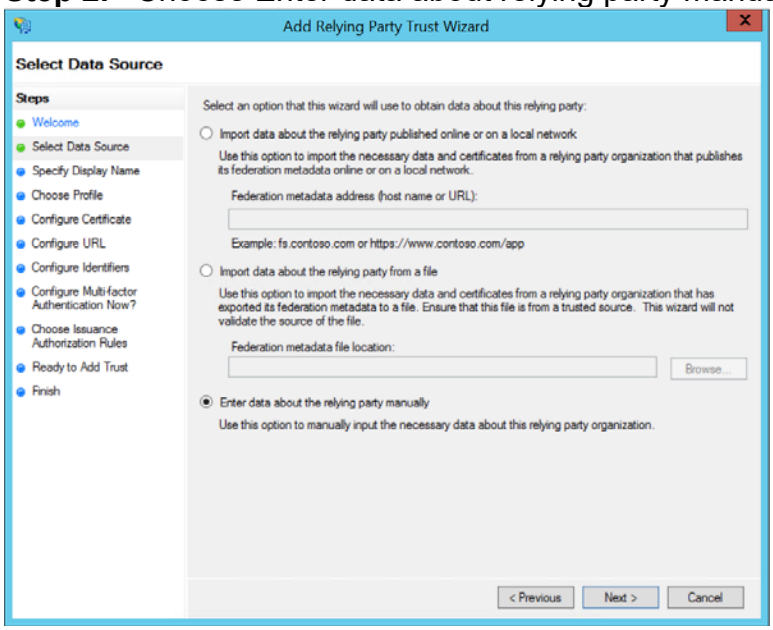
- Self-signed certificates are **NOT** supported
- Your ADFS server or proxy must be accessible to the Causelink service
- An understanding that our implementation is a Service Provider (SP) initiated logon
- Users must log into the system before their name appears as a user within Causelink

Configuration

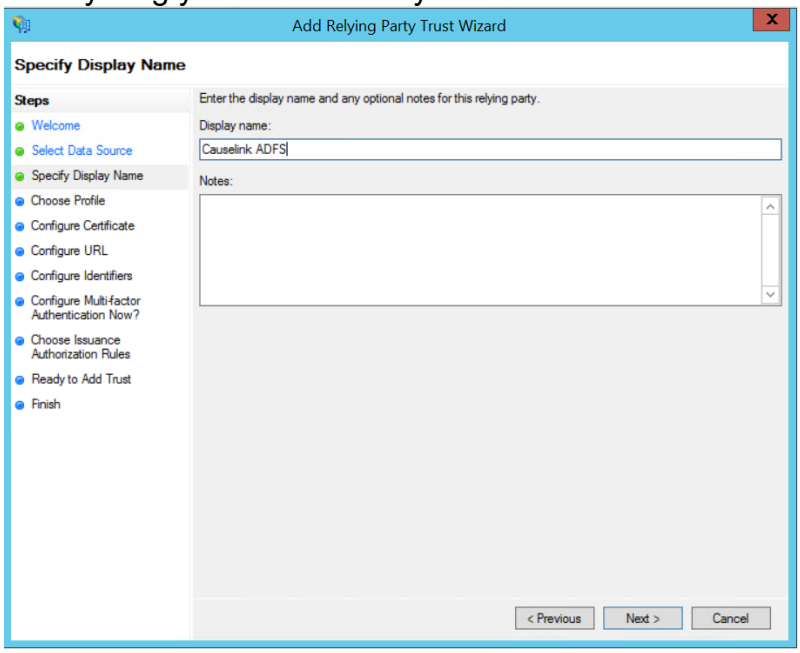
Step 1. In the ADFS Management Console right click Relying Party Trusts then click on Add Relying Party Trust.



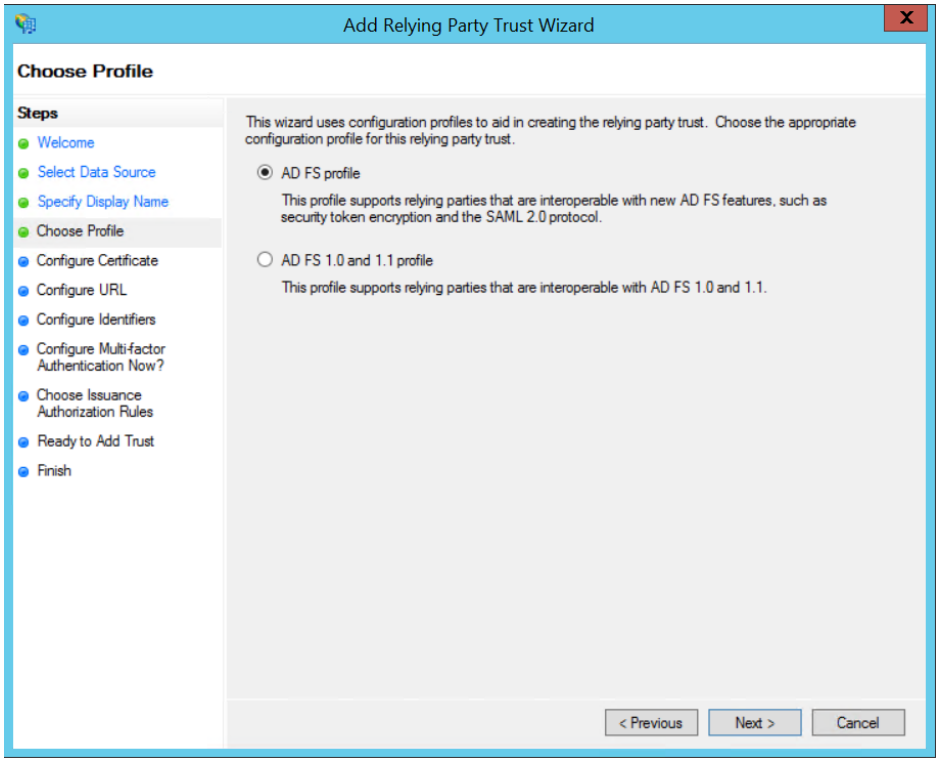
Step 2. Choose Enter data about relying party manually then click Next



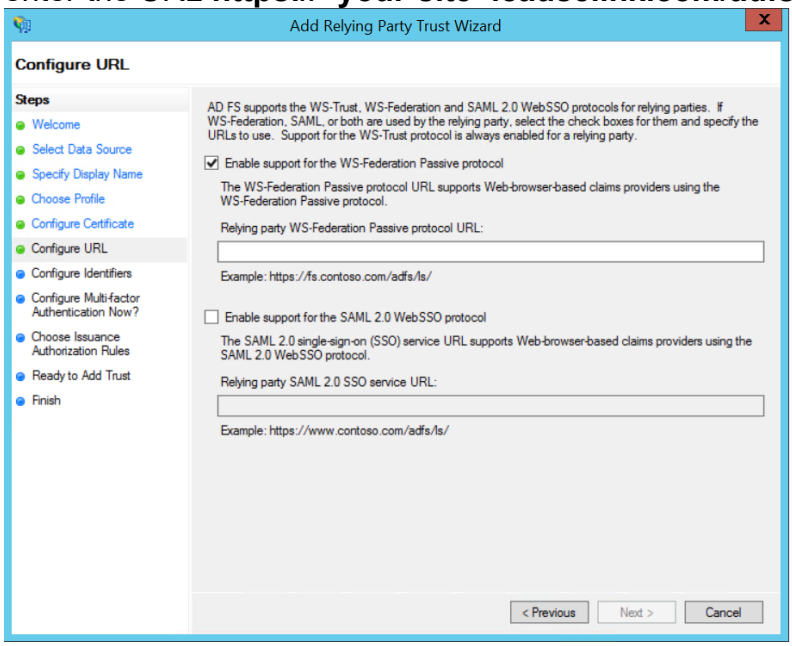
Step 3. Enter a display name and any notes that may be necessary then click Next. In the example below Causelink ADFS is entered as an example. It can be anything you want for easy identification.



Step 4. Choose AD FS profile then click Next

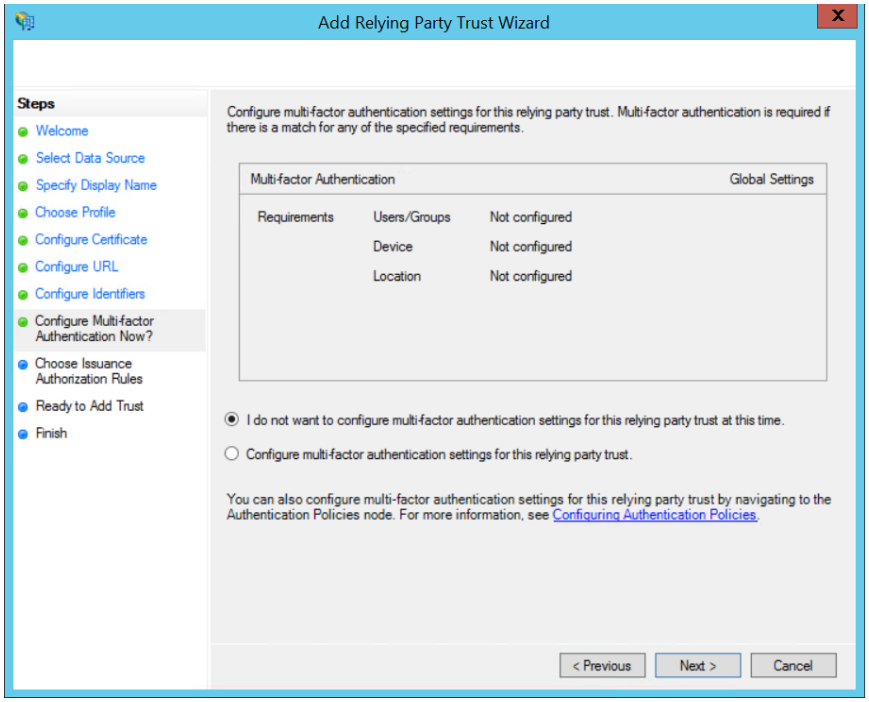


Step 5. Choose Enable support for the WS-Federation Passive Protocol and enter the URL **https://<your-site>.causelink.com/adfs** then click Next.

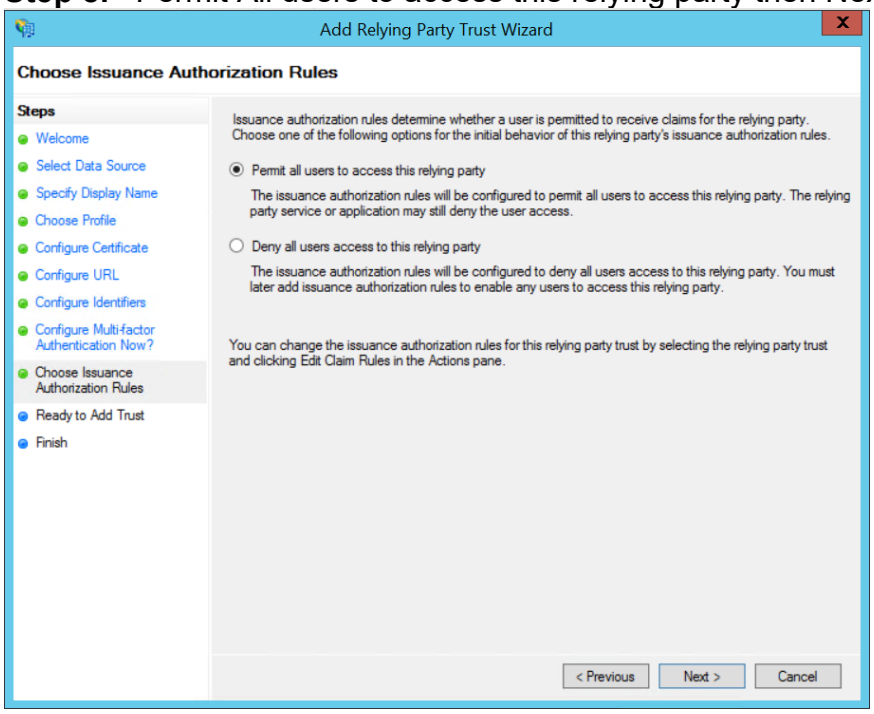


Step 6. On the next screen just click Next.

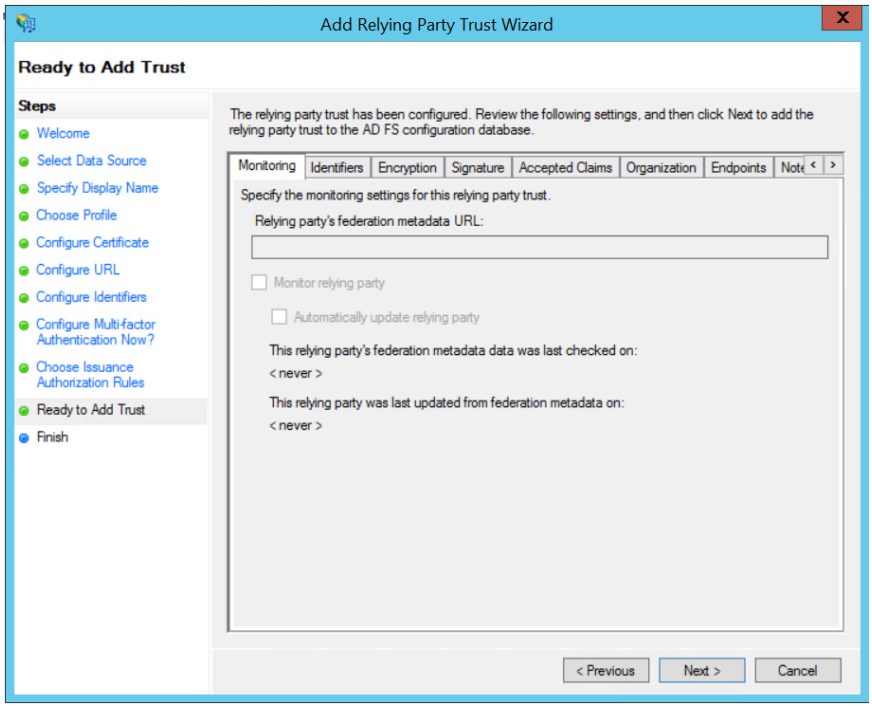
Step 7. Choose I do not want to configure multi-factor authentication then click Next



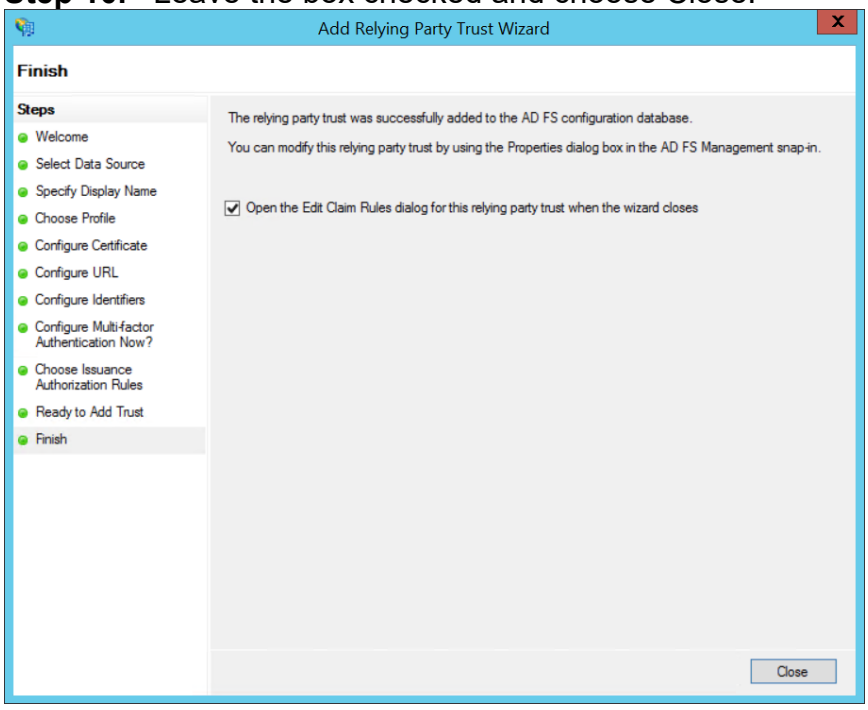
Step 8. Permit All users to access this relying party then Next



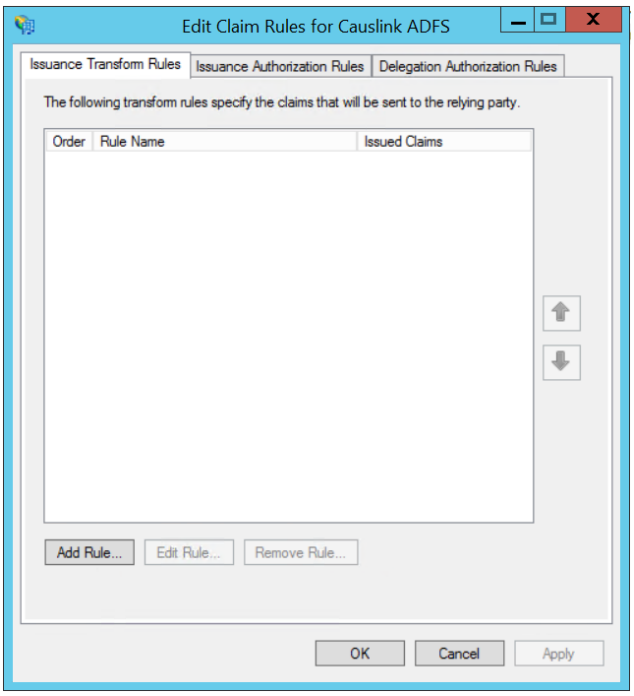
Step 9. At this point the trust has been configured click Next



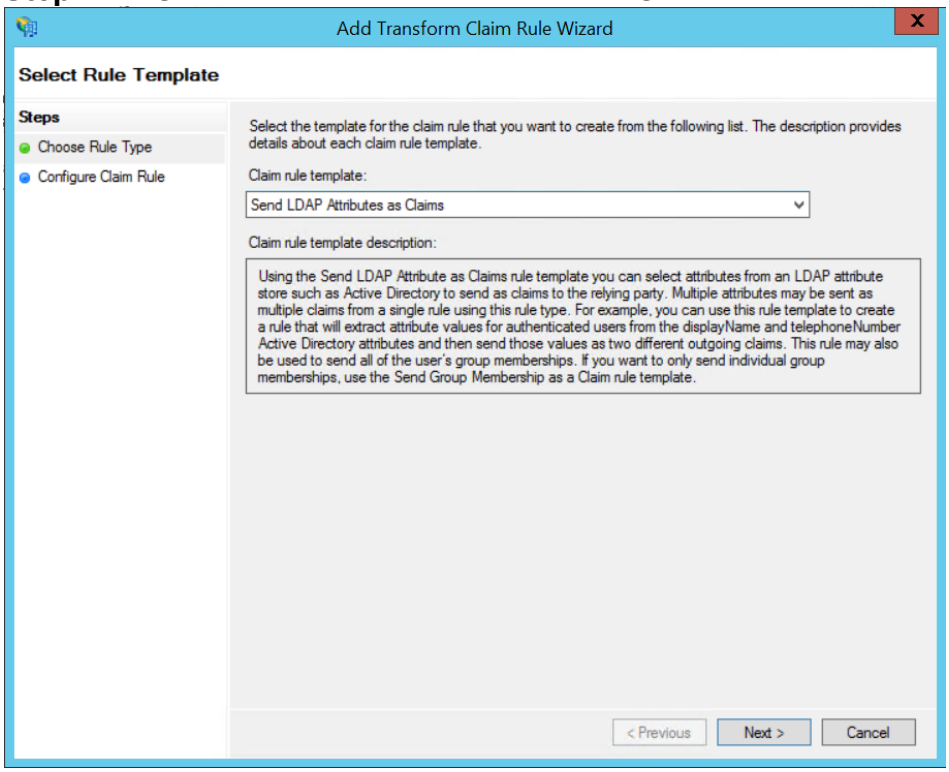
Step 10. Leave the box checked and choose Close.



Step 11. Click Add Rule

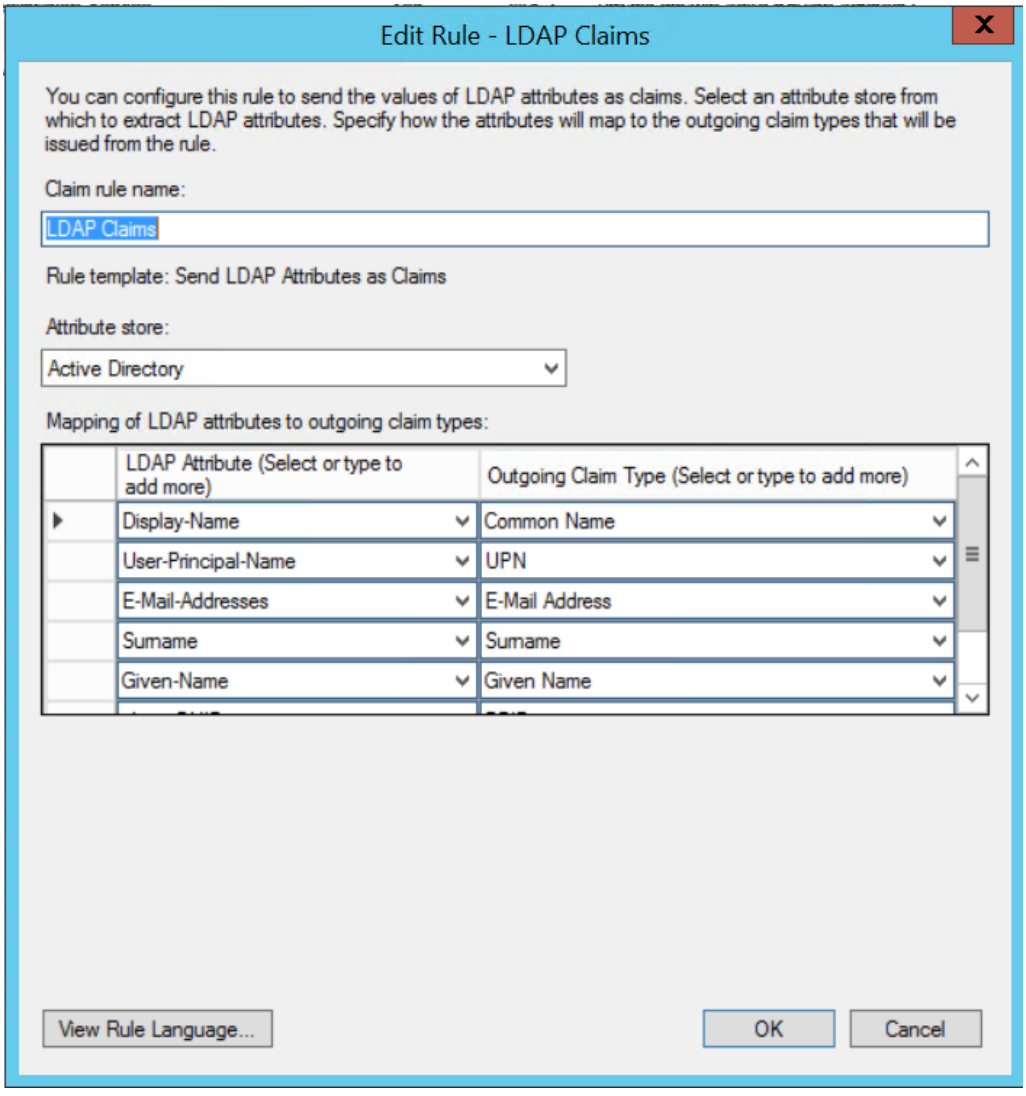


Step 12. Choose Send LDAP Attributes as Claims then click Next



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)

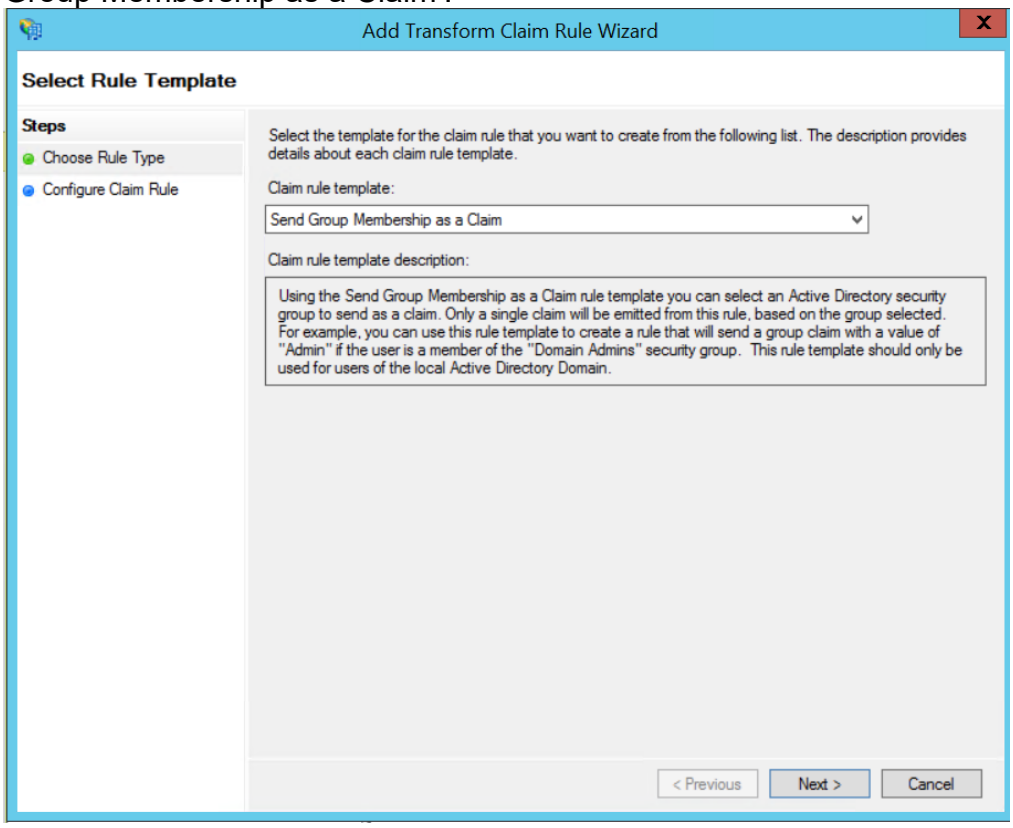


Optional – Configure Additional Claims

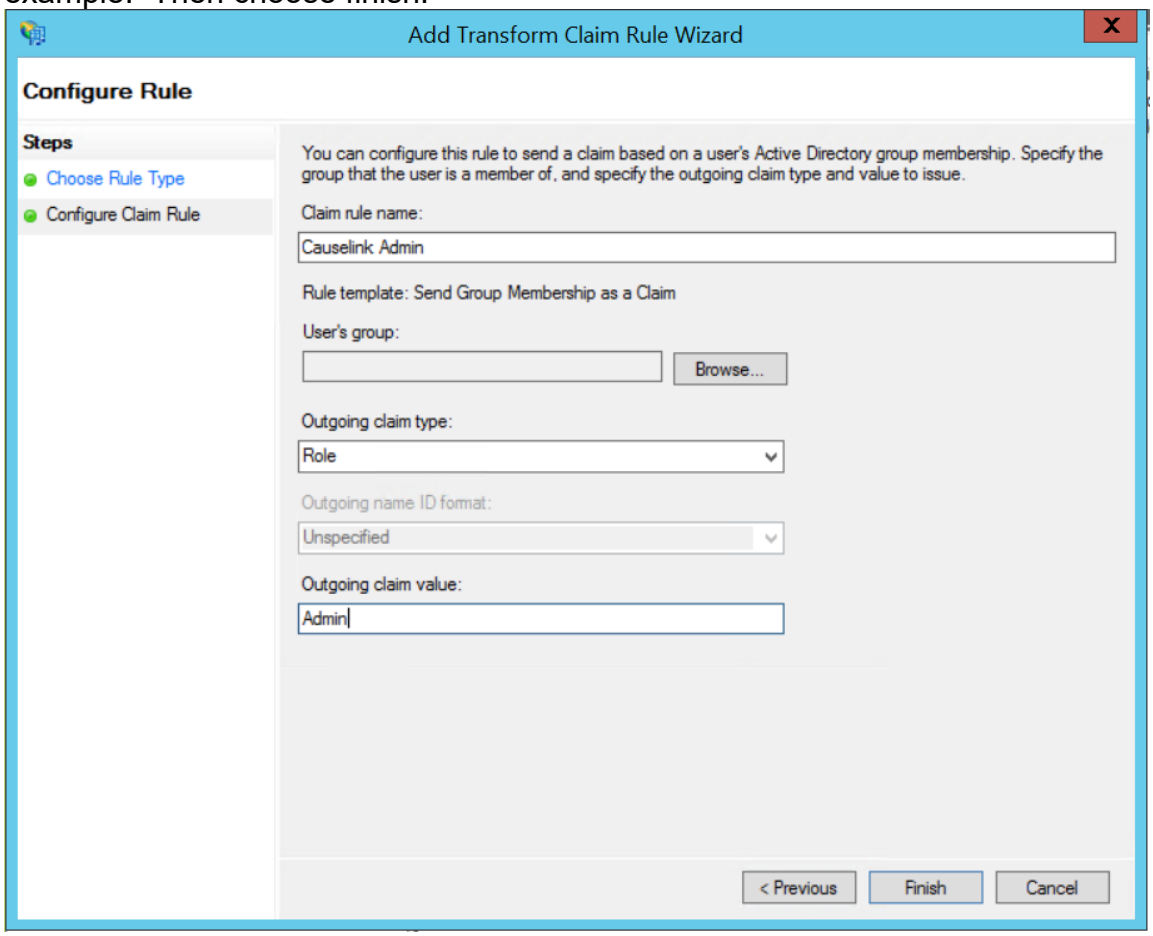
Causelink can be configured to only allow users meeting certain criteria into the system. Your claim can be whatever you like, and ADFS allows for claim chaining meaning you can combine many claims into a single outbound value.

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’.



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.



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.