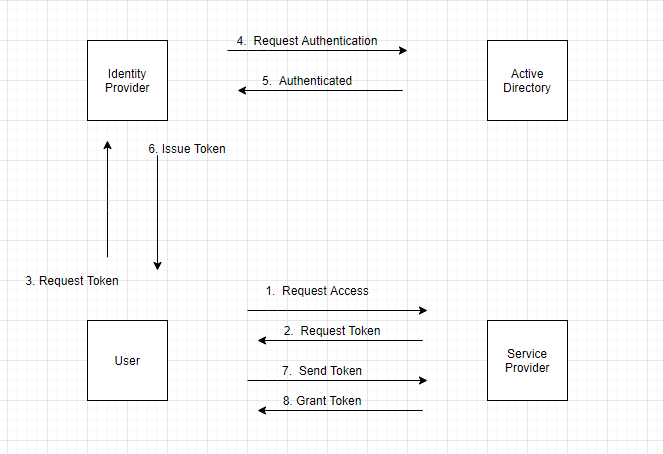
**Step by step: Configure SAML 2.0 with ADFS**

**How does SAML work? Below is the authentication flow**

1. The user navigates to a service, for example, a partner-company website (http://example.com) to obtain pricing or product details.
2. The website requests an authentication token.
3. User requests token from the ADFS server.
4. ADFS server issues token containing user’s set of claims.\
5. User forwards token to the partner-company website.
6. The website grants authorization access to the user.

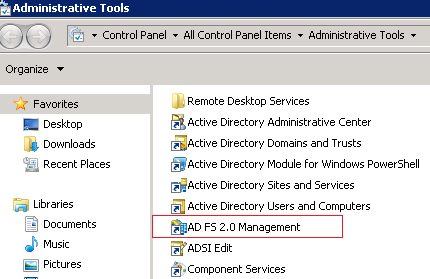


**Requirements:**

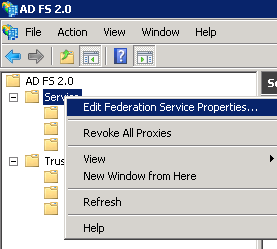
1. A fully installed and configured ADFS service.
2. A Server running 20080 R2 and above
3. An SSL certificate to sign your ADFS login page and the thumbprint of that certificate

**Steps:**

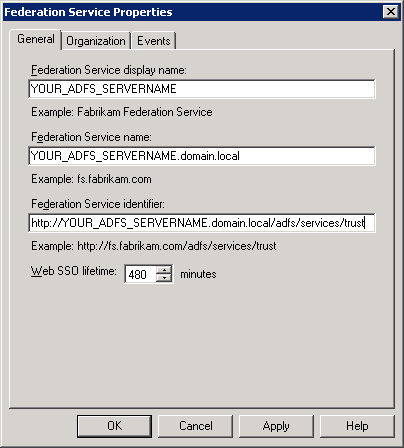
1. Login in to your AD FS server and launch the ADFS Management Console via the shortcut in Control Panel\Administrative Tools.

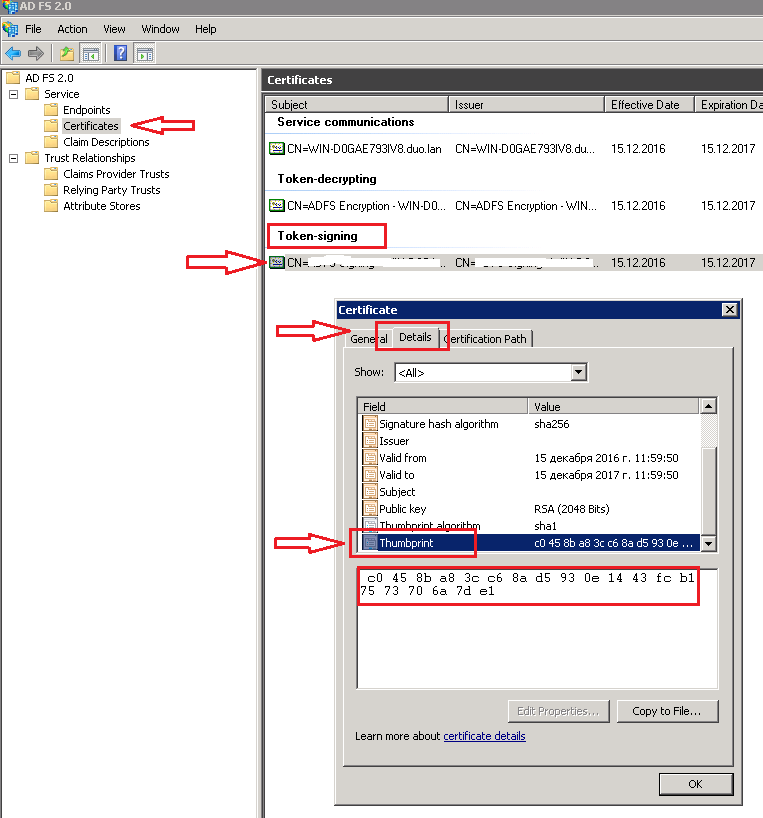


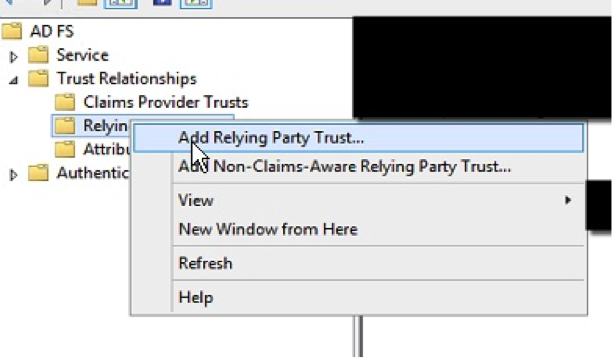
1. Check AD FS settings - Right-click on Service and sel ect Edit Federation Service Properties.



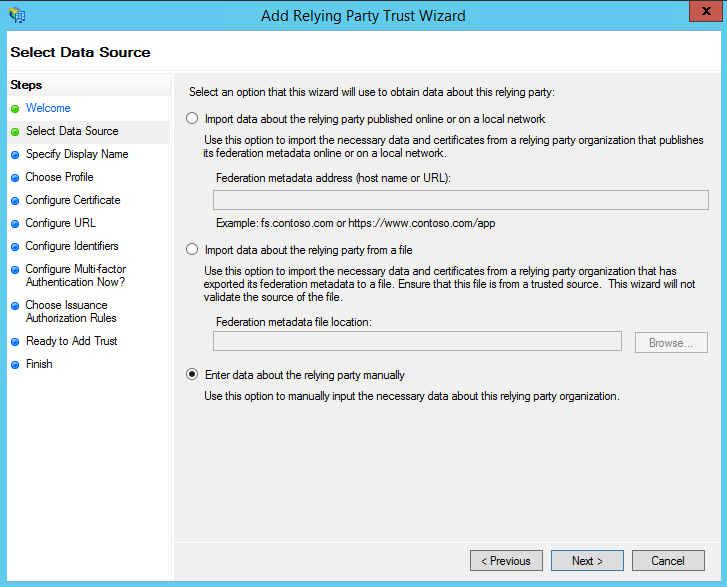
1. Confirm that the General settings match your DNS entries and certificate names. Take notes of settings



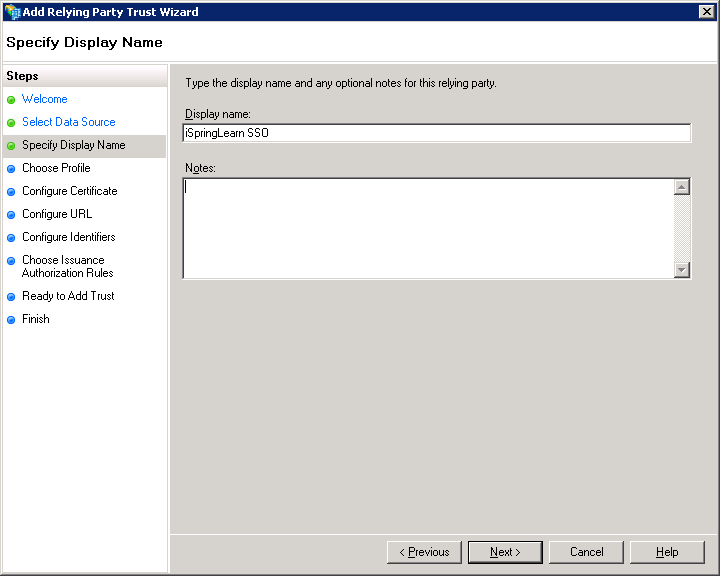
1. Browse to the certificates. Right-click on the certificate and select View Certificate. Go to the Details tab. Find the Thumbprint field and copy the contents of this field to the Windows clipboard and paste it to a notepad text file
2. Go to the ADFS Management console and select Relying Party Trusts, right-click on it and select Add Relying Party Trust.



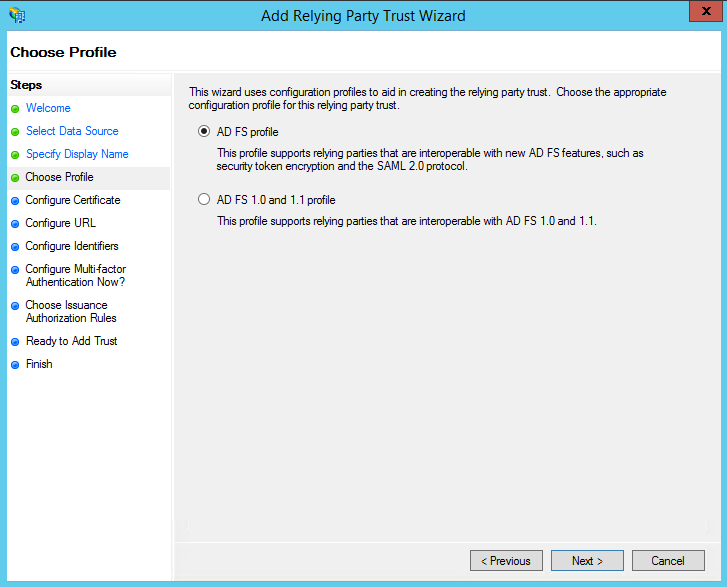
1. Select Next On the Welcome Screen of the wizard, and on the Select Data Source step, select the last option: Enter data about the relying party manually.



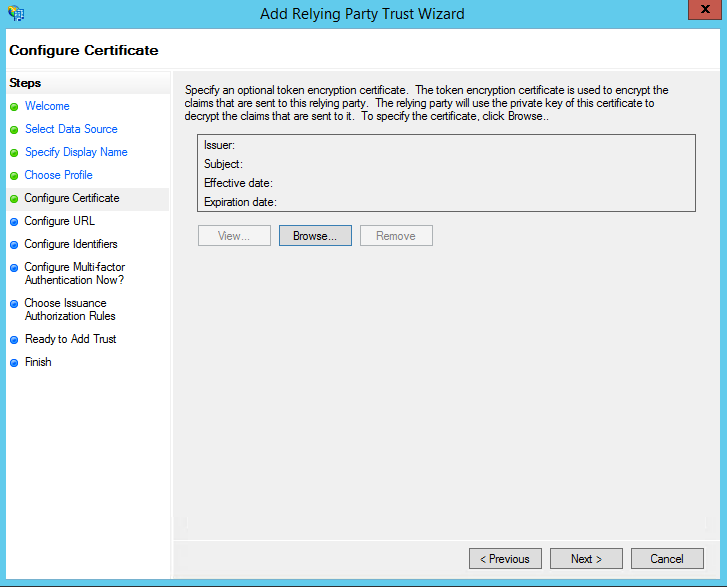
1. On the next screen, enter a Display name that you will recognize in the future.



1. Next, select AD FS profile:

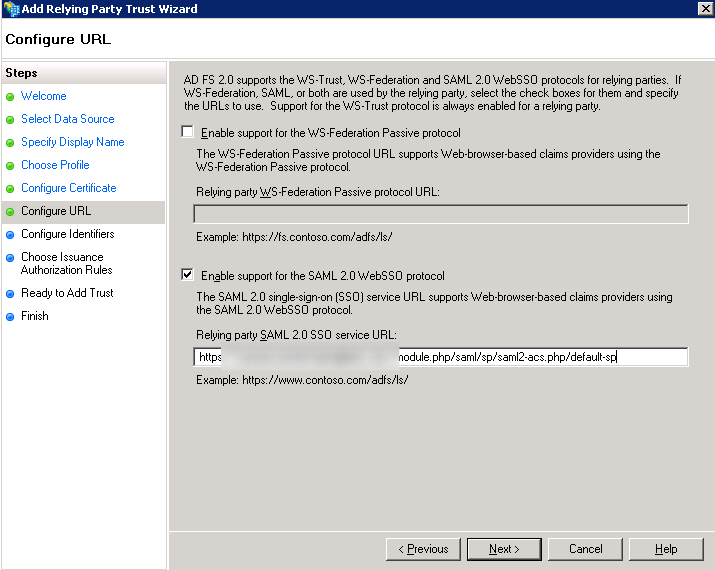


1. Leave the default values:

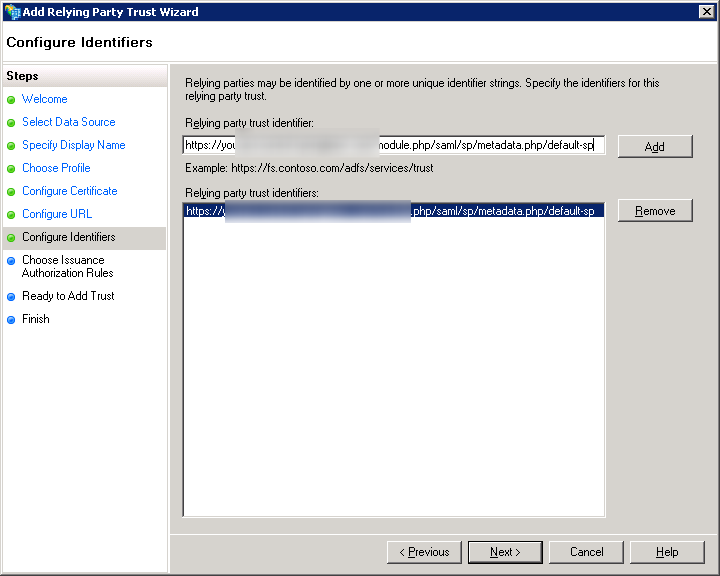


1. On the next screen, check the box labeled: Enable support for the SAML 2.0 WebSSO protocol. The service URL will be:

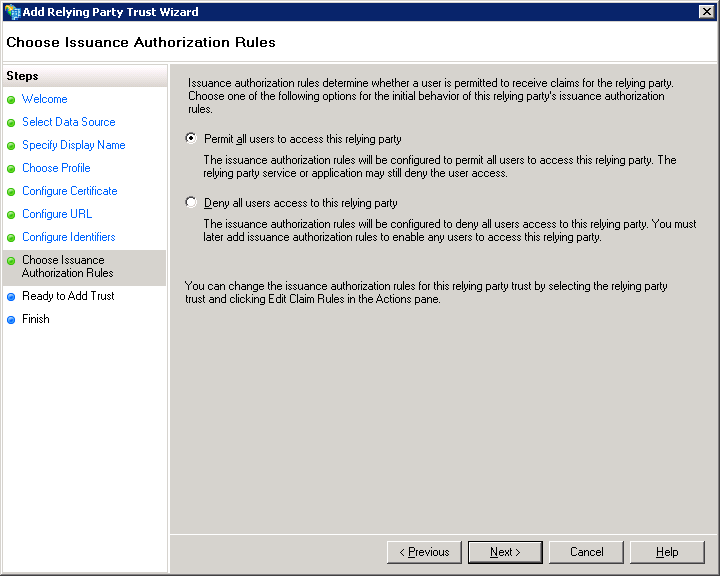
https:/domain.com/module.php/saml/sp/saml2-acs.php/default-sp



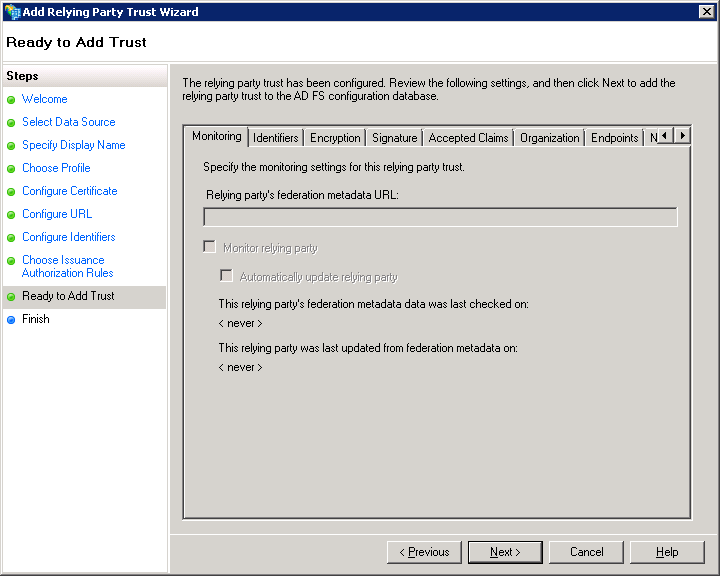
1. Click Next. Add Relying party trust identifier: [https:/domain.com/module.php/saml/sp/metadata.php/default-sp](about:blank)



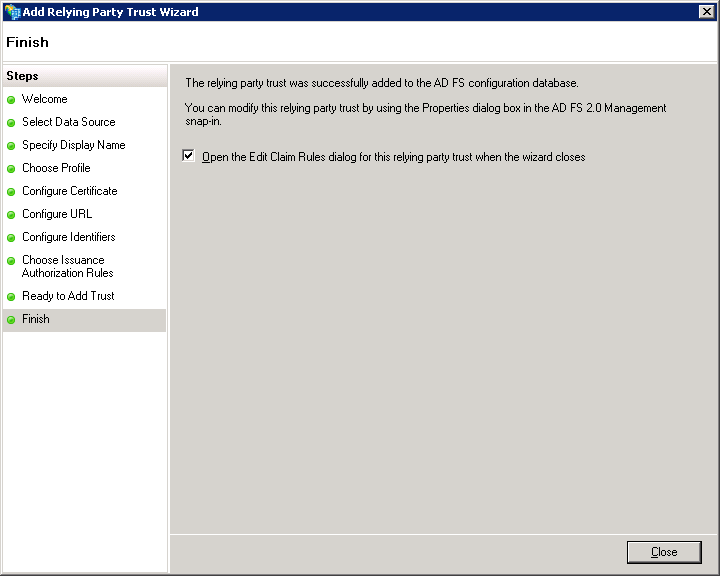
1. Choose Permit all users to access this relying party.



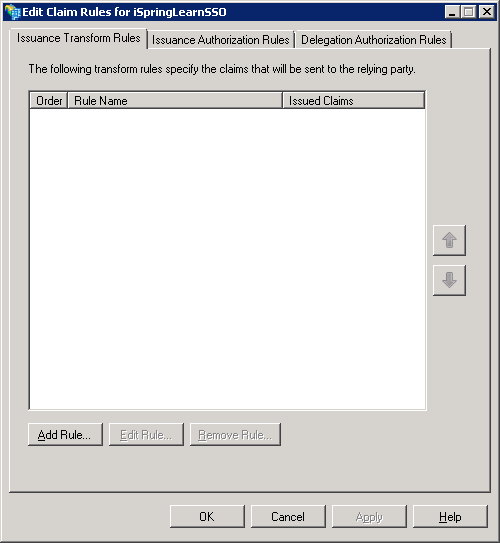
1. On the next step, just click Next.



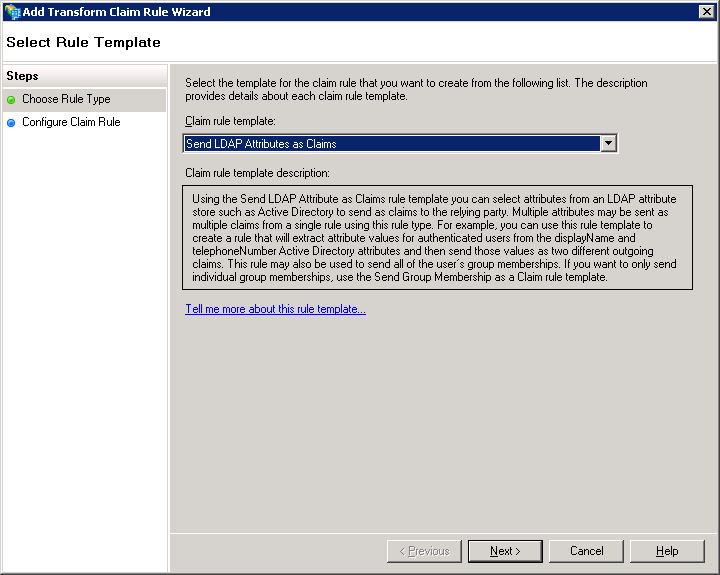
1. On the final screen, check the box Open the Edit Claim Rules dialog and use the Close button to exit.



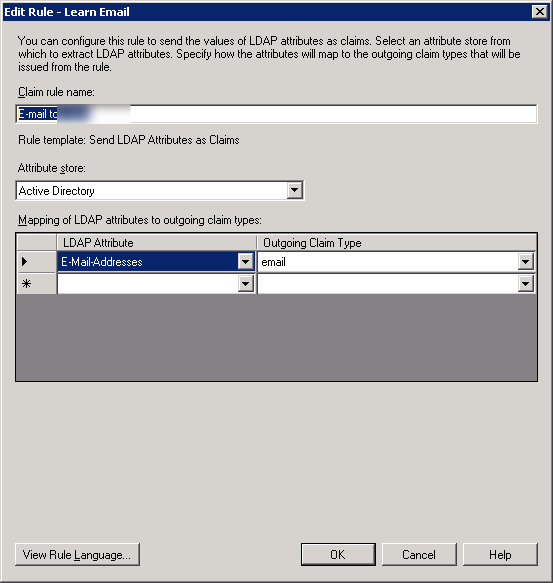
1. Creating Claims Rules - Add the first rule



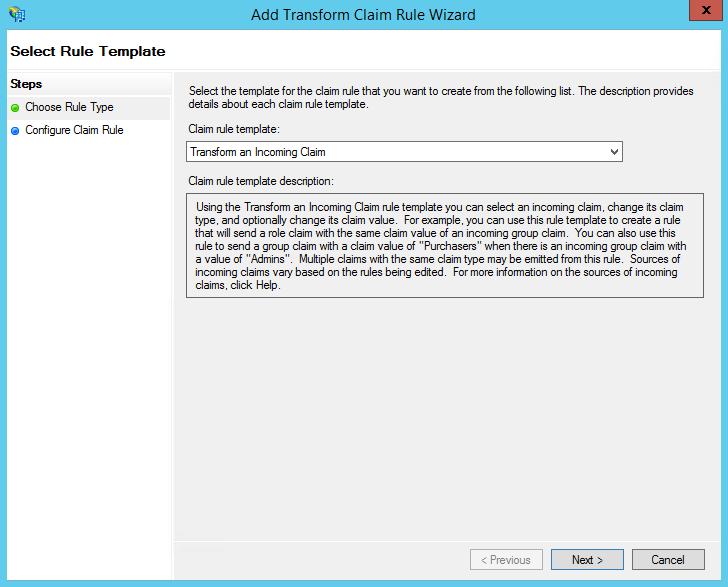
1. Select Send LDAP Attributes as Claims



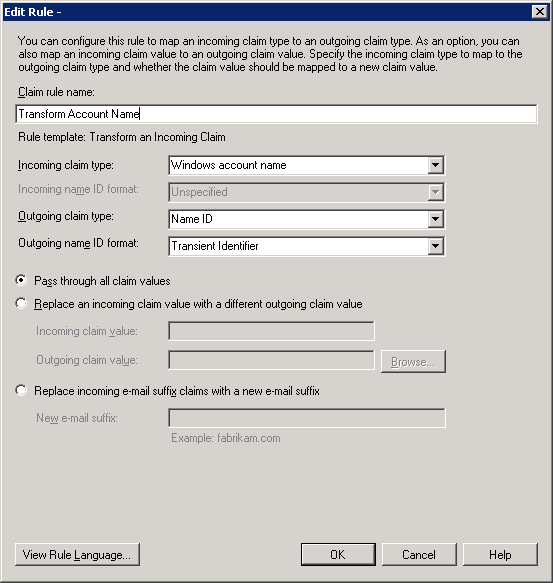
1. On the next screen, specify your Claim Rule, for Example E-mail to xxx, using Active Directory as your attribute store, and do the following
2. From the LDAP Attribute column, select E-Mail Addresses
3. From the Outgoing Claim Type, enter “email”
4. Click on Finish or OK to save the new rule



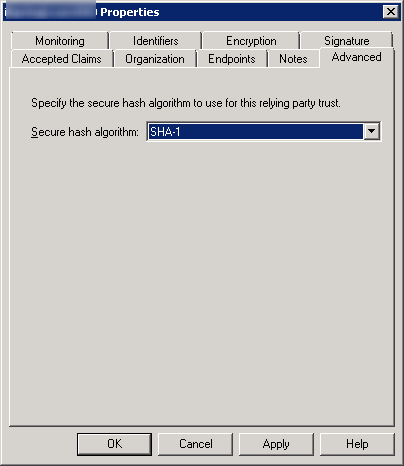
1. After that, add the second rule and select Transform an Incoming Claim as the template



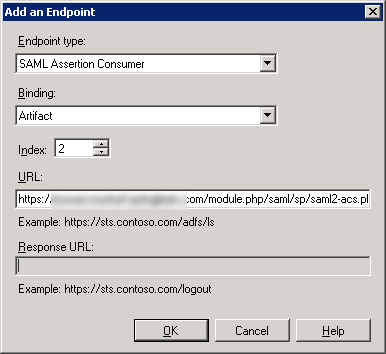
1. Configure Flame rule Properties
2. Give your Claim Rule a title, for example, Transform Account Name
3. Select Windows account name as the Incoming Claim Type
4. Under Outgoing Claim Type, select Name ID
5. Under Outgoing Name ID Format, select Transient Identifier
6. Leave the default rule Pass through all claim values



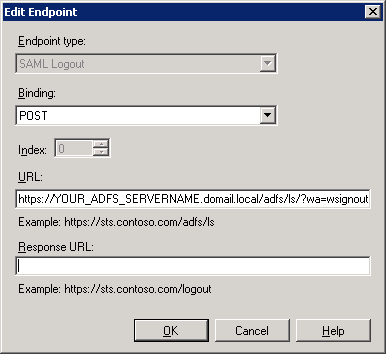
1. Click on OK to create the claim rule, and then OK again to finish creating rules.
2. Adjusting the Trust Settings - Some settings on your Relying Party Trust will need to be adjusted. To access these settings, select Properties from the Actions sidebar on the right while you have the Relying Party Trust selected.
3. Under the Advanced tab, make sure that the selection is SHA-1



1. Under the Endpoints tab, click ADD to add a new endpoint
2. For the Endpoint type, select SAML Assertion Consumer
3. For the Binding, choose Artifact with Index 2
4. The URL field should look like this: https://domain.com/module.php/saml/sp/saml2-acs.php/default-sp
5. Leave the Response URL blank and click on OK



1. Click ADD one more time
2. For the Endpoint type, select SAML Logout
3. For the Binding, choose POST
4. The URL field should look like this: https://YОUR\_ADFS\_SERVERNAME.domail.local/adfs/ls/?wa=wsignout1.0
5. Leave the Response URL blank and click on OK



1. Go to your SSO login page: https://domain.com/sso/login and enter your credentials.