Configure SAML 2.0 for Shufflrr using ADFS

A SAML 2.0 identity provider (IDP) can take many forms, one of which is a self-hosted Active Directory Federation Services (ADFS) server. ADFS is a service provided by Microsoft as a standard role for Windows Server that provides a web login using existing Active Directory credentials.

NOTE: This document is for guidance purposes only. Every enterprise has different policies and business rules and some things may not apply to everyone.

Requirements

To use ADFS to log in to your Shufflrr instance, you need the following components:

- An Active Directory instance where all users have an email address attribute.
- An Admin Shufflrr account for your Site to be able to make configuration changes.
- A server running Microsoft Server 2012 or 2008. This guide uses screenshots from Server 2012R2, but similar steps should be possible on other versions.
- An SSL certificate to sign your ADFS login page and the fingerprint for that certificate.

NOTE: After you meet these basic requirements, you need to install ADFS on your server. Configuring and installing ADFS is beyond the scope of this guide, but it's detailed in this Microsoft KB article.

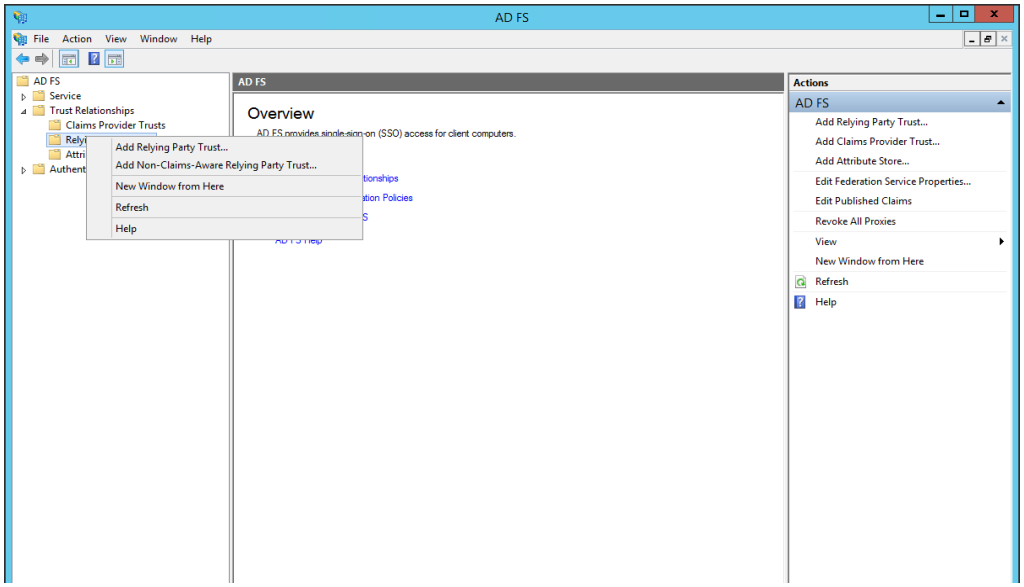
When you have a fully installed ADFS installation, note down the value for the 'SAML 2.0/W-Federation' URL in the ADFS Endpoints section. If you chose the defaults for the installation, this will be '**/adfs/ls/**'.

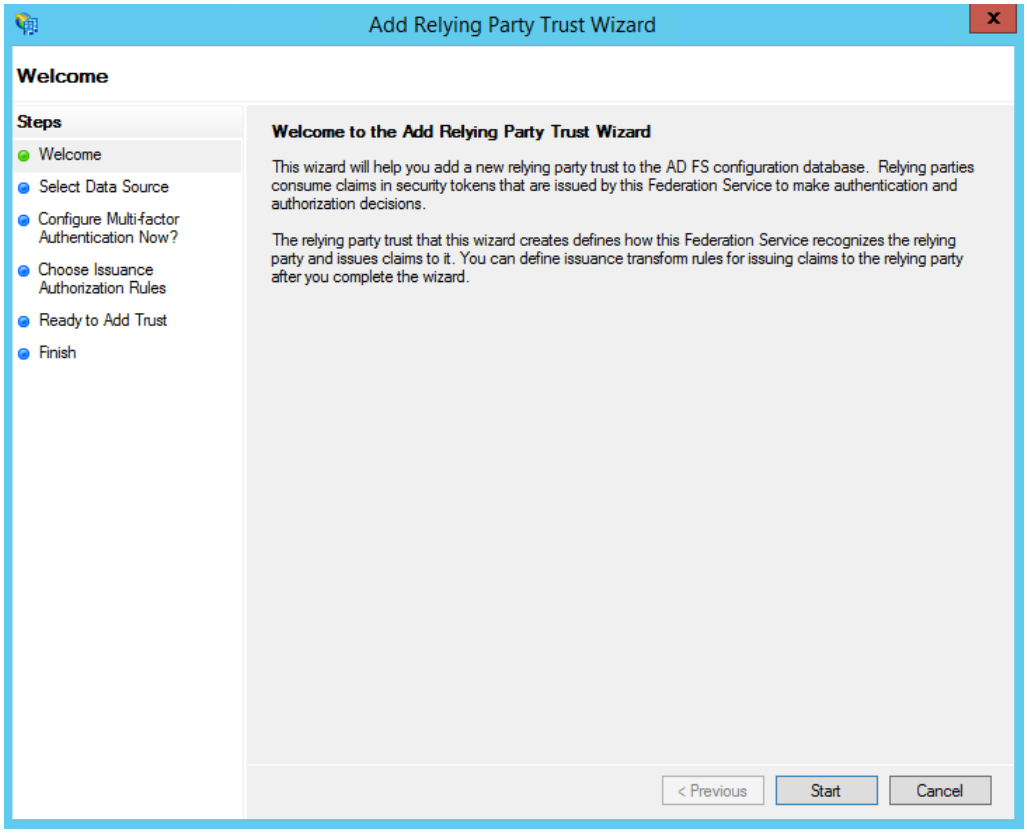
Also, for this document, we will use the service provider id **https://ADFS.Shufflrr.local** to test. In your case, it will be **https://YourShufflrrSiteName.Shufflrr.com**

Step 1 - Adding a Relying Party Trust

At this point you should be ready to set up the ADFS connection with your Shufflrr instance. The connection between ADFS and Shufflrr is defined using a Relying Party Trust (RPT).

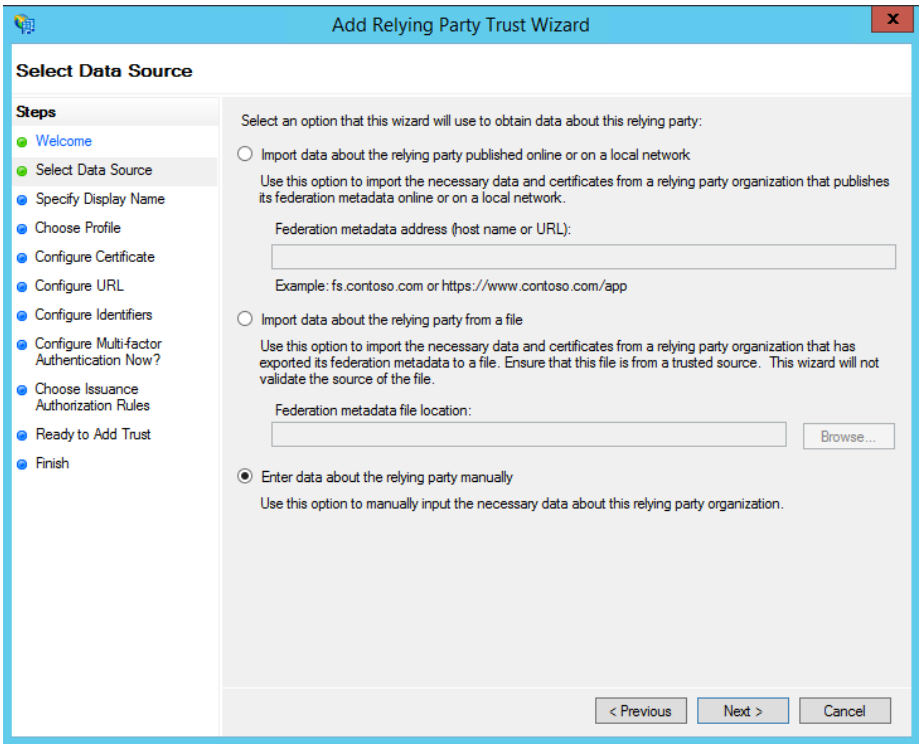
Select the **Relying Party Trusts** folder from **AD FS Management**, and add a new **Standard Relying Party Trust** from the **Actions** sidebar. This starts the configuration wizard for a new trust.



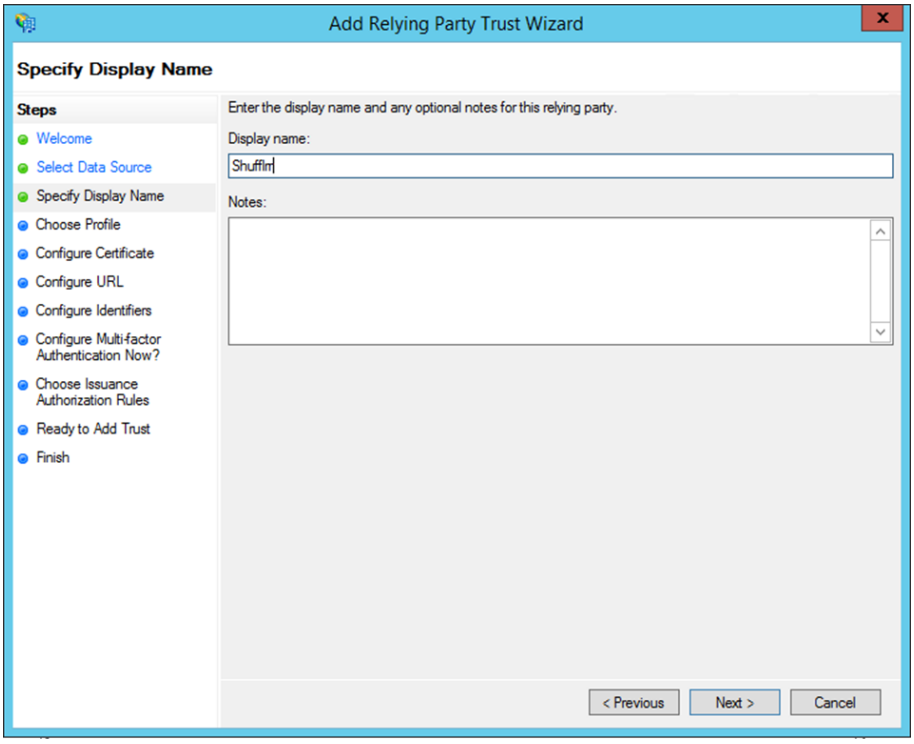


1. In the **Select Data Source** screen, select the last option, **Enter Data About the Party Manually** and hit **Next**

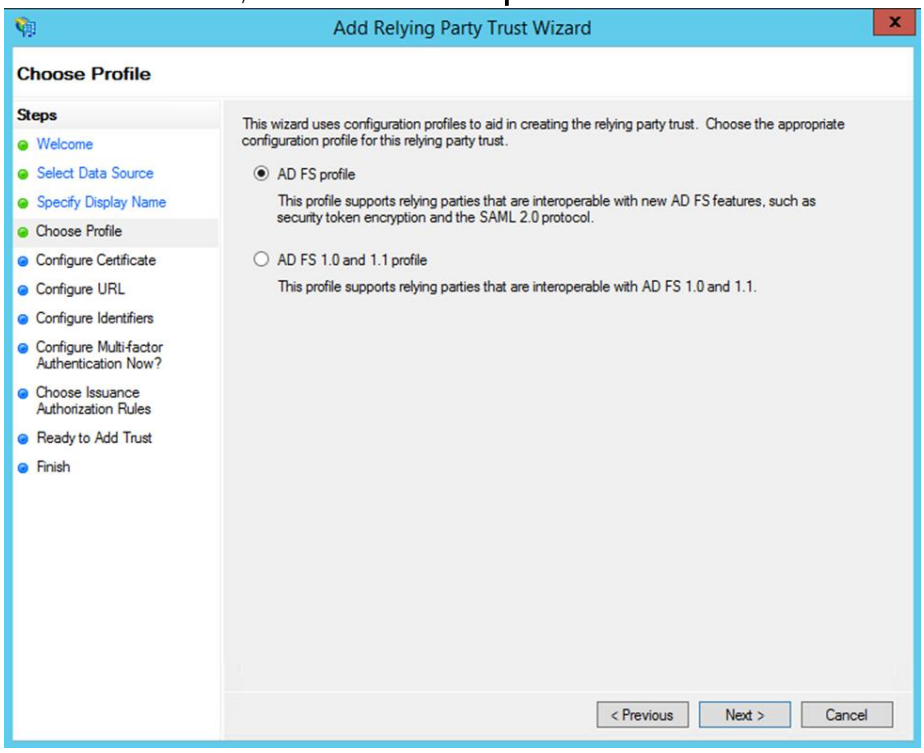
   NOTE: In this guide, we chose to enter data manually, but your Enterprise might be importing from a file or from the Federation metadata xml.



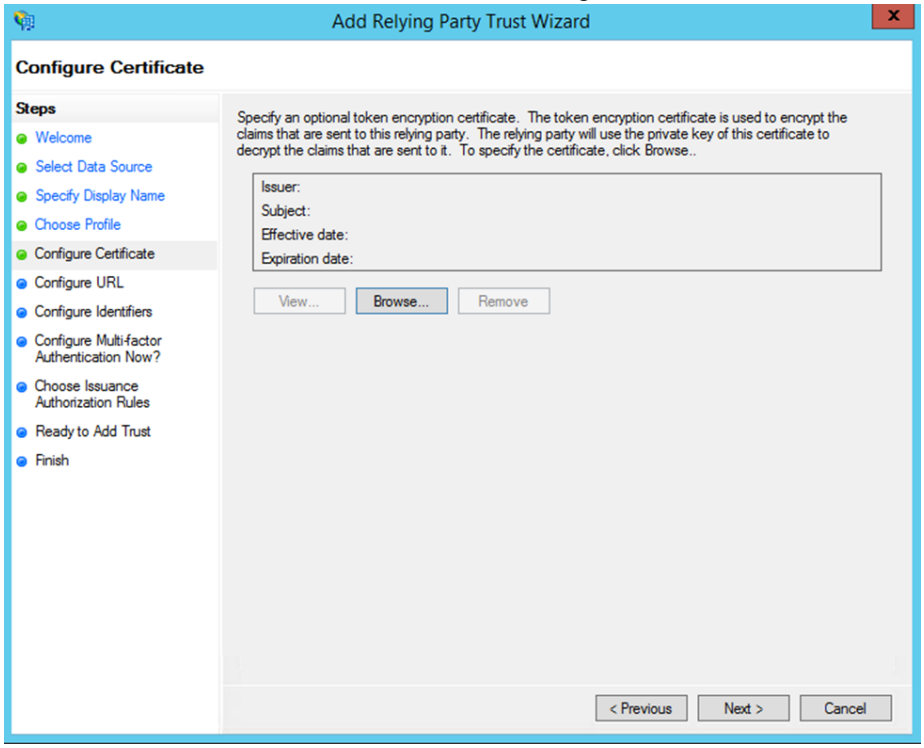
2. On the next screen, enter a **Display name** that you'll recognize in the future, and any notes you want to make.



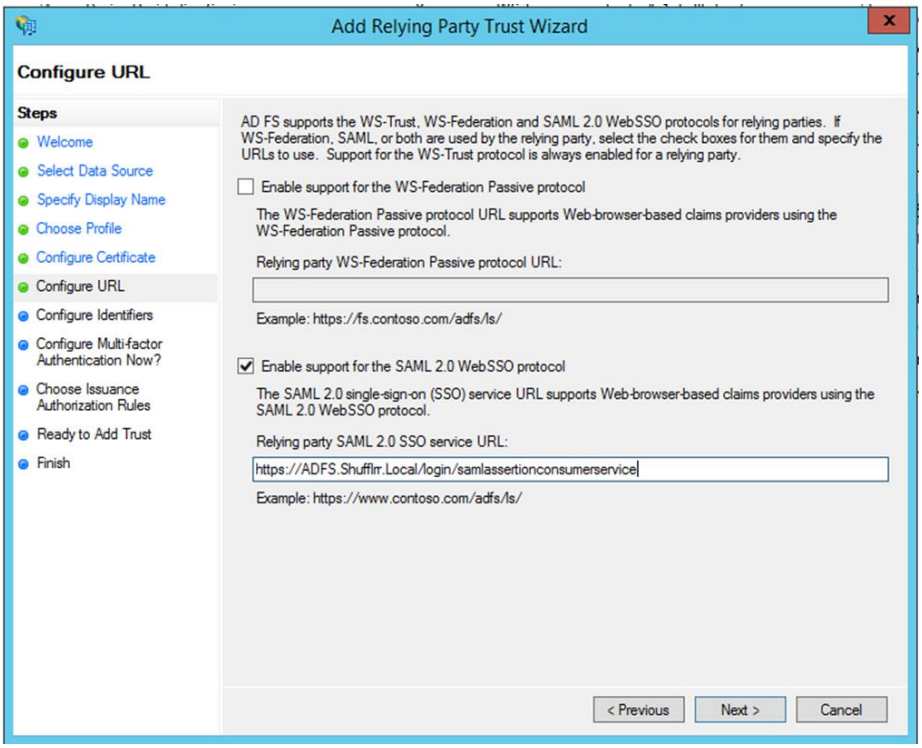
3. On the next screen, select the **ADFS FS profile** radio button.



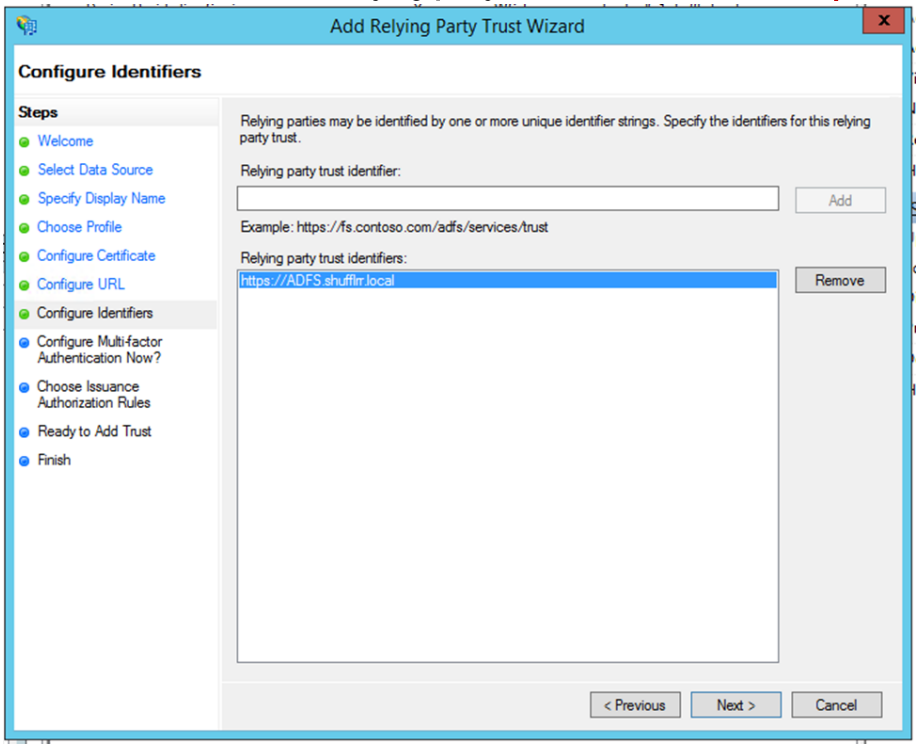
4. On the next screen, leave the certificate settings at their defaults.



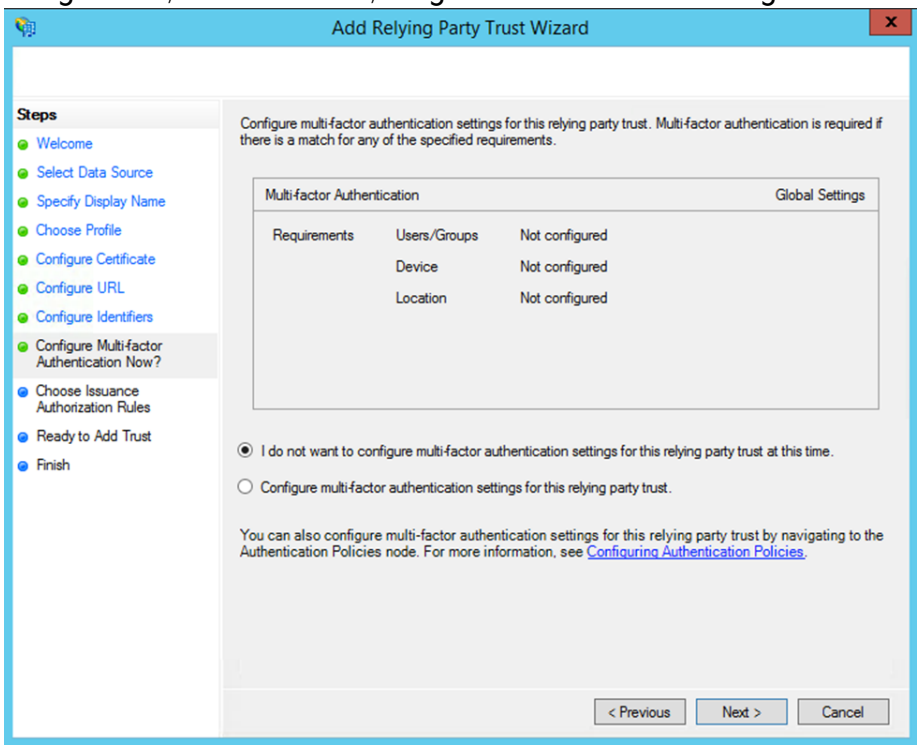
5. On the next screen, check the box labeled **Enable Support for the SAML 2.0 WebSSO protocol**. The service URL will be https://ADFS.Shufflrr.Local/login/samlassertionconsumerservice.
Note that there's no trailing slash at the end of the URL.



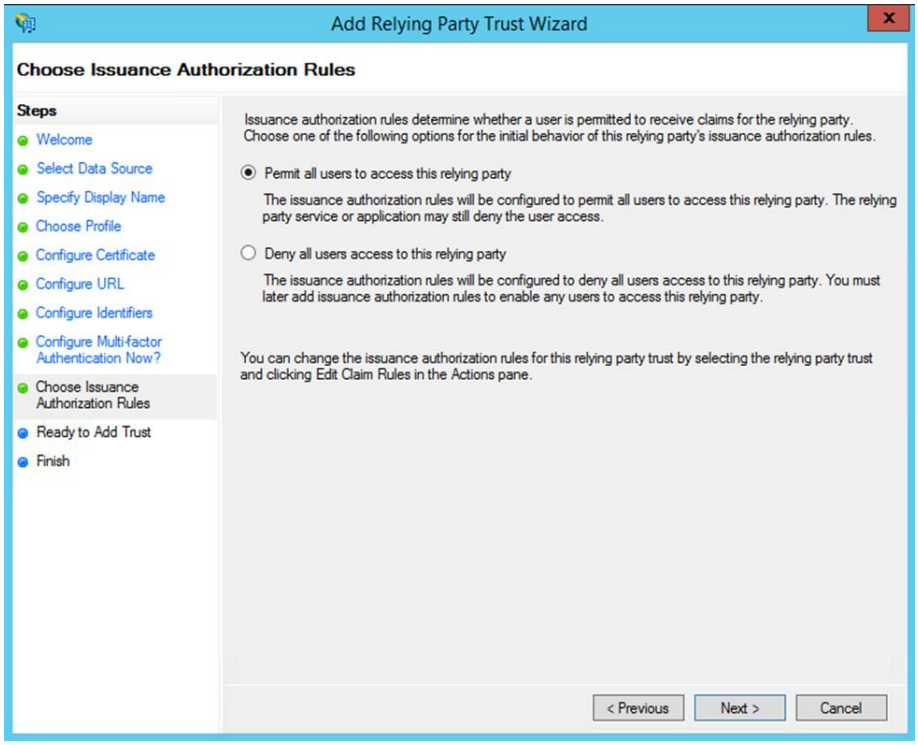
6. On the next screen, add a **Relying party trust identifier** as such https://ADFS.shufflrr.local



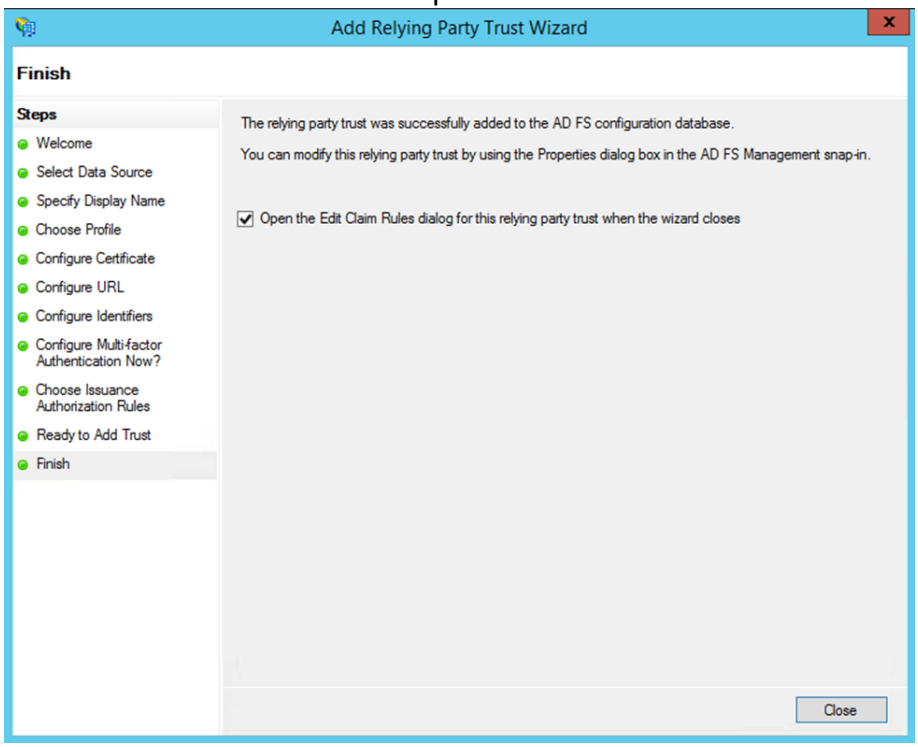
7. On the next screen, you may configure multi-factor authentication, but this is beyond the scope of this guide so, in this instance, we go ahead and DON'T configure it. Hit **Next**.



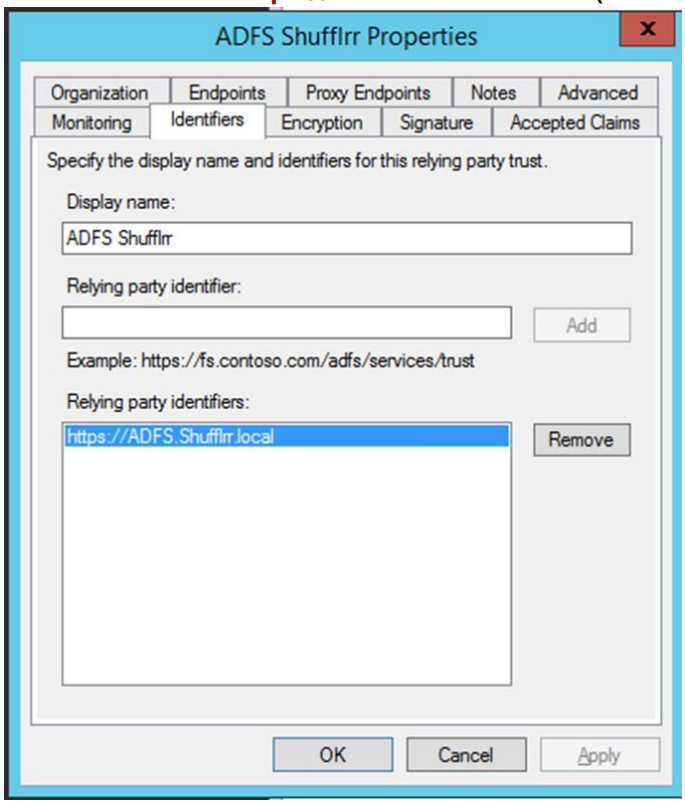
8. On the next screen, select the **Permit all users to access this relying party** radio button.



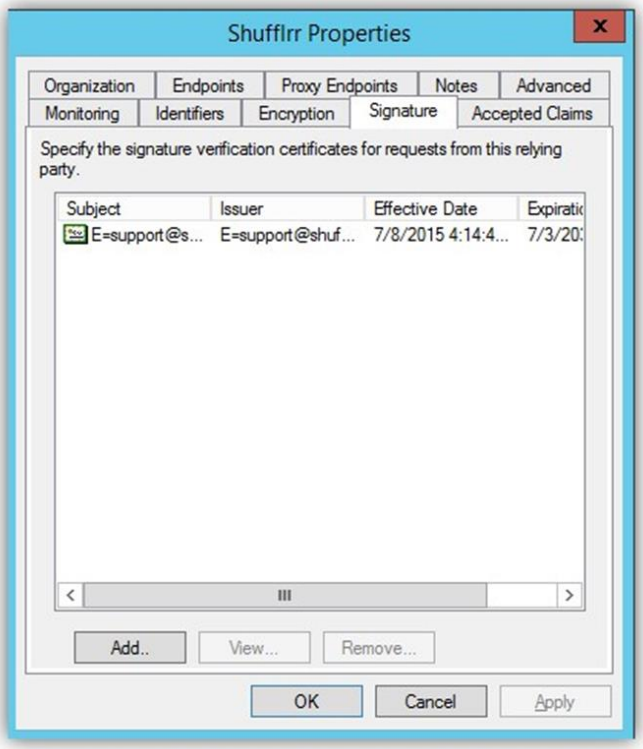
9. On the next two screens, the wizard will display an overview of your settings. On the final screen use the **Close** button to exit and open the **Claim Rules** editor.



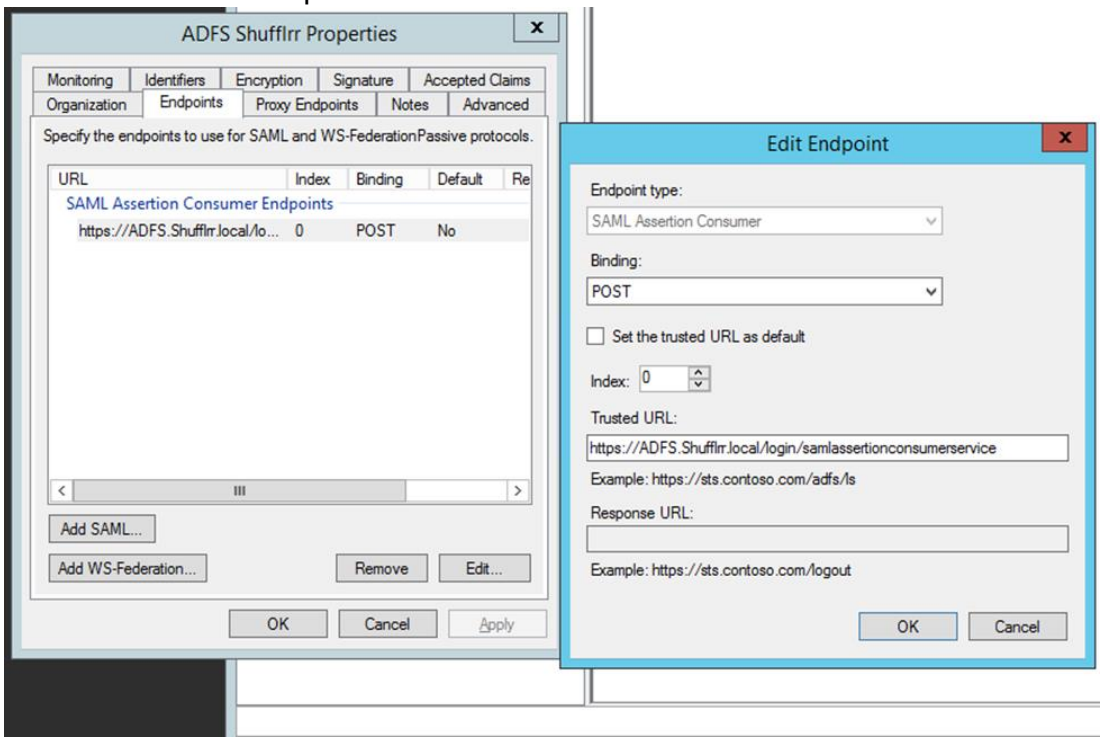
10. DoubleClick on the newly created RPT to view its properties. Once open, on the Identifiers tab, Add the identifier **https://ADFS.Shufflrr.local** (Service Provider ID).



11. On the signature tab, add the signature certificate from the Shufflrr admin portal. "**Service Provider Certificate**".



12. On the Endpoints tab, Create a SAML Assertion Endpoint with the "Service Provider ACS URL" from the Shufflrr admin portal.

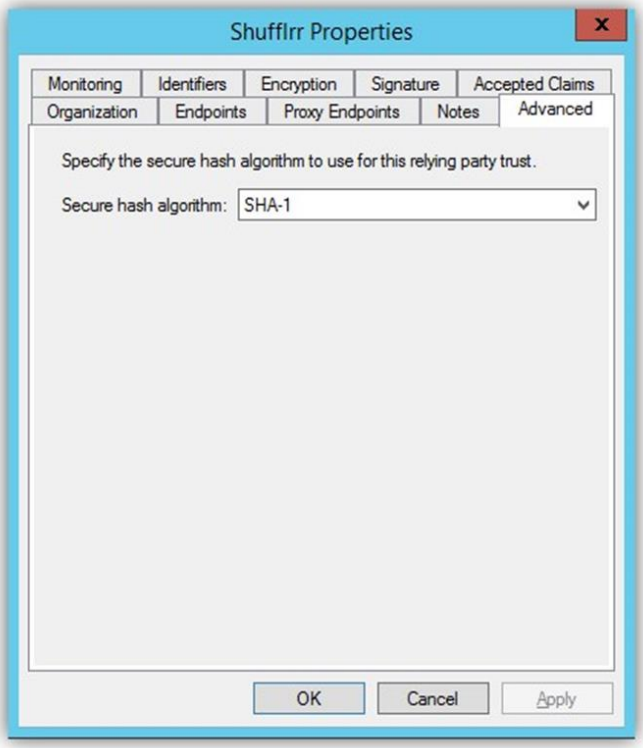


13. On the Advanced tab, Configure the hash algorithm for SHA-1 (Current Shufflrr signature cert is SHA-1) and then Configure the Relying Party trust so that both the Assertion and the Response are signed:

    Open PowerShell as an admin and run the command below. This action will add the signature to SAML messages, making verification successful.

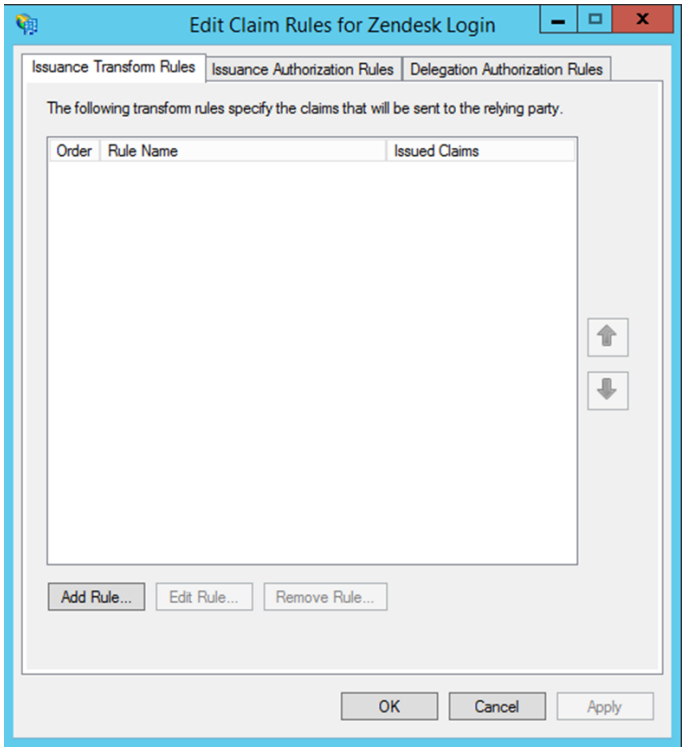
    Note: Your TargetName is the Display name for your Identifier and in this case 'ADFS Shufflrr'.

```
Add-PSSnapin Microsoft.Adfs.PowerShell Set-AdfsRelyingPartyTrust -TargetName
'ADFS Shufflrr' -SamlResponseSignature MessageAndAssertion
```

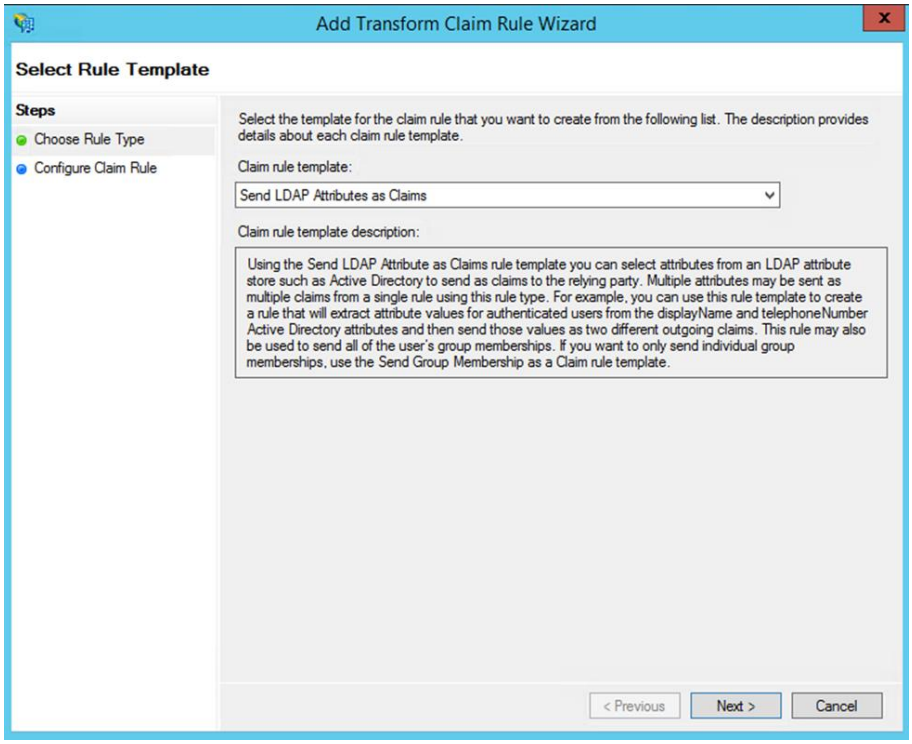


Step 2 - Creating claim rules

Once the relying party trust has been created, you can create the claim rules and update the RPT with minor changes that aren't set by the wizard. By default, the claim rule editor opens once you created the trust.



1. To create a new rule, click on **Add Rule**. Create a **Send LDAP Attributes as Claims** rule.

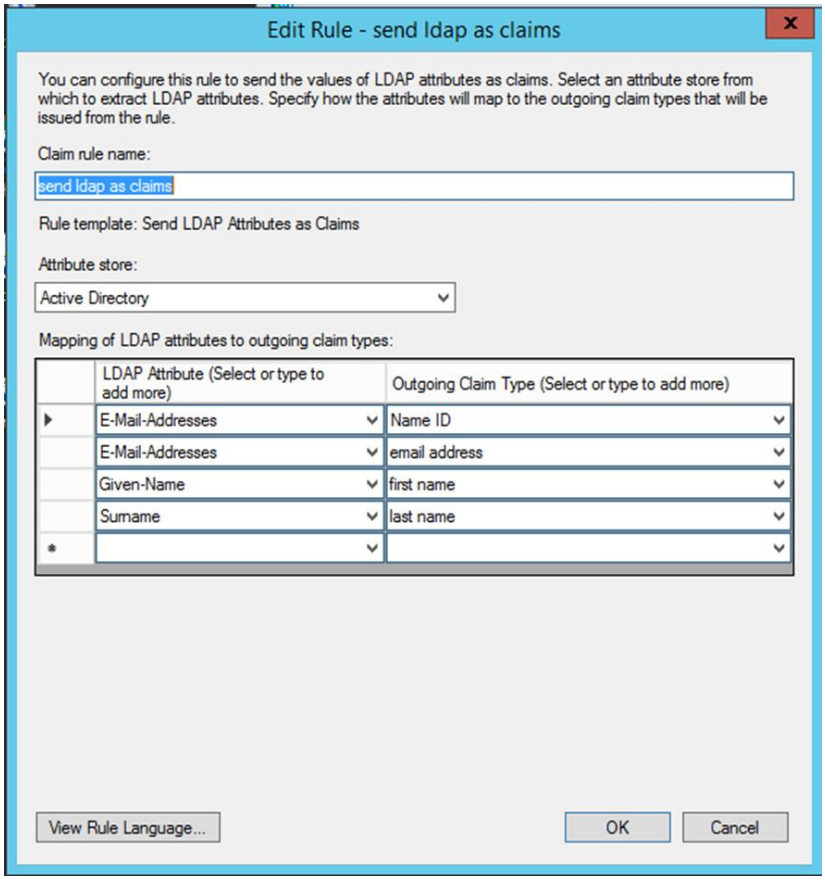


2. On the next screen complete the form as such;
   a. Claim rule name: Send LDAP as Claims
   b. Attribute Directory: Active Directory
   c. Mapping of LDAP attributes to outgoing claim types- Outgoing Claim Type

E-Mail-Addresses	***Name ID***
E-Mail-Addresses	***email Address***
Given-Name	***first name***
Surname	***last name***

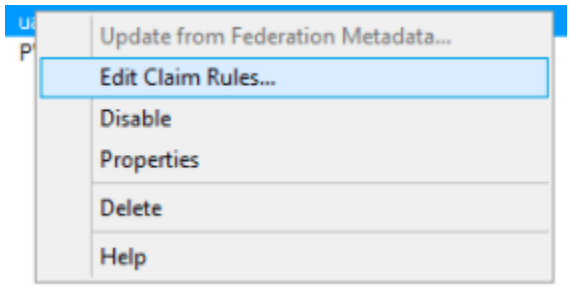
NOTE: Enter all claim Types Using the dropdown, DO NOT TYPE THEM IN!

Click **OK** to save the new rule

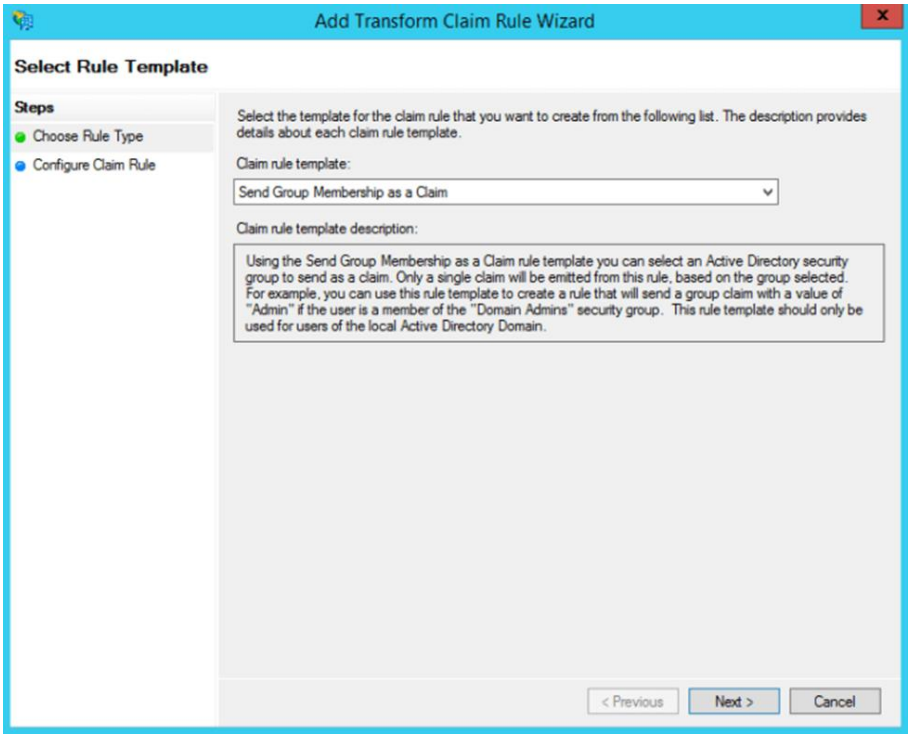


Step 2 - Setting Up Groups in SAML from ADFS

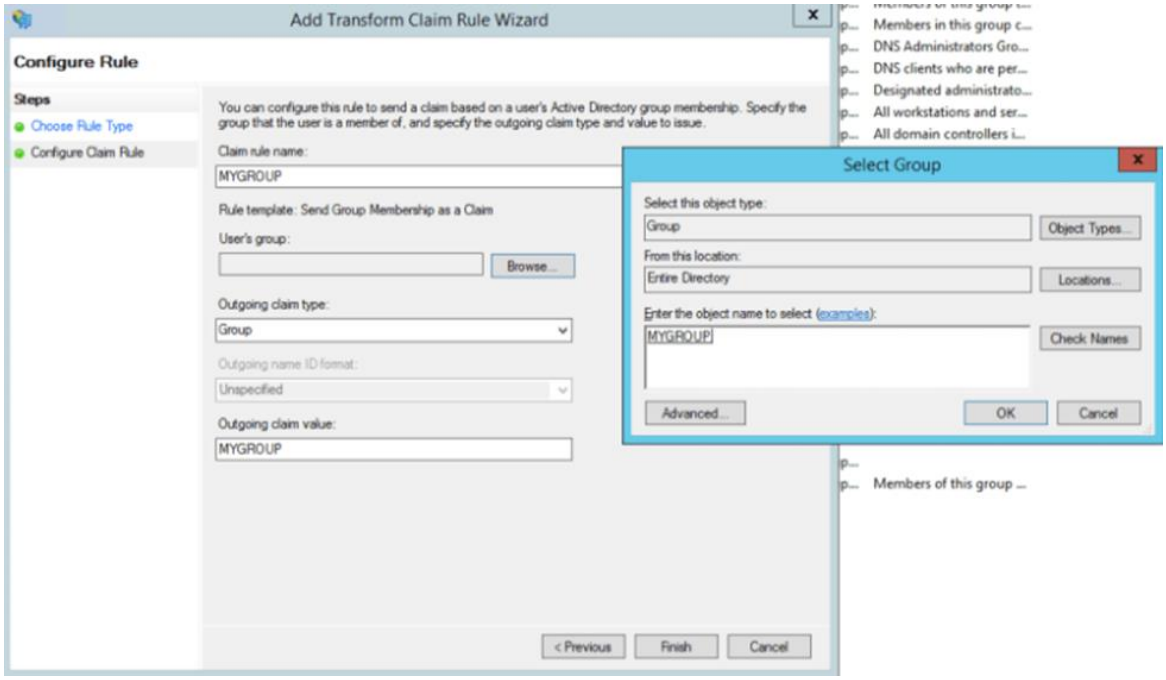
1. **Right-click your Relying Party Trust and select Edit Claim Rules….**



2. Select **Add Rule.**
3. Select **Send Group Membership as a Claim** and click **Next.**

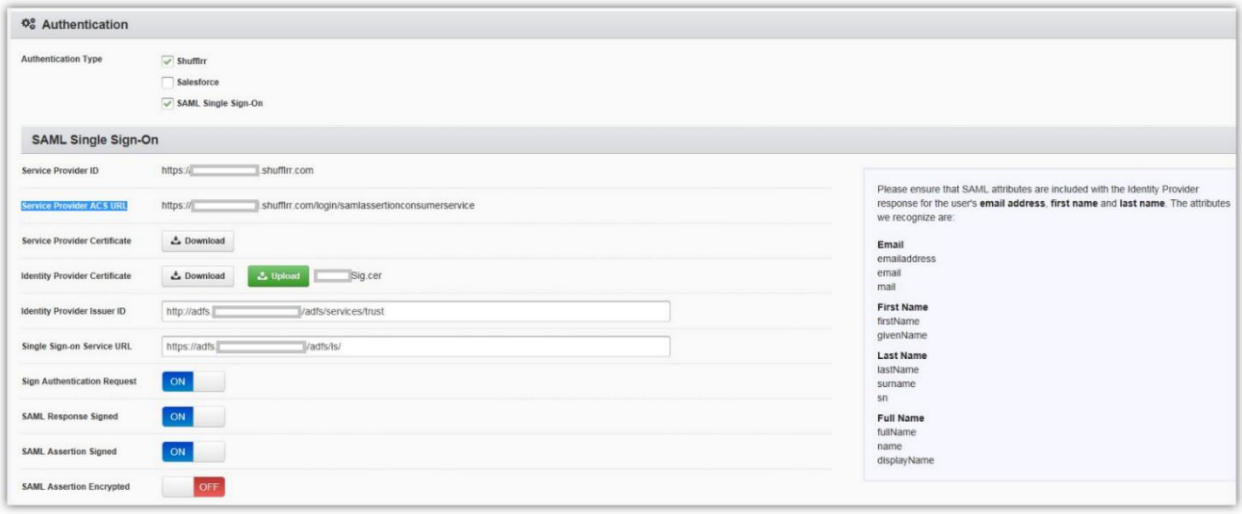


4. Enter the **Claim rule name**.
5. Click **Browse** to select your **User's group**.
6. Select **Group** as your **Outgoing claim type**.
7. Set your **Outgoing claim value** to match your group's name.
8. Click **Finish**.



Step 4 – Testing SSO login

1. When done, the Shufflrr Admin page should look something like this.



2. Logout of Shufflrr and try to log in using the blue Single Sign-On button