

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](#).

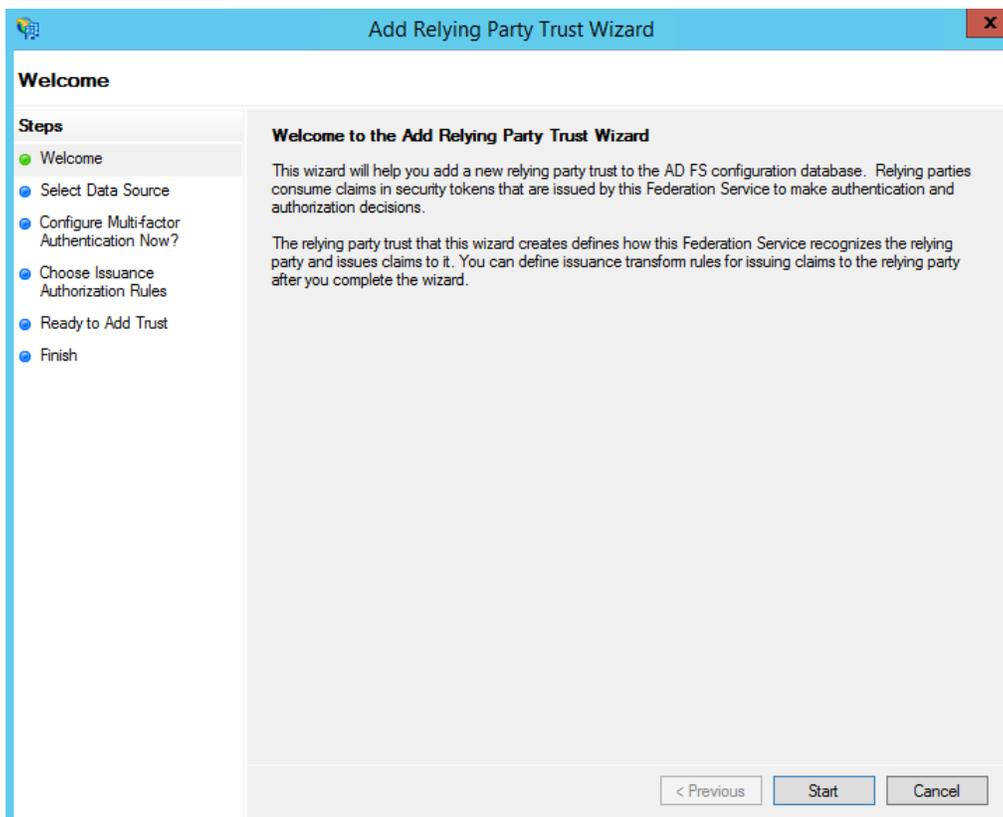
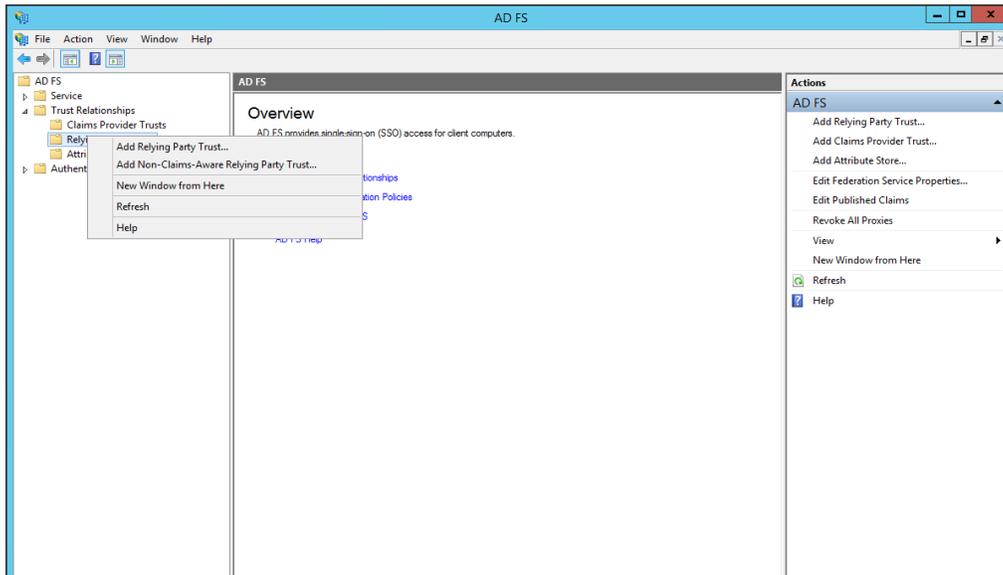
When you have a fully installed ADFS installation, note down the value for the 'SAML 2.0/W-Federation' URL in the ADFS Endpoints section. If you chose the defaults for the installation, this will be `/'adfs/ls/'`.

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

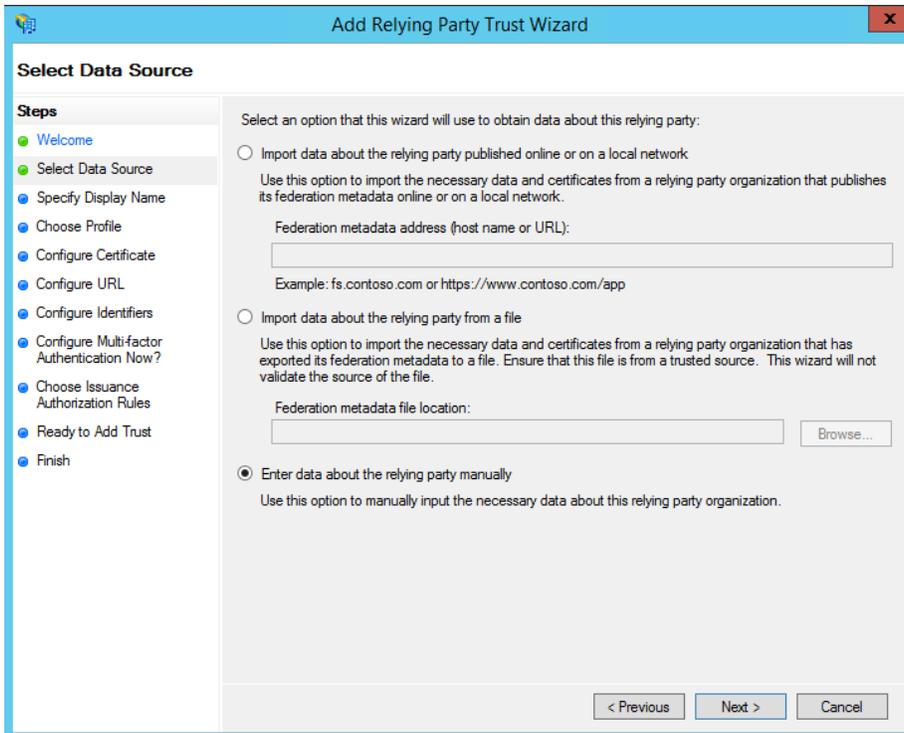
At this point you should be ready to set up the ADFS connection with your Shufflrr instance. The connection between ADFS and Shufflrr is defined using a Relying Party Trust (RPT).

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.



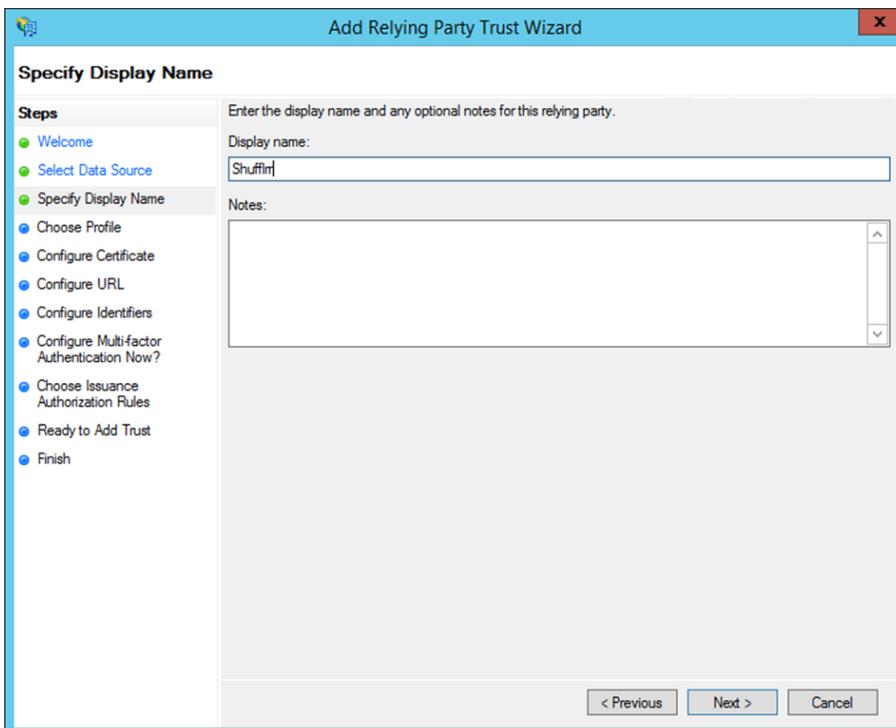
1. In the **Select Data Source** screen, select the last option, **Enter Data About the Party Manually** and hit **Next**

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.



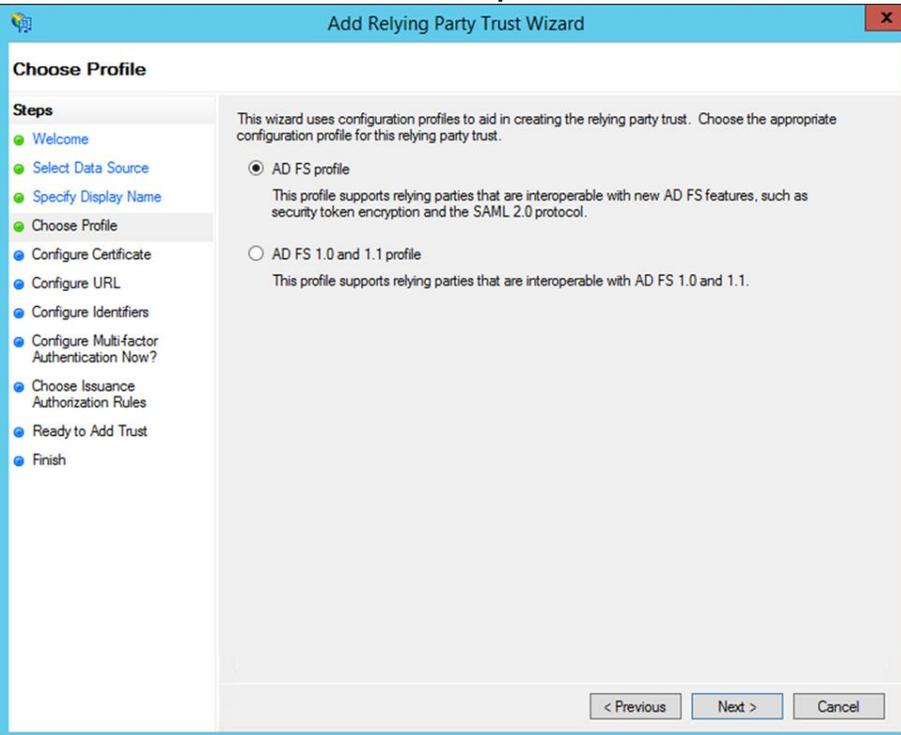
The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Select Data Source' step. The window title is 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: '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' with a description: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' Below this is a text box for 'Federation metadata address (host name or URL):' with an example: 'fs.cortoso.com or https://www.cortoso.com/app'. 2. 'Import data about the relying party from a file' with a description: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' Below this is a text box for 'Federation metadata file location:' and a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected) with a description: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

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

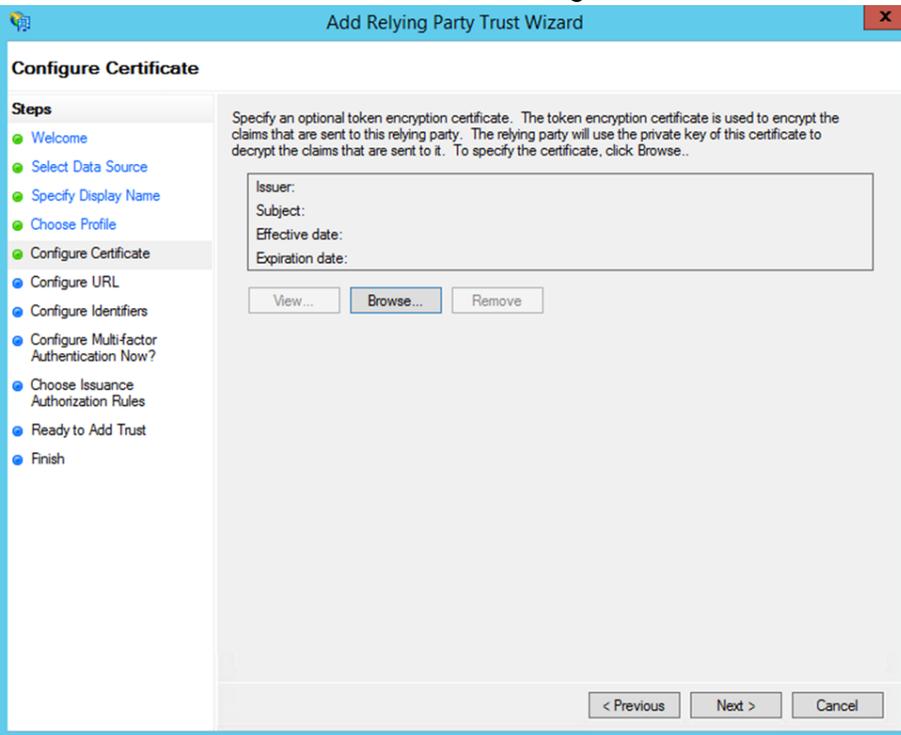


The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The window title is 'Add Relying Party Trust Wizard'. On the left, the 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Profile, Configure Certificate,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

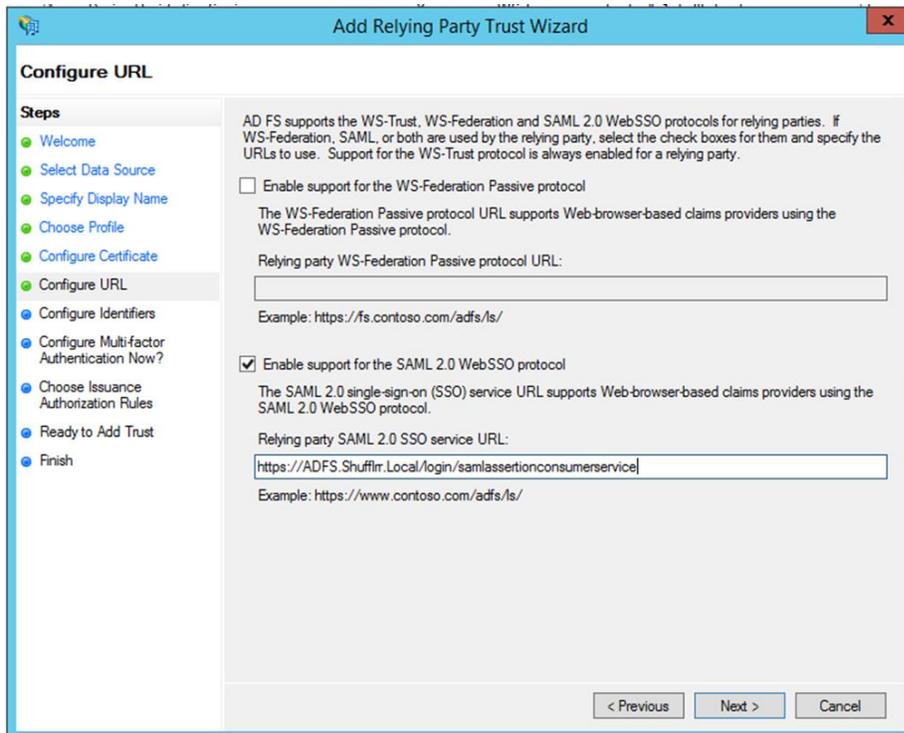
3. On the next screen, select the **ADFS FS profile** radio button.



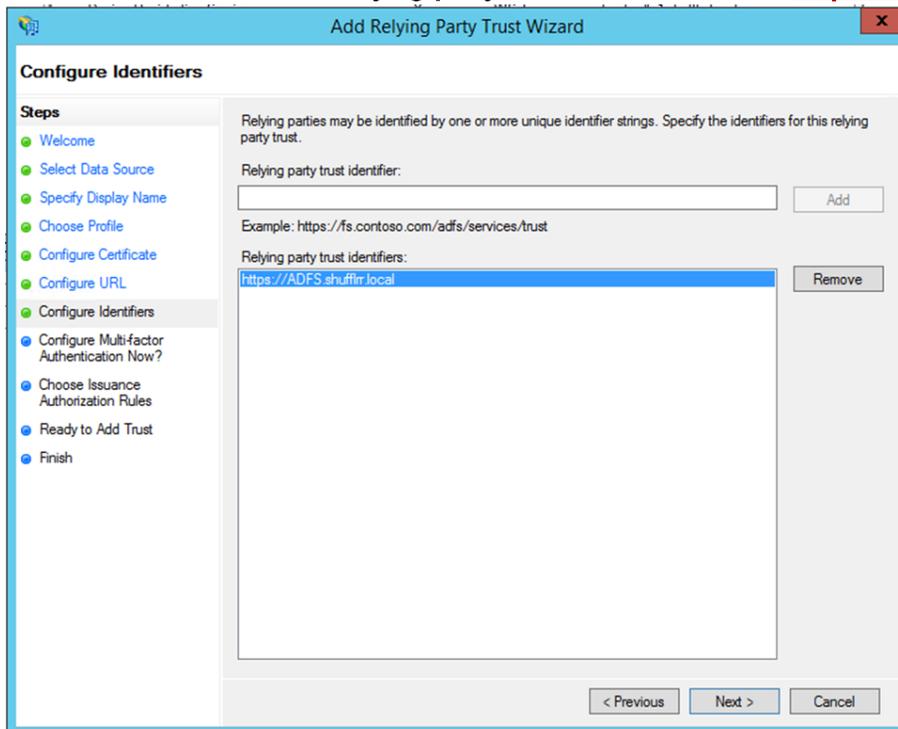
4. On the next screen, leave the certificate settings at their defaults.



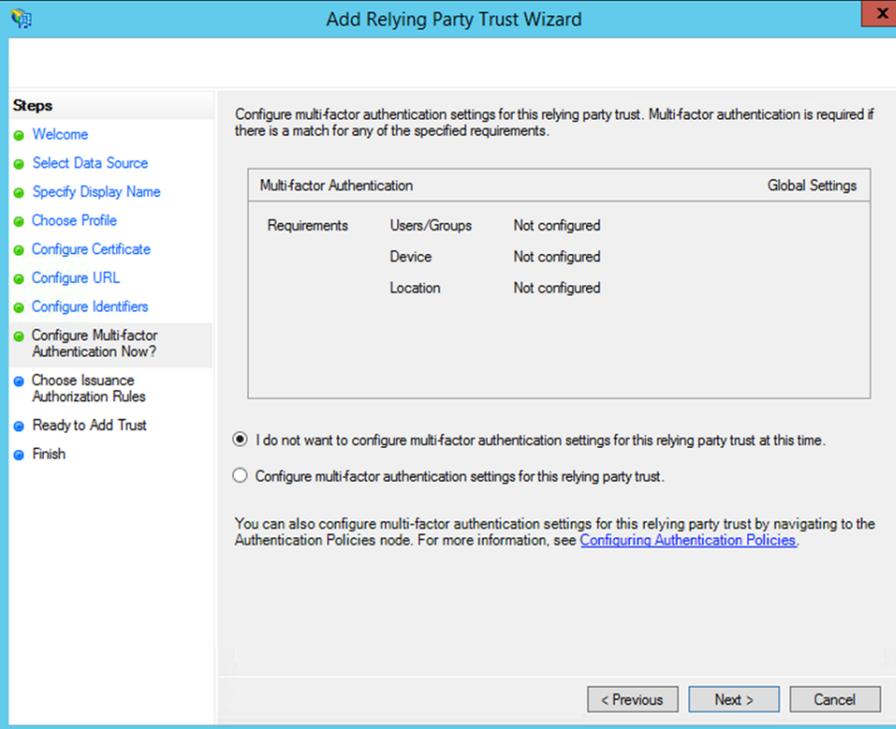
- On the next screen, check the box labeled **Enable Support for the SAML 2.0 WebSSO protocol**. The service URL will be <https://ADFS.Shufflrr.Local/login/samlassertionconsumerservice>. **Note that there's no trailing slash at the end of the URL.**



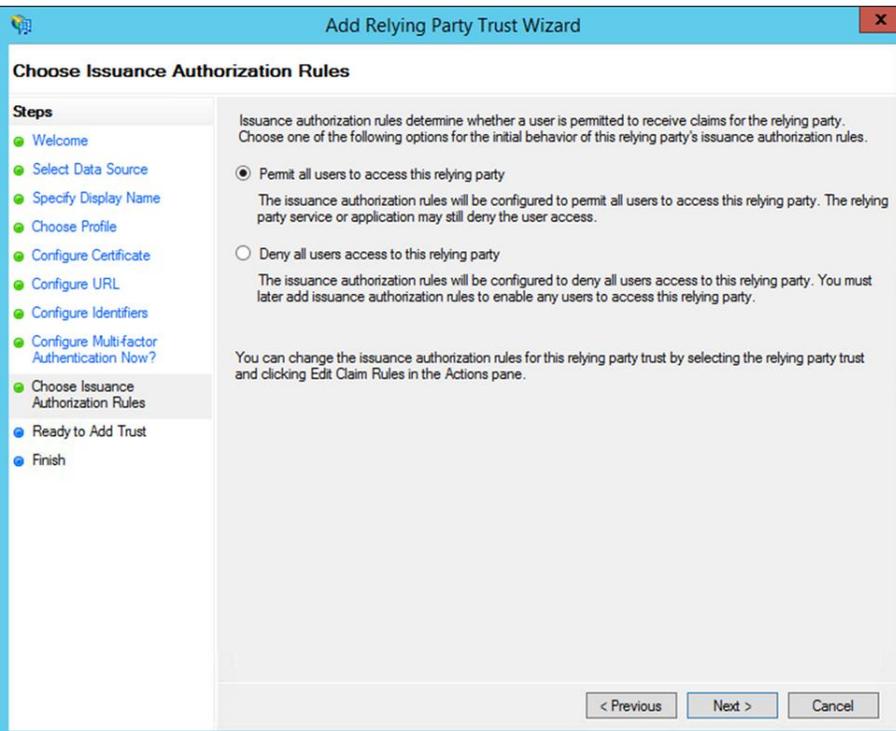
- On the next screen, add a **Relying party trust identifier** as such <https://ADFS.shufflrr.local>



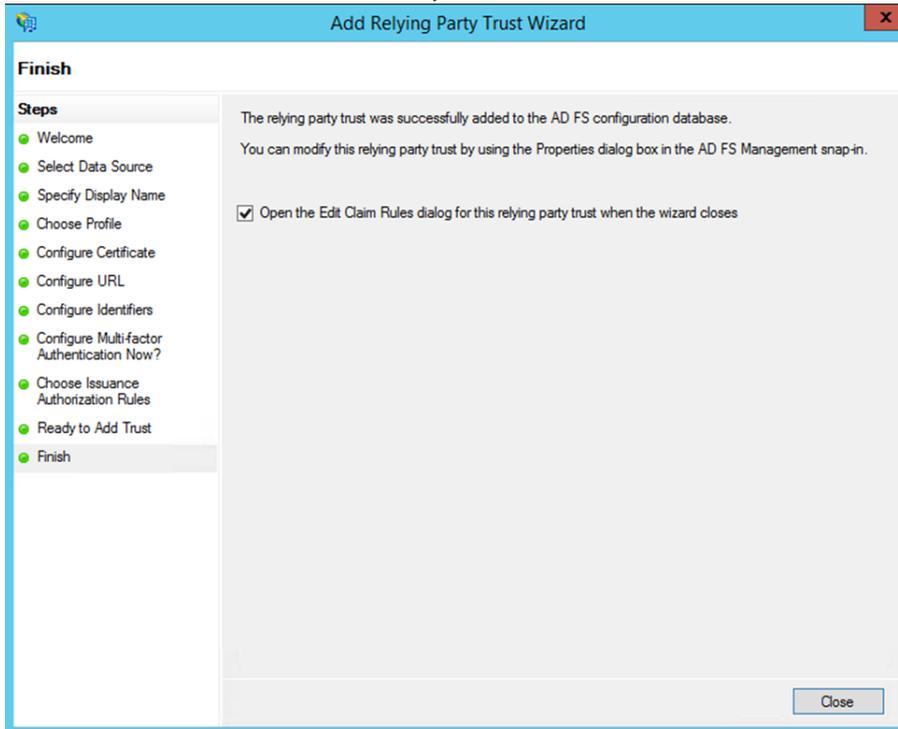
- On the next screen, you may configure multi-factor authentication, but this is beyond the scope of this guide so, in this instance, we go ahead and DON'T configure it. Hit **Next**.



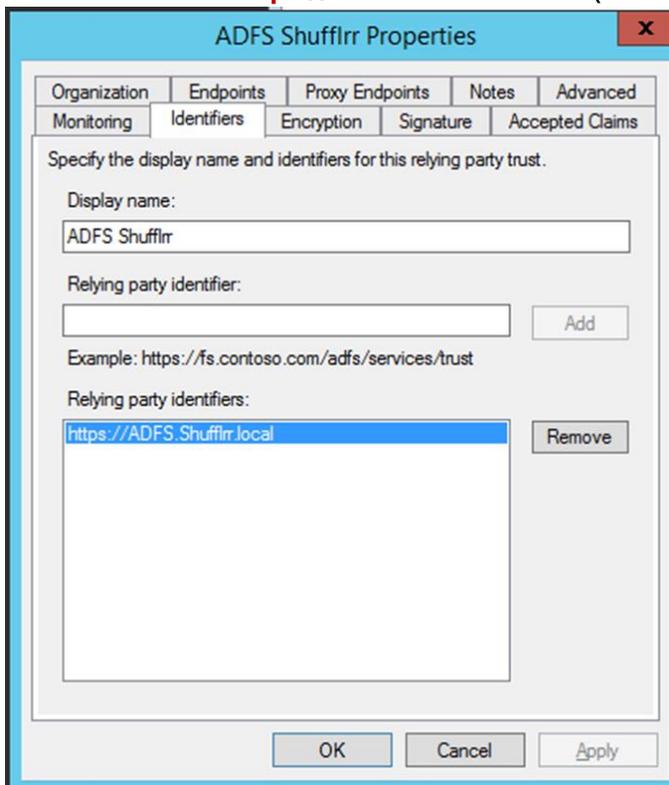
- On the next screen, select the **Permit all users to access this relying party** radio button.



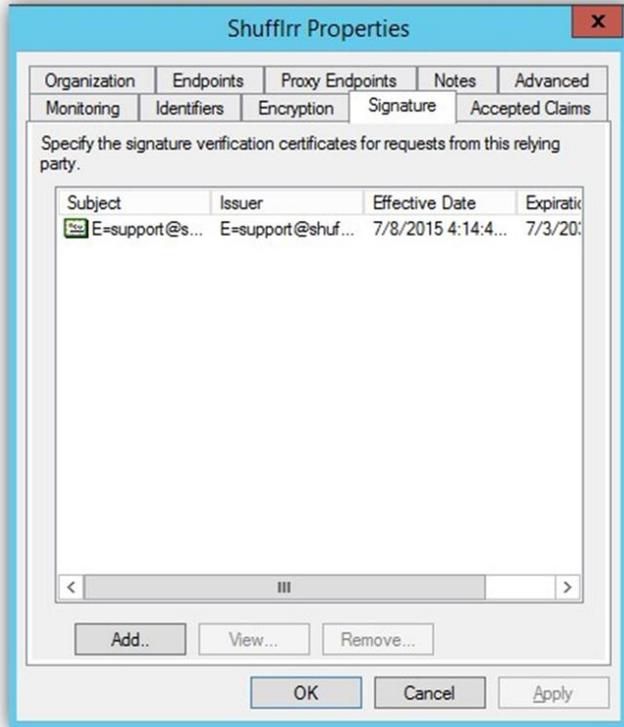
- On the next two screens, the wizard will display an overview of your settings. On the final screen use the **Close** button to exit and open the **Claim Rules** editor.



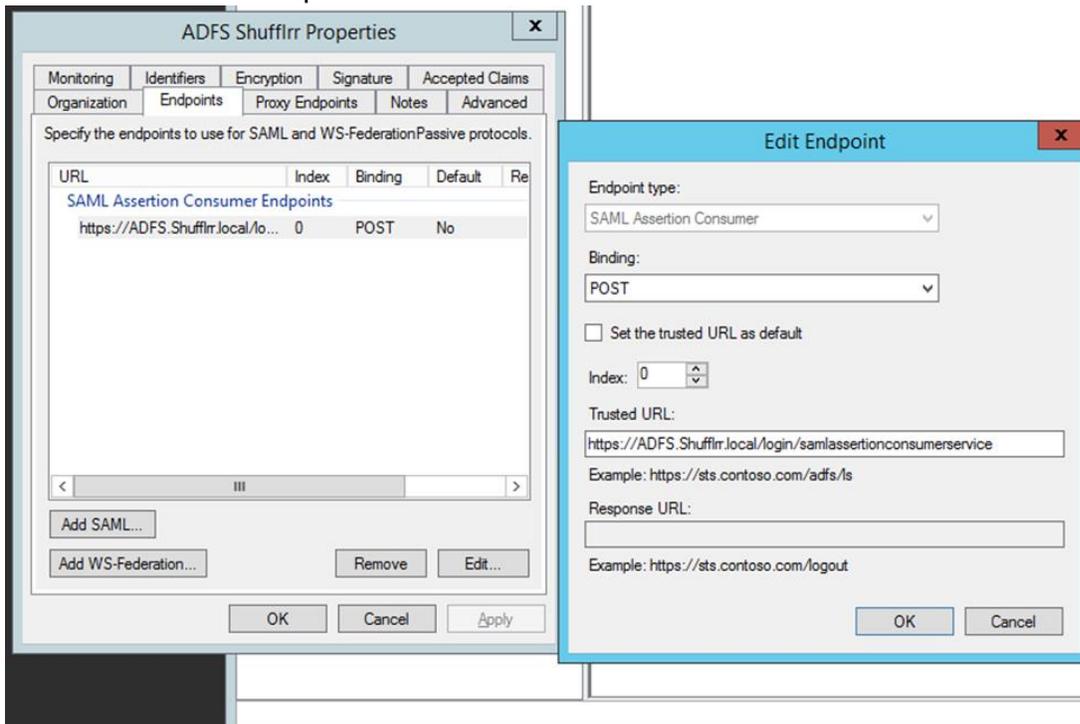
- DoubleClick on the newly created RPT to view its properties. Once open, on the Identifiers tab, Add the identifier **https://ADFS.Shufflrr.local** (Service Provider ID).



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.

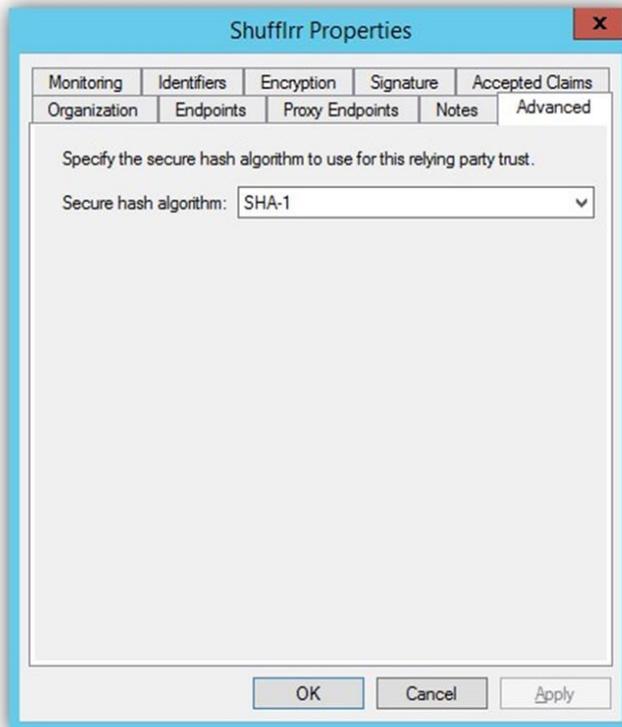


13. On the Advanced tab, Configure the hash algorithm for SHA-1 (Current Shufflrr signature cert is SHA-1) and then Configure the Relying Party trust so that both the Assertion and the Response are signed:

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

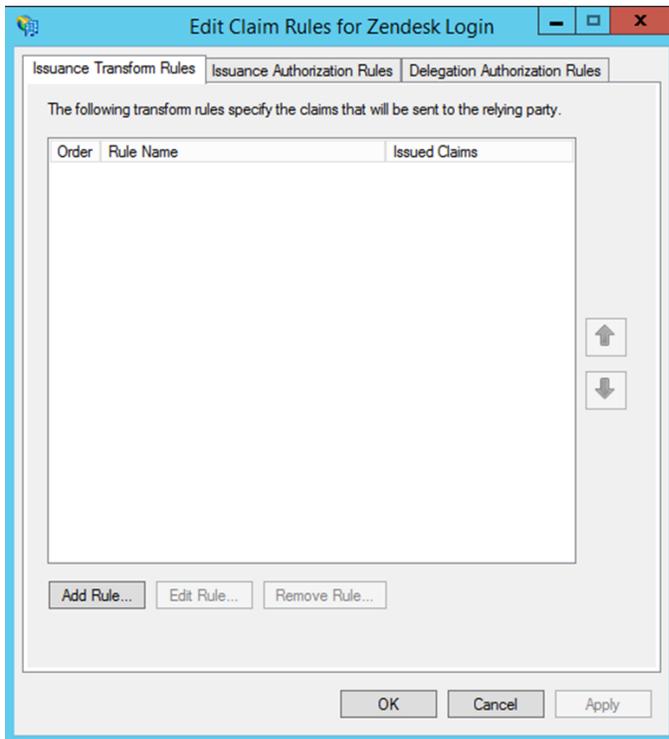
Note: Your TargetName is the Display name for your Identifier and in this case 'ADFS Shufflrr'.

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

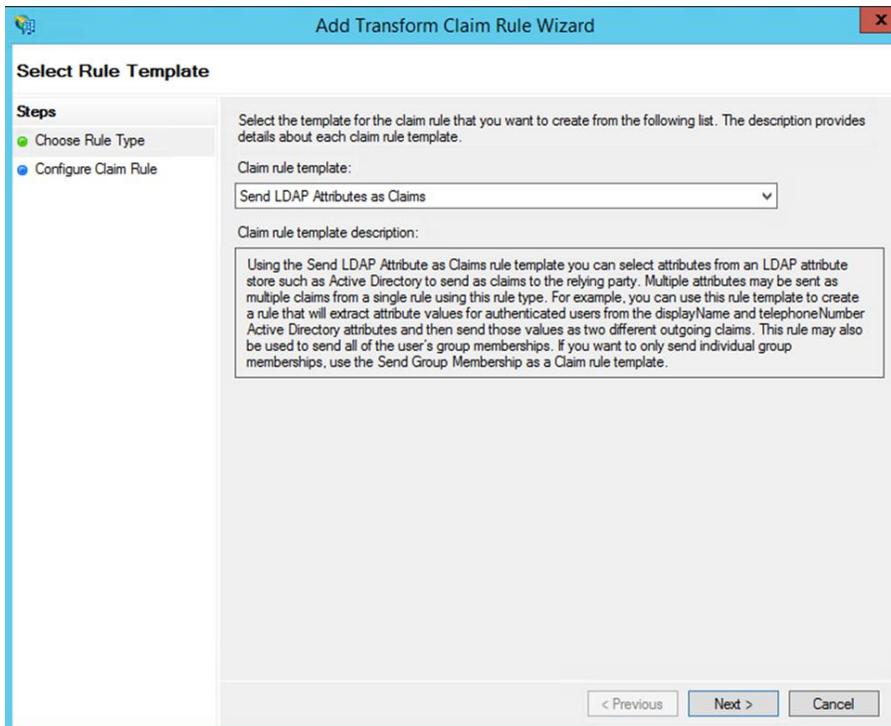


Step 2 - Creating claim rules

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

x
Edit Rule - send ldap as 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)
▶	E-Mail-Addresses ▼	Name ID ▼
	E-Mail-Addresses ▼	email address ▼
	Given-Name ▼	first name ▼
	Surname ▼	last name ▼
*	▼	▼

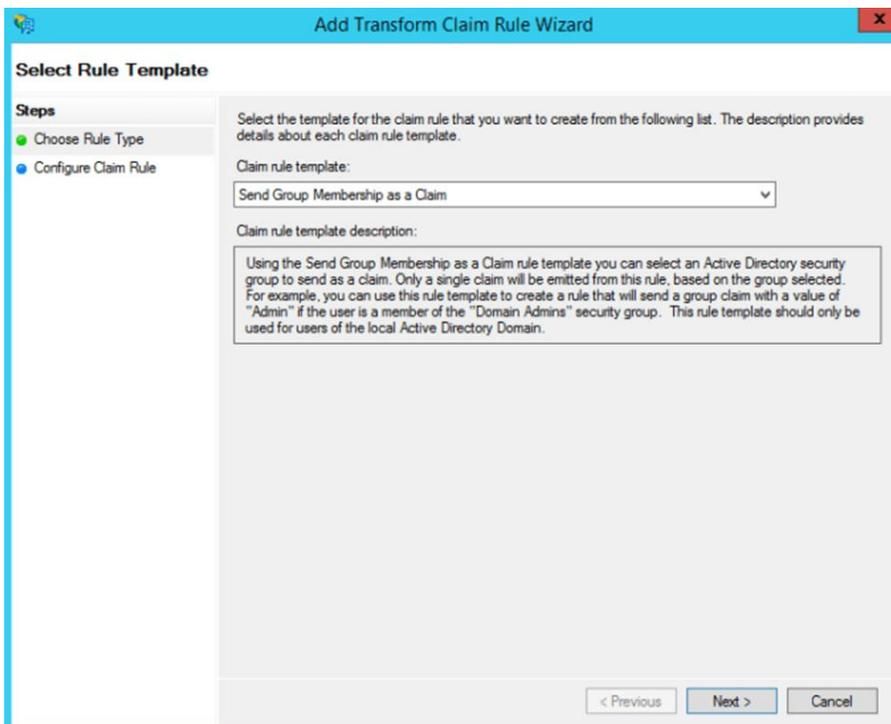
View Rule Language...
OK
Cancel

Step 2 - Setting Up Groups in SAML from ADFS

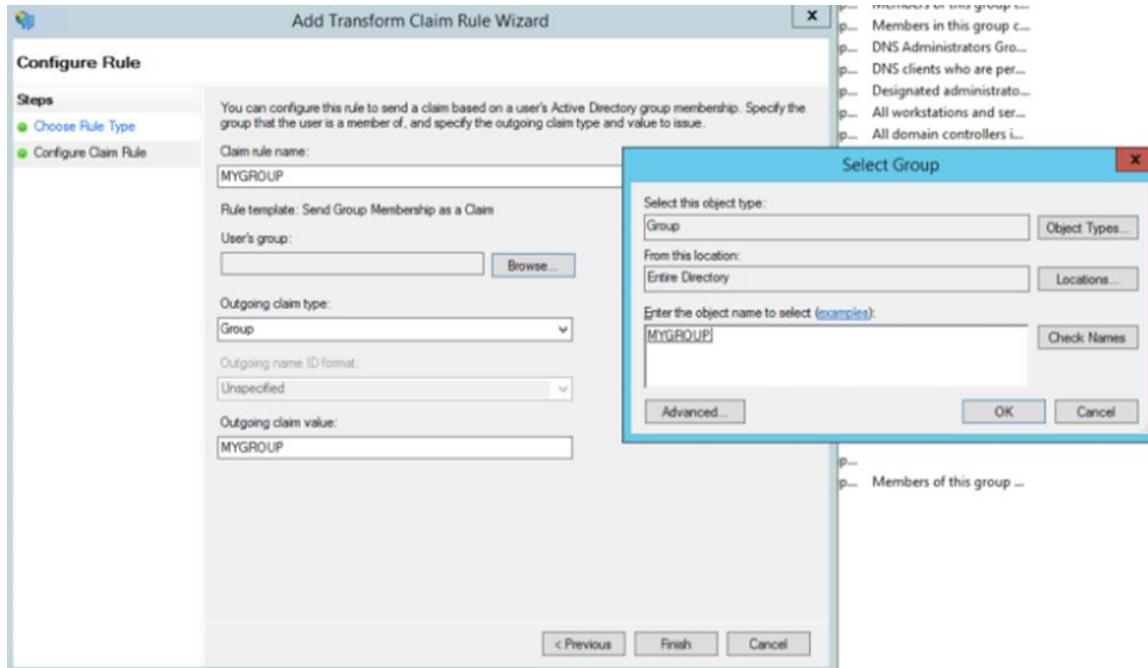
1. Right-click your Relying Party Trust and select Edit Claim Rules....



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

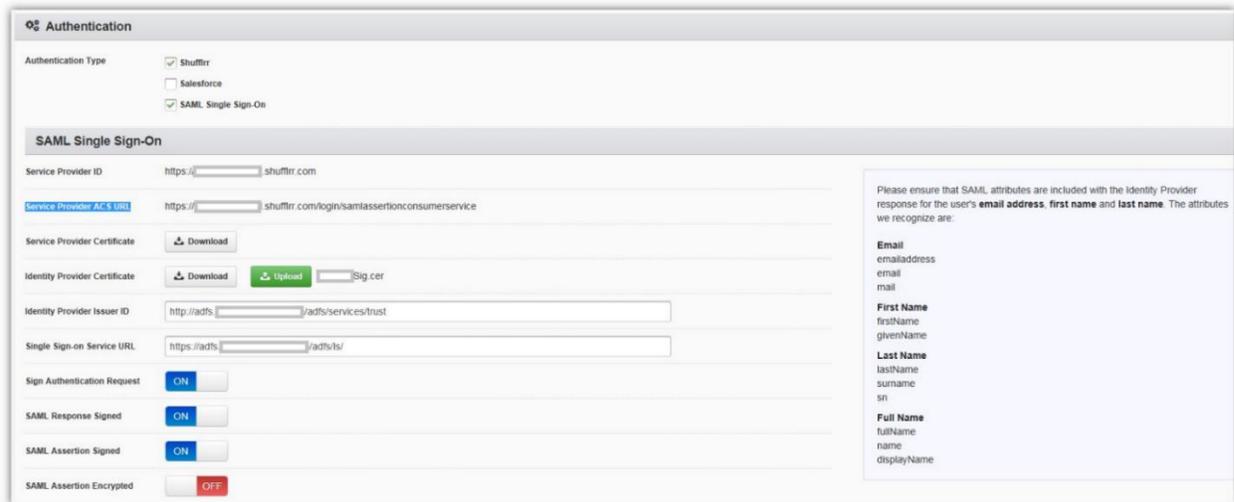


4. Enter the **Claim rule name**.
5. Click **Browse** to select your **User's group**.
6. Select **Group** as your **Outgoing claim type**.
7. Set your **Outgoing claim value** to match your group's name.
8. Click **Finish**.



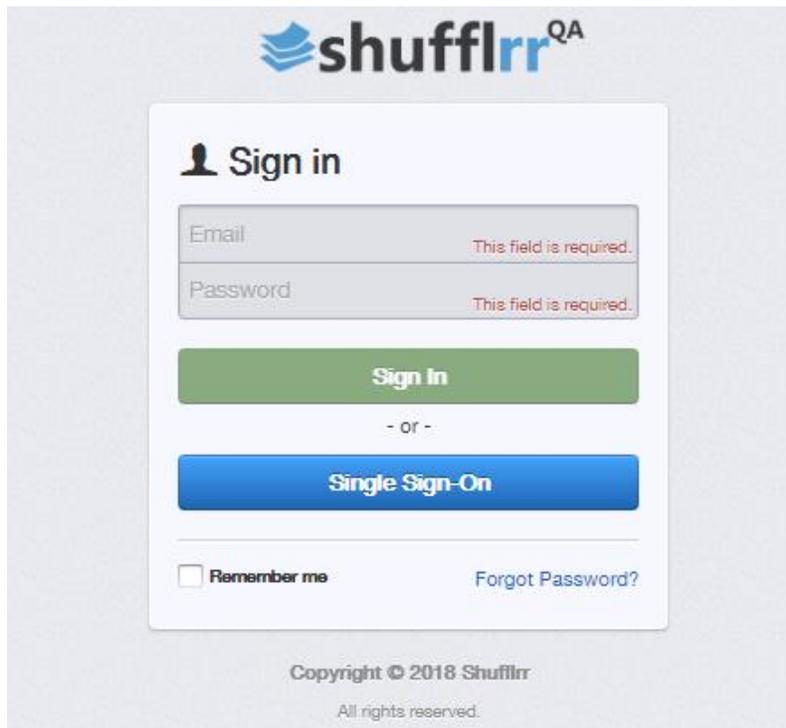
Step 4 – Testing SSO login

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



The screenshot shows the 'Authentication' configuration page in the Shufflrr Admin interface. It features a 'SAML Single Sign-On' section with various fields and toggle switches. The 'Authentication Type' section has 'Shufflrr' and 'SAML Single Sign-On' checked. The 'SAML Single Sign-On' section includes fields for 'Service Provider ID', 'Service Provider ACS URL', 'Service Provider Certificate', 'Identity Provider Certificate', 'Identity Provider Issuer ID', and 'Single Sign-on Service URL'. There are also toggle switches for 'Sign Authentication Request', 'SAML Response Signed', 'SAML Assertion Signed', and 'SAML Assertion Encrypted'. A 'Download' button is present for the 'Service Provider Certificate'. A 'Please ensure that SAML attributes are included with the Identity Provider response for the user's email address, first name and last name. The attributes we recognize are:' note lists attributes: Email (emailaddress, email, mail), First Name (firstName, givenName), Last Name (lastName, surname, sn), and Full Name (fullName, name, displayName).

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



The screenshot shows the 'Sign in' page for Shufflrr QA. It features a 'Sign in' header with a user icon. Below the header are two input fields: 'Email' and 'Password', both with a red error message 'This field is required.'. A green 'Sign In' button is positioned below the input fields. Below the button is a '- or -' separator. A blue 'Single Sign-On' button is positioned below the separator. At the bottom of the form, there is a 'Remember me' checkbox and a 'Forgot Password?' link. The footer of the page reads 'Copyright © 2018 Shufflrr All rights reserved.'