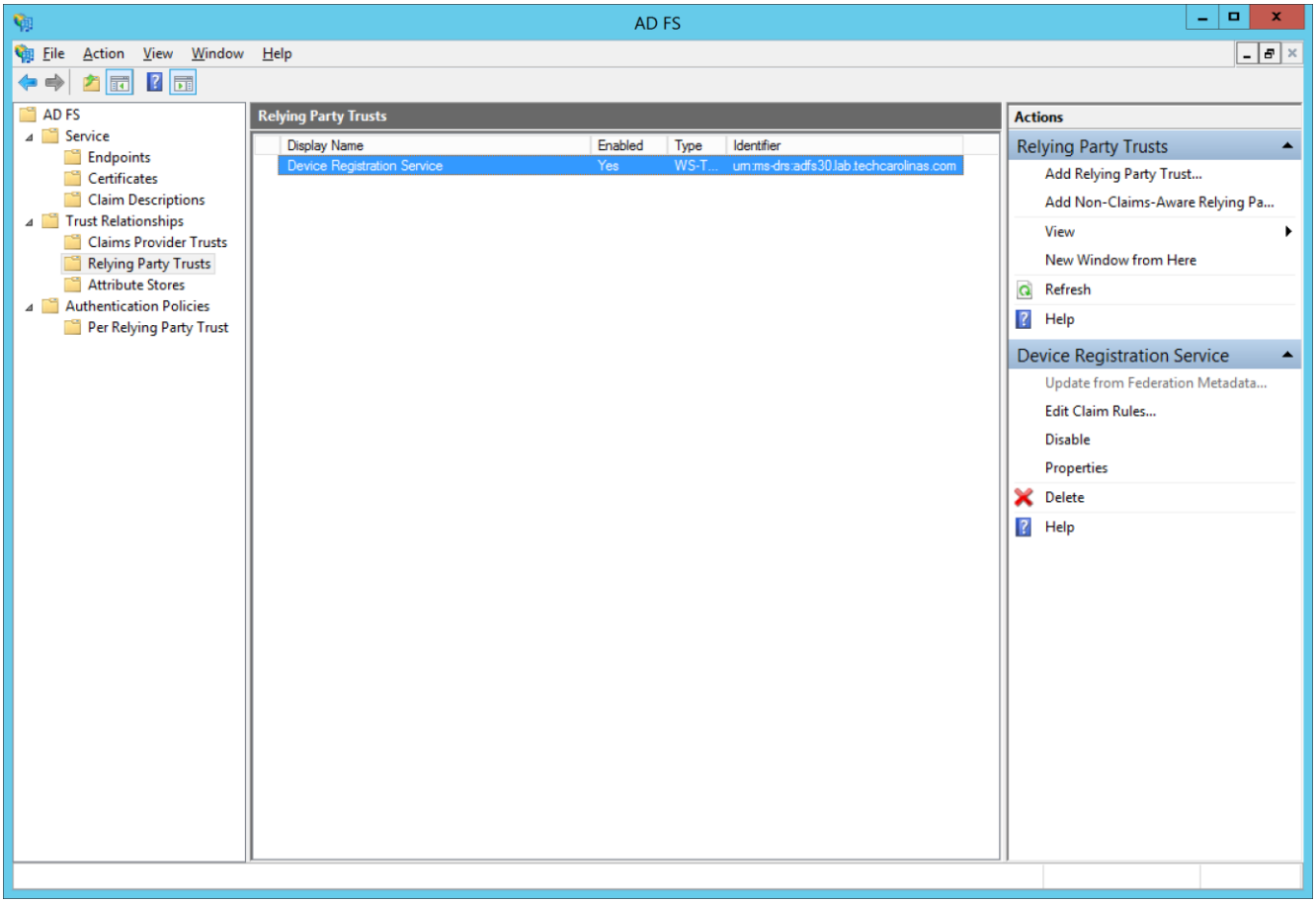
Microsoft ADFS 3.0 Configuration Guide for the 7SIGNAL Mobile Eye Dashboard

Microsoft ADFS 3.0 Configuration

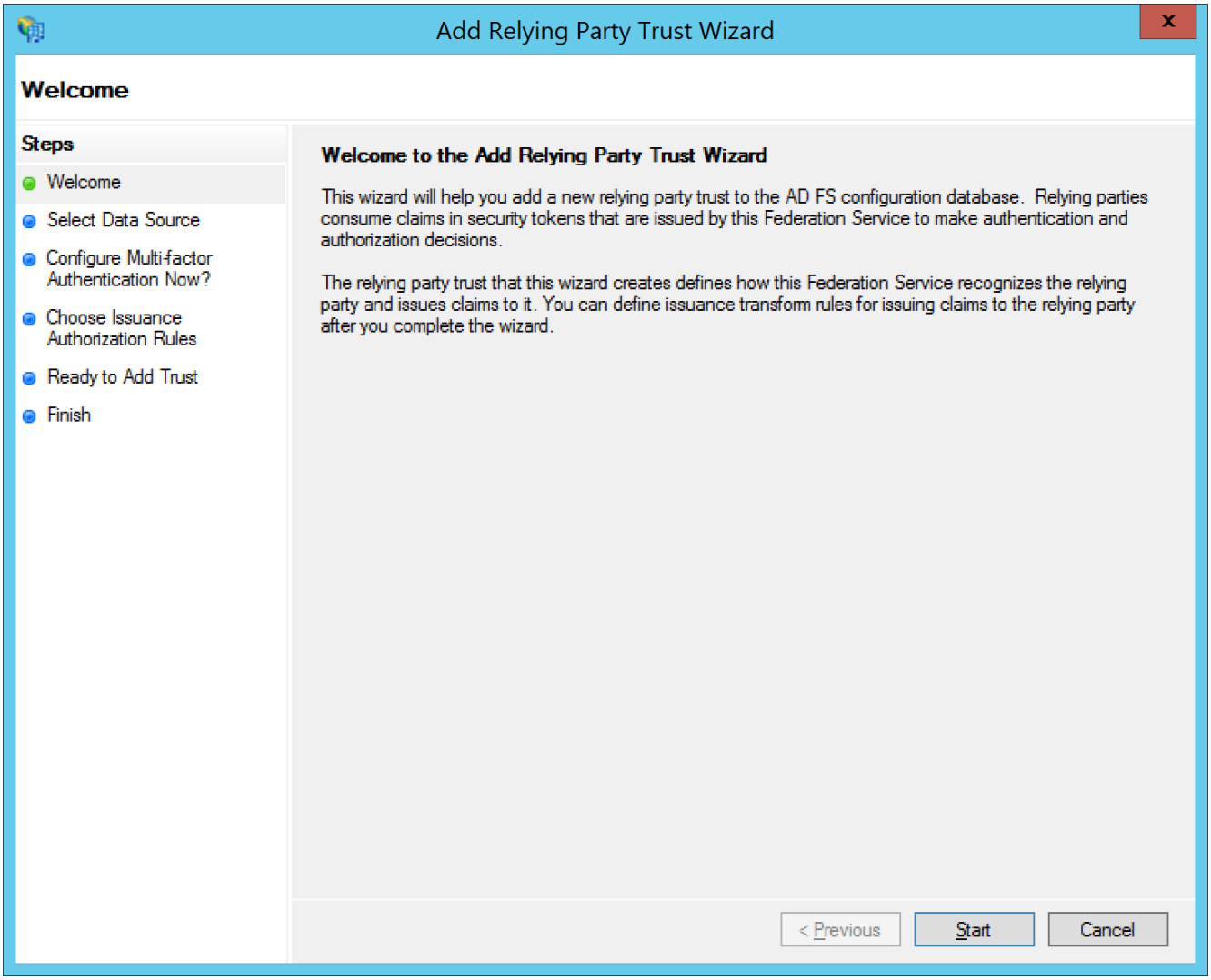
Relying Party Trust implementation for 7SIGNAL SSO

This configuration guide will walk through the steps to configure Active Directory Federation Services 3.0 (Windows Server 2012R2) to work with the 7SIGNAL Mobile Eye Dashboard. It is worth noting that your Active Directory domain and forest functional version may be different that your ADFS version. For instance, this test was done leveraging a Microsoft Active Directory domain running Windows 2016 for both forest and domain functional levels while still implementing the ADFS services at version 3.0 which comes as part of Window Server 2012R2.

To get started, open the AD FS Management console and navigate to the Relying Party Trusts area under Trust Relationships. This is where you will add 7SIGNAL for the SAML authentication to be allowed.

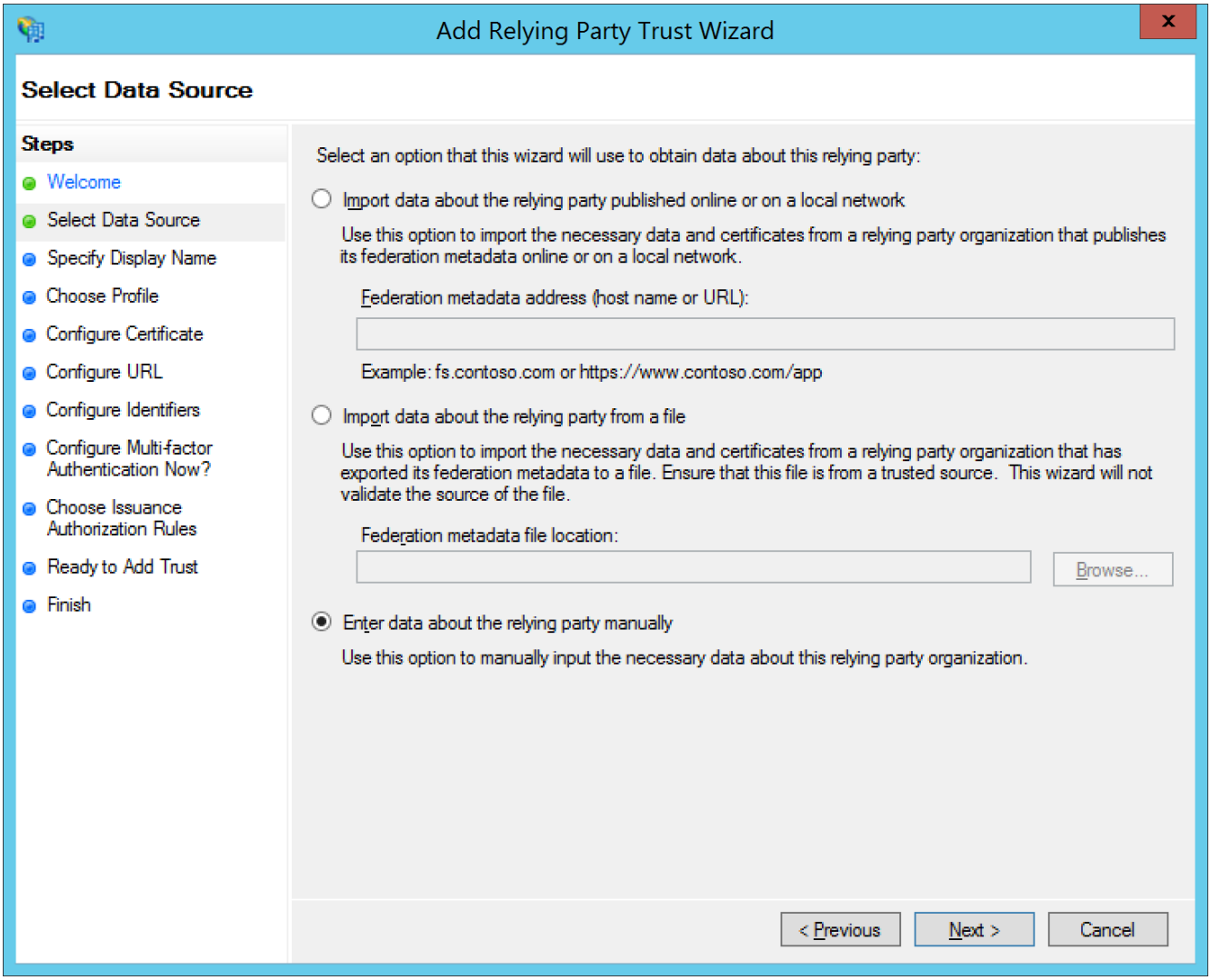


From here you will want to click “Add Relying Party Trust…” from the Actions menu which will kick off the following wizard.



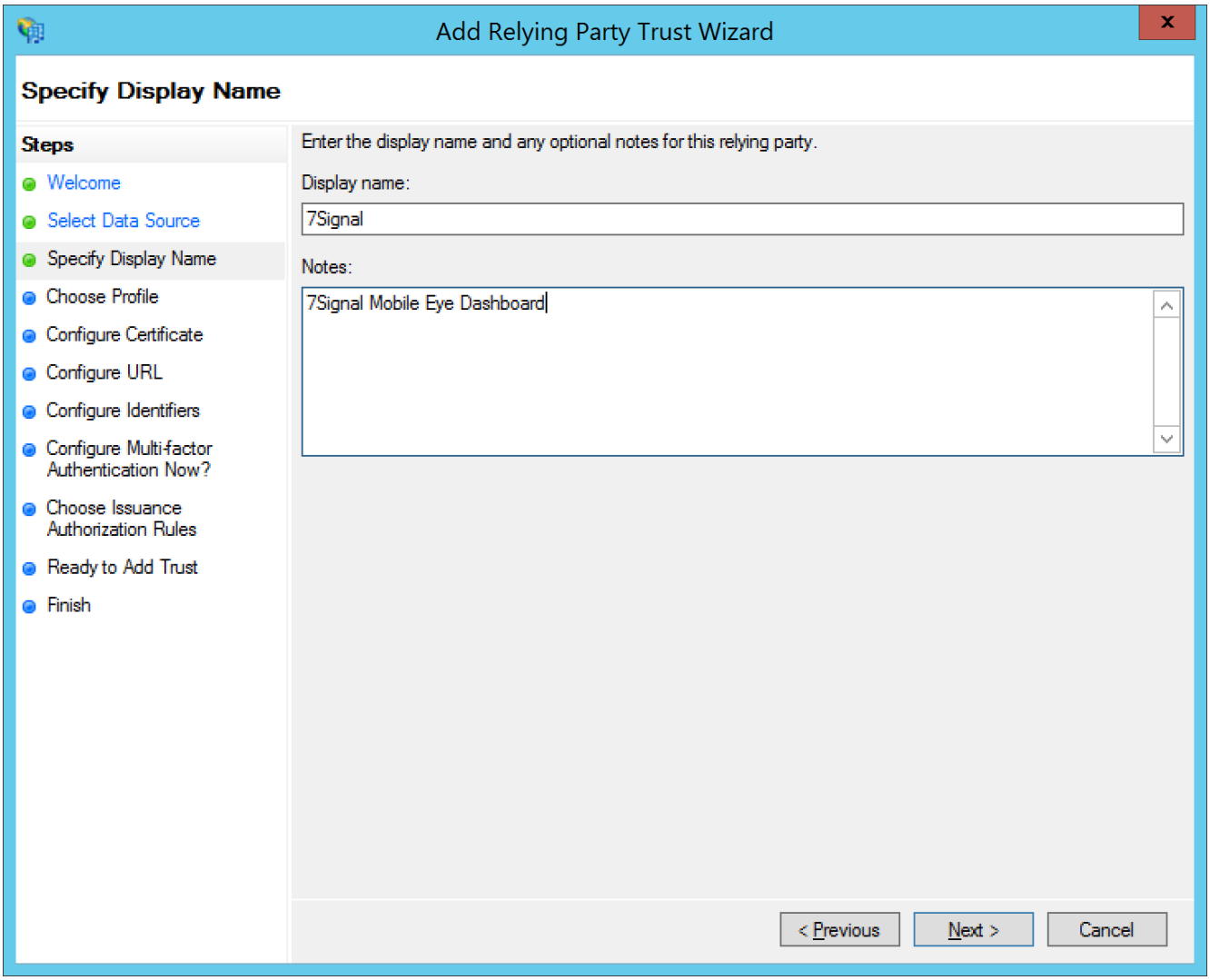
Click Start to continue

For the Data Source selection, switch the setting to the manual option at the bottom.



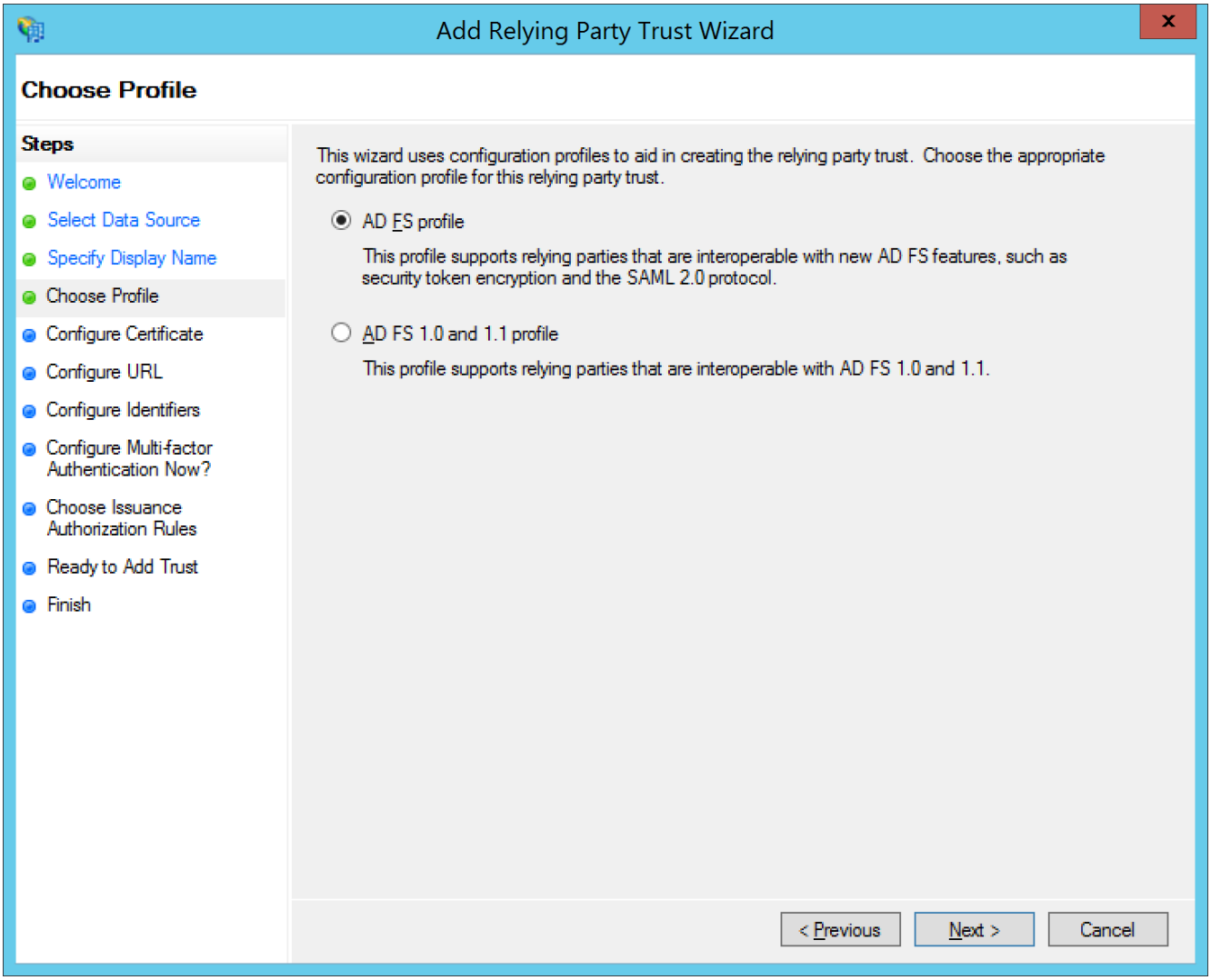
Click Next to continue

Fill in the display name for the Trust and a description/notes as desired



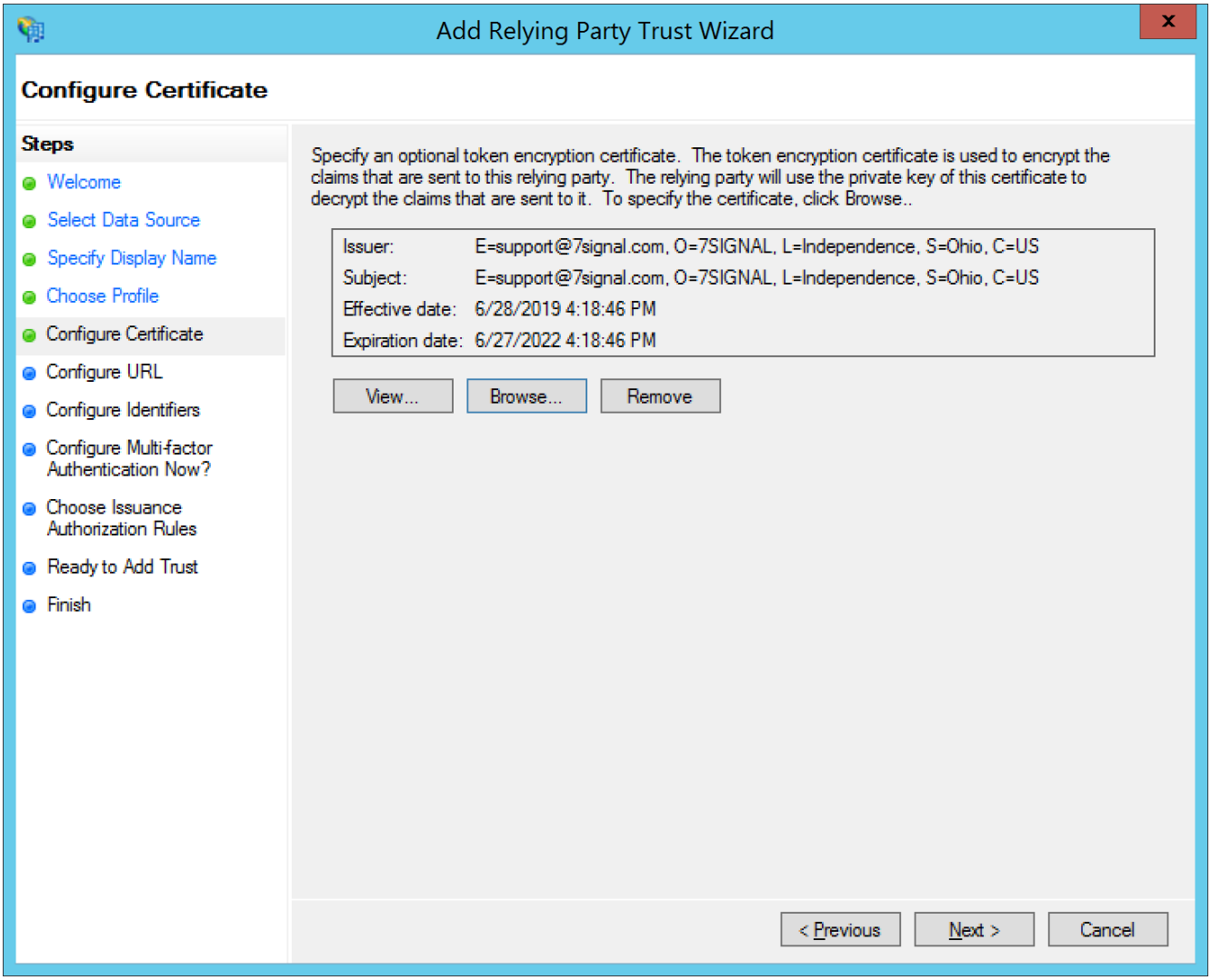
Click Next to continue

Since we will be leveraging SAML 2.0 for this relationship, leave the default of AD FS profile selected.



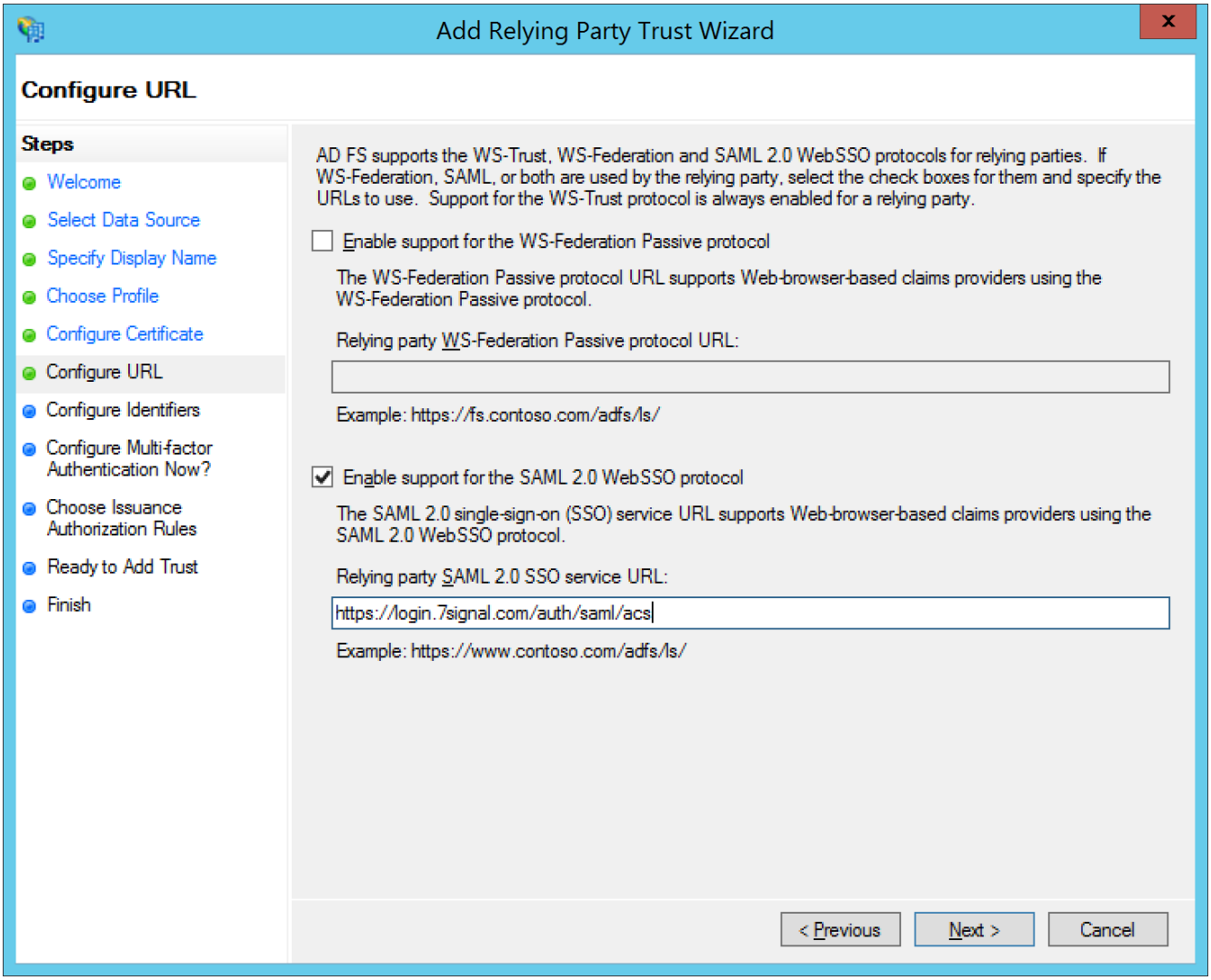
Click Next to continue

Use the Browse button to select the 7SIGNAL certificate file provided. View the details to validate it if desired.



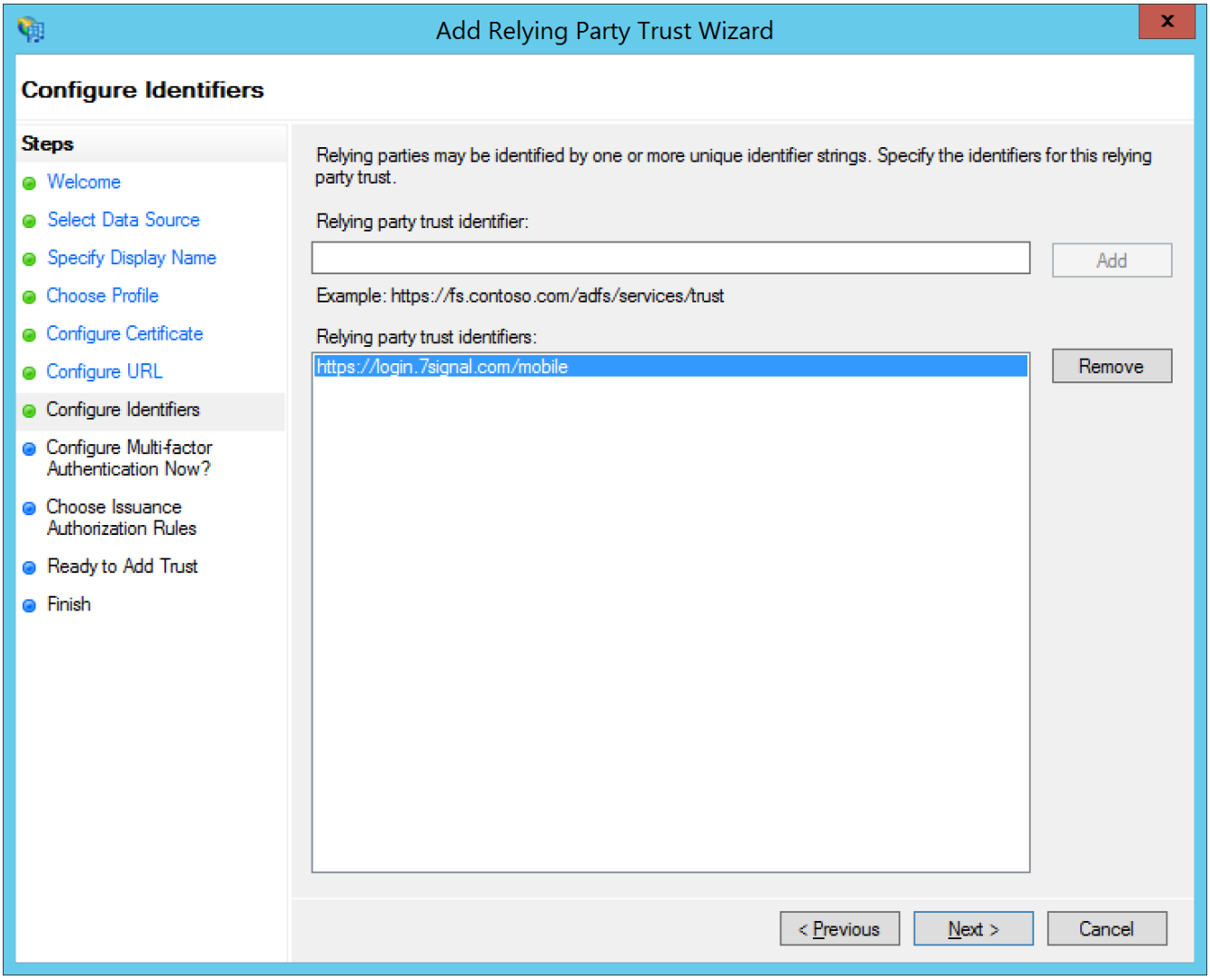
Click Next to continue

Once again, since we will be leveraging SAML 2.0, check the bottom option to enable support for this and input the SAML 2.0 SSO service URL provided by 7SIGNAL.



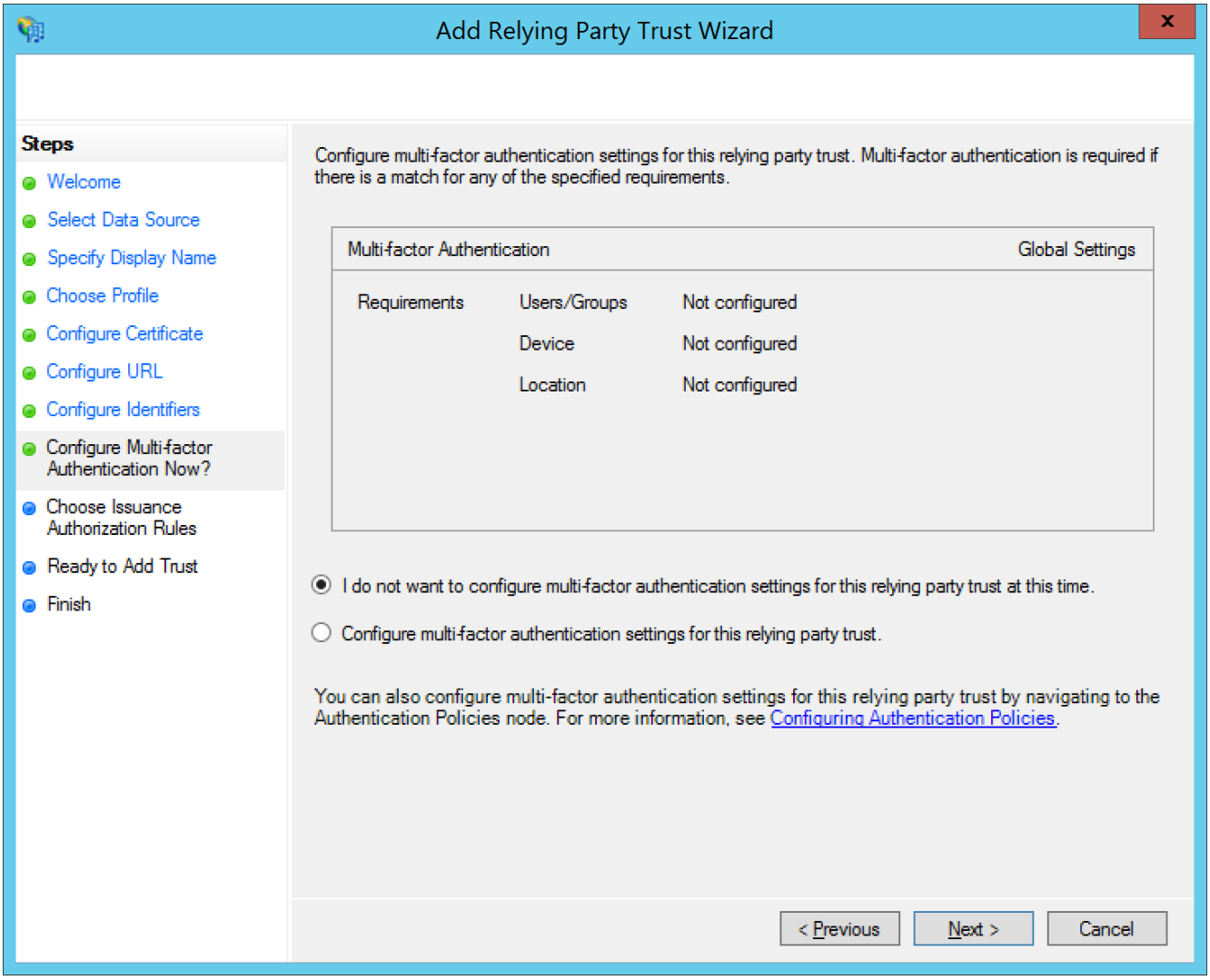
Click Next to continue

Here we need to input the Entity ID as provided by 7SIGNAL. This is the unique identifier which tells ADFS which 3rd party the SSO request is coming from to ensure the proper Trust details are used in terms of certificate associated and claims to provide.



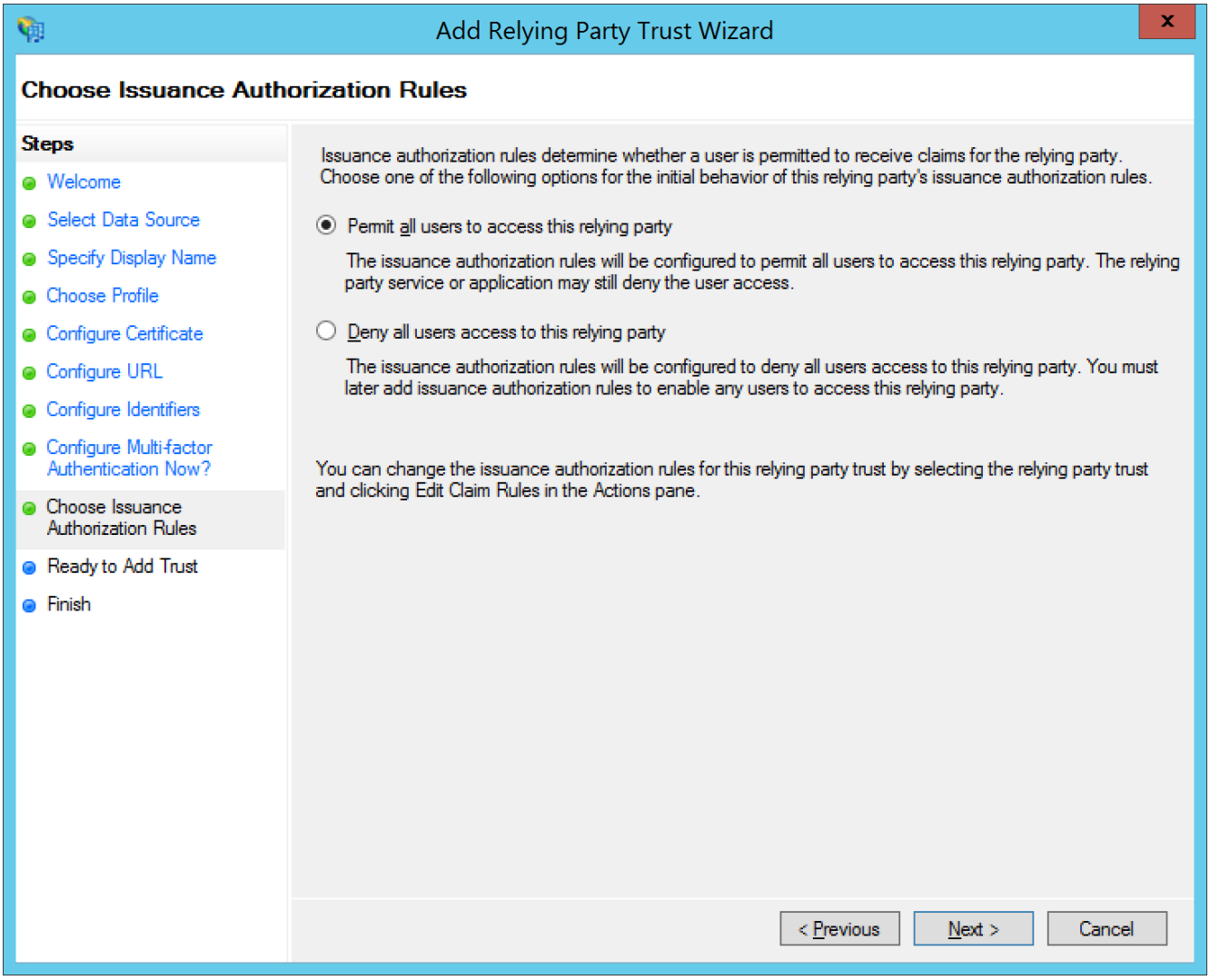
Click Next to continue

The next page deals with Multi-Factor Authentication and whether that will be configured and enforced for users or devices trying to authenticate against ADFS. You may want to leverage this for your environment, but it is outside of the scope of this document and will be left disabled.



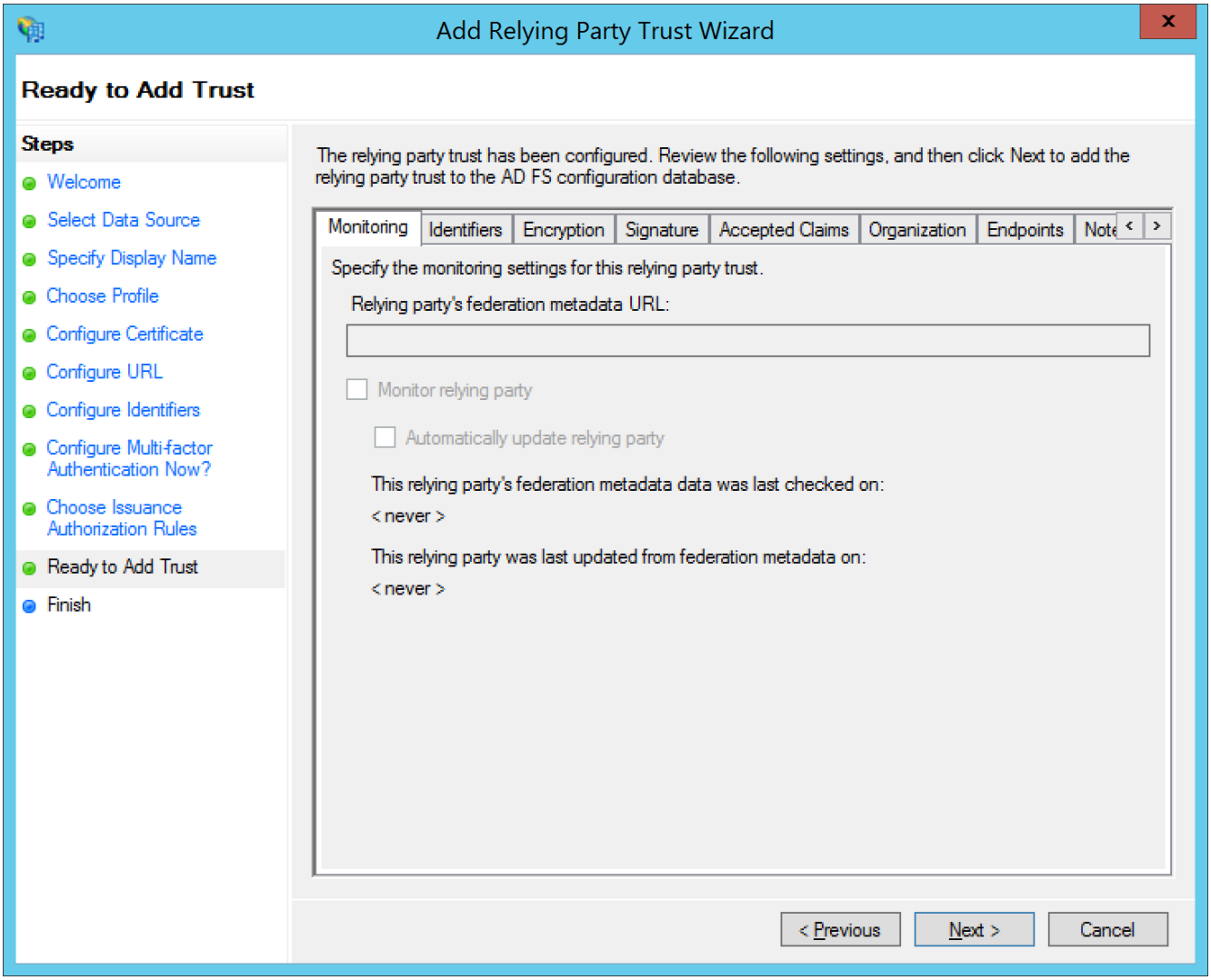
Click Next to continue

The Authorization Rules page is another way for you to decide how granular you want your services to be. For the purposes of this guide, we will leave it at the default to Permit all users in the Active Directory domain to access this relying party we are defining.



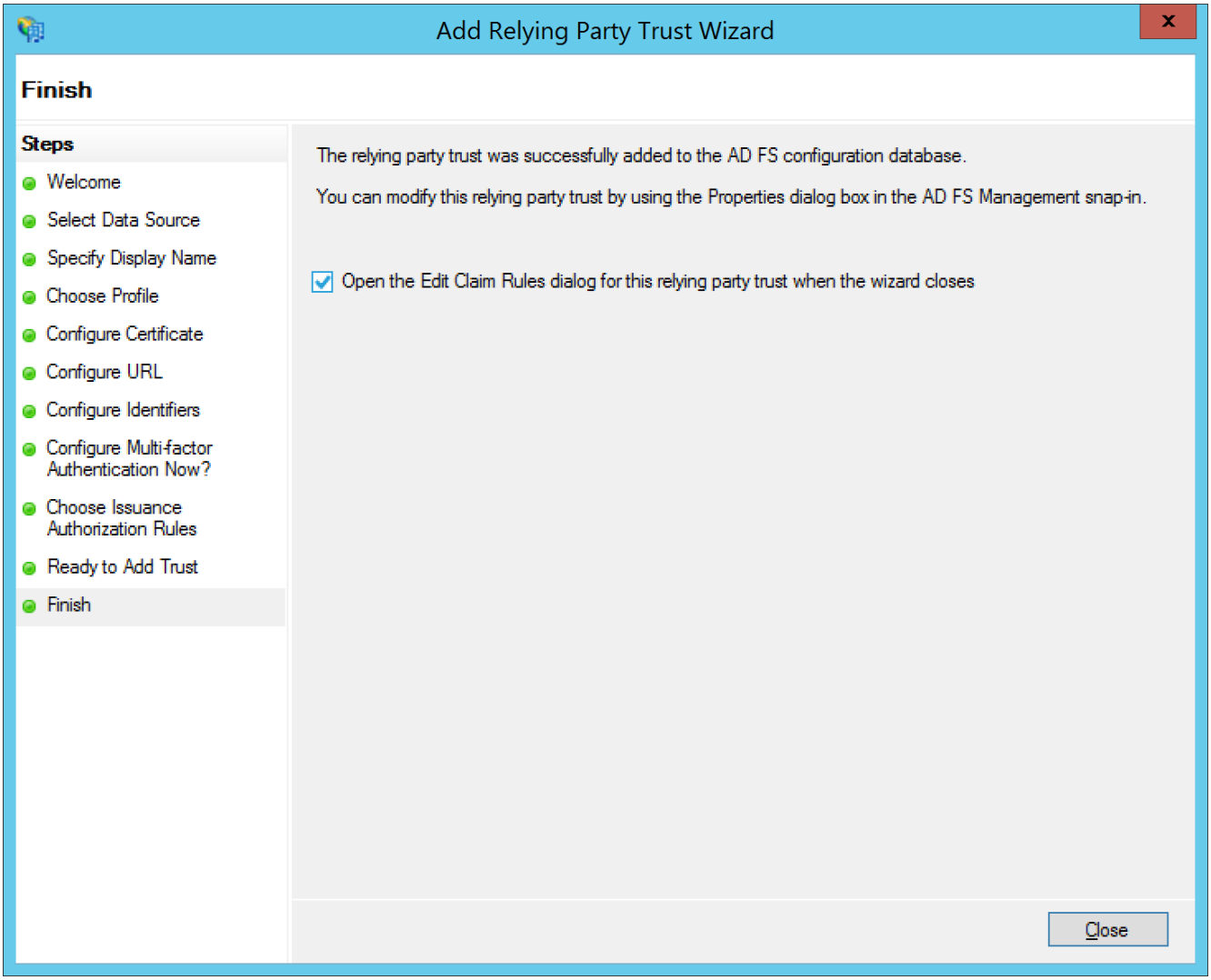
Click Next to continue

This will bring us to the page summarizing all settings made to this point. You can click through the various tabs to review things if you like.



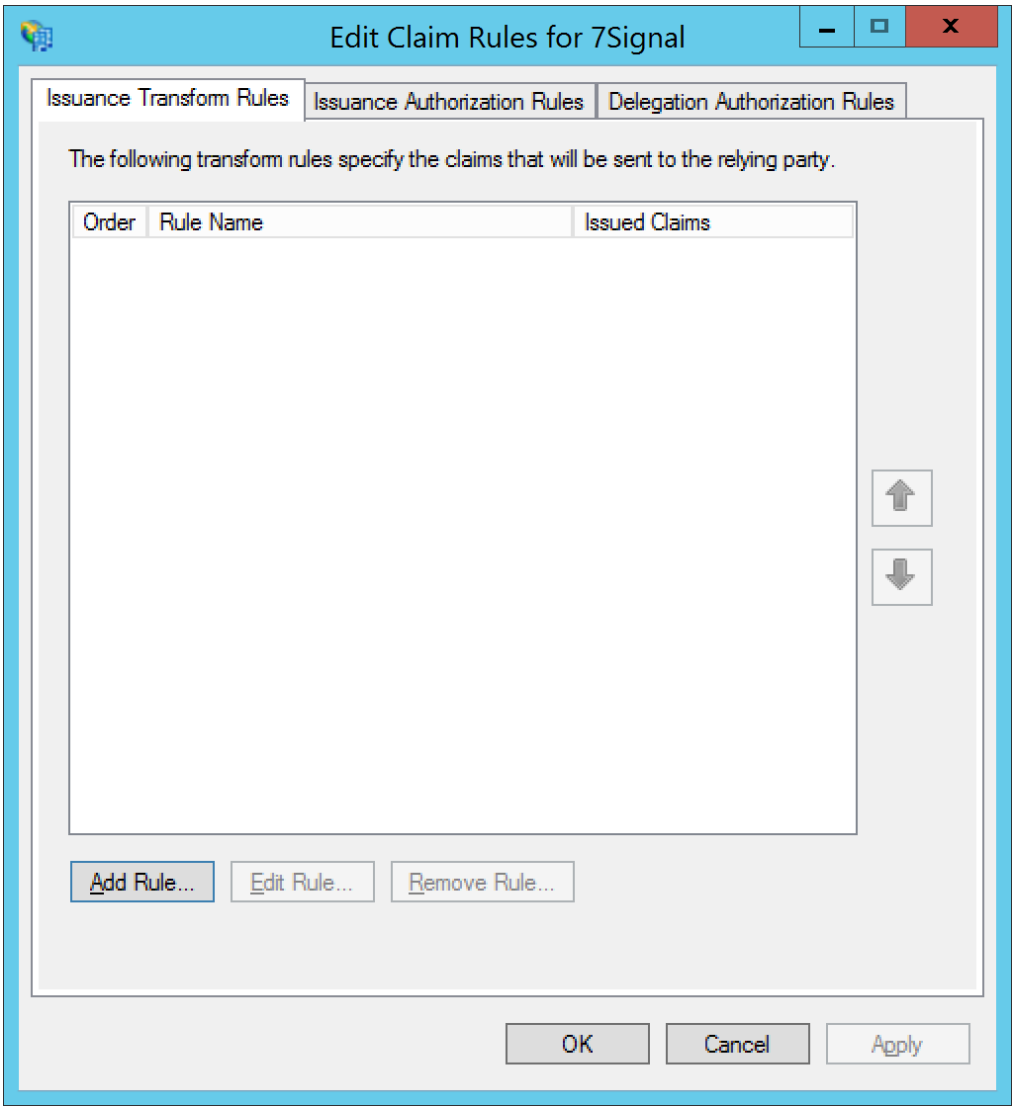
Click Next to continue

This completes adding the Relying Party Trust. By default, the Wizard will Open the Claims Rules to allow us to continue by defining that relationship.



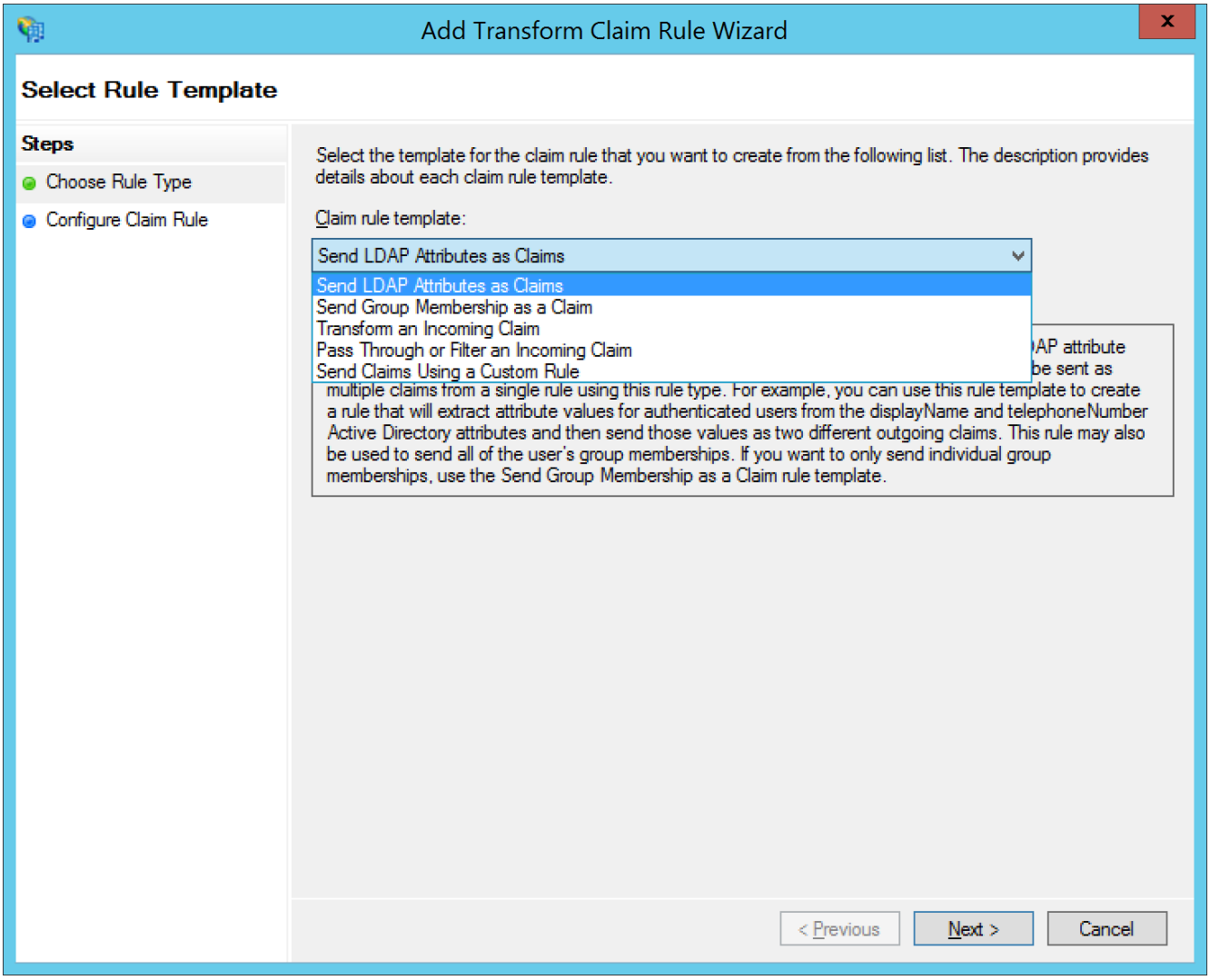
Click Close and the Edit Claims Rules window for the Trust should open

Here we will add an Issuance Transform Rule to send the appropriate Active Directory attribute in response to the SAML SSO request if the user authenticates successfully.



Click Add Rule and the following window will open

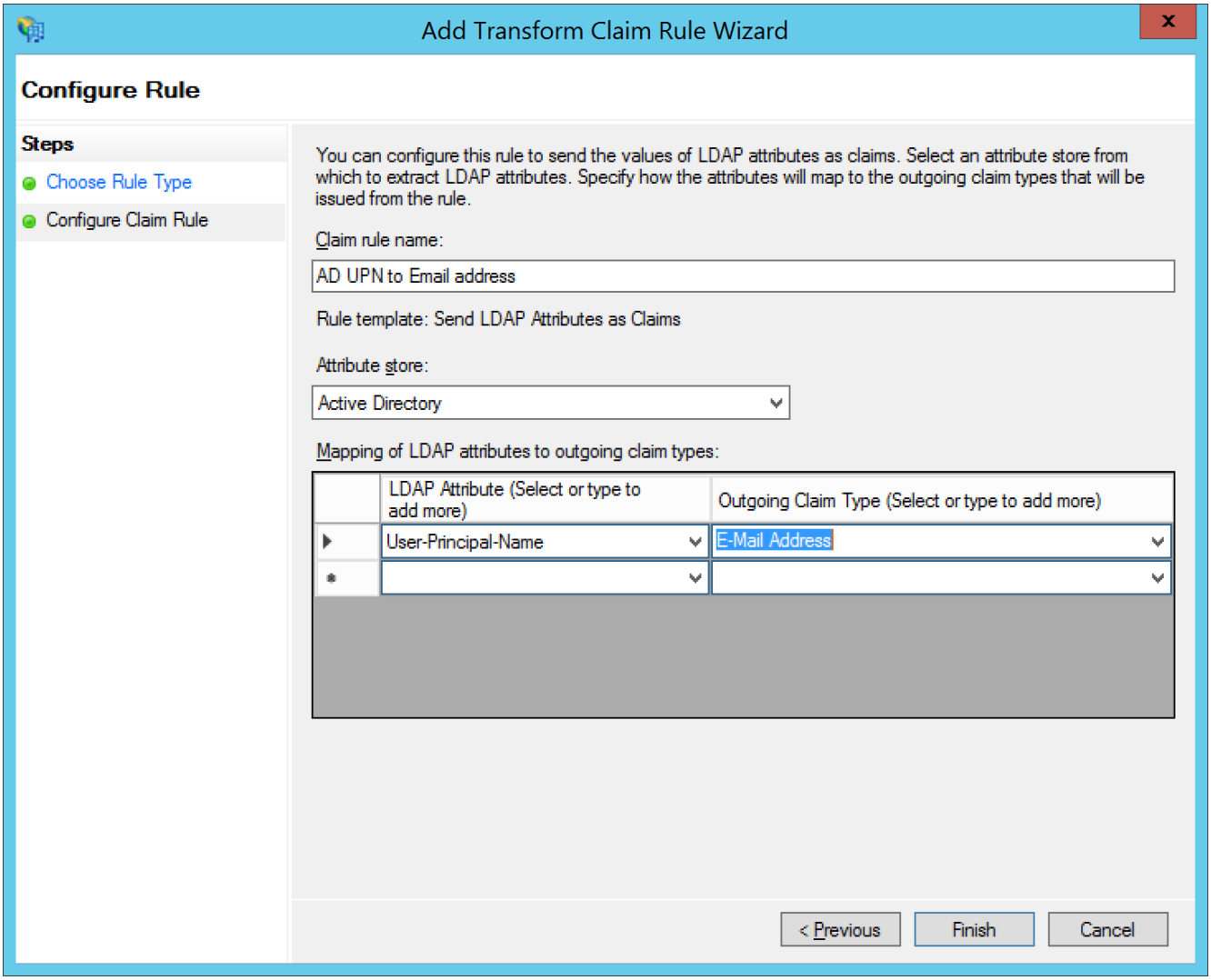
There are different templates you may choose from but for the purposes of this guide, we will assume LDAP user object Attributes will be used as 7SIGNAL looks for the user's email address to associate them to the proper details in the Mobile Eye dashboard.



Click Next to continue

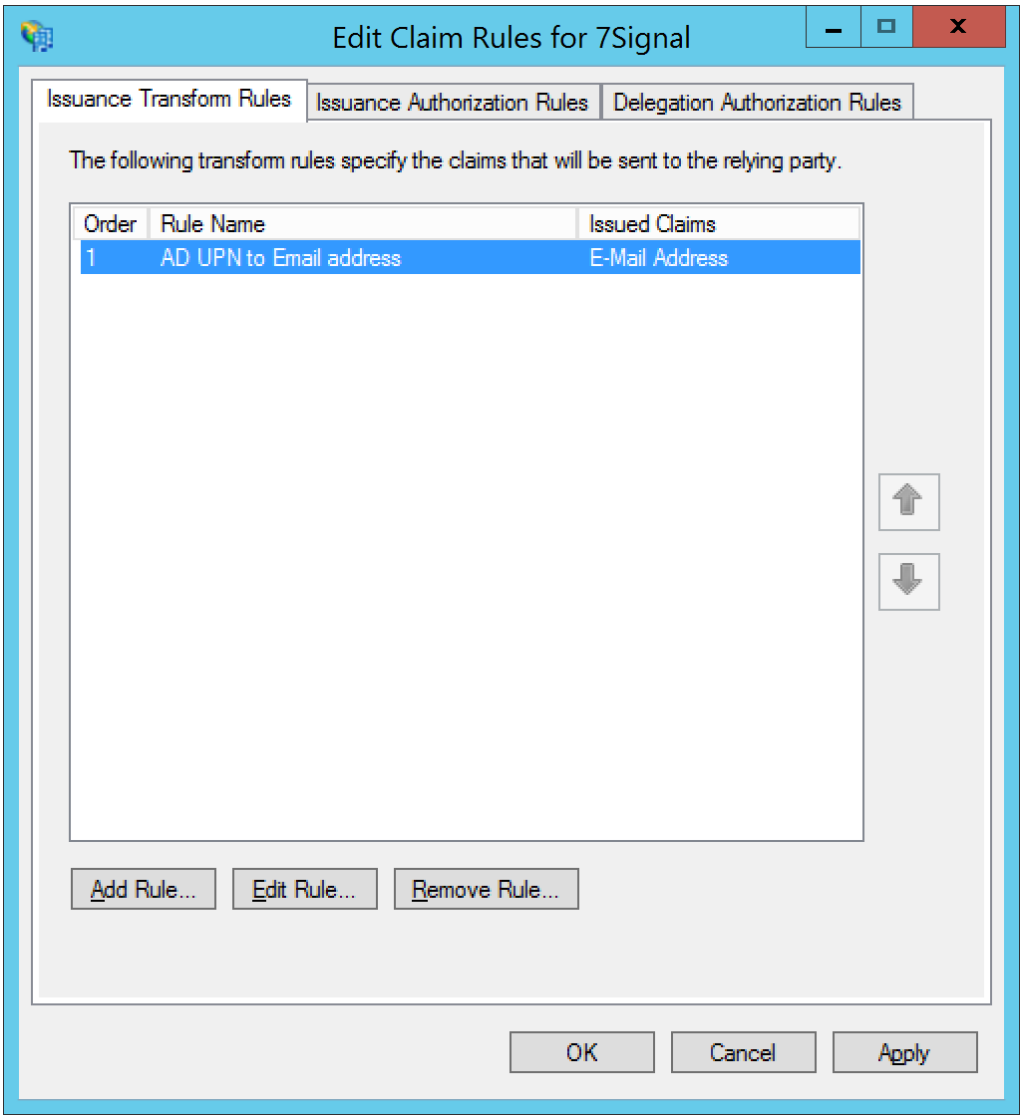
For the Claim Rule definition, you will provide a Rule name, select Active Directory as your LDAP attribute store, choose your LDAP Attribute and then the Outgoing Claim Type it will map to.

In this test environment, we did not have Microsoft Exchange Server or O365 configured so we chose to leverage the User Principal Name and send that as the Email Address claim. You may want to map the Active Directory Email Address attribute as your LDAP attribute if that is the field that matches the expected value on the 7SIGNAL side.



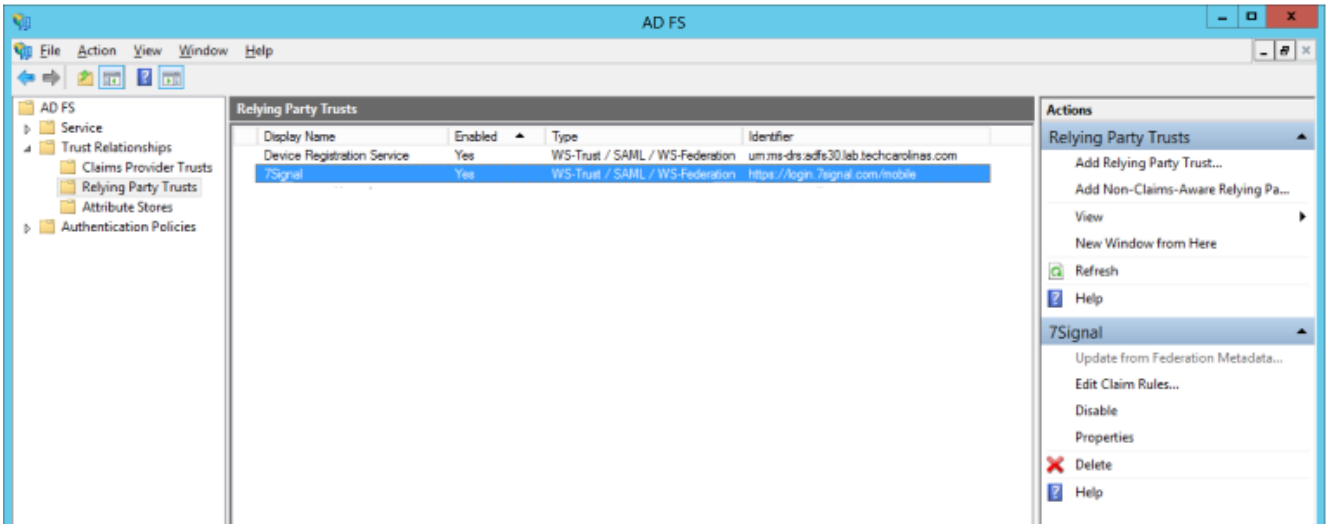
Click Finish since 7SIGNAL is only looking for this one claim to be passed

This takes you back to the overall Claim Rules screen showing your one rule you just added. You can explore the other tabs available on this window, but no changes are necessary based on how we configured things thus far.



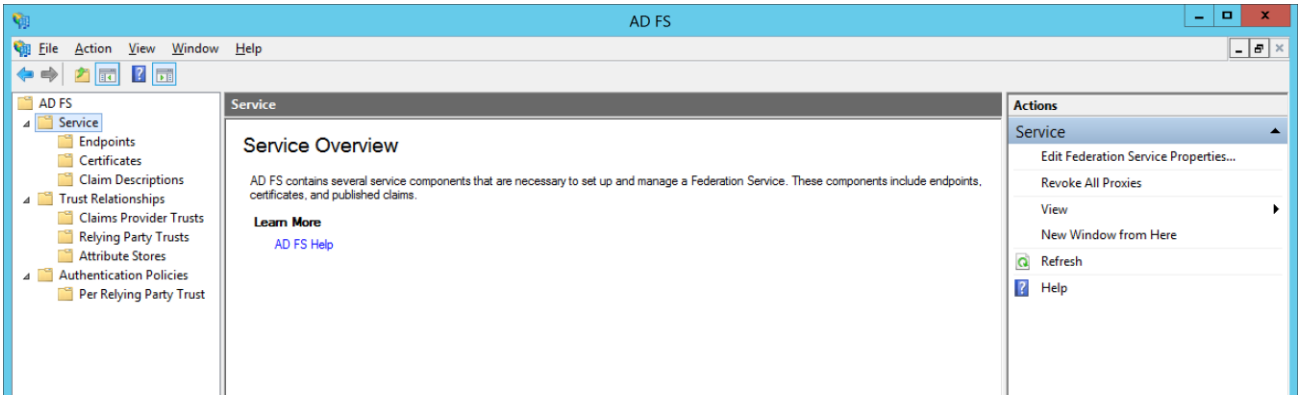
Click OK to close this Claims Rules window out

We now see our Relying Party Trust listed and it is enabled by default

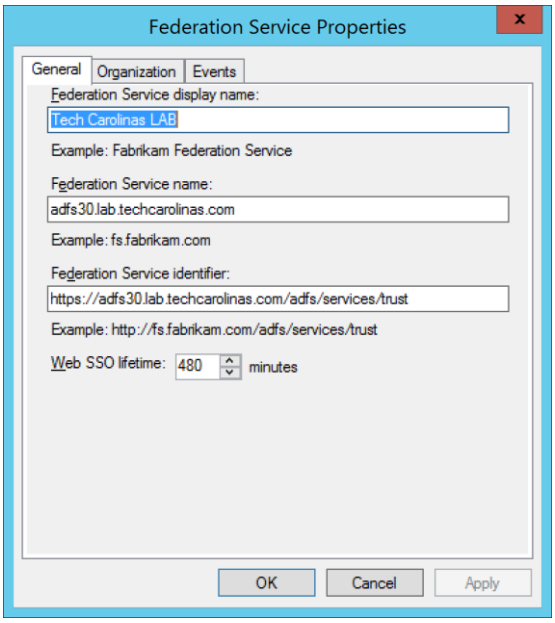


Gathering our AD FS details for 7SIGNAL to configure their side

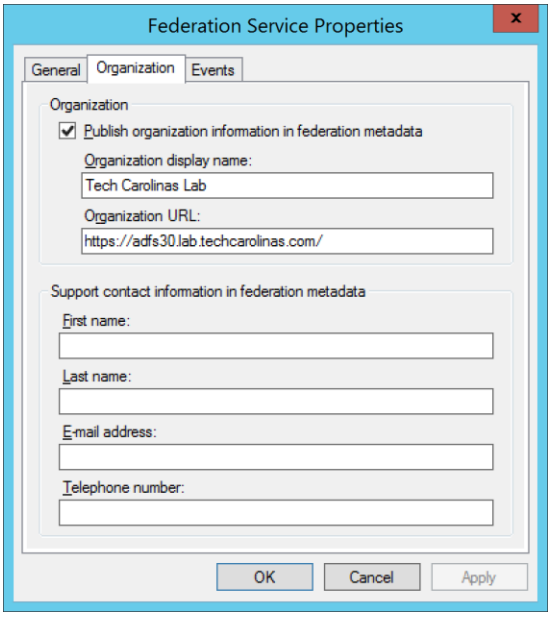
In order to configure and/or retrieve the details of our AD FS implementation, we navigate to the Service folder in the AD FS Management console and choose “Edit Federation Service Properties” from the Actions menu or by right-clicking the Service folder.



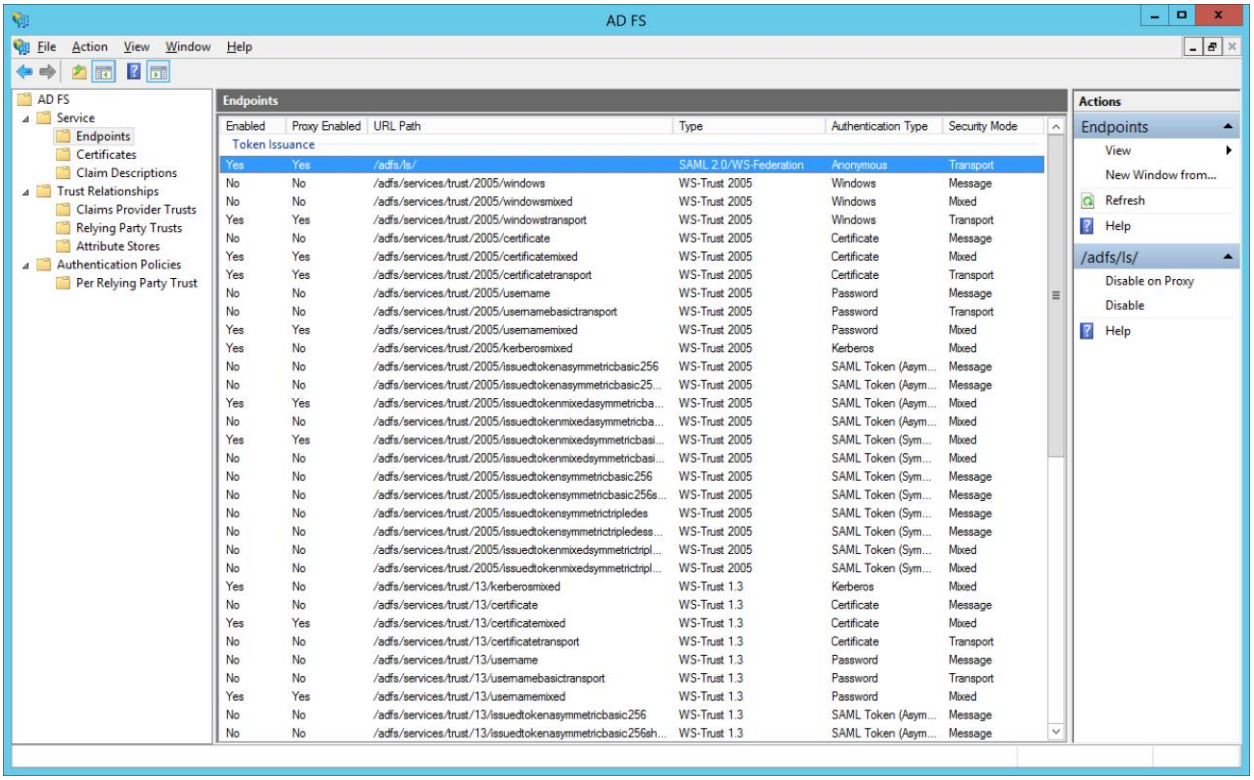
This brings up the properties of our implementation of ADFS as show below. You will need to provide 7SIGNAL with the Federation Service ID from the 3rd field below.



On the Organization tab, all of our enabled services will need to be reachable by way of the Organization URL so we need to make note of this and ensure any firewalls or other security measures are configured to allow traffic through to this server address.

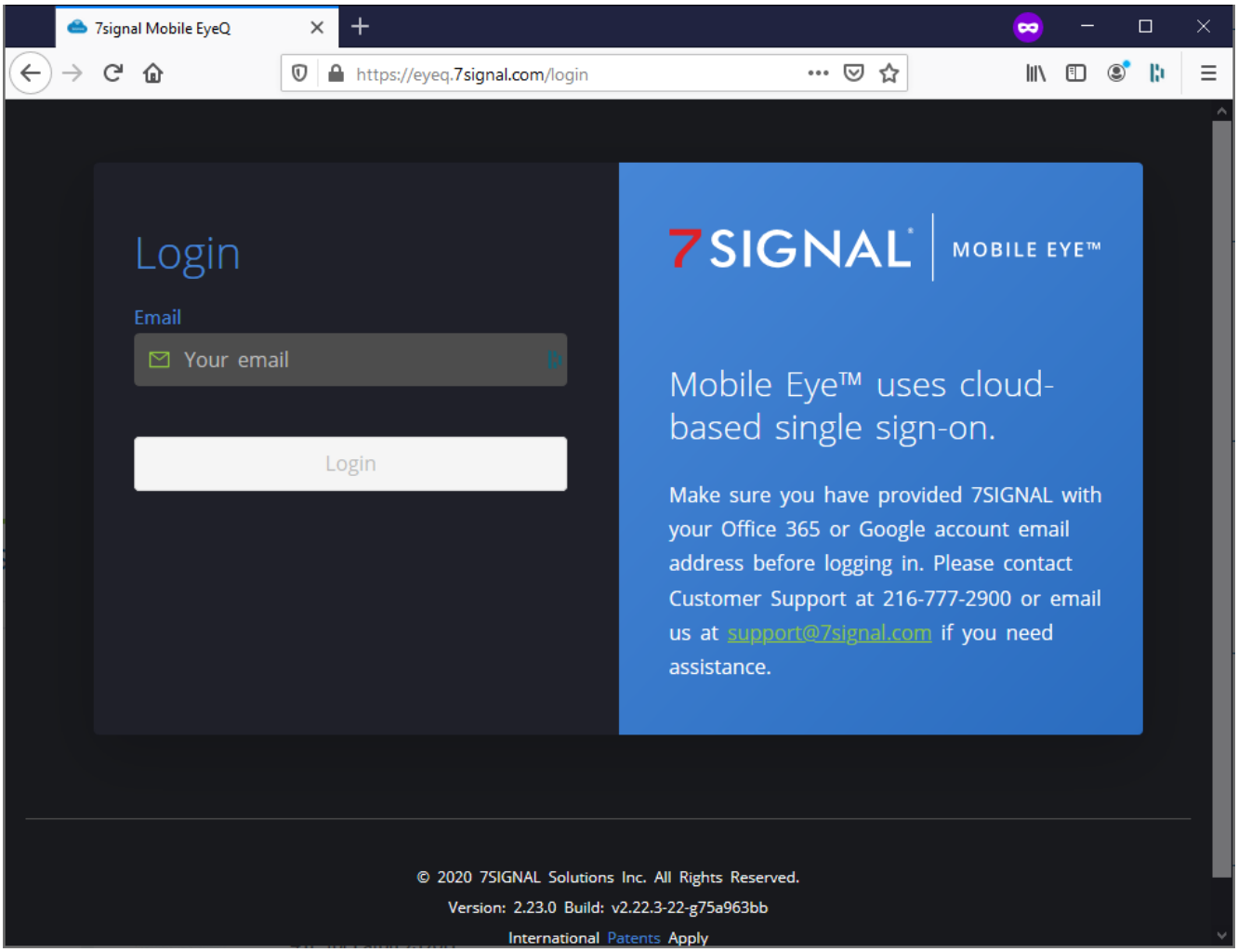


If we navigate to Service and then Endpoints in the AD FS Management utility, we can see that by default, the SAML 2.0 service is at the path /adfs/ls/. This path appended to the Organization URL from the previous page is another piece of information to be given to 7SIGNAL.

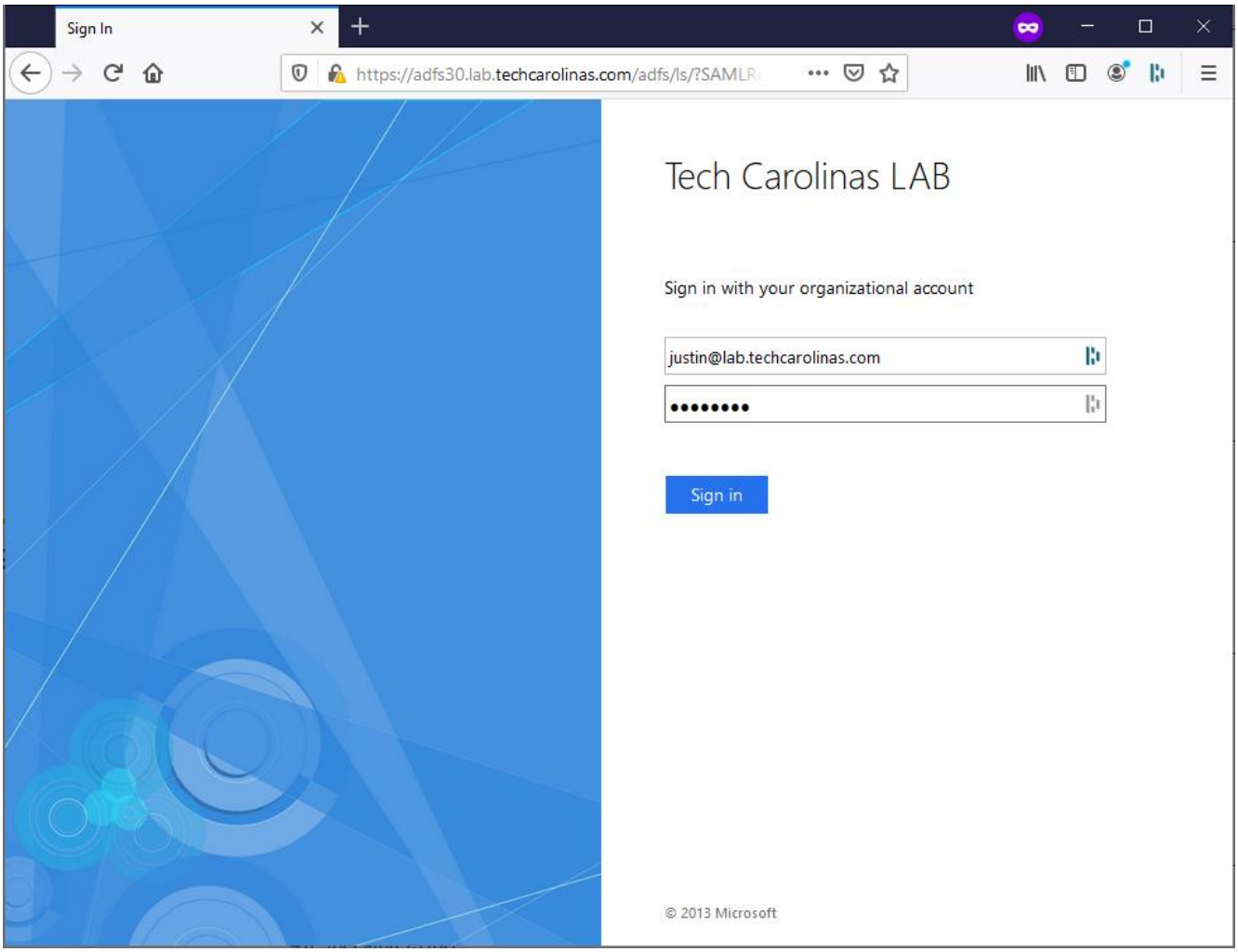


Testing the Services

Assuming both sides are configured at this point, we will begin to validate the solution. In this instance, we will be navigating to the login URL given by 7SIGNAL where we put in the email address of a user who has been configured for access to the Dashboard.



Clicking login will redirect us over to our AD FS site appending our SAML Request ID as part of the path. Here we login using our Active Directory User ID and credentials.



Upon successful authentication against Active Directory, you will be redirected back to the 7SIGNAL Mobile Eye dashboard with appropriate access and visibility as assigned.