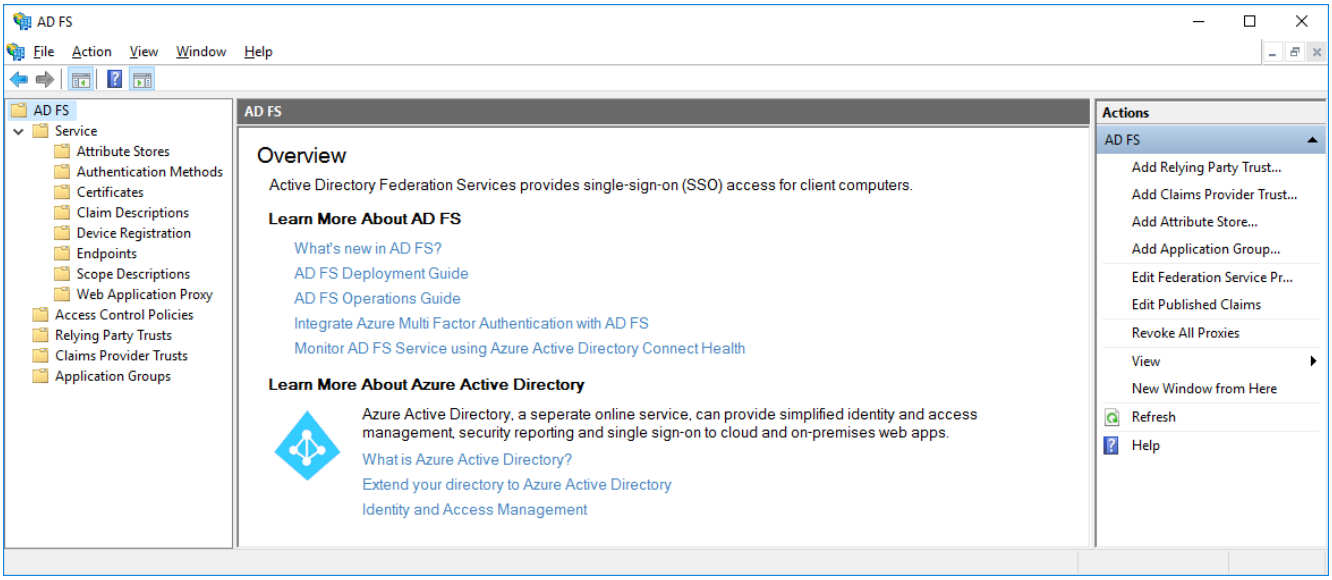
Microsoft ADFS 4.0 Configuration Guide for the 7SIGNAL Mobile Eye Dashboard

Microsoft ADFS 4.0 Configuration

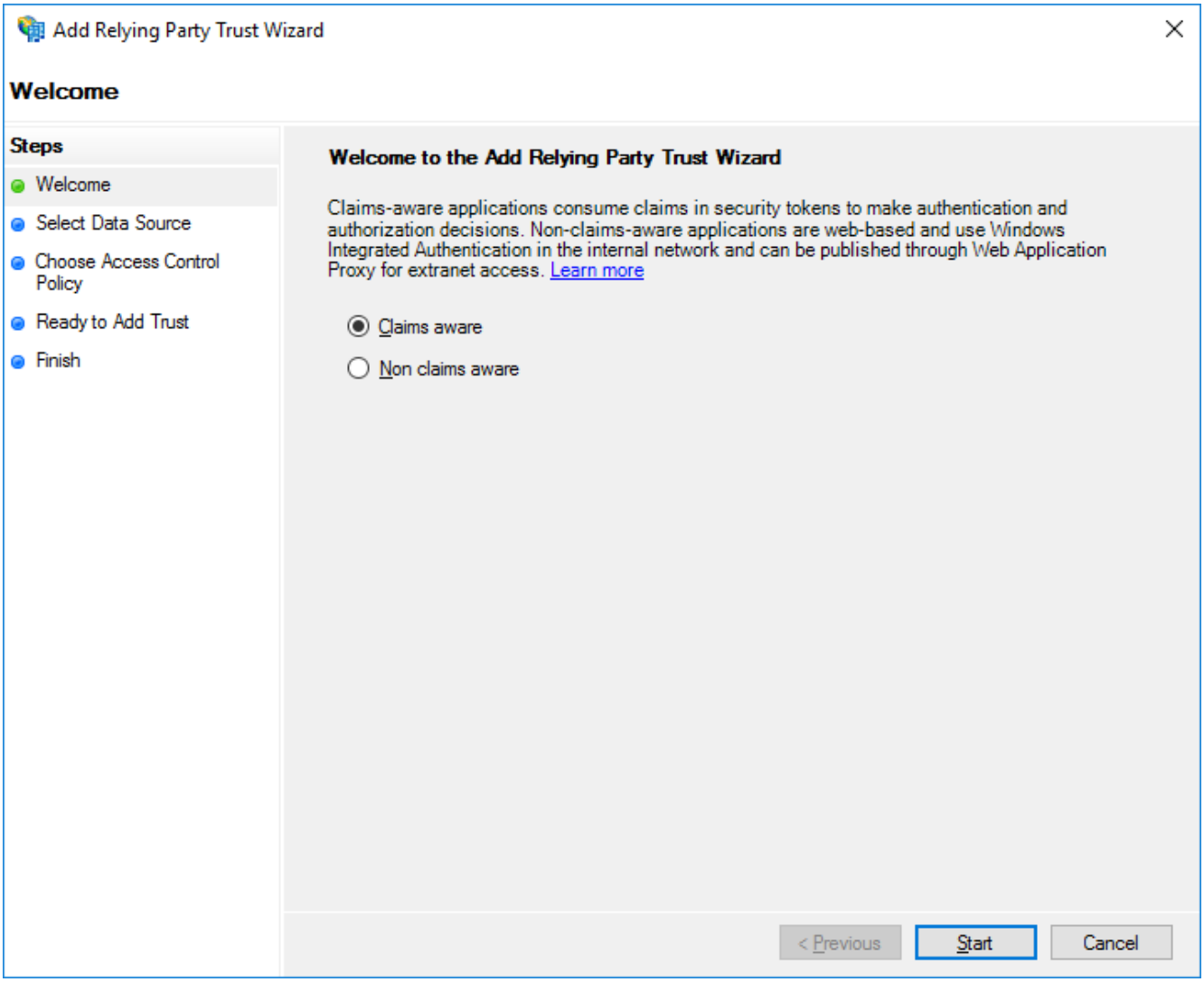
Relying Party Trust implementation for 7SIGNAL SSO

This configuration guide will walk through the steps to configure Active Directory Federation Services 4.0 (Windows Server 2016) 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 also implementing the AD FS services at version 4.0 on a different server running Window Server 2016. Other version combinations can exist and work together though configuration details may change.

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.

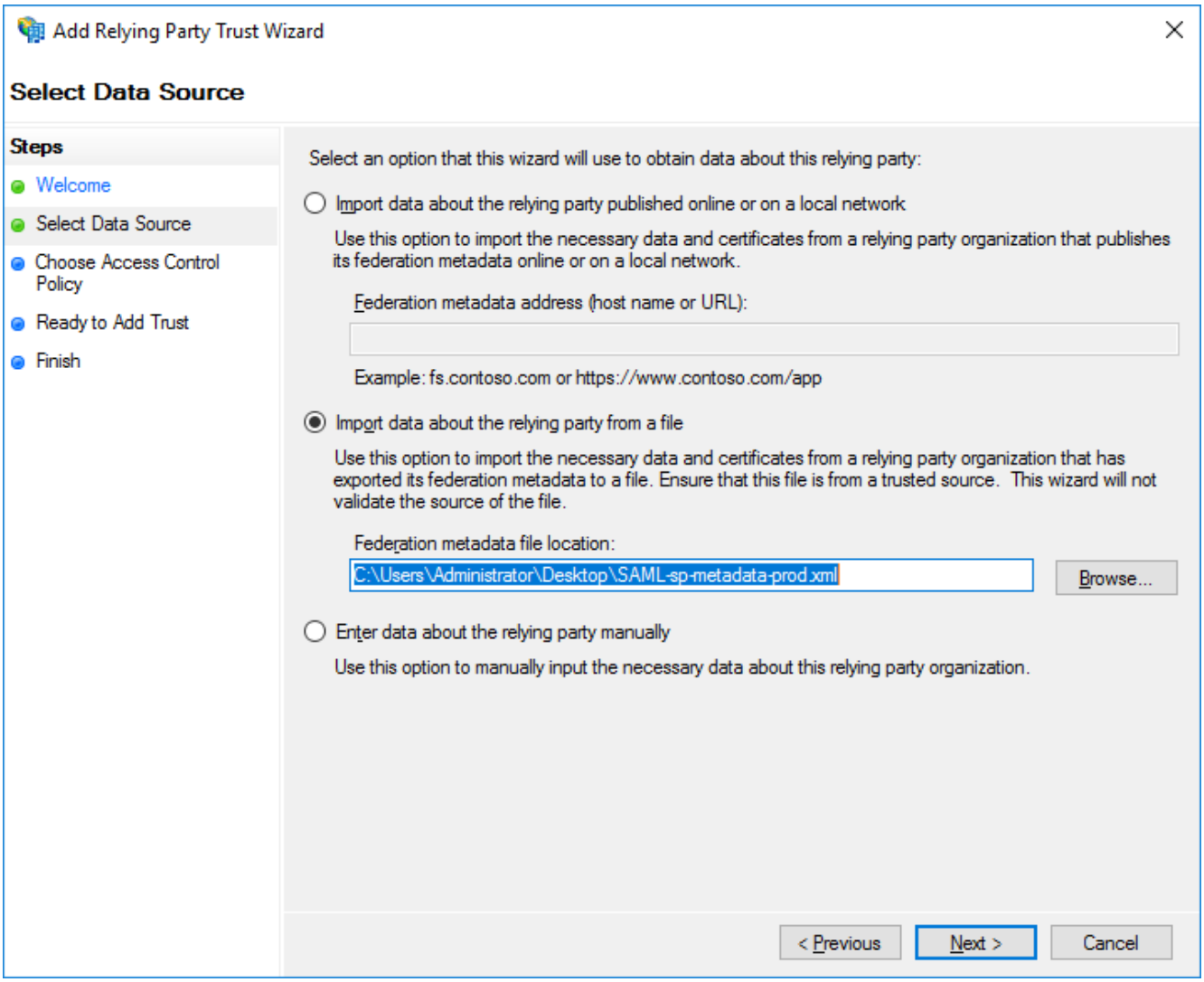


From here you will want to click “Add Relying Party Trust…” from the Actions menu which will kick off the following wizard.



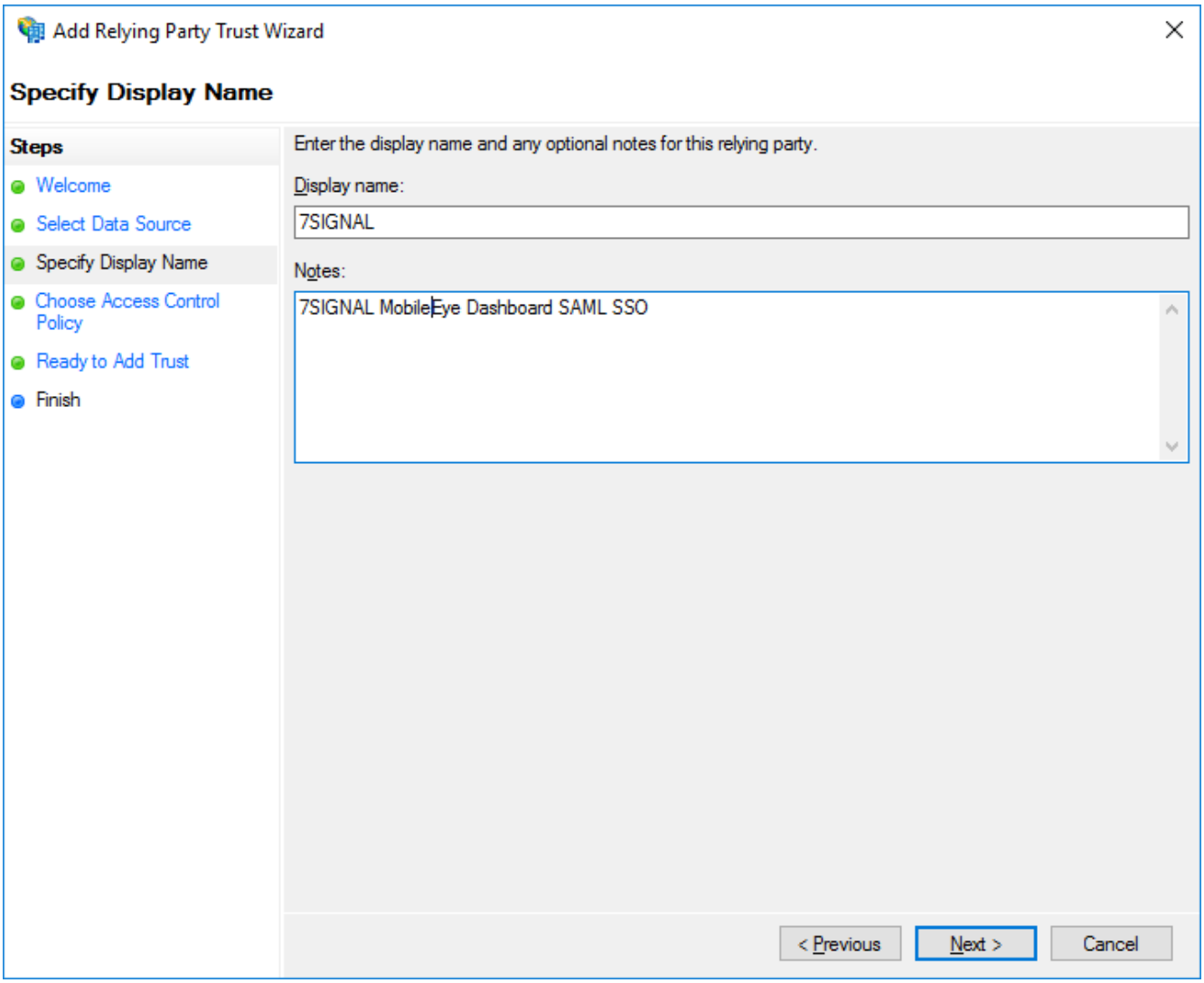
Leave the radio button for “Claims aware” selected and click the Start button to continue

For the Data Source selection, choose the middle option to “Import data about the relying party from a file” and then browse to the copy of the XML metadata file provided by 7SIGNAL.



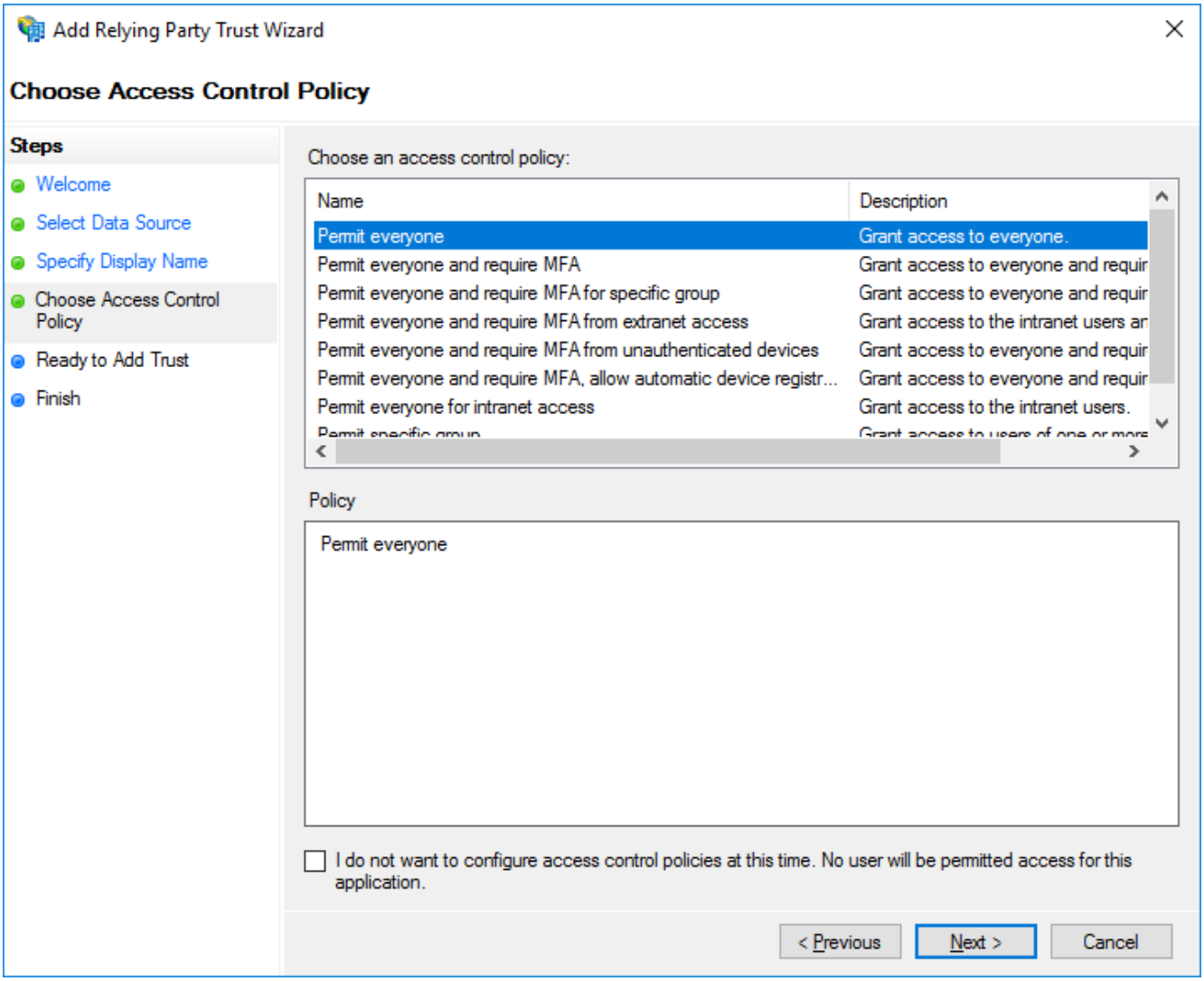
Click Next to continue

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



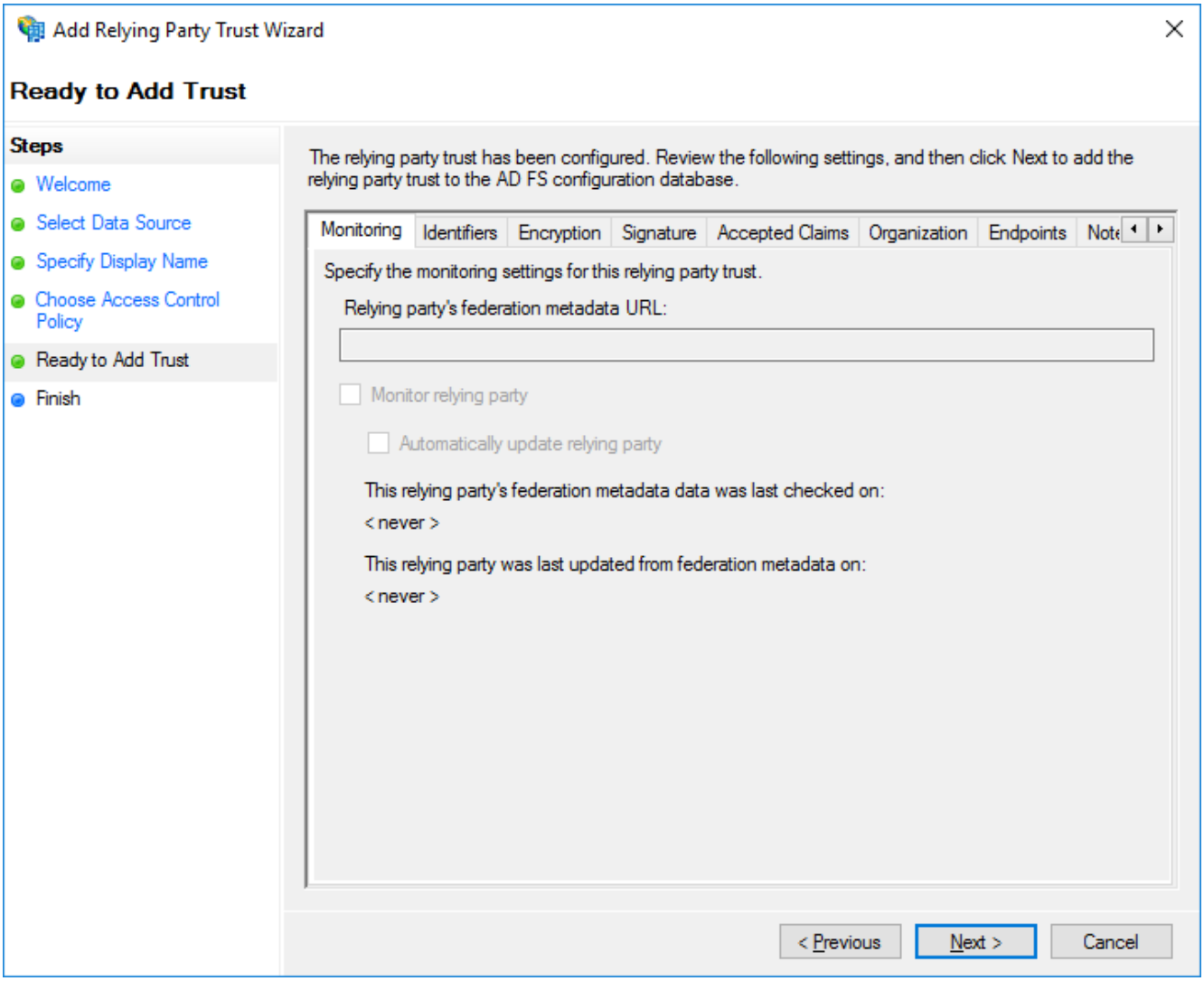
Click Next to continue

The Access Control Policy page is another way for you to decide how granular you want your services to be. For the purposes of this guide, we will choose the existing “Permit Everyone” policy from the list which allows any user in the Active Directory domain to access the relying party application we are defining.



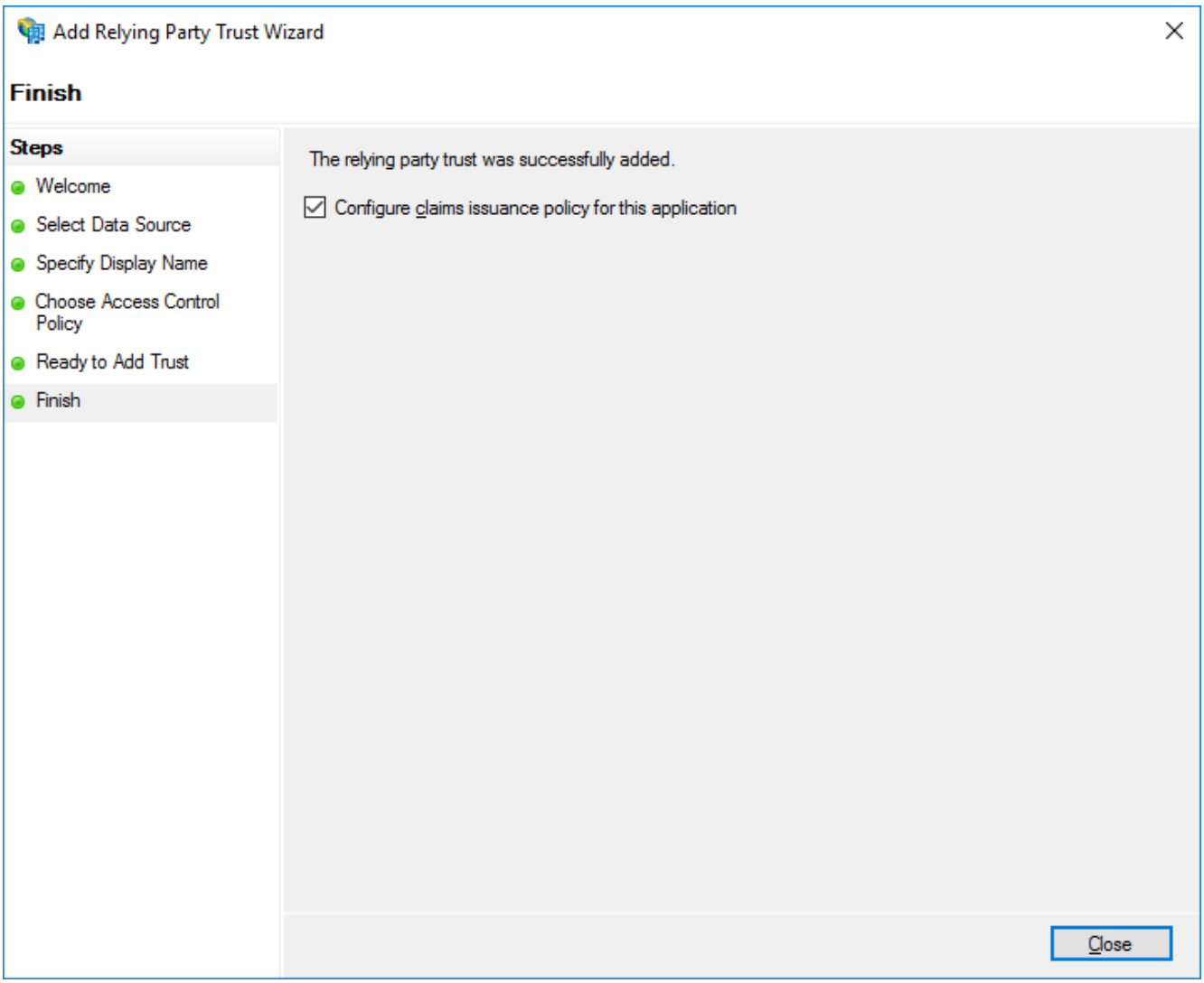
Click Next to continue

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. These will include imported certificates for encryption and signing of authentication requests, the relying party trust identifier URL, the SAML endpoint service URL and other details.



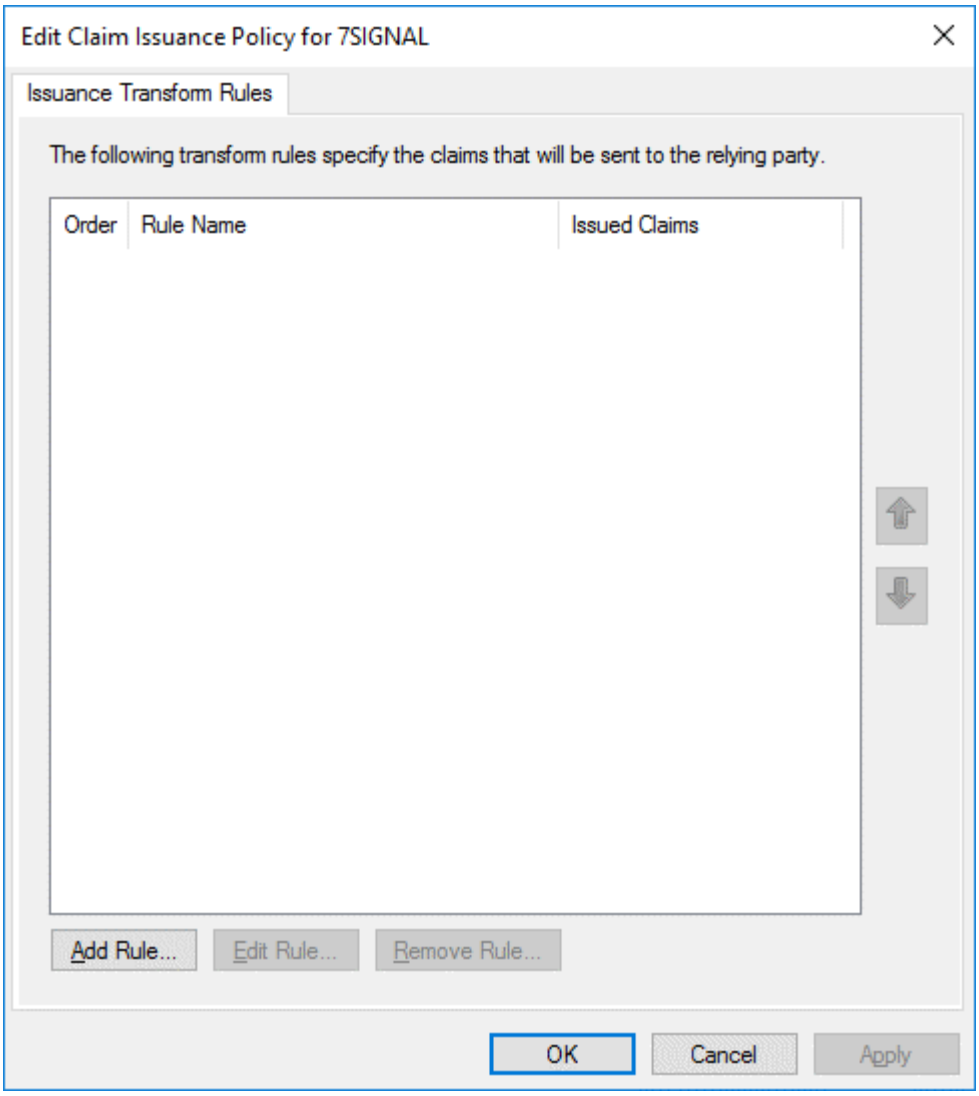
Click Next to continue

This completes adding the Relying Party Trust to our AD FS environment. By default, the Wizard will open the Claims Issuance Policy configuration.



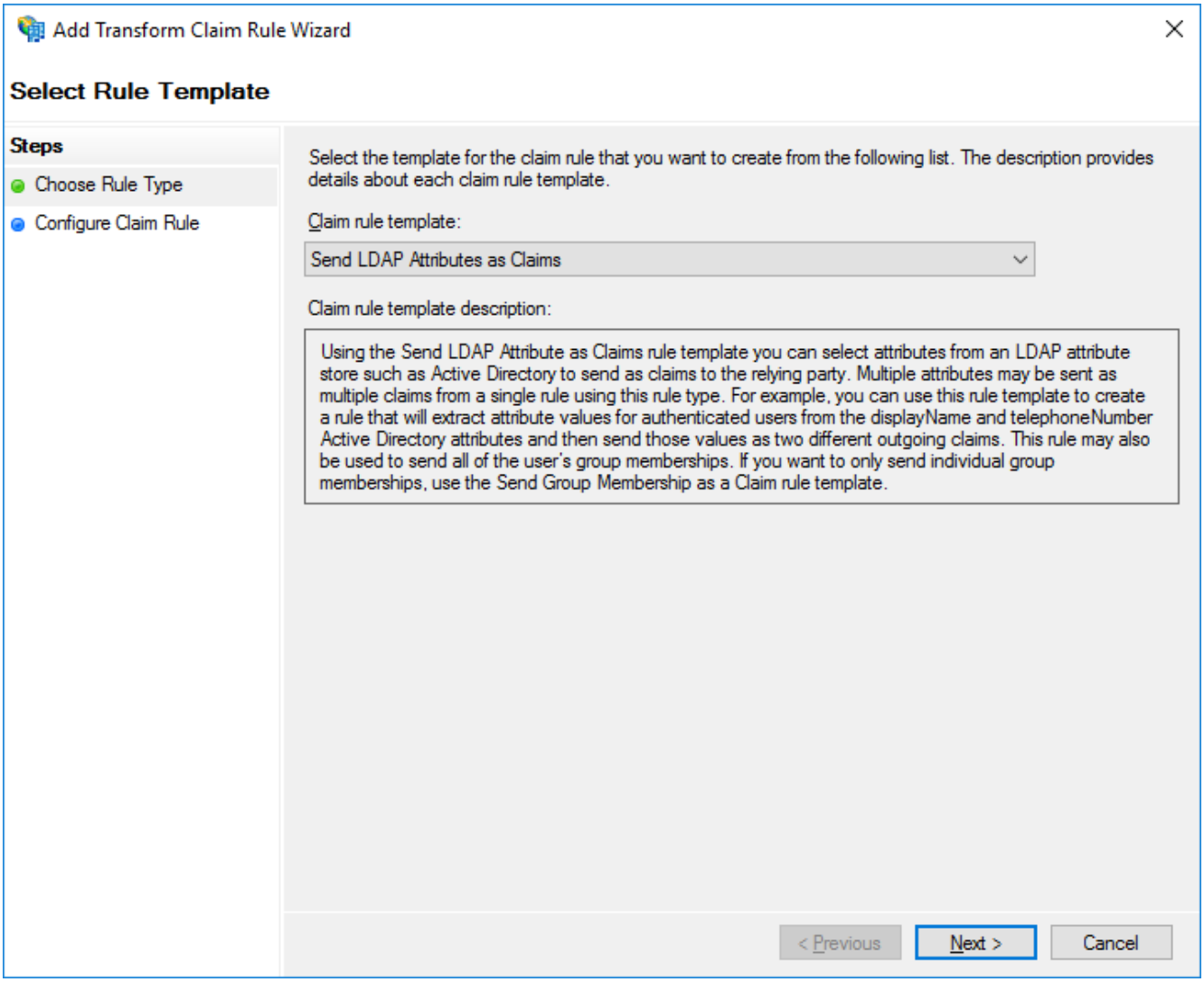
Click Close and this will launch the Claims Issuance Policy configuration and allow us to define our Claims Transform rule.

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 against AD FS.



Click the “Add Rule…” button to get started.

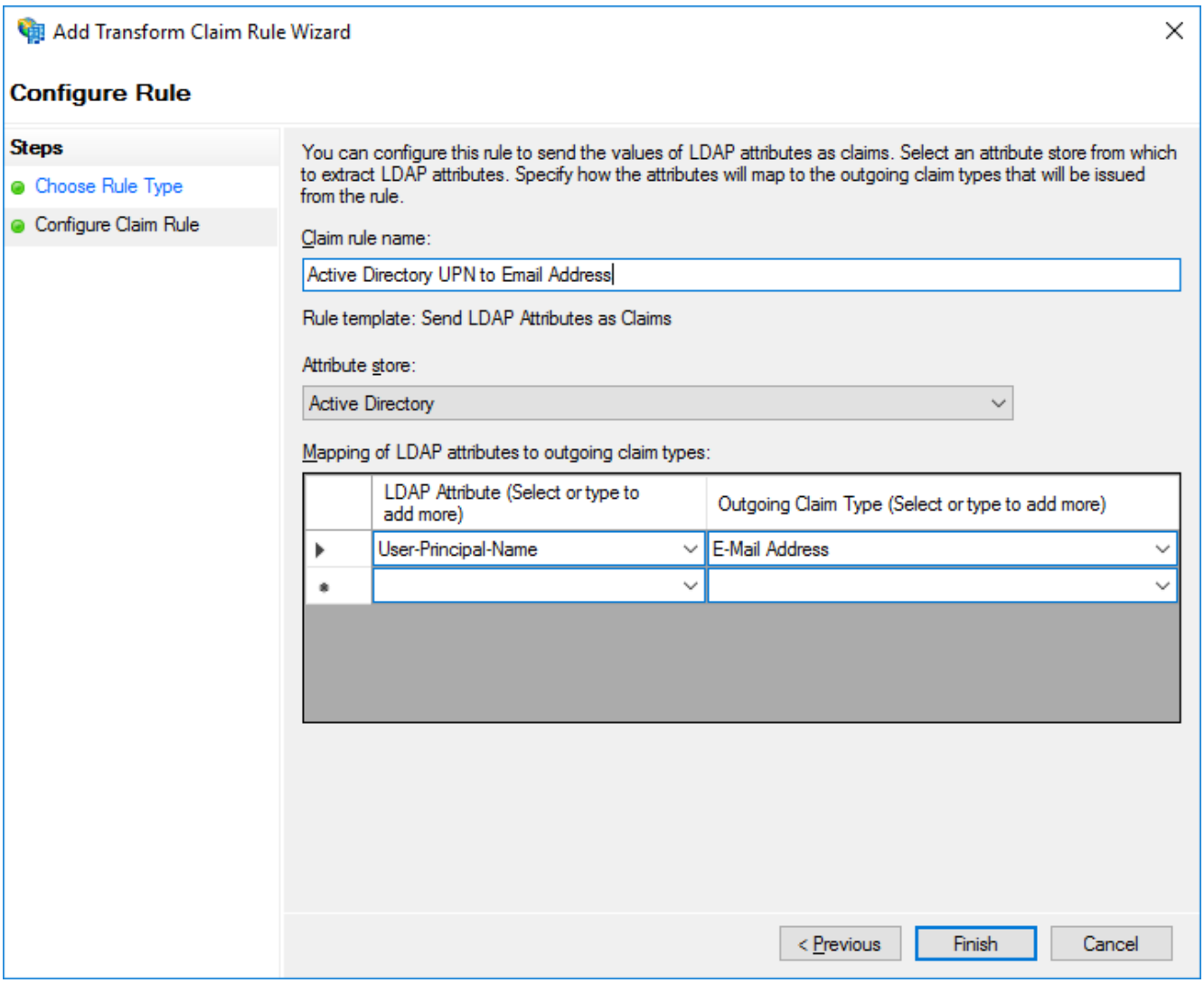
There are different templates you may choose from but for the purposes of this guide, we will assume LDAP user object Attributes will be used as 7SIGNAL looks for the user's email address to associate them to the proper details in the MobileEye dashboard.



Click Next to continue.

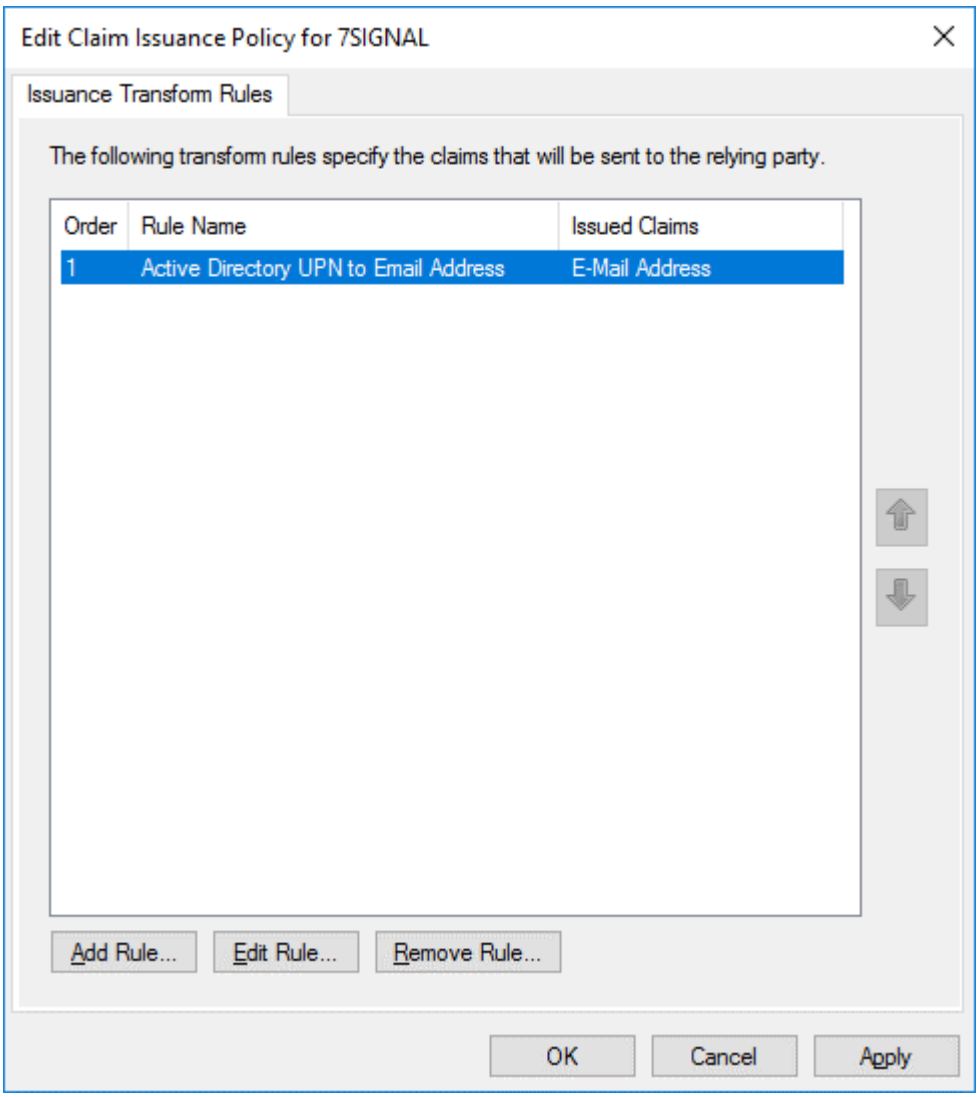
For the Claim Rule definition, you will provide a Rule name, select Active Directory as your LDAP attribute store, choose your LDAP Attribute and then the Outgoing Claim Type it will map to.

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.



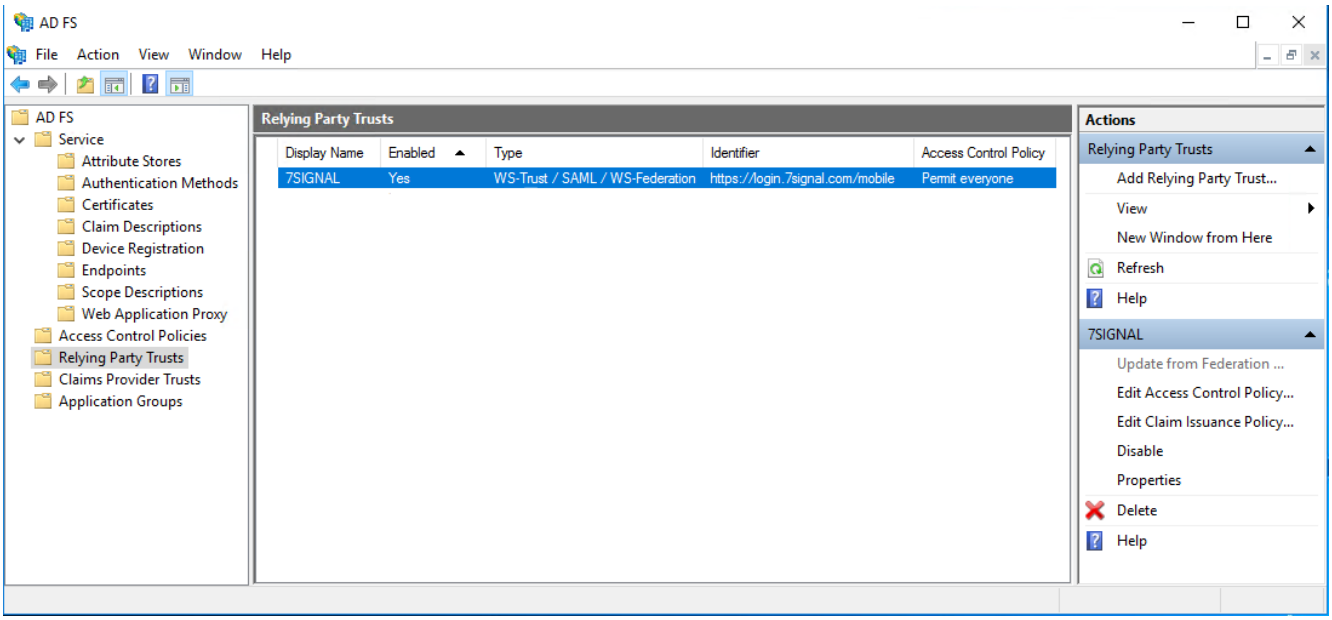
Click Finish since this is the only Claim we need to be passed to the MobileEye dashboard.

This takes you back to the overall Claim Issuance Policy screen showing your one rule you just added.



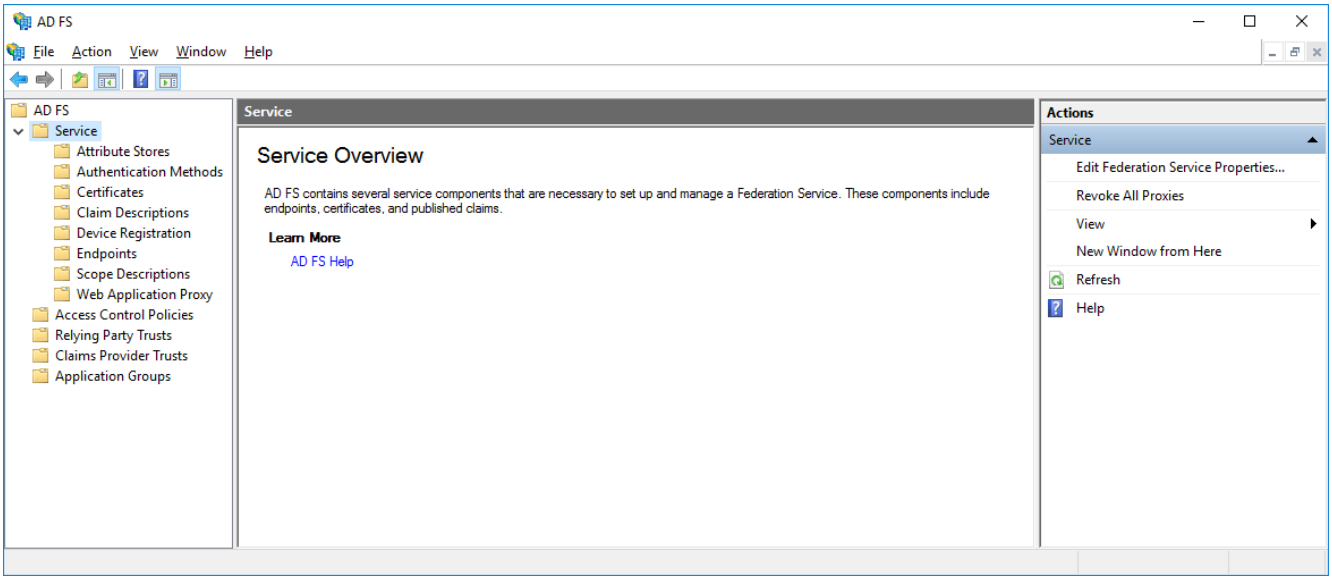
Click OK to close this Claim Issuance Policy window out.

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

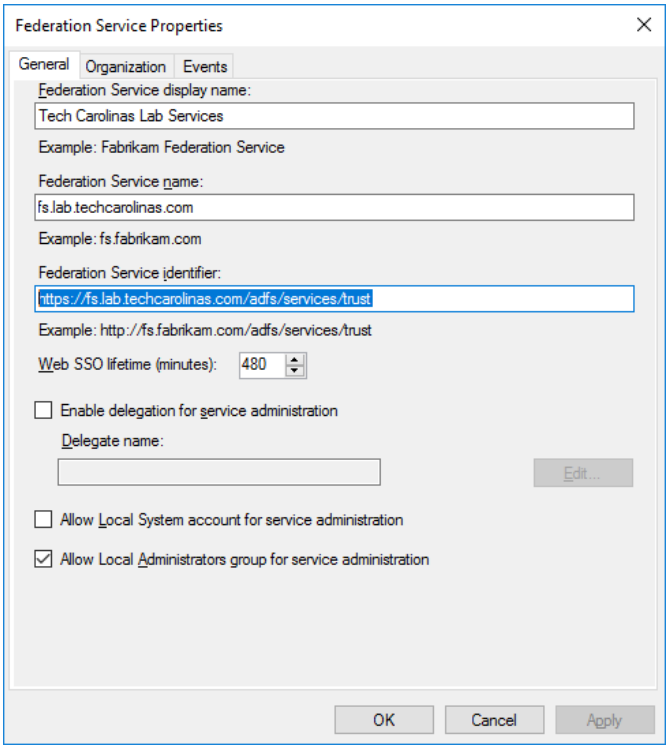


Gathering our AD FS details for 7SIGNAL to configure their side

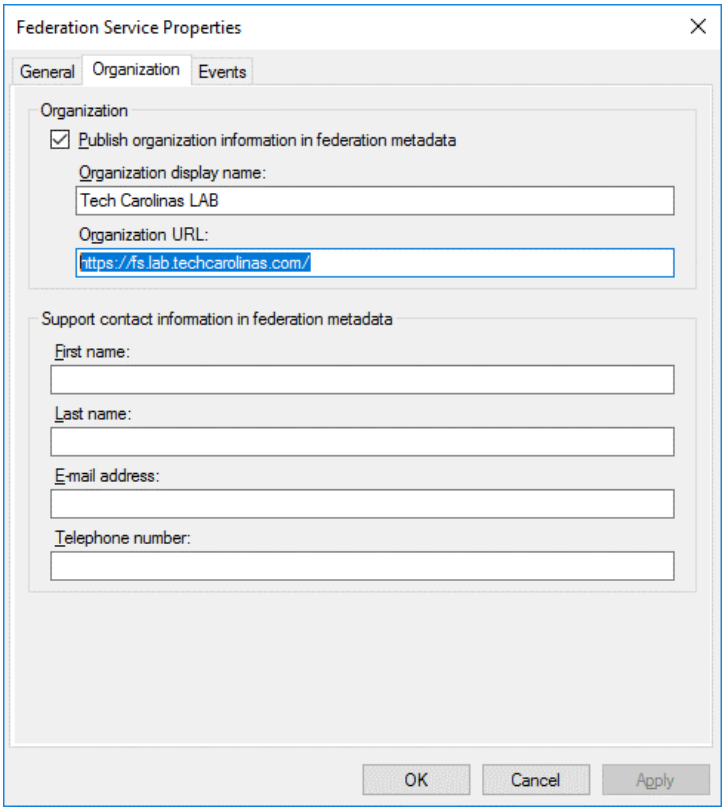
In order to configure and/or retrieve the details of our AD FS implementation, we navigate to the Service folder in the AD FS Management console and choose “Edit Federation Service Properties” from the Actions menu or by right-clicking the Service folder.



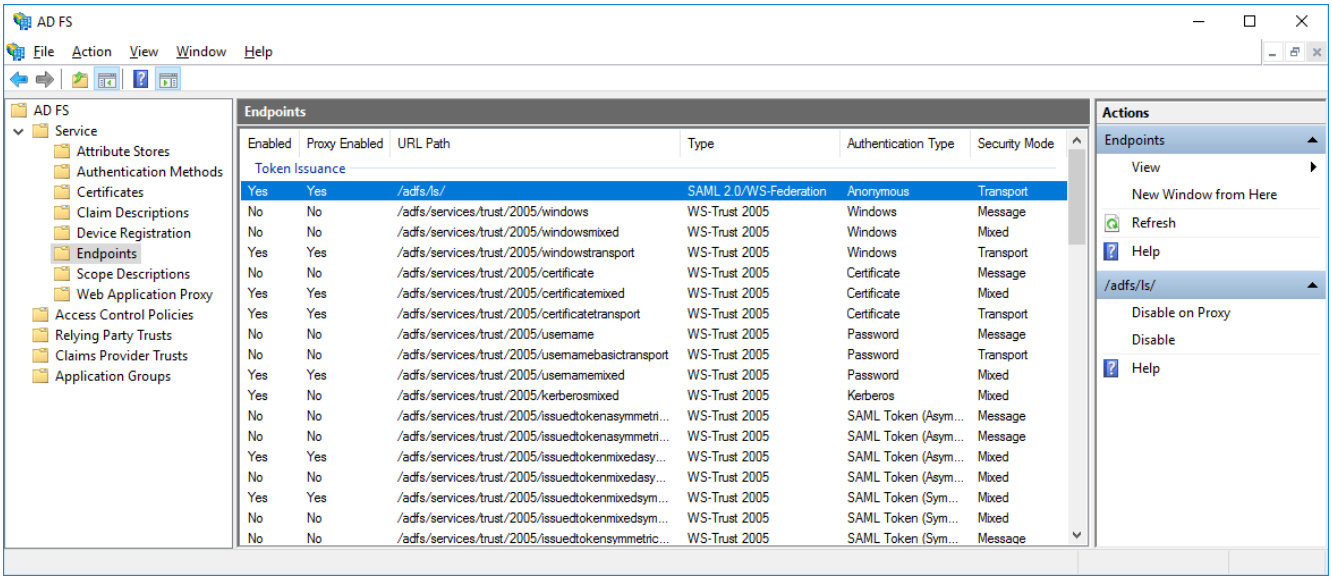
This brings up the properties of our implementation of ADFS as show below. You will need to provide 7SIGNAL with the Federation Service ID from the 3rd field below.



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.



In this example, our SAML 2.0 Service Endpoint URL is:

https://fs.lab.techcarolinas.com/adfs/ls/

And from the previous section, the Federation Service Identifier URL is:

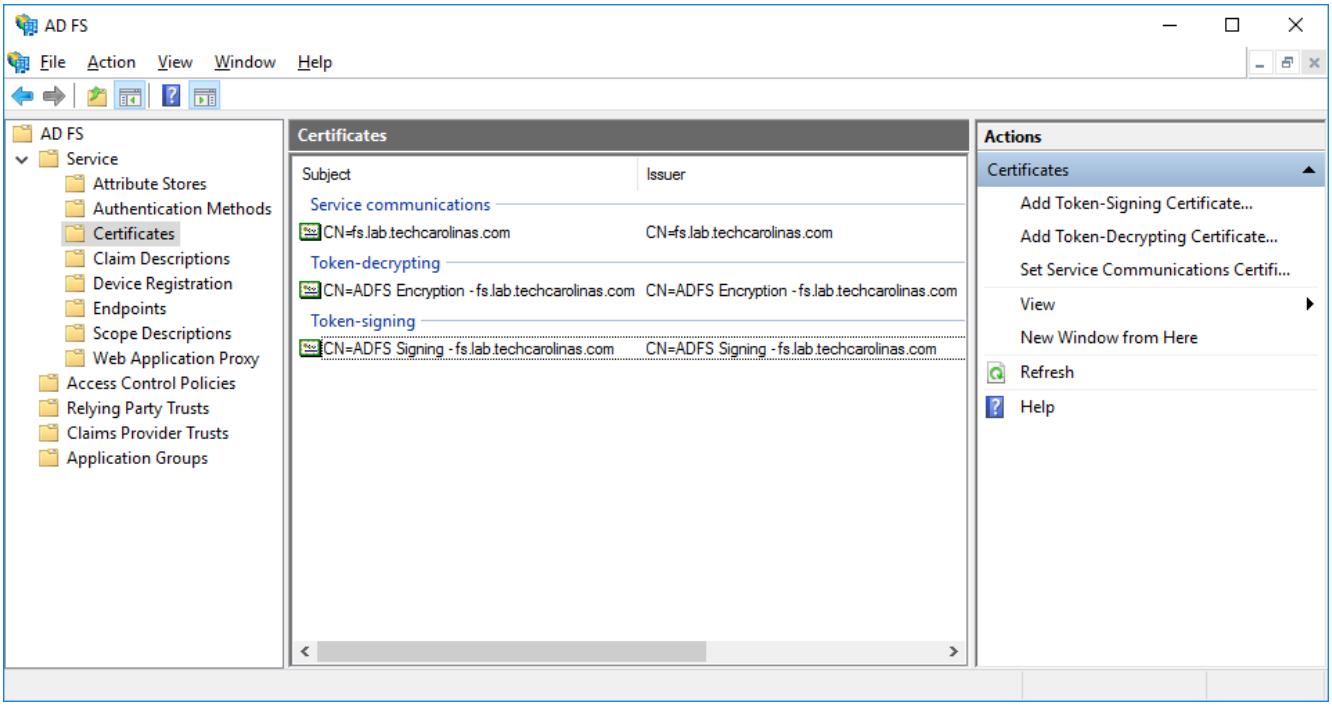
https://fs.lab.techcarolinas.com/adfs/services/trust/

Lastly, we will also need to provide 7SIGNAL with our ADFS Signature certificate as covered in the next section. These 3 pieces of information will be used by them to setup our SAML SSO capabilities for the MobileEye Dashboard.

Certificates

Since we will be leveraging TLS certificates for encrypting and signing communications between the systems, we also need to provide 7SIGNAL with the appropriate public certificate for our AD FS services.

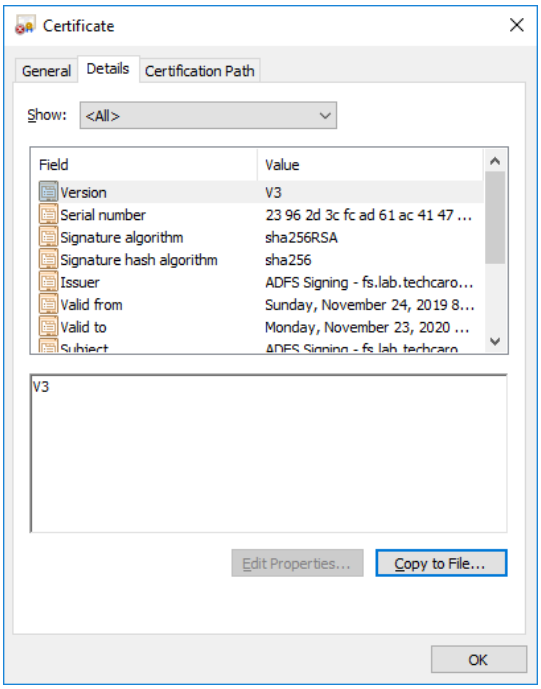
Although we only presented AD FS with a single self-signed certificate during setup, it assigned that for overall Service Communications and then created 2 more certificates for use in other functions as shown below.



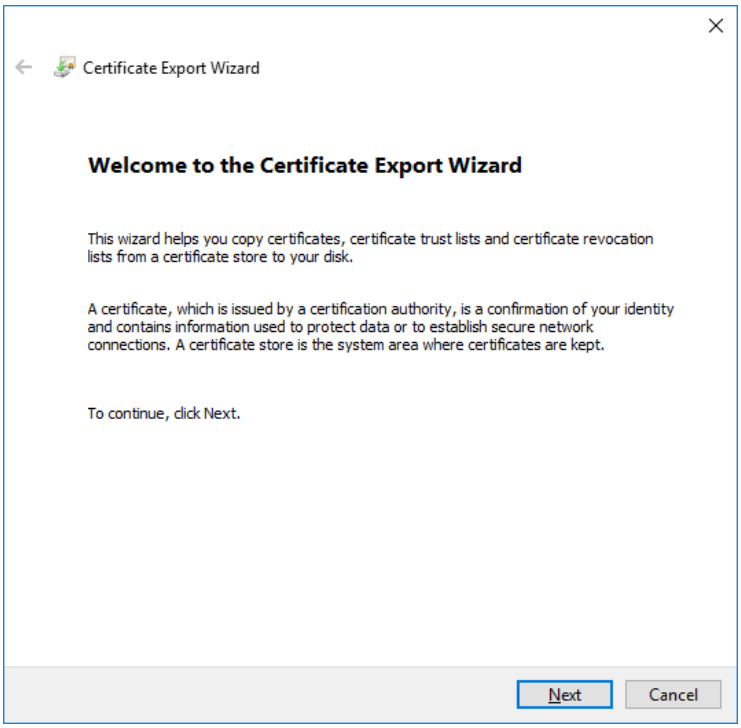
Since we will be using the signing certificate in sending our Claim back to the 7SIGNAL system, we need to use the Certificate Export Wizard to give 7SIGNAL a copy of the public certificate file.

You can choose to View the Certificate by selecting it in the preceding screenshot.

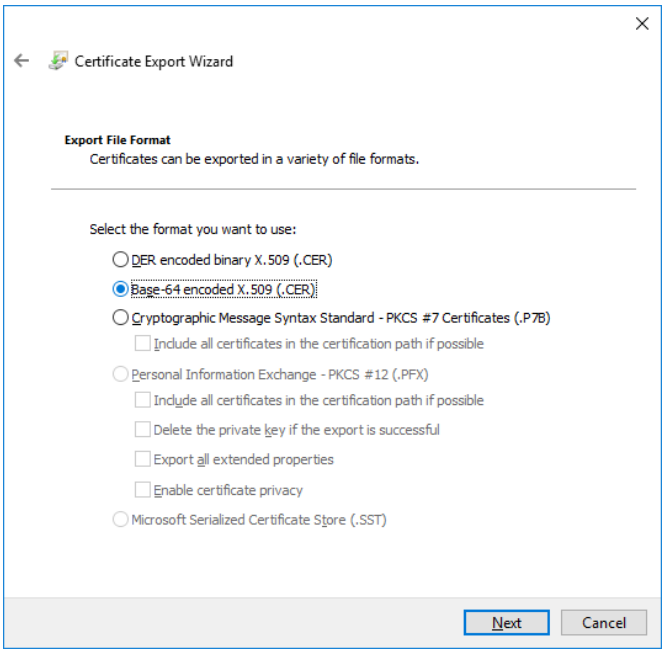
From there, you follow the standard practice on the Certificate to “Copy to File…” from the Details tab.



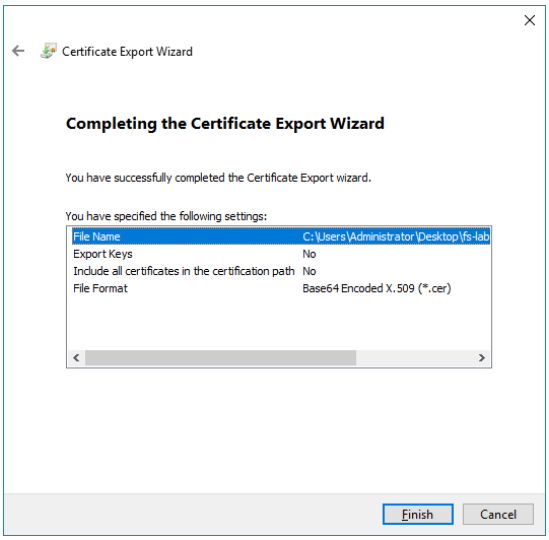
Walk through the Certificate Export Wizard

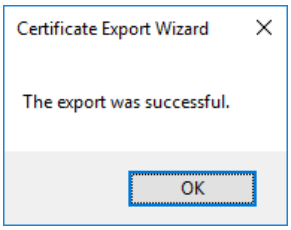

Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel

Choose the ‘Base-64 encoded X.509 (.CER)’ file format as shown below.



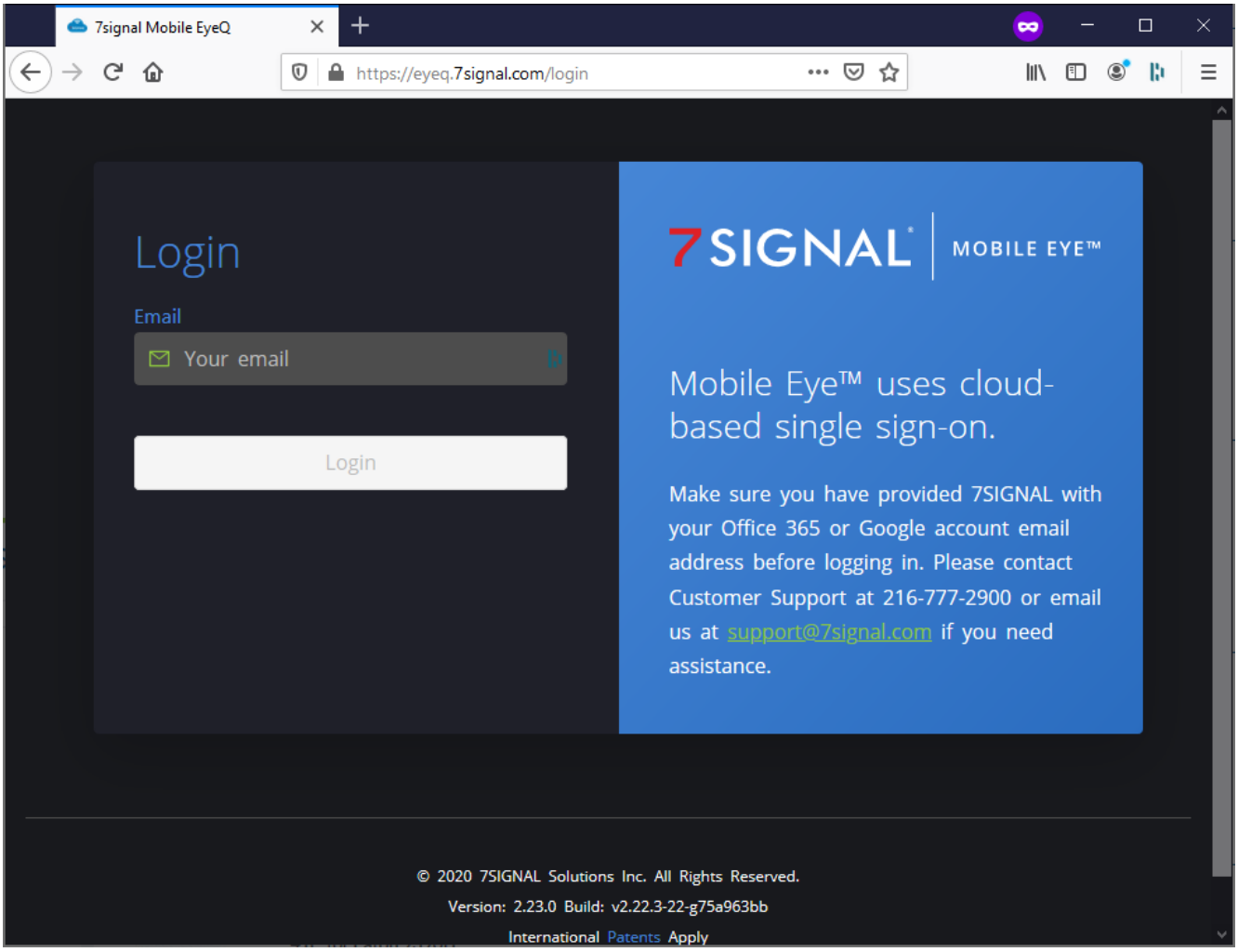
Browse to a path on the machine and give the file a name.



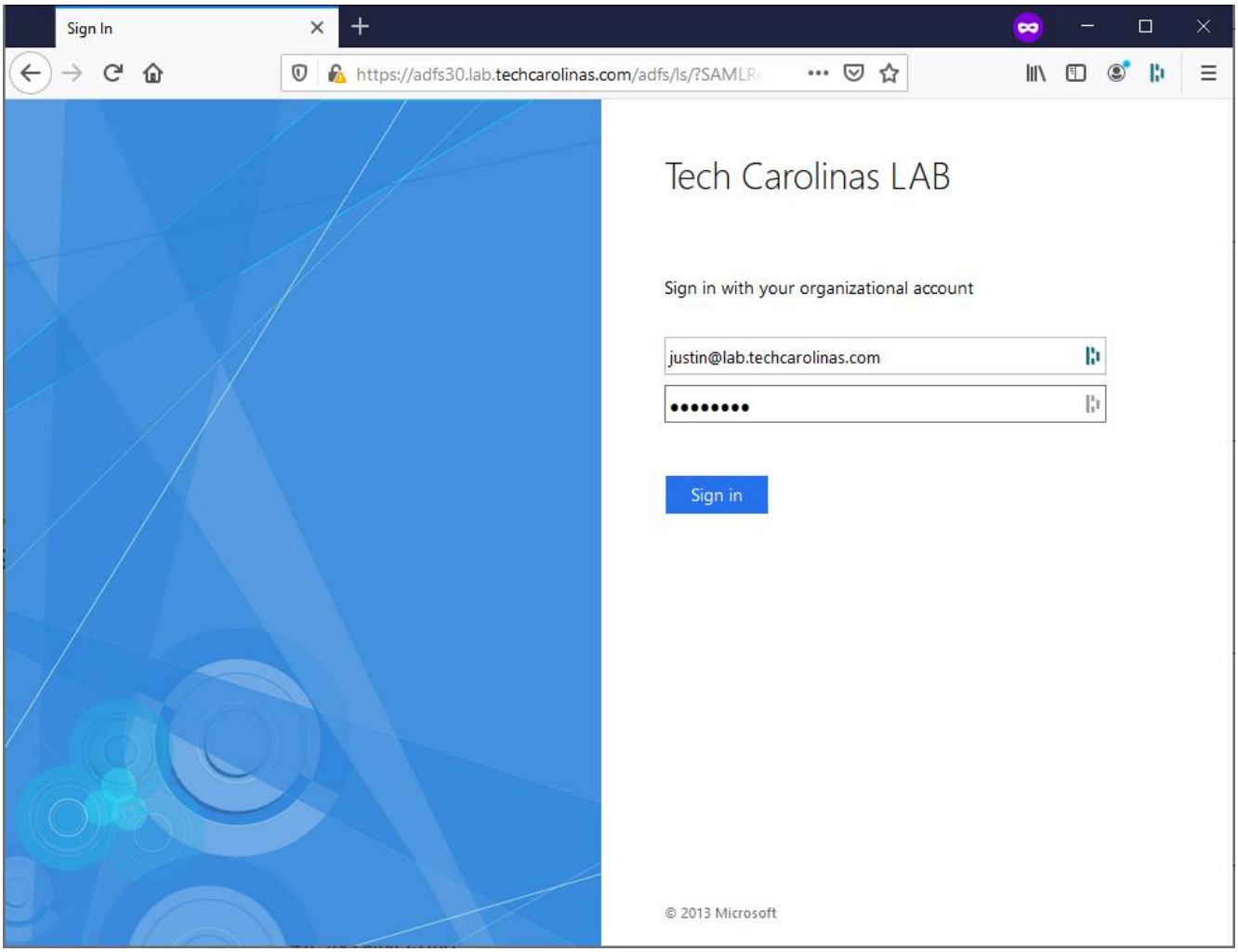


Testing the Services

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.