Nimonik Documentation for Single Sign On (SSO)

Single Sign-On

Nimonik supports Single Sign-On (SSO), a process that allows users to authenticate themselves against an external Identity Provider (IDP) rather than obtaining and using a separate username and password handled by Nimonik.

Under the SSO setup, Nimonik can work as a Service Provider (SP) through SAML (Security Assertion Markup Language) allowing user to provide Single Sign-On (SSO) services for the enterprise.

We are using ADFS Identity Provider (IDP) which will handle the sign-in process and will eventually provide the user details to Nimonik Application. User's email will be considered as the unique identifier for the application. Also, the application does not store passwords.

The IDP response will be encrypted by the public certificate provided by the Nimonik and decrypted from the private key stored in the application.

Prerequisites

1. A windows instance to install AD (tested on Windows Server 2016).
2. Active Directory installed on the server. Link to install the Active Directory in the server: https://blogs.technet.microsoft.com/canitpro/2017/02/22/step-by-step-setting-up-active-directory-in-windows-server-2016/
3. Active Directory Federation Services (ADFS) installed in the server. Here's the link to setup the ADFS: https://www.virtuallyboring.com/how-to-setup-microsoft-active-directory-federation-services-adfs/

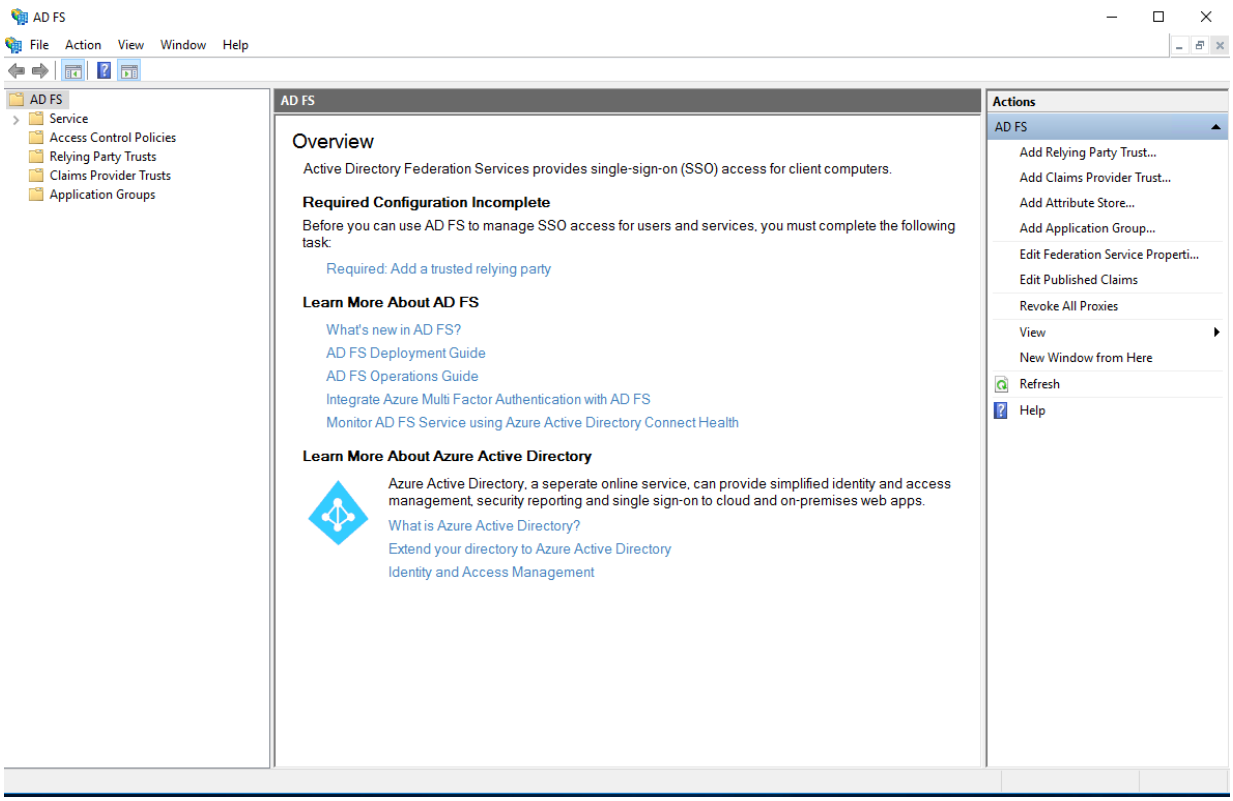
ADFS Configuration

Following is the step-by-step guide to configure ADFS in the windows instance:

Step 1: ADFS Basic Configuration

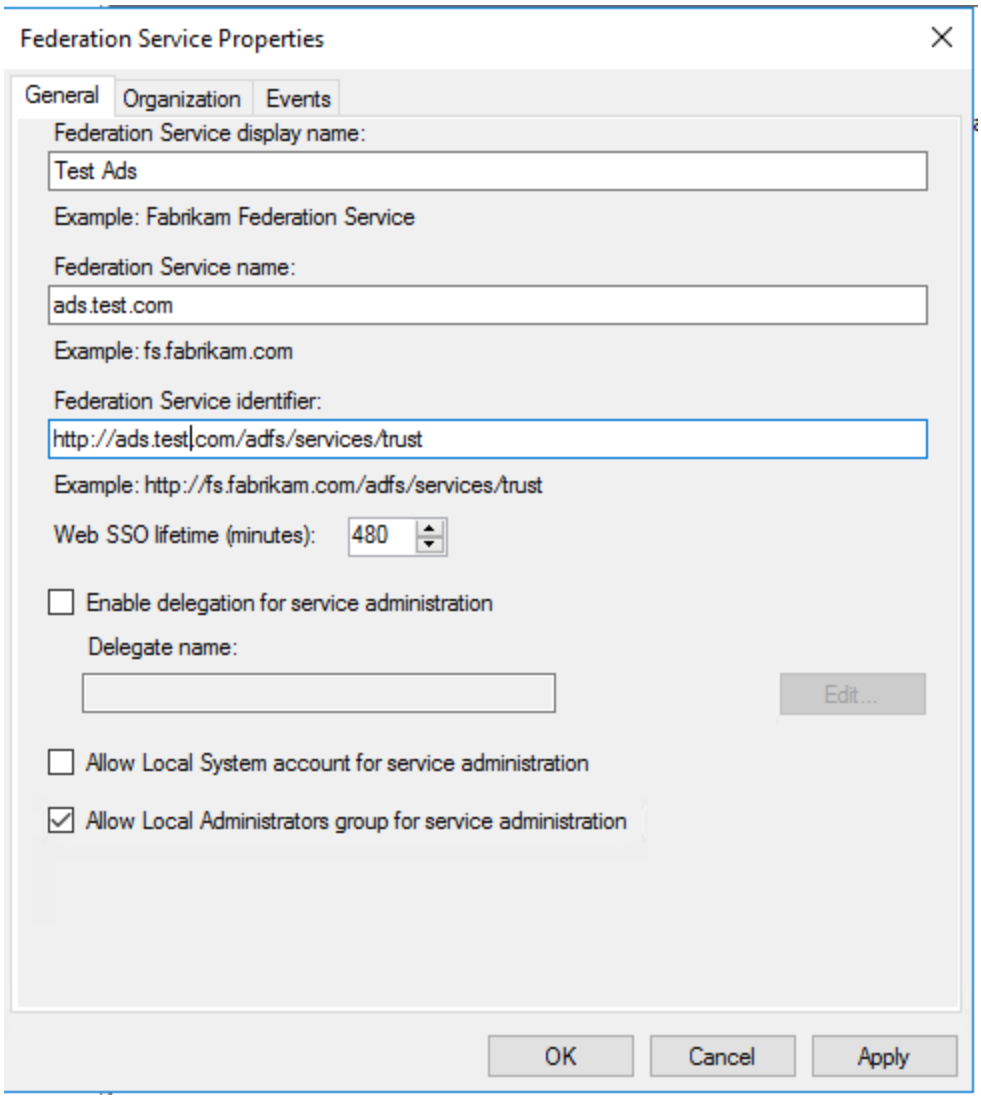
Open the ADFS Management through Start→Administrative Tools→ADFS Management.

1. Right-click on **Service** from the left tree-view and click on **Edit Federation Service** Properties.

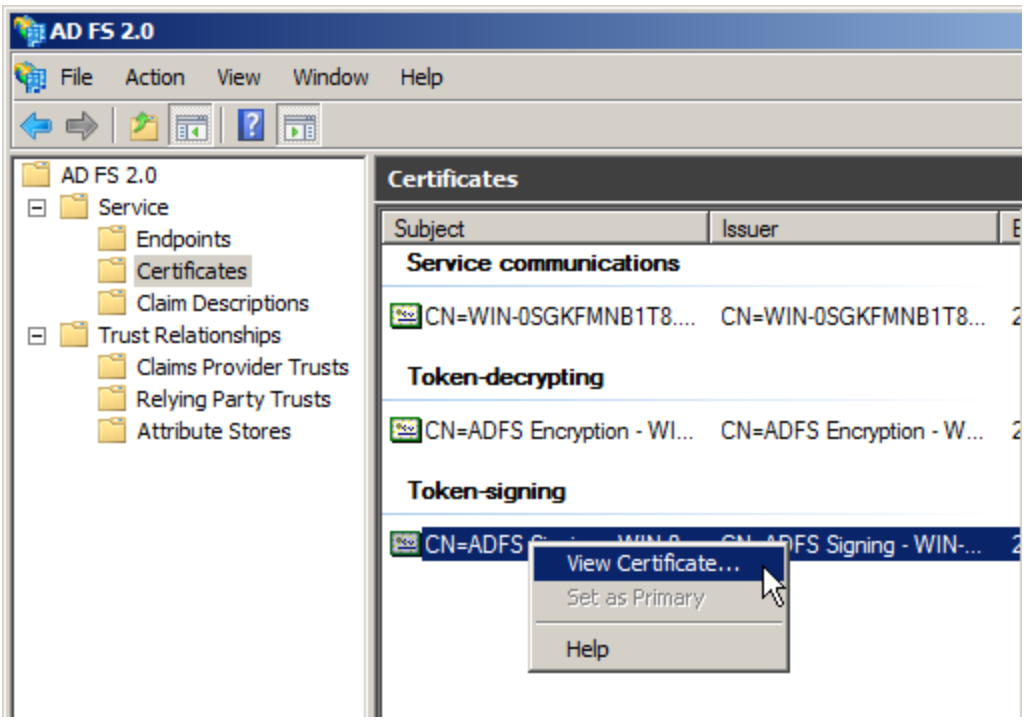


2. Go to the **General** tab. The **Federation Service Identifier** (http://ads.test.com/adfs/services/trust) is the identity provider's URL. This identifier will be required by Nimonik. Please check screenshot added in below point.

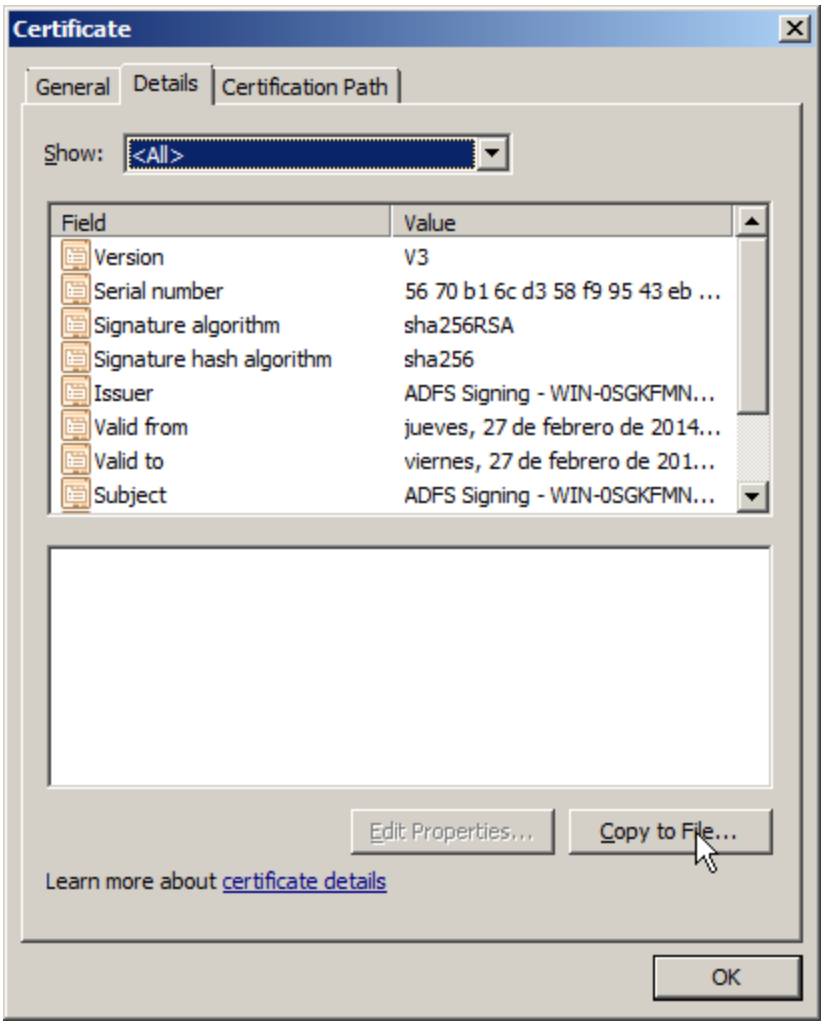
3. On the **General** tab, check the other values to confirm that they match the DNS settings for your server and click **OK**.



4. Click on the Certificates Entry from the left tree-view, right-click on Token-Signing certificate and then click on View Certificate.



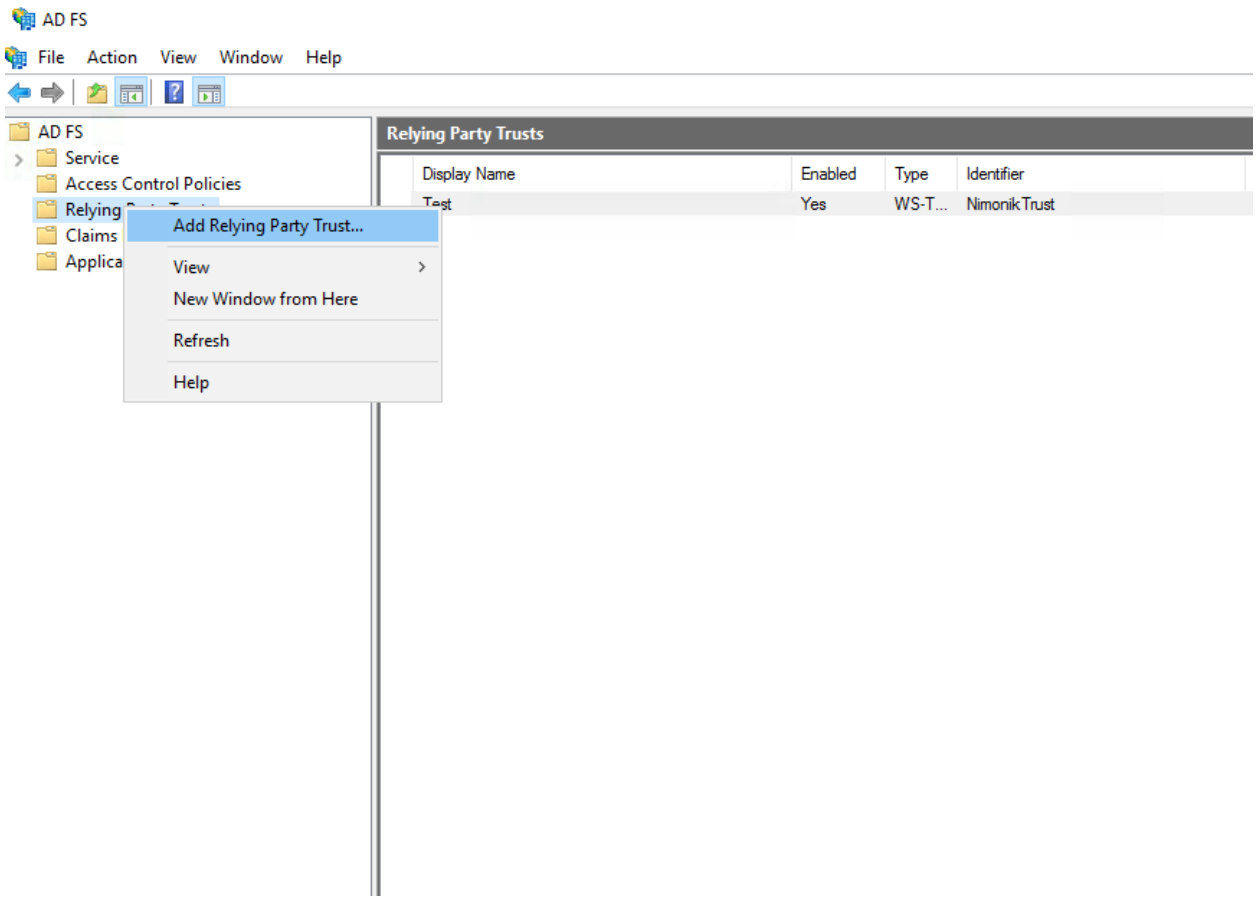
5. In the details tab,
    a. Click on “Copy to File” to launch the Certificate Export Wizard.
    b. Click on Next, select DER encoded binary X.509 (.cer) format, and then click Next.
    c. Select the directory where you want to save the certificate and click on Finish.



6. The exported certificate will be required by Nimonik.

Step 2: ADFS Relying Party Trust Configuration

1. Select **Relying Party Trusts** from the left tree-view under the **Trust Relationships**, right-click on the **Relying Party Trusts** and click on **Add Relying Party Trust**. The wizard launches.



2. Select claims aware and click on **Start**.

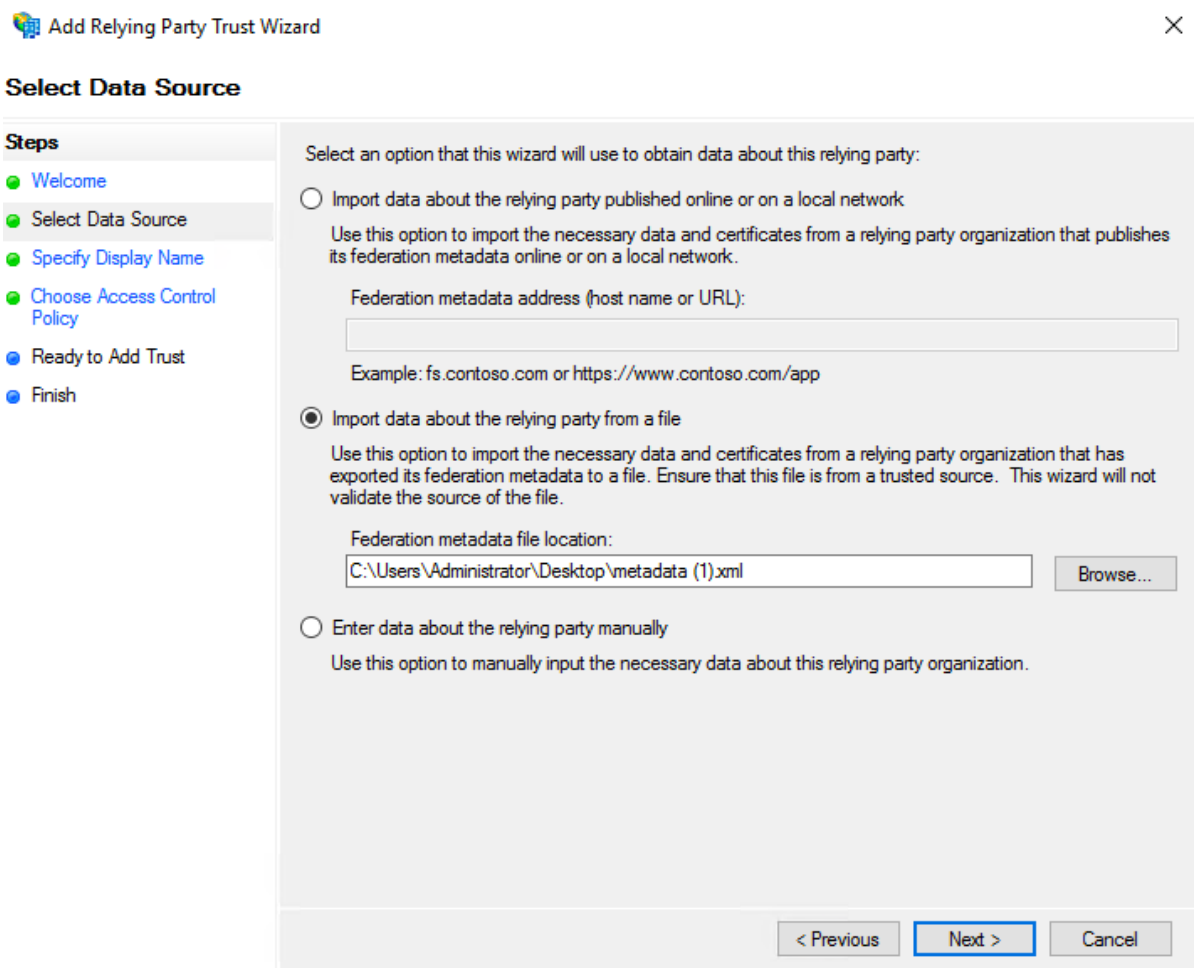
3. There are two ways for adding Relying Party Trust.

    a. One is using *“Import data about the relying party from a file”.*
    b. Other is *“Enter data about the relying party manually”.*

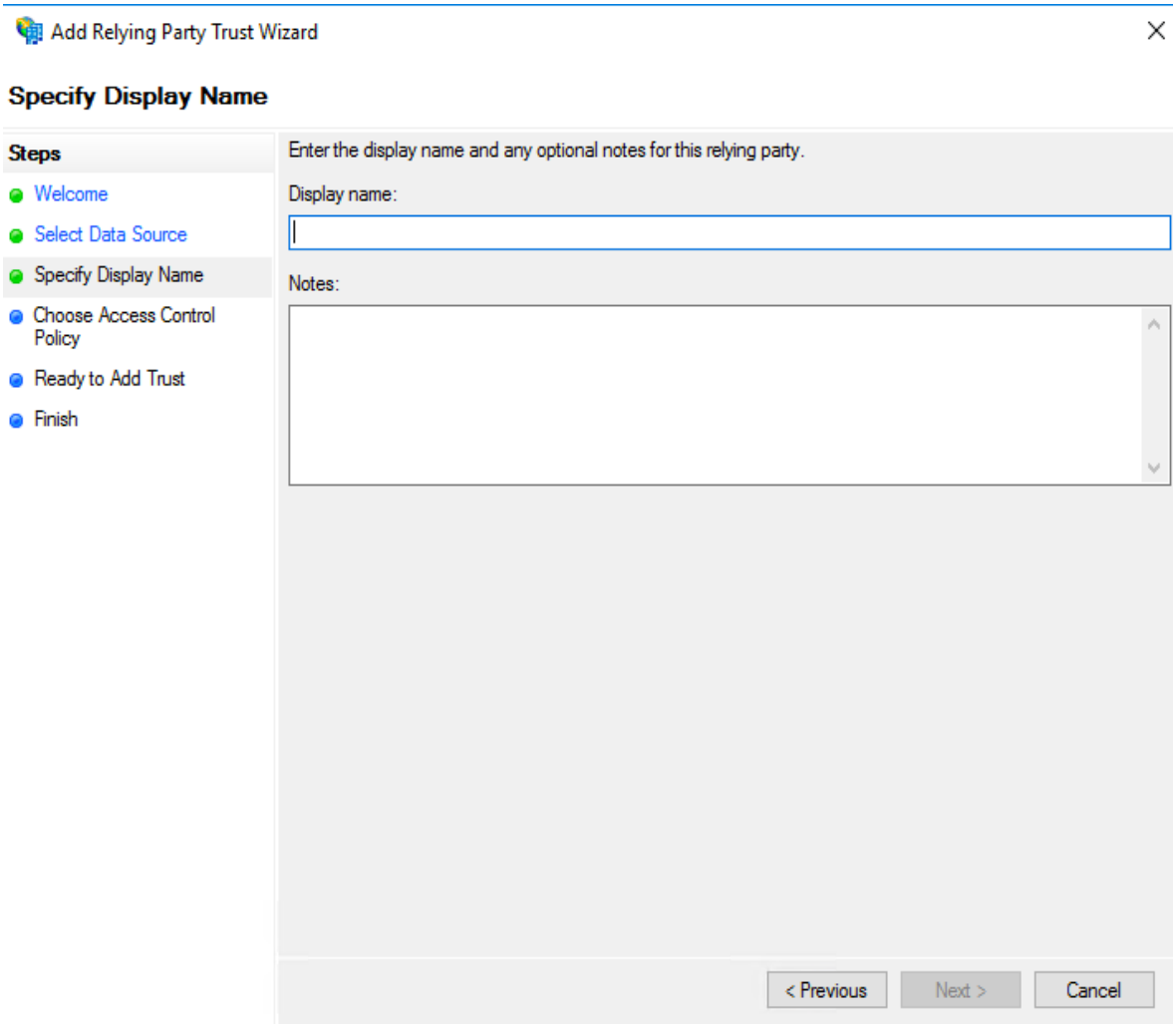
a. Import data about the relying party from a file

a.1 Select “Import data about the relying party from a file” and click **Next**.

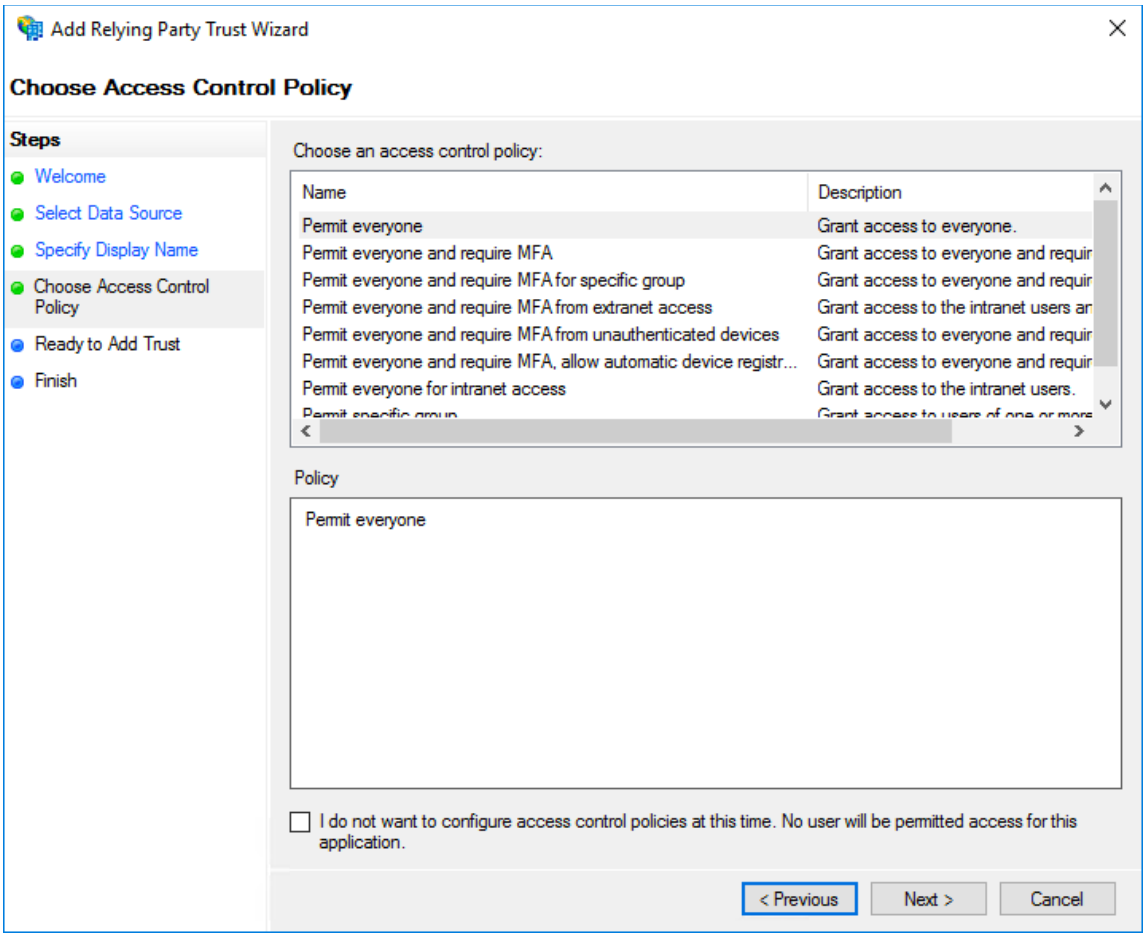
a.2 This file will be provided by Nimonik. Locate the path of the file and click **Next.**



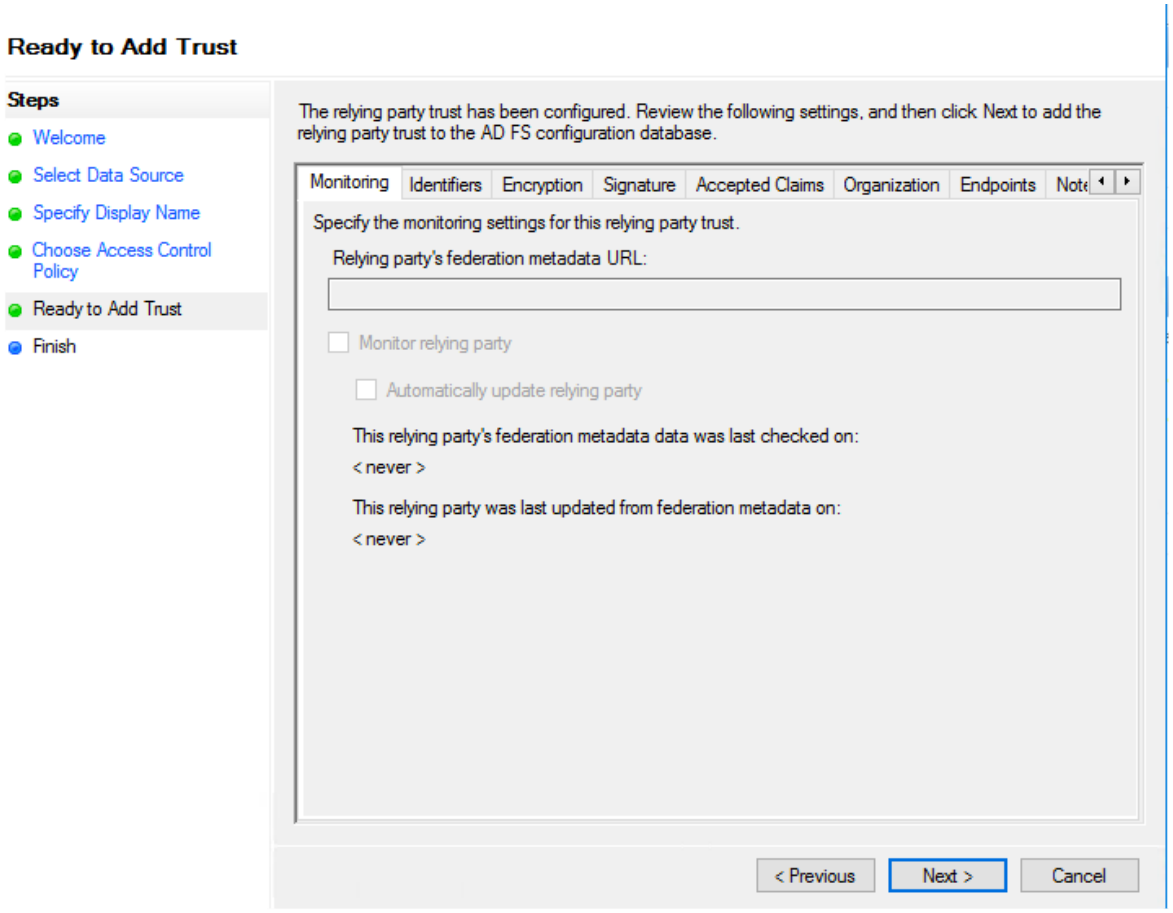
a.3 Provide a name for this relying party trust and click **Next**. Enter “Enter the issuer name provided by Nimonik for the name of the relying party. By any chance, if issuer is not provided by Nimonik then use "NimonikTrust" or any other value and pass the same to Nimonik admin."



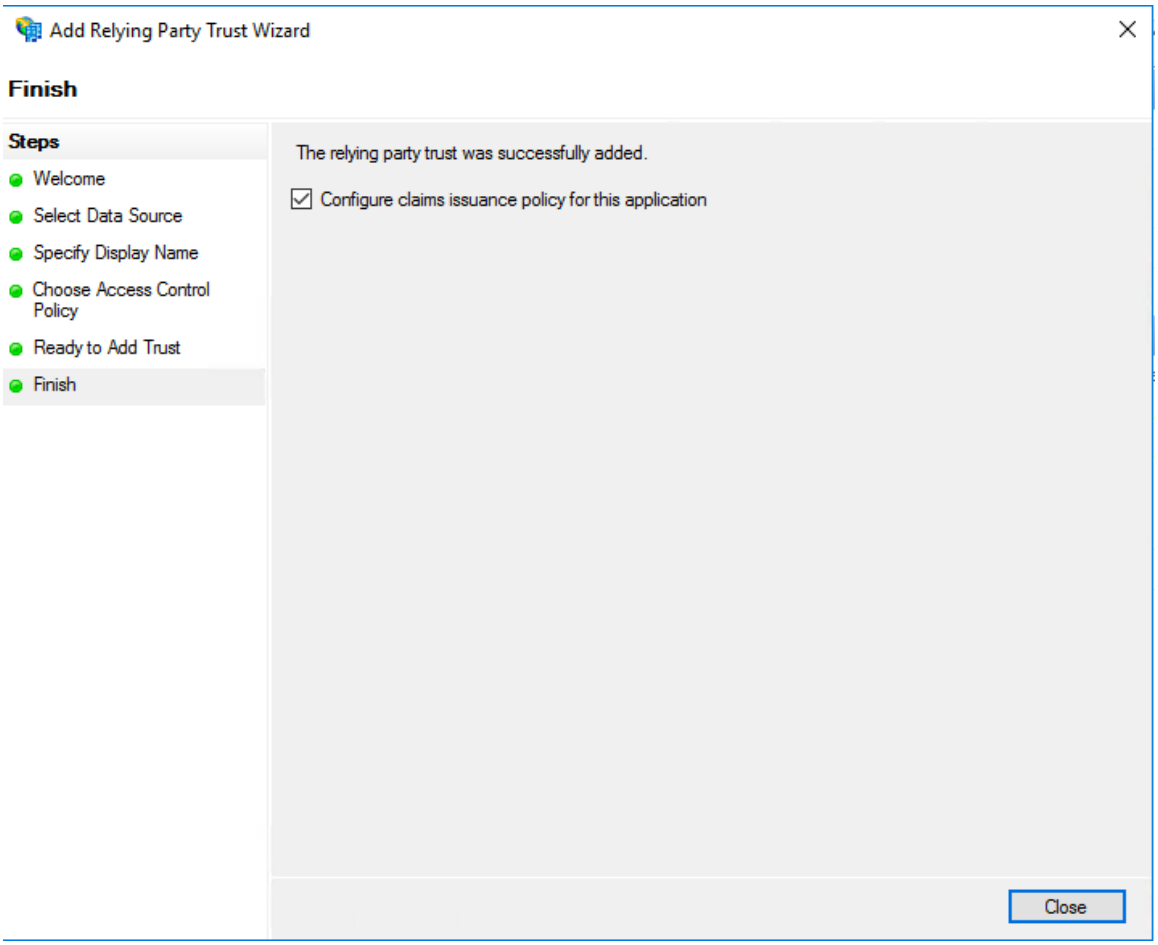
a.4 Choose 'Permit Everyone' or the user groups that you wish access to Nimonik in Choose Access Control Policy and click **Next**.



a.5 Click **Next** on the *Ready to Add Trust* window**.**

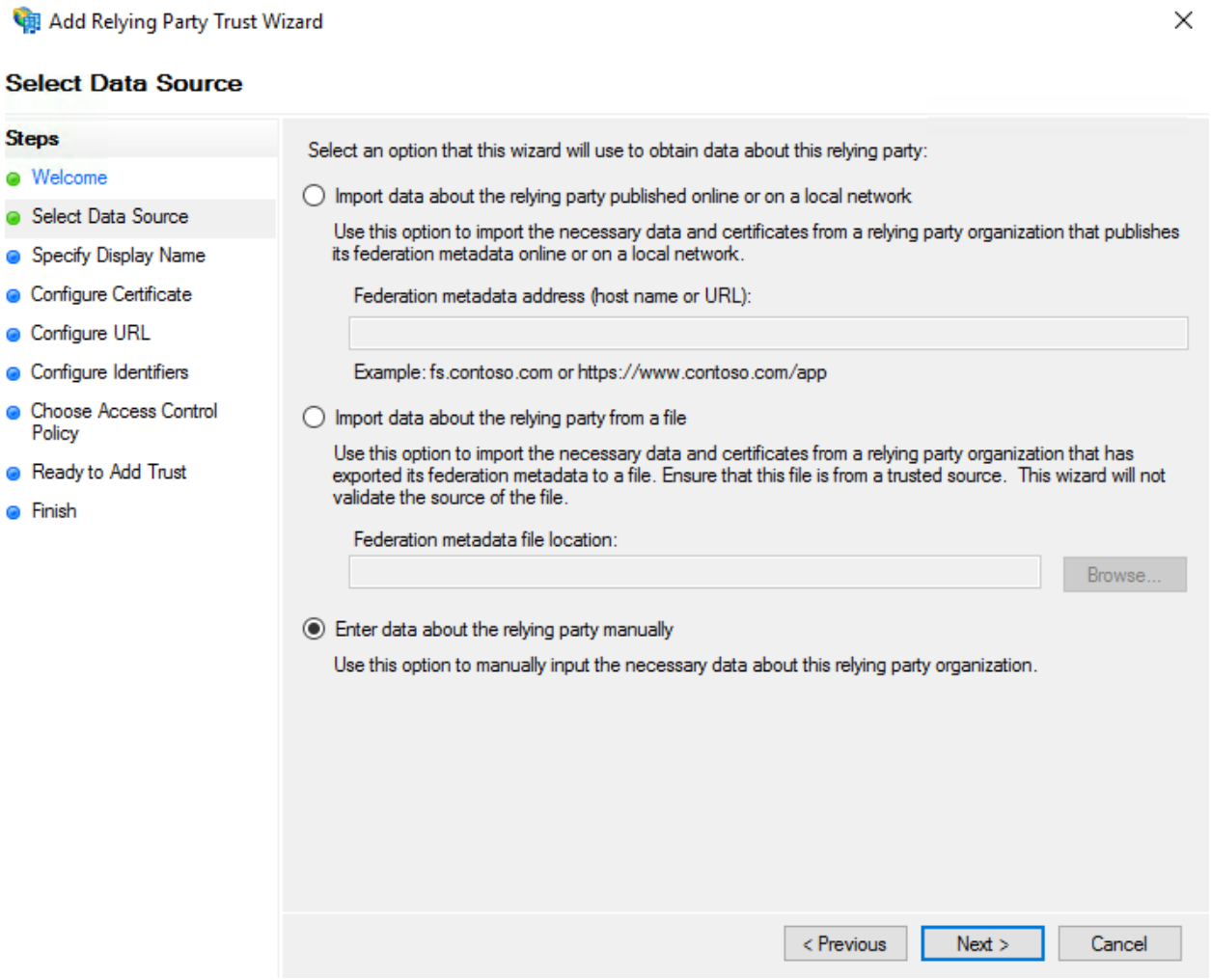


a.6 Check *Configure issuance policy for this application* and click **Close** and refer to STEP 3.



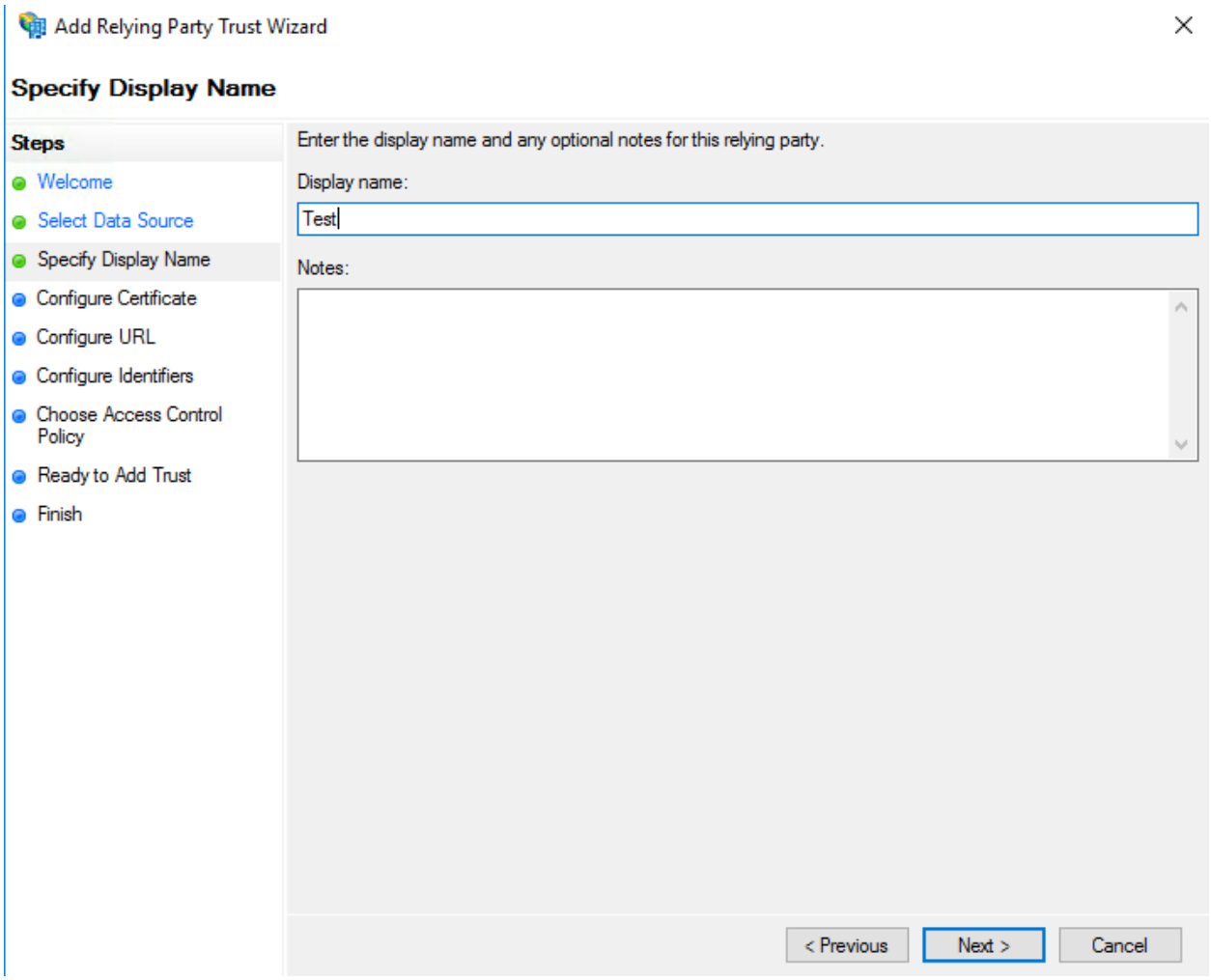
b. Enter data about the relying party manually

b.1 Select “Enter data about the relying party manually” and click **Next**.

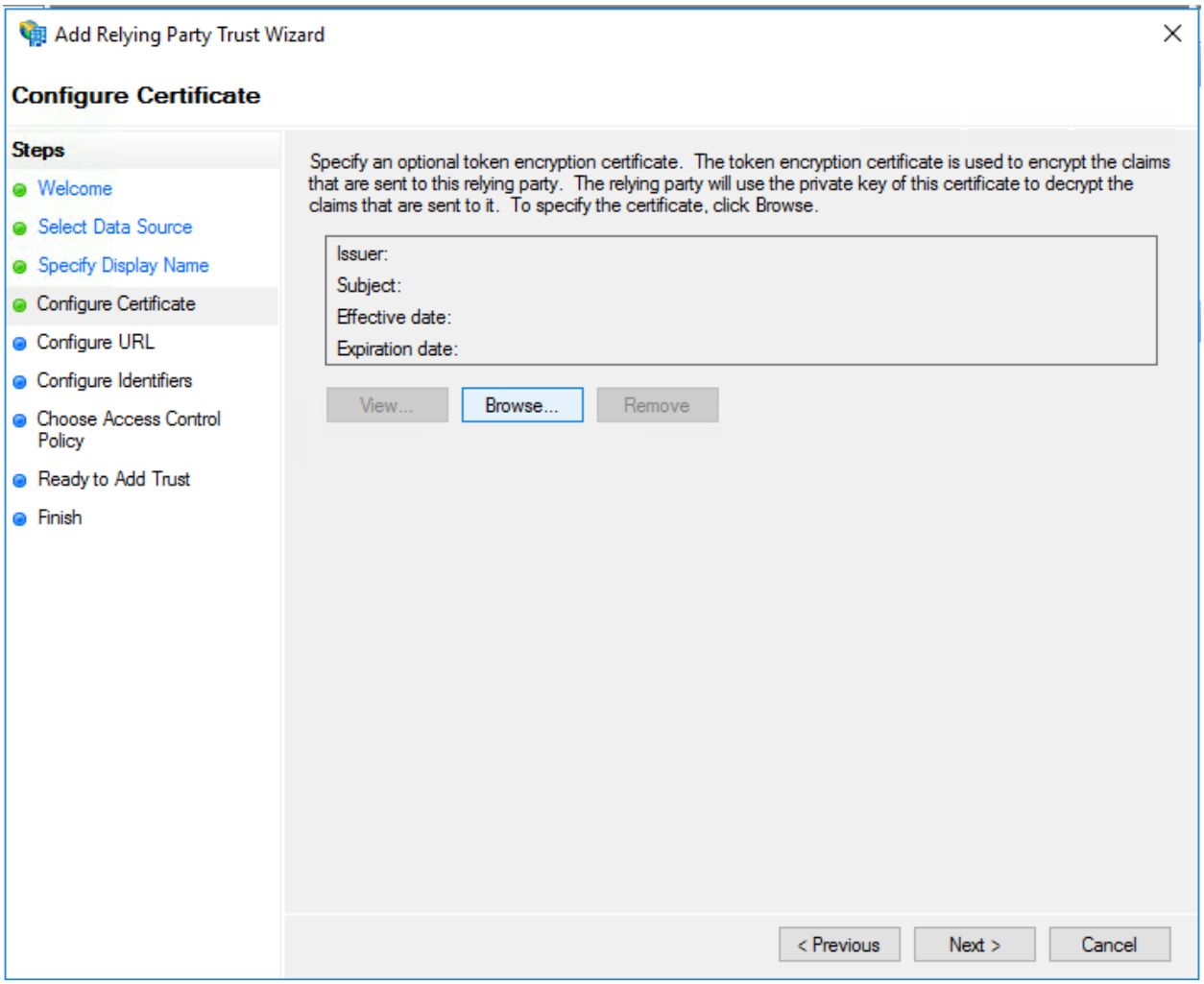


b.2 Next screen allows you to enter a display name and optional notes for this relying party.Enter the issuer name provided by Nimonik for the name of the relying party. By any chance, if issuer is

not provided by Nimonik then use "NimonikTrust" or any other value and pass the same to Nimonik admin.

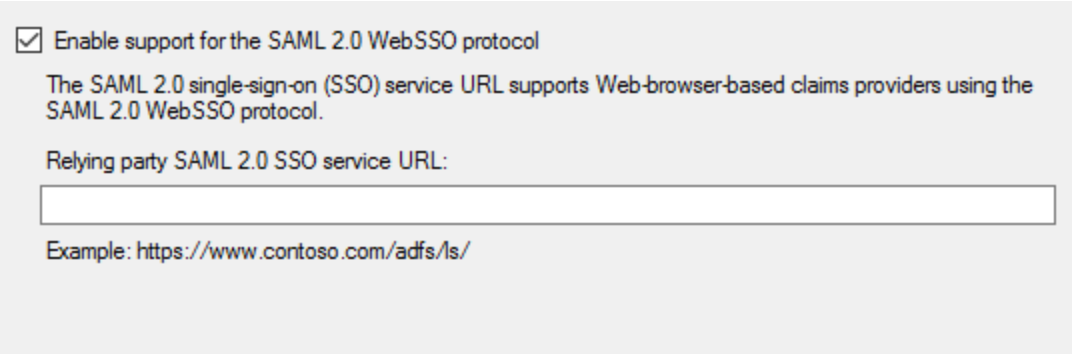


b.3 Configure the certificate to allow encryption of the SAML response. This certificate will be provided by the Nimonik Admin (Step 4). Nimonik will decrypt the response with a private key.

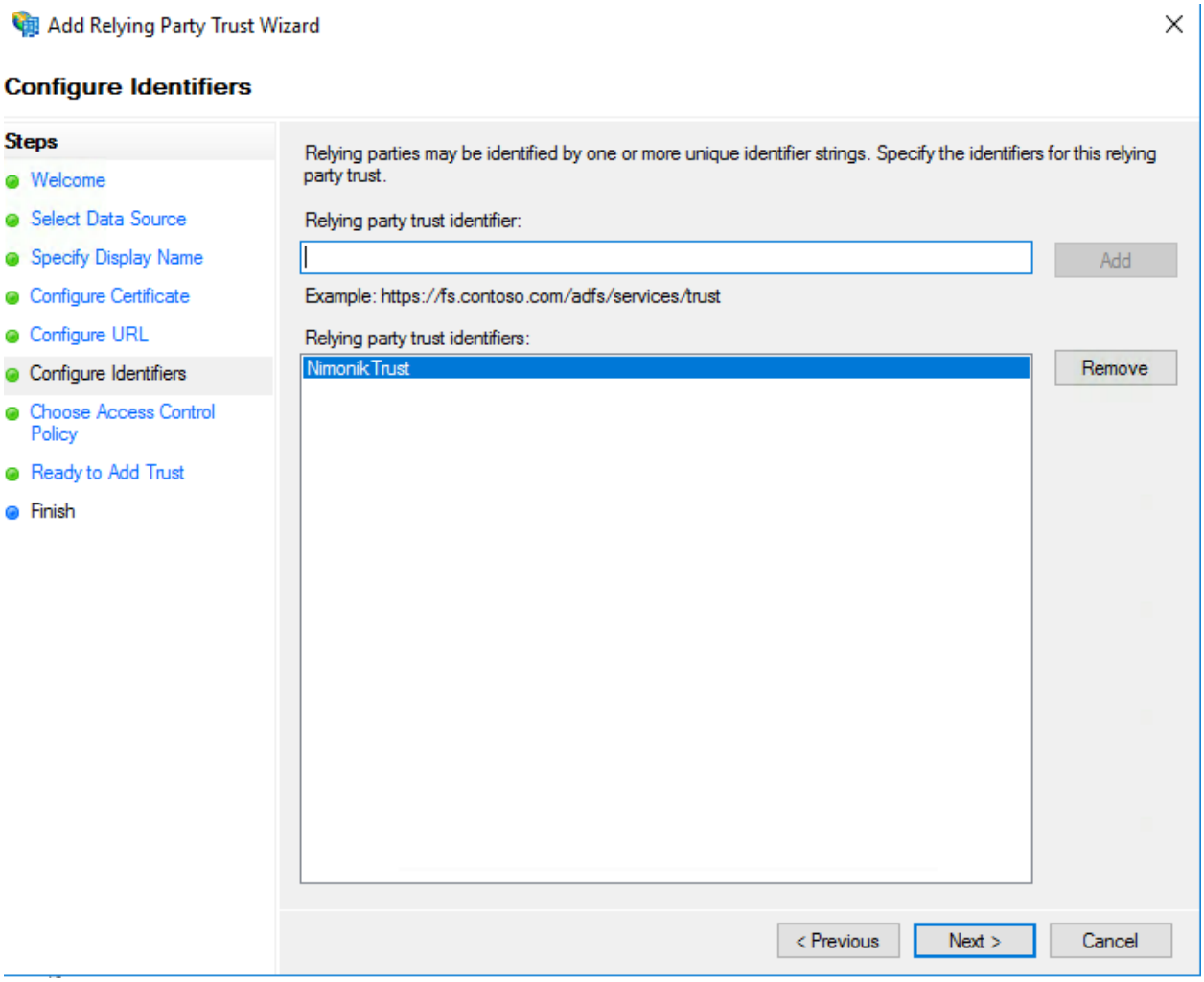


b.4 In next step, choose ‘Enable support for the SAML 2.0 WebSSO protocol’. And provide a SAML 2.0 SSO service url like: “https://<subdomain>.nimonik.com/users/auth/saml/callback”. Please note:

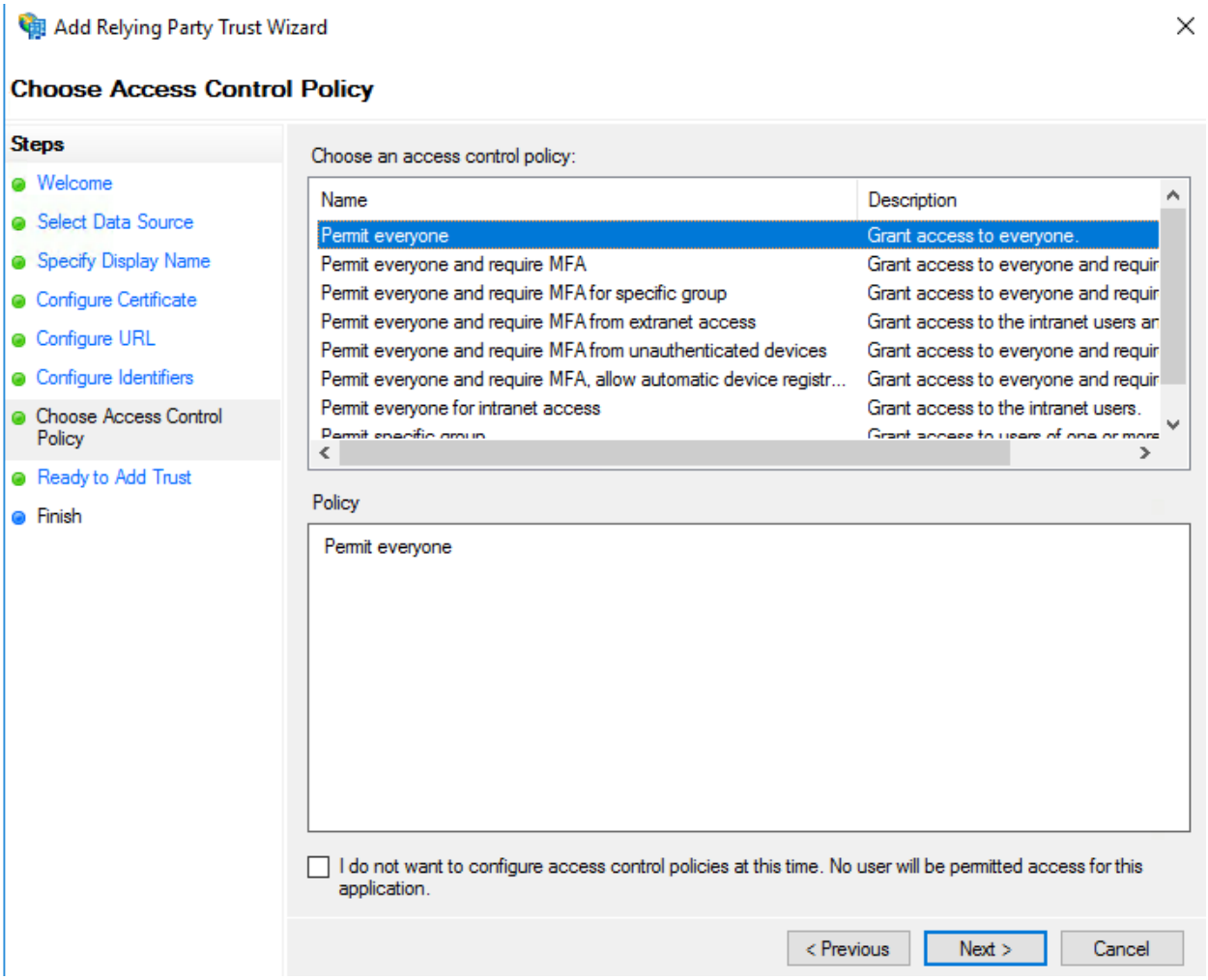
a. the URL must be in HTTPS.
b. subdomain is the Company’s subdomain slug.



b.5 Add a relying party string. This name will the name of “issuer” for Nimonik.



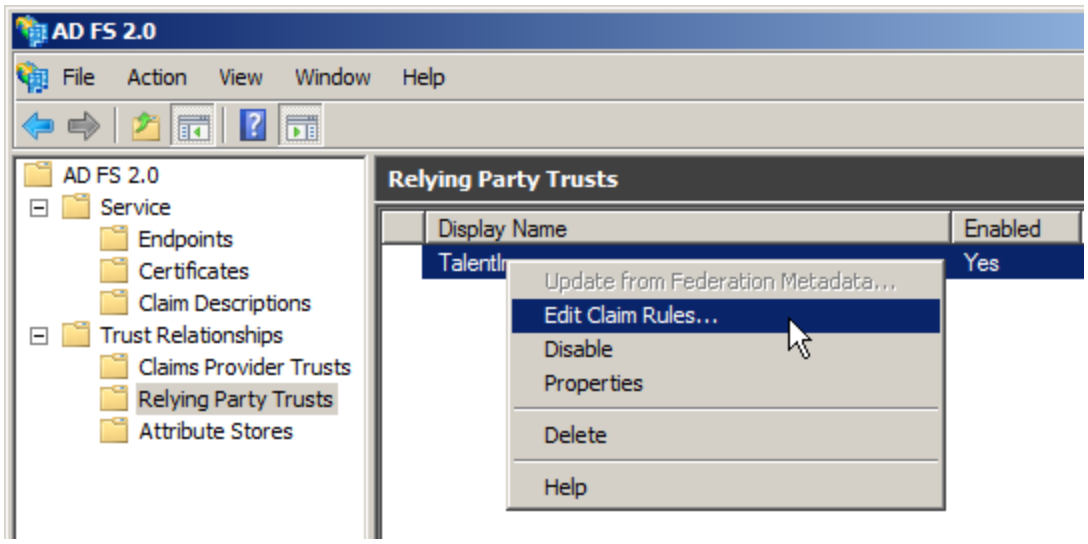
b.6 In next step choose **Permit everyone** and click **Next**



b.7 Follow the next step and Relying party will be added.

Step 3: ADFS Claim Rules Configuration

1. On the center Column right-click on the relying part you've just created and then select Edit Claim Rules.

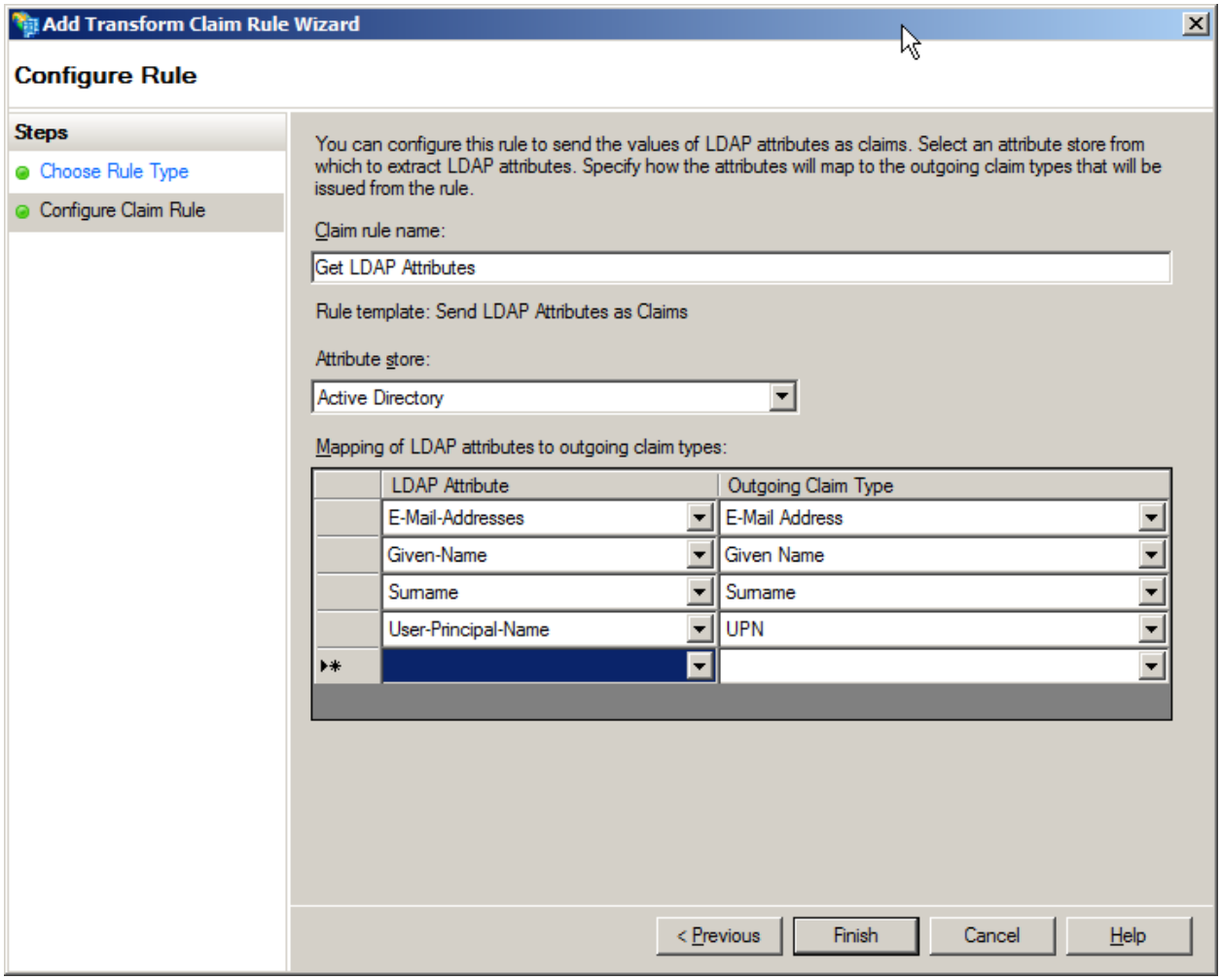


2. On the Issuance Transform Rules Tab click on Add Rules. The wizard launches.

3. Select Send LDAP Attribute as Claims and click on Next.

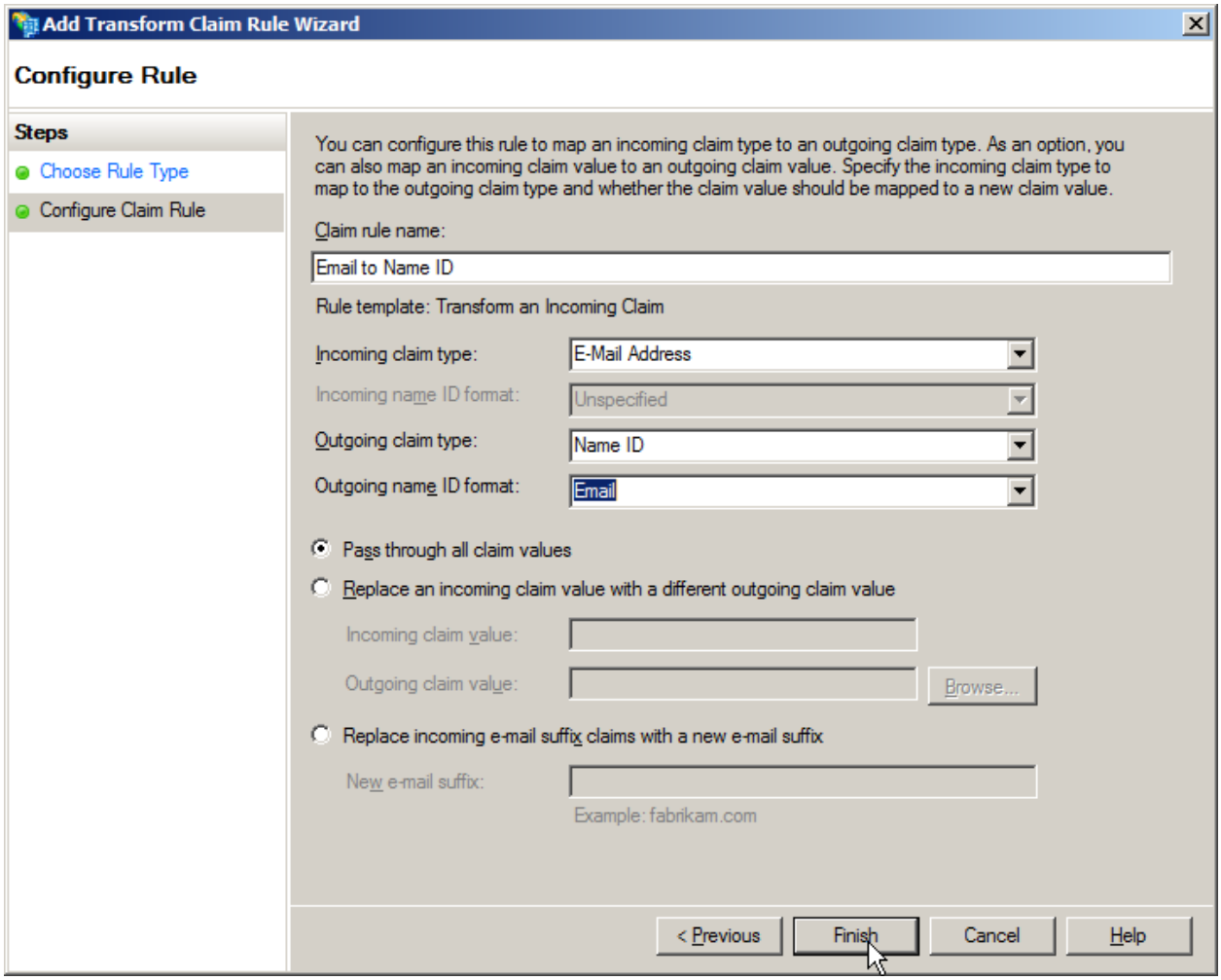
4. Define the Claim rule name (eg. Get LDAP Attributes) and select Active Directory in Attribute Store. In the Mapping of LDAP attributes to outgoing claim type select the following:

   - LDAP Attribute: **E-Mail-Addresses**, Outgoing Claim Type: **E-mail Address**
   - LDAP Attribute: **Given-Name**, Outgoing Claim Type: **Given Name**
   - LDAP Attribute: **Surname**, Outgoing Claim Type: **Surname**
     and then click on Finish



5. Add a second Rule following the same procedure. Select **Transform an Incoming Claim** and click on Next.

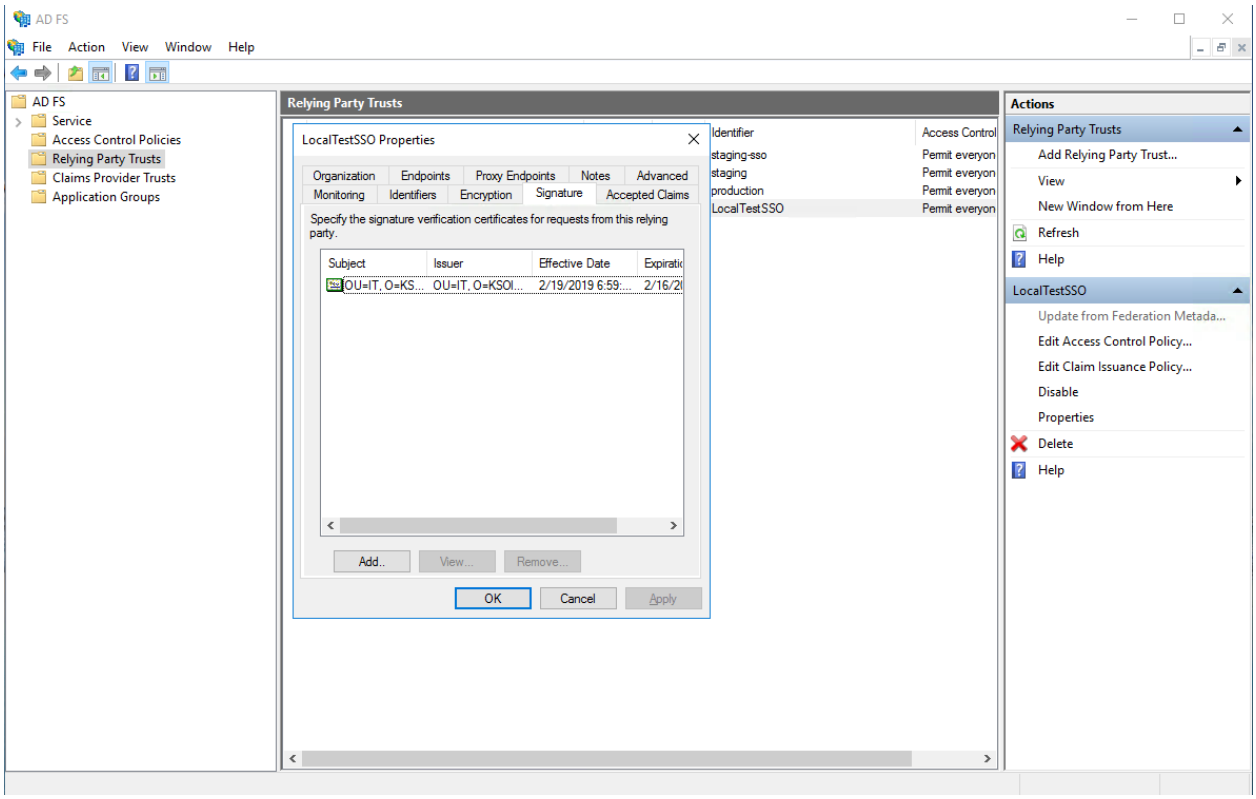
6. Define the Claim rule name (eg. Email to Name ID) and set Incoming claim Type as **E-Mail Address** (the same one from the previous rule), Outgoing claim type as **Name ID** and Outgoing name ID format as **Email.** Then click on Finish.
   Please note that the email should be defined in all users to achieve a proper communication between your ADFS and Nimonik.



Step 4: SSO Request Signing (Optional)

***Note**: This step must be ignored if Relying Party Trust is added through XML file provided by Nimonik or request need not be signed (encrypt).*

1. Select **Relying Party Trusts** from the left tree-view under the **Trust Relationships**, right-click on the **Relying Party Trusts** and right click on relying party you created and select properties.
2. Select the **Signature** option and add Nimonik public certificate here(.pem format).



3. Now open **Advanced** option and select Secure hash algorithm as **SHA-256.**
   Note: Nimonik only supports SHA-256 algorithm.