



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/>

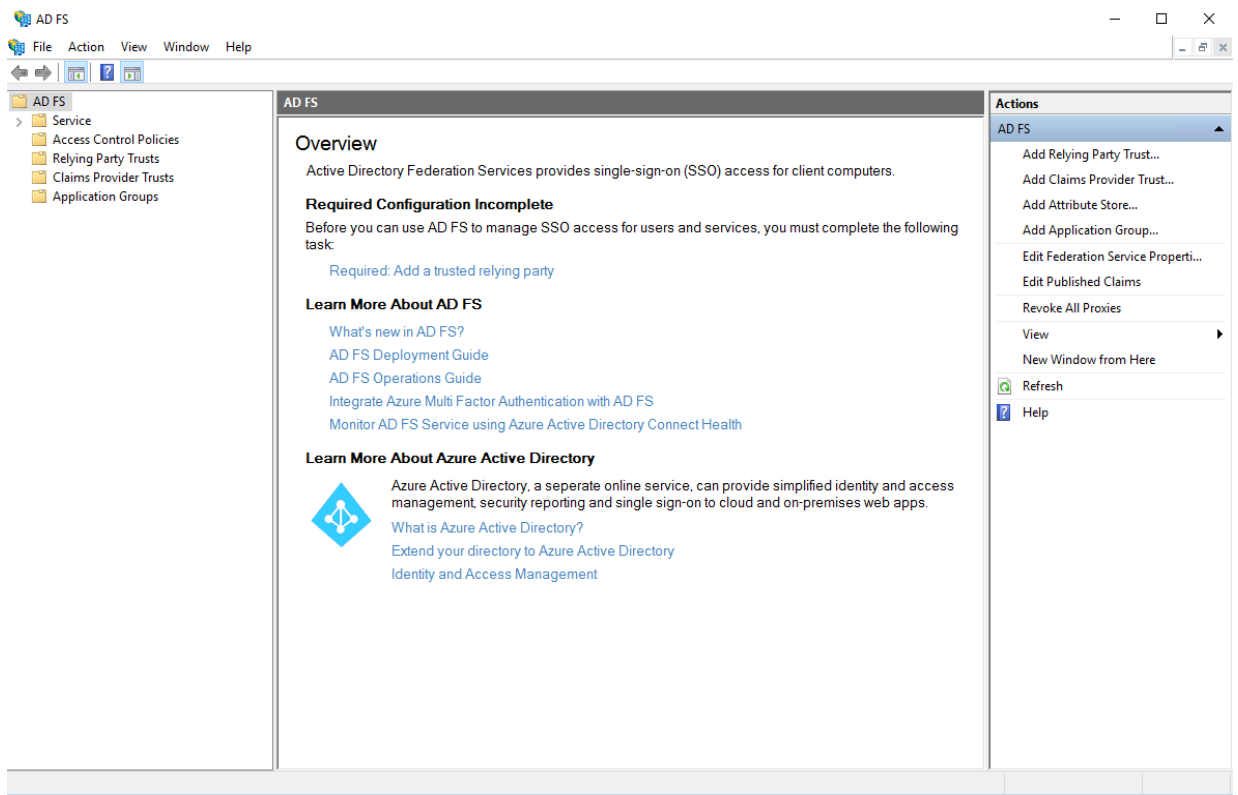
ADFS Configuration

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

Step 1: ADFS Basic Configuration

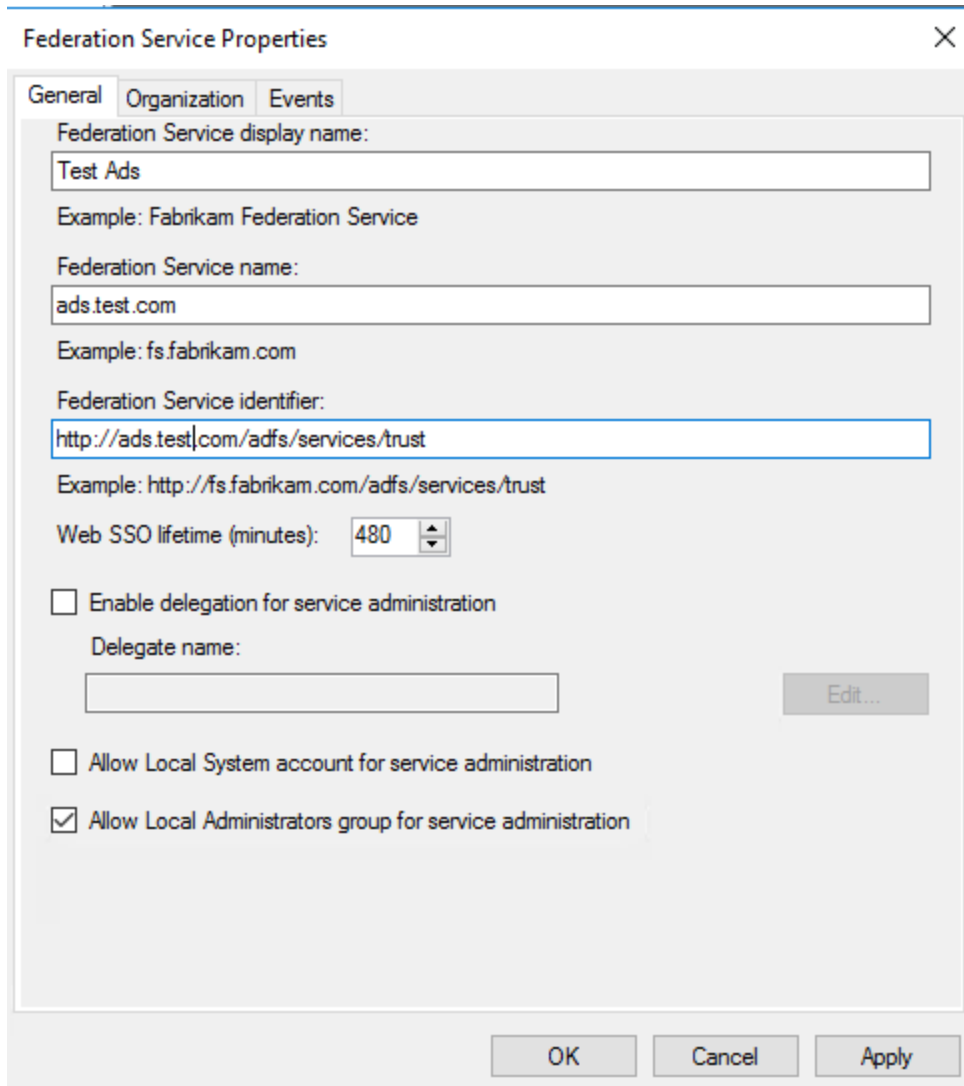
Open the ADFS Management through Start→Administrative Tools→ADFS Management.

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**.

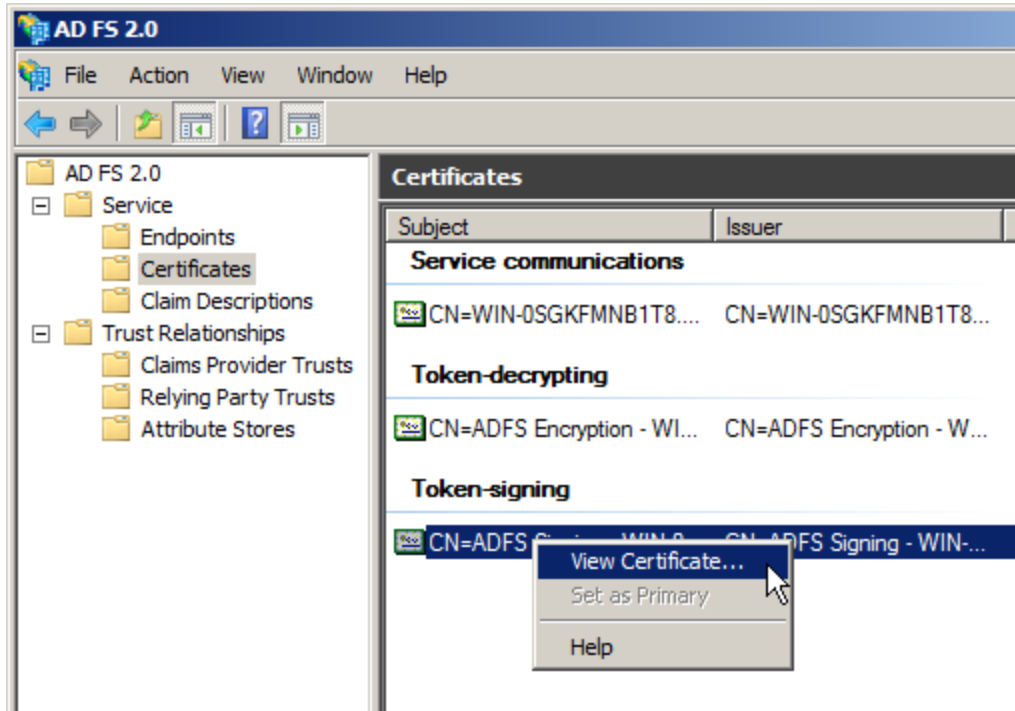


The screenshot shows the 'Federation Service Properties' dialog box with the 'General' tab selected. The fields are filled with the following values:

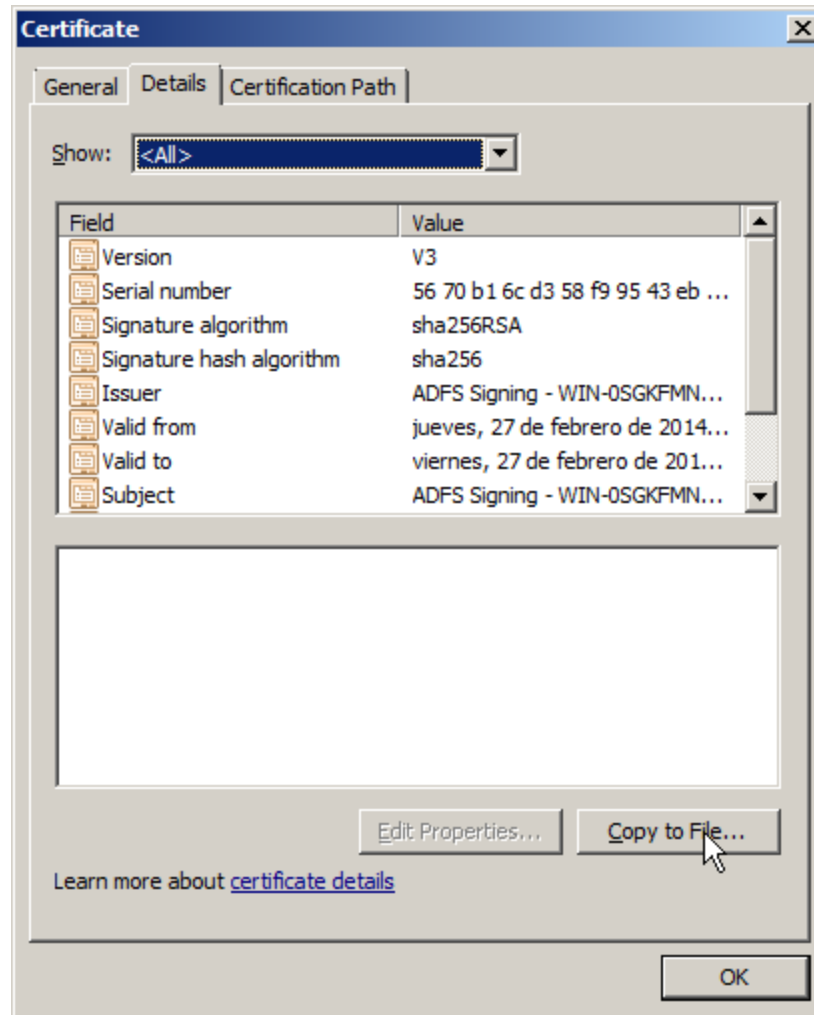
- Federation Service display name: Test Ads
- Example: Fabrikam Federation Service
- Federation Service name: ads.test.com
- Example: fs.fabrikam.com
- Federation Service identifier: http://ads.test.com/adfs/services/trust
- Example: http://fs.fabrikam.com/adfs/services/trust
- Web SSO lifetime (minutes): 480
- Enable delegation for service administration
- Delegate name: (empty field)
-
- Allow Local System account for service administration
- Allow Local Administrators group for service administration

At the bottom of the dialog are three buttons: OK, Cancel, and Apply.

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



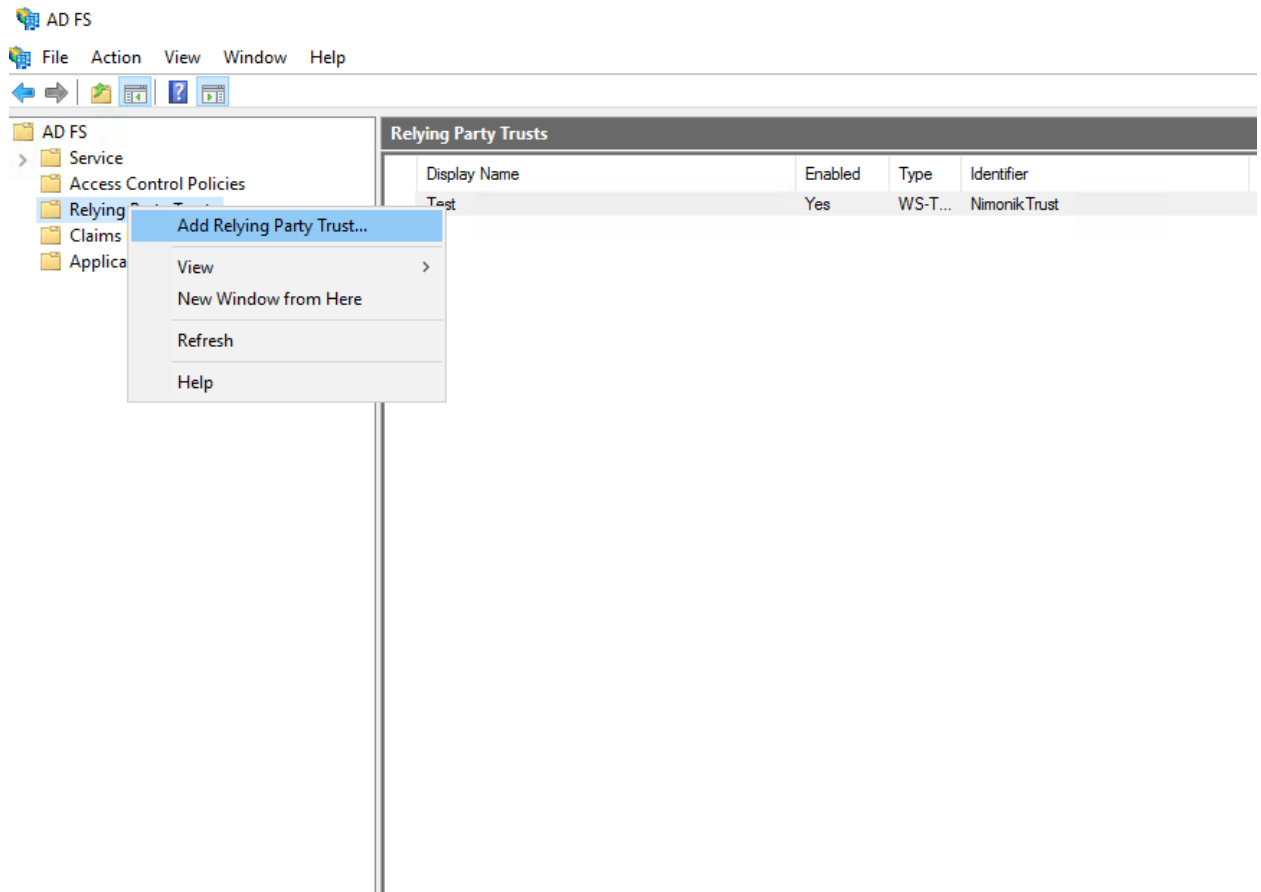
5. In the details tab,
 - a. Click on “Copy to File” to launch the Certificate Export Wizard.
 - b. Click on Next, select DER encoded binary X.509 (.cer) format, and then click Next.
 - c. Select the directory where you want to save the certificate and click on Finish.



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**.

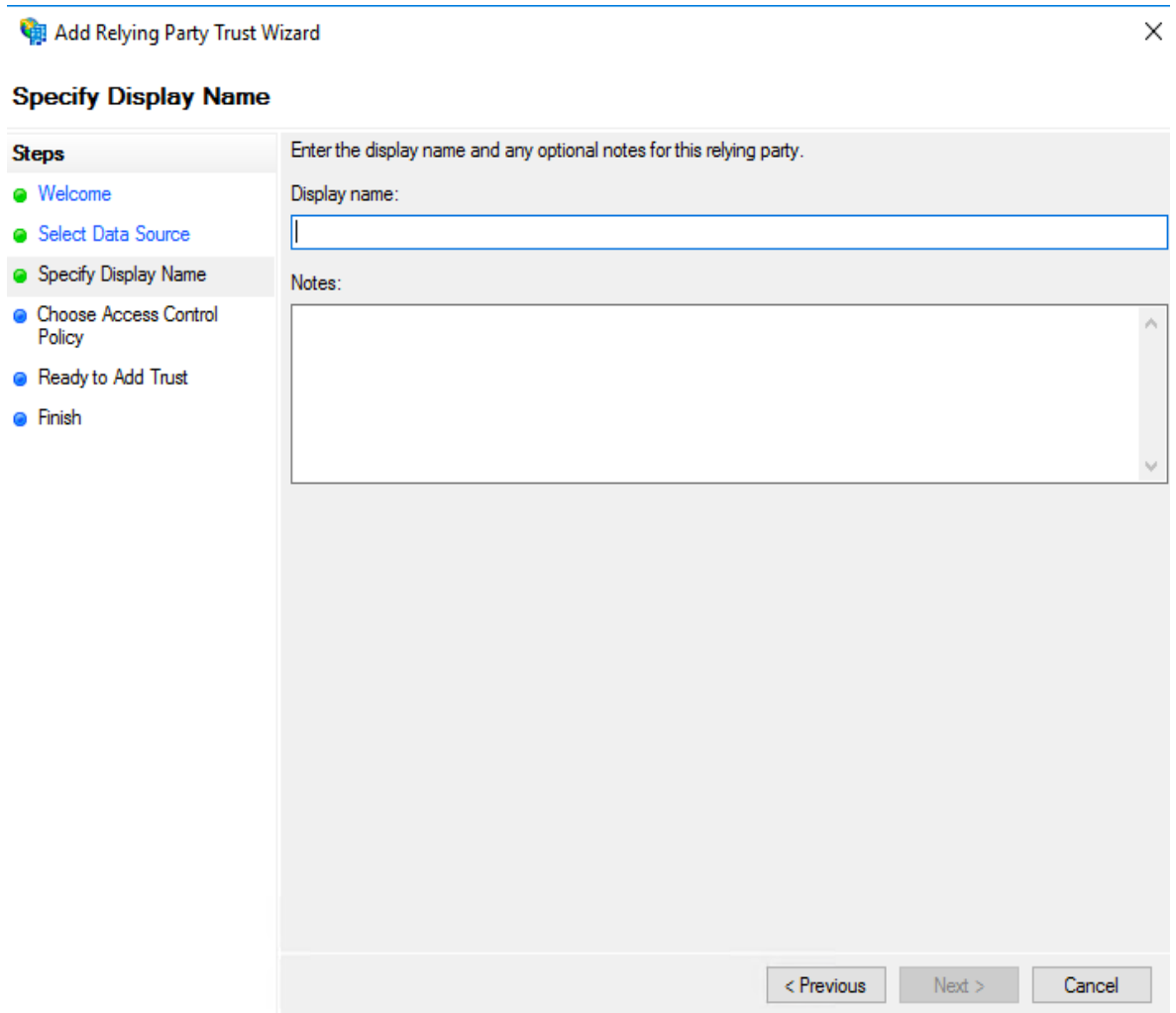
a.2 This file will be provided by Nimonik. Locate the path of the file and click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options:

- Import data about the relying party published online or on a local network. 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. Federation metadata address (host name or URL): [text box]. Example: fs.contoso.com or https://www.contoso.com/app.
- Import data about the relying party from a file. 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. Federation metadata file location: [text box with 'C:\Users\Administrator\Desktop\metadata (1).xml'] and a 'Browse...' button.
- Enter data about the relying party manually. Use this option to manually input the necessary data about this relying party organization.

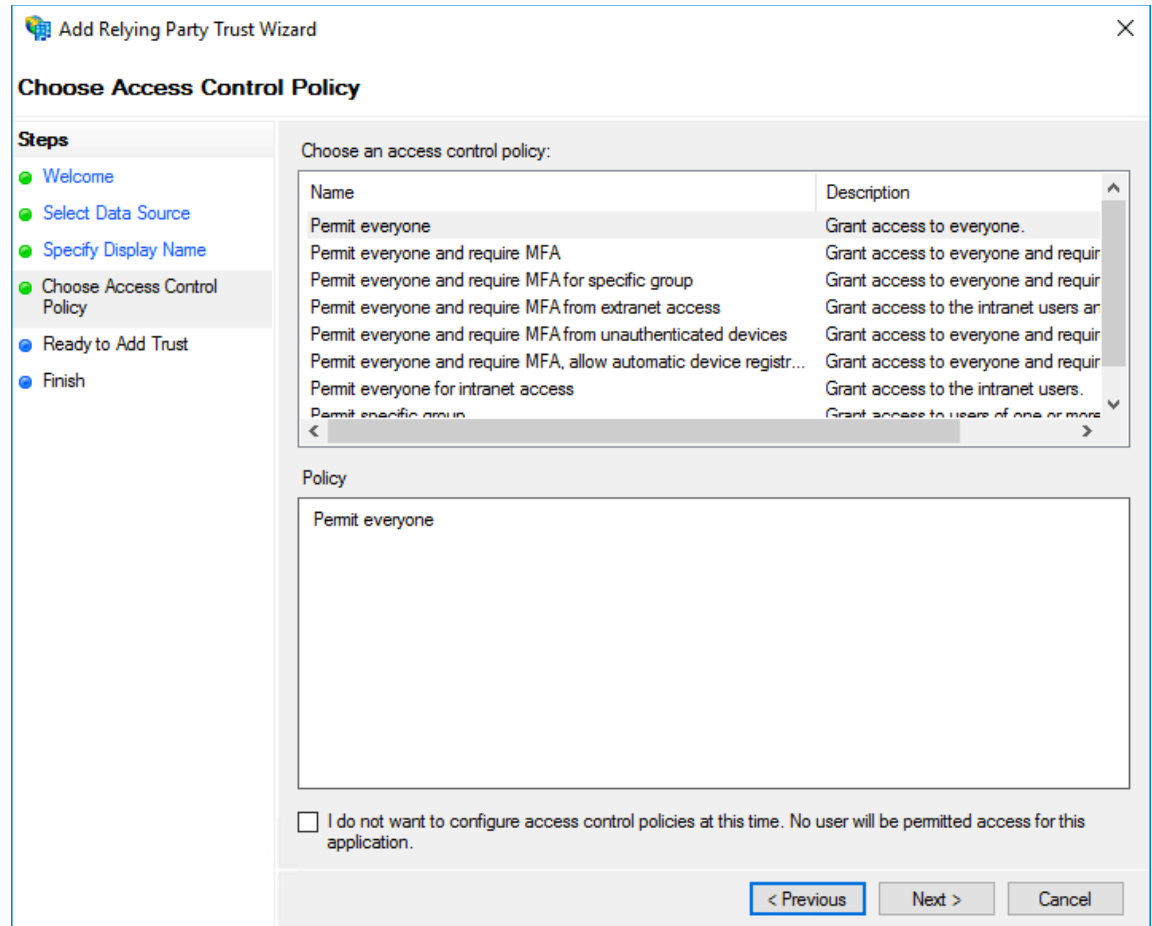
At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

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."



The screenshot shows a wizard window titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The main heading is "Specify Display Name". On the left, a "Steps" list shows the following steps: "Welcome" (green dot), "Select Data Source" (green dot), "Specify Display Name" (green dot and highlighted), "Choose Access Control Policy" (blue dot), "Ready to Add Trust" (blue dot), and "Finish" (blue dot). The main area contains the instruction "Enter the display name and any optional notes for this relying party." Below this, there is a "Display name:" label followed by an empty text input field. Underneath is a "Notes:" label followed by a large, empty text area with a vertical scrollbar on the right. At the bottom right, there are three buttons: "< Previous" (disabled), "Next >" (disabled), and "Cancel" (disabled).

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.

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

Monitor relying party

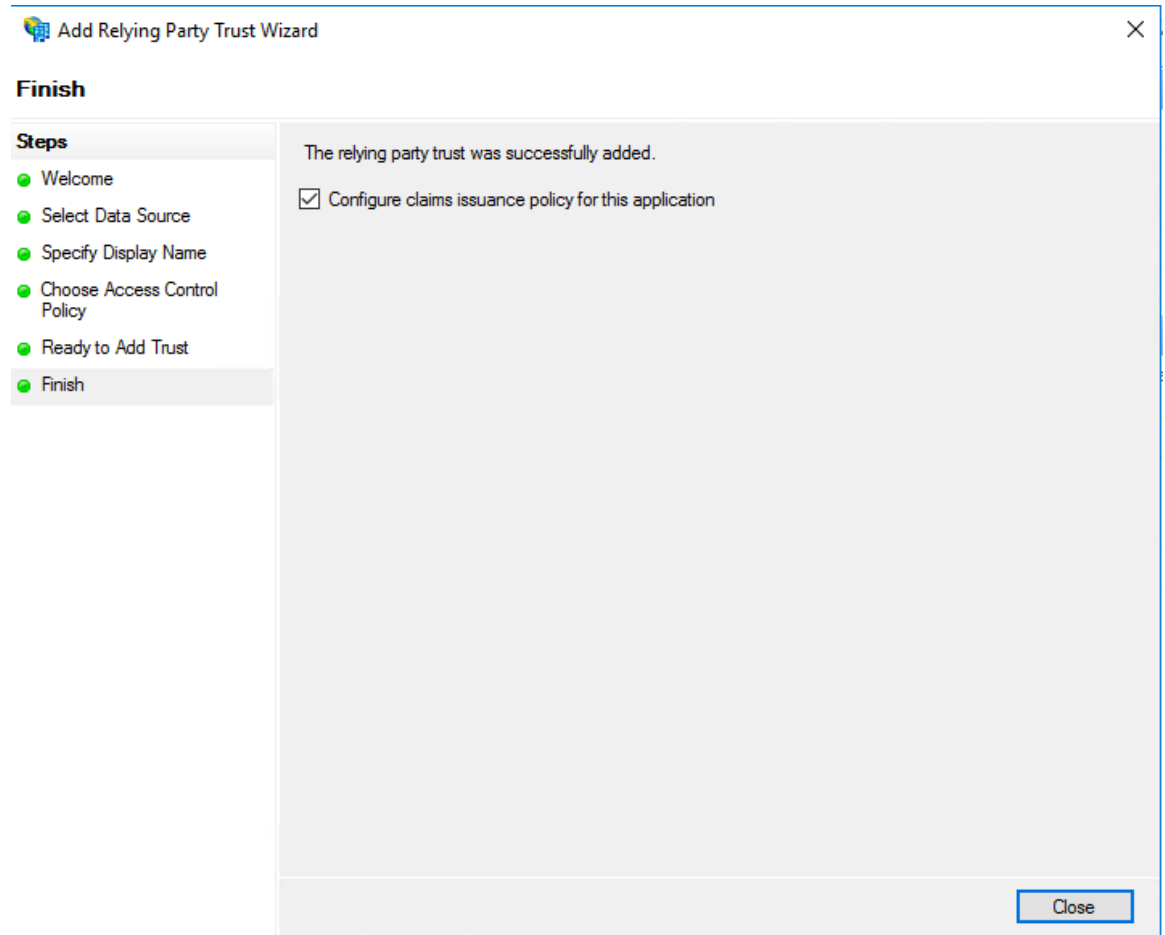
Automatically update relying party

This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

< Previous Next > Cancel

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**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source (highlighted), Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options:

- Import data about the relying party published online or on a local network. 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.contoso.com or https://www.contoso.com/app'.
- Import data about the relying party from a file. 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:' with a 'Browse...' button to its right.
- Enter data about the relying party manually. Use this option to manually input the necessary data about this relying party organization.

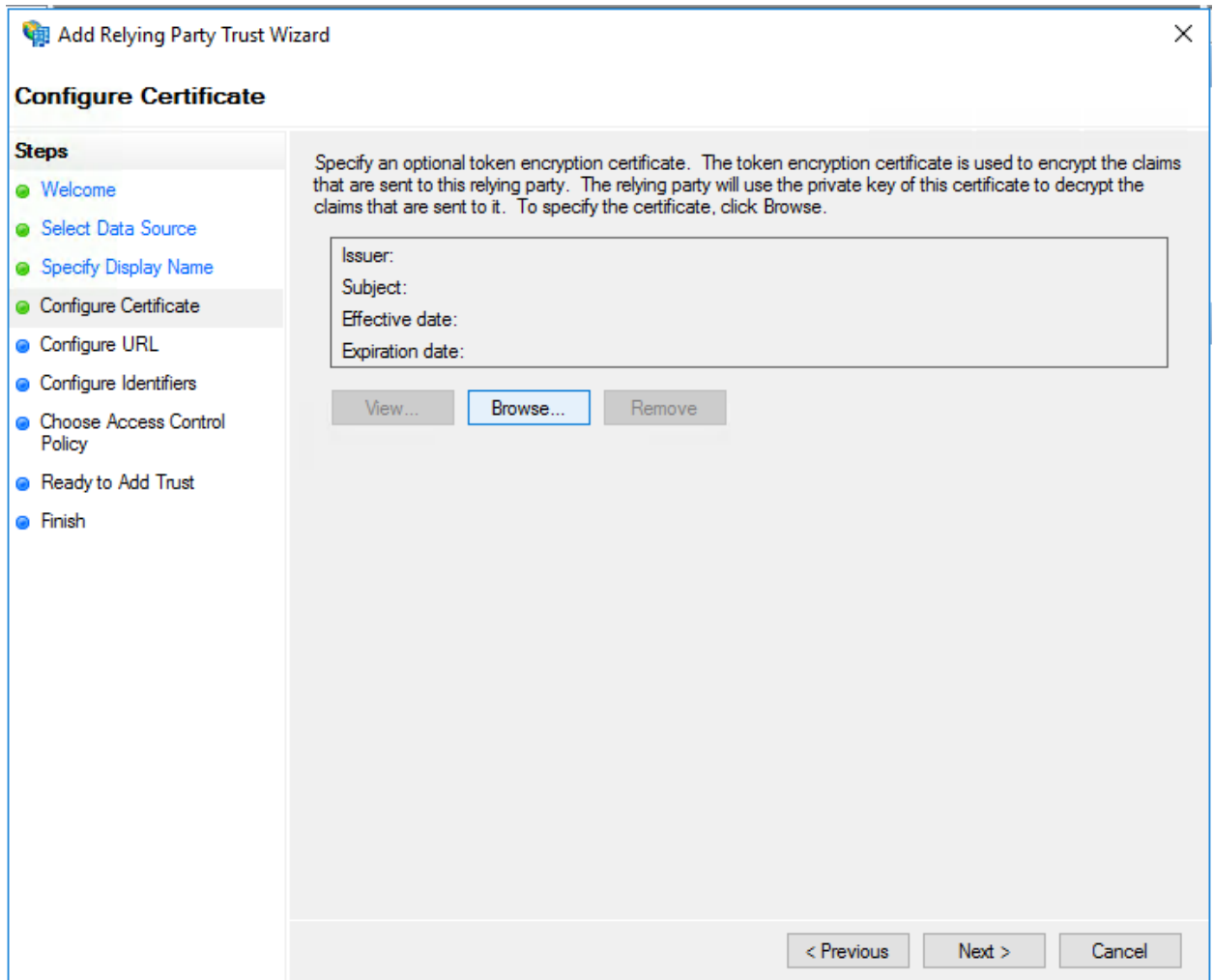
 At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

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.

The image shows a screenshot of the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (highlighted), Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text input field containing the text 'Test'. Below the input field is a 'Notes:' label followed by a large, empty text area with a vertical scrollbar. At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

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.

Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

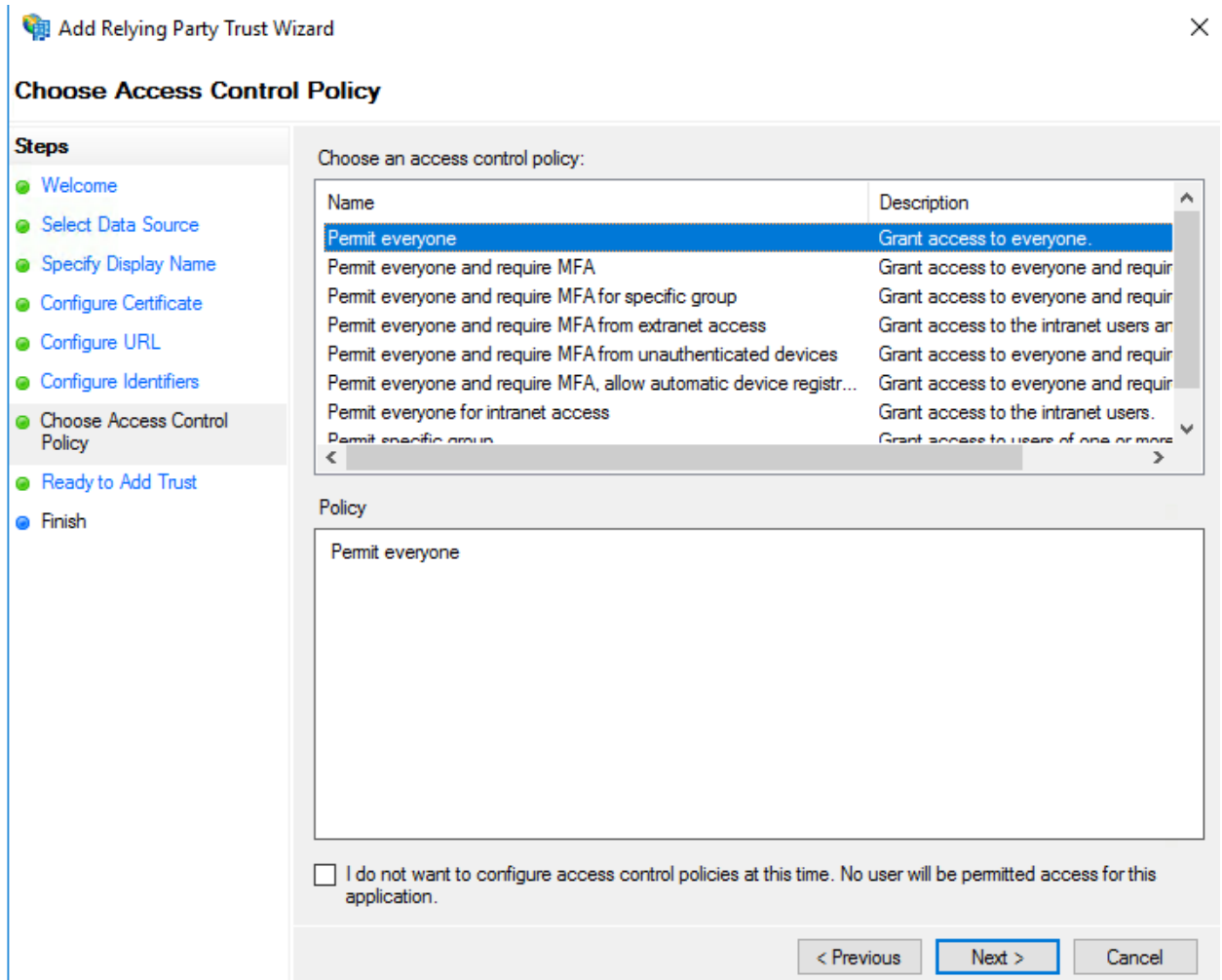
Relying party SAML 2.0 SSO service URL:

Example: <https://www.contoso.com/adfs/ls/>

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

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure Identifiers' step. The wizard has a close button (X) in the top right corner. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers (which is the current step), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area of the wizard contains the following text: 'Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.' Below this is a text input field labeled 'Relying party trust identifier:' with an 'Add' button to its right. An example URL is provided: 'Example: https://fs.contoso.com/adfs/services/trust'. Below the input field is a list box labeled 'Relying party trust identifiers:' containing one entry, 'Nimonik Trust', which is currently selected. A 'Remove' button is located to the right of the list box. At the bottom of the wizard, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

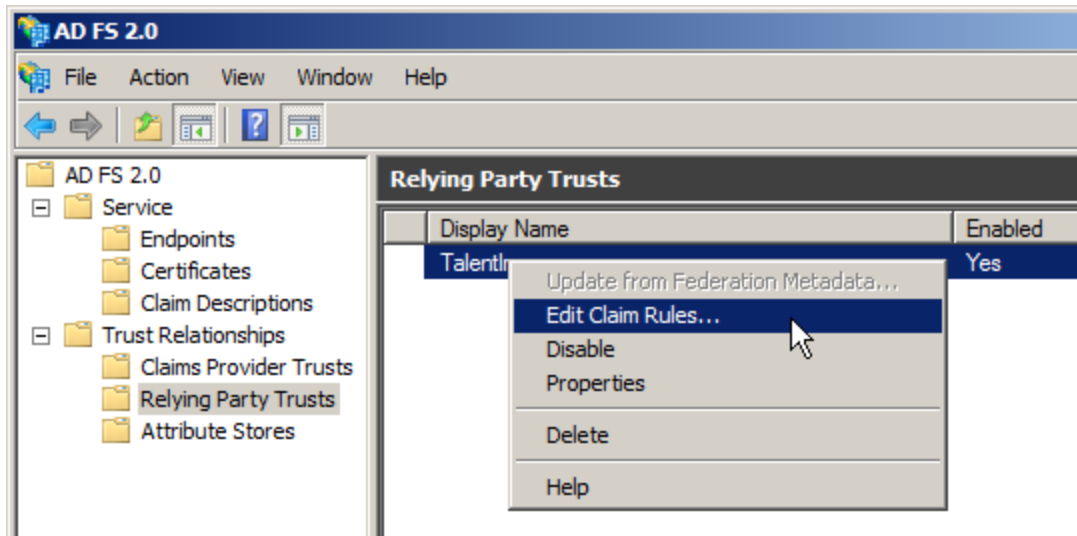
b.6 In next step choose **Permit everyone** and click **Next**



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

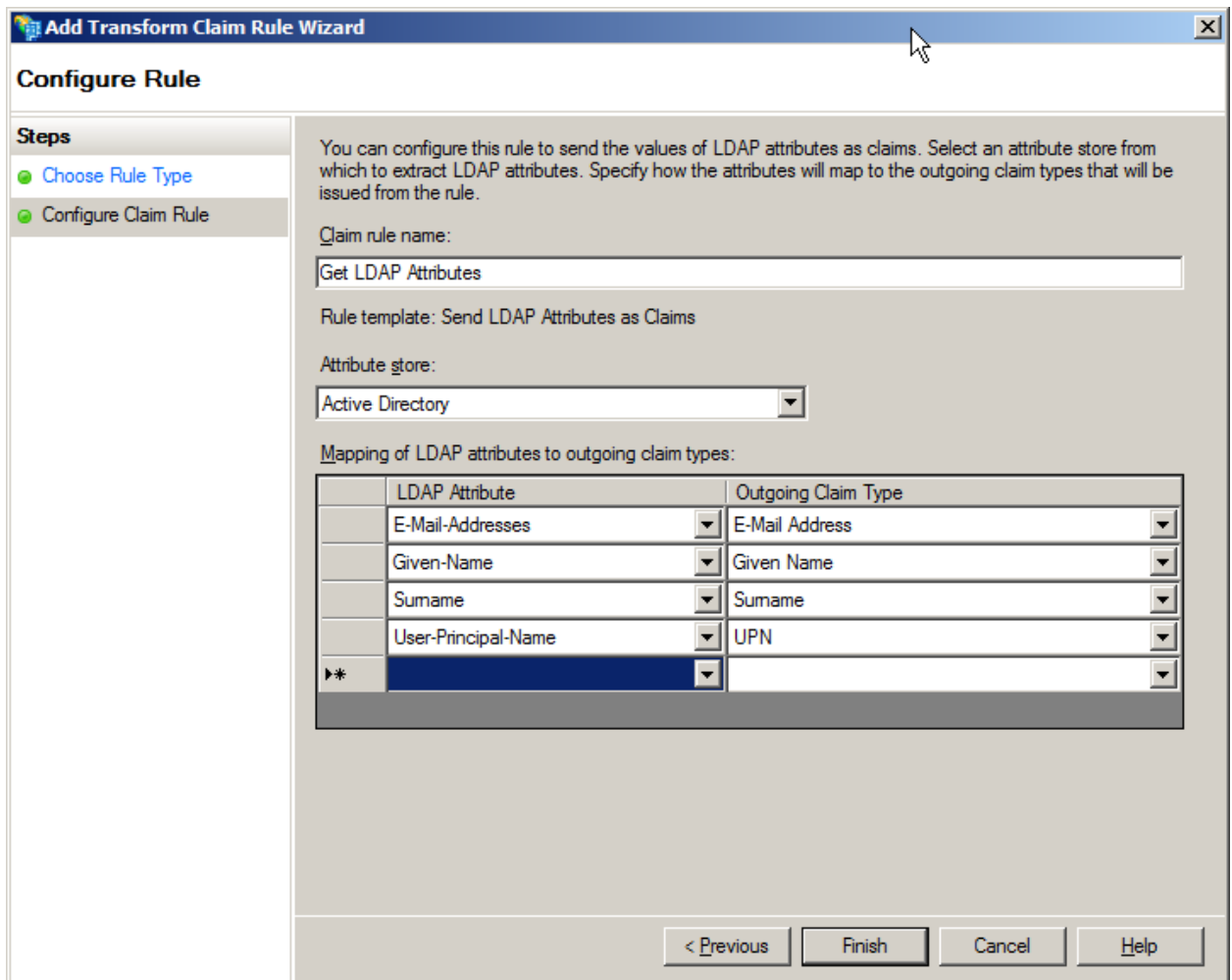
Step 3: ADFS Claim Rules Configuration

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.

- 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.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

Pass through all claim values

Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

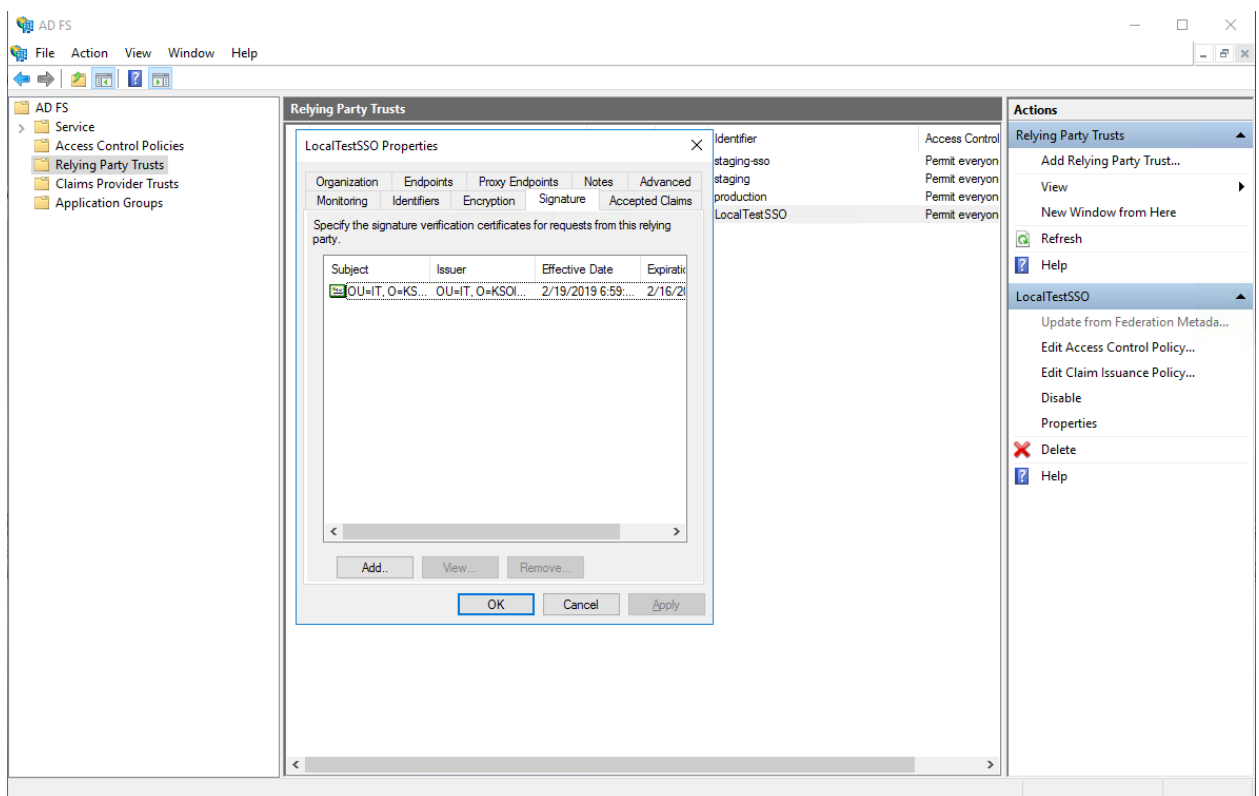
Example: fabrikam.com

< Previous **Finish** Cancel Help

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.

