KICS - SAML / ADFS / Federated Services Set Up

With SAML, a user is redirected to a company's authentication server for sign-in. When the user authenticates, the SAML server provides an authentication token to KICS. This token provides the account properties (Account Name, Group Membership, First Name, Last Name, Email, Account Serial), which KICS uses to lookup / map / create a Linked account for the user.

KICS SAML Installation Steps

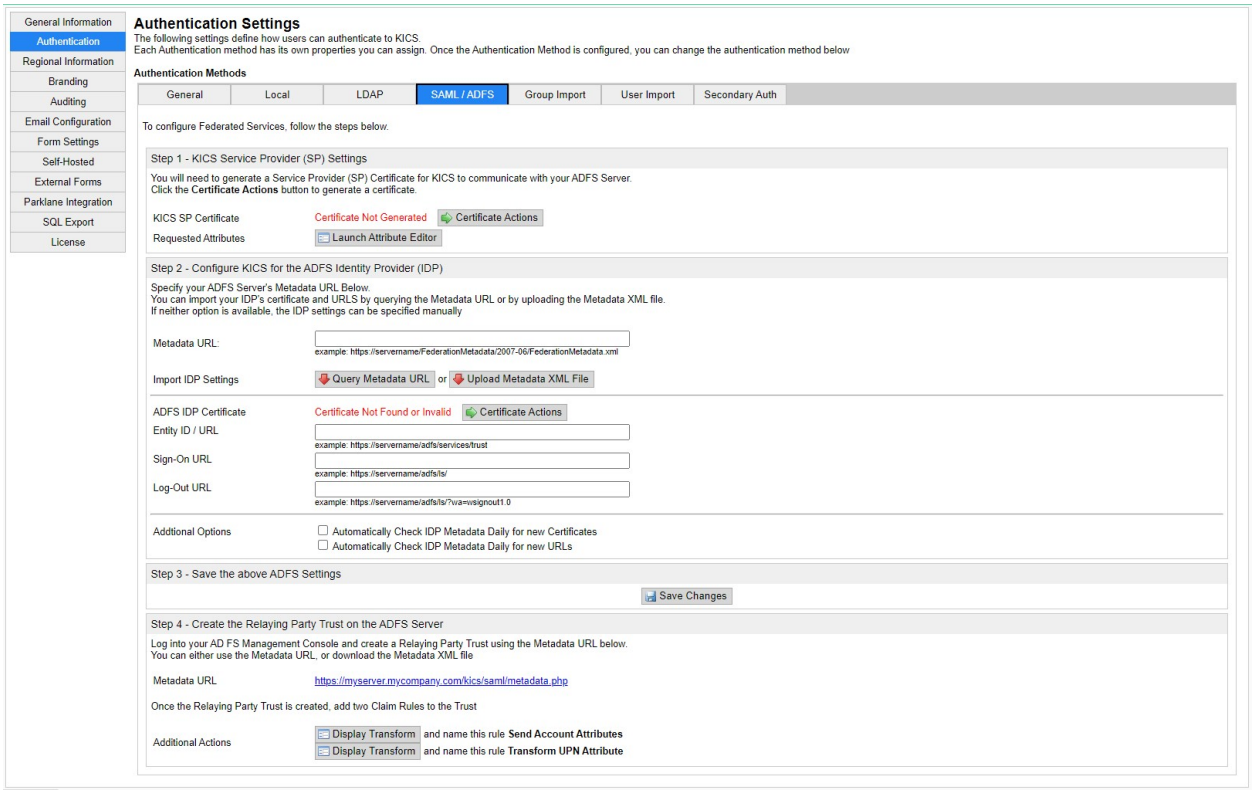
- For onsite installs, HTTPS / SSL needs to be enabled. Refer to the **Web Framework HTTPS Technical Document** for install instructions
- A Service Provider Certificate (SP) will be generated within KICS
- The authentication URLs (login/logout) and the Identity Provider Certificate (IDP) for the federation server will be configured. These can be imported from the Server's metadata file.
- A Relaying Party trust will be configured on the Federation Server for KICS
- Transform Rules will be set up to send attributes from ADFS to KICS.

Azure AD Notes

This document is oriented towards on-premises ADFS Deployments. These instructions can also apply for Azure AD Deployments and notes have been provided throughout the document for items specific for Azure AD.

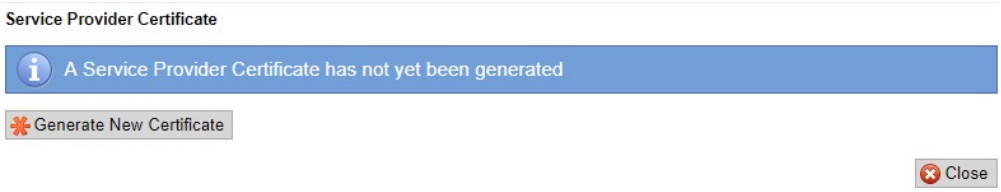
Generating the Service provider Certificate

In KICS, go to **System Settings > Authentication > SAML / ADFS**

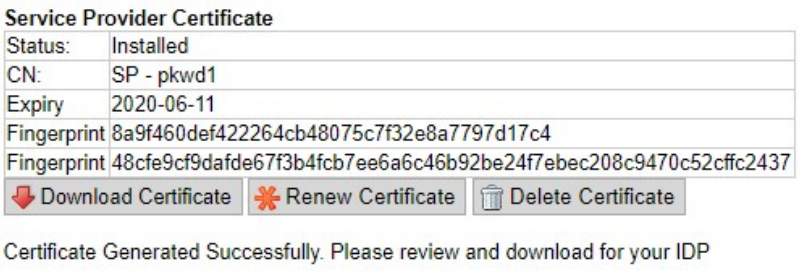


Under **Step 1**, click **Certificate Actions** beside the **KICS SP Certificate** option

A Dialog for the Service Provider Certificate will appear



Click **Generate New Certificate**. Certificate Generation will take a couple seconds.



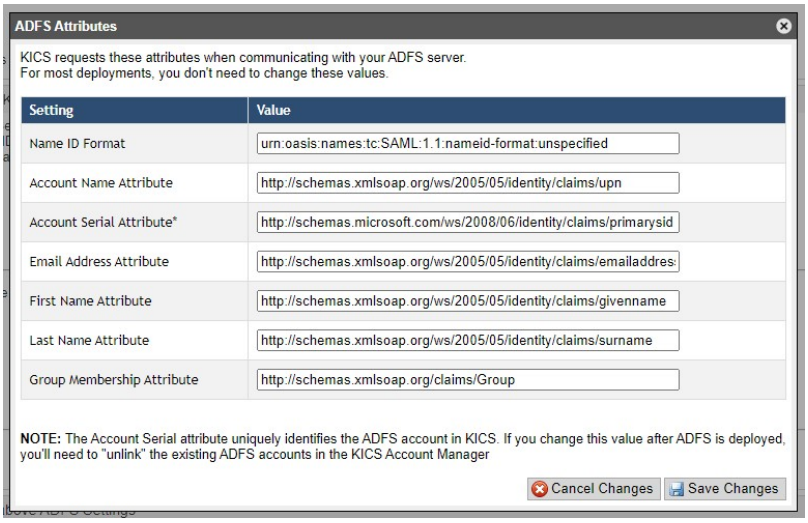
Click **Close**

Setting up the Federated Services Attributes

On-Premises ADFS and Azure AD use different attributes, so you will need to confirm the appropriate attributes for your deployment.

Launch the Attribute Editor

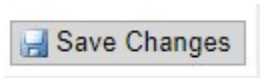
The Attribute Editor will display



KICS comes preconfigured for on-premises attributes. If you are using Azure AD, please update the attributes listed below:

Attribute	Value
Name ID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Account Name	**ADFS** - http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn **Azure AD** - http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Account Serial	**ADFS** - http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid **Azure AD** - http://schemas.microsoft.com/identity/claims/objectidentifier
Email Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Group Membership	http://schemas.xmlsoap.org/claims/Group

Click Save Changes

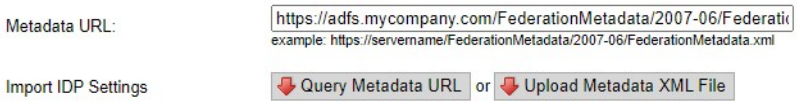


Setting up the ADFS IDP Parameters

On the **System Settings > Authentication > SAML** page, **Step 2** focuses on setting up the URLS and Certificates for your ADFS Identity Provider (IDP). KICS can import this data from your ADFS's Metadata URL. If KICS can't reach the Metadata URL, you have the option to upload the Metadata XML file, or configure the certificate and URLS manually

Option 1 - Import IDP Parameters using the ADFS Metadata URL

Specify your ADFS Server's Metadata URL and then click **Query Metadata URL**. The ADFS Server's URLS and Certificates will be imported.

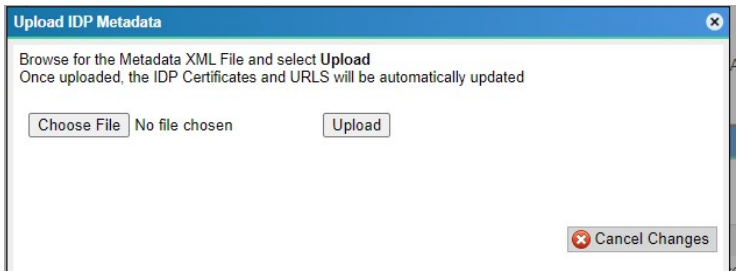


Option 2 - Import IDP Parameters using the ADFS Metadata XML File

IF your ADFS server is not reachable by KICS, you can upload the Metadata XML File to KICS.

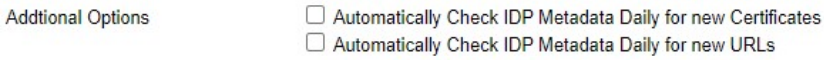
Select the **Upload Metadata XML File** button.

Browse for the Federation Metadata XML File and click Upload.



When Option 1 or Option 2 is used, you will see the ADFS IDP Certificate and URLS configured in KICS.

Most ADFS server certificates will last for 1 year. You have the option to configure KICS to query the ADFS Metadata once a day to check for certificate updates and URLS. Note: KICS will require access to your ADFS Server's Metadata URL to use this feature.



With the ADFS IDP Settings configured, click **Save Changes**

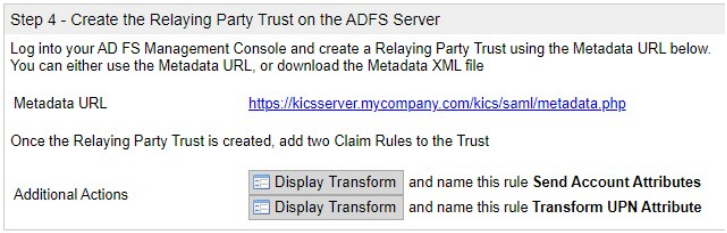
Click **Save** to save the current settings into KICS

NOTE: For Azure AD deployments, we have noticed that the Azure-generated metadata URL does not contain the proper IDP certificates for a few minutes after the trust is created in the Azure console.

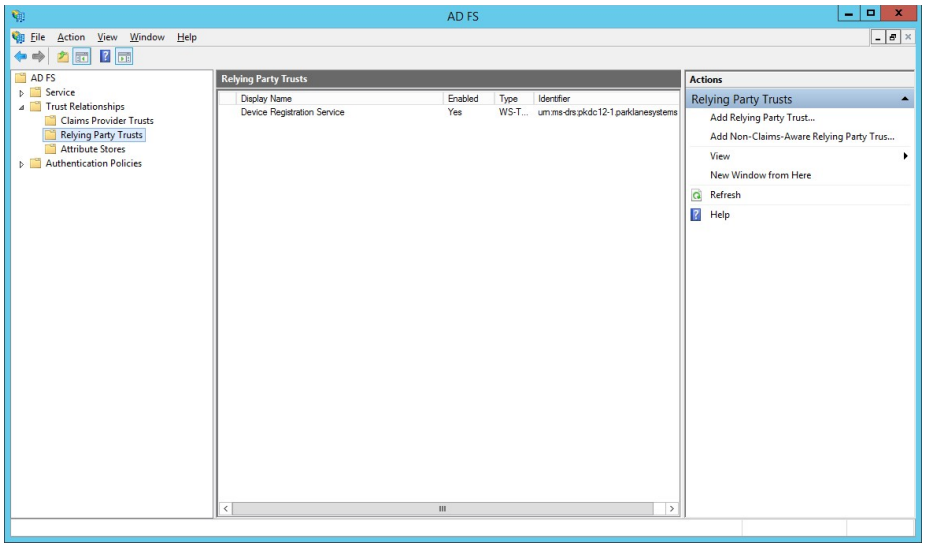
Therefore we recommend re-querying the Metadata URL in KICS after you have completed the setup.

On-Premises ADFS Server: Setting up the Relaying Party Trust

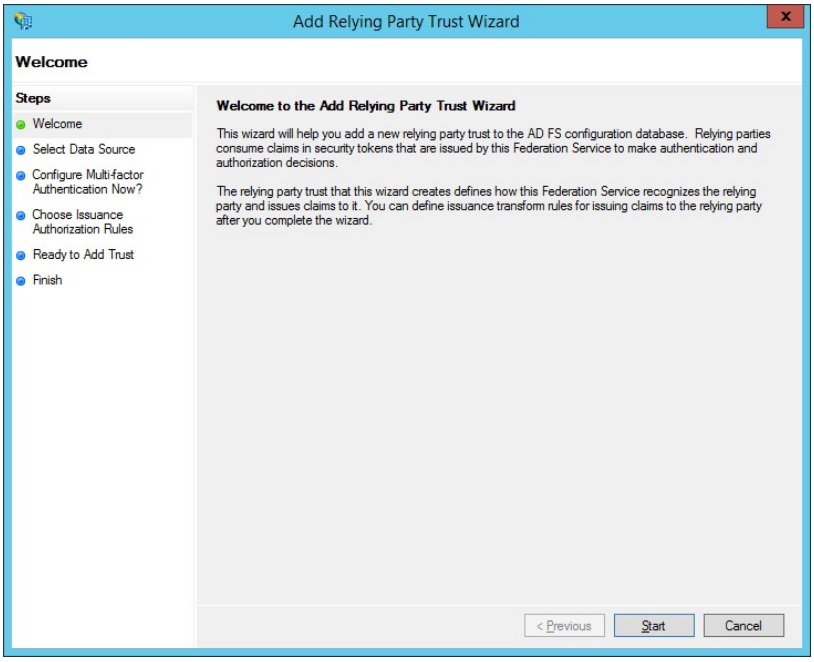
Under Step 4, copy the **Service Provider Metadata URL** (In Blue) for your next step.



Log into your ADFS Federation Server
Open up **Administrator tools > AD FS Management**

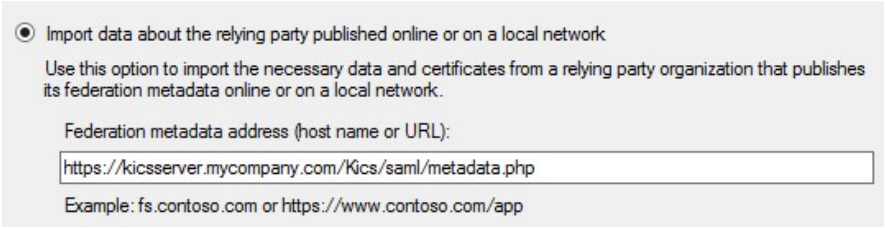


Go to **AD FS > Trust Relationships > Relying Party Trusts**
Click **Add Relying Party Trust**



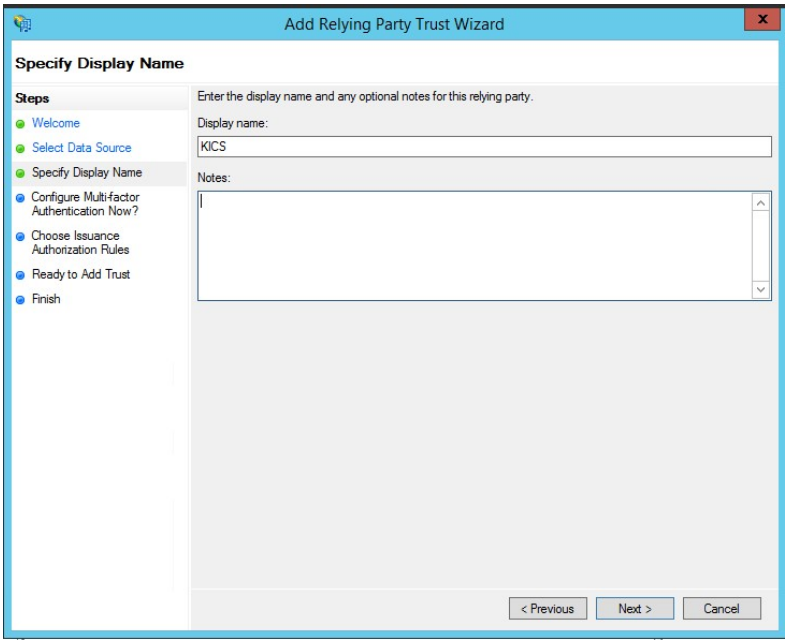
Click **Start**

Select **Import data about the relying party published online or on a local network**
Paste in the metadata URL from KICS into the **Federation metadata address** field



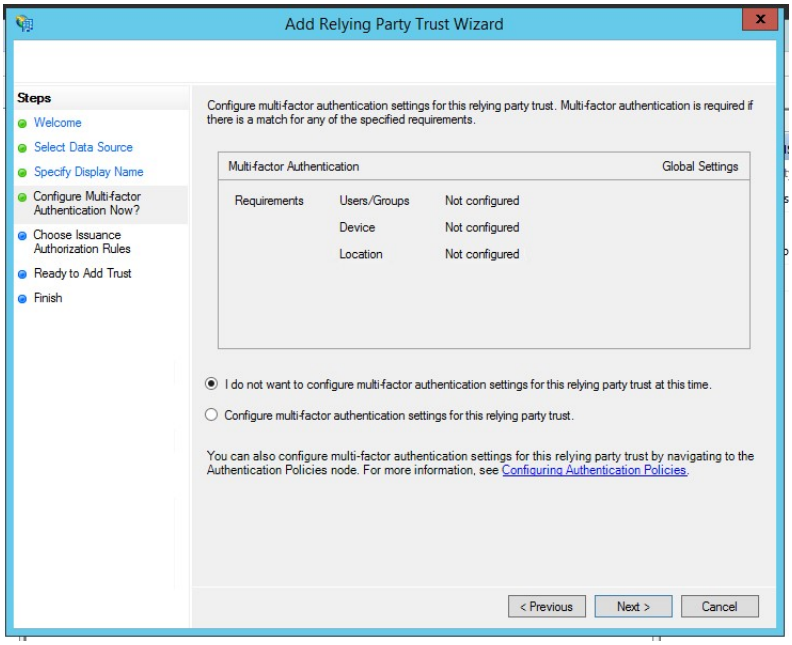
Click **Next >**

NOTE: If you receive an error at this point, you need to go back to KICS and click **Save Changes** on the SAML Authentication Settings Page.



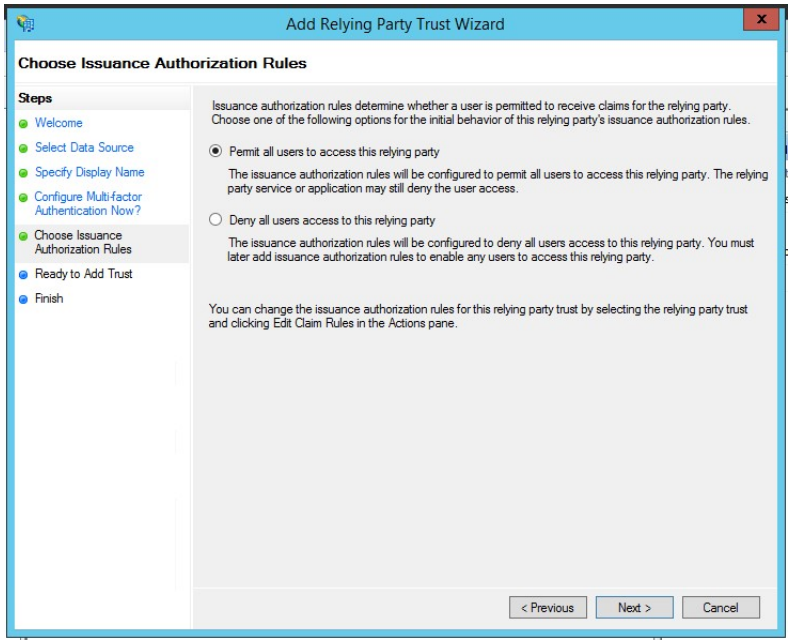
Assign a Display Name (such as KICS), or leave as-is

Click **Next**



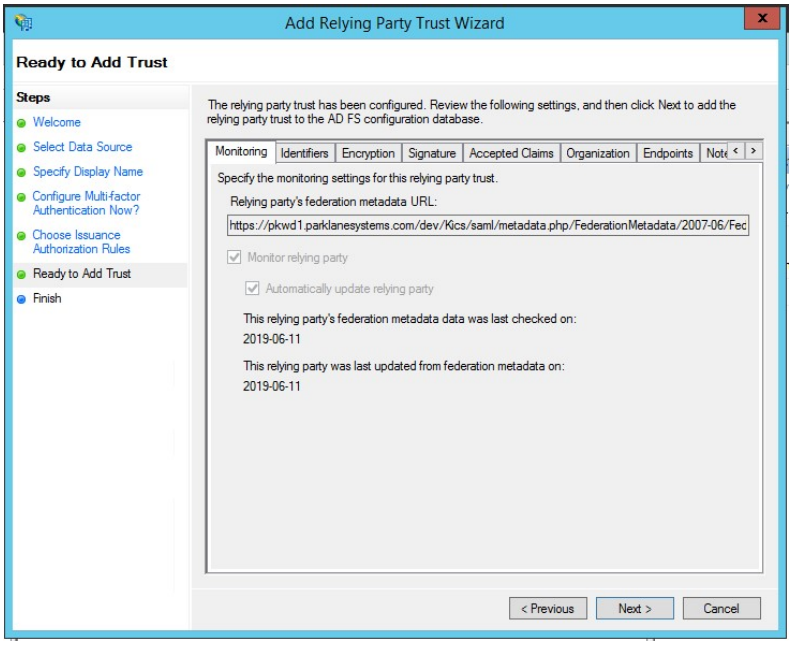
If your organization requires multi-factor configuration, you can set it up here.

Otherwise, click **Next >**



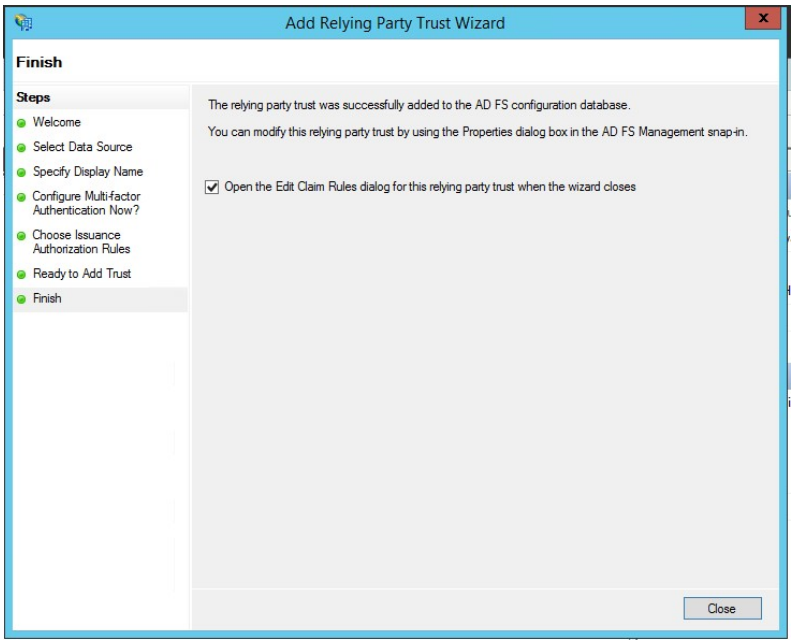
Select **Permit all users to access this relying party**

Click **Next >**



Review the provisioned settings

Click **Next >**



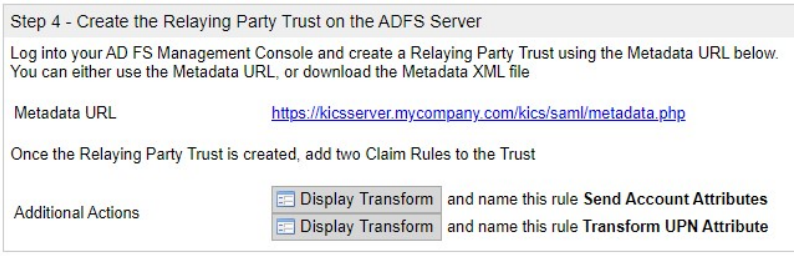
On the last page, keep "**Open the Edit Claim Rules dialog**" option checked

Click **Close**

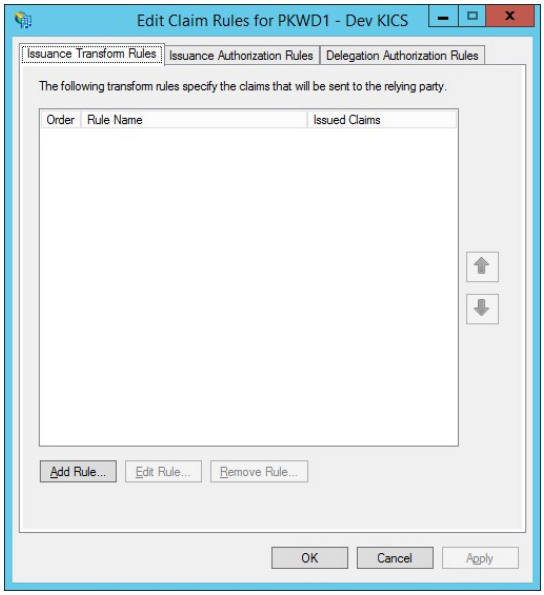
On-Premises ADFS Server: Setting up the Transform Rules

We now need to add rules to the Federation Server in order to provide the correct attributes to KICS. This includes the User's account name, serial number, email address, first name, last name, and group membership. We also need to inform the Federation Server of the specifications for the account name.

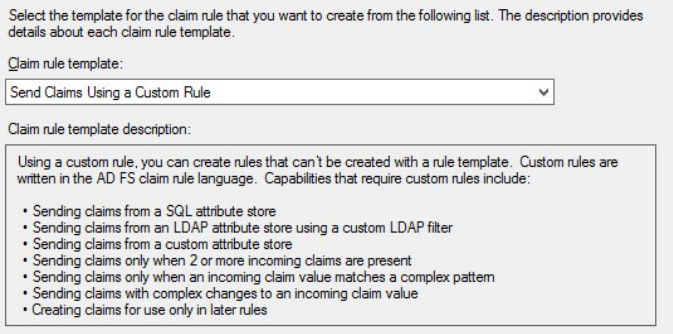
On the KICS ADFS Settings Page, you will see two buttons for displaying the Transforms that will be configured.



On the ADFS Server, you should have the "Edit Claim Rules" dialog open.
(If not, right-click the Relying Party Trust under AD FS and select **Edit Claim Rules**)



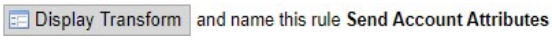
Under the **Issuance Transform Rules** tab, click **Add Rule**



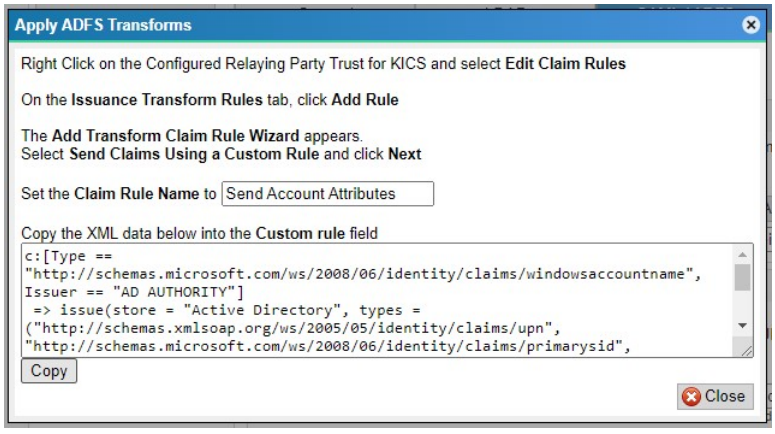
Select **Send Claims Using a Custom Rule**

Click **Next >**

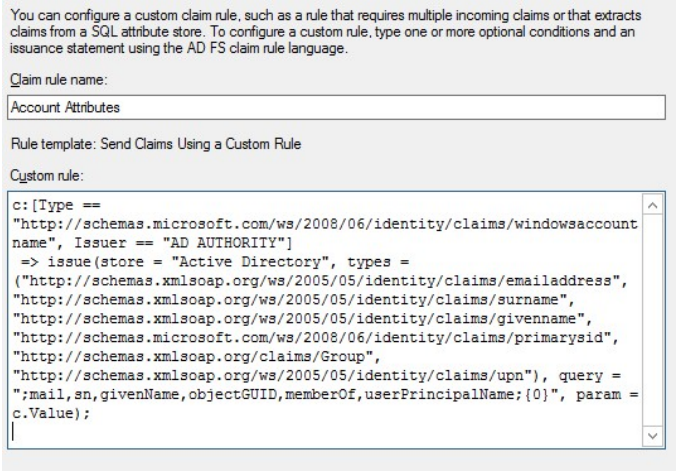
On the **KICS ADFS Settings** page, select the first **Display Transform** button



Select **Copy**

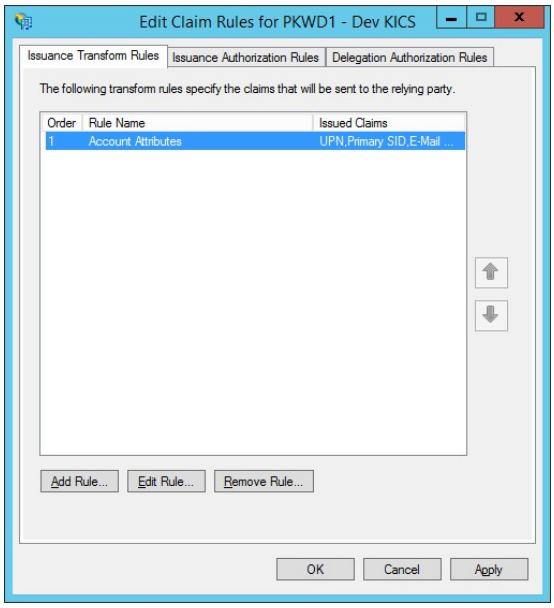


Paste the XML Data into the **Custom Rule** entry box on the ADFS Server

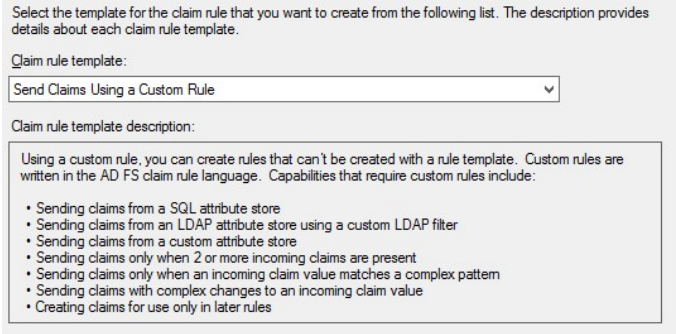


Give the rule a name, such as "**Account Attributes**"

Click **Finish**

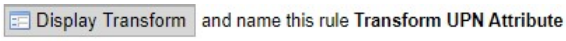


Under the **Issuance Transform Rules** tab, click **Add Rule**

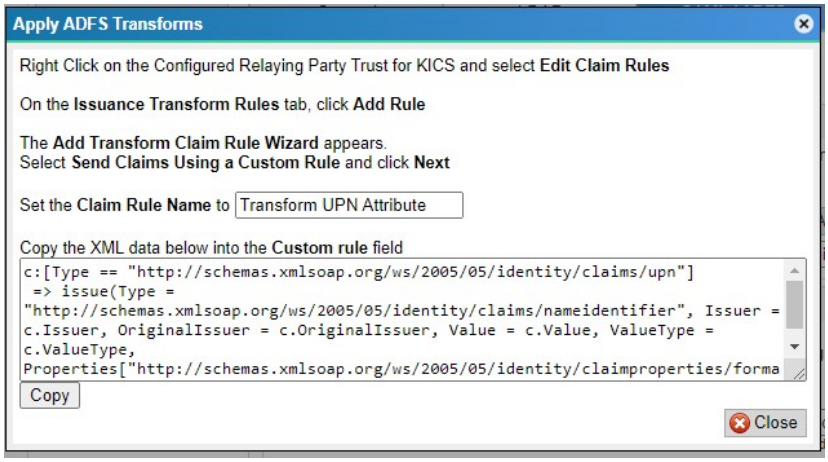


Select **Send Claims Using a Custom Rule**

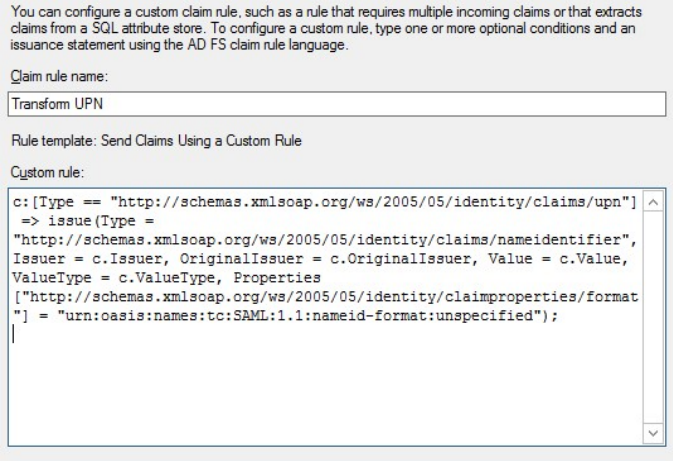
On the **KICS ADFS Settings** page, select the second **Display Transform** button



Select **Copy**

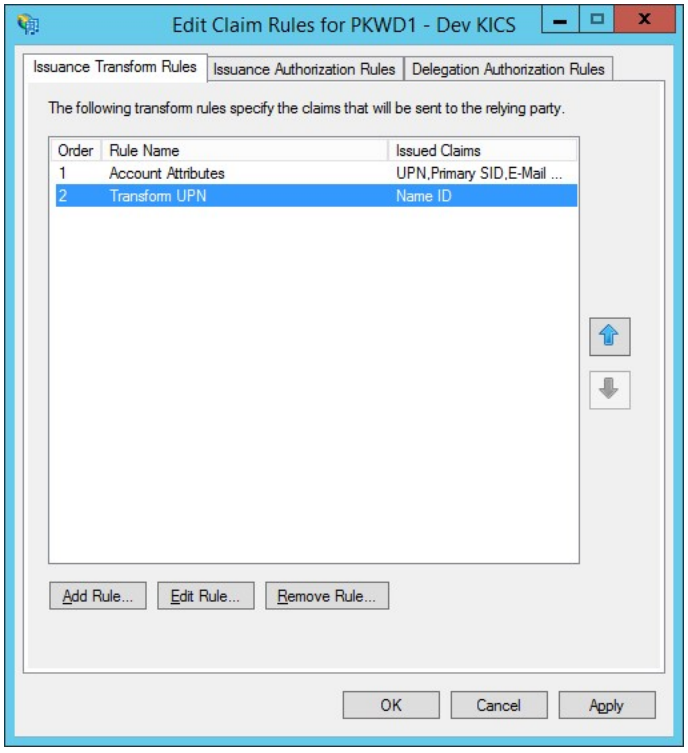


Paste the XML Data into the **Custom Rule** entry box on the ADFS Server



Set the Claim Rule name to **Transform UPN**

Click **Finish**



The two rules have been created. Click **OK**.

parklane SYSTEMS

Azure AD: Setting up the Relaying Party Trust

Under Step 4, copy the **Service Provider Metadata URL** (In Blue) for your next step.

Open the Azure Active Directory Admin Center and refer to the following URL to add an application for Federated Services:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-setup-sso

Ensure that the Application has User Attributes & Claims configured for:

- givenname
- surname
- emailaddres
- name

Change the primary KICS authentication method to Federated Services

At this point, ADFS has been configured.

On the **System Settings - Authentication - General** page, change the **Primary Authentication Method** over to **SAML/ADFS**.

To test the sign in process, you can retain your administrator session by opening an Incognito window and attempt to sign in.