

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.

Status:	Installed
CN:	SP - pkwd1
Expiry	2020-06-11
Fingerprint	8a9f460def422264cb48075c7f32e8a7797d17c4
Fingerprint	48cfe9cf9dafde67f3b4fcb7ee6a6c46b92be24f7ebec208c9470c52cffc2437

Certificate Generated Successfully. Please review and download for your IDP

Click **Close**

Setting up the Federated Services Attributes

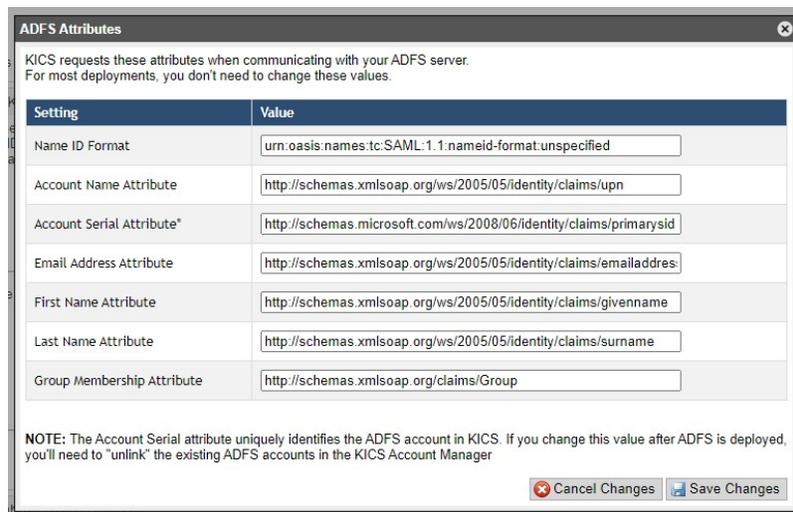
On-Premises ADFS and Azure AD use different attributes, so you will need to confirm the appropriate attributes for your deployment.

Launch the Attribute Editor

Requested Attributes



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**

 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.

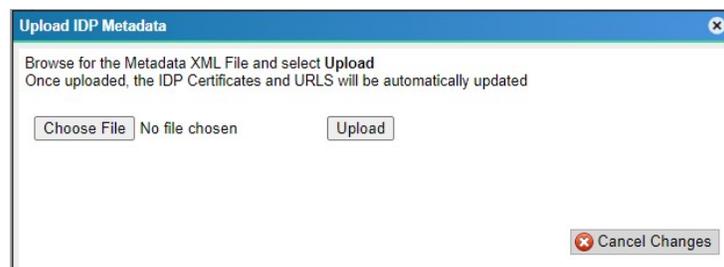
Metadata URL:	<input type="text" value="https://adfs.mycompany.com/FederationMetadata/2007-06/Federati"/> <small>example: https://servername/FederationMetadata/2007-06/FederationMetadata.xml</small>
Import IDP Settings	<input type="button" value="Query Metadata URL"/> or <input type="button" value="Upload Metadata XML File"/>

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.

ADFS IDP Certificate	Certificate Installed <input type="button" value="Certificate Actions"/>
Entity ID / URL	<input type="text" value="https://dc.mycompany.com/adfs/services/trust"/> <small>example: https://servername/adfs/services/trust</small>
Sign-On URL	<input type="text" value="https://dc.mycompany.com/adfs/ls/"/> <small>example: https://servername/adfs/ls/</small>
Log-Out URL	<input type="text" value="https://dc.mycompany.com/adfs/ls/?wa=wsignout1.0"/> <small>example: https://servername/adfs/ls/?wa=wsignout1.0</small>

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.

Additional Options

- Automatically Check IDP Metadata Daily for new Certificates
- Automatically Check IDP Metadata Daily for new URLs

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.

Step 4 - Create the Relaying Party Trust on the ADFS Server

Log into your AD FS Management Console and create a Relaying Party Trust using the Metadata URL below. You can either use the Metadata URL, or download the Metadata XML file

Metadata URL <https://kicsserver.mycompany.com/kics/saml/metadata.php>

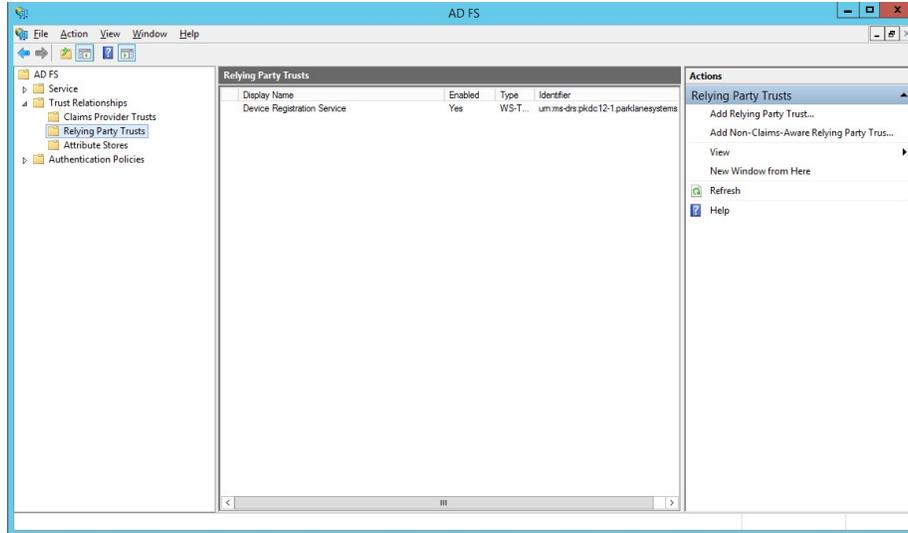
Once the Relaying Party Trust is created, add two Claim Rules to the Trust

Additional Actions

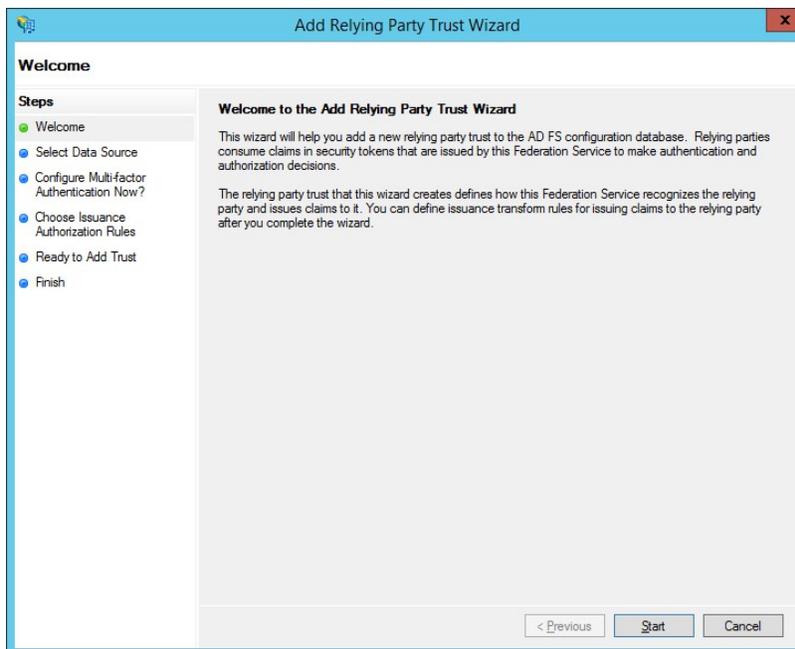
 Display Transform	and name this rule Send Account Attributes
 Display Transform	and name this rule Transform UPN Attribute

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

Import data about the relying party published online or on a local network

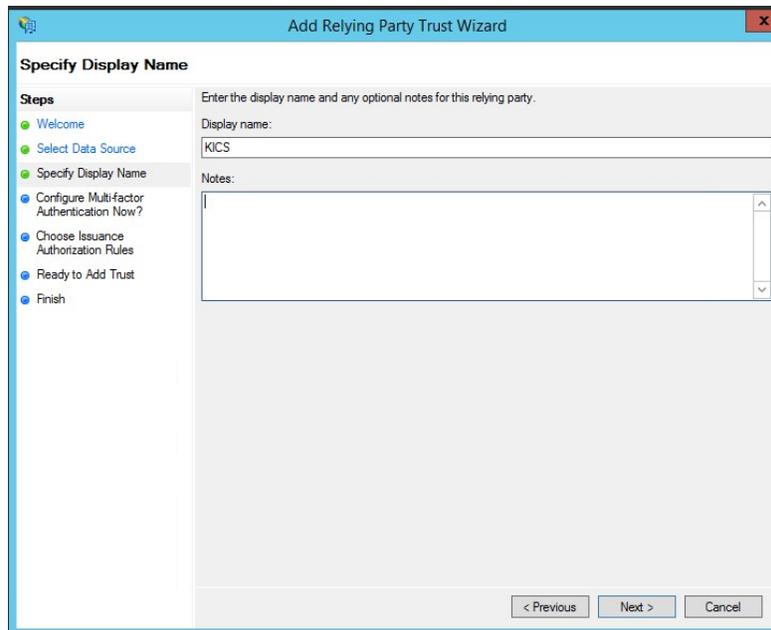
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

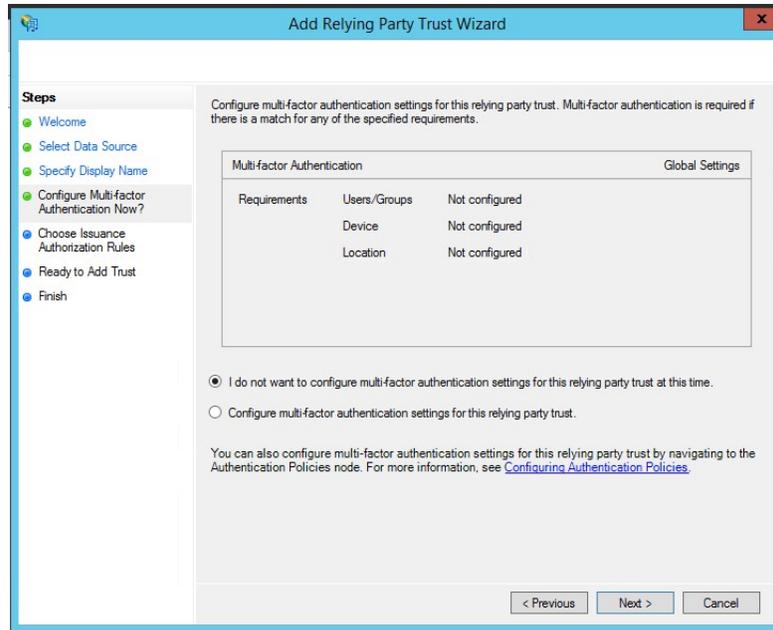
Click **Next >**

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.



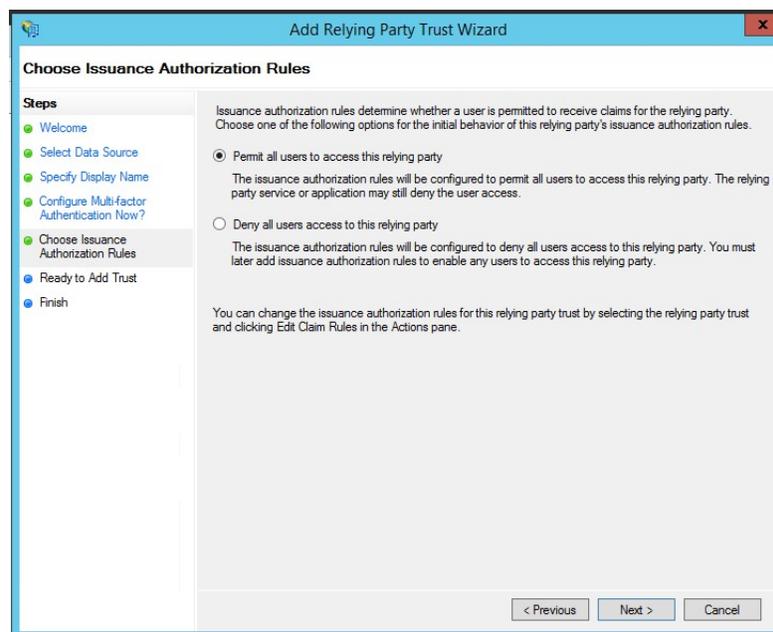
Assign a Display Name (such as KICS), or leave as-is

Click **Next**



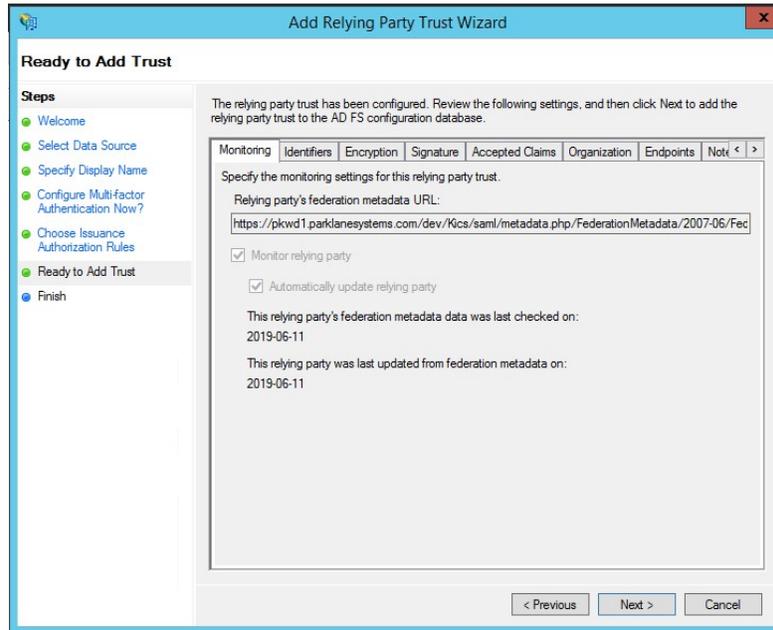
If your organization requires multi-factor configuration, you can set it up here.

Otherwise, click **Next >**



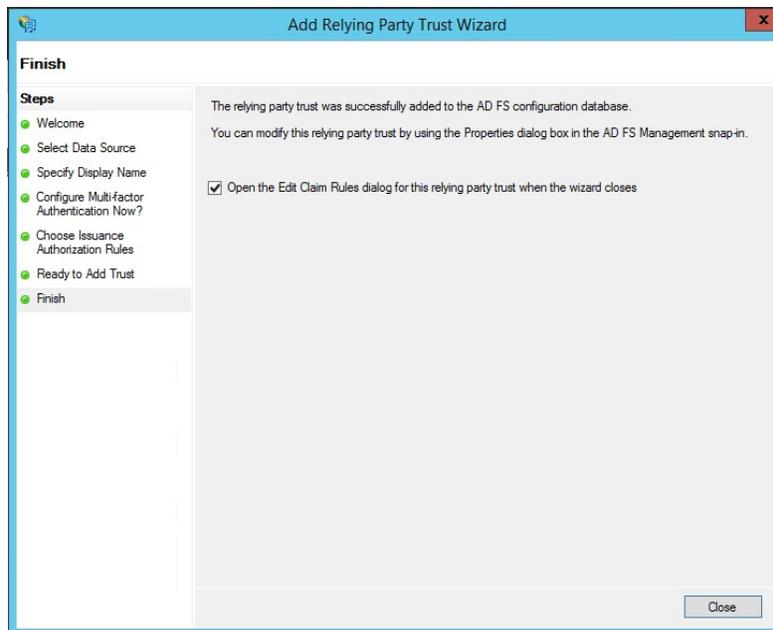
Select **Permit all users to access this relying party**

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.

Step 4 - Create the Relaying Party Trust on the ADFS Server

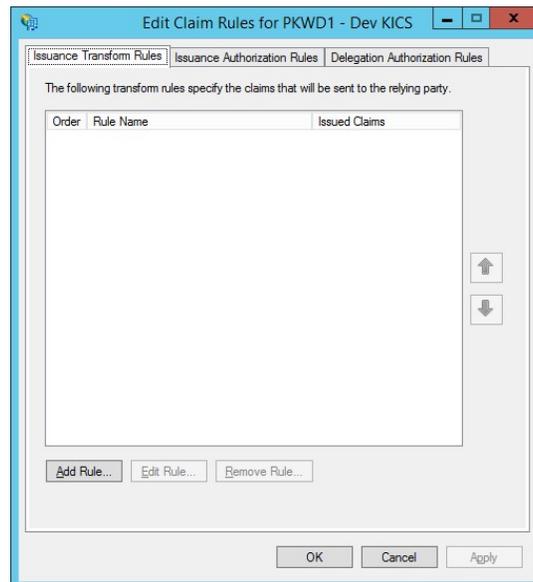
Log into your AD FS Management Console and create a Relaying Party Trust using the Metadata URL below. You can either use the Metadata URL, or download the Metadata XML file

Metadata URL <https://kicsserver.mycompany.com/kics/saml/metadata.php>

Once the Relaying Party Trust is created, add two Claim Rules to the Trust

Additional Actions and name this rule **Send Account Attributes**
 and name this rule **Transform UPN Attribute**

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 the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

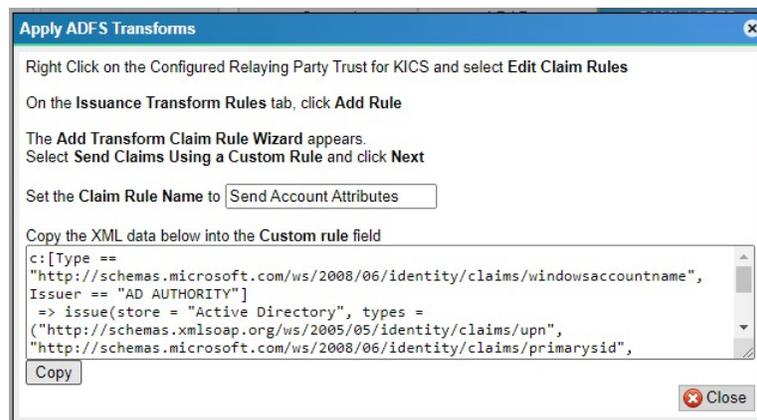
Select **Send Claims Using a Custom Rule**

Click **Next >**

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

 **Display Transform** and name this rule **Send Account Attributes**

Select **Copy**



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

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
Account Attributes

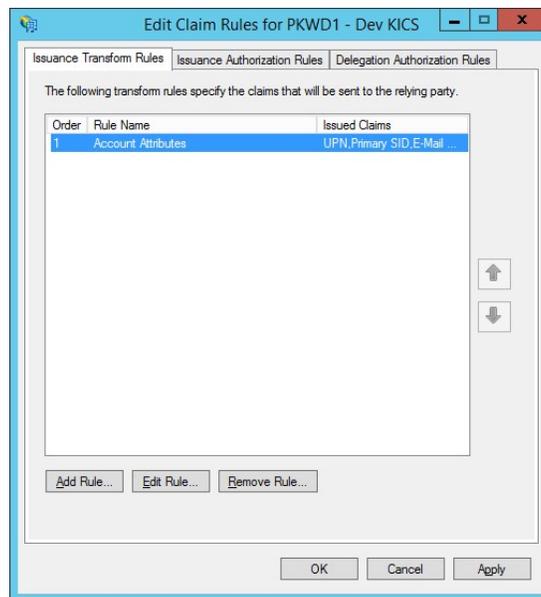
Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount  
name", Issuer == "AD AUTHORITY"]  
=> issue(store = "Active Directory", types =  
(("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname",  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname",  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid",  
"http://schemas.xmlsoap.org/claims/Group",  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =  
";mail,sn,givenName,objectGUID,memberOf,userPrincipalName;{0}", param =  
c.Value);
```

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

Click **Finish**



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

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

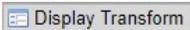
Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

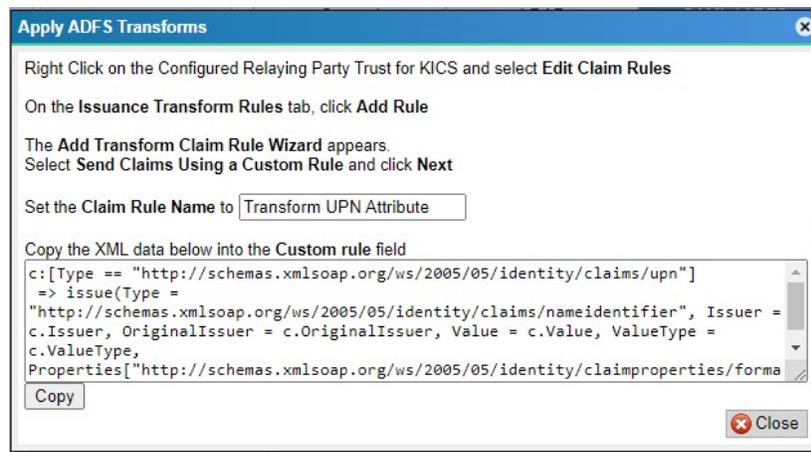
- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

Select **Send Claims Using a Custom Rule**

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

 and name this rule **Transform UPN Attribute**

Select **Copy**



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

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

Transform UPN

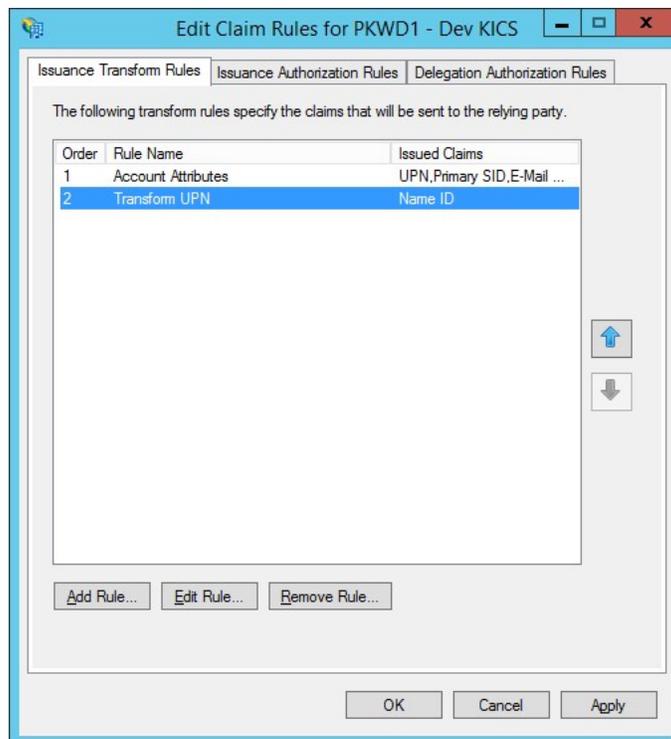
Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"] => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```

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

Click **Finish**



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

Azure AD: Setting up the Relaying Party Trust

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

Step 4 - Create the Relaying Party Trust on the ADFS Server

Log into your AD FS Management Console and create a Relaying Party Trust using the Metadata URL below. You can either use the Metadata URL, or download the Metadata XML file

Metadata URL <https://kicsserver.mycompany.com/kics/saml/metadata.php>

Once the Relaying Party Trust is created, add two Claim Rules to the Trust

Additional Actions and name this rule **Send Account Attributes**
 and name this rule **Transform UPN Attribute**

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
- emailaddress
- 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.