

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



General Information	Authentication Settin	ngs						
Authentication	The following settings define how	v users can authenticate to k	ICS.	ication Mathed is con	foured you can cha	upporthe authentication method below		
Regional Information								
Branding	Authentication Methods		_					
Auditing	General Lo	cal LDAP	SAML / ADFS	Group Import	User Import	Secondary Auth		
Email Configuration	To configure Federated Service	es, follow the steps below.						
Form Settings								
Self-Hosted	Step 1 - KICS Service Provider (SP) Settings							
External Forms	You will need to generate a S Click the Certificate Actions	Service Provider (SP) Certific	ate for KICS to commun	icate with your ADFS	Server.			
Parklane Integration	Citer are continente Actions	batton to generate a certain						
SQL Export	KICS SP Certificate Act Generated 🔹 Certificate Actions							
License	Requested Attributes	E Launch Attribut	e Editor					
	Step 2 - Configure KICS for	or the ADFS Identity Provi	der (IDP)					
	Specify your ADFS Server's You can import your IDP's ce If neither option is available,	Metadata URL Below. rtificate and URLS by queryi the IDP settings can be spec	ng the Metadata URL or ified manually	by uploading the Met	adata XML file.			
	Metadata URL:	example: https://servern	name/FederationMetadata/20	07-06/FederationMetadat	a.xml			
	Import IDP Settings duery Metadata URL or 🐥 Upload Metadata XML File							
	ADFS IDP Certificate Entity ID / URL	Certificate Not Four	nd or Invalid 📦 Certifi	cate Actions				
	Sign-On URL	example: https://serveri	name/adfs/services/trust					
	Log-Out URL	example: https://serveri example: https://serveri	name/adfs/ls/ name/adfs/ls/?wa=wsignout1.	0				
	Addtional Options	Automatically C	heck IDP Metadata Daily heck IDP Metadata Daily	/ for new Certificates / for new URLs				
	Step 3 - Save the above A	DFS Settings						
					🔚 Save (Changes		
	Step 4 - Create the Relayi	ng Party Trust on the ADF	S Server					
	Log into your AD FS Manage You can either use the Metad	ment Console and create a data URL, or download the N	Relaying Party Trust usir letadata XML file	ig the Metadata URL	below.			
	Metadata URL	https://myserver.my	company.com/kics/saml/	metadata.php				
	Once the Relaying Party Tru:	st is created, add two Claim	Rules to the Trust					
	Additional Actions	Display Transfe	orm and name this rule orm and name this rule	Send Account Attril Transform UPN Attr	outes ibute			

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

KIOD OD O- HE-sta	Cartificate Nat Concepted	Cartificate Actions
KIUS SP Certificate	Certificate Not Generated	Certificate Actions

A Dialog for the Service Provider Certificate will appear



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

Service Pr	ovider Certific	ate		
Status:	Installed			
CN:	SP - pkwd1	SP - pkwd1		
Expiry	2020-06-11			
Fingerprint	8a9f460def422	264cb48075c7f32e8a77	797d17c4	
Fingerprint	48cfe9cf9dafd	e67f3b4fcb7ee6a6c46b9	2be24f7ebec208c9470c	:52cffc2437
- Downlo	ad Certificate	₭ Renew Certificate	Delete Certificate	

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

E Launch Attribute Editor

The Attribute Editor will display

etting	Value
ame ID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
ccount Name Attribute	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
ccount Serial Attribute*	http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid
mail Address Attribute	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddres
irst Name Attribute	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
ast Name Attribute	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
roup Membership Attribute	http://schemas.xmlsoap.org/claims/Group

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:	https://adfs.mycompany.com/FederationMetadata/2007-06/Federatik example: https://servername/FederationMetadata/2007-06/FederationMetadata.xml			
Import IDP Settings	🐥 Query Metadata URL or 🐥 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.

- Upload Metadata XML File

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
Entity ID / URL	https://dc.mycompany.com/adfs/services/trust
	example: https://servername/adfs/services/trust
Sign-On URL	https://dc.mycompany.com/adfs/ls/
	example: https://servername/adfs/ls/
Log-Out URL	https://dc.mycompany.com/adfs/ls/?wa=wsignout1.0
	example: https://servername/adfs/ls/?wa=wsignout1.0

Copyright ©2022 Parklane Systems Inc. All rights reserved. Proprietary and Confidential - Not for distribution



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.

Addtional 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.



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



\$		AD FS		_ _ ×
🗌 File Action View Window Help				- 0 ×
🗢 🔿 🙇 📰 🖬 🗊				
AD FS	Relying Party Trusts			Actions
Service In the service of	Display Name	Enabled	Type Identifier	Relying Party Trusts
Claims Provider Trusts	Device negliciation Service	Tes	W3-1 diministars.pkdc.rz-r.parkiaresystem	Add Relying Party Trust
Attribute Stores				Add Non-Claims-Aware Relying Party Trus
Authentication Policies				View F
				Refrech
				7 Help
				- rep
		ш	>	

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):	
	https://kicsserver.mycompany.com/Kics/saml/metadata.php	
	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.

\$	Add Relying Party Trust Wizard
Specify Display Nan	ne
Steps	Enter the display name and any optional notes for this relying party.
Welcome	Display name:
Select Data Source	KICS
Specify Display Name	Notes:
Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules	
Ready to Add Trust	
e Frish	
	< Previous Next > Cancel

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

Click Next



Steps Welcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance	Configure multi-factor at there is a match for an Multi-factor Authen	uthentication settings y of the specified requ tication	for this relying party trust. Multi-fa irrements.	ctor authentication is required if
Authorization Rules Ready to Add Trust Finish 	requirements	Users/Groups Device Location	Not configured Not configured Not configured	according and
	I do not want to co Configure multi-fact You can also configur Authentication Policie	nfigure multi-factor au or authentication sett e multi-factor authen s node. For more inf	thentication settings for this relying ngs for this relying party trust. tication settings for this relying (ormation, see <u>Configuring Authe</u> < Previous	party trust at this time. xarty trust by navigating to the trication Policies. Next > Cancel

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.

ng Party Trust on the ADFS Se	erver
ment Console and create a Rela ata URL, or download the Metad	ying Party Trust using the Metadata URL below. lata XML file
https://kicsserver.mycom	pany.com/kics/saml/metadata.php
t is created, add two Claim Rule	s to the Trust
E Display Transform	and name this rule Send Account Attributes
Display Transform	and name this rule Transform UPN Attribute
	g Party Trust on the ADFS So ment Console and create a Rela ata URL, or download the Metad https://kicsserver.mycom t is created, add two Claim Rule

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. @Jaim 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 Sending claims from an USAP 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 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

E 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.

<u>Claim rule name:</u>	
Account Attributes	_
Rule template: Send Claims Using a Custom Rule	
Custom rule:	
c:[Type ==	1
<pre>"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/givenname", "http://schemas.xmlsoap.org/ws/2008/06/identity/claims/givenname", "http://schemas.xmlsoap.org/ws/2008/06/identity/claims/primarysid", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/primarysid", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query = ";mail.sn.givenName.objectGUID.memberOf.userPrincipalName;[0]", param = c.Value);</pre>	
	~

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

Click Finish

🖗 Edi	it Claim Rules for PKWD1 - Dev KICS 📃 💻	x
Issuance Transform Rules	Issuance Authorization Rules Delegation Authorization Rules	
The following transform r	rules specify the claims that will be sent to the relying party.	
Order Rule Name	Issued Claims	
1 Account Attribu	outes UPN,Primary SID,E-Mail	
Add Rule Edit h	Rule	
	OK Cancel Apply	

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.

<u>C</u> laim 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 temp written in the AD FS claim rule language. Capabilities that require custom rules i	late. Custom rules are 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 patter Sending claims with complex changes to an incoming claim value Creating claims for use only in later rules 	m

Select Send Claims Using a Custom Rule

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

E Display Transform and name this rule Transform UPN Attribute

Select Copy

Right Click on the Configured Relaying Party Trust for KICS and select Edit Claim R	lules
On the Issuance Transform Rules tab, click Add Rule	
The Add Transform Claim Rule Wizard appears. Select Send Claims Using a Custom Rule and click Next	
Set the Claim Rule Name to Transform UPN Attribute	
Copy the XML data below into the Custom rule field	
<pre>c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims => issue(Type =</pre>	s/upn"]
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidenti	ifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, Val	LueType =
c.varuerype,	conecties/forma

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:	
<pre>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");</pre>	< >

Set the Claim Rule name to Transform UPN

Click Finish

御	Edit	t Claim Rules for PKWI	D1 - Dev KICS	
Issuance 7	ransform Rules	Issuance Authorization Rules	Delegation Authorization I	Rules
The follo	wing transform n	ules specify the claims that will l	be sent to the relying party.	
Order	Rule Name		Issued Claims	1
1	Account Attribu	ites	UPN, Primary SID, E-Mail	
2	Transform UPN		Name ID	
Add F	ule	Rule		₽
		OF	Cancel	Apply

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.



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-setupsso

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.