

THE WI-FI PERFORMANCE COMPANY

Microsoft ADFS 3.0 Configuration Guide for the 7SIGNAL Mobile Eye Dashboard

Microsoft ADFS 3.0 Configuration

<u>Relying Party Trust implementation for 7SIGNAL SSO</u>

This configuration guide will walk through the steps to configure Active Directory Federation Services 3.0 (Windows Server 2012R2) to work with the 7SIGNAL Mobile Eye Dashboard. It is worth noting that your Active Directory domain and forest functional version may be different that your ADFS version. For instance, this test was done leveraging a Microsoft Active Directory domain running Windows 2016 for both forest and domain functional levels while still implementing the ADFS services at version 3.0 which comes as part of Window Server 2012R2. To get started, open the AD FS Management console and navigate to the Relying Party Trusts area under Trust Relationships. This is where you will add 7SIGNAL for the SAML authentication to be allowed.



From here you will want to click "Add Relying Party Trust..." from the Actions menu which will kick off the following wizard.

\$	Add Relying Party Trust Wizard
Welcome	
 Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
	< Previous Start Cancel

Click Start to continue

For the Data Source selection, switch the setting to the manual option at the bottom.

\$	Add Relying Party Trust Wizard
Select Data Source	
Steps • Welcome • Select Data Source • Specify Display Name • Choose Profile • Configure Certificate • Configure URL • Configure Identifiers • Configure Multifactor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	Select an option that this wizard will use to obtain data about this relying party: 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.
	< Previous Next > Cancel

Fill in the display name for the Trust and a description/notes as desired

\$	Add Relying Party Trust Wizard
Specify Display Name	
Steps	Enter the display name and any optional notes for this relying party.
Welcome	Display name:
Select Data Source	7Signal
Specify Display Name	Notes:
Choose Profile	7Signal Mobile Eye Dashboard
Configure Certificate	
Configure URL	
Configure Identifiers	
Configure Multi-factor Authentication Now?	
 Choose Issuance Authorization Rules 	
Ready to Add Trust	
🥥 Finish	
	< Previous Next > Cancel

Since we will be leveraging SAML 2.0 for this relationship, leave the default of AD FS profile selected.

\$	Add Relying Party Trust Wizard					
Choose Profile						
Steps	This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate					
Welcome	configuration profile for this relying party trust.					
Select Data Source	AD <u>F</u> S profile					
Specify Display Name	This profile supports relying parties that are interoperable with new AD FS features, such as					
Choose Profile	security token encryption and the SAML 2.0 protocol.					
Configure Certificate	○ AD FS 1.0 and 1.1 profile					
Configure URL	This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.					
Configure Identifiers						
Configure Multi-factor Authentication Now?						
 Choose Issuance Authorization Rules 						
Ready to Add Trust						
🥥 Finish						
	< Previous Next > Cancel					

Use the Browse button to select the 7SIGNAL certificate file provided. View the details to validate it if desired.

\$	Add Relying Party Trust Wizard					
Configure Certificate						
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to it. To specify the certificate, click Browse. Isuer: E-support@7signal.com, 0=7SIGNAL, L=Independence, S=Ohio, C=US Subject: E-support@7signal.com, 0=7SIGNAL, L=Independence, S=Ohio, C=US Effective date: 6/28/2019 4:18:46 PM Expiration date: 6/27/2022 4:18:46 PM View Browse Remove					

Once again, since we will be leveraging SAML 2.0, check the bottom option to enable support for this and input the SAML 2.0 SSO service URL provided by 7SIGNAL.

\$	Add Relying Party Trust Wizard
Configure URL	
Steps Velcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Finat protocol is always enabled for a relying party. □ Enable support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL:

Here we need to input the Entity ID as provided by 7SIGNAL. This is the unique identifier which tells ADFS which 3rd party the SSO request is coming from to ensure the proper Trust details are used in terms of certificate associated and claims to provide.

\$	Add Relying Party Trust Wizard	×
Configure Identifiers		
Steps	Relving parties may be identified by one or more unique identifier strings. Specify the identifiers	for this relving
Welcome	party trust.	
Select Data Source	Relying party trust identifier:	
Specify Display Name		Add
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust	<u></u>
Configure Certificate	Relying party trust identifiers:	
Configure URL	https://login.7signal.com/mobile	Remove
 Configure Identifiers 		
Configure Multi-factor Authentication Now?		
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
Finish		
	< Previous Next >	Cancel

The next page deals with Multi-Factor Authentication and whether that will be configured and enforced for users or devices trying to authenticate against ADFS. You may want to leverage this for your environment, but it is outside of the scope of this document and will be left disabled.

\$	Add Relying Party Trust Wizard
Steps	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if
⊖ Welcome	there is a match for any of the specified requirements.
Select Data Source	
Specify Display Name	Multi-factor Authentication Global Settings
Choose Profile	Requirements Users/Groups Not configured
Configure Certificate	Device Not configured
Configure URL	Location Not configured
Configure Identifiers	
Configure Multi-factor Authentication Now?	
 Choose Issuance Authorization Rules 	
 Ready to Add Trust Finish 	 I do not want to configure multifactor authentication settings for this relying party trust at this time. Configure multifactor authentication settings for this relying party trust. You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.
	< <u>P</u> revious <u>N</u> ext > Cancel

The Authorization Rules page is another way for you to decide how granular you want your services to be. For the purposes of this guide, we will leave it at the default to Permit all users in the Active Directory domain to access this relying party we are defining.

\$	Add Relying Party Trust Wizard						
Choose Issuance Authorization Rules							
Steps	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party.						
 Welcome Select Data Source 	Permit all users to access this relying party						
 Specify Display Name Choose Profile 	The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.						
 Configure Certificate 	○ <u>D</u> eny all users access to this relying party						
Configure URL	The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.						
Configure Identifiers							
Authentication Now?	You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking. Edit Claim Bules in the Actions page						
 Choose Issuance Authorization Rules 							
 Ready to Add Trust Finish 							
	< <u>P</u> revious <u>N</u> ext > Cancel						

This will bring us to the page summarizing all settings made to this point. You can click through the various tabs to review things if you like.

19	Add Relying Party Trust Wizard						
Ready to Add Trust							
Steps The rely • Welcome Image: Select Data Source • Specify Display Name Image: Select Data Source • Choose Profile Image: Choose Profile • Configure Certificate Image: Configure URL • Configure Identifiers Image: Configure Multifactor Authentication Now? • Choose Issuance Authorization Rules Image: Choose Issuance Ready to Add Trust • Finish Image: Choose Issuance Ready to Add Trust	e relying party trust has been configured. Review the following settings, and then click Next to add the ing party trust to the AD FS configuration database. onitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Not < pecify 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 >						

This completes adding the Relying Party Trust. By default, the Wizard will Open the Claims Rules to allow us to continue by defining that relationship.

\$	Add Relying Party Trust Wizard
Finish	
Steps	The relying party trust was successfully added to the AD FS configuration database.
Welcome	You can modify this relying party trust by using the Properties dialog box in the AD ES Management snap-in
Select Data Source	
Specify Display Name	
Choose Profile	Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
Configure Certificate	
Configure URL	
Configure Identifiers	
Configure Multi-factor Authentication Now?	
 Choose Issuance Authorization Rules 	
Ready to Add Trust	
🥥 Finish	
	Qlose

Click Close and the Edit Claims Rules window for the Trust should open

Here we will add an Issuance Transform Rule to send the appropriate Active Directory attribute in response to the SAML SSO request if the user authenticates successfully.

Ş			Edit	Claim R	ules fo	r 7Signal		_		x
Iss	Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules									
	The follo	owing transform n	iles speci	ify the clair	ns that will	l be sent to t	he relying p	arty.		
	Order	Rule Name				Issued Clair	ns			
										_
									1	
										-
	Add F	Rule Edit P	lule	Remove	Rule				1	
					0	К	Cancel		Арр	ły

Click Add Rule and the following window will open

There are different templates you may choose from but for the purposes of this guide, we will assume LDAP user object Attributes will be used as 7SIGNAL looks for the user's email address to associate them to the proper details in the Mobile Eye dashboard.

\$	Add Transform Claim Rule Wizard
Select Rule Template	
Select Rule Template Steps Choose Rule Type Configure Claim 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. Qaim rule template: Send LDAP Attributes as Claims Send Group Membership as a Claim Transform an Incoming Claim Pass Through or Filter an Incoming Claim Send Claims Using a Custom Rule multiple claims tfrom a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	< Previous Next > Cancel

For the Claim Rule definition, you will provide a Rule name, select Active Directory as your LDAP attribute store, choose your LDAP Attribute and then the Outgoing Claim Type it will map to.

In this test environment, we did not have Microsoft Exchange Server or O365 configured so we chose to leverage the User Principal Name and send that as the Email Address claim. You may want to map the Active Directory Email Address attribute as your LDAP attribute if that is the field that matches the expected value on the 7SIGNAL side.

\$		Add Transform Claim Rule	Wizard
Configure Rule			
Steps • Choose Rule Type • Configure Claim Rule	You ca which issued Qlaim r AD UF Rule te Attribut Active	an configure this rule to send the values of L to extract LDAP attributes. Specify how the from the rule. ule name: ?N to Email address emplate: Send LDAP Attributes as Claims te <u>store</u> : Directory ng of LDAP attributes to outgoing claim type LDAP Attribute (Select or type to add more) User-Principal-Name	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be s: Outgoing Claim Type (Select or type to add more) E-Mail Address
			< <u>P</u> revious Finish Cancel

Click Finish since 7SIGNAL is only looking for this one claim to be passed

This takes you back to the overall Claim Rules screen showing your one rule you just added. You can explore the other tabs available on this window, but no changes are necessary based on how we configured things thus far.

•	💱 Edit Claim Rules for 7Signal 🗕 🗖 🗙										
	Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules										
	The following transform rules specify the claims that will be sent to the relying party.										
		Order	Rule Name				Issued Clain	ns]	
		1	AD UPN to Em	ail address	3		E-Mail Addr	ess			
											_
										1	<u>-</u>
											- 1
											7
		Add B)ula Edit E	lula	Remove	Rula					
		<u>A</u> uu n		uie	<u>n</u> emove	andie					
	OK Cancel Apply										

Click OK to close this Claims Rules window out

We now see our Relying Party Trust listed and it is enabled by default



<u>Gathering our AD FS details for 7SIGNAL to configure</u> <u>their side</u>

In order to configure and/or retrieve the details of our AD FS implementation, we navigate to the Service folder in the AD FS Management console and choose "Edit Federation Service Properties" from the Actions menu or by right-clicking the Service folder.



This brings up the properties of our implementation of ADFS as show below. You will need to provide 7SIGNAL with the Federation Service ID from the 3rd field below.

Federation Service Properties	x						
General Organization Events <u>F</u> ederation Service display name:	_						
Tech Carolinas LAB]						
Example: Fabrikam Federation Service							
Federation Service name:							
adfs30.lab.techcarolinas.com							
Example: fs.fabrikam.com							
Fe <u>d</u> eration Service identifier:	,						
https://adfs30.lab.techcarolinas.com/adfs/services/trust							
Example: http://fs.fabnkam.com/adfs/services/trust							
Web SSO lifetime: 480 - minutes							
OK Cancel Apply							

On the Organization tab, all of our enabled services will need to be reachable by way of the Organization URL so we need to make note of this and ensure any firewalls or other security measures are configured to allow traffic through to this server address.

Federation Service Properties						
General Organization Events						
Organization						
Publish organization information in federation metadata						
Organization display name:						
Tech Carolinas Lab						
Organization URL:						
https://adfs30.lab.techcarolinas.com/						
Support contact information in federation metadata <u>First name:</u>						
Email address:						
Telephone number:						
OK Cancel Apply						

If we navigate to Service and then Endpoints in the AD FS Management utility, we can see that by default, the SAML 2.0 service is at the path /adfs/ls/. This path appended to the Organization URL from the previous page is another piece of information to be given to 7SIGNAL.

			AD FS					
<u>Action View W</u> indow	<u>H</u> elp							-
2 📰 🛽 🖬								
FS	Endpoints							Actions
Service	Enabled	Proxy Enabled	URL Path	Туре	Authentication Type	Security Mode	^	Endpoints
Endpoints	Token Iss	uance				1.000.00		View
	Yes	Yes	/adfs/ls/	SAML 2.0/WS-Federation	Anonymous	Transport		
Claim Descriptions	No	No	/adfs/services/trust/2005/windows	WS-Trust 2005	Windows	Message		New Window from
Trust Relationships	No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005	Windows	Mixed		Q Refresh
Claims Provider Trusts	Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005	Windows	Transport		
Relying Party Trusts	No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005	Certificate	Message		Пер
Attribute Stores	Yes	Yes	/adfs/services/trust/2005/certificatemixed	WS-Trust 2005	Certificate	Mixed		/adfs/ls/
Authentication Policies	Yes	Yes	/adfs/services/trust/2005/certificatetransport	WS-Trust 2005	Certificate	Transport		Dischla an Deser
Per Relying Party Trust	No	No	/adfs/services/trust/2005/usemame	WS-Trust 2005	Password	Message	=	Disable on Proxy
	No	No	/adfs/services/trust/2005/usemamebasictransport	WS-Trust 2005	Password	Transport		Disable
	Yes	Yes	/adfs/services/trust/2005/usemamemixed	WS-Trust 2005	Password	Mixed		Help
	Yes	No	/adfs/services/trust/2005/kerberosmixed	WS-Trust 2005	Kerberos	Mixed		
	No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic256	WS-Trust 2005	SAML Token (Asym	Message		
	No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic25	WS-Trust 2005	SAML Token (Asym	Message		
	Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedasymmetricba	WS-Trust 2005	SAML Token (Asvm	Mixed		
	No	No	/adfs/services/trust/2005/issuedtokenmixedasymmetricba	WS-Trust 2005	SAML Token (Asym	Mixed		
	Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi	WS-Trust 2005	SAML Token (Svm	Mixed		
	No	No	/adfs/services/tnust/2005/issuedtokenmixedsymmetricbasi	WS-Trust 2005	SAML Token (Svm	Mixed	1.1	
	No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256	WS-Trust 2005	SAML Token (Sym.	Message		
	No	No	/adfs/services/trust/2005/issuedtokensymmetrichasic/256s	WS-Trust 2005	SAML Token (Sym	Message		
	No	No	/adfs/services/trust/2005/issuedtokensymmetrictrioledes	WS-Trust 2005	SAML Token (Sym	Message		
	No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledess	WS-Trust 2005	SAMI Token (Sym	Message		
	No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictrinl	WS-Trust 2005	SAMI Token (Sym	Mixed		
	No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl	WS-Trust 2005	SAMI Token (Sym	Mixed		
	Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberns	Mixed		
	No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate	Message		
	Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate	Mixed		
	No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate	Transport		
	No	No	/adfs/services/trust/13/usemame	WS-Trust 1.3	Password	Message		
	No	No	/adfs/services/trust/13/usemamebasictransport	WS-Trust 1.3	Password	Transport		
	Yes	Yes	/adfs/services/trust/13/usemamemixed	WS-Trust 1.3	Password	Mixed		
	No	No	/adfs/services/trust/13/issuedtokenasymmetrichasio256	WS-Trust 13	SAMI Token (Amm	Message		
	No	No	/adfe/een/cee/hist/13/seuedtokenae/mmeticbasic256	WS.Truet 13	SAMI Token (Asm	Massage	-	

Testing the Services

Assuming both sides are configured at this point, we will begin to validate the solution. In this instance, we will be navigating to the login URL given by 7SIGNAL where we put in the email address of a user who has been configured for access to the Dashboard.



Clicking login will redirect us over to our AD FS site appending our SAML Request ID as part of the path. Here we login using our Active Directory User ID and credentials.

Sign In	× +		🗙 – 🗠 🗙
← → ♂ @	🛛 🔞 https://adfs30.lab.techcarolinas.co	m/adfs/ls/?SAMLR 🛛 🕶 🔽 🏠	II\ 🗊 📽 🐌 😑
		Tech Carolinas LAB	
VX		Sign in with your organizational account	
		justin@lab.techcarolinas.com	D)
		••••••	131
		Sign in	
		© 2013 Microsoft	

Upon successful authentication against Active Directory, you will be redirected back to the 7SIGNAL Mobile Eye dashboard with appropriate access and visibility as assigned.