

#### THE WI-FI PERFORMANCE COMPANY

## Microsoft ADFS 4.0 Configuration Guide for the 7SIGNAL Mobile Eye Dashboard

# Microsoft ADFS 4.0 Configuration

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

This configuration guide will walk through the steps to configure Active Directory Federation Services 4.0 (Windows Server 2016) 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 also implementing the AD FS services at version 4.0 on a different server running Window Server 2016. Other version combinations can exist and work together though configuration details may change. 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 W	ïzard	×
Welcome		
Welcome Steps Welcome Select Data Source Choose Access Control Policy Ready to Add Trust Finish	<ul> <li>Welcome to the Add Relying Party Trust Wizard</li> <li>Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more</li> <li>@ glaims aware</li> <li>Mon claims aware</li> </ul>	
	< <u>P</u> revious <u>Start</u> Cance	I

Leave the radio button for "Claims aware" selected and click the Start button to continue

For the Data Source selection, choose the middle option to "Import data about the relying party from a file" and then browse to the copy of the XML metadata file provided by 7SIGNAL.

🇌 Add Relying Party Trust W	izard	×
Select Data Source		
Steps	Select an option that this wizard will use to obtain data about this relying party:	
Welcome	Import data about the relying party published online or on a local network	
Select Data Source	Use this option to import the necessary data and certificates from a relying party organization that publish	ies
<ul> <li>Choose Access Control Policy</li> </ul>	its federation metadata online or on a local network.	
Ready to Add Trust	<u>F</u> ederation metadata address (host name or URL):	
Finish	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 no validate the source of the file.	ıt
	Federation metadata file location:	
	C:\Users\Administrator\Desktop\SAML-sp-metadata-prod.xml	
	Enter data about the relying party manually	
	Use this option to manually input the necessary data about this relying party organization.	
	< <u>P</u> revious <u>N</u> ext > Cancel	

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

翰 Add Relying Party Trust W	/izard	Х
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:	
<ul> <li>Choose Access Control Policy</li> </ul>	7SIGNAL MobileEye Dashboard SAML SSO	^
Ready to Add Trust		
Finish		
		~
	< Previous Next > Cancel	

The Access Control Policy page is another way for you to decide how granular you want your services to be. For the purposes of this guide, we will choose the existing "Permit Everyone" policy from the list which allows any user in the Active Directory domain to access the relying party application we are defining.

翰 Add Relying Party Trust Wi	zard		$\times$
Choose Access Control	Policy		
Steps	Choose an access control policy:		
<ul> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Access Control Policy</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	Choose an access control policy:          Name         Permit everyone         Permit everyone and require MFA         Permit everyone and require MFA for specific group         Permit everyone and require MFA from extranet access         Permit everyone and require MFA from unauthenticated devices         Permit everyone and require MFA, allow automatic device registr         Permit everyone for intranet access         Parmit specific group            Policy         Permit everyone	Description Grant access to everyone. Grant access to everyone and requir Grant access to everyone and requir Grant access to the intranet users and Grant access to everyone and requir Grant access to the intranet users. Grant access to the intranet users.	
	I do not want to configure access control policies at this time. No application.	user will be permitted access for this	
	< <u>P</u> rev	rious <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. These will include imported certificates for encryption and signing of authentication requests, the relying party trust identifier URL, the SAML endpoint service URL and other details.

🍿 Add Relying Party Trust W	fizard	×
Ready to Add Trust		
Steps	The relying party trust has been configured. Review the following settings, and then click Next to add the	
Welcome	relying party trust to the AD FS configuration database.	
Select Data Source	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note	۲
Specify Display Name	Specify the monitoring settings for this relying party trust.	
<ul> <li>Choose Access Control Policy</li> </ul>	Relying party's federation metadata URL:	
Ready to Add Trust		
• Finish	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 >	
	< <u>P</u> revious <u>N</u> ext > Cancel	

This completes adding the Relying Party Trust to our AD FS environment. By default, the Wizard will open the Claims Issuance Policy configuration.

훾 Add Relying Party Trust W	/izard X
Finish	
Steps  Welcome  Select Data Source  Specify Display Name  Choose Access Control Policy  Ready to Add Trust  Finish	The relying party trust was successfully added.
	Close

Click Close and this will launch the Claims Issuance Policy configuration and allow us to define our Claims Transform rule.

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 against AD FS.

Edi	t Claim	Issuance Polic	y for 7SIG	NAL				×
Iss	uance T	Transform Rules						
1	The follo	wing transform n	ules specify	/ the claims t	hat will be s	ent to the relying p	oarty.	
	Order	Rule Name			Issue	ed Claims		
[	<u>A</u> dd R	<b>lule</b> <u>E</u> dit F	Rule	<u>R</u> emove Ru	ıle			
				[	OK	Cancel	A	pply

Click the "Add Rule..." button to get started.

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 MobileEye dashboard.

🏟 Add Transform Claim Rule	Wizard	×
Select Rule Template		
Steps	Select the template for the claim rule that you want to create from the following list. The description provides	
Choose Rule Type	details about each claim rule template.	
Configure Claim Rule	<u>Claim</u> rule template:	
	Send LDAP Attributes as Claims $\qquad \checkmark$	
	Claim rule template description:	
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from 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.	
	< <u>Previous</u> <u>Next</u> > 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.

훾 Add Transform Claim Rule	Wizard		×		
Configure Rule					
Steps	You can	configure this rule to send the values of LD	AP attributes as claims. Select an attribute store from which		
Choose Rule Type	from the	rule.	s will map to the outgoing claim types that will be issued		
Configure Claim Rule	<u>C</u> laim rul	e name:			
	Active I	Directory UPN to Email Address			
	Rule ten	nplate: Send LDAP Attributes as Claims			
	Attribute	store:			
	Active	Directory	~		
	<u>M</u> apping	g of LDAP attributes to outgoing claim types			
	LDAP Attribute (Select or type to add more)         Outgoing Claim Type (Select or type to add more)				
	•	User-Principal-Name 🗸 🗸	E-Mail Address 🗸 🗸		
	•	~	~		
			< Previous Finish Cancel		

Click Finish since this is the only Claim we need to be passed to the MobileEye dashboard.

This takes you back to the overall Claim Issuance Policy screen showing your one rule you just added.

Edit Claim Issuance Policy for 7SIGNAL	×
Issuance Transform Rules	
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
1 Active Directory UPN to Email Address E-Mail Address	
	-
Add Rule Edit Rule Remove Rule	
OK Cancel	Apply

Click OK to close this Claim Issuance Policy 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 3<sup>rd</sup> field below.

Federation Service Properties X
General Organization Events
Eederation Service display name:
Tech Carolinas Lab Services
Example: Fabrikam Federation Service
Federation Service name:
fs.lab.techcarolinas.com
Example: fs.fabrikam.com
Federation Service identifier:
https://fs.lab.techcarolinas.com/adfs/services/trust
Example: http://fs.fabrikam.com/adfs/services/trust
Web SSO lifetime (minutes):
Enable delegation for service administration
Delegate name:
Edit
Allow Local System account for service administration
Allow Local Administrators group for service administration
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.

General       Organization       Events         Organization <ul> <li>Publish organization information in federation metadata</li> <li>Organization display name:</li> <li>Tech Carolinas LAB</li> <li>Organization URL:</li> <li>(<ul> <li>(<ul></ul></li></ul></li></ul>		
Organization ✓ Publish organization information in federation metadata Organization display name: Tech Carolinas LAB Organization URL: fttps://fs.lab.techcarolinas.com/ Support contact information in federation metadata First name: Last name: Email address: Telephone number:		
Publish organization information in federation metadata         Organization display name:         Tech Carolinas LAB         Organization URL:         Ittps://fs.lab.techcarolinas.com/         Support contact information in federation metadata         First name:		
Organization display name:         Tech Carolinas LAB         Organization URL:         Ittps://fs.lab.techcarolinas.com/         Support contact information in federation metadata         First name:	n federation metadata	
Egendation deploy name:         Tech Carolinas LAB         Organization URL:         Introstrict information in federation metadata         First name:         Last name:         Email address:         Telephone number:		
Organization URL:          Ittps://fs.lab.techcarolinas.com/         Support contact information in federation metadata         First name:         Last name:         E-mail address:         Ielephone number:		
Support contact information in federation metadata		
Support contact information in federation metadata	2	
Support contact information in federation metadata	1	
Support contact information in reperation metadata	an and data	
Eirst name:  Last name:  E-mail address:  Ielephone number:	on metadata	
Last name:  E-mail address:  Ielephone number:		
Last name:  Email address:  Telephone number:		
E-mail address:  Telephone number:		
E-mail address:		
elephone number:		
_elephone number:		

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								- 🗆 X
翰 <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow	<u>H</u> elp							_ <i>8</i> ×
🗢 🏟 🖄 📰 🚺 🖬								
📔 AD FS	Endpoint	ts					1	Actions
✓ <sup>™</sup> Service	Enabled	Prove Enabled	IIRI Path	Tune	Authentication Type	Security Mode	56	Endpoints
Attribute Stores	criableu	Floxy Enabled	UNL Fain	Type	Autrientication Type	Security Mode	i F	10
Authentication Methods	Token Issuance					View		
Certificates	Yes	Yes	/adfs/ls/	SAML 2.0/WS-Federation	Anonymous	Transport		New Window from Here
Claim Descriptions	No	No	/adfs/services/trust/2005/windows	WS-Trust 2005	Windows	Message	117	Refrech
Device Registration	No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005	Windows	Mixed	113	G Keresh
Endpoints	Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005	Windows	Transport	111	? Help
Scope Descriptions	No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005	Certificate	Message		/adfa/la/
Web Application Proxy	Yes	Yes	/adfs/services/trust/2005/certificatemixed	WS-Trust 2005	Certificate	Mixed	11	/ auis/ is/
Access Control Policies	Yes	Yes	/adfs/services/trust/2005/certificatetransport	WS-Trust 2005	Certificate	Transport		Disable on Proxy
Relying Party Trusts	No	No	/adfs/services/trust/2005/usemame	WS-Trust 2005	Password	Message		Disable
Claims Provider Trusts	No	No	/adfs/services/trust/2005/usemamebasictransport	WS-Trust 2005	Password	Transport	11.	2 11 1
Application Groups	Yes	Yes	/adfs/services/trust/2005/usemamemixed	WS-Trust 2005	Password	Mixed	111	👔 нер
	Yes	No	/adfs/services/trust/2005/kerberosmixed	WS-Trust 2005	Kerberos	Mixed		
	No	No	/adfs/services/trust/2005/issuedtokenasymmetri	WS-Trust 2005	SAML Token (Asym	Message		
	No	No	/adfs/services/trust/2005/issuedtokenasymmetri	WS-Trust 2005	SAML Token (Asym	Message		
	Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedasy	WS-Trust 2005	SAML Token (Asym	Mixed		
	No	No	/adfs/services/trust/2005/issuedtokenmixedasy	WS-Trust 2005	SAML Token (Asym	Mixed		
	Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedsym	WS-Trust 2005	SAML Token (Sym	Mixed		
	No	No	/adfs/services/trust/2005/issuedtokenmixedsym	WS-Trust 2005	SAML Token (Sym	Mixed		
	No	No	/adfs/services/trust/2005/issuedtokensymmetric	WS-Trust 2005	SAML Token (Sym	Message	1	

In this example, our SAML 2.0 Service Endpoint URL is:

https://fs.lab.techcarolinas.com/adfs/ls/

#### And from the previous section, the Federation Service Identifier URL is:

https://fs.lab.techcarolinas.com/adfs/services/trust/

Lastly, we will also need to provide 7SIGNAL with our ADFS Signature certificate as covered in the next section. These 3 pieces of information will be used by them to setup our SAML SSO capabilities for the MobileEye Dashboard.

#### **Certificates**

Since we will be leveraging TLS certificates for encrypting and signing communications between the systems, we also need to provide 7SIGNAL with the appropriate public certificate for our AD FS services.

Although we only presented AD FS with a single self-signed certificate during setup, it assigned that for overall Service Communications and then created 2 more certificates for use in other functions as shown below.



Since we will be using the signing certificate in sending our Claim back to the 7SIGNAL system, we need to use the Certificate Export Wizard to give 7SIGNAL a copy of the public certificate file.

You can choose to View the Certificate by selecting it in the preceding screenshot.

From there, you follow the standard practice on the Certificate to "Copy to File..." from the Details tab.

😽 Certificate		×
General Details Certification Path	1	
Show: <all></all>	~	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm	V3 23 96 2d 3c fc ad 61 ac 41 47 sha256RSA sha256	
Valid from Valid from Valid to	ADFS Signing - IS.lab.techtaro Sunday, November 24, 2019 8 Monday, November 23, 2020 ADFS Signing - fs lab techtaro	~
V3		
6	dit Properties Copy to File,	5
	OK	

Walk through the Certificate Export Wizard

÷	F Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, dick Next.	
	<u>N</u> ext Cance	I

#### Choose the 'Base-64 encoded X.509 (.CER)' file format as shown below.



#### Browse to a path on the machine and give the file a name.

← <i>₽</i> Certificate Export Wizard	×	
Completing the Certificate Expo	ort Wizard	
You have successfully completed the Certificate Ex	xport wizard.	
File Name	·\/ Jeers\Administrator\Deskton\fs.Jab	
Export Keys N Export Keys N Include all certificates in the certification path N File Format Bi	o ase64 Encoded X.509 (*.cer)	
٢	>	Certificate Export Wizard X
		The export was successful.
	<u>F</u> inish Cancel	ОК

## **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	× +		😄 – 🗆 🗙
← → ♂ û	🛛 🗞 https://adfs30.lab.techcarolinas.com	n/adfs/ls/?SAMLR 🛛 🕶 🔽 🟠	II\ 🗉 🔹 🖡 😑
		Tech Carolinas LAB	
		Sign in with your organizational account	
		justin@lab.techcarolinas.com	B)
		•••••	B)
		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.