## Single Sign On Configuration for ADFS





### **Table of Contents**

1. Disclaimer and Confidentiality Notice	3
2. Executive Summary	5
3. Adding Workvivo to ADFS as a Relying Party Trust	7
4. Setting up ADFS Claim Rules	12
5. Gathering ADFS Endpoints and X.509 Certificate	15



## Disclaimer & Confidentiality Notice



l

### 1. Disclaimer & Confidentiality Notice



The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Workvivo Ltd.

> The opinions expressed are in good faith and while every care has been taken in preparing these documents, Workvivo makes no representations and gives no warranties of whatever nature in respect of these documents, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

Workvivo Ltd, its subsidiaries, the directors, employees and agents cannot be held liable for the use of and reliance of the opinions, estimates, forecasts and findings in these documents.



## **Executive Summary**



### 2. Executive Summary



This document provides guidelines on how to configure Workvivo to authenticate via Single Sign On (SSO) using Microsoft Active Directory Federation Services (ADFS) as the identity provider (IdP) solution in a SAML2 SSO configuration. The information contained in this document is intended as a guideline only – there may be significant differences in any given ADFS configuration that require a different approach to be taken.

These guidelines were written based on the configuration of an ADFS 3.0 environment running on Windows Server 2012 R2. The steps may be different on other versions of ADFS or Windows Server.



## Adding Workvivo to ADFS as a Relying Party Trust



# 3. Adding Workvivo to ADFS as a Relying Party Trust

The first step to configuring Workvivo in ADFS is to add it as a Relying Party Trust. In the ADFS Management tool, navigate to **"Trust Relationships -> Relying Party Trusts"** in the left navigation pane.

Next, click **"Add Relying Party Trust..."** in the Actions pane on the right hand side of the window. This will launch the **"Add Relying Party Trust Wizard"**.





Click the **"Start"** button to begin. On the **"Select Data Source"** screen, ensure that the option **"Import data about the relying party published online or on a local network"** is selected, and enter the following URL in the "Federated metadata address (host name or URL)" field:

#### https://[companyname].workvivo.com/saml/metadata

Note that the format of the address above may be different if your organisation has configured a custom domain name for Workvivo. If you do not know your Workvivo domain name, please contact our Support team at **support@workvivo.com for assistance.** 

Press the "Next" button to continue.

On the next screen, feel free to customise the Display name and add any relevant notes if you wish. Otherwise, click **"Next"** to move on.

For the **"Configure Multi-factor Authentication Now?"** step, leave this as the default **"I do not want to configure multi-factor authentication settings for this relying party trust at this time"** and press **"Next"**.



On the **"Choose Issuance Authorization Rules"** setting, leave it as the default "Permit all users to access this relying party" and click **"Next".** 

Ŷ	Add Relying Party Trust Wizard	X
Steps Welcome Select Data Source	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is require there is a match for any of the specified requirements.	d if
Configure Multifactor Authentication Now?     Choose Issuance Authorization Rules     Ready to Add Trust     Finish	Requirements       Users/Groups       Not configured         Device       Not configured         Location       Not configured         I do not want to configure multi-factor authentication settings for this relying party trust at this time.         Configure multi-factor authentication settings for this relying party trust.         You can also configure multi-factor authentication settings for this relying party trust by navigating to Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .	the
	< Previous Next > Cancel	

<b>\$</b>	Add Relying Party Trust Wizard
Choose Issuance A	uthorization Rules
Steps Welcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	<ul> <li>Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.</li> <li>Permit all users to access this relying party 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.</li> <li>Deny all users access to this relying party 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. You must and clicking Edit Claim Rules in the Actions pane.</li> </ul>
	< Previous Next > Cancel

On the **"Ready to Add Trust"** screen, feel free to review the settings. When you're ready to continue, press **"Next"**.



<b>\$</b>	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 span-in
Select Data Source	
Specify Display Name	
Configure Multi-factor Authentication Now?	Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
<ul> <li>Choose Issuance Authorization Rules</li> </ul>	
Ready to Add Trust	
Finish	
	Qose

On the final **"Finish"** screen, you'll see an option to **"Open the Edit Claim Rules dialog for this relying party trust when the wizard closes".** Ensure this is checked and press the **"Close"** button.

We'll cover the process of setting up claim rules in the next section.



## Setting up ADFS Claim Rules





### 4. Setting up ADFS Claim Rules

In this section, we'll cover setting up ADFS claim rules, which define what Active Directory attributes are sent by ADFS to Workvivo in a SAML2 response. This is important, as we use this to identify the user in the Workvivo database. At the end of the previous section, after you clicked the **"Close"** button, an **"Edit Claim Rules"** window should have opened.

Click the **"Add Rule"** button to launch the **"Add Transform Claim Rule Wizard"**. In the first screen, leave the default **"Send LDAP Attributes as Claims"** option selected and click **"Next"**.

Order Rule Name		ls	sued Claims	
				•
Add Rule Edit	Rule Remov	e Rule		



In the "Configure Claim Rule" screen, give the rule a name (e.g. "LDAP Email"). Select "Active Directory" from the "Attribute store" dropdown. We will create a single mapping – in the left-hand column ("LDAP Attribute") select "E-Mail-Addresses", and in the right-hand column ("Outgoing Claim Type") select "E-Mail Address". Click "Finish" to create the rule.

Next, we'll create a second rule. Click **"Add Rule"** again. This time, select "Transform an Incoming Claim" under "Claim rule template".

Give the rule a name (e.g. "Email Transform"), and select the following options:

- Incoming claim type: E-Mail Address
- Outgoing claim type: Name ID
- Outgoing name ID format: Email
- Ensure that "Pass through all claim values" is selected and press "Finish" to create the claim rule.
- At this point, you have completed the ADFS configuration and are ready to gather information from ADFS to send to Workvivo for final configuration.

<b>\$</b> 11	Add Transform Claim Rule Wizard
Configure Rule	
Steps Choose Rule Type Configure Claim Rule	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be iasued from the rule. Claim rule name: LDAP Email Rule template: Send LDAP Attributes as Claims Attribute store: Active Directory
	Mapping of LDAP attributes to outgoing claim types:           LDAP Attribute (Select or type to add more)           E-Mail-Addresses         Qutgoing Claim Type (Select or type to add more)           E-Mail-Addresses         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or type to add more)           Image: Select or type to add more)         Image: Select or
<b>Q</b>	Add Transform Claim Rule Wizard
Select Rule Templat	
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. Claim rule template: Transform an Incoming Claim V Claim rule template description: Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a rule claim with a claim value of an incoming group claim. You can also use this rule template to create a rule that will send a rule claims with the same claim value of an incoming group claim. You can also use this rule to create a group claims. While of "Purchases" When there is an incoming roup claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims, click Help.



## Gathering ADFS Endpoints & X.509 Certificate



### 5. Gathering ADFS Endpoints & X.509 Certificate

In order to configure your ADFS IdP in Workvivo, we need to gather the following information for your ADFS installation:

- ADFS Metadata Endpoint
- ADFS Single Sign On Endpoint
- ADFS Single Log Out Endpoint
- ADFS Base64 Encoded X.509 Certificate

For the first three of these options, these are usually the same on most ADFS installations. You can verify the endpoints for the Metadata and Single Sign On endpoints in the ADFS Management tool on your server. In the navigation pane on the left hand side, select **"ADFS -> Service -> Endpoints"**. You'll find the Single Sign On Endpoint under the **"Token Issuance"** section – it will have a type of **"SAML 2.0/WS-Federation"** and is typically **"/adfs/ls/"**.

The Metadataendpoint can be found under the **"Metadata"** section, has the type **"Federation Metadata"** and typically has the value **"/FederationMetadata/2007-06/** FederationMetadata.xml".

w Help						
Endpoints	i.					Actions
Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode A	Endpoints
Token Is	suance					View
Yes					Transport	View
No	No	/adfs/services/trust/2005/windows	WS-Trust 2005	Windows	Message	New Window from Here
No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005	Windows	Mixed	G Refresh
Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005	Windows	Transport	17 Halo
No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005	Certficate	Message	L Hop
Yes	Yes	/adfs/services/trust/2005/certificatemixed	WS-Trust 2005	Certficate	Moxed	/adfs/ls/
Yes	Yes	/adfs/services/trust/2005/certificatetransport	WS-Trust 2005	Certificate	Transport	Disable on Provy
No	No	/adfs/services/trust/2005/usemame	WS-Trust 2005	Password	Message	
No	No	/adfs/services/trust/2005/usemamebasietransport	WS Trust 2005	Pasoword	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	Mored	
No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic256	WS-Trust 2005	SAML Token (Asym	Message	11
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 (Aaym	Mixed	
No	No	/adfs/services/trust/2005/issuedtokenmixedasymmetricba	WS-Trust 2005	SAML Token (Asym	Mored	
Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi	WS-Trust 2005	SAML Token (Sym	Mixed	
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi	WS-Trust 2005	SAML Token (Sym	Mod	
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256	WS-Trust 2005	SAML Token (Sym	Message	
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256s	WS-Trust 2005	SAML Token (Sym	Message	
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledes	WS-Trust 2005	SAML Token (Sym	Message	
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledess	WS-Trust 2005	SAML Token (Sym	Message	
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl	WS-Trust 2005	SAML Token (Sym	Mixed	
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl	WS-Trust 2005	SAML Token (Sym	Mixed	
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberos	Moxed	
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate	Message	
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certficate	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/issuedtokenasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym	Message	
No	No	/adfs/services/trust/13/ssuedtokenasymmetricbasic256sh	WS-Trust 1.3	SAML Token (Aaym	Message	
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic	WS-Trust 1.3	SAML Token (Asym	Moved	
No	No	/adfs/services/trust/13/ssuedtokenmixedasymmetricbasic	WS-Trust 1.3	SAML Token (Aaym	Mixed	11
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2	WS-Trust 1.3	SAML Token (Sym	Mored	
No	No	/adfs/services/trust/13/ssuedtokenmixedsymmetricbasic2	WS-Trust 1.3	SAML Token (Sym	Mixed	11
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3	SAML Token (Sym	Message	
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256eha	WS-Trust 1.3	SAML Token (Sym	Message	11
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trust 1.3	SAML Token (Sym	Message	
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha	WS-Trust 1.3	SAML Token (Sym	Message	11
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trust 1.3	SAML Token (Sym	Mored	
No	No	/adts/services/trust/13/issuedtokenmixedsymmetrictripled	WS-Irust 1.3	SAML Token (Sym	Moted	
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows	Message	
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mored	11
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport	
Yes	No	/adfs/services/trusticp/windows	WS-Trust 2005	Local Windows	Message	11
No	No	/adfs/services/trust/attifactresolution	SAML-Atifact Resolution	Anonymous	Transport	
Yes	Yes	/adfs/oauth2/	OAuth	Anonymous	Transport	11
Metadat	a					
Yes	Yes	/adfs/services/hust/mex	WS-MEX	Acommous	Transport	
	149	(herderation Metartata / 200 / US/Ferderation Metardata vm)	bederation Metadata	Anonymous	Transport	11
Tes	100				the second se	

The Single Log Out endpoint does not always appear in this screen, but is typically **"/adfs/ls/?wa=wsignout1.0"**.

When sending these endpoints to Workvivo, ensure that you add the fully qualified domain name as part of the endpoint. The following show examples of what these endpoints might look like:

Туре	Endpoint
Metadata	https://[ADFS FQDN]/FederationMetadata/2007-06/Federation-Metadata.xml
Single Sign On	https://[ADFS FQDN]/adfs/ls/
Single Log Out	https://[ADFS FQDN]/adfs/ls/?wa=wsignout1.0

The final element we require to be sent to us in order to configure SSO is a Base64 encoded X.509 certificate for your ADFS configuration. On your ADFS server, open the ADFS management tool. From the left hand navigation pane, go to **"ADFS -> Service -> Certificates"**. In the main body you should see a number of certificates. Find the certificate under the heading **"Token-signing"** and right-click it, selecting **"View Certificate"** from the drop-down menu.

Select the **"Details"** tab in the window that opens and click the **"Copy to File"** button. This will open the **"Certificate Export Wizard"**. On the first screen, click **"Next"** to get started.

### 🐓 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. Next Cancel

For the Export File Format, make sure that **"Base-64** encoded X.509 (.CER)" is selected and press **"Next"**.



**Note:** some versions of ADFS may ask if you wish to export a private key – if you see this, select **"No, do not export the private key"**.

On the **"File to Export"** screen, select a location for the certificate file and give it a name (e.g. workvivo-adfs. cer). On the **"Completing the Certificate Export Wizard"** screen press **"Finish"** to close the wizard. A dialog will pop up confirming that the export was successful.

Find the certificate file you just exported. Open the file in a text editor you should see a lot of Base64 encoded text surrounded by a -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- line. The contents of this file is the certificate we require, so please send this to us along with the aforementioned endpoints.

Once you have gathered this information, please send it to your technical contact in Workvivo who will configure it in our platform and revert back to you with next steps for commencing testing of the Single Sign On configuration.





U





workvivo.com