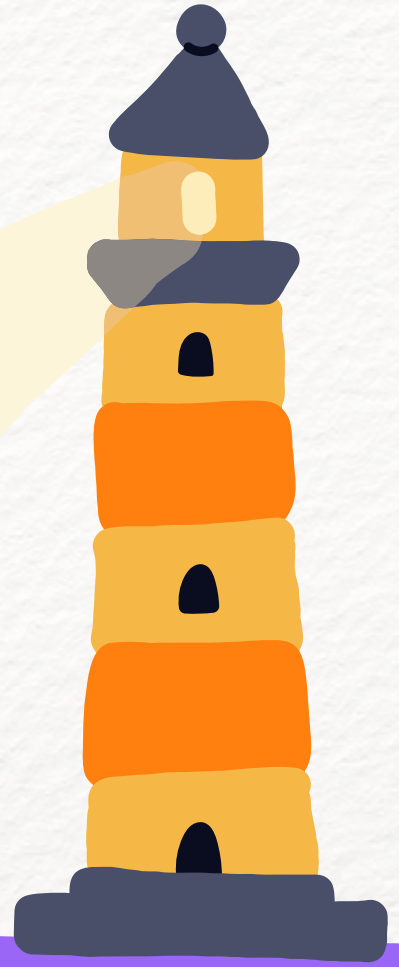
Single Sign On Configuration for ADFS

workvivo

Table of Contents



Disclaimer & Confidentiality Notice

workvivo

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.

2

Executive Summary

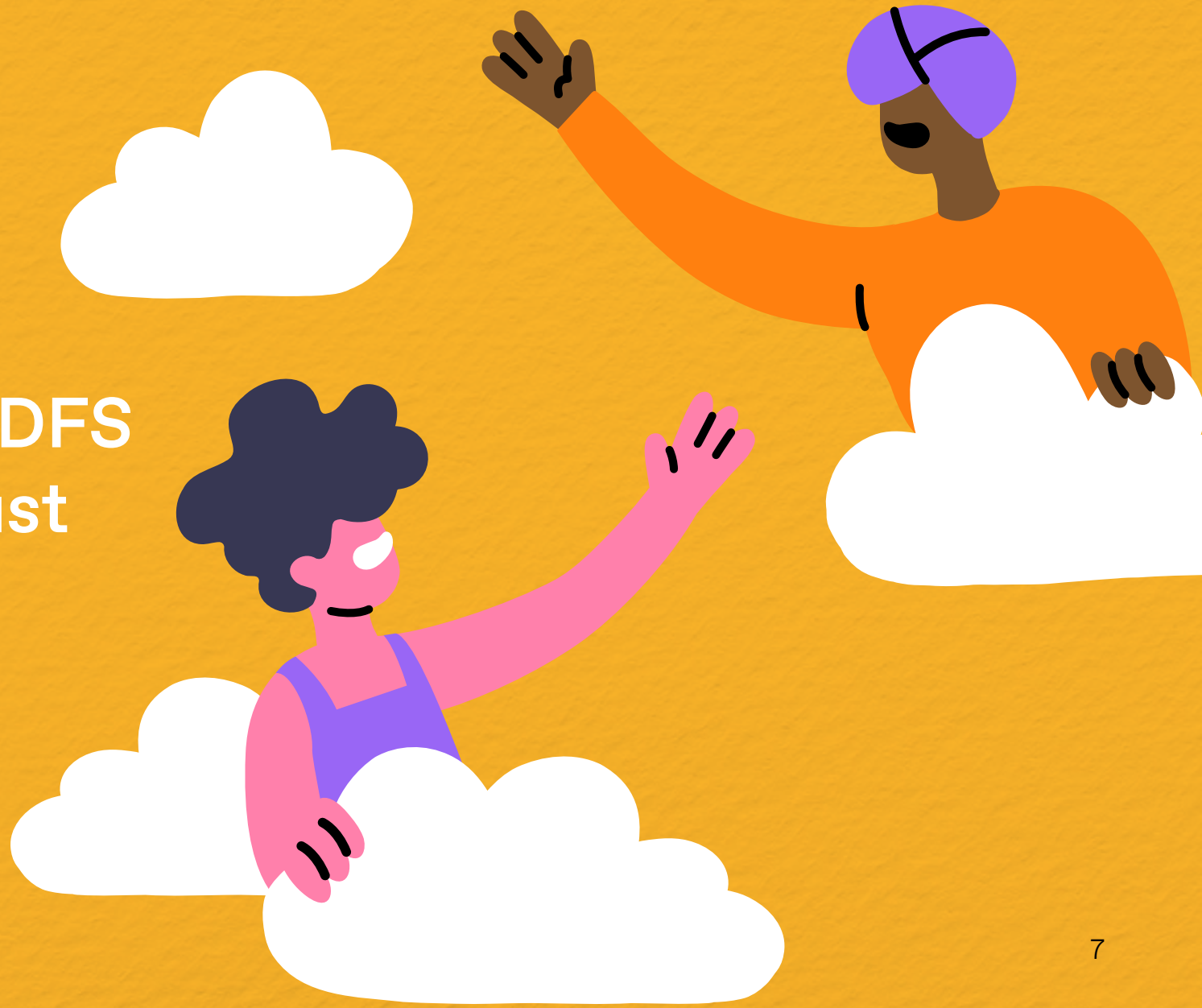
workvivo

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

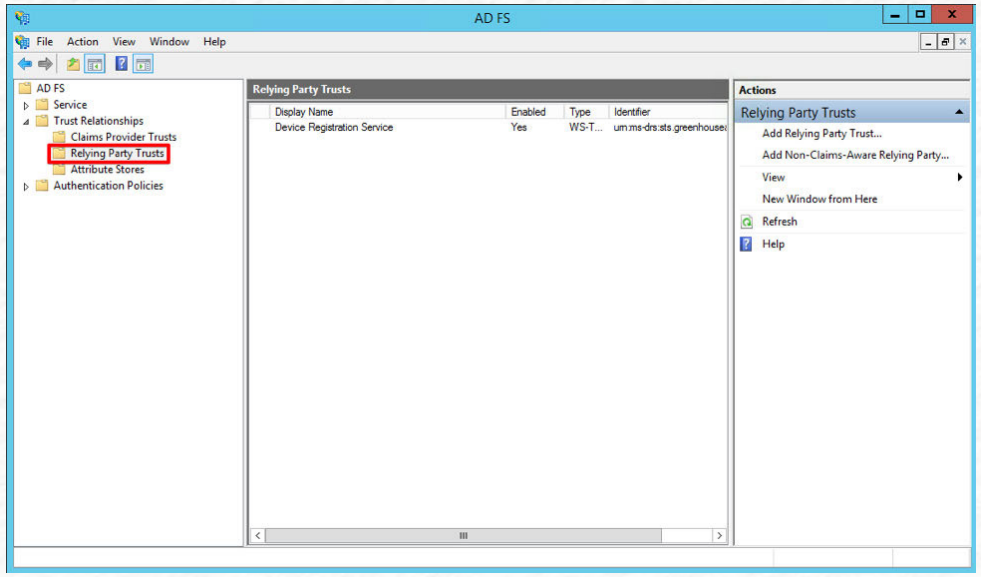


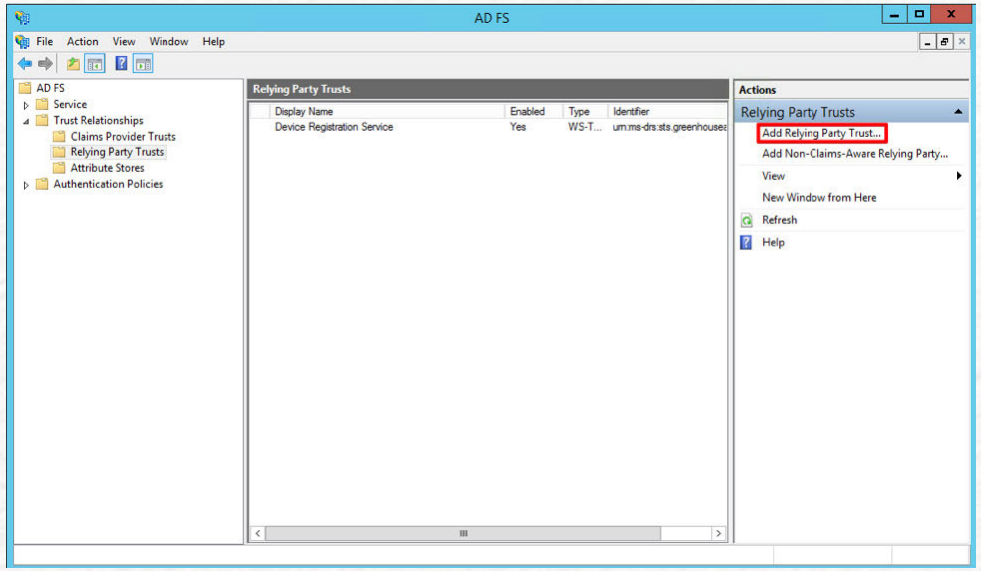
workvivo

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”.**





workvivo

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:

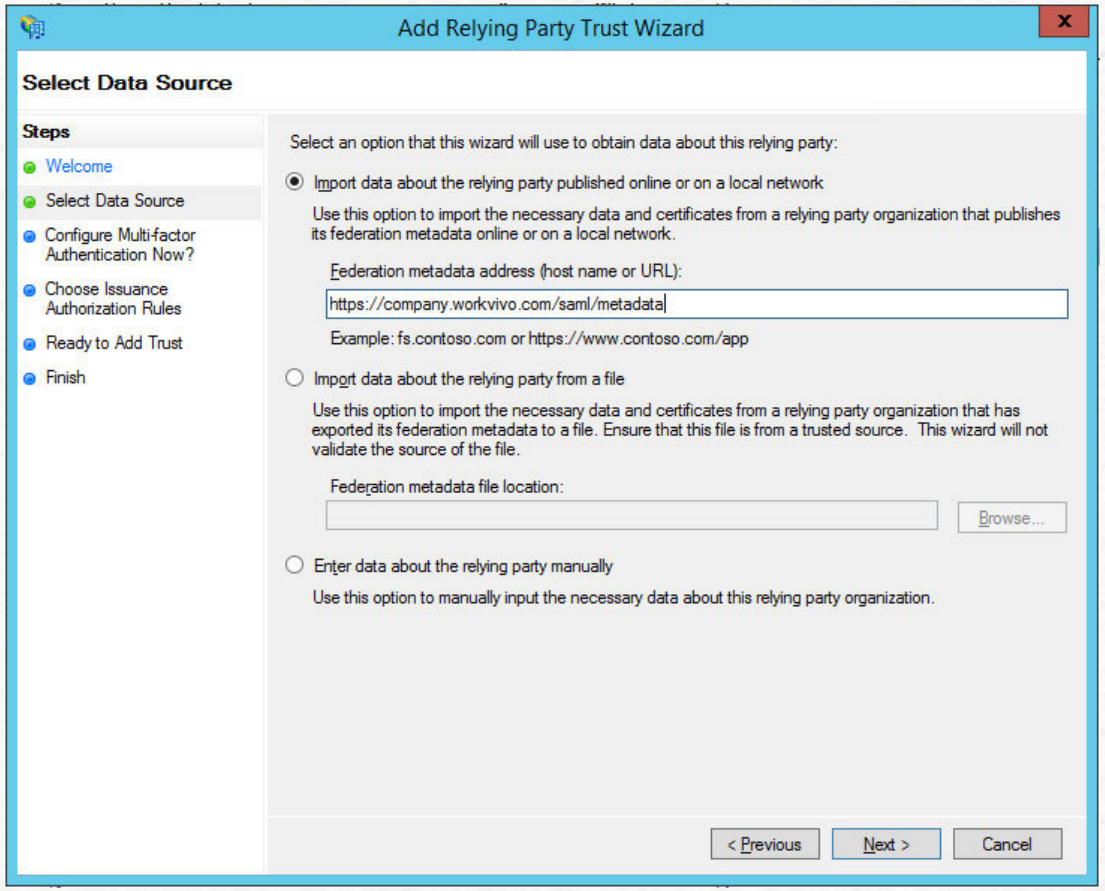
https://[companyname].workvivo.com/saml/metadata

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.**

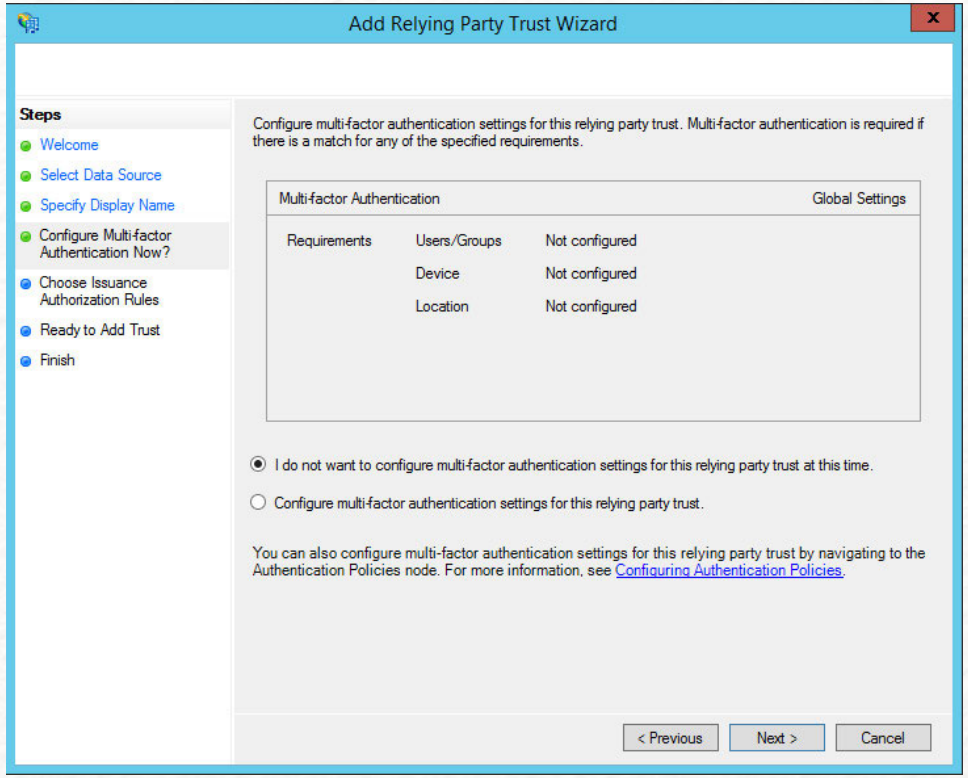
Press the **“Next”** button to continue.

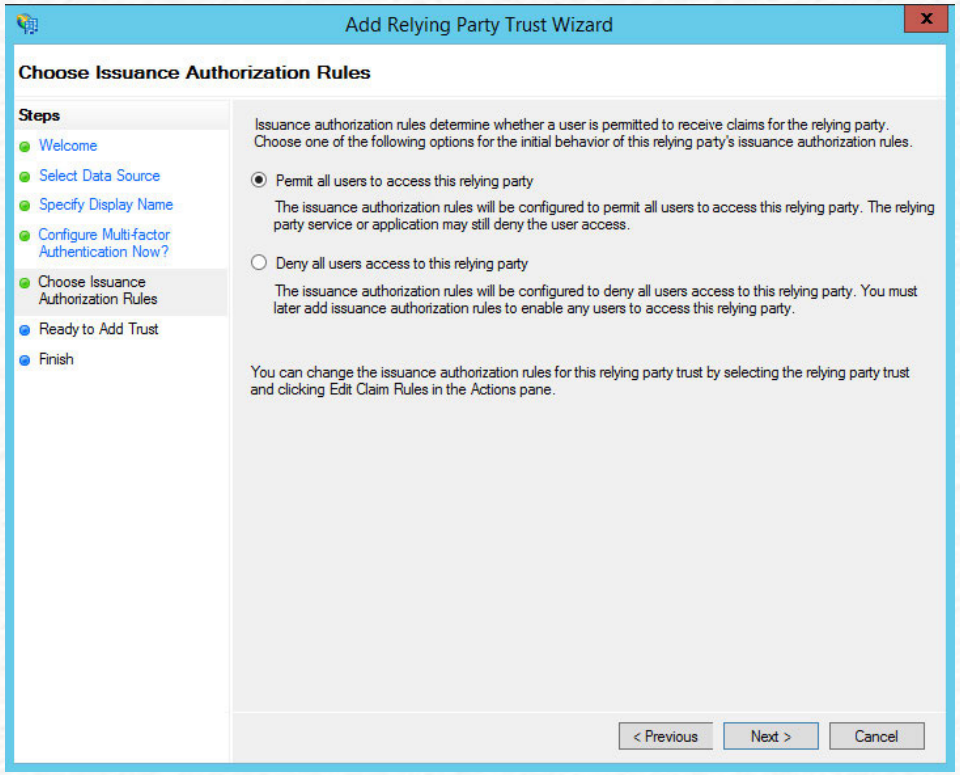
On the next screen, feel free to customise the Display name and add any relevant notes if you wish. Otherwise, click **“Next”** to move on.

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”.**

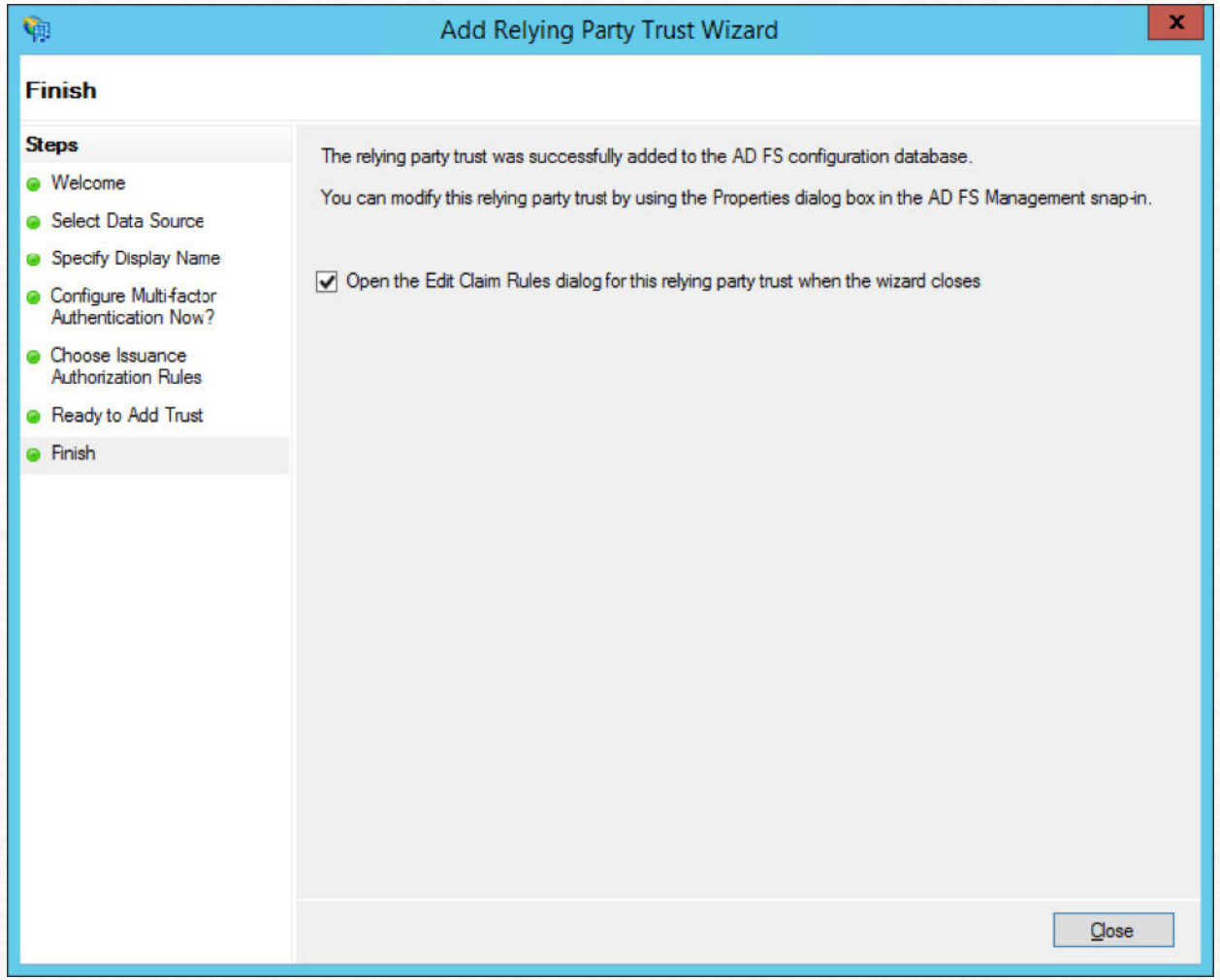


On the **“Choose Issuance Authorization Rules”** setting, leave it as the default “Permit all users to access this relying party” and click **“Next”.**





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



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.

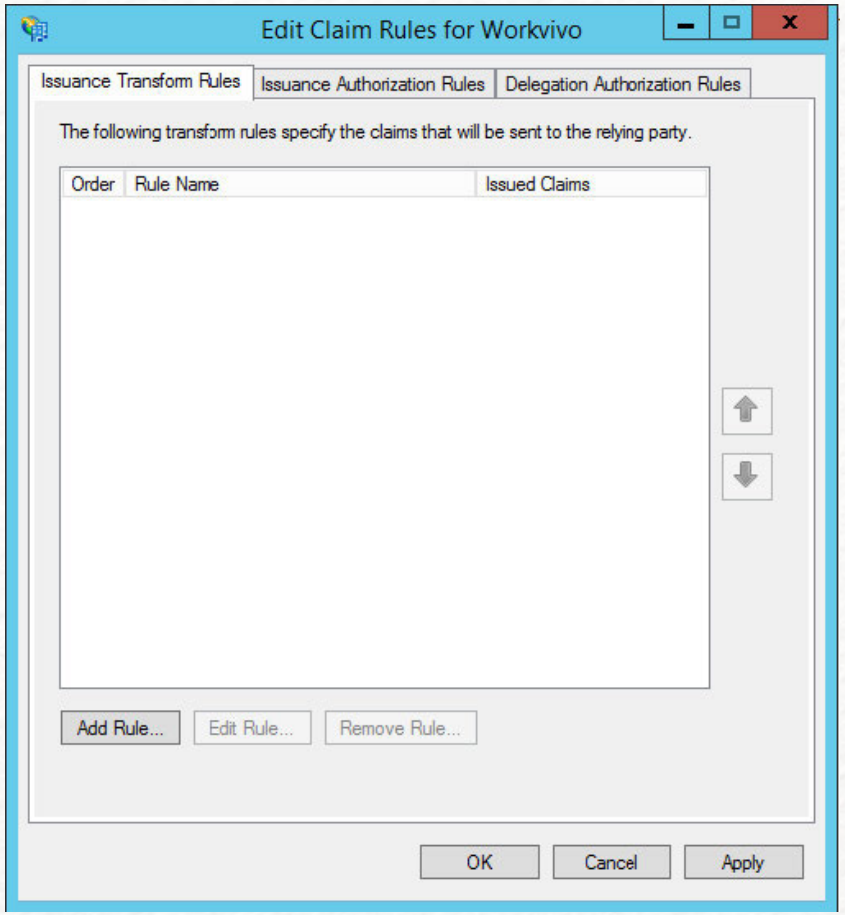
Setting up ADFS Claim Rules

workvivo

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".**

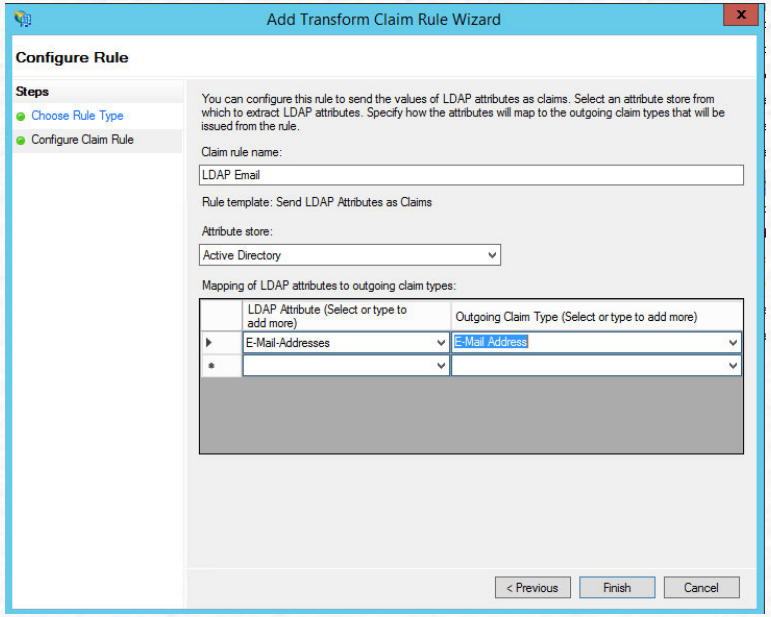


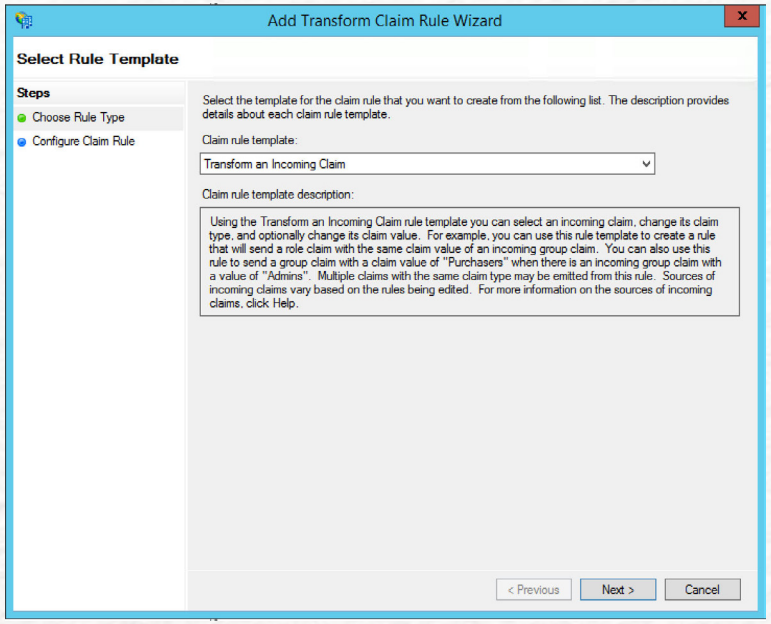
In the **“Configure Claim Rule”** screen, give the rule a name (e.g. **“LDAP Email”**). Select **“Active Directory”** from the **“Attribute store”** dropdown. We will create a single mapping – in the left-hand column (**“LDAP Attribute”**) select **“E-Mail-Addresses”**, and in the right-hand column (**“Outgoing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





Gathering ADFS Endpoints & X.509 Certificate

workvivo

5. Gathering ADFS Endpoints & X.509 Certificate

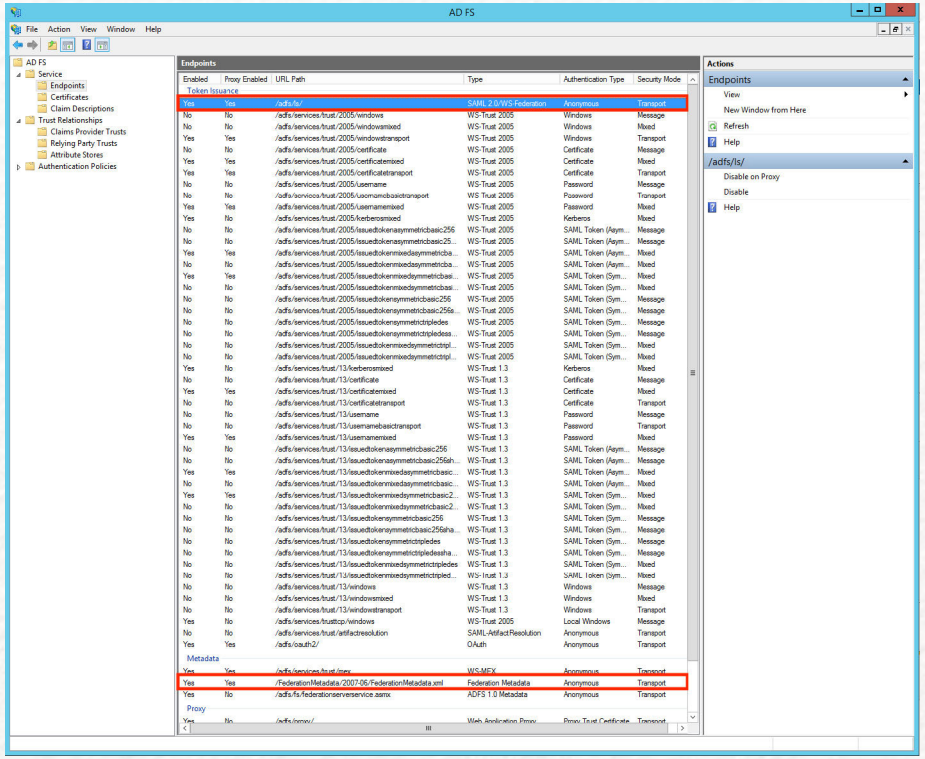
In order to configure your ADFS IdP in Workvivo, we need to gather the following information for your ADFS installation:

- 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”.**



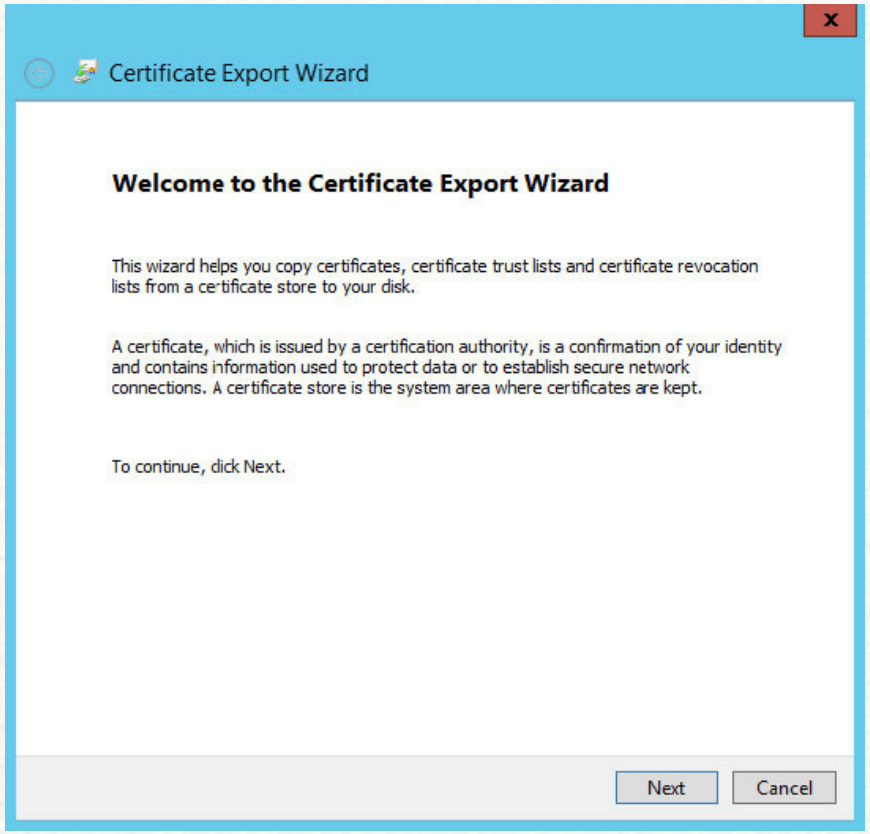
The Single Log Out endpoint does not always appear in this screen, but is typically **“/adfs/ls/?wa=wsignout1.0”.**

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:

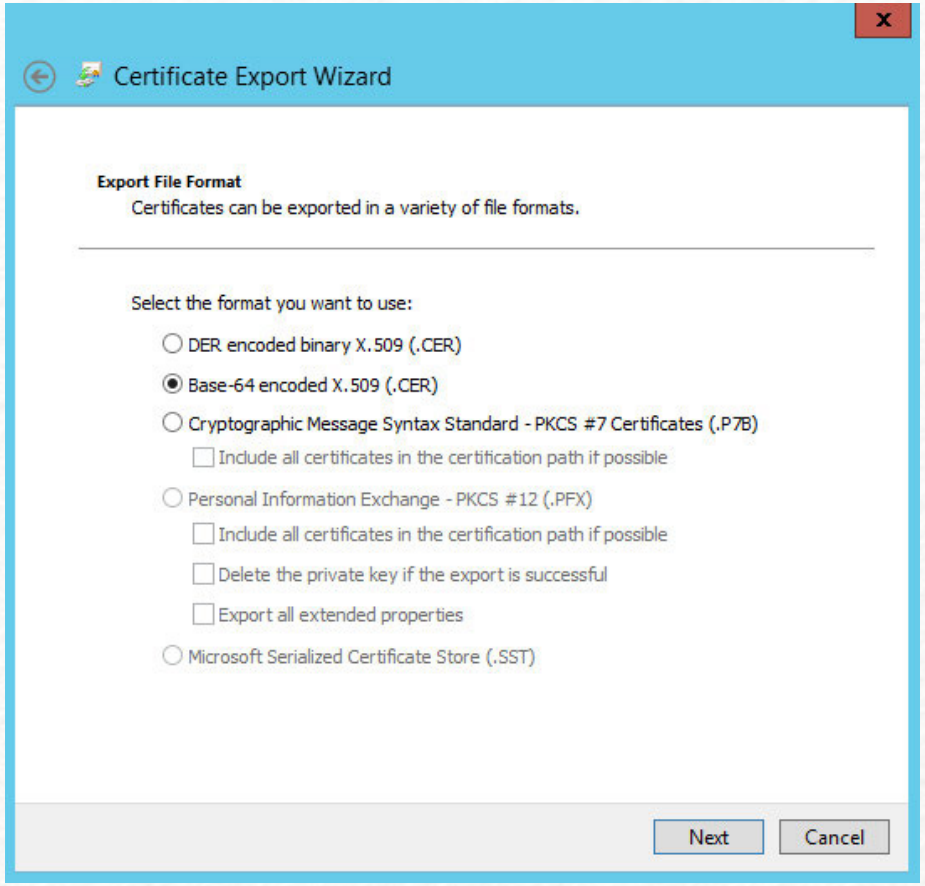
Type	Endpoint
Metadata	https://[ADFS FQDN]/FederationMetadata/2007-06/Federation-Metadata.xml
Single Sign On	https://[ADFS FQDN]/adfs/ls/
Single Log Out	https://[ADFS FQDN]/adfs/ls/?wa=wsignout1.0

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.



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.

thank you

workvivo

workvivo.com