# FOIAXpress popexus

# SAML Login and Proof of Identity Configuration

v11.3.0 August 2023

# FX 11.3.0 SAML Login and Proof of Identity Configuration

### Notice of Rights

Copyright © 2023, AINS, LLC d/b/a OPEXUS. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publisher: AINS, LLC. For information on obtaining permission for reprints and excerpts, contact info@opexustech.com.

Additionally, all copyrights, confidential information, patents, design rights and all other intellectual property rights of whatsoever nature contained herein are, and shall remain, the sole and exclusive property of the publisher.

### Notice of Liability

The information in this publication is believed to be accurate and reliable. However, the information is distributed by the publisher (AINS, LLC.) on an "As Is" basis without warranty for its use, or for any infringements of patents or other rights of third parties resulting from its use.

While every precaution has been taken in the preparation of this publication, neither the author (or authors) nor the publisher will have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused, directly or indirectly, by the information contained in this publication or by the computer software and hardware products described in it.

### Notice of Trademarks

The publisher's company name, company logo, company patents, and company proprietary products are trademarks or registered trademarks of the publisher: AINS, LLC. All other trademarks or registered trademarks are the property of their respective owners.

### Non-Disclosure Statement

This document's contents are confidential and proprietary to AINS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from AINS, LLC.

Images in this manual are used as examples and may contain data and versioning that may not be consistent with your version of the application or information in your environment.

### Additional Notice

Information in this documentation is subject to change without notice and does not represent a commitment on the part of AINS, LLC.

Notwithstanding any of the foregoing, if this document was produced as a Deliverable or other work for hire under a contract on behalf of a U.S. Government end user, the terms and conditions of that contract shall apply in the event of a conflict.

# Contents

1	Ab	out	SAML Login and Proof of Identity Configuration	4
2	Az	ure	AD Configuration	5
3	Ins	stall	and Configure ADFS Service	8
	3.1	Ad	d Relying Party Trusts	9
	3.2	Co	nfigure the Claim Rules	
	3.3	FC	IAXpress Configuration for SAML SSO	24
4	PA	AL SA	ML Configuration	
	4.1	PA	L SAML Login/Proof of Identity Configuration	
	4.1	1.1	Enable PAL Requester Login Using Forms Authentication	
	4.1	1.2	Enable PAL Requester Login Using SAML Authentication	
	4.1	1.3	Enable Proof of Identity Verification in PAL	
	4.2	PA	L SAML Configuration Tool	
	4.3	Cr	eate PFX Certificate	

# 1 About SAML Login and Proof of Identity Configuration

The FOIAXpress SAML Login and Proof of Identity Configuration manual was created to assist administrators when configuring the SAML Login and Proof of Identity Verification features. It covers the following information:

- **Azure AD Configuration**: This section provides instructions on how to configure Single Sign On (SSO) in Azure AD.
- Install and Configure ADFS Service: Consult this section for information on how to install and configure the ADFS Service, as well as additional procedures which support this process.
- **PAL SAML Configuration**: This section provides information on how to complete PAL SAML Configuration, as well as Proof of Identity Configuration, and using the PAL SAML Configuration Tool to create a PFX Certificate.

# 2 Azure AD Configuration

Complete the steps below for configuring Single Sign On in Azure AD:

1. Login to the Azure portal and create an application for ATIPXpress (under **Enterprise Application**), and Select **Set up Single Sign On:** 

(!!) Note: OPEXUS will provide the Identifier (Entity ID) and Reply URL (Assertion Consumer Service URL) information prior to SAML configuration.



2. Click SAML:

#### Azure AD Configuration

*	Home > fxsso	
+ Create a resource	🕤 fxsso   Single sig	1-on
🟫 Home	Enterprise Application	
🖾 Dashboard		<
I All services	Overview	Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in sure grading to the user application that user with only one account. Once the user long into an application that
* FAVORITES	Deployment Plan	credential is used for all the other applications they need access to. Learn more.
All resources	Manage	
😥 Resource groups	Properties	Select a single sign-on method Help me decide
S App Services	2 Owners	
SQL databases	Roles and administrators	
S Azure Cosmos DB	Users and groups	Disabled SAML Password-based Password storage and replay using a
📮 Virtual machines	Single sign-on	won't be able to launch the app from applications using the SAML (Security web browser extension or mobile app. My Apps. Assertion Markup Language) protocol
💠 Load balancers	Provisioning	
Storage accounts	Application proxy	
Virtual networks	G Self-service	
Azure Active Directory	Custom security attributes	
Monitor	(preview)	Linked
💁 Advisor	Security	and the second and paper
O Microsoft Defender for	Conditional Access	
Cloud	Permissions	
Help + support	Token encryption	
Cost Management + Billing	Activity	
	sign-in logs	
-	🕍 Usage & insights	
	Audit logs	
	Provisioning logs	

#### 3. Click Edit within the Basic SAML Configuration section.

40	Home > Ains, Inc > fxsso > fxsso	< 0			
+ Create a resource	fxsso   SAML-based	Sign-on			
A Home	Enterprise Application				
🖾 Dashboard		≪ ⊼ι	Ipload metadata file 🏾 🏷 Change single sign-on	mode 🔳 Test this application 🛛 🔗 Got feedb	ack?
All services	K Overview	An SSG	o implementation based on reperation protocols in ment. Choose SAML single sign-on whenever poss	inproves security, reliability, and end user experiences ible for existing applications that do not use OpenID	s and is easier to Connect or OAuth, Lea
★ FAVORITES	Deployment Plan	more.	and ansate some single sign of manere poss	and on county oppressions that are not are opened	
All resources	Manage	Read	the configuration guide d' for help integrating fxs	50.	
() Resource groups	Properties	0	Basic SAML Configuration		1
📀 App Services	2 Owners		destifier (Entity ID)	ATIDYDRESS	Edit
📴 SQL databases	Roles and administrators		Reply URL (Assertion Consumer Service URL)	https://dev.ains.com/atixpress/HomePage.aspx	
S Azure Cosmos DB	Users and groups		Sign on URL Relay State (Optional)	Optional Optional	
Virtual machines	Single sign-on		Logout Url (Optional)	Optional	
🚸 Load balancers	Provisioning				
E Storage accounts	Application proxy	0	Attributes & Claims		C Edit
Virtual networks	G Self-service		givenname	user.givenname	
Azure Active Directory	Custom security attributes		sumame	user.surname	
Monitor	(preview)		name	user.userprincipalname	
Advisor	Security		Unique User Identifier	user.userprincipalname	
O Microsoft Defender for	🍨 Conditional Access	0			
Cloud	Permissions		SAML Signing Certificate		0 Edit
Help + support	Token encryption		Status	Active	
🙆 Cost Management + Billing	Activity		Thumbprint Expiration	2/18/2025, 4:05:38 PM	
	Activity		Notification Email		
	Sign-in logs		App Federation Metadata Un	https://L_	. 0
	📫 Usage & insights		Certificate (Base64) Certificate (Raw)	Download	
	Audit logs		Federation Metadata XML	Download	
	Provisioning logs				
	3≡ Access reviews	4	Set up fxsso		

4. Enter the **Entity ID** that OPEXUS provided into the *Identifier* (*Entity ID*) field.

- 5. Click the **Default** checkbox adjacent the *Identifier* field.
- 6. Enter the **Reply URL** that OPEXUS provided into the *Reply URL* field.
- 7. Click the **Default** checkbox adjacent the *Reply URL* field.

#### 8. Click Save.

«	Home > fxsso >				Basic SAML Configuration			×			
+ Create a resource	fxsso   SAML-based Sig	in-on			<b>jj</b>						
1 Home	Enterprise Application				🗟 Save 🔗 Got feedback?						
Dashboard	~	Ťι	Upload metadata file 🌼 Change single sign-on	mode 🔳 Test this application 🕴 🕺							
E All services	Sverview				Identifier (Entity ID) * 💿						
* FAVORITES	Deployment Plan	Set u	up Single Sign-On with SAML		The default identifier will be the audience of the SAML response for IDP-initiated SSO			_			
All resources	Manage	An SS	O implementation based on federation protocols	improves security, reliability, and end user		Default					
(•) Resource groups	Properties	impler more.	ment. Choose SAML single sign-on whenever poss	sible for existing applications that do not i	ATIPXPRESS	/ 🔽 C	Î				
App Services	A Owners	Read	the configuration quide r <sup>2</sup> for help integrating for	500	Add identifier						
🧧 SQL databases	👃 Roles and administrators	-	Contraction game to not neep integrating its		Penkel IPI (Assertion Consumer Service   IPI ) *						
S Azure Cosmos DB	Users and groups	•	Basic SAML Configuration		The default reply URL will be the destination in the SAML response for IDP-initiated SSO						
Virtual machines	Single sign-on		Identifier (Entity ID)	ATIPXPRESS		Default					
Load balancers	Provisioning		Sign on URL	Optional	hites://doi.org.com/alivesce/linesce/linesce/		Ê				
Storage accounts	Application proxy		Relay State (Optional) Logout Url (Optional)	Optional Optional	Add reply URL						
Virtual networks	Self-service										
Azure Active Directory	Custom security attributes	2	Attributes & Claims		Sign on URL (Optional) ①						
Monitor	(preview)				Enter a sign on URL		~				
o Advisor	Security		sumame	user une							
O Microsoft Defender for	Conditional Access		emailaddress name	user.userprincipalname	Relay State (Optional)						
Cloud	🖧 Permissions		Unique User Identifier	user.userprincipalname	Enter a relay state						
Help + support	Token encryption				Lines o reny state						
Cost Management + Billing	Activity	8	8	8	3 SAML SI	SAML Sing Certificate		Logout Url (Optional) 💿			
	Sign-in logs		aratus	Active	Enter a logout ur		~				
	🕍 Usage & insights		Thumbprint Expiration	083DE1FB1209B2171EF5797CA899F1C 2/18/2025, 4:05:38 PM							
	Audit logs		Notification Email	sbasheerbad@ainsinc.onmicrosoft.com							
	Provisioning logs		Certificate (Base64)	nttps://login.microsoftonline.com/2e6 Download							
			A STATE STATE (ASSA)	President and a second s							

5. Once complete, download the **Federation Metadata XML** and email it to your OPEXUS Project Manager or Implementation Specialist.

# 3 Install and Configure ADFS Service

Ensure that ADFS is properly installed and that the *Federation Service Properties* are configured as indicated in the following screenshot:

Federation Service Properties
General Organization Events Federation Service display name:
DEV-ADFS01 Example: Fabrikam Federation Service
Federation Service name:
Example: fs.fabrikam.com
Federation Service identifier:
Example: http://fs.fabrikam.com/adfs/services/trust
Web SSO lifetime: 480 🔶 minutes
OK Cancel Apply

The *Federation Service Property* Fields above utilize example values, however during installation and configuration you should replace these values with information unique to your organization.

# 3.1 Add Relying Party Trusts

To create a new relying party trust for the FOIAXpress Application you must first install ADFS Service for Server Roles. Follow the steps below to install ADFS Service and add Relying Party Trusts.

- 1. Login to the ADFS server and click **AD FS Management** within the Administrative Tools application menu. The AD FS window appears.
- 2. Expand the *Trust Relationship* folder to display the *Relying Party Trusts* subfolder. Click **Relying Party Trusts**.



3. Click **Add Relying Party Trust...** within the context menu. The *Add Relying Party Trust* wizard appears.



#### 4. Click Start.



5. Select the Enter data about the relying party manually radio button and then click Next.

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         • Specify Display Name       Import data about the relying party published online or on a local network.         • Choose Profile       Federation metadata online or on a local network.         • Configure Cetificate       Federation metadata address (host name or URL):         • Configure Multi factor       Example: fs.contoso.com or https://www.contoso.com/app         • Choose Issuance       Import data about the relying party from a file         • Choose Issuance       Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata file location:         • Federation metadata file location:       Federation metadata file location:         • Finish       Import data about the relying party manually         • Enter data about the relying party manually       Use this option to manually input the necessary data about this relying party organization.	<b>\$</b>	Add Relying Party Trust Wizard
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         • Specify Display Name       Import data about the relying party published online or on a local network.         • Choose Profile       Federation metadata and certificates from a relying party organization that publishes its federation metadata address (host name or URL):         • Configure URL       Federation metadata address (host name or URL):         • Configure URL       Import data about the relying party from a file         • Configure Multifactor Authentication Now?       Import data about the relying party from a file         • Choose Issuance Authorization Rules       Federation metadata file location:         • Federation metadata file location:       Federation metadata file location:         • Finish       © Enter data about the relying party manually         • Ethis option to manually input the necessary data about this relying party organization.	Select Data Source	
< Previous Next > Cancel	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	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 address (host name or URL):         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 explored its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.         Pederation metadata file location:       Browse         Import data about the relying party manually       Use this option to manually input the necessary data about this relying party organization.

6. Enter **FOIAXpress** in the *Display Name* field and click **Next**.

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

7. Select the **AD FS profile** radio button and click **Next**.

Ŷ	Add Relying Party Trust Wizard	x
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	<ul> <li>AD FS profile</li> </ul>	
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 SAIVIL 2.0 protocol.	
<ul> <li>Configure Certificate</li> </ul>	O 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?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
Finish		
	< Previous Next > Cance	:I

8. Click Next.

<b>\$</b>	Add Relying Party Trust Wizard	x
Configure Certificate		
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	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         Issuer:         Subject:         Effective date:         Expiration date:	
	< Previous Next > Cance	:I

<b>\$</b>	Add Relying Party Trust Wizard
Configure URL	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Profile</li> <li>Configure Certificate</li> <li>Configure URL</li> <li>Configure Identifiers</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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-Trust 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: ☐ Example: https://fs.contoso.com/adfs/ls/ ✔ Enable support for the SAML 2.0 WebSSO protocol The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 webSSO protocol. Relying party SAML 2.0 SSO service URL supports Web-browser-based claims providers using the SAML 2.0 SSO service URL: https://fx.dev.ains.com/foiaxpress/HomePage.aspx] Example: https://fx.dev.ains.com/adfs/ls/
	< Previous Next > Cancel

- 9. Click the Enable support for the SAML 2.0 WebSSO protocol checkbox.
- 10. Enter the **https URL** for the FOIAXpress Application in the *Relying party SAML 2.0 SSO service URL* field and then click **Next**.

<b>\$</b>	Add Relying Party Trust Wizard	x
Configure Identifiers		
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this reh	ying
Welcome	party trust.	-
Select Data Source	Relying party trust identifier:	
Specify Display Name	FOIAXPRESS	ł
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust	
Configure Certificate	Relying party trust identifiers:	
Configure URL	Remo	ve
Configure Identifiers		
Configure Multi-factor Authentication Now?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
<ul> <li>Finish</li> </ul>		
	< Previous Next > Cance	el

- 11. Enter **FOIAXPRESS** in the *Relying party trust identifier* field and click **Add**. FOIAXpress appears in the *Relying Party Trust Identifiers* list.
- 12. Click Next.



13. Select the I do not want to configure multi-factor authentication settings for this relying party trust at this time radio button, and then click Next.



14. Ensure that the **Permit all users to access this relying party** radio button is selected and then click **Next**.

<b>\$</b>	Add Relying Party Trust Wizard	x
Ready to Add Trust		
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	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.         Monitoring       Identifiers       Encryption       Signature       Accepted Claims       Organization       Endpoints       Note < >         Specify the monitoring settings for this relying party trust.       Relying party's federation metadata       URL:	

15. Click Next.

<b>\$</b>	Add Relying Party Trust Wizard
Finish	
Steps  Welcome  Select Data Source  Specify Display Name  Choose Profile  Configure Cettificate  Configure URL  Configure Identifiers  Configure Multifactor Authentication Now?  Choose Issuance Authorization Rules  Ready to Add Trust  Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.
	Close

16. Ensure the **Open the Edit Claim Rules** checkbox is selected, and then click **Close**. The *Edit Claim Rules* pop-up window appears.

(!!) Note: You can navigate directly to the *Edit Claim Rules* pop-up window by selecting *Edit Claim Rules* in the in the right panel of the *ADFS Management Console*.

- 17. Click Add Rule. The Add Transform Claim Rule Wizard pop-up window appears.
- 18. Select **Send LDAP Attributes as Claims** from the *Claim Rule Template* drop-down list and then click **Next**.

Select Rule Template Steps © Choose Rule Type © Configure Claim Rule Send Send Transf Pass Send Activi be u multi a rule	t the template for the claim rule that you want to create from the following list. The description provide about each claim rule template. rule template: LDAP Attributes as Claims Group Membership as a Claim form an Incoming Claim Through or Filter an Incoming Claim Claims Using a Custom Rule ple claims trom a single rule using this rule type. For example, you can use this rule template to create that will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory will exten attribute values for authenticated users from the displayName attribute values for attribute values for authenticated users	s
Steps     Select details <ul> <li>Configure Claim Rule</li> <li>Claim Send</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Transf</li> <li>Pass</li> <li>Send</li> <li>Multi</li> <li>a rule</li> <li>Activity</li> <li>be u</li> <li>mem</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Multi</li> <li>a rule</li> <li>Activity</li> <li>Be u</li> <li>mem</li> <li>Send</li> <li>Send</li></ul>	t the template for the claim rule that you want to create from the following list. The description provide a about each claim rule template. rule template: LDAP Attributes as Claims Group Membership as a Claim form an Incoming Claim Through or Filter an Incoming Claim Claims Using a Custom Rule ple claims trom a single rule using this rule type. For example, you can use this rule template to create e that will exten attribute values for authenticated users from the displayName and telephoneNumber ve Directory wates and then send those values as two different outgoing claims. This rule may also	r
Choose Rule Type     details     Configure Claim Rule     Claim     Send     Transt     Pass     Send     multi     a rule     Activ     be u     mem	AP attributes as Claims     AP attribute     as and then send those values as two different outgoing claims. This rule may also     yee that will extend attribute values and then send those values as two different outgoing claims. This rule may also	ŗ
<ul> <li>Configure Claim Rule</li> <li>Send</li> <li>Send</li> <li>Send</li> <li>Trans</li> <li>Send</li> <li>multi</li> <li>a ruli</li> <li>Activ</li> <li>be u</li> <li>mem</li> </ul>	LDAP Attributes as Claims <ul> <li>LDAP Attributes as Claims</li> <li>LDAP Attributes as Claims</li> <li>Group Membership as a Claim</li> <li>form an Incoming Claim</li> <li>Through or Filter an Incoming Claim</li> <li>Claims Using a Custom Rule</li> <li>pe claims from a single rule using this rule type. For example, you can use this rule template to create e that will extent attribute values for authenticated users from the displayName and telephoneNumbere Directory wates and then send those values as two different outgoing claims. This rule may also</li> </ul>	r
Send Send Trans Pass Send multi a rule Activ be u mem	LDAP Attributes as Claims  LDAP Attributes as Claims  LDAP Attributes as Claims  Group Membership as a Claim  form an Incoming Claim  Through or Filter an Incoming Claim  Claims Using a Custom Rule  ple claims from a single rule using this rule type. For example, you can use this rule template to create that will extra attribute values for authenticated users from the displayName and telephoneNumbe re Directory outes and then send those values as two different outgoing claims. This rule may also	ŗ
Send Send Trans Pass Send multi a ruli Activ be u mem	LDAP. Attributes as Claims Group Membership as a Claim form an Incoming Claim Through or Filter an Incoming Claim Claims Using a Custom Rule ple claims from a single rule using this rule type. For example, you can use this rule template to create e that will extend attribute values for authenticated users from the displayName and telephoneNumber ve Directory the utes and then send those values as two different outgoing claims. This rule may also	5
	sed to send of of the user's group memberships. If you want to only send individual group berships, the send Group Membership as a Claim rule template.	

19. Verify the properties in different tabs after the relying party is created and click **OK** to close the window. The Relying Party Trust is finalized and added to the ADFS Service.

	FOIA	XPRESS Pr	opertie	es		x
Monitoring	Identifiers	Encryption	Signatu	re Acc	epted Claims	
Organization	Endpoints	Proxy End	points	Notes	Advanced	
Specify the er	ndpoints to use	for SAML and	WS-Fede	rationPass	ive protocols.	
JRL				Inde	ex Binding	
SAML Asse	rtion Consum	ner Endpoints				
https://de	vfx.ains.com/fo	piaxpress/Hom	ePage.asp	ox O	POST	
<					>	
Add SAML						
Add WS-Fe	deration		Rem	nove	Edit	
		OK	Ca	incel	Apply	

- 20. Click the *Endpoints* tab. Provide **SAML assertion Consumer Endpoint** as the application URL and select **POST** as the binding.
- 21. Click **OK**.

# 3.2 Configure the Claim Rules

To configure the ADFS Claim Rules:

- 1. Login to the ADFS server and click **AD FS Management** within the *Administrative Tools* application menu. The *AD FS* Window appears.
- 2. Click Add/Edit Claim Rules.



3. The Add Transform Claim Rule Wizard pop-up window appears. Click Next.

Add Transform Claim Rule Wizard	X
Select the template for the claim rule that you want to create from the following list. The description provided details about each claim rule template. Claim rule template: Send LDAP Attributes as Claims 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.	r b
< Previous Next > Cancel	_
	Add Transform Claim Rule Wizard Select the template for the claim rule that you want to create from the following list. The description provide details about each claim rule template. Claim rule template: Send LDAP Attributes as Claims 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 nule that will extract attribute site of authenticated users from the displayName and telephoneNumbe 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.

- 4. The pop-up window refreshes to display the *Configure Claim Rule* tab. Select **Active Directory** from the *Attribute Store* drop-down list.
- 5. Select **SAM-Account-Name** from the LDAP Attribute drop-down list.
- 6. Select Name ID Mapping from the Outgoing Claim Type drop-down list.

(!!) Note: The *Outgoing Claim Type* drop-down list selection must be *Name ID Mapping*.

<b>\$</b>		Add Transform Claim Rule	Wizard
Configure Rule			
Steps • Choose Rule Type • Configure Claim Rule	You ca which t issued Claim r FOIAX Rule te Attribut Active Mappir	an configure this rule to send the values of L to extract LDAP attributes. Specify how the from the rule. ule name: press amplate: Send LDAP Attributes as Claims te store: Directory ng of LDAP attributes to outgoing claim type: LDAP Attribute (Select or type to add more) SAM-Account-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) Name ID
			< Previous Finish Cancel

- 7. Within the next blank *LDAP Attribute Row*, select **Given Name** from the *LDAP Attribute* drop-down list.
- 8. Select **Given Name** from the *Outgoing Claim Type* drop-down list.
- 9. Within the next blank LDAP Attribute Row, select **Surname** from the LDAP Attribute dropdown list.
- 10. Select Surname from the Outgoing Claim Type drop-down list.
- 11. Click **Finish** to save the changes.

## 3.3 FOIAXpress Configuration for SAML SSO

To complete the FOIAXpress Configuration for SAML SSO:

- 1. Login to the FOIAXpress application.
- 2. Run the Database Configuration tool as an Administrator and select/enter the following values in the corresponding fields:

- a. Sign On Mode: SAML SSO
- b. Service Provider: Relying party identifier in ADFS
  - i. Example: FOIAXPRESS
- c. Partner Identity Provider: Federation service identifier for ADFS
- d. **Provider default page**: The application URL. FOIAXpress App URL ends with /FOIAXpress/HomePage.aspx
  - i. Example: https://fxdev.ains.com/foiaxpress/HomePage.aspx
- e. **Service URL**: The Login page from the Identity Provider (ADFS SSO URL ends with /ADFS/Is).
- f. **Partner Certificate File**: It should be the signing certificate from ADFS or Internet Information Services (IIS) cert.

POIAXpress Database Configuration
Configuration Sign-On Mode
Please choose the Sign-On Mode you want to configure.
FOIAXpress Sign-On Mode
Sign-On Mode: SAML SSO 🗸
Service Provder: FOIAXPRESS
Partner Identity Provider: http://sso.sts.irs.gov/adfs/sen
Provider Default Page: https://fxdev.ains.com/foiaxpre
Service URL: https://sso.sts.irs.gov/adfs/ls
Partner Certificate File: adfs.cer
Details Save Close

- 3. Click **Save**. The Sign-On Mode settings are updated in the database as well as the saml.config and web.config files.
- 4. Copy and paste the .CER file into the same folder the web.config file is located.
- 5. Verify that web.config has the *PartnerIdP* set to specified partner identity provider in <a ppsettings> section.

# 4 PAL SAML Configuration

# 4.1 PAL SAML Login/Proof of Identity Configuration

The Public Access Link (PAL) works with forms authentication by default, however if an agency needs to enable Security Assertion Markup Language (SAML) Authentication for requester login, the system can be configured with your identity provider details following the directions in this section. PAL can also be configured to provide Proof of Identity verification with identity providers such as Login.gov.

# (!!) Note: The Assertion Consumer URL for PAL Requester Login and Proof of Identity are different. Consult step 5 in the

#### PAL SAML Configuration Tool section of this document for additional information.

Ensure you have the Personal Exchange Format (PFX) file and its public key ready as well. You will need to provide the PFX file in PAL SAML Configuration, and the corresponding public key in the IDP app/account. Consult the Create PFX Certificate section for information on how to get the PFX Certificate file and its public key.

### 4.1.1 Enable PAL Requester Login Using Forms Authentication

There are no configuration settings to configure for forms authentication. You can either use forms authentication or configure the requester's initial login to PAL to use a SAML Authentication method.

### 4.1.2 Enable PAL Requester Login Using SAML Authentication

Follow the steps below to enable PAL requester login using SAML authentication:

- 1. Log in to PAL Configuration, and access **Authentication** in the left-hand menu.
- 2. Select the Enable Login with SAML Authentication checkbox:

	Authentication Configur	ation
General Settings	Plassa complete all the required fields marked	with an actoricle( * )
Enterprise	Please complete an the required helds that kee	Nor an ascense in the
Modules		
Web API		
Security		
Authentication		
Email Templates	Authentication Options	
Email Log	CEnable Login with Forms Authentication	
Lieore	C Enable Eogin with Forms Addenication	
Audit Lee		
Audit Log	COTP Settings	
Requester Fields		
Request Fields	* OTP Notification Type: None	~
Append Fields		
Appeal Fields	* OTP Expiry Time: 5	
Other Settings		
Reading Room		
Reading Room Documents	Enable Login with SAML Authentication	
Display Order	Use SAML Configuration Tool for configuring identity provider.	
Dashboard Administration		
Online Payment		Save
Main Manu Linka		

- 3. Click **Save**, then see the
- 4. PAL SAML Configuration Tool section of this document for next steps.

### 4.1.3 Enable Proof of Identity Verification in PAL

Review the following identity provider prerequisites if you are enabling PAL to support proof of identity verification.

- Configure your IDP entity account(s). You cannot use the same account for PAL login and for Proof of Identity Configuration.
- Set up your sandbox environment (See your provider's instructions; some providers allow you to set up the environment while other providers will perform the setup on your behalf
- When enabling Proof of Identity Verification in PAL, you can use either level 1 or level 2 for login, however level 2 is required for Proof of Identity Verification. Ensure that the assertion URL in your *Identity Provider Entity* settings matches with URL provided in step 5 of the
- PAL SAML Configuration Tool section.

Follow the steps below to enable proof of identity verification in PAL:

- 1. Log in to PAL Configuration and select Request Fields in the left-hand menu.
- 2. Locate the *Proof of Identity Mode* request field and select **Digital Authentication** or **Upload Attachment/Digital Authentication** from the drop-down list within the *Default* column.

	Please complete all the	required feits marked with	an asterisk( * ).			
						Seel.Ch
Label Name	Display Name	Notes	Required	Vaible	Default	Display Information
General Information (Header)	Request Information	-				
Action Office	Regional Office		12	0	Default Office: Headquarters	Action Office Name
Action Office Details	Regional Office Instructions		0	0	Allowed Offices: Sitems checked	· Action Office Details
Request Type	Request Type	-	8	8	( v)	
Requester Category	Requester Category	-	8	8	Use Profile Category 💌	
Delivery Hole	Delivery Mole	-	0	0	(Au, V)	
Payment Hole	Payment Hode	-	0	0		
Expedite Information (Header)	Expedite Information	-				
Expedite Repeated	Expedite Requested	_		-		
Expedite Reason	Expedite Tasson	_	1 .			
Expedite Request Status	Expedite Request Status		0	0		
Shipping Address (Header)	Haling Address					
Streets	Street)		0	0		
Street2	Struet2		0	0		
City	Oty		0	0		
State	State		0	0		
State (Other)	State (Other)			0		
Country	Country		0	0		
Zip Code	Zg Code		0	0		
Request Information (Header)	Request Details	-				
Description Document	Description Document	-		2		
* Description	Description	-	2	5		
Date Range for Record Search	Date Range for Record Search	-	0	2		
Proof of Identity/Consent (Header)	Proof of Identity/Consent					
Proof of Identity Hode	Verification Hole				Proof of Identity Option: Upload Attache	nent/CW
Consent	Canaert Porm		2	5	Upload Attach	nerd, Tright Authentication
Proof of Stantity	Proof of Edentity Consent Form		12	5		
Digital Authentication	Diptal Authentication		12	0		

3. Scroll down and click Save.

# 4.2 PAL SAML Configuration Tool

Follow the steps below to use the PAL SAML Configuration Tool:

- 1. Navigate to the PAL Application Server.
- 2. Search for **SAML** in the windows search box, then select the tool once located.
  - a. Alternatively, navigate to the PAL Setup folder and locate the PAL.WebApp folder and in the bin folder you will find the application file 'FOIAXpress.Utilities.SamlConfig'
- 3. Right click SAML Configuration Tool and select **Run as administrator**.
- 4. The SAML Configuration interface appears as shown below. Select either Login or Proof of Identity from the SAML Using For drop-down list:

20.00					
* Certificates	Signature Certificate Te	ext:			
	Encryption Certificate Te	ext:			
			OR		
	IDP Certificat	le :		Browse X	
		Sign Authentica	tion Request		
		Want SAML Re	sponse Signed		
		Want Assertion	Signed		
		Want Assertion	Encrypted		
	Encrypt Logout Name ID				
Force Authentication					
Sign Logout Request					
Sign Logout Response					
		Disable In Resp	onse To Check		
SAML Field Mappin	gs				
	PAL Field	Provider Field	Description	Action	
•	Login	email	attribute used to login	Delete	
	Email	email	email address	Delete	
First Name first		first_name	first name	Delete	
Last Name last_name			last name	Delete	
Add					
			S	ave Close	

5. Next, configure the *Service Provider* information, as shown below and detailed in the following table:

SAML Configuration			×
Use of SAML SAML Using For:	Login ~		
Service Provider * Issuer:			
* Assertion Consumer URL:			
Signature Certificate:		Browse X	
Signature Certificate Password:			
Encryption Certificate:		Browse X	
Encryption Certificate Password:			
Identity Provider			
* IDP Entity ID/Issuer URL :			
SAML SSO URL:			'
SAML SSO URL Binding Type:			
SAML SLO URL:			
SAML SLO URL Binding Type:			
Name ID Format:			
Authentication Context:			
Authentication Context Comparison:			

Field	Description
Issuer	Enter the Service Provider Entity ID. This is a unique ID/name for an identity provider. (!!) Note: This is case-sensitive.
Assertion Consumer URL	For PAL Login, enter https://mypal/App/AssertionConsumerService.aspx For Proof of Identity, enter https://mypal/App/AssertionConsumerService.aspx?aal=2 (!!) Note: Replace 'mypal' in the above URL with your 'hostname'

Field	Description
Signature Certificate/Encryption Certificate	Use the PFX file that you have ready for SAML use, as mentioned at the beginning of this document. (!!) Note: This PFX file should correspond to the public key you uploaded in your Identity Provider account. If you are using a different public key in your Identity Provider account, extract the public key form this PFX file and replace your public key in the Identity Provider account with this public key. Enter the password for the PFX file in the Signature Certificate Password/Encryption Certificate Password fields. Also provide the IDP Entity ID/Issuer URL.

6. Next, complete the required *Identity Provider* fields, as shown below and described in the following table:

Identity Provider	
* IDP Entity ID/Issuer URL :	
SAML SSO URL:	
SAML SSO URL Binding Type:	
SAML SLO URL:	
SAML SLO URL Binding Type:	
Name ID Format:	
Authentication Context:	
Authentication Context Comparison:	

Field	Description
IDP Entity ID/Issuer URL, SAML SSO URL, SAML SLO URL	<ul> <li>To be provided by IDP.</li> <li>(!!) Notes:</li> <li>These will be different for test and production. Some IDPs do not support single logout, and it won't be provided. If SLO is not supported, you should leave the SLO URL and SLO Binding fields blank.</li> <li>For some IDPs, SAML SSO URL and SAML SLO URL must be updated each year, approximately quarterly.</li> </ul>
SAML SSO URL Binding Type	To be provided by IDP if required.
Name ID Format	To be provided by IDP if required.
Authentication Context	To be provided by IDP if required.
Authentication Context Comparison	To be provided by IDP if required.

7. Once that is complete, fill in the *Certificates* field, as shown below and detailed in the following table:

Signature Certificate Text:	MIID7TCCAtWgAwIBAgIUCethW2gYqC2N96czVCEaAkR/AiAwI				
Encryption Certificate Text:	MIID7TCCAtWgAwIBAgIUCethW2gYqC2N96czVCEaAkR/AiAwI				
	OR				
IDP Certificate :	Browse X				

Field	Description
Signature Certificate Text	To be provided by IDP.
Encryption Certificate Text	To be provided by IDP (same as Signature Certificate Text). (!!) Note: For some IDPs the x509 certificate text has to be updated each year and a reminder that the sandbox and production certificates may not be the same.
IDP Certificate	We recommend using Signature Certificate text and Encryption Certificate Text and skipping this field. For Login.gov the IDP certificate x509 can be found at the following URL: https://developers.login.gov/saml/

8. The five checkboxes (Sign Authentication Request, Want SMAL Response Signed, Want Assertion Signed, Want Assertion Encrypted, Encrypt Logout Name ID) should remain unchecked, which is the default setting. If ID Provider provides single logout service, then the Single Logout Request and Single Logout Response checkboxes must be checked.

Sign Authentication Request
Want SAML Response Signed
Want Assertion Signed
Want Assertion Encrypted
Encrypt Logout Name ID
Force Authentication
Sign Logout Request
Sign Logout Response
Disable In Response To Check

- 9. When all fields are complete, move on to the SAML Field Mapping section. Here, you can add or delete the fields based on what attributes/return value you have selected for your IDP entity app settings. The First Name, Last Name, Email, and Login fields are mandatory and cannot be removed. All three fields (*Provider Field*, PAL Field, and Description) are required while adding a new SAML Field in Mappings.
- (!!) Note: The provider fields for both 'Email' and 'Login' PAL Fields are the same.

#### System Data Services

	PAL Field	Provider Field	Description	Action	^
	City	city	City	Delete	
	Login	email	User Name		
•	Phone	phone	Phone Number	Delete	
	Street 1	address1	Address 1	Delete	
	Street 2	address2	Address 2	Delete	

Column	Description
PAL Field (Proof of Identity)	The PAL Field column contains labels for corresponding Provider fields that display in the Proof of Identity attachment. For Proof of Identity, the selected fields are displayed in the verification document provided with the request submission to FOIAXpress/ATIPXpress. The attachment is automatically added to the Proof of Identity attachment area and available in the Correspondence Log of the request.
	Digitally Verified Proof of Identification         PAL Verification Date       2021-09-30         Email       FAKEY         Last Name       MCFAKERSON         Address 1       1 FAKE RD         City       GREAT FALLS         State       MT         Zipcode       59010         Date of Birth       1938         Security Number       *******3456         Phone       +14435274664         D Verification Date       2021-06-15T20:05:50Z

Column	Descripti	on					
PAL Field (Login)	PAL Field displayed (requeste W Prefix Middle Name Suffix Street 2 State Zip Code Phone Organization Fax	s are the l in the SA r whose e /e need to co 	abels for c ML Reques mail doesr apture the fo	orresponding ster Registrati n't exist in the Ilowing information First Name Last Name Street 1 City State (Other) Country Email Requester Category Language	provider on page f PAL). on to serve	fields that a for a new re you better.	are quester
Provider Field	Provider requester	Fields are 's details	the corres such as firs	ponding IDP a st name, last na	ittribute ame, add	Save & Continue Ca names for t ress 1, and	he country.
Description	Descripti	on of map	ped field.				

(!!) Note: For Social Security number, the field will be masked only if the PAL Field is named 'SSN', 'Social Security', or 'Social Security Number'.

10. Once all the required fields are complete, click **Save** to save the settings.

(!!) Note: If using forms authentication, you'll need to provide dummy data for the Proof of Identity settings options, even if these settings are not being used.

For login.gov, please visit <u>https://developers.login.gov/</u> for all details about identity provider fields.

# 4.3 Create PFX Certificate

Follow the steps below to create a PFX certificate file and extract a public key from the PFX file using OpenSSL.

- 1. Open IIS and click **Server**.
- 2. In the Security section, double click the Server Certificates.



3. In the top right corner, click **Create Self-Signed certificate**:



- 4. A pop-up window appears where you can *Specify a friendly name for the certificate* in the field provided.
- 5. Next, select **Personal** from the Select a certificate store dropdown:

- 6. Now that the certificate is created, and you can export the certificate into the PAL folder. Go to *Manage Computer Certificate* (located in the *Control Panel* or by using the Windows search feature)
- 7. In the Manage Computer window, click **Personal** and then click **Certificate**.
- 8. From the list of certificates, locate your certificate using the friendly name provided.
- 9. Right click the **Certificate**, select **All Tasks**, and then select **Export**.
- 10. In the new pop-up window, click **Next** to continue.
- 11. Under *Export Private Key*, select **Yes**, **export the private key** and click **Next**.
- 12. Under Export File Format:
  - a. Select Personal Information Exchange (PFX)
  - b. Uncheck 'Delete the private key if the export key if successful.
  - c. Check all other options, then click Next.
- 13. Under Security, check Password, and type the password for your certificate.

# (!!) Note: You will need this password in order to use the certificate i.e., in SAML configuration tool and to extract public key

- 14. For Encryption, select AES256-SHA256, then click Next.
- 15. Under *File to Export*, click **Browse** and choose your certificate location. We recommend putting the certificate in the PAL folder where your PAL web.config is located.
- 16. Type in your certificate name and click **Next**. Once the process is complete, Click **Finish**.
- 17. Now you have PFX certificate ready for SAML Service Provider Certificate. Next, we will derive public key from this PFX file. Remember the certificate containing public key, which we upload to login.gov, must be generated from the PFX certificate file that we use in SAML Configuration tool.

- 18. To create a certificate with public key, install OpenSSL on your computer and then open the command prompt by typing "cmd" in Windows search.
- 19. Go to you PFX file location (type cd full\_path\_of\_pfx), and type the following command: openssl pkcs12 -in your\_file\_name.pfx -clcerts -nokeys -out give\_name\_for\_cert\_public\_key.crt\
- 20. When complete, press **Enter**. The certificate with a public key for login.gov is created.