

ATIPXpress

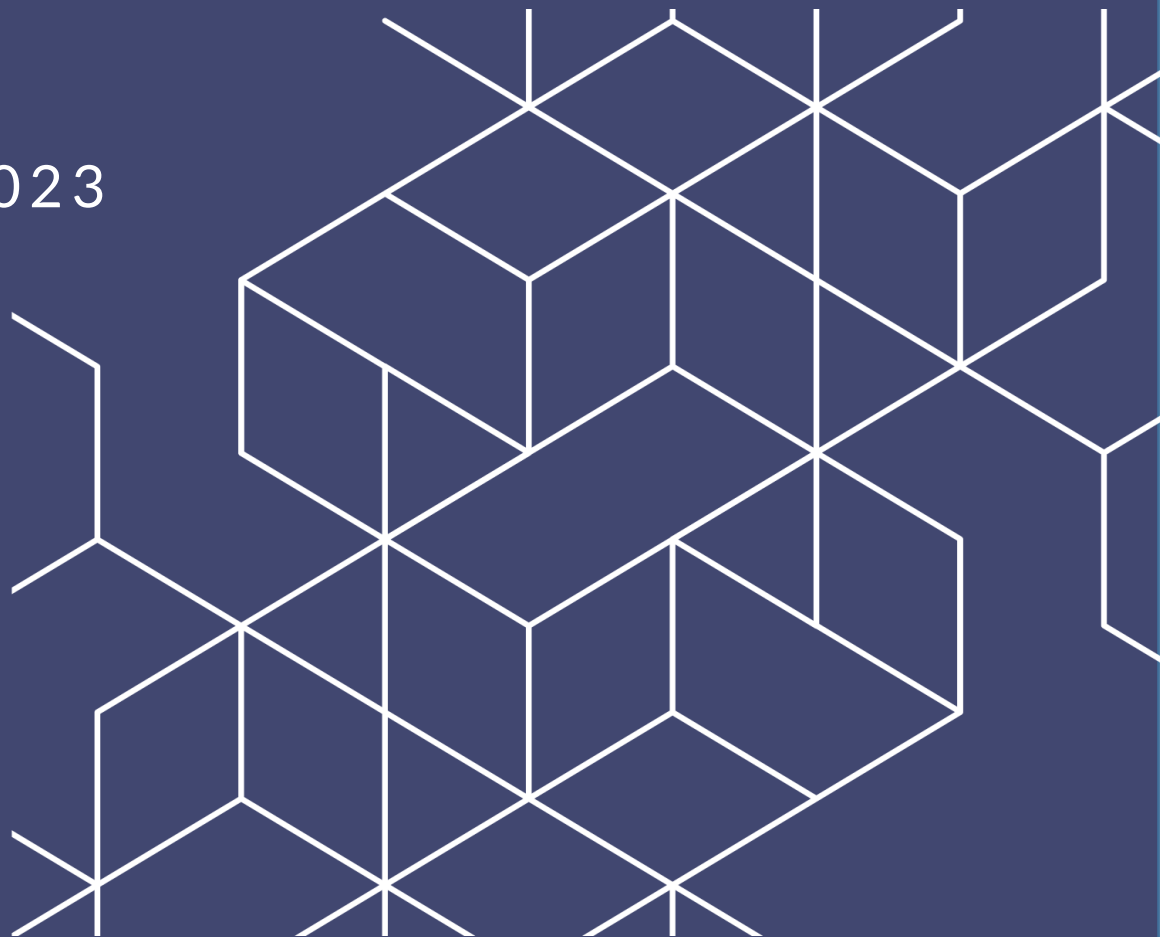


OPEXUS

SAML Login and Proof of Identity Configuration

v11.3.0

August 2023



AX 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	About SAML Login and Proof of Identity Configuration	4
2	Azure AD Configuration	5
3	Install and Configure ADFS Service	8
3.1	Add Relying Party Trusts	9
3.2	Configure the Claim Rules.....	22
3.3	ATIPXpress Configuration for SAML SSO.....	24
4	PAL SAML Configuration	26
4.1	PAL SAML Login/Proof of Identity Configuration.....	26
4.1.1	Enable PAL Requester Login Using Forms Authentication.....	26
4.1.2	Enable PAL Requester Login Using SAML Authentication	26
4.1.3	Enable Proof of Identity Verification in PAL	27
4.2	PAL SAML Configuration Tool.....	28
4.3	Create PFX Certificate	35



1 About SAML Login and Proof of Identity Configuration

The ATIPXpress 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:

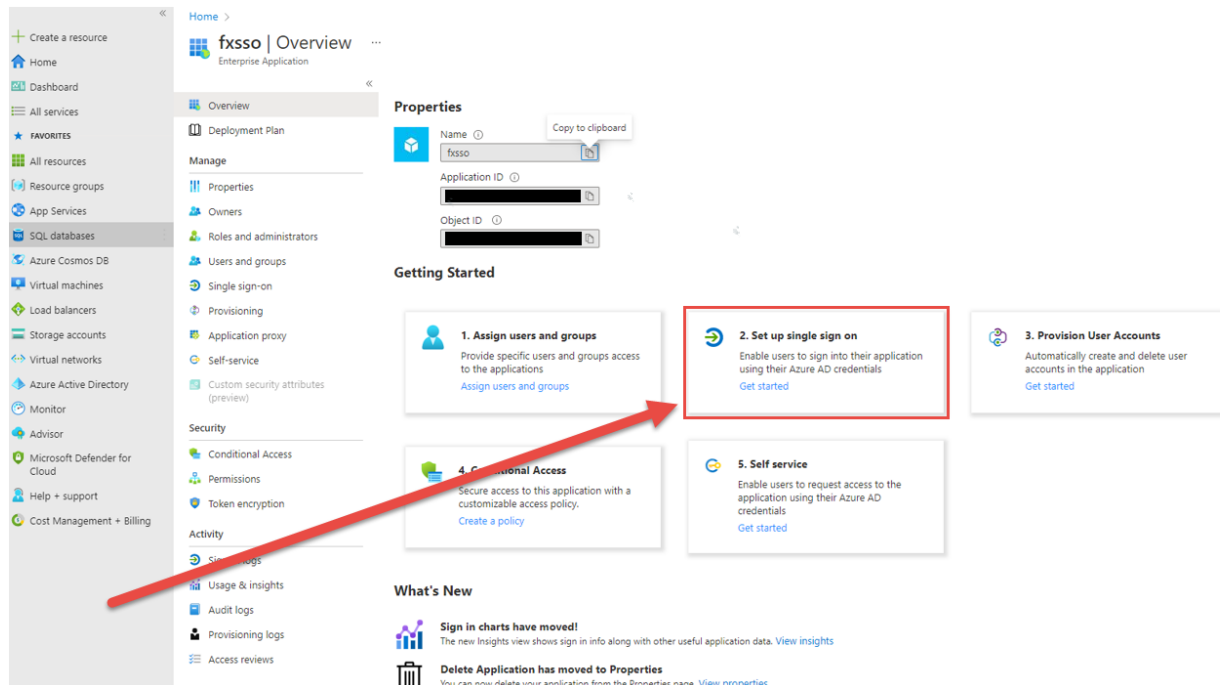
- **Azure AD Configuration:** This section provides instructions on how to configure Single Sign On (SSO) in Azure AD.
- **Install and Configure ADFS Service:** Consult this section for information on how to install and configure the ADFS Service, as well as additional procedures which support this process.
- **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:

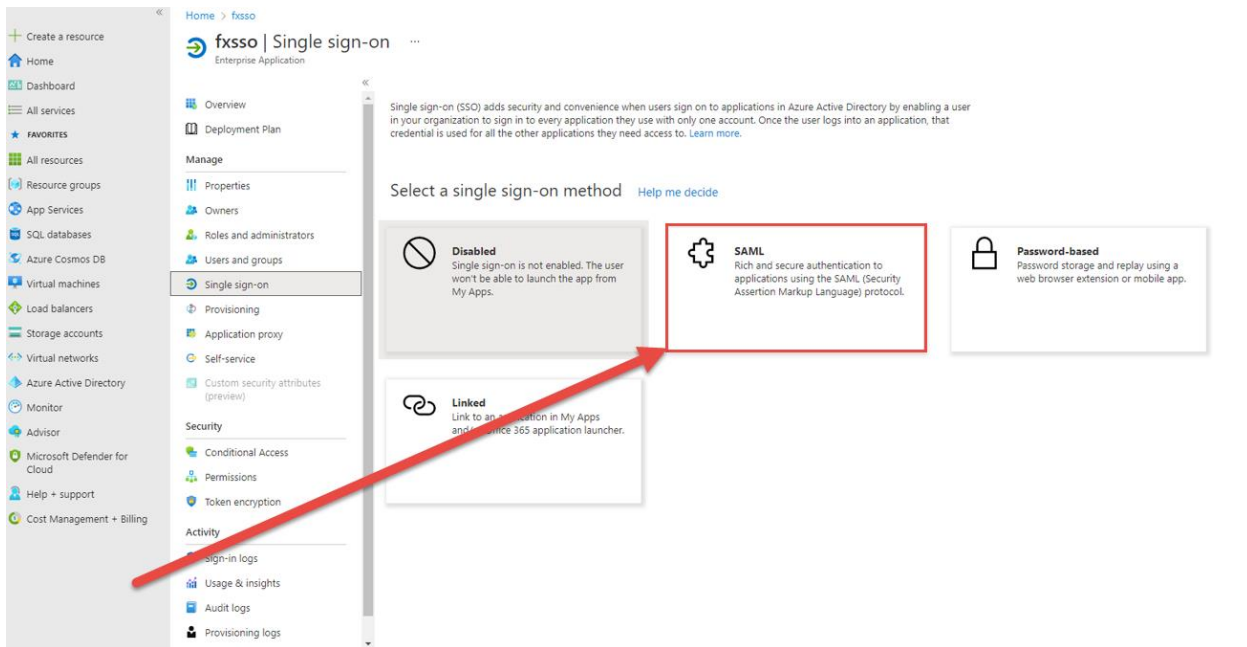
1. Login to the Azure portal and create an application for ATIPXpress (under **Enterprise Application**), and Select **Set up Single Sign On**:

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

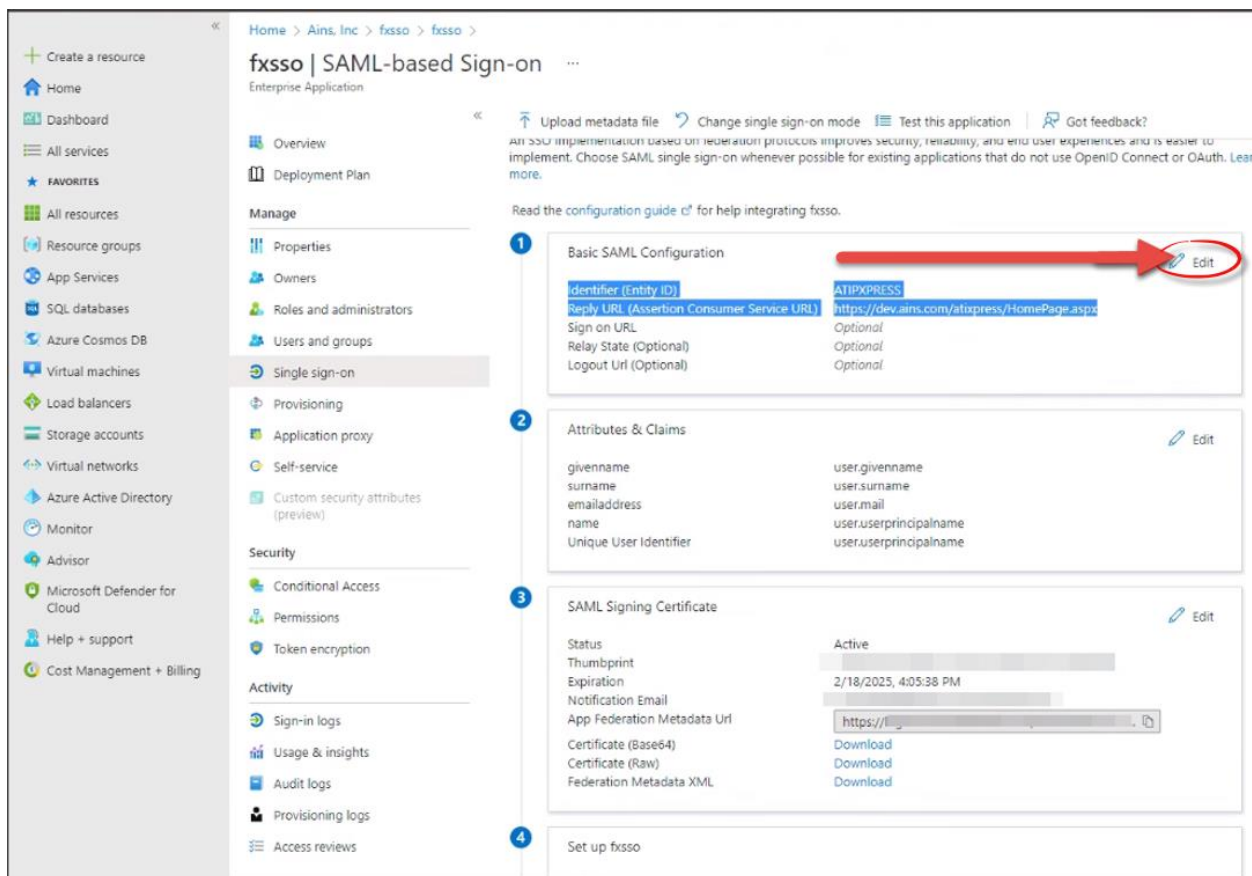


2. Click **SAML**:

Azure AD Configuration



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

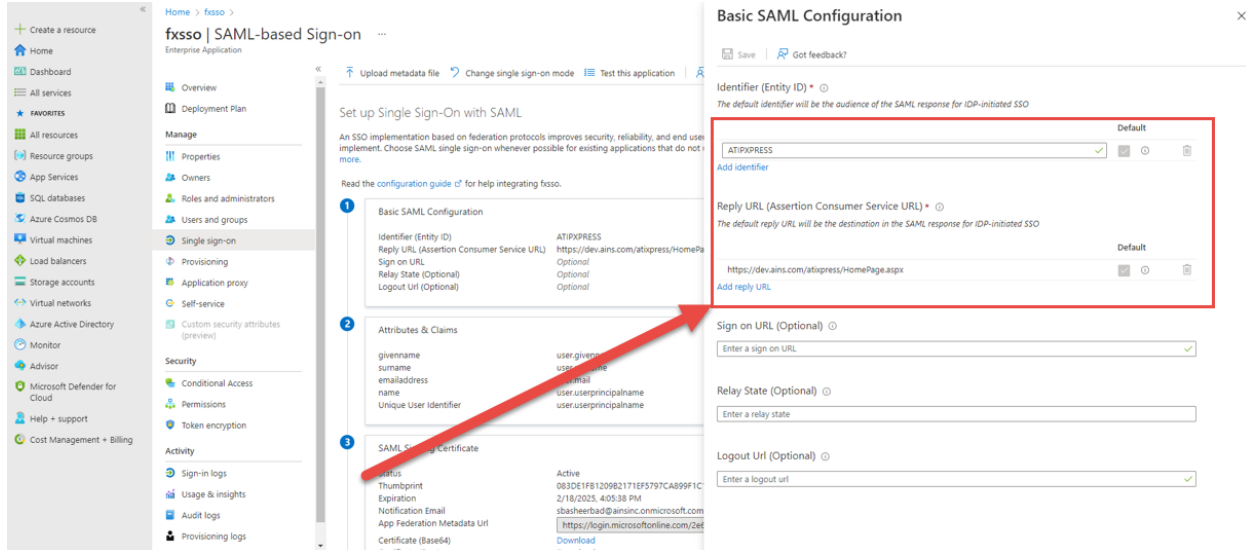


4. Enter the **Entity ID** that OPEXUS provided into the *Identifier (Entity ID)* field.



Azure AD Configuration

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**.

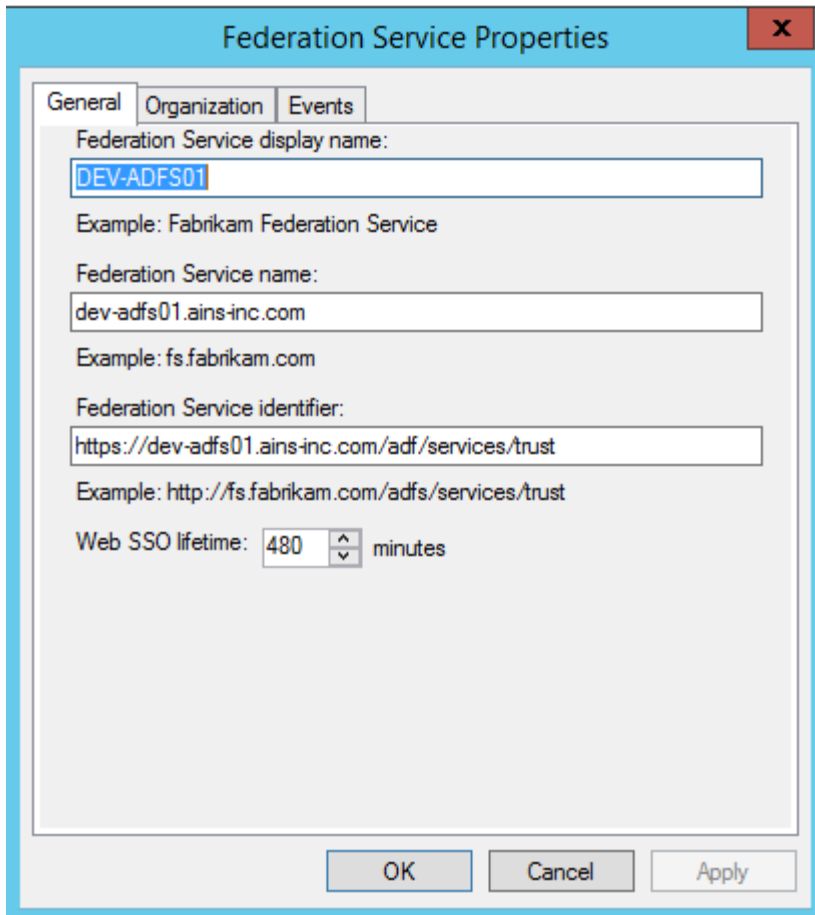


5. Once complete, download the **Federation Metadata XML** and email it to your OPEXUS Project Manager or Implementation Specialist.



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:



The screenshot shows the 'Federation Service Properties' dialog box with the 'General' tab selected. The fields are configured as follows:

- Federation Service display name:** DEV-ADFS01 (Example: Fabrikam Federation Service)
- Federation Service name:** dev-ads01.ains-inc.com (Example: fs.fabrikam.com)
- Federation Service identifier:** https://dev-ads01.ains-inc.com/adf/services/trust (Example: http://fs.fabrikam.com/adfs/services/trust)
- Web SSO lifetime:** 480 minutes

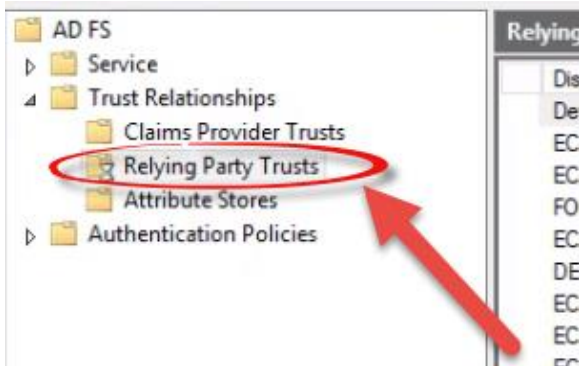
At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

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.

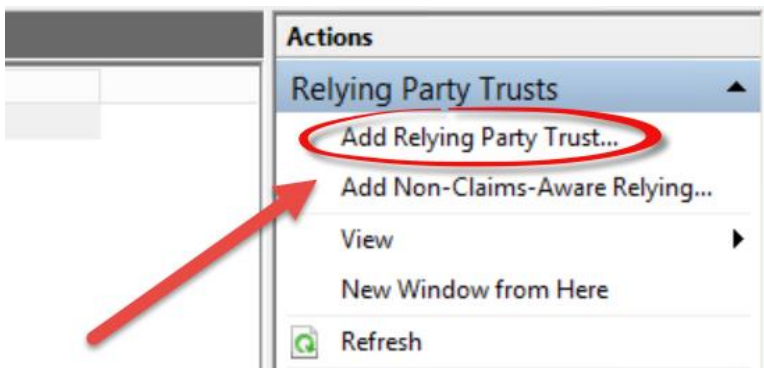
3.1 Add Relying Party Trusts

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

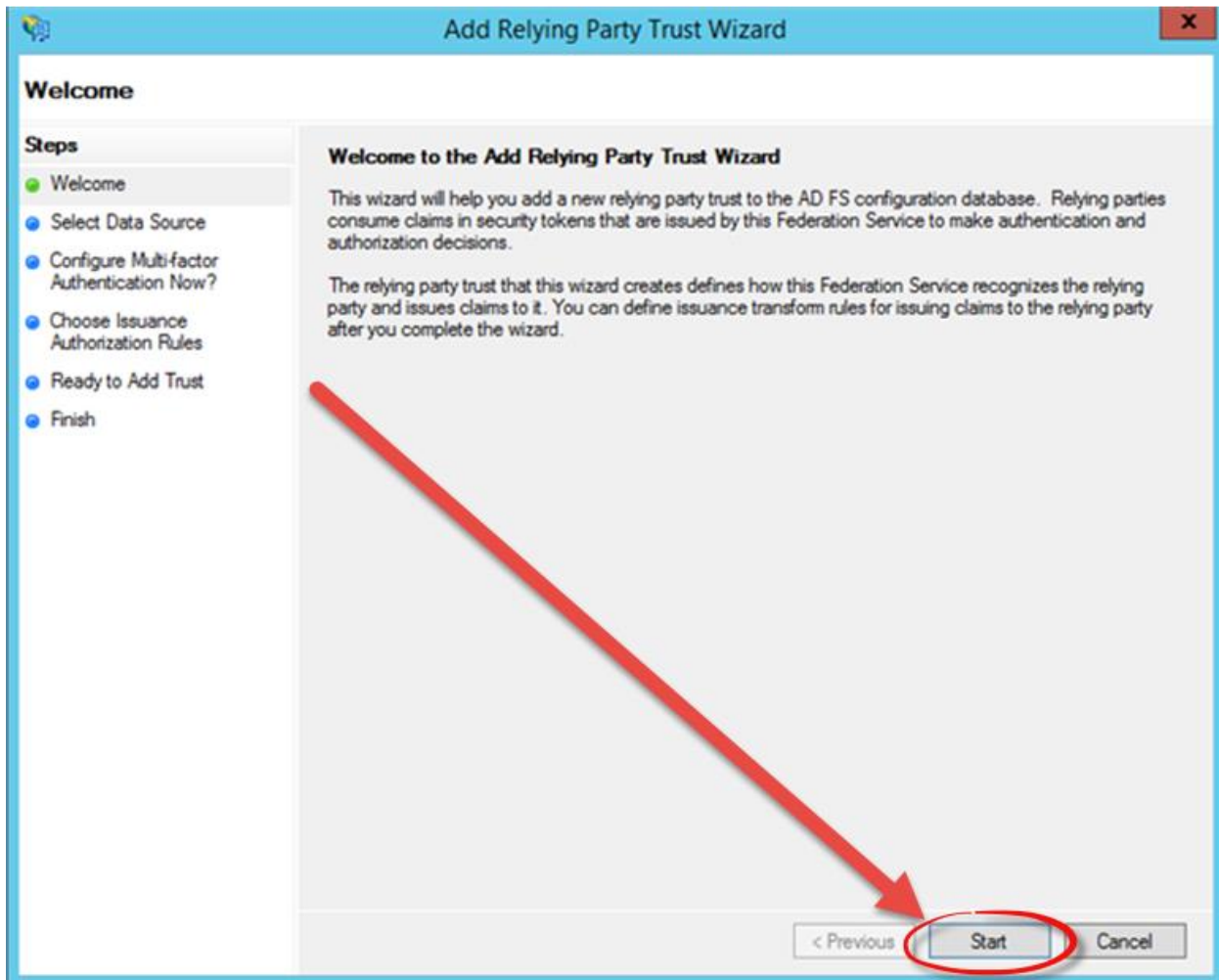
1. Login to the ADFS server and click **AD FS Management** within the *Administrative Tools* application menu. The *AD FS* window appears.
2. Expand the *Trust Relationship* folder to display the *Relying Party Trusts* subfolder. Click **Relying Party Trusts**.



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**.

Install and Configure ADFS Service

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main window has a light blue header with the text 'Select Data Source'. On the left, there is a 'Steps' pane with a list of steps: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area of the wizard contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network'. Below this is a text box for 'Federation metadata address (host name or URL):' with an example: 'fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Below this is a text box for 'Federation metadata file location:' with a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected). Below this is a text box for 'Enter data about the relying party manually'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure 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 online or on a local network.

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 exported 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.

Federation metadata file location:

Browse...

☒ Enter data about the relying party manually

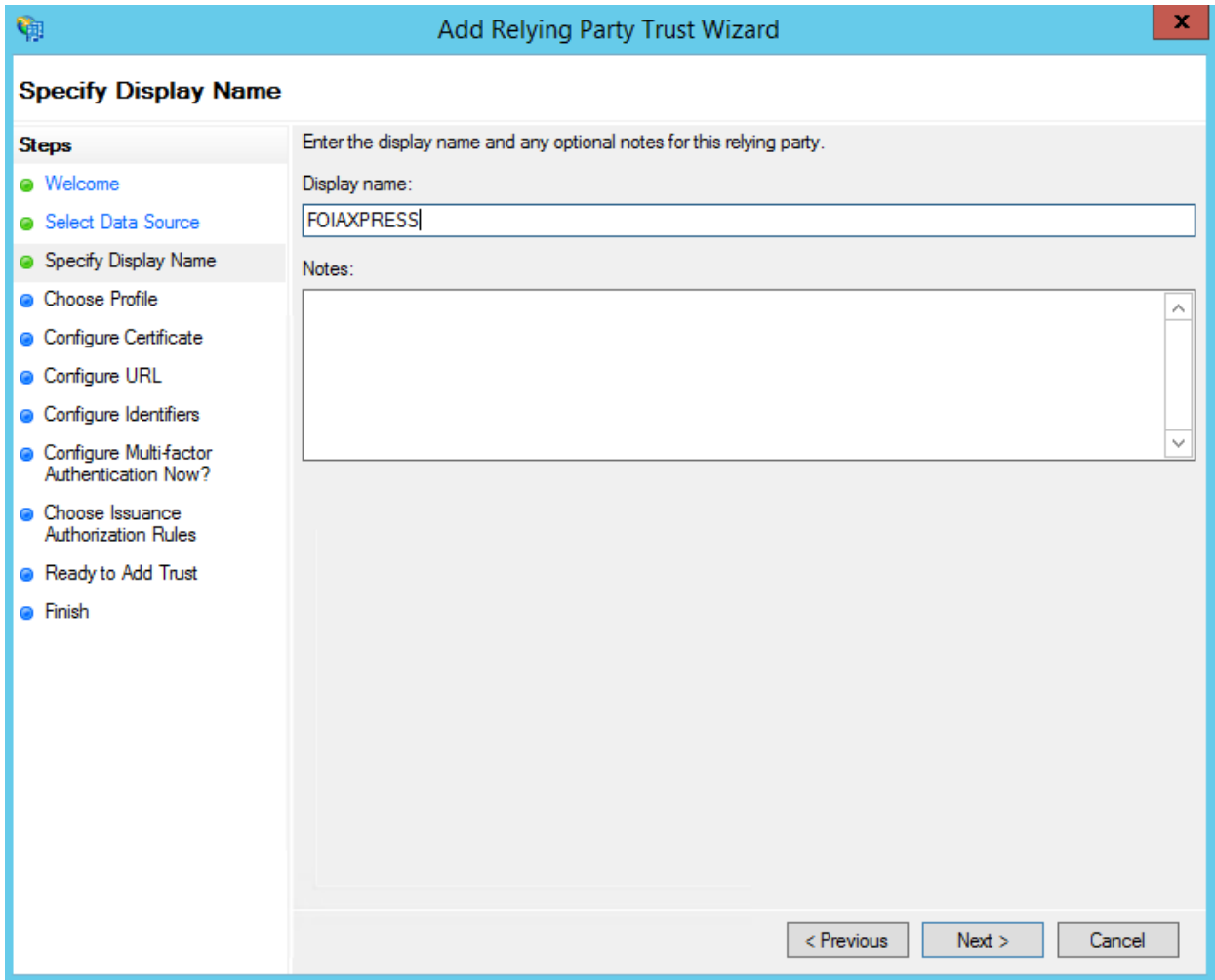
Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

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



Install and Configure ADFS Service



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main window has a light blue header with the text 'Specify Display Name'. On the left, there is a 'Steps' pane with a list of steps: 'Welcome', 'Select Data Source', 'Specify Display Name' (highlighted with a green dot), 'Choose Profile', 'Configure Certificate', 'Configure URL', 'Configure Identifiers', 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area of the wizard has a light gray background. At the top, it says 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label and a text box containing 'FOIAXPRESS'. Below the text box is a 'Notes:' label and a large text area. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name:

FOIAXPRESS

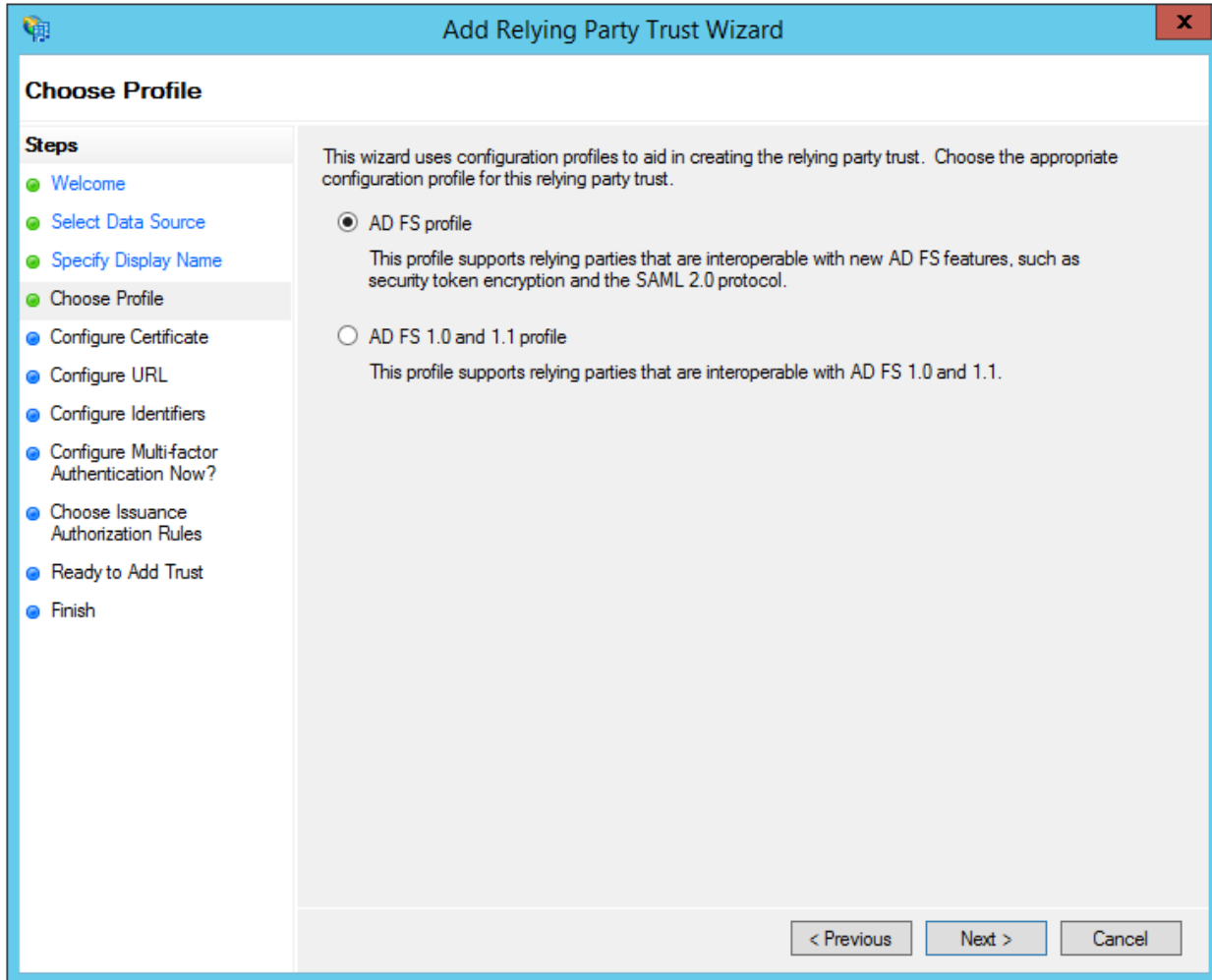
Notes:

< Previous Next > Cancel

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



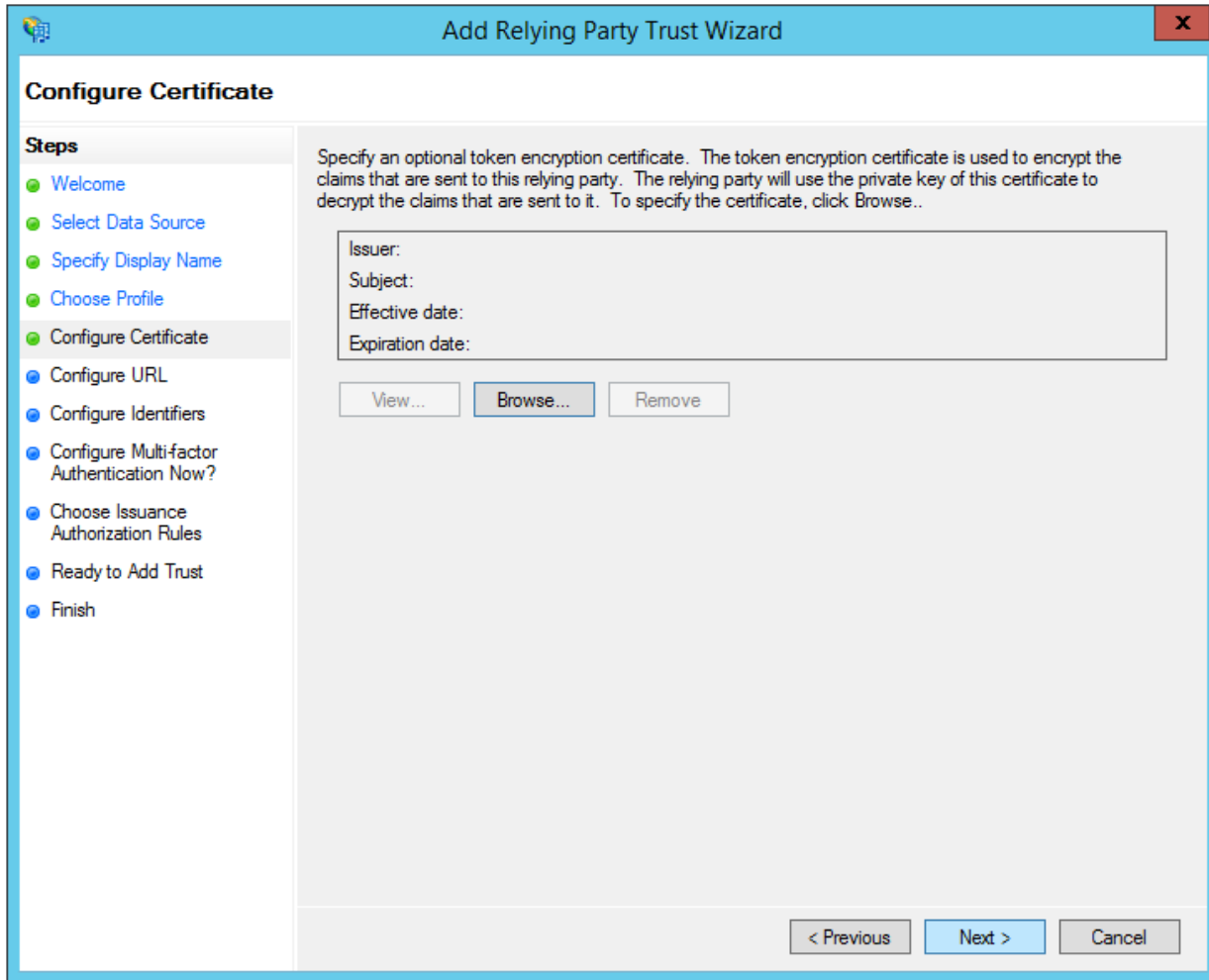
Install and Configure ADFS Service



8. Click **Next**.



Install and Configure ADFS Service



Add Relying Party Trust Wizard

Configure Certificate

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate**
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

< Previous Next > Cancel

Install and Configure ADFS Service

The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Configure URL' step selected in the left-hand 'Steps' pane. The main area contains instructions and configuration options for the WS-Federation Passive protocol and the SAML 2.0 WebSSO protocol. The 'Enable support for the SAML 2.0 WebSSO protocol' checkbox is checked, and the 'Relying party SAML 2.0 SSO service URL' field contains the text 'https://fxdev.ains.com/foiaexpress/HomePage.aspx'. The 'Previous', 'Next', and 'Cancel' buttons are at the bottom right.

Add Relying Party Trust Wizard

Configure URL

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

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.

Relying party 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:

`https://fxdev.ains.com/foiaexpress/HomePage.aspx`

Example: `https://www.contoso.com/adfs/ls/`

< Previous Next > Cancel

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



Add Relying Party Trust Wizard

Configure Identifiers

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

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

FOIAXPRESS

Add

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

Remove

< Previous Next > Cancel

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

Install and Configure ADFS Service

Add Relying Party Trust Wizard

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
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.

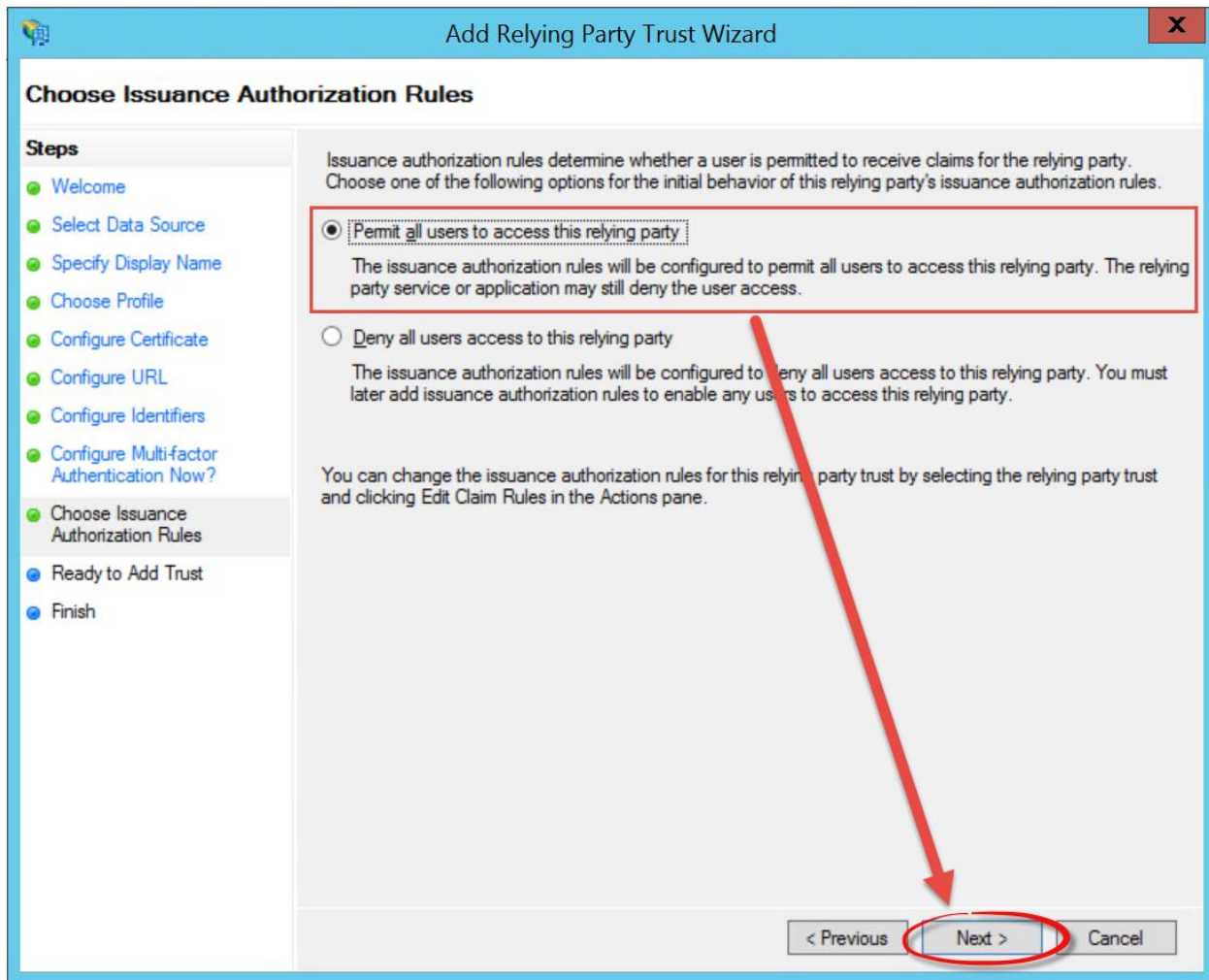
☐ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous **Next >** Cancel

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**.

Install and Configure ADFS Service



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

Install and Configure ADFS Service

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main window has a light blue header with the text 'Ready to Add Trust'. On the left, there is a 'Steps' pane with a list of 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 (highlighted), and Finish. The main area contains a message: '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.' Below this message is a tabbed interface with tabs: Monitoring (selected), Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Notes. The 'Monitoring' tab is active, showing a section titled 'Specify the monitoring settings for this relying party trust.' with a text box for 'Relying party's federation metadata URL:' and two checkboxes: 'Monitor relying party' and 'Automatically update relying party'. Below these are two status lines: 'This relying party's federation metadata data was last checked on: < never >' and 'This relying party was last updated from federation metadata on: < never >'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

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 | Notes

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

☐ Monitor relying party

☐ Automatically update relying party

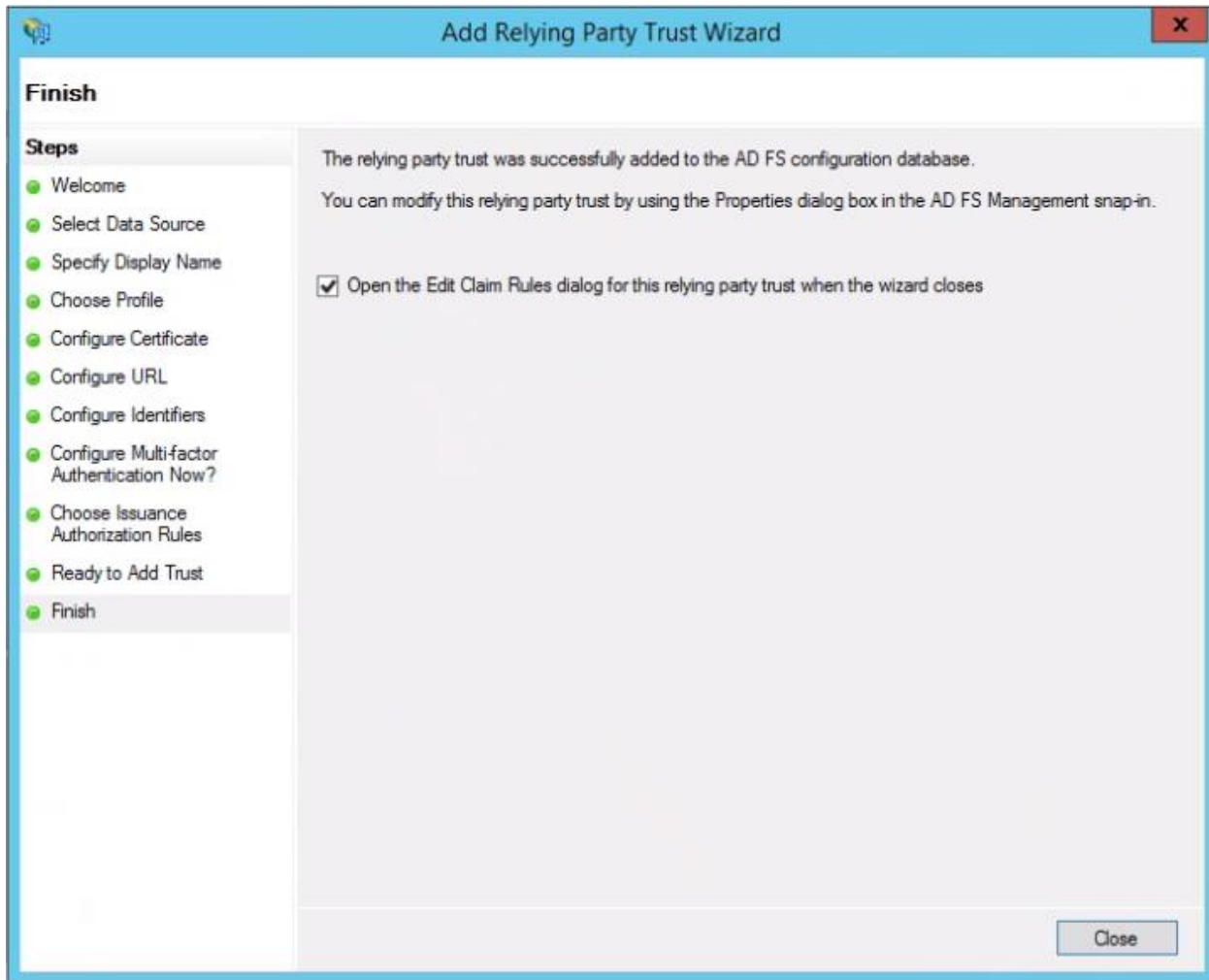
This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

< Previous Next > Cancel

15. Click **Next**.



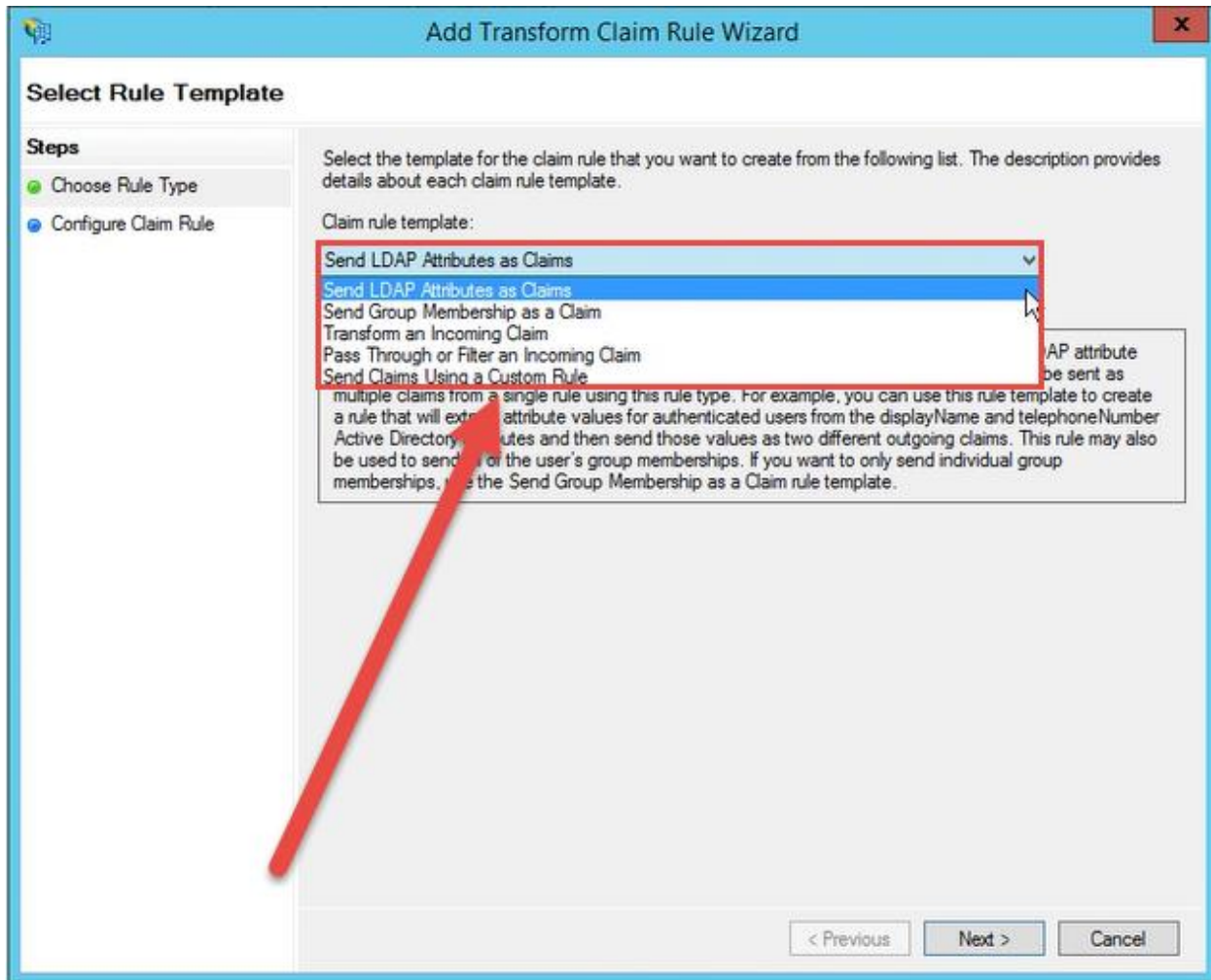


16. Ensure the **Open the Edit Claim Rules** checkbox is selected, and then click **Close**. The *Edit Claim Rules* pop-up window appears.

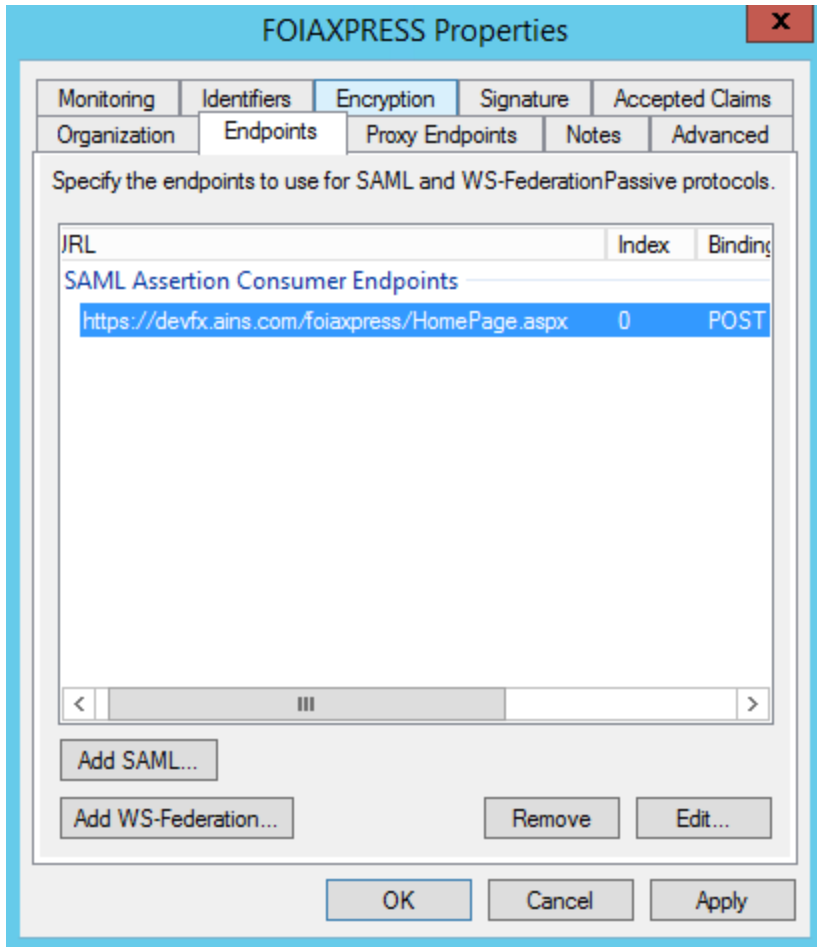
(!!) Note: You can navigate directly to the *Edit Claim Rules* pop-up window by selecting *Edit Claim Rules* in the right panel of the *ADFS Management Console*.

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**.



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.



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

21. Click **OK**.

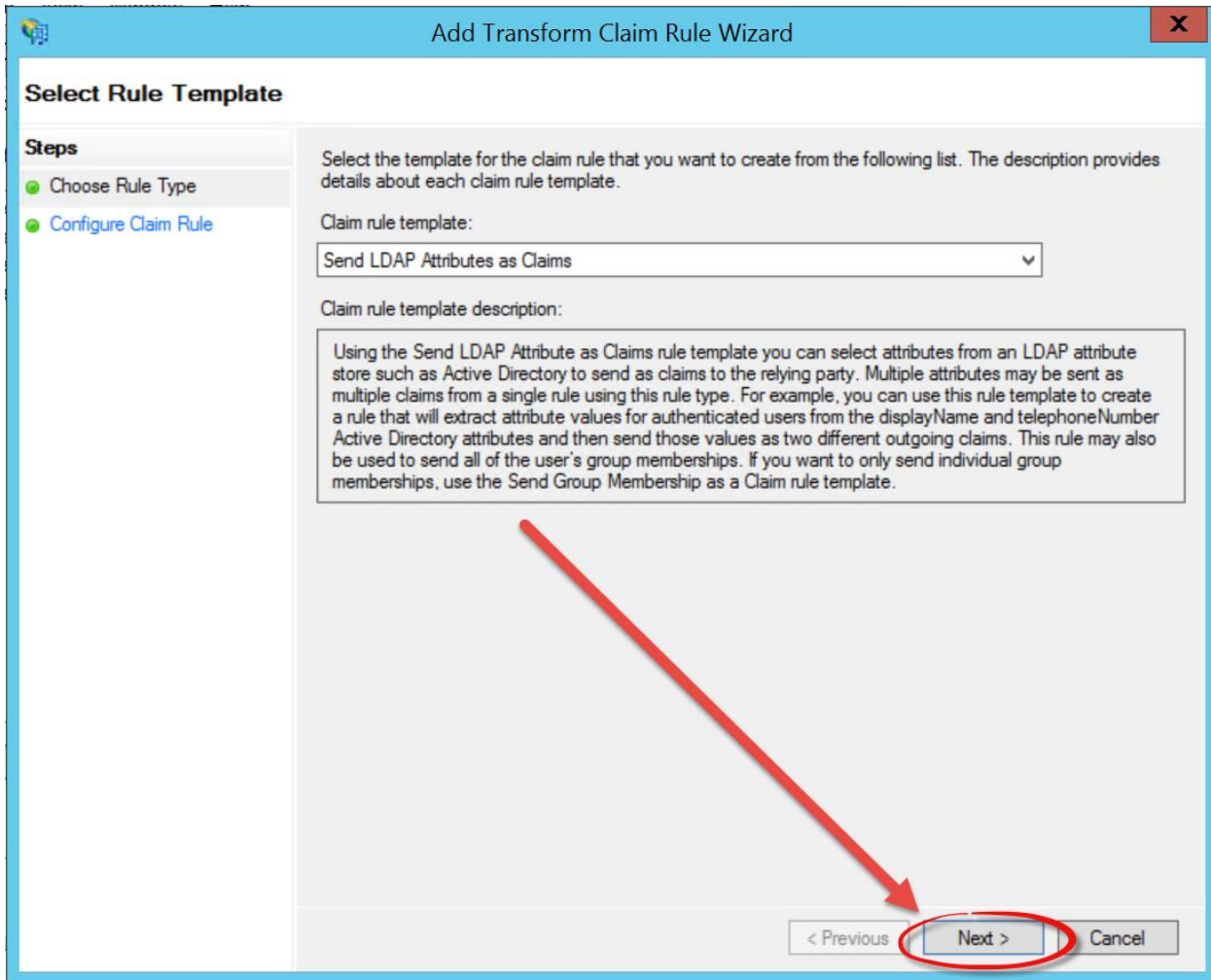
3.2 Configure the Claim Rules

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**.



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*.

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 issued from the rule.

Claim rule name:
FOIAXpress

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)	Outgoing Claim Type (Select or type to add more)
	SAM-Account-Name	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* drop-down list.
10. Select **Surname** from the *Outgoing Claim Type* drop-down list.
11. Click **Finish** to save the changes.

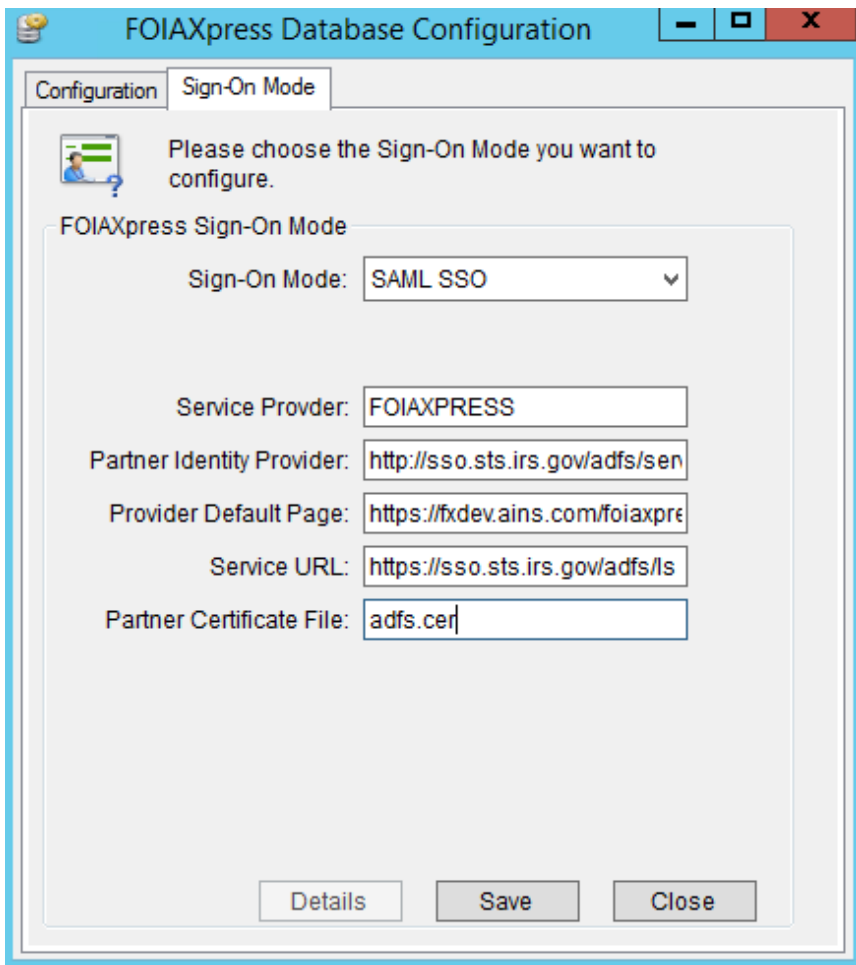
3.3 ATIPXpress Configuration for SAML SSO

To complete the ATIPXpress Configuration for SAML SSO:

1. Login to the ATIPXpress 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: ATIPXPRESS
- c. **Partner Identity Provider:** (federation service identifier for ADFS)
- d. **Provider default page:** The application URL. (ATIPXpress App URL ends with /ATIPXpress/HomePage.aspx)
 - i. Example: https://fxdev.ains.com/ATIPXpress/HomePage.aspx
- e. **Service URL:** The Login page from the Identity Provider (ADFS SSO URL ends with /ADFS/ls)
- f. **Partner Certificate File:** (It should be the signing certificate from ADFS or Internet Information Services (IIS) cert)



The screenshot shows a Windows application window titled "FOIAXpress Database Configuration". It has two tabs: "Configuration" and "Sign-On Mode", with "Sign-On Mode" currently selected. The window contains a message: "Please choose the Sign-On Mode you want to configure." Below this, there is a section titled "FOIAXpress Sign-On Mode" with several input fields:

- Sign-On Mode:** A dropdown menu set to "SAML SSO".
- Service Provider:** A text box containing "FOIAXPRESS".
- Partner Identity Provider:** A text box containing "http://sso.sts.irs.gov/adfs/sen".
- Provider Default Page:** A text box containing "https://fxdev.ains.com/foiaxpre".
- Service URL:** A text box containing "https://sso.sts.irs.gov/adfs/ls".
- Partner Certificate File:** A text box containing "adfs.cer".

At the bottom of the window, there are three buttons: "Details", "Save", and "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 <appsettings> 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:

The screenshot shows the 'Authentication Configuration' page in the PAL system. On the left is a navigation menu with options like General Settings, Enterprise, Modules, Web API, Security, Authentication, Email Templates, Email Log, Users, Audit Log, Requester Fields, Request Fields, Appeal Fields, Other Settings, Reading Room, Reading Room Documents, Display Order, Dashboard Administration, and Online Payment. The main content area is titled 'Authentication Configuration' and includes a note: 'Please complete all the required fields marked with an asterisk(*)'. Below this is a section titled 'Authentication Options' with two radio buttons. The first option, 'Enable Login with Forms Authentication', is unselected. The second option, 'Enable Login with SAML Authentication', is selected. Under the SAML option, there is a text box with the instruction 'Use SAML Configuration Tool for configuring identity provider.' and a 'Save' button at the bottom right.

- Click **Save**, then see the
- 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:

- Log in to *PAL Configuration* and select **Request Fields** in the left-hand menu.
- 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.

Request Fields Configuration
Please complete all the required fields marked with an asterisk (*).

[Save/Check](#)

Label Name	Display Name	Notes	Required	Visible	Default	Display Information
General Information (Header)						
Action Office	Regional Office		<input type="checkbox"/>	<input type="checkbox"/>	Default Office: Headquarters	Action Office Name
Action Office Details	Regional Office Instructions		<input type="checkbox"/>	<input type="checkbox"/>	Allowed Offices: 5 items checked	Action Office Details
Request Type	Request Type		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Requester Category	Requester Category		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Use Profile Category	
Delivery Mode	Delivery Mode		<input type="checkbox"/>	<input type="checkbox"/>	File	
Payment Mode	Payment Mode		<input type="checkbox"/>	<input type="checkbox"/>		
Expedite Information (Header)						
Expedite Requested	Expedite Requested		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Expedite Reason	Expedite Reason		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Expedite Request Status	Expedite Request Status		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Shipping Address (Header)						
Street1	Street1		<input type="checkbox"/>	<input type="checkbox"/>		
Street2	Street2		<input type="checkbox"/>	<input type="checkbox"/>		
City	City		<input type="checkbox"/>	<input type="checkbox"/>		
State	State		<input type="checkbox"/>	<input type="checkbox"/>		
State (Other)	State (Other)		<input type="checkbox"/>	<input type="checkbox"/>		
Country	Country		<input type="checkbox"/>	<input type="checkbox"/>		
Zip Code	Zip Code		<input type="checkbox"/>	<input type="checkbox"/>		
Request Information (Header)						
Description Document	Description Document		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
* Description	Description		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Date Range for Record Search	Date Range for Record Search		<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Proof of Identity/Consent (Header)						
Proof of Identity Mode	Verification Mode		<input type="checkbox"/>	<input type="checkbox"/>	Proof of Identity Option: Upload Attachment	
Consent	Consent Form		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Upload Attachment	
Proof of Identity	Proof of Identity/Consent Form		<input type="checkbox"/>	<input type="checkbox"/>	Upload Attachment	
Digital Authentication	Digital Authentication		<input type="checkbox"/>	<input type="checkbox"/>		

- 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 'ATIPXpress.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:

Certificates

Signature Certificate Text:

Encryption Certificate Text:

OR

IDP Certificate :

☐ 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

SAML Field Mappings

	PAL Field	Provider Field	Description	Action
▶	Login	email	attribute used to login	Delete
	Email	email	email address	Delete
	First Name	first_name	first name	Delete
	Last Name	last_name	last name	Delete

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



The screenshot shows a 'SAML Configuration' window. At the top, 'Use of SAML' is set to 'SAML Using For: Login'. Below this, the 'Service Provider' section includes fields for 'Issuer' (marked with a red asterisk), 'Assertion Consumer URL' (marked with a red asterisk), 'Signature Certificate' (with a 'Browse' button and a red 'X' icon), 'Signature Certificate Password', 'Encryption Certificate' (with a 'Browse' button and a red 'X' icon), and 'Encryption Certificate Password'. The 'Identity Provider' section includes fields for 'IDP Entity ID/Issuer URL' (marked with a red asterisk), 'SAML SSO URL', 'SAML SSO URL Binding Type', 'SAML SLO URL', 'SAML SLO URL Binding Type', 'Name ID Format', 'Authentication Context', and 'Authentication Context Comparison'.

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

Field	Description
Signature Certificate/Encryption Certificate	<p>Use the PFX file that you have ready for SAML use, as mentioned at the beginning of this document.</p> <p>(!!) 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 from this PFX file and replace your public key in the Identity Provider account with this public key.</p> <p>Enter the password for the PFX file in the Signature Certificate Password/Encryption Certificate Password fields. Also provide the IDP Entity ID/Issuer URL.</p>

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

Identity Provider	
* IDP Entity ID/Issuer URL :	<input type="text"/>
SAML SSO URL:	<input type="text"/>
SAML SSO URL Binding Type:	<input type="text"/>
SAML SLO URL:	<input type="text"/>
SAML SLO URL Binding Type:	<input type="text"/>
Name ID Format:	<input type="text"/>
Authentication Context:	<input type="text"/>
Authentication Context Comparison:	<input type="text"/>



Field	Description
IDP Entity ID/Issuer URL, SAML SSO URL, SAML SLO URL	<p>To be provided by IDP.</p> <p>(!!) Note:</p> <ul style="list-style-type: none"> 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. For some IDPs, SAML SSO URL and SAML SLO URL must be updated each year, approximately quarterly.
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:

★ Certificates

Signature Certificate Text:

MIID7TCCAtWgAwIBAgIUCethW2gYqC2N96czVCEaAkR/AiAwI

Encryption Certificate Text:

MIID7TCCAtWgAwIBAgIUCethW2gYqC2N96czVCEaAkR/AiAwI

OR

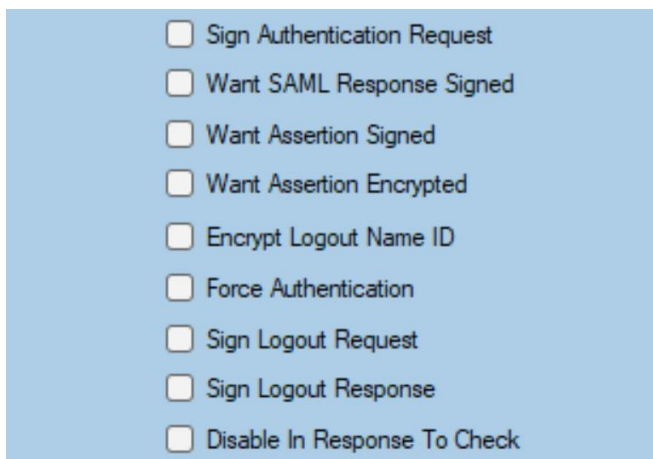
IDP Certificate :

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 SAML 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.



A screenshot of a configuration interface showing a list of checkboxes on a light blue background. The checkboxes are arranged vertically and are all currently unchecked. The labels for the checkboxes are: 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, and 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.



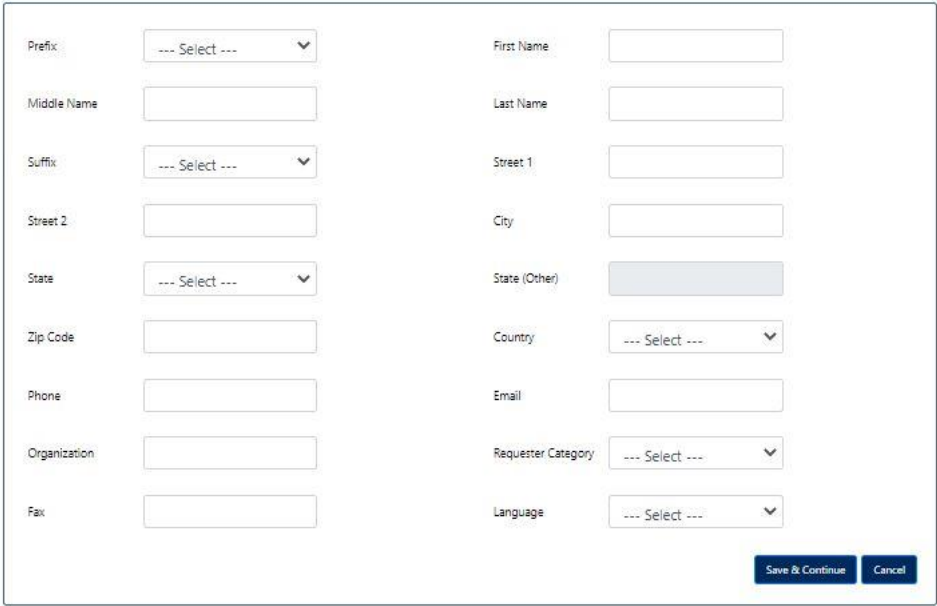
SAML Field Mappings

	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

Add

Save Close

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

Column	Description
PAL Field (Login)	<p>PAL Fields are the labels for corresponding provider fields that are displayed in the SAML Requester Registration page for a new requester (requester whose email doesn't exist in the PAL).</p>  <p>The screenshot shows a registration form titled "We need to capture the following information to serve you better." The form contains the following fields:</p> <ul style="list-style-type: none"> Prefix: Dropdown menu (--- Select ---) Middle Name: Text input Suffix: Dropdown menu (--- Select ---) Street 2: Text input State: Dropdown menu (--- Select ---) Zip Code: Text input Phone: Text input Organization: Text input Fax: Text input First Name: Text input Last Name: Text input Street 1: Text input City: Text input State (Other): Text input Country: Dropdown menu (--- Select ---) Email: Text input Requester Category: Dropdown menu (--- Select ---) Language: Dropdown menu (--- Select ---) <p>At the bottom right of the form are two buttons: "Save & Continue" and "Cancel".</p>
Provider Field	Provider Fields are the corresponding IDP attribute names for the requester's details such as first name, last name, address 1, and country.
Description	Description of mapped 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.

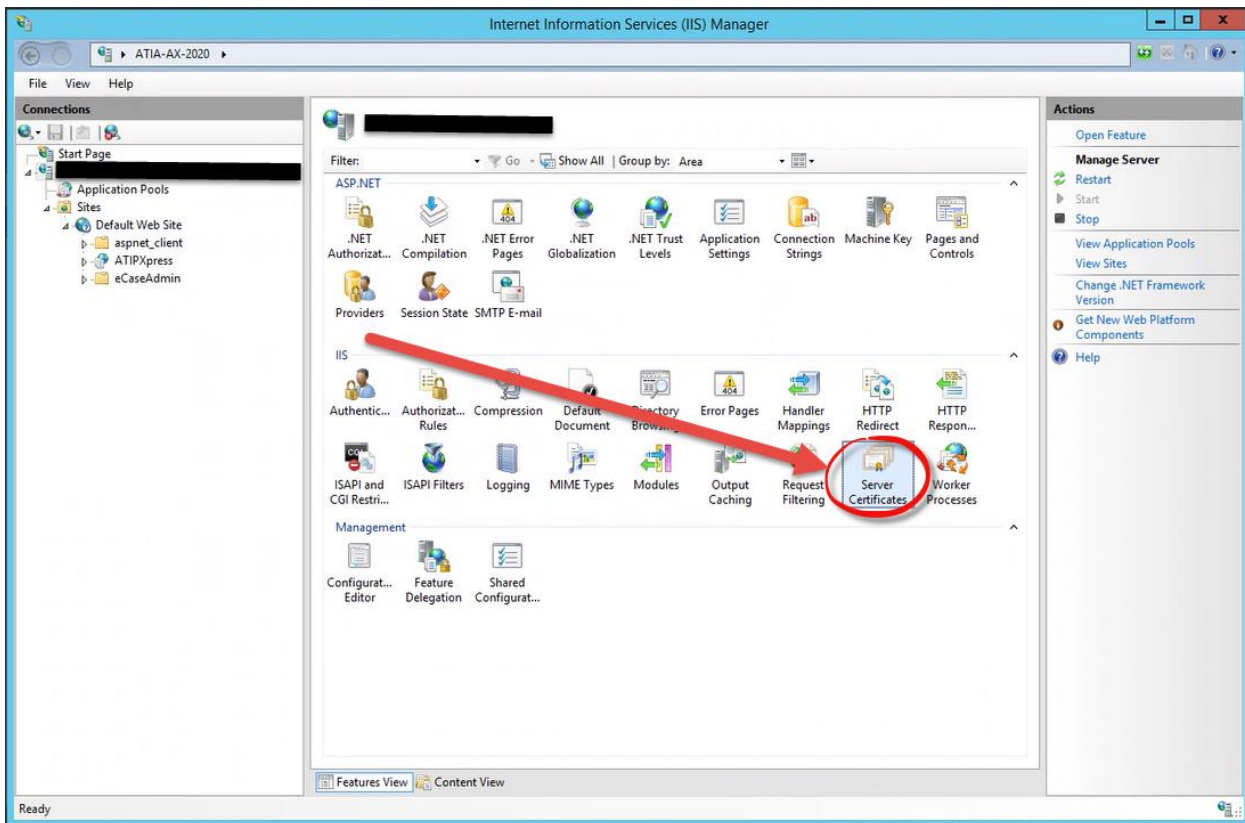


For login.gov, please visit <https://developers.login.gov/> for all details about identity provider fields.

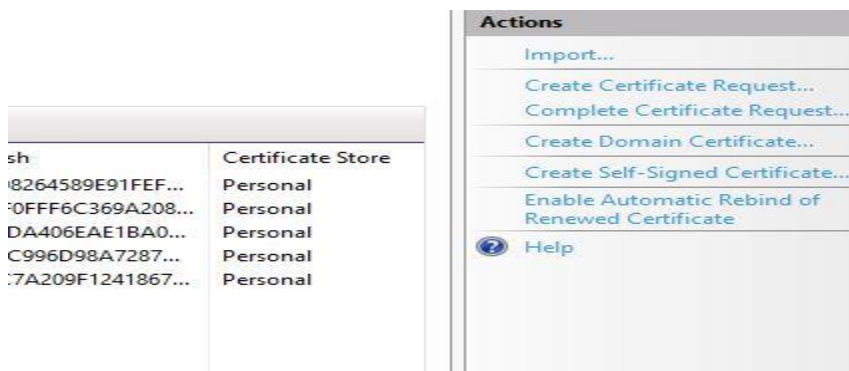
4.3 Create PFX Certificate

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

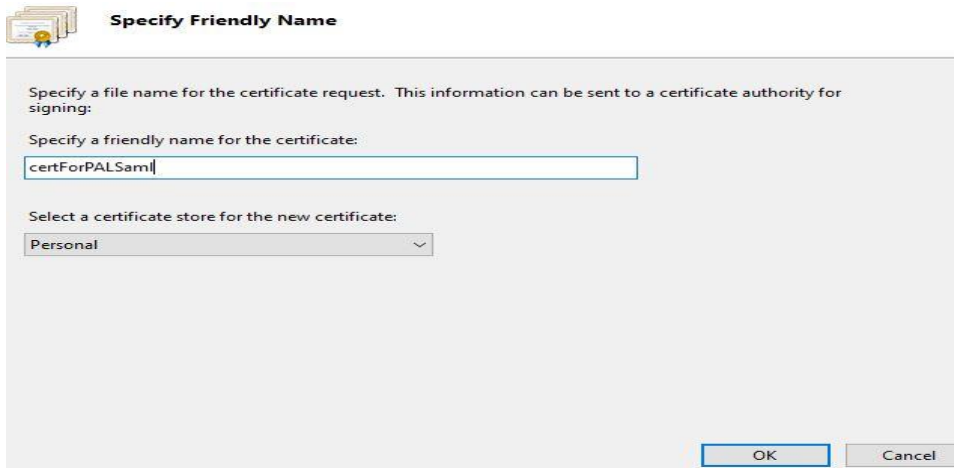
1. Open IIS and click **Server**.
2. In the *Security* section, double click the **Server Certificates**



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 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.

