FOIAXpress

OPEXUS

Collaboration Portal SAML SSO Configuration

Version 1.0

v11.5.0

January 2024

FX v11.5.0 Collaboration Portal SAML SSO Configuration

Notice of Rights

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 Collaboration Portal SAML SSO Configuration

1.1 About SAML SSO Configuration

To log into Collaboration Portal with SAML Single Sign On (SSO), you'll need to configure your application. Your ID provider will request an SP entity ID, Assertion URL, and public key.

(!!) Note: Before starting SAML SSO, you will need to have PFX certificate.

1.2 Using This Manual

The following formatting conventions are used in this manual to highlight important information:

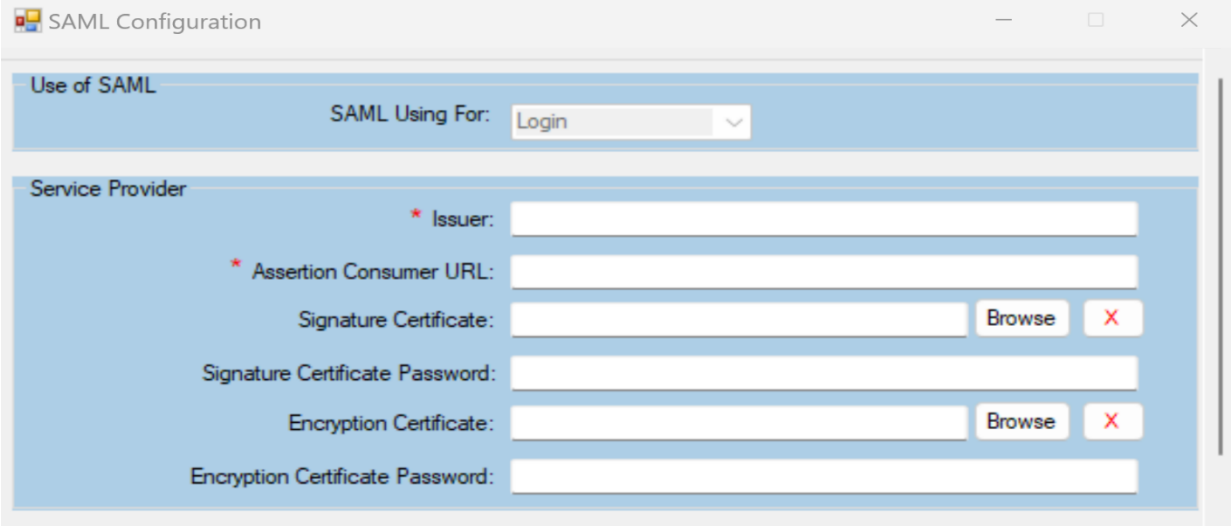
- *Italicized* text indicates a location, for example a particular *Folder*, *Tab*, or *Window*.
- **Bold** text indicates a specific user action, such as clicking a **button**.
- **Red** text and this symbol **(!!)** are used in Notes to **bring attention to crucial information**.

1.3 Complete SAML Configuration

1. Go to the Collaboration Portal application location (on the application server) and open the *Tools* folder.
2. Right click on **SAML Config** and select **Run as administrator**.

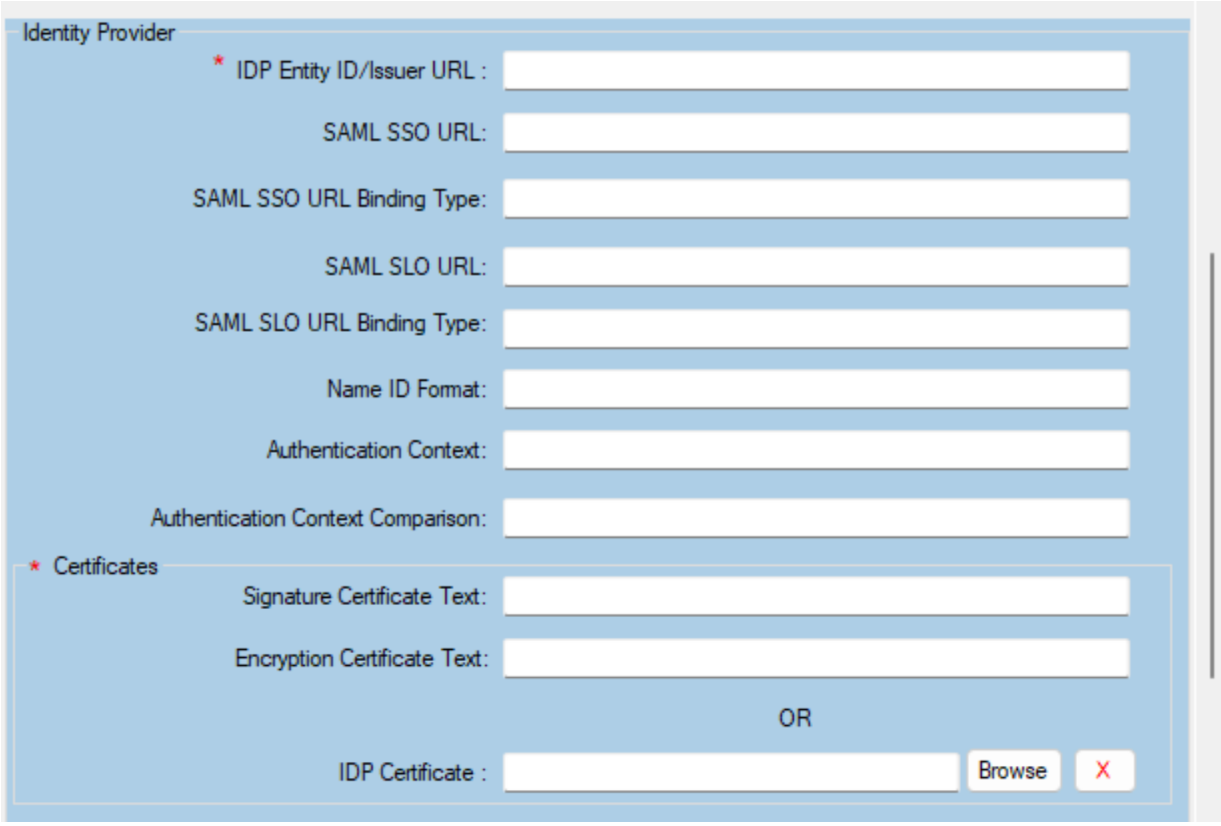
(!!) Note: White space characters are not allowed in any of the fields. Do not include any leading or trailing white space characters if you are copying text from other sources.

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



Field	Description
Issuer	Enter the Issuer (SP Entity ID) provided by your Identity Provider. **(!!) Note: This is case-sensitive.**
Assertion Consumer URL	https:// CollabAppURL /AssertionConsumerService.aspx **(!!) Note: Replace 'CollabAppURL in the above URL with your Collaboration Portal Application URL. For example:** https://dns/Collaboration/AssertionConsumerService.aspx **or** https://dns:8443/Collaboration/AssertionConsumerService.aspx
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 the public key in your 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.**

4. Next, complete the required Identity Provider fields, as shown below:



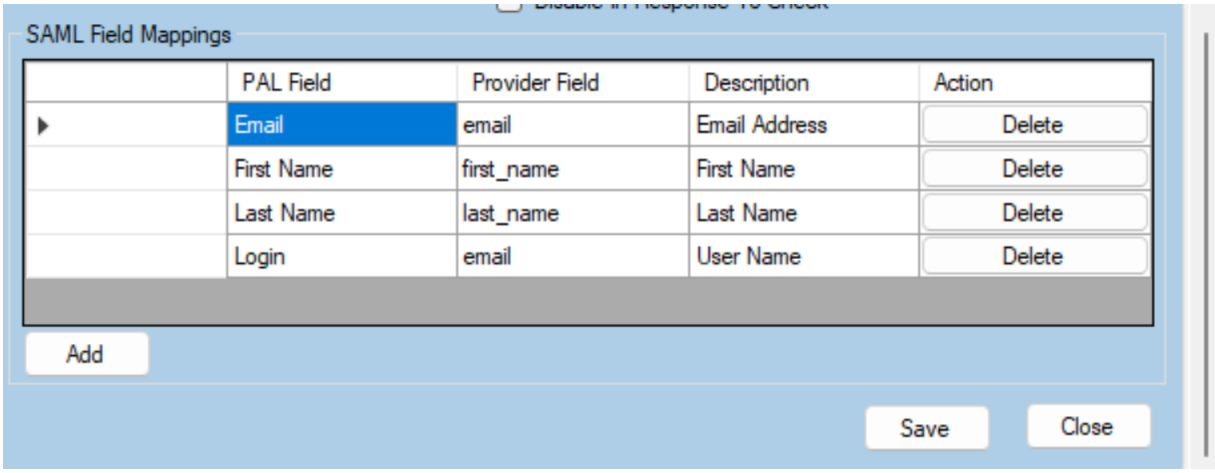
(!!) Note: Your Identity Provider provides you either an xml file or a URL with the metadata that you'll need for this form. We recommend using the 'Signature Certificate Text' and 'Encryption Certificate Text'. If your ID provider has provided only x509 certificate text, then use the same certificate text for both.

5. Configure the following list of checkboxes as needed. By default, all the checkboxes are unchecked. We recommend checking Sign Authentication Request, Want Assertion Signed, and Force Authentication.

(!!) Notes:

- **If you are using Single Logout Service, then you must check Sign Logout Request and Sign Logout Response.**
- **We recommend that you do not check Disable In Response To Check unless IDP initiated SSO is required. Please verify this with your Identity Provider. Most Identity Providers work with SP initiated SSO and do not require users to enable this option.**

6. The SAML Field Mappings table defines the attributes used for login. Only email and login fields are required. Values of Provider Field for email and login should be available in IDP Provider's metadata.



1.4 Change Collaboration Portal Login Type

Once you have completed the steps above and saved the SAML configuration, you need to change the login type for your Collaboration Portal application.

1. Go your Collaboration Portal application location on the application server and open the *Tools* folder.
2. Right click **Database Configuration** and select **Run as administrator**.
3. Select **FOIAXpress Application/ATIPXpress Application** from the dropdown Application/Service menu.
4. If you have already configured the database, click **Save**.
5. You will likely see an option for Sign-On Mode. If you do not see this option, then you may need to select **All** from dropdown Application/Service and **Save** the details.
6. Click **Sign-On Mode** and select **SAML SSO** option from the Sign-On Mode drop-down and save the changes.
7. Reset/restart the IIS.