FOIAXpress

# SAML SSO Login

v11.8.0

October 2024

OPEXUSTECH.COM

# FOIAXpress v11.8.0 SAML SSO Login

## 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 (OPEXUS, 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: OPEXUS, 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 OPEXUS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from OPEXUS, 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 OPEXUS, 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.

# Version History

| # | Date | Description |
|---|---|---|
| 1.0 | 5/30/2024 | New document for v11.7.0:<br>▪ We've split this document from the PAL SAML Configuration for clarity.<br>▪ Updated Section 4 -FOIAXpress Configuration for SAML SSO with new screens and additional details on the configuration fields |
| 2.0 | 10/4/2024 | Updates for v11.8.0:<br>▪ Removed outdated content that is no longer required as part of SAML Configuration.<br>▪ Heavily revised section 3 – *FOIAXpress Configuration for SAML SSO* for clarity and ease of use.<br>▪ Added new section Update Assertion URL which is a new required process for v11.8.0. See section 2 for details.<br>▪ Added a new section with steps to retrieve your service provider metadata. This is an option step, see Section 4 – *Service Provider Metadata File* for details. |

# Contents

# 1 About SAML Login and Proof of Identity Configuration

The FOIAXpress SAML Login Configuration manual was created to assist administrators when configuring the SAML SSO Login. It covers the following information:

1. Updating the Assertion URL (new for v11.7.0 and up)
2. FOIAXpress Configuration for SAML SSO.
3. Retrieving the Service Provider Metadata File

# 2 Update Assertion URL

Follow the steps in this section to update Assertion URL in FX/FX. This is required when upgrading to from any version below 11.7.2.

**Note: If the application is already on 11.7.2 or up, an assertion URL update is not required**

1. The customer must first obtain and provide their Identity Provider Metadata from their identity provider. This just be provided as either an XML file or URL.
2. Next, we'll confirm or update the Identity Provider Certificate in SAML Configuration. This must be confirmed otherwise SAML authentication will fail. Open the provided metadata file and locate for the signing cert in x.509 format, as highlighted below:


```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ID="_57bffb06-2281-4252-869d-57486d674975"
 entityID="https://idp.int.identitysandbox.gov/api/saml">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#_57bffb06-2281-4252-869d-57486d674975">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>FphGwjL+0bmaYBaLKHE2CgN7qujl+Tn8qQvTfRFgD10=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>xYDzjCCHMZyqWqzrnkUhIaDgxEoafBvRRW0e73u/CURXRNESej27qg9zshY1TiRtfNQLHDdtxOu8wWEmdZvlk1aGxeR8DI3zNSh+WIDrBH24j3W/QtlY
    </ds:SignatureValue>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIID7TCCAtWgAwIBAgIUYePi2i1UjRg3fIK0FG15rZaSOvAwDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlVTMR0wGwYDVQQIDBREaXN0cml
        </ds:X509Certificate>
      </ds:X509Data>
    </KeyInfo>
  </ds:Signature>
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>MIID7TCCAtWgAwIBAgIUYePi2i1UjRg3fIK0FG15rZaSOvAwDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlVTMR0wGwYDVQQIDBREaXN0cmljc
          </X509Certificate>
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://idp.int.identitysandbox.gov/api/saml/auth2024"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://idp.int.identitysandbox.gov/api/saml/auth2024"/>
  </IDPSSODescriptor>
  <AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>MIID7TCCAtWgAwIBAgIUYePi2i1UjRg3fIK0FG15rZaSOvAwDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlVTMR0wGwYDVQQIDBREaXN0cmljc
          </X509Certificate>
```


3. You'll use this value to create a certificate. Follow these steps:

a. Copy the **full text** following <X509Certificate> (highlighted in yellow below):

```
▼<X509Data>
  <X509Certificate>MIID7TCCAtWgAwIBAgIUYePi2i1UjRg3fIK0FG15rZaSOvAwDQYJKoZIhvcNAQELBQAwgY
  </X509Certificate>
</X509Data>
```

b. Open Notepad, then paste the copied Certificate text into a new Notepad document.

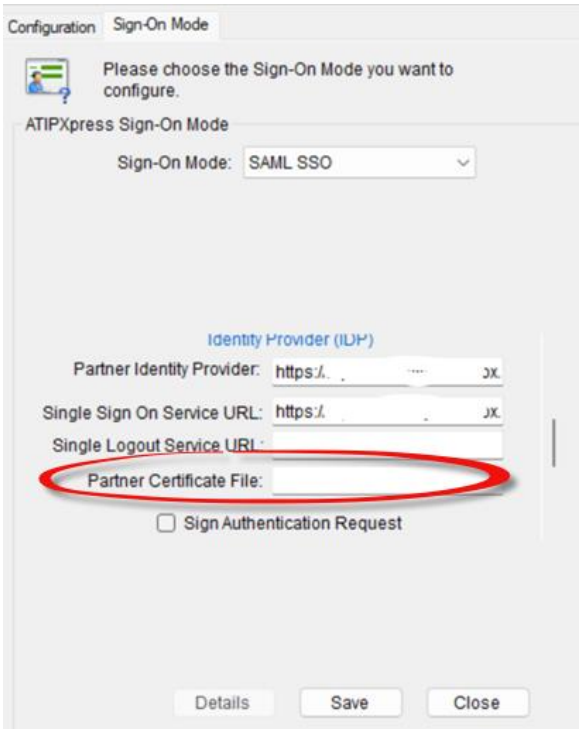
c. Paste the following at the beginning then hit Enter to add a line break:
-----BEGIN CERTIFICATE-----

d. Add another line break at the end, then paste the following on the new line:
-----END CERTIFICATE-----

e. It should look like the example below. Save the file with a .cer file extension

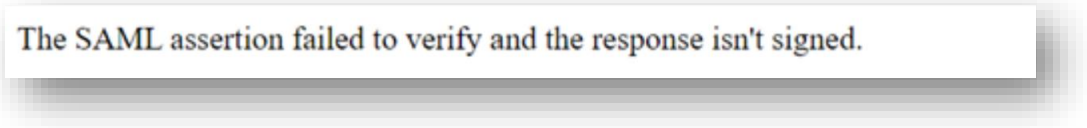
```
-----BEGIN CERTIFICATE-----

MIID7TCCAtWgAwIBAgIUYePi2i1UjRg3fIK0FG15rZaSOvAwDQYJKoZIhvcNAQELBQAwgYUxCzAJBgNVBAYTAlVTMR0wGwYDVQQIDBREaXN0cmljdCBv
ZiBDb2x1bWJpYTETMBEGA1UEBwwKV2FzaGluZ3RvbjEMMAoGA1UECgwDR1NBMRIwEAYDVQQLDAlMb2dpbi5nb3YxIDAeBgNVBAMMF2ludC5pZGVudGl0
eXNhbmRib3guZ292MB4XDTI0MDExNjIwMTEyMloXDTI1MDQwMTIwMTEyMlowgYUxCzAJBgNVBAYTAlVTMR0wGwYDVQQIDBREaXN0cmljdCBvZiBDb2x1
bWJpYTETMBEGA1UEBwwKV2FzaGluZ3RvbjEMMAoGA1UECgwDR1NBMRIwEAYDVQQLDAlMb2dpbi5nb3YxIDAeBgNVBAMMF2ludC5pZGVudGl0eXNhbmRi
b3guZ292MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0K9gJdCDRwndI
-----END CERTIFICATE-----
```

4. Save the .cer file in a location that is accessible by the FX/FX application, we suggest directly within the application folder.
5. Open the FOIAXpress Database Configuration tool, select the **Sign-On Mode** tab, then paste the file name (if placed within the application folder) or network location and file name in the *Partner Certificate File* field:



6. Update the *Assertion Service URL*. If you are upgrading from version 11.5.4 or under, you need to update the assertion URL after upgrade. See Section 1.2.1 in the v11.7.0 Release Notes for details.
7. You must request that the customer's SAML ID provider update the assertion URL on their end. The ID provider team can update the assertion URL on their end during or after an upgrade.

**Note: If you see the following error message, it is likely due to an incorrect identity provider's certificate.**

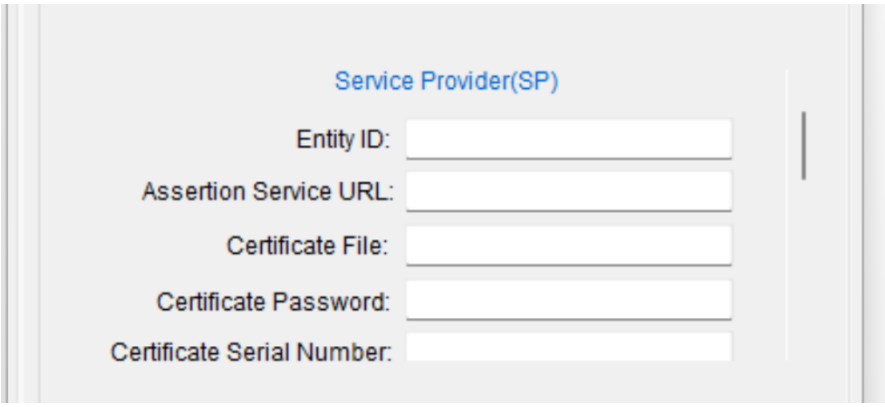


# 3 FOIAXpress Configuration for SAML SSO

To complete the FOIAXpress Configuration for SAML SSO:

1. Login to the FOIAXpress application server.
2. Run the Database Configuration tool as an Administrator.
3. Configure the database connection. If you have already configured the database connection, then save the existing database setting.
4. Click the **Sign-On Mode** tab at the top menu bar and select **SAML SSO**.


5. Enter the *Service Provider* details for the relying party identifier in ADFS. These are shown below and described in the following table:

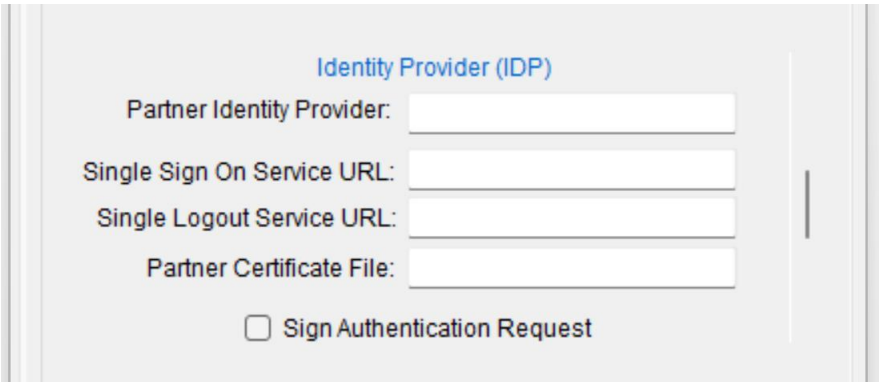


| Field | Description |
|---|---|
| Entity ID | Enter the Service Provider Entity ID. This can be defined by an FOIAXpress team lead using one of two approaches:<br>▪ We recommend using FX application domain name or domain name. Make sure to avoid certain characters in the entity ID. The URL should not include a port number, query string, fragment identifier, ampersand (&), or URN. The host part of the URL should not contain the substring "www".<br>▪ Use a unique name. The entity ID should be a globally unique name that identifies the service provider in the SSO process. You can use OrganizationApplicationNameEnvironmentType format. i.e., OPEXUSFOIAXpressProd, OPEXUSFOIAXpressTest, OPEXUSFOIAXpressProd, OPEXUSFOIAXpressTest |
| Assertion Service URL | Enter the URL below, replacing **<<DNS>>** with your organization's FOIAXpress URL:<br>https://**<<DNS>>**/FOIAXpress/AssertionConsumerService.aspx<br>For example, if your FOIAXpress application URL is:<br>https://myDns/FOIAXpress<br>Then the assertion URL value for this field would be:<br>https://myDns/FOIAXpress/AssertionConsumerService.aspx<br>**Note: The Assertion Service URL was updated for v11.7.0. If you are upgrading from a version below v11.7.0, you must update the value for Service Provider Assertion URL in SAML Configuration through a database configuration tool. You must also inform your Identity Provider about this change so they can record the updated assertion URL. See Section 2 for steps to update the URL** |
| Certificate File | Full file path for Service provider certificate (pfx) file |

| Field | Description |
|---|---|
| Certificate Password | Password of the Service provider certificate (if you enter path in the *Certificate File* field) |
| Certificate Serial Number | Serial Number of the service provider |

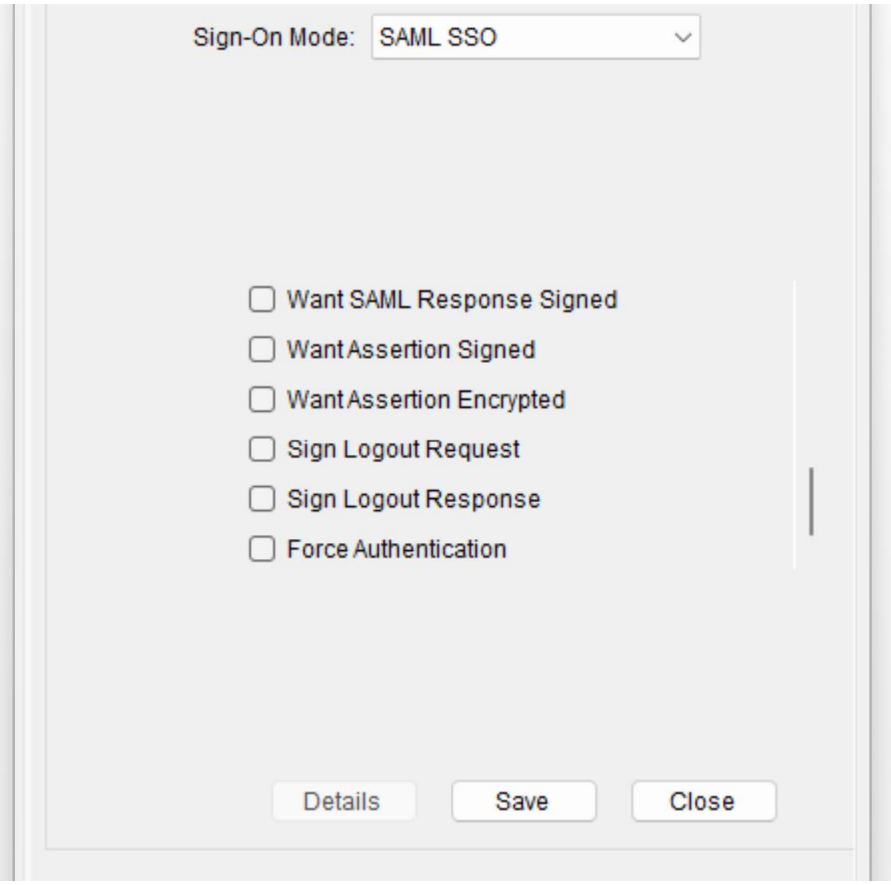
**Note: You need to provide either certificate file or certificate's serial number. Make sure the application has permission to read private key from the certificate file.**

6. Enter the **Identity Provider** values (SAML SSO Identity Provider) in the corresponding fields. These are shown below and described in the following table:




| Field | Description |
|---|---|
| Partner Identity Provider | Partner Identity Provider's name/entityId (Required) |
| Single Sign On Service URL | Single Sign On Service URL (Required) |
| Single Logout Service URL | This is an optional field. If you configure the URL, the application will redirect to this configured URL once user signs out or user's session times out. |
| Partner Certificate File | Full path for Identity Provider provided certificate (Required) |

7. Select the remaining checkboxes as needed depending on your configuration requirements.




8. Click **Save**.
9. Copy and paste the .CER file into the configured location Follow steps 3-5 in the *Update Assertion URL* section to configure the a partner certificate file.

# 4 Service Provider Metadata File

## 4.1 Generate Service Provider Metadata File

Follow the steps below to generate the FX Service Provider Metadata file:

1. First, have the pfx file ready (as used in the previous section).
2. Get the public key (.cer file) from pfx in base64 format (you can use OpenSSL, or do it from Certificate Management Console using the steps in the next section)
3. If you are preparing metadata for existing configuration then you will need to collect the following details from your current configuration:
    a. Assertion URL (if you upgrading from v11.5.4 or earlier, then the assertion URL has changed)
    b. Service Provider Name (first text field)
    c. Want Authentication Request Signed (checkbox)
    d. Want Assertion Signed (checkbox)
4. Go to the SAML Service Provider (SP) Metadata XML Builder and provide your information to generate an XML file.
5. Provide the generated XML file to your Identity Provider.

## 4.2 Retrieve .cer via Certificate Management Console

Follow these steps to retrieve a .cer file from pfx through the Certificate Management Console:

**Note: This requires that the pfx is installed in the system.**

1. Go to Certificate Management Console
2. Select the cert (pfx) then right click and select **All Tasks > Export**.
3. Select **Public key only (no private key)**.
4. Select **Base 64 format**.