pitney bowes

Shipping & Mailing
Outbound and Inbound Package Management

SendPro Enterprise

SAML 2.0 Authentication Configuration User Reference

Introduction

This guide serves as a reference for configuring SAML 2.0 authentication in SendPro Enterprise version 8.34.2 and above.

Service Collateral
SV63299 Rev. D
August 2020

About SAML

Frequently used in large enterprise cloud deployments, SAML (Security Assertion Markup Language) is an XML based data format for exchanging authentication and authorization data (assertions) between an identity provider (IdP) and a service provider (SP) (the SendPro Enterprise instance). Organizations can enable their preferred identity provider (for example, PingFederate or OneLogin) to provide a single sign-on (SSO) capability. Some, but not all, identity providers use certificates. Your chosen identity provider should have further content explaining SAML.

Note: SendPro Enterprise does not support specific identity providers. Ensure that your chosen identity provider supports the SAML 2.0 assertion format.

Overview of the Authentication Process

SendPro Enterprise supports SP-initiated SAML authentication. Below outlines the process:

1. A user selects a browser link, this action attempts to navigate the user to the service provider.
2. The service provider checks if the user is already authenticated.
3. If yes, the user is logged in at the service provider, and directed to the link they requested.
4. If no, a standard Authn request is sent to the Single Sign On (SSO) Uri that is configured within the SAML setup. The request is signed by the service provider's configured certificate. It can contain relayState information (the full Url originally requested by the user) and other information that the identity provider uses in its response.
5. The identity provider receives the Authn request, and then validates that the service provider is recognized. This is typically done by the URI. Also, the identity provider checks the contents of the request using the certificate it has configured for that service provider.
6. The identity provider determines if the user is logged in. If not, a login screen is presented.
7. Once logged in, the identity provider sends a SAML assertion to the service provider. This contains a NameID based on the username or email of the signed in user. If provided, it will also send the relayState information.
8. The service provider receives the assertion, and validates it based on the configured identity provider certificate. Also, it checks the NameID in the assertion is allowed access to the service provider.
9. If the user is granted access, a service provider authentication ticket is created, and the user is logged in. If relayState information is provided, the user is taken to the requested Uri. If not, they are directed to the default page of the service provider's choice (SendPro Enterprise Admin). If the user is unknown or disabled, the service provider displays an access denied error message.

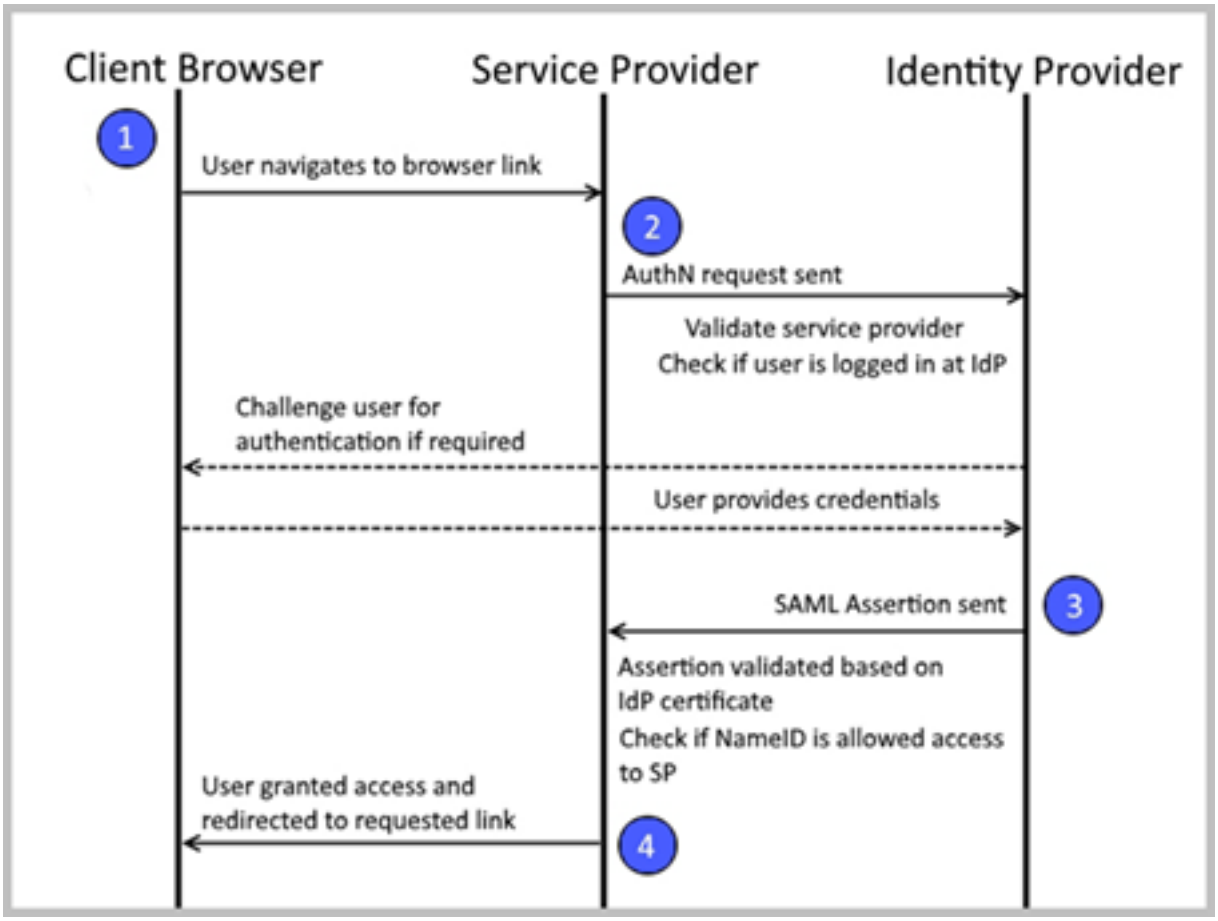


Figure 1: Graphical representation of the SPE SAML authentication process.

About Metadata

As part of SAML authentication, the service provider and identity provider exchange metadata. The metadata file also includes the public key, which ensures a secure transaction when validating the service provider's requests. An example of this metadata is shown below:

```
<md:EntityDescriptor entityID="urn:PierbridgeIdP" ID="_06dc0696-c1e8-4700-9a02-212e876e6160">
  <md:SPSSODescriptor ID="_0120c257-7fa6-463d-aa2a-36a8129b9f06" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
      AuthnRequestsSigned="false" WantAssertionsSigned="false">
    <md:KeyDescriptor>
      <KeyInfo>
        <X509Data>certificate</X509Data>
      </KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://login.tscloudidp.com/te/hostname.sendproenterprise.com/SAML/SingleLogoutService"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://login.tscloudidp.com/te/hostname.sendproenterprise.com/SAML/SingleLogoutService"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://login.tscloudidp.com/te/hostname.sendproenterprise.com/SAML/AssertionConsumerService" index="0" isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Figure 2: Metadata example.

SPE SAML 2.0 Configuration Options Detail

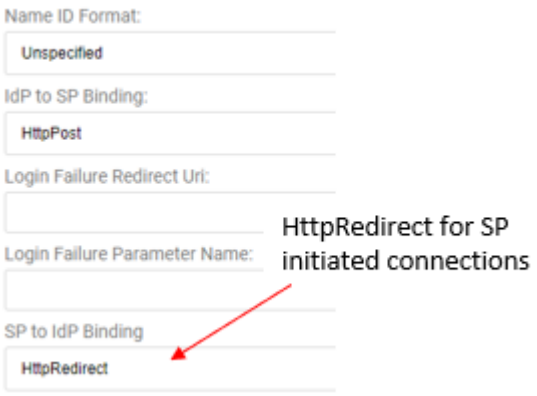
In the SAML tab of SendPro Enterprise Composer, the following options are available:

Option	Description
Import Metadata (Button)	Use to import the identity provider metadata. Note that the import can handle namespaces for the **KeyInfo** (certificate) elements.
Download Metadata (Button)	Use to download the configured metadata.
Import Certificate (Button)	Use to upload your identity provider certificates where required. Multiple IdP certificates can be imported, allowing for alternative certificates to be included within the system configuration. Each certificate is tried during the login sequence; an error is only returned if no certificate has resulted in a valid match. On successful upload, a confirmation popup appears. The entire contents of the chosen file is base64 encoded and stored in the [Authentication Settings] database table. If there is an error upon uploading the certificate data, no data will be uploaded and an error message is shown. **Note**: it is the responsibility of you and your integrator to configure any certificates. Only once configured can they be imported into SendPro Enterprise.
Delete Configuration (Button)	Use to clear the current SAML configuration. Note that the option only displays after the page has been edited, saved and reloaded.
Entity ID	A unique customer identifier. This value is mandatory, and must be globally unique over all customers; errors are returned if multiple customers are configured with the same Entity ID. When importing metadata, the value is taken from the entityID attribute within the **md:EntityDescriptor** element. Once set the value cannot be edited, and can only be amended by using the **Delete Configuration** option.
Single Sign On (SSO) Uri	The url for the identity provider page where users are sent to log in. The entered value must exactly match or a 404 error is displayed.
Single Log Out (SLO) Uri	The url for the identity provider page where users are sent to log out. The entered value must exactly match or a 404 error is displayed. If provided, users will only be redirected to the logout Uri if a valid logout response from the identity provider is received. If not provided, the default logout Uri will be used.
Name ID Format	Defines the Name ID Format in use. This determines which element is used to authenticate users, and is supplied by the external customer IdP. Note that it defaults to **Unspecified**, meaning both usernames and email addresses are accepted. Other supported values

	are **Transient** (usernames only) and **EmailAddress** (email addresses only).
IdP to SP Binding	How the identity provider communicates with the service provider. Defaults to **HttpPost**.
Login Failure Redirect Uri	The url where users are sent in the event of a failed login (E.g. if logging into the system fails for the SAML credentials supplied by the IdP). If not configured, users are not redirected.
Login Failure Parameter Name	The name of a query string parameter that is appended to the **Login Failure Redirect Uri**. It will contain a numeric identifier indicating the type of failure. For example, if the **Login Failure Redirect Uri** has a value of "http://mydomain.com/samlFailure.aspx", and **Login Failure Parameter Name** has a value of "errorNumber", login failures would return "http://mydomain.com/samlFailure.aspx?errorNumber=X". See the **Login Failure Parameters section** of this guide for potential codes and associated descriptions.
SP to IdP Binding	How the service provider communicates with the identity provider. Defaults to **HttpRedirect**.
Sign Authn Requests	Controls if the product IdP should use a signature during Authn requests for additional security.
Require Signed Responses	Specifies if SAML responses / assertions received from the partner IdP should be signed. If enabled and responses / assertions are not signed, or the signature cannot be verified, an error is flagged. Signing ensures the identity of the sender and integrity of the content. Signatures are generated by the partner identity provider with its private key, and verified by the local provider with the partner provider's public key. It is recommended this value is set to **True**.
Add Bindings To Metadata Locations	Adds the binding **urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST** to the Assertion Service Location and Logout Location.
Clock Skew	Specifies the time span to allow for differences between local and partner computer clocks when checking time intervals. It is recommended that this value is kept short, but not set so as to cause issues if server clocks are not correctly synchronized (E.g. 3 minutes).
Disable Assertion Replay Check	Controls if checks for SAML assertion replay attacks are performed. Each assertion includes a unique ID. A cache of assertion IDs are maintained; an error is flagged if an ID matches a previously received ID.
Disable Recipient Check	Controls if checks for intended recipients are performed. SAML assertions may contain a subject confirmation recipient URL used to identify the intended recipient of the assertion. If included, it should match the service provider's assertion consumer URL, as specified by the **AssertionConsumerServiceUrl** configuration property.

Use Embedded Certificate	Indicates if X.509 certificates embedded in XML signatures are used when verifying signatures. If the embedded certificate is used, no assumptions can be made about the identity of the sender. It is recommended that this setting is not enabled in production environments.
Disable Authn Context Check	Controls if checks for authentication context are performed. This identifies the mechanism by which the user was authenticated by the identity provider (E.g. via a password). If included in the SAML assertion, it should match the value specified by the optional **ExpectedAuthnContext** configuration property.
Disable Time Period Check	Controls if checks for validity are performed. SAML assertions may contain attributes indicating a time frame during which the assertion is valid. If included in the SAML assertion, the assertion is only valid if received within this time frame.
Disable Audience Restriction Check	Controls if checks for audience restrictions are performed. SAML assertions may contain an audience restriction URI, if included it should match the service provider's name.
Disable Pending Logout Check	Controls if checks for pending logouts are performed. The setting verifies, upon receiving a logout response, that a logout request was sent. If a logout request has not been sent, an error is flagged.
Disable In ResponseTo Check	Controls if checks for in-response-to elements are performed. SAML responses to particular SAML requests include an **in-response-toattribute**, which identifies the request using its unique ID. This setting verifies the attribute is present and correct.
Disable Destination Check	Controls if checks for target destinations are performed. SAML messages may include a destination URL specifying a target address. If included, it should match the provider's URL where the message was received. E.g. for a SAML response, the destination would be the local service provider's assertion consumer service URL as specified by the **AssertionConsumerServiceUrl** configuration property.

SPE SAML 2.0 Configuration Steps

Step	Comment	Action
1	Obtain IdP metadata and a certificate from the customer. Once customer metadata is successfully uploaded, the IdP Single Sign On Uri and the IdP Single Log out Uri should be auto-populated. A temporary uri can be entered if the customer cannot provide IdP metadata prior to the SP metadata and certificate being sent to them. Only "HttpPost" is supported for IdP to SP Binding. Binding is set as an attribute with the sign-on url in the customer metadata. Attempting to upload metadata with a binding attribute of "HTTP-Redirect" to SPE will result in an unsupported binding error. The customer must set their IdP to initiate connection using the HttpPost binding before issuing metadata for upload into SPE.	
2	The SP to IdP Binding is for SPE initiated connections and is optionally "HttpPost" or "HttpRedirect." In practice, this setting is always configured to "HttpRedirect."	
3	SAML configuration can now be saved.	Click Save on the lower right of the Security page.
4	The metadata supplied to the customer should provide the correct url's for the SAML transaction. **Note**: Some information that goes into case sensitive fields in the IdP configuration may	Provide customer with endpoint trusted url, e.g.: *https://<tenantname>.sendproenterprise.com/Composer/Runtime/Index/View%20App*

	need to be changed to upper or lower case. The IdP will need to have the endpoint trusted url entered which will be what the app users will access. It should be a page all users will have permission to.	
5	In order for a connection to be successful, the person logged in needs a user permission set up in SPE. For user name the user email address is generally used. Password is required by SPE but is not used for anything other than forms authentication, and so can be set to an arbitrary value. The NameIDFormat values in the SP metadata also allow other fields to be used for authentication.	Configure or import users mapping the user's email to SPE username.

Login Failure Parameters

This table lists the login failure parameter error codes, with associated descriptions, that are appended to redirect Uris.

Code	Description
1 = No Response	• Unexpected error reading the response. • No SAML logout response received, aborting.
2 = No Status Message	• Something is wrong with the token and it doesn't contain a status message.
3 = No Assertion	• The SAML response contained no assertions.
4 = No Name Identifier	• The SAML response didn't contain a name identifier.
5 = Authentication Failed	• Authentication for [User] failed ([Status]).
6 = Different Message Certificate	• The included IdP certificate is not being used to sign the SAML message. • The configured IdP certificate is not being used to sign the SAML message.
7 = Different Assertion Certificate	• The included IdP certificate is not being used to sign the SAML assertion. • The configured IdP certificate is not being used to sign the SAML assertion.
8 = Empty Certificate	• The certificate is empty.
9 = Unknown Binding	• Binding [Binding] is unknown.
10 = Incorrect Metadata	• The metadata doesn't contain any 'KeyInfo' elements. • The metadata doesn't contain an IdP certificate. • The metadata doesn't contain any compatible single sign on service binding types. • Invalid metadata xml, expecting at least one IDPSSO descriptor. • Invalid metadata xml, expecting entity descriptor.
11 = Other/Unknown	• An error that was returned by the IdP.