Webcast Attendee guide to SAML SSO

SAML Background

Security Assertion Markup Language 2.0 (SAML) is a standard for securely exchanging authentication and authorization data between two parties. The standard is an XML-based protocol that uses security tokens to pass information about an end user between a SAML Identity Provider and a SAML Service Provider.

The GlobalMeet Webcast platform is capable of integrating with any third-party system that supports SAML.

Definitions

“Identity Provider” means the organization responsible for authorizing and authenticating individuals prior to exchanging data with a Service Provider.

“Service Provider” means the organization responsible for validating incoming security tokens, before granting access to a secure Web site.

“**X.509 certificate**” means a digital certificate that uses the international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or organization contained within the certificate.

With respect to this documentation, client systems are considered to be Identity Providers and the GlobalMeet Webcast platform is the Service Provider.

Integration Steps

1. GlobalMeet Webcast tests SAML integrations on two unique development platforms before enabling on a production environment. The Identity Provider’s internal DevOps team must confirm the number of environments they support internally in order to coordinate development efforts.

2. The Identify Provider must supply X.509 certificates for each environment to be supported. GlobalMeet Webcast will install these certificates on corresponding systems.
3. The Identify Provider must supply a SAML XML response file containing the user registration fields to be tracked by the webcast platform. Within the XML these fields are called “attributes”. They contain information about the user, including first name, last name, email or custom information. GlobalMeet Webcast will provide a sample SAML XML response file if needed.
4. GlobalMeet Webcast will configure a webcast template to map all standard and custom attributes to webcast registration fields. Please note that **email is a required field** and is used to uniquely identify the user within the webcast.
5. GlobalMeet Webcast will provide a Response Destination URL. All submissions from the Identity Provider system should be posted to this URL. GlobalMeet Webcast will validate incoming SAML XML responses using the X.509 certificate provided.
6. If possible, the Identity Provider should supply a way for GlobalMeet Webcast to test the integration using an account authorized by the client SAML system.

Post Data to GlobalMeet Webcast

Below is an example of a simple form post that the Identity Provider can use to submit user data to the Service Provider. Please note that **every webcast has a RelayState ID that must be passed within the form post** to properly route requests to the correct presentation.

The items listed in bold are variables:

<html>

<body>

<form method="post" action="
GLOBALMEET_WEBCAST_RESPONSE_DESTINATION_URL">

<input name="RelayState" value="**EVENT_ID-TP_KEY**" />

<input name="SAMLResponse" value="**BASE64_ENCODED_SAML_RESPONSE_XML**" />

<input type="Submit" name="submit" value="submit" />

</form>

</body>

</html>

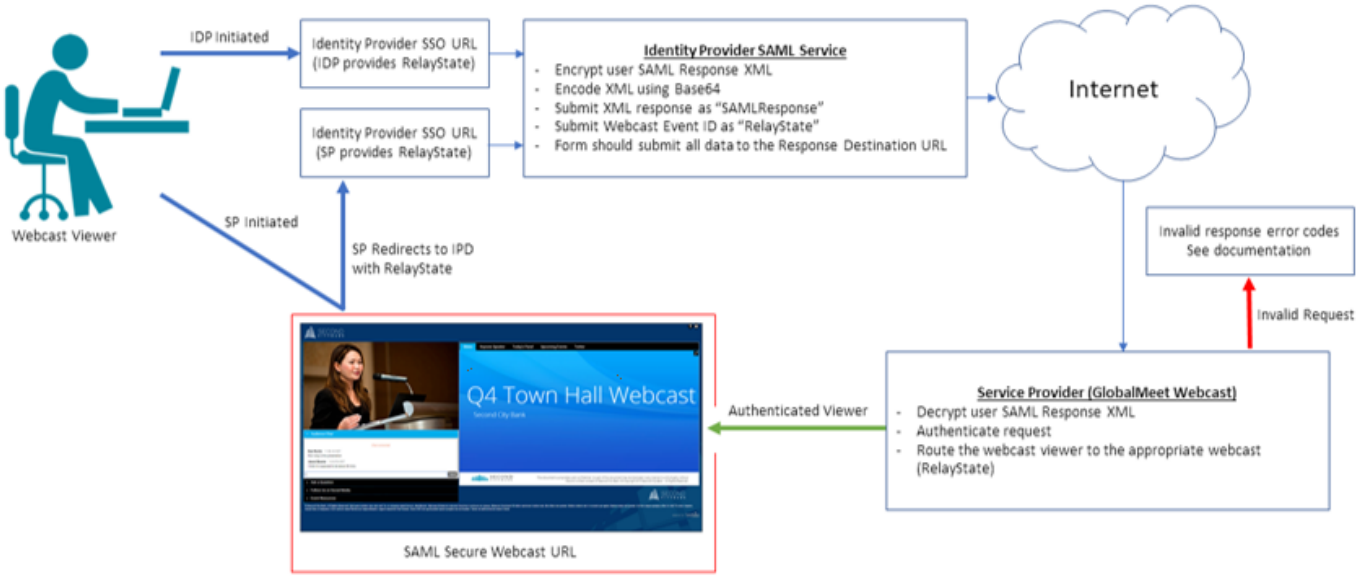
RelayState

GlobalMeet Webcast uses RelayState to identify the unique webcast event that user is joining when the Identity Provider is sending user data to GlobalMeet Webcast. The RelayState is the same as the GlobalMeet webcast Event ID and TP_Key. You may have 100s or 1000s of webcast and identifying which webcast the view wants to view is an important step. An example relaystate would look like this “1234567-ab177c1f4e”

SP Initiated or IDP Initiated

You may choose to create a SAML SSO integration where the user initiates their entry from your (Identity Provider) site or the GlobalMeet Webcast URL (SP Initiated.) Please note that in both cases the XML post will need to include RelayState however with SP Initiated GlobalMeet will send the RelayState to the IDP.

SAML SSO Workflow



Enabling SAML SSO for Webcast Attendees

Enabling SSO for Webcast Attendees will require that all webcast attendees validate through your corporate SSO or Identity Provider system. Enabling this feature will restrict any users from joining the event without authenticating properly.

We support both IdP (Identity Provider) Initiated SSO and SP (Service Provider) Initiated SSO. When using IdP initiated users will first click on a link provided by the IdP system or some non-webcast related workflow. When using SP Initiated SSO users will first click on the webcast link to start the SSO workflow.

To Enable IdP-Initiated SSO

1. Navigate to the security settings page of your webcast.
2. Under Message for Unauthorized Users, select “Redirect to My Custom Error Page”.
3. Insert a message to be shown to anyone accessing the webcast directly or who fails IdP login.
4. Check Require Custom Token
5. Check Enforce URL Security Key

6. Provide webcast attendees with the IdP link for login, or other workflow for authentication outside the webcast system.

Troubleshooting and Error Codes

Any user request that cannot be validated will be redirected to an invalid request page.

Typical error codes:

- 0a – General error.
- 1a – No “EVENT_ID” passed in “RelayState” field.
- 1b – No “BASE64_ENCODED_SAML_RESPONSE_XML" passed in “SAMLResponse” field.
- 1c – SAML misconfiguration (E.g. Invalid 509 certificate or other configuration issue).
- 2a – Invalid SAML signature.
- 2b – No email address passed as a user attribute.
- 3a – “EVENT_ID” is not a number.
- 3b – “EVENT_ID” does not exist.
- 3c – “EVENT_ID” is not available to the requester.

Revision #6

Created 6 January 2023 18:42:24 by Matt Engel

Updated 12 January 2023 21:13:26 by Matt Engel