Womply

Partner Technical Integration Guide

SAML Single Sign-On (SSO) Service

Version 4.0
May 30th 2014

CONFIDENTIAL

This document is the sole and confidential property of Oto Analytics, Inc., and is being shared with the partner for the purposes of collaboration, or for evaluating a possible collaboration, to enable products and services, as provided by Oto Analytics, Inc..

The partner agrees to treat any and all information contained or referenced in this document as confidential, to use it solely for the purpose of the evaluation and definition of a collaboration, to make it accessible only to such employees who have a need to know, not to disclose it to any third party, and not to make it publicly available or accessible in any way, except with the prior written consent of Oto Analytics, Inc.

All information contained or referenced in this document shall remain the exclusive property of Oto Analytics, Inc. as well as all patent, copyright, trade secret, trademark and other intellectual property rights therein. No license or conveyance of any such rights to the partner is granted or implied.

Table of Contents

Revision History

Date	Version	Revision Description
July 2013	01	Document creation.
December 2013	02	Partner SSO Integration approach added.
February 2014	03	Additional Partner SSO Integration attributes added.
May 2014	04	Added additional SAML initialization requirements Added sample elements

Overview of the SAML Single Sign-On (SSO) Service

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.

Womply offers a SAML-based Single Sign-On (SSO) service that provides partner companies with full control over the authorization and authentication of hosted user accounts that can access their branded Insights website. Using the SAML model, Womply acts as the service provider. Womply partners act as identity providers and control usernames, passwords and other information used to identify, authenticate and authorize users for their own web applications. There are a number of existing open source and commercial identity provider solutions that can help you implement SSO with Womply.

The Womply SSO service is based on the SAML v2.0 specifications. SAML v2.0 is supported by several widely known vendors.

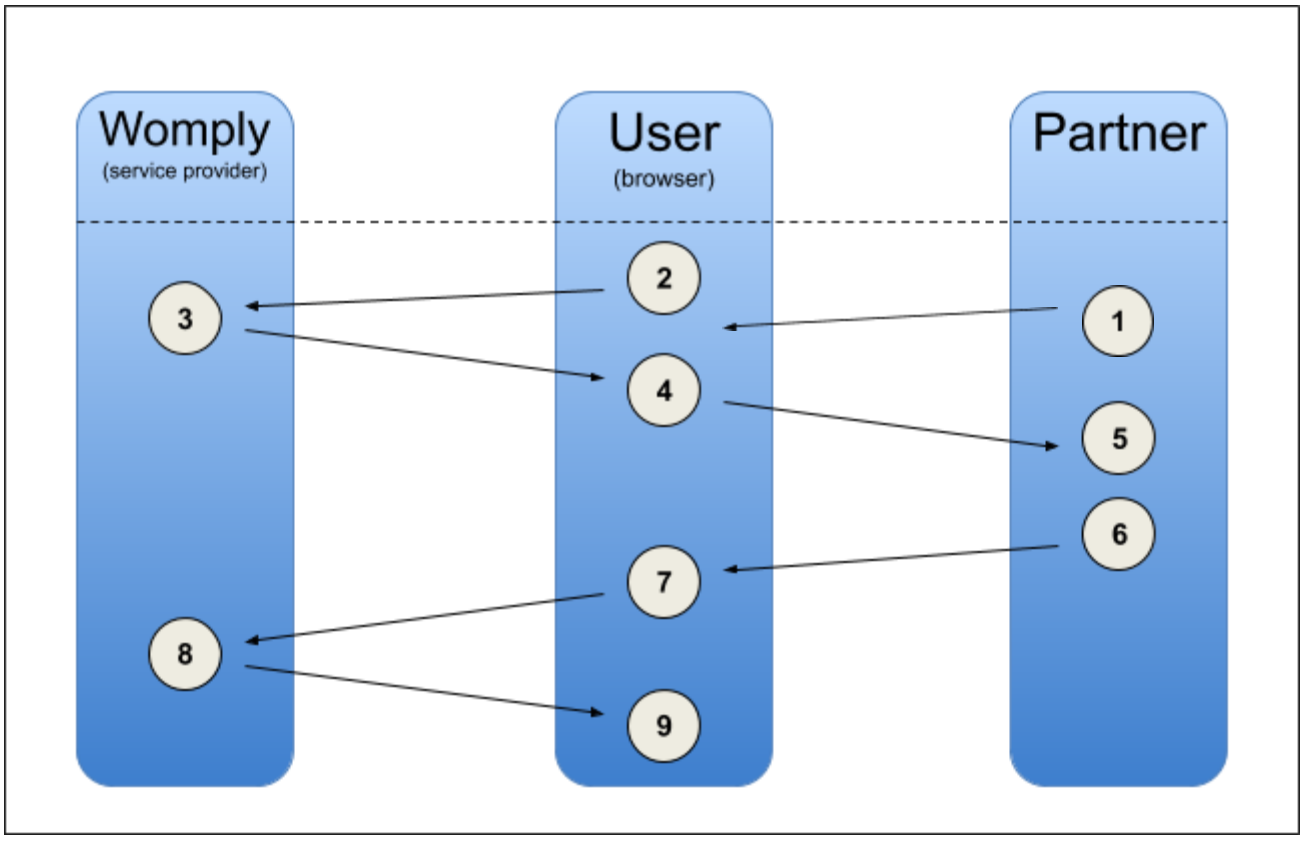
Understanding SAML-based SSO for Womply

The following process explains how a user logs into Insights through a partner-operated, SAML-based SSO service.

Figure 1, shown below, illustrates the process by which a user logs in to Insights through a SAML-based SSO service. The numbered list that follows the image explains each step in more detail.

Note: Before this process takes place, the partner must provide Womply with the URL for its SSO service as well as the X.509 certificate fingerprint that Womply should use to verify SAML responses.

Figure 1: Logging in using SAML



This image illustrates the following steps:

1) The user logs in to the partner's portal.
2) The user attempts to reach a Womply-hosted application such as the Insights portal. The request URL indicates that the partner should be used for authentication.
3) Womply generates a SAML authentication request. The SAML request is encoded and embedded into the URL for the partner's SSO service. The RelayState parameter containing the encoded URL of the Womply application is also embedded in the SSO URL. This RelayState parameter is meant to be an opaque identifier that is passed back without any modification or inspection.
4) Womply sends a redirect to the user's browser. The redirect URL includes the encoded SAML authentication request that should be submitted to the partner's SSO service.
5) The partner decodes the SAML request and extracts the URL for both Womply's ACS (Assertion Consumer Service) and the user's destination URL (RelayState parameter). The partner then authenticates the user. The partner could re-authenticate the user (if necessary) by either asking for valid login credentials or by checking for valid session cookies.
6) The partner generates a SAML response that contains the authenticated user's guid, as well as additional fields, documented below. In accordance with the SAML 2.0 specification, this response is digitally signed with the partner's X.509 certificate fingerprint.
7) The partner encodes the SAML response and the RelayState parameter and returns that information to the user's browser which issues a POST request to Womply's ACS.
8) Womply's ACS validates the SAML response using the partner's certificate fingerprint. If the response is successfully validated, ACS redirects the user to the destination URL.
9) The user arrives at the Womply application. On the first visit, the user will be required to set up their account and accept the Terms Of Service. On the second and later visits, the user will be automatically logged in.

Partner SSO Integration with Womply

To set up SSO integration with Womply, the partner must provide Womply with:

1. **X.509 Certificate Fingerprint.** This will be used to validate the signed SAML responses between the partner and Womply.
2. **URL of their SSO service.** This is the URL to which a user will be sent to authenticate with the partner as part of the SSO process, also known as the SSO Target URL.
3. **SP metadata from Womply on the IP**. it is useful to view the partner's SP metadata for Womply on their IP to make sure things are set up correctly.
4. **Test Merchant IDs**. A list of valid MIDs the test user will be signing up with.

SAML Initialization

When a user is sent from the partner site to Womply, the destination should be Womply's SAML initialization point:

https://partnersite.com/saml/initialize

Where "partnersite" is the partner's domain associated with Womply's Insights product.

Womply will then generate a SAML authentication request to the partner's SSO Target URL.

1) The Assertion Consumer Service (ACS) URL for Womply will be sent to the partner's Identity Provider in the request:

https://partnersite.com/saml/callback

2) The saml:Issuer in the Authentication Request is defined as:

https://partnersite.com

3) The interoperable SAML 2 profile specifies that attributes should be delivered using the urn:oasis:names:tc:SAML:2.0:attrname-format:uri NameFormat and so the SAML SP expects such a format.

4) It is preferable that the NameID field has attribute 'guid' (see User Metadata) and format:

urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

This is in reference to Section 8.3 of SAML V2.0.

For example, here is a sample SAML Authentication Request:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://partnersite.com/saml/callback"
Destination="http://ip.example.com/simplesaml/saml2/idp/SSOService.php"
ID="_9c418cf0-c2ab-0131-6b1f-7831c1d46762" Issue Instant="2014-05-21T00:20:17Z"
Version="2.0">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                https://partnersite.com
        </saml:Issuer>
        <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified"/>
</samlp:AuthnRequest>
```

This <samlp:AuthnRequest> message is deflated, base64-encoded, URL-encoded and set to the SAMLRequest parameter in the URL query string of the HTTP GET request. The RelayState parameter is also present in the GET request.

SAML Callback

After the partner decodes the Authentication Request, validates the request, and authorizes the user, the Authentication Response element <samlp:Response> is base64-encoded and set to the SAMLResponse input parameter of the HTTP POST Binding. The RelayState parameter is also set as received in the Authentication Request.

User Metadata

When Womply directs a user to the partner's SSO service URL, the partner's system must authenticate the user and submit back to Womply's ACS URL with a set of fields describing the user (the metadata) via an Attribute Assertion <saml:AttributeStatement>.

The fields are as follows:

Field Name	Type	Required	Description
username	String	Y	
guid	String	Y	Unique identifier for the user
mids	String Array	Y	Set of MIDs the user is authorized to view
first_name	String	N	
last_name	String	N	
email	String	N	
position	String	N	User's position at the business
phone_mobile	String	N	Mobile phone number
phone_alternate	String	N	

Womply uses the GUID to uniquely identify the user, and is thus able to determine if the user has been seen before. The first time a user is authorized via SSO from a partner, the GUID will be new, and the user will be taken through a one-time setup flow. After that point, Womply will recognize the GUID, and sign the user in. A GUID will typically be an integer, but can be a String.

The first time a user enters and is setup, Womply will use the information sent by the partner (such as name, email, phone) to auto-fill the setup forms.

Note the mids are represented by multiple AttributeValue fields. Here is a sample representation expected within an SAML Authentication Response if the mids were 1111111111 and 2222222222.

```
<saml:Attribute Name="mids" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xsi:type="xs:string">11111111111</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">22222222222</saml:AttributeValue>
</saml:Attribute>
```

Additional Integration Details

Session duration: The partner site can enable whatever user session duration is desired, which can be long-term. This will allow the user to navigate back to the partner site while remaining signed in to that site, for convenience. If the session is shorter, and expires, the user will need to sign in again when returning to the partner site. This is independent of any Womply site access.

Clock drift: Server clocks drift naturally to some extent, unless synchronized. Because NTP synchronization between Womply and all partners is not practical, some clock drift must be expected. If the partner's server, acting as Identity Provider, drifts ahead of Womply's server, response validation may return the error "Current time is earlier than NotBefore". If this is observed during testing, it may be necessary to attempt to specify an allowed clock drift. This can increase some security risks, though only to a minor extent if the drift is kept to a minimum.