GIFTS Online

Single Sign-On – 2017

GIFTS Online clients interested in streamlining their users experience can utilize MicroEdge's single sign-on (SSO) capabilities to federate user identities. Single sign-on allows MicroEdge to configure a client's GIFTS Online application to redirect their users to a branded, secure client login page. Upon authenticating themselves via the login page by entering their company-issued credentials users are then seamlessly logged into GIFTS Online. To achieve this cohesion, GIFTS Online supports a service provider-initiated version of the SAML V2.0 protocol.

Support

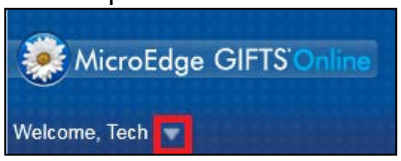
If you have questions or need assistance in any way, please contact MicroEdge Technical Support.

Support Hours: M-F, 8:00 am – 8:00 pm ET **Phone:** 877.704.3343

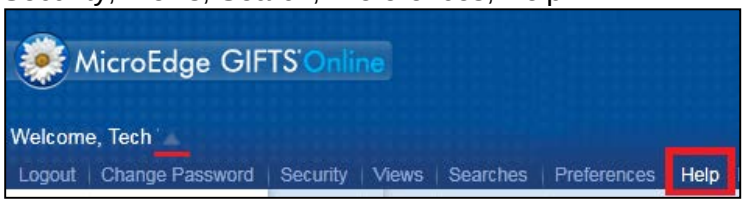
Email: helpdesk@microedge.com **Online:** www.microedge.com

For information on troubleshooting common issues, see the **Technical Support** section in the online help.

1. In the top menu bar of **GIFTS Online**® under your name, is the *User Menu*.



2. Select the triangle next to your name to view the User Menu options: Logout, Change Password, Security, Views, Search, Preferences, Help



3. Select **Help** and the online web help opens in a new window.

How-to Documentation

Have questions or need to quickly get up to speed? Check out these help files, guides, videos, walkthroughs, and other assistance for step-by-step instructions and detailed information**:**
https://www.blackbaud.com/howto/giftsonline

The MicroEdge Community Resources Site

To keep up with all the latest news on MicroEdge products, access our knowledgebase, or join in relevant discussions on our forums, go to - https://community.blackbaud.com/products/microedge.

What Is SAML V2.0?

Security Assertion Markup Language 2.0 (SAML 2.0) is an XML-based framework for communicating user authentication, entitlement, and attribute information between security domains.

SAML V2.0 was developed by the Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS) and was ratified as an OASIS Standard in March 2005, replacing SAML 1.1.

What Are the Components of SAML?

SAML is defined in terms of assertions, protocols, bindings, and profiles. This section is excerpted from the OASIS SAML Executive Overview document.

Assertions

An assertion is a package of information that supplies one or more statements made by a SAML authority. SAML defines three different kinds of assertion statement that can be created by a SAML authority.

- Authentication: The specified subject was authenticated by a particular means at a particular time. This kind of statement is typically generated by a SAML authority called an identity provider, which is in charge of authenticating users and keeping track of other information about them.
- Attribute: The specified subject is associated with the supplied attributes.
- Authorization Decision: A request to allow the specified subject to access the specified resource has been granted or denied.

The outer structure of an assertion is generic, providing information that is common to all of the statements within it. Within an assertion, a series of inner elements describe the authentication, attribute, authorization decision, or user-defined statements containing the specifics. The diagram below illustrates the high-level structure of a typical SAML authentication assertion.

Sample SAML V2.0 Implementation in GIFTS Online

Here is a sequence diagram, courtesy of ComponentSpace's SAML Developer Guide, that demonstrates the possible Service Provider (SP) initiated interaction between GIFTS Online (SP) and a client's Identity Provider (IdP).

1. The user browses to the SP site: https://exampleclient.gogiftsonline.com
2. The user attempts to access a protected page requiring the user to be authenticated.
3. The SP sends an authentication request to the IdP's SSO service endpoint.
4. If the user is not already authenticated at the IdP, the user must present their credentials and login.
5. The IdP sends a SAML response containing a SAML assertion to the SP.
6. The SP uses the information contained in the SAML assertion, including the user's name and any associated attributes, and performs an automatic login.

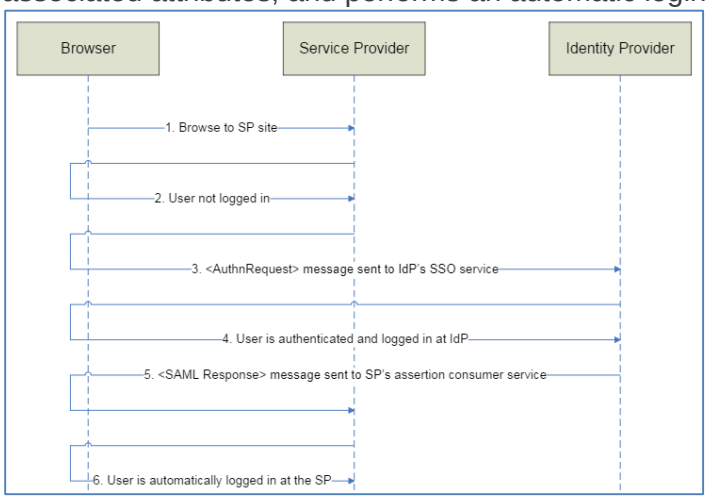


Image courtesy of ComponentSpace SAML Developer Guide

SAML V2.0 Resources

Below are several additional SAML-related resources you may find useful.

- Security Assertion Markup Language (SAML) V2.0 Technical Overview: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf
- Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf
- SAML V2.0 Specifications: http://saml.xml.org/saml-specifications
- SAML V2.0 Executive Overview: https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf
- ComponentSpace SAML Developer Guide: http://www.componentspace.com/Documentation/SAML%20v2.0%20Developer%20Guide.pdf

Specifications

Please follow these specifications before attempting to stage the SSO handshake:

- GIFTS Online supports **only** the SP Initiated Authentication Request Protocol. GIFTS Online does not support IP initiated requests.
- GIFTS Online supports the SP Redirect Request/IdP POST Response variant of the Web Browser SSO Profile.
- GIFTS Online can accept responses from the IdP where just the response is digitally signed, just the assertion is digitally signed, or both the response and assertion are digitally signed. GIFTS Online supports both SHA256 (as of version 6.1) and SHA1.
- GIFTS Online does not digitally sign or encrypt the AuthnRequest.
- The assertion generated by the IdP must contain an attribute having the name “go_loginid”. The value of the attribute must be a valid GIFTS Online login ID that maps to the assertion’s authenticated identity. For the prototype, you can use a value of “CR”. The value must be all caps.
    - Sample response:

```
<ns2:AttributeStatement>
<ns2:Attribute Name="go_loginid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<ns2:AttributeValue>CR</ns2:AttributeValue>
</ns2:Attribute>
</ns2:AttributeStatement>
```

- The ID of the AuthnRequest must be referenced by the InResponseTo attribute of the assertion’s SubjectConfirmationData node.

```
<ns2:Subject>
<ns2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">acmeuser1</ns2:NameID>
<ns2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<ns2:SubjectConfirmationData InResponseTo="id80b111452d5b4256919c447c3288c865"
NotOnOrAfter="2015-11-20T20:58:48Z"
Recipient="https://ssostaging.gogiftsonline.com/sl/saml2acs.aspx"/>
</ns2:SubjectConfirmation>
</ns2:Subject>
```