Ford’s Notes: Security Association Markup Language (SAML)

What is the Security Assertion Markup Language (SAML)?

The primary role for SAML it enables users to access multiple web applications using one set of login credentials. It works by passing authentication information in a particular format between two parties, usually an identity provider (idP) and a web application or service provider.

SAML is an open standard used for authentication. Based upon the Extensible Markup Language (XML) format, web applications use SAML to transfer authentication data between an identity provider (IdP) and the service provider (SP).

What is the Extended Markup Language (XML)?

XML stands for eXtensible Markup Language, a language that's used to describe data. Data stored in XML is known as being "self-defining." XML is a format to store data along with its structure. This feature makes it useful for many things, including transferring data, formatting documents, creating layouts, and more.

XML is one of the most widely used formats for sharing structured information between programs, computers, and people, both locally and across networks. Unlike HTML, XML can link an unlimited combination of data types by tagging them with a standard, machine-readable language to define each piece of data and determine what it does.

Security Assertion Markup Language (SAML) is a login standard that helps users access applications based on sessions in another context. It’s a single sign-on (SSO) login method offering more secure authentication (with a better user experience) than usernames and passwords.

The powerful capabilities of these XML data sets coupled with dynamic links present new threat vectors because the code defined by XML tags can carry virtually any payload through the firewall unchecked. Dynamic Links are smart URLs that allow you to send existing and potential users to any location within

How Does SAML Work?

SAML works by exchanging user information, such as logins, authentication state, identifiers, and other relevant attributes between the identity and service provider. As a result, it simplifies and secures the authentication process as the user only needs to log in once with a single set of authentication credentials.

https://cloud.google.com/architecture/identity/single-sign-on#:~:text=SAML%20is%20an%20open%20standard,SAML%202.0%20HTTP%20Redirect%20binding.

Ford's Notes: Security Association Markup Language (SAML)

Cloud Identity and Google Workspace support SAML version 2.0 for single sign-on (SSO). When a user uses SSO for Cloud Identity or Google Workspace, their external IdP is the SAML IdP and Google is the SAML service provider.

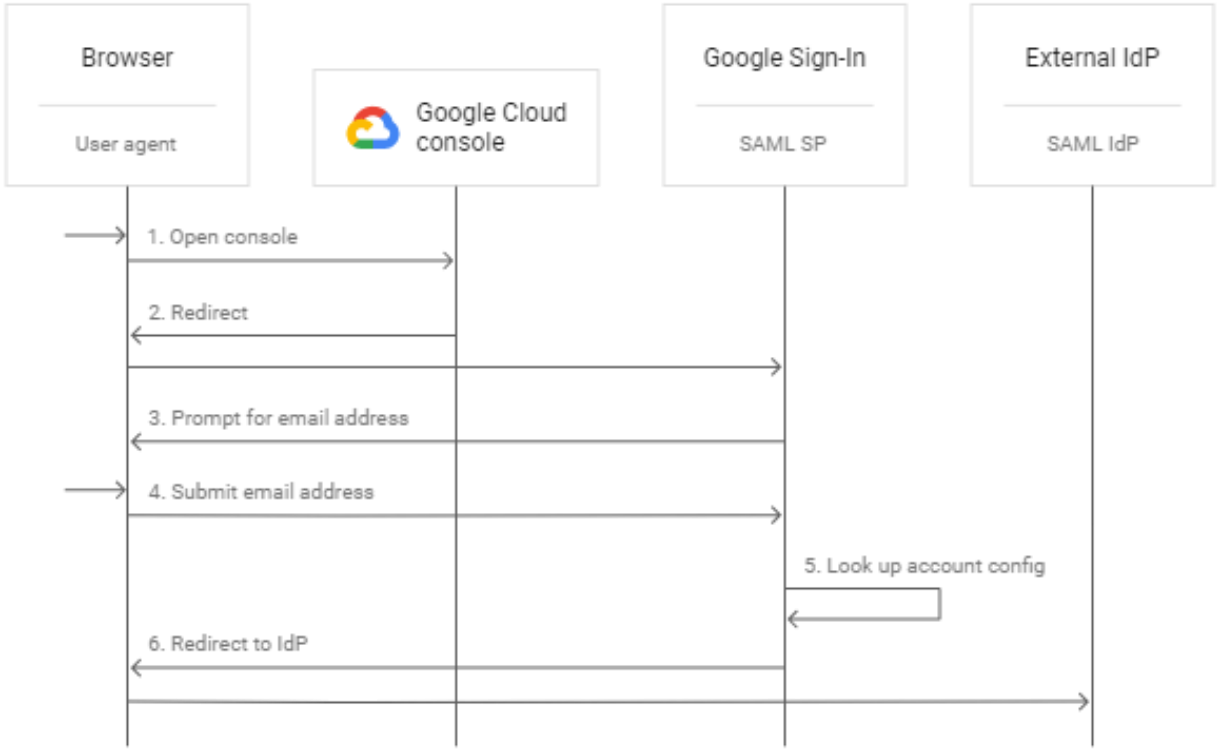

Figure 1- Accessing Google Cloud via SAML

1. User points browser to the console (or any other Google resource that requires authentication).
2. Because the user is not yet authenticated, the console redirects their browser to Google Sign-In.
3. Google Sign-In returns a sign-in page, prompting the user to enter their email address.
4. The user enters their email address and submits the form.
5. Google Sign-in looks up the user's Cloud Identity or Google Workspace account that is associated with their email address.
6. Because the associated Cloud Identity or Google Workspace account has single sign-on enabled, Google Sign-In redirects the browser to the URL of the

configured external IdP. Before issuing the redirect, it adds two parameters to the URL, RelayState and SAMLRequest.

- RelayState contains an identifier that the external IdP is expected to pass back later. That's usually the URL that the user's browser will be directed to after a successful authentication through SAML.
- SAML Request contains the *SAML authentication request* (the login request), in an XML document that has been DEFLATED. DEFLATE is a lossless data compression file format designed by Phil Katz, for version 2 of his PKZIP archiving tool (RFC 1951).

At the end of a successful SAML exchange a SAML Response is generated by the Identity Provider. It contains the actual assertion of the authenticated user (the login). In addition, a SAML Response may contain additional information, such as user profile information and group/role information, depending on what the Service Provider can support.

References

Single sign-on (Google) - https://cloud.google.com/architecture/identity/single-sign-on

SAML-based SSO: technical overview (Google) -

https://support.google.com/a/answer/6262987?hl=en#:~:text=Security%20Assertion%20Markup%20Language%20(SAML,trying%20to%20access%20secure%20content.

Configure Google Workspace as SAML Service Provider - https://auth0.com/docs/authenticate/protocols/saml/saml-sso-integrations/configure-auth0-saml-identity-provider/configure-auth0-as-idp-for-google-g-suite

Security Assertion Markup Language (SAML) V2.0 Technical Overview -

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

SAML Specifications - http://saml.xml.org/saml-specifications