Learn More About SAML

Abstract

This document provides information about the Security Assertion Markup Language (SAML).

October 2022

Revisions

Date	Description
October 2022	Initial release

Acknowledgments

Author: D M Vinod Kumar

Support: NA

Other: NA

Table of contents

Executive summary

Note: This section is required for Reference Architectures, Best Practices guides, and Technical White Papers. It is optional for Deployment and Configuration guides.

The executive summary includes a problem statement and the Dell Technologies solution that is detailed in the remainder of the paper. It should include key findings and information that gives the reader insight as to why they would be interested in this solution.

1 What is SAML?

Security Assertion Markup Language (SAML) is an open standard used for authentication. The primary role of SAML in security is that it enables access to multiple web applications using one set of login credentials. It works by passing authentication information in a particular format between two parties, usually a web application and an identity provider (IdP).

1.1 How SAML works?

Web applications use SAML based upon the Extensible Markup Language (XML) format to transfer authentication data between the service provider (SP) and the identity provider (IdP). SAML simplifies the authentication process where users need to access multiple, independent web cookies that are only viable within the same domain. It achieves this objective by centralizing user authentication with an identity provider. Web applications can then leverage SAML via the identity provider to grant access to their users. This SAML authentication approach means users do not need to remember multiple usernames and passwords. It also benefits service providers as it increases security of their own platform, primarily by avoiding the need to store (often weak and insecure) passwords and not having to address forgotten password issues.

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. So, when the user tries to access a site, the identity provider passes the SAML authentication to the service provider, who then grants the user entry. The following illustration explains this concept with a real-world analogy:

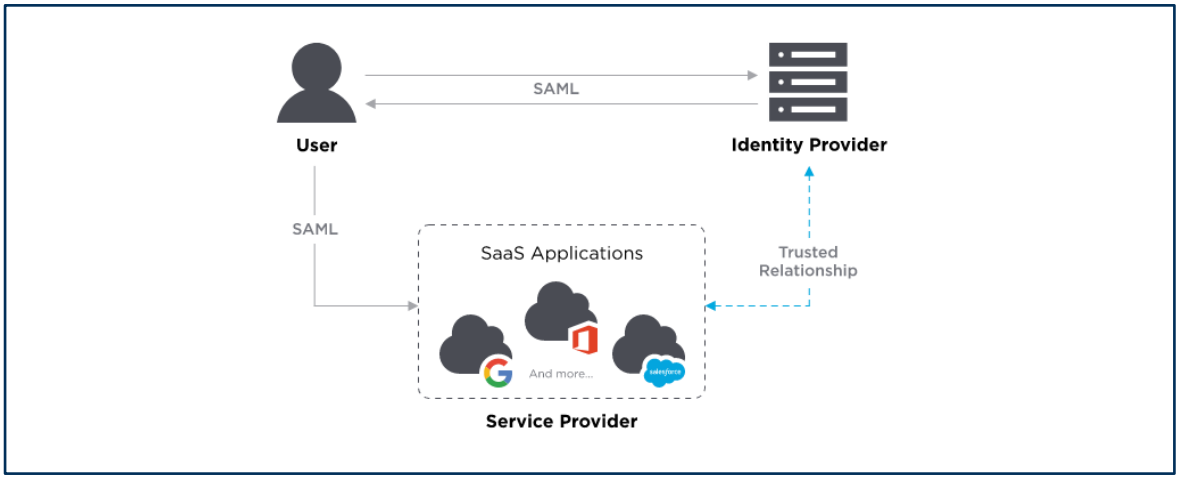

Figure 1 SAML Process

Organizations often need to confirm your identity before granting you access. A good case is the airline industry. Before you board an aircraft, the airline needs to confirm your identity to ensure the security of other passengers. They verify your identity with some form of government-issued picture identification. Once they confirm that your name on your identity matches the name on your airline ticket, they then allow you to board the aircraft.

In the example above, the government is the identity provider, and the airline is the service provider. Your government-issued identification is the SAML assertion. When you apply for a government ID, you usually

need to complete a form, have your picture taken, and in some circumstances, your fingerprints as well. The government (service provider) then stores these identifying attributes in their database and issues you with a physical ID associated with your identity. In the airline example, when you arrive at the gate, the airline (service provider) checks your ID (SAML) assertion. The airline accepts your ID as it contains your details, and the identity card or passport passes scrutiny as a valid document. After successful authentication, the airline then allows you to board the aircraft.

1.2 What is SAML SSO?

SAML Single Sign-On is a mechanism that leverages SAML allowing users to log on to multiple web applications after logging into the identity provider. As the user only has to log in once, SAML SSO provides a faster, seamless user experience.

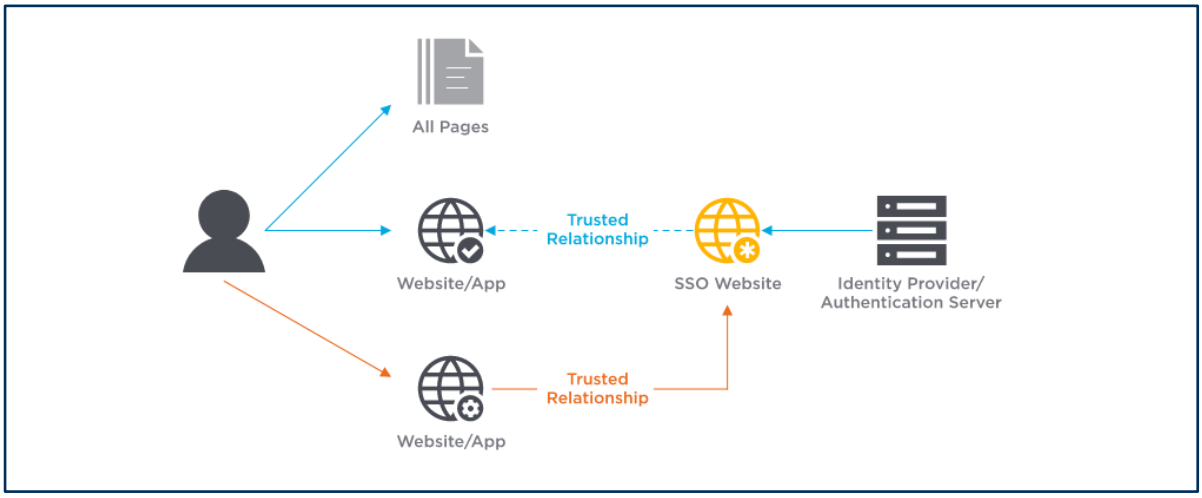

Figure 2 SAML SSO

SAML SSO is easy to use and more secure from a user perspective as they only need to remember one set of user credentials. It also provides fast and seamless access to a site as every application they access does not prompt them to enter a username and password. Instead, the user logs into the identity provider and then accesses the relevant web application by clicking on its icon or navigating to the site via its URL.

SAML SSO also offers other benefits in addition to an enhanced user experience. It improves productivity for both the user and the Help Desk. Users do not need to waste time logging into multiple web applications with a unique set of credentials for each one. Consequently, they do not inundate the Help Desk with password reset requests, freeing the service team to attend to other service-related issues.

In addition to increased user satisfaction and improved productivity, SAML SSO also helps reduce costs. For example, Help Desks need to manage fewer calls. Instead of building a local authentication implementation for their solution, they can subscribe to an identity provider, reducing the labor cost of building and maintaining it internally.

1.3 Advantage of SAML

SAML is a widely adopted enterprise solution as it has many advantages. SAML improves the user experience as you only need to sign in once to access multiple web applications. Not only does this speed

up the authentication process, but it also means you only need to remember one set of credentials. The organization also benefits from this feature as it means fewer Help Desk calls for password resets.

In In addition to improving the user experience, SAML also offers increased security. Since the identity provider stores all login information, the service provider does not need to store any user credentials on their system. Furthermore, as the identity provider specializes in providing secure SAML authentication, they have the economies of scale to invest time and resources in implementing multiple layers of security. For example, IdP's have comprehensive identity security solutions that include built-in features such as multi-factor authentication (MFA) that protect against common password attacks.

1.4 SAML Example

SAML uses a claims-based authentication workflow. First, when a user tries to access a site, the service provider asks the identity provider to authenticate the user. Then, the service provider uses the SAML assertion issued by the identity provider to grant the user access. Let's illustrate the workflow with an example.

1. The user opens their browser and navigates to the service provider's web application, which uses an identity provider for authentication.
2. The web application responds with a SAML request.
3. The browser passes SAML request to the identity provider.
4. The identity provider parses the SAML request.
5. The identity provider authenticates the user by prompting for a username and password or some other authentication factor.
   NOTE: The identity provider will skip this step if the user is already authenticated.
6. The identity provider generates the SAML response and returns it to the user's browser.
7. The browser sends the generated SAML response to the service provider's web application which verifies it.
8. If the verification succeeds, the web application grants the user access.