What is SAML?

Security Assertion Markup Language, or SAML, is a standardized way to tell external applications and services that a user is who they say they are. SAML makes single sign-on (SSO) technology possible by providing a way to authenticate a user once and then communicate that authentication to multiple applications. The most current version of SAML is SAML 2.0.

Think of SAML authentication as being like an identification card: a short, standardized way to show who someone is. Instead of, say, conducting a series of DNA tests to confirm someone's identity, it is possible to just glance at their ID card.

In computing and networking, one of the major challenges is getting systems and devices built by different vendors for different purposes to work together. This is called "interoperability": the ability for different machines to interact with each other, despite their differing technical specifications. SAML is an interoperable standard — it is a widely accepted way to communicate a user's identity to cloud service providers.

What is single sign-on (SSO)?

Single sign-on (SSO) is a way for users to be authenticated for multiple applications and services at once. With SSO, a user signs in at a single login screen and can then use a number of apps. Users do not need to confirm their identity with every single service they use.

For this to take place, the SSO system must communicate with every external app to tell them that the user is signed in — which is where SAML comes into play.

How does SAML work?

A typical SSO authentication process involves these three parties:

- Principal (also known as the "subject")
- Identity provider
- Service provider

Principal/subject: This is almost always a human user who is trying to access a cloud-hosted application.

Identity provider: An identity provider (IdP) is a cloud software service that stores and confirms user identity, typically through a login process. Essentially, an IdP's role is to say, "I know this person, and here is what they are allowed to do." An SSO system may in fact be separate from the IdP, but in those cases the SSO essentially acts as a representative for the IdP, so for all intents and purposes they are the same in a SAML workflow.

Service provider: This is the cloud-hosted application or service the user wants to use. Common examples include cloud email platforms such as Gmail and Microsoft Office 365, cloud storage services such as Google Drive and AWS S3, and communications apps such as Slack and Skype. Ordinarily a user would just log in to these services directly, but when SSO is used, the user logs into the SSO instead, and SAML is used to give them access instead of a direct login.

This is what a typical flow might look like: The principal makes a request of the service provider. The service provider then requests authentication from the identity provider. The identity provider sends a **SAML** assertion to the service provider, and the service provider can then send a response to the principal.

If the principal (the user) was not already logged in, the identity provider may prompt them to log in before sending a SAML assertion.

What is a SAML assertion?

A SAML assertion is the message that tells a service provider that a user is signed in. SAML assertions contain all the information necessary for a service provider to confirm user identity, including the source of the assertion, the time it was issued, and the conditions that make the assertion valid.

Think of a SAML assertion as being like the contents of a reference for a job candidate: the person providing the reference says when and for how long they worked with the candidate, what their role was, and their opinion on the candidate. Based on this reference, a company can make a decision about hiring the candidate, just as a SaaS application or cloud service can allow or deny user access based on a SAML assertion.

What is SAML 2.0?

SAML 2.0 is the modern version of SAML, and it has been in use since 2005. SAML 2.0 combined several versions of SAML that had previously been in use. Many systems support earlier versions, such as SAML 1.1, for backwards compatibility, but SAML 2.0 is the modern standard.

Is SAML authentication the same thing as user authorization?

SAML is a technology for user authentication, not user authorization, and this is a key distinction. User authorization is a separate area of identity and access management.

Authentication refers to a user's identity: who they are and whether their identity has been confirmed by a login process.

Authorization refers to a user's privileges or permissions: specifically, what actions they are allowed to perform within a company's systems.

Think about the difference between authentication and authorization like this: Imagine Alice attends a music festival. At the entrance to the festival, she presents her ticket and an additional form of identification to prove that she has the right to possess the ticket. On doing this, she is allowed to enter the festival. She has been authenticated.

However, just because Alice is within the festival does not mean she can go anywhere and do anything she wants. She can watch the festival acts, but she cannot go on stage and perform, nor can she go backstage and interact with the performers — because she is not authorized to do so. If she had purchased backstage passes, or if she was a performer in addition to being an attendee, she would have a greater amount of authorization.

Access management technologies handle user authorization. Access management platforms use several different authorization standards (one of which is OAuth), but not SAML.

Cloudflare Access is one example of an access management solution. Cloudflare Access enables companies to manage user access to internal resources and data without the use of a virtual private network (VPN). It integrates easily with SSO providers to offer both user authorization and user authentication.

Learn more about SSO.