

GOOGLE SINGLE SIGN ON (SSO) OVERVIEW

Owner

Amplifi.io Product Team

Summary

AMPLIFI.IO is a cloud-based digital asset management software designed to help product brands rapidly *organize, convert, manage and share* marketing content and digital assets.

Document Purpose

This document summarizes the concepts and set-up of the Amplifi.io SSO via SAML 2.0.

- **Benefits include:**
 - Single Sign On capabilities and security
 - Amplifi.io DAM system opens immediately for users and remembers user's collections
 - Admins can see user history
 - Streamlined bulk user onboarding
 - Ensure fast user access and broad system usability

Single Sign-On

Enterprise single sign-on allows employees in a company to access all the company application with one set of credentials. Depending on the company, the credentials can include email, phone number or username along with the password. The company routes all logins through an IDP (Identity Provider) with which the company has a purchased license. The IDP usually hosts a login page for the employees to enter their company credentials before entering any application. Single Sign On provides better security with the central authentication point, limiting the possibility of phishing.

About enterprise single sign-on

When you enable enterprise single sign-on, you're bypassing Amplifi.io and authenticating your users externally. When users navigate to your Amplifi.io sign-in page or click a link to your Amplifi.io, they can authenticate by signing into a corporate server or a third-party identity provider.

If you're using enterprise single sign-on, your users' sign-in flow will follow the sequence below:

- 1) Users navigate to your Amplifi.io subdomain.
- 2) If not already authenticated, users are redirected to your corporate server or third party identity provider login page, depending on the enterprise SSO option you selected.
- 3) Users enter their sign-in credentials.
- 4) If valid, users are redirected back to the Amplifi.io home page.

Note: Users can also start the sign-on process from your corporate server or the third-party identity provider sign-in page. They will then be authenticated automatically when accessing Amplifi.io.

All users can sign in to your Amplifi.io using enterprise single sign-on.

The advantage to using enterprise single sign-on is that you have complete control over your users, behind your firewall. You authenticate your users once, against your own user authentication system, and then grant them access to many other resources both inside and outside of your firewall. This does not mean that your Amplifi.io user management is performed outside of your Amplifi.io subdomain, the user accounts must exist within Amplifi.io to allow access. So if you add a user account for a new employee, you will need to create the user using their email address on Amplifi.io.

By default, the only data that Amplifi.io stores for each user is their name and email address.

Enterprise single sign-on options

There are two types of enterprise single sign-on options available in Amplifi.io:

Secure Assertion Markup Language (SAML) is not enabled by default and requires proper licensing to be enabled. SAML is supported by many identity provider services, such as Okta, Active Directory, and LDAP.

Using SAML

Amplifi.io Support supports Secure Assertion Markup Language (SAML), which allows you to provide single sign-on (SSO) for your Amplifi.io Support account using enterprise identity providers such as Active Directory and LDAP. Single sign-on using SAML is available on Amplifi.io Professional and Enterprise edition.

Implementing single sign-on via SAML means that the sign in process and user authentication are handled entirely outside of Amplifi.io Support. Your users will not directly visit your Amplifi.io login page to sign in. Instead users sign in to the corporate system (authenticated by Active Directory or LDAP for example) and click a link to access Amplifi.io and are automatically signed in. No need to enter separate sign-in credentials for Amplifi.io.

The user data required to be stored in Amplifi.io is the user's name and email address. However, there are other fields available to enrich the user's information such as their geographical location. You do this by adding these attributes to your SAML assertion code. See User attributes that can be set in SAML. Amplifi.io does not store user passwords.

How SAML for Amplifi.io works

SAML for Amplifi.io works the way SAML does with all other service providers. The typical use case is that your users belong to a corporation and all user authentication is managed by your corporate authentication system (for example, Active Directory or LDAP), which is referred to generically as an identity provider (IdP). The service provider (SP), in this case Amplifi.io, establishes a trust relationship with IdP and allows that external IdP to authenticate users and then seamlessly sign them in to Amplifi.io. In other words, a user signs in at work and then has automatic access to the many other corporate applications such as email, your CRM, and so on without having to sign-in separately to those services. Aside from the convenience this provides to users, all user authentication is handled internally by a system that you have complete control over.

After you've enabled SAML as the type of single sign-on for Amplifi.io, users who visit your Amplifi.io account and attempt to sign in are redirected to your SAML server for authentication. Your users' identities can be stored either on the SAML server or can be validated by an identity directory such as Microsoft Active Directory or LDAP. Once authenticated, users are redirected back to your Amplifi.io account and automatically signed in.

Another supported workflow is having the user sign in to your own website directly rather than to your Amplifi.io instance. The website sends a request to the identity provider to validate the user. The website then sends the provider's response to the SAML server, which forwards it to your Amplifi.io instance, which grants a session to the user.

Returning visitors are automatically authenticated if their SAML assertions are cached. Assertions are packets of security information that are used to make access-control decisions.

Configuring Amplifi.io for new users

An Amplifi.io user profile is created for any new user who accesses your Amplifi.io account through SAML. Because they're authenticated with a non-Amplifi.io password, the profile is created without a password because they don't need to sign in to Amplifi.io.

Configuring your SAML implementation

You have a number of options when considering a SAML service, including building a SAML server in-house (for example, OpenAM) or choosing a SAML service such as Okta, OneLogin, and PingIdentity.

To set up SSO in your Amplifi.io, you'll need the following a SAML server with provisioned users or connected to an identity repository, in this case Google Workspace.

The Remote Login URL for your SAML server (sometimes called SAML Single Sign-on URL)

The SHA1 or SHA2 fingerprint of the SAML certificate from your SAML server. X.509 certificates are supported and should be in PEM or DER format. There is no upper limit on the size of the SHA fingerprint.

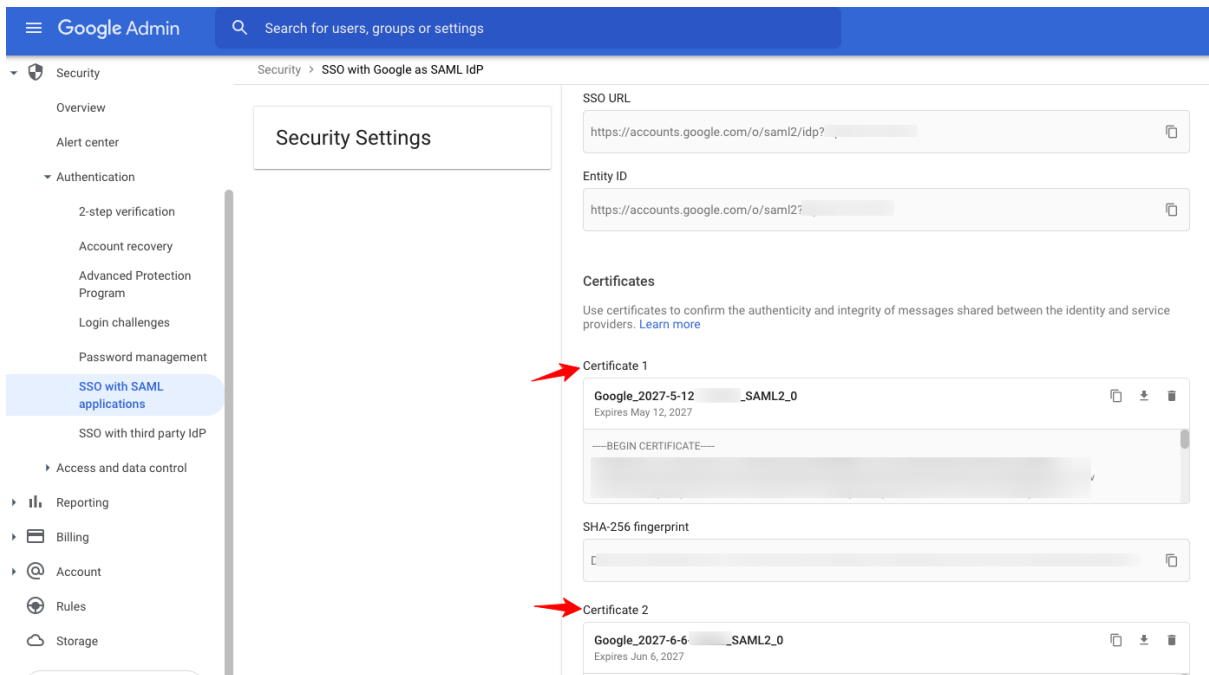
After you have your SAML server properly configured, you can use the remote login URL and the SHA fingerprint to configure SAML in Amplifi.io.

Google SAML Setup Instructions

Generating Certificates

1. In Google Workspace Admin navigate to **Security > Authentication > SSO with Google as SAML IdP**.

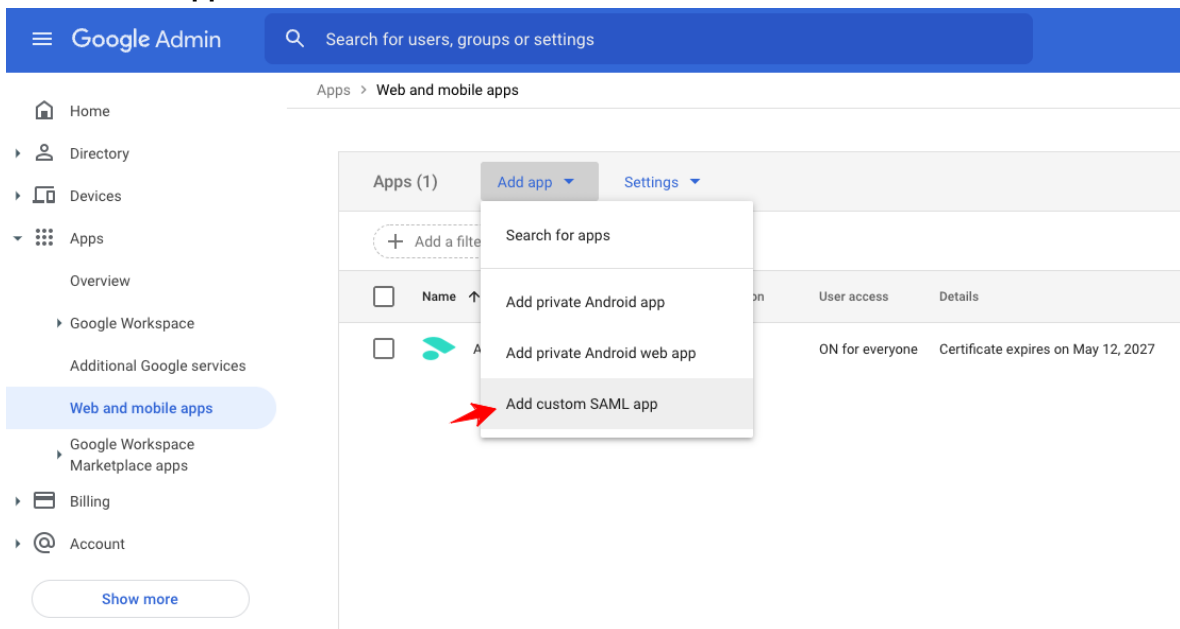
2. Click the button Add Certificate to and ensure that there are 2 certificates in your view.



3. Proceed to next section of this document **Creating a SAML App in Google Workspace**

Creating a SAML App in Google Workspace

1. In Google Workspace Admin navigate to **Apps > Web & Mobile Apps**
2. Choose **Add App**



3. Give your app a name (this will be the name that shows in your app selector menu for your users), add an optional description, and then add an icon for the app (square images are the best).
4. In the next window choose **Option 1: Download IdP metadata** and download your certificate XML.
5. Click **Continue**.
6. Enter the following
 - a. Access URL:
https://saml.amplifi.io/saml/module.php/saml/sp/saml2-acis.php/[**companyname**]
 - b. Entity ID: [**companyname**]

NOTE: "**companyname**" is the name/alias of your organization in your Amplifi instance. The customer's Amplifi.io DAM instance url is https://**companyname**.amplifi.io your Entity is going to be the same as the first part of your Amplifi subdomain.

 - c. Leave Signed Response unchecked
 - d. Start URL: your full amplifi.io subdomain with no trailing slash
 - e. Name ID: set your name ID to be Email: basic information > primary email
7. Click **Continue**.
8. Map the following information from the Google profile to the Amplifi user data


Google Property	Amplifi User Attributes (case-sensitive)
Primary Email	email
First Name	firstname
Last Name	lastname
Phone Number	phone
Locale	language_code

9. You can ignore any group assignments.
10. Click **Finish**.






Send your downloaded IdP Metadata XML to your Amplifi onboarding lead and they will get your certificate installed in the SAML application. Once installed you can test your application.

Apps > Web and mobile apps > Test App

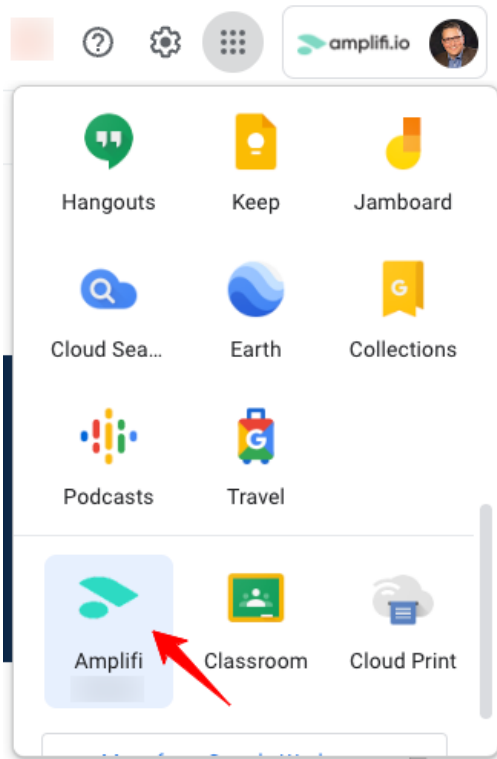
SAML



Test App

-  TEST SAML LOGIN 
-  DOWNLOAD METADATA
-  EDIT DETAILS
-  DELETE APP

Once completed your application will now also show in your application selector.



The application selector interface shows a grid of application icons. At the top, there are utility icons: a square, a question mark, a gear, a grid, and a profile card for 'amplifi.io'. The grid contains icons for Hangouts, Keep, Jamboard, Cloud Sea..., Earth, Collections, Podcasts, and Travel. At the bottom, there are icons for Amplifi, Classroom, and Cloud Print. A red arrow points to the Amplifi icon.