BIG THINK +

Set up SSO with Google Workspace

Last Modified on 11/10/2026 3:57 pm EST

This article explains how to set up Single Sign-On (SSO) for Big Think+ with Google Workspace using SAML 2.0.

This guide is for Google Workspace administrators. When setup is complete, your users sign in to Big Think+ with their Google Workspace accounts. Google is the identity provider (IdP) and Big Think+ is the service provider (SP).

What do I need before I start?

- **Super administrator access** to your Google Admin console. Google requires a super admin to add and turn on custom SAML apps.
- **Your Big Think+ organization permalink**, provided by your Big Think+ Partner Services contact. Wherever this guide shows `<permalink>`, replace it with yours.
- **The email domains** your users sign in with (for example, `yourcompany.com`).

What values do I enter in Google Workspace?

Google field	Value
ACS URL	`https://plus.bigthink.com/o/<permalink>/auth/saml/acs`
Entity ID	`plus.bigthink.com`
Start URL	Leave blank
Signed response	Leave unchecked (default)
Name ID format	EMAIL
Name ID	Basic Information > Primary email

The ACS URL ends in `/acs`, not `/metadata`. You can confirm both values in the Big Think+ metadata at `https://plus.bigthink.com/o/<permalink>/auth/saml/metadata`: the ACS URL is the `Location` of the `AssertionConsumerService` entry and the Entity ID is the `entityID` value.

How do I set up SSO with Google Workspace?

1. Add Big Think+ as a custom SAML app

1. Sign in to the Google Admin console as a super administrator.
2. Go to **Menu** > **Apps** > **Web and mobile apps**.

3. Click **Add app** > **Add custom SAML app**.
4. On *App details*, enter **Big Think+** as the app name. Optionally upload a Big Think+ icon (ask Partner Services for one); it appears in your users' Google app launcher. Click **Continue**.
5. On *Google Identity Provider details*, click **Download metadata** under Option 1 and save the XML file. You will send this file to Big Think+ in Step 2. Click **Continue**.
6. On *Service provider details*, enter the **ACS URL** and **Entity ID** from the table above. Leave **Start URL** blank and **Signed response** unchecked.
7. Under *Name ID*, set **Name ID format** to EMAIL and **Name ID** to **Basic Information > Primary email**. Click **Continue**.
8. On *Attribute mapping*, no mappings are required: Big Think+ identifies users by the email in the Name ID. If you want first and last names in Big Think+ analytics, click **Add mapping**, map **First name** and **Last name** from Basic Information, and tell Partner Services the app attribute names you used.
9. Click **Finish**.

The app now exists but is **off for all users**. Do not turn it on until Big Think+ confirms your metadata is loaded (Step 3).

2. Send your metadata and domains to Big Think+

Email your Partner Services contact (or partnerservices@bigthink.com) with:

- The **metadata XML file** you downloaded in Step 1.
- The **email domains** your users sign in with. Big Think+ uses these to send users to Google from the sign-in page.
- The **email address of your first Big Think+ admin**. That person signs in once through SSO, and Big Think+ promotes them to admin.

Unlike Okta and Microsoft Entra ID, Google Workspace does not publish a metadata URL for custom SAML apps, so you send the XML file itself. Because Big Think+ cannot refresh it automatically, you must send a new file whenever your signing certificate changes (see the certificate section below).

3. Turn on user access

After Big Think+ confirms your metadata is loaded:

1. In the Admin console, go to **Menu** > **Apps** > **Web and mobile apps** and select **Big Think+**.

2. Click **User access**.
3. To give everyone access, select **On for everyone** and click **Save**. To limit access, select an organizational unit on the left (or an access group) and set **Service status** to **On**.

Google says access changes can take up to 24 hours, though they usually apply sooner. Users who are not turned on will see a Google error, not a Big Think+ error, when they try to sign in.

Make sure each user's primary Google email is the address they should use in Big Think+. That email becomes their Big Think+ identity.

Google's User access setting is the only gate. Anyone you turn the app on for gets a Big Think+ account the first time they sign in, so limit access in Google if not everyone in your organization is licensed.

4. Test the connection

Test with a user who has access turned on in Step 3.

- **From Big Think+ (SP-initiated):** open `https://plus.bigthink.com/o/<permalink>` in a private browser window. You should be sent to Google sign-in, then returned to Big Think+ signed in.
- **From Google (IdP-initiated):** in the Admin console, open the Big Think+ app and click **Test SAML login**, or click the Big Think+ tile in the Google app launcher. Big Think+ should open in a new tab, signed in.

What happens when my signing certificate expires?

Google's SAML signing certificate is valid for five years and does not renew itself. When it nears expiry:

1. In the Admin console, open the Big Think+ app and click **Service provider details**.
2. Under *Certificate*, add a new certificate, then select it for the Big Think+ app and save.
3. Click **Download metadata** and send the new XML file to Partner Services.

Schedule the switch with Partner Services so the certificate change in Google and the metadata update on the Big Think+ side happen together; otherwise sign-in fails in between. Set a calendar reminder a few months before the expiry date shown on the certificate.

What if something is not working?

See Troubleshooting SSO sign-in. Google's own reference: Set up your own custom SAML app.

Back to Single Sign-On (SSO) / SAML 2.0 overview