BIG THINK +

Set up SSO with Microsoft Entra ID (Azure AD)

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 Microsoft Entra ID (formerly Azure AD) using SAML 2.0.

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

What do I need before I start?

- **An Entra ID role that can create enterprise applications**, such as Cloud Application Administrator or Application Administrator.
- **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 Microsoft Entra ID?

Entra ID field	Value
Identifier (Entity ID)	`plus.bigthink.com`
Reply URL (Assertion Consumer Service URL)	`https://plus.bigthink.com/o/<permalink>/auth/saml/acs`
Sign on URL, Relay State, Logout URL	Leave blank

The Reply 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 Reply URL is the `Location` of the `AssertionConsumerService` entry and the Identifier is the `entityID` value.

How do I set up SSO with Microsoft Entra ID?

1. Create the Big Think+ enterprise application

1. In the Microsoft Entra admin center, go to **Enterprise applications** (under Identity > Applications, or Entra ID > Enterprise apps, depending on your portal version) and click **New application**.

2. Click **Create your own application**.

3. Enter **Big Think+** as the name, select **Integrate any other application you don't find in the gallery (Non-gallery)**, and click **Create**.

2. Configure SAML

1. In the Big Think+ application, open **Single sign-on** and choose **SAML**.
2. In the *Basic SAML Configuration* box, click **Edit**. Enter the **Identifier (Entity ID)** and **Reply URL** from the table above, and click **Save**. If Entra offers to test now, choose to test later.
3. In the *Attributes & Claims* box, check the **Unique User Identifier (Name ID)**. Big Think+ identifies each user by this value, so it must be the user's email address. The default is `user.userprincipalname`. If your users' UPNs are not their email addresses, change the source attribute to `user.mail`.
4. Entra sends first name and last name claims by default. If you want names in Big Think+ analytics, tell Partner Services and they will map them.

3. Send your metadata and domains to Big Think+

1. In the *SAML Certificates* box, copy the **App Federation Metadata URL**.
2. Email your Partner Services contact (or partnerservices@bigthink.com) with:
    - The **App Federation Metadata URL**.
    - The **email domains** your users sign in with. Big Think+ uses these to send users to Microsoft 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.

4. Assign users and groups

After Partner Services confirms your metadata is loaded, open the application's **Users and groups** page, click **Add user/group**, and assign the people or groups who should have Big Think+.

Entra ID is the only gate. Anyone who can sign in to the app gets a Big Think+ account the first time they sign in. Keep **Assignment required?** set to **Yes** (under the application's **Properties**) unless everyone in your tenant should have access.

5. Test the connection

- **From Microsoft (IdP-initiated):** on the application's *Single sign-on* page, click **Test**, or

open the Big Think+ tile in My Apps. Big Think+ should open, signed in.

- **From Big Think+ (SP-initiated):** open `https://plus.bigthink.com/o/<permalink>` in a private browser window. You should be sent to Microsoft sign-in, then returned to Big Think+ signed in.

What happens when my signing certificate changes?

The SAML signing certificate Entra creates for the app expires (three years by default). Before you activate a new certificate, contact Partner Services so the change on both sides happens together.

What if something is not working?

See Troubleshooting SSO sign-in. Microsoft's own reference: Enable SAML single sign-on for an enterprise application.

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