BIG THINK +

Single Sign On (SSO) / SAML 2.0

Last Modified on 06/18/2026 10:59 am EDT

This article explains how Single Sign-On (SSO) works with Big Think+, why your organization might use it, and what's required to set it up.

SAML 2.0 SSO Integration Overview

Single Sign-On (SSO) via SAML 2.0 allows learners to seamlessly and securely access Big Think+ using their existing company credentials. While not a content integration in itself, SAML-based SSO is a foundational access method that enables and supports many other integrations, including many of our API integrations.

SSO enables users to log in to Big Think+ without creating or managing a separate password, improving user experience and reducing friction. It also ensures that only authorized employees can access your Big Think+ instance.

Supported Use Cases

This integration allows organizations to:

- Provide frictionless, secure access to Big Think+ for learners.
- Ensure that only authorized users within the company access the platform.
- Support integrations that require authenticated user access.
- Use existing identity providers like Okta, Microsoft Entra, PingIdentity, and others to manage access.

What's Required

To complete the SSO setup, Big Think+ needs:

- Your organization's SAML 2.0 metadata (either URL or XML).
- An IT administrator to test the login and confirm successful access.
- Optional: A logo for your login tile (for platforms like Okta).

User Access & Management

SSO handles all user authentication. You **do not** need to manually create user accounts in Big

Think+.

Instead:

- A designated administrator at your organization logs in via SSO and is promoted to an admin role by our team.
- This administrator can then manage organization settings and permissions.
- Additional user data, such as email, can be passed through SAML, depending on your setup.

Integration Checklist

1. Big Think+ provides metadata to our partner organizations with a URL: http://plus.bigthink.com/o/<client-permalink>/auth/saml/metadata

2. We ask partner organizations to provide metadata back, either as a URL or an XML file. Note: The IDP Metadata URL is preferred, since that allows us to stay in sync with any changes to their system and does not expire.

3. The partner organization tests either by setting up a tile in SSO system or by clicking a testing link provided by Big Think+ (https://plus.bigthink.com/o/<client-permalink>)

4. In some systems, partners will need to go into their SSO admin portal and grant users specific permissions.

Domain Registration and SSO Redirect

To route your users to the correct identity provider, Big Think+ registers your organization's email domains (for example, `yourcompany.com`) on our end during setup. You provide the domains your organization uses, and our team adds them to your organization's configuration.

Once your domains are registered, the redirect works automatically:

- When a user goes to the Big Think+ sign-in page, we check the domain of the email or organization they're associated with.
- If we recognize the domain as one tied to your organization, we redirect the user to your SSO provider to authenticate.
- After they authenticate successfully, they're returned to Big Think+ with access.

This means your users do not need a separate Big Think+ login. As long as they're signing in from a registered domain, they'll be routed to your identity provider every time.

A Note on Account Creation

Whether a user can have an account created depends entirely on your SSO provider's configuration. If your SSO provider can authenticate a user to Big Think+, an account will be created for them, even if they do not have an email address on your primary domain. If your SSO provider cannot authenticate that user, no account will be created.

In short: account creation follows whatever rules your identity provider enforces. If you need users outside your primary domain to gain access, confirm that your SSO provider is configured to authenticate them.