PLURALSIGHT | HELP CENTER

Managing team access with SSO

Tags: ACG

Single Sign-On (SSO) gives our clients the ability to manage access to the A Cloud Guru platform directly through their team's Identity Provider (IdP).

SSO features

ACG utilizes the SAML 2.0 version of SSO, as well as both IdP and SP-initiated login flows. SSO has several inherent features.

- Just-in-Time provisioning—Easily manage the authentication and authorization of learners by allocating licenses as learners click to log in to ACG.
- One-click login—Reduce time spent entering multiple login details by allowing learners to log in via your IdP.
- No more password—Cut down the number of usernames and passwords a learner has to remember, and reduce password reset requests.

Current identity providers

- Okta
- Microsoft Azure AD
- OneLogin

Enabling SSO

1. Reach out to your Relationship Manager or Customer Success Manager to start this process. Then, an ACG Integrations Consultant will reach out to you to learn more about your IdP and provide you with credentials to help create the SSO connection.
2. Provide the ACG Integrations Consultant with the metadata needed to complete the connection.

The ACG Integrations Consultant will let you know when the connection is created and is ready for testing. Please reach out to our Support team if you have any questions.

Adding users to a plan roster via SSO

Enabling SSO removes the invitation feature and replaces it with the SSO authentication. If the authentication grants a user permission to join your plan's roster, they'll be able to do so without an invitation.
