SAML - what it is, how single sign-on works, and setup essentials

Gridinsoft Help Center

What it is

SAML is a standard that lets you use one login to access multiple websites and apps. You sign in once at an identity provider (like your company or school account), and that provider sends a signed "assertion" to other services proving who you are. The services trust that proof, so you don’t create a new password for each one. Background and examples: https://gridinsoft.com/saml

Why it matters

Fewer passwords to manage means fewer weak or reused passwords. Centralized login also makes it easier to turn access on or off when someone joins or leaves a team.

How it works - quick tour

- You try to open an app. It redirects you to the identity provider (IdP).
- You sign in at the IdP.
- The IdP sends a signed SAML response back to the app (the service provider).
- The app checks the signature and logs you in without asking for another password.

Red flags

- Clock drift on devices causing "invalid or expired SAML" errors.
- Mismatched URLs or certificate problems after a settings change.
- Unexpected logins if a stolen session isn’t revoked at the IdP.
- Users still asked for separate passwords because SSO isn’t enforced.

Do it right

- Keep IdP and app clocks in sync and rotate SAML certificates before they expire.
- Lock down which apps can accept SAML from your IdP and review who has access.
- Use MFA at the IdP so one strong login protects all connected apps.
- After an account is removed at the IdP, verify access is cut off across apps.