

Simple and Secure Single Sign-on

Data

- Librarians **control which attributes are released** to providers via OpenAthens to protect personally identifiable information (PII).
- Library administrators can create **custom attributes** (text, date, yes/no, multiple choice formats) to store on user accounts and permission groups for reporting purposes.
- All user attribute data is **ENCRYPTED** before it is shared with service providers and publishers.
- [Privacy Policy](#)

Account Misuse Monitoring

- If a single account is used to sign in from different regions of the world in a short period of time, the account will automatically be suspended, and a report sent to the administrator.
- **Protect your users.** Early detection of misused accounts helps safeguard those who use the same password for all their accounts, such as personal financial and social accounts.
- Prevent publishers from suspending your institution's access to their resources.

Technology

- Cloud-based SaaS product that uses JAVA, Javascript, and PHP.
- [Google Cloud Platform's](#) leading security measures.
- Uses Security Assertion Markup Language / **SAML** (sam-l) a well-established open standard, designed for the best possible user experience with the added benefit of maximum security. It passes selective information about an individual without ever giving out user's credentials.
- SSO integrations with existing systems and directories such as Microsoft Azure, G Suite, OneLog, Shibboleth, CAS, SirsiDynix, OKTA, Ping Identity, and many more.



**Learn more about
OpenAthens**