EBSCO | Stacks SECURITY

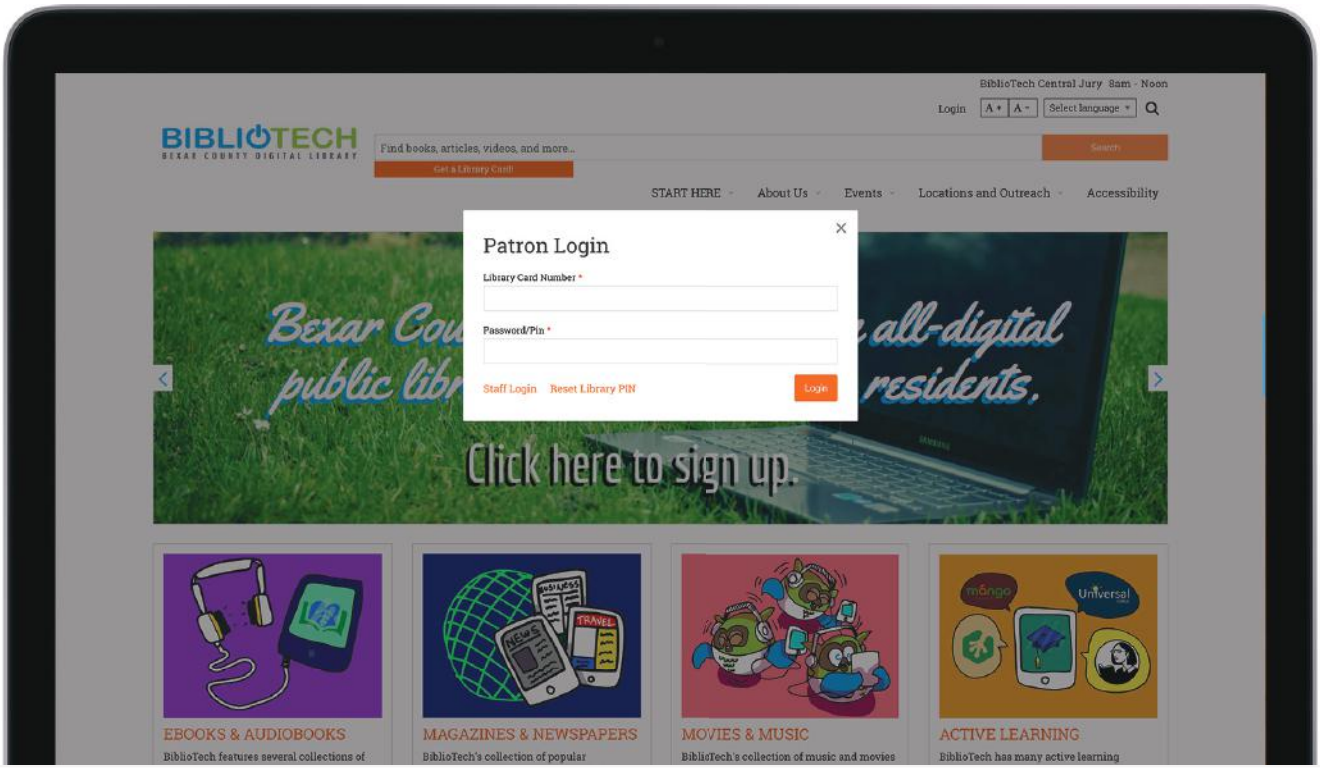
Security Features

Ensuring your information is safe and secure is paramount for any organization. Stacks is built to prevent the worst from happening by providing a secure CMS and application framework with robust security. Organizations around the world rely on Stacks for portals and applications, testing its security against the most stringent standards and ensuring protection against the most critical internet vulnerabilities in the world.

Authentication Integrations

Authentication may be integrated using Stacks plug and play ILS API integrations, SIP2 or standard SSO integrations such as LDAP, ADFS, SAML and Shibboleth. Additional statistical benefits are added when pairing one of these external integrations with Stacks OpenAthens integration.

- OpenAthens
- SSO
- LDAP
- ADFS
- SAML
- Shibboleth



Stacks Inc.

www.StacksDiscovery.com

information@ebsco.com

Login Services

Stacks provides a library-specific hierarchical role structure which is designed to support all levels of staff. Intricate moderation rules such as requiring proofing and approval before publishing with email notifications, ensures safe and responsible workflows within your organization. These roles can be further refined by individual libraries post implementation as necessary. Default roles include: Administrator, Moderator, Editor, Contributor and Patron.

Performance and Hosting

Stacks production instances are run on a 99.9% uptime-guaranteed managed host with 24/7 support. The managed host also monitors hardware and network connections for reliability purposes. 99.99% uptime available with Stacks Premium.

Stacks utilizes a cloud environment to maintain a high degree of security while integrating all recommended information security standards as defined by ISO 27001. This includes the following:

- Enforces the use of highly secure RSA keys for server access and encryption;
- Maintains centralized logging of all servers;
- Regularly patches servers and applications;
- Enforces the use of firewalls and server monitoring; and
- Follows the openSCAP security guidelines for all servers not on our managed host.

CMS and Application Framework

- Account passwords are encrypted--salted and repeatedly hashed--when they are stored in the database.
- Stacks protects against brute-force password attacks by limiting the number of login attempts from a single IP address over a predefined period of time. Failed login attempts are logged and visible via the administrative interface.
- Stacks includes features that address all of the Open Web Application Security Project's top ten security risks, a list of the most commonly seen risks in practice.

Response and Support

Stacks is a cloud-based research portal and is sold as a managed service meaning there are no additional staff required for support and maintenance. To ensure you are able to receive help when you need it, Stacks is supported by both EBSCO Customer Support and the Stacks Support Desk.