Single Sign-On Authentication - Frequently Asked Questions

EBSCO's SSO solution provides seamless authentication and personalization to EBSCO resources. It works with any SAML-compliant identity solution, including OpenAthens, Shibboleth, Ping, Okta, Microsoft ADFS, and more.

The FAQs on this page provide general information about EBSCO's Single Sign-On authentication as well as information about implementation of the service.

General Questions

My organization is interested in deploying SSO, how do we get started?
To learn how your institution can enable EBSCO SSO, contact your EBSCO Sales representative who will initiate next steps with our SSO support team. Our SSO Support team will work with you to review requirements, SAML metadata needs and expected time frame to ensure SSO can be enabled for your EBSCO resources.

Which SSO software solutions can be used with EBSCO?
Any SSO platform can be used so long as it supports Shibboleth 1.0, or SAML.

My institution uses OCLC’s EZ Proxy, Can we use SSO?
EZProxy is not supported as SSO software, it is a service provider (like EBSCO) and not an identity provider.

What is the difference between an Identity Provider and Service Provider?
An Identity Provider, abbreviated as IdP, is the entity (e.g. company, university) which creates and maintains user accounts. A Service Provider, abbreviated as SP, is typically a publisher or content provider owning and providing a service or resource which the IdP-based users consume.

What is the difference between OpenAthens and SSO?
OpenAthens is a family of products whose core components are identity and access management. Developed and maintained by Eduserv, an EBSCO partner, OpenAthens offers users a single username and password (i.e. identity management) to access all of a library’s various internal and external, subscription-based content resources (i.e. access management). It is a system which can be locally hosted behind an organization’s firewall or be hosted by an internet service provider on behalf of the organization. OpenAthens is also capable of acting as the IdP.

As part of its identity management offering, OpenAthens offers a SAML-based approach to user authentication for external, subscription-based content resources such as EBSCO. Customers can purchase OpenAthens from EBSCO and use it to manage their student or employee user accounts, and optionally integrate it with EBSCO SSO. This integration enables end users to be automatically authenticated and personalized so they can download EBSCO eBooks, save content to folders, create alerts and more without having to log in separately to EBSCO.
Implementation Questions

Will the EBSCO user experience change when migrating to SSO from my current EBSCO authentication method?
No. SSO can be configured so that a non-SSO authentication method is utilized for authentication (e.g. IP, User ID) but also opt to use SSO for personalization, at the point users choose to access their My EBSCO host folders. Alternatively, SSO can be configured so that both authentication and personalization are both automatic and seamless for the end user, whereby, users are immediately directed to the target EBSCO page (e.g. main page, search results or article) without any interim authentication or personalization steps needed after clicking any EBSCO access link.

My organization uses IP Address authentication for EBSCO access, can we test SSO in a segregated testing environment before deploying to production?
Yes. SSO is enabled at the group level in EBSCO admin. By creating a new group or using an existing, non-production group (e.g. Trial), we can conduct user acceptance testing in an isolated way without impacting production users.

Which user data attributes must be included within the IdP-generated SAML assertion?
Only a unique user ID (e.g. employee ID, organization-specific email) is required to be sent in the SAML assertion. It is recommended that First Name, Last Name and Email also be sent to better support sharing and email from within the EBSCO user interface.

Is it necessary to modify any/all EBSCO persistent links to include the SSO query string parameters?
Yes. For SSO authentication to be properly initiated for end users, all actively deployed persistent links must be updated to reflect SSO authentication and your institution’s EBSCO customer ID. Failure to do so may result in anonymous access or users being prompted to log in to EBSCO.

How does guest access work with SSO?
Guest access can be used with SSO when the “Personalize using SSO” parameter for your user group is turned on.

In this instance, your EBSCO persistent link would remain as it is today with the standard authentication types in the URL.

For example: http://search.ebscohost.com/login.aspx?authtype=ip,guest&group=library&profile=ehost

Note: The authentication string authtype=sso,guest is not supported.

When a guest user logs in, the user is directed to your proxy server, signs in, and is authenticated back into EBSCO’s platform.

Next, when the user attempts to personalize (sign in to My EBSCO host), the user is directed to your institution’s Identity Provider page because the “Personalize using SSO” setting has been turned on.

After signing in through your institution’s login screen, the user is directed back into EBSCO host EBSCO’s platform and is no longer a guest user.
What are the Scoped Affiliation and Entitlement fields?

Affiliation: A high-level expression of the relationship of the user to the university or organization specified in the domain. A user can possess many affiliations, though some values are mutually exclusive. This attribute is often made available to any Shibboleth service provider, and is a good way to filter or block users of a given general type. In particular, "member" is an indication that the user is somebody with relatively official standing with a university at the present time, and does not apply to guests, other temporary accounts, terminated employees, unpaid/unregistered students, and other exceptional cases.

Entitlement: Multiple values, each a uniform resource identifier, representing a license, permission, right, etc. to access a resource or service in a particular fashion. Entitlements represent an assertion of authorization to something, precomputed and asserted by the identity provider. This attribute is typically used to assert privileges maintained centrally rather than within specific application databases.


For more details on Affiliation and Entitlement, see: http://www.incommon.org/federation/attributesummary.html

See also: Single Sign-On Authentication - An Overview