

What authentication methods are available for accessing EBSCOhost?

EBSCOhost offers several different methods of authentication for users: *En Español*

IP Address

Patterned IDs

Patron ID files

Referring URL

User ID and Password

Cookie Authentication

Athens Authentication

Shibboleth Authentication

HTTPS Authentication

IP Address authentication is the traditional method of identifying users requesting access to vendor databases. Users gain access based on their computer or site's IP address (numerical address). The URL to use for IP authentication is **<http://search.ebscohost.com/login.aspx?authtype=ip>**

Patterned ID authentication provides access to EBSCOhost via a library card or bar code number. If the number entered does not match an ID set up by the library administrator, access is not permitted. The administrator can decide which characters are significant and compare up to 30 characters if needed. The URL to use for Patterned ID authentication is

<http://search.ebscohost.com/login.aspx?authtype=cpid&custid=custid>

Patron ID (Customer Coordinated) authentication lets you use library or patron card numbers (up to 20 characters) to control access. The librarian provides EBSCO with a list of IDs that are used to identify users asking for access to databases. Without an ID number, assigned by library staff, a user cannot access EBSCOhost. You can also customize the login prompts and easily delete one user's access without affecting another's. The URL to use for Patron ID authentication is

<http://search.ebscohost.com/login.aspx?authtype=custuid&custid=custid>

Referring URL authentication provides access to EBSCOhost from a secure home page on the library's web server. This identifies users by the originating URL (the page from which they came) and eliminates the need for user IDs. EBSCOhost validates the user if they are coming from an approved URL. If a user is trying to log in from a different URL, the system will not authenticate. The URL that should be used with Referring URL authentication is **<http://search.ebscohost.com/login.aspx?authtype=url>**

[User ID and Password authentication](#) can be useful to users who access EBSCO*host* remotely. The library administrator can provide users with a user ID and password, providing instant access to EBSCO*host* from their home or school computer. The URL that should be used with User ID/Password authentication is **<http://search.ebscohost.com/login.aspx?authtype=uid>**

[Cookie authentication](#) tells EBSCO*host* to write a cookie so that users do not have to key in authentication information every time they log in. The URL that should be used with Cookie authentication is **<http://search.ebscohost.com/login.aspx?authtype=cookie>**

[Athens authentication](#) is available for European customers with academic reference systems. The user is prompted for an Athens user name and password. The URL that should be used with Athens authentication is **<http://search.ebscohost.com/login.aspx?authtype=athens>**

[Shibboleth authentication](#) is also available. If you are using Shibboleth to authenticate your users, you must set up your Shibboleth affiliations. The URL that should be used with Shibboleth authentication is **<http://search.ebscohost.com/login.aspx?authtype=shib>**

[HTTPS authentication](#) enables users to keep the transmission of their searches and results confidential. HTTPS denies unauthorized users from viewing a customer's searches or results information. The library administrator enables HTTPS access at the profile level.

You may also combine different authentication types on a single login URL. When more than one authentication type is used, they will be recognized in the order listed.

For example, the following link will attempt to use the current IP address to authenticate, if not found it will proceed to look for an EBSCO*host* cookie, and then prompt for an ID and password if neither IP nor cookie is recognized: **<http://search.ebscohost.com/login.aspx?authtype=ip,cookie,uid>**