EBSCO's Upcoming Privacy and Security Enhancements

EBSCO is committed to ensuring the security and privacy of customer and end-user data. After making significant investments over the last few years, we are continuing with enhancements aligned to our goal of providing an optimal experience, meeting the privacy standards for all customers around the globe. These changes will allow users and customers to have the appropriate controls and protections while allowing us to provide a secure, safe and reliable research environment.

We are actively implementing a program to ensure full compliance with the enhanced European Union data protection legislation, the General Data Protection Regulation, when it comes into effect on May 25, 2018.

In 2018, EBSCO is upgrading our platform and services with the following enhancements:

- Implementing tools to enforce the use of strong passwords
- Transitioning our platforms to HTTPS (secure data transfer)
- Providing privacy controls for end users

Strong Passwords

When creating a new User ID and password combination, or updating the password for an existing User ID in EBSCOadmin, strong passwords will be required. Passwords will need to follow these guidelines:

- Include at least one number
- Include at least one special character (!, @, #, etc. A space is not a valid special character.)
- Password must be at least 6 characters
- Password cannot include your user ID
- Password cannot include any form or variation of the following words: ebsco, ehost, admin, dynamed and password

Note: These new guidelines will also apply to creating or updating passwords for Personal User accounts, My EBSCOhost Folders, and DynaMed Plus personal accounts.

Watch a short tutorial here: Creating Strong Passwords in EBSCOadmin

For more information, see:

- What are strong passwords in EBSCO products and interfaces?
- How do I set up User ID/Password Authentication?
Transition to HTTPS

Access points into EBSCO products will transition to HTTPS. HTTPS ensures that data exchanged between end-users and EBSCO is secure and the privacy of your end users and patrons is protected.

For customers who have not updated their institution's links to their EBSCO resources, a redirect will be in place to ensure access for end users.

In addition, HTTPS authentication should be enabled in EBSCOadmin. To learn how to enable HTTPS authentication, please see: Enabling HTTPS authentication in EBSCOadmin

Proxy Server Updates

Customers who utilize proxies to authenticate users will require acknowledgement of a SSL certificate. This should be worked out with the proxy vendor.

An SSL certificate purchased from a Certificate Signing Authority is recommended. While free self-signed certificates can be used, they will trigger a browser warning that end-users will have to acknowledge and choose to ignore before accessing EBSCO interfaces.

A certificate from a Certificate Signing Authority will allow end-users seamless access to EBSCO interfaces without a browser warning.

For more information, see the following page from OCLC's support site: https://www.oclc.org/support/services/ezproxy/documentation/cfg/ssl.en.html

To learn how to add your proxy server, please see: How do I add a Proxy Server in EBSCOadmin and embed it in my EBSCOhost URL?

Referring URL Updates

Referring URL authentication will require HTTPS in order to properly work with EBSCO URLs. This means any link that has been added to the Referring URL authentication page in EBSCOadmin must be a secure HTTPS link.

If you're using Referring URL and have not updated your URL in EBSCOadmin to a secure HTTPS link, your users will receive the following error message when trying to access EBSCO interfaces:

"We are unable to validate your login credentials. Please contact your institution for assistance. Please note, Referring URL authentication may have been prevented by antivirus or privacy control software. [Authentication Error Code 103]"

For more information, see:

• Referring URL Authentication - FAQs
Browser Requirements

Browsers that are not supported will have issues properly displaying elements of EBSCO interfaces. Ensure that your institution's browsers are running the most recent versions to prevent these issues.

Note: EBSCO uses Transport Layer Security (TLS) 1.2. TLS 1.2 is enabled in most browsers by default, but needs to be enabled in Internet Explorer 10.

To enable TLS 1.2 in IE 10:
1. Go to Settings in you Internet Explorer 10 browser.
2. Click Internet Options.
3. Click the Advanced tab.
4. Under the Security header, select the checkbox for "Use TLS 1.2".
5. Click OK.

For more information, see:
- Minimum Browser Requirements for EBSCO Interfaces

Privacy Controls

EBSCO will be enabling a set of privacy controls that will allow your end users and patrons to have control over their personal information, including the ability to remove that information from EBSCO's services at any time.

Any user creating a new personal account (My EBSCOhost Folder, Personal User Account, DynaMed Plus Personal User Account) will be provided privacy policy information and must give consent to complete the account creation process. Users with existing accounts will also be prompted to read the policy and provide consent the first time they log in after these new privacy controls become available.

Users who do not wish to provide consent to the privacy policy have the option to use the Forget Me option and have their account removed from EBSCO's system. Accounts that are removed are not recoverable.

Users can also request a report detailing their personal account activity within EBSCO products.

To learn more about creating a personal account, see: How to Create a My EBSCOhost Account