Transitioning to Secure Account Access – Passwords and HTTPS

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.

EBSCO will upgrade our platform and services with the following enhancements:

• Enforcing the use of strong passwords for EBSCO customer account access
• Transitioning our platforms to HTTPS (secure data transfer)

Strong Passwords

Beginning in late August 2018, all EBSCO customers using Username/Password for authentication will have an expiration date applied to their password. We will be notifying customers over the next few months, including contacts listed in EBSCOadmin as account administrators. If you need to verify your account contacts, please contact Customer Support.

This change follows the introduction in April of strong password requirements for accounts.

When creating a new User ID and password combination, or updating the password for an existing User ID in EBSCOadmin, strong passwords are required. Passwords must 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 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

EBSCO has made the decision to postpone the mandatory transition to HTTPS (version TLS 1.2), previously scheduled for July 2018. After the initial announcement, we received feedback that many customers needed more time to ensure their customized environments are properly supported through the transition. Customers of EBSCOhost and EBSCO Discovery Service can still opt to turn it on prior to the scheduled enforcement using EBSCOadmin. Additional details will be available later this year, prior to the transition deadline.

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 after the transition occurs.

Customers that would like to enable HTTPS for their products now can do so in EBSCOadmin. To learn how to enable HTTPS authentication, please see Enabling HTTPS authentication in EBSCOadmin.

Please note, the change to EBSCOadmin’s HTTPS tab should take place within 15 minutes. If these changes are not reflected in that time, the customer should navigate to the profile in EBSCOadmin for which they enabled HTTPS and click the View Changes on EBSCO link. Contact Support if changes are not updating. For the best experience, it is recommended that customers also update their links.

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?

Transport Layer Security

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.

Please note: EZproxy users must be running version 6.1 or higher in order to use TLS 1.2. Click here to find your EZproxy version.
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 your 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