Próximamente mejoras en la seguridad de contraseñas EBSCO

EBSCO se compromete a garantizar la seguridad y la privacidad de los datos del cliente y del usuario final. Después de realizar importantes inversiones en los últimos años continuamos con mejoras alineadas con nuestro objetivo de proporcionar una experiencia óptima, cumpliendo con los estándares de privacidad para todos los clientes de todo el mundo. Estos cambios permitirán a los usuarios y clientes contar con los controles y las protecciones adecuadas, al tiempo que nos permiten brindar un entorno de investigación seguro, confiable y confiable.

Estamos implementando activamente un programa para garantizar el cumplimiento de la legislación mejorada de protección de datos de la Unión Europea, el Reglamento General de Protección de Datos, cuando entre en vigor el 25 de mayo de 2018.

En 2018, EBSCO está actualizando nuestra plataforma y servicios con las siguientes mejoras:

- Implementar herramientas para hacer cumplir el uso de contraseñas seguras
- Transición de nuestras plataformas a HTTPS (transferencia segura de datos)
- Proporcionar controles de privacidad para los usuarios finales

Contraseñas seguras

Al crear una nueva combinación usuario y contraseña, o al actualizar la contraseña para un usuario existente en EBSCO*admin*, se requerirán contraseñas seguras. Las contraseñas deberán seguir estas pautas:

- Incluir al menos un número
- Incluir al menos un carácter especial (!, @, #, Etc. Un espacio no es un carácter especial válido.)
- La contraseña debe tener al menos 6 caracteres
- La contraseña no puede incluir su ID de usuario
- La contraseña no puede incluir ninguna forma o variación de las siguientes palabras: ebsco, ehost, admin, dynamed y contraseña

Nota: Estas nuevas pautas también se aplicarán a la creación o actualización de contraseñas para cuentas de usuario personal, My EBSCOhost Folders y cuentas personales de *DynaMed Plus.*

Transición a HTTPS

Los puntos de acceso a los productos de EBSCO pasarán a HTTPS en julio. HTTPS garantiza que los datos intercambiados entre los usuarios finales y EBSCO sean seguros y la privacidad de sus usuarios finales y usuarios esté protegida.

Para los clientes que no han actualizado los enlaces de su institución a sus recursos de EBSCO, se implementará una redirección para garantizar el acceso de los usuarios finales cuando ocurra la transición.

Además, la autenticación HTTPS debe estar habilitada en EBSCO*admin*. Para saber cómo habilitar la autenticación HTTPS:

1. Inicie sesión en EBSCO*admin* en http://eadmin.ebscohost.com.
2. Haga clic en la pestaña **Autenticación**, luego haga clic en la subpestaña **HTTPS**.
3. Ubique el perfil que desea habilitar y establezca el botón de opción en **Activado**.
4. Haga clic en **Enviar**. Cuando los usuarios inicien sesión, se dirigirán a una conexión segura.

Nota: Esta configuración puede tardar hasta 24 horas en aplicarse una vez que se haya habilitado.

Tenga en cuenta que si su institución decide habilitar HTTPS en EBSCOadmin antes de la transición de EBSCO, deberá actualizar sus enlaces a las interfaces de EBSCO para usar HTTPS. Si sus enlaces utilizan HTTP después de imponer HTTPS, los usuarios encontrarán problemas de diseño en las interfaces de EBSCO hasta que el redireccionamiento de HTTPS esté en su lugar.

Actualizaciones de Proxy Server

Los clientes que utilizan proxies para autenticar usuarios requerirán el reconocimiento de un certificado SSL. Esto debería resolverse con el proveedor de proxy.

Se **recomienda** un certificado SSL comprado a una Autoridad de Firma de Certificado. Si bien se pueden usar certificados autofirmados gratuitos, activarán una advertencia del navegador que los usuarios finales deberán reconocer y elegir ignorar antes de acceder a las interfaces de EBSCO.

Un certificado de una Autoridad de Firma de Certificado permitirá a los usuarios finales el acceso sin problemas a las interfaces de EBSCO sin una advertencia del navegador.

Para obtener más información, consulte la siguiente página del sitio de soporte de OCLC: https://www.oclc.org/support/services/ezproxy/documentation/cfg/ssl.en.html

Actualizaciones de URL de referencia

La autenticación URL de referencia requerirá HTTPS para funcionar correctamente con las URL de EBSCO. Esto significa que cualquier enlace que se haya agregado a la página de autenticación de la URL de referencia en EBSCO*admin* debe ser un enlace HTTPS seguro.

Si está utilizando la URL de referencia y no ha actualizado su URL en EBSCO*admin* a un enlace HTTPS seguro, sus usuarios recibirán el siguiente mensaje de error cuando intenten acceder a las interfaces de EBSCO:

"No podemos validar sus credenciales de inicio de sesión. Póngase en contacto con su institución para obtener asistencia. Tenga en cuenta que la autenticación URL de referencia puede haberse evitado con antivirus o software de control de privacidad. [Código de error de autenticación 103]"

Requisitos del navegador

Los navegadores que no son compatibles tendrán problemas para mostrar correctamente los elementos de las interfaces de EBSCO. Asegúrese de que los navegadores de su institución ejecuten las versiones más recientes para evitar estos problemas.

Nota: EBSCO usa Transport Layer Security (TLS) 1.2. TLS 1.2 está habilitado en la mayoría de los navegadores de forma predeterminada, pero debe estar habilitado en Internet Explorer 10.

Para habilitar TLS 1.2 en IE 10:

1. Vaya a **Configuración** en su navegador de Internet Explorer 10.
2. Haga clic en **Opciones de Internet.**
3. Haga clic en la **pestaña Avanzado**.
4. En el encabezado **Seguridad**, seleccione la casilla de verificación "**Usar TLS 1.2**".
5. Haga clic en **Aceptar**.

Controles de privacidad

EBSCO habilitará un conjunto de controles de privacidad que le permitirán a sus usuarios finales y usuarios tener control sobre su información personal, incluida la capacidad de eliminar esa información de los servicios de EBSCO en cualquier momento.

Cualquier usuario que cree una nueva cuenta personal (Mi carpeta EBSCOhost, Cuenta de usuario personal, Cuenta de usuario personal DynaMed Plus) recibirá información sobre la política de privacidad y deberá dar su consentimiento para completar el proceso de creación de la cuenta. A los usuarios con cuentas existentes también se les pedirá que lean la política y den su consentimiento la primera vez que inicien sesión después de que estén disponibles estos nuevos controles de privacidad.

Los usuarios que no desean dar su consentimiento a la política de privacidad tienen la opción de utilizar la opción **Olvidarme** y que su cuenta se elimine del sistema de EBSCO. Las cuentas que se eliminan no son recuperables.

Los usuarios también pueden solicitar un informe detallando la actividad de su cuenta personal dentro de los productos de EBSCO.

https://help.ebsco.com/interfaces/News_and_Alerts/Support_News/EBSCOs_Upcoming_Privacy_and_Security_Enhancements