Transport Security Layer (TLS) Support

Transport Layer Security (TLS) is a critical cryptographic protocol that provides authentication and data encryption between different endpoints (for example, the user's desktop and the application server) and secures HTTPS. To best safeguard this Web traffic, it is important to use current and more secure versions of the TLS protocol. The legacy TLS 1.0 and 1.1 versions, which date back to 1999, account for a very small percentage of Web traffic today, and various vulnerabilities (such as POODLE and DROWN) have been found in these legacy versions in recent years. TLS 1.2 was published in 2008 to address weaknesses in TLS 1.0 and 1.1 and has enjoyed wide adoption since then.

With the recent finalization of TLS 1.3 by the IETF in August 2018, Apple, Google, Microsoft, and Mozilla announced the end of support for TLS 1.0 and 1.1 in Chrome, Edge, IE, Firefox, and Safari. In line with these industry standards, Ex Libris deprecated TLS 1.0 and TLS 1.1 from web access on all production environments starting on May 2019. Therefore, any non-API inbound or outbound connections that rely on TLS 1.0 and TLS 1.1 will fail.

This change - together with similar actions from Microsoft, Apple, Google, and Mozilla - supports better performance, more secure connections, and helps advance a safer Web experience.

We understand that the security of your data is important, and we are committed to transparency about changes that may affect your use of the TLS service.

Ex Libris Higher Education Platform APIs TLS 1.0 and 1.1 deprecation

Ex Libris plans to continue removing security vulnerabilities and to align with industry standards by deprecating TLS 1.0 and 1.1 for the Higher Education Platform API. Starting in 2021 and continuing into 2022, Ex Libris will gradually allow only the use of TLS 1.2 for API. We recommend that when approaching technical support, you ask about potential APIs. Additional technical details can be found below.

Required Configurations for On-Premise/Local Systems

The user using the newest web browsers can use Alma, as today. Users with very old versions of web browsers cannot access Alma. They should upgrade to a later web browsers version, which supports TLS 1.2. See below for the list of supported browsers

Web pages or applications accessing Alma work if they support TLS 1.2. For example, the ILLiad (ILL system) hosted supports TLS 1.2. If there are web pages or applications that don't support TLS 1.2, they cannot integrate with Alma until they are updated to support TLS 1.2.

Ex Libris recommends that customers with on-premise/local systems follow their server vendor's instructions and disable TLS 1.0 and TLS 1.1.

For customers using load balancer, follow your vendor's instructions.

For customers using Apache SSL configuration, see Ex Libris best practice for TLS configuration in Apache.

A comprehensive list of clients that support TLS 1.2 can be found here: https://www.ssllabs.com/ssltest/clients.html.

Browser Support

The following table lists the date by which common internet browsers support TLS 1.2:

Bwoser	Support From
Internet Explorer	Version 11 (October 2013)
Edge	Version 12 (July 2015)
Firefox	Version 27 (February 2014)
Chrome	Version 30 (August 2013)
Safari	Version 7 (October 2013)

Source: https://caniuse.com/#feat=tls1-2.

To identify your browser, visit https://detectmybrowser.com/.

To test if your browser supports TLS 1.2, visit this link and look for the below message:

If you try to connect to Ex Libris using an incompatible browser, you will likely see one of the following messages:

- `ERR_SSL_VERSION_OR_CIPHER_MISMATCH`
- `SSL_ERROR_UNSUPPORTED_VERSION`
- `Cannot connect securely to this page`

Scripts and Integration

In addition to using Ex Libris products with a browser, many institutions maintain scripts, integration, and other software that connect to products on the Ex Libris Higher Education Platform using known standards that communicate via HTTPS. Such standards include the following:

- OAI
- SRU
- NCIP
- LTI

For example, you may use an ILL client that performs NCIP calls against Alma, a script to harvest metadata via OAI, or a tool that searches your Alma repository using SRU. To prevent an interruption in service, ensure that your scripts and software support TLS 1.2.

Testing

TLS 1.0/1 were disabled on all sandbox environments from July 7, 2019. Point your script or software to your Alma sandbox and ensure it works with TLS 1.2. If you receive an error regarding security, HTTPS, or TLS communication, your software may be written in a language or environment that does not support TLS 1.2. Contact your developer or vendor and request that the script or software be updated so that it uses a version of the underlying technology that supports TLS 1.2.

Development Environments

Below is a list of common development environments along with the minimum version requirements to support TLS 1.2:

Environment	Version
Java	Java 8 (1.8) To support TLS 1.2 with Java 7, use the **https.protocols Java system property for HttpsURLConnection.**
Python	2.7.9
.NET	.NET 4.6
Node	All recent versions, including 10.0 and above
Ruby	2.0.0, when used with OpenSSL 1.0.1 or higher. Check the version of OpenSSL used by your Ruby installation by running: `ruby -ropenssl -e 'puts OpenSSL::OPENSSL_LIBRARY_VERSION'`
PHP	Uses cURL- see below.
cURL	7.34.0 with OpenSSL 1.0.1 or higher

ILLiad

For those customers who use ILLiad for interlibrary loan automation in a hosted environment, OCLC has ensured that ILLiad will make requests from Alma using TLS 1.2. Customers using ILLiad in a locally hosted environment should follow these instructions:

For ILLiad 8.7, the framework did not support TLS 1.2 natively and some workarounds had to be added to make that possible: https://support.atlas-sys.com/hc/en-...Enable-TLS-1-2. This article covers changes to all .NET applications to enable TLS 1.2 support. OCLC recommend customers experiencing this behavior should be in the planning stages to update to ILLiad 9.0 as well since TLS 1.2 is enabled by default in ILLiad 9.0 and above.

Relias

Customers who use the Relais windows app are required to use the Relais portal instead. Relais windows does not support TLS 1.2. Relais portal integration with Alma was tested successfully using TLS 1.2. For more details, contact OCLC support.

INN-Reach

Customers who use INN-Reach for interlibrary loan automation are required to use IR 3.3 and above. The target release date for IR 3.3 is Dec 9, 2019. Versions before 3.3 do not support TLS 1.2. Customers are required to contact Innovative and coordinate the upgrade and reconfiguration.

Outbound Communication

Ex Libris systems make outbound calls to other systems. These outbound requests include the following:

- OAI and SRU to external repositories
- NCIP to external broker systems
- Alma Webhooks

To test your Webserver to ensure that it supports TLS 1.2, we recommend that you use the test page located at https://www.ssllabs.com/ssltest/. The SSL test page indicates if your Website supports TLS 1.2..

Additional Information

You can find additional information on TLS at:

- https://en.wikipedia.org/wiki/Transport_Layer_Security
- https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
- https://www.zdnet.com/article/chrome-edge-ie-firefox-and-safari-to-disable-tls-1-0-and-tls-1-1-in-2020/