Security Advisory- Deprecation of TLS 1.0 and TLS 1.1 Versions for Higher Education Platform API - Updated July 22, 2021

Overview

TLS is a cryptographic protocol that provides authentication and data encryption between different endpoints (for example, the user's desktop and the application server). Various vulnerabilities (such as POODLE and DROWN) have been found in TLS versions 1.0 and 1.1 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. In line with these industry standards, Ex Libris will deprecate TLS 1.0 and TLS 1.1.

This change - together with similar actions from Microsoft, Apple, Google, and Mozilla and many other vendors - support better performance and more secure connections.

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.

In order to avoid security vulnerabilities and to align with industry standards, Ex Libris will block TLS 1.0 and 1.1 traffic for it Higher Education Platform API in production environments and will support only TLS 1.2.

After Ex Libris deprecates TLS 1.0 and TLS 1.1, any Higher Education Platform API connections that rely on these protocols will fail.

TLS 1.0/1.1 Deprecation plan for API

The deprecation will be done gradually starting with the first region in October 2021 and concluded by May 2022.

Detailed plan can be found in Ex Libris Higher Education Platform API - deprecation of TLS 1.0 and TLS 1.1.

Affected Systems


See Ex Libris Transport Security Layer (TLS) Support for more details.

Additional Information

You can find additional information on TLS at:

Required Configurations for Hosted Systems

Ex Libris will deploy the required configuration to all Ex Libris cloud servers.

Required Configurations for On-Premise/Local Systems

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.

Record of Changes

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Document Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title:</td>
<td>Security Advisory- Deprecation of TLS 1.0 and TLS 1.1 Versions For Higher Education Platform</td>
</tr>
<tr>
<td>Document Owner:</td>
<td>Tomer Shemesh - Ex Libris Chief Information Security Officer (CISO)</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Barak Rozenblat – VP Cloud Services</td>
</tr>
<tr>
<td>Issued:</td>
<td>July 22, 2021</td>
</tr>
<tr>
<td>Reviewed &amp; Revised:</td>
<td>July 22, 2021</td>
</tr>
</tbody>
</table>

Revision Control

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Nature of Change</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial version</td>
<td>July 22, 2021</td>
</tr>
</tbody>
</table>