TLS encryption for CDN traffic in Optimizely

Skip Ahead

Performance and security
HSTS
PCI CDN
Ciphersuites
Opting out of TLS

THIS ARTICLE WILL HELP YOU:

• QA and debug experiments and campaigns
• Check goal firing with the network console

Optimizely uses Transport Layer Security (TLS) for 100% of its CDN traffic to protect against Man In The Middle attacks and meet customers’ compliance requirements. This article provides an overview of how Optimizely manages the security and performance aspects of TLS.

Performance and security

Optimizely acts to minimize the impact of TLS on both CPU and performance. For more details, visit istlsfastyet.com.

<table>
<thead>
<tr>
<th>Feature</th>
<th>TLS 1.3</th>
<th>TLS 1.2</th>
<th>D-TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>session identifiers</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>session tickets</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>OCSP stapling</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Dynamic</td>
<td>configurable</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>hijacking defense (ALPN)</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP/2</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>TLS 1.3</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Optimizely TLS encryption is highly secure, maintaining an A grade from SSL Labs.

HSTS

Optimizely’s CDN cdn.optimizely.com will send the HSTS header. This header will inform clients to connect to
cdn.optimizely.com over HTTPS regardless of whether it is using the http:// or https:// URL. Performance impact should be negligible, due to the TLS optimizations in use (described at https://istlsfastyet.com).

**PCI CDN**

Customers who have PCI-enabled accounts and load their assets from cdn-pci.optimizely.com have all of their assets served over TLS.

**Ciphersuites**

Ciphersuites are reviewed at least annually and updated to address security risks and meet PCI compliance requirements for TLS.

**Opting out of TLS**

Optimizely has an alternative CDN available at cdn-s-optional.optimizely.com for customers who wish to opt out of TLS. This domain will point to Optimizely’s same primary CDN but will not send the HSTS header. To transition to this CDN, change your //cdn.optimizely.com URLs to point to //cdn-s-optional.optimizely.com. Optimizely will commit to supporting this cdn-s-optional URL until at least April 30, 2019.

For information on how to change your cdn.optimizely.com URLs to cdn-s-optional, please see our Knowledge Base article on implementing the Optimizely snippet and change `<script src="//cdn.optimizely.com">` to `<script src="//cdn-s-optional.optimizely.com">`.

If you have any questions, please contact your CSM.