TLS 1.1 Retirement Guide

To ensure Moneris® maintains Payment Card Industry (PCI) compliance, **we will be retiring Transport Layer Security (TLS) protocol version 1.1 in May 2022**, as it no longer provides an adequate level of protection. In addition, most modern browsers currently support newer protocol versions, such as TLS 1.2 or higher. Below we have outlined background information, required next steps, as well as some helpful resources.

What is TLS?

TLS is a protocol that provides privacy and data integrity between two communicating applications. TLS is currently the most widely deployed security protocol, and is used for web browsers and other applications that require data to be securely exchanged over a network. TLS ensures a connection to a remote endpoint is the intended endpoint through encryption and endpoint identity verification.

What do you need to do?

To avoid business disruption and potential security threats, you are required to update your Production and QA environment to TLS 1.2 or higher before May 2022. Fortunately, updating can be as simple as recompiling the solution with updated libraries, or updating a config file.

If you have any questions or require further assistance, feel free to contact us via Moneris.com/Support/Contact.

Some helpful resources…

While TLS 1.2 can be configured in a web application, we also recommend requiring the web server to use a minimum security-level of TLS 1.2. A guide on how to do this can be found via the link here.

Browsers that support TLS 1.2 and TLS 1.3 are as follows:

- Microsoft Windows 10 using Microsoft Edge, Internet Explorer 11, or a current version of Firefox, or Chrome
- Microsoft Windows 8 using Internet Explorer 11 or later, or a current version of Firefox, or Chrome
- Mac OS X 11 or later using Safari 7 or later, or a current version of Firefox, or Chrome

Browser	TLS 1.2 Supported (Not enabled by default)	Enabled by default
Internet Explorer	Version 8	Version 11
Microsoft Edge	-	All Versions
Google Chrome	Version 29	Version 29
Mozilla Firefox	Version 23	Version 27
Apple Safari	Version 7	Version 7

Application framework support for TLS 1.2:

- For *Java*: We recommend *Java 8* or later. *Java 7* may be used but requires TLS 1.2 to be explicitly enabled by the application.
- For *.NET*: We recommend *.NET 4.6* or later. While *.NET 4.5* may be used, it requires TLS 1.2 to be explicitly enabled by the application. In addition, *.NET* depends on TLS 1.2 support by Windows (see chart above).
- For applications using *OpenSSL*: We recommend *OpenSSL 1.01* or later.

Validating requests

Listed below are two methods that can be used to determine which TLS version is being used:

1. **https://www.howsmyssl.com**: Provides you with an analysis in its response and does not require JavaScript processing for the result. Your response should be as follows:

   "Your client is using TLS 1.2, the most modern version of the encryption protocol. It gives you access to the fastest, most secure encryption possible on the web"

2. **SSL Labs**: Lists all available TLS versions and ciphers as a server or a client.

   Server: https://www.ssllabs.com/ssltest/analyze.html?d=account-d.docusign.com

   Client: https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html