FAQ and Instructions for Enabling TLS 1.2

1. **What is TLS**?
   Transport Layer Security (***TLS***) is a protocol that provides privacy and data integrity between two communicating applications. It's the most widely deployed security protocol in use today, and is used for Web browsers and other applications that require data to be securely exchanged over a network (including the Internet). The newest and most secure version of this protocol is 1.2.

2. **Why am I unable to connect to Online Banking (or a specific banking application)**?
   To align with the latest security recommendations, our online applications (including Merchant Capture and ACH Manager) will cease to function with any operating system or browser that does not support TLS 1.2. All newer versions of the major Internet browsers provide the option for using TLS 1.2.

3. **What operating systems and browsers support TLS 1.2**?
   Currently Windows XP and Vista can only upgrade to Internet Explorer 8, which does not support TLS 1.2. However, users of these operating systems can still install a newer version of Firefox, which does support TLS 1.2. Chrome no longer supports Windows XP as of April 2015. Windows 7 and above can support TLS 1.2.

Browser	Versions
Internet Explorer	9, 10 & 11
Chrome	41, 42, 43 and above
Firefox	36, 37, 38 and above
Opera	27, 28, 29 and above
Safari	7 & 8

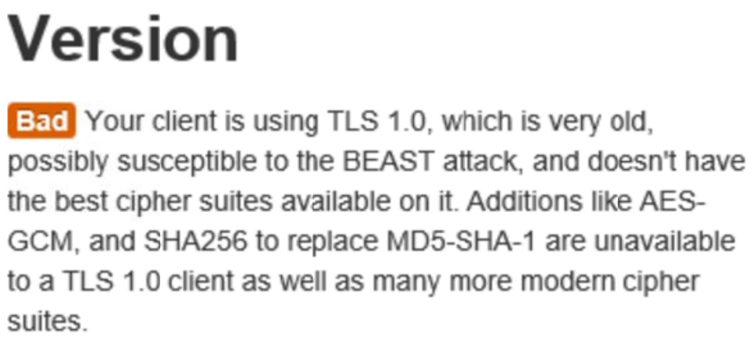
Testing for TLS 1.2 Compatibility

There is a web site that will test your browser's capability to utilize TLS 1.2. Link is below:

https://www.howsmyssl.com/

PLEASE NOTE: *Clicking the link above will result in leaving the Citizens 1st Bank web site. We are not responsible for the content on any external sites.*

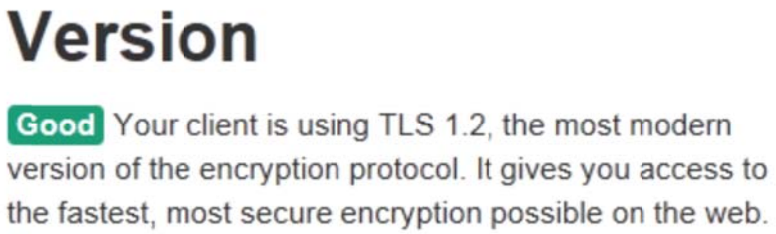
The test returns a lot of test results, but the test result to pay attention to is 'Version'. If it reports 'Bad' (Figure 1), it either means your browser does not support TLS 1.2, or it is not currently enabled (see below for instructions to enable on various browsers). If it reports 'Good'(Figure 2), your browser is up-to-date, and there is no further action needed.



Version

Bad Your client is using TLS 1.0, which is very old, possibly susceptible to the BEAST attack, and doesn't have the best cipher suites available on it. Additions like AES-GCM, and SHA256 to replace MD5-SHA-1 are unavailable to a TLS 1.0 client as well as many more modern cipher suites.

Figure 1 – Fail Result



Version

Good 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.

Figure 2 - Pass Result

If you are receiving a connection error when attempting to access any online application, it is possible that your browser is capable of using TLS 1.2, but it has been disabled. Use the section below to enable TLS 1.2 on supported browsers.

Internet Explorer:

1. Open Internet Explorer
2. Click 'Tools' and choose 'Internet Options'
3. Select the 'Advanced' tab
4. Scroll down to the 'Secuity' section
5. Ensure a checkmark is in the 'Use TLS 1.2' box
6. Press 'OK'.

Google Chrome:

1. Open Google Chrome
2. Click 'File' and choose 'Settings'
3. Scroll down and select 'Show advanced settings…'
4. Scroll to Network section and click on 'Change proxy settings…'
5. Select the 'Advanced' tab
6. Scroll down to 'Security' section
7. Ensure a checkmark is in the 'Use TLS 1.2' box
8. Press 'OK'

Firefox:

1. Open Firefox
2. Type in 'about:config' in the URL bar and press Enter
3. Scroll down to 'security.tls.version.max' and press Enter
4. Set the value to 3
5. Press 'OK'

Opera:

1. Open Opera
2. Click CTRL+F12
3. Click on 'Security'
4. Click on 'Security Protocols…'
5. Ensure a checkmark is in the 'Enable TLS 1.2'
6. Press 'OK' twice

Safari:

1. There are no options for enabling TLS. Any version of Safari 7 or greater has these protocols enabled by default