Frequently Asked Questions & Instructions for Enabling

1. **What exactly changed and how did that affect our members from connecting to Online Banking?**

   In an effort to provide the highest level of security for our members, we disabled connection to Online Banking from devices using any Transport Layer Security (TLS) less than 1.1. Any device that is not using TLS 1.1 or higher will not be able to connect to Online Banking. Today, all recent versions of the major internet browsers provide the option to use TLS 1.1 & higher.

2. **Exactly what browsers/versions will provide the option for TLS 1.1 and higher?**

   The Online Banking requirements document state that the previous three versions of the browsers listed below are certified and tested for use with Online Banking. Only the last two versions of the Safari browser are certified. These browser versions will support the option to use TLS 1.1 and higher, regardless of what operating system they are used on. Below is a list of the browsers and versions that are certified for use on our Online Banking and support TLS 1.1 & higher.

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

3. **Are there older versions of operating systems/ browser combinations that will not support TLS 1.1 & higher?**

   Yes. Windows XP and Windows Vista are only capable of upgrading up to Internet Explorer version 8. Therefore, users of these operating systems using Internet Explore as their browser will not be able to connect to our Online Banking. However, they would have the option of loading the latest version of another browser such as Chrome* or Firefox.

   *Chrome has announced that they will end new updates for Windows XP as of April 2015.

Enabling SSL Versions TLS 1.1 & TLS 1.2

Please select the browser that you are using to connect to NetBranch:

Internet Explorer:

1. Open Internet Explorer
2. Click Alt T and select “Internet Options”.
3. Select the "Advanced" tab.
4. Scroll down to the "Security" section.

5. Locate and check "Use TLS 1.1 and TLS 1.2".
6. Then, press the "OK" button.

Google Chrome:

1. Open Google Chrome
2. Click Alt F and select “Settings”.
3. Scroll down and select “Show advanced settings…”
4. Scroll down to the Network section and click on “Change proxy settings…”
5. Select the "Advanced" tab.
6. Scroll down to the "Security" section.
7. Locate and check "Use TLS 1.1 and TLS 1.2".
8. Then, press the "OK" button.

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. Then, press the "OK" button.

Opera:

1. Open Opera
2. Click Ctrl+F12
3. Click on “Security”
4. Click on “Security Protocols…”
5. Check on “Enable TLS 1.1 & TLS 1.2”
6. Press the "OK" button.
7. Then, press the "OK" button.

Safari:

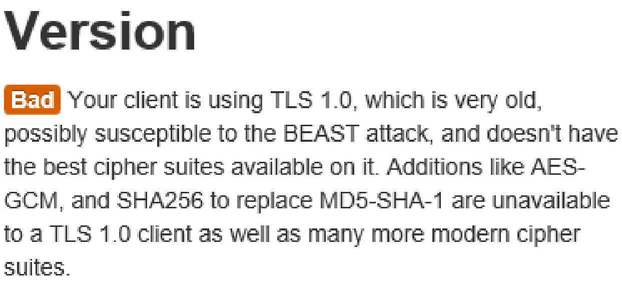
1. There are no options for enabling SSL protocols. If you are using Safari version 7 or greater, TLS 1.1 & 1.2 are automatically enabled.

Troubleshooting

The following steps will aid in determining the issue you may have with connecting to Online Banking as it relates to this change:

a) Check if TLS 1.1 & 1.2 has been enabled in your browser settings. Please see the attached document titled – ***Instructions for enabling TLS 1.1 & TLS 1.2*** for instructions on how to enable these options.

b) If these options are enabled and you still cannot connect, go to https://www.howsmyssl.com and verify what is showing in the Version section on this page. If you see verbiage similar to what is below and you verified that you have enabled the TLS 1.1 & TLS 1.2 options in the previous step, this could be an indication of an issue with your machine such as a virus or malware. You will need to troubleshoot whatever issue is causing your machine to not have the ability to make the appropriate changes.



Version

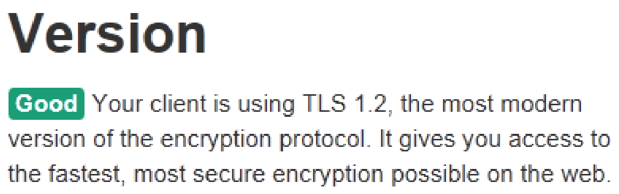
Bad Your client is using TLS 1.0, which is very old, possibly susceptible to the BEAST attack, and doesn't have the best cipher suites available on it. Additions like AES-GCM, and SHA256 to replace MD5-SHA-1 are unavailable to a TLS 1.0 client as well as many more modern cipher suites.

Until the "Version" listed when visiting https://www.howsmyssl.com reports "Good" you will be unable to connect to Online Banking from this machine.

Suggestions for troubleshooting may include:

- Check if you have current antivirus and/or malware protection
  1. If "yes" then verify the definitions are current and to run a scan. After any issues have been corrected, try https://www.howsmyssl.com" to verify if the version now shows "Good", if it does then proceed to verify they can access Online Banking.
  2. If "no" consider evaluating some of the programs available, some of which are free. Once current virus/malware scans have run and any issues have been corrected to try the site https://www.howsmyssl.com to verify if the version now shows "Good", if it does then proceed to verify if you can access Online Banking.
- You also may want to seek local computer repair, if necessary, to determine what is causing your computer to not report "good" even though they have TLS1.1 and TLS 1.2 options enabled

c) If the results of https://www.howsmyssl.com show that TLS 1.1 or 1.2 is enabled – similar to the verbiage below, and you still cannot connect to NetBranch, you will need to call Member Services at 791-7070 ext. 3503 for further research



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.

Problems connecting directly to Online Banking using your mobile device?

Online Banking is not certified for connecting to mobile devices. As stated in the Online Banking requirements document, the only devices certified for access to Online Banking are Windows and Apple/Macintosh PC’s and Laptops.