

Check Internet Browser Settings to Protect Yourself and Continue Access to BankNet – Security Upgrade

The OCC is implementing Transport Layer Security (TLS) 1.1 and 1.2 on BankNet since industry reports state that prior versions have been compromised. If you do not have TLS 1.1 or 1.2 enabled in your browser (see instructions below), you will not be able to access BankNet after September 2016. Although you will continue to have access to BankNet until September 2016 without making any changes, updating your settings now will provide better protection when you use the Internet.

TLS is a security protocol that enables private communication between Users and Web Servers. When the user and server communicate, TLS ensures that no one can eavesdrop or tamper with any of the communication.

To ensure you have the best protection and can access BankNet after September 2016, **configure Internet Explorer, Firefox, Chrome, Safari, or Opera to support TLS 1.1 and 1.2 by following the steps below. If you are using a web browser other than those listed here, consult the 'Help' for your web browser to enable TLS 1.1 and 1.2.**

FAQs and Troubleshooting Tips are contained at the end of this document.

Internet Explorer

To enable TLS 1.1 and 1.2 in Internet Explorer, perform the following steps:

1. Open Internet Explorer.
2. Click the **Tools** drop down menu on the toolbar.
3. Select **Internet Options** to open the Internet Options dialog window.
4. Click the **Advanced** tab at the top of the **Internet Options** dialog window.
5. Scroll down to the header labeled "**Security**".
6. In the **security** section, scroll down and check the box next to "**Use TLS 1.2**" and "**Use TLS 1.1**" to add both.
7. **(optional)** You may **deselect "Use TLS 1.0"** if your institution does not require it for other work you do.
8. Click both the **Apply** and **OK** button at the bottom of the dialog window to confirm the change.
9. Press the "**F5**" key to refresh your browser.

Mozilla Firefox (Two options)

A. To enable TLS 1.1 and 1.2 in **newer** versions of Firefox, perform the following steps:

1. Open FireFox
2. Type in "**about:config**" in the URL bar and press **Enter**
3. Scroll down to "**security.tls.version.max**", press **Enter**, and **set the value to "3"** (TLS 1.2)
4. Scroll down to "**security.tls.version.min**", press **Enter**, and **set the value to "2"** (TLS 1.1).
5. **(optional)** You may want to select a **minimum value of "1"** (TLS 1.0) in the prior step if your institution requires TLS 1.0 for other work you do.
6. Click "**OK**".

B. To enable TLS 1.1 and 1.2 in **older** versions of Firefox, perform the following steps:

1. Open the browser.
2. Click the **Tools** drop down menu
3. Select **Options** to open the Options dialog window.
4. Click the **Advanced** icon at the top of the **Options** dialog window.
5. Click the **Encryption** tab in the area of the window below the icons.
6. Check the box next to "Use TLS 1.2" and "Use TLS 1.1" under **Protocols** to add them.
7. **(optional)** You may **deselect "Use TLS 1.0"** if your institution does not require it for other work you do.
8. Click the **OK** button at the bottom of the dialog window to confirm the change.

Google Chrome:

To enable TLS 1.1 and 1.2 in Chrome, perform the following steps:

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 1.2**" and "**Use TLS 1.1**" to add them.
8. **(optional)** You may **deselect "Use TLS 1.0"** if your institution does not require it for other work you do.
9. Click the "**OK**" button.

Safari:

To enable TLS 1.1 and 1.2 in Safari, perform the following steps:

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

Opera:

To enable TLS 1.1 and 1.2 in Opera, perform the following steps:

1. Open Opera
2. Click **Ctrl+F12**
3. Click on "**Security**"
4. Click on "**Security Protocols...**".

5. Locate and check "Use TLS 1.2" and "Use TLS 1.1" to add them.
6. **(optional)** You may **deselect "Use TLS 1.0"** if your institution does not require it for other work you do.
7. Click the "OK" button.
8. Click the "OK" button.

Frequently Asked Questions & Instructions for Enabling

1. What exactly changed and how did that affect our users from connecting to BankNet?

In an effort to provide the highest level of security and because industry reports that prior versions of TLS have been compromised, as of September 2016, BankNet will no longer support devices with versions older than TLS 1.1. Any device that is not using TLS 1.1 or higher at that time will not be able to connect to BankNet. Today, all recent versions of the major internet browsers provide the option to use TLS 1.1 and 1.2.

2. Exactly what browsers/versions will provide the option for TLS 1.1 and 1.2?

| Browser | Versions |
|-------------------|--|
| ----- | ----- |
| Internet Explorer | 9 or higher |
| Chrome | 41 or higher |
| Firefox | 36 or higher |
| Opera | 27 or higher |
| Safari | 7 or higher; 5 or higher on Windows, iOS 9 |

3. Are there older versions of operating systems/ browser combinations that will not support TLS 1.1 and 1.2?

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 Explorer as their browser will not be able to connect to BankNet as of September 2016. However, they would have the option of loading the latest version of another browser such as Firefox or Chrome. Please note that Chrome ended new updates for Windows XP as of April 2015. In addition, Microsoft ended support for Internet Explorer version 8 in January 2016.

Troubleshooting

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

- a) Check if TLS 1.1 and 1.2 have been enabled in your browser settings. Please see the instructions at the top of this document.
- b) If these options are enabled and you still cannot connect, go to <https://www.howssmyssl.com> and check 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 and 1.2 option 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 the issue that is not allowing your machine to accept the TLS 1.1 and 1.2 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" (TLS 1.2 – Figure 1.1 below) or "Improvable" (TLS 1.1 – Figure 1.2 below) you will be unable to connect to BankNet.

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 1.1 – Using TLS 1.2

Note: If you are running TLS 1.1 and not 1.2 due to your institution's limitations, please note that instead of "Good" you will receive an "Improvable". Although this is not as secure as TLS 1.2, you can still connect to BankNet with TLS 1.1 even after September 2016.

Version

Improvable Your client is using TLS 1.1. It would be better to be TLS 1.2, but at least it isn't susceptible to the BEAST attack. But, it also doesn't have the AES-GCM cipher suite available.

[Learn More](#)

Figure 1.2 – Using TLS 1.1, but not TLS 1.2

Other Suggestions for Troubleshooting:

1. Check if you have current antivirus and/or malware protection.
 - a. 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" or "Improvable", if it does then try to log in BankNet again.
 - b. 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, try the site <https://www.howsmyssl.com> to verify if the version now shows "Good" or "Improvable", if it does then try to log in BankNet.

2. You also may want to seek local computer repair, if necessary, to determine what is not permitting your computer to report “Good” or “Improvable” even though the TLS 1.1 and 1.2 options are enabled.
3. If the results of <https://www.howssmyssl.com> show that TLS 1.1 and 1.2 are enabled – similar to the verbiage below, and you still cannot access BankNet, please call the BankNet helpdesk at 800-641-5925.

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.

Version

Improvable Your client is using TLS 1.1. It would be better to be TLS 1.2, but at least it isn't susceptible to the BEAST attack. But, it also doesn't have the AES-GCM cipher suite available.

[Learn More](#)