Announcement

Publication Date: February 7, 2018

Action Required: eCommerce Solutions – Enabling Transport Layer Security (TLS) 1.2

Overview:

As previously communicated, the disabling of TLS 1.0 and 1.1 is occurring so that we can maintain the highest standards for our data security and to align with the payment card industry data security standards (PCI DSS) and industry best practices.

TLS v1.0 and v1.1 are being discontinued due to security implications. The security standard that Fiserv employs has mandated the use of Transport Layer Security (TLS) v1.2 protocol for secure app communications versus previous versions. TLS is the layer that ensures that connection from the app to the platform is secure, encrypted and safe from attacks.

If your financial institution has not already done so, you will need to enable TLS 1.2 to access the following **eCommerce Solutions** without interruption before **Monday, April 9, 2018**.

Affects:

- Access Manager
- Business Online
- Retail Online

Note: All of your financial institution's users accessing Fiserv systems, including your customers with Business Online or Retail Online, who are on older Operating Systems (OS) versions or browsers that do not support TLS 1.2.

Effective: **April 9, 2018**

Action Required: We recommend that you add messaging to your Financial Institution's website to alert all your customers to the need for them to enable TLS 1.2.

Note: Do not instruct users to uncheck TLS 1.0 and 1.1, as access to other Fiserv solutions or third-party sites that have not yet enabled TLS 1.2 will be adversely affected.

To ensure your users that access the **affected** solutions do not experience unnecessary service interruptions, Fiserv recommends that

your organization complete and share the following steps with your users and customers **as soon as possible** in preparation for the TLS 1.2 effective date of **Monday, April 9, 2018**. For further guidance consult your internal technology partner, or Microsoft via https://support.microsoft.com.

Questions: If you have questions, please contact a member of the eCommerce Client Service team at (844) 650-4791, or submit a case through the Collaborative Care Center (C3).

For further compatibility questions, contact your specific vendor(s) for full details.

Table of Contents

About Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol that ensures that a connection to a remote endpoint is securely encrypted in order to provide privacy and data integrity. Fiserv web applications and application programming interface (API) connections use TLS as a key component of their security. TLS 1.2 is the most current version and is considered to be the most secure. TLS 1.0 and 1.1 are earlier, now less secure versions. The predecessor to TLS, Secure Sockets Layer (SSL), has been disabled in Fiserv Bank Solutions systems.

Enabling TLS 1.2

Fiserv Bank Solutions has enabled TLS 1.2 for most internal and all external web applications and API connections. Most user connections to Fiserv services currently are already using TLS 1.2. Browsers and operating systems that support TLS 1.2 will typically utilize it by default, preferring TLS 1.2 over older, less secure encryption protocols.

Fiserv is disabling the less secure TLS 1.0 and 1.1 encryption protocols across all applicable Fiserv Bank Solutions services. After this change, users accessing Fiserv Bank Solutions systems must use operating systems and browser versions that support TLS 1.2 and ensure that TLS 1.2 is enabled.

TLS Preparations

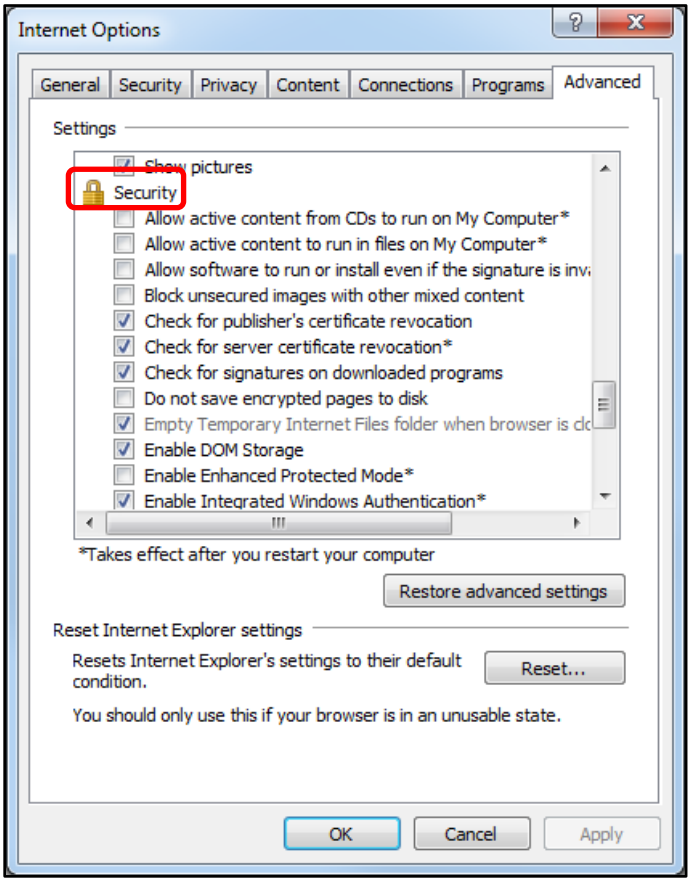
To prepare for this change, your institution will need to ensure that all users accessing Fiserv Bank Solutions services, including your customers, are using operating systems and browsers that support TLS 1.2. Below is a basic TLS 1.2 compatibility chart. Please contact your specific vendor(s) for full details.

Browsers and Operating Systems	TLS 1.2 Compatibility Notes
Microsoft Edge	Compatible by default
Microsoft IE Desktop and mobile version 11	Compatible by default
Microsoft IE Desktop versions 9 and 10	Capable when run in Windows 7 or newer, but not enabled by default
Firefox 27 and higher	Compatible by default
Google Chrome 38 and higher	Compatible by default

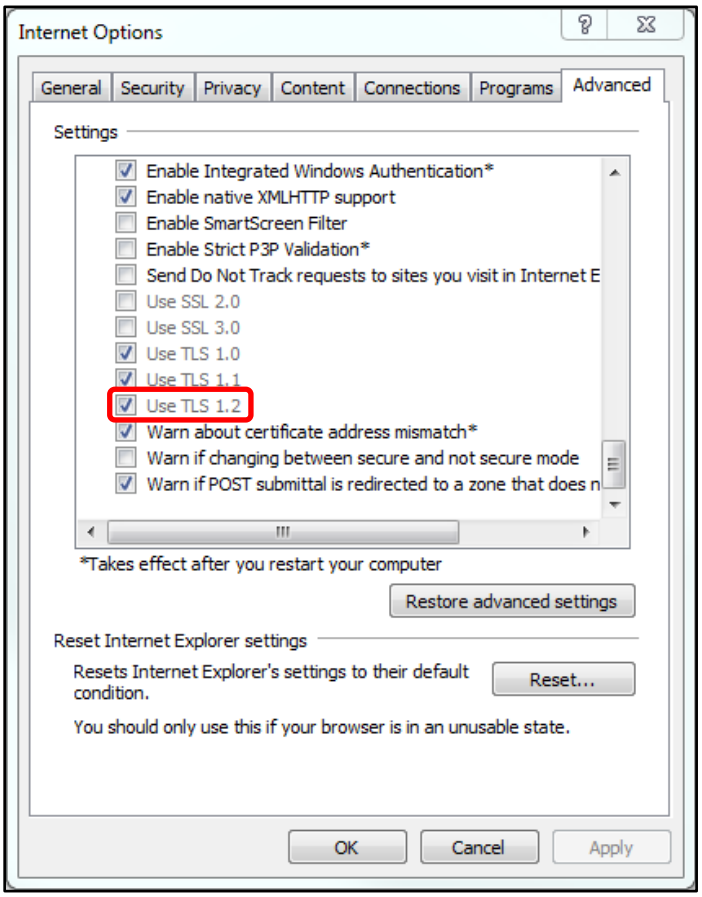
Oracle Java version 1.7 and higher	Compatible by default
Mobile Safari versions 5 and higher	Compatible by default
Microsoft Windows Server 2008 R2 and higher	Compatible by default
Microsoft Windows Server 2008 and below	Not compatible with TLS 1.2
Microsoft Windows 7, 8.0, 8.1 and 10	Compatible by default
Microsoft XP/Vista and below	Not compatible with TLS 1.2

How to Enable Transport Layer Security (TLS) 1.2

1. From your internet browser, select **Tools**, then **Internet Options**.
2. Click the **Advanced Tab**, and scroll down to Security section.



3. Ensure TLS 1.2 is checked, if not check **TLS 1.2** and select, **Apply**, **OK**.



Note: Do not instruct users to uncheck TLS 1.0 and 1.1, as access to other Fiserv solutions or third-party sites that have not yet enabled TLS 1.2 will be adversely affected.

Service Disruption

Fiserv clients are advised to start working toward ensuring support for TLS 1.2 in their Fiserv facing environments now. If applicable, notifications should be sent to your customers informing them of the pending change. Not supporting TLS 1.2 prior to Fiserv's disabling of TLS 1.0 and 1.1 will result in a disruption of service.