TLS 1.0 Notification

Apex no longer supporting TLS 1.0

Apex will no longer be supporting TLS version 1.0 for secure communications after September 1, 2017. In order to align with security industry best practices and changing regulatory requirements, this change will be made for all Apex's Internet facing web sites and systems. This article contains all of the information currently available on Apex's end of support for the TLS 1.0 encryption protocol.

What is TLS 1.0?

TLS stands for "Transport Layer Security." It is a protocol that provides privacy and data integrity between two communicating applications. It is the most widely deployed security protocol used today and is used for web browsers, FTP clients, and other applications that require data to be securely exchanged over a network. TLS ensures that a connection to a remote endpoint is the intended endpoint through encryption and endpoint identity verification. The versions of TLS, to date, are TLS 1.0, 1.1, and 1.2.

Client web browsers, FTP clients, and connection applications may use TLS as a component of their security.

Apex highly recommends the use of TLS 1.2 for all communications.

What is the change?

MyEasyView , MySecureBill, and Apex's FTP site is requiring an upgrade to TLS 1.1 or higher by September 1, 2017. On that date Apex will disable support for the TLS 1.0 encryption protocol, which will prevent customers from using it to access Apex services. This change is important to protect the security of our customer's data while they interact with our systems.

How will customers be impacted?

After Apex disables TLS 1.0, any inbound connections to or outbound connections from Apex that rely on TLS 1.0 will fail. This will impact a number of Apex services including access to websites including MyEasyView and MySecureBill and certain types of secure file transfers.

How can customers avoid a service disruption?

The action required by your organization will depend on which Apex systems are accessed and the method by which they are accessed.

Internet Browsers

You and your users will experience issues accessing Apex systems if you have disabled the supported encryption protocols or if a browser other than the **supported browsers** is being used to connect to MyEasyView or MySecureBill.

Test your browser compatibility

There are many websites that allow you to verify your browser's support for TLS protocol versions. Please contact your IT support for information regarding file transfer methods that may use TLS 1.0.

Example: https://www.ssllabs.com/ssltest/viewMyClient.html

Action required for browser compatibility

If you experience errors, you will need to ensure your browsers are compatible with TLS 1.1 or higher. If your browser is not compatible with TLS 1.1 or higher, after September 1, 2017, **your users will NOT be able to access Apex systems.** The minimum required action is to ensure TLS 1.1 or TLS1.2 are supported encryption protocols within your browser's security settings.

Supported Browsers

Microsoft Internet Explorer (IE)

Version 11

Versions 8, 9, and 10 when running Windows 7 or newer. TLS 1.1 must be manually enabled.

Microsoft Edge

Microsoft Firefox

Version 27 and higher

Versions 23 to 26 are compatible if configured

Google Chrome

Versions 38 and higher

Versions 22 to 37 are compatible running on Windows XP SP3, Vista, OS X10.6 or newer, Android 2.3 or newer

Google Android OS Browser

Android 5.0 and higher

Android 4.4 to 4.4.4 may be compatible

Apple Safari

Desktop Versions 7 and higher for OS X 10.9 and higher

Mobile versions 5 and higher for iOS5 and higher

Have questions or need help? Please contact us for immediate assistance.