RevSpring will discontinue support for older and less secure Internet Protocols. After March 31, 2020, RevSpring systems will no longer support TLS versions 1.0 and 1.1 for secure communications. In order to align with security industry best practices and changing regulatory requirements, this change will be made for some of RevSpring's internet facing websites and systems. This notice contains all of the information currently available on RevSpring's end of support for the TLS 1.0 and 1.1 encryption protocol.

What is TLS 1.0/1.1?

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 assures 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, 1.2 and 1.3.

Client web browsers, FTP clients, and connection applications may use TLS as a component of their security. RevSpring highly recommends the use of TLS 1.2 for all communications.

What is the change?

DataExpress View's portal site is requiring an upgrade to TLS 1.2 or higher by March 31, 2020. On that date, RevSpring will disable support for the TLS 1.0 and 1.1 encryption protocol, which will prevent customers from using it to access some RevSpring 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 RevSpring disables TLS 1.0 and 1.1., any inbound connections to, or outbound connections from RevSpring that rely on TLS 1.0 or 1.1 will fail. This will impact some RevSpring services including access to websites including DataExpress View, and certain types of secure file transfers.

How can customers avoid a service disruption?

The action required by your organization will depend on which method is used to access the system.

Internet browsers

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

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 or 1.1. 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 1.2 or higher. If your browser is not compatible with TLS 1.2 or higher, after March 31, 2020, your users will not be able to access RevSpring systems. The minimum required action is to ensure TLS 1.2 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 1.2 must be manually enabled and/or TLS 1.0 and TLS 1.1 must be manually disabled.
- 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

If you have additional questions, please contact us. Thank you for your ongoing partnership with RevSpring.