TLS Version Disablement

Deprecation of Older TLS Versions

Summary

With the upcoming deprecation of the TLS 1.1 protocol, it will be necessary to use an operating system and/or browser that have support for the TLS 1.2 (or higher) encryption protocol. This will be necessary for customers to connect to Simplifie hosted products or services. Simplifie will be deprecating this protocol beginning February 28, 2020.

Most Simplifie customers using modern browsers and operating systems will not be impacted. Only very old browsers and operating systems will be unable to make connections using the newer TLS protocols. Beginning February 28, 2020 it will be necessary to use an operating system and browser capable of connections using TLS 1.2 or higher.

- Security standards and industry best practice require that older TLS protocol versions (1.0 and 1.1) no longer be used for secure communications. Effective February 28, 2020, Simplifie will disable TLS 1.1 on our web servers. Our servers will refuse connections using TLS 1.1 beginning February 28, 2020.

- All customers and partners using the Simplifie applications and/or APIs should ensure that end users and API-calling systems support TLS 1.2 or higher by February 28, 2020 to avoid any disruption of service.

- If your end users or integration API broker/middleware relies on TLS 1.1, you are advised to disable it and transition to TLS 1.2 or higher. Any attempt to connect to our hosted applications or APIs with an operating system or browser that does not support TLS 1.2 or higher will experience a disruption in service.

How do I check if this will affect me?

- Please visit www.howsmyssl.com for more information. This site will provide a lot of information about the browser configuration including the highest version of TLS that is compatible. If all of your users browsers, that will be connecting to Simplifie hosted products or services, are reporting a TLS version of 1.2 or higher then you do not need to take any further action in relation to this communication.

What is the risk?

- Older TLS protocol versions (1.0 and 1.1) are vulnerable to man-in-the-middle attacks and intercepts, risking the integrity and authentication of data sent between a website and a browser. Disabling these older TLS versions at the server level is sufficient to mitigate this issue.

- Because Simplifie will end support for TLS 1.1 on February 28, 2020, all connections to our hosted properties using the protocol will not be accepted. End users and API users are strongly encouraged to configure their servers to support TLS 1.2 or higher before this date.

How can I fix this issue?

- Simplifie Integration or API hosted Web server administrators should disable TLS 1.1 and lower on their servers.
- End users should similarly use a browser with TLS 1.2 or higher enabled. NCSC guidelines for the selection, configuration, and use of TLS are available here: https://www.ncsc.gov.uk/guidance/tls-external-facing-services