To: Avaya Customers
From: Avaya Support Team
Date: February, 2020

Re: Impact of browser changes to Transport Layer Security (TLS 1.0 and 1.1) on Avaya Solutions

Dear Customers,

On October 15, 2018 all major web browser developers announced that they will stop using the standards TLS 1.0 and TLS 1.1 in 2020. This was in response to security standards organization (IETF) announcing that the older TLS standard did not allow for current encryption standards. The new standards are TLS 1.2 and 1.3.

The major browsers have now started to communicate how they will start moving to TLS 1.2. For example, starting with Google Chrome 79, Chrome will give sites a "not secure" label if TLS 1.0 and 1.1 is used. Starting with Google Chrome 81, Chrome will prevent connections to sites that use TLS 1.0 and TLS 1.1. The approach and timing to deprecating the older versions of TLS varies by each browser company.

Here are the links referencing the original announcements:

CHROME: https://security.googleblog.com/2018/10/modernizing-transport-security.html
APPLE: https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/
MICROSOFT: https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/
MOZILLA: https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/

This browser change affects a large number of sites and services, of which Avaya applications are some of the services affected. To see if you have Avaya product affected by the TLS change please reference Product Support Notices, PSN020444u and PSN005538u

https://downloads.avaya.com/css/P8/documents/101062983

https://downloads.avaya.com/css/P8/documents/101063983

Avaya's current software loads support TLS 1.2. Avaya recommends customers upgrade to a load which meets the new TLS 1.2 standards.

Most customers use browsers to access and administer their Avaya products. If you cannot upgrade impacted Avaya products ahead of the your browser moving to TLS 1.2, it is important to come up with a workaround to maintain browser access that will use TLS 1.0 or 1.1. Avaya recommends you work with your internal Security team to develop a solution which meets your own company's requirements.

The type, size and duration of your workaround solution to provide TLS 1.0 and 1.1 access, will vary depending on the number of users who need access to a browser that supports older TLS. It is recommended this workaround is sized to support not only Avaya solutions but other applications affected by this browser change.

Avaya is also implementing internally a solution in order to ensure we can continue to deliver services for customers with active support contracts for the duration of that contract, or until they move to an Avaya solution which supports TLS 1.2.

Sincerely,

Avaya Customer Service