STIBO SYSTEMS
MASTER DATA MANAGEMENT

Q&A Support for TLS version 1.3

- Is the change affecting both inbound and outbound traffic to/from STEP?
  - No, the change in supported TLS version is only for traffic inbound to STEP and only for HTTPS traffic. Outbound traffic from STEP is not affected.

- What type of algorithm is being used? Have we eliminated unnecessary ciphers in the frontend?
  - On TLSv1.2 we support:
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - On TLSv1.3 we support:
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384

- What would be the impact of this TLS version change where step is using 3rd party tools such as SFTP integrations?
  - The change affects only HTTPS traffic inbound to STEP. The change does not affect SFTP traffic.

- Do we need to force the use of this newer protocol by setting the configuration option Standalone.JVMArgs=mail.smtps.ssl.protocols=TLSv1.3?
  - Not relevant since you cannot send mail to STEP, and the change affects only HTTPS traffic inbound to STEP.

- What encryption (TLS 1.2 or TLS 1.3 or any other) is used by STIBO for the "https" endpoint for outbound configuration to deliver the file to Azure Data blob storage?
  - The question is irrelevant as the change only affects traffic inbound to STEP. Nevertheless, STEP will use TLSv1.3 for outbound traffic from STEP to Azure BLOB storage accounts.

- Do we need to do any pre or post deployment activity, Will there be any impact/ changes to the existing system. How will we be doing the upgrade and any downtime required for this activity?
  - The change involves no downtime on the STEP side. The customer must ensure their integration software or business applications supports TLSv1.3 when sending data to STEP over HTTPS.

- Where can I find more information or support document for TLS1.3?
  - Refer to external sources or search online for more detailed information and documentation on TLS 1.3.

- What is the impact to STEP if this recommendation is implemented. E.g. minimum client browser versions. Minimum TLS 1.3 and higher ciphers?
  - A client application such as a web-browser will select the highest protocol version that a server supports. STEP has started to support TLSv1.3, and the customer can verify if the browser supports TLSv1.3 by visiting a validation-page that Stibo has deployed. If the page is visible, it means the customers browsers supports TLSv1.3.
    https://tls-check.mdm.stibosystems.com/
    Information exists on the Internet telling what browser versions supports TLSv1.3.

- Which ELBSecurityPolicy supports TLS 1.3?
  - The question is irrelevant as the change affects only HTTPS traffic inbound to STEP and not outbound from STEP to a loadbalancer in AWS.