

How does PCI DSS Appendix A2 apply after the SSL/early TLS migration deadline?

PCI SSC FAQ | Article 1440 | August 2018

Prior to 30 June 2018, PCI DSS v3.2 Appendix A2 applied to all scenarios where SSL/early TLS was used as a security control to protect cardholder data or the cardholder data environment. As of 1 July 2018, SSL/early TLS may only be used as a security control by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect; Appendix A2 was updated to reflect this in PCI DSS v3.2.1.

While Appendix A2 identifies PCI DSS Requirements 2.2.3, 2.3, and 4.1 as examples of requirements directly affected by the use of SSL/early TLS, applicability of the Appendix is not limited to these three requirements. The impact to all requirements must be considered. For example; per Requirement 8.2.1, strong cryptography must be used to render all authentication credentials unreadable during transmission and storage on all system components. Since SSL/Early TLS does not constitute strong cryptography, it cannot be used to satisfy this requirement except as allowed by POS POI terminal connections.

After 30 June 2018, organizations using SSL/early TLS to meet any PCI DSS requirement, except as allowed by POS POIs and their termination points, must have compensating controls in place to mitigate the risks associated with using SSL/early TLS. Merchants and service providers using SSL/early TLS to meet a PCI DSS requirement for POS POI terminal connections should complete the applicable requirements in Appendix A2. Additionally, because SSL/early TLS is considered an insecure protocol, its allowed use through firewalls must be documented and approved, with security features documented and implemented, in accordance with Requirement 1.1.6. Similarly, the presence of SSL/Early TLS on a system component must be justified in accordance with documented configuration standards per Requirement 2.2.2. If SSL/early TLS is enabled but is not necessary for the function of the system, it must be disabled.

If SSL/early TLS is present but is not being used as a security control, Appendix A2 would not apply. However, the use of SSL/early TLS must still be documented and addressed in accordance with applicable requirements surrounding the presence of insecure protocols.

All organizations are strongly encouraged to replace SSL/early TLS with a strong cryptographic protocol as soon as possible.

Additional guidance can be found in the Information Supplements: Use of SSL/Early TLS and Impact on ASV Scans and Use of SSL/Early TLS for POS POI Terminal Connections, available in the PCI SSC Document Library.