

Amazon's "Require TLS" still delivers over protocols retired in 2021




Turning it on blocks plaintext. Email still ships over TLS 1.0 and 1.1 when the receiver offers them.

What we found

"Require TLS" confirms only that a TLS handshake completed, not which version it used.

So when a receiving server offers only TLS 1.0 or 1.1, Amazon SES delivers over that retired protocol. Federal guidance set TLS 1.2 as the minimum years ago, and the IETF retired 1.0 and 1.1 in 2021. The setting reads like a version guarantee. It is a yes-or-no check on whether any handshake completed.




What it means for buyers

-  **TLS 1.0 and 1.1 still deliver**
Both were retired across the industry in 2021. Amazon SES sends over them anyway.
-  **Below the TLS 1.2 standard**
Modern guidance sets TLS 1.2 as the minimum for protected data. SES dips beneath it.
-  **Only no-TLS is actually blocked**
"Require TLS" rejects a send only when the receiver offers no encryption at all.

WHY PAUBOX

100%

of outbound email encrypted by default, secured at TLS 1.2 or higher.

-  **TLS 1.2 enforced as a minimum**
Paubox sends only over modern, authenticated TLS, or to a patented Secure Message Center.
-  **No downgrade to old TLS**
Paubox never falls back to a retired protocol to force a delivery.
-  **HITRUST certified**
Annual third-party audit of every control.