PAUBOX

SECTION 01

SES documentation says one thing. SES does another.

The Amazon SES Developer Guide states the service requires TLS 1.2 and recommends TLS 1.3. The headers say otherwise.

What the SES docs say vs. what SES does

Even with "Require TLS" enabled, SES delivered email using TLS 1.0 and TLS 1.1, protocols retired in 2021.

WHAT THE SES DOCS SAY

Requires TLS 1.2.
Recommends TLS 1.3.

WHAT SES DOES (REQUIRE TLS ENABLED)

Delivers over TLS 1.1.
Delivers over TLS 1.0.

The Amazon SES Developer Guide is unambiguous about the requirement. "Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3," the guide reads.[1] The behavior recorded in our test headers tells a different story.

With the "Require TLS" configuration enabled, the setting AWS presents as its enforcement mechanism for outbound encryption, SES delivered email over TLS 1.1 when the receiver offered up to TLS 1.1, and over TLS 1.0 when the receiver offered up to TLS 1.0. The `Received` header on the recipient side captured each protocol version on its way through, leaving an audit trail that does not match the documented requirement.

Only one scenario actually triggered the protective behavior the setting's name implies. When the receiving server offered no TLS at all, SES bounced the message with a delivery failure notice. In every other case, even when the receiver only offered TLS 1.1 or TLS 1.0, SES still delivered the message, encrypted with whatever outdated version the receiver supported.

A setting called "Require TLS" implies a minimum acceptable version of TLS, the kind of guarantee a developer building a healthcare product reasonably expects when they enable it. What the headers actually show is a binary check on whether any TLS handshake completed, no matter how outdated the version negotiated.

The standards retired five years ago

IETF retired TLS 1.0 and 1.1 in 2021. Amazon SES still delivers over both.

IETF RFC 8996 deprecated TLS 1.0 and TLS 1.1 in March 2021, moving both protocols to "Historic" status, which is the standards body's classification for specifications that should no longer be used in production.[2]

The National Institute of Standards and Technology (NIST) reached the same conclusion. SP 800-52 Revision 2 requires TLS 1.2 as the minimum version for U.S. federal systems, and it required support for TLS 1.3 by January 1, 2024.[3]

That leaves Amazon SES in an awkward position as it is still sending over deprecated protocols.

The "Require TLS" configuration is named for what it implies, not for what it does. A developer building a healthcare product on SES would reasonably expect it to enforce the minimum the SES documentation describes in the same guide. The behavior recorded in the message headers does not match that expectation.

> "Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance."
>
> **IETF RFC 8996**
>
> Deprecating TLS 1.0 and TLS 1.1, March 2021[2]

PAUBOX

Secure every email you send and receive

Paubox combines healthcare compliance with AI to protect organizations from the most sophisticated attacks.

Talk to an expert