## Messaging, Malware and Mobile Anti-Abuse Working Group

# TLS for Mail: M³AAWG Baseline Recommendations

**Updated April 2026**
**Originally Published in 2014**

The reference URL for this document is m3aawg.org/TLSBaselineRecs2026

## Executive Summary

2010's global surveillance disclosures[1] and ongoing reports regarding pervasive monitoring of email traffic have increased public interest in the technical measures that providers can deploy to protect user mail from eavesdropping. In this document, M³AAWG recommends three basic measures that messaging providers can implement relatively quickly to enhance the security and privacy of their users' mail.

## Introduction

This document has been kept brief and simple, targeting "low-hanging fruit" that can be implemented relatively quickly. M³AAWG recognizes that a short document cannot explore all the implications of an area as complex as this one, but we feel there is a significant benefit in providing a recommended introductory approach. Additional technical documents that expand on these recommendations are available.

This document focuses on measures that messaging providers can deploy. It does not address additional end-user-controlled encryption options, such as the use of PGP/GPG or S/MIME for the privacy of message content, both in transit and at rest.

### 1) Protect mail flows between providers with Opportunistic TLS.

At this time, we recommend using only TLSv1.2 and TLSv1.3. Consistent with the IETF's published guidance in RFC 8996, we recommend disabling earlier versions such as SSLv3, TLSv1, and TLSv1.1 due to the known security issues impacting protocols.

By default, mail flows between providers are not encrypted and therefore are subject to both unauthorized monitoring and man-in-the-middle (MiTM) attacks. Both of these attacks can be prevented with the mandatory use of TLS based on a publicly trusted certificate.

While many aspects of certificate management have become easier over time, there is still some operational friction until the tools are fully integrated into your environment. Without universal TLS adoption, forced TLS is infeasible. However, most common Mail Transfer Agents (MTAs) can be instructed to attempt to negotiate Opportunistic TLS session encryption by employing ad-hoc,

[1] "2010's global surveillance disclosures," https://en.wikipedia.org/wiki/2010s_global_surveillance_disclosures

session-based keys to protect MTA-to-MTA flows from attacks on a best-effort basis, though they are still susceptible to MiTM attacks. Additionally, many MTAs now support DANE and MTA-STS, two protocols that further strengthen the TLS session encryption by protecting against downgrade and MiTM attacks. Site administrators should refer to their MTAs' documentation to understand how to set up STARTTLS using recent TLS versions/ciphers, and how to properly disable obsolete versions.

**M[3]AAWG strongly encourages all operators to enable Opportunistic TLS on all mail servers.**

One important limitation to note: SMTP is a hop-by-hop protocol, and since TLS works as part of a TCP connection that supports a direct SMTP session, opportunistic TLS also works on a hop-by-hop basis. If some hops in the message-delivery path deploy TLS but others do not, protection against eavesdropping will be correspondingly incomplete. There is also a risk of MiTM attacks due to the way Opportunistic TLS works. That said, while opportunistic TLS is not perfect, it will help protect at least some traffic from some passive attacks.

If you have already implemented opportunistic TLS on your mail servers, you can review the opportunistic TLS offered to your users along the mail flow by visiting a "TLS for SMTP" testing tool.[2]

M[3]AAWG specifically urges you to ensure that your mail server supports **only** modern versions of TLS from 1.2 to 1.3. Older versions, such as 0.9, 1.0, or 1.1, are considered obsolete and **do not** adequately protect data in transit.

**2) Protect intracompany network traffic from eavesdropping.**

Historically, internal provider network traffic over dedicated links was assumed to be secure and thus was not encrypted. Given what has been disclosed about the scale of pervasive network monitoring,[3] that assumption is no longer warranted. M[3]AAWG urges you to encrypt all traffic within your own network infrastructure, whether with TLS or alternative cryptographic methods, just as we are now recommending that you use opportunistic TLS to encrypt MTA-to-MTA messaging traffic flowing over the internet.

**3) Protect user credentials from eavesdropping (IMAPS/POPS/SMTP submission/web email interface).**

Moreover, when users provide their credentials to access their mailbox or to send a message, providers should use encryption to protect those credentials from interception, too. This includes using:

- IMAP (or POP) with TLS on ports 993 and 995, and/or STARTTLS on ports 143 and 110.
- Mail submission over port 465 with TLS and/or port 587 with STARTTLS.

[2] For example, SMTP TLS Checker (https://luxsci.com/smtp-tls-checker) or CheckTLS (https://www.checktls.com/TestReceiver). Both are free for non-commercial use.

[3] MUSCULAR (DS-200B), https://en.wikipedia.org/wiki/MUSCULAR;Carnivore, https://en.wikipedia.org/wiki/Carnivore_(software)

- Web email interface using https.

**4) Log TLS version and cipher data.**

M[3]AAWG additionally recommends that both senders and receivers log data related to the TLS version and cipher being used by a connected TLS session. They may also log data relating to failed connections, and that could be useful with TLSRPT reports. Detailed data could be useful in the short term, and aggregate data could be used to better display trends.

## Conclusion

The Messaging, Malware and Mobile Anti-Abuse Working Group recommends that industry messaging providers enable the basic encryption technologies in external and internal mail flows and user authentication as first-line defenses against eavesdropping on user messaging. These recommendations should be considered fundamental steps rather than comprehensive encryption guidance. More advanced topics on messaging security are covered in other M[3]AAWG documents. Recommendations and policies should be reviewed from time to time to ensure sites are adhering to best practices.

Note: Before making changes to existing configurations, IT managers should be aware of how changes may affect their users, especially those with older client software. While this document makes recommendations, real-world user data should influence those decisions.

## Related RFCs


- RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2," https://datatracker.ietf.org/doc/html/rfc5246
- RFC 7258: "Pervasive Monitoring Is an Attack," https://www.rfc-editor.org/rfc/rfc7258.html
- RFC 7672: " SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)," https://datatracker.ietf.org/doc/html/rfc7672
- RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3," https://datatracker.ietf.org/doc/html/rfc8446
- RFC 8460: "SMTP TLS Reporting," https://datatracker.ietf.org/doc/html/rfc8460
- RFC 8461: "SMTP MTA Strict Transport Security (MTA-STS)," https://datatracker.ietf.org/doc/html/rfc8461
- RFC 8996, "Deprecating TLS 1.0 and TLS 1.1," https://www.ietf.org/rfc/rfc8996.html


**Keywords:** Messaging, Malware and Mobile Anti-Abuse Working Group, M[3]AAWG, mail security, TLS, SMTP, network traffic security, user password security, opportunistic TLS, eavesdropping, pervasive monitoring, transport layer security

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates.