Government Digital Services Delivery

Secure Government Email TLS Deployment Guide

Issued by

Digital Services branch

Internal Affairs
Te Tari Taiwhenua

New Zealand Government

Contents

1. Document Control

Service Name	Secure Government Email
Author	Matt Oliver, Operations Security Specialist, Department of Internal Affairs
Title	Secure Government Email TLS Deployment Guide
Date and Version	2 February 2026, v1.0
Index Number	GDSD.SGE.Guidance.2026_043

2. Introduction

The Secure Government Email (SGE) Common Implementation Framework was confirmed late in 2024 with a goal to improve email security standards across the New Zealand Government. This deployment guide complements the Framework through providing guidance on the deployment of Transport Layer Security (TLS) in line with both the framework and to meet the requirements of the New Zealand Information Security Manual (NZISM).

Services are available for Agencies via the Secure Email Management and Administration service in Marketplace.

Marketplace | Pae Hokohoko — Infrastructure Managed Services catalogue

3. NZISM and SGE Framework requirements for TLS

Chapter 15.2 (Email Infrastructure) of the NZISM directs that Agencies SHOULD enable opportunistic TLS on servers that make incoming or outgoing email connections over public infrastructure. It also says Agencies SHOULD implement TLS between email servers where significant volumes of classified information are passed via email to other agencies.

The SGE Framework maps back to the NZISM but extends it further requiring a minimum of TLS1.2 on all email connections. It advises: TLS1.1, 1.0, SSL, no-TLS or sending unencrypted, must not be used.

Feedback through the Early Adopters Group identified strictly enforcing TLS on all email (Implicit TLS) would likely impact email flows. There are still several public organisations not using TLS, and some older system monitoring services also do not support TLS. To address this, the requirement has been further defined as applying to all email transmitted between Government organisations.

4. TLS Configuration Requirements

In most cases there are no specific actions required to achieve the framework's requirements for TLS. All of the major players in the email space support Opportunistic TLS by default. There is a separate guide for MTA-STS which provides a key control to enforce TLS.

4.1. Desktop to Desktop email

The vast majority of all Government Agencies are using Microsoft 365 or Microsoft Exchange for their Agency to Agency desktop email. In this scenario outbound email will prefer TLS1.3 by default and administrators do not need to do anything. TLS may negotiate version 1.3 or 1.2. While the sending server may have the ability to downgrade to sending in the clear, any SGE compliant destination will have MTA-STS enabled in enforce mode, preventing any possible downgrade to sending in the clear.

Recipient domain administrators should confirm they have MTA-STS enabled on their domains as per the Secure Government Email MTA-STS deployment guide.

Agencies using other email platforms need to review their services to determine how requirements will be met. For instance within Google you must configure TLS compliance rules in the Google Workspace Admin console to prevent downgrades to using TLS1.1 and 1.0.

4.2. External email sending services, including CRM platforms

All major players in the mass mail market support the use of TLS and it is generally enabled as opportunistic TLS by default. When sending from those services to a New Zealand Government organisation this is acceptable as once again the recipient domain should have MTA-STS enabled, preventing the downgrading of the connection to sending in the clear.

If your organisation uses a platform or service which does not support TLS on outbound email it is strongly recommended you engage with the supplier to find out why not, and when this will be resolved. TLS became a standard for email in 2002. A service incapable of supporting it 24 years later raises significant security concerns.

4.3. Legacy email sending systems

There are likely some legacy tools (typically system monitoring tools) used within Government which do not support TLS. Administrators of these services should review their use to determine if they are still needed, or if there is a path to upgrade the service to support TLS. Organisations need to carefully consider the data being transmitted over such a path to determine its confidentiality requirements. Again, consider “Would I be happy to have this information sent on the back of a postcard?”

Where legacy systems, which do not support TLS, send to destination domains with MTA-STS in enforced mode, there is no impact. Such a sending device will not check for the presence of an MTA-STS policy, so it will simply open a standard email SMTP session and send it in the clear.

4.4. Email between Government and public destinations

TLS is preferred on all communications, however these emails may revert back to sending in the clear (Opportunistic TLS). It is recommended email platform administrators review their TLS-RPT logs or TLS session logs to understand what email they are transmitting or receiving unencrypted. Consider if this information is suitable to be sent on the back of a postcard. If not, then it’s possible you may need to work with those organisations you are communicating with to determine the best solution. If it is your systems which do not support TLS, measures should be taken to address this. If an organisation is regularly sending you unencrypted email it might be a matter of working with them to determine why this is happening.

The risk is these emails could be silently intercepted with data harvested for later extortion attempts resulting in reputational damage or financial loss.

4.5. Classified email between Government Agencies

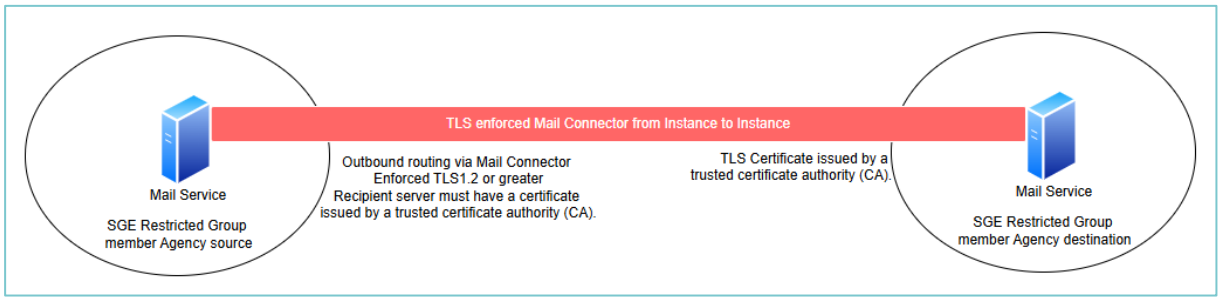
Implicit TLS is mandatory and enforced on all email between members of the SGE Restricted Group. Refer to the Secure Government Email Restricted Group Connectors Deployment Guide for details.

5. TLS mail flow scenarios

There are three sources and destinations for email in the context of this document. They are SGE Restricted Group member Agencies, other NZ Government organisations, and Public (or anything else). Some Agencies may have other custom configurations in place for other services, like custom mail connectors to partners. Those are not considered in this document and are not impacted by the security settings applied to the different flows.

This section references MTA-STS in several places. MTA-STS also provides destination verification ensuring email is reaching the right destination service. More information on how MTA-STS works and the required configuration is in the Secure Government Email MTA-STS Deployment Guide.

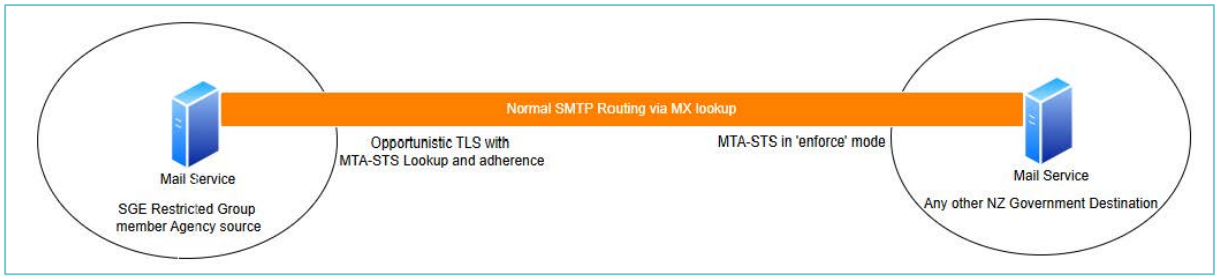
5.1. Email between two SGE Restricted Group members



Mail between two SGE Restricted Group members will route directly to the destination instance through Mail Connectors. The source service will not perform an MX lookup, and also will not perform any MTA-STS check. TLS security settings and restrictions on these connectors are applied and controlled entirely at the source. The source requires the destination to have a valid TLS certificate issued by a trusted CA. It also enforces TLS through the tunnel. Although it does not specify versions of TLS, all major providers support TLS1.2 and greater. At the time of writing no Agencies are using mail services who support TLS1.1 or 1.0. Should a destination Agency move to a service which does, part of their move will require the disabling of TLS1.1 and 1.0.

If the destination does not meet the security requirements as set on the connector by the sender the connector will not be established. SGE Restricted Group members should see the Secure Government Email MTA-STS Deployment Guide for more information.

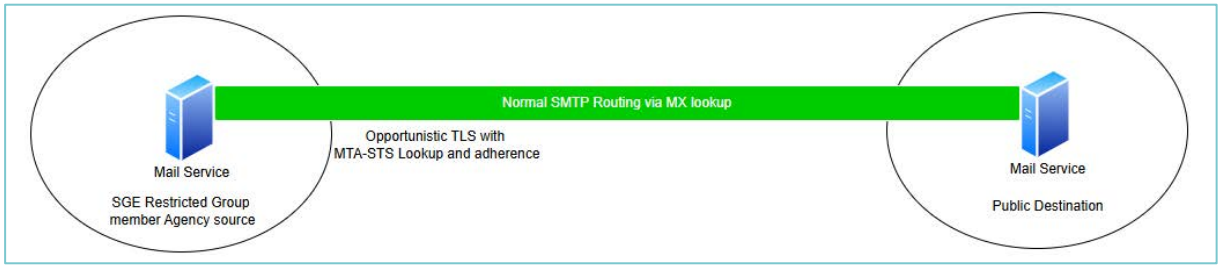
5.2. Email from SGE Restricted Group members to other NZ Government destinations



When an SGE Restricted Member sends mail to another NZ Government destination who is not a member of the SGE Restricted group, mail will route through a standard MX DNS lookup. Opportunistic TLS will be used and an MTA-STS lookup will be performed. The source will prefer to use TLS through opportunistic TLS, however the security demanding it is controlled by the destinations MTA-STS policy. The MTA-STS policy at the destination denies the downgrading of the connection to sending in the clear. The important distinction is the TLS security, in this instance, is controlled by the destination.

To force this to happen at the sender would require Implicit TLS be enabled generally, or the creation of an extremely complex set of rules covering all NZ Government destinations (which is way beyond just everything .govt.nz). Enabling Implicit TLS generally at the sender would likely impact other non-government destinations. See Appendix 1 for further information on the risk of enabling Implicit TLS.

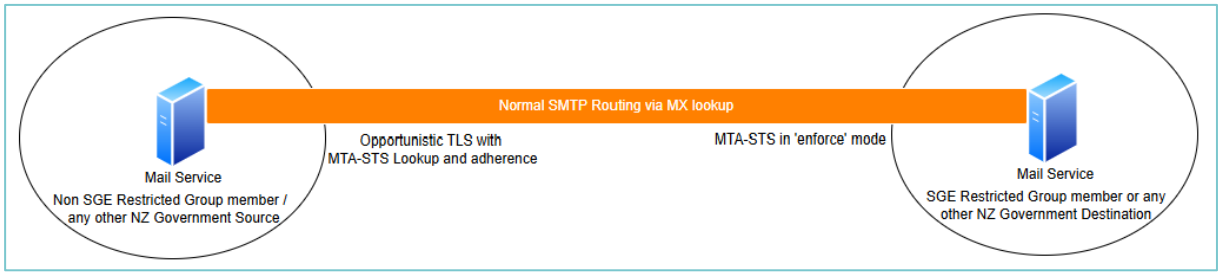
5.3. Email from SGE Restricted Group members to public destinations



Standard mail to any other destination will be routed via a standard MX DNS lookup. TLS is preferred through Opportunistic TLS, and an MTA-STS check will be performed. Any security enforcement is based on the destinations use of MTA-STS or they may have Implicit TLS enabled.

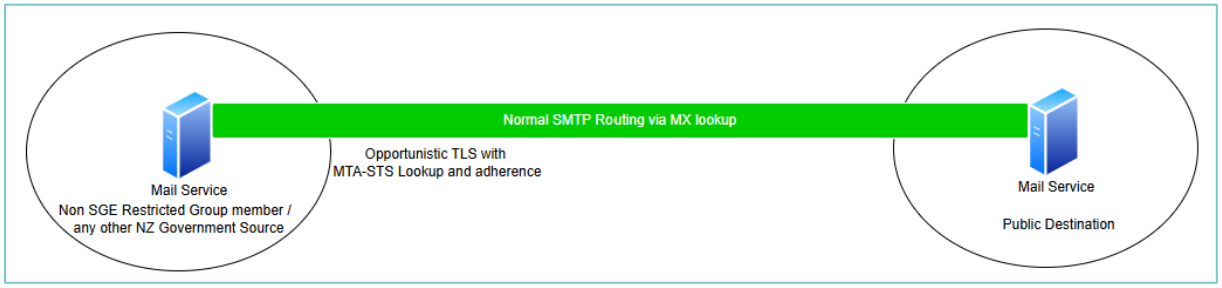
For mail coming from a public source to an SGE Restricted Group member, opportunistic TLS will be enabled and MTA-STS will be set to enforce mode. This means where the source supports TLS, it will be enforced by the MTA-STS policy at the destination preventing a downgrade to sending in the clear. If the public source does not support TLS an MTA-STS check will not be performed and the incoming connection will not be encrypted.

5.4. Email between other NZ Government organisations



Mail between New Zealand Government organisations who are not members of the SGE Restricted Group will be routed via a standard MX DNS lookup. The source service users opportunistic TLS to prefer TLS. The destination enforces TLS through the use of an MTA-STS policy set to enforce.

5.5. Email from NZ Government organisations to public destinations



Mail to any other destination will be routed via a standard MX DNS lookup. TLS is preferred through Opportunistic TLS, and an MTA-STS check will be performed. Any security enforcement is based on the destinations use of MTA-STS or they may have Implicit TLS enabled.

For mail coming from a public source to a Government organisation, opportunistic TLS will be enabled and MTA-STS will be set to enforce mode. This means where the source supports TLS, it will be enforced by the MTA-STS policy at the destination preventing a downgrade to sending in the clear. If the public source does not support TLS an MTA-STS check will not be performed and the incoming connection will not be encrypted.

Appendix 1: Possible impact of deploying Implicit TLS

Deploying Implicit TLS on all email could impact mail flows. It is estimated up to 6% of all email traffic remains processed by systems which do not support TLS. These systems are outliers, however we cannot reasonably deny using email as a communication method because systems outside of our control do not support it.

While the vast majority of all email services support TLS encryption today, it may be possible some external organisations are using email platforms which do not support encryption. Agencies will need to monitor their Mail Flow Reports to confirm if they are sending or receiving email via non-TLS channels.

At the time of writing:

- Microsoft do not support any lower version of TLS1.2 inbound or outbound via Exchange Online, however they do allow transmission of unencrypted email.
- Google prefer TLS1.3 and 1.2, however will also permit TLS1.1, 1.0 and sending in the clear.
- All major ISPs in New Zealand, and all major email service providers support a minimum of TLS1.2, though some may also support TLS1.0, 1.1, and unencrypted email.

Organisations communicating via email who do not support TLS1.2 are in the absolute minority, running on old email servers, which are likely unsupported. TLS1.2 became a standard in 2008, and even the 16 year old version of Microsoft Exchange 2010 (with SP3 & RU19) supports TLS1.2.

TLS1.0 and 1.1 were both deprecated under RFC 8996 with an end of life date of 23 March 2021.

Google reports approximately 2% of email being sent unencrypted, while Cloudflare report approximately 6%. Microsoft do not publicly share these email statistics.

It is recommended where Agencies platforms do not support TLS, or where clients' platforms do not support TLS, this be raised as a security risk, and options to secure the platforms be considered. Sending potentially private information without TLS encryption over the internet exposes that data to interception, inspection, or manipulation by any system or actor along the transmission path. Consider the question "Would you send this information on the back of a postcard?"

Appendix 2: List of Acronyms

Acronym	Definition
CA	Certificate Authority
DNS	Domain Name System
M365	Microsoft 365
MTA-STS	Mail Transfer Agent Strict Transport Security
MX	Mail Exchange
NZISM	New Zealand Information Services Manual
SGE	Secure Government Email (Framework)
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
TLS-RPT	Transport Layer Security Reporting