# All of Government

# Secure Government Email TLS Reporting (TLS-RPT) Deployment Guide

*Issued by*

*Digital Services branch*

Internal Affairs
Te Tari Taiwhenua

New Zealand Government

# Contents

1 Document Control ..... 3

2 Introduction ..... 3

3 NZISM and SGE Framework requirements for TLS-RPT ..... 3

4 TLS-RPT Configuration ..... 4

Appendix 1 – TLS-RPT Description ..... 6

Appendix 2 – Frequently asked Questions ..... 8

Appendix 3 – List of Acronyms ..... 9

# 1 Document Control

| | |
|---|---|
| **Service Name** | Secure Government Email |
| **Author** | Matt Oliver, Operations Security Specialist, Department of Internal Affairs |
| **Title** | Secure Government Email TLS Reporting Deployment Guide |
| **Date and Version** | 4 November 2025, v1.0 |
| **Index Number** | AoGSD.SGE.Guidance.2025_254 |

# 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 compliments the Framework through providing examples on how to deploy Transport Layer Security Reporting (TLS-RPT) in line with both the framework and to meet the requirements of the New Zealand Information Security Manual (NZISM).
It provides configuration examples covering commonly used platforms and configurations but is not an exhaustive guide. It is recommended Agencies without experience in the deployment of email security tools engage with a provider with expertise in this area.
Services are available for Agencies via the Secure Email Management and Administration service in Marketplace [Marketplace | Pae Hokohoko — Infrastructure Managed Services catalogue](Marketplace | Pae Hokohoko — Infrastructure Managed Services catalogue).

# 3 NZISM and SGE Framework requirements for TLS-RPT

Chapter 15.2 (Email Infrastructure) of the NZISM recommends TLS-RPT be configured.

The SGE Framework maps back to the NZISM but extends it further requiring “All email sending domains must have TLS Reporting enabled.”

# 4 TLS-RPT Configuration

Enabling TLS-RPT is very simple and comes with no risk to your normal mail flows. It is a reporting service only. TLS-RPT requires the addition of a DNS record for each of your mail enabled domains. Configuration will be similar across most DNS platforms. You need to:

1. Confirm the destination for TLS reports.
2. Construct your TLS-RPT record.
3. Publish the record in DNS.
4. Test the record.
5. Monitor the TLS-RPT Inbox or DMARC reporting service.

It is assumed you have the required access and knowledge to configure the required services.

**Step 1: Confirm the destination for the TLS Reports**

Most DMARC reporting services also support TLS-RPT, if yours does, this is the best place to send TLS reports to as they can integrate into your overall email security reporting providing easy access for investigations. The destination is a standard email address. EG: `tls-reports@minties.govt.nz`

**Step 2: Construct your TLS-RPT record**

There are really no options when building a TLS-RPT record. You must have a version number of 1 (v=TLSRPTv1). This version number is case sensitive, RFC8460 specifies it must exactly be v-TLSRPTv1.

The record name must be _smtp._tls.yourdomain

You must include a Reporting Address (RUA) for the report message to go to. You can have more than one reporting address.

The only other option is a percentage (pct) field for the percentage of reports to be sent. This is not widely supported and anything less than 100% means you will not get all the reports, possibly impacting troubleshooting.

For minties.govt.nz where the destination email address is tls-reports@minties.govt.nz, the TLS-RPT record will be:

Name: `_smtp._tls.minties.govt.nz`

Record: `"v=TLSRPTv1; rua=mailto:tls-reports@minties.govt.nz"`

**Step 3: Add TXT Records to your DNS**

The following assumes use of the Govt DNS platform, exact steps may vary for other platforms.

1. Log in to the DNS portal and browse to your domain.
2. Click on the Current tab under DNS Zones.
3. Click on Edit.
4. Click on the + symbol to add a new row.
5. Set the name to _smtp._tls
6. Set the TTL to 3600 (or whatever is required for your domain).
7. Change the type to TXT.

8. Copy and Paste the record created in step 2.
9. Add a comment or change number if needed for your environment.
10. Click on Publish.
11. Repeat this for other domains if required.

**Step 4: Test your TLS-RPT Record**

Once DNS records are published, use an external service to check your record is valid. Using a TXT record check on the MXToolbox supertool provides a useful test. (https://mxtoolbox.com/SuperTool.aspx#)

Enter _smtp._tls.yourdomain and select the TXT Record Lookup. This will return your TXT record. Confirm it is as you were expecting.

**Step 5: Monitor the TLS-RPT mailbox or DMARC reporting service**

After enabling the TLS-RPT record in DNS TLS-RPT is active. From then onwards you should receive reports of TLS connections. These reports will include both successful and failed TLS connections. This is where having them processed through a DMARC reporting service becomes most useful as in most instances you are only interesting in resolving failures.

# Appendix 1 – TLS-RPT Description

**What is TLS-RPT?**

TLS-RPT (Transport Layer Security Reporting), defined in RFC 8460, is an email security standard that allows domain owners to receive reports about STARTTLS negotiation failures when other mail servers try to send email to their domain.

Its purpose is to help domain owners:

- Monitor and troubleshoot TLS-related issues in email delivery.
- Ensure that email is being transmitted securely using STARTTLS.
- Detect misconfigurations, expired certificates, or downgrade attacks.

**How it works:**

When a TLS-RPT record is configured in DNS, sending mail servers which support TLS-RPT will check if the domain has published a valid _smtp._tls DNS record. If so it will:

- Attempt to deliver mail using STARTTLS (as usual).
- Log the outcome of the TLS negotiation (success or failure).
- Send a JSON format report to the rua address you specified in your TLS-RPT record.

TLS-RPT is passive — it doesn't influence whether TLS is used, but provides visibility into how TLS is performing when it is used.

**The TLS Report contains:**

- Sending server IP and domain,
- Receiving domain,
- TLS negotiation results, (success/failure)
- Failure reasons, (e.g., handshake error, certificate issue)
- Volume of affected messages.

**Sample TLS Report**

| Sending Domain | Sending IP | Connection Count | TLS Negotiated | Failure Type | Failure Reason |
|---|---|---|---|---|---|
| gmail.com | 209.85.220.41 | 120 | Yes | None | — |
| outlook.com | 40.107.12.55 | 85 | Yes | None | — |
| mail.example.org | 192.0.2.45 | 30 | No | STARTTLS Not Offered | Receiving server did not advertise STARTTLS |
| smtp.badmail.net | 203.0.113.77 | 15 | No | TLS Handshake Failure | Certificate expired |
| relay.testmail.io | 198.51.100.23 | 50 | Yes | None | — |

| | | | | | |
|---|---|---|---|---|---|
| sendgrid.net | 149.72.212.101 | 60 | No | Downgrade Attack Suspected | STARTTLS stripped during negotiation |

# Appendix 2 – Frequently asked Questions

**What happens if the sending server does not support TLS-RPT?**

No reports will be sent from that server.

The most likely scenario is the sending server does not support TLS at all, so there will not be any initiation of the STARTTLS SMTP extensions. In this case the sending server will attempt to connect via an unencrypted SMTP connection. This connection attempt will not be visible via any TLS reporting console, as no reports will be generated.

**Does TLS-RPT enforce encryption?**

No. TLS-RPT is purely a reporting mechanism. It does not enforce encryption or block messages. It simply provides visibility into whether TLS was successfully negotiated.

**How often are TLS-RPT reports sent?**

Reports are usually sent daily, depending on the sending server's implementation and volume of email traffic.

**Do all email providers support TLS-RPT?**

No. Only some major providers (e.g., Gmail, Microsoft, Yahoo) currently support TLS-RPT. Adoption is growing but not universal.

**How does TLS-RPT relate to DMARC and MTA-STS?**

- DMARC: Focuses on authentication (SPF/DKIM).
- MTA-STS: Enforces TLS for SMTP.
- TLS-RPT: Reports on TLS negotiation outcomes.

Together, they form a layered approach to email security.

# Appendix 3 – List of Acronyms

| Acronym | Definition |
|---|---|
| **DKIM** | Domain Keys Identified Mail |
| **DMARC** | Domain-based Message Authentication, Reporting, and Conformance |
| **DNS** | Domain Name System |
| **JSON** | JavaScript Object Notation |
| **NZISM** | New Zealand Information Services Manual |
| **RUA** | Reporting URI for Aggregate data |
| **SGE** | Secure Government Email (Framework) |
| **SMTP** | Simple Mail Transfer Protocol |
| **STARTTLS** | Start Transport Layer Security |
| **TLS** | Transport Layer Security |
| **TLS-RPT** | Transport Layer Security Reporting |