

This document is provided for your information only, on non-reliance basis and without any representations or warranties (express or implied) that these instructions will be suitable for your mailbox.

TLS for Email Transport

Purpose. TLS encrypts the connection between email systems while a message is in transit. Both sides must support a secure SMTP connection for TLS to work.

Guide 1. Public Email Services

For users of Gmail, Outlook.com, iCloud Mail, Yahoo Mail, Proton Mail, and other external email services.

What to do

1. Use the provider's official website or current email application and keep it updated.
2. When configuring an email client manually, select a TLS/SSL-secured connection for sending and receiving email.
3. Do not disable certificate validation or accept warnings about an untrusted certificate.
4. If the service reports that secure delivery is unavailable, contact its support team. You do not need to install a server certificate on the user's computer.

How to check

Open the test service: [CheckTLS TestReceiver](#)

1. Enter your full email address in the eMail Target field.
2. Keep the Output Level set to Detail and click Run Test. The service checks the receiving MX servers without sending a message.
3. Confirm that the servers support STARTTLS, establish a TLS connection, and report no certificate errors.

Expected result

- All tested MX servers establish a TLS connection.
- The report shows no certificate errors, and the Score in the test table is 90 or higher.

Guide 2. Corporate Email Server

For organizations that receive or send email through their own SMTP servers and gateways.

What is required

- Public DNS names of the email servers and administrative access to the servers, DNS, and firewall.
- A TLS certificate from a publicly trusted certificate authority, its private key, and the complete certificate chain.

Implementation

1. Identify the public DNS names of all MX servers and SMTP gateways and confirm that port 25 is reachable.
2. Obtain a certificate covering these names from a publicly trusted certificate authority.
3. Install the certificate, private key, and complete chain on every server; enable STARTTLS for SMTP on port 25.
4. Allow TLS 1.2 and TLS 1.3 and disable obsolete protocols. If encryption is mandatory, enable Required TLS without fallback to plaintext.

Important. Store the private key only on trusted servers. Do not send it by email, and restrict file access at the operating-system level.

How to check

Open the test service: [CheckTLS TestReceiver](#)

1. Enter a full email address in the corporate domain in the eMail Target field.
2. Keep the Output Level set to Detail and click Run Test. If the organization uses several domains, repeat the test for each domain.
3. Confirm that every row in the MX Matrix passes STARTTLS and reports no certificate errors.

Expected result

- All published MX servers establish a TLS connection.
- The report shows no certificate errors, and the Score in the test table is 90 or higher.