TECHNICAL PAPER

Configuring TLS in MailSite 11

A guide for MailSite Administrators

A MailSite Technical White Paper

November 2026

© 2026 Rockliffe Systems, Inc. All rights reserved. MailSite is a registered trademark of Rockliffe Systems, Inc. All other trademarks are the property of their respective owners.

Contents

1 Introduction 2
2 Prerequisites 3
2.1 Host Names and DNS 3
2.2 Checking an Existing Certificate 3
2.3 How MailSite Chooses a Certificate 3
3 Getting Certificates 4
3.1 Requesting a Certificate from Let’s Encrypt 4
3.2 Using a Certificate from Another Provider 4
3.3 Using the Windows Certificate Store 5
3.4 Protecting Private Keys 5
4 Verifying the Certificate 6
4.1 In the Console 6
4.2 From Outside Your Network 6
5 Setting the TLS Policy 7
5.1 Receiving SMTP, POP3 and IMAP4 7
5.2 Sending SMTP 7
5.3 Web and Exchange Connections 8
6 Verifying MailSite 9
7 References 10
7.1 Disclaimer 10
7.2 Assistance 10

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

1 Introduction

MailSite provides secure messaging with Transport Layer Security (TLS). TLS encrypts the connection between a mail app and your server, and between your server and other mail servers. It also lets the app check that it is talking to your server, using a certificate and public key cryptography.

Security best practice recommends against SSL, TLS 1.0 and TLS 1.1 because of known weaknesses, and recommends modern cipher suites. With MailSite 10, meeting that advice meant changing the Windows registry, often with third-party tools, and setting a matching cipher list for MailSite.

MailSite 11 handles TLS itself, so none of that is needed:

- It offers only TLS 1.2 and TLS 1.3. SSL, TLS 1.0 and TLS 1.1 are never offered, whatever Windows allows.
- It chooses modern cipher suites itself. There is no cipher list to maintain and no registry setting to change.
- It picks the certificate that matches the host name the client asks for, so one server can present the right certificate for each domain it hosts.
- It can request and renew certificates from Let’s Encrypt for each domain.
- A new or renewed certificate is used within about a minute, without restarting any service.

This paper describes how to give MailSite the certificates it needs, how to set the TLS policy for each mail protocol and how to check the result. Familiarity with Windows Server administration and with DNS is assumed.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

2 Prerequisites

Before you configure TLS, plan the host names that people and other mail servers will use to reach MailSite.

2.1 Host Names and DNS

A certificate must cover the host name the client uses, and it must chain to an issuer the client trusts. Decide on:

- The server's public name, for example `mail.yourcorp.com`. Set it in the Console under Server Properties.
- The MX host names of each domain, which other mail servers use to deliver mail to you.
- `autodiscover.<domain>` for each domain, which Outlook and other apps use to find their settings.

Each name must resolve in public DNS to your MailSite server. To use Let's Encrypt certificates, port 80 must also be reachable from the internet, so that Let's Encrypt can confirm that you control each name.

2.2 Checking an Existing Certificate

MailSite loads certificates from two places:

- **MailSite's Certs folder**, under the installation directory. Each certificate is a `.chain.pem` file with its private key in a matching `.key.pem` file. Certificates that MailSite requests are stored here.
- **The Windows certificate store.** A certificate there is used for any name that has no certificate file in the Certs folder. This keeps the certificates of a server upgraded from MailSite 10 working.

A certificate file takes precedence over the Windows store for the names it covers. To see which certificate a domain is using, open the domain's Certificates dialog in the Console and choose Active Certificate (see section 3).

2.3 How MailSite Chooses a Certificate

MailSite 10 looked up the reverse DNS name of the server's IP address and searched the Windows certificate store for a certificate with that name. MailSite 11 no longer does this. Each connection gets the certificate for the host name the client asks for. There is no HOSTS file or reverse DNS setting to change, and one server can hold certificates for many domains.

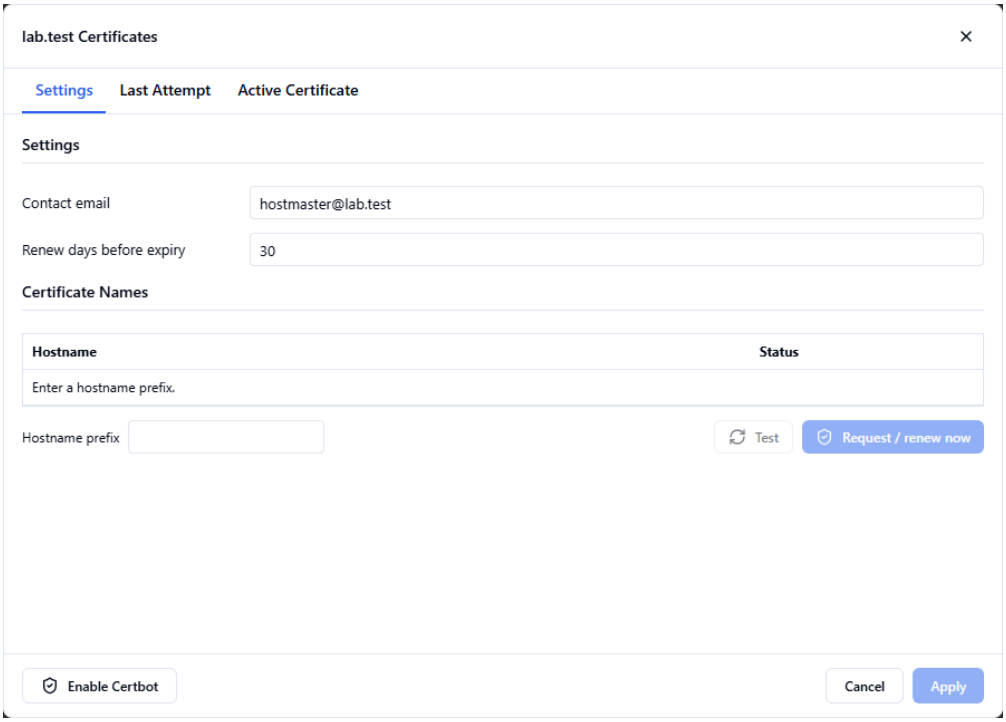
© 2026 Rockliffe Systems, Inc. · www.mailsite.com

3 Getting Certificates

3.1 Requesting a Certificate from Let's Encrypt

MailSite can request and renew a certificate for each domain from Let's Encrypt. A domain created in MailSite 11.1 or later, including the default domain of a new installation, starts with this turned on. So do domains copied from MailSite 10 at the first upgrade.

1. In the Console, expand Domains, select the domain and open Certificates.
2. On the Settings tab, enter the Contact email and the number of days before expiry to renew.
3. Leave Hostname prefix empty to let MailSite choose the names itself each time it requests: the server's public name, the domain's MX hosts and `autodiscover.<domain>`, for the domain and each synonym. A name that already has a valid certificate from a file or the Windows store is left alone. To choose the names yourself, enter a prefix; the certificate then names `<prefix>.<domain>` and `autodiscover.<domain>`.
4. Choose Test to check every name. Each must resolve to your server, and port 80 must reach the server from the internet. Fix any failed check before you request.
5. Make sure Certbot is enabled, apply the settings, then choose Request / renew now.



When no name passes the check, MailSite does not contact Let's Encrypt and tries again once a day. Certificate issuance is an external operation: follow the result the Console shows rather than repeating the same request.

3.2 Using a Certificate from Another Provider

You can also use a certificate from another certificate authority. Place its certificate chain and its private key in MailSite's Certs folder as a `.chain.pem` and a matching `.key.pem` file. MailSite starts using it within about a minute.

If the key file is incomplete or does not match, MailSite keeps serving the certificate it had for those names until the pair can be read.

3.3 Using the Windows Certificate Store

A certificate installed in the Windows certificate store is still used for names that have no certificate file. It is loaded when the MailSite services next start, or at the next change in the Certs folder.

For a customized deployment, settings in the services' environment can change where certificates come from: `TLS_SOURCE=win_store` uses only the Windows store, `TLS_CERT_DIR` names another certificate folder, and `TLS_CERT_PATH` with `TLS_KEY_PATH` names one certificate and its key. Set these for the MailSite services, not just in an interactive shell, and check the service logs after a change.

3.4 Protecting Private Keys

Restrict access to private keys to the accounts that need them. Include the Certs folder and its permissions in your backup. Never copy a private key into a support request.

In a cluster, each server loads certificates from its own Certs folder. A certificate that MailSite requests is saved on the server that made the request, so copy it to the other servers.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

4 Verifying the Certificate

4.1 In the Console

Open the domain's Certificates dialog:

- **Active Certificate** shows the certificate in use: its subject, issuer, DNS names, expiry and thumbprint.
- **Last Attempt** shows the account registration, validation type, expiry, next renewal, thumbprint and the result of the most recent request. If a request fails, read this tab and the HTTPMA log.

Keep port 80 reachable so that later renewals succeed. Include certificate expiry and renewal results in your routine checks.

4.2 From Outside Your Network

A certificate file on disk does not prove that the running services use it. Connect from a real client outside your network, using the host name your users use. A connection from the server itself does not prove that DNS, the firewall or the certificate names are right.

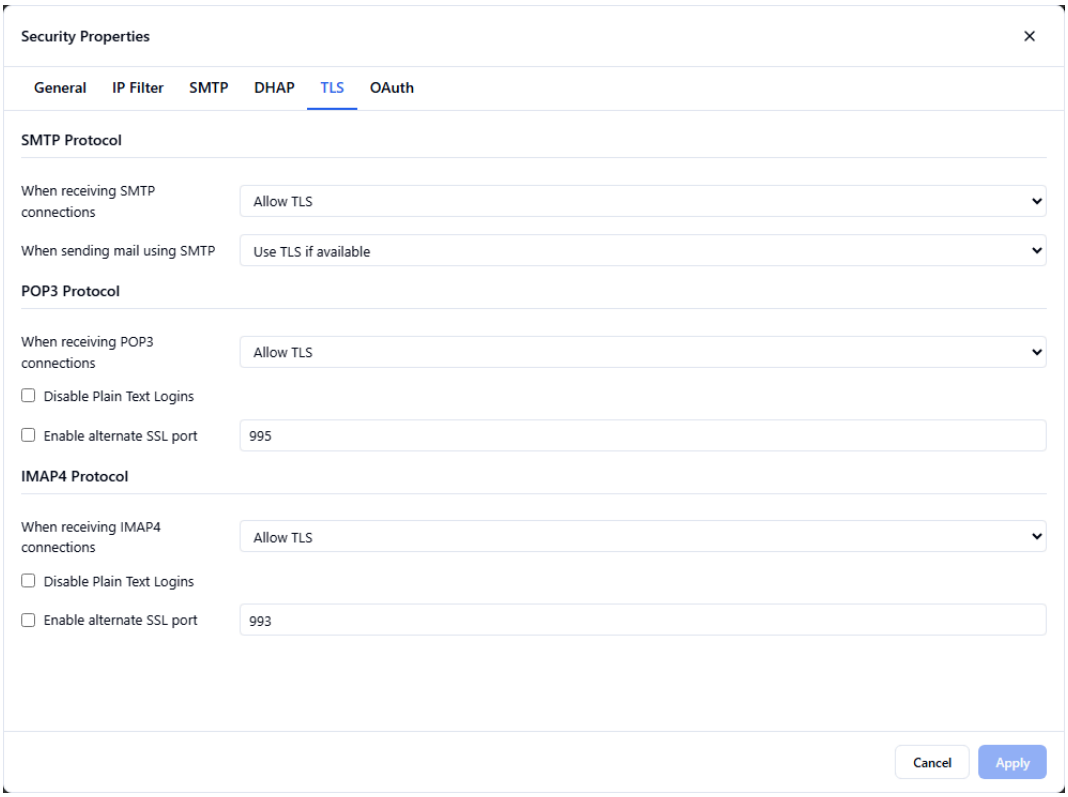
For the web address, a public TLS test service can check the certificate chain and the protocol versions offered on port 443. It should report TLS 1.2 and TLS 1.3 only, with SSL, TLS 1.0 and TLS 1.1 not supported.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

5 Setting the TLS Policy

A certificate makes encryption possible; the TLS policy decides when it is used. Installing a certificate does not by itself require encryption for every protocol.

Open Server, Security, Security Properties and choose the TLS tab. SMTP, POP3 and IMAP4 each have their own settings.



5.1 Receiving SMTP, POP3 and IMAP4

- **Disable TLS:** MailSite does not offer TLS.
- **Allow TLS:** MailSite offers TLS and encrypts the connection when the client asks for it. This is the default on a new installation.
- **Require TLS:** MailSite insists on encryption. For IMAP4 it refuses to sign a client in until the client has started TLS.

For POP3 and IMAP4 you can also choose:

- **Disable Plain Text Logins**, to refuse a password sent over an unencrypted connection.
- **Enable alternate SSL port**, for clients that connect with TLS from the start. The usual ports are 995 for POP3 and 993 for IMAP4. A new installation also receives SMTP on port 465 this way, and on the submission port 587 beside port 25. These ports open once a certificate is loaded.

5.2 Sending SMTP

- **Disable TLS:** MailSite sends in clear text, even if the remote server offers TLS.
- **Use TLS if available:** MailSite uses TLS when the remote server offers it, and sends in clear text otherwise. This is the default on a new installation.

- **Require TLS if supported:** if the remote server offers TLS but the secure connection fails, MailSite tries again later. If the remote server does not offer TLS, MailSite sends in clear text.
- **Require TLS:** MailSite sends only to remote servers with which it can establish a secure connection.

TLS between mail servers is opportunistic, so MailSite accepts any certificate a remote mail server presents. A relay login set for SMTPDA is the exception: it is sent only after TLS, to a certificate that a trusted root issued for the relay's name.

5.3 Web and Exchange Connections

ExpressPro webmail, the Console, Classic Outlook, Exchange Web Services (EWS) and Exchange ActiveSync all connect over HTTPS. Once a certificate is loaded, plain HTTP on port 80 redirects to HTTPS.

An installation upgraded from MailSite 10 keeps its earlier TLS choices until you change them. Requiring TLS can stop mail exchange with servers or apps that cannot encrypt, so test before you require it.

6 Verifying MailSite

Once the certificates and the TLS policy are set, check the result with real mail and real clients.

1. Send a message to MailSite from a mail server outside your network, and send one from MailSite to an outside mailbox.
2. Open the message you received and read its `Received` header. MailSite names the cipher suite the connection used, for example `using TLS13_AES_256_GCM_SHA384`.
3. In the Console, open Server, Services and read the SMTPRA and SMTPDA logs for the two messages.
4. Connect an IMAP or POP client with TLS required, and sign in to ExpressPro over HTTPS.
5. Set up Outlook or a phone with the public host name, and check that it connects without a certificate warning.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

7 References

The MailSite 11 Administrator Guide describes every setting in this paper, in its chapters on TLS certificate management and Security. See also the TLS and Certificate Management page at www.mailsite.com.

7.1 Disclaimer

Although Rockliffe has made reasonable efforts to ensure accuracy at the time of publication, the accuracy of the information in this guide is not guaranteed. It is provided free of charge by Rockliffe. Rockliffe disclaims all warranties, either express or implied, regarding this document and is not liable for any damages arising directly or indirectly from the information in it.

7.2 Assistance

To discuss help with your MailSite installation, contact sales@mailsite.com.