MailSite 11
Administrator Guide

MailSite 11 beta

This guide explains installation, administration and supported migration workflows for MailSite 11. It retains the earlier guide's chapter organization, with current Console and ExpressPro screenshots, automatic contents, page references and index. Compatibility notes identify retired functions and changes that require migration.

Installation, configuration and operation of MailSite Server, Console and ExpressPro.

Rockliffe Systems Incorporated

Contents

Acknowledgments

MailSite is based on the Freeware IMS for Windows NT that was developed under the EMWAC project. EMWAC was funded by Datalink Computers, Digital, Microsoft, Research Machines, Sequent and the University of Edinburgh.

Certain algorithms used in parts of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Introduction

MailSite 11 hosts email, calendars, contacts and mailing lists on Windows. This guide is for administrators installing the server, configuring domains and mailboxes, securing connections, and diagnosing delivery or synchronization problems.

MailSite 11 is a beta release. Evaluate the exact build with the clients and workflows your organization uses before upgrading production. Back up the installation, configuration and mailbox data before an upgrade. Earlier MailSite 11 development builds can cross database reset boundaries; these are different from the supported MailSite 10 upgrade path.

MailSite packaging options

MailSite SE is intended for smaller installations, LE for larger enterprises, and SP for service providers. Licensed capabilities and the selected configuration connector determine the features available to an installation. Review the license information in the Console rather than assuming that every option shown in this guide is enabled.

MailSite components

MSDBMA is the Message Store and Database Management Agent. It owns shared configuration access, mailbox files, indexes and databases for the other MailSite services. Its internal endpoint must remain private.

HTTPMA is the HTTP Management Agent. It serves ExpressPro and the Console and accepts public web and synchronization requests. Exchange Web Services, Exchange ActiveSync and MAPI over HTTP requests pass through HTTPMA to their respective worker services.

EWSMA handles Exchange Web Services (EWS). ExpressPro and compatible desktop clients use it for mailbox, contact and calendar operations. EASMA handles Exchange ActiveSync (EAS) for mobile synchronization. MAPIMA handles MAPI over HTTP for classic Outlook; the service supports classic Outlook clients.

SMTPRA receives email over Simple Mail Transfer Protocol (SMTP), applies receiving policy and queues accepted mail. SMTPDA delivers queued messages locally or to another server. IMAP4A and POP3A provide Internet Message Access Protocol (IMAP) and Post Office Protocol (POP3) access to mailboxes.

Console and ExpressPro

Use the MailSite desktop Console or open Console from ExpressPro after signing in. They share the administration interface. A server administrator can manage server settings and domains. A domain administrator has access within the assigned domain. A mailbox user and a list moderator see only the resources and operations allowed by their privileges.

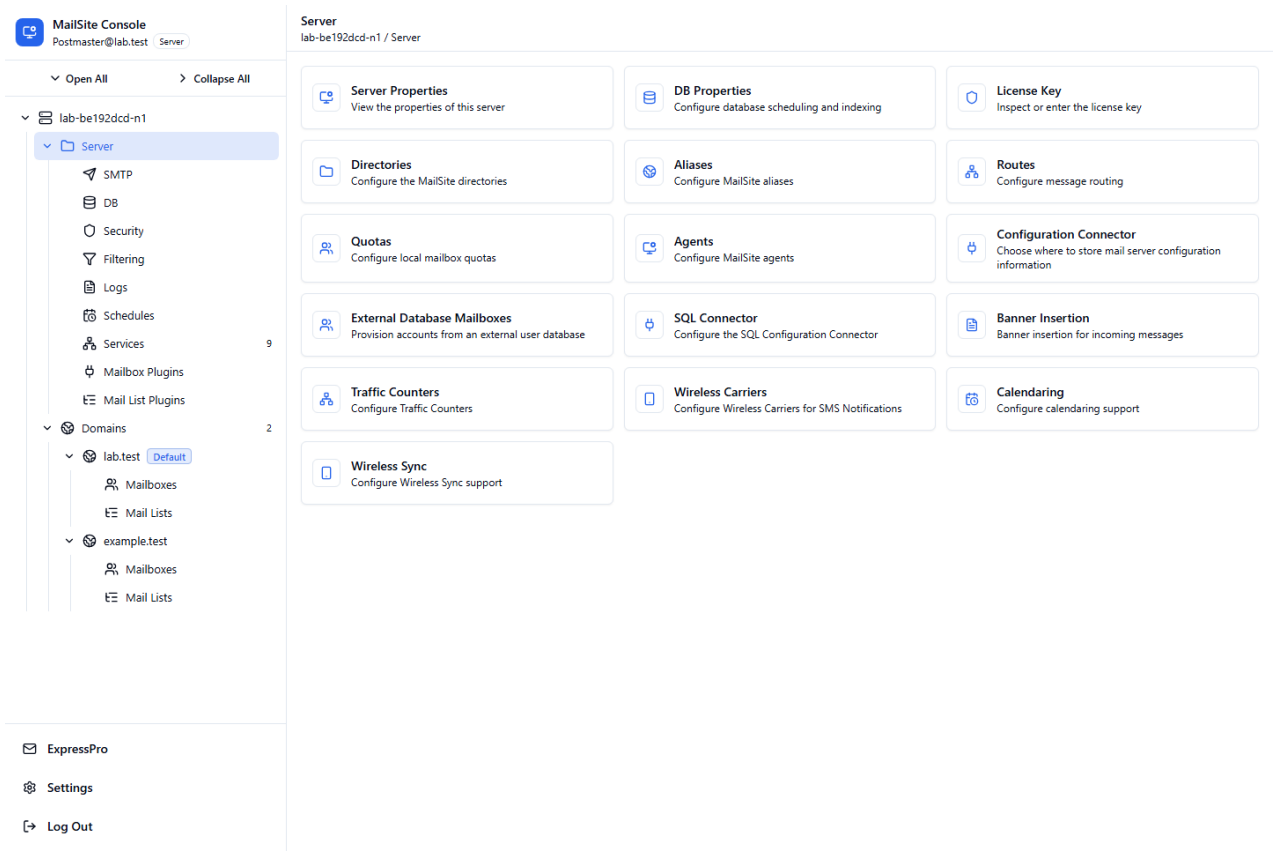

Figure 1 The MailSite 11 Console

ExpressPro provides mail, contacts, calendars, search and account settings. HTTPMA serves these applications directly; an IIS application or the old Express, Pocket or WConsole installation is not required.

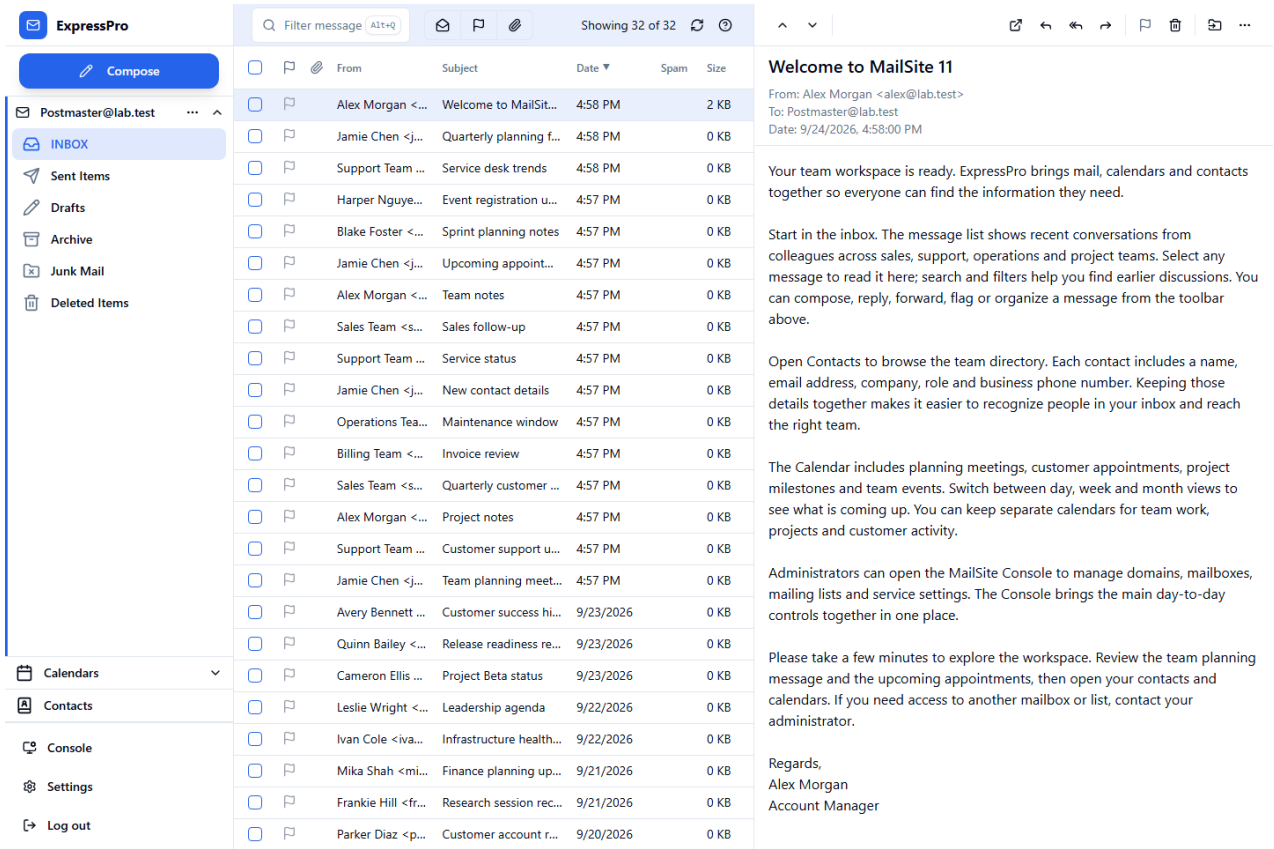

Figure 2 Reading a message in ExpressPro

How to use this guide

The chapters introduce the main administration tasks. The Console reference describes configuration areas in more detail. The appendices retain command-line and protocol reference material. Use the contents and index to navigate; page references are generated from the document rather than maintained by hand.

Available controls depend on your privileges, configuration connector, and licensed features.

Changes from the previous guide

The chapter organization is retained, while the installation, service, Console, ExpressPro and synchronization instructions describe v11. EASMA, EWSMA and TLS management have dedicated chapters. Old native Console and InstallShield illustrations are replaced or retired. Unsupported legacy workflows are identified rather than presented as current steps.

The main migration differences are explicit mailbox Copy/Move semantics, retired dial-up/RAS scheduling, current external-provider contracts, recreated calendar publication/subscription links, and separately handled legacy pending list data and archives. The original MailSite 10 PDF remains a separate reference; it is not overwritten by generating this guide.

What is new in Version 11

MailSite 11 replaces the web interface and modernizes the mail and synchronization services while retaining the MailSite domain, mailbox and mail-list administration model.

Exchange Web Services

EWSMA provides Exchange Web Services behind HTTPMA. Compatible desktop clients can access mail, calendars and contacts through /EWS/Exchange.asmx. Test each supported client version with the operations your organization needs; EWS support is not a claim of complete Microsoft Exchange feature parity.

Exchange ActiveSync

EASMA replaces the IIS-based ActiveSync application. It supports Exchange ActiveSync through version 16.1 for mobile email, folders, contacts, calendars and attachments. The public endpoint remains /Microsoft-Server-ActiveSync.

ExpressPro and administration

ExpressPro has a three-pane mail interface, full text search, integrated contacts and calendars, account settings and themes. The desktop and web Console share the administration interface. Domain, mailbox, mailing-list and service settings are available from the Console navigation tree.

Mail transport and filtering

The new SMTP and IMAP services include native ClamAV integration, Bayesian spam filtering, search and updated operational diagnostics. Review the current scanning dialogs and the policies they control when migrating from the old AVG or Mailshell configuration.

TLS certificates

Domain certificate management includes hostname testing, certificate requests, renewal settings and issuance diagnostics. MailSite-owned certificate files take precedence for matching hostnames; Windows-store certificates remain a compatibility source for names without certificate files. Services load certificates at startup.

Deployment and compatibility

HTTPMA replaces the IIS dependency. MSDBMA supplies shared storage and configuration services, and the installed service set includes EWSMA, EASMA and MAPIMA. Install matching binaries from one release rather than replacing selected services independently.

MailSite 11 supports classic Outlook through MAPI over HTTP. Read the release notes for known issues and development-database reset boundaries before upgrading. A reset can discard database-only data and synchronization state even when live message, contact and calendar files remain.

Installation

Use the installer supplied with the MailSite 11 release. The current installer supports a new installation, an eligible MailSite 10 upgrade, and replacement or repair of an installation owned by the current v11 installer. Do not use the older InstallShield or IIS setup procedures for v11.

Preparation

Confirm the release's Windows, memory, storage and SQL requirements. Allow space for mailbox growth, logs, queues, indexes and backups in addition to the application binaries. Plan the public server hostname, DNS records, TLS certificate names and network ports before exposing the server.

Back up the existing installation and all configured data locations. For an upgrade, retain a recovery copy of registry or SQL configuration, mailbox data and certificate material. Record the installed version and the Windows identities under which services run. Ensure those identities can access the required directories and any remote resources.

Use an elevated PowerShell session for installation. The installer checks prerequisites and provisions its services, credentials, application files and desktop applications. Read its prompts and the recorded installation log if a check fails.

Install a release

Download the release installer and MailSite.zip from the MailSite release distribution. Run the installer from the downloaded release directory. The default install directory is C:\Program Files\MailSite.

```
powershell -NoProfile -File .\install-mailsite.ps1
```

With no version argument, the installer presents the available installation choices. An exact v11 version can be supplied to select that release. The PackagePath option uses a downloaded package instead of retrieving one.

```
powershell -NoProfile -File .\install-mailsite.ps1 -PackagePath .\MailSite.zip
```

The installer validates package ownership and version consistency. An interrupted or unrecognized previous development installation may require its matching uninstaller; do not fabricate an install.json marker or bypass the ownership checks.

The release also includes mailsite-installer.exe for a graphical setup flow. It presents the installation folder, license or email entry, domain and Postmaster password, Windows service account, and final review. The figures below use its safe preview mode, which shows the real screens without changing the computer. A real installation requests administrator approval when you choose Install.

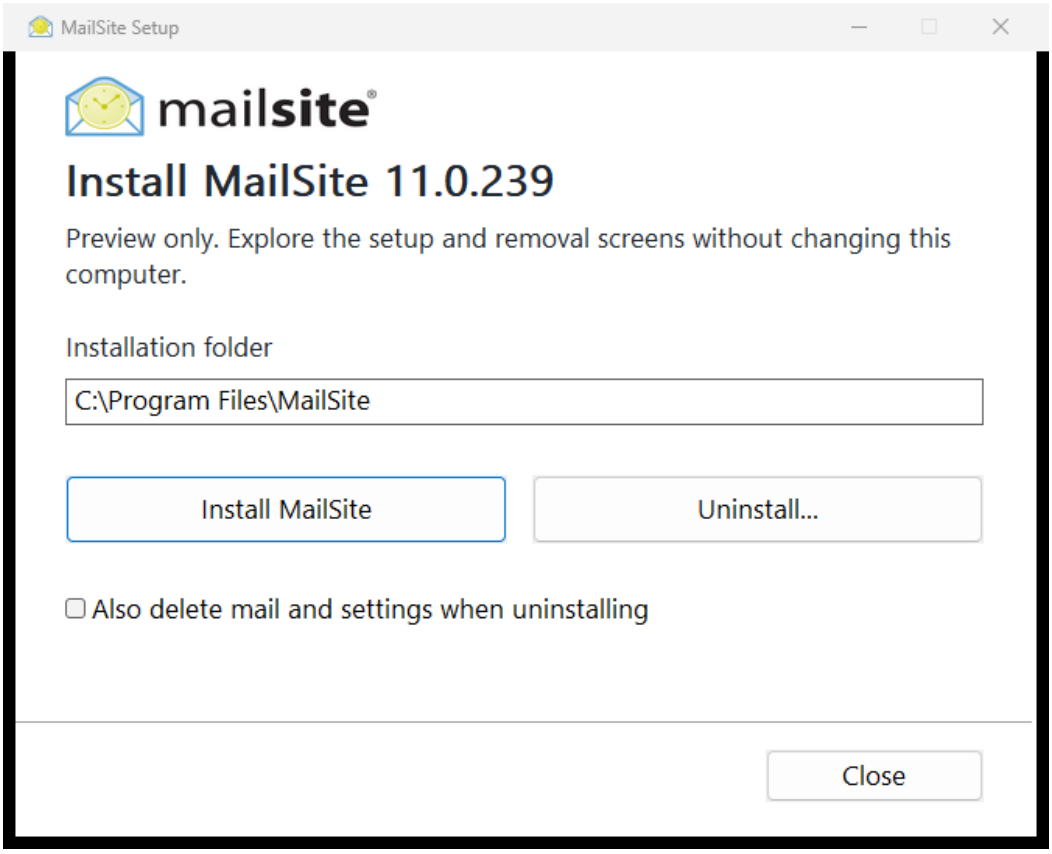

Figure 3 Native installer welcome screen in preview mode

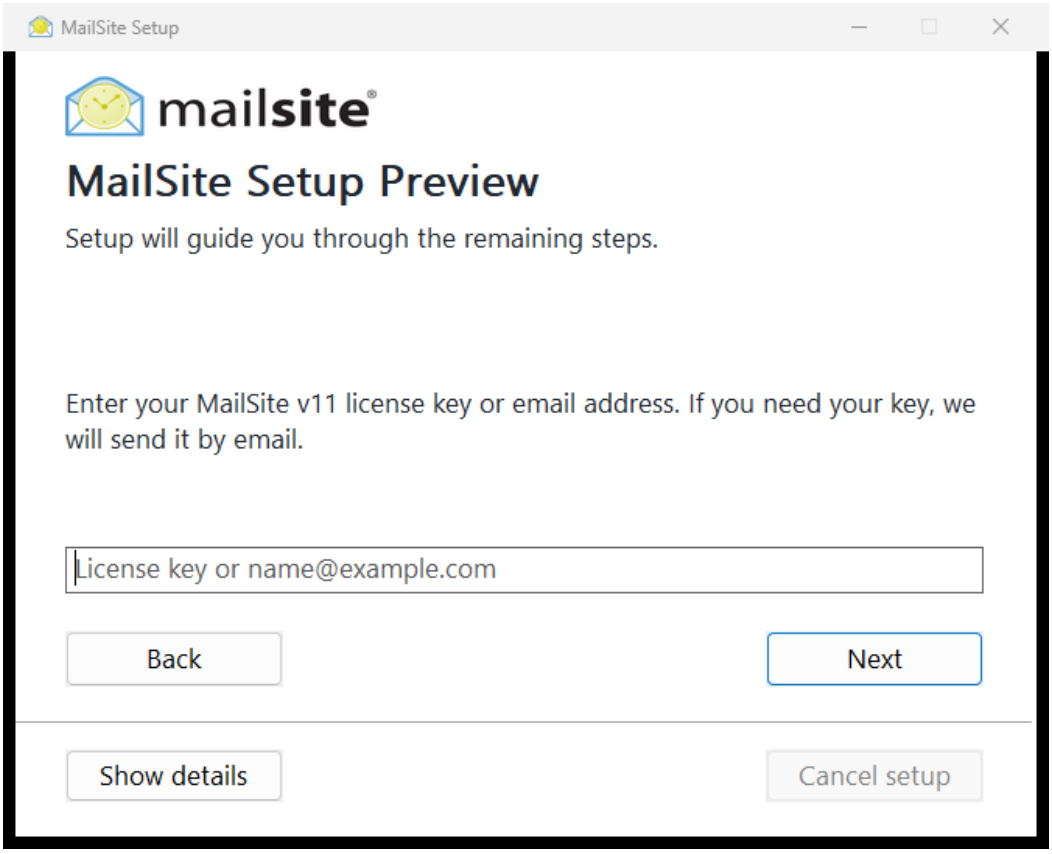

Figure 4 Native installer license step in preview mode

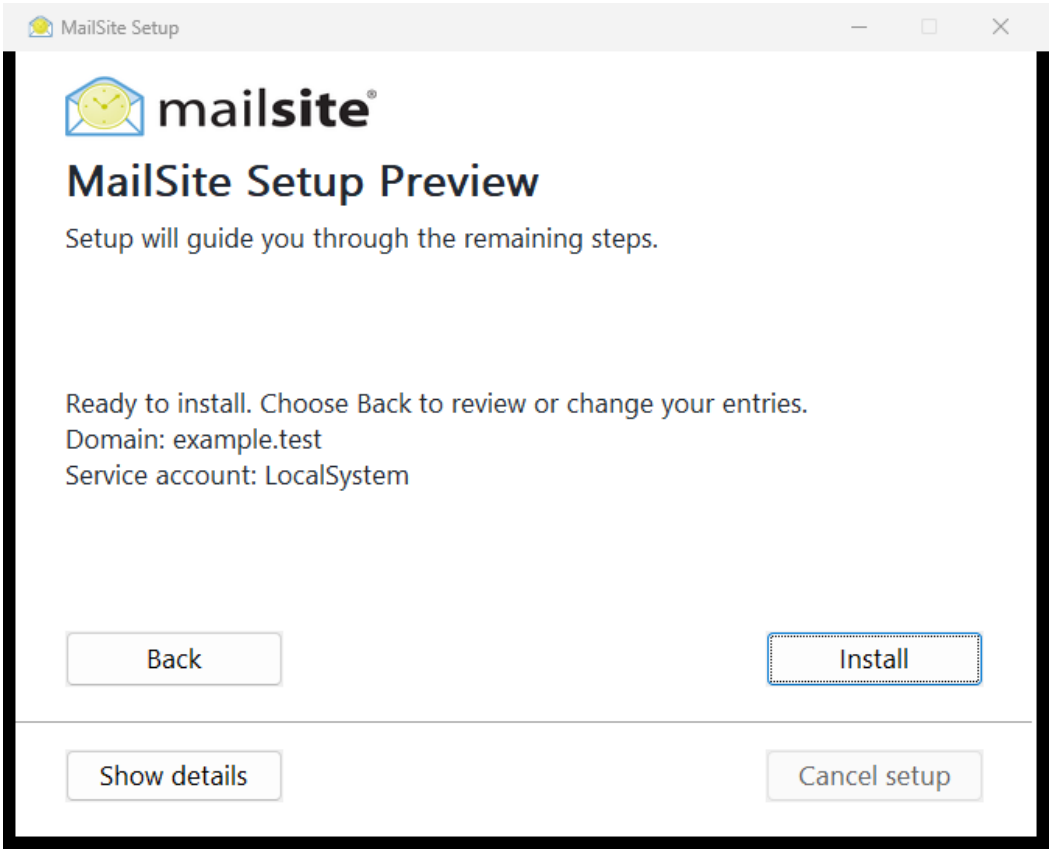

Figure 5 Native installer review screen in preview mode

During setup, the status line shows each step. Show details opens more messages. Stick to bottom is on by default; turn it off to read earlier messages. The full diagnostic log is saved separately.

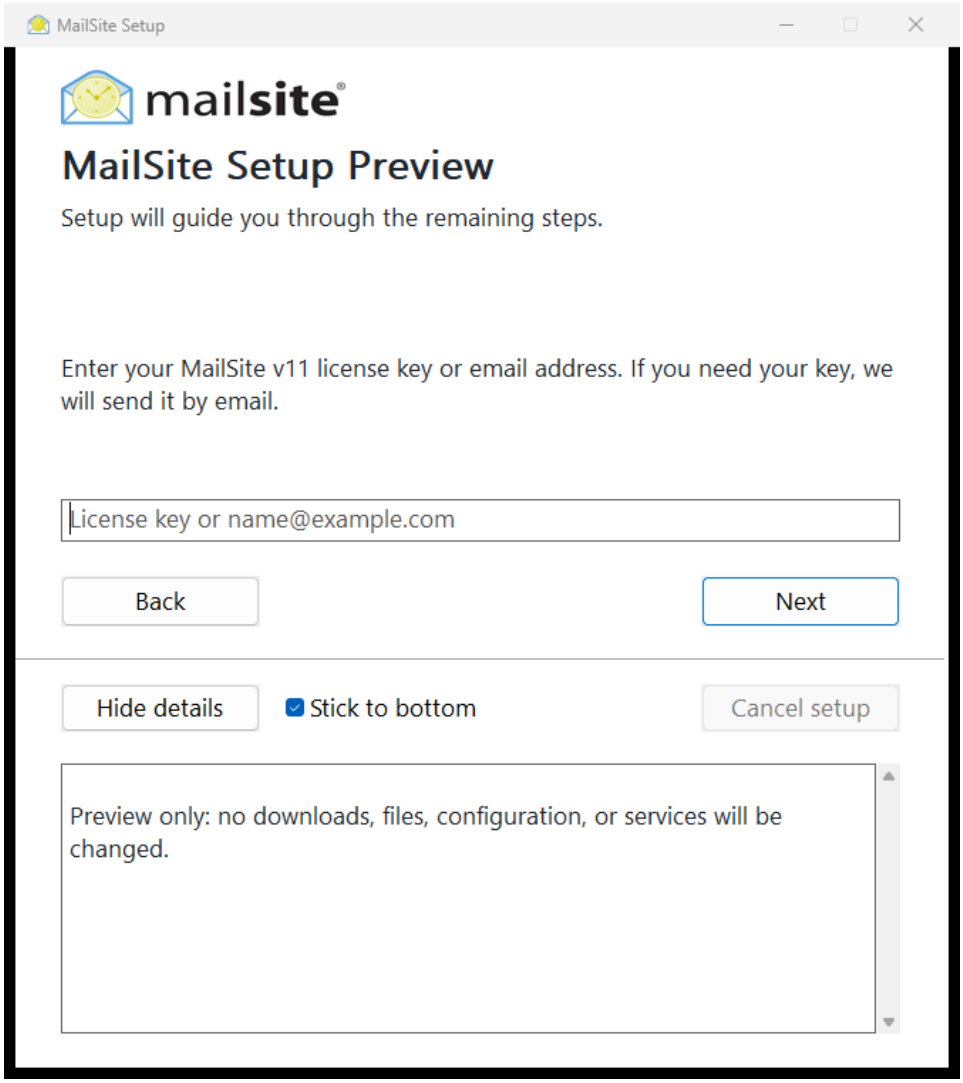

Figure 6 Native installer details in preview mode

Services and installed files

The installed services are MSDBMA, HTTPMA, EWSMA, MAPIMA, EASMA, IMAP4A, POP3A, SMTPRA and SMTPDA. The package also includes the ExpressPro and MailSite Console desktop applications, supporting files, release notes and mailsite-admin-guide.pdf.

MSDBMA is a dependency of the services that use shared storage. EWSMA, EASMA and MAPIMA listen on private worker endpoints behind HTTPMA. Expose the public client endpoints required by your deployment, not the worker ports.

Upgrade or repair

Deploy the complete matching release with its installer. A coherent existing installation can be repaired using the reinstall target. If its binaries disagree about the installed version, the installer uses a complete replacement rather than trusting one component's version.

```
powershell -NoProfile -File .\install-mailsite.ps1 reinstall
```

An upgrade from MailSite 10 and an upgrade between v11 beta builds have different compatibility rules. Before crossing a development-database reset boundary, back up database-only data as well as live mailbox files. Clients may need to synchronize again after a reset. Restoring old binaries alone does not restore discarded database state.

Verify installation

Check the installation log under the Install directory. Open the Console, confirm the installed services are running and check their logs for startup failures. Verify the default domain and postmaster account, then test webmail, inbound and outbound email, and the synchronization clients in use.

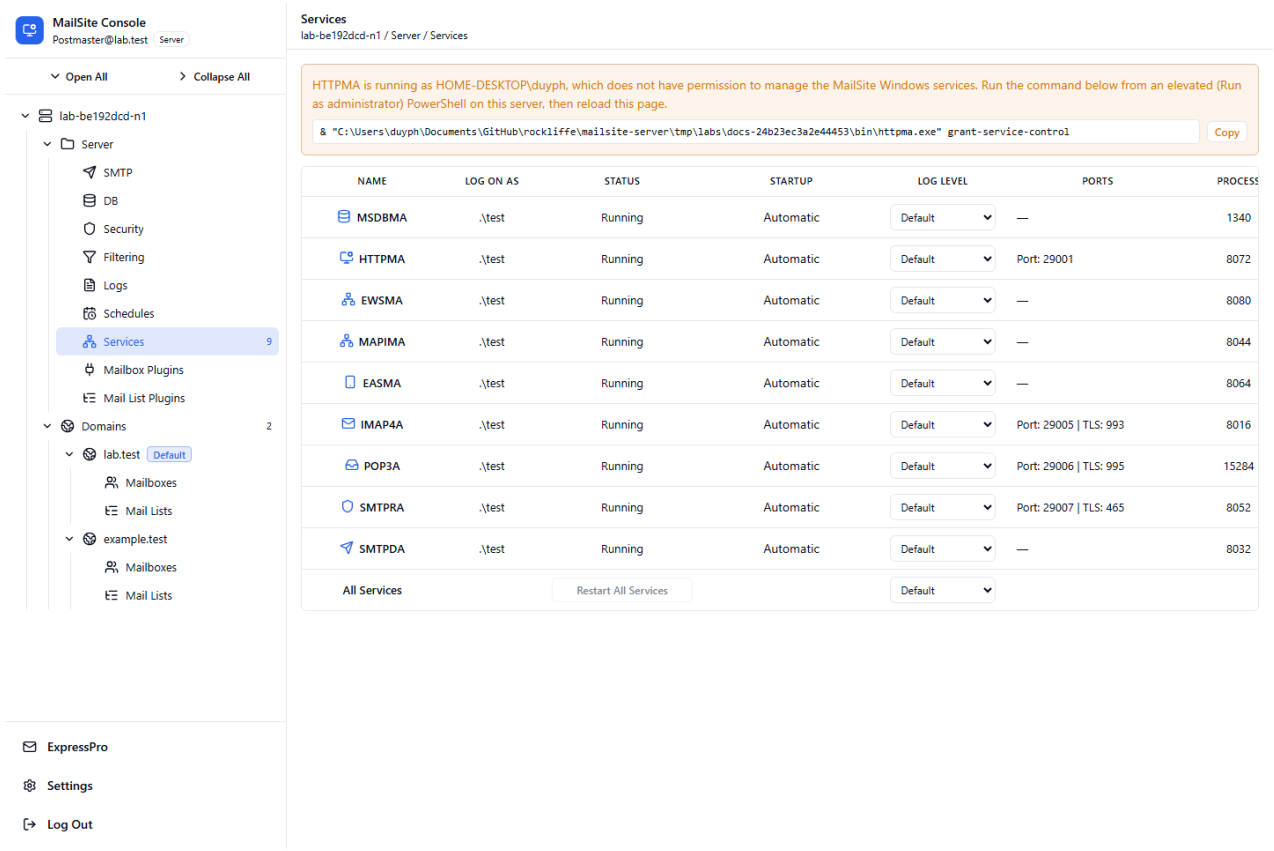

Figure 7 Service status in the Console

Verify the public TLS certificate from a client outside the server. A successful connection through localhost does not verify DNS, firewall rules, certificate names or public reachability.

Uninstall

Use the matching uninstaller from the installed release. Read the removal plan before confirming it. The DeleteData option explicitly requests removal of data and configuration; do not use it when you intend to retain the installation's data for recovery.

```
powershell -NoProfile -File .\uninstall-mailsite.ps1
```

Keep the backup until the replacement installation and its client workflows have been verified. Do not substitute manual deletion of program files or service registry keys for the supported uninstall process.

Quick Start

Complete installation and certificate configuration before accepting production traffic. Use a test mailbox and a controlled external account for the following checks.

Confirm the server and domain

Sign in to the Console with a server administrator account. Review Server Properties and the default domain. The public hostname must agree with the client configuration and the names in the certificate. Verify the domain's DNS records and its mail routing.

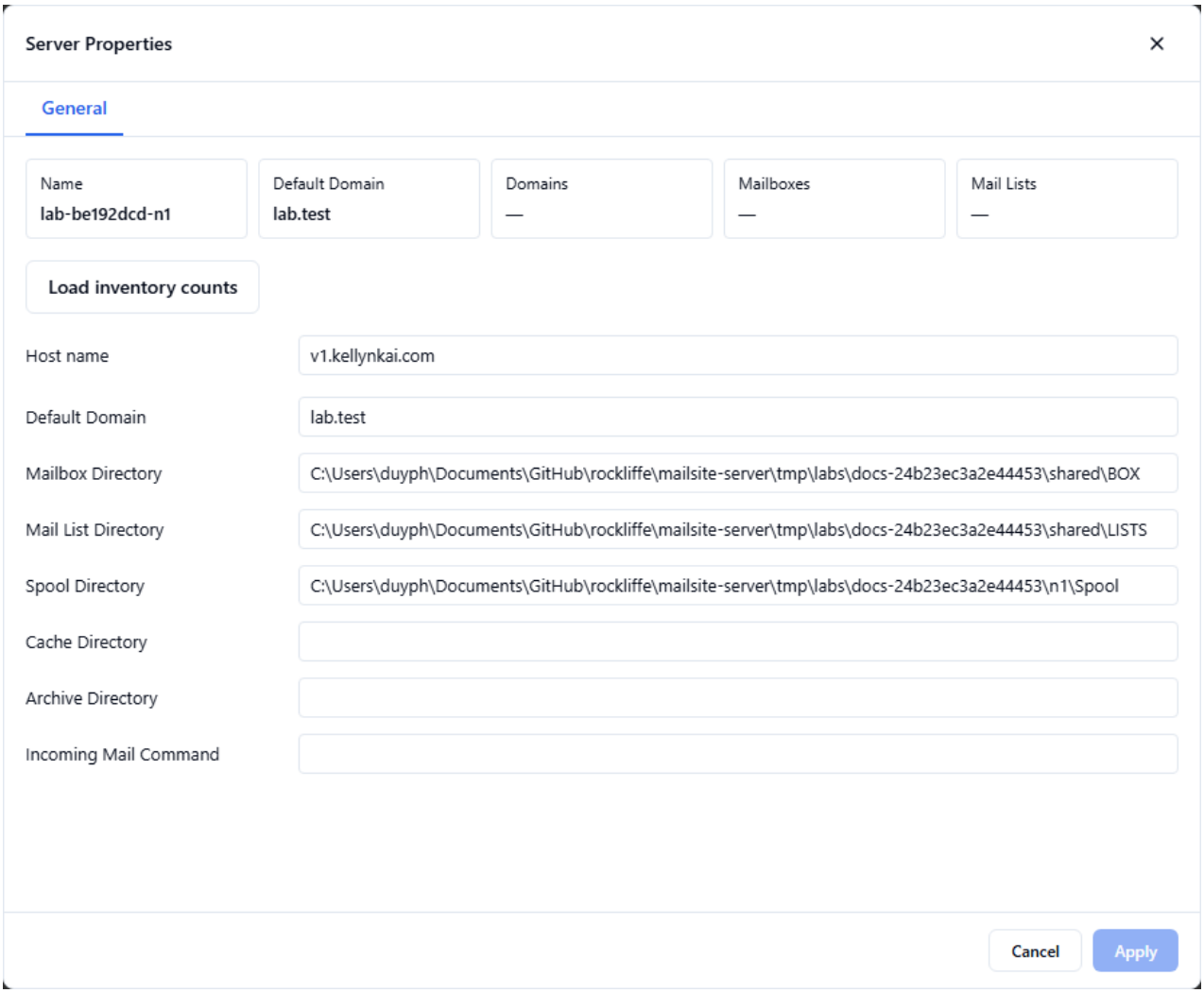

Figure 8 Server properties

Check services

Open Server, Services. Confirm MSDBMA and the public mail services are running. Also verify EWSMA for ExpressPro and EWS clients, EASMA for ActiveSync clients, and MAPIMA for classic Outlook MAPI connectivity.

Create a test mailbox

Expand Domains, select the intended domain, and open Mailboxes. Create a mailbox with a unique name and initial password. Sign in as that user and confirm that its access is limited to the intended resources. Do not use the server administrator's credentials in a normal client test.

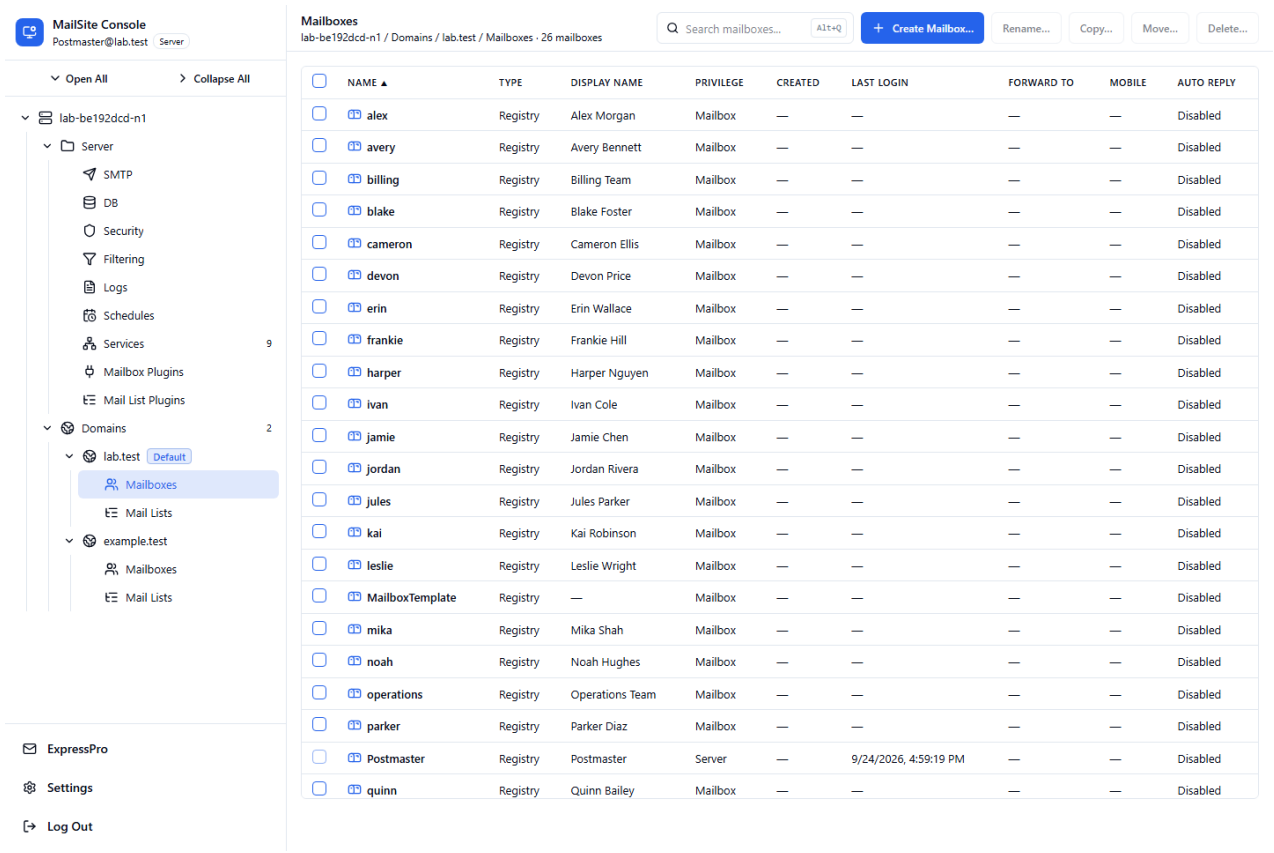

Figure 9 Mailboxes in a domain

Test mail delivery

Send a message from the test mailbox to a controlled external mailbox, then reply. Confirm both delivery directions and inspect the SMTPRA and SMTPDA logs if either direction fails. Test a message with an ordinary attachment and verify that scanning and mailbox quota policies produce the intended result.

Test webmail and synchronization

Open ExpressPro at the public HTTPS address. Read a message, create a contact and create a calendar event. Configure one client of each type you will support, then verify changes in both directions. Test folder changes and attachments as well as the initial sign-in.

Review security policy

Review relay restrictions, authenticated access, TLS settings, anti-virus and anti-spam policies. Confirm that the intended rejection, deferral or delivery behavior appears in the logs. A screenshot of a configured option is not evidence that the whole mail flow has been tested.

Mobile Connectivity

MailSite supports mobile access through Exchange ActiveSync and through mail protocols supported by the device. Use Exchange ActiveSync when the client needs mail, contacts and calendars together. An IMAP account synchronizes email; it does not by itself provide contact and calendar synchronization.

Configure an ActiveSync client

Obtain the mailbox address, password and public HTTPS server hostname from the administrator. Choose the client's Exchange or ActiveSync account type and enter the account details. If automatic discovery is unavailable, supply the public hostname manually. The certificate must be trusted by the device and match that hostname.

Confirm that Wireless Sync is enabled at the appropriate server, domain and mailbox levels and that the license permits it. Select the collections to synchronize in the client. Test a new message, contact and calendar event in both directions, followed by an attachment and a folder change.

Diagnose a device problem

First confirm that the same account can sign in to ExpressPro. Then check the EASMA and HTTPMA services, the Wireless Sync policy and the client account settings. Record the device and client versions and the time of the failure before inspecting service logs.

If a previous v11 development upgrade reset synchronization state, follow that release's client resynchronization instructions. Do not repeatedly recreate the account without checking the underlying server error.

Exchange ActiveSync service EASMA

EASMA is the MailSite Exchange ActiveSync service. Exchange ActiveSync synchronizes mail, folders, contacts, calendars and attachments with supported clients. MailSite 11 supports protocol versions through 16.1; feature coverage still depends on the client and server build.

Request path and prerequisites

A device connects over HTTPS to /Microsoft-Server-ActiveSync on the public server. HTTPMA accepts the request and forwards it to EASMA. EASMA uses MSDBMA for mailbox and configuration access. HTTPMA, EASMA and MSDBMA must therefore all be available for synchronization.

Use a public hostname with correct DNS and a trusted matching TLS certificate. Keep EASMA's worker endpoint private. Confirm that the account is enabled and that its license and service policies permit Wireless Sync.

Configure Wireless Sync

Open Server, Wireless Sync in the Console. Enable Wireless Sync on the server and select whether it applies to all mailboxes or to configured domains and mailboxes. Apply the change.

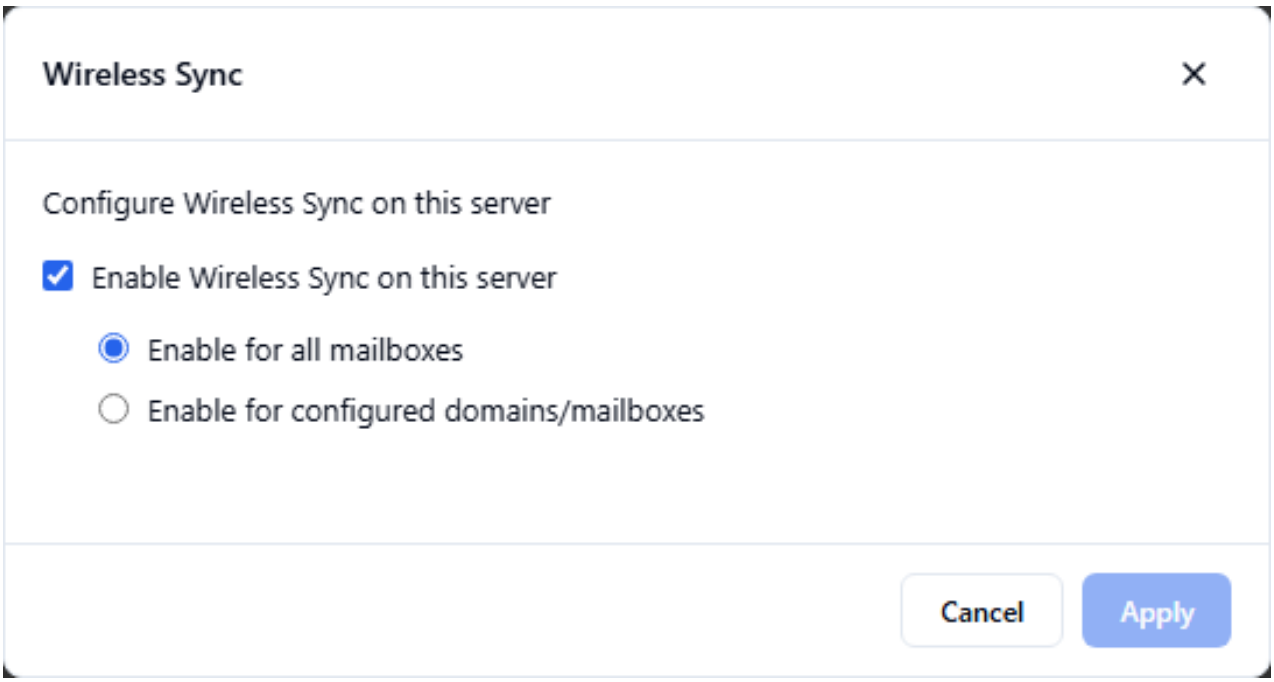

Figure 10 Wireless Sync policy in the Console

When using a restricted scope, review the domain's Wireless Sync tab and the mailbox's service settings. Test with a normal mailbox account after changing policy; a server administrator's access is not a substitute for that check.

Verify the service

Open Server, Services and inspect EASMA, HTTPMA and MSDBMA. Configure a supported device with the public server hostname and mailbox credentials. Check initial synchronization, message read state, folder changes, attachment download, contact edits and calendar edits. Repeat after disconnecting and reconnecting the device.

Troubleshooting

Check public TLS and DNS first when no device can connect. For account-specific failures, compare account credentials, enabled services, license scope and mailbox initialization. For a gateway error, check whether EASMA is running and reachable from HTTPMA. Use logs from the same time window across HTTPMA, EASMA and MSDBMA.

Record the client and operating-system versions, affected collection, operation and error text when reporting an interoperability problem. Redact credentials and private message content from shared logs.

Exchange Web Services service EWSMA

EWSMA implements Exchange Web Services, the mailbox protocol used by ExpressPro and compatible desktop clients. EWS operations include mail and folder access, contacts and calendars. It is separate from ActiveSync and MAPI over HTTP.

Request path and prerequisites

Clients send HTTPS requests to /EWS/Exchange.asmx on the public host. HTTPMA forwards those requests to the EWSMA worker. EWSMA accesses shared mailbox and configuration services through MSDBMA. The worker's private endpoint is not a client configuration address.

Install matching HTTPMA, EWSMA and MSDBMA binaries. Configure the public hostname, a trusted matching certificate, the domain and mailbox before testing a client. Verify the current client's supported account type and authentication method.

Verify ExpressPro first

Sign in to ExpressPro as a normal test mailbox. Open its folders and read a message, then create a contact and a calendar event. A successful page load alone is insufficient because the web interface and mailbox operations use different parts of the service stack.

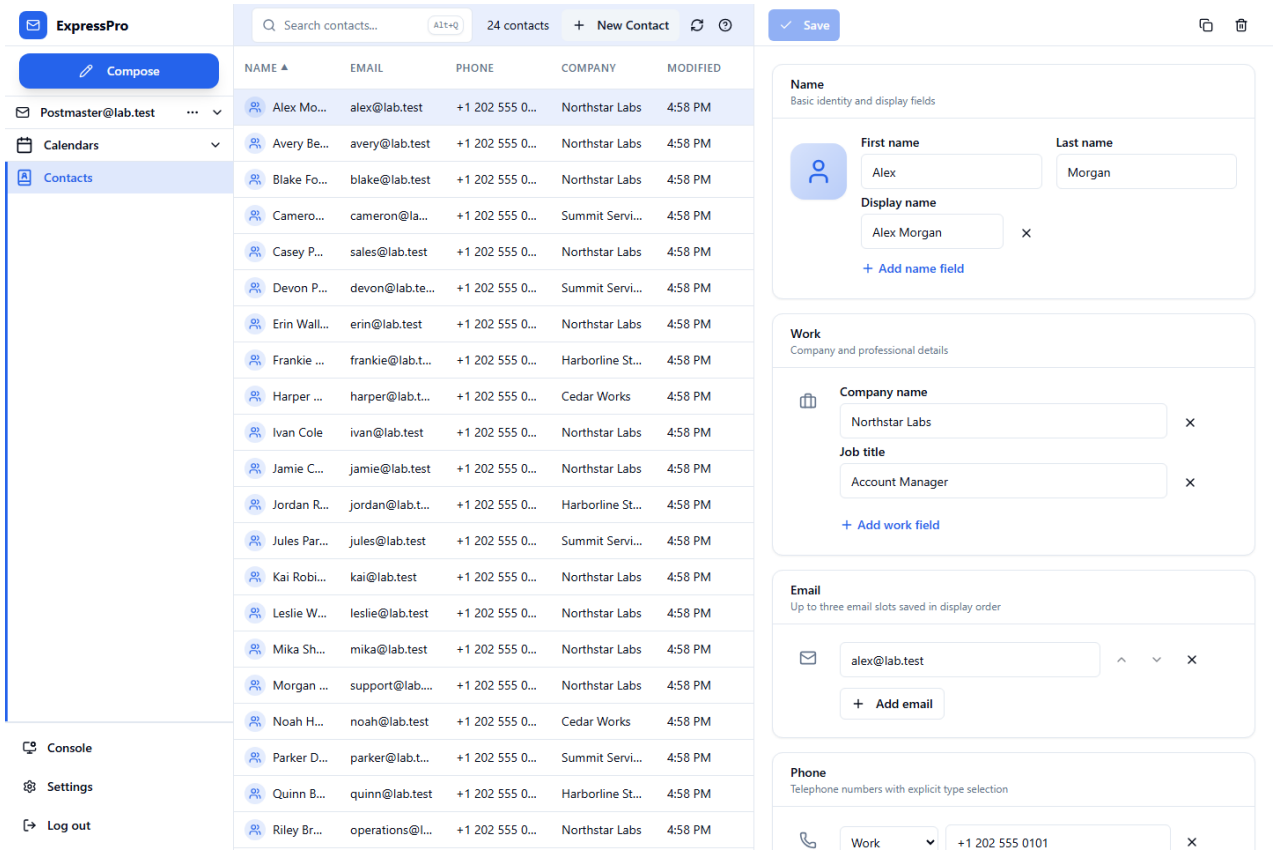

Figure 11 Contact data served through the MailSite mailbox services

Validate desktop clients

Configure the EWS account using the public hostname or a working discovery configuration. Verify initial folder synchronization, message operations, attachments, contact changes and calendar changes in both directions. Include recurring events and reconnection in testing when those workflows matter to your users.

Do not infer complete Exchange compatibility from a successful sign-in. Validate the exact client version and required operations against the current MailSite release. Classic Outlook MAPI connectivity uses MAPIMA and must be evaluated separately.

Troubleshooting

If the site opens but EWS operations fail, inspect the EWSMA service and its logs, then MSDBMA and the mailbox's initialization state. Compare the public endpoint with the worker path through HTTPMA. Record the failing operation and time so related log entries can be correlated.

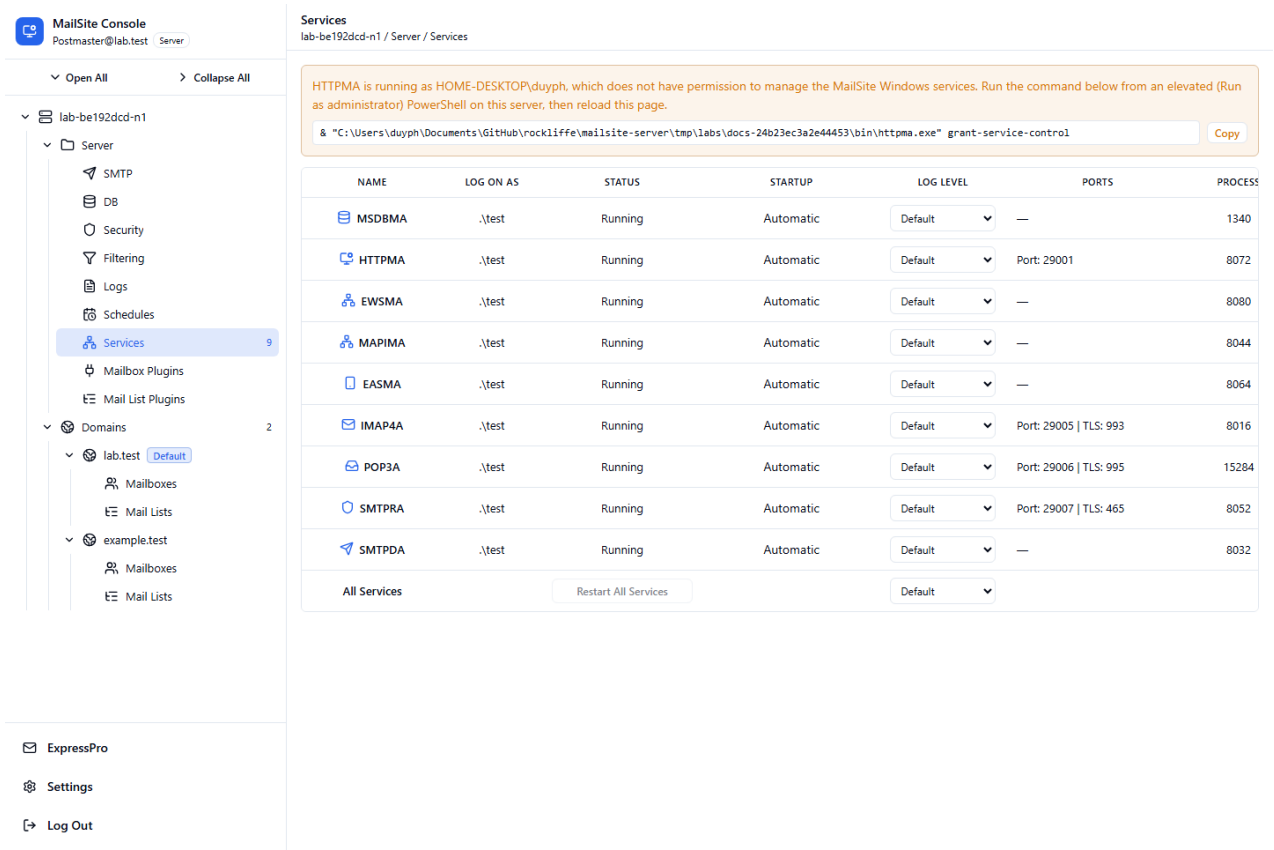

Figure 12 Inspect EWSMA and its dependencies in Services

Outlook Connectivity

Choose a connection method supported by the exact Outlook edition and build being evaluated. The name Outlook covers clients with different protocol capabilities. Do not assume that classic Outlook for Windows, new Outlook, Outlook for Mac and mobile Outlook use the same account setup.

Mail protocols and synchronization

IMAP and SMTP provide email access for clients that support those protocols. Exchange Web Services, Exchange ActiveSync and MAPI over HTTP are separate protocol paths with different capabilities and client support. Configure the public hostname and certificate before testing any of them.

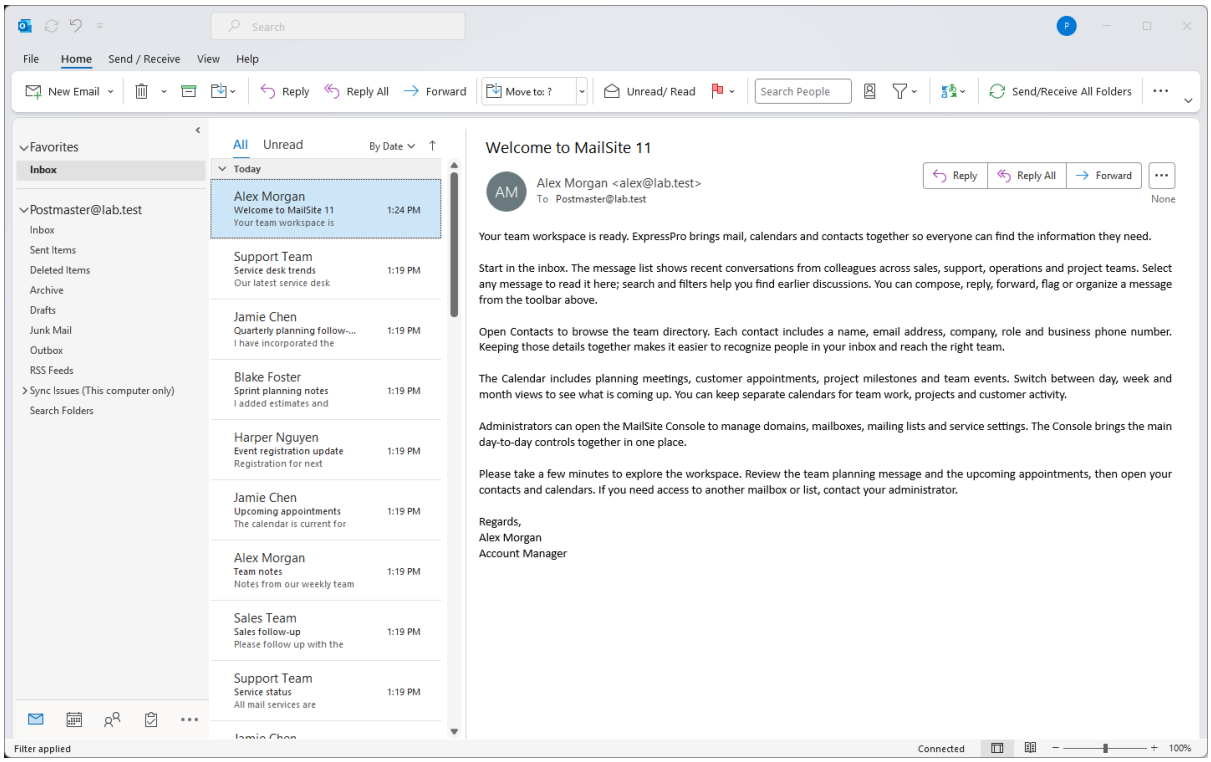

Figure 13 Classic Outlook Inbox connected to MailSite over IMAP

Classic Outlook and MAPI over HTTP

MAPIMA implements MAPI over HTTP behind HTTPMA. Test the Outlook build and operations your organization uses. Validate initial profile creation, mail and folder operations, attachments, contacts, calendars and reconnection against the current release before choosing it for production users.

If ExpressPro works but a MAPI client fails, check MAPIMA as well as HTTPMA and MSDBMA. An EWS or ActiveSync test cannot establish MAPI compatibility. Preserve relevant service logs and the exact Outlook build when reporting a problem.

Validate an upgrade

Read the release notes before reusing an existing Outlook cache after a development-database reset. Server identities or synchronization state may have changed. Keep recoverable copies of local-only data and follow the applicable resynchronization procedure.

Calendaring Server

MailSite stores calendars alongside mailbox data and makes them available through ExpressPro and supported synchronization clients. EWSMA and EASMA serve calendar operations for their respective clients; the old IIS calendar application is not part of the v11 setup.

Enable calendaring

In Server, open Calendaring. Enable the service for all mailboxes or for configured domains and mailboxes, according to your policy and licensed capabilities. Review the domain's Calendaring settings and the mailbox's service settings when using a restricted scope.

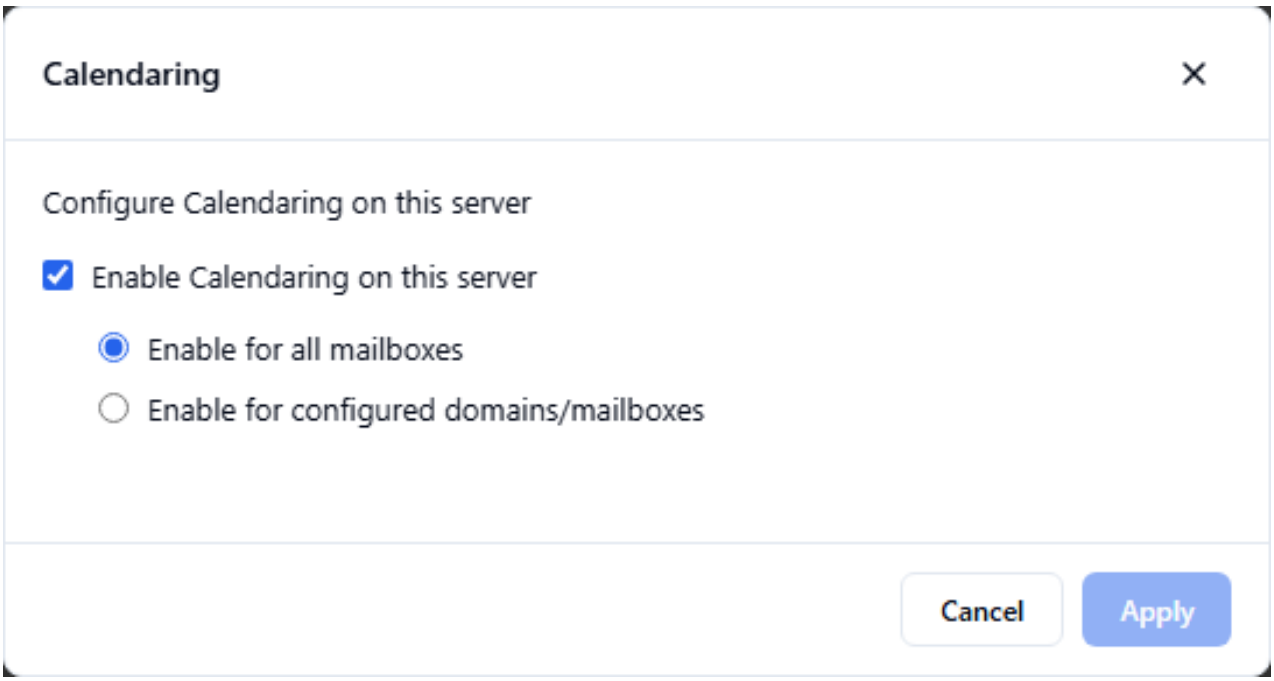

Figure 14 Server calendaring policy

Work with calendars

Open Calendars in ExpressPro to create and review events. Check the event's calendar, dates, time zone, recurrence and participants before saving or sending invitations. An appointment without attendees and a meeting invitation have different delivery effects.

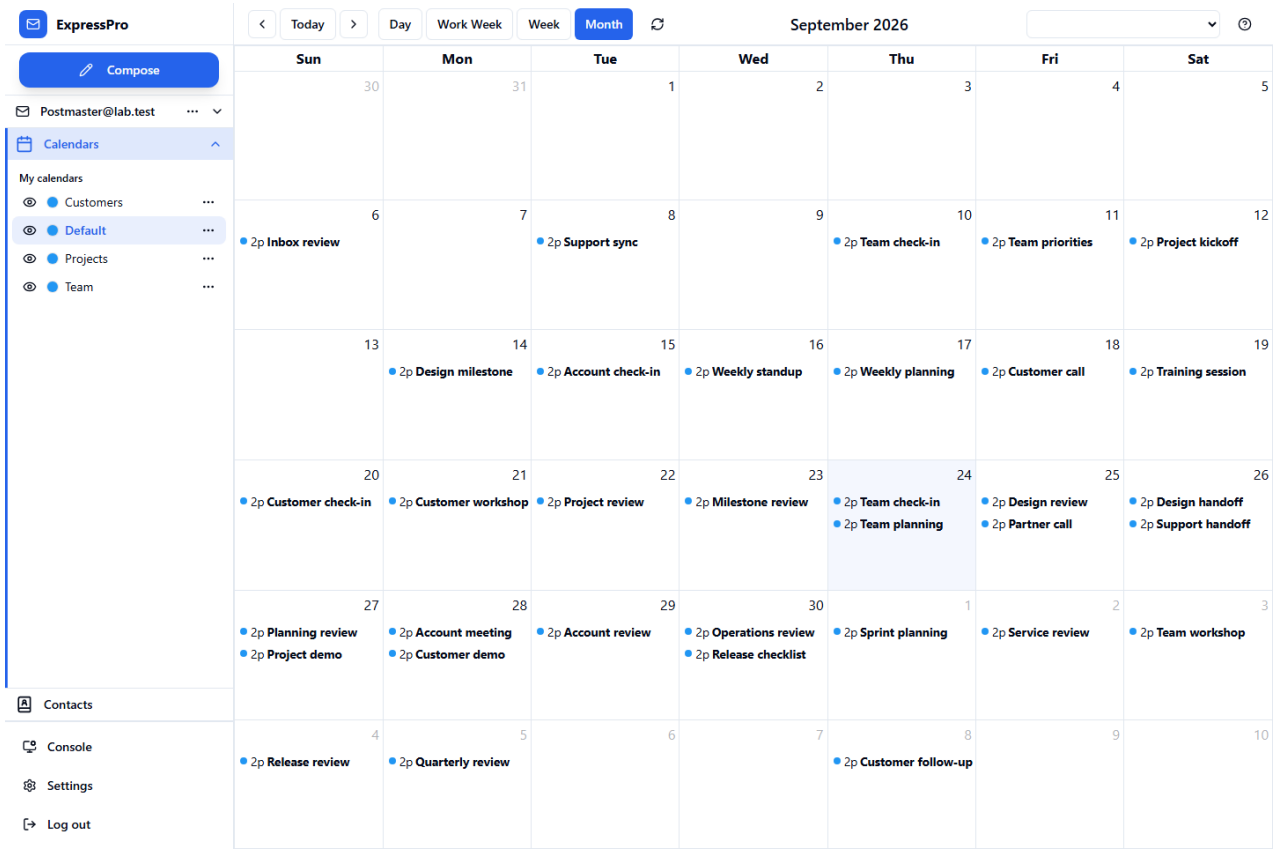

Figure 15 Calendar in ExpressPro

Test synchronization and sharing

Verify event creation, changes and deletion through each supported client in both directions. Include an all-day event, a recurring event and a meeting with attendees in your acceptance testing. Test shared-calendar access with the actual permissions and client versions that will be used.

The presence of a calendar in one client does not prove another client supports the same sharing or subscription workflow. Check service logs and access permissions if the same collection behaves differently across clients.

Publishing a calendar

In ExpressPro, open Calendars. Use the calendar's More actions menu and choose Publish. Create a named view, choose who can use it, select busy times or event details, set days before/after today and a timezone, then save and copy the subscription link.

Only me and My domain require sign-in. Anyone with the link grants access through the link token; share it only with intended recipients. Private/confidential events show busy times even in an event-details view. Reminders and attachments are excluded. The date window rolls with the current date.

Rotate the link to replace its token, or revoke the view to stop future downloads. These actions cannot erase calendar copies already downloaded by another application. Publishing is controlled by the calendar owner; it does not grant permission to edit the source calendar.

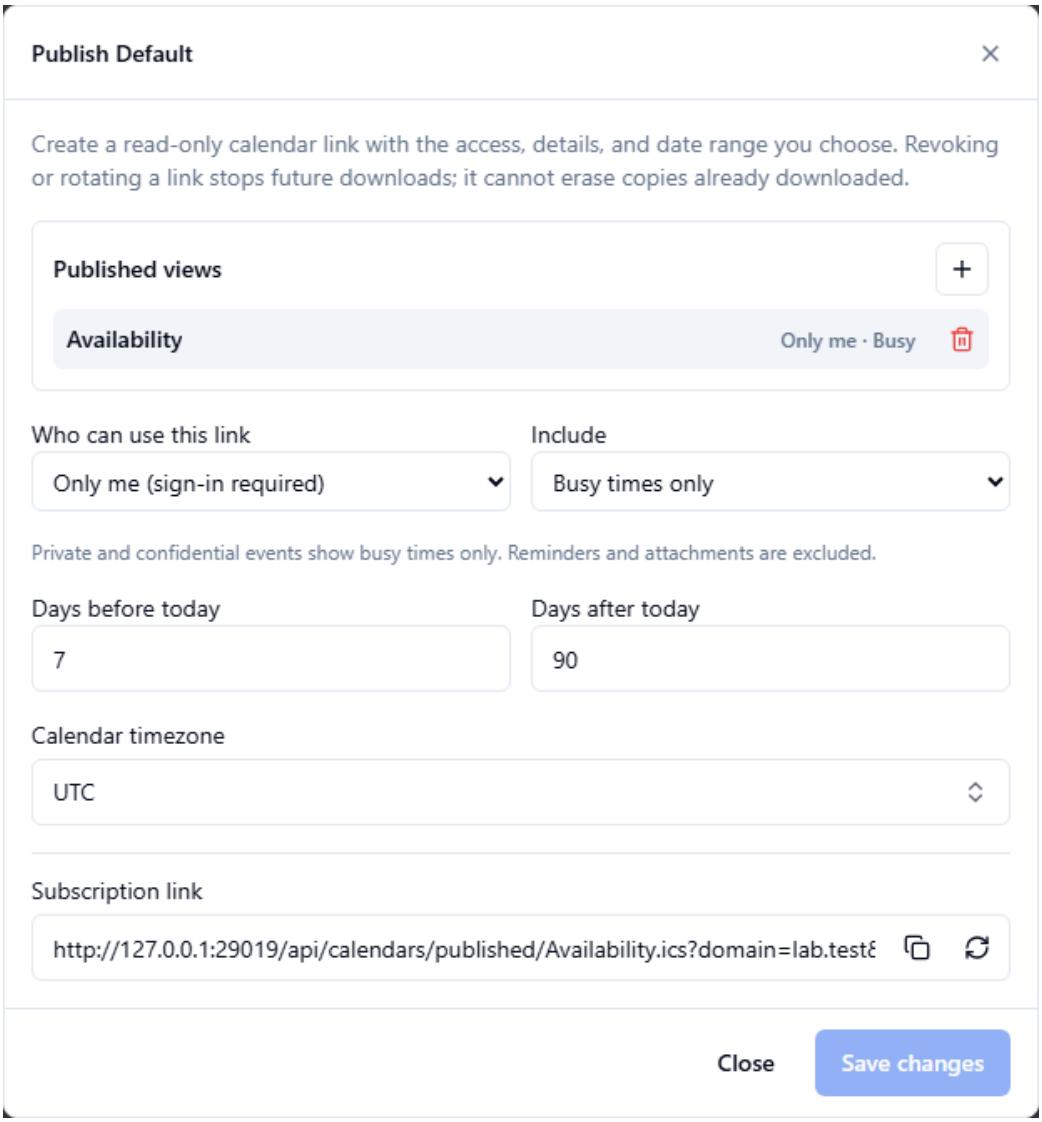

Figure 16 Calendar publishing settings

Subscribing to an external calendar

In ExpressPro's calendar controls, choose Subscribe to calendar. Enter a name and supported calendar feed URL, choose the refresh interval, and save. The server downloads and validates the feed. A subscription appears as a read-only calendar; edit the original at its provider.

Refreshes preserve event identities and support recurring events and timezone definitions. A changed valid feed replaces its previous content, including withdrawn events. A failed download or malformed feed leaves the last successful content visible. Review the reported refresh error instead of assuming unchanged content is current. Delete the subscribed calendar to unsubscribe.

Ordinary public HTTPS feeds are the default deployment. URL checks block disallowed private-network destinations and unsafe redirects. Private-network feeds require an explicit server policy exception. Fetch time, redirects, response size and event count are bounded; a feed that exceeds a limit fails without silently truncating its events.

Background refresh is scheduled for subscriptions used by the server; it does not scan every mailbox during startup. After migrating, open the subscribed calendars and confirm a successful refresh. Recreate legacy subscriptions and published links rather than relying on old calendar metadata being imported automatically.

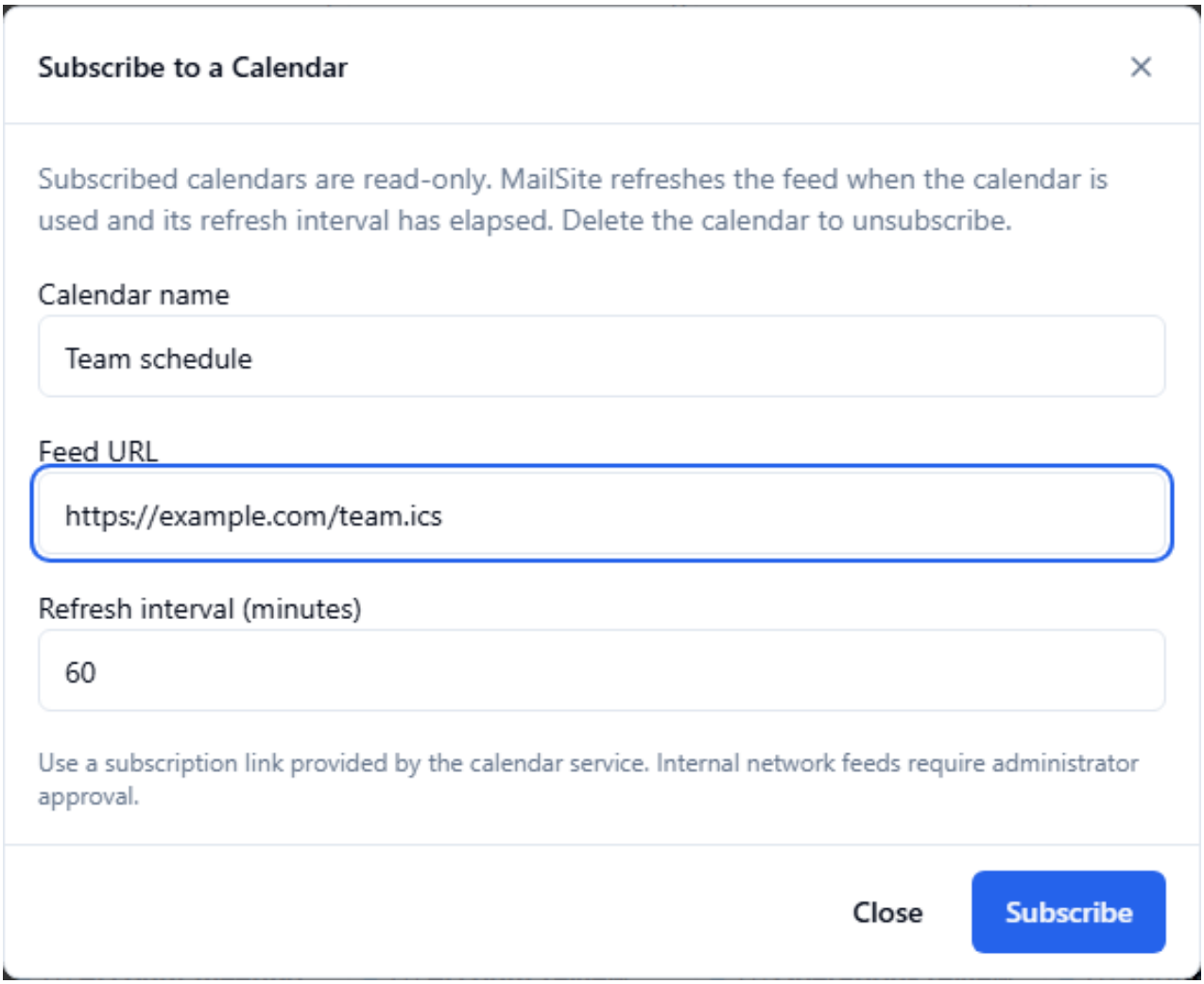

Figure 17 External calendar subscription

Upgrade published links and subscriptions

MailSite 10 publishing.dat records and /Calendars/WebCal URLs are not imported or redirected automatically. Republish calendars, distribute the new links and recreate external subscriptions in ExpressPro. Existing legacy files remain available as migration reference. Opening a subscribed calendar activates its refresh scheduling; confirm a successful refresh after upgrading.

Mailboxes

A mailbox combines an account definition with its message, contact and calendar storage. Account information is held by the active configuration backend. Mail content and the current mailbox databases are managed through MSDBMA; their configured paths may be outside the installation directory.

Types

Native accounts use MailSite-managed credentials in registry or SQL configuration. Windows-backed accounts authenticate through Windows. External database accounts use the configured Generic or Emerald source. The active configuration connector and account authentication type are separate choices. Available choices also depend on licensed capabilities.

Creating a mail account does not itself grant Windows file-system or interactive-login permissions. Windows-backed authentication requires an existing eligible Windows identity and appropriate service-account/domain access; the current Console does not offer the old NT user/group selection wizards.

Adding mailboxes

Open Console, Domains, the domain, then Mailboxes and choose Create Mailbox. Enter the account name, type and required credentials. Open Properties to configure the mailbox's services, security, delivery actions and other settings. For external database accounts, configure and preview the source from Server, External Database Mailboxes, then create selected eligible accounts.

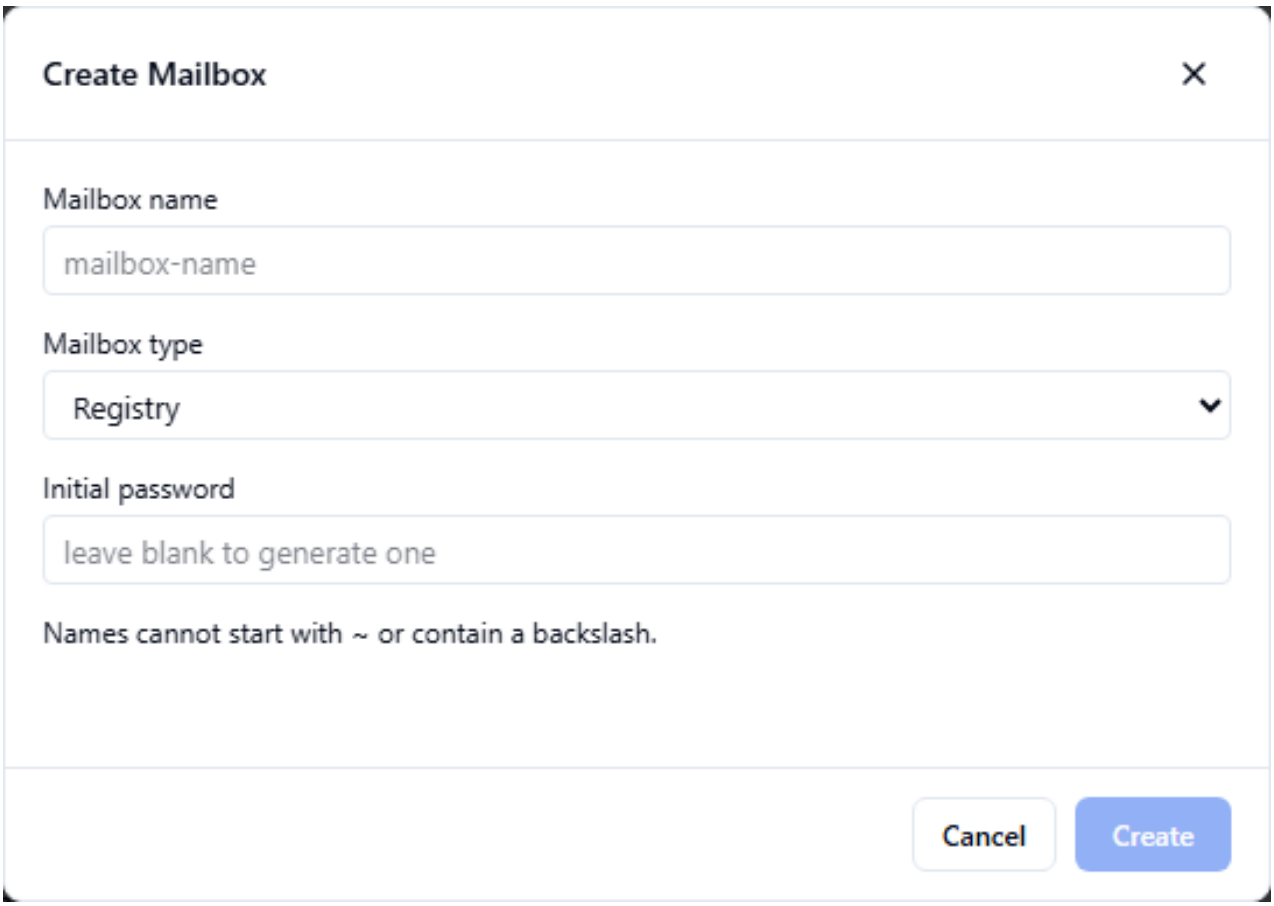

Figure 18 Creating a mailbox

Verify login and delivery with the intended authentication method before enabling the account for general use. Configure aliases separately. The available Alias controls depend on the active configuration connector.

Postmaster and catchall accounts

The default postmaster account supplies an administrative destination. Domain postmaster handling and catchall rules can affect mail addressed to names that do not otherwise exist. Configure the intended account or forwarding explicitly and test both the domain-specific and default-domain cases; do not rely on a successful submission alone as proof of the final destination.

A catchall routes otherwise unknown local recipients when applicable. Domain forwarding, list/account name collisions and the active connector can affect recipient classification; see Delivery Precedence. A catchall is not a substitute for configuring each intended account.

Converting mailboxes

The legacy MSBOX -plugin operation is not implemented in the current utility and returns an unsupported-operation error. Do not follow the old bulk conversion example. Changing configuration storage, provisioning an external account, copying account settings and migrating mailbox content are distinct operations.

Use the supported SQL connector and MSIMPORTEXPORT workflows for configuration migration. Preview external accounts without overwriting native identities. A change of authentication authority or physical mail location requires a planned migration with a backup and access checks; it must not be inferred from a type selector.

Automatic reply and forwarding

Open the mailbox's Auto Reply and Delivery Actions settings. Configure the reply text, reply address, one-time behavior and whether to include the incoming message according to your policy. For a vacation reply, use a bounded absence message and verify that repeated mail does not generate unwanted repeated replies.

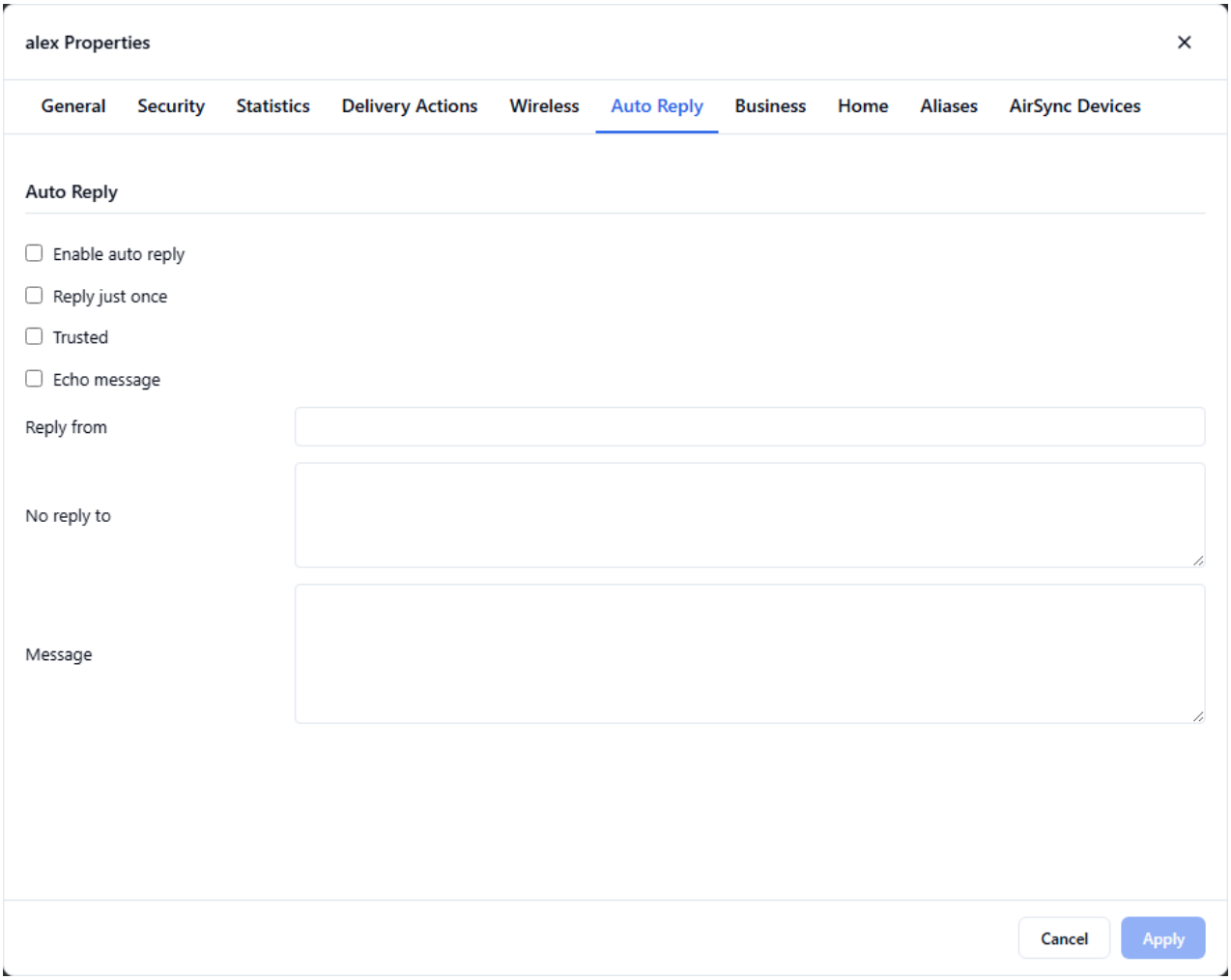

Figure 19 Automatic reply settings

Forwarding directs incoming mail to the configured recipients; retaining a local copy is a separate choice. Check the forwarded destination and local-copy result using test mail. Avoid creating loops through aliases, forwarding or automatic responders.

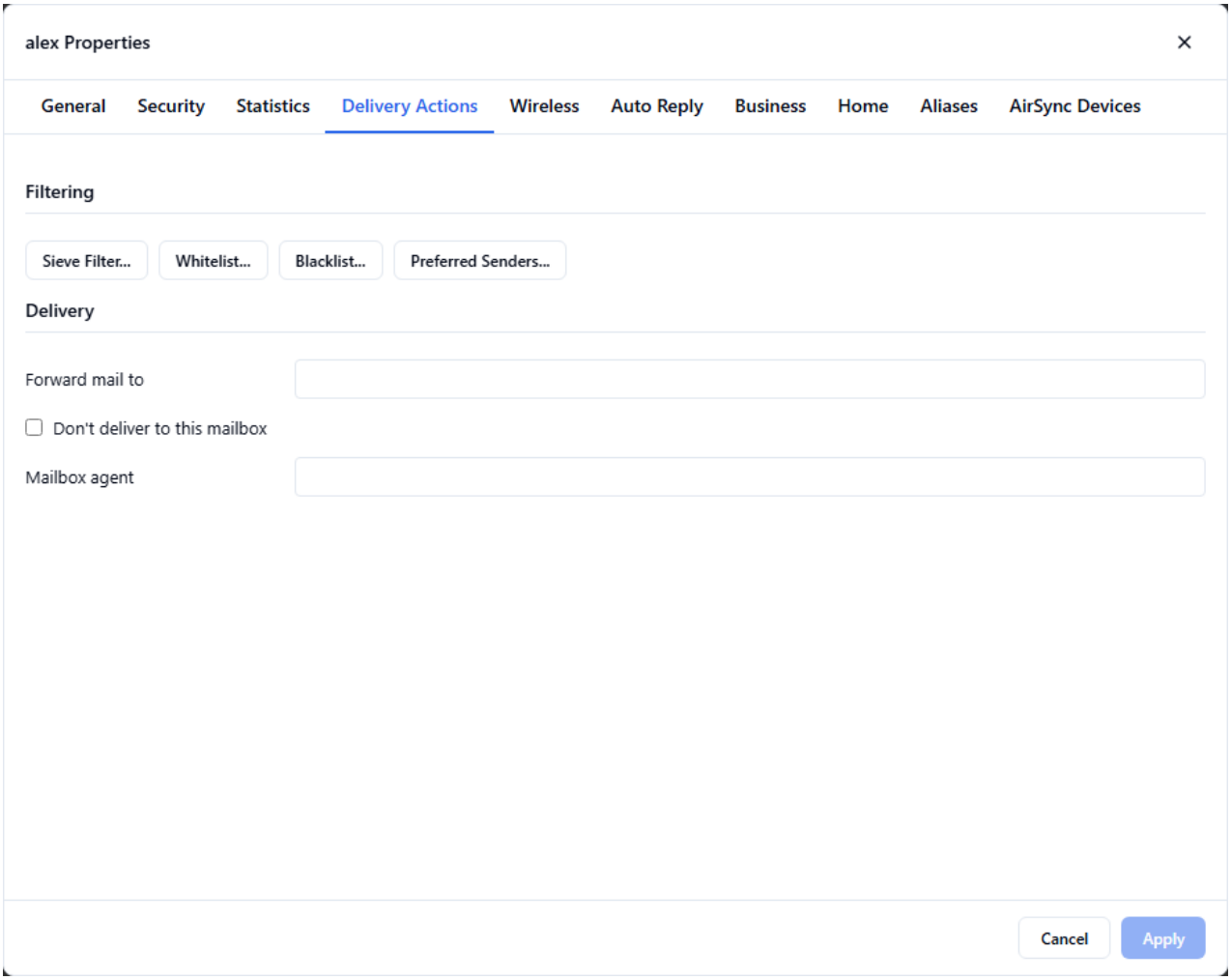

Figure 20 Mailbox delivery actions

Mailbox quotas

Quota and warning settings can be configured at server, domain and mailbox scope. Inspect the effective account settings and current usage before changing a limit. Over-quota handling depends on the configured policy; a warning threshold is separate from rejection. Deleting or moving mail must complete before usage and new-delivery behavior can be assessed.

Web mailbox administration

Connect to the configured public HTTPS address and sign in to ExpressPro. Open Console when your account has administration privileges. The old port-90 Web Console and its automatic Mailbox Properties landing page are not the v11 workflow.

Server administrators manage all permitted server resources. Domain administrators manage resources in their domain. Ordinary mailbox users use their account settings; a moderator email address does not grant Console administration privileges. Use the actual interface and role checks to verify the intended access.

Mail Lists

A mail list distributes an accepted message to its current subscribers. Members may be local mailboxes or external addresses. Configuration and member resolution are shared through MSDBMA; SMTPDA delivers accepted posts through the normal mail queue.

Types

Native lists store members in MailSite's active registry or SQL configuration. Text-file, Windows-group, external database and server-mailbox sources resolve their members from the selected provider. Switching MailSite's configuration connector is separate from selecting an external membership source.

Creating and managing a list

Open Console, Domains, the domain, then Mail Lists. Create the list with its intended membership source, open Properties and configure policy before enabling it. Use Members to inspect resolved addresses. A membership-source error is displayed above the tabs and must be corrected; it is not an empty subscriber list.

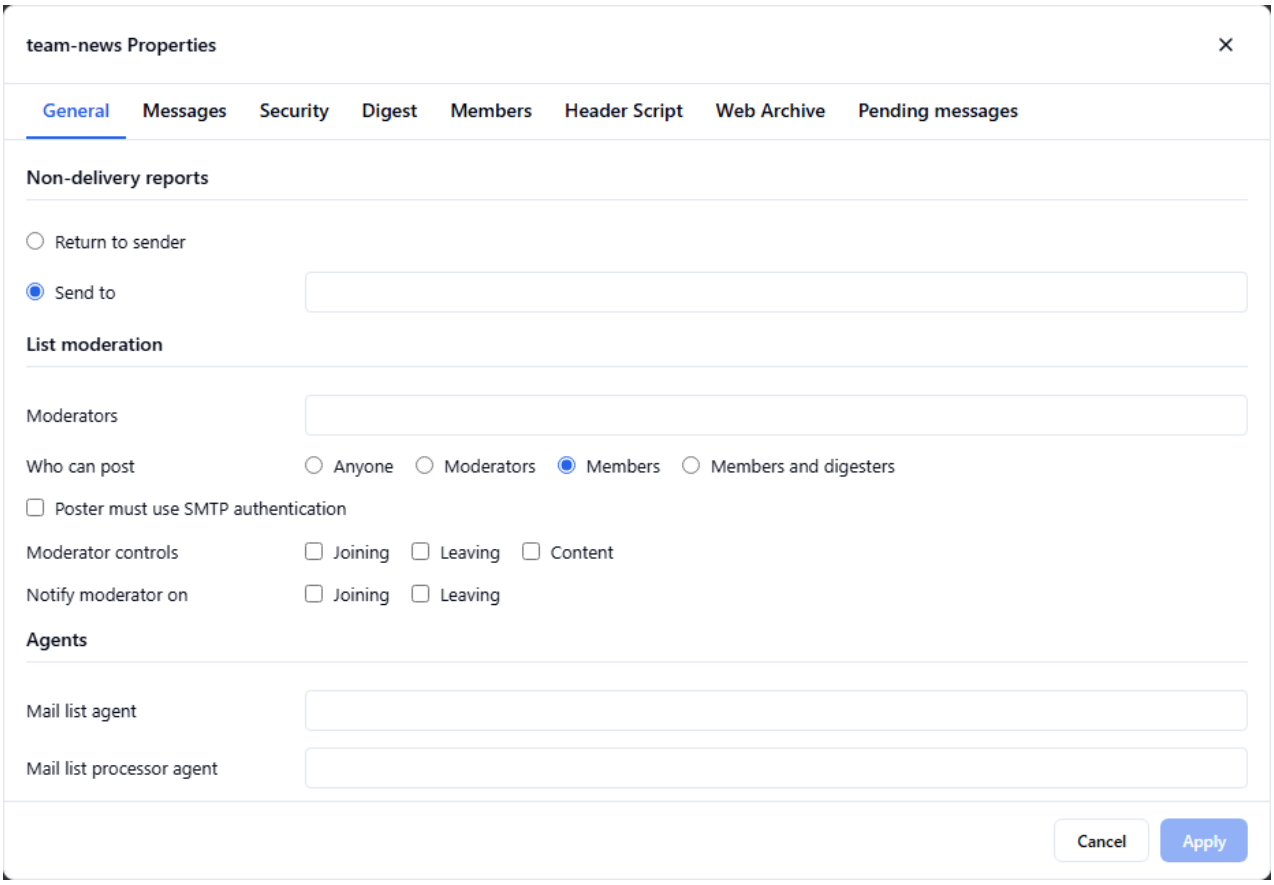

Figure 21 Mailing-list general settings

Use Rename or Delete from the list actions when needed. The current Console has no list Copy or Move command. Configuration transfer with MSIMPORTEXPORT can move selected list configuration, but it does not migrate archived messages or pending delivery files.

Mailing-list delivery and moderation

Open Console, expand the domain, select Mail Lists, and create or open a list. Add native members on the Members tab, or configure a supported external source. Set Who can send, maximum message size, moderators and bounce handling before enabling the list.

On General, Reply-To header has three choices: keep the original, use the list only when Reply-To is absent, or always use the list. Sender and bounce-envelope settings are separate. A sender confirmation excludes that author from the ordinary subscriber copy and returns a wrapped confirmation instead.

Accepted posts go to eligible local and remote subscribers through the normal mail queue. Repeated addresses are deduplicated within a list. Nested lists retain loop markers; a person reached through two different lists can still receive two copies. An empty list produces no subscriber mail. Temporary delivery failures stay queued for retry.

For moderated content, configure a moderator address and enable Content under Moderator controls on General. A domain or server administrator opens Pending messages, downloads the original for review, and selects Approve or Reject. Approval queues delivery; rejection removes the post without a reply to its author. Receiving a moderator notification does not itself grant Console access.

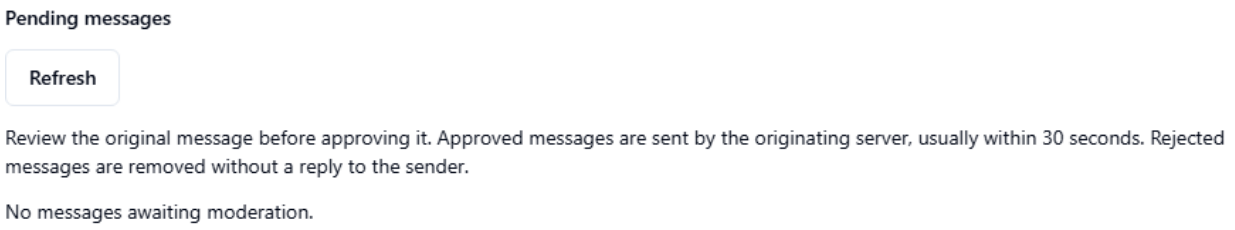

Figure 22 Mailing-list moderation review

Digest subscribers and list migration

Create a companion list whose name ends in -digest, such as team-news-digest, and put digest subscribers there. Posts to team-news are accumulated for the companion list as well as distributed to ordinary members. Direct posts to the -digest address are rejected.

On the companion list's Digest tab, select a frequency, subject template and whether to include a table of contents. Hour/day/month values use quantity followed by unit, such as 1H or 1D. Periodic delivery uses UTC period boundaries; the one-minute option uses 0H. An empty frequency disables timed emission; a configured size threshold can still trigger a digest. Digest settings do not enable content moderation.

The originating transport node emits approved messages and digests in the background. Normal restarts retain pending work and completed-delivery evidence. Restart with the same machine identity and spool location; automatic takeover by another node is not supported. Disabling a list pauses its pending delivery.

New held source messages are limited to 32 MiB. Queue and digest batches are bounded. Inspect the server log when a configured list does not drain; a failed list does not prevent other lists from being processed.

Before migration, drain old pending posts and digests. Review custom header/body scripts. Header ADD, REMOVE, REWRITE, conditions, bounded jumps and ABORT are supported. Arbitrary process execution and the legacy INCLUDE/EXECUTE body directives are not supported; replace those customizations before enabling the list.

Dynamic mailing-list membership

Choose the membership source when creating a list. Native membership is stored in MailSite. The built-in alternatives resolve their current source in the storage service, so Console, delivery and command-line enumeration use the same membership.

- Text file: configure the file path on the source tab. Use UTF-8, UTF-8 with BOM, or UTF-16LE. Addresses may include display names. Invalid entries are skipped and duplicate addresses are removed. Convert legacy ANSI files explicitly. Adding/removing a member updates the file; preserve service-account read/write access.

- Windows group: configure the local or domain group and group type. Windows account names become addresses in the list's domain. Membership is read-only in MailSite and depends on the service identity's Windows permissions. Validate domain/nested-group access against your own Active Directory environment.

- Database: configure a 64-bit ODBC data source, credentials and query. A custom membership query returns email address first and optional display name second. The default query reads EmailAddress and FullName from the list-derived table name. Optional join/leave statements support %1 for the quoted address, %2 for the derived table name, and %% for a literal percent. Display-name edits remain source-managed.

- Server mailboxes: configure mailbox/domain masks and a privilege mask. Comma-separated masks use first-match order; ! excludes, * matches any sequence and ? matches one character. This source is read-only. Privilege bits are 1 for users, 2 for domain administrators and 4 for server administrators.

An unavailable source is an error, not an empty membership result. Check the displayed error, source permissions, 64-bit ODBC configuration and server log. Database timeouts are bounded. Custom membership DLLs and legacy SQL member-property update statements require migration work rather than automatic execution.

Mail list processor commands

Send request commands in the message body to listname-request@domain. Use HELP for the list's configured help, SUBSCRIBE listname@domain to join, UNSUBSCRIBE listname@domain to leave, and STOP to stop processing the rest of the body. JOIN and LEAVE are aliases. The list's multiple-command, moderator and membership-source policies still apply.

REVIEW exposes membership only under the configured moderator policy. Extended join/leave operations require the corresponding setting and moderator authorization. Moderated membership changes are forwarded to the moderator; an administrator must make the permitted source change. They are distinct from the Pending messages queue for reviewing message content.

Windows-group and server-mailbox membership is source-managed and cannot be edited by request mail. Text and database sources permit changes only when their configured file permissions or join/leave statements support the action.

Messages and scripts

The Messages tab stores help, welcome/farewell and message prefix/suffix text. Prefix and suffix directives apply to supported plain-text bodies; they do not rewrite multipart, HTML or base64 content. File inclusion and process-execution directives are not supported in the v11 list path.

Header Script supports ADD, REMOVE, REWRITE, conditional jumps, labels and ABORT. It has a bounded execution limit. See Appendix C for syntax and the effect of the Trusted setting.

Archiving and list agents

Mailing lists can run an external program before normal processing and publish a static web archive. Only a server administrator can change external program or archive settings. New archive pages are written below HypermailDir in a mailsite-v11 subdirectory; existing Hypermail files remain unchanged. Publish that new directory through your chosen web server. See Agents and Appendix B for prerequisites, retry behavior and migration limits.

Pending data and restart

Pending content and digest data are managed by MSDBMA. Do not edit or delete their files to approve, reject or retry a message. Use the Console's Pending messages controls and inspect service logs when delivery is delayed. Restart with the originating machine identity and spool path; automatic takeover by another node is not supported.

Domains

A MailSite server can host independent mailbox domains and additional names for the same domain. Choose the relationship first, then configure DNS, accounts and routing consistently. Use a fully qualified account name such as joe@example.com when signing in to avoid ambiguity between hosted domains.

Synonym domains

A synonym delivers corresponding addresses into the same underlying domain. For example, joe@example.net can identify the same mailbox as joe@example.com when example.net is a synonym of example.com. It does not create a second independent mailbox or duplicate its stored messages.

Configure synonyms in the owning domain's Properties, Synonyms page. Verify the public DNS records and incoming delivery for every advertised name. See Delivery Precedence for the relationship between synonyms, aliases and mailbox lookup.

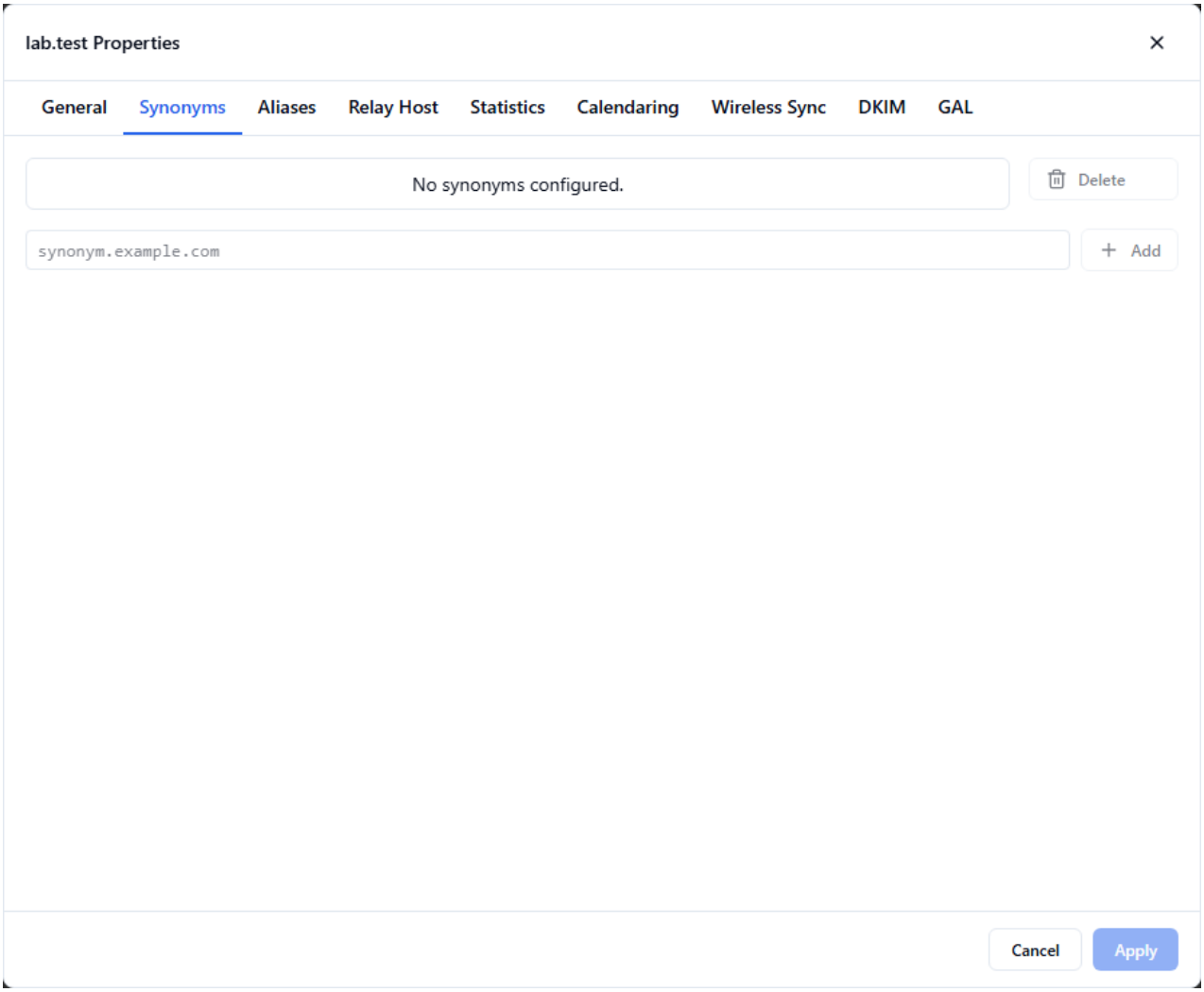

Figure 23 Additional names for a domain

Independent virtual domains

Independent domains keep separate mailboxes and mailing lists. They can share the server's IP address or use separately configured addresses. Sharing an IP does not merge their accounts. Each advertised mail hostname must resolve to the intended listener, and each domain's MX records must direct incoming mail appropriately.

Open Domains in the Console, create the domain, and review General settings and any address binding. Create the intended mailboxes and postmaster/catchall policy in that domain. Do not assume a bare username or a service greeting selects the intended domain across every protocol.

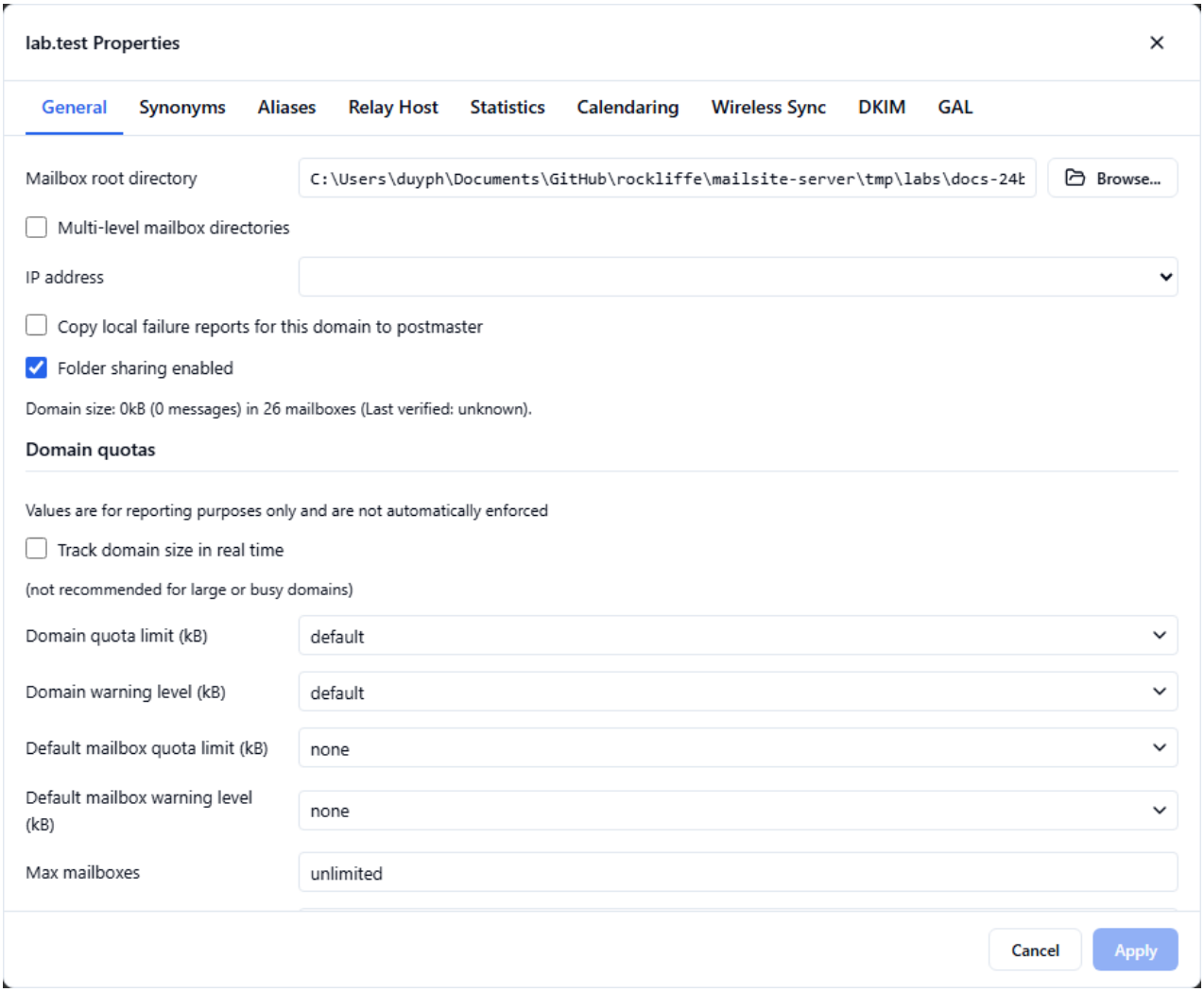

Figure 24 Domain general settings

Default domain

Review the server's configured default domain when handling unqualified account names or addresses. Use the current Console domain actions for any supported rename and test account login, local delivery, aliases and public DNS afterward. A renamed domain in MailSite does not update external DNS or client profiles automatically.

Forwarding domains

The Domain Relay Host setting routes the domain toward another mail server. Confirm the destination hostname, port, DNS and relay permissions, and avoid routing loops back to the same gateway. Test both a known recipient and a rejected recipient; accepting a message at the gateway does not prove final delivery.

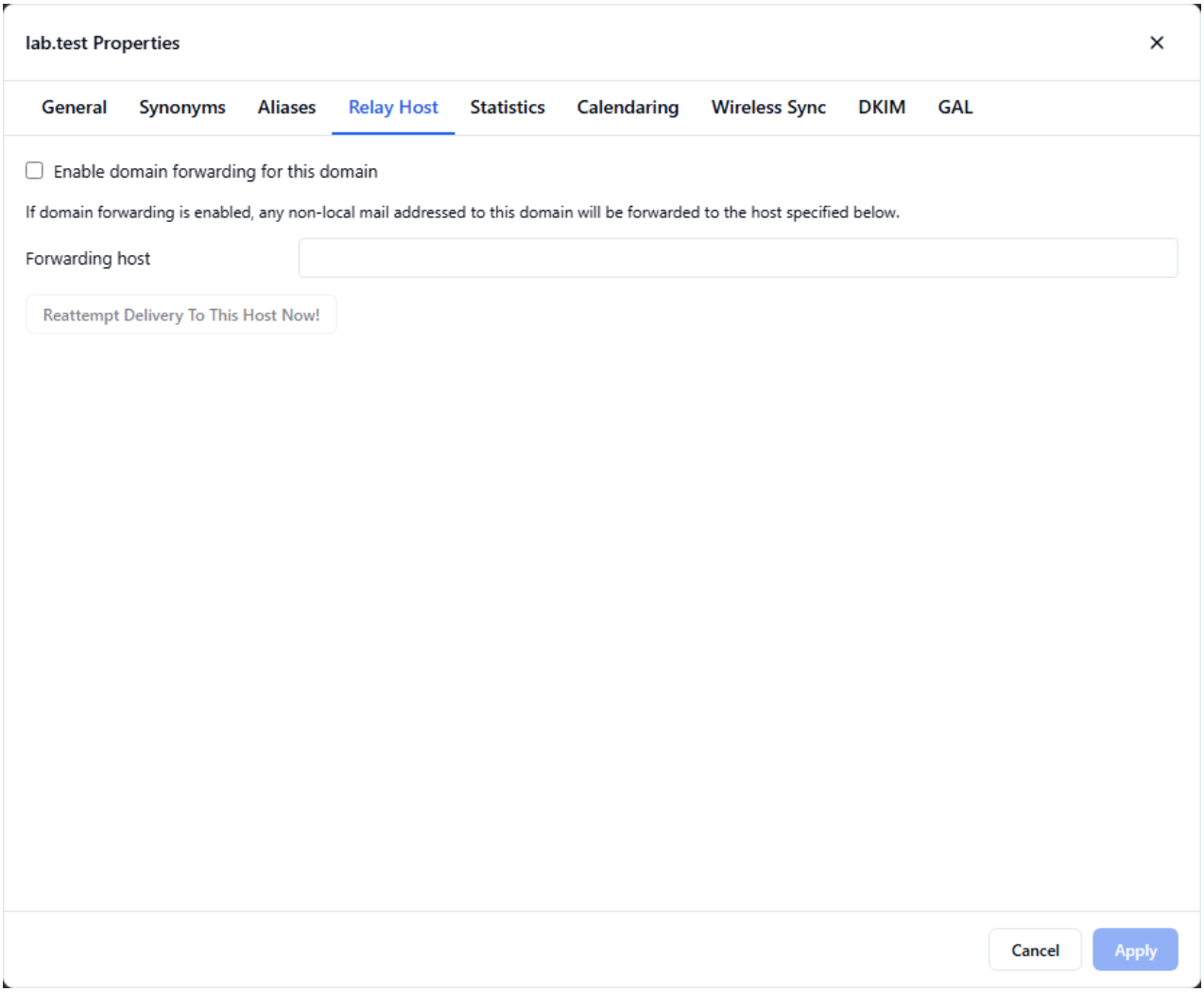

Figure 25 Domain relay destination

Verify the configuration

Send and receive test mail for every independent domain and synonym. Check authentication with the full account name, local and remote routing, TLS certificate hostnames and any domain-specific policy. Use the recorded queue result and service logs to distinguish DNS, connection, policy and account failures.

Aliases

An alias is a rule that redirects messages sent to an address in a domain hosted by MailSite to another address. Aliases can be configured in MailSite Console by double clicking on the Aliases icon within the Server folder. The following dialog will be displayed:

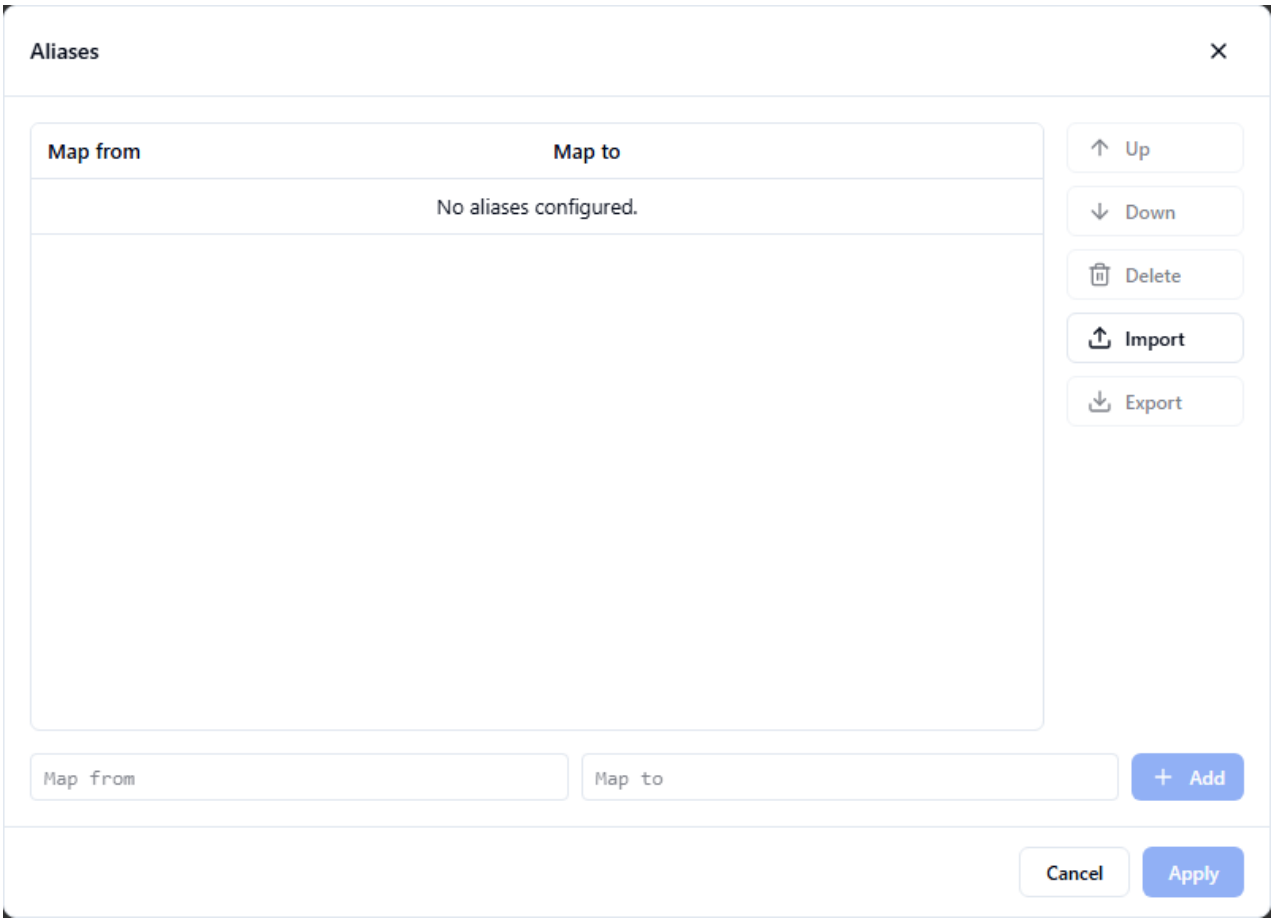

Figure 26 Aliases

When MailSite processes a message, it first checks the addressee's name against this list. If a matching entry is found, the message will be redirected to the replacement address that is specified in this table.

Setting up an alias

In the Map from field (bottom left), type the address that you wish to redirect (for example, jane@mycompany.com). In the Map to field (bottom right), type the address to which messages should be sent (for example, j.smith@abc.com) . Then click the Add button. Once this alias is added, any message sent to jane@mycompany.com will be redirected to j.smith@abc.com.

If you omit the domain part from the Map from field, the default domain is assumed. Note that the domain name of the Map from field must be the name of a virtual domain, or of the default domain. You cannot use the alias mechanism to redirect mail addressed to a recipient elsewhere on the Internet.

Deleting an alias

Select one or more aliases in the list box and click Delete.

Wildcard aliases

You can specify wildcards in the Map from field. This can be used to redirect mail for all names matching a pattern. For instance, specifying T*Y would match Tony, Tiny, toby, terry, etc. (Note that matching is not case sensitive.)

You can also specify a single wildcard as the first character of the Map to field. This will be replaced by the actual addressee's name when the table entry is used. For instance, if the Map from is f* and the Map to is

*-blue@abc.com, then a message for fargle@thismachine.mycompany.com will be redirected to fargle-blue@abc.com

Map table order

The order of entries in the map table is significant. It is processed top-to-bottom, and the first matching entry is used. Thus, more specific entries (i.e. those not containing wildcards) should be positioned near the top of the list, and less specific entries (those containing wildcards) towards the end of the list. Use the Up and Down buttons to move entries around.

Importing and Exporting

The list of aliases may be exported and imported to and from text files using the Export and Import buttons.

Aliases versus Synonym Domains

Synonym domains are discussed in the preceding section. There is some similarity between synonym domains and aliases. For example, an alias of the form

@xyzcompany.com -> *@xyz.com

has the same effect as a synonym of xyzcompany.com for the virtual domain xyz.com.

The advantage of using synonym domains comes when you need to use aliases in addition to them. For example, if you have synonyms of abccompany.com and abcinc.com for the virtual domain abc.com, you can alias an individual user (say jim@abc.com) to another address using a single entry in the alias table such as:

jim@abc.com -> james.smith@abc.com

Because synonym domains affect aliases the same way that they do mailboxes, the addresses jim@abccompany.com

and jim@abcinc.com are synonymous with the alias jim@abc.com shown above.

Mailbox Aliases

In addition to system-level aliases described above, MailSite supports assigning aliases to each mailbox. Mailbox-level aliases allow sites to more easily manage accounts with multiple e-mail addresses. This type of alias is supported only for SQL mailboxes.

To assign aliases to a mailbox, open the mailbox using the MailSite Console and select the Aliases tab:

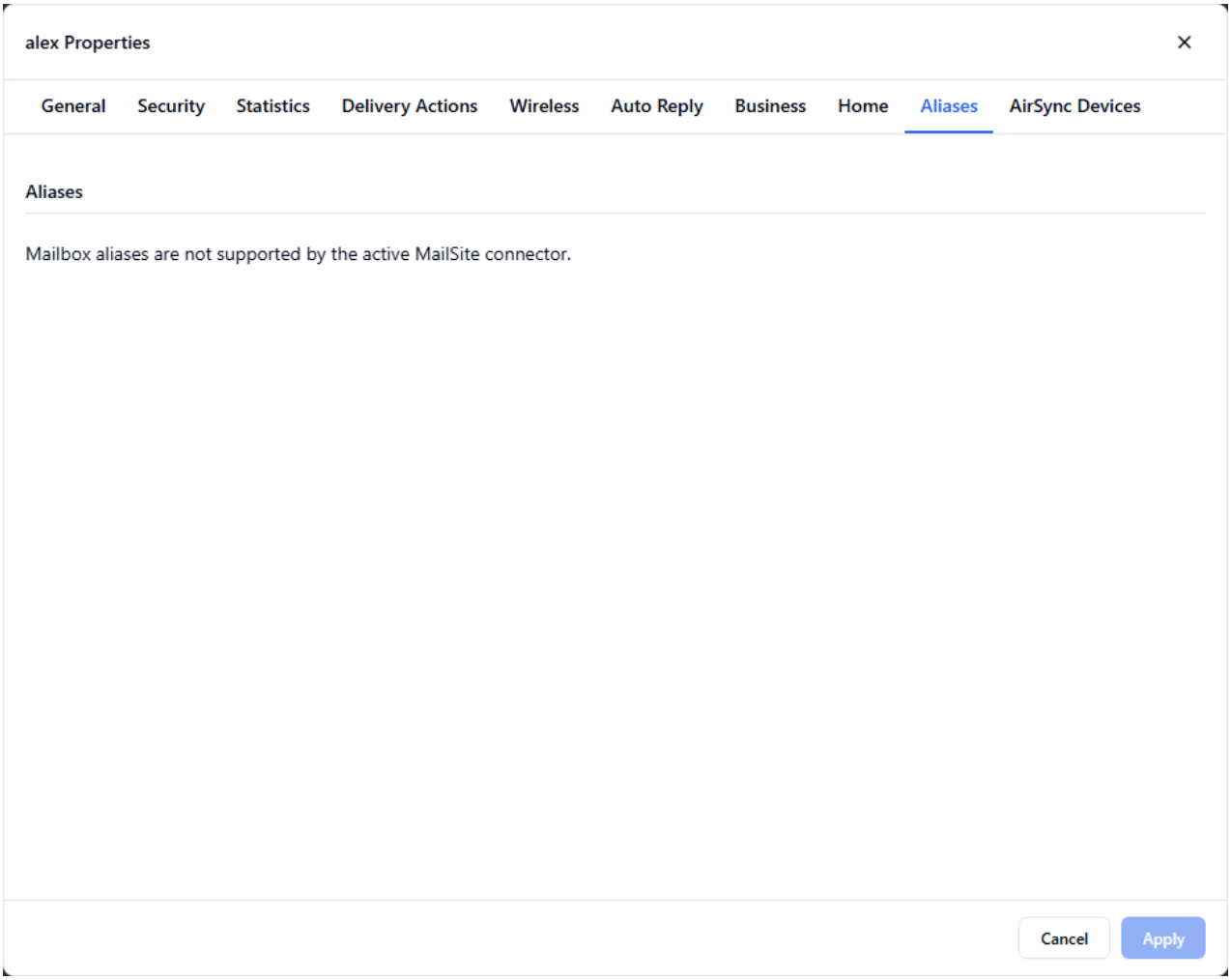

Figure 27 Mailbox Aliases

Mailbox-level aliases must be include a local domain name defined in MailSite. Mail that arrives for any mailbox alias will be delivered to the mailbox exactly as if they had been addressed to the account's main e-mail address.

Viewing Mailbox Aliases

You can view all of the mailbox-level aliases created for SQL mailboxes in a specific domain by opening the Domain Properties window and selecting the Aliases tab:

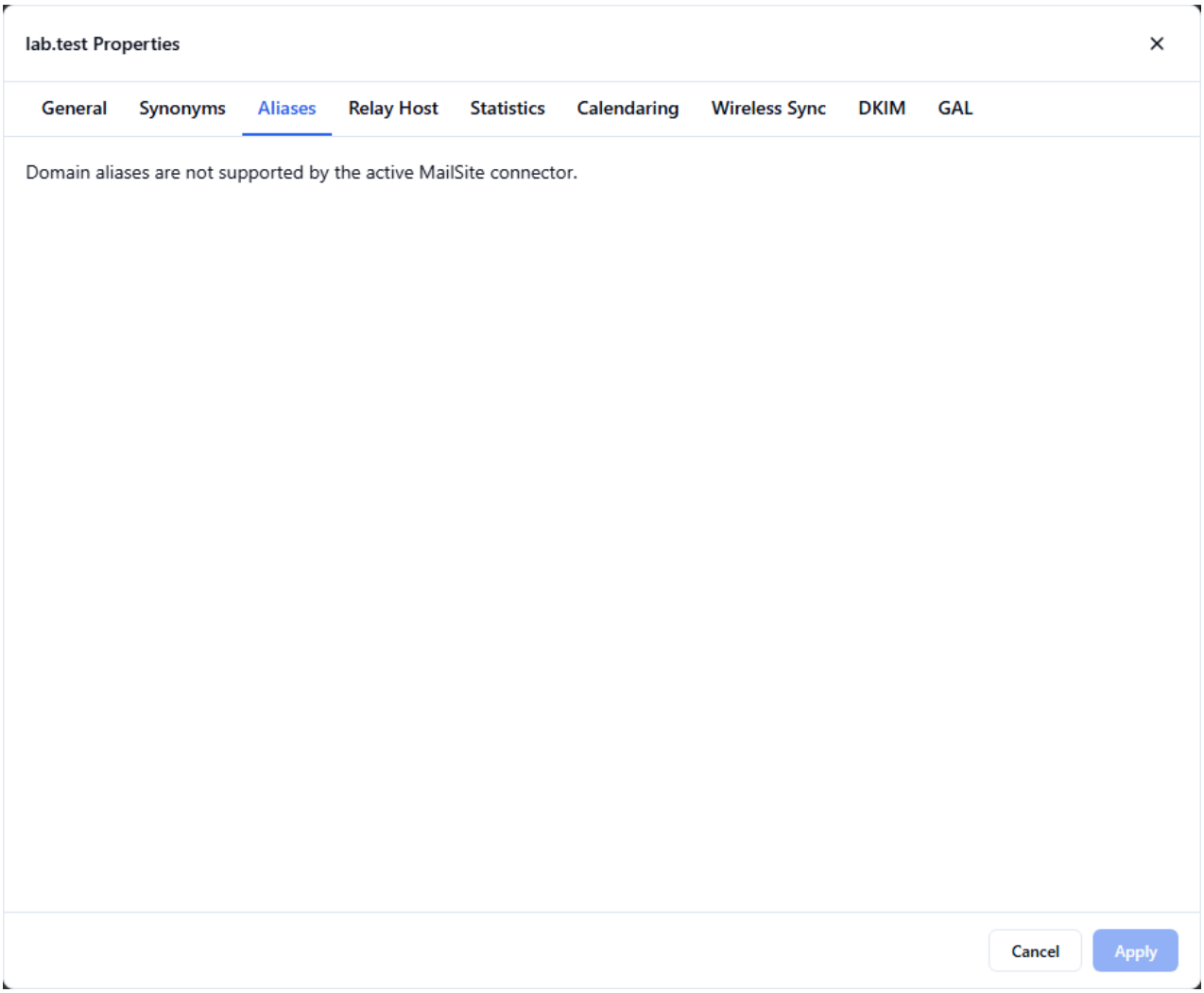

Figure 28 Viewing Mailbox Aliases

Note that the aliases shown on this page are read-only and cannot be modified at the domain level. To modify mailbox-level aliases, open the mailbox associated with the alias.

Delivery Precedence

MailSite distinguishes SMTP recipient acceptance from delivery of a queued message. Do not use the old single flowchart as a complete description of both stages.

Recipient classification

For a local recipient, SMTPRA checks mailing lists before mailboxes when the configuration's ClusterVariant is not 4. With ClusterVariant 4, it checks the mailbox first. If neither matches, it checks domain forwarding and then catchall handling. Domain and default-domain catchall configuration can affect otherwise unknown recipients.

Queued delivery

SMTPDA resolves system aliases and then routes recipients through its list, local-mailbox and remote-delivery paths. Alias expansion, domain forwarding, address collisions and catchall policy must be tested together on the connector and topology in use. The old guide's unconditional list-before-mailbox diagram omitted the connector-dependent recipient-classification case.

Mailing-list delivery

Accepted list submissions are expanded to eligible members under list policy. Duplicate addresses within one list are removed, and nested lists carry loop markers. Separate noncyclic lists may each deliver a copy to the same person. Temporary member-source and delivery failures retain work for retry; completed expansion evidence prevents ordinary restart from replaying a finished distribution.

Intermittent Connectivity

MailSite can queue mail while a destination is temporarily unavailable. Current SMTPDA retries queued delivery through ordinary network connectivity. It does not implement the previous Windows RAS dial-up subsystem, connection-trigger commands or time-of-day/per-domain dial-up scheduling.

Queued delivery

Inspect the recipient's recorded error and next retry before intervening. Temporary connection or remote-server failures are retried; permanent failures are handled as delivery failures. Configure the supported elapsed retry schedule and retain appropriate delayed/failure notification policy.

Use the Console queue controls or MSRETRY to request another attempt after restoring connectivity. Repeatedly forcing retries will not repair an invalid recipient, a DNS problem or a remote relay restriction.

Incoming delivery triggers

An SMTP server that supports ETRN can be asked to start delivery using MSSTART after connectivity exists. The target's ETRN policy determines whether authentication or a trusted host is required. MSPOP can retrieve mail from a remote POP mailbox, subject to its routing and retention options. Neither command activates the retired MailSite dial-up scheduler.

Migration from dial-up installations

Establish and manage network connectivity outside MailSite. Review any old NoDialupDomainMask, time-of-day, phonebook and trigger settings as migration data. They remain in configuration but do not provide current dispatch behavior. The original reference manual preserves the historical procedure for systems still running that implementation.

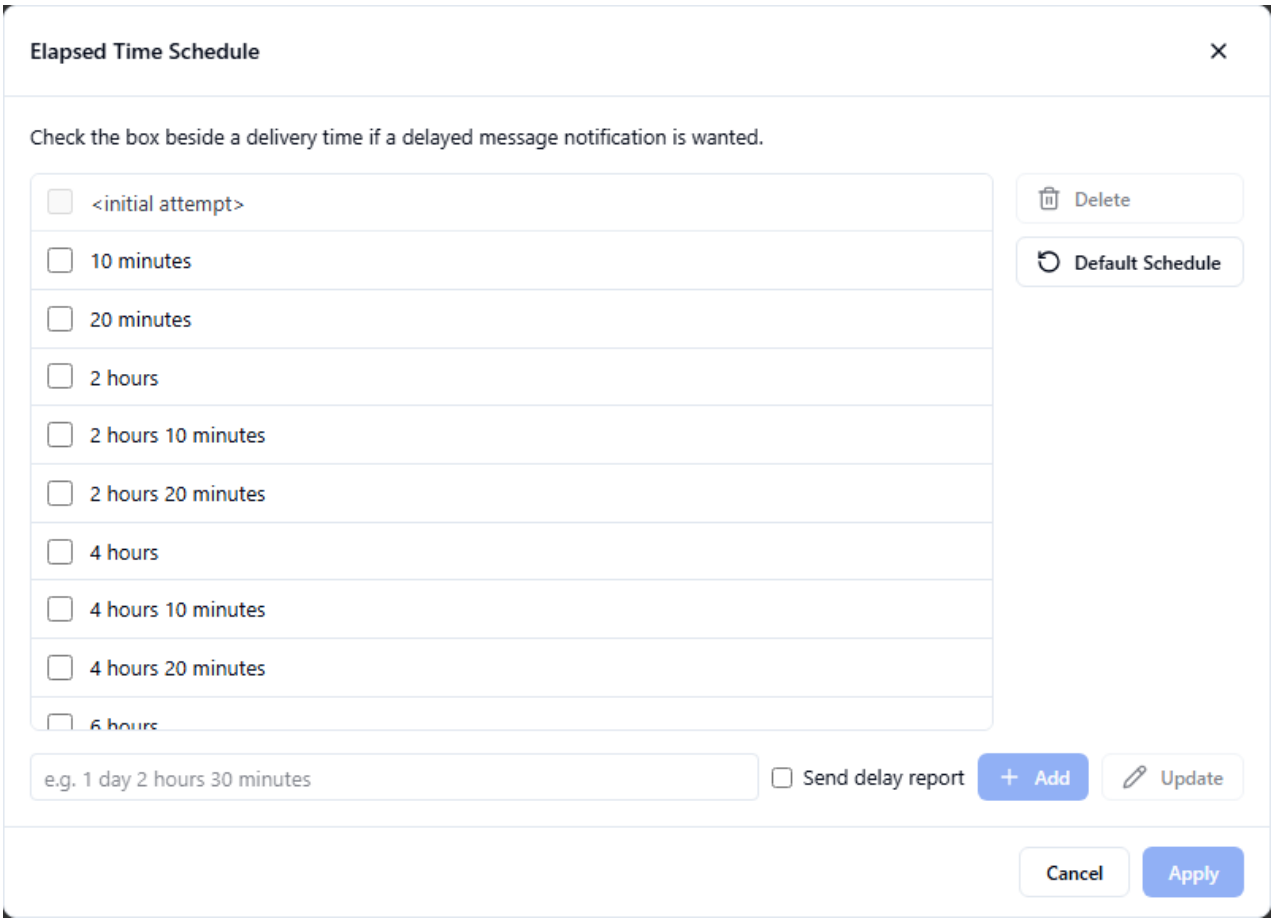

Figure 29 Elapsed retry settings

Backup

Back up the complete installation state needed to recover MailSite: configuration, live mailbox files, mailbox databases, mail queues, certificate keys and chains, and service configuration. The data can reside outside the program directory; inventory the actual server and domain paths before defining the backup job.

Back up configuration with MSBACK

The release includes MSBACK for exporting and restoring registry-backed MailSite configuration. It does not back up message files, mailbox databases, queues or TLS private keys. SQL configuration installations must use SQL Server backup; MSBACK rejects that connector.

Run the installed utility with an output filename to export configuration, for example:

```
msback.exe C:\Backup\mailsite-configuration.txt
```

The v11 utility connects through MSDBMA, so MSDBMA must be available during export or restoration. Unlike the old guide's sequence, do not stop every MailSite service before invoking MSBACK. Prevent configuration changes while establishing the recovery point; export configuration while MSDBMA is available, then stop its clients and MSDBMA for the offline data copy.

MSBACK also accepts -restore and the optional -deleteold switch. Restoration replaces configuration and can affect service access; validate the complete restore procedure on an isolated recovery installation before using it on the live server. Consult the installed utility's usage output for the exact build and retain the pre-restore configuration.

Export configuration for migration

MSIMPORTEXPORT exports selected configuration from registry or SQL through MSDBMA. For example, use msimportexport -export config.xml -server -domains -mailboxes -maillists. Protect the XML as a credential-bearing backup. It excludes messages and does not replace a database/data backup. Restore using explicit selectors and verify the destination's storage connection, permissions and dependent sources; see Appendix A for destructive replacement options.

Create a consistent recovery point

Use a backup procedure that produces a consistent view across the mailbox files, databases and configuration. For an offline backup, schedule maintenance, stop the MailSite protocol services and workers, then stop MSDBMA before copying the owned data. Start MSDBMA before its clients when returning to service.

If configuration is in SQL Server, include the SQL database and the information required to restore access. Preserve the Windows service identities, directory permissions and any external resources they depend on. Protect backups containing passwords, message content and private keys.

Test restoration

Restore to an isolated server and verify configuration, mailbox access, mail delivery, contacts and calendars before relying on the backup. Prevent the recovery test from sending mail or answering production client requests. Check the service versions and database compatibility rules before opening restored data.

Development database resets

Some MailSite 11 beta upgrades cross an explicitly declared reset boundary. A reset is not necessarily a lossless index rebuild. Live message, contact and calendar files can remain while database-only

Outlook data, flags, identities, settings and synchronization state are discarded. Retain a recoverable pre-upgrade backup and review the release-specific impact before proceeding.

Do not delete Databases directories as a generic repair step. MSDBMA reports failed, newer or unrecognized database state; diagnose the reported state and follow the applicable recovery procedure.

Security

Mail transport, user authentication and administration require explicit security policy. Configure encrypted client connections, relay restrictions and access to stored messages. Then verify that legitimate users can work and unauthorized sessions are rejected. The settings in this chapter complement the TLS and scanning chapters.

Message Store Security

Mail content, indexes, configuration exports and logs can contain private messages and credentials. Restrict their directories to the service identities and administrators that require access. Review the actual account used by each installed service and grant the required filesystem and network access; the old installer's Simple/Secure policy labels are not the current installer choices.

Use the supported backup workflow for both live message files and authoritative v11 databases. Keep backups separately protected. Do not use manual edits or deletion of current database/index files as an account-repair procedure. See Backup and the release's migration notes before restoring older data.

Password Security

Require an encrypted connection before sending credentials: HTTPS for the web interface and the configured TLS connection for mail clients. SMTP AUTH authenticates a connection but does not itself encrypt it. APOP or a legacy challenge-response example is not a replacement for validating transport security.

Use a separate ordinary mailbox account for routine mail access rather than a privileged Windows administrator identity. Protect credentials in scripts, XML configuration exports, process command lines and backups. Windows-backed password changes use Windows policy and service-account permissions; external database changes use the configured provider workflow.

Review authentication failures in the current service logs and test access restrictions from a normal user's session. Change compromised credentials and revoke affected sessions as appropriate to your incident procedure. The old MailSite Password Server and Windows NT performance-counter instructions are not the current v11 administration workflow.

MailSite Security

MailSite includes numerous security features that allow you control the flow of mail to your site. These include features to block junk email (a.k.a., “spam”), combat third-party relay, and verify the identity of end users who send mail through your site. Setting proper security policies is one of the most important tasks for email administrators, and is crucial for those whose mail server systems are accessible from the Internet.

MailSite security settings are invoked by double clicking on the Security Properties icon in the MailSite Console. You can also use an Anti-Relay Wizard and SMTP Security Wizard to assist you in setting these policies.

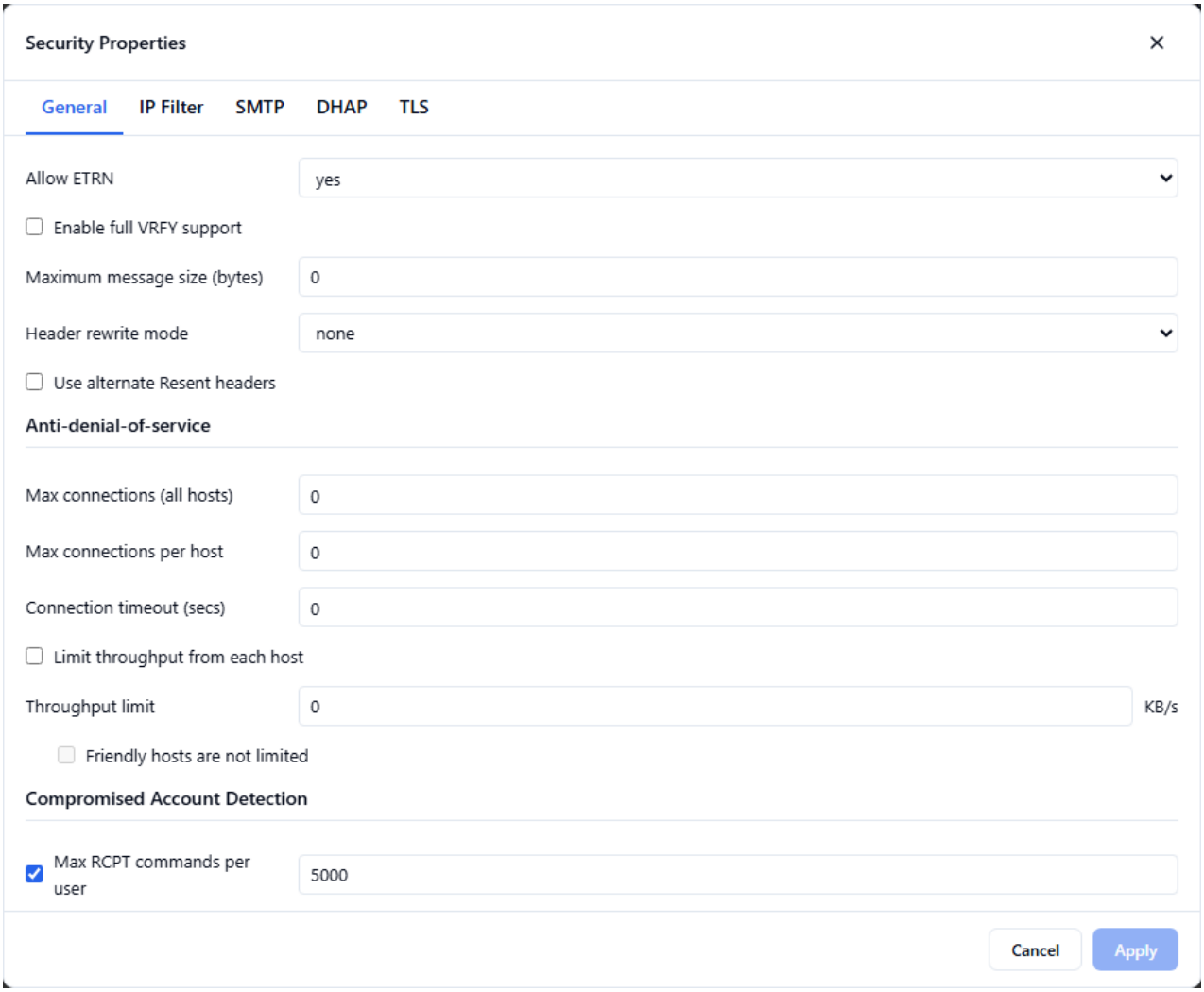

Figure 30 MailSite Security

General Security Settings

Included among the options in the General Security Properties window are the following general security preferences:

Enable full VRFY support

By default, an SMTP command of the form VRFY name@domain.com will return a “success” response if the server will accept mail for domain.com, regardless of whether the name is valid. If you check the Enable full VRFY support box, then the command will only succeed if name@domain.com is a valid mailbox or a mail list (or is an alias). If you leave this box unchecked, it reduces the amount of information an attacker or spammer can find out about your users. For that reason, it is recommended that you do not enable this option.

Authenticated ETRN

The SMTP ETRN command is used to request an SMTP server to start sending mail for a particular domain. (This command is used by the MSSTART utility.) If you check the Authenticated ETRN option, then the SMTP client must be authenticated (using the AUTH command with a valid mailbox name and password), otherwise the ETRN command will be rejected.

Maximum Message Size

The maximum message size in bytes that the SMTP Receiver will accept. The default is 0, which means that there is no size limit (apart from memory and disk space constraints). To prevent excessively large messages from impacting your system, it is recommended that you set this value to 10 MB (10,000,000 bytes) or less.

Anti-Denial of Service Policies

In addition to spam and relaying, denial-of-service (DoS) attacks are a significant threat to the smooth operation of a mail server. DoS attacks involve one or more systems bombarding your SMTP server with millions of connections and/or messages. These attacks can cause you mail server system to perform very poorly as it tries to cope with the exceptionally high loads.

MailSite includes policies that allow you to contain DoS attacks to prevent them from overwhelming your server system. The anti-DoS features provided in the MailSite Security window are the following:

Max connections (all hosts)

This setting provides a limit to the total number of incoming SMTP connections that MailSite will respond to at any time. When this number of connections are active, SMTPRA will no longer accept new connections until a current connection has been closed.

Max connections per host

This setting limits the number of incoming SMTP connections allowed from any one system. When this number of SMTP connections from any one host are active, SMTPRA will no longer accept new connections from that host. This option is very useful for containing potential damage from an abusive system without blocking incoming connections from other (non-abusive) systems.

Connection timeout

This option sets a limit to the number of seconds that MailSite will keep open a non-responsive SMTP connection.

Limit throughput from each host

This option provides a throttle on the amount of data (in kilobytes per second) that SMTPRA will accept from any one host. This allows you to control DoS attacks that send large amounts of data over relatively few connections. When using this option it is recommended that you exempt your “friendly” hosts from this limit to avoid slowing mail traffic from your own network.

SMTP Security Properties

MailSite’s SMTP Security policies allow you to block mail from specific hosts or users, and include the following options:

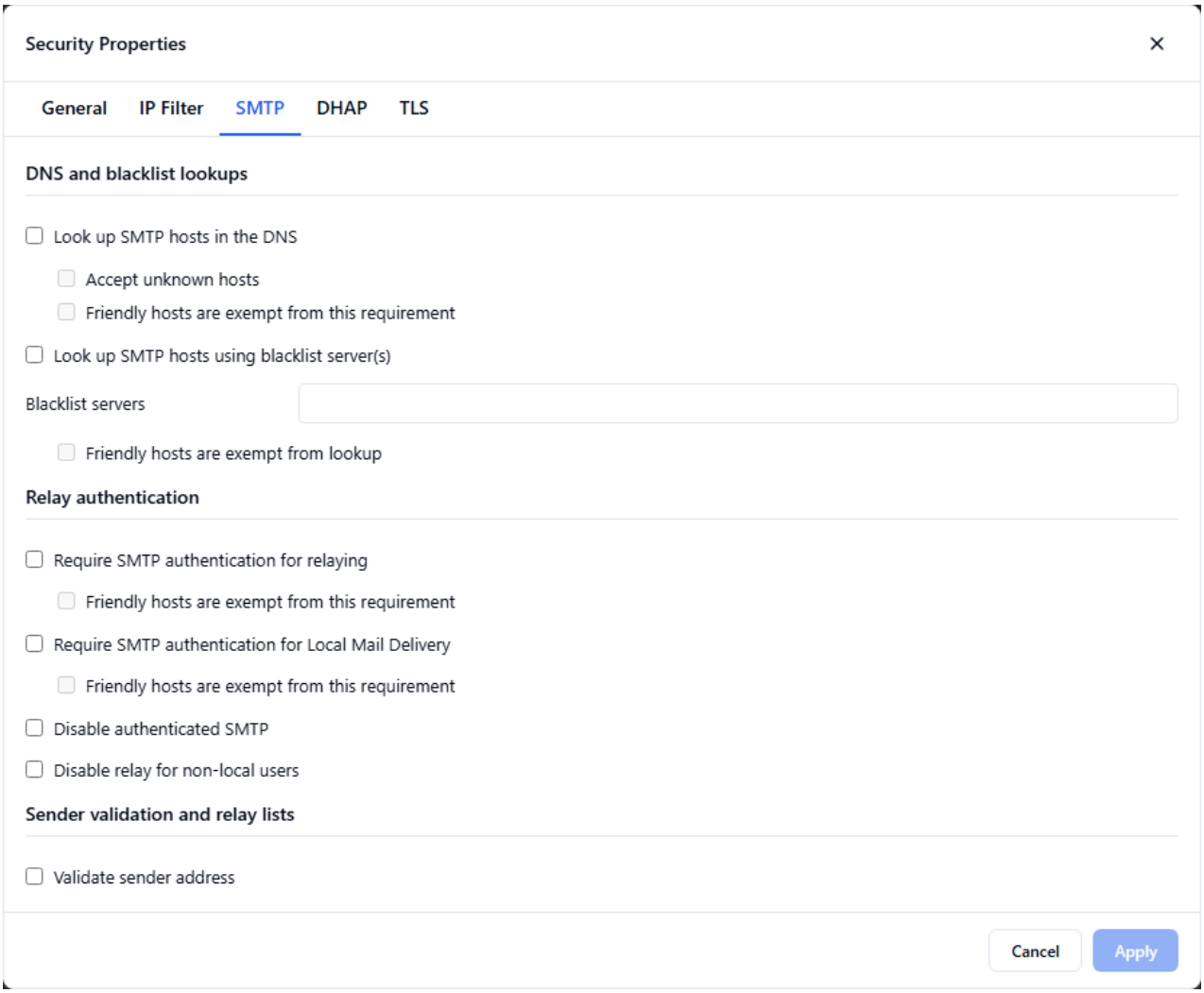

Figure 31 SMTP Security Properties

Block mail from unknown hosts. Most legitimate sources of email are hosts that can be located in the DNS. In other words, these machines are well-established and correspond to known host.domain names. Many systems used to distribute spam are not defined in the DNS, and are accessible only through TCP/IP address (i.e., 12.34.56.78). Be aware that blocking mail from unknown hosts is a very conservative policy and may lead to legitimate mail being blocked from your users.

Block mail from blacklisted hosts. Sources of high-volume spam are tracked by blacklist services, which provide lists of sites that have been responsible for such mailings. MailSite allows you to block all messages from hosts named by a blacklist service, and also allows you to select the blacklist service you wish to use. The default service is the MAPS Realtime Blackhole List (RBL). Use of this feature is recommended for ISP sites. IP addresses known to belong to legitimate users can be added to the DHAP whitelist by the administrator. When this is done, the RBL lookup is bypassed as it is considered unnecessary.

Block mail from specific hosts. In addition to unknown hosts and blacklisted hosts, you can block mail from any other source. You can choose to block mail from servers based on hostname or IP address. As with other

blocking methods, this prevents the named system from sending any mail – spam or otherwise – to your site, so it should be used conservatively.

Block mail from specific users. Mail can also be blocked from specific users, as defined by the envelope return address (MAIL FROM). This option is particularly useful if one or more specific users are sending junk mail to your users. When blocking addresses, you can use wildcard notation (*@domain.com) to block mail coming from all addresses within a domain.

Set maximum recipients per message. Because spam is typically sent to large numbers of users, setting a maximum on the number of recipients per message allows you to combat mass mailings. When you set a limit to the number of recipients, messages sent to more than this number of addresses (as given by the RCPT TO command) will have all recipients after the maximum number rejected. For example, if you set a maximum of 20, and a message arrives for 50 of your users, only the first 20 users will receive the message.

All of these policies can be set in the SMTP tab of the Security Properties window. MailSite also provides an SMTP Security wizard that leads you through the process of implementing an anti-spam strategy for your site. Using the wizard is highly recommened, particularly for new users. For more information, double-click the SMTP Security Wizard icon in the MailSite Console's Server:Security folder.

Experienced users can also use mask lists to specify hosts and addresses which should be blocked from sending mail to your site. These lists can be opened from the SMTP Tab of the Security Properties window by clicking the buttons Reject all incoming mail from these addresses, and Reject all incoming mail from these hosts. See the following section on Advanced SMTP Security for more information.

Mail Filters (described in the following chapter) provide an additional mechanism to combat spam. Filters allow you to search the contents of the message (headers, body, and attachments) for specific content and block it from entering your system. For example, using filters you can reject all mail that contains the subject "Make money fast!", regardless of the host used to send the mail.

Anti-Relay Policies

Along with spam, mail administrators must contend with a type of abuse known as third-party relay. Relay occurs when your mail server accepts a message addressed to another site and sends it to the proper destination. Third-party relay is a scenario in which a distributor of junk mail uses another site's mail server to distribute his/her mass mailing. This can result in a loss of your network resources and can even cause your site to be blacklisted as a source of spam.

To combat third-party relay MailSite includes policies to restrict relaying, including:

Require SMTP authentication for relay. The simplest technique for combating third-party relay, this option requires that users provide a login name and password that matches a mailbox on your site before they are allowed to relay mail to other sites. You can also specify that users connecting from "friendly" sites (for example, your own network) are exempt from this requirement.

Allow relay only from specific hosts. This option specifies the hosts from which relay is allowed. Typically, this is a range of IP addresses that correspond to your own network. When relay is allowed only from your own network, third-party relay from outside your network is prevented.

Disable relay for non-local users. This option disallows relay if the return address of a message is not within one of your domains.

Require valid return address for relay. This option disallows relay if the return address of a message contains an unknown domain (or a domain for which no mail records exist in the DNS).

Allow relay to specific domains. This option allows MailSite to accept relay for specific domains, such as friendly sites. This allows you to set strict relay-prevention policies while still allowing delivery to domains for which your site is a gateway.

As with anti-spam features, all of these relay policies can be set in the SMTP tab of the Security Properties window or with a wizard. Because of the complexities of relay, it is highly recommended that administrators use the Anti-Relay Wizard to set these policies. For more information, double-click the Anti-Relay Wizard icon in the MailSite Console's Server:Security folder.

Experienced users can also use mask lists to specify hosts and addresses for which relay is allowed or disallowed. These lists can opened from the Security window by clicking the buttons Accept mail for relay to these domains, and Accept mail for relay from these friendly hosts. See the following section on Advanced SMTP Security for more information.

SMTP Authentication

As described above, SMTP authentication is one of the best ways to combat third-party relay because it requires that relay is permitted only for authorized users of your site. Because it requires a login name and password, SMTP authentication makes relay as secure as POP3 and IMAP4 mailbox access. However, this option requires that your users have mail clients that support SMTP authentication, which is not included with all clients.

When using SMTP authentication, you can also specify that users are exempt from this requirement if they are within your own network (or from other specific hosts). This allows you to support your dial-up users whose mail clients do not support SMTP authentication.

Require SMTP authentication for Local Delivery

This is a very conservative approach, and should be used with great care. Internet standards require servers to accept mail for local delivery without authentication, otherwise it would be virtually impossible for servers to relay as the sending server is not able to authenticate. However, on machines which are not externally referenced this option can be enabled, providing the most stringent protection against unsolicited mails.

Directory Harvest Attack Protection (DHAP) Settings

MailSite provides a mechanism for identifying a directory/dictionary harvest attack or DHA (otherwise known as email harvesting) and preventing the attack from continuing for a “block duration” configurable in the MailSite console. When the block duration expires the host regains access but may be blocked again.

When a host is deemed a harvester its IP address, host name, the time of blocking, block duration and the total number of times blocked is written to the SMTPRA log and the host is disconnected.

You may wish to permanently block an IP address that has been identified as a harvesting address using the "Reject all incoming mail from these hosts option" in the SMTP security dialogue or by using your firewall.

Occaisionally legitimate users may be deemed harvesters after mistyping a number of addresses, or if their address book is out of date. To prevent this, known legitimate IP addresses can be added to the DHAP White List.

DHAP settings are invoked by clicking on the DHAP Settings tab in the Security Properties dialog in the MailSite admin console.

For more information on how to configure MailSite DHAP settings, please refer to the Windows Administration Console section of this manual.

Advanced SMTP Security

When setting up SMTP security features you can use the SMTP Security and Anti-Relay wizards to easily set these policies. If you want greater control over SMTP security, you can also modify certain settings directly through the Security window. This section provides information on manually setting spam and relay policies through the use of mask lists.

Using the mask lists

If a call comes in to MailSite’s SMTP server from a host whose name, IP address, or EHLO identification matches the Reject all incoming mail from these hosts list, then all attempts by that host to transfer mail to MailSite will be rejected when the client issues the MAIL FROM command. (Note that you should check the Lookup SMTP hosts in the DNS box to get maximum benefit from this feature.)

If a connection comes in to MailSite from a host that does not appear in the Accept mail for relay from these friendly hosts list, then MailSite will refuse to accept mail from that host for recipients other than local mailboxes, unless the destination mail domain appears in the Accept mail for relay to these domains list.

If a MAIL FROM: command is issued with an e-mail address that appears in the Reject all incoming mail from these addresses list, the MAIL FROM command will be rejected.

Spam Policies

When SMTP mask lists are enabled, MailSite uses these masks to define a spam policy for each SMTP connection. These policies define which (if any) messages will be accepted during the SMTP session. The spam policies used by MailSite are:

AcceptAllMail, which causes all messages to be accepted regardless of sender and recipient.

AcceptLocalMailOnly, which causes messages to be accepted only if they are addressed to mailboxes or mail lists within your MailSite domains.

RejectAllMail, which causes all messages to be rejected regardless of sender and recipient.

RejectAllMailFrom, which causes messages to be rejected only if they are from one or more specific users.

Procedure when receiving mail

The procedure that MailSite follows to determine what to do with incoming mail is as follows:

Connection establishment

When the client establishes an SMTP connection, MailSite does the following:

- If so configured, will look up the client IP address in the DNS, and record the host name.
- If so configured, will look up the client IP address in the given blacklist service.
- Accept the connection by replying with the normal greeting message.

EHLO command

When an SMTP client sends an EHLO or HELO, MailSite determines the spam policy for the connection as follows:

- If the DNS reverse lookup failed, and the Accept unknown hosts flag is not set, the spam policy is

RejectAllMail.

- Otherwise, if the blacklist lookup succeeded, the spam policy is RejectAllMail.
- Otherwise, if the client's IP address/host name/EHLO identification is in the Reject all mail from these hosts list, the spam policy is RejectAllMail.
- Otherwise, if the client's IP address/host name is in the Accept for relay from list, the spam policy is AcceptAllMail.
- Otherwise, the spam policy is AcceptLocalMailOnly.

AUTH command

At this point in the conversation the client may choose to authenticate using the AUTH command. If the spam policy was

AcceptLocalMailOnly, and authentication succeeds, the spam policy becomes AcceptAllMail.

MAIL FROM command

When the client sends the MAIL FROM command, MailSite performs the following:

- If the spam policy is RejectAllMailFrom, it rejects the command with a 5XX response code and an appropriate text message.
- If the Disable relay for non-local users box is checked, it determines whether the return path corresponds to a local mailbox or alias. If not, or if the return path is empty, the spam policy (for this message only) is AcceptLocalMailOnly.
- If the supplied return path is in the Reject all mail from these addresses list then it rejects the command with a 5XX code and appropriate text message.

- If the Validate sender address box is checked, MailSite will attempt to verify the sender address supplied. MailSite will look up the domain name supplied in the MAIL FROM: command, and if it is local, will ensure that the mailbox exists. If the domain is remote, MailSite will ensure that there is a valid A record or MX record in the DNS for it. If not, it rejects the command with a 5XX code and appropriate text message.
- Otherwise, it accepts the command.

RCPT TO command

When the client sends a RCPT TO command, MailSite does the following:

- If the number of recipients exceeds the configured limit, it rejects the recipient with a 5XX reply code and a suitable text message.
- If the recipient address is not local and the destination domain is not in the Accept for relay to list, and if the spam policy is AcceptLocalMailOnly, then the recipient is rejected with a 5XX reply code and a suitable text message.
- Otherwise, accept the recipient.

Security Examples

Here are examples of how to use the Reject all incoming mail from these hosts, Accept mail for relay from these friendly hosts and Accept mail for relay to these domains features for certain situations:

Organization with permanent Internet connection

Reject all incoming mail from these hosts	*.spammer.com known.troublemaker.com
Accept mail for relay from these friendly hosts	*.myco.com
Accept mail for relay to these domains	

This causes all mail which comes on connections from host known.troublemaker.com and hosts with names which match *spammer.com to be rejected. This mail will not reach users within your company.

Mail addressed to non-local users from all other hosts (except those which match *myco.com) will be rejected. This ensures that mail users within the company can use the server to send mail anywhere, while preventing the server being used for mail reflection by others.

Mail received via ISP

Reject all incoming mail from these hosts:	!*.myco.com !*.myisp.com *
Accept mail for relay from these friendly hosts:	123.123.123.*
Accept mail for relay to these domains:	

This causes all mail to be rejected unless it comes on a connection from either the ISP or from within the company. Nobody can send mail out onto the Internet unless their IP address matches 123.123.123.*, but users within the company can use the server for local mail.

ISP relaying mail to customers

Reject all incoming mail from these hosts:	
Accept mail for relay from these friendly hosts:	*.thisisp.com, mailserver.customer.com
Accept mail for relay to these domains:	*.customer.com

The mail server is providing mail services to an ISP's customers, most of whom get their mail using POP, using PC clients with domain names matching *.thisisp.com. Mail from and to them will be accepted. However, the ISP also handles mail for large customers with their own mail server. Mail from

that server will be accepted for relaying, and mail from anywhere else for *.customer.com addresses will be accepted and relayed, no matter which host it comes from.

Security for Mail Lists

You can block mail with a specific From: addresses at a mail list level by excluding those addresses from the list. To do this, use the fields: Don't accept messages from and Don't accept commands from in the List Security Page. For example:

Don't Accept Messages From:	spammer@spamdomain.com !knownperson@evildomain *@evildomain

This setting rejects mail that is addressed to this mail list and from spammer@spamdomain.com. Likewise mail from any user in evildomain (except mail from knownperson@evildomain) would be blocked. All other messages to the mailing list would also be processed as usual.

Don't accept commands from: !me@mydomain,*

This setting rejects all mail to the list-request address unless it is from me@mydomain.

It is relatively easy for knowledgeable people to forge e-mail addresses so that messages appear to come from someone else. This feature will not block these messages.

Refer to the List Security Page in the Console section for more information.

Transport Layer Security

TLS encrypts client and server connections. Configure certificate identity and protocol encryption policy separately. See the TLS certificate management chapter for certificate requests, renewal, certificate sources and activation.

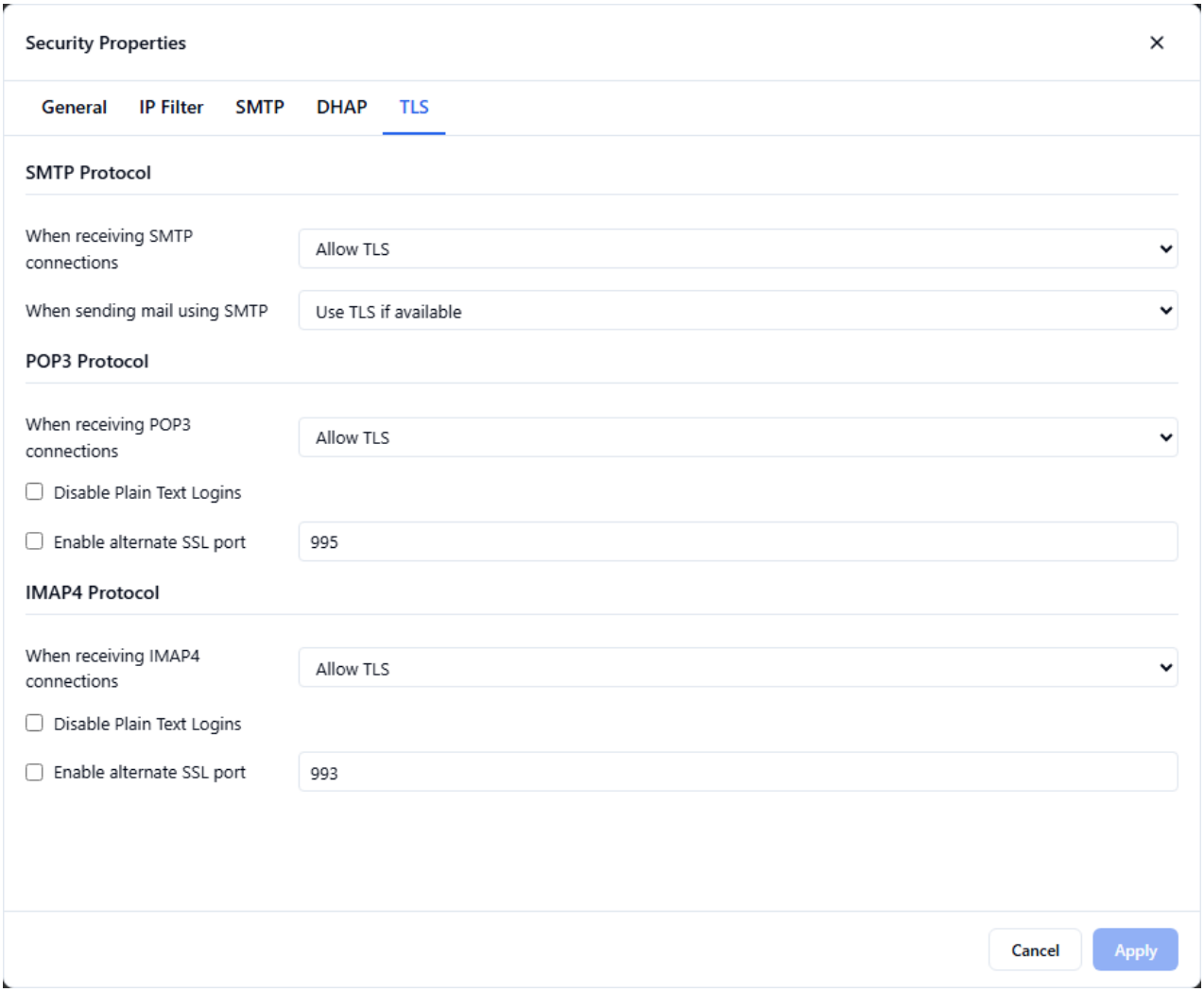

Figure 32 Protocol encryption policy

TLS certificate management

Transport Layer Security (TLS) encrypts connections and allows clients to verify the server's identity. A certificate must cover the hostname the client uses and chain to a trusted issuer. Certificate selection and protocol policy are separate settings: installing a certificate does not automatically require encryption for every protocol.

Certificate sources

MailSite normally loads certificates from its Certs directory under the installation root. Certificate chains use .chain.pem files and their private keys use matching .key.pem files. File-backed certificates take precedence for matching hostnames; Windows-store certificates are also considered for names without matching files, preserving the upgrade path from store-based configurations.

Administrators with a customized deployment can select TLS_SOURCE=win_store for the Windows-store-only path or use TLS_CERT_DIR for another certificate directory. TLS_CERT_PATH and TLS_KEY_PATH select a single explicit certificate and key and must be supplied together. Configure the environment of the actual services, not just an interactive shell, and verify the startup logs after a change.

Restrict private-key access to the identities that need it. Include certificate material and its permissions in your recovery plan. Do not copy a private key into a support report or an issue comment.

Request a domain certificate

Expand Domains, select the domain and open Certificates. On Settings, enter the Contact email, Renew days before expiry and Hostname prefix. Review every generated Certificate Name before proceeding.

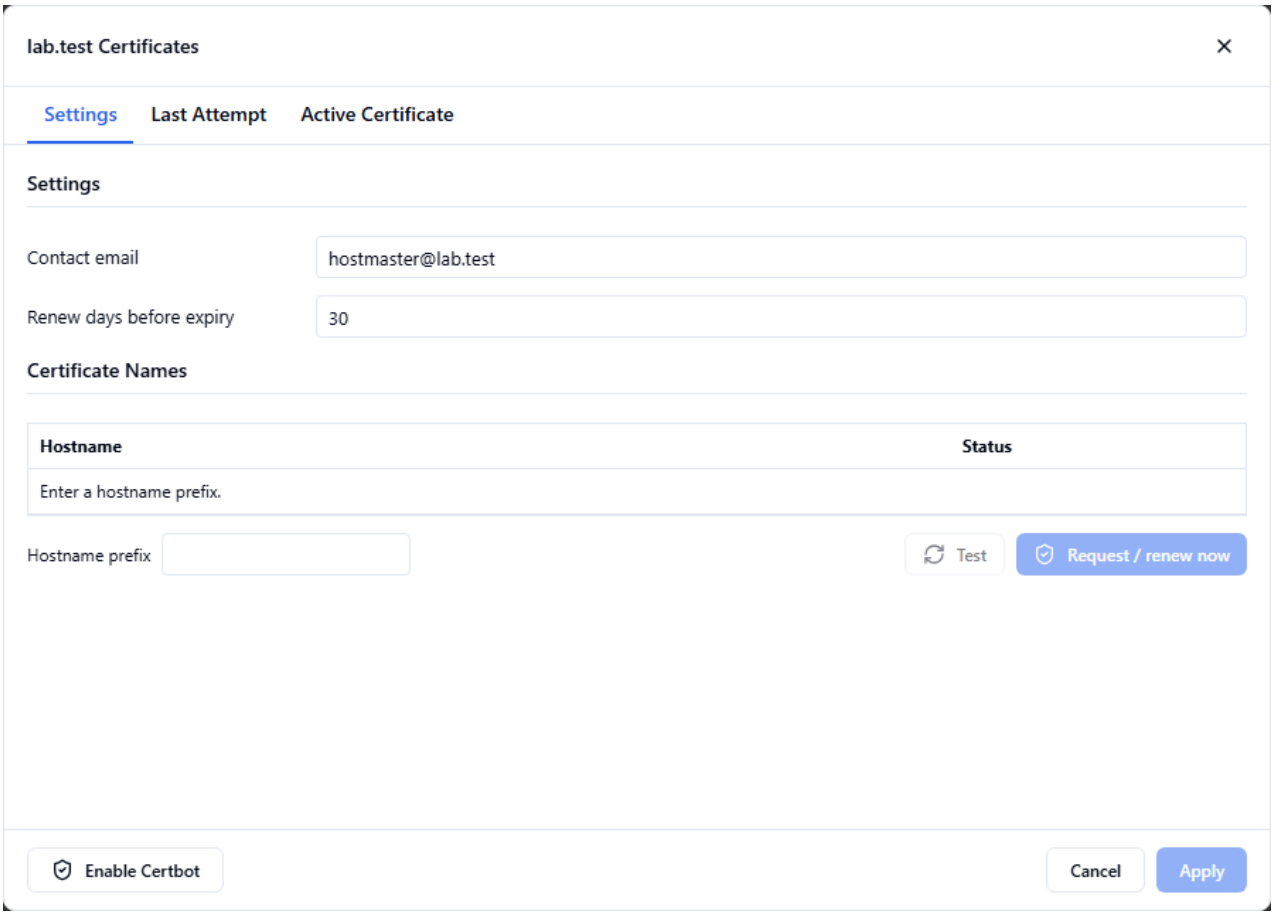

Figure 33 Domain certificate settings

Use Test to check the hostnames. Each name must resolve to the intended server and public port 80 must reach the HTTP-01 validation path. Fix failed checks before requesting a certificate. A rate-limited public probe requires waiting and retrying; it is not evidence that the certificate was issued.

Enable Certbot when using automatic certificate management. Apply the intended settings and use the request control when the prerequisites are satisfied. Certificate issuance is an external operation; follow the result shown by the Console rather than repeatedly submitting the same request.

Activate and verify

After successful issuance, use the offered service restart flow. Services load TLS certificates at startup. The Console may disconnect briefly while HTTPMA restarts, then reconnect. Confirm that the affected services return to the running state.

Open Active Certificate to inspect its subject, issuer, DNS names, expiry and thumbprint. Verify the certificate from a real external client using the intended hostname. A certificate file on disk is not sufficient evidence that the running service has loaded it.

Renewal and failures

The Last Attempt tab shows account registration, validation type, expiry, next renewal, thumbprint and the last result. Inspect this information and the HTTPMA log when issuance fails. Keep public validation reachability working for future renewals and verify that renewed certificates are activated after service restart.

Protocol TLS policy

Open Server, Security, Security Properties, TLS. Review receiving SMTP, sending SMTP, POP3 and IMAP4 independently. Incoming policies include Disable TLS, Allow TLS and Require TLS. Outgoing SMTP also distinguishes Use TLS if available from Require TLS if supported and Require TLS.

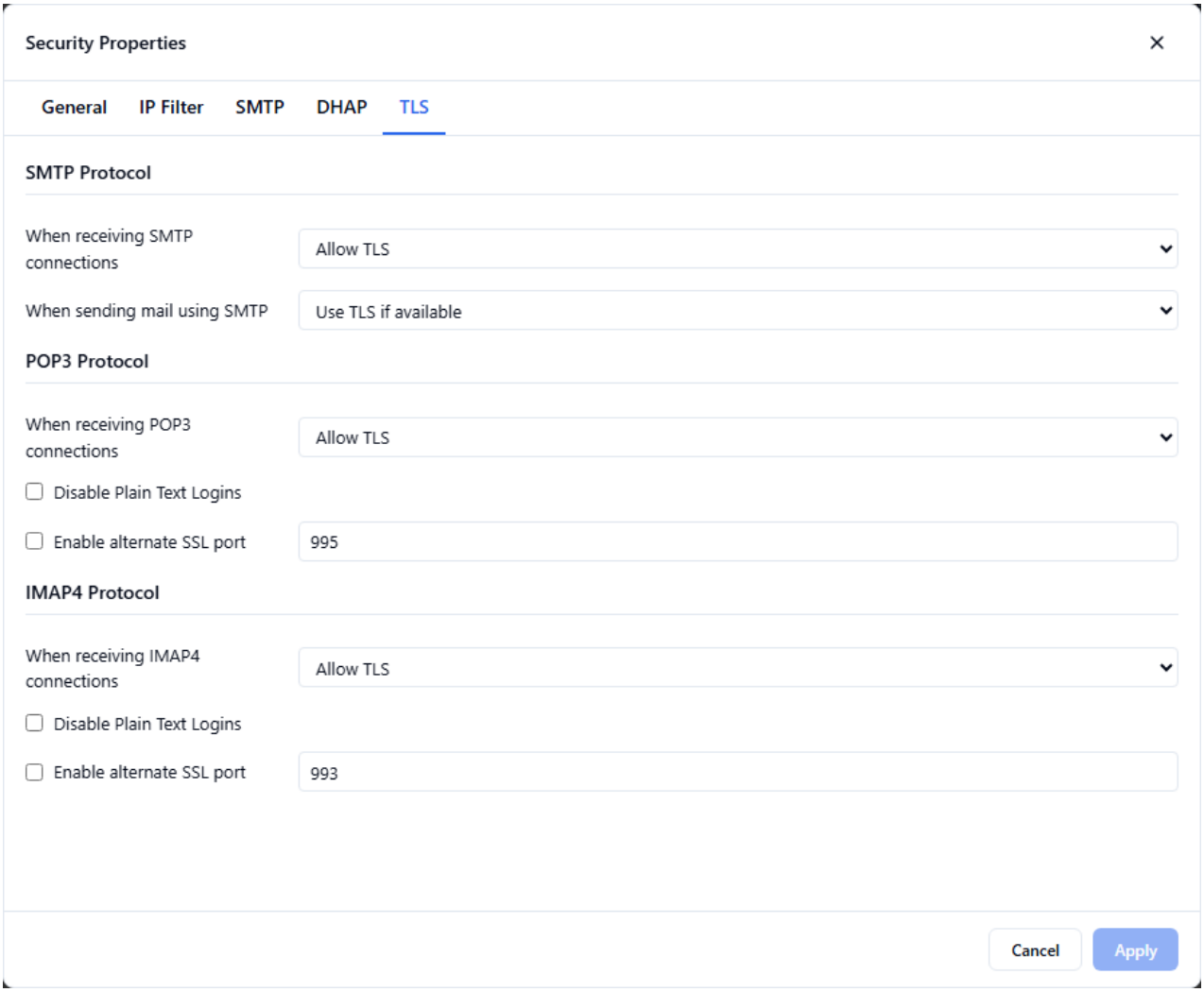

Figure 34 TLS policies for mail protocols

For POP3 and IMAP4, review Disable Plain Text Logins and the alternate SSL port controls. Defaults shown for alternate ports are 995 for POP3 and 993 for IMAP4; use the ports actually configured on the server. Test client access and remote delivery after a policy change. Requiring TLS can prevent communication with peers that cannot meet that requirement.

Mail Filters

MailSite uses Sieve scripts to apply mail rules during SMTP reception, local mailbox delivery and outbound relay. Rules can retain, file, redirect, reject or discard messages according to their stage and conditions. Export the current script before editing and verify both matching and nonmatching mail in a test environment.

Filtering stages

The Server Receive Script runs in SMTPRA before accepted mail is published to the delivery queue. Use this stage for receiving policy; it does not represent a particular recipient's final mailbox folder.

During local delivery, SMTPDA runs the Domain Script once for all local recipients in that domain, before mailbox filtering and mailing-list expansion. A domain keep or stop allows normal recipient processing to continue; discard or reject suppresses delivery to those recipients. Domain scripts can redirect messages but cannot file them into a mailbox folder. An invalid domain script notifies the domain postmaster and allows normal mailbox filtering to continue. Mailbox filtering then runs the Forced Mailbox Delivery Script, the mailbox’s own script and the server Mailbox Delivery Script, in that order. A stop in this mailbox stage stops the remaining mailbox scripts.

The Server Outbound Script applies on the outbound relay path. A local delivery test alone does not exercise it. List expansion, redirects and multiple recipients can create distinct delivery outcomes; test the complete intended route.

Using the Console editor

Open Server, Filtering, Sieve Filter and select the stage. New and Modify edit a rule's name, description and Sieve body. Apply the parent dialog after confirming a rule edit. Use the rule checkbox to enable or disable it, and Move Up or Move Down to change its order.

Copy, Rename, Delete, Import and Export manage existing rules and scripts. Advanced opens the full script editor. The current interface does not use the old multi-page criteria/action wizard. Its Test control is disabled; validate scripts by sending controlled messages through the relevant services.

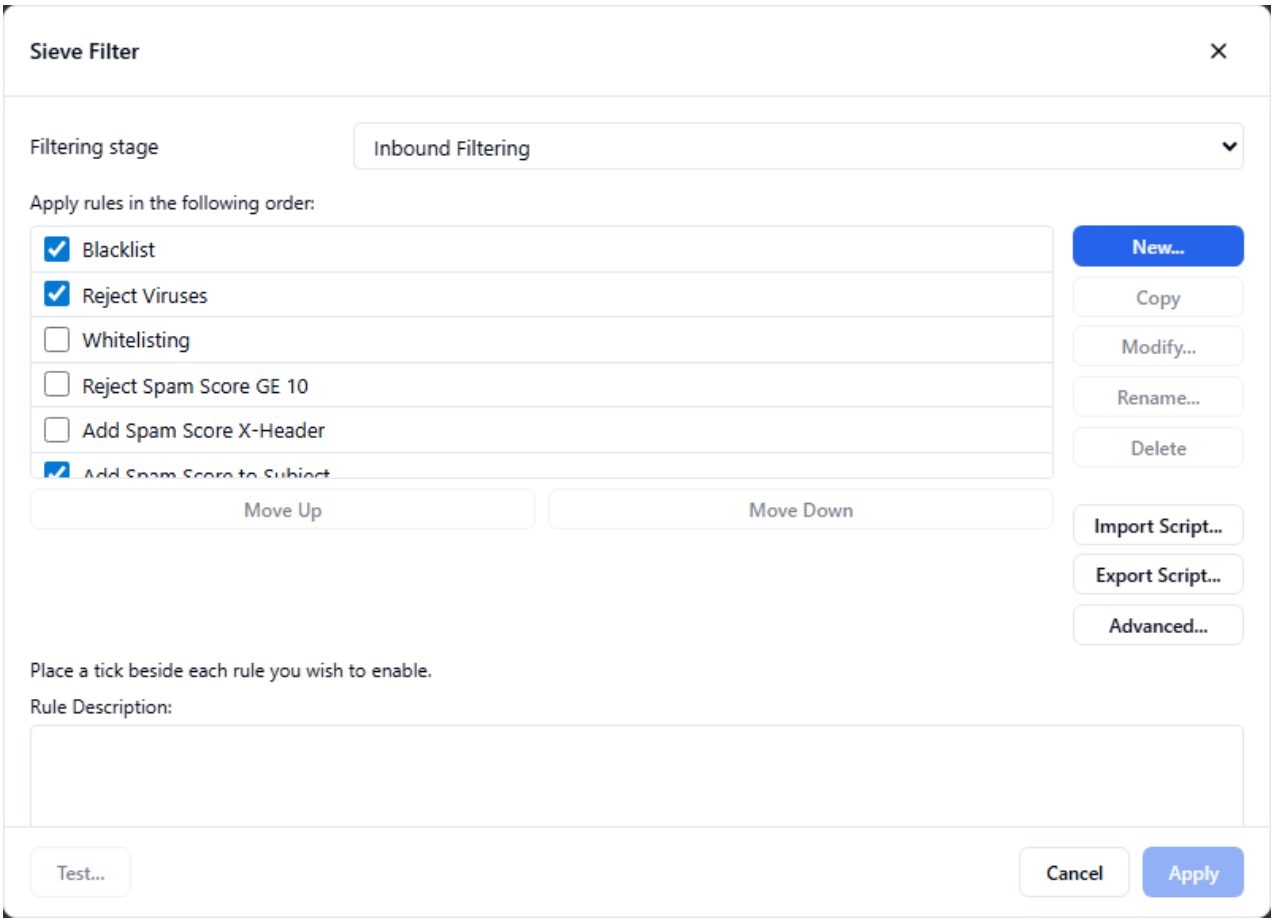

Figure 35 Filtering stages and rules

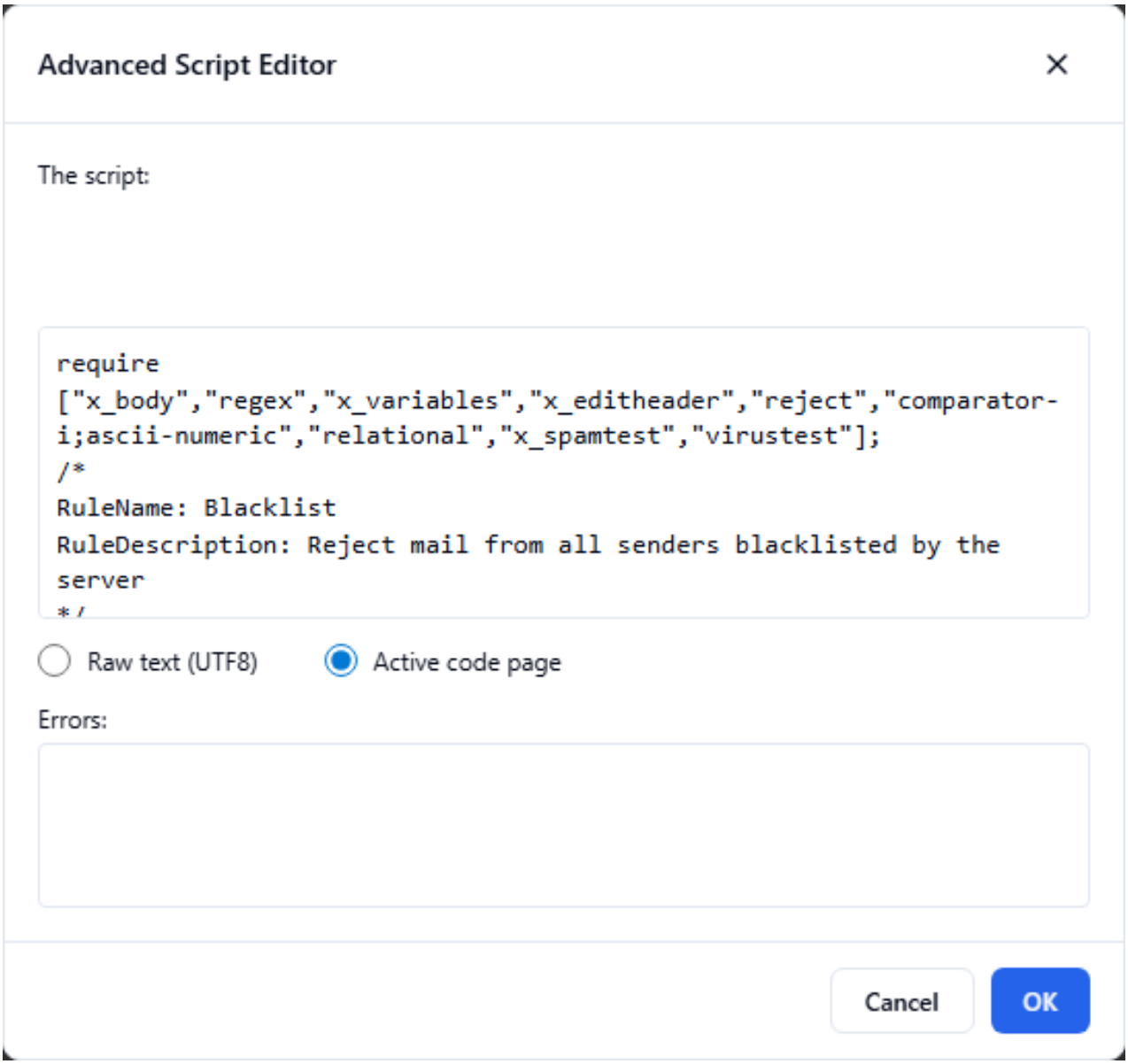

Figure 36 Full Sieve script editor

A simple mailbox rule

This example files a message whose Subject contains Project into an existing Projects folder. Apply it at a mailbox delivery stage, use straight quotation marks, and confirm the folder outcome from that mailbox's client.

```
require ["fileinto"];
if header :contains "Subject" "Project" {
    fileinto "Projects";
    stop;
}
```

Review how explicit delivery actions and stop interact with the other rules. An apparent match is not proof of final placement if another configured stage changes the outcome.

Conditions and extensions

The current interpreter supports fileinto, reject, regex, body/x_body, relational comparisons, numeric and octet comparators, and the MailSite extensions x_spamtest, x_editheader, x_variables, virustest,

x_sms, x_mime and x_foreverypart. Declare required extensions in the script; do not assume every Sieve extension supported by another product is available.

Use :contains or :matches for simple tests. Regular-expression tests use the current Rust regex engine; the old table's tagged braces, ~X and ^N syntax is not a current syntax reference. Start with a small expression and exercise matching, nonmatching and malformed input before deploying a complex rule.

Spam filing and retention

The supplied Spam Trap rule can file detected spam into Junk Mail when enabled. Review its score threshold and address-list exceptions with the scanner policy. Filing spam into a folder is distinct from rejecting it during SMTP reception.

Automatic retention removes aged messages from configured Junk/quarantine folders. The default age is thirty days; both the received date and the time MailSite indexed the message must be older than that limit. An upgrade or index rebuild starts a fresh grace period when the earlier admission time is unknown. Trash is excluded by default. Verify the selected folders and preserve wanted mail before shortening the age.

Verification

Test receiving and delivery separately, including several recipients, affected domains, user rules, forced rules, virus/spam results and outbound relay where relevant. Inspect the message and service logs. Retain the previous script and restore it if the result differs from the intended policy.

Wireless Email Integration

Wireless notification sends a short notification through a carrier's email-to-SMS gateway. This is separate from Exchange ActiveSync, which synchronizes mailbox data with a device.

Wireless configuration

Open a mailbox's Wireless tab to review its phone number, carrier and notification setting. Configure an appropriate notification rule in the mailbox's filtering policy. Selecting a carrier alone does not define which messages should generate a notification.

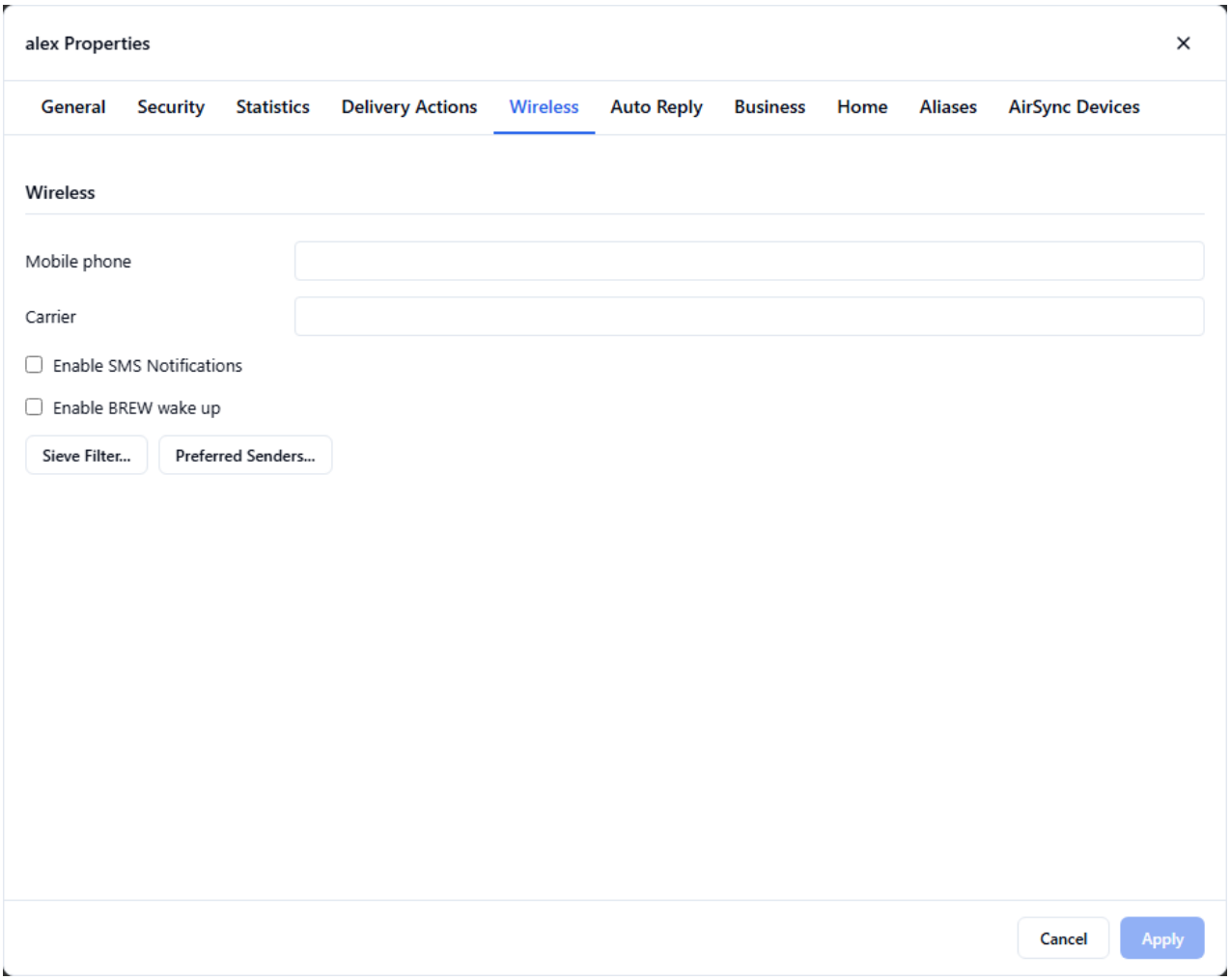

Figure 37 Mailbox wireless notification settings

Review Server, Wireless Carriers for configured gateway addresses. Carrier gateway availability and acceptance policies can change; verify delivery with the actual carrier before relying on notifications. Avoid including confidential message content in a notification sent through an external gateway.

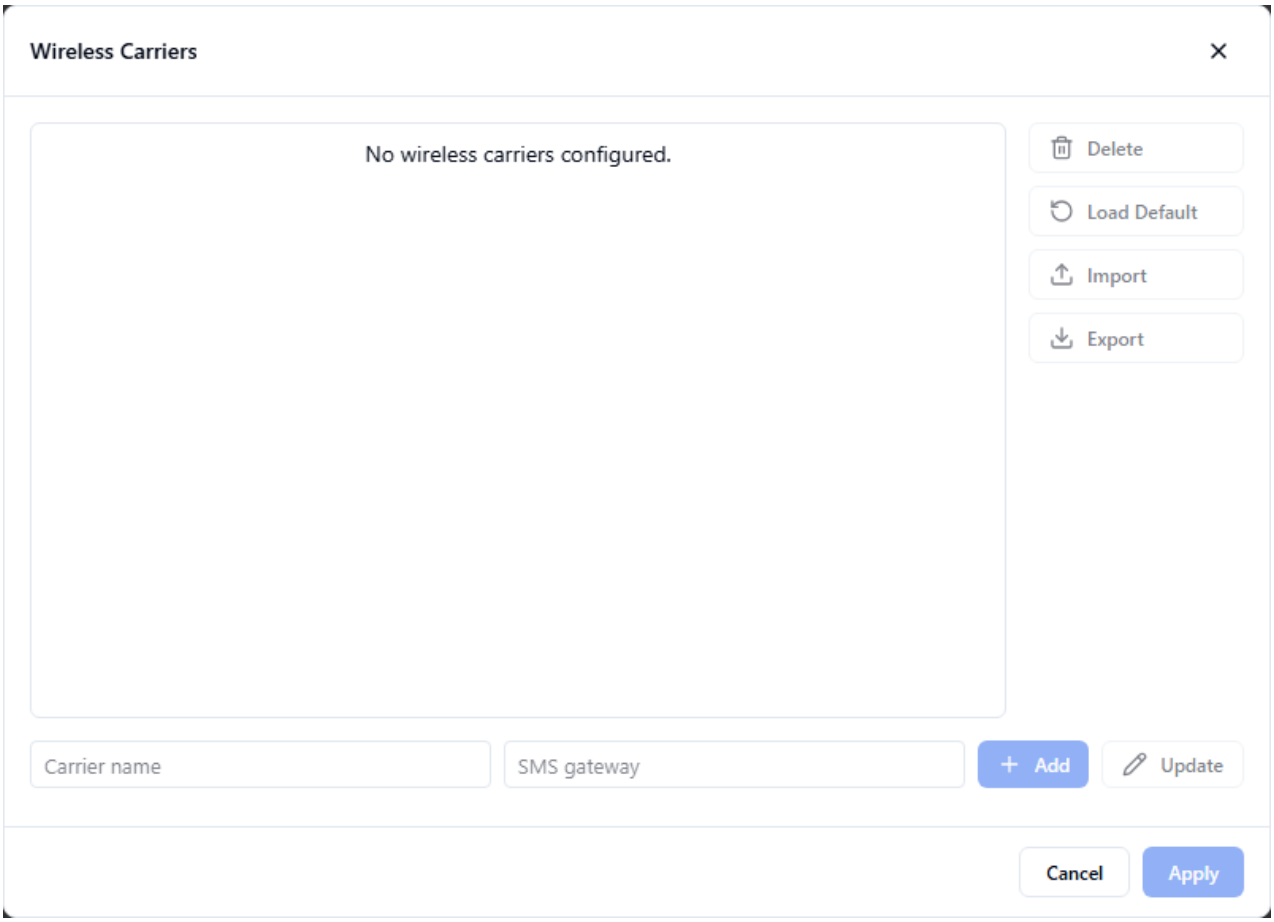

Figure 38 Configured wireless carrier gateways

Virus Scanning

MailSite 11 includes native ClamAV integration. Scanning scope and failure policy determine which messages are checked and what happens when scanning is unavailable. Review these policies during an upgrade from the old AVG-based configuration.

Server policy

Open Server, Filtering, Anti-Virus Filter. Enable virus processing and choose whether to process all SMTP messages or only messages associated with scan-enabled domains and mailboxes. Review the maximum message size excluded from scanning.

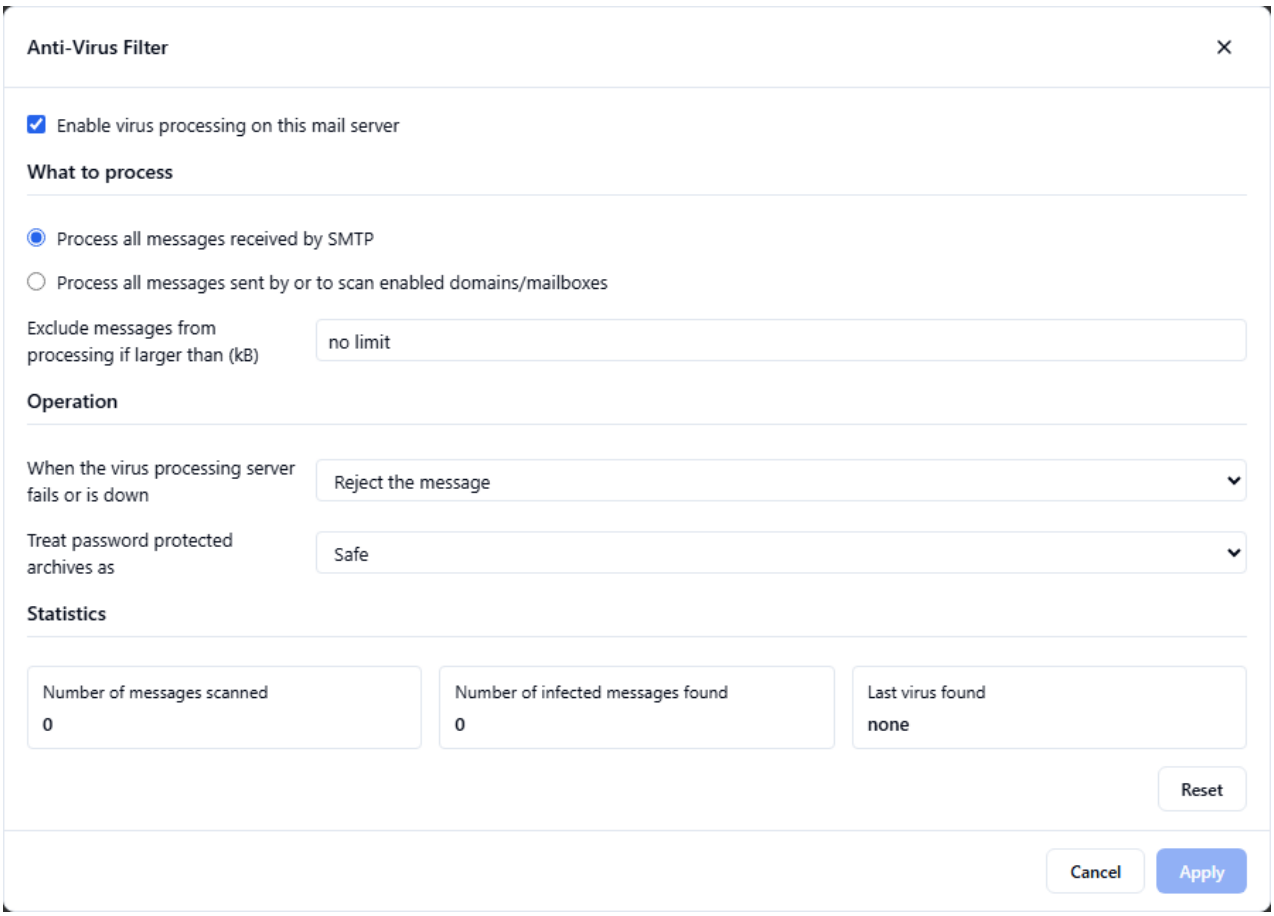

Figure 39 Anti-virus policy and scanner statistics

Choose the behavior when the scanning server fails or is down. Accepting a message in that situation favors mail availability; rejecting it prevents that unscanned delivery but can interrupt mail flow. Review the handling of password-protected archives, which may prevent inspection of their contents.

Domain and mailbox scope

For configured scope, open the domain's Anti-Virus Filter and the mailbox's service or delivery settings as appropriate. Verify the intended effective policy with normal test accounts. A server-wide checkbox does not establish that every domain or mailbox is included in a restricted scope.

Detection and message disposition

Detection and disposition are separate. Spam and virus enforcement remains Sieve-driven. Review the receiving and delivery scripts that act on scan results; enabling scanning alone does not establish that

infected messages will be rejected or quarantined. Preserve the intended action when migrating policies from the previous release.

Verify operation

Inspect the scanned and infected counters, the last virus result and definition-update status. Use a controlled antivirus test message under your organization's test procedure and confirm the expected mail-flow result. Check the SMTPRA logs for scan failures and verify that definition updates remain current.

Spam Scanning

MailSite 11 uses built-in spam scoring, including Bayesian classification, together with receiving policy and message filtering. Scoring and disposition are separate: a spam score must be interpreted by the configured delivery or Sieve policy.

Scanning policy

Open Server, Filtering, Anti-Spam Filter. On Scanning, enable scanning and choose all incoming SMTP mail or configured domains and mailboxes. Review message-size exclusions, authenticated-connection exemptions and friendly-host or subnet exemptions.

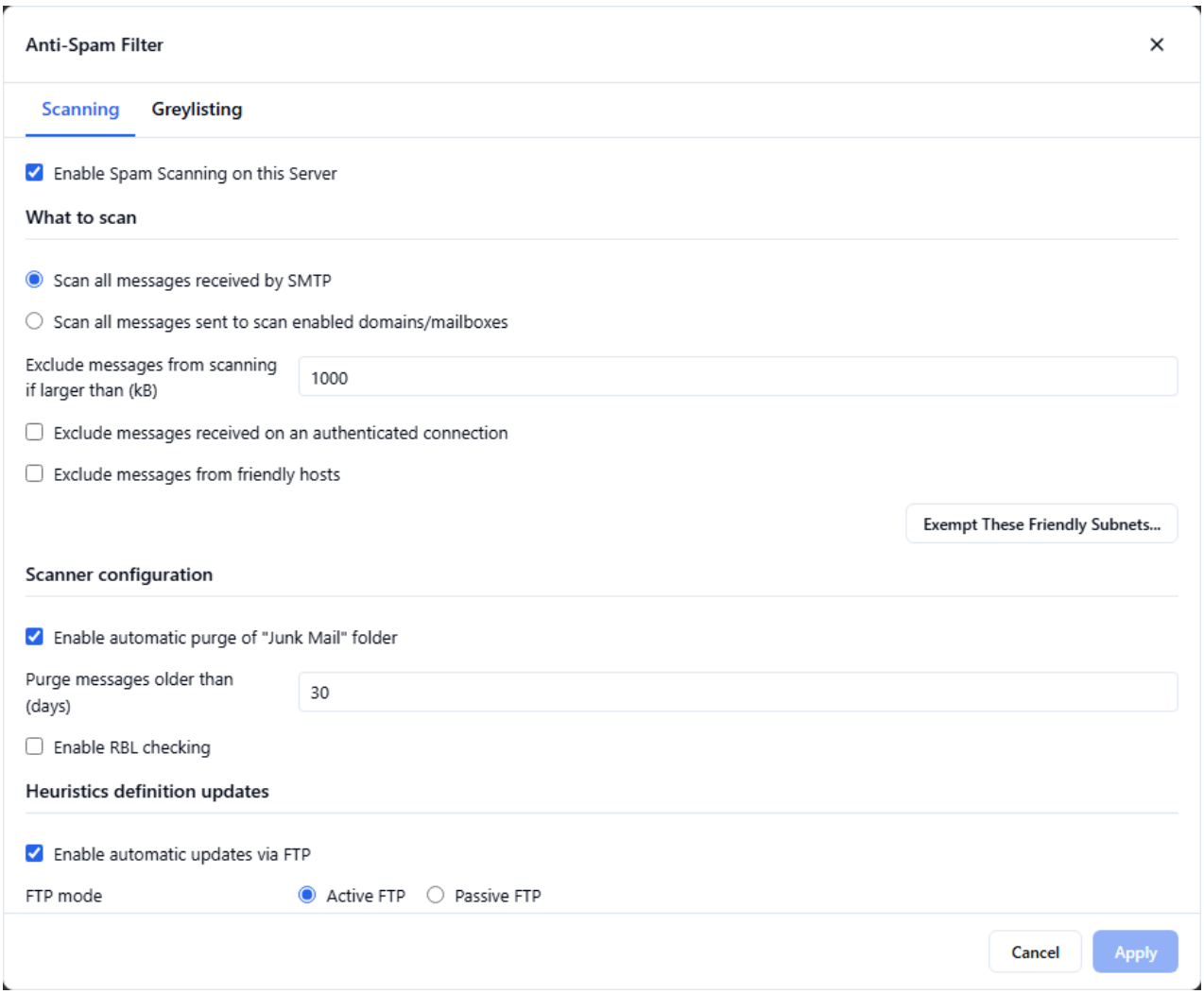

Figure 40 Anti-spam scanning policy

Automatic retention runs in bounded background batches after mailbox login or activity, normally no more than once per day unless settings change or a batch has more work. PurgeFoldersMask selects the server quarantine folder (1), mailbox Junk folder (2), and Trash folder (4); the default is 3. SpamQuarantinePurgeAge is in seconds. A zero mask, zero age or the unlimited age value disables deletion. Shared folders and paths outside the mailbox are excluded.

Greylisting

The Greylisting tab controls temporary deferral of eligible first-time delivery attempts. Correct sending servers normally retry. Review exemptions and timing with your mail flow so trusted systems are not delayed unexpectedly.

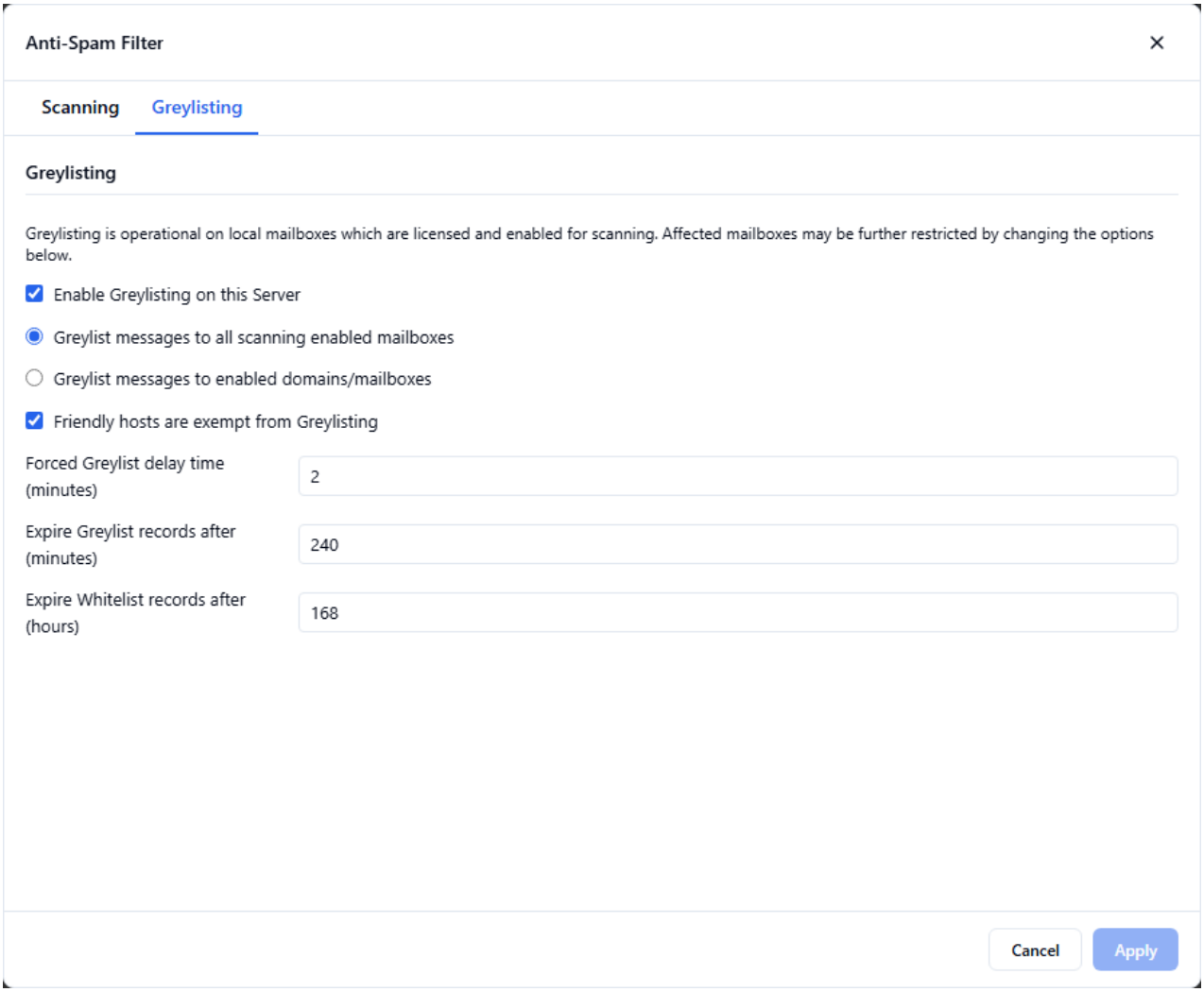

Figure 41 Greylisting settings

Disposition and exceptions

Review Sieve rules and the server, domain and mailbox address lists used by those rules. Test both a message that should be treated as spam and one that should be delivered normally. Avoid overly broad trusted-host exemptions, which can prevent the messages you intended to inspect from reaching the scanner.

Monitor results

Inspect scanner counters and SMTPRA logs. Compare false positives and missed spam against the policy that applied at receipt. Preserve the relevant headers and timestamps for diagnosis, subject to your organization's privacy and retention policies.

Agents

MailSite supports external processing at specific points in mail reception and mailbox delivery. Configure only noninteractive programs whose files, permissions, timeout behavior and effect on mail have been verified under the service's Windows identity.

Server incoming agent

Server, Agents contains the incoming-mail command and archive directory. The incoming agent receives message and recipient-file paths; the receiving service waits for the configured processing outcome before final queue publication. Quote paths in command templates and test both success and timeout/failure behavior. A program that works interactively may lack permissions or environment variables as a service.

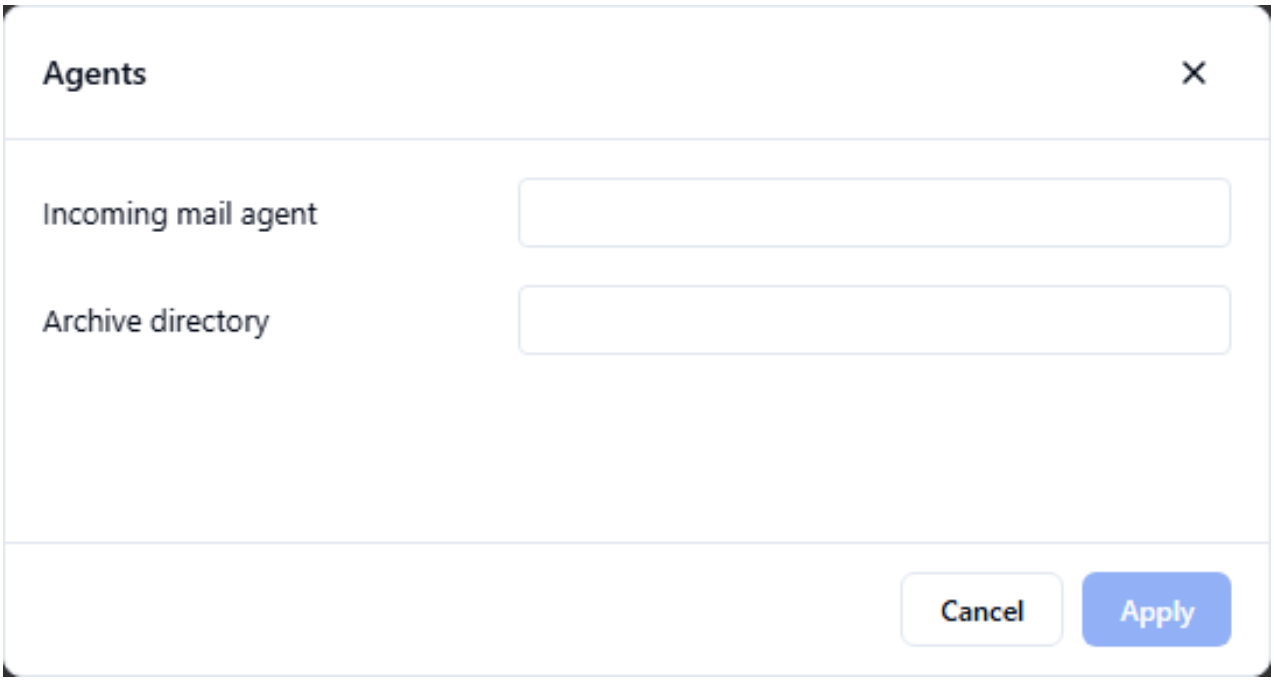

Figure 42 Server incoming agent and archive settings

Do not assume that a scanner launched by an external command has the same policy as the native virus or spam controls. Verify which messages the integration receives and how its result changes acceptance or delivery.

Mailbox agent

The mailbox's Delivery Actions contain its external agent command. The legacy substitutions include %f for the message file, %u for mailbox name, %h for mailbox directory, %d for domain and %% for a percent character. Confirm the behavior with a test account before enabling it broadly. The command runs with service permissions and must terminate without prompting.

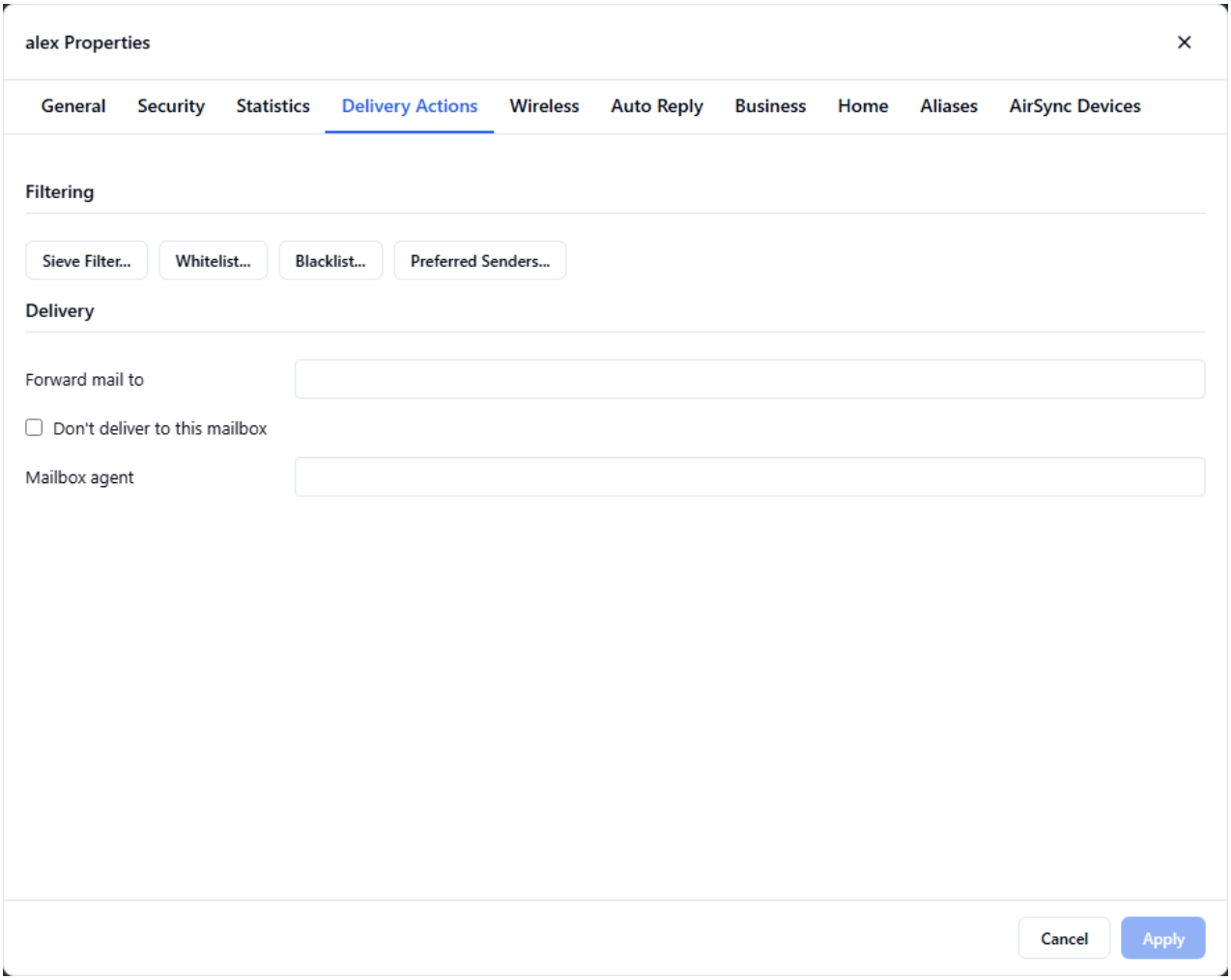

Figure 43 Mailbox delivery actions

The mail item must complete the normal storage publication path before it is available to clients. Do not use an agent to edit unrelated mailbox databases or treat its temporary input filename as the permanent client identity.

List agents and list processor agents

CommandLine runs for ordinary list messages and RequestCommandLine runs for request-address messages before normal list processing. Use %f for the temporary message file, %n for list name, %d for domain, %m for moderators (or a hyphen when absent), and %% for a literal percent. Quote executable and file paths. The program may edit the message file; exit zero commits that output. Programs run under SMTPDA permissions without interaction, have a sixty-second limit, and must leave a nonempty message of at most 100 MiB. Shell metacharacters in substituted values are rejected.

A nonzero exit delays delivery and permits a retry. After a successful transformation, delivery retries reuse its saved output. A timeout, process error or server interruption can leave an unknown external outcome; MailSite retains an invocation-started marker and delays delivery rather than blindly rerunning the program. Stop processing that source, inspect the source/list directory under list-agent-results beside the incoming spool and check the program effects before removing that marker to authorize another attempt. Preserve any result.eml file: it is the committed transformed message.

Archive copies

The configured server archive directory receives mail/recipient copies from the applicable receiving and queue paths. Archive files are organized into date directories. Verify actual ingress, rejection, locally

generated and delivery cases needed by your retention policy; the existence of an archive directory alone is not proof of complete organizational mail retention.

Web archives, mail-store backups and compliance retention are different functions. MailSite writes new static archive pages below the configured archive directory in mailsite-v11. Existing Hypermail indexes and articles remain unchanged. Web serving, access control, backup and retention of these archive files remain administrator responsibilities.

Databases

MailSite uses ODBC (Open Database Connectivity) for external mailbox authentication and mailing-list membership. Configure a supported 64-bit source as described below. Direct ODBC logging from the previous implementation is not supported; see Appendix E.

You must have ODBC drivers installed if you wish to use this feature. Note that you should not attempt to use this these features if you are not familiar with databases and their terminology.

Setting up database access

Install a compatible 64-bit ODBC driver and configure the data source required by the external account or membership connector. Use credentials and permissions available to the Windows identity running the service, not merely to an interactive administrator. Validate the source from the actual service context.

For a remote SQL server, verify name resolution, its configured listener, network access, database authentication and object permissions. A successful local connection in an administration tool does not prove the service can connect. MailSite's SQL configuration connector and its external user/member databases are separate connections with separate recovery requirements.

External database mailbox provisioning

Open Console, select the server, and open External Database Mailboxes. This connects an external user directory to mailbox accounts. It is separate from the SQL Connector that stores MailSite's own configuration; either registry or SQL configuration can use an external user database.

Configure a 64-bit ODBC source and select Generic or Emerald. Generic maps the table, mailbox/full-name/password columns, optional domain column, and eligible-user filter. The supported source contract supplies usable password values; it is not a generic password-hash adapter. Emerald uses ListMailUsers, VerifyMailUser and ChangeMailUserPassword with the configured ESID.

Save settings, select a domain, preview eligible accounts and provision selected names. Existing external accounts are reported as existing; native mailbox/list collisions are not overwritten. Limit a preview or batch to 500 accounts, narrowing the filter when necessary. Batches stop starting new accounts after their time budget; a database call already running retains its timeout. Review each result and retry only the remaining accounts.

Enable automatic creation only for intended domains. A lookup of an eligible external user may create that user's MailSite mailbox. Authentication continues to check current external eligibility. Disabling/removing a source user prevents external login without deleting existing mail. Repeated provisioning and interrupted batches preserve accounts already created.

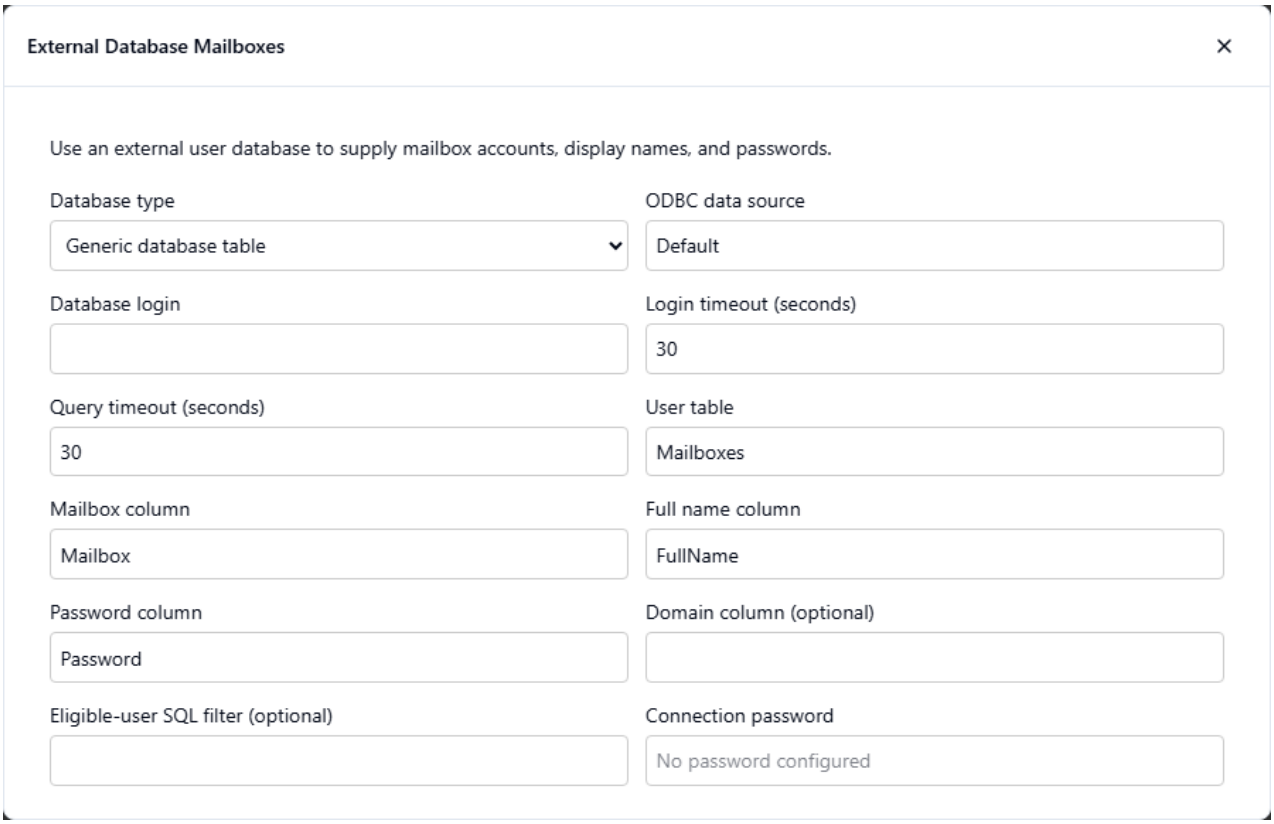

Figure 44 External database mailbox configuration

Database Mail List Plugin

The Database Mail List Plugin makes use of some default properties. This makes it possible to create Database Mail Lists with minimal configuration. For the default configuration, the following applies:

An ODBC data source can be used for all domains. This will need to be entered into the Mail list properties in the Database Tab of the Database Mail List.

A separate table is used for each mail list. The name of the table must be the same as the name of the mail list, except that where the mail list name contains a dot or hyphen character. If the list name contains a dot or hyphen you must create the table using the underscore character. This is because dot and hyphen are not legal table name characters in some databases.

The table must contain at least two columns, called EmailAddress and FullName. These columns must contain the e-mail addresses and names of the mail list members.

For example, create a database mailing list called customers in the virtual domain abc.com. The list address would be customers@abc.com. To map this to a database, create a data source called abc.com and a table customers in this data source. The table customers must have columns EmailAddress and FullName.

An example of using the Database Mail List Plugin is provided in the appendix on Database Examples.

SQL Connector

The SQL configuration connector stores shared MailSite configuration in SQL Server. It is distinct from the mailbox databases managed by MSDBMA. Switching the configuration connector does not replace the need to back up mailbox data.

Prepare the SQL server

Use a supported SQL Server installation and an account with the permissions required to create or refresh the MailSite configuration database. Verify connectivity from the MailSite server and decide whether the service uses Windows trusted authentication or explicit SQL credentials.

Configure the connector

Open Server, SQL Connector in the Console. Enter the SQL server and authentication settings, then use Test Connection. Create or refresh the database through the provided control when appropriate. Review the result before changing the active configuration connector.

The current Console uses explicit SQL connection settings; the old ODBC Administrator and native SQL Connector wizard are not required for this workflow.

Switch configuration storage

Open Configuration Connector to select Registry or SQL. Review validation results and any migration option before applying the change. A connector switch affects the server's configuration authority and requires the MailSite services to restart. Schedule it as a maintenance operation and retain a configuration backup.

After switching, reconnect to the Console and verify domains, mailboxes, aliases, mailing lists, licensed features and service operation. Check the migration result and service logs rather than assuming that a successful connection test proves that the configuration was migrated.

Monitoring

Use the Console to inspect service health, runtime logs, mailbox initialization and delivery behavior. Correlate an error with the service responsible for the failing operation rather than assuming that the service which reported it caused the problem.

Service status and logs

Open Server, Services. Check the required service is running and open its log viewer. The viewer supports current and historical files, paging, live following and search. Select a relevant time range and operation before increasing verbosity or exporting logs.

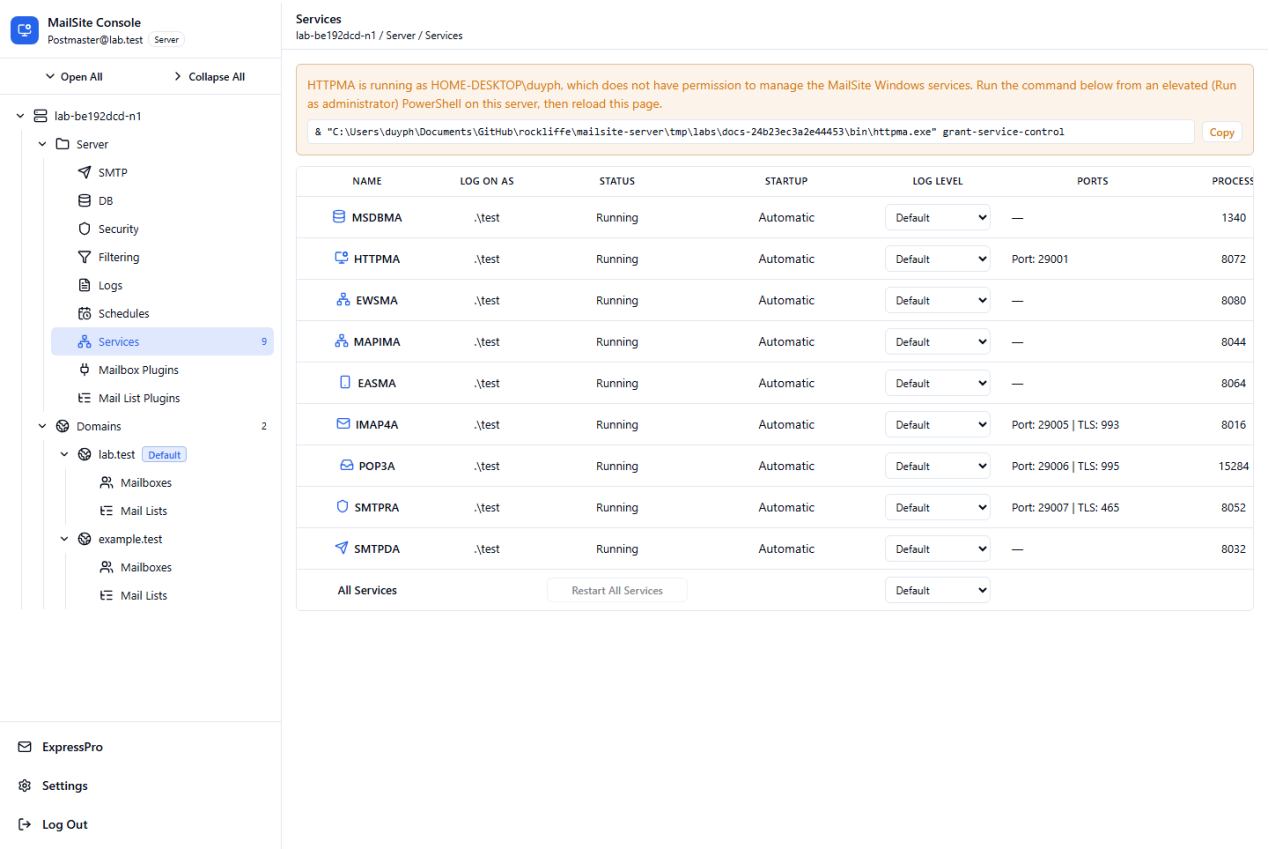

Figure 45 Service operations and status

Runtime log levels can be changed per service, or together from the Services table controls. Return temporary diagnostic verbosity to the normal level after troubleshooting. Logs may contain mailbox addresses and operational details; review them before sharing externally.

Mail flow

SMTPRA records receiving and policy decisions; SMTPDA records delivery and retry behavior. Investigate accepted-but-undelivered mail across both services and the relevant queue. For mailbox access, include MSDBMA and the protocol service used by the client.

Database health

The Console's database views expose mailbox preparation, indexing and failed database operations. A failed or incompatible database must be diagnosed; do not clear the error by deleting data without understanding the recovery impact.

Storage and scanning

Monitor free space, mailbox growth, queue age and log retention. Review anti-virus definition status and the scanning counters as well as the availability of the services. Include certificate expiry and renewal results in routine operational checks.

MailSite Engine

The MailSite engine is a set of cooperating Windows services. The public protocol services authenticate requests and implement protocol behavior, while MSDBMA provides shared storage and configuration access. Deploy all of these services from the same build.

Message storage and databases

MSDBMA owns access to shared mailbox-store files, mailbox indexes and configuration. It manages initialization and reconciliation and publishes changes used by the protocol services. Stop its clients before stopping it for maintenance; when starting services, make MSDBMA available first to avoid dependency waits.

SMTP receiving and delivery

SMTPRA accepts SMTP connections, applies receiving policies and filtering, and queues accepted messages. SMTPDA processes queued mail for local mailboxes, mailing lists or remote delivery. Check both sides of this flow when a message is accepted but does not arrive.

Mailbox access

IMAP4A provides IMAP access to mail folders and search. POP3A provides POP3 access. EWSMA serves Exchange Web Services operations for ExpressPro and compatible desktop clients. EASMA serves Exchange ActiveSync requests. MAPIMA serves the MAPI over HTTP path used by classic Outlook clients.

HTTP front door

HTTPMA serves webmail, administration and public HTTP protocol endpoints. It forwards EWS, EAS and MAPI traffic to private worker services. A working HTTPS connection proves that HTTPMA is reachable; it does not prove that a particular worker or MSDBMA is available.

Working directories

The configured mailbox directories contain live user data. The mail spool contains messages in delivery or waiting for retry. Logs, certificates, configuration and mailbox databases have separate operational roles. Use the Console's Directories and domain settings to identify the actual paths in your deployment.

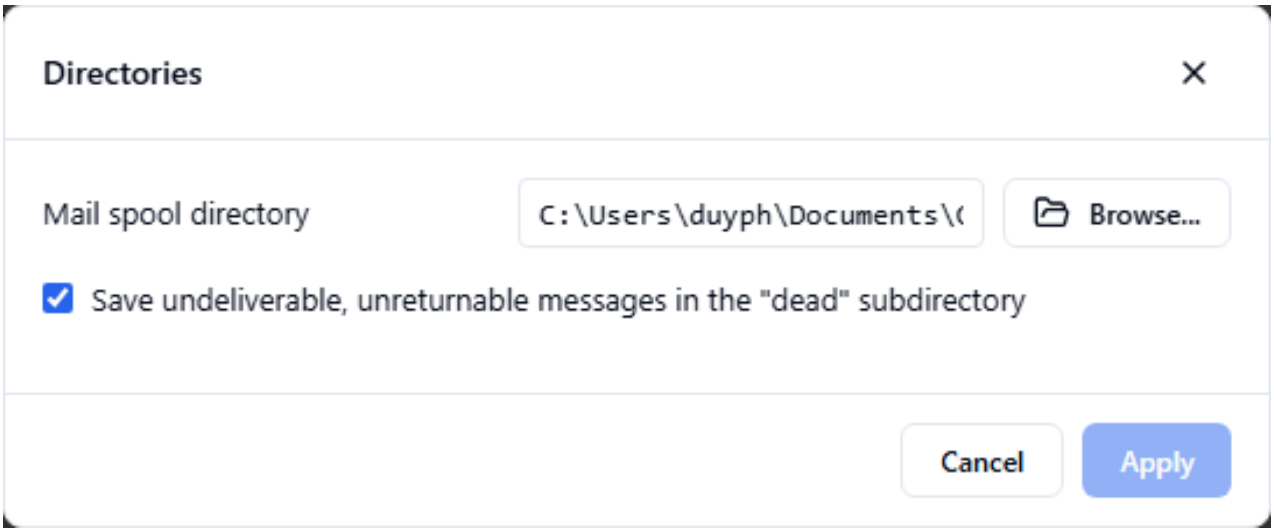

Figure 46 Server directory settings

Back up configured paths and their access permissions. Do not delete a mailbox's Databases tree as routine maintenance: development reset boundaries can discard database-only information as well as indexes. Use documented recovery or upgrade procedures for the installed release.

Windows Console Reference

The Windows Console allows you to configure your local or remote MailSite Engine. You can use the Windows Console to manage MailSite on the local system as well as on servers elsewhere on the network.

MailSite Server Administration

Open the MailSite desktop Console or choose Console from ExpressPro after signing in. The desktop and browser applications share the administration interface. Use the navigation tree to select Server, a domain, Mailboxes or Mail Lists, then open the relevant item or properties dialog.

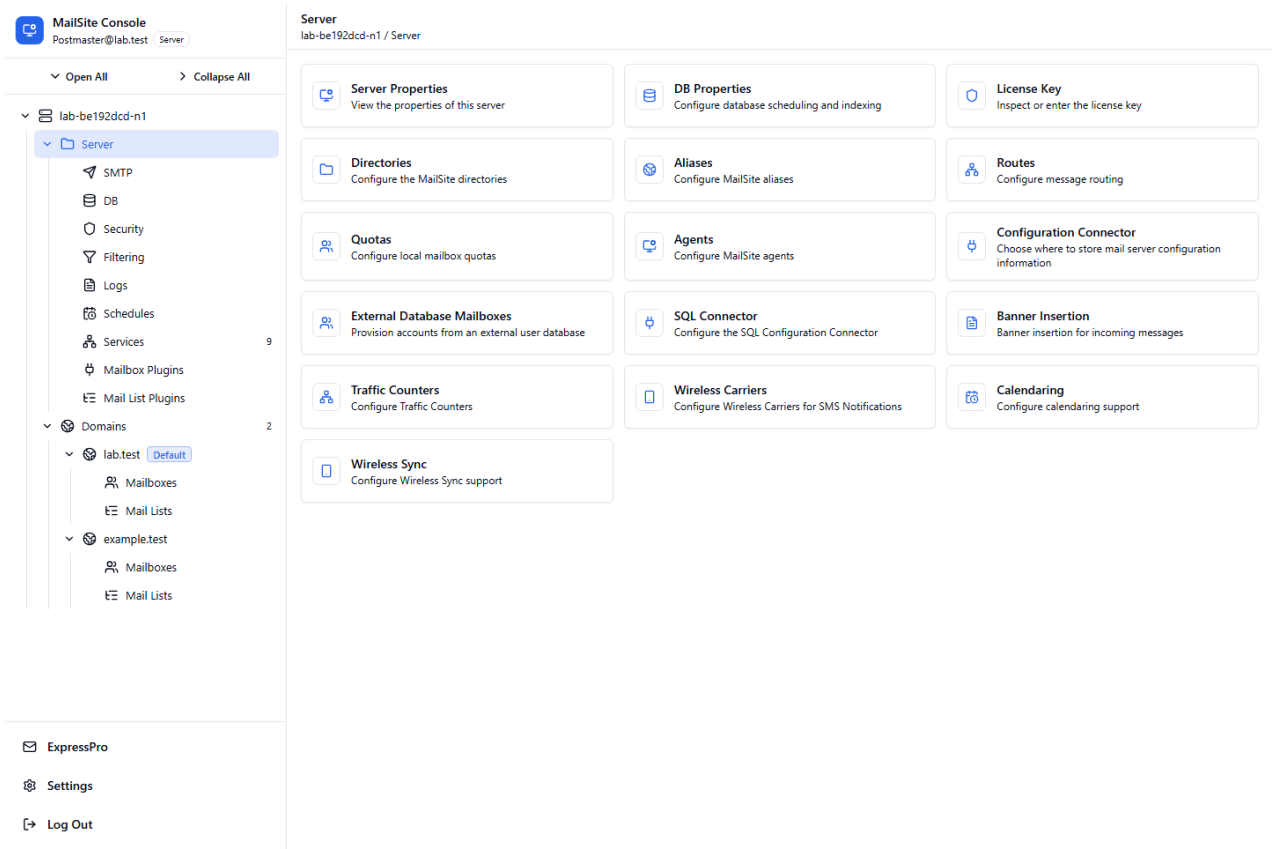

Figure 47 Console navigation and server settings

Apply saves changes made in a properties dialog; Cancel closes it without applying unsaved changes. Controls can be hidden or disabled because of privilege, licensed features or the selected configuration connector. Use a normal target account when verifying a permission change.

The browser Console manages the HTTPMA server to which it is connected. The old Windows workstation's Register Server and De-register Server instructions do not describe browser session management. Sign out when leaving an administration session.

Server

Under each server shown in the list of MailSite systems on the left side of the MailSite Console are two folders: Server and Domains. The Server folder contains icons corresponding to the many options that can be configured for the MailSite Engine.

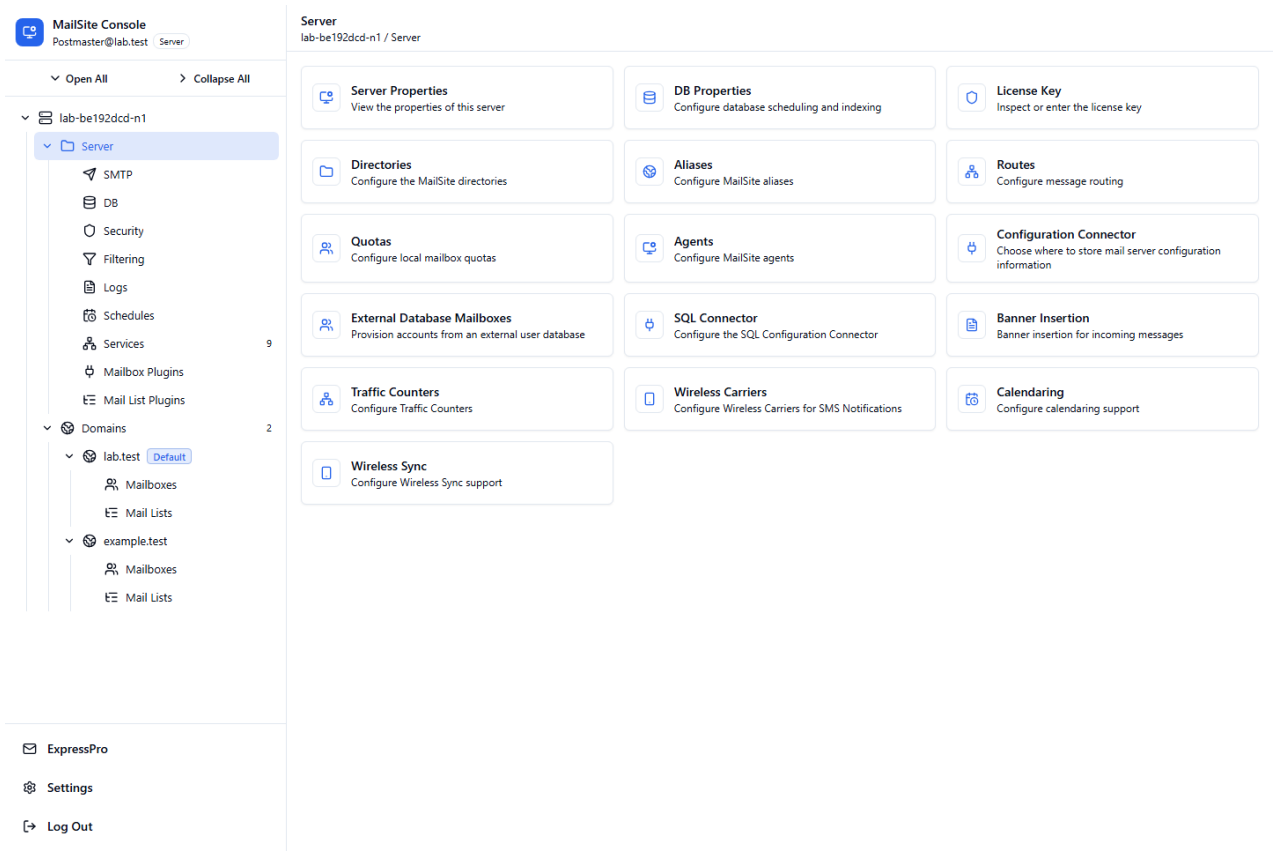

Figure 48 Server

The following sections describe Console controls and their operational meaning. Explicit compatibility notes identify retained settings whose previous implementation is not part of v11. A visible or saved property does not by itself establish runtime support.

License Key

If you did not enter a valid License Key during the installation process, you can enter it in the License key dialog. Display this dialog by clicking on the License key icon:

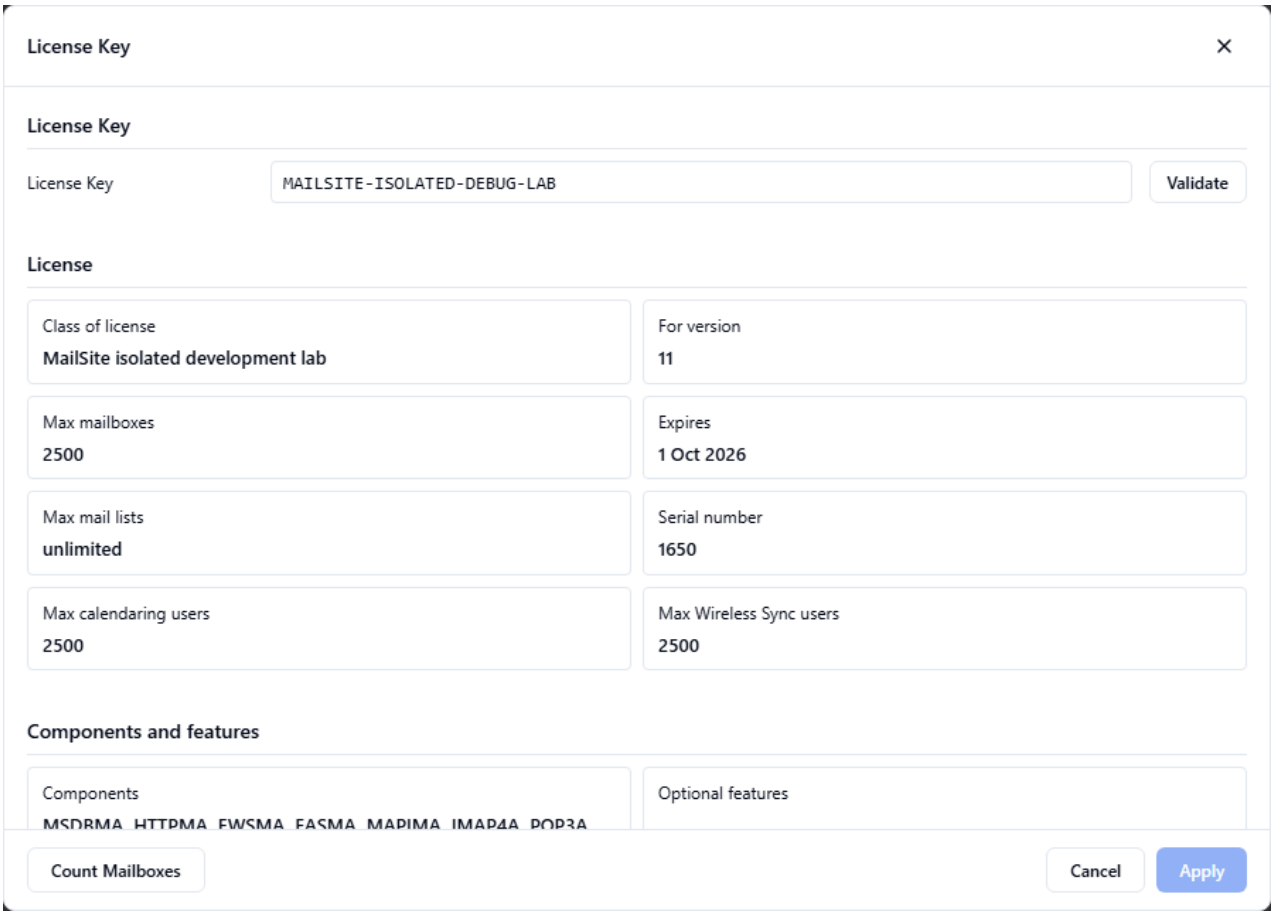

Figure 49 License Key

The License Key determines the licensed features, account limits and any expiration date. Use Validate and inspect the actual entitlement returned for your key; do not infer its duration solely from whether it was issued for evaluation or purchase.

License Key

Type your License Key into the field provided. License Keys consist of five groups of four characters. Each group is separated by a hyphen. The characters will always be between 0 to 9 and A to F. The letters must be entered in uppercase, and make sure that you do not confuse the character O (upper-case "o") with the number 0. You will never be issued with a key that contains the upper-case "o" character.

Click the Validate button to ensure that you've not made a typing mistake, and to see exactly what the License Key entitles you to do. The License Key determines:

- Your MailSite Serial Number.
- The maximum number of mailboxes you may create.
- The maximum number of mail lists you may create.
- The date on which your license to use the software expires.
- Any optional features which you are licensed to use.

Remember that your MailSite license does not permit you to disclose your License Key to anyone else.

Click the Count mailboxes button to get the total number of domains, mailboxes, and mail lists on your system.

Directories

Click on the Directories icon to set the mail spool directory for MailSite.

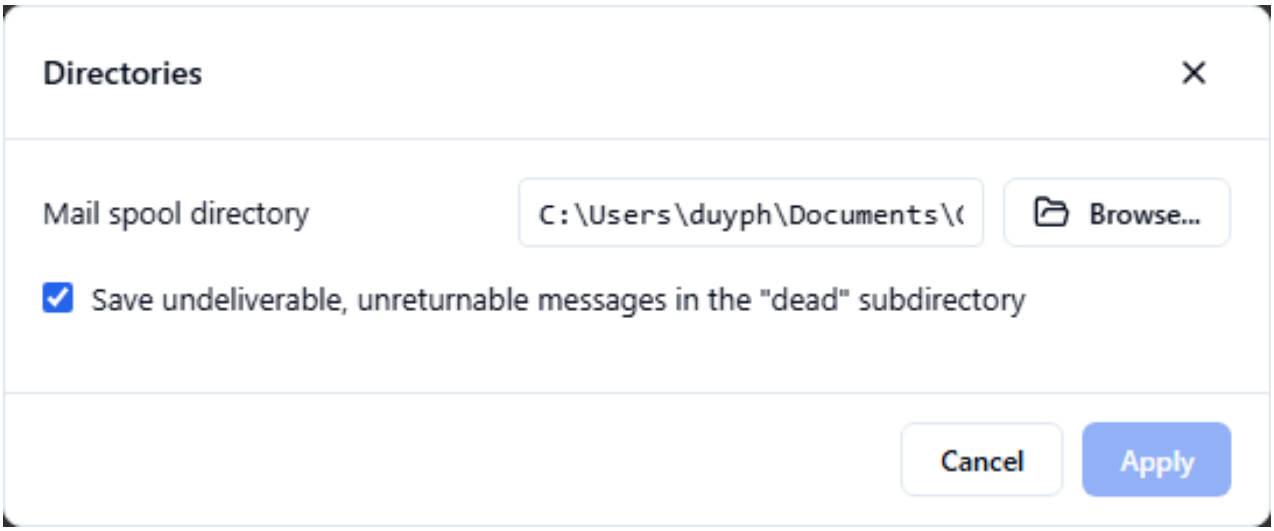

Figure 50 Directories

Mail Spool Directory

The Mail Spool Directory is a staging post for messages in transit through the system. Enter the name of the directory that you wish to use as the mail spool directory. MailSite will create subdirectories under this directory. For further information refer to the section on the MailSite Engine.

It is recommended that the mail spool directory is located on a NTFS partition. See the Message Store Security section for additional information. The default is: C:\Program Files\MailSite\SPOOL.

To configure the location where the mail server will store messages for local mailboxes, see the section on Domains later in this chapter.

Save Messages to Dead Directory

By default, messages that are both undeliverable and un-returnable are stored under the Spool directory in a subdirectory named dead. Keeping these messages allows you to diagnose potential mail delivery problems. However, if your site is particularly busy or hosts a large number of mailboxes, saving dead messages can be an unnecessary use of disk space. Use the option in the Directories dialog to specify whether these messages should be saved to dead. If this option is disabled, MailSite will discard all undeliverable and un-returnable mail.

Aliases

Click on the Aliases icon to open the Aliases dialog:

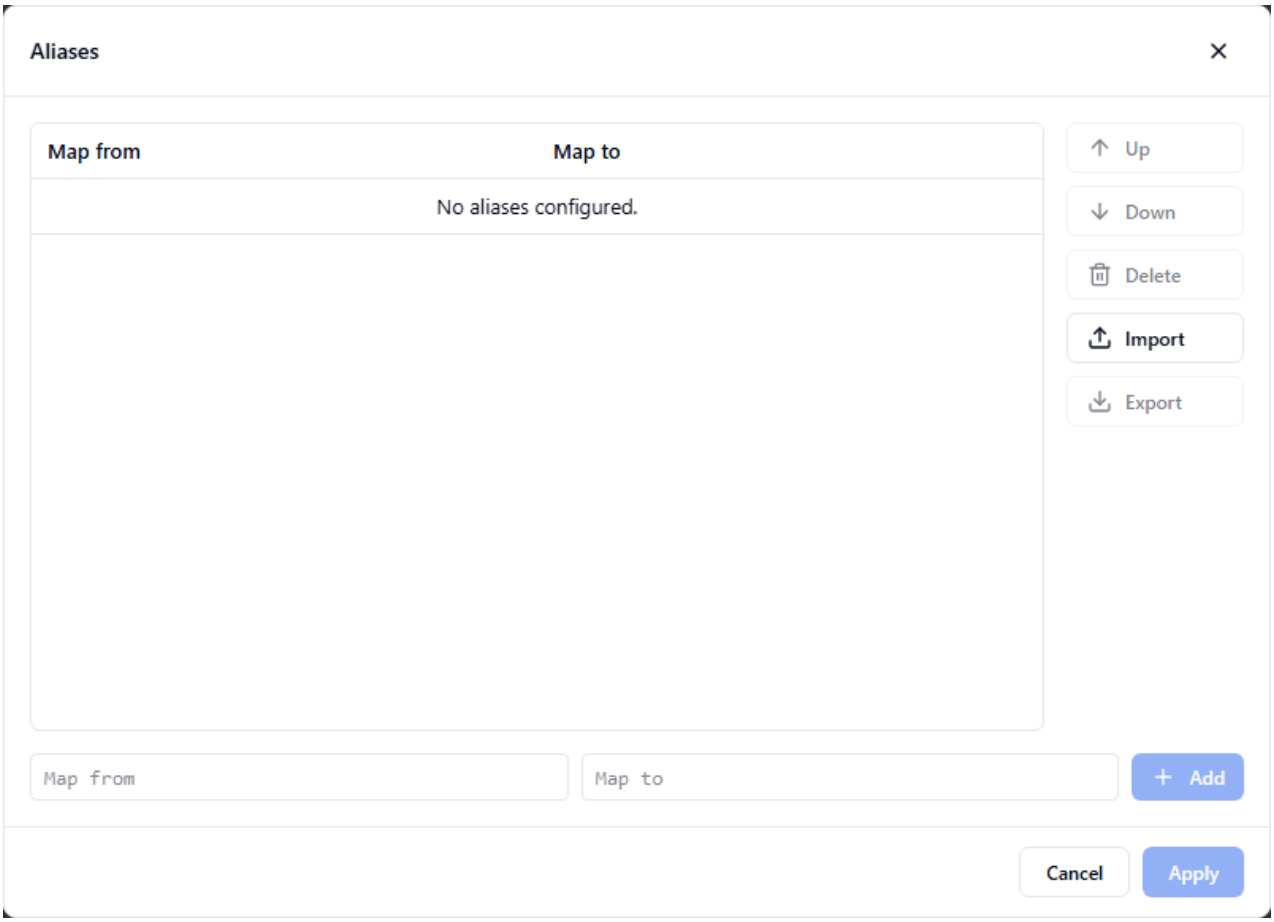

Figure 51 Aliases

Server aliases redirect matching SMTP envelope recipients using the ordered map.

The visible To header is not the authoritative delivery address.

Adding Aliases

Enter the Map From and Map To entries and click on the Add button.

Modifying Aliases

Select an alias, edit Map From and Map To, then choose Update. Apply saves the map.

Deleting Aliases

Select the aliases to remove and choose Delete. Apply saves the change.

Map From

Type the address that you wish to alias. The alias can be a simple user name (such as fred), or can be a fully qualified Internet Mail Address. This is especially useful if you have configured MailSite to support multiple domains. See the section on Multiple Domains for more information.

Map To

Type the address to which messages should be sent. This address could be a local mailbox listed in the Mailboxes folder (for example, fred) or it can be a remote user (for example, fred@abc.com).

Wildcard Aliases

You can specify wildcards in the Map From field. This can be used to redirect mail for all names matching a pattern. For instance, specifying a user name of t*y would match Tony, Tiny, toby, terry, etc. (Note that matching is not case sensitive.)

You can also specify a single wildcard as the first character of the Map To field. This will be replaced by the actual user name when the table entry is used. For instance, if the Map From string is f* and the corresponding Map To string is

*-blue@xyz.com, then a message for fred@abc.com will be redirected to fred-blue@xyz.com.

This feature can be used to redirect all mail for one domain to a second domain. The second domain could be local to this machine, or on a remote machine. This is done by specifying a Map From string of *@abc.com and a Map To string of *@xyz.com.

Map Table Order

The order of entries in the alias table is significant. It is processed top-to-bottom, and the first matching entry is used. Thus, specific entries should be positioned near the top of the list, and less specific entries (containing wildcards) towards the end of the list. Use the Up and Down buttons to move entries around.

Import Aliases

The Import button allows you to import aliases from a text file. The button displays the Open file dialog. Locate the text file containing the list of Aliases that you wish to import. Click on the OK button to import the Aliases. Each line of the text file should consist of the Alias, followed by a colon, followed by the address. For example:

jgd: johnd
john*: johnd
jd: johnd

Export Aliases

The Export button allows you to export aliases to a text file. This button displays the Save As file dialog.

Enter the name of text file for exporting the list of Aliases. Click on the OK button to export the Aliases. Each line in the text file will consist of the Alias, followed by a colon, followed by the Address. For example:

jgd: johnd
john*: johnd
jd: johnd

Routes

Click on the Routes icon to display the Routing dialog, which is used to set rules for how messages are routed through MailSite:

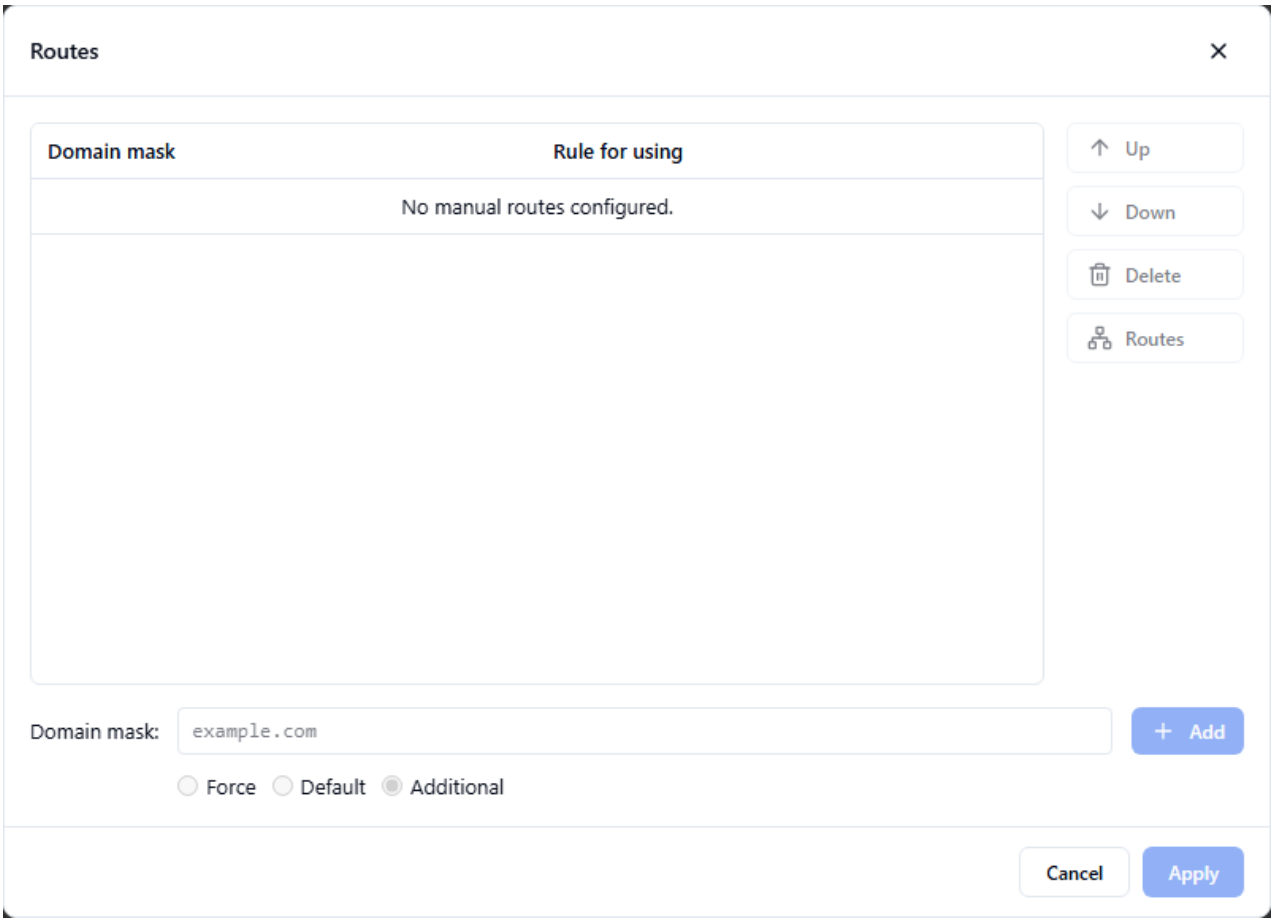

Figure 52 Routes

Normally, MailSite uses DNS MX records to decide which host to contact in order to deliver mail for a particular domain. In some circumstances it may be necessary to augment or replace the use of the DNS records by manual routing information. For example, you may wish to use MailSite on a proxy relay server to route incoming messages to a secure mail server on the LAN. This form allows you to set up a manual routing table to do this.

The manual routing table consists of an ordered list of entries that are shown in a scrolling list. Each entry consists of a domain mask, a combination rule, and one or more associated routes.

The order of the entries in the manual routing table is significant. It is processed top-to-bottom, and the first matching entry is used. Thus, more specific entries (not containing wildcards) should be positioned near the top of the list, and less specific entries (containing wildcards) towards the end of the list. Use the Up and Down buttons to move entries around.

To specify the routes on which messages for the domain are sent, select a domain mask and click the Routes button.

Domain Mask

Enter the name of the domain for which a route is being defined. The domain may include one or more wildcards (*). For instance, a domain of *abc.com will match both user@one.abc.com and user@two.abc.com. Do not use the @ symbol with the domain in this field. Routing is done strictly on the mail domain name not on the user name.

Option

The option determines how the manual route relates to the information returned by the DNS. It can have three values:

- Force: The manual route overrides any routes in the DNS records
- Default: The manual route will only be used if the DNS does not return any routing information for the domain

- Additional: The manual route will be merged with the routes returned by the DNS.

Route Definition

Use this dialog to set manual routes for the selected domain.

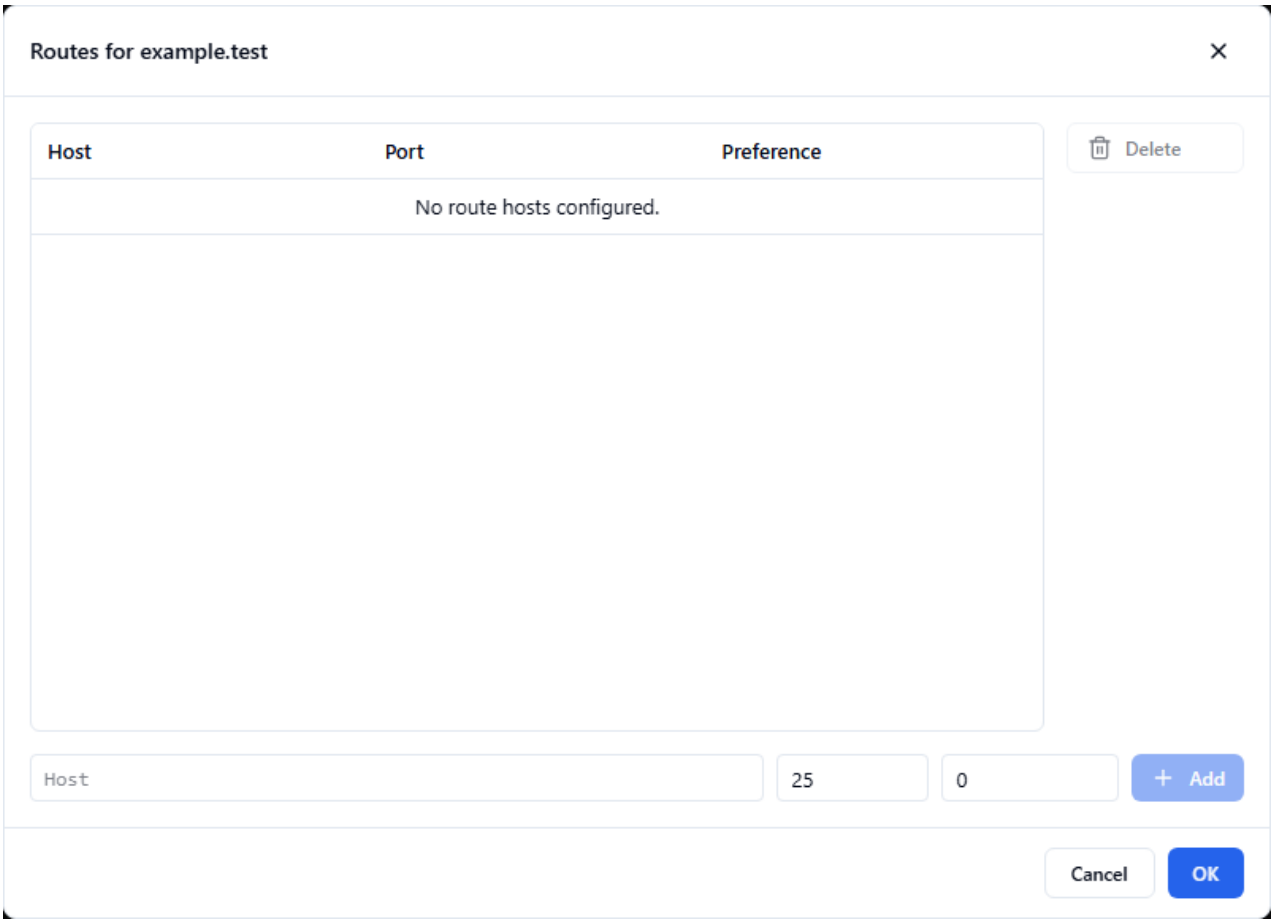

Figure 53 Route Definition

Each domain can have one or more manual routes.

Host

Enter the name (or IP address) of the host for the manual route. This will override or supplement the DNS record for this domain (depending on the preference setting).

Port

Enter the port number on the destination host to which MailSite will connect to deliver outgoing mail. The default is 25. It is usually not necessary to change the default.

Preference

Enter the preference number for this route. Lower preferences are tried first. This is equivalent to the MX preference number in DNS.

Quotas

To enable support for mailbox quotas, open the Server folder in the Windows Console and select the Quotas icon. To configure the domain-wide default quotas (which apply if a mailbox does not have an explicit quota set), use the Domain General Page. To configure individual mailbox quotas, use the Mailbox General Page.

The Quotas dialog looks like this:

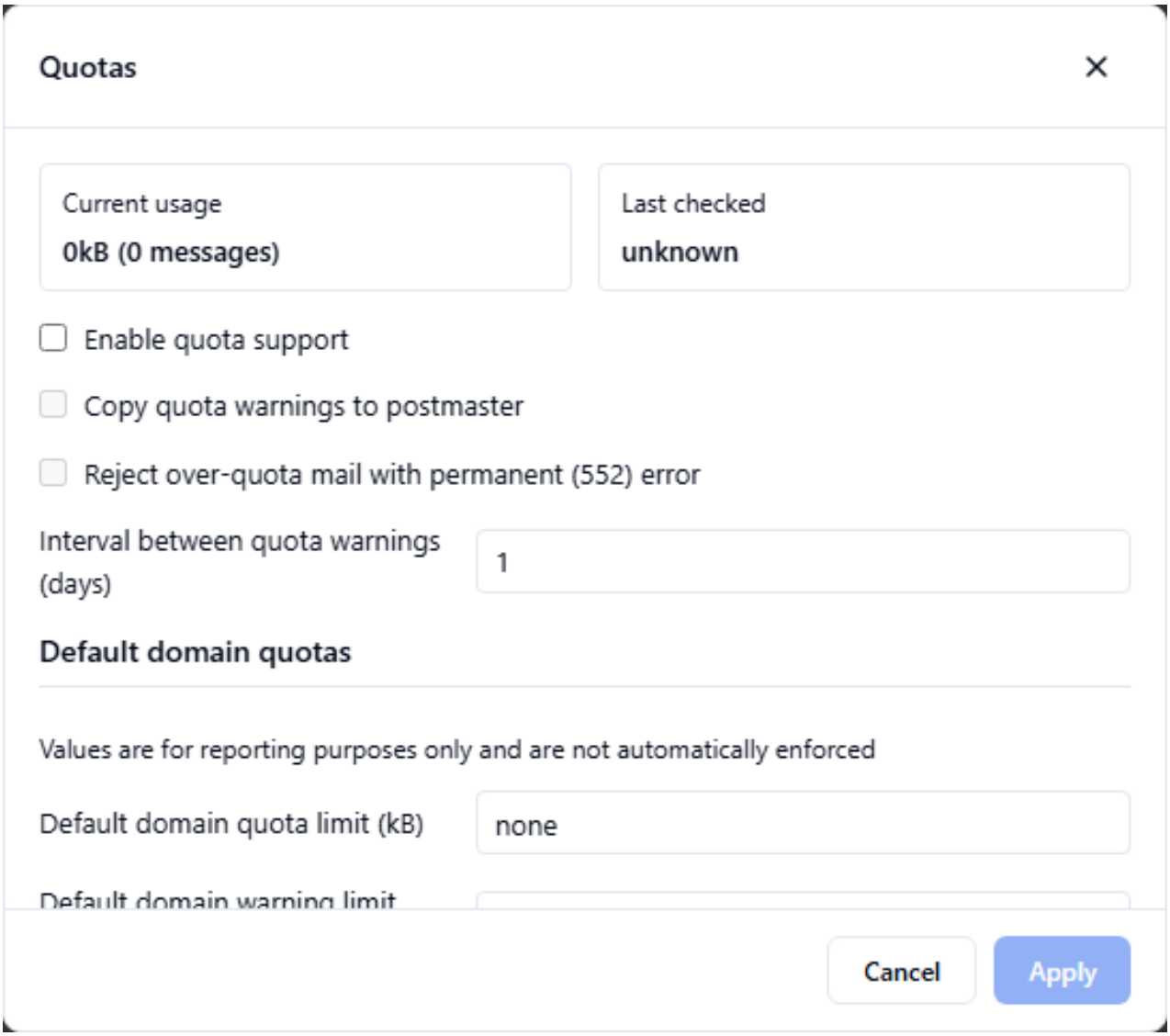

Figure 54 Quotas

The Quotas dialog displays the approximate number of messages and their total size, and allows you to set certain associated parameters.

Enable quota support

Check this box to turn on quota checking. If quota support is enabled, then incoming mail to an over-quota mailbox will be rejected.

Copy quota warnings to postmaster

When a mailbox exceeds a warning level, and when it exceeds its quota limit, a message is placed in the mailbox. This flag controls whether this message is also sent to the domain postmaster.

Reject over-quota mail with permanent (552) error

When a message arrives that would cause a mailbox to exceed its quota, SMTPRA can reject the message, indicating to the sender that retrying is unlikely to help. This alerts the sender to the fact that the message has not been received, and cannot be at this time. If this option is not checked, the default response is 452 indicating a temporary failure.

It should be noted that internet standards suggest 552 as the correct response. 452 has been retained as the default as MailSite has worked this way for many years and administrators are used to this behavior.

Interval between quota warnings (days)

This controls how often the quota warning message is generated.

Default domain quota limit (kB)

If quota limits are not set for each individual domain, this default value will apply. Quotas for the total size of a domain are not enforced, but can be entered here to assist with administration and as the basis of database queries.

Default domain warning limit (kB)

If warning limits are not set for each individual domain, this default value will apply. Quotas for an entire domain are not enforced, but can be entered to here to assist with administration and as the basis of database queries.

Agents

Click the Agents icon to configure the Server Agent and the Archive Directory:

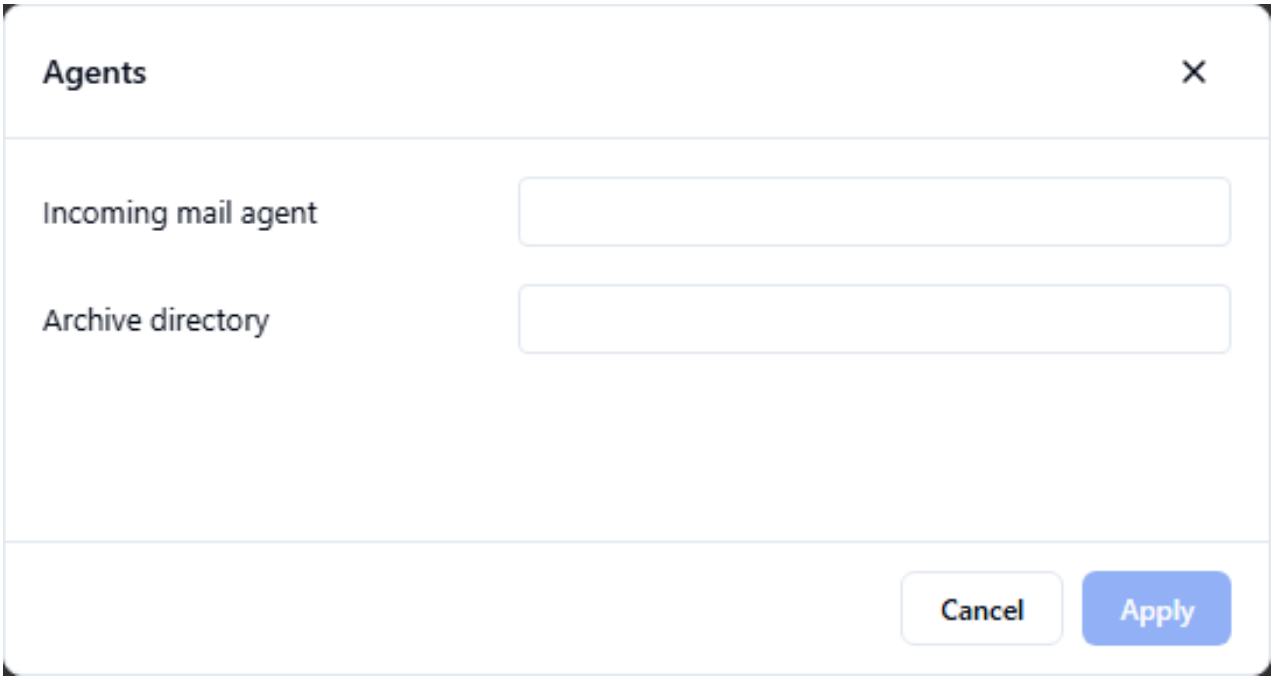

Figure 55 Agents

Incoming Mail Agent

MailSite executes the Server Agent for every message that is received. The agent is passed the names of two files: the message file itself, and a file containing SMTP envelope information.

The message file is a text file with a MSG extension. The file containing the SMTP envelope information is known as the recipients file, although it contains more than just recipient information. The recipients file is a text file with a RCO extension when it is passed to the Server Agent. When the agent terminates, MailSite will rename the file to its normal RCP extension.

This field should contain a command-line template. An occurrence of %r in the template is replaced by the name of the recipients file, and an occurrence of %m in the template is replaced by the name of the message file. The resulting command line is then passed to the command-line interpreter to execute.

Thus, if the template were:

copy "%r" c:\temp & copy "%m" c:\temp

MailSite would copy both the message file and the recipients file to the c:\temp directory.

Multiple commands can be executed, as in the above example, by separating each command with the & character (or by using a batch file).

The agent is executed by the SMTPRA service and agent inherits the access rights of the SMTPRA service. If you installed MailSite to run its services as a specific Windows user, you must grant this user execute access for the agent application.

It is important that the Server Agent should not take too long to execute. Otherwise, a busy mail server could easily run out of memory or saturate its processor.

It is possible for the Server Agent to delete or move the message file and recipients files – for instance if the agent determines that the message contains a virus. In this case, the agent should respect the wishes of the sender regarding delivery status notifications, as expressed in the recipients file. This means that the agent may need to send a Delivery Status Notification message. Not to do so may be a violation of the SMTP protocol.

Archive Directory

A copy of every incoming message can be archived to a directory by entering the directory name in this field. MailSite will create a folder under this directory with the name equal to the current date. MailSite will copy every incoming MSG message file and corresponding RCP recipients file into this directory.

Configuration Connector

Open Server, Configuration Connector to select Registry or SQL. Use SQL Connector to configure the SQL server, authentication, timeouts and database schema, and test the connection. The current workflow validates SQL settings and restarts services when switching the active connector. Schedule the switch and retain a recovery backup.

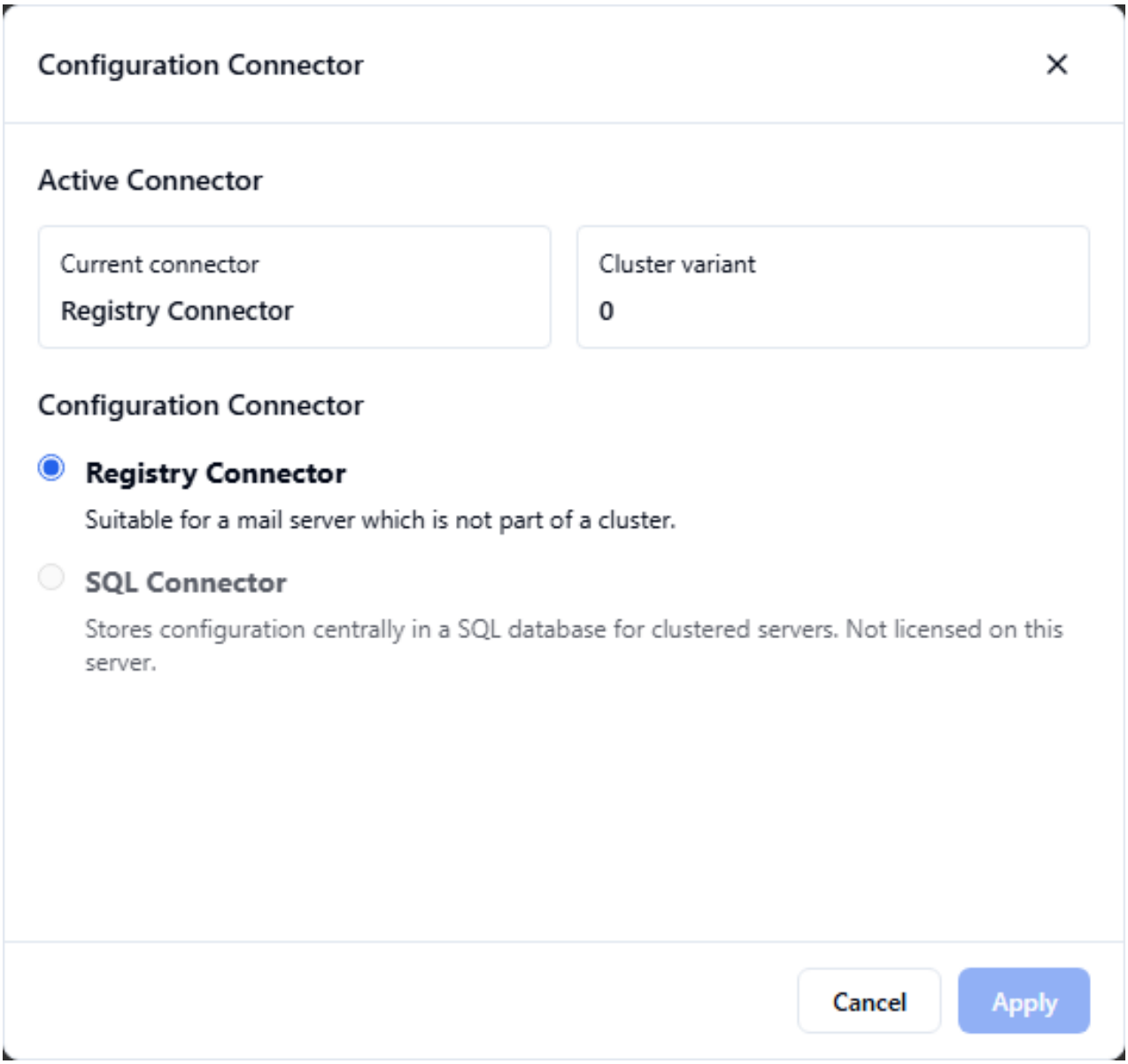

Figure 56 Configuration connector selection

This replaces the native connector-selection and ODBC wizards. See the SQL Connector chapter for migration and verification. The SQL configuration connector is separate from the legacy Database Mailbox Plugin.

Banner Insertion

Click the Banner Insertion icon to configure the e-mail banners to be added to all messages received via SMTP:

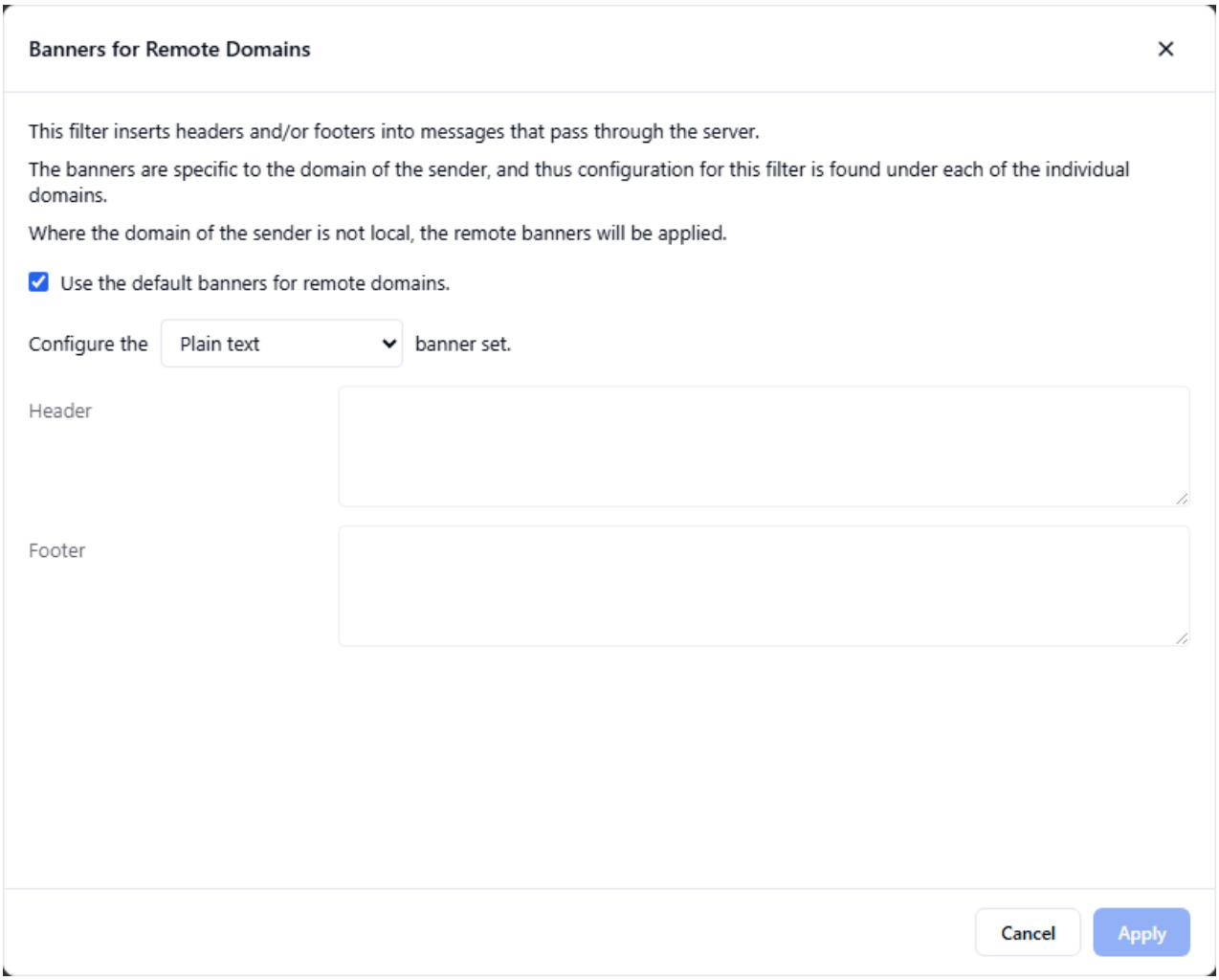

Figure 57 Banner Insertion

Banners can be defined at the domain level and the server level. Domain-level banners are added to all messages sent from that domain, while server-level banners can be added to all mail sent from remote domains (that is, domains not defined in MailSite).

There are two types of banners: Header and Footer. Headers are inserted at the top of the body of the email message, while footers are appended to the bottom of the message body (above all attachments).

You can set separate banners for plain text messages and HTML messages. This allows you to insert sophisticated HTML content (including banner advertisement graphics) in messages that contain HTML. If an HTML banner is not defined, the plain text banners for the domain are applied to both text and HTML messages.

Traffic Counters

Click the Traffic Counters icon to configure the traffic data collected by MailSite.

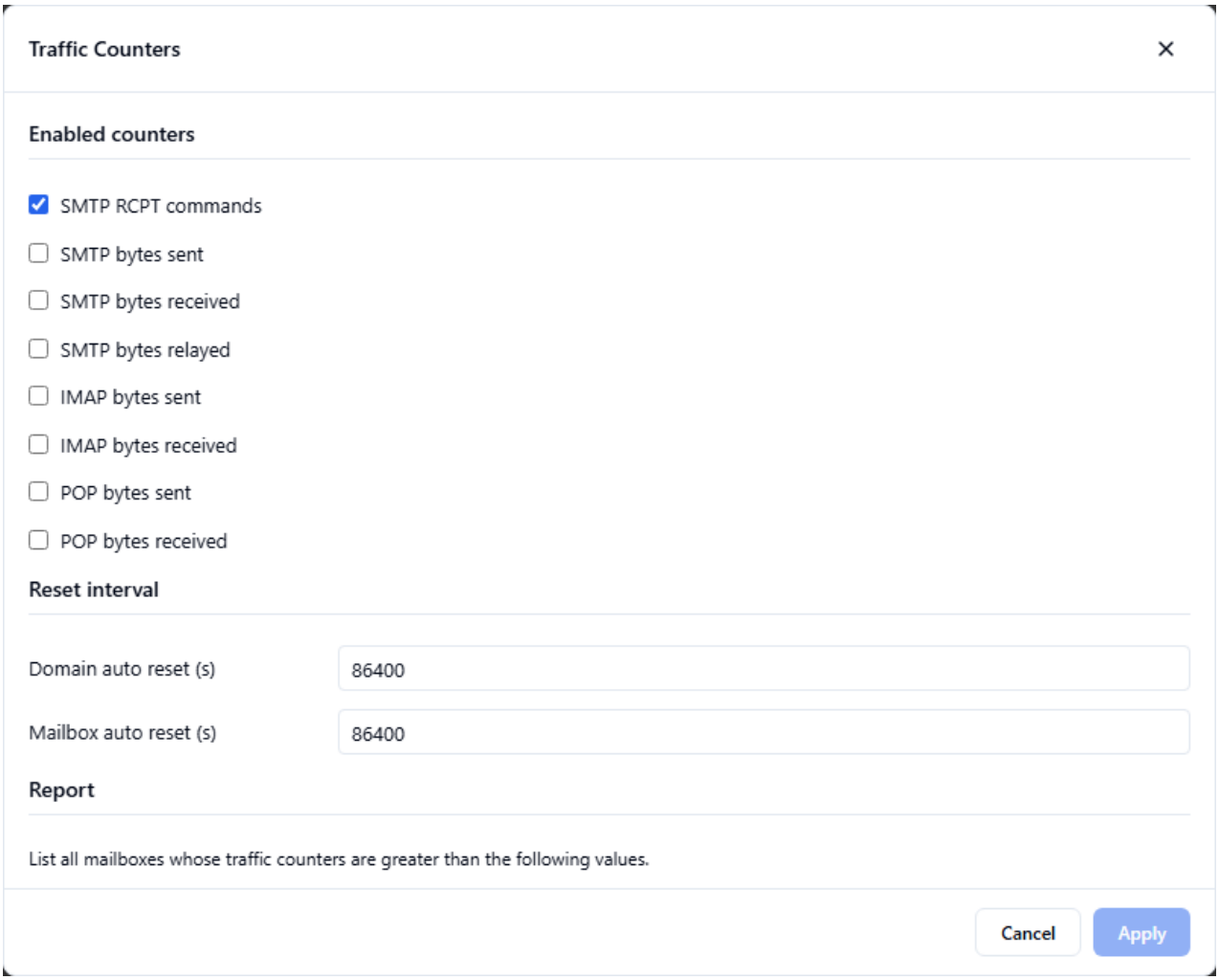

Figure 58 Traffic Counters

Traffic counters are enabled and the settings configured at server level. Once enabled, the statistics are collected for all relevant traffic and the displayed at domain level and mailbox level. The counters will be automatically reset at a configurable interval, by default this will be every 24 hours.

Reports can be generated which will either contain all data, or only data for the most heavily used mailboxes in each of the monitored categories. The report produced is in CSV format and can be saved to any location.

Wireless Carriers

Click the Wireless Carriers icon to edit the list of wireless carriers available for SMS based notification.

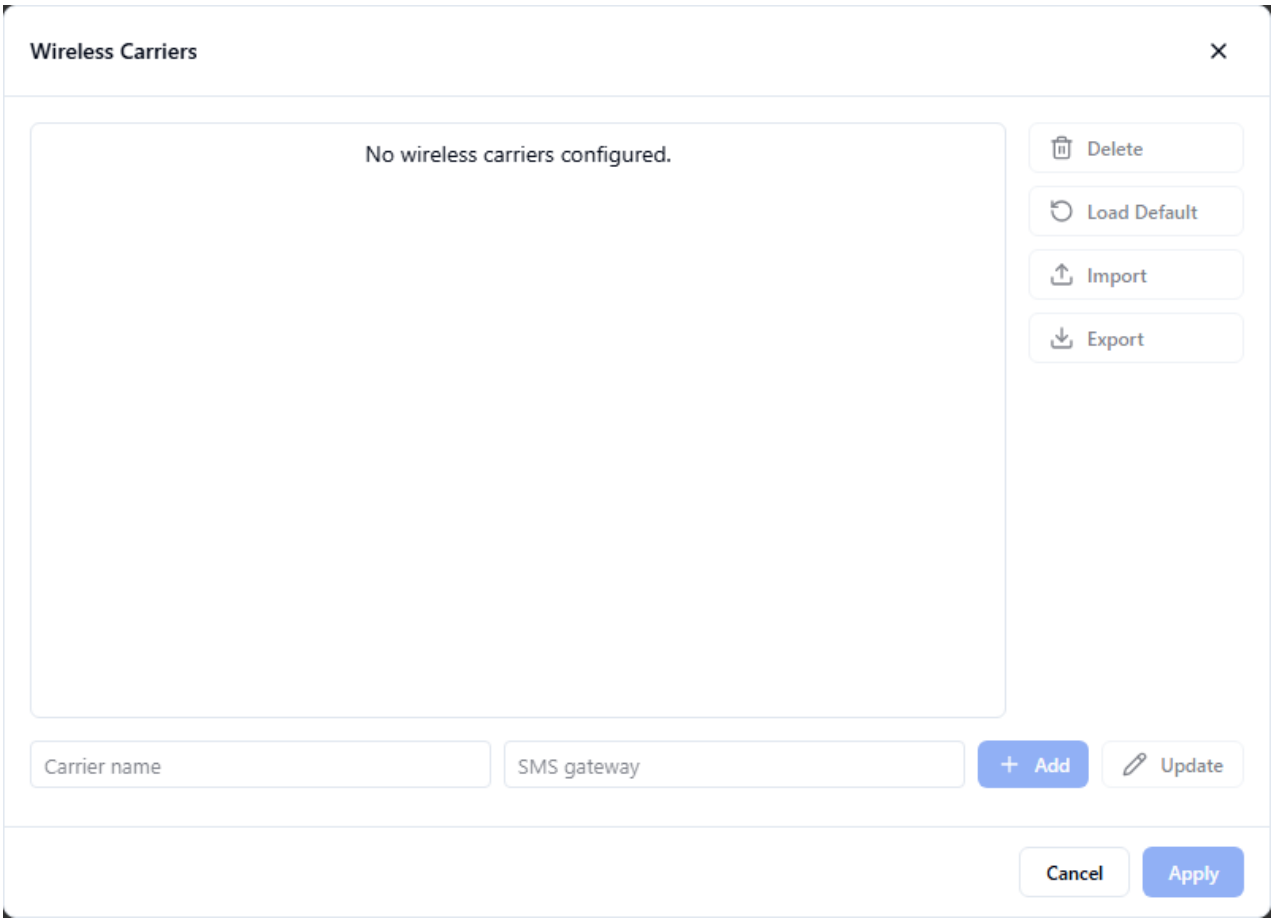

Figure 59 Wireless Carriers

A selection of carriers have been added to MailSite by default. If this list is not suitable for your customers, it is easy to delete unwanted entries and add new ones. Once this list is modified, end-users will see the modified list of carriers when setting up SMS notifications in MailSite Express.

If the list becomes corrupted due to incorrect updates the Load Default button will restore the default MailSite list of carriers.

Calendaring

Click the Calendaring icon to configure calendaring settings for this server.

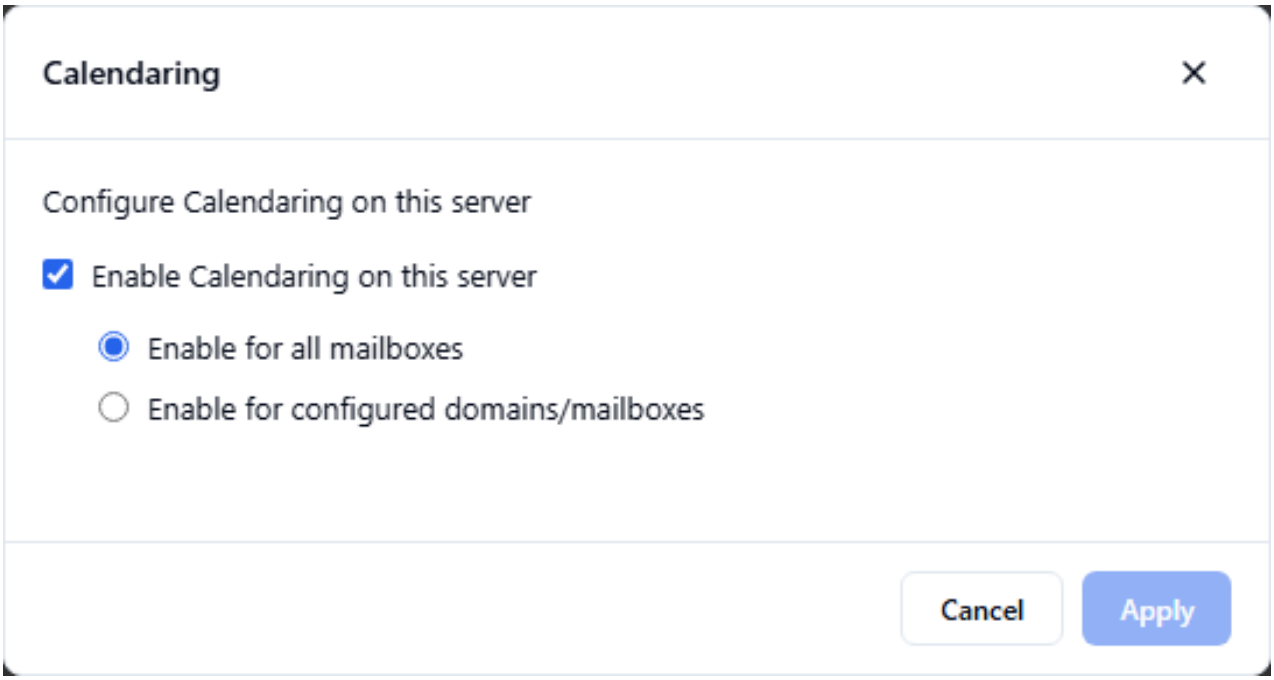

Figure 60 Calendaring

Once enabled, calendaring functionality will be available to either all users or those configured at domain and mailbox level. Calendaring support is part of the MailSite license and so not all licenses will include calendaring for every mailbox.

Wireless Sync

Click the Wireless Sync icon to configure over-the-air mobile device synchronization for this server.

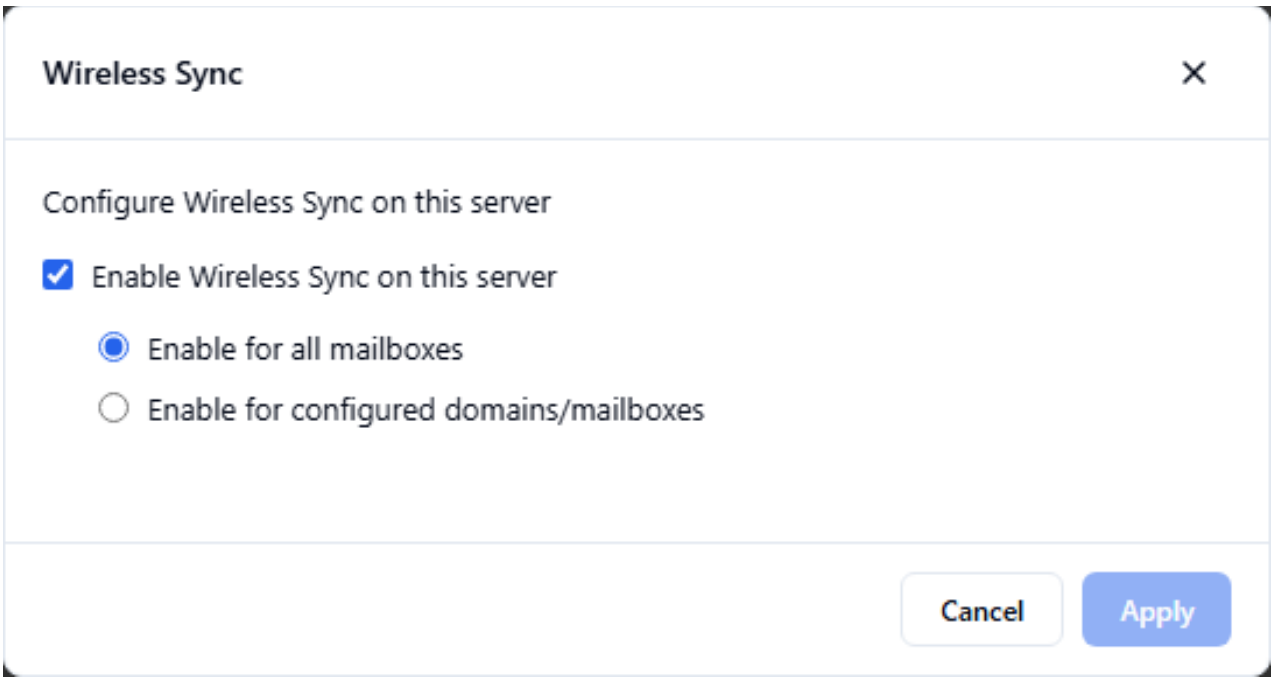

Figure 61 Wireless Sync

Once enabled, wireless synchronization functionality will be available to either all users or those configured at domain and mailbox level. Wireless synchronization is part of the MailSite license and so not all licenses will include this feature for every mailbox.

Security

MailSite provides security features to help protect your server against abuse and unsolicited commercial e-mail (also known as spam). MailSite integrated anti-spam and anti-virus filters and sieve filtering engine are found under the Filtering folder. Other Security features can be seen by clicking on the Security folder:

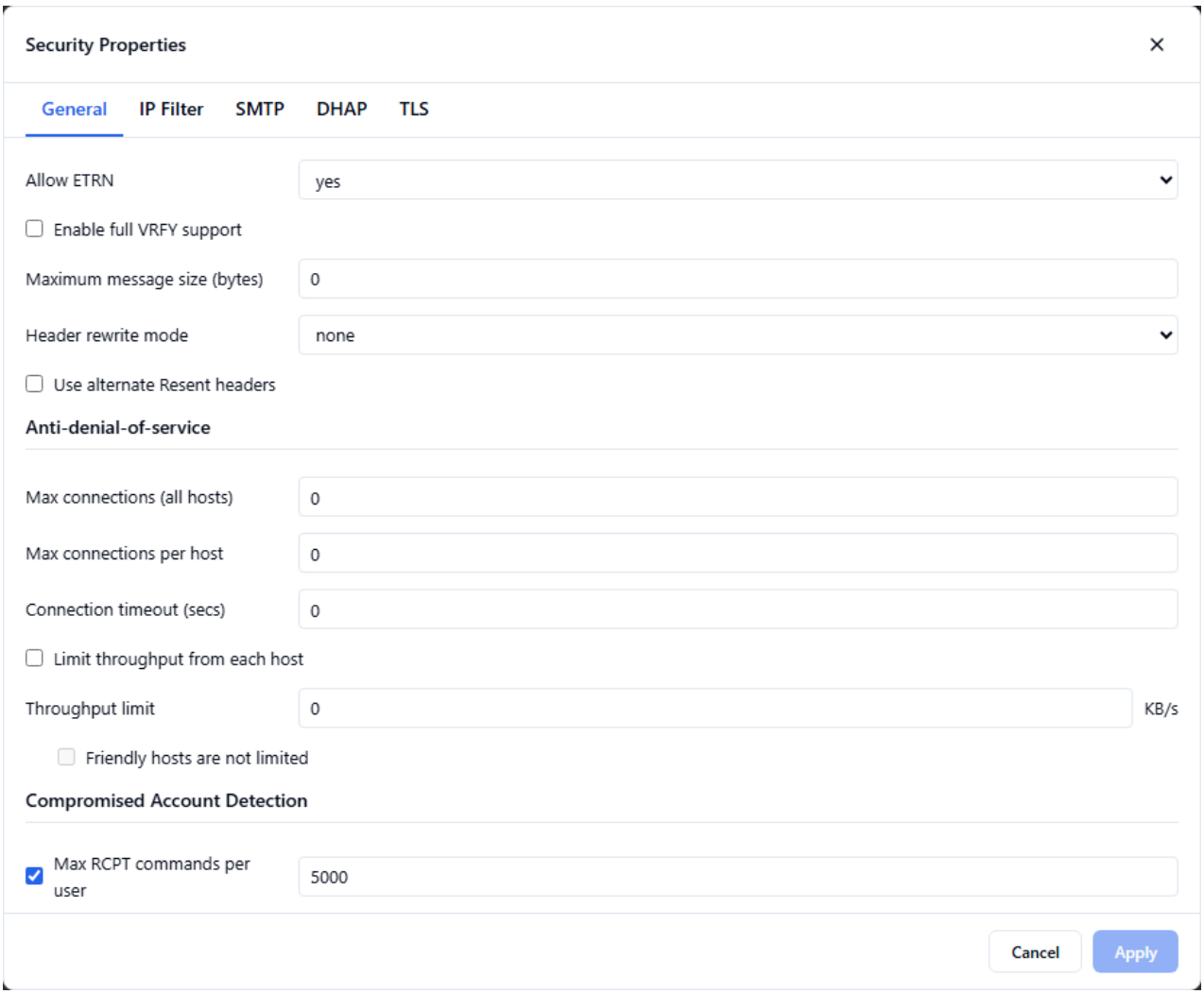

Figure 62 Security

These Security properties help you block unauthorized use of your mail server. It is easy to block authorized access to your mail server by mistake, so take great care to set these properties. Refer to the section on Advanced SMTP Security for more information. You can also set these policies through the Anti-Relay Wizard and SMTP Security Wizard.

General Security Settings

The Security Properties dialog is invoked by double-clicking on the Security Properties icon:

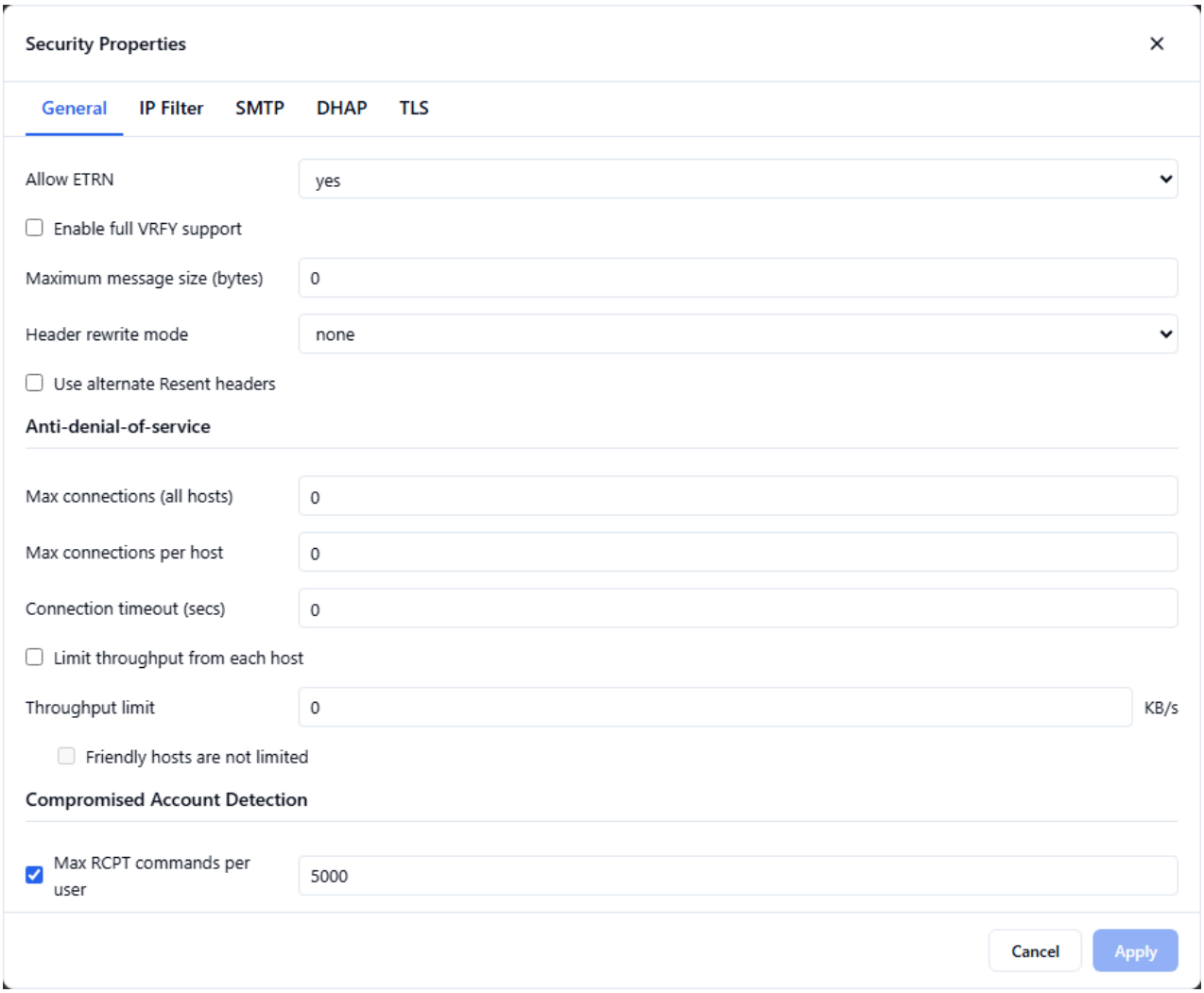

Figure 63 General Security Settings

Enable Full VRFY Support

VRFY is an SMTP command that allows sending mail servers to verify the To: address. By default, a command of the form VRFY name@domain.com will return a successful response if this server accepts mail for domain.com.

If Enable Full VRFY Support is set, then MailSite will respond to the VRFY command with information about whether name@domain.com is known, and if so whether it is a mailbox or a mail list.

If you leave this box unchecked, it reduces the amount of information an attacker or spammer can find out about your users.

Authenticated ETRN

The SMTP ETRN command is used to request an SMTP server to start sending mail for a particular domain. (This command is used by the MSSTART utility.) If you check this box then the SMTP client must be authenticated (using the AUTH command with a valid mailbox name and password), otherwise the ETRN command will be rejected.

Maximum message size (bytes)

Enter the maximum message size in bytes that the SMTP Receiver will accept. The default is 0, which means that there is no size limit apart from memory and disc space constraints.

Header Rewrite Mode

Select a format that MailSite will use to rewrite an invalid From header address. The choices are:

- None

- “Jane User” <user@domain>
- user@domain (Jane User)

Use Alternate Resent Headers

This option controls the way that MailSite defines Resent headers, which are used to save information about forwarded messages. By default, resent headers are created in the format Resent-Header, such as Resent-To and Resent-From. You can change the format of resent headers by enabling this field, which causes these headers to be created in the format X-Resent-Header.

Anti-Denial-of-Service: Max connections (all hosts)

This setting provides a limit to the total number of incoming SMTP connections that MailSite will respond to at any time. When this number of connections are active, SMTPRA will no longer accept new connections until a current connection has been closed.

Anti-Denial-of-Service: Max connections per host

This setting limits the number of incoming SMTP connections allowed from any one system. When this number of SMTP connections from any one host are active, SMTPRA will no longer accept new connections from that host. This option is very useful for containing potential damage from an abusive system without blocking incoming connections from other (non-abusive) systems.

Anti-Denial-of-Service: Connection timeout

This option sets a limit to the number of seconds that MailSite will keep open a non-responsive SMTP connection.

Anti-Denial-of-Service: Limit throughput from each host

This option provides a throttle on the amount of data (in kilobytes per second) that SMTPRA will accept from any one host. This allows you to control DoS attacks that send large amounts of data over relatively few connections. When using this option it is recommended that you exempt your “friendly” hosts from this limit to avoid slowing mail traffic from your own network.

Anti-Denial-of-Service: Compromised Account Detection

This option sets a limit on the number of RCPT commands a user account can send in a given period. Once this limit is reached SMTP access for this user is revoked preventing excessive spam relay from compromised accounts.

SMTP Security Properties

The SMTP Security Properties dialog is invoked by clicking on the SMTP tab:

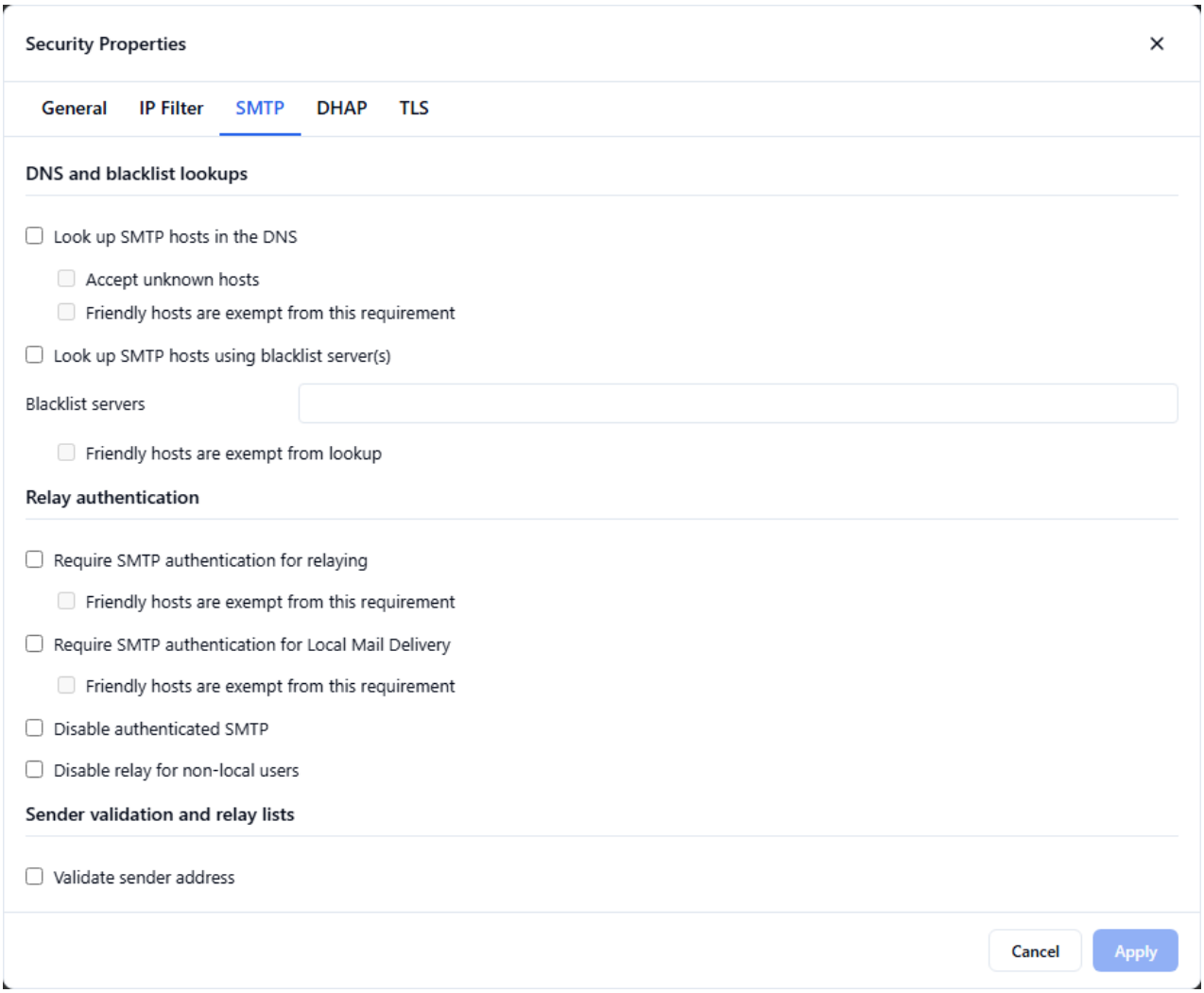

Figure 64 SMTP Security Properties

Lookup SMTP hosts in the DNS

MailSite can be configured to perform a reverse lookup of the IP address of the incoming SMTP host. The resulting host name is used in the log files and in the Received: header. If the reverse lookup fails then connection is rejected unless the Accept Unknown Hosts option is turned on.

This option can help block unauthorized SMTP relay because many junk mail distributors do not have a valid reverse DNS record.

This option can have a serious impact on performance. MailSite must submit a reverse DNS lookup query for each incoming connection. If your DNS server is slow then incoming connections may experience significant delays.

Lookup SMTP hosts using blacklist server(s)

This option allows MailSite to block messages coming from known sources of junk email, as compiled by blacklist servers. If you check this box, and a host listed with the given blacklist server connects to MailSite, then all mail from that server will be rejected. Note that checking this box may slow down the rate at which you can accept mail because of the extra time required to perform the lookup.

To use this option, specify the host name of the blacklist server in the Blacklist servers field. When entering multiple values in field separate each entry with a comma.

When using blacklist servers it is recommended that you exempt your “friendly” hosts from blacklist lookup. This will prevent numerous unnecessary blacklist queries that would otherwise slow MailSite’s SMTP performance. Addresses on the DHAP whitelist will also be exempt.

Require SMTP authentication for relaying

Checking this option requires that anyone relaying mail through your SMTP server must log in via Authenticated SMTP. This prevents unknown users from using your server to relay junk mail. However, this also requires that all of your end users have mail clients that support Authenticated SMTP and that they enable this feature in their client.

This feature also includes and option to exempt your “friendly” hosts from SMTP authentication. Enabling this option allows non-authenticated SMTP traffic from hosts listed under the Accept mail for relay from these friendly hosts… option.

When this option is selected, the Disable authenticated SMTP option in this window is automatically disabled.

Require SMTP authentication for Local Delivery

Checking this option requires that anyone sending mail to local users through your SMTP server must log in via Authenticated SMTP. This prevents unknown users from sending you junk mail. However, this is a very conservative approach that should not be used for a publicly addressed SMTP server as it will stop remote MTAs sending legitimate mail to your users. It also requires that all of your end users have mail clients that support Authenticated SMTP and that they enable this feature in their client.

This feature also includes an option to exempt your “friendly” hosts from SMTP authentication. Enabling this option allows non-authenticated SMTP traffic from hosts listed under the Accept mail for relay from these friendly hosts… option.

When this option is selected, the Disable authenticated SMTP option in this window is automatically disabled.

Disable relay for non-local users

Checking this box is a quick way to stop your mail server being used to relay spam to other sites. If you check this, then MailSite will not accept mail for relay unless the MAIL FROM: address in the SMTP envelope refers to a local domain. (Note that the MAIL FROM: address specifies the return address for non-delivery reports – it is not necessarily the same as the From: address in the message header.)

This option will not protect your mail server against determined spammers, who are capable of forging the MAIL FROM: address. You can get better protection using the Require SMTP authentication for relaying option, or through the Accept mail for relay from these friendly hosts mask list. (Note that if you set up the Accept mail for relay from these friendly hosts list, you should turn off this option since it overrides the value in that field.)

Validate sender address

If you check this box MailSite will attempt to verify the sender address supplied. MailSite will look up the domain name supplied in the MAIL FROM: command, and if it is local, will ensure that the mailbox exists. If the domain is remote, MailSite will ensure that there is a valid A record or MX record in the DNS for it. If there is not, the address is assumed to be illegal, and the mail will be rejected. As local addresses have to exist, this feature will not be appropriate for some systems, such as those where users need to send from non-existent mailboxes, relying on catchall to deliver replies.

Turning this feature on may reduce performance since the DNS server may take some time to respond.

Max number of recipients per message

You can specify the maximum number of recipients allowed for an individual message. These are the recipients specified on the SMTP envelope (that is, given by the RCPT TO: command). If you specify 0, there is no maximum.

Disable authenticated SMTP

Check this option if you do not want to use authenticated SMTP to control mail relay. Enabling this field automatically disables the Require SMTP authentication for relaying field.

Reject All Incoming Mail From These Addresses

If you click on Reject All Incoming Mail From These Addresses from the SMTP tab of the Security Properties window, the following form will be displayed:

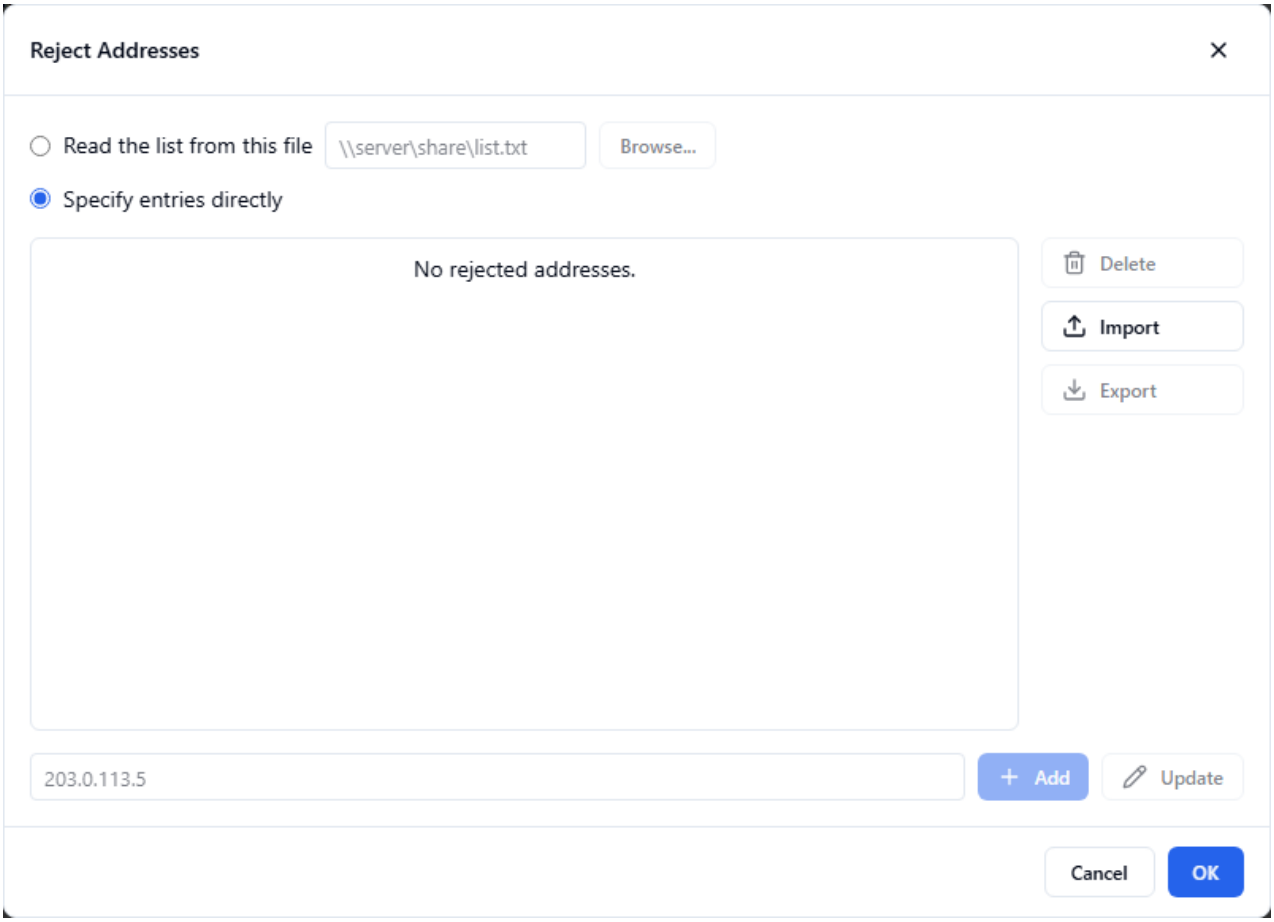

Figure 65 Reject All Incoming Mail From These Addresses

If a message arrives from an e-mail address that is listed in this form, then the message will be rejected. It is possible to enter either a full email address, or to specify the sending domain in the format *@example.com.

Refer to the section on Security Masks and Advanced SMTP Security for more information. You can also set these policies with the SMTP Security Wizard.

Reject All Incoming Mail From These Hosts

If you click on Reject All Incoming Mail From These Addresses from the SMTP tab of the Security Properties window, the following form will be displayed:

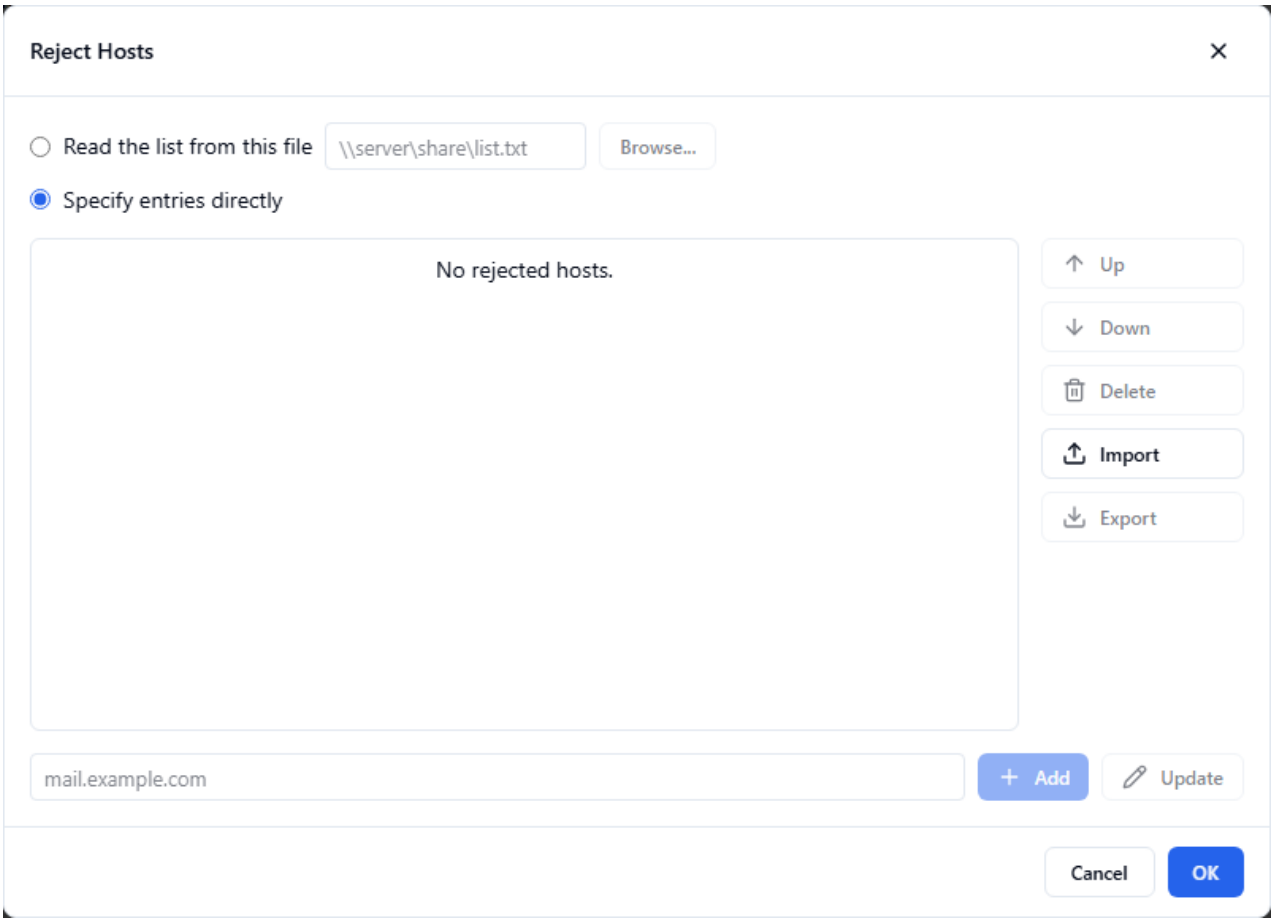

Figure 66 Reject All Incoming Mail From These Hosts

If a message arrives from a host that is listed in this form then the message will be rejected.

If you specify host names as opposed to IP addresses, you must check Look up SMTP hosts In The DNS so that MailSite can determine the host name.

Refer to the section on Security Masks and Advanced SMTP Security for more information. You can also set these policies with the SMTP Security Wizard.

If this list becomes very large, managing it can be difficult and it can eventually degrade SMTPRA performance. For these very large lists, consider representing the entries as subnets using the Reject All Incoming Mail From These Subnets dialog.

Reject All Incoming Mail From These Subnets

If you click on Reject All Incoming Mail From These Subnets from the SMTP tab of the Security Properties window, the following form will be displayed:

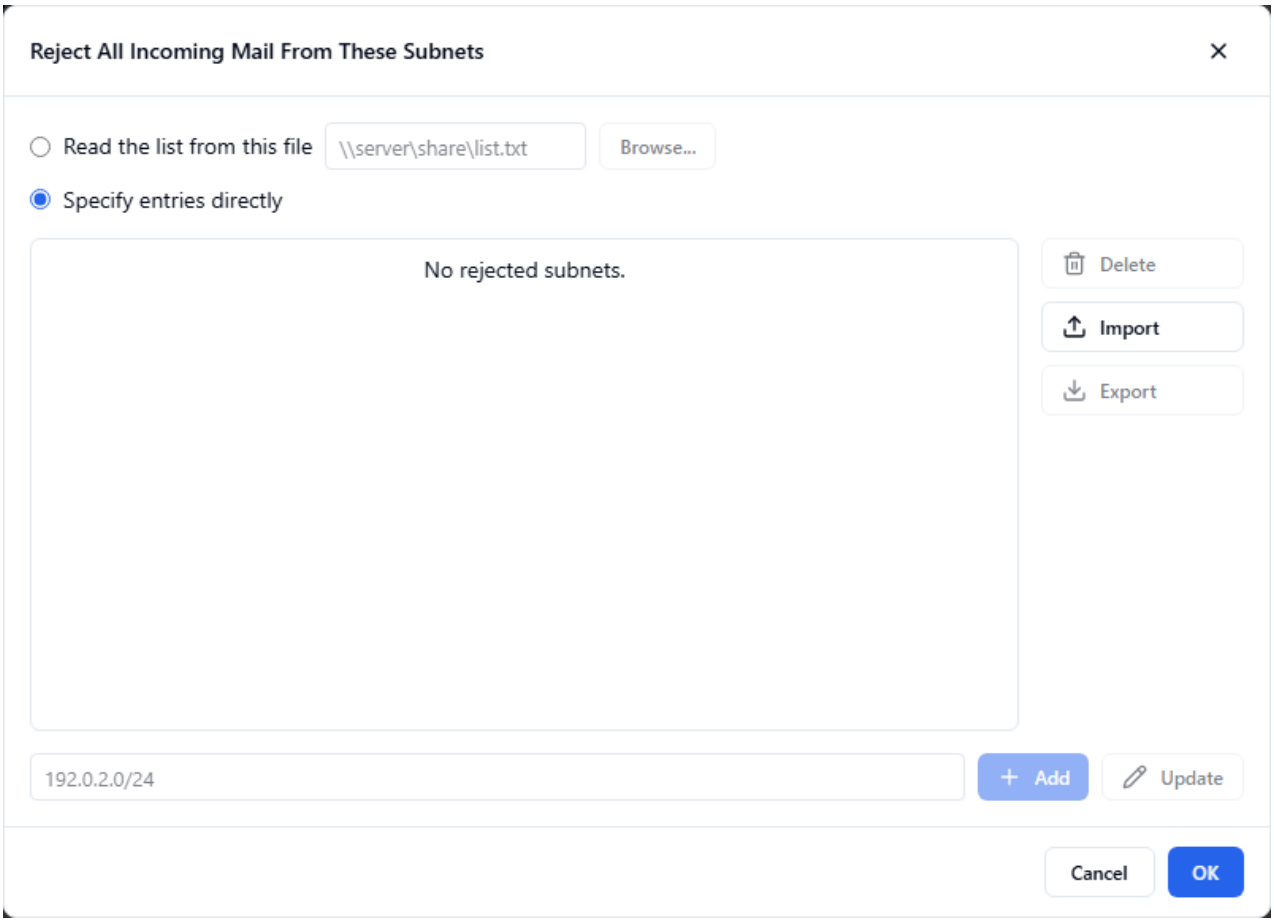

Figure 67 Reject All Incoming Mail From These Subnets

Rejecting incoming mail based on a network address and subnet mask is very similar to Reject All Incoming Mail From These Hosts. Specifying subnets is a more efficient way of managing large lists of addresses you wish to reject mail from. It is therefore recommended that administrators plan to represent large lists of hosts as subnets. Once the addresses are removed from the list under Reject All Incoming Mail From These Hosts, the SMTPRA service should have less information to look up, and will therefore be more efficient.

Network Addresses and Subnet Masks are specified in CIDR format. It is beyond the scope of this document to explain the possible options. Information on CIDR format can be widely found on the internet. MailSite does not support wildcard characters in this dialog.

Accept Mail For Relay To These Domains

If you click on Accept Mail For Relay To These Domains from the SMTP tab of the Security Properties window, the following form will be displayed:

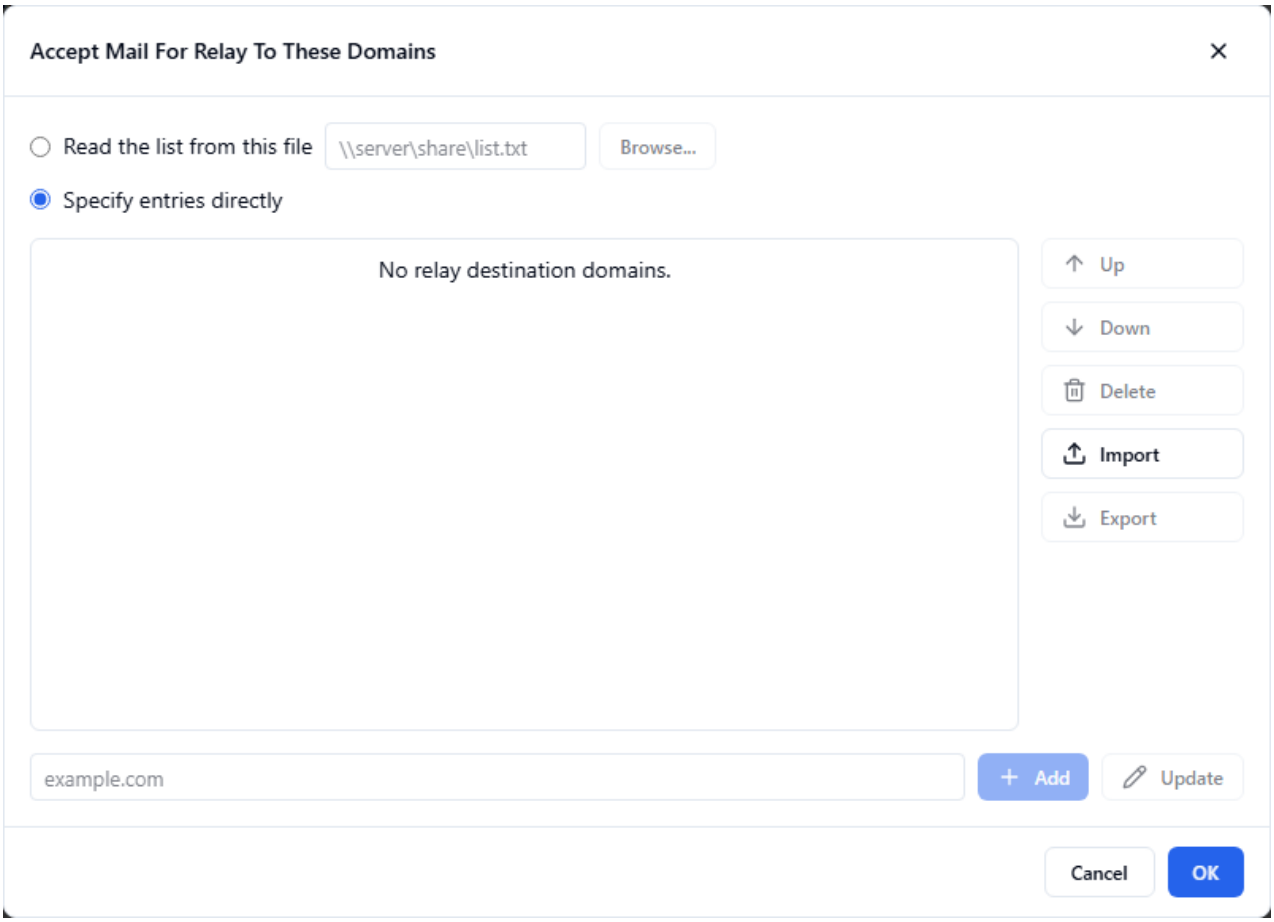

Figure 68 Accept Mail For Relay To These Domains

This feature is useful if your server acts as a secondary SMTP relay host for some other domains. In this case you would enter a list of all of the relay domains in this field.

If a message comes in from a host not listed in Accept Mail For Relay From These Hosts, and the To: address is not local, then the server will refuse to accept the message unless the destination mail domain is listed in this field.

Refer to the section on Security Masks and Advanced SMTP Security for more information. You can also set these policies with the Anti-Relay Wizard.

Accept Mail For Relay From These Friendly Hosts

If you click on Accept Mail For Relay From These Friendly Hosts from the SMTP tab of the Security Properties window, the following form will be displayed:

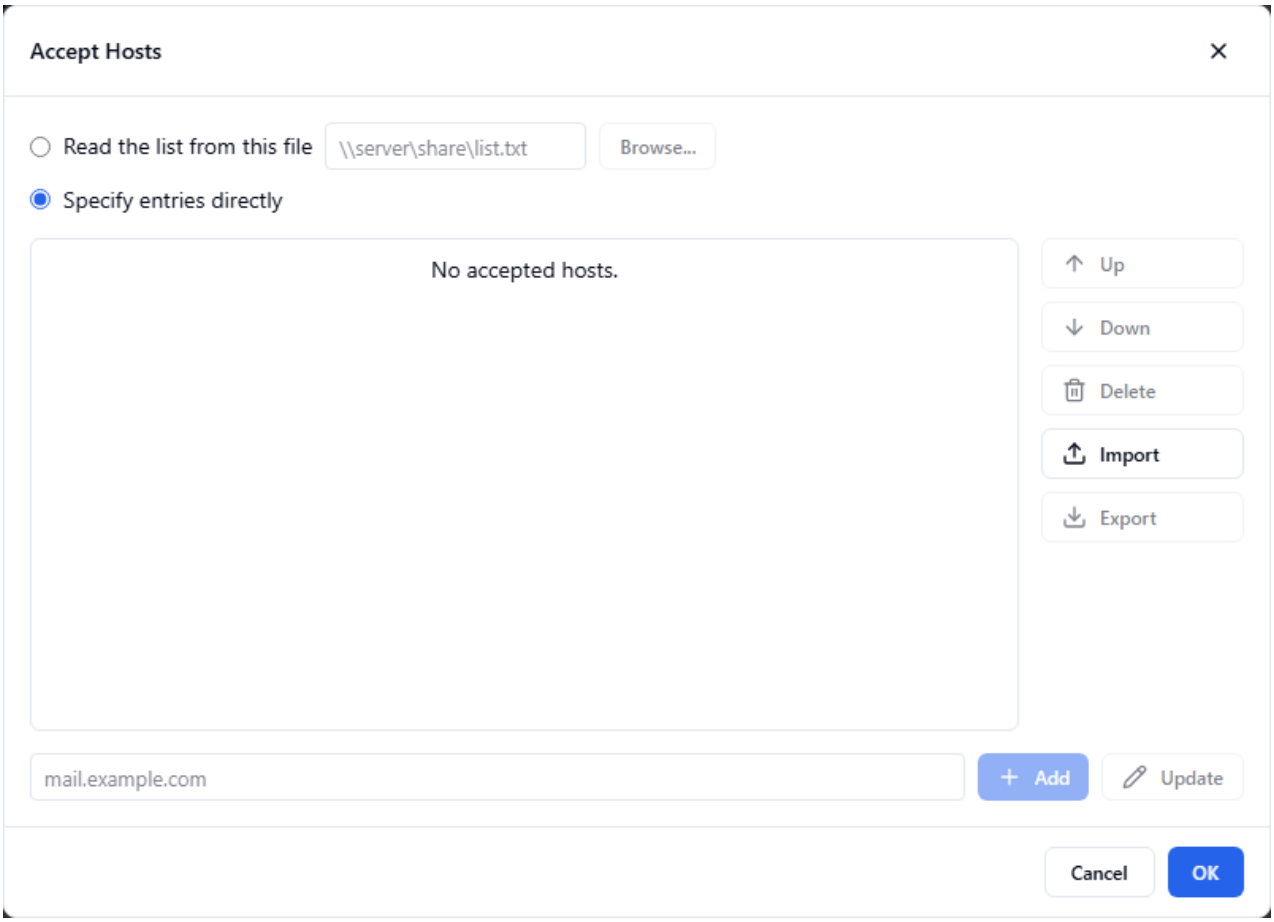

Figure 69 Accept Mail For Relay From These Friendly Hosts

Use this form to enter the host names or IP addresses trusted for relay under the configured policy. A wildcard * matches every host; restrict the list to the intended systems and test both authorized and unauthorized relay.

If a message comes in from a host that is not listed in this field, and the To: address is not local, then the server will refuse to accept the message unless the destination mail domain is listed in Accept Mail For Relay To These Domains.

If you specify host names as opposed to IP addresses, you must check Look up SMTP hosts In The DNS so that MailSite can determine the host name.

WARNING! It is very easy to block valid messages with this feature. Be careful to make correct entries. Test your settings by sending e-mail from a variety of client machines.

Refer to the section on Security Masks and Advanced SMTP Security for more information. You can also set these policies with the Anti-Relay Wizard.

If this list becomes very large, managing it can be difficult and it can eventually degrade SMTPRA performance. For these very large lists, consider representing the entries as subnets using the Accept Mail For Relay From These Friendly Subnets dialog.

Accept Mail For Relay From These Friendly Subnets

If you click on Accept Mail For Relay From These Friendly Subnets from the SMTP tab of the Security Properties window, the following form will be displayed:

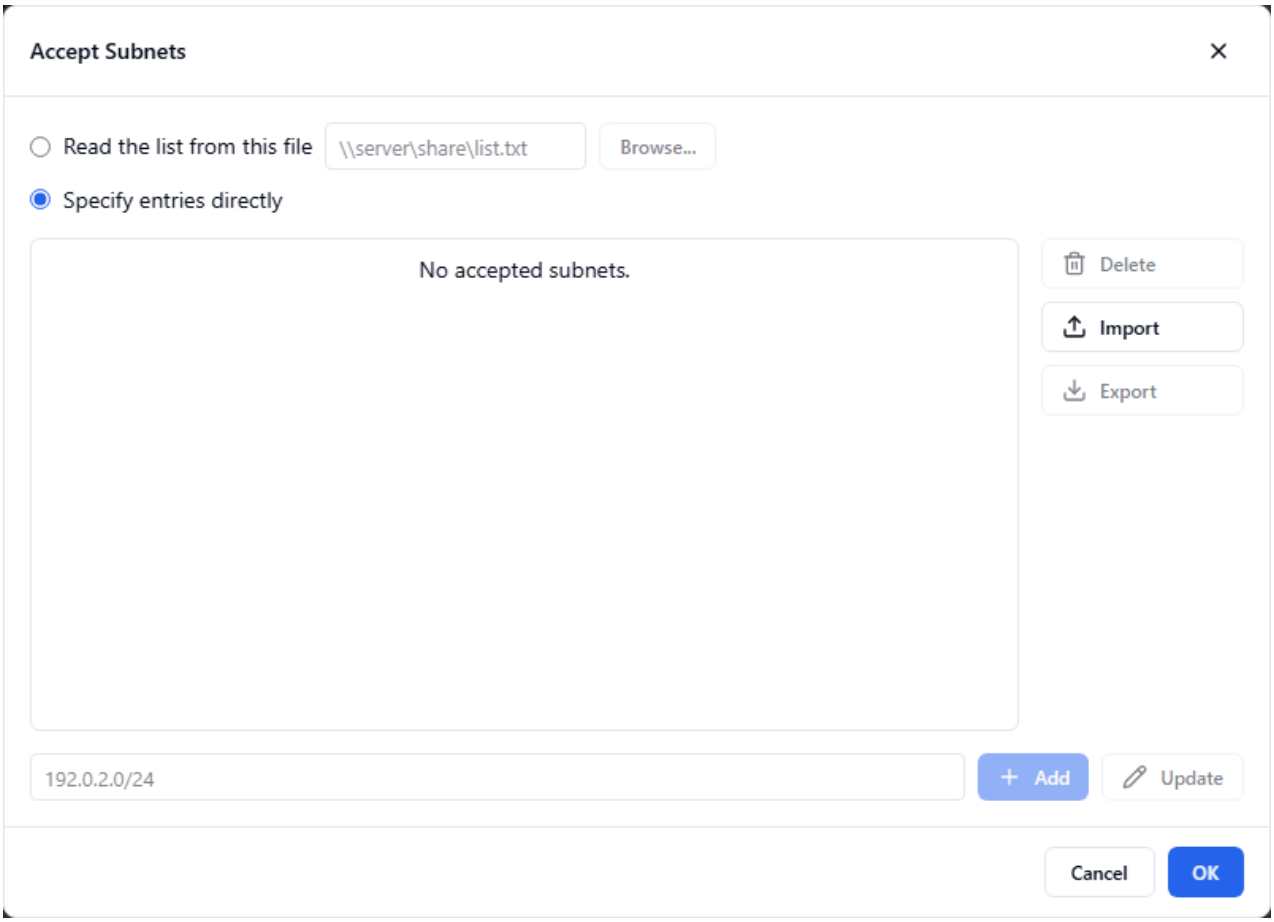

Figure 70 Accept Mail For Relay From These Friendly Subnets

Use this form to enter a list of subnets in CIDR format which are permitted to relay mail through this server. It is beyond the scope of this document to explain the possible options. Information on CIDR format can be widely found on the internet. MailSite does not support wildcard characters in this dialog.

This dialog provides a more efficient way of representing the list accessed through Accept Mail For Relay From These Friendly Hosts and so addresses should be removed from that list once covered by a subnet in this dialog.

WARNING! It is very easy to block valid messages with this feature. Be careful to make correct entries. Test your settings by sending e-mail from a variety of client machines.

Security Masks

You can use the security forms to specify a list of name or address masks. They are called masks because they can contain the asterisk character * as a wildcard. They can also be preceded by an exclamation point, !, meaning negation. The list of names can be read from a text file, or you can specify the names directly in the scrolling list.

If you plan to maintain a list of names in a text file, select the Read mask list from this file option and enter the full name of the text file in the corresponding field. If you are running the Windows Console on the same machine as you are administering, you can use the Browse button to browse for the file. The text file must contain a list of name (or address) masks, one per line.

Alternatively, you can use the Specify mask list directly option. You may then enter a mask in the edit field to the left of the Add button, and click Add to add it to the list. The order of items in the list is significant—use the Up and Down buttons to move them around. The Remove button removes a single entry from the list, while Remove All clears the list entirely. There are also buttons to allow you to import and export name lists to and from text files.

What you are allowed to put in the mask list depends on which button you clicked:

Mask list	Contains	! (Negation marker)

Mask list	Contains	! (Negation marker)
Reject all incoming mail from these addresses	E-mail addresses	Not allowed
Reject all incoming mail from these hosts	Host names or IP addresses	Yes
Accept mail for relay from these friendly hosts	Host names or IP addresses	Yes
Accept mail for relay to these domains	Mail domain names	Yes

A mask list works as follows. A host name (or IP address, domain name or e-mail address, depending on the list in question) either matches or does not match the list. The host name is tested against each mask in the list in turn, starting from the top. If it fits the mask, this is treated as a match, unless the mask is preceded by an exclamation point (meaning “exclude from the list”). This is treated as a failure to match the list, and no further masks in the list will be examined. If the end of the list is reached without a match being found, the host name is deemed not to match the list.

DHAP Security Properties

DHAP settings are invoked by clicking on the DHAP Settings tab in the Security Properties dialog.

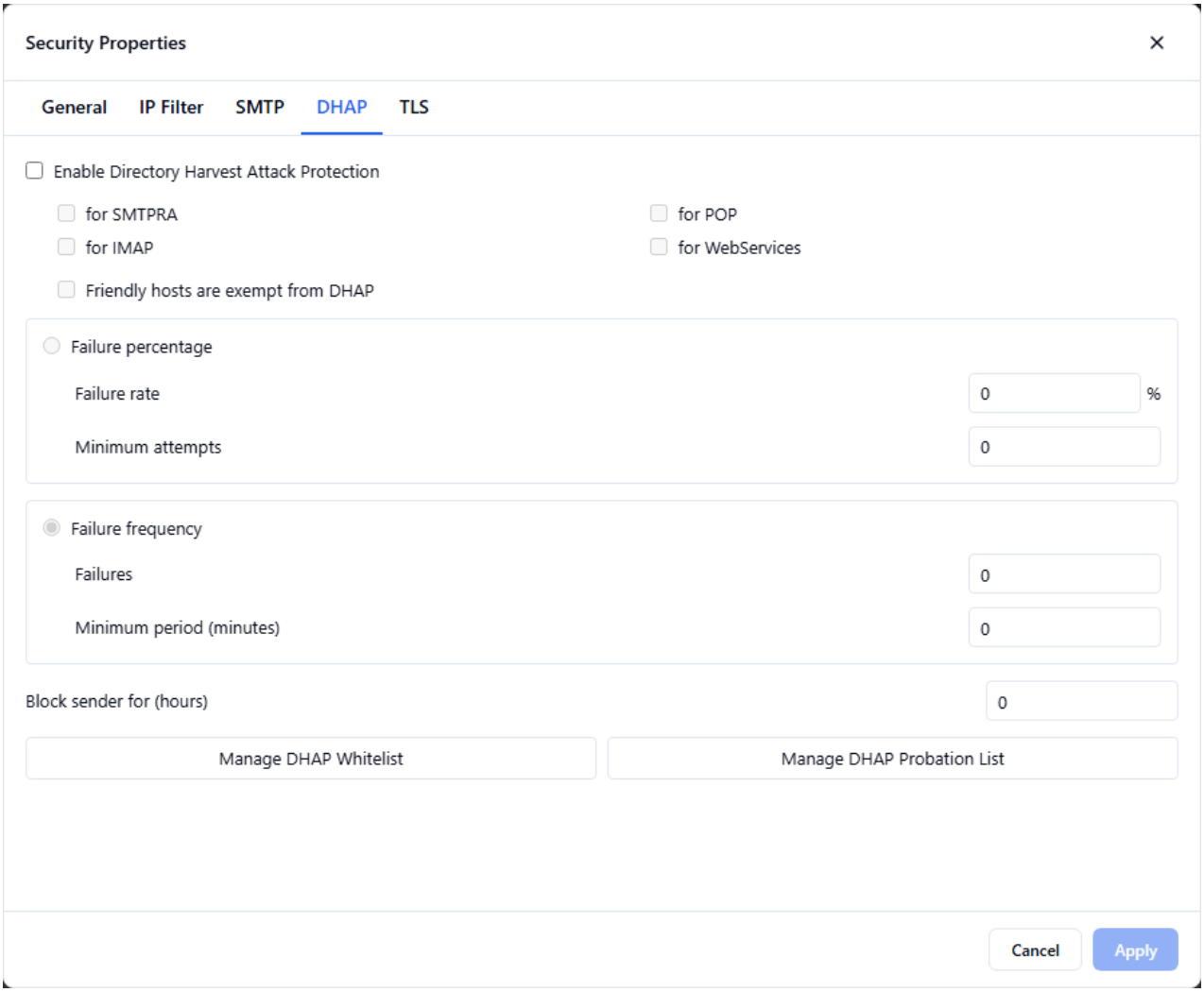

Figure 71 DHAP Security Properties

Enabling DHAP

DHAP is not enabled by default.

To enable DHAP check the “Enable Directory Harvest Attack Protection” checkbox then check the appropriate boxes for the services you wish to detect DHAP on.

Disabling DHAP

If you wish to disable DHAP on a single service uncheck the box relating to that service. To fully disable DHAP uncheck the “Enable Directory Harvest Attack Protection” checkbox. This will halt the collection of any statistics on connecting hosts and allow hosts that have been deemed harvesters to reconnect.

DHAP Detection Methods

MailSite can prevent a DHA in two ways. Only one of these methods will be active at any time when DHAP is enabled. Enabling DHAP will allow you to choose and configure one of the two detection methods.

Percentage failure detection method

To select this method of detection select the Failure Percentage option.

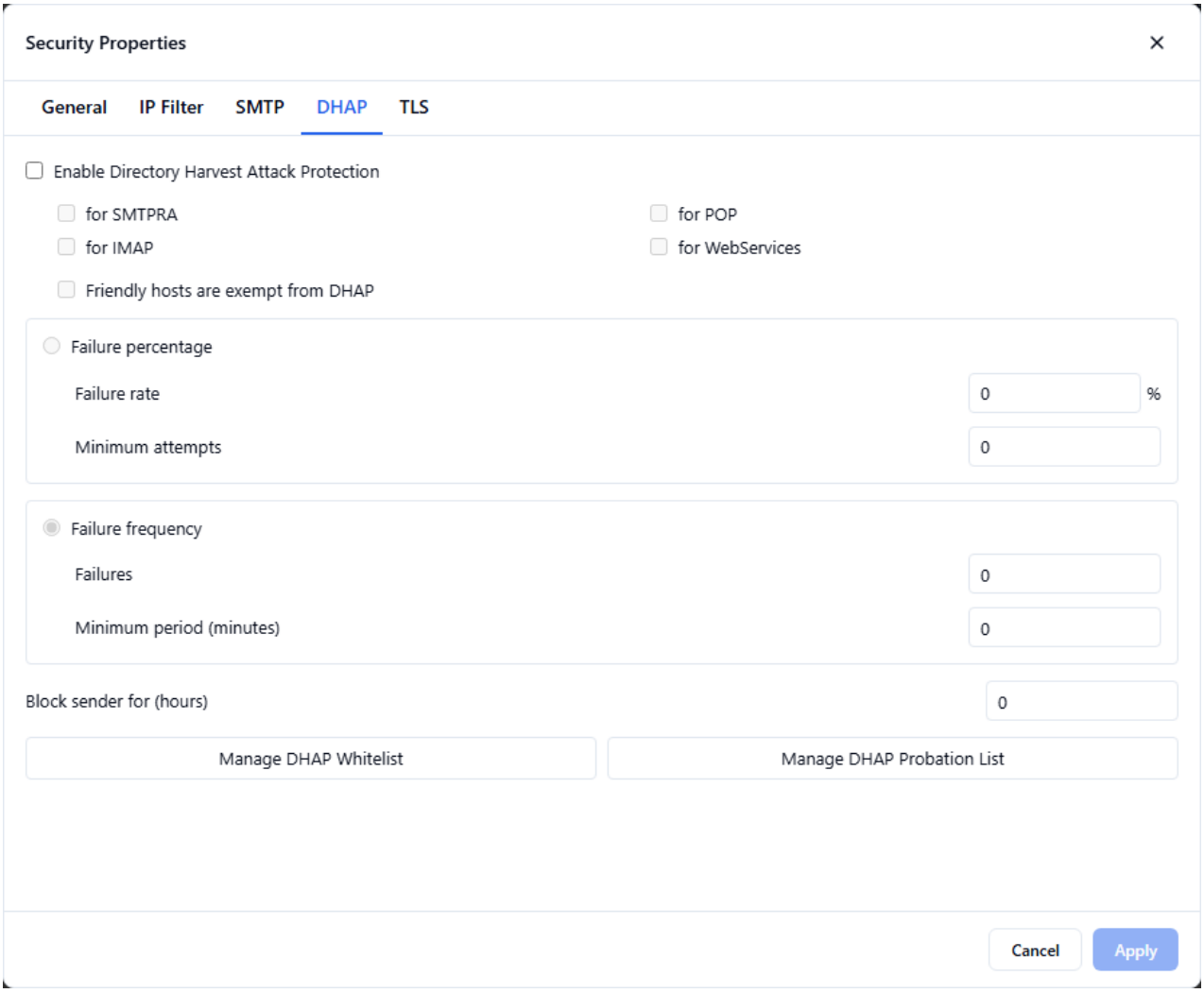

Figure 72 Percentage failure detection method

If you do not wish to use the default values you may now configure the failure rate that you deem a DHA and the minimum number of attempts that the failure rate is calculated over. You can also configure the block duration that a host deemed a harvester is blocked for.

The failure rate is the percentage of non-existent email addresses with respect to the total number of email addresses attempted by a connecting host.

For example, configure a 50% failure rate, a minimum sample of 100 attempts and a 24-hour block period to apply that policy. The illustration shows example fields, not these populated values.

Failure frequency detection method

To select this method of detection select the Failure Frequency option.

If you do not wish to use the default values you may configure the number failures that must occur within a configurable minimum period to determine a DHA. You can also configure the block duration that a host deemed a harvester is blocked for.

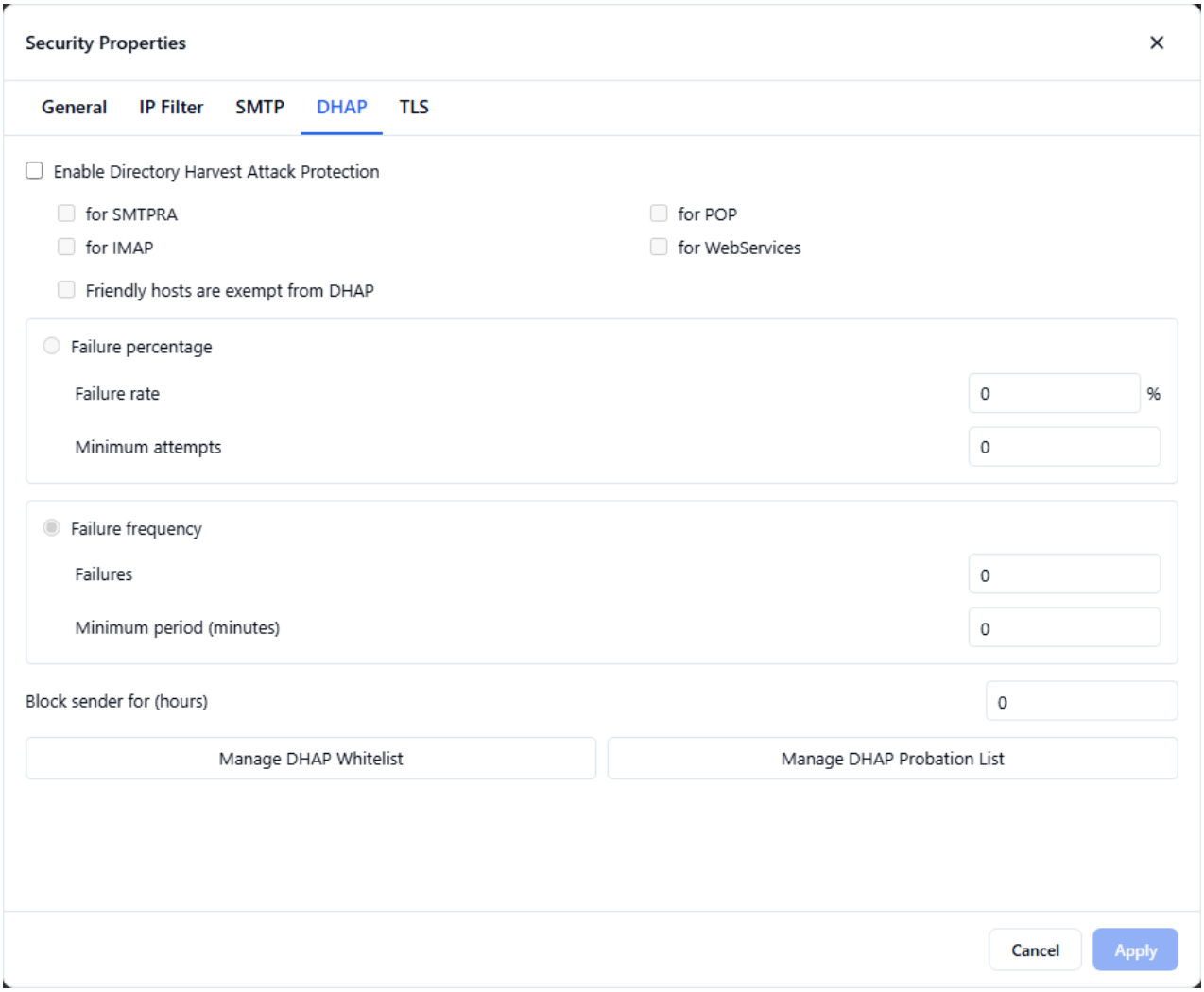

Figure 73 Failure frequency detection method

For example, configure 100 failures within two minutes and a 24-hour block period to apply that policy. The illustration shows example fields, not these populated values.

Managing DHAP

MailSite offers the ability to whitelist IP addresses so that they are not subject to DHAP checking, and to manage the probation list which contains those addresses being monitored by DHAP.

Manage DHAP whitelist

To manage the DHAP whitelist, click the Manage DHAP whitelist button on the DHAP tab of the Security Properties Page.

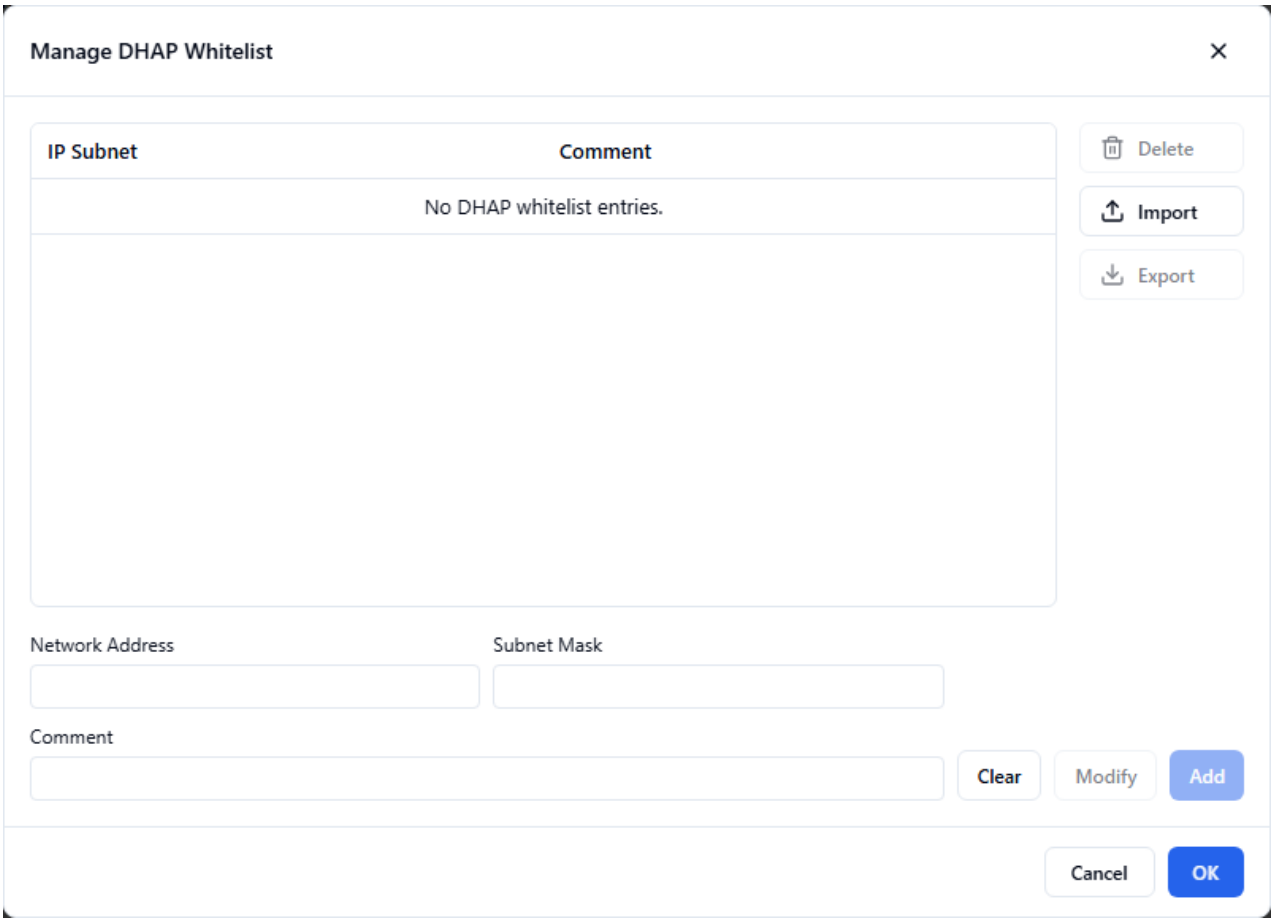

Figure 74 Manage DHAP whitelist

IP subnets can be added via this dialog, or from the Manage DHAP probation list dialog. It is also possible to import from and export to a text file and to modify or delete incorrect entries.

Manage DHAP probation list

The DHAP probation list contains IP addresses that DHAP is monitoring. To manage the DHAP probation list, click the

Manage DHAP probation list button on the DHAP tab of the Security Properties Page.

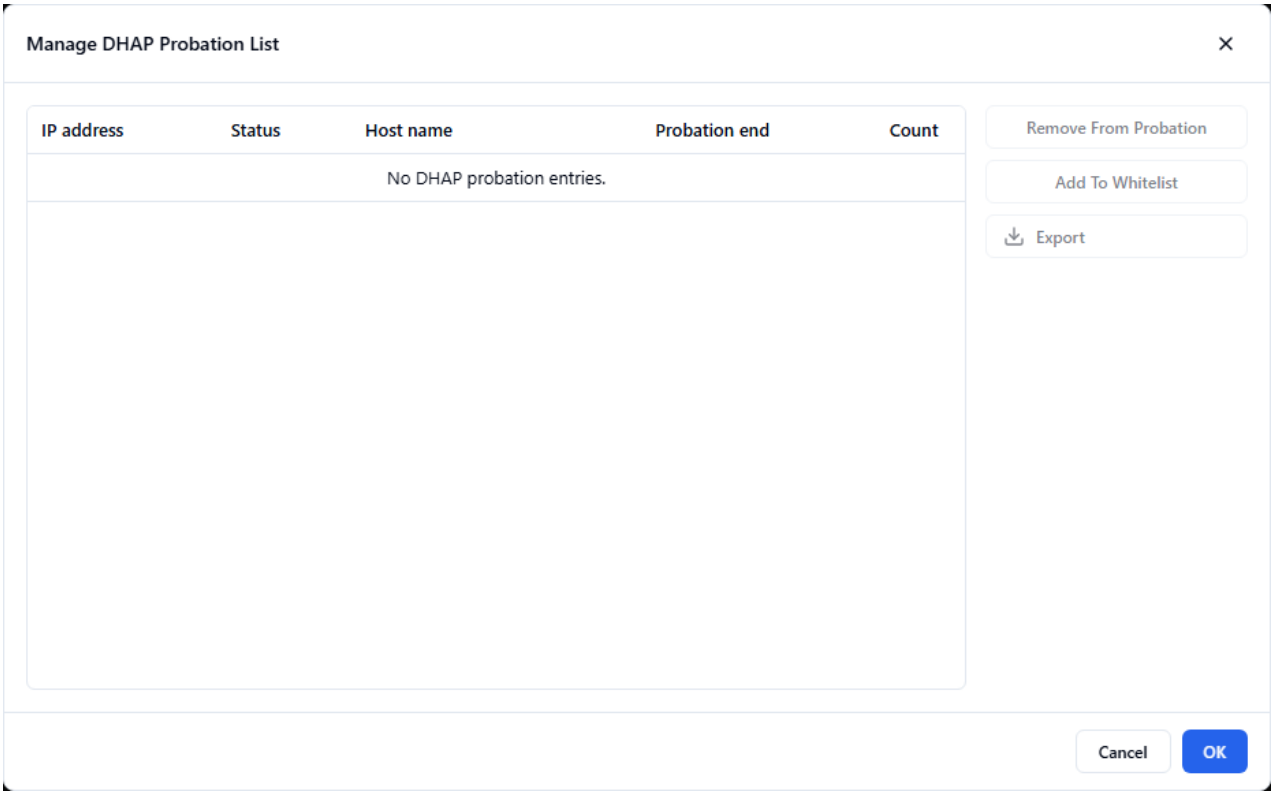

Figure 75 Manage DHAP probation list

IP subnets can be removed from probation, or if they are known to belong to legitimate users, added directly to the DHAP whitelist. The probation list can also be exported to a text file for review.

TLS Security Properties

TLS settings are invoked by clicking on the TLS settings tab in the Security Properties dialog.

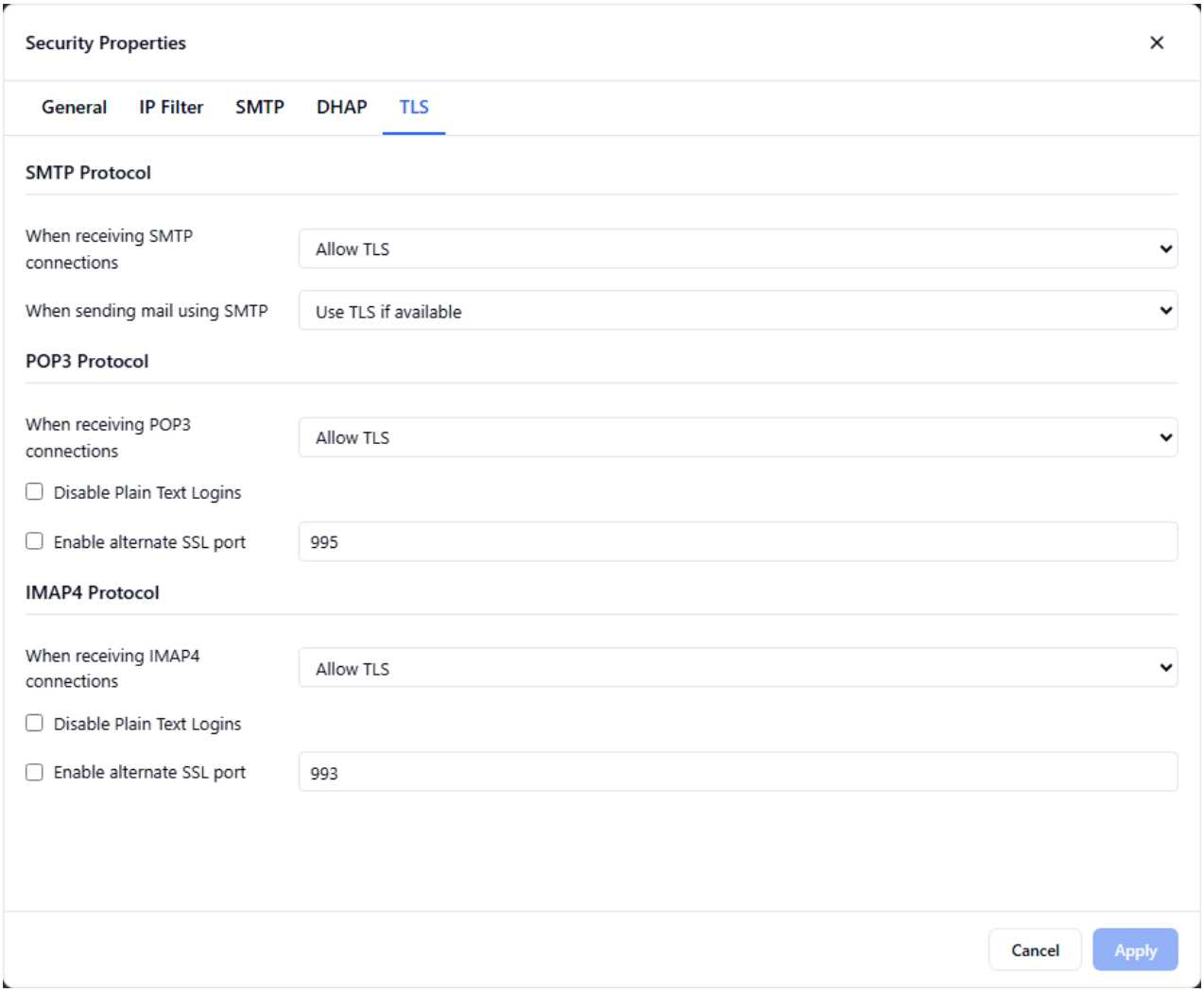

Figure 76 TLS Security Properties

The TLS tab configures SMTP receiving, SMTP sending, POP3 and IMAP4 separately. Choose the intended connection policy for each protocol and verify it with a real client. Certificate configuration is covered in TLS certificate management.

SMTP Protocol

When receiving SMTP connections, the settings available from the drop-down menu are:

Disable TLS - MailSite communicates in clear text mode and does not advertise TLS to the client.

Allow TLS (default) - MailSite negotiates with the mail client and optionally encrypts messages if the client has SSL/TLS configured.

Require TLS - MailSite forces messages to be encrypted.

You must also specify how mail will be sent (relayed) by SMTP. The settings available from the drop-down menu are:

Disable TLS - MailSite communicates in clear text mode even if the remote server advertises TLS.

Use TLS if available (default) - If the remote SMTP server advertises support for TLS it will attempt to use TLS but will send in clear text mode if unable to establish a secure connection.

Require TLS if supported - If the remote SMTP server advertises support for TLS but is unable to establish a secure connection then it is treated as a temporary failure and MailSite wil attempt to redeliver. If the remote SMTP server does not advertise support for TLS then MailSite will send in clear text mode.

Require TLS - MailSite will only send messages to remote SMTP servers that advertise support for TLS if it is able to establish a secure connection.

POP3 Protocol and IMAP4 Protocol

The POP3 and IMAP4 Protocol areas of the Security Properties window provide the same configuration setting choices. To limit redundancy, they are described together in this subsection.

When receiving POP3 connections or IMAP4 connections, the settings available from the drop-down menu are:

Disable TLS - MailSite communicates in clear text mode.

Allow TLS (default) - MailSite negotiates with the mail client and optionally encrypts messages if the client has SSL/TLS configured.

Require TLS - MailSite forces messages to be encrypted. Two checkboxes may also be set:

Disable Plain Text Logins - Restricts unencrypted password login. Configure TLS and confirm that the actual client negotiates an encrypted connection before supplying credentials.

Enable alternate SSL port - Enables the separately configured implicit TLS listener. Enter its port and configure the client to match. This label does not imply support for obsolete SSL 3.0.

Anti-Relay Wizard

To simplify the task of setting anti-relay policies, MailSite includes an Anti-Relay Wizard. This wizard leads you step-by-step through options that combat third-party relay. To start the wizard, double-click on the Anti-Relay Wizard icon in the MailSite Console.

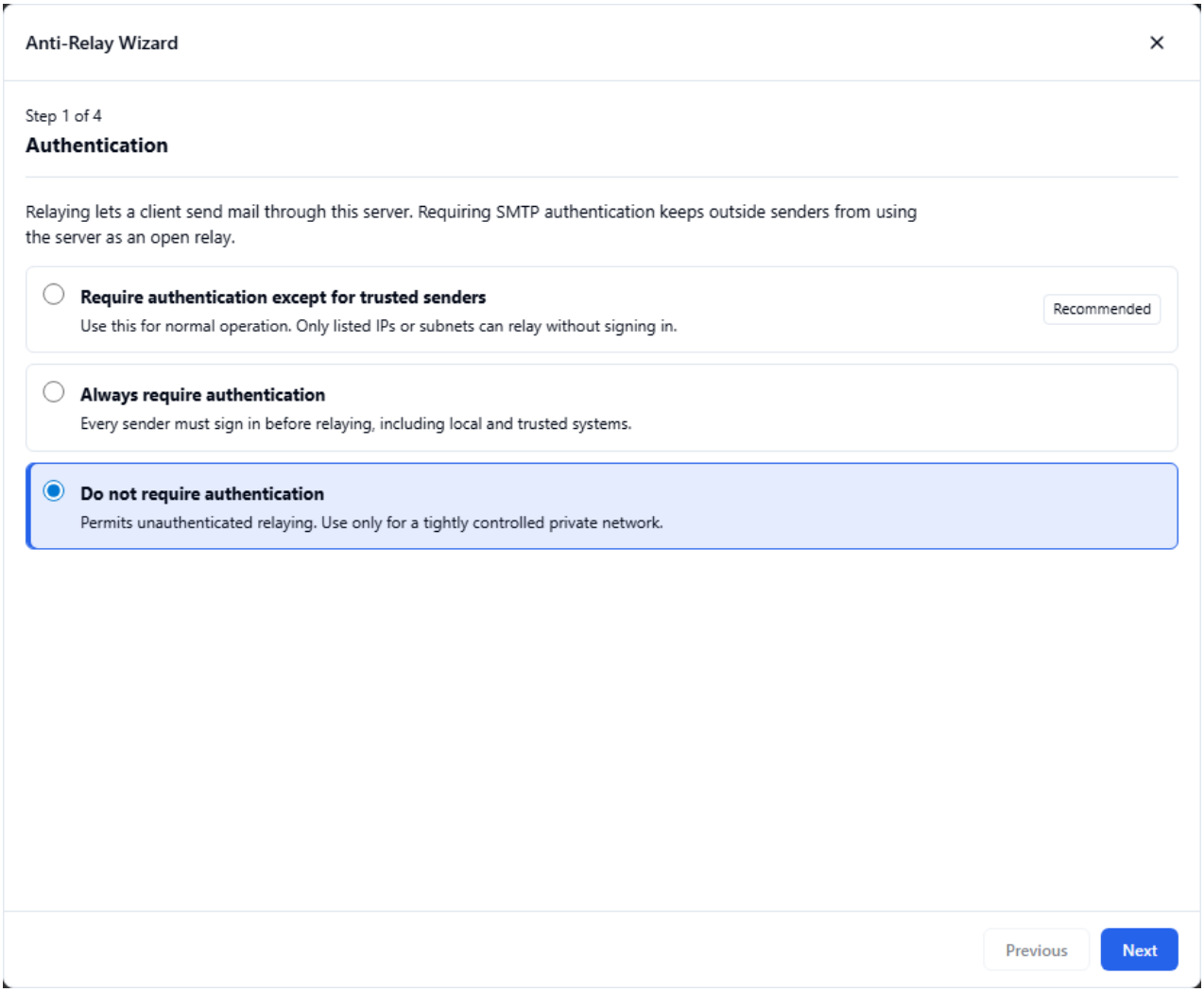

Figure 77 Anti-Relay Wizard

SMTP Security Wizard

To simplify the task of setting SMTP security policies, MailSite includes an SMTP Security Wizard. This wizard leads you step-by-step through options that combat the flow of junk mail (“spam”) to your site. Once these settings have been correctly configured the flow of spam throught the system should be reduced. It is still necessary to scan unexpected messages to determine the likelihood that they are spam. This is achieved through appropriate sieve filters acting on the spam score. Please refer to the section on Filtering.

To start the wizard, double-click on the SMTP Security Wizard icon in the MailSite Console.

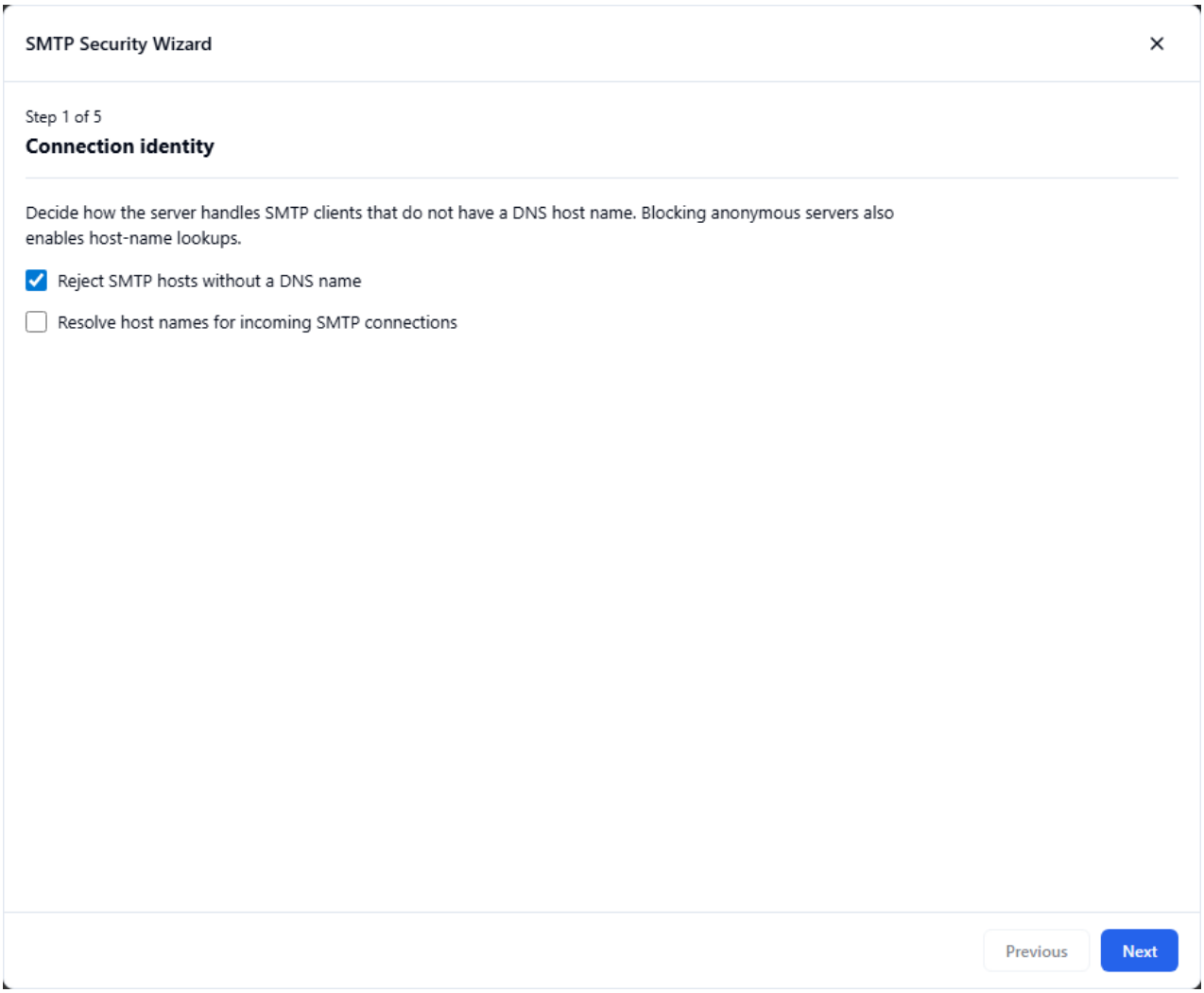

Figure 78 SMTP Security Wizard

Anti-DoS Wizard

To simplify the task of setting anti-denial of service (Dos) attack policies, MailSite includes an Anti-DoS Wizard. This wizard leads you step-by-step through options that combat potentially crippling denial-of-service attacks. To start the wizard, double-click on the Anti-DoS Wizard icon in the MailSite Console.

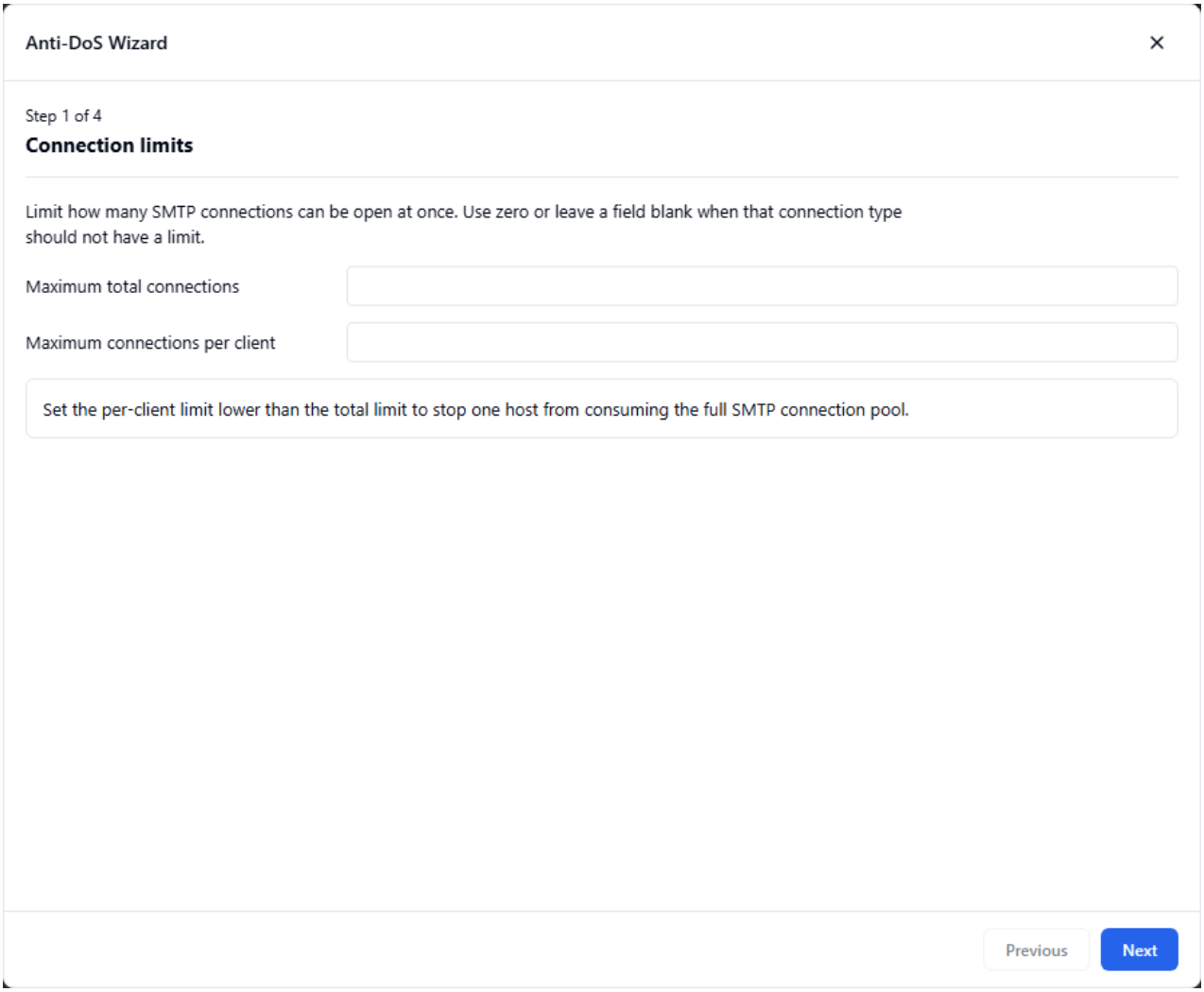

Figure 79 Anti-DoS Wizard

Filtering

Anti-Virus Filter

The current Anti-Virus Filter uses the MailSite 11 scanning configuration. Review scope, message-size exclusions, scanner-failure behavior and protected archives. Inspect scan counters and definition-update status. See Virus Scanning for the policy and validation workflow.

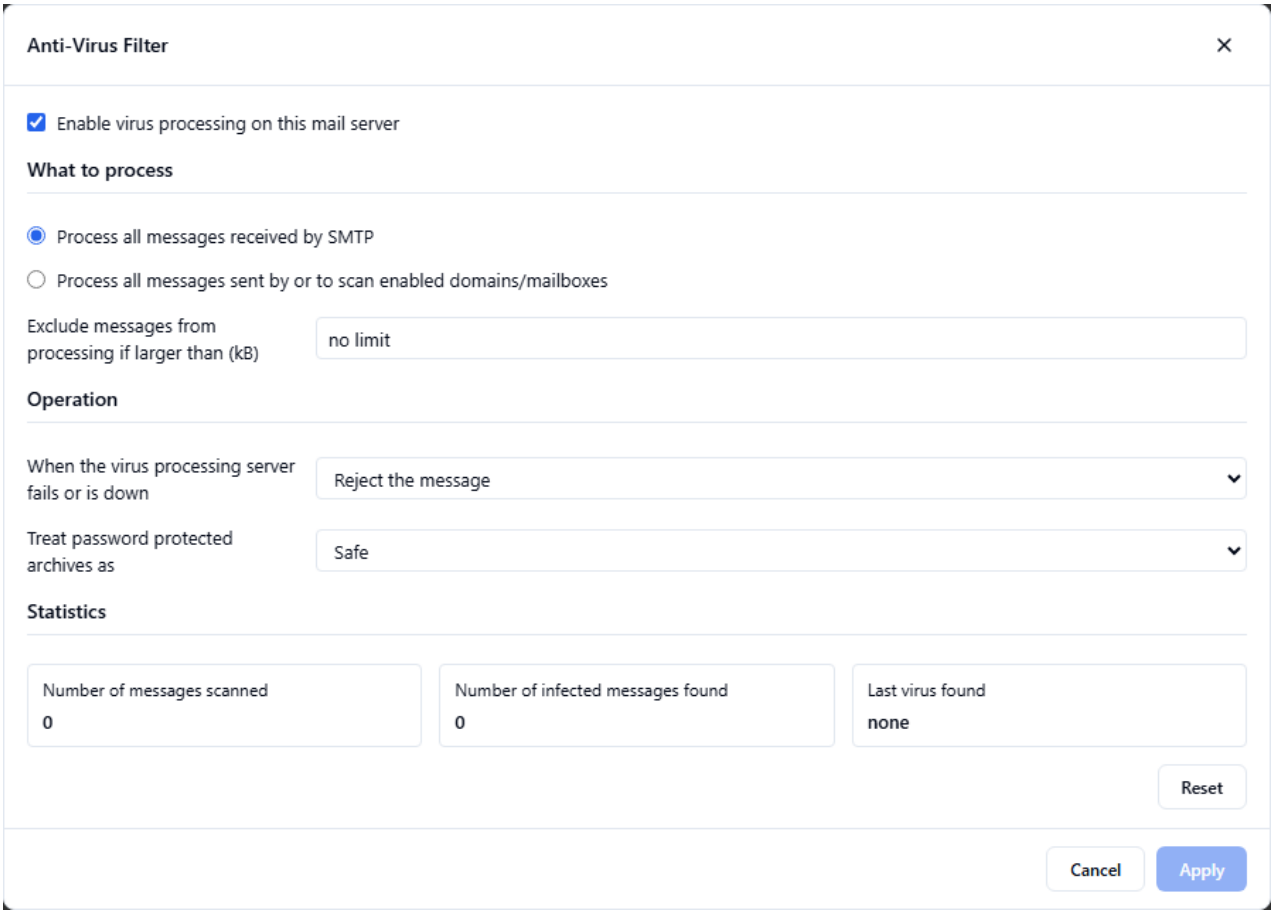

Figure 80 Anti-virus settings

Anti-Spam Filter

The Scanning tab controls scanning scope, size limits and exemptions. Review authenticated and friendly-host exemptions along with Junk Mail retention. Use the Spam Scanning chapter when validating scoring and message disposition.

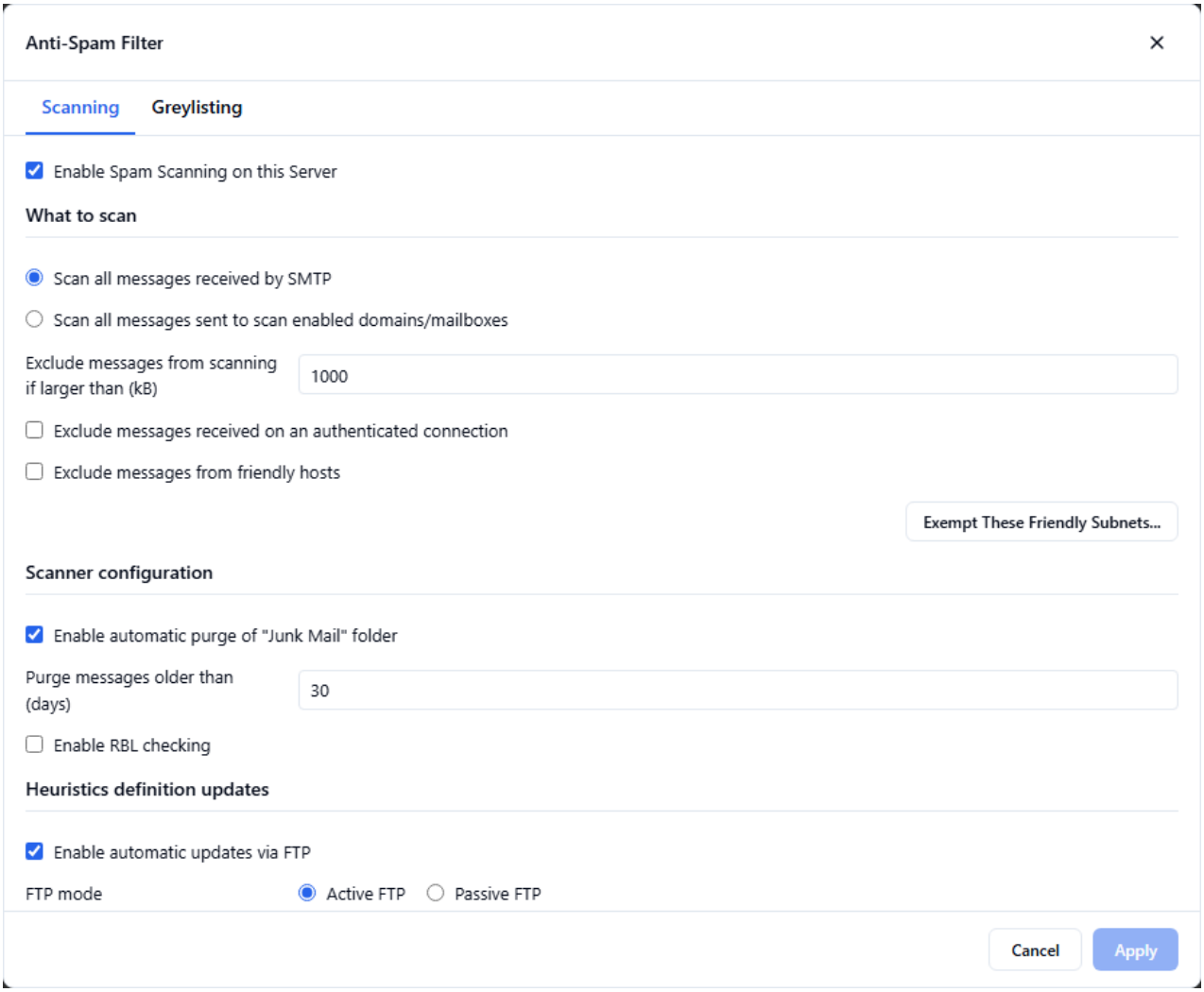

Figure 81 Anti-spam settings

Greylisting

The Greylisting tab controls delivery deferral and its exceptions. Verify retry behavior and trusted-system exemptions against your actual receiving traffic.

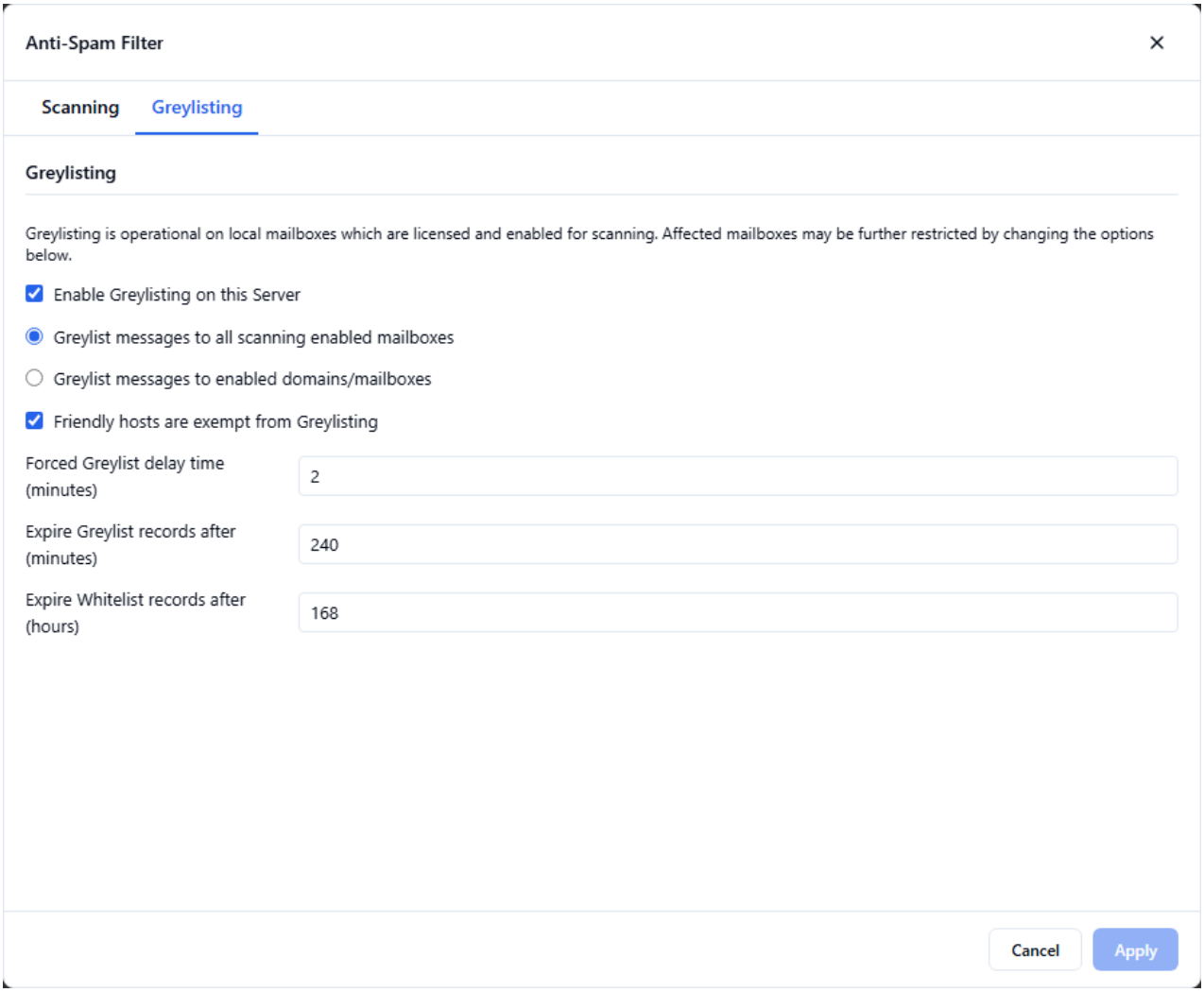

Figure 82 Greylisting settings

Sieve Filter Rules

Open Server, Filtering, Sieve Filter, or the corresponding domain or mailbox filtering control. Select the stage when more than one script is available. New and Modify edit a rule's name, description, enabled state and Sieve body; they do not open the old step-by-step criteria wizard.

Use the rule checkbox to enable it, and Move Up or Move Down to change evaluation order. Copy, Rename and Delete maintain the selected rule. Import and Export work with script files. Advanced opens the complete script for editing. Apply saves the parent dialog's changes.

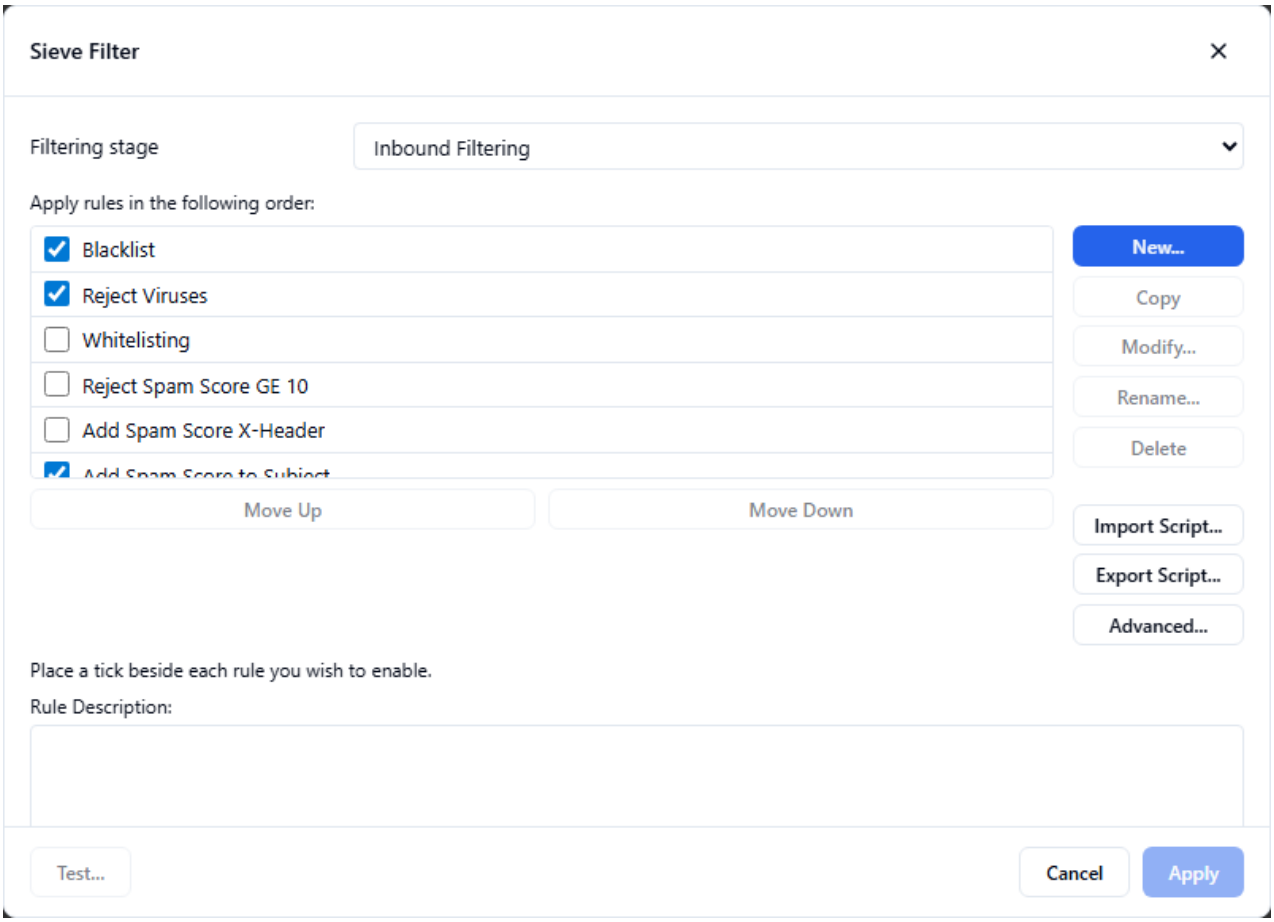

Figure 83 Current Sieve script editor

The action and Sieve syntax reference in the Mail Filters chapter describes message handling. Test policy through controlled mail flow before using it on production traffic. The Console's Test button is currently disabled.

Whitelist

This dialog controls the Whitelist. A whitelist contains all addresses, domains and so on that are known to be legitimate senders of mail. MailSite supports whitelists at server, domain and mailbox levels. Sieve scripts such as the Server Receive Script are then used to take the appropriate action, typically to allow messages to bypass further security checking such as the anti-spam filtering.

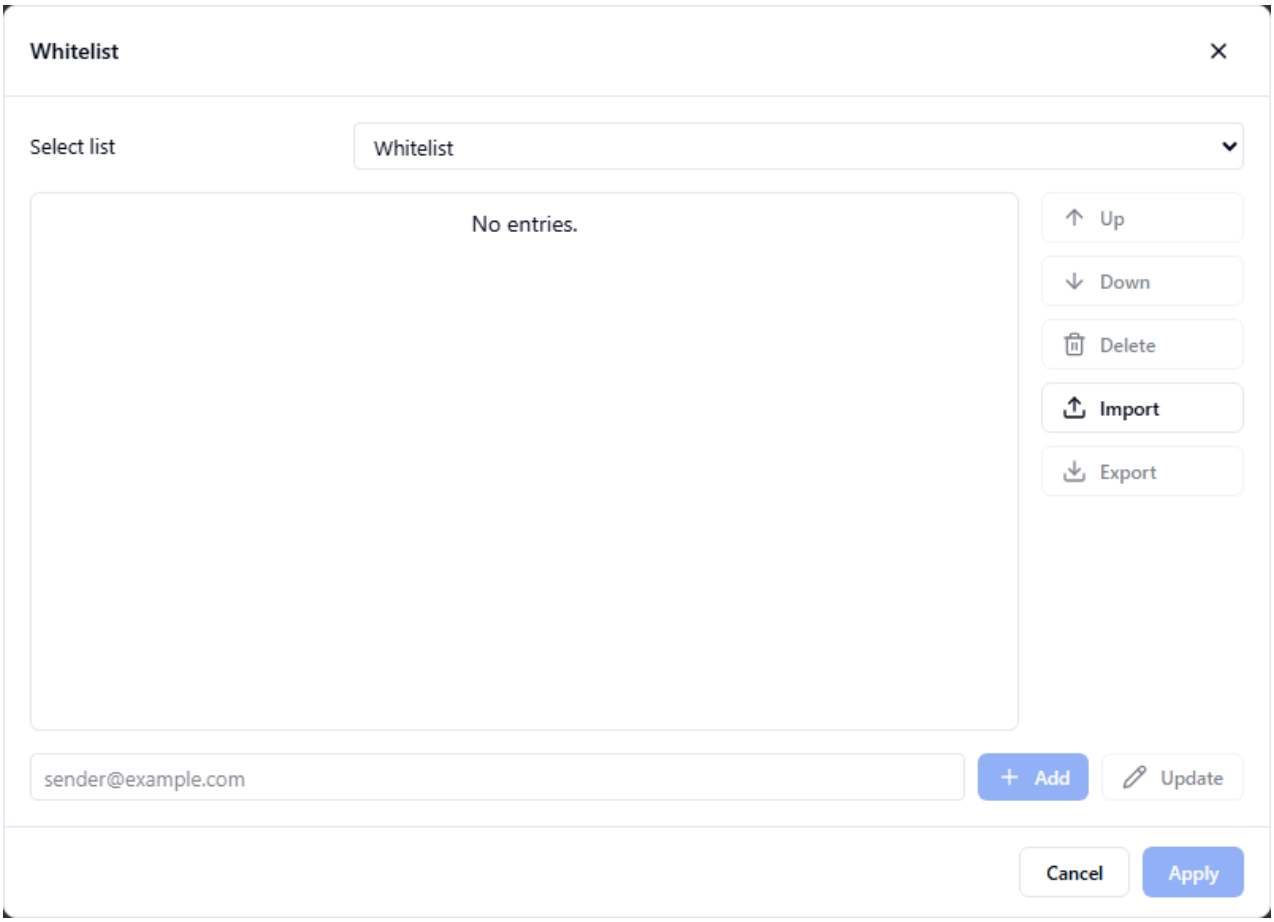

Figure 84 Whitelist

Large lists of addresses can be exported to a comma separated list using the “Export” button, modified in other programs and then imported through the “Import” button in this dialog. The dropdown list allows you to quickly change to the Blacklist dialog as these two lists are closely related.

Blacklist

This dialog controls the Blacklist. A blacklist contains all addresses, domains and so on that are known to be unwanted senders of mail. MailSite supports blacklists at server, domain and mailbox levels. Sieve scripts such as the Server Receive Script are then used to take the appropriate action, typically to reject the message.

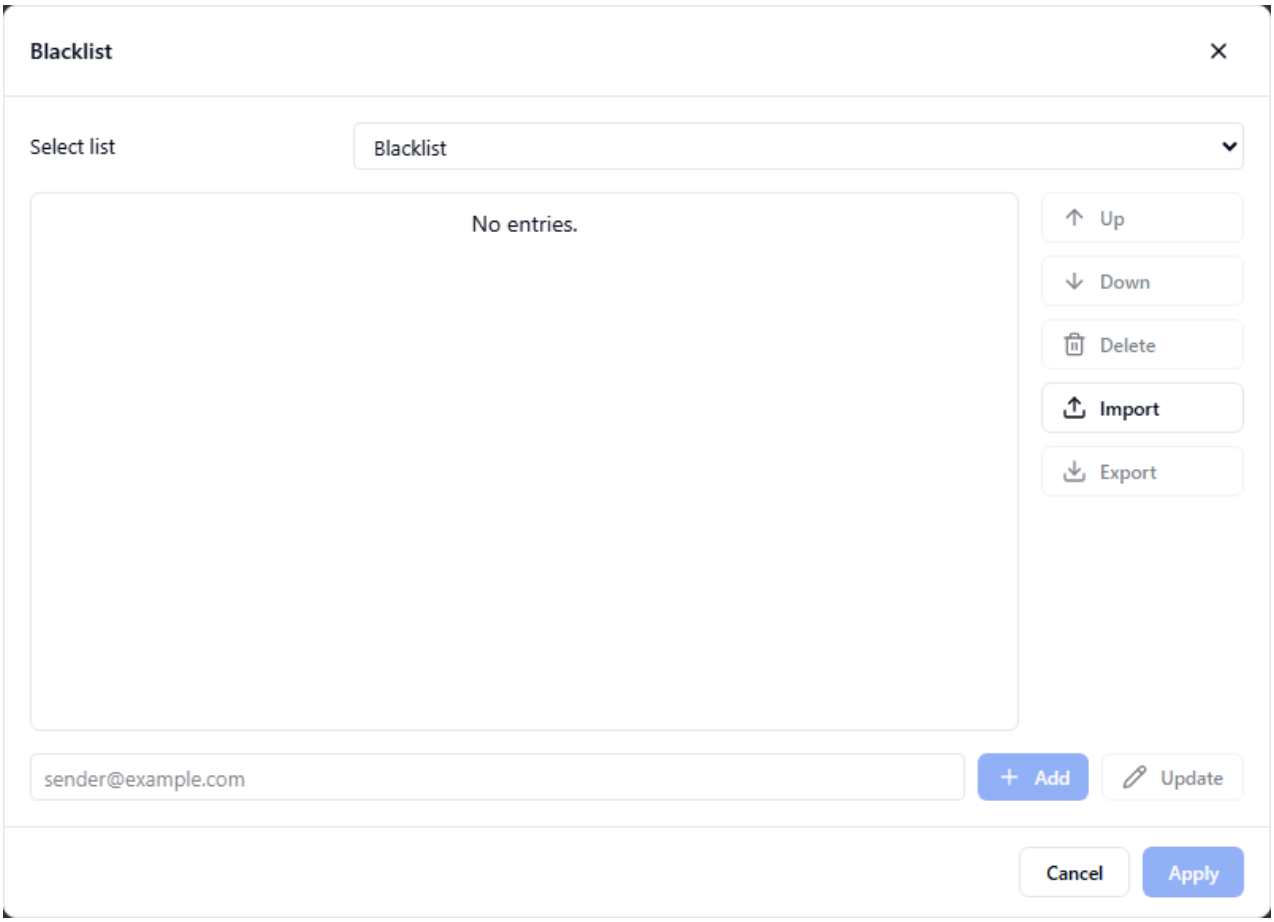

Figure 85 Blacklist

Large lists of addresses can be exported to a comma separated list using the “Export” button, modified in other programs and then imported through the “Import” button in this dialog. The dropdown list allows you to quickly change to the Whitelist dialog as these two lists are closely related.

Logs

MailSite logging options can be set using the items in the Logs folder.

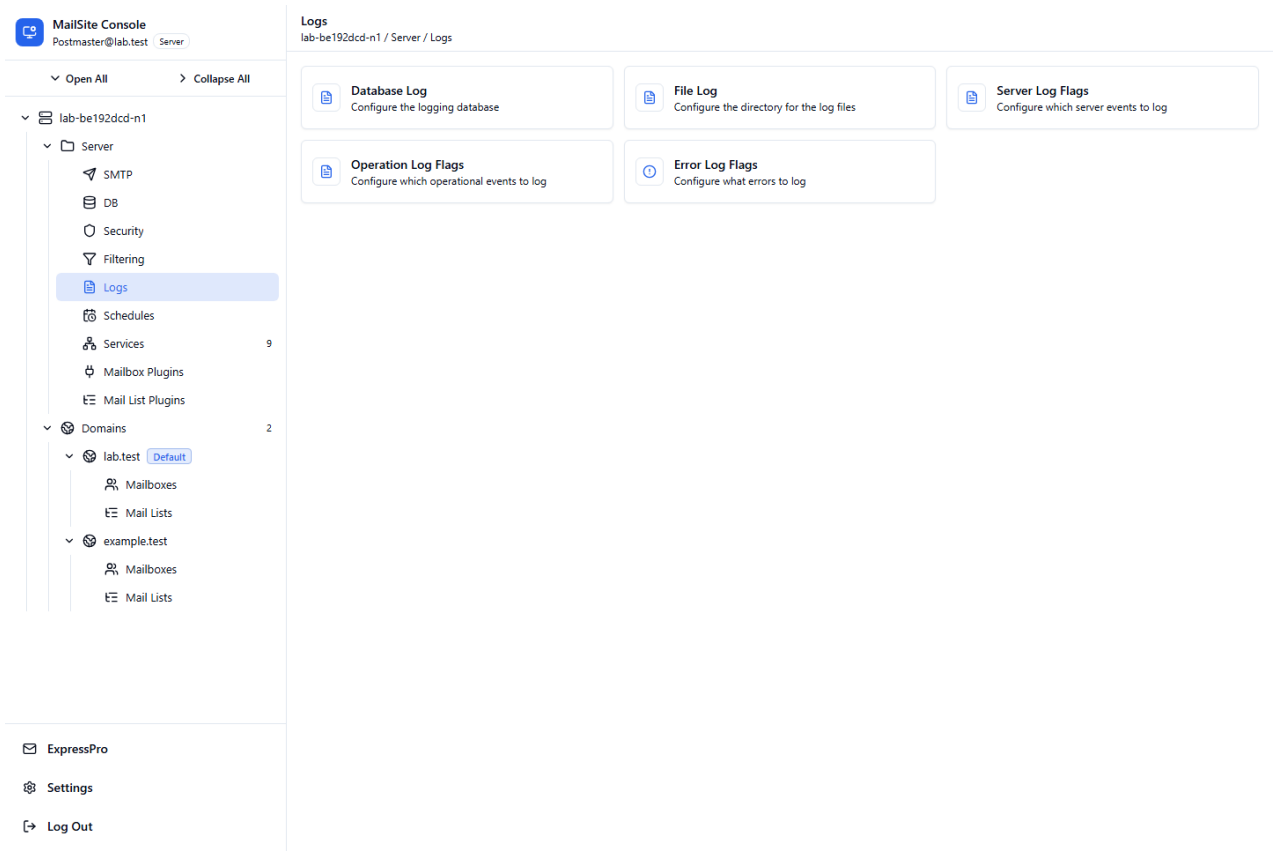

Figure 86 Logs

Use these controls to configure the supported logging categories for the selected services. Current Rust services write structured file and console logs. The retained Database Log controls do not activate the legacy direct ODBC log destination; see Appendix E.

Open File Log to review the directory, or the relevant log-flags control to review categories. Inspect the service log output after a change. Database Log is retained for configuration compatibility only.

Database log compatibility

These retained fields describe the old direct ODBC log destination. Current Rust services write through the shared structured logging runtime and do not execute the old SQL log template. Use the Console log viewer and current service log files; migrate external database reporting through a verified collector if required. See Appendix E.

Advanced Database Log Configuration

The retained Database Log fields do not activate a current ODBC logging destination. The old advanced service-name and parameter-length editor is absent. See Appendix E for the current logging workflow and migration of database reports.

File Log

Set MailLogDir to the service-writable directory for current log files. The Rust services use a shared structured logger with service-specific files and runtime logging flags. Inspect the files actually produced by the installed service and use Console, Logs to read them; the old SRV/ERR naming table is not a v11 file inventory.

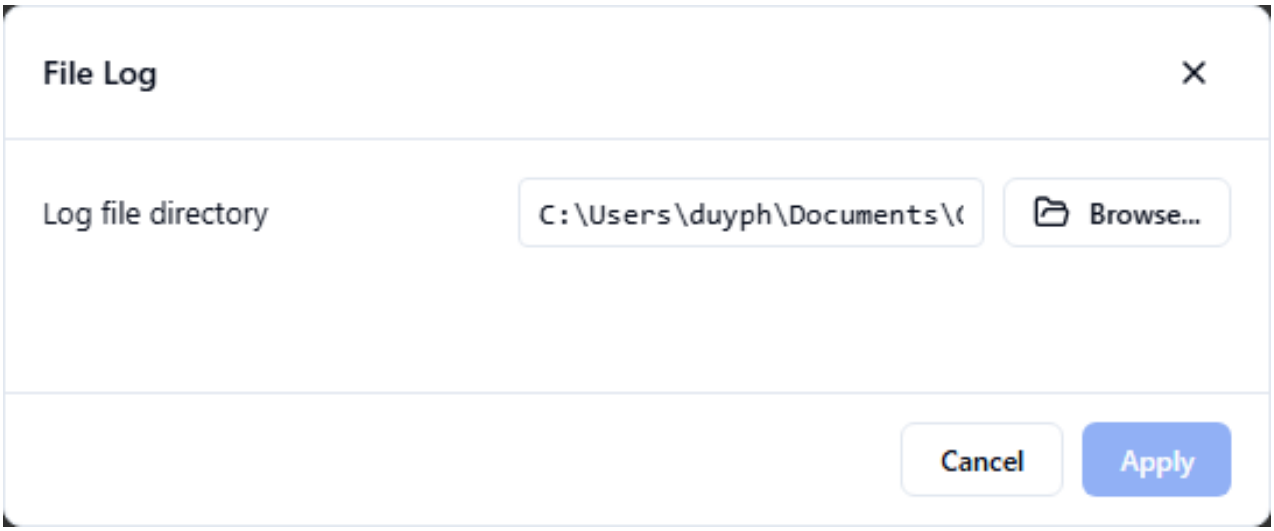

Figure 87 Log directory configuration

The service can begin with a fallback log directory before the shared authority is available, then switch to the configured directory. Include startup logs when diagnosing a service that failed before that switch. Keep log files access-controlled and configure retention appropriate to their contents.

Error Log Flags

Click on the Error Log Flags icon to set options for logging of errors:

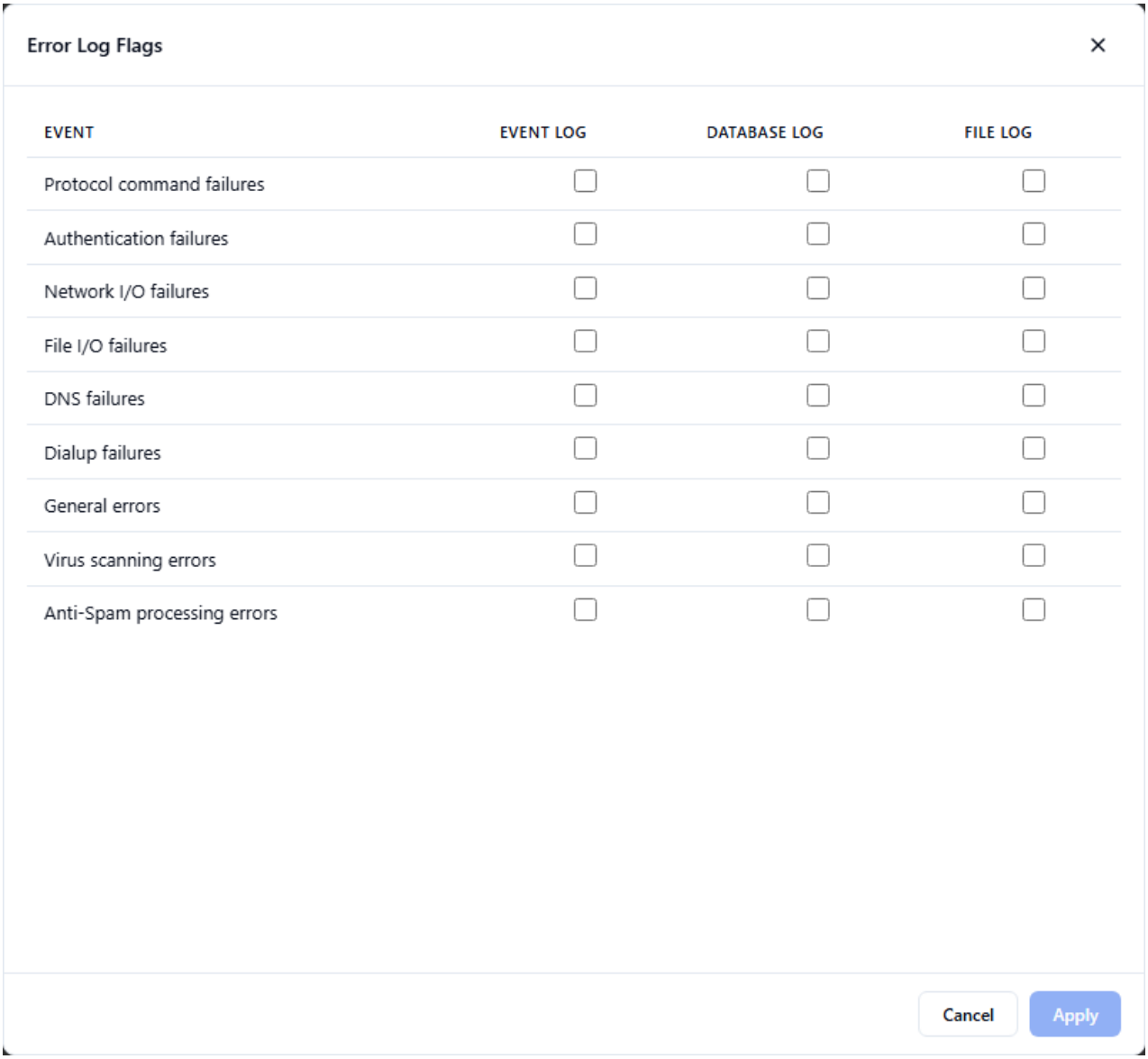

Figure 88 Error Log Flags

Protocol Command Failures

Select this option to record SMTP, POP3, IMAP4, LDAP3A, MAILMA and HTTPMA protocol failures. We recommend you enable this option.

Authentication Failures

Select this option to record SMTP, POP3, IMAP4, LDAP3A and MAILMA user and password authentication failures. We strongly recommend that you enable this option.

Network I/O failures

Select this option to record network communication failures. We recommend you enable this option.

File I/O failures

Select this option to record mail file access failures. We recommend you enable this option.

DNS failures

Select this option to record DNS resolution failures. We recommend you enable this option.

Dialup Failures

Retained legacy category. MailSite 11 does not establish dial-up connections.

General Errors

Select this option to log general MailSite errors. We recommend that you enable this option.

Virus Scanning Errors

Select this option to log errors related to virus scanning or virus definition updates. We recommend that you enable this option.

Operation Log Flags

Click on the Operation Log Flags icon to set options for logging routine operations:

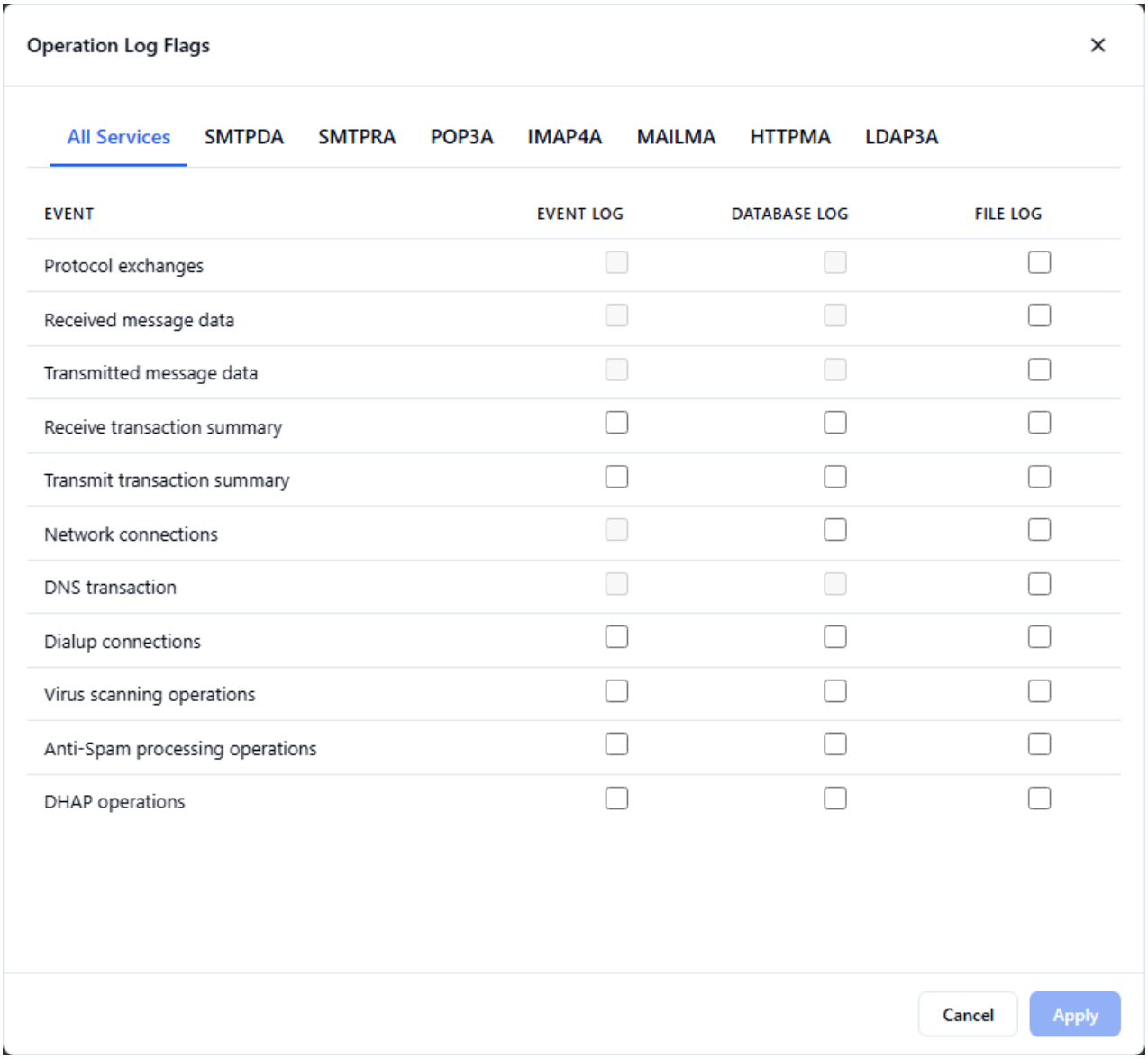

Figure 89 Operation Log Flags

Protocol Exchanges

Select this option to record all SMTP, POP3, IMAP4, HTTPMA and MAILMA protocol exchanges that MailSite makes. This option produces a large volume of information. This option should be used to debug problems and has an impact on performance.

Received Message Data

Select this option to record all incoming SMTP data. This option produces a huge volume of information. This logging will take a large amount of system memory and a large amount of disk space.

This option should only be enabled for specific problem resolution purposes. On no account should it be turned on in everyday use.

Transmitted Message Data

Select this option to record all outgoing SMTP data. This option produces a huge volume of information. This logging will take a large amount of system memory and a large amount of disk space. This option should only be enabled for specific problem resolution purposes. On no account should it be turned on in everyday use.

Receive transaction summary

Select this option to record header information for incoming SMTP messages. This option has an impact on performance.

Transmit transaction summary

Select this option to record header information for all outgoing messages. This option has an impact on performance.

Network connections

Select this option to record all network connections made by MailSite. This option produces a large volume of information. This option should be used to debug problems and has a significant impact on performance.

DNS Transactions

Select this option to record all DNS queries by MailSite. This option produces a large volume of information. This option should be used to debug problems with DNS name resolution and has an impact on performance.

Dialup Connections

Select this option to record when MailSite makes and breaks the dialup connection.

Virus Scanning Operations

Select this option to record successful virus scans of incoming mail.

Anti-Spam Processing

Select this option to record successful spam scans of mail including the score attributed to the message. Greylisting operations will also be recorded if greylisting is enabled.

DHAP Processing

Select this option to record DHAP operations.

Server Log Flags

Click on the Server Log Flags icon to set options for logging operations related to MailSite services:

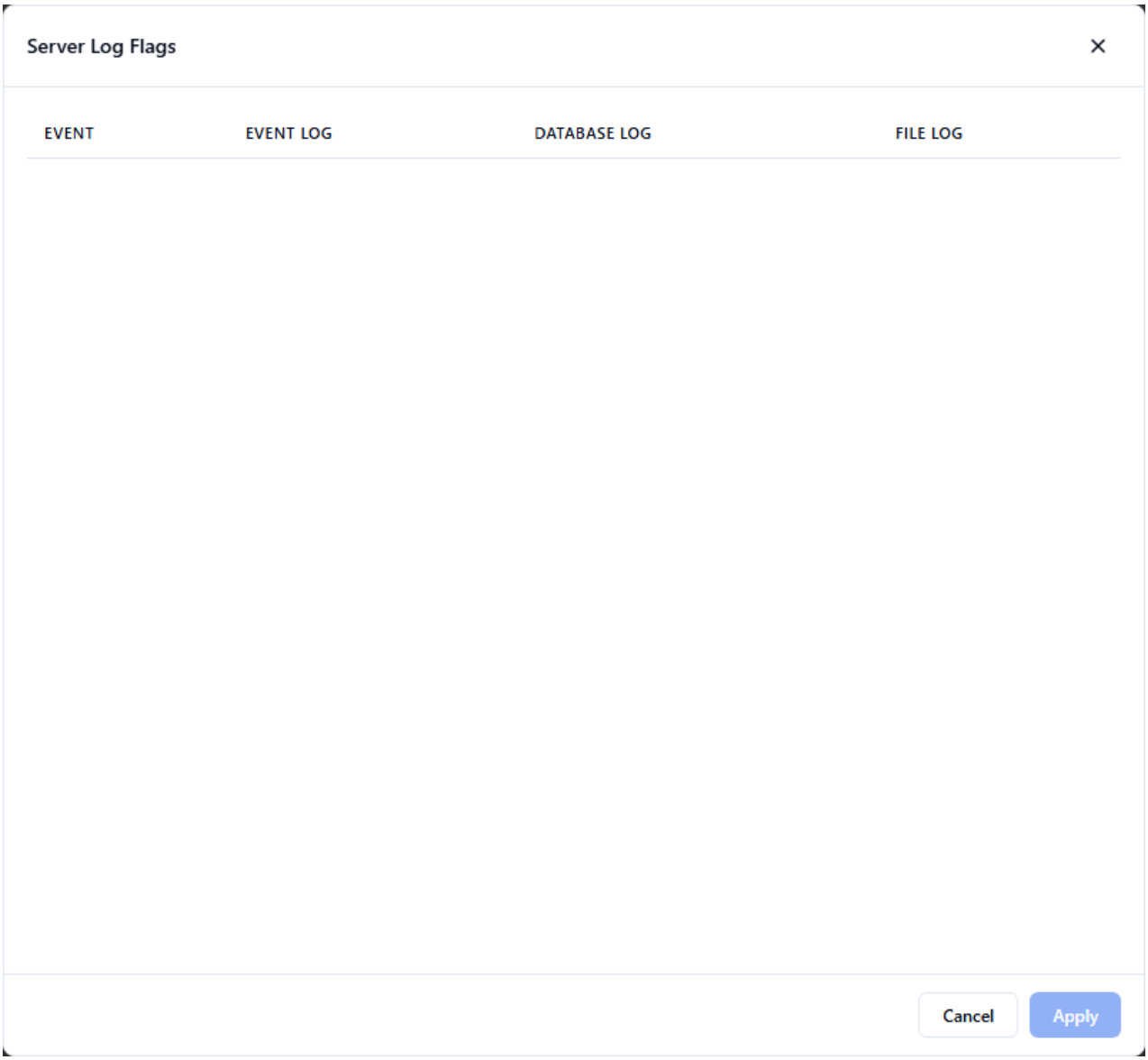

Figure 90 Server Log Flags

Service Start and Stop

Select this option to record when the mail services are started and stopped. We recommend you select this option.

Retry Domain(s)

Select this option to make a record when MailSite attempts to re-send any outgoing mail. We recommend you select this option.

Change Configuration

Select this option to record when changes are made to MailSite configuration. We recommend you select this option.

Schedules

Use this folder for elapsed delivery retries and retained legacy scheduling settings.

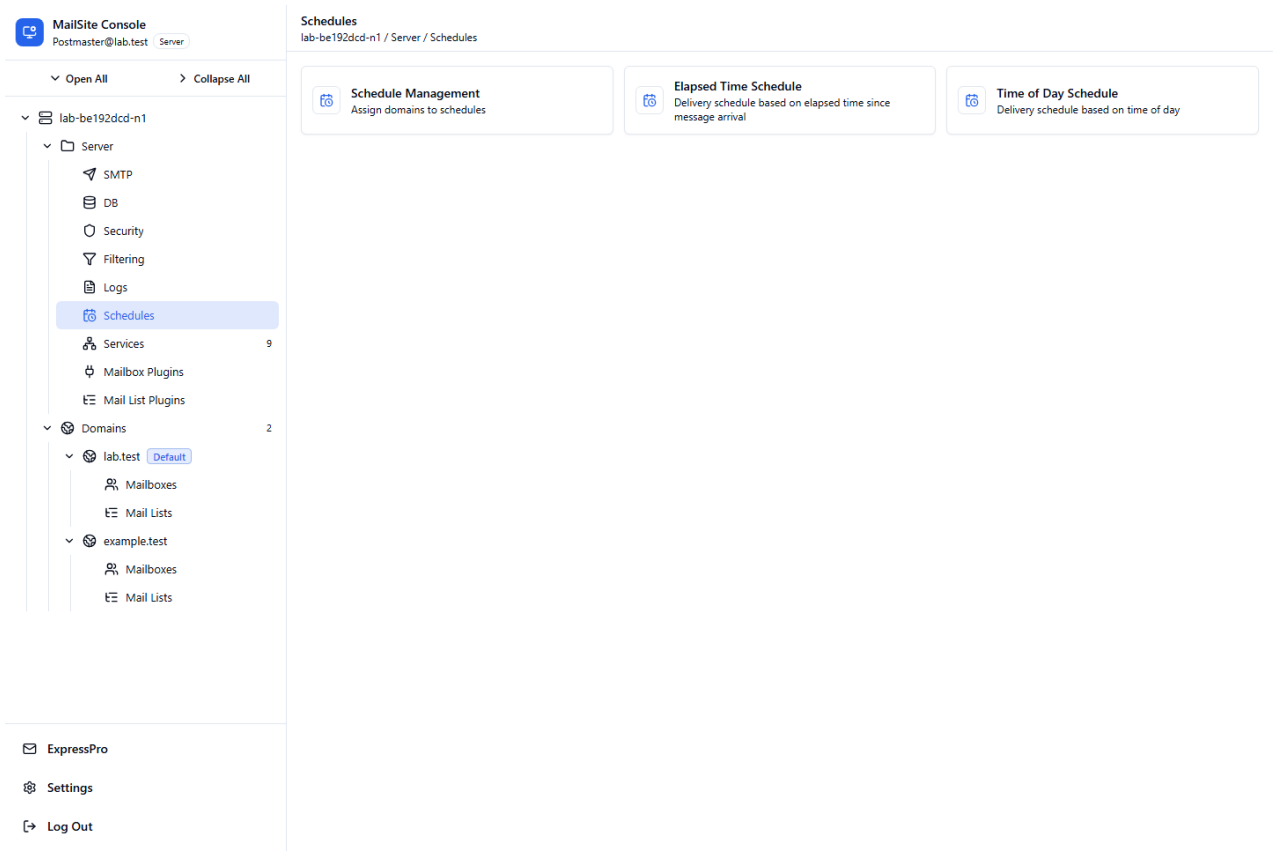

Figure 91 Schedules

The current delivery queue supports elapsed retry handling. The two-method selector below retains the legacy configuration vocabulary; time-of-day/dial-up dispatch is not implemented in v11.

Elapsed Time is operational; Time of Day is retained configuration.

Schedule Management

Schedule Management retains domain schedule masks and provides Reattempt Delivery Now. Current delivery uses elapsed retries; a saved time-of-day selection does not enable timed dispatch.

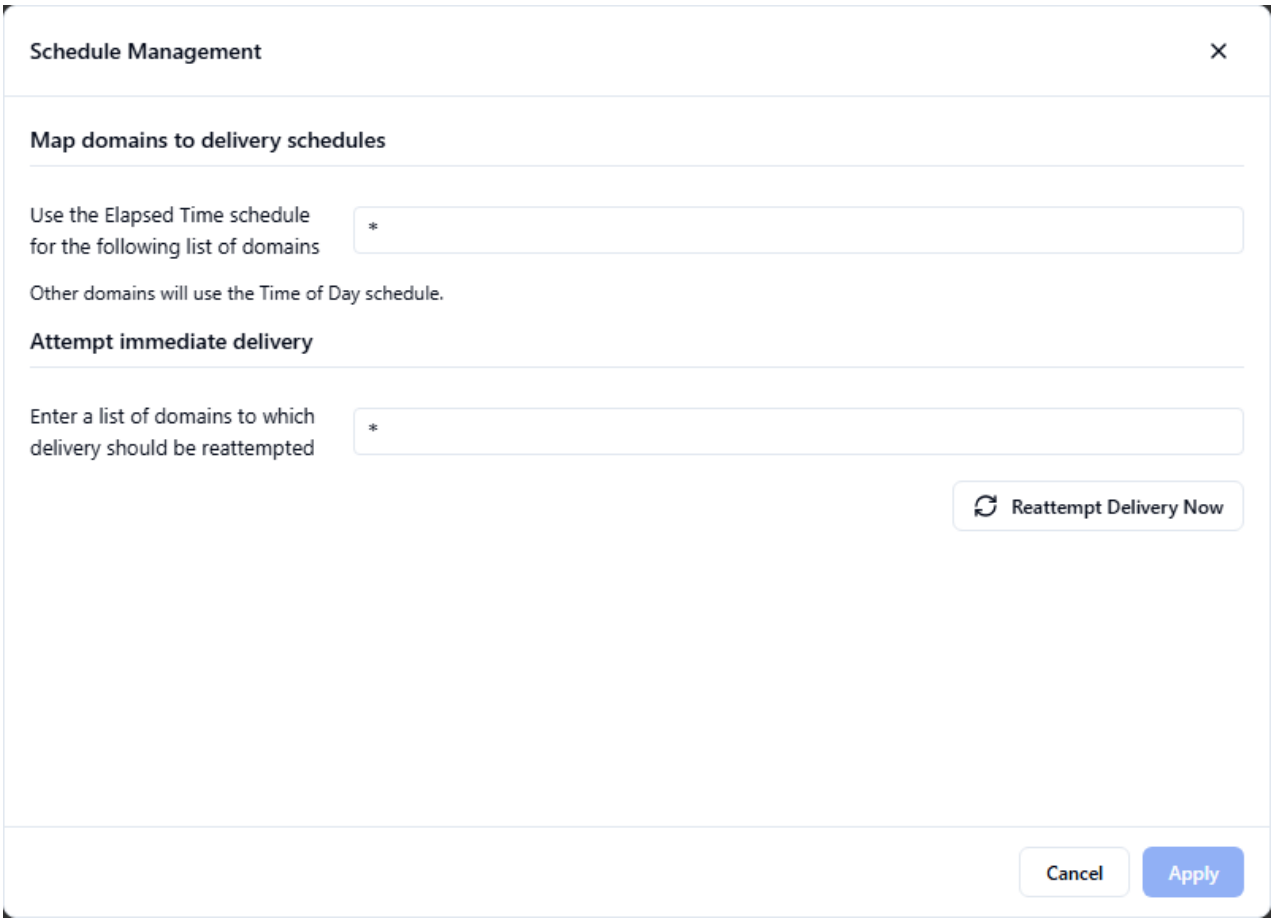

Figure 92 Schedule Management

Map domains to delivery schedules

Enter a list of domain names, separated by commas. The list is processed from left to right. You may specify * as part of a domain name, representing a wildcard. You can also have an exclamation mark ! in front of a domain name, indicating that matching domains don't belong in the list.

This mask belongs to the retained per-domain schedule selection. Current SMTPDA uses ordinary queued delivery and elapsed retry handling; it does not dispatch through the old time-of-day/dial-up subsystem. Do not use this field to promise delivery at a particular time.

Legacy migration example: a former installation might have separated intranet domains from domains reached through an intermittent connection.

Its saved mask may still be visible after import.

For example, this retained mask distinguishes domains using first-match order:

!italy.mycompany.com,*mycompany.com,!*

In the previous implementation this mask selected a time-of-day schedule for some destinations. In v11 it does not delay delivery until a scheduled connection window. Arrange connectivity outside MailSite.

Schedule selection is separate from routing. Use DNS and Routes to select the destination host; verify elapsed retries through the current queue controls.

Attempt immediate delivery

You can enter a list of domain masks (domain names, possibly containing wildcards, separated by commas) in this field. When you click the button labeled Reattempt delivery to these domains now, any messages for foreign domains which match the domain mask list will be scheduled for an immediate delivery attempt.

By default, the field contains a single asterisk. If you click the button, all messages for foreign domains will be scheduled for immediate retry.

Once you have clicked the button, the field is cleared.

Elapsed Time Schedule

The elapsed time delivery schedule can be configured through this dialog:

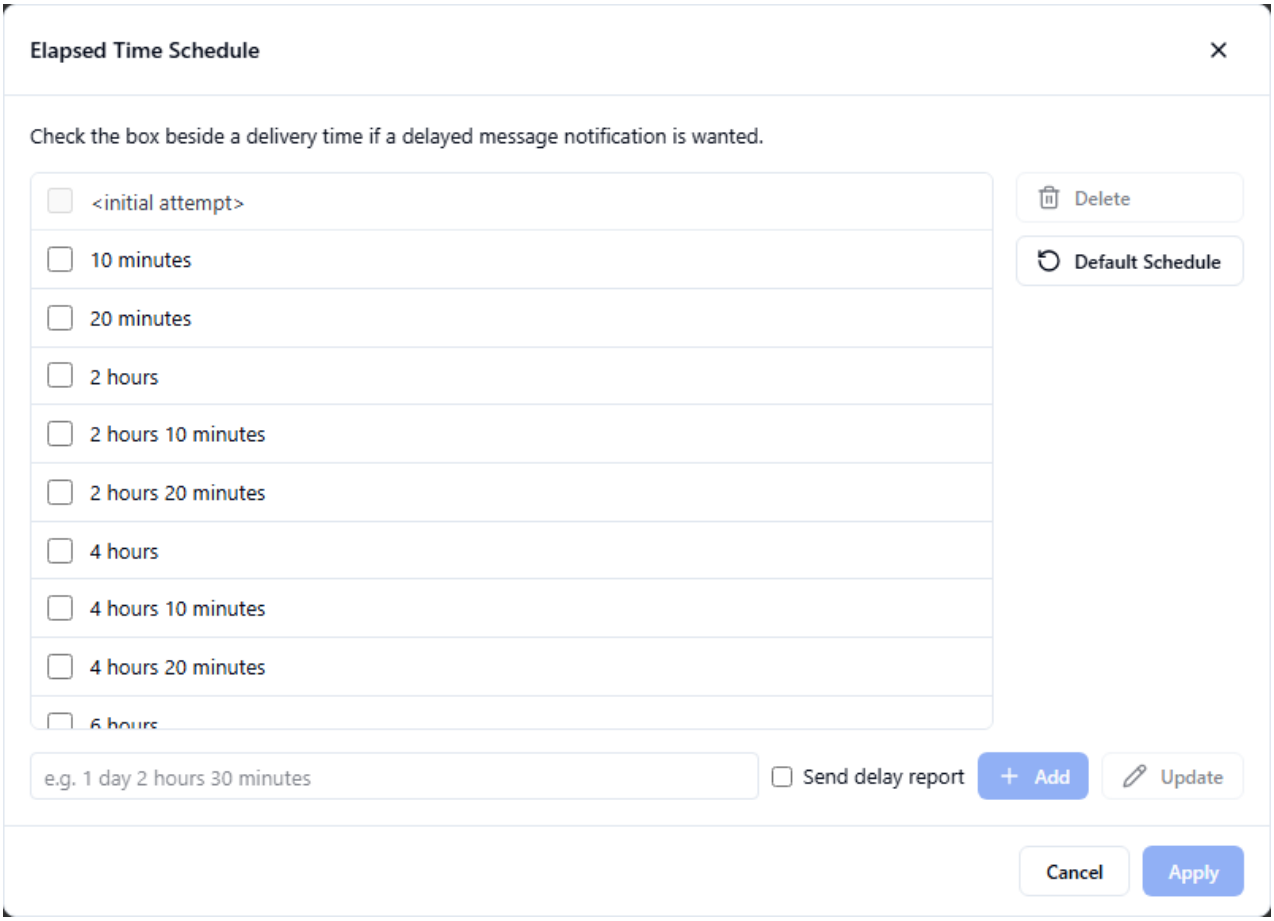

Figure 93 Elapsed Time Schedule

The elapsed time schedule is a list of times (measured in minutes from the time the first attempt is made) at which MailSite will attempt to send remote messages. By default, the pattern begins: 10, 10, 100, 10, 10, 100. This means that if the first attempt fails, MailSite will wait for ten minutes before the second attempt, and a further ten minutes before the third attempt. It will then wait 100 minutes before the fourth attempt (which will therefore be made two hours after the first attempt), and so on.

At certain points in this delivery schedule, MailSite will return a message delayed warning to the originators of the messages for the domain in question. The Elapsed Time Schedule contains information about when such warning messages will be generated.

If delivery to a domain has been attempted without success so often that the end of the delivery schedule is reached, then messages for that domain are treated as undeliverable.

To add a delivery attempt to the Elapsed Time Delivery schedule, enter a time (in the form of a number followed by d, h or m for days, hours or minutes) and click the Add button.

To request a warning message to be generated if a particular delivery attempt fails, check the checkbox beside the delivery attempt.

To delete a delivery attempt from the schedule, select it and click the Delete button.

To revert to the default elapsed time delivery schedule, click the Default schedule button.

Time-of-Day Schedule and Dialup Configuration

These retained controls describe the old Windows RAS subsystem. Current SMTPDA does not establish dial-up connections, run connection-trigger commands or dispatch through the old time-of-day schedule. Saving those fields does not enable scheduled dial-up delivery.

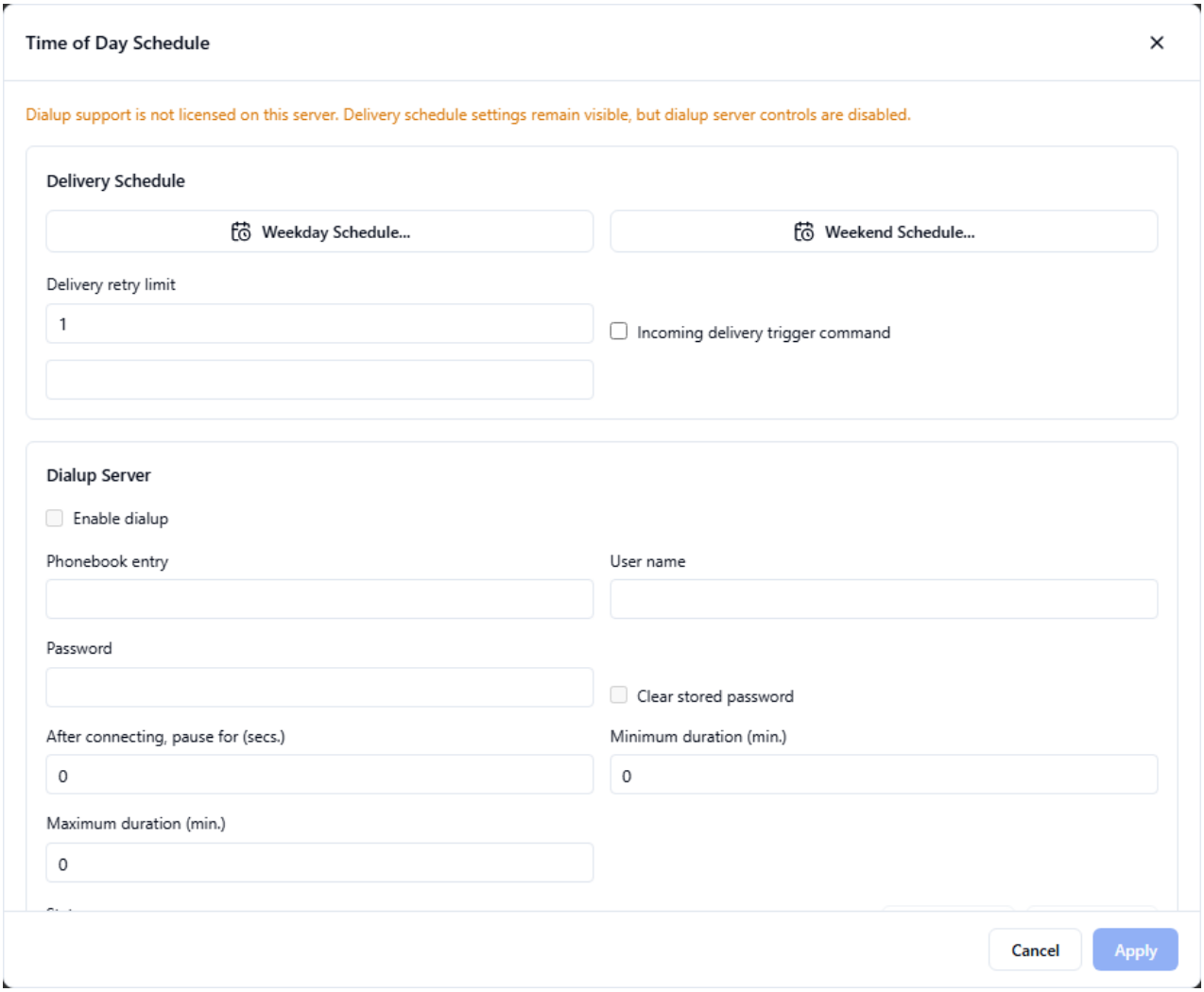

Figure 94 Retained time-of-day configuration

Use ordinary network connectivity and the current elapsed retry/queue controls. Preserve the original guide and configuration if migrating an installation that depended on RAS; arrange connectivity outside MailSite before moving mail delivery to v11.

Weekday and Weekend schedules

The editor preserves weekday/weekend values for migration. They are not an active v11 dispatch schedule. Use the current queue retry controls and verify delivery through the recorded recipient outcomes.

Services

Open Server, Services to inspect installed services, state and logs. Use the available row actions for service operations; open a service's properties for its supported port controls. Privileges and desktop/web host capabilities can affect available actions.

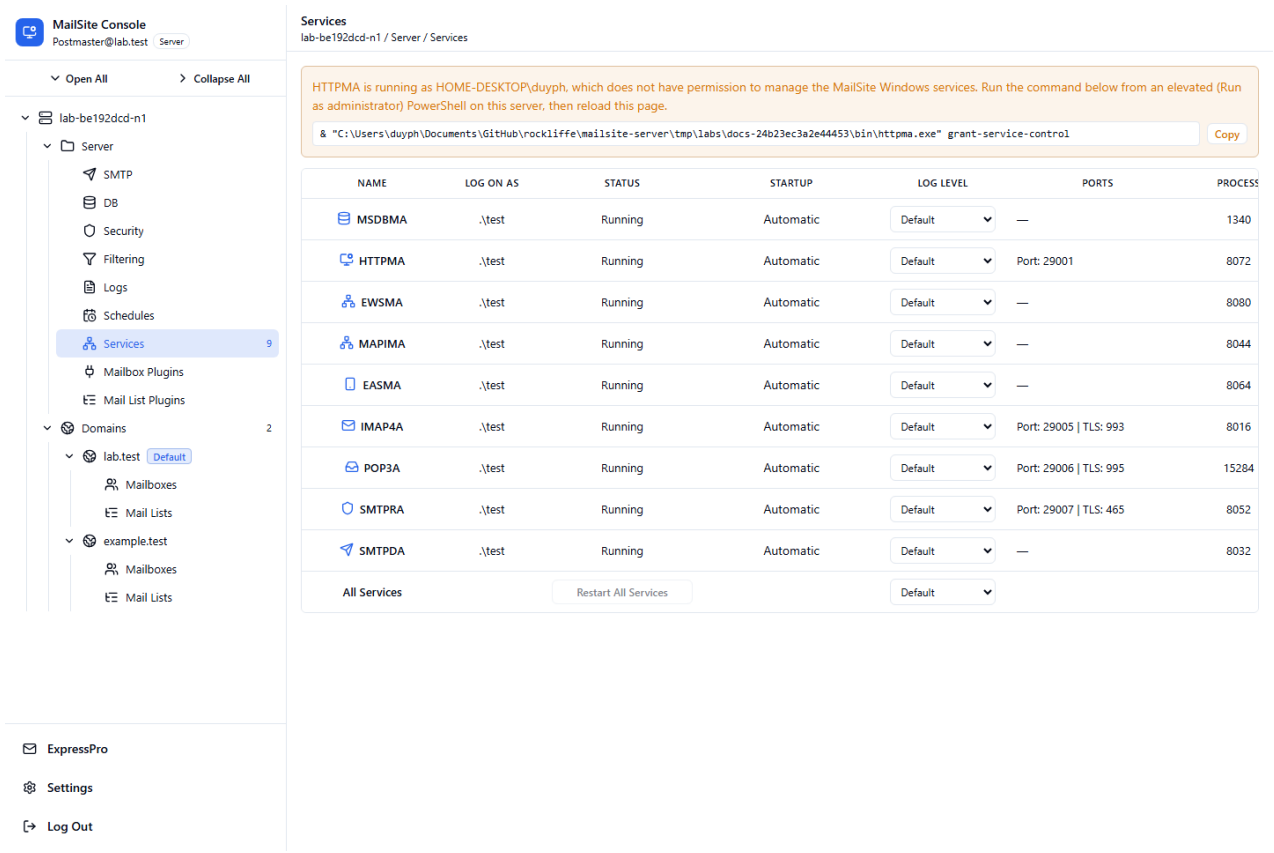

Figure 95 Current service management

MSDBMA supplies shared storage and configuration to its clients. Start it before dependent services and stop dependent services before stopping it. Stopping HTTPMA interrupts the web interface and the public EWS, EAS and MAPI endpoints it proxies. SMTPRA receives mail; SMTPDA delivers queued mail. IMAP4A and POP3A serve their corresponding mailbox clients.

EWSMA, EASMA and MAPIMA are private workers behind HTTPMA. Their endpoints must not be exposed as public administration ports. The old MAILMA and LDAP3A service descriptions are not the service set installed by the current v11 package.

Service Properties

Open the service properties from the Services table. Supported controls depend on the service; not every service exposes listening-port settings.

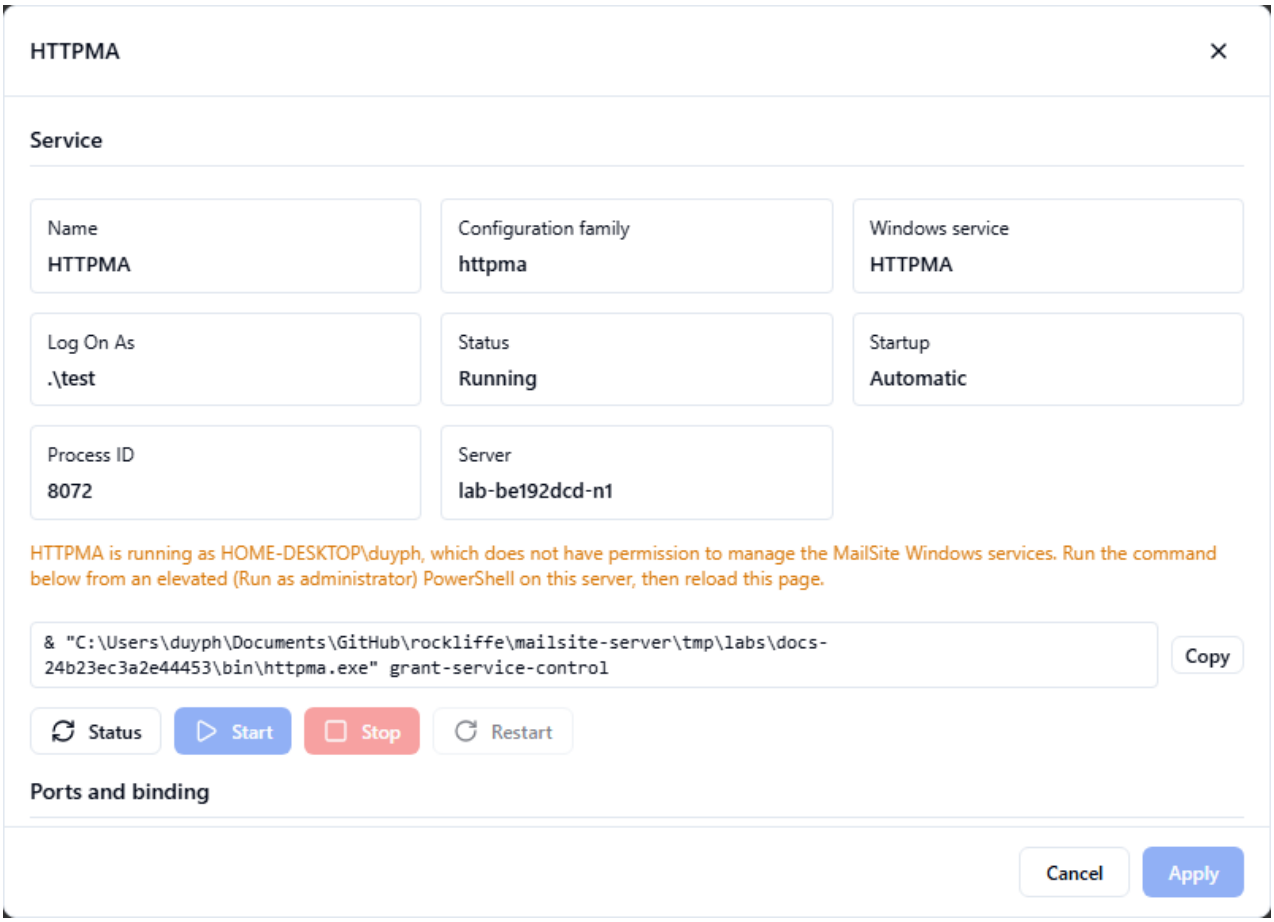

Figure 96 Service Properties

Port Number

Enter the Port Number that the Service will listen on.

Use default

Disable this field to edit the port number for the service, or enable the field to restore the default port number.

Alt SSL Port

Enter the Port Number that the MailSite service will listen on when communicating over SSL.

IP Address

Enter the IP address that the MailSite service will bind its listening sockets to. Multiple IP addresses may be entered by separating them by commas (ex. 192.168.0.1, 192.168.0.2, etc.).

Mailbox Plugins

Click on the Mailbox Plugins folder to configure the available mailbox plugins on the target server.

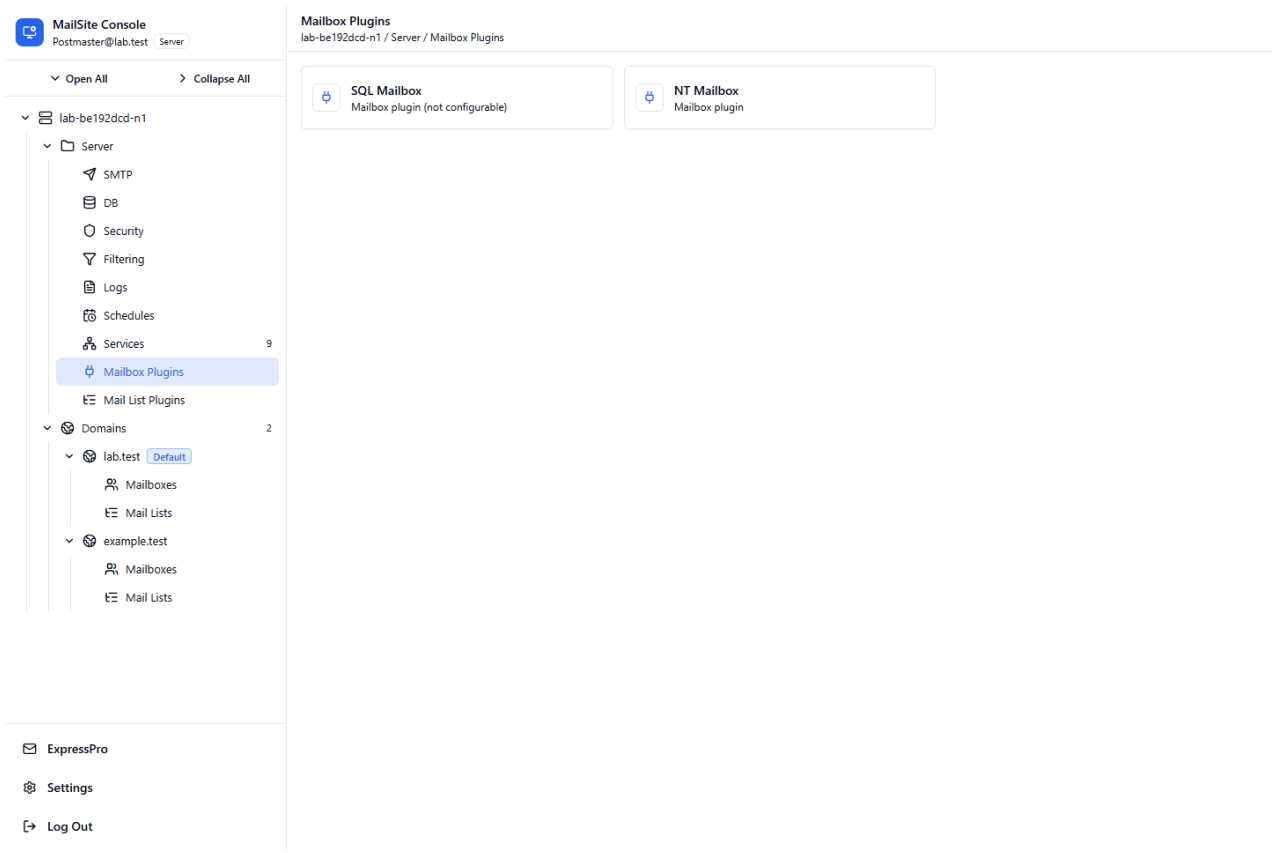

Figure 97 Mailbox Plugins

You can configure any of the Plugins by double clicking on its icon.

Each mailbox type is implemented by a Mailbox Plugin. MailSite ships with four Mailbox Plugins: Registry, NT , Database, and SQL. Only one of the Registry and SQL mailbox plugins will appear depending on whether your mail server is in Registry or SQL Connector mode. Your license key may not enable the SQL Connector mode and the SQL mailbox plugin.

External database mailbox configuration

Use Server, External Database Mailboxes. Select Generic database table or Emerald, configure the 64-bit ODBC data source, connection user, password and bounded timeouts, then save. Leave the password blank to retain the current secret; use the explicit clear control to remove it.

Choose the domains allowed to create eligible external accounts automatically. Automatic creation is disabled unless explicitly enabled for a domain. A current source lookup controls authentication; disabling an external user prevents login without deleting existing messages.

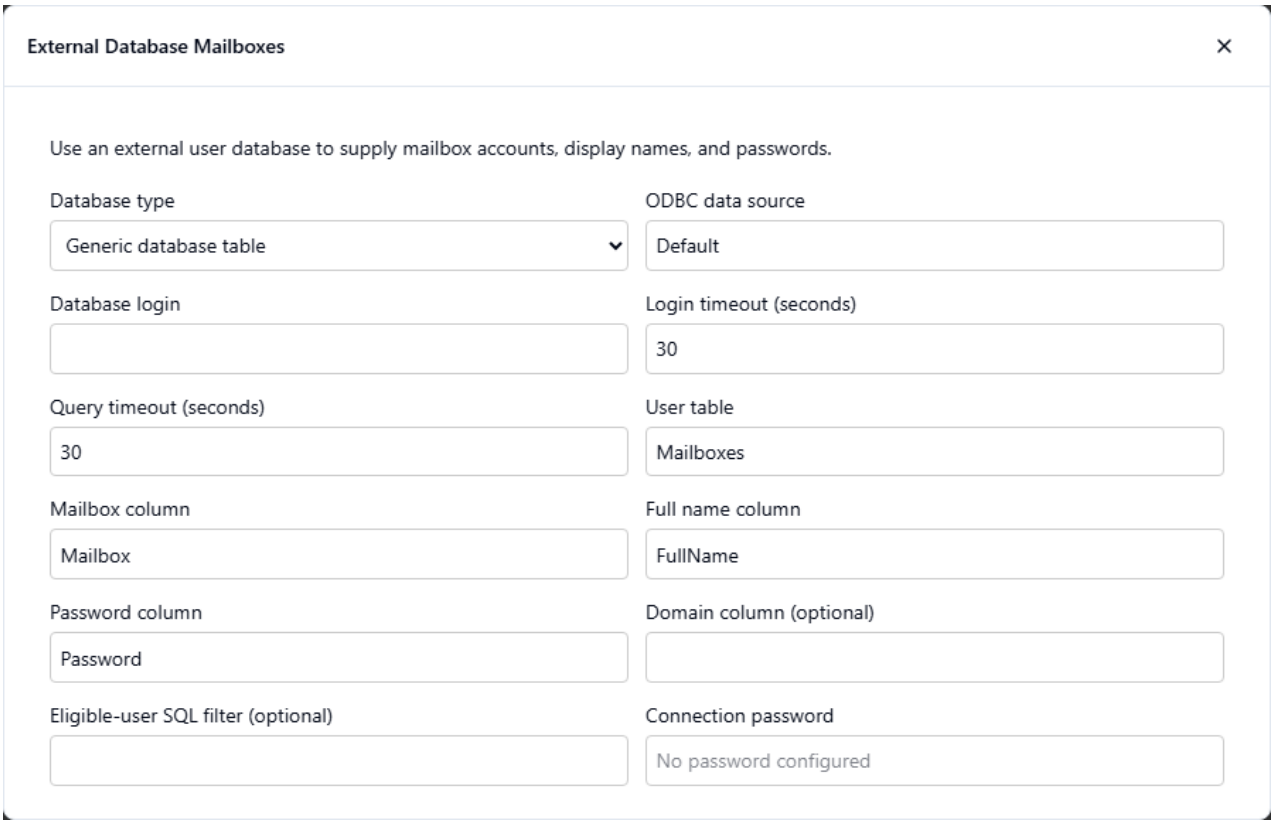

Figure 98 External database mailbox configuration

Generic database configuration

Configure the user table and mailbox, full-name and password columns. The optional domain column limits rows to the selected MailSite domain; the optional eligible-user SQL filter excludes rows such as disabled accounts. The source password contract expects password values and is not a general adapter for arbitrary password hashes.

Preview the saved source before provisioning. Invalid names, duplicate rows and collisions with native accounts are not silently converted. Batches are limited to 500 accounts, retain completed accounts after interruption and stop starting new work at the time budget. Narrow the source filter and retry remaining accounts when necessary.

Emerald database configuration

Select Emerald and configure the data source, credentials, timeouts and ESID. The connector uses ListMailUsers, VerifyMailUser and ChangeMailUserPassword according to the retained Emerald contract. Confirm stored-procedure permissions and returned columns against your database before enabling automatic creation. Preview and provisioning use the same current Console workflow as Generic mode.

NT Mailbox Plugin Configuration

Use this form to configure the NT Mailbox Plugin.

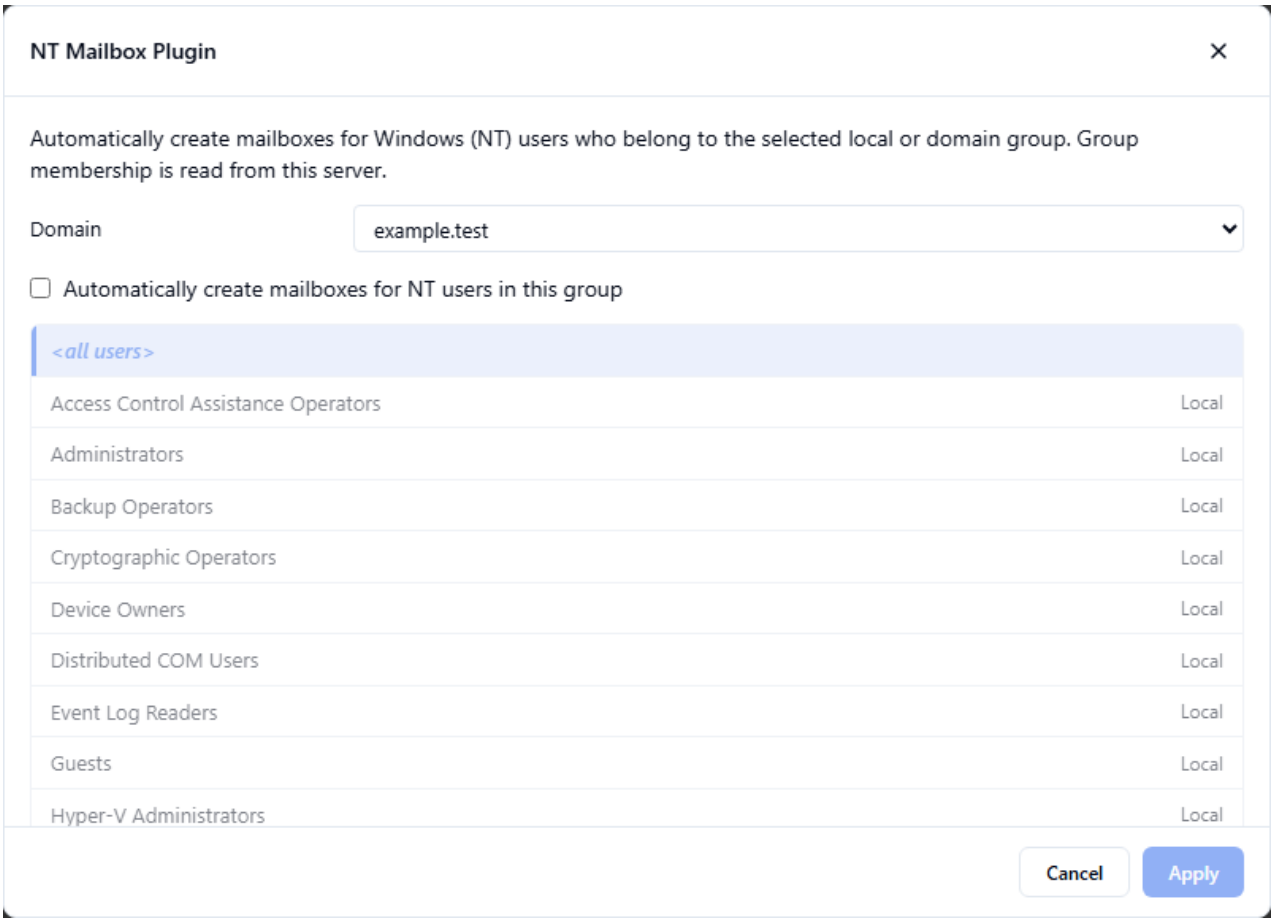

Figure 99 NT Mailbox Plugin Configuration

The NT Mailbox Plugin page configures Windows-group automatic mailbox creation for the selected domain. These settings are independent of external database mailbox provisioning.

Automatically Create NT Mailboxes

When enabled, a missing-mailbox lookup during login or delivery can create a Windows-backed MailSite mailbox for an existing enabled Windows user. An empty group permits all eligible Windows users; otherwise the user must belong to the selected local or domain group. Group lookup failures do not grant eligibility. Existing MailSite identities are preserved. Creating the mailbox does not authenticate the requester: Windows credentials and normal access policy still apply. Validate domain-controller access under the actual service identity.

NT Group

Select one of the NT Groups that you wish to use. Local Groups are listed with a computer icon. Domain Groups are listed with a server icon.

Mail List Plugins

Click on the Mail List Plugins folder to view the available mail list plugins on the target server.

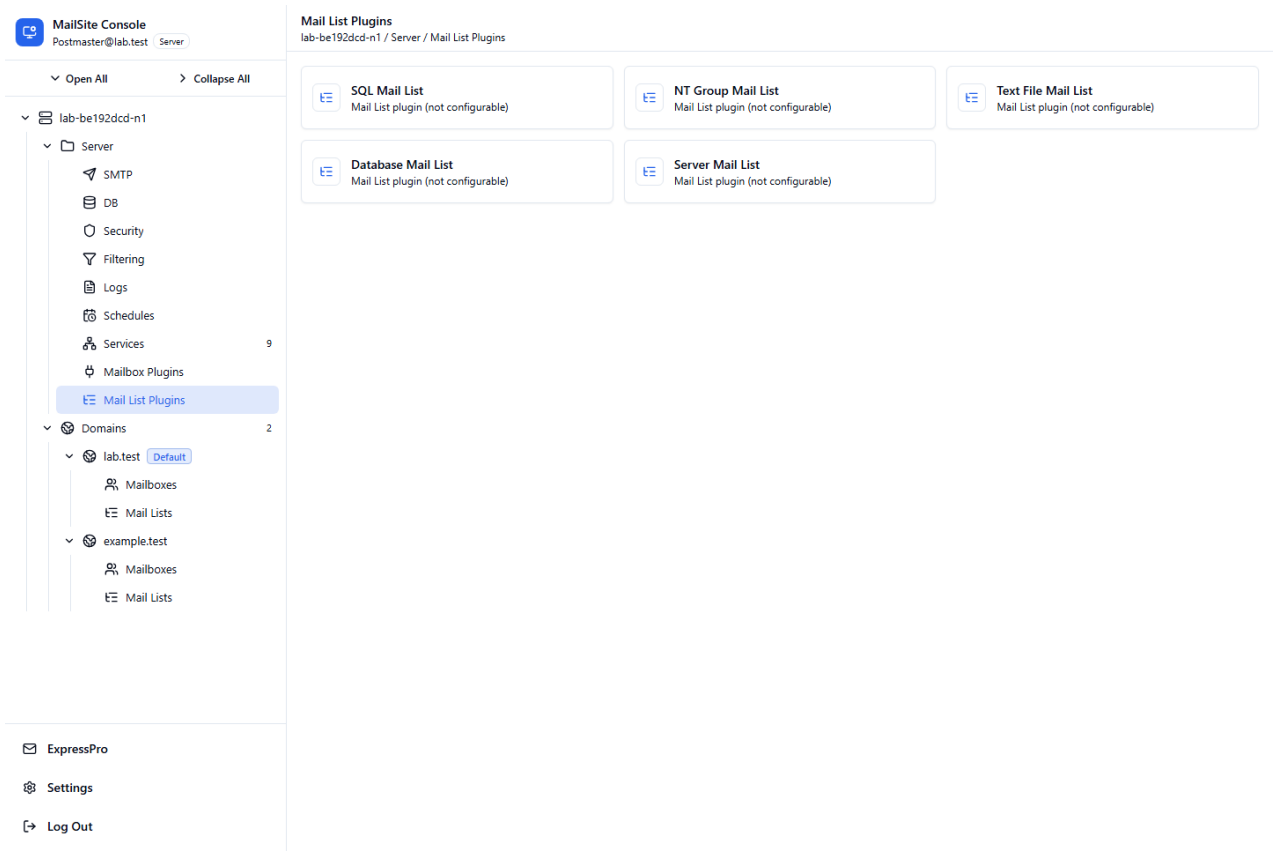

Figure 100 Mail List Plugins

Mailing-list sources are native MailSite membership, Windows groups, text files, databases and server-mailbox masks. Configure source-specific values in each list. These are built-in providers; arbitrary legacy membership DLLs are not loaded.

Domains

The Console contains a Domains Folder that expands to show a list of the mail domains that are managed by the Console. Each domain is represented by a folder, which itself contains folders for the mailboxes and mail lists belonging to that domain, and icons representing properties and options for the domain itself.

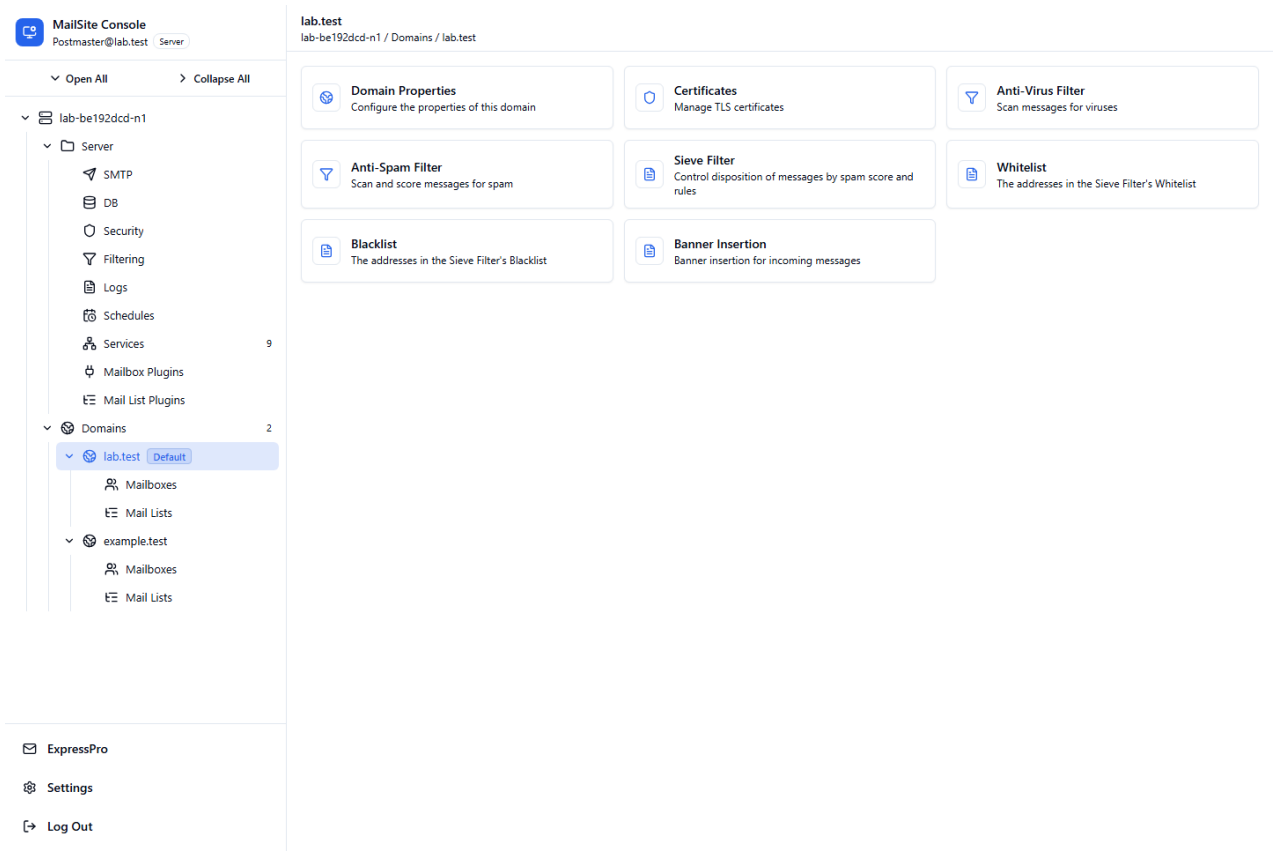

Figure 101 Domains

Default Domain

The default domain is marked Default in the domain list. Review its configured name in Server Properties; it is not inferred afresh from the Windows DNS settings when you open the Console.

The default domain always exists—you cannot delete it. However, the default domain name can be changed. For example, if MailSite was installed with the default domain mail.mycompany.com , you can change this to be mycompany.com.

Rename Default Domain

Select the domain and choose Rename Domain from its actions. Enter the new name and confirm.

Review account addresses, client logins and external DNS after renaming.

If you rename the default domain, it is your responsibility to ensure that the new domain name has an appropriate MX record in the DNS, so that mail addressed to user@mucompany.com gets routed to the mail server at mail.mycompany.com.

Use the current domain action when renaming an eligible domain. Do not replace it with an improvised copy/delete operation; verify mailbox access, list delivery and any dependent routes afterward.

New Domain

Open Domains and choose Create Domain. Enter the new domain name and required settings.

Configure the public DNS separately and verify delivery before creating production traffic.

Delete Domain

To delete a domain, select the domain(s) you wish to delete, then either select Delete from the right-button pop-up menu, or click the Delete button. You cannot delete a domain if it still contains mailboxes or mail lists.

Domain Properties

To change the properties of a domain, double-click on its Domain Properties icon, or select the domain and choose Properties from the right-button pop-up menu. The resulting dialog lets you associate an IP address with the domain and control whether you want non-delivery messages from this domain to be copied to the postmaster. Note that it is not possible to associate the default domain with an IP address.

Anti-Virus Filter

The current Anti-Virus Filter uses the MailSite 11 scanning configuration. Review scope, message-size exclusions, scanner-failure behavior and protected archives. Inspect scan counters and definition-update status. See Virus Scanning for the policy and validation workflow.

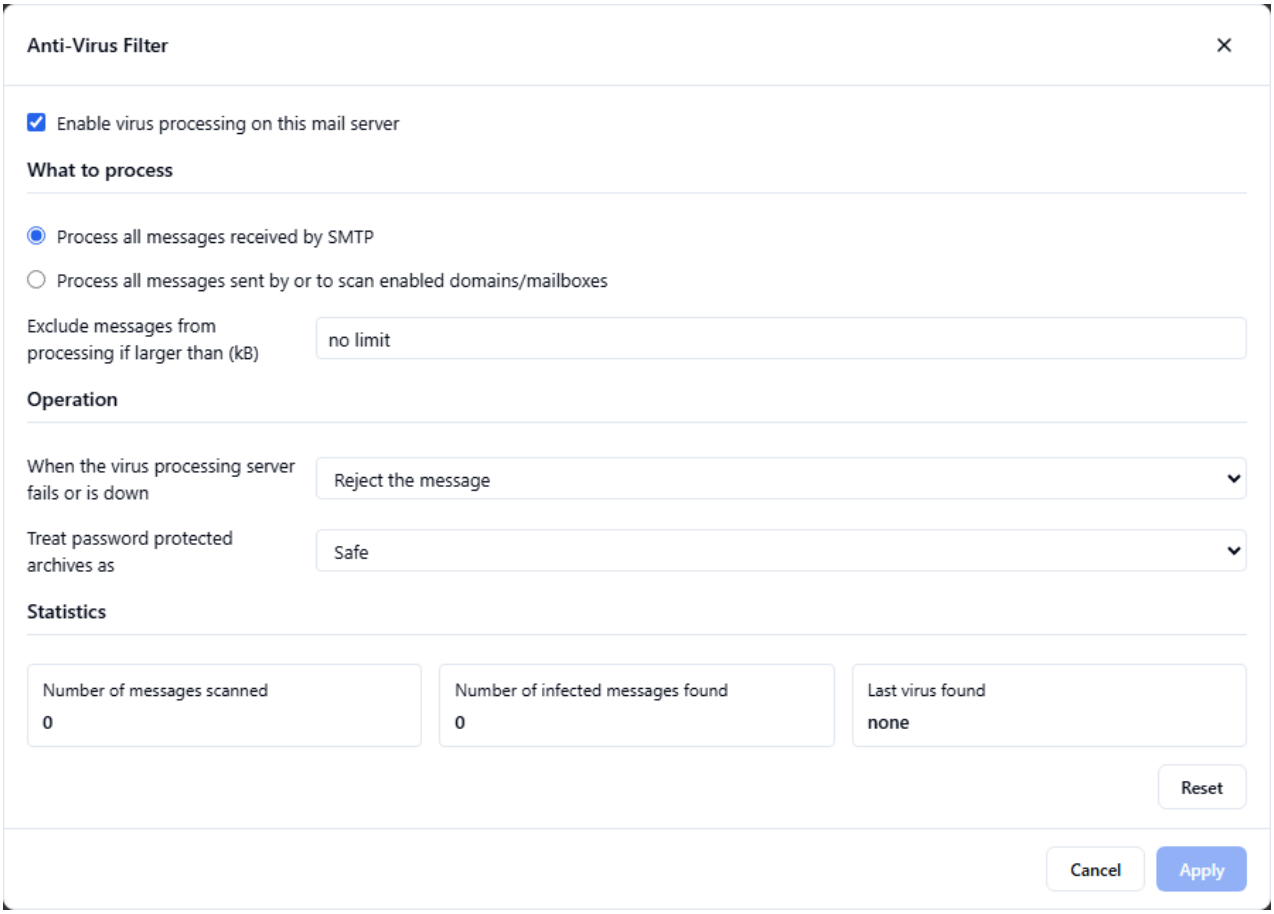

Figure 102 Anti-virus settings

Anti-Spam Filter

The Anti-Spam Filter controls scanning and exemptions. Junk/quarantine retention runs separately using the configured purge age and folder mask. The default is thirty days for Junk/quarantine, with a grace period for recently indexed messages. See Spam Scanning and Mail Filters before enabling Trash purging or reducing the age.

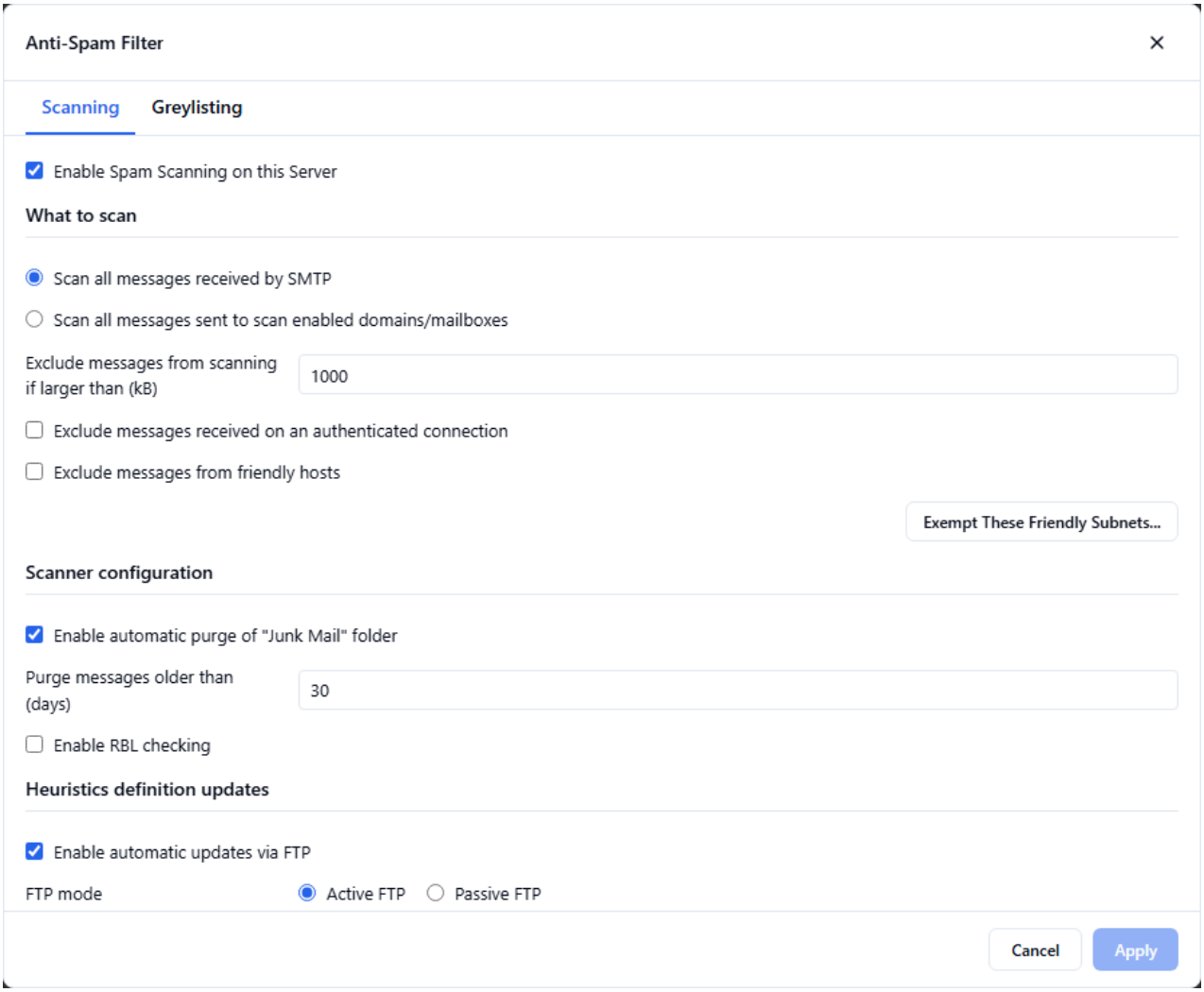

Figure 103 Anti-spam settings

Sieve Filter

To set domain-level mail filters, double-click on the Sieve Filter icon. This displays the Sieve filter rules associated with the domain and allows you to create, modify, and delete filter rules. Domain-level filter rules are applied only to messages sent to or from mailboxes in this domain.

Banner Insertion

To set custom message banners for a domain, double-click on the Banner Insertion icon. For each domain, you can specify a header and/or footer to be added to the contents of each message sent by users within that domain.

Virtual Domains

You can receive mail addressed to multiple domains on a single server. To do this, create a new entry for each under the Domains Folder. With virtual domains, mailboxes and mail lists can be managed on a per-domain basis, and each domain may have its own postmaster.

For example, if you add a virtual domain xyz.com, then incoming mail sent to someone@xyz.com will be delivered to mailbox someone in domain xyz.com.

Note that the DNS MX record for xyz.com must resolve to the IP address that is associated with domain xyz.com listed here. This is necessary so that other SMTP mail servers connect to the correct machine. See the DNS Overview section and the section on Multiple Domains for more information.

Each virtual domain can be (but need not be) associated with one of the IP addresses on the server. If a POP3, IMAP4 or SMTP call is received at an IP address which has a domain associated with it, then the server will assume that domain name if a mailbox name without attached domain is sent by the

POP3, IMAP4 or SMTP client. If the IP address does not have a domain associated with it, then the default domain name will be assumed. (See the section on the POP3 Server for additional discussion of how the domain name may be specified when a client logs in.)

Domain General Page

You can configure the properties of the domain by double clicking on the Domain Properties icon. The domain properties form contains tabbed property pages. The General domain property page looks like this:

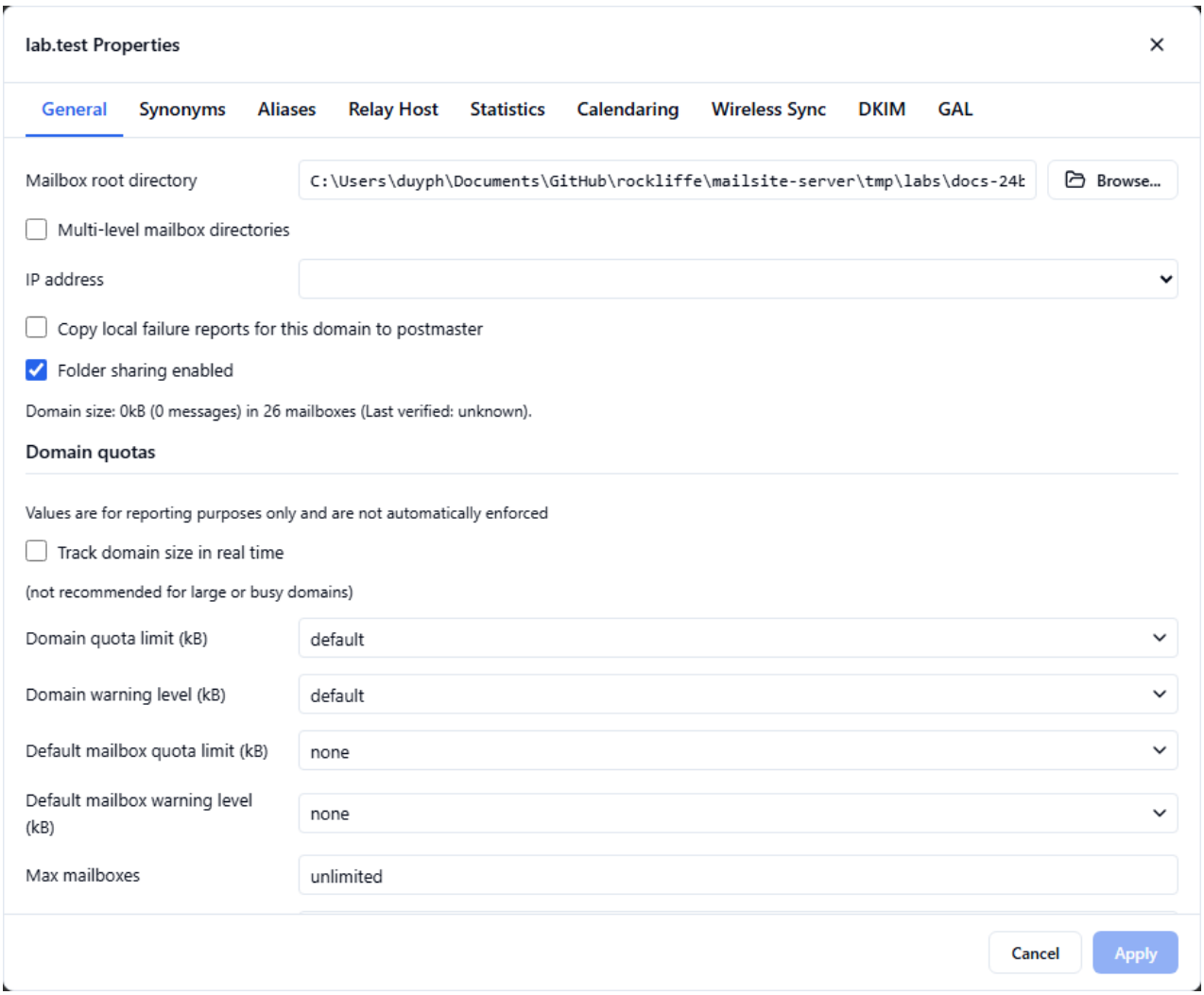

Figure 104 Domain General Page

Mailbox Root Directory

Enter the mailbox root directory that you wish to use to for the message store for your mail users. The mailbox directory root defines the location of the directories for each mailbox.

A mailbox consists of two things:

- Mailbox Properties are stored in the active registry or SQL configuration backend and managed through MSDBMA and the Console.
- Mailbox Directory, whose location is determined by the mailbox directory root and whose name matches the associated mailbox.

The mailbox directory contains a sub-directory called inbox in which incoming mail is stored. This is referred to as the

incoming mail directory for that mailbox.

It is recommended that mailbox directories are located on a NTFS partition. See the Security section for additional information.

If you wish to reset the mailbox root directory for a domain to its default value, simply leave the field blank. When you re-display the dialog, it will show the default value. The default is: C:\Program Files\MailSite\BOX

Multi-Level Mailbox Directories

Use this option to specify that mailbox directories for the domain should be multi-level.

By default, mailbox directories are located within the mailbox root directory for the domain. For example, if the mailbox directory root is C:\MAILBOX, then the mailbox directory for the mailbox fred will be C:\MAILBOX\fred.

However, if an extremely large number of mailbox directories exist at the same level of the file system, mail access can become less efficient and performance can be affected. For this reason, it is advisable to use multi-level mailbox directories for domains with more than 1,000 mailboxes.

When a domain uses this option, MailSite will use the first three letters of the mailbox name (each following an exclamation mark) to construct a three-level directory path. For example, if the mailbox directory root is C:\MAILBOX, then the multi-level mailbox directory for fred will be at C:\MAILBOX\!f\!r\!e\fred.

It's important to know that changing this option for a domain in the Windows Console does not convert the domain's existing mailboxes to the multi-level directory structure (or back to single level). If you enable this option for an existing domain, you must manually convert the domain's mailboxes using the MSCVTDIR utility. For example, to convert mailbox directories in the domain mailsite.com to multi-level, execute:

mscvtdir mailsite.com

Refer to the Utilities Appendix for more information on MSCVTDIR.

IP Address

Use this field to select the IP address for this virtual domain. If it is set to <none>, then the domain will share the IP address with the default domain. In this case, POP3 and IMAP4 users must log in with a fully qualified user name, such as joe@example.com.

In addition, users must use this DNS address as their SMTP and POP3 server. In this case, POP3 and IMAP4 users can log in with their simple name, such as joe, or with their fully qualified name, such as joe@example.com.

If you associate the virtual domain with an IP address, then the DNS record for this domain must resolve to this IP address. This is particularly important when hosting domains for other organizations as MailSite will use the name associated with the IP address whenever it would normally present the machine name. For example, the greeting string presented by each of the services will include this name so that end-users and those they communicate with will be unaware that the domain is hosted on another cluster.

The hostname associated with the domain is stored in the HostName domain property, and can be overridden for domains where the IP address is associated with an unsuitable name.

SMTPDA uses the HostName property when relaying messages to remote domains. If this behaviour is not required, set the UseDefaultOutboundIpAddress server property to FALSE directly in the registry or database.

See the section on Multiple Domains for more information.

Copy local failure reports to postmaster

Check this box to copy any local delivery failure reports to the postmaster in addition to the sender. Delivery failures occur when an incoming message for the selected domain is addressed to a mailbox or mail list that does not exist.

Track domain size in real time

Tracking domain size in real time can be an expensive task, particularly for very large or heavily used domains. It is therefore recommended that this option is enabled only for smaller domains. If quota checking is enabled but this option is disabled, the quota will be updated periodically by the housekeeping thread in SMTPDA.

Domain Quota Limit

If quota support is licensed and enabled, use this field to set a quota limit for this domain. This is a total size for all mailboxes in the domain. This limit is not currently enforced by MailSite due to the potential of increased administration

when dealing with disabled domains. Domain quotas are provided in order to assist with common reporting and administration tasks, particularly when hosting multiple domains.

Domain Warning Level

If quota support is licensed and enabled, use this field to set a warning level for this domain. This warning level is not currently enforced by MailSite and is provided to assist with common reporting and administration tasks, particularly when hosting multiple domains.

Default Mailbox Quota Limit

If quota support is licensed and enabled, the page also displays the approximate count of mailboxes, total number of messages and total message size in the domain. You can set default values for the mailbox quota limit and for the warning level. See the section on Quotas for more information.

Default Mailbox Warning Level

If quota support is licensed and enabled, use this field to set the quota warning level. This is the level of mailbox volume that will trigger a warning message to the user, alerting them that their mailbox is nearly full. See the section on Quotas for more information.

Max Mailboxes

You can use this field to limit the number of mailboxes that can be created in this domain. You may wish to use this feature if you delegate management of mailboxes for this domain to your users through the Web Console. Leave this field blank if you do not want a limit. If you try to set the maximum value to less than number of existing mailboxes, you will be warned but will be permitted to do so. Enter zero if you do not want to create any mailboxes in this domain. Note that your license key may override the value that you enter here, and may further limit the number of mailboxes that can be created.

Max Mail Lists

You can use this field to limit the number of mail lists that can be created in this domain. You may wish to use this feature if you delegate management of mail lists for this domain to your users through the Web Console. Leave this field blank if you do not want a limit. If you try to set the maximum value to less than number of existing mail lists, you will be warned, but will be permitted to do so. Enter zero if you do not want to create any mail lists in this domain. Note that your license key may override the value that you enter here, and may further limit the number of mail lists that can be created.

Mail list Root Directory

Enter the root directory that you wish to use to for the storage of mail list messages and related information. This mail list root directory will contain sub-directories corresponding to each mail list in the domain. When using MailSite in a clustered configuration, this root directory should be a shared file system used by each MailSite node.

Domain Synonyms Page

The Synonyms page of the Domain Property dialog looks like this:

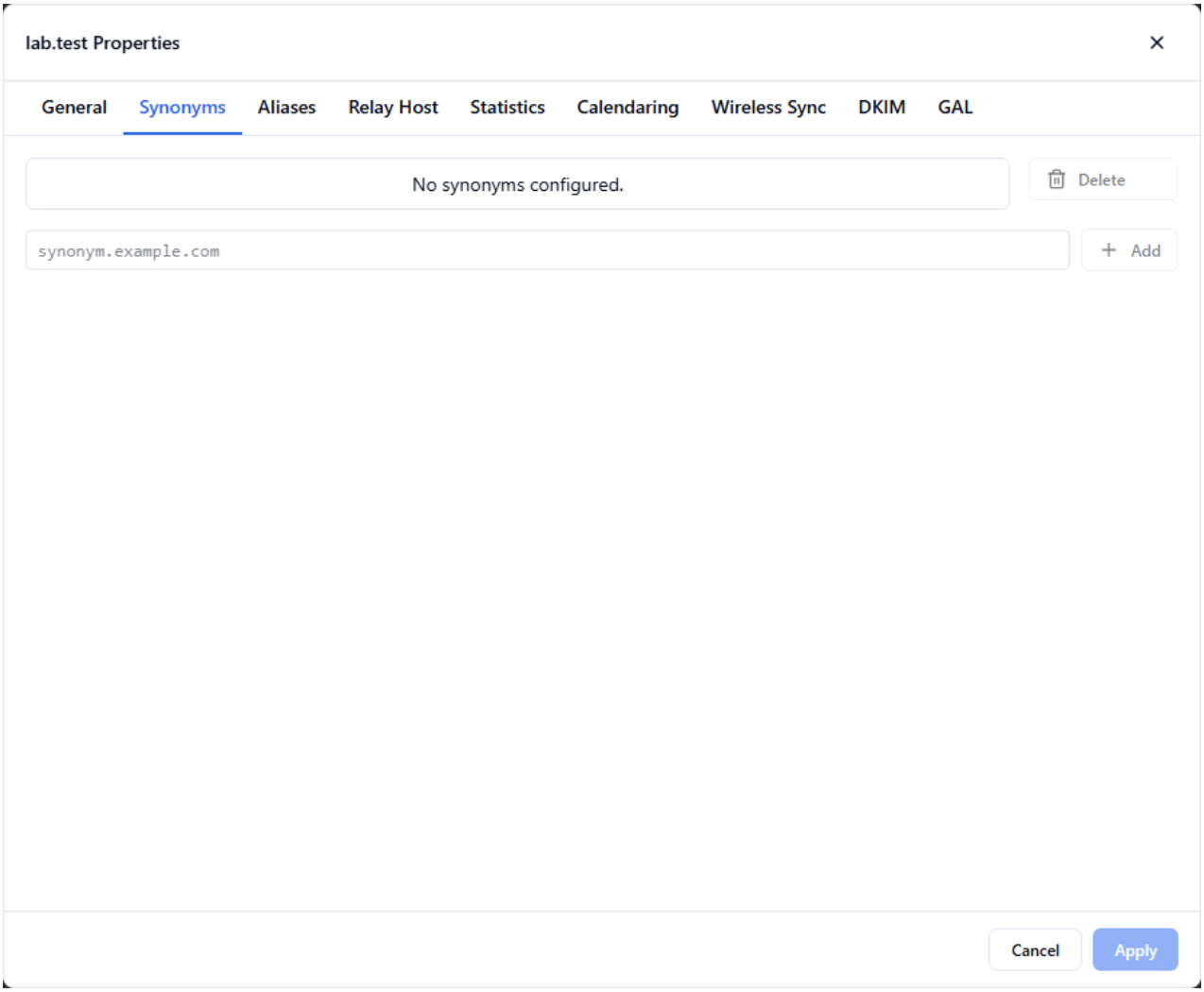

Figure 105 Domain Synonyms Page

A Domain Synonym is a name that is equivalent to the virtual domain in question. If your virtual domain is xyz.com, and you create a synonym of xyzcompany.com, then mail addressed to you@xyzcompany.com will go to you@xyz.com. See the section on Multiple Domains for further information on synonyms.

To create a new synonym, type the synonym in the edit box and click Add. To delete a synonym, select it in the list box and click Delete.

Domain Aliases Page

The Aliases page of the Domain Property dialog is available only when MailSite is configured to use the SQL Connector and displays list of mailbox aliases in the domain:

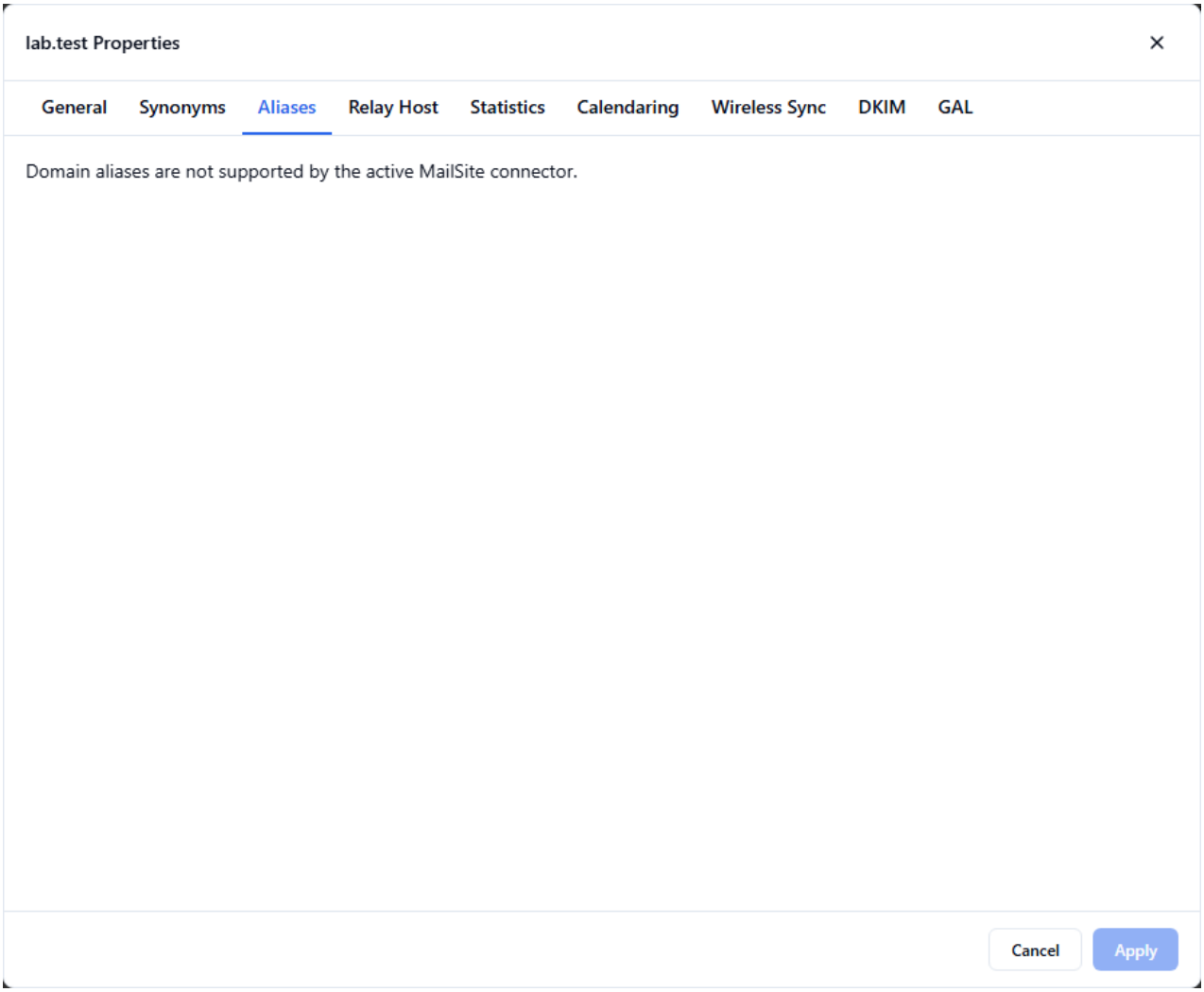

Figure 106 Domain Aliases Page

The aliases displayed on this page are read-only. To add, delete, or modify mailbox aliases, use the Aliases page of the Mailbox Properties window for the target mailbox.

Relay Host Page

The Relay Host page of the Domain Property dialog looks like this:

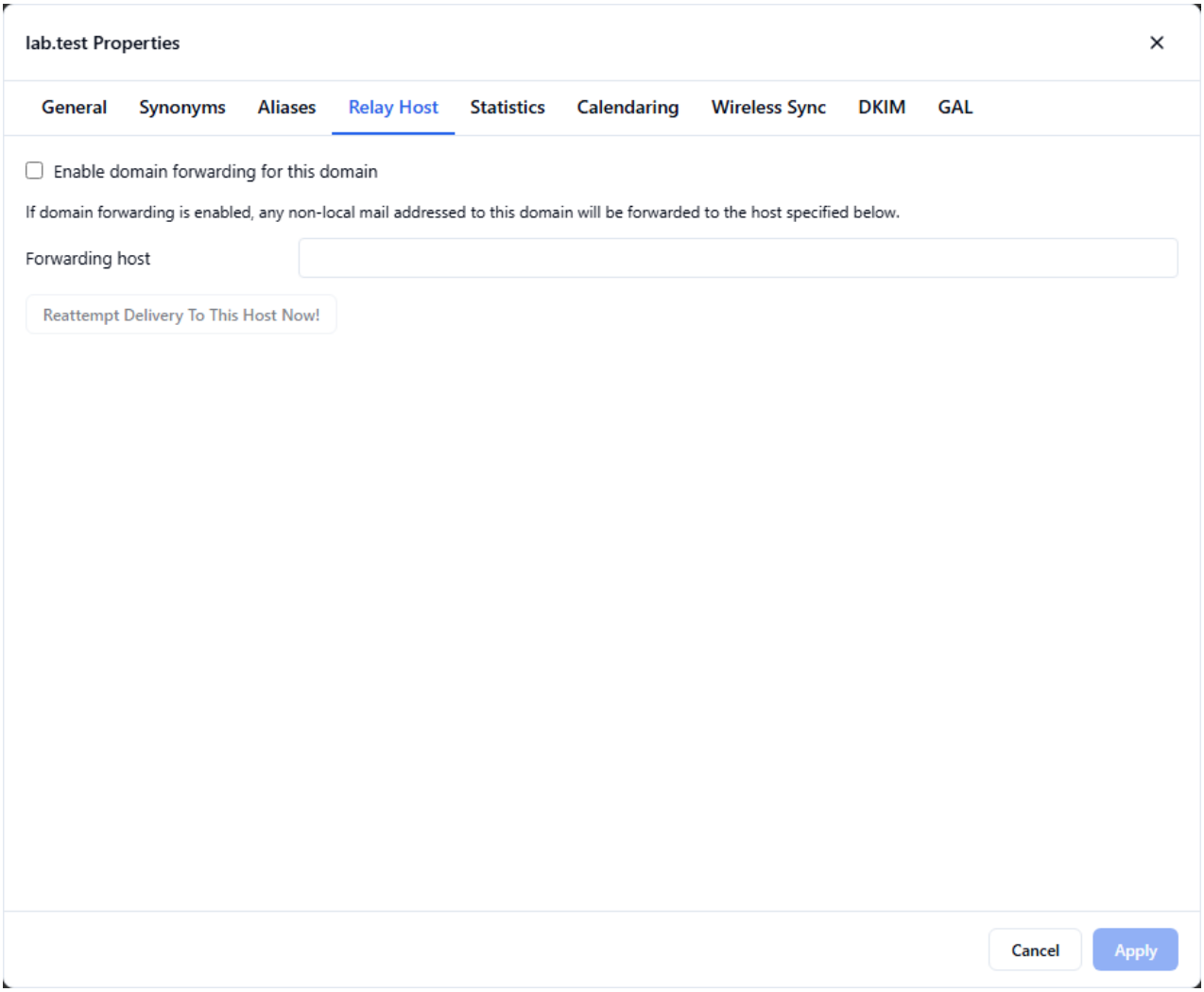

Figure 107 Relay Host Page

Mail servers that act as intermediaries in mail delivery are often referred to as “relays.” When your system is acting as a relay, messages meant for other computers will be placed in your server’s queue and delivered accordingly. MailSite can act as an Internet gateway relaying mail to and from the Internet. Internet gateways have no local users. A relay host handles local users.

The checkbox on this dialog enables or disables domain forwarding for this domain.

All mail addressed to this domain will be automatically forwarded to the hostname specified on this page. Any valid domain name or IP address may also be entered in this field.

The “Reattempt delivery to this host now!” button will force an instant attempt to deliver any queued mail for this domain to the specified host. This button will only work when forwarding is enabled and will be disabled until the button is pressed again.

Domain Keys Identified Mail (DKIM) Page

MailSite includes the ability to sign messages using DomainKeys Identified Mail. DKIM is a method for email authentication that allows an organization to take responsibility for a message in a way that can be validated by a recipient

DKIM is configured on a per domain basis.in the Domain Properties dialog DKIM tab.

To enable DKIM on outbound messages you must enable it in MailSite and also update DNS. You will need to contact your DNS administrator for assistance with DNS management.

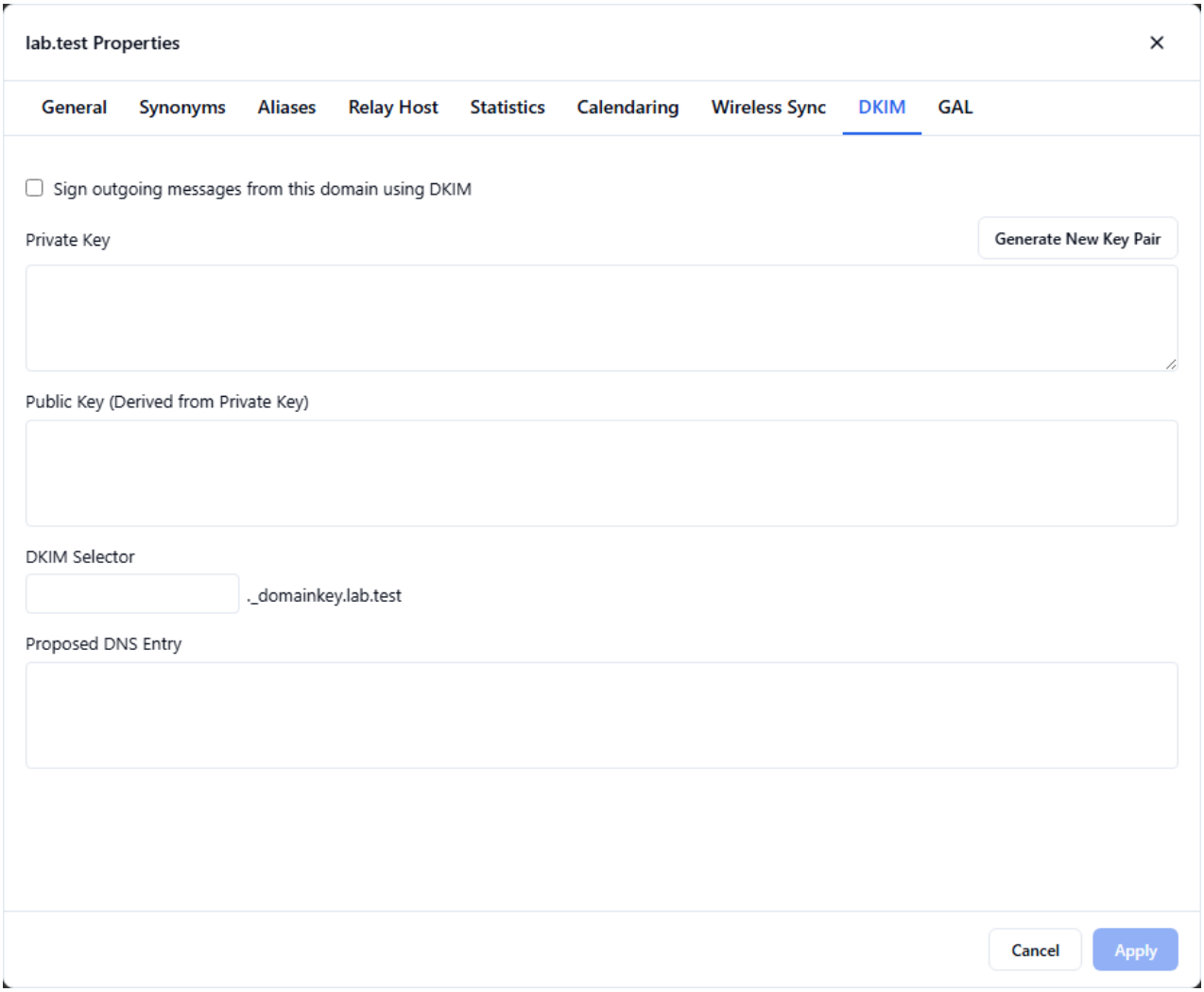

Figure 108 Domain Keys Identified Mail (DKIM) Page

To Enable DKIM in MailSite:

Load the MailSite Console and select the domain you want to enable DKIM for, eg domain.com.

Select Domain Properties on the right hand side.

Select DKIM tab

Select 'Sign outgoing messages from this domain using DKIM

If you already have a Private key you wish to use, paste it into the 'Private Key' box, The 'Public Key' and 'Proposed DNS Entry' box should auto fill. If they fail to auto fill, it means the Private key you entered is invalid.

If you do not have a private key already, select 'Generate New Key Pair.

Enter a DKIM Selector. This name will also be used in DNS, eg "mail", so it will read mail._domainkey.domain.com

To Enable DKIM in DNS

Create a TXT record at your authoritative DNS provider using the selector and proposed public record shown in the Console.

For selector mail and domain example.com, the full record name is mail._domainkey.example.com.

Some DNS providers append the zone name automatically; enter the relative name they require.

Paste the Proposed DNS Entry as the TXT value. Never publish the private key.

Save the DNS change and verify the record through an external resolver.

Apply the corresponding DKIM settings in MailSite and send a test message.

Confirm the resulting signature at the recipient before relying on the configuration.

Domain Statistics Page

The page shows a number of useful statistics about the domain.

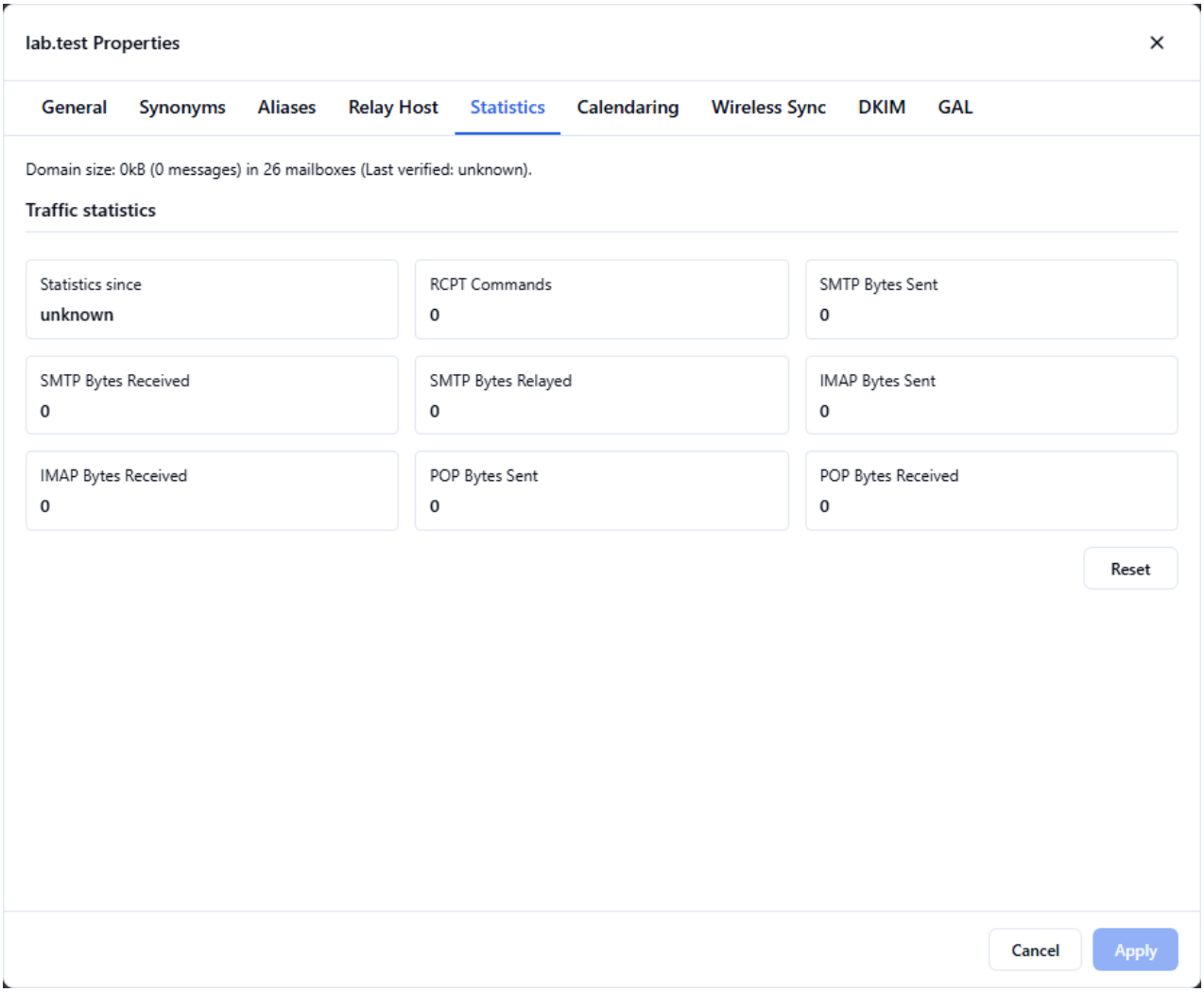

Figure 109 Domain Statistics Page

Domain Size

The domain size is calculated at regular intervals and so the figure shown will be recent, but not necessarily right up to date.

Traffic Statistics

A number of useful statistics are included to assist in management of domains. SMTP data only includes authenticated SMTP sessions as non-authenticated sessions cannot definitively be linked to a specific mailbox or domain. Collected data can be reset as needed.

Statistics gathering is enabled or disbled at server level.

Domain Calendaring Page

The page allows calendaring to be provisioned as appropriate for this domain. If this tab is greyed out, calendaring is being controlled at a higher level (server level).

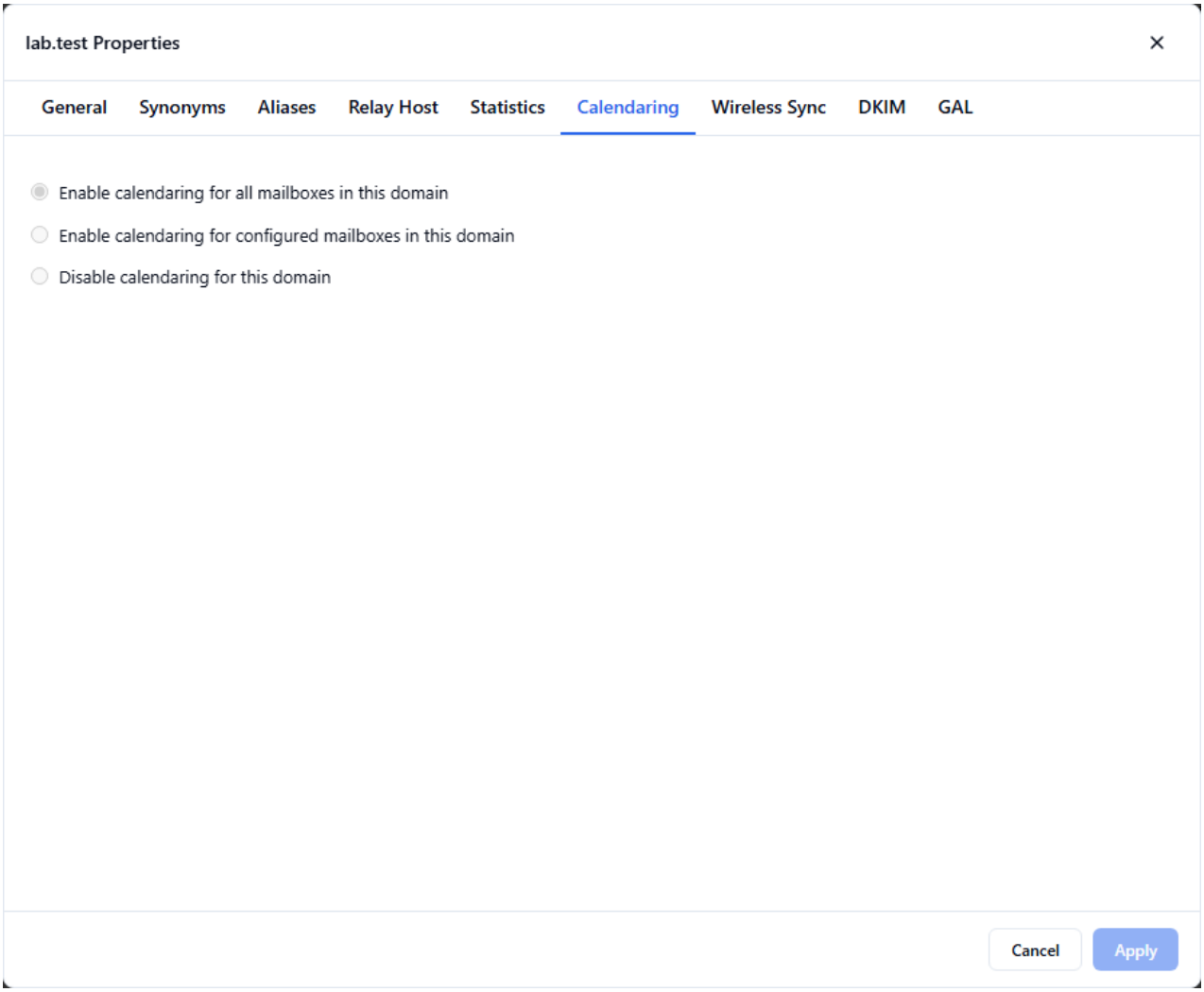

Figure 110 Domain Calendaring Page

Domain Wireless Sync Page

The page allows over-the-air device synchronization to be provisioned as appropriate for this domain. If this tab is greyed out, wireless synchronization is being controlled at a higher level (server level).

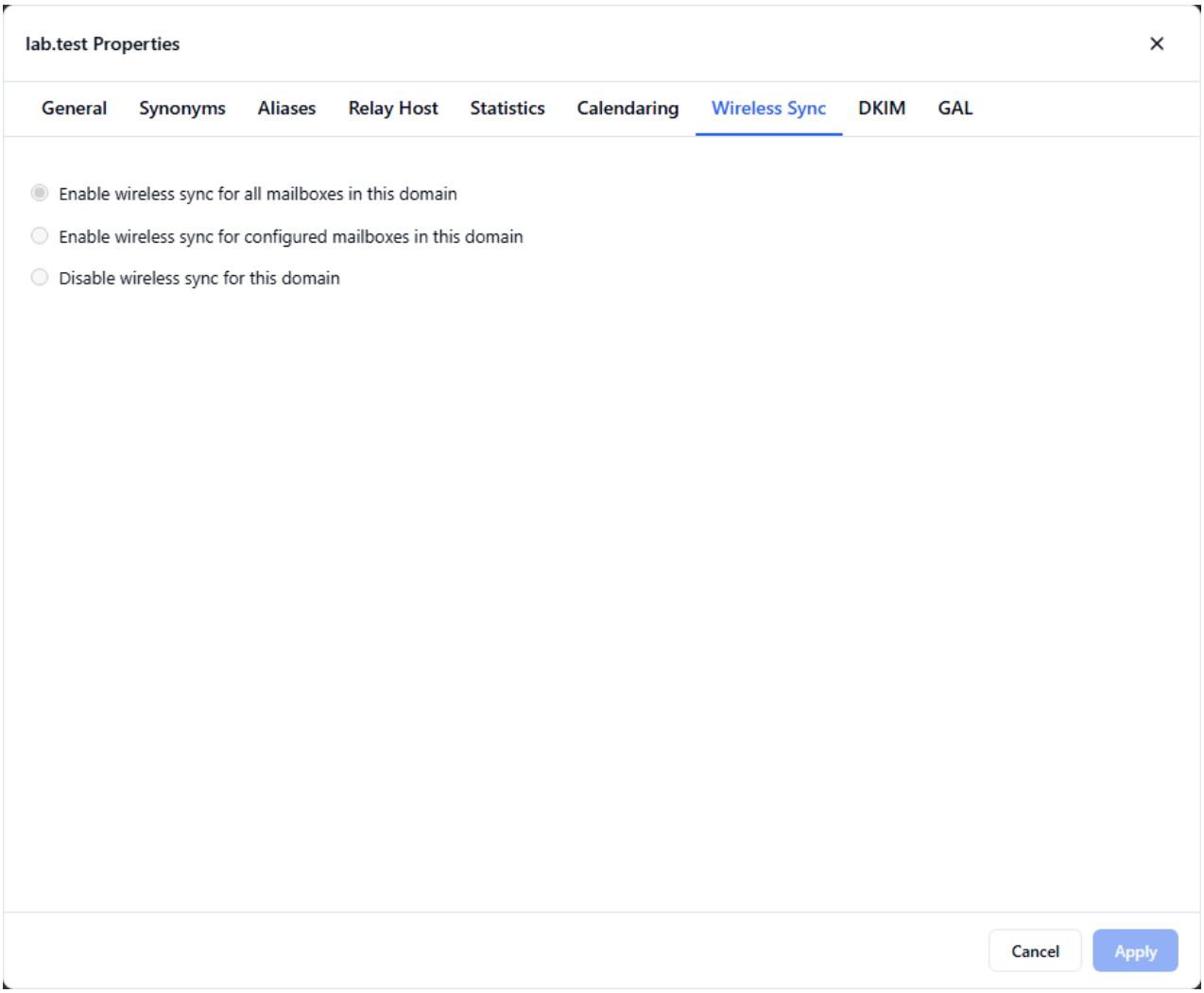

Figure 111 Domain Wireless Sync Page

Domain Virus Filter

To configure domain virus scanning options, open the domain folder in the MailSite Console, double-click the Anti-Virus Filter icon. This displays the Virus Scanning Filter window:

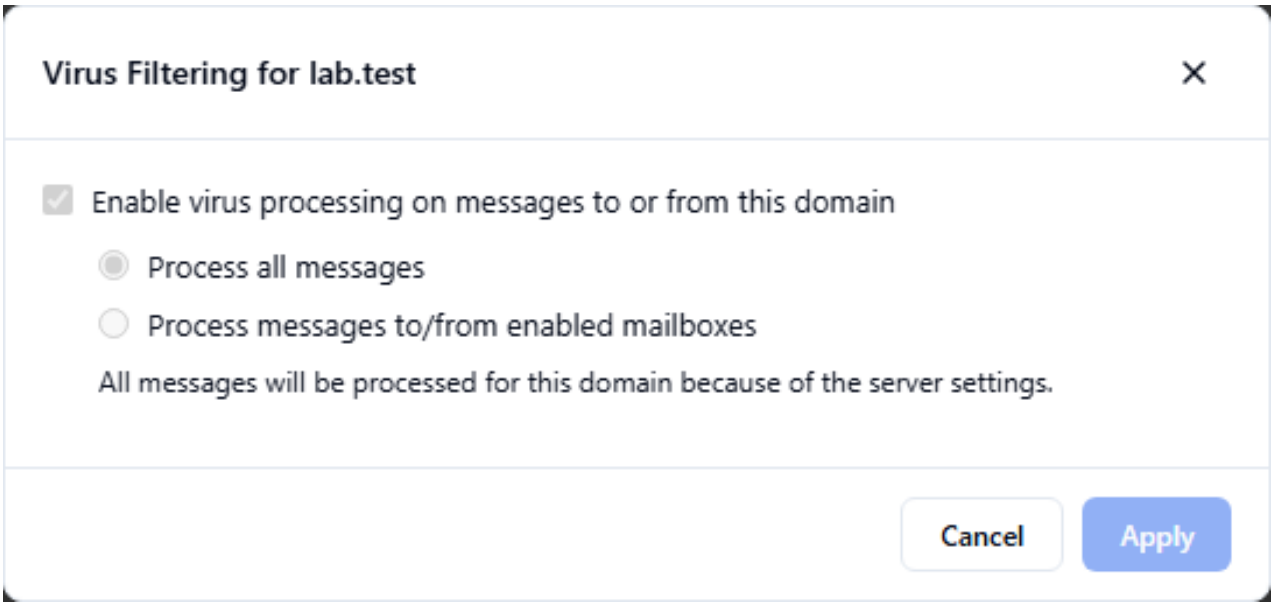

Figure 112 Domain Virus Filter

Enable virus scanning on messages to or from this domain

This option controls the virus scanning policy for this domain. If disabled, MailSite will not scan any messages sent to or from this domain. Otherwise, MailSite will scan messages according to the virus scanning policy that you select here.

Process all messages

This selection causes all messages received by MailSite's SMTP server that are sent to or from any mailbox within this domain to be scanned. Use this option if you want all mailboxes in the domain to be protected from viruses.

Process messages sent to/from enabled mailboxes

This selection causes messages to be scanned only if they are sent to or from mailboxes that have the virus scanning option enabled. Use this option if you want only certain mailboxes to be protected from viruses.

Mailboxes

Select the Mailboxes folder within a domain to display a list of mailboxes:

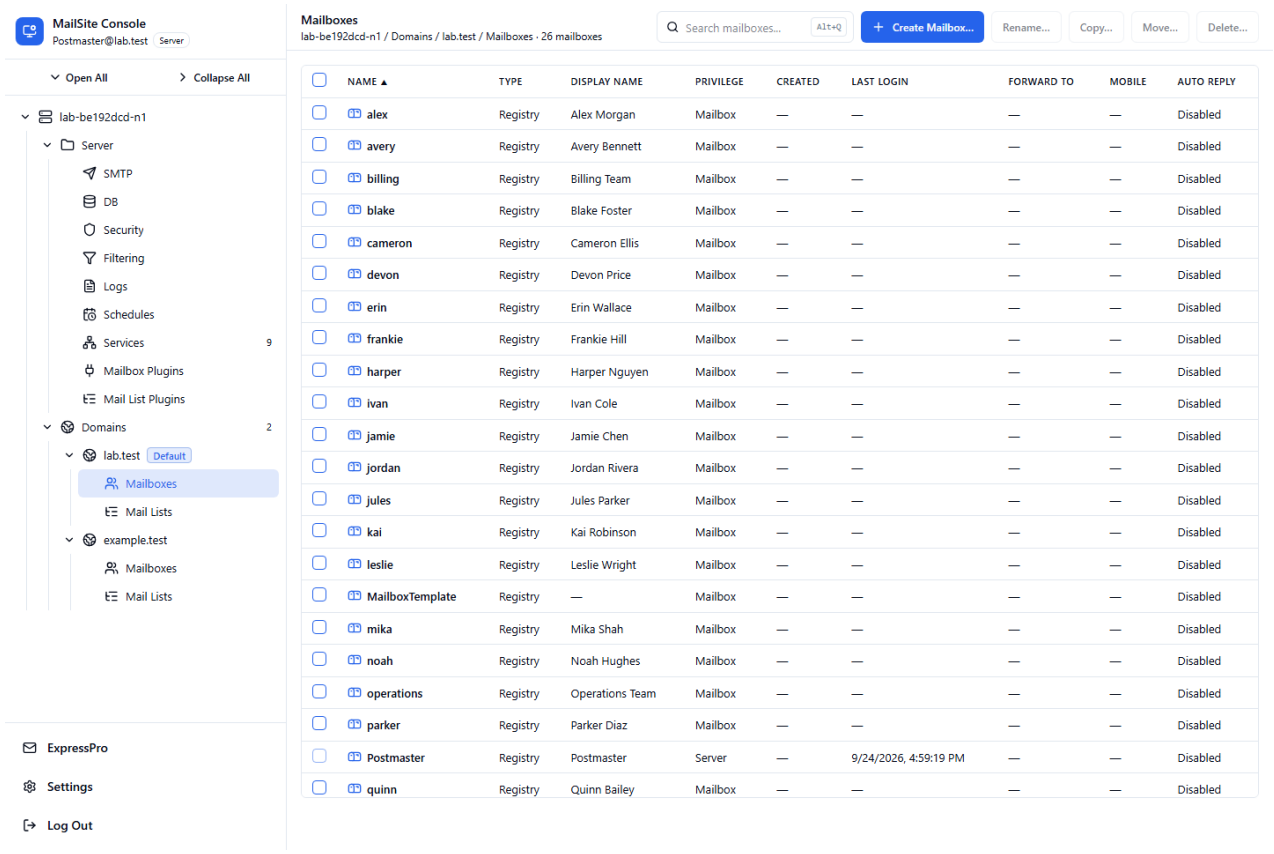

Figure 113 Mailboxes

Mailboxes are slots for delivering messages for a specific user on this server. You can create four types of MailSite mailboxes (depending on your license key): Registry mailboxes, NT mailboxes, Database mailboxes, and SQL mailboxes.

If your users will access other components of your NT server, such as the file system, then you will probably want to use NT Mailboxes. This will mean that they can use the same user name and password to read their mail that they use to log into the Windows network and connect to the file system.

Native Registry or SQL mailboxes use MailSite-managed credentials. Their MailSite privileges do not create or revoke Windows login rights; manage Windows identities separately.

If you have a database that contains a list of usernames and passwords, and you wish to integrate mail authentication with this database, then create Database Mailboxes.

If you want to use clustering to support mailboxes across multiple systems, then create SQL mailboxes.

The current mailbox list provides search and account actions. Select the intended account before using Properties, Rename, Copy, Move or Delete.

You can maintain the properties for a mailbox by double clicking on the mailbox icon. This will open the Mailbox General Page.

Viewing Mailboxes

Use Search mailboxes to narrow the current domain list. Clear the search to view all available accounts, and confirm the full account identity before changing it.

Postmaster Mailbox

A mailbox called postmaster is created in the default domain during installation. This mailbox is not counted for licensing purposes. If you wish the mail for the postmaster to go to a different address, you can set the forwarding address for this mailbox.

Mail addressed to postmaster@virtual.domain will be delivered to postmaster@default.domain, unless a postmaster mailbox is created in the virtual domain.

Add Registry Mailbox

Choose Create Mailbox, select Registry when offered by the current configuration, and enter the name and initial password. Create saves the account; verify it before use.

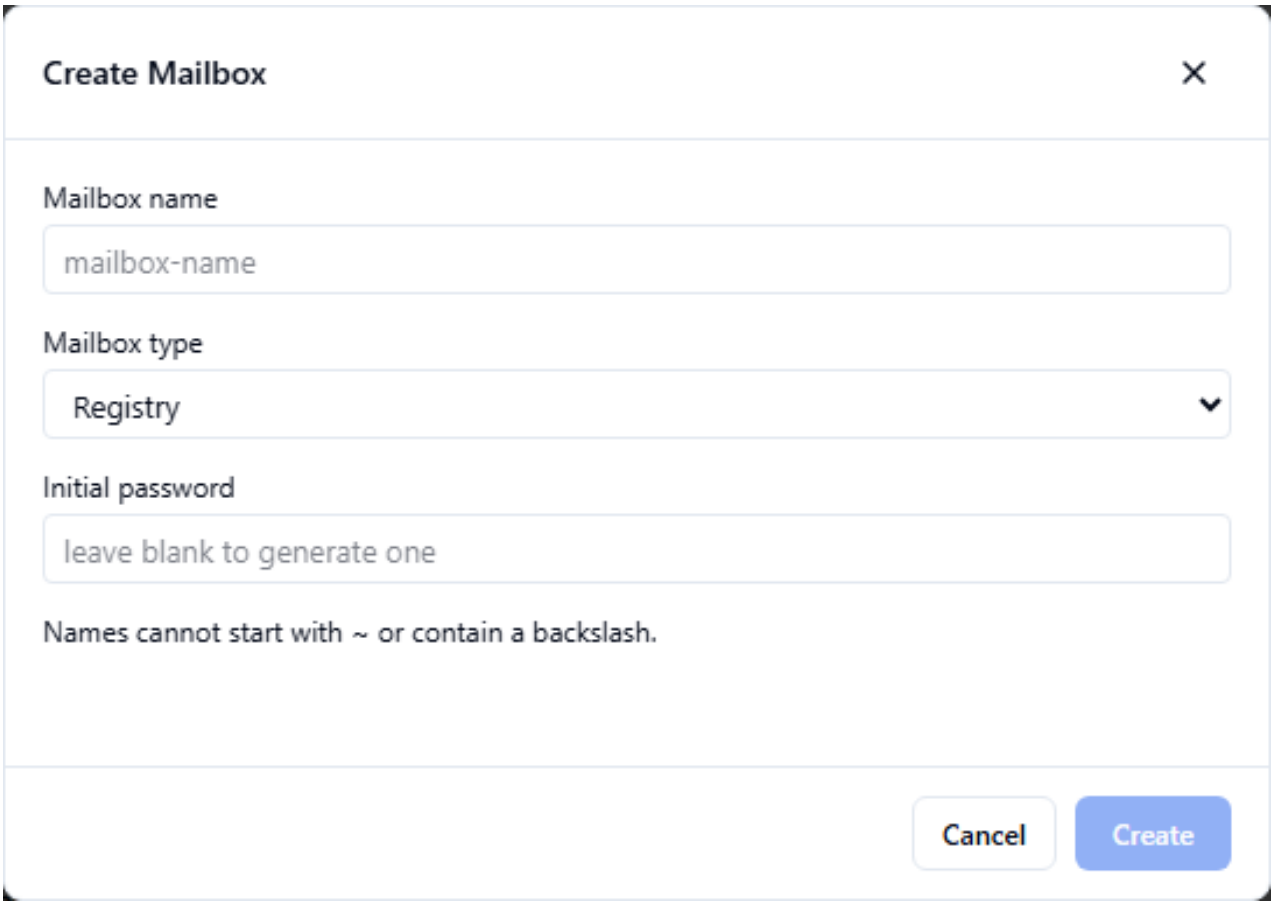

Figure 114 Add Registry Mailbox

Add NT Mailbox

Choose Create Mailbox and the Windows-backed type when available. The current dialog does not enumerate Windows users; the Windows account and required access must already exist.

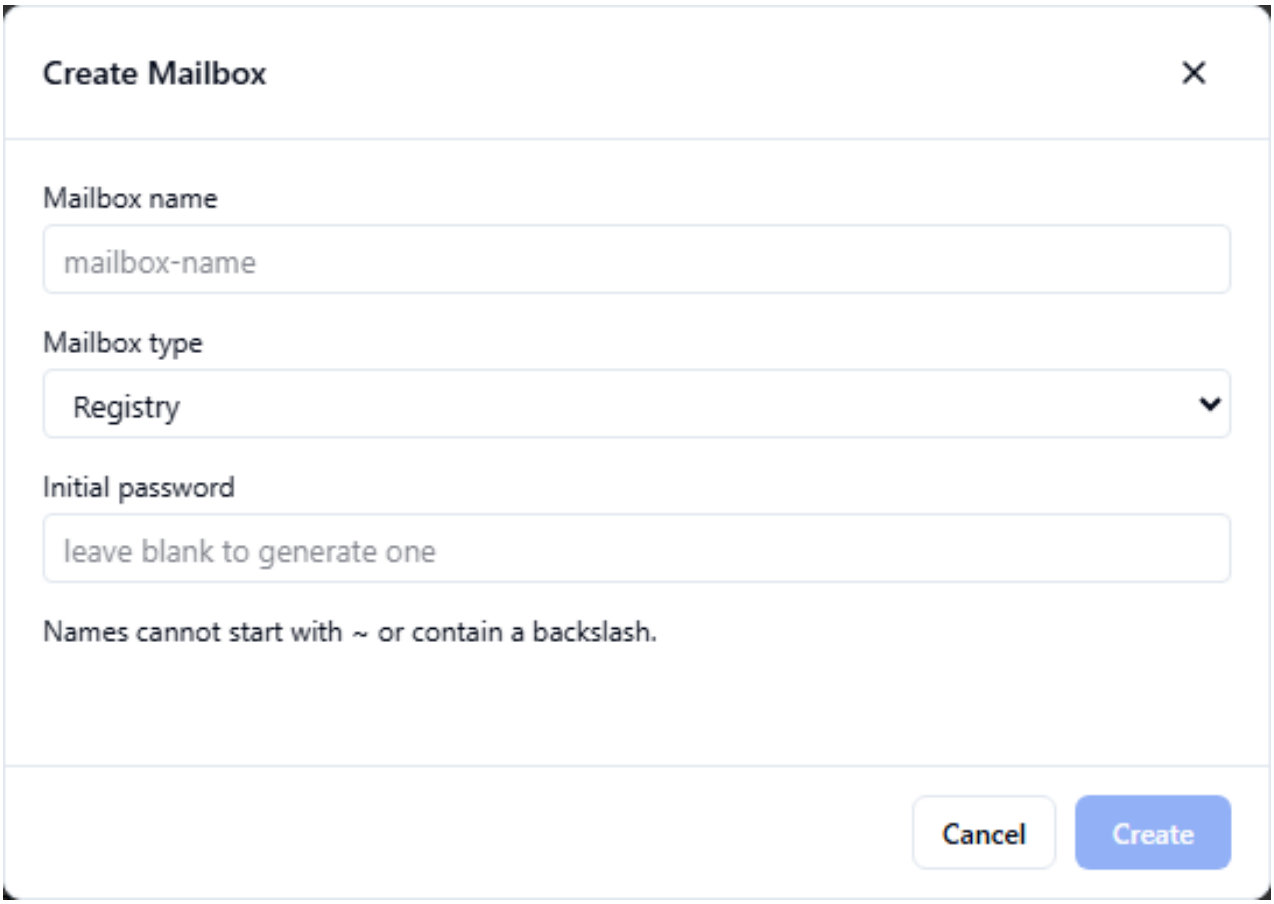

Figure 115 Add NT Mailbox

Add Database Mailbox

Use Server, External Database Mailboxes to preview the configured source and create selected eligible accounts. The old Add Database Mailbox user-picker is not the current workflow.

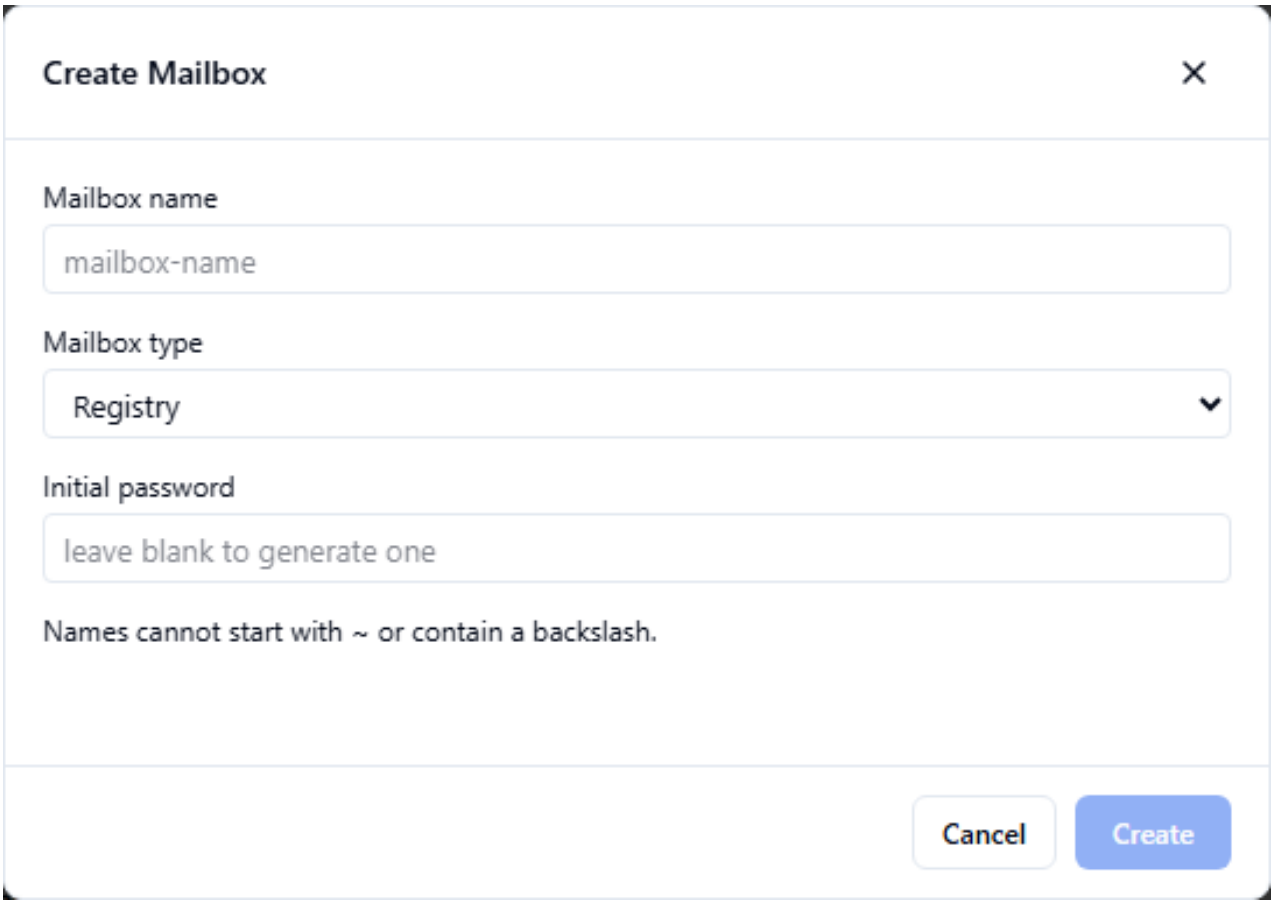

Figure 116 Add Database Mailbox

Add SQL Mailbox

With SQL configuration active, use Create Mailbox and the available native type. SQL configuration storage and an external user database are separate choices.

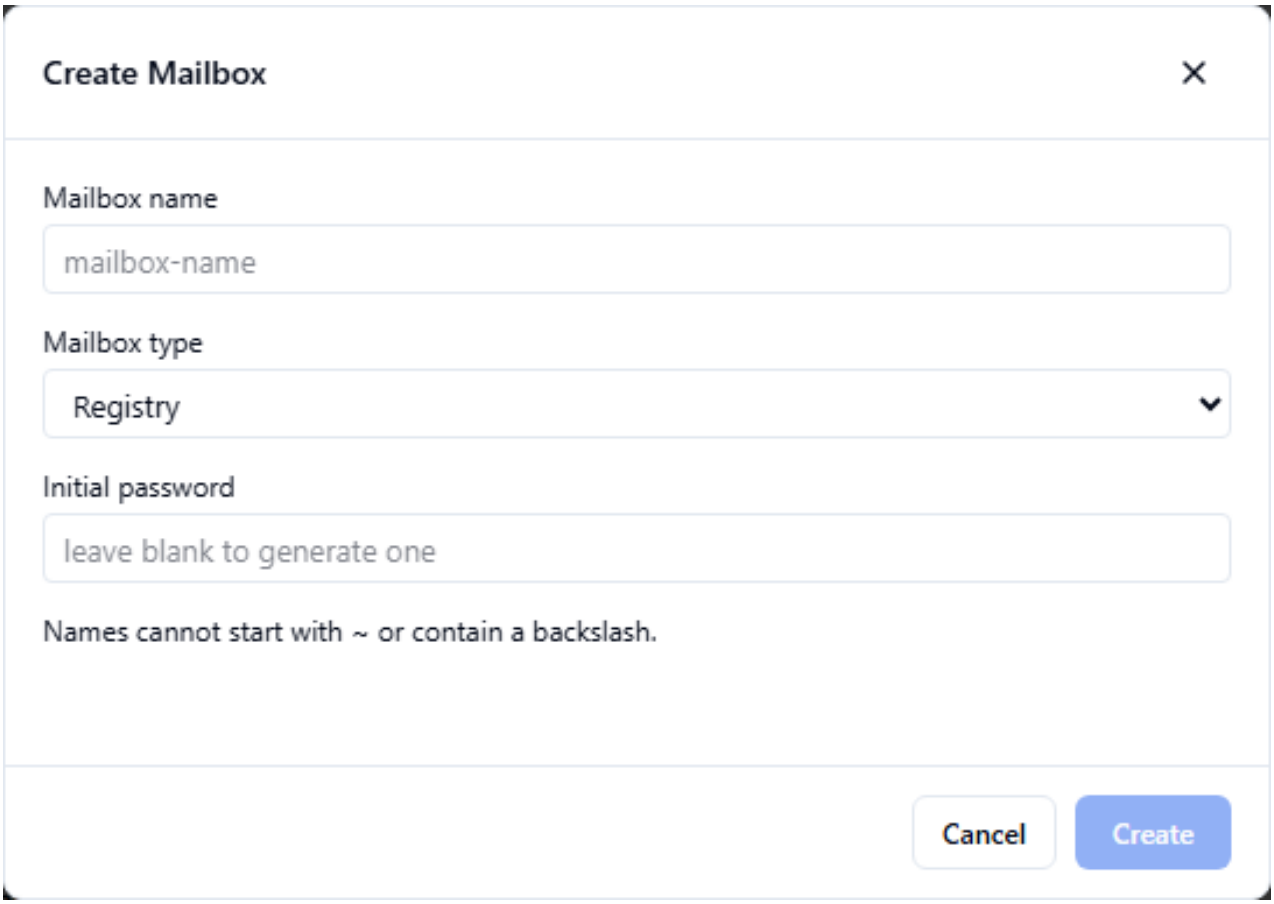

Figure 117 Add SQL Mailbox

Mailbox Names

You can use any of the following characters to name a mailbox:

- Alphanumeric (a-Z)
- Period (.)
- Hyphen (-)
- Underline (_)

The following characters are illegal in a mailbox name:

- Round Bracket (())
- Square Bracket ([])
- Angle Bracket (<>)
- At Symbol (@)
- Comma (,)
- Semi-colon (;)
- Colon (:)
- Slash (\)
- Quote (“)
- Space ( )
- Any Control Character

Renaming a Mailbox

You can rename a Registry or SQL mailbox by selecting the icon with a single click, then clicking once on the mailbox name. You cannot rename an NT Mailbox. Use the User Manager to manage local users instead.

Deleting a Mailbox

To delete a Mailbox, select the icon with a single click and then hit the Delete button.

Move or Copy Mailbox

Select a mailbox, choose Copy or Move, and select a different destination domain. Copy creates an account definition with settings; it does not copy messages, aliases or the mail directory. It is not a mailbox-content backup or migration command.

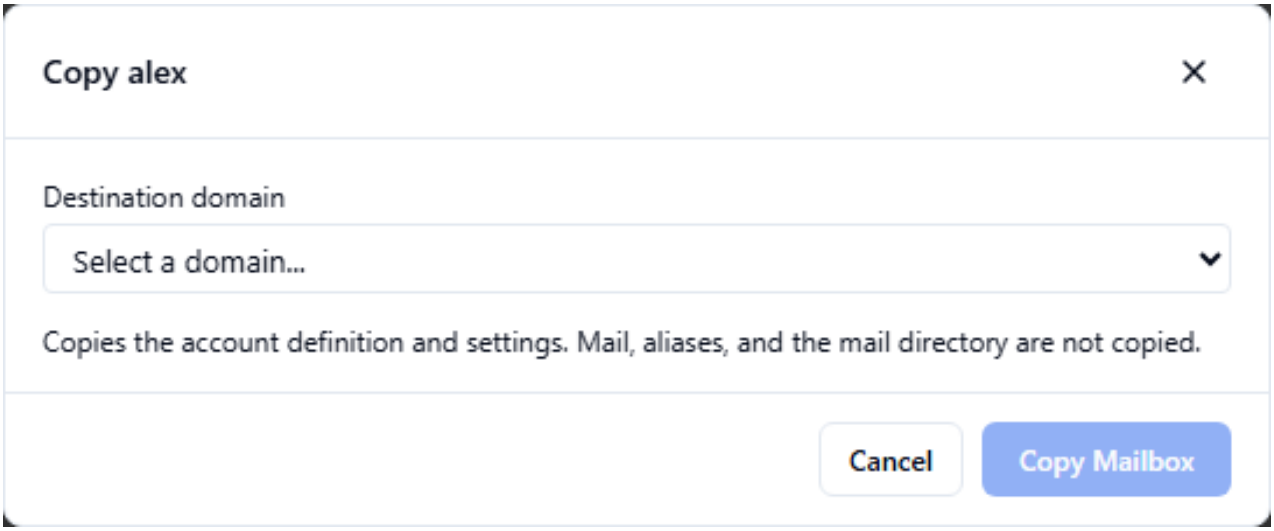

Figure 118 Copy account settings to another domain

Move changes the account's domain and keeps existing mail reachable by pinning the existing directory where needed. It does not relocate the physical directory. Aliases keep working, while existing sessions for the old address stop working. Verify client access and delivery after the move.

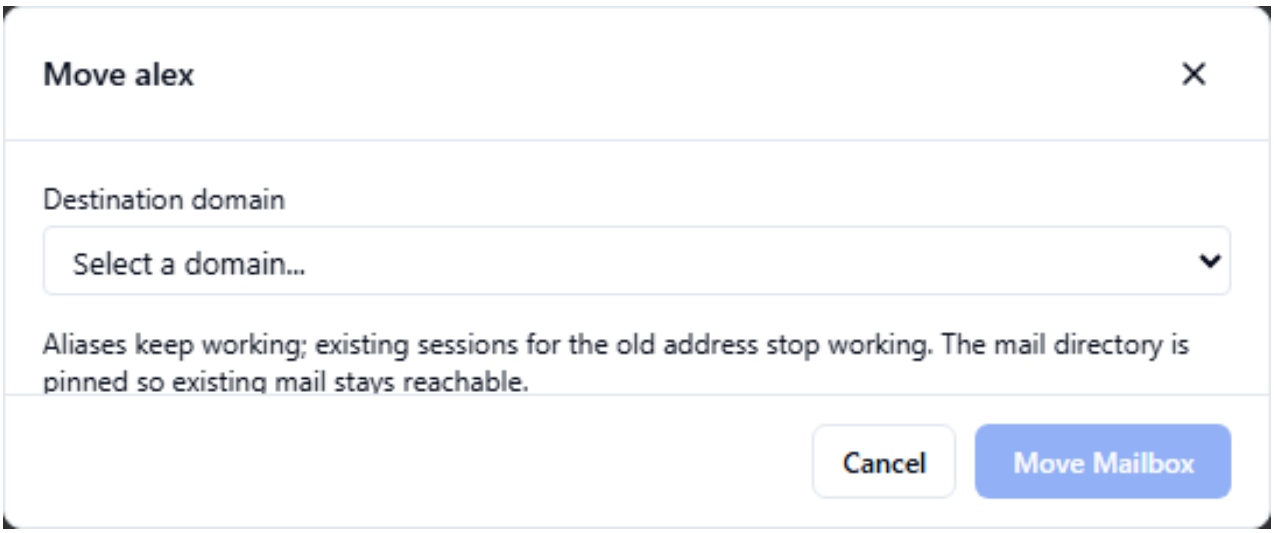

Figure 119 Move an account while retaining its mail directory

The v10 Move or Copy Directory option and its manual XCOPY fallback do not describe this operation.

Add NT User

The previous Console enumerated local and domain Windows accounts in a picker. That picker is not available in the current shared Console. Review the mailbox type and authentication requirements before creating an account; do not infer Windows account enumeration from the Create Mailbox type selector.

Add NT Group

The previous Console could select a Windows group for bulk account creation. The current shared Console does not expose that group picker. NT Mailbox plugin settings remain visible, but their presence alone does not verify group-based provisioning in this beta.

Create Database Mailboxes

Open Server, External Database Mailboxes. Save and validate the connection, choose a domain, then use Preview saved source and Create selected. The preview identifies existing accounts and collisions. Only server administrators may configure or run provisioning. This replaces the old database-user wizard; the SQL configuration connector is a separate feature.

Mailbox General Page

Use this form to set the general properties for this mailbox.

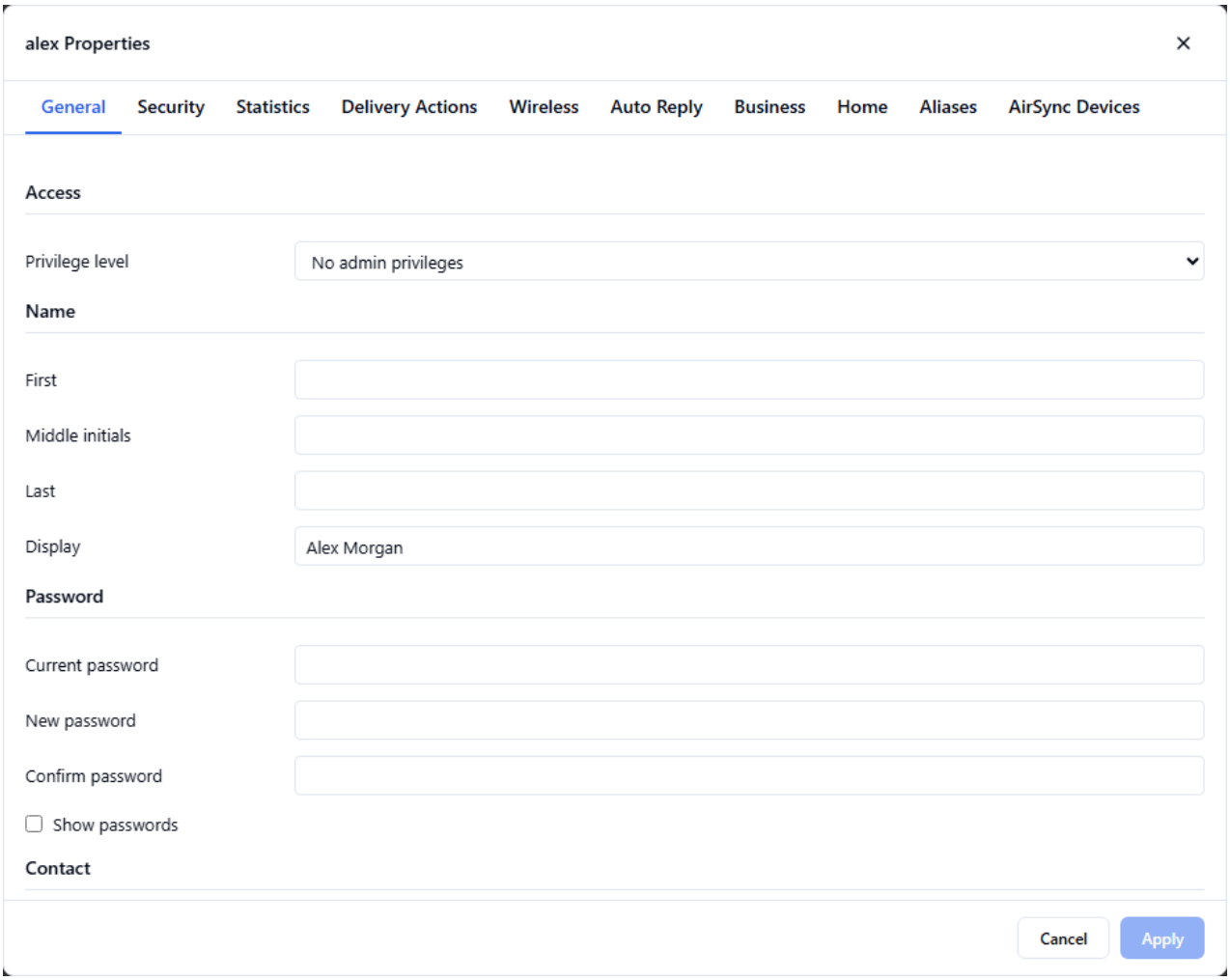

Figure 120 Mailbox General Page

First

Enter the first name of the person who will use this mailbox.

Middle Initials

Enter the middle initials of the person who will use this mailbox.

Last

Enter the last name of the person who will use this mailbox.

Display

Enter the full name of the person who will use this mailbox. This field will be filled in automatically if this is an NT or Database mailbox.

Password

Native account passwords are stored in the active configuration backend; database account changes use the external provider. For Windows-backed accounts, self-service changes require the current password and use Windows password-change policy. An administrator reset requires the MailSite service identity to have Windows reset permission. MailSite updates its cached password only after Windows accepts the change. If cache persistence then fails, the Windows password has already changed: use the new password and resolve the reported storage error. No elevation dialog is launched.

Confirm Password

Re-enter the same new password to confirm it. The old fourteen-character Windows NT restriction is not the current MailSite password rule; apply the requirements of the account provider and your organization.

Webmail Address

This is a retained webmail address property. Verify the sending identity offered by the current ExpressPro client; saving a contact address does not authorize arbitrary From addresses or create a mailbox alias.

Alternate Email

Enter the alternate contact address for this person. This contact property does not create an alias or forwarding rule. Use the explicit alias or delivery settings to change routing.

Web Site

Enter the web site of the person who will use this mailbox.

Privilege Level

The Privilege Level determines your administrative privilege on the server. The choices are None, Domain and Server. If set to None, the user will only be able to control his own mailbox. If set to Domain, the user can manage other mailboxes in that domain. If set to Server, the user may manage all mailboxes on that server. Refer to the section on Web Mailbox Administration for more information.

Services (Mailbox Level)

Indicates the services which this mailbox is entitled to use. If greyed out, access to the service is controlled by a setting at a higher level (server or domain).

Mailbox Statistics Page

The page shows a number of useful statistics about the mailbox.

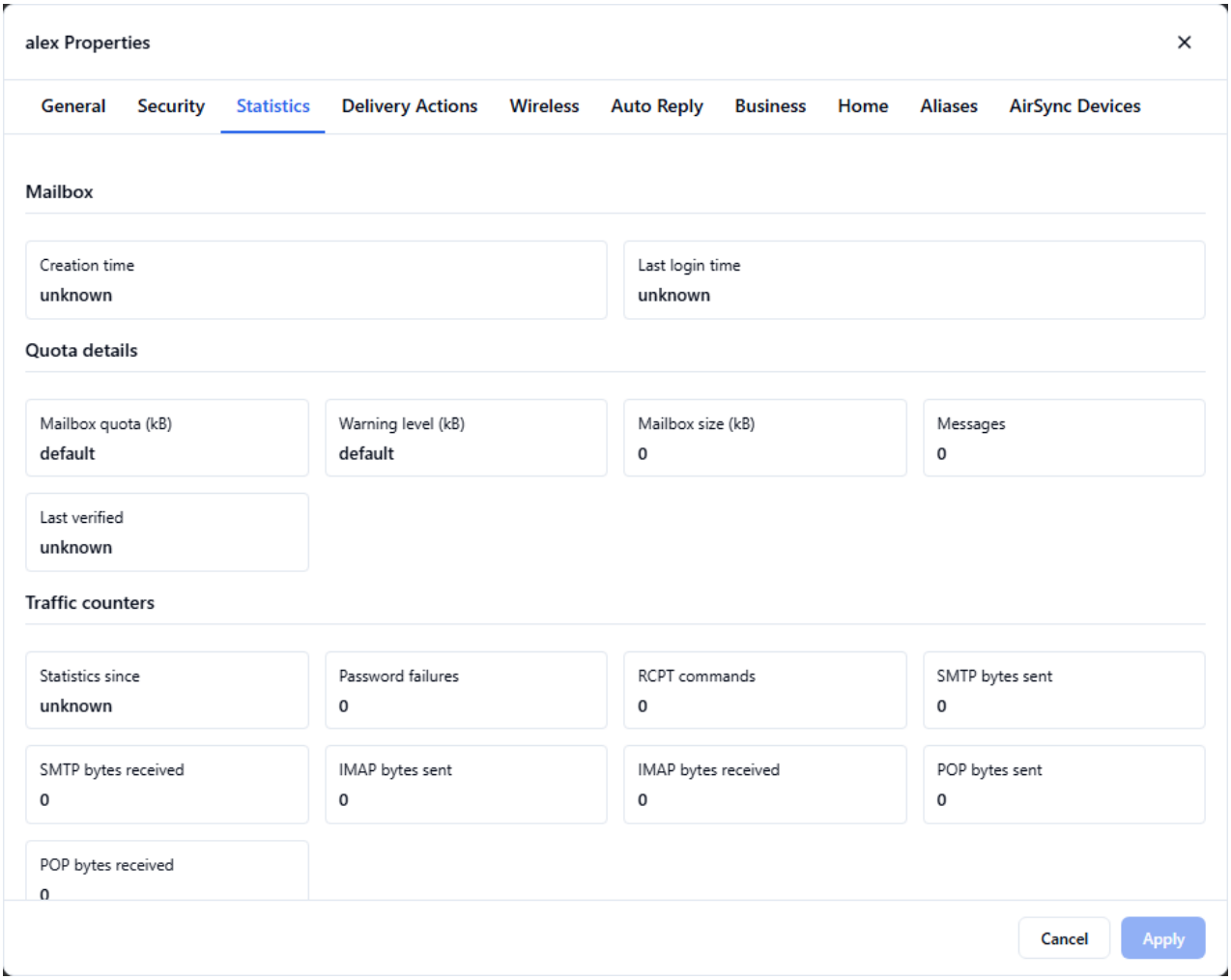

Figure 121 Mailbox Statistics Page

Quota Details

Quota levels can be set here using one of the values in the dropdown box, or your own value. Quota support must be enabled at server level before mailbox level checking becomes effective.

Traffic Statistics

A number of useful statistics are included to assist in management of mailboxes. SMTP data only includes authenticated SMTP sessions as non-authenticated sessions cannot definitively be linked to a specific mailbox. Collected data can be reset as needed.

Statistics gathering is enabled or disbled at server level.

Mailbox Delivery Actions Page

Use this form to configure actions related to the delivery of mail.

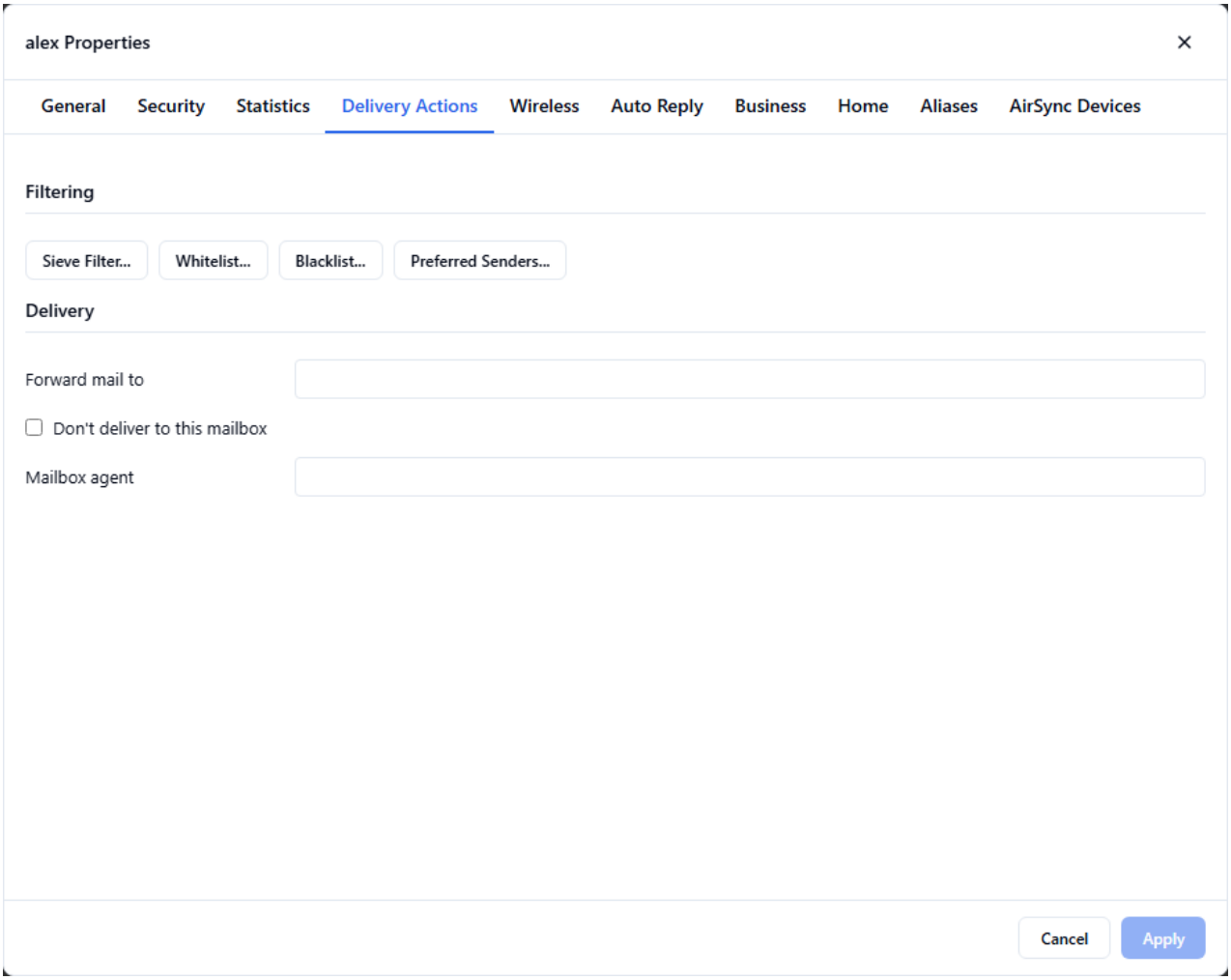

Figure 122 Mailbox Delivery Actions Page

Sieve Filter

Sieve filters are described in more detail in the Mail Filters section. Sieve filters can be used to take a large variety of powerful actions depending on the characteristics of the mail being delivered. For example, sieve filters can be configured to handle mails from whitelisted or blacklisted addresses correctly, or to send an SMS notification when a mail arrives from someone on the Preferred Senders List.

Enable spam scanning on all mail to this mailbox

Spam scanning can be enabled at server, domain or mailbox level. If it is only enabled for specific mailboxes, this checkbox indicates which mailboxes are protected.

Enable greylisting on all mail to this mailbox

Greylisting can be enabled at server, domain or mailbox level. If it is only enabled for specific mailboxes, this checkbox indicates which mailboxes are protected. Greylisting is only available for spam scanning enabled mailboxes.

Enable virus scanning on all mail to or from this mailbox

Virus scanning can be enabled at server, domain or mailbox level. If it is only enabled for specific mailboxes, this checkbox indicated which mailboxes are protected.

Mobile phone

Specify the mobile or cellular phone number for SMS alerts. As many cellular companies cover more than one country, numbers must be added with the country code (+1 for the USA/Canada, etc). Numbers are entered with no spaces.

Carrier

Choose the appropriate mobile/cellular carrier from the drop down list. The list is configurable at server level under Wireless Carriers.

Enable SMS Notifications

Administrators may wish to enable SMS notifications on a per mailbox basis. When this checkbox is enabled, the user will be able to receive SMS notifications providing appropriate sieve filters are set.

Enable BREW Wakeup

BREW Wakeup is a retained setting for the historical Eudora2Go integration. It is not the current ActiveSync mobile synchronization workflow. Leave it disabled unless maintaining a separately verified compatible integration.

Whitelist

Whitelists are supported at server, domain and mailbox levels. Whitelists contain addresses of senders or domains known to the user. When appropriate sieve filters are enabled, messages from whitelisted senders will typically bypass spam checking.

Blacklist

Blacklists are supported at server, domain and mailbox levels. Blacklists contain addresses of senders known to be spammers, or originators of unwanted mail for some other reason. When appropriate sieve filters are enabled, messages from blacklisted senders will typically be rejected.

Preferred Senders

The preferred senders list is designed to be used when creating SMS notifications. When someone is away from the office, they often only want to be notified of mails from a small set of important people – perhaps their manager or specific relatives or friends. When appropriate sieve filters are enabled, only messages from people on the preferred senders list will lead to an SMS notification being sent.

Forward Mail To

Enter an Internet mail address to which messages for this user will be forwarded. Leave empty to disable forwarding. You can enter a fully qualified Internet mail address, or if the destination address is in the default MailSite domain, you can enter just the mailbox name. You can auto-forward to multiple addresses by separating each address with a comma.

Don't Deliver to this Mailbox

Select this field to prevent any mail messages from being delivered to this mailbox. It is normally set only if the

Forward To or the Auto Reply feature is being used.

Mailbox Agent

This feature allows a command line to be executed when a message is delivered to the mailbox. You can specify any command that can be executed at the Windows command-line prompt, including built-in commands and batch files.

The following substitutions are performed in the command line you specify before it is executed:

Special symbols	Replaced by
%f	Full file name of the message which was received
%u	Name of the mailbox
%h	Mailbox directory
%d	Domain to which the mailbox belongs
%%	Single percent character

The message file %f will be located in the mailbox directory, but will not have a MSG extension. The command may change the contents of the message or may even delete the file. When the command completes, MailSite will automatically rename the file (if it still exists) to have a MSG extension so that it is available for access by the POP and IMAP servers.

For more information, see the section on Mailbox Agents.

Mailbox Wireless Page

Use this form to configure the wireless notification properties for this mailbox. All the items here are available on the Delivery Actions tab, and are therefore grouped together here for clarity. Any changes made on either tab will update the same properties.

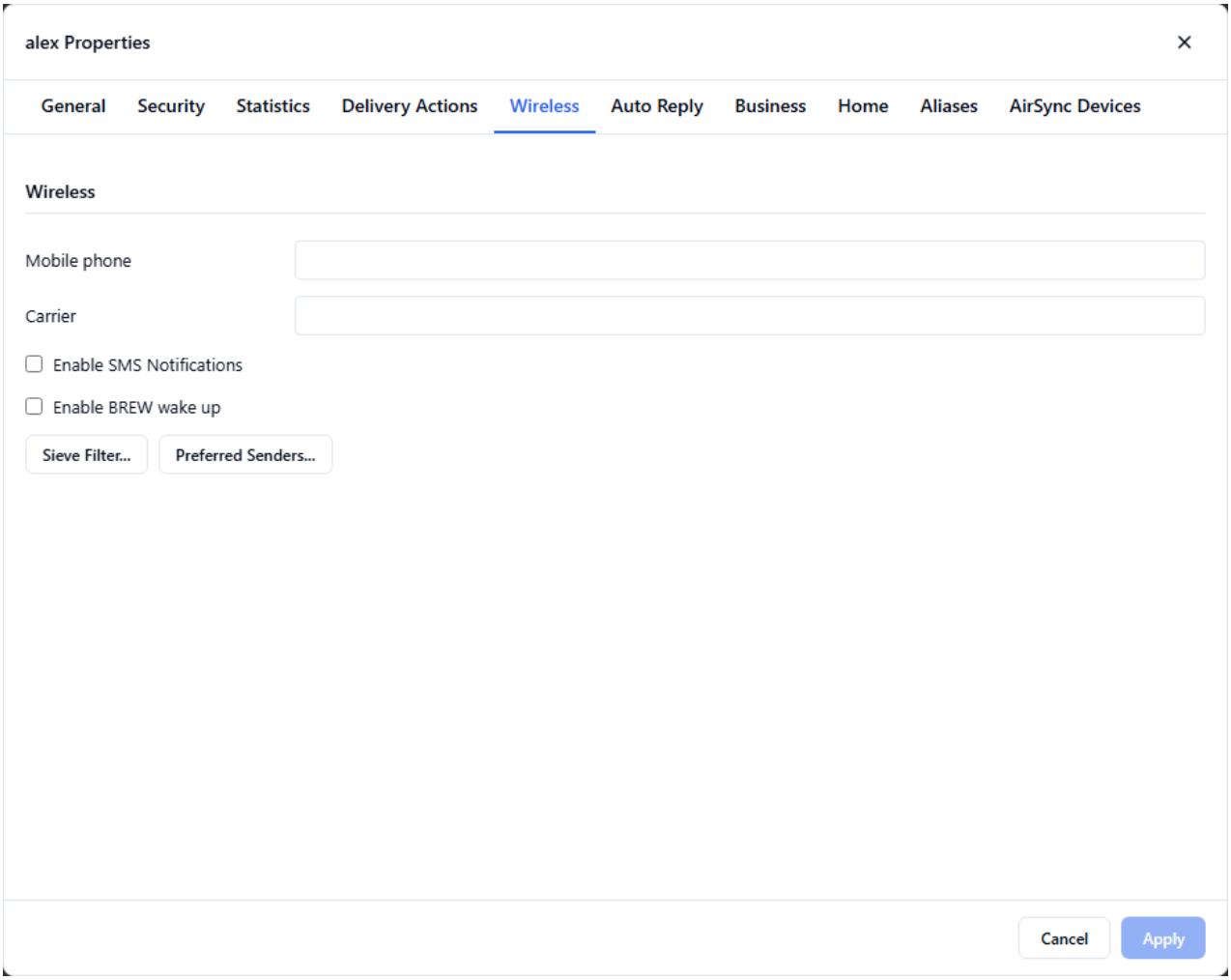

Figure 123 Mailbox Wireless Page

Mobile phone

Specify the mobile or cellular phone number for SMS alerts. As many cellular companies cover more than one country, numbers must be added with the country code (+1 for the USA/Canada, etc). Numbers are entered with no spaces.

Carrier

Choose the appropriate mobile/cellular carrier from the drop down list. The list is configurable at server level under Wireless Carriers.

Enable SMS Notifications

Administrators may wish to enable SMS notifications on a per mailbox basis. When this checkbox is enabled, the user will be able to receive SMS notifications providing appropriate sieve filters are set.

Enable BREW Wakeup

BREW Wakeup is a retained setting for the historical Eudora2Go integration. It is not the current ActiveSync mobile synchronization workflow. Leave it disabled unless maintaining a separately verified compatible integration.

Sieve Filter

Sieve filters are described in more detail in the Mail Filters section. Sieve filters can be used to take a large variety of powerful actions depending on the characteristics of the mail being delivered. For example, sieve filters can be configured to handle mails from whitelisted or blacklisted addresses correctly, or to send an SMS notification when a mail arrives from someon on the Preferred Senders List.

Preferred Senders

The preferred senders list is designed to be used when creating SMS notifications. When someone is away from the office, they often only want to be notified of mails from a small set of important people – perhaps their manager or specific relatives or friends. When appropriate sieve filters are enabled, only messages from people on the preferred senders list will lead to an SMS notification being sent.

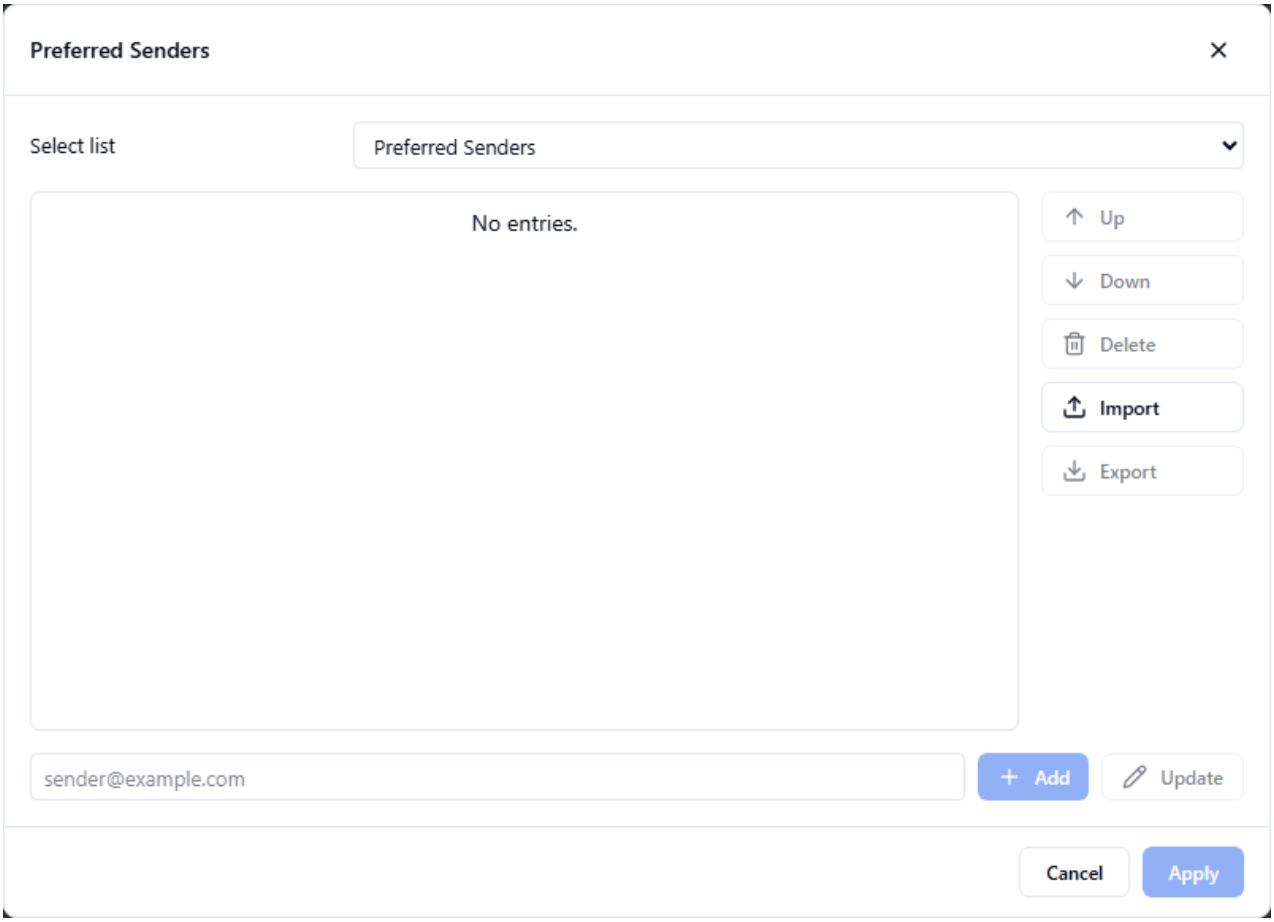

Figure 124 Preferred Senders

Addresses can be added to, and removed from the list as needed. Large lists can be exported to a comma separated file, modified in another program, and then imported back to MailSite.

Mailbox AutoReply Page

Use this form to configure the auto-reply properties for this mailbox.

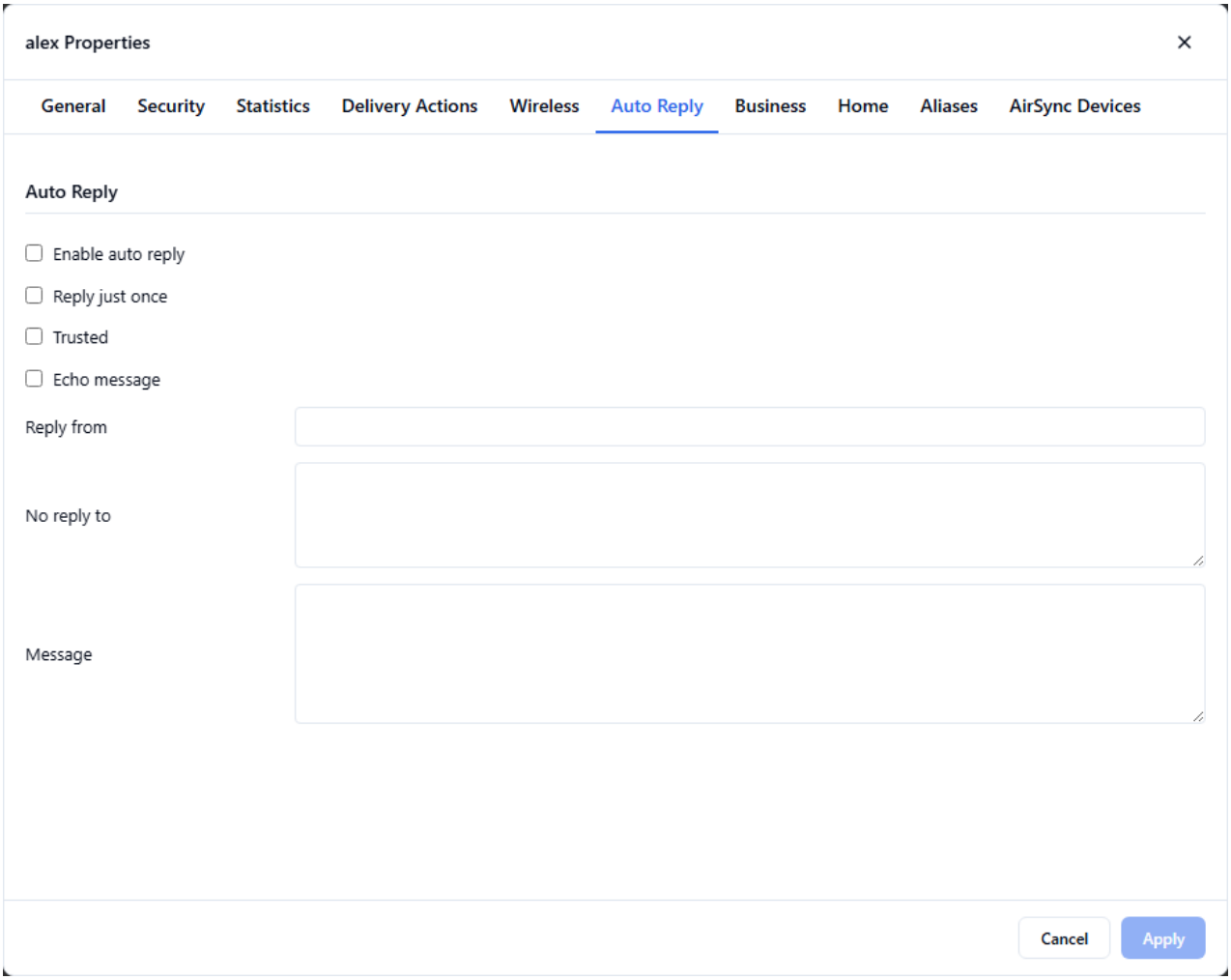

Figure 125 Mailbox AutoReply Page

Enable Auto Reply

Select this field to enable the auto reply feature for this mailbox. Auto Reply causes MailSite to automatically generate a reply message to the sender when an incoming e-mail arrives for this mailbox.

Reply Just Once

Reply Just Once records reply targets in AlreadyRepliedTo and suppresses repeated replies while they remain recorded. A positive server AlreadyRepliedToMax bounds this list by retaining the newest entries; it is not a fixed 10,000-entry limit. Verify the reset behavior when changing the automatic reply.

Trusted

This field controls the behavior of certain directives in the message. Select this field to permit the message to include file directives that access the file system outside of the local mailbox directory.

Echo Message

Select this field to return the original message with all auto-reply messages.

Reply From

Enter an e-mail address that MailSite will use as the From: address when creating auto-reply messages.

No Reply To

Enter list of e-mail addresses (one per line) to which auto reply messages will not be sent. Press Return to enter multiple lines. If a message is received which is addressed or copied to one of these addresses, then no automatic reply will be sent. You would typically include addresses of mail lists in

here, since automatic replies to mail list messages are antisocial. Note that MailSite will never send an auto reply to an address like owner-listname or like lisname-request, for the same reason.

Message

Enter the text of the auto reply message. Press Return to enter multiple lines. You may include auto reply directives to include files and special fields in your reply message.

Auto Reply Directives

The automatic reply message for a mailbox may contain directives that are replaced by other text when the auto-reply message is actually sent. The full list of directives follows:

Directive	Replacement text
%ADDRESS	The e-mail address of the person who sent the original message
%DATE	The current date
%TIME	The current time
%INCLUDE(filename)	The contents of the filename (which must be located in the mailbox's INBOX directory, unless the mailbox is trusted)
%EXECUTE(commandline)	The output produced by executing the commandline (trusted mailboxes only)
%%	A single percent character

If you want to put a large amount of text into your message, use the %INCLUDE directive, rather than typing text into the message field. This will save space in the Registry. The operation of the %INCLUDE directive depends on the mailbox's Trusted setting. If the mailbox is trusted, then the filename should be the full path to a file that is accessible to the mail server. If the mailbox is not trusted, only files located in the mailbox's INBOX directory can be included—in this case, specify the filename as a relative path and not the full path.

The %EXECUTE directive only works for trusted mailboxes. The commandline parameter can specify any command or batch file.

Mailbox Business Page

Use this form to set the mailbox business contact fields. The old LDAP3A service is not part of the current installed service set; use the supported address-book clients and endpoints.

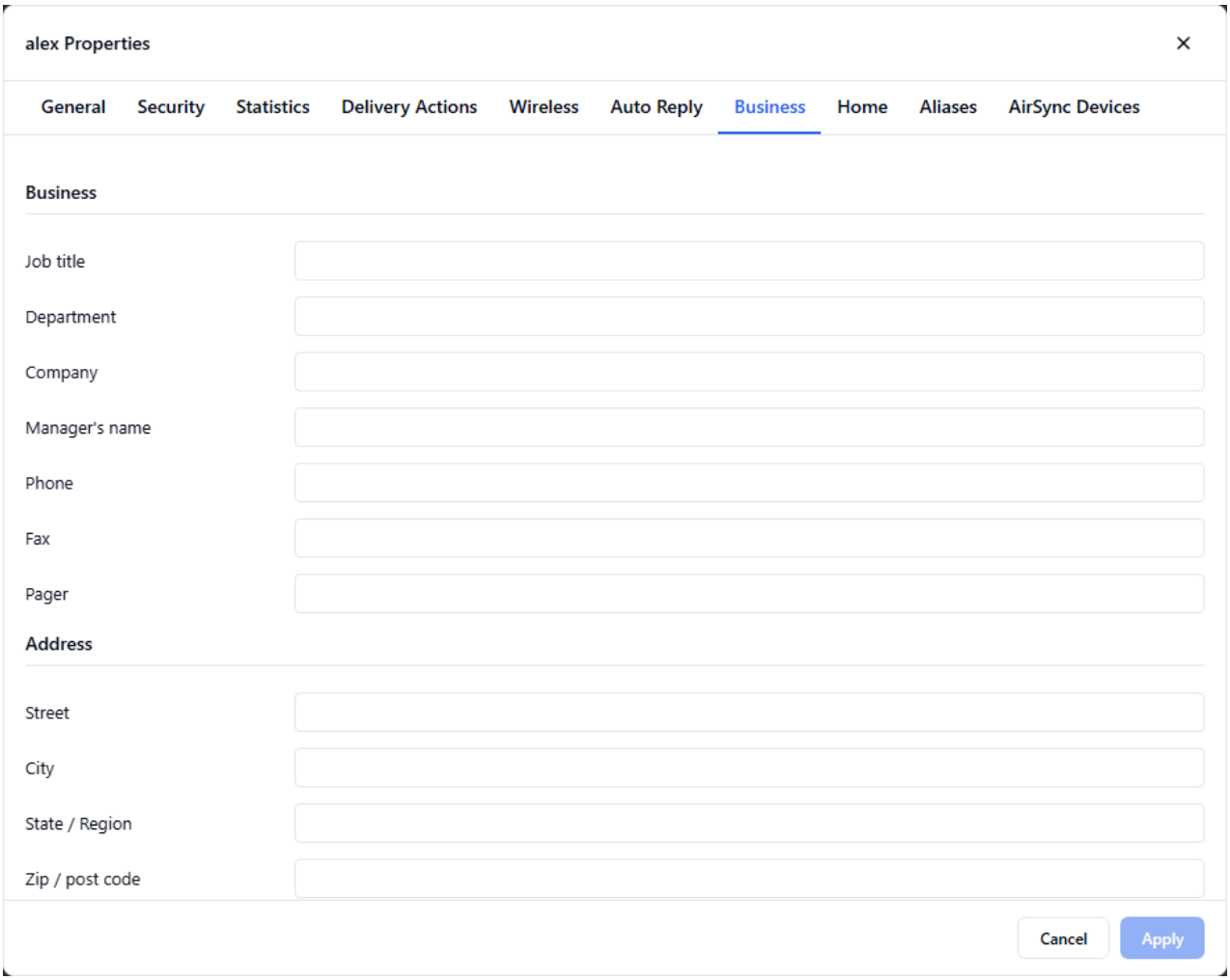

Figure 126 Mailbox Business Page

Job Title

Enter the job title of the person who will use this mailbox.

Department

Enter the department of the person who will use this mailbox.

Company

Enter the company of the person who will use this mailbox.

Manager's Name

Enter the name of the manager of the person who will use this mailbox.

Phone

Enter the business phone number of the person who will use this mailbox.

Fax

Enter the business fax number of the person who will use this mailbox.

Pager

Enter the pager number of the person who will use this mailbox.

Street

Enter the business street address of the person who will use this mailbox.

City

Enter the business city address of the person who will use this mailbox.

State/Region

Enter the business state address or region of the person who will use this mailbox.

Zip/Post Code

Enter the business zip or post code address of the person who will use this mailbox.

Country

Enter the business country address of the person who will use this mailbox.

Mailbox Postal Address

Use this form to set the postal address for this mailbox.

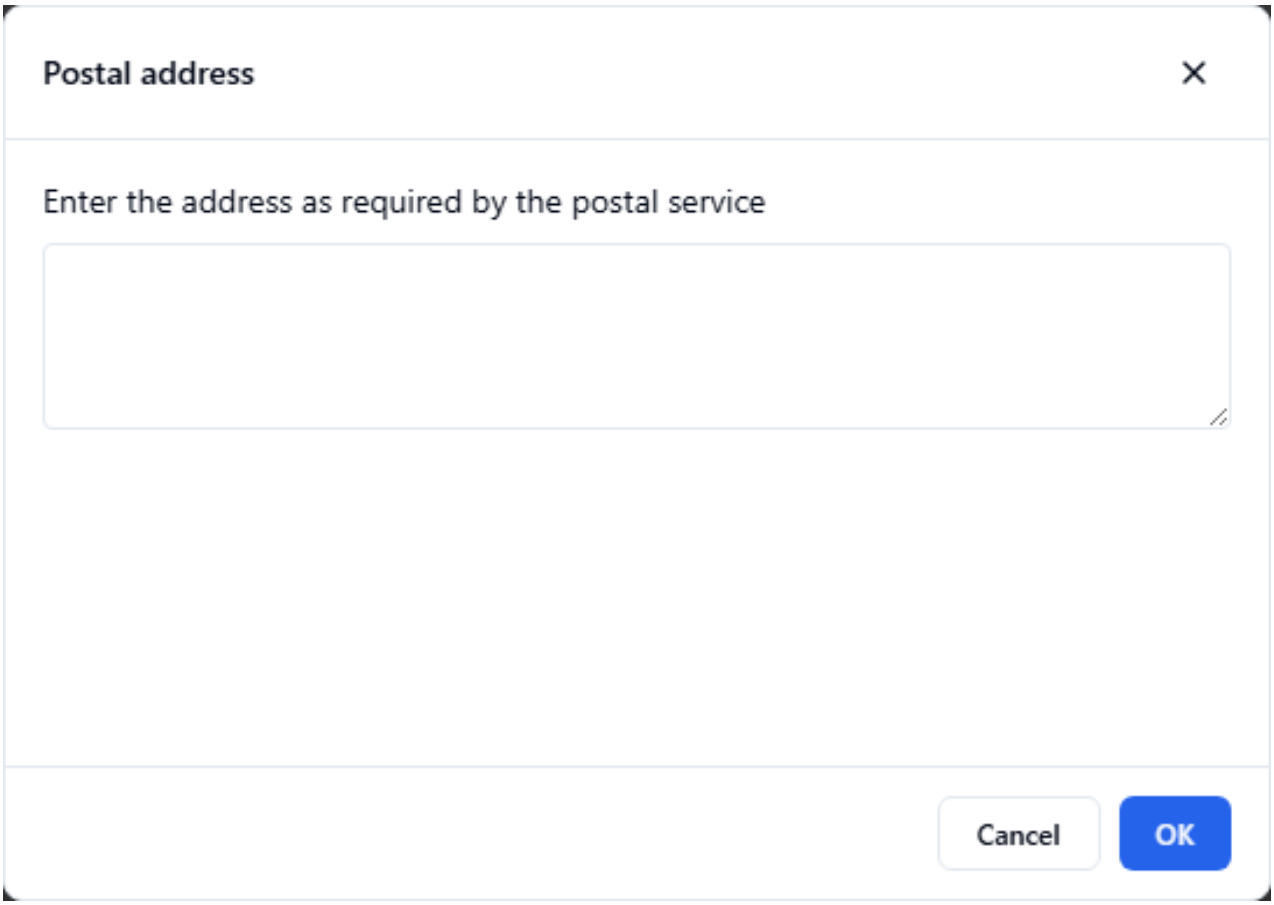

Figure 127 Mailbox Postal Address

Use this form if the mailbox user's address does not conform to the standard structure of the Business or Personal page. Hold the Ctrl key and press Return to enter multiple lines.

Mailbox Home Page

Use this form to set the home address for this mailbox.

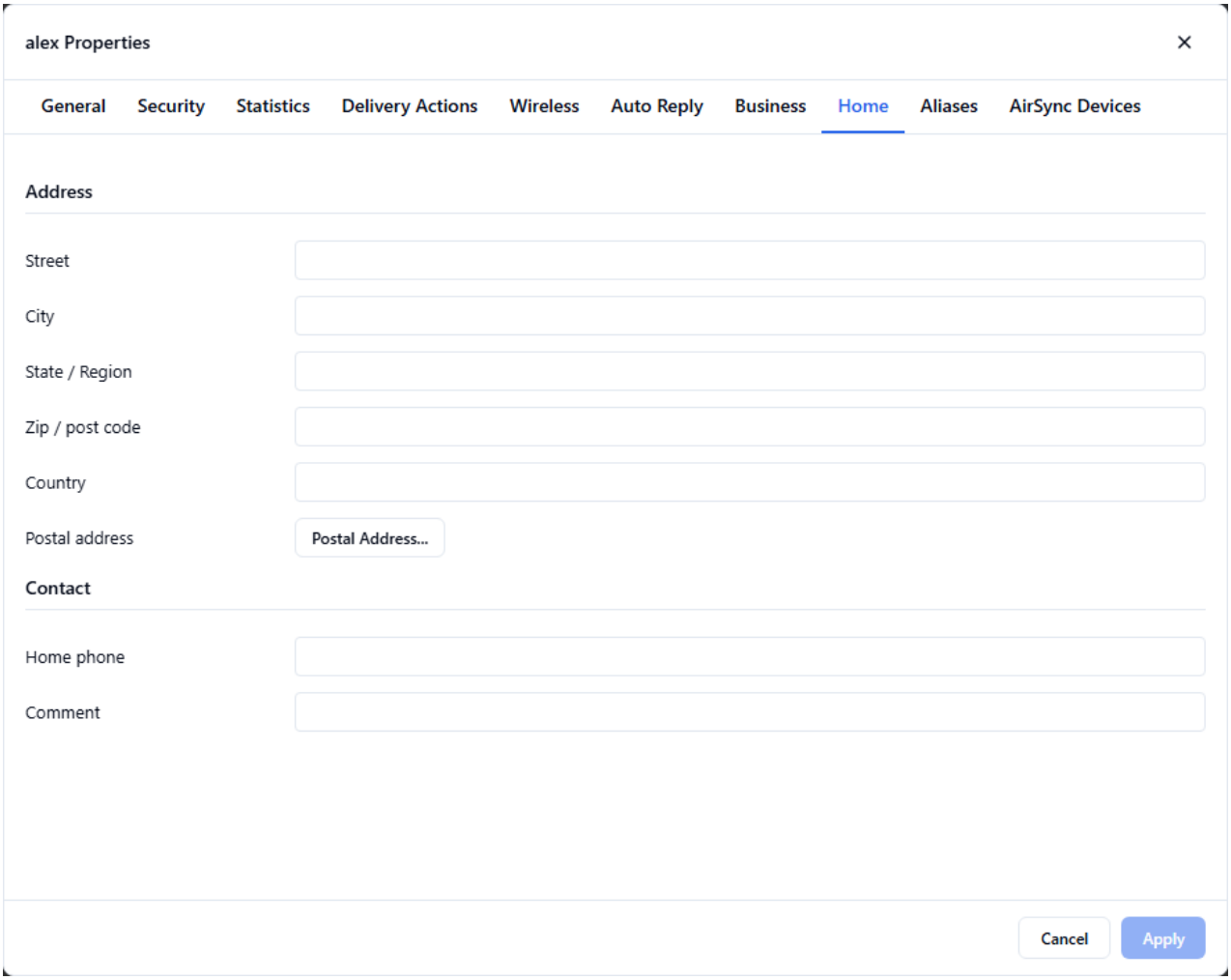

Figure 128 Mailbox Home Page

Street

Enter the home street address of the person who will use this mailbox.

City

Enter the home city address of the person who will use this mailbox.

State/Region

Enter the home state address or region of the person who will use this mailbox.

Zip/Post Code

Enter the home zip or post code address of the person who will use this mailbox.

Country

Enter the home country address of the person who will use this mailbox.

Home Phone

Enter the home phone number of the person who will use this mailbox.

Comment

Enter notes or comments for the person who will use this mailbox.

Mailbox Aliases Page (SQL Mailboxes)

Use this page to manage aliases for SQL mailboxes:

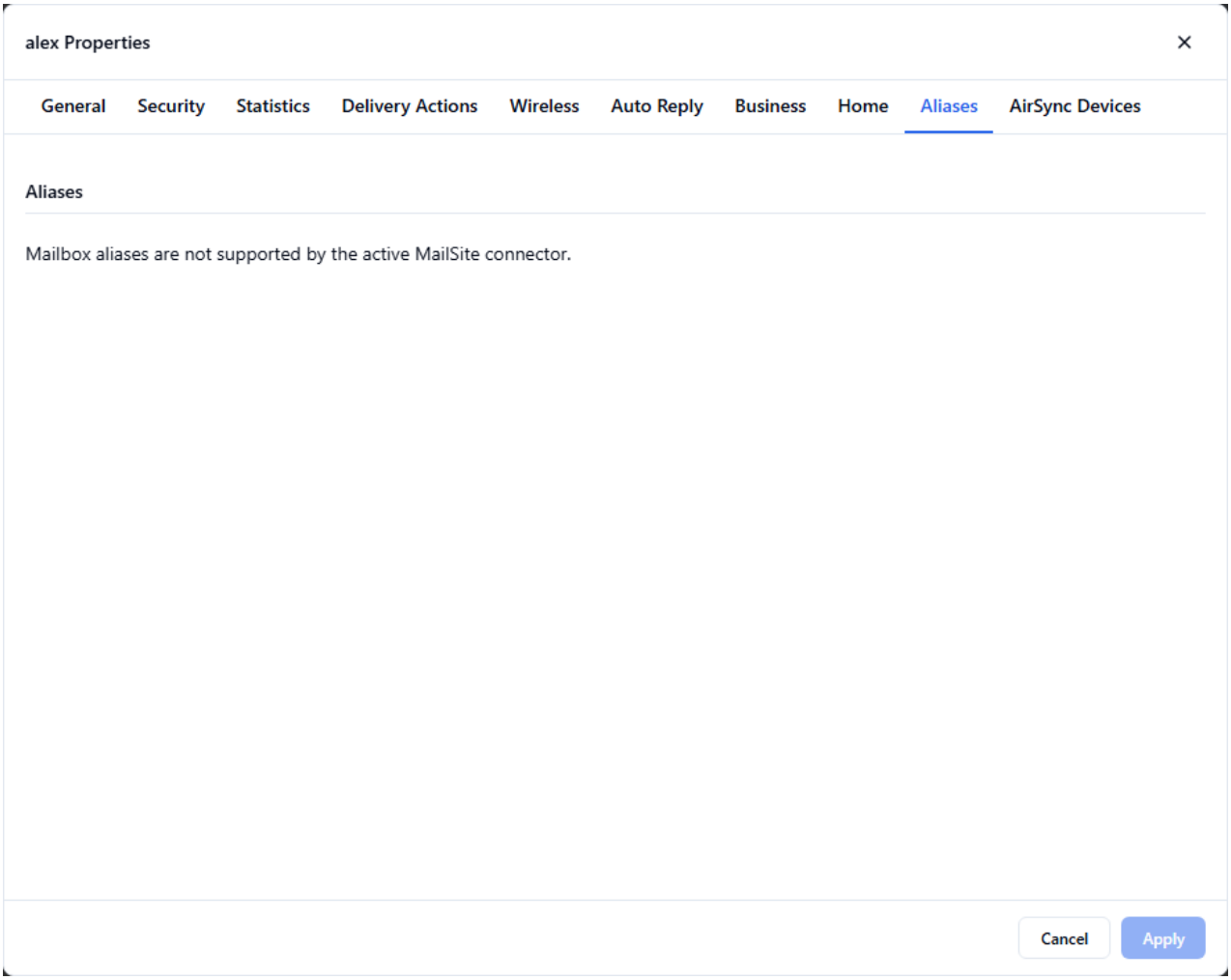

Figure 129 Mailbox Aliases Page (SQL Mailboxes)

To manage mailbox-level aliases, click the appropriate button.

When entering a new alias you must include a local domain. If you enter an alias with no domain, the alias is assumed to belong to the default MailSite domain.

Mail Lists

Select a domain's Mail Lists node, then create, rename, delete or open a list. The creation dialog selects the member source. General, Messages, Security, Digest, Members, Header Script and Pending messages provide the current management workflow. Provider-specific tabs are available for the selected source; configuring external paths, database credentials or source masks requires server-administrator access.

List general page

General controls the list's size limit, disabled state, sender permissions, moderator addresses, bounce handling, reply behavior and sender confirmation. Reply-To has three modes: keep the original, supply the list only when absent, or always use the list. It is one selector; the old separate Force checkbox is not a separate setting.

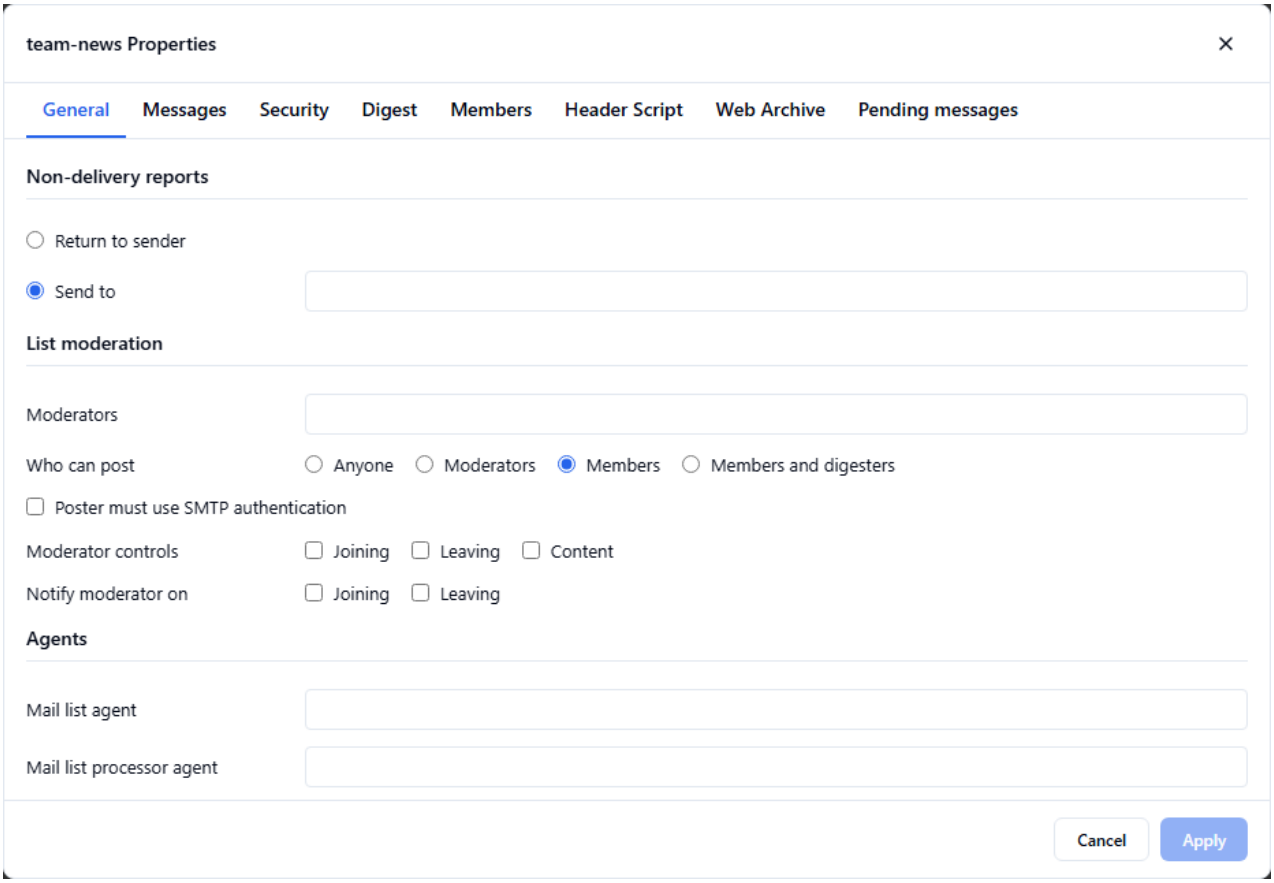

Figure 130 List general properties

Who can send can allow anyone, members, moderators, or members and digest subscribers. Moderator addresses are permitted under the restricted modes. The secure submission check uses the SMTP return path instead of the From header when enabled; server receiving/authentication policy remains a separate control.

The Sender header, message From address and envelope return path have different purposes. Alternate Sender affects the list Sender header. Bounce policy chooses the return path used for delivery failures. Sender confirmation replaces the author's ordinary member copy with a wrapped confirmation; an empty list creates no subscriber messages.

Maximum recipients limits recipient batches, not the total membership. A zero value does not impose a per-batch limit. Check the selected source and queue results when a large list is delayed.

List messages page

Messages contains the text and directives for help, welcome/farewell replies and message prefixes/suffixes. Prefix/suffix changes apply only to supported plain-text encodings. Multipart, HTML and base64 bodies retain their original content. INCLUDE and EXECUTE are not available in the current list path.

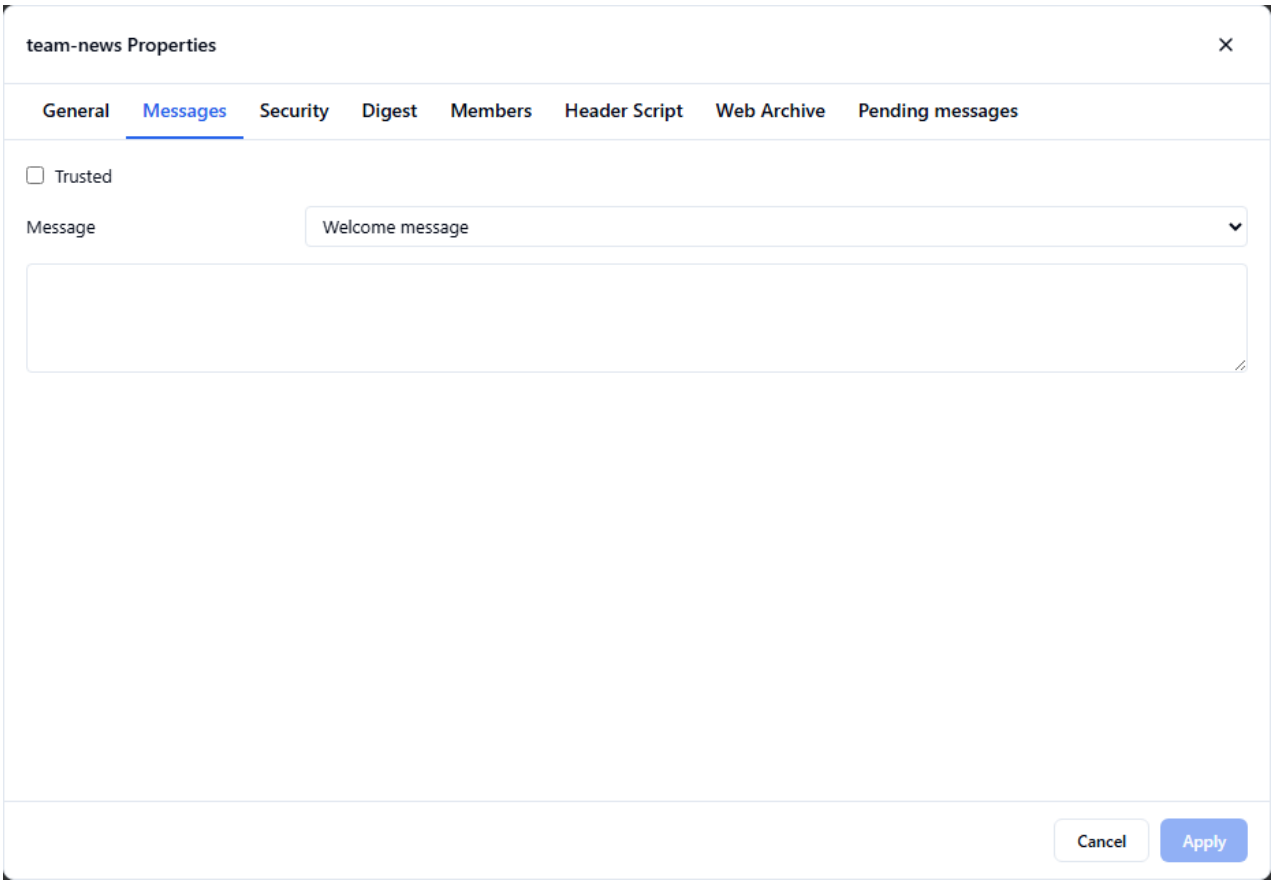

Figure 131 List messages

List security page

Security controls REVIEW and extended JOIN/LEAVE command permissions and ignored-address masks. Moderator addresses and moderation of content or membership changes are configured on General. Content moderation holds the original message for administrator review. A moderator email address alone does not grant Console administration privileges.

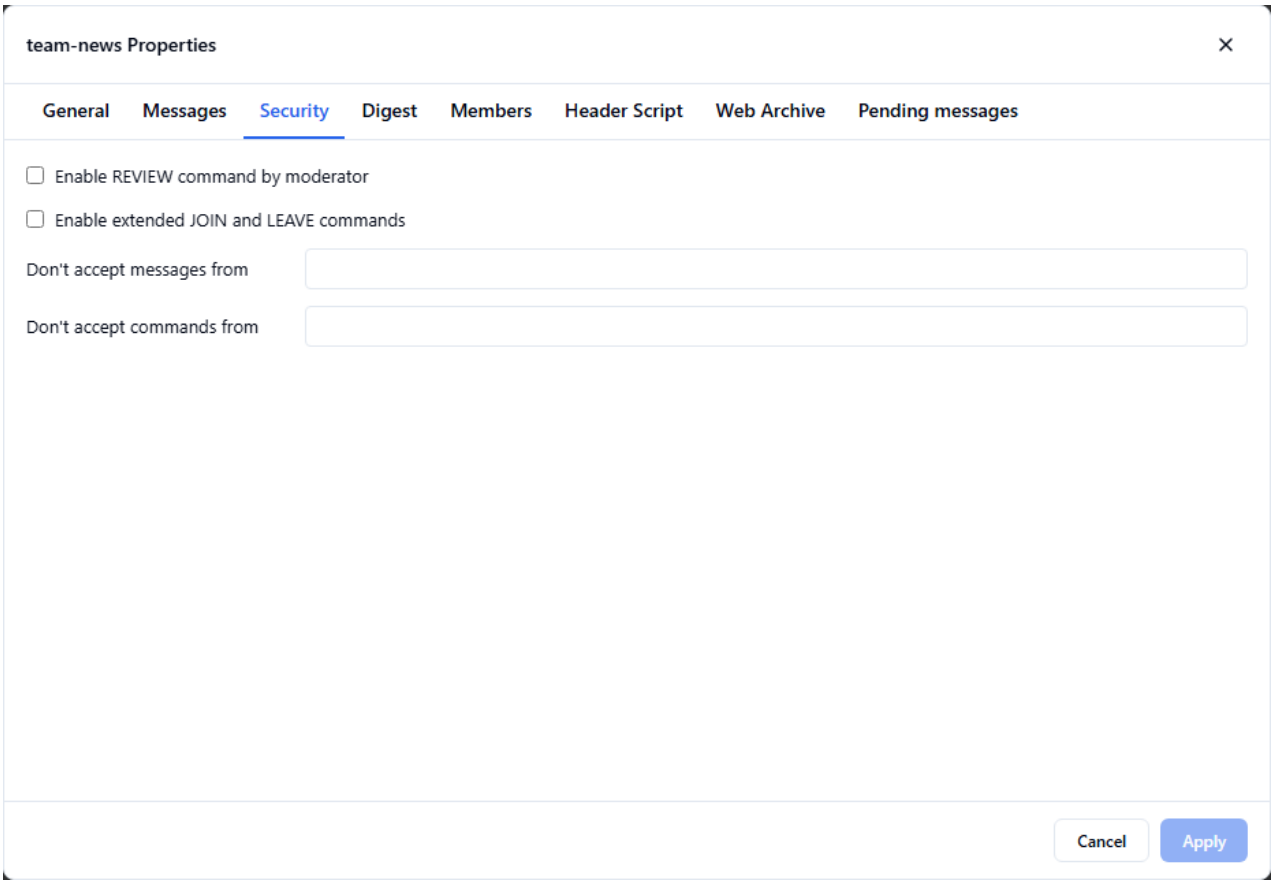

Figure 132 List security

Mailing-list delivery and moderation

Open Console, expand the domain, select Mail Lists, and create or open a list. Add native members on the Members tab, or configure a supported external source. Set Who can send, maximum message size, moderators and bounce handling before enabling the list.

On General, Reply-To header has three choices: keep the original, use the list only when Reply-To is absent, or always use the list. Sender and bounce-envelope settings are separate. A sender confirmation excludes that author from the ordinary subscriber copy and returns a wrapped confirmation instead.

Accepted posts go to eligible local and remote subscribers through the normal mail queue. Repeated addresses are deduplicated within a list. Nested lists retain loop markers; a person reached through two different lists can still receive two copies. An empty list produces no subscriber mail. Temporary delivery failures stay queued for retry.

For moderated content, configure a moderator address and enable Content under Moderator controls on General. A domain or server administrator opens Pending messages, downloads the original for review, and selects Approve or Reject. Approval queues delivery; rejection removes the post without a reply to its author. Receiving a moderator notification does not itself grant Console access.

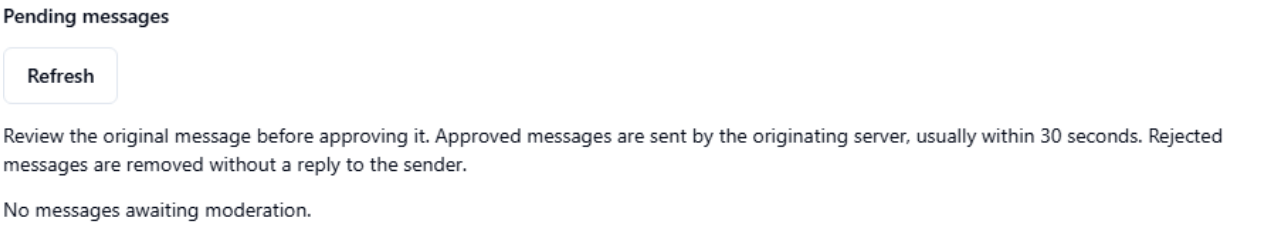

Figure 133 Mailing-list moderation review

Digest subscribers and list migration

Create a companion list whose name ends in -digest, such as team-news-digest, and put digest subscribers there. Posts to team-news are accumulated for the companion list as well as distributed to ordinary members. Direct posts to the -digest address are rejected.

On the companion list's Digest tab, select a frequency, subject template and whether to include a table of contents. Hour/day/month values use quantity followed by unit, such as 1H or 1D. Periodic delivery uses UTC period boundaries; the one-minute option uses 0H. An empty frequency disables timed emission; a configured size threshold can still trigger a digest. Digest settings do not enable content moderation.

The originating transport node emits approved messages and digests in the background. Normal restarts retain pending work and completed-delivery evidence. Restart with the same machine identity and spool location; automatic takeover by another node is not supported. Disabling a list pauses its pending delivery.

New held source messages are limited to 32 MiB. Queue and digest batches are bounded. Inspect the server log when a configured list does not drain; a failed list does not prevent other lists from being processed.

Before migration, drain old pending posts and digests. Review custom header/body scripts. Header ADD, REMOVE, REWRITE, conditions, bounded jumps and ABORT are supported. Arbitrary process execution and the legacy INCLUDE/EXECUTE body directives are not supported; replace those customizations before enabling the list.

List members page

Members displays resolved addresses. Native lists can be edited in the current Console. Text-file changes require write permission to the source; database changes require configured join/leave statements. Windows-group and server-mailbox sources are read-only here. Display names in external sources remain source-managed.

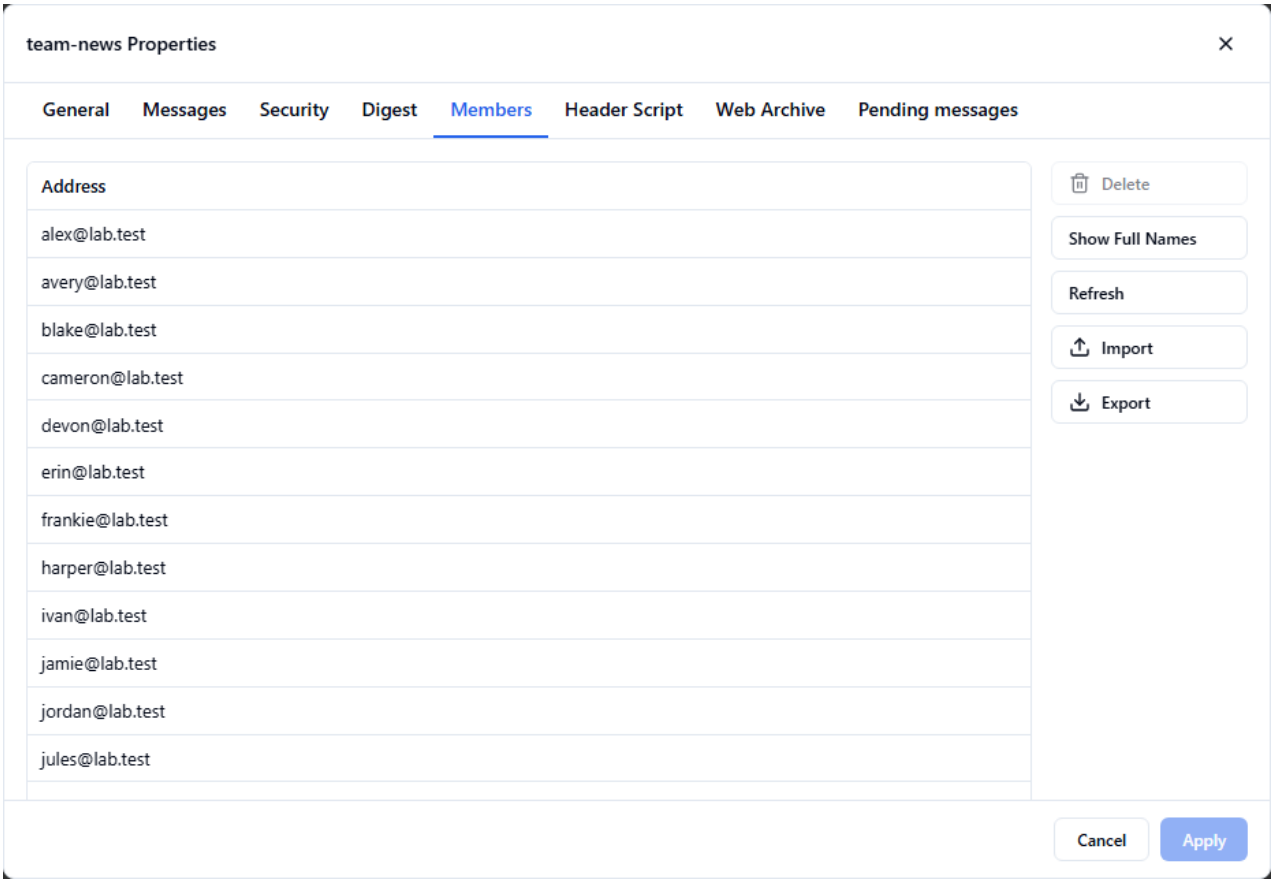

Figure 134 Current list membership

List header script page

Header Script changes headers before distribution. Supported commands and bounded control flow are described in Appendix C. Save a script only after checking it with representative mail; a script error delays processing instead of dropping the original.

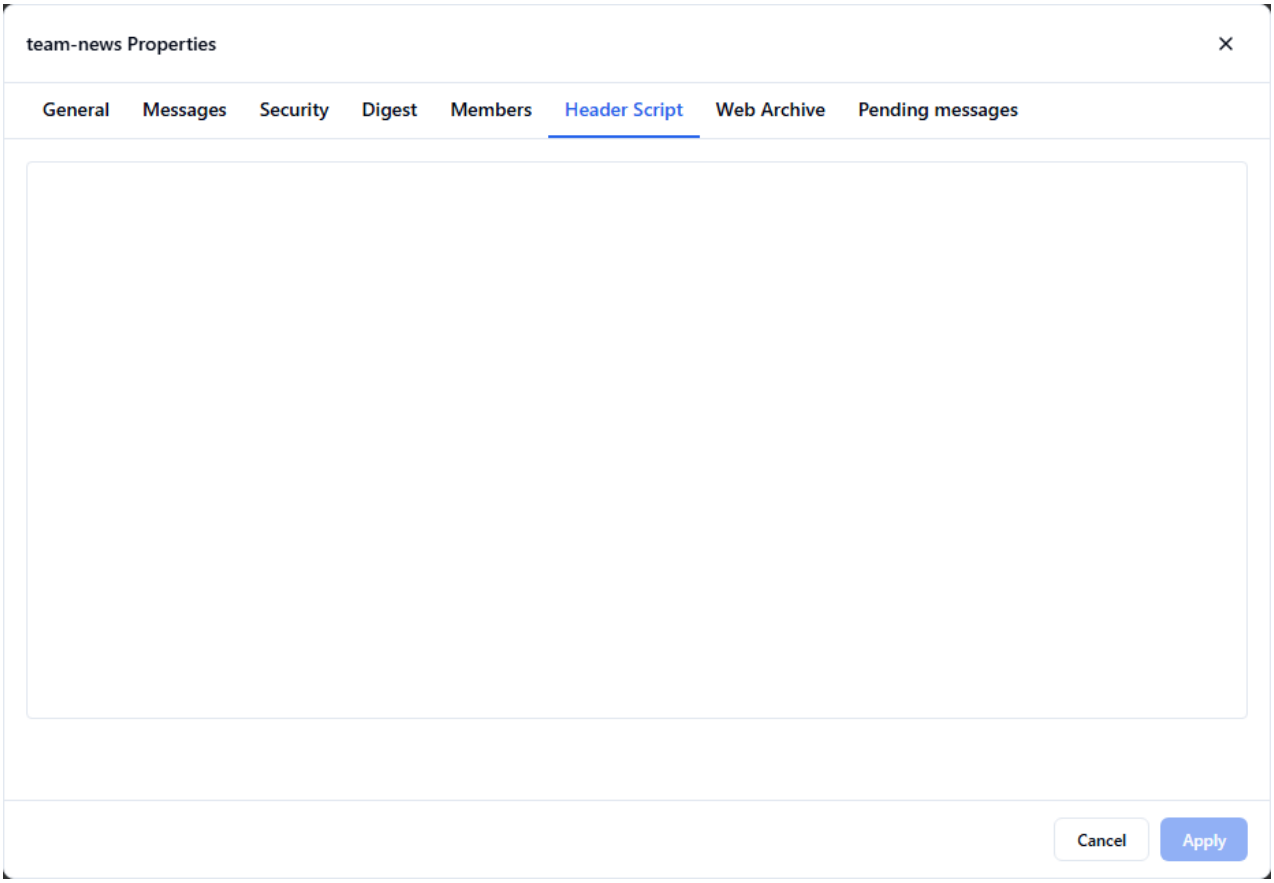

Figure 135 List header processing

List web archive page

To generate web archive pages, a server administrator enables HypermailEnabled and sets HypermailDir to an absolute directory writable by SMTPDA. Serve its mailsite-v11 subdirectory through a web server with appropriate access controls. Default-index and reverse-index settings are supported. Old templates, inline attachment rules and legacy appearance options are not applied; see Appendix B before migrating a customized archive.

Dynamic mailing-list membership

Choose the membership source when creating a list. Native membership is stored in MailSite. The built-in alternatives resolve their current source in the storage service, so Console, delivery and command-line enumeration use the same membership.

- Text file: configure the file path on the source tab. Use UTF-8, UTF-8 with BOM, or UTF-16LE. Addresses may include display names. Invalid entries are skipped and duplicate addresses are removed. Convert legacy ANSI files explicitly. Adding/removing a member updates the file; preserve service-account read/write access.

- Windows group: configure the local or domain group and group type. Windows account names become addresses in the list's domain. Membership is read-only in MailSite and depends on the service identity's Windows permissions. Validate domain/nested-group access against your own Active Directory environment.

- Database: configure a 64-bit ODBC data source, credentials and query. A custom membership query returns email address first and optional display name second. The default query reads EmailAddress and FullName from the list-derived table name. Optional join/leave statements support %1 for the

quoted address, %2 for the derived table name, and %% for a literal percent. Display-name edits remain source-managed.

- Server mailboxes: configure mailbox/domain masks and a privilege mask. Comma-separated masks use first-match order; ! excludes, * matches any sequence and ? matches one character. This source is read-only. Privilege bits are 1 for users, 2 for domain administrators and 4 for server administrators.

An unavailable source is an error, not an empty membership result. Check the displayed error, source permissions, 64-bit ODBC configuration and server log. Database timeouts are bounded. Custom membership DLLs and legacy SQL member-property update statements require migration work rather than automatic execution.

Database list settings

Use the Database tab to configure the data source and credentials, membership query and optional join/leave SQL. The default query reads EmailAddress and FullName from the list-derived table. In the current join/leave templates, %1 is the quoted member address, %2 is the table name and %% is a literal percent. Do not substitute the old member-property update syntax; those statements are preserved as configuration only and are not executed.

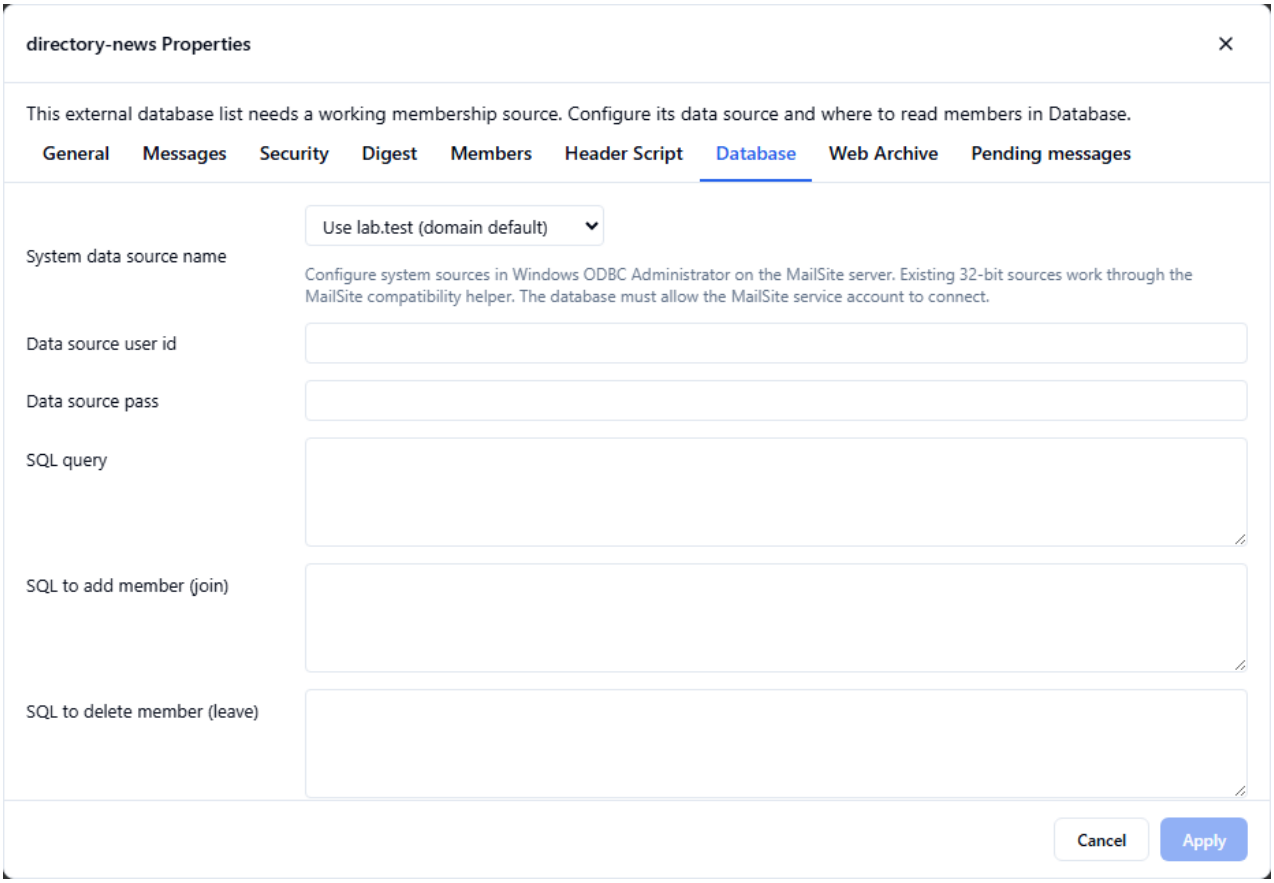

Figure 136 Database list source

Migrating a list

Use the documented configuration-transfer selectors to copy list definitions where appropriate. External providers own their members, so restore their source configuration and data rather than importing a native-member payload into them. Drain old pending posts/digests before upgrading and preserve existing archives separately. There is no current Console list Copy or Move command.

MailSite Web Services

HTTPMA provides the web front door for ExpressPro, the Console and synchronization endpoints. MailSite 11 does not require IIS applications for these services.

Public endpoints

ExpressPro and Console use the server's public HTTPS address. Exchange Web Services uses /EWS/Exchange.asmx, Exchange ActiveSync uses /Microsoft-Server-ActiveSync, and MAPI over HTTP uses the /mapi path. Configure client discovery and DNS for the same public hostnames and verify the certificates clients actually receive.

Worker services

HTTPMA forwards requests to EWSMA, EASMA or MAPIMA on private loopback endpoints. In the default service configuration these are 18082, 18081 and 18083 respectively; MSDBMA uses 18084. Installation and development environments may override internal ports. Do not expose worker or storage ports as public client endpoints.

Service operations

Use Server, Services to inspect status, properties and logs. Restarting HTTPMA interrupts the web Console briefly. Certificate changes take effect when the TLS services restart; verify successful restart and the served certificate before completing maintenance.

If webmail opens but mailbox operations fail, inspect EWSMA and MSDBMA. If only mobile synchronization fails, inspect EASMA. A gateway error can mean that the corresponding worker is unavailable, not that the mailbox password is wrong.

Troubleshooting Procedure

Start with one reproducible symptom, its time, the affected account and the exact client/service version. Check service availability and logs before changing configuration. Preserve a backup and the evidence for the failing operation; avoid clearing databases or replaying mail as a generic first step.

Check connectivity and naming

Resolve the public hostname and the domain's MX records from the network where the failure occurs. Check the configured service port, firewall route and TLS certificate hostname. A ping result alone does not prove a TCP listener or mail protocol is working, and a blocked ping does not prove mail connectivity is broken.

For outgoing delivery, perform the equivalent checks from the MailSite server to the destination. Inspect the queued recipient's recorded failure and retry status. Distinguish temporary remote failure from a permanent recipient rejection.

Check the owning services

MSDBMA must be available for shared configuration and mailbox operations. HTTPMA is the public front door for ExpressPro and the EWS/EAS/MAPI workers. SMTPRA receives mail and SMTPDA processes delivery. A failure logged by a client service may originate in an unavailable storage worker or external source; follow the associated error rather than restarting every component without evidence.

Reproduce with appropriate logging

Use Console, Logs and the service's logging controls to capture a bounded reproduction. Keep timestamps, protocol responses and relevant message/request identities together. Avoid sharing passwords, tokens or full message contents when a small redacted excerpt is sufficient. Restore normal logging after collecting the required information.

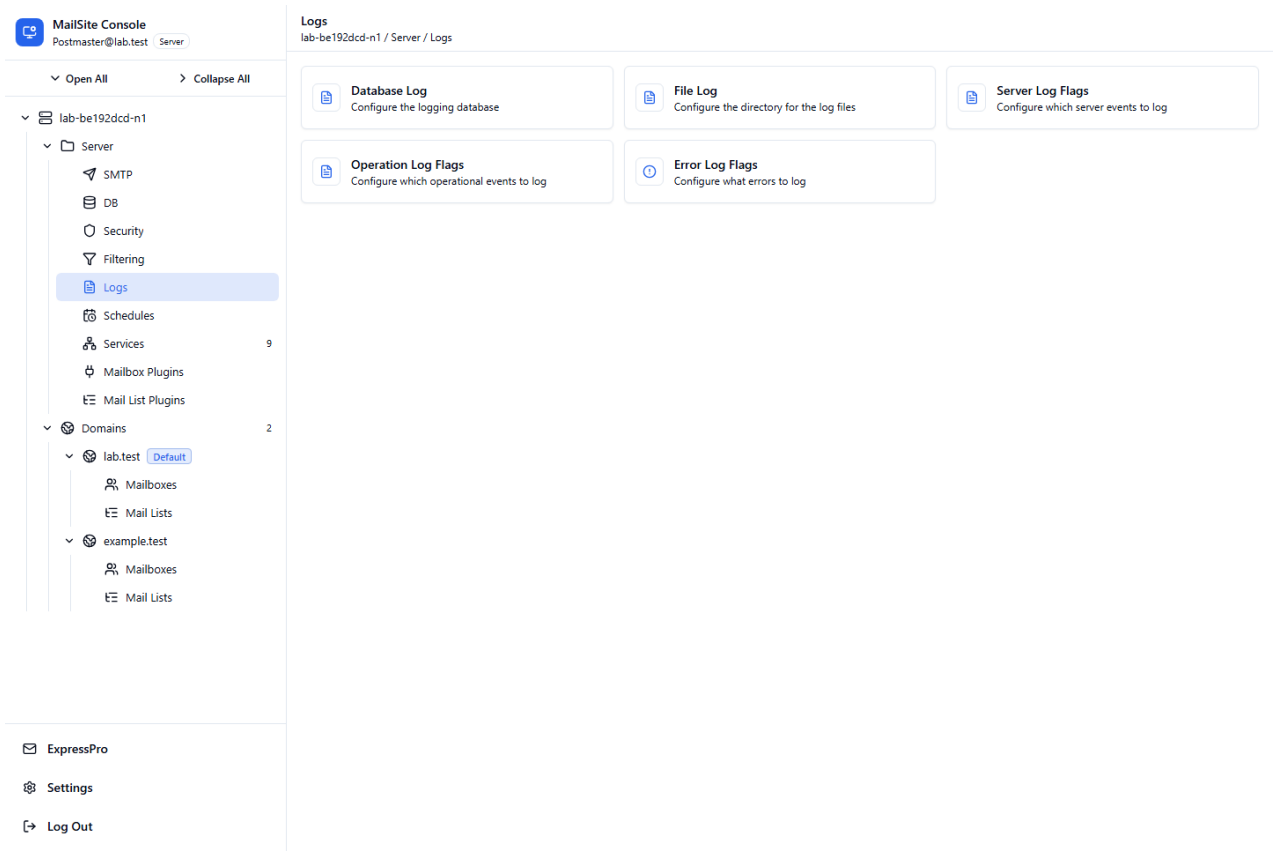

Figure 137 Service diagnostics in the Console

Test protocols

Use an actual configured client or a TLS-capable protocol tool with a disposable test account. The old Telnet USER/PASS and IMAP LOGIN examples send credentials without encryption and are not suitable for a production authentication test. Confirm the TLS connection and certificate first, then test login and the specific operation that failed.

For SMTP, distinguish connection, EHLO, authentication where required, recipient acceptance, data acceptance and final delivery. Acceptance into the queue is not proof that a remote recipient received the message. Use a local test recipient and inspect the queue/mailbox result.

Check storage and external dependencies

Use the Console database diagnostics when a collection reports a schema, indexing or access error. Do not delete Databases directories or alter message files to clear the warning. Check the current build's migration rules, file permissions, available storage and the specific failed state.

For database mailboxes and dynamic lists, validate the source under the service identity and inspect its explicit error. For calendar subscriptions, inspect the refresh result; failed refresh leaves the last good events visible and does not prove the feed is current.

Escalate with evidence

Provide the release version, service state, reproducible steps, expected and actual result, relevant redacted logs, and any recent configuration or upgrade change when requesting support. Review release notes before testing a newer build and retain a recovery path for the existing installation.

DNS Overview

DNS connects public names to the hosts that provide mail and other services. Mail delivery depends on both destination records and reachable listeners.

Domain Name System (DNS) records include host addresses, mail exchangers and TXT values used for email authentication.

A client normally asks a recursive resolver, which obtains the answer from the relevant authoritative DNS servers and caches it according to its lifetime.

Configure the client and server resolvers for the deployment. Check records from outside the mail server as well as locally.

A records map a host name to an IPv4 address; AAAA records map it to IPv6. For example, a documentation-only host record is:

- mail.example.com. A 192.0.2.25

MX records name the destination mail servers and their preferences. Lower numbers are preferred. For example:

example.com. MX 10 mail1.example.com.
example.com. MX 20 mail2.example.com.

Resolve the chosen mail host to its address and verify its SMTP listener. If a preferred host is unavailable, delivery can try another eligible MX destination.

An absent MX record may fall back to a host address. An explicit null MX announces that the domain does not accept mail. Diagnose the actual DNS result before changing routing.

The following points should be noted:

- It is wise to ask your provider to act as a secondary mail server for you in case your machine becomes unavailable. For example, your disks could become full; your Internet connection could break.
- The MX records and A records for the same name could be different (thus one machine receives mail and another machine receives all other traffic).
- If MX records exist, they must be correct; otherwise your domain will not receive mail.

License Agreement

The following license text is retained from the previous reference guide. References to bundled legacy products describe that distribution; this chapter is not an inventory of v11 components. Consult the agreements supplied with the installed release.

MAILSITE FUSION SOFTWARE LICENSE AGREEMENT

LICENSE AGREEMENT: This Software License Agreement (this "Agreement") is a legal agreement between you, the end customer ("Licensee" or "you") and MailSite Software Incorporated ("MailSite, Inc." or "Licensor"). PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE ACCOMPANYING MAILSITE FUSION ENGINE (THE "SOFTWARE"). BY USING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT CONSENT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, CLICK ON THE "I DO NOT AGREE" BUTTON OR RETURN FOR REFUND THE UNUSED SOFTWARE AND ALL ACCOMPANYING DOCUMENTATION WITHIN TEN (10) DAYS OF PURCHASE TO THE VENDOR FROM WHOM YOU OBTAINED IT.

GRANT: Licensor grants you a non-exclusive, non-transferable license (the "License") to use the Software on a single computer owned or leased by you ("Server") or on multiple Servers connected in a network that authenticate against a single subscriber database ("Cluster of Servers") limited to the total number of mailboxes that you purchased. The Software is deemed "in use" on a single Server or on a Cluster of Servers when it is loaded into the temporary memory (i.e. RAM) or installed onto the permanent memory (e.g. hard disk or other storage medium) of the Server(s). If you have more than one License for the Software, then at any time you may have as many copies of the Software in use as you have Licenses. The MailSite Console is subject to this Agreement, however it may be freely installed on any of your Servers.

LICENSE KEY: A License Key may have been supplied to you to activate your use of the Software. The License Key is confidential information of MailSite, Inc, and you may not disclose it to any other person or entity.

RESTRICTIONS: The Software and the accompanying Administration Guide ("Manual") contain copyrighted material, trade secrets, and other proprietary information belonging to Licensor and/or its licensors and are therefore protected by United States copyright laws, international treaty provisions and all other applicable laws. In order to protect them, and except as permitted by applicable law, you may not: (a) modify, decompile, disassemble, decrypt, or otherwise reverse engineer the Software or create derivative works based upon the Software in whole or in part; (b) rent, transfer, assign, lease, sublicense or grant any rights in the Software, or any portion thereof, in any form to any person without the prior written consent of Licensor which, if given, shall be subject to the conferee's consent to the terms and conditions of this Agreement; or (c) remove any proprietary notices, labels or marks on the Software.

LIMITED WARRANTY AND DISCLAIMER: The sole warranty regarding the Software is that the Software will perform in substantial compliance with the Manual on that hardware and operating system software for which it was designated (as stated in the Manual) for a period of 90 days from the date of purchase. The entire liability of MailSite, Inc. and your sole and exclusive remedy for any breach of this limited warranty shall be, at the option of MailSite, Inc, either (a) the refund of your payment for the Software upon your return of Software and the Manual along with a copy of your receipt, or (b) the replacement of the Software on an exchange basis without charge provided you return the Software and the Manual along with a copy of your receipt. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. Any replacement Software will be warranted for the remainder of the original warranty period or 30 days, whichever is longer.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MAILSITE, INC. DISCLAIMS ALL OTHER WARRANTIES EITHER EXPRESS OR IMPLIED, BY STATUTE OR OTHERWISE, REGARDING THE SOFTWARE AND THE MANUAL, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, THEIR QUALITY, THEIR MERCHANTABILITY, OR THEIR NON-INFRINGEMENT. SOME JURISDICTIONS

DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. IN THAT EVENT, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO 90 DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MAILSITE, INC. AND ITS SUPPLIERS AND REPRESENTATIVES SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR THE LIKE), WHETHER BASED ON BREACH OF

CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR ANY OTHER THEORY OF LIABILITY EVEN IF LICENSOR OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. IN ANY EVENT, THE ENTIRE LIABILITY OF MAILSITE, INC. UNDER ANY PROVISION OF THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE, OR TO $1000, WHICHEVER IS THE LESSER AMOUNT. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TERMINATION: This License is effective until terminated. You may terminate this License at any time by destroying the Software, the Manual and any copies thereof. This License will terminate immediately without notice from Licensor if you fail to comply with any provision of this License. Upon termination you must destroy or return to Licensor the Software, the Manual and any copies thereof.

JURISDICTION AND INTERPRETATION: This Agreement shall be governed by and construed in accordance with the laws of the United States and the State of California, as applied to agreements entered into and to be performed entirely within California between California residents. If for any reason a court of competent jurisdiction finds any provision of this Agreement or portion thereof, to be unenforceable, that provision of the License shall be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect. This Agreement is deemed entered into at Campbell, California, and jurisdiction for resolution of any disputes shall reside solely in the state and federal courts of the County of Santa Clara, State of California. This Agreement shall be construed as to its fair meaning and not strictly for or against either party.

MISCELLANEOUS: You acknowledge that, in providing you with the Software, Licensor has relied upon your agreement to be bound by the terms of this Agreement. You further acknowledge that you have read, understood, and agreed to be bound by the terms of this Agreement, and hereby reaffirm your acceptance of those terms. You further acknowledge that this Agreement constitutes the complete statement of the agreement between you and Licensor, and that the Agreement does not include any other prior or contemporaneous promises, representations, or descriptions regarding the Software. However, this Agreement does not limit any rights that Licensor may have under trade secret, copyright, patent, or other laws that may be available to it. The agents, employees, distributors, and dealers of Licensor are not authorized to make modifications to this Agreement, or to make any additional representations, commitments, or warranties binding on Licensor. Accordingly, additional statements such as dealer or other advertising or presentations, whether oral or written, do not constitute representations or warranties by Licensor and should not be relied upon. This Agreement may be modified only in writing. If any provision of this Agreement is invalid or unenforceable under applicable law, it is to that extent, deemed omitted and the remaining provisions will continue in full force and effect.

Use, duplication or disclosure by the U.S. Government is subject to restrictions stated in paragraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013.

AVG END USER SOFTWARE LICENSE AGREEMENT

License Grant; Related Provisions

Grant of License

AVG Technologies, subject to the terms and conditions of this Agreement, hereby grants to you a non-exclusive and non-transferable license during the Term to use the Software only in executable or object code form solely for your

personal or internal business purposes. This license authorizes you to use the Software on or in conjunction with up to (i) the number of computers specified by your order for the Software, or (ii) in the case of Software purchased on a CD or other physical medium, the number specified on the Software package, or (iii) if you received the Software in combination with other hardware or software, solely in conjunction with such other hardware or software.

Limitations

You shall not, and shall not permit any third party to,

duplicate the Software for any purpose other than as reasonably necessary to use the same as contemplated by this Agreement and for off-line archival and disaster recovery purposes;

except for temporary transfer in the event of computer malfunction, install the Software on a second computer;

publish the Software or use the same other than for the purposes described in Section 1.a of this Agreement;

except as expressly authorized by law, reverse engineer, disassemble, decompile, translate, reconstruct, transform or extract the Software or any portion of the Software (including without limitation any related malware signatures and malware detection routines);

except as expressly authorized by law, change, modify or otherwise alter the Software (including without limitation any related malware signatures and malware detection routines);

transfer, pledge, rent, share or sublicense the Software other than in connection with the sale or other transfer of the computer on which it is initially installed;

grant any third party access to or use of the Software on a service bureau, timesharing, subscription service, rental or application service provider basis or otherwise; or

defeat or circumvent, attempt to defeat or circumvent, or authorize or assist any third party in defeating or circumventing controls on the installation or use of copies of the Software.

Updates

AVG Technologies, from time to time during the Term, may provide updates to the Software and/or the malware signatures included therein (each, an “Update”). Updates will be deemed Software for all purposes under this Agreement. You acknowledge that you must routinely download and permit installation of Updates in order to obtain maximum benefit from the Software.

Term; Termination

Term

The initial term of this Agreement will commence on the date you download or otherwise acquire the Software, and will continue

for the term you specified in your order for the Software, or

if you purchased the Software on CD or other physical medium, on the Software package, or

if you received the Software in combination with other hardware or software, the term specified by your supplier. If renewal terms are available, AVG Technologies will provide notice offering you the

opportunity to purchase renewals at the then-current renewal price. The initial term and any renewals purchased are referred to in this Agreement as the “Term”.

Termination

AVG Technologies, in addition to such other rights may be available at law or equity, shall be entitled to terminate this Agreement at any time without notice if you commit a material breach of this Agreement.

Effect of Termination

On the expiration or termination of this Agreement, you will cease using the Software, AVG Technologies may cease making Updates available to you, and the Software may cease functioning. Sections 1.b, 3, 4, 5 and 6 will survive the expiration or termination of this Agreement.

Ownership

AVG Technologies reserves all rights in the Software not expressly granted by this Agreement. All copyrights, trademarks and other conceivable intellectual property rights in and to the Software (including, but not limited to, malware signatures and other data files, images appearing in the Software and screen displays as well as any and all documentation relating to the Software) are owned by AVG Technologies or its licensors, and are protected by United States and foreign copyright laws, international treaties and other applicable laws. Any copy of the Software you are allowed to make pursuant to this Agreement must contain the entire copyright and other notices included with the original copy of the Software.

Warranties

General

AVG Technologies warrants, that on delivery of the Software and for a period of thirty (30) days thereafter, that the medium (if any) on which the Software is delivered will be free of material defects, and that the Software will perform substantially in accordance with the applicable specifications. The foregoing warranty applies only to the Software as originally delivered, and does not apply to Updates. Your sole and exclusive remedy for breach of this Warranty is replacement of the defective media or Software or, at AVG Technologies’ option, return of the Software for a full refund. In order to exercise your rights under this Section 4, you must deinstall and destroy all copies of the Software you may have made (including all archival copies), and (i) if you purchased the Software by download, follow the instructions on the confirmation email you received in connection with the purchase, or (ii) for all other purchases, return the Software in its original package, along with your receipt, to the point of purchase.

Beta Versions

Notwithstanding the provisions of Section 4.a, THE PROVISIONS OF THIS SECTION 4.b APPLY IN PLACE OF SECTION 4.a IF (AND ONLY IF) THE SOFTWARE IS A “BETA TEST” VERSION. In view of the evaluation nature of Software, Software is provided on an “as is”, “as available” basis, without warranty and without support or other services by AVG Technologies. YOU AGREE TO USE THE AVG BETA SOFTWARE STRICTLY FOR THE PURPOSES OF EVALUATION AND TESTING, AND THAT YOUR RELIANCE ON THE AVAILABILITY OR ACCURACY OF THE AVG BETA SOFTWARE SHALL BE ENTIRELY AT YOUR OWN RISK.

Disclaimer

EXCEPT AS EXPRESSLY PROVIDED BY SECTION 4.a OF THIS AGREEMENT, AVG TECHNOLOGIES DISCLAIMS ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, MEDIA AND ANY OTHER SUBJECT MATTER OF THIS AGREEMENT, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, THE IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND IMPLIED WARRANTY OF NONINFRINGEMENT. AVG TECHNOLOGIES DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT THE SOFTWARE WILL PROVIDE 100% PROTECTION. Some

jurisdictions do not allow limitations on an implied warranty, so the above limitations may not apply to you. You may have other rights that vary from jurisdiction to jurisdiction.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL AVG TECHNOLOGIES OR ITS SUPPLIERS OR RESELLERS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE OR SPECIAL DAMAGES WHATSOEVER, WITHOUT REGARD TO CAUSE OR THEORY OF LIABILITY (INCLUDING, WITHOUT LIMITATION,

DAMAGES INCURRED FOR LOSS OF BUSINESS PROFITS OR REVENUE, LOSS OF PRIVACY, LOSS OF USE OF ANY COMPUTER OR SOFTWARE INCLUDING THE SOFTWARE, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR OTHER PECUNIARY LOSS) ARISING OUT OF THIS AGREEMENT OR THE SOFTWARE PROVIDED HEREUNDER, EVEN IF AVG TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL AVG TECHNOLOGIES' LIABILITY RELATED TO THE SOFTWARE EXCEED THE LESSER OF THE FEES YOU ACTUALLY PAID FOR THE SOFTWARE AND AVG TECHNOLOGIES' SUGGESTED RETAIL PRICE FOR THE SOFTWARE AS OF THE DATE YOU RECEIVED IT. THE FOREGOING LIMITATION SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

Miscellaneous

Notice

AVG Technologies may deliver any notice to you via pop-up window, dialog box or other means, even though you may not receive the notice unless and until you launch the Software. Any such notice will be deemed delivered on the date AVG Technologies first makes it available through the Software, irrespective of when you actually receive it.

Privacy

You acknowledge that AVG Technologies collects certain information regarding the users of the Software, including certain personally identifiable information. You hereby consent to AVG Technologies' collection and use of such information, and agree that AVG Technologies' collection and use of such information will be governed by AVG Technologies' Privacy Policy, currently published at www.avg.com as AVG Technologies may revise the same from time to time.

BY PROCEEDING TO INSTALL THE TOOLBAR, YOU ACKNOWLEDGE AND ACCEPT THAT, UPON ITS INSTALLATION, THE TOOLBAR WILL MODIFY VIA THE SETTINGS OF YOUR BROWSER THE "DNS ERROR PAGE" AND "ERROR 404 PAGE". FURTHERMORE, ONCE INSTALLED, THE TOOLBAR MAY COMMUNICATE CERTAIN BASIC USAGE INFORMATION TO VISICOM MEDIA INC. VIA ("APPLICATIONSTAT.COM") TO HELP VISICOM COMPILE GLOBAL STATISTICS CONCERNING USAGE

OF THE TOOLBAR BY USERS (for example concerning the number of installations and unique users, the number of clicks which the Toolbar receives, the number of searches performed by users, etc.). Such statistical information will not include any personally identifiable information regarding users.

U.S. Government License

Any Software provided to the U.S. Government is provided with the commercial license rights and restrictions described elsewhere herein. AVG Technologies reserves all unpublished rights under the United States copyright laws.

Complete Agreement

This Agreement constitutes the complete Agreement between the parties and supersedes all previous communications and representations or agreements, either oral or written, with respect to the subject matter hereof.

Amendments; Waiver

This Agreement may be modified or changed in whole or in part in any manner other than by an Agreement in writing duly signed by both parties hereto or by a further electronic agreement presented by AVG Technologies and accepted by you. AVG Technologies' failure to insist upon or enforce strict performance of any provision of this Agreement shall not be construed as a waiver of any provision or right.

Severability

The parties desire and intend that all of the provisions of this Agreement be enforceable to the fullest extent permitted by law. If any provision of this Agreement or the application thereof to any person or circumstances is, to any extent, construed to be illegal, invalid or unenforceable, in whole or in part, then such provision will be construed in a manner to permit its enforceability under applicable law to the fullest extent permitted by law. In any case, the remaining terms of this Agreement or the application thereof to any person or circumstance, other than those that have been held illegal, invalid or unenforceable, will remain in full force and effect.

Governing Law

This Agreement will be governed by the laws of the State of Delaware. The exclusive jurisdiction for any dispute will be state or federal courts sitting in the State of Delaware.

Export Controls

You acknowledge that portions of the Software may be of U.S. origin. You agree to comply with all applicable U.S. and international laws governing export and reexport of the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments.

Language

This Agreement was originally prepared in the English language. Although AVG Technologies may provide one or more translations for your convenience, the English version will control in the case of any conflict or discrepancy.

NetBSD Copyright

MailSite tools include UNIX password, and DES, encryption developed by Berkeley. The following copyright notice applies:

Copyright (c) 1989, 1993

The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Tom Truscott.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Appendix A - Utilities

The following utilities assist with administrative tasks. Current configuration and storage utilities require a compatible running MSDBMA authority and appropriate administration access. Use the help from the installed build for its accepted options. Protect password-bearing commands and output. SMTP/POP network utilities use their explicitly selected protocol targets; they are separate from authority-based configuration operations.

MSALIAS

Current CLI limitation: map-to values cannot contain a wildcard, and duplicate map-from masks are rejected without changing the map. Existing wildcard resolution in the server is separate from the values accepted by this utility.

The command-line utility MSALIAS.EXE can be used to manage the alias table. The syntax is:

```
msalias -versionmsalias -machine \\system -login user[@domain] -loginpass password …

msalias -listmsalias -addstart mapfrom mapto

msalias -addstart -file aliasfile

msalias -addend mapfrom mapto

msalias -addend -file aliasfile

msalias -delete mapfrommsalias -deleteall [-noprompt]

msalias -reorder mapfrom beforemapfrom
```

One and only one of the -version, -list, -addstart, -addend, -delete, -deleteall and -reorder

flags may be present. The command arguments are as follows:

-version

Display the version number of the mail server.

–machine \\system -login user[@domain] -loginpass password ...

Specifies the name of a target remote machine (preceded by a double backslash), as well as login data for a mailbox on the target server that has MailSite server privileges. This option is used in conjunction with any of the other flags to execute the given operation on the remote system. If this is omitted, the local machine is assumed.

-list

List all the aliases, in order. The format is one alias per line, each line containing the map-from address, a single space, then the map-to address.

-addstart mapfrom mapto

Add an alias at the start of the alias table. The arguments specify the map-from address and the map-to address that will form the new alias.

-addstart -file aliasfile

Add aliases at the start of the alias table. The argument specifies the name of a text file from which the aliases will be read. The format of the file is one alias per line, each line containing the map-from address and the map-to address, separated by one or more white space characters, and/or one or more colons. Blank lines, and lines on which the first non-blank character is a #, are ignored.

-addend mapfrom mapto

Add an alias at the end of the alias table. The arguments specify the map-from address and the map-to address that will form the new alias.

-addend -file aliasfile

Add aliases at the end of the alias table. The argument specifies the name of a text file from which the aliases will be read. The format of the file is one alias per line, each line containing the map-from address and the map-to address, separated by one or more white space characters, and/or one or more colons. Blank lines, and lines on which the first non-blank character is a #, are ignored.

-delete mapfrom

Delete the alias that has the given map-from address.

-deleteall [-noprompt]

Delete all the aliases, prompting for confirmation. If the –noprompt flag is present, you will not be prompted for confirmation.

-reorder mapfrom beforemapfrom

Remove the alias that has the mapfrom map-from address from the table, and replace it immediately before the alias that has the beforemapfrom map-from address. If either alias does not exist, the command fails.

MSBACK

You can use the utility program MSBACK.EXE to save and restore your MailSite configuration to and from a text

file. You should include this command in your nightly backup script. MSBACK.EXE is a console program (i.e. it should be run at the command-line prompt). The syntax for this command is:

```
msback [-version]

msback [-machine \\system] [-restore [-deleteold]] filename
```

The command arguments are as follows:

-version

Display the version number of the mail server.

-machine \\name

Specify the name of the target MailSite server. If this is omitted, the local machine is assumed. Note that the machine name must be preceded by a double backslash.

-restore

Read the configuration from the file and write it to the Registry. If this argument is omitted, the configuration will be read from the Registry and written to the file.

-deleteold

Delete the old configuration in the Registry before restoring the configuration from the file. If this argument is omitted, the configuration from the file will be merged with the existing configuration. This argument is only relevant if - restore is specified.

filename

The name of the file to which the configuration will be written (or from which it will be read, if -restore was specified). This argument is required.

MSBACK uses a text format to store the mail server configuration information. The format is described in BNF below. Examining a generated backup file will help make this clearer.

<configurationfile> ::= <key> [<key>]<key> ::= <openingmarker>[<value>..][<subkey>..]<closingmarker><openingmarker> ::= "["<escapedkeyname>"]"<closingmarker> ::= "[""/"<escapedkeyname>"]"<escapedkeyname> ::= key name, control chars, %, / [and] chars replaced by %xx<value> ::= <valuename> "=" <valuedata><valuename> ::= value name with any control chars, % and = chars replaced by %xx<valuedata> ::= <dwordvaluedata>|<stringvaluedata>|<multistringvaluedata><dwordvaluedata> ::=

string of decimal digits<stringvaluedata> ::= ""[<stringdata>]""<stringdata> ::= sequence of chars with any control chars, % and " replaced by %xx<multistringvaluedata> ::= <stringvaluedata>[<stringvaluedata>..]""""""<subkey> ::= <key>

Note that an empty multistring is represented as "" "" whereas an empty string is represented as "". It is vital that the opening and closing markers and each value are on a line by themselves - i.e. no newlines within <openmarker>,

<closemarker> or <value>.

MSBACK supports registry configuration only. Keep MSDBMA available while exporting or restoring configuration, and prevent other configuration edits during the operation. Stop dependent services before restoration as appropriate, but do not stop the authority needed by the utility. See Backup for the separate offline data-copy procedure and SQL configuration backup requirements.

MSBOX

MSBOX lists and manages account configuration through the current MailSite authority. Use its help for the supported list, create, delete and property operations. Mailbox paths and credentials are sensitive configuration; review the selected domain and account before a mutation.

The legacy -plugin conversion syntax is recognized but returns error 50 (operation not supported). It does not convert Registry, Windows or database authentication. Do not use the old two-command bulk conversion example. Use explicit configuration migration and external-account provisioning workflows and verify authentication afterward.

Listing external/Windows-backed accounts does not export their source password as a usable MailSite password. A list of account definitions is not a mail-content backup. See MSIMPORTEXPORT for selected XML configuration transfer.

Account commands

Run MSBOX with no arguments to display usage for the installed build. MSDBMA must be running, and the caller must have the required administration access. Quote names, paths and values that contain spaces.

```
msbox -list [Domain [Pluginid]]
```

Lists configured accounts, optionally narrowed by domain and account provider.

```
msbox -list2 [Domain [Pluginid]] -security pass
```

Produces the extended list. Password fields for Windows-backed provider IDs 1 and 2 are suppressed. Treat other exported credential fields as sensitive; do not publish command output.

```
msbox -create Name[@Domain] Pluginid
```

Creates account configuration for the selected provider. External accounts also require a valid source configuration; creating an account does not create a Windows or external database identity.

```
msbox -get Name[@Domain] Property
```

```
msbox -set Name[@Domain] Property Value
```

Reads or changes a named mailbox property. Use the supported property name and value type; see Appendix L. A stored value alone does not prove that a retained legacy feature is active.

```
msbox -pass Name[@Domain] [Plaintextpassword]
```

Changes the account password where the selected provider supports that operation. An explicit command-line password can be visible in process listings and shell history.

```
msbox -createalias Name[@Domain] Alias[@Domain]
```

```
msbox -deletealias Alias[@Domain]
```

```
msbox -listalias Mailbox[@Domain]
```

Manages mailbox aliases on the SQL configuration backend. These are separate from the server alias map managed by MSALIAS.

```
msbox -delete Name[@Domain]
```

Deletes the selected account configuration. Preserve the required configuration and mail-store backups first, and verify the complete account identity before running a destructive command.

MSCVTDIR

The command-line utility MSCVTDIR.EXE can be used to convert mailbox directories from a single level to a multi-level structure (and vice versa). The multi-level directory structure allows for more efficient disk usage, and is recommended for domains that have more than 1,000 mailboxes. Note that this conversion is not executed when you enable multi-level mailboxes for a domain in the Windows Console; converting mailboxes can be done only by MSCVTDIR.

The syntax for MSCVTDIR is as follows:

```
mscvtdir [-revert] domain
```

The command arguments are as follows:

-revert

Specifies that mailbox directories for the given domain should be converted from multi-level to single level.

domain

Specifies the domain for which mailboxes should be converted. Note that multi-level mailbox directories must be enabled for this domain (even if reverting to old-style directories); otherwise the utility will not run.

When a mailbox directory is converted to the multi-level structure, its new location is based on the first three letters of the mailbox name. For example, the mailbox directory C:\MAILBOX\fred will be converted to C:\MAILBOX\!f\!r\!e\fred. If a mailbox name has less than three characters, an underscore character ("_") takes the place of the missing characters in the intermediate directories. For example, the mailbox directory C:\MAILBOX\f will be converted to C:\MAILBOX\!f\!_\!_\f.

After it is executed, MSCVTDIR displays the number of directories moved and the total number of mailboxes.

MSDOMAIN

The command-line utility MSDOMAIN.EXE can be used to manage virtual domains. The syntax is:

```
msdomain –version
msdomain –machine \\system -login user[@domain] -loginpass password …
msdomain –list
msdomain -create domain
msdomain -delete domain
msdomain -set domain property value
msdomain -get domain property
msdomain -createsynonym domain synonym
msdomain -deletesynonym [domain] synonym
msdomain -listsynonyms [domain]
```

One and only one of the option flags may be present (excluding the -machine flag). The command arguments are as follows:

-version

Display the version number of the mail server.

–machine \\system -login user[@domain] -loginpass password ...

Specifies the name of a target remote machine (preceded by a double backslash), as well as login data for a mailbox on the target server that has MailSite server privileges. This option is used in conjunction with any of the other flags to execute the given operation on the remote system. If this is omitted, the local machine is assumed.

-list

List the mail domains on the server. The first domain in the list is the default domain.

-create domain

Create a new virtual domain called domain..

-delete domain

Delete the virtual domain called domain.

-set domain property value

Set the virtual domain property property to have value value.

-get domain property

Display the value of the virtual domain property property.

-createsynonym domain synonym

Create the specified synonym for the selected virtual domain.

-deletesynonym [domain] synonym

Delete the synonym synonym corresponding to the virtual domain domain.

-listsynonyms [domain]

List the synonyms for the given virtual domain. If the domain name is absent, all the synonyms are listed.

Domain properties can be accessed via MSDOMAIN. Refer to the appendix on Domain Properties for more information.

MSIMPORTEXPORT

MSIMPORTEXPORT transfers server, domain, mailbox, alias, route and mail-list configuration through MSDBMA. It supports both registry and SQL configuration and the retained XML format. It does not copy mailbox content, certificates or a SQL disaster-recovery backup. Keep MSDBMA available while using the command and protect the XML because passwords can be recovered from it.

Export selected configuration

```
msimportexport -export config.xml -server -domains -mailboxes -maillists
```

Select a specific domain, mailbox or list with -domain name, -mailbox name or -maillist name. With no selectors, an export does not imply that all configuration is selected. Use explicit selectors and verify the resulting file. Export to - writes XML to standard output; it cannot be combined with -delete.

Import selected configuration

```
msimportexport -import config.xml -server -domains -mailboxes -maillists
```

Import parses and validates the input before submitting the change. The destination retains control of its storage connection and machine-local configuration. External membership sources own their members: import the source settings and restore the external data, rather than supplying a native-member payload to an external list.

Mapping and replacement

After a mailbox/list selector, -plugin old[:new],... maps source plugin IDs. A negative source list plugin suppresses its member payload. After a selector, -property old:new[.1|.4|.7],... renames properties and

optionally supplies the value type (string, integer or multi-string). Match these mappings to the intended destination semantics; changing a type identifier does not implement a missing external provider.

-delete removes all selected backend configuration, regardless of narrower selectors. With -import it clears configuration before applying the imported replacement; with -export it clears only after successful file publication. It does not delete mail files. Use -delete only as a deliberate full configuration replacement, with a verified export and separate data backup. A malformed import or failed export must be corrected before retrying.

MSLDIF

The command-line utility MSLDIF.EXE can be used to export information about MailSite mailboxes in LDAP Data Interchange Format (LDIF). (LDAP stands for Lightweight Directory Access Protocol – an LDAP server supplies Directory services to its clients.)

There are a number of RFCs and Internet Drafts dealing with LDAP – principally RFCs 2251 to 2256. LDIF is defined in an Internet Draft draft-good-ldap-ldif-01.txt. This utility creates entries in the inetOrgPerson object class defined in draft-smith-ldap-inetorgperson-01.txt.

The syntax is as follows:

```
msldif [-s system] [-f outputfile][-l locality] [-st state] [-ou orgunit] [-o org] [-c country]
[domain [domain [...]]]
```

The command arguments are as follows:

-s system

Specify the name of a remote machine from which mailbox information is to be exported. If this is omitted, the local machine is assumed.

-f outputfile

Specify the name of a file to receive the exported data. If this is omitted, the standard output is assumed, and the output information may thus be piped to another process.

-l locality

–st state

–ou orgunit

–o org

–c country

Each entry in an LDIF file starts with a Distinguished Name (DN) which locates the entry relative to other objects in the Directory. The DN may contain any of the above attributes. Exactly which attributes you need to specify, and what values you should give them, depend on the structure of your Directory. If none of these attributes are specified, the conversion utility will use the mail domain name to construct a default DN for each entry.

[domain [domain [...]]]

You may (optionally) specify one or more domains for which you wish to export mailbox information. If no domains are specified, mailbox information for all the domains on the mail server will be exported.

MSLIST

Provider IDs are 0 native, 1 Windows group, 2 text file, 3 ODBC and 4 server-mailbox masks. Members resolve through MSDBMA. Add/remove operates only on writable providers (0, 2 and 3); group and mask membership is source-managed. Provider failures are errors, not empty lists.

The command-line utility MSLIST.EXE can be used to manage mail lists. The syntax is:

```
mslist –version
mslist –machine \\system -login user[@domain] -loginpass password ...
mslist -list [domain]
```

```
mslist -create name[@domain] pluginid
mslist -delete name[@domain]
mslist -set name[@domain] property value
mslist -get name[@domain] property
mslist -members name[@domain]
mslist -add name[@domain] newmember
mslist -remove name[@domain] member
```

One and only one of the -version, -list, -create, -delete, -set, -get, -members, -add and -remove

flags may be present. The command arguments are as follows:

-version

Display the version number of the mail server.

–machine \\system -login user[@domain] -loginpass password ...

Specifies the name of a target remote machine (preceded by a double backslash), as well as login data for a mailbox on the target server that has MailSite server privileges. This option is used in conjunction with any of the other flags to execute the given operation on the remote system. If this is omitted, the local machine is assumed.

-list [domain]

List the mail lists in the given domain. If the domain is omitted, the mail lists in the default domain are listed.

-create name[@domain] pluginid

Create a new mail list called name in virtual domain domain, using the mail list plugin identified by the pluginid. If the

domain is omitted, the mail list is created in the default domain.

-delete name[@domain]

Delete the mail list name in virtual domain domain. If the domain is omitted, the mail list is deleted from the default domain.

-set name[@domain] property value

Set the mail list property property to have value value.

-get name[@domain] property

Display the value of the mail list property property.

-add name[@domain] newmember

Add the newmember address to the mail list.

-remove name[@domain] member

Remove the member address from the mail list.

-members name[@domain]

List all the members of the mail list.

MSPOP

MSPOP downloads messages from a remote POP3 mailbox and determines local recipients from the available message headers, unless a forced recipient is supplied. Hidden envelope recipients cannot be recovered from absent Bcc headers. Review its fallback/postmaster route, TLS policy and retention flags with test mail before processing a live account.

```
mspop -h hostname -u username -p password[-f address] [-e address] [-r] [-v] [-s size1] [+s
size2]
```

Where the arguments are:

-h hostname

The IP address or host name of the POP server. This argument is required.

-u username

The username of the account on the POP server which is to be downloaded. This argument is required.

-p password

The password of the account on the POP server which is to be downloaded. This argument is required.

-f address

If this flag is specified, then all downloaded messages will be force delivered to this address.

-e address

If this flag is specified, then all downloaded mail for which MSPOP cannot determine a local recipient address will be sent to this address.

-r

If this flag is specified, then the messages will be retained, not deleted from the POP server.

-v

If this flag is specified, then the version number will be displayed.

-s size1

If this flag is specified then only messages smaller than size1 bytes will be downloaded.

+s size2

If this flag is specified then only messages bigger than size2 bytes will be downloaded. The +s option may be used in conjunction with -s to select a range of sizes, in which case only messages whose sizes lie within the range will be downloaded.

Use MSPOP console diagnostics and the receiving SMTPRA log to investigate a transfer. The port does not append the old POPDOWN XLog record. Capture only the necessary diagnostic output and protect it because it can contain message information.

MSPURGE

Review the candidate list without -commit before deleting accounts. The retained -orphanedMailboxes option does not discover accounts removed from legacy external plugin databases. Source removal and account deletion require an explicit review; do not depend on that option for external-account cleanup.

The MSPURGE.EXE utility deletes unused mailboxes. This tool can be used to automatically remove mailboxes from your site that have not been used for some time.

```
mspurge –version
mspurge –machine \\system –user user[@domain] –pass password ...
mspurge [-domain domain][-plugin pluginid] [-age age][-unusedmailboxes] [-deletemessages] [-
commit][-silent][-noquestions][-deleteForwards][-deleteAutoReplies][-exclude mailboxNameList]
```

Where the arguments are:

-version

Display the version number of the mail server.

–machine \\system –user user[@domain] -pass password ...

Specifies the name of a target remote machine (preceded by a double backslash), as well as login data for a mailbox on the target server that has MailSite server privileges. This option is used in conjunction

with any of the other flags to execute the given operation on the remote system. If this is omitted, the local machine is assumed.

-domain domain

The domain of the unused mailboxes to purge. If omitted, the default domain is assumed.

-plugin pluginid

The type of mailboxes (specified by plugin ID) to purge. If omitted, all mailbox types are included.

-age age

The age (in days) that a mailbox must be unused for it to be purged. If omitted, one year (365 days) is the assumed value.

-unusedmailboxes

This flag specifies that mailboxes that have never been used (as opposed to mailboxes not used for a certain number of days) should be purged. If omitted, mailboxes that have never been used will not be purged.

-deletemessages

This flag specifies that the mailbox directories and messages of purged mailboxes should be deleted from the file system. If omitted, mailbox directories and messages are retained for mailboxes purged from MailSite.

-commit

This flag specifies that mailboxes selected for purging should be deleted. If omitted, MSPURGE displays a list of mailbox that would be purged by the given operation but does not purge any mailboxes.

-silent

This flag specifies that MSPURGE should not display a list of mailboxes to be purged.

-noquestions

This flag specifies that MSPURGE should not display confirmation prompts when executing.

-deleteForewards

This flag specifies that mailboxes configured to use mail forwarding should be included among the mailboxes deleted by MSPURGE. By default, these mailboxes are excluded from MSPURGE operations because they typically represent mailboxes that are not accessed via POP/IMAP but which are actively used.

-deleteAutoReplies

This flag specifies that mailboxes configured to use an automatic reply should be included among the mailboxes deleted by MSPURGE. By default, these mailboxes are excluded from MSPURGE operations because they typically represent mailboxes that have are not accessed via POP/IMAP but which are actively used.

-exclude mailboxNameList

This will exclude a list of mail boxes.

MSQUOTA

MSQUOTA recalculates stored usage for the selected domain or mailbox. It does not generate the warning/exceeded notification messages that the legacy maintenance command generated. It is not a command to remove quota limits or delete mail.

msquota – [-machine name] [-user user [-pass [pass]] [-domain domain][-mailbox mailbox] [-silent][-version] [-help]

The command arguments are as follows:

-machine name

When using remotely you will need to specify the name of the server that is running mailsite. The default is this machine.

-user user[-pass [pass]

When connecting remotely you need to logon to that server this will enable you to logon to the MailSite Server Remotly.

-domain

This option will reset the quota information for all mailboxes in a domain. * => alldomains, default domain if absent.

-mailbox

This will reset the quota information on a particular mailbox in the domain specified in the domain argument.

-silent

This option when enabled will not echo out the mailboxes and domains that have been reset.

-version

This displays the version of this utility.

-help

This displays the command line options that are available.

MSRETRY

The command-line utility program MSRETRY.EXE instructs the MailSite mail server to reattempt delivery to a given domain or domains. The syntax for this command is:

```
msretry –version
msretry [–machine \\system -login user[@domain] -loginpass password] domainmask domainmask ..
```

Where the arguments are as follows:

–machine \\system -login user[@domain] -loginpass password ...

Specifies the name of a target remote machine (preceded by a double backslash), as well as login data for a mailbox on the target server that has MailSite server privileges. If this is omitted, the local machine is assumed. If you specify the – machine option, the mail server may not recognize your request for up to two minutes

domainmask

Specify one or more fully-qualified name(s) of the domain(s) to which delivery should be re-attempted. The domain mask may contain the asterisk character as a wildcard. Specifying a single asterisk causes all domains to be retried.

MSSEND

MSSEND is a legacy utility and is not included in the current installer utility set. Use the supported mail client or a separately verified SMTP test tool for submissions. The retained MailSite 10 reference contains its historical command syntax.

MSSENDMESSAGES

MSSENDMESSAGES is not included in the current installer utility set. Do not use its old directory-replay procedure as a current mail-store recovery operation. Recover queued mail through the supported queue/storage workflow and verify that already completed deliveries are not replayed.

MSSTART

MSSTART connects to an SMTP server and requests delivery for one or more domains using ETRN. The target must support and permit the request; this command does not establish a network connection through Windows RAS.

```
msstart [-h hostname] [-u username [-p password]] domain [domain ...]
```

-h selects the target hostname or IP address. If omitted, the command targets the local machine. -u supplies the SMTP authentication username and -p its password when authentication is required by the remote policy. These arguments are not alternative hostnames. Protect credentials from command history and process listings.

Supply the domain names whose queued delivery should be triggered. A leading wildcard can request matching domains when the target supports it. Confirm the ETRN response and the actual queue/delivery result; command acceptance alone is not final message delivery.

Appendix B - Customizing Mail List Archiving

MailSite generates static HTML articles and thread, date, subject and author indexes under HypermailDir/mailsite-v11. HypermailDefaultIndex selects thread (0 or 1), date (2), subject (3), or author (4); HypermailReverseIndex reverses the ordering. Each archive directory belongs to one mailing list. Existing Hypermail pages, links, templates and attachments outside this new subdirectory remain untouched.

Articles show escaped plain text and provide the original message for HTML content and attachments. Message HTML is not executed in archive pages. Legacy index.htm/article.htm templates, mail-command links, header-selection rules, inline/ignored MIME-type settings and appearance options are not consumed. Retain the old archive URL and add a link to the new archive. Configure a new directory before exceeding 100,000 articles. Verify web-server MIME handling, download behavior, permissions and backups before publishing.

Archive publication uses one stable article identity per source message. A retry repairs derived index pages without duplicating the article. An archive failure delays list expansion; it does not silently skip the requested archive. Index files are replaced individually, so concurrent browsers can briefly see different index generations during publication. The preserved MailSite 10 reference manual remains the source for historical template syntax.

Appendix C - List Header Processing

Header Processing Script Syntax

Syntax: ADD headertemplate

Example: ADD X-advert: For great widgets, visit www.widgets.com

Adds the given header text to the end of the headers on the message. Any pre-existing headers of the same type are left unaltered. In the header template, the following combinations have effect: %% is replaced by a single %; %d is replaced by the current date and time.

Syntax: REMOVE header

Example: REMOVE Return-receipt-to:

Removes all headers of the given type from the message. Case is not significant when matching header names. The terminating colon is required.

Syntax: REWRITE header AS headertemplate

Example: REWRITE X-Sender: AS X-OriginalSender: %v

Replaces the first occurrence of the header with the header template. In the header template, the following combinations have effect: %% is replaced by a single %; %v is replaced by the original value of the header; %d is replaced by the current date and time.

Syntax: IFPRESENT header GOTO label Example: IFPRESENT Cc: GOTO ccpresent

If the header is present in the message, continue processing the script commands from the label. If the mailing list is not "trusted" (see above), only "forward" gotos are possible, to eliminate the possibility of an infinite loop.

Syntax: IFABSENT header GOTO label Example: IFABSENT Cc: GOTO ccabsent

If the header is not present in the message, continue processing the script commands from the label. If the mailing list is not "trusted", only "forward" gotos are possible, to eliminate the possibility of an infinite loop.

Syntax: IFCONTAINS header text GOTO label Example: IFCONTAINS Subject: xyz GOTO alabel

If the header is present in the message, and the value of the header contains (as a substring) text, continue processing the script commands from the label. (Note that the text may not contain white space.) If the mail list is not "trusted" (see above), only "forward" gotos are possible, to eliminate the possibility of an infinite loop.

Syntax: ABORT [recipient]

Example: ABORT postmaster@mydomain.com

The message is not sent to the mailing list. If the optional argument recipient is present, the message is forwarded to that address.

Syntax: :label Example: :ccpresent

A colon introduces a label, which can be the target of an IF... GOTO command, as previously described. Label names may not contain space - everything after the space is ignored.

Note that after the mailing list header script has been executed, the mailing list processor will do its own, built-in header processing. It will rewrite any Sender: headers as Original-sender: and add its own Sender: field. (This is to help prevent mailing list loops - your mailing list script should never remove any Original-sender: or Sender:

headers, otherwise disastrous mailing loops can result.) If the Reply to list feature is enabled, the mailing list processor will add a Reply-to: field if there isn't one already present.

You should be aware that there are certain headers that can cause Message Delivered acknowledgement messages to be sent. It is a good idea to remove these headers using a script. As a minimum, therefore, your script should contain:

REMOVE Return-receipt-to: REMOVE X-Confirm-reading-to: REMOVE X-pmrqc:

Appendix D - Database Plugin Examples

The current external database connectors use a 64-bit ODBC data source. A database used for account or list membership is independent of the connector storing MailSite's own configuration. Use a separate test source to verify table names, returned columns, eligibility filters and service-account permissions before changing production.

Generic mailbox source

Map the table and mailbox, full-name and password columns in Server, External Database Mailboxes. An optional domain column restricts the source to the selected domain; an eligible-user filter can exclude disabled rows. Preview saved source reports eligible and existing accounts and name collisions before Create selected creates accounts.

Do not point a password field at an arbitrary password-hash column. The supported Generic contract uses source password values. Existing native accounts are not overwritten by provisioning, and removal or disabling in the source prevents authentication without deleting existing MailSite data.

Database list source

A custom membership query returns an email address as the first column and an optional display name as the second. The default table supplies EmailAddress and FullName. Use a SELECT appropriate to the actual schema; returned addresses are validated and deduplicated.

Example join statement for a schema that permits an EmailAddress-only insert:

```
INSERT INTO %2 (EmailAddress) VALUES (%1)
```

Example leave statement:

```
DELETE FROM %2 WHERE EmailAddress = %1
```

The connector supplies %1 as a quoted address and %2 as the derived table name. %% produces one percent character. Validate both statements against the actual schema and permissions. The legacy SQL-to-set-member-property command is not executed; external names remain source-managed.

Failure and migration behavior

An unavailable source is an error, not an empty account or member set. Database queries have bounded timeouts and result limits. Preserve existing mail when correcting a source; do not delete mailboxes to repair connectivity. Custom database DLLs and dependencies on legacy member-property updates require a separate migration approach.

Appendix E - Database Logging

The v10 guide described direct ODBC inserts into a MailLog table, using a database destination bit in each log category and positional SQL substitutions. The current Rust logging runtime writes structured file and console output; it does not implement that direct ODBC destination. The Database Log configuration fields remain available for migration, but saving them does not create or populate an external log table.

Current logging workflow

Use the Console log viewer and service logging controls, and inspect files in the configured MailLogDir. Identify a problem by service, timestamp, mailbox/recipient and message or request identity. Increase logging for the affected service when reproducing a problem, then restore the intended operational level. Detailed message/protocol logs can contain private content and should have restricted access and retention.

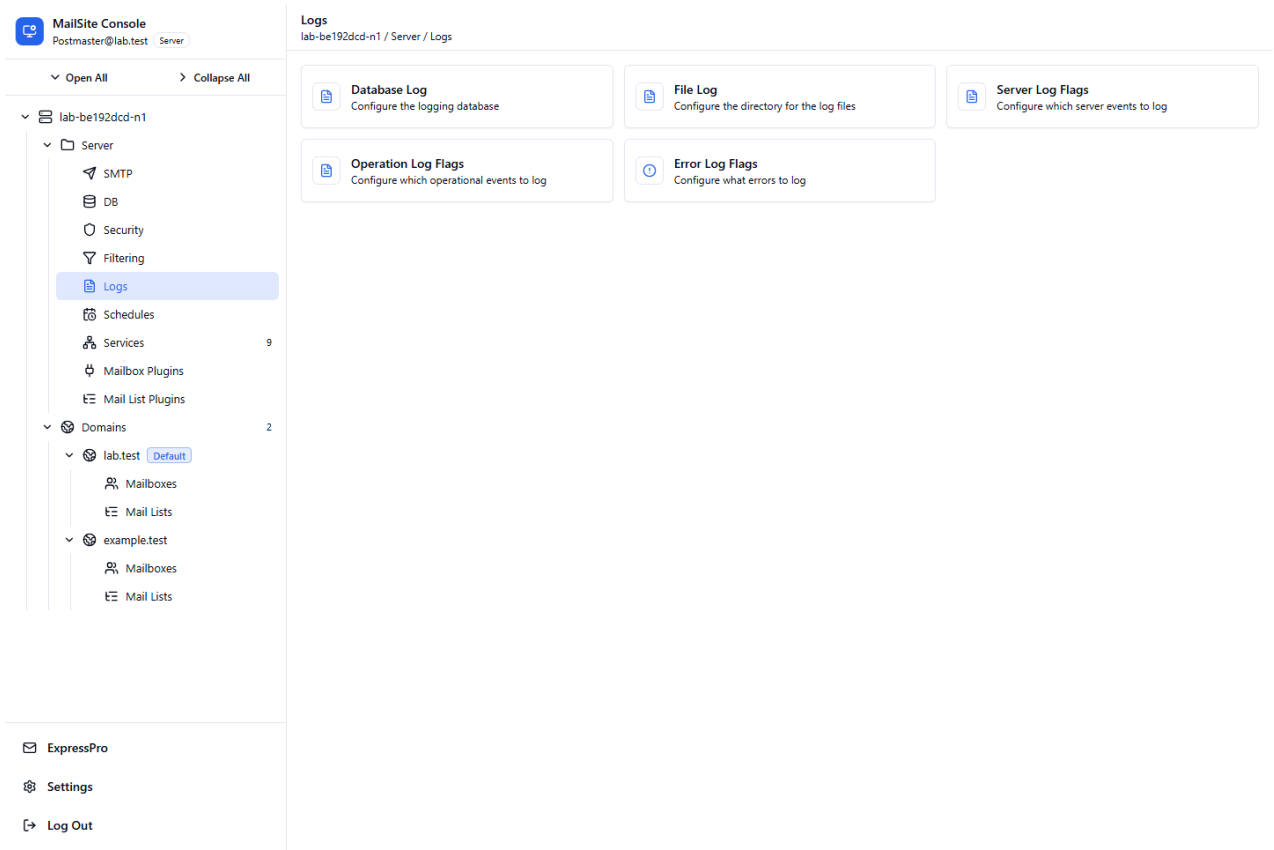

Figure 138 Current Console log viewer

Migrating database log consumers

Retain old database tables and reporting definitions as historical records. If reporting requires an external database, use a separately verified log-collection/import integration appropriate to the current event fields. Do not apply the old Microsoft Access wizard or positional INSERT template and assume the v11 services will execute it.

The original MailSite 10 manual retains the old MailLog schema and examples for installations still running that version. The active SQL configuration connector and external mailbox/list databases are unrelated to this retired logging destination.

Appendix F - Emerald Integration

Emerald mode connects external customer/user records to MailSite accounts. Configure the 64-bit ODBC data source, user, password, login/query timeouts and ESID in Server, External Database Mailboxes, then choose Emerald as the database type.

The connector uses ListMailUsers to discover users and VerifyMailUser to verify current eligibility and authentication data, with the retained column contract (full name in column 0 and password in column 4 for verification). ChangeMailUserPassword supplies the supported password-change operation. Test these procedures and their permissions against the installed Emerald schema; similarly named custom procedures are not automatically compatible.

Preview the chosen domain, inspect collisions and existing accounts, and create selected eligible accounts. Enable automatic creation only for intended domains. Repeated provisioning preserves existing accounts; disabling an external user removes login access without implicitly deleting stored mail.

The current workflow replaces the old native database-user wizard. It is separate from choosing SQL as MailSite's configuration connector. Keep the old source and a recoverable MailSite backup until authentication, delivery and required client workflows have been checked after migration.

Appendix G - Service Command Line Syntax

The MailSite 11 executables have service-specific command-line options. Use the installed executable's --help output for its exact build. Do not apply the older POP3A switch list to every service.

Service management

Use the MailSite installer for service registration and the Console or Windows service management tools for normal start, stop and restart operations. Stop services that depend on MSDBMA before stopping MSDBMA itself; start MSDBMA first.

Development operation

The repository's development launcher creates isolated configurations and starts services as owned local processes. It is suitable for development and documentation capture without installing production services. It is not a substitute for the production installer.

Appendix H - IMAP4 ACLs

Access-control lists determine which other users can discover or operate on a folder. Use supported client sharing/permission controls or the supported IMAP ACL operations with an authorized account. Verify the resulting access from the recipient's own session; owner access is not a test of another user's permissions.

Folder identity and storage

MailSite 11 keeps current mailbox and collection state through MSDBMA. Live message files remain part of the store, while current indexes, identities and synchronization state are managed in the v11 databases. The legacy folder.imp file is an import/projection format, not the sole current authority for flags and message identities.

Do not edit folder.imp, keyword.imp, subscrib.imp or ACL files manually while services run. Their legacy layout is not a complete guide to current storage, and deleting them does not define a safe reset. Use the documented backup and service-supported mutation paths.

Shared folders

The server resolves shared-folder access through the owner's mailbox, the requested collection and the caller's effective rights. A folder shown in one client may not use the same display path in another. Discover the shared namespace through the current client or protocol responses rather than constructing physical directory names.

Verify permissions

Test discovery, read access and any permitted creation, flag change, deletion or administration operation separately. Revoke access and check a fresh recipient session. Keep protocol/client limitations distinct from the underlying permission policy. See the current release notes when validating an upgrade or a development database reset.

IMAP ACL commands

GETACL retrieves a folder's access-control list. MYRIGHTS reports the current caller's effective rights. LISTRIGHTS reports the rights that can be assigned to an identifier. SETACL changes that identifier's rights, and DELETEACL removes its explicit entry. Administrative operations require the folder's administer right; authentication alone is insufficient.

SETACL accepts a rights string to replace an entry, a leading + to add rights, or a leading - to remove rights. The current rights alphabet is lrswipkxtea: lookup, read, seen-state changes, other flag changes, insert, post, create child folders, delete a folder, set deleted flags, expunge, and administer respectively. Check MYRIGHTS from the recipient's session after changing access, including any inherited or default access.

Use the mailbox name returned by the server's namespace/listing responses and the intended account identifier. A protocol success confirms the requested ACL operation; it does not prove that a particular client supports every shared-folder workflow.

Appendix I - SMTP Protocol

SMTP separates message submission from eventual delivery. The server greets a connection, the client identifies itself with EHLO (or HELO), then submits an envelope sender with MAIL FROM and one or more recipients with RCPT TO. After DATA, message bytes end with a dot on a line by itself; dot-stuffing protects body lines that start with a dot.

The envelope sender is the return path for delivery reports and need not equal the message's From header. Recipient acceptance depends on local account/list resolution, relay policy, authentication and other configured controls. A 250 response after message data means the server accepted responsibility for the queued message; it does not prove the final recipient has received it.

Capabilities and transport security

Use the extensions advertised by the actual EHLO response and listener configuration. STARTTLS upgrades an eligible connection; after TLS, obtain the current capabilities again. AUTH authenticates the client but does not itself encrypt the connection. Use TLS and the configured submission policy when sending credentials.

SIZE, recipient limits, policy failures and other advertised features depend on the current server settings. Do not assume an extension is enabled because another server or a retained v10 transcript advertised it.

Diagnose a transaction

Record the exact command stage and response. A 4xx failure is temporary; a 5xx failure is permanent for that attempted operation. A rejection of one recipient does not imply that other accepted recipients failed. Follow queued delivery in SMTPDA and the recorded recipient outcome when investigating later remote failures or delivery reports.

Use disposable recipients for protocol tests. VRFY, ETRN and relay behavior are controlled by server policy; do not enable them broadly merely to reproduce an old example.

Appendix J - Event IDs

The original v10 manual lists numeric Windows Event Log and database-log event IDs for the native services. The current Rust services use structured logging categories and service-specific messages. Those old numeric IDs are not a complete catalog of current errors and should not be used as the only monitoring filter.

Use Console, Logs to identify the service, timestamp, operation and related account/message/request. Preserve the complete error context when diagnosing an incident, including a wrapped operating-system or storage error. Log categories and configured destinations are described in Monitoring and Appendix E.

Retain old numeric-ID mappings only for historical logs or components that explicitly emit those formats. The unchanged MailSite 10 reference contains the original event table.

Appendix K - Glossary

Agent: An external program invoked at a supported processing point. Server, mailbox, ordinary-list and request-list programs have separate settings; see Agents for execution and retry behavior.

Alias: A rule that redirects a matching delivery address to another address. Server maps and SQL mailbox aliases are separate forms.

Auto-reply: An auto-reply is a message that is automatically sent in response to mail received by a mailbox. Auto-reply messages are typically used to distribute frequently requested information, or to alert senders that you'll be away from your e-mail for a few days and won't be able to immediately respond.

Cluster: A cluster is a group of computers that act as a unified system. MailSite's clustering allows multiple server machines (knows as nodes) to host mailboxes for a single domain.

DNS: Domain Name Service (DNS) is a name lookup service that translates familiar internet names (such as ibm.com) into numeric TCP/IP addresses (such as 129.34.139.30) that computers understand.

Digest: A digest is a collection of messages sent to a mail list that is distributed as a single e-mail. Digests are convenient because they allow users to receive one large message instead of having their mailbox cluttered with dozens of messages.

ESMTP: ESMTP stands for Extended SMTP. ESMTP defines a number of extensions to the SMTP protocol as defined in RFC1854, RFC1869 and RFC1870.

Event Log: The Windows NT Event Log records operating system errors, events and incidents. You can use the Event Viewer to review the entries in the event log. The Event Viewer can open event logs on remote computers.

HOSTS: The Windows file at %WINDIR%\System32\drivers\etc\hosts supplies local host-name mappings. It does not publish DNS records or define MX routing for other systems.

HTML: HTML stands for Hyper Text Markup Language. HTML is the language of the World Wide Web. HTML is often used to present entry forms for users to enter and update information from their Web browser.

HTTP: HTTP stands for Hyper Text Transfer Protocol. This is the communication language of the World Wide Web. All Web clients and Web servers communicate using this protocol.

IMAP: IMAP stands for Internet Mail Access Protocol. IMAP is an Internet standard that advances the capability of POP. IMAP provides all of the functionality found in POP. In addition it provides access to a comprehensive message and folder store on the server. MailSite has implemented this standard in the IMAP4 Service.

Internet Mail Address: The standard format for an Internet Mail Address is user@host.domain, where user is the user account on the host that the mail message will be delivered to, host is the name of the mail host and domain is the name of the internet domain. This address standard is defined in RFC822. See the DNS Overview for more information on Internet domain naming.

Internet: The Internet is the global network of computers that communicate using the standard TCP/IP protocol. All mail on the Internet is delivered using the standard SMTP protocol.

LAN: Abbreviation for Local Area Network. This is the computer network internal to your organization.

Loop: A mail loop is an error condition that occurs when a message is repeatedly routed through the same mail systems. Loops typically result from errors in DNS setup.

Mailbox: An electronic mailbox is an individual e-mail account that typically corresponds to a person who uses it to send and receive mail.

Mail list: A mail list is a special e-mail account that forwards all received messages to the members of the list.

MIME: MIME stands for Multipurpose Internet Mail Extensions. MIME is an Internet standard defined in RFC1521. MIME defines the format for embedding multimedia object types, such as picture files, in standard SMTP mail messages.

Moderator: An address authorized by mailing-list moderation policy. It does not grant Console administration privileges. Console review of pending posts requires the corresponding domain or server administrator role.

Ping: Ping is a command line utility used to verify and diagnose TCP/IP operations. You can use Ping to verify network connectivity to another computer by entering: ping hostname on the command line. Ping will attempt to resolve the hostname to a TCP/IP address by connecting to the DNS server specified in the Control Panel: Network: TCP/IP configuration.

Postmaster: A postmaster is the e-mail administrator for an Internet site. Postmasters typically create and delete mailboxes, grant access privileges to other users, and generally run the e-mail system. E-mail administrators can typically be contacted at postmaster@domain.com.

POP: POP stands for Post Office Protocol. POP is an Internet standard defined in RFC1725. POP defines the language that computers use when transferring incoming mail messages from a mail server to a mail client over a TCP/IP network. MailSite has implemented this standard in the POP3A Service.

RAS: Windows Remote Access Service, used by the historical dial-up implementation. MailSite 11 does not establish or schedule RAS connections.

Registry: The Registry contains all of the information related to the hardware and software configuration of your computer. The mail server makes several entries in the Registry to record information about the mail services, the mail configuration and the mail users. The Registry entries are created and maintained through the Installation Wizard and the Console program. Do not make any direct changes to the registry unless instructed to do so by technical support.

RFC: Request For Comment (RFC) is the term for the standards setting process used by the Internet Engineering Task Force (IETF). Each Internet standard has a unique RFC number. For example, the Simple Mail Transfer Protocol (SMTP) standard is described in RFC821. A complete list of RFCs can be found at http://www.rfc-editor.org.

SMTP: SMTP stands for Simple Mail Transfer Protocol. SMTP is an Internet standard defined in RFC821. SMTP is an application level network protocol that runs on top of TCP/IP. It defines the language that computers use when transferring mail messages between machines over a network. The mail server has implemented this standard in the SMTPRA Service.

Sniffer: A sniffer is a program that captures data exchanged on the Internet. Sniffers can be used to capture sensitive information, such as mailbox passwords transmitted by e-mail clients.

Spam: Spam is the name commonly used to describe unsolicited commercial e-mail.

TCP/IP: TCP/IP is the acronym given to the suite of networking protocols that define the communication language between computers. The protocols originated in the UNIX world and have been ported to the Personal Computer, Minicomputer and Mainframe worlds. TCP/IP stands for Transmission Control Protocol / Internet Protocol. Each computer on a TCP/IP network has a name and address. The full name is similar to host.company.com where company.com is the domain name. The address is similar to 123.45.67.89. HOSTS tables or DNS servers provide the name to address conversions.

Appendix L – MailSite Properties

MailSite has multiple properties at server, domain and individual mailbox or maillist level. These can be stored either in the Registry or a database such as SQL Server.

Server Properties

Property reference: these tables preserve names used by existing configuration and scripts, including historical fields. Dial-up dispatch, direct ODBC logging and custom membership DLLs remain unsupported. Legacy Hypermail appearance properties are retained for migration; current static archives use the supported subset described in Appendix B. Change configuration through the Console or supported utilities; MSDBMA owns registry/SQL access.

Each server has multiple properties. These properties are identified in this table:

Property name	Type	Meaning
AcceptForRelayFrom	String	Comma-separated list of host name or IP address masks controlling which hosts can use the mail server for relaying mail to other domains.
AcceptForRelayTo	String	Comma-separated list of mail domain name masks controlling which other domains the mail server will relay to.
AcceptUnknownSmtpHosts	Integer	If non-zero, mail will be accepted from hosts with IP addresses which cannot be found in the DNS.
AlternateResentHeaders	Integer	Controls whether resent messages (i.e., messages which are autoforwarded from a mailbox) have the standard Resent-* headers or the alternate set of X-Resent-* headers.
ArchiveDir		
DefaultDomainName	String	The name of the default domain.
DeliveryTriggerCommand	String	Command line which is executed when the dialup connection is established.
DeliveryTriggerEnabled	Integer	Non-zero if the delivery triggers command is enabled.
DialupEnabled	Integer	Non-zero to enable dialup support.
DialupInitialWait	Integer	Time in seconds which will elapse after connection succeeds, before any delivery attempts are made.
DialupPassword	String	Encrypted password for the dialup server.
DialupTimeMax	Integer	Maximum duration in seconds of dialup connection.
DialupTimeMin	Integer	Minimum duration in seconds of dialup connection.
DialupUserName	String	User name for the dialup server.
LookupIncomingCalls	Integer	If non-zero, SMTPDA will look up the IP address of an incoming SMTP call in the DNS. The call will be rejected if the address is not found.
MailInBoxDir	String	The directory of the mail inbox
MaxSmtpRecipients	Integer	Maximum number of SMTP RCPT TO commands which will be accepted for a given message, or 0 if no limit.
NoDialupDomainMask	String	List of domains which use the elapsed time schedule.
NoRblForFriends	Integer	If true (non-zero), friendly sites from will not be looked up in the black list servers.
NoThirdParyRelay	Integer	If non-zero, RCPT TO commands which specify non-local addresses will be rejected, unless the preceding MAIL FROM command did specify a local address.
NoUnauthenticatedEtrn	Integer	This property controls the behavior of the SMTP "ETRN" command There are six possible values, as follows. 0 means ETRN is unconditionally allowed. 1 means it is allowed only if the connection is authenticated. 2 means allowed only if the host is "friendly". 3 means allowed if the connection is authenticated or the host is "friendly". 4 means allowed if the

Property name	Type	Meaning
		connection is authenticated or the host is "friendly". 5 means ETRN is not allowed.
NoUnauthenticatedRelay	Integer	If non-zero, RCPT TO commands which specify non-local addresses will be rejected, irrespective of other constraints, unless the call has been authenticated. Definition extended at verion 4.2.5 to permit three values; 1 implies the definition as above; 2 relaxes that constraint for mail received from hosts listed in the property ACCEPTFORRELAYFROM.
QuotaCopyPostmaster	Integer	This is non-zero if the postmaster is to be copied on quota warning messages.
QuotaFailPermanent	Integer	If true (non zero), mail for over-quota mailboxes Will be rejected with a permanent (552) reply code.
QuotaMinWarningMsgGap	Integer	This is the minimum period (in days) which is allowed to elapse between quota warning messages being generated.
QuotasEnabled	Integer	Enable the use of quotas.
RblDomain	String	The domain name which is appended to the host's IP address in order to do a lookup in the RBL.
RblEnabled	Integer	If non-zero, the RBL service will be looked up to see whether a remote host is a known spam originator.
RegistryFormatVersion	Integer	This is used to prevent a down-level configuration console from configuring an up-level mail server installation, and to enable an up-level configuration console to adapt to configure a down\level mail server installation.
RejectAllMailFrom	String	Comma-separated list of host name or IP address masks controlling which hosts can use the MAIL and VRFY SMTP commands.
RejectAllMailFromAddresses	String	This contains a comma-separated list of email address masks. If an incoming MAIL FROM command has a return address which matches one of these address masks, the command (and thus the message) will be rejected.
RetrySchedule	String	A string representing the retry schedule. The string consists of a number of comma-separated "tries". Each try consists of an interval in minutes, followed by a colon and the letter T (if a "delayed" message is to be sent on this try) or the letter F (otherwise). Note that this string is generated automatically by the configuration console based on the values of RetryInterval1, WarnAfterDays and FailAfterDays. The default value is thus based on the default values of those variables.
VrfyMode	Integer	If non-zero, then a VRFY SMTP command will elicit more information about whether name@domain.com is a mailbox or a mail list (or is unknown).
WConsoleCheckWebDirOnly	Integer	If non-zero, WConsole will search for template files only in the default web directory for a given domain. Otherwise the mailbox directories will be searched first.
WeekdaySchedule	String	Time-of-day delivery schedule for weekdays. Format: comma-separated list of times in HHMM format, each optionally followed by "u" to indicate unconditional dialup.
WeekendSchedule	String	Time-of-day delivery schedule for weekdays. Same format asWeekdaySchedule.

Domain Properties

Each domain has multiple properties, most of which can be accessed using utilities such as MSDOMAIN. These properties should always be changed via the MailSite Console unless directed by a MailSite KB document or the MailSite support staff:

Property name	Type	Meaning

Property name	Type	Meaning
CalendarRemit	integer	Whether calendaring is allowed for this domain: 0 – Enabled for all mailboxes, 1 – Disabled for all mailboxes, 2 – Enabled for configured mailboxes.
DisableDomain	integer	When set, indicates that a domain is disabled. The MailSite Console still works, but messages sent to the domain will be rejected and logins for users in this domain will fail.
DMC_AutoCreate	integer	DB Mailbox specific (not SQL mailboxes). Whether auto-creation is allowed.
EnabledContactPlugins	integer	The contact plugins enabled for this domain. Value is used by ExpressPro to determine which contacts to display. A bitmask value comprising of: 0x01 - Personal Address Book, 0x02 – MailSite Express Contacts, 0x04 – Userstore Contacts, 0x08 – Mail Header Contacts.
EnabledCalendarPlugins	integer	The calendar plugins enabled for this domain. Value is used by ExpressPro to determine which events to display. A bitmask value comprising of: 0x00 – Undefined Calendar, 0x01 – Personal Calendar, 0x04 – Webcal Calendar.
ForwardingEnabled	integer	Enable domain forwarding. If this flag is set, non-local mail sent to this domain will be forwarded to the host specified in ForwardingHost.
ForwardingHost	text	The domain name of the host to forward non-local mail to.
GreylistRemit	integer	Whether greylisting is allowed for this domain: 0 – Scan all mail, 1 – Scan no mail, 2 – Scan configured mailboxes. Greylisting is dependent on Spam Scanning, and so if Spam Scanning is disabled, greylisting is disabled, whatever the setting here.
HostName	text	The host name to use when sending outbound mail from this domain.
IMAPBytesReceived	integer	Number of bytes received by IMAP for users in this domain since last statistics reset.
IMAPBytesSent	integer	Number of bytes sent by IMAP for users in this domain since last statistics reset.
LocalFailuresToPostmaster	integer	Enable mail delivery failure notification to the postmaster.
MailInBoxDir	text	Inbox directory location.
MailListDir	text	Mail list directory location.
MaxMailboxes	integer	Maximum number of mailboxes allowed for a domain.
MaxMailLists	integer	Maximum number of mailing lists allowed for a domain.
MF3_DontUseDefault	integer	If this flag is not set, the domain will use the message banners of the default domain. If set, the banners specific to the domain will be used.
MF3_HeaderPlain	text	The text Header insert set for a domain.
MF3_HeaderHtml	text	The HTML Header insert set for a domain.
MF3_FooterPlain	text	The text Footer insert set for a domain.
MF3_FooterHtml	text	The HTML Footer insert set for a domain.
MultiLevelMailboxDirs	integer	True/False value for multi-level directory structure.
NMC_AutoCreateGroupName	text	NT Mailboxes specific. Auto-create group name.
NMC_AutoCreateGroupType	int	NT Mailboxes specific. Auto-create group type.
NMC_EnableAutoCreate	int	NT Mailboxes specific. Whether auto-creation is enabled.
POPBytesReceived	integer	Number of bytes received by POP for users in this domain since last statistics reset.
POPBytesSent	integer	Number of bytes sent by POP for users in this domain since last statistics reset.
QuotaDefaultLimit	integer	Default mailbox quota limit for the domain.
QuotaDefaultTrigger	integer	Default quota warning trigger value.
QuotaLastChecked	integer	Time stamp the quota was checked last by the system.
QuotaLimit	integer	Maximum domain capacity, Kb. Zero means no limit. 0xFFFFFFFF means "use the server level settings". Default: 0xFFFFFFFF

MultiLevelMailboxDirs	integer	True/False value for multi-level directory structure.
QuotaLimitTime	integer	A number indicating the last time a "quota exceeded" message was sent.
QuotaMsgSize	integer	Size on disk of all the messages in this domain.
QuotaNoMsgs	integer	Number of messages in the message store for this domain.
QuotaRealTime	integer	Whether the domain's quota is updated in real time. This is a burden on the system and so is strongly discouraged for busy or large domains.
QuotaTotSize	integer	Total size of this domain on disk. This is bigger than the QuotaMsgSize, as it includes all the meta information like folder subscription or IMAP message flag files.
QuotaTrigger	integer	Domain capacity which, if exceeded, causes a warning message to be sent. Zero means no warning. 0xFFFFFFFF means "use the server level settings". Default: 0xFFFFFFFF
QuotaTriggerTime	integer	A number indicating the last time a "approaching quota" message was sent.
RCPTCommands	integer	The number of "RCPT to" SMTP commands seen for this domain since the last statistics reset.
SieveScript	text	The Sieve filtering script associated with the domain.
SMTPBytesReceived	integer	The number of bytes received by SMTPRA for this domain since the last statistics reset.
SMTPBytesRelayed	integer	The number of bytes relayed by SMTP for users in this domain.
SMTPBytesSent	integer	The number of bytes sent by SMTPDA from this domain since the last statistics reset.
SpamScanningRemit	integer	Whether spam scanning is allowed for this domain: 0 – Scan all mail, 1 – Scan no mail, 2 – Scan configured mailboxes
StatisticsDate	integer	Timestamp indicating the age of the domain statistics currently held.
VirusScanningRemit	integer	Whether virus scanning is allowed for this domain: 0 – Scan all mail, 1 – Scan no mail, 2 – Scan configured mailboxes
WebDir	text	Holds the directory to use for web directory location such as the hypermail list archives.

Mailbox Properties

Each mailbox has many properties, most of which can accessed via utilities such as MSBOX. These include basic mailbox properties, such as mailbox quota and auto-reply parameters, as well as directory information and web preferences affecting MailSite Express, MailSite ExpressPro and Calendaring. This table reflects the core mailbox properties, while following tables describe the directory and web properties.

These properties should always be changed via the MailSite Console unless directed by a MailSite KB document or the MailSite support staff.

Property name	Type	Meaning
AlienPassword	text	Password inherited from a legacy non-MailSite system
AlienPasswordType	integer	Indicates the type of legacy password. The possible types are not documented here. Please contact MailSite Support for more information.
AlreadyRepliedTo	text	List of addresses that have already received an auto reply.
CommandLine	text	Command line to execute when a message is received.
DontDeliver	integer	Don't deliver mail to this user.
EchoMessage	integer	If non-zero, include the original message in auto replies.
EnableAutoReply	integer	Automatically reply to incoming mail messages.
ForwardTo	text	Forward all messages to this address.
FullName	text	Full name of mailbox user.
GreylistType	integer	One of the greylist settings. Usually unset at present.
IMAPBytesReceived	integer	Number of bytes received by IMAP for this user since last statistics reset.

Property name	Type	Meaning
IMAPBytesSent	integer	Number of bytes sent by IMAP for this user since last statistics reset.
LastLoginTime	integer	Date stamp of the last mailbox login action.
MailboxDirectory	text	Full path to mailbox directory. Read only.
MailboxDomain	text	The domain of the mailbox, or the empty string if the mailbox is in the default domain. Read only.
MailboxDomain2	text	The domain of the mailbox. If the mailbox is in the default domain, the name of the default domain is returned. Read only.
MailboxName	text	The name of the mailbox. Read only.
Message	text	Text of the auto-reply message.
MobileCarrierId	integer	Indicates the mobile carrier for notifications to this user. ID is linked to the MAILSERVER_MOBILECARRIERS list.
MobileCapability	integer	Indication of whether the mobile device requires a specially formatted message.
NoReplyTo	text	Do not auto-reply to this list of addresses.
OtherMailbox	text	Alternative e-mail address for mailbox user.
Password	text	User's password. Not available via MailSite utilities for security reasons.
PluginId	integer	Indicates the plugin type associated with this mailbox such as Registry, DB or SQL. Only modify via the Windows Console.
POPBytesReceived	integer	Number of bytes received by POP for this user since last statistics reset.
POPBytesSent	integer	Number of bytes sent by POP for this user since last statistics reset.
Privilege	integer	Privilege level: 0 - not privileged; 1 - domain-wide privilege; 2 - server-wide privilege.
QuotaLastChecked	integer	A number indicating the last time a quota check was run.

Property name	Type	Meaning
QuotaLimit	integer	Maximum mailbox capacity, Kb. Zero means no limit. 0xFFFFFFFF means "use the DOMAIN_QUOTADEFAULTLIMIT Domain Property". Default: 0xFFFFFFFF
QuotaLimitTime	integer	A number indicating the last time a "quota exceeded" message was sent.
QuotaMsgSize	integer	Total size in Kb of messages in the mailbox. This is a cached value and may not always be accurate.
QuotaNoMsgs	integer	Total number of messages in the mailbox. This is a cached value and may not always be accurate.
QuotaTotSize	integer	Total size of all files in the mailbox. This is a cached value and may not always be accurate.
QuotaTrigger	integer	Mailbox capacity which, if exceeded, causes a warning message to be sent to the mailbox. Zero means no warning. 0xFFFFFFFF means "use the DOMAIN_QUOTADEFAULTTRIGGER Domain Property". Default: 0xFFFFFFFF
QuotaTriggerTime	integer	A number indicating the last time a "approaching quota" message was sent.
RCPTCommands	integer	The number of "RCPT to" SMTP commands seen for this mailbox since the last statistics reset.
ReplyFrom	text	Use this address as the From: field in auto-reply messages.
ReplyOnce	integer	If non-zero, don't auto-reply to addresses which have already received auto-replies.
ServiceExpress	integer	Non-zero if the user is permitted to use MailSite Express.
ServiceImap	integer	Non-zero if the user is permitted to use the IMAP service.
ServiceLdap	integer	Non-zero if the user is permitted to use the LDAP service.
ServiceMailma	integer	Non-zero if the user is permitted to use the MAILMA service.
ServicePop	integer	Non-zero if the user is permitted to use the POP service.
ServiceSmtp	integer	Non-zero if the user is permitted to use the SMTP service.
ServiceWconsole	integer	Non-zero if the user is permitted to use the Web Console.
SieveScript	text	The Sieve filtering script for the mailbox.
SMSEnabled	integer	When set, indicates that SMS notifications can be sent according to the

Property name	Type	Meaning
		relevant sieve filter rules.
SMTPBytesReceived	integer	The number of bytes received by SMTPRA for this user since the last statistics reset.
SMTPBytesSent	integer	The number of bytes sent by SMTPDA from this user since the last statistics reset.
SpamScannerType	integer	The type of Spam Scanner. 1 – Default Engine.
StatisticsDate	integer	Timestamp indicating the age of the mailbox statistics currently held.
Trusted	integer	Non-zero if the mailbox is trusted.
VirusScannerType	integer	The type of Virus Scanner. 1 – Default Engine.

Mailbox Directory Properties

Each mailbox has a set of directory properties, which are made available to users through MailSite's LDAP server:

Property name	Type	Meaning
City	text	City (part of mailbox user's postal address).
Comment	text	Comment describing mailbox user.
Country	text	ISO two-letter Country code (part of mailbox user's postal address).
Facsimile	text	Fax phone number for mailbox user.
GivenName	text	Given name (part of mailbox user's personal name).
HomeAddress	text	Freeform postal address of mailbox user's home.
HomeCity	text	City location of mailbox user.
HomeCountry	text	Country location of mailbox user.
HomePhone	text	Telephone number of mailbox user.
HomePostCode	text	Postal code of mailbox user.
HomeState	text	State or Region of mailbox user.
HomeStreet	text	Street name of mailbox user.
Manager	text	Name of the mailbox user's manager.
MiddleInitial	text	Middle initial(s) (part of mailbox user's personal name).
Mobile	text	Telephone number of mailbox user's mobile phone.
Organization	text	Company to which the mailbox user belongs.
OrgUnit	text	Department within the company to which the mailbox user belongs.
Pager	text	Telephone number for mailbox user's pager.
PostalAddress	text	Freeform postal address of mailbox user.
PostCode	text	Postal or ZIP code (part of mailbox user's postal address).
State	text	State or region (part of mailbox user's postal address).
Street	text	Street (part of mailbox user's postal address).
Surname	text	Surname (part of mailbox user's personal name).
Telephone	text	Telephone number of mailbox user.
Title	text	Job title of the mailbox user.
URL	text	URL of mailbox user's home page.

Mailbox Web Properties

Each mailbox has a set of web related properties, which define preferences for the user in MailSite Express, MailSite ExpressPro, and Calendaring:

Property name	Type	Meaning
AliasAddress	text	Alias address set in the general options
CalendarFeatures	integer	Indicates the calendar features active for this mailbox. A bitmap using the following defines: 0x00000000 – none, 0x00000001 – WSS, 0x00000002

Property name	Type	Meaning
		– Webcal publish, 0x00000004 Webcal subscribe, 0xFFFFFFFF – all calendar features. Default is all calendar features.
CalendarType	integer	Whether calendaring features are on or off. Default is on.
CharSet	text	Default language character set used by the mailbox
DayViewEnd	integer	Sets calendar default end date.
DayViewStart	integer	Sets calendar default start date.
DefaultCalendarView	text	Sets default calendar view mode.
DefaultPersonality	text	Selects default personality used when composing a message
DeleteConfirm	integer	Toggle delete confirm action. If set to 1, messages are sent to trash automatically.
DeleteToTrash	integer	Toggle delete to trash action. If set to 1, messages will be deleted permanently.
Display	integer	Number of messages to be displayed in the message list
DraftFolder	text	Sets the default draft folder name
EnabledContactPlugins	integer	The contact plugins enabled for this mailbox. Value is used by ExpressPro to determine which contacts to display. A bitmask value comprising of: 0x01 - Personal Address Book, 0x02 – MailSite Express Contacts, 0x04 – Userstore Contacts, 0x08 – Mail Header Contacts.
EnabledCalendarPlugins	integer	The calendar plugins enabled for this mailbox. Value is used by ExpressPro to determine which events to display. A bitmask value comprising of: 0x00 – Undefined Calendar, 0x01 – Personal Calendar, 0x04 – Webcal Calendar.
ExternalEmail	text	External POP3 email address
ExternalHost	text	External POP3 email server address
ExternalIndicator	text	ID of the indicator to be used for indicating external account pop mail
ExternalLeaveMail	text	Leave messages on remote server action
ExternalPassword	text	External email user password
ExternalPort	text	External email server port, default is port 110
ExternalStorage	text	Folder name to store external mail.
ExternalTimeStamp	text	Date time stamp of external message.
ExternalUserName	text	User name of eternal email account.
NewWinExtension	text	A comma de-limited list of file extensions that cause attachments with the specified extensions to opened in a new window.
NotifySound	text	New mail notification sound.
PersonalityDisplayName	text	Personality name display.
PersonalityEmailAddress	text	Personality email address.
PersonalityHandleReply	text	Use personality when replying to messages to this address.

Property name	Type	Meaning
PersonalityName	text	Personality name.
PersonalityReplyTo	text	Reply to address for personality.
PersonalitySignature	text	Personality signature value.
PersonalitySignatureEnable	text	Personality signature enable/disable.
PersonalizationExpress	text	Contains user information relating to information such as timezone.
RefreshInterval	integer	Refresh time interval.
ReplyInclude	integer	Include original message.
SaveOutgoing	integer	Save outgoing message by default.
SentFolder	text	Sent items folder.
SortBy	text	Sort messages by name, date, or subject.
SortOrder	integer	Alphabetic sort order of messages.
SpellCheckLanguage	integer	Numeric value for available language dictionary.
SpellCheckOptions	integer	Option values for spell checker.

Property name	Type	Meaning
TrashFolder	text	Trash folder name.
UserLanguage	text	Default user language.

Mail List Properties

Each mail list has multiple properties. These properties are identified in this table:

Property name	Type	Meaning
BounceAction	integer	A value of 1 indicates that non-delivery reports resulting from messages to this list should go to the original sender. Any other value indicates that the non-delivery reports should go to the BouncesTo address.
BouncesTo	text	Address to send non-delivery reports for list messages.
CommandLine	text	Command to be executed when messages are received by the list.
ConfirmToSender	integer	If set to 1, the sender of a message to the mail list will receive a confirmation message containing a copy of the message which went to the list. If the sender is also a member of the list, she will not receive another copy by virtue of her membership. If set to zero, no confirmation will be sent, and if the sender is a member of the list, she will receive a copy of her message by virtue of that membership. Default: 1.
DigestContents	integer	Non-zero if digest messages sent to list members should be preceded by a table of contents.
DigestFrequency	text	Frequency of digest messages, in the format nu, where n is a number and u is one of H (hours) or D (days).
DigestMessageNo	integer	Running counter of the number of messages digested so far.
DigestSubject	text	Template to be used for Subject: header in digest messages.
Disable	integer	If non-zero, new messages to the list or the list-request address will be rejected.
EnableExtendedCommands	integer	Non-zero if the extended format of the JOIN and LEAVE commands are allowed.
EnableReview	integer	Non-zero if the REVIEW command from the moderator will be accepted.
GoodbyeMessageDirectives	text	Text and directives for goodbye message.
GoodbyeMessageSubject	text	Subject for goodbye message. Default: "Goodbye".
HeaderScript	text	Header processing script for the list.
HelpMessageDirectives	text	Text and directives for help message.
HelpMessageSubject	text	Subject for help message. Default: "Help information".
HypermailEnabled	text	If set, then an archive will be kept for a mail list.
HypermailDir	text	Directory where the archive for a list will be written to
HypermailMailCommand	text	Creates links in the archives to mail addresses. The default is: mailto:$TO?subject=$SUBJECT, where $TO is replaced by an email address and $SUBJECT by the subject.
HypermailOtherArchivesURL	text	Other archives URL.
HypermailAboutArchivesURL	text	URL to page describing archive.
HypermailHeaders	text	Set to show headers in the articles.
HypermailInlineTypes	text	Which image mime types should be inlined for display.
HypermailIgnoreTypes	text	A list of MIME attachments that are quietly ignored.
HypermailDefaultIndex	text	Either author, date, subject or thread listing.
HypermailReverseIndex	integer	Set to put the most recent message at the top of the indexes.
HypermailHideHeaders	text	Set to hide headers in the articles.

Property name	Type	Meaning
HypermailShowBr	integer	Set for after each line of the message.
HypermailItalicQuotes	integer	Set for quoted lines to be in italics.
HypermailThrdLevels	integer	The number of thread level indents.
HypermailEuroDate	integer	Define as 1 to use European date format "DD MM YYYY", default is 0 to use American date form.
IgnoreCommandsFrom	text	Comma-separated list of address masks controlling who can submit commands to the list processor.
IgnoreMessagesFrom	text	Comma-separated list of address masks controlling who can submit mail to the list.
ListDir	text	The name of the directory that stores list messages. Read-only.
ListDomain	text	The domain of the mail list, or the empty string if the mail list is a member of the default domain. Read-only.
ListDomain2	text	The domain of the mail list. If the mail list is a member of the default domain, returns the default domain name. Read-only.
ListName	text	The name of the mail list. Read-only.
LocalLanguageJournal	integer	Non-zero if journal files for this list should record command output in your local language as well as in English. Not implemented in all builds.
LogRequestCommands	integer	Non-zero if commands to the list processor should be logged.
MaxMessageSize	integer	Maximum size of message which may be sent to the list (bytes).
MaxRecipients	integer	If non-zero, specifies the maximum number of recipients which will appear in an RCP file generated from this mail list. Multiple messages are created if the list contains more than this number of recipients. If zero, only one message, addressed to all the recipients, is created. Default: 0.
Members\Group	text	(NT lists only)
Members\GroupType	text	(NT lists only)
Members_MailboxMask	text	(Server lists only)
Members_DomainMask	text	(Server lists only)
Members_PrivilegeMask	integer	(Server lists only)
Members_File	text	(Text lists only)
Members_LoginTimeout	integer	(Database lists only)
Members_QueryTimeout	integer	(Database lists only)
Members_DataSourceName	text	(Database lists only)
Members_DataSourceUser	text	(Database lists only)
Members_DataSourcePass	text	(Database lists only)
Members_SqlStatement	text	(Database lists only)
Members_SqlJoin	text	(Database lists only)
Members_SqlLeave	text	(Database lists only)
Members_SqlSetMemberProperty	text	(Database lists only)
MessageFooterDirectives	text	Text and directives for end of message body.
MessageHeaderDirectives	text	Text and directives for top of message body.

Property name	Type	Meaning
Moderator	text	Comma-separated list of e-mail addresses of the list moderator(s).
ModeratorControlContent	integer	Non-zero if all list messages must be approved by the list moderator.
ModeratorControlJoin	integer	Non-zero if JOIN requests must be approved by the list moderator.
ModeratorControlLeave	integer	Non-zero if LEAVE requests must be approved by the list moderator.
NoMultipleCommands	integer	Non-zero if multiple commands in one mail message to the list processor are disallowed.
NotifyOnMemberLeave	integer	If non-zero, the list moderator will be informed (by e-mail) of a

Property name	Type	Meaning
		successful LEAVE request.
NotifyOnNewMember	integer	If non-zero, the list moderator will be informed (by e-mail) of a successful JOIN request.
ReplyToList	integer	Controls insertion of Reply-to: header. 0 - don't insert. 1 - insert if not present. 2 - insert, or replace if present.
RequestCommandLine	text	Command to be executed when messages are received by the list processor.
RequestDir	text	The name of the directory in which messages to the -request address are stored. Read-only.
SecureSubmission	integer	Non-zero if the SMTP authentication is required for submission.
Trusted	integer	Non-zero if this list is "trusted".
UserJoinAllowed	integer	Non-zero if a JOIN command to the list processor is supported for this list. Read-only.
UserLeaveAllowed	integer	Non-zero if a LEAVE command to the list processor is supported for this list. Read-only.
WelcomeMessageDirectives	text	Text and directives for welcome message.
WelcomeMessageSubject	text	Subject for welcome message. Default: "Welcome".
WhoCanSend	integer	Who can send messages to the list. 1 - members only. 2 - anyone. 3 - moderators only. 4- members and digest list members only.

Index