MailSite Fusion

Version 10

Rockliffe Systems Incorporated

Contents

Mail Lists 52

Domains 58

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

Welcome to MailSite™, the Rock Solid Internet Software™ from Rockliffe Systems Incorporated®

MailSite Fusion is a messaging server for Microsoft Windows platforms. MailSite Fusion allows your computer to host e-mail accounts, calendars, contacts and mail lists, to push that information over-the-air to mobile devices, and to communicate with other Internet mail servers and share calendars. MailSite Fusion is 100% compliant with Internet electronic mail standards, including the SMTP, POP3, IMAP4, iCalendar and LDAP3 RFC specifications.

MailSite's main job is to host *mailboxes*, which correspond to individual users. Each MailSite mailbox can be configured to forward mail to another address, and to automatically respond to incoming mail with a pre-defined message. You can create one or more *aliases* for each mailbox, allowing a single user to receive e-mail sent to multiple addresses. Users can access e-mail in their MailSite mailboxes with any POP3 or IMAP4 mail client, such as Microsoft Outlook, and can also use a web browser to manage their mail, contacts and calendars through the MailSite ExpressPro and MailSite Express webmail applications. Users can even manage their own mailboxes through a standard web browser.

MailSite Fusion optionally includes advanced calendar and address list support with the same data modifiable in Microsoft Outlook and a web browser through MailSite ExpressPro. Users can share their calendars with family, friends and colleagues and can view calendars shared by others, whether MailSite users or not.

MailSite Fusion also includes over-the-air mail, contact and calendar synchronization for the most popular leading mobile devices such as the iPhone, Android, BlackBerry, Windows Mobile, and Nokia smartphones, and now for Outlook 2013.

You can create *mail lists* on your MailSite server. Mail lists allow messages sent to a single e-mail address to be broadcast to any number of *members*. You can control the access and security of each list, and delegate mail list administrative duties.

MailSite Fusion includes extensive *spam blocking*, *virus detection*, and other SMTP security features. MailSite can automatically protect your site from destructive or offensive emails, denial-of-service attacks, and third-party relaying.

MailSite Fusion provides powerful mail *routing* capabilities. It can act as a staging post for mail destined for another host, which is useful for creating an e-mail proxy or relay server.

MailSite Fusion supports *virtual domains*, so you can configure a single MailSite server to send and receive mail for multiple domains.

MailSite Fusion also supports *dialup networking*, allowing your MailSite server to connect to your ISP or central office to send and receive mail intermittently.

MailSite Packaging Options

This MailSite administration guide covers the following MailSite products:

- MailSite Fusion SE (Small Enterprise)
- MailSite Fusion LE (Large Enterprise)
- MailSite Fusion SP (Service Provider)

MailSite Fusion SE - For Small-to-Medium Size Enterprises

MailSite Fusion SE is an affordable, easy to use standards-based email server for small businesses that includes a shared contact and calendar server and an ActiveSync server. MailSite Fusion SE is an award-winning Windows SMTP, POP and IMAP email server that also includes advanced anti-spam and anti-virus protection, powerful content filtering, multi-language webmail and push wireless email. MailSite Fusion works great with Outlook, Outlook Express, Eudora, Mozilla's Thunderbird and Sunbird and Apple's Mac Mail and iCal. It supports mobile devices such as the iPhone, BlackBerry, Windows Mobile and Nokia smartphones.

MailSite Fusion LE - For Large Enterprises

MailSite Fusion LE is high quality email server software that provides enterprises with an affordable, secure email server solution with anti-spam, anti-virus, shared calendar and mobile synchronization options that can be deployed in a load balanced cluster of email servers. Award-winning MailSite is a powerful Windows-based email server that has been meeting the performance, scalability and reliability requirements of service providers and enterprises since 1995. It includes an email server, list server, web client server, wireless synchronization server and a shared calendar server combined with a powerful arsenal of secure email services including anti-spam, anti-virus and SSL. MailSite Fusion LE offers a choice of easy to use, intuitive administration interfaces and is a cost effective alternative to Microsoft Exchange.

MailSite Fusion SP - For Service Providers

MailSite Fusion SP email hosting software provides carriers and service providers with a secure, clustered, scalable, high performance and fault tolerant SMTP, POP and IMAP email hosting platform. MailSite Fusion SP utilizes Microsoft SQL Server for its configuration and subscriber database to quickly and easily provision value-add services such as anti-virus, anti-spam, mobile device synchronization and shared calendaring.

MailSite Anti-Spam Filter

MailSite Anti-Spam Filter is an integrated part of the MailSite product line. It is a next-generation spam blocking solution that uses a “cocktail” approach of technologies to detect and eliminate spam. By providing end-user controls, false positives are avoided. MailSite Anti-Spam Filter analyzes email during processing, to identify spam before it's delivered. Configuration options allow end users to review their server-identified spam, or an automated server quarantine of spam can be used.

MailSite Anti-Virus Filter

MailSite Anti-Virus Filter is an integrated MailSite add-in that blocks viruses at their network entry point – the email server. This prevents them from getting past user defenses and protects corporate data. MailSite Anti-Virus Filter detects and removes viruses, worms and Trojans from incoming, outgoing and internal email traffic in real time, before viruses can enter or leave the network.

MailSite Calendar Server

The MailSite Calendar Server is a powerful and flexible collaboration platform. MailSite Calendar Server enables standards-based calendar sharing based on the iCalendar standard providing calendaring for many clients including Outlook, Vista’s Windows Calendar, Google Calendar, Mozilla’s Lightning/Sunbird and Apple’s Mac iCal. The server also supports native calendaring and contacts for Outlook.

MailSite ActiveSync Server

The MailSite ActiveSync Server works with the major smartphones to push email, calendar and contact updates over-the-air giving native support for many of the leading mobile devices. MailSite Fusion also includes a BlackBerry plug-in that can be quickly downloaded over-the-air to push email, calendars and contacts from the MailSite server.

MailSite Components

MailSite is comprised of three basic components: the *Engine*, which provides e-mail-related services, *Consoles*, which provide administrative access to configuration values and mailbox data, and webservices. MailSite webservices provide access to mailboxes through MailSite ExpressPro and MailSite Express webmail interfaces, the ActiveSync mobile device synchronization service and a service for Outlook connectivity.

Engine

At the heart of MailSite is the Engine, a series of services that allow MailSite to send, receive, and deliver e-mail messages. The Engine also includes services that provide access to mailbox and mail list configuration information, and others that allow end users to retrieve their mail. The Engine's services typically run continuously on your server machine, and are equivalent to UNIX daemons such as sendmail and pop3.

The Engine includes the following services, which can be started and stopped independent of each other:

- **SMTP Receiver Service**. The Receiver Service listens for incoming messages from other mail servers on the Internet. It stores incoming messages for processing by the Delivery Service.
- **SMTP Delivery Service**. The Delivery Service is the core of the Engine. It delivers mail addressed to local users to their mailboxes and forwards other mail out onto the Internet. It uses MX records from your DNS server for routing mail.
- **POP3 Service**. The POP Service allows users to download mail from their mailboxes to their own computer using a POP3 mail client, such as Microsoft Outlook.
- **IMAP4 Service**. The IMAP Service allows users to read mail in their mailboxes using an IMAP4 mail client. IMAP users can also create folders within their mailboxes to organize messages.
- **LDAP3 Directory Service**. The LDAP Directory Service allows users to search for names and addresses of other users who have mailboxes on your site. It is fully compatible with e-mail clients that support the LDAP3 protocol for address searches.
- **Calendar Service**. The Calendar Service allows users to access their calendar events either from Microsoft Outlook or any iCalendar compliant client. The same calendar data can be modified in MailSite ExpressPro. Managed as part of IIS.
- **ActiveSync Service**. The ActiveSync Service allows users to automatically synchronize mail, calendar and contacts over-the-air with leading mobile devices. Managed as part of IIS.
- **HTTP Management Agent**. The HTTP Management Agent allows administrators and users to remotely manage mailboxes and mail lists using a web browser. It is fully compatible with web browsers that support the HTML 2.0 and later standards, such as Microsoft Internet Explorer or Mozilla Firefox.
- **Mail Management Service**. The Mail Management Service allows you to remotely manage the mail server using the Windows Console. It also allows users of the Eudora mail client to change their password from Eudora.

Windows Management Console

The Windows Management Console is a Windows desktop application that allows you to configure all aspects of MailSite, including the Engine services, domains, mailboxes, and mail lists. Among the operations that you can perform in the Windows Console are starting and stopping services, setting security policies, setting delivery schedules, creating and modifying mailboxes, and creating and modifying mail lists. Although the Web Console provides access to managing mailboxes and mail lists, the Engine can be managed only from Windows Console.

The Windows Console can be installed on a different computer than the one that runs the MailSite Engine. This means that you can run the Engine on a large server system but still manage it from your desktop computer using the Windows Console. The Windows Console can manage multiple instances of MailSite, so if you have MailSite installed on two or more server machines, you can manage all of them from one Windows Console.

Web Management Console

The Web Management Console provides access to MailSite mailboxes and mail lists through a web browser, and can be used remotely. The Web Console supports Internet Explorer, and any other browser that supports HTML 2.0 and later. This interface is typically used by domain administrators, mail list moderators, and end users.

MailSite ExpressPro

MailSite ExpressPro is a cutting-edge version of MailSite Express based on AJAX technology. This web interface gives a desktop like look and feel making it a viable alternative to desktop clients such as Microsoft Outlook and Eudora. Message management is far more intuitive than in traditional webmail applications with drag and drop message filing and a desktop like folder tree.

MailSite ExpressPro supports multiple calendars whether stored within the MailSite database or externally. Contacts can be displayed from legacy MailSite Express accounts, those senders whose mail is currently in the Inbox, and other mailboxes on the same domain.

MailSite ExpressPro has been designed to make customization as easy as possible. As well as configuration options, the architecture includes “themes” so that each installation can have its own look, changing graphics to match organizational needs. Changing colors, labels and buttons is easy without detailed technical knowledge. More extensive changes are simple for those with common web skills.

MailSite Express

MailSite Express is a full-featured web-based mail client that allows users to access their mailboxes through a web browser from any computer on the Internet. This allows your users to send and receive e-mail even if they are away from their own computers. Users can also organize their messages into folders and maintain an address book. MailSite Express is implemented using HTML and JavaScript, and does not require any complex installation of Java or ActiveX controls. MailSite Express is compatible with Internet Explorer 6 (and above) and Mozilla Firefox 2 (and above).

MailSite Pocket

MailSite Pocket is an email client for Wireless Access Protocol (WAP) devices. MailSite Pocket allows users to access their mailboxes through any WAP-compatible device, such as cellular phones and other wireless Internet devices. Users can read messages, move messages between folders, and delete messages.

Key MailSite Features

This section provides an overview of some of MailSite's many features. If you are upgrading from a previous version of MailSite and want to know which features are new to this version, see the following section.

Extremely Scalable

MailSite can support an extremely large number of users, scaling to over 100,000 mailboxes on a single Windows server or on a cluster of servers. MailSite can also support over 100,000 members in a single mail list. Administrators can configure all MailSite servers in a cluster to be clones or to have specified roles (e.g. just inbound SMTP, just IMAP, etc.)

High Performance Engine

MailSite has a multi-threaded and multi-processing Engine that quickly and efficiently sends and receives large volumes of messages.

Rock Solid

MailSite is extremely reliable and has been engineered as Rock Solid Internet Software for sites where server down time cannot be tolerated.

Internet Standards

MailSite is based on open standards and protocols of the Internet, and is completely interoperable with other Internet mail systems. This means that MailSite does not require a gateway to communicate with remote Internet e-mail servers. MailSite is 100% compatible with the Internet RFC Standards for SMTP, POP3, IMAP4, iCalendar and LDAP3.

Collaboration

MailSite is a powerful and flexible collaboration platform. MailSite Calendar Server enables standards-based calendar sharing based on the iCalendar standard providing calendaring for many clients including Outlook, Vista's Windows Calendar, Google Calendar and Mozilla Lightning. The server also supports native calendaring and contacts for Outlook.

Mobile Device Synchronization

MailSite Fusion provides powerful over-the-air synchronization of mail, calendar and contacts for leading mobile devices such as the iPhone, BlackBerry, Windows Mobile and Nokia smartphones. All of this is possible without additional expensive middleware.

Native Outlook Support

MailSite Fusion allows the same mail, calendar and contacts to be accessed from a browser or Microsoft Outlook. Many other products require an Outlook plugin to be installed on every client machine creating a significant administration burden. MailSite Fusion works without any changes on client machines.

Anti-Spam Security

MailSite Software, Inc. has integrated the acclaimed spam-scanning engine from Mailshell into the MailSite server. MailSite uses a "cocktail" approach to spam filtering; combining a reputation index, profiles, keywords, white and black lists and greylisting to offer very sensitive and accurate spam filtering. This approach offers the advantage of analyzing email and identifying spam during processing, before it is delivered to the users' inbox.

As the Mailshell spam scanning engine analyzes messages, it calculates a spam score for each message based on a reputation index and techniques such as pattern matching. This language-agnostic approach makes the scoring of foreign-language spam more accurate than content based filtering. Regular updates to the spam engine ensure continued effectiveness against the changing tactics of spammers. The spam scores for each message can be used to determine how the message is handled by the system.

Anti-Virus Security

MailSite Anti-Virus Filter can automatically scan all incoming and outgoing mail for the presence of viruses. This allows your mail system to both block e-mail borne viruses before they enter your network, and protect your reputation by preventing viruses being sent out. MailSite's virus scanning facility is provided by AVG, one of the World's leading security software providers. The virus scores for each message can be used to determine how the message is handled by the system making this a powerful, flexible solution.

Message Filtering (Sieve rules)

MailSite Fusion includes *message filtering*. With filters, you can create sophisticated rules for handling incoming messages based on the contents of their headers, bodies, and attachments. It is also possible to act on the spam or virus score in a way appropriate to your system, a given domain, or even a certain mailbox.

Directory Harvest Attack Protection (DHAP)

MailSite Fusion includes the ability to protect corporate data and further reduce spam by detecting directory harvest attacks and automatically dropping the harvester's connection and blacklisting the IP address for a configurable period of time.

Spammers use directory harvest attacks to steal corporate directories from their victims. They use this information to make their subsequent spam attacks easier for them and more costly to recipients. In addition to the obvious spam problem, directory harvest attacks can cause performance degradation issues while the harvesting action is in progress. MailSite now detects these attacks and automatically drops inbound harvest connections, and then denies future connections to the sender. This safeguards sensitive corporate data.

MailSite includes powerful management tools for the DHAP probation lists with SQL based lists, white lists specific to DHAP checking and management interfaces.

Choice of Any Internet Mail or Calendar Client

MailSite Fusion adheres to Internet e-mail and calendaring standards and so your users can choose any desktop operating system and any RFC-compliant client to access their MailSite mailbox. For email, POP3 or IMAP4 compliant clients are supported, and for calendaring iCalendar compliant clients work well. For example, Mac Mail and iCal, Eudora, Mozilla Thunderbird and Lightning, Microsoft Outlook Express, Vista's Windows Mail and Windows Calendar and Microsoft Outlook all work very well with MailSite.

Windows and Web Management Consoles

MailSite Fusion provides two Management Console interfaces for managing mailboxes and mail lists, providing flexibility for both local and remote administration. These include a stand-alone application (Windows Console) and a browser-based interface (Web Console), both of which can be used to create, modify, and delete mailboxes and mail lists.

Multi-Level Administration Privileges

MailSite Fusion supports multiple levels of administration. In addition to the *server administrator*, who has access over all domains and mailboxes, you can assign *domain administrators*, who can manage only the mailboxes and mail lists in their domain. The administration of mail lists can be delegated to *mail list moderators*, who can define parameters associated with their lists, moderate membership requests, and moderate the content of list postings.

Mailbox Self-Administration

MailSite Fusion also allows end users to modify certain information related to their mailboxes. This allows each user to change their password, set delivery preferences, and enable a vacation message—all without requiring the help of the server administrator.

Custom Default Mailbox Properties

The configuration data associated with a mailbox are called mailbox properties. Common mailbox properties items include mailbox quota size, POP/IMAP/webmail access, or anti-virus and anti-spam scanning options. MailSite provides the ability to customize these default mailbox properties to ideally suit customer implementation requirements.

Mailbox property defaults can be modified through a special mailbox named MailboxTemplate, which is automatically created and located in the default domain. All mailboxes properties that have not been explicitly set will inherit that property from the new MailboxTemplate. Changing a property in the MailboxTemplate mailbox can also change that same property for all mailboxes for which that property has not been explicitly set.

Database Integration

MailSite Fusion allows you to reference mailbox and mail list data stored in an ODBC database. This means that even in registry mode, you can authenticate email users against an existing user database and create mail lists whose membership is based on database tables. In SQL Connector mode, all mailbox and mail list data is stored in the database for increased performance and scalability.

Web-Based Mailbox Access

MailSite ExpressPro provides end users with powerful control of their MailSite mailbox through a web browser from any computer on the Internet. This allows your users to send and receive e-mail, manage calendars and contacts, and much more even if they are away from their own computers.

WAP Wireless Mailbox Access

For those users without a smart-phone, MailSite Pocket provides them mailbox access through WAP-compatible wireless Internet devices, such as cell phones and personal digital assistants (PDAs).

Fast Installation

MailSite's Installation Wizard allows you to quickly and effortlessly install the application. The MailSite Engine's services are installed as NT services, allowing them to be automatically started when the machine boots up. MailSite's web services are installed under IIS. You can also start these services at the conclusion of the installation without rebooting your server.

Powerful Integrated List Server

MailSite Fusion includes a *list server*, which allows groups of users—such as employees, customers, and discussion groups—to easily exchange messages. A message sent to a *mail list* is quickly broadcast to all of its members, allowing users to distribute mail to multiple users by sending it to one e-mail address. MailSite's comprehensive list server features include multiple moderators, e-mail moderation, e-mail subscription, message size limitation, digest distributions, configurable welcome and goodbye messages, web-based message archiving, and powerful header editing macros.

Automatic Reply Facility

Each MailSite mailbox includes an optional *auto-reply message*, which defines a response that should be automatically sent to each user who sends a mail to the mailbox. You can use the auto-reply feature to create mailboxes dedicated to providing frequently requested information, such as product literature, newsletters, and product support assistance. Your users can also make use the auto-reply feature to set up an automatic response for when they are away from the office and unable to receive e-mail.

Integrated With Windows Account Passwords

MailSite Fusion allows you to create mailboxes that correspond to Windows users on your server system. When a Windows mailbox is created, its password is automatically taken from the Windows login password for the user, allowing your users to have a single password for your server. When you change a user's Windows login password, the user's MailSite mailbox immediately uses the new password.

Secure Logon

You can enhance security on your e-mail system by encrypting mailbox passwords (including NT User passwords) using the secure APOP, AUTH, AUTHORIZE or SPA protocols, which are all supported by MailSite.

Flexible Logging

MailSite Fusion includes flexible logging options that support extensive message tracking and error detection information. You can direct logging information to a file, to a database, and to the NT Event Viewer.

Virtual Domains

You can configure a single MailSite server to send and receive mail for multiple domains. This allows your site to host e-mail for "virtual" domains. Mailbox names need not be unique across domains, so you can use a particular mailbox name in each domain on your server.

Performance Monitoring

The MailSite Engine is integrated with the performance monitoring and security features of Windows 2000/2003. All Engine services can be monitored with the Performance Monitor for tracking information such as number of active connections, amount of message data received, and number of failed POP/IMAP logins. This feature is not currently supported in Windows Server 2008 due to significant changes made in that operating system.

Flexible Mailbox Authentication

User login data can be authenticated in several ways, allowing you to integrate existing user databases into MailSite. Users can be authenticated against the user database, an ODBC database, a SQL Server directory, an Emerald Database, or mailbox data stored in the registry.

Programmability

You can extend the capability of MailSite using *agents*, which are programs that are executed on individual e-mail messages that arrive for the server, for a particular mailbox, or for a particular mail list. For example, you could use an agent to automatically scan all incoming messages for virus attachments or to forward messages to your pager if they contain the word "emergency" in the subject header. Agents are extremely flexible and allow you to build-in almost any message-processing functionality.

What's New in Version 10

MailSite Release History

1996	Version 1	First high performance Windows SMTP & POP email server
1997	Version 2	IMAP added
1999	Version 3	Spam blocking and filtering; Microsoft SQL database integration
2000	Version 4	Webmail; clustering support
2002	Version 5	Anti Virus filtering
2003	Version 6	Sophisticated anti spam engine
2005	Version 7	Wireless email integration; security management
2007	Version 8	Collaboration; AJAX web interface; greylisting
2008	Version 9	Mobility – ActiveSync server
2013	Version 10	Performance, IMAP idle and Outlook 2013

MailSite Version 10

MailSite Fusion 10 includes an enhanced ActiveSync server that brings native email, calendar and contact sync to Microsoft Outlook 2013. It also brings support to an increased list smart phones for push email, calendar and contact updates over-the-air to BlackBerry, Windows Mobile, iPhone, Android, iPad and other smart phones and tablets. For all but the BlackBerry devices, this is achieved without any plugins, and no expensive and complex middleware is required.

We have invested significant amounts of time testing and profiling MailSite services against many different use cases and clients. This has allowed us to implement caching strategies to improve the responsiveness of the services while significantly reducing disk and network IO.

We have enhanced the ExpressPro web client to make use of the performance improvements, and added support for responding to meeting requests and offline mail processing.

Key MailSite Server version 10 features

- Outlook 2013 ActiveSync support providing true native calendar, contact and email synchronization to your desktop, mobile device and the ExpressPro web client.
- IMAP Idle delivering PUSH email to your inbox.
- Support for responding to meeting requests.
- Message Store performance improvements with SQL indexes.
- Significantly reduced disk and network I/O.
- Faster Anti virus update processing with progress visible though the MailSite console

A full list of features new to MailSite Fusion version 10 can be found in the release notes available from the website or in the installer package.

What is Outlook 2013 Native Sync?

MailSite has included a collaboration server for Outlook and many other clients since version 8. With MailSite version 10 we have go one step further and now provide full native email, calendar and contact sync with Outlook 2013.

The MailSite Fusion Sync server has been enhanced to provide Synchronization of Email Calendar and Contacts between your mobile devices, the MailSite server, the ExpressPro web client and Outlook 2013 on your desktop.

Microsoft Outlook 2013 now supports Exchange ActiveSync email accounts. We have adapted our MailSite ActiveSync Server to seamlessly support Outlook 2013.

To use this new feature in Outlook 2013, create a New Account and choose Exchange ActiveSync account type. Enter the same server information that you use to connect a Mobile device to your MailSite account and enjoy seamless end to end sync of your calendar and contact data together with push email delivery.

- Does not require you to install or maintain any Outlook desktop plug-ins
- Full two way read and write synchronization
- Share Calendar and Contacts with people on other clients for full collaboration

Installation

This section contains information on installing the various components of MailSite Fusion, including system requirements and an overview of the installation wizard.

System Requirements

MailSite SE Platform Availability

- ⇒ Windows XP Professional (SP2)
- ⇒ Windows 2000 Server (SP4)
- ⇒ Windows Server 2003 Standard Edition (SP2)
- ⇒ Windows Server 2008 (not Datacenter Edition)

MailSite LE and SP Platform Availability

- ⇒ Windows 2000 Server (SP4)
- ⇒ Windows 2000 Advanced Server (SP4)
- ⇒ Windows Server 2003 Standard Edition (SP2)
- ⇒ Windows Server 2003 Enterprise Edition (SP2)
- ⇒ Windows Server 2008 (not Datacenter Edition)

MailSite SE, LE and SP System Requirements

- ⇒ Intel-compatible Processor (700 MHz or faster CPU)
- ⇒ 256MB Minimum (512MB or higher recommended)
- ⇒ Additional message filtering and scanning may require additional CPU and RAM
- ⇒ Internet Explorer 6.0 or higher
- ⇒ 50MB Hard Disk space (To install)
- ⇒ DNS client installed and working
- ⇒ NTFS file system
- ⇒ TCP/IP transport installed and working
- ⇒ Microsoft SQL Server 2000 or 2005 - Required for versions with SQL integration

MailSite Express, MailSite ExpressPro, ActiveSync and MailSite Pocket Requirements

- ⇒ Windows Scripting Host
- ⇒ Internet Explorer 6.0 or higher
- ⇒ Windows 2000 Server or higher
- ⇒ Microsoft Scripting Engine 5.0 or higher
- ⇒ Microsoft Internet Information Server 5.0 or higher
- ⇒ ASP for MailSite Express
- ⇒ Microsoft .NET Framework 2.0 or Microsoft .NET Framework 3.0 for MailSite ExpressPro and ActiveSync
- ⇒ 512MB Minimum for MailSite ExpressPro (2GB or higher recommended)
- ⇒ Wireless Access Protocol (WAP) compatible wireless device for MailSite Pocket

Installation Contents

The MailSite Windows Console is the program that you use to configure and manage your MailSite server. The Windows Console can run on any of the supported computers listed in the System Requirments. It can manage local and remote MailSite servers on your network, and can even manage remote MailSite installations over the Internet.

MailSite Engine

The MailSite Engine is the component that receives, sorts, addresses and delivers e-mail. It is like the sorting office at your local post office. It does all of this work in the background and is not visible on your computer desktop.

MailSite Console

The MailSite Windows Console is the program that you use to configure and manage your MailSite server. The Windows Console can run on any supported computer as listed in the System Requirements section. It can manage local and remote MailSite servers on your network, and can even manage remote MailSite installations over the Internet.

MailSite Express

MailSite Express is a fast and efficient web messaging program that integrates fully with MailSite. MailSite Express requires a server with Internet Information Server (IIS) version 5.0 or later. It has a simpler interface than ExpressPro and so is suitable for some end-users with limited resources.

MailSite ExpressPro

MailSite ExpressPro is a feature rich AJAX web interface designed for demanding users who wish to see a desktop like experience from the browser of their choice. MailSite ExpressPro requires a server with Internet Information Server (IIS) version 5.0 or later and Microsoft .NET Framework 2.0 or higher.

MailSite Pocket

MailSite Pocket is a WAP wireless messaging program. Like MailSite Express, MailSite Pocket requires Microsoft Internet Information Server (IIS) version 5.0 or later.

MailSite Command-Line Utilities

The MailSite Command-Line utilities can be used to manage data for MailSite mailboxes, mail lists, domains, aliases, and other information from the Windows command prompt. These tools are particularly useful for creating scripts and batch files to automate MailSite configuration operations. Refer to the Utilities Appendix for more information on these utilities.

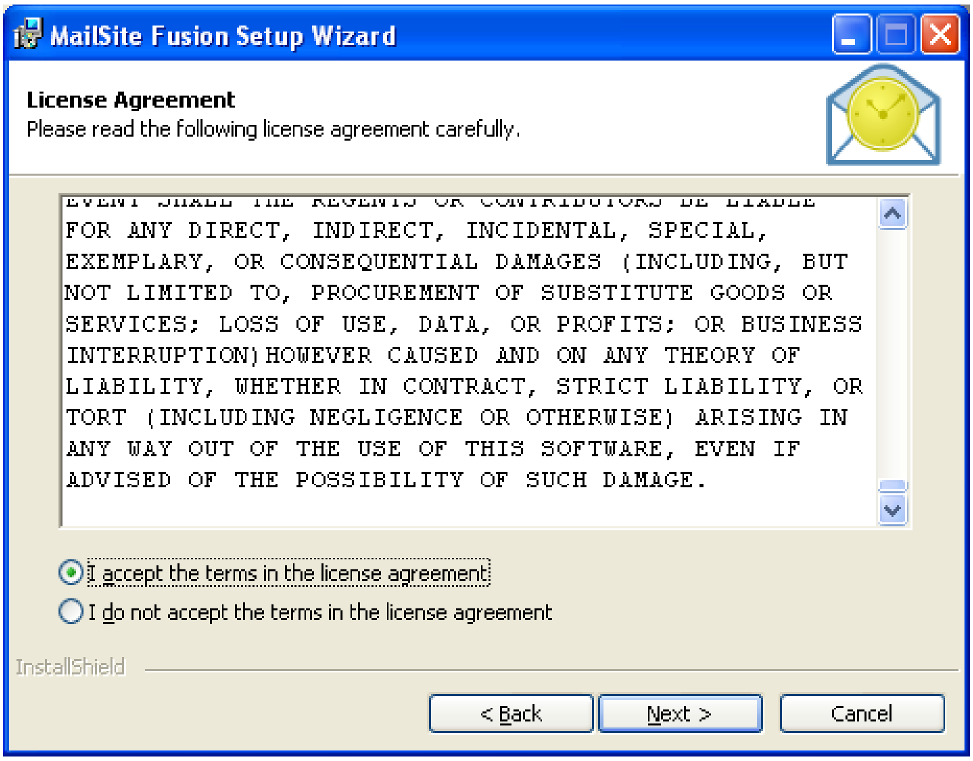
Mail System Conversion Utilities

The Mail System Conversion utilities allow you to migrate e-mail accounts and messages from your existing mail server to MailSite. Install these tools if you are upgrading from another mail server product. Refer to the Utilities Appendix for information on **MSCONV** on **MSCONVUSER** conversion utilities.

Installing MailSite SE, LE, and SP

To install any or all of the MailSite components, follow these steps on your mail server system:

- Log into Windows as a user with administrative privileges.
- MailSite is distributed as a single **SETUP.EXE** file. Begin the installation by executing this file.
- The installer displays a welcome dialog. To begin the installation, click **Next**. This displays the MailSite license agreement for your approval:



MailSite Fusion Setup Wizard

License Agreement

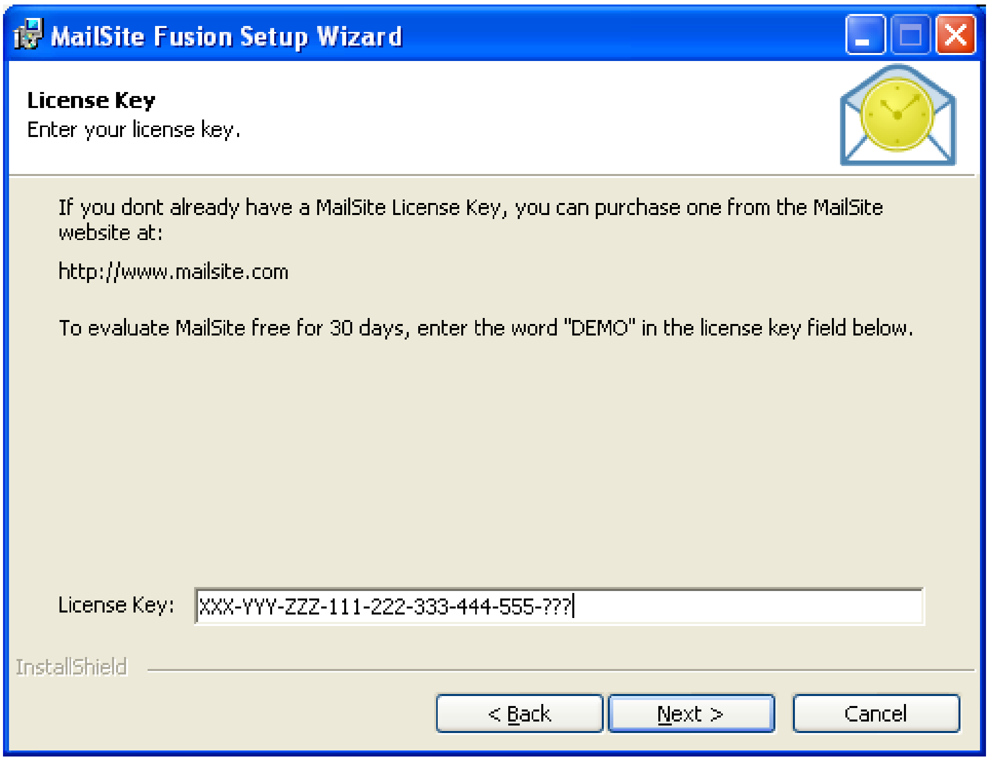
Please read the following license agreement carefully.

```
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.
```

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

- Click **I accept the terms of the License Agreement**, then **Next** to proceed with the installation.



License Key

Enter your license key.

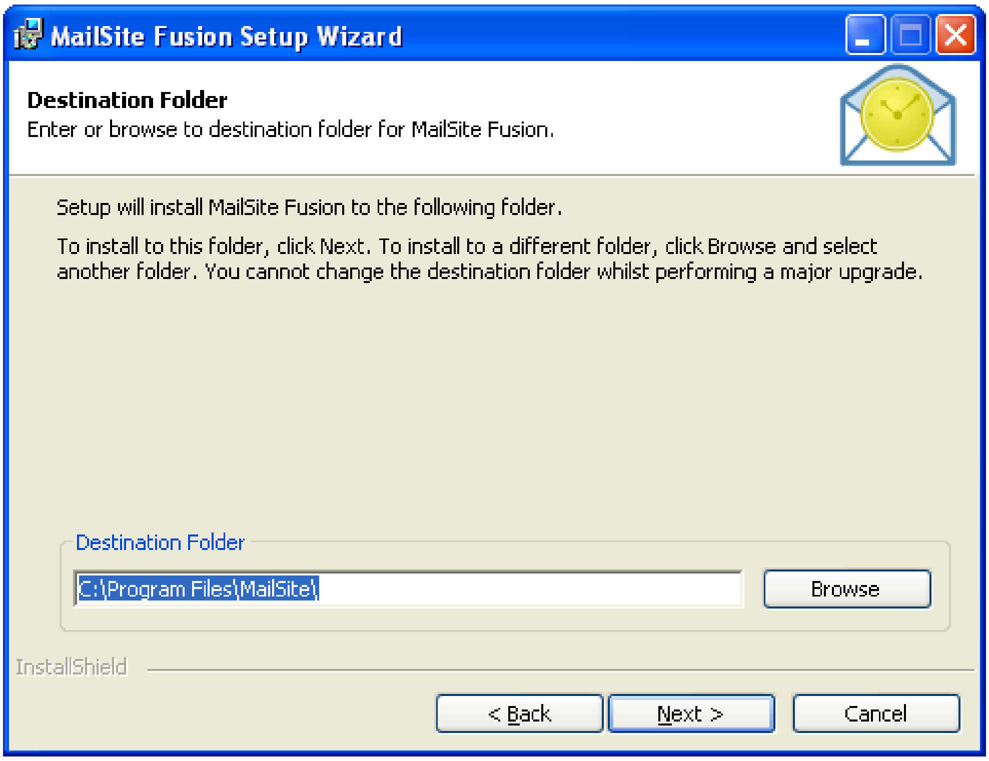
If you dont already have a MailSite License Key, you can purchase one from the MailSite website at:

http://www.mailsite.com

To evaluate MailSite free for 30 days, enter the word "DEMO" in the license key field below.

License Key: XXX-YYY-ZZZ-111-222-333-444-555-???

§ To evaluate MailSite free for 30 days, enter the word **DEMO** as the license key. Otherwise, enter your valid MailSite license key and click **Next**.:



Destination Folder

Enter or browse to destination folder for MailSite Fusion.

Setup will install MailSite Fusion to the following folder.

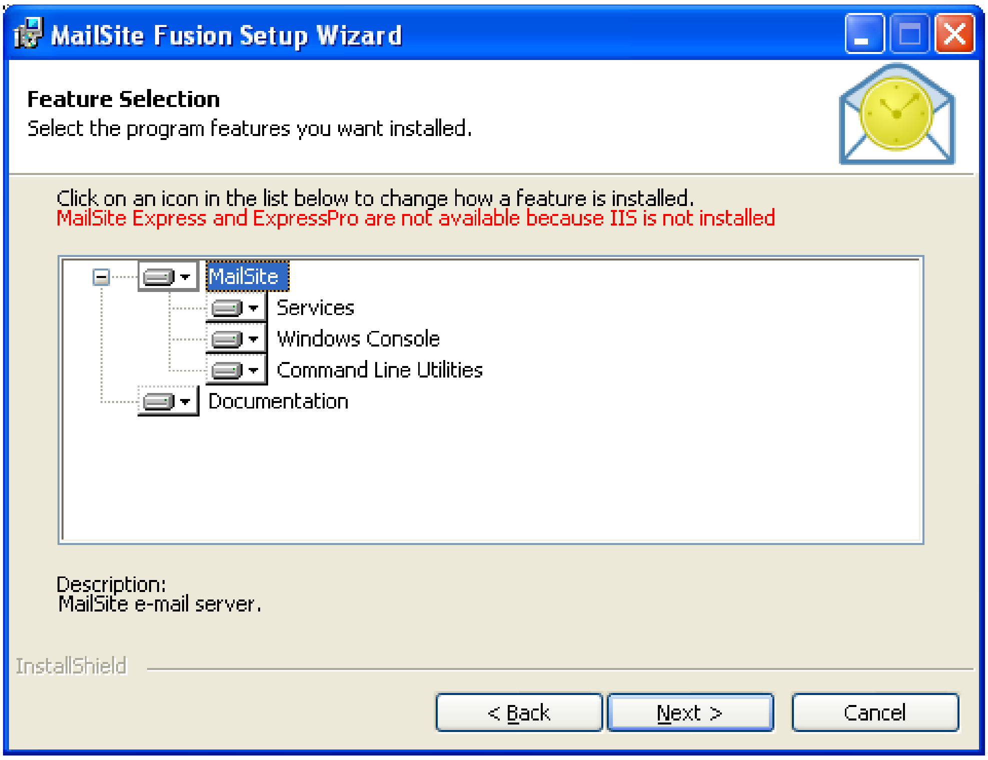
To install to this folder, click Next. To install to a different folder, click Browse and select another folder. You cannot change the destination folder whilst performing a major upgrade.

Destination Folder

C:\Program Files\MailSite\

§ This displays a prompt for the location for the MailSite files to be installed.

§ Select a location and click **Next**. This displays all the components that are available to be installed. As shown, if Microsoft IIS is not installed, important elements which rely on it such as MailSite Express, MailSite ExpressPro and wireless synchronization will not be installed.



Feature Selection

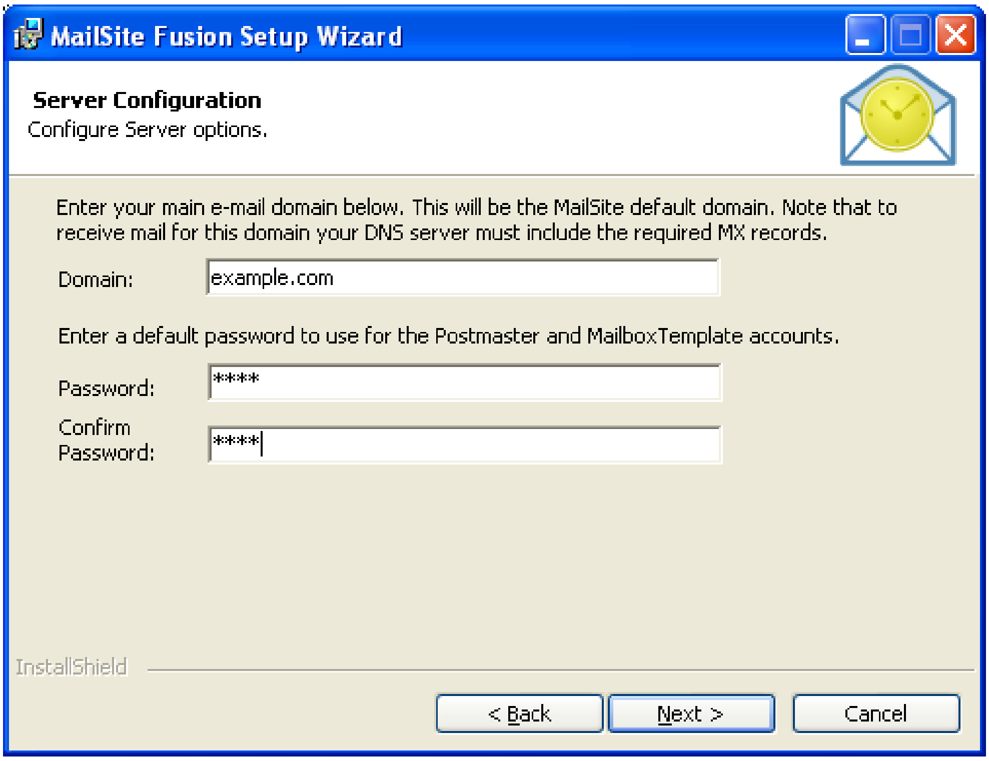
Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.
MailSite Express and ExpressPro are not available because IIS is not installed

- MailSite
  - Services
  - Windows Console
  - Command Line Utilities
- Documentation

Description:
MailSite e-mail server.

§ Select the components you want to install and click **Next**. If you chose to install the MailSite services then the installer will prompt you for the default e-mail domain for your site:



Server Configuration

Configure Server options.

Enter your main e-mail domain below. This will be the MailSite default domain. Note that to receive mail for this domain your DNS server must include the required MX records.

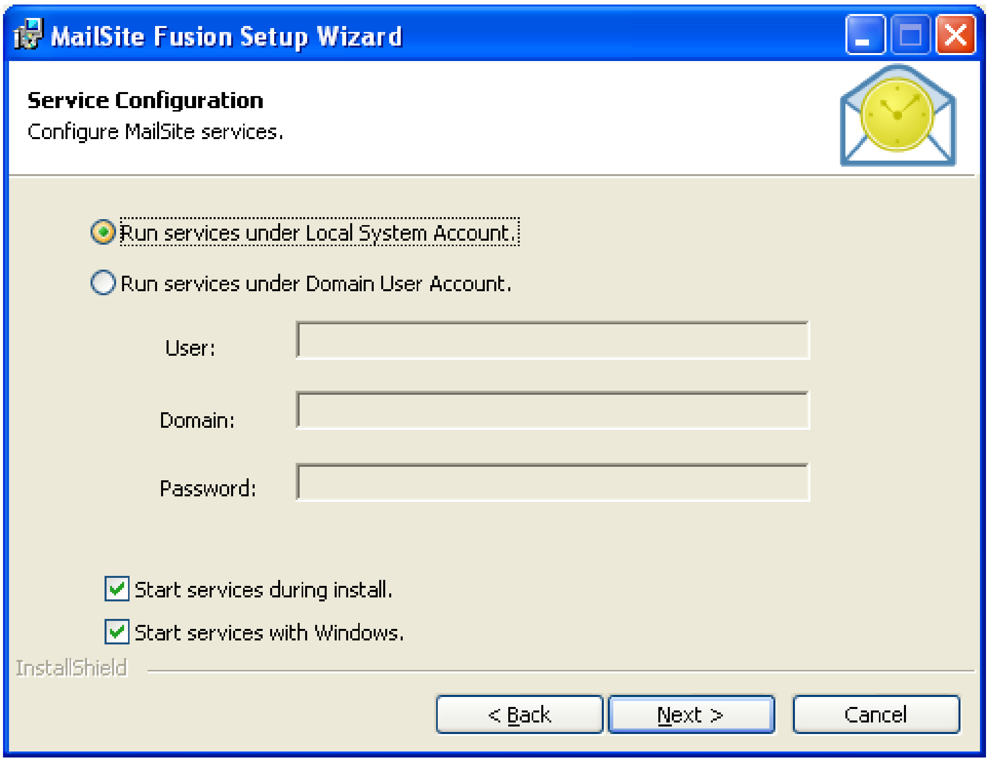
Domain: example.com

Enter a default password to use for the Postmaster and MailboxTemplate accounts.

Password: ****

Confirm Password: ****

§ By default, the domain name that is used is the same as that of the server you are installing to, but you can set a different domain if you choose. Once you have chosen a default domain name click **Next.**



Service Configuration

Configure MailSite services.

● Run services under Local System Account.

○ Run services under Domain User Account.

User:

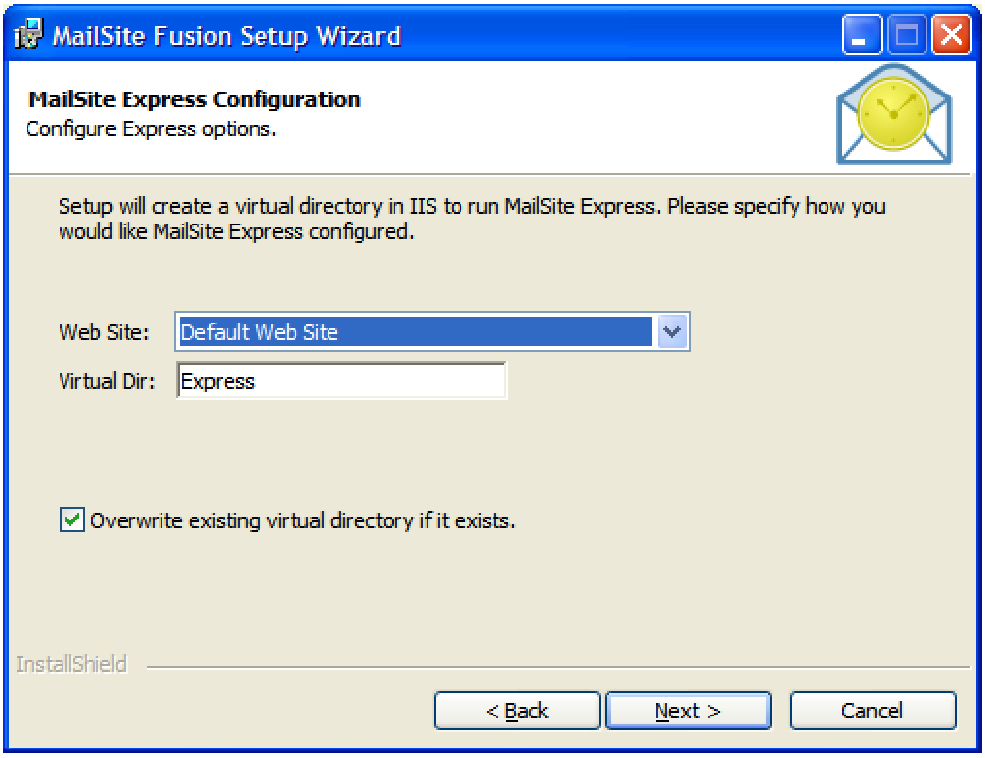
Domain:

Password:

☑ Start services during install.

☑ Start services with Windows.

- You can choose to run MailSite services under the Local System Account, or under the account for a specified domain user. It is also possible to determine whether the MailSite services will be started during the installation process, and whether they will automatically start with Windows. Once these settings are appropriate, click **Next.**
- If you choose to install MailSite Express, the installer will prompt you for information to configure IIS to run MailSite Express:



MailSite Express Configuration

Configure Express options.

Setup will create a virtual directory in IIS to run MailSite Express. Please specify how you would like MailSite Express configured.

Web Site: Default Web Site

Virtual Dir: Express

☑ Overwrite existing virtual directory if it exists.

- Select the name of the IIS web site that you would like to use. This corresponds with the web site description listed in the Internet Service Manager. The default is:

  ⇒ `Default Web Site`

  MailSite Express will be registered as an application under this web site with the name specified in the **Virtual Dir** field. The default is:

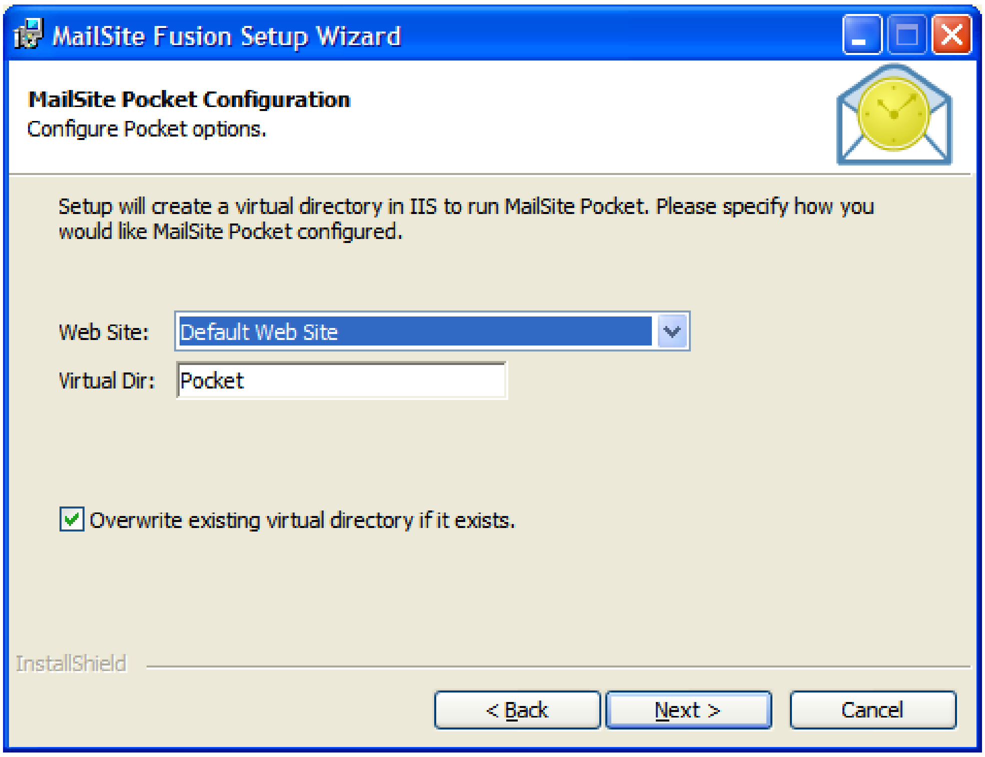
  ⇒ `Express`

  When installation is complete, verify that the IIS web site is running and log in to MailSite Express by pointing your web browser to:

  ⇒ `[Web Site]/[Virtual Dir]`

  You should see a MailSite Express login screen.

- Click **Next** to continue. If you choose to install MailSite Pocket, the installer will prompt you for information to configure IIS to run MailSite Pocket:



MailSite Fusion Setup Wizard

MailSite Pocket Configuration

Configure Pocket options.

Setup will create a virtual directory in IIS to run MailSite Pocket. Please specify how you would like MailSite Pocket configured.

Web Site: Default Web Site

Virtual Dir: Pocket

☑ Overwrite existing virtual directory if it exists.

Select the name of the IIS web site that you would like to use. This corresponds with the web site description listed in the Internet Service Manager. The default is:

⇒ `Default Web Site`

MailSite Express will be registered as an application under this web site with the name specified in the **Virtual Dir** field. The default is:

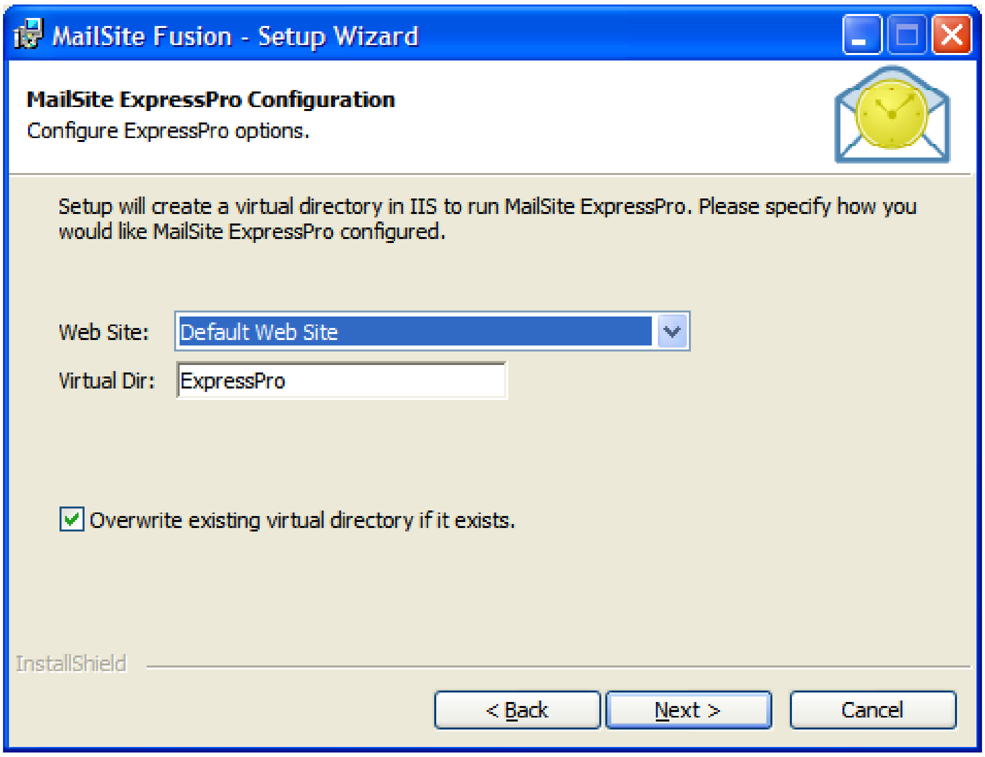
⇒ `Pocket`

When installation is complete, verify that the IIS web site is running and log in to MailSite Pocket by pointing your web browser to:

⇒ `[Web Site]/[Virtual Dir]`

You should see a MailSite Pocket login screen.

§ Click **Next** to continue. If you choose to install MailSite ExpressPro, the installer will prompt you for information to configure IIS to run MailSite ExpressPro:



MailSite ExpressPro Configuration

Configure ExpressPro options.

Setup will create a virtual directory in IIS to run MailSite ExpressPro. Please specify how you would like MailSite ExpressPro configured.

Web Site: Default Web Site

Virtual Dir: ExpressPro

☑ Overwrite existing virtual directory if it exists.

Select the name of the IIS web site that you would like to use. This corresponds with the web site description listed in the Internet Service Manager. The default is:

⇒ `Default Web Site`

MailSite Express will be registered as an application under this web site with the name specified in the **Virtual Dir** field. The default is:

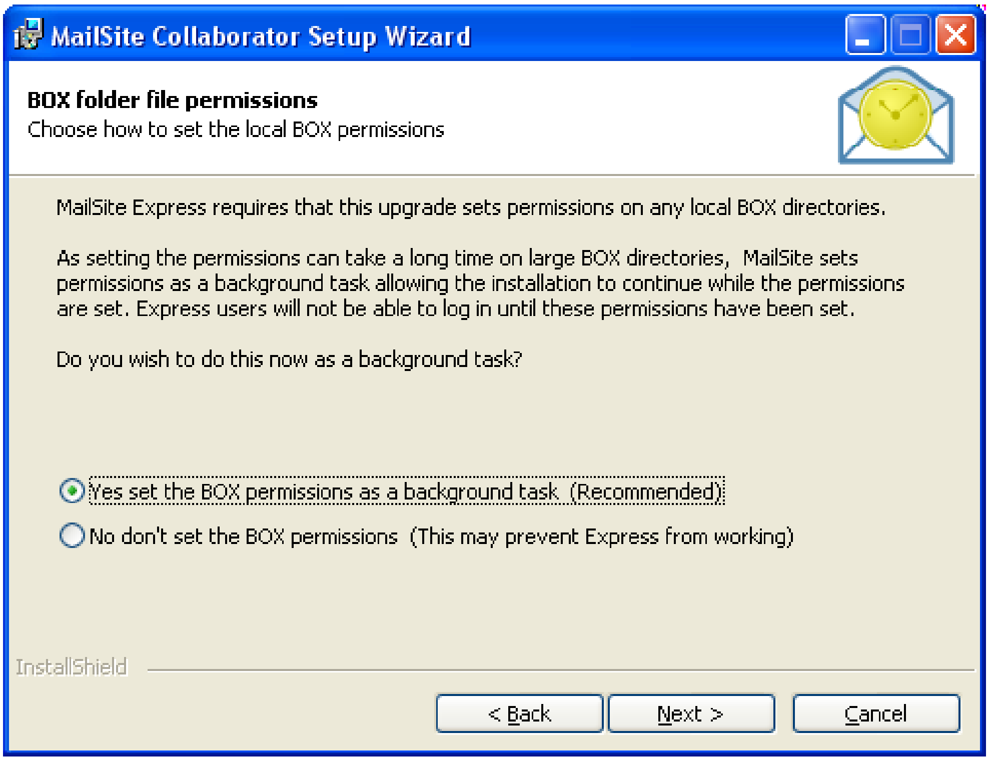
⇒ `ExpressPro`

When installation is complete, verify that the IIS web site is running and log in to MailSite ExpressPro by pointing your web browser to:

⇒ `[Web Site]/[Virtual Dir]`

You should see a MailSite ExpressPro login screen.

§ Once complete, click **Next**.



BOX folder file permissions

Choose how to set the local BOX permissions

MailSite Express requires that this upgrade sets permissions on any local BOX directories.

As setting the permissions can take a long time on large BOX directories, MailSite sets permissions as a background task allowing the installation to continue while the permissions are set. Express users will not be able to log in until these permissions have been set.

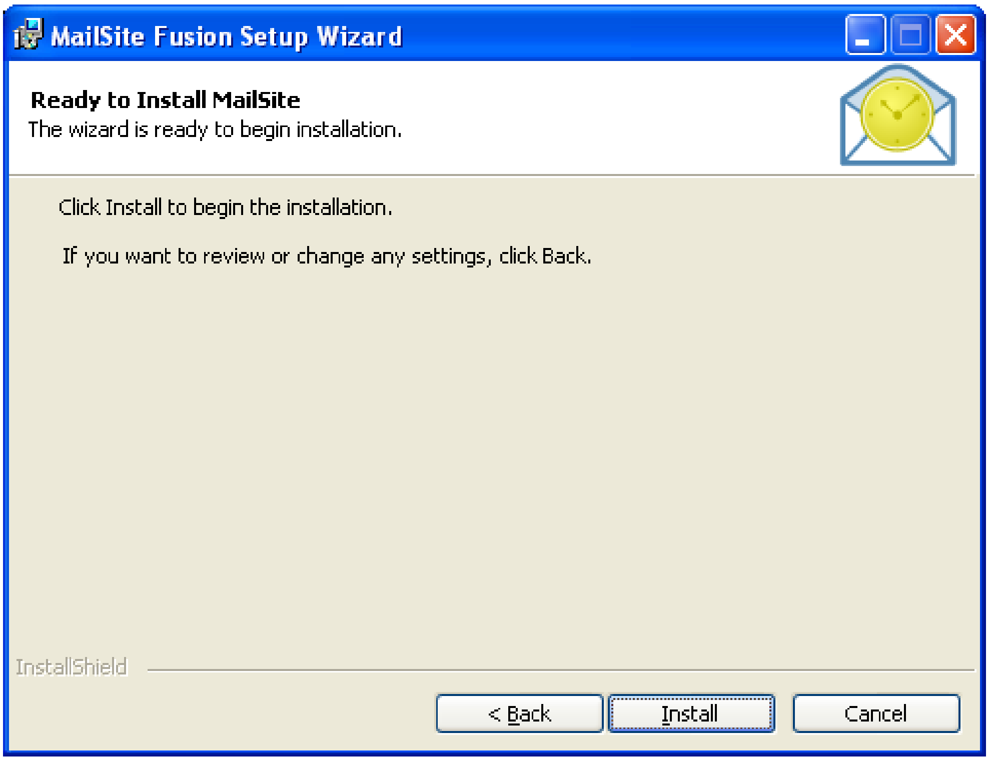
Do you wish to do this now as a background task?

● Yes set the BOX permissions as a background task (Recommended)

○ No don't set the BOX permissions (This may prevent Express from working)

If you are upgrading MailSite rather than performing a new installation, you will be prompted as to whether you wish to set BOX permissions during the installation process. It is important to select **Yes** unless you know for sure that permissions are correct. Please contact MailSite Support staff if you have a large installation and are unsure how best to proceed.

§ Once you have selected your preference, click **Next**.

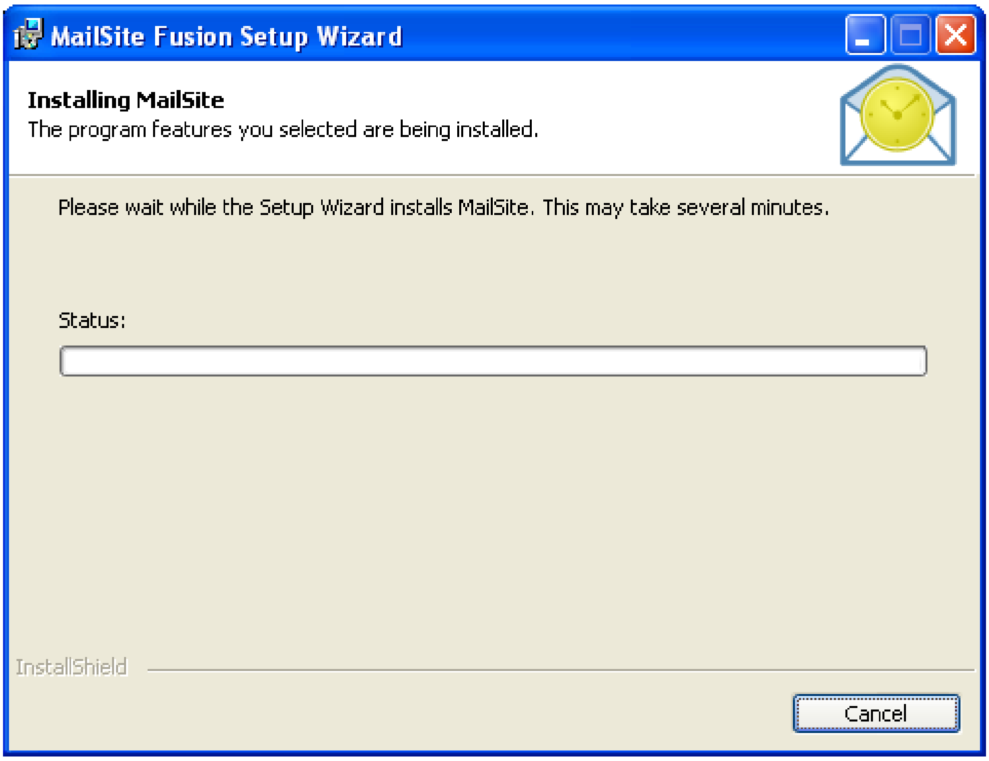


Ready to Install MailSite
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any settings, click Back.

§ Click **Install** to start the installation process.

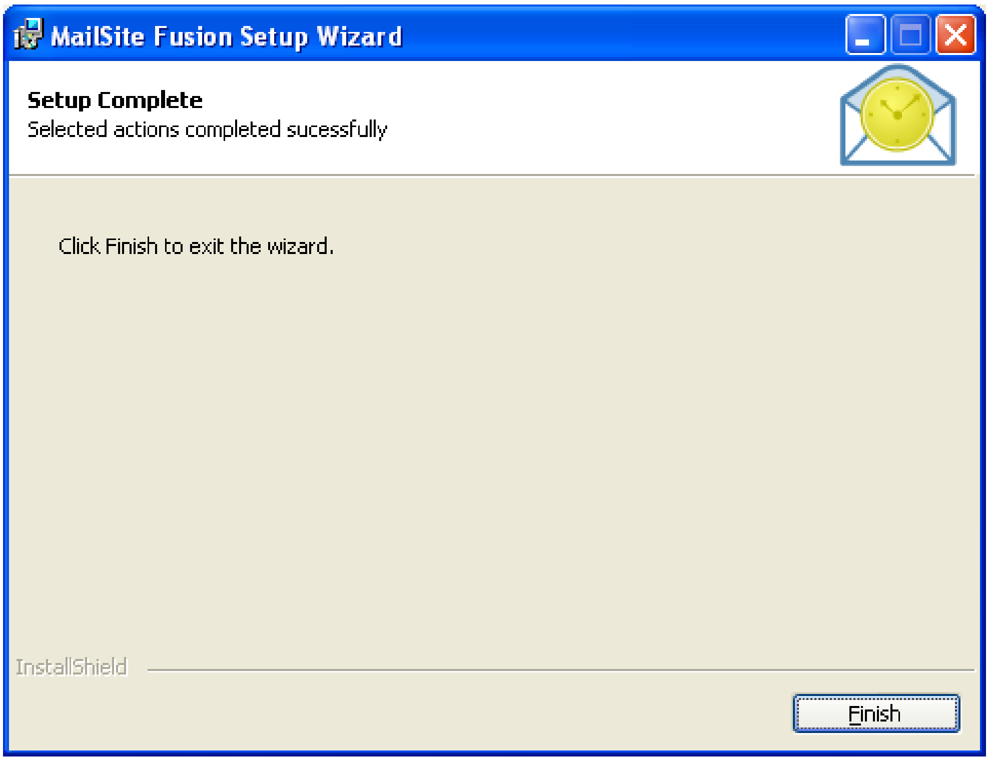


Installing MailSite
The program features you selected are being installed.

Please wait while the Setup Wizard installs MailSite. This may take several minutes.

Status:

§ Once the installation is complete you will see a confirmation dialog indicating that MailSite has successfully installed on your computer:



MailSite Fusion Setup Wizard

Setup Complete

Selected actions completed sucessfully

Click Finish to exit the wizard.

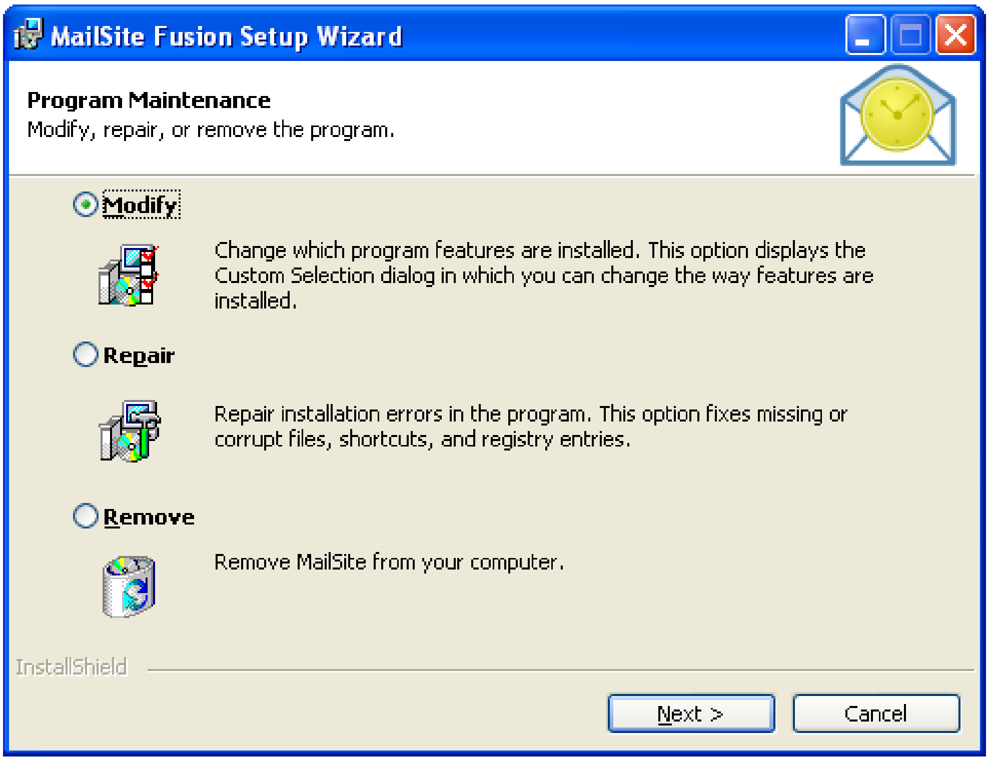
You have successfully completed the installation of MailSite Fusion. Depending upon the options chosen during the installation you are ready to use MailSite and configure users or you will need to manually turn on the MailSite Services.

Modifying MailSite

If you wish to add or remove components to your existing MailSite installation, you can do so by following these steps.

To modify a MailSite installation:

- Locate the Setup file that you chose when you installed MailSite.
- Run the Setup file.
- The following dialog will be displayed:



MailSite Fusion Setup Wizard

Program Maintenance

Modify, repair, or remove the program.

● Modify

Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.

○ Repair

Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.

○ Remove

Remove MailSite from your computer.

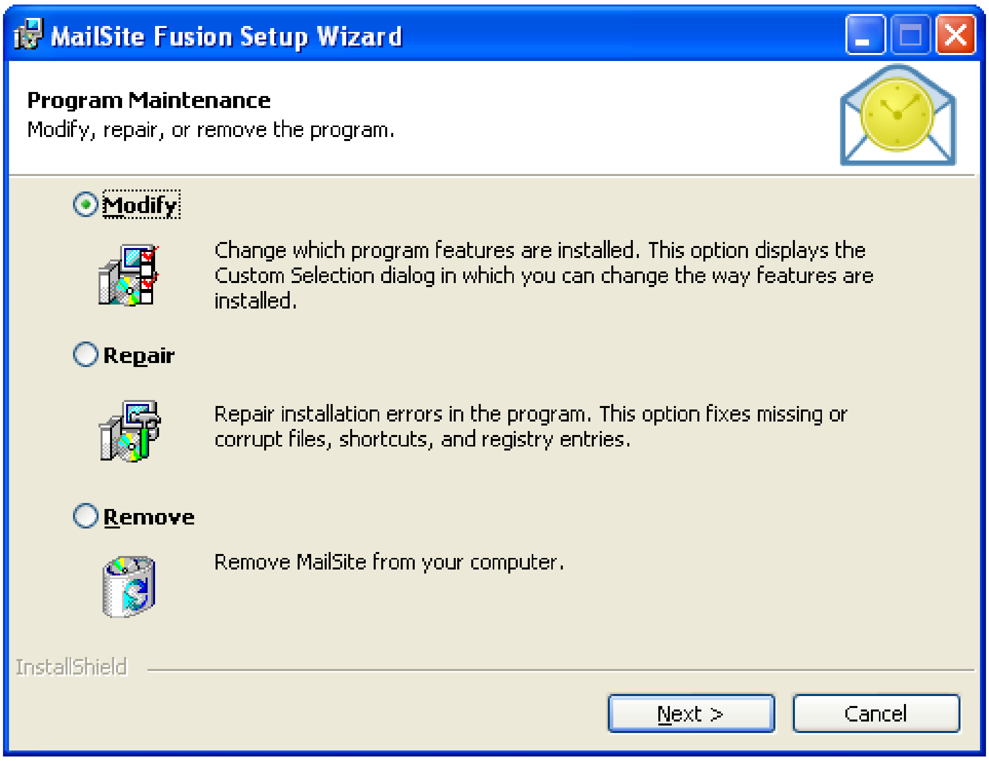
- Select the **Modify** option to begin changing your MailSite installation. The installer will display a dialog containing all the MailSite components and their current state.
- Make the required changes then click **Next**. A progress dialog will be displayed showing the progress of the modifications.
- Once the modifications are complete you will see a confirmation dialog indicating that MailSite has successfully been modified.

Repairing MailSite

If your MailSite installation has become corrupt, or is missing files you may want to repair it. To do so, follow the following steps.

To repair a MailSite installation:

- Locate the Setup file that you chose when you installed MailSite.
- Run the Setup file.
- The following dialog will be displayed:



Program Maintenance

Modify, repair, or remove the program.

● **Modify**

Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.

○ **Repair**

Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.

○ **Remove**

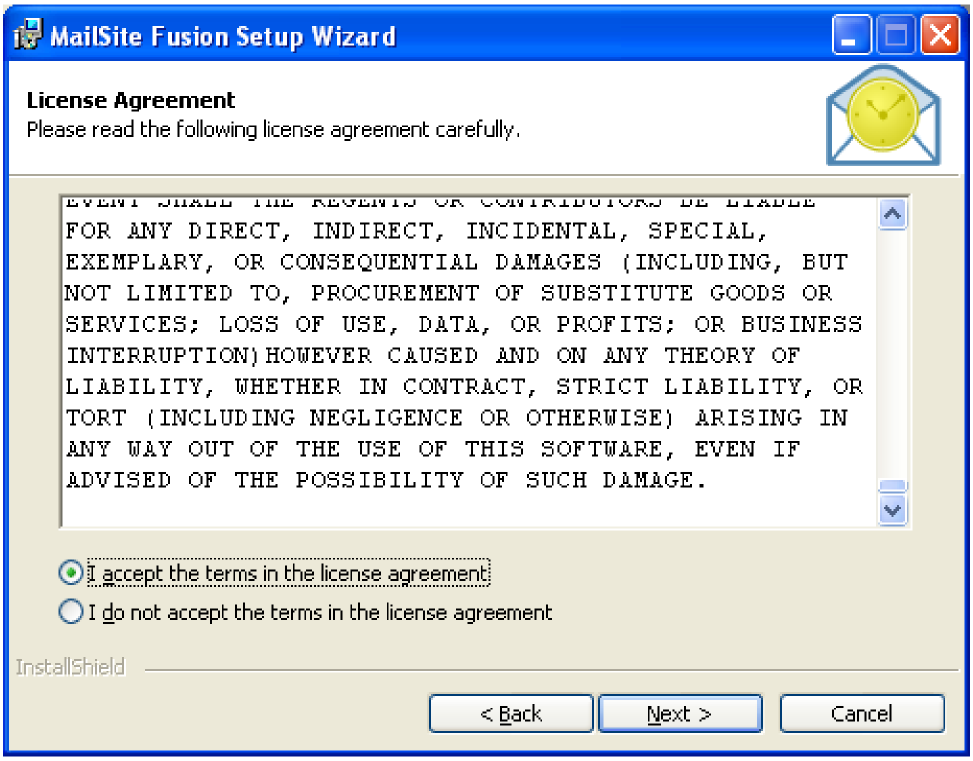
Remove MailSite from your computer.

- Select the **Repair** option to begin repairing your MailSite installation. The installer will immediately begin repairing your installation.
- A progress dialog will be displayed showing the progress of the repair.
- Once the repair is complete you will see a confirmation dialog indicating that MailSite has successfully been repaired.

Upgrading MailSite

To upgrade MailSite, follow these steps on your mail server system:

- Log into Windows as a user with administrative privileges.
- MailSite is distributed as a single **SETUP.EXE** file. Begin the upgrade by executing this file.
- The installer displays a welcome dialog. To begin the installation, click **Next**. This displays the MailSite license agreement for your approval:



License Agreement

Please read the following license agreement carefully.

```
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.
```

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

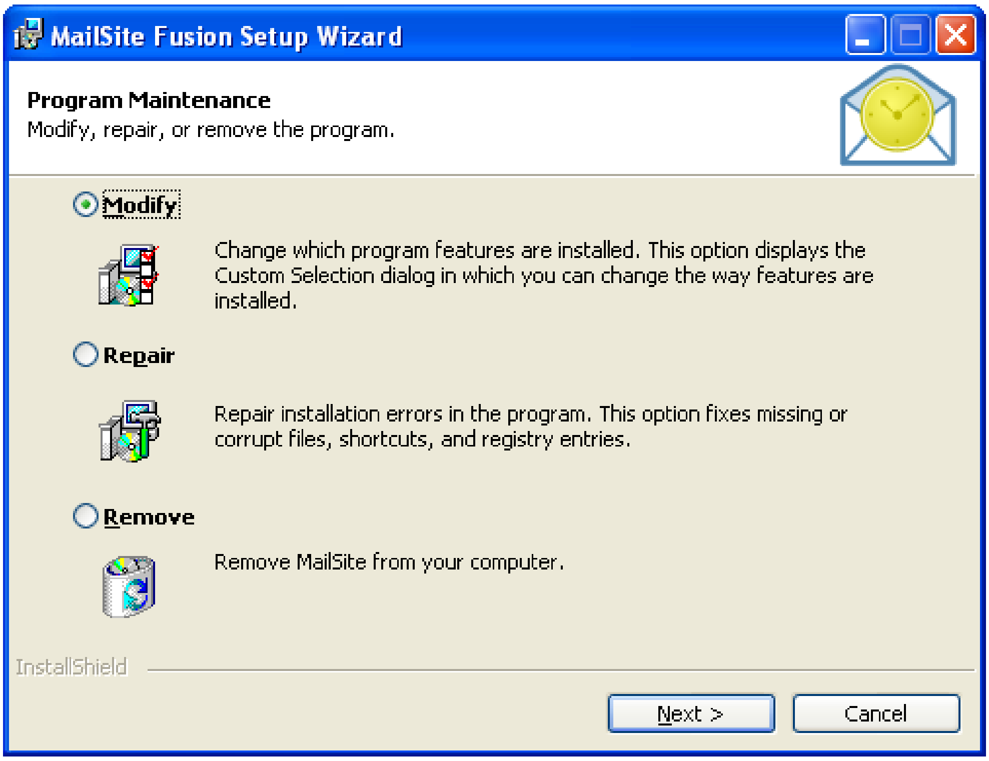
- Click I accept the terms of the License Agreement, then **Next** to proceed with the upgrade.
- The installer will show you a dialog confirming the upgrade.
- Verify that the information is correct then click **Next** to begin upgrading MailSite. A progress dialog will be displayed showing the progress of the upgrade.
- Once the upgrade is complete you will see a confirmation dialog indicating that MailSite has successfully been upgraded.

Uninstalling MailSite

If you wish to completely remove MailSite from your computer follow the following steps.

To remove MailSite from your computer:

- Locate the Setup file that you chose when you installed MailSite.
- Run the Setup file.
- The following dialog will be displayed:



MailSite Fusion Setup Wizard

Program Maintenance

Modify, repair, or remove the program.

● Modify

Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.

○ Repair

Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.

○ Remove

Remove MailSite from your computer.

- Select the **Remove** option to begin removing MailSite. The installer will show a dialog prompting you to confirm the complete removal of MailSite.
- Click **Next** to begin removing MailSite from your computer. A progress dialog will be displayed showing the progress of the removal.

Silent Installations

The **SETUP.EXE** installation program may be run with a script file for silent installations. The values given in the script will provide the parameters normally specified by the administrator during installaton. This method of installation is useful for sites that deploy multiple instances of MailSite.

MailSite Software, Inc. use Microsoft MSI technology and InstallShield DevStudio to build the MailSite installer **SETUP.EXE**. Silent installations can be more complex than meets the eye and it is recommended to read the following documentation before beginning a silent installation:

http://helpnet.installshield.com/robo/projects/helplibdevstudio9/IHelpSetup_EXECmdLine.htm

An example of a silent installation of Mailsite might be as follows:

Setup.exe /s /v"/qn INSTALLDIR=D:\Destination"

Specified properties should be set to 1 for action to be performed. If you don’t want that action to be performed simply omit that property completely.

The properties that must be set for a clean install are:

Field	Description
LICENSEKEY	Your MailSite license key.

Properties that may be set for a clean install or an upgrade:

Field	Description
STARTSERVICES	Set to 1 to start services during installation.
AUTOSTARTSERVICES	Set to 1 to start services automatically every time the server boots up.
LOCALSYSTEMSERVICE	Set to 0 to run services under different credentials to the “Local System”.
SERVICEUSERNAME	If LOCALSYSTEMSERVICE = 0 then set to the user name of account under which to run services.
SERVICEDOMAIN	If LOCALSYSTEMSERVICE = 0 then set to the domain of above user.
SERVICEPASSWORD	If LOCALSYSTEMSERVICE = 0 then set to the password of above user.
INSTALLDIR	The MailSite installation directory.
PRIMARYDOMAIN	The default mail domain for this server.
MAILBOXPASSWORD	The password of default domain’s postmaster.
DOMAINFORWARDINGHOST	The IP address or Fully Qualified Domain Name for forwarding mail to the Target Host.
EXPRESSWEBSITE	The website from which MailSite Express is served.
EXPRESSAPPNAME	The Virtual Directory name of the MailSite Express application.
POCKETWEBSITE	The website from which MailSite Pocket is served.
POCKETAPPNAME	The Virtual Directory name of MailSite Pocket application.
EXPRESSPROWEBSITE	The website from which MailSite ExpressPro is served.
EXPRESSPROAPPNAME	The Virtual Directory name of the MailSite ExpressPro application.
CONFIGUREFIREWALL	If set to 1, the MailSite installer will attempt to configure the firewall to allow the services to function correctly. This relates to Windows Server 2008 and Windows Vista which have relatively restrictive firewalls. Default is 1.

The properties that can be set for an upgrade are:

Field	Description
OVERWRITEEXPRESSAPP	Set to 1 to overwrite the MailSite Express application in IIS if it already exists.
OVERWRITEEXPRESSPROAPP	Set to 1 to overwrite the MailSite ExpressPro application in IIS if it already exists.
OVERWRITEPOCKETAPP	Set to 1 to overwrite the MailSite Pocket APP in IIS if it already exists.

The properties that must be set on upgrades are:

Field	Description

`SETBOXPERMISSIONS`	Set to 1 to force MSIIUSER permissions on the BOX directory which is recommended for Express to function properly.

The properties that should not be set on upgrades are:

Field	**Description**
`INSTALLDIR`	The MailSite installation directory.

Ensure that you specify all of the parameters with correct values. The installation may fail if any parameter is missing or is incorrect.

Quick Start

Checking the Mail Services

This section provides a quick-start overview of getting MailSite up and running on your site. To verify that MailSite is successfully installed, follow these steps:

1. Verify your Default Domain

Your **Default Domain** is the part of your e-mail address after the **@** character. If your e-mail address is **joe@abc.com**, then your default domain is **abc.com**. This is the default email domain that you should have entered during installation. If you need to change the default domain set during installation, you can do this in the MailSite Console in the Domains Folder: select the default domain, click on the right mouse button, and select **Rename domain**.

2. Check your DNS Setup

Your DNS server should resolve **abc.com** to the IP address of your server. To verify this, run **NSLOOKUP**:

```
nslookup
> set type=mx
query type = MX
> abc.com
abc.com.  ->  0, mail.abc.com.
> set type=a
query type = A
> mail.abc.com
mail.abc.com. -> 204.147.233.1
```

This session indicates that the MX record for **abc.com** points to **mail.abc.com**, which points to the IP address 204.147.233.1.

DNS is a requirement for MailSite, but not part of the software. Please refer any issues to your organization’s DNS administrator.

3. Start the MailSite Services

Run the MailSite Console program, select the Services Folder, and start all of the services (if they are not already running).

4. Check Client Connectivity

To verify TCP/IP connectivity from your client, **telnet** to the SMTP port on your MailSite server:

```
C:\>telnet mail.abc.com 25
220 abc.com MailSite SMTP Receiver Version 9.0.0 Ready
```

5. Configure your Mail Client

Configure your mail client as follows:

⇒ Set the e-mail address to **postmaster@abc.com**

⇒ Set the SMTP Server to **mail.abc.com**

⇒ Set the POP3/IMAP4 Server to **`mail.abc.com`**

6. Send a Test Message

Create a new message addressed to **`postmaster@abc.com`** and send the message.

7. Check for New Mail

Click on the button to check for new mail. You should have one new message.

If you have trouble see the Troubleshooting section.

Checking the Web Services

Many of MailSite Fusion's features are implemented as Web Services. For example, the AJAX web client MailSite ExpressPro, mobile device synchronization with the MailSite ActiveSync service and Outlook 2007 connectivity are all provided by web services.

MailSite Web Services will only have been offered during installation if Microsoft Internet Information Services (IIS) and the .NET Framework were installed on the machine. See the System Requirements section of the Manual for more details.

1. Start the MailSite Web Services

The MailSite Web Services will normally be running after installation. If they are not running, or you wish to check, bring up Microsoft IIS Manager and navigate to the website (typically Default Web Site). If the web site is not running, click Start Item, or refer to Microsoft documentation for more details on managing IIS. Once that website is running, all the MailSite Web Services you installed should be active.

2. Check Client Connectivity with ExpressPro

The easiest Web Service to check is MailSite ExpressPro as this requires an internet browser rather than adding the complexity of a mobile device as with MailSite ActiveSync. Bring up a supported internet browser such as a recent version of Internet Explorer or FireFox and browse to the location you specified for ExpressPro. This will typically be something like www.example.com/expresspro, though you may have changed this during the installation process. If you see the login screen, clearly the web service is running, so login and use as required.

If you intend to check ActiveSync connectivity, it would make sense to add one or more contacts and events in ExpressPro so that there is something to synchronize to the mobile device.

3. Check ActiveSync Connectivity

The MailSite ActiveSync (sometimes referred to as AirSync) service can be checked with Microsoft ActiveSync compatible devices such as iPhone 2.0 or Windows Mobile devices. Device configuration is device specific, but typically follows the format described in the Mobile Connectivity section of the Manual.

Not all MailSite licenses include mobile connectivity using ActiveSync. To check the capabilities of your license key, bring up the MailSite Console, and choose Server->License Key. The field “Max Wireless Sync Users” indicates whether this feature is licensed. If you are unsure, please contact MailSite Sales.

Anti-Spam and Anti-Virus

MailSite Anti-Virus and Anti-Spam are packaged with every version of MailSite Fusion and do not require a separate installation. In order to use these products, the license key must include protection for one or more mailboxes. If you are not licensed and wish to evaluate MailSite Anti-Virus or Anti-Spam, please contact MailSite Sales.

Mobile Connectivity

MailSite Fusion has native support for ActiveSync compatible devices, allowing end-users to automatically synchronize their mail, calendar and contacts from the device of their choice. This is achieved without any complex and expensive middleware and without plugins to install on the user's device.

Linking an ActiveSync Compatible Device to MailSite

The following instructions are based on a Windows Mobile 6 handset. They may vary depending on your chosen device.

1. Open the ActiveSync application on the device
2. Click Menu and select 'Add Server Source'
3. Enter the domain name of the server **but NOT the virtual directory name**, e.g. mail.example.com
4. Enter the mailbox name, password and domain of the account you wish to sync.
5. Select the services you wish to sync from Calendars, Contacts and Email. **Do NOT select tasks** as these are not supported by MailSite Fusion's ActiveSync service.

Once complete, the device will automatically synchronize with MailSite Fusion's ActiveSync service, and will remain synchronized whenever a data connection is available. New mail will appear automatically on the device in line with the device settings, which is usually much faster than a desktop client such as Outlook.

Linking a BlackBerry Device to MailSite

BlackBerry devices show the latest mail for standards based email servers such as MailSite using the BlackBerry Internet Service (BIS). However, the BIS does not offer over-the-air contacts and calendars, and does not automatically keep the inbox synchronized.

AstraSync is separate software, not included in MailSite Fusion. It is designed to provide over-the-air synchronization between a BlackBerry smartphone and an ActiveSync server and is downloadable from the AstraSync website: www.astrasync.com

Outlook Connectivity

MailSite Fusion has rich native support for Microsoft Outlook 2007, automatically synchronizing the most important data with the MailSite data store so that it can be accessed just as easily from a browser using MailSite ExpressPro.

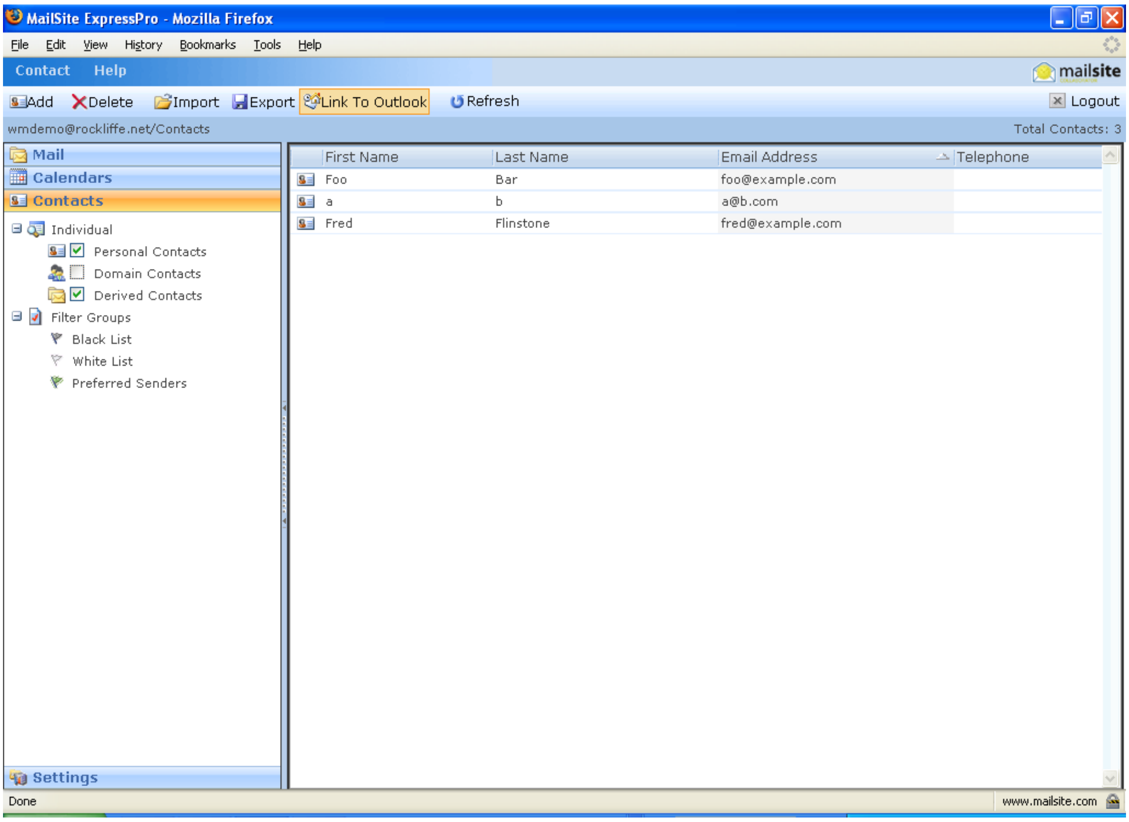
Linking Outlook to MailSite

Outlook 2007 needs to be linked to the MailSite server so that it knows to synchronize calendar updates. In order to make this link, each end-user needs to do the following on their machine where Outlook is installed:

§ Login to MailSite ExpressPro using a supported browser.

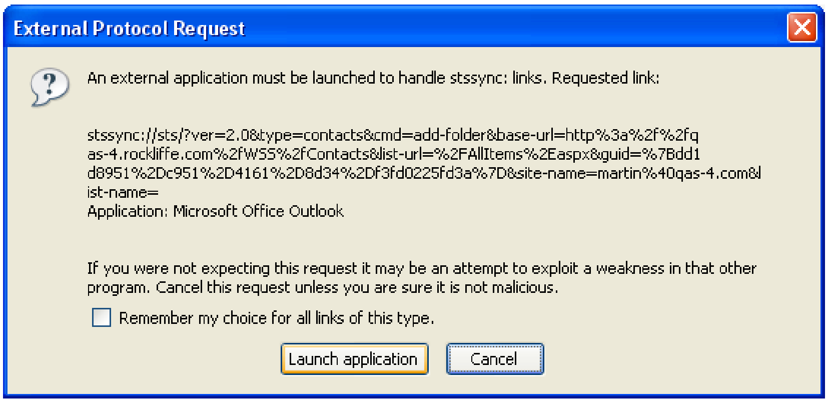
Once logged in to MailSite ExpressPro, it is possible to either link personal contacts or a calendar with Outlook.

§ To link contacts, click **Contacts** on the section navbar (left side of the screen).



First Name	Last Name	Email Address	Telephone
Foo	Bar	foo@example.com	
a	b	a@b.com	
Fred	Flinstone	fred@example.com	

§ Click **Link to Outlook** which will launch a dialog similar to the following:



An external application must be launched to handle stssync: links. Requested link:

stssync://sts/?ver=2.0&type=contacts&cmd=add-folder&base-url=http%3a%2f%2fq
as-4.rockliffe.com%2fWSS%2fContacts&list-url=%2FAllItems%2Easpx&guid=%7Bdd1
d8951%2Dc951%2D4161%2D8d34%2Df3fd0225fd3a%7D&site-name=martin%40qas-4.com&l
ist-name=
Application: Microsoft Office Outlook

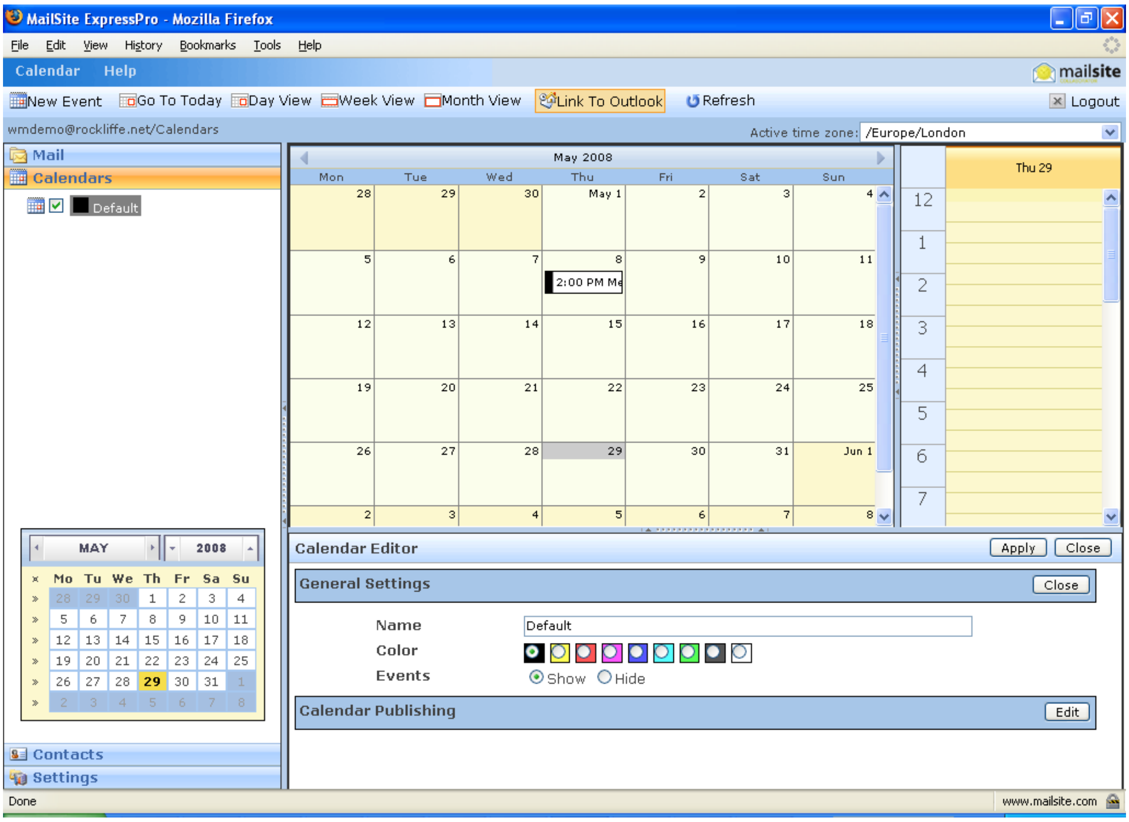
If you were not expecting this request it may be an attempt to exploit a weakness in that other program. Cancel this request unless you are sure it is not malicious.

□ Remember my choice for all links of this type.

§ Click **Launch application** to allow MailSite Fusion to contact Outlook.

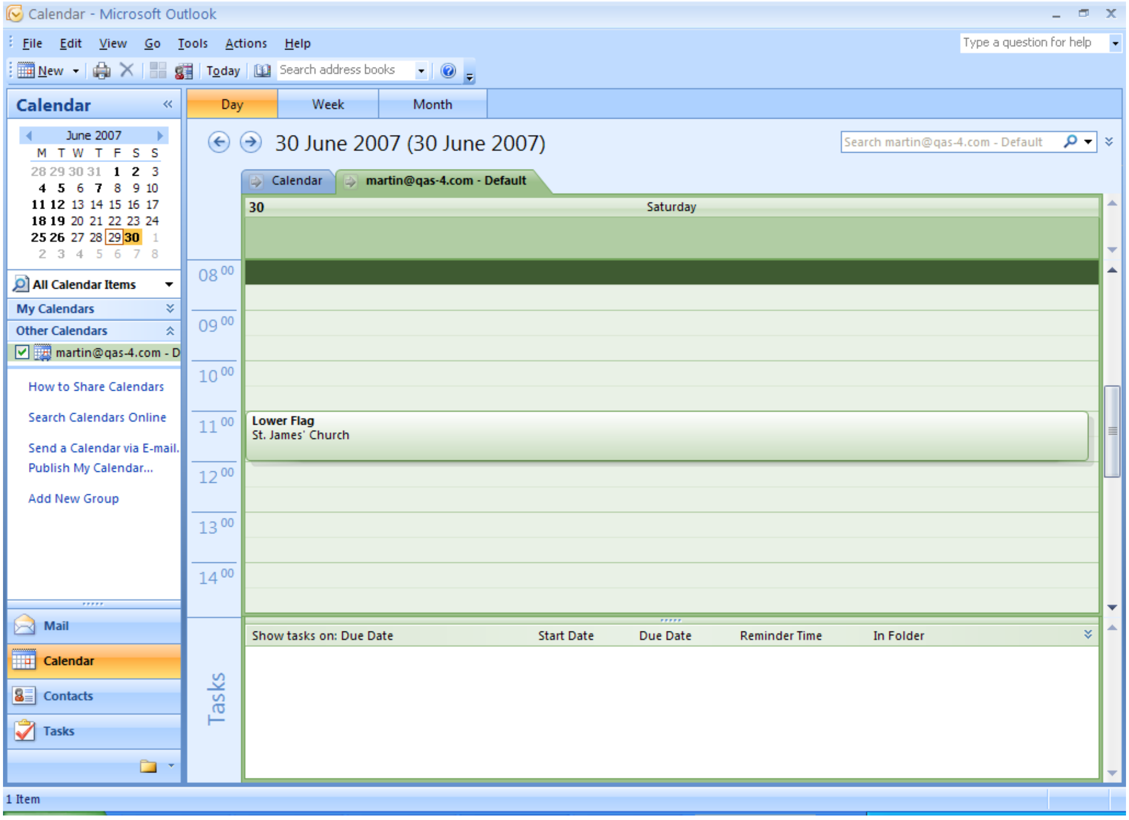
Once complete, you will see the contacts shown in Outlook. This collection is then available in Outlook, allowing the user to lookup and modify contacts, copy to and from other contact collections and so on. It is important to note that contacts from a number of sources can be seen in the MailSite ExpressPro interface. Only personal contacts will be synchronized with Outlook.

§ To link a calendar, click **Calendars** on the section navbar (left side of the screen) in MailSite ExpressPro.
§ Select the calendar you wish to synchronize such as **Default.**



Name: Default
Color
Events: ● Show ○ Hide

§ Click **Link to Outlook** which will launch the external protocol dialog as shown above.
§ Click **Launch application** to allow MailSite Fusion to contact Outlook. Once complete, you will see the MailSite calendar in Outlook such as the following:



Outlook 2007 provides rich support for multiple calendar collections. The user can choose to view multiple calendars side-by-side, in overlay mode, or simply to see one calendar at a time. It is possible to drag and drop events between calendar collections and anything in the MailSite Fusion calendar in Outlook will be automatically synchronized with the server making the same data available in MailSite ExpressPro.

It is only possible to synchronize a single MailSite Fusion calendar with Outlook at this time. Attempting to link multiple calendars to the same Outlook installation will result in events being duplicated.

Calendaring Server

MailSite Fusion includes a calendar server which is a powerful and flexible collaboration platform. MailSite Calendar Server enables standards-based calendar sharing based on the iCalendar standard providing calendaring for many clients including Outlook 2007, Vista’s Windows Calendar, Google Calendar, Mozilla’s Lightning/Sunbird and Apple’s Mac iCal. The server also supports native calendaring and contacts for Outlook.

Organize everyone, not just your team

Existing calendar solutions typically make it easy to share calendar information within an organization, but traditionally have not been so effective at bringing together all of a user’s scheduling information. MailSite Fusion allows users to review both internal and external calendar data from the web or desktop client of choice, providing flexibile collaboration without dictating the end-user platform.

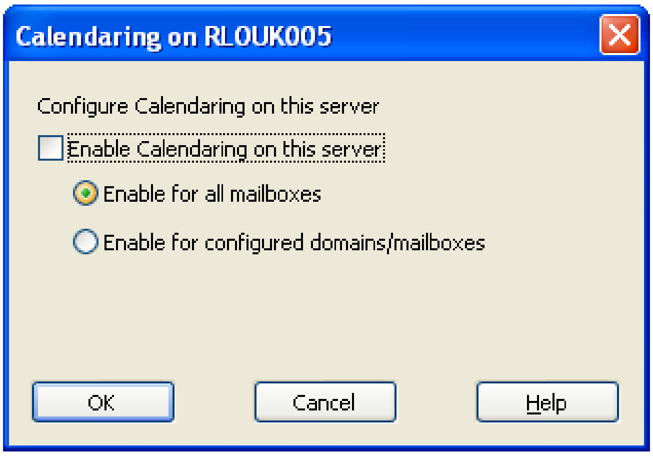
MailSite ExpressPro allows end-users to view and modify their own calendars including those normally maintained in Outlook. ExpressPro users can also view public calendars in the popular iCalendar format. MailSite uses the WebCAL protocol to access iCalendar files allowing it to poll for updates.

MailSite Fusion’s calendar server allows calendars to be shared with Outlook, or with a range of standards-based calendar clients such as Apple’s iCal, Mozilla’s Lightning/Sunbird, Google Calendar and Vista’s Windows Calendar via WebCal.

Being able to share calendar data across platforms, clients and even public calendars without hard to manage plugins is something valuable to all organizations and many families. Other calendar solutions typically organize an internal team all using similar software. MailSite Fusion allows modern users to organize their busy lives whatever their favored setup.

Calendar Provisioning

Calendaring is not always provisioned for all mailboxes. To configure calendaring, in the MailSite Administration Console under **`Server`** click the **`Calendaring`** icon to configure calendaring settings for this server.



Calendaring on RLOUK005

Configure Calendaring on this server

□ Enable Calendaring on this server

● Enable for all mailboxes

○ Enable for configured domains/mailboxes

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.

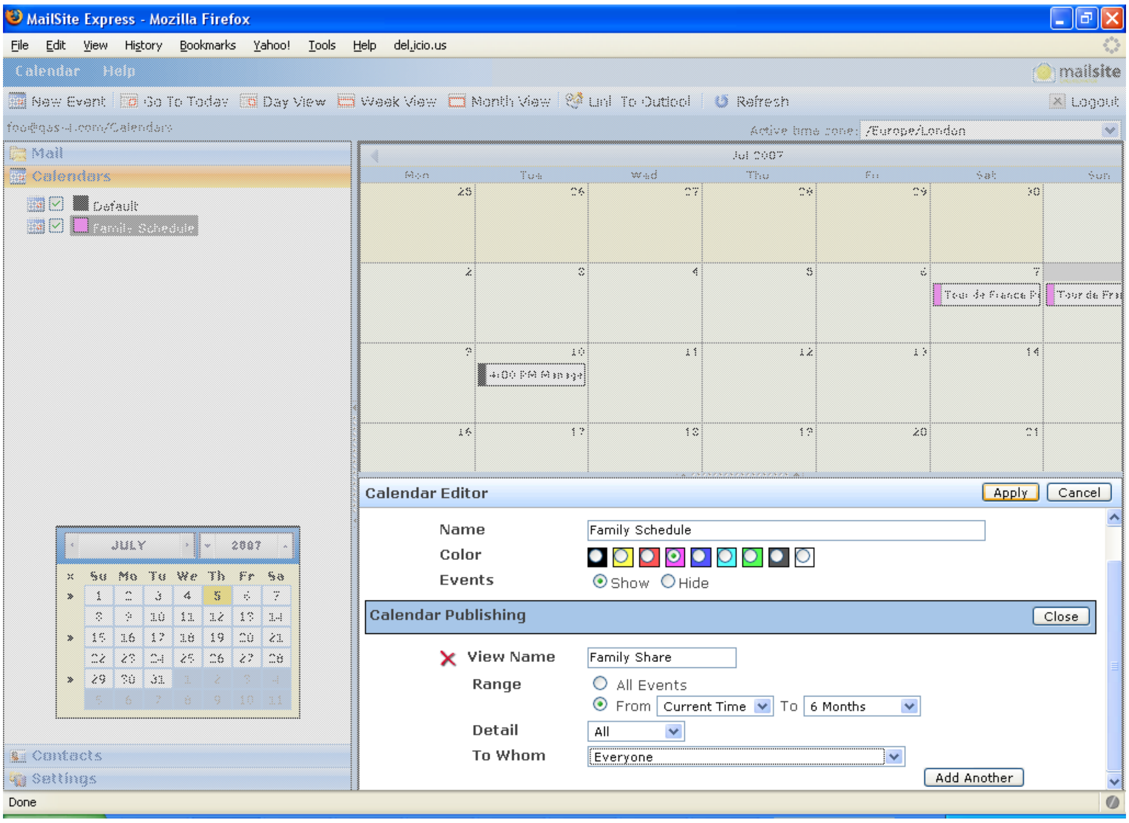
If calendaring is set to be enabled for configured domains/mailboxes then similar controls are available at domain and mailbox level to determine the parts of the system to enable.

Sharing or publishing calendars

Calendar data is easy to share via MailSite Fusion’s WebCal support. Users can manage published views of their calendars, giving different options to different people as required.

To setup a view, users login to MailSite ExpressPro and select the calendar they wish to share with others as with the “Family Schedule” calendar shown below. The Calendar Editor appears with the details for the selected calendar. Under the Calendar Publishing section, a new view can be created for the calendar. This view can be for ever or a selected time period and consist of all events or just free busy information.

Users then click **Apply** to save the new view:


MailSite Express - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help del.icio.us
Calendar Help
mailsite
New Event Go To Today Day View Week View Month View Link To Outlook Refresh Logout
foo@qas-4.com/Calendars
Active time zone: /Europe/London
Mail
Calendars
Default
Family Schedule
Jul 2007
Mon Tue Wed Thu Fri Sat Sun
Tour de France
4:00 PM Manage
JULY 2007
Su Mo Tu We Th Fr Sa
Contacts
Settings
Done

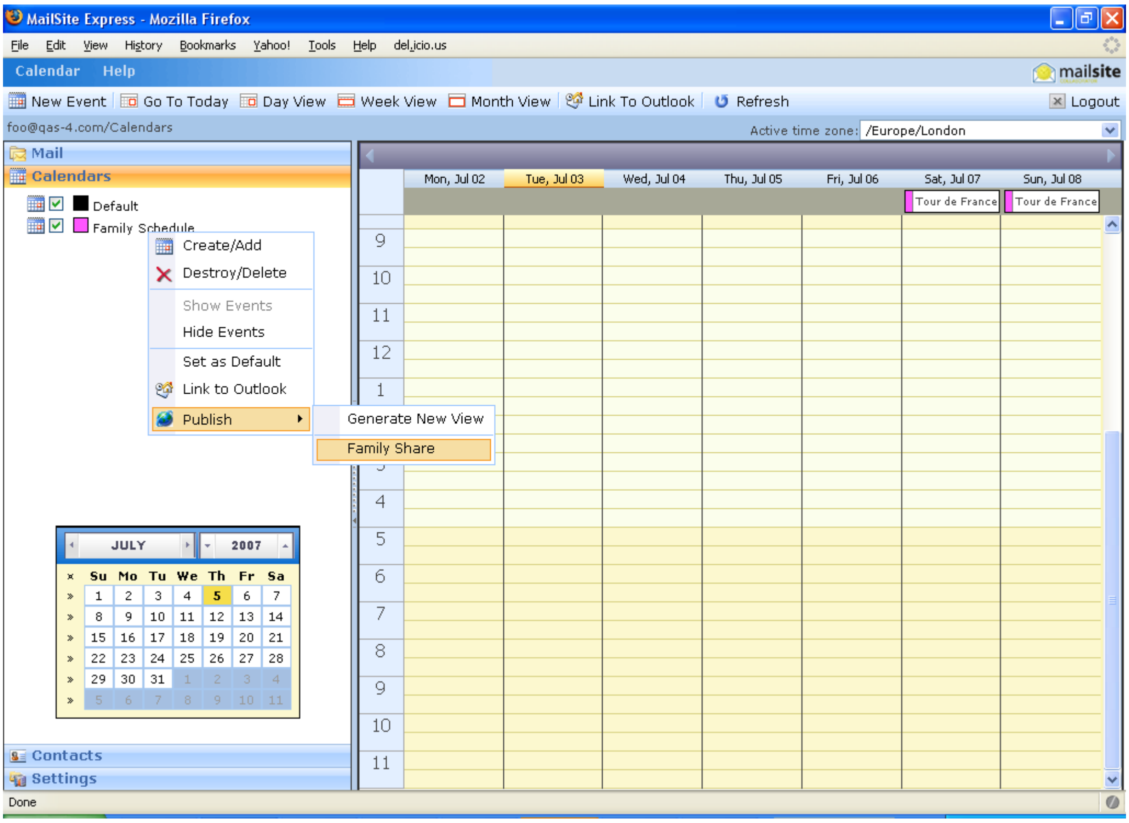
Calendar Editor
Apply Cancel

Name: Family Schedule
Color
Events: ● Show ○ Hide

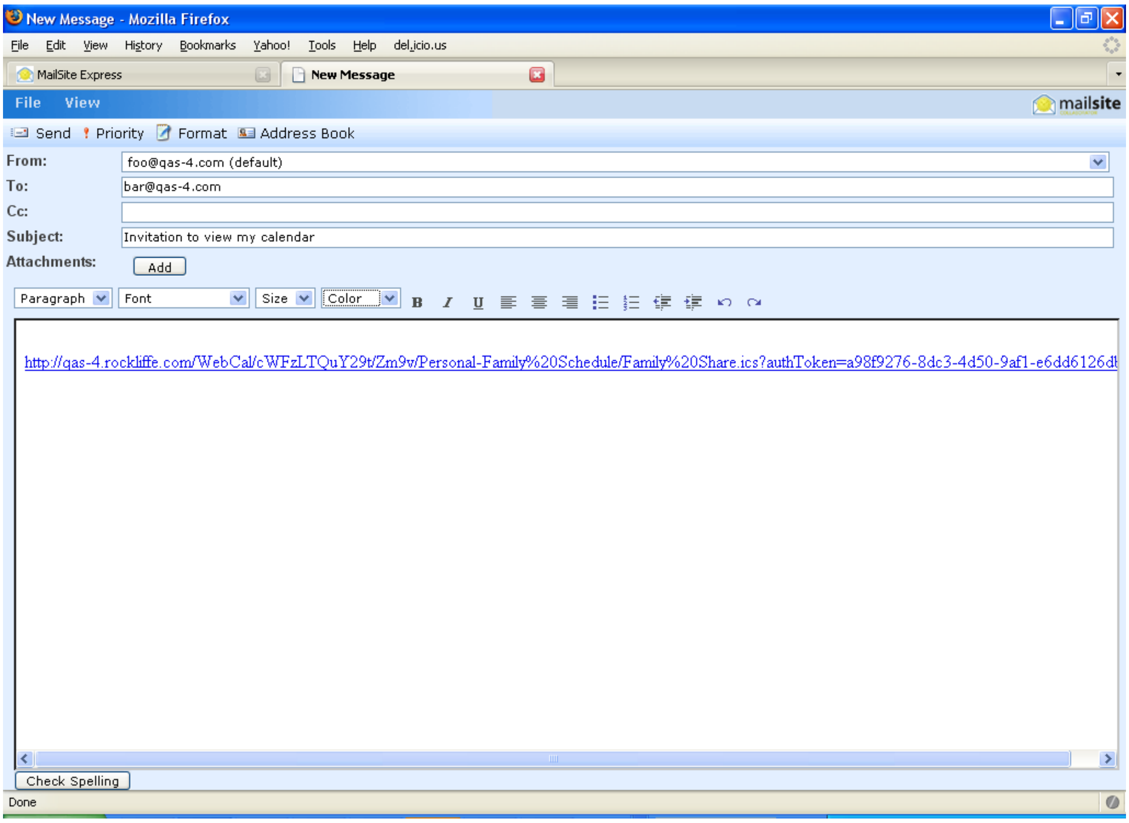
Calendar Publishing
Close

View Name: Family Share
Range: ○ All Events
● From Current Time To 6 Months
Detail: All
To Whom: Everyone
Add Another

Once the view has been created, it can be published. This can be done via the Calendar Editor as before, or by right-clicking on the calendar:



This brings up the compose mail screen with the link ready to send to the person or people with whom the calendar should be shared.



From: foo@qas-4.com (default)

To: bar@qas-4.com

Cc:

Subject: Invitation to view my calendar

Attachments:

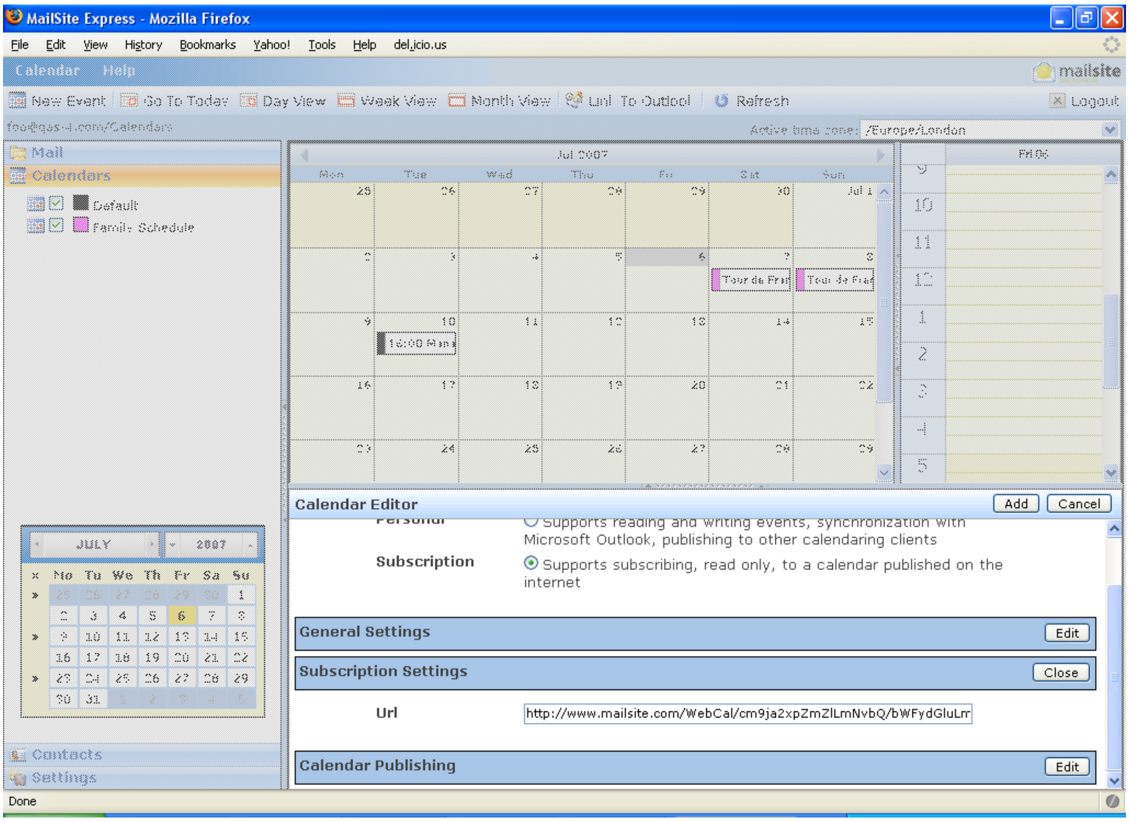
http://qas-4.rockliffe.com/WebCal/cWFzLTQuY29t/Zm9v/Personal-Family%20Schedule/Family%20Share.ics?authToken=a98f9276-8dc3-4d50-9af1-e6dd6126d

Assuming the recipient has an iCalendar compliant client such as Microsoft Outlook 2007, Apple iCal or Mozilla Lightning/Sunbird, their calendar client will subscribe to the published view when they click on this link. MailSite calendar views refresh periodically so that the subscriber keeps up to date with calendar changes.

Subscribing to calendars

MailSite ExpressPro allows users to subscribe to remote calendars in the iCalendar format. These will have a URL with the .ics extension. The calendar might belong to another MailSite Fusion user or one of the many other iCalendar compliant services such as Google Calendar or iCalShare.

To add a calendar subscription to MailSite ExpressPro, it is necessary to create a new calendar via the Calendar menu or by right-clicking on one of the existing calendars and selecting **Create/Add**.



MailSite Express - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help del.icio.us
Calendar Help
mailsite
New Event Go To Today Day View Week View Month View Link To Outlook Refresh
Logout
foo@qas-4.com/Calendars
Active time zone: /Europe/London
Mail
Calendars
☑ Default
☑ Family Schedule
Jul 2007
Mon Tue Wed Thu Fri Sat Sun
Tour de Fra
Tour de Fra
16:00 Mari
Fri 06
JULY 2007
Mo Tu We Th Fr Sa Su
Contacts
Settings
Done

Calendar Editor Add Cancel

Personal ○ Supports reading and writing events, synchronization with Microsoft Outlook, publishing to other calendaring clients

Subscription ● Supports subscribing, read only, to a calendar published on the internet

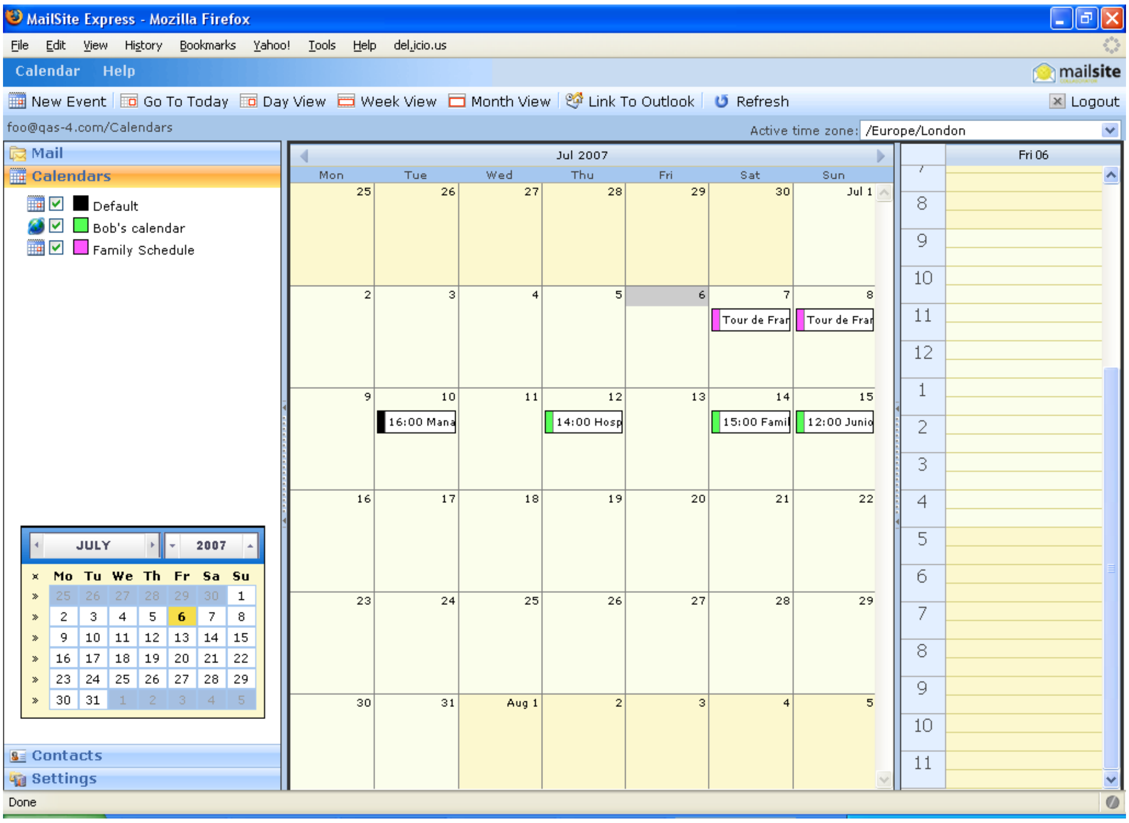
General Settings Edit

Subscription Settings Close

Url http://www.mailsite.com/WebCal/cm9ja2xpZmZlLmNvbQ/bWFydGluLm

Calendar Publishing Edit

Users select the Subscription calendar type, choose a name and color for this calendar, and then provide the URL for this resource. Once Add is clicked, this calendar will be added to the calendars available as shown below, where “Bob’s Calendar” is the view of a co-worker’s calendar allowing them to schedule meetings effectively. Subscribed calendars are read-only but will check for updates when appropriate.


MailSite Express - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help del.icio.us
Calendar Help
mailsite
New Event Go To Today Day View Week View Month View Link To Outlook Refresh Logout
Mail
Calendars
Contacts
Settings
Done

foo@qas-4.com/Calendars

Active time zone: /Europe/London

☑ ■ Default
☑ 🟩 Bob's calendar
☑ ■ Family Schedule

Jul 2007

Mon	Tue	Wed	Thu	Fri	Sat	Sun
25	26	27	28	29	30	Jul 1
2	3	4	5	6	7 Tour de Fran	8 Tour de Fran
9	10 16:00 Mana	11	12 14:00 Hosp	13	14 15:00 Famil	15 12:00 Junio
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	Aug 1	2	3	4	5

JULY 2007

×	Mo	Tu	We	Th	Fr	Sa	Su
»	25	26	27	28	29	30	1
»	2	3	4	5	6	7	8
»	9	10	11	12	13	14	15
»	16	17	18	19	20	21	22
»	23	24	25	26	27	28	29
»	30	31	1	2	3	4	5

Fri 06

7
8
9
10
11
12
1
2
3
4
5
6
7
8
9
10
11

Mailboxes

A *mailbox* is an individual e-mail account that typically corresponds to a person who uses it to send and receive mail. Each MailSite mailbox is comprised of two things:

⇒ *Mailbox information*, which defines the e-mail address, name, auto-reply settings, and other information related to the account

⇒ A *mailbox directory*, which contains the e-mail messages received for the account.

Mailbox directories are stored on the file system, while mailbox information may be stored in a variety of locations, depending on your preferences (and MailSite license). The following sections describe the types of mailboxes available and the tasks associated with managing mailboxes.

Types

MailSite supports four different types of mailboxes, depending on your license key: Registry Mailboxes, NT Mailboxes, Database Mailboxes, and SQL Mailboxes.

Registry Mailboxes are local to MailSite and do not have access to any other parts of your operating system. The password and user configuration information is stored in the Registry. Use Registry Mailboxes if your users will only use the server to send and receive mail. This will limit their permission to mail and will definitely prevent them from accessing any other part of the operating system.

NT MailBoxes are authenticated against the Windows NT User Database. NT Users may have access to other aspects of your NT system such as part of the file system. The password is maintained in the NT user Database. Use this type of mailbox if you want your users to access other components of your NT server, such as the file system. This means 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.

Database Mailboxes are authenticated against a table in an ODBC database. The password is maintained in the database table. Your license key may not enable this mailbox type. Use this type of mailbox if you have a database that stores all of your usernames and passwords and wish to authenticate against this database.

SQL Mailboxes are fully integrated with a table in an ODBC database. All mailbox properties for SQL mailboxes are stored in the database table. This is the type of mailbox that is used when MailSite is configured to use the SQL Connector. Your license key may not enable this mailbox type.

Adding Mailboxes

Before your users can send and receive mail with MailSite, you must create a mailbox for each user. To create mailboxes from the MailSite Console program, open the **Domains** folder, select one of the existing domain directories within it, and open that domain's **Mailboxes** directory.

To create a new mailbox, click on one of these buttons:

Create a new **Registry Mailbox** by selecting this button on the toolbar. A **New Registry Mailbox** icon will be displayed and you can enter the name of the mailbox in the field next to the icon.

Create a new **NT Mailbox** by selecting this button on the toolbar. The **Add NT User** form will be displayed. NT Users are created through the User Manager program. Select the **User Manager** icon in the MailSite program group to run this program.

Create a new **Database Mailbox** by selecting this button on the toolbar. The **Add Database Mailbox** form will be displayed. Your license key may not enable this mailbox type.

Create a new SQL Mailbox by selecting this button on the toolbar. The Add SQL Mailbox form will be displayed. Your license key may not enable this mailbox type.

Each MailSite mailbox can have one or more aliases. If you wish to create aliases for the user, click on the Aliases Folder.

Postmaster Mailboxes

In MailSite, a mailbox called **postmaster** is created automatically in the default domain (this mailbox is not counted for licensing purposes.) If you wish messages addressed to the **postmaster** to go to a different address, you can use either the mail forwarding facility or the alias table to achieve this.

Mail addressed to **postmaster@virtual.domain** will cause that account to be automatically created in accordance with accepted internet standards.

Catchall Mailboxes

The mailbox name catchall is special. If the **catchall** mailbox exists in the virtual domain **abc.com**, then incoming mail addressed to a non-existent mailbox, such as **unknown@abc.com**, will instead be delivered to the **catchall@abc.com** mailbox. If the **catchall** mailbox does not exist in the virtual domain, the message will be delivered to the **catchall** mailbox in the default domain, if it exists.

Converting Mailboxes

As described above, there are four different types of MailSite mailboxes. Although you will typically create mailboxes of one type, you can also convert your existing mailboxes to any of the four types. For example, as your user base grows, you may want to convert your Registry Mailboxes to Database Mailboxes.

To convert a mailbox from on type to another, use the **MSBOX** utility. This utility includes options for listing mailboxes by type and changing the type of one or more mailboxes. For example, you can convert all of your existing Database Mailboxes to Registry Mailboxes by executing the following commands in the Command Prompt:

```
msbox -list mailsite.com 2 > users.txt
msbox -plugin @users.txt 0
```

With these two commands, **MSBOX** generates a list of Database Mailboxes (type **2**) and saves the list to the file **users.txt**, and then converts each mailbox listed in this file to Registry Mailboxes (type **0**). Refer to the Utilities Appendix for more information on **MSBOX**.

Automatic Mail Handling

MailSite provides very powerful features for automatically handling incoming messages. This can be useful in a variety of circumstances.

The automatic mail handling features are set up on an individual mailbox basis. These features include Automatic Reply and Automatic Forwarding. These features are configured using the Mailbox AutoReply page in the MailSite Console.

Automatic Reply Facility

You can configure MailSite to automatically reply to incoming messages for a specific mailbox. The Auto Reply feature is set up on an individual mailbox basis. To set up the auto reply feature for a particular mailbox, invoke the Properties form by double clicking on the appropriate icon in the Mailbox folder in the MailSite Console.

The Automatic Reply feature can be useful in a variety of circumstances:

- You may wish to setup a mailbox for receiving sales inquiries for your corporation. For instance, you can create a **sales** mailbox and configure MailSite to send an automatic reply that acknowledges receipt of the message and forwards the message to the appropriate destination.
- You may wish to setup special mail handling for a former employee. For instance, you can configure MailSite to automatically reply to all messages for that employee with a new message with a forwarding address explaining that the person is no longer employed with your company. You can also configure MailSite to automatically forward the messages to the former employee’s new address.
- A user who is on vacation may wish to automatically reply to new mail with a message explaining that she is on vacation and when she will return.

Here are some detailed examples of these scenarios:

Former Employee

Enter the text of the reply in the **Message** field on the Mailbox AutoReply form:

```
Ms Smith has left the ABC organization.  Her new address is
smith@xyz.com.  Please do not send further
correspondence to smith@abc.com.
```

Select **Echo Message** to repeat the original message in the replied message. You should select to **Reply Just Once** to prevent mail bouncing off a mail list server. Enter **postmaster@abc.com** in the **Reply From** field. You should also enter Ms Smith's new address in the **Forward To** field and select **Don't Deliver to this mailbox**.

Vacation

Enter the text of the vacation reply in the **Message** field on the Mailbox AutoReply form:

```
Thanks for your mail. This is an automatic reply.
I'm on vacation until 13 July, and will attend to your
message then.  You can send me more mail, and you won’t get a
second copy of this message.
```

Select **Echo Message** to repeat the original message in the reply message. You should select to **Reply Just Once** to ensure that each sender just gets one vacation message. Make sure that you do not have a **Forward To** address.

Automatic Forwarding

You can configure MailSite to automatically forward messages arriving for a specific mailbox. You can forward messages to one or more addresses by separating each address with a comma.

Automatic Forwarding can be useful in a variety of circumstances. For example:

Sales Inquiries

You can create a **sales** mailbox for prospects to use when inquiring about your products and prices. Set the **Forward To** field in the Properties form to forward all incoming mail messages to the employee in your company that deals with these inquiries. You have the option of discarding the original message after it has been forwarded, or selecting to deliver the message to the **`sales`** mailbox.

Mailbox Quotas

MailSite provides support for Mailbox Quotas, which allow you to limit the size to which a mailbox can grow. This is particularly useful for IMAP mailboxes, where the messages typically remain on the server.

Mailbox Quotas can be set at three different levels: for the whole server, for all users in a domain, or for a specific mailbox. Each quota setting has two levels: **`Quota Level`** and **`Warning Level`**. When the size of a mailbox reaches the Warning Level, the user (and optionally the postmaster) receives a warning message from the system. When the size of a mailbox reaches the Quota Level, all new messages addressed to the user are rejected. Delivery of new messages to the mailbox will resume once the user deletes some messages from his mailbox.

Refer to the section on Quotas for more information.

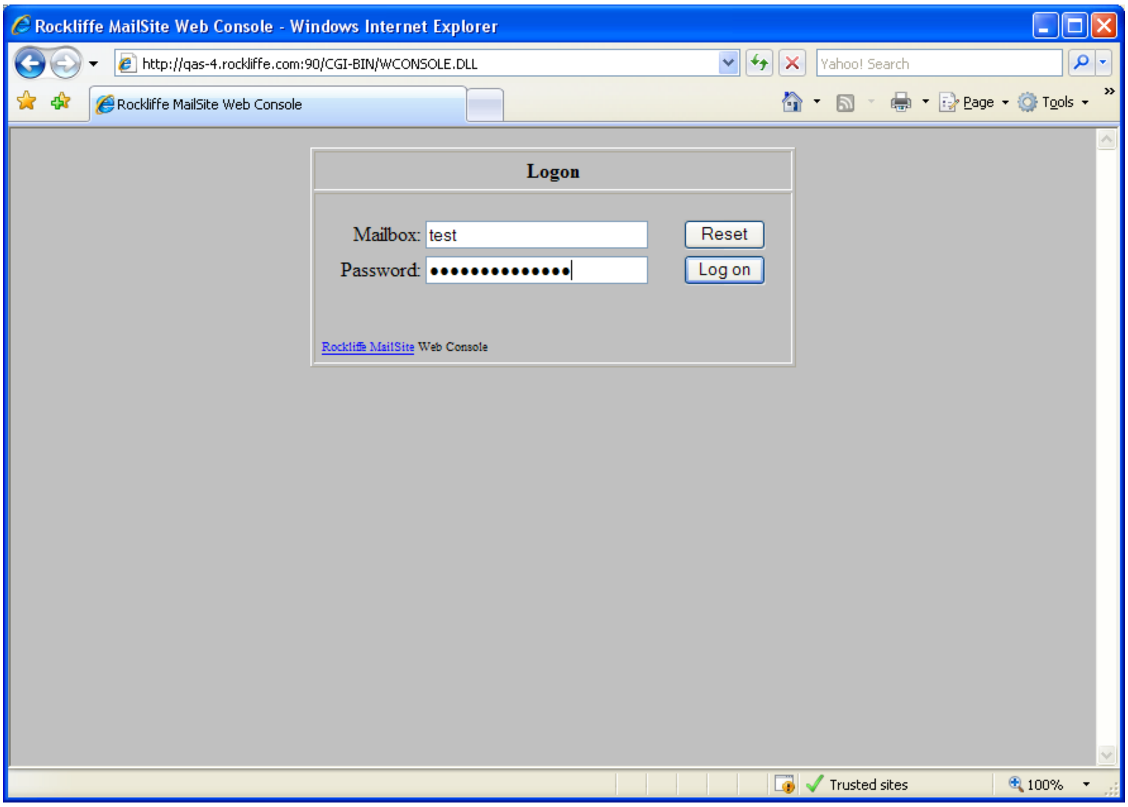
Web Mailbox Administration

You can administer mailboxes from any Web browser on the Internet. The HTTP Management Agent provides this function. To login to the Web Console, connect to the following URL:

⇒ **`http://host.domain.com:port`**

Where **`host.domain.com`** is the TCP/IP name of your MailSite server, and **`port`** is the HTTP Port configured in the properties of the HTTP Management Service. The default **`port`** number is **`90`**.

This will display the Logon Page of the Web Console:


Rockliffe MailSite Web Console - Windows Internet Explorer
Yahoo! Search
Rockliffe MailSite Web Console
Page
Tools
Logon
Reset
Log on
Rockliffe MailSite Web Console
Trusted sites
100%

http://qas-4.rockliffe.com:90/CGI-BIN/WCONSOLE.DLL

Mailbox: test

Password: ••••••••••••••

Enter your e-mail address and password. Your e-mail address consists of the name of your mailbox, the @ character, and the name of your mail domain. If your mailbox is in the default domain, then you can omit your mail domain.

Your privilege level determines whether you can administer your own mailbox, other mailboxes in your domain, or mailboxes in all domains. Your privilege level also determines which mail lists you can administer. The **`Privilege Level`** is a property of your mailbox and is set in the Mailbox General form. The choices are **`Server`**, **`Domain`**, or **`None`**.

If your privilege level is **`None`**, then you will be logged onto your Mailbox Properties form. You can set all of your mailbox properties using this form (except your privilege level). You can also administer mail lists that you moderate.

If you have **`Domain`** privilege, then you will be able to add, delete and modify mailboxes and mail lists in your own domain. If you have **`Server`** privilege, then you will be able to add, delete and modify mailboxes and mail lists in all domains. A more detailed guide *Customizing the MailSite Web Console* is available for download from the MailSite website.

Mail Lists

Mail Lists allow messages to be easily distributed to groups of users. By using a mail list, you can broadcast a message to all *members* of the list by sending it to a single e-mail address. This is useful in a number of scenarios, such as:

⇒ Broadcasting a news letter to subscription list

⇒ Hosting an e-mail based discussion forum.

MailSite includes an integrated mail list processor to provide this capability. This section explains how to perform common mail list tasks, how mail lists work, and how to use the list processor commands.

Types

MailSite supports six types of Mail Lists, which each use a different method to store membership information.

Registry Lists store list membership in the registry. You can add and remove members through the console or by **SUBSCRIBING** and **UNSUBSCRIBING**.

SQL Lists store list membership in the SQL Server database. You can add and remove members through the console or by **SUBSCRIBING** and **UNSUBSCRIBING**.

NT Lists derive list membership from an NT Group. Use this type of list if you want to send mail to all users of a particular NT Group in your domain.

Text File Lists store list membership in a text file. You can add and remove members through the console or by **SUBSCRIBING** and **UNSUBSCRIBING**, or by editing the text file directly. Use this type of list if you want greater flexibility in changing list membership. Text File Lists are stored locally on the application server under the SPOOL. Clustered MailSite installations should therefore use SQL Lists or Database Lists.

Database Lists read list membership from a table or view in an ODBC database. You must maintain list membership with your database program outside of MailSite. Use this type of list if you want to include membership information from an existing database. This is also the ideal list type if you want to create a web-based tool for subscribing and unsubscribing users from lists.

Server Lists derive list membership from selected mailboxes on the server itself. Use this type of list if you want your mail list to broadcast messages to all users on your server, all users in a particular domain, or all users of a particular privilege level (Server, Domain, or None). Server Lists also include filters that allow certain mailboxes to be excluded from these lists.

How Mail Lists Work

When MailSite receives a message it checks the domain name component in the **To:** address. If the domain name corresponds to a domain registered on your server, MailSite assumes the message is for a local user or for a mail list. It checks the list names to see if a list with a matching name exists. If so, the message is temporarily delivered to that list directory.

Note that it is no longer possible to create a mailbox with the same name as a mail list. It is advised that any such clashes which exist from previous installations should be resolved by the administrator.

MailSite will *explode* messages delivered to the mail lists by sending them onward to all list members. It handles messages delivered to **`-request`** directories by parsing them for commands and creating a *journal* file that it then returns to the sender.

Mail List Tasks

Creating a Mail List

Use the Mail Lists Folder in the Console program to create a new mail list in a specific domain. Messages addressed **`list@host.domain.com`** will be sent to members of this new mail list.

Joining a Mail List

Anyone can join a MailSite mail list. To join a list called **`info`**, send an email to **`info-request@host.domain.com`** in plain text format containing:

⇒ **`SUBSCRIBE`**

or

⇒ **`JOIN`**

as the first and only line in the message body. MailSite will respond with a message indicating success or failure.

If a list is moderated and **`Moderator Control Join`** is enabled, any **`SUBSCRIBE`** request will be forwarded to the moderator. The moderator can determine whether the subscription request should be permitted, and if so can add the address to the list of members.

If you wish to subscribe under an alias e-mail address, include a **`Reply-to:`** header in your mail message. This is the address that will be subscribed to the list and the response to your command will be sent to that address.

The extended JOIN command is disabled by default, but can be enabled on the List Security Page of the MailSite Console.

Leaving a Mail List

Leaving a list is similar to joining a list. To leave a list called **`info`**, send an email to **`info-request@host.domain.com`** in plain text format containing:

⇒ **`UNSUBSCRIBE`**

or

⇒ **`LEAVE`**

as the first and only line in the message body. If a list is moderated and **`Moderator Control Leave`** is enabled, any **`UNSUBSCRIBE`** request will be forwarded to the moderator. The moderator can determine whether the unsubscription request should be permitted, and if so can remove the address manually.

If you have changed your mail address, and wish to unsubscribe your old address subscribing your new address, then include a **`Reply-to: oldname@old.domain.com`** header in your mail message. **`oldname@old.domain.com`** will be removed from the list (but the response to your command will be sent to that old address).

The extended LEAVE command is disabled by default, but can be enabled on the List Security Page of the MailSite Console.

Removing a Mail List

To remove a mail list, use the **`Delete`** button in the Mail Lists Folder of the MailSite Console.

Creating a Digest List

Suppose you've created a popular mailing list called **`cars`**, which receives 10 or 20 messages per day. There may be people who would like to subscribe to the list, but don't want to receive every message the moment it is sent. You can set up a *digest* mail list (in this case, **`cars-digest`**) which accumulates all the messages received in one day and sends them in a single message.

With MailSite, you create a digest mailing list that is associated with an existing MailSite mailing list. To do this, select the Mail List folder in the Console. Select the domain containing the list you want to create a digest for, and use the normal list-creation mechanism to create a new mailing list. Assign the same name as the existing list with the word **`-digest`** appended to it. So if you want to create a digest list for an existing list called **`discuss`**, create a new list called **`discuss-digest`**. The **`-digest`** postfix tells MailSite to treat the list specially.

As far as the mail list subscriber is concerned, the digest list can be subscribed to and unsubscribed from just like other mailing lists. For instance, to subscribe, the user would send a **`JOIN`** command **`to discuss-digest-request@myco.com`**. Note that a digest mailing list must be in the same domain as the list that it digests.

You cannot submit messages to the digest list. Any attempt to do so will result in a non-delivery message being returned. Messages must be submitted to the main list (**`discuss@myco.com`**).

When you open the properties for a digest list in the Console, you will find that there is an extra page called **`Digest`**. You can use this page to control the extra properties of the digest list.

In the List General Page, you will find that the fields relating to list moderation have been disabled. This is because list moderation is not necessary for digests.

Also in the List General Page, the function of the **`Maximum message size`** field is slightly different for digest lists. If this is non-zero, then messages will be accumulated until the maximum size is reached, or the normal digest accumulation period is reached (whichever is sooner).

If a mail list has a digest, you can use the **`Members and digesters`** radio button to specify that members of the list itself and members of the digest list may both submit messages to the list.

Mail List Processor Commands

Commands understood by the mail list processor are as follows.

`HELP`	Replies with a help message
`JOIN [listname] [address]`	Subscribe to mailing list
`LEAVE [listname] [address]`	Unsubscribe from mailing list
`STOP`	Stop processing commands (*e.g.* to avoid processing a signature)
`SUBSCRIBE [listname] [address]`	Subscribe to mailing list
`UNSUBSCRIBE [listname] [address]`	Unsubscribe from mailing list
`REVIEW`	Request a membership listing

The extended form of the **`JOIN`** and **`LEAVE`** command using the **`[listname] [address]`** is disabled by default. It can be enabled through the List Security Page. The **`[address]`** can be in any valid RFC822 form.

The **`REVIEW`** command is available to the list moderator if enabled on the List Security Page.

List Processor Examples

Here are some example extended **`JOIN`** and **`LEAVE`** commands. Note that **`SUBSCRIBE`** and **`UNSUBSCRIBE`** are synonyms for **`JOIN`** and **`LEAVE`**.

```
JOIN thelist "John Smith" jsmith@myco.co.uk
LEAVE thelist smith@domain.com (Joe Smith)
SUBSCRIBE thelist Jane Doe <janed@super-isp.net>
UNSUBSCRIBE thelist peter@my-university.edu
```

List Agent

A message to a mailing list (or to a mail list's **`-request`** address) may be pre-processed by an external program before being acted upon by MailSite. The external program must be a command-line program or a batch file. It must not be an interactive program (i.e. requiring user keyboard input), nor may it be a Windows program. It must be efficient and must terminate reasonably quickly, since MailSite will not process any other list messages while it is running.

Mailbox agents can be used to implement a wide range of features. Some examples are:

- ⇒ A program that filters **`LEAVE`** and **`UNSUBSCRIBE`** messages
- ⇒ A program that checks a mail message for offensive language
- ⇒ A program that provides additional mail list processor commands
- ⇒ A program that implements additional mail loop prevention techniques

Mail List Directories

When MailSite receives a message addressed to a mail list in one of its local domains, the way in which the message is handled depends on the type of mail list.

Local Lists

For local lists such as Text File lists, the message is temporarily delivered to an appropriate subdirectory under the **`BOX`** directory. The list itself is stored under the **`lists`** directory.

For example, suppose the mail spool directory is **`C:\Program Files\MailSite\SPOOL,`** and the **`BOX`** directory is **`C:\Program Files\MailSite\BOX`**. MailSite will automatically create a subdirectory called **`lists`** under the **`SPOOL`** location. Inside this **`lists`** directory, there will be a subdirectory for each mail list in the default domain which stores the text file containing members of that list. MailSite will also automatically create a subdirectory for each list in the `BOX` location, with an `INBOX` below it, in similar style to individual mailboxes. Mails to the `list-request` address will be stored in a `Request` folder created below the `INBOX`.

Subdirectories will also be created for each virtual domain to contain the list directories for lists within those domains. Thus, if there is a list called **`staff`** in the default domain, and there is another list called **`chat`** within the virtual domain **`xyz.com`**, then the directory structure would be:

```
C:\Program Files\MailSite\BOX\staff\INBOX
C:\Program Files\MailSite\BOX\staff\INBOX\Request
C:\Program Files\MailSite\SPOOL\lists\staff-request
C:\Program Files\MailSite\BOX\~xyz.com\chat\INBOX
C:\Program Files\MailSite\BOX\~xyz.com\chat\Request
C:\Program Files\MailSite\SPOOL\lists\~xyz.com\chat-request
```

Centralized Lists

For centralized lists such as SQL lists, the message is stored under the BOX directory in the same manner as messages to individual mailboxes, and the list itself is stored in the SQL database rather than the filestore.

For example, suppose the BOX directory is **`\\NAS-1\BOX`**. MailSite will automatically create two subdirectories for each mail list in the default domain: one for messages to the list itself, and one for messages to the **`list-request`** address. Subdirectories will also be created for each virtual domain to contain the list directories for lists within those domains. Thus, if there is a list called **`staff`** in the default domain, and there is another list called **`chat`** within the virtual domain **`xyz.com`**, then the directory structure would be:

```
\\NAS-1\BOX\staff\INBOX
\\NAS-1\BOX\staff\INBOX\Request
\\NAS-1\BOX\~xyz.com
\\NAS-1\BOX\~xyz.com\chat\INBOX
\\NAS-1\BOX\~xyz.com\chat\INBOX\Request
```

These directories are created automatically by MailSite as needed. Note that domain subdirectories are preceded by a tilde (~), to distinguish them from list directories. Mail list names may not contain a tilde.

Messages are only held briefly in these directories, so you will typically find them empty. However, you may place certain files in these directories, which will affect how MailSite deals with mail list messages. Refer to the section on List Messages for details.

Mail List Content Moderation

Content Moderation is a feature that allows mail list moderators to approve or reject messages sent to a mail list. This level of list administration requires that the user have an account in a local domain. To enable this feature, select the **`Moderator controls content`** feature in the List General Page.

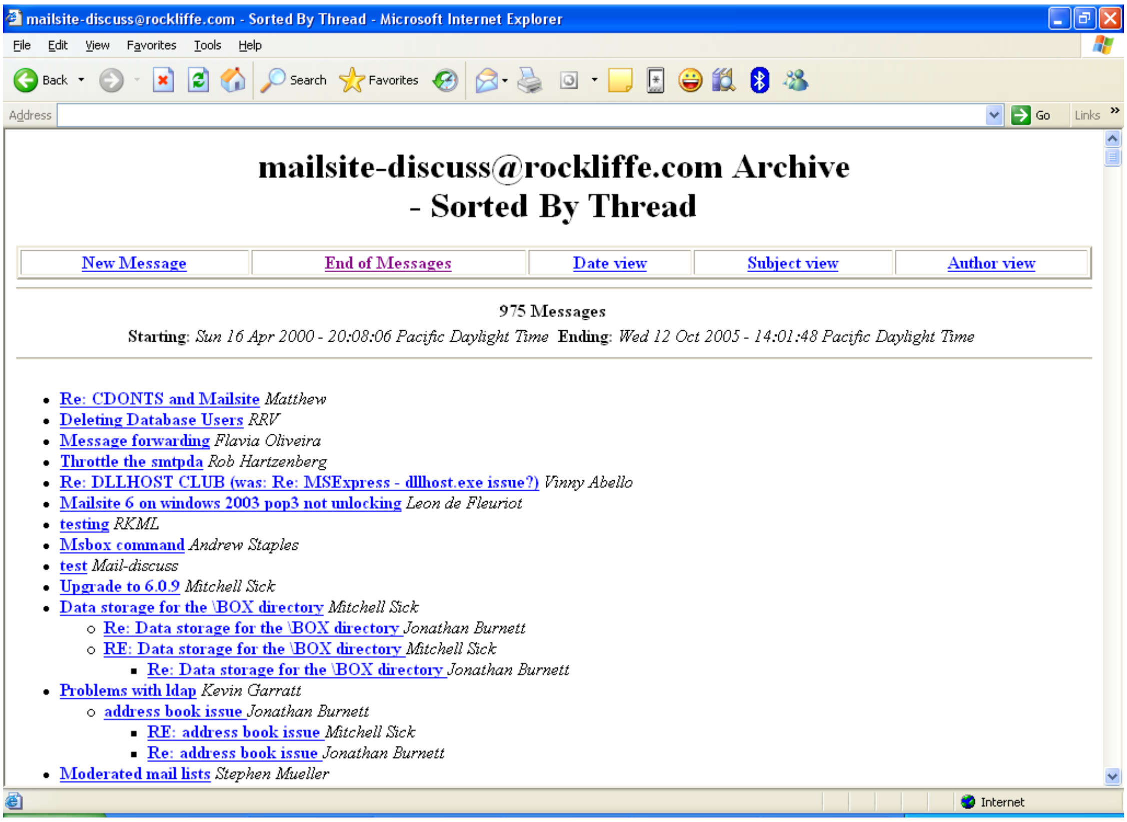
When a new mail list message arrives to MailSite, it will first be checked to see if its author may post to the list. If the author does not have posting permission (*e.g.* if he is not a member of the mail list and the mail list is set to disallow posting by non-members), the message will be returned to the author with an appropriate rejection message. If the author does have permission, delivery processing depends on whether content moderation is enabled for the list.

If content moderation is enabled, then the message will be placed in the **`pending`** directory for that list. If content moderation is not enabled, then the message is placed directly into the mail list directory. List messages will remain in the **`pending`** directory until one of the mail list moderators logs in to the Web Console and select the Review page to review pending messages. Messages may be reviewed, and rejected, accepted or discarded where appropriate.

A more detailed guide *Customizing the MailSite Web Console* is available for download from the MailSite website.

Archiving List Messages

Messages sent to a mail list can be archived in HTML format so that they can be read through a web browser. Use the Web Archive mail list property page to enable this feature. When viewing a mail list archive, users can sort messages by sender, subject, date, or message thread:



mailsite-discuss@rockliffe.com - Sorted By Thread - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Internet

mailsite-discuss@rockliffe.com Archive - Sorted By Thread

New Message	End of Messages	Date view	Subject view	Author view

975 Messages

Starting: *Sun 16 Apr 2000 - 20:08:06 Pacific Daylight Time* **Ending**: *Wed 12 Oct 2005 - 14:01:48 Pacific Daylight Time*

- Re: CDONTS and Mailsite *Matthew*
- Deleting Database Users *RRV*
- Message forwarding *Flavia Oliveira*
- Throttle the smtpda *Rob Hartzenberg*
- Re: DLLHOST CLUB (was: Re: MSExpress - dllhost.exe issue?) *Vinny Abello*
- Mailsite 6 on windows 2003 pop3 not unlocking *Leon de Fleuriot*
- testing *RKML*
- Msbox command *Andrew Staples*
- test *Mail-discuss*
- Upgrade to 6.0.9 *Mitchell Sick*
- Data storage for the \BOX directory *Mitchell Sick*
  - Re: Data storage for the \BOX directory *Jonathan Burnett*
  - RE: Data storage for the \BOX directory *Mitchell Sick*
    - Re: Data storage for the \BOX directory *Jonathan Burnett*
- Problems with ldap *Kevin Garratt*
  - address book issue *Jonathan Burnett*
    - RE: address book issue *Mitchell Sick*
    - Re: address book issue *Jonathan Burnett*
- Moderated mail lists *Stephen Mueller*

The format of the web archive is controlled not only by the settings on that property page, but also by Archive Template files. For more information on customizing mail list archiving, see the appendix on Customizing Mail List Archiving.

Domains

MailSite allows you to receive messages addressed to multiple domains on a single server. This section discusses the steps you should follow to configure this feature.

Selecting the Domain Type

Before creating an additional domain, you need to understand which type of domain you want. There are three types of domains: Synonym Domains, Virtual Domains with Separate IP Addresses, and Virtual Domains with Shared IP Addresses.

Synonym Domains

Use Synonym Domains if you wish to deliver messages addressed to multiple domains into mailboxes in one domain. For example, you may receive messages for **`joe@mail.abc.com`** and **`joe@abc.com`** but wish to deliver them to mailbox **`joe`** in the default domain **`abc.com`**. The following restrictions apply:

⇒ The DNS record for each domain must point to the IP address of the domain

⇒ Users can login as **`joe`** or as **`joe@domain.com`**

⇒ The MailSite services will display the name of the default domain in the greeting message

For more information about the way that synonym domains affect the way the MailSite delivers mail, see the section on Delivery Precedence.

Virtual Domains with Separate IP Addresses

Use this configuration if you wish to create true virtual domains on your mail server. All of the mailboxes and mail lists will be created and managed separately under each domain. If you are an Internet Service Provider and you are hosting e-mail services for many business customers on a single server, then you may wish to choose this option. The following restrictions apply:

⇒ You must have one IP address available for each domain

⇒ The DNS record for each domain must point to the correct IP address

⇒ You can have a separate postmaster for each domain

⇒ Users can login as **`joe`** or as **`joe@domain.com`**

⇒ The MailSite services will display the name of the virtual domain in the greeting message

Virtual Domains with a Shared IP Address

Use this configuration if you wish to create virtual domains on your mail server. All of the mailboxes and mail lists will be created and managed separately under each domain. If you are an Internet Service Provider and you are hosting e-mail services for many business customers on a single server, then you may wish to choose this option. The following restrictions apply:

⇒ All domains can share a single IP address

⇒ The DNS record for each domain must point to the single IP address

⇒ You can have a separate postmaster for each domain

⇒ Users must login as **`joe@domain.com`** or **`joe%domain.com`**

⇒ Some e-mail clients do not support logging in as **`joe@domain.com`**. MailSite has implemented an alternative **`joe%domain.com`** to work around this limitation.

⇒ The MailSite services will display the name of the default domain in the greeting message

Setting the Default Domain Name

The Default Domain is identified in the MailSite Console by a gray folder with a red dot. You can rename the Default Domain by selecting the domain, clicking on the right mouse button, and selecting **`Rename`**.

If you wish to receive mail addressed to **`joe@abc.com`** and have it delivered to mailbox **`joe`** in the default domain, then you must set the name of the default domain to **`abc.com`**.

Creating the DNS Entries

Enabling MailSite to receive messages for multiple domains begins with your DNS configuration. You must create **`MX`** or **`A`** records in your DNS server for each domain. Each DNS record must resolve to the correct IP address. The IP address may be different if you selected domain option (2).

The TCP/IP addresses for your computer are maintained through the Network icon in the Control Panel. See the DNS Overview section for more information on configuring your DNS server.

Adding the Virtual Domains

If you selected domain option (2) or option (3), then the next step is to add a complete list of the domain names. You do this in the Domains folder in the MailSite Console. If you selected option (2), then you must associate an IP address with each domain. Do this by double-clicking on the Domain Properties Folder and setting the IP Address.

Adding the Mailboxes

Every user in each domain must have a unique mailbox. Create the mailboxes using the Mailboxes Folder in the MailSite Console. To create mailboxes in one of the virtual domains, select the name of the domain in the tree view.

Forwarding Domains

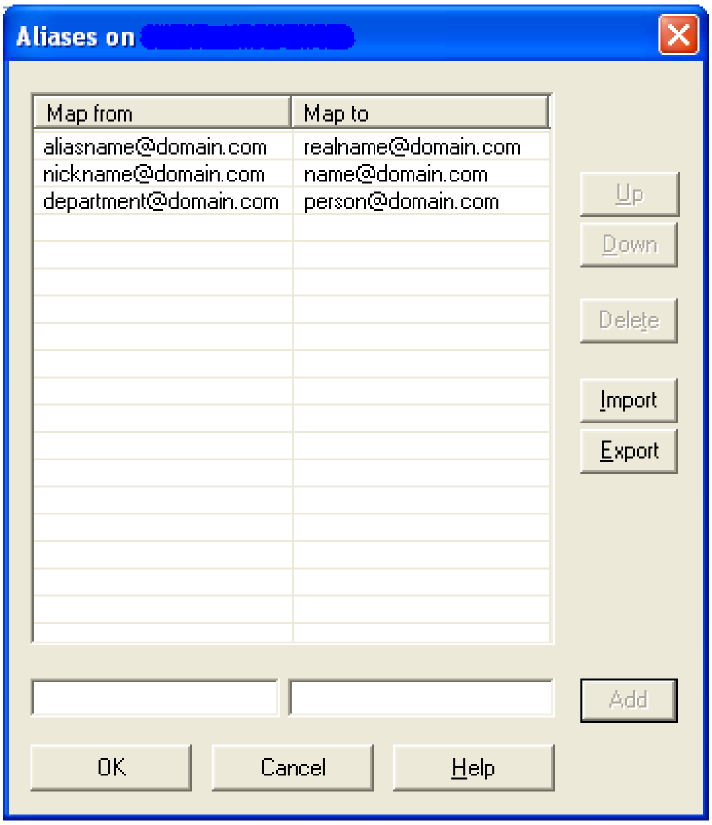
MailSite can also be used as an SMTP gateway to relay mail to and from other non-MailSite email servers. Once you have your domain created and your DNS configured properly, you can specify the mail server you want to forward mail to by entering this hostname in the Domain Properties: Relay Host option through the MailSite Admin Console.

Testing the Configuration

MailSite should be ready to send and receive mail for all of the domains at this point. Use an e-mail client to verify this. If you have problems, check the Troubleshooting section.

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:



Aliases on [redacted]

Map from	Map to
aliasname@domain.com	realname@domain.com
nickname@domain.com	name@domain.com
department@domain.com	person@domain.com

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:

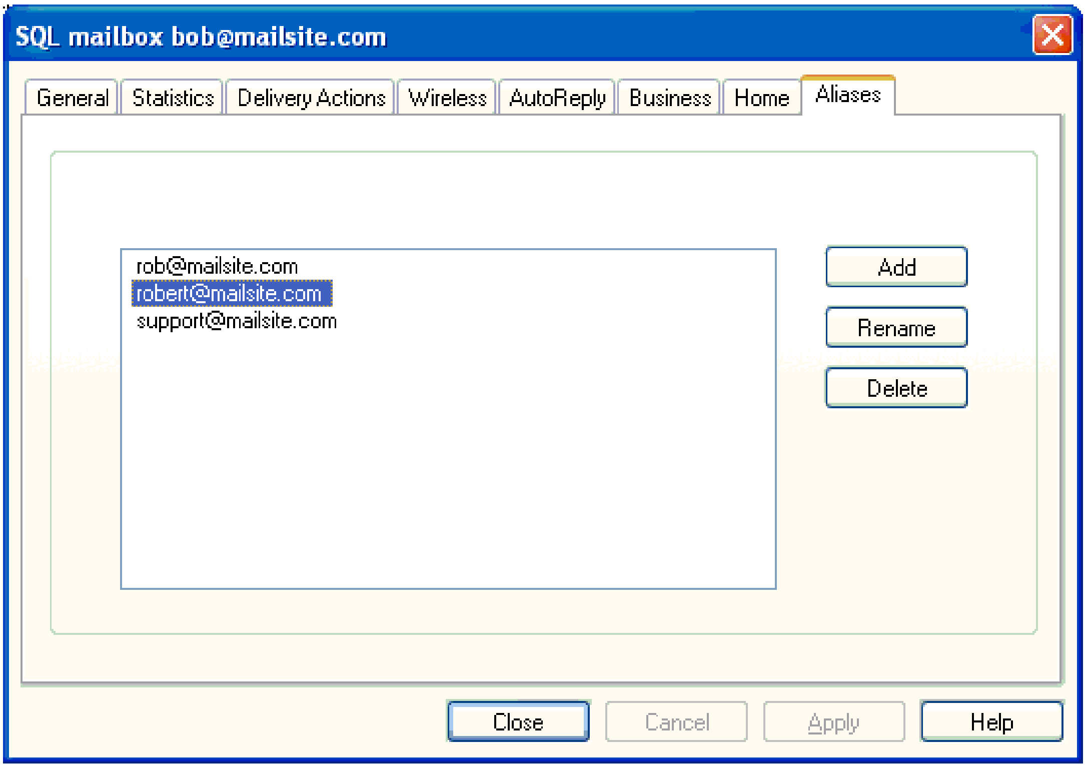
⇒ **`jim@abc.com -> james.smith@abc.com`**

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:

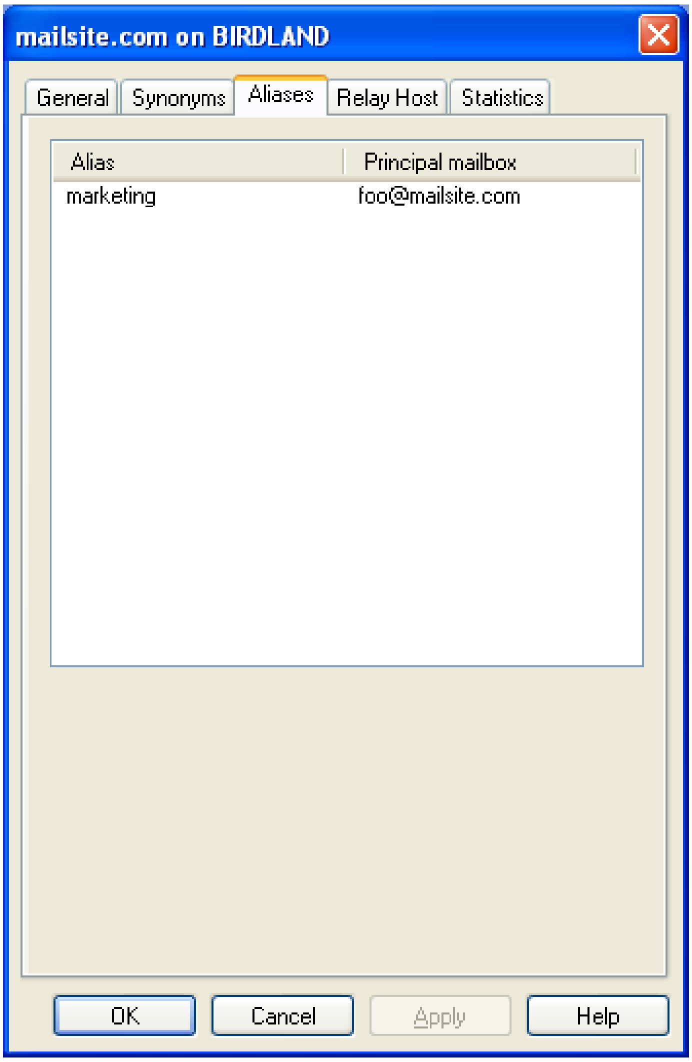


rob@mailsite.com
robert@mailsite.com
support@mailsite.com

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:



Alias	Principal mailbox
marketing	foo@mailsite.com

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 delivers messages to destination recipients based on an address precedence order. MailSite matches the **To:** address in this order:

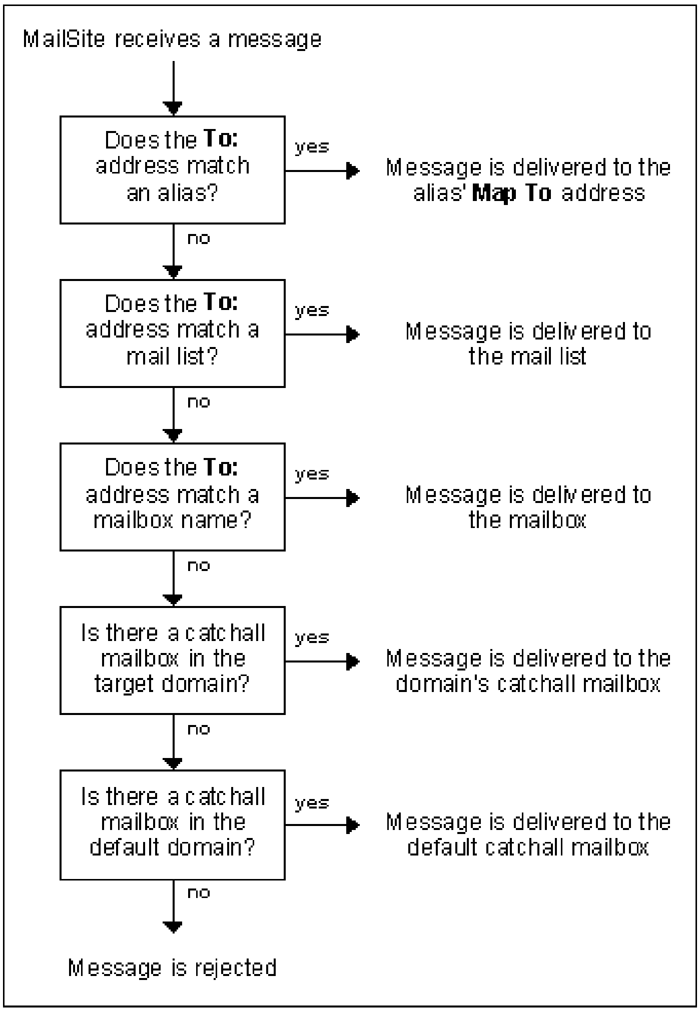
1. System-Level Aliases

2. Mail Lists

3. Mailbox-Level Aliases (SQL only)

4. Mailboxes

If a match is not found among these address types, the message will be delivered to a catchall mailbox (if one exists), or rejected by MailSite. The following diagram illustrates these delivery precedence rules in action:


MailSite receives a message
Does the **To:** address match an alias?
yes
Message is delivered to the alias' **Map To** address
no
Does the **To:** address match a mail list?
yes
Message is delivered to the mail list
no
Does the **To:** address match a mailbox name?
yes
Message is delivered to the mailbox
no
Is there a catchall mailbox in the target domain?
yes
Message is delivered to the domain's catchall mailbox
no
Is there a catchall mailbox in the default domain?
yes
Message is delivered to the default catchall mailbox
no
Message is rejected

Intermittent Connectivity

MailSite supports mail servers that do not have a full time Internet connection. This is useful in two situations:

- ⇒ MailSite is used as a central mail hub for dialup satellite mail servers.
- ⇒ MailSite is used as a satellite mail server with a dialup connection to an ISP or a central hub.

Central Hub with Dialup Satellite Servers

The SMTP Receiver supports the ETRN command, defined in RFC 1985, which allows a remote client to request delivery of mail queued for its domain. The **`MSSTART`** utility connects to a mail server and uses the **`ETRN`** command to initiate a mail download. An intermittently connected satellite server can initiate delivery of mail queued for its domain by establishing a TCP/IP connection and then running **`MSSTART`**.

Dialup Satellite Server

MailSite can be configured to dialup to the central hub on a predefined schedule. Once connected, MailSite can deliver any queued outgoing mail and can trigger delivery of any queued incoming mail.

Delivery of incoming mail can be triggered in one of two ways:

- ⇒ If the central hub is configured as a SMTP relay for the satellite, and it supports the **`ETRN`** command, then the **`MSSTART`** command will trigger incoming delivery.
- ⇒ If the central hub is configured to deliver all mail for the domain into a single POP mailbox, then the **`MSPOP`** command will pickup the mail and redistribute it to local mailboxes.

The dialup schedule and the incoming delivery trigger are set in the Time Of Day window in the MailSite Console. A batch file can be run as the incoming delivery trigger if **`MSSTART`** or **`MSPOP`** must be executed multiple times.

Mail Delivery Schedules

When MailSite attempts to deliver a message to a foreign domain (*i.e.* a domain other than the default domain or a virtual domain), it may encounter a number of problems. For example, the mail server for that domain may be down or otherwise temporarily inaccessible, or the server may not have enough disk space for the message.

A temporary delay of this nature will not cause the message to be treated as undeliverable. Instead, MailSite will store the message on disk (in the **`holding`** directory), and try again at some later time. Eventually, if the message still cannot be transmitted after a reasonable time, it will be treated as undeliverable. The Delivery Schedule Management tells MailSite when to attempt delivery of such stored messages.

MailSite supports two types of mail delivery schedules:

- ⇒ The Elapsed Time Schedule. Under this schedule, attempts to contact a domain will be made at a series of pre-configured intervals, commencing from the time at which the message was received.
- ⇒ The Time-Of-Day Schedule. Under this schedule, attempts to contact a domain will be made at specific, configurable, times of day.

You can control which destination domains use which kind of schedule. You can also force all domains to use Time-Of-Day Schedule by specifying **`!*`** in the Delivery Schedule Management dialog.

The elapsed time schedule is ideal when MailSite has a continuous, uninterrupted connection to the Internet. The time-of-day schedule is more appropriate when the Internet connection is intermittent – typically, a dialup connection.

You can also request MailSite to attempt immediate delivery of all messages for one or more domains.

MailSite can manage a dialup connection for you, if you so wish. Refer to the next section for more information.

Mail delivery schedules are managed through the Schedules Folder in the Windows Console. Refer to Schedule Management in the Windows Console Reference section for more information.

Dialup Support

The MailSite supports dialup connectivity to the Internet through the Microsoft Remote Access Service (RAS). This allows a computer running MailSite to dial into an Internet Service Provider (ISP) to exchange mail on a predetermined schedule.

In order to use the dialup support, you must install RAS. See the Microsoft documentation concerning RAS installation. You will need to create at least one RAS phonebook entry, containing the phone number of your ISP. Before configuring the dialup support in MailSite, check the basic RAS setup by dialing out to your ISP using the Dialup Networking tool provided with RAS. If this does not work, MailSite will not be able to dial out.

Dialup support in MailSite works like this: At regular intervals (which you can configure), MailSite dials your ISP. Once connected, it will execute a command to request the ISP's mail server to send mail to MailSite. It will also attempt to deliver outgoing mail through the normal MailSite mail routing mechanism (i.e. the DNS and the manual routing table). If you wish, you can configure the manual routing table such that all outgoing mail is routed to your ISP's mail server for it to forward—this may help reduce the time spent connected. When there is no more outgoing mail to send, and there are no incoming connections, the dialup connection will be closed and the phone disconnected.

Refer to Schedule Management in the Windows Console Reference section for more information.

Backup

Performing a Comprehensive Backup

To perform a comprehensive backup of your MailSite post office, you need to save several components:

Registry Configuration

When run with the Registry connector (the default mode), MailSite stores all of its settings in the Windows Registry of your server.

MailSite comes with a utility, **`MSBACK`**, that you can use to backup your registry configuration data to a text file. This file can then be included in your backup schedule. We highly recommend that you run this command in your daily backup script. Refer to the Utilities Appendix for more information on **`MSBACK`**.

Database Configuration

When run with the SQL connector, MailSite stores all of its settings in the database defined by this connector. Use the standard utilities that are part of your database software to back up the MailSite database on a regular basis.

Spooled Mail Messages

These files are located in the directories specified in the Directories dialog in the MailSite Console. All of these directories, together with any lower level directories, should be included in your backup schedule.

Mailbox Directories

These directories store e-mail messages for the mailboxes on your system, and are located in the mailbox root directory for each domain. The mailbox directory is defined in the General page of the Domain Properties window. All mailbox directories should be included in your backup schedule.

Directory Store Database

If you are using SQL mailboxes, you should also backup the SQL Server database file that contains account information.

Transferring MailSite to another computer

If you need to transfer your MailSite installation to another computer, you can do so by following this procedure:

- q Install the same version of MailSite on the destination computer
- q Stop the MailSite services on the source and destination computers
- q Run **`MSBACK`** on the source computer to save the configuration to a text file
- q Copy the text file to the destination computer
- q Edit the text file using **`NOTEPAD`**
- q Search for **`InstallDir`**, **`MailInBoxDir`**, **`MailLogDir`** and **`MailSpoolDir`**
- q Verify that these directories are correct on the destination computer
- q Run **`MSBACK`** to restore the configuration on the destination computer
- q **`XCOPY`** the spool and mailbox directories from the source to the destination computer
- q Reconfigure the DNS records to point to the IP address of the destination computer

- q Check the configuration on the destination computer using the Console
- q Start the MailSite services on the destination computer
- q Test the destination server by sending a message to yourself with your mail client

Refer to the Troubleshooting section if you have problems getting the destination server to work correctly. Refer to the Utilities Appendix for more information on **`MSBACK`**.

Security

Internet messaging protocols depend on messages, user names, and passwords that are mostly transmitted in clear text over TCP/IP connections. Without special configuration, the SMTP protocol allows unscrupulous Internet users to illegally relay messages through your server or send messages in bulk to mailboxes on your server. As the administrator of this system, you need to be aware of these security issues. This knowledge will help you set acceptable security policies for your site and configure your MailSite server accordingly.

Message Store Security

Mail messages and log files are stored on the file system on the MailSite server in plain text format. Mail messages may contain confidential information and log files may contain user names and message contents. We recommend that you take the following steps to prevent unauthorized access to these files:

⇒ Store mail messages and log files on an NTFS partition.

⇒ Use the File Manager or Windows Explorer to ensure that only the Windows account that the MailSite services run as has access to these files and directories. If you installed using the Simply security policy, MailSite runs as the **`SYSTEM`** user. If you installed using the Secure policy, MailSite runs as **`MailSite-user`** (or whatever account was specified during installation).

Password Security

In most cases, mailbox passwords are transmitted in clear-text over the network. It is possible for an unscrupulous computer expert to “sniff” the password by watching the TCP/IP packets pass by over the network. This risk is increased if your users are logging in to MailSite from a remote Internet site.

Passwords are exposed in the following transactions:

⇒ Checking mail from a POP or IMAP client.

⇒ Changing the password from a POP or IMAP client.

⇒ Logging in to the mailbox from a Web Browser.

⇒ Changing the password from a Web Browser.

There are a few precautions that you can take to minimize these risks:

⇒ **Use** APOP**,** AUTH **and** AUTHORIZE **to logon whenever possible**. These commands provide a method by which a POP3 or IMAP4 client can log into the server with an encrypted password. If you POP3 or IMAP4 client supports this capability, then we recommend that you use it.

⇒ **Change Passwords regularly**. It is good practice to establish a procedure that requires that your users change their passwords on a regular basis. This minimizes the exposure to sniffed passwords. You can use the MailSite Password Server to do this if your mail client supports this capability.

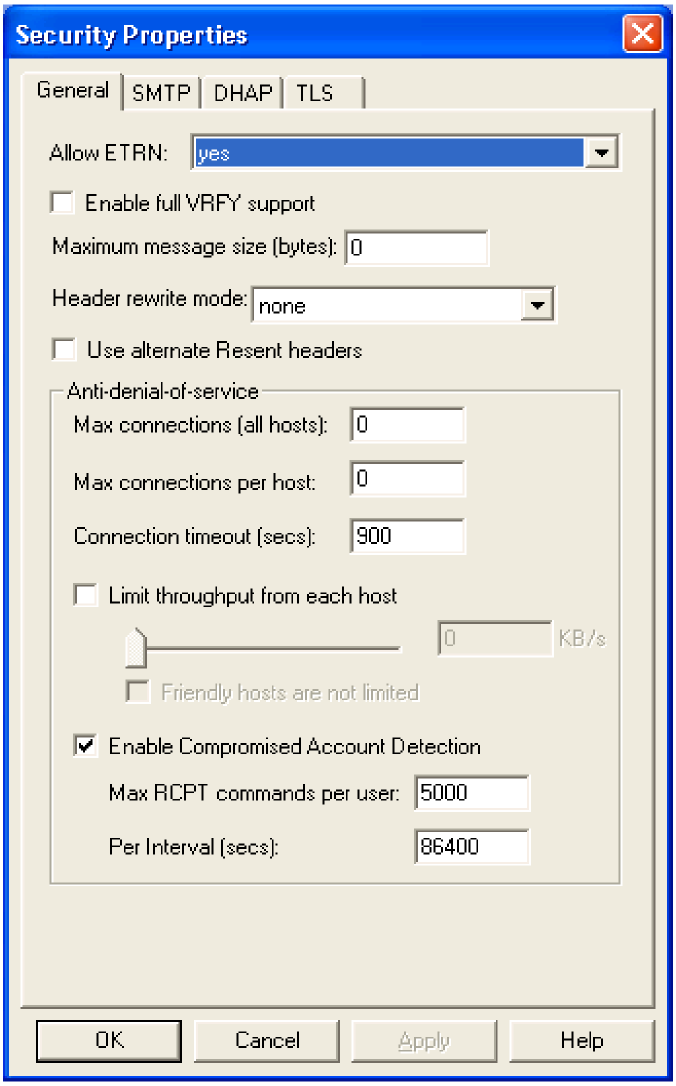
⇒ **Do not create Mailboxes for NT Administrators**. Your exposure is magnified if you create a MailSite mailbox based on an NT User with Administrative privileges. If the password for this user is sniffed then your whole NT Server is compromised. You can use MailSite Aliases and Auto Forwarding capabilities to forward incoming mail for administrative users to a secure Registry Mailbox. The drawback of this configuration is that the administrative users will have to maintain two passwords.

⇒ **Track Login Failures with the Performance Monitor**. You can use the Windows NT Performance Monitor to keep track of failed login attempts. This is useful to monitor password hacking attempts on the POP3 and IMAP4 servers. See the Performance Monitor section for more information.

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.



Allow ETRN: yes

☐ Enable full VRFY support

Maximum message size (bytes): 0

Header rewrite mode: none

☐ Use alternate Resent headers

Anti-denial-of-service

Max connections (all hosts): 0

Max connections per host: 0

Connection timeout (secs): 900

☐ Limit throughput from each host

0 KB/s

☐ Friendly hosts are not limited

☑ Enable Compromised Account Detection

Max RCPT commands per user: 5000

Per Interval (secs): 86400

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`

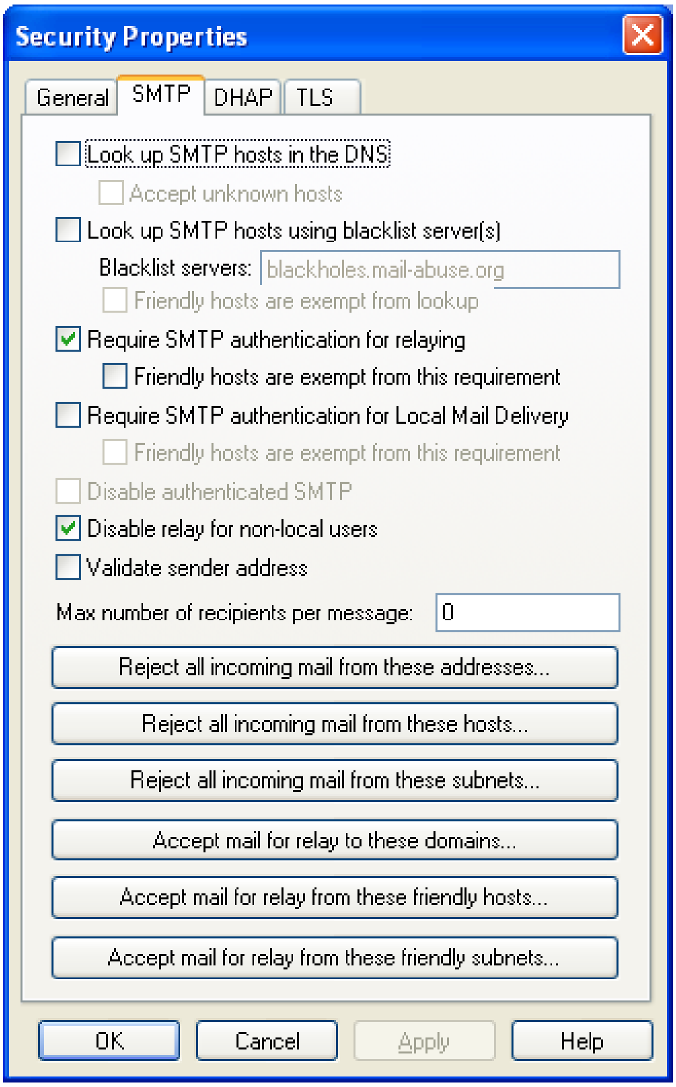
This option sets a limit to the number of seconds that MailSite will keep open a non-responsive SMTP connection.

`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:


Security Properties
General
SMTP
DHAP
TLS
Reject all incoming mail from these addresses...
Reject all incoming mail from these hosts...
Reject all incoming mail from these subnets...
Accept mail for relay to these domains...
Accept mail for relay from these friendly hosts...
Accept mail for relay from these friendly subnets...
OK
Cancel
Apply
Help

□ Look up SMTP hosts in the DNS

□ Accept unknown hosts

□ Look up SMTP hosts using blacklist server(s)

Blacklist servers: blackholes.mail-abuse.org

□ Friendly hosts are exempt from lookup

☑ Require SMTP authentication for relaying

□ Friendly hosts are exempt from this requirement

□ Require SMTP authentication for Local Mail Delivery

□ Friendly hosts are exempt from this requirement

□ Disable authenticated SMTP

☑ Disable relay for non-local users

□ Validate sender address

Max number of recipients per message: 0

- **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/SSL)

Security is a critical issue for system administrators. The best system administrators work to protect their email systems and are on constant guard against unauthorized system access.

A protocol is a standard format that enables two devices to transmit and receive date. In the world of Internet communications, protocols are the agreed-upon rules for messaging components, such as handshaking, message delimitation, and transmission mode and rate.

Email communications, Web server and browser interactions (such as online commerce), and telecommuting would not be possible—or safe—without these accepted protocols.

MailSite includes the Secure Sockets Layer (SSL) protocol. Secure Sockets Layer protocol, initially developed by Netscape Corporation, is a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Transport Layer Security (TLS), more commonly known as SSL, is a popular mechanism for enhancing TCP communications with privacy and authentication. TLS or Transport Layer Security is the IETF-endorsed version of SSL. TLS is a standard closely related to SSL 3.0, and is sometimes referred to as "SSL 3.1". MailSite supports both TLS 1.0 ("SSL 3.1") and SSL 3.0.

The SSL/TLS protocol uses signed digital certificates and a special cryptography method, called public key, for authentication. This method of authentication furnishes a way to verify the identity of each communicating pair, providing improved security not only for a particular email exchange, but also for the mail server and the system that host the exchange. In short, the SSL/TLS protocol enables the secure encryption of messages transmitted between client and server and between server and server. Administrators should be aware, however, that this added encryption and decryption activity places an extra processing load on the server.

While a full examination of digital certificates and public key cryptography is beyond the scope of this manual, brief descriptions of both are provided to assist system administrators in their duties.

Certificates

Digital certificates provide:

- Authentication—information stored on a certificate verifies that the person sending a message is who he or she asserts to be.
- Encryption—the encryption safeguards email so that it only those who are authorized can read it.
- Security—certificates help safeguard private information that is shared during exchanges, such as credit card information shared during online commerce transactions.

A certificate provides this protection by means of the information that is stored on it and the cryptographic keys that are linked with this stored data. The distinguished name (DN) format (the X.509 standard) defines how and what information is stored on certificates. Much like a paper-based driver's or business license that is kept in a wallet or in an office file and proffered to prove identity, a digital certificate contains identification information that is stored on a machine's hard disk. This identification information includes the common name (CO), organization name, city, state, and country location associated with a particular computer. Each certificate includes a serial number and the time period for which the certificate is valid (different certificates expire at different times). The private key and public key pair provides the encryption used with the certificate (see "Public Key Cryptography" below).

A company or entity that generates certificates is known as a certificate authority (CA). Many companies, including VeriSign/Thawte, GeoTrust, and Comodo (InstantSSL), sell digital certificates to individuals and businesses. An alternative to third-party certificates are self-signed certificates. Usually these certificates are created by an administrator that acts as his or her own certificate authority. (See the "Certificate Requirements" section of this chapter for more information about creating and installing certificates).

Although MailSite will work with self-signed certificates, we recommend that you obtain a certificate from a known and trusted certificate authority (CA).

Public Key Cryptography

Public key cryptography was developed over a quarter of a century ago. It is sometimes referred to as asymmetric encryption because it uses two keys—a public key and a private key. This cryptography system provides the authentication safeguards for digital certificates. Private key security is safeguarded by the numeric formulas and the number of digits (more than 100) used in these cryptographic operations.

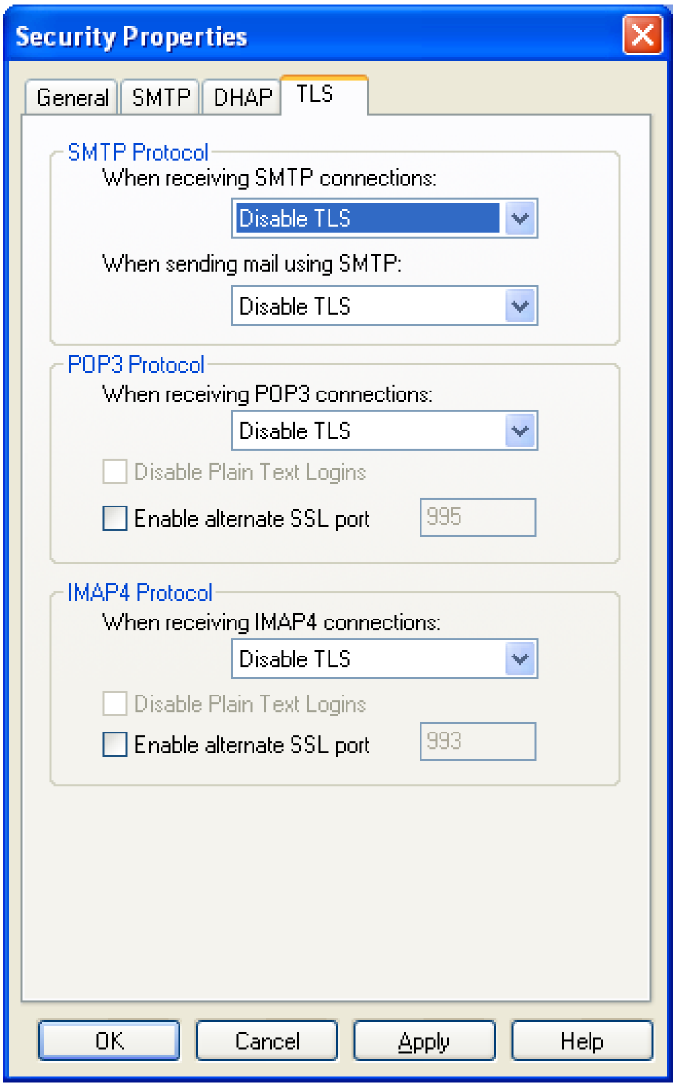
As its name implies, the public key is known to everyone and is used to encrypt an email message. The private key is known to only one entity (the message recipient) and is used to decrypt the message. Here is how it works: Jack sends an encrypted message to Jill by using Jill's public key. Once she receives this message, Jill uses her private key to decrypt the email.

Of course, Jack and Jill don't really have to worry about such encryption and decryption chores—their mail software and certificates manage this activity in the background.

Configuring MailSite to Use SSL/TLS

The system administrator must perform the following steps to configure MailSite to enable the new SSL/TLS protocol feature:

- Obtain a certificate from a trusted certificate authority or create a self-signed certificate (see the "Generating a Test Certificate" section that follows). A system administrator may want to use a self-signed certificate for testing purposes.
- Install the certificate in the Personal folder of the Computer certificate store using the MMC Certificates snap-in.
- Use the MailSite Security Properties window to configure the appropriate level of SSL/TLS deployment. The three possible levels are: Disable TLS, Allow TLS, and Require TLS.
- Use the MailSite Security Properties window to "Enable alternate SSL port” usage for POP and IMAP. Check the "Enable" checkbox in both the POP3 and IMAP4 areas of the Security Properties window and specify the port to be used in each of the adjacent text boxes.
- Start or restart the MailSite services.



SMTP Protocol

When receiving SMTP connections: Disable TLS

When sending mail using SMTP: Disable TLS

POP3 Protocol

When receiving POP3 connections: Disable TLS

□ Disable Plain Text Logins

□ Enable alternate SSL port 995

IMAP4 Protocol

When receiving IMAP4 connections: Disable TLS

□ Disable Plain Text Logins

□ Enable alternate SSL port 993

Certificate Requirements

The certificate must meet several requirements before the MailSite server is able to use it to secure email connections.

- The *Intended Purposes* of the certificate must include Server Authentication. Certificates purchased from trusted certificate authorities or issued by a domain certificate authority using the Web Server template will include this intended purpose.
- The *Common Name (CN)* of the certificate must match the hostname of the Reverse DNS (PTR) record for the IP addresses that the MailSite services are listening on or the Windows HOSTS file must be updated to override the PTR record returned by your DNS servers. MailSite does a reverse DNS lookup to find out the Common Name of the certificate to use before searching the certificate store for an appropriate certificate.

  Example: The network adapters in your mail server are assigned the IP addresses 192.168.1.10 and 192.168.1.11 and your DNS servers report that the reverse DNS entries for 192.168.1.10 and 192.168.1.11 are both mail.yourcorp.com. MailSite will look for a certificate with a common name of mail.yourcorp.com in the certificate store.

If MailSite is unable to locate an appropriate certificate it will log the following error indicating the name of the Common Name of the certificate that it attempted to locate:

```
TLS/SSL: The service failed to find a suitable certificate in the
predefined MY System store for the LocalMachine
     : No certificates were found matching the Subject
'smtp.yourcorp.com'.
```

The HOSTS files located in the %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC on your server can be updated to override the reverse DNS entries and point MailSite to the appropriate certificate.

- The certificate must be stored in the Personal folder of the Computer certificate store. This is the same location where web server certificates are stored.
- The MailSite services must have permission to read and use the private key of the certificate in the certificate store. If the MailSite services are running in a secured mode as a user account without administrator privileges then the system administrator must explicitly grant the necessary permissions.

  The WinHTTP Certificate Configuration Tool (WinHTTPCertCfg) is a command-line tool that enables administrators to import certificates and set permissions. It is located in the MailSite installation directory.

  Example: Listing accounts with access to the private key

  The task in this example is to determine which Windows accounts have permission to access the certificate's private key. To do this use the `/l` to request a list of accounts, `/c local_machine\my` to select the Personal folder of the Computer certificate store and `/s mail.mycorp.com` for the certificate with a Common Name of `mail.mycorp.com`.

  ```
  winhttpcertcfg /l /c local_machine\my /s mail.mycorp.com
  ```

  Example: Granting Access to a Private Key from a User Account

  The task in this example is to grant access to a certificate's private key to a user account. To do this, use `/g` to grant access, `/c local_machine\my` to select the Personal folder of the Computer certificate store, `/s mail.mycorp.com` to select the certificate with the common name `mail.mycorp.com` and `/a MYCORP\MailSite-User` to grant access to the MailSite-User account in the MYCORP domain.

  ```
  winhttpcertcfg /g /c local_machine\my /s mail.mycorp.com /a
  MYCORP\MailSite-User
  ```

- Certificates use a variety of cryptographic algorithms. MailSite requires a certificate that specifies the `Microsoft RSA SChannel Cryptographic Provider` and the `SHA-1` hash algorithm. The cryptographic provider and hash algorithm are specified when requesting your certificate from the certificate authority.

Generating a Test Certificate

For testing purposes, create a self-signed X.509 certificate using the `makecert` utility provided with the Core SDK component of the Windows Platform SDK. The certificate must identify the common name of the MailSite server as specified above in the Certificate Requirements and the extended key usage as "server authentication" (OID 1.3.6.1.5.5.7.3.1). For example:

```
makecert -r -pe -n "CN=mail.mycorp.com" -b 01/01/2001 -e 01/01/2099 -eku
1.3.6.1.5.5.7.3.1 -ss my -sr localMachine –a sha1 -sky exchange -sp "Microsoft
RSA SChannel Cryptographic Provider" -sy 12
```

Open the Microsoft management console and add the local computer certificate snap-in. Check that the certificate has been created in the personal store and copy it to the trusted root certification authority.

Resources

You can obtain the Windows Platform SDK from the following URL:

http://www.microsoft.com/msdownload/platformsdk/sdkupdate/

Be aware that you must download the entire SDK. This utility is free; however, the file size is almost 500 MB. Make sure that your system has adequate disk space and that you have enough time to oversee the operation before you begin downloading the file.

Specific documentation for the `makecert` utility can be found at the following URL:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/makecert.asp

You can obtain the Windows HTTP Services SDK from the following URL:

http://www.microsoft.com/downloads/details.aspx?familyid=c42e27ac-3409-40e9-8667-c748e422833f&displaylang=en

Specific documentation for the `winhttpcertcfg` utility can be found at the following URL:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winhttp/http/winhttpcertcfg_exe__a_certificate_configuration_tool.asp?frame=true

SSL/TLS Settings

All SSL/TLS security settings are available via the TLS tab of the Security Properties window. MailSite allows you to specify the level of TLS deployment separately for each of the three mail protocols— SMTP, POP3, and IMAP4. Each protocol has a separate area within the window. All three protocols use the same drop-down menu settings.

SMTP Protocol

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

- Disable TLS (default) — MailSite communicates in clear text mode.
- Allow TLS — 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.

When the "Allow TLS" setting is selected, you must specify how mail will be sent when using SMTP. The two settings available from that drop-down menu are:

- Use TLS if available — MailSite optionally encrypts messages.
- Require TLS is supported — MailSite forces the client to encrypt messages, but only if the client software supports TLS.

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 (default) — MailSite communicates in clear text mode.

- Allow TLS — 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 — Checking this box forces the client to encrypt login details (when both the server and client have agreed to use SSL/TLS).
- Enable alternate SSL port — Checking this box supports the use of an alternate secure port (this feature is required when the client software supports SSL 3.0 but not TLS 1.0). The alternate port number must be entered in the adjacent text box.

Mail Filters

MailSite includes support for *mail filters*. Filters are rules for mail handling that allow you to specify that messages should be handled in special ways – for instance, forwarded to a specific email address, saved to the file system, or rejected – based on characteristics of the message. Filters are especially useful for identifying messages that may be dangerous or inappropriate and preventing them from entering your system.

Filter Levels

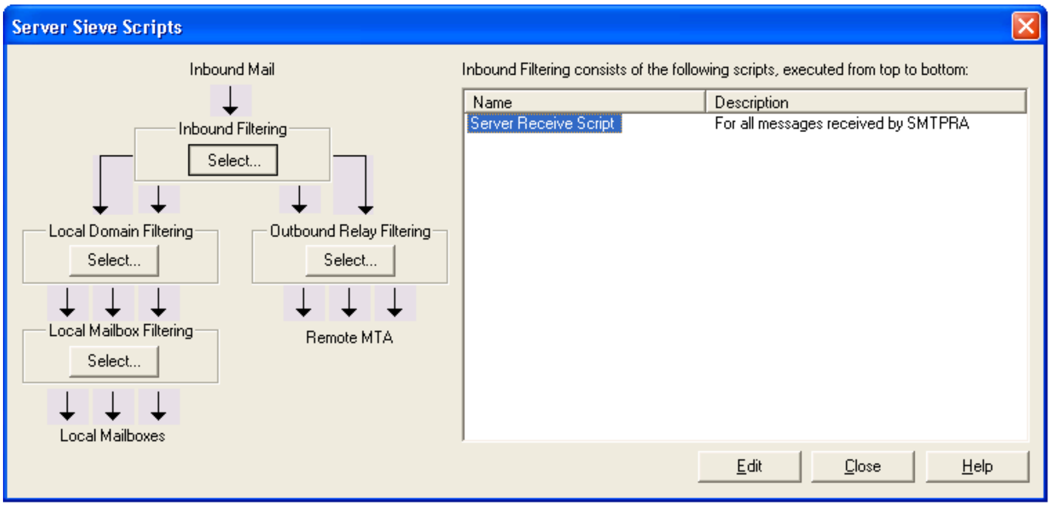
MailSite supports mail content filters at three different levels:

- **Server filters**, which are applied to every message received by MailSite's SMTP server.
- **Domain filters**, which apply only to messages sent to or from a mailbox in a specific domain.
- **Mailbox filters**, which apply only to messages sent to or from a specific mailbox.

For all three types, the user MailSite Console interface described in this section can be used by the administrator to create, modify, and delete filter rules. Mailbox filters can also be defined by end users through the MailSite Express interface.

Using Mail Filters

To use mail filters, open the **Filtering** folder in the MailSite Console and double-click **Sieve Filter**. This displays the Server Sieve Scripts window, which lists the different layers of sieve filtering available in MailSite.



Inbound Filtering consists of the following scripts, executed from top to bottom:

Name	Description
Server Receive Script	For all messages received by SMTPRA

Inbound Filtering

Server Receive Script

This script is executed for all messages received by SMTPRA, and is the first script to act on the message. It is therefore appropriate for actions which are taken at server level such as rejecting mail, or copying suspect content to the postmaster.

Local Domain Filtering

Domain Script

These scripts are specific to a given domain, and are therefore set at domain level, not server level. They are executed after the **Server Receive Script**, but before any of the mailbox scripts. Typically, domain scripts are appropriate for hosting environments. Certain domains may have a requirement to be very strict on suspected spam, and this can be addressed with a domain script.

Local Mailbox Filtering

Forced Mailbox Delivery Script

This is a script which is defined at server level, but which is executed during delivery to a mailbox. This makes it possible to deliver to the “Junk Mail” folder, or take other actions which require knowledge of the target mailbox and its folders. This is the first of the mailbox scripts, and so is the ideal place for rules which it would be problematic if overridden by the mailbox owner’s own rules. Commonly the Forced Mailbox Delivery Script is used to take action on spam, viruses, and other content that should not be allowed into the Inbox.

Mailbox Script

These scripts are specific to a given mailbox, and are therefore set at mailbox level. They are executed after the **Forced Mailbox Delivery Script**, but before the **Mailbox Delivery Script**. Mailbox Scripts are often edited by the end-user via MailSite Express.

`Mailbox Delivery Script`

This script is defined at server level, but is executed during delivery to a mailbox. It is executed after the Mailbox Script, and so can easily be made redundant by end-user defined rules.

Outbound Relay Filtering

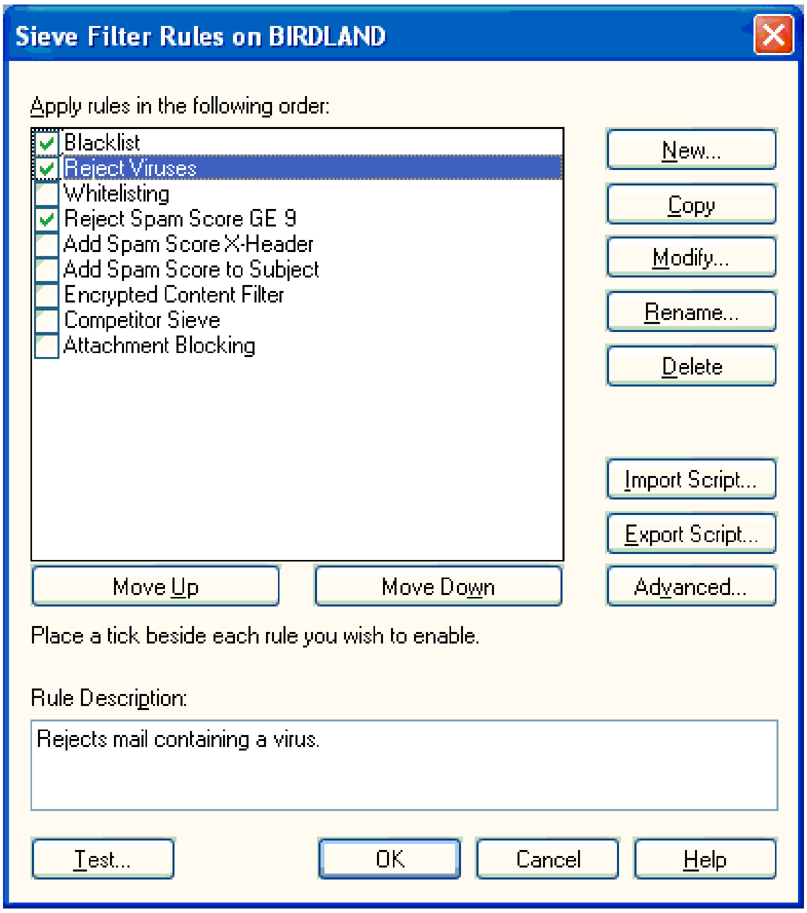
`Server Outbound Script`

These scripts are executed during message relay to a remote server. This makes it possible to block, tag or archive messages generated by (e.g. non delivery reports) or sent through MailSite.

Defining Filters

The four server level defined scripts; **Server Receive Script, Forced Mailbox Delivery Script**, **Mailbox Delivery Script** and **Server Outbound Script,** can be defined by selecting the appropriate filtering level, highlighting the required script and clicking Edit.

This brings up the **Sieve Filter Rules** window, which lists the sever-level content filters currently defined in the selected script. An identical window for managing domain filters can be accessed by clicking the **Sieve Filter** icon within the domain's folder in the MailSite Console. At mailbox level, sieve scripts can be found under **Mailbox Properties** on the **Delivery Actions** tab.



Sieve Filter Rules on BIRDLAND

Apply rules in the following order:

- ☑ Blacklist
- ☑ Reject Viruses
- ☐ Whitelisting
- ☑ Reject Spam Score GE 9
- ☐ Add Spam Score X-Header
- ☐ Add Spam Score to Subject
- ☐ Encrypted Content Filter
- ☐ Competitor Sieve
- ☐ Attachment Blocking

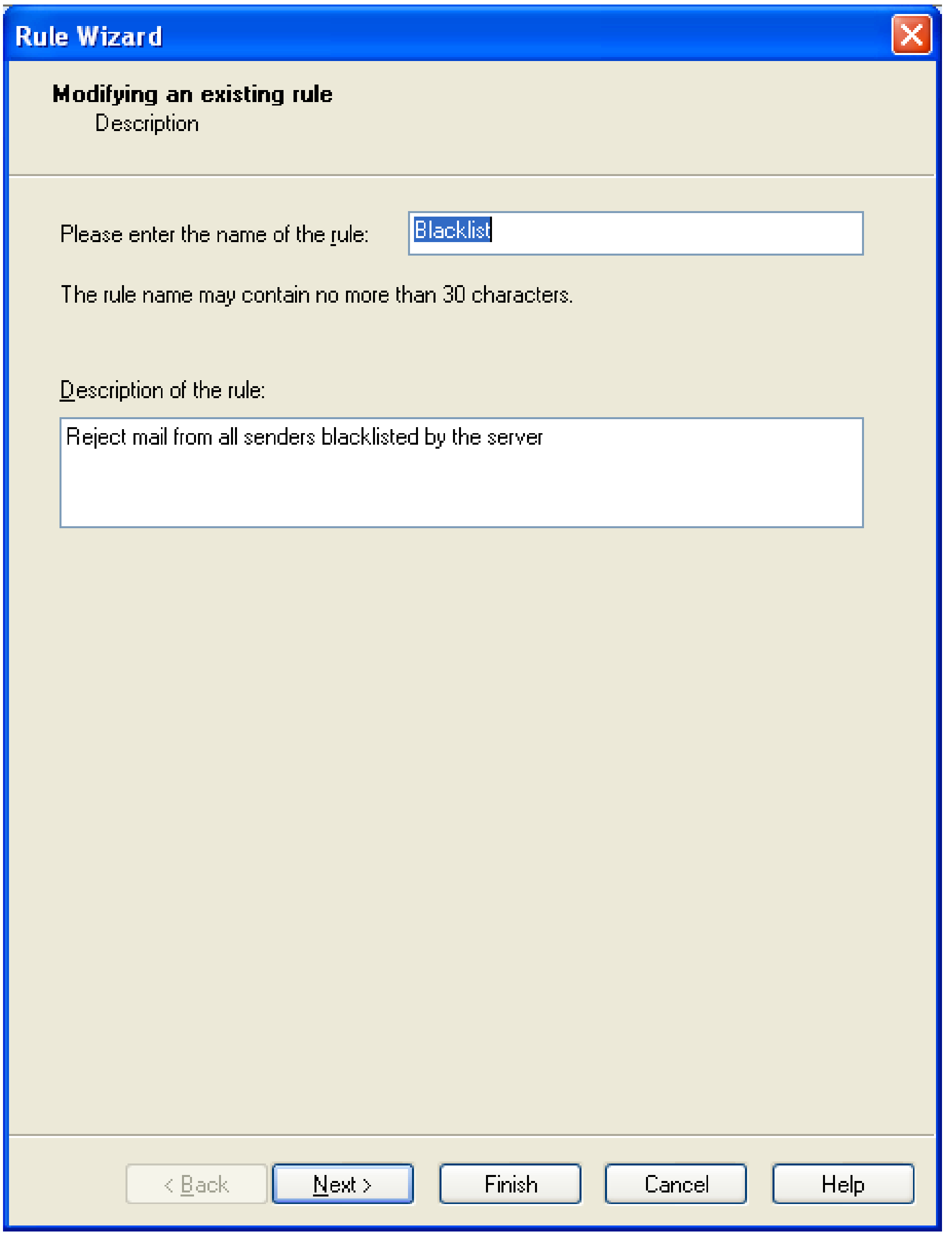
Place a tick beside each rule you wish to enable.

Rule Description: Rejects mail containing a virus.

The rules defined in this list are applied sequentially, so if a message is rejected by an initial filter it will not be subject to subsequent rules. You can move filters up and down in this list to refine your filtering strategies. To create a new filter rule click **New**, which launches the Rule Wizard.

Name and Description

The first panel of the Rule Wizard defines the name and description of your new filter rule. Both the name and description of each filter appears in the Sieve Filter Rules window.



Please enter the name of the rule: Blacklist

The rule name may contain no more than 30 characters.

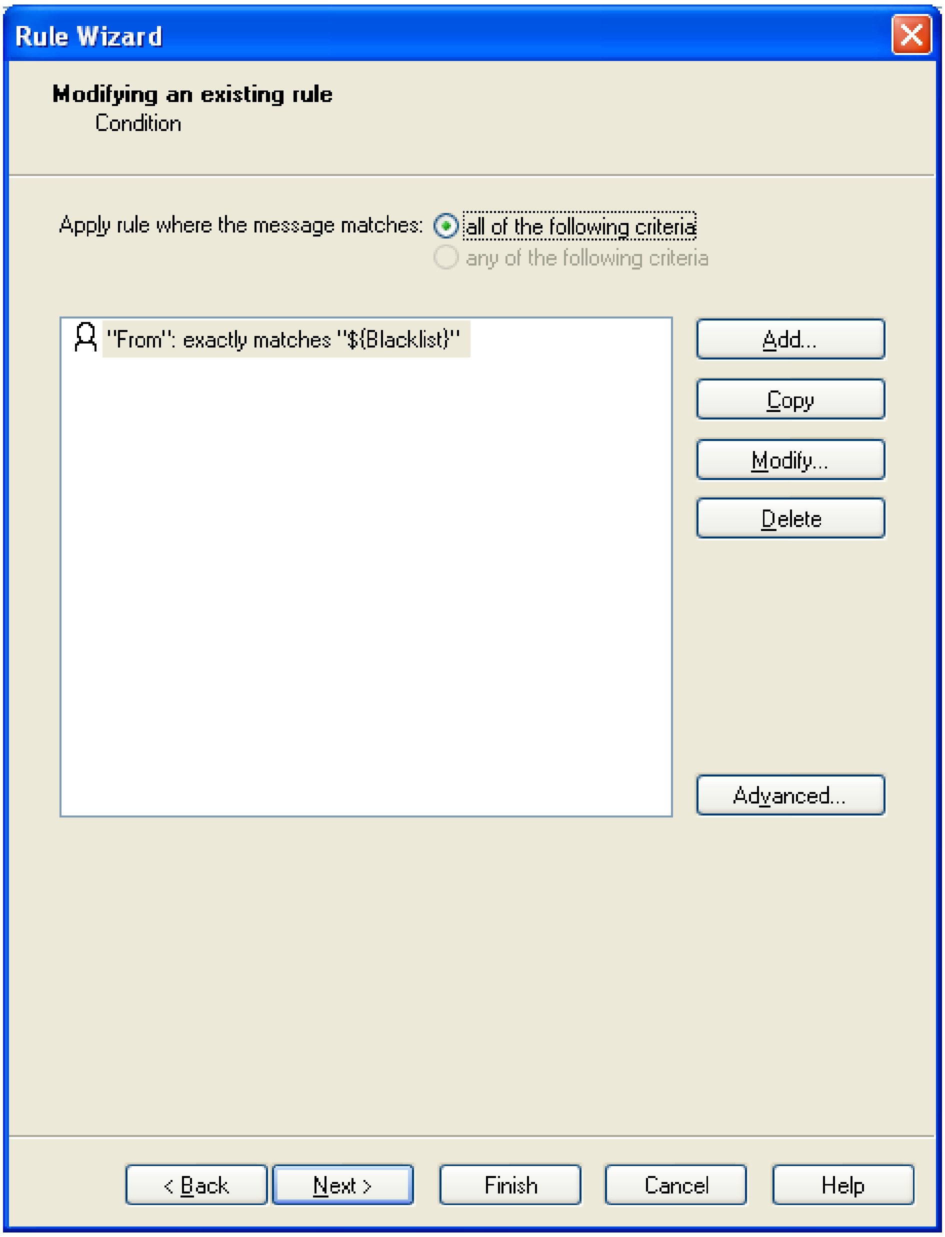
Description of the rule:

Reject mail from all senders blacklisted by the server

Filter names must be unique and can be contain up to 30 characters. When you finish entering your filter rule's name and description, click **Next**.

Adding Filter Criteria

The next panel of the Rule Wizard displays the filtering criteria for your filter rule. These are the conditions that will cause a message to be subject to the filter rule.



Rule Wizard

Modifying an existing rule
Condition

Apply rule where the message matches: ● all of the following criteria
○ any of the following criteria

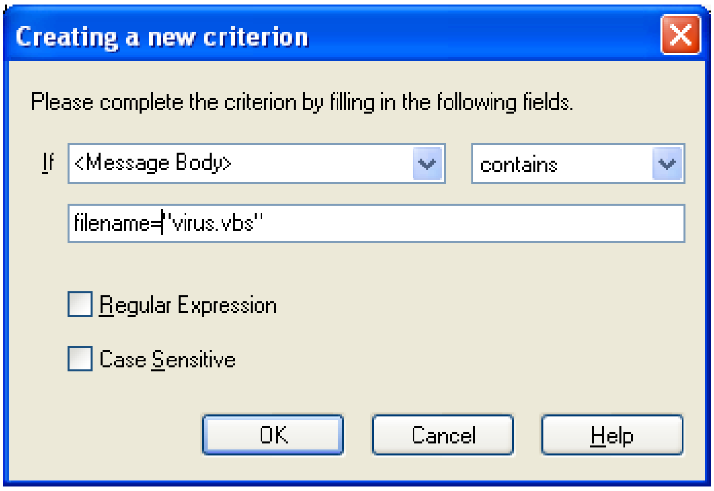
"From": exactly matches "${Blacklist}"

By default, a message must match *all* of the criteria defined in this list to be subject to the filter rule. You can modify this behavior to filter messages that match *any* of the given criteria by selecting the appropriate option at the top of this panel. To add criteria to your filter rule, click **Add**.

To define filter criteria, select the part of the message that you want to search and the text string for which you are searching. You can also use regular expressions to define sophisticated text searches.

When defining filtering criteria, you can search for the given text in either the headers (From, Subject, To, Cc, Bcc, Sender, Reply-To, etc.) or body of the message. You can also test for the existance of a header, as well as for the size of the entire message (including headers, body, and all attachments). To search in a header not given shown in the menu, click in the menu value and enter the header you wish to search. Attachments are considered part of the message body, so when searching for attachment content select **`<Message Body>`**.

For example, to filter messages that contain the attachment **`virus.vbs`**, use the following criteria:



Please complete the criterion by filling in the following fields.

If <Message Body> contains

filename="virus.vbs"

□ Regular Expression

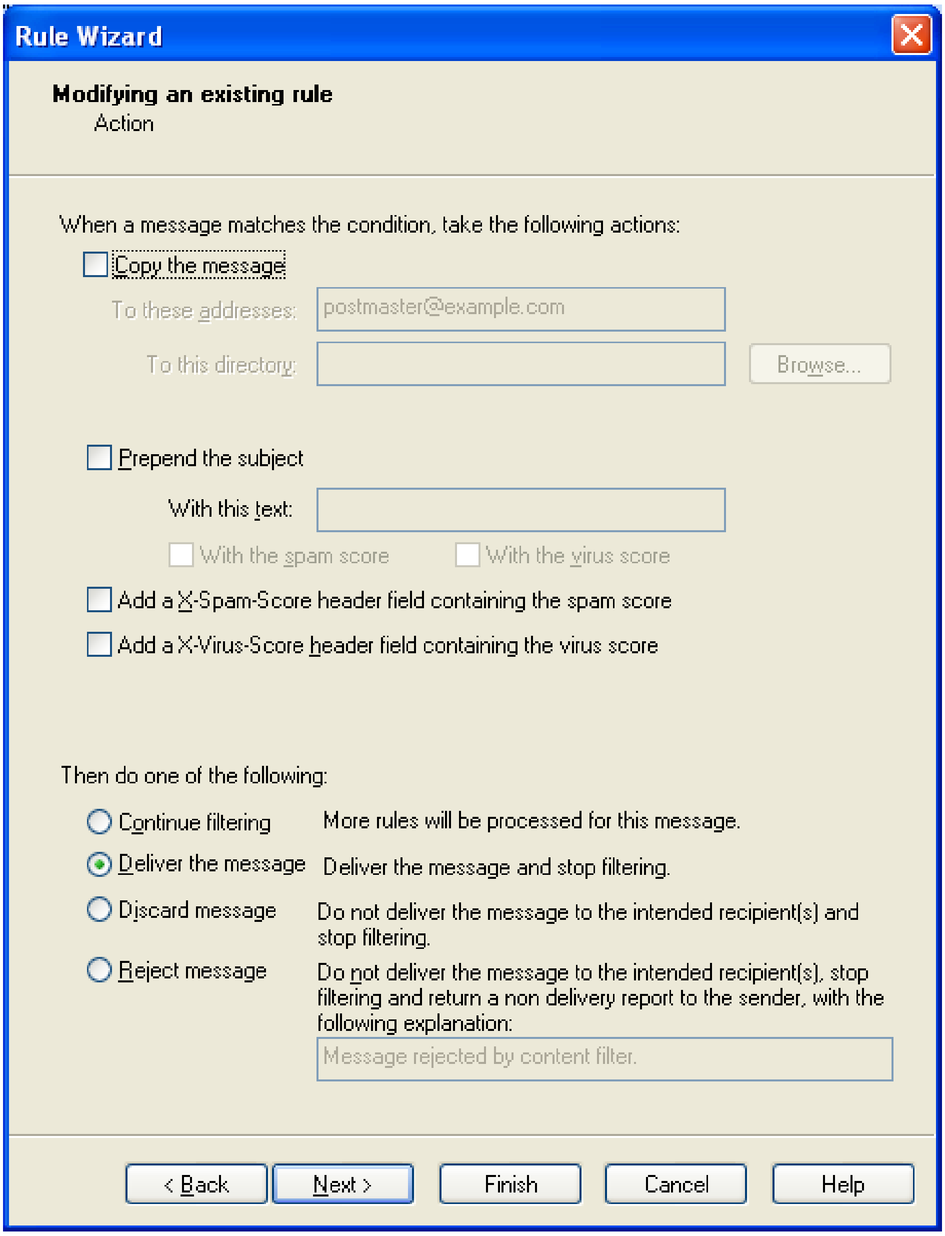
□ Case Sensitive

To specify a regular expression search, enable the **Regular Expression** option. This also enables a **Test** button that allows you to test your regular expression syntax on sample message content. See the following section on Advanced Filter Options for more information.

After you have finished adding criteria for your filter rule, click **Next**.

Set a Filter Action

The next panel of the Rule Wizard defines the action to be taken against messages that satisfy the criteria for the filter rule. In other words, if a message contains the characteristics that you set for this rule, MailSite will handle that message according to the actions you set here.



Rule Wizard

Modifying an existing rule
Action

When a message matches the condition, take the following actions:

□ Copy the message

To these addresses: postmaster@example.com

To this directory:

□ Prepend the subject

With this text:

□ With the spam score □ With the virus score

□ Add a X-Spam-Score header field containing the spam score

□ Add a X-Virus-Score header field containing the virus score

Then do one of the following:

○ Continue filtering — More rules will be processed for this message.

● Deliver the message — Deliver the message and stop filtering.

○ Discard message — Do not deliver the message to the intended recipient(s) and stop filtering.

○ Reject message — Do not deliver the message to the intended recipient(s), stop filtering and return a non delivery report to the sender, with the following explanation:

Message rejected by content filter.

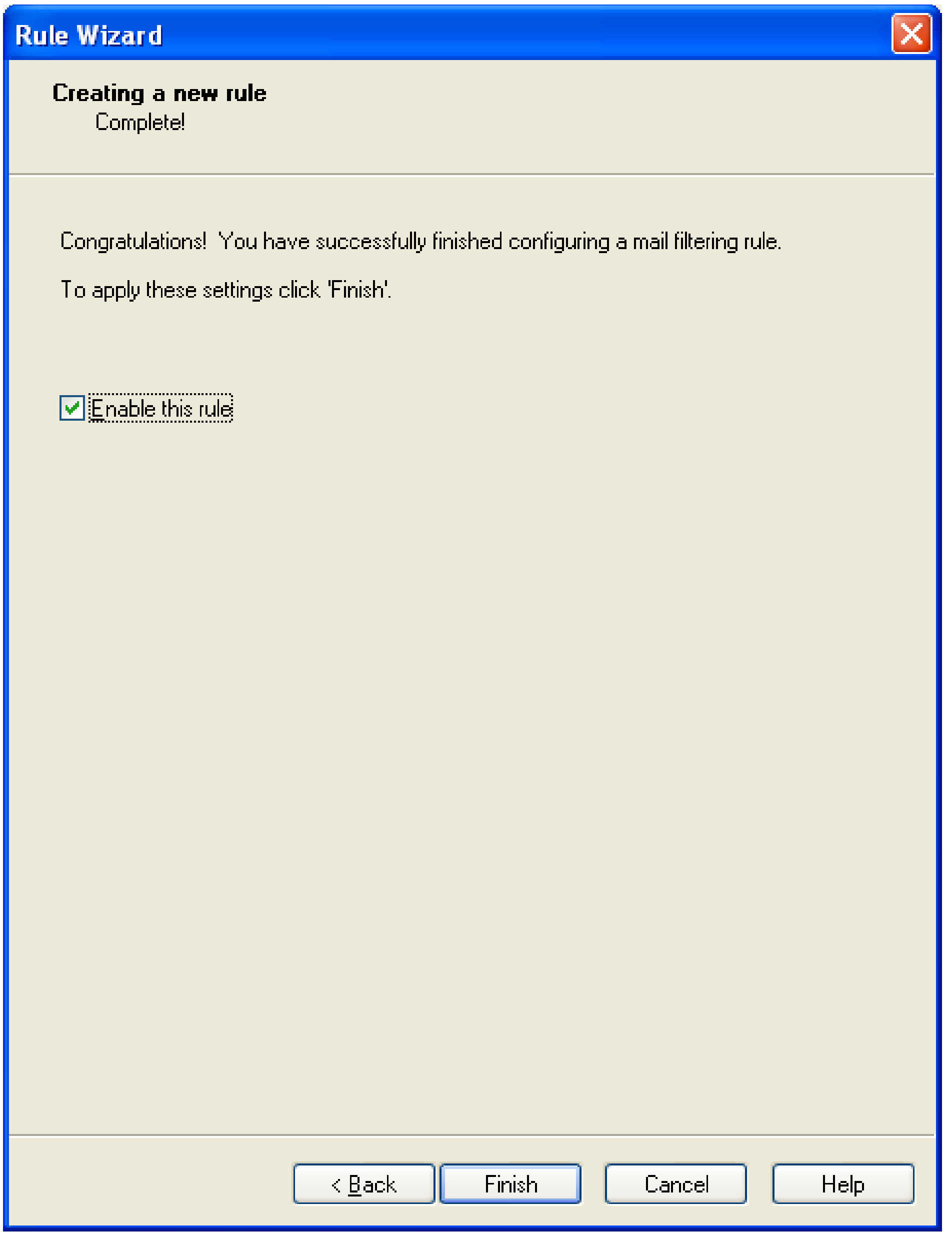
You can specify that messages caught by your filter rule should be rejected, forwarded, saved to a given file system directory, or any combination of the above. If the message is not rejected, you can also choose whether or not the message should be delivered to its intended recipients.

The choices you should make here are dependent on the type of filter rule you are creating. For example, if your filter rule scans for messages that have virus attachments, you will probably want to reject any such messages; if your filter rule archives urgent messages sent to the postmaster, you should save copies of these messages and also allow normal delivery.

Note that the actions available in this panel change slightly when creating domain or mailbox filters. For domain filters, copying a message to a file is not available. For mailbox filters, a message can only be copied to a folder within the recipient's mailbox folder.

Rule Wizard Finish

The final panel of the Rule Wizard allows the option to apply the settings chosen by clicking 'Finish'. Checking **Enable this rule** enables it immediately.



Rule Wizard

Creating a new rule

Complete!

Congratulations! You have successfully finished configuring a mail filtering rule.

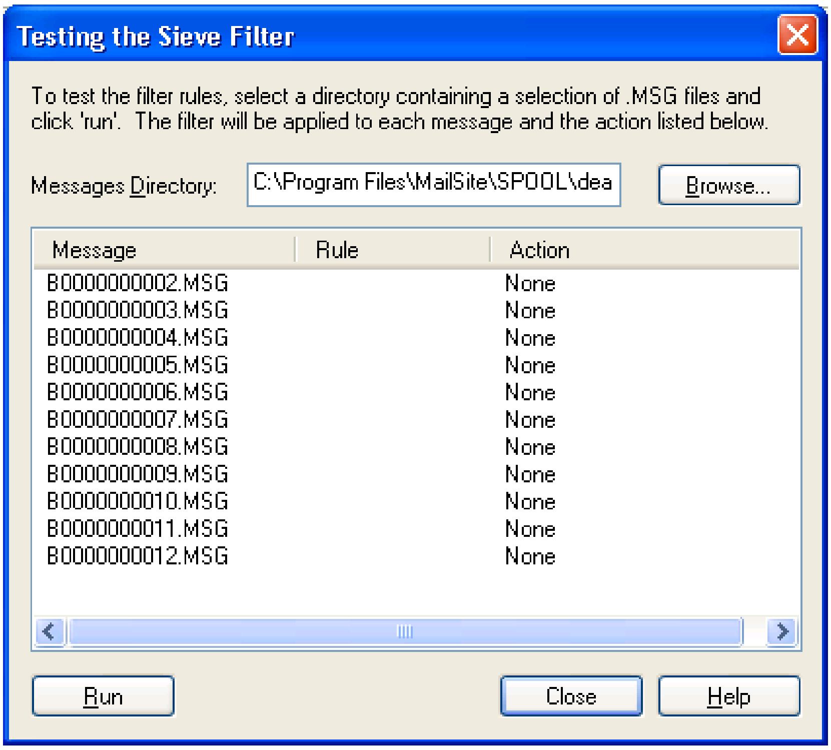
To apply these settings click 'Finish'.

☑ Enable this rule

Testing Filters

After you have created filter rules you can test their behavior on sample messages. Testing filter rules is important to verify the affect that they will have on your site's mail activity, and to confirm that they work as intended.

To test your filter rules, open the **Sieve Filter Rules** window and click **Test**. The following window is displayed:



Testing the Sieve Filter

To test the filter rules, select a directory containing a selection of .MSG files and click 'run'. The filter will be applied to each message and the action listed below.

Messages Directory: C:\Program Files\MailSite\SPOOL\dea

Message	Rule	Action
B0000000002.MSG		None
B0000000003.MSG		None
B0000000004.MSG		None
B0000000005.MSG		None
B0000000006.MSG		None
B0000000007.MSG		None
B0000000008.MSG		None
B0000000009.MSG		None
B0000000010.MSG		None
B0000000011.MSG		None
B0000000012.MSG		None

Filter tests are run against all messages in a specific directory. Use the **Browse** button to select a test message directory, such as an existing mailbox. If you have created filter rules to screen out specific viruses, be sure that your test directory includes messages that include the targeted viruses. You should also test your filters against "normal" messages to insure that the filters do not catch them by mistake.

After you select a message directory, click **Run**. This will cause your filtering rules to be applied to the messages in this directory exactly as if they are incoming messages. If a message is subject to a filter rule, then this window displays the name of the message file, the filter rule that applies to it, and the action(s) taken against the message. The possible actions are **Reject** (message blocked), **Forward** (message forwarded to the given address), **Copy** (copy of the message is saved), **Discard** (message is not delivered to its recipients), and **Stop** (no more filter rules are applied to the message). If a message is shown with no rule or action, then that message would be delivered normally.

The order of entries in the **Filter Rules** window is significant: rules are applied in the order that they appear in this list. This means that if the first filter rejects a message (**Reject**), or specifies that additional filter rules should not be applied to it (**Stop**), then the remaining filter rules are irrelevant for that message. It is therefore important to test your general filtering strategy, not just individual filter rules. Move entries up and down in the rules list to fine-tune mail filtering on your site.

Message Quarantine

MailSite sieve scripts have the ability to file messages into any folder in the recipient's mailbox. When MailSite is installed it will have a default rule named 'Spam Trap' in the **Forced Mailbox Delivery Script** script which files spam messages into a special folder 'Junk Mail'. The rule is by default turned off, but the administrator may choose to enable this rule immediately and modify the trigger level. The intention of this rule is to allow administrators to enable a message quarantine for messages considered to be spam without having to configure the details of the script.

The MailSite message quarantine is bound to the special folder 'Junk Mail'. Messages filed into this folder will remain there until the recipient explicitly deletes the message or until a thirty day quarantine period has passed, after which they will be automatically deleted. You may choose to file these messages into a differently named folder, but the quarantine operation only works with the 'Junk Mail' folder.

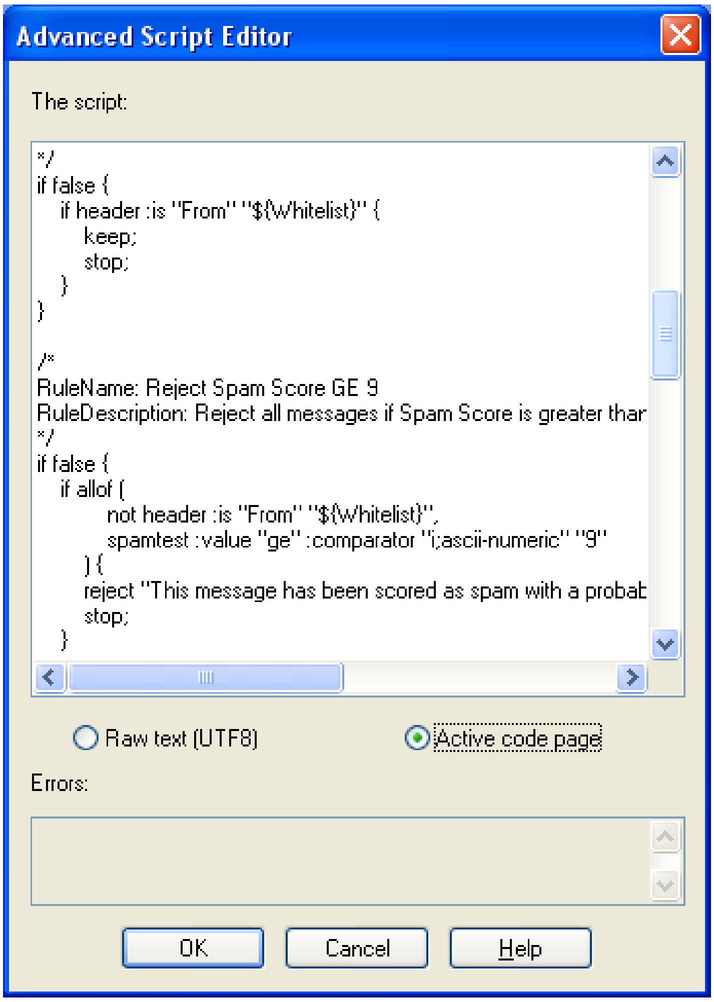
The recipient is able to override actions taken by the **Mailbox Delivery Script** by editing their own mailbox sieve script using the MailSite Express web interface, and so it will usually be more appropriate to act on spam in the **Forced Mailbox Delivery Script**.

Advanced Filter Options

In addition to the standard filter functionality, there are two advanced methods of creating filters in MailSite: by editing the scripts that define filter rules, and by specifying regular expressions, which define sophisticated text searches.

Script Editing

Within MailSite, filter rules are defined by scripts. These scripts are generated automatically when you create filter rules in the MailSite Console, but can be manually edited to refine filter rules. To edit a filter script, click the **Advanced** button on the Condition panel of the Rule Wizard.



The script:

```
*/
if false {
    if header :is "From" "${Whitelist}" {
        keep;
        stop;
    }
}

/*
RuleName: Reject Spam Score GE 9
RuleDescription: Reject all messages if Spam Score is greater thar
*/
if false {
    if allof (
            not header :is "From" "${Whitelist}",
            spamtest :value "ge" :comparator "i;ascii-numeric" "9"
        ) {
        reject "This message has been scored as spam with a probat
        stop;
    }
```

○ Raw text (UTF8) ● Active code page

Errors:

The scripts shown in this dialog consist of one or more clauses, which are statements that are either true or false.

Scripts are always stored in **Raw Text (UTF8)** format, but it is possible to type scripts in the **Active Code Page** of the current MailSite Console session. This means that an administrator can write scripts more naturally using non-US-ASCII symbols such as the British Pound symbol “£”, umlauts “ü” and so on.

MailSite’s script syntax is based on the Sieve filtering language, and includes the following types of clauses:

Header Clause

Header clauses search specific headers (such as “Subject”, “From” and “To”) for a given value. These searches can be for a substring using the **contains** test, or for an exact match using the **is** test. Header clauses are defined in the format:

```
header :contains “HeaderName” “SearchString”
header :is “HeaderName” “SearchString”
```

For example:

```
header :contains “Subject” “I love you”
header :is “From” “postmaster@mailsite.com”
```

Exists Clause

Exist clauses test the existence of a particular header (such as “Subject”, “From” and “To”) in a message. Exists clauses are defined in the format:

```
exists “HeaderName”
```

For example:

```
exists “Reply-To”
```

Body Clause

Body clauses search the body of a message (including attachments) for a given value. Body clauses are defined in the format:

```
x_body :contains “SearchString”
```

For example:

```
x_body :contains “virus.vbs”
```

Size Clause

Size clauses test for the total size of a message, and can test for whether is message size is over or under a specific size. The comparison size is defined in bytes, but you can use K, M, and G to denote kilobytes, megabytes, and gigabytes (respectively). Size clauses are defined in the format:

```
size :over Bytes
size :under Bytes
```

For example:

```
size :under 5000
size :over 300K
```

Allof Clause

Allof clauses consist of two or more individual clauses, and are true if (and only if) all of the enclosed clauses are true. Allof clauses are defined in the format:

```
allof (Clause, Clause, ...)
```

For example:

```
allof (
   exists: “From”,
   header :contains “Subject” “URGENT”
   size :under 100K
)
```

This clause is true for a message if it contains a “From” header and also includes the word URGENT in the “Subject” header.

Anyof Clause

Anyof clauses consist of two or more individual clauses, and are true if any of the enclosed clauses is true. Anyof clauses are defined in the format:

```
anyof (Clause, Clause, ...)
```

For example:

```
anyof (
   exists “To”,
   exists “Cc”,
   exists “Bcc”
)
```

This clause is true for a message if it contains a “To” header, a “Cc” header, or a “Bcc” header; in any of these cases, the entire clause is true.

Not Clause

Not clauses contain a single clause, and are true if (and only if) the enclosed clause is false. Not clauses are defined in the format:

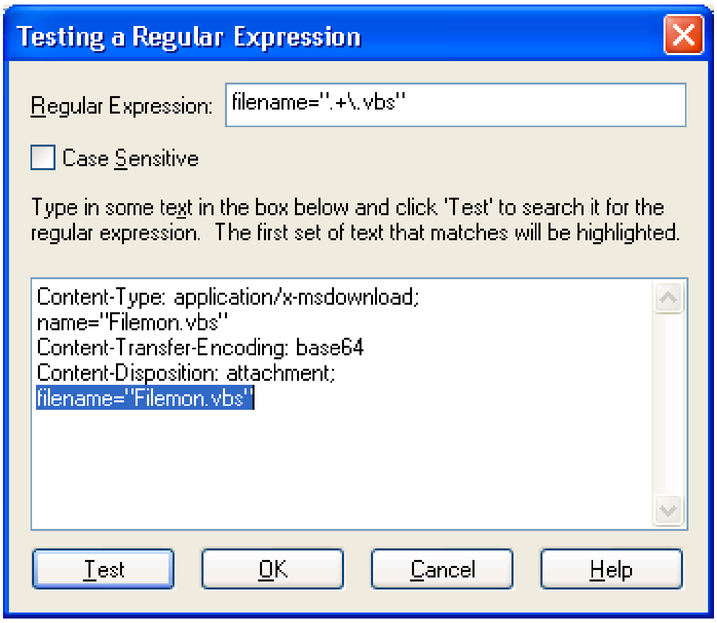
```
        not Clause
```

For example:

```
        not header :contains “From” “postmaster”
```

Regular Expressions

For each type of clause, you can use regular expressions instead of simple text strings as your search criteria. To use a regular expression as your search criteria, enable the **Regular Expression** option on the filter rule criteria dialog. This also enables the **Test** button, which allows you to test your expression syntax.



Regular Expression: filename=".+\.vbs"

□ Case Sensitive

Type in some text in the box below and click 'Test' to search it for the regular expression. The first set of text that matches will be highlighted.

```
Content-Type: application/x-msdownload;
name="Filemon.vbs"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="Filemon.vbs"
```

When testing your regular expression, enter sample message text in the field provided. This allows you to run simulations of the mail filter on the type of content you are looking for. When you click **Test**, the sample text will be searched for text that matches your search criteria.

The following table provides syntax rules for regular expressions:

Expression	Syntax	Description
Any Character	.	Matches any one character.
Zero or More	*	Matches zero or more occurrences of the preceding expression.
One or More	+	Matches at least one occurrence of the preceding expression.
Zero or One	?	Matches zero or one occurrence of the preceding expression.
Set of Characters	[]	Matches any one of the characters within the []. To specify a range of characters, list the starting and ending character separated by a dash (-), as in [a-z].
Character Not in Set	[^]	Matches any character not in the set of characters following the ^.
Grouping	()	Groups a sub-expression.
Or	|	Matches the expression before or after the |. Mostly used within a group. For example, "(sponge)|(mud) bath" matches "sponge bath" and "mud bath."
Beginning of Line	^	Starts the match at the beginning of a line. Significant only at the start of an expression.

Expression	**Syntax**	**Description**
End of Line	$	Anchors the match to the end of a line. Significant only at the end of an expression.
Tagged Expression	{}	Tags the text matched by the enclosed expression, You can match another occurrence of the tagged text using **\N** and +. Useful to repeated expressions such as repeated characters.
Nth Tagged Text	\N	Matches the text matched by the Nth tagged expression, where N is a number from 1 to 9. For example <{.}\1+> would match any repeated character surrounded by angle brackets.
Escape	\	Matches the character following the backslash (\). This allows you to find characters used in the regular expression notation, such as { and ^.
Prevent Match	~X	Prevents a match when X appears at this point in the expression. For example, "rea~(ity)" matches the "real" in "realty" and "really," but not the "real" in "reality."
Repeat N Times	^N	Matches N occurrences of the preceding expression. For example, "[0-9]^4" matches any 4-digit sequence.
Whitespace	\s	Matches space, tab, newline, etc
A word boundary	\b	Matches the end or start of a word
Alphanumeric Character	\a	Matches the expression ([a-zA-Z0-9]).
Alphabetic Character	\c	Matches the expression ([a-zA-Z]).
Decimal Digit	\d	Matches the expression ([0-9]).
Quoted String	\q	Matches the expression (("[~"].*")|('[~'].*')).
Alphabetic String	\w	Matches the expression ([a-zA-Z]+).
Decimal Integer	\z	Matches the expression ([0-9]+).
Tab Character	\t	Matches a tab character

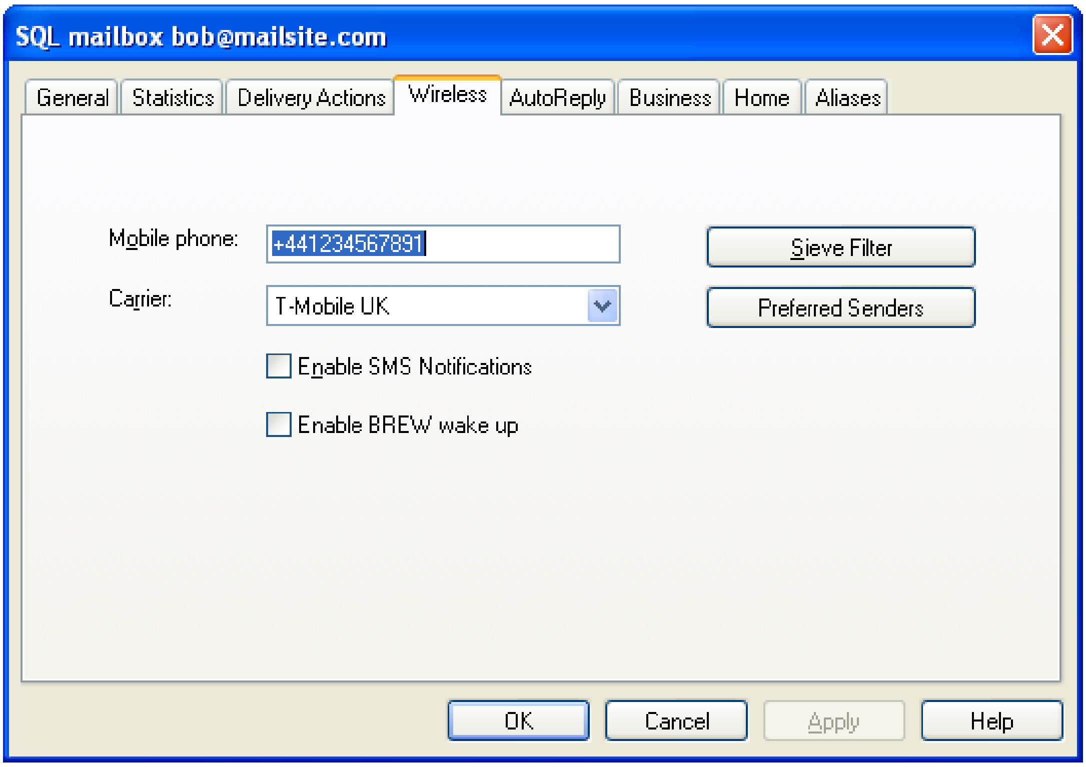
Wireless Email Integration

MailSite includes push email functionality that enables subscribers to receive notification of important messages via SMS to a cellphone. Push email is integrated with MailSite's powerful sieve filter implementation meaning that the subscriber can determine which messages are to be forwarded to their cellphone. Support for the major cellular carriers using their SMTP to SMS gateway is included as standard.

Wireless Configuration

MailSite's wireless push functionality is part of the sieve filter implementation. Notification will usually be managed by the end-user in MailSite Express. There is a **Wireless** page which groups together everything needed to tailor notifications for each user.

Administrators can review and manage wireless notification from the MailSite Console. To edit the wireless settings, bring up the **Mailbox Properties** dialog, and select the **Wireless** tab.



SQL mailbox bob@mailsite.com

Mobile phone: +441234567891

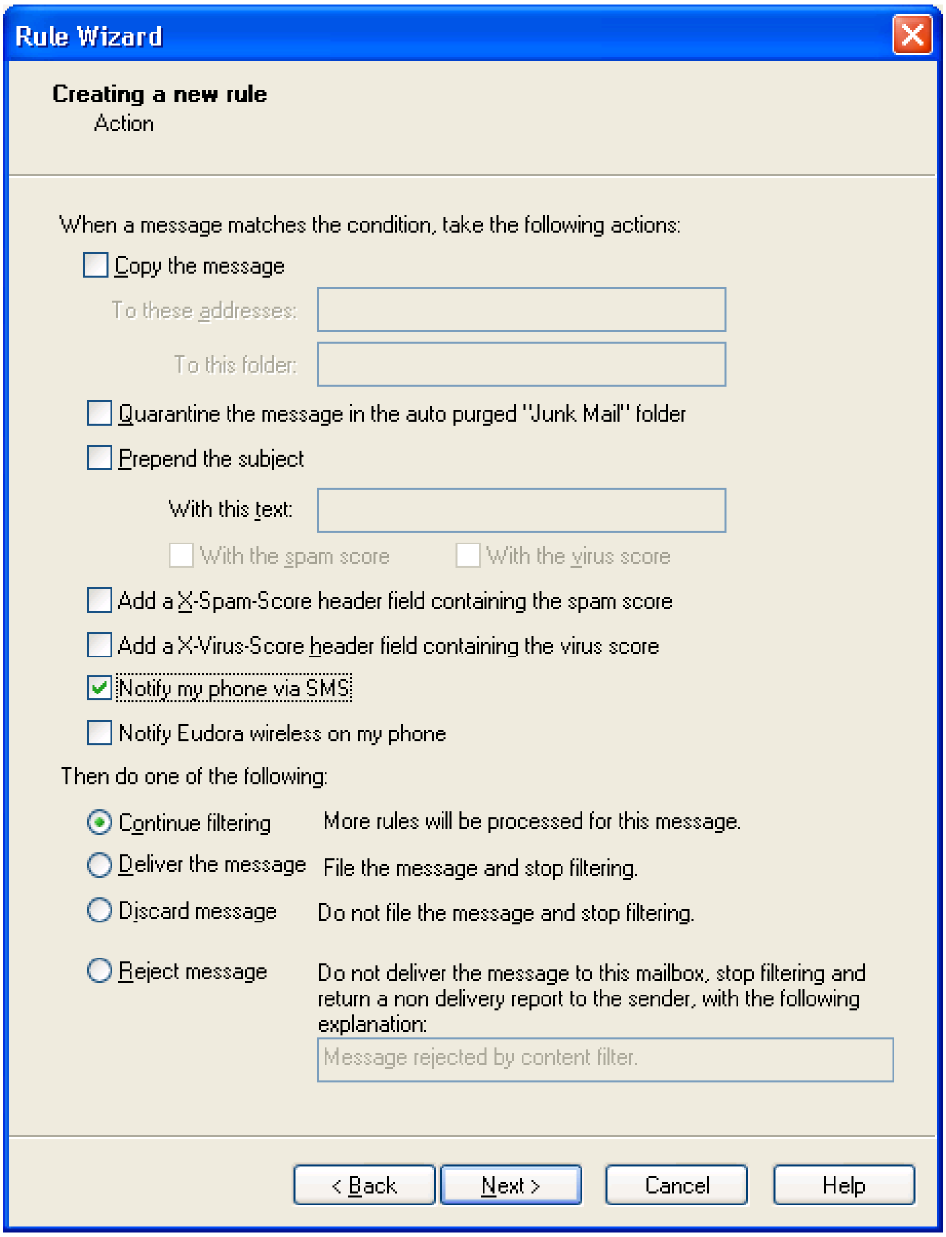
Carrier: T-Mobile UK

□ Enable SMS Notifications

□ Enable BREW wake up

The mobile or cellular phone number and cellular carrier for this mailbox can be modified as needed. The list of carriers can be altered by the administrator at server level. SMTP to SMS gateways provided by the cellular carriers require the cellular numbers and so it is important that both fields are correctly set. Check the "Enable SMS Notifications" checkbox to enable wireless push functionality for this mailbox. A warning will appear explaining that an appropriate sieve filter is needed before SMS notification will work.

Wireless notification is controlled by MailSite's powerful sieve implementation. The SMS notification sieve rules are created and modified by the end-user, although they can be added or administered through the MailSite Console. Click the "Sieve Filter" button, to create a rule tailored to the notification requirements of this mailbox. See the section on Mail Filters for more information about the options available in the Rule Wizard. The part specific to SMS notifications is the checkbox "Notify my phone via SMS" on the "Action" page as shown below.



Creating a new rule

Action

When a message matches the condition, take the following actions:

□ Copy the message

To these addresses:

To this folder:

□ Quarantine the message in the auto purged "Junk Mail" folder

□ Prepend the subject

With this text:

□ With the spam score □ With the virus score

□ Add a X-Spam-Score header field containing the spam score

□ Add a X-Virus-Score header field containing the virus score

☑ Notify my phone via SMS

□ Notify Eudora wireless on my phone

Then do one of the following:

● Continue filtering — More rules will be processed for this message.

○ Deliver the message — File the message and stop filtering.

○ Discard message — Do not file the message and stop filtering.

○ Reject message — Do not deliver the message to this mailbox, stop filtering and return a non delivery report to the sender, with the following explanation:

Message rejected by content filter.

Virus Scanning

MailSite includes support for integrated *virus scanning*. These features allow MailSite to identify messages that have potentially destructive virus content and block them before they enter your network. When virus scanning is enabled and a message that contains a virus is received by MailSite, it will deal with the message according to the actions in the sieve filter which has caught the message. By default, MailSite will reject the message and inform the sender of the infection.

AVG Anti-Virus Filter

MailSite's virus scanning engine is provided by AVG. This is integrated into MailSite, and so no configuration of the engine is required for use with MailSite.

Virus Scanning Policy

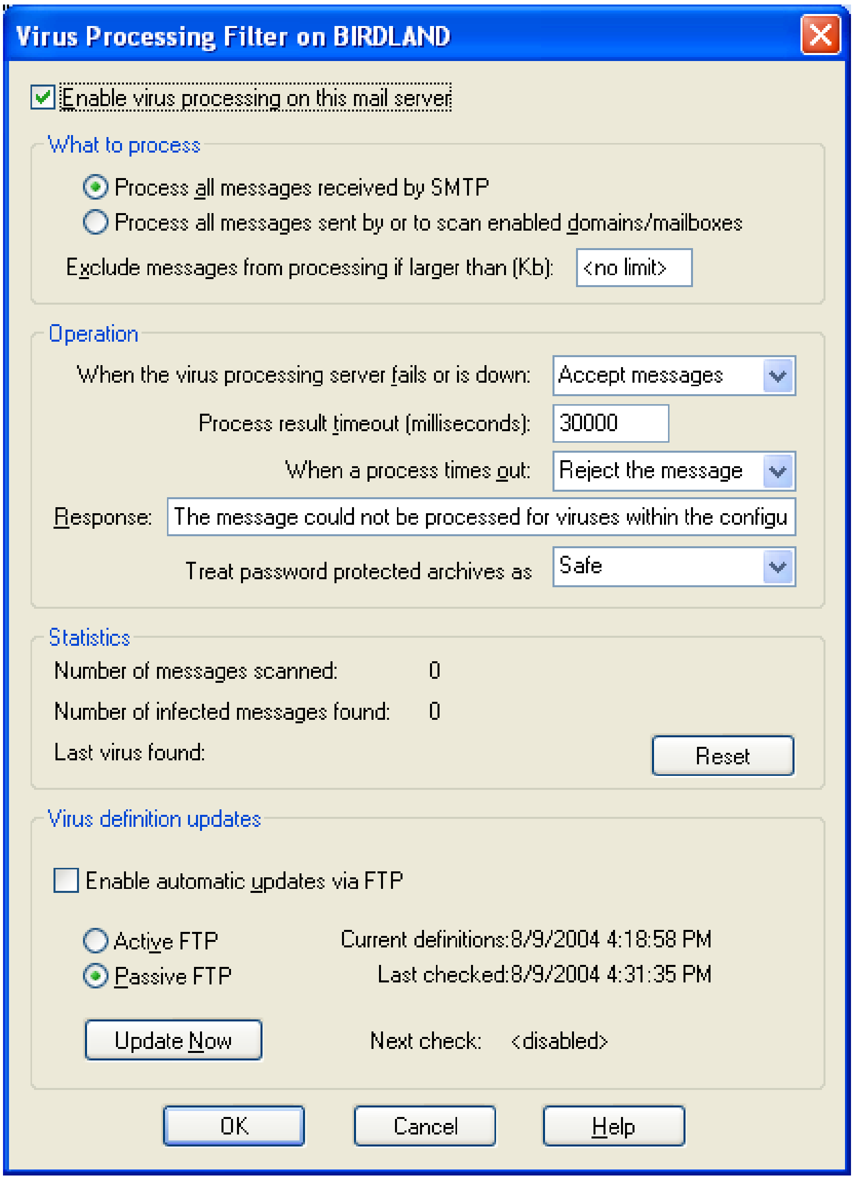
MailSite supports three different virus-scanning policies:

- **Server-level virus scanning**, which causes every message received by MailSite's SMTP server to be scanned for viruses. This policy is typically used by offices, universities, and other organizations.
- **Domain-level virus scanning**, which specifies that messages should be scanned for viruses only if they are sent to or from a mailbox in specific domains. This policy is typically used by mail hosting companies that wish to sell virus scanning as a value-added feature for hosted domains.
- **Mailbox-level virus scanning**, which specifies that messages should be scanned for viruses only if they are sent to or from specific mailboxes. This policy is typically used by ISPs that wish to sell virus scanning as a value-added feature for their subscribers.

Note that the domain and mailbox virus scanning policies can be used together. This means that you can configure virus scanning to occur for all mailboxes in one domain, while scanning only for selected mailboxes in a second domain.

Server Virus Scanning

To configure MailSite's virus scanning policies, open the MailSite Console and double-click the **AVG Anti-Virus Filter** icon in the **Security** folder. This displays the Virus Scanning Filter window:



Virus Processing Filter on BIRDLAND

☑ Enable virus processing on this mail server

What to process

● Process all messages received by SMTP

○ Process all messages sent by or to scan enabled domains/mailboxes

Exclude messages from processing if larger than (Kb): <no limit>

Operation

When the virus processing server fails or is down: Accept messages

Process result timeout (milliseconds): 30000

When a process times out: Reject the message

Response: The message could not be processed for viruses within the configu

Treat password protected archives as Safe

Statistics

Number of messages scanned: 0

Number of infected messages found: 0

Last virus found:

Virus definition updates

□ Enable automatic updates via FTP

○ Active FTP

● Passive FTP

Current definitions:8/9/2004 4:18:58 PM

Last checked:8/9/2004 4:31:35 PM

Next check: <disabled>

The option **Enable virus scanning on this mail server** controls the global virus scanning policy. If this option is disabled, MailSite will not scan any messages. Otherwise, MailSite will scan messages according to the other settings here.

If you want to protect all users on your site from viruses and scan every incoming message, select **Scan all messages received by SMTP**. When this option is selected, all mail received by MailSite's SMTP server will be scanned for viruses regardless of sender or destination.

If you want to instead use domain or mailbox-level virus scanning, select **Scan all messages sent by or to enabled mailboxes/domains**. When this option is selected, MailSite will scan mail based on the virus scanning preferences of the sender or recipient domains on your site.

When the virus scanner fails or is down, MailSite can be configured to defer or accept messages.

The maximum time allowed for a scan is configurable in milliseconds.

When a scan times out, we can accept, reject or defer the message.

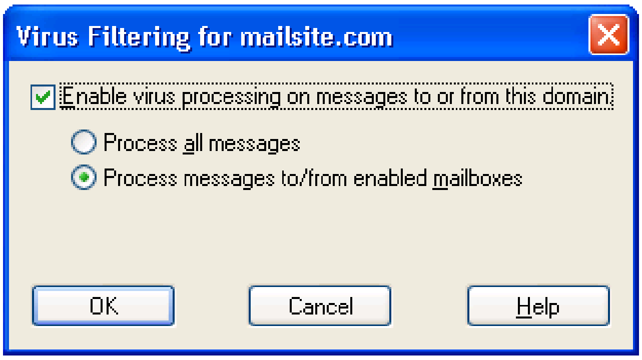
The SMTP server's response when rejecting a message due to a timeout can be set.

Some viruses are transmitted via password protected archives which are encrypted and can not be scanned by MailSite. MailSite can be set to reject messages containing password protected archives by treating them as unsafe or to accept by treating them as safe.

Included in the Virus Scanning Filter window are controls for downloading updated virus definition files, which are needed for MailSite to block new viruses as they are discovered. By default, MailSite polls once an hour for updates to virus definition files. You can force an immediate update by clicking **Update now**. Note that your license may not support virus updates; in this case, MailSite will automatically disable polling for updates.

Domain Virus Scanning

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



Virus Filtering for mailsite.com

☑ Enable virus processing on messages to or from this domain

○ Process all messages

● Process messages to/from enabled mailboxes

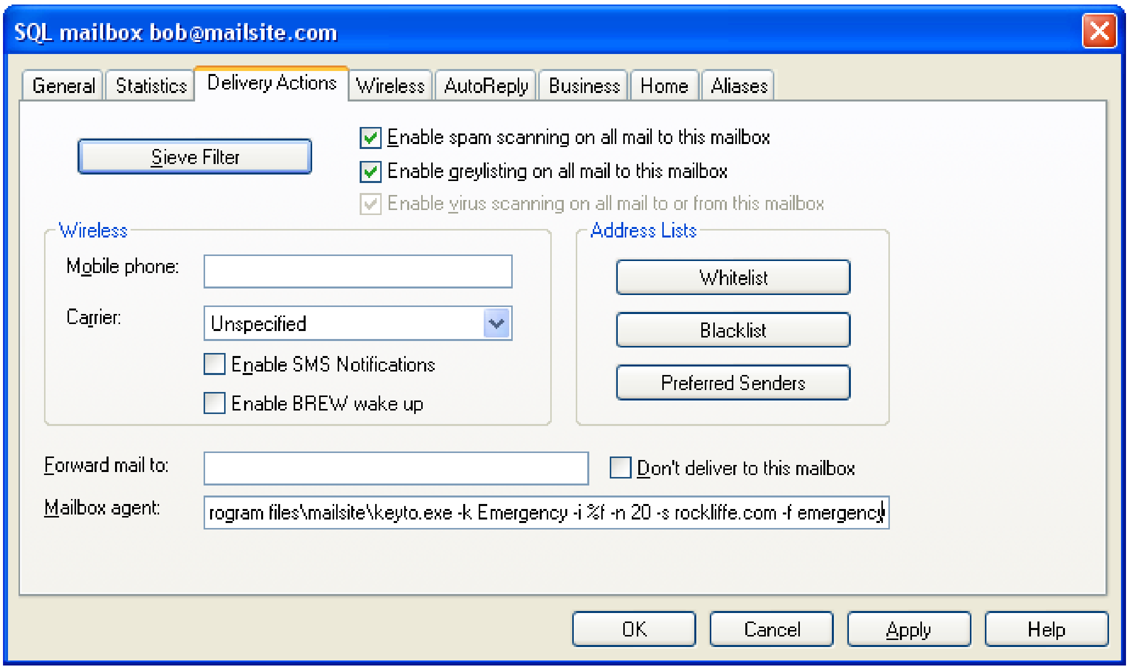
The option **Enable virus scanning on messages to or from this domain** controls the virus scanning policy for this domain. If this option is disabled, MailSite will not scan any messages sent to or from this domain. Otherwise, MailSite will scan messages according to the other settings here.

If you want virus scanning to occur for all users in the domain, select **Scan all messages**. When this option is selected, all mail received by MailSite's SMTP server that is sent to or from a mailbox within this domain will be scanned.

If you want to instead use mailbox-level virus scanning, select **Scan messages sent to/from enabled mailboxes**. When this option is selected, MailSite will scan mail based on the virus scanning preferences of the sender or recipient mailbox.

Mailbox Virus Scanning

To configure mailbox virus scanning, open the mailbox in the MailSite Console and select the Delivery Actions tab:



☑ Enable spam scanning on all mail to this mailbox

☑ Enable greylisting on all mail to this mailbox

☑ Enable virus scanning on all mail to or from this mailbox

Mobile phone:

Carrier: Unspecified

□ Enable SMS Notifications

□ Enable BREW wake up

Forward mail to:

□ Don't deliver to this mailbox

Mailbox agent: rogram files\mailsite\keyto.exe -k Emergency -i %f -n 20 -s rockliffe.com -f emergency

The **Enable virus scanning on all mail to or from this mailbox** controls virus scanning for the individual mailbox. When this option is enabled, messages received by MailSite's SMTP server will be virus scanned if they are sent to or from this mailbox. If disabled, no virus scanning occurs for this mailbox. Note that this field will be disabled if the server or domain virus scanning policies are not configured for mailbox-level scanning.

Spam Scanning

MailSite includes support for integrated *spam scanning*. These features allow MailSite to determine how likely it is that a given message is spam. Customers can then take appropriate action using sieve scripts. Typically, messages likely to be spam are delivered to a “junk mail” folder.

Mailshell Anti-Spam Filter

MailSite’s spam scanning engine is provided by Mailshell. This is integrated into MailSite, and so no configuration of the engine is required for use with MailSite.

Greylisting

MailSite includes greylisting, a technique which can help to reduce spam and server resources. Greylisting works by examining a triplet of information about the message which is being received: sender address; recipient address; remote IP address. If that triplet has not been seen before, the message is “greylisted” meaning that MailSite refuses the mail with a temporary failure code. It is then the responsibility of the sending server to retry delivery later.

Some spam networks will not retry delivery, immediately reducing unwanted mail without CPU intensive scanning. The delay period also helps other anti-spam resources to correctly identify the spammers.

Spam Scanning Policy

MailSite supports three different spam-scanning policies. If spam scanning is enabled, MailSite scans appropriate messages as they arrive, and it is the associated sieve scripts that determine the action taken. Scanning can be enabled at three levels:

- **Server-level spam scanning**, which causes every message received by MailSite’ SMTP server to be scanned for potential spam. This policy is typically used by offices, universities, and other organizations.
- **Domain-level spam scanning**, which specifies that messages should be scanned for spam only if they are sent to or from a mailbox in specific domains. This policy is typically used by mail hosting companies that wish to sell spam scanning as a value-added feature for hosted domains.
- **Mailbox-level spam scanning**, which specifies that messages should be scanned for spam only if they are sent to or from specific mailboxes. This policy is typically used by ISPs that wish to sell spam scanning as a value-added feature for their subscribers.

Note that the domain and mailbox spam scanning policies can be used together. This means that you can configure spam scanning to occur for all mailboxes in one domain, while scanning only for selected mailboxes in a second domain.

Taking Action On Spam with Sieve Filters

While the Mailshell spam-scanning engine provides the power to determine how likely it is that a given message is spam, MailSite’s enhanced Sieve rule implementation provides administrators and end-users alike the power to implement and enforce their own personal spam policy. Actions include: reject, redirect, annotate, quarantine, and deliver.

Spam Quarantine

Rather than immediately discarding or rejecting messages suspected of being spam, MailSite administrators have the option of sending these messages to a special spam quarantine folder which is automatically created for each user and is located in each users mailbox.

End-users can periodically review their spam quarantine folder to identify any false positives, which may be eliminated through a whitelisting process. This “Junk Mail” folder can be reviewed by end-users through MailSite ExpressPro, MailSite Express or any standard IMAP email client.

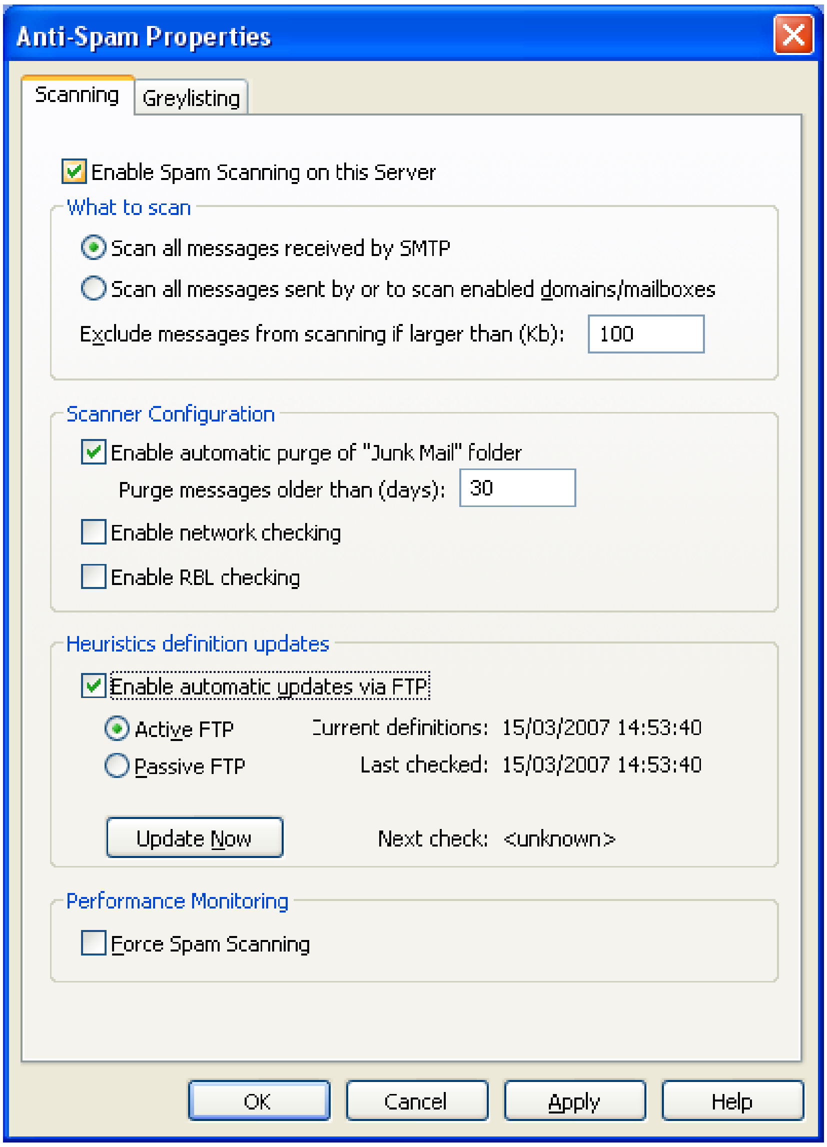
End-users can also implement their own policy for sending messages to the spam quarantine. This special quarantine folder automatically purges messages every 30 days in order to avoid any over-quota concerns.

Personal Whitelisting

A white list is a list of addresses of trusted senders whose messages are delivered unchecked. The white list can be used to recognize mailing list traffic and opt-in marketing messages that might otherwise be classified as spam. With MailSite, end-users can create and manage their own personal white lists, thus relieving the system administrator of this task.

Server Spam Scanning (Scanning Tab)

To configure MailSite’s spam scanning policies, open the MailSite Console and double-click the **Mailshell Anti-Spam Filter** icon in the **Filtering** folder. This displays the Spam Scanning Filter window:



Anti-Spam Properties

☑ Enable Spam Scanning on this Server

What to scan

● Scan all messages received by SMTP

○ Scan all messages sent by or to scan enabled domains/mailboxes

Exclude messages from scanning if larger than (Kb): 100

Scanner Configuration

☑ Enable automatic purge of "Junk Mail" folder

Purge messages older than (days): 30

□ Enable network checking

□ Enable RBL checking

Heuristics definition updates

☑ Enable automatic updates via FTP

● Active FTP   Current definitions: 15/03/2007 14:53:40

○ Passive FTP   Last checked: 15/03/2007 14:53:40

Next check: <unknown>

Performance Monitoring

□ Force Spam Scanning

The option **Enable spam scanning on this mail server** controls the global spam scanning policy. If this option is not selected, MailSite will not scan any messages. Otherwise, MailSite will scan messages according to the other settings here.

Note: *Upon entering this dialog the following test will be performed. If there are more mailboxes provisioned for Anti-Spam then there are licenses for, this option will be unchecked. Upon exiting the dialog another test for this same condition is done. If the licensed amount of mailboxes has been exceeded, then the user will be notified that this option will be turned off.*

If you want to protect all users on your site from spam and scan every incoming message, select **Process all messages received by SMTP**. When this option is selected, all mail received by MailSite's SMTP server will be scanned for spam regardless of sender or destination.

Note: *If there are more mailboxes in the server than there are Anti-Spam licenses for, this option will be disabled.*

If you want to instead use domain or mailbox-level spam scanning, select **Process all messages sent by or to enabled mailboxes/domains**. When this option is selected, MailSite will scan mail based on the spam scanning preferences of the sender or recipient domains on your site.

By default, MailSite will not scan messages of over 100KB for spam. Unsolicited mails are typically very small, but this value can be changed if required.

Included in the Spam Scanning Filter window are controls for downloading updated anti-spam files, which are needed for MailSite to block new forms of spam as they are discovered. By default, MailSite polls once an hour for updates to anti-spam files. You can force an immediate update by clicking **Update now**.

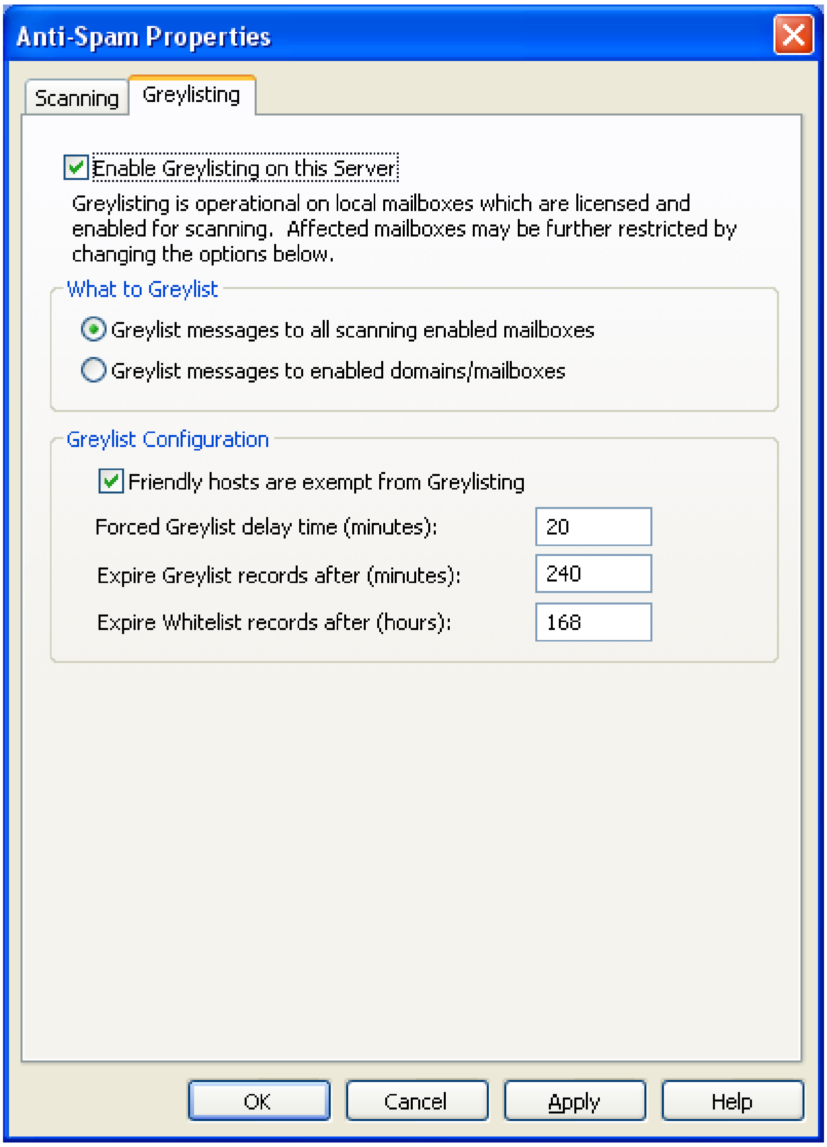
The option **Enable automatic purge of “Junk Mail” folder** determines whether MailSite purges old messages at the end of a POP or IMAP session. The number of days after which a message is considered old is configurable in the text box below.

The options **Enable DNS network checking** and **Enable RBL network checking** control functionality in the Anti-Spam engine. These are provided in addition to the existing MailSite security DNS and RBL features. If these options are selected, spam scoring will be more accurate at the expense of increased network traffic and slower processing.

Spam scanning can be forced on. This allows an administrator to monitor the level of spam passing through the system even if the license does not allow scanning.

Server Spam Scanning (Greylisting Tab)

To configure MailSite’s greylisting policies, open the MailSite Console and double-click the **Mailshell Anti-Spam Filter** icon in the **Filtering** folder, then select the **Greylisting** tab. This displays the Greylisting window:



☑ Enable Greylisting on this Server

Greylisting is operational on local mailboxes which are licensed and enabled for scanning. Affected mailboxes may be further restricted by changing the options below.

What to Greylist

● Greylist messages to all scanning enabled mailboxes

○ Greylist messages to enabled domains/mailboxes

Greylist Configuration

☑ Friendly hosts are exempt from Greylisting

Forced Greylist delay time (minutes): 20

Expire Greylist records after (minutes): 240

Expire Whitelist records after (hours): 168

The option **Enable greylisting on this mail server** controls the global greylisting policy. If this option is not selected, MailSite will use greylisting techniques on any SMTP sessions. Otherwise, MailSite will use this technique according to the other settings here.

Note: *Greylisting is part of MailSite's anti-spam armoury and as such is only an option for mailboxes provisioned for anti-spam. If anti-spam is not provisioned, greylisting will appear as disabled.*

If you want to protect all users on your site from spam and test every incoming message with a new triplet of sender, recipient and remote IP, select **Greylist messages to all scanning enabled mailboxes**. When this option is selected, all mail received by MailSite's SMTP server will be subject to greylist checks.

If you want to instead use domain or mailbox-level greylist provisioning, select **Greylist messages to enabled domains/mailboxes**. When this option is selected, MailSite will use greylist checks based on the greylisting settings of the recipient domains on your site.

The option **Friendly hosts are exempt from Greylisting** indicates whether those hosts in the **Friendly Hosts** list should be exempt from greylisting checks.

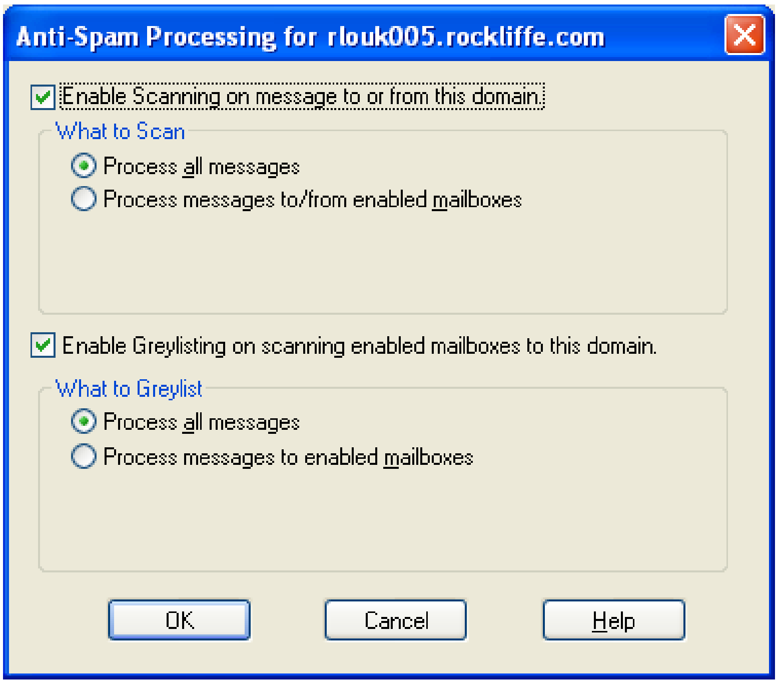
Forced Greylist delay time sets the minimum period after which a greylisted message will be accepted for resubmission. The remote server determines the actual retry interval.

Expire Greylist records after sets the time within which a greylisted message must be resubmitted. Messages which are not resubmitted within this time will be subject to renewed greylisting checks.

Expire Whitelist records after sets the time after which messages will again be greylisted. The longer the period, the less often mail delivery will be delayed.

Domain Spam Scanning

To configure domain spam scanning options, open the domain folder in the MailSite Console double-click the **Mailshell Anti-Spam Filter** icon. This displays the Anti-Spam Processing window:



Anti-Spam Processing for rlouk005.rockliffe.com

☑ Enable Scanning on message to or from this domain.

What to Scan

● Process all messages

○ Process messages to/from enabled mailboxes

☑ Enable Greylisting on scanning enabled mailboxes to this domain.

What to Greylist

● Process all messages

○ Process messages to enabled mailboxes

The option **Enable Anti-Spam scanning on messages to or from this domain** controls the spams scanning policy for this domain. If this option is not selected, MailSite will not scan any messages sent to or from this domain. Otherwise, MailSite will scan messages according to the other settings here.

If you want spam scanning to occur for all users in the domain, select **Process all messages**. When this option is selected, all mail received by MailSite's SMTP server that is sent to or from a mailbox within this domain will be scanned.

Note: *If the number of mailboxes in this domain plus the number of mailboxes provisioned for Anti-Spam in all other domains is greater than the Anti-Spam licensed mailbox count, this option will be disabled.*

If you want to instead use mailbox-level spam scanning, select **Scan messages sent to/from enabled mailboxes**. When this option is selected, MailSite will scan mail based on the spam scanning preferences of the sender or recipient mailbox.

If you are processing Anti-Spam at the server level, then no options on this dialog will be enabled.

The option **Enable Greylisting on scanning enabled mailboxes to this domain** controls the greylisting policy for this domain. If this option is not selected, MailSite will not greylist any messages sent to this domain. Otherwise, MailSite will greylist messages according to the other settings here.

If you want greylisting checks for all users in the domain, select **Process all messages**. When this option is selected, all mail received by MailSite's SMTP server that is sent to a mailbox within this domain will be checked.

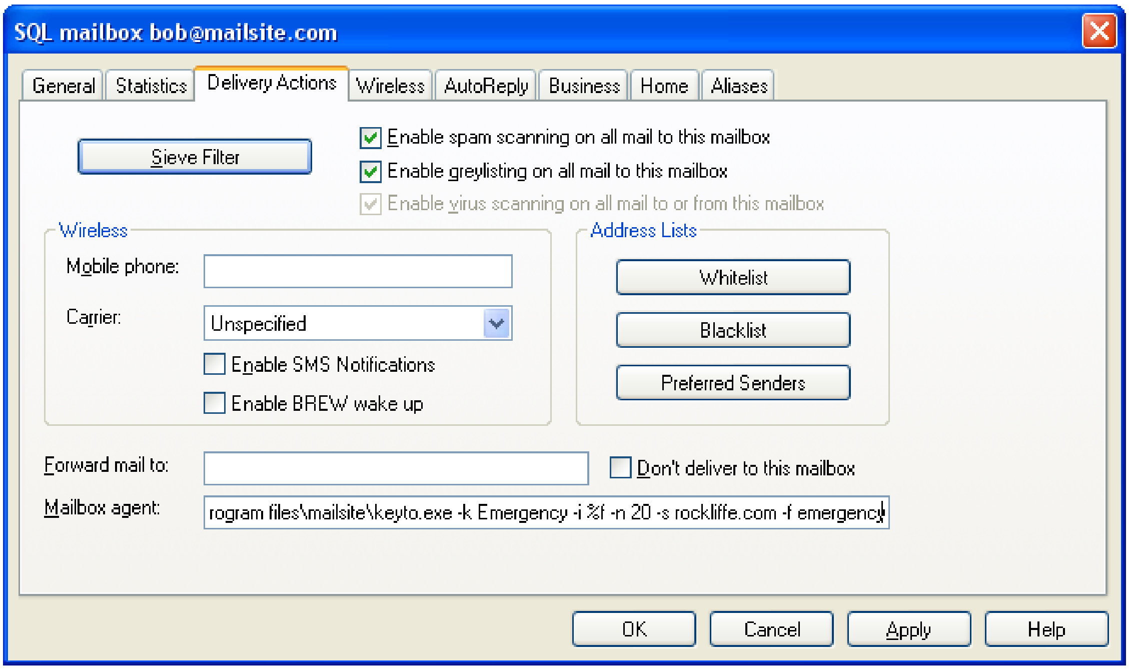
Note: *Greylisting is part of MailSite's anti-spam armoury. If anti-spam processing is not enabled, greylisting will be disabled.*

If you want to instead use mailbox-level greylisting, select **Process messages to enabled mailboxes**. When this option is selected, MailSite will greylist mail based on the setting of the recipient mailbox.

If you are processing greylisting at the server level, then no options on this dialog will be enabled

Mailbox Spam Scanning

To configure mailbox spam scanning, open the mailbox properties in the MailSite Console and select the Delivery Actions tab:



☑ Enable spam scanning on all mail to this mailbox

☑ Enable greylisting on all mail to this mailbox

☑ Enable virus scanning on all mail to or from this mailbox

Mobile phone:

Carrier: Unspecified

☐ Enable SMS Notifications

☐ Enable BREW wake up

Forward mail to:

☐ Don't deliver to this mailbox

Mailbox agent: rogram files\mailsite\keyto.exe -k Emergency -i %f -n 20 -s rockliffe.com -f emergency

The **Enable spam scanning on all mail to or from this mailbox** option controls spam scanning for the individual mailbox. When this option is selected, messages received by MailSite's SMTP server will be spam scanned if they are sent to or from this mailbox. If not selected, no spam scanning occurs for this mailbox.

Note: *This field will be disabled if the server or domain spam scanning policies are not configured for mailbox-level scanning or if by provisioning this mailbox for Anti-Spam, you would exceed the count of licensed mailboxes for Anti-Spam.*

The **Enable greylisting on all mail to this mailbox** option controls greylisting for the individual mailbox. When this option is selected, messages received by MailSite's SMTP server will be greylisted if they are sent to this mailbox. If not selected no spam scanning occurs for this mailbox.

Note: *This field will be disabled if the server or domain greylisting policies are not configured for mailbox-level greylisting or if anti-spam processing is disabled for this mailbox.*

Monitoring Spam Traffic

MailSite provides new Windows performance monitor counters to assist administrators with tracking the flow of spam through the system. These performance monitor counters can be used to display a spam histogram, which indicated the distribution of spam scores for scanned messages across all possible spam score values. This monitoring is particularly helpful for administrators in setting up spam disposition policies.

Spam Score Logging

The likelihood that each message is spam is written to the SMTPRA log:

```
---- SMTPRA log entry made at 05/20/2005 17:55:55

Message B0000111111@example.mailsite.com received spam score of: 8
```

Agents

An *agent* is an external program or command, supplied by you, that manipulates a mail message. MailSite supports the following types of agents:

⇒ The **Server Agent** is executed for every incoming message.

⇒ **Mailbox Agents** are run when a message is delivered to a mailbox.

⇒ **List Agents** are run when a message is delivered to a mail list.

⇒ **List Processor Agents** are run when a message is delivered to a list command address.

⇒ **Archive Agent** is a built-in agent which copies all incoming messages to an archive directory.

An agent must be a command-line program or batch file (not an interactive program requiring keyboard input, nor a Windows program).

Server Agent

Every time MailSite receives a message, it invokes the Server Agent. The agent is told the names of two files: the message file itself, and a file containing SMTP *envelope* information.

The message file has extension **`MSG`**. The file containing the SMTP envelope information is known as the *recipients file***,** although it contains more than just recipient information. When it is passed to the incoming mail agent, it will have extension **`RCO`**; when the agent terminates, MailSite will rename the file to its normal **`RCP`** extension.

Server agents are configured through the Agents dialog in the MailSite Console. Possible uses for Server agents include:

⇒ Checking messages for viruses

⇒ Checking for unsolicited commercial e-mail

⇒ Adding a server wide message footer

⇒ Automatically adding a disclaimer to mail being sent outside the company

⇒ Generating statistics

Mailbox Agents

Each mailbox may be configured with a unique Mailbox Agent. This is an external program that will be executed whenever a message is delivered to a local user's mailbox directory.

The Mailbox Delivery Actions Page includes a **`Mailbox Agent`** field. This field should contain a command-line template that will have various substitutions performed on it before being executed. The substitutions are:

Special Symbol	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**) is placed in the mailbox **INBOX** directory with an **MSF** extension. If no mailbox agent is defined, the **MSF** file extension is renamed immediately to **MSG**. If a mailbox agent is defined, the agent is executed. The mailbox agent may change the message contents or may delete the file. When the agent terminates, the **MSF** file (if it still exists) is renamed to **MSG**.

Multiple commands can be executed by interposing the **&** character between them, or by using a batch file.

The agent is executed by SMTPDA and therefore inherits the NT access rights of SMTPDA. Only when the agent has finished executing will the message be made available to IMAP4A and POP3A.

It is important that the Mailbox agent should not take too long to execute. Otherwise, a busy mailbox could cause the server to run out of memory or saturate its processor.

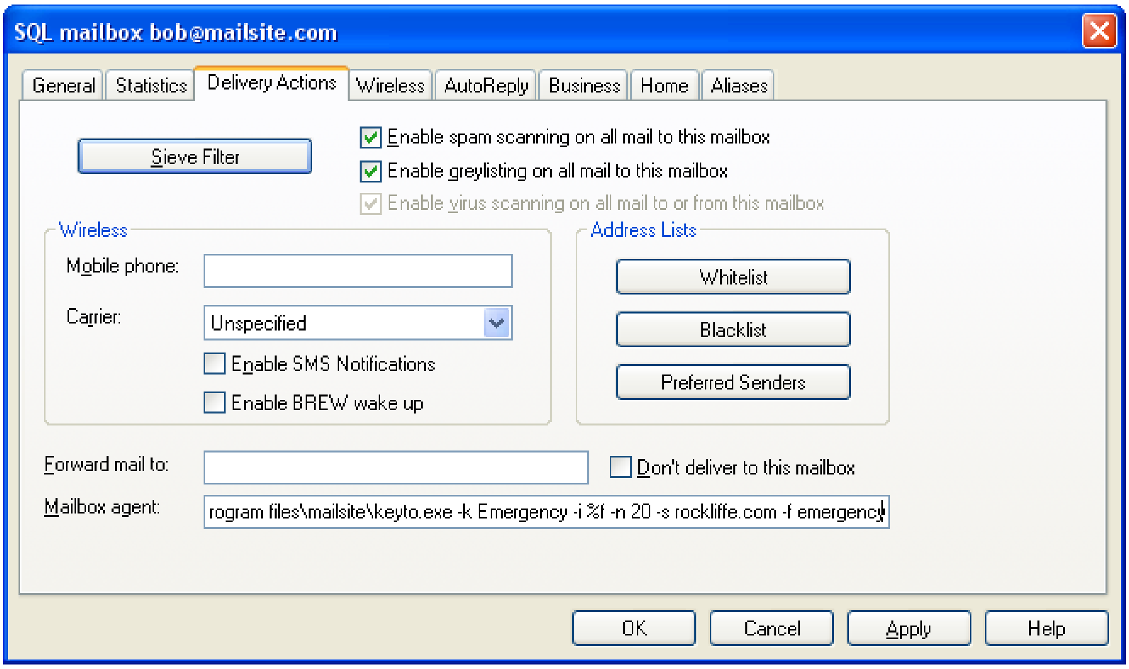
Mailbox Agent Example

This Mailbox agent example uses a tool called **KeyTo**, which searches incoming messages for keywords. If the keyword is present then **KeyTo** sends a short message to a specified address. For example, you may wish to send a message to your pager whenever you receive a message containing the word "emergency".

The **KeyTo** utility is a Windows console program that takes several parameters:

```
-k  Keyword to search for
-i  file to search
-n  Number of lines to search
-s  SMTP relay server
-f  From address
-t  To address
-c  CC address
-u  "Subject"
```

To use this agent with a mailbox, open the mailbox from the MailSite Console. In the Mailbox Delivery Actions, enter the full **KeyTo** execution statement in the **Mailbox agent** field:



SQL mailbox bob@mailsite.com

☑ Enable spam scanning on all mail to this mailbox

☑ Enable greylisting on all mail to this mailbox

☑ Enable virus scanning on all mail to or from this mailbox

Mobile phone:

Carrier: Unspecified

☐ Enable SMS Notifications

☐ Enable BREW wake up

Forward mail to:

☐ Don't deliver to this mailbox

Mailbox agent: rogram files\mailsite\keyto.exe -k Emergency -i %f -n 20 -s rockliffe.com -f emergency

After this information is saved, **KeyTo** will be executed with these parameters on all messages that arrive for this mailbox.

List Agents

Each mail list may be configured with a unique List Agent that pre-processes each message to a mail list before it is delivered by MailSite.

The List General Page includes a **`List Agent`** field. This field should contain a command-line template that has various substitutions performed on it before being executed. These substitutions are listed below:

Special Symbols	Replaced By
`%f`	Full file name of the message which was received
`%m`	Moderator address of the mail list, or **-** if no moderator
`%n`	Name of the mail list
`%d`	Domain to which the mail list belongs
`%%`	Single percent character

The message file (**`%f`**) will be located in the mail list directory, but will not have a **`MSG`** extension. The external program may change the message contents or delete the message file. When the external program completes, MailSite will automatically rename the file (if it still exists) to have a **`MSG`** extension, and will process it as normal.

Multiple commands can be executed by interposing the **&** character between them, or by using a batch file.

The agent is executed by SMTPDA and therefore inherits the NT access rights of SMTPDA. When the agent has finished executing the message will be distributed to list members. Note that the message is queued for content moderation *before* the agent executes.

It is important that the agent should not take too long to execute, since MailSite will not process any other messages for the mail list while the agent is running.

List agents can be used to implement a wide range of features, such as:

⇒ Filter out **`LEAVE`** and **`UNSUBSCRIBE`** messages sent to the main list address

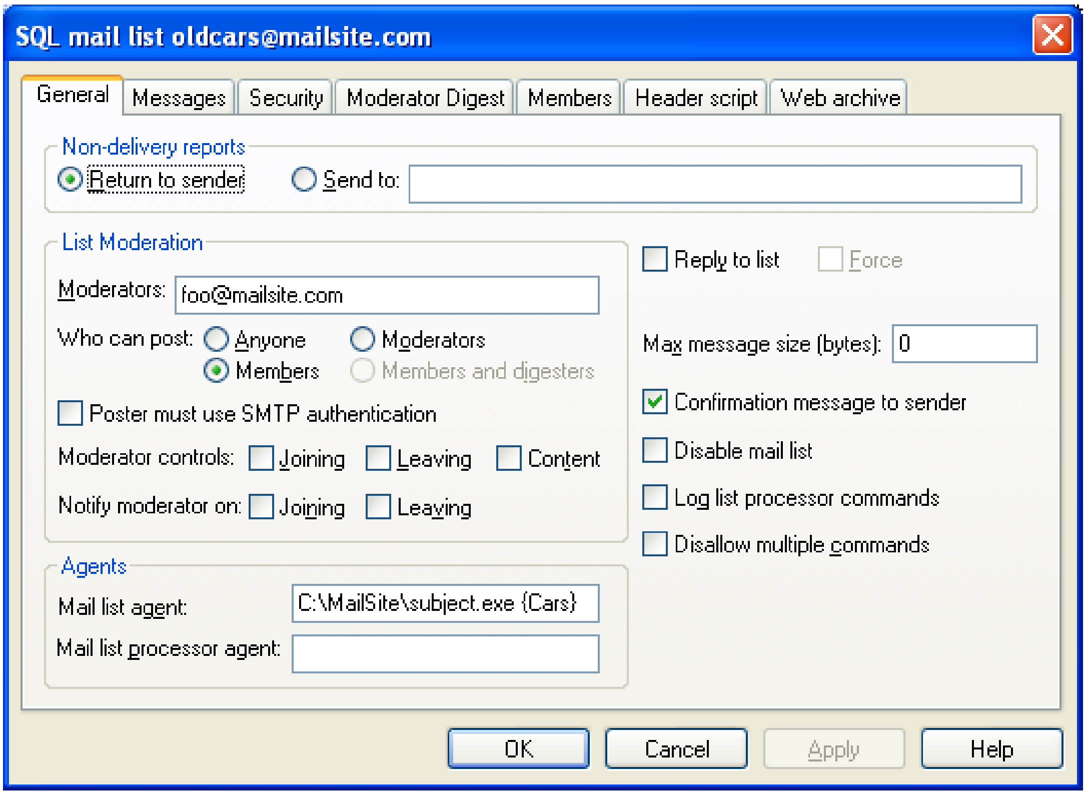
⇒ Check a mail message for offensive language

⇒ Implement additional mail loop prevention techniques

List Agent Example

This List agent example uses a tool called **`SubjectTag`**, which inserts a configurable block of text into the Subject header of each message sent by the list. Setting a subject prefix allows users to filter their incoming list messages from their normal e-mail. For example, if you are running a mailing list related to cars, you might add the subject prefix "[Cars]:" to each list message; in this case, a message sent with the subject "parts for 68 Camaro?" will arrive to list members with the subject "[Cars]: parts for 68 Camaro?".

The **`SubjectTag`** utility is a Windows console program that takes two parameters: the header prefix value, and the name of the message file to modify (**`%f`**). To use this agent with a mail list, open the list from the MailSite Console. In the List General Page, enter the full **`SubjectTag`** execution statement in the **`Mail list agent`** field:



Non-delivery reports
● Return to sender ○ Send to:

List Moderation
Moderators: foo@mailsite.com
Who can post: ○ Anyone ○ Moderators ● Members ○ Members and digesters
□ Poster must use SMTP authentication
Moderator controls: □ Joining □ Leaving □ Content
Notify moderator on: □ Joining □ Leaving

Agents
Mail list agent: C:\MailSite\subject.exe {Cars}
Mail list processor agent:

□ Reply to list □ Force
Max message size (bytes): 0
☑ Confirmation message to sender
□ Disable mail list
□ Log list processor commands
□ Disallow multiple commands

After this information is saved, **`SubjectTag`** will insert this subject prefix on all messages that arrive for this mail list.

List Processor Agents

Each mail list may be configured with a List Processor Agent that pre-processes messages sent to a mail list's **`-request`** address before they are interpreted by MailSite.

The List General Page includes a **`List Processor Agent`** field. This field should contain a command-line template that will have various substitutions performed on it before being executed. These substitutions are:

Special Symbols	Replaced By
`%f`	Full file name of the message which was received
`%m`	Moderator address of the mail list, or **`-`** if no moderator
`%n`	Name of the mail list
`%d`	Domain to which the mail list belongs
`%%`	Single percent character

The message file (**`%f`**) will be located in the mail list directory, but will not have a **`MSG`** extension. The external program may change the message contents or delete the message file. When the external program completes, MailSite will automatically rename the file (if it still exists) to have a **`MSG`** extension, and will process it as normal.

Multiple commands can be executed by interposing the **&** character between them, or by using a batch file.

The agent is executed by SMTPDA and therefore inherits the NT access rights of SMTPDA. When the agent has finished executing then the message will be interpreted by the mail list processor.

It is important that the agent should not take too long to execute, since MailSite will not process any other mail list messages while it is running.

Mail list processor agents can be used to implement a wide range of features, including providing additional mail list processor commands.

Archive Agent

Unlike other agents, the Archive Agent is built in to the mail server. Its purpose is to make a copy of every message received by the mail server. The Archive Agent can help to satisfy the legal requirement to retain all e-mail sent by a company in some jurisdictions.

To enable the Archive Agent, click on the Agents icon in the Window Console's Server folder, which displays the Agents dialog. Enter the archive directory name in the **`Archive directory`** field of this window.

The archive directory will be automatically created if it does not already exist. Under this directory, the agent will create a new subdirectory each day for that day’s messages. The archive subdirectories will have a name of the form **`YYYYMMDD`**, where **`YYYY`** is the year, **`MM`** is the month (01 to 12) and **`DD`** is the day of the month (01 to 31). The agent will copy each **`RCP`** file and **`MSG`** file that is received by MailSite into this directory.

Note that the agent will archive not only messages received by MailSite, but also messages generated by the mail server itself, such as delivery status notifications and messages expanded by the mail list processor.

Databases

MailSite can integrate with a relational database through ODBC (Open Database Connectivity). MailSite can use a database for three things - mailbox authentication; storing mail list membership; and logging. This chapter describes how MailSite can be configured to do this.

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

If your ODBC database is running on a different machine than the MailSite Engine, you may need to take additional setup steps. By default, MailSite services run as the Windows **`SYSTEM`** account, which can access to other machines only via TCP/IP. This means that if your database does not allow connections via TCP/IP, MailSite will not be able to access the database.

To enable database access between systems, you must do one of the following:

- Configure your database to allow TCP/IP connections (refer to your database's documentation for instructions on doing this).
- Change the account that the MailSite services run as from **`SYSTEM`** to an NT account that has access rights to the database. You can do this from the Services Control Panel.

Database Mailbox Plugin

The database mailbox plugin allows you to base authentication on a database. You will find this useful if you have an existing database of users to whom you wish to offer mailbox facilities. Note that you should not attempt to use this plugin unless you are familiar with databases and their terminology.

To configure the database mailbox plugin, select the Plugins Folder in the Console and double click on the Database Mailbox Plugin. The Database Mailbox Plugin supports two kinds of databases: Generic and Emerald databases.

Emerald Database

Information on using the Database Plugin with an Emerald Database is provided in the appendix on Emerald Integration.

Generic Database

The Generic database assumes a very straightforward database schema. User information is contained in a single table, **`Mailboxes`**, with columns **`Mailbox`**, **`FullName`**, **`Password`** and **`Domain`**. You can override these defaults by filling in the fields on the configuration form.

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

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

MailSite has the ability to store all of its configuration data and mailbox information in a SQL database. This type of configuration is used to create clusters of MailSite nodes, which allow sites to handle more mailboxes and e-mail traffic than a single server system could support. Database storage also allows sites to integrate MailSite mailbox information with popular commercial billing packages.

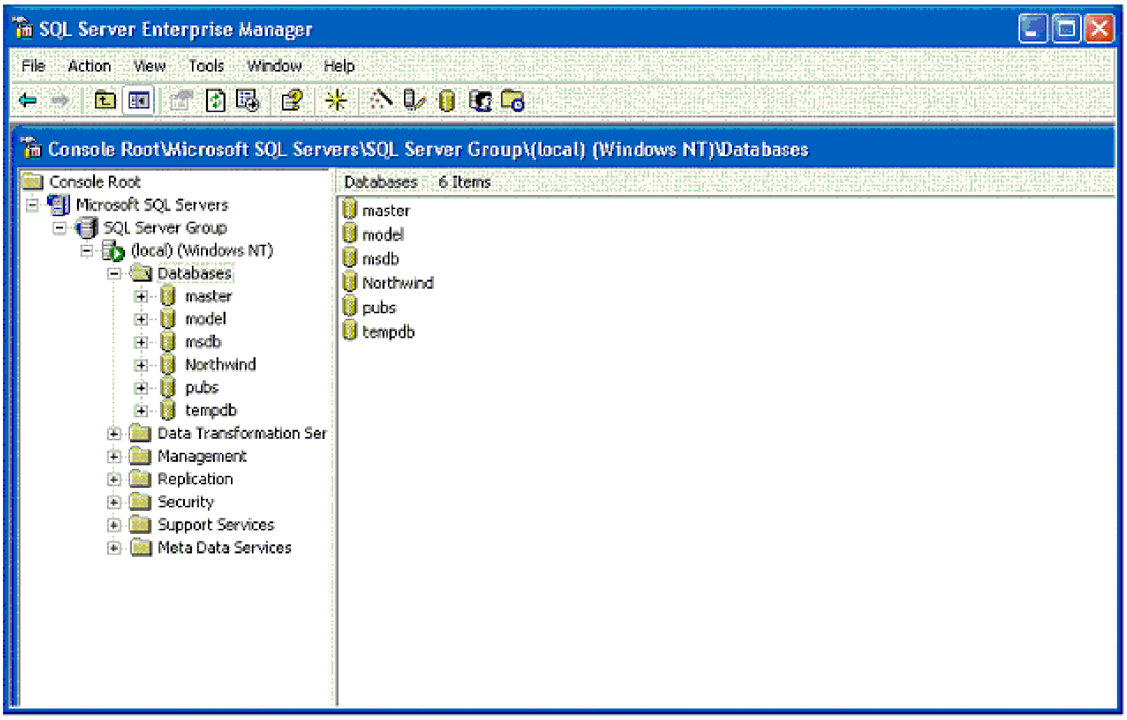
This section describes the configuration of the MailSite SQL Connector, the component that provides database integration. Your MailSite license type may not support the functions described here.

Setting Up the SQL Server Database

The first step in setting up the MailSite SQL Connector is to create a SQL Server database to contain MailSite data. Only one SQL Server database is required for all MailSite configuration, domain, mailbox, and mail list data. Note that if you are upgrading from an old version of MailSite and have an existing database of DataCenter mailboxes, you should create a new database for MailSite data (your existing DataCenter mailboxes will be imported to the new database during setup of the SQL Connector).

To create a SQL Server database for MailSite:

1. Open the SQL Server Enterprise Manager.
2. Under the icon that corresponds to your database server system, right-click on the **Databases** folder and select **New Database**.

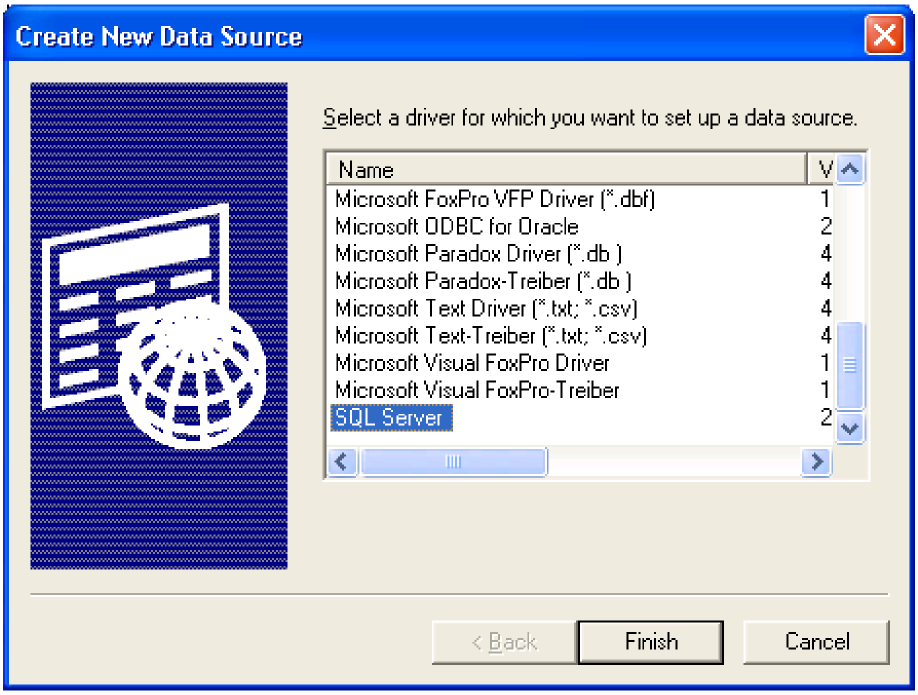


3. Enter an appropriate name for the new database (for example, **mailsite_db**).
4. Click **OK** to create the database.

Creating the Data Source

Once the MailSite database has been created, you can create a connection to this data source from your MailSite server system. This is required to allow MailSite to communicate with the database. To create the data source:

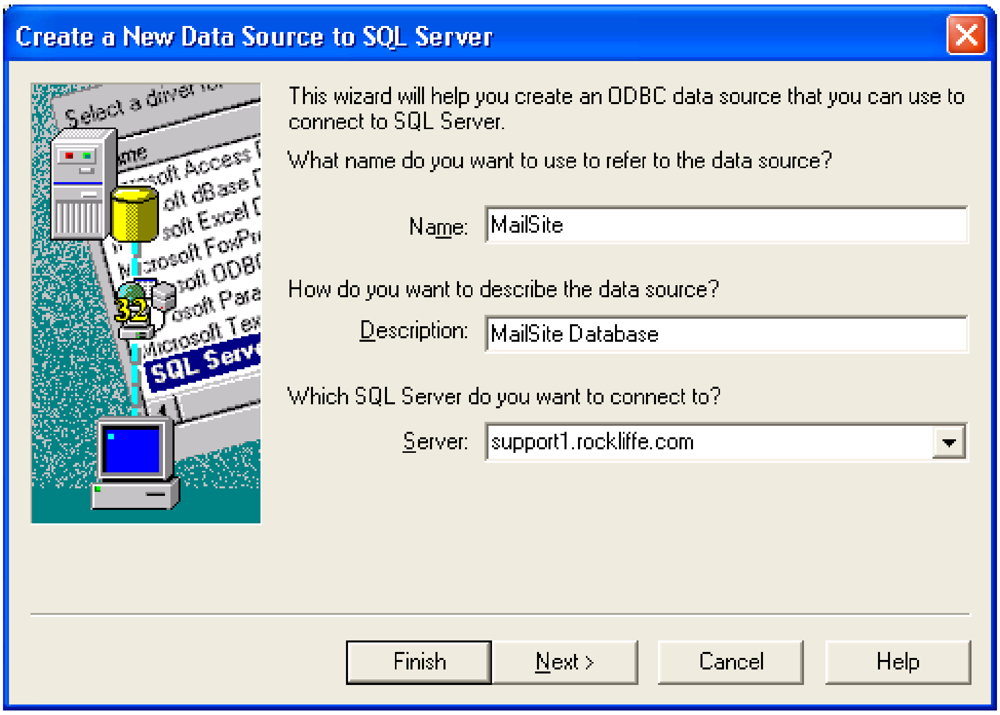
1. On your mail server system, open **Start>Programs>Administrative Tools>Data Sources (ODBC)**.
2. Select the **System DSN** tab, and click **Add**.
3. From the list of database drivers, select **SQL Server** and click Finish.



Select a driver for which you want to set up a data source.

Name	V
Microsoft FoxPro VFP Driver (*.dbf)	1
Microsoft ODBC for Oracle	2
Microsoft Paradox Driver (*.db)	4
Microsoft Paradox-Treiber (*.db)	4
Microsoft Text Driver (*.txt; *.csv)	4
Microsoft Text-Treiber (*.txt; *.csv)	4
Microsoft Visual FoxPro Driver	1
Microsoft Visual FoxPro-Treiber	1
SQL Server	2

4. Enter a name and description for the data source, and enter the host name or IP address of your database system:



Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: MailSite

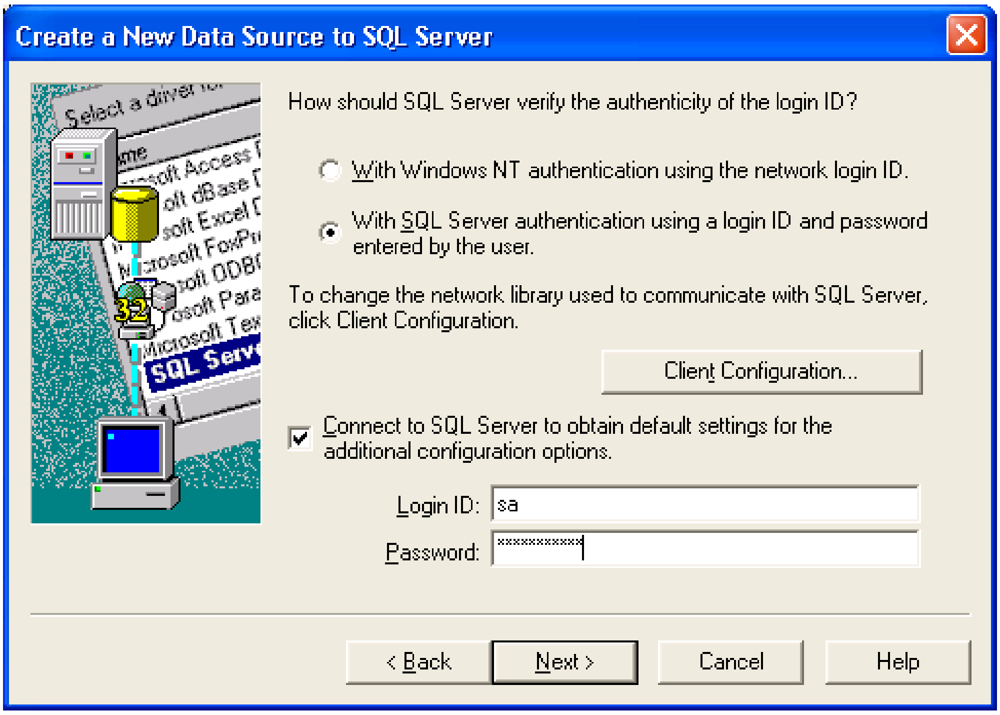
How do you want to describe the data source?

Description: MailSite Database

Which SQL Server do you want to connect to?

Server: support1.rockliffe.com

5. Click **Next**. On the authentication panel, select SQL Server authentication and enter the name and password for the SQL Server login **sa**:



Create a New Data Source to SQL Server

How should SQL Server verify the authenticity of the login ID?

○ With Windows NT authentication using the network login ID.

● With SQL Server authentication using a login ID and password entered by the user.

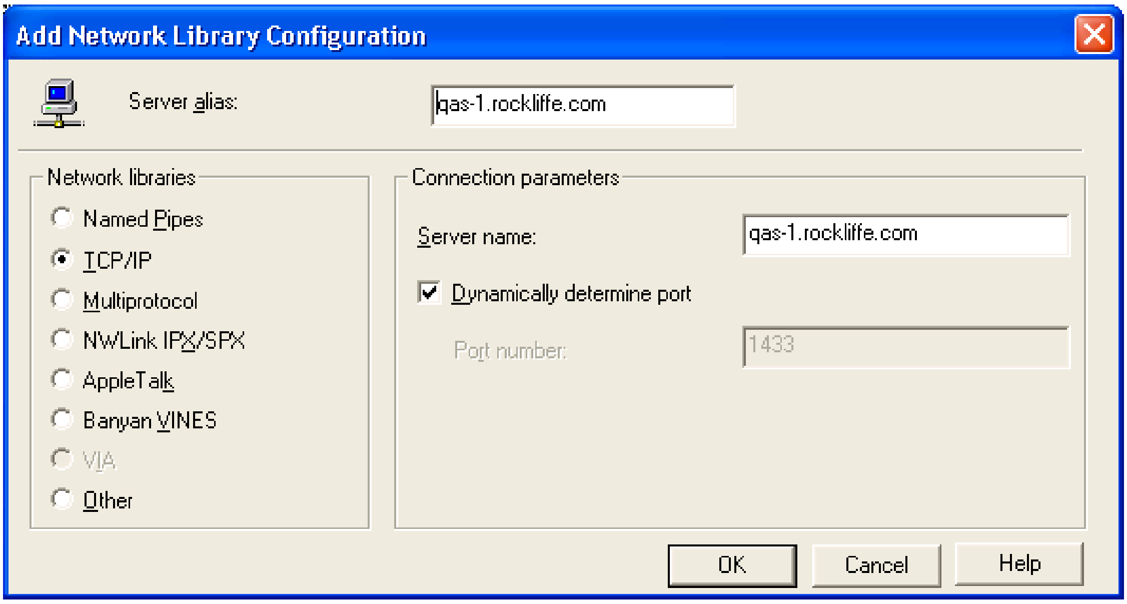
To change the network library used to communicate with SQL Server, click Client Configuration.

☑ Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID: sa

Password: ***********

6. The MailSite SQL Connector requires TCP/IP communication to the data source, which may or may not be the default. To set the protocol of the data source, click the **Client Configuration** button on the authentication page, which displays this dialog:



Add Network Library Configuration

Server alias: qas-1.rockliffe.com

Network libraries

○ Named Pipes
● TCP/IP
○ Multiprotocol
○ NWLink IPX/SPX
○ AppleTalk
○ Banyan VINES
○ VIA
○ Other

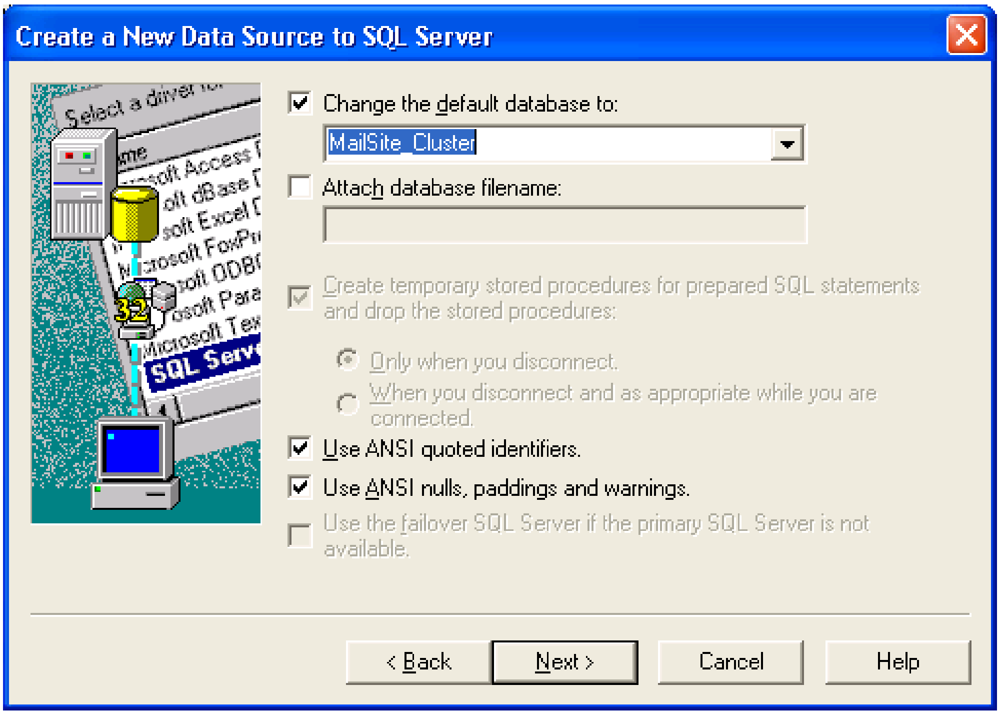
Connection parameters

Server name: qas-1.rockliffe.com

☑ Dynamically determine port

Port number: 1433

7. After selecting **TCP/IP** as the network library, click **OK** to confirm the client parameters, and then click **Next** on the authentication page. .



Create a New Data Source to SQL Server

☑ Change the default database to:

MailSite_Cluster

☐ Attach database filename:

☑ Create temporary stored procedures for prepared SQL statements and drop the stored procedures:

● Only when you disconnect.

○ When you disconnect and as appropriate while you are connected.

☑ Use ANSI quoted identifiers.

☑ Use ANSI nulls, paddings and warnings.

☐ Use the failover SQL Server if the primary SQL Server is not available.

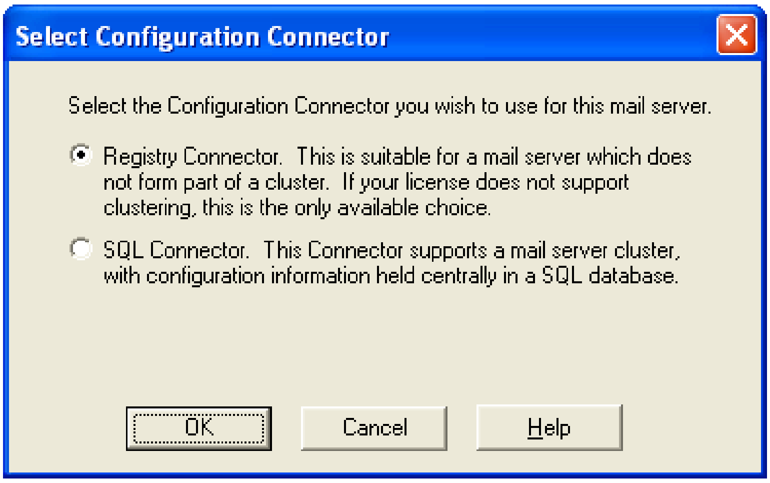
8. Select the name of your MailSite database in SQL Server from the pull-down menu.

9. Click **Next**, and then click **Finish**. The data source is now ready for use by MailSite.

Changing the Configuration Connector

By default, MailSite operates using the Registry connector, which stores all configuration and mailbox data in the Windows registry. Using MailSite with the SQL connector requires that you change the MailSite configuration connector from Registry to SQL.

In the Server folder of the MailSite Console, double-click the **Configuration connector** icon, which displays this dialog:



Select the Configuration Connector you wish to use for this mail server.

● Registry Connector. This is suitable for a mail server which does not form part of a cluster. If your license does not support clustering, this is the only available choice.

○ SQL Connector. This Connector supports a mail server cluster, with configuration information held centrally in a SQL database.

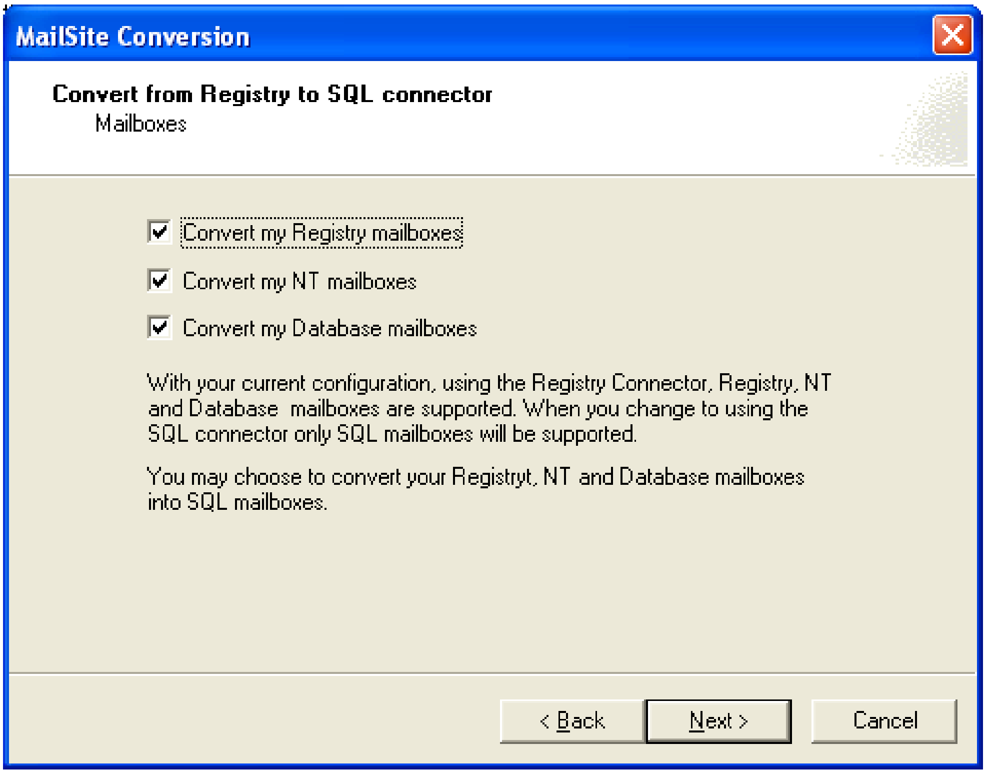
Select **SQL Connector** and click **OK**. You will then be asked if you are creating a new MailSite cluster or adding this MailSite node to an existing cluster. If you are creating a new MailSite cluster you will proceed to the Migration Wizard, which allows you to specify the MailSite data that should be migrated from the registry to the database. If you are adding this MailSite node to an existing cluster, you will go directly to the SQL Connector wizard.

Migration Wizard

When creating a new MailSite cluster, the domain and configuration information stored by MailSite in the Windows registry will automatically be imported to the SQL Connector database, which is will then use as its data source. During this process you may optionally migrate existing mailboxes and mail lists from the registry to the SQL Connector database as well.

The Migration wizard is automatically launched when you change the MailSite configuration connector to SQL Connector and choose to create a new cluster.

1. Select the mailbox types that should be migrated. These mailboxes will be converted from their current types to SQL mailboxes. All existing mailboxes on your system of the selected types will be imported to the database and will be available after migration, while mailboxes of types not selected will not be migrated:



Convert from Registry to SQL connector

Mailboxes

☑ Convert my Registry mailboxes

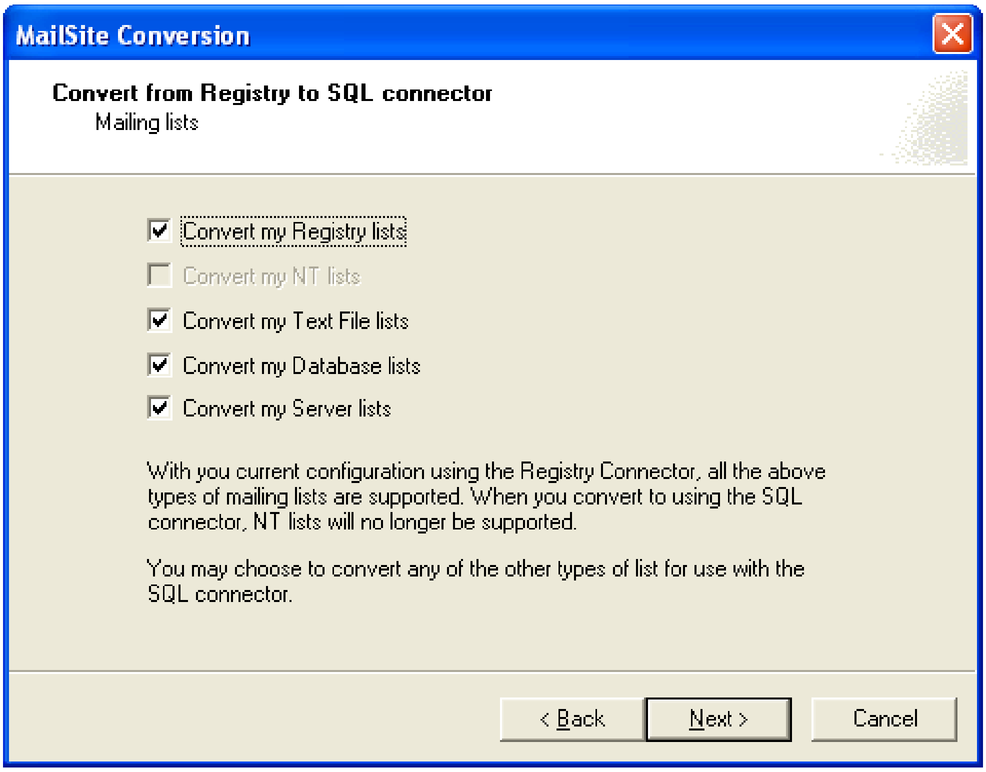
☑ Convert my NT mailboxes

☑ Convert my Database mailboxes

With your current configuration, using the Registry Connector, Registry, NT and Database mailboxes are supported. When you change to using the SQL connector only SQL mailboxes will be supported.

You may choose to convert your Registryt, NT and Database mailboxes into SQL mailboxes.

2. Select the mail list types that should be migrated to the SQL connector database. All existing mail lists on your system of the selected types will be imported to the database and will be available after migration, while mail lists of types not selected will be unavailable when MailSite is running with the SQL Connector.



Convert from Registry to SQL connector

Mailing lists

☑ Convert my Registry lists

□ Convert my NT lists

☑ Convert my Text File lists

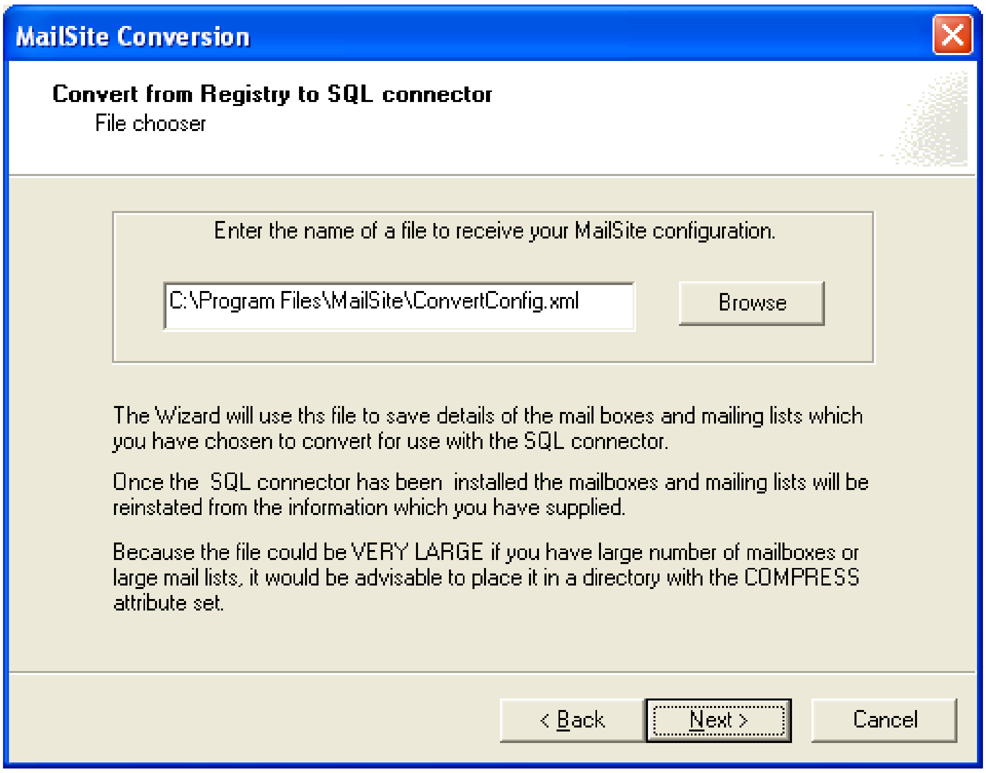
☑ Convert my Database lists

☑ Convert my Server lists

With you current configuration using the Registry Connector, all the above types of mailing lists are supported. When you convert to using the SQL connector, NT lists will no longer be supported.

You may choose to convert any of the other types of list for use with the SQL connector.

3. Specify a file name for the MailSite conversion file (or click **Next** to select the default file name):



MailSite Conversion

Convert from Registry to SQL connector

File chooser

Enter the name of a file to receive your MailSite configuration.

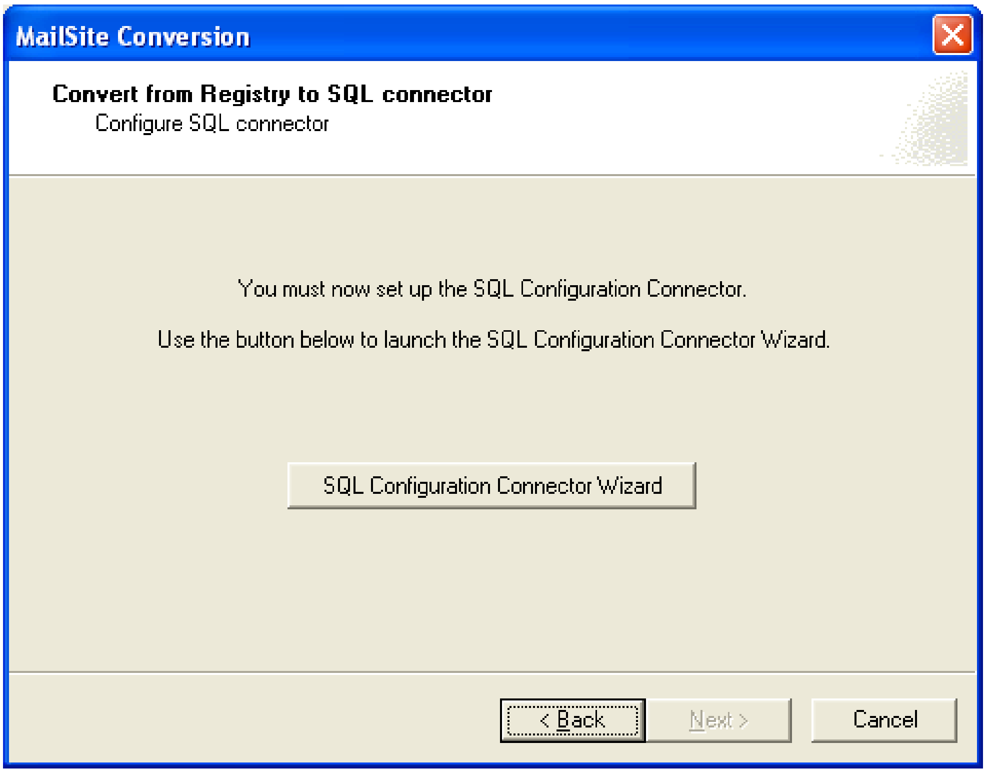
C:\Program Files\MailSite\ConvertConfig.xml

The Wizard will use ths file to save details of the mail boxes and mailing lists which you have chosen to convert for use with the SQL connector.

Once the SQL connector has been installed the mailboxes and mailing lists will be reinstated from the information which you have supplied.

Because the file could be VERY LARGE if you have large number of mailboxes or large mail lists, it would be advisable to place it in a directory with the COMPRESS attribute set.

4. The Migration wizard will now prompt you to launch the SQL Connector wizard, which is used to define the MailSite database that will contain the migrated data:



MailSite Conversion

Convert from Registry to SQL connector

Configure SQL connector

You must now set up the SQL Configuration Connector.

Use the button below to launch the SQL Configuration Connector Wizard.

5. After you complete the SQL Connector wizard you will return to the Migration wizard, which will then finish by prompting you to commit the migration process.

SQL Connector Wizard

The SQL Connector wizard is used to set MailSite database. This wizard is automatically launched when you change the MailSite configuration connector to SQL connector.

Server roles

The SQL Connector wizard can be used additionally to manage server “roles”.

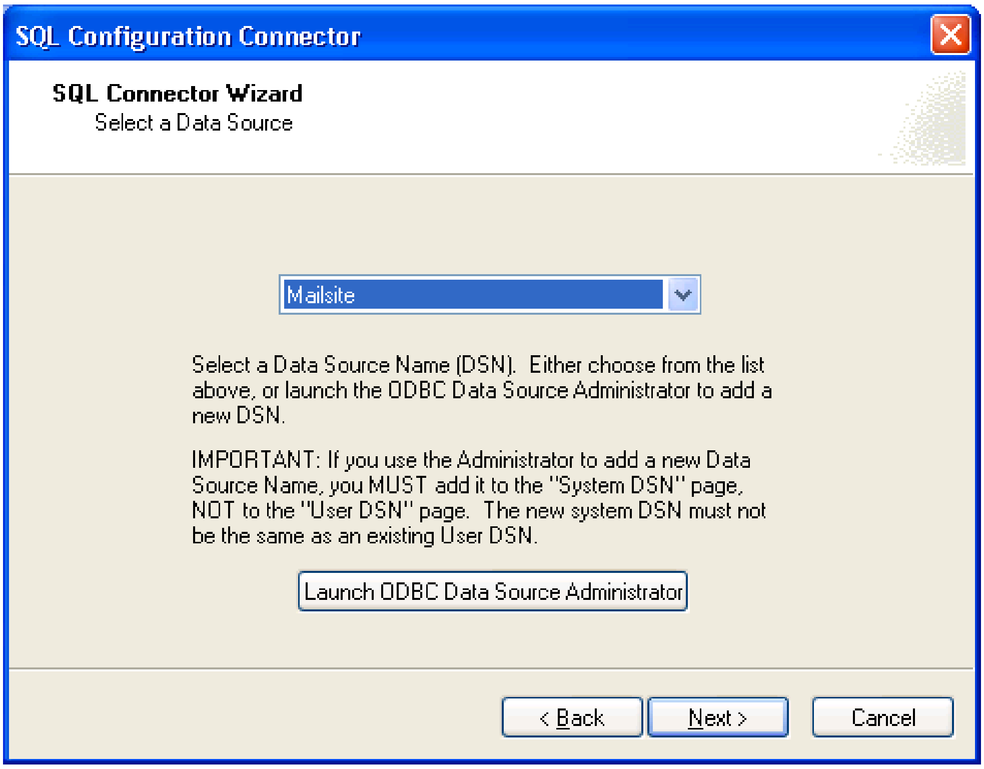
Server roles can be assigned to a number of servers so that they share the same configuration. If you later wish to reconfigure a group of servers that share the same role, you need only reconfigure one of the servers and all the servers assigned the same role will pick up the new configuration. This removes the need to make the same change to every server instance in the group.

There are no limits to the number of servers that may be assigned a role.

Servers may also be assigned unique roles. To implement this create a new role for each server in the cluster. For example you may have heavy IMAP use and light POP use so you might want only one POP server which is configured differently to a group of IMAP servers.

A server’s role is changeable. Administrators should be aware that services which are affected by a change in role must be manually stopped and restarted in order to pick up any new properties.

1. Begin by selecting the data source you created for your MailSite database (if you have not already created the data source, click the button to launch the ODBC control panel):



SQL Configuration Connector

SQL Connector Wizard

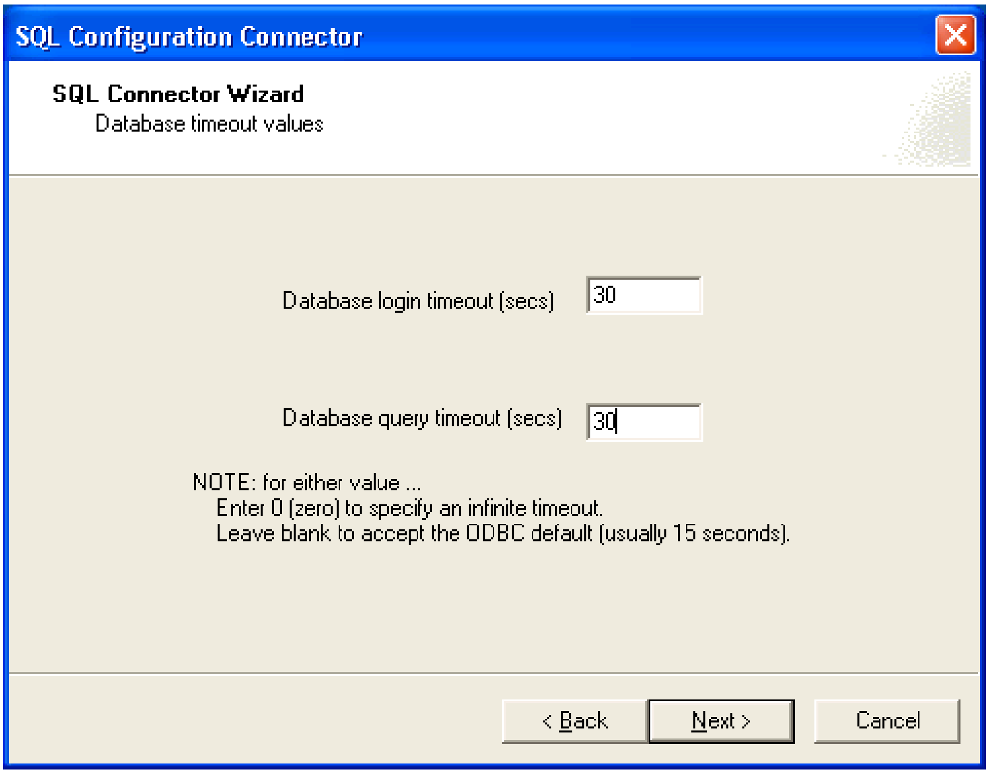
Select a Data Source

Mailsite

Select a Data Source Name (DSN). Either choose from the list above, or launch the ODBC Data Source Administrator to add a new DSN.

IMPORTANT: If you use the Administrator to add a new Data Source Name, you MUST add it to the "System DSN" page, NOT to the "User DSN" page. The new system DSN must not be the same as an existing User DSN.

2. Set timeout values for database connections, or leave blank to accept the default SQL Server timeouts (the recommended choice):



SQL Connector Wizard

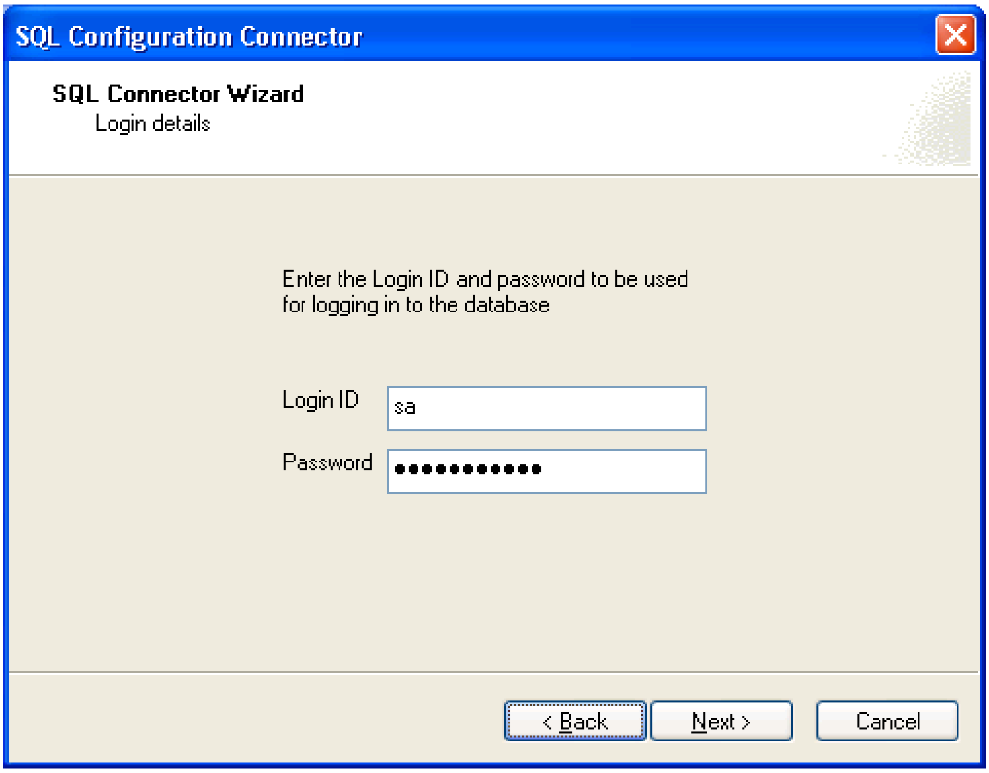
Database timeout values

Database login timeout (secs) 30

Database query timeout (secs) 30

NOTE: for either value ...
Enter 0 (zero) to specify an infinite timeout.
Leave blank to accept the ODBC default (usually 15 seconds).

3. Enter the name and password for the **sa** SQL Server login:



SQL Connector Wizard

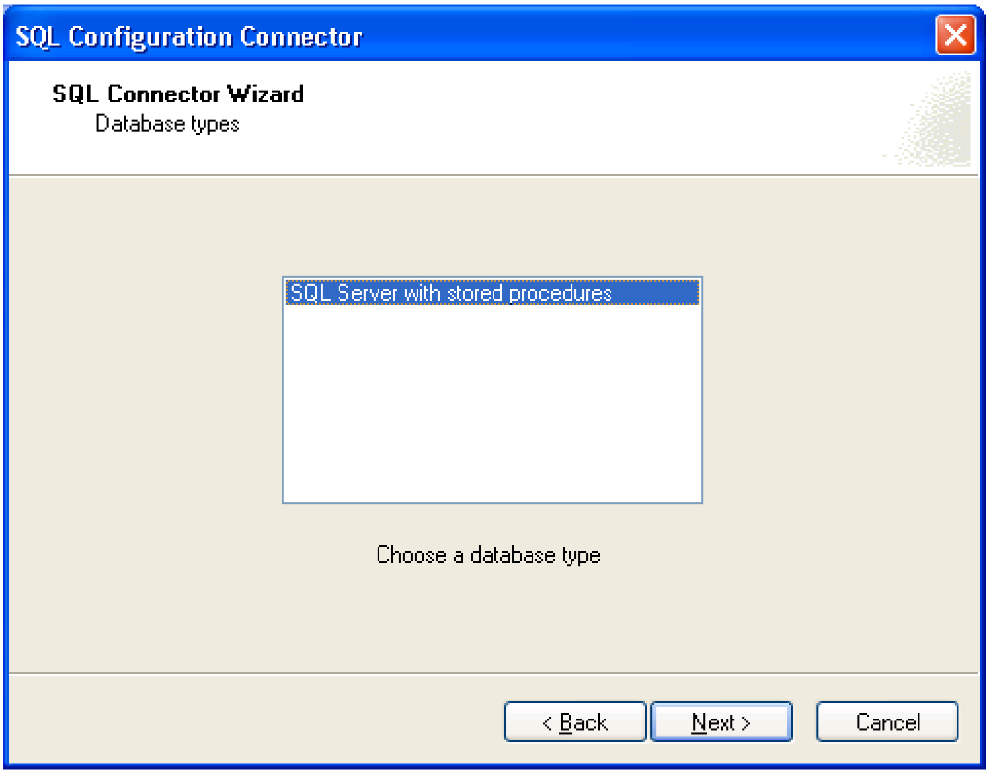
Login details

Enter the Login ID and password to be used for logging in to the database

Login ID sa

Password ●●●●●●●●●●●

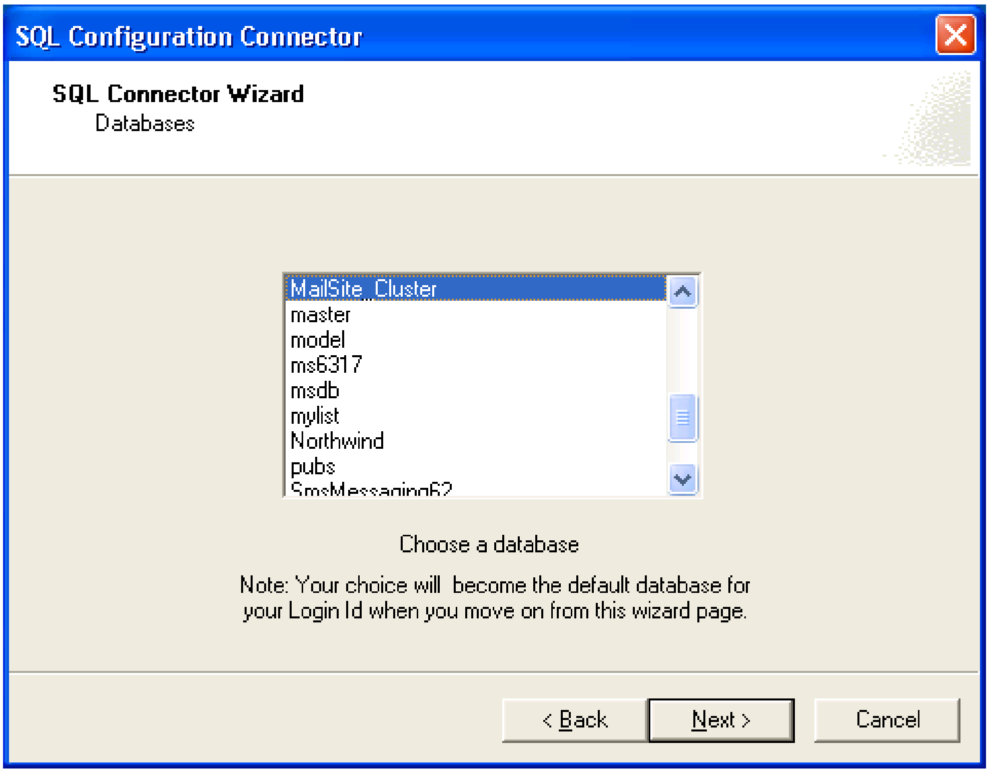
4. When prompted for database type, select **SQL Server with stored procedures**:



SQL Server with stored procedures

Choose a database type

5. The SQL Connector wizard will display the databases available in SQL Server. Select the database that you created to store MailSite data:

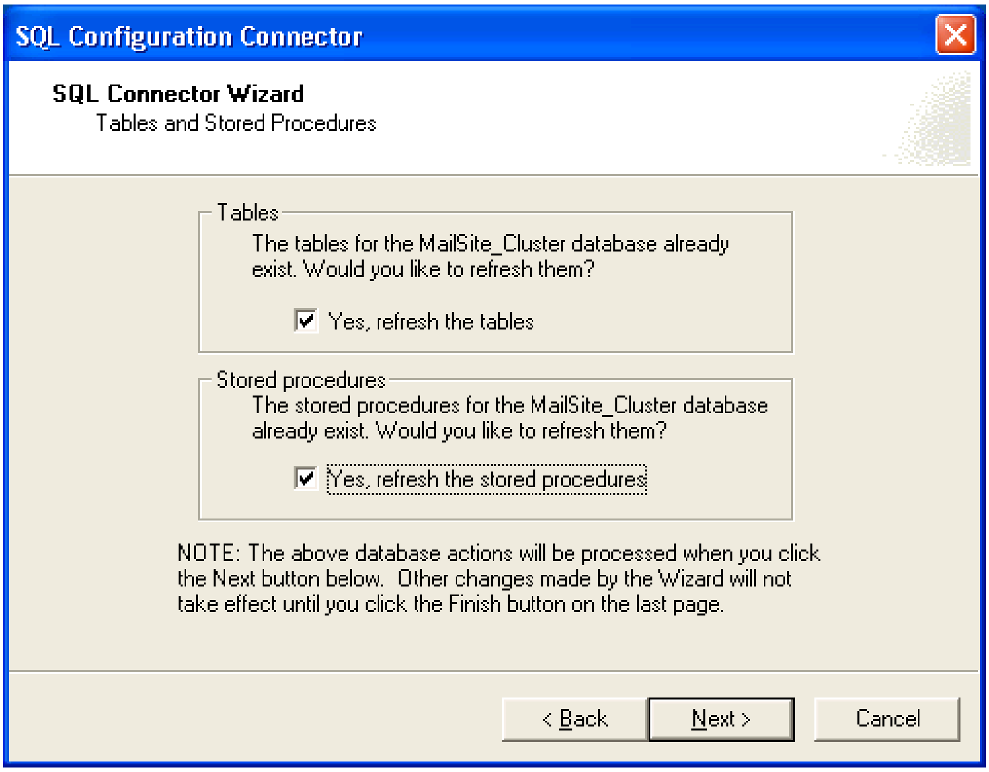


MailSite_Cluster
master
model
ms6317
msdb
mylist
Northwind
pubs
SmsMessaging62

Choose a database

Note: Your choice will become the default database for your Login Id when you move on from this wizard page.

6. If the MailSite tables and stored procedures have not previously been added to your database, the SQL Connector wizard will prompt you to add them. You must create the tables and stored procedures before MailSite can use the database:



SQL Connector Wizard

Tables and Stored Procedures

Tables

The tables for the MailSite_Cluster database already exist. Would you like to refresh them?

☑ Yes, refresh the tables

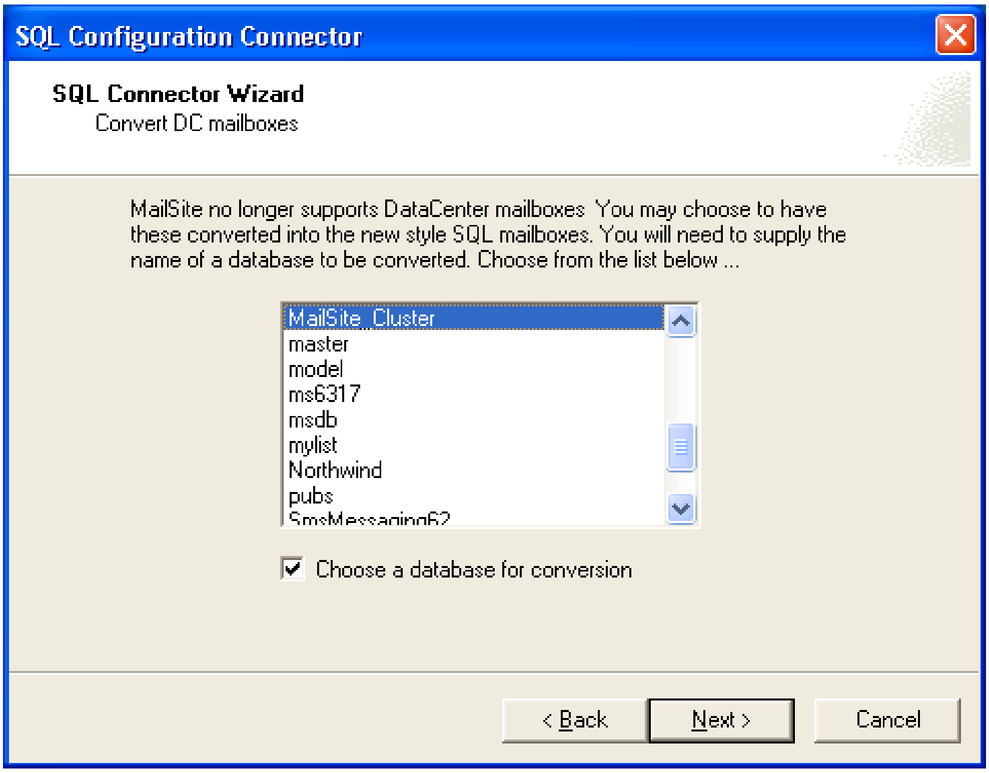
Stored procedures

The stored procedures for the MailSite_Cluster database already exist. Would you like to refresh them?

☑ Yes, refresh the stored procedures

NOTE: The above database actions will be processed when you click the Next button below. Other changes made by the Wizard will not take effect until you click the Finish button on the last page.

7. If you are creating a new MailSite cluster, you will be prompted to select a previous MailSite DataCenter database for conversion to the latest version:



SQL Configuration Connector

SQL Connector Wizard

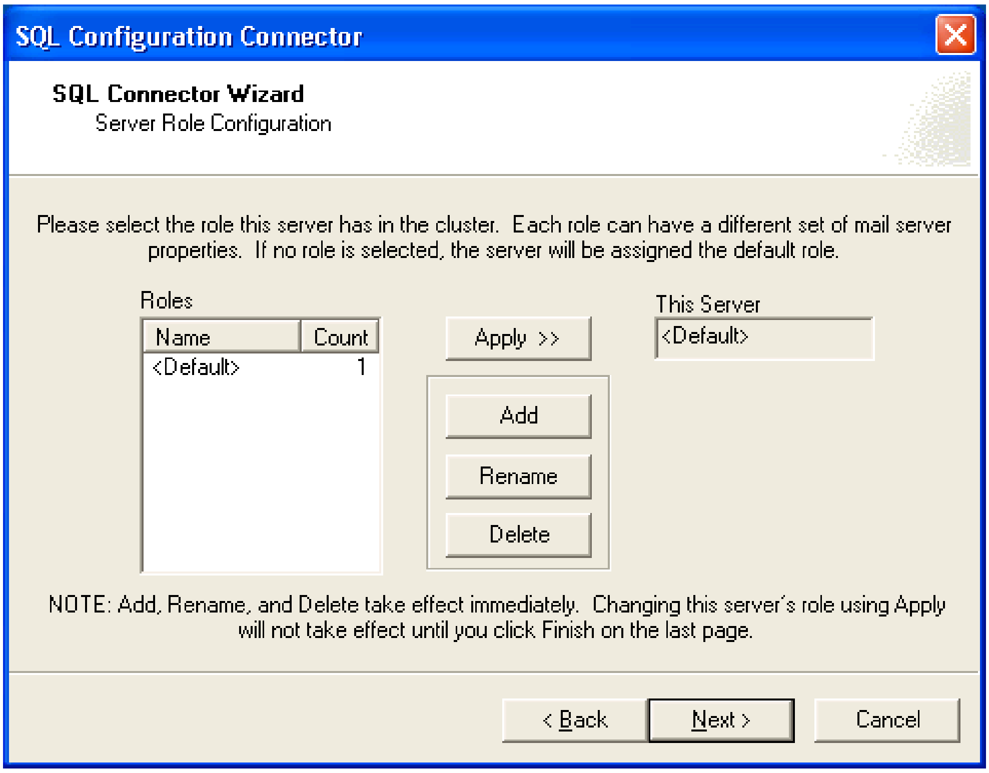
Convert DC mailboxes

MailSite no longer supports DataCenter mailboxes You may choose to have these converted into the new style SQL mailboxes. You will need to supply the name of a database to be converted. Choose from the list below ...

- MailSite_Cluster
- master
- model
- ms6317
- msdb
- mylist
- Northwind
- pubs
- SmsMessaging62

☑ Choose a database for conversion

8. Select the role of this server from the list and assign it to this server using the Apply button. If you want this server to have new role that is not in the list, you may Add a new role and Apply the new role to this server. You may also Rename and Delete roles (You may only delete roles that have no servers assigned to them.)



SQL Configuration Connector

SQL Connector Wizard

Server Role Configuration

Please select the role this server has in the cluster. Each role can have a different set of mail server properties. If no role is selected, the server will be assigned the default role.

Roles

Name	Count
<Default>	1

This Server

<Default>

NOTE: Add, Rename, and Delete take effect immediately. Changing this server's role using Apply will not take effect until you click Finish on the last page.

9. Click **Finish** to complete the wizard. If this is the first time through the SQL connector Wizard the MailSite Console will automatically shutdown and restart.

   If this is NOT the first time through the SQL connector wizard and you are changing a servers role the Mailsite Console will not automatically restart and you will be prompted to stop and start any services that the change in role may affect.

Monitoring

There are two ways that you can monitor the operation of your MailSite server. You can monitor activity using the Performance Monitor, or log a range of information to one or more log files, to the Event Viewer, and to an ODBC database.

Logging

MailSite supports three categories of logging: server logging, operation logging and error logging.

§ Server logging is concerned with events such as services starting up and closing down, manual commands to retry domains, and configuration reloads.

§ Operation logging is concerned with network connections made and released, protocol exchanges and transaction summaries.

§ Error logging is concerned with protocol syntax/sequence errors, failed protocol commands, authentication errors, and network or file I/O errors.

You can record this log information in three different places:

⇒ In log files. Each of the three logging categories have their own log files, created in a configurable log directory.

⇒ In the Application Event Log. Use the Event Viewer application, which you can find in the Administrative Tools program group, to examine the Event Log.

⇒ In an ODBC database.

To control logging, use the Logs Folder in the Windows Console. Refer to the MailSite web site for a comprehensive list of error codes.

Performance Monitor

Within Windows 2000/2003 you can monitor the dynamic activities of MailSite by using the Performance Monitor. The Performance Monitor is a standard utility and can be found in the program group **`Administrative Tools`**. This is not possible when MailSite is installed on Windows Server 2008 due to changes in the operating system's support for this feature. The MailSite Installation Wizard creates a shortcut to the Performance Monitor in the MailSite group. You can start it from the program group, or execute **`PERFMON`** from the Command Prompt.

Eight performance objects are provided: POP3A, IMAP4A, SMTPDA, SMTPRA, LDAP3A, MAILMA, HTTPMA and Spamtest Result. These tables list the performance objects, counters and an explanation text for each:

POP3A Object

Counter Name	Explanation Text
Active Connections	The number of currently active connections to the service. Indicates current service activity.
Bytes Sent/Sec	The number of bytes the service has sent to the network for messages retrieve operations. Indicates how busy the service is.
Messages Retrieved/Sec	The number of messages retrieved per second. Indicates how busy the service is.
Total Connections	Total Connections includes all connections (successful logons and failed logons) to the service since the service is last restarted.
Total Logon Failures	The number of failed logon attempts to the service since the service is last restarted. Can indicate whether password-guessing programs are being used to crack the security on the service.

IMAP4A Object

Counter Name	Explanation Text
Active Connections	The number of currently active connections to the service. Indicates current service activity.
Bytes Sent/Sec	The number of bytes the service has sent to the network in response to commands. Indicates how busy the service is.
Commands Received/Sec	The number of commands received from clients per second.
Total Connections	Total Connections includes all connections (successful logons and failed logons) to the service since the service is last restarted
Total Logon Failures	The number of failed logon attempts to the service since the service is last restarted. Can indicate whether password-guessing programs are being used to crack the security on the service

SMTPDA Object

Counter Name	Explanation Text
Bytes Sent/Sec	The number of bytes the service has sent on the network. Indicates how busy the service is.
Currently Active Connections	The number of outgoing SMTP connections which are currently open.
Messages Delivered Locally/Sec	The number of messages delivered from the service per second.
Messages Sent/Sec	The number of messages sent from the service per second.
Total Messages Delivered locally	The number of messages delivered locally by the service since the service was last restarted
Total Messages Sent	The number of messages sent to other mail servers since the service was last restarted.

SMTPRA Object

Counter Name	**Explanation Text**
Active Connections	The number of currently active connections to the service. Indicates current service activity.
Bytes Received/Sec	The number of bytes the service has received from the network. Indicates how busy the service is.
Message Received/Sec	The number of messages received per second.
Total Connections	Total Connections includes all connections to the service since the service was last restarted.
Total Messages Received	The total number of messages per second received by the service since it was last restarted.

Spamtest Result Object

Counter Name	**Explanation Text**
Messages Scanned	The percentage of messages scanned by the anti spam engine. Indicates the distribution of spam scores for scanned messages across all spam score values.
Messages Scanned/Sec	The number of messages per second scanned by the anti spam engine. Indicates the rate of spam scores for scanned messages.

Note: The Spamtest Result object has 11 instances corresponding to the 11 possible spam score values [0-10]. When all instances are viewed as a bar chart the columns will be sorted from Band 0 to Band 10. The Messages Scanned counter will then provide a histogram of the spam score distribution.

LDAP3A Object

Counter Name	**Explanation Text**
Connections/Sec	Connections/Sec is the rate at which the server is receiving LDAP transaction requests.
Total Bytes/Sec	Total Bytes/Sec is the rate at which the server is transmitting transaction response data.

HTTPMA Object

Counter Name	**Explanation Text**
Connections/Sec	Connections/Sec is the rate at which the server is receiving HTTPS transaction requests.
Total Bytes/Sec	Total Bytes/Sec is the rate at which the server is transmitting transaction response data.

MAILMA Object

Counter Name	**Explanation Text**
Active Connections	The number of currently active connections to the service. Indicates current service activity.

Total Connections	Total Connections includes all connections (successful logons and failed logons) to the service since the service is last restarted.
Total Logon Failures	The number of failed logon attempts to the service since the service is last restarted. Can indicate whether password-guessing programs are being used to crack the security on the service.

Disk Maintenance

High volumes of mail traffic can cause NT disk drives to become fragmented, which can lead to decreased disk performance. For this reason it's recommended that you regularly run a defragmenting utility such as Norton Disk Doctor on your disk partitions where mail is stored.

Monitoring Spam Traffic

There are two ways to monitor the operation of a MailSite server. Activity can be monitored using the Windows performance monitor or information can be logged to one or more log files, to the Event Viewer, and to an ODBC database. Spam-related information such as message spam scores, spam processing activity, and DHAP activity is written to one or more logs within MailSite. Additionally, you can monitor the dynamic activities of MailSite from the Windows Performance Monitor.

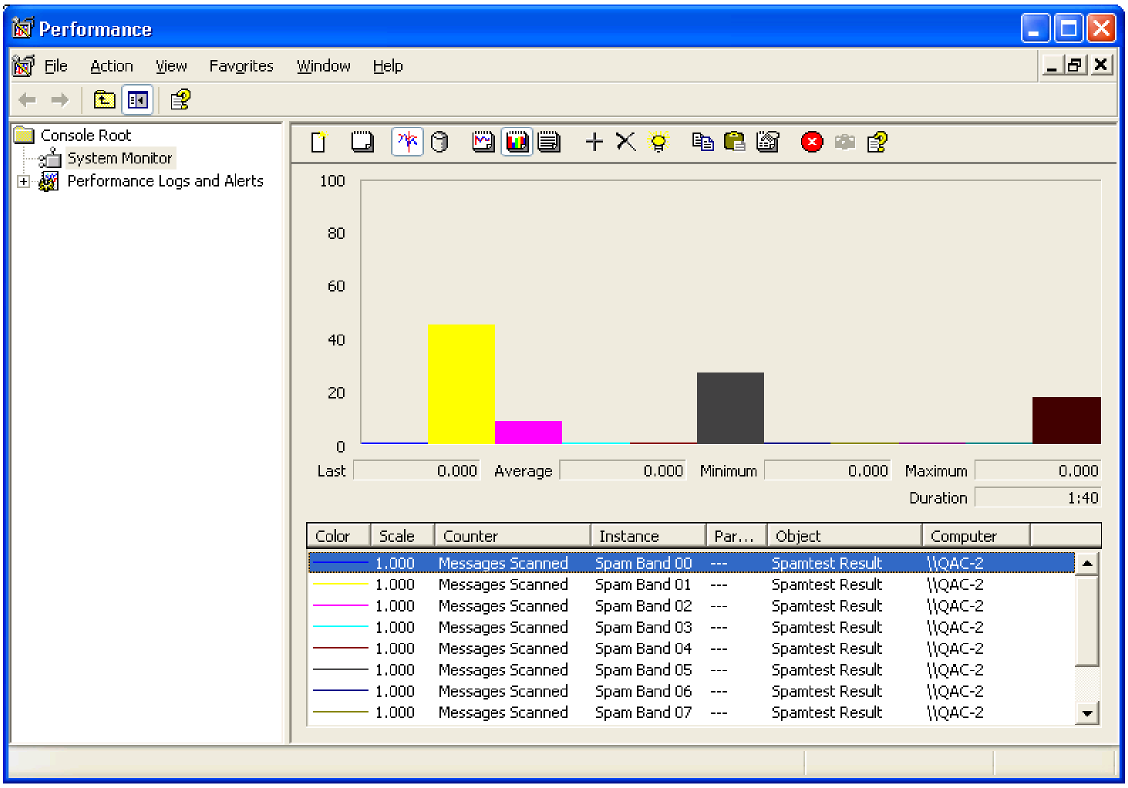
The Performance Monitor is a standard utility and can be found in the program group Administrative Tools. Eight Windows performance-monitoring objects are provided with MailSite, including the Spamtest Result Object.

Spamtest Result– A Performance Monitoring Object

Counter Name	Explanation Text
Messages Scanned	The percentage of messages scanned by the anti spam engine. Indicates the distribution of spam scores for scanned messages across all spam score values.
Messages Scanned/Sec	The number of messages per second scanned by the anti spam engine. Indicates the rate of spam scores for scanned messages.

For more information regarding the other performance monitoring objects provided with Mailsite, please refer to the section entitled "*Monitoring*" in the MailSite Administration Guide.

Monitoring Spam Traffic from Windows Performance Monitor



Last 0.000 Average 0.000 Minimum 0.000 Maximum 0.000

Duration 1:40

Color	Scale	Counter	Instance	Par...	Object	Computer
▬	1.000	Messages Scanned	Spam Band 00	---	Spamtest Result	\\QAC-2
▬	1.000	Messages Scanned	Spam Band 01	---	Spamtest Result	\\QAC-2
▬	1.000	Messages Scanned	Spam Band 02	---	Spamtest Result	\\QAC-2
▬	1.000	Messages Scanned	Spam Band 03	---	Spamtest Result	\\QAC-2
▬	1.000	Messages Scanned	Spam Band 04	---	Spamtest Result	\\QAC-2
▬	1.000	Messages Scanned	Spam Band 05	---	Spamtest Result	\\QAC-2
▬	1.000	Messages Scanned	Spam Band 06	---	Spamtest Result	\\QAC-2
▬	1.000	Messages Scanned	Spam Band 07	---	Spamtest Result	\\QAC-2

The Spamtest Result object has 11 instances corresponding to the 11 possible spam score values [0-10]. When all instances are viewed as a bar chart the columns will be sorted from Band 0 to Band 10. The Messages Scanned counter will then provide a **histogram** of the **spam score distribution**.

Monitoring Last Access

The last login time and service type can be logged to one or more log files or to an ODBC database. This information is logged when the **Receive Transaction Summary** is selected under **Operation Log Flags**. The resultant log entries capture the service name, date, time, login name and client IP address.

The summary is written to the log for the service:

```
---- POP3A log entry made at 06/20/2005 17:37:13

User foo@example.com successfully logged in from 127.0.0.1
```

MailSite Engine

The MailSite Engine consists of seven services, which are equivalent to UNIX daemons such as **sendmail** and **pop3**. These services are:

- ⇒ **SMTPDA**, which handles outgoing SMTP transactions. This is the service responsible for routing messages to remote domains.
- ⇒ **SMTPRA**, which handles incoming SMTP transactions. This is the service that receives mail from other sites.
- ⇒ **POP3A**, which provides mail client access through the POP3 protocol.
- ⇒ **IMAP4A**, which provides mail client access through the IMAP4 protocol.
- ⇒ **MAILMA**, which is used by the MailSite Console to remotely manage mailbox and mail list data, and allows Eudora users to change their e-mail password.
- ⇒ **HTTPMA**, which allows users to access to the Web Console with a web browser.
- ⇒ **LDAP3A**, which provides access to account information through the LDAP protocol.

The following sections provide details about these services and other MailSite resources.

SMTP Receiver Service

The Receiver implements the SMTP Internet mail standard. It appears to the outside world exactly the same as a UNIX **sendmail** server.

The Receiver listens for incoming messages on TCP/IP port 25. It places the messages in the **incoming** mail directory.

A message is stored as two separate files, named **uniquename.MSG** and **uniquename.RCP.** The **uniquename** is a unique identifier by which the message is known while it is in the system.

The **MSG** file contains the message itself. The file is byte-stuffed (i.e. a redundant dot is inserted at the beginning of lines which start with a dot), and the end of the file is indicated by a single dot on a line by itself.

The **RCP** file contains the names of the recipients of the message, and the originator of the message (to whom non-delivery reports will be sent).

The Receiver will log incoming and outgoing transactions if the Logging options are set. This can be useful for analyzing mail transactions and errors.

The service is multi-threaded. This means that it can handle multiple connections from other mail servers at the same time.

The SMTP Receiver Service implements the SMTP and Extended SMTP protocols (ESMTP) defined in RFCs 821, 1652, 1869, 1870, 1985. Refer to **http://www.rfc-editor.org** for a complete list of RFCs.

The following SMTP commands are supported:

```
HELO        DATA
EHLO        RSET
QUIT        NOOP
MAIL        VRFY
RCPT
```

The following Extended SMTP commands are supported:

```
SIZE        8BITMIME
```

By default, a command of the form VRFY **`name@domain.com`** will return a successful response if the server accepts mail for domain.com. If **`Enable Full VRFY Support`** is set using the Security window, then this service will give information about whether **`name@domain.com`** is a mailbox or a mail list (or is unknown).

SMTP Delivery Service

The SMTP Delivery Service is the internal sorter for MailSite. It deals with messages that have been received by the SMTP Receiver.

It moves messages from the **`incoming`** directory, and stores them in a **`holding`** directory. For each distinct domain in the list of message recipients, the service creates a subdirectory (within the **`domains`** directory), where it places information about the recipients in that directory.

For local deliveries, the service temporarily stores recipient information in a special **`$local$`** subdirectory within the **`domains`** directory. It then copies messages into each local recipient's **`inbox`** directory.

For mail that is destined elsewhere, the service will submit a DNS request for a MX record for the corresponding domain. (It determines the DNS server address from the computer's TCP/IP configuration, so you must configure your computer with a correct DNS server address.) It uses the MX record to determine the TCP/IP address(es) to which it should attempt to send messages for that domain. The service will attempt to establish contact with the mail server at that domain and transmit the message. If unsuccessful, it will wait a while before attempting to contact the mail server again. It will persistently try to contact the mail server for several days, according to the Retry Schedule.

The message files in the **`holding`** directory are of the form **`uniquename.MSG`**. These files are byte-stuffed (i.e. a redundant dot is inserted at the beginning of lines which start with a dot), and the end of the file is indicated by a single dot on a line by itself.

The files in the **`domains`** directory are of the form **`uniquename.RCP`**. These files contain the names of the recipients of the message, and the originator of the message (to whom non-delivery reports will be sent).

The **`domains`** directory also contains a file **`DOMAIN.MRI`** that records routing information and details of how many times the SMTP Delivery Agent has attempted to contact each domain.

The SMTP Delivery Agent is multi-threaded and can deliver mail to multiple destinations at the same time.

POP3 Server

The POP3 server implements the Post Office Protocol version 3 Internet standard. It is responsible for passing incoming mail messages to e-mail clients.

It listens on TCP/IP port 110 for connections from e-mail clients. When a mail client connects, the server authenticates the username and password. If the username and password are valid then the server transfers messages from a user's **`inbox`** directory to the mail client program.

The server logs transactions if the Logging options are set. The service is multi-threaded. This means that multiple clients can pickup their mail at the same time.

The POP3 Service implements RFCs 1734, 1939, and 2095. Refer to **`http://www.rfc-editor.org`** for a complete list of RFCs.

The following POP3 commands are supported:

```
USER name
PASS string
APOP string
AUTH
STAT
LIST [msg]
RETR msg
DELE msg
NOOP
RSET
TOP msg n
UIDL [msg]
QUIT
```

IMAP4 Server

The IMAP4 server implements the Internet Mail Access Protocol version 4 standard. The IMAP4 protocol provides a rich interface for managing mail in a mailbox on a remote server.

The IMAP4 server provides an alternate way for mail users to logon and read their e-mail. It provides all of the capabilities of the POP3 service, with some major enhancements.

The IMAP4 protocol makes it possible for mail users to leave their messages on the server and organize them into folders.

This is very useful for people that use more than one computer to read their mail. Using the IMAP protocol, they can walk up to any computer that has an IMAP client installed, can log onto their mailbox and read their e-mail.

The IMAP4 Service implements RFCs 2060, 2086, 2095. Refer to **`http://www.rfc-editor.org`** for a complete list of RFCs.

LDAP3 Server

The LDAP3 server implements the Lightweight Directory Access Protocol version 3 standard. The LDAP3 protocol allows e-mail clients to search for names and addresses of users on the server.

Users search the LDAP3 server by creating a new directory service account in their e-mail client and submitting a query from the address book.

HTTP Management Server

The HTTP server provides a way for MailSite users to configure their mailbox properties through any Web browser.

When a user connects with a Web browser, a Login form is displayed. If the user enters a valid username and password then the Mailbox Properties form will be displayed. This form allows the user to change his mailbox properties, such as the AutoReply and Reply Message. This is useful if the user is going on vacation and wants MailSite to automatically reply to all of his incoming mail with a vacation message.

MAILMA Server

The function of the Mail Management Agent is to listen on port 106 and allow Eudora mail clients to change mailbox passwords. It also communicates with the MailSite Console to allow MailSite administration to be performed remotely over a TCP/IP connection.

The Change Password protocol is very simple, and is best documented by example. Here **S** is the server, **C** is the client:

```
S: 200 HELLO
C: USER yourloginname
S: 300 Please send your password now
C: PASS yourcurrentpassword
S: 200 Ok
C: NEWPASS yournewpassword
S: 200 Ok
C: QUIT
S: 200 Bye-bye\r\n
S: <closes connection>
C: <closes connection>
```

Working Directories

This section describes how MailSite uses directories to spool mail.

Mailbox Directory

Each MailSite user or list has a separate mailbox directory. The **Mailbox Directory** in the Domain General Page in the MailSite Console sets the mailbox directory location. The SMTP Delivery Agent delivers mail into this directory. The POP3 and IMAP4 services may remove mail from this directory under control of a e-mail client.

It is highly recommended that you store your mailboxes on an NTFS partition. During installation, the Windows user that the MailSite services run as is granted Full Control the default mailbox root directory. If you move this directory after installation, or if you create additional mailbox root directories for virtual domains, you must manually grant the MailSite user Full Control over these directories (and all subdirectories).

Mail Spool Directory

You can use the Console to specify the **Mail Spool Directory**. The spool directory contains a number of subdirectories that are used as *staging posts* for messages. On Windows NT it is recommended that the **Mail Spool Directory** is on an NTFS partition. The directory structure under the **Mail Spool Directory** is as follows.

incoming

This directory holds messages received by the SMTP Receiver. The SMTP Delivery Agent also places messages here, for example, non-delivery reports and messages which are sent to mail lists.

holding

The SMTP Delivery Agent moves messages from the **incoming** directory into this directory.

domains

When a message is moved into the **holding** directory, the SMTP Delivery Agent creates a subdirectory within the **domains** directory for each separate domain to which the message is addressed. If the message is addressed to a local user, it creates a subdirectory called **`$local$`**. In each subdirectory it stores routing information and information about the message recipients in that domain. (The message itself stays in the **`holding`** directory.)

dead

This directory collects messages which are both undeliverable and un-returnable.

lists

This directory contains subdirectories corresponding to locally stored mail lists such as text lists. For every mail list, a directory is created with the **`-request`** address for the list. List members are stored in this location. Messages themselves are moved into subdirectories under the BOX location temporarily while they are being delivered to list members.

untrusted

This directory is related to the .NET services, and so can be used by both the ExpressPro and ActiveSync web services. Whether this directory is used is controlled by the web.config file. In that file there is the following property:

```
<outboundConfiguration trusted=”true”/>
```

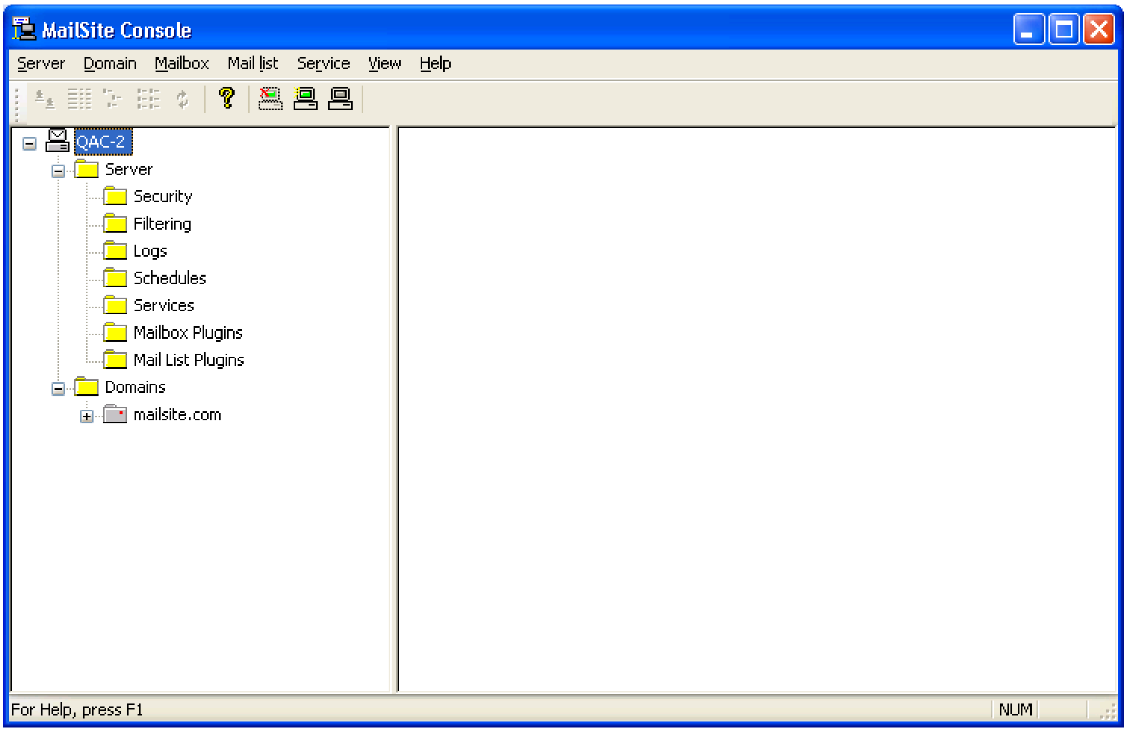
This property determines whether mails create by ExpressPro or ActiveSync will be created in the untrusted folder rather than the incoming folder. Mails which SMTPDA picks up from the untrusted folder will be relayed to the Smtpda\UntrustedRelayHost, which defaults to 127.0.0.1. Therefore, mail sent through the untrusted folder will be subject to the usual SMTPRA security checks.

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

When you start the Windows Console it displays a list of registered MailSite computers. Select the MailSite server that you wish to administer by double-clicking on the name of the server in the tree view, or selecting the **`Register New Mail Server`** button and entering the computer name.



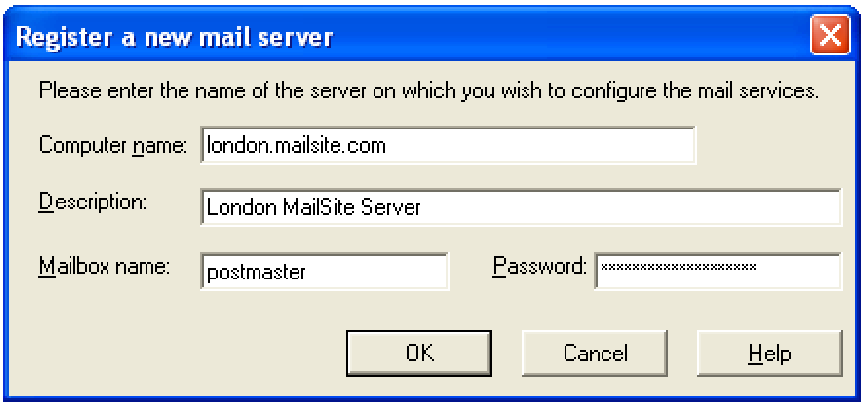
Initially, the left-hand pane contains only one icon, representing the computer on which you have just installed MailSite, and on which you are running the Windows Console. Click on the **`[+]`** symbol to the left of the icon to see the items that you can configure on the server.

If you have not yet entered a valid License Key for MailSite, you will see only a **`License Key`** icon, which you should double-click to allow you to enter your License Key (see later in this chapter). Otherwise, you will see folders labeled **`Server`** and **`Domains`**. Click on the **`[+]`** symbol to the left of the folder icons to expand the tree further.

You may double-click on the configuration icons (some of which are within their own folders) to configure that particular feature.

Registering a New Server

To register a new server, select **`Register`** from the Server menu (or use the corresponding toolbar button, or right-click on an existing server icon and select **`Register`** from the popup menu). This will display the following form:



Register a new mail server

Please enter the name of the server on which you wish to configure the mail services.

Computer name: london.mailsite.com

Description: London MailSite Server

Mailbox name: postmaster

Password: ********************

You can repeat this process for all MailSite servers on your network. Server registration information is maintained on a per-user basis, so that if you log on to computer under a different name, you will have to register the servers again.

`Computer Name`

Enter the name of the target system here. You must specify the system name by its **`host.domain`** name or IP address.

`Description`

You may also enter a description for the computer, which will appear beside the computer name in the Windows Console.

`Mailbox Name & Password`

Enter the name and password of a mailbox on the target server that has server-level access. If this user and password is not valid on the target computer, or if the permissions are not sufficient, then the connection will fail.

De-registering a Server

De-registering a server is also very straightforward, using the same techniques. Note that de-registering a server does not mean that the server's configuration information is lost—it simply means that the Console cannot access it until you re-register the server.

Editing a Server

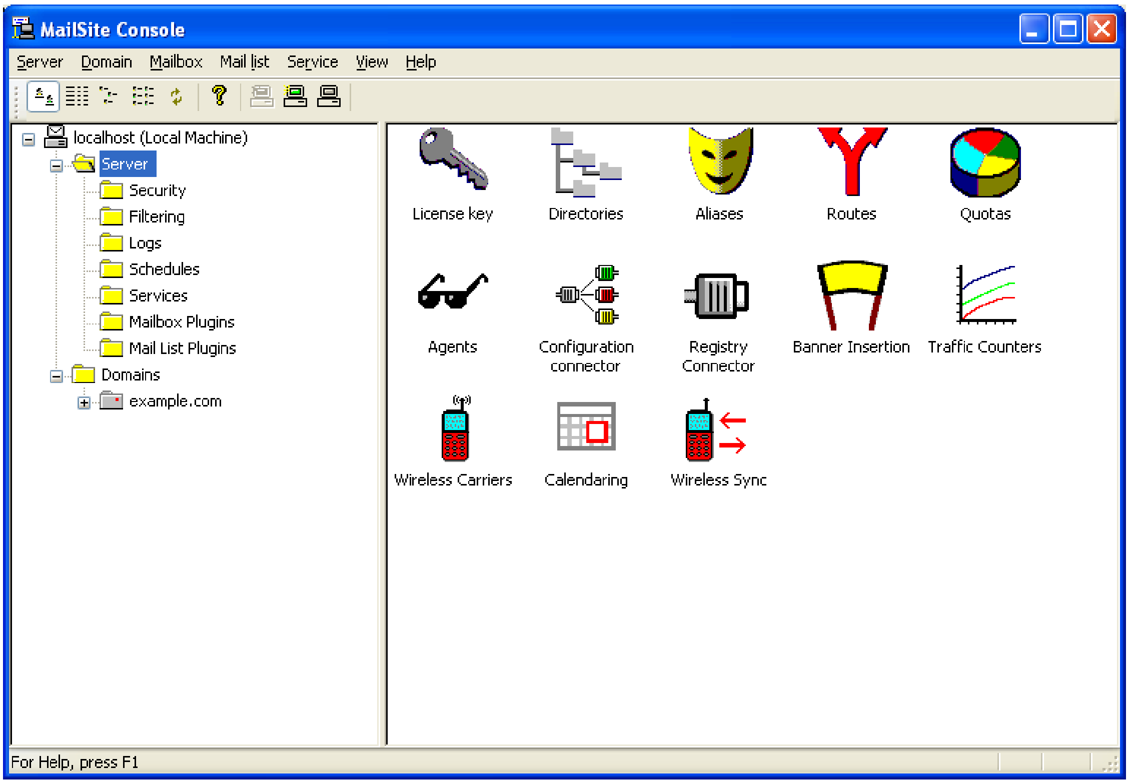
You can change the server comment using the Edit command from the Server menu (or the popup menu).

Disconnecting from a Server

If you have connected to a registered server (for instance, if you have expanded the server icon by clicking on the **`[+]`** symbol to its left), you may disconnect by selecting **`Disconnect`** from the Server menu. This can be useful if the server you are administering goes down—in this case you should disconnect from it and then reconnect after it has been rebooted.

Server

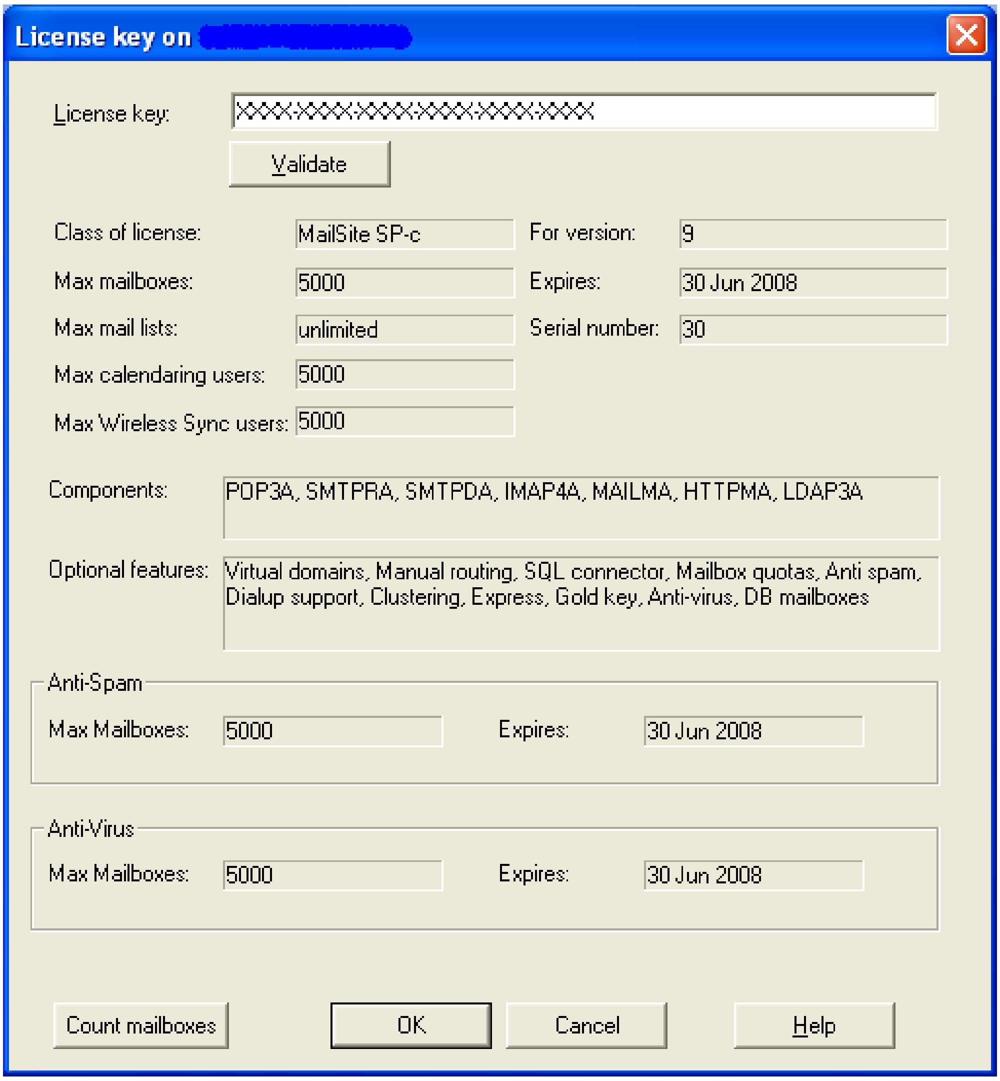
Under each server shown in the list of MailSite systems on the left side of the MailSite Console are two folders: **Server** and **Domains**. The Server folder contains icons corresponding to the many options that can be configured for the MailSite Engine.



The following sections contain complete information on all of the items in the **Server** folder and its sub-folders.

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:



License key on [redacted]

License key: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX

Class of license: MailSite SP-c

For version: 9

Max mailboxes: 5000

Expires: 30 Jun 2008

Max mail lists: unlimited

Serial number: 30

Max calendaring users: 5000

Max Wireless Sync users: 5000

Components: POP3A, SMTPRA, SMTPDA, IMAP4A, MAILMA, HTTPMA, LDAP3A

Optional features: Virtual domains, Manual routing, SQL connector, Mailbox quotas, Anti spam, Dialup support, Clustering, Express, Gold key, Anti-virus, DB mailboxes

Anti-Spam

Max Mailboxes: 5000

Expires: 30 Jun 2008

Anti-Virus

Max Mailboxes: 5000

Expires: 30 Jun 2008

The License Key unlocks MailSite features. If you are using an evaluation key, then your license will expire in 30 days. If you are using a purchased key, then the license will not expire.

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.

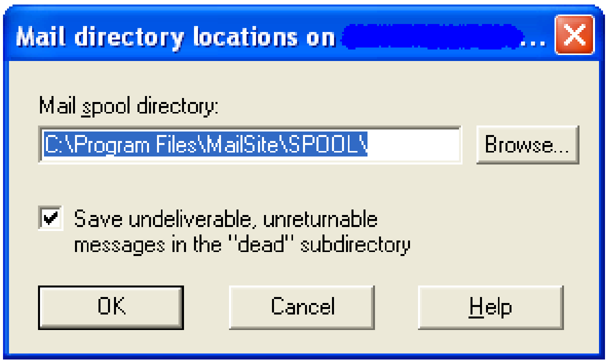
⇒ Any optional features which you are licensed to use.

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.



Mail directory locations on [redacted]...

Mail spool directory: C:\Program Files\MailSite\SPOOL\

☑ Save undeliverable, unreturnable messages in the "dead" subdirectory

`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`**.

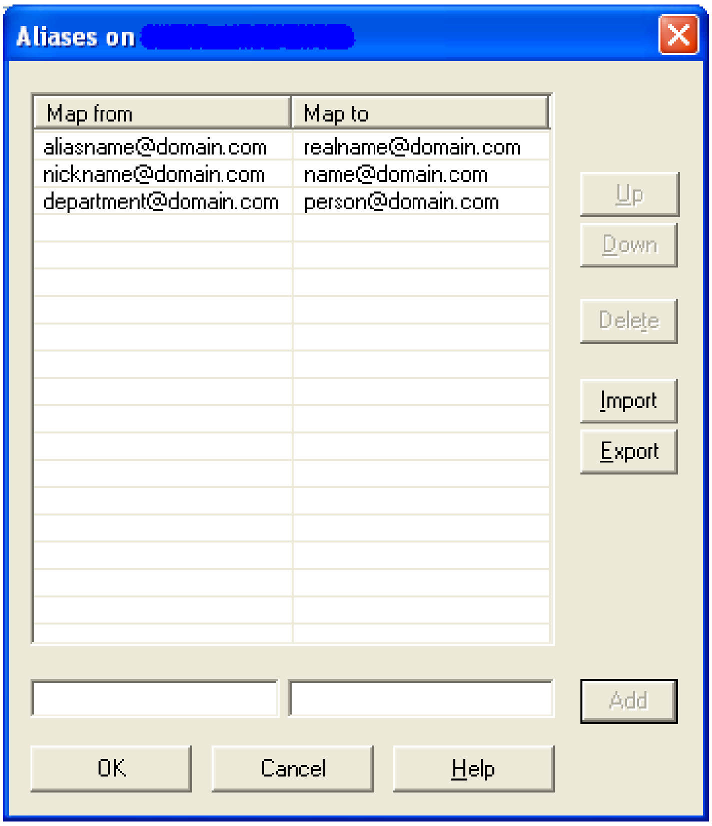
To configure the location where the mail server will store messages for local mailboxes, see the section on Domains later in this chapter.

`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:



Map from	Map to
aliasname@domain.com	realname@domain.com
nickname@domain.com	name@domain.com
department@domain.com	person@domain.com

You can configure MailSite to redirect incoming messages using **Aliases**. When the server receives a message and the **To**: address matches an entry in this **alias table**, then the mail is redirected.

Adding Aliases

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

Modifying Aliases

To modify an alias, select it in the list. Enter the new **Map From** and **Map To** entries and click on the **Modify** button.

Deleting Aliases

To delete one or more aliases, select them using the **Shift** and **Ctrl** keys then click the **Delete** button.

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
krg: keving
kev*: keving
kg: keving
gg: gregg
greg*: gregg
greg: gregg
```

Export Aliases

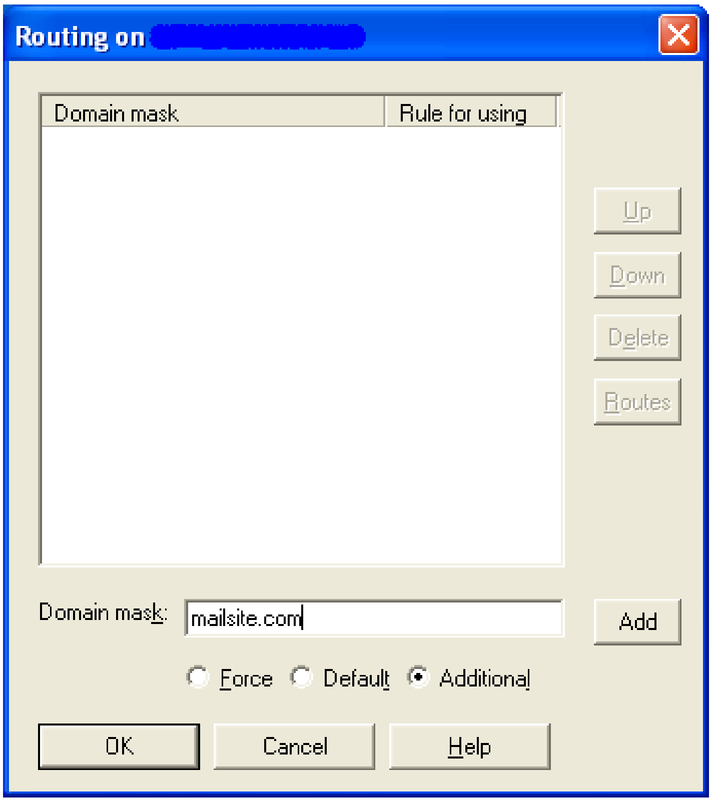
The **Export** button allows you to export aliases to a text file. This button displays the **Save As** file dialog.

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
krg: keving
kev*: keving
kg: keving
gg: gregg
greg*: gregg
greg: gregg
```

Routes

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



Routing on [redacted]

Domain mask	Rule for using

Domain mask: mailsite.com

○ Force ○ Default ● Additional

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:

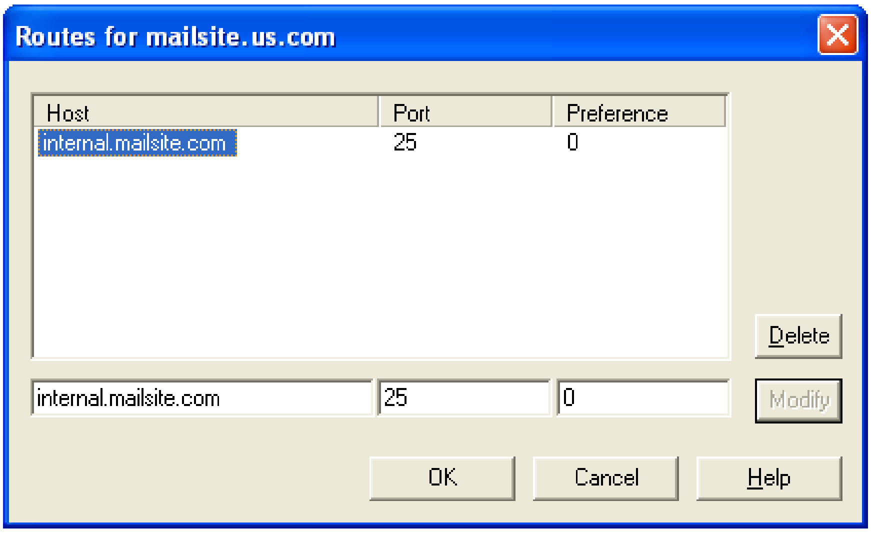
⇒ **`Force:`** The manual route overrides any routes in the DNS records

⇒ **`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.


Routes for mailsite.us.com

Host	Port	Preference
internal.mailsite.com	25	0

internal.mailsite.com | 25 | 0

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.

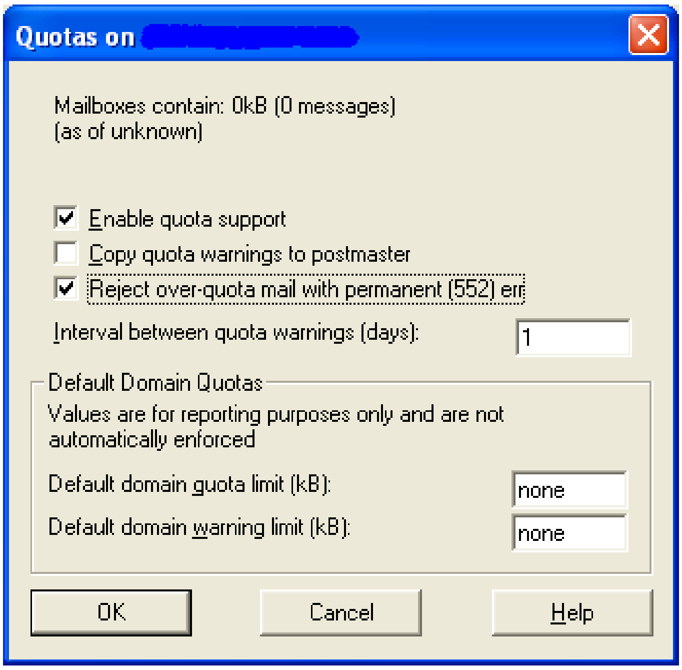
Preference

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:



Quotas on [redacted]

Mailboxes contain: 0kB (0 messages)
(as of unknown)

☑ Enable quota support
□ Copy quota warnings to postmaster
☑ Reject over-quota mail with permanent (552) err

Interval between quota warnings (days): 1

Default Domain Quotas
Values are for reporting purposes only and are not automatically enforced

Default domain quota limit (kB): none
Default domain warning limit (kB): none

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)`

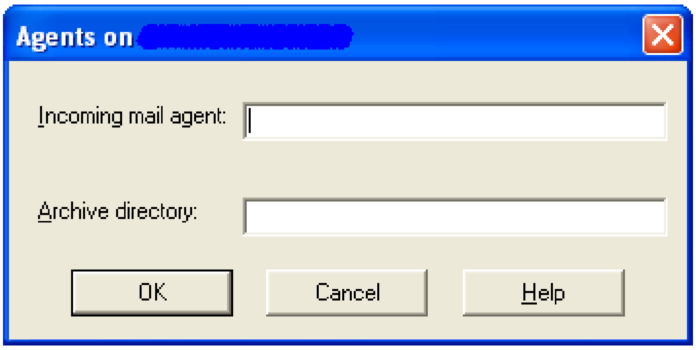
If quota limits are not set for each individual domain, this default value will apply. Quotas for the total size of a domain are not enforced, but can be entered here to assist with administration and as the basis of database queries.

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:



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.

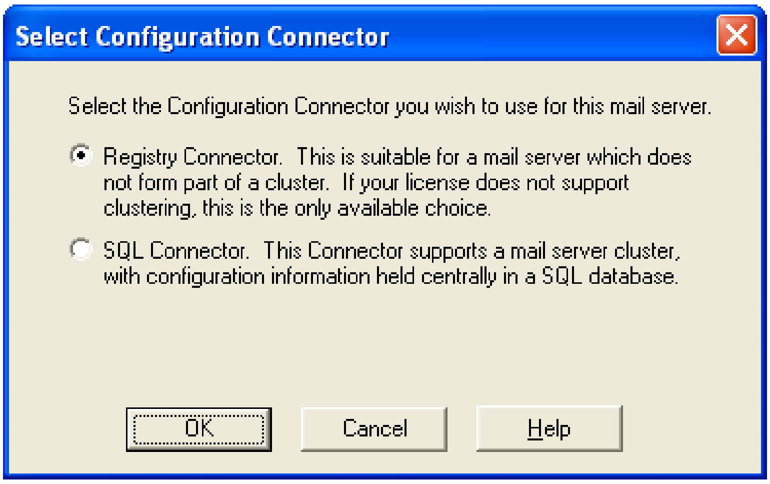
It is possible for the Server Agent to delete or move the message file and recipients files – for instance if the agent determines that the message contains a virus. In this case, the agent should respect the wishes of the sender regarding delivery status notifications, as expressed in the recipients 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

The Configuration Connector controls the method that MailSite uses to store its configuration and mailbox data. Your license may not allow you to configure this option.



Select Configuration Connector

Select the Configuration Connector you wish to use for this mail server.

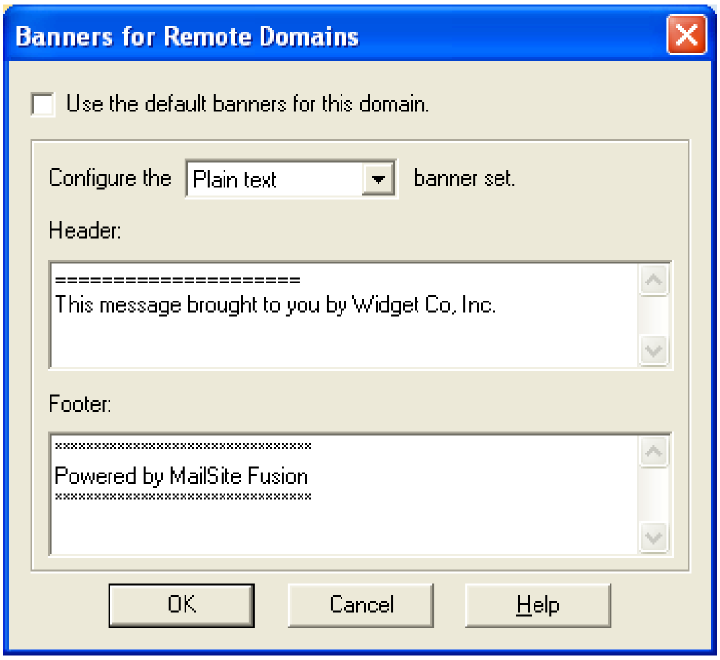
● Registry Connector. This is suitable for a mail server which does not form part of a cluster. If your license does not support clustering, this is the only available choice.

○ SQL Connector. This Connector supports a mail server cluster, with configuration information held centrally in a SQL database.

By default, MailSite is installed using the Registry Connector, which stores all configuration data in the Windows registry. Meanwhile, the SQL Connector stores all of its data in a SQL database, which allows you to create a cluster of MailSite nodes. To convert MailSite to database storage, select **SQL Connector** and click **OK**, which will launch the SQL Connector wizard and/or the Migration Wizard. Refer to the section on the SQL Connector for more information.

Banner Insertion

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



Banners for Remote Domains

□ Use the default banners for this domain.

Configure the Plain text banner set.

Header:

```
=====================
This message brought to you by Widget Co, Inc.
```

Footer:

```
**********************************
Powered by MailSite Fusion
**********************************
```

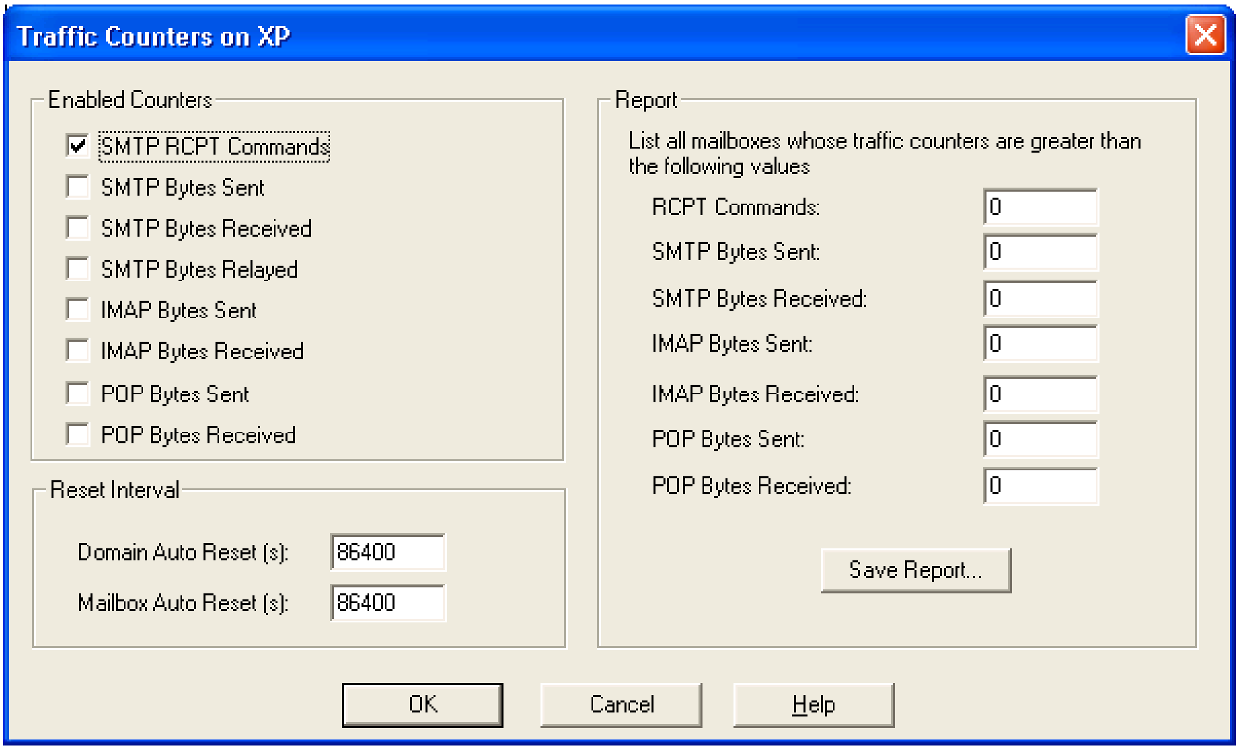
Banners can be defined at the domain level and the server level. Domain-level banners are added to all messages sent from that domain, while server-level banners can be added to all mail sent from remote domains (that is, domains not defined in MailSite).

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.



Enabled Counters

- ☑ SMTP RCPT Commands
- □ SMTP Bytes Sent
- □ SMTP Bytes Received
- □ SMTP Bytes Relayed
- □ IMAP Bytes Sent
- □ IMAP Bytes Received
- □ POP Bytes Sent
- □ POP Bytes Received

Reset Interval

Domain Auto Reset (s): 86400

Mailbox Auto Reset (s): 86400

Report

List all mailboxes whose traffic counters are greater than the following values

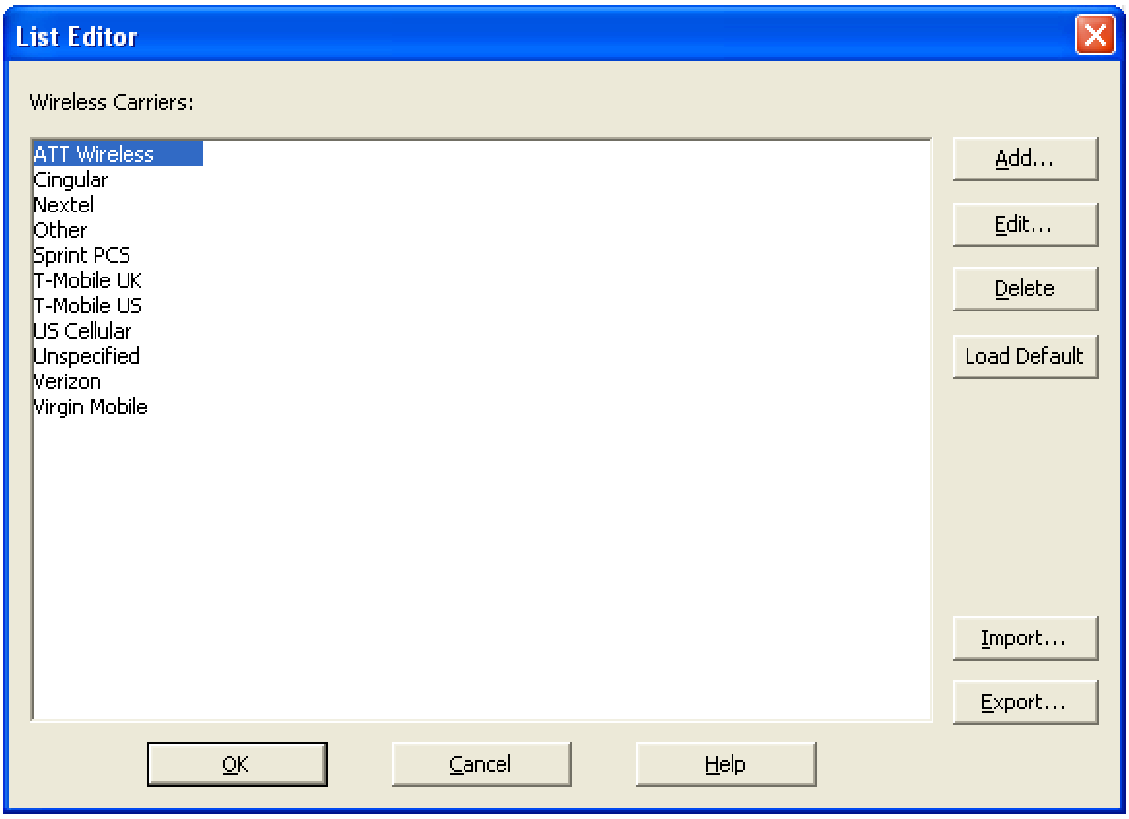
RCPT Commands:	0
SMTP Bytes Sent:	0
SMTP Bytes Received:	0
IMAP Bytes Sent:	0
IMAP Bytes Received:	0
POP Bytes Sent:	0
POP Bytes Received:	0

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.



Wireless Carriers:

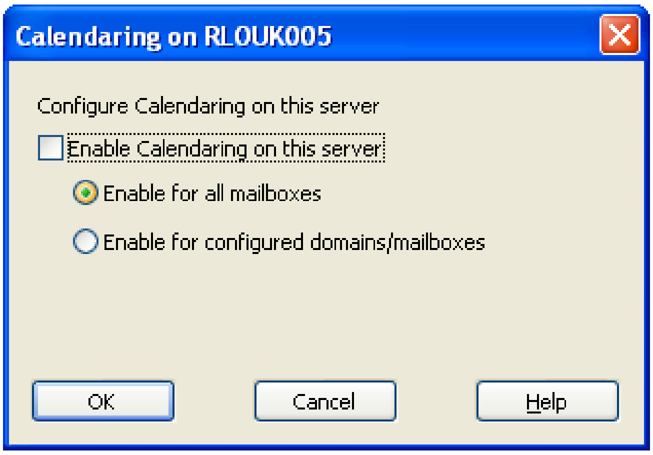
- ATT Wireless
- Cingular
- Nextel
- Other
- Sprint PCS
- T-Mobile UK
- T-Mobile US
- US Cellular
- Unspecified
- Verizon
- Virgin Mobile

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.



Configure Calendaring on this server

□ Enable Calendaring on this server

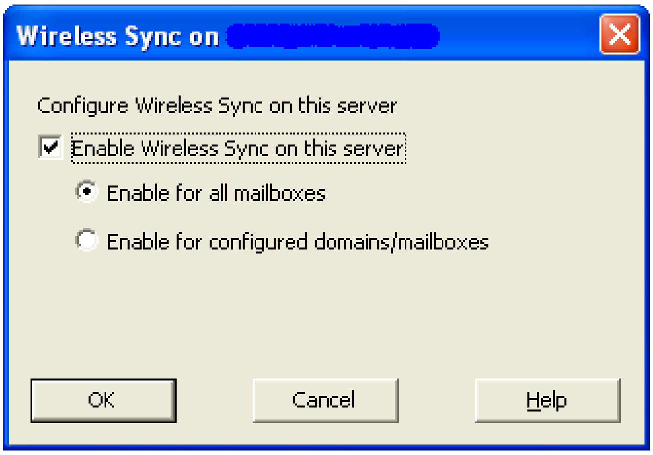
● Enable for all mailboxes

○ Enable for configured domains/mailboxes

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.



Wireless Sync on [redacted]

Configure Wireless Sync on this server

☑ Enable Wireless Sync on this server

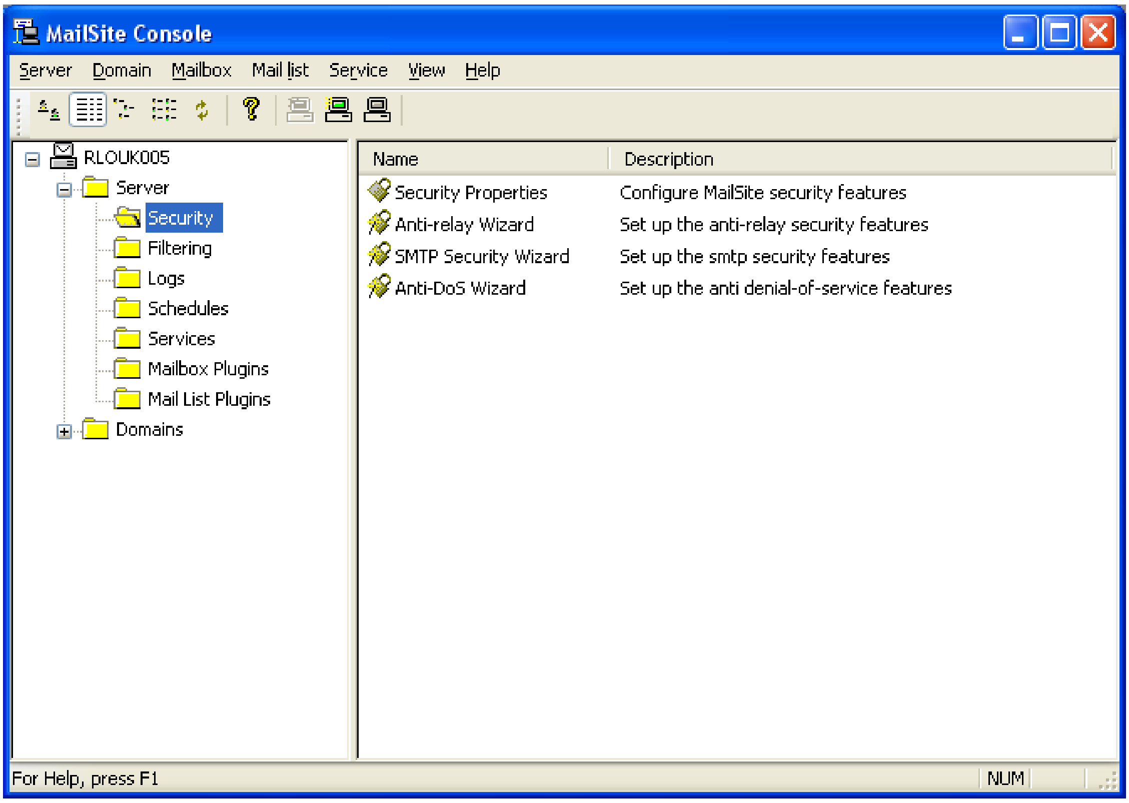
● Enable for all mailboxes

○ Enable for configured domains/mailboxes

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:

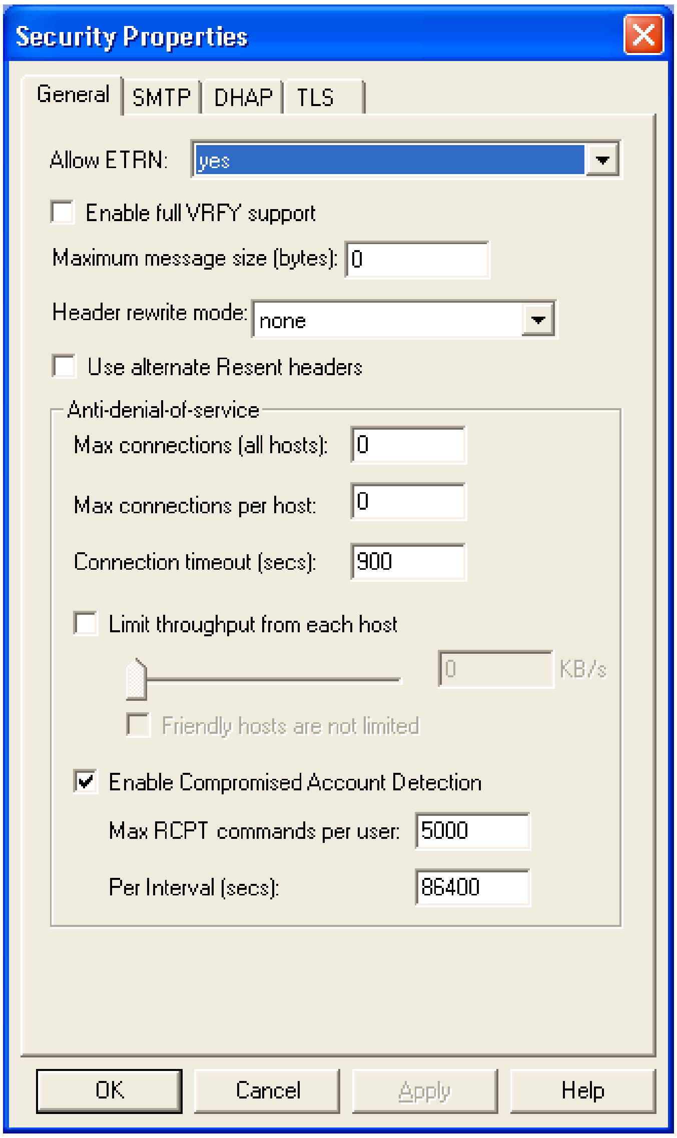


Name	Description
Security Properties	Configure MailSite security features
Anti-relay Wizard	Set up the anti-relay security features
SMTP Security Wizard	Set up the smtp security features
Anti-DoS Wizard	Set up the anti denial-of-service features

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:



Allow ETRN: yes

☐ Enable full VRFY support

Maximum message size (bytes): 0

Header rewrite mode: none

☐ Use alternate Resent headers

Anti-denial-of-service

Max connections (all hosts): 0

Max connections per host: 0

Connection timeout (secs): 900

☐ Limit throughput from each host

0 KB/s

☐ Friendly hosts are not limited

☑ Enable Compromised Account Detection

Max RCPT commands per user: 5000

Per Interval (secs): 86400

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

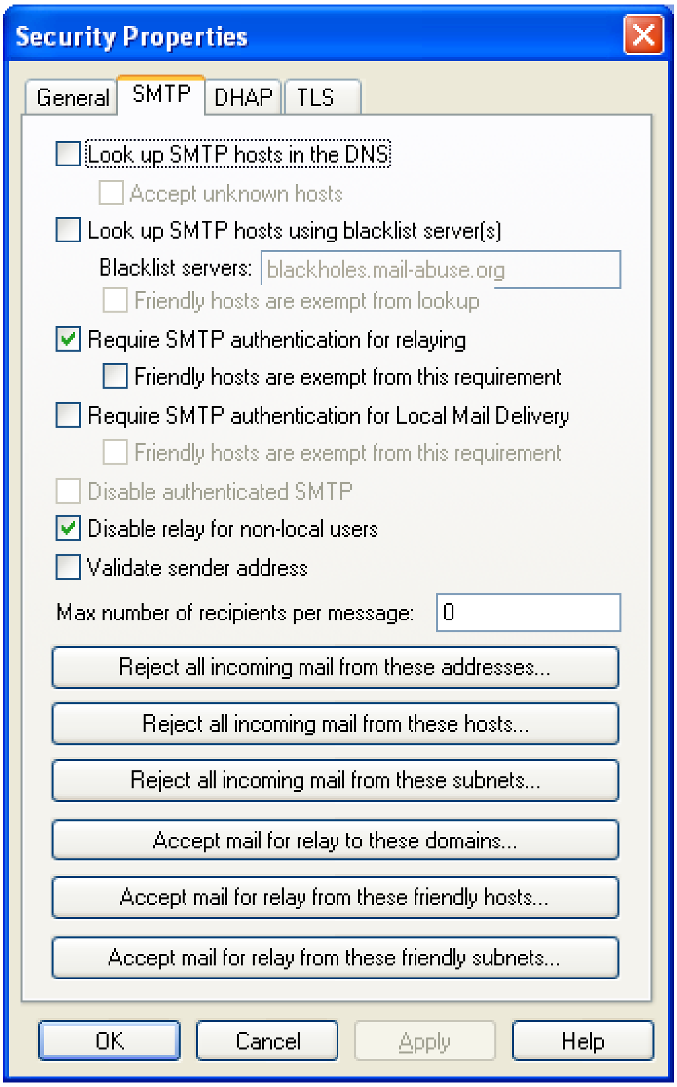
This option provides a throttle on the amount of data (in kilobytes per second) that SMTPRA will accept from any one host. This allows you to control DoS attacks that send large amounts of data over relatively few connections. When using this option it is recommended that you exempt your “friendly” hosts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



☐ Look up SMTP hosts in the DNS

☐ Accept unknown hosts

☐ Look up SMTP hosts using blacklist server(s)

Blacklist servers: blackholes.mail-abuse.org

☐ Friendly hosts are exempt from lookup

☑ Require SMTP authentication for relaying

☐ Friendly hosts are exempt from this requirement

☐ Require SMTP authentication for Local Mail Delivery

☐ Friendly hosts are exempt from this requirement

☐ Disable authenticated SMTP

☑ Disable relay for non-local users

☐ Validate sender address

Max number of recipients per message: 0

Reject all incoming mail from these addresses...
Reject all incoming mail from these hosts...
Reject all incoming mail from these subnets...
Accept mail for relay to these domains...
Accept mail for relay from these friendly hosts...
Accept mail for relay from these friendly subnets...
OK
Cancel
Apply
Help

`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`

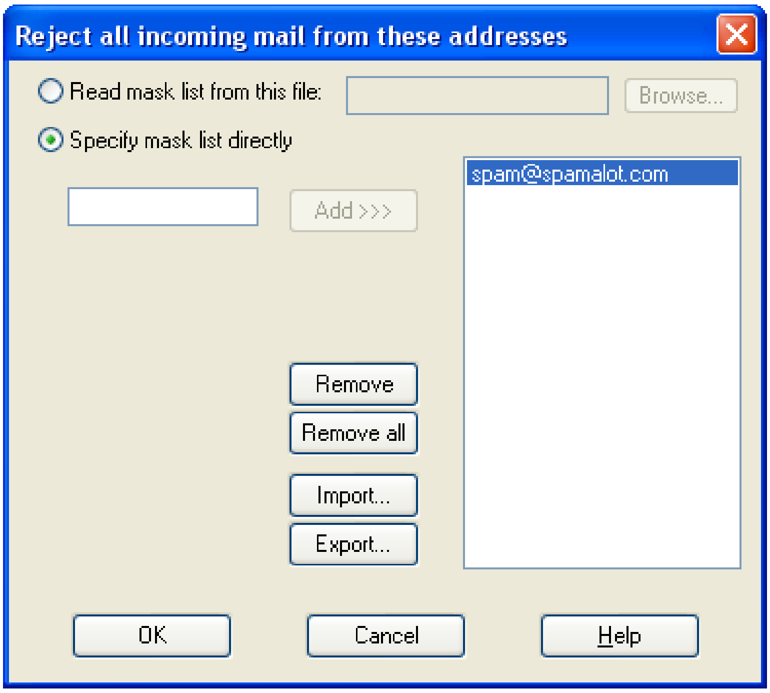
You can specify the maximum number of recipients allowed for an individual message. These are the recipients specified on the SMTP envelope (that is, given by the **`RCPT TO:`** command). If you specify 0, there is no maximum.

`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:


Reject all incoming mail from these addresses
○ Read mask list from this file:
Browse...
● Specify mask list directly
Add >>>
Remove
Remove all
Import...
Export...
OK
Cancel
Help

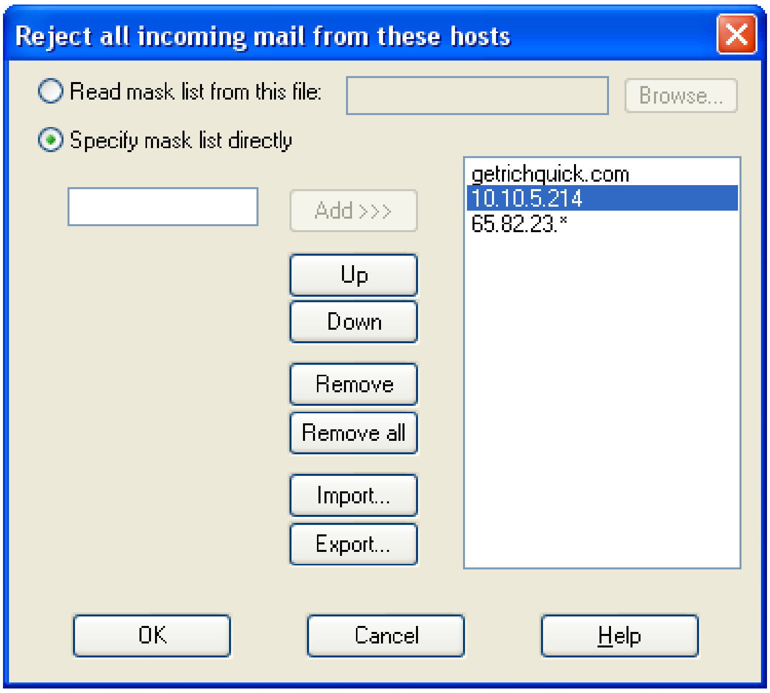
spam@spamalot.com

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:



Reject all incoming mail from these hosts

○ Read mask list from this file:

● Specify mask list directly

getrichquick.com
10.10.5.214
65.82.23.*

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

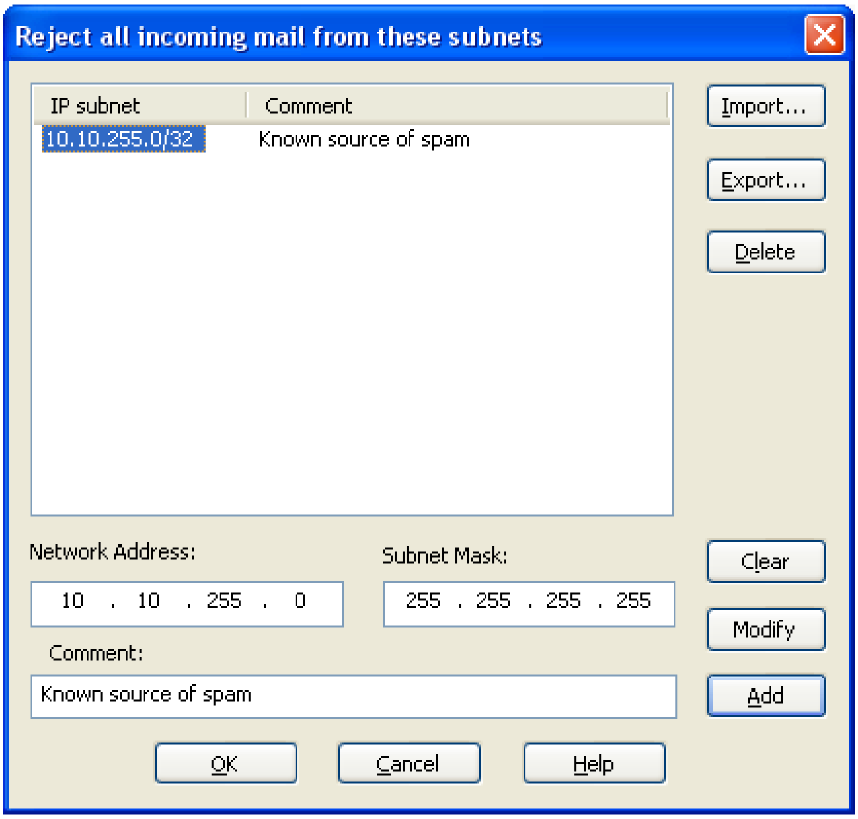
If you specify host names as opposed to IP addresses, you must check **Look up SMTP hosts In The DNS** so that MailSite can determine the host name.

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:



Reject all incoming mail from these subnets

IP subnet	Comment
10.10.255.0/32	Known source of spam

Network Address: 10 . 10 . 255 . 0

Subnet Mask: 255 . 255 . 255 . 255

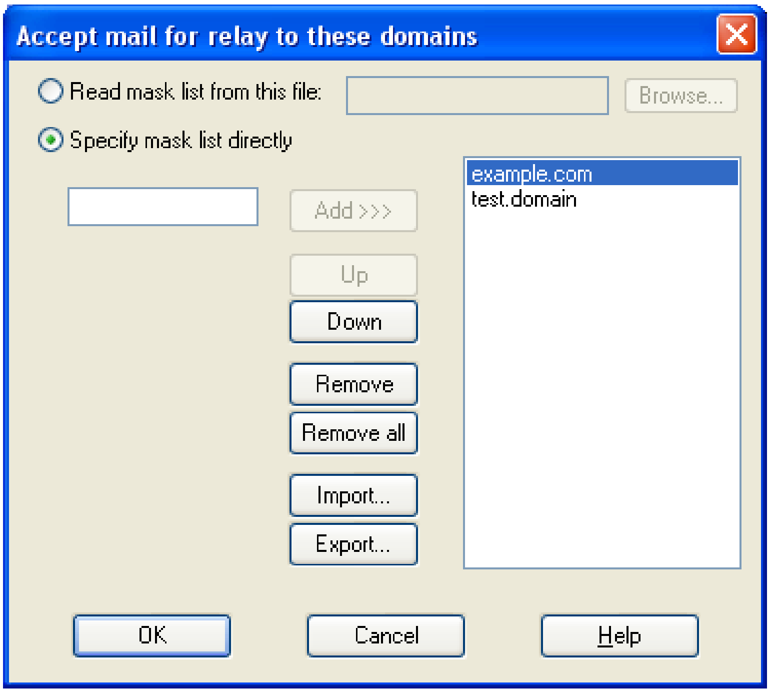
Comment: Known source of spam

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:



Accept mail for relay to these domains
○ Read mask list from this file:
Browse...
● Specify mask list directly
Add >>>
Up
Down
Remove
Remove all
Import...
Export...
OK
Cancel
Help

example.com
test.domain

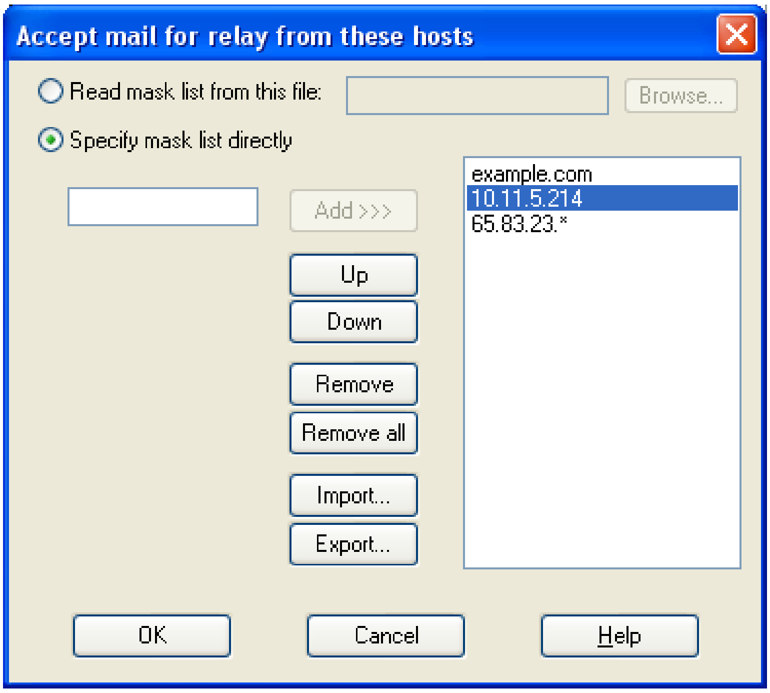
This feature is useful if your server acts as a secondary SMTP relay host for some other domains. In this case you would enter a list of all of the relay domains in this field.

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:



Accept mail for relay from these hosts

○ Read mask list from this file:

● Specify mask list directly

example.com
10.11.5.214
65.83.23.*

Use this form to enter a list of host names or IP addresses that are permitted to relay mail through this server. The default entry is **`*`**, meaning all hosts can relay mail through this server.

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.

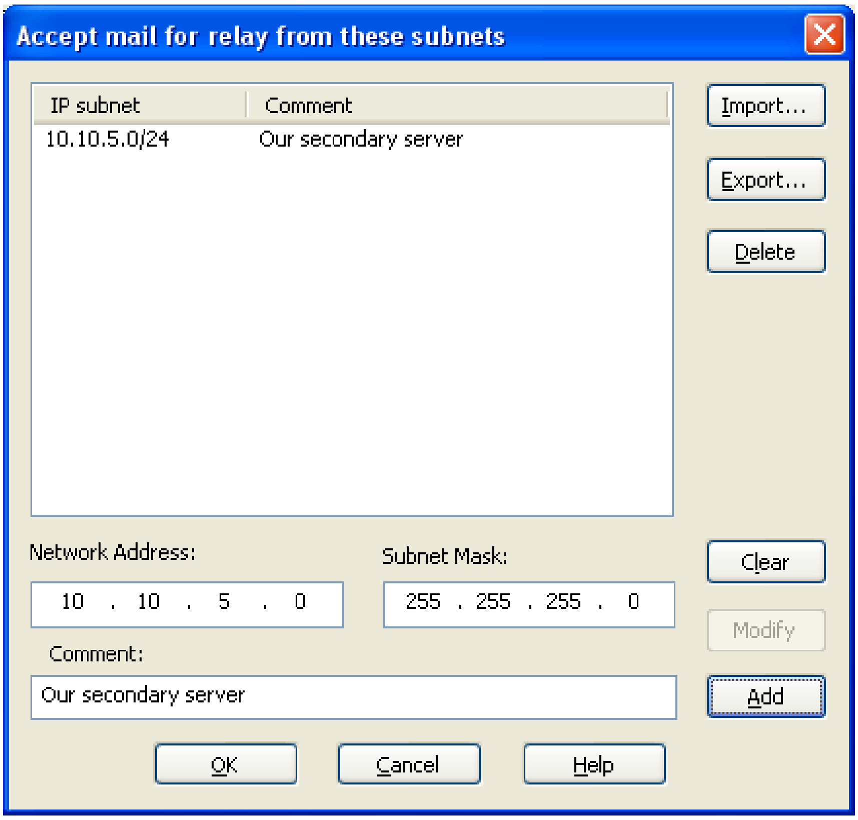
WARNING! It is very easy to block valid messages with this feature. Be careful to make correct entries. Test your settings by sending e-mail from a variety of client machines.

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:



Accept mail for relay from these subnets

IP subnet	Comment
10.10.5.0/24	Our secondary server

Network Address: 10 . 10 . 5 . 0

Subnet Mask: 255 . 255 . 255 . 0

Comment: Our secondary server

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.

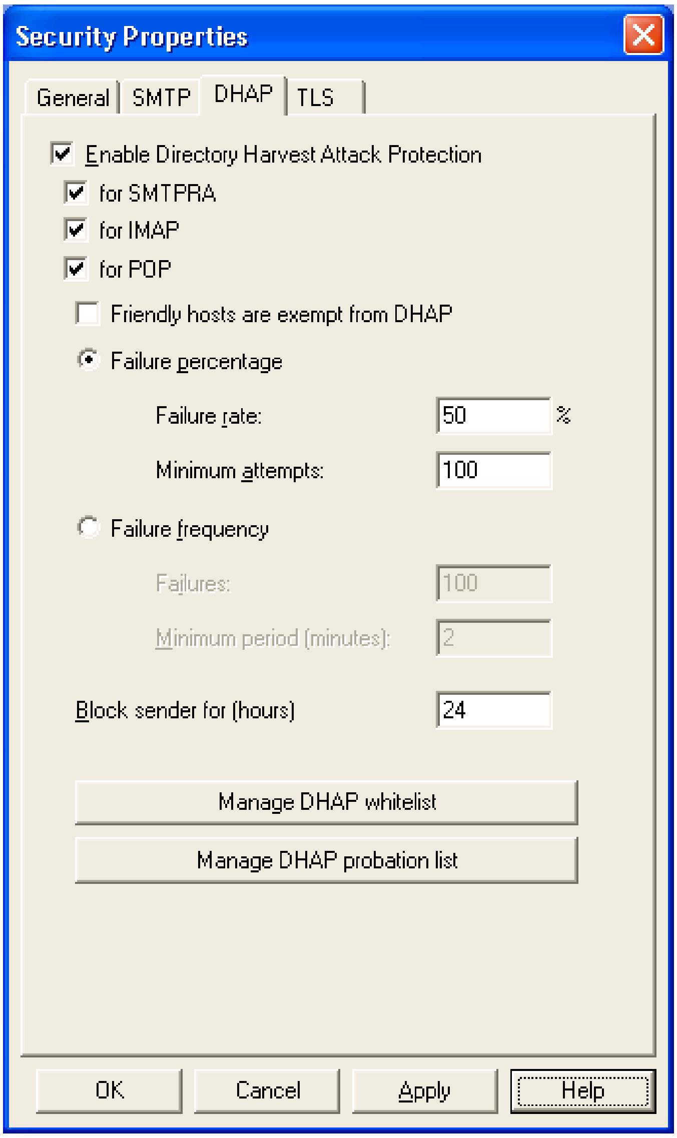
What you are allowed to put in the mask list depends on which button you clicked:

Mask list	**Contains**	**! (Negation marker)**
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.



☑ Enable Directory Harvest Attack Protection
☑ for SMTPRA
☑ for IMAP
☑ for POP
□ Friendly hosts are exempt from DHAP
● Failure percentage
Failure rate: 50 %
Minimum attempts: 100
○ Failure frequency
Failures: 100
Minimum period (minutes): 2
Block sender for (hours) 24

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

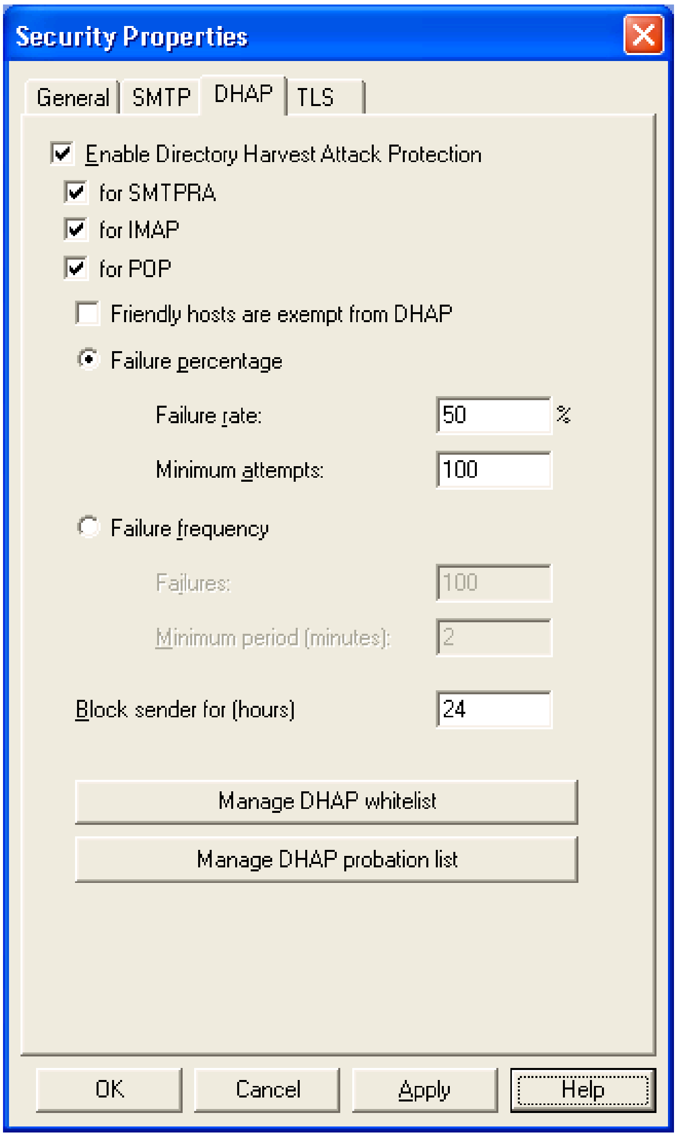
If you wish to disable DHAP on a single service uncheck the box relating to that service. To fully disable DHAP uncheck the "Enable Directory Harvest Attack Protection" checkbox. This will halt the collection of any statistics on connecting hosts and allow hosts that have been deemed harvesters to reconnect.

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.



☑ Enable Directory Harvest Attack Protection
☑ for SMTPRA
☑ for IMAP
☑ for POP
□ Friendly hosts are exempt from DHAP
● Failure percentage
Failure rate: 50 %
Minimum attempts: 100
○ Failure frequency
Failures: 100
Minimum period (minutes): 2
Block sender for (hours) 24

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.

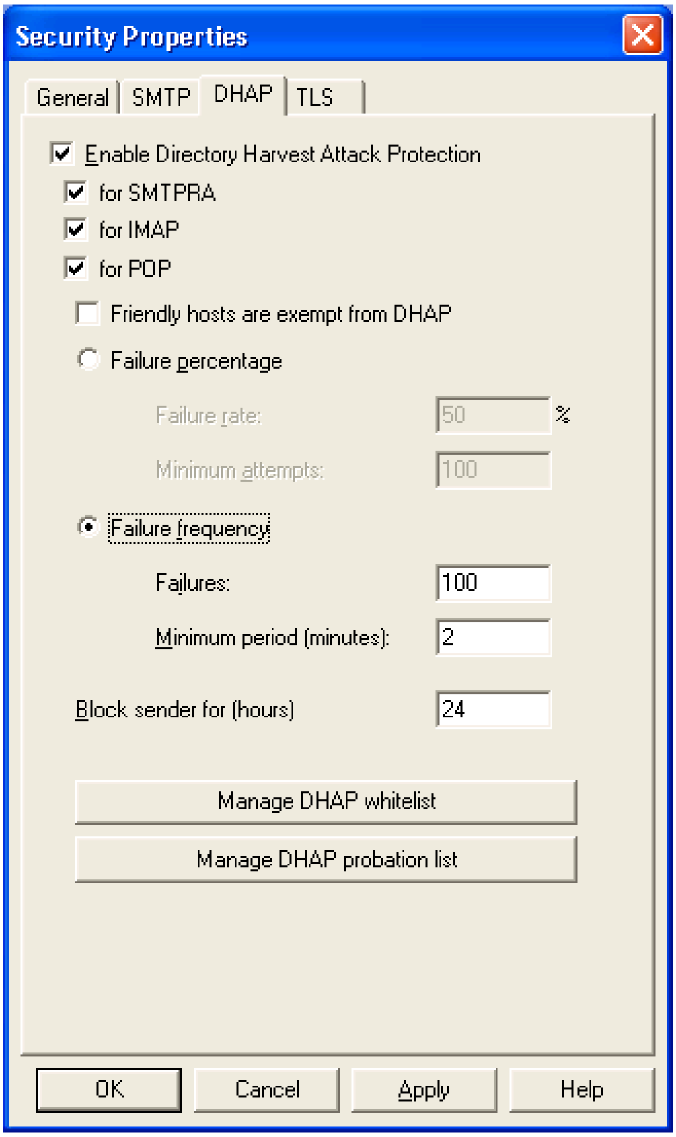
The failure rate is the percentage of non-existent email addresses with respect to the total number of email addresses attempted by a connecting host.

With the configuration above, if a connecting host attempts to sends over 50% of its mail (minimum email address sample size 100) to invalid email addresses, that host will be disconnected and blocked from reconnecting for a period of 24 hours.

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.



☑ Enable Directory Harvest Attack Protection
☑ for SMTPRA
☑ for IMAP
☑ for POP
□ Friendly hosts are exempt from DHAP
○ Failure percentage
Failure rate: 50 %
Minimum attempts: 100
● Failure frequency
Failures: 100
Minimum period (minutes): 2
Block sender for (hours) 24

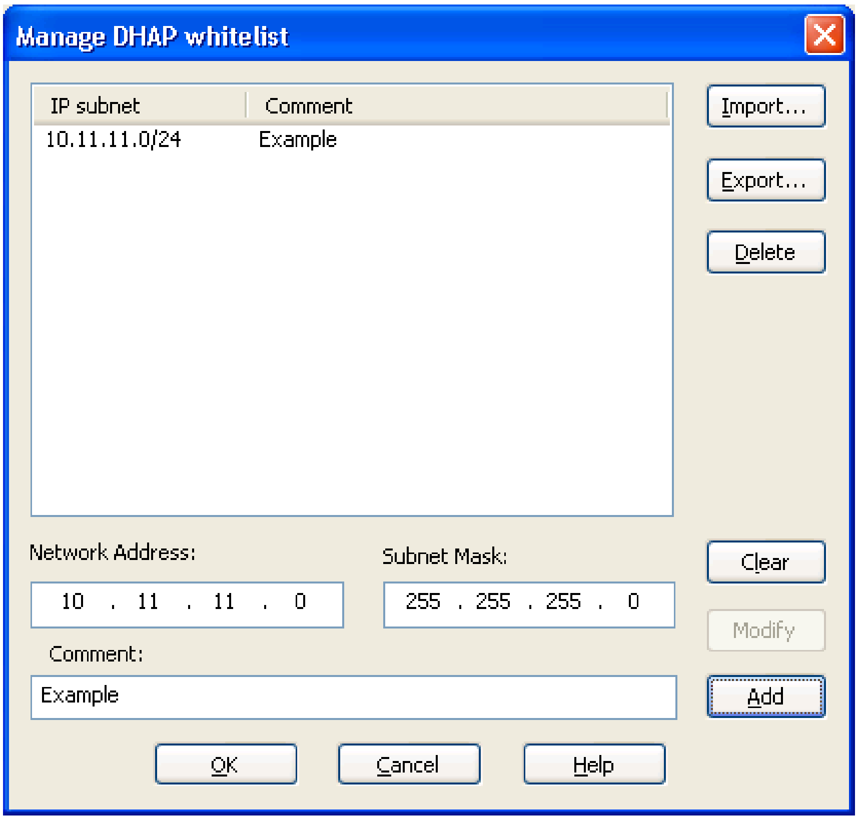
With the configuration above, if a connecting host attempts to send mail to 100 invalid email addresses within a 2-minute period of time, that host will be disconnected and blocked from reconnecting for a period of 24 hours.

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.



Manage DHAP whitelist

IP subnet	Comment
10.11.11.0/24	Example

Network Address: 10 . 11 . 11 . 0

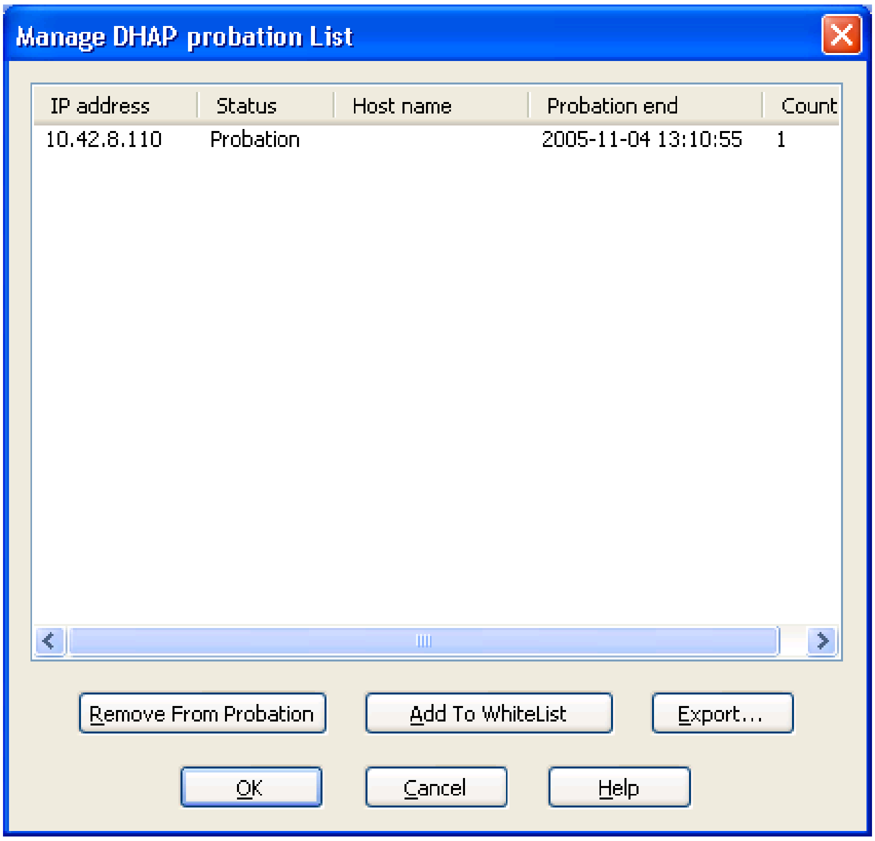
Subnet Mask: 255 . 255 . 255 . 0

Comment: Example

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.



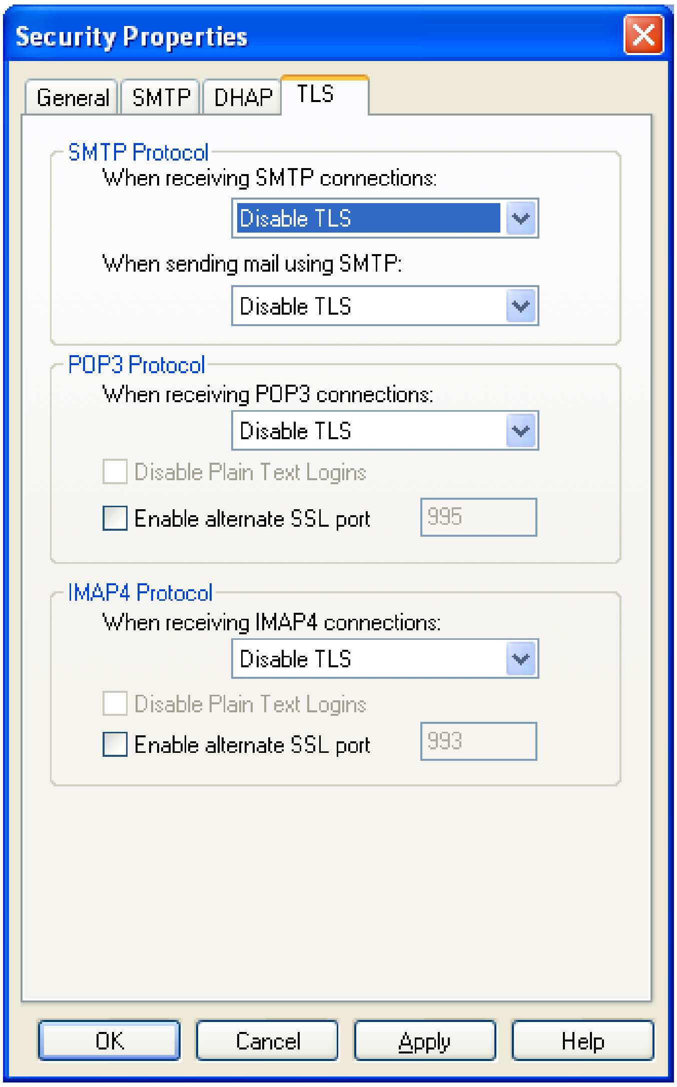
Manage DHAP probation List

IP address	Status	Host name	Probation end	Count
10.42.8.110	Probation		2005-11-04 13:10:55	1

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.



SMTP Protocol

When receiving SMTP connections: Disable TLS

When sending mail using SMTP: Disable TLS

POP3 Protocol

When receiving POP3 connections: Disable TLS

□ Disable Plain Text Logins

□ Enable alternate SSL port 995

IMAP4 Protocol

When receiving IMAP4 connections: Disable TLS

□ Disable Plain Text Logins

□ Enable alternate SSL port 993

All SSL/TLS security settings are available via the TLS tab of the Security Properties window. MailSite allows you to specify the level of TLS deployment separately for each of the three mail protocols— SMTP, POP3, and IMAP4. Each protocol has a separate area within the window. All three protocols use the same drop-down menu settings.

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:

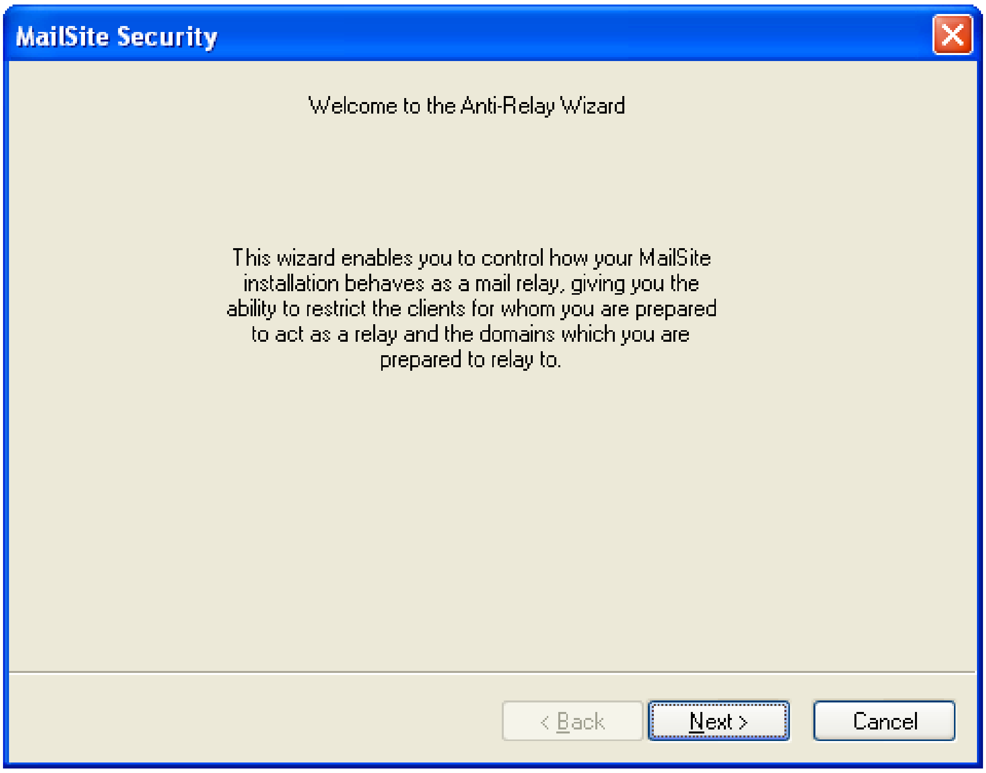
- Disable TLS — MailSite communicates in clear text mode.
- Allow TLS (default) — MailSite negotiates with the mail client and optionally encrypts messages if the client has SSL/TLS configured.
- Require TLS — MailSite forces messages to be encrypted.

Two checkboxes may also be set:

- Disable Plain Text Logins — Checking this box forces the client to encrypt login details (when both the server and client have agreed to use SSL/TLS).
- Enable alternate SSL port — Checking this box supports the use of an alternate secure port (this feature is required when the client software supports SSL 3.0 but not TLS 1.0). The alternate port number must be entered in the adjacent text box.

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.



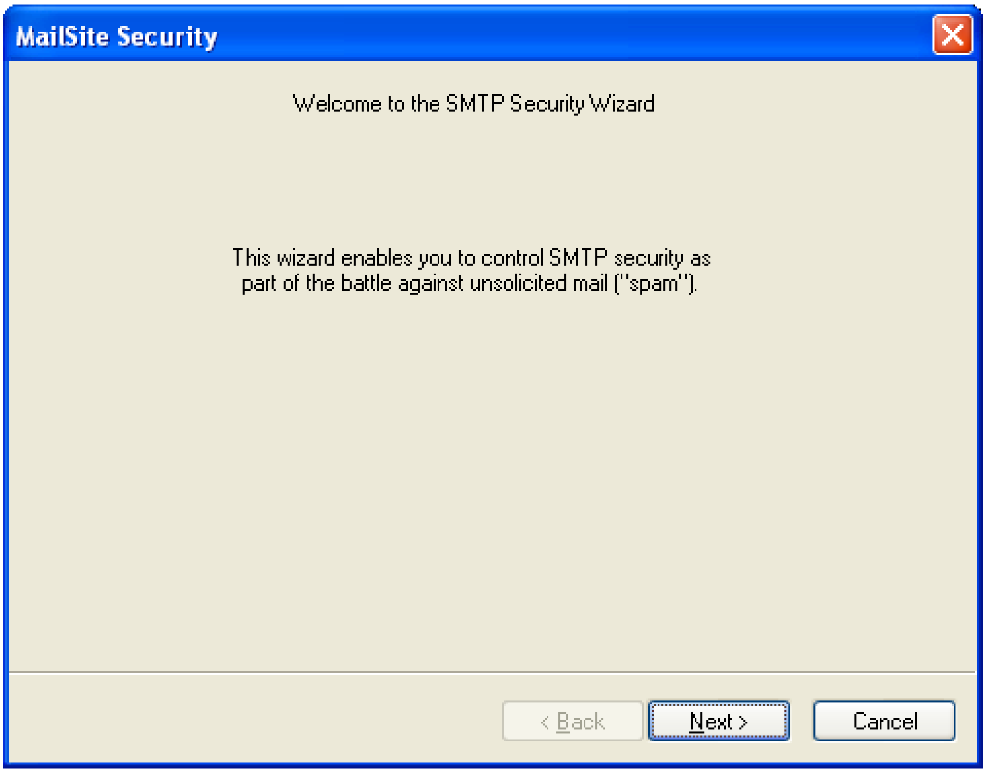
Welcome to the Anti-Relay Wizard

This wizard enables you to control how your MailSite installation behaves as a mail relay, giving you the ability to restrict the clients for whom you are prepared to act as a relay and the domains which you are prepared to relay to.

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.



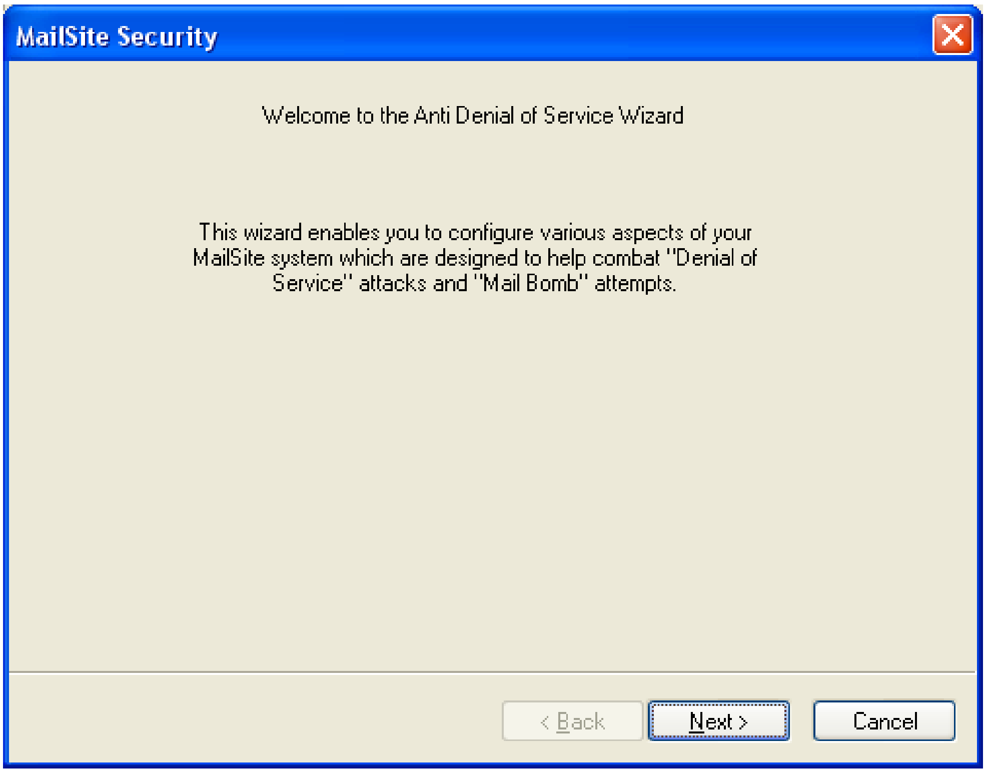
MailSite Security

Welcome to the SMTP Security Wizard

This wizard enables you to control SMTP security as part of the battle against unsolicited mail ("spam").

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.



MailSite Security

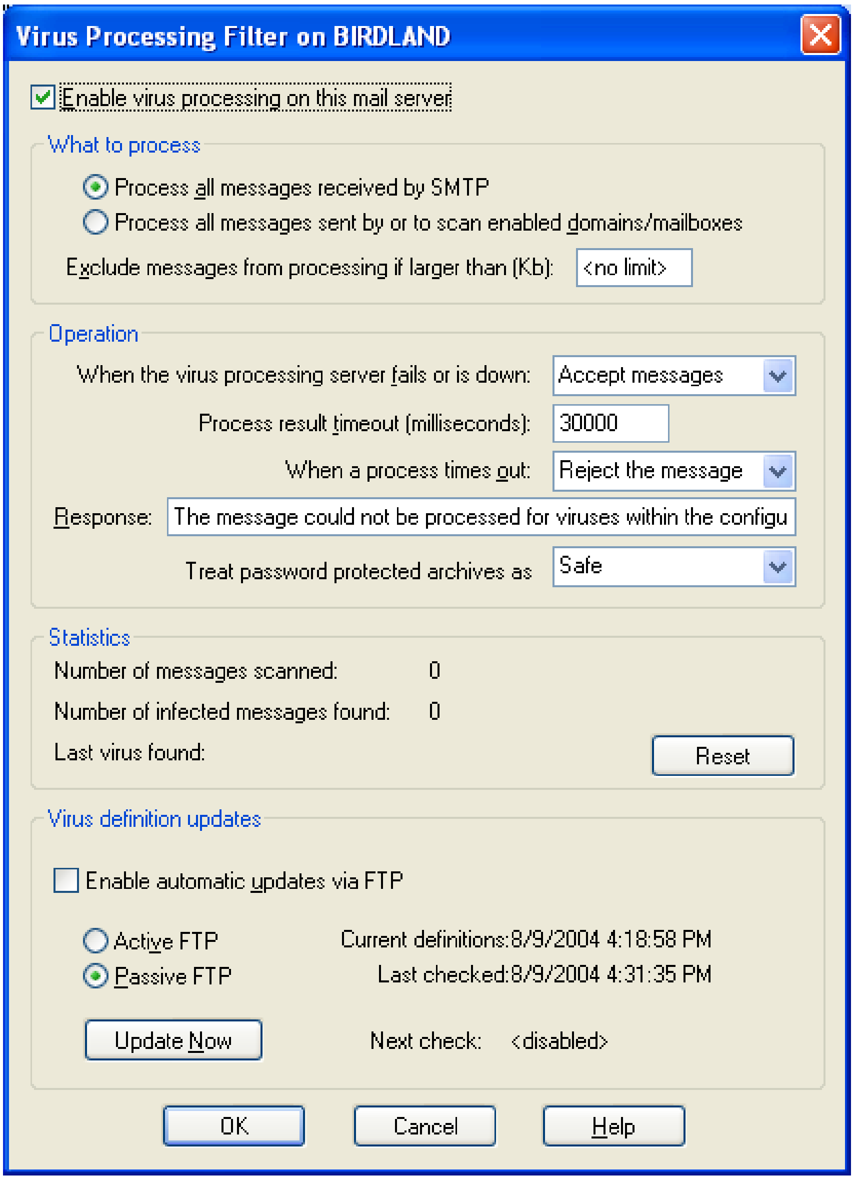
Welcome to the Anti Denial of Service Wizard

This wizard enables you to configure various aspects of your MailSite system which are designed to help combat "Denial of Service" attacks and "Mail Bomb" attempts.

Filtering

AVG Anti-Virus Filter

This dialog provides options for the AVG virus-scanning component.



Virus Processing Filter on BIRDLAND

☑ Enable virus processing on this mail server

What to process

● Process all messages received by SMTP
○ Process all messages sent by or to scan enabled domains/mailboxes

Exclude messages from processing if larger than (Kb): <no limit>

Operation

When the virus processing server fails or is down: Accept messages

Process result timeout (milliseconds): 30000

When a process times out: Reject the message

Response: The message could not be processed for viruses within the configu

Treat password protected archives as Safe

Statistics

Number of messages scanned: 0

Number of infected messages found: 0

Last virus found:

Virus definition updates

□ Enable automatic updates via FTP

○ Active FTP
● Passive FTP

Current definitions:8/9/2004 4:18:58 PM

Last checked:8/9/2004 4:31:35 PM

Next check: <disabled>

Enable virus processing on this mail server

This option controls how MailSite scans mail for viruses. When this option is enabled, mail received by MailSite's SMTP server will be scanned for viruses depending on the MailSite's various virus scanning options. If disabled, virus scanning is never used for incoming messages.

Process all messages received by SMTP

This option causes all mail received by MailSite's SMTP server to be scanned for viruses regardless of sender or destination.

Process all messages sent by or to scan enabled mailboxes/domains

This option causes mail to be scanned based on the virus scanning preferences of the sender or recipient domains on your site.

Exclude messages from processing if larger than (Kb)

Specifies the maximum size of message which will be scanned for viruses. It is advised to leave this property with no limit as many viruses are sent as attachments and so the mails will be relatively large.

When the virus processing server fails or is down

If the virus filter is not running or is too busy to accept new connections, this option determines MailSite’s behavior when receiving new messages. By default, if the virus filter is not available, all messages are accepted without being scanned for viruses. If you select **Defer all messages**, MailSite will block all incoming messages with a temporary (4xx) error, which causes the sending SMTP server to queue the message for later delivery.

Process result timeout (milliseconds)

A very small number of messages are so large, or so complex, that the virus scanning engine is unable to scan them. To avoid this slowing the entire mail server, MailSite is able to stop the scanning process after a configurable period.

When a process times out

If the virus scanning engine has taken too long attempting to scan the message, MailSite will take the action specified here. If MailSite is configured to reject mails which time out, the **Response** will be used to notify the sender why their message is being rejected.

Treatment password protected archives as

Some viruses are transmitted using password protected archives which are encrypted and can not be scanned by MailSite. MailSite will reject these messages if you select **Unsafe** and accept the messages if you select **Safe**.

Statistics

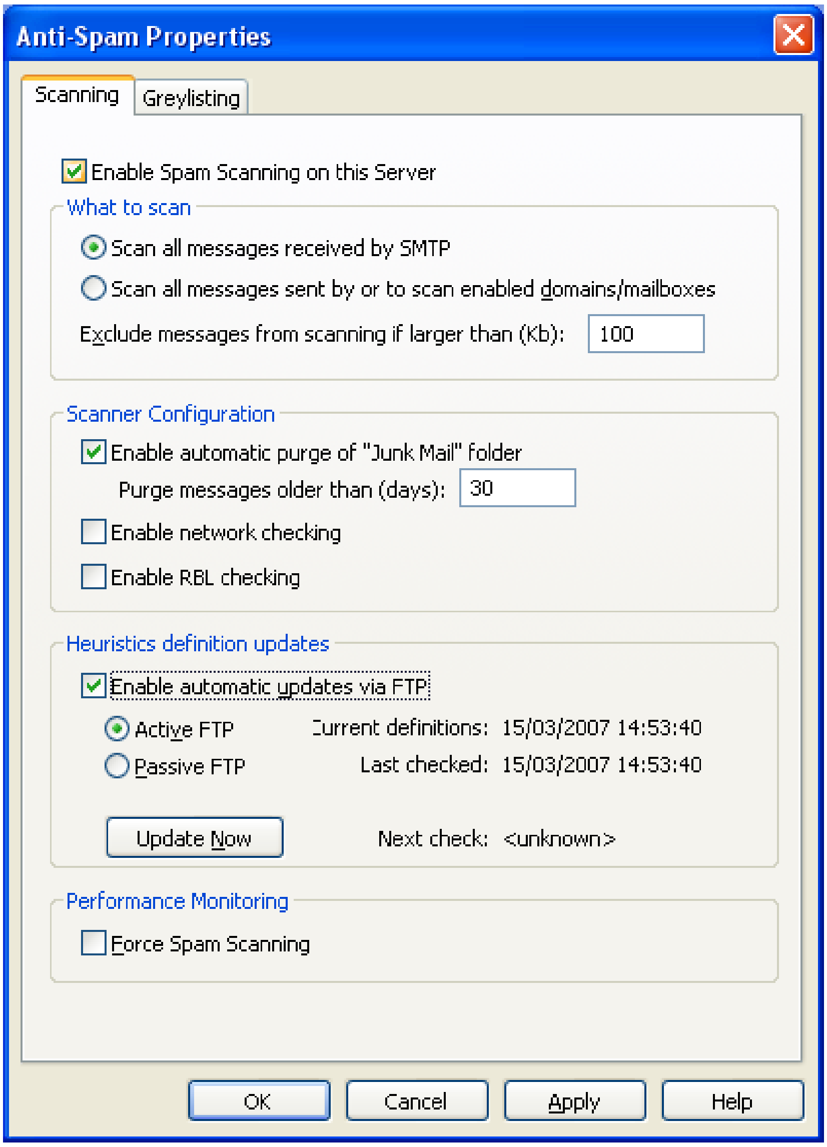
The statistics shown here will be updated if Virus Scanning is enabled on the server. The figures give an indication of the number of viruses attempting to pass through the server as well as the name of the last virus found.

Virus definition updates

This option specifies whether MailSite should periodically poll for updated virus definitions. This allows MailSite to automatically download definitions for new viruses as they are released. By default, MailSite polls once an hour for updates to virus definition files. You can force an immediate update by clicking **Update now**. Your license may not support virus updates.

Mailshell Anti-Spam Filter (Scanning Tab)

This dialog provides options for the anti-spam filter including greylisting settings.



☑ Enable Spam Scanning on this Server

What to scan

● Scan all messages received by SMTP

○ Scan all messages sent by or to scan enabled domains/mailboxes

Exclude messages from scanning if larger than (Kb): 100

Scanner Configuration

☑ Enable automatic purge of "Junk Mail" folder

Purge messages older than (days): 30

□ Enable network checking

□ Enable RBL checking

Heuristics definition updates

☑ Enable automatic updates via FTP

● Active FTP Current definitions: 15/03/2007 14:53:40

○ Passive FTP Last checked: 15/03/2007 14:53:40

Next check: <unknown>

Performance Monitoring

□ Force Spam Scanning

The option **Enable Spam Scanning on this Server** controls the global spam scanning policy. If this option is not selected, MailSite will not scan any messages. Otherwise, MailSite will scan messages according to the other settings here.

Note: *Upon entering this dialog the following test will be performed. If there are more mailboxes provisioned for Anti-Spam then there are licenses for, this option will be unchecked. Upon exiting the dialog another test for this same condition is done. If the licensed amount of mailboxes has been exceeded, then the user will be notified that this option will be turned off.*

If you want to protect all users on your site from spam and scan every incoming message, select **Process all messages received by SMTP**. When this option is selected, all mail received by MailSite's SMTP server will be scanned for spam regardless of sender or destination.

Note: *If there are more mailboxes in the server than there are Anti-Spam licenses for, this option will be disabled.*

If you want to instead use domain or mailbox-level spam scanning, select **Process all messages sent by or to enabled mailboxes/domains**. When this option is selected, MailSite will scan mail based on the spam scanning preferences of the sender or recipient domains on your site.

By default, MailSite will not scan messages of over 100KB for spam. Unsolicited mails are typically very small, but this value can be changed if required.

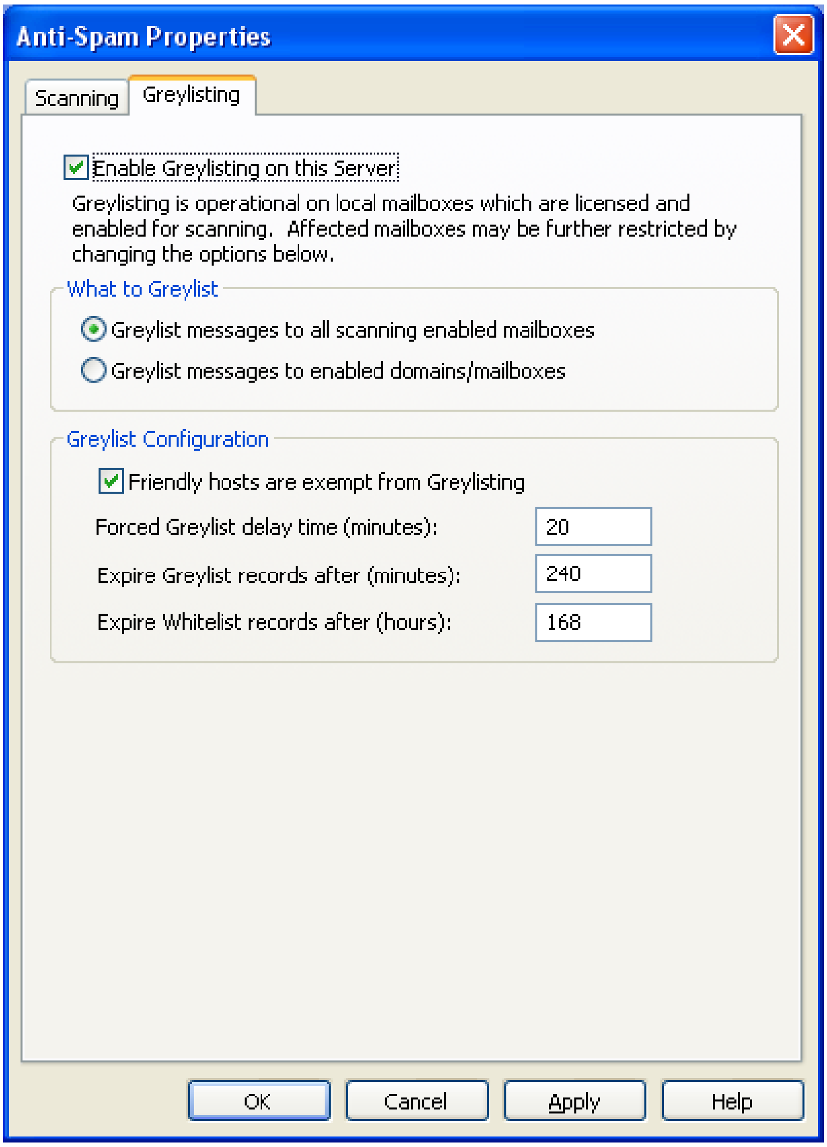
Included in the Spam Scanning Filter window are controls for downloading updated anti-spam files, which are needed for MailSite to block new forms of spam as they are discovered. By default, MailSite polls once an hour for updates to anti-spam files. You can force an immediate update by clicking **Update now**.

The option **Enable automatic purge of "Junk Mail" folder** determines whether MailSite purges old messages at the end of a POP or IMAP session. The number of days after which a message is considered old is configurable in the text box below.

The options **Enable network checking** and **Enable RBL checking** control functionality in the Anti-Spam engine. These are provided in addition to the existing MailSite security DNS and RBL features. If these options are selected, spam scoring will be more accurate at the expense of increased network traffic and slower processing.

Spam scanning can be forced on. This allows an administrator to monitor the level of spam passing through the system even if the license does not allow scanning. No actions can be taken to control the spam without an appropriate license.

Mailshell Anti-Spam Filter (Greylisting Tab)



Anti-Spam Properties

☑ Enable Greylisting on this Server

Greylisting is operational on local mailboxes which are licensed and enabled for scanning. Affected mailboxes may be further restricted by changing the options below.

What to Greylist

● Greylist messages to all scanning enabled mailboxes

○ Greylist messages to enabled domains/mailboxes

Greylist Configuration

☑ Friendly hosts are exempt from Greylisting

Forced Greylist delay time (minutes): 20

Expire Greylist records after (minutes): 240

Expire Whitelist records after (hours): 168

The option **Enable Greylisting on this Server** controls the global greylisting policy. If this option is not selected, MailSite will not utilize greylisting for any SMTP sessions. Otherwise, MailSite will enforce greylisting according to the other settings here.

Note: *Greylisting is a technique designed to reduce the problem of spam. Greylisting is therefore an anti-spam option and is not available for mailboxes which are not provisioned for anti-spam filtering.*

If you want to protect all users on your site from spam using greylisting, select **Greylist messages to all scanning enabled mailboxes**. When this option is selected, all mail received by MailSite's SMTP server will be subject to greylisting checks subject to the other settings here.

If you only want greylisting to apply to specific mailboxes or domains, select **Greylist messages to enabled domains/mailboxes**.

The option **Friendly hosts are exempt from Greylisting** indicates that those known IP addresses, typically local machines, will not be checked.

Forced Greylist delay time indicates the number of minutes for which a remote host will not be able to successfully resubmit a mail. A greater delay time increases the cost to the potential spammer, and increases the chance that they will be known as such. An increased time also delays delivery of legitimate mail to recipients, which may be unacceptable.

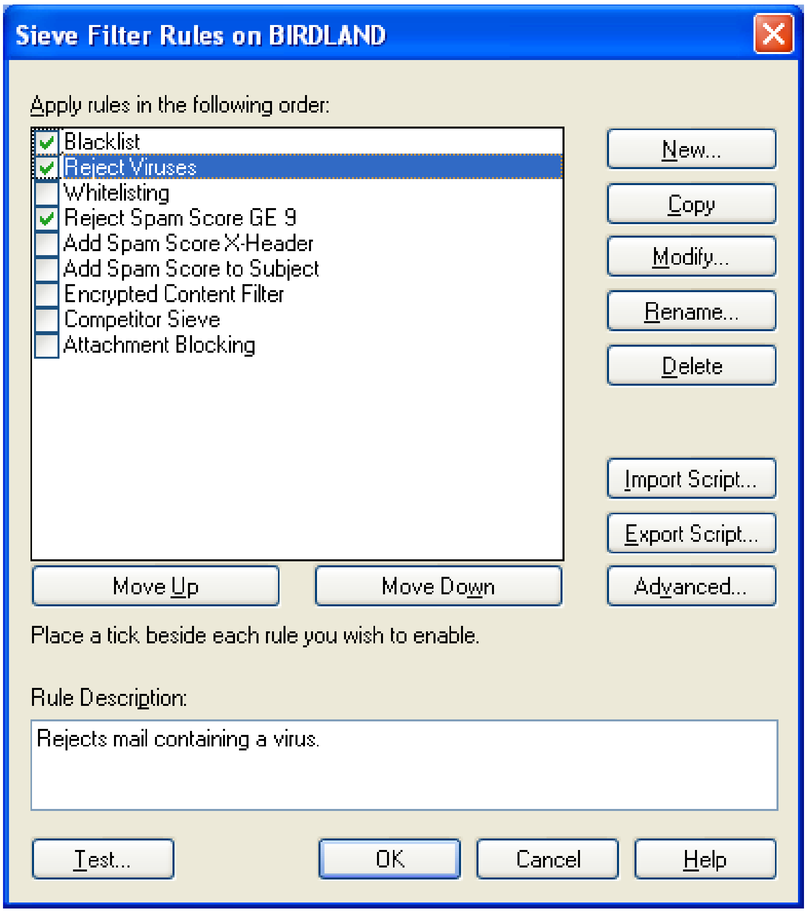
__Note__: *This determines the time after which MailSite will accept a resubmitted mail. The actual retry interval is determined by the sending server and may be much longer.*

Expire Greylist records after indicates how long the system will wait for the retry. A well configured mail server will retry at gradually increasing intervals, but there is no fixed period for retries. This setting should be high enough to cover all legitimate servers which send mail to the system.

Expire Whitelist records after indicates how long "passing" the greylist check should be valid for. The higher the period, the more mail which will be delivered without delay. This will be a benefit for legitimate mail. A shorter period will mean less out of date and therefore unused rows in the database.

Sieve Filter Rules

The Sieve Filter Rules window lists the content filters currently defined on your site, and allows you to add new filter rules. To open this window, double-click on the **Sieve Filter** icon in the Security folder. You can also create filter rules that apply to only a specific domain by similarly opening the **Sieve Filter** icon within the target domain's folder in the MailSite Console.



Sieve Filter Rules on BIRDLAND

Apply rules in the following order:

- ☑ Blacklist
- ☑ Reject Viruses
- □ Whitelisting
- ☑ Reject Spam Score GE 9
- □ Add Spam Score X-Header
- □ Add Spam Score to Subject
- □ Encrypted Content Filter
- □ Competitor Sieve
- □ Attachment Blocking

Place a tick beside each rule you wish to enable.

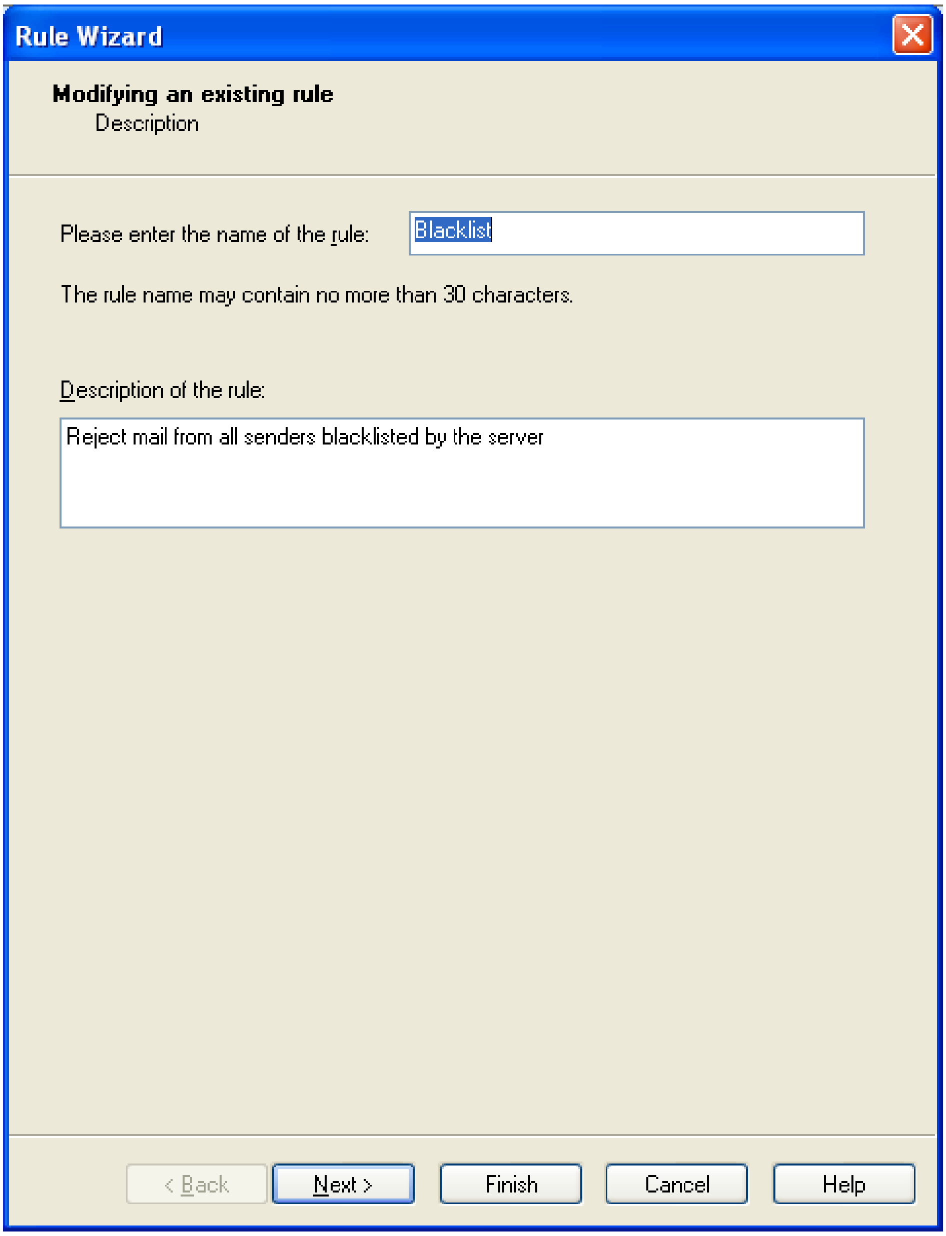
Rule Description: Rejects mail containing a virus.

The rules defined in this list are applied sequentially, so if a message is rejected by an initial filter it will not be subject to subsequent rules. You can move filters up and down in this list to refine your filtering strategies. You can also enable/disable filters by checking the box at the left of each filter rule in this list. To create a new filter rule click **New**, which launches the Rule Wizard.

To bypass the Rule Wizard and edit the Sieve script directly, click the **Advanced** button. This displays an editor window that allows you to create, modify, and delete filter rules by editing the Sieve filtering syntax.

Description

Use this panel of the Rule Wizard to enter a name and description of your new filter rule. Both the name and description of each filter appears in the Mail Filter Rules window.



Modifying an existing rule

Description

Please enter the name of the rule: Blacklist

The rule name may contain no more than 30 characters.

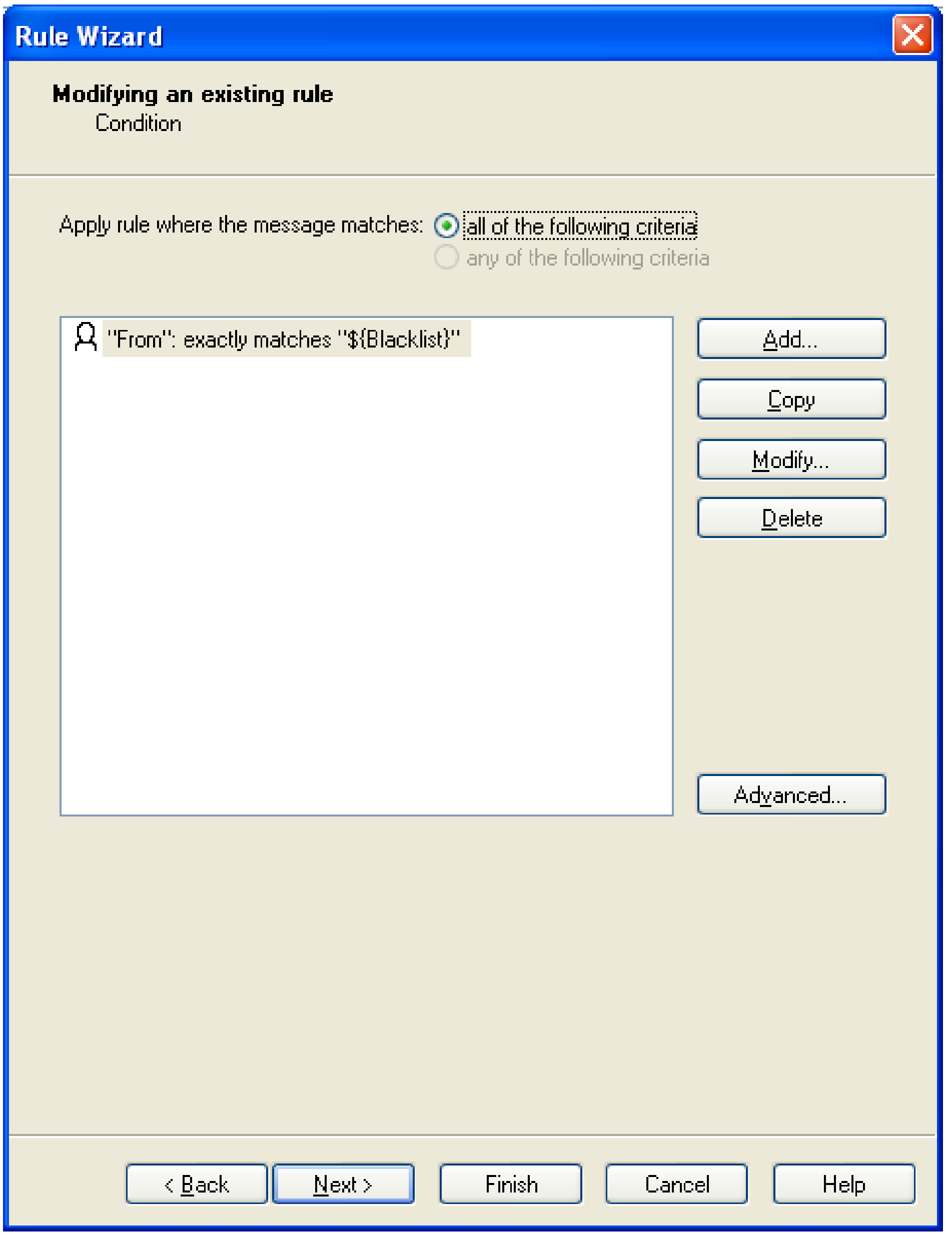
Description of the rule:

Reject mail from all senders blacklisted by the server

Filter names must be unique and can contain only alphanumeric (A-Z, a-z, 0-9), dot (.) and dash (-) characters.

Condition

This panel of the Rule Wizard displays the filtering criteria for your filter rule. These are the conditions that will cause a message to be subject to the filter rule.

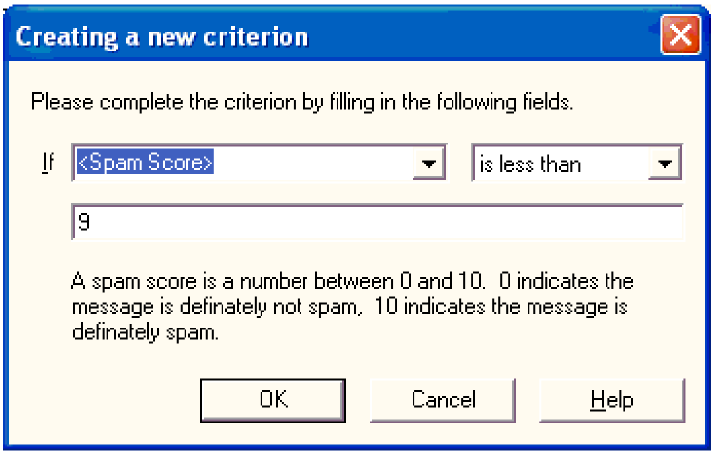

Rule Wizard
Modifying an existing rule
Condition
Apply rule where the message matches: ● all of the following criteria
○ any of the following criteria
"From": exactly matches "${Blacklist}"
Add...
Copy
Modify...
Delete
Advanced...
< Back
Next >
Finish
Cancel
Help

By default, a message must match *all* of the criteria defined in this list to be subject to the filter rule. You can modify this behavior to filter messages that match *any* of the given criteria by selecting the appropriate option at the top of the Condition dialog.

To add criteria to your filter rule, click **Add**. If you would like to edit the filter rule in the Advanced Condition Editor, click the **Advanced** button. When you are done adding criteria, click **Next**.

Creating a New Criterion

Use this dialog to create new criteria for your filter rule. To define a criterion, select the part of the message that you want to search in and the text string for which you are searching. You can also use regular expressions to define sophisticated text searches.



Please complete the criterion by filling in the following fields.

If <Spam Score> is less than

9

A spam score is a number between 0 and 10. 0 indicates the message is definately not spam, 10 indicates the message is definately spam.

When defining filtering criteria, you can search for the given text in either the headers (From, Subject, To, Cc, Bcc, Sender, and Reply-To) or body of the message. For each message header, your criteria can specify the following types of tests:

`contains` the search string
`does not contain` the search string
`exactly matches` the search string
`does not exactly match` the search string
`exists`
`is absent`
`exists and is not empty`
`is absent or is empty`

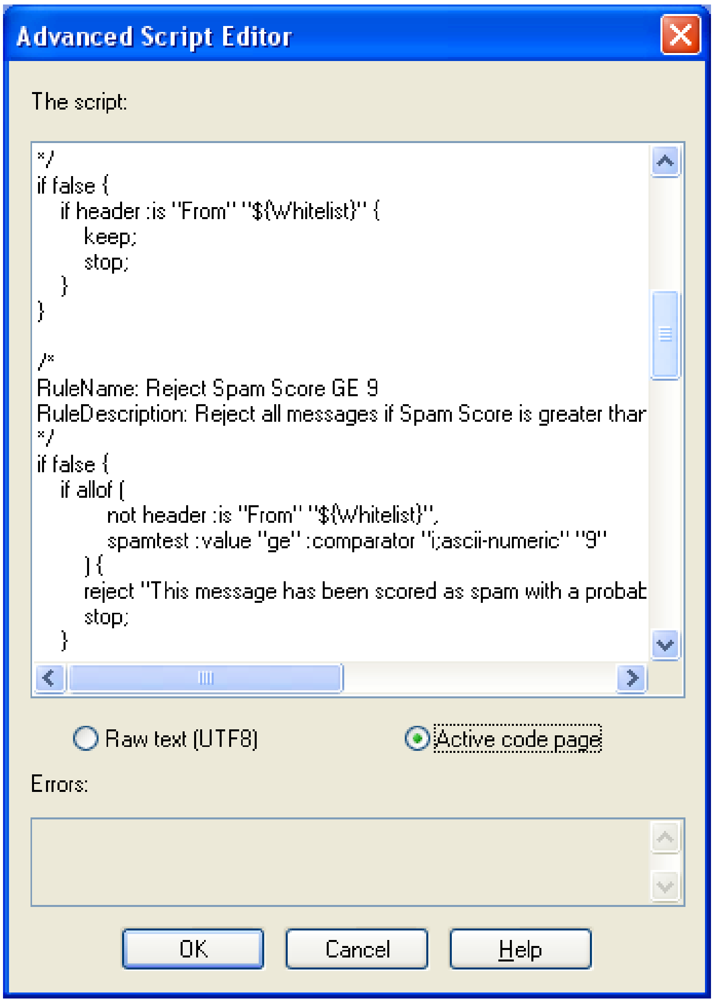
For the body of the message, your criteria can specify the following types of tests:

`contains` the search string
`does not contain` the search string
size **`is over`** the given value
size **`is under`** the given value

When searching for specific text in the headers or body, you can also enable the **Regular Expression** option to specify a regular expression search. This also enables a **Test** button that allows you to test your regular expression syntax on sample message content. Testing regular expression syntax is highly recommended. For information on regular expression syntax, refer to the section on Regular Expressions.

Advanced Script Editor

This dialog allows you to manually edit the scripts that MailSite uses to define filter rules. These scripts are generated automatically when you create filter rules in the MailSite Console, but can be manually edited here to refine filter rules.



The script:

```
*/
if false {
    if header :is "From" "${Whitelist}" {
        keep;
        stop;
    }
}

/*
RuleName: Reject Spam Score GE 9
RuleDescription: Reject all messages if Spam Score is greater thar
*/
if false {
    if allof (
            not header :is "From" "${Whitelist}",
            spamtest :value "ge" :comparator "i;ascii-numeric" "9"
        ) {
        reject "This message has been scored as spam with a probab
        stop;
    }
```

○ Raw text (UTF8) ● Active code page

Errors:

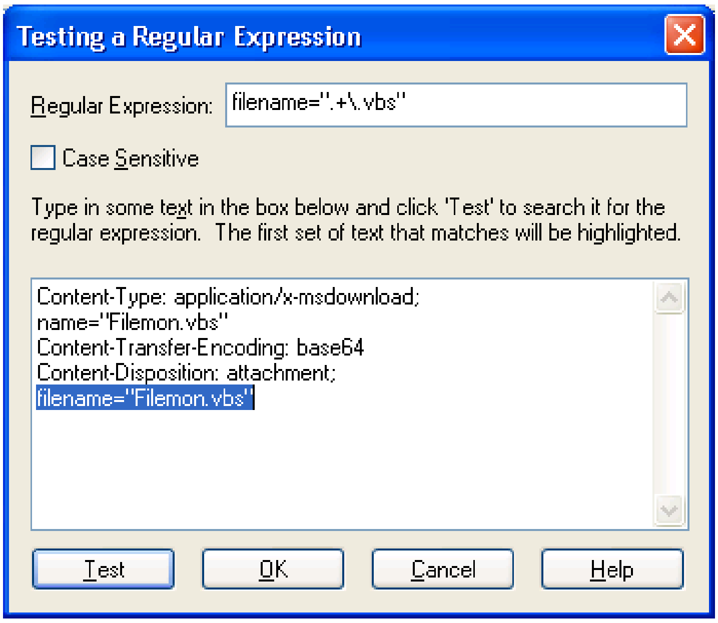
The scripts in this dialog consist of one or more clauses, which are statements that are either true or false.

Scripts are always stored in **Raw Text (UTF8)** format, but it is possible to type scripts in the **Active Code Page** of the current MailSite Console session. This means that an administrator can write scripts more naturally using non-US-ASCII symbols such as the British Pound symbol “£”, umlauts “ü” and so on.

For complete message syntax and examples, refer to the section on Script Editing.

Testing a Regular Expression

Use this dialog to test the syntax of your regular expression filter rule. Testing regular expressions before using them in filters is *highly* recommended.



Regular Expression: filename=".+\.vbs"

□ Case Sensitive

Type in some text in the box below and click 'Test' to search it for the regular expression. The first set of text that matches will be highlighted.

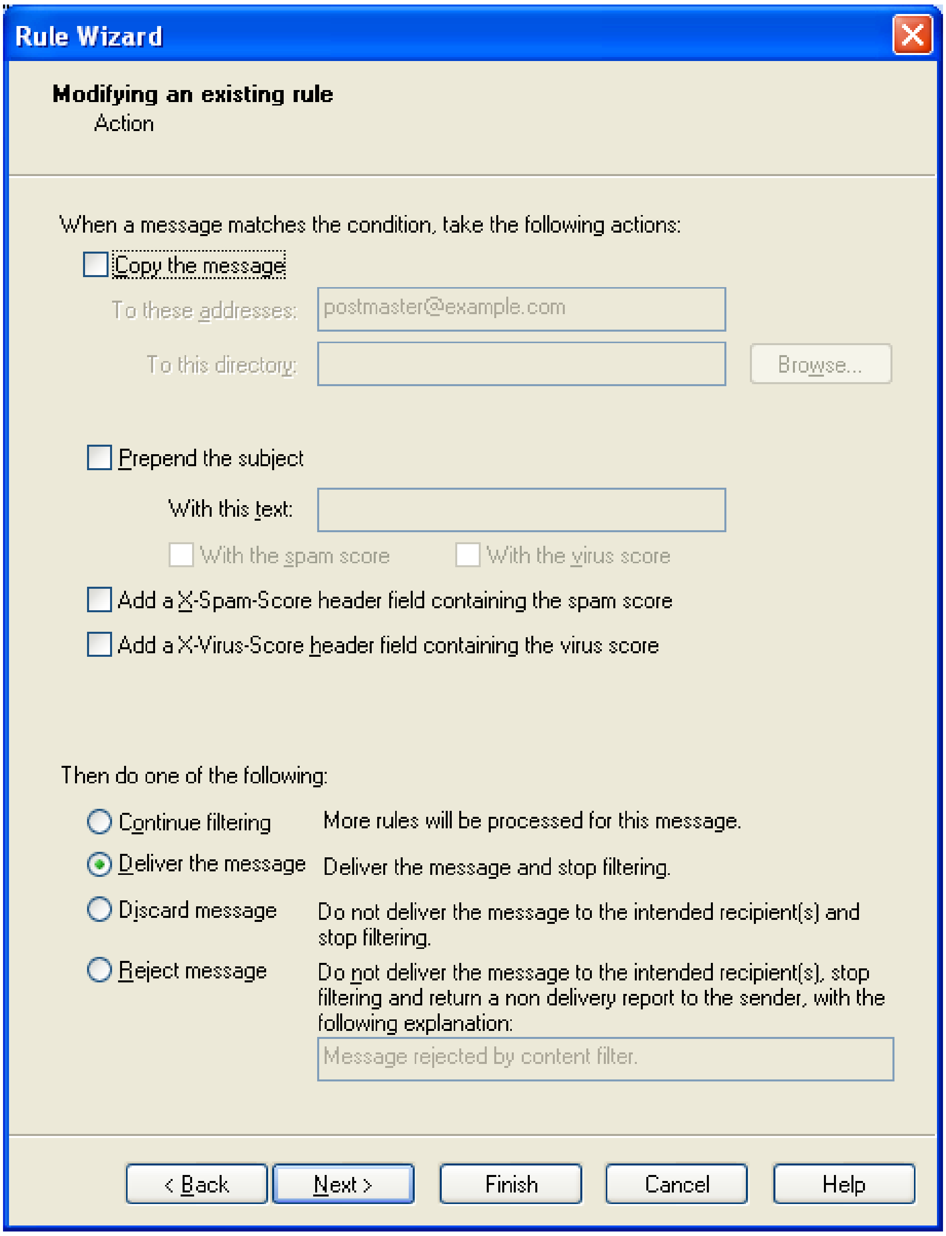
```
Content-Type: application/x-msdownload;
name="Filemon.vbs"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="Filemon.vbs"
```

Enter sample message text in the field provided to test your regular expression. This allows you to simulate the mail filter on the type of content you are looking for. When you click **Test**, the sample text will be searched for text that matches your search criteria.

For information on regular expression syntax, refer to the section on Regular Expressions.

Action

This panel of the Rule Wizard defines the action to be taken against messages that satisfy all of the criteria for the filter rule. In other words, if a message contains all of the characteristics that you set for this rule, MailSite will handle that message according to the actions you set here.



Rule Wizard

Modifying an existing rule
Action

When a message matches the condition, take the following actions:

☐ Copy the message

To these addresses: postmaster@example.com

To this directory:

☐ Prepend the subject

With this text:

☐ With the spam score ☐ With the virus score

☐ Add a X-Spam-Score header field containing the spam score

☐ Add a X-Virus-Score header field containing the virus score

Then do one of the following:

○ Continue filtering — More rules will be processed for this message.

● Deliver the message — Deliver the message and stop filtering.

○ Discard message — Do not deliver the message to the intended recipient(s) and stop filtering.

○ Reject message — Do not deliver the message to the intended recipient(s), stop filtering and return a non delivery report to the sender, with the following explanation:

Message rejected by content filter.

Copy the message

This action is optional, and causes a copy of the message to be forwarded to a specific e-mail address and/or stored in a file system directory. This option is useful for archiving important mail or causing suspect messages to the held for your inspection. Depending on the other actions chosen in this window, the message may or may not be delivered to its intended recipient.

The actions available when copying a message change slightly when creating domain or mailbox filters. For domain filters, copying a message to a file is not available. For mailbox filters, the a message can only be copied to a folder within the recipient's mailbox folder.

Continue Filtering

This action specifies that messages which meet your filter criteria should be subject to your other filter rules. When this action is selected, a message that is copied by this filter rule will also be processed by other filters, which may accept, reject, or delete the message.

Deliver the message

This action specifies that messages which meet your filter criteria should be delivered to their intended recipients and not processed by any additional filter rules.

Discard message

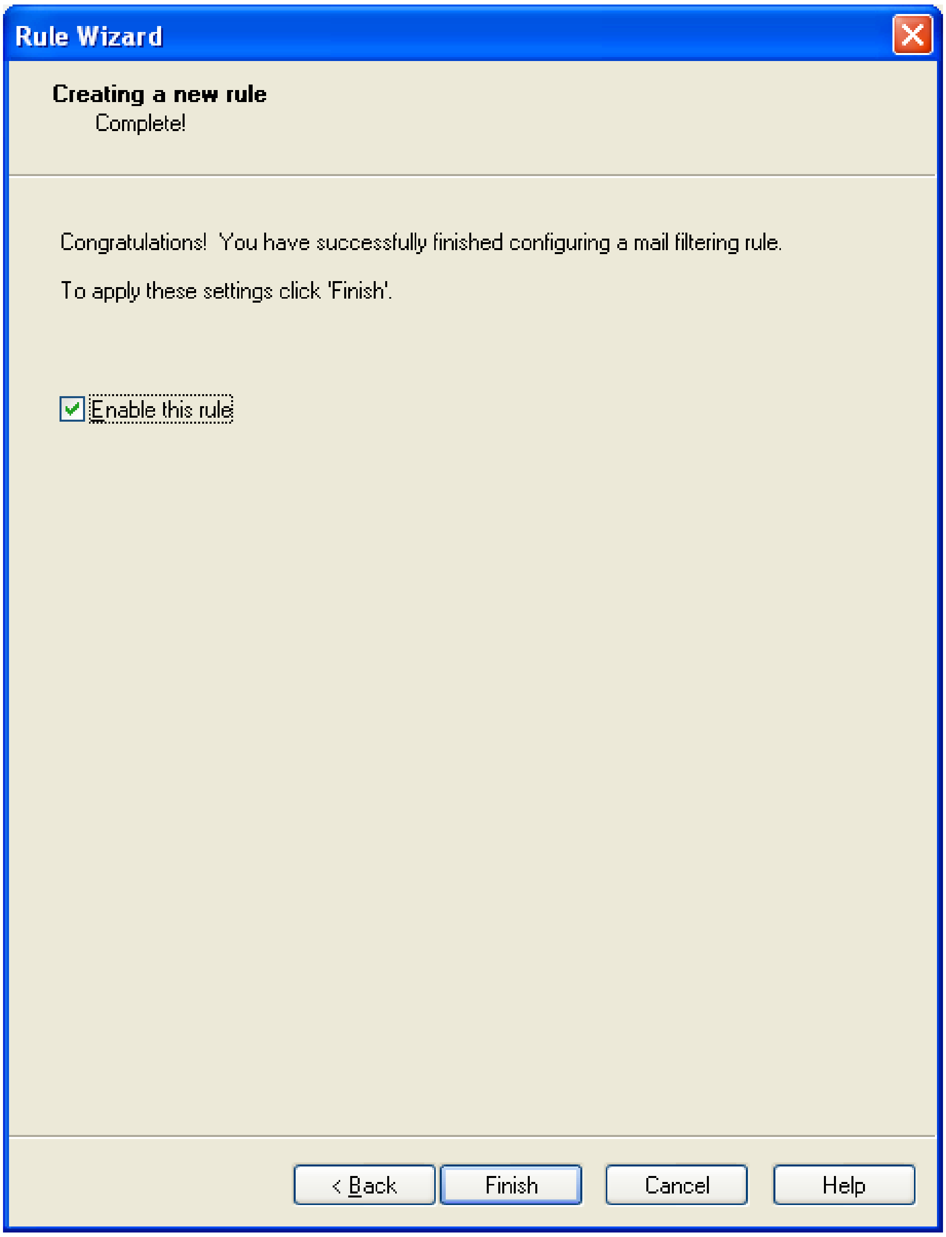
This action specifies that messages should not delivered to their intended recipients and should be simply deleted from the system. When this action is selected messages will not be processed by any subsequent filter rules. Unlike the Reject action, Discard does not return messages or give the sender any indication that the message was not delivered.

Reject Message

This action causes messages to be rejected by MailSite's SMTP server. Rejected messages are not delivered to any recipients and no additional filter rules will be applied to them. When a message is rejected, MailSite blocks it and returns the explanation in the given text field, which allows you to specify the reason why the message was rejected.

Complete

This panel of the Rule Wizard verifies that the filter rule was created successfully and allows you to enable the new rule. The rule must be enabled before MailSite will use the rule to filter incoming mail.



Creating a new rule

Complete!

Congratulations! You have successfully finished configuring a mail filtering rule.

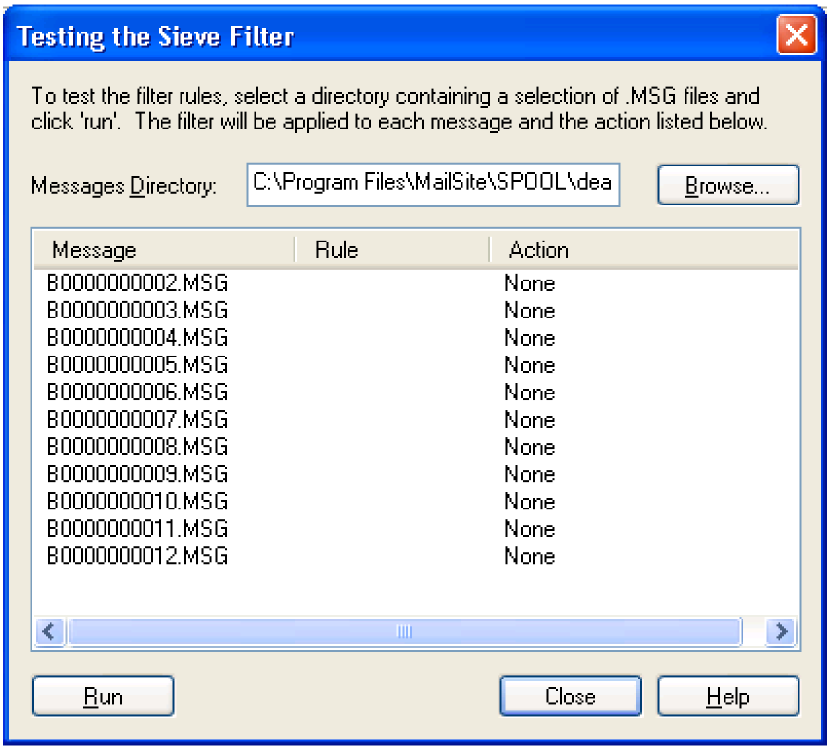
To apply these settings click 'Finish'.

☑ Enable this rule

Click **Finish** to close the wizard and enable the new filter rule.

Testing the Sieve Filter

Use this dialog to test your Sieve Filter rules on sample messages. Testing filter rules is important to verify the affect that they will have on your site's mail activity, and to confirm that they work as intended.



To test the filter rules, select a directory containing a selection of .MSG files and click 'run'. The filter will be applied to each message and the action listed below.

Messages Directory: C:\Program Files\MailSite\SPOOL\dea

Message	Rule	Action
B0000000002.MSG		None
B0000000003.MSG		None
B0000000004.MSG		None
B0000000005.MSG		None
B0000000006.MSG		None
B0000000007.MSG		None
B0000000008.MSG		None
B0000000009.MSG		None
B0000000010.MSG		None
B0000000011.MSG		None
B0000000012.MSG		None

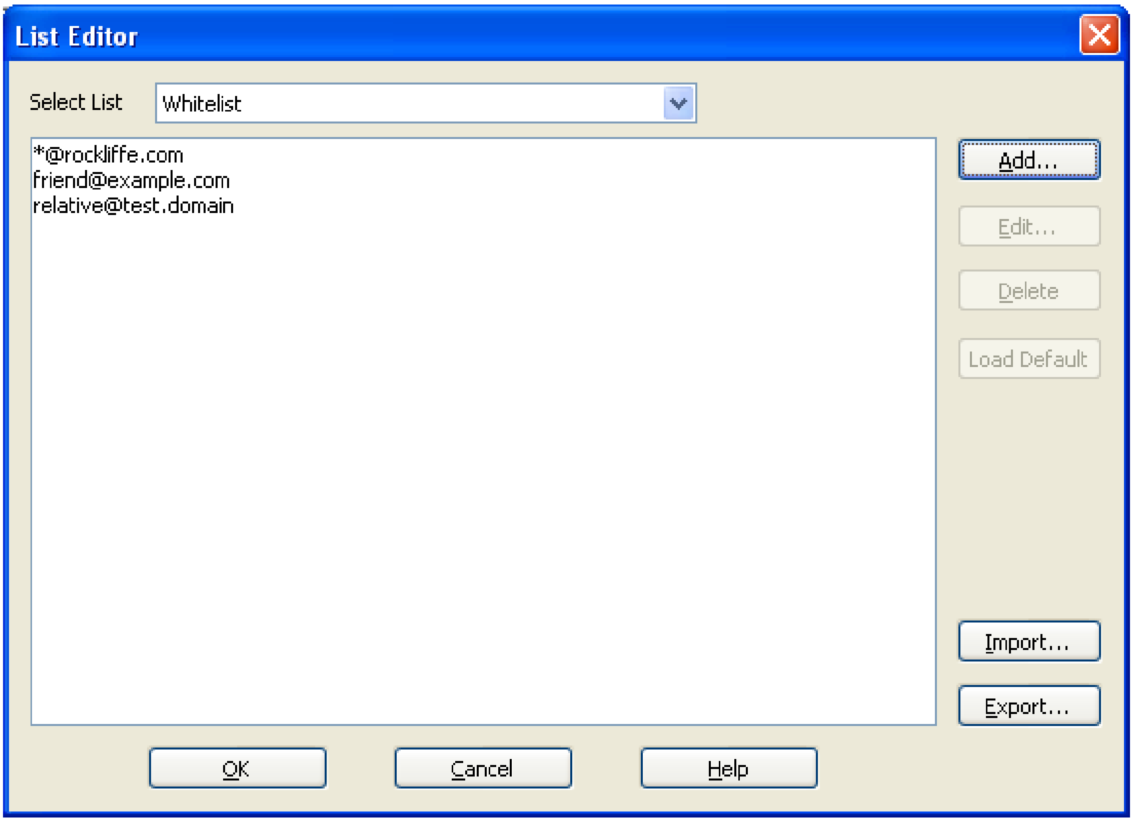
Use the **Browse** button to select the source of the test messages, and then click **Run** to execute your filtering rules against the messages in this directory.

If a message is subject to a filter rule, then this window displays the name of the message file, the filter rule that applies to it, and the action(s) taken against the message. The possible actions are **Reject** (message blocked), **Forward** (message forwarded to the given address), **Copy** (copy of the message is saved), **Discard** (message is not delivered to its recipients), and **Stop** (no more filter rules are applied to the message). If a message is shown with no rule or action, then that message would be delivered normally.

Refer to the section on Testing Filters for more information on using these features to test your filtering strategy.

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.

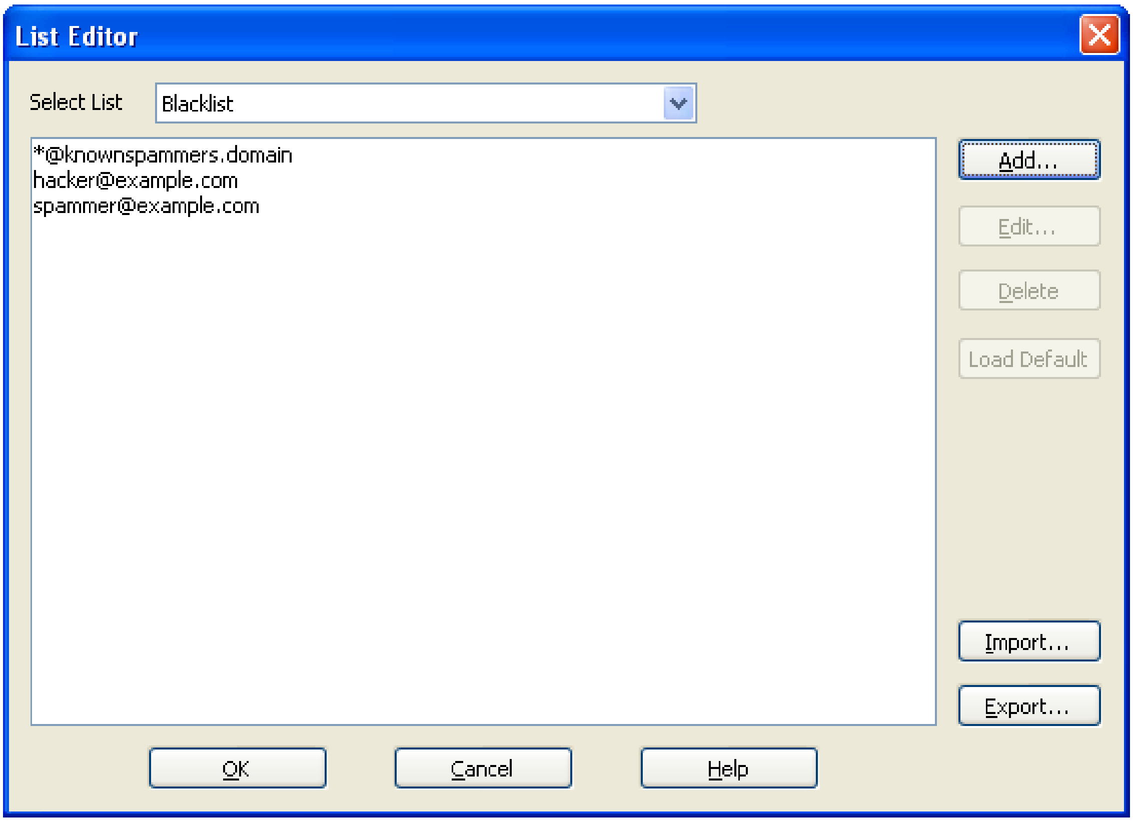


```
*@rockliffe.com
friend@example.com
relative@test.domain
```

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.

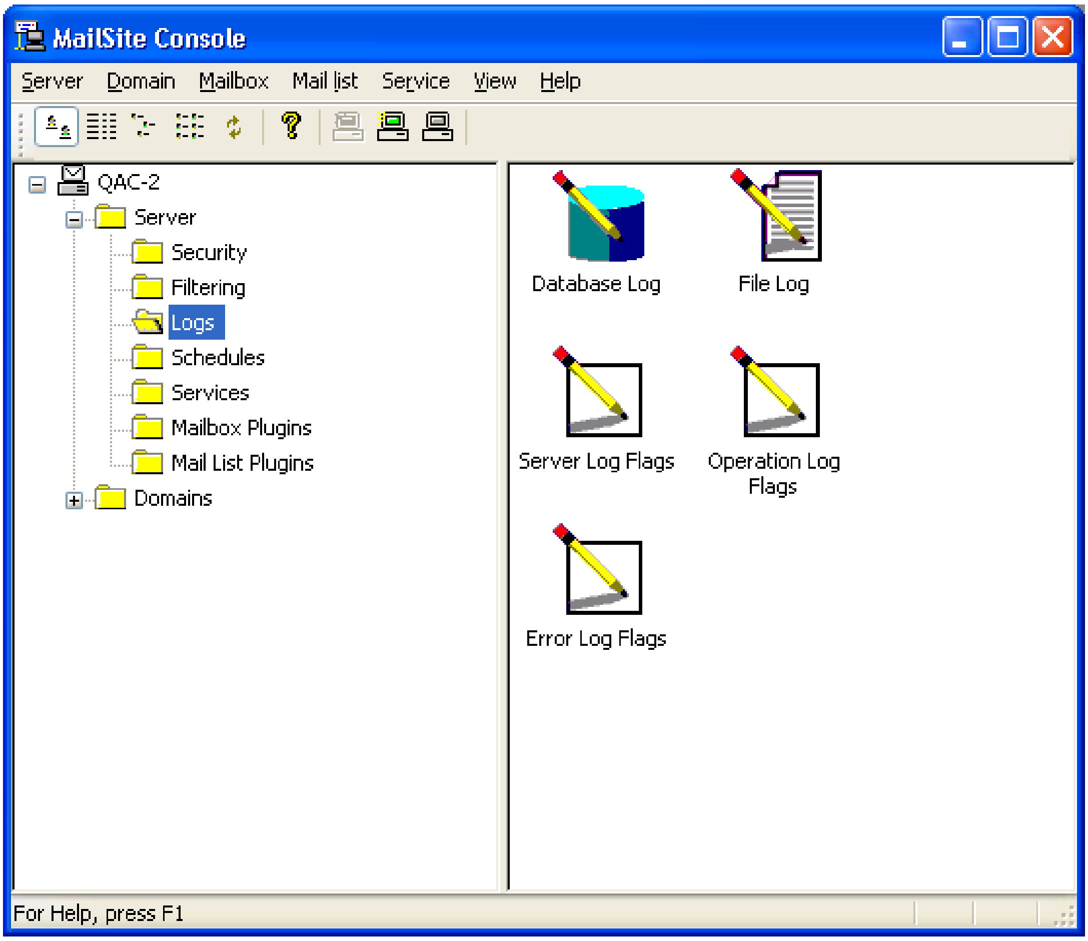


*@knownspammers.domain
hacker@example.com
spammer@example.com

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.

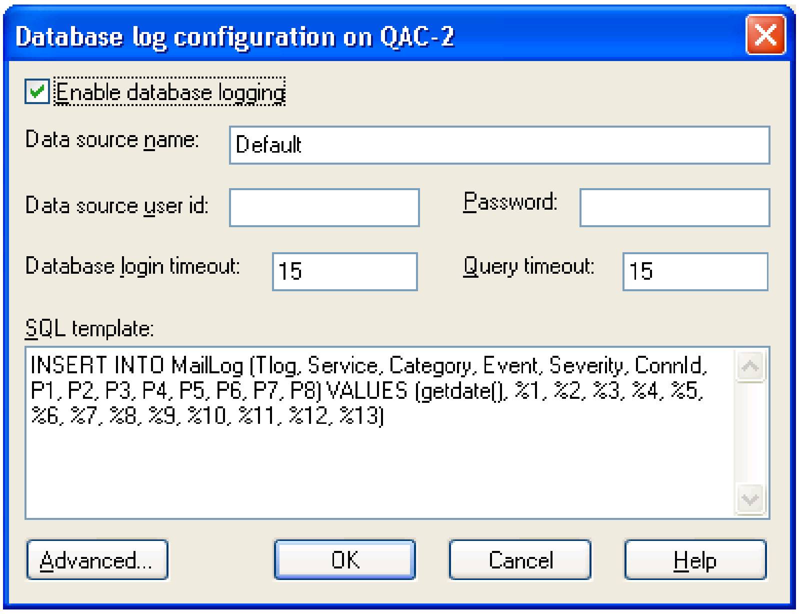


You can use these items to enable and disable logging options for different MailSite components. The logging options change depending on the logging categories that you have selected. You can log to the Event Log for some of the options if you are running Windows NT. You can log to the **`Database Log`** if you have enabled and configured this option.

To configure the database log or the file log, double click on the appropriate icon. To configure exactly what is logged under each of the three logging categories, double-click the appropriate log flags icon.

Database Log

To configure details of the log files, double-click the **`Database`** icon. You will see the following dialog.



☑ Enable database logging

Data source name: Default

Data source user id:

Password:

Database login timeout: 15

Query timeout: 15

SQL template:

```
INSERT INTO MailLog (Tlog, Service, Category, Event, Severity, ConnId,
P1, P2, P3, P4, P5, P6, P7, P8) VALUES (getdate(), %1, %2, %3, %4, %5,
%6, %7, %8, %9, %10, %11, %12, %13)
```

`Enable database logging`

Check this to turn on database logging. Database logging will not take place unless you check this, regardless of what logging options you have turned on.

`Data source name`

The name of the data source which points to the database log, as configured in the System DSN page of the ODBC Data Source Administrator in the Control Panel.

`Data source user id`

The username which MailSite should use when connecting to the data source.

`Password`

The password which MailSite should use when connecting to the data source.

`Database login timeout`

The time in seconds which is allowed for connecting to the database. A value of zero means an infinite timeout.

`Query timeout`

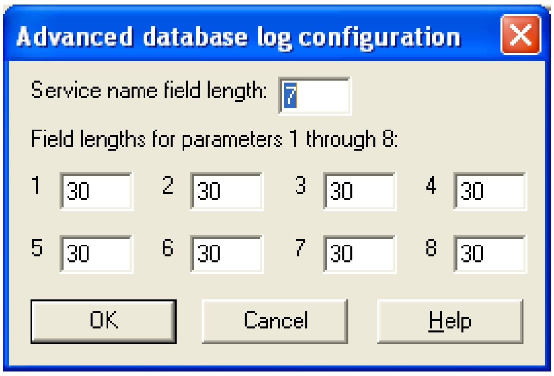
The time in seconds which is allowed for executing the database query. A value of zero means an infinite timeout.

`SQL template`

A template for the SQL command which MailSite should use when adding information to the database. See the appendix on Database Logging for further details.

Advanced Database Log Configuration

The Advanced button brings up another dialog, which allows you to configure additional details of the database:



Advanced database log configuration

Service name field length: 7

Field lengths for parameters 1 through 8:

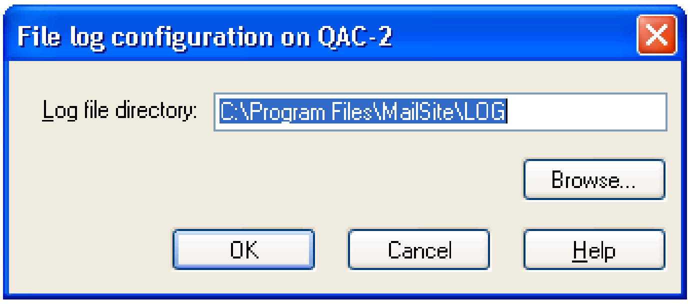
1 30 2 30 3 30 4 30

5 30 6 30 7 30 8 30

Refer to the section on Database Logging for further details.

File Log

To configure details of the log files, double-click the File Log icon. You will see the following dialog.



File log configuration on QAC-2

Log file directory: C:\Program Files\MailSite\LOG

File Log Directory

Enter the full path to the directory where the log files are to be created. If the Windows Console is running on the same machine as the MailSite server, you may use the **Browse** button to select the directory. The default value is **C:\Program Files\MailSite\LOGS**.

Log files will be created in this directory, with names like **TTTYYYYMMDD.LOG**, where:

⇒ **TTT** is one of **SRV** (for "server" log files), **SMTPRA, SMTPDA, IMAP4A, POP3A, MAILMA, HTTPMA, LDAP3A** (for "operation" log files) and **ERR** (for "error" log files).

⇒ **YYYY** is the year.

⇒ **MM** is the month (01 to 12).

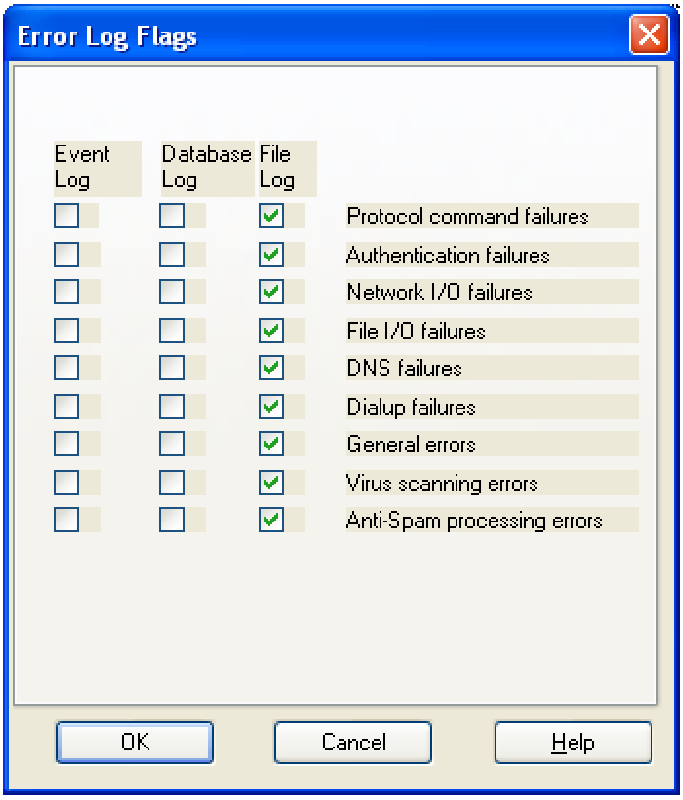
⇒ **DD** is the day of the month (01 to 31).

A new set of log files is created every day.

Previous versions of MailSite used a different convention for log file names. Therefore, if you are administering a previous version of the mail server, you will see some additional fields that are not relevant to the version described by this manual. (The additional fields will appear in the blank area below the log file directory.)

Error Log Flags

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



Event Log	Database Log	File Log	
□	□	☑	Protocol command failures
□	□	☑	Authentication failures
□	□	☑	Network I/O failures
□	□	☑	File I/O failures
□	□	☑	DNS failures
□	□	☑	Dialup failures
□	□	☑	General errors
□	□	☑	Virus scanning errors
□	□	☑	Anti-Spam processing errors

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

Select this option to log when MailSite fails to make a dialup connection. We recommend you enable this option.

General Errors

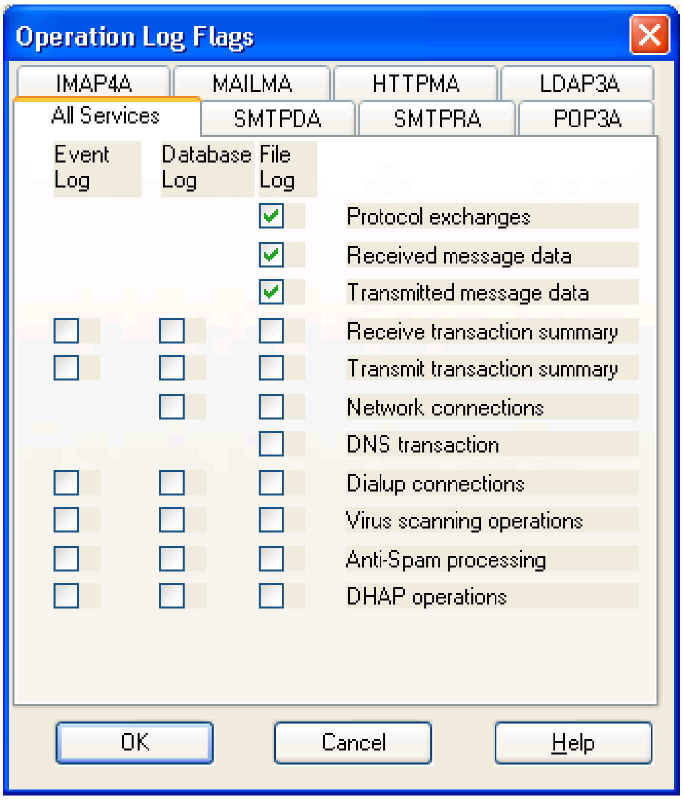
Select this option to log general MailSite errors. We recommend that you enable this option.

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:



Event Log	Database Log	File Log	
		☑	Protocol exchanges
		☑	Received message data
		☑	Transmitted message data
□	□	□	Receive transaction summary
□	□	□	Transmit transaction summary
	□	□	Network connections
		□	DNS transaction
□	□	□	Dialup connections
□	□	□	Virus scanning operations
□	□	□	Anti-Spam processing
□	□	□	DHAP operations

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

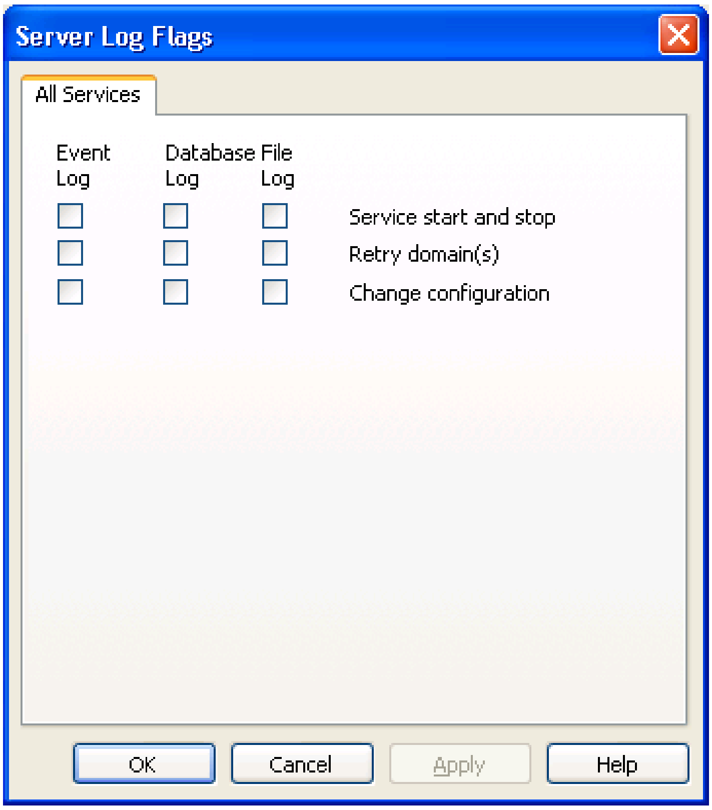
Select this option to record successful spam scans of mail including the score attributed to the message. Greylisting operations will also be recorded if greylisting is enabled.

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:



Server Log Flags

All Services

Event Log	Database Log	File Log	
□	□	□	Service start and stop
□	□	□	Retry domain(s)
□	□	□	Change configuration

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)

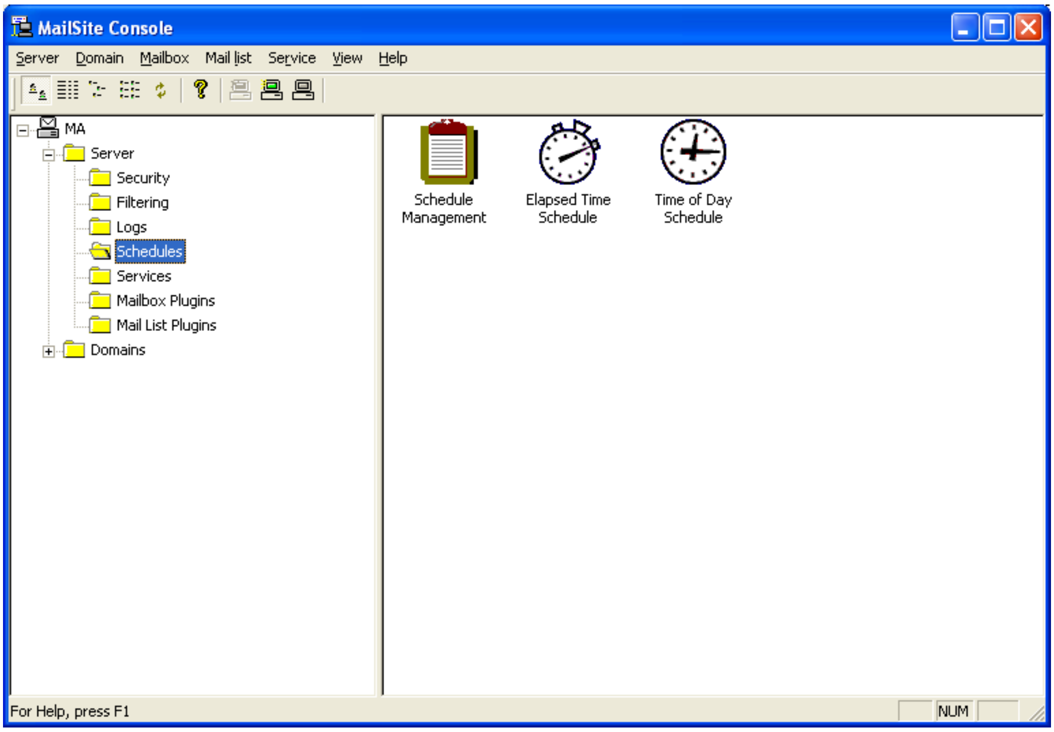
Select this option to make a record when MailSite attempts to re-send any outgoing mail. We recommend you select this option.

Change Configuration

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

Schedules

Use the items in this folder to enable and configure delivery schedules and dialup connectivity.

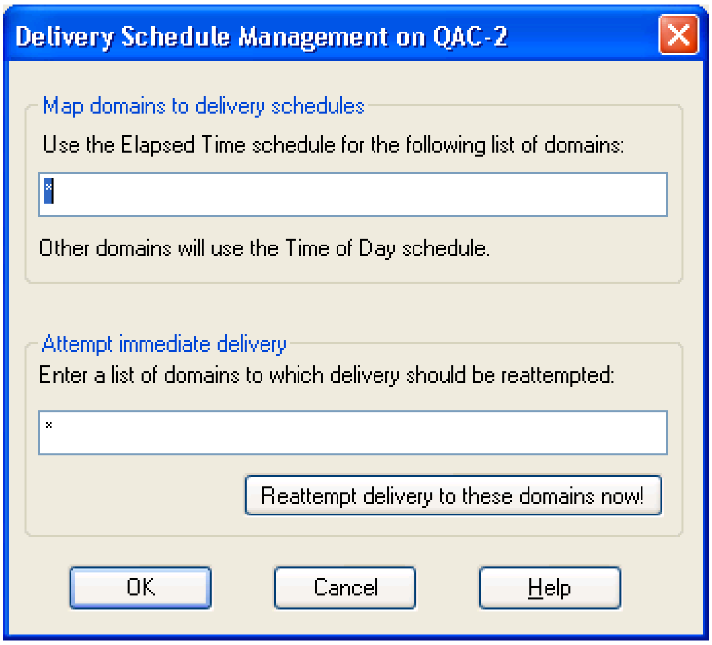


Delivery to remote domains can be schedule using two different methods. The Schedule Management form allows you to choose which method you wish to use for which domain.

The two methods are: **`Elapsed Time`** and **`Time of Day`**.

Schedule Management

Use the Schedule Management dialog to specify which domains will use the elapsed time schedule and which will use the time-of-day schedule. It is also used to initiate an immediate delivery attempt of messages for specified domains.



Delivery Schedule Management on QAC-2

Map domains to delivery schedules

Use the Elapsed Time schedule for the following list of domains:

*

Other domains will use the Time of Day schedule.

Attempt immediate delivery

Enter a list of domains to which delivery should be reattempted:

*

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.

Messages for foreign domains that match this list will be delivered according to the elapsed time schedule. By default, this field contains a single asterisk, meaning that all foreign domains use the elapsed time schedule. If you wish all foreign domains to use the time-of-day schedule instead (for instance, if you have a dialup connection to the Internet), you should enter the value **`!*`** in this field.

For example, suppose your MailSite system is located at company HQ, and is hosting a single domain **`engineering.mycompany.com`**. It is running on the HQ Intranet that contains other mail servers, hosting domains like **`sales.mycompany.com`**. Your company's Internet connection is established only at certain times of the day. There is a branch office in another country, not connected to the company Intranet, but which has its own Internet connection and has a mail server hosting the domain **`italy.mycompany.com`**. In these circumstances, you might want to set the domain mask string to:

⇒ **`!italy.mycompany.com,*mycompany.com,!*`**

This ensures that mail to **`users@italy.mycompany.com`** would be scheduled for delivery according to the time-of-day schedule, whereas mail to **`users@anywhere.else.mycompany.com`** would be scheduled according to the elapsed time schedule (since it is destined for servers on the local Intranet). All other foreign mail would be delivered according to the time-of-day schedule.

Note that this field has nothing to do with routing, which is always performed according to the DNS and the manual routing table. In the above example, you might wish to route mail to **`italy.mycompany.com`** and mail to domains outside the company via your ISP's mail server, and route mail to the other domains within your company in a different way. You should use the Routing dialog to achieve this.

Attempt immediate delivery

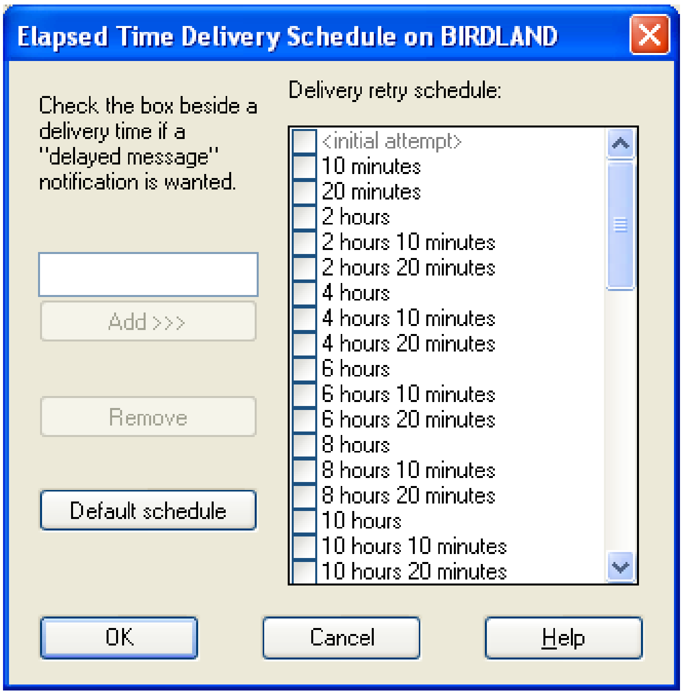
You can enter a list of domain masks (domain names, possibly containing wildcards, separated by commas) in this field. When you click the button labeled **`Reattempt delivery to these domains now`**, any messages for foreign domains which match the domain mask list will be scheduled for an immediate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



Elapsed Time Delivery Schedule on BIRDLAND

Check the box beside a delivery time if a "delayed message" notification is wanted.

Delivery retry schedule:

- □ <initial attempt>
- □ 10 minutes
- □ 20 minutes
- □ 2 hours
- □ 2 hours 10 minutes
- □ 2 hours 20 minutes
- □ 4 hours
- □ 4 hours 10 minutes
- □ 4 hours 20 minutes
- □ 6 hours
- □ 6 hours 10 minutes
- □ 6 hours 20 minutes
- □ 8 hours
- □ 8 hours 10 minutes
- □ 8 hours 20 minutes
- □ 10 hours
- □ 10 hours 10 minutes
- □ 10 hours 20 minutes

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.

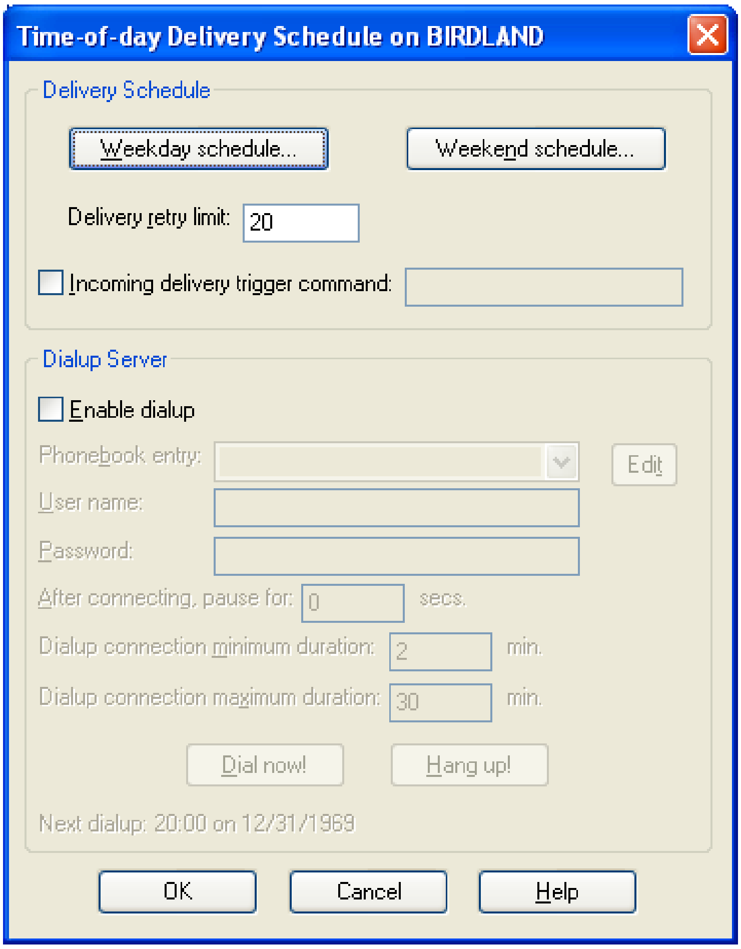
To request a warning message to be generated if a particular delivery attempt fails, check the checkbox beside the delivery attempt.

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

The Time-of-Day Delivery Schedule dialog lets you configure the time-of-day delivery options and control the dialup features of MailSite.



Delivery retry limit: 20

□ Incoming delivery trigger command:

□ Enable dialup

After connecting, pause for: 0 secs.

Dialup connection minimum duration: 2 min.

Dialup connection maximum duration: 30 min.

Next dialup: 20:00 on 12/31/1969

Delivery Schedule

The time-of-day schedule consists of a list of times of the day at which delivery will be attempted. A different list of times pertains on weekdays and weekends.

You can specify the maximum number of times that message delivery will be attempted before a message is treated as undeliverable.

Delivery Retry Limit

A delivery attempt for each outstanding mail domain (other than domains in the **Exclude Domains** field) will be made every time a dialup connection is established. If the delivery attempt is unsuccessful (for example, if the remote mail server is down or inaccessible at the scheduled dialup time), MailSite will retain the message and retry later. However, if the number of delivery attempts exceeds a preset limit, delivery will be abandoned and a non-delivery notification will be generated. This field sets the limit for the number of attempts. The default value is 20.

Incoming Delivery trigger command

When it is time for a delivery attempt to be made, before doing anything else, MailSite will execute the **Delivery Trigger Command**. This can be any command you specify, but often it will be either the **MSSTART** or the **MSPOP** command, which can be used to request your Internet Service Provider's mail server to deliver queued messages to MailSite.

Once connected to your ISP it is often necessary to take some action to cause your ISP's mail server to start sending your mail. For instance, some ISP's let you use a **finger** command. Others (such as MailSite itself) will respond to an **ETRN** SMTP command. If your ISP's mail server needs prompting in this way, check this box and type in the command line to execute. The command line can either invoke a program or a batch file. You must specify the full path.

If your ISP's mail server understands the **ETRN** command, you could use the **MSSTART** command to trigger delivery of queued mail for your domain:

⇒ `C:\Program Files\MailSite\msstart -h mailserver.isp.com myco.com`

This tells the mail server to start sending mail for **myco.com**.

Alternatively, your ISP may accumulate mail for you in a mailbox, and expect you to download it using POP. The **MSPOP** utility will help in this situation. **MSPOP** will retrieve mail from the mailbox at your ISP and will redirect it to recipients on your local system. You might type in the following trigger command line:

⇒ `C:\Program Files\MailSite\mspop -h mailserver.isp.com -u myusername -p mypassword`

Note that when calculating the duration of the dialup connection, MailSite will not start counting until the Delivery Trigger Command (if it exists) has finished. Thus, a command that does not terminate could cause the dialup connection to stay open indefinitely.

See the section on Intermittent Connectivity for more information.

See the Utilities Appendix for the full **MSPOP** and **MSSTART** syntax.

Dialup Server

MailSite supports dialup connectivity to the Internet through the Microsoft Remote Access Service (RAS). This allows a computer running MailSite to dial into an Internet Service Provider (ISP) to exchange mail on a predetermined schedule.

In order to use the MailSite dialup support, you must install RAS on the computer running MailSite. See the Microsoft documentation concerning RAS installation. You will need to create at least one RAS phonebook entry, containing the phone number of your ISP. Before configuring the dialup support in MailSite, check the basic RAS setup by dialing out to your ISP using the "Dialup Networking" tool provided with RAS. If this does not work, MailSite will not be able to dial out.

If you enable dialup, then your MailSite server will dial the phonebook entry according to the schedule that you define. Once connected, it will send any queued outgoing mail and will initiate delivery of incoming mail using the **Incoming Delivery Trigger Command**.

When there is no more outgoing mail to send, and there are no incoming connections to MailSite, the dialup connection will be closed and the phone line hung up.

The Dialup Server part of the Time of Day Schedule dialog contains the following controls:

Enable dialup

Check this box to turn on dialup support in MailSite. Dialup support is disabled by default.

Phonebook Entry

Select an entry from the RAS phonebook that corresponds with your ISP's service. You can use the **Edit** button on the right to edit the phonebook entry.

User name

Your ISP will have given you a username and password to give you access to the dialup server. Type the username here. If the ISP is running a RAS server, you may be given a Microsoft domain name as well. For example, if the domain name is **ISPDOM**, you should add this prefix to your username, as in **ISPDOM\username**.

Password

Type in your ISP password here.

Pause after connecting

With some Internet Service Providers you have to wait for a short time (for example, 15 seconds) after you connect to their service before the connection becomes fully functional. Usually, this is to allow the ISP to update routing information. You can specify a time in to wait using this field.

Dialup connection time

You can specify (in minutes) the maximum time for which a dialup connection will remain open. MailSite will close the connection after this time, even though the connection may be in use for sending and receiving mail. The default is 30 minutes. You can also specify a minimum time that the connection will remain open—MailSite will not close the dialup connection before this time, even if it is not being used for mail. If you reduce this too far, your ISP's mail server may not have enough time to establish an SMTP connection to you. The default is 2 minutes. (Note that both these times are approximate—the actual time may be longer by up to two minutes.)

Note that when calculating the duration of the dialup connection, MailSite will not start counting until the delivery trigger command (if there is one) has finished. Thus, a command that does not terminate could cause the dialup connection to stay open indefinitely.

Dialup Status and Controls

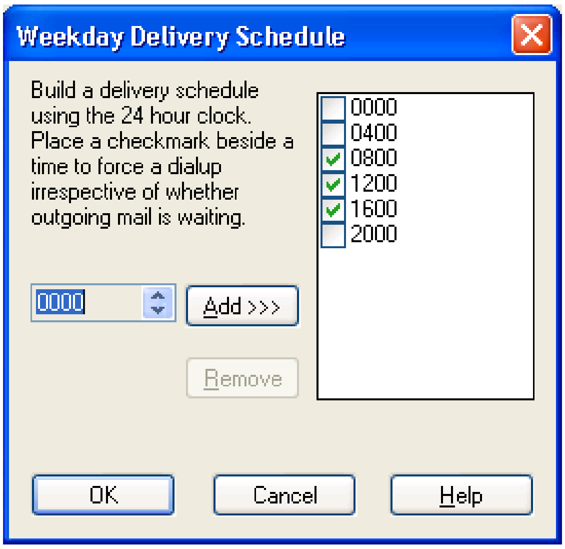
These fields show the status of the dialup connection. If no connection is in progress, it will show the time of the next scheduled connection, otherwise it will show **Connecting**, **Connected** or **Disconnecting.**

If there is no connection in progress, you can request an immediate dialup using the **Dialup Now!** button. In the **Connected** state, you may terminate the connection using the **Hang up!** button.

These buttons are useful for testing and debugging your dialup configuration.

Weekday and Weekend schedules

To configure the weekday and weekend delivery schedules, click on the appropriate button. You will see a dialog like this:



Build a delivery schedule using the 24 hour clock. Place a checkmark beside a time to force a dialup irrespective of whether outgoing mail is waiting.

☐ 0000
☐ 0400
☑ 0800
☑ 1200
☑ 1600
☐ 2000

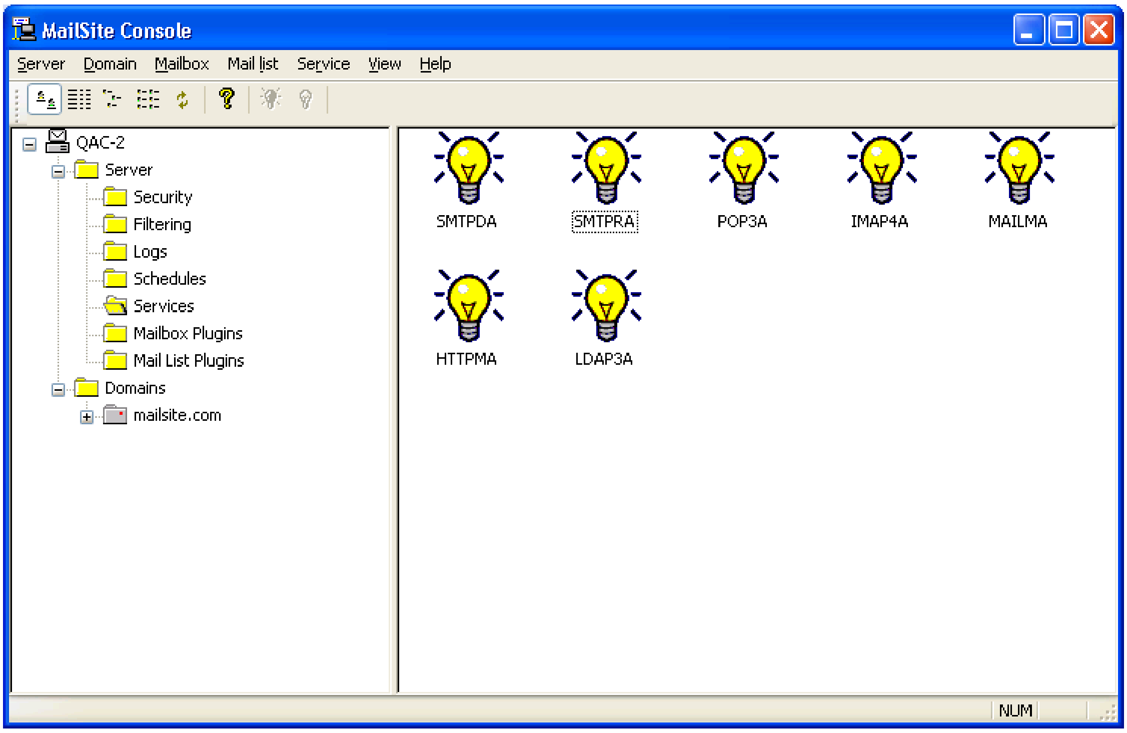
0000

Times for delivery attempts are given using the 24-hour clock. To add a delivery time to the schedule, use the spin control to select a time, then click the **Add** button. To remove a time from the schedule, click on the time and then click the **Remove** button.

To request a dialup even when there is no outgoing mail waiting to be delivered, place a checkmark beside the corresponding time. (The checkmarks are irrelevant if dialup is not enabled.)

Services

If you are administering MailSite on your local computer, or if you are administering MailSite from another system, you will see a Services folder in the Console. When you select this folder, the right-hand pane will display the installed MailSite services:



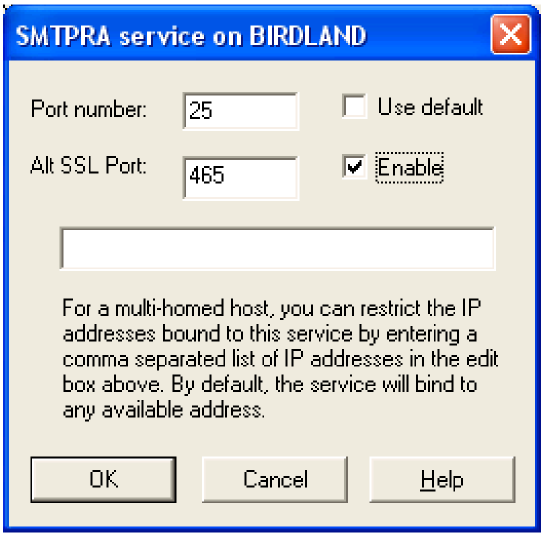
This form displays the current status of each MailSite service. The light bulb icon shows the state of each service. To see the icons in a different format, choose one of the four leftmost buttons on the toolbar, or select the type of view you want from the View menu. To refresh the right-hand pane, choose **`Refresh`** from the View menu or click the **`Refresh`** button (the one with the two arrows).

To start a service, select it and then choose the **`Start`** option from the Service menu. Alternatively, you can use the corresponding toolbar button, or you can right-click on the icon and select **`Start`** from the popup menu. Stopping services works the same way by selecting **`Stop`** from these menus. By selecting multiple icons, you can stop and start more than one service.

Stopping the SMTP Receiver Service will prevent MailSite from receiving mail. Stopping the SMTP Delivery Service will prevent MailSite from sending mail. Stopping the POP3 Service will prevent users from receiving any new mail. Stopping the IMAP4 Service will prevent users from accessing their mailbox. Stopping the HTTP Management Service will prevent users from configuring their mailboxes from their Web browser. Stopping the MAILMA service will prevent users from changing their password from their e-mail client and will disable remote MailSite Console access. Stopping the LDAP3A service will stop MailSite responding to directory searches.

Service Properties

Most of the services listen on a TCP/IP Port. You can configure this Port by selecting **Service** and **Port** from the menu. The following form will be displayed:



Port number: 25 □ Use default

Alt SSL Port: 465 ☑ Enable

For a multi-homed host, you can restrict the IP addresses bound to this service by entering a comma separated list of IP addresses in the edit box above. By default, the service will bind to any available address.

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

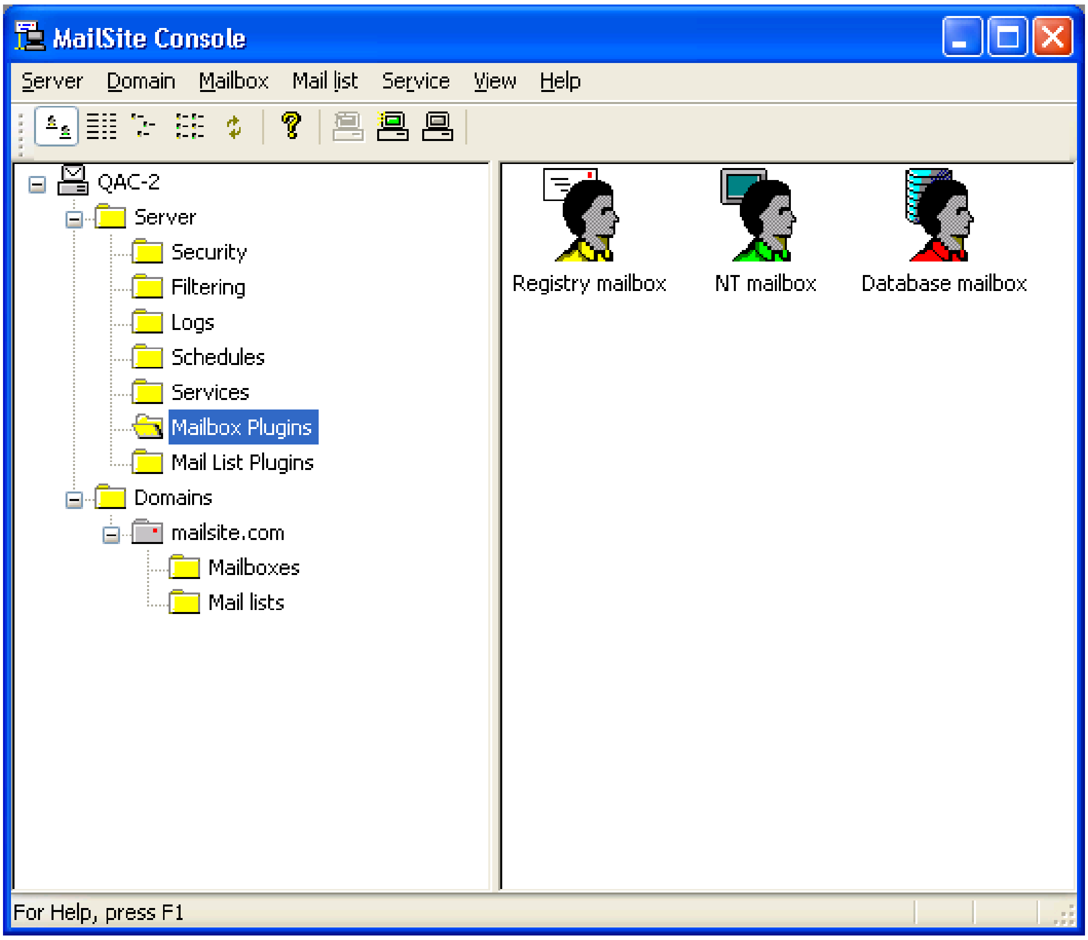
Enter the Port Number that the MailSite service will listen on when communicating over SSL.

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.

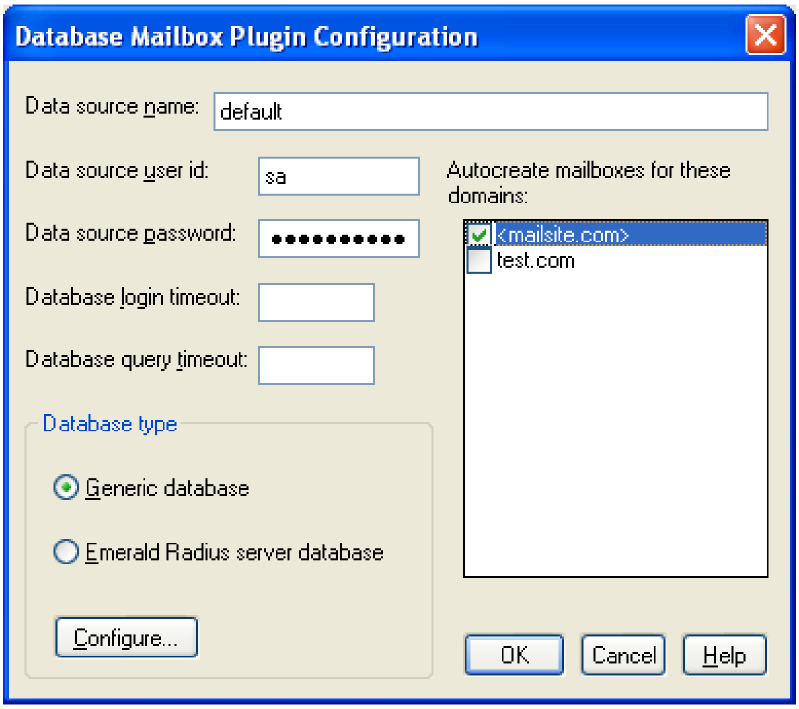


You can configure any of the Plugins by double clicking on its icon.

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.

Database Mailbox Plugin Configuration

Use this form to configure the database table that you wish to use for authenticating mailboxes.



Database Mailbox Plugin Configuration

Data source name: default

Data source user id: sa

Data source password: ●●●●●●●●●●

Database login timeout:

Database query timeout:

Autocreate mailboxes for these domains:

☑ <mailsite.com>

□ test.com

Database type

● Generic database

○ Emerald Radius server database

Data Source Name

Enter the name of the ODBC data source. This is configured in the **System DSN** page of the ODBC Data Source Administrator in the Control Panel.

The data source must be defined in the **System** pane of the ODBC Data Source Administrator, so that the data source is visible to the MailSite services.

Data Source User ID

Enter the username that MailSite should use to log into to the data source.

Data Source Password

Enter the password that MailSite should use to log into to the data source.

Database Login Timeout

Enter the time in seconds that is allowed for connecting to the database. If you leave this blank, the default timeout of 15 seconds will be used. A value of zero means an infinite timeout.

Database Query Timeout

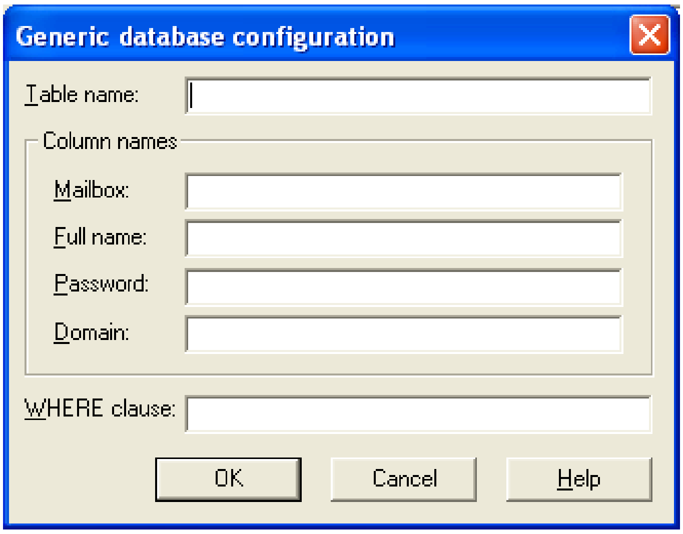
Enter the time in seconds that is allowed for executing the database query. If you leave this blank, the default timeout of 15 seconds will be used. A value of zero means an infinite timeout.

Database Types

The database mailbox plugin supports two kinds of databases: **Generic** and **Emerald**.

Generic Database Configuration

Use this form to override default configuration settings for the Database Mailbox Plugin. See the appendix on Database Plugin Examples for an example of using this feature.



The Generic database assumes a very straightforward database schema. User information is contained in a single table, **`Mailboxes`**, with columns **`Mailbox`**, **`FullName`**, **`Password`** and **`Domain`**. You can override these defaults by filling in the fields on this form:

Table Name

Enter the name of the table or view that contains a list of your database mailboxes. The default name is **`Mailboxes`**.

Mailbox Column

Enter the name of the database column that maps to the mailbox name. Make this column the table's primary key for faster access. The default column name is **`Mailbox`**.

Full Name Column

Enter the name of the database column that contains the mailbox Full Name. The default name is **`FullName`**.

Password Column

Enter the name of the database column that contains the user's password, in plain text. The default name is **`Password`**.

Domain Column

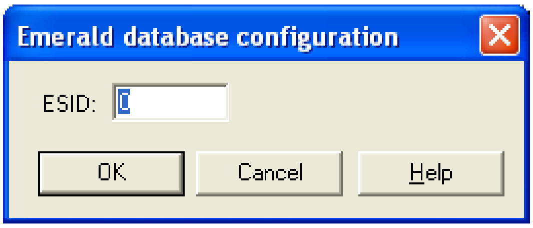
Enter the column that contains the domain name for the user's mailbox. If this column has a null value, the default domain is assumed. If this column does not exist in the database, then MailSite will not differentiate mailboxes in different domains when authenticating. This means that mailboxes with the same name in different domains will be authenticated with the same password.

WHERE Clause

You can further qualify the contents of the table through a filter expression which will form part of a SQL **`WHERE`** clause.

Emerald Database Configuration

Use this form to configure options for your Emerald database. See the appendix on Emerald Integration for an example of using this feature.



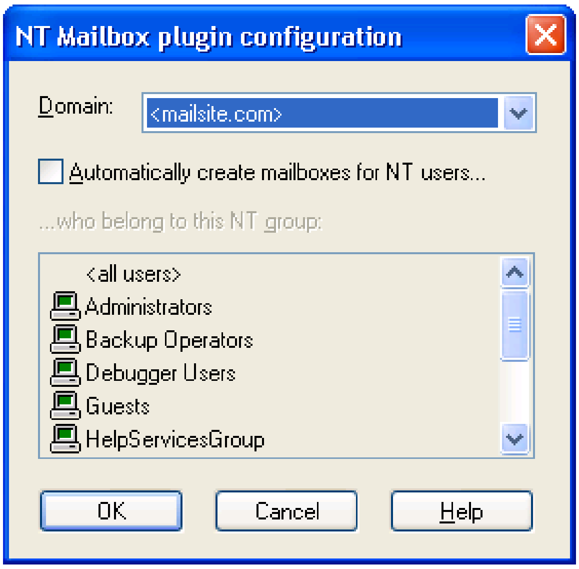
Your Emerald system administrator will need to help you configure this form.

ESID

You can create External System IDs in your Emerald Database. Use your Emerald application to create an ESID for MailSite. You may choose to use 2, for example.

NT Mailbox Plugin Configuration

Use this form to configure the NT Mailbox Plugin.



You can configure the NT Mailbox Plugin to automatically create mailboxes for members of a NT Group. This configuration can be set differently for each virtual domain.

Automatically Create NT Mailboxes

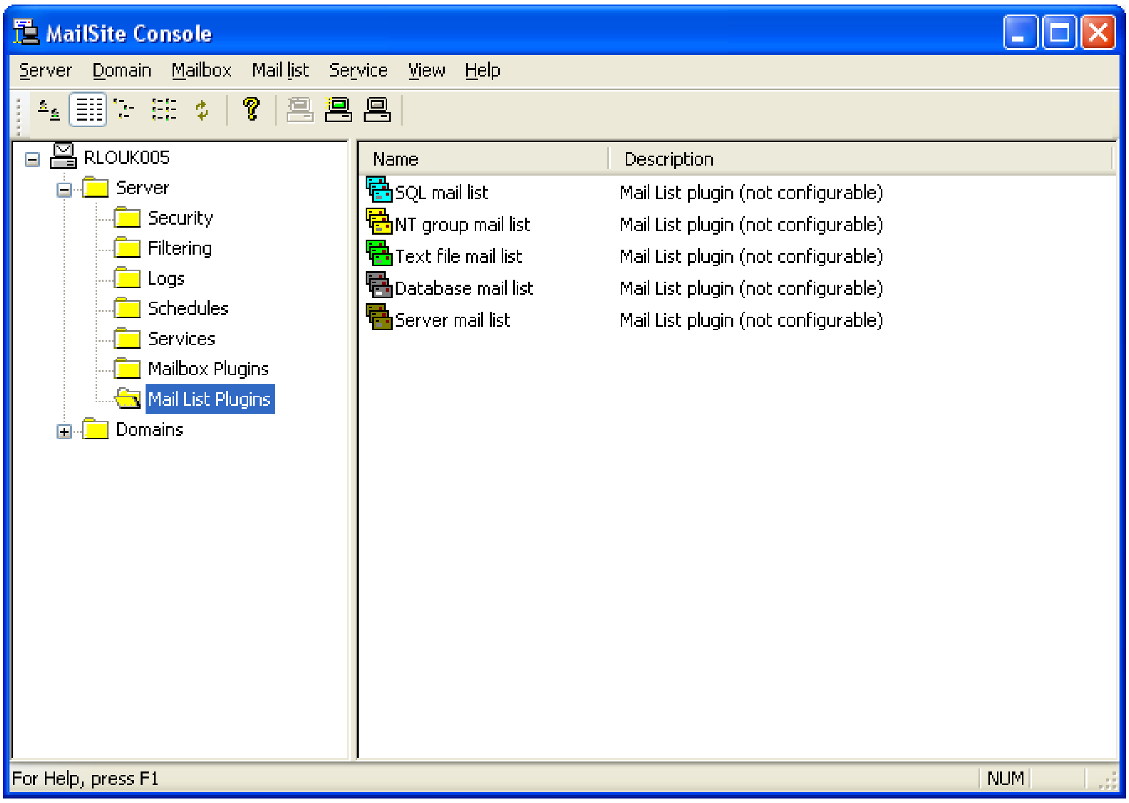
When a user tries to log on using POP or IMAP, or when a new message arrives for the mailbox, the logon attempt or delivery will normally fail if that mailbox does not exist. If you enable mailbox auto-creation for the selected NT group, then provided the user is listed in the group, the mailbox will be created automatically and the logon attempt or delivery will succeed. You can enable automatic mailbox creation for each domain individually.

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.

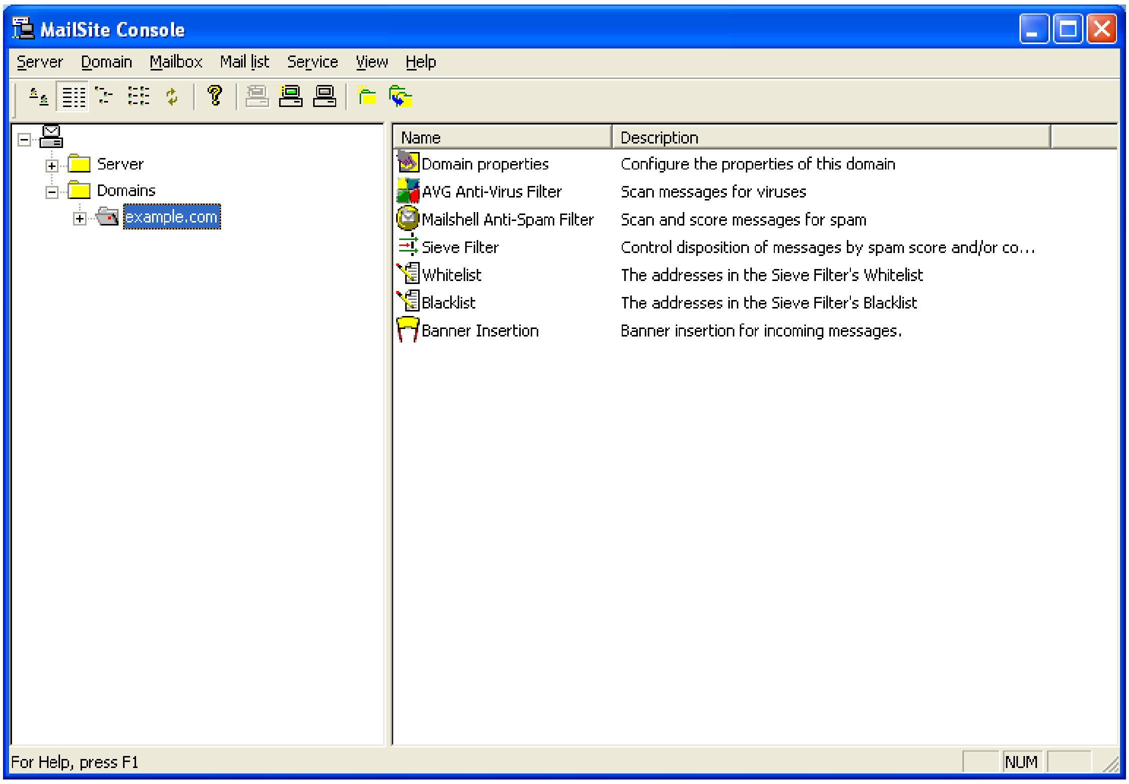


Name	Description
SQL mail list	Mail List plugin (not configurable)
NT group mail list	Mail List plugin (not configurable)
Text file mail list	Mail List plugin (not configurable)
Database mail list	Mail List plugin (not configurable)
Server mail list	Mail List plugin (not configurable)

Each mail list type is implemented by a Mail List Plugin. MailSite ships with five Mail List Plugins: **`Registry`**, **`NT`**, **`Text File`**, **`Database`**, and **`Server`**. Note that none of the Mail List Plugins have any configuration options.

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.



Name	Description
Domain properties	Configure the properties of this domain
AVG Anti-Virus Filter	Scan messages for viruses
Mailshell Anti-Spam Filter	Scan and score messages for spam
Sieve Filter	Control disposition of messages by spam score and/or co...
Whitelist	The addresses in the Sieve Filter's Whitelist
Blacklist	The addresses in the Sieve Filter's Blacklist
Banner Insertion	Banner insertion for incoming messages.

Default Domain

The default domain can be identified by the gray folder icon. This is the "home" domain for this server. MailSite reads the name of the default domain from the **HOST** and **DOMAIN** fields in your TCP/IP: DNS configuration.

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

To rename the default domain, select the domain, then click on the domain name. Or, select the domain and select **Rename** from the right-button pop-up menu.

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**.

You can only rename the default domain. To rename other domains, create a new domain, move the users and mailing lists from the old domain into the new one, then delete the old domain.

New Domain

Select the Domains Folder or one of the existing virtual domain folders. Then choose the **New** option from the Domain menu (or click the corresponding toolbar button, or right-click on the folder and select **New** from the popup menu). A new domain folder will appear, and you should give it a unique name. It is your responsibility to register the domain in the DNS.

`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.

`AVG Anti-Virus Filter`

To set virus scanning policies for a domain, double-click on the **`AVG Anti-Virus Filter`** icon. For each domain, you can specify that all messages sent to or from the domain will be scanned for viruses, or only messages that are addressed to mailboxes that have the virus scanning option enabled.

`Mailshell Anti-Spam Filter`

To set spam scanning policies for a domain, double-click on the **`Mailshell Anti-Spam Filter`** icon. For each domain, you can specify whether mail to all mailboxes will be scanned, or only messages that are addressed to mailboxes that have the virus scanning option enabled.

For all spam scanning enabled mailboxes greylisting can be enabled, helping to improve spam catch rates.

`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.

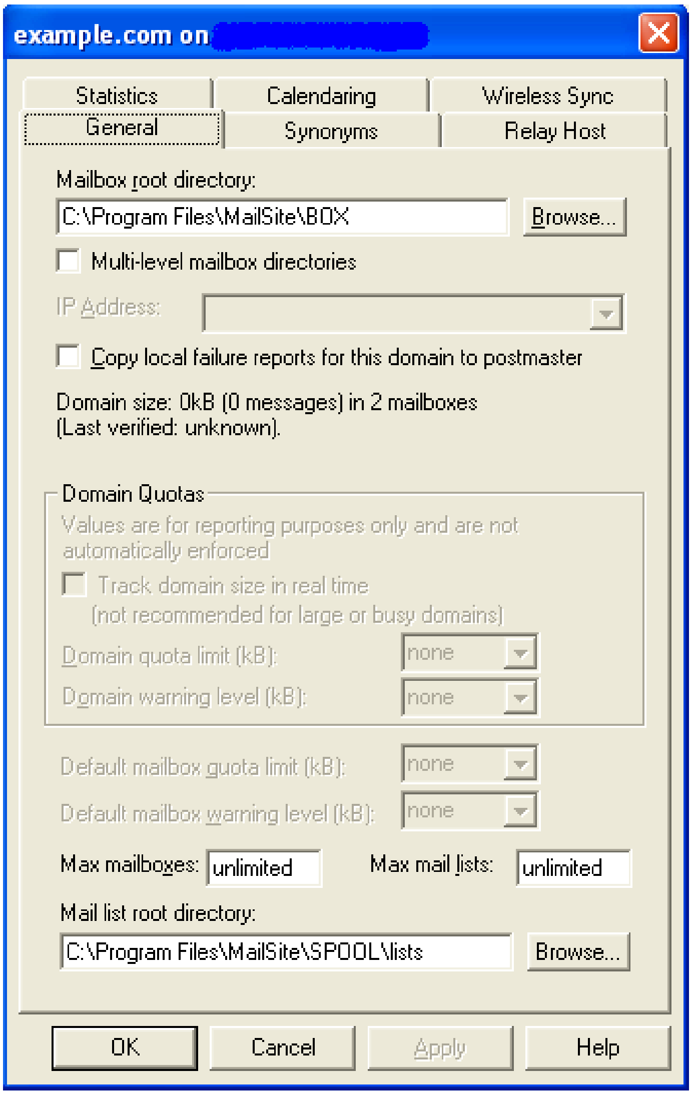
For example, if you add a virtual domain **`xyz.com`**, then incoming mail sent to **`someone@xyz.com`** will be delivered to mailbox **`someone`** in domain **`xyz.com`**.

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:



example.com on [redacted]

Mailbox root directory: C:\Program Files\MailSite\BOX

☐ Multi-level mailbox directories

IP Address:

☐ Copy local failure reports for this domain to postmaster

Domain size: 0kB (0 messages) in 2 mailboxes
(Last verified: unknown).

Domain Quotas

Values are for reporting purposes only and are not automatically enforced

☐ Track domain size in real time
(not recommended for large or busy domains)

Domain quota limit (kB): none

Domain warning level (kB): none

Default mailbox quota limit (kB): none

Default mailbox warning level (kB): none

Max mailboxes: unlimited

Max mail lists: unlimited

Mail list root directory: C:\Program Files\MailSite\SPOOL\lists

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**, which are stored in the Registry. The properties are set through the Mailboxes folder in 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

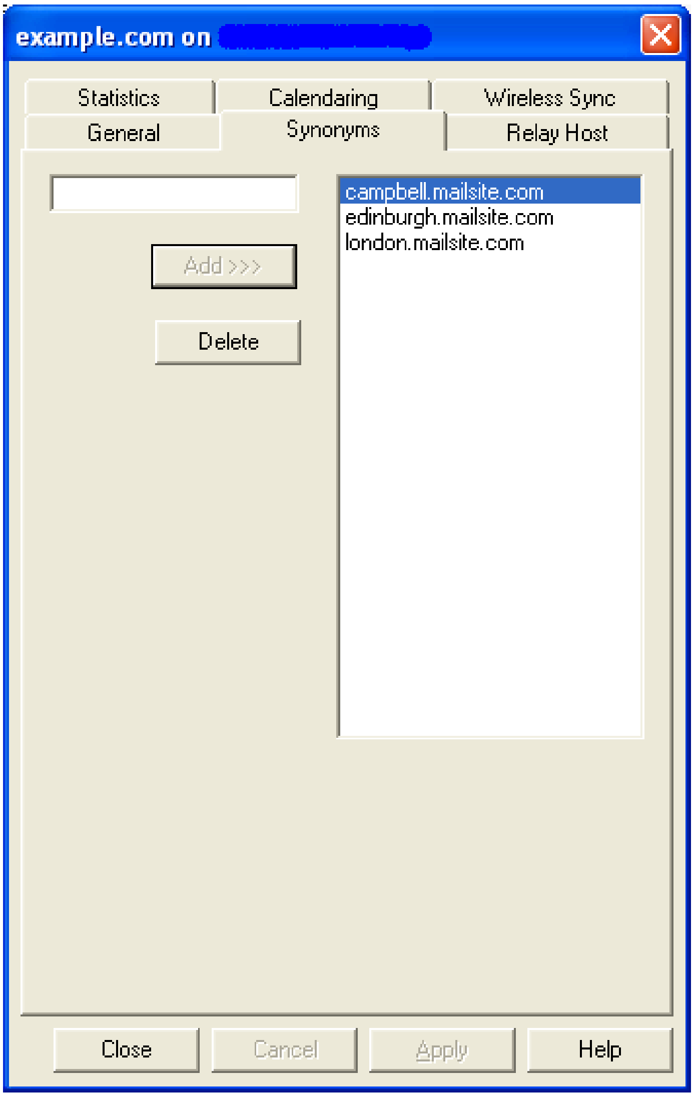
You can use this field to limit the number of mail lists that can be created in this domain. You may wish to use this feature if you delegate management of mail lists for this domain to your users through the Web Console. Leave this field blank if you do not want a limit. If you try to set the maximum 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:



example.com on [redacted]

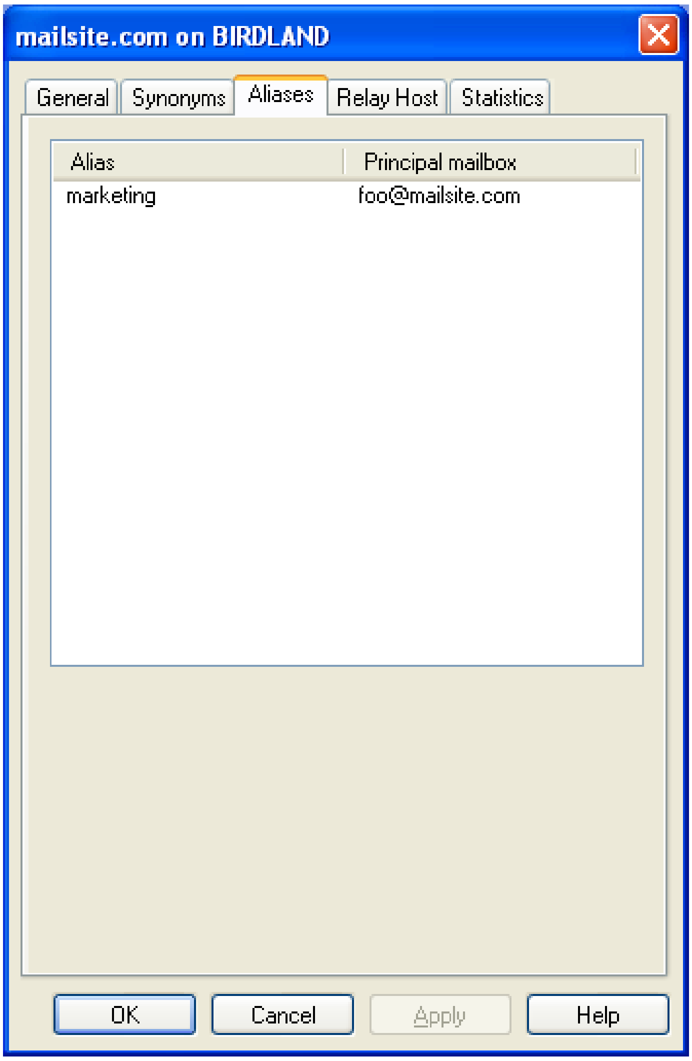
campbell.mailsite.com
edinburgh.mailsite.com
london.mailsite.com

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:

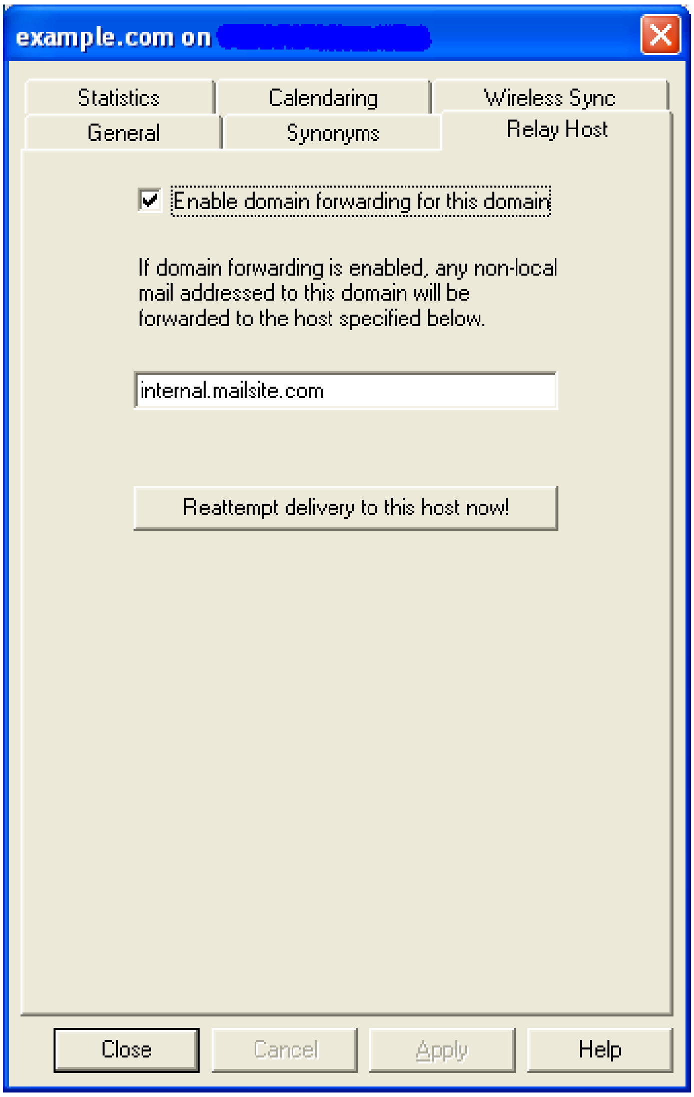


Alias	Principal mailbox
marketing	foo@mailsite.com

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:



example.com on [redacted]

☑ Enable domain forwarding for this domain

If domain forwarding is enabled, any non-local mail addressed to this domain will be forwarded to the host specified below.

internal.mailsite.com

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.

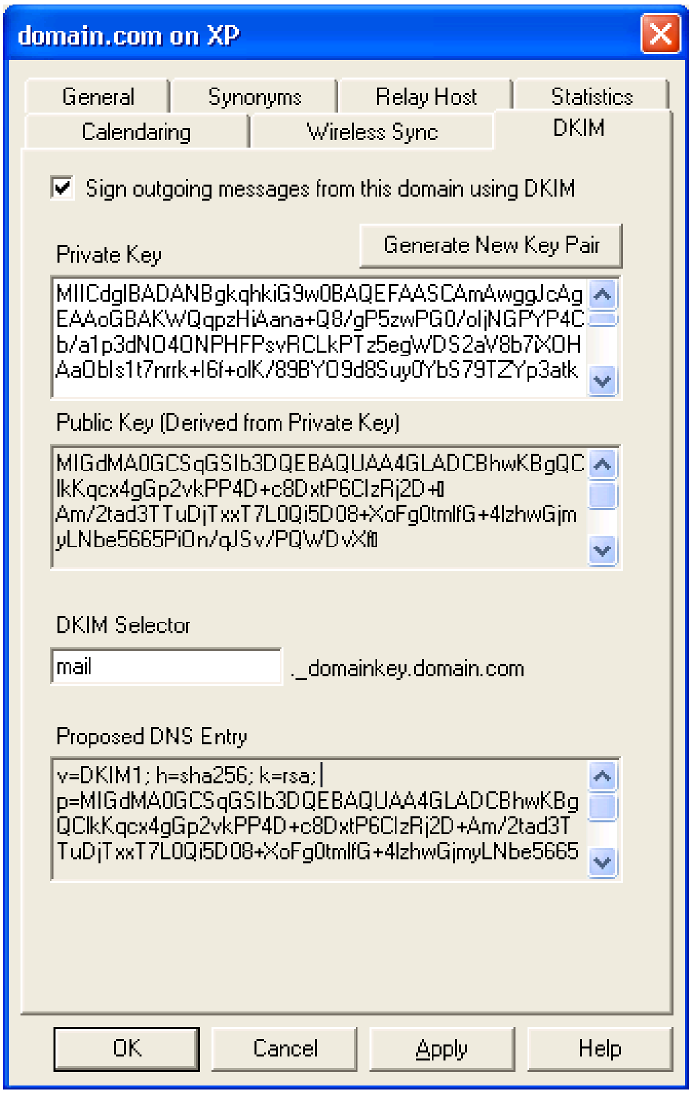
The “Reattempt delivery to this host now!” button will force an instant attempt to deliver any queued mail for this domain to the specified host. This button will only work when forwarding is enabled and will be disabled until the button is pressed again.

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.



☑ Sign outgoing messages from this domain using DKIM

Private Key

```
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAg
EAAoGBAKWQqpzHiAana+Q8/gP5zwPG0/oljNGPYP4C
b/a1p3dNO4ONPHFPsvRCLkPTz5egWDS2aV8b7lXOH
Aa0bls1t7nrrk+l6f+olK/89BYO9d8Suy0YbS79TZYp3atk
```

Public Key (Derived from Private Key)

```
MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQC
lkKqcx4gGp2vkPP4D+c8DxtP6ClzRj2D+
Am/2tad3TTuDjTxxT7L0Qi5D08+XoFg0tmlfG+4lzhwGjm
yLNbe5665PiOn/qJSv/PQWDvX
```

DKIM Selector

mail ._domainkey.domain.com

Proposed DNS Entry

```
v=DKIM1; h=sha256; k=rsa;
p=MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBg
QClkKqcx4gGp2vkPP4D+c8DxtP6ClzRj2D+Am/2tad3T
TuDjTxxT7L0Qi5D08+XoFg0tmlfG+4lzhwGjmyLNbe5665
```

To Enable DKIM in MailSite:

1) Load the MailSite Console and select the domain you want to enable DKIM for, eg domain.com.
2) Select Domain Properties on the right hand side.
3) Select DKIM tab
4) Select 'Sign outgoing messages from this domain using DKIM

5) 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.
6) If you do not have a private key already, select 'Generate New Key Pair.
7) Enter a DKIM Selector. This name will also be used in DNS, eg "mail", so it will read mail._domainkey.domain.com

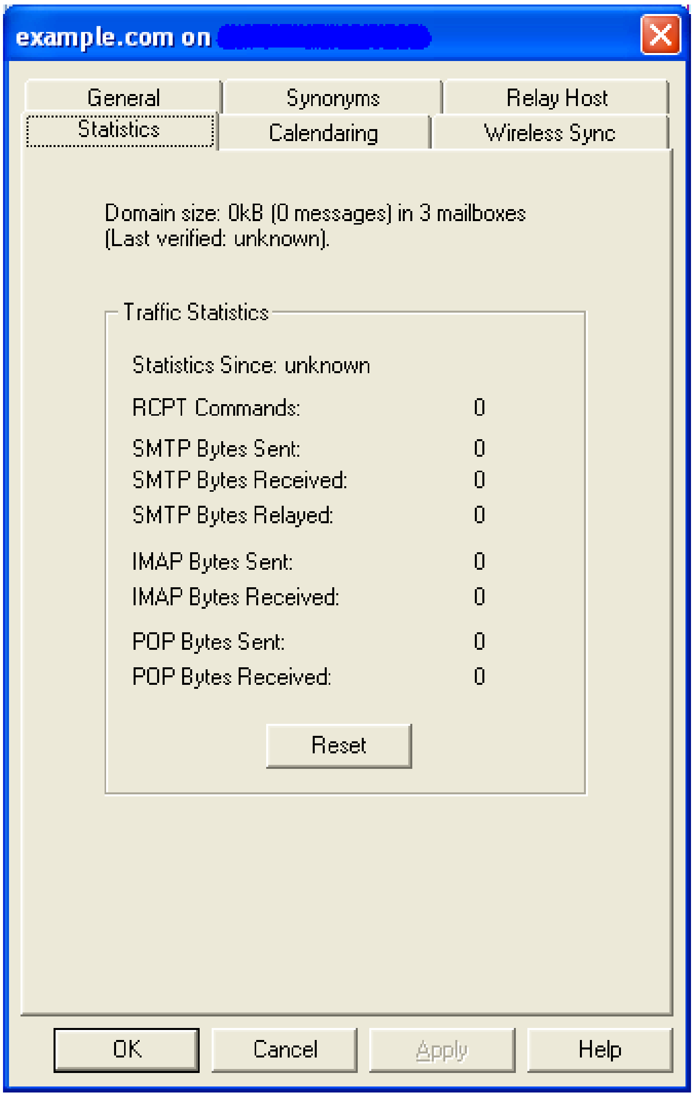
To Enable DKIM in DNS

this example is provided for a Windows 2003 DNS server. Your DNS administrator or provider can help you with setting up the record.

1) Select your domain name in the Forward Lookup Zones for domain.com
2) Right click on the domain root and select 'New Domain. Name this "_domainkey”
3) Select this newly created domain and on the right hand side right click and select "Other new records" and choose TXT record
4) Set the record name to the selector specified in MailSite, in this case ‘mail’
5) Copy and paste the 'Proposed DNS Entry' string from MailSite console into the 'text' box
6) Save the changes.

Domain Statistics Page

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



example.com on [redacted]

Domain size: 0kB (0 messages) in 3 mailboxes
(Last verified: unknown).

Traffic Statistics

Statistics Since: unknown

RCPT Commands: 0

SMTP Bytes Sent: 0
SMTP Bytes Received: 0
SMTP Bytes Relayed: 0

IMAP Bytes Sent: 0
IMAP Bytes Received: 0

POP Bytes Sent: 0
POP Bytes Received: 0

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.

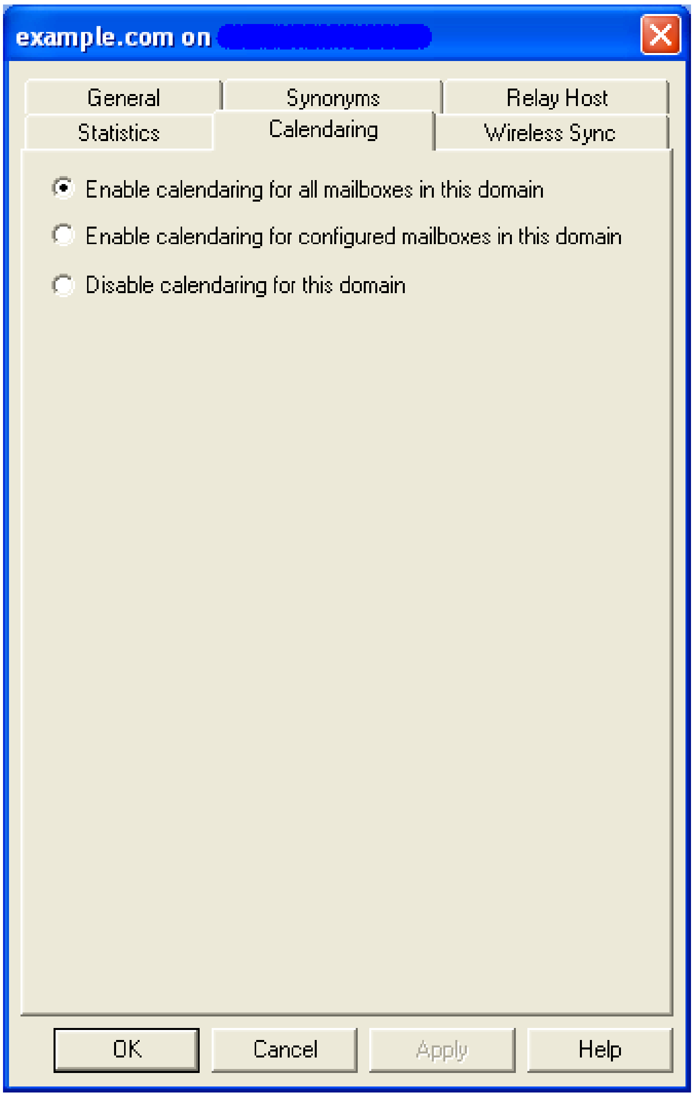
Traffic Statistics

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).



example.com on [redacted]

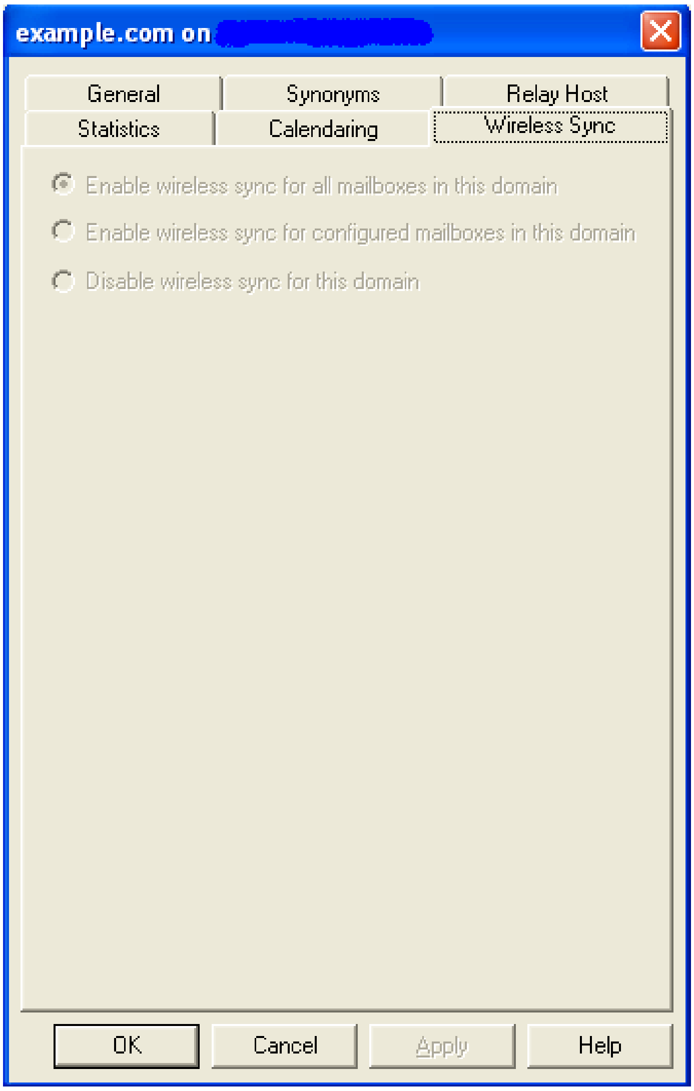
● Enable calendaring for all mailboxes in this domain

○ Enable calendaring for configured mailboxes in this domain

○ Disable calendaring for this domain

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).



example.com on [redacted]

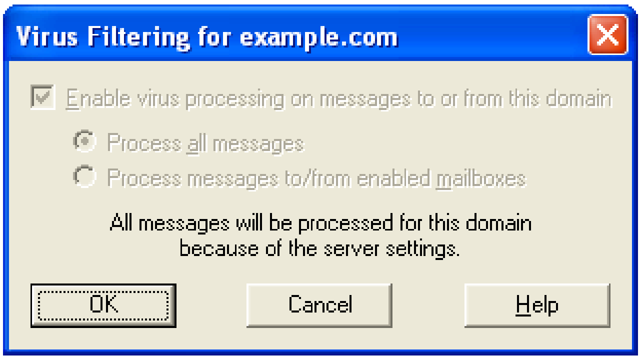
● Enable wireless sync for all mailboxes in this domain

○ Enable wireless sync for configured mailboxes in this domain

○ Disable wireless sync for this domain

Domain Virus Filter

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



Virus Filtering for example.com

☑ Enable virus processing on messages to or from this domain

● Process all messages

○ Process messages to/from enabled mailboxes

All messages will be processed for this domain
because of the server settings.

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

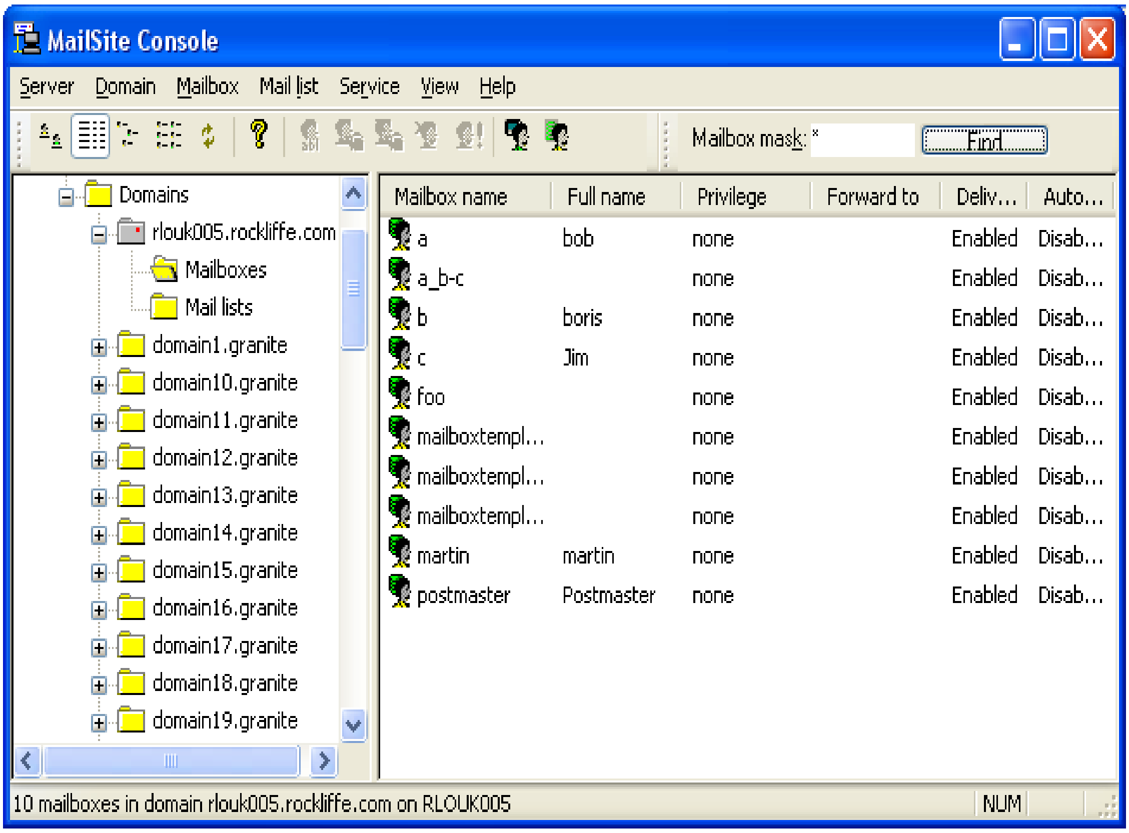
This selection causes all messages received by MailSite's SMTP server that are sent to or from any mailbox within this domain to be scanned. Use this option if you want all mailboxes in the domain to be protected from viruses.

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:



- Domains
  - rlouk005.rockliffe.com
    - Mailboxes
    - Mail lists
  - domain1.granite
  - domain10.granite
  - domain11.granite
  - domain12.granite
  - domain13.granite
  - domain14.granite
  - domain15.granite
  - domain16.granite
  - domain17.granite
  - domain18.granite
  - domain19.granite

Mailbox name	Full name	Privilege	Forward to	Deliv...	Auto...
a	bob	none		Enabled	Disab...
a_b-c		none		Enabled	Disab...
b	boris	none		Enabled	Disab...
c	Jim	none		Enabled	Disab...
foo		none		Enabled	Disab...
mailboxtempl...		none		Enabled	Disab...
mailboxtempl...		none		Enabled	Disab...
mailboxtempl...		none		Enabled	Disab...
martin	martin	none		Enabled	Disab...
postmaster	Postmaster	none		Enabled	Disab...

10 mailboxes in domain rlouk005.rockliffe.com on RLOUK005 NUM

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.

If your users will only use the server to send and receive mail, then you may wish to create Registry Mailboxes for them. This will limit their privileges to mail and will definitely prevent them from accessing any other part of the NT system.

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.

You can select the type of mailbox display in the right-hand panel using one of the four leftmost buttons in the toolbar, or by using the View menu. Refresh the mailbox display using the Refresh command in the View menu, or by clicking the Refresh button (the one with the two arrows).

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

Viewing Mailboxes

To view mailboxes in a domain, enter a name filter in the **Mailbox mask** field and click **Find**. For example, to list all mailboxes enter the wildcard (*****) character; to list only mailboxes that begin with **j**, enter **j*** in this field. After you click **Find**, the list of mailboxes that match the naming criteria in the current domain will be displayed.

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

You can create a new Registry Mailbox by selecting the **Add Registry Mailbox** button on the toolbar. This will create a new icon in the list and position the cursor next to the icon. Type the name of the new mailbox directly into the textbox.

Add NT Mailbox

You can create a new NT Mailbox by selecting the **Add NT Mailbox** button on the toolbar. This will display a form with a list of NT Users that do not already have a mailbox on the target server

Add Database Mailbox

You can create a new Database Mailbox by selecting the **Add Database Mailbox** button on the toolbar. This will display a form with a list of Database Users.

Add SQL Mailbox

You can create a new SQL Mailbox by selecting the Add SQL Mailbox button on the toolbar. This will display a dialog for setting the mailbox name.

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

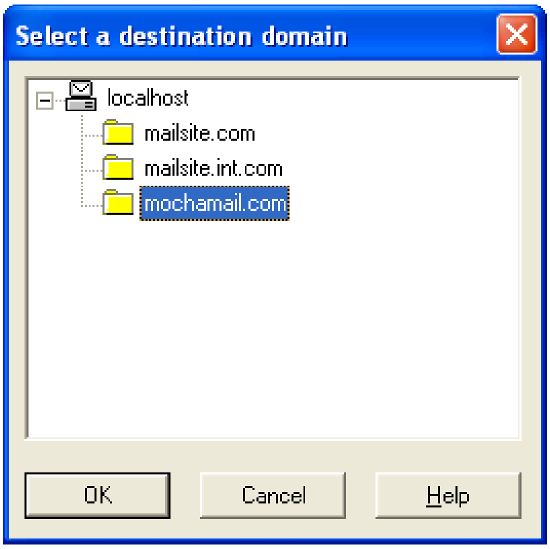
You can rename a Registry or SQL mailbox by selecting the icon with a single click, then clicking once on the mailbox name. You cannot rename an NT Mailbox. Use the User Manager to manage local users instead.

Deleting a Mailbox

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

Move or Copy Mailbox

Use this form to move or copy a mailbox to a different domain.



You can move the selected mailboxes to another domain. Select the destination domain and click **OK**.

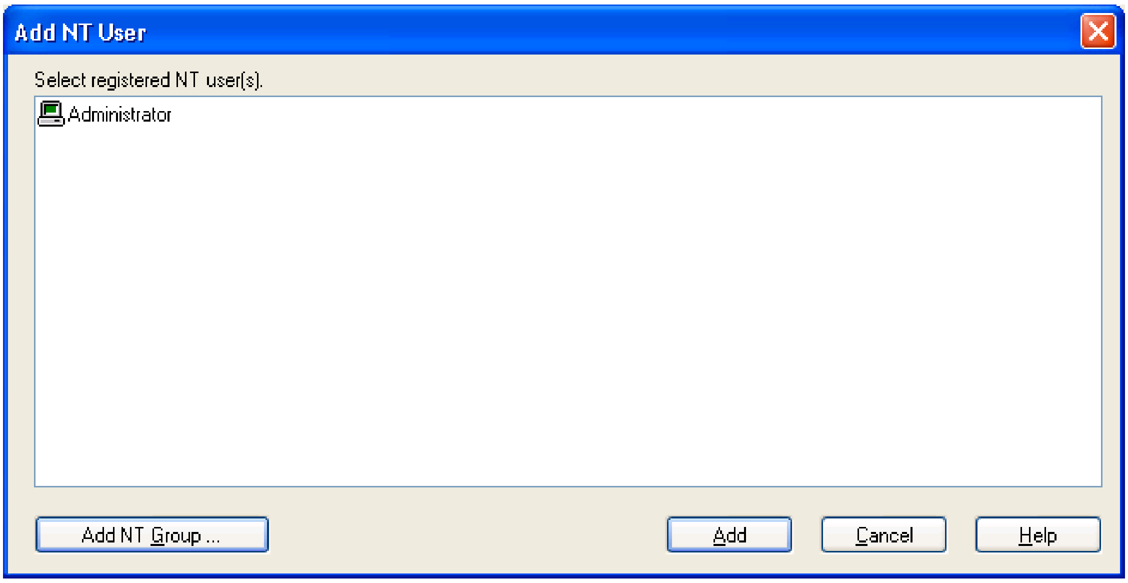
You can choose to move the mailbox directory. The directory will be moved under the **~virtual.domain** subdirectory. Note that this will not work if you are running the Console remotely, or if the directory is active. If the directory move fails, you can use **XCOPY** to manually move the files.

Move or Copy Directory

Select this option to move the associated directory.

Add NT User

Use this form to select Users for creating NT mailboxes.



This form contains a list of NT Users that can be used to create mailboxes. Previously defined users will not appear.

Users identified by the computer icon are Local Users. This means that the account has been created in the User Manager on your MailSite server.

Users identified by the server icon are Domain Users. This means that the account has been created on the Domain Controller to which your MailSite server belongs.

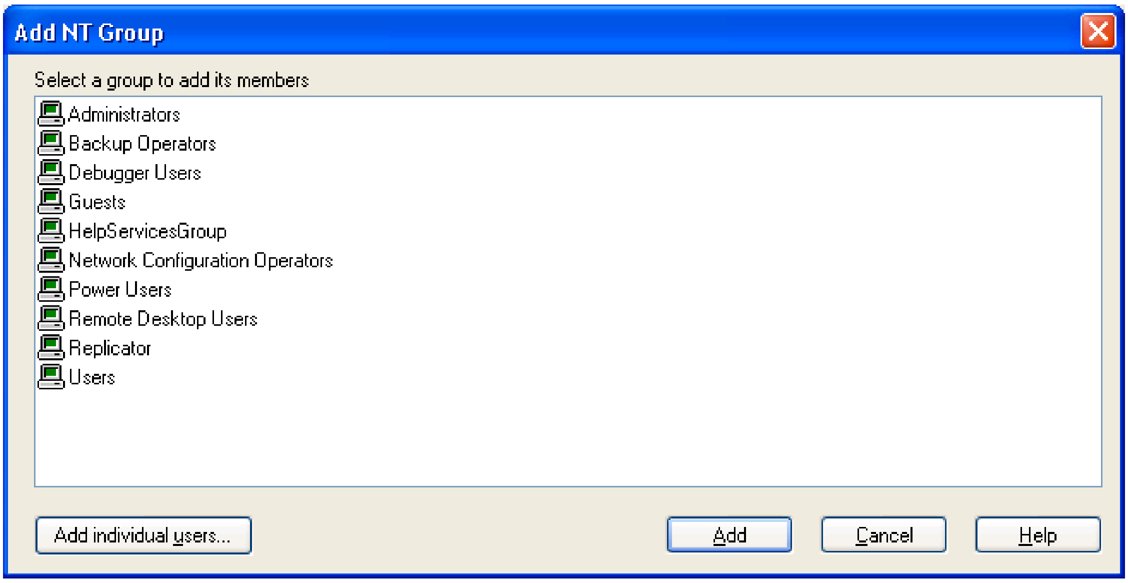
Select one or more Windows NT user that you wish to enable for sending and receiving mail. Use the **`Shift`** and **`Control`** keys to select multiple users.

Note that it is not a good idea to select NT user names containing spaces or underlines. Although MailSite will handle such names correctly, many mail clients and other mail software will have problems. Enclosing the name in double quotes when sending mail to it, such as **`"Fred Jones"@abc.com`**, may help, but such names are better avoided altogether.

You can create mailboxes for members of a NT Group by clicking on the **`Add NT Group`** button. You can automatically create NT mailboxes. See the section on the NT Mailbox Plugin for more information.

Add NT Group

Use this form to select a Group for creating NT mailboxes.



Select a group to add its members

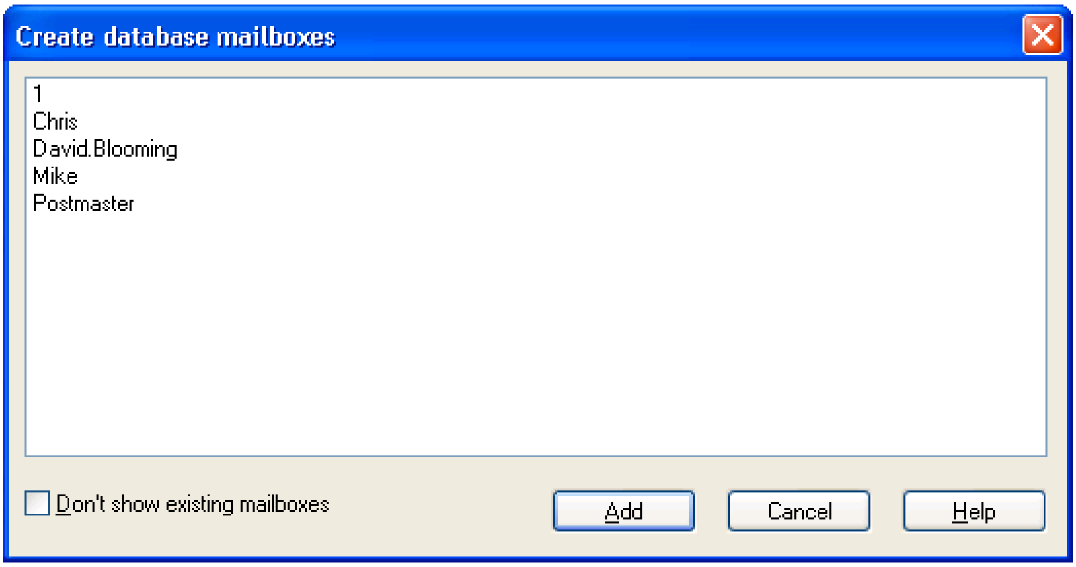
- Administrators
- Backup Operators
- Debugger Users
- Guests
- HelpServicesGroup
- Network Configuration Operators
- Power Users
- Remote Desktop Users
- Replicator
- Users

You can create mailboxes for all users in an NT Group by selecting the group and clicking on the **Add** button. You can automatically create NT mailboxes. See the section on the NT Mailbox Plugin for more information.

If you wish to create mailboxes for individual NT Users, select the `Add Individual Users` button.

Create Database Mailboxes

Use this form to display a list of candidate database users for creating mailboxes.



1
Chris
David.Blooming
Mike
Postmaster

□ Don't show existing mailboxes

The list of mailboxes is retrieved from the database that you configured in the Database Mailbox Plugin Configuration. You can automatically create database mailboxes. See the section on configuring the Database Mailbox Plugin for more information.

Mailbox List

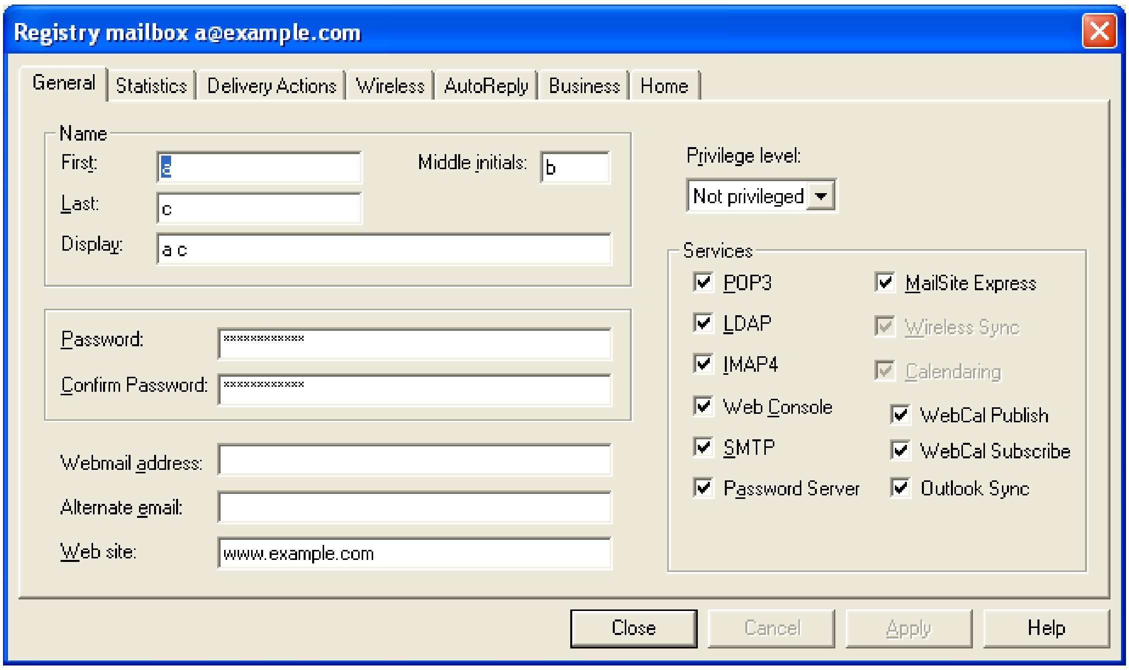
If your database is configured correctly, a list of users will be displayed. You can select one or more users by using the **`Ctrl`** and **`Shift`** keys. Click **`Add`** to create mailboxes for the selected users.

Don't Show Existing Mailboxes

Select this option to remove existing mailboxes from the list of users.

Mailbox General Page

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



Registry mailbox a@example.com

Name

First: a

Middle initials: b

Last: c

Display: a c

Password: *************

Confirm Password: *************

Webmail address:

Alternate email:

Web site: www.example.com

Privilege level: Not privileged

Services

☑ POP3

☑ LDAP

☑ IMAP4

☑ Web Console

☑ SMTP

☑ Password Server

☑ MailSite Express

☑ Wireless Sync

☑ Calendaring

☑ WebCal Publish

☑ WebCal Subscribe

☑ Outlook Sync

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

You can change the password for this mailbox by entering a new value here. You must retype the password in the confirmation field. Note that changing the password for NT Mailboxes will change the user's password in the NT User Database. Passwords are limited to 14 characters to maintain consistency with the Windows NT limit.

Confirm Password

Re-enter the new password to confirm the change. Note that passwords are limited to 14 characters to maintain consistency with the Windows NT limit.

Webmail Address

Enter an alternate e-mail address for the user. MailSite Express will use this address as the Reply-To: address when sending email. MailSite ExpressPro supports multiple personalities and this will be one of the offered addresses.

Alternate Email

Enter an alternate e-mail address for the person who will use this mailbox. This address will be displayed in LDAP properties for this account. Note that this address is not used for any delivery or forwarding of email.

Web Site

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

Privilege Level

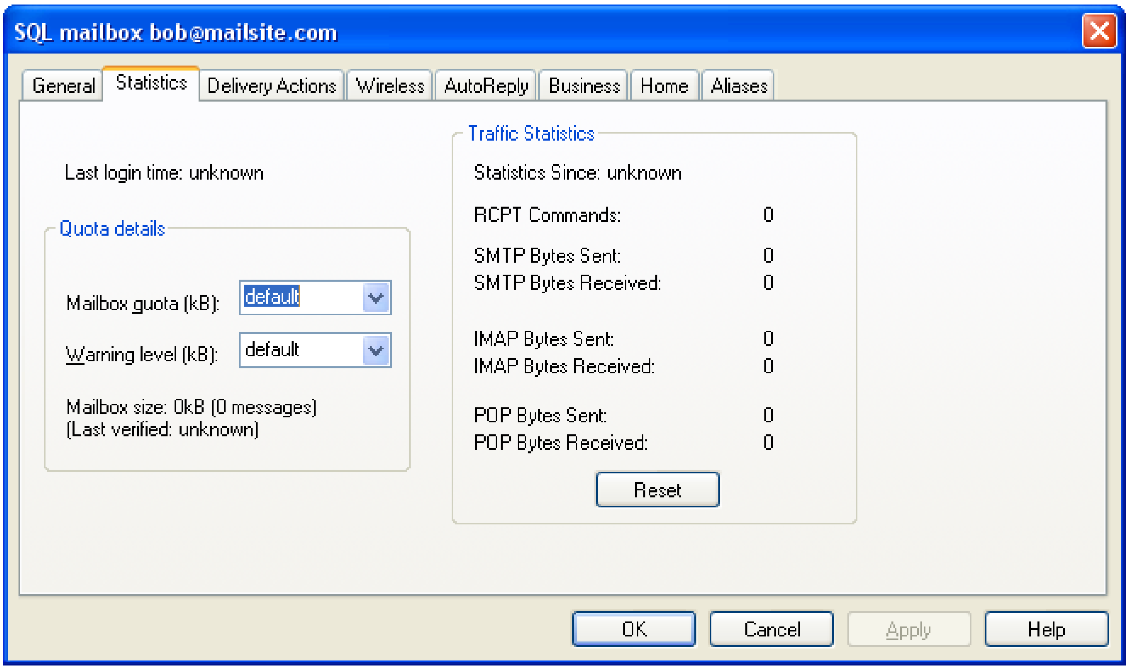
The Privilege Level determines your administrative privilege on the server. The choices are None, Domain and Server. If set to None, the user will only be able to control his own mailbox. If set to Domain, the user can manage other mailboxes in that domain. If set to Server, the user may manage all mailboxes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



SQL mailbox bob@mailsite.com

Last login time: unknown

Quota details

Mailbox quota (kB): default

Warning level (kB): default

Mailbox size: 0kB (0 messages)
(Last verified: unknown)

Traffic Statistics

Statistics Since: unknown

RCPT Commands:	0
SMTP Bytes Sent:	0
SMTP Bytes Received:	0
IMAP Bytes Sent:	0
IMAP Bytes Received:	0
POP Bytes Sent:	0
POP Bytes Received:	0

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.

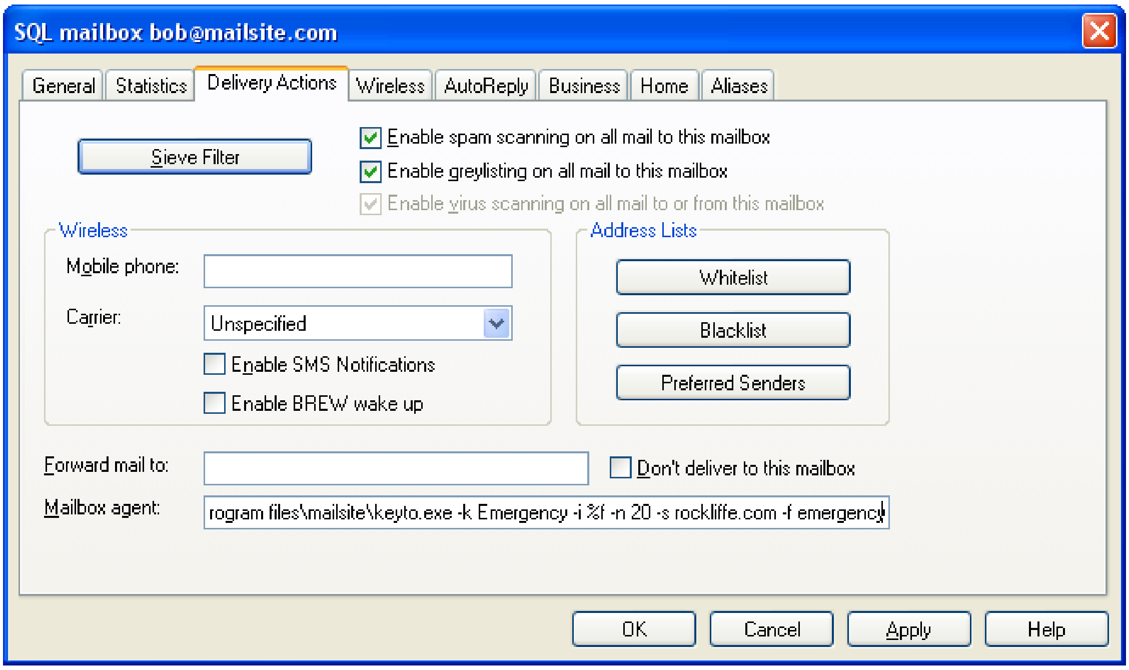
Traffic Statistics

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.



☑ Enable spam scanning on all mail to this mailbox

☑ Enable greylisting on all mail to this mailbox

☑ Enable virus scanning on all mail to or from this mailbox

Wireless

Mobile phone:

Carrier: Unspecified

□ Enable SMS Notifications

□ Enable BREW wake up

Address Lists

Forward mail to:

□ Don't deliver to this mailbox

Mailbox agent: rogram files\mailsite\keyto.exe -k Emergency -i %f -n 20 -s rockliffe.com -f emergency

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`

The Eudora2Go service uses a differently formatted message to other SMTP to SMS gateways in order that the cellular phone will wake the BREW application. This should be left unchecked for all other systems at present. This option is not exposed in MailSite Express by default meaning that end users cannot enable it.

`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:

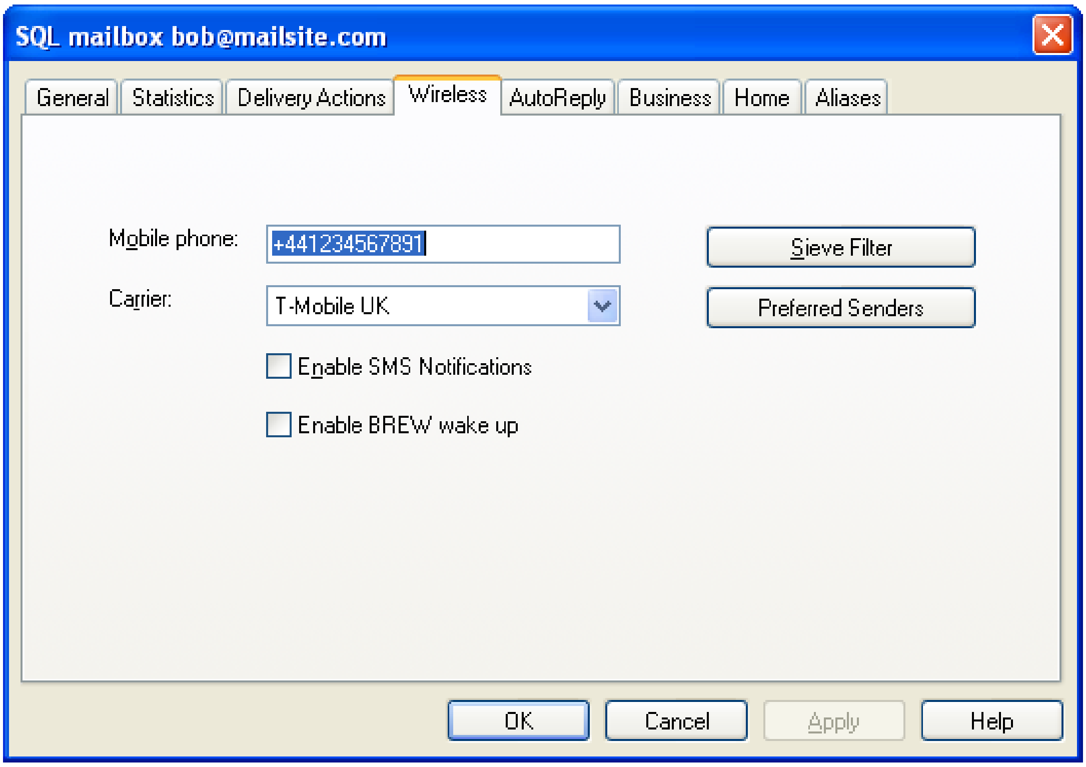
Special symbols	**Replaced by**
`%f`	Full file name of the message which was received
`%u`	Name of the mailbox
`%h`	Mailbox directory
`%d`	Domain to which the mailbox belongs
`%%`	Single percent character

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.



SQL mailbox bob@mailsite.com

Mobile phone: +441234567891

Carrier: T-Mobile UK

□ Enable SMS Notifications

□ Enable BREW wake up

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

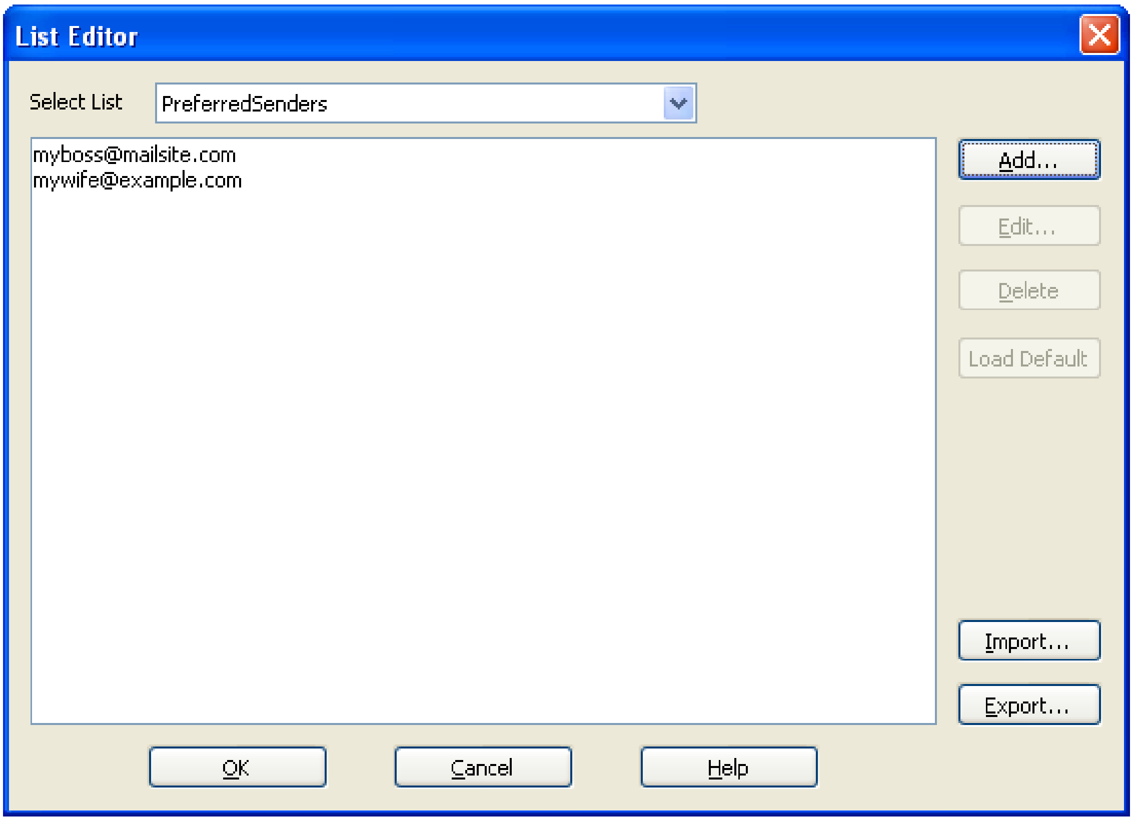
The Eudora2Go service uses a differently formatted message to other SMTP to SMS gateways in order that the cellular phone will wake the BREW application. This should be left unchecked for all other systems at present. This option is not exposed in MailSite Express by default meaning that end users cannot enable it.

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.



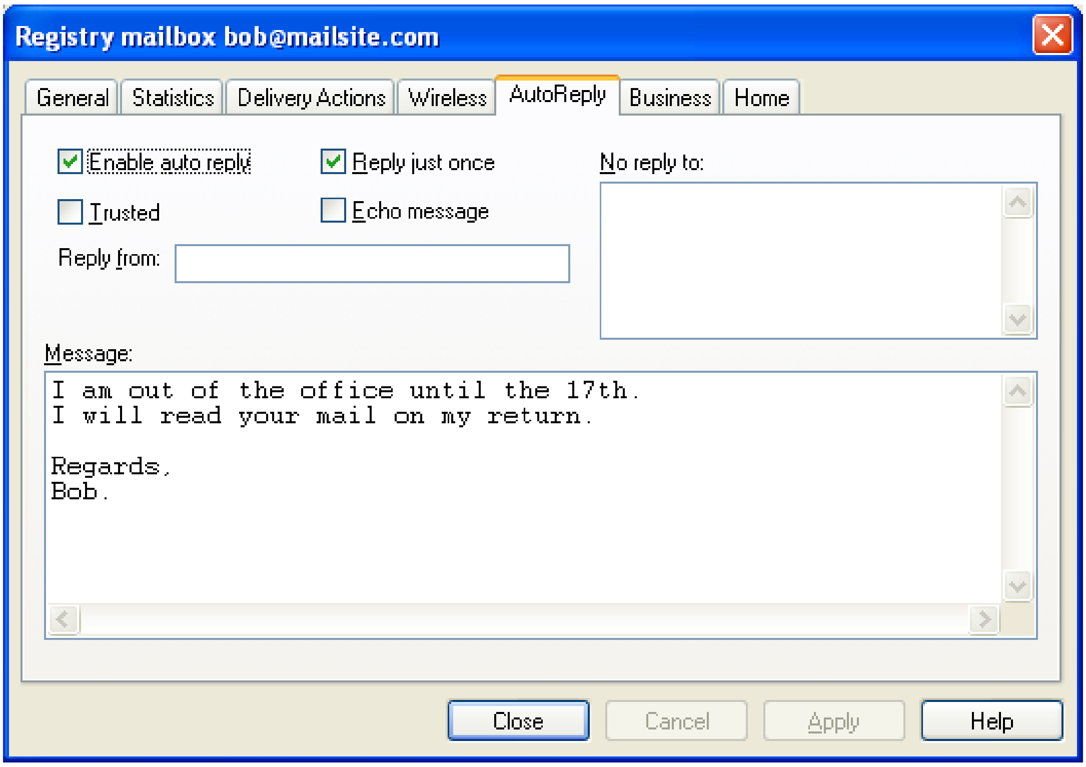
Select List: PreferredSenders

myboss@mailsite.com
mywife@example.com

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.



☑ Enable auto reply

☑ Reply just once

No reply to:

□ Trusted

□ Echo message

Reply from:

Message:

```
I am out of the office until the 17th.
I will read your mail on my return.

Regards,
Bob.
```

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

Select this field to ensure that no sender receives more than one auto reply. When this is checked, MailSite will append the e-mail address to which it replies to within either the registry or the SQL database within the mailbox property **AlreadyRepliedTo** and is deleted when the EnableAutoReply is reset. For performance reasons this property is limited to 10,000 entries.

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. Hold the **Ctrl** key and 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. Hold the **`Ctrl`** key and 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:

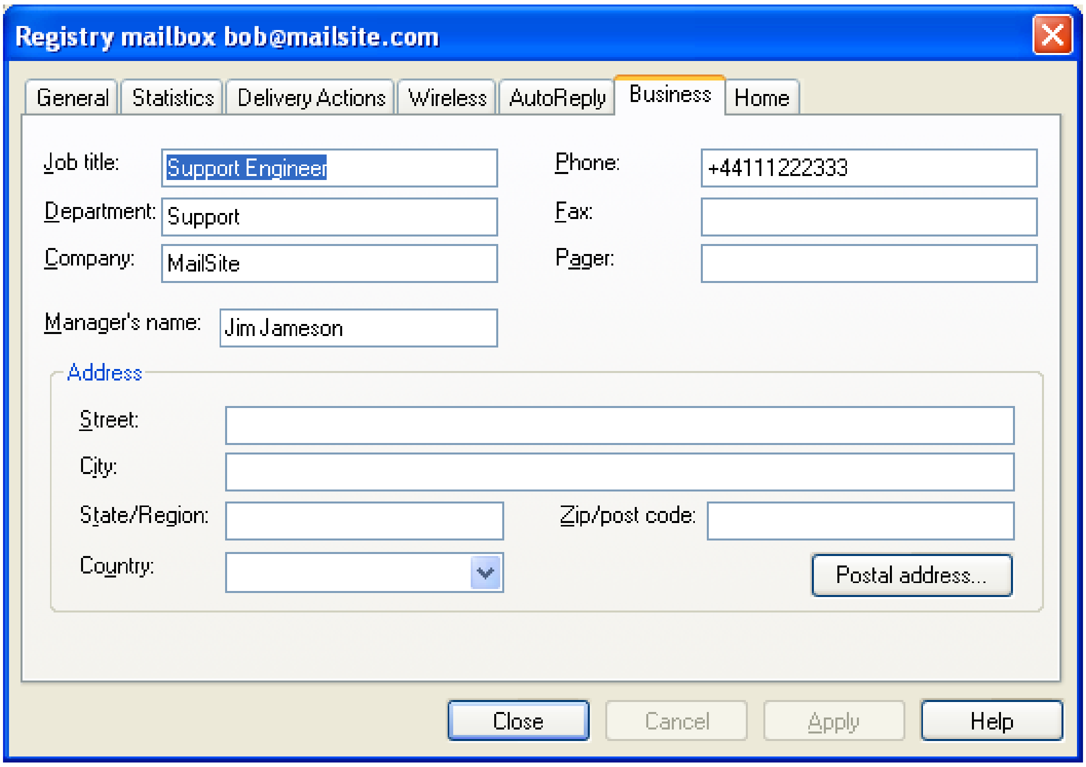
Directive	Replacement text
`%ADDRESS`	The e-mail address of the person who sent the original message
`%DATE`	The current date
`%TIME`	The current time
`%INCLUDE(filename)`	The contents of the filename (which must be located in the mailbox's **`INBOX`** directory, unless the mailbox is trusted)
`%EXECUTE(commandline)`	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 business address for this mailbox. The LDAP Service returns this information in response to directory searches.



Job title: Support Engineer

Department: Support

Company: MailSite

Manager's name: Jim Jameson

Phone: +44111222333

Fax:

Pager:

Street:

City:

State/Region:

Zip/post code:

Country:

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`

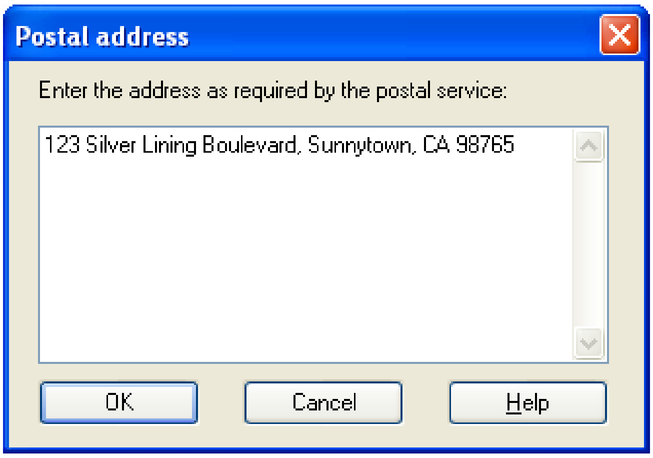
Enter the business zip or post code address of the person who will use this mailbox.

`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. The LDAP Service will return this information in response to directory searches.



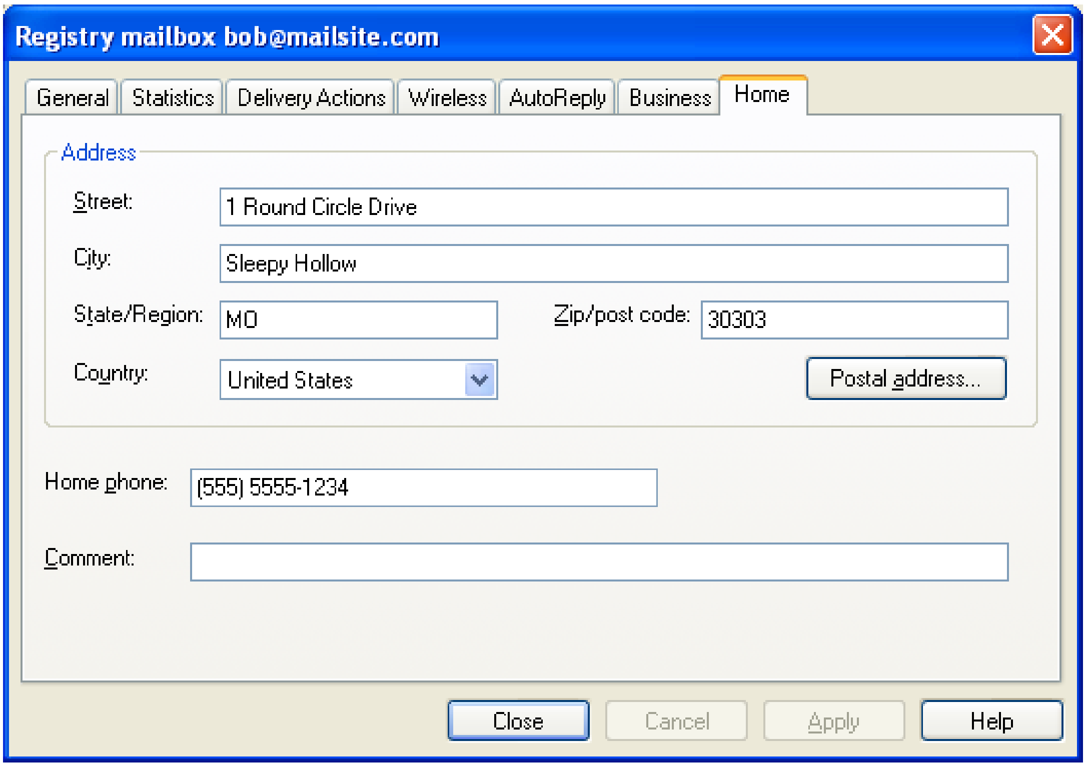
Enter the address as required by the postal service:

123 Silver Lining Boulevard, Sunnytown, CA 98765

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. The LDAP Service will return this information in response to directory searches.



Street: 1 Round Circle Drive

City: Sleepy Hollow

State/Region: MO

Zip/post code: 30303

Country: United States

Home phone: (555) 5555-1234

Comment:

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

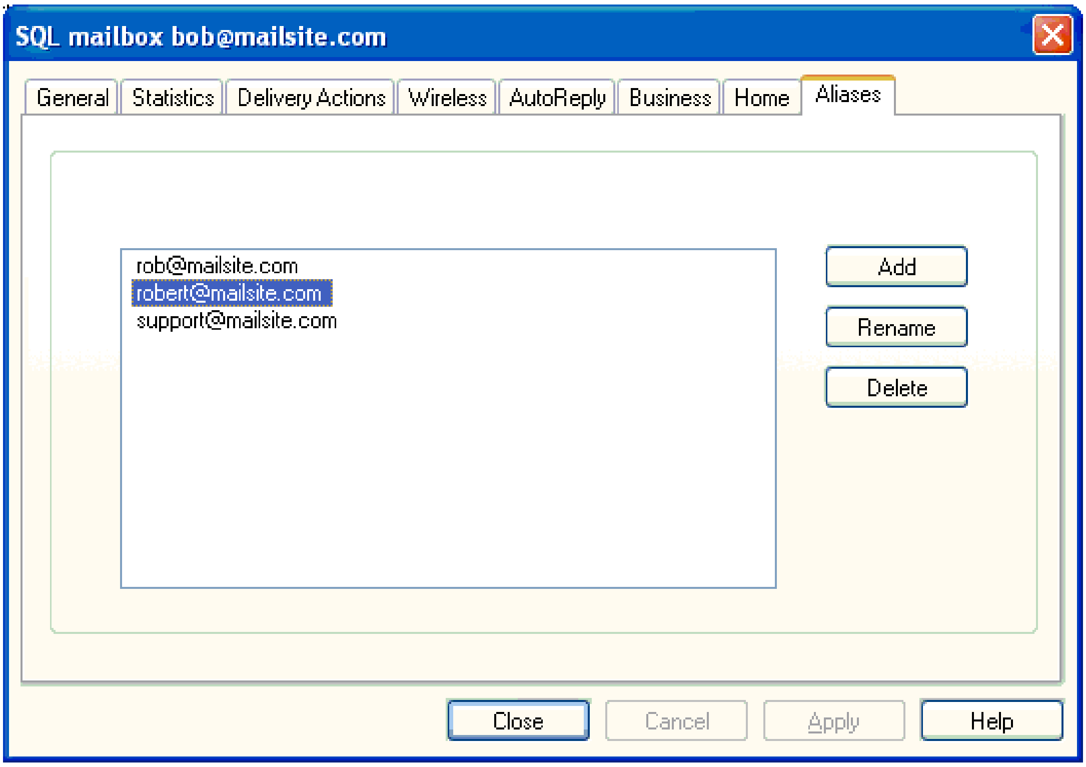
Enter the home phone number of the person who will use this mailbox.

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:



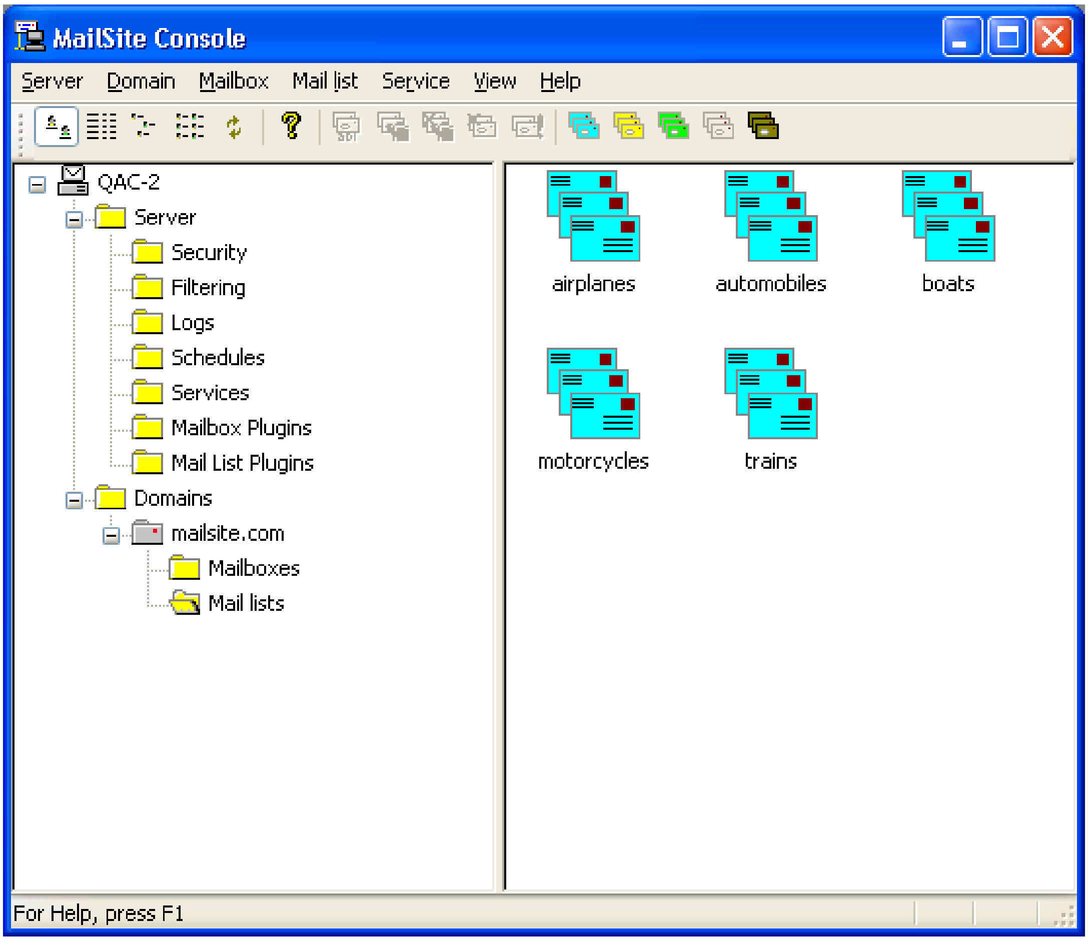
rob@mailsite.com
robert@mailsite.com
support@mailsite.com

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 the Mail Lists folder to display a list of mail lists in the right-hand pane:



You can select the type of mail list display in the right-hand panel using one of the four leftmost buttons in the toolbar, or by using the View menu. Refresh the mail list display using the **`Refresh`** command in the View menu, or by clicking the **`Refresh`** button (the one with the two arrows).

To create a new list, click on the appropriate button in the toolbar. Type the name of the new list in the edit field and press **`Enter.`**

New Registry List

You can create a new Registry List by selecting the **`Add Registry List`** button on the toolbar. Only supported when the Registry Connector is configured.

New SQL List

You can create a new SQL List by selecting the **`Add SQL List`** button on the toolbar. Only supported when SQL Connector is configured.

New NT List

You can create a new NT List by selecting the **Add NT List** button on the toolbar.

New File List

You can create a new Text File List by selecting the **Add File List** button on the toolbar.

New Database List

You can create a new Database List by selecting the **Add Database List** button on the toolbar.

New Server List

You can create a new Server List by selecting the **Add Server List** button on the toolbar.

Rename a List

To rename a Mail List, select its icon with a single click and then click once on the list name. Type the new name and press **Enter**.

Delete a List

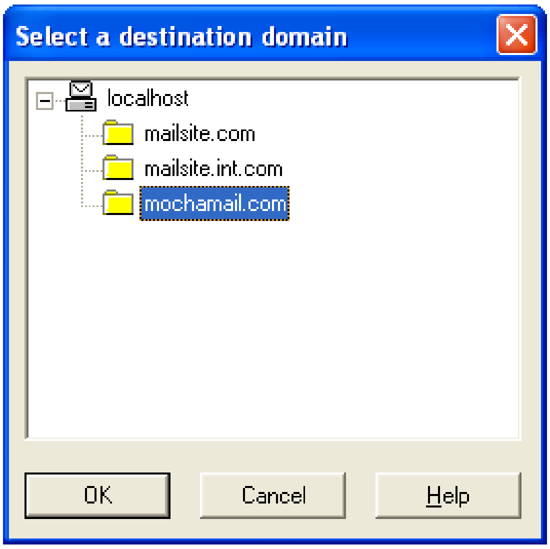
To delete a Mail List, select its icon and click on the **Delete** button.

Configure a List

You can maintain the properties of a List by double clicking on the icon for the list. This will open the **Properties** form.

Move or Copy a List

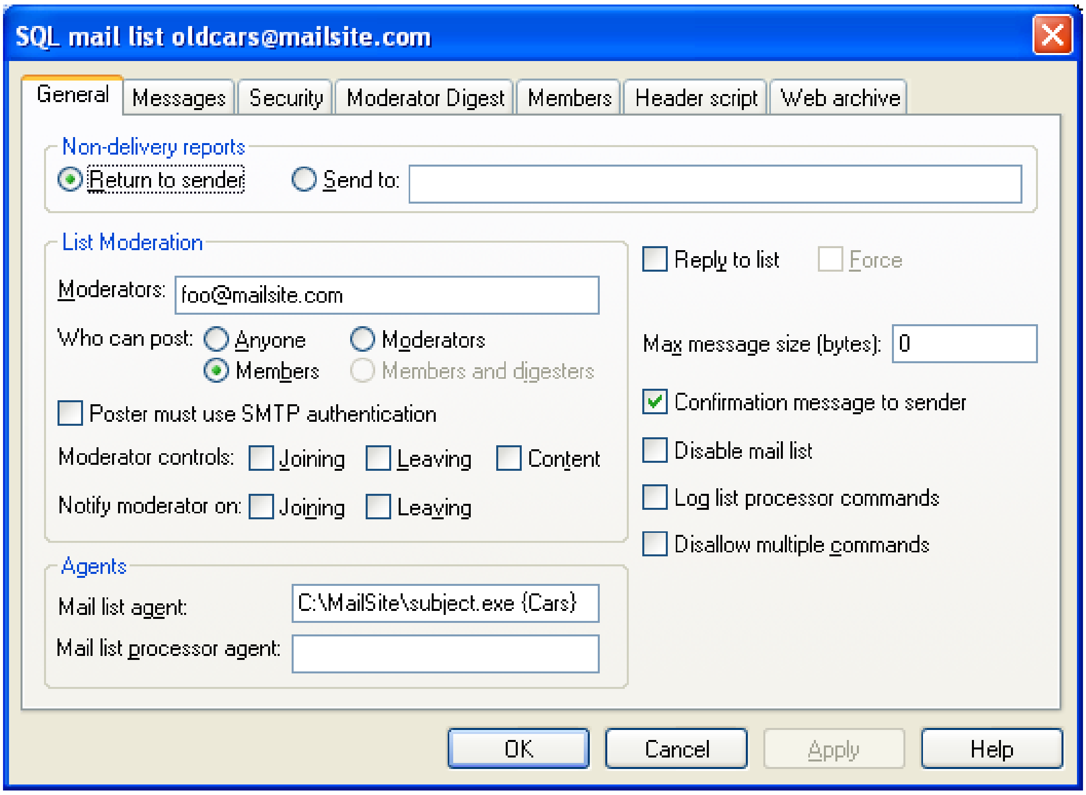
To move or copy a mail list to a different domain, select one or more mail list icons and then choose Move or Copy from the Mail List menu (or click the corresponding toolbar button, or select Move from the right-click popup menu). The Destination Domain dialog allows you to select a new location for the selected mail lists.



If you are running the MailSite Console on the same machine as the MailSite Engine (in other words you are not administering MailSite remotely), and you are simply moving the mail list to another domain on the same machine, then the Console will give you the option of moving or copying the mail list directories as well (if they exist). However, if you are running the Console remotely, or if you are moving or copying the mail list to another machine, you will have to manually move the directories yourself.

List General Page

Use this form to configure the general list properties.



SQL mail list oldcars@mailsite.com

Non-delivery reports

● Return to sender ○ Send to:

List Moderation

Moderators: foo@mailsite.com

Who can post: ○ Anyone ○ Moderators ● Members ○ Members and digesters

□ Poster must use SMTP authentication

Moderator controls: □ Joining □ Leaving □ Content

Notify moderator on: □ Joining □ Leaving

Agents

Mail list agent: C:\MailSite\subject.exe {Cars}

Mail list processor agent:

□ Reply to list □ Force

Max message size (bytes): 0

☑ Confirmation message to sender

□ Disable mail list

□ Log list processor commands

□ Disallow multiple commands

Non Delivery Reports

This specifies what action should be taken if a message to an address on the Mail List cannot be delivered. The options are:

⇒ Return to sender with a non-delivery report (the default)

⇒ Send to the non-delivery report to a specified e-mail address

Moderators

Enter the Internet mail address of the moderator(s) for this list. You can specify multiple moderator addresses for a mailing list, just separate each address by commas. Each moderator must have a mailbox on your site.

If a list is not moderated, anyone can join or leave the list by sending a message with **JOIN** or **LEAVE** in its body to the **-request** address of the list.   The moderator (s) can control who can join the list, who can leave it, and may also control posting to the list.

Who Can Post

A list can be configured to allow various people to post messages to the list. By default, only members can post, but you can select any of four posting policies:

- **Anyone** specifies that any email user can post a message to the list
- **Members** specifies that only users with addresses listed in the Members page can post.
- **Moderators** specifies that only the list moderators can post.

- **`Members and Digesters`** specifies that both members of the list and members of the associated digest list can post.

Poster must use SMTP authentication

This option specifies that only users with mailboxes on the local system can post to the list. When this option is enabled, senders must a login name and password via SMTP authentication to successfully post a message; if SMTP authentication is not used, or if the given name and password do not match a local mailbox, the posting will be denied.

Moderator Controls

These fields define the degree of control exercised by the list moderator.

- **`Joining`** specifies that subscription (**`JOIN`**) requests are forwarded to the moderator for approval.
- **`Leaving`** specifies that unsubscription (**`LEAVE`**) requests are forwarded to the moderator for approval.
- **`Content`** specifies that any messages to this list will be stored in a **`pending`** directory, and will only be released to the mail list when the moderator has approved them. A more detailed guide *Customizing the MailSite Web Console* is available for download from the MailSite website.

Notify Moderator

These fields define whether moderators are notified when users join or leave the list.

- **`Joining`** specifies that the moderator will be notified when new members join by e-mail.
- **`Leaving`** specifies that the moderator will be notified when of the face by e-mail.

Reply To List

Check this field to add a **`Reply-to:`** header to each list message. This is useful when recipients reply to list messages. Replies to list messages will be addressed to the list, rather than to the originator.

The exception is that if the incoming message already has a **`Reply-to`**: header, that header is left untouched and no additional **`Reply-to`**: header is added. You can force the list to overwrite an existing **`Reply-to`**: header with the **`Force`** option.

Force

If you select this option, MailSite will discard any **`Reply-to`**: headers in an incoming message and will add the mail list's own **`Reply-to`**: header.

You can use Header Processing for more advanced editing of message headers.

Maximum Message Size

A list may be configured to reject messages greater than a certain size. Large messages sent to the list will generate a non-delivery report to the sender saying why the message was not acceptable. A value of zero (the default) means that no size limit is applied.

Mail List Agent

This feature allows a command line to be executed when a new message arrives for the list or for the list-request processor. 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 on the command line you specify before it is executed:

Special symbol	Replaced by
`%f`	Full file name of the message which was received
`%m`	Moderator address of the mailing list, or **-** if no moderator
`%n`	Name of the mailing list

%d	Domain to which the mailing list belongs
%%	Single percent character

The message file **%f** will be located in the mail list directory, but will not have a **MSG** extension. The external program may change the contents of the message or may delete the file. When the external program completes, MailSite will automatically rename the file (if it still exists) to have a **MSG** extension, and will continue processing as normal.

For more information, see the section on List Agents.

Disable Mail List

This option disables the entire list. This is useful if you wish to retain the list configuration but wish to hide the list for security purposes.

Confirmation Message To Sender

Check this box to send a confirmation message to the sender. The confirmation message contains a copy of the message that was delivered 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 you do not check this option then no confirmation will be sent. If the sender is a member of the list, she will receive a copy of her message by virtue of that membership.

This option will guarantee that third party out of office auto-responders will not create mail list *loops*. By default, this option is checked.

Log List Processor Commands

If you select this option MailSite will log commands that are sent to the **list-request** address. It will record the log information in a file called **CMDLOG.TXT**, located in the list-request directory. Note that this file is not cycled and MailSite keeps appending to it. Therefore, you should remember to delete the file every so often, to ensure you don't run out of disk space.

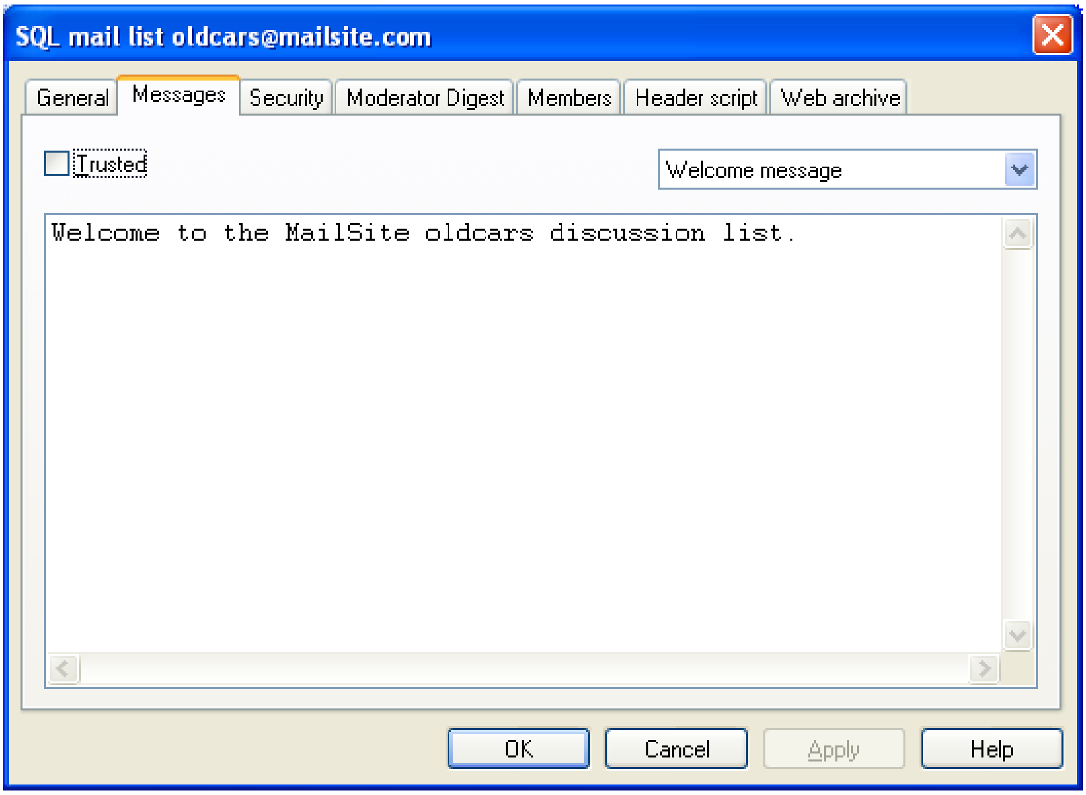
Disallow Multiple Commands

This option is provided to help list users who may be relatively unfamiliar with list processors. Select this option to process only the first command in messages that are sent to the **list-request** address. This means that users do not need to disable their e-mail *signature*, ensuring that any accidental coincidence of signature lines with valid list processor commands is harmless.

If you enable multiple commands by turning off this option, all lines (up to the end of the message or to a **STOP** command) are processed.

List Messages Page

Use this form to configure messages for this list.



□ Trusted

Welcome message

```
Welcome to the MailSite oldcars discussion list.
```

You can configure a list to send a custom Welcome message when someone joins. Similarly, you can send a custom Goodbye message when someone leaves. Someone who sends a **HELP** command to the mailing list processor can also be sent a custom help message. To configure these messages, select the message category from the drop-down list. Type in a short message in the text window.

Message Category

You can create custom messages that the list processor sends in response to different commands:

- **Welcome Message**, which is sent when someone **JOIN**s or **SUBSCRIBE**s to the list.
- **Goodbye Message**, which is sent when someone **LEAVE**s or **UNSUBSCRIBE**s to the list.
- **Message Prolog**, which is inserted at the beginning of each list message.
- **Message Postscript**, which is appended to the end of each list message.
- **Help Message**, which is sent in response to the **HELP** command.

List Message Text

Enter the text that you would like the list command processor to return to the sender. Use message directives for advanced message processing.

If you want to put a large amount of text into your message, use the **%INCLUDE** directive, rather than typing text into the configuration console directly. This is to save space in the Registry. In fact, you will find that the configuration console will only accept a relatively small amount of text; enough for a short message and a few directives.

Message Prologs and Postscripts

You can arrange for each message sent to the list to have a prolog or postscript added. This is very useful for reminding list members how to leave the list. Use the corresponding dropdown items in the Messages page in the list properties form to set this up.

You may use the same message directives as for Welcome and Goodbye messages, but the **%ADDRESS** directive will be replaced by the address of the mailing list, not the address of an individual recipient. Other remarks in the preceding section also apply to prologs and postscripts.

If a message to a mail list contains a MIME **Content-type:** header, and the content type is not text/plain, neither the prolog nor the postscript will be added. This is to avoid corrupting data such as image, movie, etc.

List Message Directives

The message that you type in can contain directives, which are replaced by other text when the message is actually sent. The full list of directives is as follows:

Directive	Replacement text
%ADDRESS	The e-mail address of the person joining or leaving the list or sending the HELP command
%DATE	The current date
%TIME	The current time
%INCLUDE(filename)	The contents of the filename
%EXECUTE(commandline)	The output produced by executing the command line (trusted mailing lists only)
%%	A single percent character

The operation of the **%INCLUDE** directive depends on the **Trusted** setting. If the list is trusted, then the filename should be the full path to a file that is accessible to the mail server. If the list is not trusted, only files located in the mailing list directory can be included—in this case, the filename should be specified as a relative path and not a full path.

The **%EXECUTE** directive only works for **Trusted** lists. The **commandline** parameter can specify any command or batch file.

List Message Directive Examples

Some examples may help to explain message directives. Suppose a Welcome message for a list **discuss@abc.com** (which is not trusted) contains the following text:

```
Welcome to the discuss@abc.com mailing list!

You have subscribed to the list as %ADDRESS - please remember to unsubscribe
using the same address.

%INCLUDE(purpose.txt)

Thank you for joining.  Enjoy the list!
```

When a user joins the list, she will be sent a welcome message containing the above text, with the directives replaced as described above. The file **purpose.txt** (which presumably contains some information about the purpose of the list) must be located on the mail server in the directory **lists\~abc.com\discuss** (or, if **abc.com** is the default domain, in directory **lists\discuss**).

Suppose a Goodbye message for the list **discuss@abc.com** (which we'll assume is trusted) contains:

```
Thank you for using this list.
%EXECUTE(c:\myutils\goodbye %ADDRESS)
Bye!
```

When a user leaves this list, she will receive a Goodbye message containing the above text, with the **%EXECUTE** directive replaced by the output of the program **c:\myutils\goodbye**. Note that the **%ADDRESS** is replaced by the user's e-mail address and passed to the program as a command-line argument. Only the **%ADDRESS** directive can be used in this way, and only with the **%EXECUTE** directive.

Only console programs (that is, programs which you would run from the operating system command line) can be used with the **%EXECUTE** directive. Batch files, interactive programs which prompt for user input, or programs that have a windowed user interface will not work.

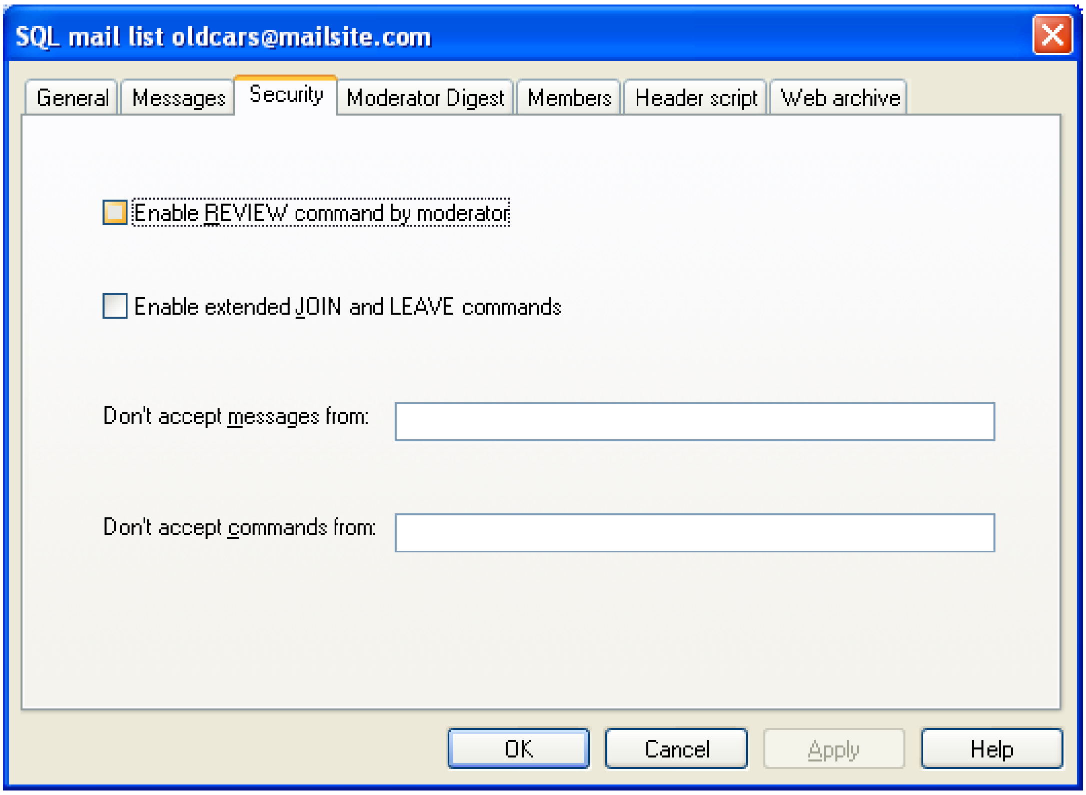
Suppose a message containing the command **HELP** is sent to **discuss-request@abc.com** (as before, we'll assume list **discuss** is trusted). If the configurable help message for the list contains:

```
%INCLUDE(c:\special\place\abchelp.txt)
```

The response from the mailing list processor will be a message that includes the specified file. Note that if no help message is configured, a built-in default message will be sent as part of the normal command response (the journal message).

List Security Page

Use this page to configure the security settings for this list.



SQL mail list oldcars@mailsite.com

□ Enable REVIEW command by moderator

□ Enable extended JOIN and LEAVE commands

Don't accept messages from:

Don't accept commands from:

Enable REVIEW Command by Moderator

If you are the moderator of a mailing list, you may use the **REVIEW** command in a message to the list-request address. The server will respond with a message containing a list of all current members.

Because list membership is potentially confidential, and because it is relatively easy to forge e-mail addresses, the **REVIEW** command is disabled by default.

Enable Extended JOIN and LEAVE Commands

Following the list name in the **JOIN** and **LEAVE** commands, you can specify a full e-mail address, in any valid RFC822 form. This extended form of the **JOIN** and **LEAVE** command is disabled by default.

As for other Mail List Commands, send an email in plain text format to list-request@domain.com with a command such as “JOIN list username@example.com” as the only line in the body.

Here are some example extended **JOIN** and **LEAVE** commands. Note that **SUBSCRIBE** and **UNSUBSCRIBE** are recognized synonyms.

```
JOIN thelist "John Smith" jsmith@myco.co.uk
LEAVE thelist smith@domain.com (Joe Smith)
SUBSCRIBE thelist Jane Doe <janed@super-isp.net>
UNSUBSCRIBE thelist peter@my-university.edu
```

Don't Accept Messages From

Enter a list of addresses that you want to block from this list. Separate each address with a comma.

The syntax for these fields is:

⇒ **addressmask, addressmask, addressmask,...**

where **addressmask** can be an e-mail address, possibly containing a wildcard asterisk (*****). You can also have an exclamation mark (**!**) in front of an **addressmask**, indicating that matching addresses don't belong in the excluded list. The list is processed from left to right.

Don't Accept Commands From

Enter a list of addresses that you want to block from this list-request processor. Separate each address with a comma.

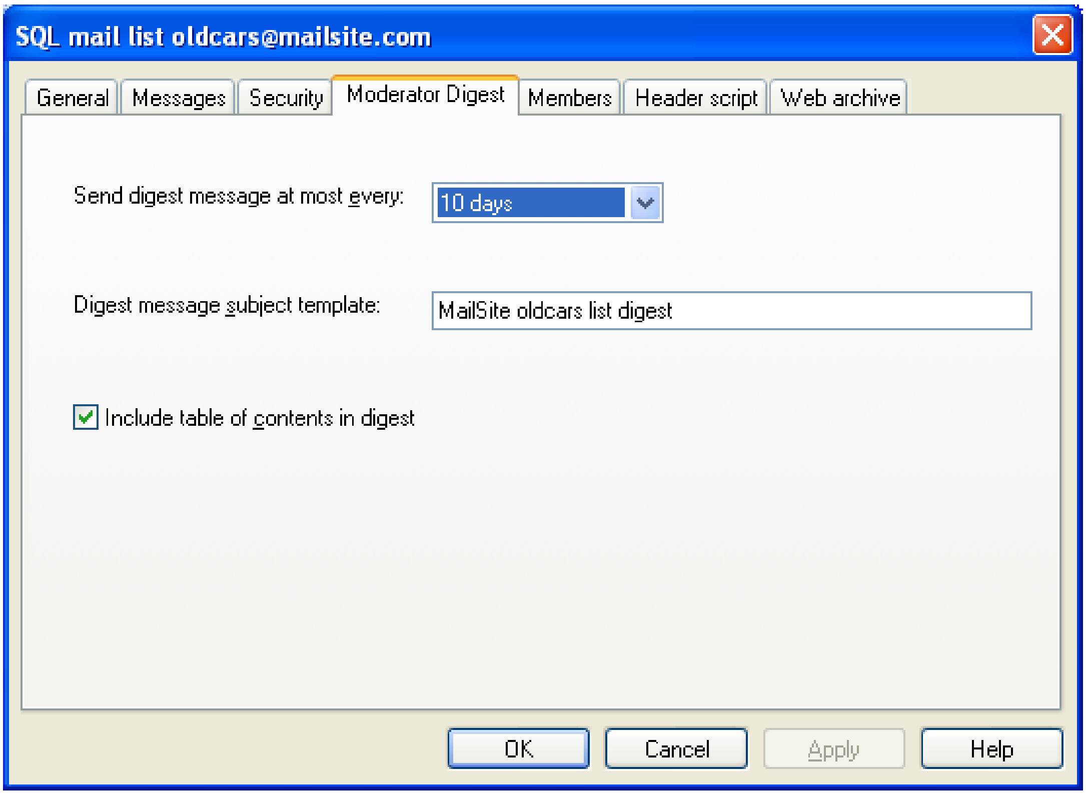
The syntax for these fields is:

⇒ **addressmask, addressmask, addressmask,...**

where **addressmask** can be an e-mail address, possibly containing a wildcard asterisk (*****). You can also have an exclamation mark (**!**) in front of an **addressmask**, indicating that matching addresses don't belong in the excluded list. The list is processed from left to right.

Moderator Digest Page

Use this page to configure the moderator digest message that will be sent for this list.



Send digest message at most every: 10 days

Digest message subject template: MailSite oldcars list digest

☑ Include table of contents in digest

Many mailing lists allow unmoderated posts. For those where moderation is required, the moderator will receive a digest of the messages sent to the list over a configurable period.

Send digest message at most every

The digest frequency controls how long the digest accumulates messages for before it sends them out. The default is 1 day.

Digest Subject Template

You can specify the **`Subject`**: field of the messages sent out by the digest. To incorporate the date and time from when messages were accumulated, use the percent substitution variables defined below.

Variable	Replacement text
%a	Weekday name (abbreviated)
%A	Weekday name (full)
%b	Month name (abbreviated)
%B	Month name (full)
%c	"Short" date and time representation appropriate to the server's locale
%d	Day of the month as a two-digit number (01-31)
%H	Hour as a two-digit number (24-hour format: 00-23)
%I	Hour as a two-digit number (12-hour format: 00-11)

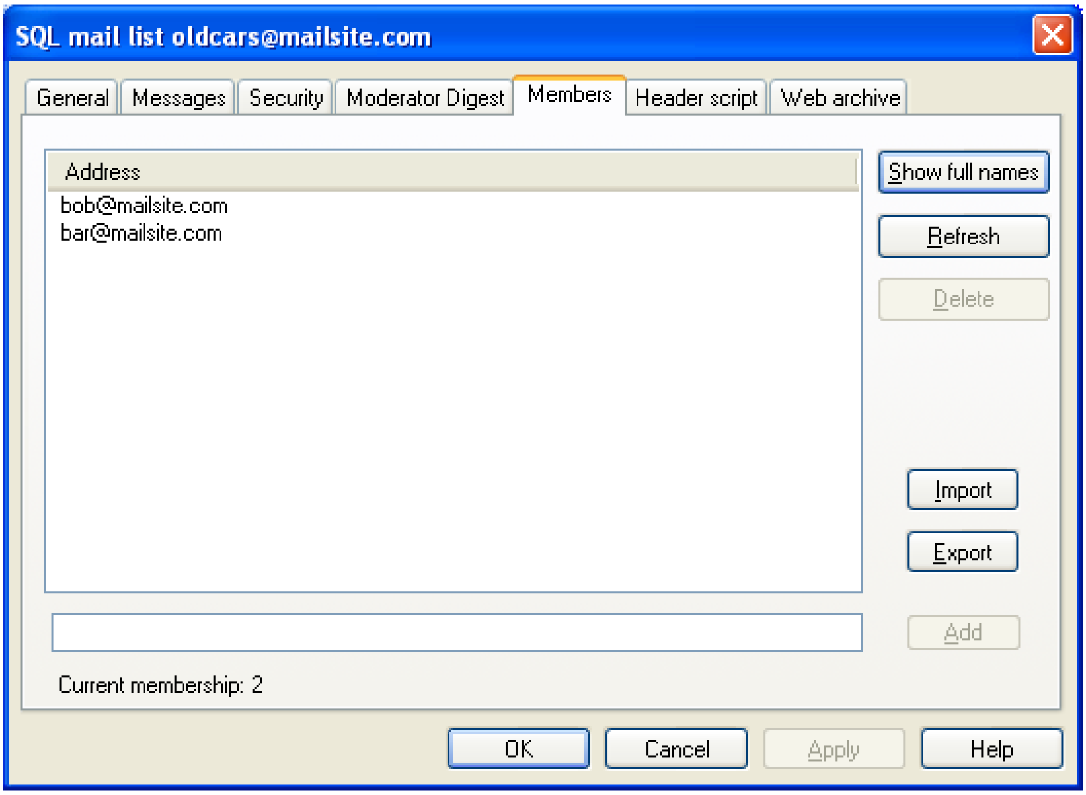
`%j`	Day of the year as a three-digit number (001-366)
`%m`	Month as a two-digit number (01-12)
`%M`	Minute as a two-digit number (00-59)
`%p`	AM/PM indicator (appropriate to server's locale) for a 12-hour clock
`%S`	Second as a two-digit number (00-59)
`%U`	Week of the year as a two-digit number (00-51), counting Sunday as the first day of the week
`%w`	Weekday as a single-digit number (0-6), counting Sunday as the first day of the week
`%W`	Week of the year as a two-digit number, with Monday as the first day of the week (00-51)
`%x`	"Short" date representation appropriate to server's locale
`%X`	Time representation appropriate to server's locale
`%y`	Year as a two-digit number (00-99)
`%Y`	Year as a four-digit number
`%z, %Z`	Server's time zone name or abbreviation; empty if the time zone is unknown

Include Table of Contents

Select this option to control whether the digest message will start with a table of contents.

List Members Page

Use this page to manage list membership.



bob@mailsite.com
bar@mailsite.com

Current membership: 2

The Address field shows the e-mail addresses of all of the list members. In the case of Database mail lists, the list membership to be viewed in this list, but not changed; to modify membership of Database lists, make changes to the database table that contains the member list.

Modifying Members

You can modify the address and the full name of a list member by clicking on the entry in the list. The entry will appear in the edit field. Make your changes and click the **Modify** button.

Sorting Membership

You can sort the list of members either by **Address** or by **Full Name** by clicking on the corresponding column heading.

Deleting Members

Existing members can be removed using the **Delete** button. Use the **Ctrl** and **Shift** keys to select multiple members for deletion.

Adding Members

New members can be added by entering the mail address in the field and clicking on the **Add** button.

Show Full Names Button

Mail list members can have a descriptive string associated with them—typically their full name. Click on this button to display the full name of each list member.

The full name is set when a member joins the list using the **JOIN** command, or it can be set by typing the name and e-mail address into the Members page and clicking the **Add** button. Any valid SMTP e-mail address syntax is accepted.

Tip: Depending on the type of mailing list, the time taken for operations such as sorting, deleting or adding addresses may be significantly greater when full names are displayed. Keep them turned off unless you really need to see them.

Import Members

The **Import** button allows you to import mail list members from a text file. The button displays the Open file dialog. Locate the text file containing the Internet mail addresses of the members you wish to import into the list. Click on the **OK** button to import the addresses.

Each line of the text file should consist of one Internet mail address; lines can be commented by starting with #. You can also use any valid RFC822 address, for example:

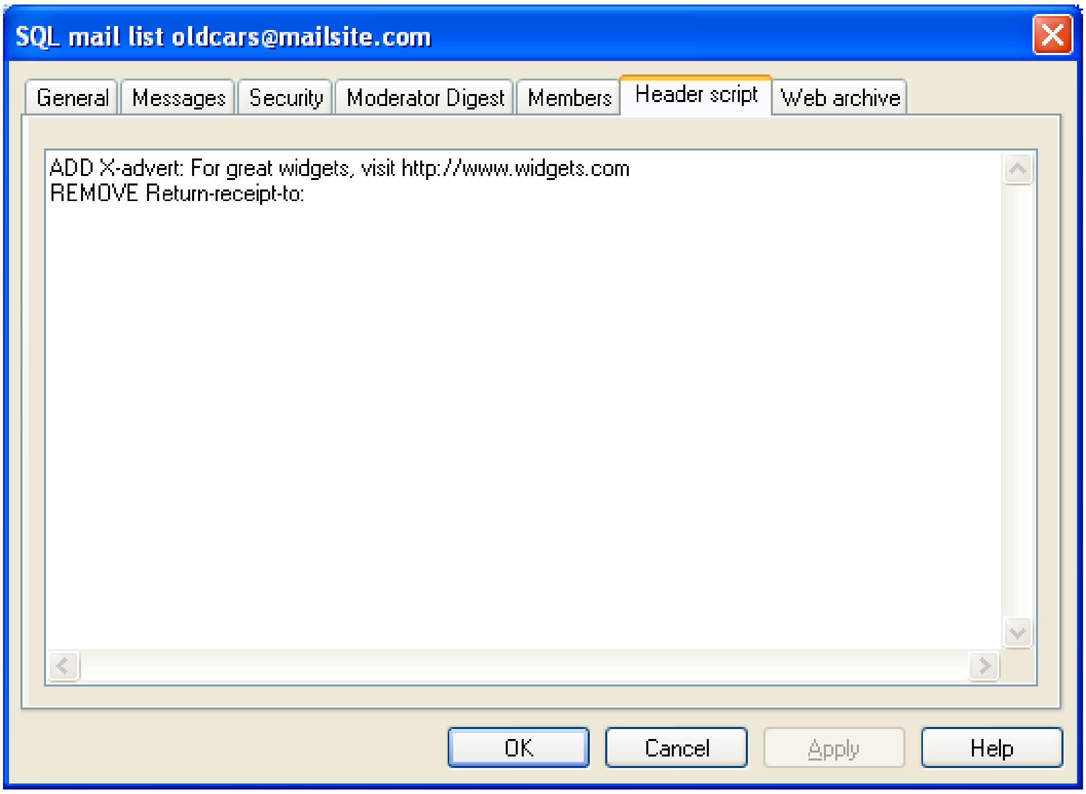
```
"John Smith" john@abc.com
fred@abc.com
joe@efg.com
bill@hij.com
#john@xyz.com
```

Export Members

The **Export** button allows you to export mail list members to a text file. The button displays the **Save As** file dialog. Enter the location and name of the text file that you would like to use. Click on the **OK** button to export the addresses.

List Header Script Page

Use this form to create and edit the header script for this list.



```
ADD X-advert: For great widgets, visit http://www.widgets.com
REMOVE Return-receipt-to:
```

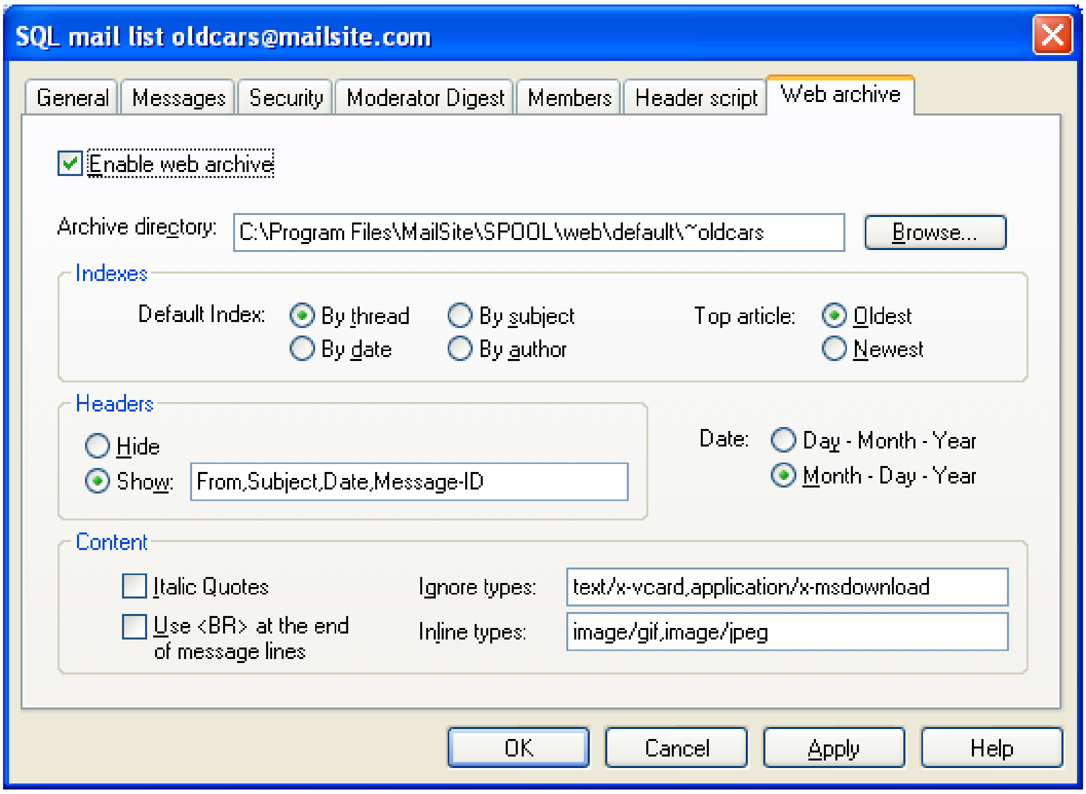
MailSite provides a simple script language for editing the headers of messages sent to a mail list. Script commands are provided to add, rewrite and remove headers, and to test for the presence of specific headers. If you wish to perform more complex processing, you can use the Mail List Agent.

A script consists of a series of commands, one per line. The script is executed line-by-line, top to bottom. Refer to the section on List Header Processing in the Appendix for a complete description. The script commands are:

- ⇒ **`ADD headertemplate`**
- ⇒ **`REMOVE header`**
- ⇒ **`REWRITE header AS headertemplate`**
- ⇒ **`IFPRESENT header GOTO label`**
- ⇒ **`IFABSENT header GOTO label`**
- ⇒ **`IFCONTAINS header text GOTO label`**
- ⇒ **`ABORT [recipient]`**
- ⇒ **`:label`**

List Web Archive Page

The web archive property page controls the creation of an HTML archive of messages sent to the mail list. For more information about mail list archiving, see the sections on Archiving List Messages and Customizing Mail List Archiving.



SQL mail list oldcars@mailsite.com

☑ Enable web archive

Archive directory: C:\Program Files\MailSite\SPOOL\web\default\~oldcars

Indexes

Default Index: ● By thread ○ By subject ○ By date ○ By author

Top article: ● Oldest ○ Newest

Headers

○ Hide
● Show: From,Subject,Date,Message-ID

Date: ○ Day - Month - Year ● Month - Day - Year

Content

□ Italic Quotes
□ Use <BR> at the end of message lines

Ignore types: text/x-vcard,application/x-msdownload
Inline types: image/gif,image/jpeg

`Enable web archive`

Check this box to create a web-accessible archive of messages sent to the mail list.

`Archive directory`

Specify the name of a directory that will contain the archive. If you are running the Windows Console on the same machine as the mail server, you can use the **`Browse`** button to select a directory. You should select a directory which can be accessed by a web server (such as HTTPMA), so that Web users can view the archive.

`Default index`

Several index pages for the archive will be created. This setting controls the default page, which will be named `index.html`.

`Top article`

Controls the order of the entries in the index.

`Headers`

Controls whether individual message headers appear in the archive files, and which headers are shown.

`Date`

Controls how dates are displayed in the archive.

`Italic quotes`

If set, quoted messages within a message will be displayed in italics.

`Use <BR>`

If set, line breaks in a message will be preserved in the archive, using the HTML `<BR>` tag.

`Ignore types`

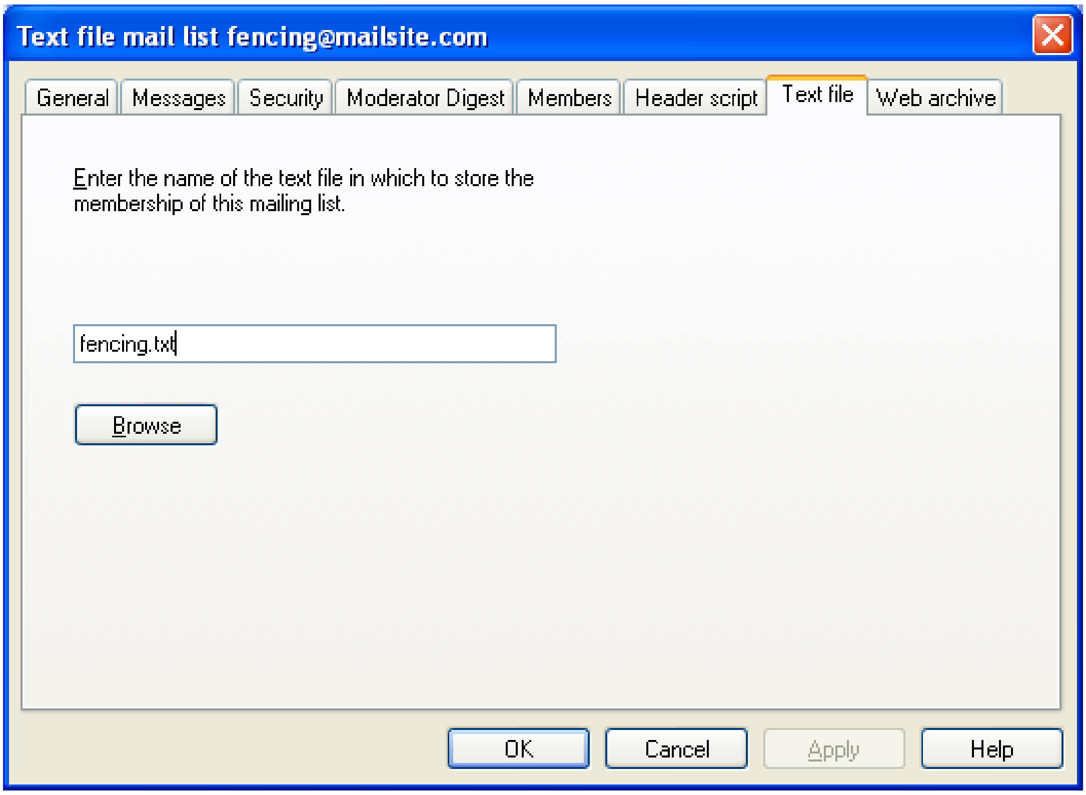
Comma-separated list of MIME types which are ignored when a message is archived.

`Inline types`

Comma-separated list of MIME types which are treated as inline images when a message is archived.

List Text File Page (Text File Lists)

Use this form to configure your text file mail list.



Enter the name of the text file in which to store the membership of this mailing list.

fencing.txt

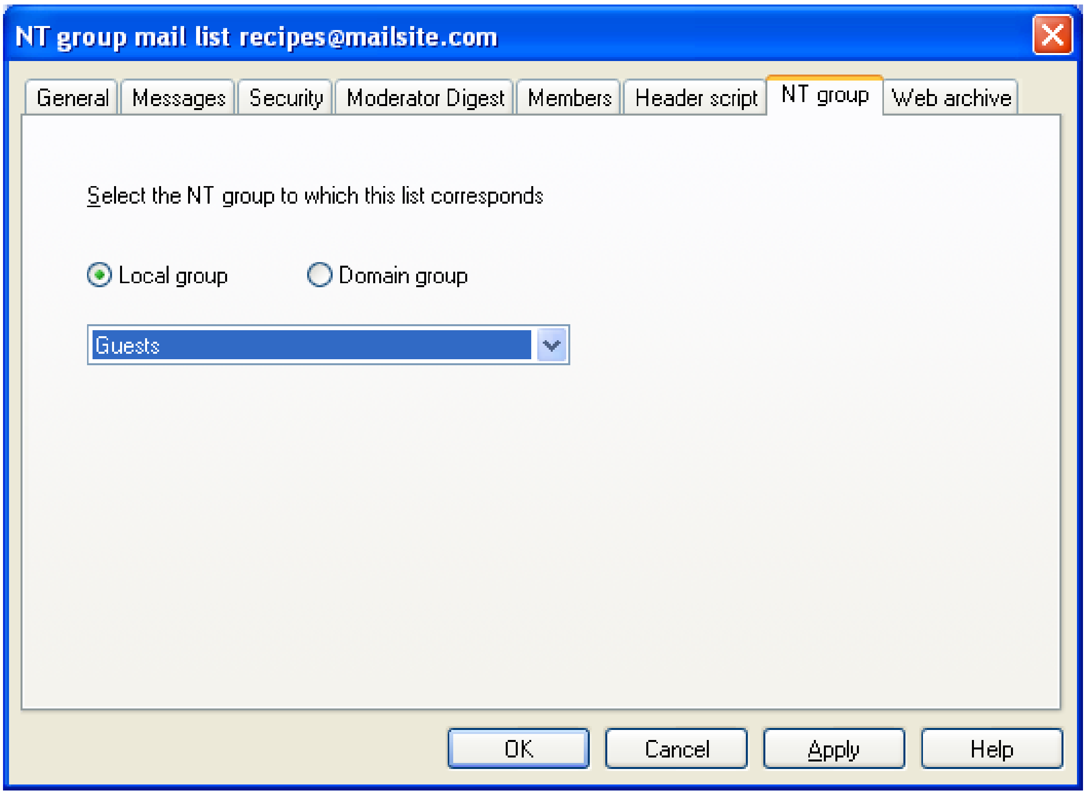
This type of mail list allows you to store membership in a text file. This is useful if you wish to maintain list membership outside of MailSite. You still have the option of managing list membership through the Members tab in the list properties form. MailSite will add and remove entries in the text file when **JOIN** and **LEAVE** subscription requests are received by the **list-request** processor.

File Name

Enter the name of the text file that stores the membership for this list. To search through the file system, select the **Browse** button.

List NT Group Page (NT Lists)

Use this form to configure your NT list.



NT group mail list recipes@mailsite.com

Select the NT group to which this list corresponds

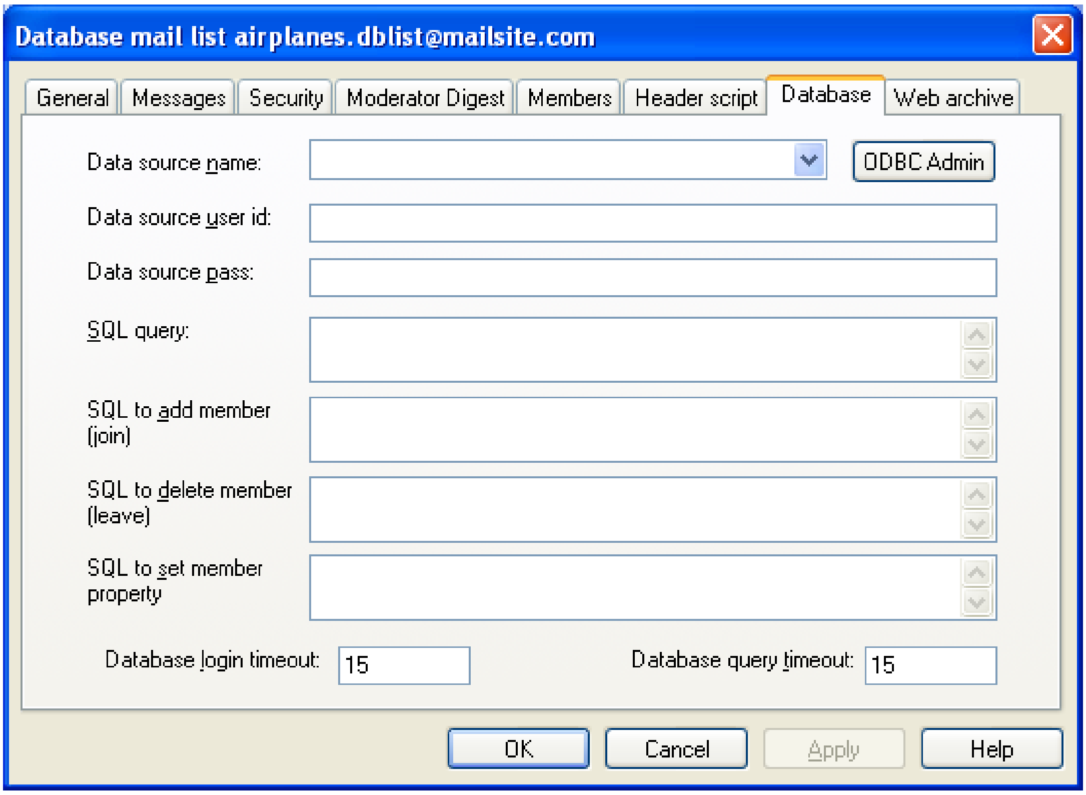
● Local group ○ Domain group

Guests

This type of mail list allows you to send a message to every member of an NT Group that has a mailbox on this server. Select the NT Group that you wish to use.

List Database Page (Database Lists)

Use this form to configure your database mail list. See the section on the Database Mail List Plugin for more information on using this feature.



Data source name:

Data source user id:

Data source pass:

SQL query:

SQL to add member (join)

SQL to delete member (leave)

SQL to set member property

Database login timeout: 15

Database query timeout: 15

Complete the fields on this form. MailSite will use this information to log onto your database and submit a query for list membership.

Data Source Name

Enter the name of the ODBC data source. This is configured in the **`System DSN`** page of the ODBC Data Source Administrator in the Control Panel.

Data Source User ID

Enter the username that MailSite should use to log into to the data source.

Data Source Password

Enter the password that MailSite should use to log into to the data source.

SQL query

The SQL statement to execute to obtain the list of e-mail addresses and full names. The SQL statement you type here must return a result set containing at least two columns, the first of which must contain an e-mail address, while the second should contain the full name of the recipient.

If you do not enter anything here, the default SQL query will be **`SELECT EmailAddress, FullName FROM tablename`**, where **`tablename`** is formed from the mailing list name by replacing any dots and hyphens by underlines.

To execute a stored procedure, use this syntax:

⇒ **`{CALL ProcName(parameters)}`**

There must be no space between the **{** and the **CALL**.

`SQL to add member (join)`

The SQL statement to execute to add a member to the list. By default the statement is:

⇒ **`INSERT INTO tablename (EmailAddress) VALUES (%1)`**

where tablename is formed from the mail list name by replacing any dots and hyphens by underlines. To avoid duplicates, it is important that the “EmailAddress” column of the database is defined to be a primary key. Parameter substitution occurs before the SQL is executed , as follows:

Marker	Type	Description
%1	String	The email address of the new member

`SQL to remove member (leave)`

The SQL statement to execute to remove a member from the list. By default the statement is:

⇒ **`DELETE FROM tablename WHERE EmailAddress = %1`**

where tablename is formed from the mail list name by replacing any dots and hyphens by underlines. Parameter substitution occurs before the SQL is executed, as follows:

Marker	Type	Description
%1	String	The email address of the deleted member

`SQL to set member property`

The SQL statement to execute to set the value of a member property. By default the statement is:

⇒ **`UPDATE tablename SET %2 = %3 WHERE EmailAddress = %1`**

where tablename is formed from the mail list name by replacing any dots and hyphens by underlines. Parameter substitution occurs before the SQL is executed, as follows:

Marker	Type	Description
%1	String	The email address of the member
%2	String	The name of the parameter
%3	String	The value of the parameter

`Database Login Timeout`

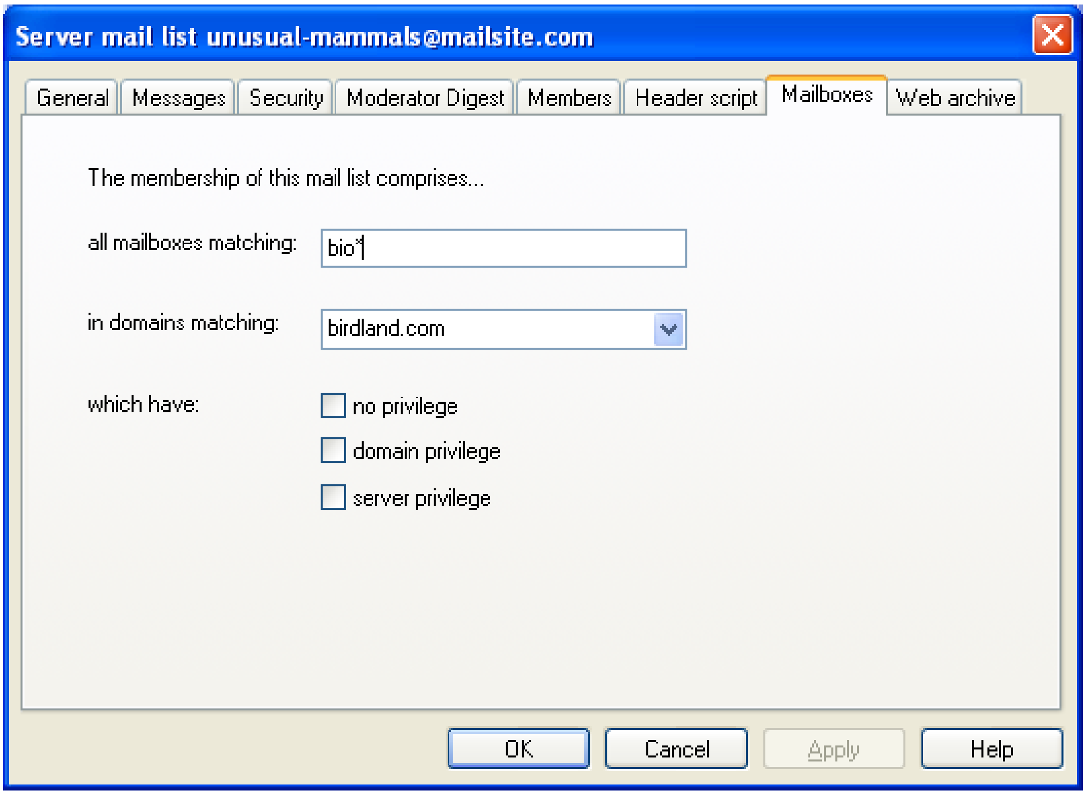
Enter the time (in seconds) that is allowed for connecting to the database. If you leave this blank, the default timeout of 15 seconds will be used. A value of zero means an infinite timeout.

`Database Query Timeout`

Enter the time (in seconds) that is allowed for executing the database query. If you leave this blank, the default timeout of 15 seconds will be used. A value of zero means an infinite timeout.

List Mailboxes Page (Server Lists)

Use this form to configure your server mail list.


Server mail list unusual-mammals@mailsite.com

The membership of this mail list comprises...

all mailboxes matching: bio*

in domains matching: birdland.com

which have:

□ no privilege

□ domain privilege

□ server privilege

The membership of a Server mail list comprises those mailboxes on the mail server that match certain masks that you specify.

All mailboxes matching

Specify a mask string that matches all the mailbox names that the list is to contain. For instance, **`web*`** includes all mailboxes starting with **`web`**. You can specify a comma-separated list of masks (*e.g.* **`web*,post*`**), and you can also specify exclusions using an exclamation point (*e.g.* **`web*,!weber,post*`**). To include all mailboxes, specify a single asterisk.

In domains matching

Specify a mask string that matches all the (local) domain names that the selected mailboxes may be in. For instance, **`www.*`** includes all domains starting with **`www.`**. You can specify a comma-separated list of masks (*e.g.* **`www.*,mail.*`**), and you can also specify exclusions using an exclamation point (*e.g.* **`www.*,!www.mycompany.com,mail.*`**). There is a drop-down list that allows you to select a domain name. To include all domains, specify a single asterisk.

Which have

Specify the privilege level of mailboxes that are to be in the list. See the section on Mailboxes for more information about mailbox privileges.

MailSite Web Services

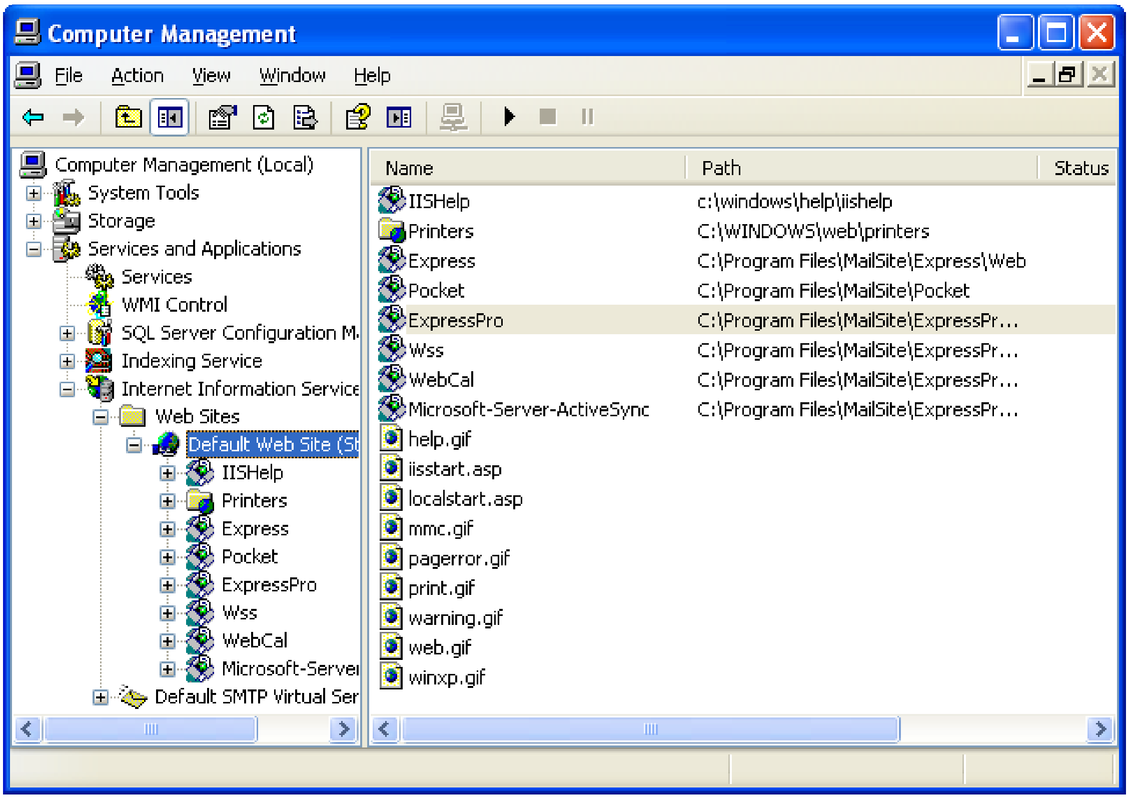
A number of MailSite's most important features are implemented as Web Services rather than stand-alone Windows services. These web services are therefore managed from the operating system's Microsoft Internet Information Services (IIS) Manager rather than the MailSite Console. MailSite Web Services will only be installed if both IIS and the .NET Framework are installed on the server. See the System Requirements section for more information.

Managing MailSite Web Services

MailSite Fusion includes the following web services:

- Express – MailSite Express. A web client suitable for end-users with limited resources such as a slow internet connection or an old internet browser.
- ExpressPro – MailSite ExpressPro. A cutting-edge web client based on AJAX technology giving a desktop like look and feel.
- Microsoft-Server-ActiveSync – MailSite ActiveSync. Provides native over-the-air synchronization of Mail, Calendars & Contacts for Windows Mobile, iPhone and Nokia devices.
- Pocket – MailSite Pocket. An email client for Wireless Access Protocol (WAP) devices.
- WebCal – MailSite Calendar Server. Provides standards based iCalendar compatible access to calendar information.
- WSS – MailSite Outlook Connectivity. Support for synchronized MailSite Calendar and Contacts in Outlook 2007, without installing client-side plugins.

These web services will normally be managed from Windows IIS Manager:



Name	Path	Status
IISHelp	c:\windows\help\iishelp	
Printers	C:\WINDOWS\web\printers	
Express	C:\Program Files\MailSite\Express\Web	
Pocket	C:\Program Files\MailSite\Pocket	
ExpressPro	C:\Program Files\MailSite\ExpressPr...	
Wss	C:\Program Files\MailSite\ExpressPr...	
WebCal	C:\Program Files\MailSite\ExpressPr...	
Microsoft-Server-ActiveSync	C:\Program Files\MailSite\ExpressPr...	
help.gif		
iisstart.asp		
localstart.asp		
mmc.gif		
pagerror.gif		
print.gif		
warning.gif		
web.gif		
winxp.gif		

Troubleshooting Procedure

Whenever you experience problems with MailSite we recommend that you follow this step by step procedure:

- **Check TCP/IP Connectivity**

Frequently the problem lies with the TCP/IP connection to the computer. See the section on TCP/IP Debugging for more information.

- **Check the Server Log File or the Windows NT Event Log**

Look for incidents around the date and time when the problem occurred. If the problem is associated with a specific mail message, search for the Message ID.

- **Reconfigure the Logging Options using the Logging Page**

Examine the on-line help to determine which logging options would provide relevant information to your problem and enable these options.

- **Reproduce the problem**
- **Re-examine the Server Log File or the Windows NT Event Log**

Look for incidents around the date and time when the problem occurred. If the problem is associated with a specific mail message, search for the Message ID in the file system and examine the file with a text editor.

- **Decode the error message**

Error codes fall into two categories: TCP/IP errors and Windows NT errors. Most TCP/IP errors are greater than 10000, while most Windows NT errors are less than 10000. To decode a TCP/IP error, refer to the list on the MailSite web site. To decode a Windows NT error, run this command:

⇒ `net helpmsg NNN`

Where NNN is the Windows NT error code number.

- **Troubleshoot the server by following the** Telnet Debugging procedure

Debugging TCP/IP Connections

Frequently the problem lies with the TCP/IP connection to the computer. Follow this procedure to debug TCP/IP connections to the MailSite server.

Problems Receiving Mail

Resolve the IP Address

Log on to a remote computer and use the command **`nslookup`** to resolve the IP address:

```
nslookup
Server: 192.153.156.22
> mailsite.com
> SET TYPE=MX
  query type = MX
> mailsite.com
  mailsite.com.
    0, mail.mailsite.com.
  mailsite.com.
    10, nic.scruz.net.
> SET TYPE=A
  query type = A
> mail.mailsite.com
  mail.mailsite.com.
    204.147.233.1
```

In this case the host `mailsite.com` does not have an A record (since the first query did not return any records). However `mailsite.com` does have two MX records, one of which points to the host `mail.mailsite.com`. A third query for the A record for `mail.mailsite.com` reveals that this host has IP address `204.147.233.1`.

This is the procedure that external mail servers use to resolve mail addressed to `users@mailsite.com`. Substitute the name of your MailSite server for `mailsite.com`.

PING the Server

Once you have resolved the IP address for your MailSite server, you can establish TCP/IP connectivity by `pinging` the host:

⇒ `C:\> ping 204.147.233.1`

```
Pinging 204.147.233.1 with 32 bytes of data:
Reply from 204.147.233.1: bytes=32 time=10ms TTL=32
Reply from 204.147.233.1: bytes=32 time<10ms TTL=32
Reply from 204.147.233.1: bytes=32 time<10ms TTL=32
```

Telnet to the MailSite Services

If all of the above steps work, then look at the section on Telnet Debugging for more information.

Problems Sending Mail

If MailSite has problems sending mail to one or more remote domains, then follow the procedure above, except:

⇒ Do it from your MailSite server, rather than from a remote computer

⇒ Replace `mailsite.com` with the name of the problematic domain

Debugging with Telnet

Sometimes mail clients do not display very helpful error messages. In these situations, it can be helpful to `telnet` to MailSite to check whether the problem lies with the server or the client.

POP Server

To troubleshoot the POP server from a client, execute the following command:

⇒ `telnet host.domain 110`

Replace `host.domain` with the name or IP address of the MailSite server. The Telnet window will open and a greeting from the server will appear. Enter the following POP commands:

⇒ USER yourusername
⇒ PASS yourpassword
⇒ RETR 1
⇒ QUIT

IMAP Server

To troubleshoot the IMAP server from a client, execute the following command:

⇒ **`telnet host.domain 143`**

Replace **`host.domain`** with the name or IP address of the MailSite server. The Telnet window will open and a greeting from the server will appear. Enter the following IMAP commands:

⇒ A1 LOGIN username password
⇒ A2 LIST “” “*”
⇒ A3 LOGOUT

SMTP Server

To troubleshoot the SMTP server from a client, execute the following command:

⇒ telnet host.domain 25

Replace **`host.domain`** with the name or IP address of the MailSite server. The Telnet window will open and a greeting from the server will appear. Enter the following SMTP commands:

⇒ HELO yourcomputername
⇒ MAIL FROM: <yourusername>
⇒ RCPT TO: <yourusername>
⇒ DATA
⇒ type the text of your message
⇒ . (period <return> to end the data)
⇒ QUIT

There should be a new mail message waiting for **`yourusername`**.

Technical Support

If the above troubleshooting steps don’t resolve an issue that you are encountering, check the MailSite Software, Inc. technical support web site for more information:

⇒ http://www.mailsite.com/support

At this site you will find many support tools:

1. **Knowledge Base**. The MailSite knowledge base includes answers to common questions and solutions to known issues. Start here when looking for assistance.

   ⇒ http://www.mailsite.com/support/docs

2. **Latest downloads**. MailSite Software, Inc. regularly issues new MailSite releases that include various fixes and updates, so common problems can often be fixed simply by upgrading to the latest version. Log in the MailSite Software, Inc. User Room to access the downloads page:

   ⇒ http://www.mailsite.com/userroom

3. **Discussion list**. The MailSite-discuss list is a peer support mail list that allows MailSite customers to get help from other MailSite sites. You can subscribe to this and other MailSite lists through the User Room.

4. **Open a Case**. To open a technical support case; use the appropriate form in the MailSite Software, Inc. Portal. Note that you must have a current MailSite support subscription to use MailSite technical support. Use the MailSite ordering system to purchase a MailSite support subscription:

   ⇒ http://www.mailsite.com/order

   Visit the Portal to check the status of your MailSite support subscription.

DNS Overview

The Internet is a global network of computers connected using the TCP/IP protocol. Each computer has a unique numerical TCP/IP address that other computers use to communicate with it.

People find it easier to refer to computers by name. Domain Name Service (DNS) takes care of this dilemma. It's sole purpose in life is to translate (or *resolve*, in technical terminology) TCP/IP addresses to computer names (and vice-versa).

DNS services run on many computers on the Internet. DNS is designed so that if a computer is asked to resolve an address and does not know the answer, it will pass the request on to a higher level authority.

Your computer, as a DNS client, will submit resolution requests to DNS servers when you try to connect to Internet sites such as **`www.ibm.com`**. The primary and secondary DNS servers for your computer are entered in numerical format in the Network TCP/IP Settings.

The DNS database on the server contains a number of different mappings of names to addresses, called record types. The most common, A, is the one that most people think of as DNS. A records are the ones used for resolving WWW and FTP addresses. In general you will find one numeric address for a given host name. For example, the A record for **`www.ibm.com`** is:

⇒ 165.87.194.133

There is a second record type is called Mail eXchange (MX) records. These records are devoted to the delivery of mail. A MX record for a particular name will have several addresses and priorities. For example, to send e-mail to DEC, you need to use the name **`dec.com`**. DEC has the following MX records, each with a different priority number:

```
16.1.0.22           inet-gw-2.pa.dec.com   70
16.1.0.33           inet-gw-3.pa.dec.com   90
16.1.0.23           inet-gw-2.pa.dec.com   100
```

These records tell mail software where to send the mail and what to do if the first machine is not available. If the mail server **`inet-gw-2.pa.dec.com`** is being rebooted, a mail server will send mail to **`inet-gw-3.pa.dec.com`** (since these are the entries with the next higher priority in the MX record).

Many destinations do not have MX records. In this case, mail software will attempt to use the A instead. Mail will be held until it is possible forward if none of these machines are available.

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

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

1. License Grant; Related Provisions

a. 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.

b. Limitations

You shall not, and shall not permit any third party to,
(i) 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;
(ii) except for temporary transfer in the event of computer malfunction, install the Software on a second computer;
(iii) publish the Software or use the same other than for the purposes described in Section 1.a of this Agreement;
(iv) 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);
(v) except as expressly authorized by law, change, modify or otherwise alter the Software (including without limitation any related malware signatures and malware detection routines);
(vi) 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;
(vii) 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
(viii) 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.

c. 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.

2. Term; Termination

a. Term

The initial term of this Agreement will commence on the date you download or otherwise acquire the Software, and will continue
(i) for the term you specified in your order for the Software, or
(ii) if you purchased the Software on CD or other physical medium, on the Software package, or
(iii) 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”*.

b. 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.

c. 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.

3. 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.

4. Warranties

a. 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.

b. 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.

c. 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.

5. 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.

6. Miscellaneous

a. 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.

b. Privacy

(i) 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.

(ii) 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.

c. 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.

d. 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.

e. 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.

f. 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.

g. 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.

h. 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.

i. 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:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. 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.
3. 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 common administrative and management tasks relating to MailSite installations.

MSALIAS

The command-line utility **`MSALIAS.EXE`** can be used to manage the alias table. The syntax is:

```
msalias -version
msalias –machine \\system -login user[@domain] -loginpass password …
msalias -list
msalias -addstart mapfrom mapto
msalias –addstart -file aliasfile
msalias -addend mapfrom mapto
msalias –addend -file aliasfile
msalias -delete mapfrom
msalias –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>**.

You can backup the MailSite configuration at any time. However, it is important to stop all services before restoring the configuration.

MSBOX

The utility **MSBOX.EXE** can be used to manage mailboxes. You can use this utility to create a batch of mailboxes or to migrate mailboxes from another mail server. The syntax is as follows:

```
msbox –version
msbox –machine \\system -login user[@domain] -loginpass password ...
msbox -list [domain]
msbox -list2 [domain] -security pass
msbox -create name[@domain] pluginid
msbox -delete name[@domain]
msbox -set name[@domain] property value
msbox -get name[@domain] property
msbox -pass name[@domain] [Plaintextpassword]
msbox -plugin name[@domain] pluginid
msbox -plugin @filename pluginid
msbox -createalias name[@domain] alias[@domain]
msbox -deletealias alias[@domain]
msbox -listalias name[@domain]
```

One and only one of the flags must be present.

-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 mailboxes in the given domain. If the domain is omitted, the default domain is assumed.

-list2 [*domain*] -security *pass*

List the mailboxes in the given domain. If the domain is omitted, the mailboxes in the default domain are listed. The plugin ID, mailbox name, full name and password separated by tabs are listed. Because this command reveals mailbox passwords, a security pass must be supplied. The ***pass*** must be the password for the postmaster mailbox in the default domain. Note that the postmaster mailbox must exist and must have a password that does not contain spaces.

-create *name*[@*domain*] *pluginid*

Create a new mailbox called **name** in virtual domain **domain**, using the mailbox identified by the **pluginid** (see below). If the domain is omitted, the mailbox is created in the default domain.

-delete *name*[@*domain*]

Delete the mailbox **name** in virtual domain **domain**. If the domain is omitted, the mailbox is deleted from the default domain.

-set *name*[@*domain*] *property value*

Set the mailbox property **property** to **value**.

-get name[@domain] property

Display the value of the named mailbox property. See below for a list of property names.

-pass *name*[*@domain*] [*plaintextpassword*]

Set the mailbox password to **plaintextpassword**.

-createalias *name*[*@domain*] *alias*[*@domain*]

Create the given alias for the mailbox. This operation is supported only for SQL mailboxes.

-deletealias *alias*[*@domain*]

Deletes the given mailbox alias. This operation is supported only for SQL mailboxes.

-listalias *name*[*@domain*]

Lists the aliases for the given mailbox. This operation is supported only for SQL mailboxes.

-plugin name[@domain] pluginid
-plugin @filename pluginid

Change the plugin which is responsible for the mailbox. The second form allows you to specify the name of a file containing a list of mailbox names, one per line. The **pluginid** indicates which plugin the mailbox should be moved to.

You can use this option to move mailboxes between Registry, NT User and Database plugins. However, note that you cannot move a mailbox (called **fred**, say) to use the NT User plugin or the Database plugin unless there is already an NT user with that name, or a database row with that value in the Mailbox column.

You can use the mailbox utility to convert all Registry mailboxes in a domain to Database mailboxes as follows:

⇒ Create a text file containing all the Registry mailboxes using the command:

```
msbox -list my.domain.com 0 >mailboxes.txt
```

⇒ Create a row in the database table for each of the mailboxes in the list. Exactly how to do this will depend on the database package you are using and on its facilities for importing data, and on the database structure you have set up.

⇒ Use the following command to convert the Registry mailboxes to use the database plugin:

```
msbox –plugin @mailboxes.txt 2
```

Mailbox properties can be accessed via **MSBOX**. Refer to the appendix on Mailbox Properties for more information.

PluginId

PluginId determines the type of the Mailbox. There can be up to six different types of mailboxes. Currently three are implemented. Each mailbox type has its own icon, and a **PluginId** reference number between 0 and 5. The implemented **PluginIds** are:

Number	Mailbox type	Comment
0	Registry/SQL	Default mailbox plugin. Mailbox information stored in Registry in Registry Connector mode and in SQL Server database in SQL Connector mode.
1	NT User	Mailbox information stored in Registry and in NT user database
2	Database	Stores mailbox name, domain and password in ODBC/ SQL database

Mailbox properties can be accessed via **MSBOX** Refer the the appendix on Mailbox Properties for more information.

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 a new synonym *synonym* for the virtual domain *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

This utility exports and imports all the server’s configuration information to and from an XML file.

The syntax is as follows:

```
msimportexport –[im|ex]port filename
               -delete
               -server [-property old1[:new1][,old2[:new2]]..]
               -domains [-property old1[:new1][,old2[:new2]]..]
               -mailboxes [-plugin old1[:new1][,old2[:new2]]..]
                          [-property old1[:new1][,old2[:new2]]..]
               -maillists [-plugin old1[:new1][,old2[:new2]]..]
                          [-property old1[:new1][,old2[:new2]]..]
```

The command arguments are as follows:

-import

This indicates that you want to import the xml file into MailSite.

-export

This indicates that you want to export to the xml file from MailSite.

Filename.xml

This is the name for the file that you wish to export or import with the extension of .xml

-delete

This is the only argument that can be used on its own. This will delete all settings from the MailSite server.

-server [-property old1[:new1][,old2[:new2]..]

This argument restores the Server properties from the xml file. With the option –property the information in the XML file can be overridden. This can be used to alter one or more server properties with a format such as –property 0:1.

-domains [-property old1[:new1][,old2[:new2]..]

This argument restores the Domains properties from the xml file. With the option –property the information in the XML file can be overridden. This can be used to alter one or more domain properties with a format such as –property 0:1.

-mailboxes [-plugin old1[:new1][,old2[:new2]..] [-property old1[:new1][,old2[:new2]..]

This argument restores the Mailboxes properties from the xml file. This option needs to be used in conjunction with –domains.

MSImportExport’s default –plugin value is 0 which is Registry, if you have SQL mailboxes the –plugin option will need to be used to enable msimportexport to restore these mailboxes correctly. See the table of PluginIds below for more information.

With the option –property the information in the XML file can be overridden. This can be used to alter one or more mailbox properties with a format such as –property 0:1.

-maillists [-plugin old1[:new1][,old2[:new2]..] [-property old1[:new1][,old2[:new2]..]

This argument restores the Mailboxes properties from the xml file. This option needs to be used in conjunction with –domains and –mailboxes.

MSImportExport’s default –plugin value is 0 which is Registry, if you have SQL mailboxes the –plugin option will need to be used to enable msimportexport to restore these mailboxes correctly. See the table of PluginIds below for more information.

With the option –property the information in the XML file can be overridden. This can be used to alter one or more maillist properties with a format such as –property 0:1.

PluginId

PluginId determines the type of the Mailbox. There can be up to six different types of mailboxes. Currently three are implemented. Each mailbox type has its own icon, and a **PluginId** reference number between 0 and 5. The implemented **PluginIds** are:

Number	Mailbox type	Comment
0	Registry/SQL	Default mailbox plugin. Mailbox information stored in Registry in Registry Connector mode and in SQL Server database in SQL Connector mode.
1	NT User	Mailbox information stored in Registry and in NT user database
2	Database	Stores mailbox name, domain and password in ODBC/ SQL database

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

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

The **MSPOP.EXE** utility downloads e-mail messages from a mailbox on a remote POP3 server. It examines the **To: CC:** and **Bcc:** fields on the downloaded message to determine which local mailboxes (or mail lists) to send them to. If **MSPOP.EXE** cannot determine where a message should go, it will forward it to the postmaster.

```
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.

To debug the operation of **MSPOP**, turn on logging for **Protocol Exchanges** and **Received Message Data**. **MSPOP** will make logging entries to the Log File.

MSPURGE

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

This utility resets the quota information of a given domain, mailbox or all mailboxes.

The syntax is as follows:

```
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

The command-line program **MSSEND.EXE** sends a text file to a specified address. The syntax for this command is:

```
mssend -s server -f from -i file -t to    -u "subject" -v
```

Where the arguments are:

-s server

The host name of the destination SMTP server.

-f from

The e-mail address of the sender.

-i file

The text file to send.

-t to

The e-mail address of the recipient.

-u "subject"

The subject for the mail message, enclosed in "double quotes".

-v

Displays the version of **MSSEND**.

MSSENDMESSAGES

A utility program for sending .MSG files through SMTPRA. The return path for the message is taken from the Sender or the From headers, and the recipients are taken from the To, Cc, and Bcc headers.

```
mssendmessages [DontStartSMTPRA] -DirectoryName <DirectoryName>
```

DontStartSMTPRA

If specified, then the program will make no attempt to start SMTPRA on the local machine.

-DirectoryName

All the .MSG files in this directory will be processed.

MSSTART

The command-line program **`MSSTART.EXE`** connects to a remote mail server and uses the ETRN command to initiate delivery of queued mail. The SMTP receiver service at the target mail server must support the **`ETRN`** command. The MailSite SMTP Receiver service supports this command.

The syntax for this command is:

```
msstart [-h hostname] [-u username [-p password]] domain [domain ...]
```

Where the arguments are:

-h hostname

The IP address or fully-qualified domain name of the mail server. If omitted, the machine on which the command is executed is assumed to be the mail server.

-u username

The IP address or fully-qualified domain name of the mail server. If omitted, the machine on which the command is executed is assumed to be the mail server.

-p password

The IP address or fully-qualified domain name of the mail server. If omitted, the machine on which the command is executed is assumed to be the mail server.

domain

A domain name or machine name for which mail is to be downloaded. Multiple names can be specified. If a name is preceded by the wildcard **`*`** character (e.g. **`*myco.com`**), then all matching domains will be started (which might in this case include **`mail.myco.com`** and **`myco.com`**).

MSCONV

The utility **`MSCONV.EXE`** is used to convert mailbox directories (and messages from third-party mail servers to MailSite. The syntax for this command is:

```
msconv [-h?vtqd] -s source [-u username] -m type directory
```

Where the arguments are as follows:

-h,?

Displays usage information.

-v

Displays version number.

-t

Displays trace information.

-q

Runs **`MSCONV`** in “quiet” mode, which suppresses output.

-d

Specifies that MailSite create multi-level mailbox directories.

-s source

Specifies the source mailbox directory. If omitted, the current directory is assumed.

-u username

User name of the mailbox to convert. If this option is omitted, all mailboxes will be converted.

-m type

Defines the source mailbox type. The available mailbox types are:

⇒ **Post.Office**
⇒ **SendMail**
⇒ **SLMail**
⇒ **NTMail**
⇒ **Imail**
⇒ **IMS**

directory

Defines the destination MailSite mailbox directory.

MSCONVUSER

The utility `MSCONVUSER.EXE` is used to convert user information from third-party mail servers to MailSite.

To use `MSCONVUSER`, first install MailSite on the same machine as the third-party mail server, but do not start any MailSite services. Start the third-party server's LDAP server (which `MSCONVUSER` uses to obtain user information), and then execute `MSCONVUSER`.

The syntax for this command is:

```
msconvuser [-h?vtq] -s src_domain -m mbox_type mailsite_domain
```

Where the arguments are as follows:

-h,?

Displays usage information.

-v

Displays version number.

-t

Displays trace information.

-p

MailSite plugin ID for created users (default 0=Registry)

-q

Runs `MSCONVUSER` in "quiet" mode, which suppresses output.

-s domain

Specifies the domain of the user accounts to be converted.

-m type

Defines the source mailbox type. The available mailbox types are:

⇒ **IMail**

mailsite_domain

The destination MailSite domain for the user information.

MSCONVUSER2

The utility **`MSCONVUSER2.EXE`** is used to convert user information from third-party mail servers to MailSite.

To use **`MSCONVUSER2`**, first install MailSite on the same machine as the third-party mail server (but do not start any MailSite services) and then execute **`MSCONVUSER2`**. As **`MSCONVUSER2`** uses other MailSite dlls, it is recommended to run it from the installation directory or another location which contains an up to date set of dlls.

The syntax for this command is:

```
msconvuser2 -[abh?vtq] -m mailsystem [-o xmlfile] [-i indent]
               [-p plugin] [-d domain] --
```

Where the arguments are as follows:

-a

Output only mailnames that are aliases.

-b

Output only mailnames that are mailboxes.

-h,?

Displays usage information.

-v

Displays version number.

-t

Displays trace information.

-q

Runs **`MSCONVUSER2`** in "quiet" mode, which suppresses output.

-m mailsystem

Defines the source user type. The available mailbox types are:

- ⇒ **Post.Office**
- ⇒ **WorldMail**

-o xmlfile

Defines the name of the output file (stdout by default):

-i indent

Indent factor to use when writing XML output (default is 0).

-p plugin

The MailSite mailbox type of the converted mailboxes. The default is 0 (Registry mailboxes).

-d domain

The destination MailSite domain for the user information.

Appendix B - Customizing Mail List Archiving

Messages sent to a mail list can be archived in HTML format so that they can be viewed with a web browser. Use the Web Archive mail list property page to enable this feature.

The format of the web archive is controlled not only by the settings on the property page, but also by Archive Template files. Template files may be useful if:

⇒ You want to display the archive pages in a different language.
⇒ You want to personalize the pages with information, logos, and such that are specific to the mail list or to your site.

Archive Template Files

MailSite ships with the following template files for the List Archive pages:

Template File Name	List Archive Page
`article.htm`	Message page
`index.htm`	Index of mail list postings

These template files are written using standard HTML containing special tags. MailSite reads the template file and converts the special tags into useful information. Locate the sample template files under your MailSite program directory, for example:

⇒ **`C:\Program Files\MailSite\templates\archive`**

Installing the Template Files

The list archive templates must be located in the mail list root directory of the default domain. For example:

⇒ **`C:\Program Files\MailSite\SPOOL\lists`**

If you wish the archive to have a different appearance depending on which domain the mail list belongs to, you can place templates in the mail list root directory for the domain in question. For example:

⇒ **`C:\Program Files\MailSite\SPOOL\lists\~domain.com`**

If you wish the archive for one mail list to have a different appearance from the other mail lists in the same domain, then template files may be placed in the list directory for that list. For example:

⇒ **`C:\Program Files\MailSite\SPOOL\lists\~domain.com\Listname`**

Editing the Template Files

After you have installed the sample template files you can use a text editor or Microsoft FrontPage to edit them. Note that other HTML editors may corrupt the format of the template files and consequently are not supported.

The template files are written in standard HTML and contain special template tags. The archive template tags take the following format:

⇒ **`<%Hypermail:PropertyName%>`**.

The MailSite archiving facility recognizes the **`Hypermail`** template tag, reads the **`PropertyName`** and replaces the tag with the appropriate data before sending the web page to the browser. Each Template page has a different set of **`PropertyNames`** as described in the following sections. Note that alphabetic case is significant, and no spaces are allowed.

Index.htm

Each of the four index pages (by thread, by date, by subject and by author) is generated from the same index template. The available properties on this page are as follows:

`ArchiveAddress`	The e-mail address of the archive
`GenerationDate`	The generation date of this archive including hours, minutes, seconds, days, months, years and time-zone.
`IndexSummary`	Three links of HTML describing the number of messages in the archive, the date of the first article, and the date of the last article in the archive.
`IndexSummaryTable`	A summary of the archive containing the same information given by the `IndexSummary` property, but in table format.
`IndexName`	The name of the index page, either ‘By Thread’, ‘By Date’, ‘By Subject’ or ‘By Author’.
`IndexTableTop`	The navigation table without a link to the current index, and including a link to the `IndexTableBottom` table.
`IndexTableBottom`	The navigation table without a link to the current index, and including a link to the top of the page, where we expect to find the `IndexTableTop` table.
`IndexLinksTop`	A list of index links in [a|b|c] format, excluding a link to the current index.
`IndexLinksBottom`	A list of index links in [a|b|c] format, excluding a link to the current index.
`Index`	The entries of the index. Each is surrounded by <LI>,</LI> tags and it is therefore suitable to surround this tag with <UL>,</UL>.

Article.htm

The available properties on this page are as follows:

`ArchiveAddress`	The e-mail address of the archive
`GenerationDate`	The generation date of this archive including hours, minutes, seconds, days, months, years and time-zone.
`IndexSummary`	Three links of HTML describing the number of messages in the archive, the date of the first article, and the date of the last article in the archive.
`IndexSummaryTable`	A summary of the archive containing the same information given by the `IndexSummary` property, but in table format.
`IndexTableArticle`	The navigation table with links to all the index pages at the point where they reference this article, and a link to send a reply to the archived message.
`IndexLinksArticle`	Links to all the index pages at the point where they reference this article.
`AuthorLink`	The author’s name, E-mail address and the date the article was sent.
`Email`	The E-mail address of the author.
`SubjectMeta`	A meta tag describing the content of the message for use in the <HEAD> section of the document..
`AuthorMeta`	A meta tag defining the author of the message for use in the <HEAD> section of the document.
`Subject`	The subject of the current message.

`MessageId`	The id of the current message.
`MessageLinks`	A list of navigation links including ‘next’, ‘previous’ and ‘next in thread’ links. Each link is surrounded by <LI></LI> tags.
`MessageReplyLinks`	A list of links that are likely to be replies to this message. Each link is surrounded by <LI></LI> tags.
`EmailBody`	The content of the message, starting with the headers, then the body, then the attachments if any.

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

This section contains examples of configuring the Database Mailbox Plugin and Database Mail List Plugin.

Database Mailbox Plugin Example

Here is a step-by-step example of how to use the Database Mailbox Plugin in Generic mode with a Microsoft Access database.

1. Install Microsoft Access
2. Install the Microsoft Access ODBC driver
3. Create a default data source

    q Go to the control panel and start the **ODBC Data Source Administrator**

    q Select the **System DSN** page

    q Click the **Add** button

    q Select the Microsoft Access driver and click **Finish**

    q Type **Default** as the data source name

    q Optionally, enter a description of the data source

    q Click **Create** to create a new database

    q Enter a name for the new database file (of type .**MDB**) and click **OK**. You will be told that the database has been created correctly

    q Click **OK** to finish creating the data source

    q Click OK once more to dismiss the ODBC Data Source Administrator

4. Create a table in the new database for your mailboxes

5. Start Microsoft Access

    q Open the database you created in the preceding step

    q In the database window, select the Tables tab and click the **New** button

    q Select **Design View** and click **OK**

    q In the **Field Name** column of the design view, enter the following fields:

    ⇒ **Mailbox**

    ⇒ **FullName**

    ⇒ **Password**

    ⇒ **Domain**

    All should be of type **Text**

    q Select the row containing the Mailbox field and then choose **Primary Key** from the Edit menu

    q Close the design view window. When prompted to save the changes to the table, say **Yes** and call the table Mailboxes

6. Enter information into the table

    q If the table worksheet is not already displayed, double-click on the corresponding icon under the **Tables** tab to open it q Enter (say) ten users, each with a unique mailbox name

q Under the **Mailbox** column, enter a unique mailbox name. Only use the characters alphanumeric, period, hyphen and underscore

q Under the **FullName** column, enter the corresponding user's name

q Under the **Password** column, enter a password for this user

q Leave the **Domain** field blank unless you have defined some virtual domains in MailSite; in that case you may wish to specify virtual domain names for each user, but still leave a few blank

q Repeat until you have got several users (say ten) in the table

q Close the table worksheet

q Close the database and quit Access

7. Configure the database mailbox plugin

q Start the Console and open the **Plugins** Folder

q Double click on the **Database Mailbox Plugin** icon

q Leave the fields in the configuration dialog blank, and verify that the **Generic database** type is selected

q Click the **Configure** button to edit the configuration information for the Generic database type

q Where the dialog asks for **Domain** column name, enter **Domain**. Leave the other fields blank

q Click **OK** to save the Generic Database configuration

q Click **OK** to dismiss the database plugin configuration dialog

8. Add mailboxes from the database to MailSite

q In the Mailboxes folder, ensure that the default domain is selected. Right-click in the display area and select **New** database mailbox from the popup menu

q You will see a list containing the users you entered into the database with blank domain entries. Select one or more of those users and click **Add**. New mailboxes will be created in the default domain for those users

q Double-click on one of the new mailboxes to display its properties. Observe that the full name matches what is in the database

q Send mail to one of the new mailboxes, and verify that it is delivered and can be retrieved using POP or IMAP. Note that the password to use is the one specified in the database

Database Mail List Plugin Example

This is a step-by-step example of how to set up a simple database list with Microsoft Access:

1. Install Microsoft Access
2. Install the Microsoft Access ODBC driver
3. Create a data source for the default domain

q Go to the control panel and start the **ODBC Data Source Administrator**.

q Select the **System DSN** page

q Click the **Add** button

q Select the Microsoft Access driver and click **Finish**

q Type **Default** as the data source name

- Optionally, enter a description of the data source
- Click **Create** to create a new database
- Enter a name for the new database file (of type **.MDB**) and click **OK**. You will be told that the database has been created correctly
- Click **OK** to finish creating the data source
- Click **OK** once more to dismiss the ODBC Data Source Administrator

4. Create a table in the new database for your mailing list
   - Start Microsoft Access
   - Open the database you created in the preceding step
   - In the database window, select the **Tables** tab and click the **New** button
   - Select **Table Wizard** and click **OK**
   - Select the **Mailing List** sample table
   - Select the **EmailAddress** sample field and click the **>** button to add it to the fields in your new table
   - Select the **LastName** sample field and click the **>** button to add it to the fields in your new table
   - Select the **LastName** field in your new table and click **Rename** Field
   - Rename the field to **FullName** and click **OK**
   - Click **Next** to go on to the next stage in the Table Wizard procedure
   - Enter a name for the table. This will be the same as the mailing list name, so choose a name that starts with a letter and contains only letters and digits
   - Click **Next** to go on to the next stage in the Table Wizard procedure
   - Click **Finish** to complete the table creation
5. Enter information into the table
   - If the table worksheet is not already displayed, double-click on the corresponding icon under the **Tables** tab to open it
   - Under the **EmailAddress** column, enter an e-mail address
   - Under the **FullName** column, enter the corresponding name
   - Repeat until you have got several addresses in the table
   - Close the table worksheet
   - Close the database and quit Access
6. Create a mailing list in MailSite
   - Start the MailSite Console and select your default domain
   - Open the **Mail Lists** folder
   - Right-click in the mail list pane
   - Select **New Database Mail List** from the popup menu
   - Give the new mailing list a name - it must be the same name as the table you created earlier
   - Double-click the mailing list icon to display the mailing list properties. Do NOT enter anything on the Configuration page!

- Select the **`Members`** page
- If you are running the Console locally, you should see the addresses and names you entered into the table earlier

7. Test the mailing list

   - Send a mail message to the new mailing list. Everyone whose address is in the database table should receive a copy of the message

Appendix E - Database Logging

You can configure MailSite to log operational information to any ODBC database. This section explains how to configure MailSite to do this.

There are three steps:

⇒ Setting up the database
⇒ Configuring MailSite
⇒ Retrieving the logged information

We will discuss each of these in turn.

Setting up the database

You need a database that supports ODBC, such as Microsoft SQL Server (for busy sites) or Microsoft Access (less busy sites). You will probably wish to create a new database for MailSite, although you can use an existing database if you want. If your database package supports authentication you may also wish to create a database login ID and password for MailSite to use.

Your first task with the new database will be to set up an ODBC data source. Be sure to create the data source in the System page of the ODBC Data Source Administrator.

Your next task will be to create a database table in which the log information will be stored. The default MailSite configuration assumes that the table is called **`MailLog`**, but you may change this if you wish. The table should have one column for each of the fields that you wish MailSite to record - the default configuration specifies fourteen columns. The default column names, their types and default widths, and their purpose are shown below:

Column name	Type	Substitution Number	Purpose
`Tlog`	`Datetime`	`None`	Time at which the log entry was made.
`Service`	`Char(7)`	`%1`	Name of service making the log entry.
`Category`	`Smallint or tinyint`	`%2`	0 = error log; 1 = operation log; 2 = server log.
`Event`	`Smallint`	`%3`	Identifies the type of entry.
`Severity`	`Smallint or tinyint`	`%4`	0 = success; 1 = information; 2 = warning; 3 = error
`ConnId`	`Int`	`%5`	Unique number for every connection (per service), for tying together log entries relating to the same connection.
`P1`	`Char(30)`	`%6`	Text parameter, the use of which depends on the particular Event.
`P2`	`Char(30)`	`%7`	As above.
`P3`	`Char(30)`	`%8`	As above.
`P4`	`Char(30)`	`%9`	As above.
`P5`	`Char(30)`	`%10`	As above.
`P6`	`Char(30)`	`%11`	As above.
`P7`	`Char(30)`	`%12`	As above.

P8	Char(30)	%13	As above.

Here is a SQL script to create an appropriate default database structure. Note that some databases do not support **tinyint** - you can use **smallint** instead.

```
CREATE TABLE MailLog (
    Tlog      datetime,
    Service   char(7),
    Category  tinyint,
    Event     smallint,
    Severity  tinyint,
    ConnId    int,
    P1        char(30) NULL,
    P2        char(30) NULL,
    P3        char(30) NULL,
    P4        char(30) NULL,
    P5        char(30) NULL,
    P6        char(30) NULL,
    P7        char(30) NULL,
    P8        char(30) NULL)
```

Note that the parameters **P1** through **P8** must be capable of having **NULL** values.

Example (Part 1): Microsoft Access

This example shows how to set up MailSite and Microsoft Access to log details of each incoming and outgoing message. First, set up Microsoft Access and ODBC. (The example is continued later in this chapter.)

q Ensure you have installed MailSite, Microsoft Access, and Microsoft's ODBC drivers, including the Microsoft Access ODBC driver

1. Create a new database

q Start Microsoft Access
q When prompted which database to use, select **Create new blank database**
q Name the new database **MAILSITE.MDB** and specify a suitable location for it
q When the database property sheet is displayed, select the **Tables** tab and click the **New** button to create a new table
q Select **Design View** and click **OK** to start defining the table
q Create the following fields in the table. Be sure to set the field sizes correctly. (Read the help information provided with Access if you are unsure how to do this.)

Field	Type	Field Size	Comments
Tlog	Date/time		Set the Default Value to be Date()+Time()
Service	Text	7	
Event	Number	Integer	
MsgId	Text	11	This width ensures that only the most useful portion of the message ID is stored.
HostAddress	Text	15	
HostName	Text	80	
Frm	Text	100	We can't use the name "From" because it is a SQL reserved word.
To	Text	255	This is the largest size we can make a column in Access.

Size	Text	12	

- Close the **Design View** window. When prompted, name the table **MailLog**. You do not need to give the table a primary key
- Close Microsoft Access

2. Create a Data Source
   - Go to the control panel and start the ODBC Data Source Administrator.
   - Select the System DSN page
   - Click the **Add** button
   - Select the Microsoft Access driver and click **Finish**
   - Type **MAILSITESRC** as the data source name.
   - Optionally, enter a description of the data source.
   - Click **Select** to select the database file. Specify the file **MAILSITE.MDB** that you created in the preceding step
   - Click **OK** to finish creating the data source
   - Click **OK** once more to dismiss the ODBC Data Source Administrator.

You have now set up the database and ODBC data source ready for MailSite. This example is continued below

Configuring MailSite

The next step is to configure MailSite so that it logs information to your new database. Read the chapter that discusses logging carefully, and in the Database Log Configuration dialog, fill in the data source name, the user ID and password if required.

Unless you have adopted the default database table structure outlined above, you will also need to modify the **VALUES** clause in the SQL template.

You should replace **MailLog** in the default template with the name of your table. You should also replace the column names in the default template with your own column names.

If you have decided to use fewer than fourteen columns in your table, you will need to modify the **VALUES** clause in the SQL template. When adding a row to the table, MailSite replaces every occurrence of **%1** in the SQL template with the name of the server, **%2** with the category value, and so on through **%13**. (See above for a complete list of the substitution parameters.) The default SQL template records all thirteen parameters; however, you can omit parameters from the SQL template if you do not wish to log the corresponding information.

Note that the first column in the default SQL template (**Tlog**) gets its value from the **getdate()** built-in SQL function. It has no corresponding substitution parameter.

If your table uses widths for the text columns (the **Service** and **Px** columns or their equivalents in your table) which differ from the default widths, you will need to tell MailSite about the new widths. Click the Advanced button, and enter the new widths into the resulting Advanced dialog. This ensures that MailSite truncates the text values if necessary (because storing a long string in a column too small for it causes a SQL error).

Finally, select the options you wish to log to the database in each of the Server, operation and Error categories. Dismiss the configuration console. The services will now start logging information to the database.

If you have problems with database logging, turn on file logging of General Errors. The error log file should indicate the nature of the problem.

Example (Part 2): Microsoft Access

This continues the example begun in the preceding subsection. In this part, we configure MailSite to use the database we created earlier.

- In the MailSite Windows Console, open the Logs Folder and double click on the **Database Log** icon to bring up the Database Log Configuration Page q In the dialog, enter **MAILSITESRC** as the data source name. Leave the **User ID**, **Password** and **Login Timeouts** unchanged.

q In the **SQL Template** field, enter the following string:

```
INSERT INTO MailLog (Service, Event, MsgId, HostAddress, HostName, Frm,
To, Size) VALUES (%1, %3, %6, %8, %9, %10, %11, %12)
```

q Click the **Advanced** button and enter the following field lengths:

Service: **7**

1: **11**	2: **30**	3: **15**	4: **80**
5: **100**	6: **255**	7: **12**	8: **30**

q Click **OK** twice to dismiss the dialogs.

q In the Operation section of the logging page, select the **Received Message Summary** and **Transmitted Message Summary** options under the **Database** column. Turn off all other options under that column (in the Error and Server categories as well).

q Click **OK** to dismiss the dialog.

You should now find that MailSite is logging information about received and transmitted messages to the Access database.

Retrieving the logged information

MailSite does not come with any tools for examining the data in the log database. Your database package will have its own tools for running database queries. However, this section gives some brief guidance about appropriate SQL queries that you can use with the default database.

To interpret the log information, it is important to appreciate the significance of the **Event** column. This indicates what the log entry is about, and allows you to interpret the parameters ***Px*** correctly. The appendix on Event ID's lists all of Event Ids with explanations.

To obtain a list of all outgoing SMTP connections, use the SQL query:

```
SELECT * FROM MailLog
    WHERE Service='SMTPDA'
    AND Event=261
```

Another important value is the **ConnId** column. Rows that have the same **Service** and **ConnId** values relate to the same TCP/IP connection. Thus, to look at all log records relating to connection number 5432 to the POP server, you could use the query:

```
SELECT * FROM MailLog
    WHERE Service='POP3A'
    AND ConnId=5432
```

Appendix F - Emerald Integration

The Emerald software contains a Radius server for validating access to the network. The Radius server uses a Microsoft SQL Server database containing user information. If you select the Emerald Database option in the database mailbox plugin, the plugin will use the Emerald Database for mailbox authentication.

The database mailbox plugin does not contain detailed knowledge of the Emerald Database schema. All access to the database is performed by calling *stored procedures*. Two stored procedures are used: **VerifyMailUser** and **ListMailUsers**. These are shipped as part of the Emerald release 2.5 and RADIUSNT release 2.5. If you do not have them, you should approach IEA-Software (supplier of the Emerald and RADIUSNT packages) to obtain them.

You can further qualify the contents of the table through a filter expression which will form part of a **SQL WHERE** clause.

Emerald Database Example

To configure MailSite to work with Emerald, you will need to work with the person who manages the Emerald Database. Review the following configuration procedure with that person. You may need to alter the procedure slightly depending on your particular setup.

1. Install the Microsoft SQL Server ODBC driver
2. Install Emerald

(It may be installed on a different machine)

3. Create a data source for Emerald
   - On the machine running MailSite, go to the control panel and start the **ODBC Data Source Administrator**
   - Select the **System DSN** page
   - Click the **Add** button
   - Select the **Microsoft SQL Server** driver and click **Finish**
   - Type **EmeraldDataSource** (or some other suitable name) as the data source name
   - Optionally, enter a description of the data source
   - In the **Server** field, enter the name of the machine on which SQL Server is running
   - Click **Options** to display additional configuration choices
   - Enter the name of the Emerald database. The SQL Server administrator will be able to tell you this
   - Click **OK** to create a new data source
   - Click **OK** once more to dismiss the ODBC Data Source Administrator
4. Configure SQL Server to work with MailSite

(The SQL Server administrator should perform this step)

- Create a new database login called **MailServer** (or some other suitable name) and give it a password
- Ensure the new login has adequate permissions. MailSite needs to read all the tables in the database, but does not need to update them
- Ensure you have the stored procedures **VerifyMailUser** and **ListMailUsers**, and that the login you just set up has permission to execute them
- Create a new External System in Emerald called MailSite (or some other suitable name), and note the External System ID (**ESID**) which it is allocated
- Set the External System ID for the accounts that you want to use with MailSite

5. Configure the database mailbox plugin
   - On the machine running MailSite, start the MailSite configuration console and select the **Plugins** folder
   - Double click on the **Database Mailbox Plugin** icon
   - Enter the **Data Source Name**, the **Data Source Login** and the **Data Source Password** from above
   - Select the **Emerald Database** type, and click the **Configure** button to edit the configuration information for the database

- Enter the **ESID** value for MailSite from above
- Click **OK** to save the Emerald database configuration
- Click **OK** to dismiss the database plugin configuration dialog

6. Add mailboxes from the database to MailSite
   - In the **Mailboxes** page, ensure that the default domain is selected. Right-click in the display area and select **New Database Mailbox** from the popup menu
   - You will see a list containing the Emerald users who have blank domain entries. Select one or more of those users and click **Add**. New mailboxes will be created in the default domain for those users
   - Double-click on one of the new mailboxes to display its properties. Observe that the full name matches the database
   - Send mail to one of the new mailboxes, and verify that it is delivered and can be retrieved using POP or IMAP. Note that the login password is the one specified in the database

Appendix G - Service Command Line Syntax

The POP3A, SMTPDA, SMTPRA, IMAP4A, HTTPMA, MAILMA and LDAP3A programs may be executed from the command line. The POP3A syntax is described below. The syntax for the other programs is the same.

Syntax

```
POP3A [-remove | -install] [-version][-ipaddress] [-status]
      [-start] [-stop]     [-pause]  [-resume]    [-silent]
```

Parameters

```
-control <number>  Service control switched, please see numbers below
         130    Generate dump file safely
         131    Crash Deliberately
         132    Generate dump file without entering critical section

-install   Add the POP3 service to the services database
-version   Report the version number of POP3 service
-ipaddress Report the IP addresses on which POP3 service listens
-status    This reports the current status of the
           POP3 service - i.e. whether or not it is running
-start     This starts the POP3 service
-stop      This stops the POP3 service
-pause     This pauses the POP3 service if it is running
-resume    This starts the POP3 service if it is paused
-remove    Remove the POP3 service from the services
           database.  This will also delete the POP3
           server-specific configuration information
           from the Registry
-silent    Do not display a result dialog form
```

Notes

`-silent` is the only parameter that can be combined with another parameter.

Appendix H - IMAP4 ACLs

This section describes issues relating to IMAP folders and to Access Control Lists (ACLs).

IMAP Folders

Each IMAP mailbox has to store information about each message in the mailbox (or folder). The IMAP server keeps such information in four files:

File	Purpose
`folder.imp`	holds the per message information such as its flags and the name of the file holding the actual message.
`subscrib.imp.user`	is used to record if the user has subscribed to the folder.
`keyword.imp`	holds the set of user definable keywords associated with the folder. Up to 63 separate keywords can be associated with each folder.
`acl.imp`	holds the access control list for the folder.

An IMAP mailbox/folder is in effect a directory that holds all the information about the mailbox. Normally the messages are held in the same directory as the **`*.imp`** files but in some circumstances the messages will actually be held in a separate directory. (A collection of news messages for example would be held in one directory and which would be accessed by all users although an individual user's view of such a message collection would be held in a separate per user directory).

The default IMAP inbox corresponds to the **`user\inbox`** directory. Any personal folders created by the user are mapped as sub directories of the **`inbox`** directory. The association of folders and directories is shown (by example) in the table below

IMAP folder	Directory
Inbox	user/inbox
Development	user/inbox/development
Development/internet	user/inbox/development/internet
Development/wan	user/inbox/development/wan
expenses	user/inbox/expenses

By default, users will have access only to their own folders, but they can make some or all of their folders accessible to other users by creating access control lists for the folder. The access control list allows the user to specify which users are to have access to the folder and the type of access they are allowed.

To access these shared folders a user would specify the name of a folder as:

`#shared/username/foldername`

The **`#shared`** tag tells the server that the folder is not the user's own folder and that the next component of the mailbox name is the name of the user who owns the folder.

All the accessible folders of another user can be found by using an IMAP LIST command with a mailbox name such as **`#shared/username/*`**, and all the accessible folders can be obtained by a LIST command with a mailbox name of **`#shared/*`**.

ACL files

The access rights for a folder are held in the file **ACL.IMP**, located in that folder. Each such access control list (ACL) file contains a sequence of ASCII text records in the format:

```
name access-right access-right access-right
```

Where spaces are used to separate the components. Any records starting with a semicolon are ignored and treated as comment lines. The name must be the name of an individual user (with her own mailbox). The name anybody specifies the access rights available to all users. To determine the rights for a user, the access control file is scanned from top to bottom and the specified user accumulates rights - unless the access right is none in which case the user will have no access rights. (In a future version the name can be the name of a mailing list and every user in the list will have the specified access rights).

The access-right can be one of the following:

Access	Description
None	no access allowed
lookup	to allow the folder name to be reported by LIST/LSUB.
read	to allow a user to select or examine a folder and search or copy from the folder.
write	to allow the user to update the flags in a folder and delete messages
insert	to allow the user to append or copy into the folder
create	to allow the user to create sub-folders
post	to allow the user to send mail (not enforced)
rename*	to allow the user to rename the folder
administer	to allow the user to update the access rights
full	gives the user all possible rights
delete*	to allow the user to delete the folder

The access rights marked with * are extensions to the access rights that are standardized in the IMAP ACL extension.

The IMAP server supports stronger authentication mechanisms, through the AUTHENTICATE command. This command is generic - it takes a parameter that identified the actual authentication mechanism that the mail client wishes to use.

Appendix I - SMTP Protocol

Proper use of some of MailSite's security features requires an elementary understanding of the SMTP protocol. An SMTP client program makes a TCP connection to an SMTP server program (in this case, to MailSite). The SMTP client then issues an SMTP command, often followed by parameters; on receiving the command, the SMTP server performs some action and returns a response indicating success, temporary failure, or permanent failure of the action. The client and server continue to exchange commands and responses in order to transfer mail messages from the client to the server. When the client has no more mail to send, it will terminate the connection.

A typical exchange is shown below. Lines starting **`C:`** are sent by the client; lines starting **`S:`** are sent by the server. (Of course, the **`C:`** and **`S:`** are not actually part of the protocol!)

(Client establishes TCP connection)	
S: `220 myserver.mycompany.com ESMTP receiver ready`	Initial greeting from SMTP server
C: `EHLO theclient.somewhere.com`	This command identifies the client to the server and requests a list of server capabilities. Sometimes the (older) HELO command is used instead.
S: `250- myserver.mycompany.com` S: `250-SIZE 0` S: `250-ETRN` S: `250 8BITMIME`	The server responds with its identification and a list of the protocol extensions it supports.
C: `MAIL FROM: <`mailbox@somedomain.com`> SIZE=1234`	The client initiates a message transfer with the MAIL FROM command. The address folloging the command is called the “return path” – it indicates where any non-delivery reports for this message should be sent. In this example, the client indicates the size of the message to the server.
S: `250` mailbox@somedomain.com `OK`	The server confirms that it is happy to accept mail from this address.
C: `RCPT TO: <`user1@mycompany.com`>`	The client specifies a recipient for the message.
S: `250` user1@mycompany.com `OK`	The server confirms that it is happy to deliver the message to that recipient.
C: `RCPT TO: <`user2@otherdomain.com`>`	The client specifies another recipient for the message.
S: `551 We do not relay mail to otherdomain.com.`	The server rejects the recipient, giving its reason. Note that “success responses start with a ‘2’ whereas (permanent) “failure” responses start with a ‘5’.
C: `DATA`	The client indicates it is ready to send the message itself.
S: `354 Please send message data`	The server is ready to accept the data.
C: (message data)	The client sends the message data, terminated by a single dot on a line by itself.
S: `250 message received`	The server confirms it has received the message, and accepts responsibility for

	transferring it to the acknowledged recipients.
C: `QUIT`	The client is finished transferring messages.
S: `221 Bye`	Server responds to the QUIT command.
(Client closes connection)	

Other SMTP commands not illustrated above include: **`VRFY`** (verifies an address); **`ETRN`** (requests that the mail server initiates delivery to a specified domain); and **`AUTH`** (provides secure authentication of the client).

If you'd like to know more about the SMTP protocol, consult RFC 821 and RFC 1123 (available from **`http://www.ietf.org/`**).

Appendix J - Event IDs

HEX	ID	Description
0x0001	1	%1 service terminating.
0x0002	2	%1 service pausing.
0x0003	3	%1 service resuming.
0x0000	0	Windows Sockets call %1 failed with error %2.
0x0100	256	The %1 service is starting.
0x0101	257	The %1 service is stopping.
0x0102	258	The %1 service has loaded new configuration information.
0x0103	259	>>> %1
0x0104	260	<<< %1
0x0105	261	Outgoing SMTP call established to %1 at %2.
0x0106	262	Outgoing SMTP call to %1 completed at %2.
0x0107	263	Outgoing POP call established to %1 at %2.
0x0108	264	Outgoing POP call to %1 completed at %2.
0x0109	265	Incoming SMTP call from %1 at %2.
0x010A	266	Incoming SMTP call from %1 completed at %2.
0x010B	267	Incoming SMTP call from %1 aborted at %2.
0x010C	268	Incoming POP call from %1 at %2.
0x010D	269	Incoming POP call from %1 completed at %2.
0x010E	270	Incoming POP call from %1 aborted at %2.
0x010F	271	Incoming management call from %1 at %2.
0x0110	272	Incoming management call from %1 completed at %2.
0x0111	273	Incoming management call from %1 aborted at %2.
0x0112	274	Incoming IMAP call from %1 at %2.
0x0113	275	Incoming IMAP call from %1 completed at %2.
0x0114	276	Incoming IMAP call from %1 aborted at %2.
0x0115	277	Incoming HTTP call from %1 to %3 at %2.
0x0116	278	Incoming HTTP call from %1 completed at %2.
0x0117	279	Incoming HTTP call from %1 aborted at %2.
0x0118	280	Incoming LDAP call from %1 accepted at %2.
0x0119	281	Incoming LDAP call from %1 completed at %2.
0x011A	282	Incoming LDAP call from %1 aborted at %2.
0x011B	283	Incoming SMTP call from %1 closed by client at %2.

0x011C	284	Incoming POP call from %1 closed by client at %2.
0x011D	285	Incoming POP call from %1 closed due to timeout at %2.
0x011E	286	Incoming SMTP call from %1 closed due to timeout at %2.
0x011F	287	MailFilter2 function "%1" succeeded with data : %2
0x0120	288	MsHimalaya function "%1" succeeded with data : %2
0x0121	289	The %1 service is suspending; %2
0x0122	290	The %1 service is resuming.
0x0200	512	SMTP command failed when talking to %3: <<< %1 >>> %2
0x0201	513	SMTP command failed when talking to %3: >>> %1 <<< %2
0x0202	514	POP command failed when talking to %3: <<< %1 >>> %2
0x0203	515	POP command failed when talking to %3: >>> %1 <<< %2
0x0204	516	IMAP command failed when talking to %3: >>> %1 <<< %2
0x0205	517	Authentication failed for mailbox %1 in domain %2 with error %3
0x0206	518	Authentication failed for mailbox %1 in domain %2 with error %3 client IP address %4
0x0300	768	Function "%1" failed with error: %2
0x0301	769	C run-time library function "%1" failed.
0x0302	770	The service could not determine the IP address of this computer. Please check that TCP/IP is correctly installed and configured.
0x0303	771	InitThisService() failed with error %1 at checkpoint %2.
0x0304	772	The authentication DLL %1 could not be loaded: error %2.
0x0305	773	Unable to access the %1 entry point in the authentication DLL %2.
0x0306	774	The authentication DLL %2 refused to support the server reason code = %1.
0x0307	775	Memory allocation error (%1) detected at line %2 in module %3.
0x0308	776	This component is not licensed for use.
0x0309	777	This software is not licensed for this operating system.
0x030A	778	The license for this software has expired. Please contact your supplier.
0x030B	779	The license key for this software is missing or invalid. Please contact your supplier for a valid license key.
0x030C	780	The license key for this software failed validation (reason unspecified).
0x030D	781	The license key for this software is in an unrecognised format.
0x030E	782	The license key for this software is not in a recognised format.
0x030F	783	There are more than the licensed maximum number of mailboxes.
0x0310	784	There are more than the licensed maximum number of mail lists.
0x0311	785	Network I/O error %2 encountered when sending command to %1.
0x0312	786	Network I/O error %2 encountered when sending command response to %1.
0x0313	787	Network I/O error %2 encountered when awaiting command from %1.

0x0314	788	Network I/O error %2 encountered when awaiting response from %1.
0x0315	789	Network I/O error %2 encountered when transmitting file to %1.
0x0316	790	File I/O error %2 encountered when reading message data from %1.
0x0317	791	File I/O error %2 encountered when writing message data to %1.
0x0318	792	Network I/O error %2 encountered when sending message data to %1.
0x0319	793	Network I/O error %2 encountered when reading message data from %1.
0x031A	794	Message %1 is dead: %2
0x031B	795	When recording an event in the logging database execution of a SQL statement failed. SQL statement: %1 Error code: %2 Explanation: %3 Error source: %4
0x031C	796	Could not connect to the logging database. Data source: %1 Error code: %2 Explanation: %3 Error source: %4
0x031D	797	The license key is for a different version of the product.
0x031E	798	Could not create directory %1. The Win32 error code was %2.
0x031F	799	Could not initialise domain manager. The Win32 error code was %1.
0x0320	800	Could not initialise mailbox manager. The Win32 error code was %1.
0x0321	801	Could not initialise mail list manager. The Win32 error code was %1.
0x0322	802	Could not determine DNS server address.
0x0323	803	Error %2 encountered when reading recipient file %1.
0x0324	804	Error %3 encountered in function %4 when attempting to open mailbox %1 in domain %2.
0x0325	805	The outgoing SMTP connection to %1 was unexpectedly closed by the remote host while the following command was in progress: %2
0x0326	806	Could not add message %1 to mail list archive: %2
0x0327	807	GetMailboxClusterNode failed on mailbox %1 in domain %2 with error: %3
0x0328	808	SetMailboxClusterNode failed on mailbox %1 in domain %2 with error: %3
0x0329	809	GetClusterNodeInfo failed for host name%1' with error: %2
0x032A	810	The licensed mailbox limit has been exceeded. The service is terminating.
0x032B	811	The connection is in an invalid state (code %1).
0x032C	812	Network I/O error %2 in state %3 encountered on connections with %1.
0x032D	813	Could not open message %1 - error %2.
0x032E	814	Could not open folder %1 for mailbox %2 - error %3.
0x032F	815	Could not add message to folder %1 for mailbox %2 - error %3.
0x0330	816	Could not start asynchronous file copy from %1 to %2. The error code was %3.
0x0331	817	Could not initialise mail folder manager. The Win32 error code was %1.
0x0332	818	MailFilter1 function "%1" failed with error: %2
0x0333	819	MailFilter2 function "%1" failed with error: %2
0x0334	820	MailFilter3 function "%1" failed with error: %2
0x0335	821	MsHimalaya function "%1" failed with error : %2

0x0336	822	This mail server is not licensed for clustering and another mail server was detected using the same configuration database. The service is terminating.
0x0337	823	Failed to send a message to "%1" from "%2" while %5 The message was to have subject "%3" and content: %4
0x0338	824	SQLConnector database exception Error code: %1 Explanation: %2
0x0339	825	SQLConnector database connection counters Connection count: %1 Exception count: %2 Transaction count: %3 Average duration: %4
0x1100	4352	The %1 service will retry outstanding domains matching "%2".
0x1101	4353	Message %1 sent at %2 to %3 (%4). Size: %7 bytes Return-path: %5 Recipients: %6
0x1102	4354	Looking up %1 with DNS request ID %2
0x1103	4355	Send the DNS request to %1
0x1104	4356	Response received from %1
0x1105	4357	DNS response code (RCODE) %1 for DNS request ID %2.
0x1106	4358	The response contains %1.
0x1107	4359	AN Record: Name %1 2%
0x1108	4360	MX Record: Preference %1 Name %2.
0x1109	4361	AR Record: Name %1 2%
0x110A	4362	A Record: IP Number %1.
0x110B	4363	Response truncated. Sending DNS query to %1 using TCP.
0x110C	4364	NS Record: Name %1 2%
0x110D	4365	NS Record: Name server %1.
0x110E	4366	Dialup connection to %1 successfully established at %2.
0x110F	4367	Dialup connection to %1 successfully hung up at %2.
0x1200	4608	Mailbox agent failed when executing on %1: error %2.
0x1201	4609	Could not copy %1 to %2: error %3.
0x1202	4610	Could not build mailbox agent command line with %1 and %2 The error code was %3.
0x1203	4611	Could not execute mailbox agent command line %1. The error code was %2.
0x1204	4612	Could not autoforward message %1 on behalf of %2@%3. The error code was %4.
0x1205	4613	Could not create autoreply message to %1 on behalf of %2. The error code was %3.
0x1300	4864	%1 could not be loaded. Dialup is disabled.
0x1301	4865	Cannot create or write to file %1 for message from %2.
0x1302	4866	Query ID mismatch in DNS response. Sent %1 received %2.
0x1303	4867	Truncated DNS response for domain %1.
0x1304	4868	The incoming message %1 from %2 cannot be found.
0x1305	4869	The gateway %1 is invalid or does not exist.
0x1306	4870	Autoreply to message %1 failed.
0x1307	4871	The route %1 is invalid or does not exist. It will be ignored.

0x1308	4872	The message %1 in directory %2 is invalid.
0x1309	4873	The SMTP Delivery Service could not delete file %1 due to system error %2. Please delete the file manually.
0x130A	4874	The message file %1 for message %2 could not be opened.
0x130B	4875	The incoming message file %1 from %2 cannot be found.
0x130C	4876	Cannot create or write to file %1 for message from %2.
0x130D	4877	Autoreply to message %1 failed.
0x130E	4878	The incoming message file %1 from %2 is invalid.
0x130F	4879	No response from any DNS server when searching for %1.
0x1310	4880	Truncated DNS response for domain %1.
0x1311	4881	Query ID mismatch in DNS response. Sent %1 received %2.
0x1312	4882	DNS response code (RCODE) indicates an error %1.
0x1313	4883	Failed to parse the DNS response.
0x1314	4884	Reached the maximum recursion limit. Failed to look up %1.
0x1315	4885	Could not dial out to %1. %2
0x1316	4886	Could not hang up connection to %1. %2
0x1317	4887	Status error during hang up of connection to %1. %2
0x1318	4888	Error executing dialup delivery trigger command %1
0x1319	4889	Error on dialup connection: %1
0x131A	4890	Dialup connection terminated unexpectedly.
0x131B	4891	Unexpected state of dialup connection: %1
0x131C	4892	Cannot lock "%1": error code %2.
0x131D	4893	Cannot move "%1" to "%2": error code %3.
0x131E	4894	Cannot start writing to %1: error %2.
0x131F	4895	Cannot start reading from %1: error %2.
0x1320	4896	The recipient file %1 contains multiple message IDs.
0x1321	4897	Unexpected block size returned when reading recipient file %1.
0x1322	4898	Cannot create or write to file %1 for message from %2. The error code was %3.
0x2100	8448	Message %1 received at %2 from %8 (%4 [%3]). Size: %7 bytes Return-path: %5 Recipients: %6
0x2101	8449	Address %1 resolves to %2.
0x2102	8450	The address %1 (%2) was found in the Realtime Black List.
0x2300	8960	Asynchronous DNS completion with WinSock error %2 on unknown task handle %1.
0x2301	8961	DNS reverse lookup of %1 fails with error %2.
0x2302	8962	AsyncDnsAccessOpen failed in %1.
0x2303	8963	RBL lookup not performed - the RblDomain name is empty.
0x2304	8964	DNS lookup of %1 not performed. The AsyncDnsGetHostByName error code was %2.

0x2305	8965	DNS lookup of %1 not performed. The AsyncDnsGetHostByAddress error code was %2.
0x2306	8966	Could not rename %1 to %2 The error code was %3.
0x2307	8967	Could not lock directory %1 The error code was %2.
0x2308	8968	Could not build command line with %1 and %2 The error code was %3.
0x2309	8969	Could not execute command line %1 The error was: %2.
0x230A	8970	Could not create new thread for %1. The error code was %2.
0x3300	13056	File I/O error %2 encountered when creating/opening a file in CMD %1.
0x3301	13057	File I/O error %2 encountered when reading from file in CMD %1.
0x3302	13058	File I/O error %2 encountered when writing to file in CMD %1.
0x3303	13059	File I/O error %2 encountered when setting file pointer in CMD %1.
0x3304	13060	File I/O error %2 encountered in GetFileSize in CMD %1.
0x3305	13061	The mailbox for %1 in %2 is in use.
0x3306	13062	Cannot determine mailbox directory for %1 in %2.
0x4100	16640	>>> %2 %3 %4
0x4101	16641	<<< %2
0x4102	16642	IMAP4 log record switched due to size of log at %1.
0x4103	16643	IMAP4 log record reopened for connection from %1 and user %2 at %3.
0x4104	16644	... %2
0x4105	16645	Fetch command duration: %1 seconds
0x4300	17152	IMAP4 Change Password command too long: >>> %1
0x4301	17153	The UID of message %1 in folder %2 for mailbox %3 changed unexpectedly from %4 to %5 at location %6.
0x5300	21248	The directory %1 could not be created.
0x5301	21249	Needs %1.dll version %2 found version %3.
0x6300	25344	Cannot change current directory to "%1".
0x6301	25345	Error opening log file "%1" - logging temporarily disabled.
0x6302	25346	Error writing to log file "%1" - logging temporarily disabled.
0x6303	25347	Network I/O error %2 encountered when reading HTTP request from %1.
0x6304	25348	Network I/O error %2 encountered when sending HTTP response to %1.
0x6305	25349	HTTP command failed when talking to %1: >>> %2 <<< HTTP/1.0 %3 %4

Appendix K - Glossary

Agent: An agent is a program that is executed by MailSite whenever a message arrives to the system, to a mailbox, to a mail list, or to a mail list processing address. Agents allow you to extend MailSite's functionality by adding sophisticated message-handling abilities, such as checking e-mail for virus attachments or archiving messages.

Alias: An alias is a delivery rule that causes messages received for a particular e-mail address to be redirected to another e-mail address. maps one e-mail address to another. mapping of one e-email

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 HOSTS table is used to maintain a local list of TCP/IP names and addresses. On your Windows NT machine the HOSTS table can be found in: **`%WINDIR%\SYSTEM32\DRIVERS\ETC\HOSTS`**. On your Windows 95 machine the HOSTS table can be found in: **`%WINDIR%.`** The file is in ASCII format and can be edited using **`NOTEPAD`**. Any changes will take effect immediately.

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: A moderator is a user who is responsible for managing a mail list. Moderators can define the parameters associated with the list, set the mail list's membership, and control the content of messages posted to the list.

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: Remote Access Service (RAS) provides network connectivity for an NT machine over the serial (modem) port. The capability of this connection nearly matches the capability of a direct network connection using an Ethernet board, for example. The main difference is that some event needs to make and break the RAS connection; whereas an Ethernet connection is always available.

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

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
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
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.
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 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 – 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.
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 <BR> 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.
LocalLanguageJoumal	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 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