Table of Contents

1. Introduction
   1.1. Introduction  
   1.2. Prerequisites  
   1.3. How Internet Email Works  
   1.4. What's New in Version 4 
2. Overview
   2.1. Overview 
   2.2. Structure of MailEnable  
   2.3. Administration  
   2.4. Email Delivery Flow 
3. Installation
   3.1. Installation Overview  
   3.2. Installation process 
   3.3. Upgrading 
      3.3.1. Upgrading Overview  
      3.3.2. Configuration repository location  
      3.3.3. Replace configuration files 
   3.4. Post-installation configuration 
      3.4.1. MailEnable Diagnostic Utility 
      3.4.2. Check and configure DNS settings 
      3.4.3. To set up PTR records under Microsoft's DNS Server 
4. Administration
   4.1. Administration Overview  
   4.2. Messaging Manager 
      4.2.1. Messaging Manager Overview  
      4.2.2. Messaging Manager - General settings 
      4.2.3. Security and authentication settings 
4.3. Post office configuration 
   4.3.1. Post office configuration Overview 
   4.3.2. Authentication settings
5.5.2. Post office connector - General 56-57
5.5.3. Logging 57
5.6. IMAP Service 57
  5.6.1. IMAP Service Overview 57-58
  5.6.2. IMAP - General 58-59
  5.6.3. Logging 59
5.7. HTTPMail Service 59
  5.7.1. HTTPMail Protocol 59-60
  5.7.2. Configuration 60-61
5.8. Mail Transfer Agent (MTA) 61
  5.8.1. MTA Overview 61
  5.8.2. MTA properties 61-62
5.9. Web mail 62
  5.9.1. Webmail Overview 62-63
  5.9.2. Web mail configuration 63
    5.9.2.1. Web mail configuration - General 63-64
    5.9.2.2. Logging 64
    5.9.2.3. Spam 64-65
  5.9.3. Configuring web mail 65
    5.9.3.1. Configuring web mail Overview 65
    5.9.3.2. Publishing web mail through host headers 65
    5.9.3.3. Publishing web mail through virtual directories 65-66
  5.9.4. Web mail properties 66
  5.9.5. Browser compatibility 66-67
  5.9.6. File Storage 67-68
5.10. Web administration 68
  5.10.1. Web administration server configuration 68-70
  5.10.2. Web administration properties 70
  5.10.3. Accessing web administration 70-71
5.11. COM component 71-73
  5.11.1. Configuring the server 73
  5.11.2. Using the COM component 73-75
11.3. DNS error codes and descriptions 112-113
11.4. Diagnosing Outlook/Outlook Express error codes 113
11.5. Manually testing if MailEnable can send mail to remote servers 113-115
11.6. Log analyser 115
11.7. Configuring redundant or backup (MX) mail servers 115-116
11.8. Increasing upload limit for Windows 2003 116
11.9. Logical architecture and message flow 116-118
12. Glossary 119
13. Warranty 120
1 Introduction

1.1 Introduction

Contact the MailEnable Team

MailEnable Pty. Ltd. (ACN 100 453 674) is an Internet Messaging product company that develops, markets and supports software for hosted messaging solutions. MailEnable’s mail server suite provides a tightly integrated hosted messaging solution for the Microsoft platform.

MailEnable is a 100% privately owned Australian Company and was established in early 2001. MailEnable’s customers include some of the world’s largest Internet/Application Service Providers, Educational Institutions, Organizations, Government Agencies and Corporates.

59 Murrumbeena Road
Murrumbeena Victoria, Australia
Tel: +613 9563-4177 (AEST)
Fax: +613 9530-4066
Email: info@mailenable.com

Support

For any support issues including program defects and general support inquiries, please follow the link below. The web page displayed here shows a form, which once correctly filled out, will permit the MailEnable support team to assist in any support requests.

http://www.mailenable.com/support/supportrequest.asp

Web site

MailEnable’s web site provides links to reference materials, product information, knowledge base, forums, etc.

Knowledge base

The MailEnable Knowledge base is available at http://www.mailenable.com/kb. It contains the latest information on user queries and application configuration issues.

Forums

MailEnable forums are found at http://forum.mailenable.com (http://forum.mailenable.com/). The forums contain public posting and replies from MailEnable users.

How to download

To download MailEnable Enterprise Edition, follow the link below to obtain the latest supported update:

http://www.mailenable.com/download.asp

Any patches and hot fixes deemed necessary for the continual use of the MailEnable product will also be made available here.

1.2 Prerequisites

Pre-requisite hardware

MailEnable will run on virtually any computer capable of running a Windows server environment. Webmail and web administration require .Net 2.0 to be installed.

Note: While the MailEnable product suite can be installed and has been tested on XP and workstation environments the company does not support these platforms.
To administer a mail server on the Internet requires knowledge of how email works. It is important to know how messages are delivered and sent, how mail servers contact each other, and how users retrieve their email. This will help in diagnosing problems, tracking faults, and knowing who to contact (or blame!) when something goes wrong. The information in this section is not specific to MailEnable; this applies to all mail servers. This information is essential to know in order to properly administer an Internet mail server.

### Email Clients

An email client is a software application that is used to send, receive, store and view e-mail.

Some examples of email clients include

- Microsoft Outlook
- Microsoft Outlook Express
- Mozilla Thunderbird
- Pegasus Mail

### Email server

An email server holds and distributes e-mail messages for email clients. The email client connects to the email server and retrieves messages. An email server may also be known as a mail server, or a mail exchange server.

### Sending and receiving mail

To send Internet e-mail, requires an Internet connection and access to a mail server. The standard protocol used for sending Internet e-mail is called SMTP (Simple Mail Transfer Protocol). The SMTP protocol is used to both send and receive email messages over the Internet.

When a message is sent, the email client sends the message to the SMTP server. If the recipient of the email is local (i.e. at the same domain as the email originated from) the message is kept on the server for accessing by the POP, IMAP or other mail services for later retrieval.

If the recipient is remote (i.e. at another domain), the SMTP server communicates with a Domain Name Server (DNS) to find the corresponding IP address for the domain being sent to. Once the IP address has been resolved, the SMTP server connects with the remote SMTP server and the mail is delivered to this server for handling.

If the SMTP server sending the mail is unable to connect with the remote SMTP server, then the message goes into a queue. Messages in this queue will be retried periodically. If the message is still undelivered after a certain amount of time (30 hours by default), the message will be returned to the sender as undelivered.

### 1.4 What’s New in Version 4

The following sections outlines the new functionality provided in Version 4 of MailEnable.

#### SyncML (Enterprise Only)

SyncML allows the synchronization of MailEnable calendar, tasks and contacts with Mobile devices (Phones, PDAs and...
Mobile Webmail Client (Enterprise Only)

MailEnable now includes a mobile webmail client that can be used on WAP Enabled devices, browsers and mini-browsers to access mail remotely. The client is designed to provide core messaging functionality over low bandwidth.

The Mobile WebMail Client is ideal for those who wish to manage their mail via a mobile appliance or PDA. It can also be used in a regular browser for those who wish to read their e-mail without loading the graphics and scripts of MailEnable's regular webmail client.

(http://www.mailenable.com/version4/mobile/demo.asp)

Server Storage / My Files

MailEnable now allows users to store documents, files, images, video etc on the MailEnable server in a new storage location. The server storage presents itself as a remote storage location to which you are able to save attachments from messages. You can also then access files from server storage and attach them to your e-mail messages without needing to upload them from your webmail client.

Server Storage Publishing

Mail client users are able to publish folders from their "My Files" Server Storage to the web community. As an example, a webmail user may wish to publish their vacation photos for others to view on the web. To do this, the webmail user simply places their files on server storage (either by uploading them or extracting from e-mail messages) and configures their storage folder to be read by internet users. Other webmail users are then able to use the published URL to view/access the content via their browser and can toggle through the contents of the published folder.

This powerful addition provides a simple and hassle free method for MailEnable end users to publish images, presentations or documents to the greater community.

MailEnable Connector for Microsoft Outlook (Enterprise Only)

MailEnable provides Outlook tightly coupled connectivity to MailEnable. The MailEnable Connector for
Outlook provides message store (messages, calendar, contacts and tasks), global address book, transport, public folders and free and busy integration for Microsoft Outlook. Specifically, Outlook users will now have seamless integration between Outlook folders, messages, calendar, contacts and tasks and the MailEnable message store.

The connector receives real-time updates from MailEnable, at a property level. Specifically, if a user updates the details of a contact in webmail, any connected Outlook users will see the contact details update in Outlook in real time.

The connector provides a single integrated solution for integrated messaging/scheduling/addressbook within the Outlook client, providing a comparable experience to the level of integration experienced by Microsoft Exchange End Users.

The connector also supports delegate access to other mailboxes, meaning that users can share mailboxes, folders, contacts etc to other Outlook and webmail users.

This also provides the massive benefit of allowing MailEnable to tightly integrate with applications that currently interface with the Outlook client. As specific examples, desktop phone synchronization and contact management software that integrate with Microsoft Outlook will interact in real time with MailEnable.

The Enterprise Edition Server will provide a flexible licensing model for Outlook clients allowing administrators to purchase bulk license packs according to their user requirements.

MailEnable is excited at the prospect of bringing this functionality to the market and think that the end user experience and affordability will make it very compelling indeed.

MailEnable Webmail Client

MailEnable's WebMail interface has been updated with some feature enhancements as well as style and layout changes.

The updated webmail client boasts some significant speed improvements over previous versions. The Version 4 webmail client also includes some cost/management time saving features such as a forgotten password / saved question and answer feature.

Version 4.x webmail includes a new graphical treatment/skin called 'Gun Metal'. The existing skin distributed with Version 3.x has been updated for Version 4.x and is also available.

Extended Calendar Control

MailEnable has replaced its calendar to provide a more usable and practical calendar for webmail users. The new calendar allows you to manage your appointments via drag and drop and inline editing. It also supports calendar overlays to allow you to view calendars simultaneously. Webmail users can now also see free and busy times across multiple months.

The extended calendaring features provide group scheduling features and allow webmail users to overlay calendars of multiple users.

These calendar enhancements, combined with MailEnable's new mobile connectivity provide a powerful feature set for mobile web users.

MailEnable DomainKeys (DKIM)

MailEnable's Domain Keys (DKIM) implementation provides inbound validation and outbound signing of messages. The extensive filtering provided by MailEnable allows you to discriminate messages according to their domain key validation. Administrators can either use inbuilt simple criteria or tailor complex scripts according to filtering requirements.

Improved Monitoring and Security (Mailbox Activity Report)
MailEnable Enterprise Edition Version 4 includes end-user activity reporting. This allows mail users to view the last 5 days of significant activity performed against their mailbox. For example, a user can see whether messages were deleted from their mailbox or even whether an e-mail message to their account has been greylisted/suspended for later delivery.

Abuse Detection and Prevention Policy
Currently, MailEnable can permanently block IP addresses if they issue too many invalid commands to the server. MailEnable can also lock out accounts after too many failed password attempts. Version 4 of MailEnable provides a new feature whereby services to maintain a list of IP addresses and record any significant activity. This record can then be used to determine whether the source addresses have violated a security policy and should be temporarily blocked. As an example, an IP address that is connecting and attempting to spoof user accounts might be blocked for an hour as a means of protecting password dictionary attacks.

SMS Connector (Enterprise Only)
MailEnable Enterprise Edition includes an SMS connector to allow you to send SMS messages from MailEnable. Administrators are able to define SMTP addresses that are mapped to mobile phones. Any messages received to that address are processed by the connector.

Mail messages are queued to an SMS message queue where they are picked up by the SMS connector for pre-processing and delivery as an SMS message.

The SMS Connector allows you to select from an array of SMS transmission carriers as well as providing connectivity to any phones connected via USB/Serial interfaces. The Generic/USB SMS device is useful for testing the functionality of the connector without needing to sign up with a bulk sms carrier.

MailEnable has the ability to throttle the usage of the SMS connector and to procure message contents before they are converted to SMS.

Log File Archiving
MailEnable version 4 allows you to archive log files into cabinet files so you may conserve disk space. Compressed files can also be purged/deleted once they become a certain age.

Message Archiving
MailEnable now has the ability to automatically collect and archive by date all messages that are processed by MailEnable. The archiving feature will allow messages to be saved to a folder named by date within a pre-selected MailEnable internal mailbox. The administrator can control which messages are archived (according to whether they are being picked up by the Mail Transfer Agent or delivered by the Mail Transfer Agent).

Advertising and Campaign Management
MailEnable's webmail client allows administrators to enable advertising for their webmail customers. The advertising feature allows banner adds to be presented either server wide, or at a postoffice level.

System Administrators are able to logically group advertising material into Campaigns. They can control the
frequency of banner rotations and the designated click through URL.

System Administrators and Postoffice Administrators can then select which campaigns they would like to distribute to users.

Feature Availability

The following table lists the availability of version 4 features in respective versions.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Professional</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar Overlays</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS Connector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SyncML</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Web Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAPI Connectivity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS SMTP Outbound support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertising and Campaign Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Storage/My files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Storage Publishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New WebMail Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Calendar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DKIM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event auditing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abuse Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log File Archiving</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Archiving</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gun Metal and Clean Skins</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple Password Prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failed Auth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Lockout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Scripting on inbound SMTP conversation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL support for POP Retrieval</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Microsoft Outlook and Exchange are registered trademarks of Microsoft Corporation.

MailEnable is a registered trademark of MailEnable Pty. Ltd.
MailEnable has multiple services that interact in order to deliver a message to a mailbox. This interaction is done by a system of queues, which are used to move the emails around. The actual moving of the messages is done by the MTA service, which is logically the central service to the whole MailEnable system. The MTA will pick up messages waiting in a queue and move them to the queue of another service to be processed.

### 2.2 Structure of MailEnable

#### Structure of MailEnable

MailEnable is comprised of Connectors, Agents and Services. The definitions of these components are described in the table below and in detailed in following sections.

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectors</td>
<td>Connectors move mail between systems or subsystems (local or remote)</td>
</tr>
<tr>
<td>Agents</td>
<td>Agents run perform specific management or operating functions for MailEnable itself. An example of an Agent is the Mail Transfer Agent. Its function is to move messages between connectors.</td>
</tr>
<tr>
<td>Services</td>
<td>Services expose MailEnable functionality to external agents or programs. An example of a service is the POP3 service. This service allows mail clients to access mail from their post office.</td>
</tr>
</tbody>
</table>

#### Services

Services allow external programs (usually email clients) to access the message store.

When a user wants to read email that has been sent to their mail server for handling, there are several mail services that can be used to retrieve the email messages so that the user can read them in their email client. These services include:
Each of these mail services is described in more detail in the Configuration of connectors, services and agents section.

Connectors
Mail connectors move mail between systems or subsystems (local or remote). A mail connector allows MailEnable to send and receive mail messages to and from external systems. MailEnable has several mail connectors: SMTP, POP Retrieval, Post office and List server connectors.

2.2.1 SMTP connector
The SMTP connector is responsible for both receiving inbound SMTP mail and delivering outbound SMTP mail.

2.2.2 Post office connector
The Post office connector is responsible for delivering mail to a post office. It processes mailbox level filters, handles quotas, auto responders, delivery events, groups and redirections.

2.2.3 List server connector
The list server connector is responsible for receiving and delivering mail to users that are subscribed to the lists.

2.2.4 POP Retrieval connector
The POP Retrieval connector will download mail from a remote POP server and deliver to a local mailbox.

Agents
2.2.5 Mail Transfer Agent (MTA)
The Mail Transfer Agent is responsible for moving messages between connectors. It also processes the pickup event and global filters.

2.3 Administration
From an administration perspective, MailEnable is comprised of the following components.

- Post offices
- Domains
- Mailboxes
- Lists
- Groups
Post offices

A post office is used to host multiple mailboxes and domains under one area. For example, to provide mail hosting for multiple companies, each company would have a post office. A post office can have multiple domains and mailboxes assigned to it. A small mail server might only have one post office. Post offices can have the same name as a domain. It is common for hosting companies to use a domain name as a post office name and to only have one domain within that post office with the same name.

Domains

Multiple domains can be assigned to a post office. At least one domain needs to be configured in order to have a valid email address.

Mailboxes

A mailbox is a repository for email. It is used to store emails for one or more email addresses. When a user connects with a mail client application (Outlook Express, Eudora, etc.), they connect to a mailbox to retrieve their email. When creating a mailbox, MailEnable will automatically create an email address for each domain in the post office, using the format `mailboxname@domain`. A mailbox can have multiple email addresses. This means a user only requires one mailbox to connect to, from which they can retrieve email from all their email addresses.

Email addresses

Each mailbox can have one or more email address mapped to it. It is only possible to add an email that matches an existing domain for the post office. When a mailbox is created, MailEnable will automatically create email addresses for each of the domains for the post office.

Lists

MailEnable contains a list server that enables people to subscribe and unsubscribe to a list. A list is an online discussion group or information mailout, where emails are sent out to all the members. People are able to post to the list (e.g. list@companyx.com), and the server will duplicate their email and send it out to all the members.

Groups

A group is an email address that maps to one or more other email addresses. For example, a group which has the recipient as staff@companyx.com can have 50 email addresses as members of this group. When someone emails staff@companyx.com, the email is duplicated and sent to all 50 members.

2.4 Email Delivery Flow
Sending Email

When mail is being sent to a non-local address, this is known as “relaying” i.e. MailEnable has to “relay” the email back out.

Requiring users to authenticate against the server prior to sending email can stop spammers from using the mail server to send email out to anyone.

When email is being delivered to a local address, this is not relaying, and MailEnable will always accept this email. This is how email is received from other mail servers on the Internet, as they do not need to authenticate.

Receiving Email

When an email arrives via SMTP, the SMTP service saves this message to its inbound queue. The MTA service is constantly checking this queue for new items. When the MTA sees the message arrive it examines the message to determine where it is to go. If the MTA service determines it is to go to a local mailbox, then it will move the message to the post office connector service outgoing queue. The post office connector will be checking its outgoing queue and can then process this message and deliver it to a users mailbox.

The naming of the Inbound/Outgoing queues may be confusing initially. But think of the queues as always relative to the MTA service. So the MTA service will check all the inbound queues of the services and move messages to the outgoing queues of the services. Services only check their outgoing queue and if they need to create a message then they will do this in their inbound queue.

Since the MTA service is the central service responsible for moving messages around the system, it is the logical place for all the global filters, and items such as anti-virus, Bayesian filtering, etc. (the features available are determined which version of MailEnable). Even messages arriving via SMTP and sent via SMTP are processed by the MTA service, since only the MTA can move the email from the SMTP Inbound queue to the SMTP Outgoing queue.

Utilizing different services in this way gives MailEnable a high level of flexibility, such as allowing services to be split across machines and to permit more than one type of service to be running on different servers. But this flexibility does create one hurdle for an administrator of MailEnable, and that is the problem of being able to track a message. A message being sent to a local mailbox will be logged in the SMTP logs, the MTA logs and the post office connector logs. Fortunately there are tools and monitoring software that come with MailEnable that makes this tracking easier, but understanding the queue mechanism will make administering the MailEnable server a lot easier.
3 Installation

3.1 Installation Overview

**Note:** Installing MailEnable requires administrative privileges on the server MailEnable is to be installed on.

Run the installation executable. The installation program will then guide the rest of the installation process. Each screen of the installation program contains data entry fields, Next, Back and Cancel control buttons.

The **Next** button proceeds to the next step of the installation process.

The **Back** button steps back through the installation process.

To exit the installation at any time, select the **Cancel** button.

3.2 Installation process

**Welcome screen**

The welcome screen informs that MailEnable is about to be installed. It also provides a warning outlining the copyright protection of the MailEnable product suite.

To continue installing the application, click on the **Next** button.

Please click the Next button to continue.

**License Agreement**

The License Agreement dialog box explains the licensing terms and conditions of installing and using the MailEnable product suite.

Read this carefully as it outlines all conceptual and legal issues between MailEnable and the End User in relation to the way the program can be used.

Please click the Yes button to continue.

**Registration details**

This screen is for entering registration details, which will be used and displayed in the Diagnostic Utility that will be outlined later in this document. Enter your name and company name in the boxes provided.

Please click the Next button to continue.

**Select installation components**

The next part of the installation process is to select the MailEnable components to install.

**MailEnable Core Components (Server)** - This will select the base programs and functionality. This option must be selected if MailEnable is being installed for the first time on this server.

**Web Administration Service (Server)** - This service will install web administration for MailEnable. This option requires that Microsoft Internet Information Services (IIS) is installed.

**Web Mail Service (Server)** - This will install web mail for MailEnable. This option requires that Microsoft Internet Information Services (IIS) is installed.

Select the components to install. Check that there is enough disk space required to install the selected components.

Please click the Next button to continue.

**Select application directory**

This specifies the location where application files for MailEnable will be installed.

Please click the Next button to continue.
Select Program Manager group
The installation wizard will now prompt for the program group in Windows for the MailEnable icons and shortcuts installed. Accept the default settings to install the icons under the “Mail Enable” Program Group. Please click the Next button to continue.

Select configuration Repository
The Configuration Repository is a place to store the configuration files of MailEnable. By default MailEnable uses a TAB Delimited file structure (flat file structure), and since the configuration files are accessed continually, consider using a fast disk I/O sub system for this storage path to improve performance.

If intending to cluster MailEnable, specify a shared file services as the Configuration Repository location. If the installation is only on a single server, use a directory that is local to that server (i.e. the default setting).

To install into a different folder, click Browse, and select another folder. If upgrading MailEnable, changing this directory will not move any existing data.

Please click the Next button to continue.

Selecting message store repository
The message store repository is where all the email data is stored. Email data can take up a large amount of disk space, so ensure a drive with plenty of space for future expansion is selected.

If intending to cluster MailEnable, specify a shared file service as the Destination folder (this can also be configured via the Administration Program after installation). For a single server installation, use a directory that is local to the server (i.e. the default setting).

Please click the Next button to continue.

Creating an initial post office
When installing MailEnable for the first time, one requirement is to create a post office. A MailEnable post office should be created for each company or organization that is hosted under MailEnable. A MailEnable post office can contain multiple domain names. It is therefore advised that post offices are named to be something more generic than the domain name. For example, MailEnable Pty. Ltd. owns domains mailenable.com, mailenable.com.au and mailenable.co.uk, so the chosen name for the post office for MailEnable Pty. Ltd. could therefore be MailEnable. The domains owned by MailEnable Pty. Ltd. would then be assigned to the MailEnable post office. Another common configuration is to name the post office the actual domain name, as this simplifies mailbox log-on (as users are often aware of the domain they log into).

A password needs to be assigned for the manager or postmaster of this new post office. The mailbox for the manager of a post office is called postmaster and is given administrative privileges for that post office (this allows the postmaster to administer the post office via web administration). It is advisable to use a complex password for this mailbox, and this password can be changed later.

Please click the Next button to continue.

SMTP connector configuration
The installation will now prompt for specific details for the SMTP Connector.

These settings are outlined in the following table (all of these settings can be changed later):

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>The first configuration setting is the Domain Name for this server. The domain name should be the domain name of the organization that owns or is operating the server. If this server is being used on the Internet, it is important that this domain name is registered. When MailEnable is sending out email to remote servers, it will announce itself as this domain.</td>
</tr>
<tr>
<td>DNS Host</td>
<td>The DNS host used by the SMTP Connector to locate mail servers. To use multiple</td>
</tr>
</tbody>
</table>
Start installation

The installation program will prompt before it commences installing files and registering the application.

Please click the Next button to continue.

The installation will now install files and display a progress window whilst the components are installed and configured.

Select web application platform (ASP or .NET)

Choose which platform to use for the web mail and the web administration interfaces. If ASP pages and icons/pictures in previous versions of MailEnable have been changed, ASP will need to be installed to continue using these. If unsure, or if this is a first installation of MailEnable, choose the default, .NET.

When installing .NET it is required that the .NET framework is installed. To verify whether the .NET framework is installed, please go to the Windows update site.

Database schema warning

If MailEnable is being upgraded from a previous version, a warning will be shown that the database schemas for the configuration storage need to be updated. If a database is being used to store configuration information the Provider Migration Utility will need to be used (see the ‘Using MySQL or Microsoft SQL Server section (‘Using MySQL or Microsoft SQL Server’ in the on-line documentation)) to ensure that the database schema is up to date. This should be done as soon as the installation is complete (do not perform this step before the installation has finished).

Please click the OK button to continue.

Select web mail site

If more than one web site is configured under IIS, the installation application will ask under which web site to install the web mail virtual directory. Install this either under the “Default Web Site” or an alternate site configured under IIS. Once the installation of MailEnable has completed, it will be possible to add or remove web mail from each of the web sites configured under IIS.

Note: Do not install MailEnable web mail under the “Administration Web Site”

Please click the Next button to continue.

The installation application will display a dialog box while it configures web mail. The configuration of web mail may take several minutes, so please be patient.

Select web mail site

Web administration is installed if it was selected as an option from the component list in the Installation process section (Section 3.2). If more than one web site is configured under IIS, the installation application will ask under which web site to install the WebAdmin Virtual Directory. Install the web administration under the “Default Web Site” or an alternate site configured under IIS.

Note: This functionality can be re-configured to another web site if required after the initial installation has been completed.

Please click the Next button to continue.

Antivirus plug-in notice

DNS addresses, enter these here, and separate the IP addresses with a space. In most cases, the same DNS host(s) should be included as configured under the network TCP/IP settings for the computer.

SMTP Port

The SMTP port is almost always set to 25. Very rarely is another port number used and it is recommended that this setting remain as 25. Corporate or hosting companies/agencies may wish to use a different SMTP port to 25 to obscure the fact that the server is running SMTP services. If unsure, leave the setting as 25.
MailEnable’s Anti-Virus Plug-in provides an interface to Anti-virus software. Once the plug-in is installed, ensure that the selected antivirus software has been installed and licensed. MailEnable anti-virus settings should be configured after installation as described in the Creating a global filter section (Section 6.2.1).

Please click the OK button to continue.

Httpmail Notice

MailEnable’s HTTP Mail (WebDAV) support will be installed on Port 8080 of the server. To access this service requires either Microsoft Outlook Express or Outlook XP configured to use the HTTP Mail provider. Please see the HTTPMail protocol section (Section 5.7.1) for more information on configuring HTTPMail support.

Please click the OK button to continue.

Completing installation

Finally, setup will inform that the installation procedure completed successfully. Please click the Finish button to complete installation of MailEnable.

The installation program will advise if a reboot is required after install or upgrade.

3.3 Upgrading

3.3.1 Upgrading Overview

To upgrade to MailEnable Enterprise from either Standard Edition, Professional or earlier Enterprise Editions, follow the same steps as outlined in the Installation and upgrading section (Section 3.1). As the same data stores are used, it is possible to run the installation over the top of the current configuration. MailEnable will detect the old version and retain the old settings (unless otherwise specified).

MailEnable set-up kits are available from the MailEnable web site at http://www.mailenable.com/download.asp

3.3.2 Configuration repository location

When MailEnable is installed over an existing installation, the installation program will prompt for the location of the configuration repository. It should default to the current configuration location as used by the existing installation of MailEnable.

3.3.3 Replace configuration files
The default setting of the installation is to **Preserve Existing Configuration Data**. Leave this option selected to retain current data and settings. To overwrite your configuration with clean installation, (i.e. do not retain post office or mailbox data) select the **Overwrite Configuration Data** option.

The installation has the option to **Backup Configuration Data BACKUP Directory**. Selecting this will ensure that the configuration repositories are backed up, which is always good practice. If you are using a database for configuration storage, this is not backed up.

Simply follow the installation wizard, verifying the settings until the wizard completes. It may be required to reboot your server at the end of the upgrade. The underlying configuration data and options are essentially the same for all MailEnable versions.

**Note**: MailEnable Enterprise by default uses the same configuration data and options as Standard and Professional, but has two-way migration wizards for changing the configuration provider (i.e. you are able to migrate data back and forth between the default TAB delimited configuration files and the database). See the Migrating data between providers section (‘Migrating data between providers’ in the on-line documentation) for more information.

### 3.4 Post-installation configuration

#### 3.4.1 MailEnable Diagnostic Utility

The MailEnable Diagnostic Utility checks the installation for system errors or warnings. The Diagnostic Utility also reports on the current system configuration. In most cases, the diagnostic report will provide enough information to determine whether the server is configured properly, or to diagnose system faults.

The MailEnable Diagnostic Utility can be found under:

1. the MailEnable Program Group under ‘System Tools’ or;
2. the MailEnable Administration Program under Servers->‘localhost’->System->Diagnose

Once the Diagnostics Utility has been selected, it may take a few seconds to load (depending on the number of domains). A web page will be invoked and will give a test output of all services installed within the MailEnable program. In order to rerun the Diagnostic through the Administration program, right click on the Diagnose icon and select ‘Refresh’ from the popup menu. Below is an example of this test output and how it is displayed. The ‘Refresh’ option can also be used if the page does not properly load.
The classes and test configurations that are run are as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version Information</strong></td>
<td>Contains all required environment data and version information.</td>
</tr>
<tr>
<td><strong>Configuration and Data Test</strong></td>
<td>Verifies that all repository stores are valid and free from any corruptions or permissions errors.</td>
</tr>
<tr>
<td><strong>Application Environment</strong></td>
<td>Checks various system files on the server that MailEnable relies on.</td>
</tr>
<tr>
<td><strong>System Services and Tests</strong></td>
<td>A test on services and whether they are correctly installed and running. Some services are not installed in all versions of MailEnable, and so therefore may fail this test. Click the Status link for confirmation of whether this is the case.</td>
</tr>
<tr>
<td><strong>Queue Status</strong></td>
<td>Calculation of the quantity of all inbound and outgoing emails is displayed here.</td>
</tr>
<tr>
<td><strong>Host TCP/IP Settings</strong></td>
<td>Basic check on IP and DNS configurations.</td>
</tr>
<tr>
<td><strong>Network Interface Report</strong></td>
<td>Check of all Network Interface Cards and validation of drivers.</td>
</tr>
<tr>
<td><strong>Mail Transfer Agent</strong></td>
<td>Reports details of the MTA service settings that can affect delivery and Antivirus/pickup event performance.</td>
</tr>
<tr>
<td><strong>SMTP Configuration Test</strong></td>
<td>Settings or properties of SMTP settings are defined. Checks security settings for this service.</td>
</tr>
<tr>
<td><strong>SMTP Relay Settings</strong></td>
<td>Relay settings are checked here - verifies that only authorized addresses can send through the mail server. See the SMTP connector - Relay section (Section 5.1.5).</td>
</tr>
<tr>
<td><strong>SMTP Inbound Bindings Test</strong></td>
<td>Provides information on the bindings to IP addresses.</td>
</tr>
<tr>
<td><strong>SMTP Outgoing Configuration</strong></td>
<td>Shows outgoing SMTP configurations.</td>
</tr>
<tr>
<td><strong>SMTP Outgoing Queue Status Test</strong></td>
<td>Shows status of messages queued to remote hosts.</td>
</tr>
<tr>
<td><strong>DNS Resolution Test</strong></td>
<td>Resolves all DNS settings.</td>
</tr>
<tr>
<td><strong>Host IP Reverse Lookup Tests</strong></td>
<td>Outlines the reverse DNS configuration settings and verifies settings. Some mail servers will reject email if there is no PTR record configured for the IP address, so if this test fails a PTR record needs to be configured.</td>
</tr>
<tr>
<td><strong>Hosted Domain Resolution Test</strong></td>
<td>Checks whether local domains have MX records.</td>
</tr>
</tbody>
</table>
In order for remote mail servers to deliver email to the MailEnable server, the correct DNS entries need to be configured in the Domain Name Services (DNS) hosting the domain records. The server should have a fixed IP address that is registered under the public DNS. If the server does not have a static IP address (i.e. the IP address changes) in order to direct emails and domains to the server, a dynamic DNS provider (e.g. no-ip.com) will be required. A dynamic DNS provider keeps track of the changing IP address and updates the DNS details accordingly. Companies that offer this service may charge a monthly fee, although there are some free services available. It is still possible to send email from MailEnable with a dynamic IP address, but unless the DNS is updated with the new IP address every time it changes, other mail servers will not be able to connect. Be aware that a number of mail servers will not accept email from the server if it does not have a static IP address, or if the server is using a cable/DSL connection.

Every domain registered on MailEnable should have mail exchanger (MX) records defined with your Internet Service Provider (ISP) or whoever is hosting the DNS.

Due to the vast array of combinations for DNS hosting and the number of vendor specific DNS implementations, consult your DNS provider for instructions or inform them of the servers published IP Address along with the domain names being hosted under MailEnable and request they configure the DNS accordingly.

If using MailEnable from a computer at your office or home, ensure that your Internet plan allows you to run a mail server. Some providers block incoming email to mail servers on their network, to avoid the possibility of spam abuse. They can also block all outgoing email that is not going through their mail server. If unsure, please contact your service provider. If MailEnable can send email correctly, but does not receive any, it is likely to be either the DNS settings, or your ISP has blocked incoming email to stop you running a mail server.

More information is available on configuring DNS in the MailEnable Knowledge Base (http://www.mailenable.com/kb).

The precise approach for configuring DNS depends on whether you are hosting your own DNS or whether an ISP or third party hosting the DNS. This section explains how you can configure your DNS if you are hosting your own DNS Server.

1. Using the DNS Management software for the DNS Server, ensure that a DNS “A” (Host) record has been created for the mail server. This record type allows the host to be identified by a host name rather than IP Address. To validate whether the A record was registered correctly, use the ping utility. Attempt to ping the host using its host name. If this works, then the A record was registered correctly.

2. Next, create an MX record that points to the A record. The way this is achieved depends on which DNS server/vendor being used.

3. When selecting a DNS for MailEnable to use, choose one that can resolve all domain names, which is not necessarily the DNS which is hosting the domain names. For example, if you host your domain names through a third party, it is unlikely that you would use their DNS IP address to resolve.

An example for registering MX records using Microsoft DNS Server is available at:
3.4.3 To set up PTR records under Microsoft's DNS Server

1. Ensure that DNS Forwarding is enabled on the server. This means that if a client cannot find DNS records on the mail server, the DNS server will forward request to your ISPs DNS servers. This can be accessed under the properties of the server - Forwarders Tab (within DNS Manager).

2. Create the Reverse Lookup Zone for address range of the public IP address (e.g.: 201.248.10.*). Create this by selecting 'New Zone' under the properties of the server (within DNS Manager).

3. Create PTR Records for all of the IPs under the Zone outlined above (within DNS Manager).

4. Ensure the primary DNS IP addresses used by MailEnable's SMTP Connector is configured to use the local DNS rather than referring upstream to your ISPs. This is much faster and more efficient. (This is done via the MailEnable Administration program under the properties of the SMTP Connector)

5. Restart the SMTP Service to place DNS Server changes into effect (Service Control Manager).

**Note:** Check with your ISP that they allow PTR referrals to your server. This can be checked using resources at [http://www.dnsstuff.com](http://www.dnsstuff.com)
4 Administration

4.1 Administration Overview

The majority of MailEnable configuration and maintenance is done through the MailEnable Administration program within a Microsoft Management Console.

Start this application by using the Start menu in Microsoft Windows and Navigating to MailEnable Enterprise by selecting:

Start>Programs>MailEnable>MailEnable Enterprise

The MailEnable Administration program will open and you will be presented with a window similar to the following:

The tree view on the left navigates through the various components of MailEnable in order to configure them.

The first item in the display is MailEnable Management. By right clicking on this icon, the option to “Connect to a MailEnable cluster” is available. This section only describes how to configure a single server installation, refer to the Cluster management section (‘Cluster Management’ in the on-line documentation) for information covering multiple server configuration.

The second item in the display is Messaging Manager. This is where various global settings, such as Domains, Post Offices and Mailboxes can be modified. Explanations of these items are contained later in this document. The panel to the right of the tree view provides either icons for options, or a view of the configuration data determined by what you have selected in the tree view.

The third item in the left tree view of the Administration program, labeled Servers, is for configuring the various server specific configuration items for MailEnable.

Many of the tree view items have configuration options. These options can be accessed by right clicking on the icon and selecting the Properties item from the popup menu.

4.2 Messaging Manager

4.2.1 Messaging Manager Overview
This section describes the configuration of the Messaging Manager. The Messaging Manager configures global settings for MailEnable. To access these settings, right click on the Messaging Manager icon and select the Properties item from the popup menu, or click the Configuration icon in the right hand panel.

4.2.2 Messaging Manager - General settings

General Settings for MailEnable’s configuration can be found under the properties of the Messaging Manager. The paths that MailEnable uses to store its configuration data can be configured here.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>New mailboxes have size limit</td>
<td>Configures the default quota for mailboxes, so every new mailbox created will have a quota configured. This can be enable/disabled in the mailbox settings.</td>
</tr>
<tr>
<td>Automatically create an email address for each domain with every new mailbox created.</td>
<td>If there are several domains in a post office and this setting is selected, then every time a mailbox is created in a post office a mail address or address mapping will be created for each domain for the mailbox.</td>
</tr>
<tr>
<td>Directory paths from the MailEnable system</td>
<td>Use these settings when clustering MailEnable and multiple servers are sharing the same configuration repository. This allows configuration of a clustered server array, or to change the location of the MailEnable configuration and storage repositories.</td>
</tr>
</tbody>
</table>

4.2.3 Security and authentication settings

The security tab contains the server settings for password encryption and Windows authentication integration as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Details/Encrypt Passwords</td>
<td>When using Tab Delimited Configuration Providers, which is the default storage within MailEnable, MailEnable passwords are stored in text files with a TAB extension under the config directory of the MailEnable directory structure. You can optionally specify to encrypt MailEnable passwords. If you are using integrated authentication, Windows</td>
</tr>
</tbody>
</table>
Professional Guide

| Enable Integrated Authentication | This is a system wide setting that allows you to simply enable or disable authentication for all hosted MailEnable post offices.

MailEnable Integrated Authentication allows you to use Windows Authentication as well as MailEnable’s inbuilt authentication. It also allows you to have mailboxes created within MailEnable as users successfully authenticate using Windows Credentials. To enable integrated authentication, you must select Messaging Manager Properties (right click on Messaging Manager) and check the box labeled “Enable Integrated Authentication”.

4.3 Post office configuration

For a description of post offices, refer to the Administration section (Section 2.3) in the Overview.

To add a new post office:

1. Select the Messaging Manager branch in the left tree view window of the MailEnable Administration program.
2. In right window, an icon labeled Create Post office will be shown.
3. Click this icon to create a post office and enter a post office name.
4. A password for the postmaster mailbox that will be created for the post office will need to be specified.
5. A new post office will be created.

**Note**: It is also possible to right click the post offices branch and select New > Post office to create a new post office. Functions that are represented by an icon are mostly available through right-clicking items in the left hand panel.

Post office configuration can be accessed using the Administration Console by selecting Messaging Manager > Post Offices > Post Office Name Properties (as shown below).

4.3.1 Post office configuration Overview

For a description of post offices, refer to the Administration section (Section 2.3) in the Overview.

To add a new post office:
1. Select the **Messaging Manager** branch in the left tree view window of the MailEnable Administration program.

2. In right window, an icon labeled **Create Post office** will be shown.

3. Click this icon to create a post office and enter a post office name.

4. A password for the postmaster mailbox that will be created for the post office will need to be specified.

5. A new post office will be created.

**Note:** It is also possible to right click the post offices branch and select **New > Post office** to create a new post office. Functions that are represented by an icon are mostly available through right-clicking items in the left hand panel.

Post office configuration can be accessed using the Administration Console by selecting **Messaging Manager > Post Offices > Post Office Name Properties** (as shown below).

![MailEnable Properties](image)

### 4.3.2 Authentication settings

Once Integrated Windows Authentication has been enabled globally as per the **Security and authentication settings section** (Section 4.2.3), each post office can then be configured with specific authentication settings.

The General tab dialog configures the Microsoft Windows domain that post office mailboxes can authenticate against. The name of the mailbox must match the corresponding Windows account name. For example, a mailbox named Administrator will be able to authenticate using the Windows Administrator password.

In simple implementations there is likely to be only one domain, or the authentication will be done against the local machine. More complicated implementations will allow authentication against specific domains (i.e.: if the organization is made up of multiple domains).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Integrated Windows Authentication</td>
<td>Defines whether the post office can use Windows Authentication.</td>
</tr>
<tr>
<td>Use Post Office Name as Windows Domain Name</td>
<td>Select this option if the name of the post office matches the desired Windows Domain Name.</td>
</tr>
<tr>
<td>Map this Post Office to the</td>
<td>Defines the Windows Domain Name that the will be used for authenticating</td>
</tr>
</tbody>
</table>
4.3.3 Restrictions

Restrict the usage of particular messaging services e.g. restrict the number of messages sent per hour. Setting a value for a post office here overrides any settings that have been created for individual mailboxes.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Maximum SMTP recipients</td>
<td>Throttles any mailbox from sending more than a configured number of emails per hour. This setting is useful for hindering spammers from sending and using the server as a source for spamming.</td>
</tr>
<tr>
<td>Same Domain Restriction</td>
<td>Under the Restrictions tab for a mailbox the checkbox “Users can only send to their local domain” prevents users of that mailbox from sending to any recipient that does not have the same domain name as they are sending from. This can also be configured at the mailbox level.</td>
</tr>
</tbody>
</table>

4.3.4 Web admin

Configures feature availability for web administration users for each post office. Further information on web administration can be found in the Web administration section (‘Overview’ in the on-line documentation).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable web administration for Post Office</td>
<td>Enables web administration for the current post office.</td>
</tr>
<tr>
<td>Can create and edit mailboxes</td>
<td>Allows mailboxes to be created and edited in web administration.</td>
</tr>
<tr>
<td>Maximum no. of mailboxes</td>
<td>Specify the maximum number of mailboxes that can be created for this post office.</td>
</tr>
<tr>
<td>Maximum and default mailbox size</td>
<td>Enforces a mailbox size for each newly created mailbox in web administration. This setting can be disabled or changed for each mailbox in the mailbox properties – see the Create mailbox - General section (Section 4.4.3.2).</td>
</tr>
<tr>
<td>Can select mailbox size (up to the default value)</td>
<td>Grants the web administrator the ability to create a quota for the post office mailboxes up to the configured default size.</td>
</tr>
<tr>
<td>Can create and edit lists</td>
<td>Grants the web administrator the ability to create lists in web administration.</td>
</tr>
<tr>
<td>Maximum number of lists</td>
<td>Sets the maximum number of lists a web administrator can create.</td>
</tr>
<tr>
<td>Maximum number of addresses in each list.</td>
<td>Limits the number of addresses a web administrator can add to a created list.</td>
</tr>
<tr>
<td>Can add, edit and remove domains</td>
<td>Allows the user the ability to add and remove domains in the web administration page.</td>
</tr>
<tr>
<td>Can brand web mail and web administration</td>
<td>Allows the user to brand webmail and web administration by changing the login logo and the banner logo.</td>
</tr>
</tbody>
</table>
4.4 Post office actions

4.4.1 Post office actions Overview

In the MailEnable Administration program, expand the post offices branch to display all the available post offices. Selecting the post office will display the available actions (as seen in the diagram below).

![MailEnable Post Office Actions]

4.4.2 Create domain

Domains are placed under the post office that owns them. Use the MailEnable Administration program to manage the domains that are serviced by a post office (or customer). A domain is needed in order to create email addresses and allow users to send emails. To add a domain, from the right hand side window of the MailEnable Administration program select the Create Domain icon.

General

After selecting the Create Domain icon, the following window will appear:
Here, enter the full domain name to receive emails for. For instance, to receive emails such as sales@mailenable.com or info@mailenable.com, enter the domain mailenable.com here. The domain will now appear under the **Domains** branch of the MailEnable Administration program.

Multiple domains can be assigned to a post office. However, at least one domain needs to be configured in order to have a valid email address.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain is disabled</td>
<td>Stops email being sent to the domain.</td>
</tr>
<tr>
<td>Abuse Address</td>
<td>Enter the email address or select the mailbox for the abuse@domain email address.</td>
</tr>
<tr>
<td>Postmaster Address</td>
<td>Enter the email address or select the mailbox for the postmaster@domain email address. This is a mandatory setting.</td>
</tr>
<tr>
<td>Catchall Address</td>
<td>A catchall address will collect all emails for a domain that do not have a mapping to a mailbox. Either select an existing mailbox, or enter another email address to act as the catchall. Implementing a catchall will capture more spam, so make sure this mailbox is monitored. Warning: It is advisable not to enter a remote email address or a local mailbox which is being redirected to a remote address as a catchall. Doing this will cause the server to on-send all the caught spam and is likely to result in blacklisting by the remote server and possibly putting the server on a global blacklist. When an inbound connection via SMTP is made and there are multiple recipients to addresses that are destined for a catchall mailbox, only one message is delivered to prevent multiple copies of the same email being delivered. Messages that are delivered to a catchall will have the recipient list in the Received header, or on the alternate catchall header line, if this is enabled.</td>
</tr>
<tr>
<td>Act as Smart Host</td>
<td>Redirects all mail for the current domain to another mail server. This would be used if, for instance, the server was acting as a backup mail server for the domain. Specify a port number by adding a colon and port number after the IP address. e.g. 192.168.3.45:30. Do not enter the IP address of your MailEnable server, as it will create a message loop (the mail server will send to itself) and messages will finally end up in the Bad Mail directory. See the <strong>Smart host section</strong> (Section 5.1.9) for more information on smart hosting. Use the ‘Only relay email from authenticated users’ option in order only to relay email from</td>
</tr>
</tbody>
</table>
Blacklist

Add blacklisted domains for the selected domain. Blacklisted domains are unable to send mail to this domain. The Domain properties blacklist checks the envelope sender of the email, which may be different to the email contents.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains</td>
<td>Remote hosts can be denied access to the system by adding them to the blacklist for a domain. This effectively denies a server the ability to send to the domain if the domain in a sender's email address matches an item in the blacklist. For example, if you add the domain “mailenable.com” to the blacklist for a domain, then the domain will not accept any emails from mailenable.com.</td>
</tr>
</tbody>
</table>

4.4.3 Create Mailbox

4.4.3.1 Create mailbox Overview

For a description of mailboxes, please see the Administration section (Section 2.3) in the Overview.

When creating a mailbox, MailEnable will automatically create an email address for each domain in the post office (if the setting for automatically creating email addresses for each domain is enabled in the Messaging Manager Properties - see the General settings section (Section 4.2.2)) using the format mailboxname@domain. When a mail client application logs onto MailEnable to retrieve email, it needs to have its username formatted as mailboxname@postofficename.

To create a mailbox, select the post office branch. Select Create Mailbox from the icons displayed.

4.4.3.2 Create mailbox - General

The General tab of mailbox properties displays as below:
### Setting | Description
--- | ---
**Mailbox Name** | This is the name of the mailbox. Once created, this cannot be changed. This both identifies the user and ensures there is no duplication of mailbox names. As the Mailbox Name is entered into the text box, the POP Logon name entry just below it will change to reflect the entry.

**POP Username for mail clients** | This is the username used for logging onto the server via POP3. Use this information to set up the client mail software. The POP Logon name is the same as the “User Name” that is used by mail clients when they connect to the server to retrieve email. MailEnable uses the @ symbol to identify the post office the mailbox belongs to. This way, the same mailbox names can exist in different post offices (although the username to retrieve their email will differ, since the username is formatted as mailboxname@postofficename).

**Password** | The password for the mailbox. The client software uses this when connecting. If SMTP authentication is turned on, this password is also used for sending email. Other extensions to the MailEnable product may also use this username/password combination. The password that is set is the same as the password used by mail clients to authenticate when they connect to the server to retrieve email.

**Select random password** | Creates a random 8 character alphanumeric password.

**Mailbox Type** | Determines the access level for the mailbox. If the mailbox is given “ADMIN” rights, then the user will be able to administer this post office in MailEnable via the web administration interface. If the user is given “SYSADMIN” rights, then they will be able to modify any post office settings.

**Mailbox has a size limit** | Limits the size of the mailbox. If an email will take the size of the inbox over this limit, the email is bounced back to the sender.

**Prevent user from authenticating** | If enabled, this will prevent a user from authenticating or logging into any service where the credentials for the mailbox are supplied.

**Logon Disabled** | When a mailbox is disabled, it cannot be accessed via a service, such as POP3 or web mail. Useful for suspending account, it makes the mailbox or email mappings to the mailbox inactive, without deleting it.

**Delete messages** | Delete messages from the mailbox.

### 4.4.3.3 Addresses

When creating a mailbox, email addresses are created for all the domains available in the post office. For instance, for the domain mailenable.com, if a mailbox called ‘sales’ was created, the email address sales@mailenable.com would be automatically created.

To create new email addresses, selecting the **Addresses** tab at the top of the mailbox properties window. A list of the current email addresses will be shown.
In order to add another email address for this mailbox, click the **Add Email** button. The first text box, **Enter email name** is where the first part of the email address is entered. E.g. to add sales@mailenable.com, only requires the word sales to be entered. The full address of the email being added is displayed in the window.

The **Available Domains** list box in this window lists domains that are entered via the **Create Domain** icon. MailEnable can only add email addresses for the available domains in each **post office** account. For the purpose of this guide we have entered only one domain. In cases where there is more than one domain in a client’s post office account, these domains will appear in this list box. It is then possible to select the appropriate and then entering the email name that is required. Select **OK** on the **Add Emails** window when the address has been entered. It will now appear in the mappings list.

Select **OK** on the **Mailbox Properties** window as your mailbox has now been configured.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly Name</td>
<td>The Friendly Name is used as the display name for emails sent via web mail and for the sender for auto-responder messages. When sending messages from email clients, the friendly name is configured within the client application, not on the server.</td>
</tr>
<tr>
<td>Reply To Address</td>
<td>This address is used as the reply to address for auto responders.</td>
</tr>
<tr>
<td>Email Addresses for Mailbox</td>
<td>Each mailbox can have one or more email address mapped to it. Use the Add Email... button to add new email addresses. It is only possible to add an email that matches an existing domain for the post office. When first creating a mailbox, MailEnable will automatically create email addresses for each of the domains for the post office.</td>
</tr>
</tbody>
</table>

**4.4.3.4 Redirection**

The redirection tab sets redirections for a specific mailbox to be forwarded to one or more email addresses.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect this mailbox to</td>
<td>Redirect all email for the mailbox to an alternative email address or addresses. To enable redirection, select the ‘Redirect this mailbox to’ checkbox. Select the Add button to add email addresses. If more than one email address is listed, the email will be copied to all of the addresses listed. There is a limit of approximately 25 email addresses that can be redirected</td>
</tr>
</tbody>
</table>
The actions tab allows for the configuration of auto responders and delivery events.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto responder</td>
<td>Enabling this will send a message back to anyone who sends an email to the mailbox. The auto responder will not reply to a message marked as bulk. It is not possible to enable auto responders for the postmaster mailbox.</td>
</tr>
<tr>
<td>Enable delivery event</td>
<td>Allows a program to be executed on every message when it is delivered to a mailbox. The command line executed is: program messagefilename connectortype Where program is the program filename, messagefilename is the name of the message file and connectortype is the type of messages (i.e. SMTP, LS, SF). Be aware that the directory path to the message is not passed to the program. The program will need to read the directory path from the Windows registry. The path to the message for the delivery event can be built from values retrieved from the Windows registry. The following registry key returns the root path of the messages queues for a server: HKLM\SOFTWARE\Mail Enable\Mail Enable\Connectors\Connector Root Directory To get the full path to the postoffice connector queue, which is holding the message for the delivery event, append the text &quot;\SF\Outgoing\Messages&quot; to the value retrieved. The parent of this folder has the command file for the message if required. Be aware that the path to the message file is different for the MTA pickup event, so scripts or external programs would have to be modified accordingly. The delivery event will not execute for any messages marked as bulk. Bulk messages are mostly system generated messages such as delivery failures, delivery reports, and autoresponder replies. Messages from list servers may also not execute the delivery event.</td>
</tr>
</tbody>
</table>

4.4.3.6 Messages

The messages tab will list up to 200 messages in the currently selected mailbox and optionally allow all email to be forwarded to another mail account.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages</td>
<td>Lists the messages in the current mailbox. Select an item to view the contents of a message. Only the most recent 200 messages are displayed.</td>
</tr>
<tr>
<td>Forward all email</td>
<td>Forward all email from this local mailbox to another mail account. It is possible to specify what account to have the messages forwarded from. This will forward the mail in the same way a mail client would. All mail will remain in the mailbox unless the option to delete mail is selected.</td>
</tr>
</tbody>
</table>

4.4.3.7 POP Retrieval

View remote or local mailboxes that have been configured for POP retrieval by the currently selected mailbox. The administrator can add and configure POP Retrieval from here, or a user may do so via the web mail interface, if permission to do so has been granted. If the feature is disabled in the Administration program only the administrator or accounts with access to Administration program can create a POP Retrieval account. See the Web mail server configuration section (‘Web mail server configuration’ in the
on-line documentation) for more information on this setting.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current POP retrieval items</td>
<td>Displays any remote or local mailboxes that have been configured to have their mail pulled down into this local mailbox.</td>
</tr>
<tr>
<td>Add Mailbox</td>
<td>The POP Retrieval service can connect to another mailbox and pull any mail in the mailbox into this local mailbox. This is useful to centralize mail receipt over many accounts and across many domains.</td>
</tr>
<tr>
<td></td>
<td>To set up an account the following details are required;</td>
</tr>
<tr>
<td>Mail Server</td>
<td>This is the MX record or DNS name of the remote server e.g.. mail.mailenable.com</td>
</tr>
<tr>
<td>Port</td>
<td>This is the port that is used to connect to the remote server. The default for this is port 110</td>
</tr>
<tr>
<td>Username</td>
<td>This is the username of the account. If it is a MailEnable mailbox this must be mailbox@postofficename</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the account.</td>
</tr>
<tr>
<td>This server requires APOP authentication</td>
<td>APOP (Authenticated POP) is an extension of the standard POP3 protocol. Authenticating to a POP server will mean the username and password are both encrypted by the client before being passed &quot;over the Internet&quot;. The receiving server must then be able to decrypt the password.</td>
</tr>
<tr>
<td>Only download new messages</td>
<td>(leave messages on server) - Will download messages leaving a copy on the server.</td>
</tr>
<tr>
<td>Enabled</td>
<td>This setting allows the enabling or disabling of a POP retrieval service account. Disabling the account will retain the settings but will stop the account retrieving mail.</td>
</tr>
</tbody>
</table>

4.4.4 Export users

A user list can be exported in CSV (comma-separated value) format, with selected fields. To export users;

1. Find the post office where the user details are to be exported.
2. Right click the post office name, select All Tasks and then select Export Users.
3. From the list, select the fields to export to the file.
4. Enter the filename to save as and select Export.

4.4.5 Import Windows users

Windows users can be imported into a MailEnable post office. This will create a mailbox for each Windows user. To import users;

1. Select the post office to import the users to
2. Select either the icon for Import users, or right click the post office name, select All Tasks and then select Import Windows Users
3. Select the Windows users to import
4. Select whether to give them a specific quota, or allow them to have an unlimited amount of space
5. The password for all selected users can be set to the same, or MailEnable can generate random passwords for users. If generating random passwords, it is possible to export a list of all the users and the passwords assigned
6. By default, users are given an email address corresponding to a domain for the post office being imported into. Select the domain to assign email addresses for. Mailboxes are automatically enabled when created.
4.4.6 Import users

This feature allows you to import users to the local post office. A comma delimited file that is formatted as `emailaddress,password,quota` must be used. Password and quota is optional. If not provided then default settings are used and domains will be created if necessary.

If quota limits are not specified in the file, these can be set to a certain limit, or unlimited.

If password settings are not specified in the file, a random password may be generated or a set password can be created for all imported users.

4.4.7 Email users (all)

An administrator is able to e-mail all the users at a post office by selecting/clicking on the post office name under Messaging Manager > Post Offices.

Then administrator then clicks on the Email users icon to send an email to all users of a particular domain.

4.4.8 Email users (individual)

An administrator can e-mail a user/mailbox owner from within the Messaging Manager by right clicking on the mailbox and selecting Send email.

4.4.9 Delete messages

Messages can be deleted from MailEnable either globally, or by post office, or mailbox. It is possible to specify how many days old the messages have to be, whether to delete all messages before a certain date, or to delete all messages.

4.4.10 Set quotas

Selecting this option will reset all mailbox quotas for the post office to the specified value. This will only affect the current mailboxes, not any future ones that will be added.

4.4.11 Edit default message

This edits the default message (which has the filename default.mai) that is created in a mailbox when the mailbox is created. For more detailed information on this selection, please see: http://www.mailenable.com/kb/Content/Article.asp?ID=me020027

4.4.12 Create a group

For a description of groups, please see the Administration section (Section 2.3) in the Overview.

When creating a group, the group name is the full text description of the group (for ease of identification).

The recipient address is the email address of the group and within this group there can contain multiple external groups. Groups can contain external addresses, so the one group can have different email addresses that are not hosted on the server.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Create a name for the group e.g. <a href="mailto:staff@example.com">staff@example.com</a></td>
</tr>
<tr>
<td>Group is disabled</td>
<td>Stops the group from working so that if someone emails the group address, the email will bounce back indicating that the address is not valid</td>
</tr>
<tr>
<td>Add email</td>
<td>Add other email addresses for the group e.g. <a href="mailto:allstaff@example.com">allstaff@example.com</a></td>
</tr>
</tbody>
</table>

To add a new group member to a group, right click the group, and select New > Group member. Type the email address in the box provided or select “Advanced” which will list all users in the post office.

**Note:** Be cautious of using the “Advanced” option if you have a large number of users in the post office.
To import users into a group from a text file, right click on the group icon in the tree view display and select the All Tasks > Import Members menu item.

4.5 Lists

4.5.1 Lists Overview

For a description of lists, please see the Administration section (Section 2.3) in the Overview.

When a user wishes to subscribe to a list, they need to send an email to the list with the word “subscribe” in the subject. When the user wishes to be removed from the list, they need to send an email with the word “unsubscribe” in the subject.

To create a new list:

1. Under the Messaging Manager select the post office to create a list for
2. Right click the Lists folder and select New > List. This will load the List Properties window (see below) to configure a new list.

![List Properties Window]

4.5.2 Lists - General

The general options associated with a list are outlined in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List name</td>
<td>The name of the list. This determines the address that people email to in order to post to the list. The full email address for the list appears at the bottom of the General property page.</td>
</tr>
<tr>
<td>Select domain for this list</td>
<td>The domain used for the list name.</td>
</tr>
<tr>
<td>List owner email (also moderator)</td>
<td>The email address of the moderator. When a list is moderated, all the emails that are posted are sent to the moderator. It is the job of the moderator to decide whether or not the email is to be posted. Only emails coming from the moderators email address will be posted to the list.</td>
</tr>
</tbody>
</table>
MailEnable also provides advanced list configuration options. These options can control who can post to lists, where list replies should be directed, who can subscribe to lists and the format of any subject prefix that is applied to posts.

### Subscription type
MailEnable can control how subscriptions are handled.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone can subscribe to this list via email</td>
<td>Allows people to subscribe to the list by sending the word “subscribe” as the subject of an email to the list.</td>
</tr>
<tr>
<td>E-mail subscriptions are not permitted for this list</td>
<td>Stops people from subscribing to the list. List members can only be added through the administration program.</td>
</tr>
<tr>
<td>E-mail subscriptions need to be confirmed</td>
<td>Enforces a subscription confirmation code to be returned to the list for successful subscription. When this option is enabled a subscription code will be sent out after a message has been sent to list with “SUBSCRIBE” in the subject field of the message. The user then needs to reply to list using the confirmation code that was sent out to him/her to successfully subscribe to the list.</td>
</tr>
</tbody>
</table>

### Posting permissions
MailEnable can control who can post to a list.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone can post to this list</td>
<td>Anyone is allowed to send a message to the list.</td>
</tr>
<tr>
<td>Only subscribers can post to this list</td>
<td>The list will only accept posts from email addresses that exist in the list.</td>
</tr>
</tbody>
</table>
| Posting to this list requires a password | Password protects the list. To send an email to a password protected list, users need to enclose the password in square brackets and colons e.g. [: and :]

### Reply options
These options determine who should receive responses when a recipient replies to a post.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribers reply to the</td>
<td>The reply to address is set to the list address, so when users reply to a message</td>
</tr>
</tbody>
</table>
List subject prefix

Some lists place a prefix in the subject of the list messages. This allows subscribers to filter the messages that are dispatched to them via the list server. These options can control the prefix that is appended to the subject of messages that are dispatched to list subscribers.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject is prefixed with the name of the list</td>
<td>The list name, enclosed in square brackets ([ and ]) is added to the start of the subject line of emails posted to the list.</td>
</tr>
<tr>
<td>Subject is not altered</td>
<td>Subject is not altered for any messages posted to the list.</td>
</tr>
<tr>
<td>Subject should have the following prefix</td>
<td>Specified text is added to the start of the subject line for all emails posted to the list.</td>
</tr>
</tbody>
</table>

4.5.4 Headers

Specify plain text or HTML headers for all list messages.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach header</td>
<td>This text is added to the top of every email when the Attach header checkbox is selected.</td>
</tr>
</tbody>
</table>

4.5.5 Footers

Specify plain text or HTML footers for all list messages.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach footer</td>
<td>This text is added to the bottom of every email when the Attach footer checkbox is selected.</td>
</tr>
</tbody>
</table>

4.5.6 Importing list members

MailEnable can import users from a text file to a list. To do this;

1. Under the Messaging Manager select the post office to import the list members into
2. Right click on the list icon in the tree view display and select the All Tasks > Import Members menu item
3. Select the file to import. The file should be in the format of emailaddress,displayname

4.5.7 List commands

Users send commands to the list by putting the command in the subject line. The available commands for the list server are:

- **Help** - sends an email back with the available commands of the list server
4.5.8 Messages

The Messages tab for a list allows the use of a custom message for the subscribe notification and the unsubscribe notification. The files that can be used for this need to be located in the following path:
Mail Enable\Config\Post Offices\[Post Office]\Annotations

The unsubscribe error message filename has to be prefixed with “ERROR-“ if this is to be custom as well.

The custom notification files recognize the following tags that can be replaced:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ME_MEMBER_EMAIL]</td>
<td>The member email address</td>
</tr>
<tr>
<td>[ME_POSTOFFICE]</td>
<td>The post office of the list</td>
</tr>
<tr>
<td>[ME_LIST]</td>
<td>The list name</td>
</tr>
<tr>
<td>[ME_LISTADDRESS]</td>
<td>The email address of the list</td>
</tr>
<tr>
<td>[ME_FROMADDRESS]</td>
<td>The moderator email address</td>
</tr>
<tr>
<td>[ME_TOADDRESS]</td>
<td>The list address</td>
</tr>
<tr>
<td>[ME_MESSAGEID]</td>
<td>The message ID formatted as <a href="mailto:filename@localdomain">filename@localdomain</a></td>
</tr>
<tr>
<td>[ME_DATE]</td>
<td>The current date/time</td>
</tr>
</tbody>
</table>

4.6 Server configuration

General Server Configuration Options are located under the properties of the Server name “localhost” to manage the local server. These settings are specific to the server that is selected.

The General tab specifies a default post office for the server and shows post office bindings to IP addresses.
4.6.1 General configuration

General Server Configuration Options are located under the properties of the Server name “localhost” to manage the local server. These settings are specific to the server that is selected.

The General tab specifies a default post office for the server and shows post office bindings to IP addresses.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Default Post Office</td>
<td>Specify the default post office for your server. This means that any username that only has the mailbox name will be assumed to be from the default post office. E.g. the <a href="mailto:sales@example.com">sales@example.com</a> user will only need to use sales to log on with.</td>
</tr>
<tr>
<td>Enable post office bindings</td>
<td>It is possible to bind each MailEnable post office to a particular IP address on the network card. This means that all post offices will only need to use the username to log-in (not just the default post office). This will also allow the welcome message when a connection is made to the server return a value that is specific for each post office.</td>
</tr>
</tbody>
</table>

4.7 Option Files

Several options for post offices and mailboxes are held in option files in the MailEnable\Config directory and
subdirectories. These option files have the .sys filename extension and are plain text files which can be edited in Notepad. Each user, post office, and server has its own file that contains relevant options. Most of these are configurable through the MailEnable administration program, so the files do not usually need to be edited.

It is possible to create default configurations for mailboxes and post offices in MailEnable by editing the base sys files that are used when a new mailbox or post office is created.

Whenever a new post office is created through the MailEnable administration program, it copies the configuration items from the Mail Enable\Config\Postoffices\Postoffice.SYS and Mail Enable\Config\Postoffices\Mailbox.sys files. When a new mailbox is created through the administration program, it copies its settings from this post office copy (which resides in Mail Enable\Config\Postoffices\[postoffice]\Mailbox.sys. This way, it is possible to create the web administration program and the base functions that developers may use. Do not copy these configuration files; it is up to the developer to copy or set the defaults if they wish.

4.8 Advertising and Campaign Management

MailEnable's webmail client allows administrators to enable advertising for their webmail customers. The advertising feature allows banner adds to be presented either server wide, or at a postoffice level.

System Administrators are able to logically group advertising material into Campaigns. They can control the frequency of banner rotations and the designated click through URL.

System Administrators and Postoffice Administrators can then select which campaigns they would like to distribute to users.
Configuration of connectors, services and agents

5.1 SMTP Connector

5.1.1 SMTP Connector Overview

SMTP is a protocol for transferring outgoing email messages from one server to another and also to accept email messages from other mail servers and email clients. SMTP is used with both POP3 and IMAP4.

Note: POP and SMTP servers are often the same server. However, in some cases, one server is used for receiving mail (POP server) and another server is used for sending mail (SMTP server); this is done mostly for load balancing and redundancy.

Using the Administration Console, the SMTP properties can be accessed by expanding the Servers > Localhost > Connectors branch.

Right click on the SMTP icon and select Properties. The options are explained below:

5.1.2 SMTP properties

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Domain Name</td>
<td>The domain name of the server that MailEnable is installed on, or the default domain for the configuration. It is used for system messages, to announce the server when it connects to remote server, and when remote servers connect to MailEnable if the host name has not been specified.</td>
</tr>
<tr>
<td>Default mail domain name</td>
<td>The default mail domain name for the server, which usually matches the default MX record. For example, if you have configured mail.example.com in your DNS to point to your mail server, then you would enter this here. If a host name has been specified for an IP address on the server, then that value will override this host name.</td>
</tr>
</tbody>
</table>
DNS Address

The DNS that the local machine uses. If using more than one DNS, separate the addresses with a space character. If the SMTP service fails to connect to the first DNS, it will try the second or subsequent DNS. Use the DNS that is configured for the local network. Remember that this is not necessarily the DNS of where the domain name is registered.

Specify the email address when sending notifications

The address from which notifications are sent. When MailEnable sends out email such as message delivery delays, or delivery failures, it will use this address as the “from” email address. Usually this would be postmaster@example.com (substitute your domain here). Make sure this is a valid email address.

Enable NTLM Authentication

If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled to use this secure authentication. For example, in Outlook the feature is called SPA - Secure Password Authentication. More information on NTLM can be found in the Overview of NTLM Authentication section (Section 11.2).

Enable CRAM MD5 Authentication

CRAM-MD5 Challenge-Response Authentication Mechanism is intended to provide an authentication extension that neither transfers passwords in clear text nor requires significant security infrastructure in order to function. Only a hash value of the shared password is ever sent over the network, thus precluding plaintext transmission.

Enable TLS

The Transport Layer Security (TLS) protocol allow clients to connect to the SMTP service over the standard port and then negotiate for a secure transaction. TLS is only available on inbound connections. The SMTP connector will use the SSL certificate that has been configured for the server.

## 5.1.3 Inbound

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP service listens on port</td>
<td>Determines the port the SMTP service is running on. The default is 25. Inbound SMTP connections from remote servers expect the mail server to be listening on port 25, but some proxy or gateway software may require this to be changed.</td>
</tr>
<tr>
<td>SMTP Enable SSL (Default Port)</td>
<td>Enables SSL certificate encryption for the default port that SMTP is running on. Place a tick in this box to enable. The service also has to be enabled at a server level in the MailEnable Administration Program &gt; Server &gt; Localhost Properties &gt; SSL tab.</td>
</tr>
<tr>
<td>Also listen on alternate port</td>
<td>The SMTP service can also listen on an alternate port by enabling this option. Usually this is done to cater for clients who may be on connections where their outgoing port 25 has been blocked.</td>
</tr>
<tr>
<td>SMTP Enable SSL (Alternate Port)</td>
<td>Enables SSL certificate encryption for the alternate port that SMTP is running on. The default port for this is 465. When enabling SSL make sure that a valid SSL certificate has been selected in the MailEnable Administration &gt; Server &gt; Localhost Properties &gt; SSL tab.</td>
</tr>
<tr>
<td>Maximum number of concurrent connections</td>
<td>The number of connections that will be available for remote servers and email clients to connect to.</td>
</tr>
<tr>
<td>Advertised Maximum message size</td>
<td>Entering a value here will inform remote mail servers and email clients of the maximum size of an email that should be sent to the server. The size is represented in bytes. Clients or remote mail servers may ignore the value. A size of 0 means that there is no limit on message size.</td>
</tr>
<tr>
<td>Enforce this message size</td>
<td>Checks each inbound message size after it is received. If it is over the limit, it will be deleted and an error returned to the remote server or email client that is trying to send.</td>
</tr>
</tbody>
</table>
Mail servers accept messages for recipients that have their mailboxes hosted on the mail server itself. Any attempt to send a message to a non-local recipient (i.e. a recipient on a different mail server) is called a ‘relay’. It is critical to regulate who can send messages to others (non-local recipients) or the server will be identified as an Open Relay. This means that people on the Internet can send email out through the server without authenticating. Secure the server by configuring strict rules as to who can relay messages to non-local recipients.

For a server on the Internet, the best relay setting to have is to only have Allow relay for authenticated senders checked, and leave Allow relay for local sender addresses unchecked. This will make everyone who wants to send email out via the server provide a username and password.

To access the SMTP Relay options, open the Administration program, expand the Servers > Localhost > Connectors branch, right click on the SMTP icon, select Properties from the popup menu, and click the Relay tab.

The following table provides an explanation of the various relay settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Specify who can connect to the email server. Specify a list of IP addresses that are either banned from connecting, or are the only ones allowed to connect. Use the * character as a wildcard.</td>
</tr>
<tr>
<td>Inbound IP Bindings</td>
<td>Select the IP addresses that the SMTP service will be bound to. On a multi-homed machine it may desirable to only listen to connections on particular IP addresses. ‘Always bind the service to all available IP addresses’ will allow connections on all IP addresses that are configured for the machine.</td>
</tr>
</tbody>
</table>

### 5.1.4 Outbound

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of send threads</td>
<td>The number of threads that are used to send email.</td>
</tr>
<tr>
<td>Timeout for Remote Mail Servers</td>
<td>How long the SMTP service will wait for a response from a remote mail server before disconnecting.</td>
</tr>
<tr>
<td>Outgoing queue poll interval</td>
<td>How often the SMTP service polls the outgoing queue directory for mail messages to send. This is measured in seconds.</td>
</tr>
<tr>
<td>Limit outbound message size</td>
<td>Forces MailEnable to check the size of each message before delivering to a remote mail server. If the message cannot be delivered it will be returned to the sender (or sent to the bad mail directory if the message is system generated).</td>
</tr>
<tr>
<td>Outbound IP Binding</td>
<td>Forces the SMTP to use a specific IP address on the server when it is trying to deliver email.</td>
</tr>
</tbody>
</table>

### 5.1.5 Relay

Mail servers accept messages for recipients that have their mailboxes hosted on the mail server itself. Any attempt to send a message to a non-local recipient (i.e. a recipient on a different mail server) is called a ‘relay’. It is critical to regulate who can send messages to others (non-local recipients) or the server will be identified as an Open Relay. This means that people on the Internet can send email out through the server without authenticating. Secure the server by configuring strict rules as to who can relay messages to non-local recipients.

For a server on the Internet, the best relay setting to have is to only have Allow relay for authenticated senders checked, and leave Allow relay for local sender addresses unchecked. This will make everyone who wants to send email out via the server provide a username and password.

To access the SMTP Relay options, open the Administration program, expand the Servers > Localhost > Connectors branch, right click on the SMTP icon, select Properties from the popup menu, and click the Relay tab.

The following table provides an explanation of the various relay settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Mail Relay</td>
<td>Mail relaying needs to be enabled in order to send mail. Otherwise MailEnable will only be able to receive email. There are four options available to limit who can send mail out through the server. It is possible to select any combination of the four, however, a client only has to match one of the items in order to relay through the mail server.</td>
</tr>
<tr>
<td>Allow relay for authenticated senders</td>
<td>Requires that people sending mail through the server enter a username and password (i.e. this option enables SMTP authentication). To set this is different for various mail clients, but in Microsoft Outlook Express and Microsoft Outlook for instance, this is done in account properties via the &quot;My server requires authentication&quot; checkbox under the</td>
</tr>
</tbody>
</table>
“Servers” tab. It is advisable to have this option enabled if the server is not using privileged IP ranges. Also, ensure that Secure Password Authentication (SPA) is not enabled.

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MailEnable/integrated authentication</td>
<td>uses the MailEnable username/password</td>
</tr>
<tr>
<td>Windows authentication</td>
<td>uses the Windows username/password valid for that machine</td>
</tr>
<tr>
<td>Authenticate against the following username/password</td>
<td>specify your own username and password</td>
</tr>
</tbody>
</table>

| Allow relay for privileged IP ranges | Allows people with certain IP addresses to send email through the server. If the IP addresses of persons who are able to send email out through the server is known, use this option. DO NOT select this option if the list of IP addresses is unknown, as this may inadvertently allow everyone access. This option is usually required to allow sending through the server from a web server or web page. |

| Allow relay for local sender addresses | Allows people to send mail if their ‘From’ address has a domain that is hosted on MailEnable. For instance, if you host example.com, and someone sends a message from your server that has their ‘From’ address as peter@example.com, the email will be sent. Unfortunately, spammers may still abuse this by spoofing ‘from’ addresses, so most servers will not use this option. Using this option may cause some anti-spam blacklists to consider the server as “open relay” and block email from the server. |

| POP before SMTP authentication | The IP address of users who authenticate via POP is remembered and permitted to relay. The time period to remember the IP address for can be set. Some client applications will try to send email before retrieving (e.g.: Microsoft Outlook), so they will generate an error message on the first send try. Subsequent send attempts will then work if they are before the specified time. This is required due to some ISPs and certain routers not allowing SMTP authentication. This feature will bypass this issue by authenticating a client using POP. If this authenticates then the SMTP service will allow this IP access for a designated period of time. To remember the IP address, a file is written to the Mail Enable\Config\Connections directory. The file name is the IP address and the file extension is .pbs. |

### 5.1.6 SMTP - Security

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject mail if sender address is from an invalid domain</td>
<td>When a user is sending mail to MailEnable, this option will check the From address in order to verify the domain it is coming from. It works through a senders (FROM) address in the envelope or command message for an email having the domain stripped from an email address. This will then have a DNS resolution lookup completed on the domain name MX record to see if it is registered as a mail server. If not then the message will fail with a permanent error. This is used to stop people abusing the mail server by using incorrect information. The majority of people who use an incorrect From address are spammers. This may affect valid email from incorrectly configured clients, so monitor the logs often.</td>
</tr>
<tr>
<td>Authenticated senders must use valid sender address</td>
<td>If this is selected, users who are authenticating to send email must configure their email client with a valid email address that is assigned to the mailbox they are using to send on. This option is useful to force clients to use a legitimate email address, thereby reducing the possibility of spam.</td>
</tr>
<tr>
<td>Prevent sender address</td>
<td>Forces anyone sending through the server with a sender address which is...</td>
</tr>
</tbody>
</table>
spoofing. Senders using a local address as the sender must authenticate to send any email. If using a sender address which does not include the @ symbol (a non-routable address), then the whole address is checked against the local domain list.

Hide IP addresses from email headers
By default, the IP address of a client connecting is displayed in the header of an email message. If the network has its own IP range which is to remain hidden to receivers of emails, this option will replace the IP address with 127.0.0.1.

Require PTR DNS entry for unauthenticated connections
If an inbound connection has not been authenticated, MailEnable will look up to see if there is a PTR DNS entry for the connecting IP address. MailEnable will not validate whether the entry is valid, it will check to see if one exists. Local IP addresses are not checked for PTR entries.

Disable all catchalls
Catchalls for domains will cause the email server to collect a lot more email and can cause the server to relay spam (i.e. if the server redirects a catchall to a remote email address). This option will stop all catchalls from working.

Allow domain literals
MailEnable will allow inbound emails to be formatted as user@[IP Address], such as user@[192.168.3.10]. MailEnable will accept emails for any of the IP address that have been configured on the server. If using NAT, or to accept extra IP addresses which are not configured on the server, select the Advanced button. This will allow these extra IP addresses to be entered.

Use alternate welcome message
When an email client or other mail server connects to MailEnable, a one line welcome message is displayed. By default, this indicates that the server is running MailEnable software, and shows the version of the software. If this option is enabled, it is possible to customize the welcome message. There are also two variables that can be used in the welcome text that will be replaced. These are:

%LOCALDOMAIN% - this will be replaced with the SMTP domain from the SMTP options
%TIME% - this will be replaced with the current time on the server

Restrict the number of recipients per email
It is possible to restrict the number of recipients per incoming email. Allowing a large number of recipients per message may help with sending to contact lists via email clients, but it also raises the benefit to spammers, as they can save on bandwidth and can send through more messages in a shorter amount of time.

Drop a connection when the failed number of commands or recipients reaches
Most email clients will recognize error codes returned by the mail server for an invalid recipient or similar. But some spammers and bulk email utilities may not recognize these errors and keep trying to send. By enabling this option, MailEnable will drop the client connection. It is recommended not to use a low value (5 for example), as some valid web scripts will not check the return codes either - but these will only produce a small number of failed commands.

Add to denied IP addresses if this number is reached
If a connection has reached the disconnection limit, it is possible to automatically add the IP address of the client to the SMTP Access Control list. Be aware that if enabling this option, the Access Control list can grow and adversely affect the performance of the SMTP service. Therefore it is recommended to check the Access Control list regularly.

5.1.7 SMTP - Advanced

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable alternate</td>
<td>When mail is sent to an invalid recipient and they are specified as a BCC on the</td>
</tr>
</tbody>
</table>
Delivery failure notifications can be customized for the SMTP service. Templates can be used for either a post office (if the message which fails can be attributed to a post office) or for the server. The template files for a post office need to be configured in the following folder:

Mail Enable\Config\Postoffices\[postoffice]

If this template file does not exist, then the server level one will be used, which is located at:

Mail Enable\Config\Postoffices

MailEnable provides two template files for non-delivery reports:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP-NDR-FAILEDRECIIPS.TXT</td>
<td>Non-Delivery Message that has a list of failed recipients (ie: one or more recipients were refused by the server)</td>
</tr>
</tbody>
</table>

### 5.1.8 SMTP - Delivery

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Retry</td>
<td>The delay before a message is retried for the first time. The default is 15 minutes.</td>
</tr>
<tr>
<td>Second Retry</td>
<td>The delay before a message is retried for the second time. The default is 30 minutes.</td>
</tr>
<tr>
<td>Third Retry</td>
<td>The delay before a message is retried for the third time. The default is 60 minutes.</td>
</tr>
<tr>
<td>Subsequent retries</td>
<td>The delay before a message is retried for the first time. The default is 240 minutes.</td>
</tr>
<tr>
<td>Failed Message Lifetime</td>
<td>This determines the amount of time a message will stay in the outbound queue before MailEnable gives up and moves the message to the Bad Mail directory. If the message has hit the maximum retry amounts, it will be moved to Bad Mail, even if the failed message lifetime has not been reached.</td>
</tr>
<tr>
<td>Delay notifications</td>
<td>When an email fails to be delivered, but the error is not permanent (which could happen if there was a network error, the remote server was down, or other errors), then MailEnable will send an email to the original sender to inform them that the message has been delayed. This option can either turn delay notifications off, send a message only on the first failure, or to send a message back for each send delay. There is also the option to only send delay notifications after a specified period of time from when the message send is first attempted. This will allow the SMTP service try to send the message more than once before the sender is informed that there is a delay.</td>
</tr>
<tr>
<td>Do not generate Non-delivery Receipts</td>
<td>When an email cannot be delivered and the error is permanent, then MailEnable will send a message to the original sender informing them of the error. Enabling this option will stop this message from being generated.</td>
</tr>
</tbody>
</table>

Delivery failure notifications can be customized for the SMTP service. Templates can be used for either a post office (if the message which fails can be attributed to a post office) or for the server. The template files for a post office need to be configured in the following folder:

Mail Enable\Config\Postoffices\[postoffice]

If this template file does not exist, then the server level one will be used, which is located at:

Mail Enable\Config\Postoffices

MailEnable provides two template files for non-delivery reports:
The following tokens can be used in a template: [ME_POSTMASTERADDRESS], [ME_TOADDRESS], [ME_DATE], [ME_MESSAGEID], [ME_FAILEDRECIPIENTS] and [ME_MESSAGEHEADERS]

5.1.9 SMTP - Smart host

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Host Enabled</td>
<td>Enabling this option will force all outbound email to be sent to one server, which is entered here. Do not configure this to point back to the MailEnable server.</td>
</tr>
<tr>
<td>This server requires authentication</td>
<td>The server that is being forwarded all of the email may require SMTP authentication. If so, enable this option and enter the username and password that has been assigned. The login method used is AUTH LOGIN.</td>
</tr>
<tr>
<td>Domain smart-hosting takes priority</td>
<td>It may be desirable to configure a local domain in MailEnable and smart-host this to a different server to the general outbound email. Enabling this option will allow the smart-hosts that have been configured for individual domains to override the SMTP outbound smart-host.</td>
</tr>
</tbody>
</table>

5.1.10 SMTP - Logging

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Options</td>
<td>MailEnable's SMTP Connector provides W3C, Activity and Debug logging. W3C logging is used to record service usage, Activity logging is used to record system activity and Debug logging is used to provide low-level information on system activity.</td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Enables W3C logging for the SMTP service. W3C logging can specify which fields are logged and the rollover frequency. The directory can also be specified.</td>
</tr>
<tr>
<td>Activity Log</td>
<td>Enables the Activity Log.</td>
</tr>
<tr>
<td>Debug Log</td>
<td>Enables the Debug Log.</td>
</tr>
</tbody>
</table>

5.1.11 SMTP - Blocked addresses

Blocked addresses are those SMTP email addresses the server will not accept email for. Any email sent to one of these addresses via SMTP will receive an error indicating that the address does not exist.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds a new SMTP email address to block.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected blocked email address.</td>
</tr>
</tbody>
</table>

5.1.12 SMTP - White list

White list IP addresses are those that are not checked for reverse DNS blacklisting or SPF and are not auto-blocked by the SMTP security options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable white list</td>
<td>Enables the SMTP white list.</td>
</tr>
</tbody>
</table>
MailEnable can also automatically whitelist IP addresses to which it has addressed outbound e-mail. This helps reduce the SMTP service from rejecting email from valid senders, as it makes the assumption that if you send to an IP address then that IP is a valid mail server and incoming email from that IP should not be blocked.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable white list</td>
<td>Enables the SMTP white list.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds an IP address to the white list.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected IP address from the white list.</td>
</tr>
</tbody>
</table>

5.1.13 SMTP - Sender Policy Framework (SPF)

SPF is an acronym for Sender Policy Framework. It describes a method of verifying whether a sender is valid when accepting mail from a remote mail server or email client. An SPF check involves verifying the email address the sender is using to send from, and the IP address they connect to the SMTP service with. SPF uses the sender’s domain to retrieve a TXT DNS record (basically a small text snippet) that describes which IP addresses the domain sends on. The retrieved record is then compared against the connecting IP address and if it matches then the sender is determined to be valid; otherwise it indicates that the sender is impersonating the sending domain.

In basic terms, Sender Policy Framework (SPF) is a method of detecting when an email sender is forging their sender address. It does this by confirming with the senders alleged domain (via DNS lookups) as to whether the connecting IP address, or other details, are valid. For example, if a spammer was sending emails as greatdeals@aol.com, a lookup is done for SPF details against the AOL.com domain. Information returned from this lookup could determine that since the IP address of the spammer is not an AOL IP address then it is likely to be spam. Email can then be marked as likely spam, or not accepted. An SPF record can also be more complicated than just a list of IP addresses, in order to give more flexibility. For details on SPF, see the following website: [http://spf.pobox.com](http://spf.pobox.com)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SPF</td>
<td>Enables SPF detection.</td>
</tr>
<tr>
<td>Reject failures</td>
<td>If an incoming connection returns a SPF fail, then the email message will not be accepted by the SMTP service.</td>
</tr>
<tr>
<td>Add Received-SPF header for unauthenticated senders</td>
<td>Adds the Received-SPF header to all unauthenticated emails arriving via SMTP.</td>
</tr>
<tr>
<td>Pass local IP addresses (no checking will be done)</td>
<td>If an IP address is determined to be local, then an SPF check is not done.</td>
</tr>
<tr>
<td>Enable local white list policy</td>
<td>Use your own SPF white list policy. The local policy is checked when the all mechanism exists for the domain being checked and is not indicating a pass. The local policy only has an effect if it is passing the domain, so you would create an SPF that indicates requirements for domains you wish to pass. The white list policy can be a complete SPF record, but must exclude the SPF version string (i.e. Must not have “v=spf1”).</td>
</tr>
<tr>
<td>Apply best guess policy for domains without</td>
<td>For connections that do not have an SPF record further checks can be added in their place. A subsequent check could be done on an MX record or even an A record for</td>
</tr>
</tbody>
</table>
With MailEnable, the results of a SPF test are added as a header item to the email. The header is **Received-SPF**. SPF tests return one of seven results, which are outlined below. The added header includes the result and a brief description. If there are filters running to check the header, the first string after the header is the result. E.g. Received-SPF: none, Received-SPF: fail. For information on configuring filters for handling SPF results, please see the **Standard filter criteria section (Section 6.2.2)**.

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>The email comes from a valid source.</td>
</tr>
<tr>
<td>Softfail</td>
<td>The email may not be from a valid source.</td>
</tr>
<tr>
<td>Fail</td>
<td>The email does not come from a valid source.</td>
</tr>
<tr>
<td>Neutral</td>
<td>The data is inconclusive in determining whether the email is coming from a valid source.</td>
</tr>
<tr>
<td>None</td>
<td>The domain has no SPF record.</td>
</tr>
<tr>
<td>Error</td>
<td>There is an error processing the SPF.</td>
</tr>
<tr>
<td>Unknown</td>
<td>There is an error processing the SPF.</td>
</tr>
</tbody>
</table>

### 5.1.14 SMTP - Reverse DNS blacklisting

**Note**: Reverse DNS Blacklisting is not available under Windows NT 4, and you will not see its configuration screen.

Reverse DNS Blacklisting allows DNS based blacklists to be used with MailEnable. This can help to control spam. It is possible to select which RBL blacklist providers to use, however, only the select providers that are needed as this feature has an impact on performance.

DNS blacklists are lists of IP addresses that are not allowed to connect to the email server. These lists are formed in various ways. Some lists are simple listings by country, some list known spammers and some are reactive and add entries only after an IP address was responsible for sending out junk email. Blacklists have a high risk of causing “false positives”, which means that legitimate email may be refused. Before using DNS blacklists, it is wise to do some research on how the lists are maintained, what the removal process for listed IPs is and what their motivations and goals are with their list.
Configure reverse DNS blacklisting as follows:

1. From the Administration program select **Servers > localhost > Connectors > SMTP > Properties**
2. Select the DNS Blacklisting TAB
3. Check the option to Enable DNS Blacklisting
4. Select the desired action to complete - the default is “Don’t accept the email”
5. Select the Add button and the following window will be displayed
6. Select a blacklist followed by OK.
7. The selected blacklist will show in the “Current Enabled DNS Blacklists” display window.
8. Repeat this process to enable multiple lists.

### DNS blacklists

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Enabled DNS Blacklists</td>
<td>Shows all lists that have been enabled for the server. This includes the MailEnable defaults and any personally created lists.</td>
</tr>
<tr>
<td>Add Button</td>
<td>To choose a blacklist, select this button, select a list and click OK. The list will now be displayed in the “Current enabled DNS Blacklists” window on the DNS Blacklisting TAB.</td>
</tr>
<tr>
<td>Remove Button</td>
<td>To remove a list at any time, select the blacklist in the “Current enabled DNS Blacklists” window on the DNS Blacklisting TAB and select the Remove button.</td>
</tr>
<tr>
<td>Enable DNS Blacklisting</td>
<td>Enables or disables reverse DNS Blacklisting for the SMTP Connector.</td>
</tr>
<tr>
<td>Action when detected</td>
<td>The two actions here are;</td>
</tr>
<tr>
<td></td>
<td><strong>Don’t accept the email</strong> - this will prevent connection by the remote server and respond accordingly. This is the best option for reducing server load.</td>
</tr>
</tbody>
</table>
MailEnable provides a list of well-known Reverse DNS Blacklist providers. It is also possible to add your own blacklist provider by selecting the **Configure...** button.

Once the provider has been added, it can be configured using the screen outlined earlier. Select the Enable button before configuring the service provider’s details.

### 5.1.15 SMTP - Greylisting

Greylisting is configured under the SMTP options and works by initially delaying an incoming email from a particular IP address. Since mail servers would normally retry sending a message, when the message is attempted to be sent after this initial delay period it will be accepted. Spammers rarely retry messages, and therefore will be blocked. If a spammer does retry a message, hopefully within that time the IP address of the sender has been reported to a DNS blacklist that is in use, and can still be blocked.

Greylisting can be enabled for the SMTP service and the message retry initial delay time and the time the IP and sender/recipient is remembered for can be configured here.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable greylisting</td>
<td>Use the post office level setting</td>
</tr>
<tr>
<td>Messages must be retried this many minutes after initial delay</td>
<td>When the SMTP service accepts a connection from an IP address it will remember the sender and recipient and the connection will be temporarily refused. The connection will be refused until after this initial delay period.</td>
</tr>
</tbody>
</table>
When a client or server is being delayed due to greylisting, they will receive the following SMTP message:

452 This server employs greylisting as a means of reducing spam. Please resend e-mail shortly.

IP Blocking acts on the IP addresses that are reported as spam by web mail users. There are two types of blocking which is used by the SMTP service. There is a system level block and a post office level block. A system level block is an IP address which is blocked for the whole server and a post office level block is done for a connection which can be attributed to a post office.

When a message is blocked by the web mail, it will add the IP entry to the post office level spam directory. For each IP address added a separate file is created which has the time the message was reported as spam, the user that reported it and the message filename. The IP is also checked against whether it has been reported at the system level for that post office. If not, then a new file is created for this IP address. The system level file contains the timestamp of the report, and the post office that reported it.

Whitelisting an IP address will prevent it from being testing against the IP blocking list. Whitelisting can be done either by adding its IP address in the SMTP Whitelist, or by it being listed as an outbound whitelisted IP address. Local server IP addresses also cannot be blocked.

Connections are given an error when they perform a RCPT TO: SMTP command. When an IP address is blocked for the system level or post office level, the following message is in the SMTP Debug log:

ME-E011X: [socket number] Message blocked: (IP address) was found in reported in System Spam database.

ME-E011X: [socket number] Message blocked: (IP address) was found in reported in Postoffice Spam database.

The connecting server will be given the error:

452 The IP Address you are sending from was reported as a source of Spam. Please contact your e-mail administrator.

Refuse e-mail from IP addresses reported as sending spam

When enabled, the SMTP service will not accept emails coming from a blocked IP address. The service determines that an IP address is blocked by using the number of reports and a time frame, set by the “Reports required” and the “Expire after” text boxes. System level records are checked first, then the post office level records. So in order for an IP address to be blocked for the whole server, it needs to be reported by more post offices than the “reports required” setting, and to be blocked to a post office needs to be reported just that many times by any post office user(s). This setting is only useful if either a post office or the server is set to allow users to mark sender IPs as a spam source, which is done either through the global web mail settings or the web mail settings for a post office.

Blocked Address Management

Since there can be a large number of blocked addresses reported, MailEnable allows the management of such addresses. To remove an IP address that is blocked, select the “Remove IP...” button. To view details about a blocked IP address, select the “View Report...” button. When viewing a report about a spam item, the dialog displayed will indicate whether the IP address is a system level block or a post office level block.

5.2 POP Service

5.2.1 POP Service Overview

POP stands for Post Office Protocol. This is a mail protocol that enables emails to be retrieved from a remote mailbox. It allows you to collect emails from a hosted account on a server to your own email software, such as Outlook, Eudora etc.
POP and SMTP servers are often the same computer. However, in some cases, one server is used for receiving mail (POP server) and another server is used for sending mail (SMTP server).

Use the Administration Program to access the POP properties by expanding the Servers > Localhost > Connectors branch.

Right click on the POP icon and select Properties. The options are explained below:

![POP Properties](image)

### 5.2.2 POP - General

The following table outlines the configuration options for MailEnable's POP service:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum concurrent connections</td>
<td>The number of concurrent connections from email clients that the service will allow.</td>
</tr>
<tr>
<td>Alternate @ characters</td>
<td>Some older mail clients don't allow the use of @ in the username section. Since the MailEnable usernames are formatted in mailboxname@postoffice format, this may cause problems. To solve this, MailEnable can specify the characters that can be used as a substitute. Just enter the list of characters such as #$. This will allow users to log on using mailboxname@postoffice, mailboxname#$postoffice, mailboxname$%postoffice and mailboxname%postoffice.</td>
</tr>
<tr>
<td>POP Port</td>
<td>The port MailEnable will allow client POP connections on. The default is 110.</td>
</tr>
<tr>
<td>POP Enable SSL (Default Port)</td>
<td>Enables SSL encryption for the default port that POP is running on. When enabling SSL make sure a valid SSL certificate has been selected in the MailEnable Administration &gt; Server &gt; Localhost Properties &gt; SSL tab</td>
</tr>
<tr>
<td>Also listen on alternate port</td>
<td>Allows the POP service to listen on an alternate port. Usually this is done to cater for clients who may be on connections where their outbound port 110 has been blocked.</td>
</tr>
<tr>
<td>POP Enable SSL (Alternate Port)</td>
<td>Enables SSL certificate encryption for the alternate port that POP is running on. The default port number is 995. When enabling SSL make sure that a valid SSL certificate has</td>
</tr>
</tbody>
</table>
been selected in the MailEnable Administration > Server > Localhost Properties > SSL tab.

Enable APOP authentication

Usually, the users’ username and password are sent in clear text format (i.e. not encrypted). Enabling this option will force clients to enable APOP authentication on their mail client software. Make sure users are using software that supports APOP, otherwise they will not be able to receive email. Some older mail clients do not support APOP.

Enable NTLM authentication

If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled to use this secure authentication. For example, in Outlook the feature is called SPA - Secure Password Authentication. More information on NTLM can be found in the Overview of NTLM Authentication section (Section 11.2).

Enable CRAM-MD5 authentication

CRAM-MD5 Challenge-Response Authentication Mechanism is intended to provide an authentication extension that neither transfers passwords in clear text nor requires significant security infrastructure in order to function. Only a hash value of the shared password is ever sent over the network, thus precluding plaintext transmission.

Timeout for idle connections

If this setting is enabled, and a client connection has been idle or not passed any commands to the server for a set period of time, the connection will be dropped by the server. Timeout setting is in seconds.

Access Control

The Access Control feature can specify who can connect to the POP service. A list of IP addresses that are either banned from connecting, or are the only ones allowed to connect by selecting the Access Control button can be specified.

IP Addresses to bind POP to

It is possible to select the IP addresses that the POP service will be bound to. On a multi-homed machine you may only wish to allow connections on particular IP addresses. ‘Always bind all IPs’ will allow connections on all IP addresses that are configured for the machine.

5.2.3 Advanced
The POP Retrieval connector can retrieve email from remote POP sites and deliver to local mailboxes. Administrators are able to configure this through the administration program, and if enabled for web mail, users can configure it for their own mailboxes.

Using the Administration program, access the POP Retrieval Connector properties by expanding the Servers > Localhost > Connectors branch.

Right click on the POP Retrieval icon and select Properties. The options are explained below:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use alternate welcome message</td>
<td>This is the welcome message which is displayed to email clients connecting to the service.</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Set the inactivity timeout for the POP service. If a connection is inactive for longer than the timeout period (in seconds) then the connection will be closed.</td>
</tr>
<tr>
<td>Allow concurrent mailbox access</td>
<td>By default POP servers only allow one connection to a mailbox at any time. Enabling this will allow multiple connections to the same mailbox. Be aware that some POP email clients expect they are the only connection to a mailbox and may produce warning or error messages if another connection deletes email during the connection</td>
</tr>
</tbody>
</table>

5.2.4 Logging

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Logging</td>
<td>Enables W3C logging for the POP service. W3C logging can specify which fields are logged and the rollover frequency. The directory can also be specified.</td>
</tr>
<tr>
<td>Logging Options</td>
<td>Produces a debug and activity log for the POP3 service. Use this to obtain more details about the service.</td>
</tr>
</tbody>
</table>

5.3  POP Retrieval Connector

5.3.1 POP Retrieval Connector

The POP Retrieval connector can retrieve email from remote POP sites and deliver to local mailboxes. Administrators are able to configure this through the administration program, and if enabled for web mail, users can configure it for their own mailboxes.

Note: Do not configure POP Retrieval to pull email down from the local server.
The List Server connector is mostly configurable through the creation and management of particular lists as described earlier in this manual.

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poll Interval</td>
<td>The delay between polling the remote mail server.</td>
</tr>
<tr>
<td>Max. number of threads</td>
<td>The maximum number of threads that the polling agent uses to poll remote mailboxes.</td>
</tr>
<tr>
<td>Days to keep history</td>
<td>In order to stop downloading the same email every time a poll is performed, MailEnable keeps a history of the messages downloaded from each server. In order to conserve resources, it is possible to specify how many days to keep this history of messages.</td>
</tr>
<tr>
<td>Add received header to retrieved emails</td>
<td>Emails retrieved via the POP Retrieval connector will be ordered in email clients at the time that they arrive in MailEnable. To avoid this, disabling this option will order them in the time that the arrived at the remote mail server.</td>
</tr>
<tr>
<td>Enable logging</td>
<td>Enables logging for the service.</td>
</tr>
<tr>
<td>Advanced Logging</td>
<td>This is the configuration and the enabling of each log namely the activity, debug and W3C.</td>
</tr>
</tbody>
</table>

### 5.4 List Server Connector

#### 5.4.1 List Server Connector

The List Server connector is mostly configurable through the creation and management of particular lists as described earlier in this manual.
The post office connector performs the delivery of emails to mailboxes. It is responsible for executing mailbox filters, delivery events, auto responders and quota handling.

It is possible to determine whether the user is notified of the quota issue and whether the message is returned to the sender or sent to the postmaster for that post office.

MailEnable can configure what notifications are sent when a quota is reached, such options such as, Notify Sender only, notify sender and mailbox and send no notifications.

Non Delivery Receipts can be configured options such as not sending NDRs or allowing the SMTP service to handle and send all default Non Delivery Receipts.

Using the Administration Console you can access the Post Office Connector properties by expanding the Servers > Localhost > Connectors branch.

Right click on the Post office icon and select Properties. The options are explained below:

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate posting failure notifications</td>
<td>By ticking this box, if a message is sent to a list and is rejected due to sender being rejected or incorrect password, then a posting failure notification is sent. Disabling this feature can help reduce traffic where spammers have sent to the address and used a forged email address.</td>
</tr>
<tr>
<td>Advanced Logging</td>
<td>This setting allows the logging of list activity and any problems that may arise. To improve speed and to not create logs disable the activity and debug logs.</td>
</tr>
</tbody>
</table>

5.5 Post Office Connector

5.5.1 Post office connector Overview

The post office connector performs the delivery of emails to mailboxes. It is responsible for executing mailbox filters, delivery events, auto responders and quota handling.

It is possible to determine whether the user is notified of the quota issue and whether the message is returned to the sender or sent to the postmaster for that post office.

MailEnable can configure what notifications are sent when a quota is reached, such options such as, Notify Sender only, notify sender and mailbox and send no notifications.

Non Delivery Receipts can be configured options such as not sending NDRs or allowing the SMTP service to handle and send all default Non Delivery Receipts.

Using the Administration Console you can access the Post Office Connector properties by expanding the Servers > Localhost > Connectors branch.

Right click on the Post office icon and select Properties. The options are explained below:
### 5.5.2 Post office connector - General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When mailbox has reached quota</td>
<td>Specify what occurs when a mailbox’s quota is exceeded. Determine whether the user is notified of the quota issue and whether the message is returned to the sender, or, sent to the postmaster for that post office.</td>
</tr>
<tr>
<td>Notifications when quota is reached</td>
<td>Configure what notifications are sent when a quota is reached, such options such as, notify Sender only, notify sender and mailbox and send no notifications.</td>
</tr>
<tr>
<td>Quota enumeration</td>
<td>When a mailbox is at its quota, it can be calculated in two different ways. 1. Only Inbox folder counts towards quota 2. All users mail folders counts towards quota (Example: Sent Items, Drafts, Inbox)</td>
</tr>
<tr>
<td>Auto responders enabled</td>
<td>When this setting is enabled there are two selections; 1. The default setting to “Always respond to the sender” 2. Send one response per sender per day can help reduce the problem of spammers generating unnecessary mail. Also if a sender needs to send to a MailEnable mailbox that has an auto responder configured, then they will not receive more than one auto-responder per day. If the check box is cleared then the auto responder feature is disabled. This can aid in the diagnosis of mail loops or any possible auto responder issues.</td>
</tr>
<tr>
<td>NDR Generation</td>
<td>Non Delivery Receipts can be configured. Options such as not sending NDRs or allowing the SMTP service to handle and send all default Non Delivery Receipts.</td>
</tr>
<tr>
<td>Redirection handling</td>
<td>Redirection handling has the following settings: 1. Normal redirection - will redirect emails. Redirected emails have the envelope sender of the original message preserved. 2. Remail from mailbox address - will redirect and send using the default email address for the mailbox. If a default address has not been set, the first address found for the mailbox will be used. This option will help prevent rejections from</td>
</tr>
</tbody>
</table>
IMAP4 is a mail protocol that allows users to be disconnected from the main messaging system and still be able to process mail. Users can store messages on a local machine or on a server.

IMAP has distinct advantages over POP because it allows management of multiple folders on the server. Mail can be accessed from different machines, as the mail is hosted on the server (unlike POP which deletes mail from the server after being accessed) and allows the user to just download message headers and envelope information, until the user selects the email to download. This is useful when operating over slow speed dial-up connections.

IMAP4 can break up and download specific parts of a multi-part email message (MIME). This means that instead of having to wait for an email with attachments to download, it is possible to select only the text portion to download, and leave the attachments on the server.

Using the Administration Console, access the IMAP properties by expanding the Servers > Localhost > Services branch.

Right click on the IMAP icon and select Properties. The options are explained below:

### 5.5.3 Logging

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>Enables the activity and debug logs for the post office connector.</td>
</tr>
</tbody>
</table>

### 5.6 IMAP Service

#### 5.6.1 IMAP Service Overview

IMAP4 is a mail protocol that allows users to be disconnected from the main messaging system and still be able to process mail. Users can store messages on a local machine or on a server.

IMAP has distinct advantages over POP because it allows management of multiple folders on the server. Mail can be accessed from different machines, as the mail is hosted on the server (unlike POP which deletes mail from the server after being accessed) and allows the user to just download message headers and envelope information, until the user selects the email to download. This is useful when operating over slow speed dial-up connections.

IMAP4 can break up and download specific parts of a multi-part email message (MIME). This means that instead of having to wait for an email with attachments to download, it is possible to select only the text portion to download, and leave the attachments on the server.

Using the Administration Console, access the IMAP properties by expanding the Servers > Localhost > Services branch.

Right click on the IMAP icon and select Properties. The options are explained below:
5.6.2 IMAP - General

The setup of IMAP is relatively simple, as it is a service that is bound to a listening port similar to HTTP. The IMAP service listens on this port and receives mail and various commands from the server. It is important to enable the default port of 143 on the firewall or any other port number stipulated in the properties of the IMAP service in the administration program as above.

To help in server traffic and load, also stipulate which IP address to bind the service to.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Concurrent connections (threads)</td>
<td>The number of threads that will be used by the IMAP service to handle client requests.</td>
</tr>
<tr>
<td>IMAP port</td>
<td>Port for listening on. Default is 143.</td>
</tr>
<tr>
<td>IMAP Enable SSL (Default Port)</td>
<td>This will enable SSL certificate encryption for the default port that IMAP is running on. Place a tick in this box to enable the service. This also has to be enabled at a server level in the MailEnable Administration program under Server &gt;Localhost Properties &gt; SSL tab.</td>
</tr>
<tr>
<td>IMAP Enable SSL (Alternate Port)</td>
<td>This will enable SSL certificate encryption for the alternate port that IMAP is running on. The default port number is 993. Place a tick in this box to enable. The service also has to be enabled at a server level in the MailEnable Administration program &gt; Server &gt; Localhost Properties &gt; SSL tab.</td>
</tr>
<tr>
<td>Also listen on alternate port</td>
<td>An alternate port can be selected.</td>
</tr>
<tr>
<td>Client Connections</td>
<td>Select either an unlimited number of client connections, or specify a maximum number of concurrent connections. Specifying a maximum number of connections may reduce server load by limiting the threads that IMAP can use.</td>
</tr>
<tr>
<td>Enable public folders</td>
<td>Public Folders allow one or more mailboxes under the post office to share data (messages in a folder that is seen by all mailboxes in the post office.) Anything placed in this folder (Program Files\MailEnable\Post Offices[Post Office Name] \Pubroot) will become visible to all other mailboxes in the post office. This feature must be enabled for the post office in Post Office Properties.</td>
</tr>
</tbody>
</table>
HTTP is the protocol that handles web traffic. It defines how web pages are formatted and the way they are delivered over the Internet. It also includes any information about the objects that are needed by proxy servers or a user's web browser. HTTPMail is a relatively new protocol for the server hosted messaging.

### Enable NTLM authentication

If enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled use this secure authentication. For example, in Outlook the feature is called SPA - Secure Password Authentication. More information on NTLM can be found in the Overview of NTLM authentication (Section 11.2).

### Enable CRAM-MD5 authentication

CRAM-MD5 Challenge-Response Authentication Mechanism is intended to provide an authentication extension to IMAP4 that neither transfers passwords in clear text nor requires significant security infrastructure in order to function. Only a hash value of the shared password is ever sent over the network, thus precluding plaintext transmission.

### Timeout for idle connections

If this setting is enabled and a client connection has not passed any commands to the server for the set period of time, the connection will be dropped by the server.

### IP Addresses to bind to

It is possible to select the IP addresses that the POP service will be bound to. On a multi-homed machine it may be desirable to only allow connections on particular IP addresses. 'Always bind all IPs’ will allow connections on all IP addresses that are configured for the machine.

## 5.6.3 Logging

### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Options</td>
<td>MailEnable's IMAP Connector provides W3C, activity and debug logging. W3C</td>
</tr>
<tr>
<td></td>
<td>logging is used to record service usage, Activity logging is used to record</td>
</tr>
<tr>
<td></td>
<td>system activity and debug logging is used to provide low-level information on</td>
</tr>
<tr>
<td></td>
<td>system activity.</td>
</tr>
</tbody>
</table>

## 5.7 HTTPMail Service

### 5.7.1 HTTPMail Protocol

HTTP is the protocol that handles web traffic. It defines how web pages are formatted and the way they are delivered over the Internet. It also includes any information about the objects that are needed by proxy servers or a user's web browser. HTTPMail is a relatively new protocol for the server hosted messaging.
services. HTTPMail provides an alternative to using POP and SMTP, with the added benefit of allowing messages to be hosted on the server (rather than downloaded onto the client). Further to this, using HTTPMail, messages can be moved between the server and local stores as required.

HTTPMail utilizes WebDAV HTTP Extensions to provide remote access to server hosted mail folders using standard HTTP communication. This service allows mail messages to be hosted on the server and provides tight integration with Outlook 2002 (and later) and Outlook Express, although subfolders are not supported in HTTPMail. Unlike IMAP, it does not require SMTP to send messages. HTTPMail posts messages into the post office where they are either locally delivered or dispatched through the SMTP Connector.

Another benefit HTTPMail has over using POP and SMTP, is that it can be configured to operate over Port 80 enabling access to mail through corporate firewalls.

Using the Administration Console you can access the HTTPMail properties by expanding the Servers > Localhost > Services branch.

Right click on the HTTPMail icon and select Properties. The options are explained below:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPMail Port</td>
<td>The HTTPMail service will listen for connections on this port.</td>
</tr>
<tr>
<td>Session timeout</td>
<td>Determines how long a connection will remain active for.</td>
</tr>
<tr>
<td>Enable public folders for post offices</td>
<td>Public Folders allow one or more mailboxes under the post office to share data (messages in a folder that is seen by all mailboxes in the post office.) Anything placed in this folder ([Program Files\MailEnable\Post Offices[Post Office Name]\Pubroot]) will become visible to all other mailboxes in the post office. This feature must be enabled for the post office in Post Office Properties.</td>
</tr>
<tr>
<td>IP addresses to bind HTTPMail to</td>
<td>It is possible to select the IP addresses that the HTTPMail service will be bound to. On a multi-homed machine you may only wish to allow connections on particular IP addresses. ‘Always bind all IPs’ will allow connections on all IP addresses that are configured for the machine.</td>
</tr>
</tbody>
</table>

5.7.2 Configuration

HTTPMail requires very few configuration settings. The major configuration settings are the IP address(es) and port bindings for the HTTPMail Service. If the option to install HTTPMail is selected, the service is published on port 8080 of the server (it is possible to change this setting to an alternate port, but 8080 is
the default so that the service does not conflict with any existing web services that may be running). Features of HTTPMail can be enabled or disabled via the administration program.

If using Outlooks Express or Outlook 2002 as a mail client, select the mail protocol as HTTP and enter in the following details:

- My incoming Mail Server is a HTTP server
- My HTTP mail service provider is: Other
- Incoming mail (POP3, IMAP or HTTP) server:

http:// Your Server: 8080/MEHTTPMail

Since HTTPMail is an authenticated service, use the usual account credentials when prompted (i.e.: User@Your Account/Postoffice). For a more detailed explanation of configuring HTTPMail for mail clients, please see the Configuring email clients section (Section 8.1).

5.8 Mail Transfer Agent (MTA)

5.8.1 MTA Overview

The Mail Transfer Agent (MTA) is primarily responsible for moving messages between connectors. The MTA moves messages from inbound queues to the respective outgoing queues of different connectors based on rules defined in an Address Map table.

Examples of MTA functionality follow:

- Receiving inbound messages from mail connectors
- Delivering mail to local mailboxes
- Queuing mail for relay to other mail connectors (including themselves, as in SMTP Relay)
- Executing external filters (such as antivirus) and pickup events

5.8.2 MTA properties

![MTA Properties](image)

The configuration options for the Mail Transfer Agent are outlined in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound mail</td>
<td>The delay time before an inbound mail message is delivered.</td>
</tr>
</tbody>
</table>
### Web mail

#### 5.9.1 Webmail Overview

The web mail information in this manual includes configuration and the various server options. For details on using web mail, please check the MailEnable Web Mail User Guide from the MailEnable website.

Web mail is a mail application that allows clients to send and receive email via the Internet. Once installed, web mail can be accessed from `http://HostName/mewebmail` - in place of the HostName in this example, use the server name as defined in DNS or under IIS. The IP address of the machine can also be used. When browsing to this location, a logon screen will be presented. Users should use the same username and password that the POP service uses. Remember that the username is formatted as: `mailboxname@postofficename` - if a default post office has been set using the administration program, there is no need to use the `@postofficename` after the mailbox name.

Leveraging Internet Information Services and the Microsoft .Net Framework, the web mail component can provide messaging services via the web browser. Users can access the messages hosted on the server to send and receive email via a web based front end.

Some of the features of MailEnable web mail include:

- Add attachments to emails
- Contact list
- Management of POP retrieval
- Configure redirection
- Reply, reply to all, forwarding, read receipts, message priority
- Viewing & editing of HTML mail
- Support for various character sets (Big5, etc.)
- Auto-signature
- Manage folders
- Configure POP Retrieval
- Custom skins

MailEnable web mail is installed as a Virtual Directory under an existing IIS Web Site. Typically there are two web sites that are pre-configured under IIS, these are the “Default Web Site” and the “Administration Web Site”. IIS allows additional sites to be created (either using host-headers or additional IP addresses) using the Internet Services Manager.
5.9.2 Web mail configuration

Use the Administration program to enable or disable various features of web mail. Using the Administration program, access the web mail properties by expanding the Servers > Localhost > Services branch.

The settings for web mail are explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users can configure POP Retrieval for web mail</td>
<td>Determines whether POP Retrieval is able to be configured in the web mail options tab.</td>
</tr>
<tr>
<td>Users can add a redirection</td>
<td>Determines whether web mail users are permitted to redirect their mail to alternate addresses.</td>
</tr>
<tr>
<td>Users can change passwords</td>
<td>Sets whether users can change their password using the web mail interface.</td>
</tr>
<tr>
<td>Users can configure auto responders</td>
<td>Permits web mail users to configure auto responses for their mailbox (for example: Out of Office automatic replies).</td>
</tr>
<tr>
<td>Users can set their display name</td>
<td>Allows users to specify the friendly name to be used. The friendly name is then edited within the Mailbox properties page under the “Addresses” tab and is also configurable within the web mail interface in the “options” page.</td>
</tr>
<tr>
<td></td>
<td>NOTE: If a friendly name has been set for a mailbox and messages are received within any Email client program then the friendly name that was set in MailEnable Administration Program or web mail will not be visible because the Email client will use the name set in the account options. The friendly name has been designed to work within the MailEnable web mail interface.</td>
</tr>
</tbody>
</table>

5.9.2.1 Web mail configuration - General
If using web mail on a Windows 2003 server, by default users are restricted to a maximum of 200 kilobyte upload. To change this, follow the instructions in Increasing upload limit for Windows 2003 (Section 11.8).

Web mail logging creates a web mail log file in your MailEnable directory. This feature should only be enabled if there is a requirement for additional logging or to debug/diagnose the web mail service.

The “Report as spam” web mail option allows web mail users to mark messages as spam and have an action perform on them.

This action is configured in the administration program either globally or at a post office level. Global settings will override post office settings.

Under the web mail option there is a new drop down list with the following options:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display HTML mails in preview window</td>
<td>This option determines whether HTML mails are shown in the preview window. Setting this option increases the system overhead of MailEnable.</td>
</tr>
<tr>
<td>Create URL and email hyperlinks for plain text messages</td>
<td>This option instructs MailEnable to render mail messages and hyperlinks in plain text messages as URLs.</td>
</tr>
<tr>
<td>Number of messages per page</td>
<td>Determines the number of messages that will be displayed per page.</td>
</tr>
<tr>
<td>Height of inbox list</td>
<td>Sets the height of the inbox list in pixels.</td>
</tr>
<tr>
<td>Default character set</td>
<td>The default character set that will be used for users who have not set it themselves through their web mail options. By default the character set is US-ASCII which does not cater for extended characters. If emails sent from web mail are missing extended characters or they are displayed incorrectly, it could mean that the user has not configured their character set.</td>
</tr>
<tr>
<td>Default time zone</td>
<td>The default time zone to be used for users who have not set it themselves through their web mail options. The time zone is taken from the client computer on the login page for web mail.</td>
</tr>
<tr>
<td>Site configuration</td>
<td>Add and remove web mail from current websites configured on the machine. For more details, please see the Configuring web mail section (Section 5.9.3.1).</td>
</tr>
</tbody>
</table>

5.9.2.2 Logging

Web mail logging creates a web mail log file in your MailEnable directory. This feature should only be enabled if there is a requirement for additional logging or to debug/diagnose the web mail service.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging status</td>
<td>The logging status can be set to either ‘Disabled’, ‘Log to Debug log’ or “Log to Windows Event log’. The sliding bar sets the level of logging from low to high. Low level logging includes only logins, high level logging includes listing messages, folders, sending, receiving, actions, and retrieval.</td>
</tr>
</tbody>
</table>

5.9.2.3 Spam

The “Report as spam” web mail option allows web mail users to mark messages as spam and have an action perform on them.

This action is configured in the administration program either globally or at a post office level. Global settings will override post office settings.

Under the web mail option there is a new drop down list with the following options:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use post office settings</td>
<td>Use the post office level setting.</td>
</tr>
<tr>
<td>Move spam to post office reported folder</td>
<td>The post office reported folder is: Mail Enable\Post offices[post office]\mail root\SPAM\Reported</td>
</tr>
<tr>
<td>Move spam to global spam</td>
<td>The global spam folder is the one selected under the Report as spam</td>
</tr>
</tbody>
</table>
MailEnable provides two ways of publishing web mail (or web administration) via the Internet. These approaches are referred to as configuring “Host Headers”, or a “Virtual Directory”.

The “Host Header” option allows web mail (or web administration) to be published through a single IIS web site. When a browser requests the URL, the host name portion of the URL request is mapped to the IIS web site that is publishing the MailEnable web mail (or web administration) application. This approach means web mail can be accessed through a URL like http://webmail.domainname or http://webadmin.domainname.

MailEnable web applications can be published through host headers through the following branch in the Administration Program:

MailEnable Administration > Servers > localhost > Services > Web Mail

The list displayed in the right hand pane contains the host names to which users can access the MailEnable application. To add a new host header, right click on the list and selecting New > Host Header...

This will present the following dialog which specifies the host name (eg: webmail.yourdomain), the IP address that the host name is published as under DNS, and the port number.

The web mail skin, base and default language that will be used when someone attempts to access web mail via the given hostname can also be selected.

It is also possible to configure which IIS Web Sites can access web mail. To enable web mail access from multiple web sites on the server, a virtual directory can be created under each of the sites on the server. A utility that does this can be found in the administration program in the following location:

MailEnable Management | Servers | localhost | Services | WebMail | Properties | General.

Select the Site Options tab and Configure to bring up the Site Configuration screen.

This utility appears as follows:

<table>
<thead>
<tr>
<th>folder</th>
<th>option.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete message</td>
<td>Any message that is marked as spam will be deleted.</td>
</tr>
<tr>
<td>Mark the sender IP as spam source</td>
<td>Extracts the sending IP address of the message from the headers of the message and creates 2 records in the following locations: Config\Postoffices\Postoffice\Connections\Spam Config\Connections\Spam The SMTP connector (and custom filters) can then use these records to determine whether or not to refuse mail from the IP address.</td>
</tr>
</tbody>
</table>

5.9.3 Configuring web mail

5.9.3.1 Configuring web mail Overview

MailEnable provides two ways of publishing web mail (or web administration) via the Internet. These approaches are referred to as configuring “Host Headers”, or a “Virtual Directory”.

The “Host Header” option allows web mail (or web administration) to be published through a single IIS web site. When a browser requests the URL, the host name portion of the URL request is mapped to the IIS web site that is publishing the MailEnable web mail (or web administration) application. This approach means web mail can be accessed through a URL like http://webmail.domainname or http://webadmin.domainname.

5.9.3.2 Publishing web mail through host headers

MailEnable web applications can be published through host headers through the following branch in the Administration Program:

MailEnable Administration > Servers > localhost > Services > Web Mail

The list displayed in the right hand pane contains the host names to which users can access the MailEnable application. To add a new host header, right click on the list and selecting New > Host Header...

This will present the following dialog which specifies the host name (eg: webmail.yourdomain), the IP address that the host name is published as under DNS, and the port number.

The web mail skin, base and default language that will be used when someone attempts to access web mail via the given hostname can also be selected.

5.9.3.3 Publishing web mail through virtual directories

It is also possible to configure which IIS Web Sites can access web mail. To enable web mail access from multiple web sites on the server, a virtual directory can be created under each of the sites on the server. A utility that does this can be found in the administration program in the following location:

MailEnable Management | Servers | localhost | Services | WebMail | Properties | General.

Select the Site Options tab and Configure to bring up the Site Configuration screen.

This utility appears as follows:
The utility lists all web sites that are published under IIS. It is then possible to install or remove web mail on each of these sites.

Select the web sites to install web mail for by placing a tick in the box next to the site name. Then select the ‘Install web mail for selected sites’ button.

Web mail can be removed from web sites by placing a tick in the box next to the site name and selecting the ‘Remove web mail from selected sites’ button.

5.9.4 Web mail properties

Right clicking on a host header in the right hand screen under MailEnable Management > Servers > Web mail will then allow the web mail layout to be configured.

The IIS host details section configures a host header to add to the MailEnable web mail site that is configured under IIS during the initial installation of MailEnable. The host name, IP address and port are added to this site in order to direct users to the web mail.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The host name is the domain name users type in their web browser to access the web mail. You may wish to give the web mail a URL similar to webmail.example.com. A DNS entry has to be created in order to direct users to the IIS server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The address that the host header will be bound to. The DNS entry for the host name has to therefore point to this IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the host header will listen on</td>
</tr>
<tr>
<td>Base</td>
<td>Set the base (Professional or Enterprise Edition) for web mail</td>
</tr>
<tr>
<td>Skin</td>
<td>Set the skin for the web mail interface</td>
</tr>
<tr>
<td>Language</td>
<td>Set the language for the mail interface</td>
</tr>
</tbody>
</table>

5.9.5 Browser compatibility

The following is a list of browsers that are compatible with composing HTML in web mail.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 5.5 +</td>
<td>Windows</td>
</tr>
<tr>
<td>Firefox</td>
<td>Windows, Linux, Unix, Mac</td>
</tr>
<tr>
<td>Mozilla 1.7+</td>
<td>Windows, Linux, Unix, Mac</td>
</tr>
</tbody>
</table>
5.9.6 File Storage

Introduction

The file storage extensions for webmail allow users of the webmail client to upload and save normal files (like pictures, documents, videos, etc.) alongside their email messages. As such, the webmail client has been extended to allow the storage of files in a dedicated File Storage Folder.

An advantage of this is that it allows users to store their attachments on the server, so they do not need to upload them when composing a message. It will also allow them to make use of a new image-share/publishing feature, where users can make a storage folder public so that others can browse their photos, view their videos, etc.

What’s Possible

A. Attach file from storage to email

From the File Storage view, select the files you wish to attach to a new email, then click the Send Files button.

From the Compose page, click the Attachments button. Then, from the Attachments page, click the Add from Storage button and select the file you wish to attach.

B. Save mail attachment to File Storage

From the message page, click the Attachments button. Now, from the Attachments page, click the Save to Storage button.
C. Upload file from local machine to File Storage

From the File Storage view of the target folder, click the **Upload** File button, then select the file to be uploaded.

D. Download file from File storage to local machine

From the File Storage view, select the file you wish to download and click the **Download File** button. Then select the location to save to on the local machine.

From the File Storage view of the folder to be published, click the **Publish Options** button. Next click the **Publish** radio button—this will generate a URL through which the folder can be viewed. Copy the URL for future reference, then click the **Okay** button. Now anybody can browse the contents of the published folder online through the URL just generated.

E. Publish File Storage folder

If another user publishes content, they can send you a URL to that content. Simply visit the URL in a web browser to view it.

F. Browse other users' published folders over the web

5.10 Web administration

5.10.1 Web administration server configuration

MailEnable Enterprise Edition provides an enhanced version of web administration. This console is better suited to managing post offices with thousands of users.

Web Administration is installed as an optional MailEnable component. The MailEnable installation program is configured to install web administration by default (i.e. it will only **not** be installed if you changed the options when you installed MailEnable). It is possible to validate whether web administration is installed by reviewing the MailEnable Diagnostic Report.

Ensure that web administration is enabled for a post office. This is done through the administration program.

1. Expand the **MailEnable Administration program > Messaging Manager > Post Offices branch**.
2. Right click on the post office name, and select **Properties** from the popup-menu.
3. A property page dialog will appear. Select the **Web Admin** tab at the top of the window to enter the properties page for the web administration.
4. To enable web administration, select the **Enable web administration for post office** checkbox.
It is now possible to configure the various options that the post office administrators can have access to. It is not recommended to give users the ability to add and edit domain properties, since changes or additions can cause problems with mail delivery.

Once web administration is enabled, specify which of the mailboxes in the post office are able to act as administrators. This is outlined below:

1. Right click on the desired mailbox and access the Mailbox Properties > General tab

2. Select ADMIN from the drop down list labeled Mailbox Type. If the mailbox has the ADMIN option selected, then the account can access the Web administration options for the post office that they belong to. If however the mail account has the option of SYSADMIN then the user can administer all post offices on the server; not only the one they are a member of.

It is also possible to configure which IIS Web Sites can access web mail. To enable WebAdmin access from
multiple web sites on the server, a virtual directory can be created under each of the site. A utility that
does this can be found in the Administration Program in the following location:

1. **MailEnable Management > Servers > localhost > Services > WebAdmin**
2. Right click and select properties on “Webadmin” to open the web admin properties window.
3. Next navigate to the “General” tab and select the “Configure” button in the site configuration section.

This utility appears as shown in the following example:

![WebAdmin Properties Window](image)

The above utility should list all the web sites that are published under IIS. You can then install or remove
web administration on each of these sites.

### 5.10.2 Web administration properties

Right clicking on a host header in the right hand screen under **MailEnable Management > Servers > Web
admin** will then allow the web administration layout to be configured.

The IIS host details section configures a host header to add to the MailEnable web administration site that is
configured under IIS during the initial installation of MailEnable. The host name, IP address and port are
added to this site in order to direct users to the web administration.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The host name is the domain name users type in their web browser to access the web administration. You may wish to give the web administration a URL similar to webadmin.example.com. A DNS entry has to be created in order to direct users to the IIS server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The address that the host header will be bound to. The DNS entry for the host name has to therefore point to this IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the host header will listen on</td>
</tr>
<tr>
<td>Base</td>
<td>Set the base (Professional or Enterprise Edition) for web administration</td>
</tr>
<tr>
<td>Skin</td>
<td>Set the skin for the web administration interface</td>
</tr>
<tr>
<td>Language</td>
<td>Set the language for the web administration interface</td>
</tr>
</tbody>
</table>

### 5.10.3 Accessing web administration

Once installed, Web Administration can be accessed from the following URL:

**Example:** http://HostName/meadmin

In place of the **HostName** in the above example, use the server name as defined in DNS or under IIS. The IP
address of the machine can also be used.
When browsing to this location, the Web Administration logon screen will appear.

**Note:** In order to allow someone to log onto the web administration, a mailbox needs to be allocated to them in the MailEnable Administration program, and set the mailbox as “ADMIN”. Also ensure that the username is formatted as: mailboxname@postofficename

If the error “Invalid User” occurs, either the post office is not enabled for web administration or the mailbox is not set as an “Admin” user.

### 5.11 COM component

This component can be used in any application that supports COM. For example, this component can be used in an ASP page to send email from a web application. This component will work against any SMTP mail server, not just MailEnable.

- The COM component allows email to be sent to a mail server (this does not need to be a MailEnable mail server). Features include:
  - Attachment support
  - Easily create HTML emails
  - Custom headers
  - SMTP authentication

The COM component allows easy integration of emailing sending from within any COM supporting application. It not only supports sending email to a MailEnable server, but also can be used to send email to any SMTP compatible mail server.

#### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttachmentFilename</td>
<td>The name of the file that to add as an attachment.</td>
</tr>
<tr>
<td>AttachmentName</td>
<td>The name to call the attachment.</td>
</tr>
<tr>
<td>AuthenticationMode</td>
<td>Allows use of SMTP authentication.</td>
</tr>
<tr>
<td></td>
<td>(0 = ) No SMTP authentication [1 = ) SMTP authentication. You must populate the Username and Password properties in order to authenticate.</td>
</tr>
<tr>
<td>ContentType</td>
<td>The ContentType of the email you are trying to send. For instance, if you wish to send a HTML email, use this property to set the content type to “text/html”.</td>
</tr>
<tr>
<td>ErrorString</td>
<td>This contains the full English language description of the last error. If you encounter an error, you can check this string for a more detailed error.</td>
</tr>
<tr>
<td>MailBCC</td>
<td>This is list of email addresses to BCC the email to. When using multiple email addresses, separate them with a semi-colon “;”.</td>
</tr>
<tr>
<td>MailCC</td>
<td>This is list of email addresses to CC the email to. When using multiple email addresses, separate them with a semi-colon “;”.</td>
</tr>
<tr>
<td>MailCCDisplayName</td>
<td>This is list of email addresses that are the display name corresponding to the email address set in MailCC. This list is optional. When using multiple email addresses, separate them with a semi-colon “;”.</td>
</tr>
<tr>
<td>MailFrom</td>
<td>This is the email address of the sender.</td>
</tr>
<tr>
<td>MailFromDisplayName</td>
<td>The display name of the MailFrom email address. This is the friendly name that the end user will see instead of the email address. For example, you may place the full name of the sender, or the department from which the email is coming from.</td>
</tr>
</tbody>
</table>
Methods

By setting the `ContentType` value to `text/html`, the component will generate a HTML and Plain Text representation of the message encapsulated in MIME format. You need only to set the `ContentType` property to `text/HTML` and, when the `SendMessage` method is called, the component generates the MIME encapsulated message with a multipart alternative content boundary. This boundary then contains respective `text/plain` and `text/HTML` boundaries. The mail client then determines which of the alternative content types it wants to read - based on the capabilities of the mail client or the users settings. If you set the `MessageBody` and `MessageBodyPlain` properties of the component, it will not generate a textual representation of the message and will use the property value specified for `MessageBodyPlain`.

**Advanced settings**

Server wide options for the MEMail component can be configured through the editing of Windows registry keys. If the registry key does not exist it will need to be added. These settings affect all uses of the component on the server.

The values are located under the following registry branch:

HKEY_LOCAL_MACHINE\SOFTWARE\mail enable\mail enable\Components\MEMail

<table>
<thead>
<tr>
<th>Value</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow attachments</td>
<td>DWORD</td>
<td>1 (default) = attachments can be added to emails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 = attachments cannot be added to emails</td>
</tr>
</tbody>
</table>
There are no options to administer the COM component other than to control access to the DLL itself (using Windows permissions). This can be achieved by setting permissions on MEASP.DLL in MailEnable’s BIN directory.

For example, to use the component to send mail from ASP on the local computer, ensure that relay rights have been granted to the local IP address of the computer.

This component can be used in any application that supports COM. For example, this component can be used in an ASP page to send email from a web application. This component will work against any SMTP mail server, not just MailEnable.

- The COM component allows email to be sent to a mail server (this does not need to be a MailEnable mail server). Features include:
  - Attachment support
  - Easily create HTML emails
  - Custom headers
  - SMTP authentication

The COM component allows easy integration of emailing sending from within any COM supporting application. It not only supports sending email to a MailEnable server, but also can be used to send email to any SMTP compatible mail server.

### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttachmentFilename</td>
<td>The name of the file that to add as an attachment.</td>
</tr>
<tr>
<td>AttachmentName</td>
<td>The name to call the attachment.</td>
</tr>
<tr>
<td>AuthenticationMode</td>
<td>Allows use of SMTP authentication.</td>
</tr>
<tr>
<td></td>
<td>0 = No SMTP authentication</td>
</tr>
<tr>
<td></td>
<td>1 = SMTP authentication. You must populate the Username and Password properties in order to authenticate</td>
</tr>
<tr>
<td>ContentType</td>
<td>The ContentType of the email you are trying to send. For instance, if you wish to send a HTML email, use this property to set the content type to “text/html”.</td>
</tr>
<tr>
<td>ErrorString</td>
<td>This contains the full English language description of the last error. If you encounter an error, you can check this string for a more detailed error.</td>
</tr>
</tbody>
</table>
Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddHeader</td>
<td>Adds a custom header to the email. Be careful when using this function, as incorrectly formed headers could prevent the mail from being sent.</td>
</tr>
<tr>
<td>ClearHeaders</td>
<td>Clears any custom headers that have been added with AddHeader. This would be used to send more than one message (i.e. put this call between the sends).</td>
</tr>
<tr>
<td>SendMessage</td>
<td>Send the email that has been configured with the options. The function will return zero for failure and number greater than zero for success.</td>
</tr>
<tr>
<td>SetDefault</td>
<td>Clears all the settings back to their default.</td>
</tr>
<tr>
<td>ClearAttachments</td>
<td>Clears the attachments.</td>
</tr>
</tbody>
</table>

By setting the ContentType value to text/html, the component will generate a HTML and Plain Text representation of the message encapsulated in MIME format. You need only to set the ContentType property to text/HTML and, when the SendMessage method is called, the component generates the MIME encapsulated message with a multipart alternative content boundary. This boundary then contains respective text/plain and text/HTML boundaries. The mail client then determines which of the alternative content types it wants to read - based on the capabilities of the mail client or the users settings. If you set the MessageBody and MessageBodyPlain properties of the component, it will not generate a textual representation of the message and will use the property value specified for MessageBodyPlain.
Advanced settings

Server wide options for the MEMail component can be configured through the editing of Windows registry keys. If the registry key does not exist it will need to be added. These settings affect all uses of the component on the server.

The values are located under the following registry branch:

HKEY_LOCAL_MACHINE\SOFTWARE\mail enable\mail enable\Components\MEMail

<table>
<thead>
<tr>
<th>Value</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow attachments</td>
<td>DWORD</td>
<td>1 (default) = attachments can be added to emails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 = attachments cannot be added to emails</td>
</tr>
<tr>
<td>Attachment Path</td>
<td>String</td>
<td>The path must include this string. If the postoffice or mailbox property value has been set on the object then the following variables can be used in the path: \n</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%MAILBOX%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If these values have been used in the path, but are not provided when someone is using the component then the path from “Default Attachment Path” will be used. \n</td>
</tr>
<tr>
<td>Default Attachment Path</td>
<td>String</td>
<td>This path will be used if no path has been set in the “Attachment Path” setting.</td>
</tr>
</tbody>
</table>

5.11.3 Examples

Sending an HTML email from an ASP page

```vbscript
<% ' Set oMail = server.CreateObject("MEMail.Message") oMail.MailFrom = "peter@mailenable.com" oMail.MailFromDisplayName = "Test Account" oMail.UserName = "Andrew@mailenable" oMail.Password = "password" oMail.ContentType = "text/html;" oMail.MailTo = "peter@mailenable.com" oMail.Subject = "Welcome to our service" oMail.MessageBody = "Hello there,<BR>Welcome to our new service." oMail.SendMessage %>
```

Sending an email with an attachment

```vbscript
<% ' Set oMail = server.CreateObject("MEMail.Message") oMail.MailFrom = "peter@mailenable.com" oMail.MailFromDisplayName = "Update Account" oMail.MailTo = "customer@mailenable.com" oMail.Attachmentfilename = "c:\documents\updateinfo_14_4.zip" oMail.Attachmentname = "updateinfo.zip" %>
```
DKIM Overview

DKIM provides a mechanism for verifying the integrity of a message. The message is signed before sending by encrypting a hash of its headers using public key encryption and then verified upon receipt by decrypting the signature using a public key (provided by the sender in a DNS record) and comparing the hash. This provides extremely strong assurance of a message’s fidelity and authenticity, since any change to the message’s headers or body will cause verification to fail.

The only real disadvantage is the extra time it takes to process each message, since signing and verifying both involve relatively expensive cryptographic calculations and verifying requires a lookup of the sender’s DNS records.

DKIM on MailEnable

To begin signing messages with DKIM, a DNS text record must be created for the sending domain in a sub domain called `_domainkey`. The text record will contain necessary information for verifiers, including the public key required for decrypting the signature hash. This information will be generated as part of the configuration process, and must be copied from the configuration window into the text record.

5.12.1 Configuring DKIM Signing

1. Open up the DKIM signing configuration utility through the MMC:
   1. Go to Mail Enable Management | Messaging Manager | Post Offices | <postoffice>.
   2. Right-click on the domain you wish to configure for and select Properties.
   3. Select the DKIM tab and click Configure.
2. Check the Sign outgoing messages box to enable message signing.
3. Set the options for message signing. The following options are present:
   - **Encryption algorithm**: choose which algorithm will be used for signing the headers hash.
   - **Canonicalization algorithm**: this can be set independently for the headers and the body. The simple algorithm is stricter and will cause verification to fail if the message is changed at all in transit, whereas the relaxed algorithm will tolerate some whitespace insertion.
   - **Impose body hash length limit**: this allows you to limit how much of the message body will be used in the body hash.
     - **Note**: setting a limit means that verification may succeed even if extra data is appended to the message somewhere in transit.
   - **Include user identity**: if checked, includes the sending user’s identity in the signature header.
4. Configure selectors. A selector represents a private/public key pairing and, from the verifier’s point of view, an entry in a DNS text record.
   1. Clicking New will bring up the New Selector dialog: enter a unique name for the selector and choose a key size (the larger the key, the more secure the encryption, but the longer it will take to sign and verify each message).
   2. Options for each selector can be set by selecting the selector from the Selectors list, setting the options on the right, and then clicking Update. The following options are present:
- **Test mode**: if this is checked, it indicates to verifiers that the server is testing DKIM, and that signed messages should not be treated any differently to unsigned messages, even if their verification fails.

- **Granularity**: tells verifiers that only messages sent by a specified user should pass verification. This works by comparing the granularity with the user identity.

- **Notes**: notes for human perusal.

- **Make this the active selector**: use this selector for all outgoing messages. Only one selector can be active at a time, activating one will deactivate all others (however, even deactivated selectors are available for verifying against previously sent messages, so long as their entry remains in the appropriate DNS text record).

3. It is recommended that selectors be regularly deactivated then decommissioned to prevent the key for the active (or a recently active) selector from being cracked. Selectors can be deleted with the **Delete** button.

4. To make a selector available to verifiers, that selector must be selected, and the text generated in the box at the bottom of the form must be copied into a specially created DNS text record. This record must exist within a `_domainkey` sub domain and must have the same name as the selector.

5. Click **OK** to save settings and exit, or **Cancel** to simply exit.

### 5.12.2 A Test Configuration

To test DKIM right away, try the following configuration:

- **Encryption algorithm**: rsa-sha256
- **Canonicalization algorithm**:
  - **Header**: relaxed
  - **Body**: relaxed
- **Impose body hash length limit**: false
- **Include user identity**: false

Create a new selector called “test” with a key size of 1024. With this new selector selected, set the following options:

- **Test mode**: true
- **Make this the active selector**: true

Click **Update**.

Now copy the text in the box into the DNS text record at `test._domainkey.<your domain>`.

### 5.13 Archiving

#### Log File Archiving

MailEnable allows you to archive log files into cabinet files so you may conserve disk space. Compressed files can also be purged/deleted once they become a certain age.

#### Message Archiving

MailEnable now has the ability to automatically collect and archive by date all messages that are processed by MailEnable. The archiving feature will allow messages to be saved to a folder named by date within a pre selected MailEnable internal mailbox. The administrator can control which messages are archived (according to whether they are being picked up by the Mail Transfer Agent or delivered by the Mail Transfer Agent).
6 Message Filtering

6.1 Global Message Filters

6.1.1 Global Message Filters

MailEnable’s Global Message Filters are configured under the Servers | localhost | Filters | MailEnable Message Filter section of the administration program.

When the MailEnable Message Filter branch is selected, the filters are listed in the right hand panel. Configure each of these by right clicking on them. By right clicking the Filters folder and selecting Properties, the system filters can be disabled or enabled for the server as shown in the diagram below.

![MailEnable Message Filter Properties Window](image)

6.1.2 Global Message Filter Properties

By selecting the properties of the MailEnable Message Filter branch, the general properties for the MailEnable Message Filter can be configured. These filter properties configure the infrastructure associated with content filtering.

The MailEnable Message Filter Properties window is shown below:
The configurable properties for the MailEnable Message Filter are outlined in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Log</td>
<td>Specify the status and location of the activity log file generated by the filter. This log file contains details of the filters that have been executed and their respective status.</td>
</tr>
<tr>
<td>Scratch Directory</td>
<td>The Scratch directory is used by the filters to unpack messages for analysis. This occurs when messages are scanned by the integrated Antivirus agents (this process is explained in more detail later in this section). This is the directory to where MailEnable will decode the email attachments while scanning. Make sure this directory is not subject to real-time scanning by any resident antivirus application.</td>
</tr>
</tbody>
</table>

### 6.2 Creating a Global Filter

#### 6.2.1 Creating a Global Filter Overview

To add a new global filter:

1. Expand the Messaging Manager
2. Right click on Filters in the administration program
3. Select *New* > *New Filter*
4. A dialog box *Add new filter* item will appear.
5. To enable the filter tick the *Filter is enabled* tick box where the option to name the filter appears

#### 6.2.2 Standard filter criteria

Once a filter has been added, it will appear in the list of Filters. Right clicking on the filter and selecting *Manage* will manage the associated criteria. The following screen will be displayed.
By selecting the criteria, it is possible to edit the associated attributes or conditions. As long as any of the criteria is matched, then the action(s) will be performed. Criteria for a filter can be enabled and disabled by ticking or un-ticking the box as shown above. Standard filtering when used in conjunction with each other will be considered with a case of OR separating the different criteria, for example:

Where the Subject header line contains specific words

OR

Where the message body contains specific words.

To use criteria with AND gates or a combination or AND/OR then scripted filtering is required which is covered further on in this section.

For filter criteria that rely on word or email address matching e.g. “Where Message Body contains specific words” or “Where the ‘To’ header line contains specific words”, wildcards can be used. Wildcards (*) can be used to locate a specific word that could be hiding in other words or characters (e.g. Filter identifies the word “porn” that is contained in the word Pornographic or 123porn1121). Wildcards (*) can also be used to cover a range of email addresses. The wildcard scenario can be used to complete an action on any message that arrives into the MTA from a specific domain. e.g. *@mailenable.com

Following is an explanation of each of the filter criteria.

**Where the Subject header line contains specific words**

Add and remove specific words to the criteria list by clicking the “Add” button. The criteria may be enabled or disabled by ticking the check box.

This filter is useful when incoming emails contain a re-occurring subject that needs to be filtered. Any word that is added into the filter list and is included within a subject line of a particular email going through the MailEnable MTA will be searched. If an exact match is found then the selected action (see 8.2.2 Filter actions) is completed.

**Where Message Body contains specific words**

Add and remove specific words to the criteria list by clicking the “Add” button. This filter is locates specific words in the body of the message (e.g. Viagra).

**Where the ‘To’ header line contains specific words**

This is used to specify a sender(s) email address. If an email address is matched, then the selected action is
completed.

Enter email addresses here and then click the Add button. If multiple addresses are to be filtered, it is possible to add multiple addresses separated by a semi colon - ensuring that no character spaces are contained in the entered line e.g. test@mailenable.com;test2@mailenable.com.au

Where the 'To' header line contains specific words

This is used to specify a sender(s) email address. If an email address is matched, then the selected action is completed.

Enter email addresses here and then click the Add button. If multiple addresses are to be filtered, it is possible to add multiple addresses separated by a semi colon - ensuring that no character spaces are contained in the entered line e.g. test@mailenable.com;test2@mailenable.com.au

Where the Cc header line contains specific words

The Cc criteria line is the same as the To criteria line in that any word or email address entered here will be identified by the filter. Cc is an abbreviation of carbon copy and in business terms is usually equated to “For Your inclusion” or “For Your Perusal”.

Where the ‘To’ or ‘Cc’ header line contains specific words

Filters words in the header lines in either of To and Cc fields. This is useful when messages contain a specific email address, that could be in the To or in the Cc fields of the message.

Where the 'From' header line contains specific words

Filter messages that contain a specific email address or domain name in the headers of the email.

Where the message is marked as priority

Filter emails that contain a priority. E.g. filtering all mail with a high priority.

Where the message size is more than the limit

Filter messages over a certain specified size limit. Tick the Size of message is greater than in the criteria properties window to enable the function and then specify the amount in bytes for the message size in the textbox.
Where the message size is more than the limit
Filter messages over a certain specified size limit. Tick the **Size of message is greater than** in the criteria properties window to enable the function and then specify the amount in bytes for the message size in the textbox.

Where the message has attachments
Filter particular file extensions attached to an email. To specify a file extension, the process is very similar to specifying email addresses or specific words. Simply type the file extension in the add window and select the **Add** button to add the file extension to the list. This filter can be used to find attachments containing viruses. This does not disinfect the file, however, the file can be moved or deleted by using an appropriate action.

Where the message has an attachment
Filters out emails with any type of attachment, i.e. filters emails that contain attachments of any file extension.

Bayesian filter spam probability
Filter to set the threshold for spam probability of Bayesian filtering e.g., define the filter to mark messages as junk if they have over 96.5% spam probability. See the Bayesian filtering section (Section 6.4.1.1) for information on configuring the Bayesian filter.

Where the message contains a virus
Scans a message for viruses using the virus checker(s) that have been configured in the antivirus settings. See the Creating a global filter section (Section 6.2.1) for information on configuring the antivirus plug-in.
See Creating a global filter section (Section 6.2.1) for information on configuring the antivirus plug-in.

**All messages**
This criteria is processed for all messages.

**Where the SPF test return results matching**
This criteria enumerates the SPF test performed by the SMTP Connector and returns a nominated result.

**Where the SPF test return results matching**
This criteria enumerates the SPF test performed by the SMTP Connector and returns a nominated result.

**Where the sender has authenticated**
This criteria is met when the person sending the message has authenticated before sending the message. This relates to whether the sender has undertaken SMTP authentication.

**Where the originators IP address matches**
This enumerates the IP address of the person sending the message. It relates to the IP address that the SMTP transaction was received from.

**Where the message is associated with this post office**
Specify the associated post office for the transaction. MailEnable will attempt to allocate an associated post office for each message.

**Where the message came from this MailEnable connector**
Enumerates the connector that the message is being delivered from.

### 6.2.3 Filter actions
A filter action is an event that occurs when a filter criteria is met.

To create a filter action,
1. Select the filter to create an action for.
2. Select the criteria to create an action for.
3. Select the Add action button to add to the actions list. This will open an action list window.
4. Select the desired action and select the OK button.

Actions are performed in a prioritized list - first to last. To move a particular action in the list to a desired position, highlight the action to move and use the up and down arrows located to the right of the actions list.

The following is a description of the possible actions that can be performed when criteria is met.

**Copy to badmail**
A copy of the message is sent to bad mail folder. The message will still be delivered to the destination mailbox as well. To send to bad mail, and not deliver to the mailbox, create a Delete Message action to occur after the Copy to BadMail.

**Copy to quarantine**
Copies the message to the Quarantine folder. The quarantine folder is a global area that filters can place email messages so they can be viewed or processed later by an administrator.

**Delete message**

Deletes the message.

**Notify sender**

This action will send a notification message to the sender of the message. The message filter allows system tokens to be inserted into notification message templates. When defining an action to notify a user with a message, a message template for the notification can then be specified.

The following table lists the tokens that can be used in message templates when constructing a notification message. Tokens are populated based on the criteria of the filter. For example, criteria for a filter that was specified to scan for viruses, only the “All” tokens and “Antivirus” tokens would be available within the notification template.

<table>
<thead>
<tr>
<th>Token Name</th>
<th>Description</th>
<th>Applicable criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>ME_FILTERNAME</td>
<td>Contains the name of the filter that executed the call</td>
<td>All</td>
</tr>
<tr>
<td>ME_ACTIONDESC</td>
<td>The description of the current action that call</td>
<td>All</td>
</tr>
<tr>
<td>ME_MSG</td>
<td>The system filename of the message</td>
<td>All</td>
</tr>
<tr>
<td>ME_CON</td>
<td>The system connector associated with the message</td>
<td>All</td>
</tr>
<tr>
<td>ME_IP</td>
<td>The originating IP Address of the message</td>
<td>All</td>
</tr>
<tr>
<td>ME_ACCOUNT</td>
<td>The account or post office “owning the message”</td>
<td>All</td>
</tr>
<tr>
<td>ME_SENDER</td>
<td>The sender of the message</td>
<td>All</td>
</tr>
<tr>
<td>ME_AVRESULT</td>
<td>The antivirus agent return value</td>
<td>Antivirus Scanning</td>
</tr>
<tr>
<td>ME_AVACTION</td>
<td>The action performed by the antivirus agent when scanning</td>
<td>Antivirus Scanning</td>
</tr>
<tr>
<td>ME_AVAGENT</td>
<td>The system name of the antivirus agent that was used to scan the message</td>
<td>Antivirus Scanning</td>
</tr>
<tr>
<td>ME_BADMAILSENDER</td>
<td>The system BadMail Sender as defined under the SMTP connectors properties</td>
<td>All</td>
</tr>
<tr>
<td>ME_MID</td>
<td>A system generated MessageID appropriate for the MessageID header</td>
<td>All</td>
</tr>
<tr>
<td>ME_HEADERS</td>
<td>The RFC 822 headers of the original message</td>
<td>All</td>
</tr>
<tr>
<td>ME_SZ</td>
<td>The size of the original message</td>
<td>Message Size Criteria</td>
</tr>
<tr>
<td>ME_SZL</td>
<td>The size limit of the original message</td>
<td>Message Size Criteria</td>
</tr>
<tr>
<td>ME_BFV</td>
<td>The Bayesian filtering value resulting from the message</td>
<td>Spam Probability</td>
</tr>
<tr>
<td>ME_BFT</td>
<td>The Bayesian filtering threshold for the message</td>
<td>Spam Probability</td>
</tr>
</tbody>
</table>

**Notify recipient**

Sends a notification email to the recipient to inform them that an action has occurred on an inbound email. For example, if a message is deleted because an attachment is an executable, this option will notify the recipient that this has happened.

The same notification options as outlined can be used when performing the Notify Sender action (see table above).
Notify address
This will send a notification message to a specified address.

Forward to address
This filter action forwards the email to an email address.

Execute application
Execute an application on the email. Since the MTA may execute an action concurrently, make sure that the application specified can have multiple instances running. If not, it may be required to change the MTA service to only use one thread.

Add header
Adds a header line to the email. If the header line already exists it will be replaced.

Mark as spam
This will mark the message as spam, which will send the message to a user's Junk E-mail folder if the post office option for this is set. See the Feature selection section ('Feature selection' in the on-line documentation) for more information on this setting.

Add Subject Prefix
This action will add a prefix to the subject of the message. If the prefix already exists for the subject it will not be added.

Stop processing filters
This action stops the processing of any more filter actions.

6.3 Antivirus filtering

6.3.1 How to implement antivirus filtering

Configuring MailEnable to filter viruses requires both:
1. Configuration of the antivirus program to use, and also
2. Creation of an antivirus filter in MailEnable

For further advice on selecting or configuring an antivirus program, please see the Antivirus configuration section ('Antivirus Configuration' in the on-line documentation).

Configuring the antivirus program
1. Install the selected antivirus application onto the same server that has Enterprise Edition installed
2. Ensure that any resident or real-time protector capabilities of the antivirus application have been disabled (or all the MailEnable directories have been excluded from being protected by the software).
   
   **Note**: Running a real time antivirus protection on a server can cause issues and each resident antivirus protection agent can have its own problems. If the resident/real-time monitor is enabled, the problems range from blank messages showing up when MailEnable tries to deliver a message with a virus, to possible corruption of mail system configuration files or messages themselves.

As a general rule, consider the following:
- Exclude MailEnable “Queues” and the “Config” Directories from the resident/real-time monitoring.
o Disable the resident/real-time monitor if exclusion of MailEnable directories is not possible within the antivirus application.

3. Open the MailEnable Administration program. Expand the **Servers > Local host > Filters** branch, select the **MailEnable Message Filter** icon, then select the **MailEnable Antivirus Filter** item in the list which appears on the right side panel.

4. Select the appropriate item from the list of available antivirus applications.

5. Make sure that the “Enable” (or “Enable selected antivirus”) is selected. It is possible to enable more than one antivirus application on the server, but this will affect the number of messages that can be scanned over a period of time.

6. Ensure that the correct program path to the command line virus scanner has been specified. Select the Options button to change this. Also ensure that the scratch directory exists. This directory is used to unpack the message as it is scanned for viruses.

7. Save changes.

8. Stop the MTA service.

9. Start the MTA service.

Make sure virus definition files are being updated. See the antivirus documentation for information on how to do this.

Some antivirus applications specifically require Administrative privileges to run. Since the MTA runs under the LocalSystem account, change this to an account with Administrative privileges. Open the Services control panel applet. For the “MailEnable Mail Transfer Agent” service, change the user account it runs under to a Windows user account that has Administrative rights (i.e. a member of the Administrators group).

The antivirus filter allows command line virus checkers to be used on emails that as they pass through the MailEnable server either for relay or for delivery to local mailboxes. The following presets are available but require a valid server license to use any of the following supported software:

- F-Prot
- Sophos
- McAfee Virus Scan
- Norton Antivirus Corporate Edition 7.6
- Norman Virus Control
Panda Antivirus Command Line
Grisoft AVG

It is important to disable any Real Time Virus Protection software on the server (since it will interfere with the scanning process). Please see the Real time antivirus protection section (Section 11.1.3) for more information on this.

Creating an antivirus filter

To enable antivirus filtering requires the creation of a filter in the MailEnable Administration program that detects when the message contains a virus and deletes the message or quarantines it, notifies sender, etc.

To create an antivirus filter:
1. Open the MailEnable Administration Program
2. Right click on the Messaging Manager|Filters branch and create a new filter.
3. In the name field enter something like “Antivirus Filter” (without the quotes).
4. Having created the filter, edit the criteria for the filter as follows:
5. Check the criteria “Where the message contains a virus”
6. Create the actions that are undertaken when the virus is detected. E.g. Copy the message to the Quarantine directory or Delete Message

6.3.2 Configuring the antivirus filter

The administration of antivirus filters can be accessed via selecting the properties of the MailEnable Antivirus Filter within the MailEnable administration program. It is possible to select which antivirus applications are used to analyze messages as they pass through the Mail Transfer Agent.

Once the Antivirus agents have been configured to be used by the server, they can be used by specific filters.

The configurable properties for antivirus agents are outlined in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable antivirus/filter support</td>
<td>Enables or disable all antivirus and other filters that may be installed for MailEnable.</td>
</tr>
<tr>
<td>Enable selected antivirus/filter</td>
<td>Indicates that the currently selected virus checker or filter will scan emails. It is possible to enable more than one antivirus/filter at once.</td>
</tr>
<tr>
<td>Options</td>
<td>Sets the advanced options for the currently selected antivirus application.</td>
</tr>
<tr>
<td>Test</td>
<td>Tests the currently selected antivirus program by writing out the test Eicar virus and determining whether the command line scanner can detect it. Be aware that this may not work with all command line scanners (Symantec’s Norton’s AntiVirus Corporate Edition is one of these). For scanners that do not work with the test button, check whether the antivirus program is functioning by running the MTA in debug mode.</td>
</tr>
</tbody>
</table>

Antivirus options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Path</td>
<td>The path to the virus checker application. Only select the command line scanner for the antivirus application (the presets in MailEnable will point to the correct application).</td>
</tr>
<tr>
<td>Command line arguments</td>
<td>The command line arguments that are used to run the antivirus scanner. There should be no need to change these options unless adding your own antivirus scanner (i.e. not a preset).</td>
</tr>
<tr>
<td>Command line arguments will</td>
<td>Selecting this will require that the command line scanner to delete any infected attachment. Some virus scanners cannot remove zip files that are infected with viruses</td>
</tr>
</tbody>
</table>
It is not advisable to notify the sender that the have an infected email. When a virus is sent via email, it will usually use a different senders address that it randomly picks from the infected machine. So by sending notifications back to the sender address it is probably not being sent to someone who is infected.

Also consider that virus-scanning email adds more load on the server. This is because the antivirus filter must extract and test every attachment that goes through the server. It is advisable to adjust the MTA maximum transfer threads under the MTA properties to ensure that the number of concurrent instances of virus scan agents is appropriately configured. Consider that each transfer thread could potentially mean a different concurrent instance of the agent’s command line scanner.

### 6.3.3 Testing Antivirus Configuration

The antivirus filter can be tested by emailing the Eicar test virus through the system. This test virus can be downloaded from [http://www.eicar.com](http://www.eicar.com). To perform more advanced testing and debugging, follow the details in this article - [http://www.mailenable.com/kb/viewarticle.asp?aid=85](http://www.mailenable.com/kb/viewarticle.asp?aid=85)

### 6.4 Bayesian filtering

#### 6.4.1 Configuring Bayesian Filtering

##### 6.4.1.1 Setting up auto-training Bayesian filtering Overview

Bayesian Filtering is founded on having two pools of messages (good and bad) and creating a word dictionary that outlines the frequency of tokens (words or text snippets) within these messages. This dictionary allows MailEnable to analyze messages and provide a probability of a message being spam, as a new message can have its tokens compared against this dictionary. For example, if the token “FREE” occurs mostly in spam emails, but rarely in good emails and a new message has the token “FREE” in it, it is likely to be spam. As multiple tokens are used, the accuracy is improved. If an incoming email has the “FREE” token but also the token “mailenable”, which may appear only in good emails, then the good token will stop the email from being marked as spam.

The effectiveness of this approach is determined by having good samples of spam and non-spam. The process of compiling a dictionary from samples of spam and non-spam is called ‘training’.

MailEnable has four options for configuring Bayesian filtering:

1. Auto-training
2. Using the default dictionary
3. Manual training via a command line utility and scripts
4. A combination of both manual and auto-training

Setting up auto or manual training (although not essential) allows the Bayesian filter to better detect spam by continuously updating and adding to the dictionary.

The option of manually training the filter is a more complex process and is described in the Manual Training section (Section 6.4.4).

#### 6.4.1.2 Step 1: Set up auto-training for the filter
The Bayesian filter can be auto-trained using ‘good’ emails (ham) and ‘bad’ emails (spam). The auto-training feature can be enabled under *Servers > Localhost > Filters > MailEnable Bayesian Filter > Properties > Auto-training tab.*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto-training</td>
<td>Check this box to enable auto-training. While the Bayesian Filter is in auto training mode, the functions to manually update the dictionary using the “mespamcmd.exe” command utility (as mentioned in the Spam Training Utility section (Section 6.4.5)) do not function. This is because when the auto-training is running, new additions to the dictionary are stored in memory, and not written to the hard drive until the MTA service is stopped. A global filter with the ‘Bayesian filter spam probability’ criteria must be configured for auto-training to work. This is described in Step 4. If a filter is not configured with a Bayesian criteria, then no auto-training will occur.</td>
</tr>
<tr>
<td>Options (Process HTML content in Messages)</td>
<td>If this option is selected and the message contains HTML, then the HTML is parsed as well as the message plain/text boundary. Tokens will therefore also include data from the HTML messages. It makes the filter more likely to detect HTML as spam because the tokens/patterns of the HTML of bad messages can be used to calculate the probability of spam.</td>
</tr>
<tr>
<td>Spam Honeypot Email Addresses (Edit address list)</td>
<td>Define email addresses that do not receive valid mail for sampling. This is described in Step 2.</td>
</tr>
<tr>
<td>Ham Addresses (Edit address list)</td>
<td>Define ‘ham’ or legitimate email addresses for sampling. This is described in Step 3.</td>
</tr>
</tbody>
</table>

Auto-training will only update the dictionary with additional spam messages when the corresponding total number of ‘good’ ham messages is the same or greater as the total number of ‘bad’ spam messages (and vice versa).

### 6.4.1.3 Step 2: Collecting spam for auto-training

By defining “honey pot” addresses, samples of spam email can be collected. “Honey pot” addresses are addresses that are designed to collect spam.

Collect spam by creating a catchall address. Set up a mailbox address (e.g. spam@example.com) as a catchall address. This address will collect all emails for a domain that do not have a mapping to a mailbox. The majority of mail in this mailbox will be spam, as spammers will often send to unknown addresses for a domain. See the Create Domain section (Section 4.4.2) for more information on setting up a catchall. If manual training is being used on conjunction with auto-training, the emails collected here should not be used for the manual training process. Also, since a catchall will collect a lot of email the mailbox will need to be purged often.

### 6.4.1.4 Step 3: Collecting ‘ham’ for auto-training

Desirable or legitimate e-mail is commonly referred to as “ham”. The ham addresses option under the auto-training settings is for valid email addresses that are used to sample legitimate email. Specify the e-mail addresses to be considered for sampling legitimate email under the administration program. It is best to sample from a variety of valid addresses in order to get a decent sample of messages, and a spread of valid types of messages.

### 6.4.1.5 Step 4: Create a global Bayesian filter

A global filter needs to be created in order for messages that pass through the server to be checked by the Bayesian filter and an appropriate action performed. The filter criteria can specify the level of spam probability and subsequent actions for those messages that are deemed to be spam. The following example will remove messages with over 95% spam probability.
1. Create a new filter called “Bayesian” here: Messaging Manager > Right Click Filters > New Filter
2. Set the criteria “Where the message has over a certain spam probability ->95%”
3. Set the action to execute when a spam message is detected. This would normally be “Mark as spam”.

6.4.1.6 Step 5: Testing the Bayesian filter

To ensure Bayesian filtering is working correctly (i.e. the Bayesian filter is using the dictionary and the designated actions are completed when messages are delivered to the system) requires testing.

There are a few ways to determine if messages are being checked against the dictionary:

- **METray** (see the System Tray Utility section (Section 10.1)) shows instances where the Bayesian filter has scanned and detected spam. When the METray display window is open, enable the “View statistics since services were restarted”. The section that details how many “Bayesian Scans” have completed along with “Bayesian Detections” will display how many emails were checked and how many have been detected as spam since the MTA service was last started.

- Filter logs will also display any Bayesian detections. The logs are accessed via: MailEnable Administration program > Servers > Localhost > Filters > MailEnable Message Filter > Logs > Filters. If any messages have been detected and actioned by the Bayesian filter then a line in the logs will be displayed similar to the following:

  
  
  [Date-Time] [Message ID] SMTP Bayesian COPY_TO_QUARANTINE,DELETE
  [SMTP:sender@remotedomain.com] [IP_Address of sender]

- Messages passing through the Bayesian filter will have a header line added indicated the spam probability that was calculated. The header item is: X-ME-Bayesian: 0.00000

6.4.2 Bayesian filter general settings

There are additional settings for configuring the Bayesian filter. These settings for Bayesian filtering can be found under MailEnable Management > Servers > Localhost > Filters > MailEnable Bayesian filter > Properties.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>MailEnable Dictionaries are located under Program Files\MailEnable\Dictionaries. MailEnable provides a default dictionary that can be used with the filter. This dictionary is located in Program Files\Dictionary\default and is called MAILENABLE.TAB. For more details please see the MailEnable Default Dictionary section (Section 6.4.3).</td>
</tr>
<tr>
<td>Options (Process HTML content in Messages)</td>
<td>If this option is selected and the message contains HTML, then the HTML is parsed as well as the message plain/text boundary. Tokens will therefore also include data from the HTML messages. It makes the filter more likely to detect HTML as spam because the tokens/patterns of the HTML of bad messages can be used to calculate the probability of spam.</td>
</tr>
<tr>
<td>Spam Calculation method</td>
<td>When a message is split into its tokens/words for analysis each token in the message is given a probability of either being spam or non-spam. As such, MailEnable can be configured to use a number of methods for calculating the final probability of a message being spam</td>
</tr>
</tbody>
</table>

  - **Measure highest and lowest percentiles of the most frequent tokens** - Only those tokens most frequently occurring in the message will be used/aggregated to measure the probability of the message being spam i.e. If this option is used, then messages containing multiple instances of a spam token will most likely be diagnosed as spam.

  - **Measure all tokens in the message** - This means that all tokens occurring in the message will be used/aggregated to calculate the probability of the message being spam. The recommended method to use is: “Measure all tokens in the message” because it provides a more balanced calculation.

  - **Measure tokens within the highest and lowest percentiles** - This means that only those tokens/words in the message that are most likely to denote the message as spam or non-
MailEnable is installed with a default dictionary which is trained with some basic spam and ham emails. While it is a good starting point for auto and manual training, it is not effective in reducing spam, so auto-training and/or manual training would also need to be configured.

6.4.4 Manual training

Manual training of the Bayesian filter involves using scripts and the Spam Training Utility to update the dictionary file with spam and ham. Manual training can occur alongside auto-training and is a good way of adding extra emails that had avoided detection to the dictionary so they can be caught in future.

Similar to auto-training, both spam and ham need to be collected, but the process for doing so varies, as detailed below.

Collecting spam for manual training

Two ways to collect spam for manual training purposes are:

1. Creating a catchall address. Set up a mailbox address (e.g. spam@example.com) as a catchall address. This address will collect all emails for a domain that do not have a mapping to a mailbox. The majority of mail in this mailbox will be spam, as spammers will often send to unknown addresses for a domain. Do not use the same address as one that is being used for auto-training.

2. Using public folders. Set up public folders for post offices for the purpose of collecting spam. IMAP users can drag and drop spam messages from their inbox into the public folder for collection. A script can then be scheduled to copy the content of these folders to a single spam repository folder for addition to the dictionary. For an example script, see the Manual Training section (Section 6.4.4).

Collecting ham for manual training

One way of collecting ham for manual training is to configure a filter that collects mail from senders who have authenticated. To do this, follow this procedure:

- Create a mailbox in the domain called ham@example.com
- Create a global filter called “Ham Collection” with the criteria of “Where the sender has authenticated” and the action “Forward message to ham@example.com”. More advanced criteria can be used to determine which messages to use for training.

The inbox of this mailbox can then be used as a source for ham messages to be used for manual training.

Compiling the dictionary using a script

In order to add emails to a dictionary, the Spam Training Utility is used. This will take spams and hams from two specified folders, process them and add them to the dictionary. Since the emails to add could be located in various public folders and catchall mailboxes, a scheduled DOS script would normally be used to copy the emails from these locations and put into two folders for the Spam Training Utility.

An example script for this is below. This script will also stop and start the MTA service in order to allow it to be used along with auto-training. Since the Spam Training Utility only works on the dictionary on the hard drive, the MTA service needs to be stopped to write out any auto-training additions that have been made.

The script is just an example and would need to be modified to match the MailEnable configuration.

Example Script

REM Copy mail stored by either a catchall account mailbox or filter into two folders,
REM Spam and NoSpam which will be used by the training utility to add to the
MailEnable provides a command line utility that can be used to manage spam/non-spam dictionaries. This program is called MESPAMCMD.EXE and is located in the MailEnable BIN directory.

The spam training utility only works on the files stored on the hard disk. The auto-training feature should be disabled, or the MTA service stopped before any manual update of the dictionary occurs.

```
REM dictionary

copy "C:\Program Files\Mail Enable\Postoffices\example.com\MAILROOT\spam\Inbox\*.mai" "C:\Program Files\Mail Enable\Dictionaries\Custom\Spam\*.*"
del /Q "C:\Program Files\Mail Enable\Postoffices\example.com\MAILROOT\spam\Inbox\*.mai"

copy "C:\Program Files\Mail Enable\Postoffices\example.com\MAILROOT\ham\Inbox\*.mai" "C:\Program Files\Mail Enable\Dictionaries\Custom\NoSpam\*.*"
del /Q "C:\Program Files\Mail Enable\Postoffices\example.com\MAILROOT\ham\Inbox\*.mai"

REM Now the email from Public folders is copied. Normally only junk emails will be REM used when using Public Folders for dictionary training

copy "C:\Program Files\Mail Enable\Postoffices\example.com\PUBROOT\SPAM\*.*" "C:\Program Files\Mail Enable\Dictionaries\Custom\Spam\*.*"

REM Remove the index file and messages from the folder

del /Q "C:\Program Files\Mail Enable\Postoffices\example.com\PUBROOT\SPAM\*.*"
del /Q "C:\Program Files\Mail Enable\Postoffices\example.com\PUBROOT\SPAM\*.xml"

REM Stop the MTA service to write out any auto-training dictionary

net stop MEMTAS

REM Process the messages in the dictionary files and convert them to the dictionary token file.

mespamcmd -m "c:\Program Files\Mail Enable\Dictionaries\default\mailenable.tab" "\Program Files\Mail Enable\Dictionaries\Custom\Spam""c:\ Program Files\Mail Enable\Dictionaries\Custom\NoSpam"

REM Clean up the dictionary spam and ham folders

del /Q "C:\Program Files\Mail Enable\Dictionaries\Custom\Spam\*.MAI"
del /Q "C:\Program Files\Mail Enable\Dictionaries\Custom\NoSpam\*.MAI"

REM start the MTA service

net start MEMTAS
```

### 6.4.5 Spam Training Utility

MailEnable provides a command line utility that can be used to manage spam/non-spam dictionaries. This program is called MESPAMCMD.EXE and is located in the MailEnable BIN directory.

The spam training utility only works on the files stored on the hard disk. The auto-training feature should be disabled, or the MTA service stopped before any manual update of the dictionary occurs.

```
MESPAMCMD -[options] [dictionary, paths]

[c] = Create Dictionary
[v] = Verify messages in the specified folder against the nominated Dictionary
[s] = Score a single message against the nominated Dictionary
```
An example command line for compiling a dictionary based on the example shown follows:

```
MESPAMCMD -c C:\TEST\ME.TAB C:\TEST\SPAM C:\TEST\NOSPAM
```

Using XML or Tab delimited files

Filtering dictionaries can be constructed as either XML or TAB delimited files. XML files are slower to load, but may be more desirable if externally managing the dictionary. Tab files are much more efficient (faster loading), so it is advisable to use the default TAB files. The filter determines whether the file is XML or TAB delimited by the file extension. The format for the XML files is:

```
<ELEMENTS>
  <ENTRIES W="[number of ham emails]" B="[number of spam emails]">
    <E W="[number in ham emails]" B="[number in spam emails]">word</E>
    <E W="[number in ham emails]" B="[number in spam emails]">word</E>
    ...
  </ENTRIES>
</ELEMENTS>
```

Verifying a dictionary

The command line utility can be used to validate a directory of messages against the dictionary. This will provide a percentage probability of spam for each message in the folder.

```
MESPAMCMD -v MailEn-1.TAB C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\Test
```

Scoring a message

Scoring a single message is much like verifying a directory, except the second parameter is a message file rather than a directory.

An example of scoring a message follows:

```
MESPAMCMD -s MailEn-1.TAB C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\Test\1A38DF23D08450B5FF51530A266.MAI
```

Merging a dictionary

Merging a dictionary is much like creating a new dictionary, except that messages in the Spam and NoSpam directories are appended to the dictionary rather than re-creating it. This is useful to add new messages to the dictionary to refine Spam detection.

An example for merging new content with an existing spam dictionary follows:

```
MESPAMCMD -m MailEn-1.TAB C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\Spam C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\NoSpam
```
Reload a dictionary

If changes are made to a dictionary while the spam filter is running, it will not automatically reload it unless it is notified, as the dictionary is held in memory. The dictionary can be reloaded by either restarting the MTA service or using the -r option of the mespamcmd program to tell the spam filter to reload it.

```
MESPAcMD -r
```

Pruning a dictionary

Pruning a directory involves removing any items from the dictionary that will not be able to be used effectively to determine spam or non-spam. This is done by removing items which very rarely occur, and items which occur almost equally in spam and non-spam emails. To prune, provide the path and filename to a dictionary file. After pruning, this file will be overwritten with the new dictionary.

```
MESPAcMD -p MailEn~1.TAB
```

Checking the dictionary

To check the dictionary, open up the DIC.tab file in the following location using Notepad;

```
C:\Program Files\Mail Enable\Dictionaries\DIC.tab
```

To check the integrity of the file make sure the first line shows the number of good and bad messages that have been added into the dictionary. The first number will equal the amount of messages that were in the SPAM folder and the second column equaling the NOSPAM folder. The first number in the line should equal the amount of bad messages (spam) merged into the dictionary the second number should match the good messages (ham). Each number after this first line equals the amount of good and bad words/tokens were found as a total in each message.
7 Scripted Filtering

7.1 Overview

7.1.1 Scripted Filtering

Scripted filtering provides a flexible and extensible means of creating complex filters. The scripting language used is similar to Microsoft VBScript and includes an in-built function for validating criteria. The variable called FilterResult is used as the return value from the filter and can be set at any time in the script. A FilterResult value of 0 indicates that the filter criteria were not met while a value of 1 indicates that the filter criteria were met, and the associated actions for the filter will be executed.

Criteria within scripts can be formed using literal values or tests. Literal values are tokens that are placed in the script and are substituted with their corresponding value. For example, a literal value of [ME_SIZE] can be placed directly in the script for comparison and will be substituted with the message size when the filter is executed. Tests are performed using the CriteriaMet function, and is used for non-numeric values, such as when string comparisons are being made.

7.1.2 Literal values

The following table lists the literal values which can be used in a script.

<table>
<thead>
<tr>
<th>Token</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ME_SPAM_PROBABILITY]</td>
<td>Contains a numeric value of the calculated Bayesian probability of a message being detected as spam.</td>
</tr>
<tr>
<td>[ME_SIZE]</td>
<td>The size of the message in bytes</td>
</tr>
<tr>
<td>[ME_SENDERAUTH]</td>
<td>Indicates whether the sender of the message authenticated in order to dispatch the message to MailEnable. The value is 1 if the sender authenticated, otherwise the value is 0.</td>
</tr>
<tr>
<td>[ME_HASVIRUS]</td>
<td>Indicates whether the message contained a virus. The value is 1 if the message contained a virus, otherwise the value is 0. When a virus is detected by filter criteria it is automatically removed from the message.</td>
</tr>
<tr>
<td>[ME_HASANATTACHMENT]</td>
<td>Indicates whether the message has an attachment. The value is 1 if the message has an attachment, otherwise the value is 0.</td>
</tr>
</tbody>
</table>

Literal enumeration example

If ([ME_SENDERAUTH] = 0) Then
  'sender has not authenticated
End If

Extra literal values are also available for substitution. These are formatted differently because they are not evaluated as the filter is being executed, but read from the command file for the message being processed.

<table>
<thead>
<tr>
<th>Token</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%IPADDRESS%</td>
<td>The TCP/IP address of the originating message</td>
</tr>
<tr>
<td>%POSTOFFICE%</td>
<td>The post office that can reasonably be assigned to the message.</td>
</tr>
<tr>
<td>%SENDER%</td>
<td>The sender of the message in Internal format of [CONNECTOR:Address]. E.g. [SMTP:<a href="mailto:xjz@mailenable.com">xjz@mailenable.com</a>]</td>
</tr>
<tr>
<td>%RECIPIENTS%</td>
<td>The recipient(s) of the message in internal format of [CONNECTOR:Address]; [CONNECTOR:Address2]. E.g. [SMTP:<a href="mailto:xjz@mailenable.com">xjz@mailenable.com</a>],[SMTP:<a href="mailto:def@mailenable.com">def@mailenable.com</a>]</td>
</tr>
<tr>
<td>%SUBJECT%</td>
<td>The subject of the message.</td>
</tr>
</tbody>
</table>
7.1.2.1 Check whether the subject of a message contains the letters ABC

If InStr(1,UpperCase("%SUBJECT%"),"ABC") > 0 then
    FilterResult=1
End If

7.1.2.2 Check if the Subject of the message contains "Re" at the start of it

If Left("%SUBJECT%",2) = "Re" then
    FilterResult=1
End If

7.1.3 Enumerations requiring the CriteriaMet syntax

<table>
<thead>
<tr>
<th>Token</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ME_TO]</td>
<td>The message envelope recipients or the To: denoted in the message headers matches the designated criteria.</td>
</tr>
<tr>
<td>[ME_CC]</td>
<td>The Cc: denoted in the message headers matches the designated criteria.</td>
</tr>
<tr>
<td>[ME_ToorCC]</td>
<td>The message envelope recipients or the To: or Cc: denoted in the message headers matches the designated criteria.</td>
</tr>
<tr>
<td>[ME_FROM]</td>
<td>The message envelope sender or the From: denoted in the message headers matches the designated criteria.</td>
</tr>
<tr>
<td>[ME_HEADERS_CONTAIN]</td>
<td>The message headers contain data matching the designated criteria.</td>
</tr>
<tr>
<td>[ME_SUBJECT]</td>
<td>The message subject contains data matching the designated criteria.</td>
</tr>
<tr>
<td>[ME_PRIORITY]</td>
<td>The priority of the message meets the designated criteria.</td>
</tr>
<tr>
<td>[ME_SPF]</td>
<td>The SPF response string associated with the message meets the designated criteria.</td>
</tr>
<tr>
<td>[ME_HASATTACHMENTSMATCHING]</td>
<td>The message contains an attachment with a file name that meets the designated criteria.</td>
</tr>
<tr>
<td>[ME_BODY]</td>
<td>The body of the message contains text meeting the designated criteria.</td>
</tr>
</tbody>
</table>

Literal Enumeration Example

If (CriteriaMet([ME_SUBJECT], "Viagra")) Then
    'Do Stuff
End If

In cases where literal values return 1 or 0, it is possible to also use literal values with the CriteriaMet function, although there is no real reason to do so. Example: CriteriaMet([ME_SENDERAUTH], 0) is the same as ([ME_SENDERAUTH] = 0) But this is not the case for string values. CriteriaMet([ME_SUBJECT], "Viagra") is not the same as ([ME_SUBJECT] = "Viagra") because string tokens cannot be used in this manner.

7.2 Basic Script Example
An example script for an advanced filter is outlined below:

**Script Example**

```vbc
FilterResult=0
If Hour(Now) > 10 Then
    If [ME_SIZE] > 1024 OR CriteriaMet([ME_BODY],"*123*") AND _
        CriteriaMet([ME_SUBJECT],"*123*") Then
        FilterResult=1
    End If
End If
```

This example script will have its criteria met under the following circumstances. If it is after the 10th hour of the day and the size of the message is greater than 1KB or the Body of the message contains the string 123.

### 7.3 Advanced Script Example

A more complicated example script for a filter is outlined below:

**Advanced Script Example**

```vbc
FilterResult=0
If Hour(Now) > 10 Then
    If [ME_SIZE] > 1024 OR CriteriaMet([ME_BODY],"*123*") AND _
        (CriteriaMet([ME_SUBJECT],"*123*") OR _
        CriteriaMet([ME_SUBJECT],"*456*")) AND _
        CriteriaMet([ME_SIZE],123) Then
        FilterResult=1
    End If
End If
```

This script is similar to the basic one, with the exception of containing more comparisons.

**Note:** In the above example, the `CriteriaMet([ME_SIZE],123)` line actually implicitly means that the message size is greater than 123 bytes.

**Reporting Matching Criteria**

MailEnable logs a return result from filters to the log file or as the [ME_CRITERIA] token replacement for actions. For example, the action to add a header to an email can use the [ME_CRITERIA] token which will be replaced with the string returned from the script. When not using scripting for a filter, this return value is preset and cannot be modified, but when a scripting filter is used the return value can be set within the script. This is done by setting the MEResultData variable within the script.

**Setting the MEResultData variable within a scripted filter**

```vbc
If "%SUBJECT%" = "ABC" Then
    MEResultData = "Subject matched ABC"
    FilterResult=1
Else
    If InStr(1,"%SUBJECT%","FRED") > 0 Then
        MEResultData = "Subject contained Fred"
    End If
End If
```

If not using a scripted filter, then a system-generated string is returned to denote which were the matching criteria. An example string returned when a filter is matching the term 'Viagra' at the beginning of the message subject follows:

```
CRITERIA=SUBJECT, DATA=<MF-W>Vagra*</MF-W>
```

An extract from an example log file is shown below. The filter column will show whether a scripted filter is
This example shows messages A.MAI and B.MAI being processed.

A.MAI was intercepted by a filter called “Scripted” because the scripted filter reported that the subject matched the term ABC.

B.MAI was intercepted by a filter called “Basic” because the Subject of the message matched a criteria string AB*. (Note: the <MF-W> mark-up around the term is used to indicate that the term was sourced from word list criteria).
8 Configuration of Email Clients

8.1 Configuring Email Clients

To read and send email from an email client, (e.g. Eudora, Microsoft Outlook or Outlook Express) requires the client to be configured and connected to MailEnable. The POP3 and SMTP server should be the server name that is running MailEnable. Email clients have to be able to resolve this server name to an IP address.

The username needs to be the full logon name for the mailbox. Remember that this is formatted as mailboxname@postofficename. Email will not be able to be retrieved if the full username is not used, unless a default post office has been specified. See the General configuration section (Section 4.6) for more information on specifying a default post office.

8.2 Netscape Messenger

To configure for Netscape Messenger:

1. Start Netscape
2. Select Edit then Preferences from the menu bar
3. Select the ‘+’ symbol on the right of Mail & Group
4. Select the Mail Server option
5. Enter values in the input boxes
6. To prevent having to re-enter the password every time email is checked, select More Options, then tick Remember mail password
7. Click on Identity
8. Type in the full name or business name in Your Name: input box
9. Type in the email address (e.g. info@mydomain)
10. Type in your reply email address (e.g. info@mydomain)
11. Select OK to accept new settings.

8.3 Microsoft Outlook Express

To configure Microsoft Outlook Express to connect to the mail server:

1. Open Outlook Express
2. Select Tools | Accounts
3. Select the Mail tab
4. On the right hand side, select Properties
5. Select on the Servers tab.

Make sure the POP Logon name is the same as the Account name (username) that is used by mail clients when they connect to the server to retrieve email. E.g.: mailbox@postoffice. If SMTP Authentication is enabled on the server, check the option instructing Outlook Express that the outbound server requires authentication. The checkbox to do this is labeled ‘My server requires authentication’.

8.4 Microsoft Outlook 2000

To configure Microsoft Outlook 2000 to connect to the mail server:

1. Access the Tools | Accounts menu
2. Select the Mail tab and click Add | Mail
3. Enter an appropriate display name, then select the Next button
4. Enter the e-mail address, then select the Next button
5. Specify whether the account being set up is POP3 or IMAP
6. Specify the incoming and outgoing mail servers. e.g. mail.[example].com, then select the Next button
7. Specify the Account Name and Password, (account name is formatted as mailboxname@postofficename) then select the Next button
8. Specify the connection method

8.5 Microsoft Outlook 2002/2003

To configure Microsoft Outlook 2002/2003 to connect to the mail server:
1. Access the Tools | E-mail Accounts menu
2. Select the Add a new e-mail account option and select Next
3. Select either POP3 or IMAP, then select Next
4. Enter the email account settings
5. Specify the incoming and outgoing mail servers. E.g. mail.[example].com
6. Specify the account name and password (account name is formatted as mailboxname@postofficename).

8.6 Microsoft Outlook 2007

To configure Microsoft Outlook 2007 to connect to the mail server:
1. Access the Tools | Account Settings... menu
2. Select the E-mail tab, and click the New... button
3. Select Microsoft Exchange, POP3, IMAP or HTTP, then select Next
4. Select Manually configure server settings or additional server types then select Next
5. Select Internet E-Mail then select Next
6. Enter the email account settings
7. Specify the incoming and outgoing mail servers. E.g. mail.[example].com
8. Specify the account name and password (account name is formatted as mailto:mailboxname@postofficename)postofficename

8.7 Mozilla Thunderbird

To configure for Mozilla Thunderbird:
1. Mozilla Thunderbird can configure the inbound email settings separate from the outgoing mail. To configure the incoming email server:
2. Access the Tools | Account Settings menu
3. Select Add Account
4. Select the Email account option in the Account Wizard window that appears and select Next
5. Enter name and e-mail address and select Next
6. Select whether to use POP or IMAP protocol and enter the incoming email mail servers. E.g. mail.[example].com, then select Next
7. Specify your Incoming User Name and select Next. (User Name is formatted as mailboxname@postofficename)
8. Enter the account name for this account select Next
9. Select Finish
To set the outgoing mail server details:

10. Access the Tools | Account Settings menu.
11. Select the Outgoing Server (SMTP) item in the list box
12. Enter the server name of the outgoing mail server. E.g.: mail.[example].com
13. Enable the username and password checkbox and enter the username (username is formatted as mailboxname@postofficename)
14. For the Use secure connection option, select No
15. Select OK to save changes.

8.8 Configuring clients for HTTPMail

The HTTPMail access protocol is currently only supported with Microsoft based clients. If using Outlook Express, Outlook 2002 or Outlook 2003 as a mail client, select the mail protocol as HTTP and enter in the following details:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>Provider</td>
<td>Other</td>
</tr>
<tr>
<td>Incoming mail (POP3, IMAP or HTTP) server</td>
<td><a href="http://machinename:8080/MEHTTPMail">http://machinename:8080/MEHTTPMail</a></td>
</tr>
</tbody>
</table>

Example

From Outlook (in the example, Outlook Express) choose Tools | Accounts from the Menu.

1. Select Add | Mail... and
2. Enter the Display Name (Friendly Name), then select Next.
3. Enter the e-mail address; then select Next.
4. Select HTTP as the mail server type and enter the URL to the HTTPMail service (http://machinename:8080/MEHTTPMail); then select Next.
5. Enter the MailEnable credentials; then select Next. Note: Since HTTPMail is an authenticated service, use the usual account credentials when prompted. (i.e.: User@ Your Account/Postoffice).
6. The wizard has now completed; please select Next.

The HTTPMail Service has now been configured under Outlook Express. For more information on using Outlook Express, please refer to the Outlook Express Online Help.

8.9 Enabling logging for Microsoft Outlook

Microsoft Outlook Express

It is possible to log mail sessions using the Outlook Express Maintenance option. This option is found under Tools > Options > Maintenance. Once this setting is enabled, the entire session will be logged to a text file. The log files are usually located under Documents and Settings\Local Settings\Application Data\Identities\Guid \Microsoft\Outlook Express folder. This is where all your Outlook Express messages and folders are stored also.

Microsoft Outlook

To enable logging in Outlook, navigate to the following location: Tools > Options > Other > Advanced Options > Enable email logging. This will log the session to a text file in the following path:

C:\Documents and Settings\[user]\Local Settings\Temp\Outlook Logging\[account]
MailEnable has a backup utility which is accessible through the Program Files > Mail Enable > System Tools menu. This utility can pass /BACKUP as a parameter to use it as an automated command line backup utility. There are three main areas where MailEnable stores configuration and user data:

- Registry: Server Configuration (Service Settings, Machine Specific Configuration Information)
- File System: Queues, Post office and Account data, etc.
- Provider Store (File System: \CONFIG Directory or SQL Server Database; depending on provider)

It is simple to backup and restore MailEnable. The most primitive way is to copy everything under the Program Files directory to an alternate location. MailEnable mostly uses flat files for configuration (by design) and therefore all messages and configuration are simple to backup.

The only additional information to (optionally) backup is the information in the registry. The registry hosts server specific information (like connector settings, etc).

To do this requires the registry editor (REGEDIT) to export the HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable registry key (and all sub keys and values) to a reg file. More information on how to use the registry editor is available from Microsoft's Web Site.

To recover the backup, stop all services, replace the directory tree from the backup and then import the saved registry file into the registry.

### 9.2 Debugging

Mail services can be run interactively in debug mode allowing debug messages to be written to the screen. The following instructions outline how to run the services in debug mode:

- Open the regedit application and move to the HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable\Mail Enable\SMTP\Debug Mode Key.
- Set the value of this key to 1. This tells the server to write debug messages to the console rather than to a file.
- Then, run the Windows command prompt and type in the following command: C:\Program Files\Mail Enable\Bin\MESMTPC -debug
- When the debug session is completed, close the console window.
- Ensure that the value of the registry key is set back to 2 when the debug session has finished.

### 9.3 Inspecting log files

Log files are an important aspect of any mail server. Understanding the various log files that MailEnable produces will assist in finding and rectifying any problem. Fortunately, MailEnable can produce a large amount of logging information to help isolate a problem.

By default, MailEnable produces 3 logs for each service. They are called W3C, Activity and Debug logs.

- The W3C log has all the information about what is passing to and from the mail server in W3C extended log file format (www.w3c.org (http://www.w3c.org/)).
- The Activity log will display all the information that is passing to and from the server.
- The Debug log is used to display information about what the service is actually doing.

When experiencing a problem with email, examining the various log files can quickly identify the problem.

### 9.4 Licensing

MailEnable is licensed on a per server basis. In order to avoid any restrictions on the features of MailEnable a license key needs to be applied to the installation. There are two ways to register.
For computers connected to the Internet

When MailEnable is installed, a registration application is made available under the MailEnable program group. This registration application queries the system and submits registration details to the licensing server. The server will need to be connected to the Internet to use this utility to register MailEnable. This utility provides a number of payment mechanisms ranging from online-credit card payments to faxed purchase orders. If registering using online credit card details, MailEnable will immediately acquire a registration key and register it with the server. However, if other payment mechanisms are selected, it simply lodges the registration request with the payment server (assuming that the payment will be reconciled by fax or purchase order). Once MailEnable receives notification of payment mechanism, the license key will be generated and mailed to the nominated e-mail address.

For computers not connected to the Internet

If the server to license is not connected to the Internet, MailEnable can be ordered via MailEnable's web site. Once this has been processed the license key will be generated and sent to the designated e-mail address. The license key must be manually entered into the registration utility (located under the Mail Enable program group on the server).

Registration key retrieval method

Retrieve a new license key by using our online services website at the following address:

http://www.mailenable.com/OnlineServices/default.asp

Here, use the email address that was used for the registration as the login, and the password that was created and emailed out when the product was purchased.

Alternatively, use the Registration Wizard on the new server as described below to get the updated key:

In order to license MailEnable Enterprise, run the Registration Wizard application that was added to the Windows Start menu when the product was installed (under Programs>Mail Enable).

This is to personalize the registration key code.

Internet access is required to request the license key using the Registration Wizard. If you do not have Internet access for the MailEnable server, please email the output from the Diagnostic Utility to sales@mailenable.com as this output contains the information necessary to generate a license code for the server.

When using the Registration Wizard, follow these steps:

1. Select Apply for a Registration Key via the Internet, select Next
2. Enter your details, select Next
3. Select Request License Key, select Next
4. Read the confirmation and select Next
10  System Utilities

10.1 System Tray Utility (METray)

The MailEnable System Tray (METray.exe) utility provides monitoring, reporting and automatic updates for MailEnable.

METray is accessible via an icon in the system tray. Right clicking the icon shows a menu with options as detailed below.

Double clicking the METray icon will bring up the System Overview Screen as shown above.

System overview

The system overview screen provides a diagrammatic representation of the MailEnable system. The operational status of each of the services (POP, IMAP, web mail, HTTPMail) can be seen in the diagram. The polling intervals and length of the inbound and outbound queues of each of the connectors can also be seen in the diagram. Clicking on the inbound and outbound queues in the diagram will produce a window with a list of the current connections, including the client IP address, remote domain, sender etc. POP and IMAP connections can be viewed by clicking on each of these services in the diagram. These connections can also be viewed under “Connections” in the METray menu.

The number of lookups and detections for antivirus scanning, Bayesian filtering, DNS blacklisting and content blacklisting are listed at the top of the System Overview window.

Ticking the box in the bottom right hand corner of the application window shows statistics since the services were restarted.

System summary

System reporting and monitoring can be enabled and disabled from within the System Summary. Tick the box to enable the feature or untick the box to disable the feature and click ‘Apply’. All MailEnable Services will need to be restarted or a reboot is required for these changes to take effect.

The System Summary provides details on the connectors (Post office, List and SMTP) showing polling intervals and queue lengths. These details are also viewable in the System Overview diagram.

Diagnostic Report

Provides a shortcut to generate a diagnostic report for MailEnable (this Diagnostic Report can also be accessed via the Administration Program or MailEnable Program Group).

Updates
Provides an automatically updated list of any major/minor updates or hotfixes that have been released for MailEnable. These updates can be selectively downloaded from the list.

**Connections**

Monitors incoming and outgoing connections for SMTP and shows a list of the current connections including the client IP address, remote domain, sender etc. A similar list of connection details for POP and IMAP services can be viewed also. Connections can also be viewed by clicking on the queues or services in the System Overview diagram.

**10.2 Activity Monitor**

The MailEnable Activity Monitor (MEActivityMonitor) allows MailEnable System Activity to be watched as it occurs. This utility is useful for tracking messages as they pass through the MailEnable system. The tool works by monitoring file I/O to the Activity and Debug logs on the server. Ensure that activity and debug logging are enabled whilst using this utility.

To avoid unnecessary consumption of system resources, this utility should only be run whilst interactively tracking MailEnable system activity.

**10.3 MEInstaller**

The MailEnable Installer (MEInstaller) utility is an application that allows various MailEnable configuration options to be reset without requiring a reinstall of the entire product. The program is located in the MailEnable\bin directory and has the filename MEInstaller.exe. The following tasks can be performed:

**Common Installation**
- Creates the IME_USER Windows user if it does not exist (and adds to Users group)
- Sets the policies for IME_USER
- Creates the IME_ADMIN Windows user if it does not exist (and adds to Users group)
- Sets the policies for IME_ADMIN
- Sets the permissions on the Mail Enable directories for IME_ADMIN
- Sets the permission on required system files for IME_ADMIN and IME_USER

**Web Mail Installation**
- Creates the IME_USER Windows user if it does not exist (and adds to Users group)
- Sets the policies for IME_USER
- Resets the password for IME_USER to the entered one
- Creates the IME_ADMIN Windows user if it does not exist (and adds to Users group)
- Sets the policies for IME_ADMIN
- Resets the password for IME_ADMIN to the entered one
- Creates the Mail Enable package in COM+/MTS under the IME_ADMIN account
- Resets the package identity of Mail Enable Administration to IME_ADMIN
- Creates the MEWebmail virtual directory under the selected IIS site
- Sets the permissions on the Mail Enable bin directory for IME_ADMIN
- Sets the permissions on the Mail Enable web mail directory for IME_ADMIN & IME_USER
- Resets all MEWebmail virtual directories to use the new password
- Resets all the MEAdmin virtual directories to use the new password
- Sets default document and session state for selected website

**WebAdmin Installation**
• Creates the IME_USER Windows user if it does not exist (and adds to Users group)
• Sets the policies for IME_USER
• Resets the password for IME_USER to the entered one
• Creates the IME_ADMIN Windows user if it does not exist (and adds to Users group)
• Sets the policies for IME_ADMIN
• Resets the password for IME_ADMIN to the entered one
• Creates the Mail Enable Administration package in COM+/MTS under the IME_ADMIN account
• Resets the package identity of Mail Enable to IME_ADMIN
• Creates the MEAdmin virtual directory under the selected IIS site
• Sets the permissions on the Mail Enable Web Mail directory for IME_ADMIN & IME_USER
• Resets all MEWebmail virtual directories to use the new password
• Resets all the MEAdmin virtual directories to use the new password
• Sets default document and session state for selected website

Re-Register MMC Components
• Reregisters the MailEnable administration MMC DLLs

Set IIS Application Isolation Levels (Low > In Process)
• Sets the MEAdmin and MEWebmail virtual directories application level to be low

Set IIS Application Isolation Levels (Medium > Pooled)
• Sets the MEAdmin and MEWebmail virtual directories application level to be medium

Set IIS Application Isolation Levels (High > Isolated)
• Sets the MEAdmin and MEWebmail virtual directories application level to be high

Clear System Blocking Files
• Removes all the blocking files from the Mail Enable\Config directory

Repair Configuration Files (Hosting Controller User’s Only)
• Resolves an issue with a specific version of Hosting Controller altering the configuration files.

Apply/Remove Strict Server Security Policy
• Configures the MailEnable services to run under a restricted Windows user, to give a higher level of security on the server.

Apply Registry Permissions for IME_ADMIN, IME_USER and IME_SYSTEM
• For webmail and when the strict server policy is applied, the mail services run under various Windows users. This step sets registry permissions required for this.

Reset IIS Virtual Directory Configuration settings for ASP/ASPX Platform
• Resets all the MailEnable webmail and web admin virtual directories to use a specific version of the .Net platform.

10.4 Command Line Send Utility (MESend)

MailEnable Command Line Send Utility is available in the MailEnable BIN directory (MeSend.exe). This utility
allows you to send email via SMTP.

Syntax

 MESend /H:{Mail Host} /F:{From Address} /T:{To Address} /S:{Subject} /A:{Attachment Local FilePath} /N: [Attachment Display Name] /B:{Message Body}

Example

 MESend /F:User@mailenable.com /T:User@mailenable.com /S:Message Subject Line /A:C:\test.txt /N:test.txt /B:Message Body /H:127.0.0.1

Note: At least one recipient must be supplied.

10.5 Message Tracking

The message routing trace utility provides an interface to track messages through MailEnable. It is a useful tool to determine whether a message was accepted by the server and as to where it was directed to.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector (mandatory)</td>
<td>From the drop down box, select the connector to trace the original message from.</td>
</tr>
<tr>
<td>Date (mandatory)</td>
<td>Date is formatted in YYMMDD format (e.g. 5th September 2006 = 060905)</td>
</tr>
<tr>
<td>Sender (optional)</td>
<td>Enter the sender’s email address</td>
</tr>
<tr>
<td>Recipient (optional)</td>
<td>Enter the recipient’s email address</td>
</tr>
</tbody>
</table>

After filling in these fields and selecting ‘Search’, a list of messages matching the criteria specified will be displayed. By selecting the Date/Time, Message ID or Data column headings, it is possible to sort the columns.

10.6 Directory Management Utility

The Directory Management utility provides a simple interface for adding, editing and managing global contacts for a post office.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current directory</td>
<td>Select the directory to edit from the drop down box.</td>
</tr>
<tr>
<td>Add directory entry</td>
<td>Create a directory entry for the selected directory. Includes details such as first name, surname, street address, work telephone, company, department etc.</td>
</tr>
<tr>
<td>Edit directory entry</td>
<td>Edits the selected directory entry.</td>
</tr>
<tr>
<td>Remove directory entry</td>
<td>Removes the selected directory entry.</td>
</tr>
<tr>
<td>Import from address map</td>
<td>Imports email addresses from the post office address map into the post office directory.</td>
</tr>
</tbody>
</table>

10.7 Backup utility

The Backup utility allows for both backup and restore of MailEnable to local disk. The backup utility is a basic tool that copies the configuration data and email data to another location in case of server failure. It will not back up the configuration data if MailEnable is configured to use MySQL or Microsoft SQL Server for configuration storage. It is recommended that you include the MailEnable directories as part of the normal
server backup processes you should have in place. Since the email data is stored in plain text files, there is no special process to follow and they can be handled like any other files.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>To backup MailEnable, select a descriptive name for the backup and select “Backup”.</td>
</tr>
<tr>
<td>Restore</td>
<td>To restore an existing backup, select the backup set name from the drop down box and select “Restore”.</td>
</tr>
<tr>
<td>Calculate size</td>
<td>Calculates the maximum storage size required in the backup location to successfully backup the complete configuration.</td>
</tr>
</tbody>
</table>

10.8 Queue overview

The Queue overview lists the number of messages in the outbound SMTP queue by the destination domain name.
11 Appendix

11.1 Antivirus Configuration

11.1.1 Using your own antivirus scanner

If antivirus support is enabled, attachments in messages are unpacked and scanned as they pass through the Mail Transfer Agent. The MTA moves mail messages internally within MailEnable. When the MTA picks up a message from a connector’s queue, it unpacks it into a scratch directory and uses the command line specified in the administration program to scan each unpacked file. In most cases, command line virus checkers have the ability to automatically delete files. If one of the scanned attachments of the message is deleted, the Antivirus filter assumes that it has a virus and when the message is reconstructed, it replaces the offending content with a note indicating that offending content was removed. MailEnable can also check the return code from a command line scanner in order to determine whether the item it processed is infected.

For example, a sample argument line for a command line scanner is:

"[AGENT]" "[FILENAME]" -remove -s -nb -nc

This can be seen if you open the registry and access HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable\Mail Enable\Agents\MTA\Filters\[Virus Scanner Short Name].

Note that the [AGENT] and [FILENAME] tokens in this registry setting are replaced by the path to the A/V Command Line Scanner and the attachment name (which is generated by the system). The "-remove -s -nb -nc" part of this registry value is the part that will vary depending on the scanner application being used.

Ensuring that the A/V app supports auto deletion is a little limiting. As a result there are registry settings that allow the use of the scanners DOS error level or exit code.

The respective settings are:

"Exit Code Enabled": 0/1 - on/off
"Exit Codes": eg: 1 2 9: space delimited string containing application exit codes
"Exit Codes Error Inclusive": 0/1 - on/off: used to configure whether the "Exit Codes" indicate errors or successes

A sample registry import file is outlined below:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable\Mail Enable\Agents\MTA\Filters\Custom]
"Status"=dword:00000000
"Antivirus Notification Message"=">
"Antivirus Scratch Directory"="C:\Program Files\Mail Enable\Scratch"
"Antivirus Parameters"="\"[AGENT]\" \"[FILENAME]\" -s -nb -nc"
"Antivirus Agent"="C:\Program Files\Virus Scanner\CUSTOM.EXE"
"Provider DLL"="MEAVGEN.DLL"
"Program Name"="Custom"
"Program Info"="This is a template for new virus scanners."
"Exit Code Enabled"=dword:00000000
"Exit Codes Error Inclusive"=dword:00000001
"Exit Codes"=1

This can be copied into Notepad, saved as a .reg file and imported using the registry editor. Once imported into the registry, the settings can be edited to those required by the antivirus command line application.
11.1.2 Selecting an antivirus application

MailEnable Enterprise Edition provides an antivirus plug-in that will allow scanning of mail messages for viruses as they pass through the Mail Transfer Agent. The following overviews are provided to assist in selecting an antivirus application.

**F-Prot**

Company: Frisk International
Configuration Guidelines: MailEnable Knowledge Base
[http://www.mailenable.com/kb/Content/Article.asp?ID=me020284](http://www.mailenable.com/kb/Content/Article.asp?ID=me020284)

**Sophos**

Company: Sophos
Configuration Guidelines: MailEnable Knowledge Base
[http://www.mailenable.com/kb/Content/Article.asp?ID=me020288](http://www.mailenable.com/kb/Content/Article.asp?ID=me020288)

**Norman Antivirus**

Company: Norman
Product Name: Norman Virus Control (NVC)
Configuration Guidelines: MailEnable Knowledge Base
[http://www.mailenable.com/kb/Content/Article.asp?ID=me020290](http://www.mailenable.com/kb/Content/Article.asp?ID=me020290)

**Panda**

Company: Panda Software
Configuration Guidelines: MailEnable Knowledge Base
[http://www.mailenable.com/kb/Content/Article.asp?ID=me020289](http://www.mailenable.com/kb/Content/Article.asp?ID=me020289)

**Symantec Norton Antivirus**

Company: Symantec
Configuration Guidelines: MailEnable Knowledge Base
[http://www.mailenable.com/kb/Content/Article.asp?ID=me020086](http://www.mailenable.com/kb/Content/Article.asp?ID=me020086) (versions 6 and 7)

**McAfee Virus Scan**

Company: McAfee
Configuration Guidelines: MailEnable Knowledge Base
[http://www.mailenable.com/kb/Content/Article.asp?ID=me020287](http://www.mailenable.com/kb/Content/Article.asp?ID=me020287)

**Grisoft AVG**

Company: Grisoft
11.1.3 Real time protection

Some antivirus agents cannot exclude directories or file types from their real time protector. Problems may occur if real-time virus protectors are not prevented from monitoring and protecting critical MailEnable directories. Depending on what the server is being used for, it may be better disable real time protectors because they drastically inhibit disk IO. An option is to schedule scans rather than using the real-time protector. The following table outlines the current features of leading antivirus manufacturers with respect to configuring real-time virus protection/IO monitoring.

<table>
<thead>
<tr>
<th>Vendor/Product</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norton Antivirus Corporate Edition</td>
<td>Can exclude directories and file types.</td>
</tr>
<tr>
<td>McAfee Virus Scan</td>
<td>Can exclude directories and file types.</td>
</tr>
<tr>
<td>Panda</td>
<td>Can exclude specific folders.</td>
</tr>
<tr>
<td>AVG</td>
<td>No ability to exclude directories or file types.</td>
</tr>
<tr>
<td>Norman</td>
<td>Can exclude directories and file types.</td>
</tr>
<tr>
<td>F-Prot</td>
<td>No ability to exclude directories or file types.</td>
</tr>
</tbody>
</table>

**Note:** Any errors or omissions in the above are unintentional. For accurate and up to date information it is recommended to consult the manual or web site of the respective antivirus software package. Whilst MailEnable provides a means for you to integrate Antivirus software, you should always check the licensing agreement supplied with the Antivirus software to determine any licensing constraints.

11.2 Overview of NTLM authentication

When MailEnable is configured to provide NTLM authentication, mail users with Outlook or Outlook Express will be able to select the option to use Secure Password Authentication when authenticating against the MailEnable Server. This provides a higher level of password encryption when clients authenticate.

NTLM is an authentication protocol used primarily by Microsoft applications to securely authenticate over a network. MailEnable provides NTLM support for the IMAP, POP, and SMTP, allowing NTLM capable mail clients to securely negotiate credentials when authenticating.

Microsoft Outlook and Outlook Express refer to the NTLM protocol as “Secure Password Authentication”. Generally speaking, unless the backend mail server can negotiate NTLM authentication, it is not possible to use the Secure Password Authentication feature of the mail client.

When the Secure Password Authentication feature is enabled within the mail client, the mail client will encrypt and send the currently logged in Windows username to the MailEnable server. The MailEnable server then looks up the user and verifies that they exist, and assuming so, will send down an encrypted password hash that can be used by the client to validate the password for that user.

This authentication mechanism, is well suited in environments where single sign-on is required or desirable. Using NTLM, once the user has logged in to Windows, they do not necessarily need to specify or configure the mail client with a designated username or password.

If the username of the currently logged in user cannot be validated against MailEnable, most mail clients will then use any credentials that have been associated with the account.

NTLM can be enabled/disabled at a service level. There are no other parameters that need to be configured other than whether it is enabled for the service or not.

11.2.1

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>

111
Configuring NTLM on the mail client

The Secure Password Authentication (SPA) feature in Outlook/Outlook Express is found under Tools > Accounts menu option when either creating or editing an email account.

Enable NTLM

If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled use this secure authentication. E.g. in Outlook the feature is called SPA - Secure Password Authentication.

11.3 DNS error codes and descriptions

The following table lists typical WIN32 DNS return codes. These return codes may appear in the SMTP Debug log file if the DNS is either incorrectly configured or there are DNS Errors being returned from the DNS Server.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9001</td>
<td>DNS server unable to interpret format.</td>
</tr>
<tr>
<td>9002</td>
<td>DNS server failure.</td>
</tr>
<tr>
<td>9003</td>
<td>DNS name does not exist.</td>
</tr>
<tr>
<td>9004</td>
<td>DNS request not supported by name server.</td>
</tr>
<tr>
<td>9005</td>
<td>DNS operation refused.</td>
</tr>
<tr>
<td>9006</td>
<td>DNS name that should not exist, does exist.</td>
</tr>
<tr>
<td>9007</td>
<td>DNS RR set that ought not to exist, does exist.</td>
</tr>
<tr>
<td>9008</td>
<td>DNS RR set that ought to exist, does not exist.</td>
</tr>
<tr>
<td>9009</td>
<td>DNS server not authoritative for zone.</td>
</tr>
<tr>
<td>9010</td>
<td>DNS name in update or prereq is not in zone.</td>
</tr>
<tr>
<td>9016</td>
<td>DNS signature failed to verify.</td>
</tr>
<tr>
<td>9017</td>
<td>DNS bad key.</td>
</tr>
<tr>
<td>9018</td>
<td>DNS signature validity expired.</td>
</tr>
</tbody>
</table>
Listed below is common Outlook/Outlook Express error codes that may be returned when attempting to send, receive or access mail.

Many ISP's block outbound SMTP traffic to ensure that spammers do not abuse their service. It is possible to validate whether mail can be sent to remote hosts by using the telnet utility. Instructions follow:

1. From the Windows Start Menu select **Start|Run** and enter **CMD** as the application to run. Select **OK**

At the command prompt, enter the following:

`telnet mail.mailenable.com 25`

The remote mail server should respond with an initiation string much like the following:

`220 mailenable.com ESMTP MailEnable Service, Version: --4.1 ready at 08/28/09 14:04:45`

Type the word **QUIT** and then press enter.

If this was successful, then no firewall (either local or the ISPs) is preventing outbound SMTP traffic. The next procedure to try is sending an actual message to the remote host (rather than just determining whether it is possible to connect). Firstly, determine which remote server to connect to. A domain may

### 11.4 Diagnosing Outlook/Outlook Express error codes

<table>
<thead>
<tr>
<th>Error</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x800CCCF4</td>
<td>HTTPMail</td>
<td>Outlook settings may be invalid or a firewall is preventing connection to the remote MailEnable Server.</td>
</tr>
<tr>
<td>0x800CCC79</td>
<td>SMTP</td>
<td>SMTP Relay settings are preventing the sending of messages to MailEnable. Ensure that SMTP Authentication is enabled.</td>
</tr>
<tr>
<td>0x80042109</td>
<td>SMTP</td>
<td>Outlook is unable to connect to the outgoing (SMTP) e-mail server.</td>
</tr>
<tr>
<td>0x8004210A</td>
<td>POP</td>
<td>The operation timed out waiting for a response from the receiving (POP) server. Establish whether it is possible to telnet to port 110 of the mail server.</td>
</tr>
<tr>
<td>0x8004210B</td>
<td>POP</td>
<td>The mail client is unable to contact the MailEnable Server, most likely because a firewall is preventing access or the supplied IP Address is incorrect.</td>
</tr>
<tr>
<td>0x8004210D</td>
<td>POP</td>
<td>Verify that the service pack for Microsoft Office XP is installed.</td>
</tr>
<tr>
<td>0x8004210E</td>
<td>POP</td>
<td>Verify the mail client is configured correctly. Either specify an IP address or a host name as the mail server when configuring the mail client settings. If using a host name then it must be defined in the DNS as a Host record.</td>
</tr>
<tr>
<td>0x800CC0E</td>
<td>SMTP</td>
<td>This error means that the mail client is connecting to the server via POP, but the SMTP Service is either not running or is configured incorrectly. Verify if the SMTP service is running by using the telnet utility to telnet to port 25 of the mail server. If the server responds, then the issue is most likely that mail client settings are invalid.</td>
</tr>
</tbody>
</table>

### 11.5 Manually testing if MailEnable can send mail to remote servers

Many ISP's block outbound SMTP traffic to ensure that spammers do not abuse their service. It is possible to validate whether mail can be sent to remote hosts by using the telnet utility.

Instructions follow:

1. From the Windows Start Menu select **Start|Run** and enter **CMD** as the application to run. Select **OK**

At the command prompt, enter the following:

`telnet mail.mailenable.com 25`

The remote mail server should respond with an initiation string much like the following:

`220 mailenable.com ESMTP MailEnable Service, Version: --4.1 ready at 08/28/09 14:04:45`

Type the word **QUIT** and then press enter.

If this was successful, then no firewall (either local or the ISPs) is preventing outbound SMTP traffic.
have more than one server that is accepting email, and these servers may not match the domain name. The MX records that have been configured in a DNS determine the mail servers for a domain. To retrieve the mail server details for a domain, use the nslookup command line utility. For example, to check which servers are accepting email for AOL, you can enter:

```
nslookup -type=MX aol.com
```

This will return the details of the mail servers, these results can be used as the hosts to connect to. This is outlined as follows:

1. From the Windows Start Menu select Start|Run and enter CMD as the application to run. Select OK.
2. At the command prompt, enter the following: `telnet mail.mailenable.com 25`
   
   The remote mail server should respond with an initiation string much like the following:
   `220 mailenable.com ESMTP MailEnable Service, Version: --4.1 ready at 08/28/09 14:04:45`
3. Type the following and press Enter: `HELO YourDomainName`
   
   The server should reply with a line similar to:
   `250 Requested mail action okay, completed`
4. Type the following and press Enter. `Senderaddress` is the email address you are sending from:
   `MAIL FROM:<senderaddress>`
   
   The server should reply with a line similar to:
   `250 Requested mail action okay, completed`
5. Type the following and press Enter. `Recipientaddress` is the email address you are sending to:
   `RCPT TO:<recipientaddress>`
   
   The server should reply with a line similar to:
   `250 Requested mail action okay, completed`
6. Type the following and press Enter. `Recipientaddress` is the email address you are sending to:
   `MAIL FROM:<senderaddress>`
   
   The server should reply with a line similar to:
   `250 Requested mail action okay, completed`
7. Now indicate to the server that you want to send the email date. Type the following and press Enter:
   `DATA`
   
   The server should reply with something like
   `354 Start mail input; end with <CRLF>.<CRLF>`
8. Enter the text of an email as follows (Note: `[CRLF]` = Enter Key). The period character on the last line indicates that all the email content has been sent:
   `Subject: Test Message[CRLF][CRLF]`
9. Type the following and press Enter:
   `QUIT`

If this was successful, then MailEnable should be able to send messages to the remote host. If an abnormal response is received for any of the commands typed in, then search the MailEnable Knowledge Base for any articles that may give an indication of the cause of the error.

**11.5.1 Example**

```
C:\>telnet mail.mailenable.com 25
220 mailenable.com ESMTP MailEnable Service, Version: --4.1 ready at 08/20/09 23:49:40
EHLO test.mydomain.com.au
250 mailenable.com [192.168.1.1], this server offers 4 extensions
```
250-AUTH LOGIN CRAM-MD5
250-SIZE 10120000
250-HELP
250 AUTH=LOGIN
MAIL FROM:<senderaddress>
250 Requested mail action okay, completed
RCPT TO:<recipientaddress>
250 Requested mail action okay, completed
DATA
354 Start mail input; end with [CRLF][CRLF]
Subject: Test Message
250 Requested mail action okay, completed
QUIT
221 Service closing transmission channel
Connection to host lost.

11.6 Log analyser

The log analyser is a useful tool that is installed with MailEnable. It simplifies analysis of the server logs and provides an overview of any errors and displays causes and fixes for these. The log analyser retrieves the latest help information from the MailEnable website.

Run the log analyzer by accessing the Start > Program Files > Mail Enable > System Tools > Log Analyzer menu. The various log files in the log path are displayed to the left. To view events in a log, click the filename. The program will scan the file for all the events and display these in the top right section. Select the item for more information concerning the event, along with a display of the instance in the log. Select the More Information button to be taken to the MailEnable website for further details.

To match up the item in the debug log with the actual data conversation between the MailEnable server and the remote application, select the instance item. It may take a few moments to scan through the activity log to find the match, depending on how large the log files are.

Some errors will always be seen if the server is connected to the Internet. People will try to relay through the server, timeout and connection issues can occur, and users can mistype email addresses when sending messages, which will all display in the logs. The number of errors that occur in the debug log is show in the square brackets in the box labeled Significant Event Instances. This gives a good indication of the severity of the event.
11.7 Configuring redundant or backup (MX) mail servers

There are two principal ways to configure redundancy with MailEnable.

The simplest way to achieve redundancy is to install a copy of MailEnable as the master server. Then install separate copies of MailEnable on other servers and smart host the domains to the IP address of the master server. This will mean that if the master server is down, that the auxiliary servers will accept mail for the domains and hold it until it is online.

The DNS/MX settings for the domains will need to be changed in order to configure the appropriate MX preferences. Other mail servers learn about your mail server via DNS MX records. They are the means by which someone enumerates a target domain to the server responsible for receiving mail for that domain. MX records have a preference associated with them that determines the order in which they are used.

The lowest preference is attempted first. The lower the preference value, the higher the priority. Hence an MX record with a preference of 1 would be attempted before an MX entry with a preference of 10. More info on DNS and MX records is available at: http://www.mailenable.com/kb/viewarticle.asp?aid=19

The above-mentioned approach is used if the backup mail servers are distributed in different geographic or logical locations.

A second alternative is to host all of the mail servers on the same local network and cluster the servers. This allows MailEnable to be installed on multiple servers and have them all use the same store for their messages and post office data. Any of these servers can then be used to access the mail. This requires that one of the servers share the mail data and configuration directories and that the others access them.

11.8 Increasing upload limit for Windows 2003

Internet Information Server (IIS 6) may restrict the maximum size of an upload to 200 kilobytes. If a user is accessing web mail and tries to upload a file over this size, they may receive the error 'The attachment could not be added to the message' when uploading files under Windows. The additional error string reported is:

File save failed for the following reason: C:\Program Files\Mail Enable\POSTOFFICES\MAILROOT\Drafts\ is an invalid path

The following error may also display:

Error MEUP001
The ASP Session expired during the upload.

Reason
IIS6.0/Windows uses a setting called 'AspMaxRequestEntityAllowed' to specify the maximum number of bytes allowed in the body of an ASP request. File uploads typically contain more data than the 200K allowed by the default setting, and therefore this value needs to be updated to a higher value.

Solution
Instructions for resolving this issue follow:

1. Stop the World Wide Web Publishing Service. This can be done from the Windows Command Prompt as:
   net stop w3svc
2. In the C:\Windows\System32\inetsrv directory, locate a file called metabase.XML.
3. Copy the original file in notepad and find the line "AspMaxRequestEntityAllowed".
4. Change the value of this entry to “1073741824”. (Specifies a maximum post size of 1 GB)
5. Save the file.
6. Start the World Wide Web Publishing Service. This can be done from the Windows Command Prompt as:
   net start w3svc

Note: If the Metabase.XML file is locked, try starting Windows in Safe-mode to be able to change that file.
The diagram below outlines the core functionality of MailEnable and how its respective modules (Connectors, Services and Agents) interact. For simplicity, the diagram does not outline the functions of the POP retrieval Connector or List Server Connector.

The following diagram provides a high level overview the POP Connector:
The List server connector is responsible for dispatching messages to large lists of mail addresses. The list server connector will allow members to subscribe to a list, enforce publishing rules for the list, add headers and footers to messages published via the list, etc.
13 Warranty

You should carefully read the following terms and conditions before using this software. Unless you have a different license agreement signed by the respective owners, authors and copyright holders of the MailEnable product suite, herewith referred to as ("ME"), your use, distribution, or installation of this copy of MailEnable indicates your acceptance of this License.

All rights of any kind in MailEnable which are not expressly granted in this License are entirely and exclusively reserved to and by "ME". You may not rent, lease, modify, reverse engineer, translate, decompile and disassemble MailEnable without the permission of its owners, authors and copyright holders of MailEnable.

You are not permitted to commercialize derivative works of MailEnable without a written agreement signed by the respective owners, authors and copyright holders of MailEnable.

All accompanying files, data and materials, are distributed "as is" and with no warranties of any kind, whether express or implied.

This disclaimer of warranty constitutes an essential part of the agreement. Any liability of "ME" will be limited exclusively to refund of purchase price. In no event shall "ME", including but not limited to its principals, shareholders, officers, employees, affiliates, contractors, subsidiaries, or parent organizations, be liable for any incidental, consequential, or punitive damages whatsoever relating to the use of MailEnable, or your relationship with "ME".

In addition, in no event does "ME" authorize you to use MailEnable in applications or systems where "ME"s failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use by you is entirely at your own risk, and you agree to hold "ME" harmless from any claims or losses relating to such unauthorized use.

You are specifically prohibited from charging, or requesting donations, for any copies, however made, and from distributing such copies with other products of any kind, commercial or otherwise, without prior written permission from "ME". "ME" reserves the right to revoke the above distribution rights at any time, for any or no reason.
Index

Accessing web administration, 70-71
Actions, 30
Activity Monitor, 105
Addresses, 28-29
Administration, 9-10, 20
Advanced, 52-53
Advanced Script Example, 97-98
Advertising and Campaign Management, 38
Archiving, 77
Authentication settings, 23-24
Backing up and restoring data, 102
Backup utility, 107-108
Basic Script Example, 96-97
Bayesian filter general settings, 90-91
Browser compatibility, 66-67
Check and configure DNS settings, 18-19
Command Line Send Utility (MESend), 106-107
Configuration, 60-61
Configuration repository location, 15
Configuring clients for HTTPMail, 101
Configuring Email Clients, 99
Configuring redundant or backup (MX) mail servers, 115-116
Configuring the antivirus filter, 87-88
Configuring the server, 73
Configuring web mail Overview, 65
Create a group, 32-33
Create domain, 25-27
Create mailbox, 27
Create mailbox - General, 27-28
Creating a Global Filter, 79
Debugging, 102
Delete messages, 32
Diagnosing Outlook/Outlook Express error codes, 113
Directory Management Utility, 107
DKIM, 76-77
DNS error codes and descriptions, 112-113
Edit default message, 32
Email Delivery Flow, 10-11
Email users (all), 32
Email users (individual), 32
Enabling logging for Microsoft Outlook, 101
Enumerations requiring the CriteriaMet syntax, 96
Examples, 75-76
Export users, 31
File Storage, 67-68
Filter actions, 83-85
Footers, 35
General configuration, 36-37, 37
Global Message Filter Properties, 78-79
Global Message Filters, 78
Headers, 35
How Internet Email Works, 2
How to implement antivirus filtering, 85-87
HTTPMail Protocol, 59-60
IMAP - General, 58-59
IMAP Service, 57-58
Import users, 31-32
Import Windows users, 31
Importing list members, 35
Inbound, 40-41
Increasing upload limit for Windows 2003, 116
Inspecting log files, 102
Installation, 12-15
Installation Overview, 12
Introduction, 1
Licensing, 102-103
List commands, 35-36
List Server Connector, 54-55
Lists, 33
Lists - General, 33-34
Literal values, 95-96
Log analyser, 115
Logging, 53, 57, 59, 64
Logical architecture and message flow, 116-118
MailEnable Default Dictionary, 91
MailEnable Diagnostic Utility, 16-18
Manual training, 91-92
Manually testing if MailEnable can send mail to remote servers, 113-115
MEInstaller, 105-106
Message Tracking, 107
Messages, 30, 36
Messaging Manager, 20-21
Messaging Manager - General settings, 21
Microsoft Outlook 2000, 99-100
Microsoft Outlook 2002/2003, 100
Microsoft Outlook 2007, 100
Microsoft Outlook Express, 99
Mozilla Thunderbird, 100-101
MTA Overview, 61
MTA properties, 61-62
Netscape Messenger, 99
Option Files, 37-38
Options, 34-35
Outbound, 41
Overview, 8
Overview of NTLM authentication, 111-112
POP - General, 51-52
POP Retrieval, 30-31
POP Retrieval Connector, 53-54
POP service, 50-51
Post office actions, 25
Post office configuration, 22, 22-23
Post office connector, 55-56
Post office connector - General, 56-57
Prerequisites, 1-2
Publishing web mail through host headers, 65
Publishing web mail through virtual directories, 65-66
Queue overview, 108
Real time protection, 111
Redirection, 29-30
Relay, 41-42
Replace configuration files, 15-16
Restrictions, 24
Scripted Filtering, 95
Security and authentication settings, 21-22
Selecting an antivirus application, 109-111
Set quotas, 32
Setting up auto-training Bayesian filtering, 88
SMTP - Advanced, 43-44
SMTP - Blocked addresses, 45
SMTP - Delivery, 44-45