MailEnable Professional Edition Configuration Guide Version 2.0

MailEnable Messaging Services
for Microsoft Windows NT/2000/2003

MailEnable Pty. Ltd.
486 Neerim Road
Murrumbeena
VIC 3163
Australia
t: +61 3 9569 0772
f: +61 3 9530 4066
www.mailenable.com

Date last modified 14/12/2005 6:02 PM

Table of Contents

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.

1 Introduction to MailEnable Professional

1.1 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 worlds largest Internet/Application Service Providers, Educational Institutions, Organizations, Government Agencies and Corporates.

486 Neerim Road
Murrumbeena, 3163
Victoria, Australia
Tel: +613 9563-4177 (AEST)
Fax: +613 9530-4066
Email: info@mailenable.com

1.1.1 Support Contact

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

1.1.1.1 MailEnable Web Site

MailEnable's web site provides links to reference materials, product information, knowledgebase, forums, etc.

1.1.1.2 MailEnable Knowledge Base

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

1.1.1.3 MailEnable Forums

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

1.2 How to Download MailEnable Professional

If you have not already done so, the following section will outline how to download the latest supported MailEnable Professional Edition.

To download follow the link below and you will be taken to the MailEnable Website download page where you will find the download location for all MailEnable versions.

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

As a registered user this link is a key location for all upgrades, which are free of charge for 6 months from first licensed installation. Stored here are any patches and hot fixes deemed necessary for the continual use of the MailEnable product.

1.3 MailEnable Pre-requisite Hardware

MailEnable will run on virtually any computer capable of running Windows NT, 2000/2003 or .NET Operating Systems.

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.

1.4 MailEnable Pre-requisite Software

For Windows NT 4:

- Service Pack 6a
- IIS/Windows NT Option Pack 4 (Please refer to note below)
- Microsoft Transaction Server, IIS
- For Windows 2000/2003:
- IIS (Please refer to note below) versions

Note: In order to install either the Web Administration or Web Mail components of MailEnable, you will need to have Microsoft Internet Information Server (IIS) installed. If you do not intend to use these components, then IIS is not a requirement.

If you are using NT4, you should ensure IIS is installed from the Windows NT Option Pack.

If you are installing MailEnable on Windows 2000/2003, IIS is included with the default package.

2 How Internet Email Works

If you are administering a mail server on the Internet you need to understand how email works. It is important to know how messages are delivered and sent, how servers know how to send to you and how your clients retrieve their email. This will help you 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 knowledge if you wish to properly administer an Internet mail server.

2.1 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

- Pegasus Mail,
- Outlook and
- Outlook Express.
- Mozilla Thunderbird

2.2 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.

2.3 Sending and Receiving Mail

To send Internet e-mail, you need 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 (usually a few days), the message will be returned to the sender as undelivered.

3 MailEnable Overview

MailEnable has a variety of 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.

3.1 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.

Component	Definition
Connectors	Connectors move mail between systems or subsystems (local or remote)
Agents	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.
Services	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 postoffice.

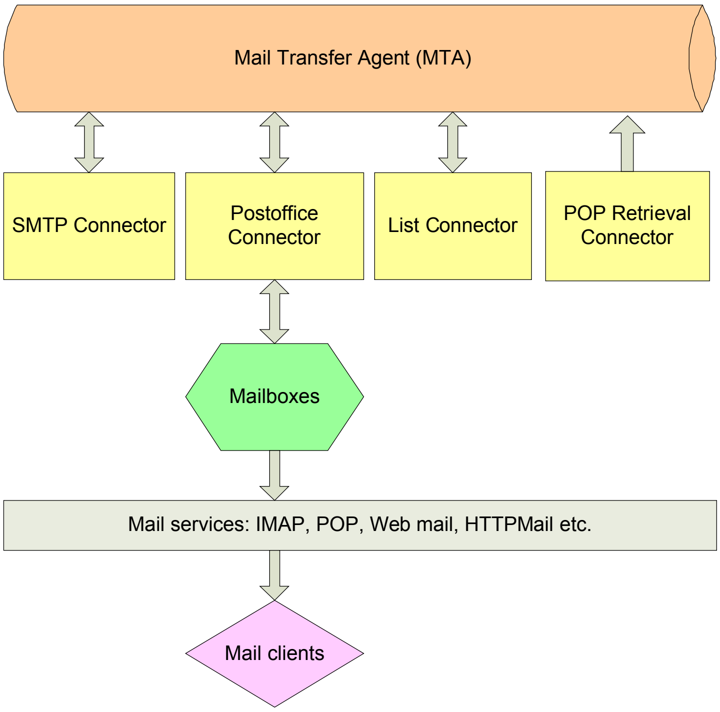


Figure 3-1 Relationship between Agents, Connectors and Mail Services in MailEnable

3.1.1 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 :

- POP3

- IMAP4
- HTTPMail
- Web mail

Each of these mail services is described in more detail in Chapter 8.

3.1.2 Connectors

Mail connectors move mail between systems or subsystems (local or remote). A mail connector allows MailEnable to send a receive mail messages to external systems. MailEnable has several mail connectors: SMTP, POP Retreival, Postoffice and List Connectors.

3.1.2.1 SMTP Connector

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

3.1.2.2 Postoffice connector

The Postoffice connector is responsible for receiving and delivering mail to a postoffice. It also determines any rules or filters applied to messages at a mailbox level.

3.1.2.3 List connector

The list connector is responsible for receiving and delivering mail to

3.1.2.4 POP Retrieval Connector

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

3.1.3 Agents

3.1.3.1 Mail Transfer Agent

The Mail Transfer Agent is responsible for sending messages between connectors.

- Receiving Inbound Messages from Mail Connectors
- Delivering Mail to Local Mailboxes
- Queuing Mail for Relay to Mail Connectors

3.2 Administering MailEnable

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

- Postoffices,
- Domains
- Mailboxes
- Lists
- Groups

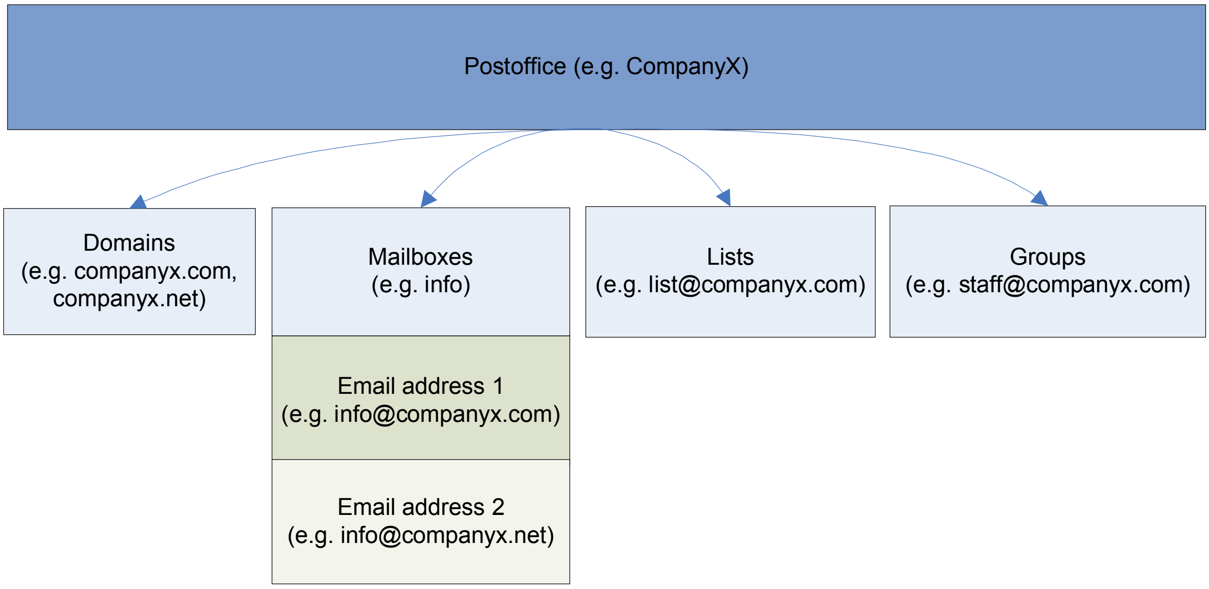


Figure 3-2 Structure of Postoffices, domains and mailboxes

3.2.1.1 Postoffices

A postoffice is used to host multiple mailboxes and domains under one area. For example, if you were providing email hosting for multiple companies, you would create a postoffice for each company. Within the postoffice you can assign multiple domains and mailboxes. If you are running a small mail server, you might only have one postoffice. Post offices can have the same name as a domain.

3.2.1.2 Domains

Multiple domains can be assigned to a postoffice. You need to have at least one domain configured in order to have a valid email address.

3.2.1.3 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 postoffice, using the format mailboxname@domain.

3.2.1.4 Email addresses

Each mailbox can have one or more email address mapped to it. You are only able to add an email that matches an existing domain for the postoffice. When you first create a mailbox, MailEnable will automatically create emails for each of the domains for the postoffice.

3.2.1.5 Lists

MailEnable contains a list server that enables people to subscribe and unsubscribe to a list. A list is a 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.

3.2.1.6 Groups

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

3.3 Email delivery flow

3.3.1 Sending Mail

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.

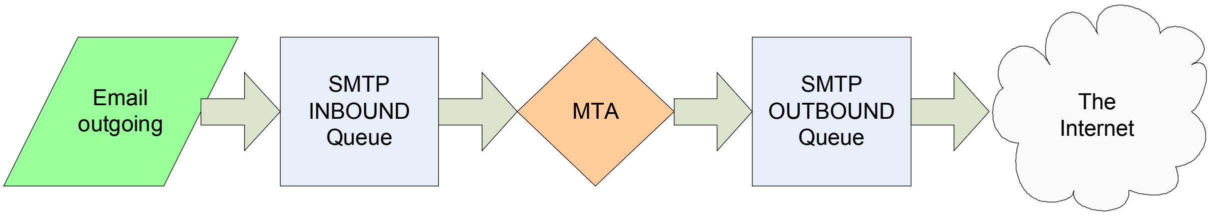


Figure 3-3 Email to remote (Relaying)

To avoid spammers from using the mail server to send email out to anyone, you can require clients to authenticate against the server prior to sending email.

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

3.3.2 Receiving mail

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 postoffice connector service **Outbound** queue. The postoffice connector will be checking its Outbound queue and can then process this message and deliver it to a users mailbox.

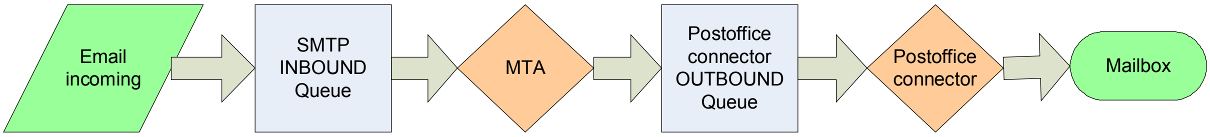


Figure 3-4 Local email delivery flow

The naming of the Inbound/Outbound queues may be confusing initially, especially with the postoffice connector service where you would think "Inbound" would be for messages going to mailboxes. 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 Outbound queues of the services. Services only check their Outbound 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 to you are determined which version of MailEnable you are running). Even messages which arrive via SMTP and have to be 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 Outbound queue.

Utilising 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 due to this flexibility it does create one hurdle for an administrator of MailEnable, and that is the problem of being able to track a message. A message just being sent to a local mailbox will be logged in the SMTP logs, the MTA logs and the postoffice connector logs. Fortunately there are tools and monitoring software that come with MailEnable that makes this easier, but understanding the queue mechanism will make administering your server a lot easier.

4 Installation

4.1 Installation Overview

Note: In order to install MailEnable Professional, you require administrative privileges of the server MailEnable is installing upon.

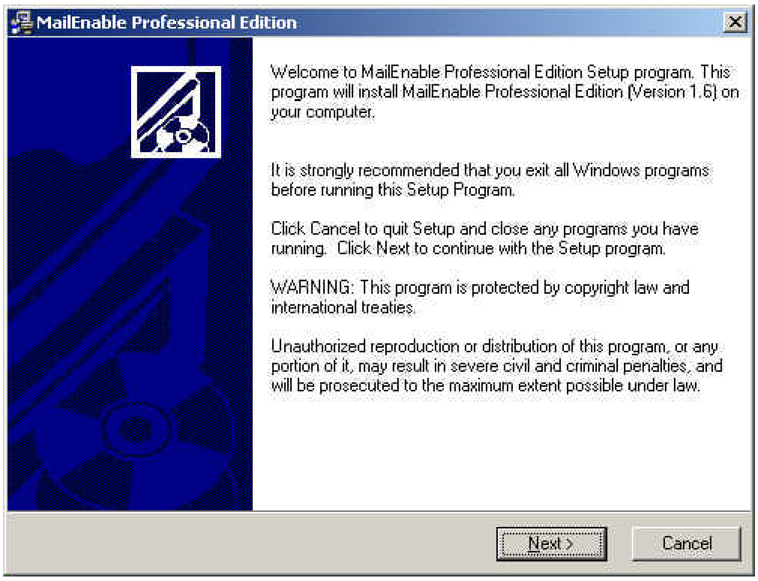
Firstly run the installation executable by double clicking on the install program. The installation program will then guide you through the rest of the installation process. Each screen of the installation program is likely to contain data entry fields, Next, Back and Cancel control buttons.

The **[Next]** button allows you to proceed to the next step of the installation process. To exit the installation at any time, you can click on the **[Cancel]** button. Likewise, the **[Back]** button allows you to step back through the installation process. At any time the [**Cancel]** button is pressed you will be shown an exit screen will be shown verifying that you do in fact want to exit the installer.

4.2 Welcome Screen

The welcome screen informs that you are installing MailEnable Messaging Services. It also provides a warning outlining the copyright protection of the MailEnable product suite.

If you wish to continue installing the application, click on the **Next** button.



Welcome to MailEnable Professional Edition Setup program. This program will install MailEnable Professional Edition (Version 1.6) on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup Program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

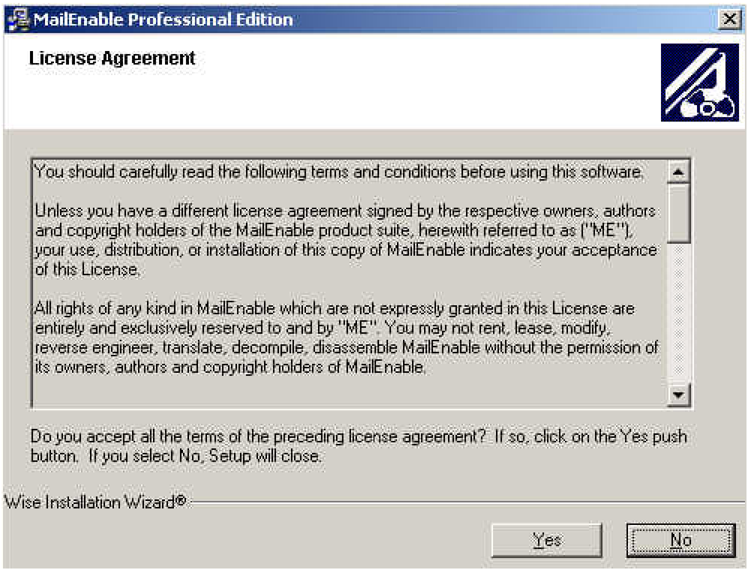
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 4-1 Installer Welcome Screen

Please click the [Next] button to continue.

4.3 Terms and Conditions

The ‘Terms and Conditions’ dialog box explains the licensing terms and conditions of installing and using the MailEnable product suite.



MailEnable Professional Edition

License Agreement

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, disassemble MailEnable without the permission of its owners, authors and copyright holders of MailEnable.

Do you accept all the terms of the preceding license agreement? If so, click on the Yes push button. If you select No, Setup will close.

Wise Installation Wizard®

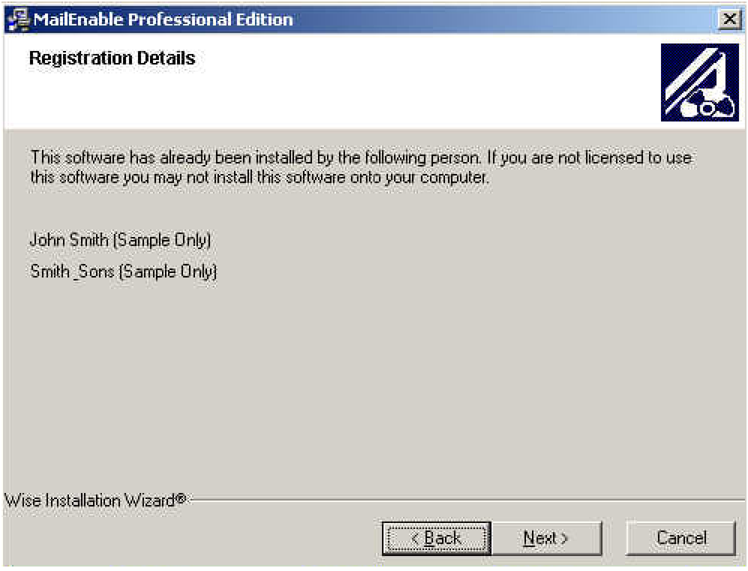
Figure 4-2 Terms and Conditions

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

Please click the [Yes] button to continue.

4.4 Registration Details

The following dialog box may appear to inform you that a previous version of MailEnable has been installed (and who it was installed by).



MailEnable Professional Edition

Registration Details

This software has already been installed by the following person. If you are not licensed to use this software you may not install this software onto your computer.

John Smith (Sample Only)

Smith_Sons (Sample Only)

Wise Installation Wizard®

Figure 4-3 Registration Details

Please click the [Next] button to continue.

4.5 Selecting Installation Components

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

MailEnable Core Components (Server) – This will select the base programs and functionality. This option must be selected if you are installing MailEnable for the first time on this server.

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

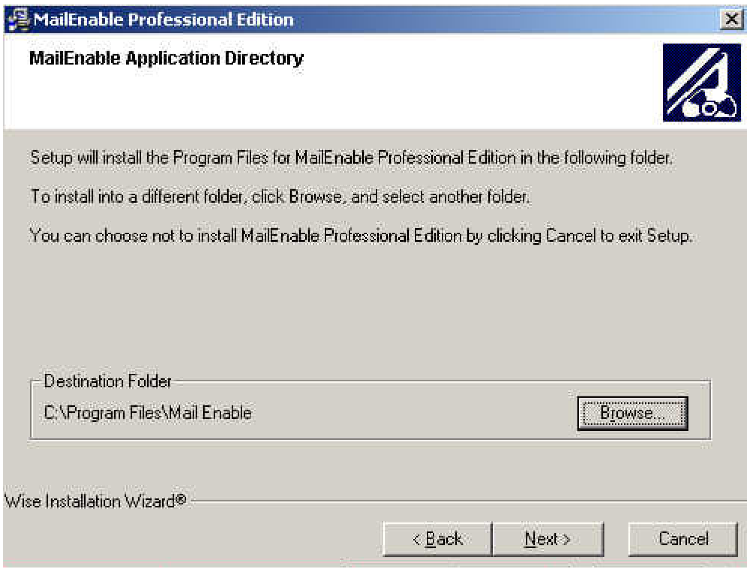
Web Mail Service (Server) – This will install web mail for MailEnable. This option requires that you have Microsoft Internet Information Services (IIS) installed.

Please click the [Next] button to continue.

4.6 Selecting Repository

MailEnable uses a file system as a repository; this effectively allows front-end servers to reference a common repository. MailEnable needs you to confirm the location of this directory so that its various services can access the repository.

MailEnable will detect the repository location if you are using the local repository. You can also nominate a repository on a backend server by pointing at the directory on this server that contains the \CONFIG, \POSTOFFICES or \QUEUES directories.


MailEnable Professional Edition

MailEnable Application Directory

Setup will install the Program Files for MailEnable Professional Edition in the following folder.

To install into a different folder, click Browse, and select another folder.

You can choose not to install MailEnable Professional Edition by clicking Cancel to exit Setup.

Destination Folder

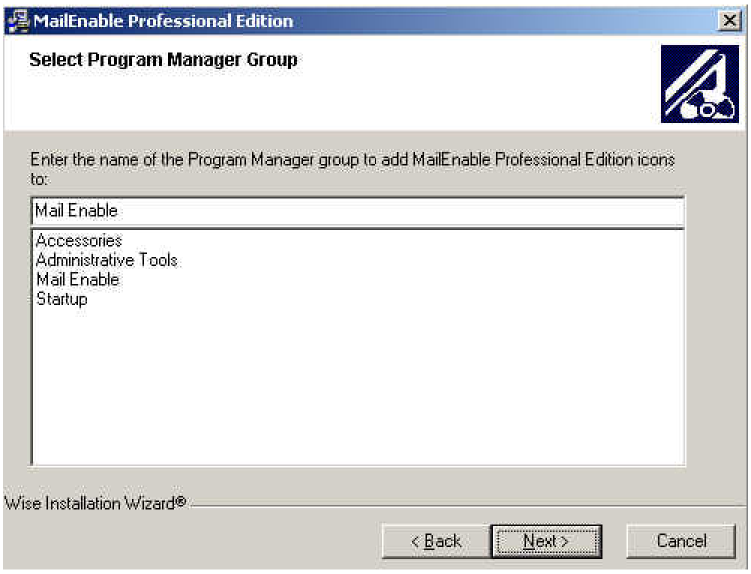
C:\Program Files\Mail Enable

Figure 4-4 Select Storage Repository

Please click the [Next] button to continue.

4.7 Selecting Program Group

The installation wizard will now prompt you for the program group where you want the MailEnable icons and shortcuts installed.



Select Program Manager Group

Enter the name of the Program Manager group to add MailEnable Professional Edition icons to:

Mail Enable

Accessories
Administrative Tools
Mail Enable
Startup

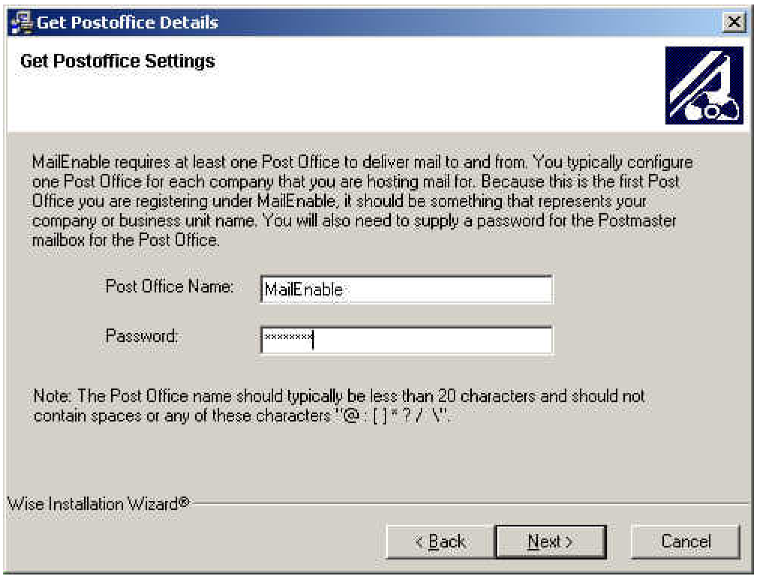
Figure 4-5 Windows Program Group

Please click the [Next] button to continue.

4.8 Creating an Initial Post Office

MailEnable requires that at least one post office is created. A MailEnable post office should be created for each company or organisation that is hosted under MailEnable. A MailEnable post office can own 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. However on this subject another common configuration for this section is to name the post office the actual domain name as this simplifies mailbox logon as users are often aware of the domain they log into.

As depicted below you need to assign a password for the post office Administrator. The mailbox for the administrator of a post office is postmaster@Postoffice name. You can use this account to access Web Administration. It is important to understand that users will authenticate as Mailbox@Postoffice name when they access their mail.



Get Postoffice Settings

MailEnable requires at least one Post Office to deliver mail to and from. You typically configure one Post Office for each company that you are hosting mail for. Because this is the first Post Office you are registering under MailEnable, it should be something that represents your company or business unit name. You will also need to supply a password for the Postmaster mailbox for the Post Office.

Post Office Name: MailEnable

Password: ********

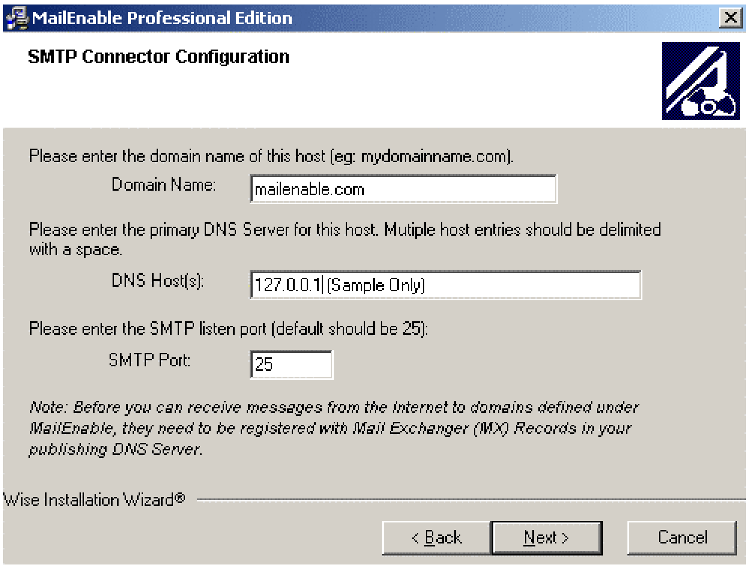
Note: The Post Office name should typically be less than 20 characters and should not contain spaces or any of these characters "@ : [ ] * ? / \".

Figure 4-6 Get Post Office Settings

Please click the [Next] button to continue.

4.9 SMTP Connector Configuration

The installation will now prompt you to enter specific details for its SMTP Connector.



SMTP Connector Configuration

Please enter the domain name of this host (eg: mydomainname.com).

Domain Name: mailenable.com

Please enter the primary DNS Server for this host. Mutiple host entries should be delimited with a space.

DNS Host(s): 127.0.0.1 (Sample Only)

Please enter the SMTP listen port (default should be 25):

SMTP Port: 25

Note: Before you can receive messages from the Internet to domains defined under MailEnable, they need to be registered with Mail Exchanger (MX) Records in your publishing DNS Server.

Figure 4-7 SMTP Connector Configuration

These settings are outlined in the following table:

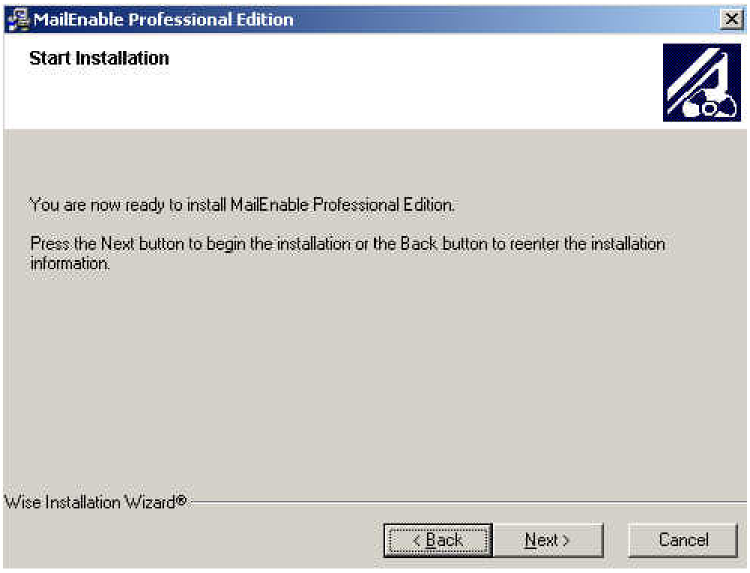
Setting	Description
Domain Name	The domain name should be the domain name of the organization that owns or is operating the server. If you are using this server on the Internet, it is important that this domain name is registered.

DNS Host	The DNS host used by the SMTP Connector to locate mail servers. If you wish to use multiple DNS addresses, you can enter these here, and separate the IP addresses with a space. In most cases, you should include the same DNS host(s) 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.

Please click the [Next] button to continue.

4.10 Commence Installation

The installation program will prompt you a final time before it commences installing files and registering the application.



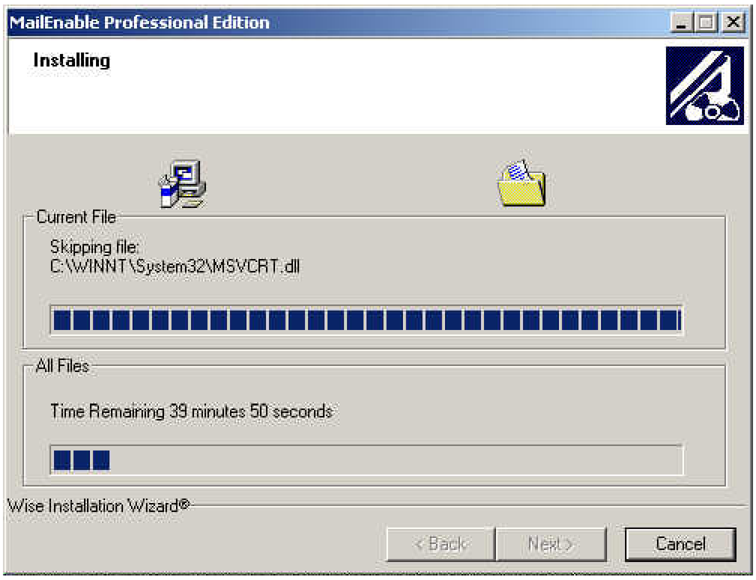
You are now ready to install MailEnable Professional Edition.

Press the Next button to begin the installation or the Back button to reenter the installation information.

Figure 4-8 Start Installation

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.



MailEnable Professional Edition

Installing

Current File

Skipping file:
C:\WINNT\System32\MSVCRT.dll

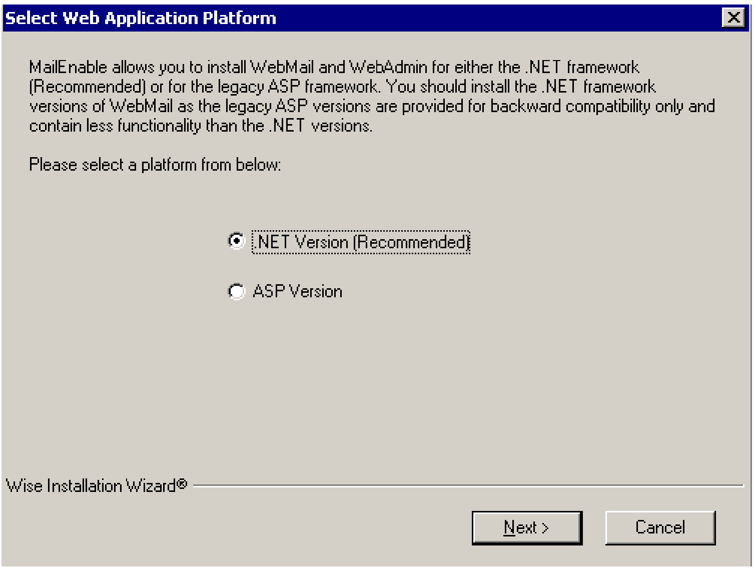
All Files

Time Remaining 39 minutes 50 seconds

Wise Installation Wizard®

Figure 4-9 Installation Windows Progress

4.11 Select Web Mail platform ASP or .NET



Select Web Application Platform

MailEnable allows you to install WebMail and WebAdmin for either the .NET framework (Recommended) or for the legacy ASP framework. You should install the .NET framework versions of WebMail as the legacy ASP versions are provided for backward compatibility only and contain less functionality than the .NET versions.

Please select a platform from below:

● .NET Version (Recommended)

○ ASP Version

Wise Installation Wizard®

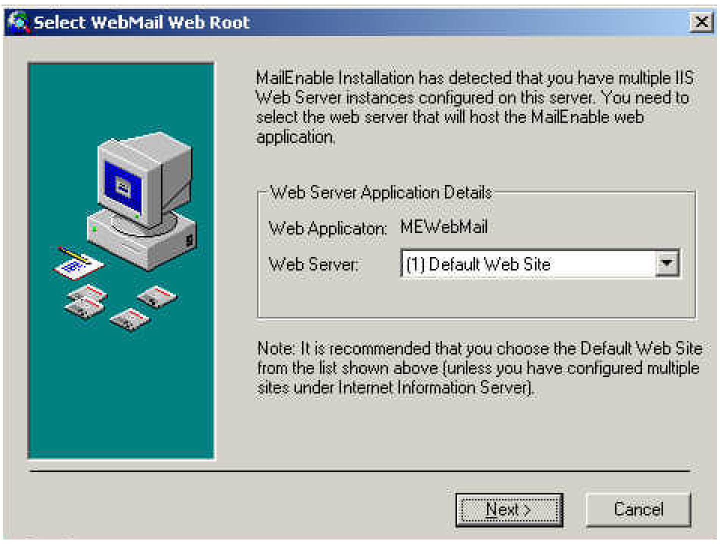
Figure 4-10 Selecting Web Application Platform

Choose here which platform you would like to use for the web mail and the web admin interfaces. Remembering that if you have changed ASP pages and icons/pictures in previous versions of MailEnable and wish to keep using these you may have to install ASP. If you are not sure and are installing MailEnable for the first time then you should choose the default, .NET. When installing .NET it is required that you have the .NET framework installed into your operating system, if you are unsure please go to the windows update site and verify.

4.12 Select Web Mail Web Site

If you have more than one web site configured under IIS, the setup application will ask you which web site you want to install the Web Mail Virtual Directory. You should install MailEnable under the "Default Web Site" or an alternate site that you may have configured under IIS. Once you have completed your installation of MailEnable Professional you will be able to add or remove web mail from each of the sites you have configured under IIS.

Note: Do not install MailEnable Web Mail under the "Administration Web Site".



Select WebMail Web Root

MailEnable Installation has detected that you have multiple IIS Web Server instances configured on this server. You need to select the web server that will host the MailEnable web application.

Web Server Application Details

Web Applicaton: MEWebMail

Web Server: (1) Default Web Site

Note: It is recommended that you choose the Default Web Site from the list shown above (unless you have configured multiple sites under Internet Information Server).

Figure 4-11 Web mail

Please select the desired web site and click the button for a Default Web Site for MailEnable Web mail to be configured.

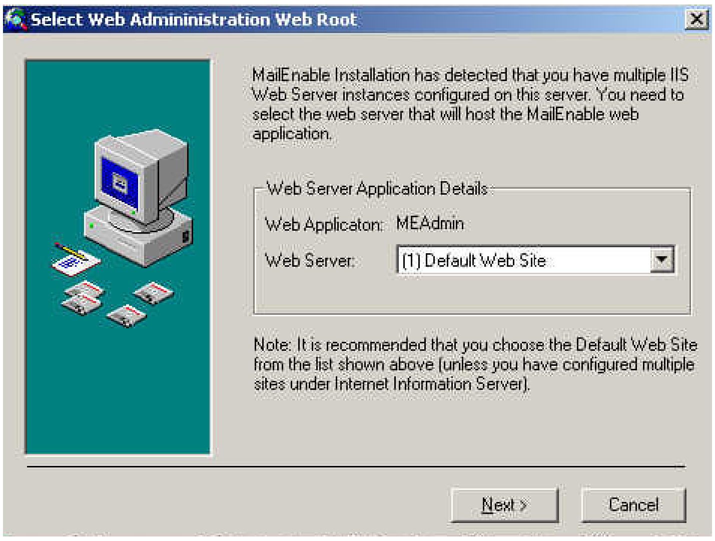
Please click the [Next] button to continue.

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

4.13 Web Administration

Web Administration is installed if you have selected Web Administration as an option from the component list as depicted earlier in section 4.5. If you have more than one web site configured under IIS, the setup application will ask you under which web site you want to install the Webadmin Virtual Directory. You should install the web administration under the "Default Web Site" or an alternate site that you have configured under IIS.

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



MailEnable Installation has detected that you have multiple IIS Web Server instances configured on this server. You need to select the web server that will host the MailEnable web application.

Web Server Application Details

Web Applicaton: MEAdmin

Web Server: [1] Default Web Site

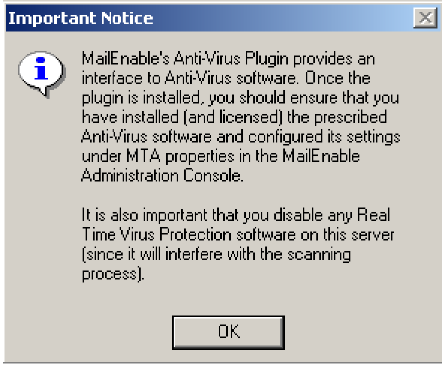
Note: It is recommended that you choose the Default Web Site from the list shown above (unless you have configured multiple sites under Internet Information Server).

Figure 4-12 Web Admin

Please click the [Next] button to continue.

4.14 Antivirus Plug-In Notice

The following notice describes the Mail Transfer Agent Anti-Virus Plug-in. (Please see section 9.1.2 on configuring anti-virus support).



MailEnable's Anti-Virus Plugin provides an interface to Anti-Virus software. Once the plugin is installed, you should ensure that you have installed (and licensed) the prescribed Anti-Virus software and configured its settings under MTA properties in the MailEnable Administration Console.

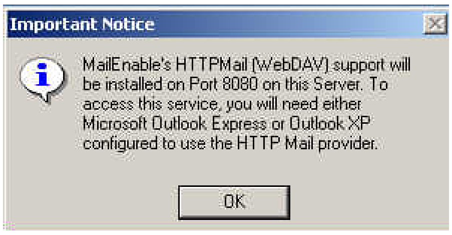
It is also important that you disable any Real Time Virus Protection software on this server (since it will interfere with the scanning process).

Figure 4-13 Anti Virus Plug-in Information

Please click the [OK] button to continue.

4.15 HTTPMail Notice

The following notice describes the HTTPMail service. (Please see further section 8.7 on configuring HTTPMail support).



Important Notice

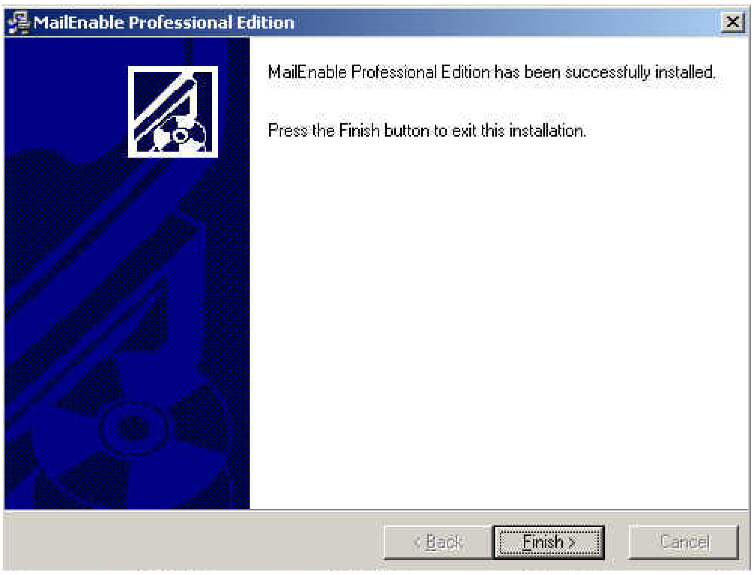
MailEnable's HTTPMail (WebDAV) support will be installed on Port 8080 on this Server. To access this service, you will need either Microsoft Outlook Express or Outlook XP configured to use the HTTP Mail provider.

Figure 4-14 HTTPMail Information

Please click the [OK] button to continue.

4.16 Completing Installation

Finally, setup will inform you the installation procedure completed successfully.



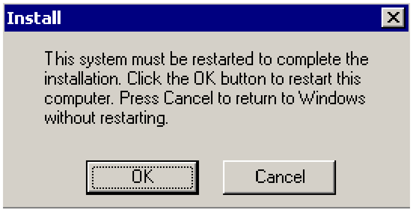
MailEnable Professional Edition

MailEnable Professional Edition has been successfully installed.

Press the Finish button to exit this installation.

Figure 4-15 Complete Installation

Please click the [Finish] button to complete installation of MailEnable



Install

This system must be restarted to complete the installation. Click the OK button to restart this computer. Press Cancel to return to Windows without restarting.

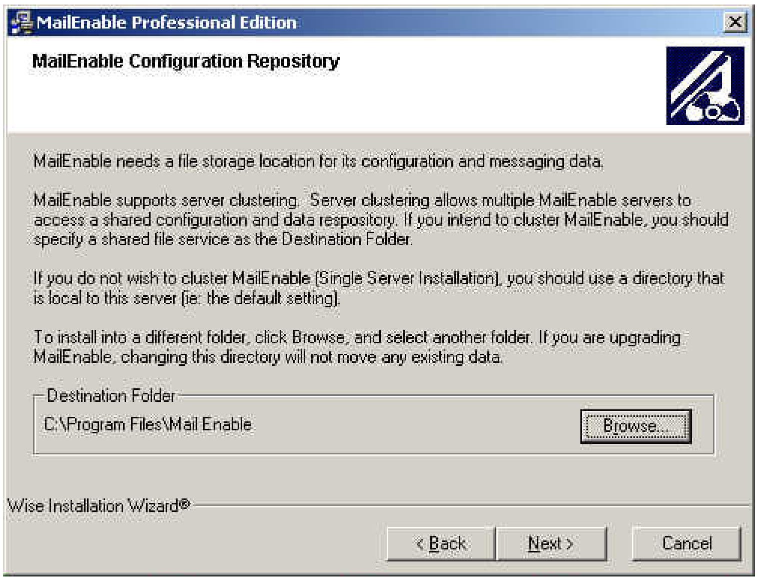
Figure 4-16 Reboot Server

Please click the **OK** button to automatically reboot. A reboot is required after install or upgrade.

5 Upgrading

To upgrade to any newer version of MailEnable Professional from either Standard Edition or earlier Professional Editions you follow the same steps as in Chapter 4 and as the same data stores are used, you can simply run the installation over the top of your current configuration. MailEnable will detect the old version and retain the old settings (unless you specify otherwise during the install process). The latest MailEnable setup kits are available from the MailEnable web site.

When you install MailEnable over an existing installation, it will prompt you to specify the location of your configuration repository. It should default to the current configuration location as used by the existing installation of MailEnable. If you change the path to your configuration repository on an upgrade, it will not move existing data. This dialog is shown below:



MailEnable Configuration Repository

MailEnable needs a file storage location for its configuration and messaging data.

MailEnable supports server clustering. Server clustering allows multiple MailEnable servers to access a shared configuration and data respository. If you intend to cluster MailEnable, you should specify a shared file service as the Destination Folder.

If you do not wish to cluster MailEnable (Single Server Installation), you should use a directory that is local to this server (ie: the default setting).

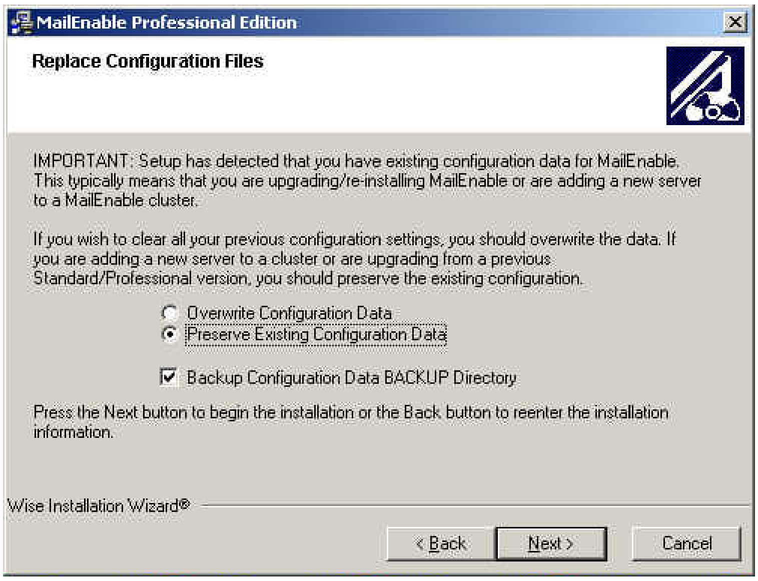
To install into a different folder, click Browse, and select another folder. If you are upgrading MailEnable, changing this directory will not move any existing data.

Destination Folder
C:\Program Files\Mail Enable

Figure 5-1 Change Configuration Storage

Please click the [Next] button to continue.

The default setting of the installation is to **Preserve Existing Configuration Data**. You should leave this selected unless you want to overwrite your configuration with clean installation. This dialog is shown below:



Replace Configuration Files

IMPORTANT: Setup has detected that you have existing configuration data for MailEnable. This typically means that you are upgrading/re-installing MailEnable or are adding a new server to a MailEnable cluster.

If you wish to clear all your previous configuration settings, you should overwrite the data. If you are adding a new server to a cluster or are upgrading from a previous Standard/Professional version, you should preserve the existing configuration.

○ Overwrite Configuration Data
● Preserve Existing Configuration Data

☑ Backup Configuration Data BACKUP Directory

Press the Next button to begin the installation or the Back button to reenter the installation information.

Figure 5-2 Overwrite or update program

The installation will ask you if you want to **Backup Configuration Data BACKUP Directory** this will ensure that your data repositories are backed up which is always good practice (So in this tick box ensure there is a tick as shown above). It is also good practice to have used the MEBACKUP utility beforehand however, since the installation makes its own backup this is not imperative. Details on the backup utility can be found in section 13.1.

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

Please click the [Next] button to continue.

6 Post-Installation Configuration

6.1 MailEnable Diagnostic Utility

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

You can find the MailEnable Diagnostic Utility in your MailEnable Program Group or under the "Diagnose" icon in the MailEnable administration program as shown below.

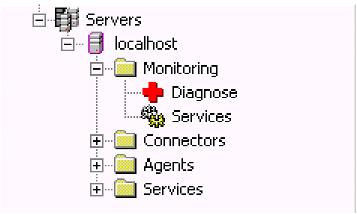
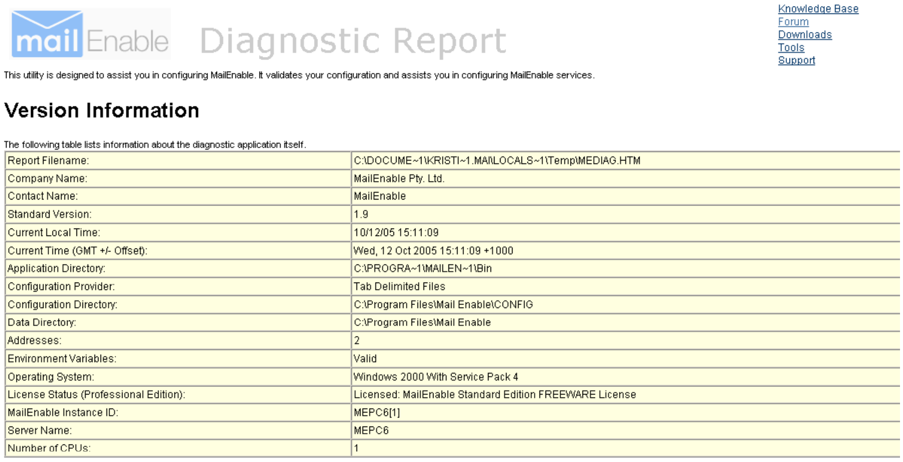


Figure 6-1 MailEnable Diagnostic Utility

Once the Diagnostics Utility has been clicked on, it may takes a few seconds (depending on the amount of domains you have) 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 or does not complete when the diagnose sub heading.



mail Enable Diagnostic Report

Knowledge Base
Forum
Downloads
Tools
Support

This utility is designed to assist you in configuring MailEnable. It validates your configuration and assists you in configuring MailEnable services.

Version Information

The following table lists information about the diagnostic application itself.

Report Filename:	C:\DOCUME~1\KRISTI~1.MAI\LOCALS~1\Temp\MEDIAG.HTM
Company Name:	MailEnable Pty. Ltd.
Contact Name:	MailEnable
Standard Version:	1.9
Current Local Time:	10/12/05 15:11:09
Current Time (GMT +/- Offset):	Wed, 12 Oct 2005 15:11:09 +1000
Application Directory:	C:\PROGRA~1\MAILEN~1\Bin
Configuration Provider:	Tab Delimited Files
Configuration Directory:	C:\Program Files\Mail Enable\CONFIG
Data Directory:	C:\Program Files\Mail Enable
Addresses:	2
Environment Variables:	Valid
Operating System:	Windows 2000 With Service Pack 4
License Status (Professional Edition):	Licensed: MailEnable Standard Edition FREEWARE License
MailEnable Instance ID:	MEPC6[1]
Server Name:	MEPC6
Number of CPUs:	1

Figure 6-2 Diagnostic Reports

The classes and test configurations that are run are as follows:

Option	Description
Version Information	This section contains all required environment data and version information.
Configuration and Data Test	This section verifies that all repository stores are valid and free from any corruptions or permissions errors.
Application Environment	Checks various system files on the server that MailEnable relies on.

System Services and Tests	A test on services and whether they are correctly installed and running is completed here. Some services do not come with all versions of MailEnable, so therefore can fail this test. Click the Status link to get confirmation of whether this is the case.
Queue Status	A calculation of quantity on all inbound and outbound emails is displayed here.
Host TCP/IP Settings	A basic check here on IP and DNS configurations is completed here.
Network Interface Report	A check of all Network Interface Cards and validation of drivers is completed here.
Mail Transfer Agent	Reports details of the MTA service settings which can affect delivery and Antivirus/pickup event performance.
SMTP Configuration Test	The settings or properties of SMTP settings are defined here this is a great place to check security settings for this service.
SMTP Relay Settings	Relay settings are checked here again this is the place to easily verify that only authorized addresses can send through the mail server.
SMTP Inbound Bindings Test	Provides information on the bindings to IP addresses.
SMTP Outbound Configuration	Shows outbound SMTP set configurations.
SMTP Outbound Queue Status Test	Informs of the status of messages queued to remote hosts a check of all logs should be immediate if and errors are found here.
DNS Resolution Test	Resolves all DNS settings.
Host IP Reverse Lookup Tests	Outlines the reverse DNS configuration settings and verifies settings. Some mail servers will reject email if there is no PTR record for your IP address.
Hosted Domain Resolution Test	Checks whether local domains have MX records.
Reverse DNS Lookup Configuration	Indicates whether reverse DNS blacklists are enabled for the SMTP service.
Web Application Configuration Test	Checks web mail and Webadmin settings ensuring sites are correct.
Message Filtering/Antivirus	Shows the status of the MTA and configurations of any Filters and AV programs.
Authentication Tests	Checks all authentication provided by MailEnable.
Post Office Status Tests	Authenticates all post office accounts and domains.

Note: The Diagnostic Utility is also a separate application which can be run through the Program Files->Mail Enable->System Utilities menu.

6.2 Check and Configure DNS Settings

Whilst MailEnable is relatively simple to install, you are likely to need to configure Domain Name Services (DNS) to publish your mail server to remote mail servers and clients. This is necessary so that a remote mail server will be able to determine the IP address of your MailEnable server (in order to deliver any mail to your server).

If you intend to use MailEnable on the Internet, you should have a fixed IP address that is registered under your public DNS. If you are not on a static IP address (i.e. your IP address changes) and you want to direct emails and domains to the server, you will need to use a dynamic DNS provider (DNS2GO is one example of this) that keeps track of your 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. You are still able to send email from MailEnable with a dynamic IP address, but unless the DNS is updated with your new IP address every time it changes, other mail servers will not be able to connect to yours. Be aware that some mail servers will not accept email from you if you are not on a static IP address, or if you are using a cable/DSL connection.

Every domain that you register on MailEnable should have mail exchanger (MX) records defined with your ISP or whoever is hosting your DNS. Due to the vast array of combinations for DNS hosting and the number of vendor specific DNS implementations, you should consult your DNS provider for instructions or inform them of your servers published IP Address along with the domain names you are hosting under MailEnable and request they configure your DNS accordingly.

If you are operating MailEnable from a computer at your office or home, make sure 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 your 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 Knowledgebase (http://www.mailenable.com/kb) and in the MailEnable forums (http://forum.mailenable.com/).

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.

Using the DNS Management software for your DNS Server, ensure that a DNS "A" (Host) record has been created for your mail server. This record type allows the host to be identified by a host name rather than IP Address. You can validate that this was successful by using the ping utility. You should attempt to ping the host using its host name. If this works, then the A record was registered correctly.

Next, you should attempt to create an MX record that points to the A record. The way this is achieved depends on which DNS server/vendor you are using.

It is important to understand the role of the Authoritative DNS Server. The authoritative server for a domain determines which DNS Server(s) holds the 'master copy' of the domains DNS entries as they are to be used throughout the Internet. An example for registering MX records using Microsoft DNS Server is available at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/datacenter/sag_DNS_pro_AddMailExchanger.asp

6.2.1 To set up PTR records under Microsoft's DNS Server

Ensure that DNS Forwarding is enabled on the server. This means that if a client cannot find DNS records on your 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)

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

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

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

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

Note: You should check with your ISP that they allow PTR referrals to your server. This can be checked using resources at http://www.dnsstuff.com

6.3 Check and Configure Integrated Antivirus

Configuring MailEnable to check for viruses requires both the configuration of the particular antivirus program you wish to use, and also the creation of a filter.

For further advice on selecting or configuring an antivirus program, please go to the following link from our Knowledge Base: http://www.mailenable.com/kb/viewarticle.asp?File=me020144.htm

1. Install your antivirus application onto the same server that you have installed MailEnable.
2. Ensure that you have disabled any resident or real-time protector capabilities of the antivirus application (or you have excluded the all the MailEnable directories from being protected by the software).

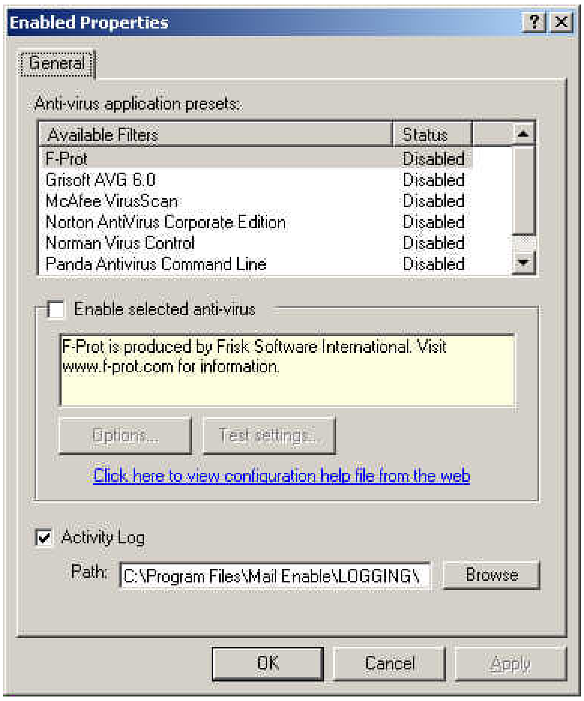
NOTE: Running a real time antivirus protection on a server can cause issues and each resident antivirus protection agent can have its own problems. Some are more forgiving than others. If the resident/real-time monitor is enabled, the symptoms range from blank messages showing up when MailEnable tries to deliver a message with a virus, to possible corruption of mail system configuration files or messages themselves.

As a general rule, you should consider the following:

- Exclude MailEnable “Queues” and the “Config” Directories from the resident/real-time monitoring.

- 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, click on the MailEnable Message Filter icon, then double click the MailEnable Antivirus Filter item in the list which appears on the right side panel.



Anti-virus application presets:

Available Filters	Status
F-Prot	Disabled
Grisoft AVG 6.0	Disabled
McAfee VirusScan	Disabled
Norton AntiVirus Corporate Edition	Disabled
Norman Virus Control	Disabled
Panda Antivirus Command Line	Disabled

☐ Enable selected anti-virus

F-Prot is produced by Frisk Software International. Visit www.f-prot.com for information.

Click here to view configuration help file from the web

☑ Activity Log

Path: C:\Program Files\Mail Enable\LOGGING\

Figure 6-3 Antivirus filter

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

5. Make sure that the "Enable" (or "Enable selected antivirus") is selected. You can enable more than one antivirus application on your server, but this will impact on the amount of messages that can be scanned over a period of time.
6. Ensure that you have specified the correct program path to the command line virus scanner. Clicking on the Options button can change this. You should 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 you are updating your virus definition files. See your antivirus documentation for information on how to do this.

Test the configuration by emailing yourself the Eicar test virus from http://www.eicar.com. You can also perform more advanced testing and debugging by following the details in this article - http://www.mailenable.com/kb/viewarticle.asp?aid=85

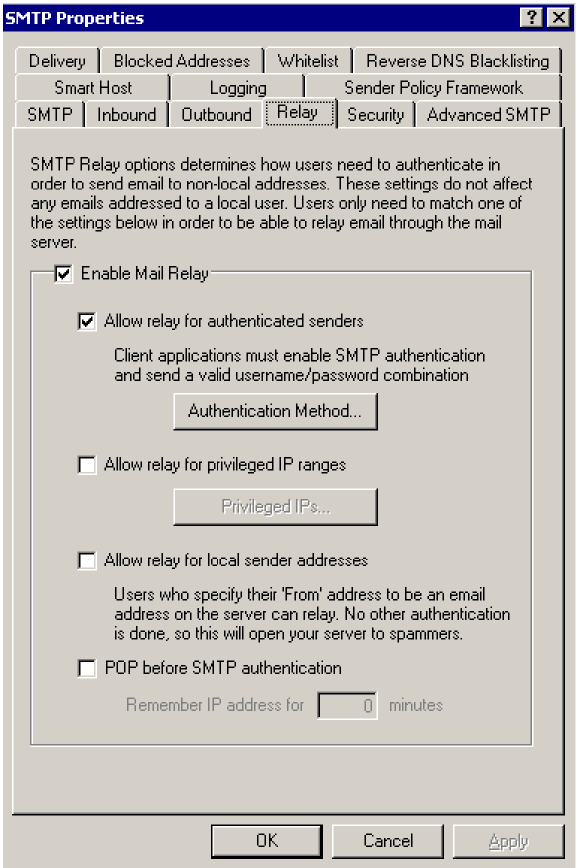
Note: Some antivirus applications specifically require Administrative privileges to run. Since the MTA runs under the LocalSystem account, you need to change this to an account with Administrative privileges. Open the Services control panel applet. For the "MailEnable Mail Transfer Agent" service, change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

6.4 Check and Configure Relay Settings

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 that you regulate who can send messages to others (non-local recipients) or your server will be identified as an Open Relay. This means that people on the Internet can send email out through your server without authenticating. Secure your server by configuring strict rules as to who can use your server to 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**, and leave **Allow relay for local sender addresses** unchecked. This will make everyone who wants to send email out via your 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 as shown below:


SMTP Properties
Delivery | Blocked Addresses | Whitelist | Reverse DNS Blacklisting
Smart Host | Logging | Sender Policy Framework
SMTP | Inbound | Outbound | Relay | Security | Advanced SMTP

SMTP Relay options determines how users need to authenticate in order to send email to non-local addresses. These settings do not affect any emails addressed to a local user. Users only need to match one of the settings below in order to be able to relay email through the mail server.

☑ Enable Mail Relay

☑ Allow relay for authenticated senders

Client applications must enable SMTP authentication and send a valid username/password combination

□ Allow relay for privileged IP ranges

□ Allow relay for local sender addresses

Users who specify their 'From' address to be an email address on the server can relay. No other authentication is done, so this will open your server to spammers.

□ POP before SMTP authentication

Remember IP address for 0 minutes

Figure 6-4 Relay Settings

Find below an explanation of the various relay settings.

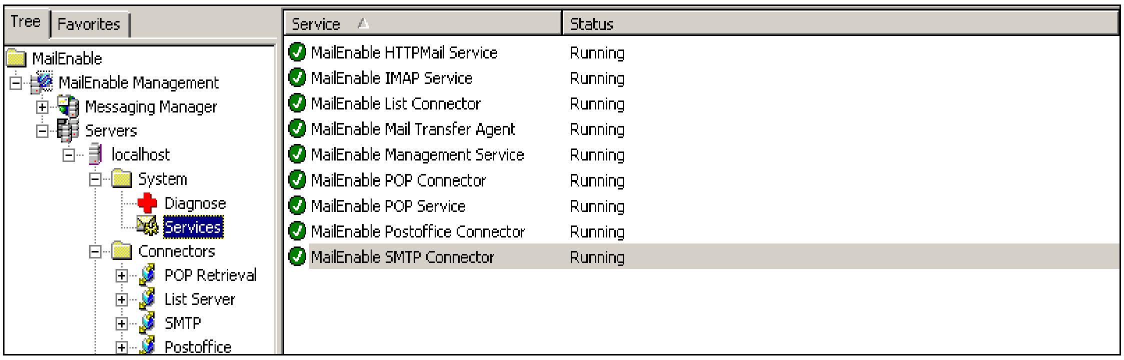
Setting	Description
Allow relay for authenticated senders	This means that people who try to send mail out through your server need to enter a username and password (i.e. this option enables SMTP authentication). To set this is different for various mail clients, but in Microsoft Outlook Express and Microsoft Outlook for instance, you do this in the account properties via the "My server requires authentication" checkbox under the "Servers" tab. It is advisable that you have this option enabled if you are not using privileged IP ranges. You should also ensure that you have not enabled Secure Password Authentication (SPA).
Allow relay for privileged IP ranges	This means that you will allow people with certain IP addresses to send email through your server. If you know the IP addresses of those persons who are able to send email out through your server, you can use this option. DO NOT select this if you haven't set a list of IP addresses, as you may inadvertently allow everyone access. Normally this option is not selected. This option is usually required to allow sending through the server from a web server or web page.

Allow relay for local sender addresses	This will allow people to send mail if their 'From' address has a domain that you host on MailEnable. E.g., if you host domain.com, and someone sends a mail that has their 'From' address as peter@domain.com, the email will be sent. Unfortunately spammers may still abuse this by pretending they are one of your users, so most servers will not use this option. Using this option may cause some anti-spam blacklists to consider your server as "open relay" and block your email.
POP before SMTP authentication	The IP address of users who authenticate via POP is remembered and permitted to relay. You can set the time to remember the IP address for. 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. 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.

6.5 Check Mail Services

There are various services that are copied onto your computer when MailEnable is installed. These services run in the background and handle the sending, receiving and distribution of email. After initial installation, you should check that these Services are running.

Expand the **Servers >localhost >System** branch, and click **Services**. You should see the following:



Service	Status
✓ MailEnable HTTPMail Service	Running
✓ MailEnable IMAP Service	Running
✓ MailEnable List Connector	Running
✓ MailEnable Mail Transfer Agent	Running
✓ MailEnable Management Service	Running
✓ MailEnable POP Connector	Running
✓ MailEnable POP Service	Running
✓ MailEnable Postoffice Connector	Running
✓ MailEnable SMTP Connector	Running

Figure 6-5 MailEnable Services

The icons indicate the status of the service:

✓ Indicates that the corresponding service is running

✗ Indicates the service is not running, or could not be started

If a service is not running, you can start it by right clicking the service and selecting **Start** from the pop-up menu. The reason for a service failing to start will be displayed in the Status column. Failure of a service to start is usually due to another service running on the same port (such as the Microsoft SMTP Service).

Make sure the services that could possibly be interfering with MailEnable are disabled. If a service fails to start, you can check its respective Debug log to get more details of the failure.

7 Administration

7.1 Overview

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

You can start this application by using the Start menu in Microsoft Windows and Navigating to MailEnable Professional by clicking:

Start >Programs >MailEnable >MailEnable Professional.

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

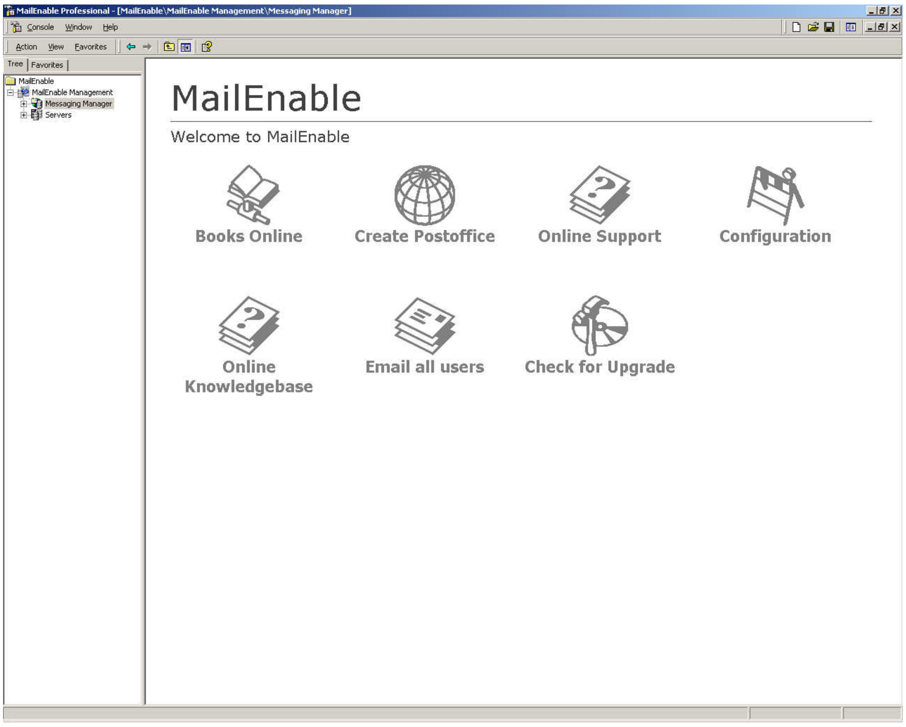


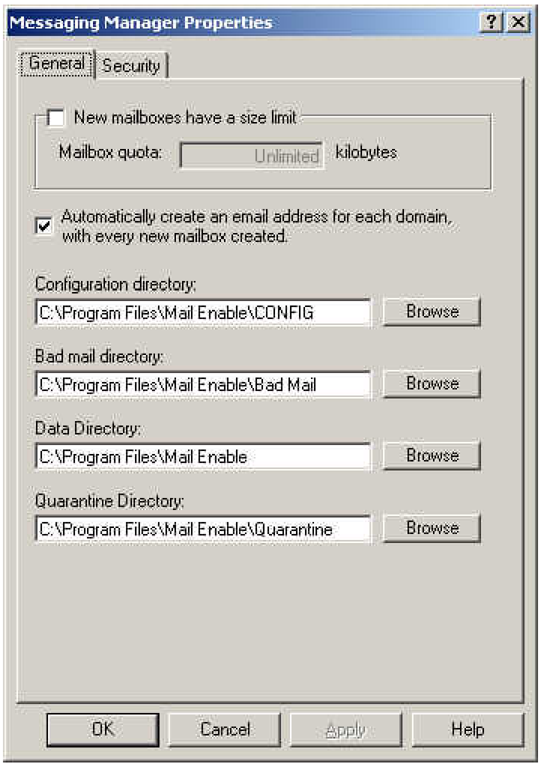
Figure 7-1 MailEnable Administration Program

The tree view on the left allows you to navigate through the various components of MailEnable in order to configure them. The first item in the display is **Messaging Manager**. This is where you modify the various global settings, such as Domains, Post Offices and Mailboxes. Explanations of these items are later in this document.

The second item, labeled **Servers**, is for configuring the various servers that are in your MailEnable configuration. This document only describes how to configure a single server installation.

7.2 Messaging Manager

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 form the popup menu, or click the Configuration icon in the right side panel



☐ New mailboxes have a size limit

Mailbox quota: Unlimited kilobytes

☑ Automatically create an email address for each domain, with every new mailbox created.

Configuration directory: C:\Program Files\Mail Enable\CONFIG

Bad mail directory: C:\Program Files\Mail Enable\Bad Mail

Data Directory: C:\Program Files\Mail Enable

Quarantine Directory: C:\Program Files\Mail Enable\Quarantine

Figure 7-2 Messaging Manager Properties

7.2.1 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.

Setting	Explanation
New mailboxes have size limit	This allows you to configure the default quota for mailboxes, so every new mailbox created will have a quota configured. This can be enable/disabled in the mailbox settings.
Automatically create an email address for each domain with every new mailbox created.	If you have 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.
Directory paths from the MailEnable system	You should use these settings when you wish to cluster MailEnable and have multiple servers share the same configuration repository. This will effectively allow you to configure a clustered server array or to change the location of the MailEnable configuration and storage repositories.

7.2.2 Managing Security and Authentication Settings

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

Setting	Explanation
Password Details/Encrypt Passwords	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 that you want to encrypt MailEnable passwords. If you are using integrated authentication, Windows credentials will take preference to these passwords.
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".

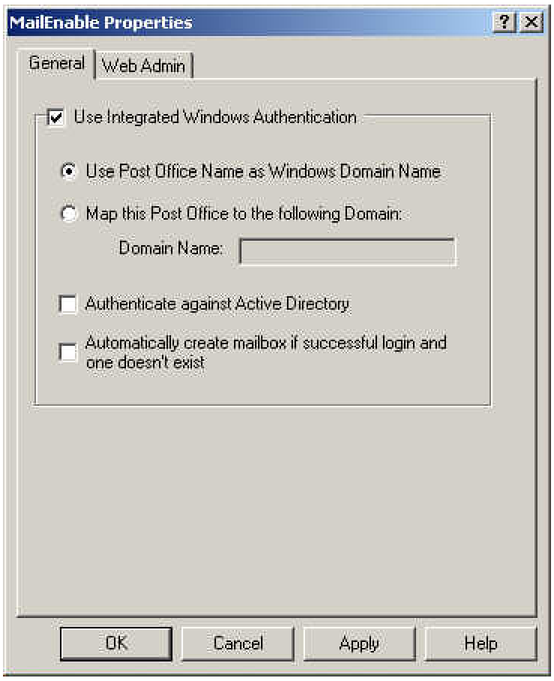
7.3 Post Office Configuration

A post office is used to host multiple mailboxes and domains under one area. For example, if you were providing email hosting for multiple companies, you would create a post office for each company. Within the post office you can assign multiple domains and mailboxes. If you are running a small mail server, you might only have one post office. If you host multiple domains for various people, you would create multiple post offices (think of them as similar to "customer accounts"). It is common for hoting 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

If you wish to add a new post office, click on the **Messaging Manager** branch in the left tree view window of the MailEnable Administration program. In right window, you will now see an icon labelled **Create Post office**. Click this icon to create a post office. You will be prompted to enter a post office name, so enter a meaningful name that describes the client. You also need to supply a password for the postmaster mailbox that will be created for the post office. You have now created a post office.

Note: You can also 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.



☑ Use Integrated Windows Authentication

● Use Post Office Name as Windows Domain Name

○ Map this Post Office to the following Domain:

Domain Name:

□ Authenticate against Active Directory

□ Automatically create mailbox if successful login and one doesn't exist

Figure 7-3 Post Office Properties

7.3.1 General

Once you have enabled Integrated Windows Authentication globally as per section 7.2.2, you can then configure each post office with specific authentication settings

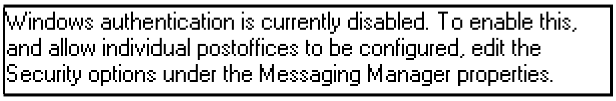
This dialog allows you to configure the Microsoft Windows domain that post office mailboxes can authenticate against. The name of the Mailbox must match the corresponding Windows account name. For example, a mailbox named Administrator will be able to authenticate using the Windows Administrator password.

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 you to authenticate against specific domains (i.e.: if the organization is made up of multiple domains).

Setting	Explanation
Use Integrated Windows Authentication	This setting allows you to define whether the post office can use Windows Authentication.
Use Post Office Name as Windows Domain Name	You should select this option if the name of the post office matches the desired Windows Domain Name.
Map this Post Office to the following Domain Name	This setting allows you to define the Windows Domain Name that the will be used for authenticating this post office's Mailbox users. If you wish to authenticate against the local machine, you can either leave the Domain Name blank or enter a single period (.).
Authenticate against Active Directory	This option configures MailEnable to use UPN style logins, rather than legacy Windows NT style logins. Both login mechanisms work equally as effectively, except Active Directory allows you to host multiple domains in its hierarchy.
Automatically create mailbox if successful login and one doesn't exist	This option allows accounts to be created as users attempt to authenticate. If a user enters valid Windows credentials, their mailbox is created automatically. By enabling this option, you can immediately provide access to mailboxes for those who have validated against the specified domain.

7.3.2 Web Admin

This tab allows the configuration of what users see when they login to the MailEnable Web Administration for each post office. Further information on web administration can be found in section 8.10

Setting	Explanation
Enable web administration for Post Office	This will enable Web Administration for the current post office. This is not configurable if you have not enabled the option of "Enable Integrated Authentication" in the Messaging Manager properties, you will be alerted to this with a message as follows;  Windows authentication is currently disabled. To enable this, and allow individual postoffices to be configured, edit the Security options under the Messaging Manager properties.
Can create and edit mailboxes	This is the maximum number of mailboxes that can be created in Web Administration.
Maximum and default mailbox size	This will enforce a mailbox size for each newly created mailbox in Web Admin. This setting can be disabled or changed for each mailbox in the mailbox properties.
Can select mailbox size (up to the default value)	This will give the web administrator the ability to create a quota for the post office mailboxes up to the configured default size.
Can create and edit lists	This allows the web administrator the option to create lists in web administration.
Maximum number of lists	This will set the maximum number of lists a web administrator can create.
Maximum number of addresses in each list.	This will limit the number of addresses a web administrator can add to a created list.
Can add and remove domains	This will allow the user the ability to add and remove domains in the web administration page.

7.4 Post Office Actions

In the MailEnable Administration Console you can now expand the post offices branch to display all the available post offices. You will see the name of post office you have just created. Clicking on the post office you created will display the available actions you can perform (as seen in the diagram below).

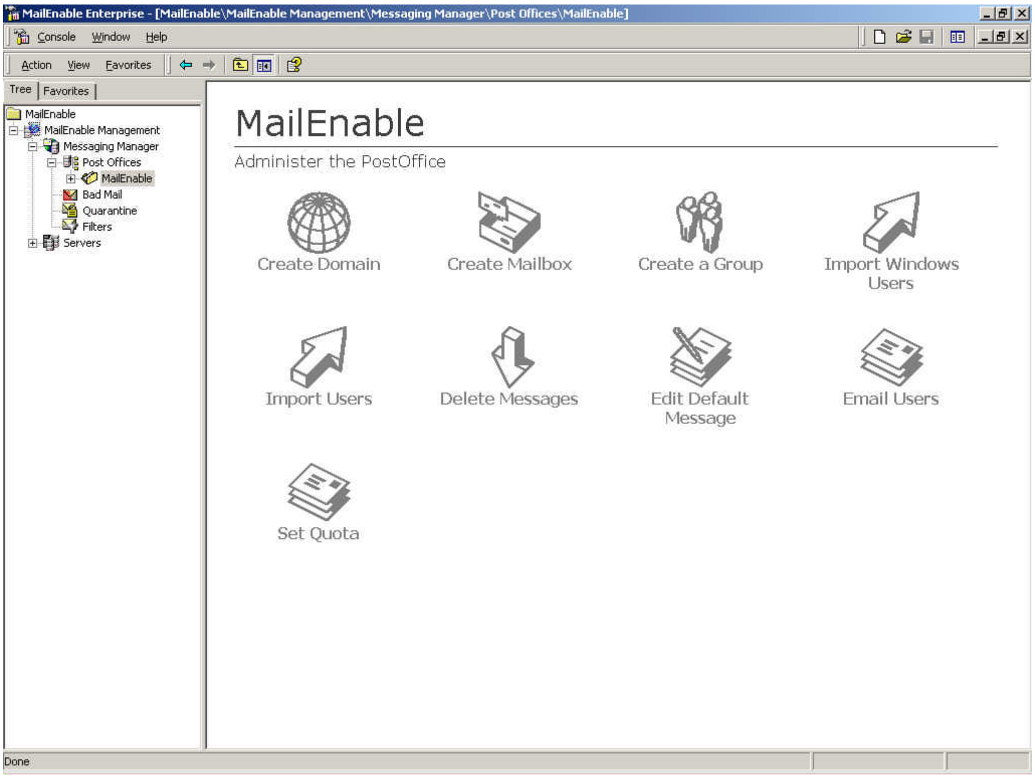


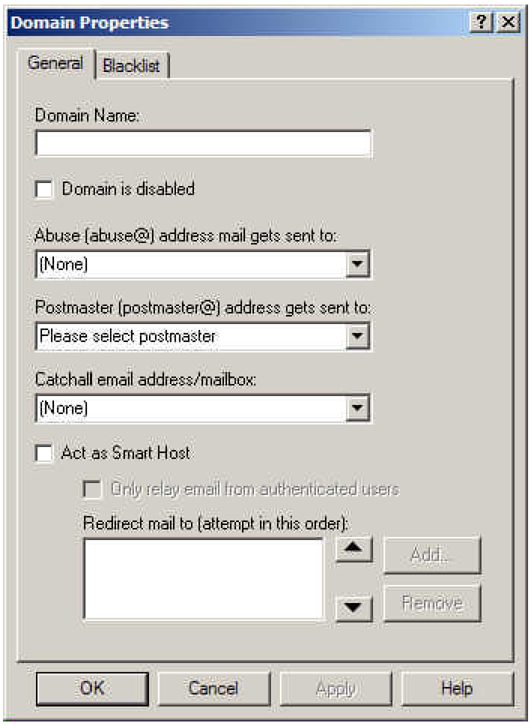
Figure 7-4 Administration program showing actions available for a post office

7.4.1 Create Domain

Domains are logically placed under the post office that owns them. You can 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 Console click on the **Create Domain** icon.

7.4.1.1 General

After clicking on the **Create Domain** icon, you will be prompted for the domain to add.



Domain Properties

General | Blacklist

Domain Name:

□ Domain is disabled

Abuse (abuse@) address mail gets sent to: (None)

Postmaster (postmaster@) address gets sent to: Please select postmaster

Catchall email address/mailbox: (None)

□ Act as Smart Host

□ Only relay email from authenticated users

Redirect mail to (attempt in this order):

Figure 7-5 Domain properties General TAB

Here, you must enter the full domain you wish to receive emails for. For instance, if you wish to receive emails such as sales@mailenable.com or info@mailenable.com, you would enter the domain **mailenable.com** here. The domain you add will now appear under the **Domains** branch.

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

Setting	Description
Domain is disabled	Stops email being sent to the domain.
Abuse Address	You are able to enter the email address or select the mailbox for the abuse@domain email address.
Postmaster Address	You are able to enter the email address or select the mailbox for the postmaster@domain email address. This is a mandatory setting.
Catchall Address	A catchall address will catch all emails for a domain that do not have a mapping to a mailbox. You are able to select an existing mailbox to send all the emails to, or you can enter the email address where you wish to send them to. By implementing a catchall, be aware that this will capture a lot more spam, so make sure you monitor the mailbox or email address you have selected as a catchall. **Warning: It is advisable not to enter a remote email address or a local mailbox which is being redirected to a remote address here. Doing this will cause your server to on-send all the caught spam and is likely to get you blacklisted by the remote server and possibly put 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, then only one message is delivered. This avoids 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.

Act as Smart Host	This will redirect all mail for the current domain to another mail server. This would be used if, for instance, you were acting as a backup mail server for the domain. You are able to 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 section 8.1.8 Smart Host for more information on this selection. Use the Only relay email from authenticated users option in order only to relay email from users that have met the SMTP relay option criteria. This can be used if you have configured a domain to send to a specific relay server (i.e. you might configure the aol.com domain to relay through to another server for your users, but don't want anyone to send aol.com messages through your server).

7.4.1.2 Blacklist

The Blacklist tab allows you to add blacklisted domains for the post office. 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.

Setting	Description
Domains	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 senders 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.

7.4.2 Create Mailbox

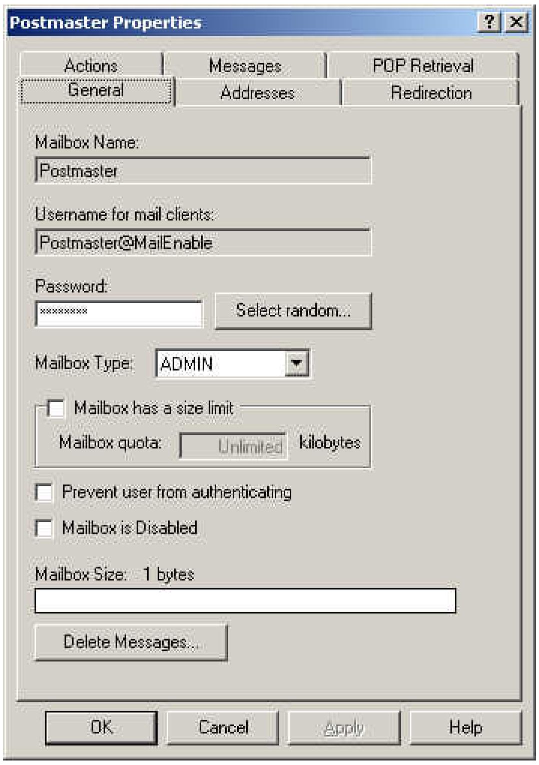
A mailbox is a repository for email. It is used to store emails for one or more email addresses. When your users connect via POP with a mail client application (such as Microsoft Outlook or Eudora), they connect to a **mailbox** in order to retrieve their email. A mailbox can have multiple email addresses. This means a user only requires one mailbox to connect to, from which they can retrieve email from all their email addresses.

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 section 7.2.1) using the format mailboxname@domain. When a mail client application logs onto to MailEnable to retrieve email, it needs to have its username formatted as mailboxname@postofficename.

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

7.4.2.1 General

You will be presented with the following window:



Mailbox Name: Postmaster

Username for mail clients: Postmaster@MailEnable

Password: ********

Mailbox Type: ADMIN

□ Mailbox has a size limit

Mailbox quota: Unlimited kilobytes

□ Prevent user from authenticating

□ Mailbox is Disabled

Mailbox Size: 1 bytes

Figure 7-6 Mailbox Properties – General TAB

The first text box is the **Mailbox Name**, where you enter a name for the mailbox you are creating. If the person who will be using this mailbox to download their emails is named **John Brown**, you may want to enter **johnbrown** here.

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 you enter the Mailbox Name in the text box, you will notice the POP Logon name entry just below it will change to reflect your 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 (this is the username). 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. Mail Enable uses the @ symbol to identify the post office the mailbox belongs to. This way, you can have the same mailbox names 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. This client software uses this when connecting. If SMTP authentication is turn on, this password is also used for sending email. Other extensions to the MailEnable product may also use this username/password combination. Once again the Password you set is the same as the password that is 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.

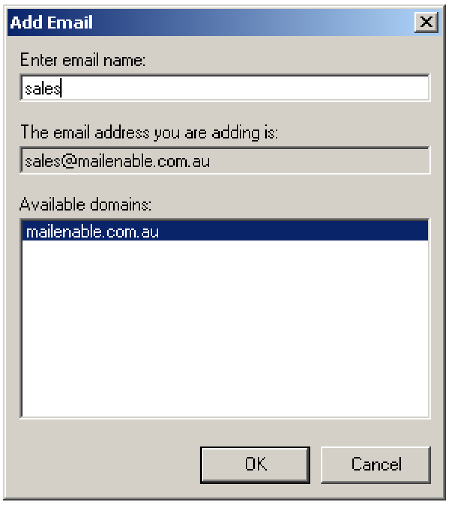
Mailbox Type	Determines the access level for the mailbox. If the mailbox is given "ADMIN" rights, then the user will be able to administer this post office in MailEnable via the administration web interface. If the user is given “SYSADMIN” rights, then they will be able to modify any post office settings.
Mailbox has a size limit	Limits the size of the mailbox. If an email will take the size of the inbox over this amount, the email is bounced back to the sender.
Prevent user from authenticating	If selected 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. It would be used when you don't want the mailbox or email mappings to the mailbox to be recognized, but don’t want to actually delete it. Useful when you wish to suspend an account.
Delete messages	Allows you to delete messages from the mailbox.

7.4.2.2 Addresses

When you create a mailbox, email addresses are created for all the domains available in the post office. For instance, if you have a domain called mailenable.com, and created a mailbox called ‘peter’, the email address peter@mailenable.com will automatically be created.

If you wish to create new email addresses, you can add them by 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 following window will appear:



Enter email name:
sales

The email address you are adding is:
sales@mailenable.com.au

Available domains:
mailenable.com.au

Figure 7-7 Add Email window

The first text box, **Enter email name** is where you enter the first part of the email address. So if you are adding **sales@mailenable.com** you only need to enter the word **sales.** As you enter the email name you will see the actual full address of the email you are adding in the label below it.

You will also notice the **Available Domains** list box in this window. The domains listed here are domains that are entered via the **Create Domain** icon. MailEnable restricts you to adding email addresses only 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. You can then select the appropriate domain by clicking on it and then entering email name that is required. Select OK on the **Add Emails** window when you have entered an address. It will now appear in the mappings list.

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

Setting	Description
Friendly Name	This is the Friendly Name that is used as the display name for emails sent via webmail and for the sender for autoresponder messages. When sending messages from email clients, the friendly name is configured within the client application, not on the server.
Reply To Address	This address is used as the reply to address for auto responders.
Email Addresses for Mailbox	Each mailbox can have one or more email address mapped to it. Use the Add Email… button to add new email addresses. You are only able to add an email that matches an existing domain for the post office. When you first create a mailbox, MailEnable will automatically create emails for each of the domains for the post office.

7.4.2.3 Redirection

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

Setting	Description
Redirect this mailbox to	The Redirection property page allows you to redirect all email for the mailbox to an alternative email address or addresses. To enable redirection, select the Redirect this mailbox to checkbox. Click the Add button to add email addresses. If you have more than one email address listed, the email will be copied to all of the addresses you have listed. There is a limit of approximately 25 email addresses you can redirect to (the limit depends on the length of each email address). If you need to have a large amount of redirections you can use a group which allows an unlimited amount of addresses.
Keep a copy of the message in mailbox	By default, when you redirect a mailbox to another email address a local copy is not retained. By enabling this option you can keep a copy of all the messages that are being redirected.

7.4.2.4 Actions

The actions tab allows for the configuration of auto responders and delivery events.

Setting	Description
Enable auto responder	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. You cannot enable auto responders for the postmaster mailbox.
Enable delivery event	This option allows you to execute a program 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 delivery event will not fire 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 fire the delivery event.

7.4.2.5 Messages

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

Setting	Description
Messages	Lists the current messages in the current mailbox. Double-click an item to view the contents of a message. Only the most recent 200 messages are displayed.
Forward all email	This button will allow you to forward all email from this local mailbox to another mail account. You can specify what account to have the messages forwarded from. The forward will forward the mail in the same way a mail client would and all mail will remain in the mailbox unless you select the option to delete mail.

7.4.2.6 POP Retrieval

The POP Retrieval tab allows you to 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 you disable the feature in the Administration program only the admin or accounts with access to Administration program can create a POP Retrieval account. See section 8.3 for more information on this setting.

Setting	Description
Current POP retrieval items.	This displays any remote or local mailboxes that have been configured to have their mail pulled down into this local mailbox. .
Add Mailbox.	The POP retrieval service allows you to connect to another mailbox and pull any mail in the mailbox into this local mailbox. If you have many accounts across many domains and wish to centralizing all mail receipt to one mailbox then this feature is useful.. To set up an account the following details are required; Mail Server – This is the MX record or DNS name of the remote server i.e. mail.mailenable.com Port – This is the port that is used to connect to the remote server. The default for this is port 110 Username – This is the username of the account. If it is a MailEnable mailbox this must be mailbox@postofficename Password – The password for the account. This server requires APOP authentication - APOP (Authenticated POP) is an extension of the standard POP3 protocol. Authenticating to a POP server will mean your username and password are both encrypted by the client before being passed "over the Internet". The receiving server must then be able to decrypt the password. Only download new messages (leave messages on server) – Will download messages leaving a copy on the server. Enabled – This setting allows the enabling or disabling of a POP service account. This is useful if you do not want to remove the settings but would like the account to stop retrieving mail.

7.4.3 Export Users

A user list can be exported in CSV (comma-separated value) format, with the fields you require. To export users, find the post office where the user details are to be exported. Right click the post office name, select **All Tasks** and then select **Export Users**.

From the list you select the fields you wish to export to the file. Enter the filename you wish to save to and select **Export**.

7.4.4 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 select the post office you wish to import the users to. Then either click the icon for Import users, or right click the post office name, select **All Tasks** and then select **Import Users**.

You will then select the Windows users you wish to import. Select whether to give them a specific quota, or allow them to have an unlimited amount of space. The password for all selected users can be set to the same, or you can let MailEnable give the users random passwords. If giving them random passwords, you are able to export users to produce a list of all the users and the passwords assigned. By default, the users are given an email address corresponding to a domain for the post office you are importing to. Select the domain you wish to assign email addresses for. Mailboxes are automatically enabled when created.

7.4.5 Import Users

This feature allows you to import users to the local postoffice. You must use a comma delimited file that is formatted as

emailaddress, password,quota

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.

7.4.6 Delete Messages

Messages can be deleted from MailEnable either globally, or by post office, or mailbox. You are able to specify how many days old the messages have to be, whether you wish to delete all messages before a certain date, or you want to delete all messages.

7.4.7 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.

7.4.8 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**

7.4.9 Set quota

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.

7.4.10 Edit default message

This edits the default message (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

NB: The default.mai will also be recreated if you moved from using tab delimited configuration storage to database configuration storage.

7.5 Create a Group

A group is an email address that maps to one or more other email addresses. For example, you can set up a group that has the recipient as socialclub@company.com and add 50 email addresses as members of this group. When someone emails socialclub@company.com, the mail is duplicated and sent to all 50 members.

When creating a group, the group name is the full text of the group name so you can easily identify it. The recipient address is the email address of the group and within this group there can contain multiple external groups.

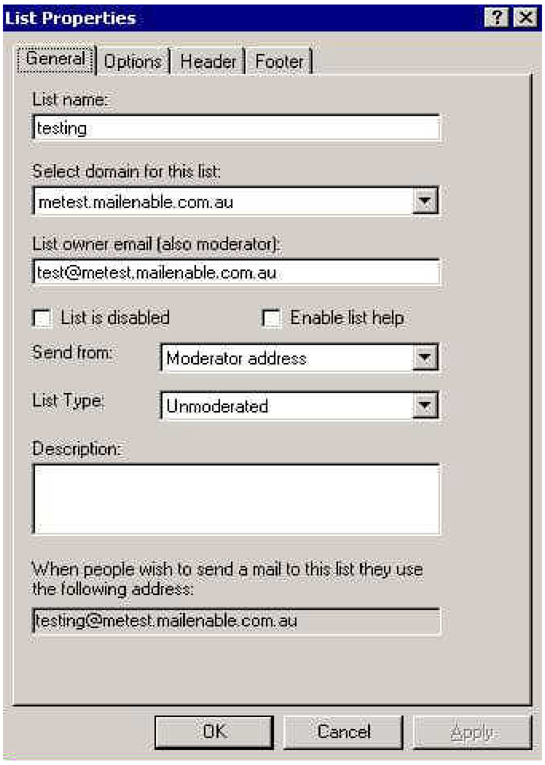
Groups can contain external addresses, so the one group can have different email addresses that are not hosted on the server.

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.

7.6 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 mail out, where emails are sent out to all the members. People are able to post to the list, and the server will duplicate their email and send it out to all the members. 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, under the Messaging Manager select the post office that you wish to create a list for. Right click the **Lists** folder and select **New >List.** This will load the List Properties window that will allow you to configure a new list.



List name: testing

Select domain for this list: metest.mailenable.com.au

List owner email (also moderator): test@metest.mailenable.com.au

□ List is disabled □ Enable list help

Send from: Moderator address

List Type: Unmoderated

Description:

When people wish to send a mail to this list they use the following address:

testing@metest.mailenable.com.au

Figure 7-8 List Properties window

7.6.1 General

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

Setting	Description
List name	The name of the list. This determines the address that people email to in order to post to the list. You can see the full email address for the list at the bottom of the General property page.
Select domain for this list	The domain used for the list name.
List owner email (also moderator)	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.
List is disabled	Disables the list so no one can post to it.
Enable list help	Enables help for the list. So if someone posts to the list with the subject of help, then they will receive an email with details of what commands the list server will accept.
Send from	This determines the From address which will be used for all emails coming from the list. This can be either the moderators email address or the list address. This does not determine where the reply goes.
List Type	Determines whether the list is moderated or not. If moderated, all incoming emails will be sent to the moderator email address.

Description	A description of the list. This is displayed in the Administration program to allow you to easily see what a list is about.

7.6.2 Options

MailEnable also provides advanced list configuration options. These options allow you to control who can post to your lists, where list replies should be directed, who can subscribe to your lists and the format of any subject prefix that is applied to posts

7.6.2.1 Subscription type

MailEnable allows you to control how subscriptions are handled.

Setting	Description
Anyone can subscribe to this list via email	Will allow people to subscribe to the list by sending the word "subscribe" as the subject of an email to the list.
E-mail subscriptions are not permitted for this list	Stops people from subscribing to the list. List members can only be added through the administration program.
E-mail subscriptions need to be confirmed	This option 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.

7.6.2.2 Posting Permissions

MailEnable allows you to control who can post to a list.

Setting	Description
Anyone can post to this list	Anyone is allowed to send a message to the list.
Only subscribers can post to this list	The list will only accept posts from email addresses that exist in the list.
Posting to this list requires a password	You are able to password protect your list. To send an email to a password protected list users need to enclose the password in square brackets e.g. [: and :]

7.6.2.3 Reply Options

These options allow you to determine who should receive responses when a recipient replies to a post.

Setting	Description
Subscribers reply to the list	The reply to address is set to the list address, so when users reply to a message that gets sent from the list, their email gets sent to the list.
Subscribers reply to the posters address	The reply to address is set to the email address of the sender, so when users reply to a message that gets sent from the list, their email gets sent to the person who made the original post.
Subscribers reply to the moderators address	The reply to address is set to the moderators email address, so when users reply to a message that gets sent from the list, their email gets sent to the moderator.

7.6.2.4 List Subject Prefix

Most 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 allow you to control the prefix that is appended to the subject of messages that are dispatched to list subscribers.

Setting	Description
Subject is prefixed with the name of the list	The list name, enclosed in square brackets ([and]) is added to the start of the subject line of emails posted to the list.
Subject is not altered	The subject is not altered for any messages posted to the list.
Subject should have the following prefix	The specified text is added to the start of the subject line for all emails posted to the list.

7.6.3 Headers

Specify plain text headers for all list messages.

Setting	Description
Attach header	This text is added to the top of every email when the Attach header checkbox is selected.

7.6.4 Footers

Specify plain text footers for all list messages.

Setting	Description
Attach footer	This text is added to the bottom of every email when the Attach footer checkbox is selected.

7.6.5 Importing List Members

MailEnable can import users from a text file to a list. Right click on the list icon in the tree view display and select the All Tasks->Import Members menu item. You can then import members from a text file.

7.6.6 List Commands

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

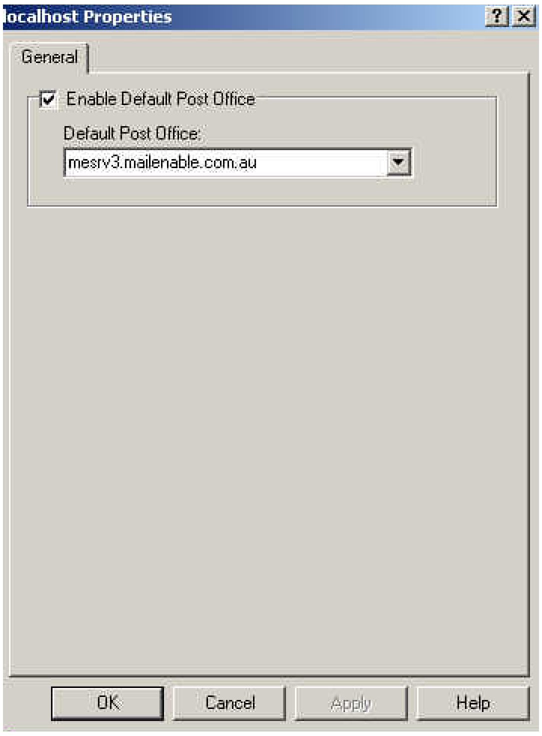
- Help – sends an email back with the available commands of the list server
- Subscribe – adds the user to the list (if the list permissions allow them)
- Unsubscribe – removes the user from the list

7.7 Managing Server Configuration

General Server Configuration Options are located under the properties of the Messaging Manager.

Using this dialog, you can 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 sales@yourdomain.com user will only need to use sales to log on with.

7.7.1 General Configuration



☑ Enable Default Post Office

Default Post Office: mesrv3.mailenable.com.au

Figure 7-9 Server Properties – General TAB

7.8 Option Files

Quite a few options for Post Offices and mailboxes are held in option files in the Mail Enable\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 which contains relevant options. Most of these are configurable through the MailEnable administration program, so the files do not usually need to be edited.

You are able to create default configurations for mailboxes and Post Offices in MailEnable by editing the base SYS files which 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 also 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, you are able to create the web administration program and the base functions which developers may use. Do not copy these configuration files. It is up to the developer to copy or set the defaults if they wish.

8 Configuration of Connectors, Services and Agents

8.1 SMTP

An SMTP, or Simple Mail Transfer Protocol connector, is used to send e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP, IMAP, HTTP or web mail.

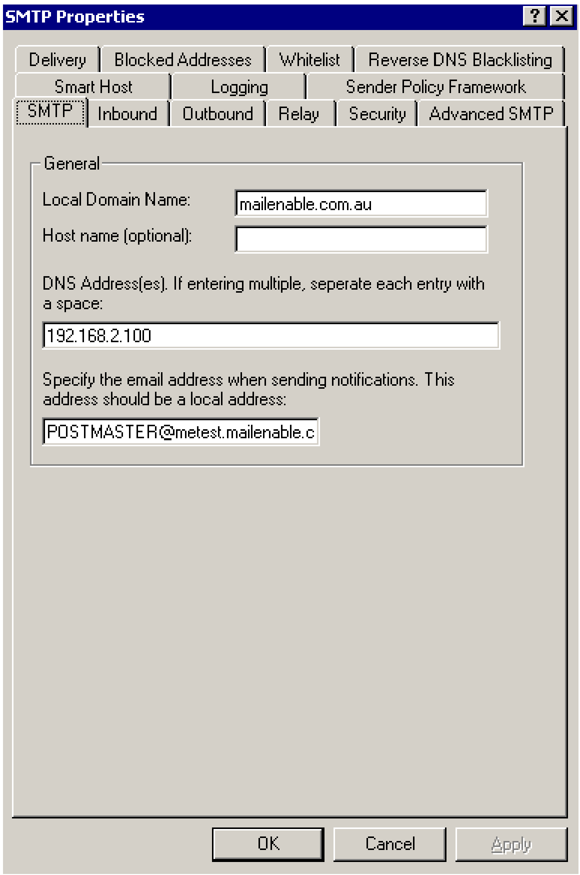
In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

Note: Frequently, POP and SMTP servers are the same computer. Some ISPs (Internet Service Providers) use one server for receiving mail (POP Server) and another for sending mail (SMTP Server); this is done mostly for load balancing and for redundancy.

Using the Administration Console you can access the SMTP properties by expanding the **Servers >Localhost >Connectors** branch.

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

8.1.1 SMTP Properties



General

Local Domain Name: mailenable.com.au

Host name (optional):

DNS Address(es). If entering multiple, seperate each entry with a space:

192.168.2.100

Specify the email address when sending notifications. This address should be a local address:

POSTMASTER@metest.mailenable.c

Figure 8-1 SMTP Properties

Setting	Description
Local Domain Name	This is the domain name of the server you have installed MailEnable onto, or the default domain for your configuration. It is used for system messages, to announce your server when it connects to remote server, and when remote servers connect to MailEnable if the host name has not been specified.
Host name (optional)	This is the host name of your mail server. For example, if you have configured mail.mydomain.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 your server, then that value will override this host name.
DNS Address	The DNS that the local machine uses. If using more than one DNS then 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 you have configured for your local network. Remember that this is not necessarily the DNS of where your 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 you would use postmaster@localdomainname.com (substitute your domain here). Make sure this is a valid email address.

8.1.2 Inbound

Setting	Description
Also listen on alternate port	You can also allow the SMTP service to listen on an alternate port by enabling this option. Usually this is done to cater for clients who may be on connections where their outbound port 25 has been blocked.
Maximum number of concurrent connections	The amount of connections that will be available for remote servers and email clients to connect to.
Advertised Maximum message size	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 kilobytes. Clients or remote mail servers may ignore the value. A size of 0 means that there is no limit on message size.
Enforce this message size	Will check each inbound message size after it is received and 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.
Access Control	The Access Control feature allows you to specify who can connect to your email server. You can specify a list of IP addresses that are either banned from connecting, or are the only ones allowed to connect. You can use the * character as a wildcard.
Inbound IP Bindings	You are able to select the IP addresses that the SMTP service will be bound to. On a multi-homed machine you may only wish to 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.

8.1.3 Outbound

Setting	Description
Maximum number of send threads	The amount of threads that are used to send email.
Timeout for Remote Mail Servers	How long the SMTP service will wait for a response from a remote mail server before disconnecting.
Outbound queue poll interval	How often the SMTP service polls the outbound queue directory for mail messages to send. This is measured in seconds.
Limit outbound message size	This option will force 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).
Outbound IP Binding	This option allows you to force the SMTP to use a specific IP address on the server when it is trying to deliver email.

8.1.4 Relay

Setting	Description
Enable Mail Relay	In order for MailEnable to send email, you need to enable Mail Relaying. Otherwise MailEnable will only be able to receive email. There are four options available to limit those who are able to send mail out through your SMTP server. You are able to select any combination of the four in order to best meet your needs. A client only has to match one of the items in order to relay through your mail server. These settings are described in Chapter 4.4.
Allow relay for authenticated senders	Enabling this feature is required for any user on the server to relay through the server. When enabled a client must supply a valid username and password to relay. Almost anyone that wants to send mail from a remote client to an address that is not on the server will require this setting to be enabled. This setting is enabled by default on the installation of MailEnable.
Allow relay for privileged IP ranges	This setting allows you to enable relay for any connecting IP, it does not require authentication as such simply allows any connection on the IP or IP range you stipulate to relay. If you are using scripts or web pages then this setting is very useful and often compulsory.
Allow relay for local sender addresses	This setting allows relay for any address that is hosted on the server. It is important to enable this only if you are sure. If this setting is enabled any user can forge a "from" address and then, without any authentication, relay through your server. This can cause serious issues.
POP Before SMTP authentication	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.

8.1.5 Security

Setting	Description
Reject mail if sender address is from an invalid domain	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 you should monitor your logs more often.
Authenticated senders must use valid sender address	If this is selected, users with authentication 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.
Senders from local domains must authenticate to relay	When selected any user sending mail must not only have a valid sender email address it must also have authenticated with a valid MailEnable password for the account. This will help stop any spam coming into the server where the senders address is a local server account.
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 you have an network with it's own IP range where you do not wish to expose what range you use to receivers of emails, then you would enable this option, which 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 your email server to collect a lot more email and can cause your server to relay spam (i.e. if you redirect 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 you are using NAT, or wish to accept extra IP addresses which are not configured on the server, you can click the Advanced… button that will allow you to enter these extra IP addresses.
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 you enable this option, you can replace the welcome message with your own. There are also two variables that you can use in your 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	You are able 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 proper 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 amount of failed commands.
Auto-ban the IP address if this number is reached	If a connection has reached the disconnection limit, you can also automatically add the IP address of the client to the SMTP Access Control list. Be aware that if enabling this option, your Access Control list can grow, and adversely affect the performance of the SMTP service. So it is recommended to check the Access Control list regularly.

8.1.6 Advanced SMTP

Setting	Description
Enable alternate catch-all header	When mail is sent to an invalid recipient and they are specified as a BCC on the message, it is difficult for the mail administrator to know who should have received the message. The Catch-All header allows you to specify the name of the message header field that is used to record any recipients that were delivered to the Catch-All account. By default, MailEnable records this information into the Received By: message header; hence this setting is supplied to provide more control over how the information is recorded within the message. Only one copy of a message with multiple recipients is delivered to the catchall mailbox.
Add required headers for authenticated senders if needed	Some email clients or applications will not add a Message-ID or Date header line to their emails. You may encounter a mail server that requires these items and will reject the email if they do not exist. By enabling this option, MailEnable will add the required lines if they don't exist to all users who are authenticated to relay through MailEnable.
Allowed SMTP Commands	The list of SMTP commands you are able to disable are shown here. For example, you may wish to disable the EXPN, which displays all the emails of users in a group, or VRFY, which will allow someone to confirm an email address on the system.

8.1.7 Delivery

Setting	Description
First Retry	The delay before a message is retried for the first time. The default is 15 minutes.
Second Retry	The delay before a message is retried for the second time. The default is 30 minutes.
Third Retry	The delay before a message is retried for the third time. The default is 60 minutes.

Subsequent retries	The delay before a message is retried for the first time. The default is 240 minutes.
Failed Message Lifetime	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 Failed message lifetime has not been reached.
Delay notifications	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 will allow you to turn this 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 amount time from when the message send is first attempted. This will allow you to have the SMTP service try to send the message more than once before the sender is informed that there is a delay.
Do not generate Non-delivery Receipts	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.

8.1.8 Smart Host

Setting	Description
Smart Host Enabled	Enabling this option will force all outbound email to be sent to one server, which you would enter here. Do not configure this to point back to your MailEnable server.
This server requires authentication	The server you are forwarding all your email to may require SMTP authentication. If so, enable this option and enter the username and password that has been assigned to you. The login method used is AUTH LOGIN.
Domain smart-hosting takes priority	You may wish to configure a local domain in MailEnable and smart-host this to a different server to your general outbound email. Enabling this option will allow the smart-hosts you have configured for individual domains to override the SMTP outbound smart-host.

8.1.9 Logging

Setting	Description
Logging Options	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.
Enable Logging	Enables W3C logging for the SMTP service. W3C Logging allows you to specify which fields are logged and the rollover frequency. The directory can also be specified.
Activity Log	Enables the Activity Log.
Debug Log	Enables the Debug Log.

8.1.10 Blocked Addresses

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

Setting	Description
Add	Adds a new SMTP email address to block.
Remove	Removes the selected blocked email address.

8.1.11 Whitelist

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

Setting	Description
Enable whitelist	Enables the SMTP whitelist.
Add	Adds an IP address to the whitelist.
Remove	Removes the selected IP address from the whitelist.

8.1.12 Sender Policy Framework

SPF is an acronym for Sender Policy Framework. It describes a method of verifying whether a sender is valid when you accept email 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 isimpersonating the sending domain.

In simple 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, then 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, it is worth visiting the following website: http://spf.pobox.com

Setting	Description
Enable SPF	Enables the SPF detection.
Reject failures	If an incoming connection returns a SPF fail, then the email message will not be accepted by the SMTP service.
Add Received-SPF header for unauthenticated senders	Adds the Received-SPF header to all unauthenticated emails arriving via SMTP.
Pass local IP addresses (no checking will be done)	If an IP address is determined to be local, then an SPF check is not done.

Enable local whitelist policy	Use your own SPF whitelist 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 affect if it is passing the domain, so you would create an SPF that indicates requirements for domains you wish to pass. The whitelist policy can be a complete SPF record, but must exclude the SPF version string (i.e. Must not have “v=spf1”).
Apply best guess policy for domains without SPF records	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 the domain lookup.

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 you are running any filters to check the header, the first string after the header is the result. I.e. Received-SPF: none, Received-SPF: fail.

For information on configuring filters for handling SPF results, please see section 9.2.1.13.

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

8.1.13 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 you to use popular DNS based blacklists with MailEnable this can help to control spam. You can select which RBL blacklist providers you want to use. You should enable only the providers that you need as it has an impact on performance.

DNS blacklists are lists of IP addresses that are not allowed to connect to your 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. If you wish to use DNS blacklists, please do some research on how the lists are maintained, what the removal process for listed IPs is and what the providers motivations and goals are with their list. Choose the list(s) that are right for you.

You can configure Reverse DNS Blacklisting as follows:

1. From the administration program select Servers|localhost|Connectors|SMTP|Properties
2. Click on the Reverse DNS Blacklisting Property Sheet
3. Check the option to Enable Reverse DNS Blacklisting
4. Scroll down the list and select the Blacklist Provider (e.g.: Spamhaus)
5. Check the box to enable the selected blacklist.

Setting	Explanation
Enable Reverse DNS Blacklist	This enables or disables Reverse DNS Blacklisting for the SMTP Connector.
Blacklist Service	You can use this combo box to list Anti-Spam service providers and their settings.
Enabled	This option allows you to specify whether you wish to configure the server to check a specific Blacklist Provider.
DNS Path	This allows you to define whether you wish to refer your lookup request to the service providers DNS Zone or to simply query a DNS Host for an entry. Most implementations of DNS Blacklists require a Zone lookup.
Zone/Name Server	This is the name of the DNS Zone or the IP Address of the DNS host that should be queried.
Record Type to check for	When the remote host or zone is queried, it may return one or more DNS Record types. Most implementations return an A record, but other implementations may return NS, PTR or MX records.

Note: You can configure a White list that will override the reverse DNS blacklist. This is configured in the administration program by selecting the White list button on the Reverse DNS Blacklisting tab under the properties of the SMTP Connector.

Note: Reverse DNS blacklists affect the performance of incoming email. The reason for this is that for each inbound connection, MailEnable will perform a lookup in the remote DNS.

MailEnable provides a list of well-known Reverse DNS Blacklist providers. You can also configure your own blacklist provider by pressing the **Add...** button. Once you have added the provider, you are able to configure it using the screen outlined earlier. You must click the Enable button before you can configure the service provider's details.

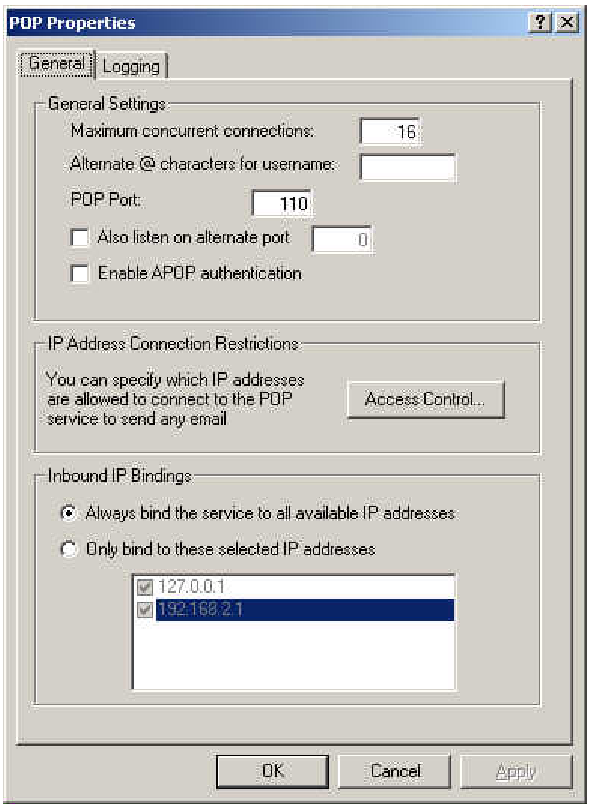
8.2 POP

POP stands for Post Office Protocol, the language used by computers to describe how mail is retrieved by the user. If you have an e-mail account where you routinely pick up your mail, you probably do so through their POP server, though some online services maintain their own proprietary mail transfer system.

Frequently, POP and SMTP servers are the same computer. Some ISPs (Internet Service Providers) use one server for receiving mail (POP Server) and another for sending mail (SMTP Server).

Using the Administration Console you can access the POP properties by expanding the **Servers >Localhost >Connectors** branch.

Right click on the **POP** icon and select **Properties**.



General Settings

Maximum concurrent connections: 16

Alternate @ characters for username:

POP Port: 110

☐ Also listen on alternate port 0

☐ Enable APOP authentication

IP Address Connection Restrictions

You can specify which IP addresses are allowed to connect to the POP service to send any email

Inbound IP Bindings

● Always bind the service to all available IP addresses

○ Only bind to these selected IP addresses

☑ 127.0.0.1

☑ 192.168.2.1

Figure 8-2 POP Properties dialog box

8.2.1 General

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

Setting	Description
Maximum concurrent connections	This is the thread setting limit for incoming POP connections at one time.
Alternate @ characters	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 allows you to 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.
POP Port	This is the port MailEnable will allow client POP connections on. The default is 110.
Also listen on alternate port	You can also allow the POP service to listen on an alternate port by enabling this option. Usually this is done to cater for clients who may be on connections where their outbound port 110 has been blocked.
Enable APOP authentication	Usually, the users' username and password are sent in clear text format (i.e. not encrypted). Due to this, people are able to "tap" into the data stream and read the username and password. To avoid this, APOP encrypts the password before sending, and it changes every time the user logs on. So even if a person manages to grab the encrypted password, they will not be able to use it to log on. Enabling this option will force clients to enable APOP authentication on their mail client software. Make sure your users are using software that supports APOP, otherwise they will not be able to receive email. A lot of the 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 use this secure authentication for example in Outlook the feature is called SPA – Secure Password Authentication. A screen shot of this feature and where to enable it in Outlook 2003 is shown below. More information on NTLM can be found in section 14.2
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 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, if this setting is enabled.
Access Control	The Access Control feature allows you to specify who can connect to your POP service. You can specify 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..
IP Addresses to bind POP to	You are able 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.

8.2.2 Logging

Setting	Description
Enable Logging	Enables W3C logging for the POP service. W3C Logging allows you to specify which fields are logged and the rollover frequency. The directory can also be specified.
Logging Options	Produces a debug and activity log for the POP3 service. Use this if you need to get more details about what the service is doing (i.e. you are debugging a problem).

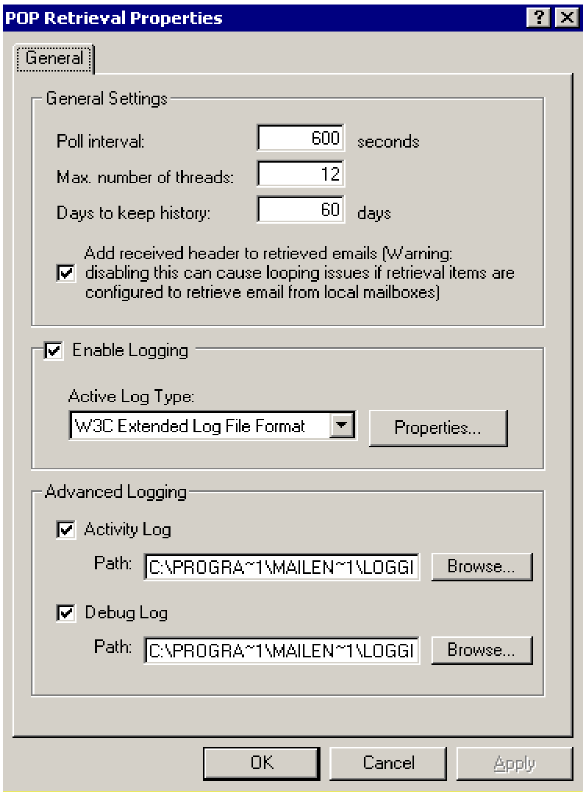
8.3 POP Retrieval Connector

The POP Retrieval Connector will allow you to 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 Console you can 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:

Note: Do not configure POP retrieval to pull email down from the local server



General Settings

Poll interval: 600 seconds

Max. number of threads: 12

Days to keep history: 60 days

☑ Add received header to retrieved emails (Warning: disabling this can cause looping issues if retrieval items are configured to retrieve email from local mailboxes)

☑ Enable Logging

Active Log Type: W3C Extended Log File Format ▼ Properties...

Advanced Logging

☑ Activity Log

Path: C:\PROGRA~1\MAILEN~1\LOGGI Browse...

☑ Debug Log

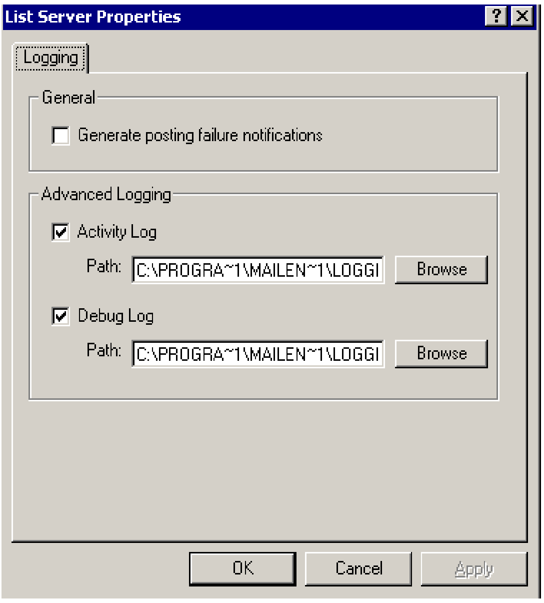
Path: C:\PROGRA~1\MAILEN~1\LOGGI Browse...

Figure 8-3 POP Retrieval Properties

Property	Explanation
Poll Interval	The delay between polling the remote mail server.
Max. number of threads	The maximum number of threads that the polling agent uses to poll remote mailboxes.
Days to keep history	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, you can specify how many days to keep this history of messages.
Add received header to retrieved emails.	This setting is used by MailEnable to detect how many hops a message has had on receipt to a mailbox. Each time a message has been received by a mail server a header line is added similar to; Received: from test.com ([127.0.0.1]) by mailenable.com.au with MailEnable ESMTP; Wed, 14 Sep 2005 15:07:55 +1000 MailEnable can use this line to detect a possible loop, as this header line will continually be added to the message header. MailEnable does a calculation on this and when the message line has been added 15 times the message will be sent to bad mail. Any looping issues will be reported in the MTA logs also.

8.4 List Server Connector

The List Server connector is mostly configurable through the creation and management of particular lists as described earlier in this manual.



List Server Properties

General

□ Generate posting failure notifications

Advanced Logging

☑ Activity Log

Path: C:\PROGRA~1\MAILEN~1\LOGGI

☑ Debug Log

Path: C:\PROGRA~1\MAILEN~1\LOGGI

Figure 8-4

Figure 8-5 List Server Properties

Property	Explanation
Generate posting failure notifications	If a message is sent to a list and is rejected due to sender being rejected or incorrect password the subsequent notification is not sent. This can help reduce traffic where spammers have sent to the address and used a forged email address.
Advanced Logging	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.
Auto responders enabled	When this setting is enabled you can select; 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 MailEnable mailbox that has an auto responder configured, then they will not receive more than one responder per day. If the check box is cleared then the auto responder feature can be disabled, this can aid in the diagnosis of mail loops or any possible auto responder issues.

8.5 Post Office Connector

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.

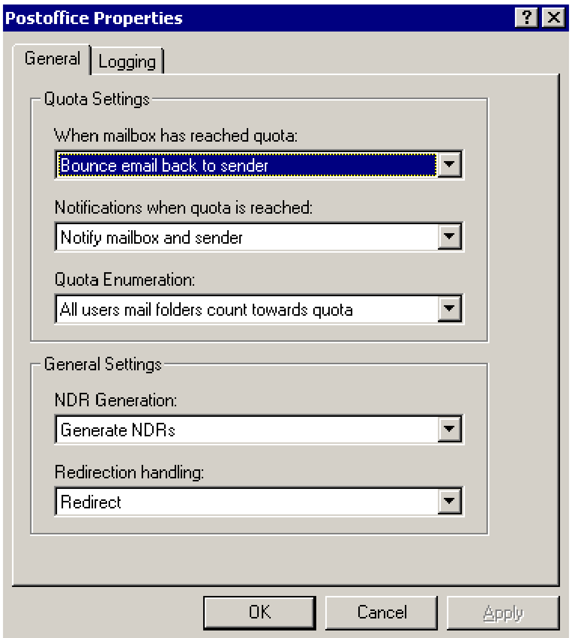
What happens when a mailboxes quota is exceeded? Specifically, you can determine whether the user is notified of the quota issue and whether the message is returned to the sender or sent to the postmaster for that post office.

You 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:



When mailbox has reached quota: Bounce email back to sender

Notifications when quota is reached: Notify mailbox and sender

Quota Enumeration: All users mail folders count towards quota

NDR Generation: Generate NDRs

Redirection handling: Redirect

Figure 8-6 Post Office Connector Properties

8.5.1 General

Setting	Description
When mailbox has reached quota	Specify what occurs when a mailbox's quota is exceeded. You can 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.
Notifications when quota is reached	You 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.
Quota enumeration	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)
NDR Generation	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.
Redirection handling	Redirection handling this has two settings, one that will perform a redirect from the mailbox address where the mailbox was sent to and one that will redirect and leave the senders address for the message, this is used mainly for and one that will allow you to redirect from a particular mailbox.

8.5.2 Logging

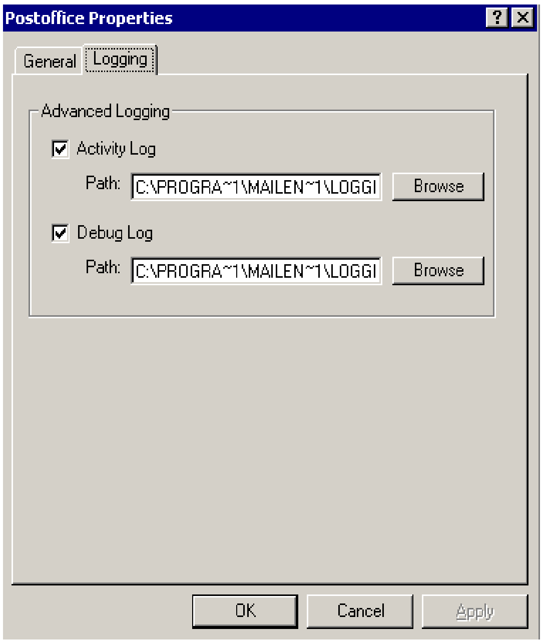


Figure 8-7 Post office properties - Logging

Setting	Description
Logging	This enables the activity and debug logs for the post office connector.

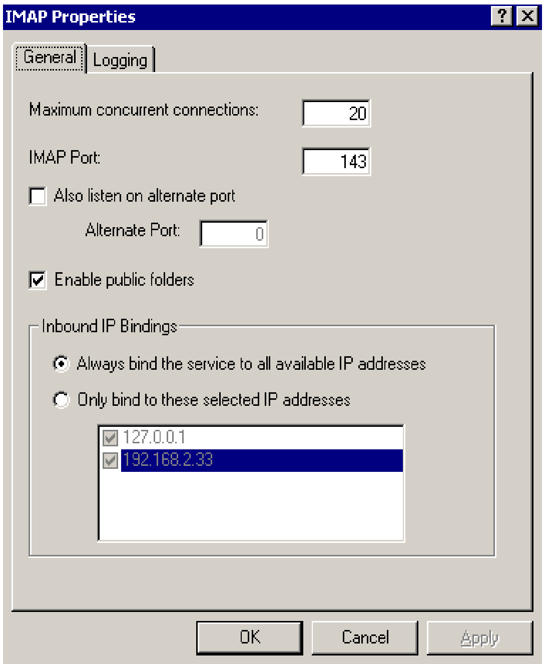
8.6 IMAP Service

IMAP stands for Internet Message Access Protocol. It is a method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. In other words, it permits a "client" email stored on an IMAP server to be manipulated from a desktop computer at home, a workstation at the office, and a notebook computer while traveling, without the need to transfer messages or files back and forth between these computers.

IMAP's ability to access messages (both new and saved) from more than one computer has become extremely important as reliance on electronic messaging and use of multiple computers increase, but this functionality cannot be taken for granted: the widely used Post Office Protocol (POP) works best when one has only a single computer, since it was designed to support "offline" message access, wherein messages are downloaded and then deleted from the mail server. This mode of access from multiple computers tends to sprinkle messages across all of the computers used for mail access. Unless all of those machines share common files system, the offline mode of access that POP was designed to support effectively ties the user to one computer for message storage and manipulation.

Using the Administration Console you can 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:



IMAP Properties

General | Logging

Maximum concurrent connections: 20

IMAP Port: 143

☐ Also listen on alternate port

Alternate Port: 0

☑ Enable public folders

Inbound IP Bindings

● Always bind the service to all available IP addresses

○ Only bind to these selected IP addresses

☑ 127.0.0.1

☑ 192.168.2.33

Figure 8-8 IMAP Properties

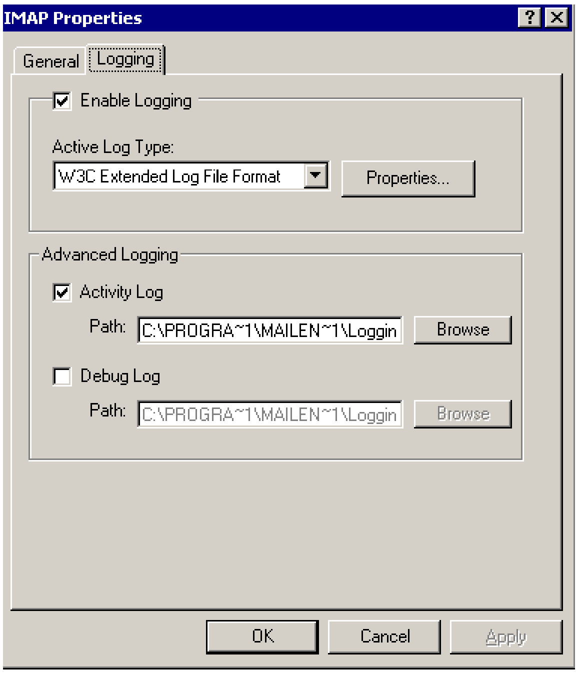
8.6.1 General

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 ensure you have enabled the default port of 143 on your firewall or any other port number you stipulate in the properties of the IMAP service in the administration program as above.

To help in server traffic and load you can also stipulate which IP address you would like to bind the service to.

Setting	Description
Max Concurrent connections (threads)	The number of threads that will be used by the IMAP service to handle client requests.
IMAP port	Port for listening on. Default is 143.
Also listen on alternate port	An alternate port can be selected.
Enable public folders	Public Folders allow one or more mailboxes under the post office to share data (messages in a folder that is seen by all mailboxes on the post office.) Anything that you place in this folder (Program Files\MailEnable\Post Offices\[Post Office Name\Pubroot) will become visible to all other mailboxes on the post office. This feature must be enabled for the post office in Post Office Properties.
IP Addresses to bind to	You are able to select the IP addresses that the IMAP 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.

8.6.2 Logging



☑ Enable Logging

Active Log Type: W3C Extended Log File Format

Advanced Logging

☑ Activity Log

Path: C:\PROGRA~1\MAILEN~1\Loggin

☐ Debug Log

Path: C:\PROGRA~1\MAILEN~1\Loggin

Figure 8-9 IMAP Properties – Logging TAB

Setting	Description
Logging Options	MailEnable's IMAP 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.

8.7 HTTPMail Protocol

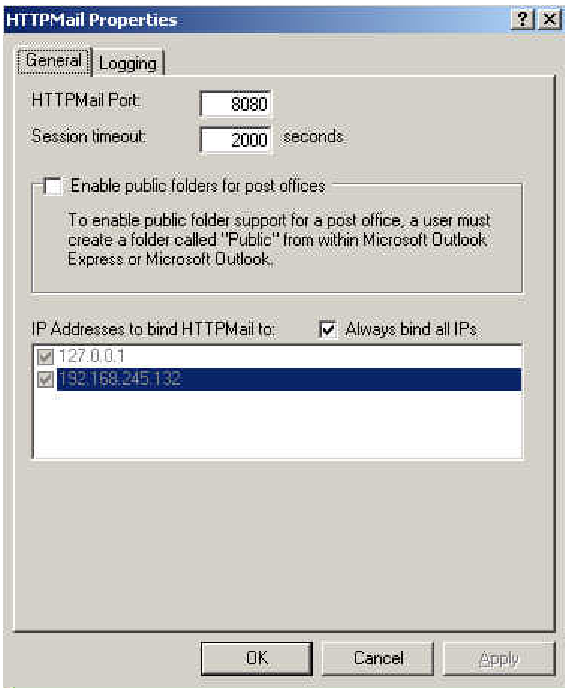
HTTP is the protocol which web handles traffic. It defines how web pages are formatted and in what way they are delivered over the Internet. It also includes any information about the objects that are needed by proxy servers or a user's web browser. HTTPMail is a relatively new protocol for the server 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, you can move messages between your server and local stores as you desire.

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 your 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:



HTTPMail Properties

General | Logging

HTTPMail Port: 8080

Session timeout: 2000 seconds

□ Enable public folders for post offices

To enable public folder support for a post office, a user must create a folder called "Public" from within Microsoft Outlook Express or Microsoft Outlook.

IP Addresses to bind HTTPMail to: ☑ Always bind all IPs

☑ 127.0.0.1

☑ 192.168.245.132

Figure 8-10 HTTPMail Properties dialog box

8.7.1 Configuration

HTTPMail requires very few configuration settings. The major configuration settings are the IP address(es) and port bindings for the HTTPMail Service. If you have selected to install HTTPMail, the service is published on port 8080 of your server (you can 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 on your server). You are able to enable or disable various features of HTTPMail via the administration program.

If you are using Outlook Express or Outlook 2002 as a mail client, you can 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, you will need to use your usual account credentials when prompted (i.e.: User@ Your Account/Postoffice). For more information, please see section 11.5.

8.7.2 Testing

Once you have configured an Outlook Express profile to use the HTTP protocol to access mail, you can debug your mail sessions using the Outlook Express Maintenance tools.

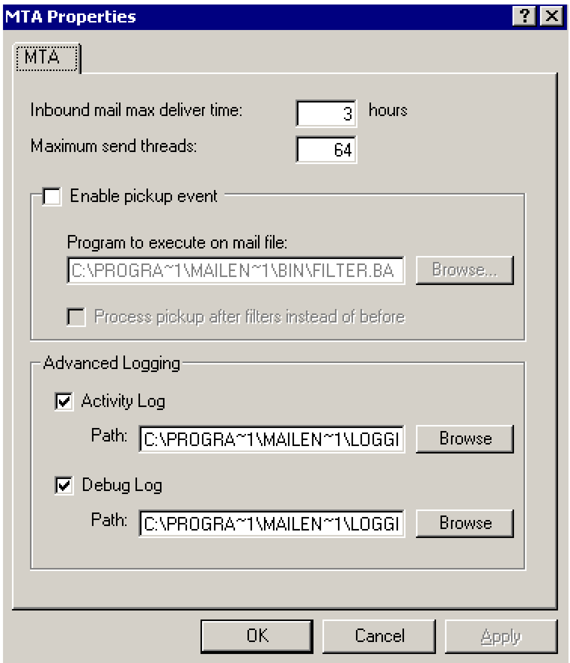
These tools are found under Tools|Options|Maintenance (Under the troubleshooting section, check HTTP). Once this setting is enabled, whenever you use HTTPMail from within Outlook Express, the entire session will be logged to a text file called HTTPMail.log The log file is usually stored under your Documents 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).

8.8 Mail Transfer Agent (MTA)

The Mail Transfer Agent (MTA) is primarily responsible for moving messages between MailEnable Connectors. The MTA moves messages from Inbound Queues to the respective Outbound Message 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

8.8.1 MTA Properties



Inbound mail max deliver time: 3 hours

Maximum send threads: 64

□ Enable pickup event

Program to execute on mail file: C:\PROGRA~1\MAILEN~1\BIN\FILTER.BA

□ Process pickup after filters instead of before

Advanced Logging

☑ Activity Log

Path: C:\PROGRA~1\MAILEN~1\LOGGI

☑ Debug Log

Path: C:\PROGRA~1\MAILEN~1\LOGGI

Figure 8-11 MTA Properties

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

Setting	Description
Inbound mail max. delivery time	The delay time before an inbound mail message is delivered.
Maximum threads	The amount of concurrent threads that will be used to move emails around. Some command line virus checkers do not like to have multiple instances running, so you can restrict the MTA to using one thread to resolve this.

Enable pickup event	When an email arrives, you are able to execute a program, and MailEnable will pass the mail message filename to the application. For example, if you write a VB script that adds some text to the end of each email that gets delivered, you would enable the pickup event. The command line used to execute the application 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. You will need to read the directory path from the registry in the program file. The pickup event is executed before any filters (antivirus for instance).
Logging Options	Produces a debug and activity log for the POP3 service. Use this if you need to get more details about what the service is doing (i.e. you are debugging a problem).

8.9 Web Mail

The web mail information in this manual includes configuration and the various server options. For details on using the web mail, please check the MailEnable Web Mail User Guide within the **Start Menu >MailEnable Program Group >Documentation.**

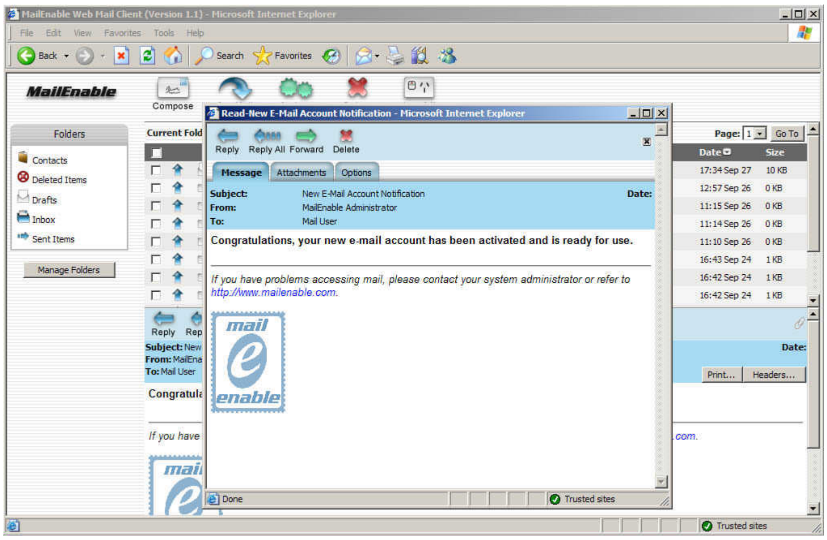
Web mail is a powerful mail application that allows clients to send and receive email via the Internet. Once installed, web mail can be accessed from http://*HostName*/mewebmail - in place of the HostName in this example, you should use the server name as defined in DNS or under IIS. You can also use the IP address of the machine. When you browse to this location, you will be presented with a logon screen. Users should use the same username and password that the POP service uses. Remember that the username is formatted as: mailboxname@postofficename . If you have set a default post office using the administration program, you don't need to use the @postofficename after the mailbox name.

Leveraging Internet Information Services versions 4.0 and above, the web mail component allows you to provide messaging services via the web browser. Users can access the messages hosted on the server and 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 redirections
- Reply, reply to all, forwarding, read receipts, message priority
- 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 also allows you to create additional sites (either using host-headers or additional IP addresses) using the Internet Services Manager.



Subject: New E-Mail Account Notification
From: MailEnable Administrator
To: Mail User

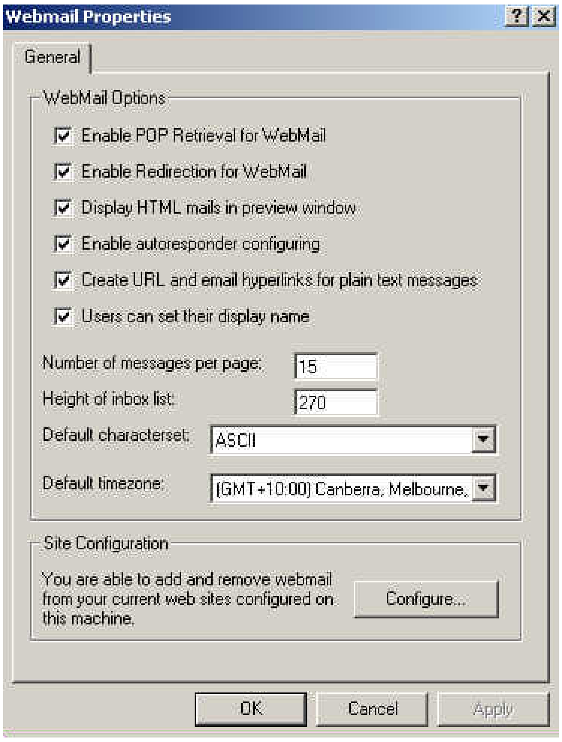
Congratulations, your new e-mail account has been activated and is ready for use.

If you have problems accessing mail, please contact your system administrator or refer to http://www.mailenable.com.

Figure 8-12 Web mail with "Jelly" skin

8.9.1 Configuring the Server

You are able to enable or disable various features of web mail via the MMC Administration console. Using the MMC Console, you can change whether your web mail users are permitted to configure POP retrieval accounts, redirect mail, or whether they view can view HTML formatted e-mails.



WebMail Options

☑ Enable POP Retrieval for WebMail

☑ Enable Redirection for WebMail

☑ Display HTML mails in preview window

☑ Enable autoresponder configuring

☑ Create URL and email hyperlinks for plain text messages

☑ Users can set their display name

Number of messages per page: 15

Height of inbox list: 270

Default characterset: ASCII

Default timezone: (GMT+10:00) Canberra, Melbourne,

Site Configuration

You are able to add and remove webmail from your current web sites configured on this machine.

Figure 8-13 Web mail properties

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

Setting	Explanation
Enable POP Retrieval for WebMail	This option determines whether POP Retrieval is able to be configured in the WebMail options tab.

Enable Redirection for WebMail	This option determines whether WebMail users are permitted to redirect their mail to alternate addresses.
Display HTML mails in preview window	This option determines whether HTML mails are shown in the preview window. Setting this option increases the system overhead of MailEnable.
Enable auto responder configuring	This option determines whether WebMail users are permitted to configure auto responses for their mailbox (for example: Out of Office automatic replies).
Create URL and email hyperlinks for plain text messages	This option instructs MailEnable to render mail messages and hyperlinks in plain text messages as URLs.
Users can set their display name	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 Webmail interface in the "options" page. 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 MMC or Webmail 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 webmail interface.
Number of messages per page	Determines the number of messages that will be displayed per page.
Height of inbox list	Sets the height of the inbox list in pixels.
Default characterset	The default characterset that will be used for users who have not set it themselves through their webmail options.
Default timezone	The default timezone to be used for users who have not set it themselves through their webmail options. This option is not used currently, as the timezone is taken from the client computer when they connect.

If you are using webmail on a Windows 2003 server, by default users are restricted to a maximum of 200 kilobyte upload. To change this, follow the instructions in Appendix 14.10.

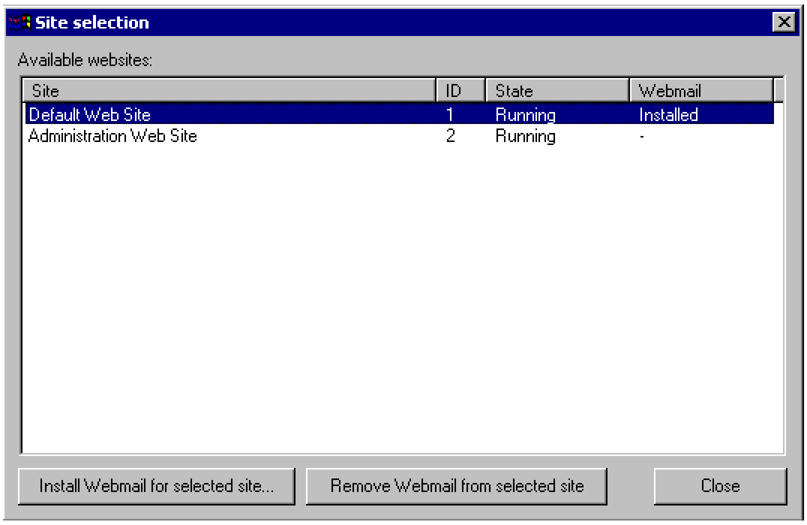
8.9.2 Configuring WebMail for Multiple Sites

MailEnable allows you to configure WebMail for each IIS Web Site hosted on your server. To enable WebMail on multiple web sites on your server, a virtual directory must be created for each Web Site.

A utility that does this can be found in the MMC in the following location:

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

This utility appears as follows:


Site selection
Install Webmail for selected site...
Remove Webmail from selected site
Close

Available websites:

Site	ID	State	Webmail
Default Web Site	1	Running	Installed
Administration Web Site	2	Running	-

Figure 8-14

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

8.9.3 Time zone

Since your web server is accessible by users throughout the world, the server needs to adjust the displayed date of the messages in a user's folder to properly reflect the time relative to their location. For example, if a user in Australia was using web mail on a server in the United States, they would want to see their inbox list displayed with the received date of the messages in their local time instead of a US time.

To do this, the web mail browser sends to the server the time zone offset configured on the client computer. If the client computer does not have the correct time zone configured, they will not see the messages with the correct times.

8.9.4 Character sets

In order for the server to know what character set a user is entering their email in, the user needs to specify this in their options once they log into web mail, unless the option has been preset for all users with the web mail administration. By default the character set is US-ASCII which does not cater for extended characters. If emails that have been sent from web mail and are missing extended characters or they are displayed incorrectly, it could mean that the user has not set their character set.

8.9.5 Web mail restrictions

Web mail is very server intensive compared to the other components in MailEnable. This is due to it processing all the emails on the server instead of the client. Decoding attachments, parsing HTML to strip out possibly troublesome scripts, and other items can increase server load. To combat this, the web mail will impose certain restrictions:

Only a maximum of 1000 messages will be listed for any folder. Every time a user displays their inbox or mail folder the server needs to read each message, this can cause high disk usage. Web mail users should purge older messages, or move them to folders with a smaller amount of messages.

If a message is taking too long to process in order to view, MailEnable will stop trying to process and display what it has. Likely this will only occur with corrupted emails.

The attachment icon for the list of messages in a folder may not always be accurate. To check whether a file has an attachment, the web mail only reads the header portion of a message. This is done to avoid a lot of disk IO reading messages in order to display a message list.

8.10 Web Administration

The web administration information in this manual includes configuration and the various server options. For details on using the web administration, please check the MailEnable Web Administration User Guide within the **Start Menu >MailEnable Program Group >Documentation.**

MailEnable Professional includes Web Administration. If you have authenticated as an Admin user, you will be able to manage users/mailboxes, lists, groups, and domains. If you are hosting multiple post offices (lets say one per customer or company), each company can manage their own configuration.

Some of the features are:

- Works with IIS4.0 and greater, allowing easy integration
- Manage domain related information
- Manage the creation of email addresses
- Manage email lists and groups
- Custom skins, leveraging skins from WebMail.

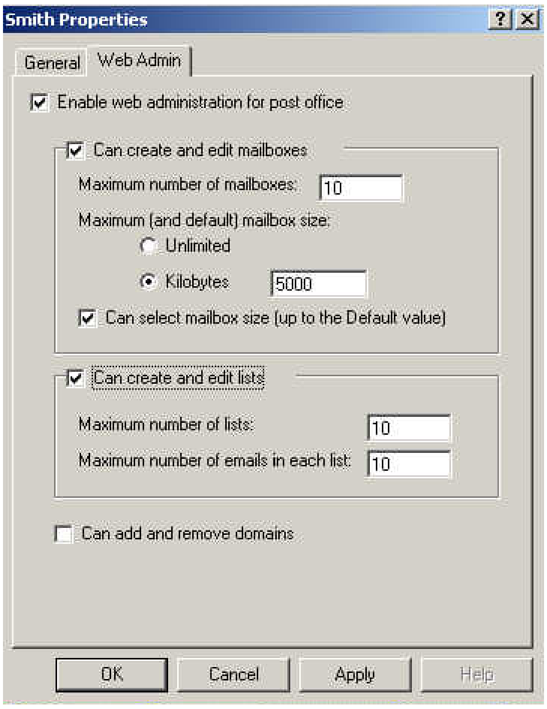
When editing lists via the Web Administration interface you have the added option of editing and adding alternate List addresses.

8.10.1 Configuring the Server

Web Administration is installed as an optional MailEnable component. The MailEnable installation program is configured to have it installed by default (hence it will only not be installed if you changed the options when you installed MailEnable). You can validate whether web administration is installed by reviewing your MailEnable Diagnostic Report.

You need to ensure that web administration is enabled for a post office before it can be administered. This is done through the administration program.

1. Expand the MailEnable Management->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. Click the Web Admin tab at the top of the window to enter the property page for the web administration.
4. To enable web administration, select the **Enable web administration for post office** checkbox.



Smith Properties

☑ Enable web administration for post office

☑ Can create and edit mailboxes

Maximum number of mailboxes: 10

Maximum (and default) mailbox size:

○ Unlimited

● Kilobytes 5000

☑ Can select mailbox size (up to the Default value)

☑ Can create and edit lists

Maximum number of lists: 10

Maximum number of emails in each list: 10

□ Can add and remove domains

Figure 8-15

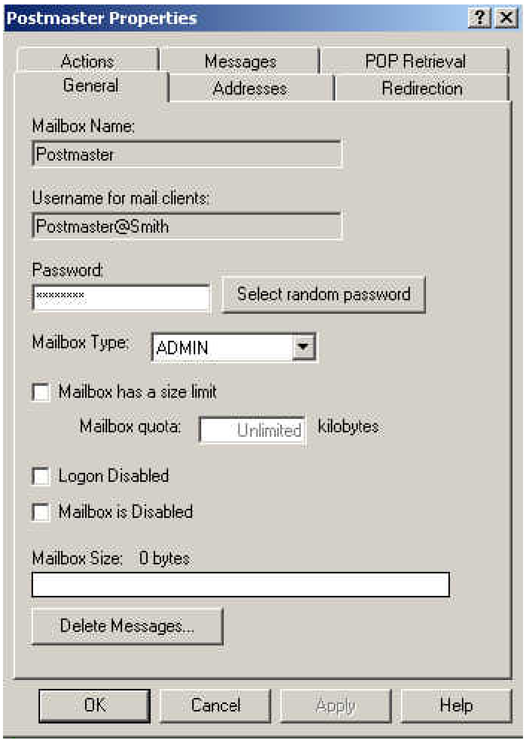
You are now free to configure the various options that the post office administrators can have access to. It is recommended not to give users the ability to add and edit domain properties, since changes or additions can cause problems with mail delivery.

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

5. Right click on the desired mailbox and access the mailbox properties

6. Select **ADMIN** from the drop down list labelled **Mailbox Type**.

You can see the option to select in the following diagram:



Mailbox Name: Postmaster

Username for mail clients: Postmaster@Smith

Password: ********

Mailbox Type: ADMIN

☐ Mailbox has a size limit

Mailbox quota: Unlimited kilobytes

☐ Logon Disabled

☐ Mailbox is Disabled

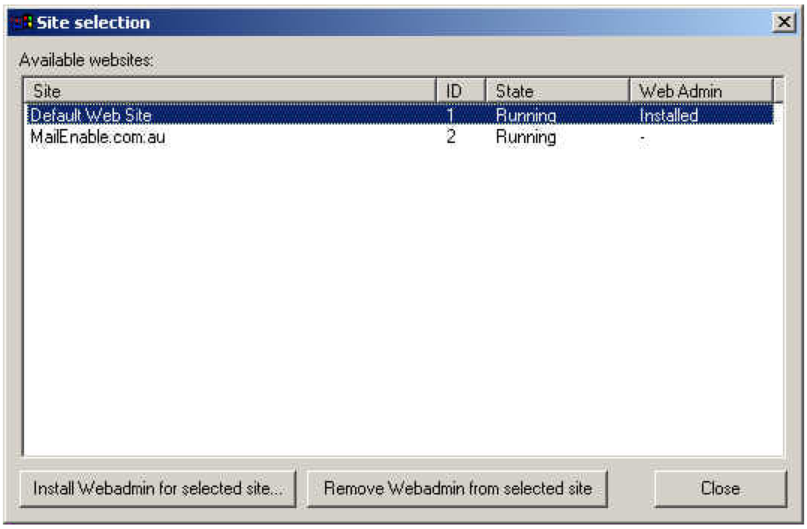
Mailbox Size: 0 bytes

Figure 8-16

You are also able to configure which IIS Web Sites can access WebMail. If you wish to enable WebAdmin access from multiple web sites on your server, a virtual directory can be created under each of the sites you on your server. A utility that does this can be found in the MMC in the following location:

MailEnable Management | Servers | localhost | Services | WebAdmin and right click and select properties on "Webadmin" to open the webadmin properties window. Next navigate to the "General" tab and click on the "Configure" button in the site configuration section.

This utility appears as shown in the following example:


Site selection
Install Webadmin for selected site...
Remove Webadmin from selected site
Close

Available websites:

Site	ID	State	Web Admin
Default Web Site	1	Running	Installed
MailEnable.com.au	2	Running	-

Figure 8-17 Site Selection Utility

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.

8.10.2 Accessing WebAdmin

Once installed, web administration can be accessed from the following URL:

Example: http://*HostName*/meadmin

In place of the *HostName* in the above example, you should use the server name as defined in DNS or under IIS. You can also use the IP address of the machine.

When you browse to this location, you will be presented with the Web Administration logon screen.

Note: Remember, in order to allow someone to log onto the web administration, you need to have created a mailbox in the MailEnable administration application, and set the mailbox as "ADMIN". You should also ensure that the username is formatted as: *mailboxname@postofficename*.

8.10.3 Troubleshooting

8.10.3.1 I can't see the web administration property page?

This is usually either because you are accessing the administration program using the MailEnable Administrator shortcut, instead of the MailEnable Professional shortcut. If you still can't see the web administration, you can extend your currently open administration application by following the steps below.

1. Open the MailEnable administration application
2. From the Console menu, select Add/Remove Snap-in…
3. A window will appear. Select the **Extensions** tab at the top.
4. From the top drop down list, labeled Snap-ins that can be extended, select MailEnable Management.
5. Select the **Add all extensions** checkbox
6. Select **OK**
7. From the **Console** menu, select **Save**
8. You should be able to right click on a post office, select **Properties** from the pop-up menu, and see the **Web Admin** tab.

8.10.3.2 When I try to log in, it always comes up as invalid user!

Make sure that the mailbox is set to "ADMIN". Then make sure that the post office has been enabled for web administration.

8.11 COM Component

This easy-to-use component can be used in any application that supports COM. For example, you can use this component 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 you to easily send email 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

8.11.1 Configuring the Server

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.

IMPORTANT: If you intend to use the COM component, you will need to ensure that you have granted the appropriate relay rights to the application that is intending to use the COM component.

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

8.11.2 Using the Component

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.

8.11.2.1 Properties

Setting	Description
AttachmentFilename	The name of the file that you wish to add as an attachment.
AttachmentName	The name you wish to call the attachment.
AuthenticationMode	Allows you to use SMTP authentication. 0 = No SMTP authentication 1 = SMTP authentication. You must populate the Username and Password properties in order to authenticate
ContentType	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;".
ErrorString	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.
MailBCC	This is list of email addresses to BCC the email to. When using multiple email addresses, separate them with a semi-colon ";".
MailCC	This is list of email addresses to CC the email to. When using multiple email addresses, separate them with a semi-colon ";".
MailCCDisplayName	This is list of email addresses that are the display name corresponding to the email address you have set in MailCC. This list is optional. When using multiple email addresses, separate them with a semi-colon ";".
MailFrom	This is the email address of the person you want as the sender.
MailFromDisplayName	The display name of the from MailFrom email address.
MailTo	The email address to send the email to. If you wish to send to multiple email addresses, separate the emails with a semi-colon ";".
MailToDisplayName	This is the display name that will be shown as the To address. It is usually the full name of the person you are sending to (i.e. "John Smith")
Messagebody	The message contents.

MessageBodyText	An optional property used to force the content for the textual content of the message. If the property is not set, MailEnable will generate a textual version of the message from the HTML content supplied (assuming the ContentType is set as text/html.
Password	Password to be used for SMTP authentication.
Server	The email server to connect to. If none is supplied it will try to connect to the local machine.
ServerPort	The port to connect to. The default is 25.
Subject	The subject of the email message.
Username	Username to be used for SMTP authentication

8.11.2.2 Methods

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

By setting the *ContentType* value to text/html, the component will generate a HTML and Plain Text representation of your 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*.

8.11.3 Examples

8.11.3.1 Sending an HTML email from an ASP page

```
<%
Dim oMail
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 = "<html><body><h1>Hello there,<BR>Welcome to our new
service.</h1></body></html>"

oMail.SendMessage

%>
```

8.11.3.2 Sending an email with an attachment

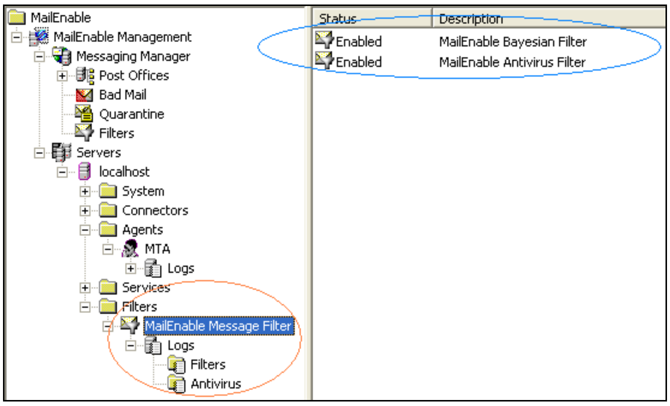
```
<%

Dim oMail

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"

oMail.Subject = "New update information"

oMail.MessageBody="Find the new info attached.”

oMail.SendMessage

%>
```

9 Message Filtering

Message Filtering allows you to filter messages that pass through MailEnable. Filtering is configured on a global level in Professional Edition. Global filters are processed by the MTA and will check every message going through the server. As the message is parsed, the criteria for all the filters are enumerated.. The filter compiles a list of all the actions that should be taken and executes them in that order. There are no copies of the messages made for each action, so if the first action is 'delete' any remaining actions will not complete. These actions can be tracked using the MEFilter logs.

9.1 Global Message Filters

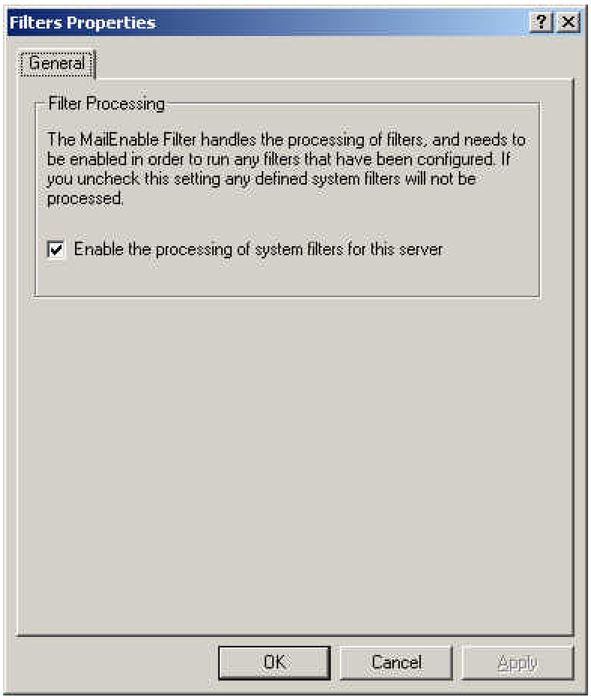
Global Message Filters are configured under the **Servers|localhost|Filters|MailEnable Message Filter** section of the administration program. This section of the MailEnable Management Console is outlined below:



Status	Description
Enabled	MailEnable Bayesian Filter
Enabled	MailEnable Antivirus Filter

Figure 9-1 Filtering Options within Management Console

When the MailEnable Message Filter branch is selected, the filters are listed in the right hand panel. You can configure each of these by right clicking on them and selecting Properties, to enable or disable the filters as shown in the diagram below.



The MailEnable Filter handles the processing of filters, and needs to be enabled in order to run any filters that have been configured. If you uncheck this setting any defined system filters will not be processed.

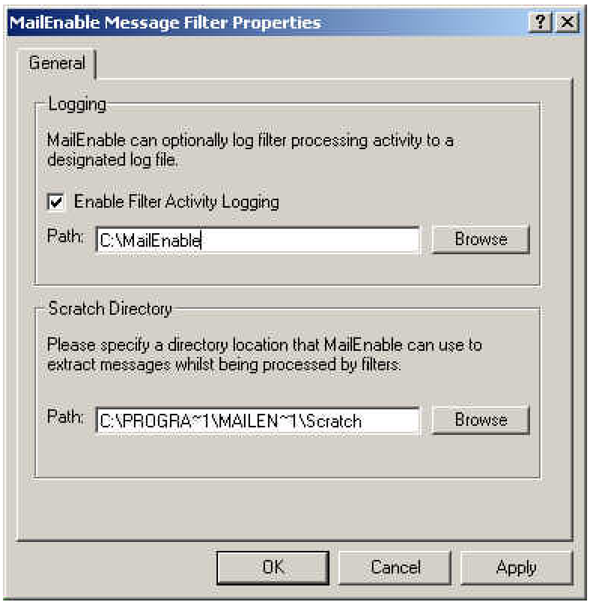
☑ Enable the processing of system filters for this server

Figure 9-2 Enable system filters

9.1.1 MailEnable Global Message Filter Properties

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

The MailEnable Message Filter Properties window is shown below:



MailEnable can optionally log filter processing activity to a designated log file.

☑ Enable Filter Activity Logging

Path: C:\MailEnable

Please specify a directory location that MailEnable can use to extract messages whilst being processed by filters.

Path: C:\PROGRA~1\MAILEN~1\Scratch

Figure 9-3 MailEnable Message Filter Properties

The configurable properties for the MailEnable Message Filter are outlined in the following table:

Setting	Description
Activity Log	This setting allows you to 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.
Scratch Directory	The Scratch directory is used by MailEnable 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 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.

9.1.2 Antivirus Filter Settings

The antivirus filter allows you to use command line virus checkers on emails that as they pass through the MailEnable server either for relay or for delivery to local mailboxes. You need a valid server license if you wish 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

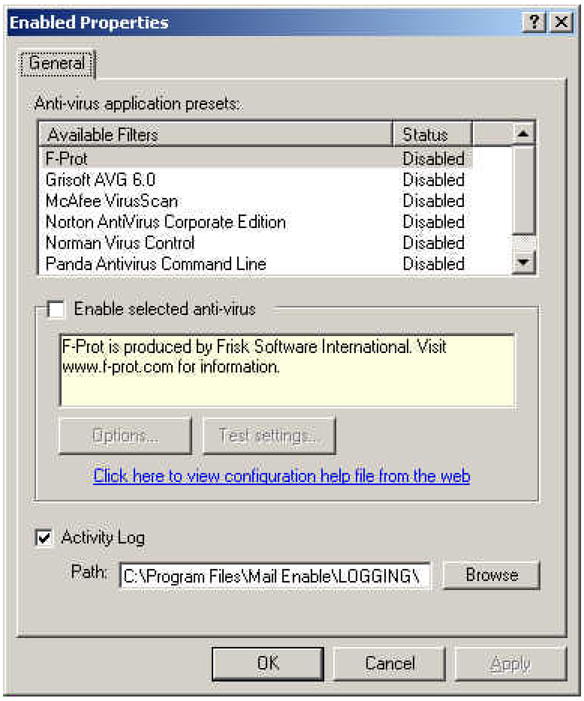
- Grisoft AVG

An entry is logged to the MTA Activity log whenever a virus is detected in an email. The entry will show what the service has done to the email (whether it has cleaned, deleted, etc.) For more information on configuration of specific antivirus software packages, please see section 14.8 Antivirus configuration.

9.1.2.1 Configuring the Server

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

Once you have configured the Antivirus agents to be used by your server, you can then use them within your specific filters.



Anti-virus application presets:

Available Filters	Status
F-Prot	Disabled
Grisoft AVG 6.0	Disabled
McAfee VirusScan	Disabled
Norton AntiVirus Corporate Edition	Disabled
Norman Virus Control	Disabled
Panda Antivirus Command Line	Disabled

☐ Enable selected anti-virus

F-Prot is produced by Frisk Software International. Visit www.f-prot.com for information.

☑ Activity Log

Path: C:\Program Files\Mail Enable\LOGGING\

Figure 9-4 Antivirus agent configuration

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

Setting	Description
Enable antivirus/filter support	This will enable or disable all antivirus and other filters that may be installed for MailEnable.
Enable selected antivirus/filter	This is to indicate that the currently selected virus checker or filter will scan emails. You are able to enable more than one antivirus/filter at once.
Options	Allows you to set the advanced options for the currently selected antivirus application.

Test	This will test 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, you can check whether the antivirus program is functioning by running the MTA in debug mode.

9.1.2.2 Antivirus Options

Setting	Description
Program Path	This is the path to the virus checker application. You should only select the command line scanner for the antivirus application (the presets in MailEnable will point to the correct application).
Command line arguments	The command line arguments that are used to run the antivirus scanner. There should be no need to change these options unless you are adding your own.
Command line arguments will delete attachment	Selecting this will require that the command line scanner delete any infected attachment. Some virus scanners cannot remove zip files that are infected with viruses using this option.
Return code will be checked against this list	This option will make MailEnable check the return code from a command line scanner. If the return code matches the return codes items in the list, then the attachment is detected as a virus. You cannot use any command line argument that deletes the attachment when you select this option. Use the "any" keyword in order to check for any return code (i.e. other than 0)
Return code check	You can also choose to detect the attachment as a virus if the return code is a number other than those in the list.

Note: 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 you are probably not sending it to someone who is infected.

Note: You should consider that virus-scanning email adds more load on your server. This is because the antivirus filter must extract and test every attachment that goes through the server. You should 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. You should consider that each transfer thread could potentially mean a different concurrent instance of the agent's command line scanner.

9.1.3 Bayesian Filter Settings

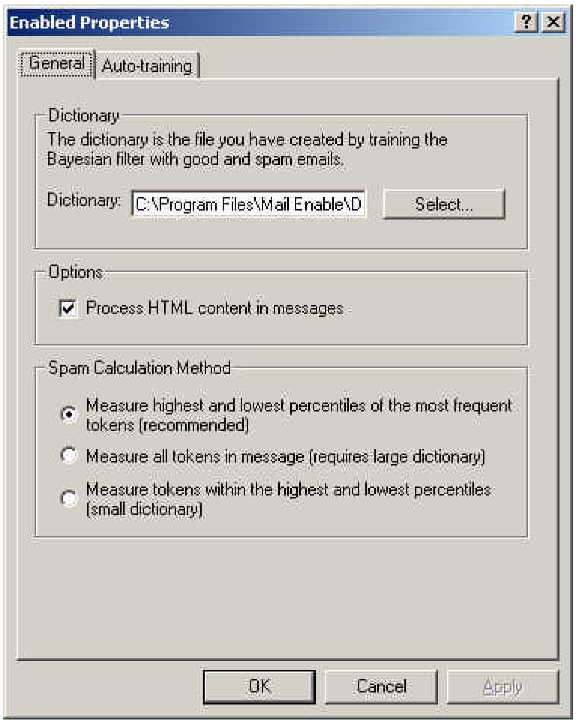
Bayesian Filtering is founded on having two pools of messages (Bad and Good) and creating a word dictionary that outlines the frequency of tokens (words or text snippets) within these messages. This effectively allows MailEnable to analyze messages and provide a probability of a message being spam as a new message can have its tokens compared against this dictionary. For examples, 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 "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 very much determined by having good samples of spam and non-spam respectively. The process of compiling a dictionary from samples of spam and non-spam is called Training. MailEnable provides a command line utility that allows you to train the Bayesian Filter, or alternatively, the filter can be auto-trained.

MailEnable Dictionaries are typically located under Program Files\Mail Enable\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.

MailEnable's Bayesian Filter is configured under the MailEnable MTA Message Filter. Once you have created the dictionary, you need only configure the location and some tuning parameters for measurement.

The options for configuring the filter are outlined as follows:



Dictionary

The dictionary is the file you have created by training the Bayesian filter with good and spam emails.

Dictionary: C:\Program Files\Mail Enable\D

Options

☑ Process HTML content in messages

Spam Calculation Method

● Measure highest and lowest percentiles of the most frequent tokens (recommended)

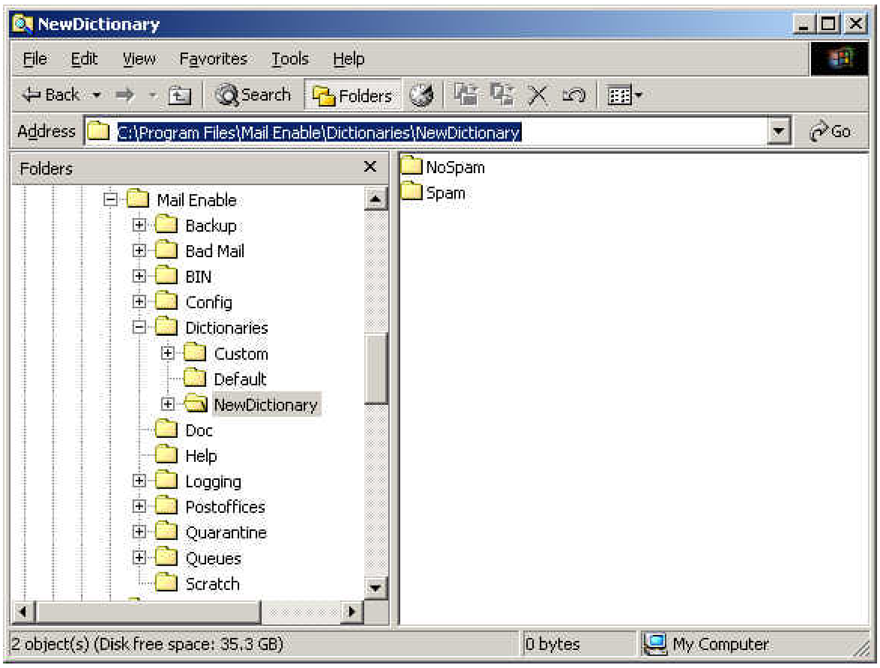
○ Measure all tokens in message (requires large dictionary)

○ Measure tokens within the highest and lowest percentiles (small dictionary)

Figure 9-5 Options for configuring Bayesian Filtering

9.1.3.1 Creating a Dictionary

Creating a dictionary involves creating a new directory under the MailEnable Dictionaries folder. You should then create directories called **Spam** and **NoSpam** under this directory. The following diagram outlines how this should look when viewed with Explorer.



Address C:\Program Files\Mail Enable\Dictionaries\NewDictionary

2 object(s) (Disk free space: 35.3 GB) 0 bytes

Figure 9-6 Creating a dictionary

The next step is to copy MAI files from your post office into each of these folders depending on whether the messages are Spam or NoSpam. A simple way to compile these message libraries is to instruct users to create folders called Spam and NoSpam and to dump messages into these folders. You can then write a DOS script that uses XCopy to add these messages into your dictionaries Spam and NoSpam folders.

Ideally, you should have at least 1,000 messages in each of these folders. Typical ranges are between 1,000 and 10,000 in each.

Once you have spam and No Spam messages in these folders, you need to use the Dictionary Management Utility to construct the dictionary file.

Filtering dictionaries can be constructed as either XML or TAB delimited files.

XML files load slower, but may be more desirable if you need to externally manage the dictionary in some way. 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>
```

MailEnable provides a command line filter that can be used to manage Spam/Non-Spam dictionaries. The File is called MESPAMCMD.Exe and is located in your MailEnable BIN directory.

```
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
```

```
[m] = Merge Spam and NoSpam folders into nominated Dictionary

[r] = Notifies the spam filter to reload the dictionary

[p] = Prunes the Dictionary to allow insertion of more words

Example:

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

An example command line for compiling a dictionary based on the example shown follows:

```
MESPAMCMD -c C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\MailEn~1.TAB
C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\Spam
C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\NoSpam
```

Note: The dictionary construction utility must use short style file paths (i.e.: the paths cannot contain spaces)

9.1.3.2 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
```

9.1.3.3 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\1A38DF23D30845E0B5FF51530A266.MAI
```

9.1.3.4 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 if you want 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
```

9.1.3.5 Reload a Dictionary

If you make changes to a dictionary while the spam filter is running, it will not automatically reload it unless it is notified. You can use the –r option to tell the spam filter to reload it.

```
MESPAMCMD -r
```

9.1.3.6 Pruning a Dictionary

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

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

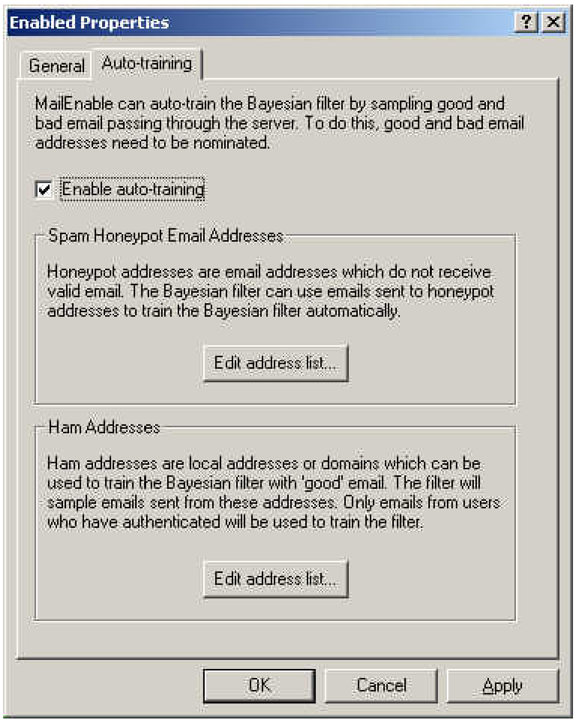
9.1.3.7 Auto-training

You have the option of auto-training the Bayesian filter dictionary using emails that are passing through the server. To do this the filter needs to take samples of both “ham” and “spam” emails.

By defining "honey pot" addresses, samples of spam email can be collected. "Honey pot” addresses are addresses that are deliberately published so that spammers will send to them. For example, spammers will scan your web site for published e-mail addresses and will send spam to these addresses. A means of publishing a “honey pot” address is to insert a mailto:HTML tag as hidden text in your contacts page. You can also subscribe the e-mail address to some “dubious” web sites (of course selecting the option not to be mailed or receive promotions, thereby receiving only unsolicited mail).

Desirable or legitimate e-mail is commonly referred to as “ham”. The ham addresses option is for valid email addresses of users that are used to sample valid email. You can specify the e-mail addresses to be considered for sampling legitimate mail under the MailEnable 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.

In summary, assuming you have enabled the auto-training mode for Bayesian Filtering, and you have defined “honey pot” and “ham” addresses for sampling, MailEnable will dynamically amend its database accordingly. The changes to the database are held in memory until the MTA service is stopped or the allocated memory becomes full (in which case an automatic update and consolidation of the permanent dictionary on disk is made).



MailEnable can auto-train the Bayesian filter by sampling good and bad email passing through the server. To do this, good and bad email addresses need to be nominated.

☑ Enable auto-training

Spam Honeypot Email Addresses

Honeypot addresses are email addresses which do not receive valid email. The Bayesian filter can use emails sent to honeypot addresses to train the Bayesian filter automatically.

Ham Addresses

Ham addresses are local addresses or domains which can be used to train the Bayesian filter with 'good' email. The filter will sample emails sent from these addresses. Only emails from users who have authenticated will be used to train the filter.

Figure 9-7 Auto training Bayesian Filtering settings

9.2 Creating a global filter

To add a new filter, you should expand the Messaging Manager and right click on Filters in the administration program and select **New|New Filter**

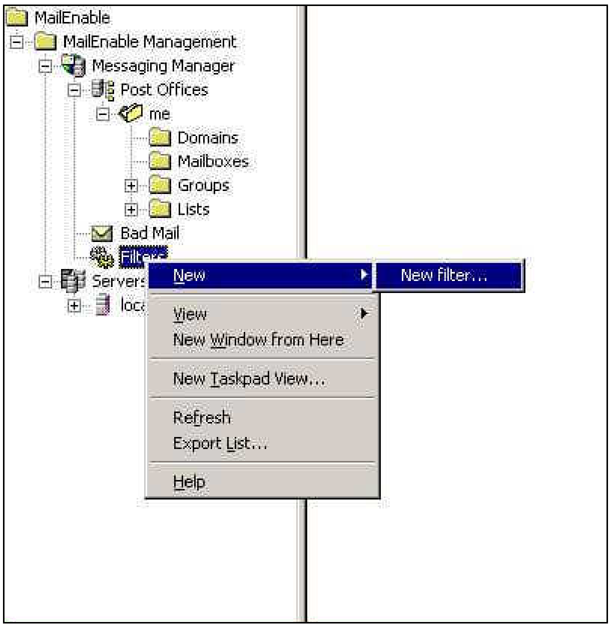
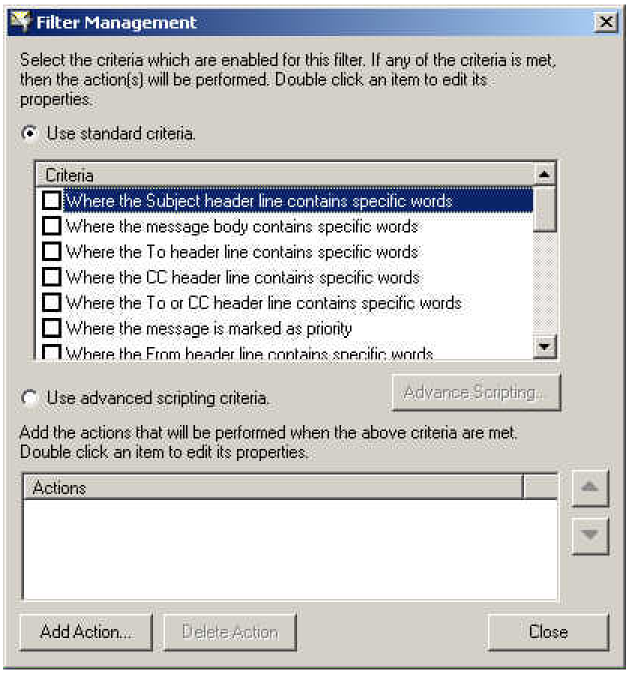


Figure 9-8 Adding a new filter

You will see a dialog box **Add new filter item**. To enable the filter you must tick the **Filter is enabled** tick box where you have the option to name the filter.

9.2.1 Standard Filter Criteria

Once a filter has been added, it will appear in the list of Filters. If you right click on the filter, you will be able to manage the associated criteria and actions by clicking **Manage**. The following screen will be displayed.



Filter Management

Select the criteria which are enabled for this filter. If any of the criteria is met, then the action(s) will be performed. Double click an item to edit its properties.

● Use standard criteria.

Criteria

- □ Where the Subject header line contains specific words
- □ Where the message body contains specific words
- □ Where the To header line contains specific words
- □ Where the CC header line contains specific words
- □ Where the To or CC header line contains specific words
- □ Where the message is marked as priority
- □ Where the From header line contains specific words

○ Use advanced scripting criteria.

Add the actions that will be performed when the above criteria are met. Double click an item to edit its properties.

Actions

Figure 9-9 Editing filter criteria

By double-clicking on the criteria, you can 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 in by ticking or un-ticking the box as shown above.

For filter criteria that rely on word or email address matching eg: "**Where Message Body contains specific words**" or "**Where the'To' header line contains specific words**", wildcards can be used. Wildcards (*) can be used to pickup a specific word that could be hiding in other words or characters (e.g. Filter identifies the word "porn" that's in the word Pornographic or 123porn1121). Wildcards (*) can also be used to cover a range of email addresses. The wildcard scenario can be used well 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.

9.2.1.1 Where the Subject header line contains specific words

You are able to 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 9.2.2 Filter Actions) is completed.

9.2.1.2 Where Message Body contains specific words

You are able to add and remove specific words to the criteria list by clicking the "Add" button. This filter is good for picking up specific words in the body of the message (e.g. Viagra).

9.2.1.3 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.

You can enter 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 column - ensuring that no character spaces are contained in the entered line e.g.. test@mailenable.com;test2@mailenable.com.au

9.2.1.4 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".

9.2.1.5 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.

9.2.1.6 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.

9.2.1.7 Where the message is marked as priority

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

9.2.1.8 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.

9.2.1.9 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 click 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.

9.2.1.10 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.

9.2.1.11 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 section 14.8 for information on configuring the antivirus plug-in.

9.2.1.12 All messages

This criteria is processed for all messages.

9.2.1.13 Where the SPF test return results matching

This criteria enumerates the SPF test performed by the SMTP Connector and returns a nominated result.

9.2.1.14 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.

9.2.1.15 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.

9.2.1.16 Where the message is associated with this postoffice

Allows you to specify the owning post office of the transaction. MailEnable will attempt to allocate an “Owning” post office for each message.

9.2.1.17 Where the message came from this MailEnable connector

Enumerates the connector that the message is being delivered from.

9.2.2 Filter Actions

A filter action is an event that occurs when a filter criteria is met. To create a filter action, select the filter that you wish to create an action for. Select the criteria that you wish to create an action for. Click the **Add action** button to add to the actions list. This will open an action list window. Click on 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 you wish 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.

9.2.2.1 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. If you wish to send to bad mail, and not deliver to the mailbox, create a **Delete Message** action to occur after the Copy to BadMail.

9.2.2.2 Copy to Quarantine

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

9.2.2.3 Delete message

Deletes the message.

9.2.2.4 Notify Sender

This action allows you to send a notification message to the sender of the message. MailEnable’s Message Filter allows you to insert system tokens into notification message templates. When you define an action to notify a user with a message, you can specify a Message Template for the notification.

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, if you had critieria for a filter that specified to scan for viruses, only the "All" Tokens and "Antivirus" tokens would be available within the notification template.

Token Name	Description	Criteria Populator
ME_ FILTERNAME	Contains the name of the filter that executed the call	All
ME_ ACTIONDESC	The description of the current action that	All
ME_MSG	The System Filename of the message	All
ME_CON	The System Connector associated with the message	All
ME_IP	The originating IP Address of the message	All
ME_ACCOUNT	The Account or Post office "owning the message"	All
ME_SENDER	The sender of the message	All
ME_ AVRESULT	The Antivirus Scanning Agent return value	Antivirus Scanning
ME_AVACTION	The action performed by the Antivirus agent when scanning	Antivirus Scanning
ME_AVAGENT	The System name of the AV Agent that was used to scan the message	Antivirus Scanning
ME_BADMAILSENDER	The System BadMail Sender as defined under the SMTP connectors properties	All
ME_MID	A System generated MessageID appropriate for the MessageID header	All
ME_HEADERS	The RFC 822 headers of the original message	All
ME_SZ	The Size of the Original Message	Message Size Critieria
ME_SZL	The Size Limit of the Original Message	Message Size Critieria

9.2.2.5 Notify Recipient

This filter action sends a message to the recipient. You may wish to send a notification email to the recipient to let them know that an action has occurred on an inbound email. For example, if you delete a message because an attachment is an executable, you may wish to notify the recipient that this has happened.

You can also use the same notification options as outlined when performing the Notify Sender action.

9.2.2.6 Notify Address

This will send a notification message to a specified address.

9.2.2.7 Forward to Address

This filter action forwards the email to an email address.

9.2.2.8 Execute Application

Allows you to execute an application on the email. Since the MTA may execute an action concurrently, make sure that the application you specify can have multiple instances running. If not, you will need to change the MTA service to only use one thread.

9.2.2.9 Add header

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

9.2.2.10 Stop Processing Filters

This action stops the processing of any more filter actions.

10 MailEnable Advanced Scripting

10.1 Overview

MailEnable's Advanced Filter Scripting provides an extremely flexible and extensible means of scripting complex filters. The scripting language similar to Microsoft VBScript and includes some custom in-built functions for validating criteria. The variable called *Filter Result* is used as the return value from the MailEnable filter and can be set at any time. A *Filter Result* value of 0 indicates that the filter criteria was not met while a value of 1 indicates that the filter criteria was met. The script can be terminated at any time using the *Quit* command.

10.2 Example 1: Simple Script

An example script for an advanced MailEnable filter is outlined below:

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

10.3 Example 2: More Complicated Script

A more complicated example script for an advanced MailEnable filter is outlined below:

```
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
                Quit
        End If
End If
```

This script is similar to the one above, 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.

11 Configuration of Email Clients

In order to read and send email from an email client such as Eudora, Microsoft Outlook or Outlook Express you need to configure them to connect to MailEnable. The POP3 and SMTP server should be the server name you are running MailEnable on. 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. You will not be able to retrieve email if you do not use the full username, unless you have specified a default post office.

11.1 Netscape Messenger

1. Start Netscape
2. Select Edit then Preferences from the menu bar
3. Click on the '+' symbol on the right of Mail & Group
4. Click Mail Server option
5. Enter values in the input boxes
6. If you don't want to re-enter your password every time you check email click More Options, then tick Remember mail password
7. Click on Identity
8. Type in your full name or business name in Your Name: input box
9. Type in the email address you would like people to contact you with (e.g. info@mydomain)
10. Type in your reply email address (e.g. info@mydomain)
11. Click OK to accept new settings.

11.2 Microsoft Outlook Express

1. Open Outlook Express.
2. Click on 'Tools | Accounts
3. Click on the 'Mail' tab.
4. On the right side, click on 'Properties'.
5. Now click 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. Eg: mailbox@postoffice. If you have enabled SMTP Authentication on your server, you should check the option instructing Outlook Express that your outbound server requires authentication. The checkbox to do this is labeled **my server requires authentication**.

11.3 Microsoft Outlook

1. Access the Tools | Accounts menu.
2. Select the Mail tab and click Add | Mail.
3. Enter an appropriate display name.
4. Enter your e-mail address.
5. Specify your incoming and outgoing mail servers. Eg: mail.[mydomainname].com.
6. Specify your Account Name and Password. Your Account Name is formatted as mailboxname@postofficename.

7. Specify how you connect to your mail server.
8. Click Finish

11.4 Mozilla Thunderbird

1. With Mozilla Thunderbird you 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 button.
4. Select the Email account option in the Account Wizard window that appears and select the Next button.
5. Enter your name and e-mail address and select Next.
6. Select whether you wish to use POP or IMAP protocol and enter the incoming email mail servers. Eg: mail.[mydomainname].com, then select Next.
7. Specify your Incoming User Name and select Next. Your User Name is formatted as mailboxname@postofficename.
8. Enter the account name for this account you have configured and select Next.
9. Select Finish
10. To now set the outgoing mail server details:
11. Access the Tools | Account Settings menu.
12. Select the Outgoing Server (SMTP) item in the listbox
13. Enter the server name of the outgoing mail server. E.g.: mail.[mydomainname].com
14. Enable the User name and password checkbox and enter your User Name. Your User Name is formatted as mailboxname@postofficename
15. For the Use secure connection option, have No selected.
16. Select OK to save changes.

11.5 Configuring Clients for HTTPMail

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

Setting	Value
Protocol:	HTTP
Provider:	Other
Incoming mail (POP3, IMAP or HTTP) server:	http://machinename:8080/MEHTTPMail

Example:

From Outlook (in the example, Outlook Express) choose **Tools | Accounts.** from the Menu. The following Dialog will be displayed:

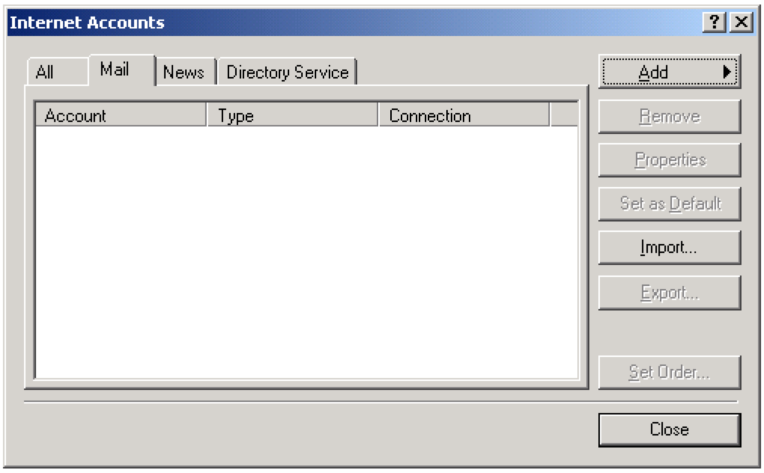
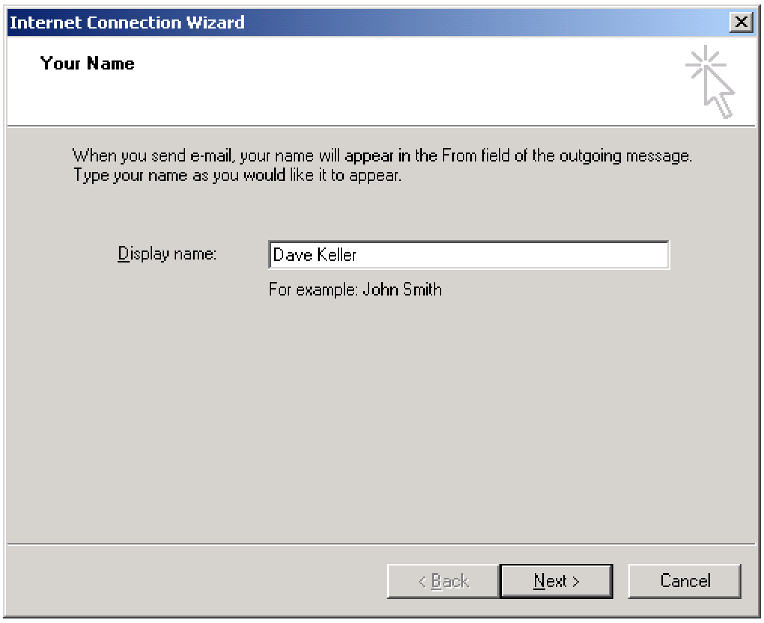


Figure 11-1

Select **Add | Mail..**. and enter your Display Name (Friendly Name) in the following Dialog; then click **Next**.



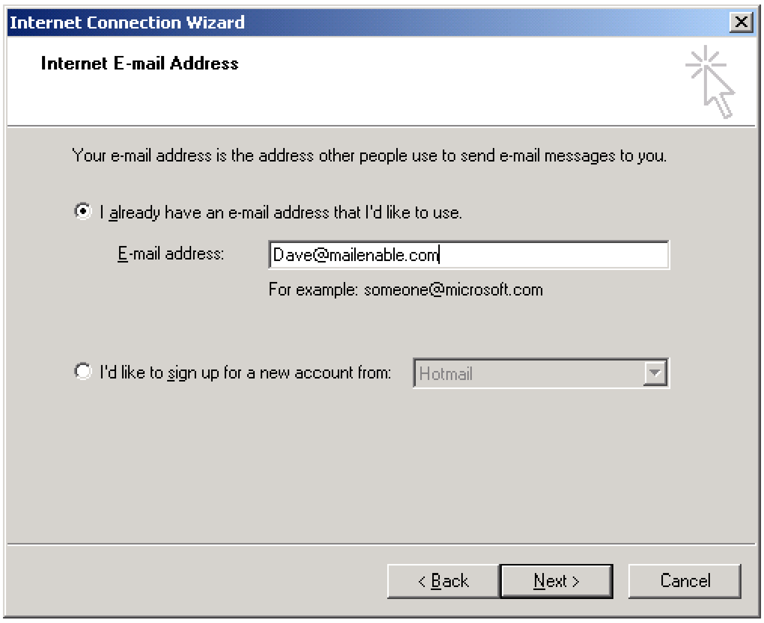
When you send e-mail, your name will appear in the From field of the outgoing message. Type your name as you would like it to appear.

Display name: Dave Keller

For example: John Smith

Figure 11-2

Enter your e-mail address; then click **Next**.


Internet Connection Wizard

Internet E-mail Address

Your e-mail address is the address other people use to send e-mail messages to you.

● I already have an e-mail address that I'd like to use.

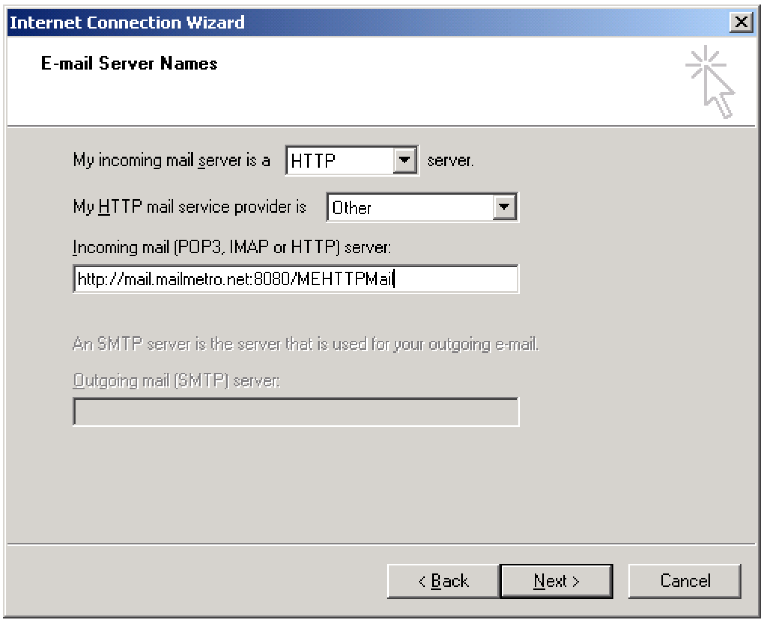
E-mail address: Dave@mailenable.com

For example: someone@microsoft.com

○ I'd like to sign up for a new account from: Hotmail

Figure 11-3

Select **HTTP** as your mail server type and enter the URL to the HTTPMail service (http://machinename:8080/MEHTTPMail); then click **Next**.


Internet Connection Wizard

E-mail Server Names

My incoming mail server is a HTTP server.

My HTTP mail service provider is Other

Incoming mail (POP3, IMAP or HTTP) server:

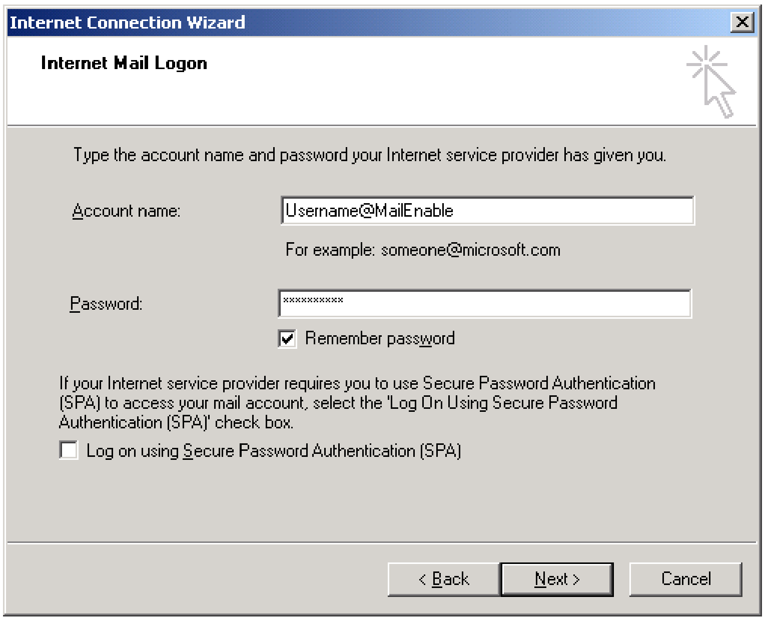
http://mail.mailmetro.net:8080/MEHTTPMail

An SMTP server is the server that is used for your outgoing e-mail.

Outgoing mail (SMTP) server:

Figure 11-4

Enter your MailEnable credentials; then click **Next**.



Type the account name and password your Internet service provider has given you.

Account name: Username@MailEnable

For example: someone@microsoft.com

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

☑ Remember password

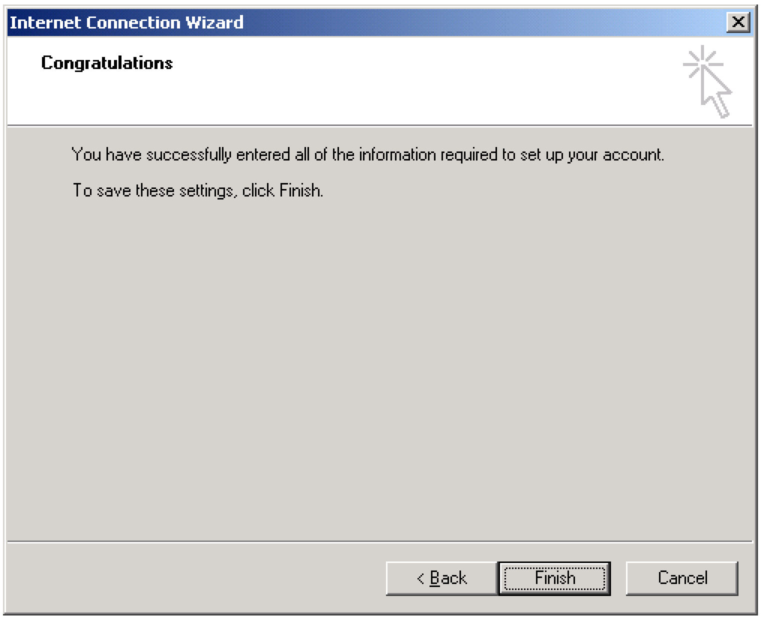
If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your mail account, select the 'Log On Using Secure Password Authentication (SPA)' check box.

□ Log on using Secure Password Authentication (SPA)

Figure 11-5

Note: Since HTTPMail is an authenticated service, you will need to use your usual account credentials when prompted. (i.e.: User@ Your Account/Postoffice)

The wizard has now completed; please click **Next**.



You have successfully entered all of the information required to set up your account.

To save these settings, click Finish.

Figure 11-6

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.

12 Logical Architecture and Message Flow

The diagram at the following link 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 (which are explained under their own sections).

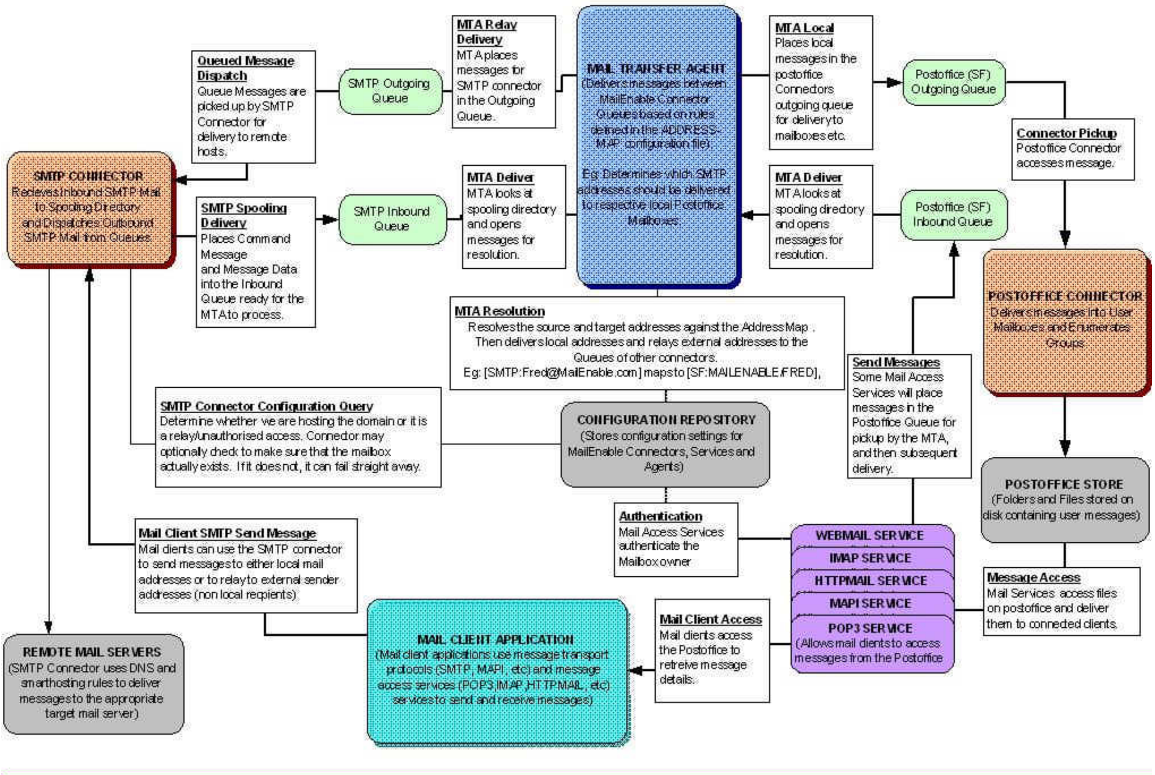

MTA Relay Delivery
MTA places messages for SMTP connector in the Outgoing Queue.
MAIL TRANSFER AGENT
(Delivers messages between MailEnable Connector Queues based on rules defined in the ADDRESS-MAP configuration file).
Eg Determines which SMTP addresses should be delivered to respective local Postoffice Mailboxes.
MTA Local
Places local messages in the postoffice Connectors outgoing queue for delivery to mailboxes etc.
Queued Message Dispatch
Queue Messages are picked up by SMTP Connector for delivery to remote hosts.
SMTP Outgoing Queue
Postoffice (SF) Outgoing Queue
Connector Pickup
Postoffice Connector accesses message.
SMTP CONNECTOR
Recieves Inbound SMTP Mail to Spooling Directory and Dispatches Outbound SMTP Mail from Queues
SMTP Spooling Delivery
Places Command Message and Message Data into the Inbound Queue ready for the MTA to process.
SMTP Inbound Queue
MTA Deliver
MTA looks at spooling directory and opens messages for resolution.
MTA Deliver
MTA looks at spooling directory and opens messages for resolution.
Postoffice (SF) Inbound Queue
POSTOFFICE CONNECTOR
Delivers messages into User Mailboxes and Enumerates Groups
MTA Resolution
Resolves the source and target addresses against the Address Map . Then delivers local addresses and relays external addresses to the Queues of other connectors.
Eg: [SMTP:Fred@MailEnable.com] maps to [SF:MAILENABLE/FRED],
Send Messages
Some Mail Access Services will place messages in the Postoffice Queue for pickup by the MTA, and then subsequent delivery.
SMTP Connector Configuration Query
Determine whether we are hosting the domain or it is a relay/unauthorised access. Connector may optionaly check to make sure that the mailbox actually exists. If it does not, it can fail straight away.
CONFIGURATION REPOSITORY
(Stores configuration settings for MailEnable Connectors, Services and Agents)
POSTOFFICE STORE
(Folders and Files stored on disk containing user messages)
Mail Client SMTP Send Message
Mail clients can use the SMTP connector to send messages to either local mail addresses or to relay to external sender addresses (non local recipients)
Authentication
Mail Access Services authenticate the Mailbox owner
WEBMAIL SERVICE
IMAP SERVICE
HTTPMAIL SERVICE
MAPI SERVICE
POP3 SERVICE
(Allows mail clients to access messages from the Postoffice
Message Access
Mail Services access files on postoffice and deliver them to connected clients.
Mail Client Access
Mail clients access the Postoffice to retreive message details.
REMOTE MAIL SERVERS
(SMTP Connector uses DNS and smarthosting rules to deliver messages to the appropriate target mail server)
MAIL CLIENT APPLICATION
(Mail client applications use message transport protocols (SMTP, MAPI, etc) and message access services (POP3,IMAP,HTTPMAIL, etc) services to send and receive messages)

Figure 12-1 Core Functionality of MailEnable

The following diagram provides a high level overview the POP Connector:

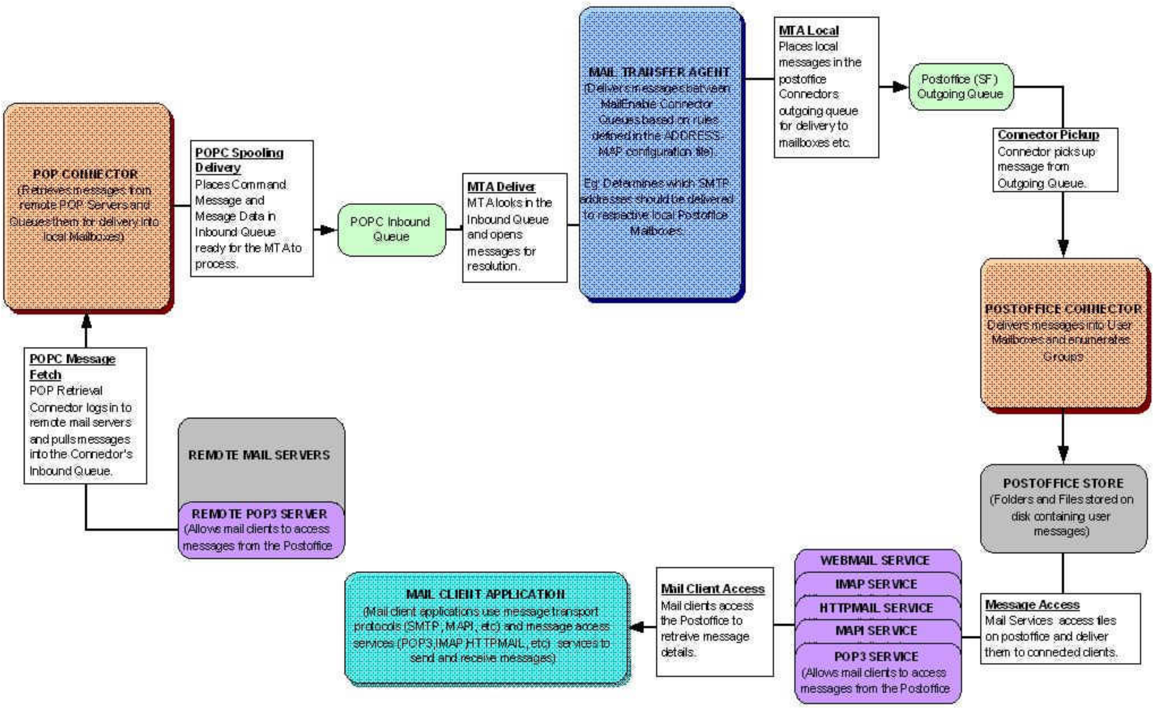

POP CONNECTOR (Retrieves messages from remote POP Servers and Queues them for delivery into local Mailboxes)
POPC Spooling Delivery
Places Command Message and Mesage Data in Inbound Queue ready for the MTA to process.
POPC Inbound Queue
MTA Deliver
MTA looks in the Inbound Queue and opens messages for resolution.
MAIL TRANSFER AGENT (Delivers messages between MailEnable Connector Queues based on rules defined in the ADDRESS-MAP configuration file).
Eg: Determines which SMTP addresses should be delivered to respective local Postoffice Mailboxes.
MTA Local
Places local messages in the postoffice Connectors outgoing queue for delivery to mailboxes etc.
Postoffice (SF) Outgoing Queue
Connector Pickup
Connector picks up message from Outgoing Queue.
POSTOFFICE CONNECTOR Delivers messages into User Mailboxes and enumerates Groups
POSTOFFICE STORE (Folders and Files stored on disk containing user messages)
Message Access
Mail Services access files on postoffice and deliver them to connected clients.
WEBMAIL SERVICE
IMAP SERVICE
HTTPMAIL SERVICE
MAPI SERVICE
POP3 SERVICE (Allows mail clients to access messages from the Postoffice
Mail Client Access
Mail clients access the Postoffice to retreive message details.
MAIL CLIENT APPLICATION (Mail client applications use message transport protocols (SMTP, MAPI, etc) and message access services (POP3,IMAP,HTTPMAIL, etc) services to send and receive messages)
REMOTE MAIL SERVERS
REMOTE POP3 SERVER (Allows mail clients to access messages from the Postoffice
POPC Message Fetch
POP Retrieval Connector logs in to remote mail servers and pulls messages into the Connector's Inbound Queue.

Figure 12-2 Overview of POP Connector

The List Connector is responsible for dispatching messages to large lists of mail addresses. The list 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.

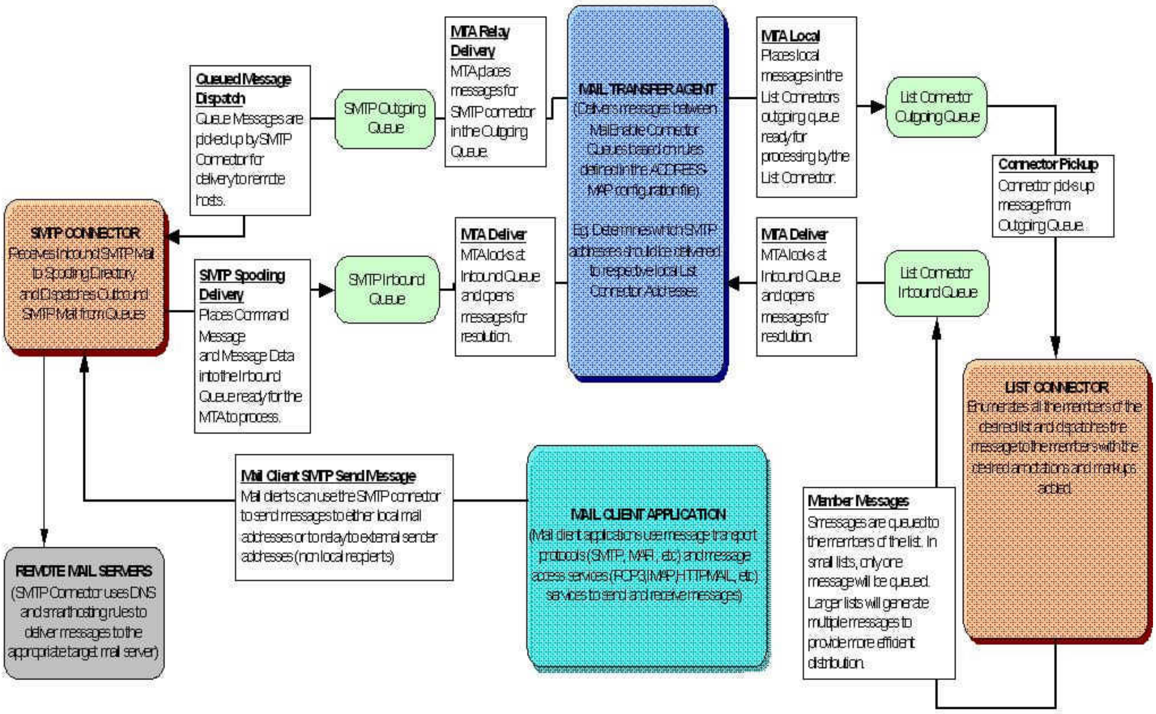

Queued Message Dispatch
Queue Messages are picked up by SMTP Connector for delivery to remote hosts.
SMTP Outgoing Queue
MTA Relay Delivery
MTA places messages for SMTP connector in the Outgoing Queue.
MAIL TRANSFER AGENT
(Delivers messages between MailEnable Connector Queues based on rules defined in the ADDRESS-MAP configuration file).
Eg. Determines which SMTP addresses should be delivered to respective local List Connector Addresses.
MTA Local
Places local messages in the List Connectors outgoing queue ready for processing by the List Connector.
List Connector Outgoing Queue
Connector Pickup
Connector picks up message from Outgoing Queue.
SMTP CONNECTOR
Receives Inbound SMTP Mail to Spooling Directory and Dispatches Outbound SMTP Mail from Queues
SMTP Spooling Delivery
Places Command Message and Message Data into the Inbound Queue ready for the MTA to process.
SMTP Inbound Queue
MTA Deliver
MTA looks at Inbound Queue and opens messages for resolution.
MTA Deliver
MTA looks at Inbound Queue and opens messages for resolution.
List Connector Inbound Queue
LIST CONNECTOR
Enumerates all the members of the desired list and dispatches the message to the members with the desired annotations and markups added.
Mail Client SMTP Send Message
Mail clients can use the SMTP connector to send messages to either local mail addresses or to relay to external sender addresses (non local recipients)
MAIL CLIENT APPLICATION
(Mail client applications use message transport protocols (SMTP, MAPI, etc) and message access services (POP3, IMAP, HTTPMAIL, etc) services to send and receive messages)
Member Messages
Sm messages are queued to the members of the list. In small lists, only one message will be queued. Larger lists will generate multiple messages to provide more efficient distribution.
REMOTE MAIL SERVERS
(SMTP Connector uses DNS and smarthosting rules to deliver messages to the appropriate target mail server)

Figure 12-3 Mailing List Connector

13 Operational Procedures

13.1 Backing Up and Restoring MailEnable Data

This section explains how you can effectively backup configuration. MailEnable comes with a backup utility which is accessible through the Program Files->Mail Enable->System Tools menu. With this utility, you 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 relatively straightforward 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 you need to (optionally) backup is the information in the registry. The registry hosts server specific information (like connector settings, etc). To do this, you need to use the registry editor (REGEDIT) to export the HKEYLOCALMACHINE\SOFTWARE\MailEnable 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, you should stop all services, replace the directory tree from your backup and then import the saved registry file into the registry.

13.2 Debugging MailEnable

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 you have completed the debug session, you can close the console window. Make sure that you set this setting back to 2 when you have completed running the server in debug mode.

13.3 Inspecting Log Files

Log files are an important aspect of any mail server. MailEnable produces several log files to help isolate and rectify any problems.

MailEnable usually 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). 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 you first identify a problem, there are some quick steps to take which involve examining the log files. The guidelines below will assist you to isolate the problem quickly.

Check the Debug log file first. This will more likely have information about the error that the service has encountered. The Debug log will show errors such as DNS failures, file errors, send problems, etc. If you cannot see the issue in the Debug log, it is likely that it is not a program error, but an error in conversation between the servers (i.e. the server may be trying a command that is not supported).

13.4 Licensing MailEnable

MailEnable is licensed on a per server basis. In order to avoid any restrictions on the features, you need to apply a license key to your installation. There are two ways that you can register.

13.4.1 For Computers Connected to the Internet

When you install MailEnable, a registration application is made available under the MailEnable program group. This registration application queries your system and submits your registration details to the licensing server. You 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 you register using online credit card details, MailEnable will immediately acquire a registration key and register it with the server. However, if you choose any other payment mechanism, it simply lodges your registration request with the payment server (assuming that you will reconcile payment by fax or purchase order). Once MailEnable receives notification of payment mechanism, your license key will be generated and mailed to the nominated e-mail address.

13.4.2 For Computers not connected to the Internet

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

13.4.3 Registration Key Retrieval Method

You can retrieve a new license key by using our online services website at the following address: http://www.mailenable.com/OnlineServices/default.asp

Here, you need to use the email address that was used for the registration, and the password that was created on purchase along with this email. These details are used to log-in.

Alternatively, you can use the Registration Wizard on the new server as described below to obtain an updated key:

In order to license your copy of MailEnable you will need to 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 personalise your registration key code.

You will need Internet access 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 your server.

When you run the Registration Wizard, follow these steps:

1. Select the "Apply for a Registration Key via the Internet", click **Next**
2. Enter your details, click **Next**
3. Select "Request License Key", click **Next**
4. Read the confirmation and click **Next**

14 Appendix

14.1 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 you are using.

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"="The virus was removed."

"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:00000001

"Exit Codes Error Inclusive"=dword:00000001

"Exit Codes"="1"
```

You can copy this into notepad, save as a .reg file and import it using the registry editor. Once imported into the Windows registry, you can edit the settings to those required by your anti-virus command line application.

14.2 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 effectively 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 loosely 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 you enable the Secure Password Authentication feature within the mail client, the mail client will typically 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 specific 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.

Setting	Description
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 for example in outlook the feature is called SPA – Secure Password Authentication.

14.3 Accessing Web Mail for Automatic Sign on

You can configure MailEnable to automatically login by using the following path syntax:

Syntax:

```
http://Server/MEWebMail/base/default/lang/EN/login.asp?LanguageID=EN&UserID=Account&Password=Password&Method=Auto&skin=default
```

Example:

```
http://127.0.0.1/MEWebMail/base/default/lang/EN/login.asp?LanguageID=EN&UserID=James@MailEnable&Password=password&Method=Auto&skin=default
```

You can make this page your startup page or home page within your browser. Also, if you have a certificate installed for your web server, you can use HTTPS. This will avoid passwords being sent to the remote host in clear text.

14.4 DNS Error Codes and Descriptions

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

Code	Error Description
9001	DNS server unable to interpret format.
9002	DNS server failure.
9003	DNS name does not exist.
9004	DNS request not supported by name server.
9005	DNS operation refused.
9006	DNS name that ought not to exist, does exist.
9007	DNS RR set that ought not to exist, does exist.
9008	DNS RR set that ought to exist, does not exist.
9009	DNS server not authoritative for zone.
9010	DNS name in update or prereq is not in zone.
9016	DNS signature failed to verify.
9017	DNS bad key.
9018	DNS signature validity expired.
9501	No records found for given DNS query
9502	Bad DNS packet
9503	No DNS packet 9504: DNS error, check rcode
9505	Unsecured DNS packet
1460	Timeout - This operation returned because the timeout period expired

14.5 Diagnosing Outlook/Outlook Express Error Codes

Some common Outlook/Outlook Express error codes that may be returned when attempting to send, receive or access mail.

Error	Service	Description
0x800CCCF4	HTTPMail	Your outlook settings may be invalid or a firewall is preventing you from connecting to the remote MailEnable Server.

0x800CCC79	SMTP	Your SMTP Relay settings are preventing you from sending messages to MailEnable. You should ensure you have enabled SMTP Authentication.
0x80042109	SMTP	Outlook is unable to connect to your outgoing (SMTP) e-mail server.
0x8004210A	POP	The operation timed out waiting for a response from the receiving (POP) server. You should establish whether you can telnet to port 110 of your mail server.
0x800CCC0F	POP	Your mail client is unable to contact your MailEnable Server, most likely because a firewall is preventing access or the supplied IP Address is incorrect.
0x8004210B	POP	If you are experiencing this issue, verify that you have installed the service pack for Microsoft Office XP.
0x800CCC0D	POP	If you are experiencing this issue, verify that you have configured your mail client correctly. You must either specify an IP address or a host name as the mail server when configuring the mail client settings. If you specify a host name then it must be defined in your DNS as a Host record.
0X800CCC0E	SMTP	This error means that you are able to connect to the server via POP, but your SMTP Service is either not running or is configured incorrectly. You can verify if the SMTP service is running by using the telnet utility to telnet to port 25 of your mail server. If the server responds, then the issue is most likely that your mail client settings are invalid.

14.6 Manually testing if MailEnable can send mail to remote servers

Many ISPs block outbound SMTP traffic to ensure that spammers do not abuse their service. You can validate whether you can send mail 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. Then click 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 Mail Enable SMTP Service, Version: 1.1 ready at 02/28/03 14:04:45
```

3. Type the word QUIT and then press enter.

If you were successfully able to do this, then no firewall (either local or your 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 you can connect to it). Firstly, you will need to determine which remote server to connect to. A domain may have more than one server which is accepting email, and these servers may not match the domain name. The mail servers for a domain are determined by the MX records which have been configured in a DNS. To retrieve the mail server details for a domain, you can 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, and you can then use these results as the hosts to connect to.

This is outlined as follows:

3. From the Windows Start Menu select Start|Run and enter CMD as the application to run. Then click OK.

4. 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 Mail Enable SMTP Service, Version: 1.1 ready at 02/28/03 14:04:45

5. Type the following and press Enter:

HELO YourDomainName

The server should reply with a line similar to:

250 Requested mail action okay, completed

6. 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

7. 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

If you wish to have multiple recipients to an email you can enter the recipient to line more than once. This is how a blind carbon copy works. If the recipient does not exist you may get an error such as:

550 Requested action not taken: mailbox unavailable or not local

8. Now you can 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>

9. 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].[CRLF]

10. 6. Type the following and press Enter:

QUIT

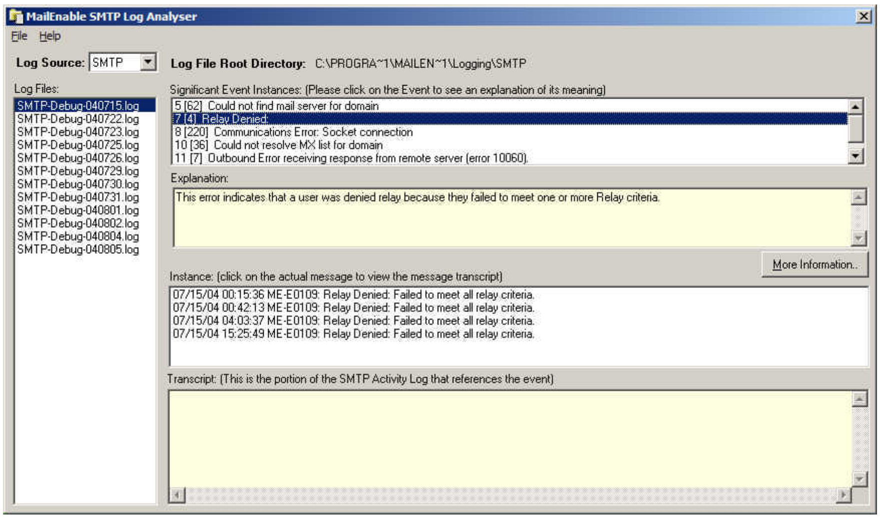
If you were able to do this then MailEnable should be able to send messages to the remote host. If your receive an abnormal response for any of the commands you typed in, then you should search the MailEnable knowledge base for any articles that may give an indication of the cause of the error.

Example:

```
C:\>telnet mail.mailenable.com 25
220 mailenable.com ESMTP MailEnable Service, Version: -1.110- ready at 11/20/03
23:49:40
EHLO test.mydomain.com.au
250-mailenable.com [144.136.51.56], 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.
```

14.6.1 Log Analyser

The log analyser is a useful tool which is installed with MailEnable. It will allow you to easily analyse the server logs to get an overview of any errors and display causes and fixes for these. The log analyser retrieves the latest help information from the MailEnable website.



Log Source: SMTP

Log File Root Directory: C:\PROGRA~1\MAILEN~1\Logging\SMTP

Log Files:

```
SMTP-Debug-040715.log
SMTP-Debug-040722.log
SMTP-Debug-040723.log
SMTP-Debug-040725.log
SMTP-Debug-040726.log
SMTP-Debug-040729.log
SMTP-Debug-040730.log
SMTP-Debug-040731.log
SMTP-Debug-040801.log
SMTP-Debug-040802.log
SMTP-Debug-040804.log
SMTP-Debug-040805.log
```

Significant Event Instances: (Please click on the Event to see an explanation of its meaning)

```
5 [62]  Could not find mail server for domain
7 [4]  Relay Denied:
8 [220]  Communications Error: Socket connection
10 [36]  Could not resolve MX list for domain
11 [7]  Outbound Error receiving response from remote server (error 10060).
```

Explanation:

This error indicates that a user was denied relay because they failed to meet one or more Relay criteria.

Instance: (click on the actual message to view the message transcript)

```
07/15/04 00:15:36 ME-E0109: Relay Denied: Failed to meet all relay criteria.
07/15/04 00:42:13 ME-E0109: Relay Denied: Failed to meet all relay criteria.
07/15/04 04:03:37 ME-E0109: Relay Denied: Failed to meet all relay criteria.
07/15/04 15:25:49 ME-E0109: Relay Denied: Failed to meet all relay criteria.
```

Transcript: (This is the portion of the SMTP Activity Log that references the event)

Figure 14-1 Log Analyser

You can run the log analyser through *Start|Program Files|Mail Enable|System Tools|Log Analyser* menu. The various log files in your 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. Click the item you are interested in and you will be given 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. If you need to match up the item in the Debug log with the actual data conversation between the MailEnable server and the remote application, click the instance item. It may take a few moments to scan through the Activity log to find the match, depending on how large your log files are.

Some errors will always be seen if your server is connected to the Internet. People will try to relay through your server, timeout and connection issues can occur, and users can mistype email addresses when sending messages, which will all display in the logs. The amount of errors that occur in the Debug log is show in the square brackets in the box labelled **Significant Event Instances**. This can give you a good indication of the severity of the event.

14.6.2 Troubleshooting SMTP Connectivity issues and Analysing Log Files

MailEnable provides extensive logging of SMTP activity. There are three log files that are used by MailEnable. These are the Debug, Activity and W3C logs. The W3C log files are essentially a replica of the Activity log, hence you really only need to investigate the Activity and Debug logs.

The debug log contains "wordy" explanations of significant actions undertaken by MailEnable. For example, when a user attempts to relay a mail message, this is recorded and timestamped in the SMTP Debug log.

The Activity log file contains a transcript of all SMTP commands exchanged between MailEnable and other remote clients or mail servers.

The simplest way to find a message and debug a SMTP transaction is to open the SMTP Activity log in Notepad and search it. You can also load the log file into Microsoft Excel as follows:

14.6.3 How to import the Activity log into Microsoft Excel

- File|Open Browse to C:\Program Files\Mail Enable\Logging\SMTP (or equivalent directory).
- Change the Files of Type combo to All Files (*.*)
- Select the activity file you want to open (the files are named as SMTP-Activity-YYMMDD).
- Excels Text Import Wizard will now be displayed. Select the option to import the text as Delimited data and click Next
- Select the format as Tab delimited and click next
- Click Finish to import the data

You should now see a worksheet with data represented as follows:

A=Transaction date and time

B=Transaction Type (Inbound or Outbound)

C=Message ID/Message file Name (This is used to match with other logs to track messages)

D=TCP/IP port number that the SMTP transaction was occurring on

E=TCP/IP Address of the remote host involved in the SMTP transaction

F=The name of SMTP Command that relates to the transaction

G=The details for the SMTP Command that relates to the current transaction

H=The details for the response to the SMTP Command that relates to the current transaction

I=The number of bytes sent when executing this command

J=The number of bytes received in executing this command

There are two important types of transactions outlined in the SMTP Activity log file. These are SMTP Inbound Transactions and SMTP Outbound Transactions. These transactions are denoted in the log files as SMTP-IN and SMTP-OU in their respective lines in the Activity log file.

14.6.4 How to relate Activity log entries to the debug log file

The most obvious way or relating an entry in the Activity log file to the Debug log file is via the time stamp recorded in the file. You can also use the Message ID (as this is often recorded in the debug log file). The message ID is also useful in tracking messages as they pass through the MTA. The MTA logs this message ID and therefore you can use the logs to track a message as it is routed through MailEnables Connectors via the MTA.

For example, a user may complain that they cannot send mail from outlook. In this case an error message will be reported back to the remote mail client.

eg: 503 This mail server requires authentication. Please check your mail client settings.

You should then use this error string to locate the transaction sequence in the SMTP Activity log.
Once you have found the entry in the SMTP Activity log, you can then check the SMTP Debug log for the same time period. You should, find that the System has recorded the reason why the relay request was denied.

14.7 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. You can then install separate copies of MailEnable on other servers and smarthost 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.

You will also need to change the DNS/MX settings for the domains to configure the appropriate MX preferences. Other mail servers learn about your Mail Server via DNS MX records. They are basically 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 that 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 typically used if your backup mail servers are distributed in different geographic or logical locations.

A second alternative is to host all your mail servers on the same local network and cluster the servers. This effectively means that all your servers. This allows you to install multiple servers with MailEnable and have them use the same store for their messages and post office data. You can then use any of these servers to access the mail. It basically requires that one of the servers share the mail data and configuration directories and that the others access them.

14.8 Antivirus configuration

14.8.1 General Guidelines

MailEnable Professional Edition provides an antivirus plug-in that allows you to scan mail messages for viruses as they pass through the Mail Transfer Agent. The following overviews are provided to assist you in selecting an antivirus application for your MailEnable Implementation.

14.8.1.1 F-Prot

Company: Frisk International

Product Name: F-Prot for Windows http://www.f-prot.com/

Configuration Guidelines: MailEnable Knowledge Base
http://www.mailenable.com/kb/Content/Article.asp?ID=me020284

Comments: MailEnable integrates with the F-Prot command line scanner and that is available in F-Prot for Windows.

14.8.1.2 Sophos

Company: Sophos

Product Name: Sophos Antivirus http://www.sophos.com/

Configuration Guidelines: MailEnable Knowledge Base
http://www.mailenable.com/kb/Content/Article.asp?ID=me020288

14.8.1.3 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

14.8.1.4 Panda

Company: Panda Software

Product Name: Panda Command Line http://www.symantec.com/index.htm

Configuration Guidelines: MailEnable Knowledge Base
http://www.mailenable.com/kb/Content/Article.asp?ID=me020289

14.8.1.5 Symantec Norton Antivirus

Company: Symantec

Product Name: Norton Antivirus (Corporate Edition) http://www.symantec.com/index.htm

Configuration Guidelines: MailEnable Knowledge Base
http://www.mailenable.com/kb/Content/Article.asp?ID=me020086 (versions 6 and 7)
http://www.mailenable.com/kb/Content/Article.asp?ID=me020277 (Corporate Edition)

Comments: Symantec Norton Antivirus requires that you purchase a 5-user pack, and are a little harder to configure/integrate with MailEnable. This is most possibly to discourage the use of their Antivirus solution with mail servers as they have their own product line that can be used to scan messages.

14.8.1.6 McAfee Virus Scan

Company: McAfee

Product Name: McAfee Virus Scan http://www.mcafee.com/

Configuration Guidelines: MailEnable Knowledge Base

MailEnable generally recommends trialing the Antivirus software before you purchase. It is also worth mentioning that some antivirus agents require that the MailEnable Mail Transfer agent run with elevated privileges.

14.8.1.7 Grisoft AVG

Company: Grisoft

Product Name: AVG http://www.grisoft.com

Configuration Guidelines: MailEnable Knowledge Base
http://www.mailenable.com/kb/Content/Article.asp?ID=me020201

Comments: By default, AVG 7 will not work with MailEnable. To integrate these versions with AVG 7, MailEnable requires a registry import. This is available at: http://www.mailenable.com/hotfix/MEAVAVG71.ZIP. You should take careful consideration of Grisoft's licensing and revamped product range.

Note: Using AVG 7 won't allow you to scan within ZIP files

14.8.2 Real Time Protection

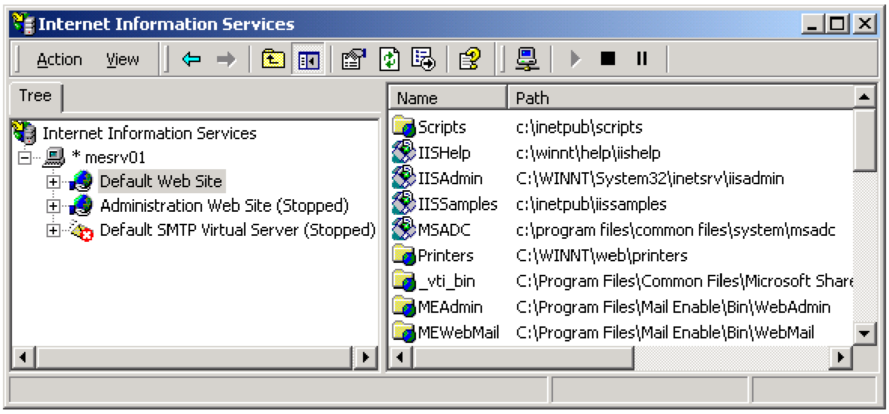
Most of the less expensive Antivirus agents cannot exclude directories or file types from their real time protector. You may experience unpredictable results if you do not prevent real-time virus protectors from monitoring and protecting critical MailEnable directories. Depending on what you are using your server for, it may be better disable real time protectors on servers because they drastically inhibits disk IO. An option is to schedule scans rather than using the real-time protector. You can further reduce the risk by not running desktop applications on the server itself (e.g.: mail clients). The following table outlines the current features of leading antivirus manufacturers with respect to configuring real-time virus protection/IO monitoring.

Vendor/Product	Support
Norton Antivirus Corporate Edition	Can exclude directories and file types.
McAfee Virus Scan	Can exclude directories and file types.
Panda	Can exclude specific folders.
AVG	No ability to exclude directories or file types.
Norman	No ability to exclude directories or file types.
F-Prot	No ability to exclude directories or file types.

Note: Any errors or omissions in the above are unintentional. For accurate and up to date information it is recommended that you 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.

14.9 IIS Configuration

The following screenshot shows the Internet Information Server Management Console (Internet Service Manager) under Windows 2000.

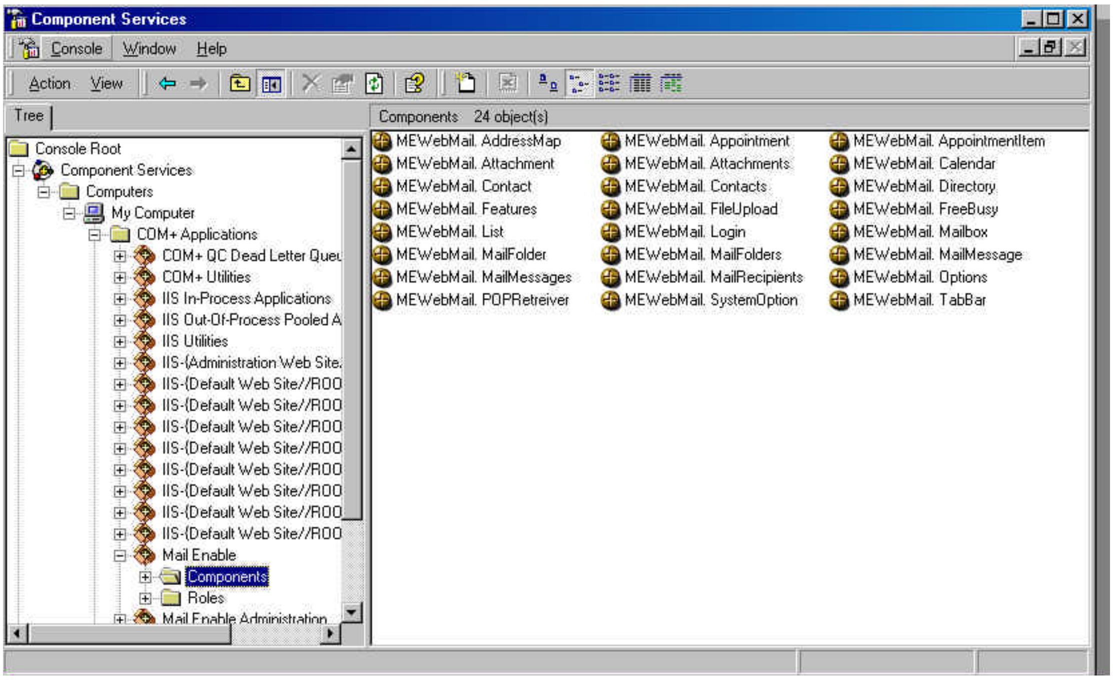

Internet Information Services
Action
View
Tree
Internet Information Services
* mesrv01
Default Web Site
Administration Web Site (Stopped)
Default SMTP Virtual Server (Stopped)

Name	Path
Scripts	c:\inetpub\scripts
IISHelp	c:\winnt\help\iishelp
IISAdmin	C:\WINNT\System32\inetsrv\iisadmin
IISSamples	c:\inetpub\iissamples
MSADC	c:\program files\common files\system\msadc
Printers	C:\WINNT\web\printers
_vti_bin	C:\Program Files\Common Files\Microsoft Share
MEAdmin	C:\Program Files\Mail Enable\Bin\WebAdmin
MEWebMail	C:\Program Files\Mail Enable\Bin\WebMail

Figure 14-2

MailEnable Web Mail installs a component (COM DLL) under Component Services for Windows 2000 or later. Under Windows NT this is put into Microsoft Transaction Server. This component is configured to run with the identity/security context of an account called IME_ADMIN.

The following screenshot shows Component Services under Windows 2000 and the Components contained within the Mail Enable package.



Console Root
Component Services
Computers
My Computer
COM+ Applications
COM+ QC Dead Letter Queu
COM+ Utilities
IIS In-Process Applications
IIS Out-Of-Process Pooled A
IIS Utilities
IIS-{Administration Web Site.
IIS-{Default Web Site//ROO
IIS-{Default Web Site//ROO
IIS-{Default Web Site//ROO
IIS-{Default Web Site//ROO
IIS-{Default Web Site//ROO
IIS-{Default Web Site//ROO
IIS-{Default Web Site//ROO
IIS-{Default Web Site//ROO
Mail Enable
Components
Roles
Mail Enable Administration

MEWebMail. AddressMap
MEWebMail. Appointment
MEWebMail. AppointmentItem
MEWebMail. Attachment
MEWebMail. Attachments
MEWebMail. Calendar
MEWebMail. Contact
MEWebMail. Contacts
MEWebMail. Directory
MEWebMail. Features
MEWebMail. FileUpload
MEWebMail. FreeBusy
MEWebMail. List
MEWebMail. Login
MEWebMail. Mailbox
MEWebMail. MailFolder
MEWebMail. MailFolders
MEWebMail. MailMessage
MEWebMail. MailMessages
MEWebMail. MailRecipients
MEWebMail. Options
MEWebMail. POPRetreiver
MEWebMail. SystemOption
MEWebMail. TabBar

Figure 14-3

14.10 Increasing Upload Limit for Windows 2003

Windows 2003 restricts 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 2003. 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

You may also have the following error displayed:

Error MEUP001: The ASP Session expired during the upload.

Reason: IIS6.0/Windows 2003 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 you will need to update the value to a higher value.

Solution: Instructions for resolving this issue follow:

You should stop the World Wide Web Publishing Service. This can be done from the Windows Command Prompt as: net stop w3svc

In the c:\Windows\System32\Inetsrv directory, you should find a file called metabase.XML.

Copy the original file in notepad and find the line "AspMaxRequestEntityAllowed".

Change the value of this entry to "1073741824". (Specifies a maximum post size of 1 GB)

You should then save the file.

You should 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, you may need to start windows in Safe-mode to be able to change that file.

14.11 Activity Monitor

The MEActivityMonitor utility allows you to watch MailEnable System Activity as it occurs. This utility is useful for tracing messages as they pass through the MailEnable system. The tool basically works by monitoring File IO to the Activity and Debug logs on your server. You should 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 tracing MailEnable system activity.

14.12 MEInstaller

MEInstaller is an application that allows you to reset various MailEnable configuration options without requiring a reinstall of the full product. The program is located in the Mail Enable\bin directory and has the filename MEInstaller.exe. It will allow you to perform the following tasks:

14.12.1 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

14.12.2 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

14.12.3 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 webmail 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

14.12.4 Re-Register MMC Components

- Reregisters the MailEnable administration MMC DLLs

14.12.5 Set IIS Application Isolation Levels (Low -> In Process)

- Sets the MEAdmin and MEWebmail virtual directories application level to be low

14.12.6 Set IIS Application Isolation Levels (Medium ->Pooled)

- Sets the MEAdmin and MEWebmail virtual directories application level to be medium

14.12.7 Set IIS Application Isolation Levels (High ->Isolated)

- Sets the MEAdmin and MEWebmail virtual directories application level to be high

14.12.8 Clear System Blocking Files

- Removes all the blocking files from the Mail Enable\Config directory

15 Glossary

Item	Description
Address Map	An address map is used to define source and target mail exchanges between Connectors by the Mail Transfer Agent. For example, mail sent to the SMTP address [SMTP:Jones@mailenable.com] is likely to have an address map to the post office address [SF:MailEnable/JONES].
Agents	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.
Connector	Connectors facilitate moving mail between systems or subsystems (whether they are local or remote).
DNS	Domain Name Server (or System) is a database of Internet names and addresses which maps domain names to the official Internet Protocol (IP) address and vice versa.
Group	A Group represents a logical combination of mail addresses addressable under a single mail address. Any mail addressed to the group is distributed to all the members belonging to that group.
IP	Internet Protocol. A network and transport protocol used for transmitting data over the Internet. Every machine on the internet has its own IP number/address.
List	A List is much like a group. The major difference between a list and a group is that lists are subscription based, can be moderated, and can have headers and footers applied to them.
Mailbox	A mailbox is a repository for email. It 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.
MTA	A Windows Service that exchanges internal messages between MailEnable Connectors.
Post office	A post office is used to host multiple mailboxes and domains under one area. For example, if you were providing email hosting for multiple companies, you would create a post office for each company. Within the post office you can assign multiple domains and mailboxes.
Provider	Providers are used by Connectors, Agents and Services to allow them to read their configurations. An example of a provider is the Tab Delimited Address Map provider. This provider reads the address map that is used to determine mail routing between connectors. In order to allow the applications to read configuration data from different sources, different providers would be used. For instance, SQL Server would have its own providers.
Recipient	The address to where the email is destined.
Services	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. MailEnable employs standard Windows Services that make it compatible with Windows NT/2000/2003.