MailEnable Standard Edition Configuration Guide Version 1.0

MailEnable Messaging Services
for Microsoft Windows NT/2000/2003

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

Date last modified 29/11/2006 5:15 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

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.

59 Murrumbeena Road
Murrumbeena
VIC 3163
Australia
Tel: +613 9563-4177 (AEST)
Fax: +613 9530-4066
Email: sales@mailenable.com

1.1.1 Support

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

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

1.1.1.1 Web site

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

1.1.1.2 Knowledge base

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

1.1.1.3 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

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

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

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

1.3 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 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, Microsoft Internet Information Server (IIS) will need to be installed. If you do not intend to use these components, then IIS is not a requirement.

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

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

MailEnable web mail and web administration use the Microsoft .Net Framework version 1.1. While the option to install the ASP version is available, it does not include a spell checker, multiple languages or light weight HTML editor.

1.5 How Internet email works

To administer a mail server on the Internet requires knowledge of how email works. It is important to know how messages are delivered and sent, how mail servers contact each other, and how users retrieve their email. This will help in diagnosing problems, tracking faults, and knowing who to contact (or blame!) when something goes wrong. The information in this section is not specific to MailEnable; this applies to all mail servers. This information is essential to know in order to properly administer an Internet mail server.

1.5.1 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

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

1.5.2 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.

1.5.3 Sending and receiving mail

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

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

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

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

2 Overview

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

2.1 Structure of MailEnable

MailEnable is comprised of Connectors, Agents and Services. 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 post office.

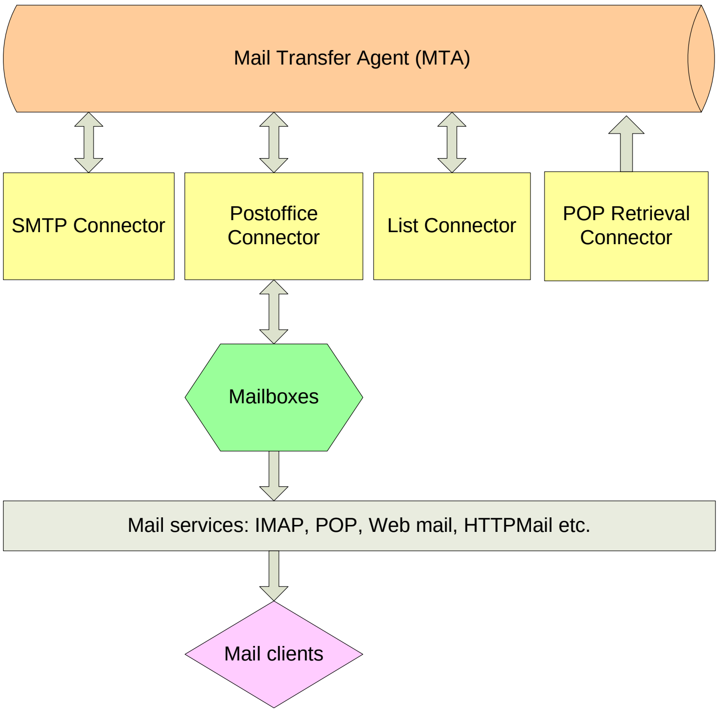


Figure 2-1 Relationship between agents, connectors and mail services in MailEnable

2.1.1 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 5.

2.1.2 Connectors

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

2.1.2.1 SMTP connector

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

2.1.2.2 Post office connector

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

2.1.2.3 List connector

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

2.1.2.4 POP Retrieval connector

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

2.1.3 Agents

2.1.3.1 Mail Transfer Agent (MTA)

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

2.2 Administration

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

- Post offices
- Domains
- Mailboxes
- Lists
- Groups

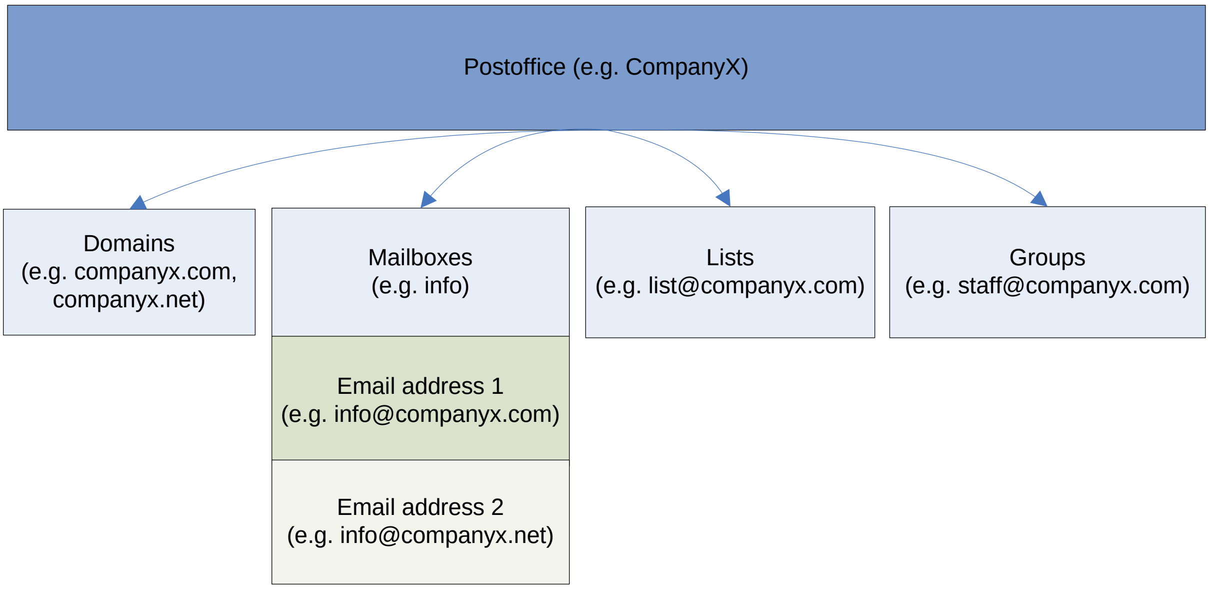

Postoffice (e.g. CompanyX)
Domains (e.g. companyx.com, companyx.net)
Mailboxes (e.g. info)
Email address 1 (e.g. info@companyx.com)
Email address 2 (e.g. info@companyx.net)
Lists (e.g. list@companyx.com)
Groups (e.g. staff@companyx.com)

Figure 2-2 Structure of post offices, domains and mailboxes

2.2.1.1 Post offices

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

2.2.1.2 Domains

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

2.2.1.3 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 post office, using the format mailboxname@domain. A mailbox can have multiple email addresses. This means a user only requires one mailbox to connect to, from which they can retrieve email from all their email addresses.

2.2.1.4 Email addresses

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

2.2.1.5 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 (e.g. list@companyx.com), and the server will duplicate their email and send it out to all the members.

2.2.1.6 Groups

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

2.3 Email delivery flow

2.3.1 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.

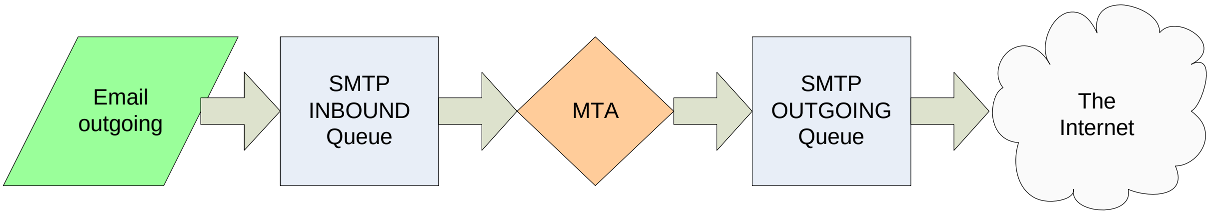


Figure 2-3 Email to remote (Relaying)

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

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

2.3.2 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 post office connector service **outgoing** queue. The post office connector will be checking its outgoing queue and can then process this message and deliver it to a users mailbox.

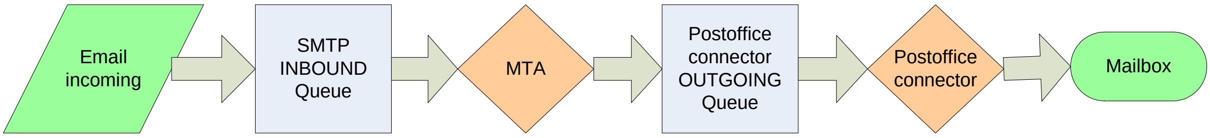


Figure 2-4 Local email delivery flow

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

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

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

3 Installation and upgrading

3.1 Installation overview

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

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

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

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

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

3.2 Installation process

3.2.1 Welcome screen

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

Please select the Next button to continue.

3.2.2 Registration details

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

Please select the Next button to continue.

3.2.3 Terms and conditions

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

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

Please select the [Next] button to continue.

3.2.4 Choose program installation location

Setup will prompt to nominate where to install its configuration and binary files. By default, MailEnable will install itself under the “Program Files” directory. This can be changed to a different directory by selecting the Browse button.

3.2.5 Select Program Manager group

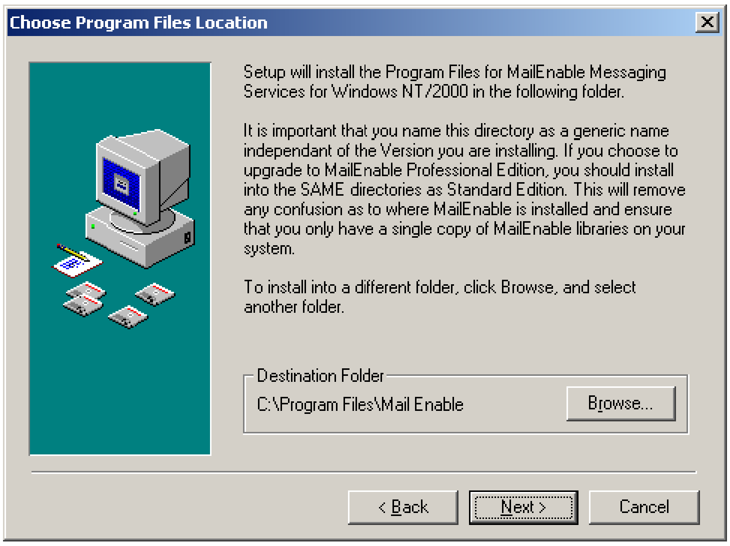
The installation wizard will now prompt for the program group in Windows for the MailEnable icons and shortcuts installed. Accept the default settings to install the icons under the “Mail Enable” Program Group

Please select the Next button to continue.

3.2.6 Selecting Repository

Setup will now prompt for a location to install configuration and messaging data. By default, MailEnable will install itself under the “Program Files” directory. This can be changed to a different directory by selecting the Browse button.

MailEnable will detect the repository location if the local repository is being used. It is also possible to nominate a repository on a backend server by pointing at the directory on this server that contains the \CONFIG, \POSTOFFICES or \QUEUES directories.



Choose Program Files Location

Setup will install the Program Files for MailEnable Messaging Services for Windows NT/2000 in the following folder.

It is important that you name this directory as a generic name independant of the Version you are installing. If you choose to upgrade to MailEnable Professional Edition, you should install into the SAME directories as Standard Edition. This will remove any confusion as to where MailEnable is installed and ensure that you only have a single copy of MailEnable libraries on your system.

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

Destination Folder
C:\Program Files\Mail Enable

Please select the [Next] button to continue.

3.2.7 Creating an initial post office

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

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

Please select the Next button to continue.

3.2.8 SMTP connector configuration

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

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

Setting	Explanation
Domain Name	The first configuration setting is the Domain Name for this server. The domain name should be the domain name of the organization that owns or is operating the server. If this server is being used on the Internet, it is important that this domain name is registered. When MailEnable is sending out email to remote servers, it will announce itself as this domain.
DNS Host	The DNS host used by the SMTP Connector to locate mail servers. To use multiple DNS addresses, enter these here, and separate the IP addresses with a space. In most cases, the same DNS host(s) should be included as configured under the network TCP/IP settings for the computer.

SMTP Port	The SMTP port is almost always set to 25. Very rarely is another port number used and it is recommended that this setting remain as 25. Corporate or hosting companies/agencies may wish to use a different SMTP port to 25 to obscure the fact that the server is running SMTP services. If unsure, leave the setting as 25.

Please select the Next button to continue.

3.2.9 Start installation

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

Please select the Next button to continue.

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

3.2.10 Viewing the README File

The installation program will now display the Read Me file. The readme file contains release history and notes. It also outlines any considerations of known issues with the current installation.

3.2.11 Completing installation

Finally, set-up will inform that the installation procedure completed successfully.

Please select the Finish button to complete installation of MailEnable.

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

3.3 Upgrading

To upgrade MailEnable Standard to either a newer release or to another version (e.g. Enterprise or Professional Edition) follow the same steps as outlined at the start of Chapter 3. As the same data stores are used, it is possible to run the installation over the top of the current configuration. MailEnable will detect the old version and retain the old settings (unless otherwise specified).

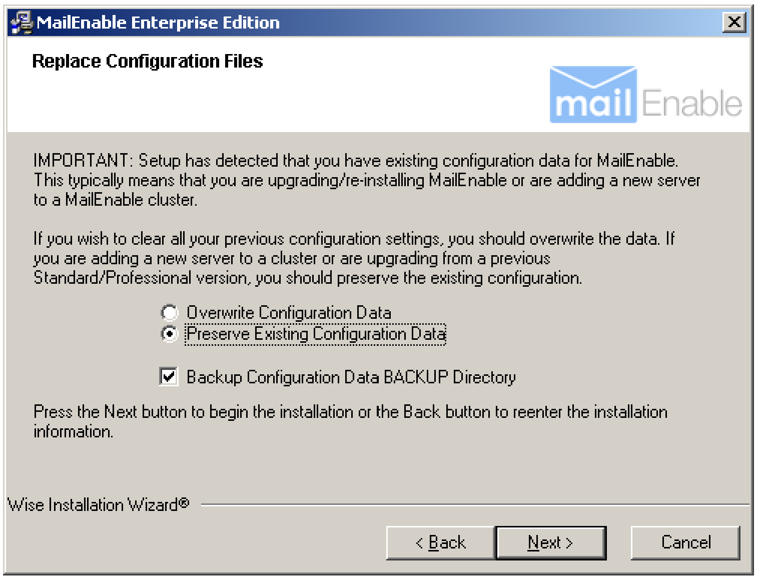
MailEnable set-up kits are available from the MailEnable web site at http://wwwmailenable.com/download.asp

3.3.1 Configuration repository location

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

3.3.2 Replace configuration files

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



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 3-1 Replace or Preserve Configuration Data

The installation has the option to **Backup Configuration Data BACKUP Directory.** Selecting this will ensure that the data repositories are backed up, which is always good practice. It is also good practice to have used the MEBACKUP utility beforehand, however, since the installation makes its own backup, this is not imperative. If you are using a database for configuration storage, this is not backed up.

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

Note: Enterprise Edition will use the same configuration data and options as Standard and Professional, but has two-way migration wizards for changing the configuration provider. E.g.: Tab delimited files >Database > Tab delimited files. Enterprise stores more data than Standard and Professional Editions, but the configuration format is backward compatible.

3.4 Post-installation configuration

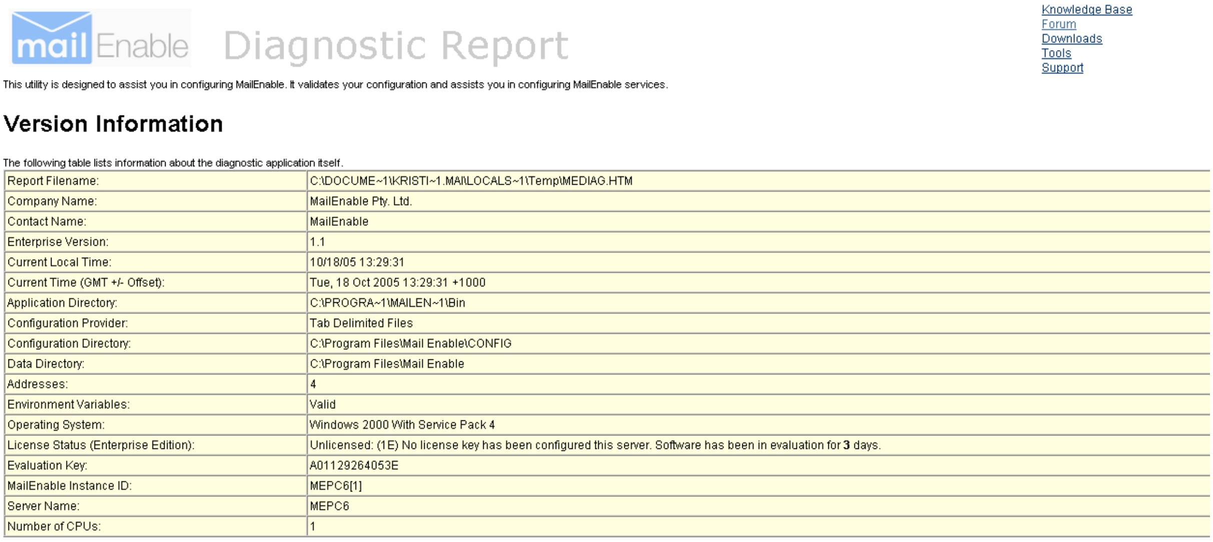
3.4.1 MailEnable Diagnostic Utility

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

The MailEnable Diagnostic Utility can be found under:

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

Once the Diagnostic Utility has been selected, it may take a few seconds to load (depending on the number of domains). A web page will be invoked and will give a test output of all services installed within MailEnable. In order to rerun the Diagnostic through the Administration program, right select 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.



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
Enterprise Version:	1.1
Current Local Time:	10/18/05 13:29:31
Current Time (GMT +/- Offset):	Tue, 18 Oct 2005 13:29:31 +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:	4
Environment Variables:	Valid
Operating System:	Windows 2000 With Service Pack 4
License Status (Enterprise Edition):	Unlicensed: (1E) No license key has been configured this server. Software has been in evaluation for **3** days.
Evaluation Key:	A01129264053E
MailEnable Instance ID:	MEPC6[1]
Server Name:	MEPC6
Number of CPUs:	1

Figure 3-2 Diagnostic Report

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

Option	Description
Version Information	Contains all required environment data and version information.
Configuration and Data Test	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. Some services are not installed in all versions of MailEnable, and so therefore may fail this test. Select the Status link for confirmation of whether this is the case.
Queue Status	Calculation of the quantity of all inbound and outgoing emails is displayed here.
Host TCP/IP Settings	Basic check on IP and DNS configurations.
Network Interface Report	Check of all Network Interface Cards and validation of drivers.
Mail Transfer Agent	Reports details of the MTA service settings that can affect delivery and Antivirus/pickup event performance.
SMTP Configuration Test	Settings or properties of SMTP settings are defined. Checks security settings for this service.
SMTP Relay Settings	Relay settings are checked here - verifies that only authorized addresses can send through the mail server. See section 5.1.4.
SMTP Inbound Bindings Test	Provides information on the bindings to IP addresses.
SMTP Outgoing Configuration	Shows outgoing SMTP configurations.

SMTP Outgoing Queue Status Test	Shows status of messages queued to remote hosts.
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 configured for the IP address, so if this test fails a PTR record needs to be configured.
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 web administration 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 authentications 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.

3.4.2 Check and configure DNS settings

In order for remote mail servers to deliver email to the MailEnable server, the correct DNS entries need to be configured in the Domain Name Services (DNS) hosting the domain records.

The server should have a fixed IP address that is registered under the public DNS. If the server does not have a static IP address (i.e. the IP address changes) in order to direct emails and domains to the server, a dynamic DNS provider (e.g. no-ip.com) will be required. A dynamic DNS provider keeps track of the changing IP address and updates the DNS details accordingly. Companies that offer this service may charge a monthly fee, although there are some free services available. It is still possible to send email from MailEnable with a dynamic IP address, but unless the DNS is updated with the new IP address every time it changes, other mail servers will not be able to connect. Be aware that a number of mail servers will not accept email from the server if it does not have a static IP address, or if the server is using a cable/DSL connection.

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

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

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

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

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

1. Using the DNS Management software for the DNS Server, ensure that a DNS "A" (Host) record has been created for the mail server. This record type allows the host to be identified by a host name rather than IP Address. To validate whether the A record was registered correctly, use the ping utility. Attempt to ping the host using its host name. If this works, then the A record was registered correctly.
2. Next, create an MX record that points to the A record. The way this is achieved depends on which DNS server/vendor being used
3. When selecting a DNS for MailEnable to use, choose one that can resolve all domain names, which is not necessarily the DNS which is hosting the domain names. For example, if you host your domain names through a third party, it is unlikely that you would use their DNS IP address to resolve.

An example for registering MX records using Microsoft DNS Server is available at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/cb7a2363-0ed6-4c7c-87ba-7cc9592a8028.mspx

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

1. Ensure that DNS Forwarding is enabled on the server. This means that if a client cannot find DNS records on the mail server, the DNS server will forward request to your ISPs DNS servers. This can be accessed under the properties of the server - Forwarders Tab (within DNS Manager)
2. Create the Reverse Lookup Zone for address range of the public IP address (e.g.: 201.248.10.*). Create this by selecting 'New Zone' under the properties of the server (within DNS Manager).
3. Create PTR Records for all of the IPs under the Zone outlined above (within DNS Manager).
4. Ensure the primary DNS IP addresses used by MailEnable's SMTP Connector is configured to use the local DNS rather than referring upstream to your ISPs. This is much faster and more efficient. (This is done via the MailEnable Administration program under the properties of the SMTP Connector)
5. Restart the SMTP Service to place DNS Server changes into effect (Service Control Manager)

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

3.4.4 Check mail services

There are various mail services installed with MailEnable. These services run in the background and handle the sending, receiving and distribution of email. Check that these services are running after the initial installation.

Expand the **Servers >localhost >System** branch, and select **Services**. A list of services and their status should be displayed.

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, it can be started 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, check its respective Debug log for more details of the failure.

4 MailEnable Administration Console

4.1 Overview

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

This application can be accessed using the Start menu in Microsoft Windows and navigating to MailEnable Standard Edition by selecting:

Start > Programs > Mail Enable >MailEnable Administrator

The MailEnable Administration program will open with a window similar to the following:

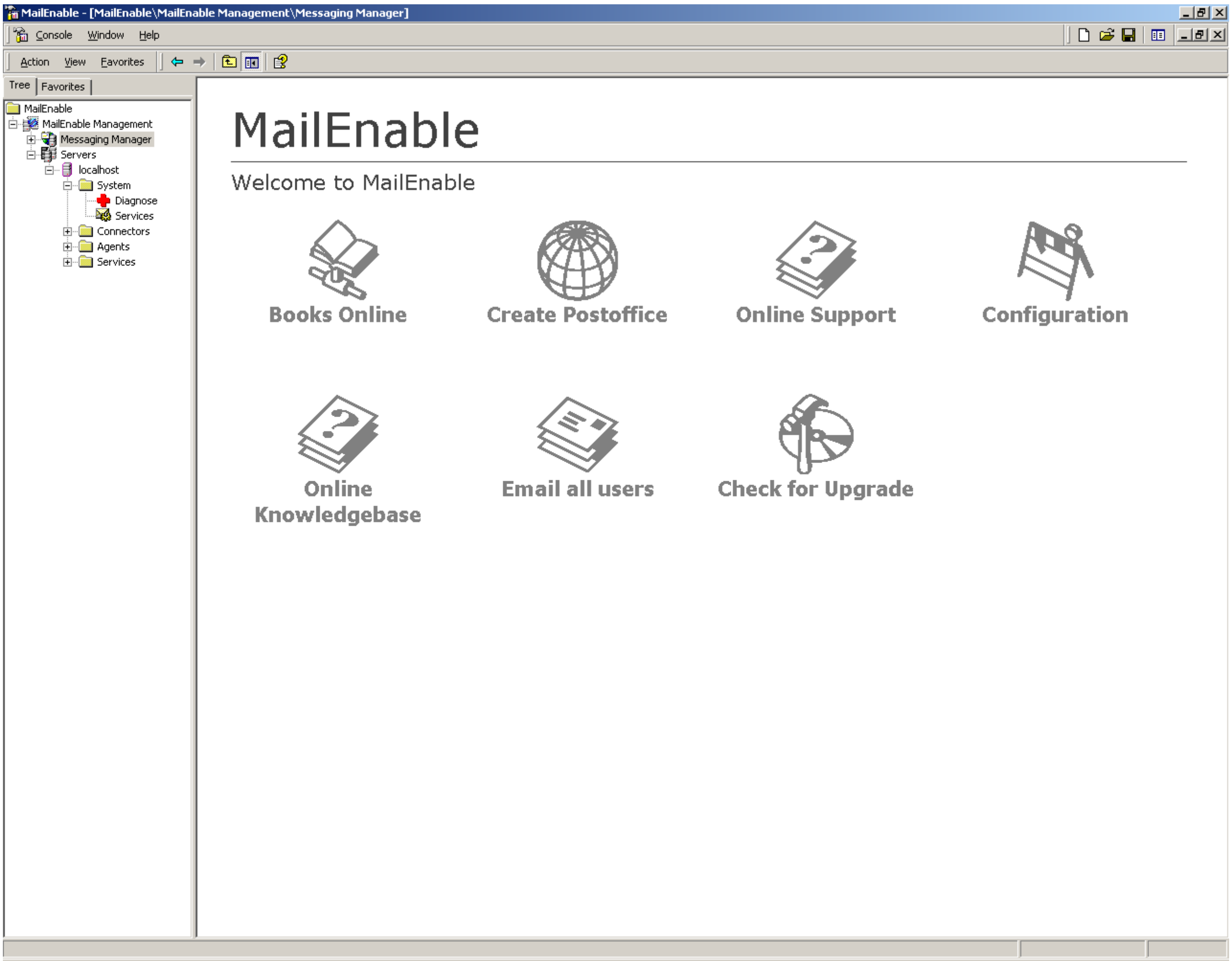


Figure 4-1 MailEnable Administration Program

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

The first item in the display is **MailEnable Management**.

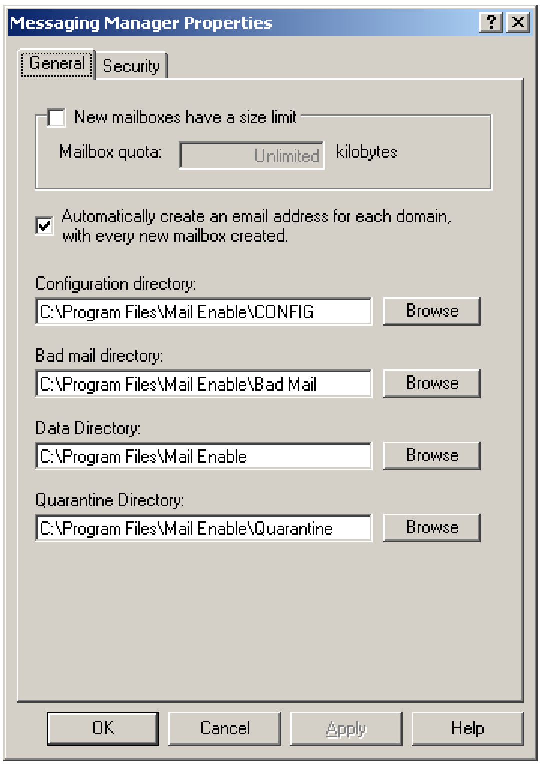
The second item in the display is **Messaging Manager**. This is where various global settings, such as Domains, Post Offices and Mailboxes can be modified. Explanations of these items are contained later in this document. The panel to the right of the tree view provides either icons for options, or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

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

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

4.2 Messaging Manager

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 select 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 4-2 Messaging Manager Properties

4.2.1 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 set here.

Setting	Explanation
New mailboxes have size limit	Configures the default quota for mailboxes, so every new mailbox created will have a quota configured. This can be enable/disabled in the mailbox settings.
Automatically create an email address for each domain with every new mailbox created.	If there are several domains in a post office and this setting is selected, then every time a mailbox is created in a post office a mail address or address mapping will be created for each domain for the mailbox.
Directory paths from the MailEnable system	This specifies the various system directories for MailEnable.

4.2.2 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. There is an option to encrypt MailEnable passwords. If integrated authentication is used, Windows credentials will take preference to these passwords.
Enable Integrated Authentication	This is a system wide setting that will enable or disable authentication for all hosted MailEnable post offices. MailEnable Integrated Authentication allows Windows Authentication to be used as well as MailEnable's inbuilt authentication. It also allows mailboxes to be created within MailEnable as users successfully authenticate using Windows Credentials. To enable integrated authentication, select Messaging Manager Properties (right click on Messaging Manager) and check the box labeled "Enable Integrated Authentication".

4.3 Post office configuration

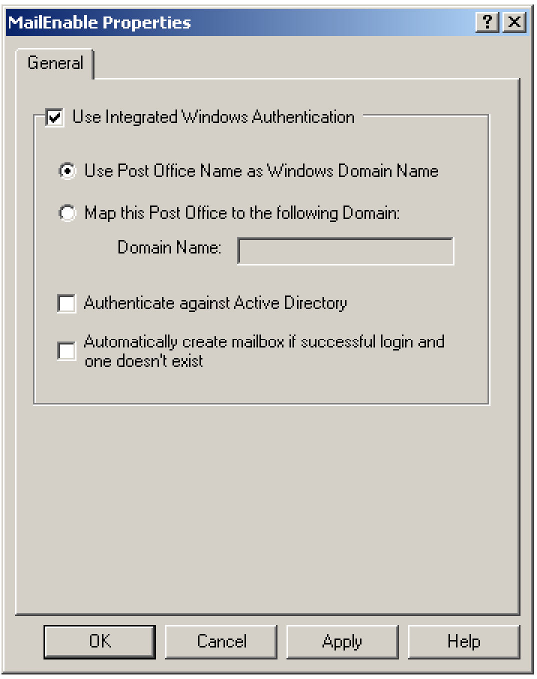
For a description of post offices, refer to section 2.2.1.1.

To add a new post office:

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

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

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



MailEnable Properties

General

☑ 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 4-3 Post office properties

4.3.1 Authentication settings

Once Integrated Windows Authentication has been enabled globally as per section 4.2.2, it is then possible to configure each post office with specific authentication settings

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

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

Setting	Explanation
Use Integrated Windows Authentication	Defines whether the post office can use Windows Authentication.
Use Post Office Name as Windows Domain Name	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	Defines the Windows Domain Name that the will be used for authenticating this post office’s mailbox users. To authenticate against the local machine, either leave the Domain Name blank or enter a single period (.).
Authenticate against Active Directory	Configures MailEnable to use User Principal Name (UPN) style logins, rather than legacy Windows NT style logins. Both login mechanisms work equally as effectively, except Active Directory hosting of multiple domains in its hierarchy.
Automatically create mailbox if successful login and one doesn’t exist	Allows accounts to be created as users authenticate. If a user enters valid Windows credentials, their mailbox is created automatically. Enabling this option immediately provides access to mailboxes for those who have validated against the specified domain.

4.4 Post office actions

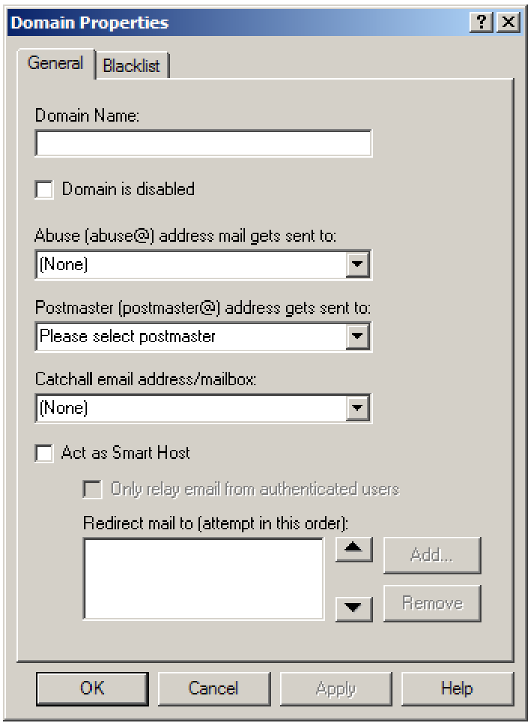
In the MailEnable Administration program, expand the post offices branch to display all the available post offices. Selecting the post office will display the available actions.

4.4.1 Create domain

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

4.4.1.1 General

After selecting the **Create Domain** icon, the following window will appear:



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 4-4 Domain properties General TAB

Here, enter the full domain name to receive emails for. For instance, to receive emails such as sales@mailenable.com, enter the domain **mailenable.com** here. The domain will now appear under the **Domains** branch of the MailEnable Administration program.

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

Setting	Description
Domain is disabled	Stops email being sent to the domain.
Abuse Address	Enter the email address or select the mailbox for the abuse@domain email address.
Postmaster Address	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 collect all emails for a domain that do not have a mapping to a mailbox. Either select an existing mailbox, or enter another email address to act as the catchall. Implementing a catchall will capture more spam, so make sure this mailbox is monitored. **Warning: It is advisable not to enter a remote email address or a local mailbox which is being redirected to a remote address as a catchall. Doing this will cause the server to on-send all the caught spam and is likely to result in blacklisting by the remote server and possibly putting the server on a global blacklist.** When an inbound connection via SMTP is made and there are multiple recipients to addresses that are destined for a catchall mailbox, only one message is delivered to prevent multiple copies of the same email being delivered. Messages that are delivered to a catchall will have the recipient list in the Received header, or on the alternate catchall header line, if this is enabled.
Act as Smart Host	Redirects all mail for the current domain to another mail server. This would be used if, for instance, the server was acting as a backup mail server for the domain. Specify a port number by adding a colon and port number after the IP address. e.g. 192.168.3.45:30. Do not enter the IP address of your MailEnable server, as it will create a message loop (the mail server will send to itself) and messages will finally end up in the Bad Mail directory. See section 5.1.8 for more information on smart hosting. 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 a domain is configured to send to a specific relay server (e.g. 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).

4.4.1.2 Blacklist

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

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 the domain “mailenable.com” was added to the blacklist for a domain, then the domain will not accept any emails from mailenable.com.

4.4.2 Create mailbox

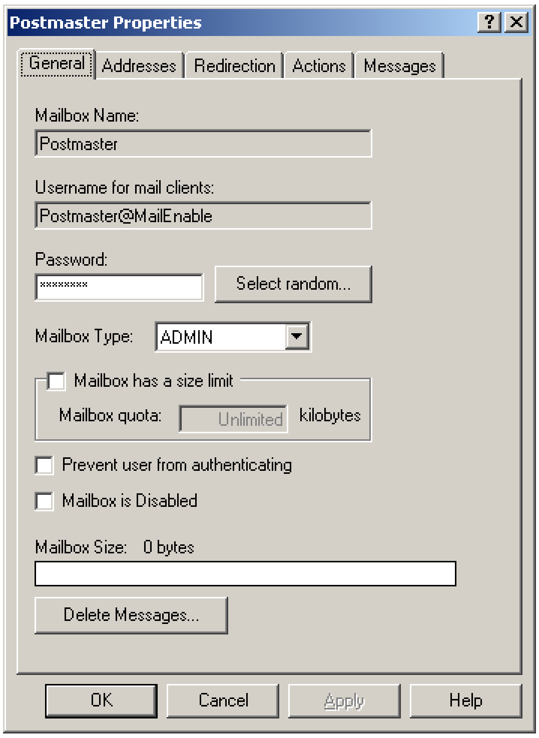
For a description of mailboxes, please see section 2.2.1.3.

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 4.2.1) 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, select the post office branch. Select **Create Mailbox** from the icons displayed.

4.4.2.1 General

The General tab of mailbox properties displays as below:



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: 0 bytes

Figure 4-5 Mailbox Properties – General TAB

Setting	Description
Mailbox Name	This is the name of the mailbox. Once created, this cannot be changed. This both identifies the user and ensures there is no duplication of mailbox names. As the mailbox name is entered into the text box, the POP Logon name entry just below it will change to reflect the entry.
Username for mail clients	This is the username used for logging onto the server via POP3. Use this information to set up the client mail software. The POP Logon name is the same as the “User Name” that is used by mail clients when they connect to the server to retrieve email. MailEnable uses the @ symbol to identify the post office the mailbox belongs to. This way, the same mailbox names can exist in different post offices (although the username to retrieve their email will differ, since the username is formatted as mailboxname@postofficename).
Password	The password for the mailbox. The client software uses this when connecting. If SMTP authentication is turned on, this password is also used for sending email. Other extensions to the MailEnable product may also use this username/password combination. The password that is set is the same as the password used by mail clients to authenticate when they connect to the server to retrieve email.
Select random password	Creates a random 8 character alphanumeric password.
Mailbox Type	Determines the access level for the mailbox. If the mailbox is given "ADMIN" rights, then the user will be able to administer this post office in MailEnable via the web administration interface. If the user is given “SYSADMIN” rights, then they will be able to modify any post office settings.

Mailbox has a size limit	Limits the size of the mailbox. If an email will take the size of the inbox over this limit, the email is bounced back to the sender.
Prevent user from authenticating	If enabled, this will prevent a user from authenticating or logging into any service where the credentials for the mailbox are supplied.
Logon Disabled	When a mailbox is disabled, it cannot be accessed via a service, such as POP3 or web mail. This setting is useful for suspending an account. It makes the mailbox or email mappings to the mailbox inactive, without deleting it.
Delete messages	Delete messages from the mailbox.

4.4.2.2 Addresses

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

To create new email addresses, select 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, select the **Add Email** button. The first text box, **Enter email name** is where the first part of the email address is entered. E.g. to add **sales@mailenable.com**, only requires the word 'sales' to be entered**.** The full address of the email being added is displayed in the window.

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

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

Setting	Description
Friendly Name	The Friendly Name is used as the display name for emails sent via web mail and for the sender for auto-responder messages. When sending messages from email clients, the friendly name is configured within the client application, not on the server.
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. It is only possible to add an email that matches an existing domain for the post office. When first creating a mailbox, MailEnable will automatically create email addresses for each of the domains for the post office.

4.4.2.3 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	Redirect all email for the mailbox to an alternative email address or addresses. To enable redirection, select the 'Redirect this mailbox to' checkbox. Select the Add button to add email addresses. If more than one email address is listed, the email will be copied to all of the addresses listed. There is a limit of approximately 25 email addresses that can be redirected to (the limit depends on the length of each email address). For a large number of redirections, use a group (see 4.4.11) - this allows an unlimited number of addresses.

Keep a copy of the message in mailbox	By default, when redirecting a mailbox to another email address a local copy is not retained. Enabling this option keeps a copy of all messages that are being redirected.

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

4.4.2.5 Messages

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

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

4.4.3 Export users

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

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

4. Enter the filename to save as and select Export.

4.4.4 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;

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

4.4.5 Import users

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

If quota limits are not specified in the import file, there is an option to set quotas to a certain limit, or unlimited.

If password settings are not specified in the import file, there is an option to set random passwords or create a set password for all imported users.

4.4.6 Delete messages

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

4.4.7 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 selects the **Email users** icon to send an email to all users of a particular domain.

4.4.8 Email users (individual)

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

4.4.9 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 subsequent ones that are added.

4.4.10 Edit default message

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

4.4.11 Create a group

For a description of groups, please see section 2.2.1.6

When creating a group, the group name is the full text description of the group (for ease of identification). The recipient address is the email address of the group and within this group there can contain multiple external groups. Groups can contain external addresses, so the one group can have different email addresses that are not hosted on the server.

Setting	Description
Group name	Create a name for the group e.g. All Staff
Group is disabled	Stops the group from working so that if someone emails the group address, the email will bounce back indicating that the address is not valid
Add email	Add other email addresses for the group e.g. allstaff@example.com

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

(NOTE: Be cautious of using the "Advanced" option if you have a large number of users in the post office)

To import users into a group from a text file, right click on the group icon in the tree view display and select the **All Tasks>Import Members** menu item.

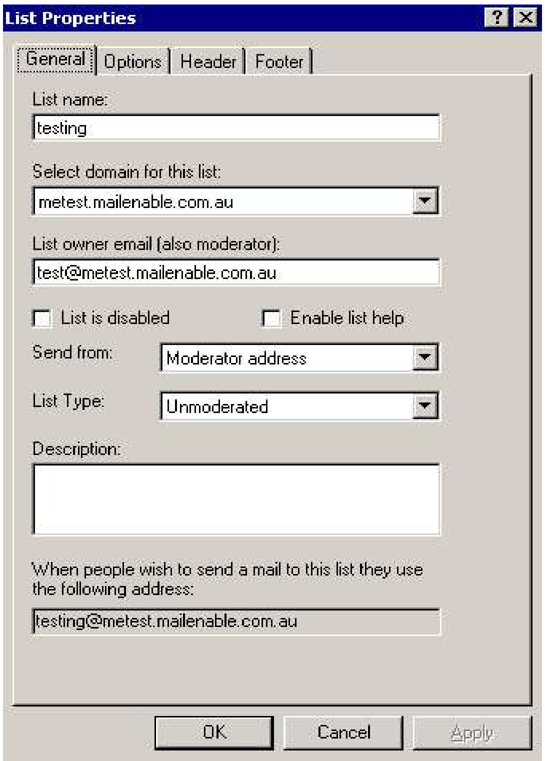
4.5 Lists

For a description of lists, please see section 2.2.1.5

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 to create a list for
- Right click the Lists folder and select New >List. This will load the List Properties window (see below) 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 4-6 List Properties window

4.5.1 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. The full email address for the list appears 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. If someone posts to the list with the subject of ‘help’ they will receive an email with details of what commands the list server will accept.
Send from	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.

4.5.2 Options

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

4.5.2.1 Subscription type

MailEnable can control how subscriptions are handled.

Setting	Description
Anyone can subscribe to this list via email	Allows subscriptions to the list by sending the word "subscribe" as the subject of an email to the list address.
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	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.

4.5.2.2 Posting permissions

MailEnable can 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	Password protects the list. To send an email to a password protected list, users need to enclose the password in square brackets and colons e.g. [: and :]

4.5.2.3 Reply options

These options 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 sent from the list, their email is 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 sent from the list, their email is sent to the moderator.

4.5.2.4 List subject prefix

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

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	Subject is not altered for any messages posted to the list.
Subject should have the following prefix	Specified text is added to the start of the subject line for all emails posted to the list.

4.5.3 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.

4.5.4 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.

4.5.5 Importing list members

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

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

4.5.6 List commands

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

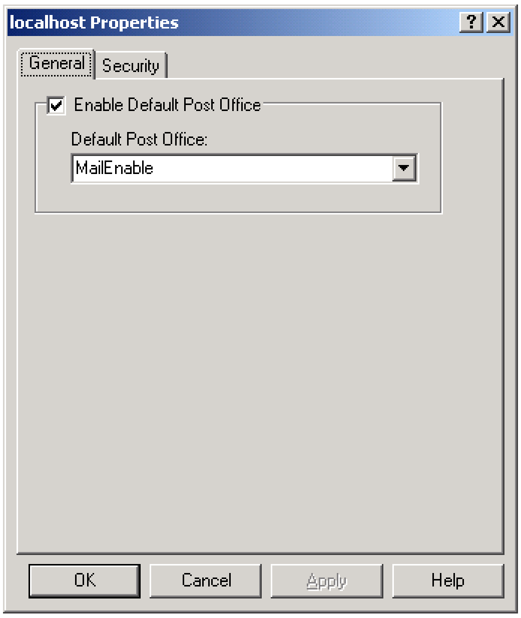
- Help – sends an email back with the available commands of the list server
- Subscribe – adds the user to the list (if the list permissions allow them)
- Unsubscribe – removes the user from the list

4.6 Server configuration

General server configuration options are available by selecting:

MailEnable Management > Servers > localhost

Right click to select Properties.



☑ Enable Default Post Office

Default Post Office: MailEnable

Figure 4-7 Messaging Manager General Options

Setting	Description
Enable Default Post Office	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@example.com* user will only need to use *sales* to log on with.

5 Configuration of Services and Agents

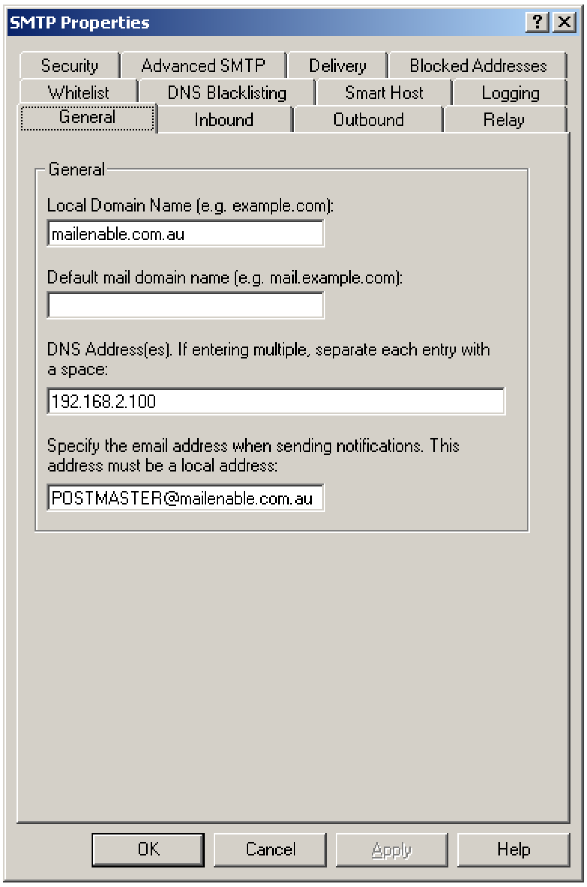
5.1 SMTP connector

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

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

Using the Administration Console 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:

5.1.1 General



General

Local Domain Name (e.g. example.com): mailenable.com.au

Default mail domain name (e.g. mail.example.com):

DNS Address(es). If entering multiple, separate each entry with a space: 192.168.2.100

Specify the email address when sending notifications. This address must be a local address: POSTMASTER@mailenable.com.au

Figure 5-1 SMTP Properties

Setting	Description
Local Domain Name	The domain name of the server that MailEnable is installed on, or the default domain for the configuration. It is used for system messages, to announce the server when it connects to remote server, and when remote servers connect to MailEnable if the host name has not been specified.

Default mail domain name	The default mail domain name for the server, which usually matches the default MX record. For example, if you have configured mail.example.com in your DNS to point to your mail server, then you would enter this here. If a host name has been specified for an IP address on the server, then that value will override this host name.
DNS Address	The DNS that the local machine uses. If using more than one DNS, separate the addresses with a space character. If the SMTP service fails to connect to the first DNS, it will try the second or subsequent DNS. Use the DNS that is configured for the local network. Remember that this is not necessarily the DNS of where the domain name is registered.
Specify the email address when sending notifications	The address from which notifications are sent. When MailEnable sends out email such as message delivery delays, or delivery failures, it will use this address as the "from" email address. Usually this would be postmaster@example.com (substitute your domain here). Make sure this is a valid email address.

5.1.2 Inbound

Setting	Description
SMTP service listens on port	Determines the port the SMTP service is running on. The default is 25. Inbound SMTP connections from remote servers expect the mail server to be listening on port 25, but some proxy or gateway software may require this to be changed.
Also listen on alternate port	The SMTP service can 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 number 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	Checks each inbound message size after it is received. If it is over the limit, it will be deleted and an error returned to the remote server or email client that is trying to send.
Access Control	Specify who can connect to the email server. Specify a list of IP addresses that are either banned from connecting, or are the only ones allowed to connect. Use the * character as a wildcard.
Inbound IP Bindings	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.

5.1.3 Outbound

Setting	Description
Maximum number of send threads	The number 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.
Outgoing queue poll interval	How often the SMTP service polls the outgoing queue directory for mail messages to send. This is measured in seconds.
Limit outbound message size	Forces MailEnable to check the size of each message before delivering to a remote mail server. If the message cannot be delivered it will be returned to the sender (or sent to the bad mail directory if the message is system generated).
Outbound IP Binding	Forces the SMTP to use a specific IP address on the server when it is trying to deliver email.

5.1.4 Relay

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

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

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

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

Setting	Description
Enable Mail Relay	Mail relaying needs to be enabled in order to send mail. Otherwise MailEnable will only be able to receive email. There are four options available to limit who can send mail out through the server. It is possible to select any combination of the four, however, a client only has to match one of the items in order to relay through the mail server.
Allow relay for authenticated senders	Requires that people sending mail through the server enter a username and password (i.e. this option enables SMTP authentication). To set this is different for various mail clients, but in Microsoft Outlook Express and Microsoft Outlook for instance, this is done in account properties via the "My server requires authentication" checkbox under the "Servers" tab. It is advisable to have this option enabled if the server is not using privileged IP ranges. Also, ensure that Secure Password Authentication (SPA) is not enabled.
Authentication method	Select the authentication method for authenticated senders. MailEnable/integrated authentication – uses the MailEnable username/password Windows authentication – uses the Windows username/password valid for that machine Authenticate against the following username/password – specify your own username and password.

Allow relay for privileged IP ranges	Allows people with certain IP addresses to send email through the server. If the IP addresses of persons who are able to send email out through the server is known, use this option. DO NOT select this option if the list of IP addresses is unknown, as this may inadvertently allow everyone access. This option is usually required to allow sending through the server from a web server or web page.
Allow relay for local sender addresses	Allows people to send mail if their 'From' address has a domain that is hosted on MailEnable. For instance, if you host example.com, and someone sends a message from your server that has their 'From' address as peter@example.com, the email will be sent. Unfortunately, spammers may still abuse this by spoofing 'from' addresses, so most servers will not use this option. Using this option may cause some anti-spam blacklists to consider the server as "open relay" and block email from the server.
POP before SMTP authentication	The IP address of users who authenticate via POP is remembered and permitted to relay. The time period to remember the IP address for can be set. Some client applications will try to send email before retrieving (e.g.: Microsoft Outlook), so they will generate an error message on the first send try. Subsequent send attempts will then work if they are before the specified time. This is required due to some ISPs and certain routers not allowing SMTP authentication. This feature will bypass this issue by authenticating a client using POP. If this authenticates then the SMTP service will allow this IP access for a designated period of time. To remember the IP address, a file is written to the Mail Enable\Config\Connections directory. The file name is the IP address and the file extension is .pbs.

5.1.5 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.
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 used to force clients to use a legitimate email address, thereby reducing the possibility of spam.
Hide IP addresses from email headers	By default, the IP address of a client connecting is displayed in the header of an email message. If the network has its own IP range which is to remain hidden to receivers of emails, this option will replace the IP address with 127.0.0.1
Require PTR DNS entry for unauthenticated connections	If an inbound connection has not been authenticated, MailEnable will look up to see if there is a PTR DNS entry for the connecting IP address. MailEnable will not validate whether the entry is valid, it will check to see if one exists. Local IP addresses are not checked for PTR entries.
Disable all catchalls	Catchalls for domains will cause the server to collect a lot more email and may cause the server to relay spam (i.e. if a catchall is redirected to a remote email address). This option will stop all catchalls from working.

Allow domain literals	MailEnable will allow inbound emails to be formatted as user@[IP Address], such as user@[192.168.3.10]. MailEnable will accept emails for any of the IP address that have been configured on the server. If using NAT, or to accept extra IP addresses which are not configured on the server, select the Advanced… button that will allow these extra IP addresses to be entered.
Use alternate welcome message	When an email client or other mail server connects to MailEnable, a one line welcome message is displayed. By default, this indicates that the server is running MailEnable software, and shows the version of the software. If this option is enabled, it is possible to customize the welcome message. There are also two variables that can be used in the welcome text that will be replaced. These are: %LOCALDOMAIN% - this will be replaced with the SMTP domain from the SMTP options %TIME% - this will be replaced with the current time on the server
Restrict the number of recipients per email	It is possible to restrict the number of recipients per incoming email. Allowing a large number of recipients per message may help with sending to contact lists via email clients, but it also raises the benefit to spammers, as they can save on bandwidth and can send through more messages in a shorter amount of time.
Drop a connection when the failed number of commands or recipients reaches	Most email clients will recognize error codes returned by the mail server for an invalid recipient or similar. But some spammers and bulk email utilities may not recognize these errors and keep trying to send. By enabling this option, MailEnable will drop the client connection. It is recommended not to use a low value (5 for example), as some valid web scripts will not check the return codes either – but these will only produce a small number of failed commands.
Add to denied IP addresses if this number is reached	If a connection has reached the disconnection limit, it is possible to automatically add the IP address of the client to the SMTP Access Control list. Be aware that if enabling this option, the Access Control list can grow and adversely affect the performance of the SMTP service. Therefore it is recommended to check the Access Control list regularly.

5.1.6 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 can 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. Some mail servers require these items and will reject the email if they do not exist. By enabling this option, MailEnable will add the required lines (if they do not exist) to all users who are authenticated to relay through MailEnable.
Allowed SMTP Commands	The list of SMTP commands that can be disabled are shown here. For example, it is possible to disable the EXPN, which displays all the emails of users in a group.

5.1.7 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 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.

5.1.8 Smart Host

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

5.1.9 Logging

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.

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

5.1.10 Blocked addresses

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

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

5.1.11 White list

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

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

5.1.12 DNS blacklisting

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

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

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

Configure reverse DNS blacklisting as follows:

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

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: It is possible to 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 the provider has been added, this can be configured using the screen outlined earlier. Select the Enable button before configuring the service provider’s details.

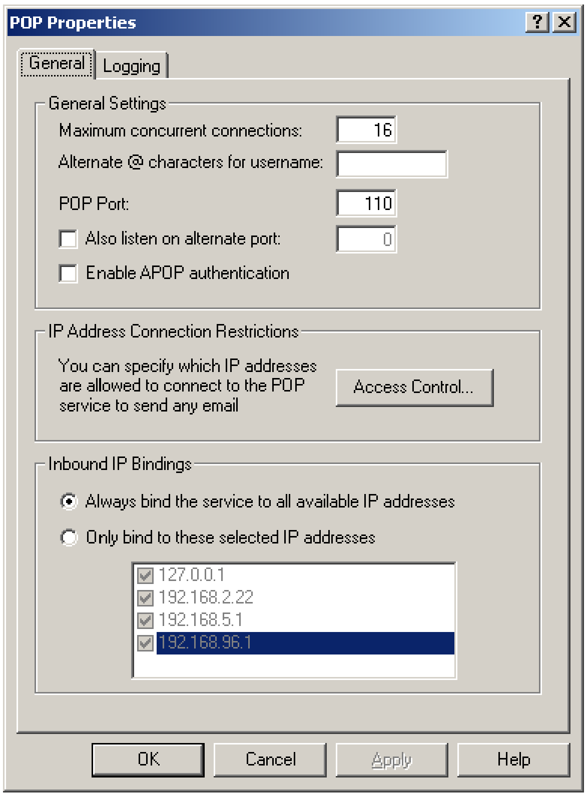
5.2 POP connector

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

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

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

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



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
☑ 192.168.2.22
☑ 192.168.5.1
☑ 192.168.96.1

Figure 5-2 POP Properties dialog box

5.2.1 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 do not allow the use of @ in the username section. Since the MailEnable usernames are formatted in mailboxname@postoffice format, this may cause problems. To solve this, MailEnable can specify the characters that can be used as a substitute. Just enter the list of characters such as #$%. This will allow users to log on using mailboxname@postoffice, mailboxname#postoffice, mailboxname$postoffice and mailboxname%postoffice.
POP Port	This is the port MailEnable will allow client POP connections on. The default is 110.
Also listen on alternate port	Allows the POP service to listen on an alternate port. Usually this is done to cater for clients who may be on connections where their outbound port 110 has been blocked.

Enable APOP authentication	Usually, the users' username and password are sent in clear text format (i.e. not encrypted). Enabling this option will force clients to enable APOP authentication on their mail client software. Make sure users are using software that supports APOP, otherwise they will not be able to receive email. Some older mail clients do not support APOP.
Access Control	Specify who can connect to the POP service. A list of IP addresses that are either banned from connecting, or are the only ones allowed to connect by selecting the Access Control button can be specified.
IP Addresses to bind POP to	It is possible to select the IP addresses that the POP service will be bound to. On a multi-homed machine you may only wish to allow connections on particular IP addresses. 'Always bind all IPs' will allow connections on all IP addresses that are configured for the machine.

5.2.2 Logging

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

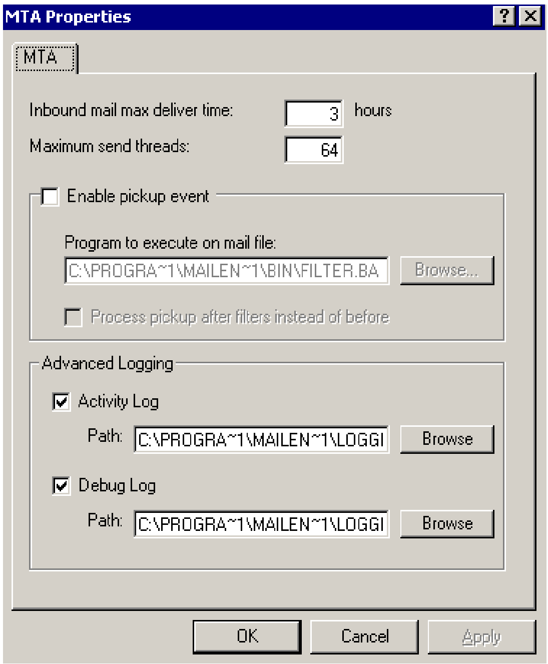
5.3 Mail Transfer Agent (MTA)

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

Examples of MTA functionality follow:

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

5.3.1 MTA Properties



MTA Properties

MTA

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 5-3 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 number of concurrent threads that will be used to move emails around. Some command line virus checkers do not function correctly with multiple instances running, so the MTA can be restricted to using one thread to resolve this.
Enable pickup event	Executes a program or application when mail arrives. 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. The directory path will need to read 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 to obtain more details about what the service is doing.

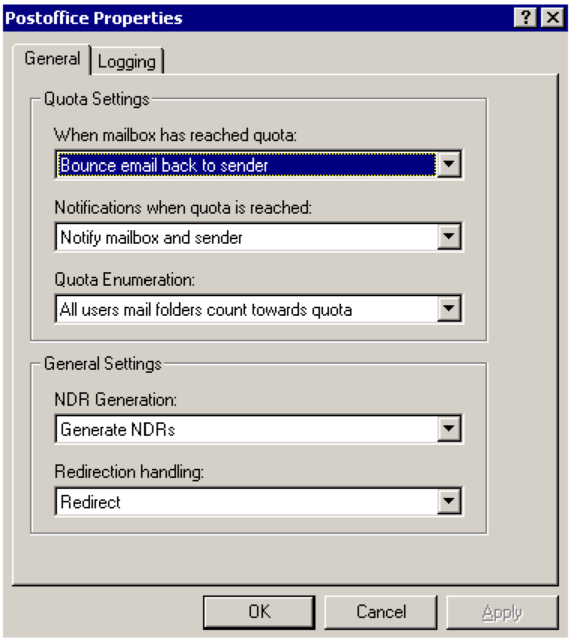
5.4 Post Office Connector

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.

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

MailEnable can configure what notifications are sent when a quota is reached. Non Delivery Receipts can also be configured. Using the Administration Console the Post Office Connector properties can be accessed 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 5-4 Post Office Connector Properties

5.4.1 General

Setting	Description
When mailbox has reached quota	Specify what occurs when a mailbox's quota is exceeded. Determine whether the user is notified of the quota issue and whether the message is returned to the sender, or, sent to the postmaster for that post office.
Notifications when quota is reached	Configure what notifications are sent when a quota is reached, options include ▪ notify sender only ▪ notify sender and mailbox ▪ 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 has the following settings: 1. Normal redirection - will redirect emails. Redirected emails have the envelope sender of the original message preserved. 2. Remail from mailbox address - will redirect and send using the default email address for the mailbox. If a default address has not been set, the first address found for the mailbox will be used. This option will help prevent rejections from remote servers who are using SPF checking. 3. Disable all redirections – will prevent any redirections configured for a mailbox from working.

5.4.2 Logging

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

6 Operational Procedures

6.1 Backing up and restoring data

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

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

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

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

To do this requires the registry editor (REGEDIT) to export the 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, stop all services, replace the directory tree from the backup and then import the saved registry file into the registry.

6.2 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 the debug session is completed, close the console window.

Ensure that the value of the registry key is set back to 2 when the debug session has finished.

6.3 Inspecting log files

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

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

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

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

6.4 Configuring 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.

6.4.1 Configuring Netscape Messenger

- Start Netscape
- Select Edit then Preferences from the menu bar
- Select the '+' symbol on the right of Mail & Group
- Select Mail Server option
- Enter values in the input boxes
- To avoid re-entering the password every time email is checked, select More Options, then tick Remember mail password
- Select ‘Identity’
- Type in the full name or business name in Your Name: input box
- Type in the email address (e.g. info@mydomain)
- Type in the reply email address (e.g. info@mydomain)
- Select OK to accept new settings.

6.4.2 Configuring Microsoft Outlook Express

- Open Outlook Express.
- Select 'Tools | Accounts...'.
- Select the 'Mail' tab.
- On the right side, select 'Properties'.
- Now select 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**.

6.4.3 Configuring Microsoft Outlook

- Access the Tools > Accounts menu.
- Select the Mail tan and select Add > Mail.
- Enter an appropriate display name.
- Enter the e-mail address.
- Specify the incoming and outgoing mail servers. E.g. mail.[example].com.
- Specify the Account Name and Password. The Account Name is formatted as Account@Postoffice.
- Specify how to connect to the mail server.
- Select Finish

For assistance in setting up other mail clients, please refer to the MailEnable web site.

6.5 Manually testing if MailEnable can send mail to remote servers

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

Instructions follow:

1. From the Windows Start Menu select **Start|Run** and enter CMD as the application to run. Select **OK**
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 this was successful, then no firewall (either local or the ISPs) is preventing outbound SMTP traffic. The next procedure to try is sending an actual message to the remote host (rather than just determining whether it is possible to connect). Firstly, determine which remote server to connect to. A domain may have more than one server that is accepting email, and these servers may not match the domain name. The MX records that have been configured in a DNS determine the mail servers for a domain. To retrieve the mail server details for a domain, use the nslookup command line utility. For example, to check which servers are accepting email for AOL, you can enter:

```
nslookup –type=MX aol.com
```

This will return the details of the mail servers, these results can be used as the hosts to connect to.

This is outlined as follows:

4. From the Windows Start Menu select Start|Run and enter CMD as the application to run. Select OK.
5. At the command prompt, enter the following: telnet mail.mailenable.com 25

The remote mail server should respond with an initiation s*tring much like the following:*

```
220 mailenable.com ESMTP Mail Enable SMTP Service, Version: 1.1 ready at 02/28/03 14:04:45
```

6. Type the following and press Enter: HELO YourDomainName

The server should reply with a line similar to:

```
250 Requested mail action okay, completed
```

7. 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
```

8. 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
```

To have multiple recipients for an email, enter the recipient to line more than once. This is how a blind carbon copy works. If the recipient does not exist, this may generate an error such as:

```
550 Requested action not taken: mailbox unavailable or not local
```

9. Now indicate to the server that you want to send the email date. Type the following and press Enter: DATA

The server should reply with something like
354 Start mail input; end with <CRLF>.<CRLF>

10. 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]
```

11. Type the following and press Enter:

```
QUIT
```

If this was successful, then MailEnable should be able to send messages to the remote host. If an abnormal response is received for any of the commands typed in, then search the MailEnable Knowledge Base for any articles that may give an indication of the cause of the error.

Example:

```
C:\>telnet mail.mailenable.com 25
220 mailenable.com ESMTP MailEnable Service, Version: -2.3- 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.
```

6.6 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 it is only required 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 time-stamped 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. The log file can be loaded into Microsoft Excel as follows:

6.6.1 How to import the Activity log into Microsoft Excel

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

A worksheet will be displayed with data represented as follows:

A=Transaction date and time

B=Transaction Type (Inbound or Outbound)

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

D=Internal socket 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.

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

The most obvious way of relating an entry in the activity log file to the Debug log file is via the time stamp recorded in the file. The message ID can also be used (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 MailEnable's 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.

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

Use this error string to locate the transaction sequence in the SMTP Activity log. Once the entry has been found in the SMTP Activity log, then check the SMTP Debug log for the same time period. The log will have recorded the reason why the relay request was denied.

6.7 Configuring redundant or backup (MX) mail servers

There are two principal ways to configure redundancy with MailEnable.

The simplest way to achieve redundancy is to install a copy of MailEnable as the master server. Then install separate copies of MailEnable on other servers and smart host the domains to the IP address of the master server. This will mean that if the master server is down, that the auxiliary servers will accept mail for the domains and hold it until it is online.

The DNS/MX settings for the domains will need to be changed in order to configure the appropriate MX preferences. Other mail servers learn about your mail server via DNS MX records. They are the means by which someone enumerates a target domain to the server responsible for receiving mail for that domain. MX records have a preference associated with them that determines the order in which they are used.

The lowest preference is attempted first. The lower the preference value, the higher the priority. Hence an MX record with a preference of 1 would be attempted before an MX entry with a preference of 10. More info on DNS and MX records is available at: http://www.mailenable.com/kb/viewarticle.asp?aid=19

The above-mentioned approach is used if the backup mail servers are distributed in different geographic or logical locations.

A second alternative is to host all of the mail servers on the same local network and cluster the servers. This allows MailEnable to be installed on multiple servers and have them all use the same store for their messages and post office data. Any of these servers can then be used to access the mail. This requires that one of the servers share the mail data and configuration directories and that the others access them.

7 Glossary

Term	Explanation
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 be 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 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.
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.