1 Table of Contents

2 Introduction

2.1 Introduction

Contact the MailEnable Team

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

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

91 Chadstone Road
Malvern East, 3145, Australia
Tel: +613 9568-4270 (AEST)
Email: sales@mailenable.com

Support

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

https://www.mailenable.com/support

Web site

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

Knowledge base

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

Forums

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

How to download

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

https://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.

2.2 Prerequisites

Pre-requisites

Component	Requirement
Operating System	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 (including R2) • Windows Server 2008 R2 • For details on running on non-server operating systems, please see: https://www.mailenable.com/kb/Content/Article.asp?ID=me020357 • Server core versions of Windows are not supported
Memory	• 4GB RAM or higher free
Hard disk	• 190MB hard disk space (excluding space for email data and configuration)
Others	• Network interface card configured to use TCP/IP • Internet connection (with fixed IP and access for at least port 25 inbound to accept email) • Microsoft IIS v6.0 or Web Server (IIS) role required for webmail, web administration and ActiveSync capabilities • Microsoft .NET Framework 3.5 or later (for webmail & web administration)

Note: While the MailEnable product suite can be installed and has been tested on workstation environments and older versions of Windows Server the company does not support these platforms.

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.

2.3 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 when something goes wrong. The information in this section is not specific to MailEnable; this applies to all mail servers. This information is essential to know in order to properly administer an Internet mail server.

Email Clients

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

Some examples of email clients include

- Microsoft Outlook
- Mozilla Thunderbird
- eM Client
- Mail (for the Mac and iOS devices)

Email server

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

Sending and receiving mail

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

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

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

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

2.4 What's New in Version 10

The following section outlines the new functionality provided in Version 10 of MailEnable.

Desktop Webmail Chat

Version 10 Webmail now provides an array of chat and real-time messaging capabilities.

The Webmail client lists online users and allows file sharing/video calls from within the browser. You can also invite third parties to participate in interactive video/audio chat. Chat sessions are fully secured and all communications can be fully encrypted.

Jabber/XMPP Chat Service

The XMPP service allows desktop and mobile XMPP/Jabber clients to connect and participate in video calls.

These clients provide the same functionality as other messaging clients (like Skype/Messenger), however communication can be restricted within your organization and can be encrypted. Desktop users can also install chat/video chat clients (like Jitsi) to provide messaging capabilities.

Mobile Webmail Video Chat

Your mobile device can now be used to place video calls, share files and chat with your colleagues.

MailEnable has integrated JSXC with both mobile and webmail clients. This provides a powerful real time messaging and collaboration solution within the context of your organization. You can also facilitate chat sessions with people who are not registered in your postoffice. If you add a contact who is external then the user will be sent a message providing them with a temporary login and a URL. When the person signs in, they will be visible in your roster and will be able to engage in text and video chat..

Feature Availability

Version 10 Features	Standard	Professional	Enterprise	Premium
Video/Audio Chat			x	x
Screen Sharing			x	x
Multi-User Chat			x	x
Integrated Webmail Chat		x	x	x
Integrated Mobile Chat		x	x	x
XMPP Sockets Chat Service		x	x	x
Proxy Authentication for ActiveSync		x	x	x
Integrated SOCKS5 Proxy	x	x	x	x
Integrated HTTP Upload Service		x	x	x

Version 10 Features	Standard	Professional	Enterprise	Premium
SSL and TLS Support (new for Standard)	x	x	x	x
Email Backup Collection		x	x	x
File Transfer Client Bridging for XMPP		x	x	x
Improved Webmail Layout/Interface	x	x	x	x
Webmail Speed Improvements	x	x	x	x
Allow E-Mail Addresses as User Names	x	x	x	x
Enhanced Mobile Webmail	x	x	x	x
SNI Support	x	x	x	x

3 Overview

3.1 Overview

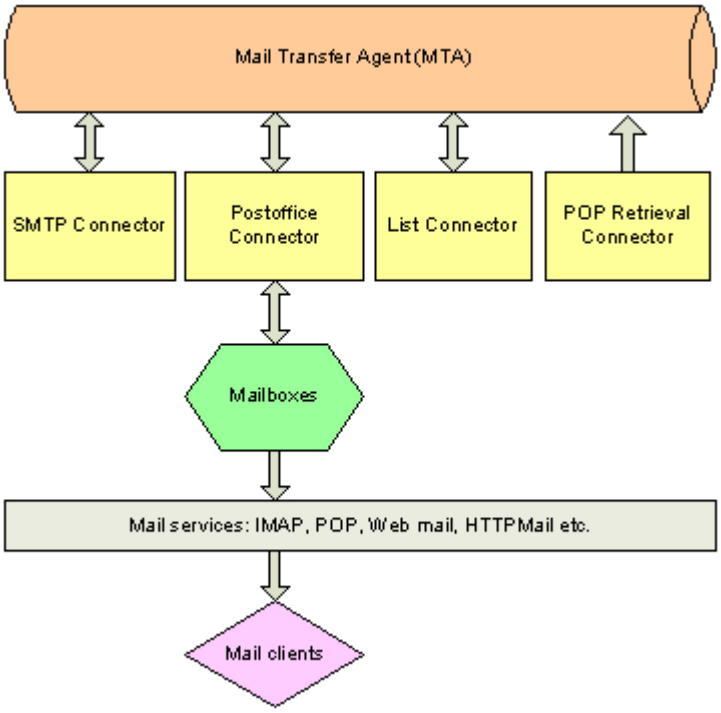
MailEnable has multiple services that interact in order to deliver a message to a mailbox. This interaction is done by a system of queues, which are used to move the emails around. The actual moving of the messages is done by the MTA service, which is logically the central service to the whole MailEnable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

3.2 Structure of MailEnable

Structure of MailEnable

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

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.



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
- Web mail

Each of these mail services is described in more detail in the Configuration of connectors, services and agents section.

Connectors

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

SMTP connector

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

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.

List server connector

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

Agents

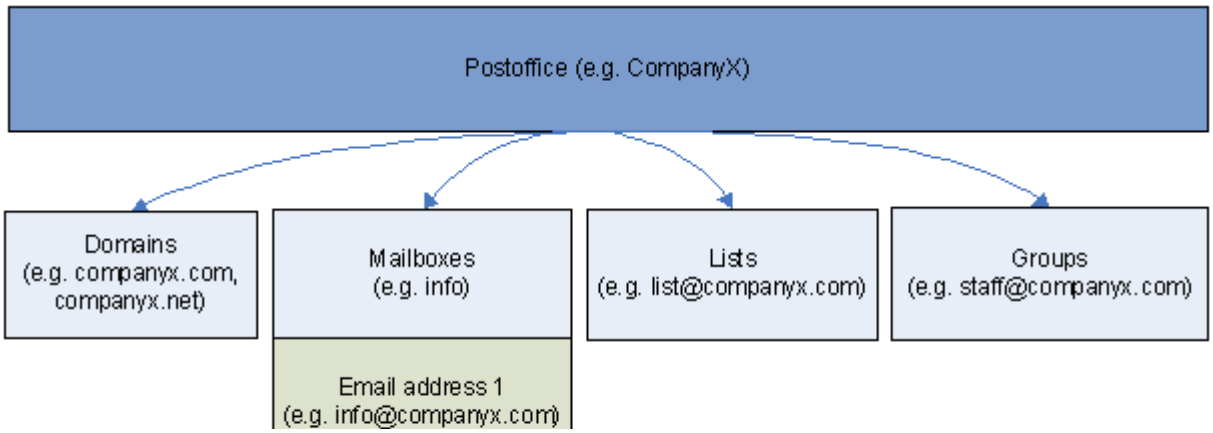
Mail Transfer Agent (MTA)

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

3.3 Administration

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

- Post offices
- Domains
- Mailboxes
- Lists
- Groups



Post offices

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

Domains

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

Mailboxes

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

Email addresses

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

Lists

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

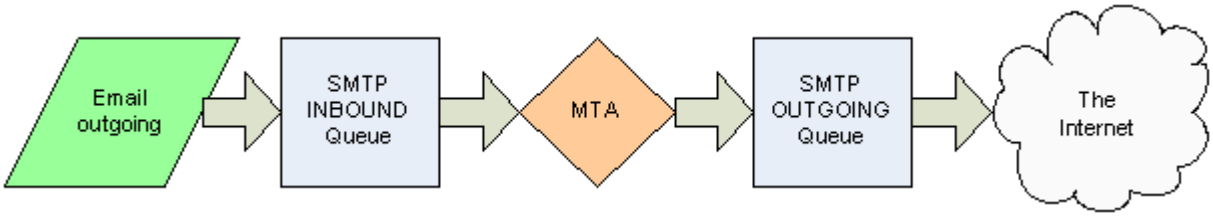
Groups

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

3.4 Email Delivery Flow

Sending Email

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



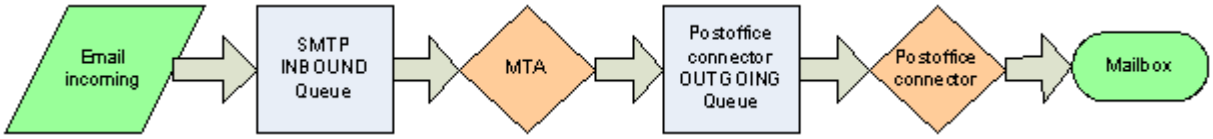
Requiring users to authenticate against the server prior to sending email can stop spammers from using the mail server to send email out to anyone.

When email is being delivered to a local address, this is not relaying, and MailEnable will always accept this

email. This is how email is received from other mail servers on the Internet, as they do not need to authenticate.

Receiving Email

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



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

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

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

4 Installation

4.1 Installation Overview

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

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

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

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

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

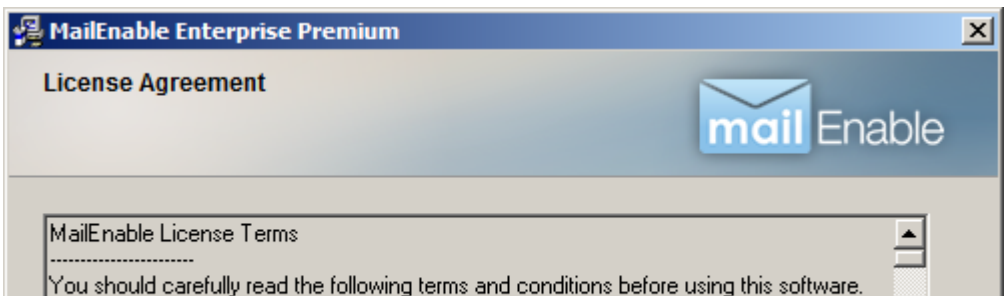
4.2 Installation

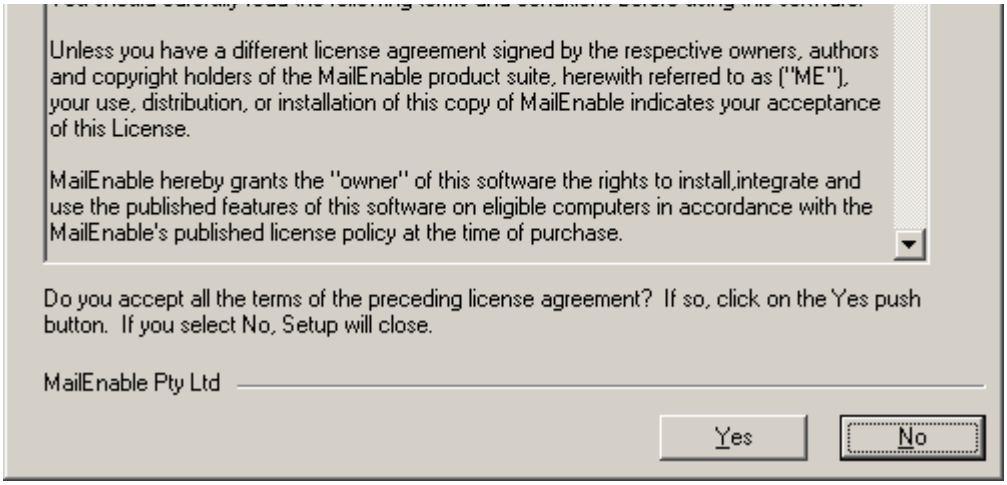
Welcome screen

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

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

Please click the Next button to continue.

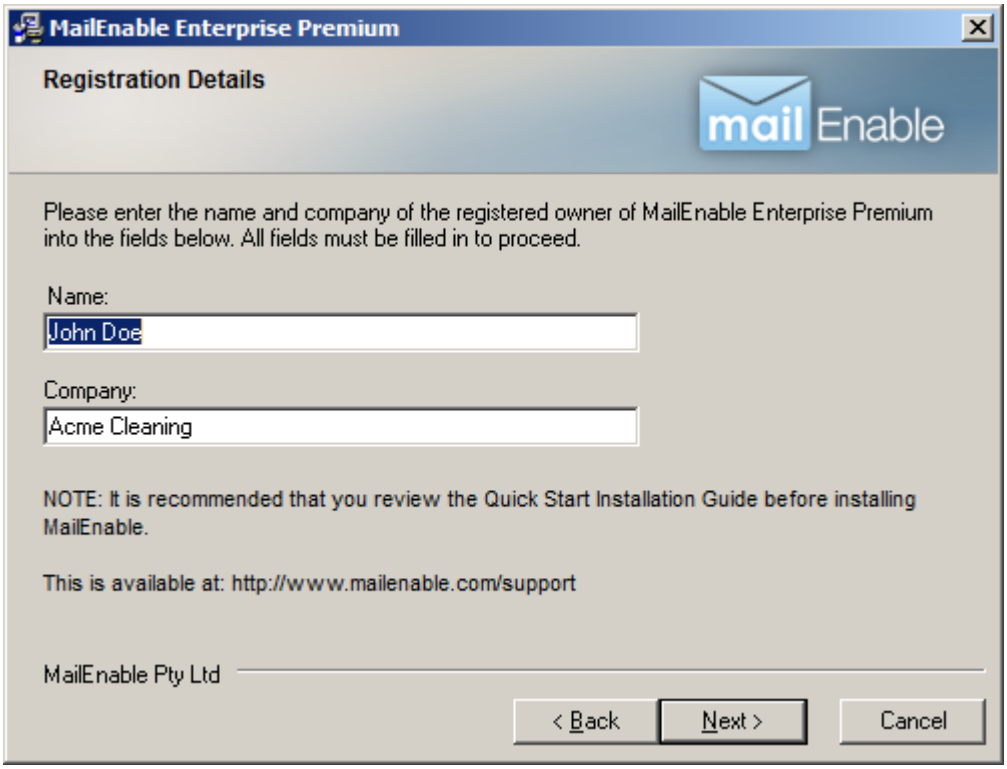




Registration details

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

Please click the Next button to continue.



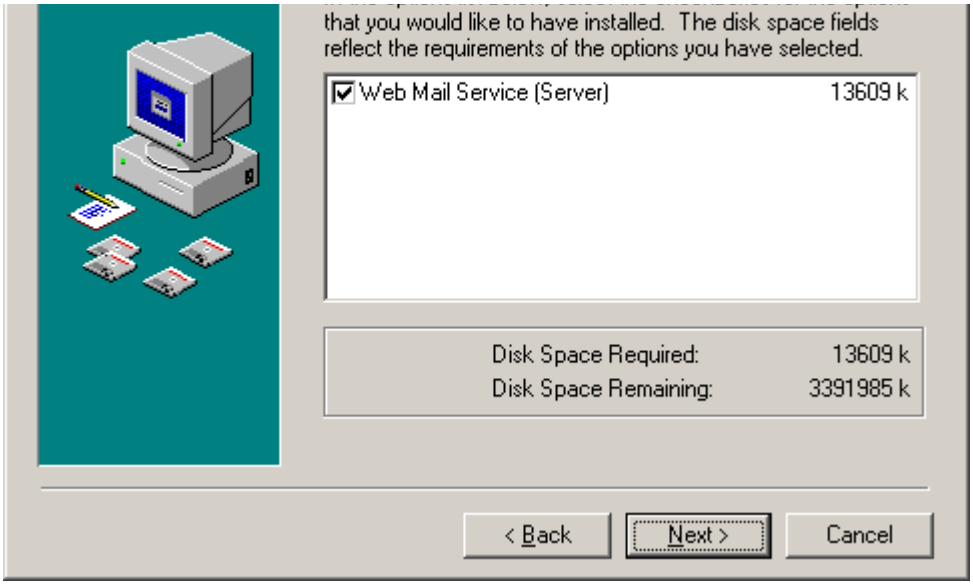
Select installation components

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

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

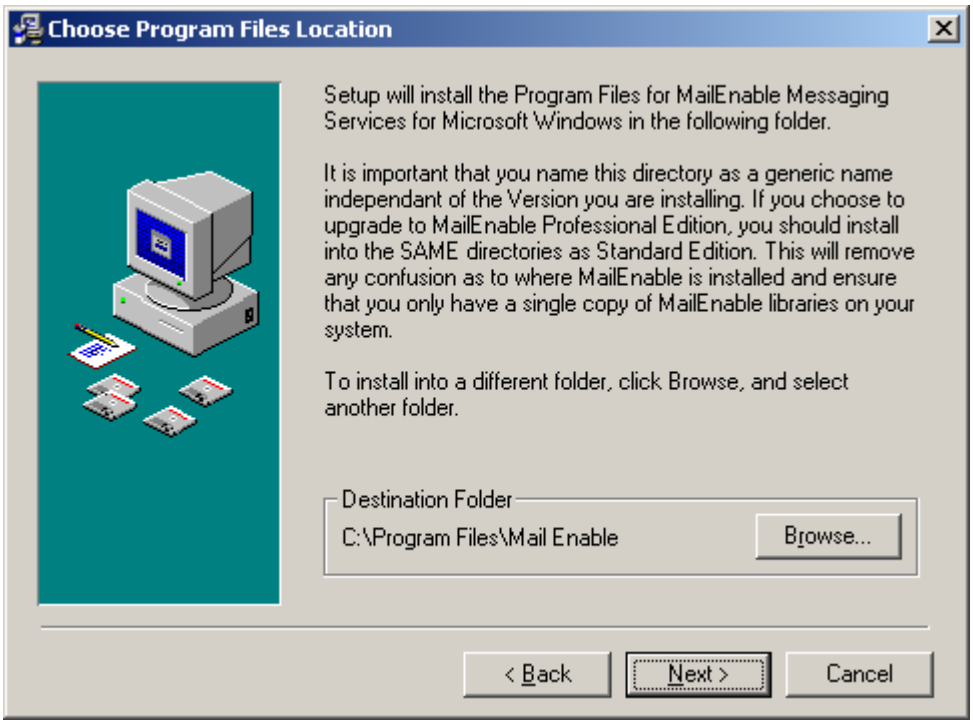
Select the components to install. Check that there is enough disk space required to install the selected components.

Please click the Next button to continue.



Choose program installation location

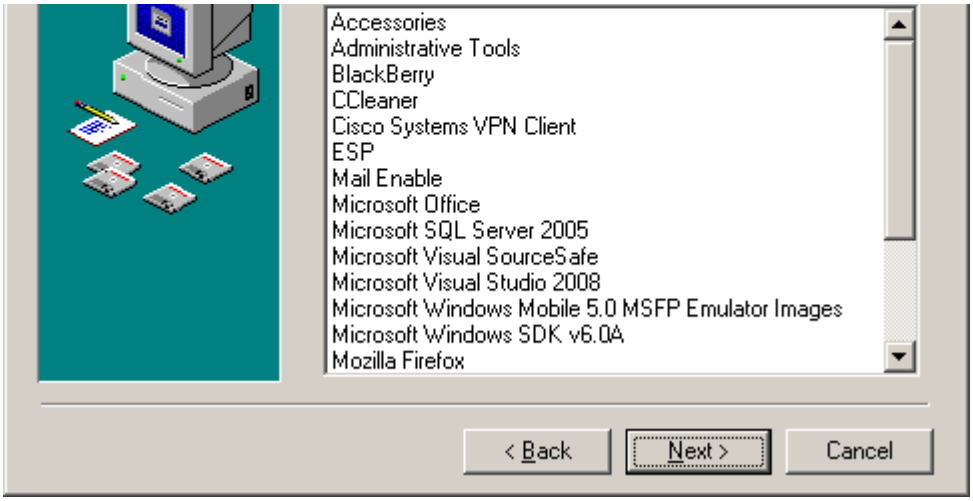
Setup will prompt to nominate where to install its configuration and binary files. By default, MailEnable will install itself under the "Program Files" directory. This can be changed to a different directory by selecting the Browse button.



Select Program Manager group

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

Please click the Next button to continue.

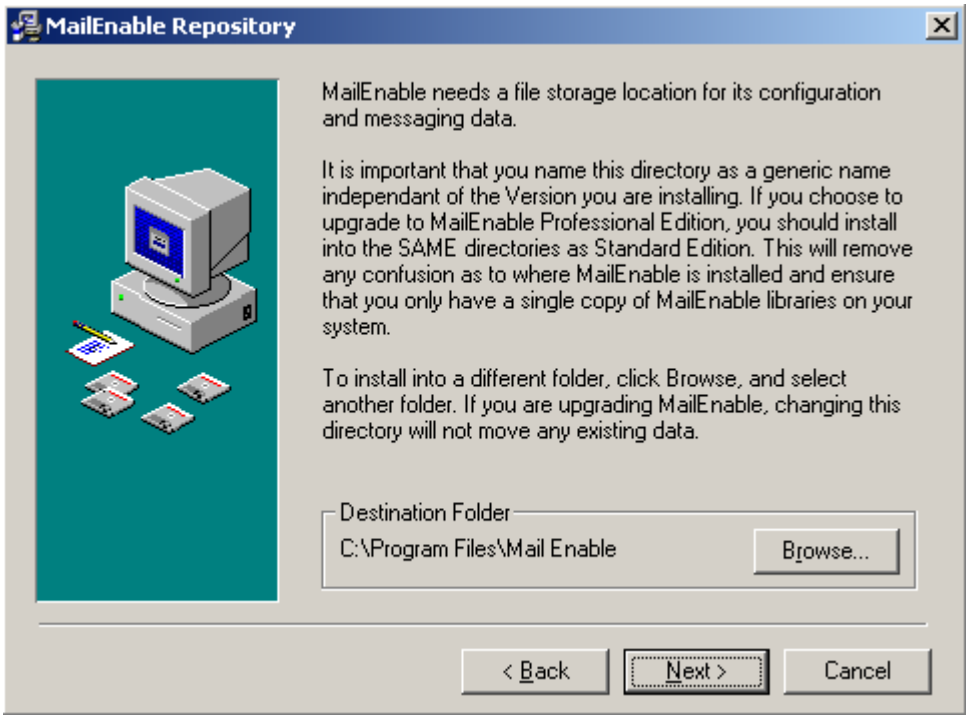


Selecting Repository

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.

Please select the [Next] button to continue.



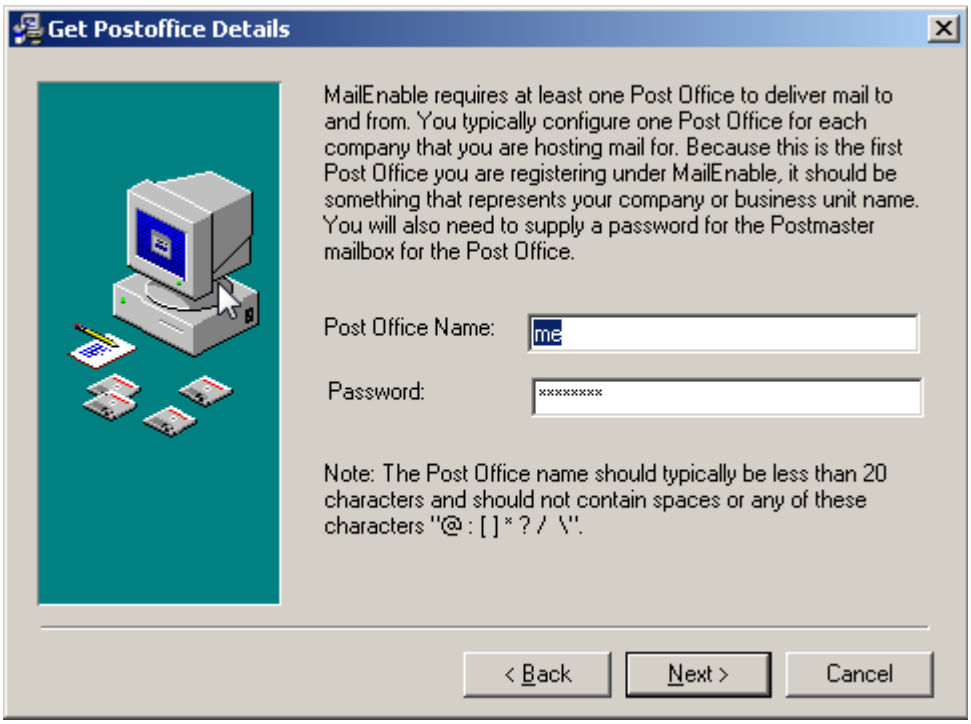
Creating an initial post office

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

A password needs to be assigned for the manager or postmaster of this new post office. The mailbox for the manager of a post office is called postmaster and is given administrative privileges for that post office (this

allows the postmaster to administer the post office via web administration). It is advisable to use a complex password for this mailbox, and this password can be changed later.

Please click the Next button to continue.

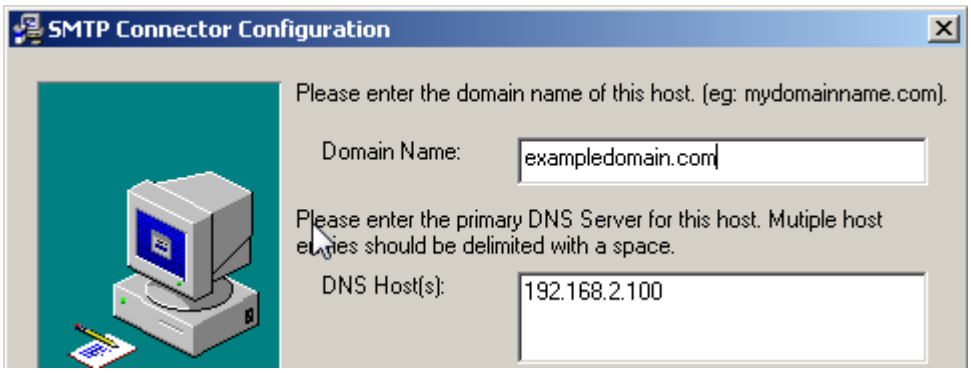


SMTP connector configuration

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

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

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 click the Next button to continue.

Start installation

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

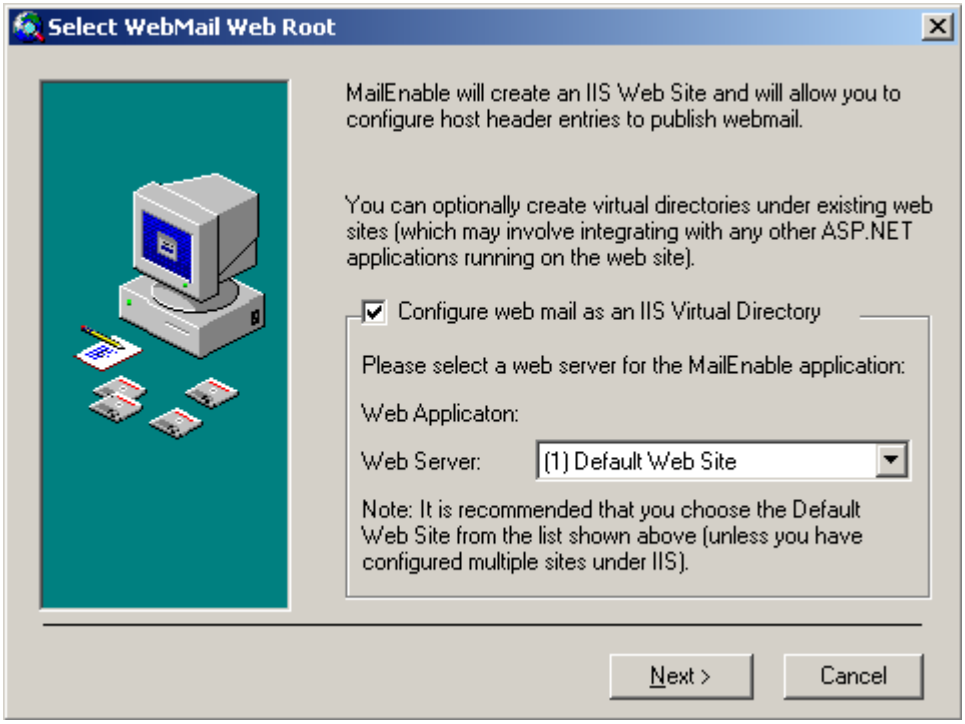
Please click the Next button to continue.

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

Select web mail site

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

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



Please click the Next button to continue.

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

Completing installation

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

Please click the Finish button to complete installation of MailEnable.

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

4.3 Upgrading

4.3.1 Upgrading

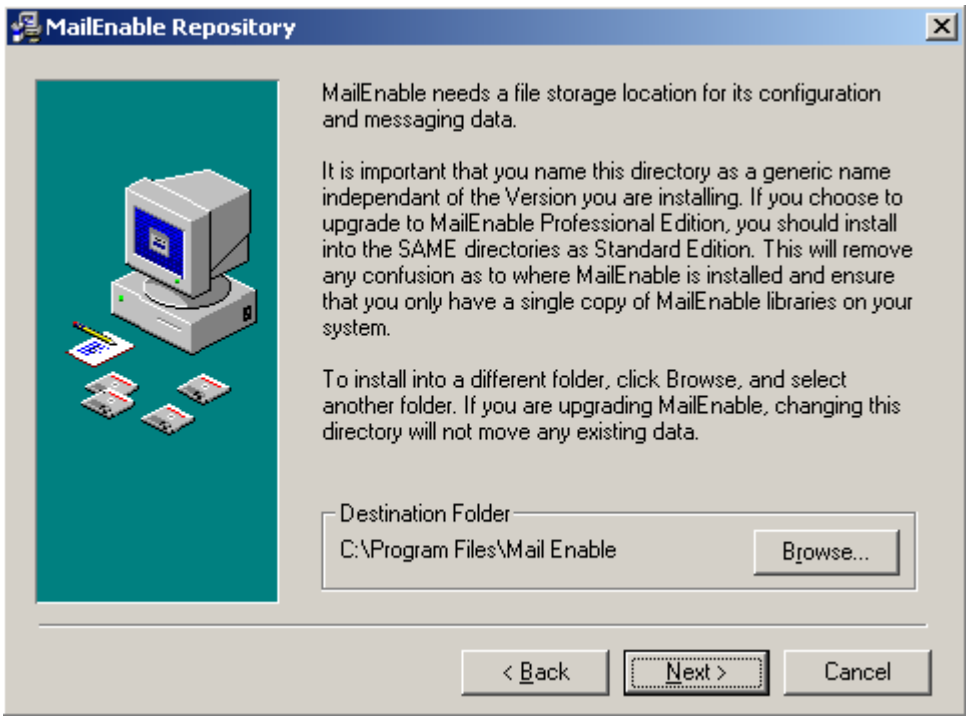
To upgrade to MailEnable Enterprise Premium from either Standard Edition, Professional, Enterprise or earlier version of Enterprise Premium editions, follow the same steps as outlined in the **Installation and upgrading section (Section 4.1)**. As the same data stores are used, it is possible to run the installation over the top of the current configuration.

MailEnable will detect the old version and retain the old settings (unless otherwise specified). More information on how to upgrade MailEnable to a newer version can be found within the following Knowledge base article: https://www.mailenable.com/kb/content/article.asp?ID=me020040

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

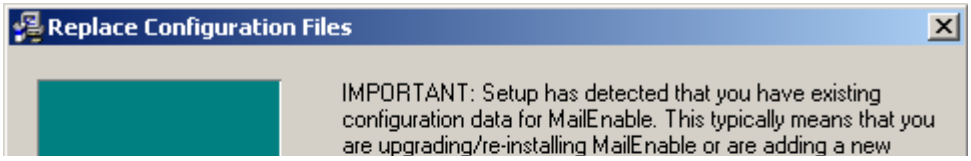
4.3.2 Configuration repository location

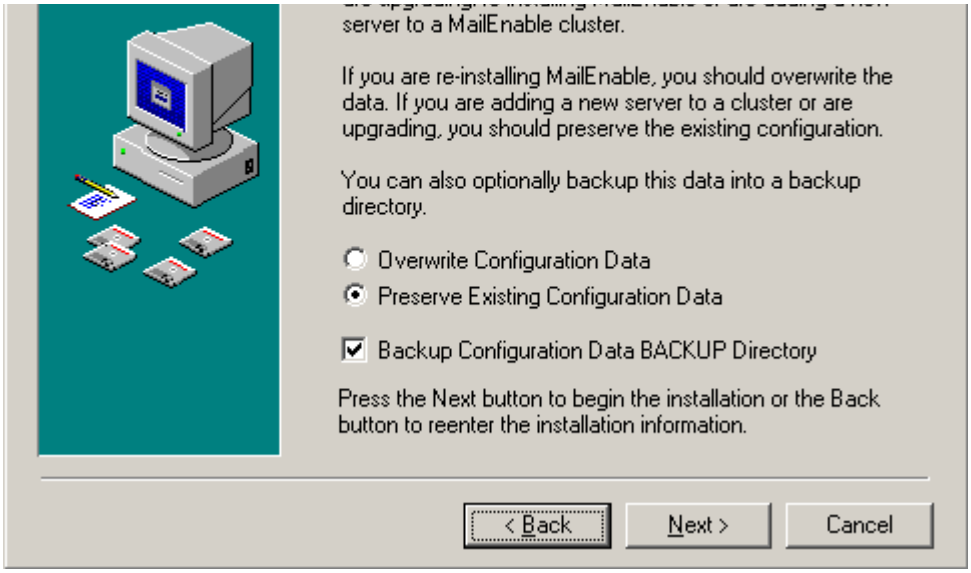
When MailEnable is installed over an existing installation, the installation program will prompt for the location of the configuration repository. It should default to the current configuration location as used by the existing installation of MailEnable.



4.3.3 Replace configuration files

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





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

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

4.4 Post-installation configuration

4.4.1 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.

How to access the MailEnable diagnostic report

1. Navigate within the MailEnable Program Group or;
2. Navigate within the MailEnable Administration console under Servers>localhost>System>Diagnose or;
3. Open a Windows "Run" command and type "mediag" (without quotes).

Once the Diagnostics Utility has been selected, it may take up to a minute or so to load, depending on the number of domains and postoffices. A web page will be invoked and will give a test output of all services installed within the MailEnable program. In order to rerun the Diagnostic through the Administration program, right click on the Diagnose icon and select ‘Refresh’ from the popup menu. The ‘Refresh’ option can also be used if the page does not properly load.

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

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. Click 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 the **SMTP connector - Relay section (Section 6.6.5)**.
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.

4.4.2 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 then it is likely that emails sent from the server will not be accepted by most major email services.

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 (https://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.

4.4.3 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 https://www.mxtoolbox.com

4.4.4 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 click **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.

5 Administration

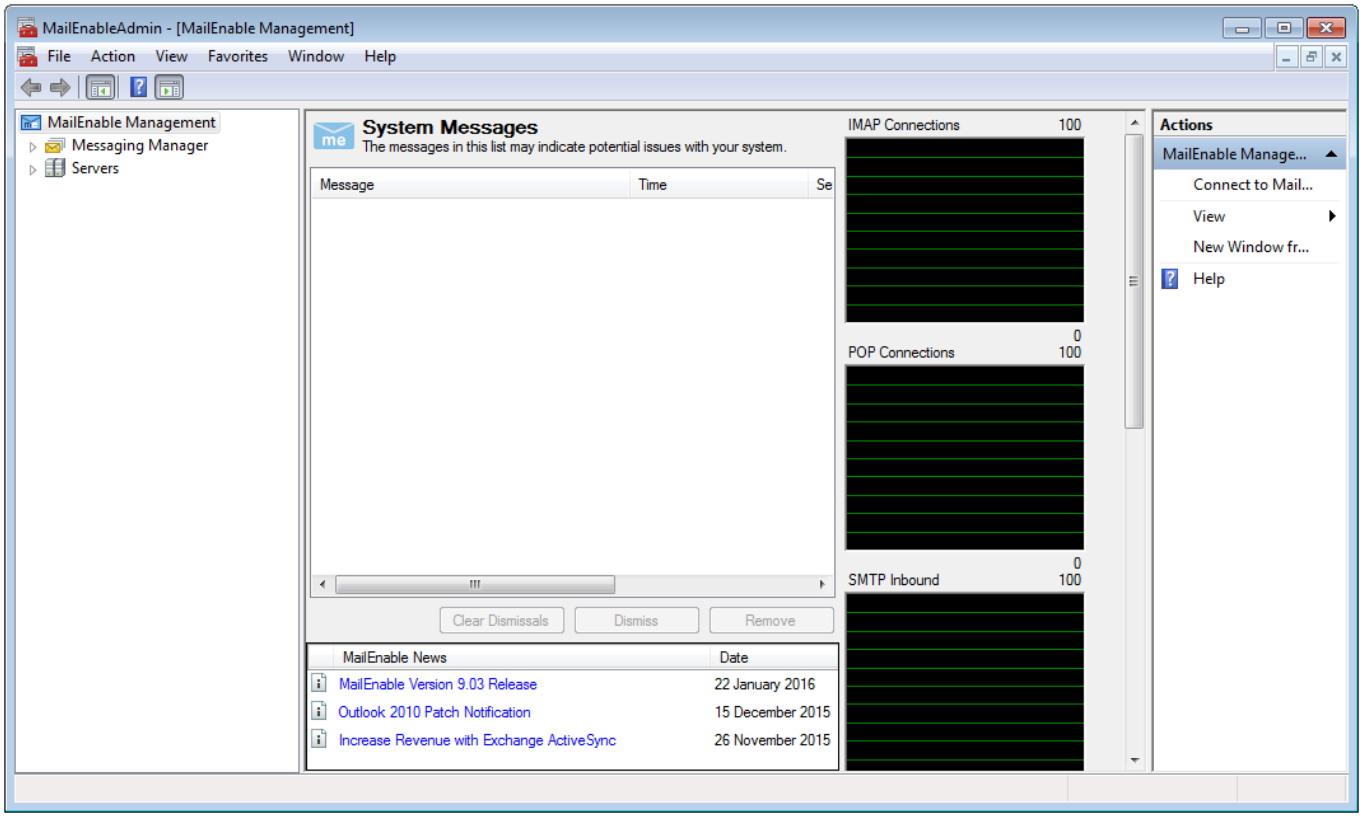
5.1 Administration

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

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

Start>Programs>MailEnable>MailEnable Administrator

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



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

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

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

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

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

5.2 Messaging Manager

5.2.1 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

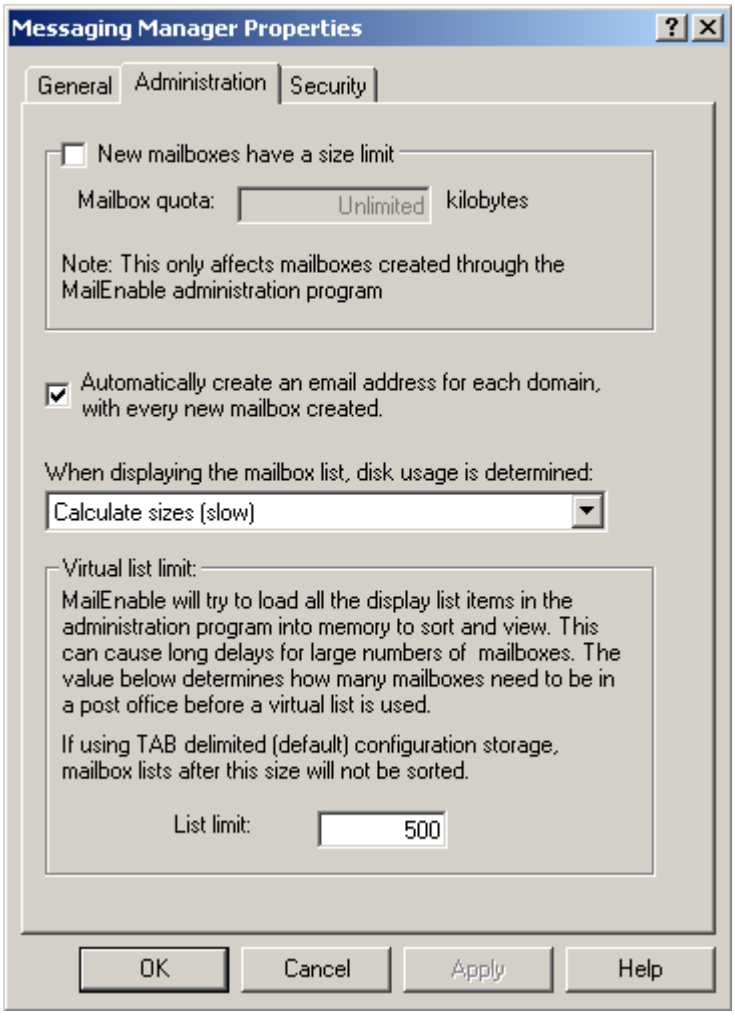
Properties item from the popup menu, or click the Properties item in the right hand panel.

5.2.2 Messaging Manager - General

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

Setting	Explanation
Configuration Repository	The configuration repository path contains the configuration information for your server. This includes the: Bad Mail Quarantine and Queues directories.
Message Store Repository	The message store path contains all the email data for the MailEnable server.

5.2.3 Messaging Manager - Administration

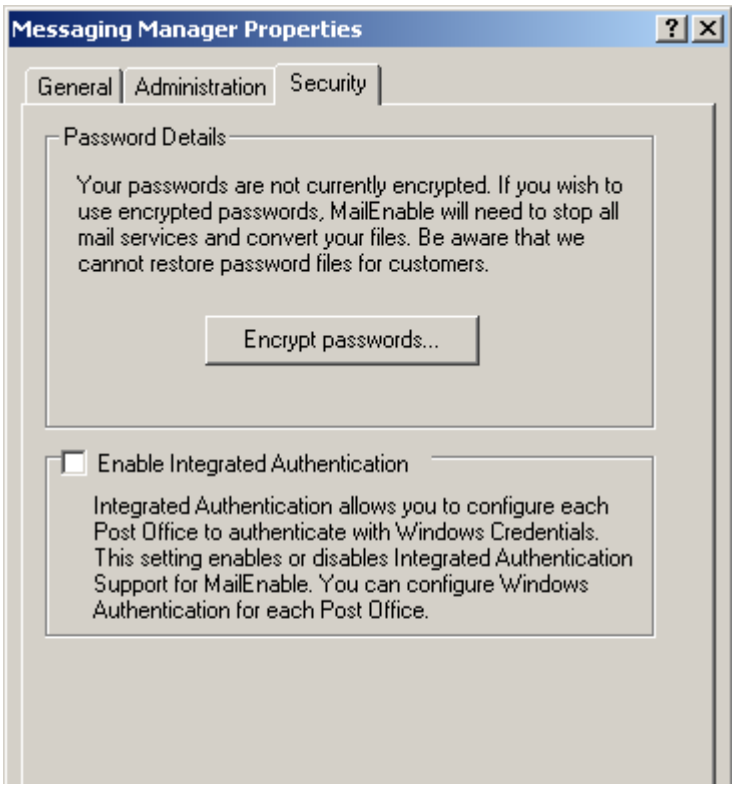


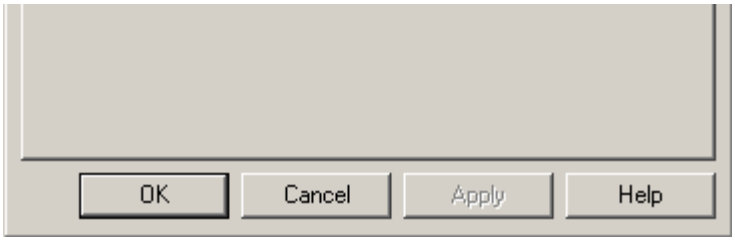
Settings	Explanation
New mailboxes have size limit	Configures the default quota for mailboxes, so every new mailbox created will have a quota configured. This only affects mailboxes that are created through the administration program. It does not set the default quota for new mailboxes created with 3rd party applications or ones that use the MailEnable API.
Automatically create an email address for each	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

domain, with every new mailbox created.	created for each domain for the mailbox. This only affects mailboxes that are created through the administration program.
Populate Asynchronously	When this option is selected the list views in the administration program will update in a background process. This may make the display slower to complete, but you may be able to access the contents earlier.
When displaying the mailbox list, disk usage is determined:	Use this option to set the size calculation method for listing mailboxes. The available options are: **Calculate sizes (slow):** This option will set the calculation method to calculate the sizes of of the mailbox folders when accessing the mailbox list. This can have an impact on performance if the list of mailboxes is large and each mailbox contains large amounts of messages. **Use precalculated sizes (fast):** Will use the pre calculated size reported within the DIRSIZE.tmp file. This file contains the current disk usage of the folder it is in. If the file is over 20 minutes old, then it will be updatred. **Dont show sizes (fastest):** This option will disable the calculation method and not display any sizes within the mailbox list. The size column in the mailbox list will show NA.
Virtual list limit:	MailEnable will try to load all the display items in the administration program into memory to sort and view the lists. This can cause long delays for large numbers of mailboxes. This option determines how many mailboxes need to be in a postoffice before a virtual list is used. **Note:** If using Tab Delimited files (default) configuration storage, mailbox lists after this size will not be sorted.

5.2.4 Messaging Manager - Security

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





Setting	Explanation
Password Details/Encrypt Passwords	When using Tab Delimited Configuration Providers, which is the default storage within MailEnable, MailEnable passwords are stored in text files with a TAB extension under the \config directory of the MailEnable directory structure. You can optionally specify to encrypt MailEnable passwords. If you are using integrated authentication, Windows credentials will take preference to these passwords.
Enable Integrated Authentication	This is a system wide setting that allows you to simply enable or disable authentication for all hosted MailEnable post offices. MailEnable Integrated Authentication allows you to use Windows Authentication as well as MailEnable's inbuilt authentication. It also allows you to have mailboxes created within MailEnable as users successfully authenticate using Windows Credentials. To enable integrated authentication, you must select Messaging Manager Properties (right click on Messaging Manager) and check the box labeled "Enable Integrated Authentication".

5.3 Post office configuration

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.

5.3.1 Post office configuration

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.

5.3.2 How to create a Post Office

How to add a new postoffice:

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

To access the postoffice **properties** window right click on the newly created postoffice and select **Properties** in the right click menu

5.3.3 Post office - General

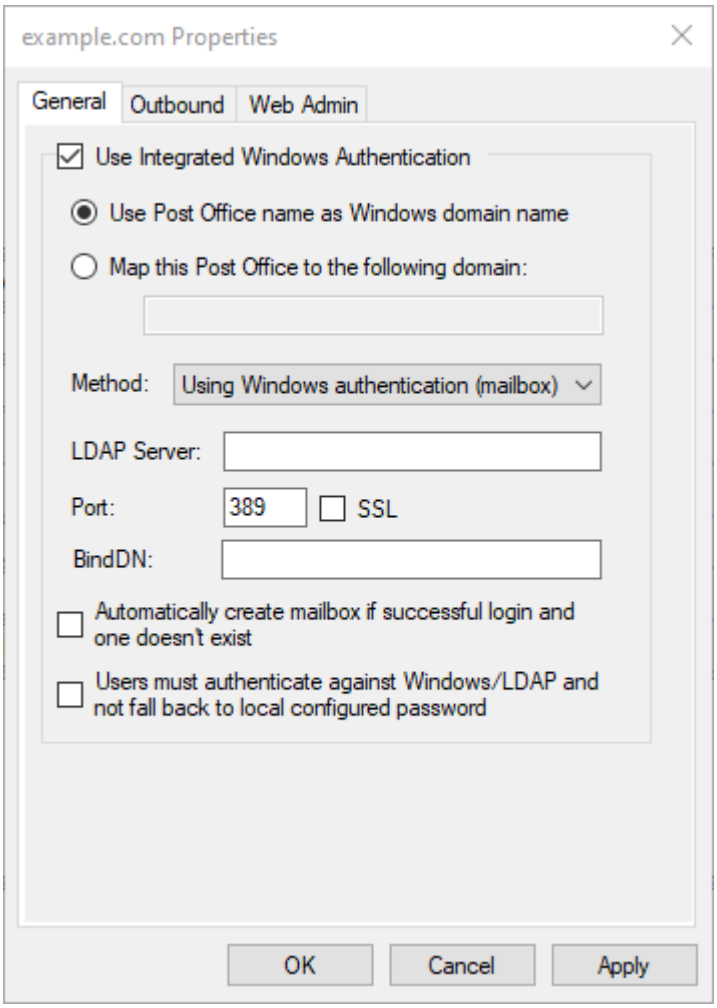
Once Integrated Windows Authentication has been enabled globally as per the **Security and authentication**

settings section ('Security and authentication settings' in the on-line documentation), each post office can then be configured with specific authentication settings.

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

In simple implementations there is likely to be only one domain, or the authentication will be done against the local machine. More complicated implementations will allow authentication against specific domains (i.e.: if the organization is made up of multiple domains). If you are authenticating against a domain, and the server is not within that domain, the server must have permissions to log in, and this is done by either adding the Windows server to the domain or configuring a trust relationship between the server and the Active Directory domain you are needing to authenticate against. Errors relating to Windows authentication for mailboxes can be found in the Windows event log.

When you configure the mail server to authenticate against Windows, it is not possible to change passwords through either the administration program, web administration or the web mail client. Password changes must be made through Windows directly.



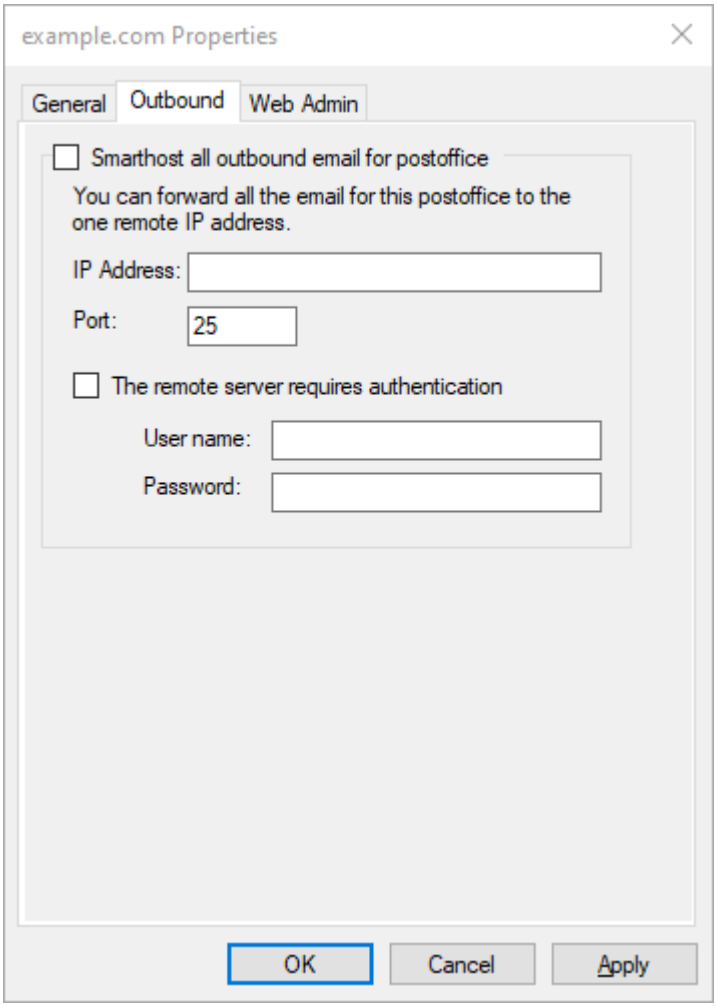
Setting	Explanation
Use Integrated Windows Authentication	Defines whether the post office can use Windows Authentication.
Use Post Office Name as Windows Domain Name	Select this option if the name of the post office matches the desired Windows Domain Name.

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 (.).
Method	**Using Windows authentication (mailbox)** This does a Windows authentication to log a user in, using the Windows domain (which is determined by the preceeding options). In order to successfully authenticate against Windows, the authentication has to be done to the Windows domain that the server is in, which can be the local server. If the mail server is not in the Windows domain, you would need to enable a trust relationship between the domains, or it may be easier to use the **Authenticate against LDAP/Active Directory** option. **Using Windows authentication (mailbox@domain)** This does a Windows authentication using User Principal Name (UPN) style logins, rather than legacy Windows NT style logins. **Authenticate against LDAP/Active Directory** This option allows you to authenticate against an LDAP/AD server.
LDAP Server	This is the IP address the LDAP server is running on. This option is only used when you have selected **Authenticate against LDAP/Active Directory** as the method.
Port / SSL	The port for the LDAP service, and whether to connect using SSL.
BindDN	This BindDN allows the substitution of %m for mailbox name and %p for the postoffice name. Some examples: CN=%m,CN=Users,DC=example,DC=com %m@%p
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.
Users must authenticate against Windows user and not fall back to MailEnable configured password	Enforces a user to only authenticate against the Windows user database and not fall back to the MailEnable authentication database.
Smarthost all outbound email for postoffice	This will route all emails for users of this postoffice to the one remote address. This would be used if you need to filter all the outbound email for just the postoffice. It does not affect email going to a local mailbox, just the outbound emails for the users of the postoffice.
IP Address	The destination IP address to route through.
Port	The port of the destination service. By default this is port 25.
The remote server requires authentication	Enable this if you need to authenticate to remote server.

5.3.4 Postoffice - Outbound

The Outbound tab allows you to redirect all outbound email for this postoffice to one remote IP address. This

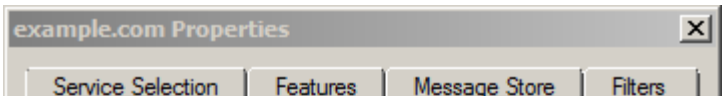
may be useful if you have a filtering service for domains under this postoffice.

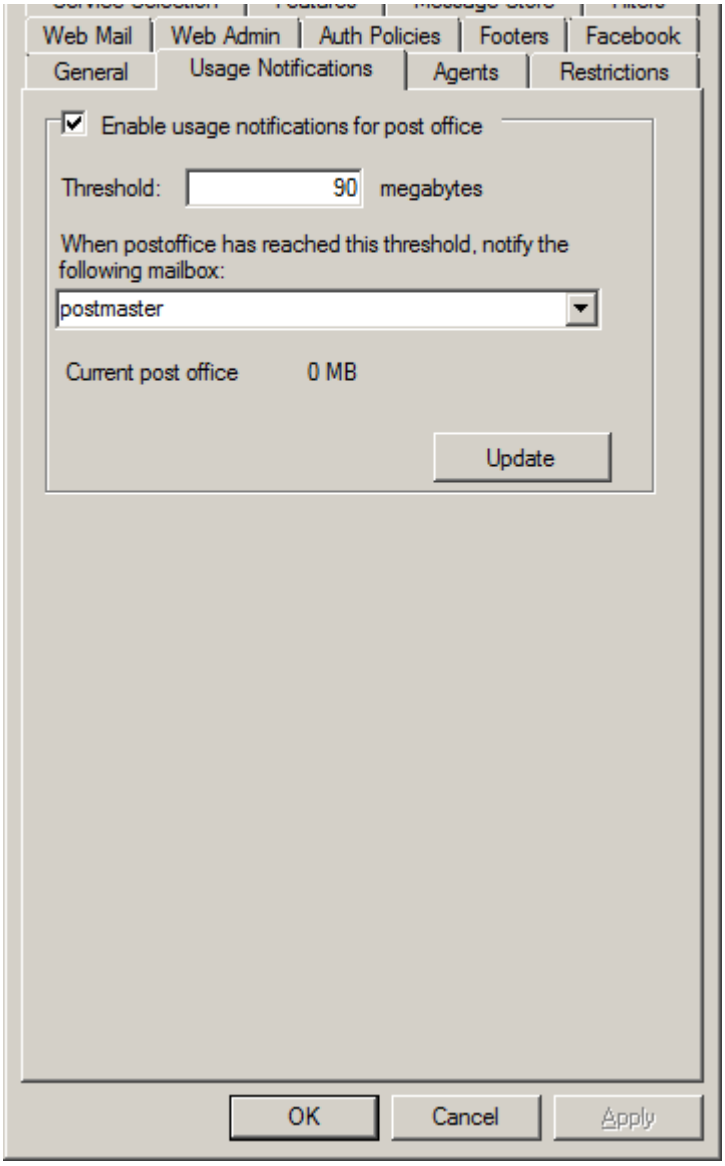


Setting	Explanation
Smarthost all outbound email for postoffice	This will route all emails for users of this postoffice to the one remote address. This would be used if you need to filter all the outbound email for just the postoffice. It does not affect email going to a local mailbox, just the outbound emails for the users of the postoffice.
IP Address	The destination IP address to route through.
Port	The port of the destination service. By default this is port 25.
The remote server requires authentication	Enable this if you need to authenticate to remote server.

5.3.5 Postoffice - Usage Notifications

The postoffice threshold value is the allocated hard drive space that has been allocated to an entire postoffice. When the limit is reached a notification message is sent.



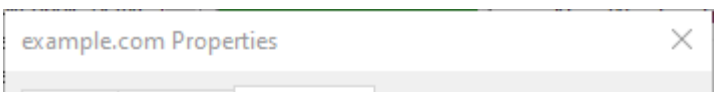


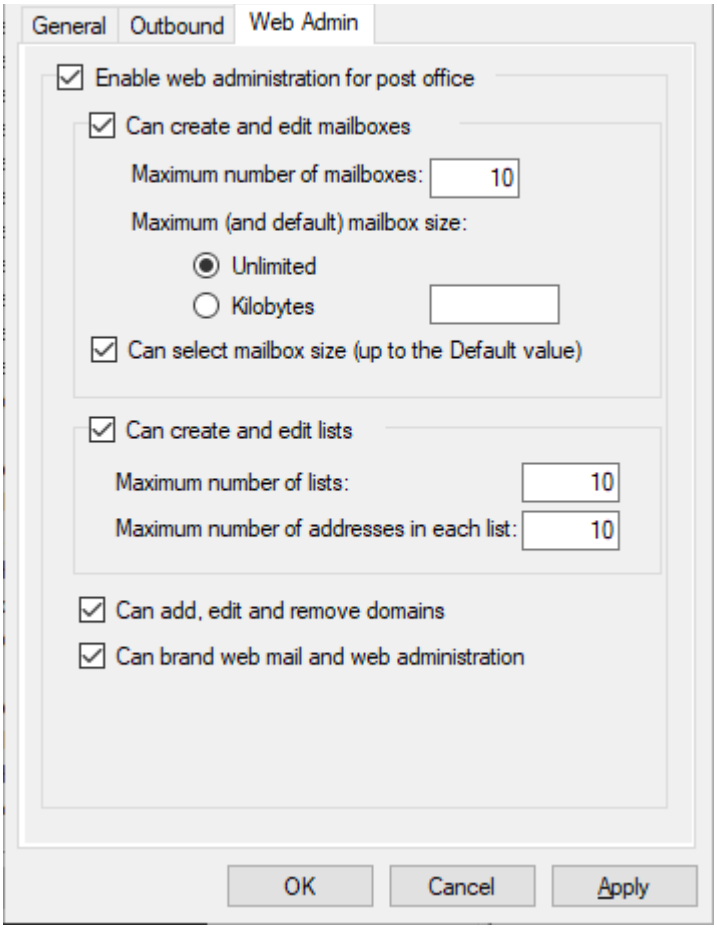
Setting	Description
Enable usage notifications for post office	Enables the quota option for the postoffice.
Threshold	The hard drive space allocated for this postoffice in megabytes.
When the post office has reached this threshold, notify the following mailbox	When the threshold is reached a notification message will be sent to this mailbox.
Update	This will update the display to show the current post office disk usage. This is not the actual usage, but a quick summary of all the mailboxes. So if a quota file is out of date this value may not be accurate.

Note: Clicking the update button on postoffices where mailbox content is very large may take a while.

5.3.6 Postoffice - Web Admin

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





Setting	Explanation
Enable web administration for post office	Enables web administration for the current post office.
Can create and edit mailboxes	Allows mailboxes to be created and edited in web administration.
Maximum no. of mailboxes	Specify the maximum number of mailboxes that can be created for this post office.
Maximum and default mailbox size	Enforces a mailbox size for each newly created mailbox in web administration. This setting can be disabled or changed for each mailbox in the mailbox properties – see the **Create mailbox - General section (Section 5.5.3)**.
Can select mailbox size (up to the default value)	Grants the web administrator the ability to create a quota for the post office mailboxes up to the configured default size.
Can create and edit lists	Grants the web administrator the ability to create lists in web administration.
Maximum number of lists	Sets the maximum number of lists a web administrator can create.
Maximum number of addresses in each list.	Limits the number of addresses a web administrator can add to a created list.

Can add, edit and remove domains	Allows the admin the ability to add and remove domains in the web administration page.
Can brand web mail and web administration	Allows the admin to brand webmail and web administration by changing the login logo and the banner logo.

5.3.7 Postoffice - Chat

By default, for the XMPP chat service, you are connected to everyone in your postoffice, but only if you have less than a couple of hundred mailboxes in the postoffice. Since if you have hundreds or more of mailboxes in a postoffice, the overhead to regularly check the status of each mailbox can add unneccessary load on the server. And it may not be convenient to list all mailboxes for users, when they may only chat to a few. This option allows you to force the buddy list to be everyone, or only the mailboxes the user has added.

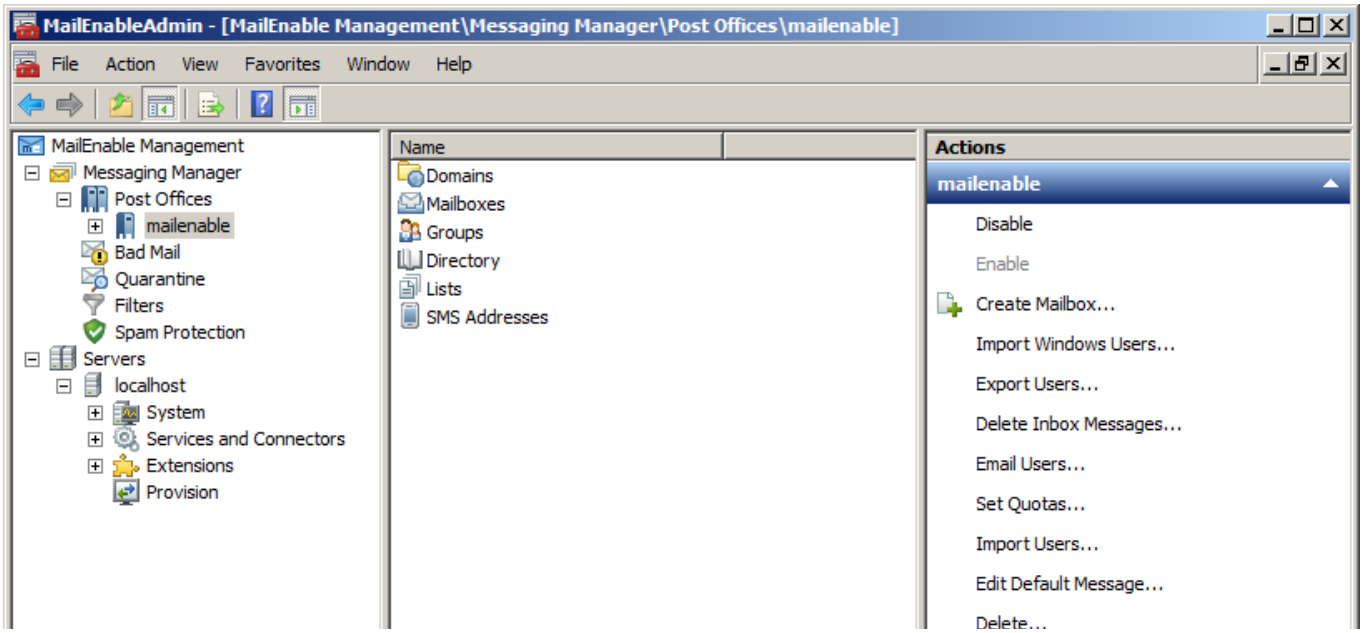
Setting	Explanation
Roster Source	**Auto Detect** If the postoffice has under 200 mailboxes, they will all be shown in the webmail chat. Default. **Postoffice Roster** All the mailboxes in the postoffice will be shown in the webmail chat. **Private Roster** The mailbox user will only see the mailboxes they add themselves in the webmail client.

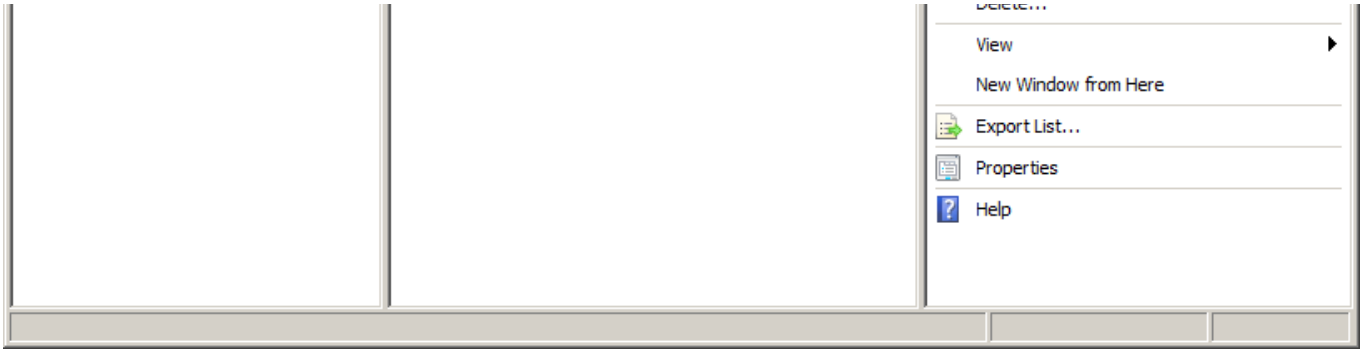
5.3.8 Post office actions

5.3.8.1 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 (as seen in the diagram below).

Note: The same actions can be found by right clicking on the postoffice.





5.3.8.2 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 **Export Users**.
3. From the list, select the fields to export to the file.
4. Select the format of the exported file, whether comma delimited or tab delimited.
5. Enter the filename to save as and select **Export**.

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

5.3.8.4 Import users

This feature allows you to import users to a postoffice. A comma delimited file that is formatted as **emailaddress,password,quota,friendly name** must be used. Password, quota and friendly name is optional. If not provided then default settings are used and domains will be created if necessary.

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

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

5.3.8.5 Email users (all)

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

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

5.3.8.6 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**.

5.3.8.7 Delete Inbox 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.

5.3.8.8 Set Quotas

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

5.3.8.9 Edit default message

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

5.4 Domain configuration

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. 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.

5.4.1 How to create a domain

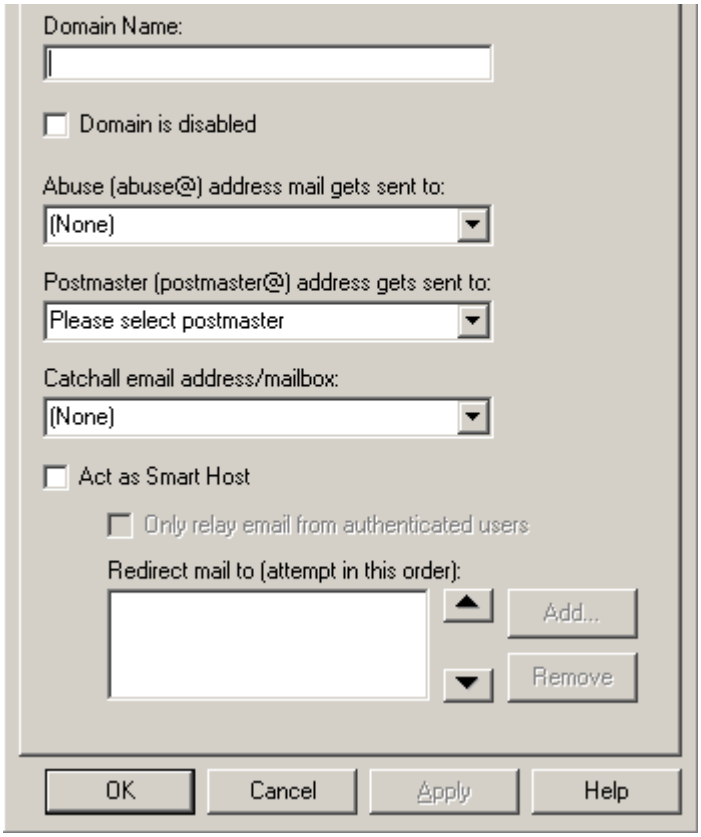
Multiple domains can be assigned to a post office. However, at least one domain needs to be configured in order to have a valid email address.

How to add a domain:

1. Navigate within the administration console to: **Messaging Manager > Post Offices > (Postofficename) > Domains.**
2. Select New Domain from the action pane.
3. Enter the full domain name when prompted.
4. Select OK, which will refresh the domain list for the postoffice.
5. If more configuration of the domain is needed, double click the newly added domain.

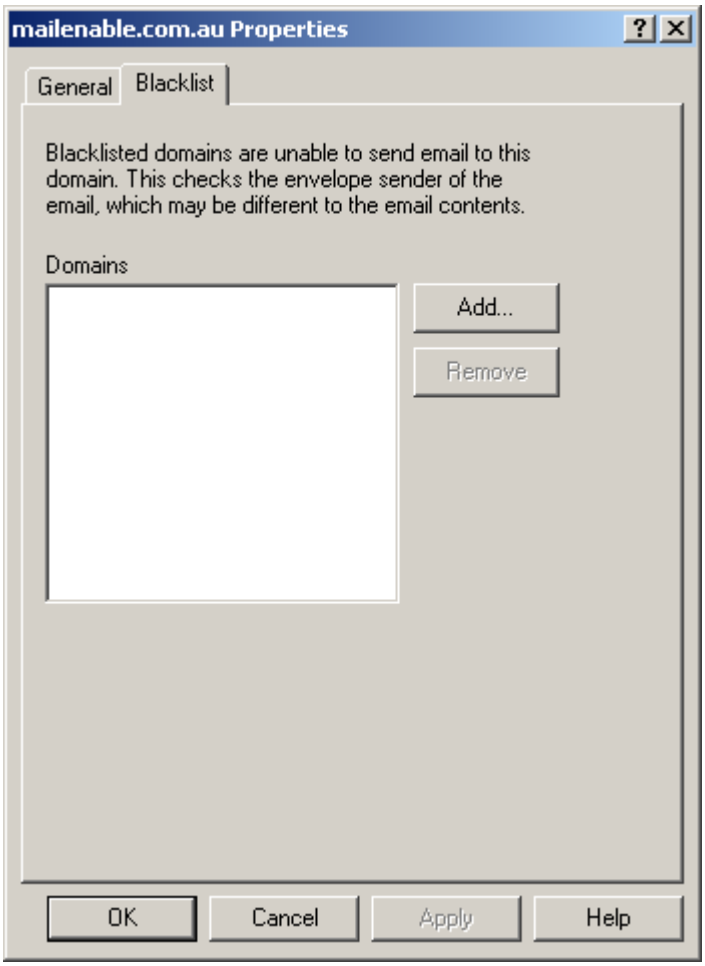
Example: To receive emails such as sales@mailenable.com or info@mailenable.com, enter the domain name as **mailenable.com** within the domain name **field.**

5.4.2 Domain - General



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 the **Smart host section (Section 6.6.9)** 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).

5.4.3 Domain - Blacklists



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

5.4.4 Domain - DKIM (DomainKeys)

DKIM Overview

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

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

How to enable DKIM for the server

1. Navigate to the following location within the administration console: **Servers > Localhost > Extensions**
2. Right click on **Domain Keys (DKIM)** and select properties.
3. Tick the option for **Enable DomainKeys Identified Mail (DKIM) functionality on this server**

How to configure DKIM for a domain

1. Navigate to within the administration console to: **MailEnable management > Messaging Manager > Post Offices > (postofficename) > Domains**
2. Right-click on the domain you wish to configure **DKIM** for and select **Properties**.
3. Select the **DKIM** tab and click the **Configure** button.

1. Check the **Sign outgoing messages** box to enable message signing.
2. Set the options for message signing. The following options are present:
    - *Encryption algorithm*: choose which algorithm will be used for signing the headers hash.
    - *Canonicalization algorithm*: this can be set independently for the headers and the body. The simple algorithm is stricter and will cause verification to fail if the message is changed at all in transit, whereas the relaxed algorithm will tolerate some whitespace insertion.
    - *Impose body hash length limit*: this allows you to limit how much of the message body will be used in the body hash.

      Note: setting a limit means that verification may succeed even if extra data is appended to the message somewhere in transit.

    - *Include user identity*: if checked, includes the sending user's identity in the signature header.
3. Configure selectors. A selector represents a private/public key pairing and, from the verifier's point of view, an entry in a DNS text record.
    a. Clicking New will bring up the *New Selector* dialog: enter a unique name for the selector and choose a key size (the larger the key, the more secure the encryption, but the longer it will take to

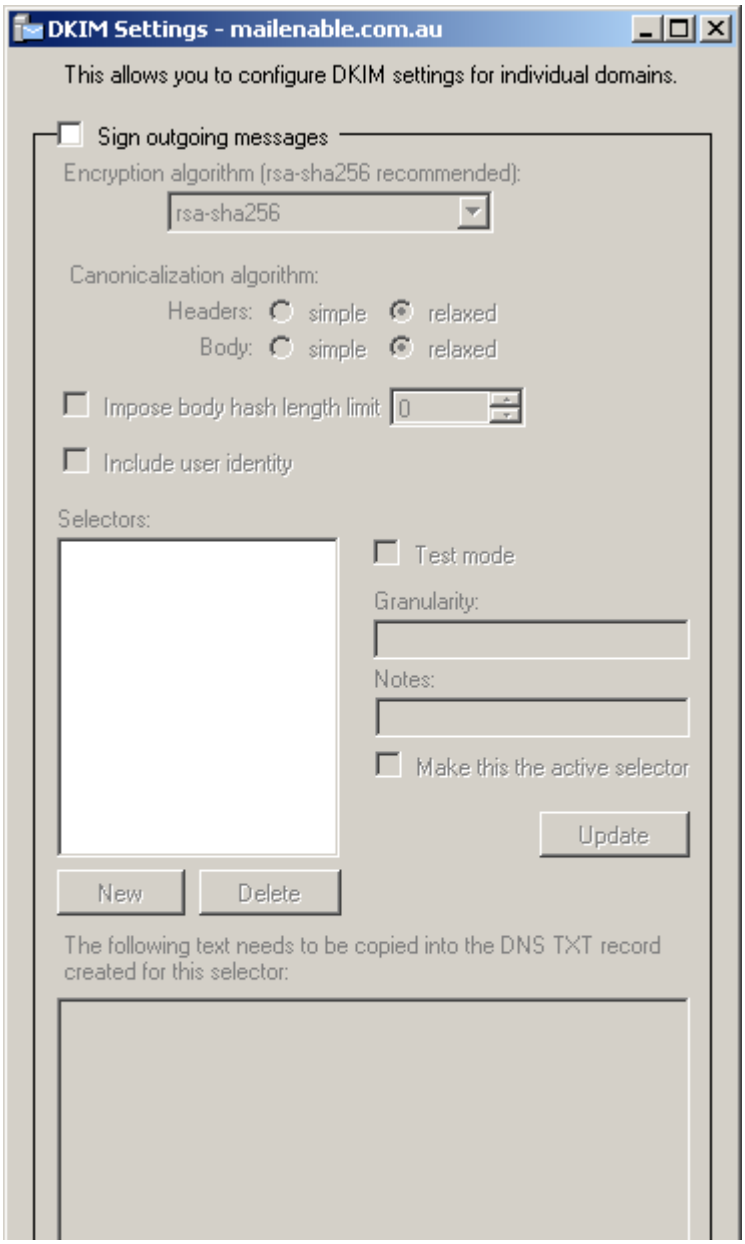
sign and verify each message).

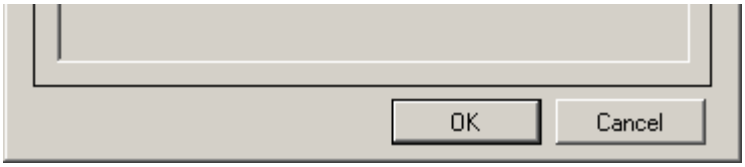
b. Options for each selector can be set by selecting the selector from the Selectors list, setting the options on the right, and then clicking Update. The following options are present:
   - *Test mode*: if this is checked, it indicates to verifiers that the server is testing DKIM, and that signed messages should not be treated any differently to unsigned messages, even if their verification fails.
   - *Granularity*: tells verifiers that only messages sent by a specified user should pass verification. This works by comparing the granularity with the user identity.
   - *Notes*: notes for human perusal.
   - *Make this the active selector*: use this selector for all outgoing messages. Only one selector can be active at a time, activating one will deactivate all others (however, even deactivated selectors are available for verifying against previously sent messages, so long as their entry remains in the appropriate DNS text record).

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

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

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





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

Note: instructions on setting up and maintaining DNS records are outside the scope of this document. Please contact your DNS administrator for more information.

Testing the DKIM Configuration

To test DKIM right away, try the following configuration:

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

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

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

Click Update.

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

5.5 Mailbox configuration

5.5.1 Mailbox Overview

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.

5.5.2 How to create a mailbox

When creating a mailbox, MailEnable will automatically create an email address for each domain in the post office (if the setting for automatically creating email addresses for each domain is enabled in the Messaging Manager Properties – see the **General settings section (Section 5.2.2)**) 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.

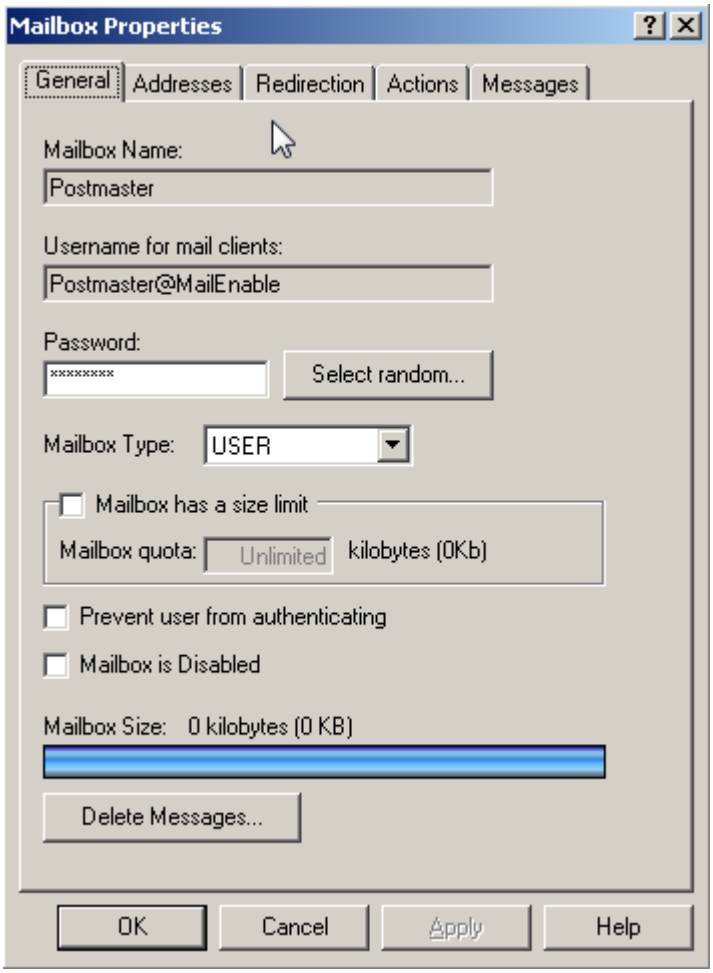
How to create a mailbox

1. Navigate within the administration console to: **Messaging Manager > Post Offices > (postofficename) > Mailboxes.**
2. Right click on mailboxes and select **New Mailbox...**
3. Specify a mailbox name.

4. Specify a mailbox password or alternatively click on **Select Random** button to set a random password.
5. Click **OK.**

5.5.3 Mailbox - General

The General tab of mailbox properties displays as below:



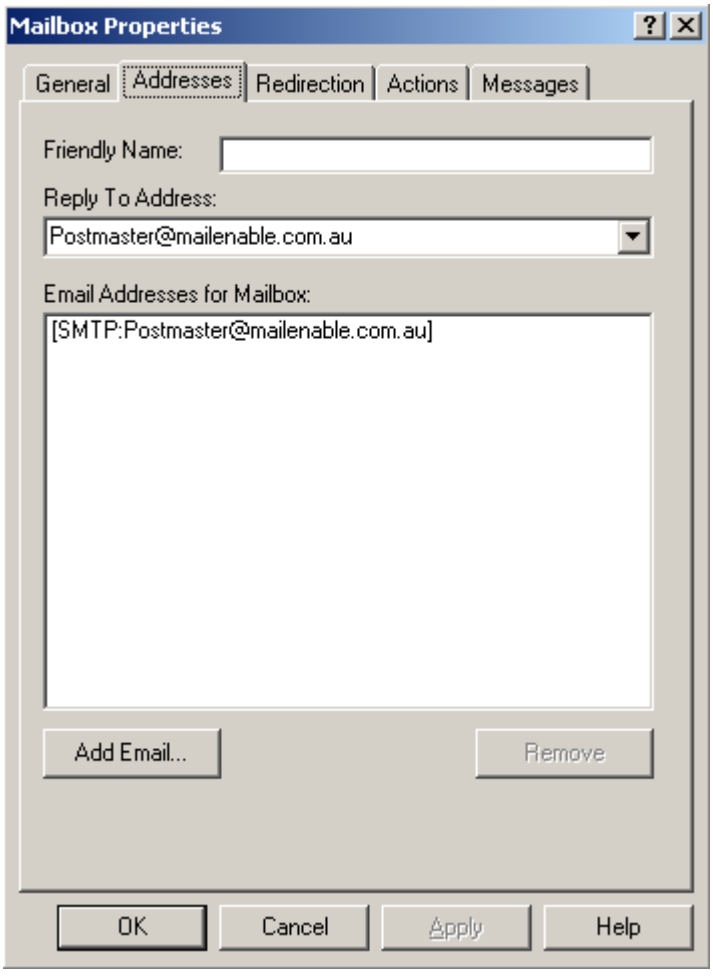
Setting	Description
Mailbox Name	This is the name of the mailbox. Once created, this cannot be changed. This both identifies the user and ensures there is no duplication of mailbox names. As the Mailbox Name is entered into the text box, the username entry just below it will change to reflect the entry.
Username for mail clients	This is the username used to be used for email clients. 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.
Select random password	Creates a random password. If password policies are enabled (which is done under the Servers->localhost setting), then it will generate a password to match.
User must change password at next login	You can force a user to change their password when they next log in by selecting this option. Forcing a user to change password is only performed by webmail. It does not affect users accessing their mailbox via other means.
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 given full control to web administration, and can alter any mail server setting.
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.
Mailbox is Disabled	When a mailbox is disabled, it cannot be accessed via a service, such as POP3 or web mail. Useful for suspending account, it makes the mailbox or email mappings to the mailbox inactive, without deleting it.
Delete Inbox Messages	Delete messages from the Inbox for the mailbox. Messages can be deleted if they are over a certain age, or all messages can be deleted.

5.5.4 Mailbox - Addresses

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

To create new email addresses, selecting the **Addresses** tab at the top of the mailbox properties window. A list of the current email addresses will be shown.



In order to add another email address for this mailbox, click the **Add Email** button. The first text box, **Enter email name** is where the first part of the email address is entered. E.g. to add **sales@mailenable.com**, only

requires the word sales to be entered. The full address of the email being added is displayed in the window.

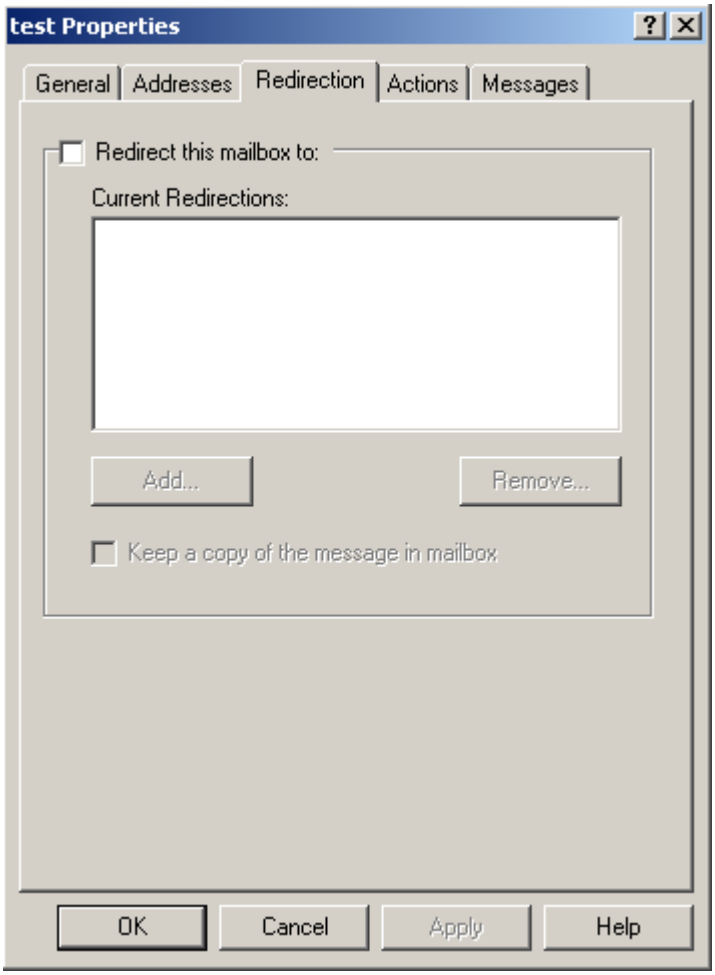
The **Available Domains** list box in this window lists domains that are entered via the **Create Domain** icon. MailEnable can only add email addresses for the available domains in each **post office** account. For the purpose of this guide we have entered only one domain. In cases where there is more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

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

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.

5.5.5 Mailbox - Redirection

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

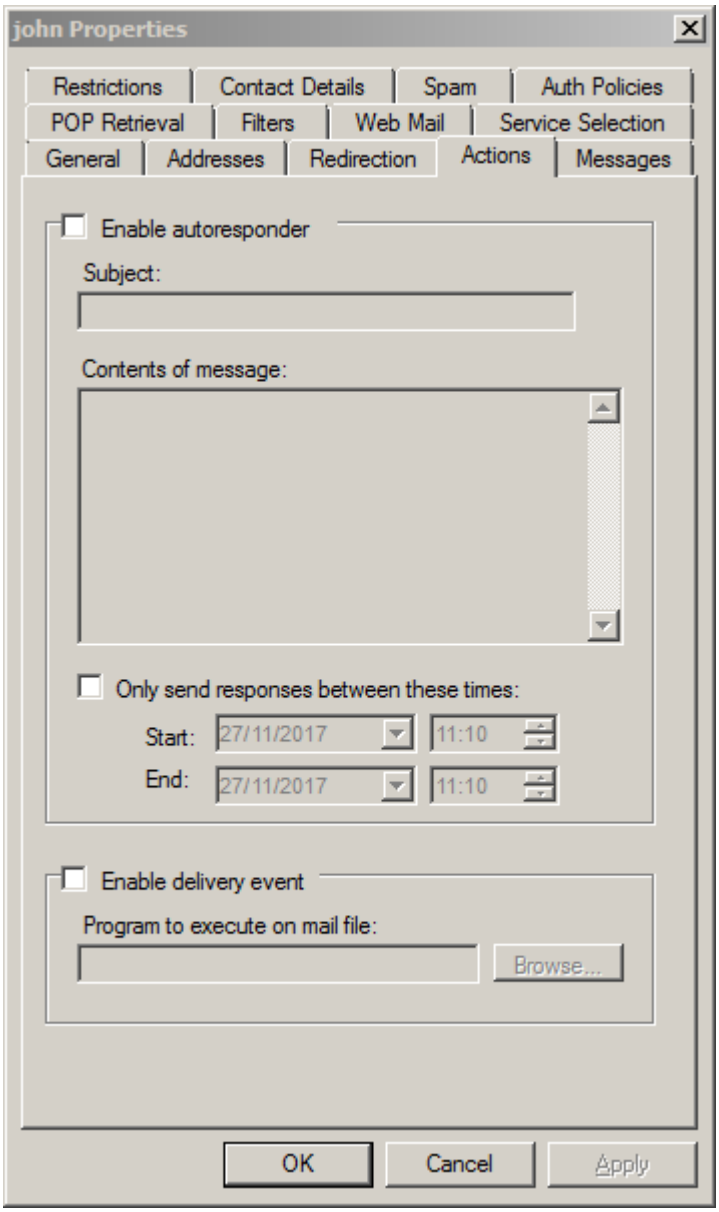


Setting	Description

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 the **Create a group section (Section 5.6.2)**) - 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.

5.5.6 Mailbox - Actions

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

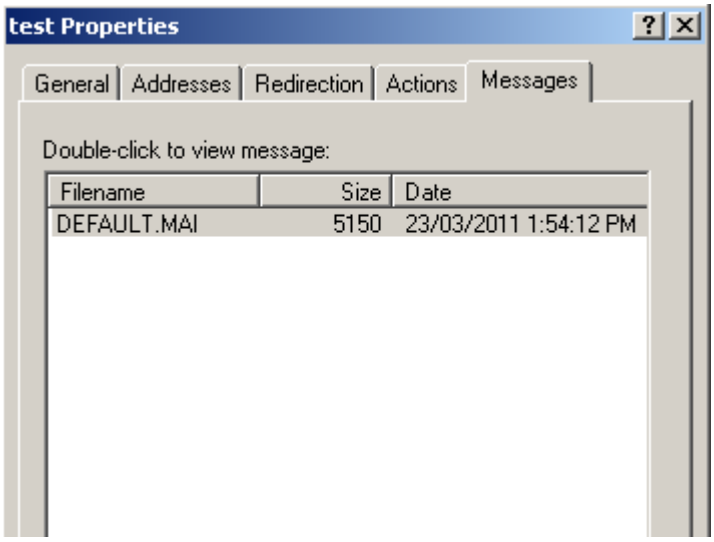


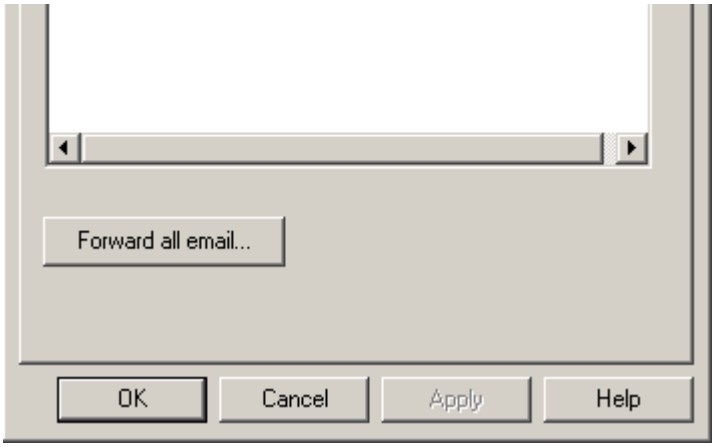
Setting	Description

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 or system generated. It is not possible to enable auto responders for the postmaster mailbox.
Only send responses between these times	You are able to limit the autoresponder to only reply to emails between specific date/times.
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: For a 64bit Windows server: HKLM\SOFTWARE\Wow6432Node\Mail Enable\Mail Enable\Connectors\Connector Root Directory For a 32bit Windows server: HKLM\SOFTWARE\Mail Enable\Mail Enable\Connectors\Connector Root Directory To get the full path to the postoffice connector queue, which is holding the message for the delivery event, append the text "\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. By default the delivery event will not execute for any messages marked as bulk. Bulk messages are mostly system generated messages such as delivery failures, delivery reports, and autoresponder replies. Messages from list servers may also not execute the delivery event. If you need to execute the delivery event on every message you can enable the Postoffice Connector option **Execute delivery event on bulk/system messages** which is found under the Postoffice Connector settings.

5.5.7 Mailbox - 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 inbox...	Forward all email from the Inbox of 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.

5.6 Group configuration

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.

5.6.1 How to create a group

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.

How to create a group

1. Navigate within the administration console to: **Messaging manager > Postoffices > (postofficename) > Groups**
2. Right click on groups and select **New > Group...**
3. Specify a group name
4. Click on **Add Email...** and enter an email name then click **OK**
5. Click **Apply** and then **OK**

5.6.1.1 How to add a group member

How to add a group member

1. Navigate within the administration console to: **Messaging Manager > Postoffices > (postoffice name) > Groups > (Group name)**
2. Right click on the group name and select **New > Group Member...**
3. Specify an email address that is to be added as a group member. Alternatively click on the **Advanced** button and select a mailbox local to the postoffice that the group resides under.

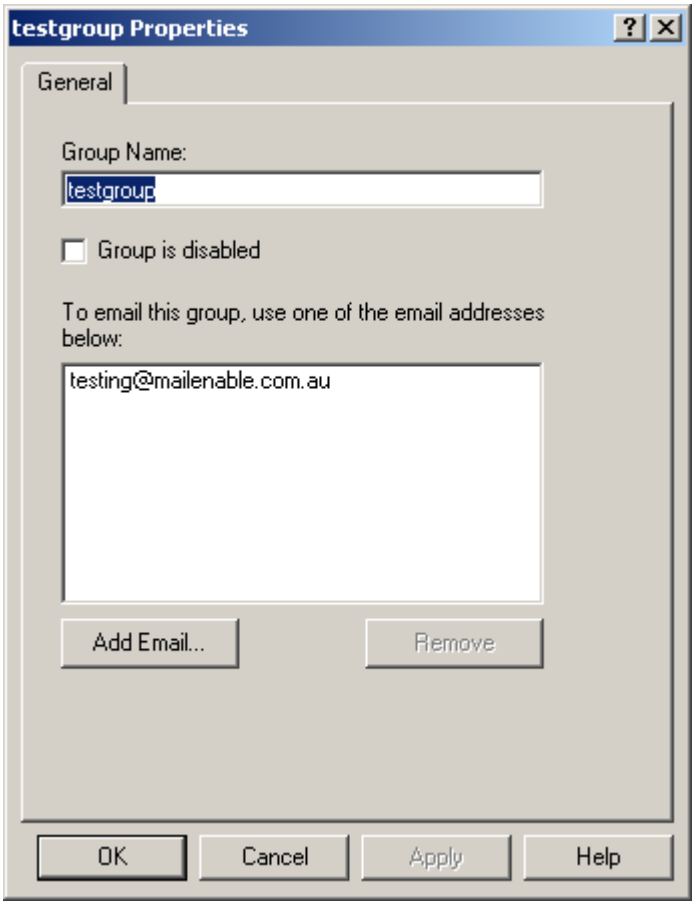
Note: Be cautious of using the Advanced option if you have a large number of users in the post office as it

may take a while to load the mailbox list.

5.6.1.2 How to import group members

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.

5.6.2 Group - General



Setting	Description
Group name	Create a name for the group e.g. staff@example.com
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

5.7 Lists configuration

5.7.1 Lists

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

5.7.2 How to create a list

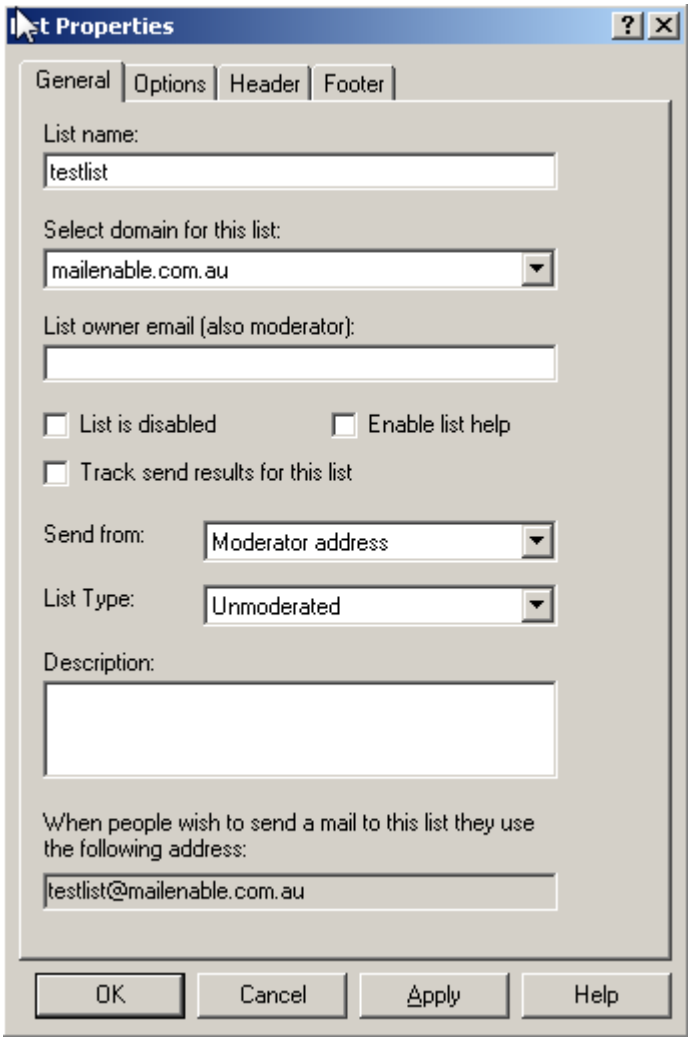
How to create a list

1. Navigate within the administration console to: **Messaging Manager > Postoffices > (postoffice name) > Lists**
2. Right click on Lists and select **New > List**
3. Specify a list name.
4. Set the domain to be used for the list address
5. Set the list owner address/moderator
6. Click **Apply** then **OK**

Note: The list moderator address cannot be the same as the System Notification address that is set within the SMTP properties.

5.7.3 Lists - General

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

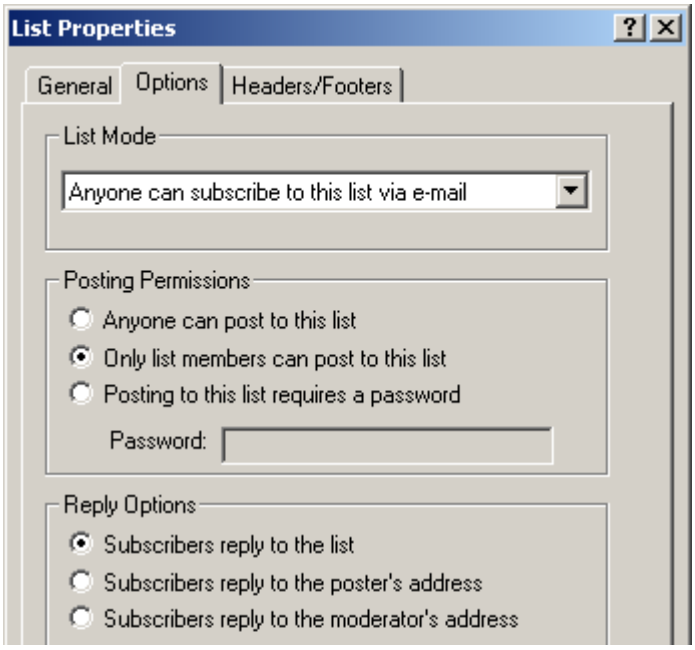


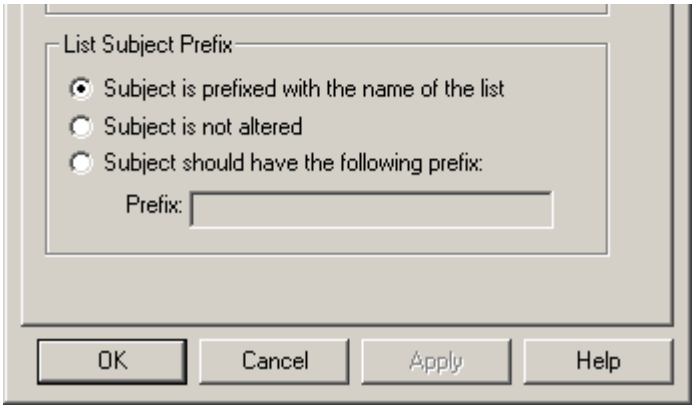
Setting	Description

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. A postmaster@domain email address cannot be used here.
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.
List Type	Determines whether the list is moderated or not. If moderated, all incoming emails will be sent to the moderator email address. Only emails posted to the list from the moderator will be sent to the members. If a password protected moderated list is configured, then users do not need to use the password, but the moderator does. All emails will go to the moderator, and the moderator needs to use the password in order to post to the list. If a list member sends with a password it will still be sent to the moderator. Normally, any bounces or similar system generated emails that are sent to the list are redirected to the Bad Mail folder. If the list is moderated though, then these emails will be directed to the moderator instead.
Description	A description of the list. This is displayed in the Administration program to allow you to easily see what a list is about.

5.7.4 Lists - 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.





Subscription type

MailEnable can control how subscriptions are handled.

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

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. This is not available when using a datasource for the list members.
Posting to this list requires a password	Password protects the list. To send an email to a password protected list, members need to enclose the password in square brackets and colons. So it would have something like **[:password:]** in the subject line. The password is removed from the subject when the email is published to the list. The list service does not decode MIME encoded-word subjects, which may occur from some clients if non-ASCII characters are used in the subject. If you find emails with the correct password are being denied, try using only ASCII characters in the subject.

Reply options

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

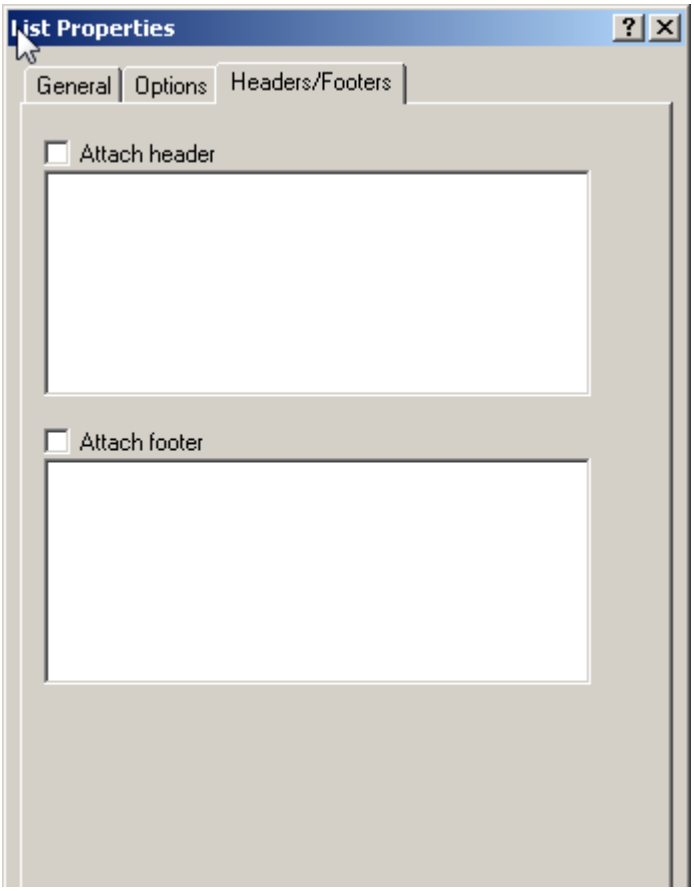
Setting	Description
Subscribers reply to the list	The reply to address is set to the list address, so when users reply to a message that gets sent from the list, their email gets sent to the list.
Subscribers reply to the posters address	The reply to address is set to the email address of the sender, 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.

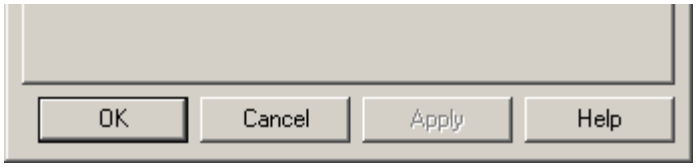
List subject prefix

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.

5.7.5 Lists - Headers and Footers





List Headers

Specify plain text or HTML 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.

List Footers

Specify plain text or HTML 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.

5.7.6 Importing list members

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

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

5.7.7 List commands

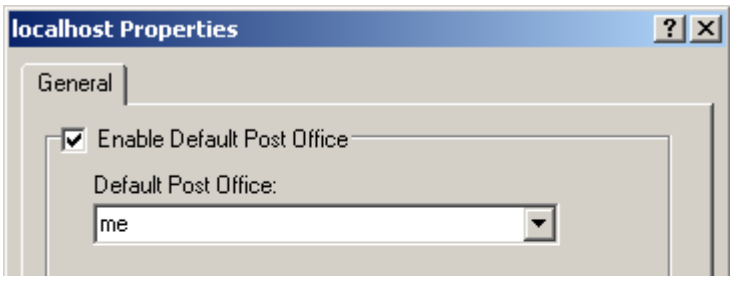
Users send commands to the list by putting the command in the subject line. The available commands for the list server are:

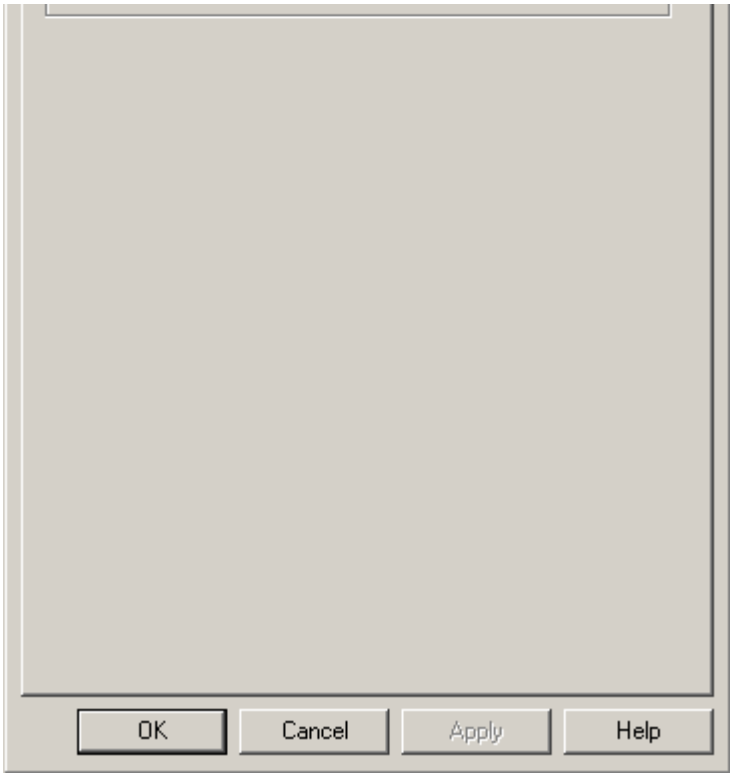
- **Help** – sends an email back with the available commands of the list server
- **Subscribe** – adds the user to the list (if the list permissions allow them)
- **Unsubscribe** – removes the user from the list

5.8 Localhost - General

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

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





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.
Enable Provisioning	When provisioning is enabled when a postoffice is created you will be able to have the administration program create any of these items: • A webmail site in the format webmail.domain (if Microsoft DNS is configured locally, the DNS entry will also be made) • A web administration site in the format webadmin.domain (if Microsoft DNS is configured locally, the DNS entry will also be made) • Exchange ActiveSync configured for the domain • Website for the domain (an IIS site will be created and the www.domain will be added if Microsoft DNS configured locally)

5.8.1 Localhost - Secure Sockets Layer (SSL) encryption

MailEnable has the ability to use SSL (Secure Sockets Layer) when transmitting data between mail clients and servers. SSL is available for IMAP, SMTP, POP, and HTTP related protocols.

Secure Sockets Layer (SSL) creates a secure connection between a client and a server over which any amount of data can be sent securely. It is a protocol for transmitting private documents via the Internet and is used with both web and email applications. URLs that require an SSL connection start with *https*: instead of *http:*.

Enabling SSL on the email client (e.g., Microsoft Outlook, eM Client, Thunderbird) provides an added level of privacy and security for the data being sent over the network.

Obtaining an SSL Certificate

For the MailEnable mail services, one SSL certificate can be configured on the server as the default certificate for connections. This default certificate is used for all connections if SNI is disabled, or for when the client requested certificate cannot be found. When using SNI, the services are able to determine what certificate the client is

requesting, and will attempt to load that certificate from the Windows certificate store.

To use SSL for web mail and web administration, then these would be configured under the IIS administration applet, since IIS in this case is responsible for the SSL handling.

Registering an SSL Certificate on the mail server

Under the Windows platform, certificates can be registered into shared certificate containers which can be accessed via IIS and other SSL enabled applications. If an SSL certificate is already registered under IIS or for a web site running on the server then the certificate should be available to be used by MailEnable.

Microsoft provides a Microsoft Management Console (MMC) application that can be used to manage certificates on the server. Access the certificate manager MMC application as follows:

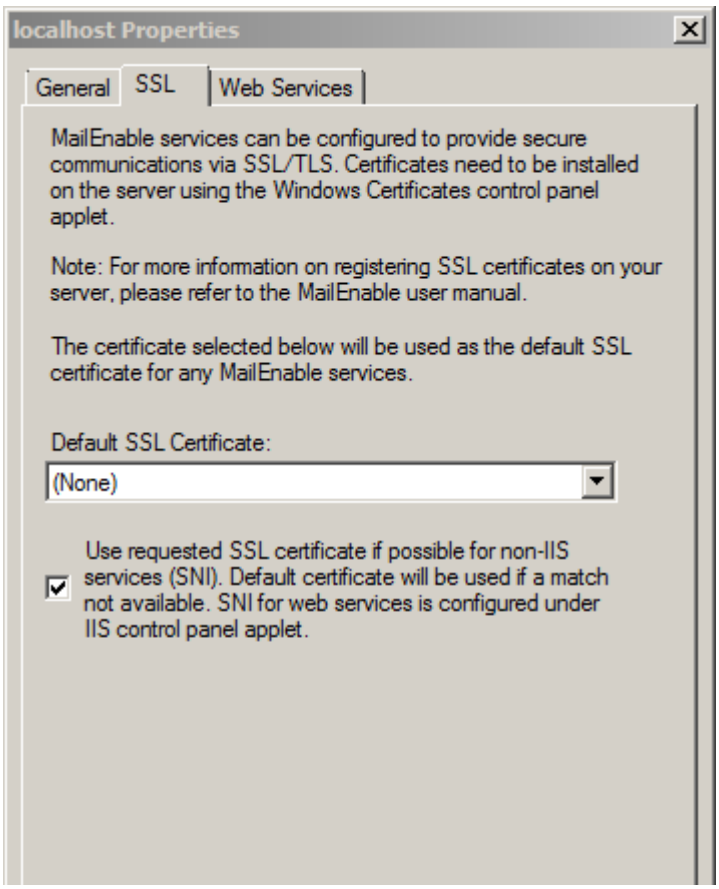
1. From the Windows Start Menu, select Run|mmc.exe
2. From within the MMC application select File | Add/Remove Snap-In | Standalone | Add
3. Select "Certificates" from the list and select the Add button.
4. Select "Computer Account" account, select finish

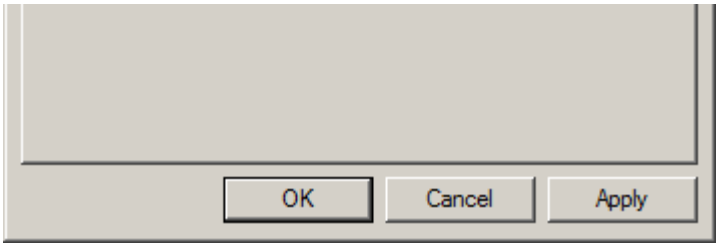
This application can be used to review and import SSL certificates into the various SSL certificate containers on the server. MailEnable uses certificates that have been configured in the “Personal Certificates” store of the Computer Account. It is not able to use the certificates under the the Web Hosting container, so if you have installed a certificate there that you need, you would need to copy it to the Personal Certificates container.

Detailed instructions for managing certificates on the Windows platform can also be found on the Microsoft web site.

Configuring MailEnable to use an SSL Certificate

Once an SSL Certificate has been configured in the server’s Personal Certificates store, select and enable that certificate for use under MailEnable. The SSL certificate that is chosen for use by MailEnable is the default used for SSL communications. The server determines certificates by the name only. If you have multiple certificates with the same name, for example, if you have renewed a certificate and added this to the server, then the software will load the first valid certificate. So it will still use the old certificate until it is not valid, before it uses the new one.





Once certificates have been registered on the server, you still need to configure which services make use of it. So under the services and connectors configuration you may wish to add an SSL port, or enable TLS support.

When SNI is selected, the mail services will try to choose the correct certificate to match the one the user is requesting. If this does not exist, then the default SSL certificate is used. Not all email clients support SNI, and these will use the default certificate.

5.9 Option Files

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

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

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

Note: The option file method for preconfigured options will not work if the configuration repository if configured to run on a database.

6 Services and Connectors

6.1 IMAP Service

6.1.1 IMAP Service

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

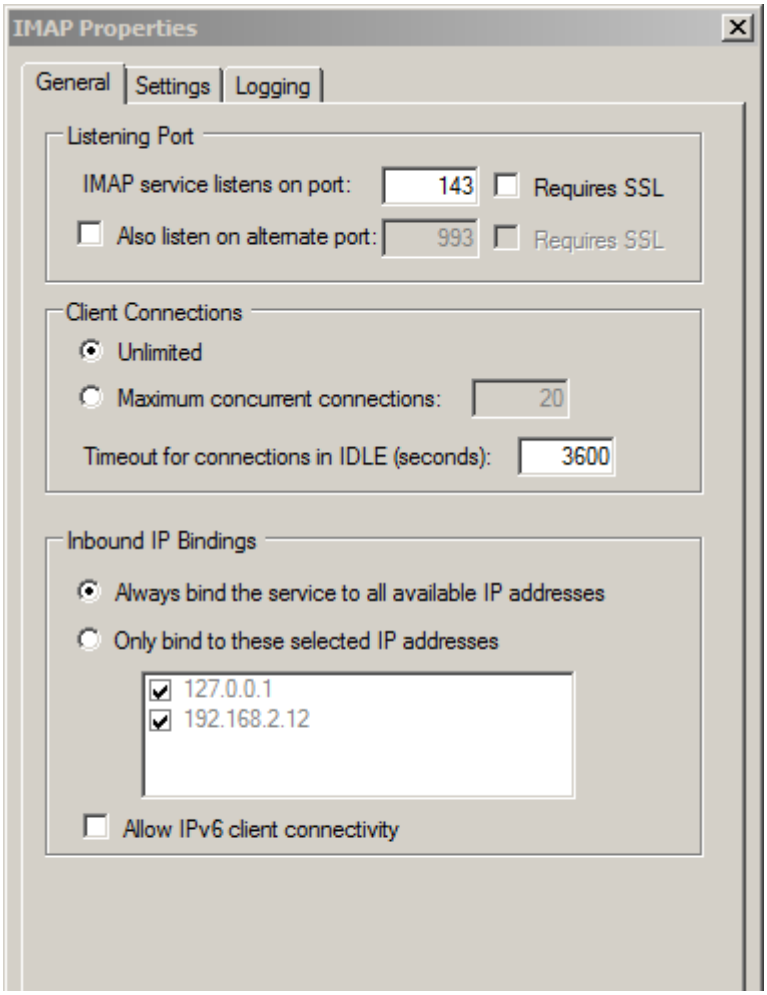
IMAP has distinct advantages over POP because it allows management of multiple folders on the server. Mail can be accessed from different machines, as the mail is hosted on the server (unlike POP which deletes mail from the server after being accessed) and allows the user to just download message headers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

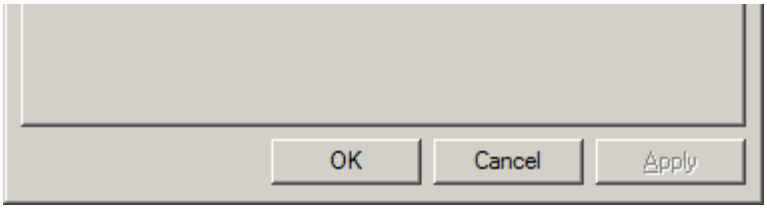
IMAP4 can break up and download specific parts of a multi-part email message (MIME). This means that instead of having to wait for an email with attachments to download, it is possible to select only the text portion to download, and leave the attachments on the server.

6.1.2 IMAP - General

The setup of IMAP is relatively simple, as it is a service that is bound to a listening port similar to HTTP. The IMAP service listens on this port and receives mail and various commands from the server. It is important to enable the default port of 143 on the firewall or any other port number stipulated in the **General** properties of the IMAP service. To help in server traffic and load, also stipulate which IP address to bind the service to.

Within the Administration Console navigate to the following location: **Servers > Localhost > Services and Connectors** branch, right click on the IMAP icon and select Properties from the popup menu. The **General** tab options are explained below:





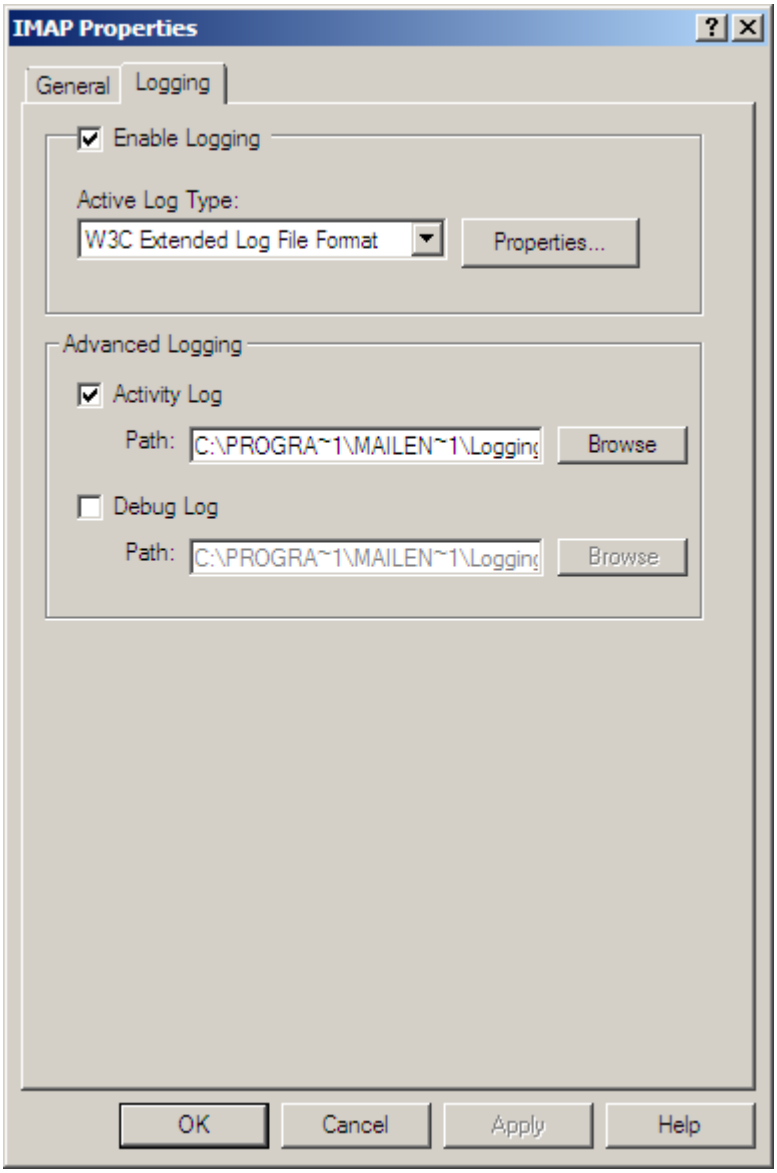
Setting	Description
IMAP service listens on port	Port for listening on. Default is 143.
Requires SSL (Default Port)	This will enable SSL encryption for the default port that IMAP is running on. Place a tick in this box to enable the service. This also has to be enabled at a server level in the MailEnable Administration program under **Servers >Localhost Properties > SSL** tab.
Also listen on alternate port	An alternate port can be selected.
Requires SSL(Alternate Port)	This will enable SSL encryption for the alternate port that IMAP is running on. The default port number is 993. A certificate needs to be selected at a server level under **Servers > Localhost Properties > SSL** tab.
Client Connections	Select either an unlimited number of client connections, or specify a maximum number of concurrent connections that the service will allow. Specifying a maximum number of connections may reduce server load by limiting the threads that IMAP can use. Be aware that IMAP clients can open multiple connections to the server for the same mailbox.
Timeout for idle connections	If this setting is enabled and a client connection has not passed any commands to the server for the set period of time, the connection will be dropped by the server.
Inbound IP Bindings	It is possible to select the IP addresses that the POP service will be bound to. On a multi-homed machine it may be desirable to only allow connections on particular IP addresses. 'Always bind all IPs' will allow connections on all IP addresses that are configured for the machine.
Allow IPv6 client connectivity	Supports accepting connections using IPv6.

6.1.3 IMAP - Settings

Setting	Description
Enable SSL/TLS support	Enables SSL and TLS support for the IMAP service.
Allow clients to login using PLAIN authentication	Enables PLAIN authentication for the IMAP service.
Force clients to login securely (over SSL)	Users are required to use SSL or TLS to authenticate.
Enforce mailbox quotas	When users copy messages up to the server via IMAP this will make sure that they do not exceed their quota and return an error message.
Enable NTLMv1 authentication	If enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be

	enabled use this secure authentication. For example, in Microsoft Outlook the feature is called SPA – Secure Password Authentication. NTLMv2 is not supported. You should not enable this unless you have a specific reason, due to it being an old authentication method that is insecure and is being phased out by Microsoft.
Enable CRAM-MD5 authentication	CRAM-MD5 Challenge-Response Authentication Mechanism is intended to provide an authentication extension to IMAP4 that neither transfers passwords in clear text nor requires significant security infrastructure in order to function. Only a hash value of the shared password is ever sent over the network, thus precluding plaintext transmission.
Enable XLIST/SPECIAL-USE support	This option allows the IMAP service to tell the email client what folders are the Junk, Deleted Items, etc. Since clients vary the name of these, especially with non-English client applications, this helps the client match it to what the server has configured. It is recommended not to enable this option if your users are generally English speaking, as Microsoft Outlook syncs slower by default when servers support this.

6.1.4 IMAP - Logging



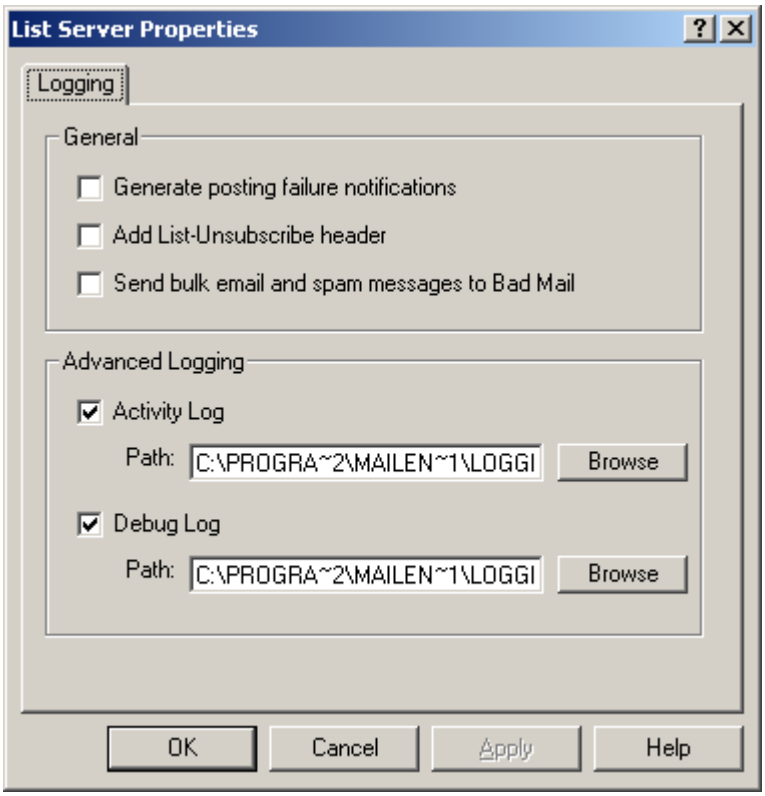
Setting	Description

Logging Options	MailEnable's IMAP Connector provides W3C, activity and debug logging. W3C logging is used to record service usage, Activity logging is used to record system activity and debug logging is used to provide low-level information on system activity.

6.2 List Server Connector

6.2.1 List Server Connector

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



Property	Explanation
Generate posting failure notifications	By ticking this box, if a message is sent to a list and is rejected due to sender being rejected or incorrect password, then a posting failure notification is sent. Disabling this feature can help reduce traffic where spammers have sent to the address and used a forged email address.
Add List-Unsubscribe Header	A header line that includes unsubscribe details is added to each email sent from the list server. Some email clients support this and will give an easy unsbuscribe option. For example Hotmail will display a link which a receiver just has to click in order to unsibscribe.
Send bulk email and spam messages to Bad Mail	Messages that arrive to a list and have been detected as spam will be sent to the Bad Mail folder.
Advanced Logging	This setting allows the logging of list activity and any problems that may arise. To improve speed and to not create logs disable the activity and debug logs.

6.3 Mail Transfer Agent (MTA)

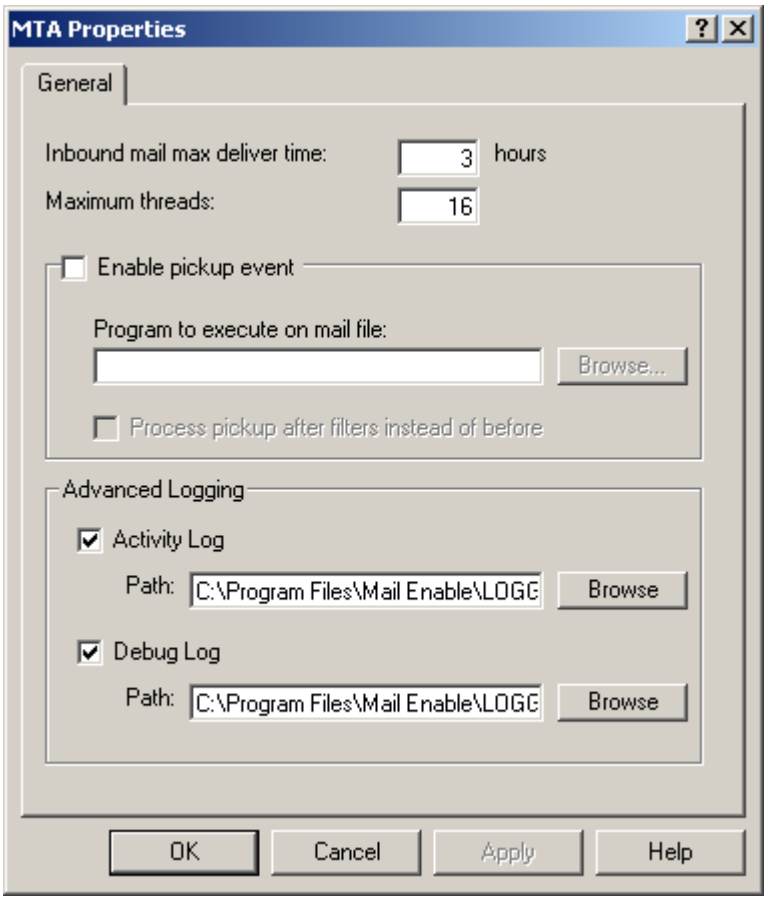
6.3.1 MTA Overview

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

Examples of MTA functionality follow:

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

6.3.2 MTA - General



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

Setting	Description
Inbound mail max. delivery time	If a message is let a inbound queue for too long without being marked as ready for delivery, then the MTA service will forcibly try to deliver the message after this time.
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	Executes a program or application when mail arrives. MailEnable will pass the mail message

pickup event	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.
Process pickup after filters instead of before	Normally the pickup event is processed before the global filters, which includes antivirus. This option allows the pickup event to execute after filters (which may delete or alter the emails).
Advanced Logging	Produces a debug and activity log for the service. Use this to obtain more details about what the service is doing.

6.4 POP Service

6.4.1 POP service

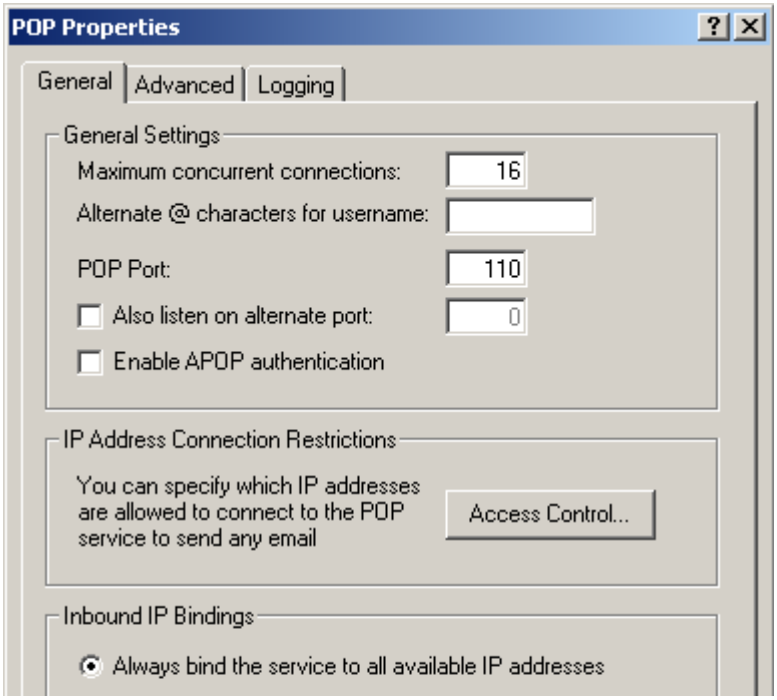
POP stands for Post Office Protocol. This is a mail protocol that enables emails to be retrieved from a remote mailbox. It allows you to collect emails from a hosted account on a server to your own email software, such as Outlook, Eudora etc.

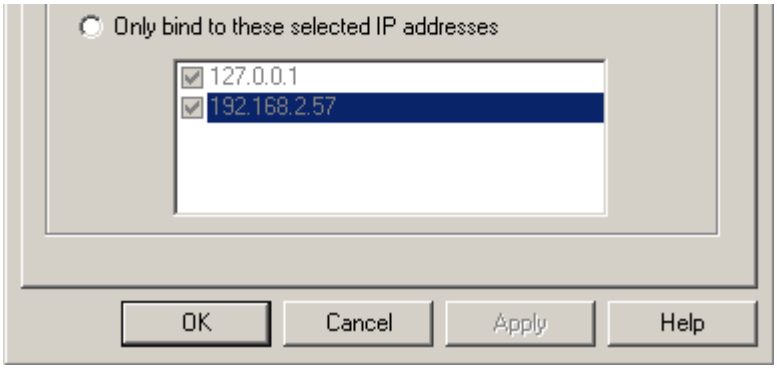
POP and SMTP servers are often the same computer. However, in some cases, one server is used for receiving mail (POP server) and another server is used for sending mail (SMTP server).

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

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

6.4.2 POP - General

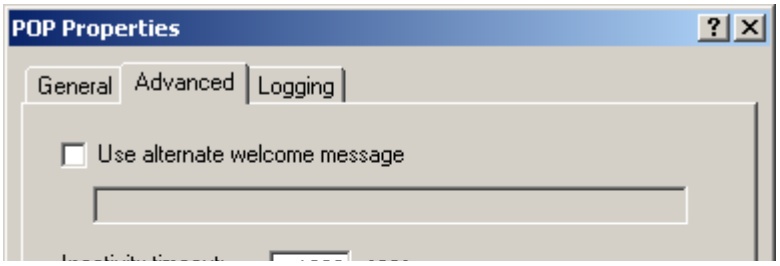


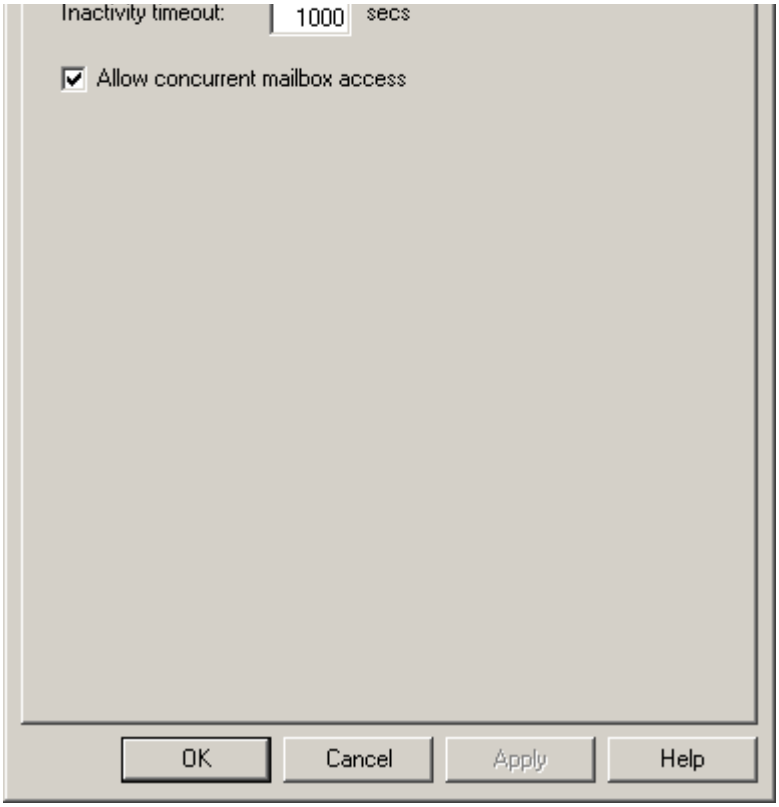


The following table outlines the configuration options for MailEnable's POP service:

Setting	Description
Maximum concurrent connections	The number of concurrent connections from email clients that the service will allow.
Alternate @ characters	Some older mail clients don't allow the use of @ in the username section. Since the MailEnable usernames are formatted in mailboxname@postoffice format, this may cause problems. To solve this, MailEnable 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	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.
Timeout for idle connections	If this setting is enabled, and a client connection has been idle or not passed any commands to the server for a set period of time, the connection will be dropped by the server. Timeout setting is in seconds.
Access Control	The Access Control feature can specify who can connect to the POP service. A list of IP addresses that are either banned from connecting, or are the only ones allowed to connect by selecting the Access Control button can be specified.
IP Addresses to bind POP to	It is possible to select the IP addresses that the POP service will be bound to. On a multi-homed machine you may only wish to allow connections on particular IP addresses. 'Always bind all IPs' will allow connections on all IP addresses that are configured for the machine.

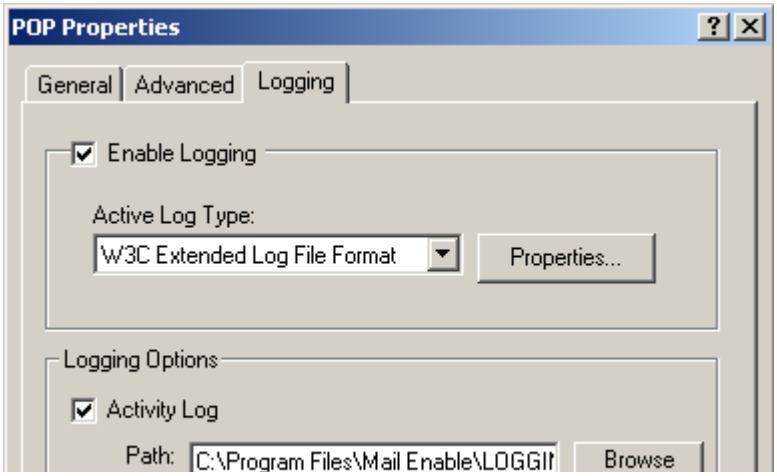
6.4.3 POP - Advanced

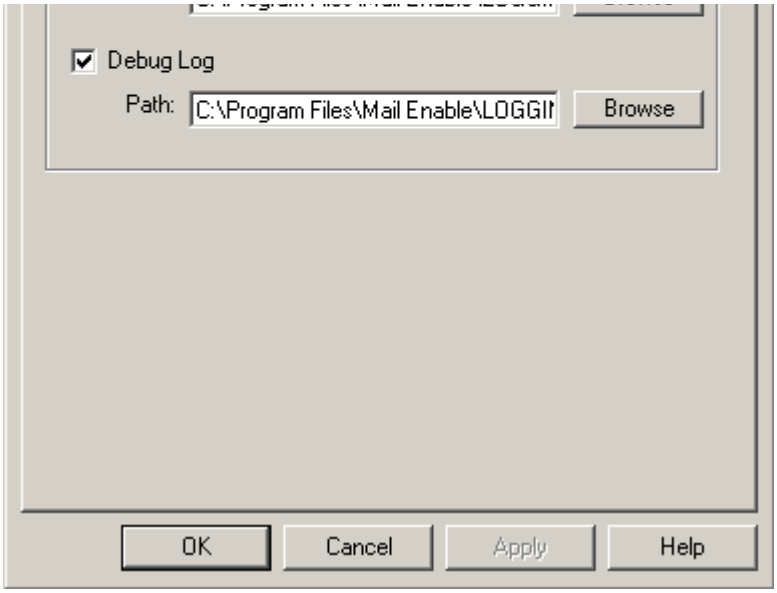




Setting	Description
Use alternate welcome message	This is the welcome message which is displayed to email clients connecting to the service.
Inactivity timeout	Set the inactivity timeout for the POP service. If a connection is inactive for longer than the timeout period (in seconds) then the connection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

6.4.4 POP - Logging





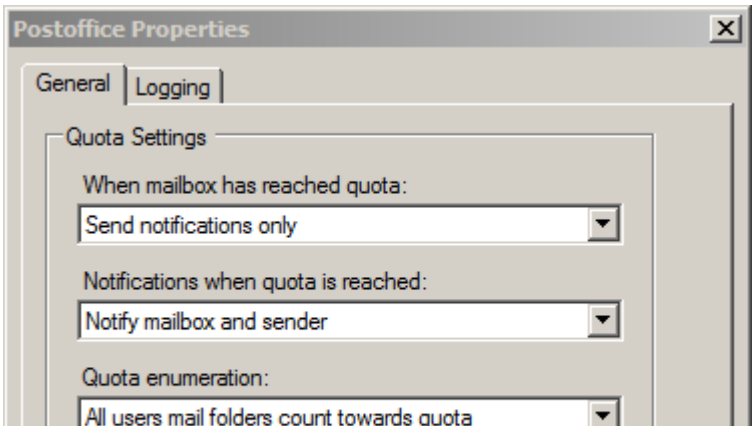
Setting	Description
Enable Logging	Enables W3C logging for the POP service. W3C logging can specify which fields are logged and the rollover frequency. The directory can also be specified.
Logging Options	Produces a debug and activity log for the POP3 service. Use this to obtain more details about the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

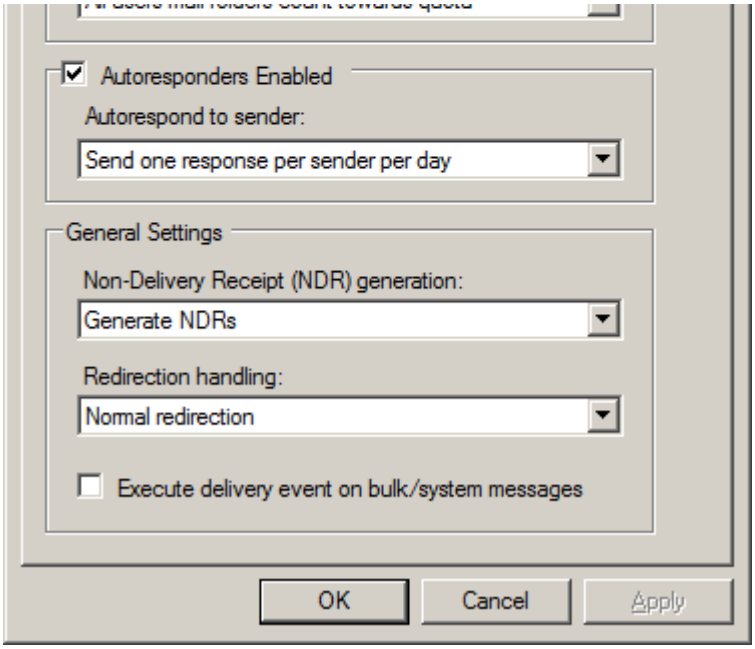
6.5 Postoffice Connector

6.5.1 Postoffice connector

The postoffice connector performs the delivery of emails to mailboxes. It is responsible for executing postoffice and mailbox filters, delivery events, auto responders and quota handling. It is possible to determine whether the user is notified of the quota issue and whether the message is returned to the sender or sent to the postmaster for that post office. MailEnable can configure what notifications are sent when a quota is reached, such options such as, Notify Sender only, notify sender and mailbox and send no notifications. Non Delivery Receipts can be configured options such as not sending NDRs or allowing the SMTP service to handle and send all default Non Delivery Receipts. Using the Administration Console you can access the Post Office Connector properties by expanding the **Servers > localhost > Services and Connectors** branch. Right click on the **Postoffice** icon and select **Properties**.

6.5.2 Postoffice connector - General

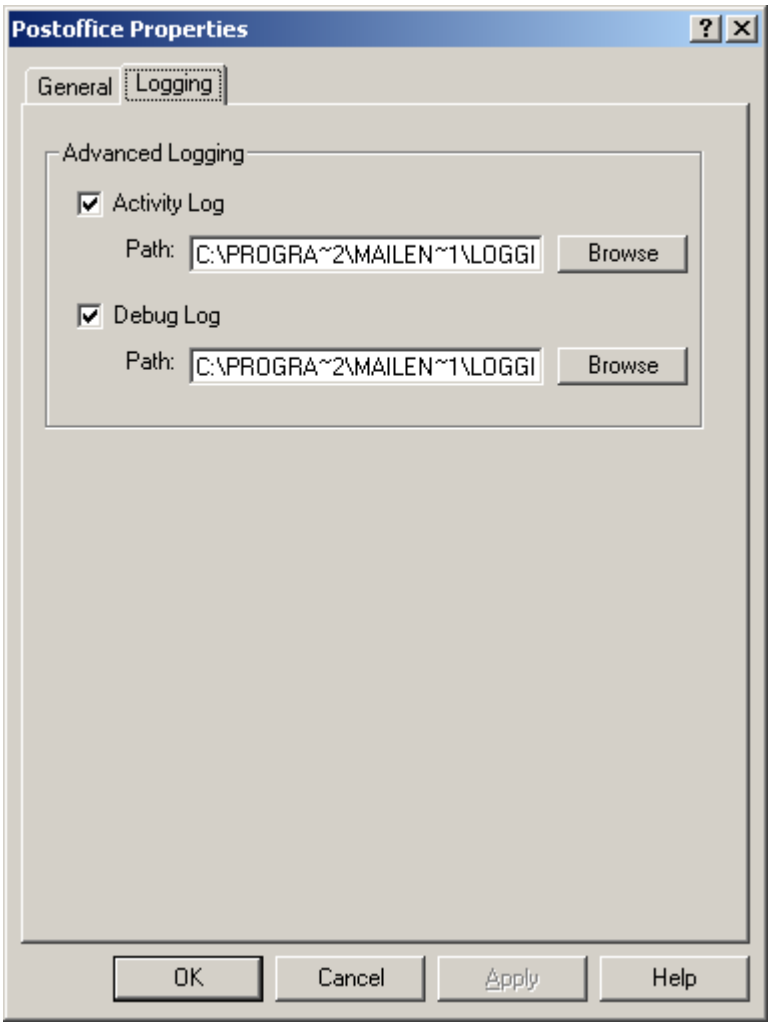




Setting	Description
When mailbox has reached quota	Specify what occurs when a mailbox's quota is exceeded. Determine whether the user is notified of the quota issue and whether the message is returned to the sender, or, sent to the postmaster for that post office. **Send incoming email to the Postmaster mailbox**: Redirects the email message that would put the mailbox over quota to the postmaster mailbox for the postoffice. **Send notifications only:** Will send a notification message and not the entire message.
Notifications when quota is reached	Configure what notifications are sent when a quota is reached, such options such as, notify sender only, notify sender and mailbox and send no notifications.
Quota enumeration	When a mailbox is at its quota, it can be calculated in two different ways. 1. Only Inbox folder counts towards quota 2. All users mail folders counts towards quota (Example: Sent Items, Drafts, Inbox)
Autoresponders enabled	When this setting is enabled there are two selections available for autoresponders: 1. The default setting is **Always respond to the sender**. This means every message delivered to the mailbox will generate a reply. 2. **Send one response per sender per day** will only reply to an email address once per day (using server time). If the check box is cleared then the autoresponder feature is disabled.
NDR Generation	The postoffice connector may deliver non-delivery receipts if a mailbox is disabled or unavailable. You can enable or disable this, or have it use the SMTP settings for NDR generation.
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. 4. Redirect as an attachment - will attach the original message to a new message indicating that the attachment is a forwarded message.
Execute delivery event on bulk/system messages	Allows delivery events to be executed on all messages arriving to a mailbox. By default system generated messages, such as notifications, are excluded from having the delivery event executed.

6.5.3 Postoffice connector - Logging



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

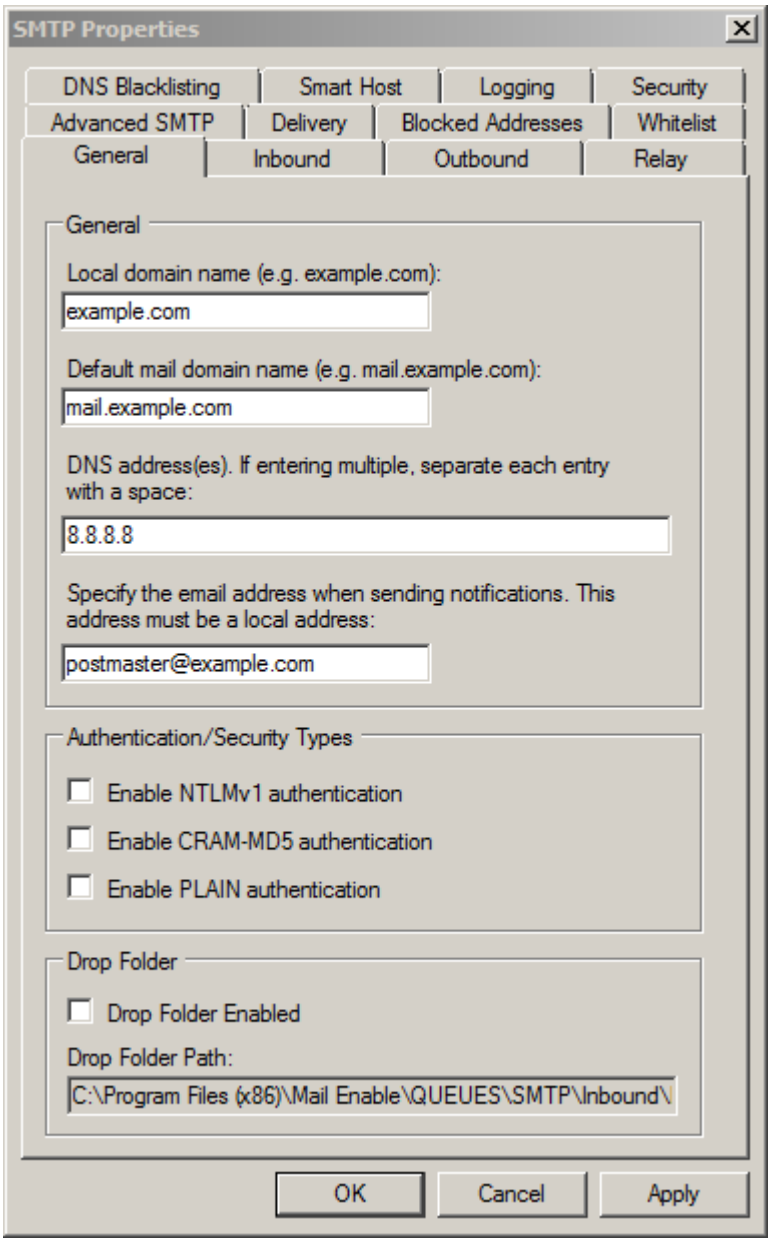
6.6 SMTP Connector

6.6.1 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.

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

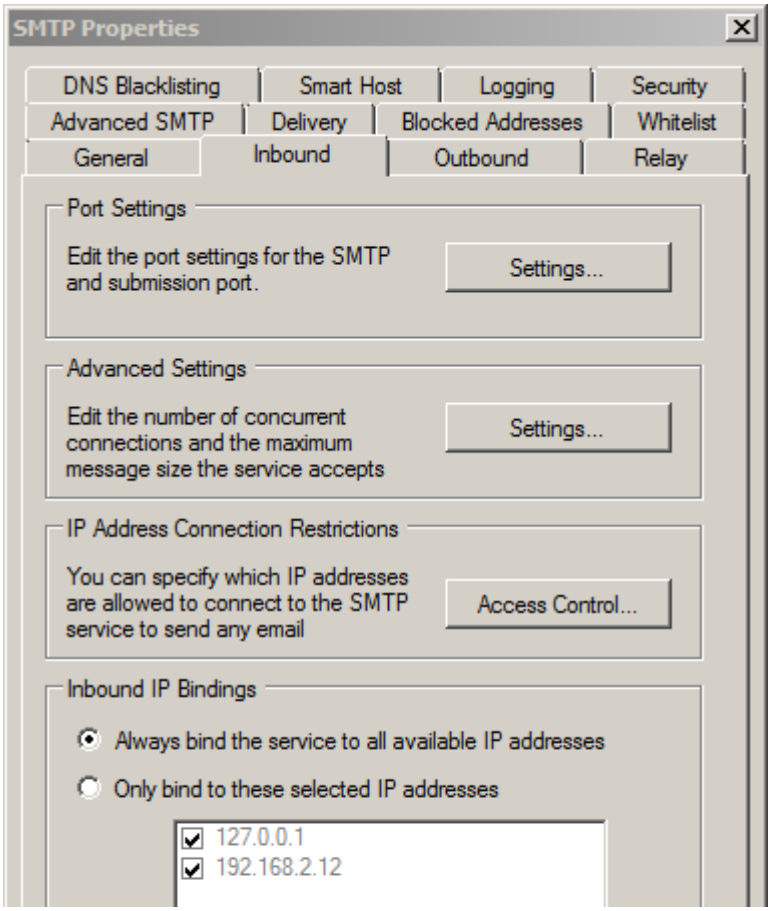
6.6.2 SMTP - General

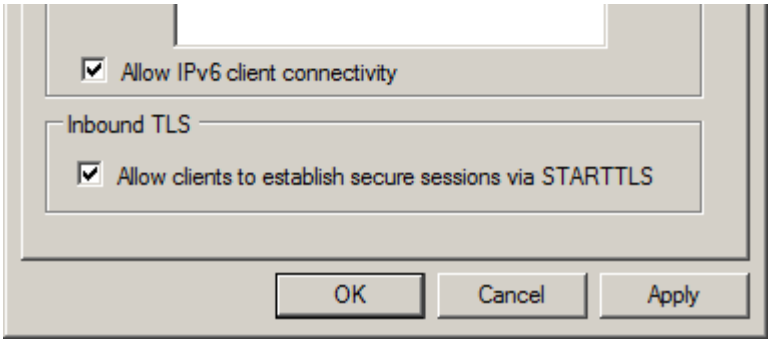


Setting	Description
Local Domain Name	The domain name of the server that MailEnable is installed on, or the default domain for the configuration. It is used for system messages, to announce the server when it connects to remote server, and when remote servers connect to MailEnable if the host name has 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.
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, where example.com is your local domain name. Make sure this is a valid email address.
Enable NTLMv1 Authentication	If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled to use this secure authentication. For example, in Microsoft Outlook the feature is called SPA – Secure Password Authentication. You should not enable this unless you have a specific reason, due to it being an old authentication method that is insecure and is being phased out by Microsoft.
Enable CRAM-MD5 Authentication	CRAM-MD5 Challenge-Response Authentication Mechanism is intended to provide an authentication extension that neither transfers passwords in clear text nor requires significant security infrastructure in order to function. Only a hash value of the shared password is ever sent over the network, thus precluding plaintext transmission. While slightly more secure than plain text, it is still recommended to always authenticate over a secure connection.
Enable PLAIN authentication	A plain text authentication method for SMTP.
Drop Folder	The drop folder is a folder that you are able to put email messages into, to be sent by the SMTP service. The email messages must be in RFC822 plain text format, and the recipient(s) of the message will be taken from the email header.

6.6.3 SMTP - Inbound

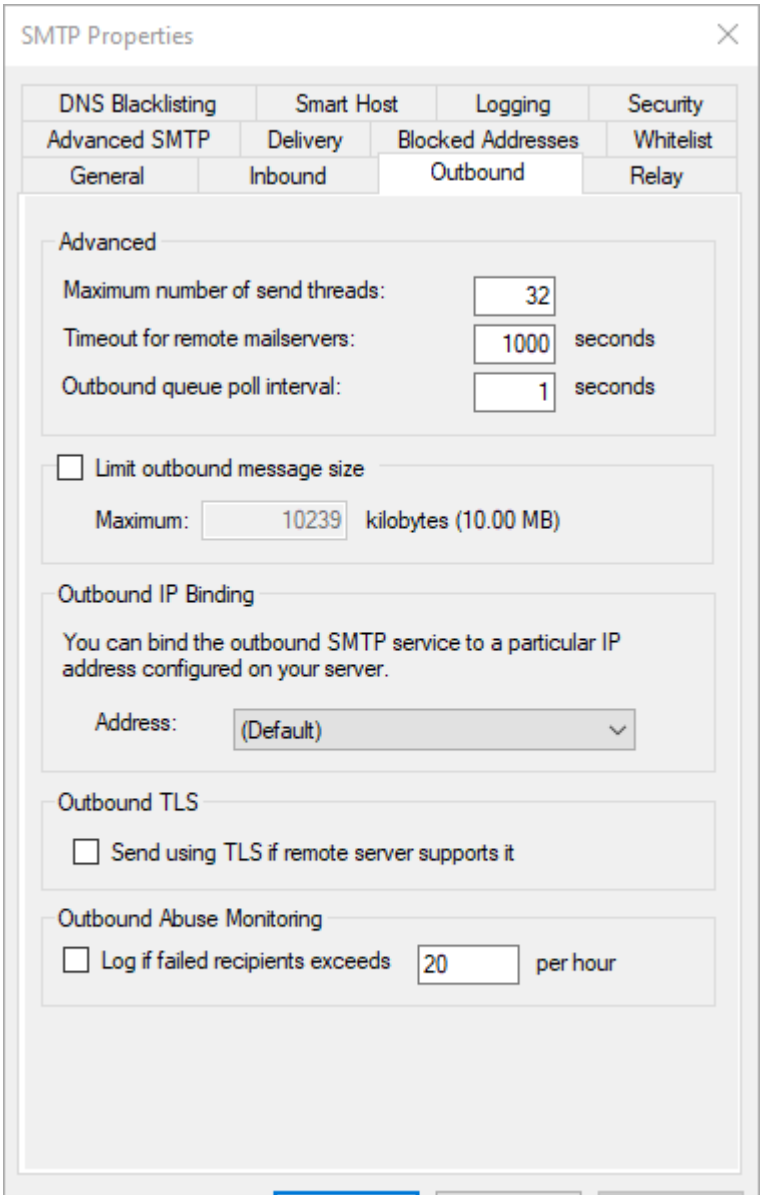


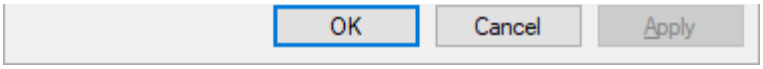


Setting	Description
Port Settings	**SMTP Port:** **SMTP service listens on port:** Determines the port the SMTP service is to listen on. The default is 25. Inbound SMTP connections from remote servers expect the mail server to be listening on port 25, but some proxy or gateway software may require this to be changed. **Requires SSL:** Enables SSL certificate encryption for the port. Please refer to **Server Configuration - Secure Sockets Layer (SSL) encryption (Section 5.8.1)** for information on how to enable SSL for the server. **Requires connections to authenticate before sending email:** When this option is enabled all inbound connections will be forced to authenticate on the default SMTP port before being able to send a message to a locally hosted mailbox. **Authentication Mode** Always allow authentication — This port will allow authentication attempts. Never allow authentication — This port does not allow any authentication. Only allow secure authentication (using SSL or TLS) — Authentication is only allowed if the connection is secure. **Submission Port:** The submission port is an alternate port to the default port 25. It is common to run another port for users to connect to, since many are blocked from connecting to mail servers on port 25 (which is done to reduce spam). **Additional Ports:** You are able to configure extra ports as needed, with the same options as the standard port.
Advanced Settings	**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 bytes. 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..

IP Address Connection Restrictions	**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 it may desirable to only listen to connections on particular IP addresses. 'Always bind the service to all available IP addresses' will allow connections on all IP addresses that are configured for the machine.
Allow IPv6 client connectivity	Enabling this option will will allow connections from clients using IPv6 addresses.
Enable TLS	The Transport Layer Security (TLS) protocol allow clients to connect to the SMTP service over the standard port and then negotiate for a secure transaction. TLS is only available on inbound connections. The SMTP connector will use the SSL certificate that has been configured for the server.

6.6.4 SMTP - 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.
Outbound TLS	Will try and establish a connection with the remote server using TLS if the remote server supports TLS, otherwise will fall back to a Non-TLS send. This does not require you to configure an SSL certificate locally.
Outbound Abuse Monitoring	This option logs to the SMTP Debug log an indication when a user has sent too many failed emails in an hour.

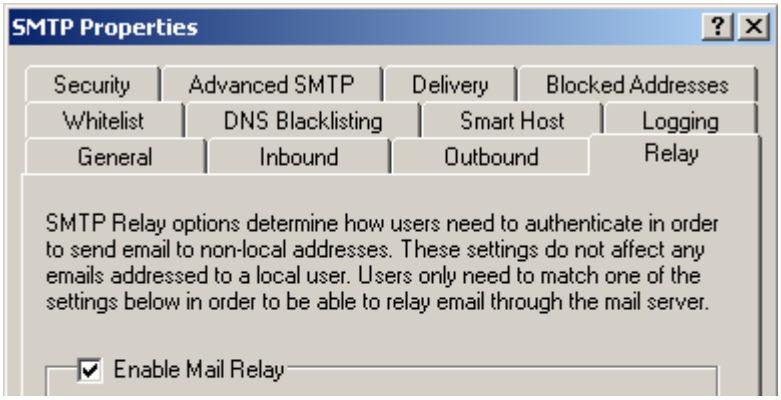
6.6.5 SMTP - Relay

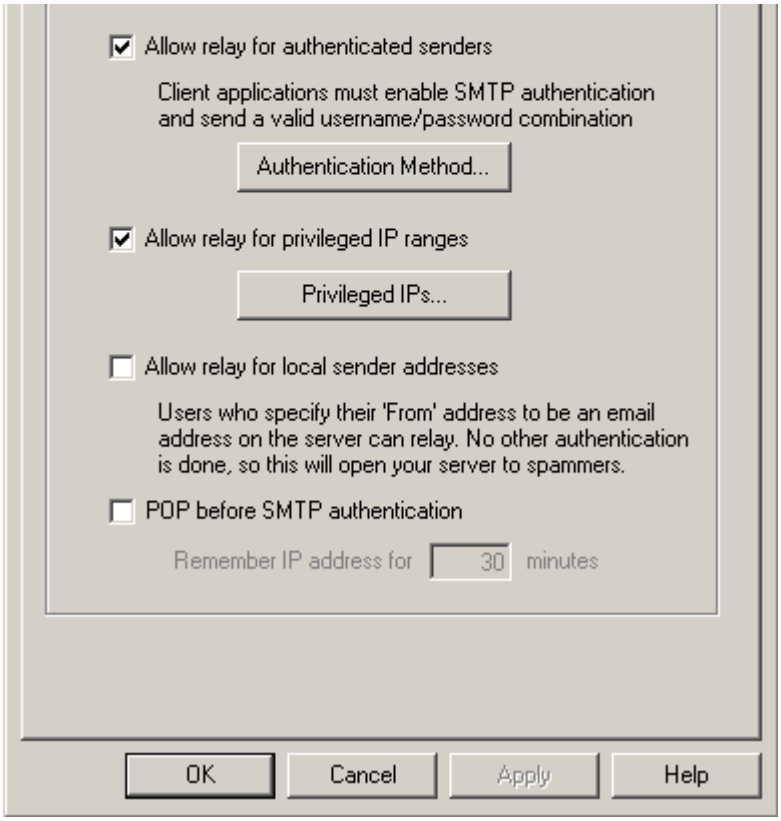
Mail servers accept messages for recipients that have their mailboxes hosted on the mail server itself. Any attempt to send a message to a non-local recipient (i.e. a recipient on a different mail server) is called a 'relay'. It is critical to regulate who can send messages to others (non-local recipients)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

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

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

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

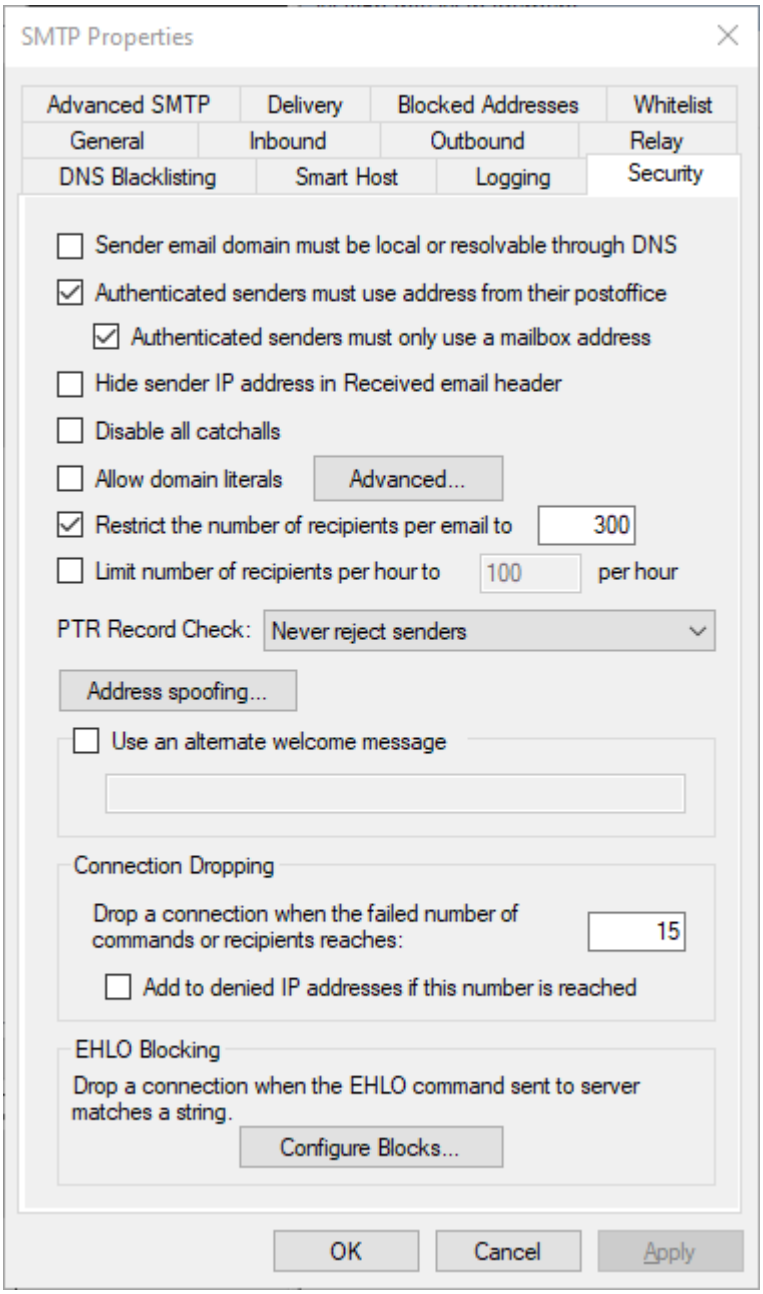




Setting	Description
Enable Mail Relay	Mail relaying needs to be enabled in order to send mail. Otherwise MailEnable will only be able to receive email. There are four options available to limit who can send mail out through the server. It is possible to select any combination of the four, however, a 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.

6.6.6 SMTP - Security

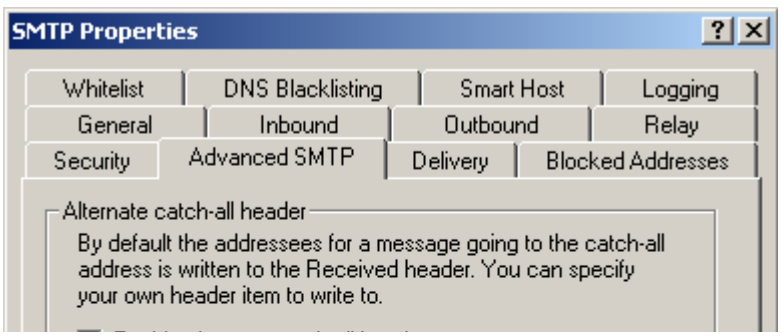


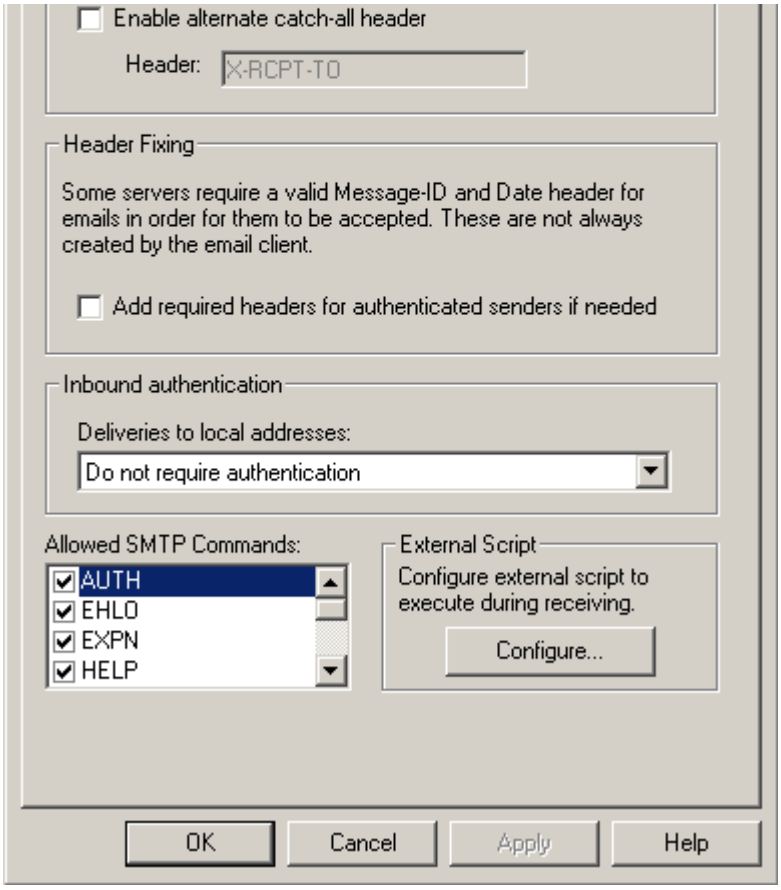
Setting	Description

Sender email domain must be local or resolvable through DNS	This option checks the domain of the SMTP envelope address to make sure it is a valid domain. The domain either has to be configured in MailEnable, or it has to be able to be resolved through DNS. If not then the message will fail with a permanent error. This can help reduce spam from senders making up email domains for send attempts.
Authenticated senders must use address from their postoffice	If this is selected, users who are authenticating to send email must configure their email client with an email address that valid for their postoffice. This option is helps force clients to use a legitimate email address, thereby reducing the possibility of spam.
Authenticated senders must only use a mailbox address	If this is selected, users who are authenticating to send email must configure their email client with an email address that is configured under their mailbox.
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
Disable all catchalls	Catchalls for domains will cause the email server to collect a lot more email and can cause the server to relay spam (i.e. if the server redirects a catchall to a remote email address). This option will stop all catchalls from working.
Allow domain literals	MailEnable will allow inbound emails to be formatted as user@[IP Address], such as user@[192.168.3.10]. MailEnable will accept emails for any of the IP address that have been configured on the server. If using NAT, or to accept extra IP addresses which are not configured on the server, select the Advanced… button. This will allow these extra IP addresses to be entered.
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.
Limit number of recipients per hour to	This setting sets how many recipients can be sent to on a hourly basis. This is per mailbox that authenticates, so each mailbox can send up to this number of messages over an hour period. When checking whether a recipient will be accepted, the mail server will check to see how many messages the mailbox has sent in the previous hour.
PTR Record Check	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. There are three options available for the check: **Setting** — **Description** Never reject senders — Does not perform any PTR checks on connections. Reject senders without PTR — If a remote server is sending to the SMTP service, and does not authenticate, then the email will be rejected if the IP address does not have a PTR record. Refer to System Spam Filter — This will mark the message as not having a PTR record. The Spam Protection filter will then be able to rank the inbound message for spam prevention.
Address Spoofing:	Address spoofing is where the user sends an email using an email address that is not mapped to the mailbox they are authenticating as. The option checks the SMTP envelope sender, not the headers of the email. i.e. it checks the email address used in the SMTP conversation (the

	MAIL FROM address). Enabling this can help identify sources of spam, and force users to only use their own email addresses. **Anyone can spoof sender addresses:** If this is selected, anyone sending email through the server can use an email address which matches a domain configured on the server, even if they do not authenticate. **Authenticated users can spoof sender addresses:** If this is selected only users who are authenticating to send email can use an email address that has a domain that is configured on the server. **Authorized connections can spoof sender addresses:** If this option is selected it will allow authenticated and any privileged IP address within the SMTP privileged IP's list to send email using an address containing a domain configured on the server.
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
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 commands to the server during a connection. By enabling this option, MailEnable will drop the client connection. If you have scripts or applications sending email that ignore errors, they may be affected.
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. The SMTP Debug log will indicate when an address is added by one of the following descriptions: ME-I0073: IP address [IP address] for account [postoffice] user [mailbox] banned for too many invalid commands. ME-I0073: Unauthenticated IP address [IP address]s banned for too many invalid commands.
EHLO Blocking	This option allows you to drop connections if they send a specific string in the SMTP EHLO command. For example, a common spam bot will use EHLO ylmf-pc. So entering ylmf-pc will drop these connections.

6.6.7 SMTP - Advanced SMTP

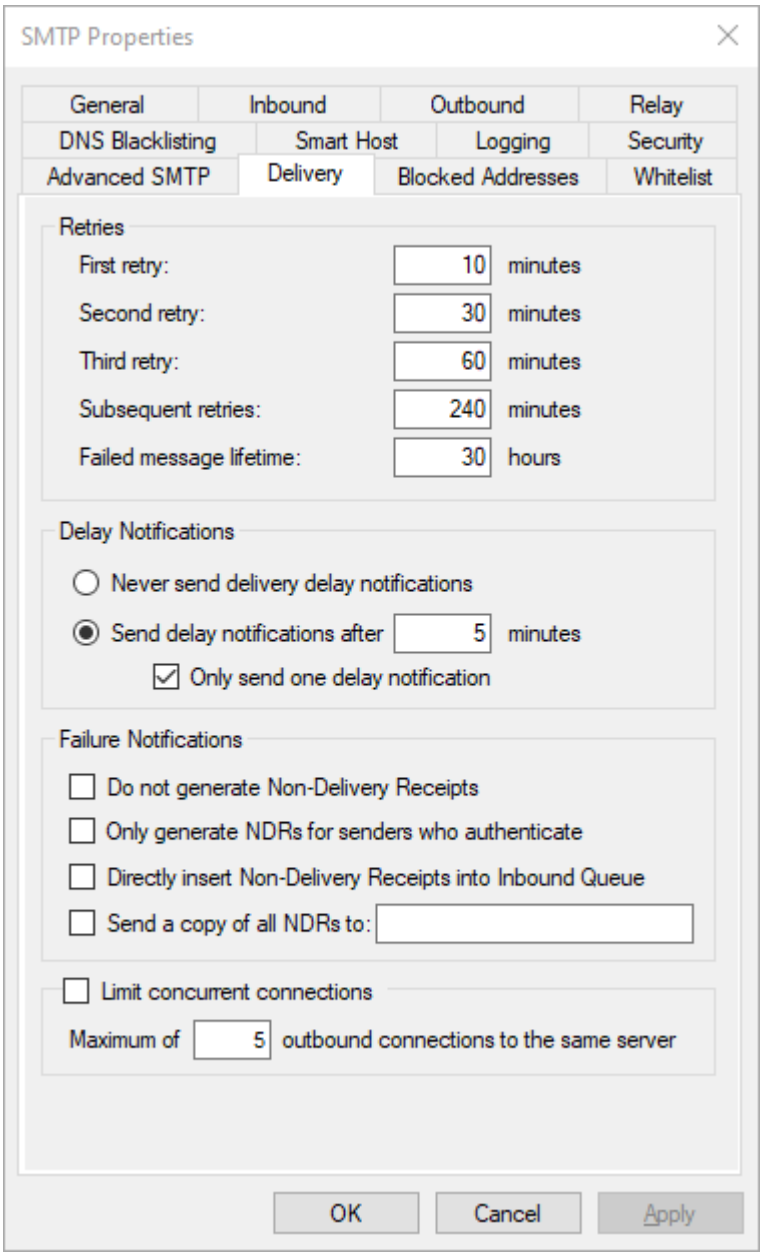




Setting	Description
Enable alternate catch-all header	When mail is sent to an invalid recipient and they are specified as a BCC on the message, it is difficult for the mail administrator to know who should have received the message. The catch-all header allows you to specify the name of the message header field that is used to record any recipients that were delivered to the catch-all account. By default, MailEnable records this information into the Received By: message header; hence this setting is supplied to provide more control over how the information is recorded within the message. Only one copy of a message with multiple recipients is delivered to the catchall mailbox.
Add required headers for authenticated senders if needed	Some email clients or applications will not add a Message-ID or Date header line to their emails. 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.
Inbound Authentication:	**Do not require authentication:** This setting will enforce that no inbound authentication is required for remote senders that send to locally hosted MailEnable addresses. **Require authentication for all connections:** This setting will enforce authentication for all inbound connections. Any remote server that tries to send to a locally hosted address within MailEnable will require authentication. **Authentication determined by postoffice:** This setting will set the inbound authentication setting to be determined by the postoffice restriction settings. Please see the postoffice **restrictions ('Postoffice - Restrictions' in the on-line documentation)** setting **Any emails to this postoffice must come from authenticated connections** for more information.
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.

External Script:	This setting will execute a script during the SMTP transaction. The settings that can be enabled are: **Enable script function for MAIL FROM command:** This setting will execute a script during the SMTP MAIL FROM command. **Enable script function for RCPT TO command:** This setting will execute a script during the SMTP RCPT TO command. **Enable script function for DATA command:** This setting will execute a script during the SMTP DATA command. The **Edit Script...** button opens the editing script window. The editing window will contain example MailEnable variables that can be used within the script. Please consult within the API guide for more information.

6.6.8 SMTP - 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 the 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 can either turn delay notifications off, send a message only on the first failure, or to send a message back for each send delay. There is also the option to only send delay notifications after a specified period of time from when the message send is first attempted. This will allow the SMTP service try to send the message more than once before the sender is informed that there is a delay.
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.
Only generate NDRs for senders who authenticate:	This setting when enabled stops NDRs to be generated for non authenticated senders. Spammers can cause problems by sending emails which return a non delivery report to the sender. Most of the time the sender address is not the spammers address and therefore the NDR creates its own spam which is also known as email bounce back scatter.
Directly insert Non-Delivery Receipts into Inbound Queue	This will insert NDRs into the SMTP inbound queue instead of the SMTP outbound queue, which is the default.
Send a copy of all NDRs to	This will allow you to send a copy of every NDR generated to a specific SMTP address.
Limit concurrent connections	This setting will limit the amount of concurrent outbound connections that can be made to the same server. This is useful to stop spammers that have managed to spam through the server and send large amounts of messages to the same server as this can consume all the available SMTP send threads and delay messages to other remote servers sitting in the outbound queue to be delayed. this can also reduce the risk of large hosting companies blacklisting your severs IP address because of bulk sends.

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

Mail Enable\Config\Postoffices\[postoffice]

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

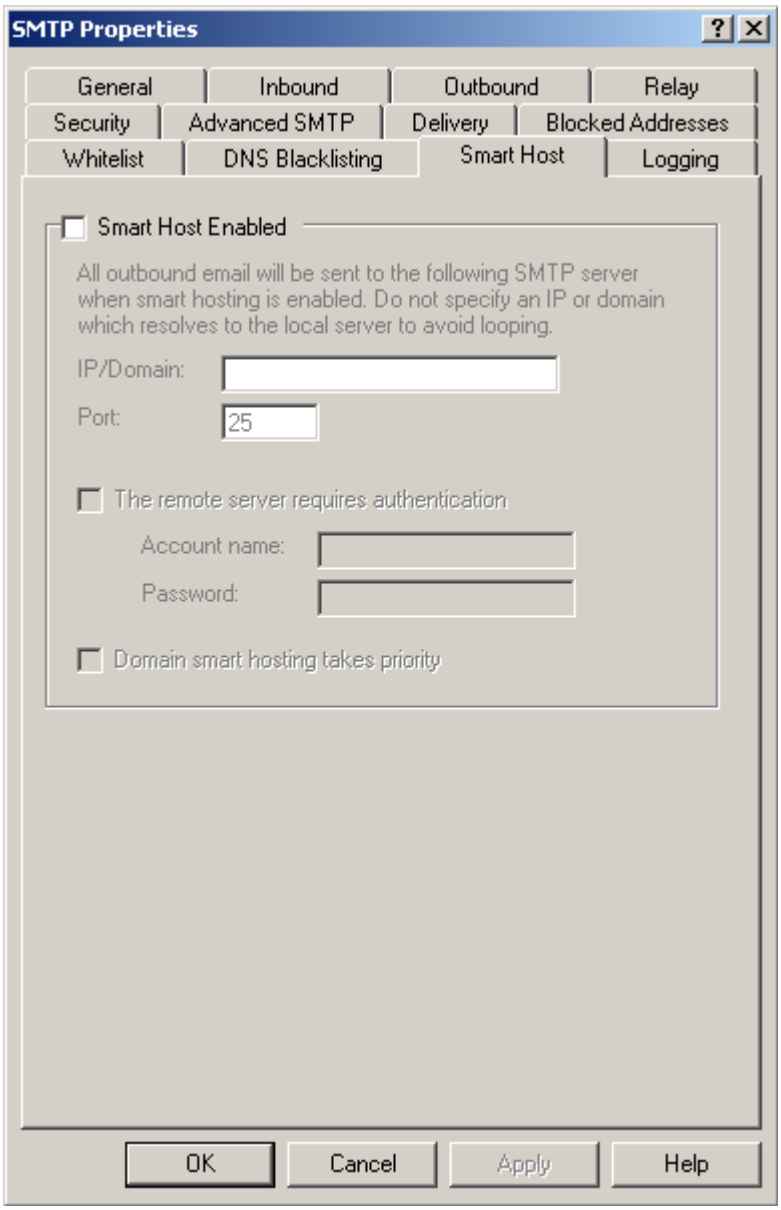
Mail Enable\Config\Postoffices

MailEnable provides two template files for non-delivery reports:

Setting	Description
SMTP-NDR-FAILEDRECIPS.TXT	Non-Delivery Message that has a list of failed recipients (ie: one or more recipients were refused by the server)
SMTP-NDR.TXT	Non-Delivery Message that has no failed recipients (ie: transmission errors, system errors)

The following tokens can be used in a template: [ME_POSTMASTERADDRESS], [ME_TOADDRESS], [ME_DATE], [ME_MESSAGEID], [ME_FAILEDRECIPIENTS] and [ME_MESSAGEHEADERS]

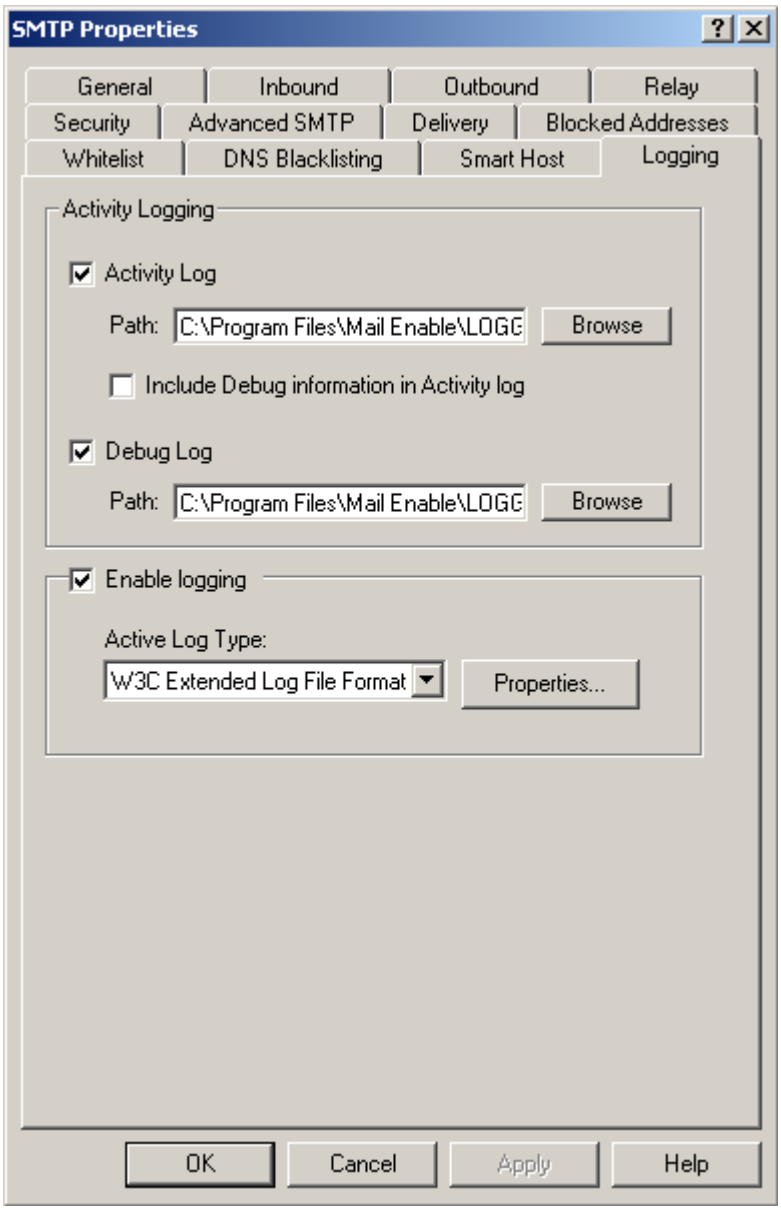
6.6.9 SMTP - Smart Host



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	The server that is being forwarded all of the email may require SMTP authentication. If so,

requires authentication	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.

6.6.10 SMTP - Logging



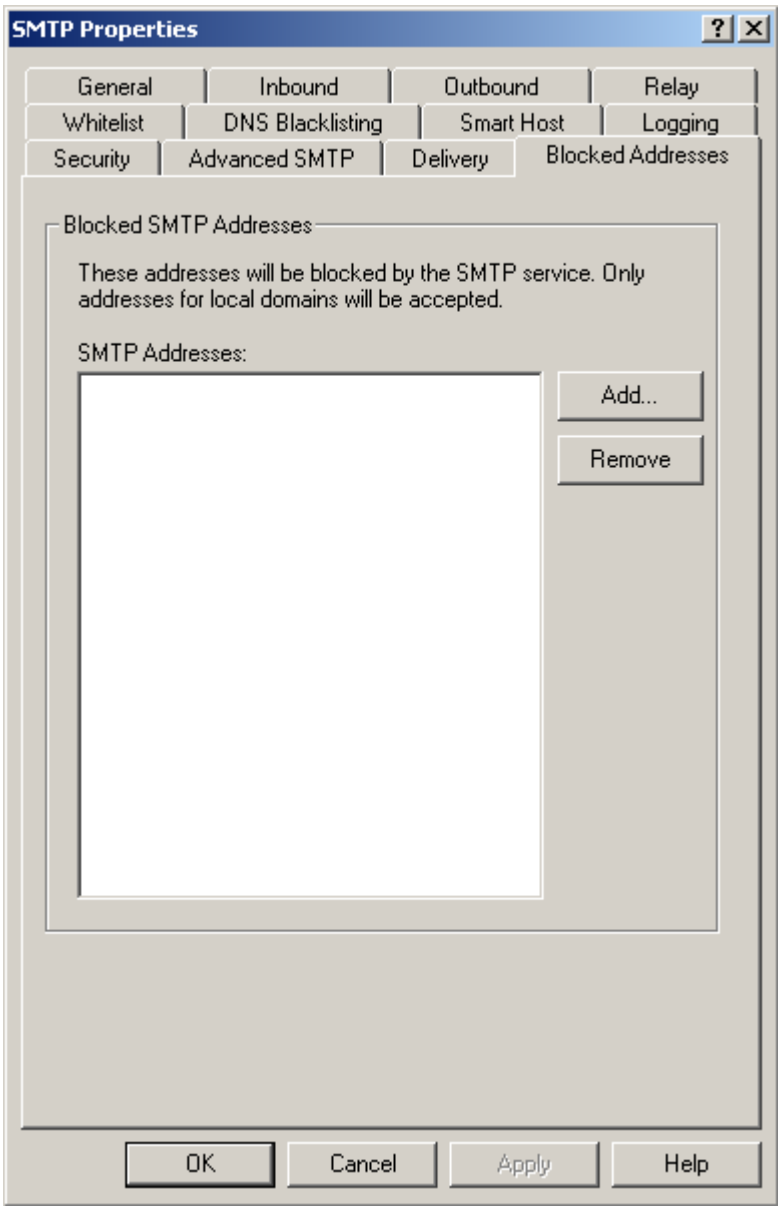
MailEnable's SMTP Connector provides W3C, Activity and Debug logging. W3C logging is used to record service usage, Activity logging is used to record system activity and Debug logging is used to provide low-level information on system activity.

Setting	Description
Activity Log	Enables the Activity Log. **Include Debug information in the Activity log -** Merges the debug logging information within the activity log file

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.

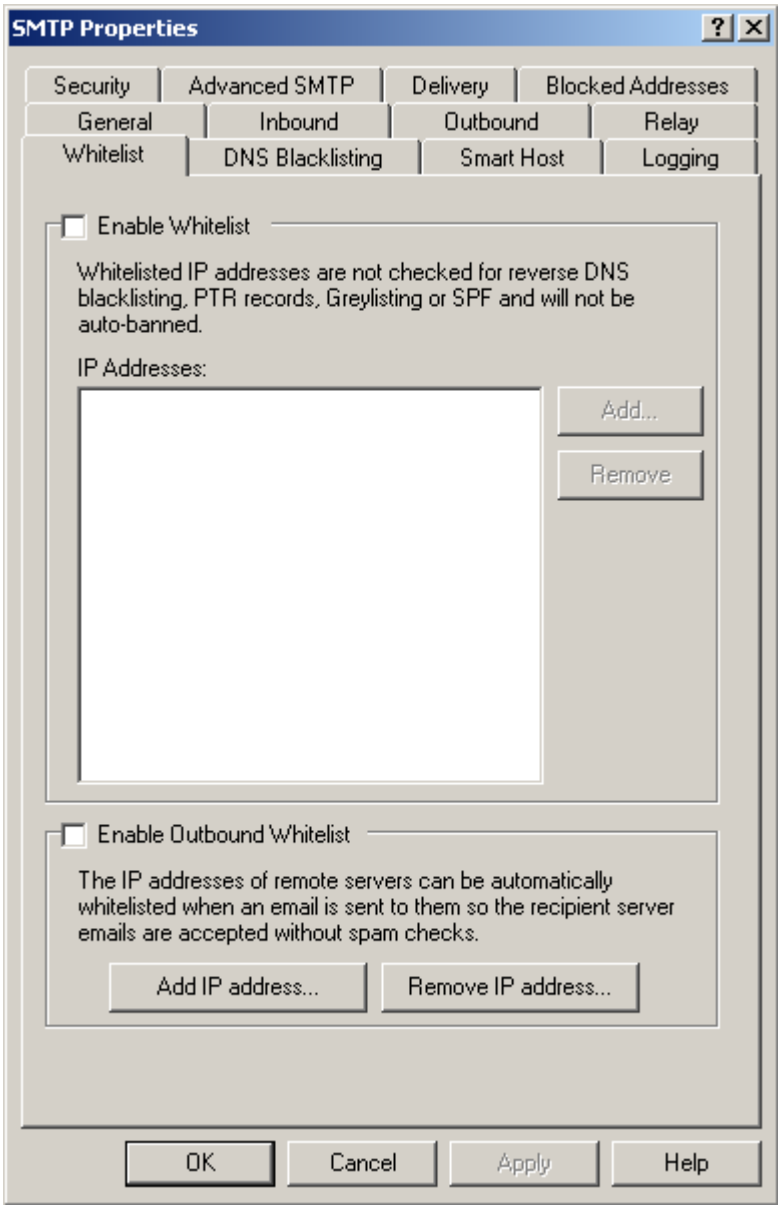
6.6.11 SMTP - Blocked addresses

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



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

6.6.12 SMTP - Whitelist



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.

MailEnable can also automatically whitelist IP addresses to which it has addressed outbound e-mail. This helps reduce the SMTP service from rejecting email from valid senders, as it makes the assumption that if you send to an IP address then that IP is a valid mail server and incoming email from that IP should not be blocked.

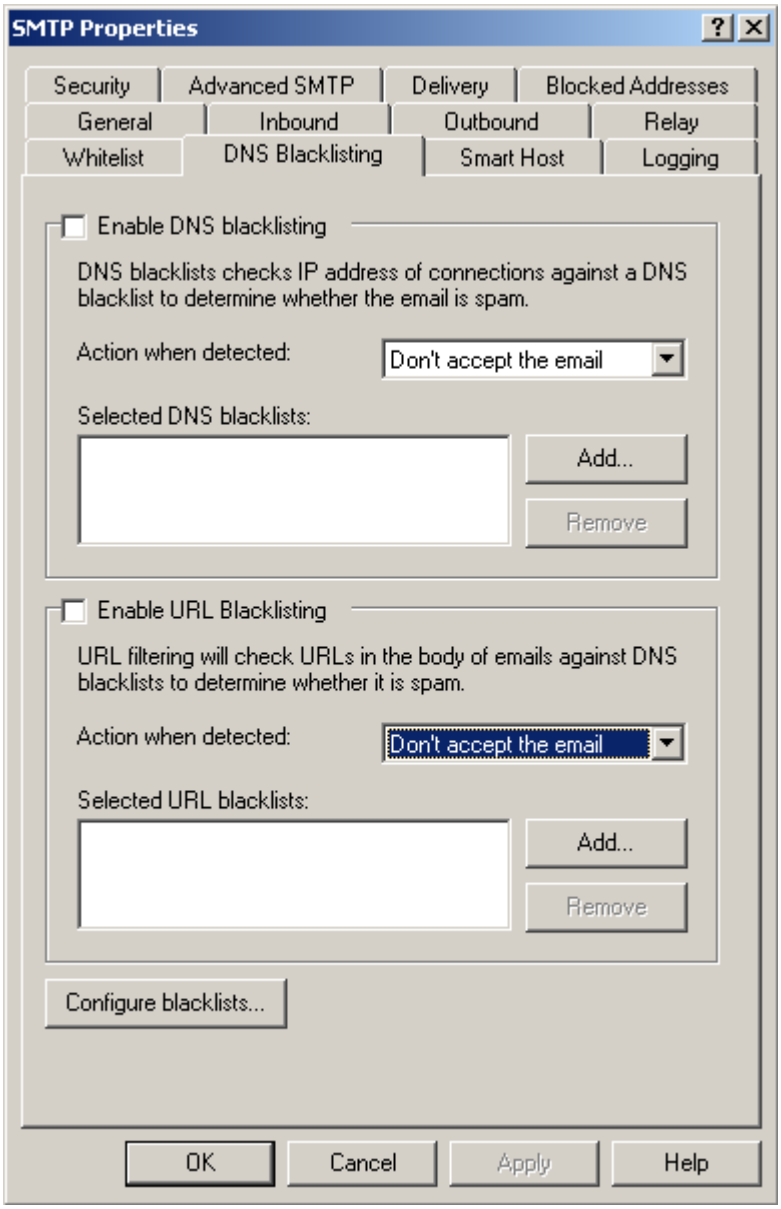
Setting	Description
Enable white list	Enables the SMTP white list.

Add	Adds an IP address to the white list.
Remove	Removes the selected IP address from the white list.

6.6.13 SMTP - DNS Blacklisting

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

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



How to add a Reverse DNS blacklist for spam filtering

1. Within the Administration program navigate to: **Servers > localhost > Connectors > SMTP**
2. Right click on **SMTP** and select **properties** in the menu.
3. Select the **DNS Blacklisting** tab.
4. Tick the option to **Enable DNS Blacklisting**
5. Select the desired **Action when detected** (the default is Don't accept the email).
6. Click on the **Add** button to select a blacklist.
7. Select a blacklist and then click **OK**.
8. The selected blacklist will be displayed within the **Selected DNS Blacklists** display window.
9. Repeat this process to enable multiple lists.

How to add a URL blacklist for spam filtering

1. Within the Administration program navigate to: **Servers > localhost > Connectors > SMTP**
2. Right click on **SMTP** and select **properties** in the menu.
3. Select the **DNS Blacklisting** tab.
4. Tick the option to **Enable URL Blacklisting**
5. Select the desired **Action when detected** (the default is Don't accept the email).
6. Click on the **Add** button to select a blacklist.
7. Select a blacklist and then click **OK**.
8. The selected blacklist will be displayed within the **Selected URL Blacklists** display window.
9. Repeat this process to enable multiple lists.

How to configure custom blacklists

1. Within the Administration program navigate to: **Servers > localhost > Connectors > SMTP**
2. Right click on **SMTP** and select **properties** in the menu.
3. Select the **DNS Blacklisting** tab.
4. Click on the **Configure Blacklists...** button.
5. Click on the **Add** button.
6. Next specify a blacklist name.
7. In the Blacklists details section specify the **lookup type** and zone and the record type to check for.
8. Next click **Save.**

DNS and URL blacklisting options

Setting	Explanation
Current Enabled DNS Blacklists	Shows all lists that have been enabled for the server. This includes the MailEnable defaults and any personally created lists.
Add Button	To choose a blacklist, select this button, select a list and click OK. The list will now be displayed in the "Current enabled DNS Blacklists" window on the DNS Blacklisting TAB.
Remove Button	To remove a list at any time, select the blacklist in the "Current enabled DNS Blacklists" window on the DNS Blacklisting TAB and select the Remove button.
Enable DNS Blacklisting	Enables or disables reverse DNS Blacklisting for the SMTP Connector.

Action when detected	The two actions here are; **Don't accept the email -** this will prevent connection by the remote server and respond accordingly. This is the best option for reducing server load. **Mark the message as spam** - by adding a line to the header. If enabled the message will be delivered to the Junk E-mail folder within the email client. For further information on the Mark Message as Spam action please review Feature selection in the **Message store section ('Postoffice - Message Store' in the on-line documentation)**.
Enable DNS Blacklitsing	When enabled all messages will have their content scanned for links to web sites. When a link is found, then MailEnable will check the IP addresses of any URLs found to see whether they are contained in the selected blacklist.
Enable URL Blacklisting	When enabled will check URL's in the body of emails against DNS blacklists to determine weather it is spam.
Action when detected	The three actions here are; **Don't accept the email** - this will prevent connection by the remote server and respond accordingly. This is the best option for reducing server load. **Mark the message as spam** - by adding a line to the email header indicating it is spam. This will allow locally delivered messages to be delivered to the Junk E-mail folder. For further information on the Mark Message as Spam action please review the **Feature selection section ('Postoffice - Feature selection' in the on-line documentation)**. The **"Replace the link"** option will remove the failed link URL of the message and replace it with "Link is removed".
Configure Blacklists Button	Opens a screen to allow blacklists to be created or added.
Lookup type	The lookup type that will be used for the blacklist.
Zone Server	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.
Response	The response that can be sent to the client when a message has been rejected.

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.

6.6.14 SMTP Connections

Both the current inbound and outbound connections can be viewed in the administration program. Connections may appear and disappear fast. If a connection is listed for a long period of time, it may be that the email is large and it is still being sent or received, or that the remote connection is no longer connected, but the disconnection has not been detected yet.

Column	Description

Connection time	The time in seconds from when the connection was made.
Socket	The socket number for the connection. This can be useful when looking through the SMTP logs for the connection conversation. Sockets numbers are reused.
ClientIP	The IP address that the connection is coming from.
Remote Domain/Domain	When an SMTP connection is made over SMTP, the remote software will indicate their identity (via the SMTP HELO/EHLO command). For remote servers it could be a domain or IP address, and generally for users it is their machine name. For outbound connections this column will indiate the domain the connection is to.
Sender	If the sender has use the MAIL FROM SMTP command, then this email address will be displayed in this column.
Last command	The last SMTP command the connection has sent.
Postoffice	The postoffice associated with the message being sent.
User	The user associated with the message being sent. If a user has authenticate to send the email, this this will be the mailbox they authenticated as.

6.6.15 SMTP Queues

There are both inbound and outbound queues for the SMTP service. Inbound messages are written into the inbound queue as they arrive, and when they are fully received, the MTA service will then move the messages to their destination queues. Inbound messages will only display in the queue list during the the brief time they are being received. For the outbound queues, emails will remain in the queue until they are successfully sent or bounced (which may be due to a recipient failure, or that the email could not be sent in a specified time, which is determined by the SMTP delivery settings).

Right clicking an email in the queue will provide you with the following options:

Menu	**Description**
Send Now	Try to send the message immediately instead of waiting for the next scheduled attempt.
View Send History...	This will use the message tracking utility to try to use the log files to show information about previous send attempts and provide more details of why they may have failed.
Delete	Deletes the email messager from the queue. The email is permanently deleted and cannot be recovered.

For emails in the queues, the following information will be displayed:

Column	**Description**
Filename	The name of the file in the queue.
Status	The socket number for the connection. This can be useful when looking through the SMTP logs for the connection conversation. Sockets numbers are reused.
Destination	The destination domain of the email message. This will be blank until the first delivery attempt.
Size	The size of the message file in bytes.
Date	The date and time the email was put into the message queue.

Subject	The subject of the email.
Retries	The number of times a delivery has been attempted. This is the number since the last time the SMTP service was restarted.
Last error	If a delivery error has occurred, this will display the reason for the last failure.

Messages in the SMTP queue can be examined by double clicking on them. When a double click is excuted, a window will appear with more details about the email message and options to perform on it.

Option	Description
Block	This will add the IP address of the sender to the SMTP access control settings, so the IP address will no longer be able to connect to the SMTP service.
Disable	This will disable the mailbox sending the email.
View message...	This will view the raw message data of the email.
View Send History...	This will use the message tracking utility to try to use the log files to show information about previous send attempts and provide more details of why they may have failed.
Delete all emails in queues for mailbox...	This will delete all emails in the queue for the mailbox.

6.7 Web Mail

6.7.1 Web Mail

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

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

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

Some of the features of MailEnable web mail include:

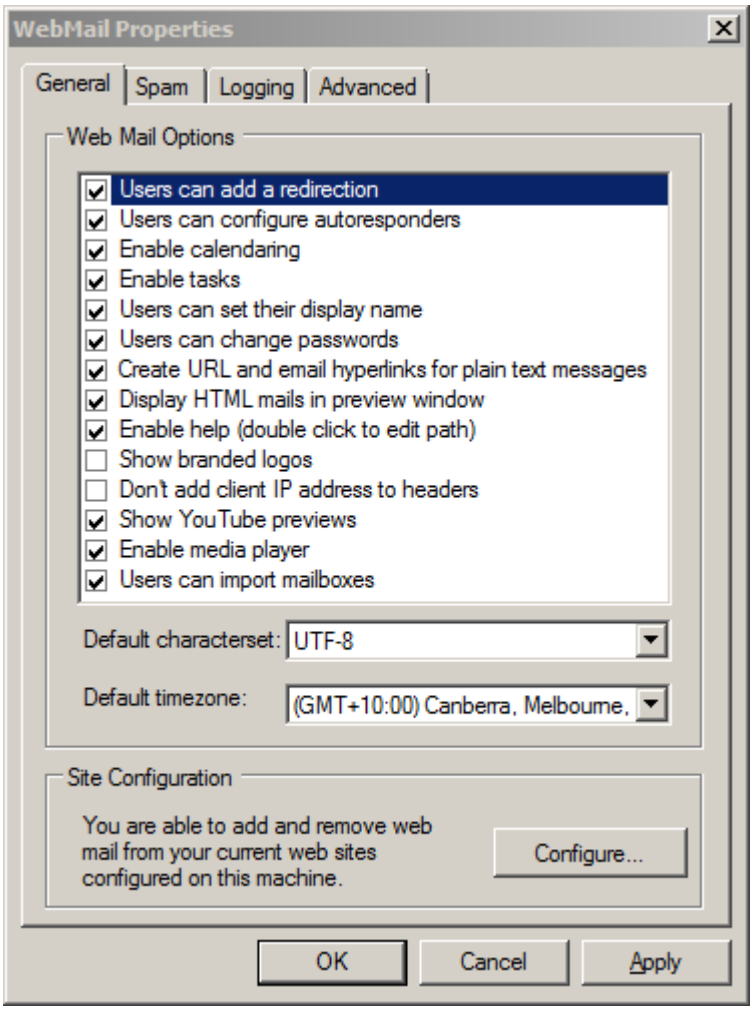
- Add attachments to emails
- Contact list
- Reply, reply to all, forwarding, read receipts, message priority
- Viewing & editing of HTML mail
- Support for various character sets (Big5, etc.)
- E-Mail Signatures
- Manage folders
- Custom skins

MailEnable web mail is installed as a Virtual Directory under an existing IIS Web Site. Typically there are two web

sites that are pre-configured under IIS, these are the **Default Web Site** and the **Administration Web Site**. IIS allows additional sites to be created (either using host-headers or additional IP addresses) using the Internet Services Manager. MailEnable will also create a MailEnable website for host headers that are created via the administration console. The website is named **MailEnable Webmail**. More information can found in **Publishing via host headers or virtual directories (Section 6.7.3.2)**

6.7.2 Web Mail - Properties

6.7.2.1 Web Mail - General

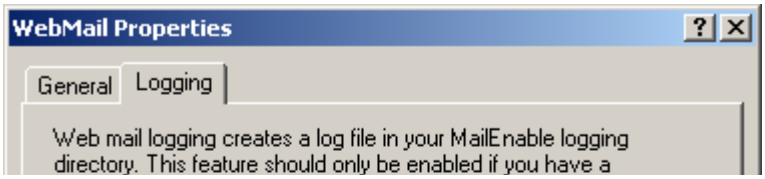


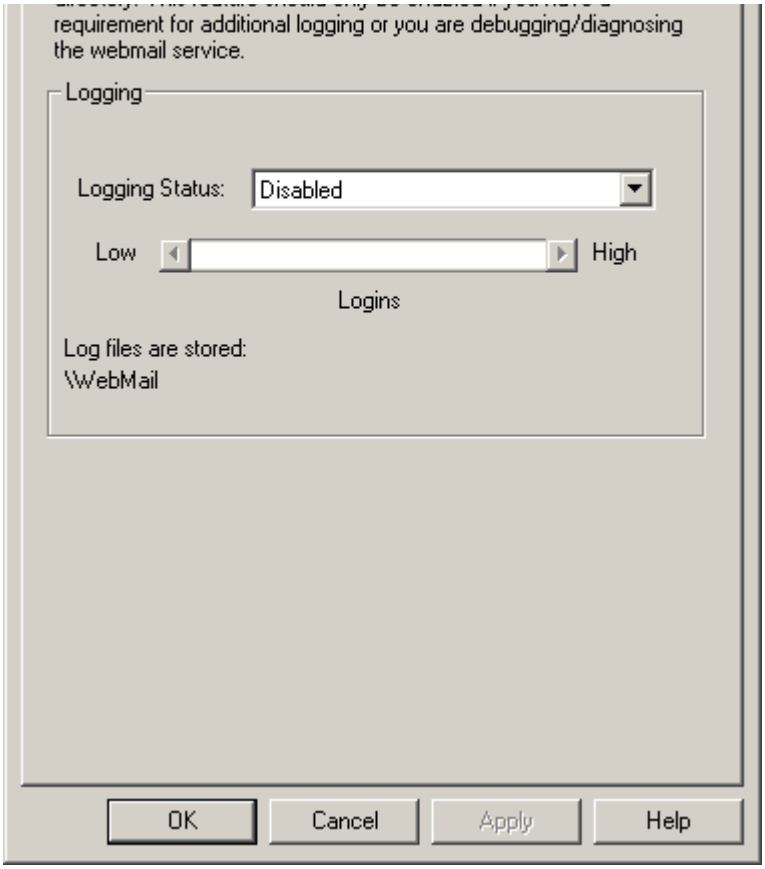
Setting	Description
Users can add a redirection	When disabled the **Redirections** option under the **Mail** branch within the Web Mail **Options** page will no longer be available.
User can configure autoresponders	When disabled the **Auto response** option under the **Mail** branch within the Web Mail **Options** page will no longer be available.
Enable calendaring	This enables a calendar to be viewed and managed in web mail. This is not a shared calendar - each mailbox has its own calendar that can be used when logging in.
Enable tasks	Enables or disables the use of tasks for all web mail users
User can set their display name	This allows a user to create a friendly name in the web mail options. This display name will only be used when sending from web mail.
User can	This gives a mailbox user the ability to change their password in the options of the web mail.

change their passwords	
Create URL and email hyperlinks for plain text messages	Enables the underlining and HTML link creation for emails and URLs in a message formatted in plain text format.
Display HTML mails in preview window	Selecting a message in the inbox the web mail message will be automatically displayed in the preview window underneath the inbox list. The main reason for not viewing in HTML would be performance reasons and, in some cases, security.
Enable help	Enables help links within the web mail interface
Show branded logos	Enables/Disables company logos within Web Mail displayed in the top left hand corner of the interface.
Don't add client IP addresses to headers	Enabling this option will hide the clients IP address within the message RECEIVED header line when sent from Web Mail.
Show YouTube Previews	Will render YouTube video links in messages so that the videos can be viewed within the message.
Enable Media Player	Enables MP3 media player so that MP3 files can be streamed from within a message attachment or within MyFiles storage files.
Users can import mailboxes	Determines whether the webmail allows users to import email from other sources from within the option pages.
Default Character Set	This is the character set that will be used as the default for web mail users. Users can change this option once they log in under the Settings option page. By default the character set is US-ASCII which does not cater for extended characters. If emails that have been sent from web mail and are missing extended characters or they are displayed incorrectly, it could mean that the user has not set their character set.
Default time zone	This is the time zone that will be used as the default for web mail users. Since the web server is accessible by users throughout the world, the server needs to adjust the displayed date of the messages in a user's folder to properly reflect the time relative to their location. For example, if a user in Australia was using web mail on a server in the United States, they would want to see their inbox list displayed with the received date of the messages in their local time instead of a US time. To do this, the web mail browser sends to the server the time zone offset configured on the client computer. If the client computer does not have the correct time zone configured, they will not see the messages with the correct times.
Site Configuration	If the **Configure…** button is selected the **Site Configuration** screen is displayed. The screen will list all the web sites that are published under IIS. Web mail can then be installed or removed for each of these sites. See the **Publishing via host headers of virtual directories section (Section 6.7.3.2)** for more details.

6.7.2.2 Web Mail - Logging

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





Setting	Explanation
Logging status	The logging status can be set to either 'Disabled', 'Log to Debug log' or "Log to Windows Event log'. The sliding bar sets the level of logging from low to high. Low level logging includes only logins, high level logging includes listing messages, folders, sending, receiving, actions, and retrieval.

Tip: Once Web Mail logging status has been changed it requires an IISRESET for changes to take effect.

6.7.2.3 Web Mail - Advanced

Web mail has

Setting	Explanation
File Upload Size Limit	A limit to the size of attachments can be set.
Service Configuration Screen	Under options in webmail, users can see a page describing the services that are available to them and how to connect to them.
Webmail Anonymous User Sign Up	Enables the anonymous signup page.

6.7.3 Configuring Web Mail

6.7.3.1 Configuring web mail Overview

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

The Host Header option allows web mail to be published through a single IIS web site. When a browser requests

the URL, the host name portion of the URL request is mapped to the IIS web site that is publishing the MailEnable web mail application. This approach means web mail can be accessed through a URL like http://webmail.domainname.

6.7.3.2 Publishing via host headers or virtual directories

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

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

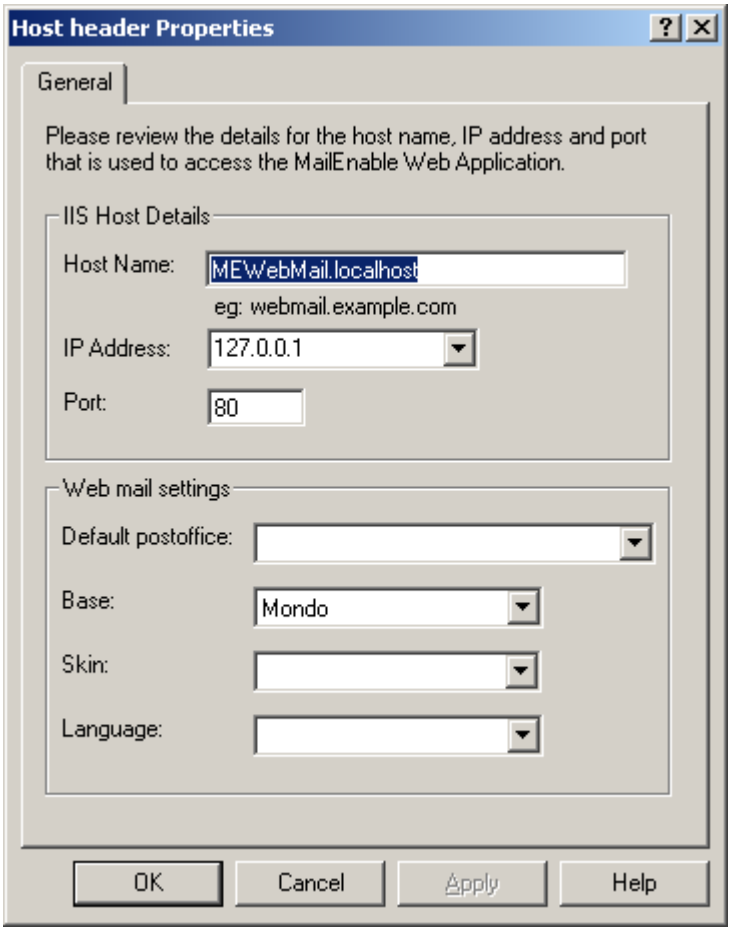
Publishing web mail through host headers

MailEnable Web Applications can be published through host headers through the following branch in the Administration Program: **Servers > localhost > Services > WebMail**

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

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

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



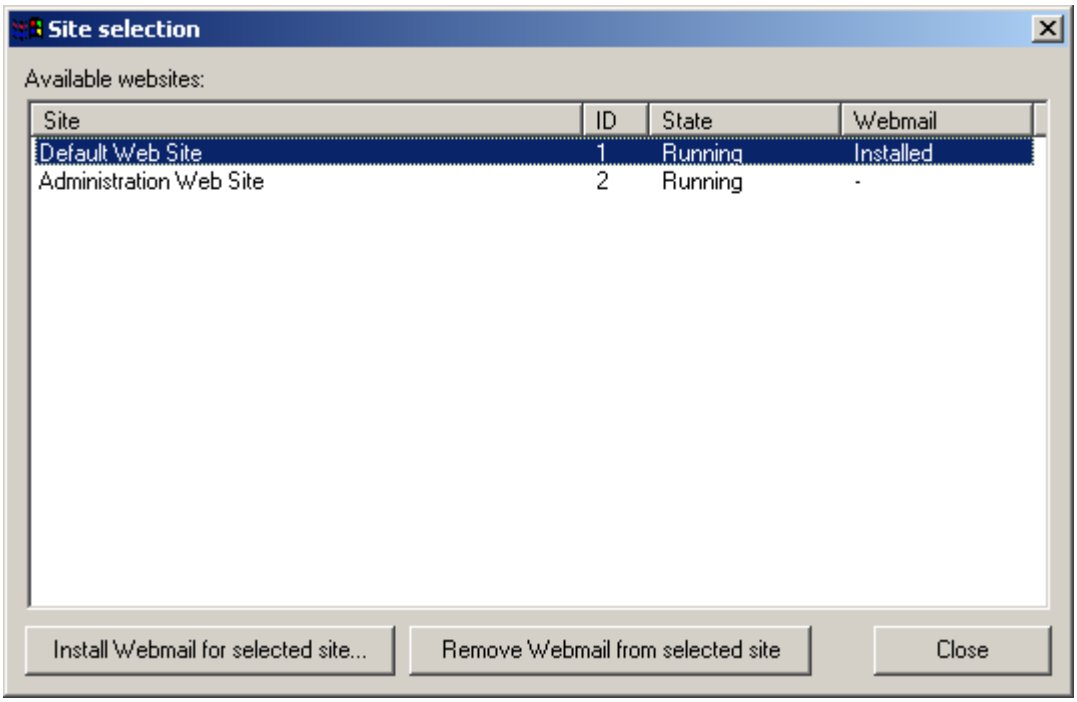
Setting	Description
Host name	The host name is the domain name users type in their web browser to access the web mail. You may wish to give the web mail a URL similar to webmail.example.com. A DNS entry has to be

	created in order to direct users to the IIS server.
IP Address	The address that the host header will be bound to. The DNS entry for the host name has to therefore point to this IP address.
Port	The port that the host header will listen on
Default postoffice	Sets the default postoffice to be used for the web mail host header
Base	Set the base (Professional or Enterprise Edition) for web mail
Skin	Set the skin for the web mail interface
Language	Set the language for the mail interface

Publishing web mail through virtual directories

To allow the Web Web Mail interface to be accessible from other web sites listed within IIS a virtual directory can be created under each of the site. The steps below explain the process involved:

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > localhost > Services > WebMail**
2. Right click on **WebMail** and select properties.
3. Under the **General** tab click on the **Configure** button in the site configuration section.
4. Select a web site within the site configuration window and click on the **Install Webmail for selected site...** button to install the Web Administration virtual directory under the site.



The utility lists all the web sites that are published under IIS. It is then possible to install or remove web mail on each of these sites.Select the web sites to install web mail for by placing a tick in the box next to the site name. Then select the **Install web mail for selected sites** button. Web mail can be removed from web sites by placing a tick in the box next to the site name and selecting the **Remove web mail from selected sites** button.

6.7.4 Browser compatibility

The following is a list of popular desktop browsers that are supported for MailEnable webmail. If you are doing video chat, please use a current version of the web browser. Video chat requires that your browser supports

WebRTC. You can test whether WebRTC is available through the website:

https://test.webrtc.org/

Screen sharing requires Google Chrome browser and a WebRTC plugin.

Browser	Minimum Supported Version
Internet Explorer	10
Microsoft Edge	20
Firefox	40
Safari	10.10
Chrome	40
Opera	10

MailEnable also includes a mobile interface which is designed for devices with a small screen. When logging into webmail the server will automatically detect your device and offer you the mobile version.

7 Configuration of Email Clients

7.1 Configuring Email Clients

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

The username needs to be the full logon name for the mailbox. Remember that this is formatted as mailboxname@postofficename. Email will not be able to be retrieved if the full username is not used, unless a default post office has been specified. See the **General configuration section (Section 5.8)** for more information on specifying a default post office.

7.2 Mail for Windows 10

Mail for Windows 10 supports POP, IMAP and Exchange ActiveSync protocols. To configure Mail for Windows 10 to connect to the mail server:

1. Open Mail
2. Click the **Settings** icon
3. Click **Accounts**
4. Click **Add Account**
5. Select **Advanced Set-up** when prompted to Choose an account
6. Select either **Exchange ActiveSync** or **Internet email**
7. Enter the required server details

7.3 Microsoft Outlook 2000

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

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

7.4 Microsoft Outlook 2002/2003

To configure Microsoft Outlook 2002/2003 to connect to the mail server:

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

7.5 Microsoft Outlook 2007

To configure Microsoft Outlook 2007 to connect to the mail server:

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

7.6 Microsoft Outlook 2010

To Connect Outlook 2010 to the mail server:

1. Click the **Office button** on the top left corner and go to the **Office Backstage**. Under **Info** > **Account Information** > Click **Account Settings** and Click on **Add Account**.
2. On the **Add New Account** screen, just choose **Manually configure server settings or additional server types** and click Next.
3. Choose **Internet E-mail**, connect to **POP** or IMAP server to send and receive e-mail messages and click Next.
4. Here give the User information, enter your Name, your **full email address.**

   Under Server information,

   Account Type – IMAP, POP

   Incoming mail server – exampledomain.com

   Outgoing mail server (SMTP) – exampledomain.com

   Also enter the logon information, enter your user name in full (mailboxname@postofficename) and enter the password.
5. Now go to **Outgoing server tab** and check **My outgoing server (SMTP) requires authentication** and choose Use same settings as my incoming mail server.
6. Click Ok and Finish.

7.7 Microsoft Outlook 2016/2019

To connect Microsoft Outlook 2016/2019 to the mail server:

1. Click the **File** menu item. Under **Info** > **Account Information** > Click **Account Settings** and Click on **Account Settings..** and then click the **New...** button.
2. On the **New Account** screen, just choose **Manually configure server settings or additional server types** and click Next.
3. Choose **Internet E-mail**, connect to **POP** or **IMAP** server to send and receive e-mail messages and click Next.
4. Here give the User information, enter your Name, your **full email address.**

   Under Server information,

   Account Type – IMAP, POP

   Incoming mail server – example.com

   Outgoing mail server (SMTP) – example.com

Also enter the logon information, enter your user name in full (mailboxname@postofficename) and enter the password.

5. Now go to **Outgoing server tab** and check **My outgoing server (SMTP) requires authentication** and choose **Use same settings as my incoming mail server**.
6. Click Ok and Finish.

7.8 Mozilla Thunderbird

To configure for Mozilla Thunderbird:

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

To set the outgoing mail server details:

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

7.9 Enabling logging for Outlook

Microsoft Outlook

To enable logging in Outlook, navigate to the following location: **Tools > Options > Other > Advanced Options > Enable email logging**. After enabling this option you will need to restart Outlook. This will log various information to the following paths:

For POP/IMAP/SMTP:

C:\Users\[user]\AppData\Local\Temp\Outlook Logging\

For Exchange ActiveSync protocol:

C:\Users\[user]\AppData\Local\Temp\EASLogFiles\

8 Operational Procedures

8.1 Backing up and restoring data

MailEnable has a backup utility which is accessible through the **Mail Enable > System Tools** menu. This utility can pass /BACKUP as a parameter to use it as an automated command line backup utility.

There are three main areas where MailEnable stores configuration and user data:

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

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

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

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

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

More information about the backup utility and the various parameters can be found here in the following knowledgebase article: https://www.mailenable.com/kb/Content/Article.asp?ID=ME020024

Information on how to automate backups with the MailEnable backup utility can be found within the following knowledgebase arrticle: https://www.mailenable.com/kb/content/article.asp?ID=ME020114

8.2 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 three logs for the majority of the services. 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.

More information on how to anayle and track messages as they pass through MailEnable can be foudn within the following articles:

https://www.mailenable.com/kb/content/article.asp?ID=ME020170

https://www.mailenable.com/kb/content/article.asp?ID=ME020252

8.3 Manually testing if MailEnable can send mail to remote servers

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

Instructions follow:

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

At the command prompt, enter the following:

telnet mail.mailenable.com 25

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

220 mailenable.com ESMTP MailEnable Service, Version: --10.0 ready at 11/09/22 14:04:45

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

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

nslookup –type=MX aol.com

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

This is outlined as follows:

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

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

   220 mailenable.com ESMTP MailEnable Service, Version: --10.0 ready at 11/09/22 14:04:45
3. Type the following and press Enter: HELO YourDomainName

   The server should reply with a line similar to:

   250 Requested mail action okay, completed
4. Type the following and press Enter. Senderaddress is the email address you are sending from:
5. MAIL FROM:<senderaddress>

   The server should reply with a line similar to:

   250 Requested mail action okay, completed
6. Type the following and press Enter. Recipientaddress is the email address you are sending to:

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

   The server should reply with something like

   354 Start mail input; end with <CRLF>.<CRLF>
8. Enter the text of an email as follows (Note: [CRLF] = Enter Key). The period character on the last line indicates that all the email content has been sent:

   Subject: Test Message[CRLF]

   [CRLF].[CRLF]
9. Type the following and press Enter:

   QUIT

If this was successful, then MailEnable should be able to send messages to the remote host. If an abnormal

response is received for any of the commands typed in, then search the MailEnable Knowledge Base for any articles that may give an indication of the cause of the error.

Example

C:\>telnet mail.mailenable.com 25

220 mailenable.com ESMTP MailEnable Service, Version: --10.0 ready at 11/09/22 23:49:40

EHLO test.mydomain.com.au

250-mailenable.com [192.168.1.1], this server offers 4 extensions

250-AUTH LOGIN CRAM-MD5

250-SIZE 10120000

250-HELP

250 AUTH=LOGIN

MAIL FROM:<senderaddress>

250 Requested mail action okay, completed

RCPT TO:<recipientaddress>

250 Requested mail action okay, completed

DATA

354 Start mail input; end with [CRLF].[CRLF]

Subject: Test Message

250 Requested mail action okay, completed

QUIT

221 Service closing transmission channel

Connection to host lost.

8.4 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:

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.

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.

8.5 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: https://www.mailenable.com/kb/content/article.asp?ID=ME020019

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.

8.6 Performance Counters

Performance Counters are added to the server during install, which allows you to monitor various activities of the mail server. The list of available performance counters and their details are below.

MailEnable List Connector

Counter	Description
Inbound Delivery Count	The number of messages that the list connector has received since the service was started.
Inbound Pickup Count	The number of messages the MTA has processed from the list connector since the MTA service was started.
Inbound Queue Last Poll	The last time the inbound queue was checked in seconds since Jan 1, 1970.
Inbound Queue Length	The number of messages the MTA processed from the list connector inbound queue in the last poll.
Outbound Delivery Count	The number of messages that the list connector has sent since it was started.
Outbound Queue Last Poll	The last time the outbound queue was checked in seconds since since Jan 1, 1970.
Outbound Queue Length	The number of messages the list connector processed from the outbound queue in the last poll.
Outbound Transfer Count	The number of messages the MTA transferred to the list connector outbound queue in the last poll.

MailEnable Message Transfer Agent Filtering

Counter	Description
Antivirus Detections	How many messages have been detected as containing a virus.
Antivirus Total Scans	How many messages have been scanned for viruses.
Bayesian Detections	How many messages the Bayesian filtering rated as greater than 95% probability of spam.
Bayesian Dictionary Current Ham	How many emails classed as good are being used in the Bayesian dictionary.
Bayesian Dictionary Current Spam	How many emails classed as spam are being used in the Bayesian dictionary.
Bayesian Total Scans	How many messages the filtering has checked using Bayesian since it was started.

MailEnable Postoffice Connector

Counter	Description
Inbound Delivery Count	The number of messages that the postoffice connector has received since the service was started.
Inbound Pickup Count	The number of messages the MTA has processed from the postoffice connector since the MTA service was started.
Inbound Queue Last Poll	The last time the inbound queue was checked in seconds since Jan 1, 1970.
Inbound Queue Length	The number of messages the MTA processed from the postoffice connector inbound queue in the last poll.
Outbound Delivery Count	The number of messages that the postoffice connector has delivered since it

	was started.
Outbound Queue Last Poll	The last time the outbound queue was checked in seconds since since Jan 1, 1970.
Outbound Queue Length	The number of messages the postoffice connector processed from the outbound queue in the last poll.
Outbound Transfer Count	The number of messages the MTA transferred to the postoffice connector outbound queue in the last poll.

MailEnable SMTP Connector

Counter	**Description**
Inbound Delivery Count	The number of messages that the postoffice connector has received since the service was started.
Inbound Pickup Count	The number of messages the MTA has processed from the SMTP connector since the MTA service was started.
Inbound Queue Last Poll	The last time the inbound queue was checked in seconds since Jan 1, 1970.
Inbound Queue Length	The number of messages the MTA processed from the SMTP connector inbound queue in the last poll.
Outbound Delivery Count	The number of messages that the SMTP connector has sent since it was started.
Outbound Queue Last Poll	The last time the outbound queue was checked in seconds since since Jan 1, 1970.
Outbound Queue Length	The number of messages the SMTP connector processed from the outbound queue in the last poll.
Outbound Transfer Count	The number of messages the MTA transferred to the SMTP connector outbound queue in the last poll.
Reverse DNS Detections	How many DNS blacklist lookups have returned a result indicating they are listed.
Reverse DNS Tests Performed	How many DNS blacklist lookups have been performed.
XBL Message Detections	How many URL blacklist lookups have returned a result indicating they are listed.
XBL Message Scans	How many URL blacklist lookups have been performed.

9 System Utilities

9.1 Activity Monitor

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

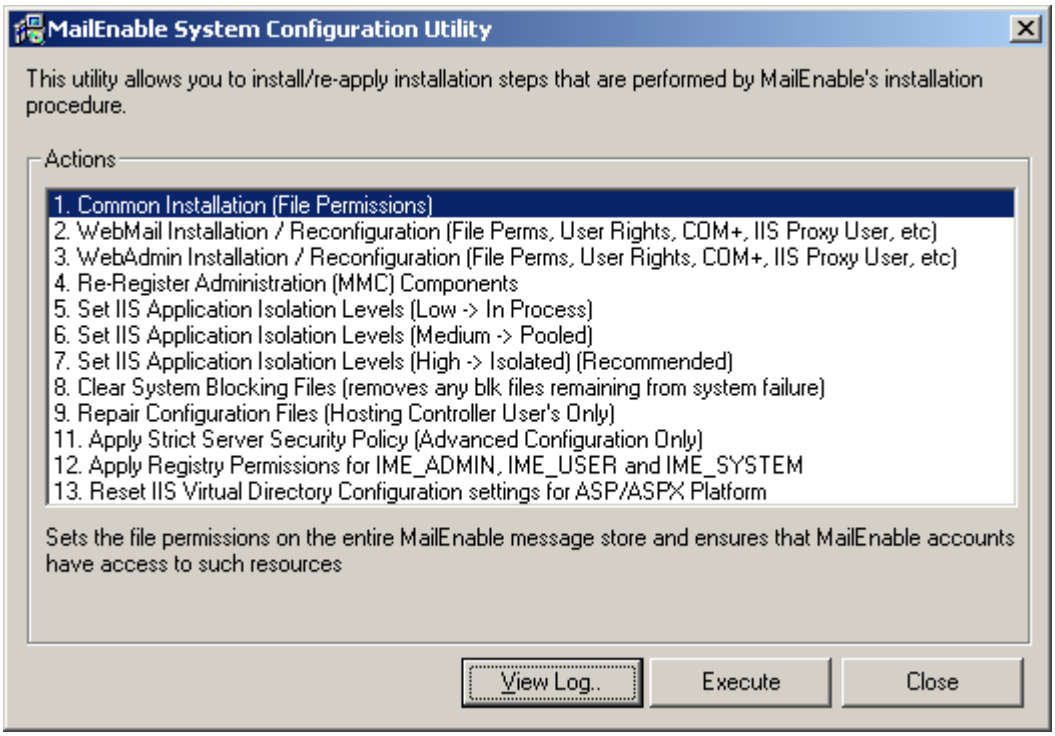
Note: To avoid unnecessary consumption of system resources, this utility should only be run whilst interactively tracking MailEnable system activity.

Note: MailEnable Standard users please download the utility from the following location: http://www.mailenable.com/utilities/addons/meactivitymonitor.zip

9.2 MEInstaller

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

Tip: The meinstaller.exe can also be accessed by opening up a Windows Run command and typing "meinstaller.exe" (without quotes).



The following tasks can be performed:

Common Installation

- Creates the IME_USER Windows user if it does not exist (and adds to Users group)
- Sets the policies for IME_USER
- Creates the IME_ADMIN Windows user if it does not exist (and adds to Users group)
- Sets the policies for IME_ADMIN

- Sets the permissions on the Mail Enable directories for IME_ADMIN
- Sets the permission on required system files for IME_ADMIN and IME_USER

Web Mail Installation

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

WebAdmin Installation (Used for Professional and Enterprise only)

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

Re-Register MMC Components

- Reregisters the MailEnable administration MMC DLLs

Set IIS Application Isolation Levels (Low > In Process)

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

Set IIS Application Isolation Levels (Medium > Pooled)

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

Set IIS Application Isolation Levels (High > Isolated)

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

Clear System Blocking Files

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

Repair Configuration Files (Hosting Controller User's Only)

- Resolves an issue with a specific version of Hosting Controller altering the configuration files.

Apply/Remove Strict Server Security Policy (Used for Professional and Enterprise only)

- Configures the MailEnable services to run under a restricted Windows user, to give a higher level of security on the server.

Apply Registry Permissions for IME_ADMIN, IME_USER and IME_SYSTEM (Used for Professional and Enterprise only)

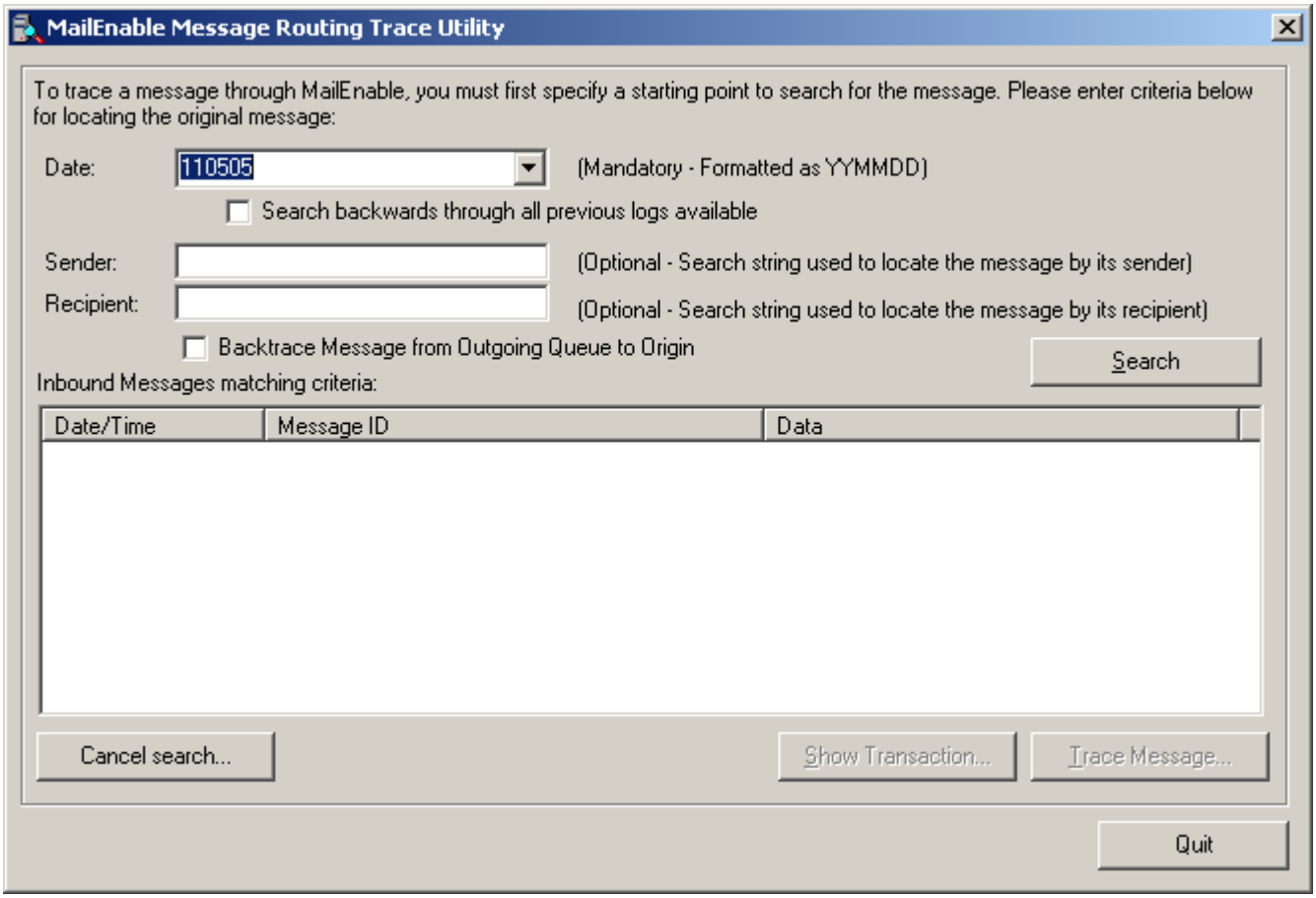
- For webmail and when the strict server policy is applied, the mail services run under various Windows users. This step sets registry permissions required for this.

Reset IIS Virtual Directory Configuration settings for ASP/ASPX Platform

- Resets all the MailEnable webmail and web admin virtual directories to use a specific version of the .Net platform.

9.3 Message Tracking

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



Setting	Description

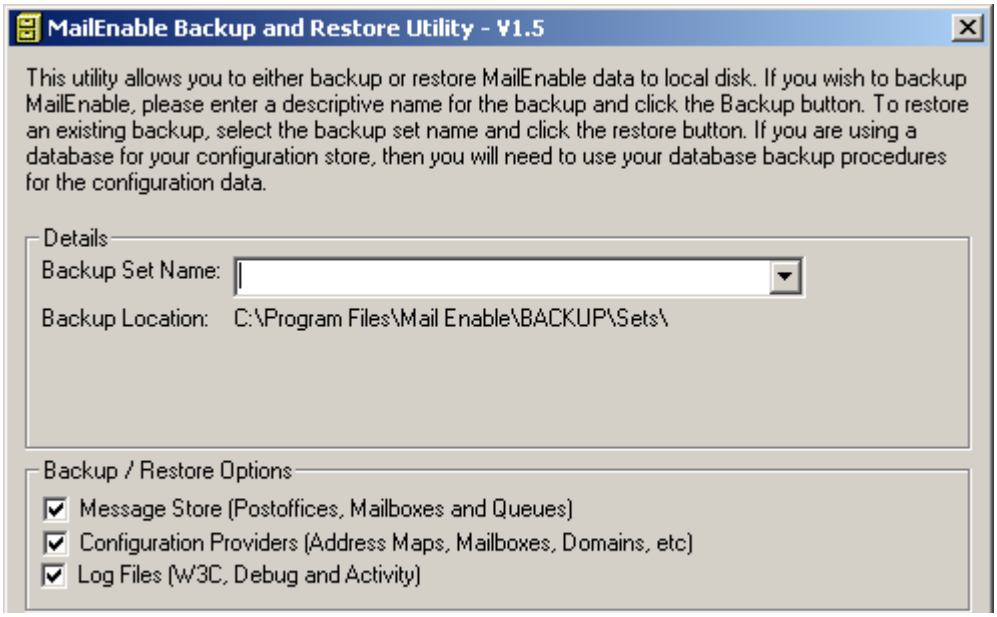
Date (mandatory)	Date is formatted in YYMMDD format (e.g. 5th September 2006 = 060905). Use the dropdown menu to select the respective date **Search backwards through all previous logs available:** When this option is ticked the utility will trace in reverse order. It will first start from the date/time the message was delivered to the recipient mailbox back to when the message was first accepeted by the MailEnable server. Eg: postoffice connector logs > MTA agent logs > SMTP connector logs
Sender (optional)	Enter the sender's email address.
Recipient (optional)	Enter the recipient's email address
Backtrace Message from Outgoing Queue to Origin	When this option is ticked the utility will trace any messages that are sitting in the SMTP outgoing queue back to origin based on the sender or recipient addresses of the message.
Cancel Search...	Cancels the search process
Show Transaction...	Displays the SMTP transaction only
Trace Message...	Will trace through all MailEnable log files from the SMTP transaction to mailbox delivery.

Information on how to track messages as they pass through the MailEnable services can be found within the following knowledgebase article: https://www.mailenable.com/kb/Content/Article.asp?ID=me020252

Note: The MailEnable Message tracking utility is provided within the Professional and Enterprise installation kits. MailEnable standard users will need to manually download the utility from the following link: https://www.mailenable.com/utilities/addons/MEMSGTRK.zip

9.4 Backup utility

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



Setting	Description
Backup	To backup MailEnable, select a descriptive name for the backup and select “Backup”.
Restore	To restore an existing backup, select the back up set name from the drop down box and select “Restore”.
Calculate size	Calculates the maximum storage size required in the backup location to successfully backup the complete configuration.

9.5 Queue overview

The Queue overview lists the number of messages in the outbound SMTP queue by the destination domain name. The utility will interate through the outgoing SMTP queue and create a report of the messages within an internet browser.

Note: Mail Enable Standard users will need to download the utility manually from the following location: https://www.mailenable.com/utilities/addons/MEQueueOverview.zip

10 Developers

10.1 PowerShell

MailEnable's PowerShell interface allows system administrators and developers to manage MailEnable via PowerShell. Administrators can perform typical actions via scripts and can develop and extend these to these commands via scripting. PowerShell significantly improves automation and integrated management of MailEnable.

LAUNCHING POWERSHELL

You can launch PowerShell either by:

1. Selecting Windows PowerShell from the Start screen, or:
2. Selecting Windows PowerShell from the taskbar.

EXECUTING MAILENABLE POWERSHELL COMMANDS

Once PowerShell opens, use the following command to add the MailEnable PowerShell Commands:

Add-PSSnapin MailEnable.Provision.Command

You can then issue specific commands depending on the area of MailEnable you wish to configure. The first command to issue is the Help command. It provides a comprehensive list of the settings that can be manipulated via PowerShell.

Example: PS> Get-MailEnablePlatform -Help "*"

The asterisk tells PowerShell to return all settings.

You can also filter them by simply providing part of the setting name.

Example: PS>Get-MailEnablePlatform -Help "Skin"
SettingId : sysSkinCatalogueEnabled
SettingType : MailEnablePlatform
SettingDataType : dword
SettingControl : 0=Disabled, 1=Enabled
Purpose : Determines whether the Management Console shows an online skin catalogue

The Help command returns the SettingId (the name of the setting), and the SettingType (which is the Command that is used to Set it).

For more information, please refer to the PowerShell reference at: https://www.mailenable.com/developer-resources.asp

11 Appendix

11.1 Accessing web mail for automatic sign-on

Configure MailEnable to automatically login by using the following path syntax:

Syntax:

```
http://server/mondo/lang/sys/login.aspx?
LanguageID=EN&UserID=Account&Password=Password&Method=Auto&skin=mondo
```

Example:

```
http://mail.example.com/mondo/lang/sys/login.aspx?
LanguageID=EN&UserID=MEDemo@Demonstration&Password=demo&Method=Auto&skin=mondo
```

It is possible make this page the startup page or home page within your browser. Also, consider using HTTPS if there is a certificate installed for the web server. This will avoid passwords being sent to the remote host in clear text.

With the examples above the timezone from the client and the server are not applied and as such you may find in some situations that the message list for messages is not correct. This can occur more often when there is a discrepancy due to any day light saving offsets.

To overcome this you can add the following to the URL with the correct time zone:

offset=-600 (remember the separator of &)

Example:
http://mail.example.com/mondo/lang/sys/login.aspx?LanguageID=EN&offset=-600&UserID=MEDemo@Demonstration&Password=demo&Method=Auto&skin=monodo

This will pass a time offset of 10 hours for the client to use against the message header when displaying the list of messages.

11.2 DNS error codes and descriptions

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

9001	DNS server unable to interpret format.
9002	DNS server failure.
9003	DNS name does not exist.
9004	DNS request not supported by name server.
9005	DNS operation refused.
9006	DNS name that should not exist, does exist.
9007	DNS RR set that ought not to exist, does exist.
9008	DNS RR set that ought to exist, does not exist.
9009	DNS server not authoritative for zone.
9010	DNS name in update or prereq is not in zone.
9016	DNS signature failed to verify.

9017	DNS bad key.
9018	DNS signature validity expired.
9501	No records found for given DNS query
9502	Bad DNS packet
9503	No DNS packet 9504: DNS error, check rcode
9505	Unsecured DNS packet
1460	Timeout - This operation returned because the timeout period expired

11.3 Diagnosing Outlook/Outlook Express error codes

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

Error	Service	Description
0x800CCCF4	HTTPMail	Outlook settings may be invalid or a firewall is preventing connection to the remote MailEnable Server.
0x800CCC79	SMTP	SMTP Relay settings are preventing the sending of messages to MailEnable. Ensure that SMTP Authentication is enabled.
0x80042109	SMTP	Outlook is unable to connect to the outgoing (SMTP) e-mail server.
0x8004210A	POP	The operation timed out waiting for a response from the receiving (POP) server. Establish whether it is possible to telnet to port 110 of the mail server.
0x800CCC0F	POP	The mail client is unable to contact the MailEnable Server, most likely because a firewall is preventing access or the supplied IP Address is incorrect.
0x8004210B	POP	Verify that the service pack for Microsoft Office XP is installed.
0x800CCC0D	POP	Verify that the mail client is configured correctly. Either specify an IP address or a host name as the mail server when configuring the mail client settings. If using a host name then it must be defined in the DNS as a Host record.
0X800CCC0E	SMTP	This error means that the mail client is connecting to the server via POP, but the SMTP Service is either not running or is configured incorrectly. Verify if the SMTP service is running by using the telnet utility to telnet to port 25 of the mail server. If the server responds, then the issue is most likely that mail client settings are invalid.

11.4 Manually testing if MailEnable can send mail to remote servers

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

Instructions follow:

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

At the command prompt, enter the following:

telnet mail.mailenable.com 25

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

220 mailenable.com ESMTP MailEnable Service, Version: --10.0 ready at 11/09/22 14:04:45

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

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

nslookup –type=MX aol.com

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

This is outlined as follows:

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

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

   220 mailenable.com ESMTP MailEnable Service, Version: --10.0 ready at 11/09/22 14:04:45
3. Type the following and press Enter: HELO YourDomainName

   The server should reply with a line similar to:

   250 Requested mail action okay, completed
4. Type the following and press Enter. Senderaddress is the email address you are sending from:
5. MAIL FROM:<senderaddress>

   The server should reply with a line similar to:

   250 Requested mail action okay, completed
6. Type the following and press Enter. Recipientaddress is the email address you are sending to:

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

   The server should reply with something like

   354 Start mail input; end with <CRLF>.<CRLF>
8. Enter the text of an email as follows (Note: [CRLF] = Enter Key). The period character on the last line indicates that all the email content has been sent:

   Subject: Test Message[CRLF]

   [CRLF].[CRLF]
9. Type the following and press Enter:

   QUIT

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

Example

C:\>telnet mail.mailenable.com 25

220 mailenable.com ESMTP MailEnable Service, Version: --10.0 ready at 11/09/22 23:49:40

EHLO test.mydomain.com.au

250-mailenable.com [192.168.1.1], this server offers 4 extensions

250-AUTH LOGIN CRAM-MD5

250-SIZE 10120000

250-HELP

250 AUTH=LOGIN

MAIL FROM:<senderaddress>

250 Requested mail action okay, completed

RCPT TO:<recipientaddress>

250 Requested mail action okay, completed

DATA

354 Start mail input; end with [CRLF].[CRLF]

Subject: Test Message

250 Requested mail action okay, completed

QUIT

221 Service closing transmission channel

Connection to host lost.

11.5 Log analyser

The log analyser is a useful tool that is installed with MailEnable. It simplifies analysis of the server logs and provides an overview of any errors and displays causes and fixes for these. The log analyser retrieves the latest help information from the MailEnable website.

Run the log analyzer by accessing the **Start > Program Files > Mail Enable > System Tools > Log Analyzer** menu. The various log files in the log path are displayed to the left. To view events in a log, click the filename. The program will scan the file for all the events and display these in the top right section. Select the item for more information concerning the event, along with a display of the instance in the log. Select the **More Information** button to be taken to the MailEnable website for further details.

To match up the item in the debug log with the actual data conversation between the MailEnable server and the remote application, select the instance item. It may take a few moments to scan through the activity log to find the match, depending on how large the log files are.

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

11.6 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: https://www.mailenable.com/kb/content/article.asp?ID=ME020019

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

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

11.7 Increasing 10000kb upload limit for Webmail

Uploading attachments larger than 10000KB fails through web mail.

CAUSE

HTTP runtime size limit restriction within the web.config file.

RESOLUTION

Navigate to the following location in the MailEnable .NET folder:

C:\Program Files\MailEnable\BIN\NETwebmail\

Locate the file "web.config" and open it up in Notepad. Locate the following line in the file:

<httpRuntime maxRequestLength="10240" executionTimeout="3600" />

The value that needs to be changed is: httpRuntime maxRequestLength="10240". Change the value to a size bigger to the file that is failing the uploading in web mail.

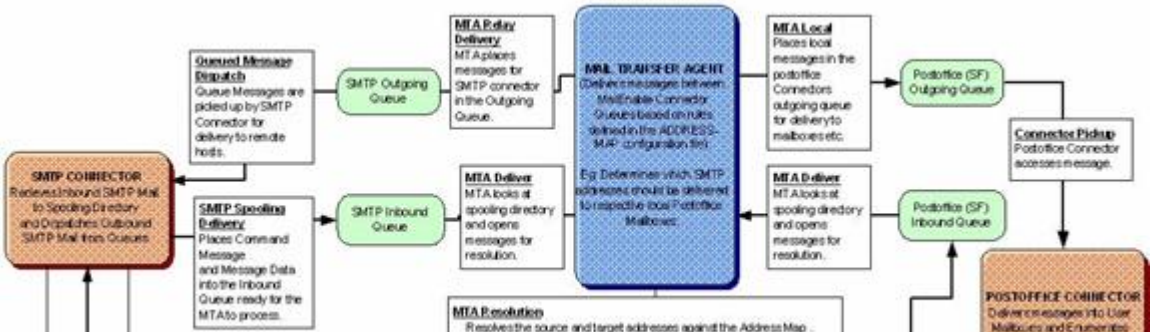
MORE INFORMATION

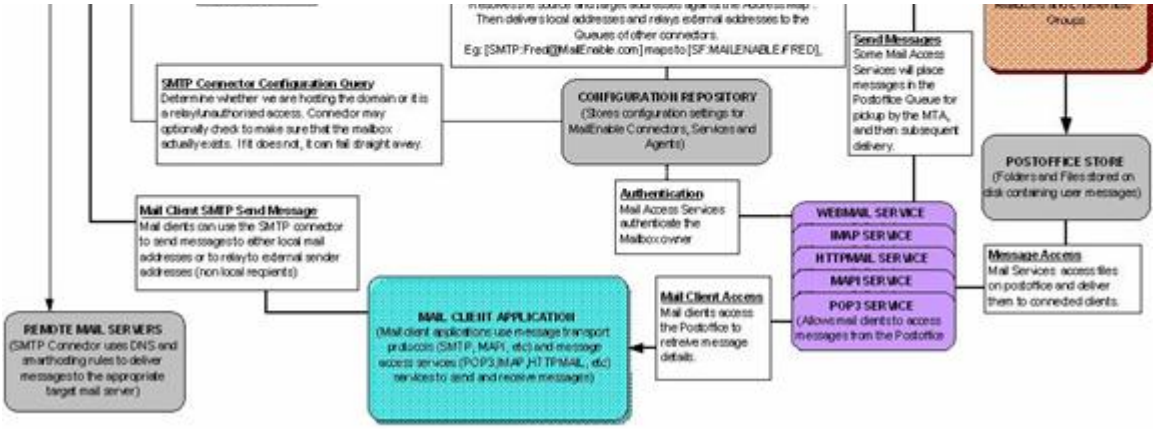
If changing the value within the MailEnable "web.config" file does not resolve the uploading failure, then the next step would be to inspect the following Microsoft Knowledge Base article that explains various situations and hardware limits that can impact on .ASPX uploading.

http://support.microsoft.com/default.aspx?scid=kb;en-us;323245

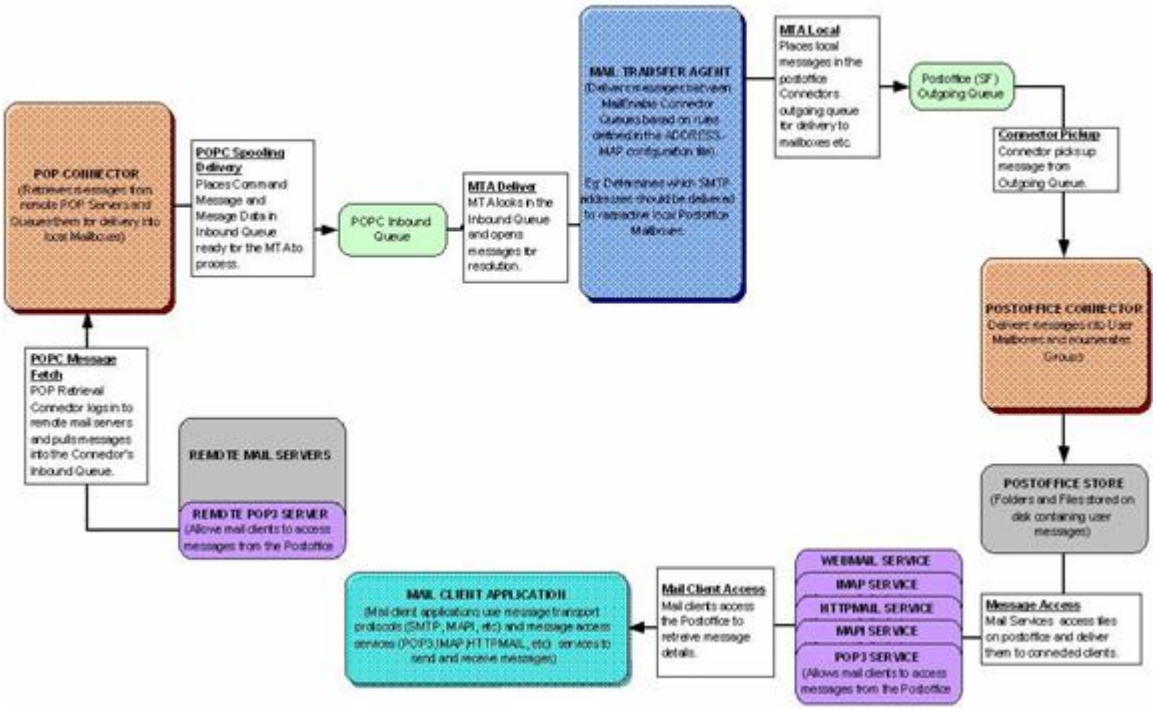
11.8 Logical architecture and message flow

The diagram below outlines the core functionality of MailEnable and how its respective modules (Connectors, Services and Agents) interact. For simplicity, the diagram does not outline the functions of the POP retrieval Connector or List Server Connector.

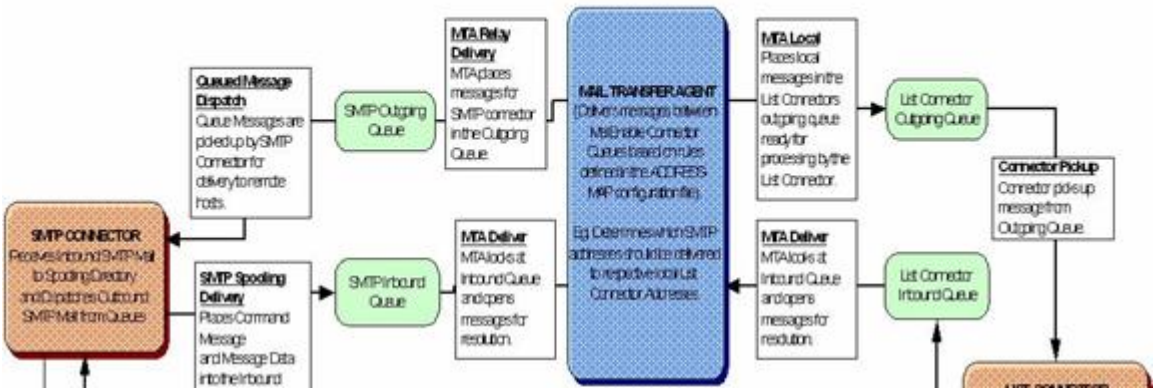


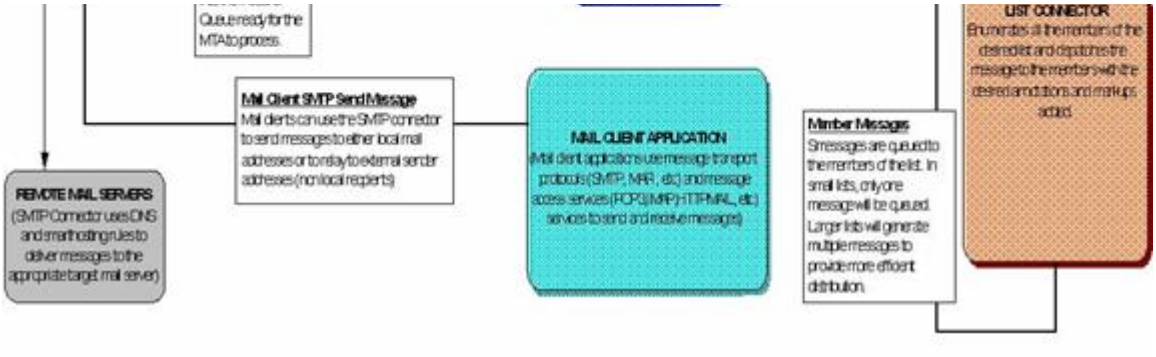


The following diagram provides a high level overview the POP Connector:



The List server connector is responsible for dispatching messages to large lists of mail addresses. The list server connector will allow members to subscribe to a list, enforce publishing rules for the list, add headers and footers to messages published via the list, etc.




Queue ready for the MTA to process
Mail Client SMTP Send Message
Mail clients can use the SMTP connector to send messages to either local mail addresses or to relay to external sender addresses (non local recipients)
MAIL CLIENT APPLICATION
Mail client applications use message transport protocols (SMTP, MAPI, etc) and message access services (POP3, IMAP, HTTP-MAIL, etc) services to send and receive messages
REMOTE MAIL SERVERS
(SMTP Connector uses DNS and smart hosting rules to deliver messages to the appropriate target mail server)
Member Messages
Messages are queued to the members of the list. In small lists, only one message will be queued. Larger lists will generate multiple messages to provide more efficient distribution.
LIST CONNECTOR
Enumerates all the members of the distribution list and copies the message to the members with the desired conditions and markups added.

12 Glossary

A

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.

C

Connector
Connectors facilitate moving mail between systems or subsystems (whether they are local or remote).

D

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.

G

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.

I

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.

L

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.

M

Mailbox
A mailbox is a repository for email. It used to store emails for one or more email addresses. When a user connects with a mail client application (Outlook Express, Eudora, etc.), they connect to a mailbox to retrieve their email.

MTA
Mail Transfer Agent. A Windows Service that exchanges internal messages between MailEnable Connectors.

P

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.

R

Recipient
The address to where the email is destined.

S

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.

13 Warranty

You should carefully read the following terms and conditions before using this software. Unless you have a different license agreement signed by the respective owners, authors and copyright holders of the MailEnable product suite, herewith referred to as ("ME"), your use, distribution, or installation of this copy of MailEnable indicates your acceptance of this License.

All rights of any kind in MailEnable which are not expressly granted in this License are entirely and exclusively reserved to and by "ME". You may not rent, lease, modify, reverse engineer, translate, decompile and disassemble MailEnable without the permission of its owners, authors and copyright holders of MailEnable.

You are not permitted to commercialize derivative works of MailEnable without a written agreement signed by the respective owners, authors and copyright holders of MailEnable.

All accompanying files, data and materials, are distributed "as is" and with no warranties of any kind, whether express or implied.

This disclaimer of warranty constitutes an essential part of the agreement. Any liability of "ME" will be limited exclusively to refund of purchase price. In no event shall "ME", including but not limited to its principals, shareholders, officers, employees, affiliates, contractors, subsidiaries, or parent organizations, be liable for any incidental, consequential, or punitive damages whatsoever relating to the use of MailEnable, or your relationship with "ME".

In addition, in no event does "ME" authorize you to use MailEnable in applications or systems where "ME"'s failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use by you is entirely at your own risk, and you agree to hold "ME" harmless from any claims or losses relating to such unauthorized use.

You are specifically prohibited from charging, or requesting donations, for any copies, however made, and from distributing such copies with other products of any kind, commercial or otherwise, without prior written permission from "ME". "ME" reserves the right to revoke the above distribution rights at any time, for any or no reason.

14 Index