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) • 680MB for ClamAV
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

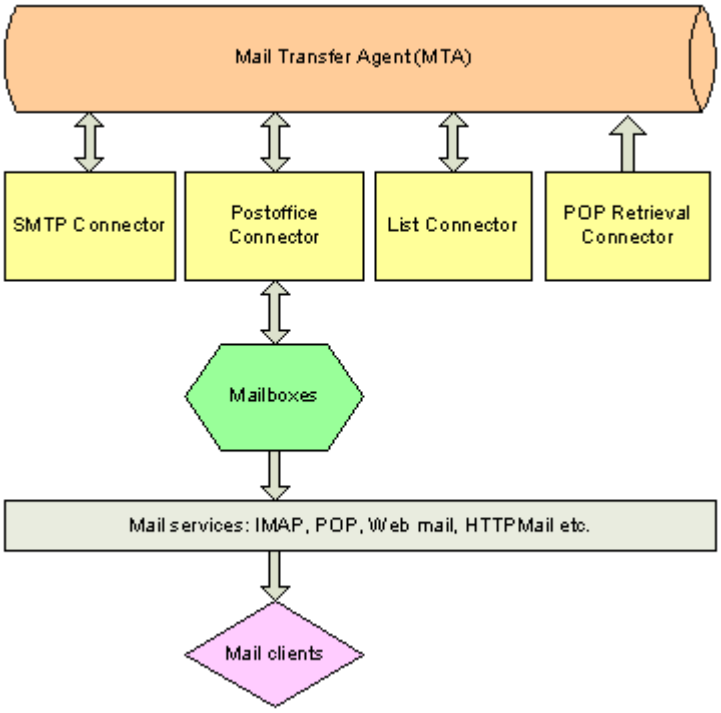
MailEnable has multiple services that interact in order to deliver a message to a mailbox. This interaction is done by a system of queues, which are used to move the emails around. The actual moving of the messages is done by the MTA service, which is logically the central service to the whole MailEnable 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
- Synchronization (HTTP Mail)
- Web mail
- Mobile 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.

POP Retrieval connector

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

Agents

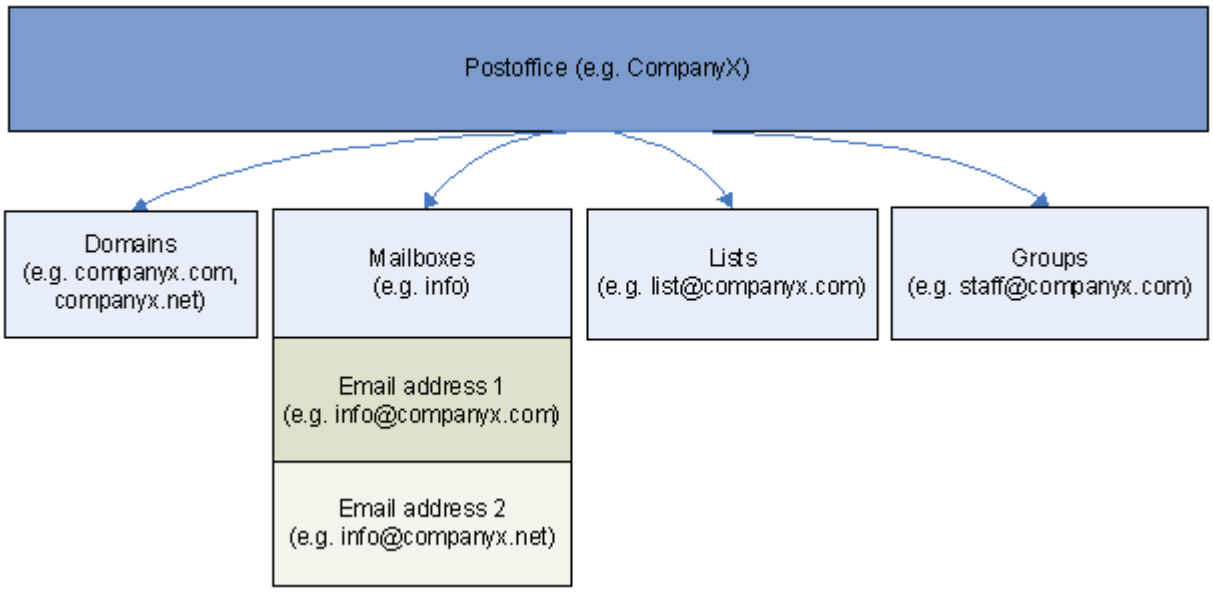
Mail Transfer Agent (MTA)

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.

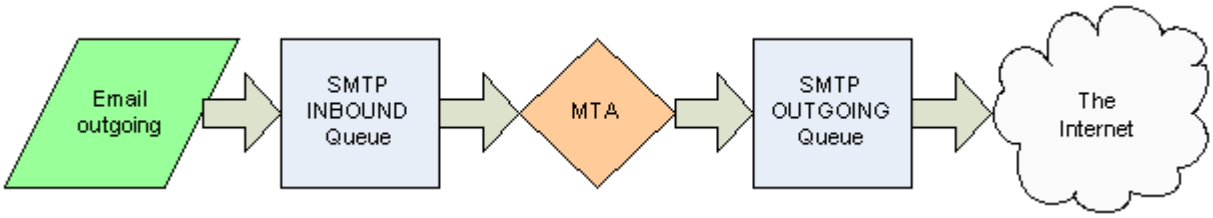
Groups

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.

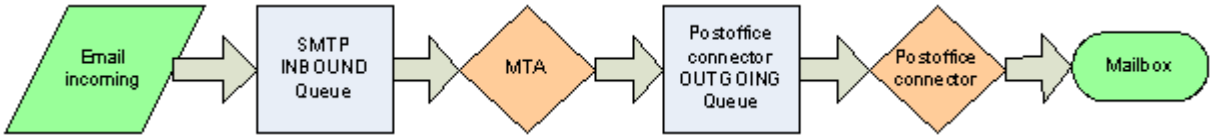


Requiring users to authenticate against the server prior to sending email can stop spammers from using the mail server to send email out to anyone.

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.

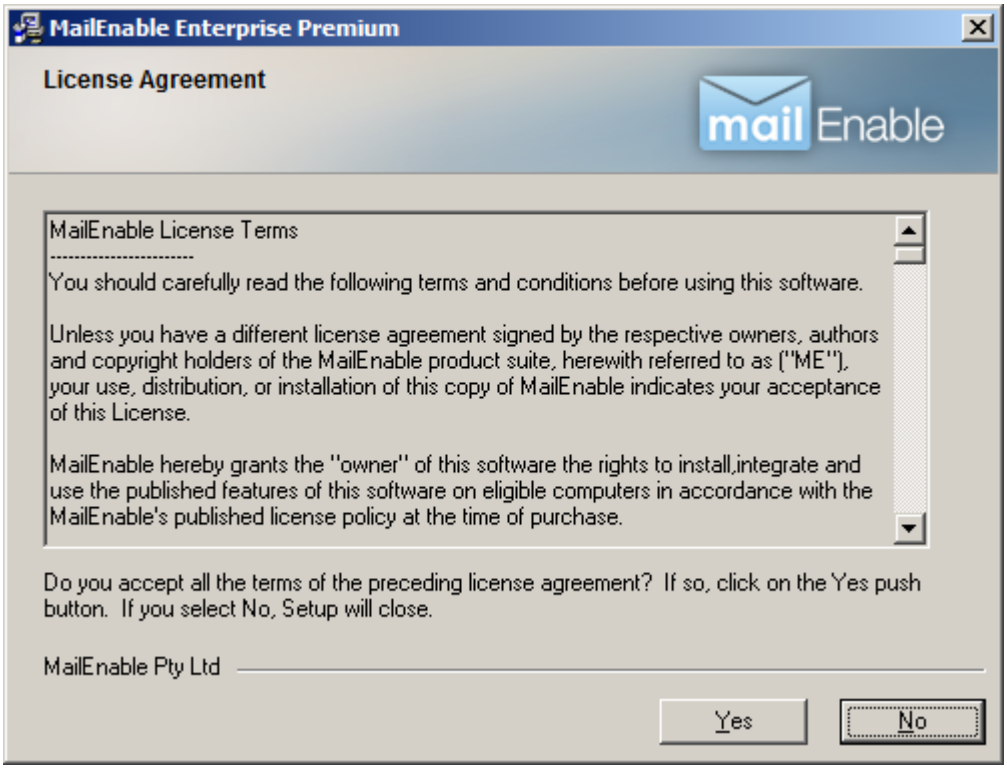
Please click the Next button to continue.

License Agreement

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

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

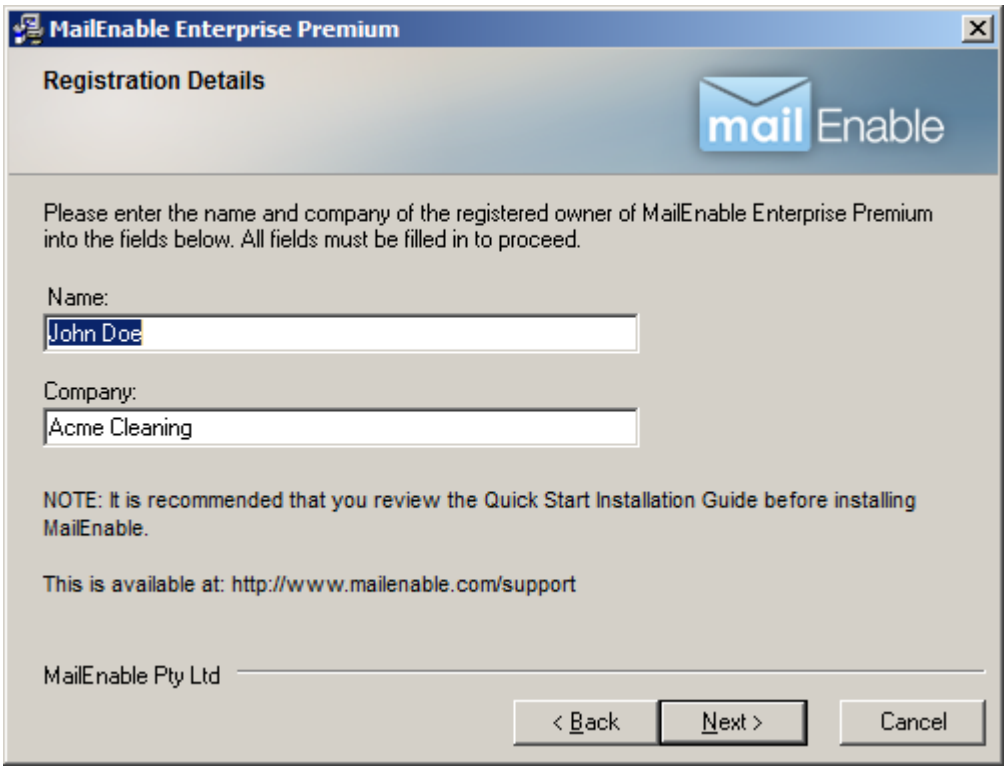
Please click the Yes button to continue.



Registration details

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

Please click the Next button to continue.



Select installation components

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

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

Information Services (IIS) is installed.

Mobile Web Mail Service (Server) - This will install the Mobile web mail interface. This option requires Microsoft Internet Information Services (IIS) is installed and Microsoft ASP.NET 3.5 framework.

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

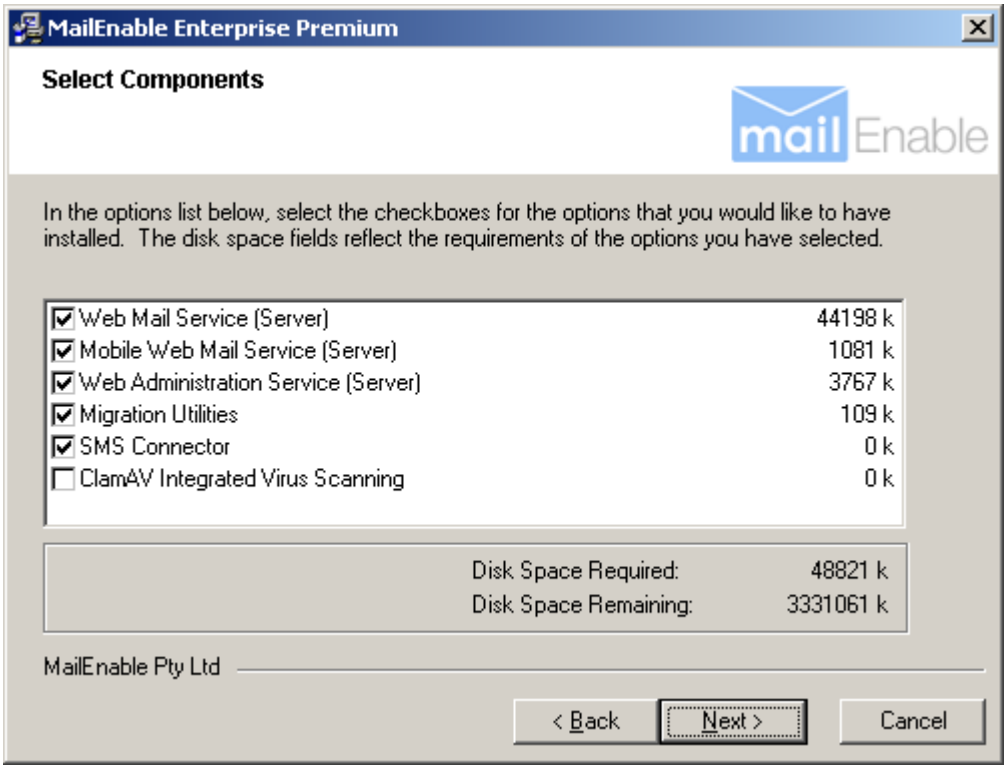
Migration Utilities - Will install the Capture Migration Utility used to migrate accounts and messages from remote servers.

SMS connector - Will install the SMS service.

ClamAV Integrated Virus Scanning - Will install the ClamAV Antivirus application for scanning incoming and outgoing messages and automatically setup the relevant filtering options. Please see **Antivirus Filtering (Section 9.8.1)** for more information about ClamAV Integrated Virus Scanning.

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

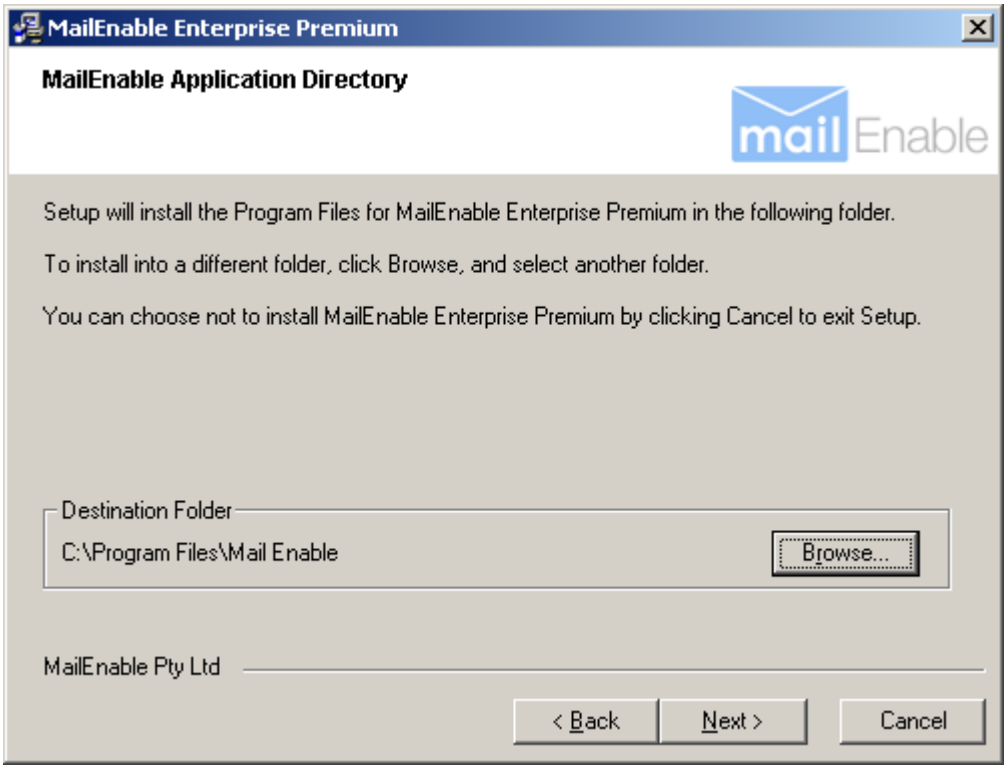
Please click the Next button to continue.



Select application directory

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

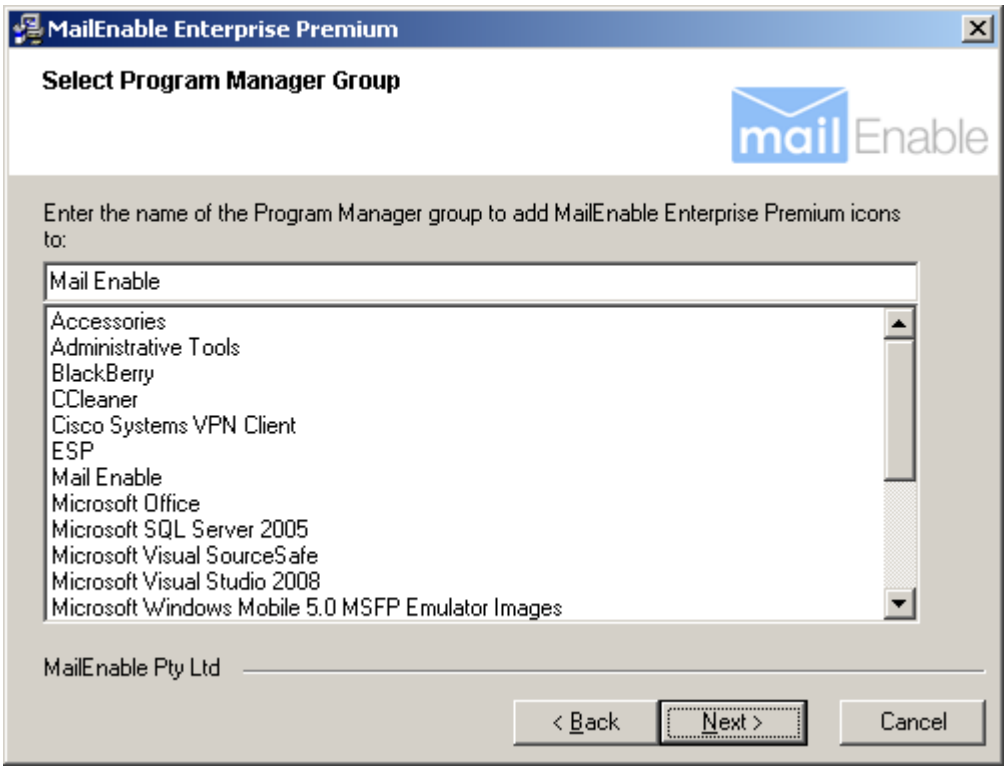
Please click the Next button to continue.



Select Program Manager group

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

Please click the Next button to continue.



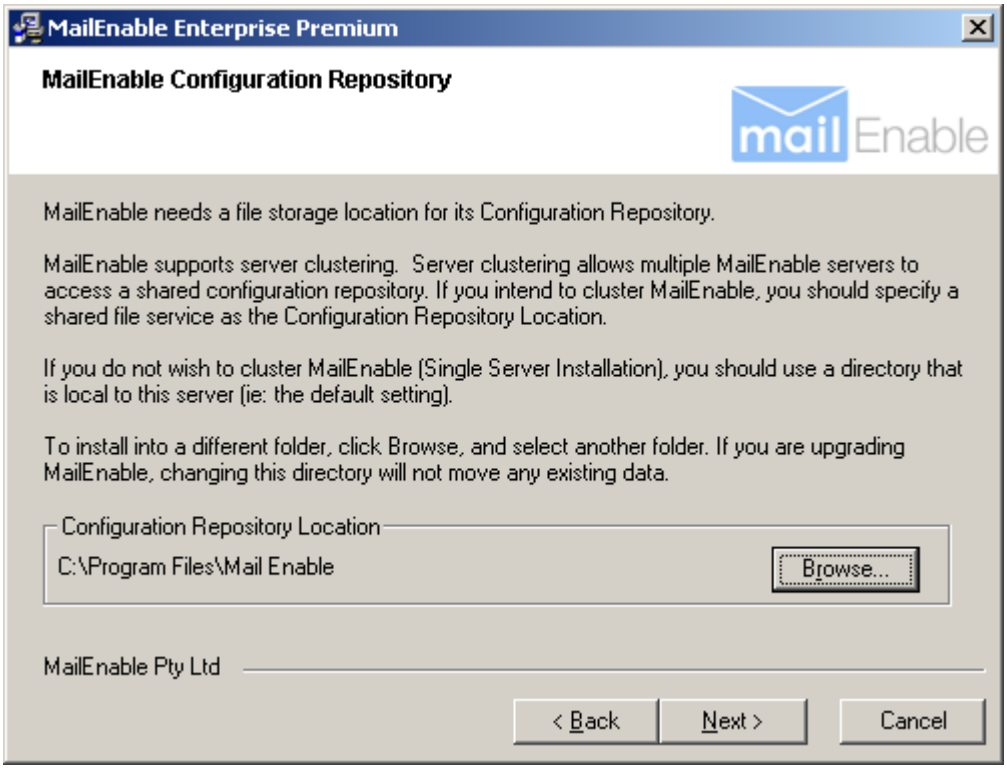
The Configuration Repository is a place to store the configuration files of MailEnable. By default MailEnable uses a TAB Delimited file structure (flat file structure), and since the configuration files are accessed continually, consider using a fast disk I/O sub system for this storage path to improve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

If intending to cluster MailEnable, specify a shared file services as the Configuration Repository location. If the

installation is only on a single server, use a directory that is local to that server (i.e. the default setting).

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

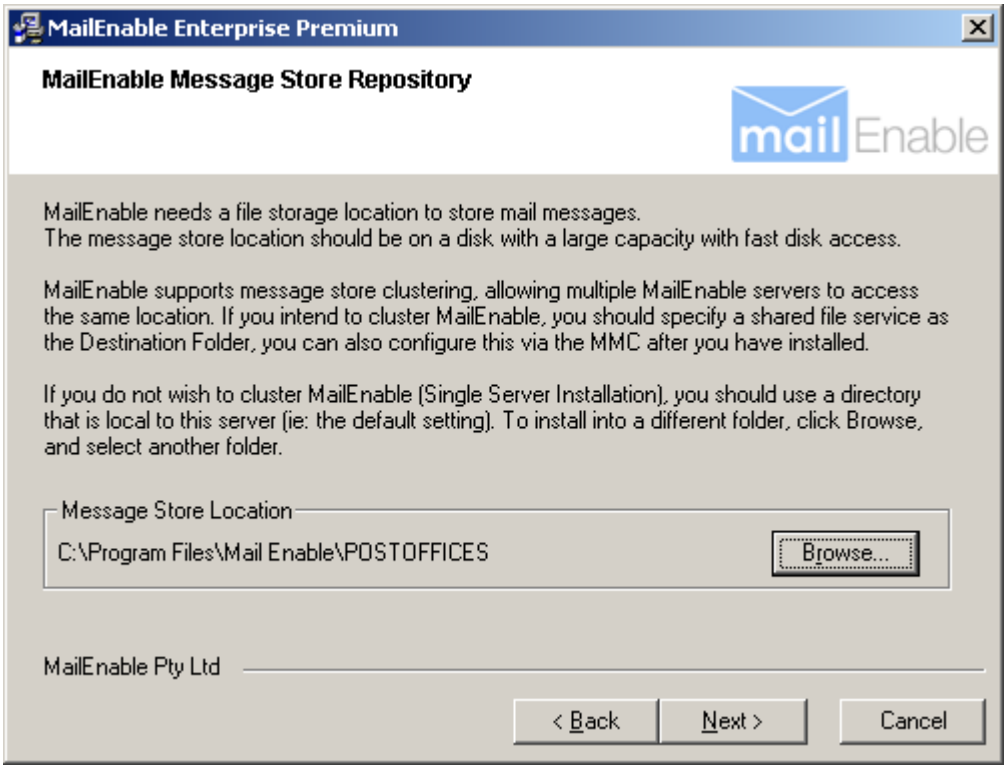
Please click the Next button to continue.



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

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

Please click the Next button to continue.

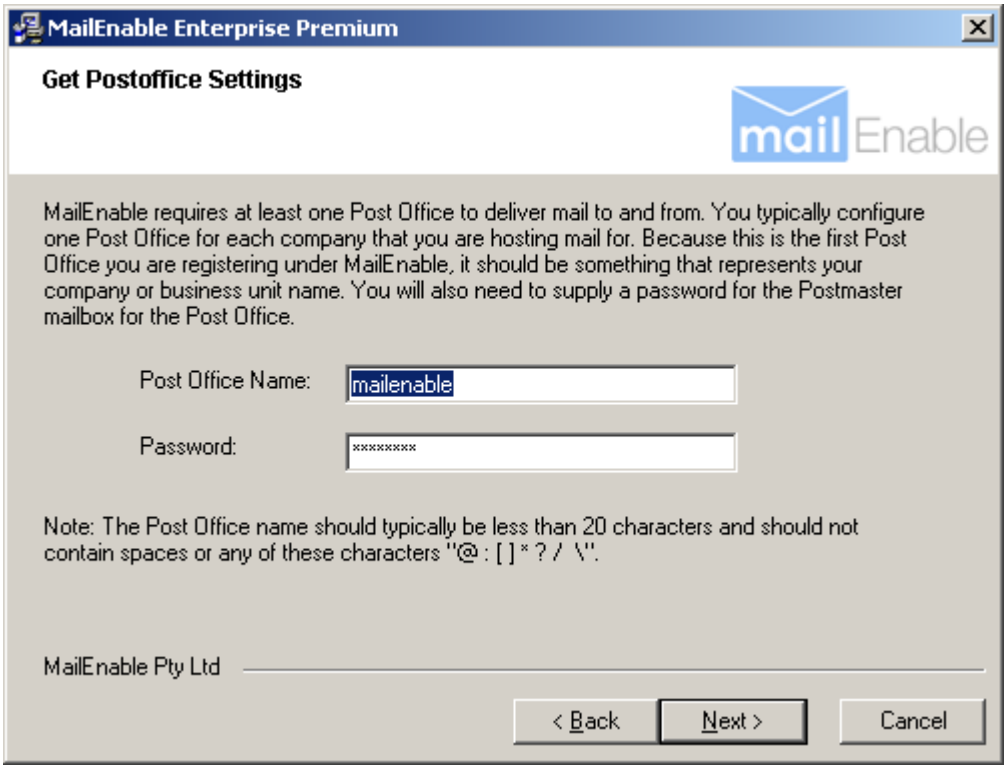


Creating an initial post office

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

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

Please click the Next button to continue.

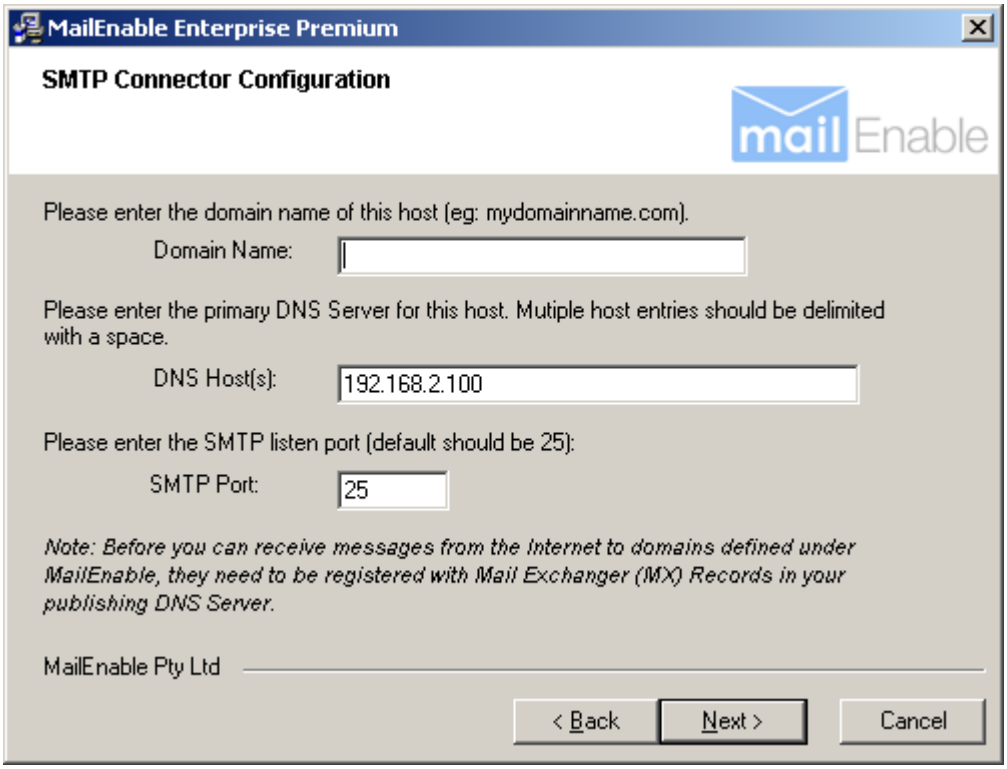


SMTP connector configuration

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

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

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.



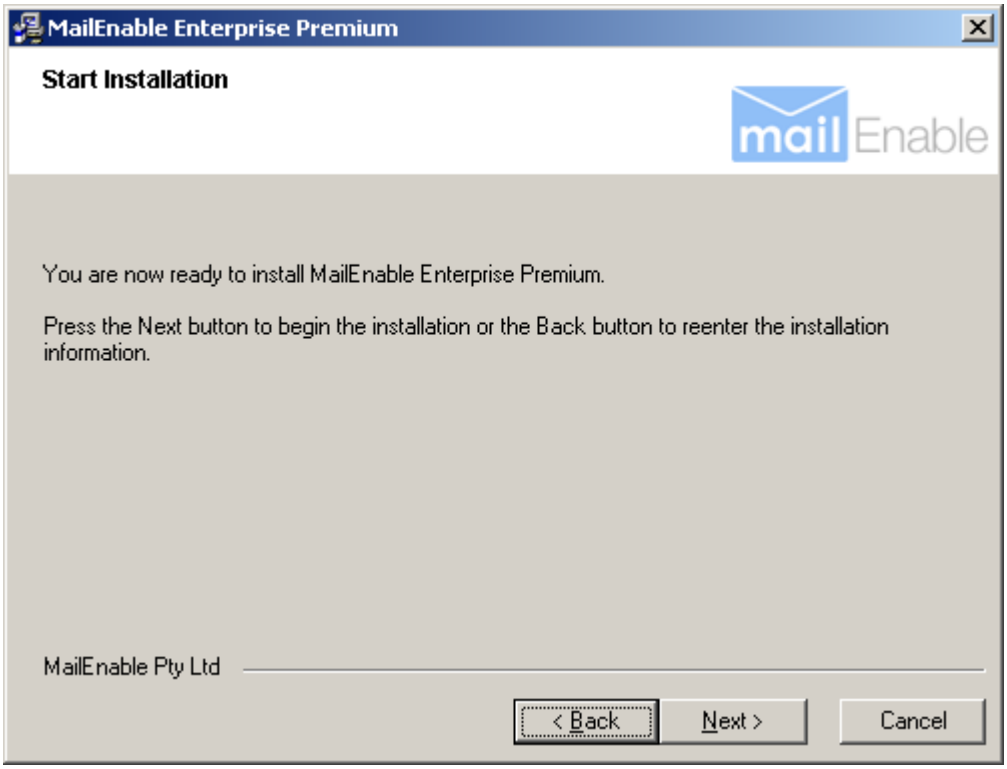
Please click the Next button to continue.

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.



Database schema warning

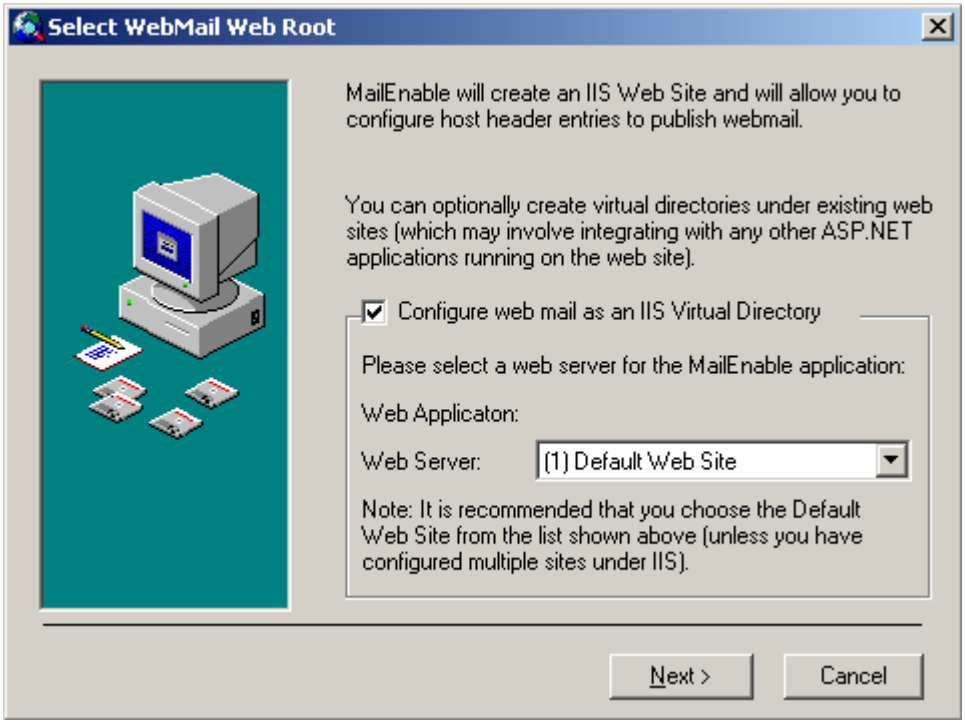
If MailEnable is being upgraded from a previous version, a warning will be shown that the database schemas for the configuration storage need to be updated. If a database is being used to store configuration information the Provider Migration Utility will need to be used (see the **Using MySQL or Microsoft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

Please click the OK button to continue.

Select web mail site

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

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



Please click the Next button to continue.

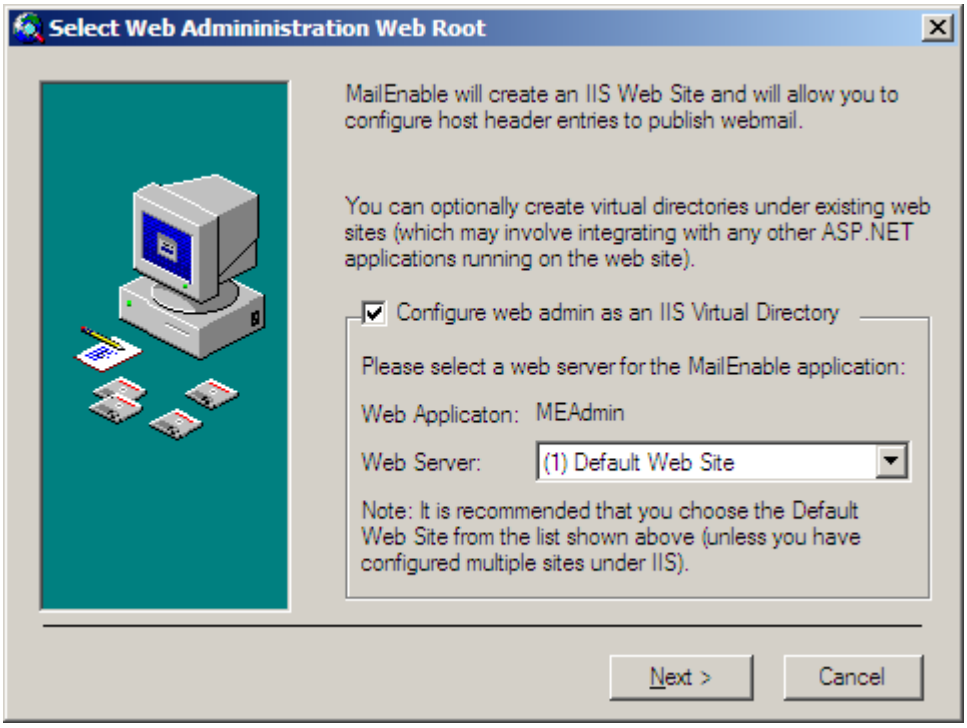
The installation application will display a dialog box while it configures web mail. The configuration of web mail may take several minutes, so please be patient.

Select web administration site

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

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

Please click the Next button to continue.



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

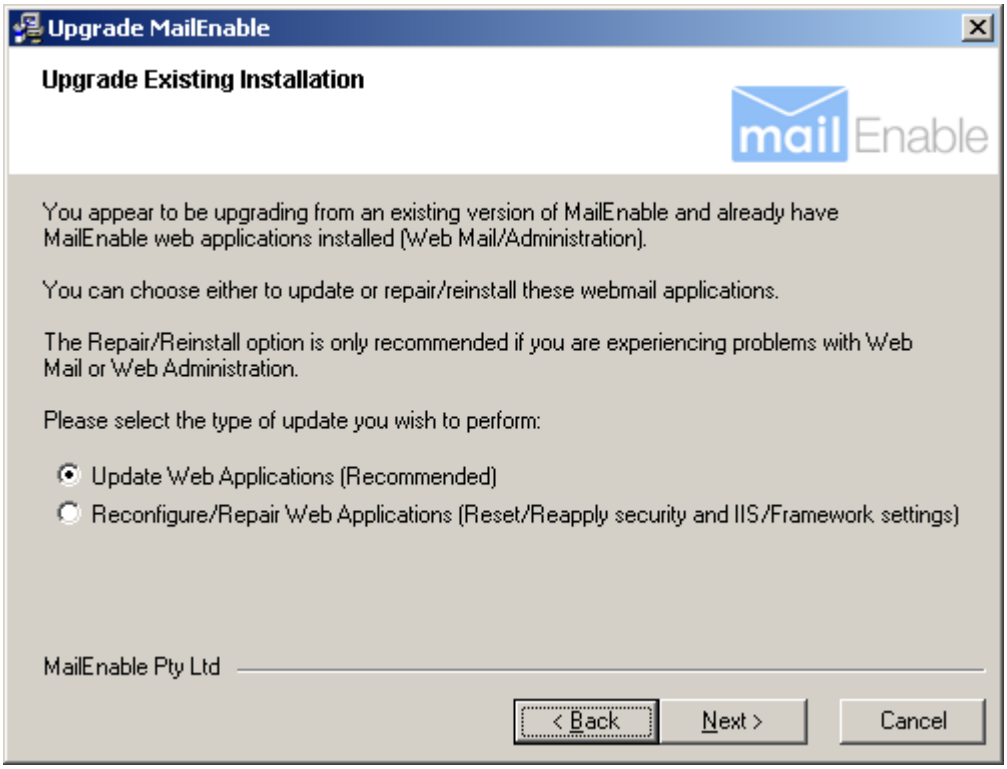
To upgrade to MailEnable Enterprise Premium from either Standard Edition, Professional, Enterprise or earlier version of Enterprise Premium editions, follow the same steps as outlined in the **Installation and upgrading section (Section 4.1)**. As the same data stores are used, it is possible to run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

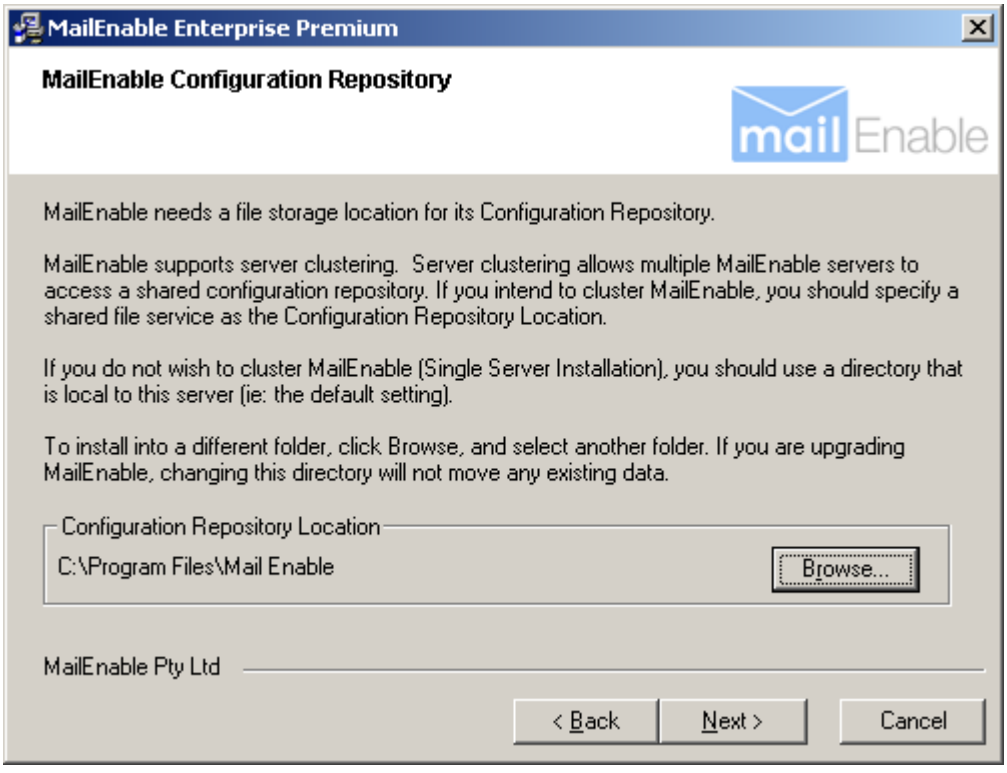
4.3.2 Upgrading an existing web mail installation

If upgrading an existing version of MailEnable the installer will detect and provide upgrade options for the Web Mail interface. Selecting **Upgrade** will improve installation times and upgrade the necessary Web Mail files that contain fixes and updates. The alternative option is to perform a **Repair/Reinstall** where the installer will proceed to reset Web Mail IIS components, ASP.NET script mappings and apply the respective permission settings for Web Mail. The Repair/Reinstall option is only recommended if you are experiencing problems with the Web Mail or Web Administration interfaces.



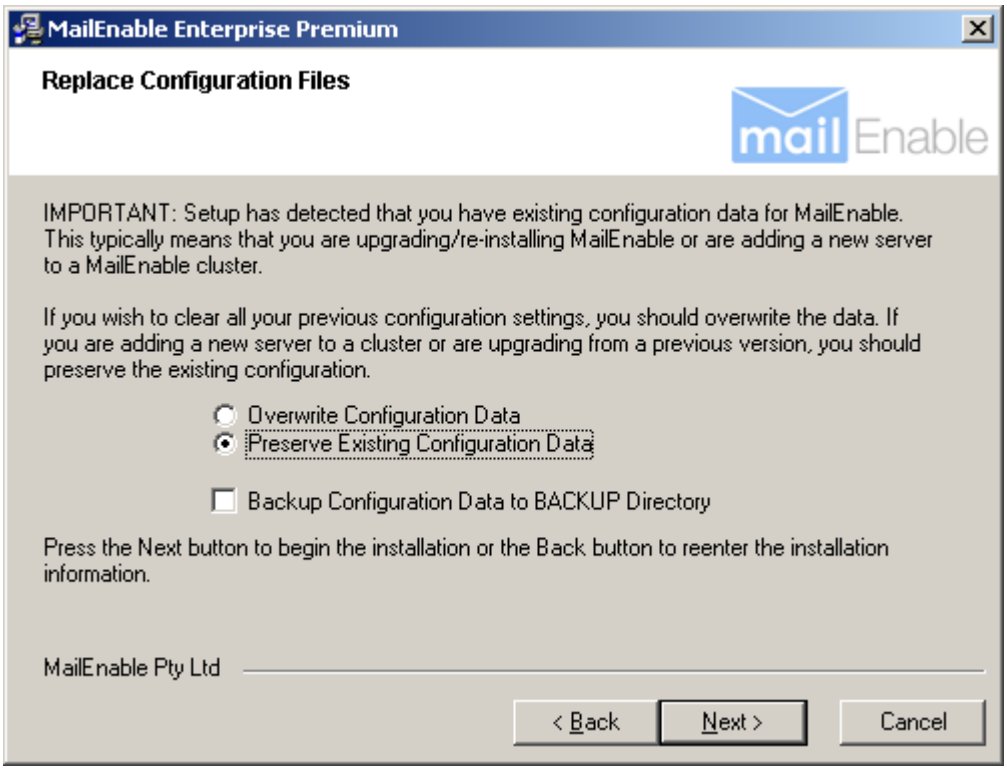
4.3.3 Configuration repository location

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.



4.3.4 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.

Note: MailEnable Enterprise by default uses the same configuration data and options as Standard and Professional, but has two-way migration wizards for changing the configuration provider (i.e. you are able to migrate data back and forth between the default TAB delimited configuration files and the database). See the **Migrating data between providers section (Section 7.3)** for more information.

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 6.14.5)**.
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

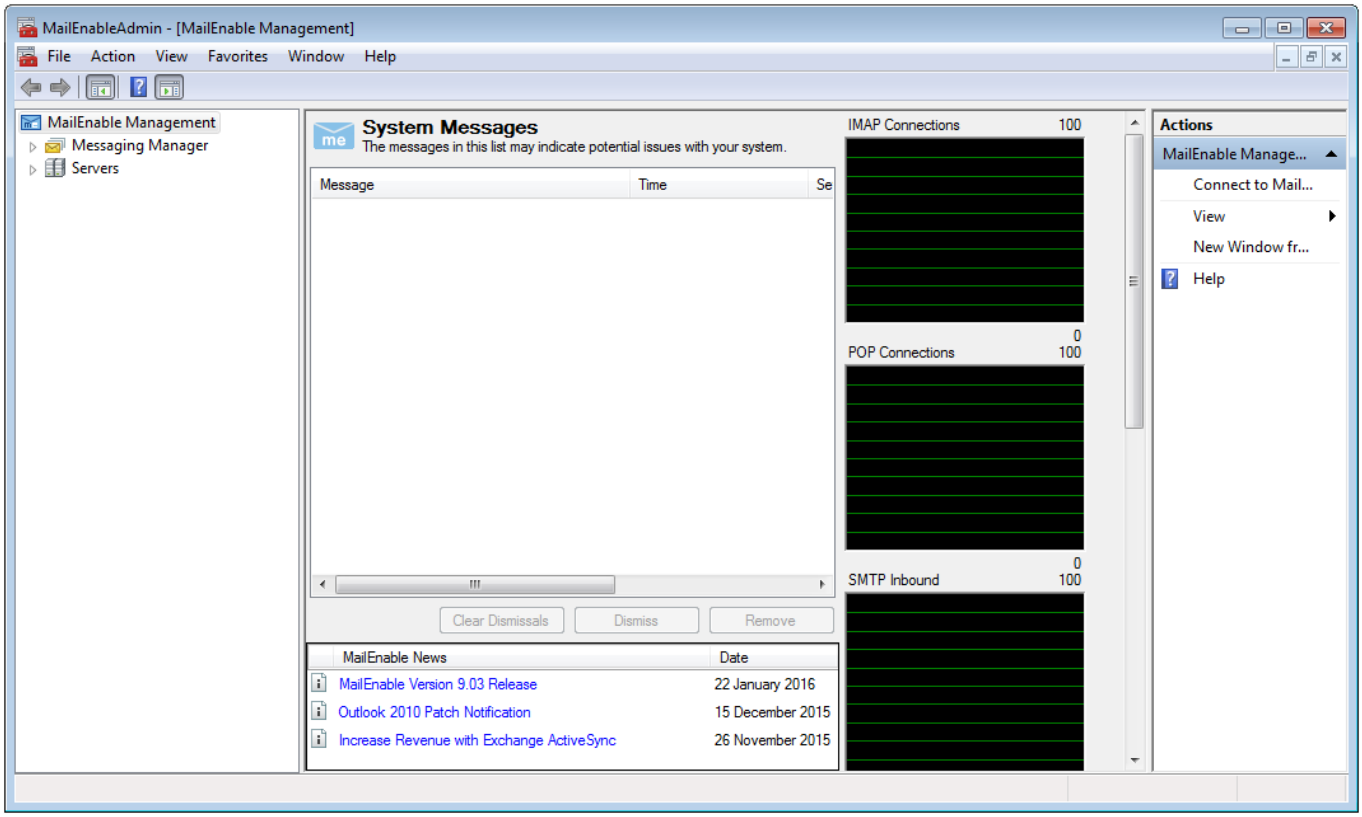
5.1 Administration

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 Enterprise

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



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

The first item in the display is **MailEnable Management**. By right clicking on this icon and selecting properties you will see the following options:, the option to “Connect to a MailEnable cluster” is available. This section only describes how to configure a single server installation, refer to the **Cluster management section (Section 10.1)** for information covering multiple server configuration.

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

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

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

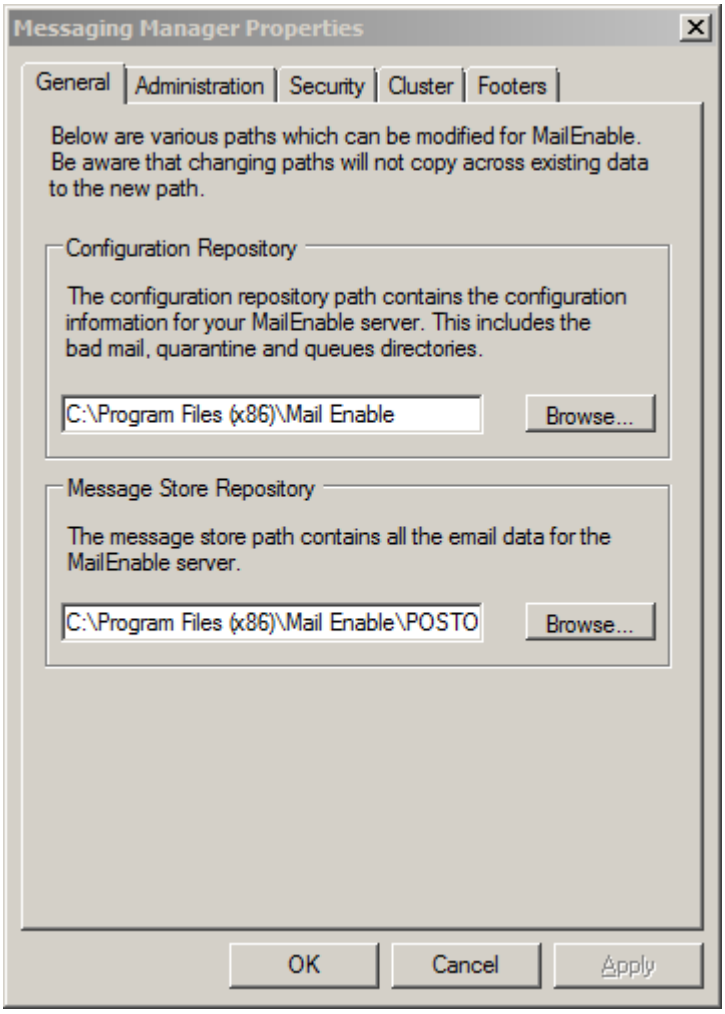
5.2 Messaging Manager

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.

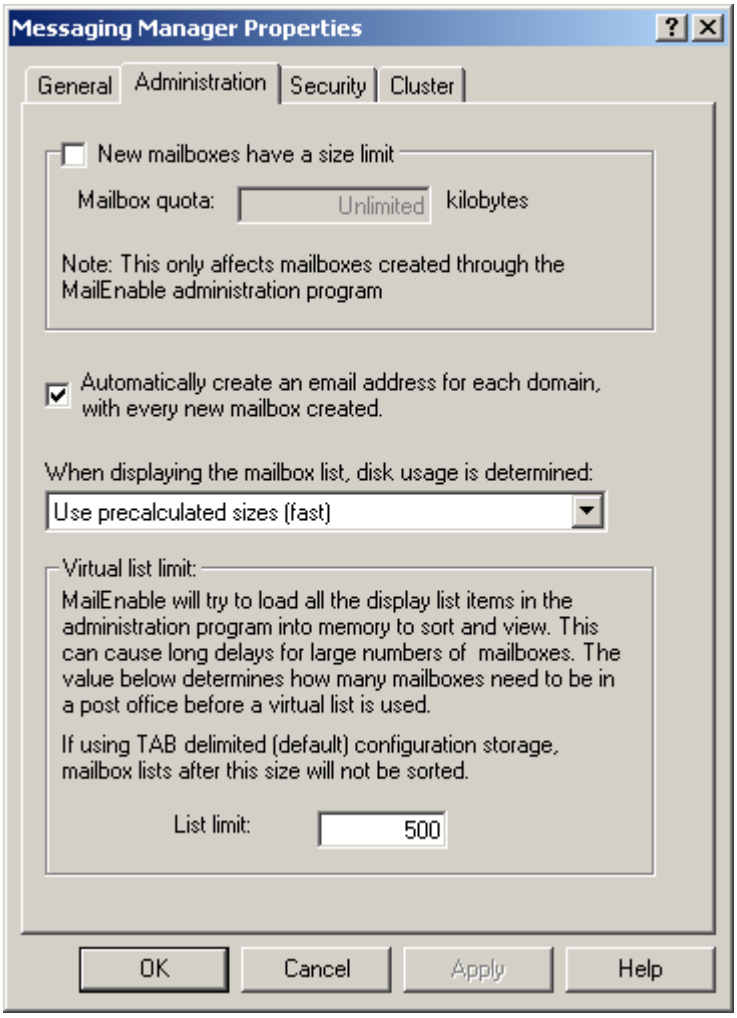
5.2.2 Messaging Manager - General

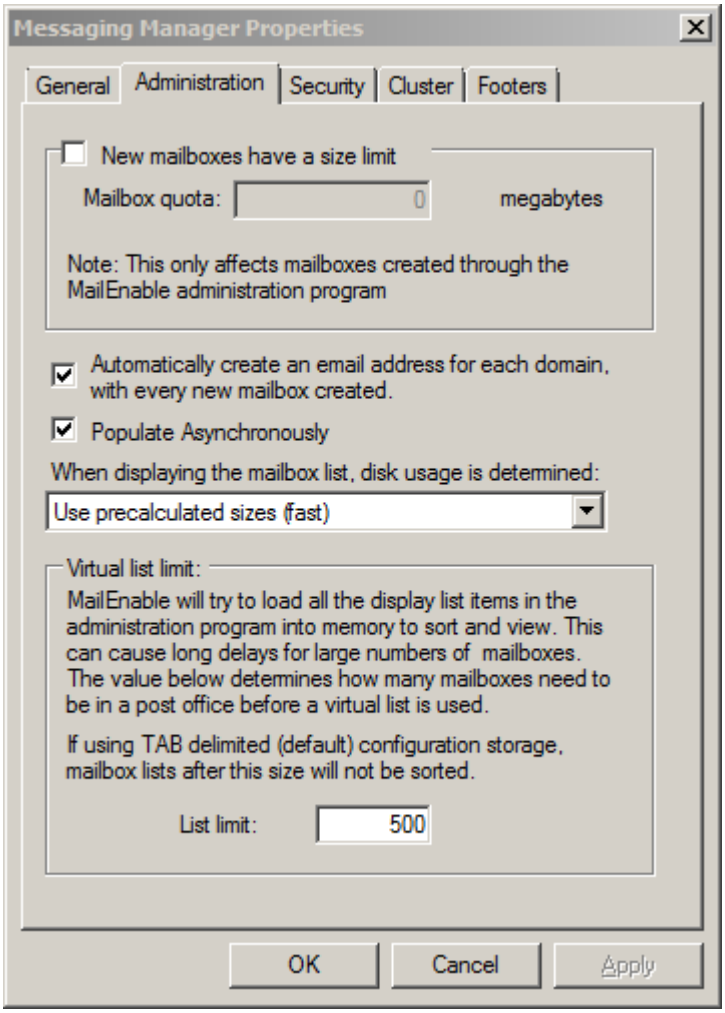
General Settings for MailEnable's configuration can be found under the properties of the Messaging Manager. The paths that MailEnable uses to store its configuration data can be configured here.



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


Messaging Manager Properties
General
Administration
Security
Cluster
New mailboxes have a size limit
Mailbox quota:
Unlimited
kilobytes
Note: This only affects mailboxes created through the MailEnable administration program
Automatically create an email address for each domain, with every new mailbox created.
When displaying the mailbox list, disk usage is determined:
Use precalculated sizes (fast)
Virtual list limit:
MailEnable will try to load all the display list items in the administration program into memory to sort and view. This can cause long delays for large numbers of mailboxes. The value below determines how many mailboxes need to be in a post office before a virtual list is used.
If using TAB delimited (default) configuration storage, mailbox lists after this size will not be sorted.
List limit:
500
OK
Cancel
Apply
Help



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 domain, with every new mailbox created.	If there are several domains in a post office and this setting is selected, then every time a mailbox is created in a post office a mail address or address mapping will be created for each domain for the mailbox. 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

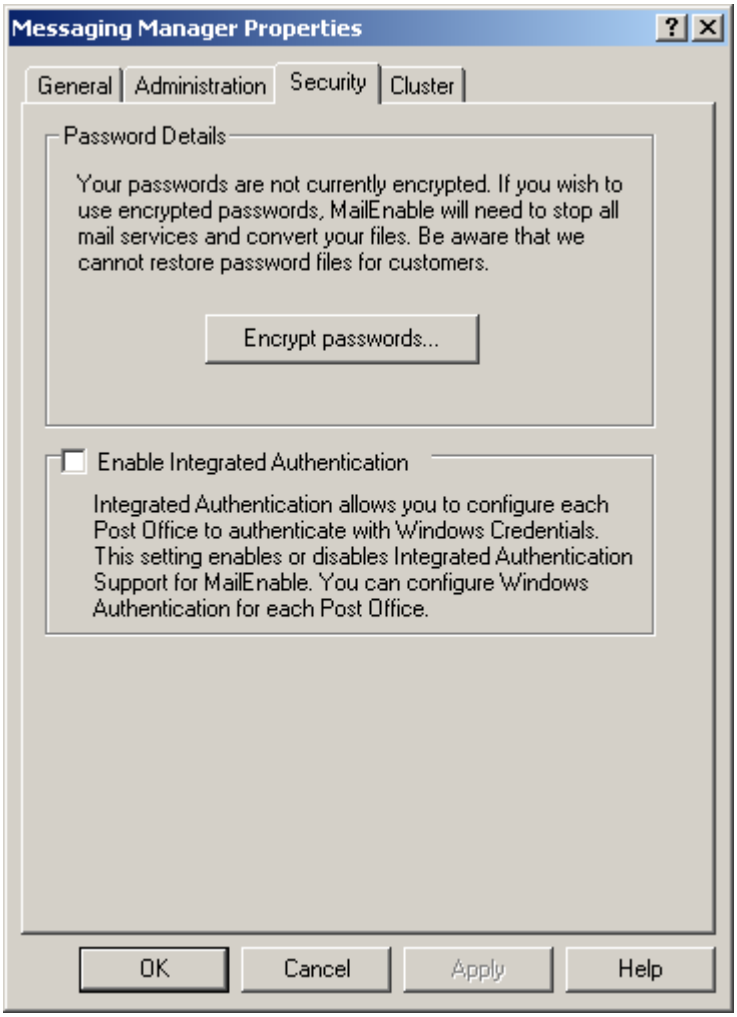
mailbox list. The size column in the mailbox list will show NA.

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:

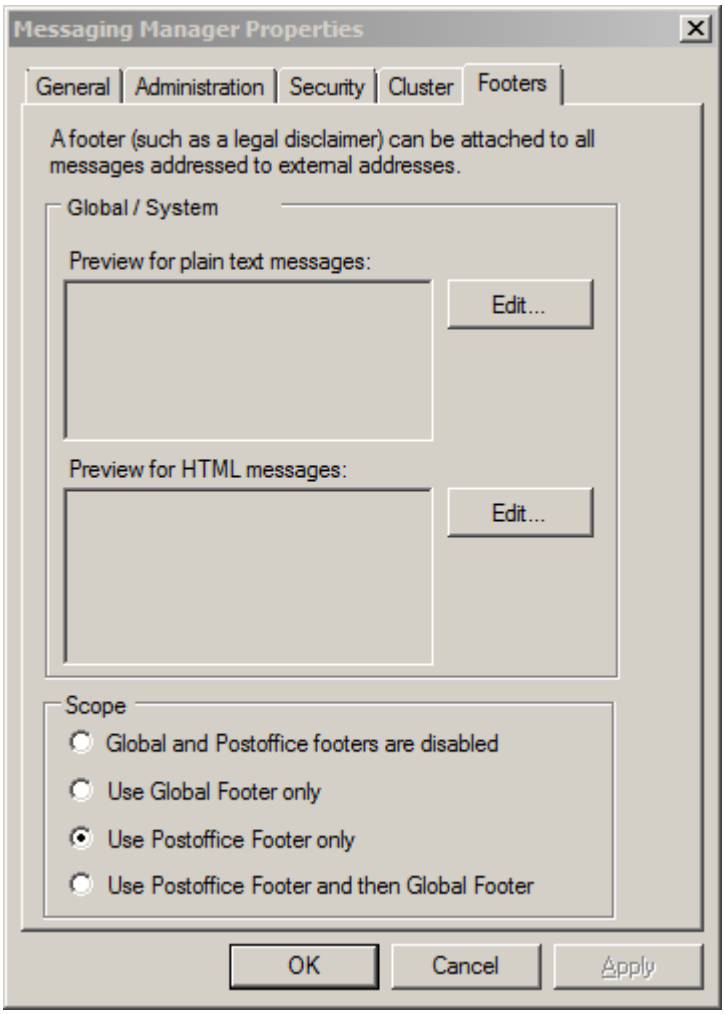


Setting	Explanation
Password Details/Encrypt Passwords	When using Tab Delimited Configuration Providers, which is the default storage within MailEnable, MailEnable passwords are stored in text files with a TAB extension under the \config directory of the MailEnable directory structure. You can optionally 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".

5.2.5 Messaging Manager - Footers

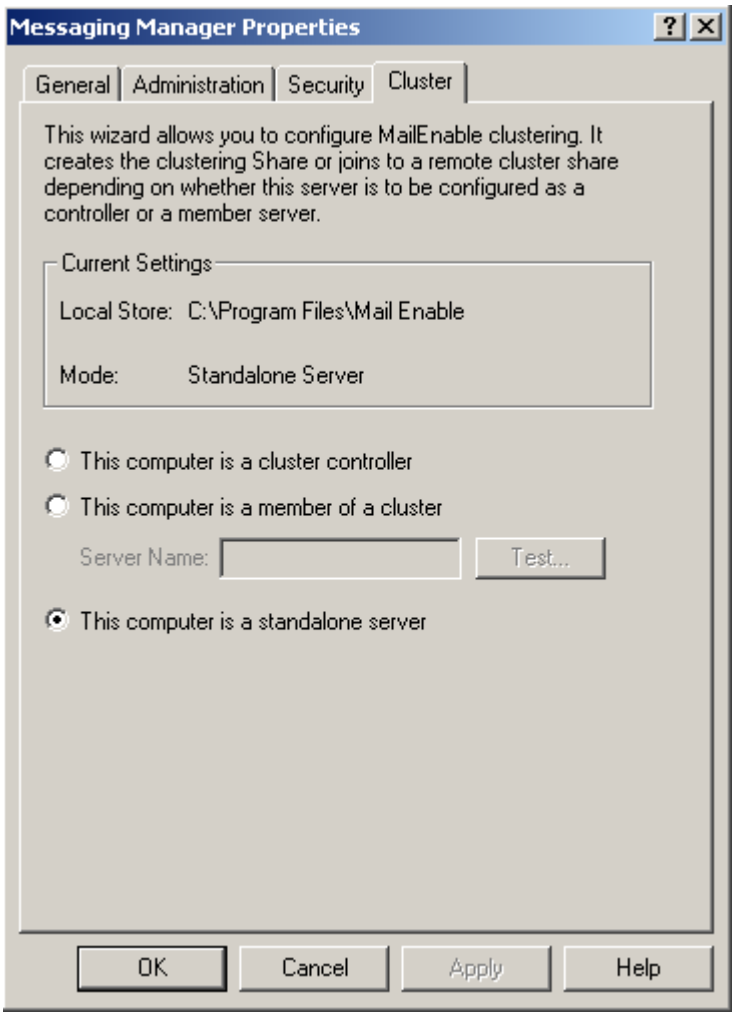
Footers, otherwise known as disclaimers can be attached to messages that are sent to external addresses. Footers can be enabled at the global level or at the postoffice level. Please see below for the available settings.



Field	Explanation
Scope	**Global and Postoffice footers are disabled:**
	This settings disables footers for global and postoffice levels
	Use Global Footer Only:
	Footers will only be used at the global. Any postoffice level footers will be used.
	Use Postoffice Footer Only:
	Footers will only be used at the postoffice and Global footers will not be used.
	Use Postoffice Footer and then Global Footer:
	Will set the postoffice footer first followed by the set global footer.

5.2.6 Messaging Manager - Cluster

The cluster tab contains settings for configuring server clustering. For more information on configuring server clusters see the **Cluster management section (Section 10.1)**.



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

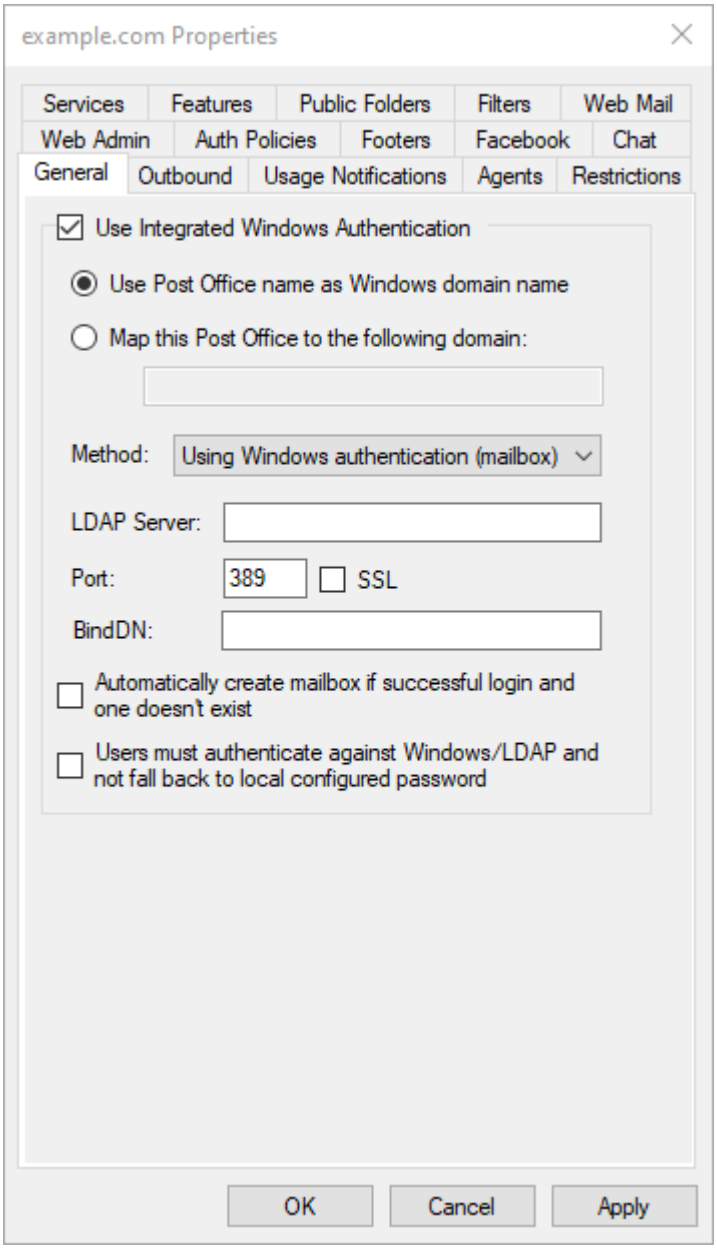
5.3.3 Post office - General

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.

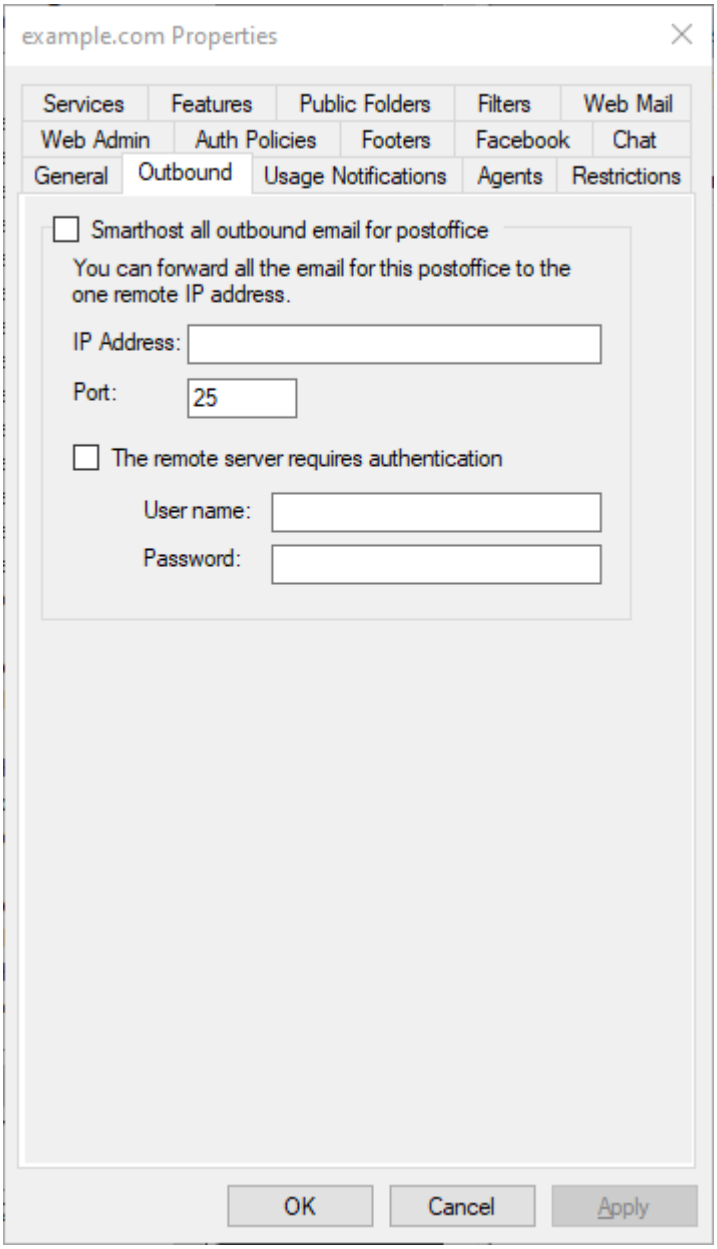


Setting	Explanation
Use Integrated Windows Authentication	Defines whether the post office can use Windows Authentication.
Use Post Office Name as Windows Domain Name	Select this option if the name of the post office matches the desired Windows Domain Name.
Map this Post Office to the following Domain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

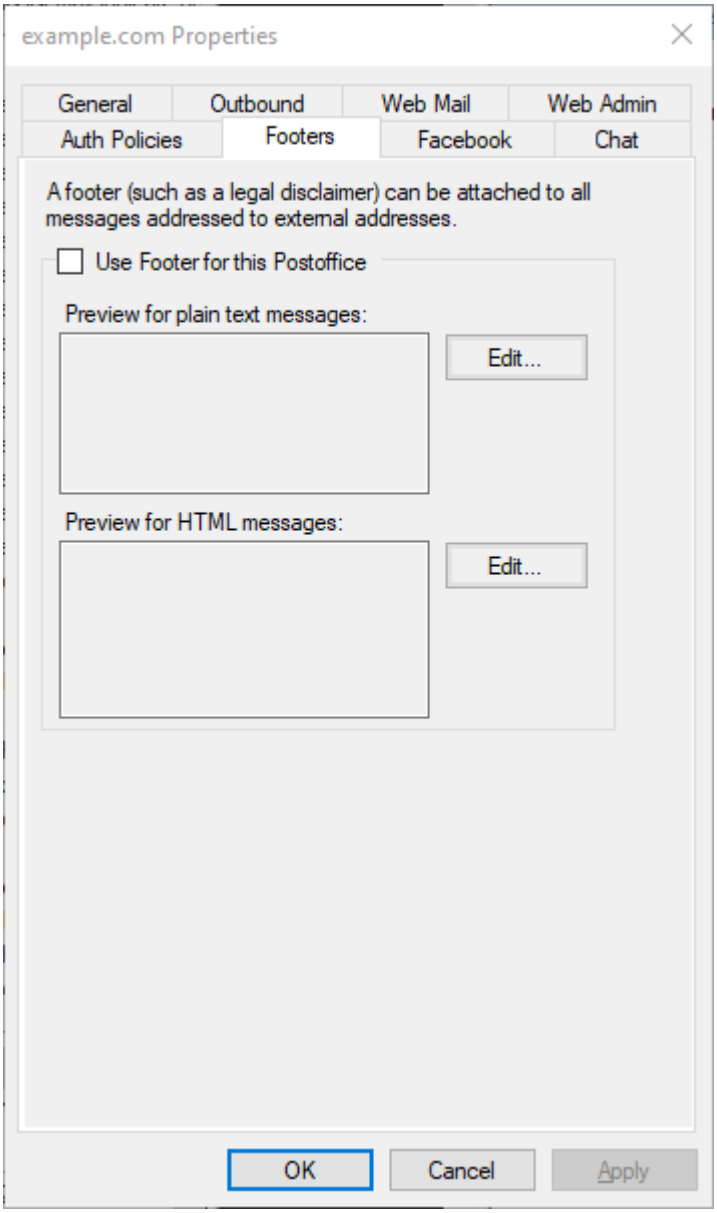


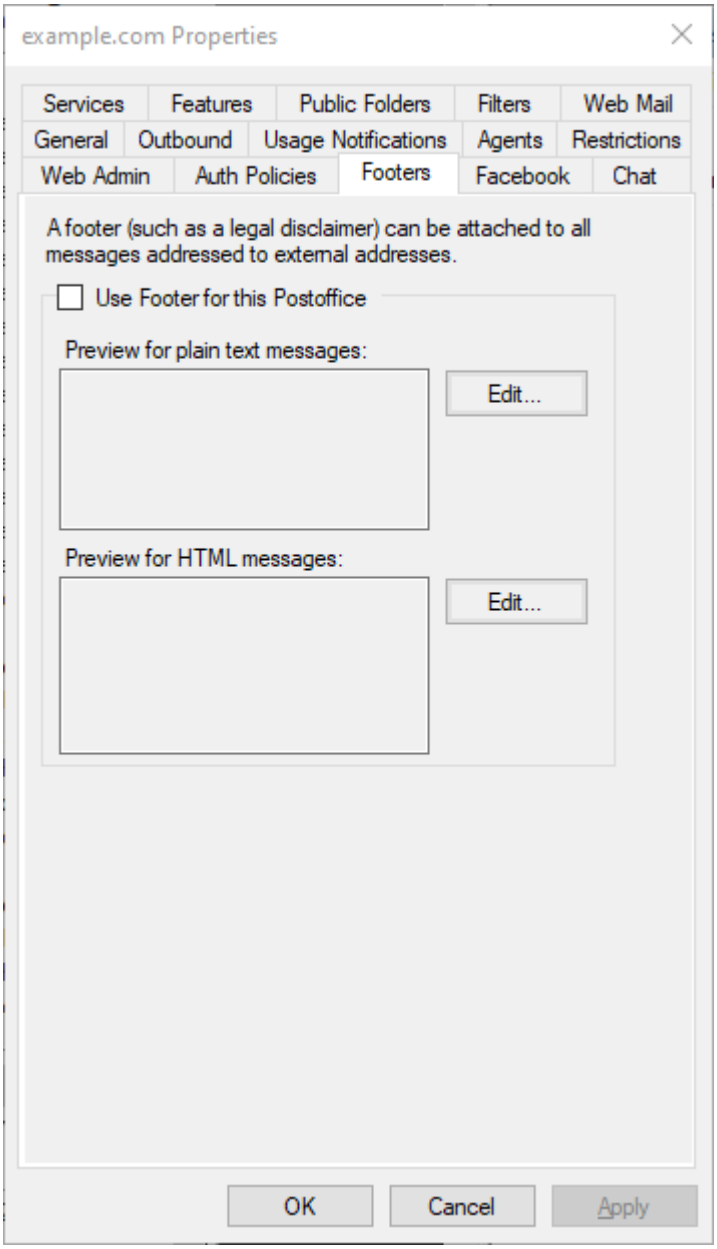
Setting	Explanation
Smarthost all outbound email for postoffice	This will route all emails for users of this postoffice to the one remote address. This would be used if you need to filter all the outbound email for just the postoffice. It does not affect email going to a local mailbox, just the outbound 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 - Footers

Footers, otherwise known as disclaimers can be attached to messages that are sent to external addresses from a postoffice. In order to determine if footers are enabled for the postoffice or have been set at a global level please see **Messaging Manager - Footers (Section 5.2.5)**

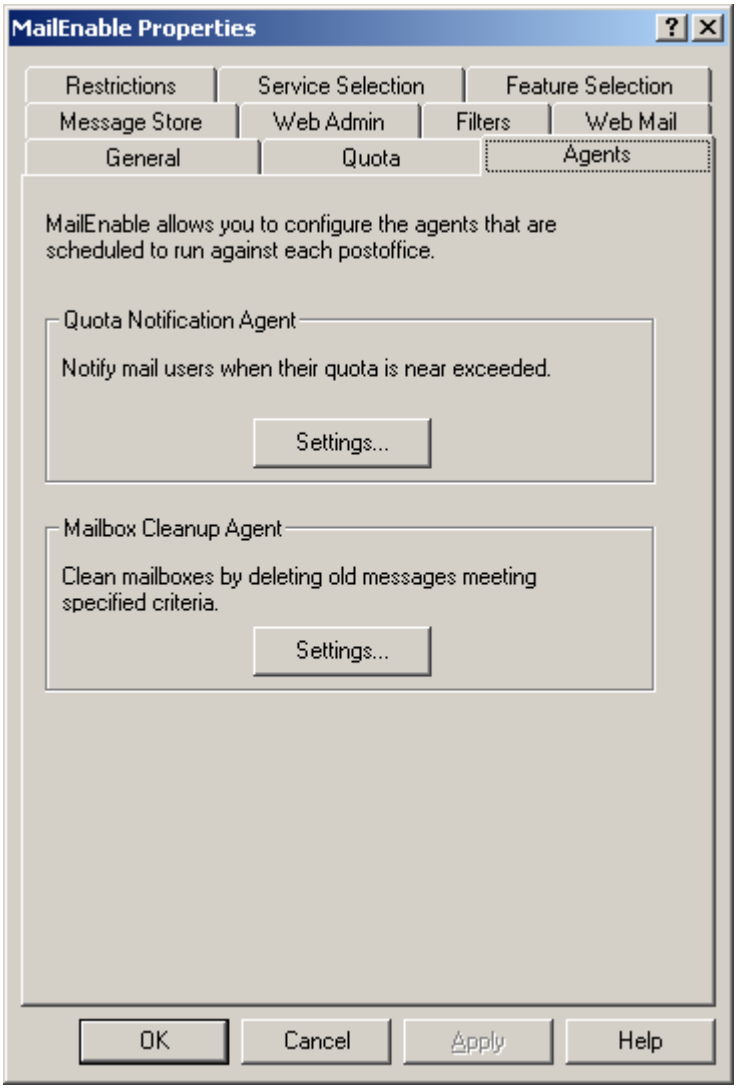
Footers can also be configured by an ADMIN user within the web administration interface. Please see the Web administration user guide for more information.





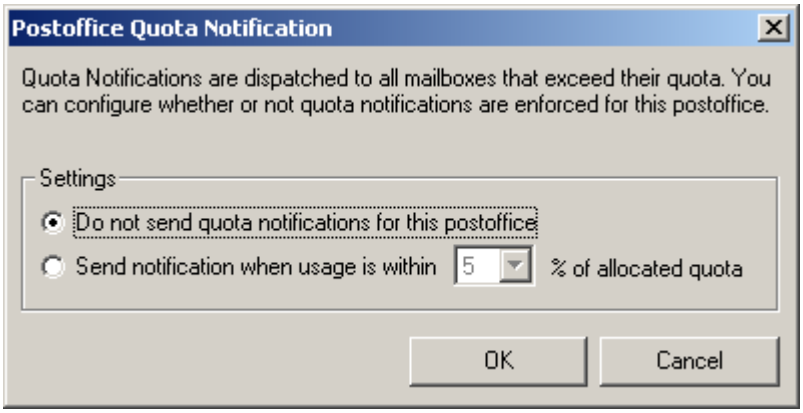
5.3.6 Postoffice - Agents

The Agents tab dialog configures the agents that are scheduled to run against each post office.



5.3.6.1 Postoffice Quota Notification Agent settings

The Postoffice Quota Notification Agent notifies mail users when their quota is near exceeded.



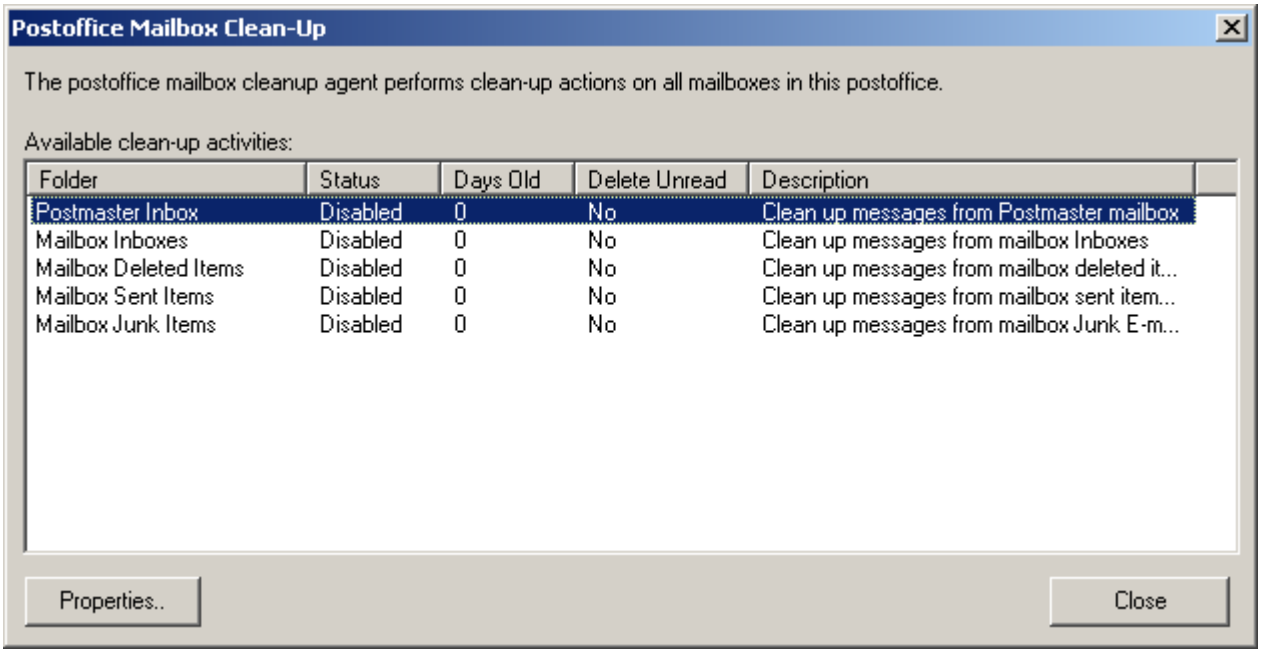
Setting	Description
Do not send quota notifications for this postoffice	Will disable quota notifications for the postoffice
Send notification when usage is	Will send out a quota notification message to the mailbox when the quota is

within % of allocated quota	within the specified percentage value of allocated quota.

Note: For more information about how to edit the polling times for the postoffice Agents please see the **Management service - Quota Notification Agent (Section 6.6.6)** section of this manual

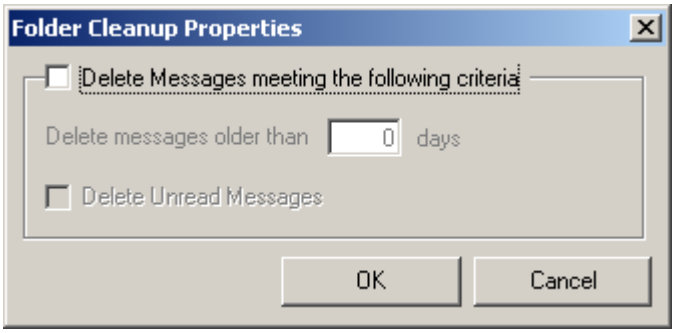
5.3.6.2 Postoffice Mailbox Clean-Up Agent settings

The Mailbox Cleanup Agent cleans mailboxes by deleting old messages meeting specified criteria.



Settings	Description
Properties..	Used to open the properties window for each criteria. Highlight a criteria in the list and then click on the properties button. Alternatively you can double click on each criteria to open the same properties window.
Close	Closes the Mailbox Clean-Up Agent settings window

Folder Cleanup Properties

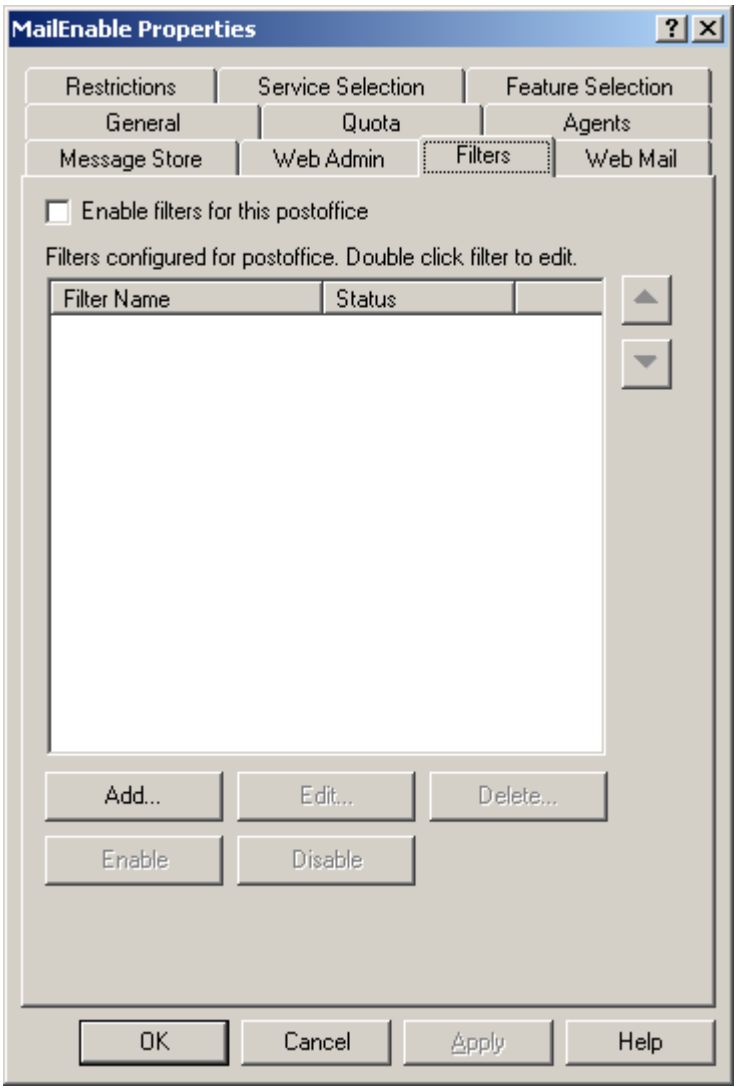


Settings	Description
Delete Messages meeting the following criteria	Enables the Mailbox Clean-Up Agent for the folder
Delete messages older than days	The Mailbox Clean-Up Agent will delete any messages older then the specified value in days
Delete Unread Messages	Enables the option for the Mailbox Clean-Up Agent to delete unread messages

Note: For more information about how to edit the polling times for the Postoffice Agents please see the **Management service - Mailbox Clean-Up Agent (Section 6.6.5)** section of this manual

5.3.7 Postoffice - Filters

Postoffice level filters will allow the configuration of filters for messages destined to a post office. These filters can be defined similar to Global Filters, however they assume the scope of the respective postoffice.



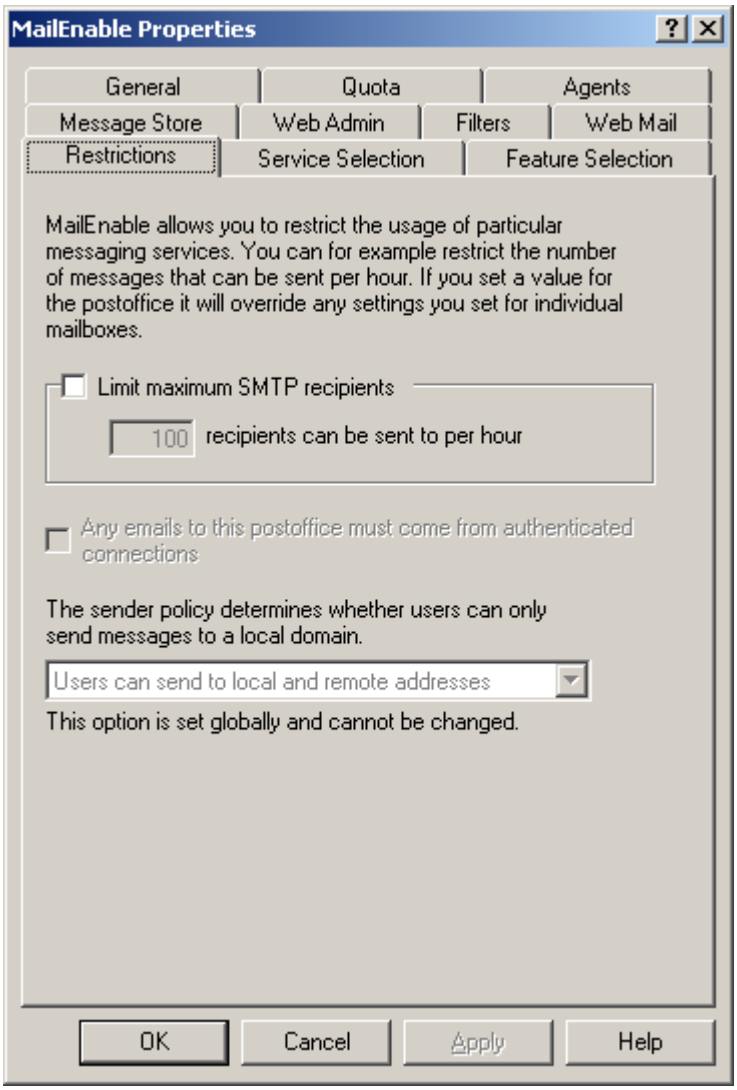
Settings	Description
Enable filters for this mailbox	Enables filtering for the postoffice.
Filters configured for this postoffice	Displays the list of filters configured for the postoffice.
Add...	Adds a new filter.
Edit...	Opens the filter criteria and actions window when a filter has been selected in the list.
Delete...	Deletes a selected filter
Enable	Enables a selected filter

Disable	disables a selected filter

Note: For information on criteria descriptions and actions please refer to Filter Criteria management and **Filter actions (Section 9.4.3)**

5.3.8 Postoffice - Restrictions

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

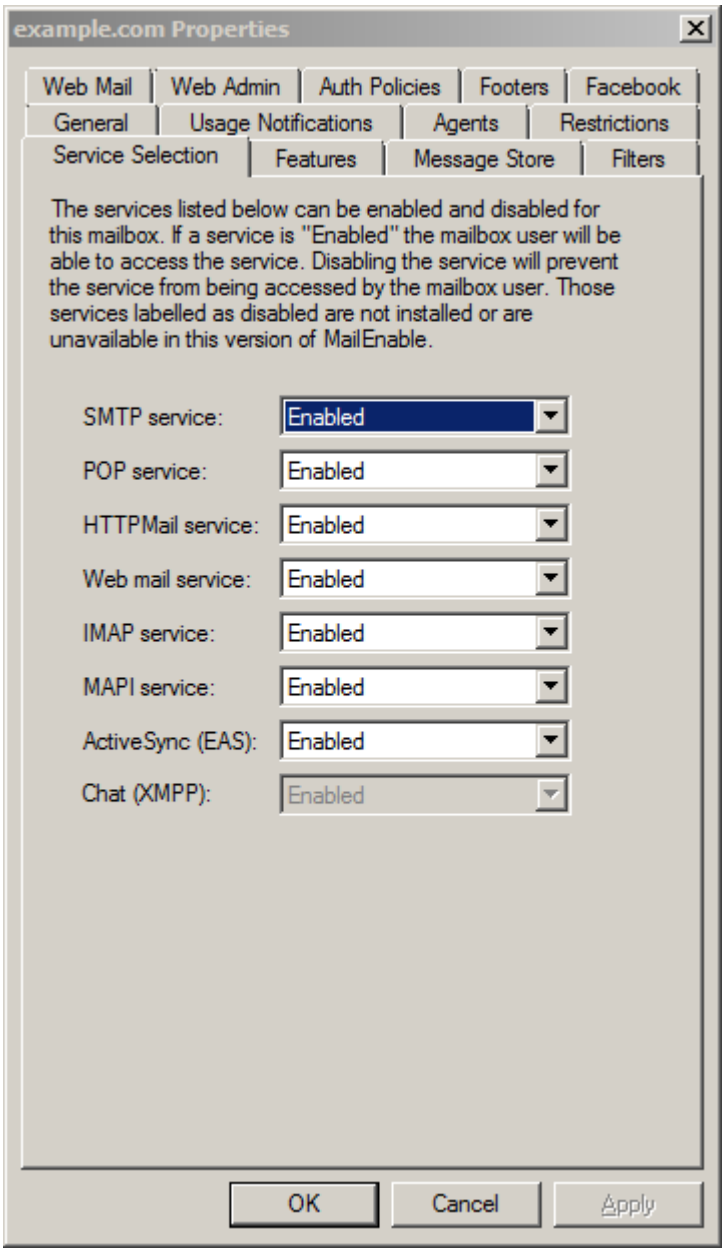


Setting	Explanation
Limit Maximum SMTP recipients	Throttles any mailbox from sending more than a configured number of emails per hour. This setting is useful for hindering spammers from sending and using the server as a source for spamming if they do guess or have otherwise have access to user credentials. The postoffice value will override the mailbox value. The postoffice value will also override the global value set under the SMTP options.
Any emails to this postoffice must come from from authenticated connections	If this setting is ticked then any message destined to mailboxes that reside under the postoffice will need to originate from an authenticated connection. Please see **SMTP - Advanced SMTP (Section 6.14.7)** for information on how to enable this option if greyed out.

Sender Policy dropdown	**Users can send to local and remote addresses:** Allows users to be able to send to local mailbox addresses hosted locally within MailEnable and to send to external addresses hosted on remote mail servers. **Users can send to local addresses only:** Allows users to only be able to send to local mailbox addresses hosted locally within MailEnable **Sender policy determined by mailbox:** Sets the sender policy to be determined by the mailbox restriction settings. Please see Mailbox - Restrictions

5.3.9 Postoffice - Service selection

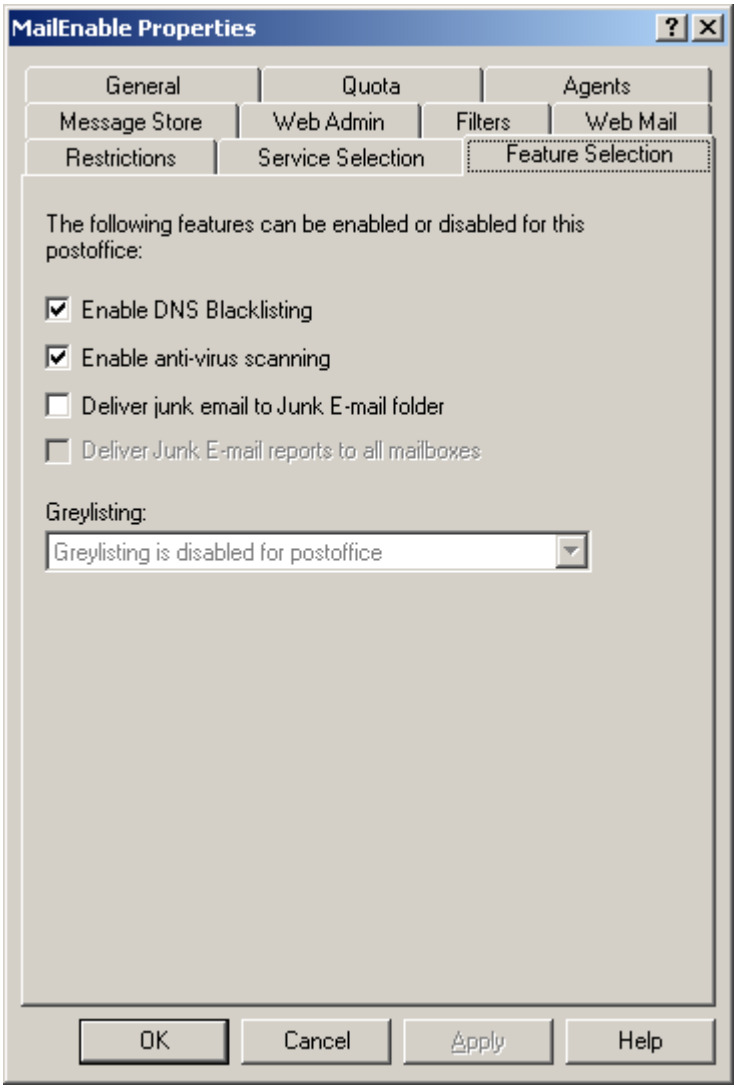
Enable or disable mail services for a post office. If a service is 'enabled' it becomes available for all users in the selected post office.



Setting	Explanation
Service Settings	Enabled services are configured at a post office level and then further arbitrated at a mailbox level. Disabling a service at a post office level will override any mailbox level service settings. For example, if web mail is disabled at a post office level, the mailboxes under the post office will not be able to access web mail. For developers, the values are stored in the postoffice.sys and mailbox.sys files and can be managed by the System Object Provider. Details for using the System Object Provider are outlined in the API Guide.

5.3.10 Postoffice - Feature selection

Features such as Reverse DNS Blacklisting, antivirus scanning and delivery of junk mail to the junk folder can be enabled or disabled for each post office.

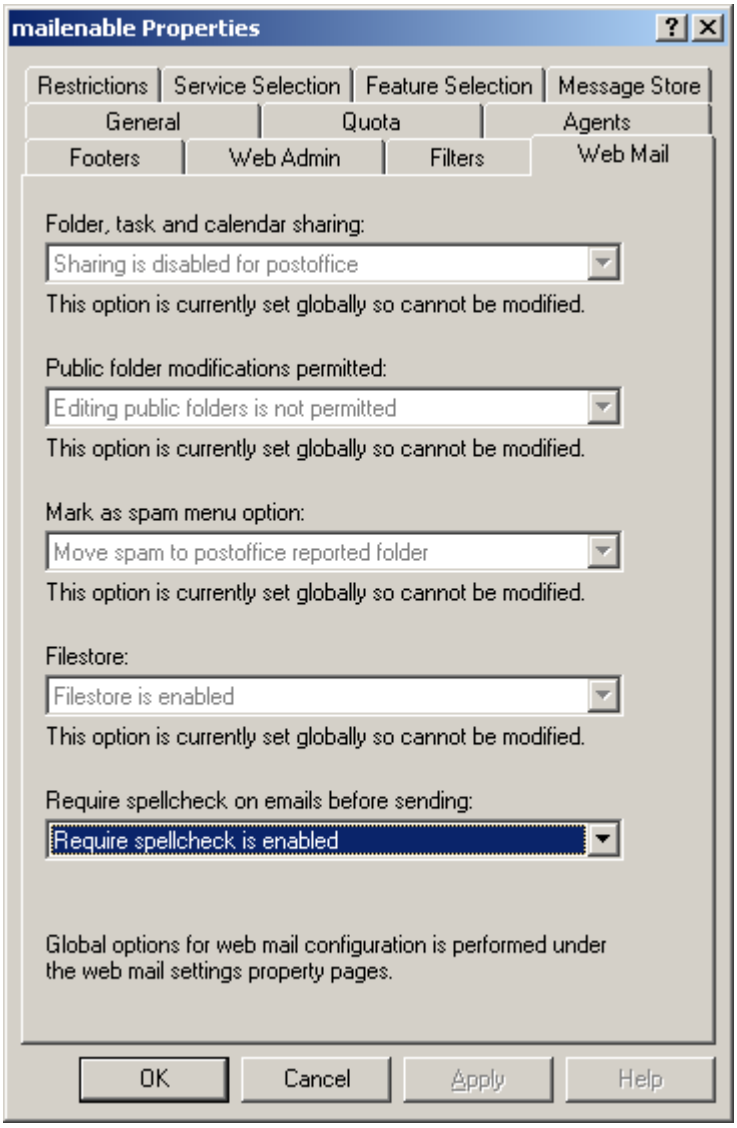


Setting	Explanation
Enable DNS Blacklisting	Allows the disabling of DNS blacklisting for a post office. Disabling this will prevent URL blacklisting from being done by the SMTP service, and will also stop the SMTP serivce from rejecting emails from a blacklisted IP address. Emails from a blacklisted IP address will still be marked as junk.
Enable	Allows the disabling of antivirus checking for a post office. Any emails attributed to the

antivirus scanning	postoffice will not be checked for viruses.
Deliver Junk Email to Junk Email folder	Disabling this feature for a post office will change the actions of any configured filters where the filter has an action of **Mark as spam**. The message will be delivered to the inbox as normal rather than the Junk E-Mail folder of a mailbox. For emails to be delivered to the Junk E-mail folder for a mailbox, the message must have the following header item: `X-ME-Content: Deliver-To=Junk` Filters can add this header. See the **Filter actions section (Section 9.4.3)** for more information. If this option is greyed out it will be configured globally. See **Message Filtering (Section 9.1)** on how to change from a global setting.
Deliver Junk E-mail reports to all mailboxes	This option will enable Junk E-mail reports to all mailboxes within the postoffice. If this option is greyed out please see **Report Agent (Section 6.6.7)** settings.
Greylisting: dropdown	**Greylisting is disabled for postoffice:** Disables greylisting for all users within the postoffice. **Greylisting is enabled for all mailboxes:** Enabled the greylisting for all mailboxes within the postoffice. **Greylisting is configured per mailbox:** This will set the greylisting option to be determined by the mailbox. Please refer to Mailbox - Spam for more information. Greylisting is described in more detail under the **SMTP section (Section 6.14.15)** of this document.

5.3.11 Postoffice - Web Mail

These options provide postoffice level options for Web Mail. The settings on this tab can also be configured at the global level under the **Web mail - Site Options (Section 6.18.2.3)**.

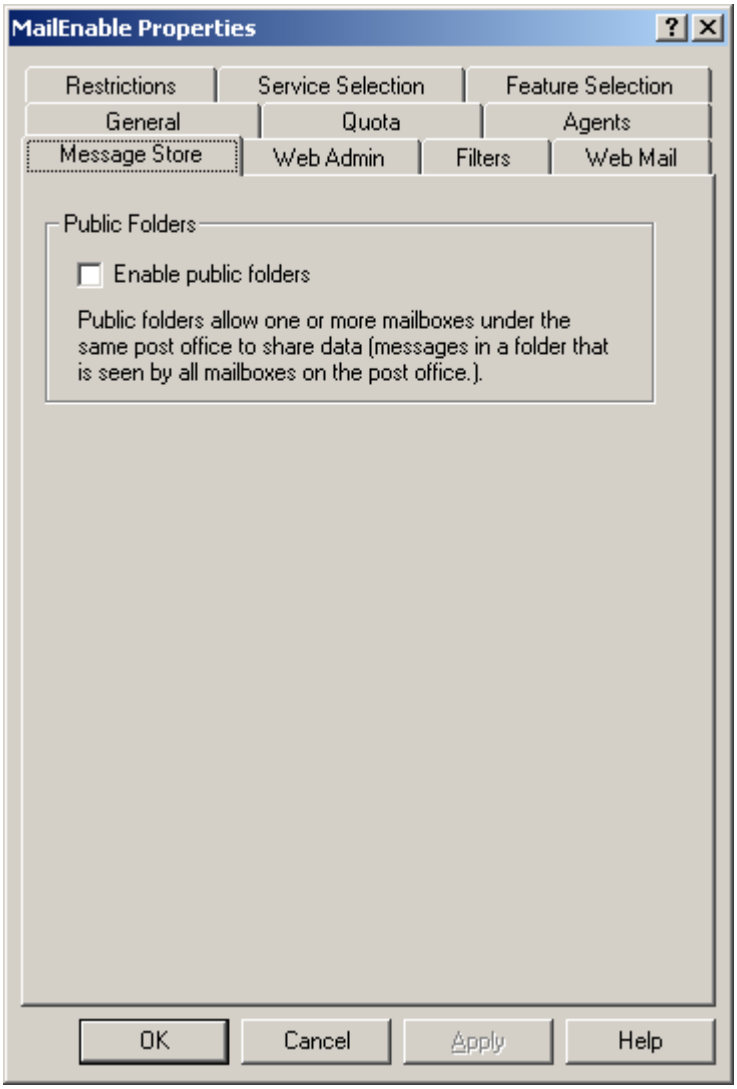


Setting	Explanation
Folder, Tasks, and Calendar Sharing	Enables Folder, Task and Calendar sharing for the post office. **Sharing is disabled for postoffice:** Disables sharing for the postoffice. **Sharing is enabled for all mailboxes:** Enables sharing for all mailboxes within the postoffice **Sharing is enabled per mailbox:** Enables sharing at the mailbox level which is set within the properties window for each mailbox under the web mail tab. Please see **Mailbox - Web mail (Section 5.5.14)**
Public Folder Modifications Permitted	Determines whether public folder is read only. **Editing of public folders is not permitted:** Disables Public Folders for the postoffice. **Editing of public folders is permitted:** Enables Public Folders for all mailboxes within the postoffice **Editing of public folders configured per mailbox:** Enables Public Folders at the mailbox level which is set within the properties window for each mailbox under the web mail tab. Please see **Mailbox - Web mail (Section 5.5.14)**
Mark As Spam Menu Option	This allows you to select the post office level spam reporting options presented to web mail users. **Move spam to postoffice reported folder:** Will move the selected spam message to the

	postoffices reported spam folder. **Mark the sender IP as spam source:** Extracts the sending IP address of the message from the headers of the message and creates 2 records in the following locations: Config\Postoffices\Postoffice\Connections\Spam Config\Connections\Spam The SMTP connector (and custom filters) can then use these records to determine whether or not to refuse mail from the IP address.
FileStore (MyFiles)	This option enables the FileStorage option. Please review the web mail properties section for more information on how to the File storage option at the postoffice level. **Filestore is disabled:** Disables File Storage for the postoffice. **Filestore is enabled:** Enables File storage for all mailboxes within the postoffice **Filestorage is configured per mailbox:** Enables Filestorage at the mailbox level which is set within the properties window for each mailbox under the web mail tab. Please see **Mailbox - Web mail (Section 5.5.14)**
Require Spellcheck on emails before sending:	This option determines whether messages need to spell checked before sending. **Require spellcheck disabled:** Disables the spellchecking before sending. **Require spellcheck is enabled:** Enables the spellchecking for the all mailboxes within the postoffice. **Require spellcheck configured per mailbox:** Enables spellchecking before sending at the mailbox level. Please see **Mailbox - Web mail (Section 5.5.14)**

5.3.12 Postoffice - Message Store

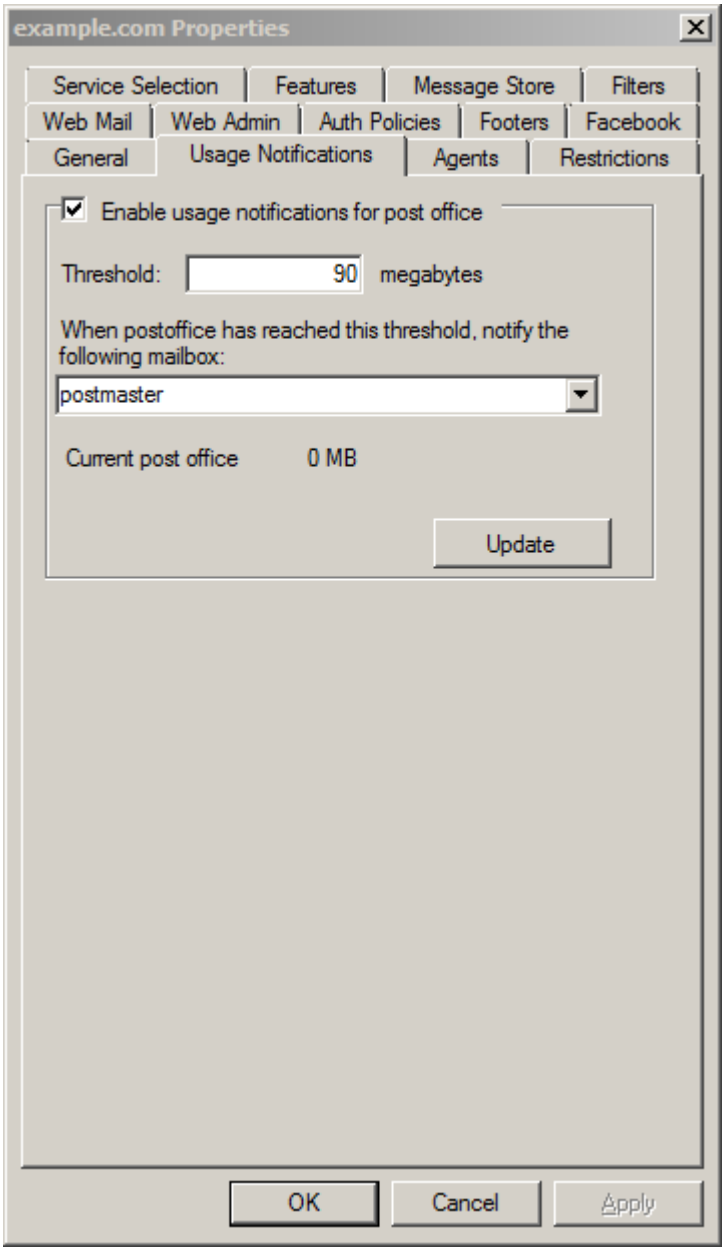
Enable or disable public folders for a post office. Public folders allow one or more mailboxes under the same post office to share data.



Setting	Explanation
Enable Public Folders	Enables public folders for a post office. Once enabled, this allows the various mail services to have a public folder that is accessible by all the mailboxes in the postoffice.

5.3.13 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.

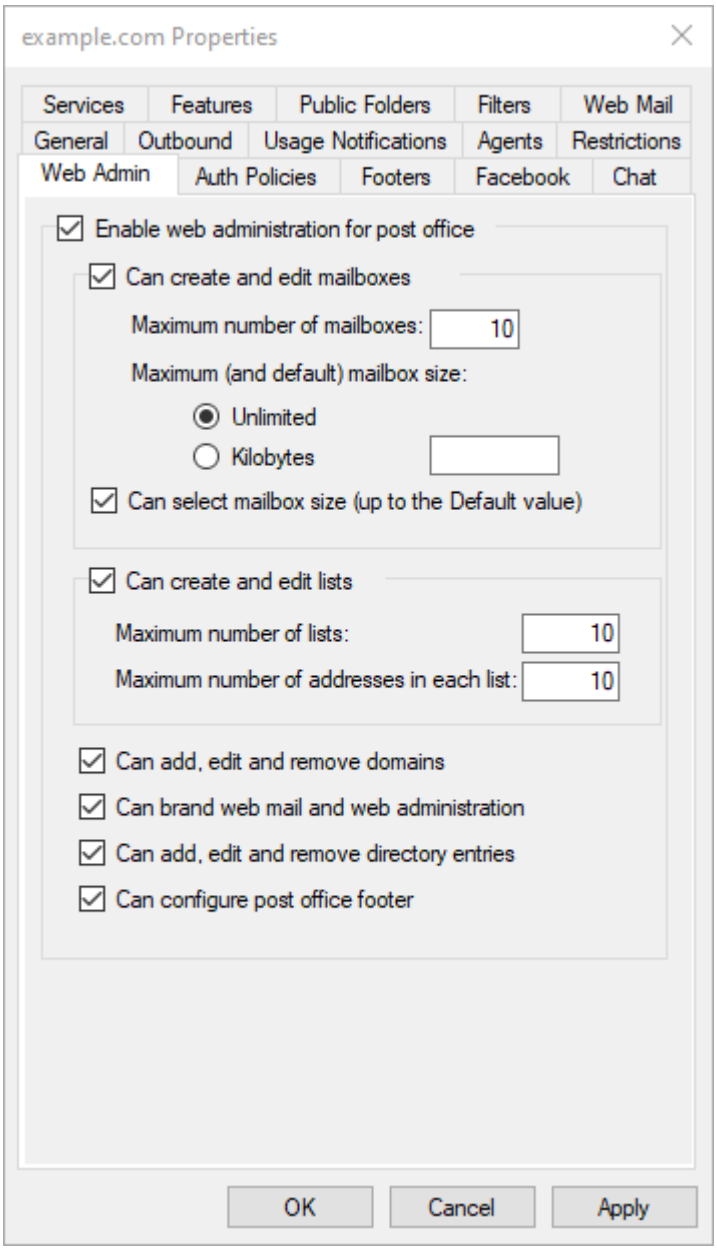


Setting	Description
Enable usage notifications for post office	Enables the quota option for the postoffice.
Threshold	The hard drive space allocated for this postoffice in megabytes.
When the post office has reached this threshold, notify the following mailbox	When the threshold is reached a notification 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.

5.3.14 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.
Can add, edit and remove directory entries	Allows the admin to manage directory entries.
Can configure post office footer	Allows the admin to edit the footer attached to each outgoing email for the postoffice. This only applies to emails that are going to another server.

5.3.15 Postoffice - Auth Policies

The post office authentication policies allows you to restrict login attempts to specific countries. The connecting IP address is checked against a country database and will either be blocked or allowed to perform a login attempt. This option can increase security by restricting login attempts to within your own country.

Setting	**Explanation**
Authentication restrictions are enabled	Country login restrictions are able to be set on a global, postoffice or mailbox level. The global level under the servers authentication policies has to be be set to configure it at a postoffice level in order for postoffice level option to be configured.
Stop connections from the countries below authenticating. All other countries can authenticate.	There are two modes available for determining whether a person in a country can authenticate. You can either block specific countries or allow specific countries. Selecting this option allows you to block individual countries.
Only connections from the countries selected below can authenticate.	Select this option when you just want to select the countries that are able to log into the postoffice.
Countries	This is the country list where you can select which countries apply to the above settings.
Allow E-mail addresses for usernames	By default, usernames are formatted as mailbox@postoffice. You may wish to allow users to use an email address connected to their mailbox to log in. Enabling this option allows users to use any email address mapped to their mailbox instead of their mailbox name.
Allow users to configure Two Factor Authentication	This will allow users to configure two factor authentication under web mail. The two factor authentication is configured under the Options->Login page.

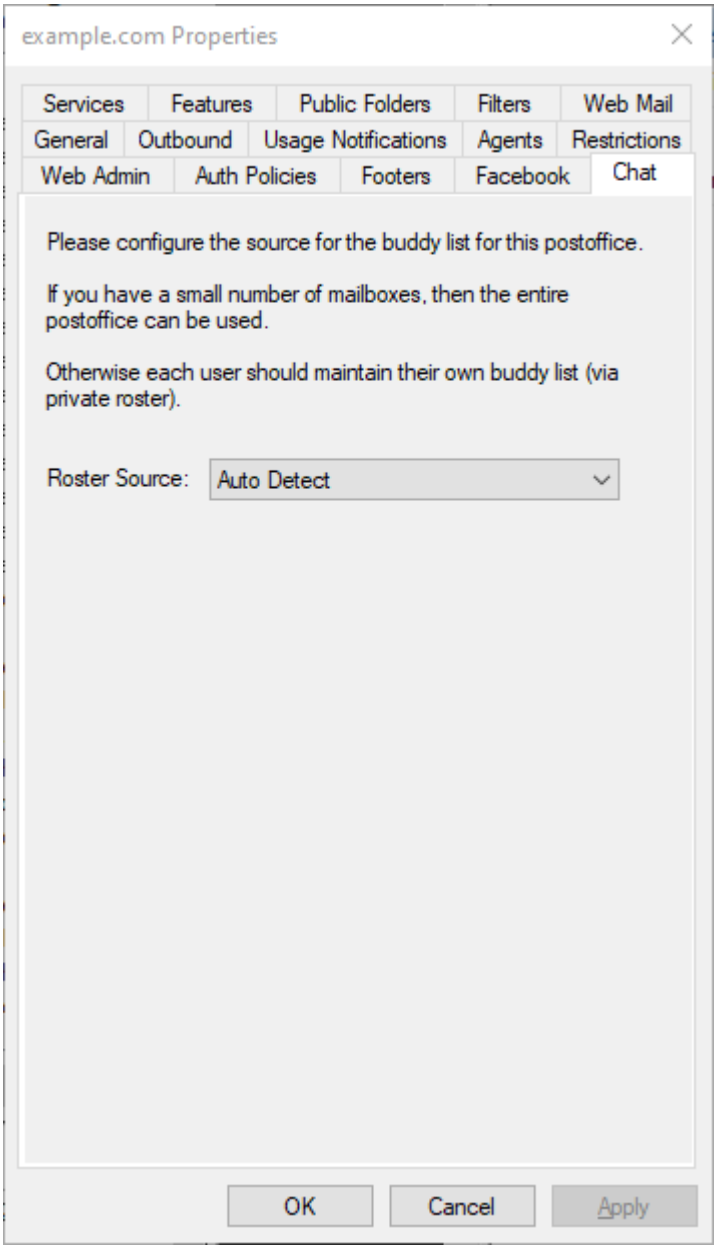
5.3.16 Postoffice- Facebook

Facebook authentication allows you to login into webmail with just a click, if you are already logged into Facebook. This can make logging into webmail a lot easier, especially for mobile users.

Setting	Description
Facebook Status	Enables Facebook login for the selected postoffice.
Facebook Application Id	The Facebook application ID for this postoffice. The host header you have configured for this postoffice needs to be configured under Facebook.
Facebook Application Secret	The Facebook Application Secret for this postoffice.

5.3.17 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.

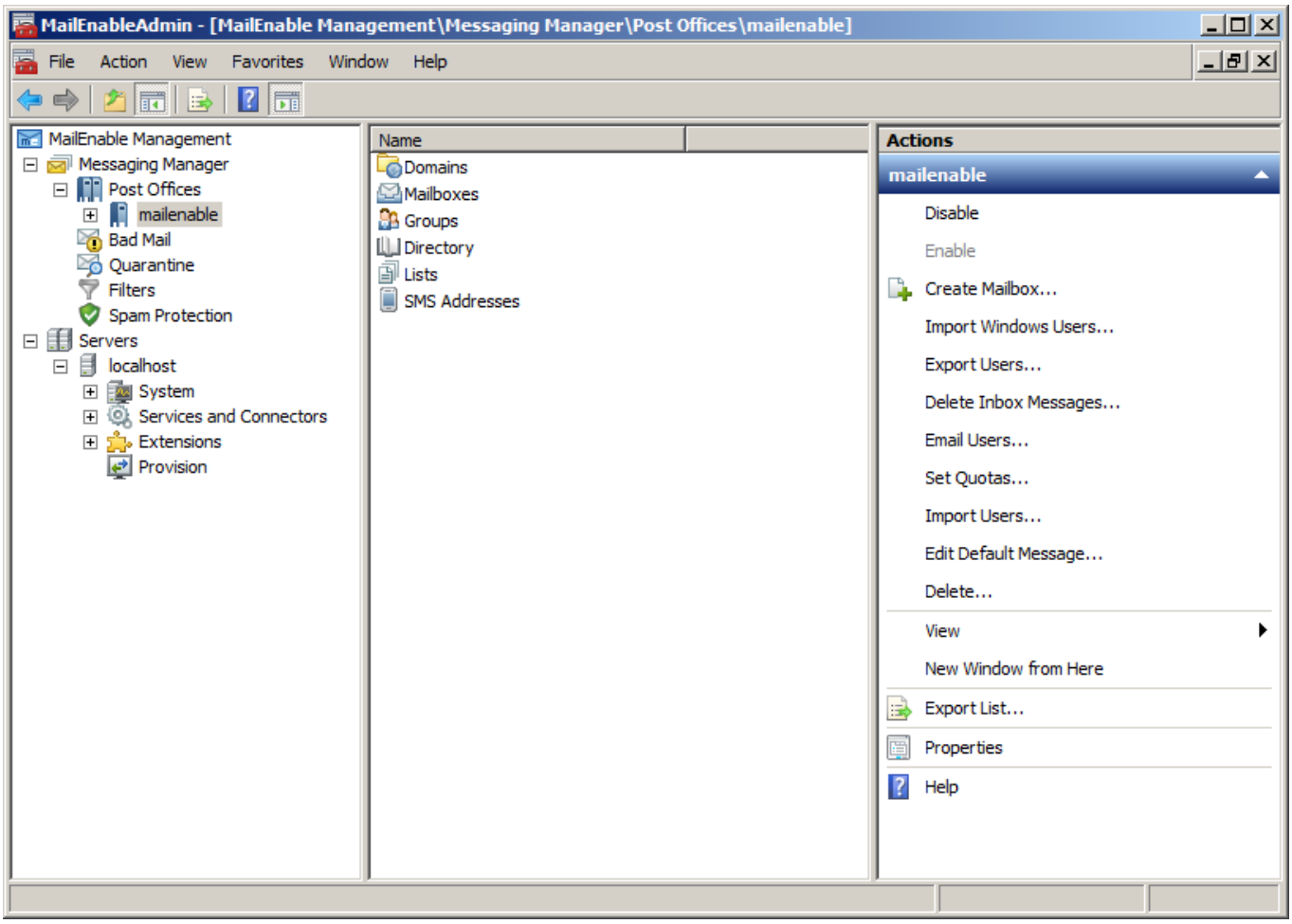
5.3.18 Post office actions

5.3.18.1 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.



5.3.18.2 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**.

5.3.18.3 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.

5.3.18.4 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.

5.3.18.5 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.

5.3.18.6 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**.

5.3.18.7 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.

5.3.18.8 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.

5.3.18.9 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

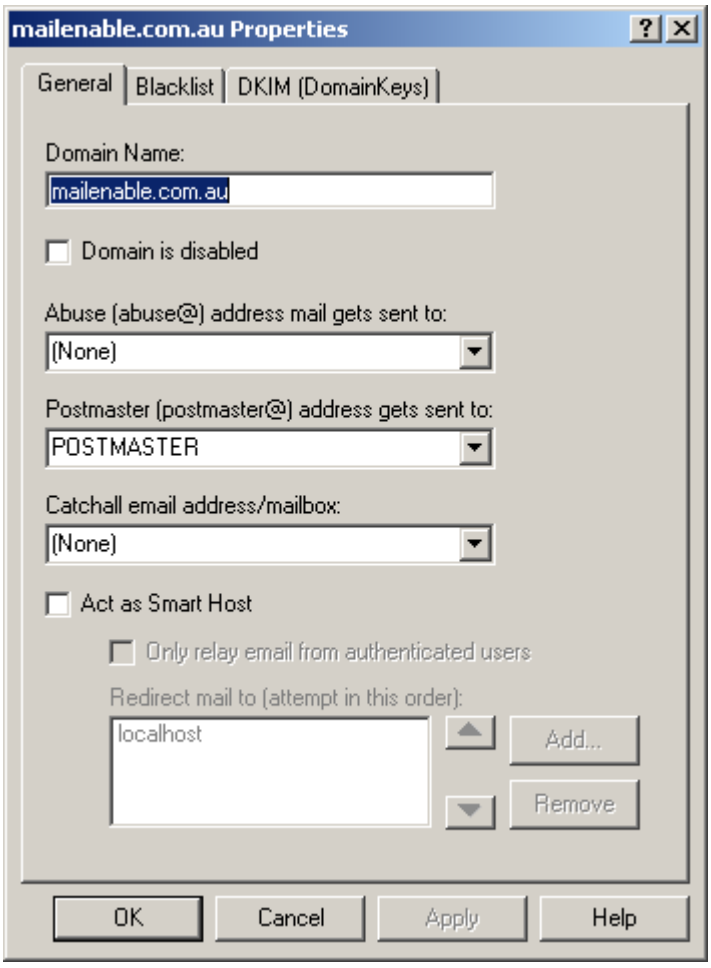
to have a valid email address.

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.**

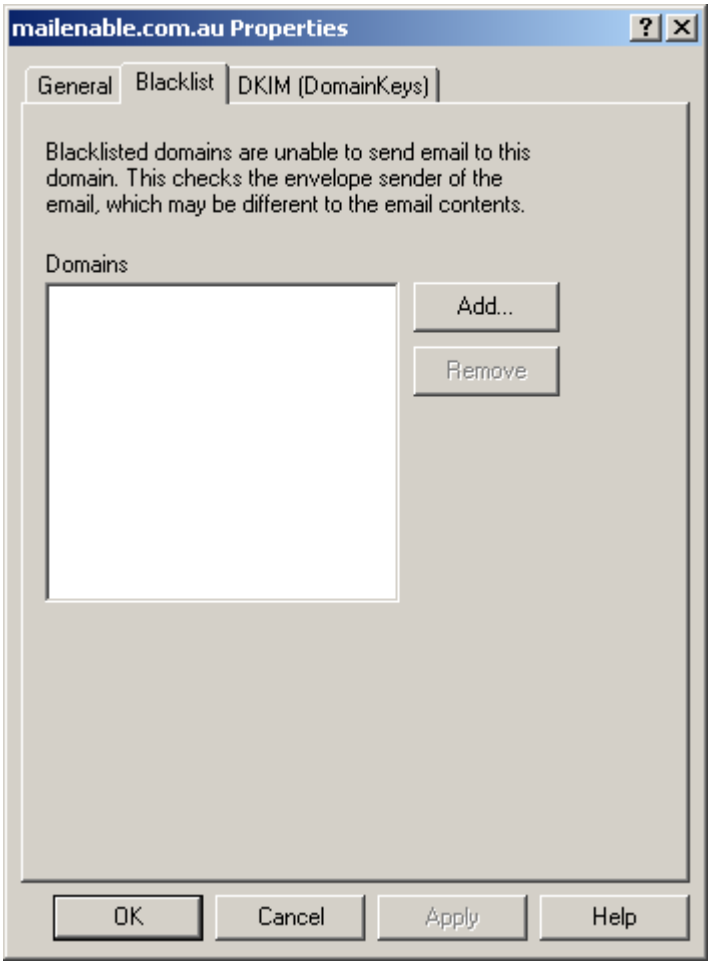
5.4.2 Domain - General



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	Enter the email address or select the mailbox for the postmaster@domain email address. This is a

Address	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 6.14.9)** 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.

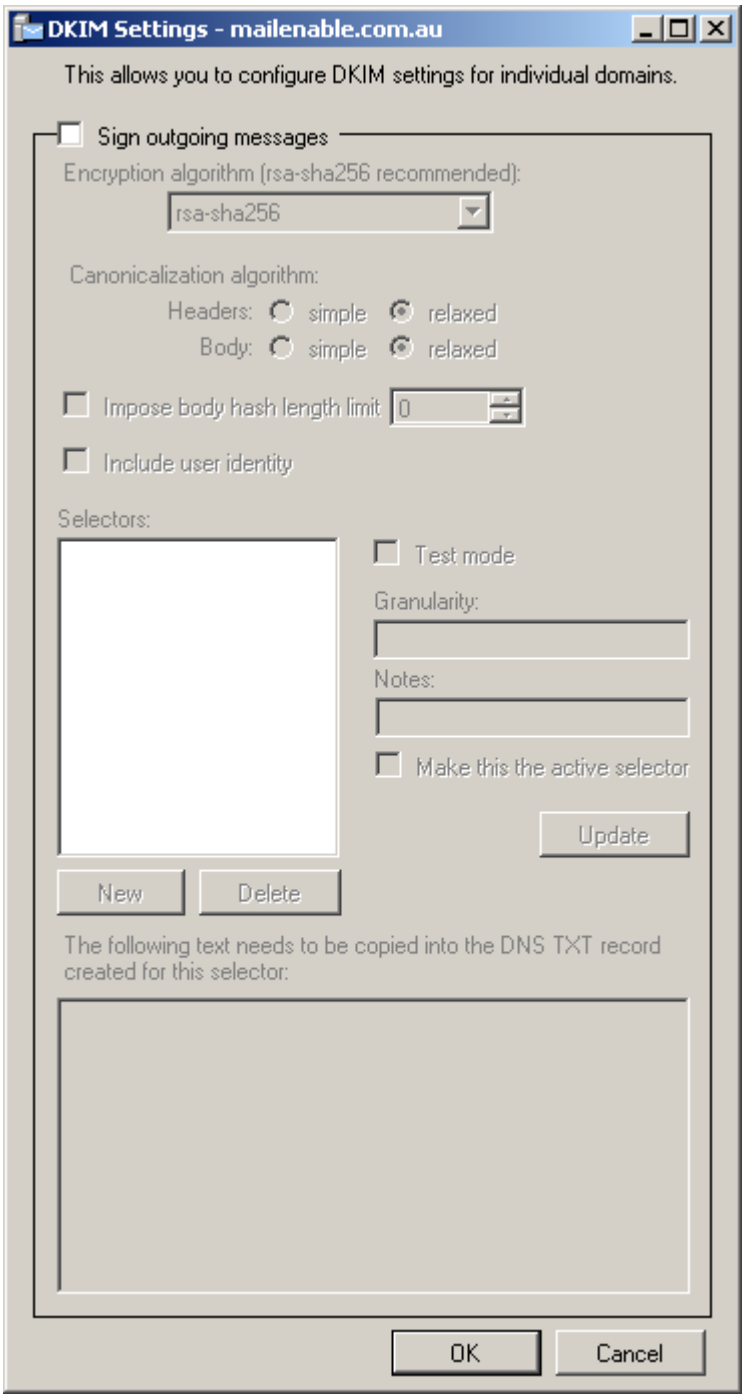
    - *Include user identity*: if checked, includes the sending user's identity in the signature header.
3. Configure selectors. A selector represents a private/public key pairing and, from the verifier's point of view, an entry in a DNS text record.
    a. Clicking New will bring up the *New Selector* dialog: 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>`.

5.4.5 Autodiscover

Each domain within MailEnable is able to provide its own Autodiscover results. This allows users to more easily configure their email client with the correct server and service details. In most cases users can just enter their email address and password in the client and the Autodiscovery feature will configure all the available services.

To configure protocols available for a domain it is easiest to click the **Detect...** button. This will try to prefill the available services using the current DNS and service settings. Once this is done you can then edit each item by double clicking it. If a service is not listed that you want to add, click the **Add...** button.

Once the autodiscover items are configured the handling of autodiscover still needs to be done, as explained below.

Autodiscover works by having email client applications retrieve an XML file from the server which describes all the services and their options (such as whether SSL is used, port numbers, etc). In order to retrieve this XML file the email clients make various HTTP requests using the email address as a starting point. For example Microsoft Outlook would initially try https://www.example.com/autodiscover/autodiscover.xml for the email address bob@example.com. A DNS SRV lookup may also be done to determine the URL to request the XML file.

For ease, the steps to configure your server would depend on whether you are hosting the websites for the domains you are providing autodiscover for.

Configuring Autodiscover for locally hosted websites

If you have an IIS site configured for a domain you can use the following steps. You must have an SSL certificate for the IIS site if using this method.

1) Run the MailEnable ActiveSync Management utility

2) Click the **IIS Integration** tab

3) Click the site you wish to configure autodiscover for an then click the Install Autodiscover button. The site you select must be accessible using https://example.com. So it must have an SSL certificate associated with the site.

Configuring Autodiscover for domains which may not be local websites

This method is also be OK to use if you host the sites locally. It does not require an SSL certificate.

1) In your DNS create the autodiscover.example.com A record (changing it to reflect the domain name being configured) and point it to the IP address of the server

2) Under IIS, for the MailEnable Protocols site, add autodiscover.example.com as a binding, to direct all requests to autodiscover.example.com to this site

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

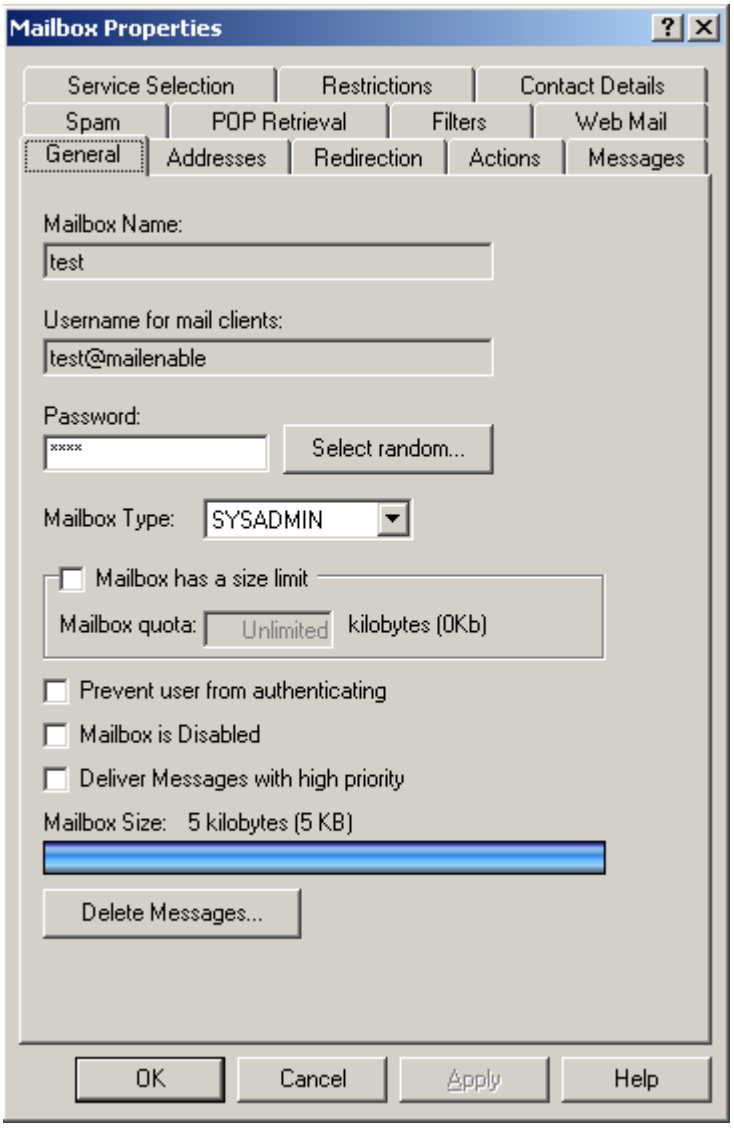
When creating a mailbox, MailEnable will automatically create an email address for each domain in the post office (if the setting for automatically creating email addresses for each domain is enabled in the Messaging Manager Properties – see the **General settings section (Section 5.2.2)**) using the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



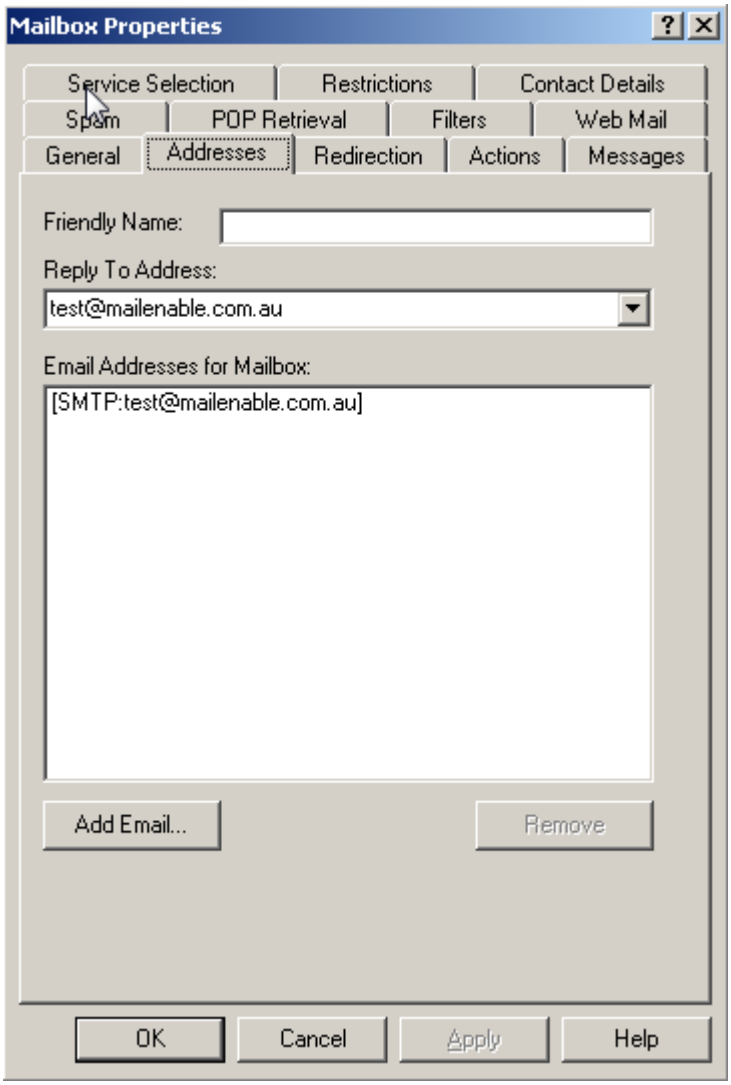
Setting	Description
Mailbox Name	This is the name of the mailbox. Once created, this cannot be changed. This both identifies the user and ensures there is no duplication of mailbox names. As the Mailbox Name is entered into the text box, the username entry just below it will change to reflect the entry.
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.
Deliver Messages with high priority	Option for setting messages that are sent from the mailbox to be sent with high priority which will be placed within the SMTP Priority queue.
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.

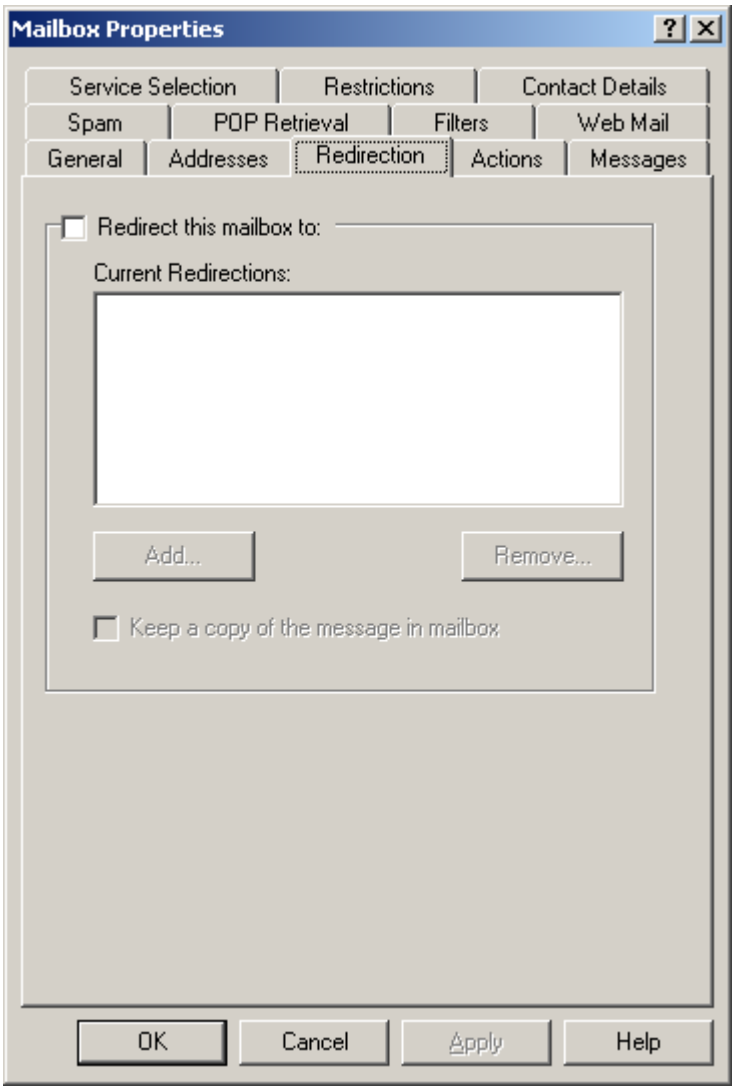
The **Available Domains** list box in this window lists domains that are entered via the **Create Domain** icon. MailEnable can only add email addresses for the available domains in each **post office** account. For the purpose of this guide we have entered only one domain. In cases where there is more 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

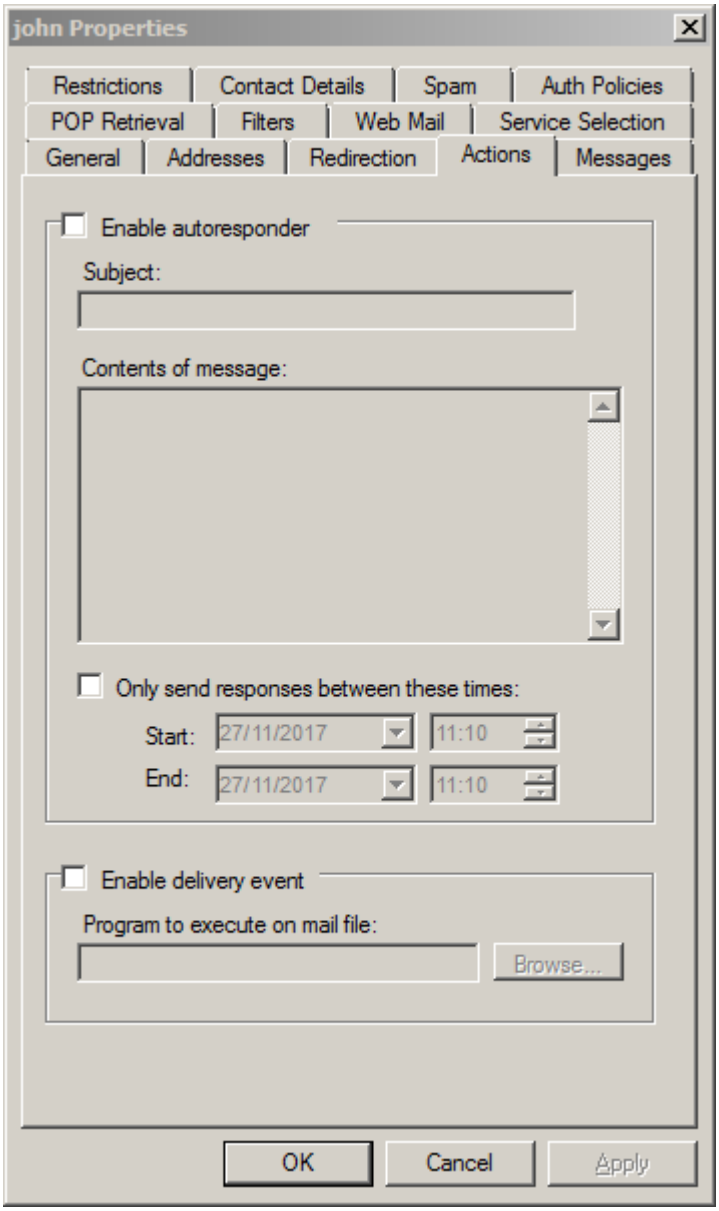
The redirection tab sets redirections for a specific mailbox to be forwarded to one or more email addresses.



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 5.7.2)**) - 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.

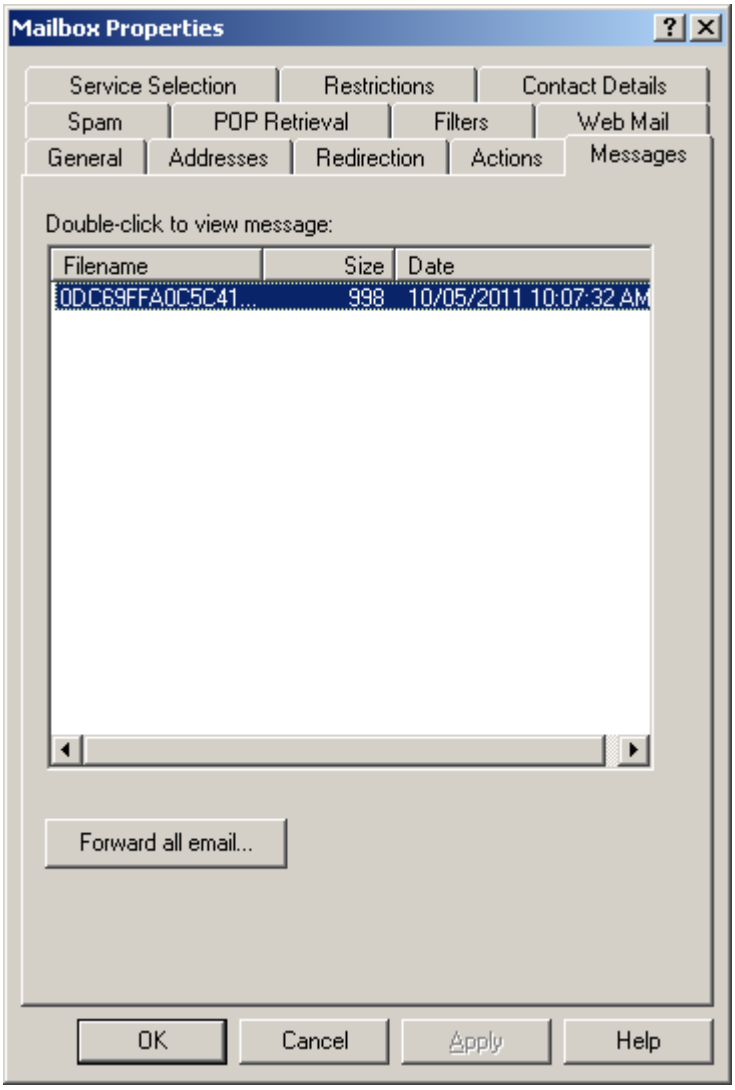


Setting	Description
Enable auto responder	Enabling this will send a message back to anyone who sends an email to the mailbox. The auto responder will not reply to a message marked as bulk or system generated. It is not possible to enable auto responders for the postmaster mailbox.
Only send responses 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.

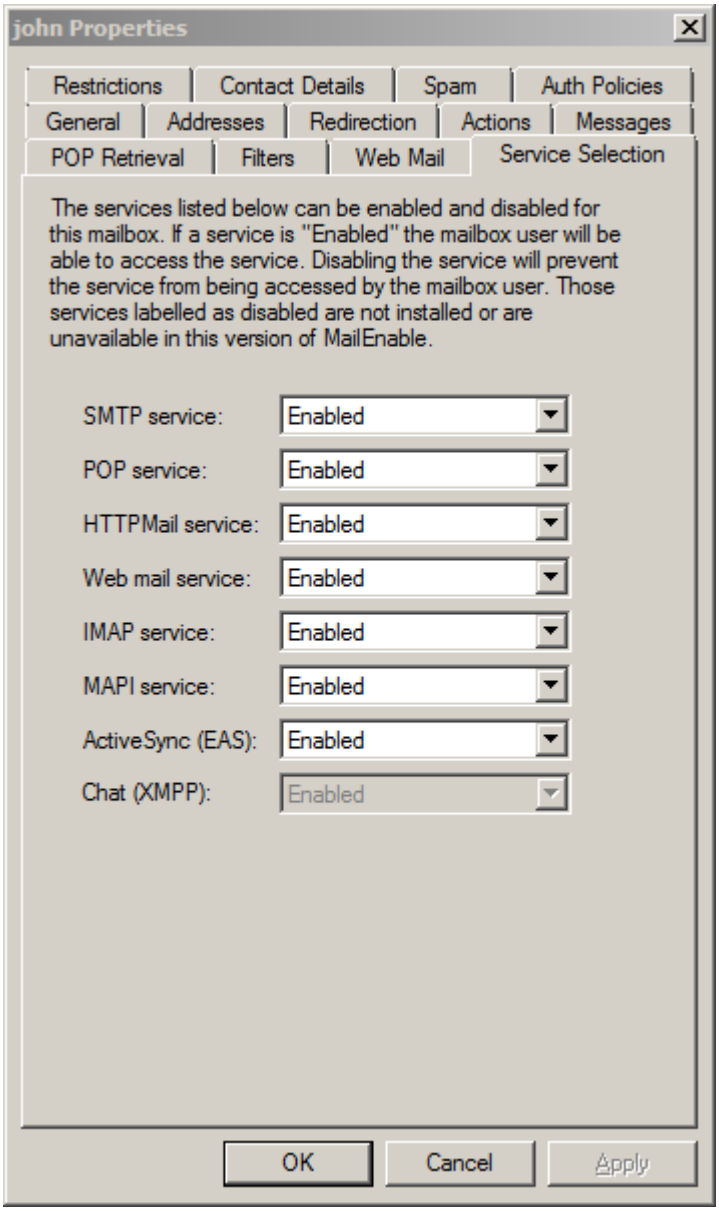


Setting	Description

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.
Request Search Reindex	Reindexes the search index for the mailbox. This operation can take a while depending on the number of messages in the mailbox.

5.5.8 Mailbox - Service Selection

The service selection tab allows you to enable or disable a mail service for a specific mailbox.

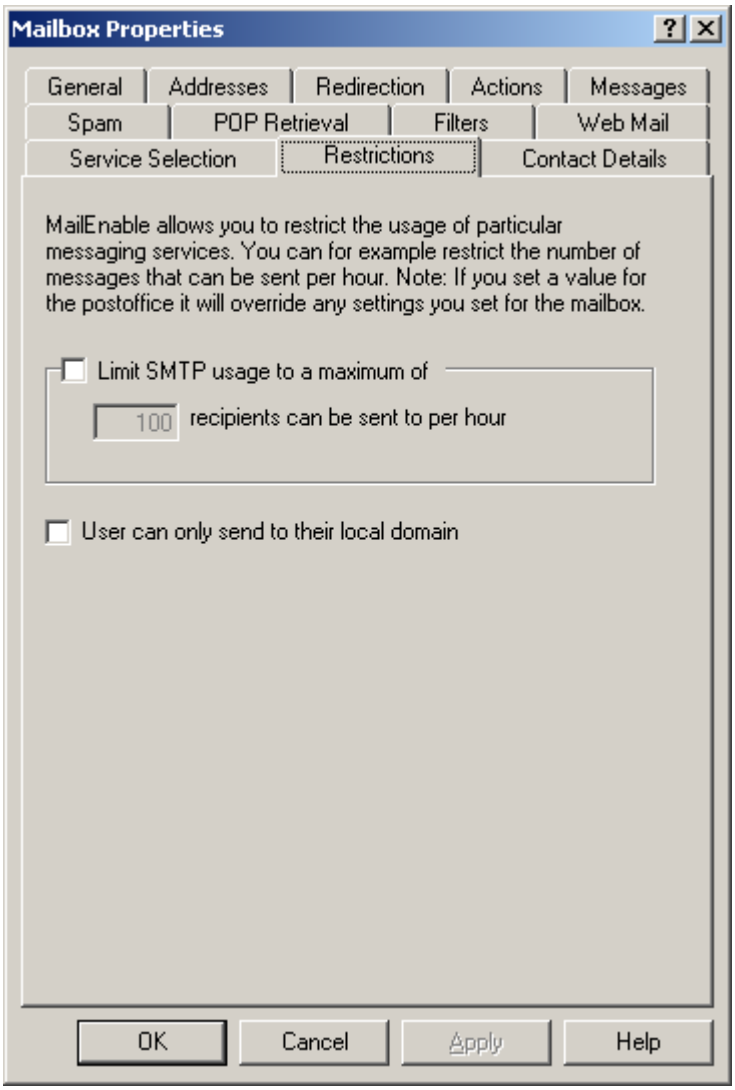


Setting	**Description**
SMTP Service	Enables or disables the SMTP service for this mailbox. Will prevent the mailbox from sending or receiving messages.

POP Service	Enables or disables the POP service for this mailbox.
HTTPMail Service	Enables or disables the HTTPMail service for this mailbox.
Web mail Service	Enables or disables the web mail service for this mailbox.
IMAP Service	Enables or disables the IMAP service for this mailbox.
MAPI Service	Enables or disables access with the Outlook Connector.
ActiveSync (EAS)	Enables or disables ActiveSync protocol.
Chat (XMPP)	Enables or disables access to the chat service.

5.5.9 Mailbox - Restrictions

Restrictions can be placed on the volume of messages sent per hour for a mailbox. Setting a value for a post office will override any values specified here for a mailbox.

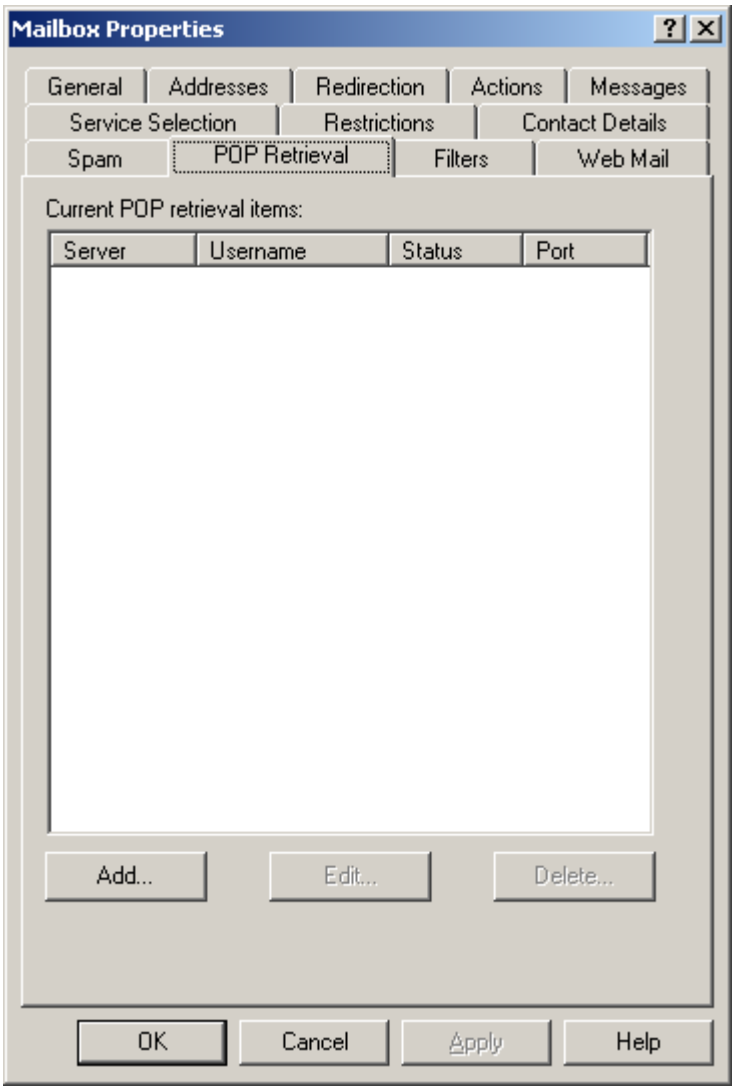


Setting	Description
Limit SMTP usage to a	Limits the maximum number of messages that can be sent using the SMTP service on an hourly basis. This setting is useful for throttling an account suspected of spamming.

maximum of:	
User can only send to their local domain	This enforces the mailboxes sender policy to only send messages to local mailboxes within their postoffice. If the option is greyed out then please see **Postoffice - Restrictions (Section 5.3.8)** on how to enable the sender policy at the mailbox level.

5.5.10 Mailbox - POP Retrieval

View remote or local mailboxes that have been configured for POP retrieval by the currently selected mailbox. The administrator can add and configure POP Retrieval from here, or a user may do so via the web mail interface, if permission to do so has been granted. If the feature is disabled in the Administration program only the administrator or accounts with access to Administration program can create a POP Retrieval account. See the **Web mail server configuration section (Section 6.18.2)** for more information on this setting.

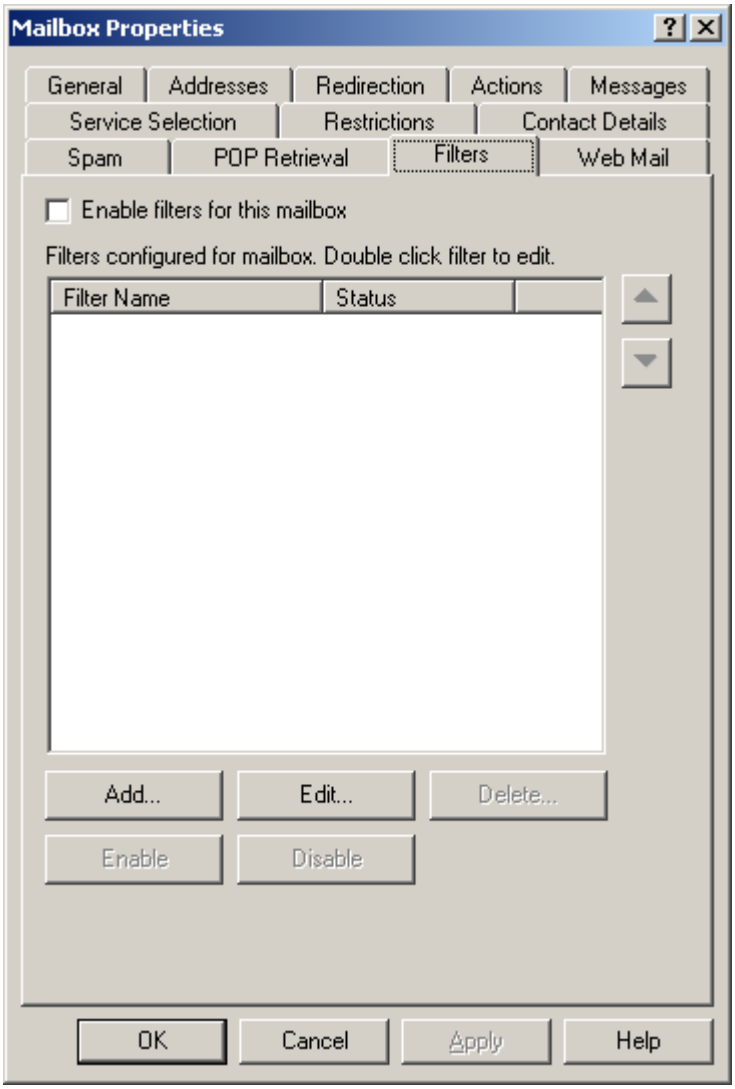


Setting	Description
Current POP retrieval items	Displays any remote or local mailboxes that have been configured to have their mail pulled down into this local mailbox.
Add Mailbox	The POP Retrieval service can connect to another mailbox and pull any mail in the mailbox into this local mailbox. This is useful to centralize mail receipt over many accounts and across many domains. To set up an account the following details are required;

Setting	Description
	Mail Server – This is the MX record or DNS name of the remote server e.g.. mail.mailenable.com **Port** – This is the port that is used to connect to the remote server. The default for this is port 110 **Username** – This is the username of the account. If it is a MailEnable mailbox this must be mailbox@postofficename **Password** – The password for the account. **This server requires APOP authentication** - APOP (Authenticated POP) is an extension of the standard POP3 protocol. Authenticating to a POP server will mean the username and password are both encrypted by the client before being passed "over the Internet". The receiving server must then be able to decrypt the password. **Only download new messages** (leave messages on server) – Will download messages leaving a copy on the server. **Enabled** – This setting allows the enabling or disabling of a POP retrieval service account. Disabling the account will retain the settings but will stop the account retrieving mail.

5.5.11 Mailbox - Filters

Enable, create and display mailbox filters.



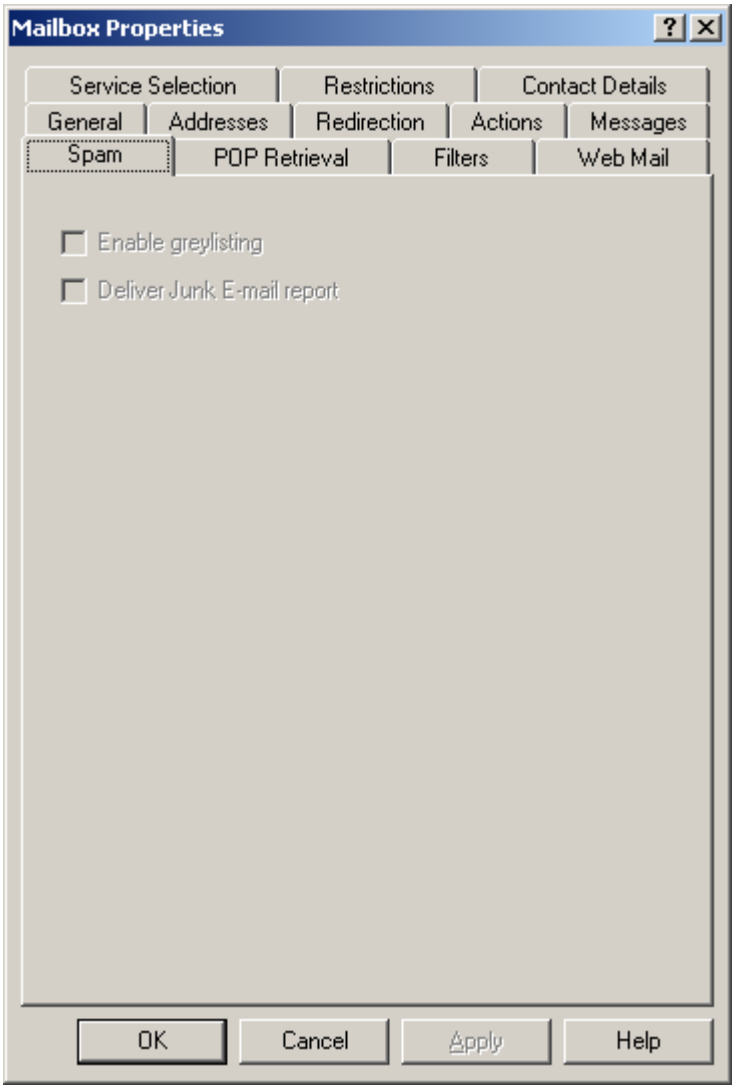
Setting	Description

Enable filters for this mailbox	Enables filtering for this mailbox only. Users also have the ability to edit their mailbox filters via the web mail interface. Please see the Web mail user guide for more information: https://www.mailenable.com/documentation/webmail/webframe.html
Filters configured for this mailbox	Displays the filters configured for the mailbox.
Add...	Adds a new filter.
Edit...	Opens the filter criteria and actions window when a filter has been selected in the list.
Delete...	Deletes a selected filter
Enable	Enables a selected filter
Disable	Disables a selected filter

Note: Please see **Mailbox Filtering (on-line documentation)** for more information

5.5.12 Mailbox - Spam

Various global spam options can be enabled/disabled under mailbox spam properties

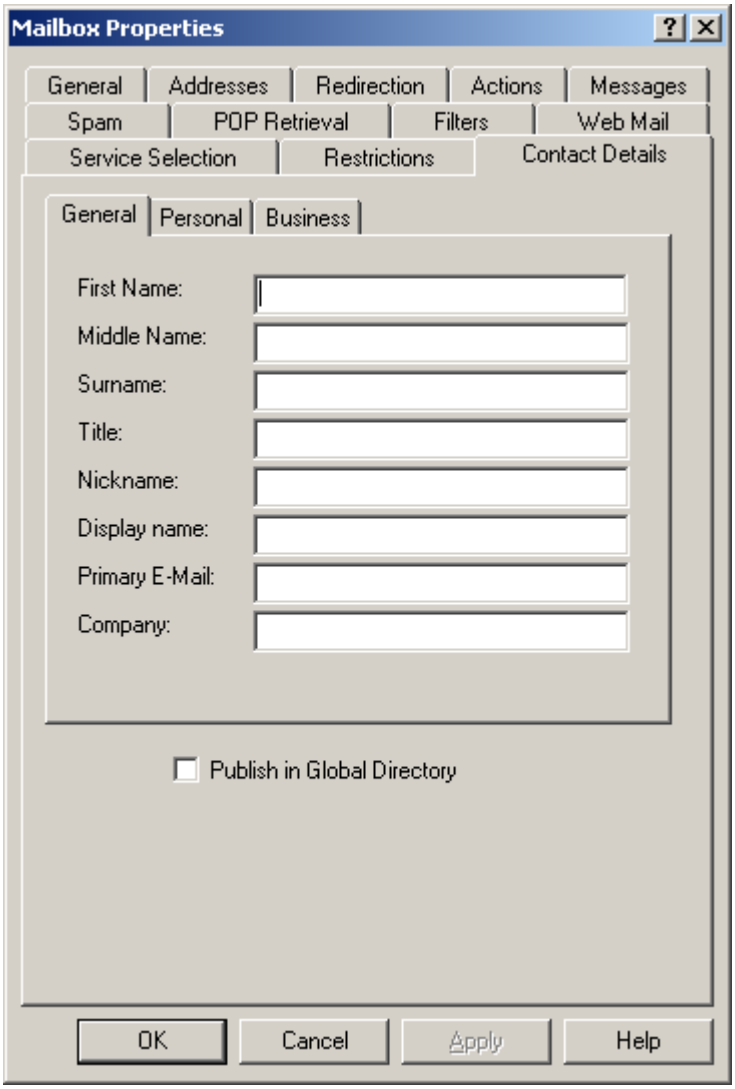


Settings	Description
Enable greylisting	When enabled enables greylisting for the mailbox. If greyed out please refer to **Postoffice - Feature selection (Section 5.3.10)**
Deliver to Junk E-mail report	When enabled will allow the report agent to deliver a Junk E-mail report for the contents of the users Junk E-mail. Please refer to the **Report - Agent (Section 6.6.7)** for more information

5.5.13 Mailbox - Contact Details

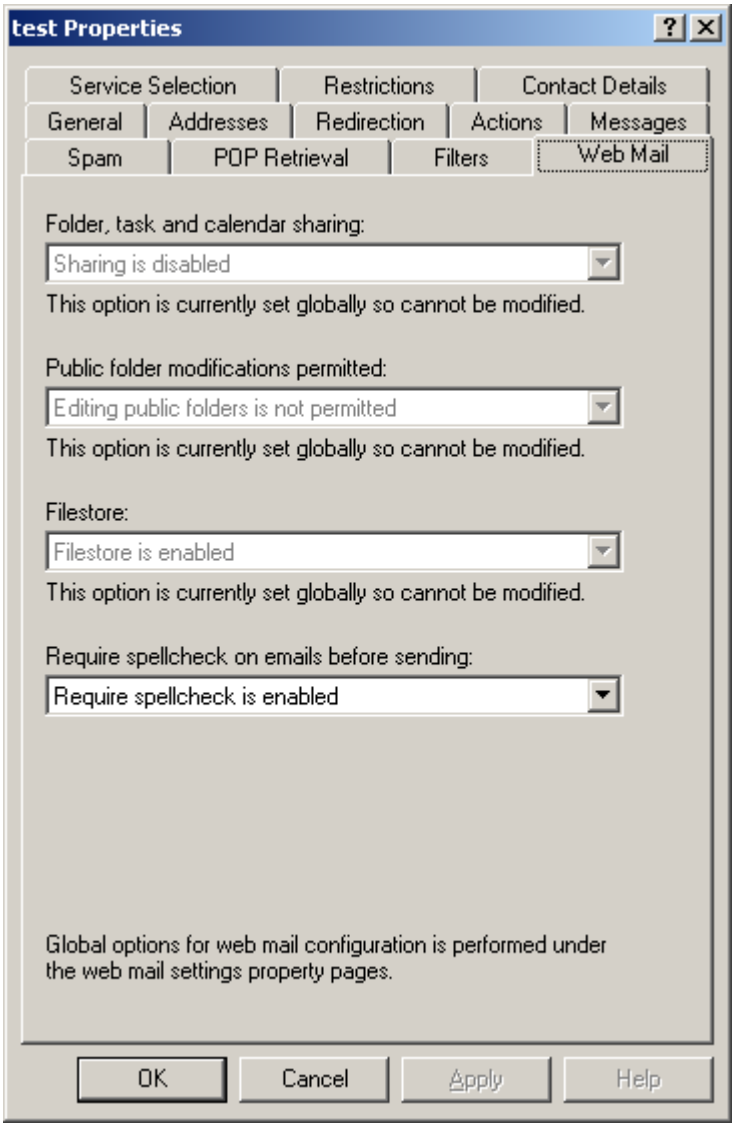
The Contact Details property tab stores contact details associated with the owner of the mailbox.

These contact details can optionally be published into the post office global address list for access by applications that use the global address list.



5.5.14 Mailbox - Web mail

These options provide mailbox level options for Web Mail. The settings on this tab can also be set at the global level under the **Web mail - Site Options (Section 6.18.2.3)**.



Setting	Explanation
Folder, Tasks, and Calendar Sharing	Enables Folder, Task and Calendar sharing for the mailbox. **Sharing is disabled:** Disables sharing for the mailbox. **Sharing is enabled:** Enables sharing for the mailbox.
Public Folder Modifications Permitted	Determines whether public folder is read only. **Editing of public folders is not permitted:** Disables Public Folders for the mailbox. **Editing of public folders is permitted:** Enables Public Folders for the mailbox.
FileStore (MyFiles)	This option enables the FileStorage option. **Filestore is disabled:** Disables File Storage for the mailbox. **Filestore is enabled:** Enables File storage for the mailbox.
Require Spellcheck on emails before sending:	This option determines whether messages need to spell checked before sending. **Require spellcheck disabled:** Disables the spellchecking before sending for the mailbox. **Require spellcheck is enabled:** Enables the spellchecking before

sending for the mailbox.

5.5.15 Mailbox - Auth Policies

Authentication restrictions allow you to limit authentication of mailboxes by country. This limitation can help avoid abuse and access to email data.

Setting	Description
Stop connections from the countries below authenticating. All other countries can authenticate.	This is used to select which specific countries are going to be blocked from authenticating. The blocked countries have to be individually selected.
Only connections from the countries selected below can authenticate.	This is used to select which countries are allowed to authenticate. All others will be blocked.
Countries	Select the countries that apply to authentication restrictions.
Allow E-mail addresses for usernames	By default, usernames for the mail server are formatted as mailbox@postoffice. In some cases you may wish to allow users to log in with mailbox@domain where domain is one of the domains associated with the postoffice.
Challenge	Two factor authentication means that users need to use two methods of authentication to log into their webmail account. **Never prompt** Two factor authentication is disabled **Prompt Always** Everytime a login is done in webmail, two-factor authentication is required. **Prompt For New IP Address** If the connection to webmail is from a different IP address than the last login, two factor authentication is required. **Prompt For New Country** If the connection to webmail is from a different country (determined by the last IP address) then two-factor authentication is required.
Address Type	There are two types of two-factor authentication methods available: **Google Authenticator (or other TOTP Client)** Google Authenticator or another TOTP client can be used for the two-factor authentication. If you select this option and it has not been configured before, then configuration is done on the first webmail login. **SMTP Address** An email is sent to an SMTP address with the required two-factor authentication code required for login.
Address	If you have selected SMTP Address for the address type, enter the SMTP address here.
Reset	If the mailbox has been configured for Google Authenticator or other TOTP client this will clear the settings for the user to configure it again.

5.6 SMS Addresses

5.6.1 SMS Addresses

An SMS address is an address that is mapped to a mobile phone number. Any messages received to that address are processed by the SMS connector. Please see **SMS connector (on-line documentation)** for more information about SMS configuration.

How to create an SMS address

1. Navigate within the administration console to: **MailEnable Management > Messaging Manager > Post Offices > (Postofficename) > SMS Addresses**
2. Right click on SMS and select: **New SMS address...**
3. Enter a phone number.
4. Set the email address that will be used for this phone number. Messages addresses to this email address will be converted to SMS and sent.
5. Click **OK** to save the address.

Note: Edit an existing address by double clicking on the address or right clicking on an address and selecting properties.

Note: To delete an address, right click on an address and select Delete.

5.7 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.

5.7.1 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**

5.7.1.1 How to add a group member

How to add a group member

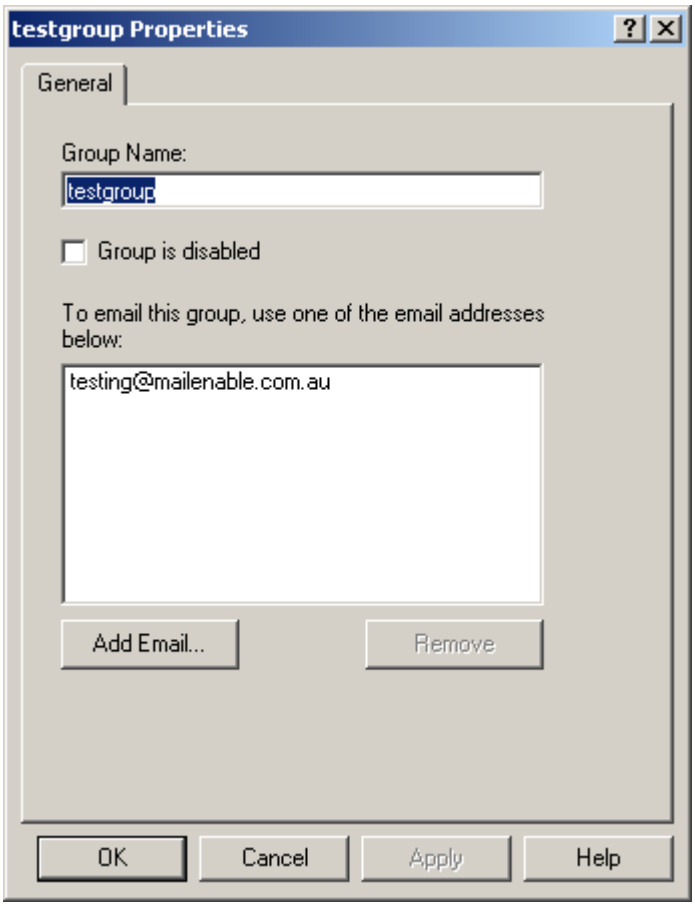
1. Navigate within the administration console to: **Messaging Manager > Postoffices > (postoffice name) > Groups > (Group name)**
2. Right click on the group name and select **New > Group Member...**
3. Specify an email address that is to be added as a group member. Alternatively click on the **Advanced**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

5.7.1.2 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.

5.7.2 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

5.8 Directory configuration

5.8.1 Directory

The directory for a post office is a list of email addresses and corresponding display name which is used for web mail as a global contact list. Web mail users will be able to see all the entries under the Global Group when viewing the address book. The address list is also available through the LDAP service.

The configuration of the directory is done through the **Messaging Manager > Post Offices > (Post Office) > Directory**. This can be right clicked on to add a new addresses. Right click an address and select properties from the pop up menu to edit an address.

Clicking the **Import Directory Entries** item from the action pane will allow you to populate this directory list from a text file.

5.9 Lists configuration

5.9.1 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.

5.9.2 How to create a list

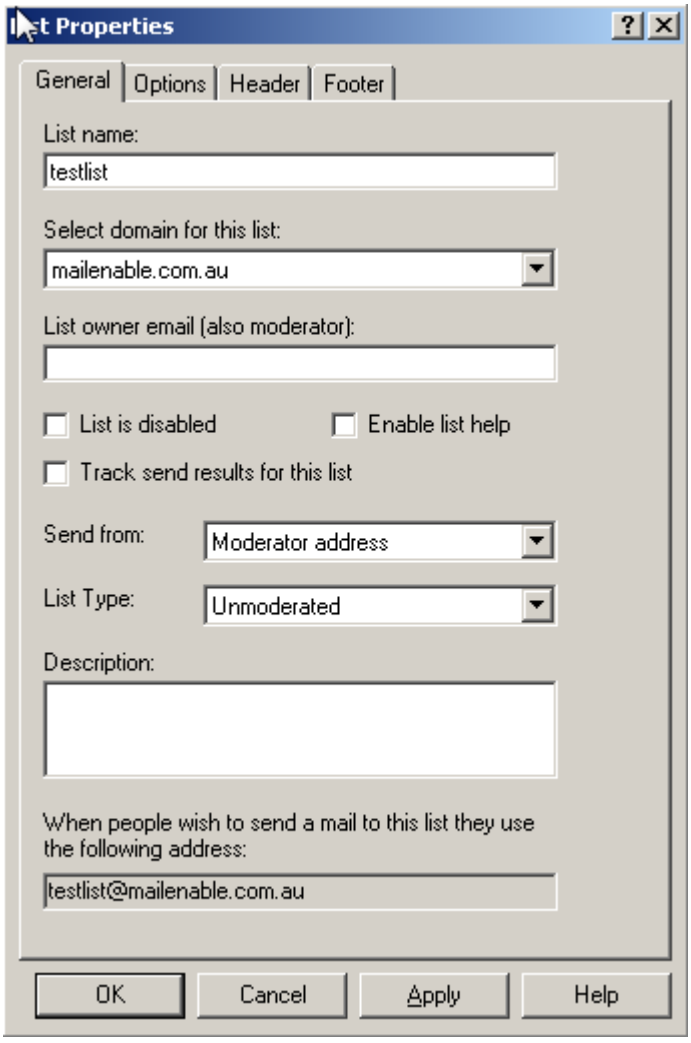
How to create a list

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.

5.9.3 Lists - General

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

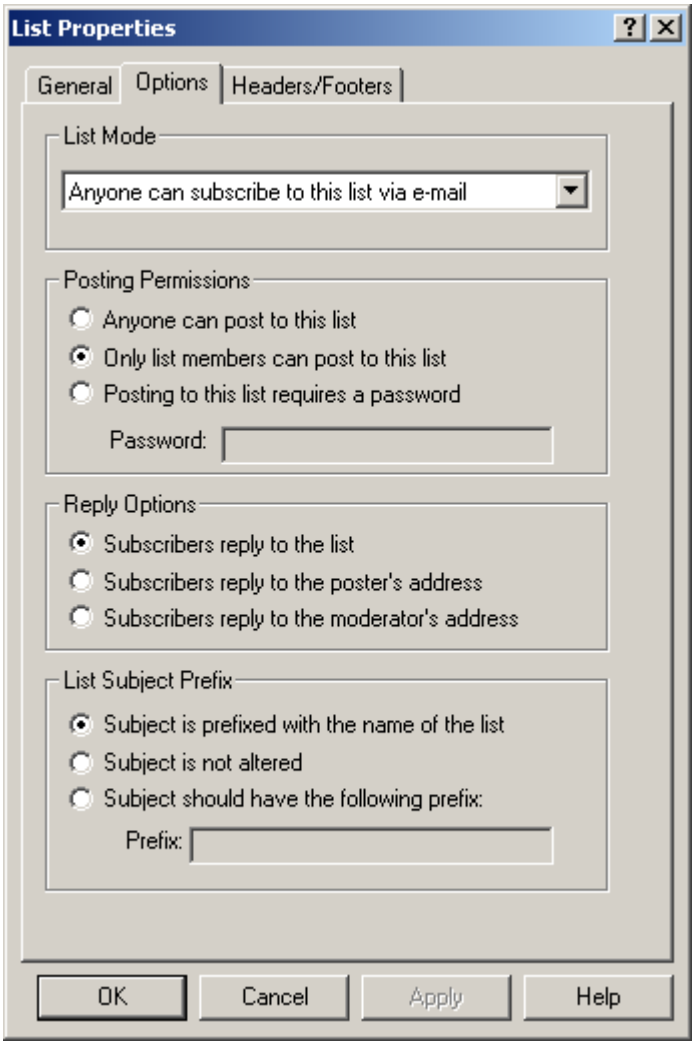


Setting	Description
List name	The name of the list. This determines the address that people email to in order to post to the list. The full email address for the list appears at the bottom of the General property page.
Select domain for this list	The domain used for the list name.
List owner email (also 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.
Track send results for this list	When enabled, the list server will track each email sent from the service to the list members. The results of the send are then available to web administration users.
Send from	Determines the From address which will be used for all emails coming from the list. This can be either the moderators email address or the list address. This does not determine where the reply goes.

List Type	Determines whether the list is moderated or not. If moderated, all incoming emails will be sent to the moderator email address. 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.

5.9.4 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.
List members come from datasource	You are able to configure a list to retrieve members from a database query. You cannot update members or view them in the administration. When you select this option you will be shown a Configure button that, when clicked, allows you to specify the details of the database lookup. As long as the query you enter returns the email address as the first column in the results, then the list service will use this for the member address.

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.

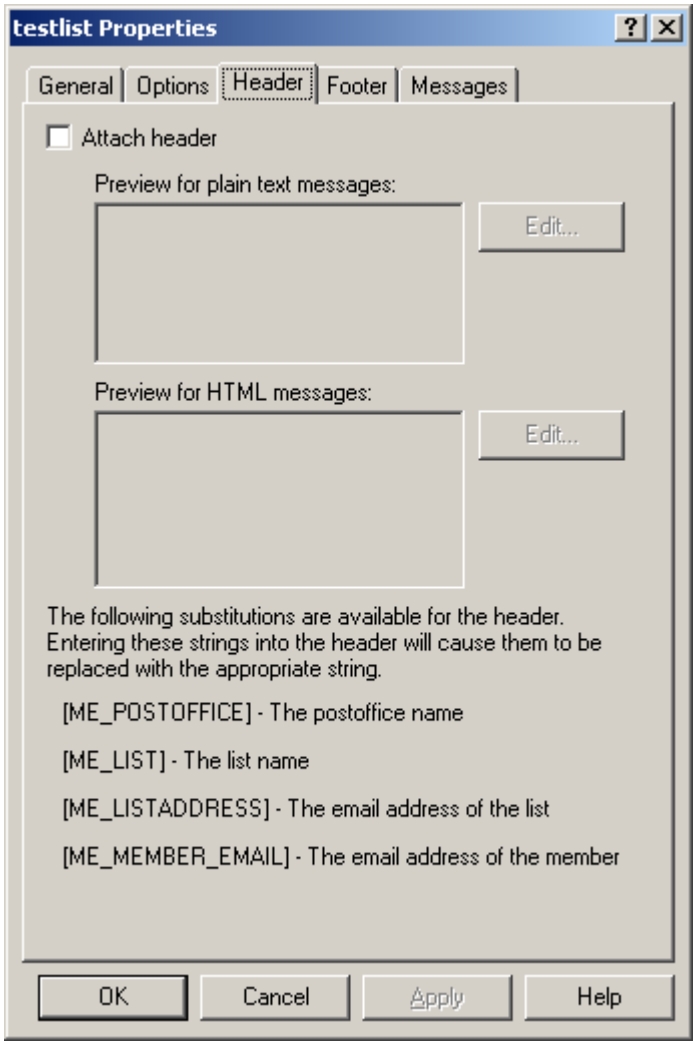
Setting	Description
Subscribers reply to the list	The reply to address is set to the list address, so when users reply to a message that gets sent from the list, their email gets sent to the list.
Subscribers reply to the posters address	The reply to address is set to the email address of the sender,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

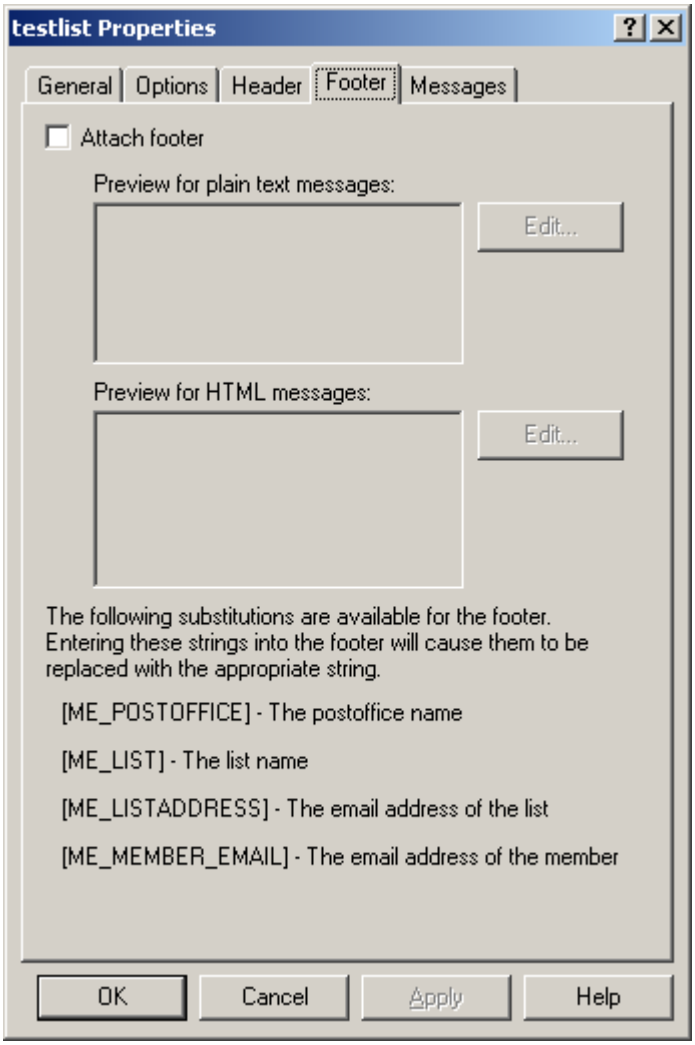
List subject prefix

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.

5.9.5 Lists - Headers and Footers





List Headers

Specify plain text or HTML headers for all list messages.

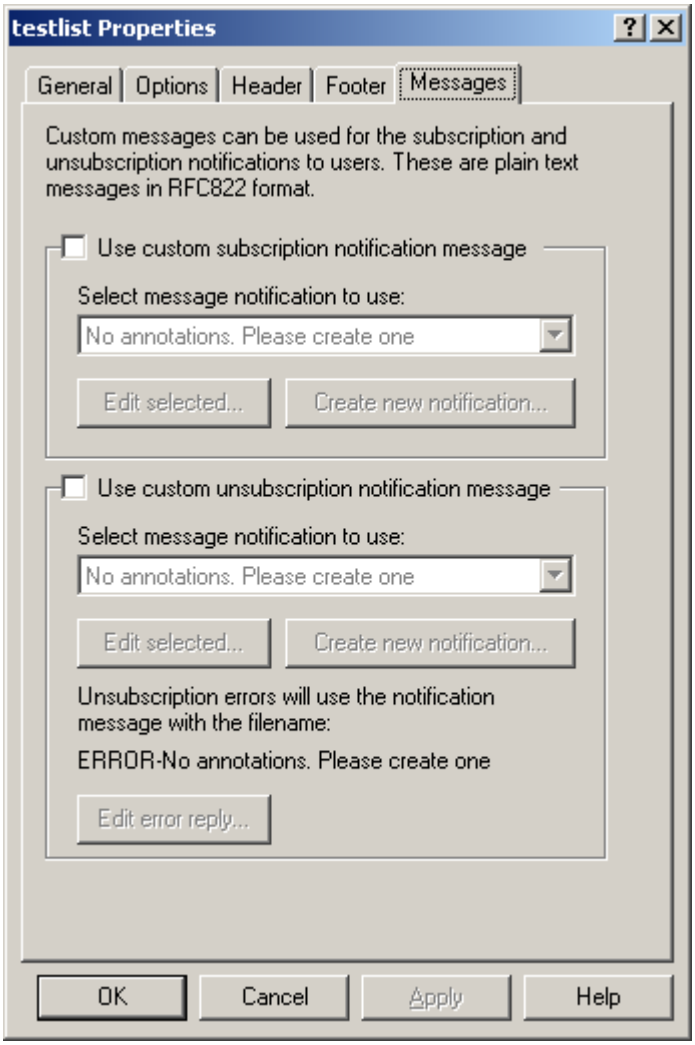
Setting	Description
Attach header	This text is added to the top of every email when the Attach header checkbox is selected.

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.

5.9.6 Lists - Messages



The Messages tab for a list allows the use of a custom messages for the subscribe notification message and the unsubscribe notification message. The files that can be used for this need to be located in the following path:

Mail Enable\Config\Post Offices\[Post Office]\Annotations

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

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

Setting	**Description**
[ME_MEMBER_EMAIL]	The member email address
[ME_POSTOFFICE]	The post office of the list
[ME_LIST]	The list name
[ME_LISTADDRESS]	The email address of the list
[ME_FROMADDRESS]	The moderator email address
[ME_TOADDRESS]	The list address
[ME_MESSAGEID]	The message ID formatted as <filename@localdomain>
[ME_DATE]	The current date/time

5.9.7 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**

5.9.8 List commands

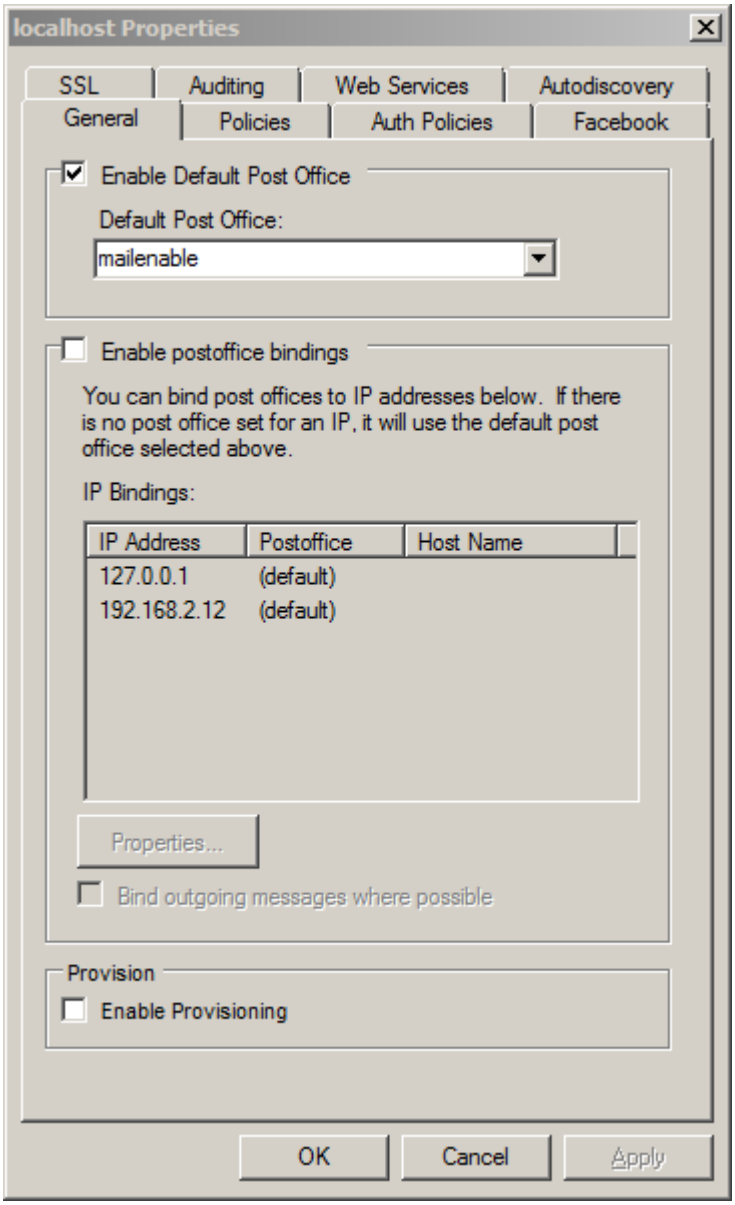
Users send commands to the list by putting the command in the subject line. The available commands for the list server are:

- **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

5.10 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.



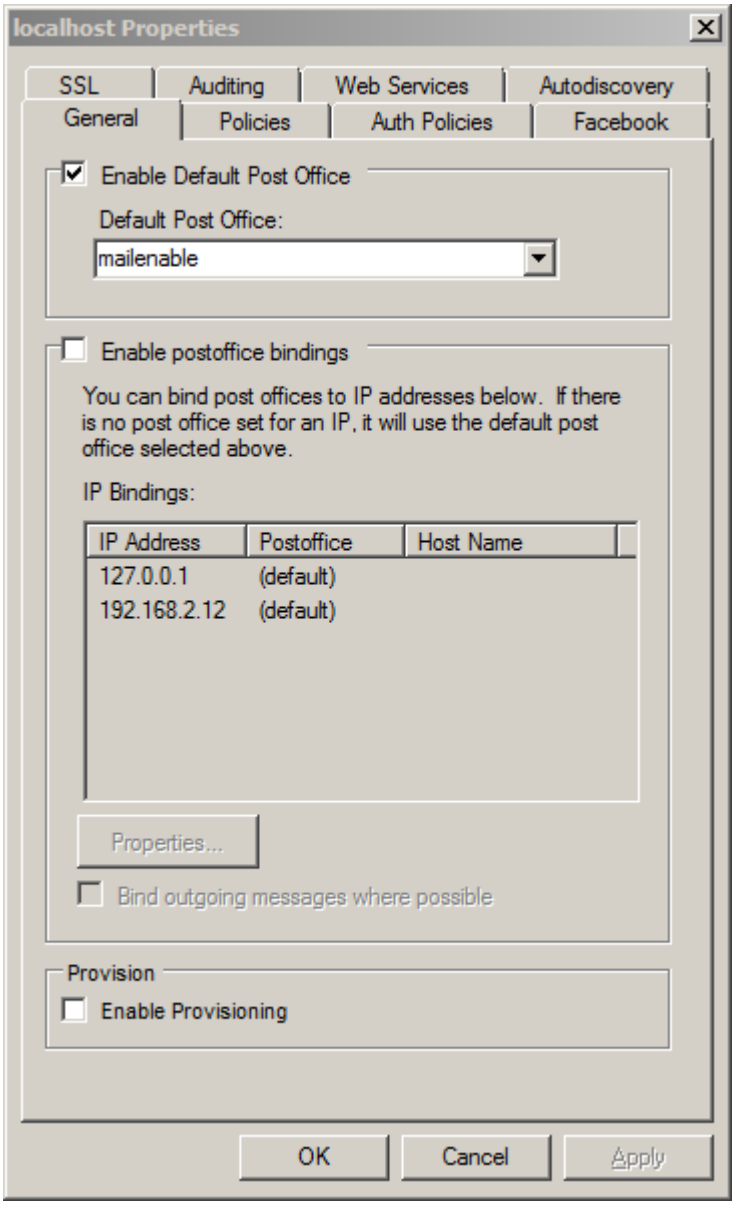
Setting	Description
Enable Default Post Office	Specify the default post office for your server. This means that any username that only has the mailbox name will be assumed to be from the default post office. E.g. the *sales@example.com* user will only need to use *sales* to log on with.
Enable post office bindings	It is possible to bind each MailEnable post office to a particular IP address on the network card. The advantage of this is: • Users only need to use their mailbox name to log-in if they connect to the bound IP address. • The SMTP welcome message when a connection is made to the server can indicate a domain for the postoffice. • The postoffice can have its own SSL certificate. • Outbound email can be smarthosted through a specific IP address. This is useful when you need to filter outbound email for a particular customer.
Bind outgoing messages where possible	Outbound emails for users of this postoffice will be sent through the bound IP address.

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)

5.10.1 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 post office bindings	It is possible to bind each MailEnable post office to a particular IP address on the network card. The advantage of this is: • Users only need to use their mailbox name to log-in if they connect to the bound IP address. • The SMTP welcome message when a connection is made to the server can indicate a domain for the postoffice. • The postoffice can have its own SSL certificate. • Outbound email can be smarthosted through a specific IP address. This is useful when you need to filter outbound email for a particular customer.
Bind outgoing messages where possible	Outbound emails for users of this postoffice will be sent through the bound IP address.
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)

5.10.2 Localhost - Policies

The Policies tab provides settings to lock out users after too many failed password attempts and prevent users from entering simple passwords.

Setting	**Description**
Lock out user for one hour after	Keeps track of mailbox authentication failures per hour. When the number of failed attempts is reached, from any mail service, the mailbox will be locked out for 1 hour. Valid authentication attempts do not affect the number of attempts. You are able to unlock a mailbox by opening its properties in the administration program - if it is blocked a button will be shown allowing you to unblock. This lock out option does allow invalid users to lock out valid users from their account (by trying incorrect credentials). Valid users can also lock themselves out if they try to authenticate with the incorrect password. Because of these two limitations it is recommended to avoid this option and use the **Enable Abuse Detection and Prevention** option instead.
Enforce password policy	When an administrator creates an account or a user changes a password, the password must meet the password complexity requirements that are enabled. Existing passwords are not affected by enabling this option. So if you have users with a simple password they will still be able to log in. Use the **Check existing passwords** button to find these mailboxes. There are some policies which are always enforced on password changes when this option is enabled. These are: • Passwords cannot include the mailbox name or the postoffice name. • Password cannot include the word **password**. • Password cannot be **pass** or **test**.

	Other password policies are then enabled as you wish. You can use the **Check existing passwords** button to produce a list of all the mailboxes which fail to meet the password requirements.
Enable abuse detection and prevention	IP addresses will be temporarily blocked if they appear to be trying to guess a password. Blocked IP addresses will be held in cache memory for hour. In order to release the blocked IP's from memory the respective service needs to be restarted, or the **Unblock IP Address** button can be used to remove an address. If an IP address is whitelisted under the SMTP options then it will not be blocked. If an IP address is just trying to use the same username/password over and over it will not be blocked, as it is just assumed to be an incorrectly configured client account.
Sender Policy dropdown	**Users can send to local and remote addresses:** Allows users to be able to send to local mailbox addresses hosted locally within MailEnable and to send to external addresses hosted on remote mail servers. **Users can send to local addresses only:** Allows users to only be able to send to local mailbox addresses hosted locally within MailEnable **Sending policy determined by postoffice:** Sets the sender policy to be determined the postoffice restriction settings. Please see **Postoffice - Restrictions (Section 5.3.8)**

5.10.3 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.

The Enterprise version of MailEnable also supports configuring an SSL certificate per IP address. This is configured under the IP bindings. The services will still try to use the certificate requested by the client, but instead of falling back to the default certificate, they will use the one allocated to that IP address.

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

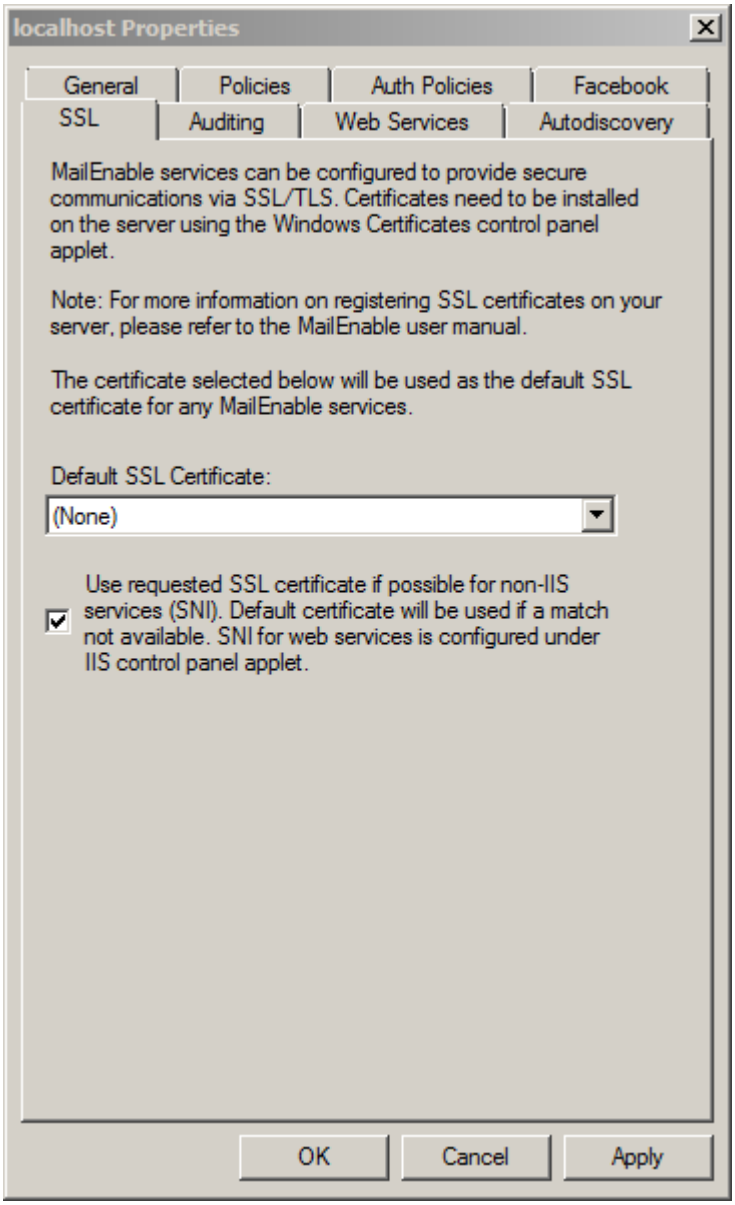
This application can be used to review and import SSL certificates into the various SSL certificate containers on

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.

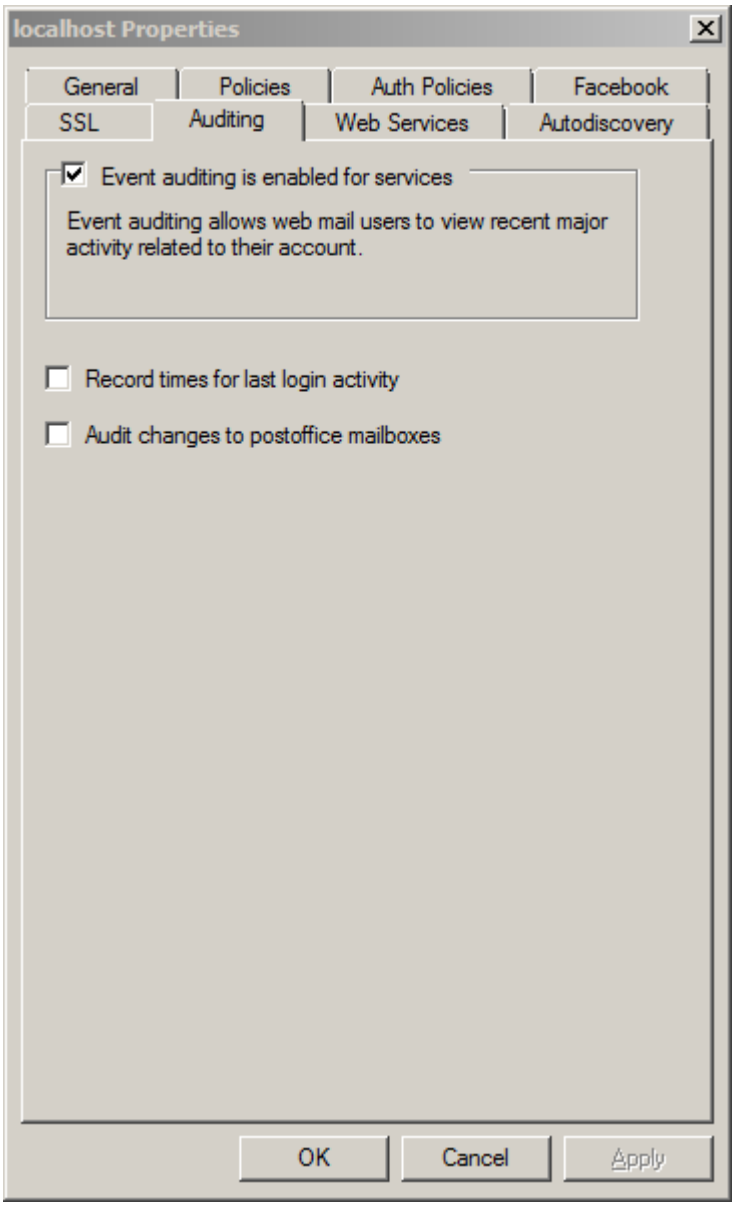


Once certificates have been registered on the server, you still need to configure which services make use of it. So under the services and connectors configuration you may wish to add an SSL port, or enable TLS support.

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.

5.10.4 Localhost - Auditing

Auditing logs various server activity to .



Setting	Description
Event auditing is enabled for services	Event auditing allows users to see activity on their mailbox through their webmail client interface. Items logged are activities like email deletion, moves, delivery, etc.
Record times for last login activity	When a user authenticates, a file is written into the directory below, indicating whether the login was successful or not: Config\Postoffices\[postoffice]\mailboxes\[mailbox]\Login-Success.txt for a successful login and Config\Postoffices\[postoffice]\mailboxes\[mailbox]\Login-Failure.txt for a failed login The last modified date of the file indicates the date/time of the login attempt. When event auditing is enabled. the mailbox properties page will indicate the last login time.
Audit changes to postoffice	Adds, edits and deletes of mailboxes using the API (which includes the administration program and 3rd party scripts or programs) are logged for each postoffice. The log file is

mailboxes	located at: Config\Audit\[postoffice] It is a text file with the name AUDIT-YYMMDD.log It contains the data and time of the mailbox change, the change made, and the mailbox name. The change in the log file is represented by numbers, so [111.5] is a mailbox creation [112.5] is a mailbox deletion [113.5] is a mailbox edit (an edit is where the mailbox name, redirection, quota or status is edited)

5.10.5 Localhost - Auth Policies

The server authentication policies allows you to restrict login attempts to any mail service to specific countries. The connecting IP address is checked against a country database and will either be blocked or allowed to perform a login attempt. This option can increase security by restricting all login attempts to within your own country.

Setting	Explanation
Enable location services for filtering and authentication	Enable this so that emails will be marked with location for filtering and authentication.
Enable country authentication restrictions	Country login restrictions are able to be set on a global, postoffice or mailbox level. You are able to set this to be global for all logins, or allow postoffices to configure their own country settings.
Stop connections from the countries below authenticating. All other countries can authenticate.	There are two modes available for determining whether a person in a country can authenticate. You can either block specific countries or allow specific countries. Selecting this option allows you to block individual countries.
Only connections from the countries selected below can authenticate.	Select this option when you just want to select the countries that are able to log in.
Countries	This is the country list where you can select which countries apply to the above settings.
Allow valid postoffice domain aliases in usernames	By default users have to authenticate using mailbox@postoffice. This option allows users to use any of the domains mapped to their mailbox as well as postoffice name. So if a mailbox called 'john' is under a postoffice that has two domains example1.com and example2.com then they can use either john@example1.com or john@example2.com as their username.

5.10.6 Localhost - Web Services

MailEnable Web Services allow remote programs to configure the MailEnable Messaging Platform. The Web Service allows mailboxes to be created and managed. Tools that support making SOAP calls can be used to remotely access the server via the Web Services interface.

By default accessing the web services requires a username and password. These credentials are for any mailbox which has been configured as SYSADMIN. If you double click a mailbox in the administration program to view the mailbox details, you can select SYSADMIN as mailbox type. Only system administrators should be set as this level, as it allows that mailbox to edit the MailEnable configuration, through web admin or web services.

Web services are accessed through Microsoft IIS, under the MailEnable Protocols website. If you run the IIS

Manager on the server you will see the MailEnable Protocols site, and configure a host name for it to make it easier to access. When you access the web services, this is done under the WebServices directory, and the available page names are below, which map to MailEnable objects:

https://MEProtocols.localhost/webservices/AddressMap.asmx

https://MEProtocols.localhost/webservices/Directory.asmx

https://MEProtocols.localhost/webservices/Domain.asmx

https://MEProtocols.localhost/webservices/Group.asmx

https://MEProtocols.localhost/webservices/GroupMember.asmx

https://MEProtocols.localhost/webservices/List.asmx

https://MEProtocols.localhost/webservices/ListMember.asmx

https://MEProtocols.localhost/webservices/Login.asmx

https://MEProtocols.localhost/webservices/Mailbox.asmx

https://MEProtocols.localhost/webservices/PostOffice.asmx

https://MEProtocols.localhost/webservices/SystemOptions.asmx

You can access the pages in a web browser to get more information about what options are available. For further details through, please see the MailEnable API documentation, as you may have to do multiple calls to do the one task. For example, creating a mailbox requires a login to be created, a mailbox, and any address maps.

5.10.7 Localhost - Autodiscovery

Autodiscovery is where email clients are able to easily able to determine the settings for an email account just by the email address and password of the user. Using the domain in the email address they request what server settings are required for the client. Microsoft Outlook supports this for configuring IMAP/SMTP accounts and most mobile devices support this for ActiveSync configuration. When using autodiscover for Microsoft Outlook it will only be able to determine the settings if the postoffice name matches the domain name of the email address, as it has to authenticate.

Setting	Explanation
Enable iOS publishing for this server	Enabling this will display a link on the webmail login page for iOS users that will allow them to have their email accounts automatically configured. When users click the link on an iOS device it will prompt the user which services to configure and then transfers these settings to the client.
Automatically detect Autodiscovery settings	If the domain for the user does not have autodiscovery settings, this will will use the current server settings to build the autodiscover information for the iOS device.
Remove	Removes the currently selected protocol setting for autodiscovery.
Edit	Edits the currently selected protocol setting for autodiscovery.
Add	Adds another service settings for autodiscovery.
Detect	This will create default autodiscovery settings which match how the mail services are configured. This can be used as a starting point for further editing.

5.10.8 Localhost - Facebook

Facebook authentication allows you to login into webmail with just a click, if you are already logged into

Facebook. This can make logging into webmail a lot easier, especially for mobile users. In order for Facebook login to work you need to have a Facebook developer account.

Setting	Description
Facebook Status	Enables Facebook login for the selected postoffice. It is possible to configure the feature per postoffice.
Facebook Application Id	The Facebook application ID for this postoffice. The host header you have configured for this postoffice needs to be configured under your Facebook developer login.
Facebook Application Secret	The Facebook Application Secret for this postoffice.

5.11 Advertising and Campaign Management

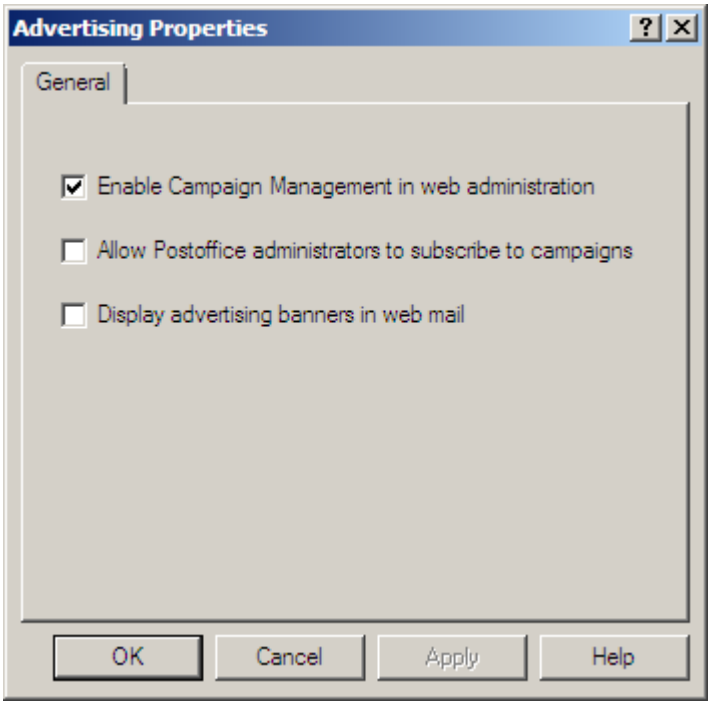
MailEnable's Web Administration interface allows administrators to enable advertising for their Web Mail customers. The advertising feature allows banner adds to be presented either server wide, or at a postoffice level. System Administrators are able to logically group advertising material into Campaigns. They can control the frequency of banner rotations and the designated click through URL. System Administrators and Postoffice Administrators can then select which campaigns they would like to distribute to users.

Please refer to the Wed Administration user guide at the following link on how to setup Campaigns and Advertising banners for web mail:

5.11.1 How to enable campaign management

How to enable Campaign Management for the Web administration interface

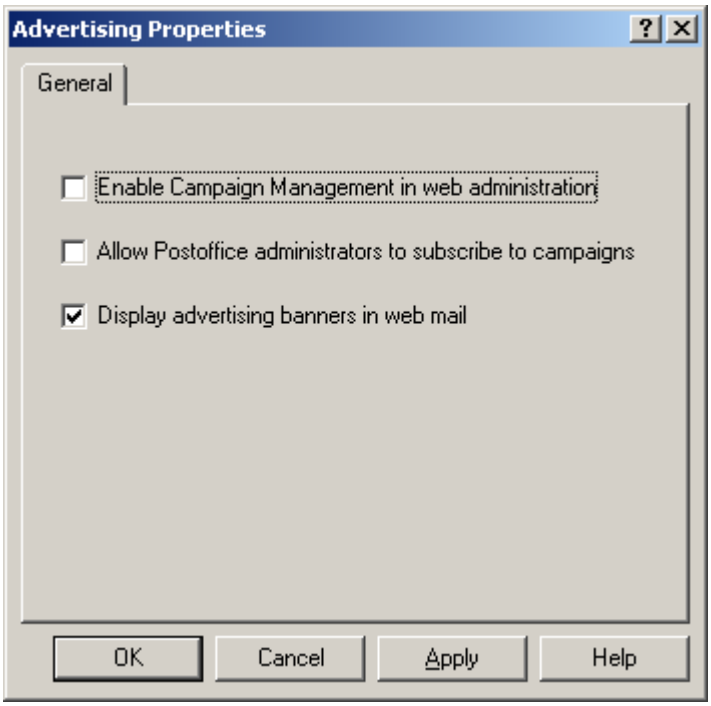
1. Navigate within the administration console to the following location: **MailEnable Management > Servers > localhost > Extensions > Advertising**
2. Right click on **Advertising** and select **properties**
3. Tick the option **Enable Campaign Management in Web Administration**



5.11.2 How to enable Advertising banners in web mail

How to enable Advertising banners for the webmail interface

1. Navigate within the administration console to the following location: **MailEnable Management > Servers > localhost > Extensions > Advertising**
2. Right click on **Advertising** and select **properties**
3. Tick the option **Display advertising banners in web mail**



5.12 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 ActiveSync

Overview
Exchange ActiveSync (or EAS as it is commonly abbreviated) allows mobile devices to synchronize Appointments, Contacts, Tasks and E-Mail over the Internet. EAS is the premium solution for rich messaging and collaboration on mobile devices. MailEnable's implementation of the Exchange ActiveSync protocol is implemented through Microsoft IIS and MailEnable's Synchronization/HTTPMail Service. By default, MailEnable provides ActiveSync connectivity on port 8080 and also installs a special Web Site under IIS called MailEnable Protocols. The MailEnable Protocols site provides Autodiscovery and ActiveSync through host headers to any IP addresses that are bound to IIS.

Please see the documentation at the following URL for more details on how to configure ActiveSync:

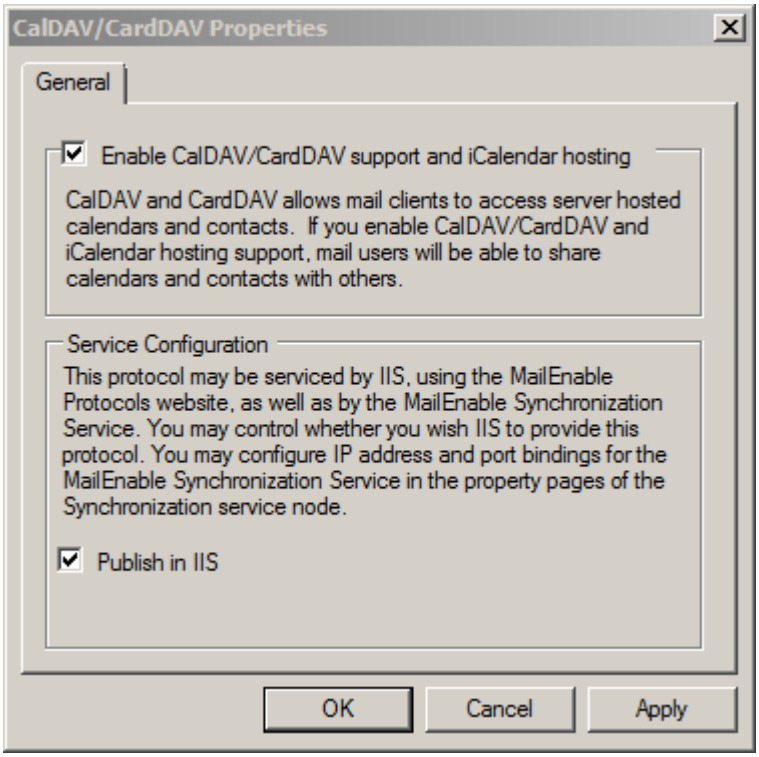
https://www.mailenable.com/references.asp

6.2 CalDAV/CardDAV

MailEnable's Synchronization Service provides both CalDAV and CardDAV protocols. These standard protocols allow email clients to access mailbox calendars and contacts. To access either the calendar or contacts the client is configured with a URL. It is also possible to configure the clients to access another user's calendar or contacts by specifying their username in the URL, provided you have been given access.

How to Enable CalDAV/CardDAV

1. Expand the following location within the administration console: **Servers > localhost > Services and Connectors**
2. Right click on **CalDAV/CardDAV** icon and select Properties from the popup menu
3. Select the option **Enable CalDAV/CardDAV support and iCalendar hosting**
4. If you wish to use Microsoft IIS to provide CalDAV and CardDAV services, then enable the **Publish in IIS** checkbox



Option	Description
Enable CalDAV/CardDAV support and iCalendar hosting	This enables the CalDAV and CardDAV protocols.
Publish in IIS	These protocols can be accessed by connecting to the synchronisation service directly, or through IIS. When you access the service directly, it is usually using a port number other than port 80 in order to avoid conflicting with IIS. When you enable this option it allows you to access the protocols through the **MailEnable Protocols** website which is configured under IIS. This gives more flexibility, as you can have multiple host names, SSL certificates, access over port 80/443, etc.

6.2.1 CalDAV and CardDAV configuration

CalDAV and CardDAV services are accessed via a URL by a client application. Clients can determine the correct server and port to connect to via DNS SRV records, so it is recommended, where possible, to add these to your DNS to make discovery for users easier.

CONFIGURING DNS INFRASTRUCTURE

This involves creating specific SRV DNS records so that they are published to clients.

For CalDAV you should configure the following SRV records for CalDAV (non-SSL and SSL), and CardDAV (non-SSL and SSL):

```
_caldav._tcp     SRV 0 1 8008  example.com.

_caldavs._tcp    SRV 0 1 8443 example.com.

_carddav._tcp     SRV 0 1 8008  example.com.
```

_carddavs._tcp SRV 0 1 8443 example.com.

Note: In the above example, you should also have a DNS A (Host) record for "example.com" that points to the IP address of the mail server. If you are running CalDAV and CardDAV over IIS, then you will need to configure the URL and ports and SSL certificate appropriately under the Windows IIS administration applet.

More information can be found at:

https://tools.ietf.org/html/rfc6764

Important: The Apple Calendar client will use port 8443 by default. If you are having issues connecting from a client, it is suggested that you consider running the server on port 8443 for SSL and 8008 for non-SSL.

6.2.2 Integrated Mailbox Calendar

Integrated mailbox calendars allows you to access the personal calendar for a mailboxes. Either the iCalendar publishing method or CalDAV can be used to do this.

If using the iCalendar publishing/subscribing method, each time an update is done all the appointments are redone on the server. This will overwrite any appointments which are added outside the client uploading the iCalendar file. Microsoft Outlook supports iCalendar, it does not support CalDAV.

Using a more intelligent client, which can use the CalDAV protocol, allows changes made in the client to be applied to the calendar in real time. i.e.: If you make changes to a calendar via CalDAV, only the change is sent up to the server and applied.

A variety of permissions can be configured for accessing calendars via CalDAV, and these are set in the webmail options, under the Shares, by setting the permissions on the Calendar folder (similar to how you would configure permissions for other webmail users).

The following table lists URLs used for connecting to mailbox calendars via CalDAV:

URL	Meaning
http://server:port/calendar	Connects to a mailbox calendar via CalDAV. You will need to supply a username and password of the mailbox being accessed.
http://server:port/calendar/mailbox@postoffice/calendar	Connects to a specific mailbox calendar via CalDAV. Authentication may not be needed depending on the permissions the mailbox user has set.

Note: If you are accessing your own calendar, you can omit the Mailbox@Postoffice portion as the mail client will prompt for credentials and will use the credentials to identify the associated mailbox calendar.

6.2.3 iCalendar Hosting

Note: Publishing an iCalendar is used when you wish to share a calendar to external users, who may not authenticate. If you wish to sync your calendar with an email client you are best to use CalDAV.

Publishing an iCalendar file allows a mail user to take a local calendar and push the entire contents of the calendar to the MailEnable server, as a hosted file which is accessible by various clients. Whenever the user makes a change to the calendar, the client application uploads the entire calendar to the server. Thunderbird (with the Lightning extension) and Microsoft Outlook can be configured to automatically re-publish the calendar to the server whenever you make changes to a local calendar. They can also periodically update themselves with a copy of the calendar from the server.

When a client makes a change to the published calendar, the mail client will fetch the entire calendar from the server, applies the change and then upload the modified calendar to the server.

A mailbox owner can publish multiple calendars and these calendars are able to be accessed as hosted iCalendar (.ics) files by e-mail clients. The owner of the mailbox is able to see the list of published calendars by logging into webmail and viewing the Shares under Options. Published calendars will appear under the Calendar folder in

the list of shares. The mailbox user can delete these items if needed, or they can be removed by the client application which uploaded it.

Published calendars are by definition available for read by the public. You can control the level of access for public users under the **Options | Shares** menu of the MailEnable WebMail client. The level configured affects all uploaded iCalendar files. Anyone providing the correct username/password for the mailbox will be given full access.

The following table lists URLs for connecting to mailbox calendars. Be aware there is a lot of difference in how clients use URLs, so this should only be used as a overview, and you should see specific documentation for each email client for correct usage.

URL	Meaning
http://host:port/calendars/mailbox@postoffice/calendar1.ics	Connects to a specific iCalendar file in a user's mailbox. In this case the file is calendar1.ics.
http://host:port/calendars	Connects to a users calendar. The server determines which user by requiring that the client application authenticate using the mailbox details. Be aware that some clients cannot authenticate to do this, such as Microsoft Outlook.

Note: When publishing or accessing a calendar, the reason you can omit the MailboxName@Postoffice portion is because the mail client will prompt for credentials and will use the passed credentials to identify the associated mailbox calendar.

6.3 IMAP Service

6.3.1 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.

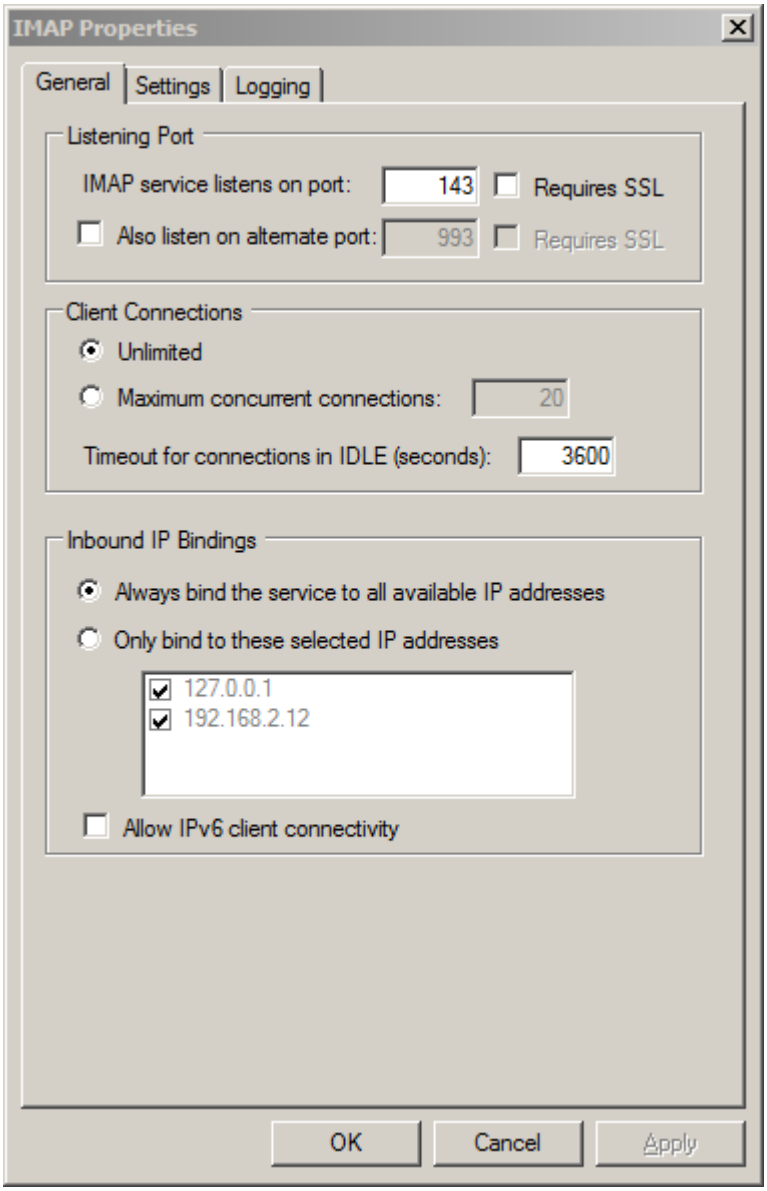
IMAP has distinct advantages over POP because it allows management of multiple folders on the server. Mail can be accessed from different machines, as the mail is hosted on the server (unlike POP which deletes mail from the server after being accessed) and allows the user to just download message headers 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.

6.3.2 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.

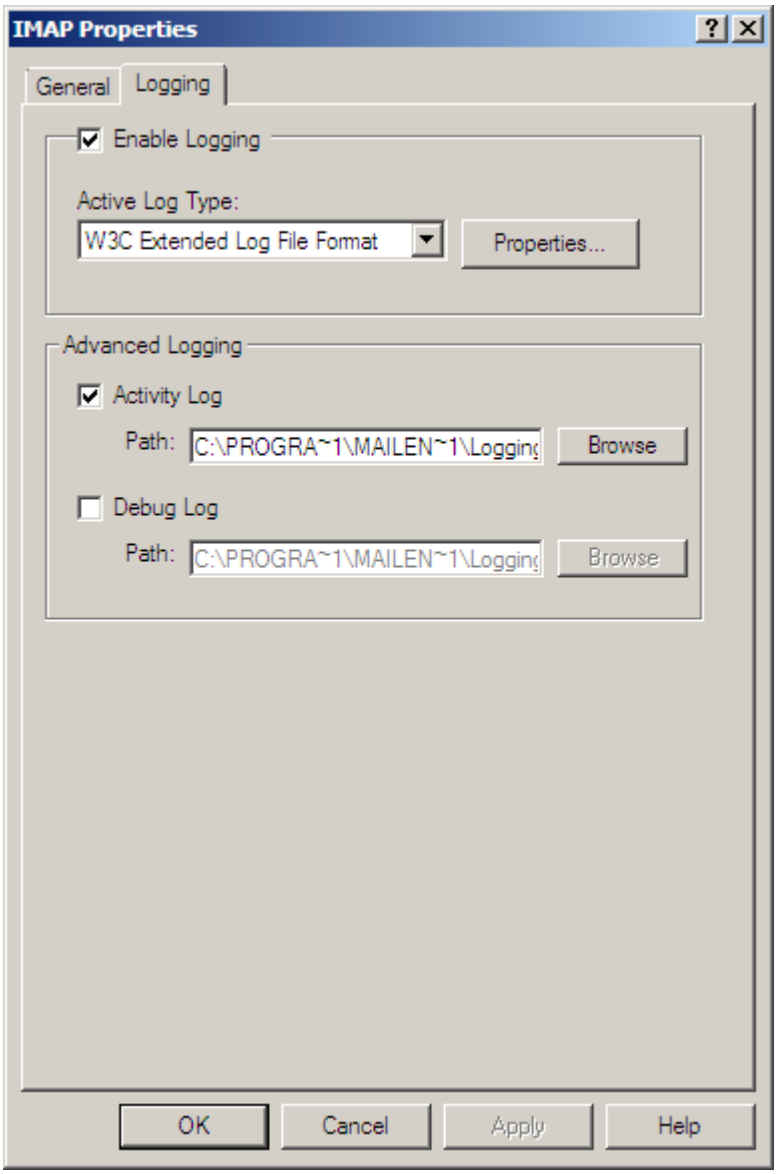
Timeout for idle connections	If this setting is enabled and a client connection has not passed any commands to the server for the set period of time, the connection will be dropped by the server.
Inbound IP Bindings	It is possible to select the IP addresses that the POP service will be bound to. On a 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.

6.3.3 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.
Enable public folders	Public Folders allow one or more mailboxes under the post office to share data (messages in a folder that is seen by all mailboxes in the post office.) Anything placed in this folder (Program Files\MailEnable\Post Offices\[Post Office Name]\Pubroot) will become visible to all other mailboxes in the post office. This feature must be enabled for the post office in Post Office Properties.
Advertise mailbox quotas to IMAP clients	This will inform IMAP clients what the quota is for the mailbox. Some clients, such as Thunderbird, will show this to the user. This does not enforce the quota though, so a client may ignore this or not support it. The **Enforce mailbox quotas** option is required still in order

	to stop them going over quota.

6.3.4 IMAP - Logging

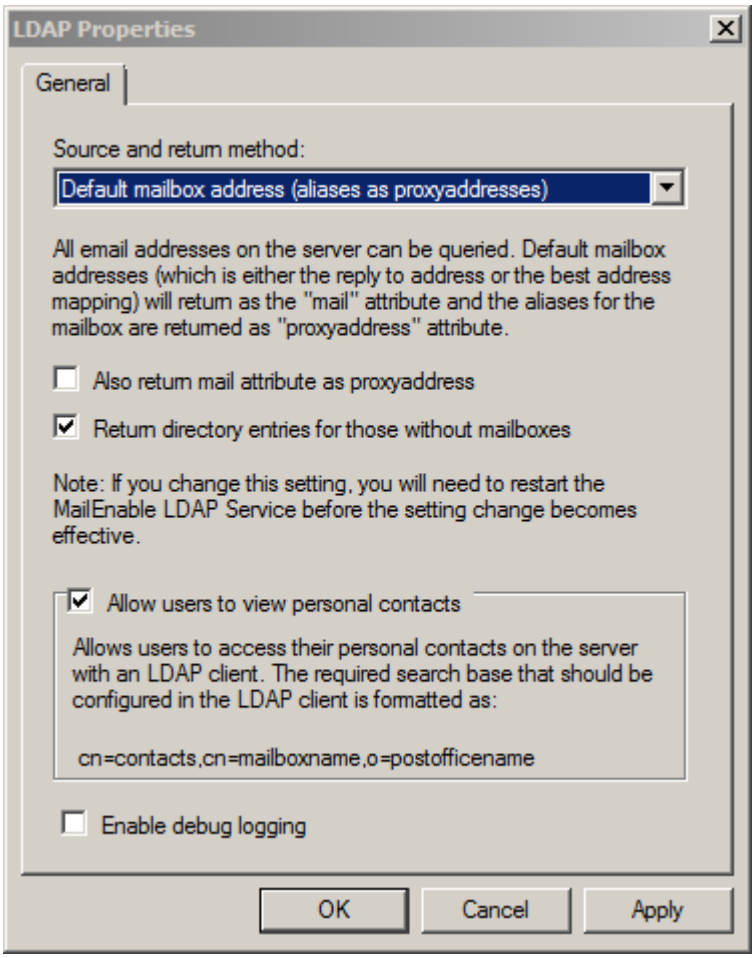


Setting	Description
Logging Options	MailEnable's IMAP Connector provides W3C, activity and debug logging. W3C logging is used to record service usage, Activity logging is used to record system activity and debug logging is used to provide low-level information on system activity.

6.4 LDAP Service

The MailEnable LDAP service can be used to perform address book queries within a specific postoffice. It can be configured to display all addresses mapped to mailboxes within a postoffice or to only display addresses within the postoffice directory list (Global contact list).

6.4.1 LDAP properties



Settings	Description
Source:	**All E-Mail Addresses (includes Directory):** Will return results based on all mapped email addresses within a postoffice. This includes any email address in the directory for the postoffice, as well as the group and list external email addresses. **Directory Contents (Default):** Will return results based on directory members (Global contact list). **Default mailbox addresses (aliases as proxyaddresses):** Will return results using the default email address for a mailbox. All other mapped email addresses for the mailbox are returned as "proxyaddress" attributes. Selecting this option also shows two more available options: **Also return mail attribute as proxyaddress:** Normally the default email address is not also returned as a proxyaddress. This option returns the default email address also as a proxyaddress attribute. **Return directory entries for those without mailboxes:** Also returns all the email addresses in the global directory, even if they have no attached local mailbox.
Allow users to view personal contacts	Allows users to access their personal contacts on the server with an LDAP client.
Enable debug logging	When enabled, LDAP will create a debug log in the Mail Enable\logging directory called **openldap.log**.

6.4.2 How to configure an email client to perform directory queries using the MailEnable LDAP service

Outlook Express:

1. Open Outlook and click on Tools>Accounts
2. Click on the "Add" button, and select the option that is labeled "Directory Service".
3. When prompted for the "Internet Directory(LDAP) Server" enter a domain name which resolves to the IP address of the mail server, or the IP address itself.
4. Tick the option for: "This server requires me to log on option", then click "Next".
5. Next specify the "username" (mailboxname@postofficename) and the "password".
6. On the next screen "Check E-mail Addresses" make sure to select "no" then click "Next".
7. Click "Finish".

Outlook 2000/2002:

1. Open Outlook and click on Tools>Email Accounts
2. Within the "directory" section tick the option "Add a new directory or Address book" and then click "Next".
3. Select "Internet Directory Service (LDAP)", then click "Next".
4. Now in the field next to "Server Name" use a domain name which resolves to the IP address of the mail server, or the IP address itself.
5. Tick the option for: "This server requires me to log on option".
6. Next specify the "username" (mailboxname@postofficename) and the "password".
7. Click "Next" and then "Finish".

Outlook 2003/2007:

1. Go to "Tools" and "Account Settings" and select the "Address Books" tab. On this tab click the "New..." button.
2. Select "Internet Directory Service (LDAP)", then click "Next".
3. Now in the field next to "Server Name" use a domain name which resolves to the IP address of the mail server, or the IP address itself.
4. Tick the option for: "This server requires me to log on option".
5. Next specify the "username" (mailboxname@postofficename) and the "password".
6. Click "Next" and then "Finish".

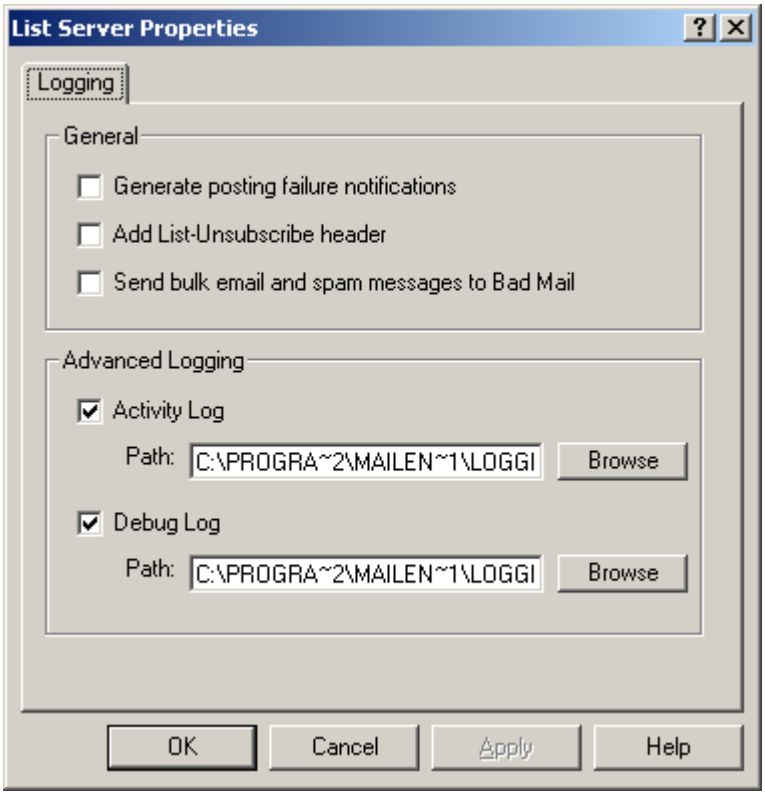
Mozilla Thunderbird:

1. Click on the "Address Book" icon in the toolbar.
2. Next click on File>New>LDAP Directory.
3. Under "General" properties window use the following data:
   - NAME = (postofficename) LDAP directory
   - HOSTNAME = domain name which resolves to the IP address of the mail server, or the IP address itself.
   - BASE DN = (blank)
   - PORT NUM = 389
   - BIND DN = mailboxname@postofficename
4. Under the "Advanced" tab for the search filter use the following: (objectclass=*)
5. Set scope to "subtree".

6.5 List Server Connector

6.5.1 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.

6.6 Management Service

6.6.1 Management Service

The management service is a general purpose feature which provides an interface to manage server wide agents. The management service includes:

- Remote management agent
- Mailbox clean-up agent
- Quota management agent
- Greylisting cleanup agent

- Log Archive Agent

Once the management service is enabled, the agents can be managed by clicking on the Management item in the following location: **MailEnable Management > Servers > localhost > Services and Connectors > Management**

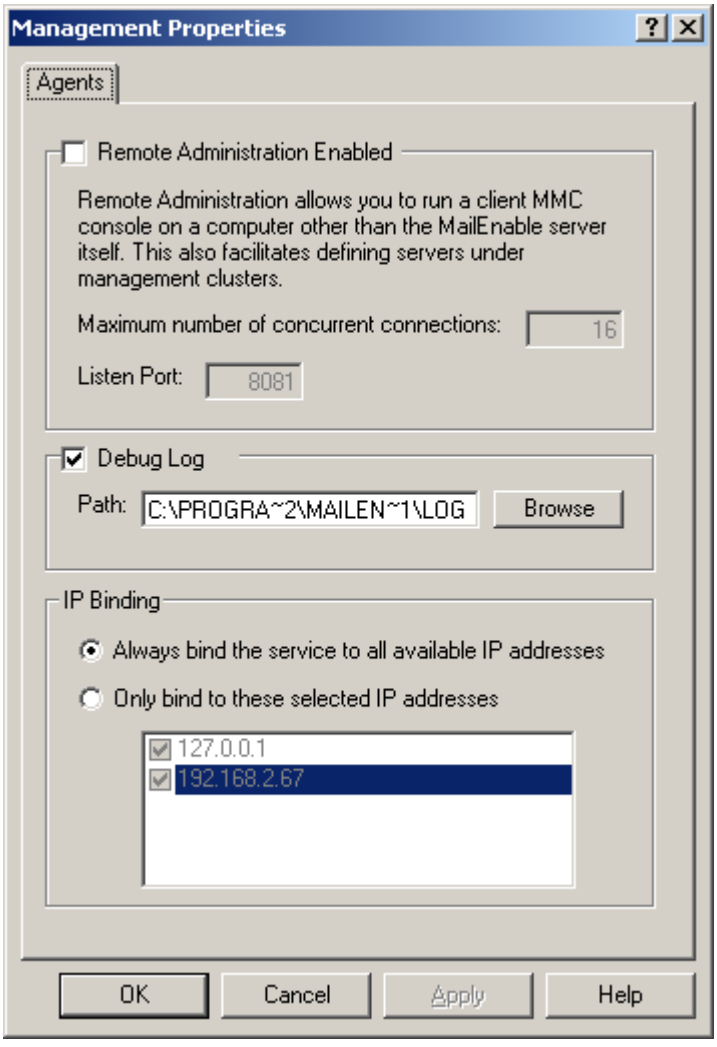
6.6.2 Management properties

How to access the Management service properties

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > Localhost > Services > Management**
2. Right click on **Management** and select properties

6.6.2.1 Remote Management Agent

Options for configuring Remote Management are available by right clicking on the **MailEnable Management > Servers > localhost > Services > Management** icon.



Remote administration will allow connection to a remote machine or cluster machine via the MailEnable administration interface. These remote servers can be added to the administration program (MMC) for ease of access, and they can then be managed in the same manner as a local machine using the MailEnable Administration program. The remote management services do not have the same complete functionality as local server management but most management features can be configured using the remote service.

Setting	Description
Remote Administration Enabled	Enables the remote administration feature of MailEnable and binds the service to the specified port. This feature allows access and configuration of a remote server using the administration program.
Maximum number of concurrent connections	Limits the threads or connections that are available for this service on the bound port.
Listen Port	The port that the service can listen on. (Default 8081)
Debug Log	All purging and notification actions will be logged to a debug log.
IP Addresses to bind to	Select the IP addresses that the Remote Admin service will be bound to. On a multi-homed machine it may be desirable to only allow connections on particular IP addresses.

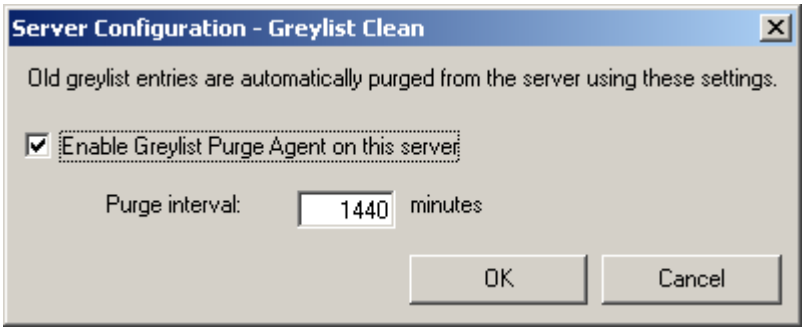
6.6.3 Greylist Cleanup agent

The Greylist cleanup agent when enabled will automatically purge old Greylist entries from the server.

How to enable the Greylist cleanup agent

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > Localhost > Services > Management**
2. Click on **Management** to highlight the management agents in the right hand pane window of the administration console
3. Right click on the **Greylist Cleanup agent** and select **properties**
4. Tick the option **Enable Greylist Purge Agent on this server**

Tip: The greylisting agent can also be enabled/disabled by right clicking on **Greylist Cleanup agents** list within the right hand pane window and selecting **Enable/Disable**



How to edit the Greylist Purge Interval

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > Localhost > Services >** Management
2. Click on Management to highlight the management agents in the right hand pane window of the administration console
3. Right click on the **Greylist Cleanup agent** and select **properties**

4. Specify the **Purge Interval** time in minutes

6.6.4 Log Archive agent

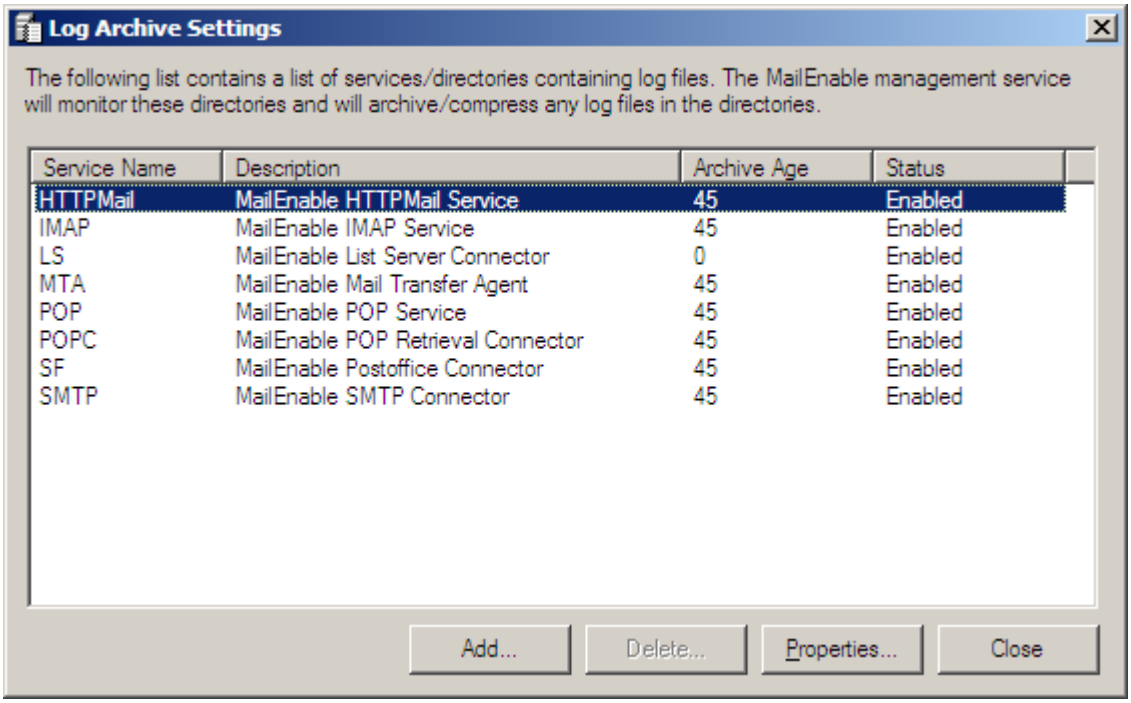
The Log Archive agent will compress log files into cabinet files so you may conserve disk space. Compressed files can also be purged/deleted once they become a certain age.

How to enable Log Archive agent

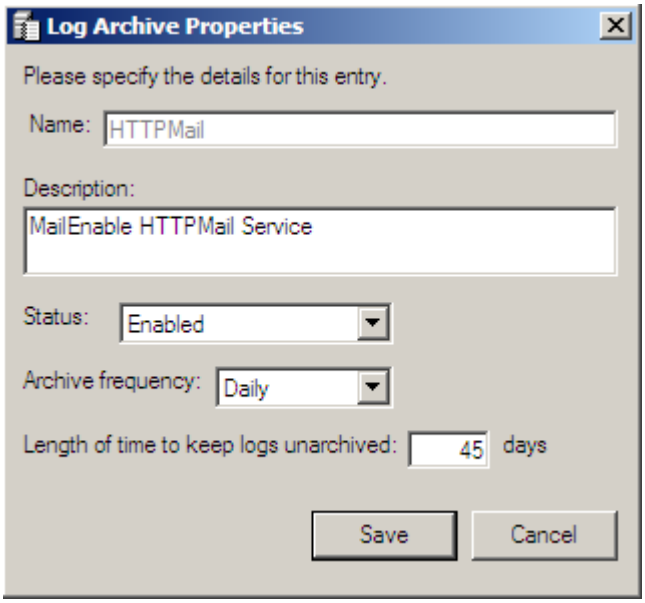
1. Navigate to the following location within the administration console: **MailEnable Management > Servers > Localhost > Services > Management**
2. Click on **Management** to highlight the management agents in the right hand pane window of the administration console
3. Right click on the **Log Archive agent** and select **Enable**

How to configure log archiving agents

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > Localhost > Services > Management**
2. Click on **Management** to highlight the management agents in the right hand pane window of the administration console
3. Right click on the **Log Archive agent** and select **properties**

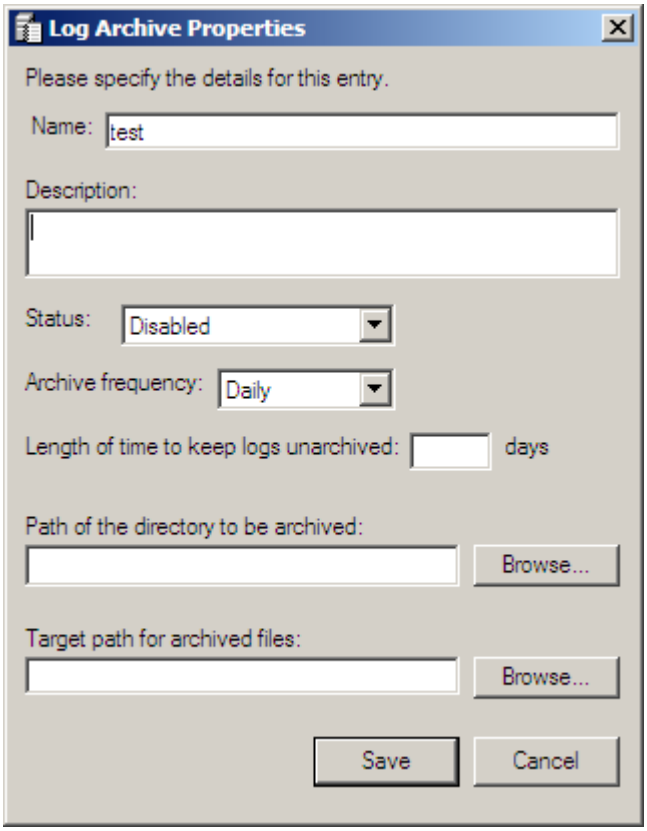


1. Double click on the respective log files **service name** to open the properties window
2. Specify the **Status** of the agent (Enabled/disabled)
3. Set the **Archive frequency** in the drop down menu **Daily, Weekly** or **Monthly**
4. Finally set the **Length of time to keep the logs unarchived** in days
5. Click **Save**.



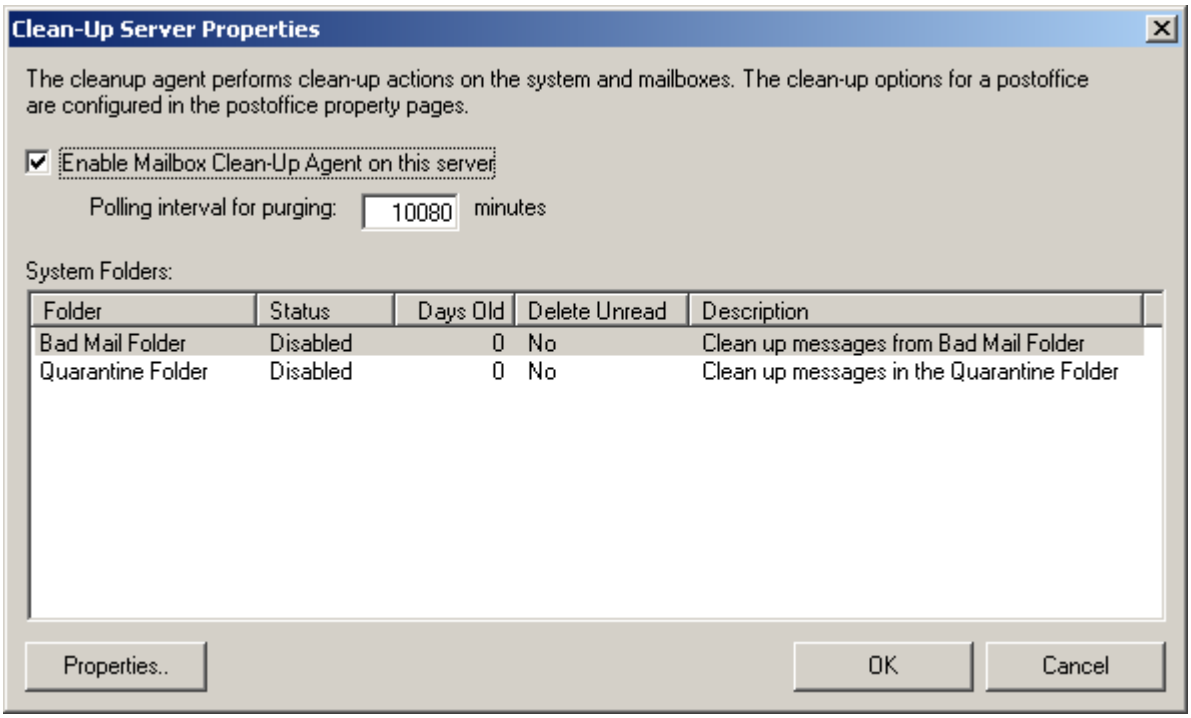
How to add custom Log archiving agents

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > Localhost > Services > Management**
2. Click on **Management** to highlight the management agents in the right hand pane window of the administration console
3. Right click on the **Log Archive agent** and select **properties**
4. Click on the **Add...** button
5. Specify a **name** for the log agent
6. Specify a **Description**
7. Specify the **Status** of the agent (Enabled/disabled)
8. Set the **Archive frequency** in the drop down menu **Daily, Weekly** or **Monthly**
9. Set the **Length of time to keep the logs unarchived** in days
10. Click on the **Browse...** button and specify the path of log file directory to be archived
11. Finally click on the **Browse...** button to specify the target folder where the archived files are to be stored
12. Click **Save**



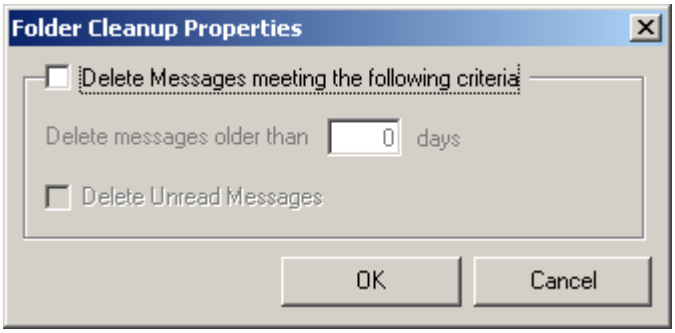
6.6.5 Global Mailbox clean-up agent

To access the Global Mailbox clean-up agent, navigate to **MailEnable Management > Servers > localhost > Services > Management**, select the **Mailbox clean-up agent** from the right panel. The Global Mailbox clean-up agent performs server-wide clean-up actions on system folders. The agent be configured to automatically purge mail that is older than a set number of days. It is possible to purge the Bad Mail folder and Quarantine folder. For information on how to setup the mailbox cleanup agent for a postoffice please see **Postoffice - Agents (Section 5.3.6)**.



Setting	Description
Enable Mailbox Clean-Up Agent on this server	Enables the Global Mailbox Clean-Up Agent and actions.
Polling interval for purging	Number of minutes between when the service will purge messages. In order to perform a purge, the service needs to examine each folder, and possibly emails for each user, which can be both time and resource intensive. It is recommended to time this so that it occurs only at off-peak times every few days, depending on the number of users configured on the server.
Properties (Folder clean up)	This can be set not to delete any unread messages and delete messages in folder over a specified number of days old.
Properties..	Used to open the properties window for each criteria. Highlight a criteria in the list and then click on the properties button. Alternatively you can double click on each criteria to open the same properties window.

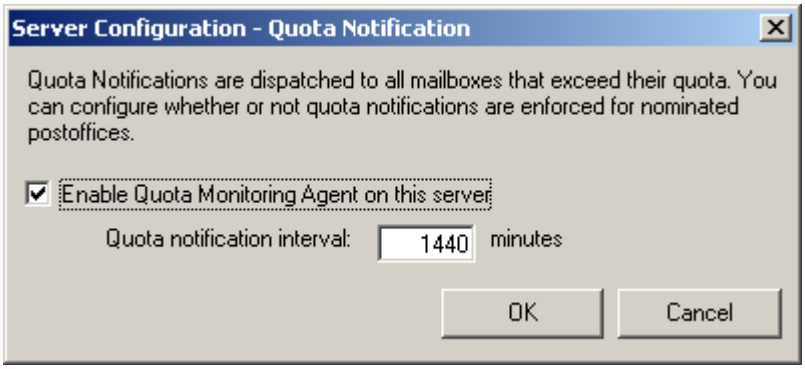
Folder cleanup properties



Settings	Description
Delete Messages meeting the following criteria	Enables the Mailbox Clean-Up Agent for the folder
Delete messages older than days	The Mailbox Clean-Up Agent will delete any messages older then the specified value in days
Delete Unread Messages	Enables the option for the Mailbox Clean-Up Agent to delete unread messages

6.6.6 Quota Notification Agent

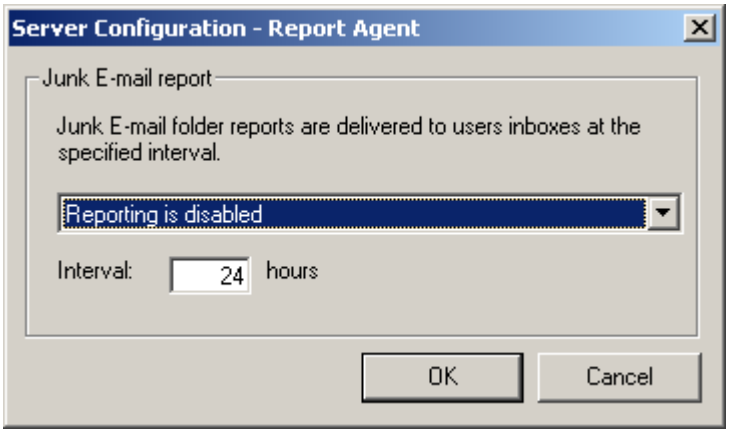
To access the Quota notification agent, navigate to **MailEnable Management > Servers > localhost > Services > Management**, select the Quota notification agent from the right panel. Quota notifications are dispatched to all mailboxes on the server that exceed their quota. It is possible to configure whether or not quota notifications are enforced for the nominated post offices. See the **Postoffice - Agents (Section 5.3.6)** for information on configuring quota notifications per post office.



Setting	Description
Enable Quota Notification Agent on this server	Quota notifications can be enabled or disabled for the server.
Quota notification interval	The quota notification interval determines how often the server will check for mailboxes that exceed quota. When a mailbox exceeds the quota, a message informing the user is placed in the Inbox for that mailbox. Only one notification message will appear in the Inbox, and if the mailbox remains over quota, this message will have its date changed so it appears as the most recent message. In order to check quotas, the service needs to examine the details for each user, which can be both time and resource intensive. It is recommended to time this so that it occurs only at off-peak times every few days, depending on the number of users configured on the server.

6.6.7 Report Agent

The Report Agent will deliver reports based on the contents of the mailboxes Junk E-mail folder at specified interval.



Settings	Description
Reporting is disabled	Disables the Report Agent
Reporting is enabled for every mailbox	Will send a Junk E-mail report to all mailboxes within all postoffices
Reporting is configured under postoffice settings	Sets the Report Agent settings to be determined by the postoffice settings. Please see **Postoffice - Feature Selection. (Section 5.3.10)**

6.7 Mobile Webmail

MailEnable includes a mobile web mail client that can be used on mobile devices. To access the mobile webmail you access the webmail clients login page and it has a link under the username and password details for accessing the mobile client.

6.8 Mail Transfer Agent (MTA)

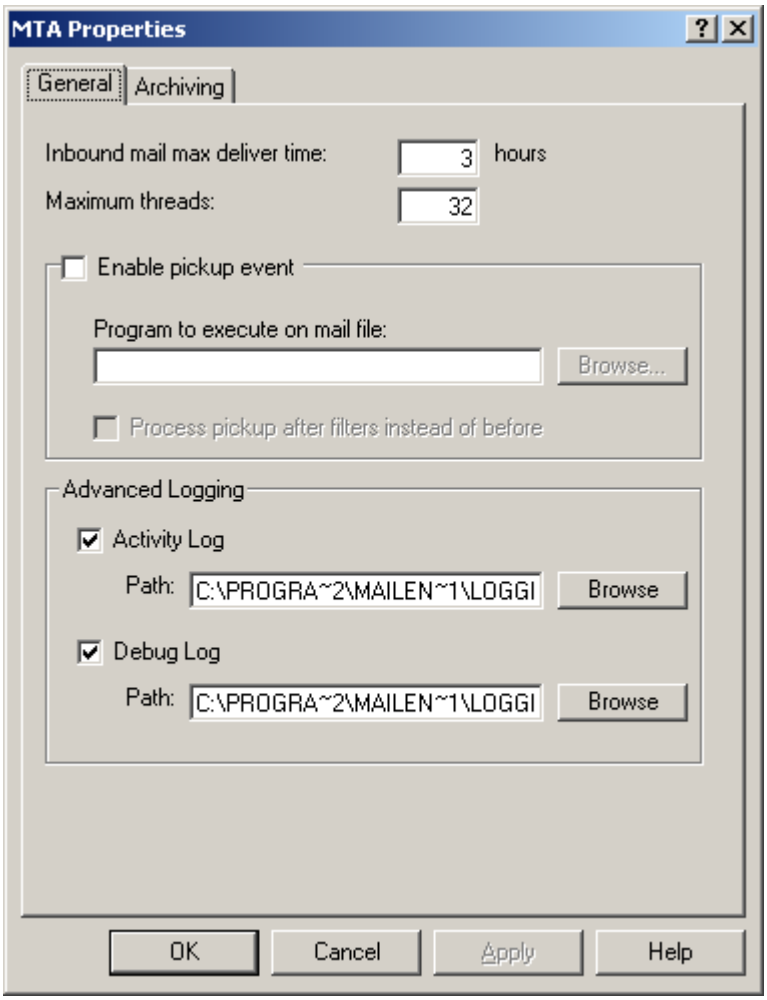
6.8.1 MTA Overview

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

Examples of MTA functionality follow:

- Receiving inbound messages from mail connectors
- Delivering mail to local mailboxes
- 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

6.8.2 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 pickup event	Executes a program or application when mail arrives. MailEnable will pass the mail message filename to the application. For example, if you write a VB script that adds some text to the end of each email that gets delivered, you would enable the pickup event. The command line used to execute the application is: program messagefilename connectortype Where program is the program filename, messagefilename is the name of the message file and connectortype is the type of messages (i.e. SMTP, LS, SF). Be aware that the directory path to the message is not passed to the program. The directory path will need to read from the registry in the program file.
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.
Use separate queue for bulk or campaign messages	When a list sends an email, if the **Track send results for this list** option is enabled for it, the emails will use a lower priority Campaign queue for the SMTP sending. This helps to avoid normal email getting delayed when larger lists are being sent.

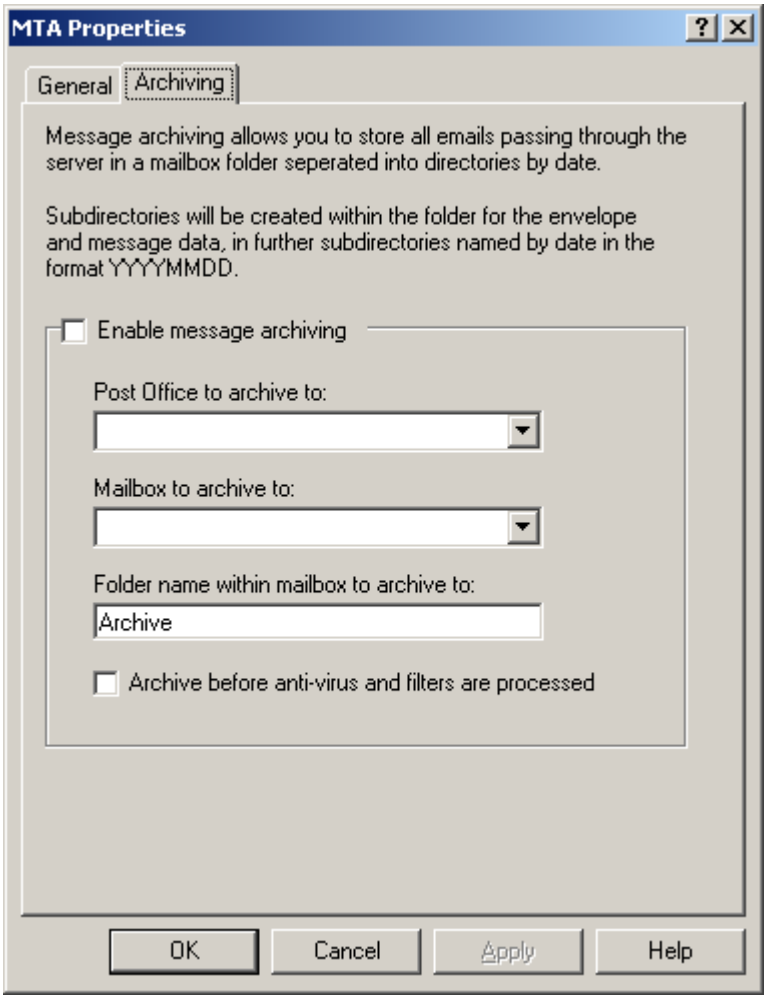
6.8.3 MTA - Archiving

Message Archiving

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

How to enable Message Archiving

1. Navigate to the following location within the administration console: **Servers > localhost > Agents > MTA**
2. Right click on **MTA** and select properties.
3. Navigate to the Archiving tab and tick the option **Enable message archiving**.
4. Use the **Post Office to archive to:** drop down menu and select a postoffice where the archiving mailbox and folder will reside under.
5. Next use the **Mailbox to archive to:** drop down menu and select the mailbox where the archive folder resides under.
6. Finally specify the mailbox folder where messages are to be archived within the **Folder name within mailbox to archive to:** field.



Setting	Description
Enable message archiving	Enables the message archiving option for the MTA agent
Post Office to archive to:	Sets the postoffice where the archiving mailbox resides under
Mailbox to archive to:	Sets the mailbox where the archiving folder resides under
Folder name within mailbox to archive to:	Specifies the folder where messages are to be archived
Archive before anti-virus and filters are processed	Sets the message archiving to occur before any antivirus scanning or message content filters are triggered

6.9 POP Retrieval Connector

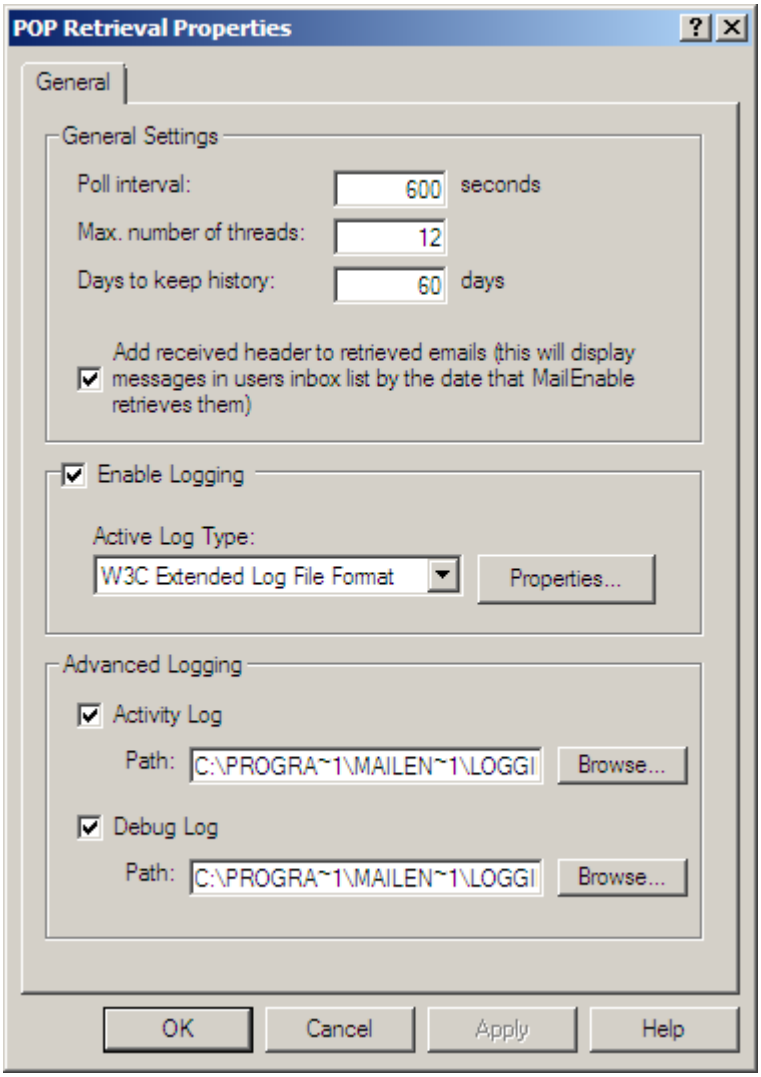
6.9.1 POP Retrieval Connector

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

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

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

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



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

6.10 POP Service

6.10.1 POP service

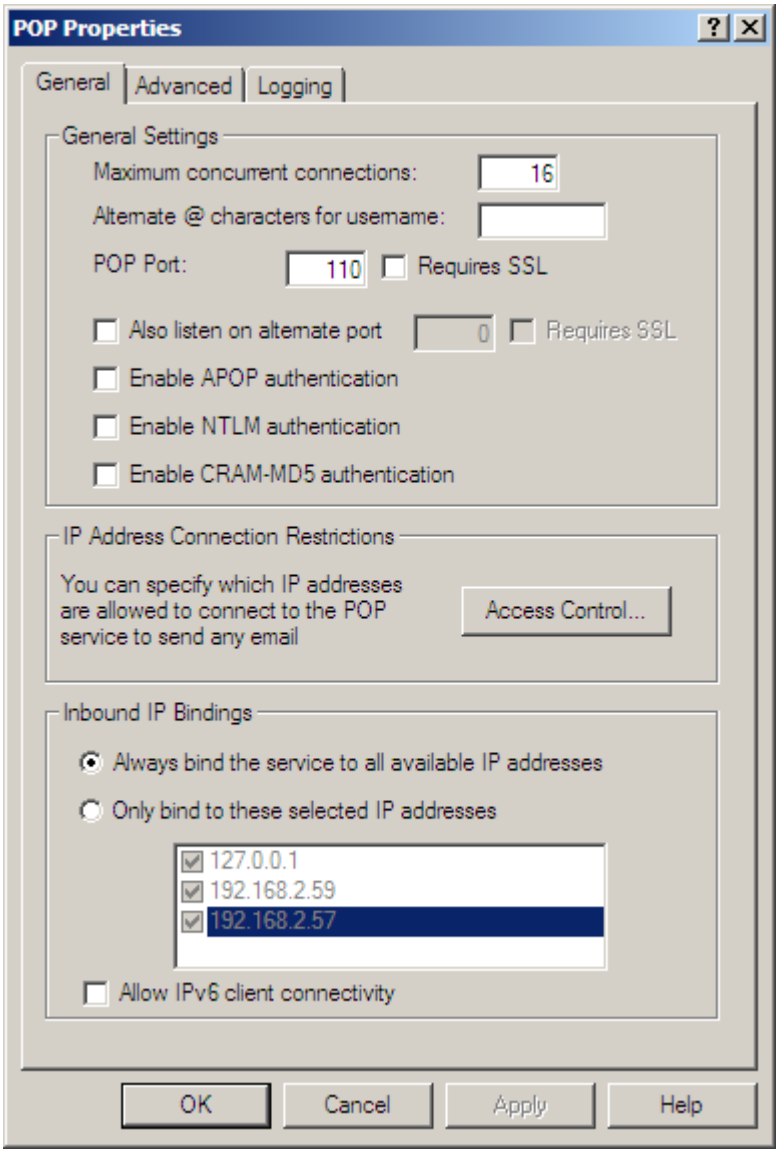
POP stands for Post Office Protocol. This is a mail protocol that enables emails to be retrieved from a remote mailbox. It allows you to collect emails from a hosted account on a server to your own email software, such as Outlook, Eudora etc.

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**.

6.10.2 POP - General

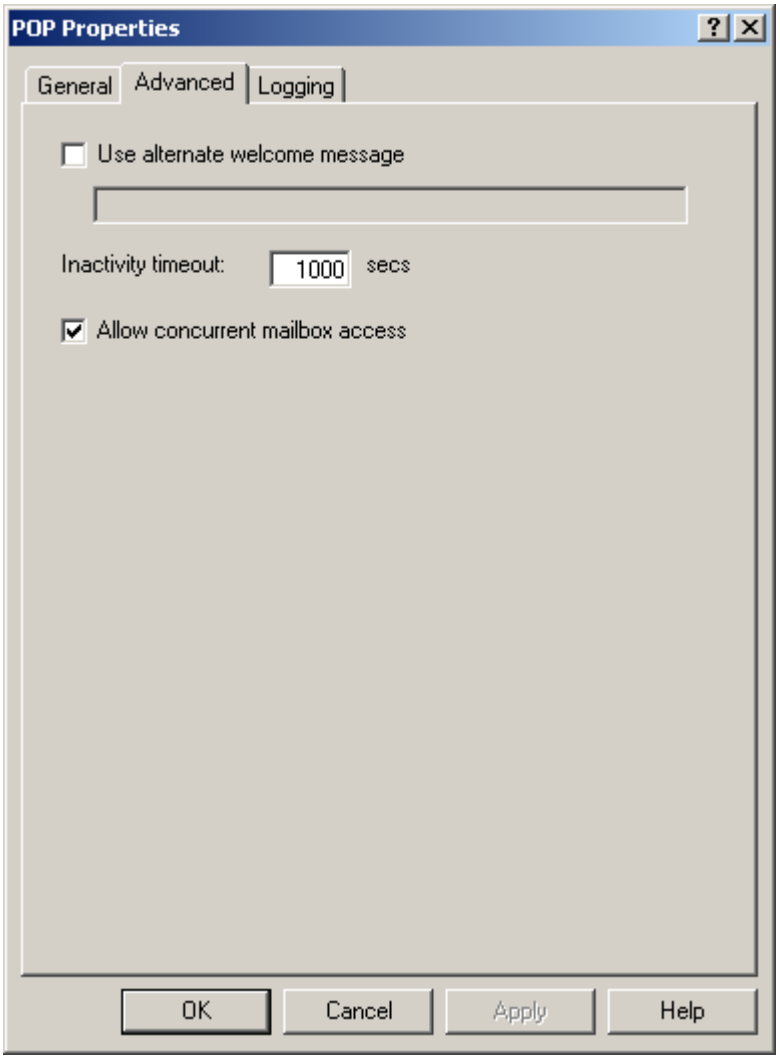


The following table outlines the configuration options for MailEnable's POP service:

Setting	Description
Maximum concurrent	The number of concurrent connections from email clients that the service will allow.

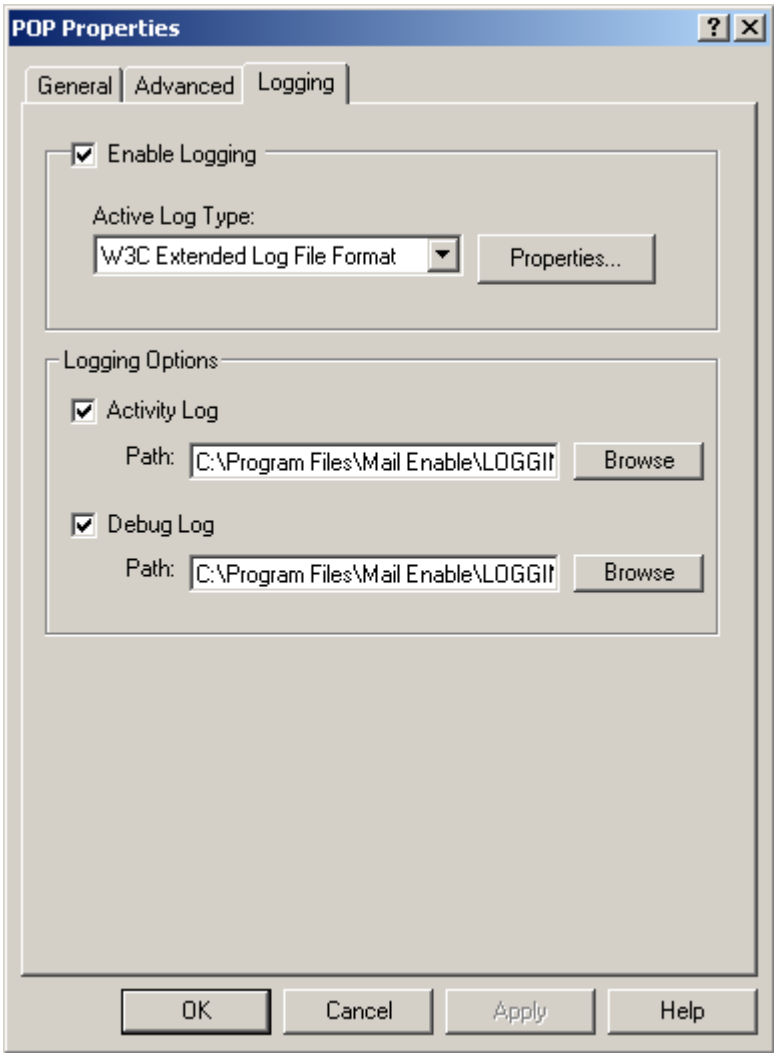
connections	
Alternate @ characters	Some older mail clients don't allow the use of @ in the username section. Since the MailEnable usernames are formatted in mailboxname@postoffice format, this may cause problems. To solve this, MailEnable can specify the characters that can be used as a substitute. 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.
POP Enable SSL (Default Port)	Enables SSL encryption for the default port that POP is running on. When enabling SSL make sure a valid SSL certificate has been selected in the **MailEnable Administration > Server > Localhost Properties > SSL tab**
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.
POP Enable SSL (Alternate Port)	Enables SSL certificate encryption for the alternate port that POP is running on. The default port number is 995. When enabling SSL make sure that a valid SSL certificate has been selected in the **MailEnable Administration > Server > Localhost Properties > SSL tab**.
Enable APOP authentication	Usually, the users' username and password are sent in clear text format (i.e. not encrypted). Enabling this option will force clients to enable APOP authentication on their mail client software. Make sure users are using software that supports APOP, otherwise they will not be able to receive email. Some older mail clients do not support APOP.
Enable NTLM authentication	If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled to use this secure authentication. For example, in Outlook the feature is called SPA – Secure Password Authentication. More information on NTLM can be found in the **Overview of NTLM Authentication section (Section 15.2)**.
Enable CRAM-MD5 authentication	
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.

6.10.3 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

6.10.4 POP - Logging



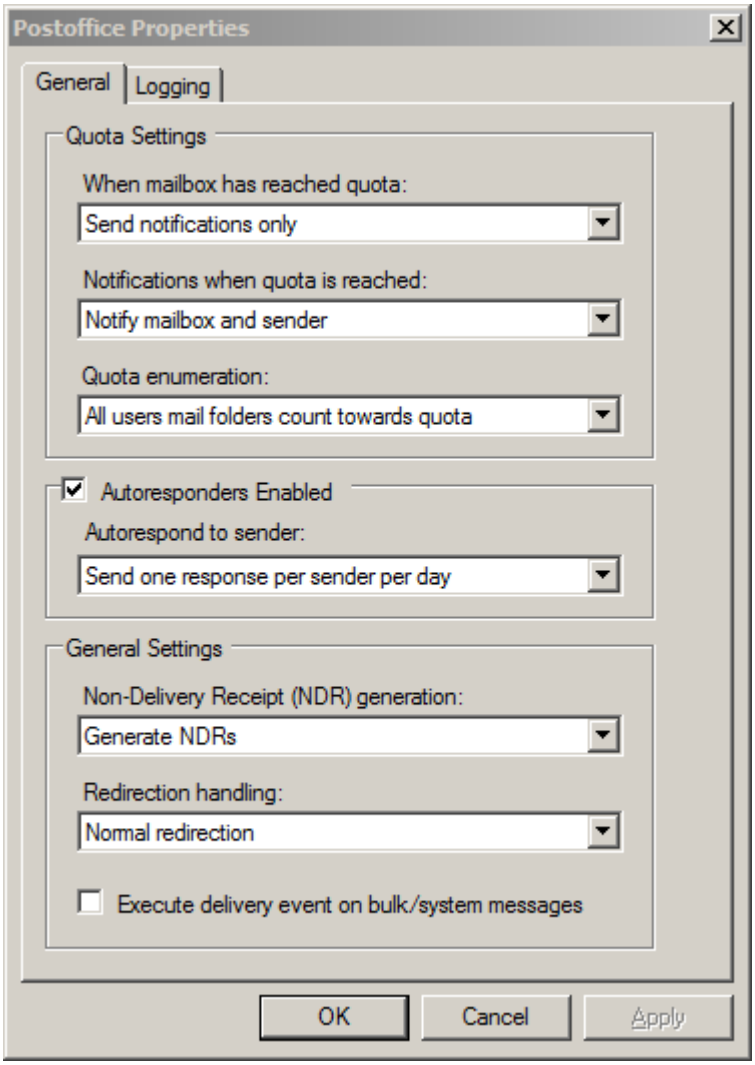
Setting	Description
Enable Logging	Enables W3C logging for the POP service. W3C logging can specify which fields are logged and the rollover frequency. The directory can also be specified.
Logging Options	Produces a debug and activity log for the POP3 service. Use this to obtain more details about the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

6.11 Postoffice Connector

6.11.1 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**.

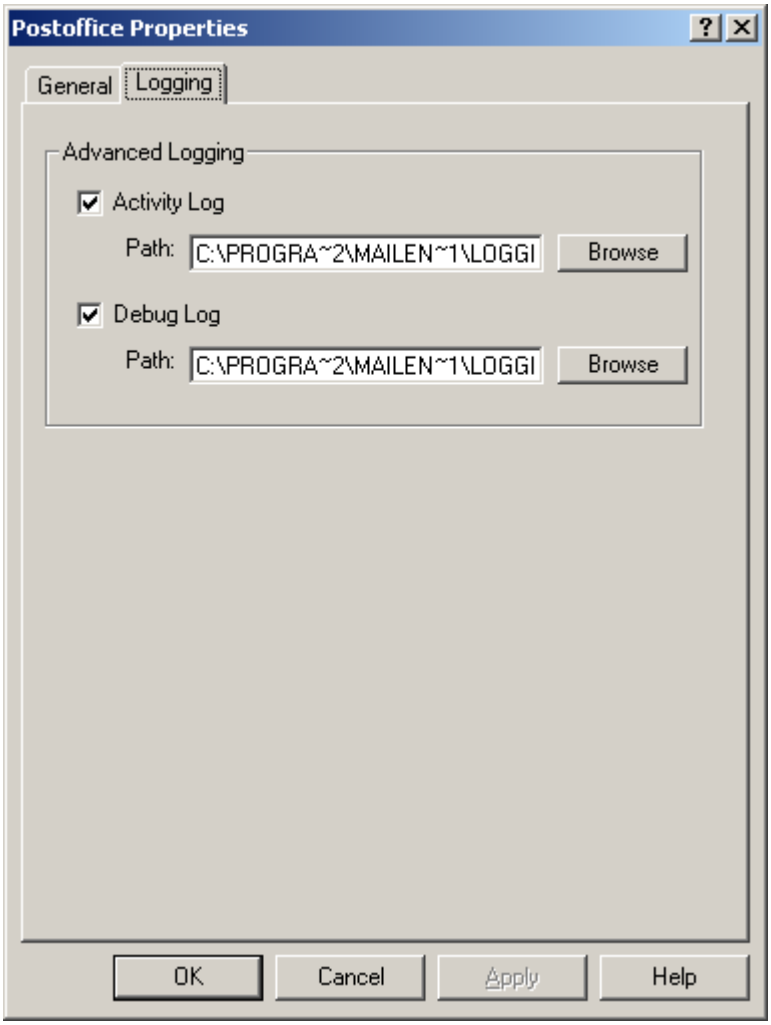
6.11.2 Postoffice connector - General



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.

6.11.3 Postoffice connector - Logging



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

6.12 Search Indexing

6.12.1 Search Indexing Overview

The Indexing service indexes emails, appointments, tasks and contacts on the server. It continually updates indexes as items are added, removed and edited. The search indexing is only used by the webmail client. If you are not using the webmail client it is best to disable the search indexing service.

6.12.2 Search Indexing Settings

Setting	Description
Search index initialisation concurrency limit	The number of threads allocated to creating a new index for a mailbox.
Search index update concurrency limit	The number of threads allocated to updating existing indexes due to a change or addition.
Logging level	**Off**

	The logging is disabled. **Information** The logging shows what items are being indexed. **Debug** All available logging is enabled for support purposes.

The properties page will show the current number of items that need to be fully indexed and also the number of individual items that also need to be indexed.

6.13 SMS Connector

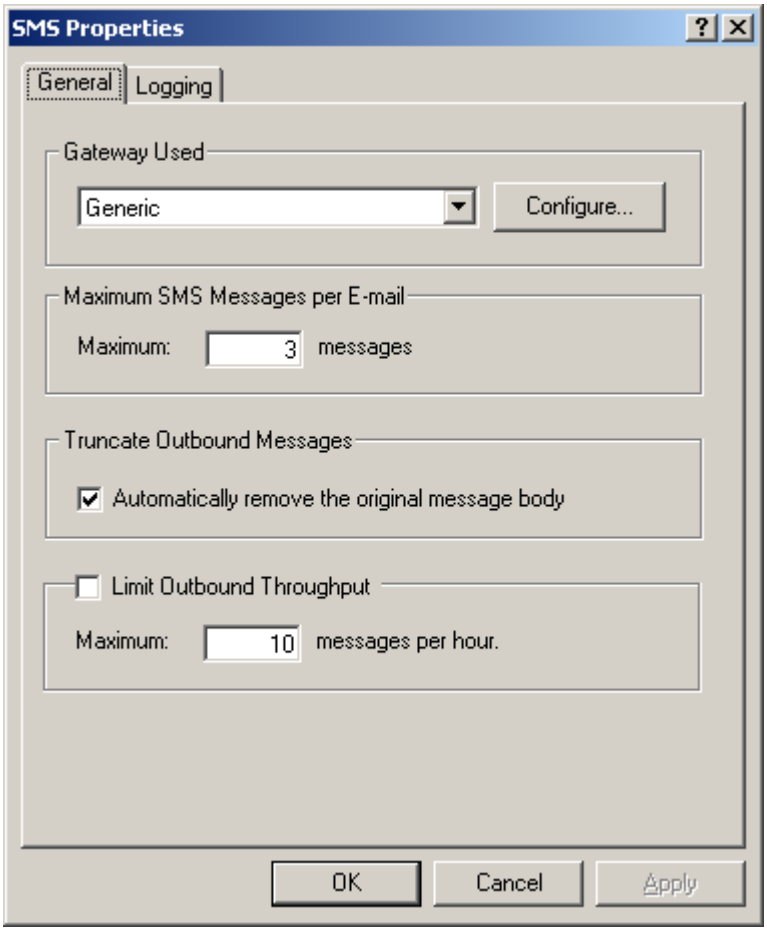
6.13.1 SMS Connector Overview

Overview

MailEnable Enterprise Edition includes an SMS connector to allow you to send SMS messages from MailEnable. Mail messages can be queued to an SMS message queue where they are picked up by the SMS connector for pre-processing and delivery as an SMS message. MailEnable has the ability to throttle the usage of the SMS connector and to procure message contents before they are converted to SMS.

6.13.2 SMS Connector - General

To configure SMS messaging, open the MailEnable administration program and go to: **Servers > localhost > Services and Connectors > SMS**, right-click on **SMS** and choose Properties.



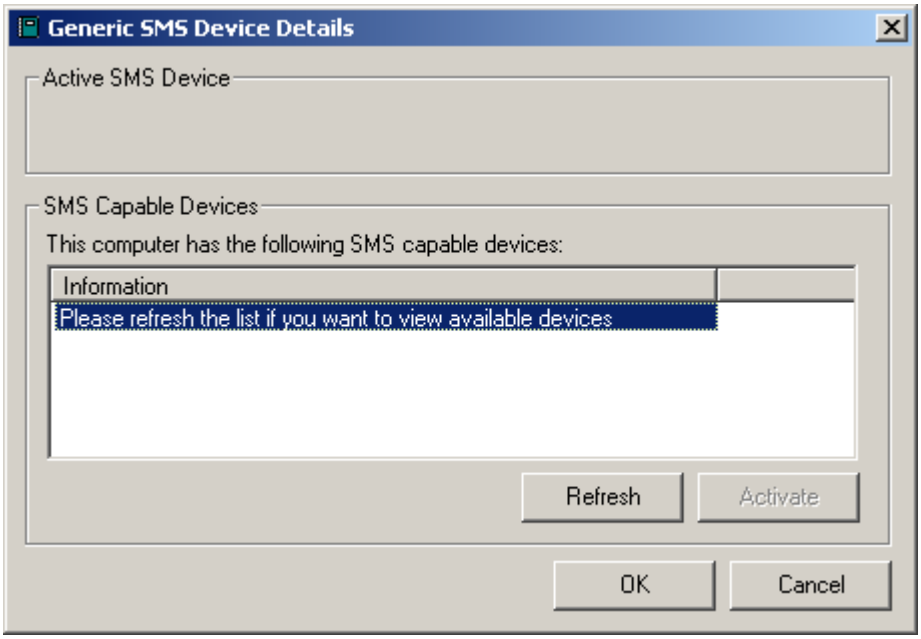
Settings	Description

Gateway Used	Selects which gateway you wish to use to send SMS messages. The **Configure…** button allows further gateway-specific options to be set (see below for more information about gateway options)
Maximum SMS Messages per E-Mail	This option determines the maximum number of SMS messages that will be generated for any given email. If an email sent to an SMS address would otherwise cause this limit to be exceeded (i.e. if the message is too long), the excess message content will be discarded.
Truncate Outbound Messages	**Automatically remove the original message body:** When this option is checked, reply emails sent to SMS addresses will have the original email content stripped from them in order to reduce the message length (and thus the number of SMS messages required to send it).
Limit Outbound Throughput	When checked, this will limit the number of SMS-addressed email messages that can be sent in a day to the number specified in the text box.

SMS Gateway options

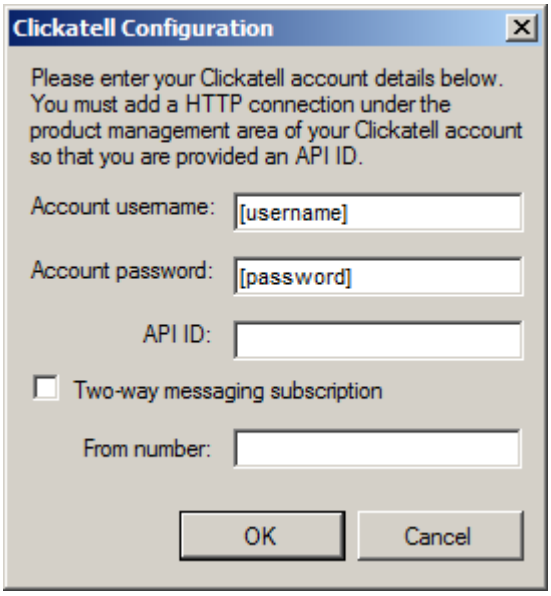
Generic

The generic gateway option allows SMS messages to be sent using devices (such as phones) connected to the local machine via a serial interface (Please inquire with your phone manufacturer for information about drivers and serial interface capabilities). Configuring the generic gateway will initiate a search for such devices, which can then be selected for sending.



Clickatell

Clickatell allows SMS messages to be sent using a Clickatell account (Please see https://www.clickatell.com for more information).

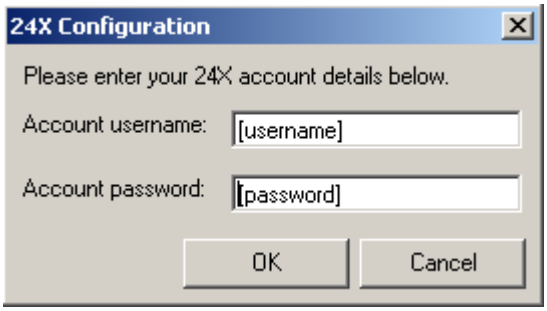


The following options must be configured:

Settings	Description
Account username	The username of a Clickatell account
Account password	The password for the same account
API ID/API Key	An API ID or API Key for the HTTP API, which must first be obtained by registering an API connection through the account management. Please visit www.clickatell.com for more more information. If you are using an API Key, then the username and password should be left, as they are not used.
Two-way messaging subscription	Enables two-way messaging when using the Clickatell service. It may be a requirement of your service to enable this.
From number	This is your two-way number.

24X

24X allows SMS messages to be sent using a 24X account (please see https://www.24x.com for more information)

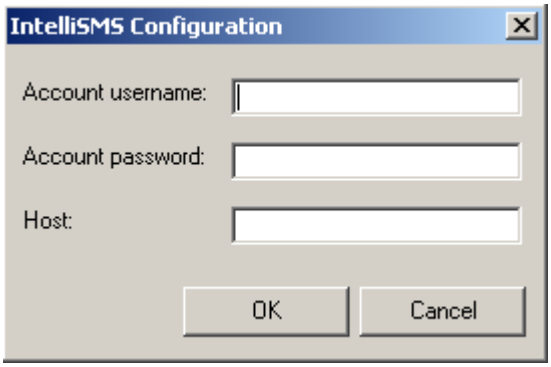


The following options must be configured:

Settings	Description
Account username	The username for the 24X account
Account password	The password for the 24X account

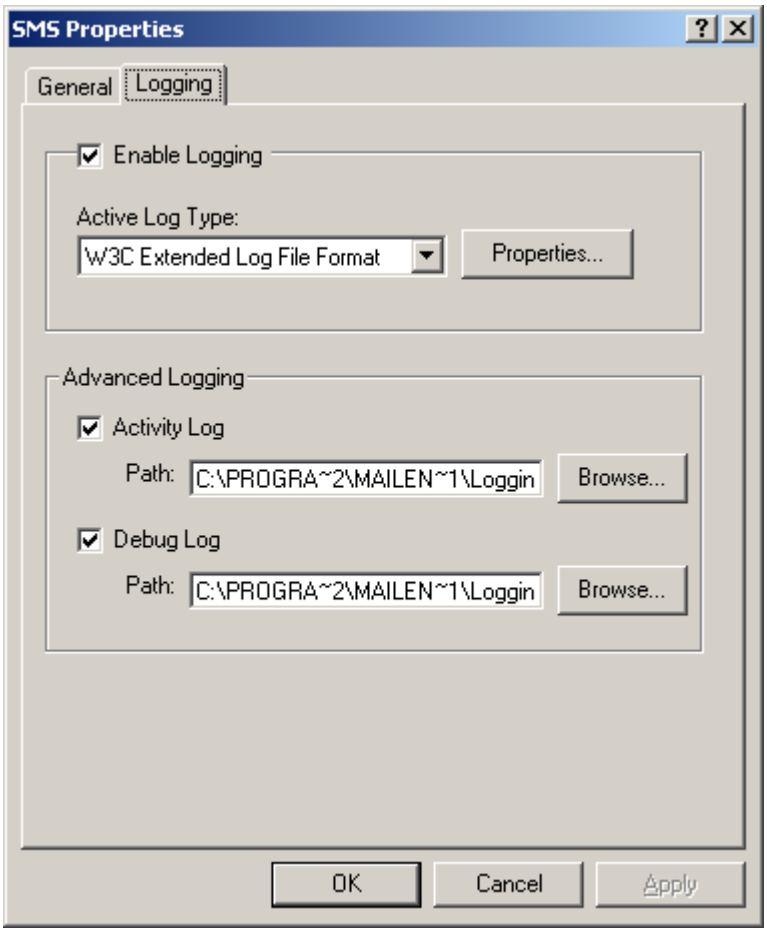
IntelliSMS

IntelliSMS allows SMS messages to be routed through the IntelliSMS gateway (please see https://www.intellisms.com.au for more information)



Settings	Description
Account username	The username for the intelliSMS account. Please obtain an account from intelliSMS
Account password	The password for the intelliSMS account
Host	Host name for the intelliSMS gateway

6.13.3 SMS Connector - Logging



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

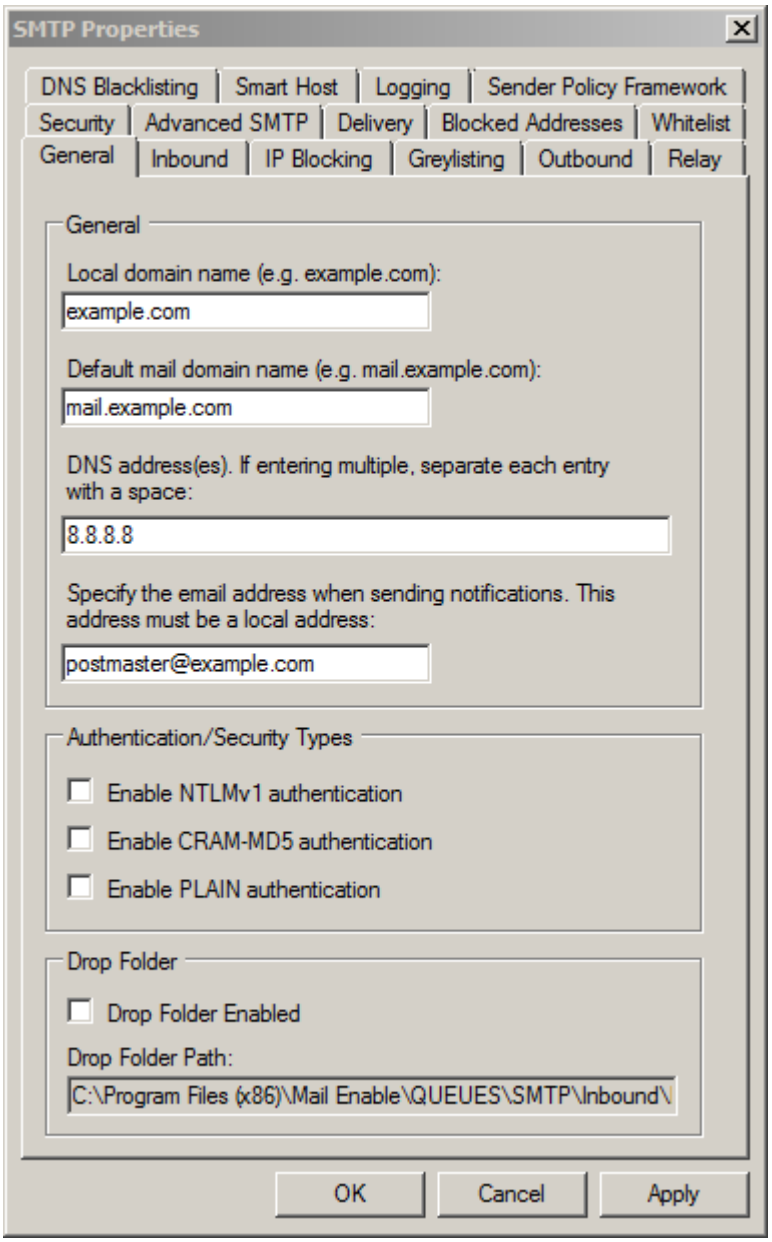
6.14 SMTP Connector

6.14.1 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.

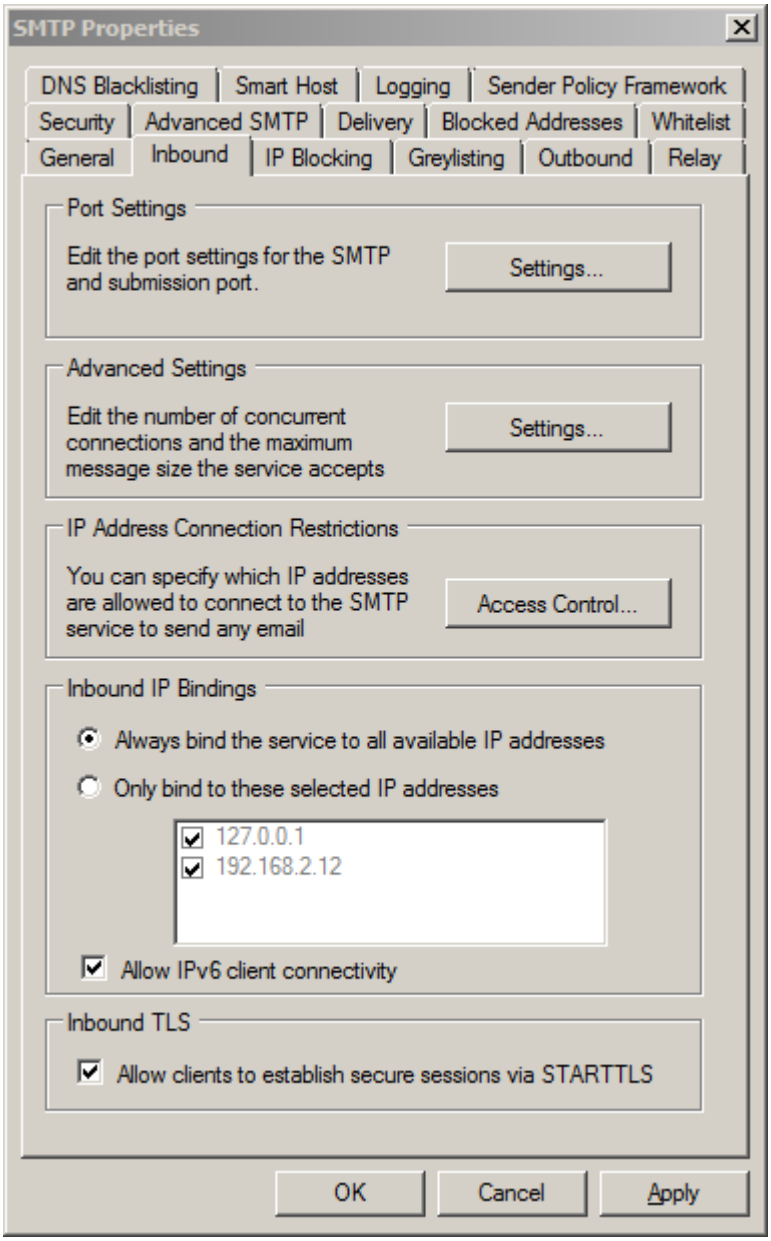
6.14.2 SMTP - General



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.

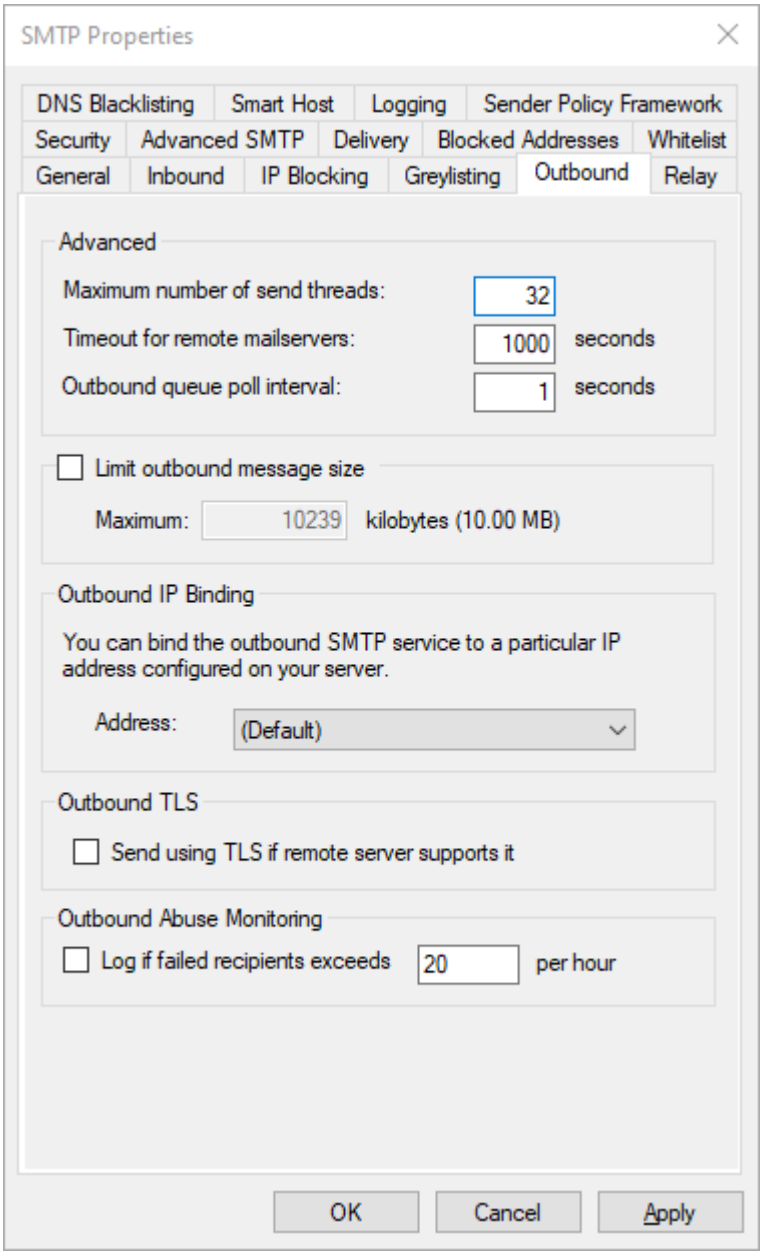
6.14.3 SMTP - Inbound



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 5.10.3)** 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.	

6.14.4 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.

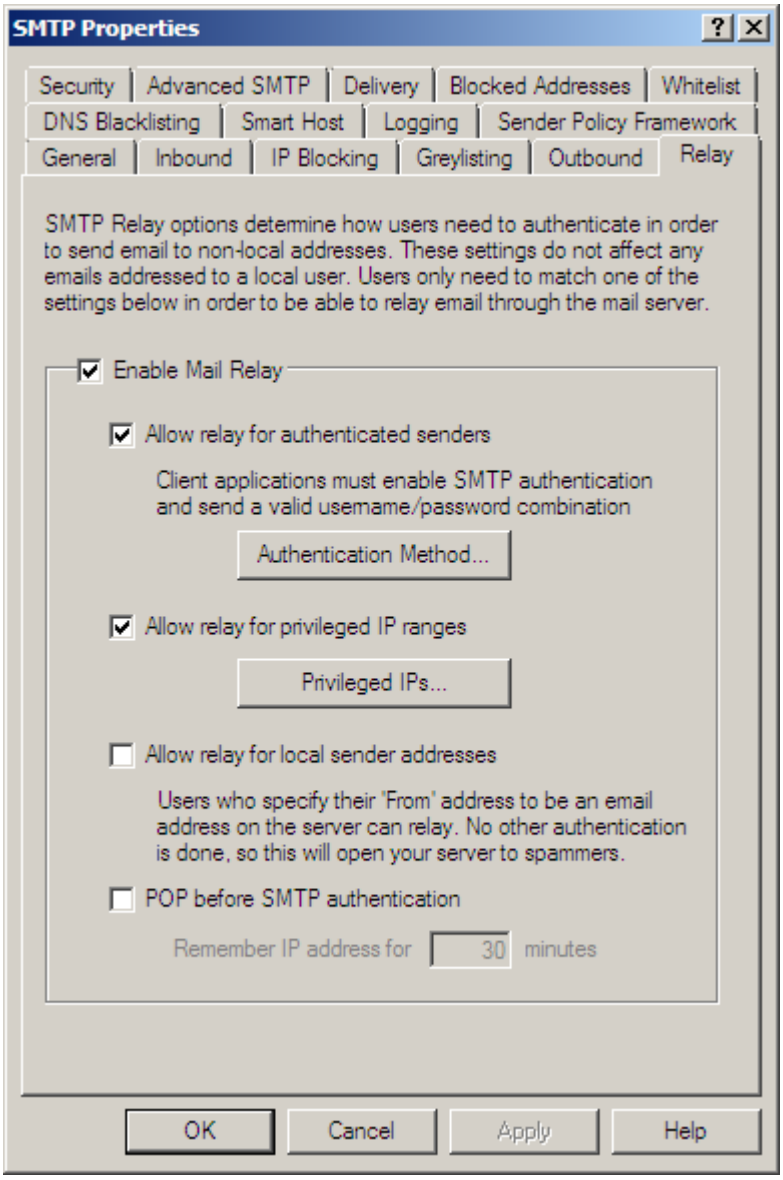
6.14.5 SMTP - Relay

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.

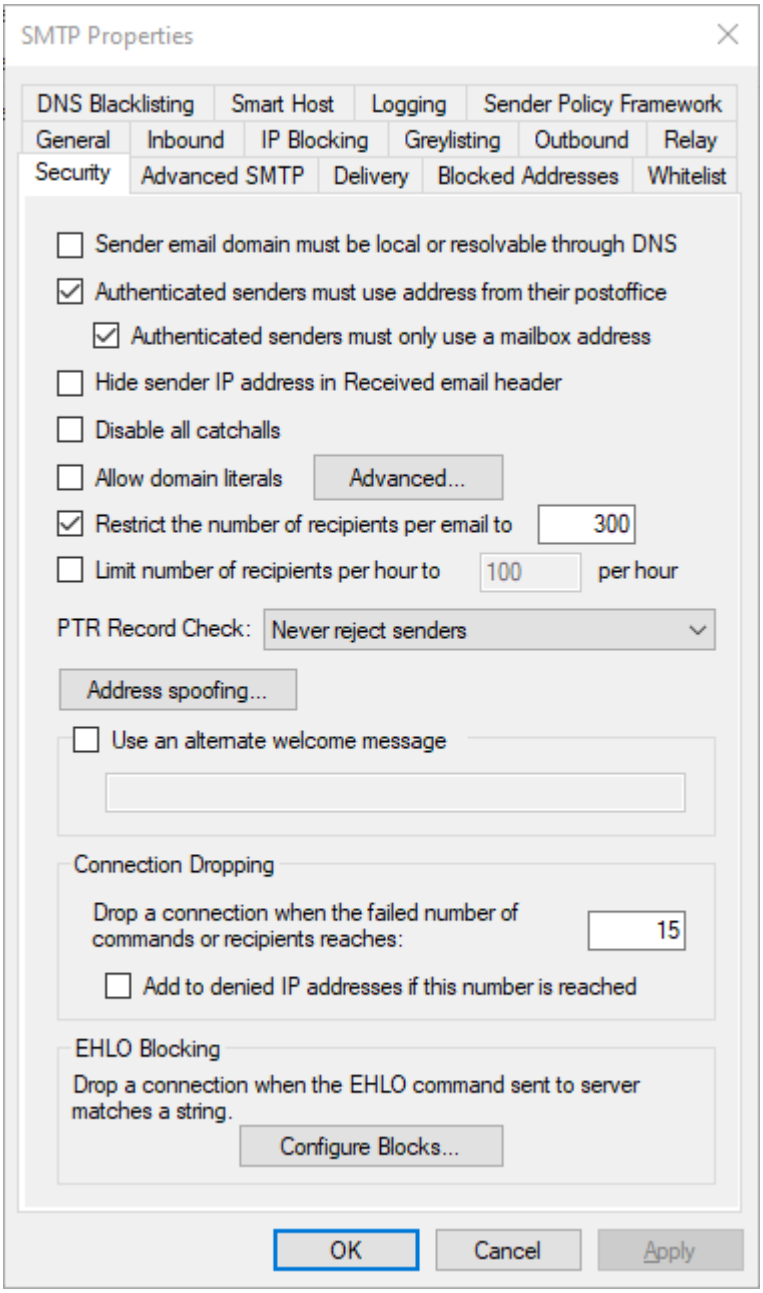
The following table provides an explanation of the various relay settings.



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	Allows people with certain IP addresses to send email through the server. If the IP addresses of

privileged IP ranges	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.

6.14.6 SMTP - Security

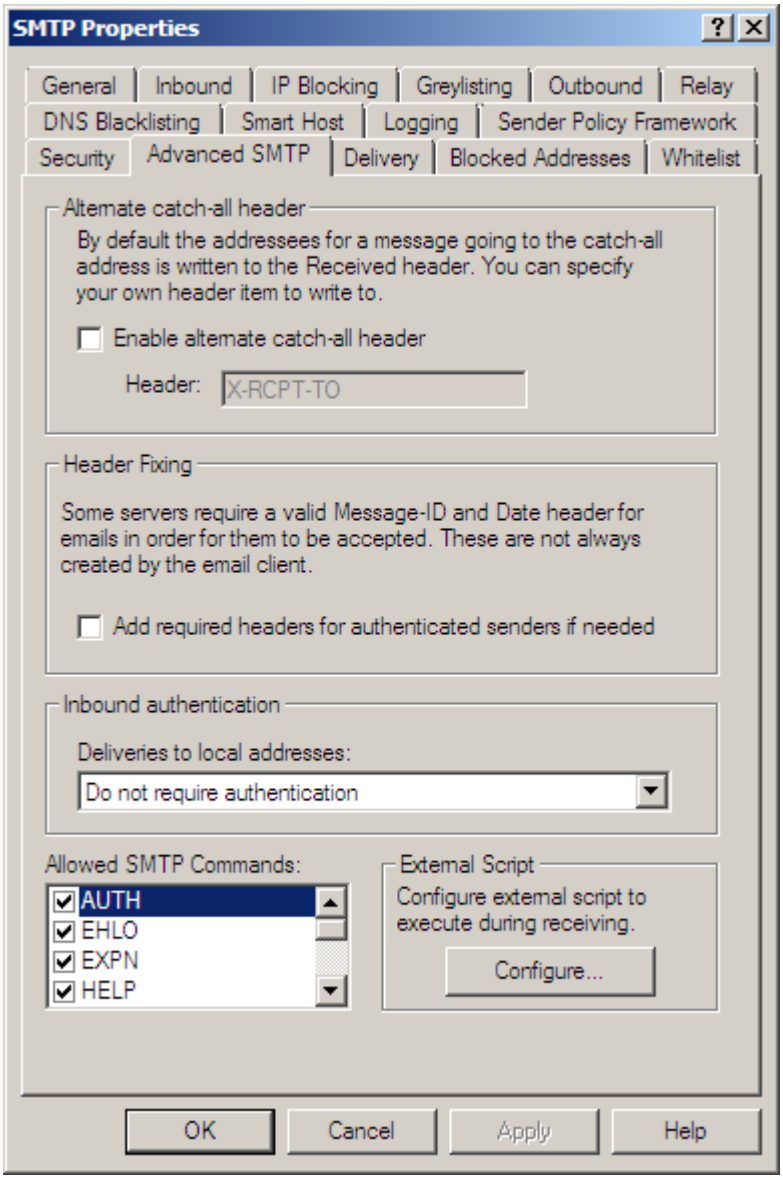


Setting	Description
Sender email domain must be local or resolvable through DNS	This option checks the domain of the SMTP envelope address to make sure it is a valid domain. The domain either has to be configured in MailEnable, or it has to be able to be resolved through DNS. If not then the message 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	When an email client or other mail server connects to MailEnable, a one line welcome

welcome message	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.

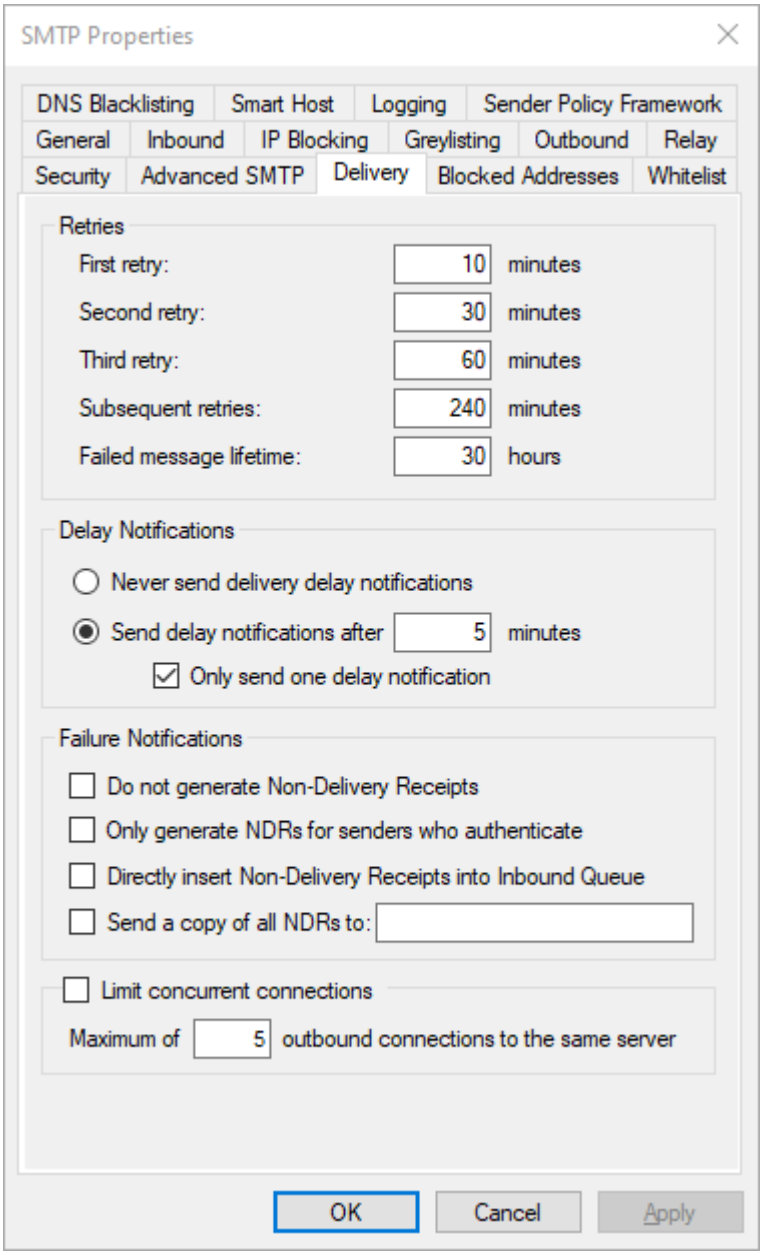
6.14.7 SMTP - Advanced SMTP



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 (Section 5.3.8)** 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.

6.14.8 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:

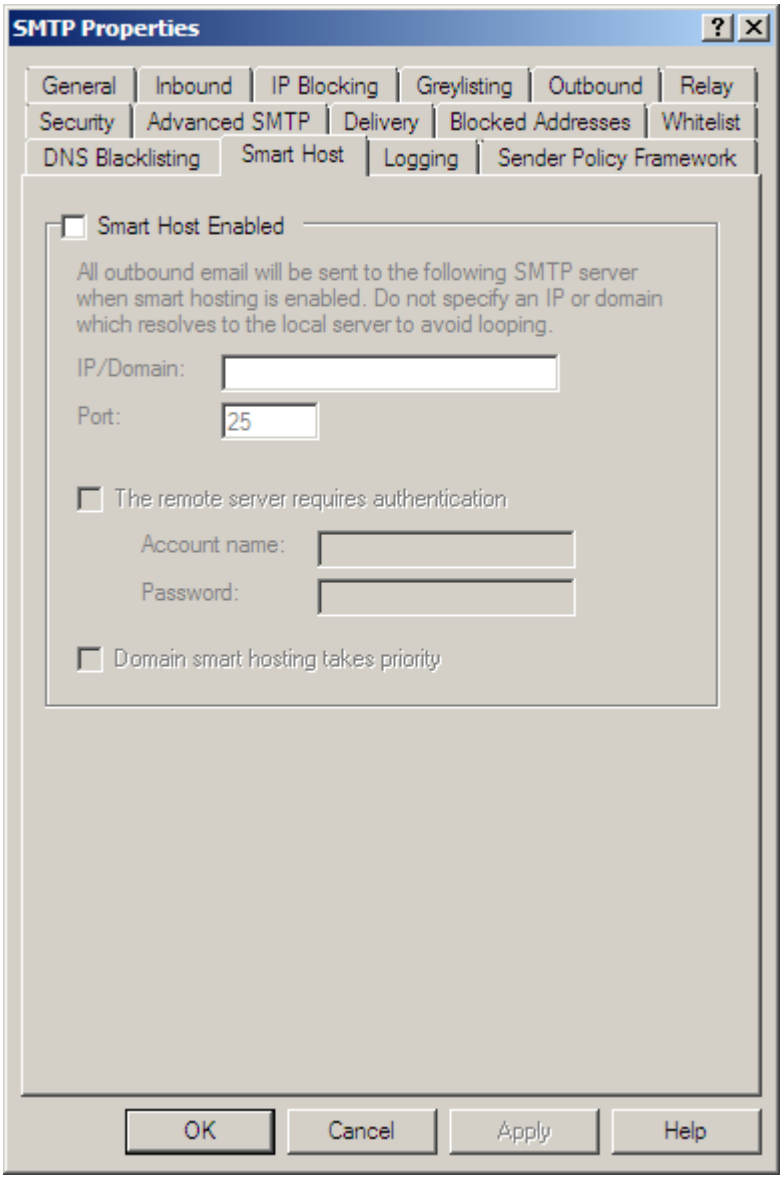
Mail Enable\Config\Postoffices

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)

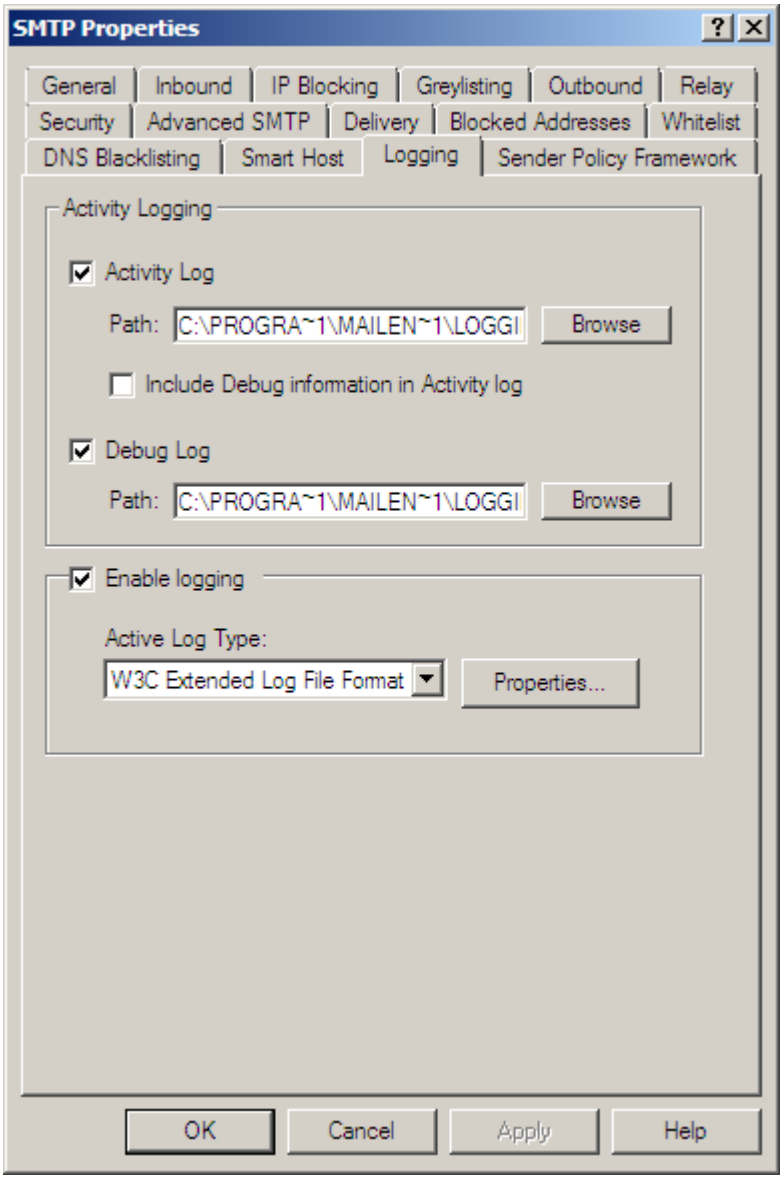
The following tokens can be used in a template: [ME_POSTMASTERADDRESS], [ME_TOADDRESS], [ME_DATE], [ME_MESSAGEID], [ME_FAILEDRECIPIENTS] and [ME_MESSAGEHEADERS]

6.14.9 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 requires authentication	The server that is being forwarded all of the email may require SMTP authentication. If so, enable this option and enter the username and password that has been assigned. The login method used is AUTH LOGIN.
Domain smart-hosting takes priority	It may be desirable to configure a local domain in MailEnable and smart-host this to a different server to the general outbound email. Enabling this option will allow the smart-hosts that have been configured for individual domains to override the SMTP outbound smart-host.

6.14.10 SMTP - Logging

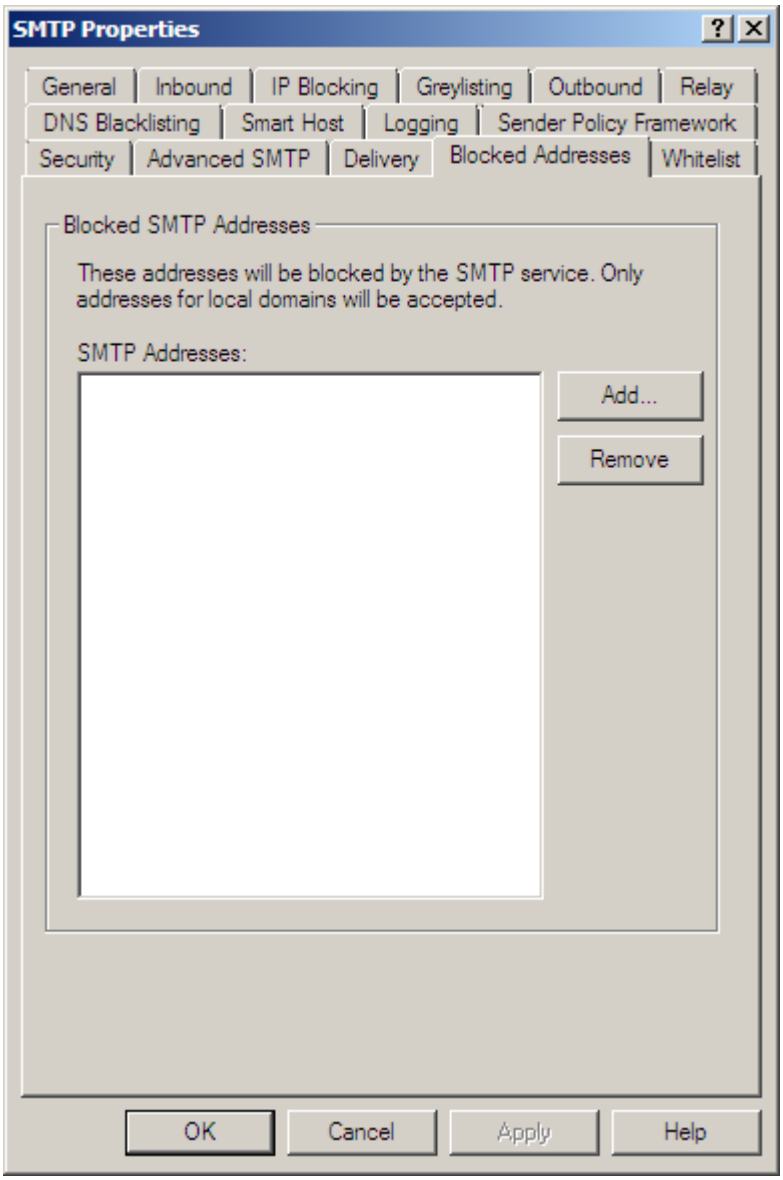


MailEnable's SMTP Connector provides W3C, Activity and Debug logging. W3C logging is used to record service usage, Activity logging is used to record system activity and Debug logging is used to provide low-level information on system activity.

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.

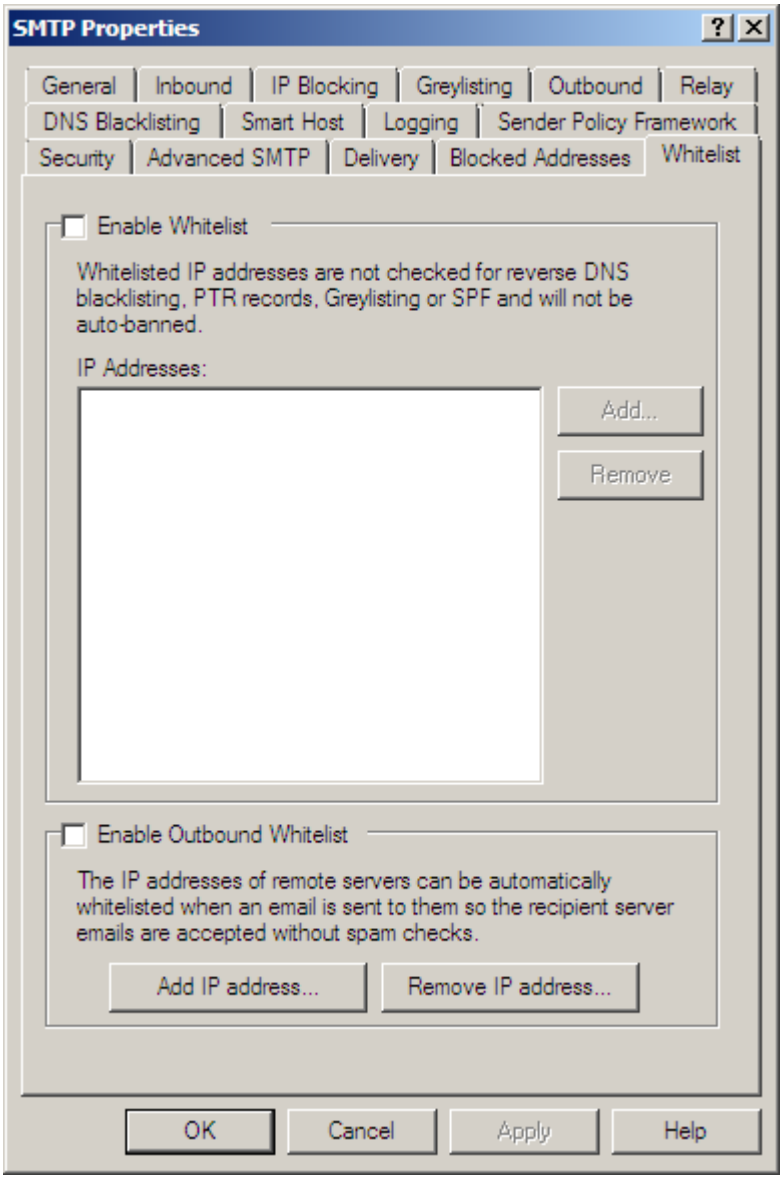
6.14.11 SMTP - Blocked addresses

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.

6.14.12 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.

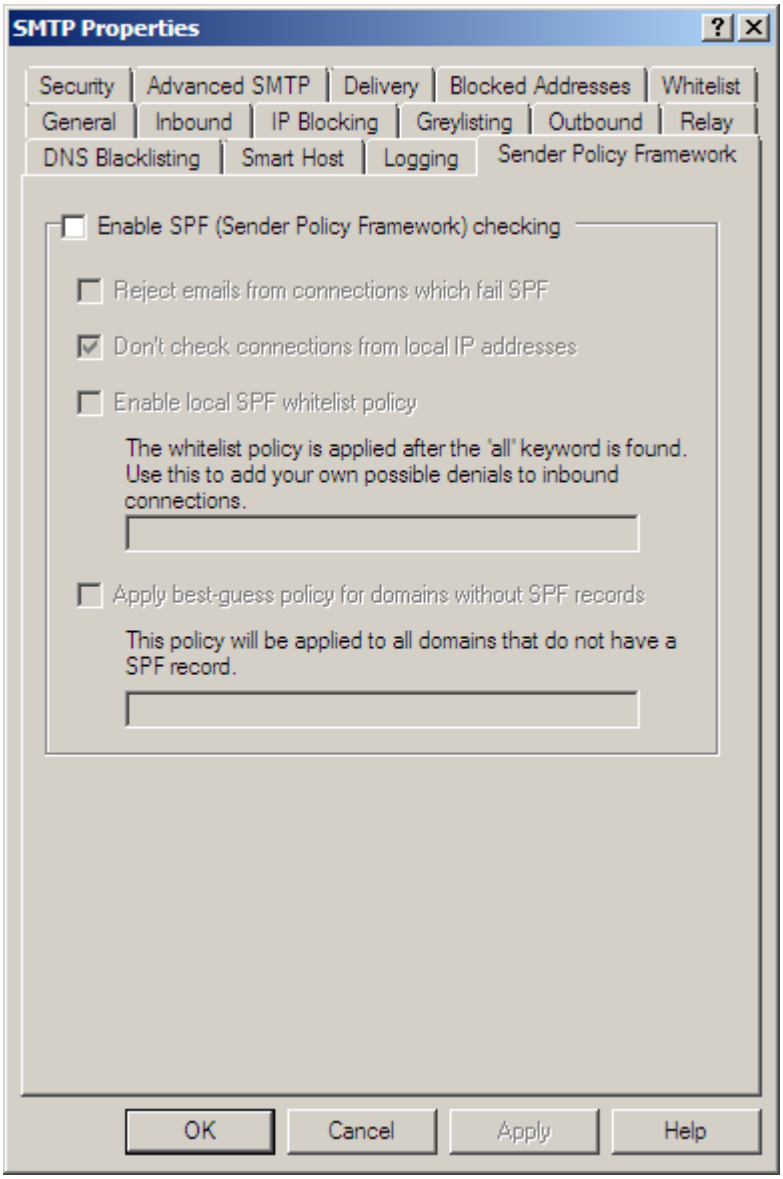
MailEnable can also automatically whitelist IP addresses to which it has addressed outbound e-mail. This helps reduce the SMTP service from rejecting email from valid senders, as it makes the assumption that if you send to an IP address then that IP is a valid mail server and incoming email from that 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.

6.14.13 SMTP - Sender Policy Framework (SPF)

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

In basic terms, Sender Policy Framework (SPF) is a method of detecting when an email sender is forging their sender address. It does this by confirming with the senders alleged domain (via DNS lookups) as to whether the connecting IP address, or other details, are valid. For example, if a spammer was sending emails as greatdeals@hotmail.com, a lookup is done for SPF details against the hotmail.com domain. Information returned from this lookup could determine that since the IP address of the spammer is not Hotmail IP address then it is likely to be spam. Email can then be marked as likely spam, or not accepted. An SPF record can also be more complicated than just a list of IP addresses, in order to give more flexibility. SPF is defined in RFC 7208 at https://tools.ietf.org/html/rfc7208.



Setting	Description

Enable SPF	Enables SPF detection.
Reject failures	If an incoming connection returns a SPF fail, then the email message will not be accepted by the SMTP service.
Add Received-SPF header for unauthenticated senders	Adds the Received-SPF header to all unauthenticated emails arriving via SMTP.
Pass local IP addresses (no checking will be done)	If an IP address is determined to be local, then an SPF check is not done.
Enable local white list policy	Use your own SPF white list policy. The local policy is checked when the **all** mechanism exists for the domain being checked and is not indicating a **pass**. The local policy only has an effect if it is passing the domain, so you would create an SPF that indicates requirements for domains you wish to pass. The white list policy can be a complete SPF record, but must exclude the SPF version string (i.e. Must not have “v=spf1”).
Apply best guess policy for domains without SPF records	For connections that do not have an SPF record further checks can be added in their place. A subsequent check could be done on an MX record or even an A record for the domain lookup.

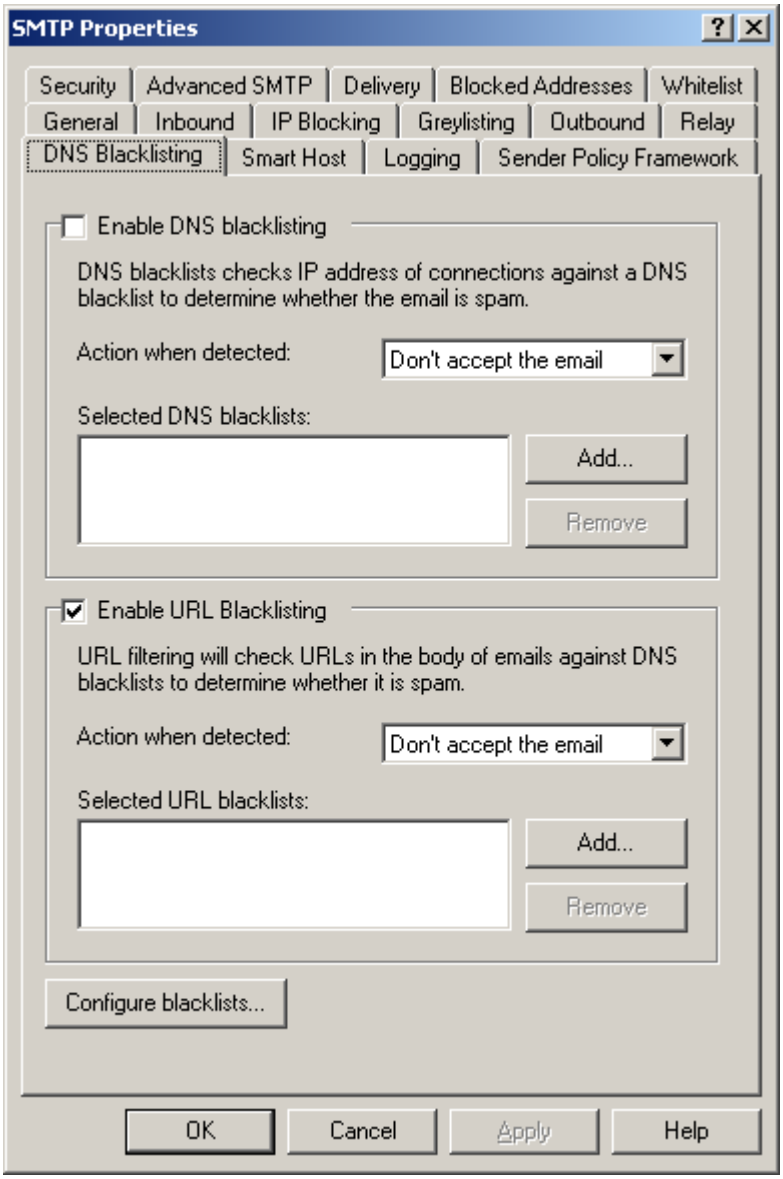
With MailEnable, the results of a SPF test are added as a header item to the email. The header is **Received-SPF**. SPF tests return one of seven results, which are outlined below. The added header includes the result and a brief description. If there are filters running to check the header, the first string after the header is the result. E.g. Received-SPF: none, Received-SPF: fail. For information on configuring filters for handling SPF results, please see the **Standard filter criteria section (Section 9.4.2)**.

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

6.14.14 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 (Section 5.3.12)**.
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 (Section 5.3.10)**. 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.

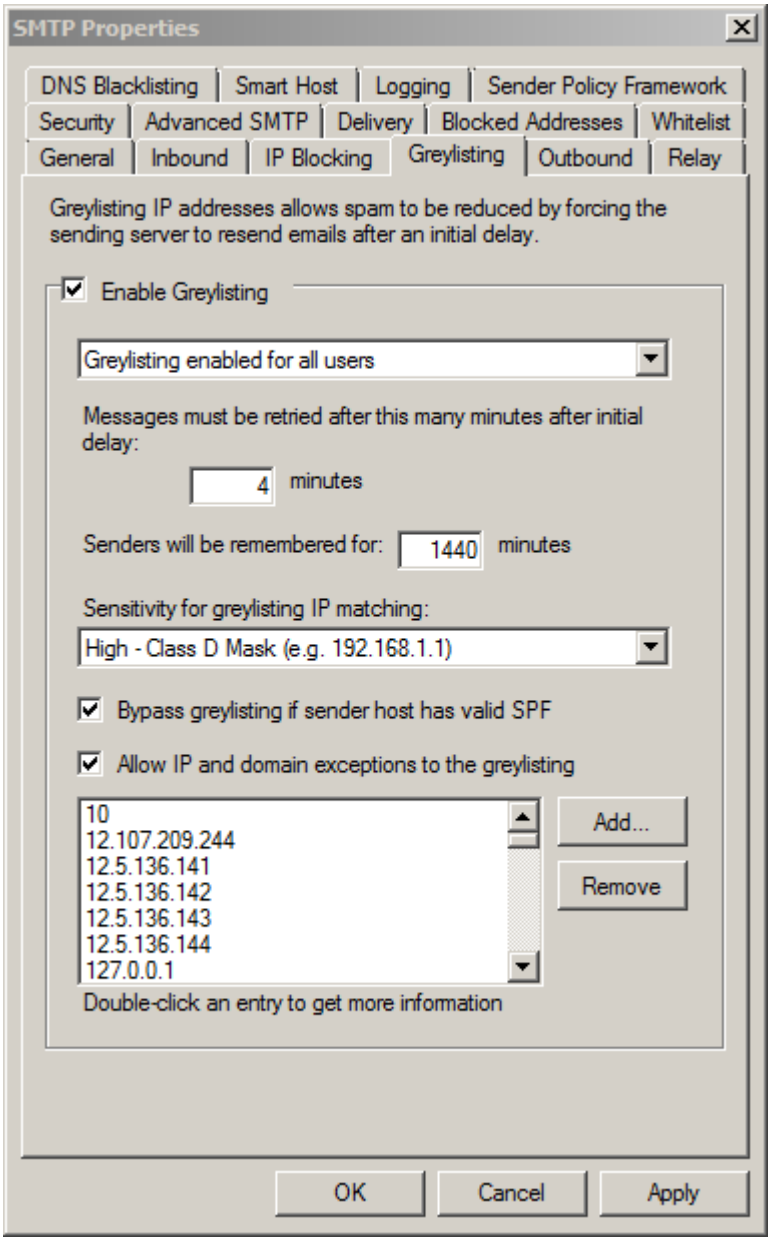
Note: It is possible to configure a white list that will override the reverse DNS blacklist. This is configured in the administration program by selecting the White list button on the Reverse DNS Blacklisting tab under the properties of the SMTP Connector.

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.

6.14.15 SMTP - Greylisting

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

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



Setting	Explanation
Enable greylisting	Enables SMTP greylisting. **Greylisting enabled for all users:** Enables SMTP greylisting for all mailboxes **Greylisting status determined by postoffice:** Will set the greylisting option to be determined by the postoffice. Please see **Postoffice - Feature Selection (Section 5.3.10)** for more information.
Messages must be retried this many minutes after initial delay	When the SMTP service accepts a connection from an IP address it will remember the sender and recipient and the connection will be temporarily refused. The connection will be refused until after this initial delay period.
Senders will be	After a sender has sent the message the second time, the sender, recipient and sender IP address are remembered for this time period, to prevent the email being delayed again.

remembered for	
Sensitivity for greylisting IP matching	By default an exact IP address is required for an incoming message to pass through. You can loosen this restriction by changing the mask matching that is done on the IP address.
Bypass greylisting if sender host has valid SPF	This option will check whether the senders domain has an SPF record and whether it is correct. If the SPF record is valid for the connection then greylisting is bypassed.
Allow IP and domain exceptions to the greylisting	Some servers do not work well with greylisting. For example, Gmail may try to send the same message from different IP addresses. By adding their IP addresses you are able to allow Gmail to bypass greylisting checks. If the domain has an SPF record you are able to enter the domain instead of the IP addresses. The SMTP service will then check to see if the IP address matches the SPF record of the domain in order to determine whether to bypass greylisting.

When a client or server is being delayed due to greylisting, they will receive the following SMTP message:

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

6.14.16 SMTP - IP Blocking

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

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

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

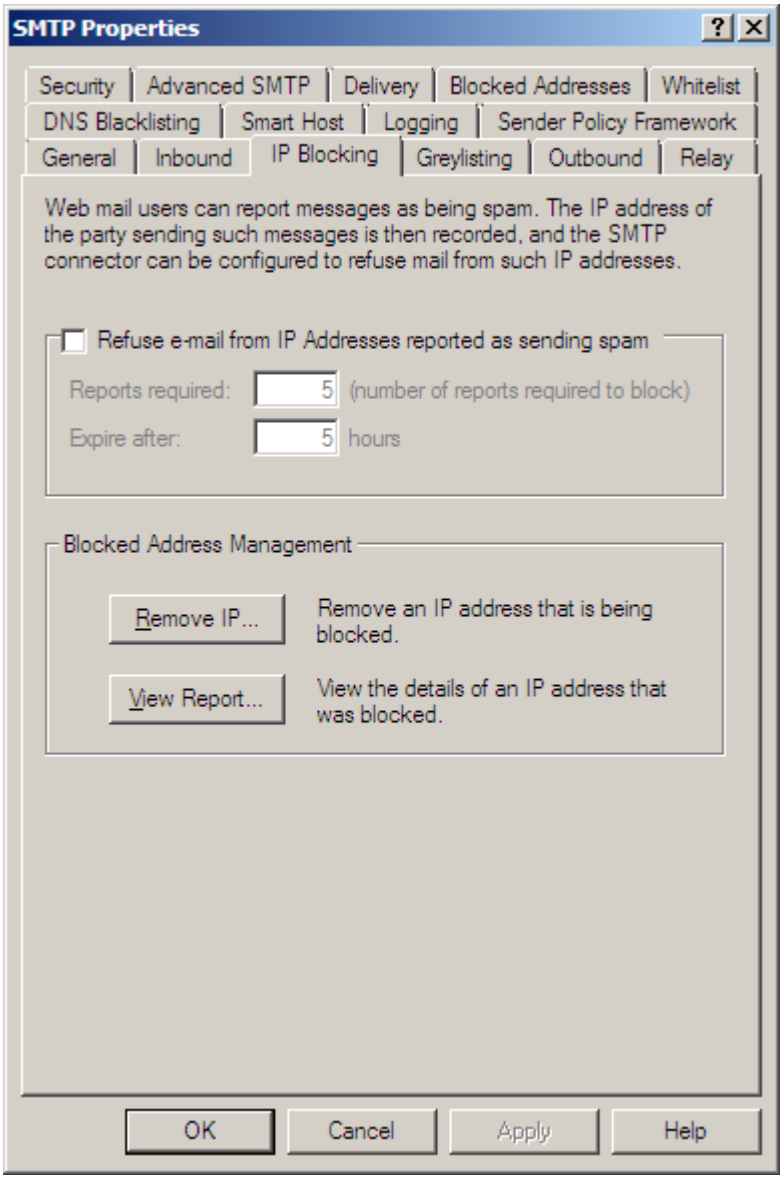
Connections are given an error when they perform a RCPT TO: SMTP command. When an IP address is blocked for the system level or post office level, the following message is in the SMTP Debug log:

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

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

The connecting server will be given the error:

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



Refuse e-mail from IP addresses reported as sending spam

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

Blocked Address Management

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

6.14.17 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.

6.14.18 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.

6.14.19 Queue Prioritization

Messages that are sent out as bulk e-mail or are part of an e-mail campaign will now automatically be assigned to a bulk mail queue. This means that bulk mail outs are less likely to impact on the delivery of regular e-mail.

Also, an administrator is able to designate users whose messages should be sent with Priority. Messages sent by these users are placed in a Priority queue so that they receive preferential treatment over other messages.

How to set messages sent from a mailbox with High Priority:

1. Navigate within the administration console to: **MailEnable Management > Messaging Manager > Postoffices > (postofficename) > Mailboxes > (mailboxname).**
2. Right click on a mailbox and select **Properties** from the popup menu.
3. Next navigate to the **General** tab.
4. Tick the option for **Deliver message with High priority.**

Please see **Mailbox - General (Section 5.5.3)**

6.15 SyncML

6.15.1 SyncML Protocol

The MailEnable SyncML server is a component of the synchronization service. It provides a means for client devices (such as mobile phones, PDA's etc.) to easily synchronize their contacts, calendar and tasks with an existing account on a MailEnable server (via HTTP requests). All that is needed on the client device is an internet

connection and SyncML support (which most mobile phones today will have).

The MailEnable SyncML server supports version 1.2 (and below) of the SyncML Synchronization Protocol. It can process SyncML conversations in one of two ways, by exchanging plain text XML packages or WBXML (WAP Binary XML).

Most phones will communicate via WBXML while other SyncML clients may communicate via plain text XML.

6.15.2 Using SyncML

Installing the SyncML Server

The MailEnable SyncML Server is a component of the Synchronization service.

Enabling the SyncML Server

The MailEnable SyncML Server needs to be enabled on the server in order for client devices to be able to connect to it and synchronize their data. This is done in the MailEnable administration program.

How to Enable:

1. Open the MailEnable administration program
2. Expand the **MailEnable Management->Servers->Localhost->Services and Connectors** branch
3. Right-click on **Synchronization** and select **Properties** from the popup menu
4. Select the **SyncML** tab and tick the **Enable SyncML Support** checkbox
5. Save the changes and restart the Synchronization service

Connecting to the SyncML Server

Once the MailEnable SyncML service has been enabled, client devices (such as mobile phones) can connect to it and perform synchronization. A SyncML profile will need to be created on the client with the information outlined below:

- **Server address**: http://www.yourserver.com/syncML
- **Server version**: 1.2 (or 1.1)
- **Synchronization type**: Both ways (or 2-Way)
- **Username**: the username of the account on the MailEnable server (e.g. 'bob@MailEnable').
- **Password**: the password for the account
- **Contacts remote database name**: card
- **Calendar remote database name**: cal
- **Tasks remote database name**: task

Advanced Settings

The installation will create a new registry branch called **SyncML** under the existing MailEnable branch for the synchronization service, i.e. *\HKEY_LOCAL_MACHINE\Software\Mail Enable\Mail Enable\Services\HTTPMAIL*.

Two new registry keys will be created under this branch:

- **MaxMsgSize** – The maximum size (in bytes) of any response **SyncML Message** to a given SyncML request message that is allowed in a **SyncML Package**.
- **MaxObjSize** – The maximum size (in bytes) of a data object that the server is able to receive

A **SyncML Message** is the primary contents of a SyncML Package. It contains the SyncML Commands, as well as the related data and meta-information. The SyncML Message is a well-formed, but not necessarily valid XML document.

A **SyncML Package** is a conceptual frame for one or more SyncML Messages that are required to convey a set of protocol semantics. It is the complete set of commands and related data elements that are transferred between an originator and a recipient.

6.15.3 SyncML Synchronization Data

The MailEnable SyncML synchronization data is stored under the **Config** folder of the MailEnable installation folder.

A **SyncML** folder is created directly under the **Config** folder by the SyncML server. It stores synchronization information such as client devices' last synchronization time, capabilities of client devices and also capabilities of the SyncML server.

File	Information
SyncMLDevices.xml	This file is created and updated (after every successful synchronization session with a client device) by the MailEnable SyncML server. It stores each client device's synchronization data, i.e. Next and Last synchronization time, client Datastore names for Contacts, Calendar and Tasks, and other properties of the client device (e.g. 'MaxMsgSize'). If this file is missing the MailEnable SyncML server will assume that no previous syncs were done between the client device so on the next sync request from the client device the server will attempt to perform a SLOW SYNC, whereby the server requests all data items from the client device and also sends back all of its server data items. This may cause duplication of data on the server and client device.
/Config/Postoffices/SyncML	The SyncML server also saves other sync data in this folder. Each Postoffice will have its own folder under here and a folder for each account being synchronized will be created under that Postoffice. E.g. **/Config/Postoffices/SyncML/MailEnable/Bob** will be created for the account **Bob** which belongs to the **MailEnable** Postoffice.

An XML file will be created for each Datastore (Contacts, Calendar or Tasks) being synchronized, each file holding information about the items that the SyncML server knows currently exist in that Datastore.

Via Webmail:

1. Login to the mailbox via Webmail and go to the Options tab
2. Click on **Advanced** > **SyncML Devices**
3. Each client device that has successfully synced with the server will be listed there and its corresponding sync cache data can be deleted via the **Clear Cache** link next to it.

Via the server's file system:

1. Go to the '**/Config/Postoffices/SyncML/*MyPostoffice*/*MyMailbox***' folder under the MailEnable installation folder; where *MyPostoffice* and *MyMailbox* is the corresponding *postoffice* and *mailbox*
2. Delete all the corresponding XML files for each DataStore (e.g. '**[MyDeviceID]-Calendar.xml**', '**[MyDeviceID]-Contacts.xml**', and '**[MyDeviceID]-Tasks.xml**')
3. Go to the '**Devices**' folder directly under the current folder

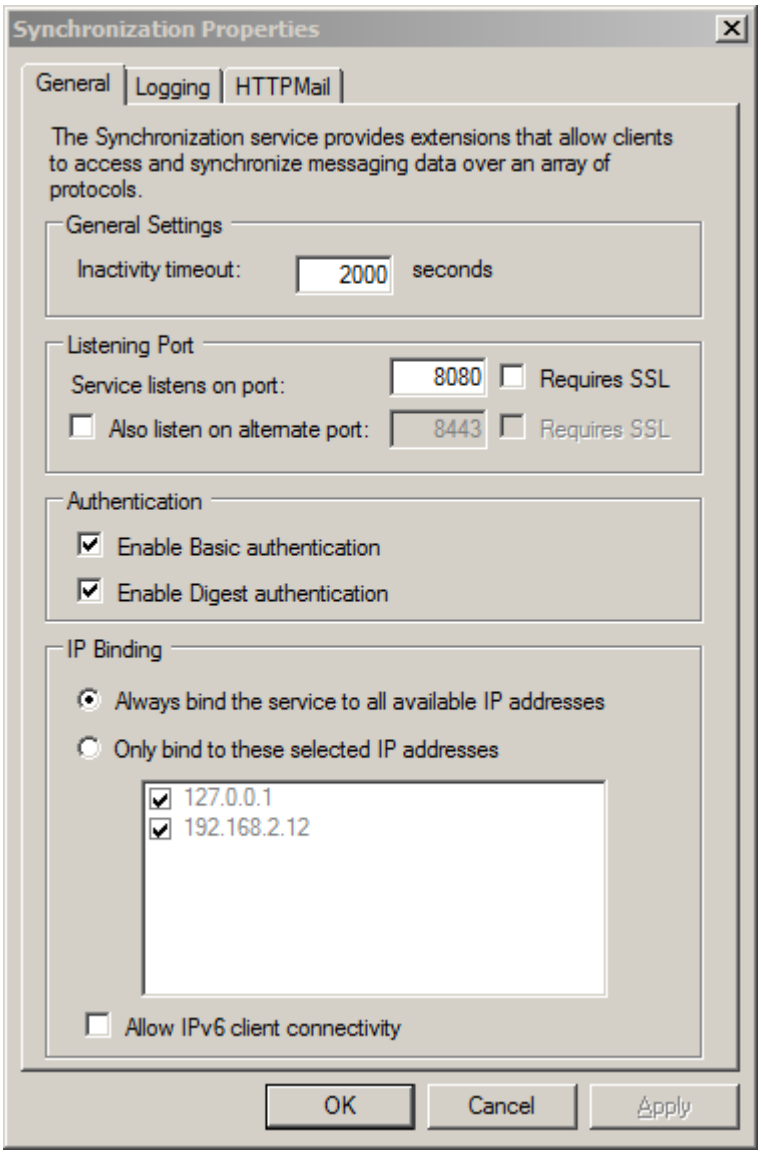
Delete the corresponding *DevData* XML file with matching client device ID.

CAUTION: Deleting **SyncMLDevices.xml** will cause ALL previous information about SynML synchronizations with ALL client devices to be lost.

6.16 Synchronization Service

6.16.1 Synchronization - General

The Synchronization Service provides extensions that allow clients to access and synchronize messaging data over an array of protocols. The service can handle SyncML, CalDAV, CardDAV and ActiveSync. CalDAV, CardDAV and ActiveSync can also be handled through IIS, which can give more flexibility for SSL and domain name configuration.

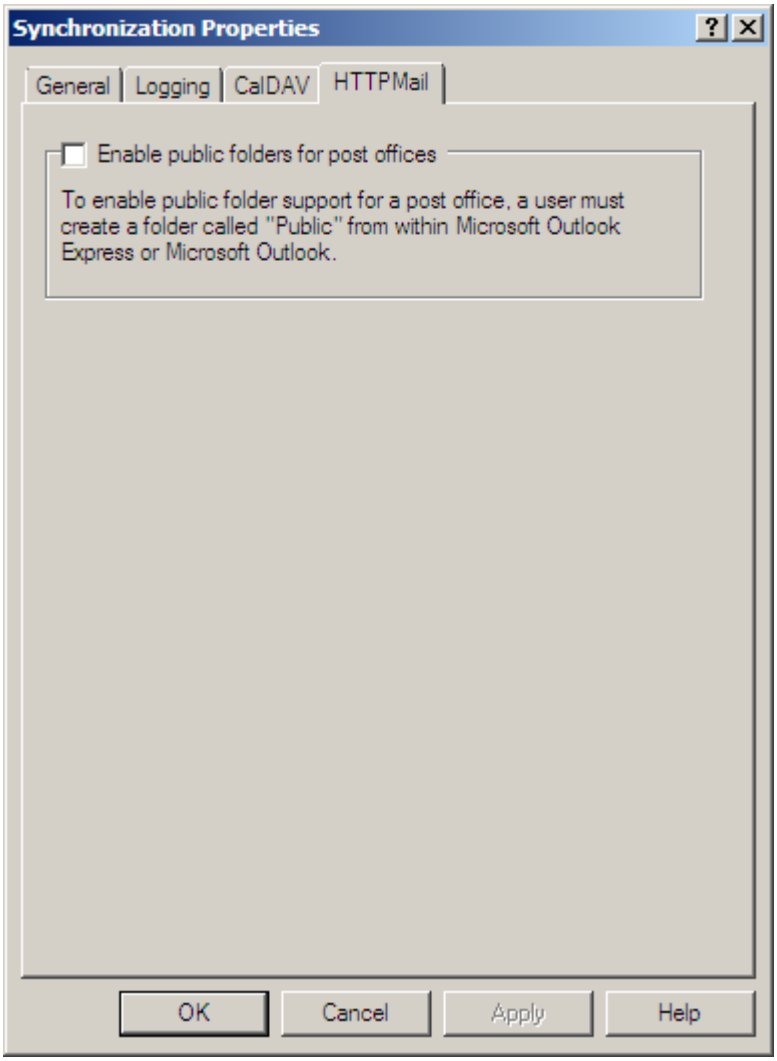


Setting	Description
Inactivity timeout	Determines how long a connection will remain active for.
Service lists on port	The Synchronization service will listen for connections on this port.
Also listen on alternate port	The Synchronization service will also listen for connections on this port.
Enable Basic authentication	Allow connections to use Basic authentication.

Enable Digest authentication	Allow connections to use Digest authentication. Digist authentication should be disabled if you wish to use Windows authentication.
IP Binding	It is possible to select the IP addresses that the Synchronization 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.
Allow IPv6 client connectivity	Allow connections using IPv6.

6.16.2 Synchronization - HTTPMail

HTTPMail is a protocol that Microsoft used for connecting Windows Live Mail and Outlook Express to Hotmail a few years ago. HTTPMail provided an alternative to using POP, IMAP, and SMTP, and had advantages such as being able to be used over the standard web page port (80). Since those clients are no longer supported by Microsoft, and Hotmail no longer uses the protocol, it is not recommended to configure new users to use this.



Setting	Description
Enable public	Public Folders allow one or more mailboxes under the post office to share data (messages in a folder that is seen by all mailboxes in the post office.)

folders for post offices	Anything placed in this folder (Program Files\MailEnable\Post Offices\[Post Office Name]\Pubroot) will become visible to all other mailboxes in the post office. This feature must be enabled for the post office in Post Office Properties. Please see **Postoffice - Message Store (Section 5.3.12)**

6.16.2.1 Configuration

HTTPMail requires very few configuration settings. The major configuration settings are the IP address(es) and port bindings for the MailEnable Synchronization Service (Please see **Synchronization General (Section 6.16.1)**). If the option to install HTTPMail is selected, the service is published on port 8080 of the server (it is possible to change this setting to an alternate port, but 8080 is the default so that the Synchronization service does not conflict with any existing web services that may be running).

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

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

http:// Your Server: 8080/MEHTTPMail

Since HTTPMail is an authenticated service, use the usual account credentials when prompted (i.e.: User@ Your Account/Postoffice). For a more detailed explanation of configuring HTTPMail for mail clients, please see the **Configuring email clients section (Section 11.1)**.

6.16.3 Synchronization WebDAV

WebDAV is a set of methods based on the Hypertext Transfer Protocol (HTTP) that facilitates collaboration between mailboxes in editing and managing documents and files stored within their respective MyFiles folders. Mailbox owners can access their **My Files** folder as a network drive over the WebDAV protocol. For example, a mailbox can take a photo with their iPhone and immediately save it to MyFiles folder on the MailEnable server using a WebDAV client on the device (I.e: WebDAV Navigator).

Required configuration settings for a WebDAV client:

Server URL: http://exampledomain.com:portnumber/MyFiles (port number is the port number that the synchronization service is running on. Please see **Synchronization General (Section 6.16.1)**)

Username: mailboxname@postofficename

Password: ******

6.17 Web Administration

6.17.1 Web administration

The Web Administration interface to allows postoffice administrators to manage various services remotely via a web browser. Web Administration allows you to delegate management of Postoffices to Postoffice administrators. This effectively reduces your administration load, especially if you are hosting multiple postoffices (for example, one per customer or company), each company can manage their own configuration. You can also restrict the number of mailboxes, lists created in each postoffice via the Web Administration interface.

Mail users who have been marked as system administrators (SYSADMIN) can use the web administration to perform the same server administration tasks as the MMC administration program.

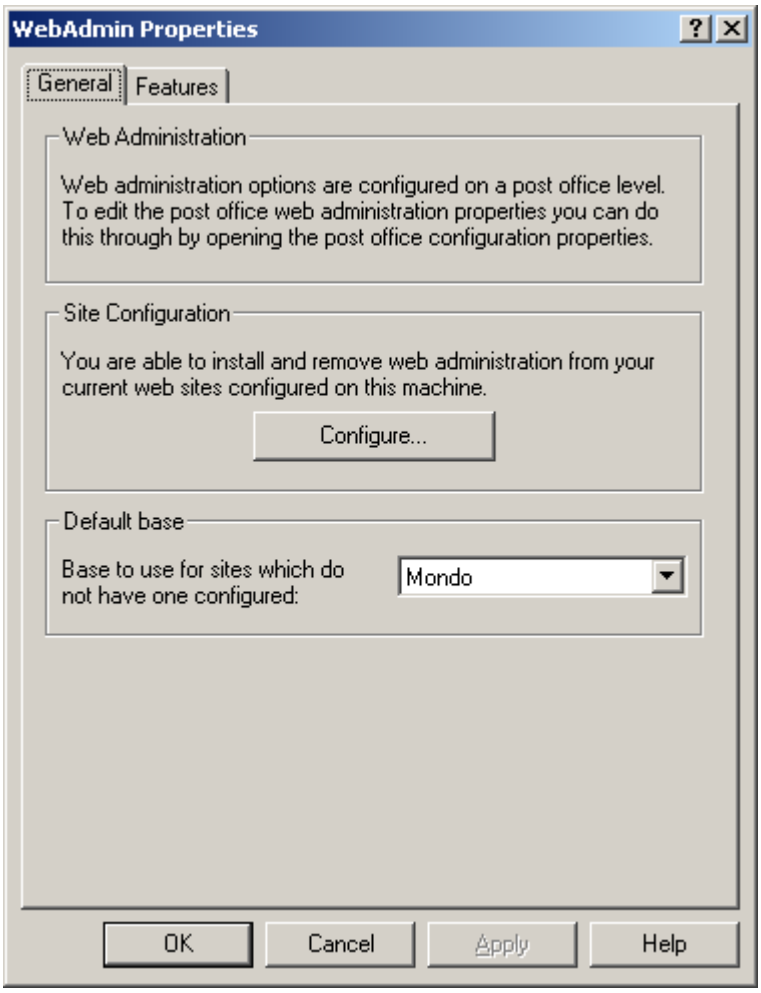
Some of the many features are:

- Manage domain related information

- Manage the creation of email addresses
- Manage email lists and groups
- Custom skins, leveraging skins from web mail

6.17.2 WebAdmin - General settings

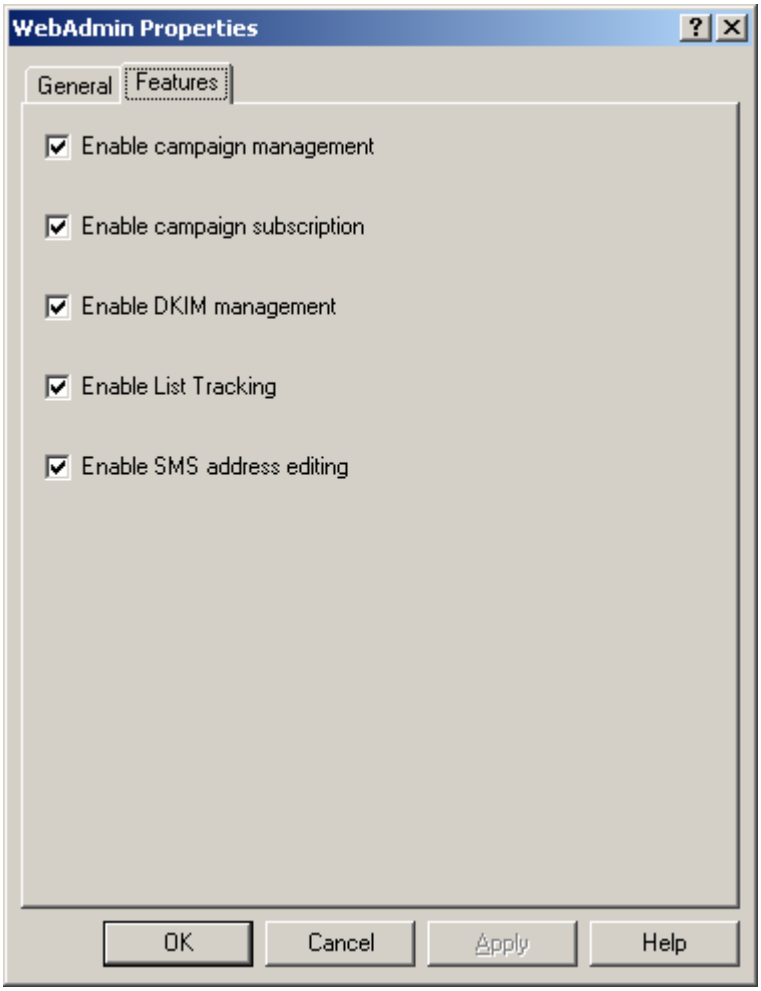
To access the Web administration general settings navigate within the administration console to: **Servers > localhost > Services > Webadmin.** Right click on Webadmin and select **properties.**



Settings	Description
Configure...	Opens the Site configuration window. Please see **How to add the Web Administration interface to web sites within IIS (Section 6.17.5)**
Default base	Is the default base folder for the Web administration interface if one has not been specifically assigned to a website.

6.17.3 WebAdmin - Features settings

To access the Web administration feature settings navigate within the administration console to: **Servers > localhost > Services > Webadmin.** Right click on Webadmin and select **properties** and navigate to the **Features** tab.



Settings	Description
Enable Campaign Management	Enables the Campaign Management page. For more information about Campaign Management please see **Advertising and Campaign Management (Section 5.11)**
Enable Campaign Subscription	Enables the option to subscribe to campaigns within Campaign Management
Enable DKIM Management	Enables the ability to manage DKIM (DomainKeys). Please see **Domain - DKIM (DomainKeys) (Section 5.4.4)** for more information about DKIM
Enable List Tracking	Enables the list tracking page for list member subscription management. Please see **Lists - General (Section 5.9.3)** on how to enable List tracking for a list.
Enable SMS address editing	Enables the ability to manage SMS addresses. Please see **SMS Addresses (Section 5.6.1)**

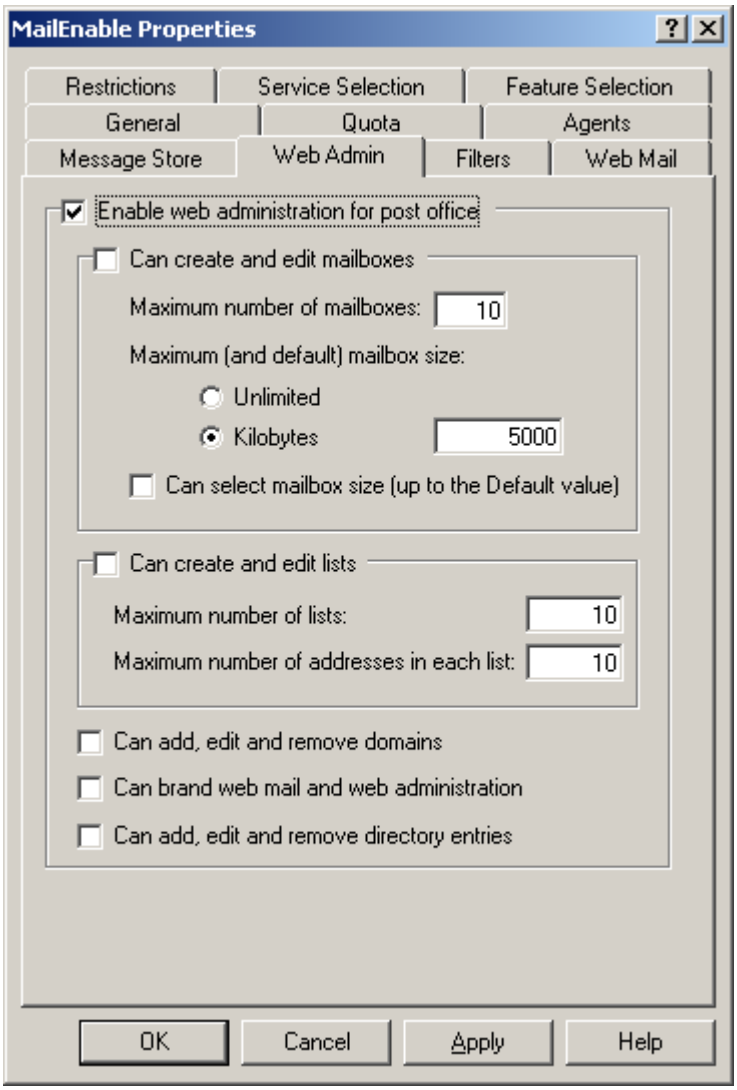
6.17.4 How to enable the Web Administration interface

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

How to Enable the Web administration interface for a postoffice

1. Navigate to the following location within the administration console: **Messaging Manager > Postoffices > (Postofficename)**

2. Right click on the post office name, and select **Properties** in the menu.
3. Next navigate to the **Web Admin** tab.
4. Select the **Enable web administration for post office** checkbox.



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

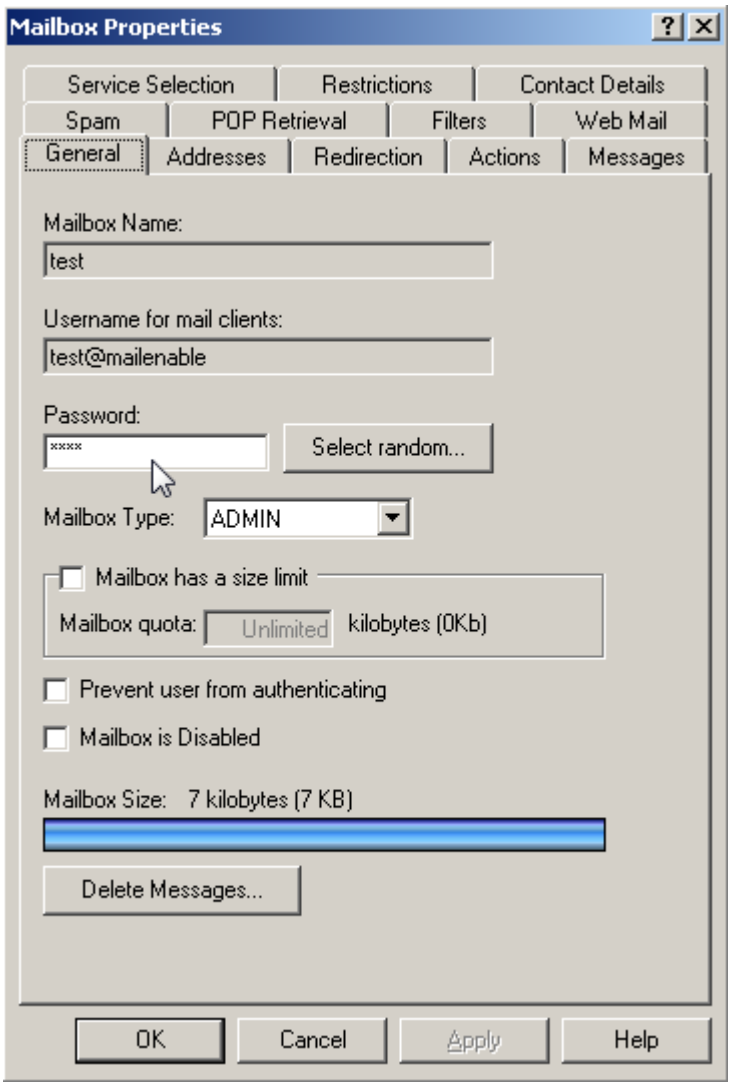
Tip: Please refer to the **Postoffice - Web admin (Section 5.3.14)** section for information about web admin properties

How to configure a mailbox as an ADMIN or SYSADMIN user for the Web Administration interface

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

1. Navigate to the following location within the administration console: **Messaging manager > Postoffices > (post office name) > Mailboxes > (mailbox name)**
2. Right click on the mailbox name and select **properties**
3. Use the drop down menu for the **Mailbox Type:** option and set the user as **ADMIN** or **SYSADMIN** (Enterprise only)

Note: A **SYSADMIN** user has the ability to administer all post offices on the server. **SYSADMIN** users are exclusive to the Enterprise and Enterprise Premium versions of MailEnable.



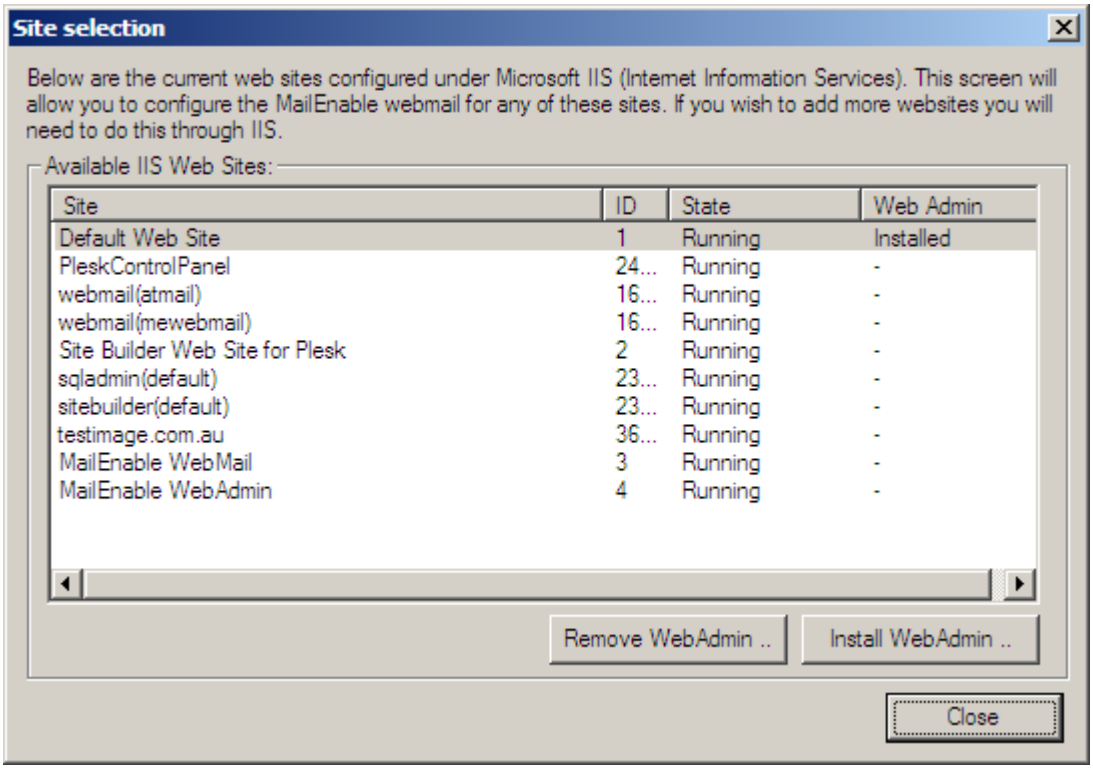
6.17.5 How to add the Web Administration interface to web sites within IIS

How to add the Web Administration interface to other web sites within IIS as Virtual Directory

To allow the Web administration 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:

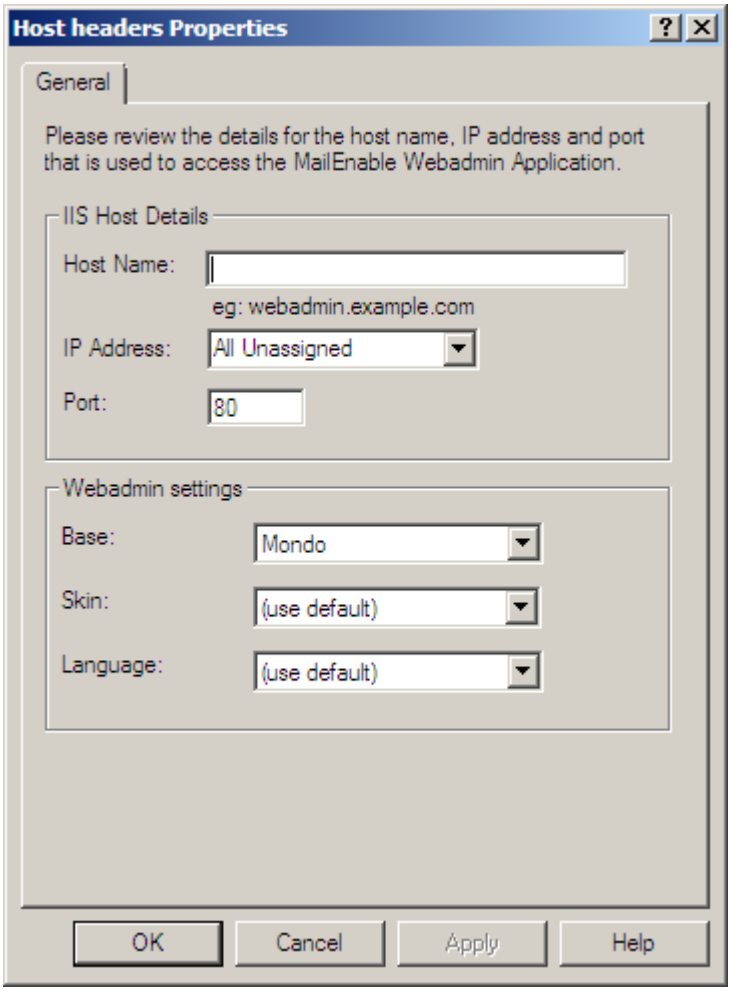
1. Navigate to the following location within the administration console: **MailEnable Management > Servers > localhost > Services > WebAdmin**
2. Right click on **Webadmin** and select properties.
3. Under the **General** tab click on the **Configure** button in the site configuration section.
4. Select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

Tip: To remove a Web Administration virtual directory from a web site repeat the above steps however use the **Remove WebAdmin** button.



How to add a Web Administration host header under the MailEnable Web Admin web site

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > localhost > Services > WebAdmin**
2. Right click on **WebAdmin** and select: **New > Host Header...**
3. Specify a host name.
4. Select an available IP Address using the drop down for **IP Address:**
5. Specify the **port** number
6. Specify which **base** folder is to be set for the host header entry
7. Specify the **skin** to set for the host header entry
8. Finally specify the default **Language** for the host header



Setting	Description
Host name	The host name is the domain name users type in their web browser to access the web administration. You may wish to give the web administration a URL similar to webadmin.example.com. A DNS entry has to be created in order to direct users to the IIS server.
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
Base	Set the base (Professional or Enterprise Edition) for web administration
Skin	Set the skin for the web administration interface
Language	Set the language for the web administration interface

6.17.6 How to access the Web Administration interface

How to access the Web Administration interface via a virtual directory under a web site in IIS

Once the Web Administration virtual directory has been installed under a web site within IIS the following URL can be used to access the interface:

Example: http://exampledomain/meadmin

In place of the *exampledomain* in the above example, use the server name as defined in DNS or under IIS. The IP address of the machine can also be used.

When browsing to this location, the Web Administration logon screen will appear.

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

Note: If the error **Invalid User** occurs, either the post office is not enabled for web administration or the mailbox is not set as an **ADMIN** user.

How to access the Web Administration interface via a host header entry under the MailEnable Webadmin web site

Once a host header entry has been created for the MailEnabel wed admin web site within IIS the following URL can be used to access the interface:

Example: http://exampledomain

6.18 Web Mail

6.18.1 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
- Management of POP retrieval
- Configure redirection
- Reply, reply to all, forwarding, read receipts, message priority
- Viewing & editing of HTML mail
- Support for various character sets (Big5, etc.)
- E-Mail Signatures
- Manage folders
- Configure POP Retrieval
- Custom skins

MailEnable web mail is installed as a Virtual Directory under an existing IIS Web Site. Typically there are two web sites that are pre-configured under IIS, these are the **Default Web Site** and the **Administration Web Site**. IIS allows additional sites to be created (either using host-headers or additional IP addresses) using the Internet Services Manager. 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 6.18.3.2)**

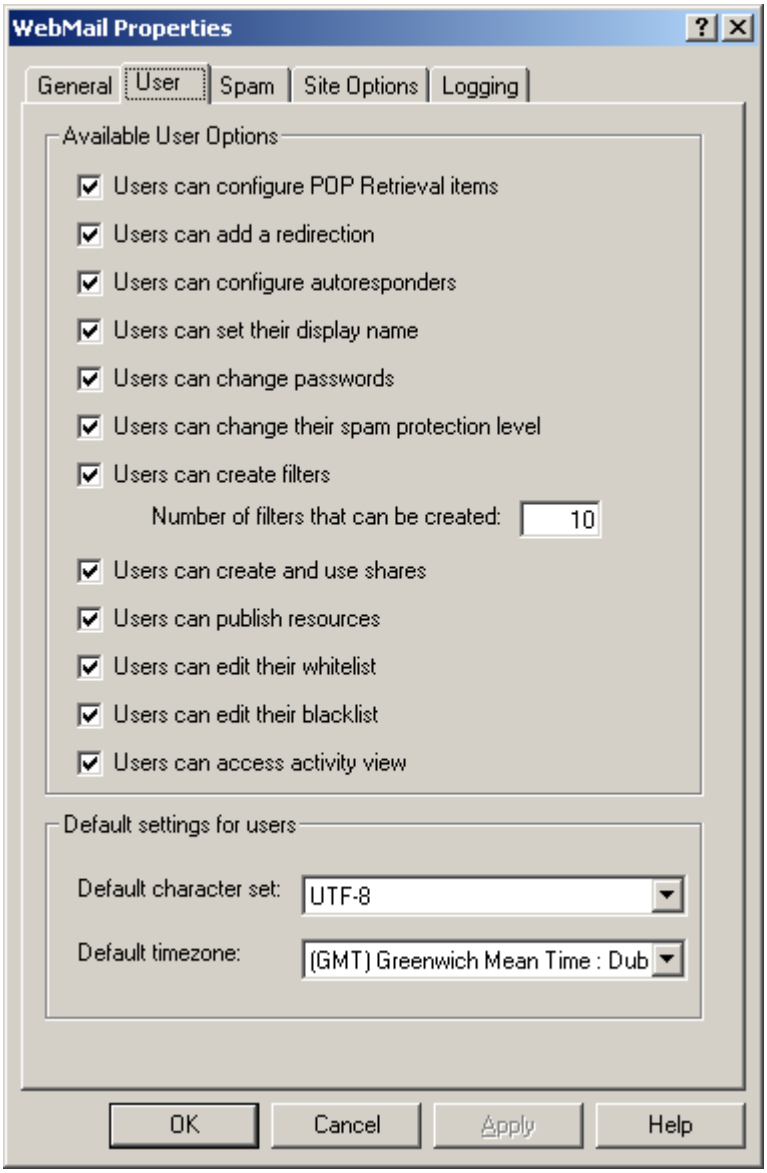
6.18.2 Web Mail - Properties

6.18.2.1 Web Mail - General

Setting	Description
Enable Global address lists	Makes global address lists visible to web mail clients when a user selects the address “TO…” link in a new message. Global address lists are created in the administration program.
Enable Public folders	This allows usage of public folders within MailEnable. Public folders allow messages to be stored on a postoffice level, so all users in a postoffice have access. It does not allow the storage of calendars or contacts, just emails. Users either have read access or full access to the public folders tree. Permissions for webmail access to the public folder tree can be set globally under the **Site Options** tab, or at a postoffice level. To do this at the postoffice level, navigate to MailEnable Management->Messaging Manager->Post Offices branch, right click on a postoffice and select the **Web Mail** tab. Public folders can be disabled for a postoffice under the **Message Store** tab under the postoffice properties.
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
Enable banner and usage display	When enabled, shows an advertising banner in the top right hand corner of the interface. Please see **Advertising and campaigns (Section 5.11)** for more information:
Enable help	Enables help links within the web mail interface
Enable notification of new emails	MailEnable allows for an alert pop up in the Windows task bar when the web mail inbox has received a new message. If the alert happens too frequently then the polling interval can be set by changing the value here “Check Every” – “X” number of minutes.
Enable forgotten password recovery option	Enables the forgotten password recovery option. Please refer to the web mail user guide for more information about the Password Recovery option: https://www.mailenable.com/documentation/webmail
Don't add client IP address to headers	When enabled will mask the clients machine within the headers of the message.
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.
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.
Remove	This option rebuilds HTML emails to remove any scripting or unrecognized HTML items in order to

unknown tags and scripts from HTML emails	help prevent exploits or oddities from occurring.
Prevent the loading of remote images in HTML emails	When displaying HTML emails, links to external images can indicate to a remote server that you have read the email (so spammers know that it is a valid email address). This option will prevent any image from displaying in an email if the image is not contained within the email itself.
Display image attachment when viewing a message	Enables/disables the ability to view message attachments within the message preview pane.
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.

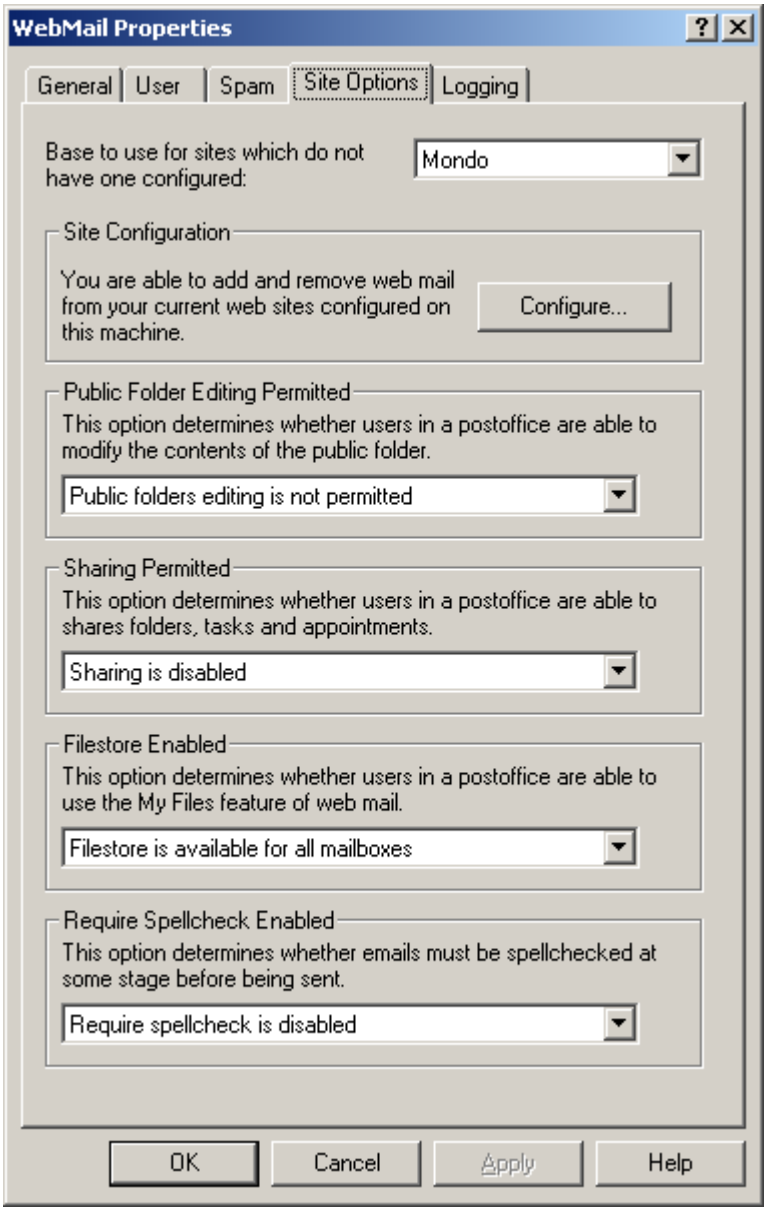
6.18.2.2 Web Mail - User



Setting	Explanation
Users can configure POP Retrieval items	Determines whether the user can configure POP retrieval in the web mail options tab.
Users can add a redirection	Determines whether web mail users are permitted to redirect their mail to alternate addresses.
Users can configure autoresponders	Determines whether web mail users are permitted to configure auto responses for their mailbox (e.g. Out of Office automatic replies).
Users can set their display name	Allows users to specify the friendly name to be used.
Users 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.
Users can change	This gives a mailbox user the ability to change their password in the options of the web mail.

passwords	
Users can change their spam protection level	Allows the mailbox to be able to configure spam protection rules.
Users can create filters	This allows the user to create filters inside the options of web mail. A limit can be placed on the number of filters each user can create.
Users can create and user shares	Allows the mailbox to be able to view the shares options and shares folder tree
Users can publish resources	Determines whether a mailbox can publish resources. Please see **Published Calendars (Section 6.2.3)** for more information
Users can edit their whitelist	Determines whether a mailbox can view their whitelists and be able to add/edit the whitelist
Users can edit their blacklists	Determines whether a mailbox can view their blacklists and be able to add/edit the blacklist
Users can access activity view	Allows the user to be able to view the statistics button to view activity reports. Please see **Localhost - Auditing (Section 5.10.4)** on how to enable activity reports
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.

6.18.2.3 Web Mail - Site Options

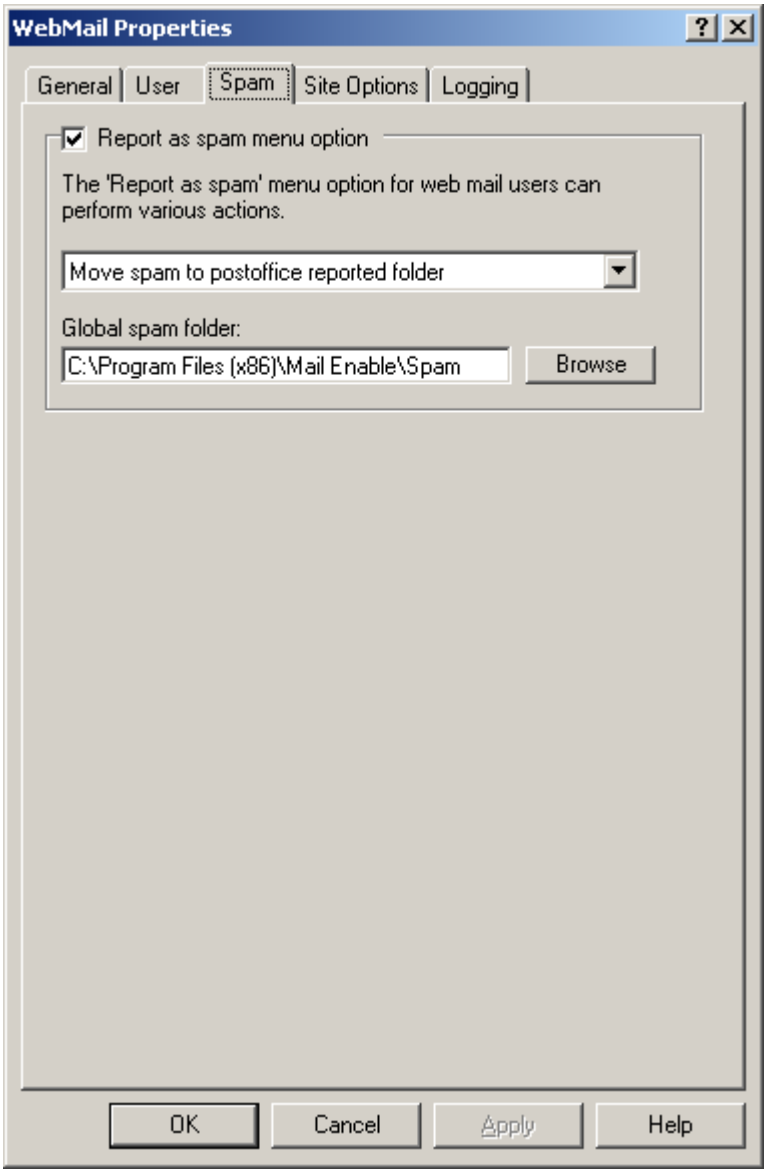


Setting	Explanation
Base to use for sites which do not have one configured	To set the base design for all sites, make a selection from the drop down combo box.
Site Configuration	If the **Configure…** button is selected the **Site Configuration** screen is displayed. This is where skin and web mail display options can be set on a per post office basis. 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. By making selections within this screen the available skins can be seen and you can check what skins are available for the MailEnable web mail server base that you have selected and choose a base skin for a selected site. See the **Publishing via host headers of virtual directories section (Section 6.18.3.2)** for more details.
Enable Web mail logging	This will enable and log web mail usage. The higher the level the more actions by a user that are logged. The default path to where this log file is saved is: Program Files\MailEnable\Logging\Webmail

Public Folder editing Permitted	This options determines whether users in a postoffice are able to modify the contents of a Public Folder. This can be set as a global option which will enable Public Folders for all mailboxes in all postoffices or alternatively set at the postoffice level. Please refer to the **Postoffice - Web mail (Section 5.3.11)** tab section for more information about postoffice level settings.
Sharing Permitted	This option determines whether users in a postoffice are able to share Folders, Tasks and Calendar appointments. This can be set as a global option which will enable Sharing for all mailboxes in all postoffices or alternatively set at the postoffice level. Please refer to the **Postoffice - Web mail (Section 5.3.11)** tab section for more information about postoffice level settings.
FileStore Enabled	This option determines whether users in a postoffice are able to use the MyFiles feature of web mail. This can be set as a global option which will enable MyFiles for all mailboxes in all postoffices or alternatively set at the postoffice level. Please refer to the **Postoffice - Web mail (Section 5.3.11)** tab section for more information about postoffice level settings.
Require Spellcheck	This option determines whether messages need to spell checked before sending. **Require spellcheck disabled:** Disables the spellchecking before sending. **Require spellcheck for all mailboxes:** Enables the spellchecking before sending for all mailboxes. **Require spellcheck configured per postoffice:** Enables spellchecking before sending at the postoffice level. Please see **Postoffice - Web Mail (Section 5.3.11)**

6.18.2.4 Web Mail - Spam

The **Report as spam** web mail option allows web mail users to mark messages as spam and have an action perform on them. The following table lists the actions that can be undertaken when a webmail user marks a message as being spam:



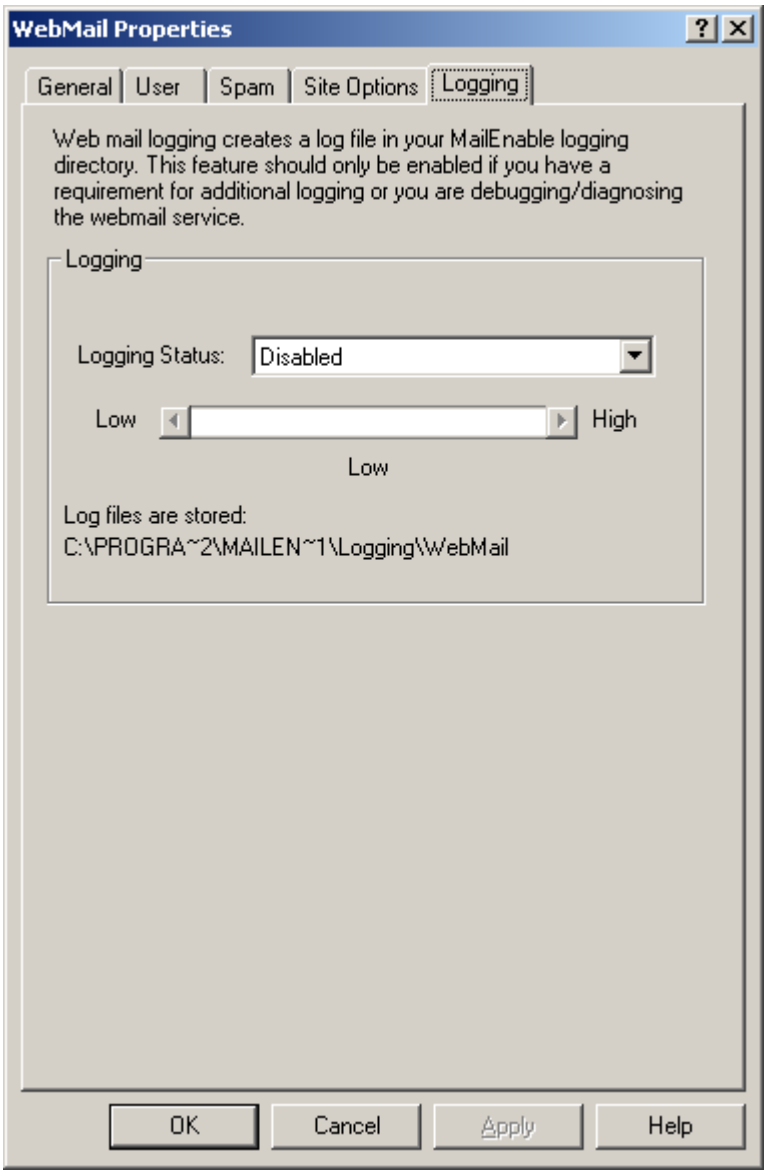
Setting	Explanation
Use post office settings	Use the post office level setting,
Move spam to post office reported folder	The post office reported folder is: Mail Enable\Post offices\[post office]\mail root\spam\Reported
Move spam to global spam folder	The global spam folder is the one selected under the Report as spam option.
Delete message	Any message that is marked as spam will be deleted.
Mark the sender IP as spam source	Extracts the sending IP address of the message from the headers of the message and creates 2 records in the following locations: Config\Postoffices\Postoffice\Connections\Spam Config\Connections\Spam The SMTP connector (and custom filters) can then use these records to determine whether or not to refuse mail from the IP address.
Copy spam to postoffice	The post office reported folder is:

reported folder then junk	Mail Enable\Post offices\[post office]\mail root\spam\Reported The message will be delivered to the users junk folder as well.
Copy spam to global spam folder then junk	The global spam folder is the one selected under the Report as spam option. The message will be delivered to the users junk folder as well.
Move message to junk folder	The message is just moved to the users junk folder.
Mark the sender IP as spam source then junk	As well as marking the sender IP as spam source the message will be delivered to the users junk folder.

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

6.18.2.5 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.

6.18.2.6 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.
SMS via Exchange ActiveSync	If an ActiveSync license is purchased for the server, webmail users can send SMS messages from their synced mobile devices by using webmail.

6.18.3 Configuring Web Mail

6.18.3.1 Configuring web mail Overview

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

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

6.18.3.2 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.

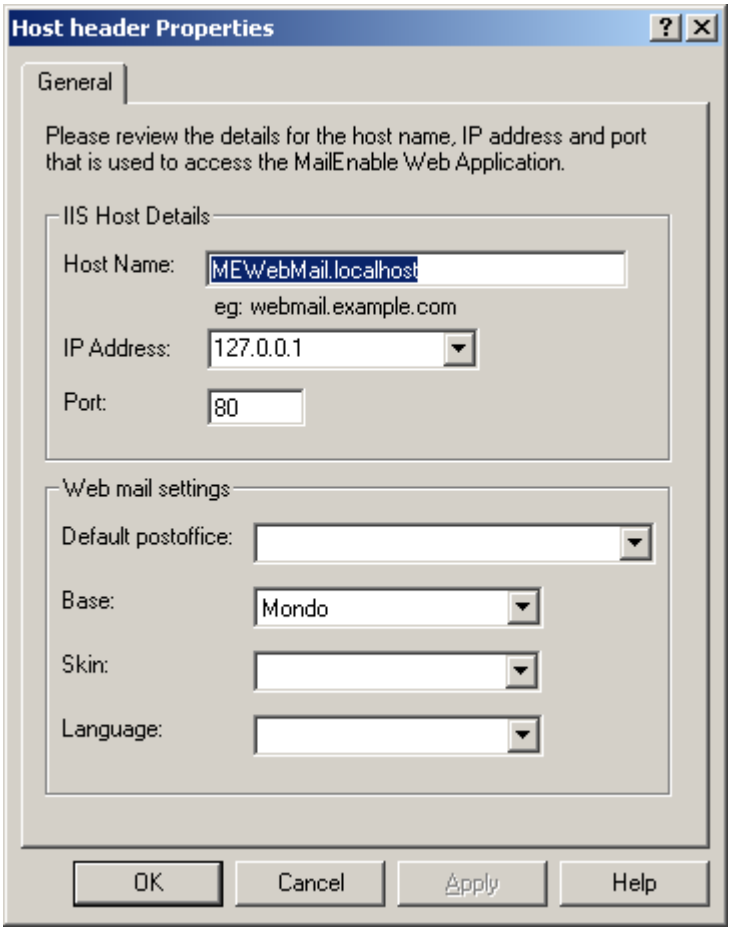
Publishing web mail through host headers

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.



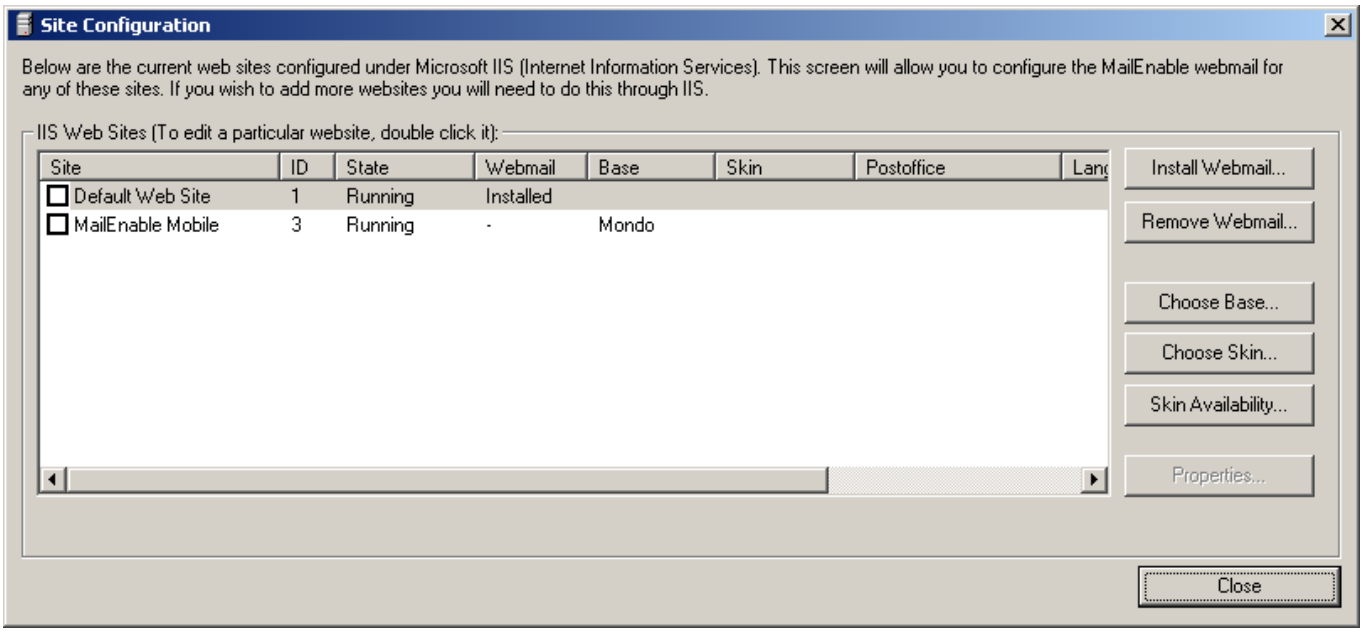
Setting	Description
Host name	The host name is the domain name users type in their web browser to access the web mail. You may wish to give the web mail a URL similar to webmail.example.com. A DNS entry has to be created in order to direct users to the IIS server.
IP Address	The address that the host 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.

Web mail skin selection

MailEnable allows for the configuration of web mail bases and skins on a per server or domain basis. A web mail base is the viewable design or style sheet that the end user of web mail can use. Usually, these will have different features.

Within the administration program there is an option to set the server level base web mail design. See the **Web Mail - Site Options (Section 6.18.2.3)** for information on setting the server level base design. This will be the default base for every domain on the server providing one has not been set for a particular domain, which would override the server setting.

To choose a base skin for a selected site or sites:

1. Select the site(s) in the top view by placing a tick in the tick box next to each domain or web site.
2. Select the button labeled Choose base for selected sites.
3. This will bring up a selection window. Using the drop down combo box, select the desired base for each of the web sites selected.

Once a base is selected per site or server, then it is possible to select a skin on a domain basis or web site basis. (also this generally occurs the same way in selecting a base).

To select a skin on a domain or website basis:

1. Place a tick in the tick box for each domain
2. Select **Choose Skin…**
3. This will bring up a selection window. Using the drop down combo box, select the desired skin

Note: When selecting a skin, you need to make sure the skin exists in the base folder selected.

Web mail skin availability

This option allows skins to be made **Private** or **Public** for a selected URL in the Site configuration screen. To do this, select the **Skin Availability** button. Highlighting the skin and double clicking will toggle availability between private and public.

- **Private** – Skin will be unavailable for selection in the skin dropdown menu of web mail's login page.

- **Public** – Skin will be available for selection in the skin dropdown menu of web mail's login page.

6.18.4 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	Supports Video Chat
Internet Explorer	10	No
Microsoft Edge	20	Yes
Firefox	40	Yes
Safari	10.10	Yes (macOS High Sierra or iOS 11)
Chrome	40	Yes
Opera	10	No

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.

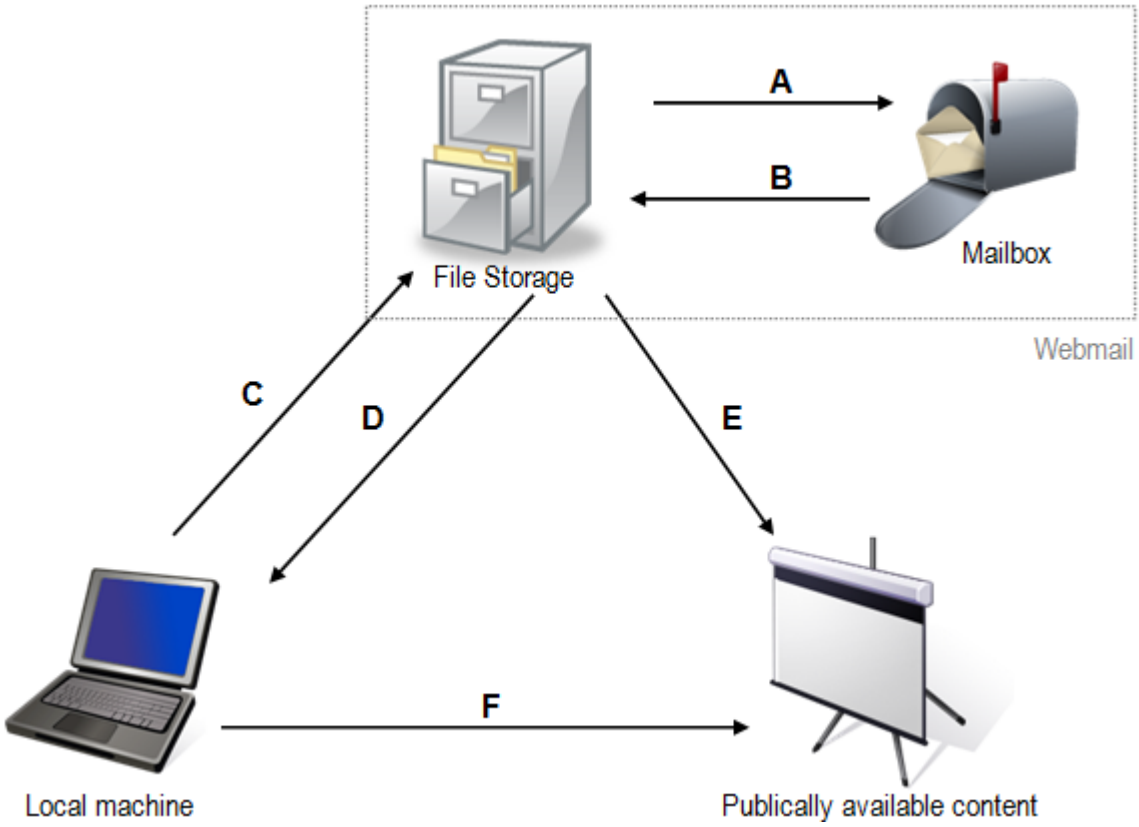
6.18.5 File Storage

Introduction

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

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

What's Possible



Action	How to perform:
A. Attach file from storage to email	Do either of the following: • From the File Storage view, select the files you wish to attach to a new email, then click the **Send Files** button. • From the Compose page, click the **Attachments** button. Then, from the Attachments page, click the **Add from Storage** button and select the file you wish to attach.
B. Save mail attachment to File Storage	From the message page, click the **Attachments** button. Now, from the Attachments page, click the **Save to Storage** button.
C. Upload file from local machine to File Storage	From the File Storage view of the target folder, click the **Upload** File button, then select the file to be uploaded.
D. Download file from File storage to local machine	From the File Storage view, select the file you with to download and click the **Download File** button. Then select the location to save to on the local machine.
E. Publish File Storage folder	From the File Storage view of the folder to be published, click the **Publish Options** button. Next click the **Publish** radio button—this will generate a URL through which the folder can be viewed. Copy the URL for future reference, then click the **Okay** button. Now anybody can browse the contents of the published folder online through the URL just generated.
F. Browse other users' published folders over	If another user publishes content, they can send you a URL to that content. Simply visit the URL in a web browser to view it.

the web

6.19 XMPP Service

6.19.1 XMPP Service

The XMPP service is responsible for the chat services on the mail server. It handles connections from the chat feature in the webmail as well as for third party applications with XMPP support. Some of the popular chat clients are:

- eM Client
- Thunderbird
- Xabber
- Jitsi Desktop
- Gajim

The XMPP service listens on all IP addresses configured on the server on port 5222 (the default for XMPP) and if TLS is enabled, will use the SSL certificate that is configured under the localhost settings.

Configuring SRV records for the XMPP service can help clients get the correct settings for a domain. The SRV record you would add for this looks like:

_xmpp-client._tcp.name TTL IN SRV priority weight 5222 target

name is the origin domain

priority is used if you have more than one server (**weight** is used if two servers have the same priority)

target is where the client needs to connect to

An example would be:

_xmpp-client._tcp.example.com TTL IN SRV 5 0 5222 mail.example.com

6.19.2 XMPP - Settings

Chat Status	**Disabled** Disables access to chat. **Enabled for Everyone** All mailboxes across the server can access chat service. **Configured per Postoffice** Mailbox access to the chat service is controlled at the postoffice level.
Enable XMPP socket connections	This allows chat clients to connect to the chat service using XMPP via port 5222.
Enable XMPP BOSH connections	This allows chat clients to use the BOSH protocol to connect to the chat service. This protocol is

	mainly used by web based chat clients or ones on mobile devices. This needs to be enabled in order for chat in webmail to function.
Enable SOCKS5 / bytestream proxy	This provides a faster and more compatible way of file transfer between chat clients. It supports file transfer using bytestreams and can also act as a intermediary between clients that do no have a common transfer method. This allows you to send files between chat clients that could otherwise not send files.
Advertise TLS Support	Enabling this indicates that users can use a secure connection to the server. This will allow you to support both secure and non-secure connections. Make sure you have an SSL certificate selected in your localhost properties before enabling this option.
Require TLS Support	Enabling this forces any chat client to use a secure connection. Non-secure connections are dropped.
Synchronize conversations at other locations (XEP-0280)	This allows conversations to appear on all clients for the account, not just one.
Allow entities to query time information (XEP-0202)	Allows entities to query time information.
Enable enhanced stream management (XEP-0198)	Enables enhanced stream management.
Allow Client State Indication (XEP-0352)	Allows clients to indicate their states (e.g. that they are active or away).
Allow clients to access chat history/archive (XEP-0313)	Allow clients to access chat history/archive.
Enable Blocking Feature (XEP-0191)	Allows JID blocking feature.
Enable PubSub Feature (XEP-0060)	Enables publish/subscribe feature.
Enable PEP (XEP-0163)	Enables personal eventing via pubsub.
PEP Notify on Presence	Does PEP notifications on presence changes.
Advertise OMEMO Support (XEP-0384)	Enables OMEMO support. OMEMO support is not available in the webmail chat client.

6.19.3 XMPP - Advanced

The webmail client allows users to send a chat request to external email addresses, to allow them to chat without having a local mail account. When a user in webmail makes this request, the server sends an invitation email to the remote address with a link to join a chat room with the mailbox. The link given has to be a URL which webmail users enter to access webmail. It is not automatically set since it is the same for all the users on the server, so you may wish to use a generic domain name.

6.19.4 XMPP - Roster

The XMPP roster is the contact list for a mailbox. These contacts are the ones shown in the XMPP client application. By default the server will populate the roster with all the other mailboxes under the post office. This can affect the performance of webmail or clients if you have a large number of mailboxes, as presence information needs to be sent and received for every mailbox shown. So the XMPP service is able to limit the number and only show those mailboxes who have been invited and added to the personal roster.

6.19.5 XMPP - Logging

Setting	Description
Logging Options	Produces a debug log for the chat service. Use this to obtain more details about the service. The XMPP service generates a large amount of data in its logs, so it is recommended not to enable this unless you have need to resolve an issue.

7 Using MySQL or Microsoft SQL Server

7.1 Installing ODBC Driver

By default, MailEnable stores its configuration information for domains and mailboxes in plain text, tab delimited files. These files are cached where needed, but if you are using over 5000 mailboxes, you can get better performance using a database. You may also want to use a database for your own reasons. MailEnable supports using Microsoft SQL Server and MySQL by accessing the configuration data via ODBC using a System DSN.

When converting from Tab Delimited files over to any SQL database, the machine must have an ODBC driver installed that corresponds to the database you are using.

To install the MySQL ODBC driver please go to the following link and select the driver available for the desired operating system:

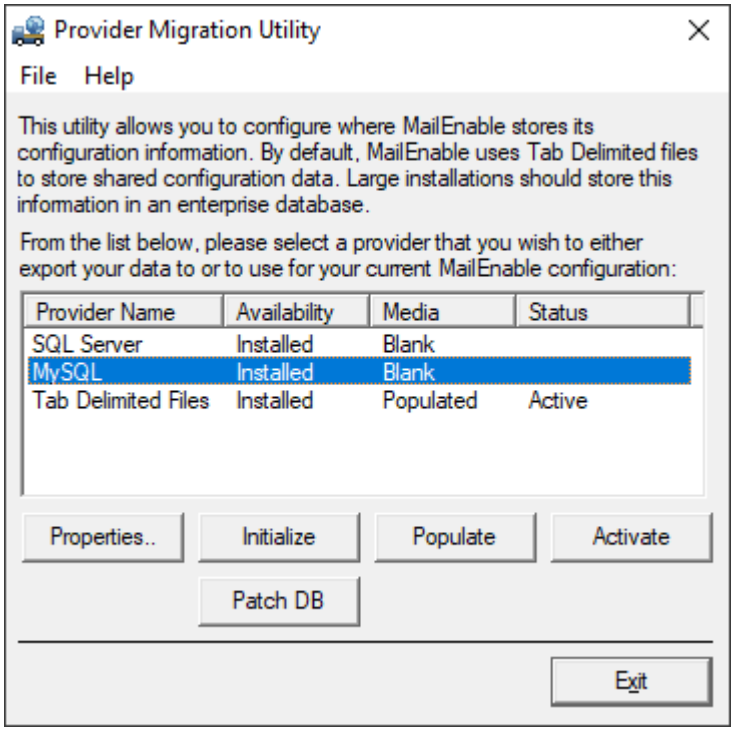
https://dev.mysql.com/downloads/connector/odbc/

For Microsoft SQL Server the ODBC driver is installed in conjunction with the SQL Server installation package.

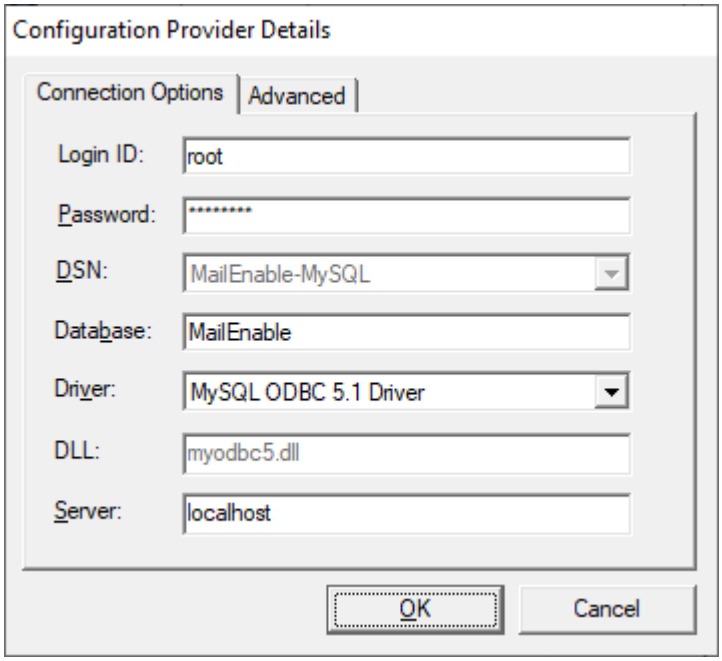
1. Navigate to Control Panel > System and Security > Administrative Tools.
2. Run the **ODBC Data Sources (64-bit)** application.
3. Navigate to the **System DSN** tab.
4. Select either a SQL Server or MySQL ODBC driver depending which database is to be used for the configuration repository and click Finish.
5. Specify the data source name as **MailEnable-SQL Server** (if using SQL Server) or **MailEnable-MySQL** (if using MySQL).
6. Enter the details that are required to connect to the database. If using SQL Server it is best to have use SQL Server authentication.

7.2 Initializing the Repository

When the Provider Migration Utility is run it will present a dialog as shown below:



From the list, select the repository to configure by selecting the corresponding Provider Name and clicking the Properties button. When clicking on the provider, the following dialog should be shown:

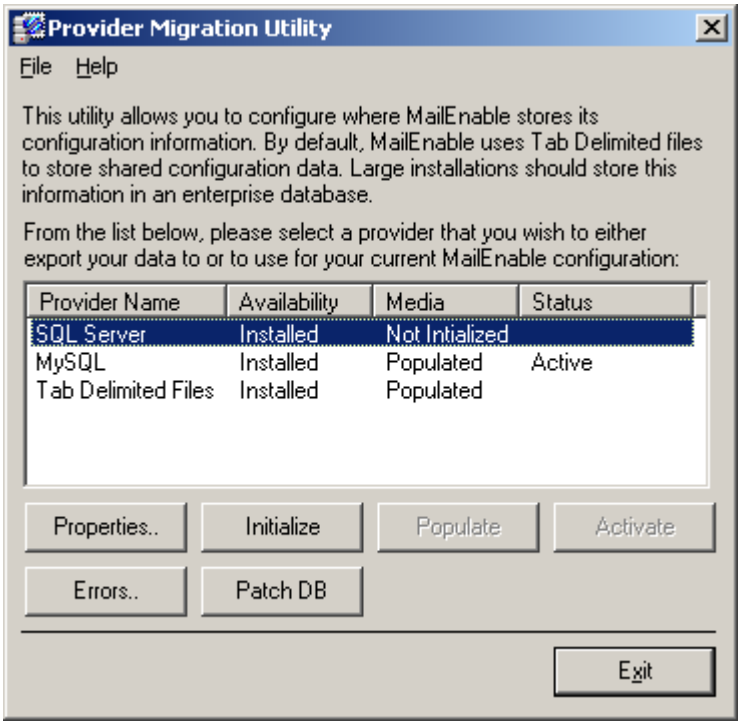


The dialog allows you to configure the System DSN for the database connection. You can enter the username and password to use and the server to connect to. Do not change the database name, as it must be called MailEnable. If you have multiple drivers available for the database type, then you can also change this. When you click the OK button the application will create the 23-bit and 64-bit System DSNs for the connection.

Once the DSN has been created, you can click the Initialize button to create the database. If it already exists you will be prompted if you wish to overwrite the existing database. This will delete all the information stored in the database.

7.3 Migrating data between providers

At this stage MailEnable is configured to use both Tab Delimited Files, as well as the ability to store its configuration in Microsoft SQL Server. The Microsoft SQL Server repository will contain no data.



This utility exports the data from Tab Delimited Files to SQL Server. To export the data, select the **Options** button and then select the fields to migrate into the database.

Unless there is a specific reason for not doing so, select all fields and click **OK.**

Initialize

Now the data is ready to be initialized. This is where the database backend is configured, where tables and data fields are created. This action is required is to activate the new provider.

Once the Apply Changes button is selected, a dialog should be displayed that shows the status of the migration.

Note: It is good practice to compare the contents of the tables in SQL Server with the contents of the respective TAB files after an export is done.

Populate

The next step is to populate the database tables/fields that were created within the initialization routine with the data that was stored within the old tab delimited files. This may take several minutes if there is a substantial amount of data to be moved.

Activate

The final step is to activate the database. This is the most intricate part of the migration, as the process informs all the relevant engines that the Microsoft SQL Server, MySQL or Tab Delimited files are to be used from this point onwards.

Once this has been completed, restart all MailEnable services including closing the administration program. It is advisable to reboot the server after this change as all registry settings are converted at this time.

Reverting to the former configuration provider

It is possible to revert back to your former configuration provider by selecting the provider in the list, and then clicking the **Populate** button followed by the **Activate** button.

Close the provider migration program and restart all MailEnable Services. It is advisable to reboot the server after this change.

Note: Most issues of database connectivity will be caused by one of the following:

- Security/Permissions – Ensure that MailEnable has permission to access the Database

- Environmental Issues (e.g.: Multilingual issues)
- Network Connectivity – Network failures can be displayed in the Windows event log viewer.

8 Remote Administration

8.1 Using Remote Administration

To connect to a remote server using MailEnable requires both the local and the remote server to be running a registered copy of MailEnable Enterprise Edition, with the Management Service running and connection to the service available through any proxies or firewalls on the designated port.

Step 1: Ensure the Management service is running and available as per the above instructions

Step 2: In the administration program, right click the MailEnable Management item in the tree view and select the 'Connect to MailEnable cluster' menu item.

Step 3: The following dialog will be presented:

Step 4: Enter the details in the username, password, server and port fields. Detailed descriptions are as follows:

Setting	Description
Username	The username on the remote server with permission to login through remote management.
Password	The password for the account username provided
Server	The IP of the remote server. That is, the IP that the management service is bound to on the remote server.
Port	The port that the remote server has the IP for remote management bound to.

Step 5: Once these details have been entered, select the Login button.

The remote server can then be managed in the same way as the local server, using the administration program.

To confirm if the remote server is connected, ensure that the admin interface server shows the IP of the remote server found in the administration program under the Servers menu icon.

If the remote server is not visible, please review the connection specifics earlier in this chapter and retry connecting to the remote MailEnable server.

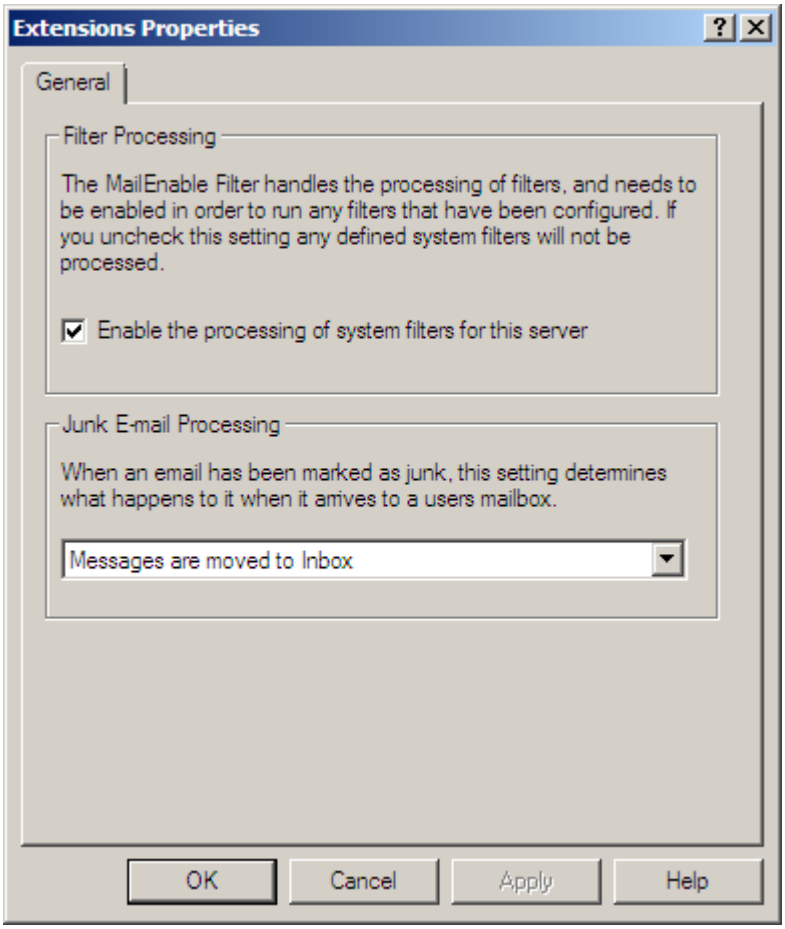
9 Message Filtering

9.1 How to enable Message Filtering

MailEnable's Message Filter processing is enabled under the **Servers > localhost > Extensions** section of the administration program.

How to enable Message content Filtering for the server

1. Navigate within the administration console to the following location: **MailEnable Management > Servers > Localhost > Extensions**
2. Right click on **Extensions** and select **properties**
3. Tick the option **Enable the processing of system filters for this server**



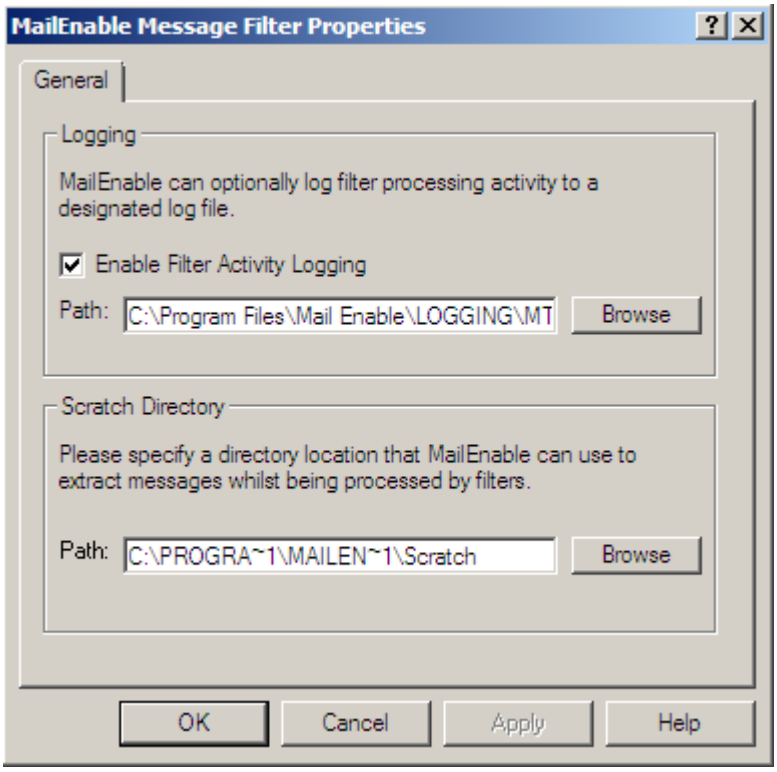
Settings	Description
Enable the processing of system filters for this server	Enables server wide level message content filtering
Junk E-mail Processing	**Messages are moved to Inbox:** Messages that have been marked as spam with the **X-ME-Content: Deliver-To=Junk** will be delivered to the mailboxes Inbox folder and not to the mailboxes Junk E-mail folder **Messages are moved to the Junk E-mail folder:** Messages that have been marked as spam with the **X-ME-Content: Deliver-To=Junk** will be delivered to the mailboxes Junk E-mail folder **Determined by postoffice settings:**

Junk E-mail processing will be determined by the Postoffice - Feature Selection options. Please see **Postoffice - Feature Selection (Section 5.3.10)** for more information.

9.2 MailEnable Message Filter Properties

Right clicking on **MailEnable Management > Servers > Localhost > Extensions > MailEnable Message Filter** and selecting properties, the general properties for the MailEnable Message Filter can be configured. These filter properties configure the infrastructure associated with content filtering.

The MailEnable Message Filter Properties window is shown below:



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

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

9.3 Spam Protection

Spam protection within is a weighted filtering system that accumulates points for each factor of a message that could be considered spam. The spam protection values can be found in the spam protection service under the Messaging Manager in your MailEnable Administration Program.

Eg: **MailEnable Managament > Messaging Manager > Spam Protection**

The goal here is to find a perfect balance of points per message for your spam. Each one of the values would not necessarily be deem a message as spam on its own but if several fail then the chance of the message being scored as spam is considerably higher.

Note: This filter by default will do nothing to the message except add a header line to the message. One of the following lines will be added to the header depending on the score of points compared to the threshold you set in the spam protection:

X-ME-Spam: Low

X-ME-Spam: Medium

X-ME-Spam: High

The actions to these header lines can be either configured in Enterprise at a post office level by searching for the above lines in the header or they can be configured by each customer in the web mail Spam Protection options of a web mail login.

Here is an article that helps with testing this service and explains a little more about its usage:

https://www.mailenable.com/kb/content/article?ID=ME020493

9.4 Global Filtering

9.4.1 How to create a Global Filter

How to add a new global filter

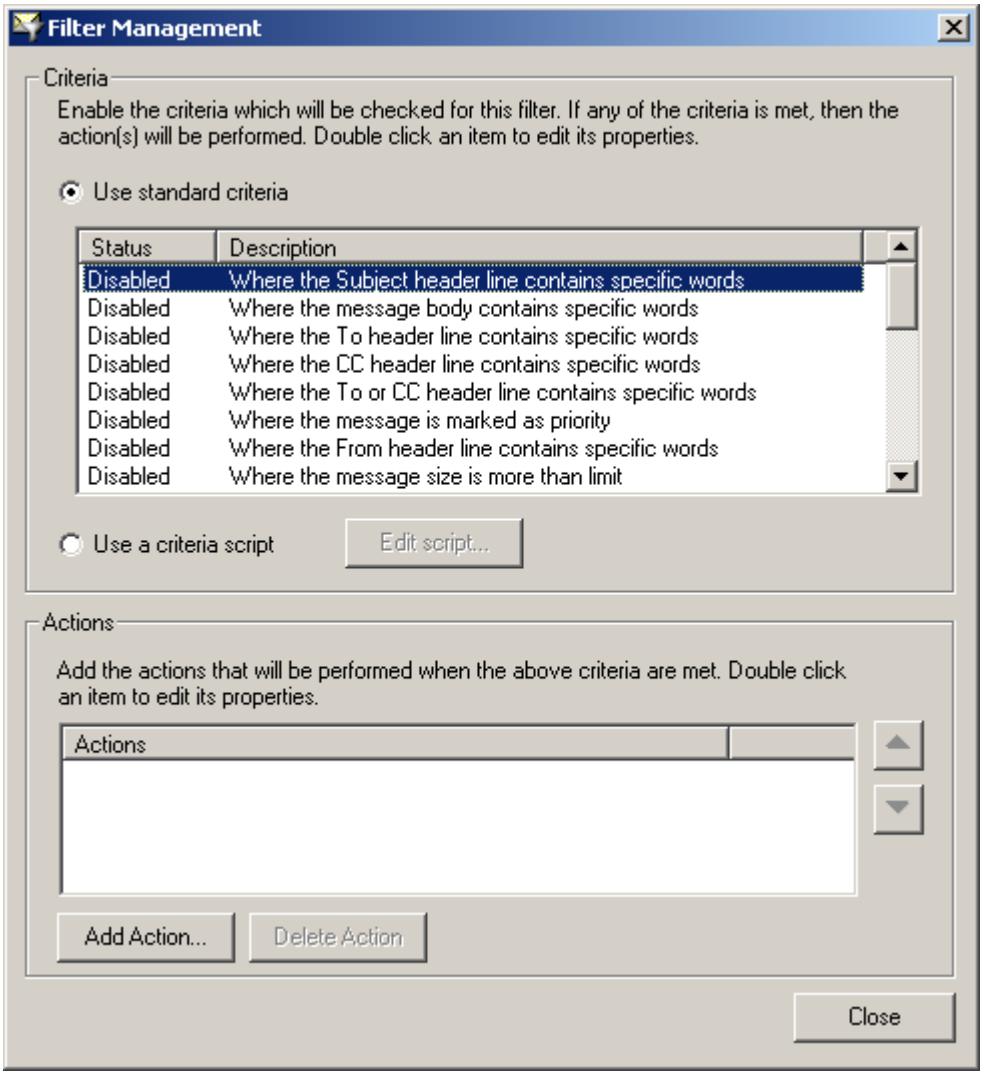
1. Navigate to the following location within the administration console: **MailEnable Management > Messaging Manager > Filters**
2. Right click on **Filters** and select **New > New Filter...**
3. Specify a name for the filter in **Add new filter item** window.
4. Click **Ok**

9.4.2 Filter Criteria

Once a filter has been added, it will appear in the list of Filters under the following location within the administration console: **MailEnable Management > Messaging Manager > Filters**.

How to add/edit Filter Criteria

1. Navigate to the following location within the administration console: **MailEnable Management > Messaging Manager > Filters**
2. Right click on a Filter within the Filters list and select **Manage...**
3. Double click on the desired criteria to open the criteria's properties window.
4. Add an action and then click **Close**



By selecting the criteria, it is possible to edit the associated attributes or conditions. As long as any of the criteria is matched, then the action(s) will be performed. Standard filtering when used in conjunction with each other will be considered with a case of OR separating the different criteria, for example;

Where the Subject header line contains specific words

OR

Where the message body contains specific words.

Note: To use criteria with AND gates or a combination or AND/OR then scripted filtering is required please visit **Scripted Filtering (Section 9.7.1.1)**

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

Following is an explanation of each of the filter criteria.

Where the Subject header line contains specific words

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

This filter is useful when incoming emails contain a re-occurring subject that needs to be filtered. Any word that is added into the filter list and is included within a subject line of a particular email going through the

MailEnable MTA will be searched. If an exact match is found then the selected action (see 8.2.2 Filter actions) is completed.

Where the message body contains specific words

Add and remove specific words to the criteria list by clicking the “Add” button. This filter is locates specific words in the body of the message. Both the plain text and the HTML of a message are checked.

Where the To header line contains specific words

This is used to specify a recipients email address. If an email address is matched, then the selected action is completed.

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

Where the CC header line contains specific words

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

Where the To or CC header line contains specific words

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

Where the From header line contains specific words

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

Where the message is marked as priority

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

Where the message size is more than limit

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

Where the message has attachments

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

Where the message has an attachment

This filter is used if you are checking for any attachment in the email.

Where a message header contains specific words

Add and remove specific words to the criteria list by clicking the “Add” button. This filter is locates specific words in the header of the message.

Where the message has over a certain spam probability

Filter to set the threshold for spam probability of Bayesian filtering e.g., define the filter to mark messages as junk if they have over 96.5% spam probability. See **Bayesian filtering section (Section 9.9.1.1)** for information on configuring the Bayesian filter.

Where the message contains a virus

Scans a message for viruses using the virus checker (s) that have been configured in the antivirus settings. See **Creating a global filter section (Section 9.4.1)** for information on configuring the antivirus plug-in.

All messages - Process this filters actions for all messages

This criteria is processed for all messages.

Where the SPF test return results matching

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

Where the sender has authenticated

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

Where the originators IP address matches

This is the IP address of the the sending client. If the message is coming from the SMTP connector, then this will be the IP address of the remote SMTP server or the email client. If it is being sent via the web mail client, it will be the IP address of the user.

Where the message is associated with this post office

Specify the associated post office for the transaction. MailEnable will attempt to allocate an associated post office for each message.

Where the message is associated with this connector

This criteria allows you to trigger on the connector that the message is coming from.

Where the message contains a URL to a blacklisted IP address

Filter will execute its actions if a URL to a blacklisted IP address has been detected within the message contents. The DNS blacklists are configured under the SMTP DNS blacklist settings.

Where the MIME boundary headers contain specific words

Filter will action on words that are found within the MIME boundary headers

Where the sender IP address is whitelisted

Filter will action if the senders IP address is found within the SMTP whitelist.

Where the message DKIM verification return results matching

Filter will execute based on the DKIM verification results. These are: Fail, Pass, Indeterminate.

Where the message fails SpamAssassin verification

Filter will execute if SpamAssassin has been configured for use and it indicates that the message has failed verification.

Where the originating country matches

Filter will execute if the originating IP address matches the selected country.

Where the originating country does not match

Filter will execute if the originating IP address does not match the selected country.

9.4.3 Filter actions

A filter action is an event that occurs when a filter criteria is met.

How to add a Filter Action

1. Navigate within the administration console to the following location: **MailEnable Management > Messaging Manager > Filters**
2. Double click on a Filter within the right hand pane filter list.
3. In the Filter management window click on the **Add Action...** button
4. Select the desired action and then click **Close**

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

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

Copy to BadMail

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

Copy to Quarantine

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

Delete Message

Deletes the message.

Notify Sender

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

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

Token Name	Description	Applicable criteria

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

Notify Recipient

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

The same notification options as outlined can be used when performing the Notify Sender action (see table above).

Notify Address

This will send a notification message to a specified email address.

Forward to Address

This filter action creates a copy of the email and forwards it to an email address. The original message will not be deleted.

Execute Application

Execute an application on the email. Since the MTA may execute this external application concurrently, make sure that the application specified can have multiple instances running. If not, a workaround would be to change the MTA service to only use one thread. Lowering the thread count will reduce the speed of message throughput.

When you specify the application to run you are able to pass parameters to it. Along with your own ones you can use the following tokens, which will be substituted with the appropriate value when the filter actions are run.

Token	Description
[ID]	Contains the message filename.
[CONNECTOR]	Contains the queue that the message is in. If you need to get access to the email contents you would use this and the [ID] value to determine the location on disk. The location on the disk is: **[Queue Path]\[CONNECTOR]\Inbound\[ID]** for the command file and **[Queue Path]\[CONNECTOR]\Inbound\Messages\[ID]** for the message file The queue path is retrieved from the Windows registry value below: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mail Enable\Mail Enable\Connectors] "Connector Root Directory"="C:\\Program Files (x86)\\Mail Enable\\QUEUES"
[TIME]	The current time in the same format as email headers include.

Add Message Header

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

Mark as spam

This will mark the message as spam, which will send the message to a users Junk E-mail folder if the post office option for this is set. See the **Feature selection section (Section 5.3.10)** for more information on this setting.

Add Subject Prefix

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

Stop processing filters

This action stops the processing of any more filter actions.

9.4.4 Token Substitutions

Some actions can benefit from having text replaced with the value.

For example, if adding a header to a message, the header value could contain the [ME_CRITERIA] enumeration value to denote the name of the rule that caused the action to fire.

It is also possible to include the word or term that caused the filter to be triggered. For example, you could include the [ME_WORDLIST] token in the text associated.

[ME_CRITERIA] The short name of the rule that caused the action to trigger. e.g. SUBJECT, TO, FROM, HASATTACHMENT

[ME_WORDLIST] The optional word list associated with the criteria causing the filter to trigger.

[ME_BFV] The Bayesian filter value associated with a parsed message

[ME_BFT] The Bayesian filter threshold associated with a parsed message

9.5 Postoffice Filtering

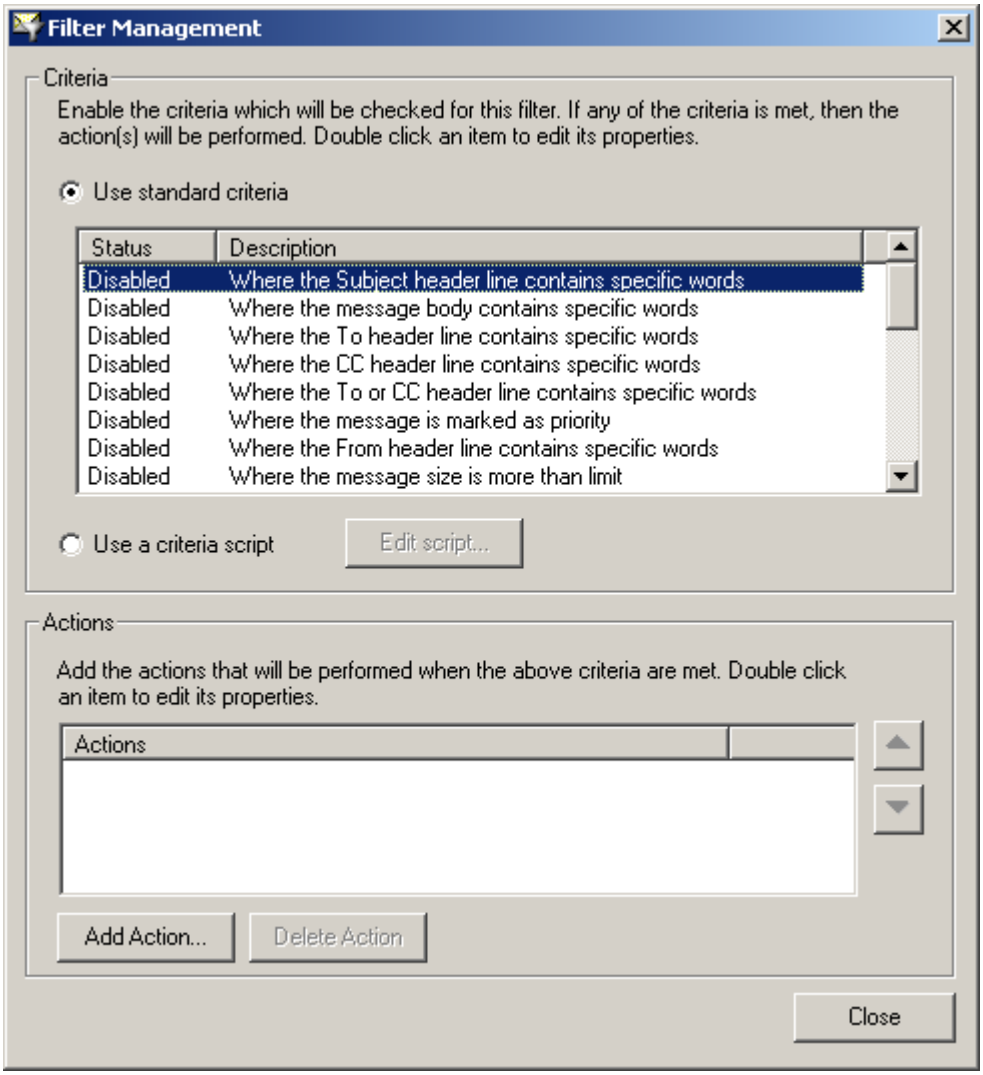
9.5.1 How to create a postoffice filter

How to create a postoffice level Filter

1. Navigate within the administration console to: **MailEnable Management > Messaging Manager > Postoffices > (postoffice name)**
2. Right click on the postoffice name and select **properties** and navigate to the **Filters** tab
3. Enable the postoffice filtering by ticking **Enable filters for this postoffice**
4. Next click the **Add...** button and specify a name for the filter and click **Ok**
5. In the filter list highlight the newly created filter and click on the **Edit...** button to open the filter criteria and actions management window
6. Add filter criteria and relevant actions to the filter and click **Close** to save.

9.5.2 Filter Criteria

Once a filter has been added, it will appear in the list of Filters where criteria and actions can be assigned to the filter. Double click on the filter to open the filters criteria and actions window.



By selecting the criteria, it is possible to edit the associated attributes or conditions. As long as any of the criteria is matched, then the action(s) will be performed. Standard filtering when used in conjunction with each other will be considered with a case of OR separating the different criteria, for example;

Where the Subject header line contains specific words

OR

Where the message body contains specific words.

Note: To use criteria with AND gates or a combination or AND/OR then scripted filtering is required please visit **Scripted Filtering (Section 9.7.1.1)**

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

Where the To line contains specific words

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

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

Where the Cc line contains specific words

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

Where the To or Cc line contains specific words

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

Where the message is from the specified account

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

Where the message is marked as priority

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

Where the message size is more than the limit

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

Where the message has attachments

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

Where the message has an attachment

Filters out emails with any type of attachment, i.e. filters emails that contain attachments of any file extension.

Where a message header contains specific words

Filters words within the message headers. Eg: any of the text before the blank gap before the message content (body).

All messages - Process this filter actions on all messages

This criteria is processed for all messages.

Where the SPF test return results matching

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

Where the sender has authenticated

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

Where the originators IP address matches

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

Where the message is associated with this post office

Specify the associated post office for the transaction. MailEnable will attempt to allocate an associated post office for each message.

Where the message came from this MailEnable connector

Enumerates the connector that the message is being delivered from.

9.5.3 Filter Actions

A filter action is an event that occurs when a filter criteria is met. Actions are performed in a prioritized list - first to last. To move a particular action in the list to a desired position, highlight the action to move and use the up and down arrows located to the right of the actions list.

Actions can be added to a postoffice filter by double clikcing on a filter within the filter list. Once in the criteria and actions window click on the Add Actions... button.

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

Copy to badmail

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

Copy to quarantine

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

Move message to public folder...

Moves a message to the public folder, or a directory under the public folder. If the directory does not exist, it will be created.

Copy message to public folder...

Makes a copy of the inbound message and sends to the public folder, or a directory under the public folder. If the directory does not exist, it will be created.

Delete message

Deletes the message.

Notify sender

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

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

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

Notify recipient

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

The same notification options as outlined can be used when performing the Notify Sender action (see table above).

Notify address

This will send a notification message to a specified address.

Forward to address

This filter action forwards the email to an email address.

Execute application

Execute an application on the email. Since this application may be executed concurrently on inbound messages, make sure that the application specified can have multiple instances running. If not, it may be required to change the postoffice connector service to only use one thread.

Add message header

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

Mark as spam

This will mark the message as spam, which will send the message to a users Junk E-mail folder if the post office option for this is set. See the **Feature selection section (Section 5.3.10)** for more information on this setting.

Add Subject Prefix

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

9.6 Mailbox Filtering

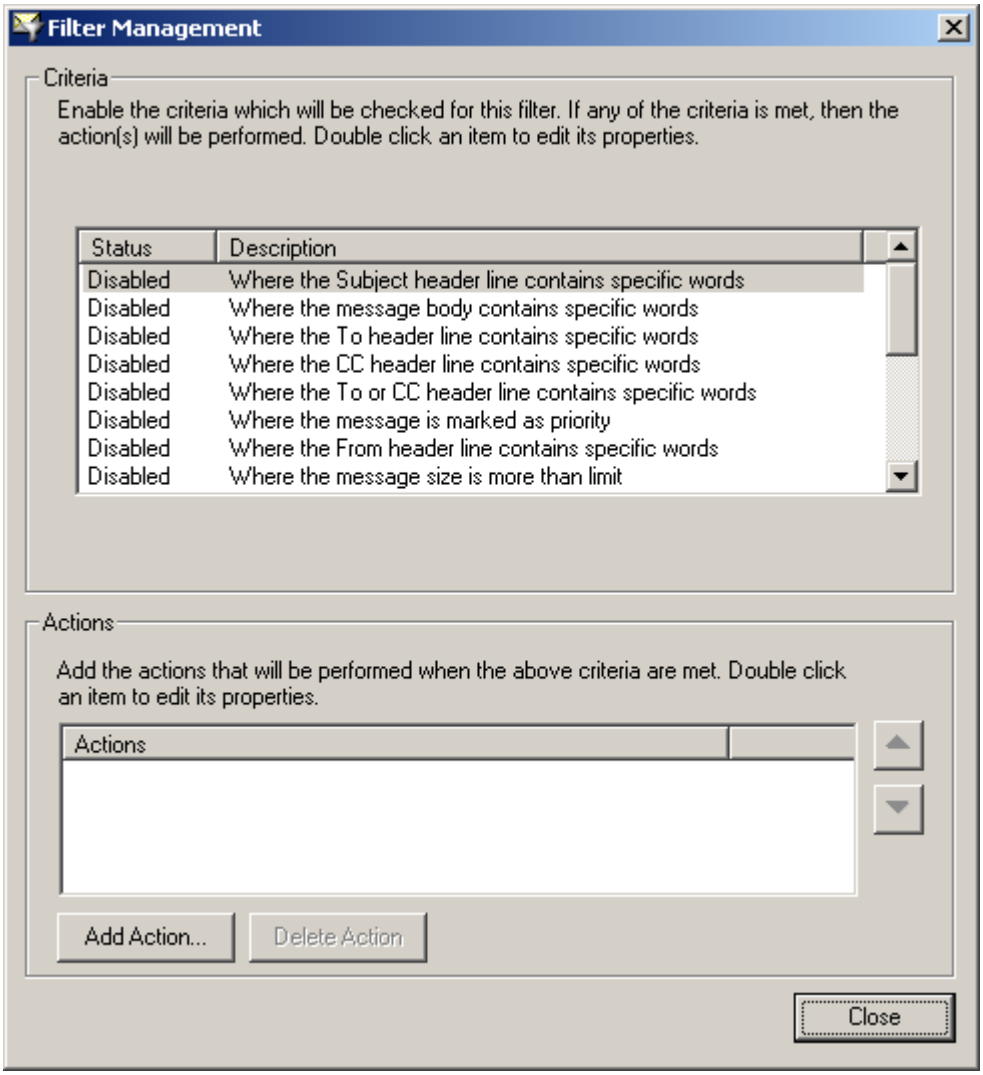
9.6.1 How to create a Mailbox Filter

How to create a Mailbox Filter

1. Navigate within the administration console to: **MailEnable Management > Messaging Manager > Postoffices > (postoffice name) > mailboxes > (mailboxname)**
2. Right click on the mailbox and select properties and navigate to the **Filters** tab
3. Enable the mailbox filters for the mailbox by ticking the option **Enable filters for this mailbox**
4. Next click the **Add...** button and specify a name for the filter and click **Ok**
5. In the filter list highlight the newly created filter and click on the **Edit...** button to open the filter criteria and actions management window
6. Add a **criteria (Section 9.6.2)** and **action (Section 9.4.3)** and then click **Close** to save.

9.6.2 Filter criteria

Once a mailbox filter has been created double click the filter in the filter list to open the criteria and actions management window.



By selecting the criteria, it is possible to edit the associated attributes or conditions. As long as any of the criteria is matched, then the action(s) will be performed. Standard filtering when used in conjunction with each other will be considered with a case of OR separating the different criteria, for example;

Where the Subject header line contains specific words

OR

Where the message body contains specific words.

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

Some of the filter criteria allow the use of an external word list. For a mailbox, you need to create this file outside of the administration program. Then it will be available to select in the administration program. The file needs to be located at:

Mail Enable\Config\Postoffices\[postoffice]\MAILBOXES\[mailbox]\RULES

The file has to be named

MEFILTER-example.txt

Where the "example" text is the

Where the Subject line contains specific words

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

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

Where Message Body line contains specific words

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

Where the To line contains specific words

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

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

Where the Cc line contains specific words

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

Where the To or Cc line contains specific words

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

Where the message is from the specified account

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

Where the message is marked as priority

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

Where the message size is more than the limit

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

Where the message has attachments

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

Where the message has an attachment

Filters out emails with any type of attachment, i.e. filters emails that contain attachments of any file extension.

Where a message header contains specific words

Filters words within the message headers. Eg: any of the text before the blank gap before the message content (body).

All messages - Process this filter actions on all messages

This criteria is processed for all messages.

Where the SPF test return results matching

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

Where the sender has authenticated

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

Where the originators IP address matches

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

Where the message is associated with this post office

Specify the associated post office for the transaction. MailEnable will attempt to allocate an associated post office for each message.

Where the message came from this MailEnable connector

Enumerates the connector that the message is being delivered from.

9.6.3 Filter actions

The following actions are available for mailbox filtering:

Delete message

Deletes the message.

Move message to folder

Moves the original message to a folder

Copy message to folder

Copies the filtered message to another folder (i.e. retains the original message and creates a copy of the message in another folder)

Move to junk email folder

Moves the filtered message to the junk email folder

Move to quarantine folder

Moves the filtered message to the quarantine folder

9.7 Scripted Filtering

9.7.1 Overview

9.7.1.1 Scripted Filtering

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

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

9.7.1.2 Literal values

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

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

Literal enumeration example

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

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

Token	Value
%IPADDRESS%	The TCP/IP address of the originating message
%POSTOFFICE%	The post office that can reasonably be assigned to the message.
%SENDER%	The sender of the message in internal format of [CONNECTOR:Address]. E.g. [SMTP:xjz@mailenable.com]
%SENDERADDRESS%	The sender email address in the format xjz@mailenable.com.

%RECIPIENTS%	The recipient(s) of the message in internal format of [CONNECTOR:Address]; [CONNECTOR:Address2]. E.g. [SMTP:xjz@mailenable.com]; [SMTP:def@mailenable.com]
%SUBJECT%	The subject of the message.

More Examples

Check whether the subject of a message contains the letters ABC

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

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

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

9.7.1.3 Enumerations requiring the CriteriaMet syntax

CriteriaMet is an inbuilt function which is used to check whether an email message matches a criteria. The criteria available match the ones that you can create in the administration program under the standard filtering options. The CriteriaMet function returns true or false and has two parameters, Token and Value. The available Tokens are described in the table below alongside their allowed values.

Token	Value	Notes
[ME_TO]	String with wildcards optional.	The message envelope recipients or the To: denoted in the message headers matches the designated criteria.
[ME_CC]	String with wildcards optional.	The Cc: denoted in the message headers matches the designated criteria.
[ME_TOorCC]	String with wildcards optional.	The message envelope recipients or the To: or Cc: denoted in the message headers matches the designated criteria.
[ME_FROM]	String with wildcards optional.	The message envelope sender or the From: denoted in the message headers matches the designated criteria.
[ME_HEADERS_CONTAIN]	String with wildcards optional.	The message headers contain data matching the designated criteria.
[ME_SUBJECT]	String with wildcards optional.	The message subject contains data matching the designated criteria.
[ME_PRIORITY]	The priority of the message. The values can	The priority of the message.

	be "Low", "Normal" or "High".	
[ME_SPF]	The SPF result, which can be "Fail", "Pass", "Soft Fail", "Error", "Neutral" or "None".	The SPF response string associated with the message is checked. This corresponds to the "Received-SPF" header item.
[ME_DKIM]	Can be 0 for a failed DKIM check, 1 for a pass or 2 for indeterminate.	Indeterminate means that either the DKIM header does not exist in the email, or that a temporary error occurred, such as DNS failure, which meant that it could not be evaluated. So if you wish to action on messages that do not have DKIM, as well as those that pass DKIM, then you should use "Not CriteriaMet([ME_DKIM],"0")" in your script, which indicates you are after those that do not have incorrect DKIM headers.
[ME_HASATTACHMENTSMATCHING]	File name pattern. This can be a filename, and wildcards can be used.	The message contains an attachment with a file name that that matches the criteria. This can be used to block file extensions, as you can format the criteria as *.extension, for example you can use *.iso.
[ME_COUNTRY_MATCH]	Two letter country code, such as "US" for United States.	The file Mail Enable\Config\GeoIPData\countries.txt contain the available country codes.
[ME_COUNTRY_NOMATCH]	Two letter country code, such as "US" for United States.	The file Mail Enable\Config\GeoIPData\countries.txt contain the available country codes.
[ME_BODY]	String with wildcards optional.	The body of the message contains text meeting the designated criteria.
[ME_SENDERAUTH]	1	For checking whether the sender authenticated in order to send the email.
[ME_BOUNDARYHEADERS_CONTAIN]	String with wildcards optional.	For checking the headers in the MIME boundaries of a message.
[ME_IPADDRESS_WHITELISTED]	1	For checking whether the originating IP address is whitelisted.
[ME_SPAM_PROBABILITY]	Number between 0 and 100.	The message is tested using the Bayesian filter and will meet the criteria if the probability is higher than the specifed amount. For example, use 95 as the value and anything over 95 (not including 95) will trigger the action.

Literal Enumeration Example

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

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

9.7.2 Basic Script Example

An example script for an advanced filter is outlined below:

Script Example

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

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

9.7.3 Advanced Script Example

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

Advanced Script Example

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

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

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

Reporting Matching Criteria

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

Setting the MEResultData variable within a scripted filter

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

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

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

An extract from an example log file is shown below. The filter column will show whether a scripted filter is being used or not.

Time	Action	Message	Connector	Filter	Result	Account	Sender	IP	Data

		ID						Address	
08/21/06 21:42:15	Start	-	-	-	-	-	-	-	-
08/21/06 21:42:31	Exec	A.MAI	SMTP	Scripted	ADD_HEADER, NOTIFY_SENDER		[SMTP:user@mailenable.com]	127.0.0.1	Subject matched ABC
08/21/06 21:43:37	Exec	B.MAI	SMTP	Basic	ADD_HEADER, NOTIFY_SENDER		[SMTP:user@mailenable.com]	127.0.0.1	CRITERIA=SUBJECT, DATA=<MF-W>AB* </MF-W>

This example shows messages A.MAI and B.MAI being processed.

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

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

9.8 Antivirus filtering

9.8.1 ClamAV Antivirus Filtering

ClamAV Antivirus Filtering

MailEnable incorporates **ClamAV Integrated Antivirus Scanning** as an out-of-box integrated Antivirus scanning solution. An added installation option has been added to the MailEnable component installation window. Enabling the ClamAV installation option will automate the installation and setup of the ClamAV Antivirus software and the MailEnable Antivirus filter by performing the following tasks:

Note: If ClamAV Antivirus filtering services are installed on the server prior to running the MailEnable ClamAV installer then the MailEnable installer will bypass the ClamAV installation step and try to use the currently installed ClamAV service.

1. Install the ClamAV Antivirus files to the following path: Mail Enable\Antivirus\ClamAV
2. Add the following registry branch for the MailEnable Antivirus plug-in window containing the ClamAV parameters: (64bit Windows)HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mail Enable\Mail Enable\Agents\MTA\Filters\MEAVCLM - (32Bit Windows) HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable\Mail Enable\Agents\MTA\Filters\MEAVCLM
3. Downloads the latest ClamAV antivirus database definitions by calling the the ClamAV **freshclam.exe** service.

After installation you will need to create a global filter to determine what to do with messages that are detected by ClamAV.

9.8.2 How to implement antivirus filtering

Configuring MailEnable to filter viruses requires both:

1. Configuration of the antivirus program to use, and also
2. Creation of an antivirus filter in MailEnable

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

Configuring the antivirus program

1. Install the selected antivirus application onto the same server that has Enterprise Edition installed
2. Ensure that any resident or real-time protector capabilities of the antivirus application have been disabled

(or all the MailEnable directories have been excluded from being protected by the software).

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

As a general rule, consider the following:

- Exclude MailEnable **Queues** and the **Config** Directories from the resident/real-time monitoring.
- Disable the resident/real-time monitor if exclusion of MailEnable directories is not possible within the antivirus application.

3. Open the MailEnable Administration program. Expand the **Servers > Local host > Extensions** branch. Click on **MailEnable Message Filter** to highlight the Message filtering extensions in the right hand side pane window. Next double click on **MailEnable Antivirus Filter.**
4. Select the appropriate item from the list of available antivirus applications.
5. Make sure that the "Enable" (or "Enable selected antivirus") is selected. It is possible to enable more than one antivirus application on the server, but this will affect the number of messages that can be scanned over a period of time.
6. Ensure that the correct program path to the command line virus scanner has been specified. Select the Options button to change this. Also ensure that the scratch directory exists. This directory is used to unpack the message as it is scanned for viruses.
7. Save changes.
8. Stop the MTA service.
9. Start the MTA service.

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

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

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

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

It is important to disable any Real Time Virus Protection software on the server (since it will interfere with the scanning process). Please see the **Real time antivirus protection section (Section 15.1.2)** for more information on this.

Creating an antivirus filter

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

To create an antivirus filter:

1. Open the MailEnable Administration Program

2. Right click on the **Messaging Manager > Filters** branch and create a new filter.
3. Specify a name for the filter. Eg: Antivirus filter
4. Having created the filter, edit the criteria for the filter as follows:
5. Check the criteria "Where the message contains a virus"
6. Create the actions that are undertaken when the virus is detected. E.g. Copy the message to the Quarantine directory or Delete Message

9.8.3 Configuring the antivirus filter

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

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

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

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

Antivirus options

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

code check	list.

It is not advisable to notify the sender that the have an infected email. When a virus is sent via email, it will usually use a different senders address that it randomly picks from the infected machine. So by sending notifications back to the sender address it is probably not being sent to someone who is infected.

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

9.8.4 Testing Antivirus Configuration

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

9.9 Bayesian filtering

9.9.1 Configuring Bayesian Filtering

9.9.1.1 Setting up auto-training Bayesian filtering

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

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

MailEnable has four options for configuring Bayesian filtering:

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

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

The option of manually training the filter is a more complex process and is described in the **Manual Training section (Section 9.9.4)**.

9.9.1.2 Step 1: Set up auto-training for the filter

The Bayesian filter can be auto-trained using 'good' emails (ham) and 'bad' emails (spam). The auto-training feature can be enabled under **Servers > Localhost > Filters > MailEnable Bayesian Filter > Properties > Auto-training** tab.

Setting	Description
Enable auto-training	Check this box to enable auto-training. While the Bayesian Filter is in auto training mode, the functions to manually update the dictionary using the "mespamcmd.exe" command utility (as mentioned in the **Spam Training Utility section (Section 9.9.5)**) do not function. This is because

	when the auto-training is running, new additions to the dictionary are stored in memory, and not written to the hard drive until the MTA service is stopped. A global filter with the 'Bayesian filter spam probability' criteria must be configured for auto-training to work. This is described in Step 4. If a filter is not configured with a Bayesian criteria, then no auto-training will occur.
Options (Process HTML content in Messages)	If this option is selected and the message contains HTML, then the HTML is parsed as well as the message plain/text boundary. Tokens will therefore also include data from the HTML messages. It makes the filter more likely to detect HTML as spam because the tokens/patterns of the HTML of bad messages can be used to calculate the probability of spam.
Spam Honeypot Email Addresses (Edit address list)	Define email addresses that do not receive valid mail for sampling. This is described in Step 2.
Ham Addresses (Edit address list)	Define "ham' or legitimate email addresses for sampling. This is described in Step 3.

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

9.9.1.3 Step 2: Collecting spam for auto-training

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

Collect spam by creating a catchall address. Set up a mailbox address (e.g. spam@example.com) as a catchall address. This address will collect all emails for a domain that do not have a mapping to a mailbox. The majority of mail in this mailbox will be spam, as spammers will often send to unknown addresses for a domain. See the **Create Domain section (Section 5.4.1)** for more information on setting up a catchall. If manual training is being used on conjunction with auto-training, the emails collected here should not be used for the manual training process. Also, since a catchall will collect a lot of email the mailbox will need to be purged often.

9.9.1.4 Step 3: Collecting ham for auto-training

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

9.9.1.5 Step 4: Create a global Bayesian filter

A global filter needs to be created in order for messages that pass through the server to be checked by the Bayesian filter and an appropriate action performed. The filter criteria can specify the level of spam probability and subsequent actions for those messages that are deemed to be spam. The following example will remove messages with over 95% spam probability.

1. Create a new filter called “Bayesian” here: **Messaging Manager > Right Click Filters > New Filter**

2. Set the criteria “Where the message has over a certain spam probability->95%”
3. Set the action to execute when a spam message is detected. This would normally be “Mark as spam”.

9.9.1.6 Step 5: Testing the Bayesian filter

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

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

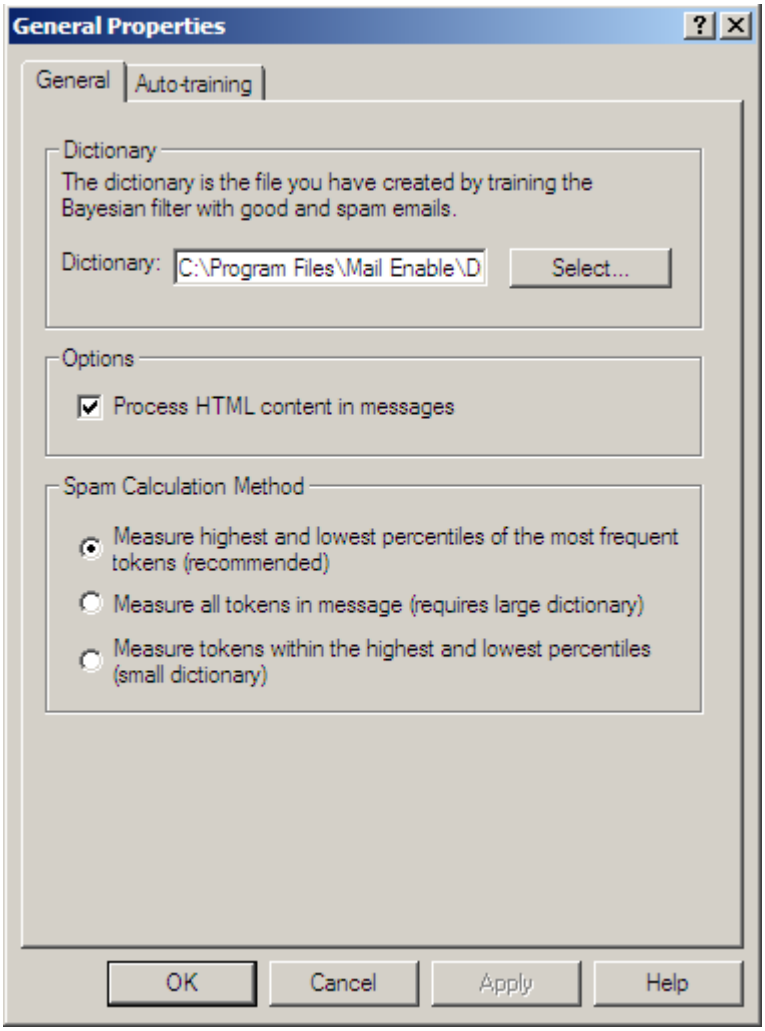
- METray (see the **System Tray Utility section (Section 13.1)**) shows instances where the Bayesian filter has scanned and detected spam. When the METray display window is open, enable the “View statistics since services were restarted”. The section that details how many “Bayesian Scans” have completed along with “Bayesian Detections” will display how many emails were checked and how many have been detected as spam since the MTA service was last started.
- Filter logs will also display any Bayesian detections. The logs are accessed via: **MailEnable Administration program > Servers > Localhost > Filters > MailEnable Message Filter > Logs > Filters**. If any messages have been detected and actioned by the Bayesian filter then a line in the logs will be displayed similar to the following:

  [Date-Time] [Message ID] SMTP Bayesian COPY_TO_QUARANTINE,DELETE [SMTP:sender@remotedomain.com] [IP_Address of sender]
- Messages passing through the Bayesian filter will have a header line added indicated the spam probability that was calculated. The header item is: **X-ME-Bayesian: 0.000000**

9.9.2 Bayesian filter general settings

How to access Bayesian Filtering properties

1. Navigate to the following location within the administration console: **MailEnable Management > Servers > Localhost > Extensions > MailEnable Message Filter**
2. Click on **MailEnable Message Filter** to highlight the available filtering extensions on the right hand pane window
3. Double click on **MailEnable Bayesian Filter**.



Setting	Description
Dictionary	MailEnable Dictionaries are located under Program Files\Mail Enable\Dictionaries. MailEnable provides a default dictionary that can be used with the filter. This dictionary is located in Program Files\Dictionary\default and is called MAILENABLE.TAB. For more details please see the **MailEnable Default Dictionary section (Section 9.9.3)**.
Options (Process HTML content in Messages)	If this option is selected and the message contains HTML, then the HTML is parsed as well as the message plain/text boundary. Tokens will therefore also include data from the HTML messages. It makes the filter more likely to detect HTML as spam because the tokens/patterns of the HTML of bad messages can be used to calculate the probability of spam.
Spam Calculation method	When a message is split into its tokens/words for analysis each token in the message is given a probability of either being spam or non-spam. As such, MailEnable can be configured to use a number of methods for calculating the final probability of a message being spam **Measure highest and lowest percentiles of the most frequent tokens** - Only those tokens most frequently occurring in the message will be used/aggregated to measure the probability of the message being spam i.e. If this option is used, then messages containing multiple instances of a spam token will most likely be diagnosed as spam. **Measure all tokens in the message** - This means that all tokens occurring in the message will be used/aggregated to calculate the probability of the message being spam. The recommended method to use is: "Measure all tokens in the message" because it provides a more balanced calculation. **Measure tokens within the highest and lowest percentiles** - This means that only those

	tokens/words in the message that are most likely to denote the message as spam or non-spam are considered i.e. If this option is used, it will mean that a legitimate message containing the word 'viagra' would be more likely to be detected as spam.

9.9.3 MailEnable Default Dictionary

MailEnable is installed with a default dictionary which is trained with some basic spam and ham emails. While it is a good starting point for auto and manual training, it is not effective in reducing spam, so auto-training and/or manual training would also need to be configured.

9.9.4 Manual training

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

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

Collecting spam for manual training

Two ways to collect spam for manual training purposes are:

1. **Creating a catchall address**. Set up a mailbox address (e.g. spam@example.com) as a catchall address. This address will collect all emails for a domain that do not have a mapping to a mailbox. The majority of mail in this mailbox will be spam, as spammers will often send to unknown addresses for a domain. Do not use the same address as one that is being used for auto-training.
2. **Using public folders**. Set up public folders for post offices for the purpose of collecting spam. IMAP users can drag and drop spam messages from their inbox into the public folder for collection. A script can then be scheduled to copy the content of these folders to a single spam repository folder for addition to the dictionary. For an example script, see the **Manual Training section**.

Collecting ham for manual training

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

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

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

Compiling the dictionary using a script

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

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

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

Example Script

```
REM Copy mail stored by either a catchall account mailbox or filter into two
```

```
folders,
REM Spam and NoSpam which will be used by the training utility to add to the
REM dictionary

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

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

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

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

REM Remove the index file and messages from the folder

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

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

net stop MEMTAS

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

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

REM Clean up the dictionary spam and ham folders

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

REM Start the MTA service

net start MEMTAS
```

9.9.5 Spam Training Utility

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

The spam training utility only works on the files stored on the hard disk. The auto-training feature should be disabled, or the MTA service stopped before any manual update of the dictionary occurs. This is because when you stop the MTA, it will write out any updated dictionary from training, overwriting the existing file.

MESPAMCMD -option [dictionary, paths]

Available options:

-c = Create dictionary

-v = Verify messages in the specified folder against the nominated dictionary

-s = Score a single message against the nominated dictionary

-m = Merge Spam and NoSpam folders into nominated dictionary

-r = Notifies the spam filter to reload the dictionary

-w = Notifies the MTA service to write out the dictionary

-p = Prunes the Dictionary to allow insertion of more words

Example:

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

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

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

Note: The Spam Training Command Line Utility must use short style file paths (i.e. the paths cannot contain spaces)

Using XML or Tab delimited files

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

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

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

Verifying a dictionary

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

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

Scoring a message

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

An example of scoring a message follows:

```
MESPAMCMD -s MailEn~1.TAB
C:\Progra~1\MailEn~1\Dictio~1\NewDic~1\Test\1A38DF23D30845E0B5FF51530A266.MAI
```

Merging a dictionary

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

dictionary to refine Spam detection.

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

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

Reload a dictionary

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

```
MESPAMCMD –r
```

Pruning a dictionary

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

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

Saving the dictionary

Dictionary updates from autotraining are saved to disk when the MTA service is stopped. You can notify the MTA service to save out the dictionary by using the -r option. This only applies if autotraining is enabled and only triggers when a message next passes through the MTA service.

```
MESPAMCMD -r
```

Checking the dictionary

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

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

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

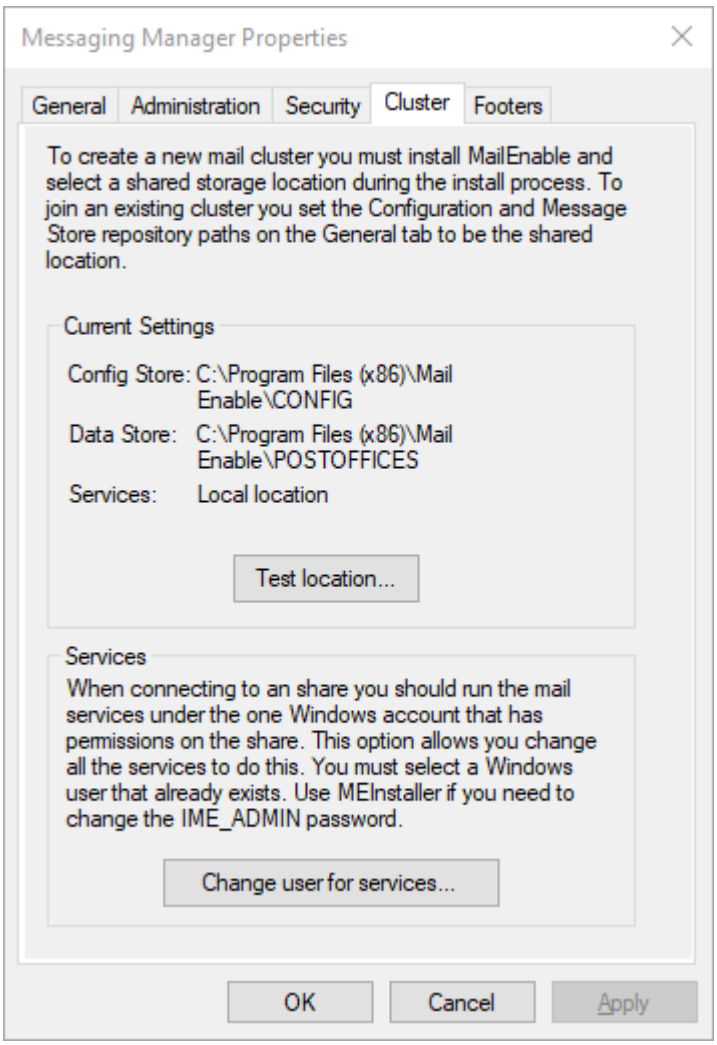
10 Cluster Management

10.1 Overview

MailEnable stores all system data in a shared storage repository. Server specific information is stored in the Windows Registry (such as details about which IP addresses a service is bound to). This means that it is possible to install multiple server nodes and point them at the same storage repository.

By load balancing and clustering front-end servers (IIS, SMTP/POP, IMAP) the system can scale out easily from the front-end perspective. Ideally, there would be a single file service (probably network attached storage or a SAN) and all the MailEnable servers are pointed to the same post office/configuration repository. This means that SMTP, IMAP, POP or MTA servers can be added as required and IP load balancing can be used to provide a clustered IP address.

The cluster management window can help configure and test the settings for a cluster.



10.2 Creating a New MailEnable Cluster

Creating a cluster is done by running the installation program after the share location has been configured. During installation you will be asked for three paths. The first path is to the MailEnable Application Directory. For

this you select a local path. This is where the program files will be installed to. The second path asked for is the Configuration Repository. For this path, select a shared storage location. The third path asked for is the Message Store Repository. You should also select the shared storage location for this. Do the same process for any other servers that you add to the cluster. If you have MailEnable already installed on the server and want to join it to a cluster, or make it use external storage, this can be done through the administration program. Run the administration program, right click the Messaging Manager icon and selecting Properties from the popup menu. The window displayed allows you to change the path to the data and configuration storage.

It is very important that when MailEnable services run that they are able to access the shared volume. As mentioned earlier, you need to consider that MailEnable services run under local Windows accounts (IME_ADMIN and IME_SYSTEM), and both these accounts will need to access the shared storage. So after installation of MailEnable you will need to change all the MailEnable Windows services to run under the one account that has permission. You can change all the MailEnable Windows services in the administration program. Right click the **Messaging Manager** icon and select Properties from the popup menu. Click the Cluster tab and there is an option to change the user for all the mail services. The web applications run under IME_ADMIN already, so you should not change the IIS configuration settings.

After installation you will need to configure all of the local options, such as IIS configuration, service options, etc. on each server.

10.3 Administering a MailEnable Cluster

You are able to log into each server in a cluster to administer it. An alternative is that the administration program can administer the majority of options of all servers in the cluster.

To connect to a MailEnable cluster, right click the MailEnable Management icon in the Administration program and select the option “Connect to a MailEnable Cluster”. This will prompt for a username and password, and the server can be selected from the drop down box. Select “Login” to connect to the server. The username and password that is used to connect to a cluster needs to be a mailbox that has SYSADMIN rights.

Once you have connected to a cluster, servers will need to be added. This only needs to be done once on the machine from where the connection is made. Right click on the Servers icon in the administration program and select the Add Server… menu item. You will be prompted to enter the name of a server you wish to add to the cluster that is being administered. While the configuration data for mailboxes, domains and other items are global to the cluster, each server has its own configuration settings for services, agents and connectors. Not all features are available from remote administration, such as viewing log files.

The administration program communicates with each server by using the Management service. This is disabled by default. To enabled, run the administration program, and expand the Servers->localhost->Services and Connectors branch, right click on the Management icon and select Properties from the popup menu. Select the Remote Administration Enabled checkbox, choose a listening port and restart the management service for the change to take effect. It is recommended to adjust your firewall to only allow connections from the IP addresses of the other servers in the cluster for this listening port.

11 Configuration of Email Clients

11.1 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 5.10)** for more information on specifying a default post office.

11.2 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

11.3 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.

11.4 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).

11.5 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)

11.6 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.

11.7 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.

11.8 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.

11.9 MAPI Configuration

Introduction

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

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

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

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

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

Configuration

Download and install the client software from the MailEnable web site. Once the client software has been installed, an Outlook profile will need to be either created or updated to allow you to access the MailEnable server.

The following instructions are available for creating a new Outlook Profile for connecting to the server.

1. Either from within Outlook or from the Windows control panel, launch the wizard for creating a new profile
2. In the **Add New E-Mail Account** window, check the box to **Manually configure server settings or additional server types** and click **Next**. A list of e-mail services should be listed containing **Internet E-mail**, **Microsoft Exchange** and **Other**. You should select the Other option, and from the list, select the **MailEnable Server** list item.
3. You can now configure the settings for connecting and accessing the MailEnable server. These follow below:
    a. In the **Server Address**, specify the host name or IP address of the mail server.
    b. For the **Account Name**, you should supply the login in the form of Mailbox@Postoffice.
    c. Enter the corresponding password for the above login
    d. Enter your friendly name - typically first name followed by surname
    e. **Email address**: Enter the primary email address for the login you have specified
    f. For the account description, you can enter a name that will allow you to identify the mailbox in Outlook - e.g.: your mailbox name
    g. An **Advanced** check box is available to allow you to configure some additional settings. In particular, the **Mailbox** field on the Mailbox tab allows you to optionally specify another users mailbox to open (so you may access the resources of their mailbox while logged in with your own credentials). Under normal configuration, you could leave this field blank or the mailbox name associated with your own login.

Having configured the above, you can click **OK** and Outlook will configure the profile for access and allow you to login.

Note:

- If you have problems logging in, you should ensure that the server/postoffice has licenses for Outlook/MAPI connectivity.
- Without additional licensing, MailEnable Enterprise will only allow you to access 20 of the mailboxes. MailEnable Enterprise Premium allows any mailbox to connect using the connector.

11.10 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\

12 Operational Procedures

12.1 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

12.2 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

12.3 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.

12.4 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.

12.5 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.

12.6 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.

12.7 Licensing

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

For computers connected to the Internet

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

MailEnable receives notification of payment mechanism, the license key will be generated and mailed to the nominated e-mail address.

For computers not connected to the Internet

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

Registration key retrieval method

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

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

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

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

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

This is to personalize the registration key code.

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

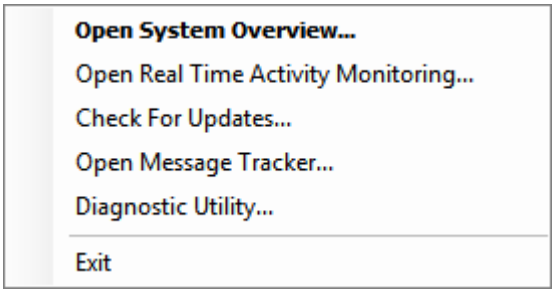
When using the Registration Wizard, follow these steps:

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

13 System Utilities

13.1 System Tray Utility (METray)

The MailEnable System Tray (METray.exe) utility provides monitoring, reporting and automatic updates for MailEnable. METray is accessible via an icon in the system tray. Right clicking the icon shows a menu with options as detailed below.



Setting	Description
Open System Overview...	Opens the METray System overview diagram window
Open Real Time Activity Monitoring...	Opens the Real time monitoring window.
Open Message Tracker...	Opens the MailEnable Message tracking utility. Please see **Message tracking (Section 13.5)**
Diagnostic Utility...	Runs the MailEnable diagnostic report. Please see **MailEnable Diagnostic Utility (Section 4.4.1)**
Exit	Closes the METray utility

System overview

The system overview screen provides a diagrammatic representation of the MailEnable system. Double clicking the METray icon will bring up the System Overview Screen as shown above. The operational status of each of the services can be seen in the diagram.

The polling intervals and length of the inbound and outbound queues of each of the connectors can also be seen in the diagram. The number of lookups and detections for antivirus scanning, Bayesian filtering, DNS blacklisting and content blacklisting are listed at the top of the System Overview window.

Setting	Description
View Statistics:	**Since services were restarted:** This option will display System Summary information since the last time the MailEnable services were restarted. **For this session:** This option will only display System Summary information from the time the METray utility has been opened.

Real Time Activity

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

diagram.

SMTP Outbound

Displays real time monitoring information for SMTP outbound connections.

Field	Description
Connection time	Indicates how long a connection has been active
Socket	Indicates the socket ID number for the active connection
ClientIP	Connecting client IP address
Domain	Domain of the recipient address
Sender	Senders email address
Last Command	Last command that was performed during the SMTP transaction
Postoffice	MailEnable Postoffice where the sender resides under
User	The senders mailbox name

SMTP Inbound

Displays real time monitoring information for SMTP inbound connections.

Field	Description
Connection time	Indicates how long a connection has been active
Socket	Indicates the socket ID number for the active connection
ClientIP	Connecting client IP address
Remote Domain	Indicates the FQDN that was specified during the SMTP EHLO command.
Sender	Senders email address
Last Command	Last command that was performed during the SMTP transaction
Postoffice	The MailEnable postoffice where the recipient resides under
User	The recipients mailbox name

IMAP

Displays real time monitoring information for IMAP connections.

Field	Description
Connection time	Indicates how long a connection has been active
Socket	Indicates the socket ID number for the active connection

ClientIP	Connecting client IP address
Last Command	Last command that was issued by the client
Postoffice	The MailEnable postoffice where the user (mailbox) resides under
User	The mailbox username
Recent transactions count	
Recent transactions elapsed time	

POP

Displays real time monitoring information for POP connections.

Field	Description
Connection time	Indicates how long a connection has been active
Socket	Indicates the socket ID number for the active connection
ClientIP	Connecting client IP address
Last Command	Last command that was issued by the client
Postoffice	The MailEnable postoffice where the user (mailbox) resides under
User	The mailbox username

Updates

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

Alerts

A monitoring agent that checks system health and can notify an email address of any problems that are detected, such as a large amount of email going through the system, or service failure.

How to setup an alert for a MailEnable service:

1. Double click on the **MeTray** icon in the windows task bar
2. Navigate to the **Alerts** tab
3. Tick the relevant service in the **Monitoring** list that will be monitored
4. Enter a valid sender email address that will be used to send the alert notification within the **Alerts** window
5. Enter the relevant recipients that will be notified of the alert
6. Enter the host name of the mail server that will be used for sending the alert notifications
7. Enter the post number for the servers SMTP service
8. Enter the authentication details that will used for relaying the notification alert for the server
9. Click test to send a test message

13.2 Activity Monitor

The MailEnable Activity Monitor (MEActivityMonitor) allows MailEnable System Activity to be watched as it occurs.

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

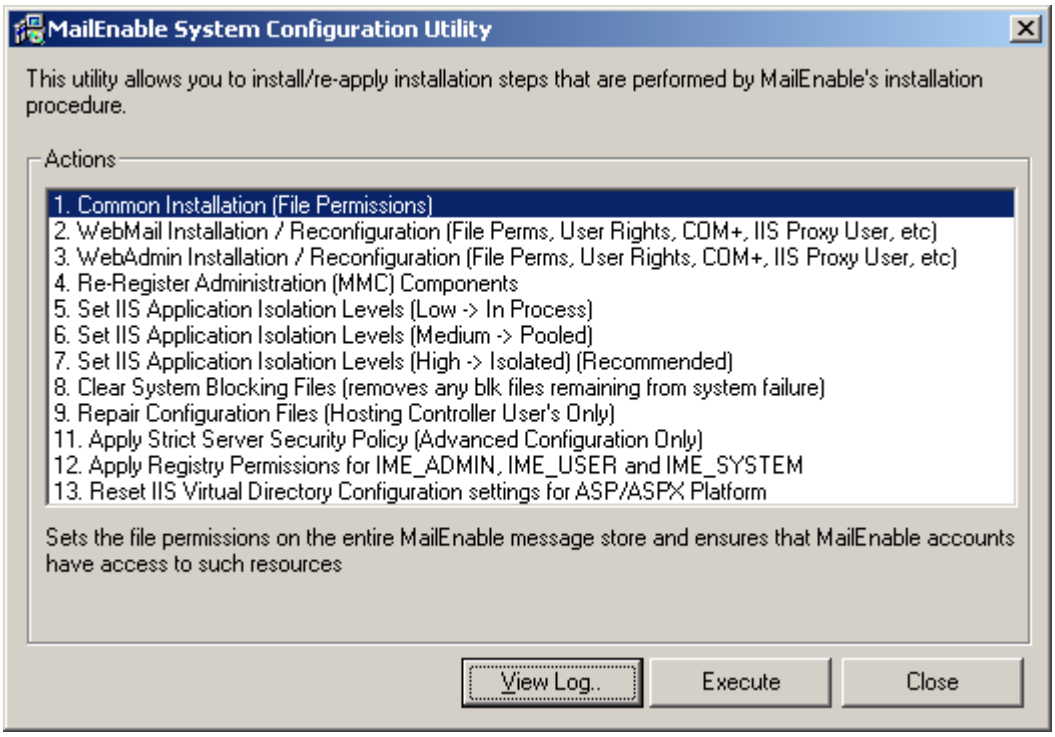
Note: To avoid unnecessary consumption of system resources, this utility should only be run whilst interactively tracking MailEnable system activity.

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

13.3 MEInstaller

The MailEnable Installer (MEInstaller) utility is an application that allows various MailEnable configuration options to be reset without requiring a reinstall of the entire product. The program is located in the 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.

13.4 Command Line Send Utility (MESend)

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

Syntax

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

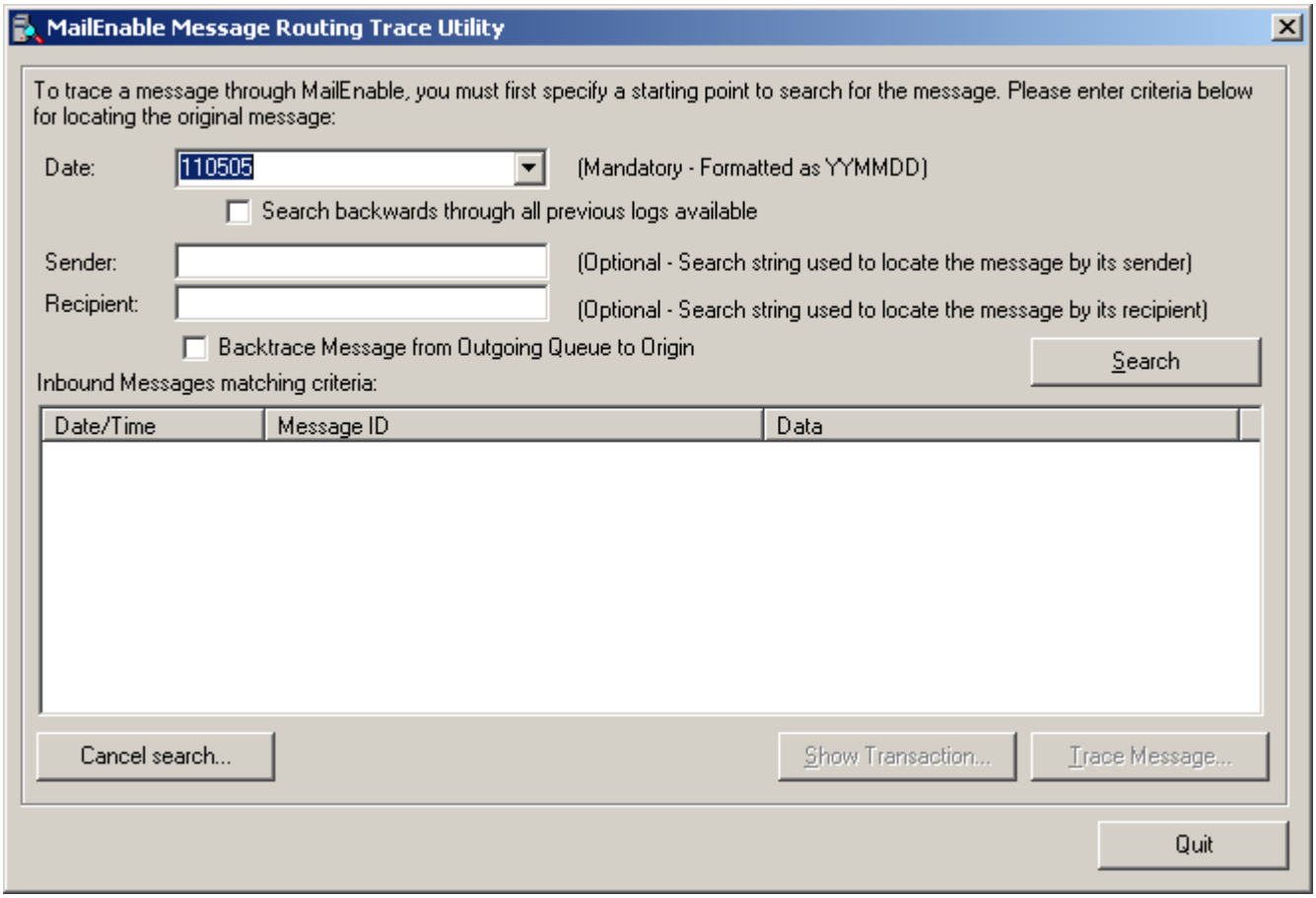
Example

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

Note: At least one recipient must be supplied.

13.5 Message Tracking

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



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

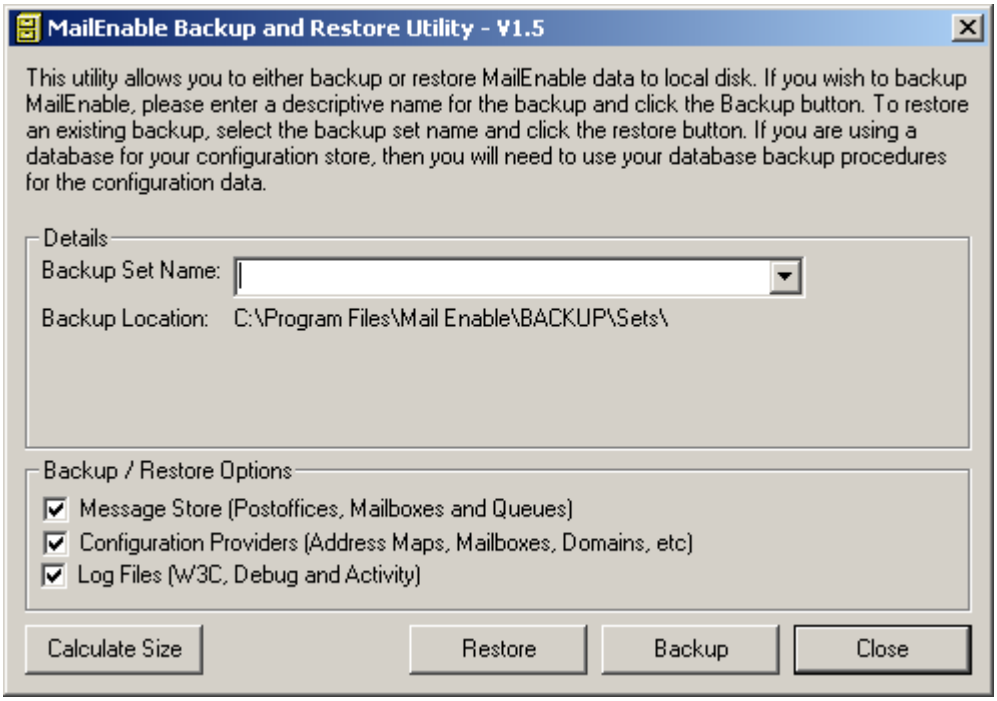
13.6 Directory Management Utility

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

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

13.7 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.

13.8 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

14 Developers

14.1 Using the COM component

This component can be used in any application that supports COM. For example, this component can be used in an ASP page to send email from a web application. This component will work against any SMTP mail server, not just MailEnable. This component is 32bit only. You will not be able to access this DLL from a 64bit application, or from a website running as 64bit. The COM component allows email to be sent to a mail server (this does not need to be a MailEnable mail server). Features include:

- Attachment support
- Easily create HTML emails
- Custom headers
- SMTP authentication

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

Properties

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

MailToDisplayName	This is the display name that will be shown as the To address. It is usually the full name of the recipient (e.g. "John Smith")
Messagebody	The message contents.
MessageBodyText	An optional property used to force the content for the textual content of the message. If the property is not set, MailEnable will generate a textual version of the message from the HTML content supplied (assuming the ContentType is set as text/html.
Password	Password to be used for SMTP authentication.
Postoffice	The post office name for the user
Server	The email server to connect to. If none is supplied, it will try to connect to the local machine.
ServerPort	The port to connect to. The default is 25.
Subject	The subject of the email message.
Username	Username to be used for SMTP authentication

Methods

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

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

Advanced settings

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

The values are located under the following registry branch:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\mail enable\mail enable\Components\MEMail

Value	Value Type	Description

Allow attachments	DWORD	1 (default) = attachments can be added to emails 0 = attachments cannot be added to emails
Attachment Path	String	The path must include this string. If the postoffice or mailbox property value has been set on the object then the following variables can be used in the path: %POSTOFFICE% %MAILBOX% If these values have been used in the path, but are not provided when someone is using the component then the path from "Default Attachment Path" will be used. The variables above cannot be used in the "Default Attachment Path" setting.
Default Attachment Path	String	This path will be used if no path has been set in the "Attachment Path" setting.

14.1.1 Configuring the server

There are no options to administer the COM component other than to control access to the DLL itself (using Windows permissions). This can be achieved by setting permissions on MEASP.DLL in MailEnable's BIN directory.

⚠ **IMPORTANT:** If using the COM component, ensure that the appropriate relay rights have been granted to the application that is intending to use the COM component.

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

14.1.2 Using the COM component

This component can be used in any application that supports COM. For example, this component can be used in an ASP page to send email from a web application. This component will work against any SMTP mail server, not just MailEnable. This component is 32bit only. You will not be able to access this DLL from a 64bit application, or from a website running as 64bit. The COM component allows email to be sent to a mail server (this does not need to be a MailEnable mail server). Features include:

- Attachment support
- Easily create HTML emails
- Custom headers
- SMTP authentication

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

Properties

Property	Explanation
AttachmentFilename	The name of the file that to add as an attachment.
AttachmentName	The name to call the attachment.
AuthenticationMode	Allows use of SMTP authentication. 0 = No SMTP authentication 1 = SMTP authentication. You must populate the Username and Password properties in order to authenticate

ContentType	The ContentType of the email you are trying to send. For instance, if you wish to send a HTML email, use this property to set the content type to “text/html”.
ErrorString	This contains the full English language description of the last error. If you encounter an error, you can check this string for a more detailed error.
MailBCC	This is list of email addresses to BCC the email to. When using multiple email addresses, separate them with a semi-colon ";".
MailCC	This is list of email addresses to CC the email to. When using multiple email addresses, separate them with a semi-colon ";".
MailCCDisplayName	This is list of email addresses that are the display name corresponding to the email address set in MailCC. This list is optional. When using multiple email addresses, separate them with a semi-colon ";".
MailFrom	This is the email address of the sender.
MailFromDisplayName	The display name of the MailFrom email address. This is the friendly name that the end user will see instead of the email address. For example, you may place the full name of the sender, or the department from which the email is coming from.
MailTo	The email address to send the email to. To send to multiple email addresses, separate the emails with a semi-colon ";".
MailToDisplayName	This is the display name that will be shown as the To address. It is usually the full name of the recipient (e.g. "John Smith")
Messagebody	The message contents.
MessageBodyText	An optional property used to force the content for the textual content of the message. If the property is not set, MailEnable will generate a textual version of the message from the HTML content supplied (assuming the ContentType is set as text/html.
Password	Password to be used for SMTP authentication.
Postoffice	The post office name for the user
Server	The email server to connect to. If none is supplied, it will try to connect to the local machine.
ServerPort	The port to connect to. The default is 25.
Subject	The subject of the email message.
Username	Username to be used for SMTP authentication

Methods

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

SetDefault	Clears all the settings back to their default.
ClearAttachments	Clears the attachments.

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

Advanced settings

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

The values are located under the following registry branch:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\mail enable\mail enable\Components\MEMail

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

14.1.3 Examples

Sending an HTML email from an ASP page

```
<%
Dim oMail
Set oMail = server.CreateObject("MEMail.Message")
oMail.MailFrom = "test@example.com"
oMail.MailFromDisplayName = "Test Account"
oMail.UserName = test@example.com
oMail.Password = "password"
oMail.ContentType = "text/html;"
oMail.MailTo = "bob@example.com"
oMail.Subject = "Welcome to our service"
oMail.MessageBody = "<html><body><h1>Hello there,<BR>Welcome to our new service.
```

```
</h1></body></html>"
oMail.SendMessage
%>
```

Sending an email with an attachment

```
<%
Dim oMail
set oMail = server.CreateObject("MEMail.Message")
oMail.MailFrom = "test@example.com"
oMail.MailFromDisplayName = "Update Account"
oMail.MailTo = "customer@example.com"
oMail.Attachmentfilename = "c:\documents\updateinfo_14_4.zip"
oMail.Attachmentname = "updateinfo.zip"
oMail.Subject = "New update information"
oMail.MessageBody="Find the new info attached."
oMail.SendMessage
%>
```

14.2 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

15 Appendix

15.1 Antivirus Configuration

15.1.1 Using your own antivirus scanner

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

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

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

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

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

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

The respective settings are:

"Exit Code Enabled": 0/1 - on/off

"Exit Codes": eg: 1 2 9: space delimited string containing application exit codes

"Exit Codes Error Inclusive": 0/1 - on/off: used to configure whether the "Exit Codes" indicate errors or successes

A sample registry import file is outlined below:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable\Mail Enable\Agents\MTA\Filters\Custom]

"Status"=dword:00000000
"Antivirus Notification Message"=">"

"Antivirus Scratch Directory"="C:\\Program Files\\Mail Enable\\Scratch"

"Antivirus Parameters"="\"[AGENT]\" \"[FILENAME]\" -s -nb -nc"

"Antivirus Agent"="C:\\Program Files\\Virus Scanner\\CUSTOM.EXE"

"Provider DLL"="MEAVGEN.DLL"

"Program Name"="Custom"

"Program Info"="This is a template for new virus scanners."

"Exit Code Enabled"=dword:00000000

"Exit Codes Error Inclusive"=dword:00000001

"Exit Codes"="1"

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

15.1.2 Real time protection

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

Vendor/Product	**Support**
Norton Antivirus Corporate Edition	Can exclude directories and file types.
McAfee Virus Scan	Can exclude directories and file types.
Panda	Can exclude specific folders.
AVG	Can exclude directories and file types.
Norman	Can exclude directories and file types.
F-Prot	Can exclude directories and file types.

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

15.2 Overview of NTLM authentication

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

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

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

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

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

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

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

Setting	Description
Enable NTLMv1	If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled use this secure authentication. E.g. in Outlook the feature is called SPA – Secure Password Authentication.

Configuring NTLM on the mail client

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

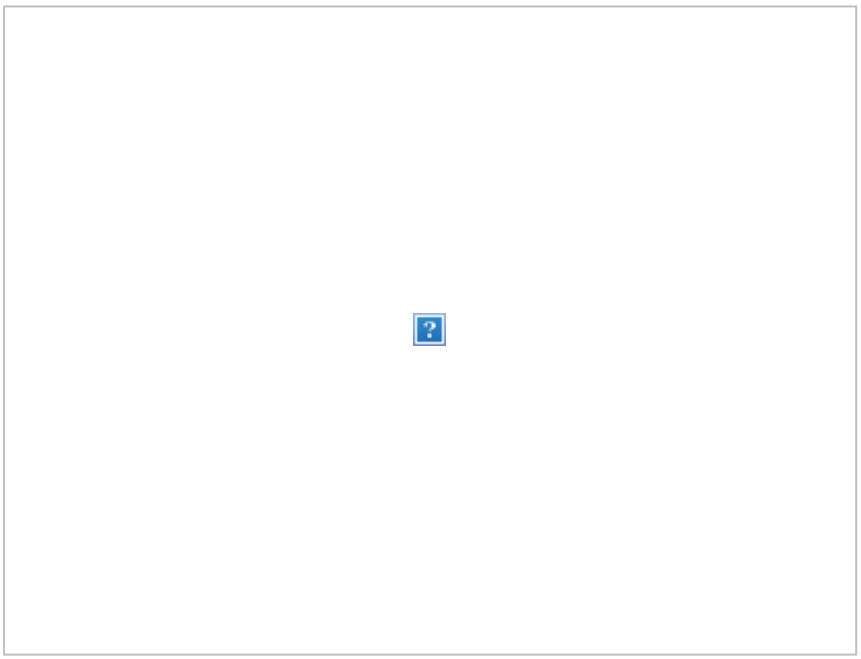


Figure 14-1 Secure Password Authentication in Outlook

15.3 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.

15.4 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

15.5 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.

15.6 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.

15.7 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.

15.8 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.

15.9 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.

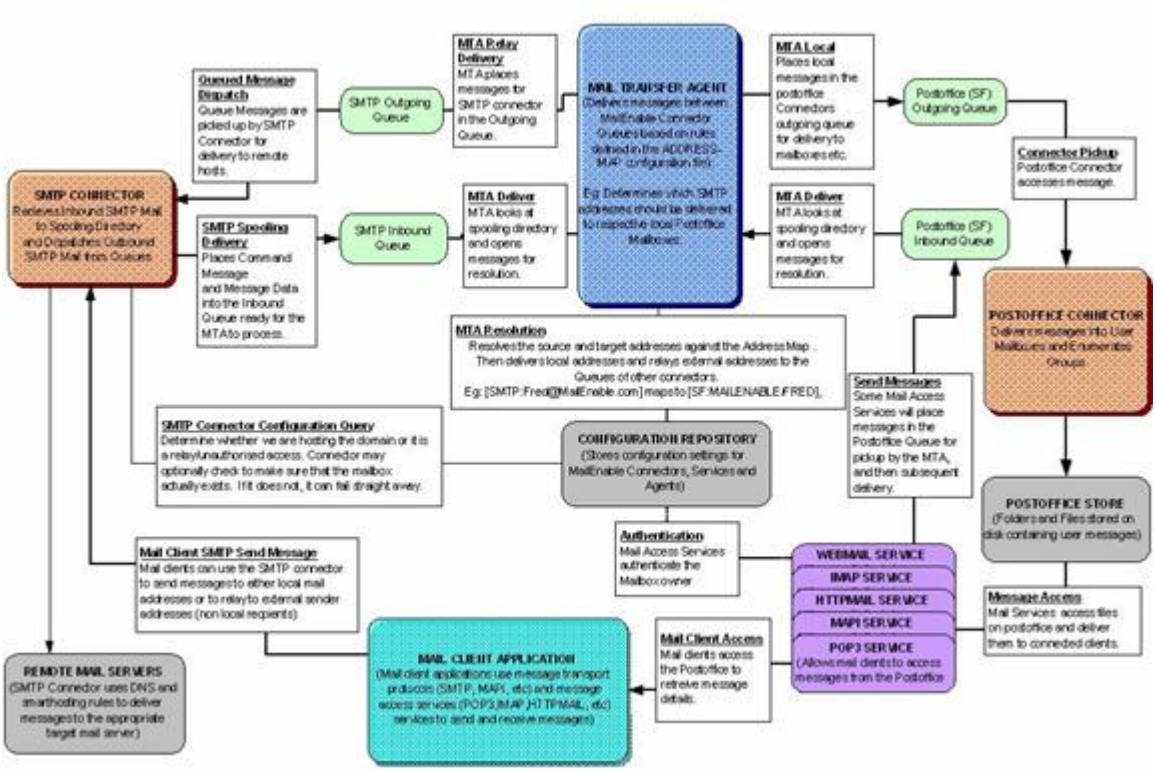
MORE INFORMATION

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.

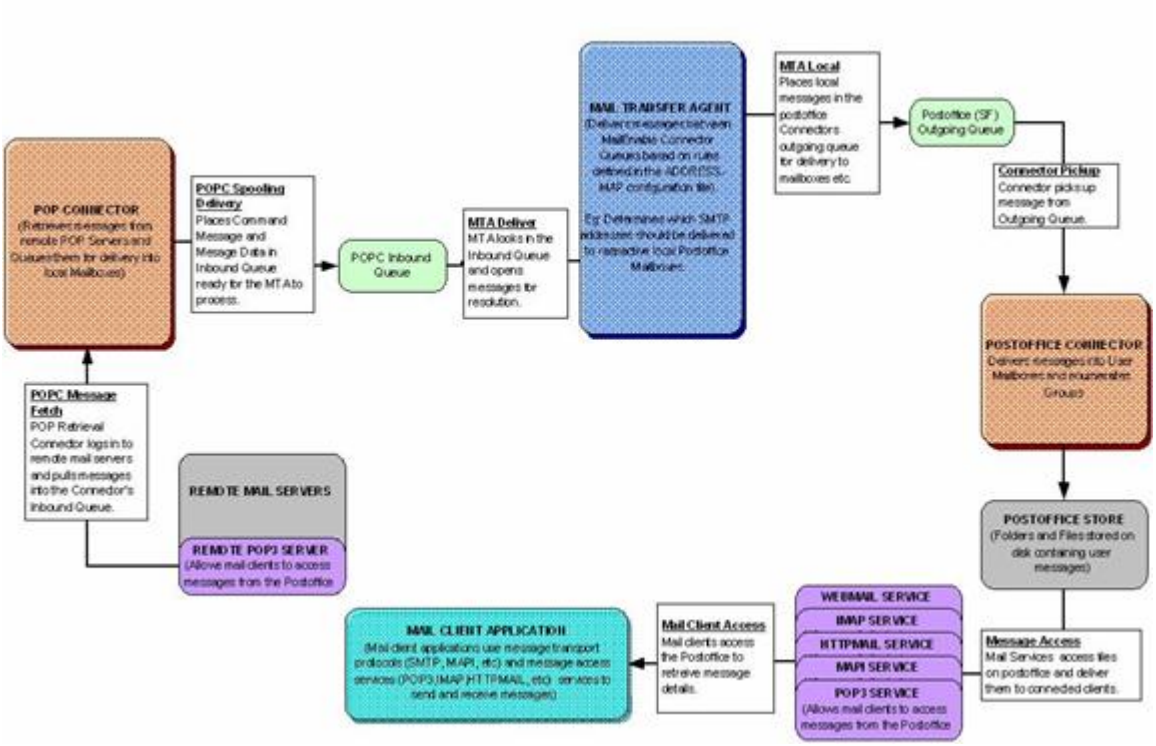
http://support.microsoft.com/default.aspx?scid=kb;en-us;323245

15.10 Logical architecture and message flow

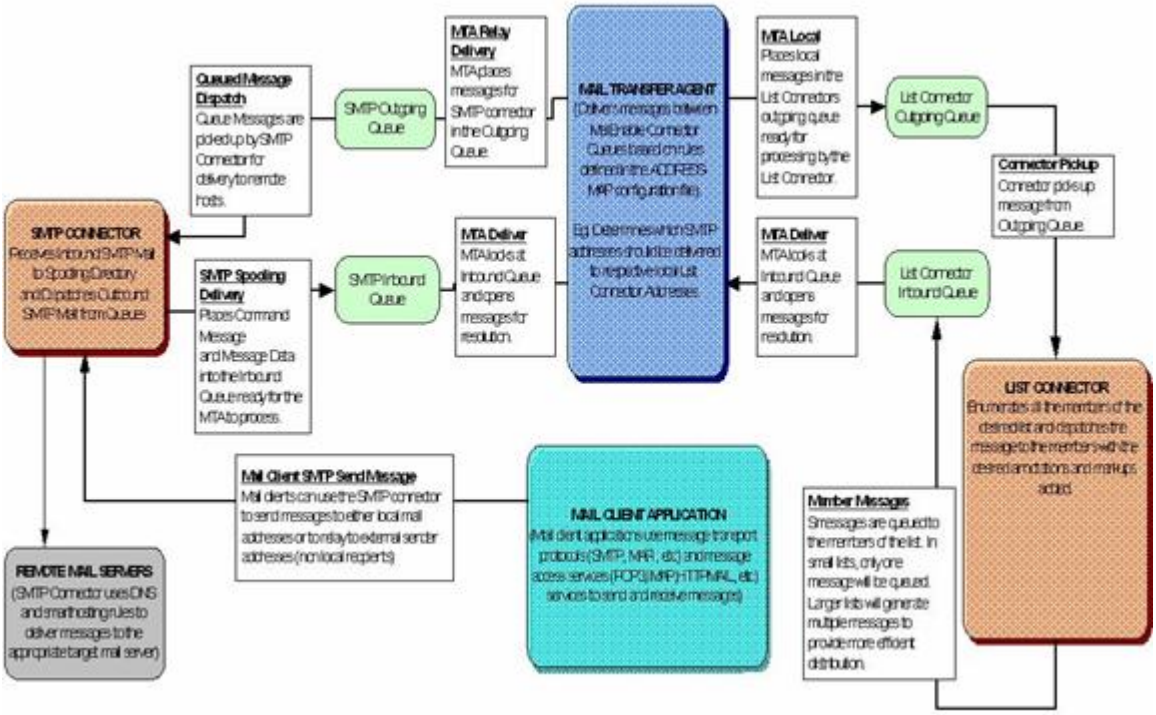
The diagram below outlines the core functionality of MailEnable and how its respective modules (Connectors, Services and Agents) interact. For simplicity, the diagram does not outline the functions of the POP retrieval Connector or List Server Connector.



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.



16 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.

17 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.

18 Index