# Table of Contents

## 1. Table of Contents

1. Table of Contents
2. Introduction
   2.1. Introduction
   2.2. Prerequisites
   2.3. How Internet Email Works
   2.4. What's New in Version 7
3. Overview
   3.1. Overview
   3.2. Structure of MailEnable
   3.3. Administration
   3.4. Email Delivery Flow
4. Installation
   4.1. Installation Overview
   4.2. Installation process
   4.3. Upgrading
      4.3.1. Upgrading Overview
      4.3.2. Upgrading an existing web mail installation
      4.3.3. Configuration repository location
      4.3.4. Replace configuration files
   4.4. Post-installation configuration
      4.4.1. MailEnable Diagnostic Utility
      4.4.2. Check and configure DNS settings
      4.4.3. To set up PTR records under Microsoft’s DNS Server
      4.4.4. Check mail services
5. Administration
   5.1. Administration Overview
   5.2. Messaging Manager
      5.2.1. Messaging Manager Overview
      5.2.2. Messaging Manager - General
      5.2.3. Messaging Manager - Administration
      5.2.4. Messaging Manager - Security

©2011 MailEnable Pty Ltd. All Rights Reserved.
5.2.5. Messaging Manager - Footers

5.3. Post office configuration
5.3.1. Post office configuration Overview
5.3.2. How to create a Post Office
5.3.3. Post office - General
5.3.4. Postoffice - Footers
5.3.5. Postoffice - Quota
5.3.6. Postoffice - Web admin
5.3.7. Post office actions
  5.3.7.1. Post office actions Overview
  5.3.7.2. Export users
  5.3.7.3. Import Windows users
  5.3.7.4. Import users
  5.3.7.5. Email users (all)
  5.3.7.6. Email users (individual)
  5.3.7.7. Delete messages
  5.3.7.8. Set quota
  5.3.7.9. Edit default message

5.4. Domain configuration
5.4.1. How to create a domain
5.4.2. Domain - General
5.4.3. Domain - Blacklists
5.4.4. Domain - DKIM (DomainKeys)

5.5. Mailbox configuration
5.5.1. Mailbox Overview
5.5.2. How to create a mailbox
5.5.3. Mailbox - General
5.5.4. Mailbox - Addresses
5.5.5. Mailbox - Redirection
5.5.6. Mailbox - Actions
5.5.7. Mailbox - Messages
5.5.8. Mailbox - POP Retrieval

5.6. Group configuration
5.6.1. How to create a group

5.6.1.1. How to add a group member

5.6.1.2. How to import group members

5.6.2. Group - General

5.7. Lists configuration

5.7.1. Lists Overview

5.7.2. How to create a list

5.7.3. Lists - General

5.7.4. Lists - Options

5.7.5. Lists - Headers and Footers

5.7.6. Importing list members

5.7.7. List commands

5.8. Server configuration

5.8.1. Localhost - General

5.8.2. Localhost - Policies

5.8.3. Localhost - Secure Sockets Layer (SSL) encryption

5.8.4. Localhost - Auditing

5.9. Advertising and Campaign Management

5.9.1. How to enable campaign management

5.9.2. How to enable Advertising banners in web mail

5.10. Option Files

6. Configuration of Connectors, Services and Agents

6.1. Mail Transfer Agent (MTA)

6.1.1. MTA Overview

6.1.2. MTA - General

6.1.3. MTA - Archiving

6.2. Connectors

6.2.1. POP Retrieval Connector

6.2.1.1. POP Retrieval Connector

6.2.2. List Server Connector

6.2.2.1. List Server Connector

6.2.3. SMTP Connector

6.2.3.1. SMTP Connector Overview
6.2.3.2. SMTP - General

6.2.3.3. SMTP - Inbound

6.2.3.4. SMTP - Outbound

6.2.3.5. SMTP - Relay

6.2.3.6. SMTP - Security

6.2.3.7. SMTP - Advanced SMTP

6.2.3.8. SMTP - Delivery

6.2.3.9. SMTP - Smart host

6.2.3.10. SMTP - Logging

6.2.3.11. SMTP - Blocked addresses

6.2.3.12. SMTP - White list

6.2.3.13. SMTP - Sender Policy Framework (SPF)

6.2.3.14. SMTP - Reverse DNS blacklisting

6.2.3.15. SMTP - Greylisting

6.2.3.16. SMTP - IP Blocking

6.2.4. Post Office Connector

6.2.4.1. Post office connector Overview

6.2.4.2. Post office connector - General

6.2.4.3. Post office connector - Logging

6.3. Services

6.3.1. Management Service

6.3.1.1. Management Service Overview

6.3.1.2. Management properties

6.3.1.2.1. Management Logging

6.3.1.3. Greylist Cleanup agent

6.3.1.4. Log Archive agent

6.3.2. Web Administration

6.3.2.1. Web administration Overview

6.3.2.2. WebAdmin - General settings

6.3.2.3. WebAdmin - Features settings

6.3.2.4. How to enable the Web Administration interface

6.3.2.5. How to add the Web Administration interface to web sites within IIS
6.3.2.6. How to access the Web Administration interface 105-106
6.3.3. IMAP Service 106
   6.3.3.1. IMAP Service Overview 106
   6.3.3.2. IMAP - General 106-108
   6.3.3.3. IMAP - Logging 108
6.3.4. POP Service 108
   6.3.4.1. POP service Overview 108-109
   6.3.4.2. POP - General 109-110
   6.3.4.3. POP - Advanced 110-111
   6.3.4.4. POP - Logging 111-112
6.3.5. Web Mail 112
   6.3.5.1. Web Mail Overview 112-113
   6.3.5.2. Web Mail - Properties 113
      6.3.5.2.1. Web Mail - General 113-115
      6.3.5.2.2. Web Mail - Spam 115-116
      6.3.5.2.3. Web Mail - Logging 116-117
   6.3.5.3. Configuring Web Mail 117
      6.3.5.3.1. Configuring web mail Overview 117
   6.3.5.4. Browser compatibility 119-120
   6.3.5.5. File Storage 120-121
6.3.6. Synchronization Service 121
   6.3.6.1. Synchronization - General 121-122
   6.3.6.2. Synchronization - CalDAV 122-123
      6.3.6.2.1. Published Calendars 123
      6.3.6.2.2. Integrated Mailbox Calendar 123-124
      6.3.6.2.3. iCal and CalDav configuration 124-125
   6.3.6.3. Synchronization - SyncML 125
      6.3.6.3.1. SyncML Protocol 125
      6.3.6.3.2. Using SyncML 125-126
      6.3.6.3.3. SyncML Synchronization Data 126-127
   6.3.6.4. Synchronization - HTTPMail 127-128
      6.3.6.4.1. Configuration 128-129
6.3.6.5. Synchronization WebDAV 129

6.4. COM component 129-131
   6.4.1. Configuring the server 131
   6.4.2. Using the COM component 131-134
   6.4.3. Examples 134

7. Message Filtering 135
   7.1. How to enable Message Filtering 135
   7.2. MailEnable Message Filter Properties 135-136
   7.3. Spam Protection 136-137
   7.4. Global Filtering 137
      7.4.1. How to create a Global Filter 137
      7.4.2. Filter Criteria 137-140
      7.4.3. Filter actions 140-142
      7.4.4. Token Substitutions 142-143
   7.5. Scripted Filtering 143
      7.5.1. Overview 143
         7.5.1.1. Scripted Filtering 143
         7.5.1.2. Literal values 143-144
         7.5.1.3. Enumerations requiring the CriteriaMet syntax 144-145
      7.5.2. Basic Script Example 145
      7.5.3. Advanced Script Example 145-146
   7.6. Antivirus filtering 146
      7.6.1. ClamAV Antivirus Filtering 146-147
      7.6.2. How to implement antivirus filtering 147-148
      7.6.3. Configuring the antivirus filter 148-149
      7.6.4. Testing Antivirus Configuration 149
   7.7. Bayesian filtering 149
      7.7.1. Configuring Bayesian Filtering 149
         7.7.1.1. Setting up auto-training Bayesian filtering Overview 149-150
         7.7.1.2. Step 1: Set up auto-training for the filter 150
         7.7.1.3. Step 2: Collecting spam for auto-training 150-151
         7.7.1.4. Step 3: Collecting ham for auto-training 151
11.1. Antivirus Configuration 174
  11.1.1. Using your own antivirus scanner 174
  11.1.2. Selecting an antivirus application 174-176
  11.1.3. Real time protection 176
11.2. Overview of NTLM authentication 176-177
11.3. Accessing web mail for automatic sign-on 177-178
11.4. DNS error codes and descriptions 178
11.5. Diagnosing Outlook/Outlook Express error codes 178-179
11.6. Manually testing if MailEnable can send mail to remote servers 179-181
11.7. Log analyzer 181
11.8. Configuring redundant or backup (MX) mail servers 181-182
11.9. Increasing 10000kb upload limit for Webmail 182
11.10. Logical architecture and message flow 182-184
12. Glossary 185-186
13. Warranty 187
14. Index 188-196
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 world’s largest Internet/Application Service Providers, Educational Institutions, Organizations, Government Agencies and Corporates.

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

Support

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

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

Web site

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

Knowledge base

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

Forums

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

How to download

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

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

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

2.2 Prerequisites

Pre-requisites

MailEnable will run on virtually any computer capable of running a Windows server environment. Web mail and web administration require .Net 2.0 to be installed.
Component | Requirement
--- | ---
Operating System | - Windows Server 2012
| - Windows Server 2008 R2
| - Windows Server 2008 (including 64 bit versions)
| - Windows Server 2003 (including 64 bit versions)
| For details on running on non-server operating systems, please see: [http://www.mailenable.com/kb/Content/Article.asp?ID=me020357](http://www.mailenable.com/kb/Content/Article.asp?ID=me020357)

Memory | 4GB RAM or higher

Hard disk | 100MB hard disk space (excluding space for email data and configuration)

Others | - Network interface card configured to use TCP/IP
| - Internet connection (with fixed IP and access for ports 25, 110, 143)
| - Microsoft IIS v5.0 or higher required for Webmail & Administration capabilities
| - Microsoft .NET Framework 2.0 or later (for .NET Webmail & Administration)

**Note:** While the MailEnable product suite can be installed and has been tested on XP and workstation environments the company does not support these platforms.

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

#### Email server

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

#### Sending and receiving mail

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

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

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

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

2.4 What's New in Version 7

The following section outlines the new functionality provided in Version 7 of MailEnable.

New Mobile Webmail

Version 7 includes a new mobile webmail client designed exclusively for smartphones and tablets. The mobile webmail client is light-weight and has support for swipe scrolling. The mobile client also allows you to automatically login, so you can access your inbox and contacts quickly. You can also tile the screens so they are readily available on your mobile device.

Webmail Enhancements - Identities, List-Unsubscribe

The updated webmail interface in Version 7 includes some new features and improvements as well as a new graphical treatment. MailEnable's webmail now allows multiple signatures, sender and reply addresses through identities. Identity support is integrated with Mailbox sharing and resources; so you can reply to e-mails using an appropriate e-mail signature. When you receive e-mails from bulk mailers, MailEnable will now utilize the List-Unsubscribe feature and allow you to unsubscribe within the Webmail interface.

Dashboard, Monitoring and Abuse Protection

When you login to the MailEnable Management Console, you will be presented with a dashboard providing a report on critical server activity and server health. This significantly reduces the need to review MailEnable's logs or the Windows Event Viewer for errors or events. It will analyze behavior and will raise events for the review of the system administrator. Version 7 also includes some significant improvements to spam filtering, providing real time statistics as well as integration with SpamAssassin.

Platform Provisioning

When new postoffices/organizations are created, MailEnable will attempt to automatically provision DNS and IIS with the appropriate configuration settings. Administrators can set up default values and customize settings when new organizations are created. These values are then applied when new postoffices and mailboxes are created (ie. you can configure templates for postoffice and mailbox creation). The provisioning function also allows you to define custom actions that can be taken when new postoffices/ organisations are created or removed from the platform.

New Management Console

MailEnable's management console has been redeveloped for MMC version 3. The new MMC is now much more responsive and intuitive. The layout is simplified and is more interactive, showing inbound and outbound connections and system usage. It also includes a Skin Catalogue Manager which provides access to a library of skins that can be chosen and installed (and uninstalled) on the platform.

Migration Centre

MailEnable's Migration Centre provides a simple solution for migrating from legacy e-mail systems. Using the migration console, it is possible to import mail for a single user, organization or entire server from a remote messaging platform.

Notes, Multiple File Download & Other Enhancements
MailEnable WebMail, ActiveSync and MAPI all now support Notes. Notes created within WebMail, MAPI or ActiveSync are now stored on the Server and are published and pushed to remote clients. The WebMail client also includes some usability extensions like multiple file download and improved screen rendering. The ability to drop RFC822 messages into a folder and have them routed to their destination. Developers can now simply drop mail messages into a system folder and MailEnable will inspect the headers and dispatch them.
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.

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

Services

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

When a user wants to read email that has been sent to their mail server for handling, there are several mail
services that can be used to retrieve the email messages so that the user can read them in their email client. These services include:

- 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.
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.

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 7.6.1) 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.

Select configuration Repository

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

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

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

Please click the Next button to continue.
Selecting message store repository

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

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

Please click the Next button to continue.

Creating an initial post office

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

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

Please click the Next button to continue.

SMTP connector configuration

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

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

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

Start installation

The installation program will prompt before it commences installing files and registering the application.
Please click the Next button to continue.
The installation will now install files and display a progress window whilst the components are installed and configured.

Select web mail site

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

Note: Do not install MailEnable web mail under the “Administration Web Site”
Please click the Next button to continue.

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

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: http://www.mailenable.com/kb/Content/Article.asp?ID=me020040

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

MailEnable needs a file storage location for its Configuration Repository.

MailEnable supports server clustering. Server clustering allows multiple MailEnable servers to access a shared configuration repository. If you intend to cluster MailEnable, you should specify a shared file service as the Configuration Repository Location.

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

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

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

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

### 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 under ‘System Tools’ 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 a few seconds to load (depending on the number of domains). A web page will be invoked and will give a test output of all services installed within the MailEnable program. In order to rerun the Diagnostic through the Administration program, right click on the Diagnose icon and select ‘Refresh’ from the popup menu. Below is an example of this test output and how it is displayed. The ‘Refresh’ option can also be used if the page does not properly load.

---

**Professional Manual**

©2011 MailEnable Pty Ltd. All Rights Reserved.

---

**Diagnostic Report**

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

**Version Information**

<table>
<thead>
<tr>
<th>Report Filename:</th>
<th>C:\Users\ADMIN\AppData\Local\Temp\MEG\DIAG.HTM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name:</td>
<td>MailEnable Pty Ltd</td>
</tr>
<tr>
<td>Contact Name:</td>
<td>MailEnable Admin</td>
</tr>
</tbody>
</table>
The classes and test configurations that are run are as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Information</td>
<td>Contains all required environment data and version information.</td>
</tr>
<tr>
<td>Configuration and Data Test</td>
<td>Verifies that all repository stores are valid and free from any corruptions or permissions errors.</td>
</tr>
<tr>
<td>Application Environment</td>
<td>Checks various system files on the server that MailEnable relies on.</td>
</tr>
<tr>
<td>System Services and Tests</td>
<td>A test on services and whether they are correctly installed and running. Note, some services are not installed in all versions of MailEnable, and so therefore may fail this test. Click the Status link for confirmation of whether this is the case.</td>
</tr>
<tr>
<td>Queue Status</td>
<td>Calculation of the quantity of all inbound and outgoing emails is displayed here.</td>
</tr>
<tr>
<td>Host TCP/IP Settings</td>
<td>Basic check on IP and DNS configurations.</td>
</tr>
<tr>
<td>Network Interface Report</td>
<td>Check of all Network Interface Cards and validation of drivers.</td>
</tr>
<tr>
<td>Mail Transfer Agent</td>
<td>Reports details of the MTA service settings that can affect delivery and Antivirus/pickup event performance.</td>
</tr>
<tr>
<td>SMTP Configuration Test</td>
<td>Settings or properties of SMTP settings are defined. Checks security settings for this service.</td>
</tr>
<tr>
<td>SMTP Relay Settings</td>
<td>Relay settings are checked here - verifies that only authorized addresses can send through the mail server. See the SMTP connector - Relay section (Section 6.2.3.5).</td>
</tr>
<tr>
<td>SMTP Inbound Bindings Test</td>
<td>Provides information on the bindings to IP addresses.</td>
</tr>
<tr>
<td>SMTP Outgoing Configuration</td>
<td>Shows outgoing SMTP configurations.</td>
</tr>
<tr>
<td>SMTP Outgoing Queue Status Test</td>
<td>Shows status of messages queued to remote hosts.</td>
</tr>
<tr>
<td>DNS Resolution Test</td>
<td>Resolves all DNS settings.</td>
</tr>
</tbody>
</table>
### 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>MailEnable>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 (i.e. the IP address changes) in order to direct emails and domains to the server, a dynamic DNS provider (e.g. no-ip.com) will be required. A dynamic DNS provider keeps track of the changing IP address and updates the DNS details accordingly. Companies that offer this service may charge a monthly fee, although there are some free services available. It is still possible to send email from MailEnable with a dynamic IP address, but unless the DNS is updated with the new IP address every time it changes, other mail servers will not be able to connect. Be aware that a number of mail servers will not accept email from the server if it does not have a static IP address, or if the server is using a cable/DSL connection.

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

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

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

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

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

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

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

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

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

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 http://www.dnsstuff.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 Professional

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

The tree view on the left navigates through the various components of MailEnable in order to configure them. The first item in the display is MailEnable Management.

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

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

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

5.2  Messaging Manager

5.2.1  Messaging Manager

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Repository</td>
<td>The configuration repository path contains the configuration information for your server. This includes the Bad Mail Quarantine and Queues directories.</td>
</tr>
<tr>
<td>Message Store Repository</td>
<td>The message store path contains all the email data for the MailEnable server.</td>
</tr>
</tbody>
</table>

5.2.3 Messaging Manager - Administration

Note: This only affects mailboxes created through the
New mailboxes have size limit
Automatically create an email address for each domain with every new mailbox created.
When displaying the mailbox list, disk usage is determined:

**Virtual list limit:**
MailEnable will try to load all the display list items 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

---

**Settings**

**Explanation**

Confirms the default quota for mailboxes, so every new mailbox created will have a quota configured.

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.

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 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

**Dont show sizes (fastest):**

This option will disable the calculation method and not display any sizes within the mailbox list.

---

**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 post office 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:
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.
### 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).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Integrated Windows Authenticator</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Use Post Office Name as Windows Domain Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Map this Post Office to the following Domain:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Domain Name:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Authenticate against Active Directory</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Automatically create mailbox if successful login and one doesn’t exist</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Users must authenticate against Windows user and not fall back to MailEnable configured password</strong></td>
<td></td>
</tr>
</tbody>
</table>

Windows authentication is currently disabled. To enable this, and allow individual postoffices to be configured, edit the Security options under the Messaging Manager properties.
<table>
<thead>
<tr>
<th>Use Integrated Windows Authentication</th>
<th>Defines whether the post office can use Windows Authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Post Office Name as Windows Domain Name</td>
<td>Select this option if the name of the post office matches the desired Windows Domain Name.</td>
</tr>
<tr>
<td>Map this Post Office to the following Domain Name</td>
<td>Defines the Windows Domain Name that 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 (.)</td>
</tr>
<tr>
<td>Authenticate against Active Directory</td>
<td>Configures MailEnable to use User Principal Name (UPN) style logins, rather than legacy Windows NT style logins. Both login mechanisms work equally as effectively, except Active Directory hosting of multiple domains in its hierarchy.</td>
</tr>
<tr>
<td>Automatically create mailbox if successful login and one doesn’t exist</td>
<td>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.</td>
</tr>
<tr>
<td>Users must authenticate against Windows user and not fall back to MailEnable configured password</td>
<td>Enforces a user to only authenticate against the Windows user database and not fall back to the MailEnable authentication database.</td>
</tr>
</tbody>
</table>

### 5.3.4 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.
5.3.5 Postoffice - Quota

The postoffice quota 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable quota notifications for post office</td>
<td>Enables the quota option for the postoffice.</td>
</tr>
<tr>
<td>Quota</td>
<td>The hard drive space allocated in megabytes</td>
</tr>
<tr>
<td>When the post office has reached</td>
<td>The percentage value that needs to be reached before a notification is sent</td>
</tr>
<tr>
<td>of its quota limit, notify this mailbox</td>
<td>to the notification mailbox</td>
</tr>
<tr>
<td>Current post office size: Not calculated</td>
<td></td>
</tr>
</tbody>
</table>

Professional Manual
### 5.3.6 Postoffice - Web admin

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

![Web Admin Configuration](image)

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

### 5.3.7 Post office actions

#### 5.3.7.1 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 and selecting All Tasks within the right click menu.*
5.3.7.2 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 All Tasks and then select Export Users.
3. From the list, select the fields to export to the file.
4. Enter the filename to save as and select Export.

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

5.3.7.4 Import users

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

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

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

5.3.7.5 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 icon to send an email to all users of a particular domain.

5.3.7.6 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.

5.3.7.7 Delete messages

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

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

5.3.7.9 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: http://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 > Postoffice > (Postofficename) > Domains
2. Right click on Domains and select properties in the right click menu
3. Enter the full domain name within the Domain name field
4. Select a postmaster address as the domains notifications address.
5. Click Apply and then OK
6. The newly created domain will be listed in the right hand pane window.

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

![MailEnable Domain Properties](image)
### Setting | Description
--- | ---
Domain is disabled | Stops email being sent to the domain.
Abuse Address | Enter the email address or select the mailbox for the abuse@domain email address.
Postmaster Address | Enter the email address or select the mailbox for the postmaster@domain email address. This is a mandatory setting.
Catchall Address | A catchall address will collect all emails for a domain that do not have a mapping to a mailbox. Either select an existing mailbox, or enter another email address to act as the catchall. Implementing a catchall will capture more spam, so make sure this mailbox is monitored.
Warning: It is advisable not to enter a remote email address or a local mailbox which is being redirected to a remote address as a catchall. Doing this will cause the server to on-send all the caught spam and is likely to result in blacklisting by the remote server and possibly putting the server on a global blacklist.
When an inbound connection via SMTP is made and there are multiple recipients to addresses that are destined for a catchall mailbox, only one message is delivered to prevent multiple copies of the same email being delivered. Messages that are delivered to a catchall will have the recipient list in the Received header, or on the alternate catchall header line, if this is enabled.
Act as Smart Host | Redirects all mail for the current domain to another mail server. This would be used if, for instance, the server was acting as a backup mail server for the domain. Specify a port number by adding a colon and port number after the IP address. e.g. 192.168.3.45:30. Do not enter the IP address of your MailEnable server, as it will create a message loop (the mail server will send to itself) and messages will finally end up in the Bad Mail directory. See the Smart host section (Section 6.2.3.9) 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

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

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

### 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 > Postoffices > (postofficename) > Domains**
2. Right-click on the domain you wish to configure **DKIM** for and select **Properties**.
3. Select the **DKIM** tab and click the **Configure** button.
1. Check the **Sign outgoing messages** box to enable message signing.

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

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

   - *Include user identity*: if checked, includes the sending user’s identity in the signature header.

3. Configure selectors. A selector represents a private/public key pairing and, from the verifier’s point of view, an entry in a DNS text record.
   a. Clicking New will bring up the **New Selector** dialog: enter a unique name for the selector and choose a key size (the larger the key, the more secure the encryption, but the longer it will take to sign and verify each message).
   b. Options for each selector can be set by selecting the selector from the Selectors list, setting the options on the right, and then clicking Update. The following options are present:
      - *Test mode*: if this is checked, it indicates to verifiers that the server is testing DKIM, and that signed messages should not be treated any differently to unsigned messages, even if their verification fails.
      - *Granularity*: tells verifiers that only messages sent by a specified user should pass verification. This works by comparing the granularity with the user identity.
      - *Notes*: notes for human perusal.
      - *Make this the active selector*: use this selector for all outgoing messages. Only one selector can be active at a time, activating one will deactivate all others (however, even deactivated selectors are available for verifying against previously sent messages, so long as their entry remains in the appropriate DNS text record).
c. It is recommended that selectors be regularly deactivated then decommissioned to prevent the key for the active (or a recently active) selector from being cracked. Selectors can be deleted with the Delete button.

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

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

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

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

To test DKIM right away, try the following configuration:

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

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

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

Click Update.

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

5.5 Mailbox configuration

5.5.1 Mailbox Overview

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

5.5.2 How to create a mailbox

When creating a mailbox, MailEnable will automatically create an email address for each domain in the post office (if the setting for automatically creating email addresses for each domain is enabled in the Messaging Manager Properties - see the General settings section (Section 5.2.2)) using the format mailboxname@domain. When a mail client application logs onto to MailEnable to retrieve email, it needs to have its username formatted as mailboxname@postofficename.

**How to create a mailbox**

1. Navigate within the administration console to: Messaging Manager > Postoffices > (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 Apply and then OK

5.5.3 Mailbox - General

The General tab of mailbox properties displays as below:

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

### 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.

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

5.5.5 Mailbox - Redirection

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

Redirect all email for the mailbox to an alternative email address or addresses. To enable redirection, select the ‘Redirect this mailbox to’ checkbox. Select the Add button to add email addresses. If more than one email address is listed, the email will be copied to all of the addresses listed. There is a limit of approximately 25 email addresses that can be redirected to (the limit depends on the length of each email address). For a large number of redirections, use a group (see the Create a group section (Section 5.6.2)) - this allows an unlimited number of addresses.

Keep a copy of the message in mailbox

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

5.5.6 Mailbox - Actions

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

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.
5.5.8 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 6.3.5.2) for more information on this setting.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current POP retrieval items</td>
<td>Displays any remote or local mailboxes that have been configured to have their mail pulled down into this local mailbox.</td>
</tr>
<tr>
<td>Add Mailbox</td>
<td>The POP Retrieval service can connect to another mailbox and pull any mail in the mailbox into this local mailbox. This is useful to centralize mail receipt over many accounts and across many domains.</td>
</tr>
<tr>
<td></td>
<td>To set up an account the following details are required;</td>
</tr>
<tr>
<td></td>
<td>Mail Server - This is the MX record or DNS name of the remote server e.g., mail.mailenable.com</td>
</tr>
<tr>
<td></td>
<td>Port - This is the port that is used to connect to the remote server. The default for this is port 110</td>
</tr>
<tr>
<td></td>
<td>Username - This is the username of the account. If it is a MailEnable mailbox this must be mailbox@postofficename</td>
</tr>
<tr>
<td></td>
<td>Password - The password for the account.</td>
</tr>
<tr>
<td></td>
<td><strong>This server requires APOP authentication</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Only download new messages</strong> (leave messages on server) - Will download messages leaving a copy on the server.</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong> - This setting allows the enabling or disabling of a POP retrieval service account. Disabling the account will retain the settings but will stop the account retrieving mail.</td>
</tr>
</tbody>
</table>

5.6 Group configuration

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

5.6.1 How to create a group

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

**How to create a group**

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

How to add a group member

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

Note: Be cautious of using the Advanced option if you have a large number of users in the post office as it may take a while to load the mailbox list.

5.6.1.2 How to import group members

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

5.6.2 Group - General

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

5.7.1 Lists

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

5.7.2 How to create a list

How to create a list

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

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

5.7.3 Lists - General

The general options associated with a list are outlined in the following table:
### 5.7.4 Lists - Options

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

---

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List name</td>
<td>The name of the list. This determines the address that people email to in order to post to the list. The full email address for the list appears at the bottom of the General property page.</td>
</tr>
<tr>
<td>Select domain for this list</td>
<td>The domain used for the list name.</td>
</tr>
<tr>
<td>List owner email (also</td>
<td>The email address of the moderator. When a list is moderated, all the emails that are posted are sent to the moderator. It is the job of the moderator to decide whether or not the email is to be posted. Only emails coming from the moderators email address will be posted to the list.</td>
</tr>
<tr>
<td>moderator)</td>
<td></td>
</tr>
<tr>
<td>List is disabled</td>
<td>Disables the list so no one can post to it.</td>
</tr>
<tr>
<td>Enable list help</td>
<td>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.</td>
</tr>
<tr>
<td>List Type</td>
<td>Determines whether the list is moderated or not. If moderated, all incoming emails will be sent to the moderator email address. 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.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the list. This is displayed in the Administration program to allow you to easily see what a list is about.</td>
</tr>
</tbody>
</table>
Subscription type
MailEnable can control how subscriptions are handled.

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone can post to this list</td>
<td>Anyone is allowed to send a message to the list.</td>
</tr>
<tr>
<td>Only subscribers can post to this list</td>
<td>The list will only accept posts from email addresses that exist in the list. This is not available when using a datasource for the list members.</td>
</tr>
<tr>
<td>Posting to this list requires a password</td>
<td>Password protects the list. To send an email to a password protected list, users need to enclose the password in square brackets and colons e.g. [: and :)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribers reply to the list</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

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

5.7.5 Lists - Headers and Footers

![List Properties](image)
### List Headers

Specify plain text or HTML headers for all list messages.

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

### List Footers

Specify plain text or HTML footers for all list messages.

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

#### 5.7.6 Importing list members

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

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

#### 5.7.7 List commands

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

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

#### 5.8 Localhost - General

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

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

Specify the default post office for your server. This means that any username that only has the mailbox name will be assumed to be from the default post office. E.g. the sales@example.com user will only need to use sales to log on with.

5.8.1 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.
### 5.8.2 Localhost - Policies

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Default Post Office</td>
<td>Specify the default post office for your server. This means that any username that only has the mailbox name will be assumed to be from the default post office. E.g. the <a href="mailto:sales@example.com">sales@example.com</a> user will only need to use sales to log on with.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock out user</td>
<td>Keeps track of mailbox authentication failures per hour; all services have the authentication</td>
</tr>
</tbody>
</table>
for one hour after logged as one. When the number of failed attempts is reached, the account will be locked out for 1 hour.

Prevent simple passwords

- When an administrator creates an account or a user changes a password, the password must meet the password complexity requirements, as outlined below, if this feature is enabled.
  - Passwords must be over 6 characters long
  - Passwords cannot match mailbox or account name, or have the mailbox or account name contained in the password string.
  - Password cannot be password or cannot have the word password contained in the password string.

Enable abuse detection and prevention

IP addresses will be blocked if they are incorrectly authenticating. Blocked IP addresses will be held in cache memory for hour. In order to release the blocked IP's from memory the respective needs to be restarted.

5.8.3 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., Outlook, Netscape Messenger, Eudora) 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, only one SSL certificate can be configured on the server. The SMTP, POP and IMAP services all use the same certificate. Because only one certificate can be used for the server, when purchasing one, try to make it generic for the server (i.e. a default domain). For example, if the server was called mail.example.com, a certificate that is valid for that host name would need to be purchased and registered (or a certificate for the entire domain could be obtained thereby allowing SSL certificates to be generated for multiple hostnames e.g. mail.example.com, www.example.com, support.example.com, etc.).

The server setting for users to configure their email application needs to match this certificate in order to avoid a security warning being displayed indicating that the server does not match the certificate.

For example, if you have a SSL certificate for a website www.example.com, this can be configured in MailEnable as the SSL certificate. If a user wishes to connect to the server via SSL, they should use the www.example.com domain as their SMTP/POP/IMAP server. They can use alternate domain or the IP address, but their email application will display a warning.

To use SSL for web mail and web administration, then these would be configured under IIS normally, 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 should be able to use any certificates that have been configured in the “Personal Certificates” store of the Computer Account.

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 used for all SSL communications.

Once certificates have been registered on the server, mail users can enable SSL from within their mail client. Please refer to the email client documentation for instructions on how to configure the client for SSL.

### 5.8.4 Localhost - Auditing

Auditing logs account activity and allows webmail users to see this recent activity within the webmail options. Account activity includes events such as folder deletion and authentication.
5.9 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:

5.9.1 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**
5.9.2 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

5.10 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  Configuration of Connectors, Services and Agents

6.1  Mail Transfer Agent (MTA)

6.1.1  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

6.1.2  MTA - General

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>If a message is let a inbound queue for too long without being marked as ready for delivery, then</td>
</tr>
<tr>
<td><strong>mail max. delivery time</strong></td>
<td>the MTA service will forcibly try to deliver the message after this time.</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Maximum threads</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **Enable pickup event**   | Executes a program or application when mail arrives. MailEnable will pass the mail message filename to the application. For example, if you write a VB script that adds some text to the end of each email that gets delivered, you would enable the pickup event. The command line used to execute the application is:  
program messagefilename connectortype  
Where program is the program filename, messagefilename is the name of the message file and connectortype is the type of messages (i.e. SMTP, LS, SF). Be aware that the directory path to the message is not passed to the program. The directory path will need to read from the registry in the program file. The pickup event is executed before any filters (antivirus for instance). |
| **Advanced Logging**      | Produces a debug and activity log for the service. Use this to obtain more details about what the service is doing. |

### 6.1.3 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.
### 6.2 Connectors

#### 6.2.1 POP Retrieval Connector

**6.2.1.1 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.

---

**Folder name within mailbox to archive to:**
- **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
### 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.

### 6.2.2 List Server Connector

#### 6.2.2.1 List Server Connector

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

6.2.3.1 SMTP Connector

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

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

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

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

### 6.2.3.2 SMTP - General
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Domain Name</td>
<td>The domain name of the server that MailEnable is installed on, or the default domain for the configuration. It is used for system messages, to announce the server when it connects to remote server, and when remote servers connect to MailEnable if the host name has not been specified.</td>
</tr>
<tr>
<td>Default mail domain name</td>
<td>The default mail domain name for the server, which usually matches the default MX record. For example, if you have configured mail.example.com in your DNS to point to your mail server, then you would enter this here. If a host name has been specified for an IP address on the server, then that value will override this host name.</td>
</tr>
<tr>
<td>DNS Address</td>
<td>The DNS that the local machine uses. If using more than one DNS, separate the addresses with a space character. If the SMTP service fails to connect to the first DNS, it will try the second or subsequent DNS. Use the DNS that is configured for the local network. Remember that this is not necessarily the DNS of where the domain name is registered.</td>
</tr>
<tr>
<td>Specify the email address when sending notifications</td>
<td>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 <a href="mailto:postmaster@example.com">postmaster@example.com</a> (substitute your domain here). Make sure this is a valid email address.</td>
</tr>
<tr>
<td>Enable NTLM Authentication</td>
<td>If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled to use this secure authentication. For example, in Outlook the feature is called SPA - Secure Password Authentication. More information on NTLM can be found in the Overview of NTLM Authentication section (Section 11.2).</td>
</tr>
<tr>
<td>Enable CRAM-MD5 Authentication</td>
<td>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 transferred.</td>
</tr>
</tbody>
</table>
sent over the network, thus precluding plaintext transmission.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port Settings | **SMTP Port:**  
SMTP service listens on port:  
Determines the port the SMTP service is to listen on. The default is 25. Inbound SMTP  
connections from remote servers expect the mail server to be listening on port 25, but some  
proxy or gateway software may require this to be changed.  
**Requires SSL:**  
Enables SSL certificate encryption for the port. Please refer to Server Configuration - Secure
Sockets Layer (SSL) encryption (Section 5.8.3) 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.

Submission Port:
Listen on alternative port:
Determines the alternative port the SMTP service is to listen on.

Requires SSL:
Enables SSL certificate encryption for the port. Please refer to Server Configuration - Secure Sockets Layer (SSL) encryption (Section 5.8.3) 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 submission port before being able to send a message to a locally hosted mailbox.

| 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 allow connections from clients using IPv6 addresses.

6.2.3.4 SMTP - Outbound
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of send threads</td>
<td>The number of threads that are used to send email.</td>
</tr>
<tr>
<td>Timeout for Remote Mail Servers</td>
<td>How long the SMTP service will wait for a response from a remote mail server before disconnecting.</td>
</tr>
<tr>
<td>Outgoing queue poll interval</td>
<td>How often the SMTP service polls the outgoing queue directory for mail messages to send. This is measured in seconds.</td>
</tr>
<tr>
<td>Limit outbound message size</td>
<td>Forces MailEnable to check the size of each message before delivering to a remote mail server. If the message cannot be delivered it will be returned to the sender (or sent to the bad mail directory if the message is system generated).</td>
</tr>
<tr>
<td>Outbound IP Binding</td>
<td>Forces the SMTP to use a specific IP address on the server when it is trying to deliver email.</td>
</tr>
<tr>
<td>Outbound TLS</td>
<td>Will try and establish a connection with the remote server using TLS if the remote server supports TLS, otherwise will fall back to Non-TLS authentication. Requires that an SSL certificate has been setup and configured for the server. Please refer to Secure Sockets Layer (SSL) encryption</td>
</tr>
</tbody>
</table>
6.2.3.5 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Mail Relay</td>
<td></td>
</tr>
<tr>
<td>Allow relay for authenticated senders</td>
<td></td>
</tr>
<tr>
<td>Allow relay for privileged IP ranges</td>
<td></td>
</tr>
<tr>
<td>Allow relay for local sender addresses</td>
<td></td>
</tr>
<tr>
<td>POP before SMTP authentication</td>
<td></td>
</tr>
</tbody>
</table>

[Image of SMTP Relay options]
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Mail Relay</td>
<td>Mail relaying needs to be enabled in order to send mail. Otherwise MailEnable will only be able to receive email. There are four options available to limit who can send mail out through the server. It is possible to select any combination of the four, however, a client only has to match one of the items in order to relay through the mail server.</td>
</tr>
<tr>
<td>Allow relay for authenticated senders</td>
<td>Requires that people sending mail through the server enter a username and password (i.e. this option enables SMTP authentication). To set this is different for various mail clients, but in Microsoft Outlook Express and Microsoft Outlook for instance, this is done in account properties via the “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.</td>
</tr>
</tbody>
</table>
| Authentication method | Select the authentication method for authenticated senders.  
MailEnable/integrated authentication – uses the MailEnable username/password  
Windows authentication – uses the Windows username/password valid for that machine  
Authenticate against the following username/password – specify your own username and password. |
| Allow relay for privileged IP ranges | Allows people with certain IP addresses to send email through the server. If the IP addresses of persons who are able to send email out through the server is known, use this option. DO NOT select this option if the list of IP addresses is unknown, as this may inadvertently allow everyone access. This option is usually required to allow sending through the server from a web server or web page. |
| Allow relay for local sender addresses | Allows people to send mail if their ‘From’ address has a domain that is hosted on MailEnable. For instance, if you host example.com, and someone sends a message from your server that has their ‘From’ address as peter@example.com, the email will be sent. Unfortunately, spammers may still abuse this by spoofing ‘from’ addresses, so most servers will not use this option. Using this option may cause some anti-spam blacklists to consider the server as “open relay” and block email from the server. |
| POP before SMTP authentication | The IP address of users who authenticate via POP is remembered and permitted to relay. The time period to remember the IP address for can be set. Some client applications will try to send email before retrieving (e.g.: Microsoft Outlook), so they will generate an error message on the first send try. Subsequent send attempts will then work if they are before the specified time.  
This is required due to some ISPs and certain routers not allowing SMTP authentication. This feature will bypass this issue by authenticating a client using POP. If this authenticates then the SMTP service will allow this IP access for a designated period of time.  
To remember the IP address, a file is written to the Mail Enable\Config\Connections directory. The file name is the IP address and the file extension is .pbs. |

## 6.2.3.6 SMTP - Security

![SMTP Properties](image)
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject mail if sender address is from an invalid domain</td>
<td>When a user is sending mail to MailEnable, this option will check the From address in order to verify the domain it is coming from. It works through a senders (FROM) address in the envelope or command message for an email having the domain stripped from an email address. This will then have a DNS resolution lookup completed on the domain name MX record to see if it is registered as a mail server. If not then the message will fail with a permanent error. This is used to stop people abusing the mail server by using incorrect information. The majority of people who use an incorrect From address are spammers. This may affect valid email from incorrectly configured clients, so monitor the logs often.</td>
</tr>
<tr>
<td>Authenticated senders must use valid sender address</td>
<td>If this is selected, users who are authenticating to send email must configure their email client with a valid email address that is assigned to the mailbox they are using to send on. This option is useful to force clients to use a legitimate email address, thereby reducing the possibility of spam.</td>
</tr>
<tr>
<td>Hide IP addresses from email headers</td>
<td>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</td>
</tr>
<tr>
<td>Require PTR DNS entry for unauthenticated connections</td>
<td>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.</td>
</tr>
<tr>
<td>Disable all catchalls</td>
<td>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.</td>
</tr>
<tr>
<td>Allow domain literals</td>
<td>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.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use alternate welcome message</td>
<td>When an email client or other mail server connects to MailEnable, a one line welcome message is displayed. By default, this indicates that the server is running MailEnable software, and shows the version of the software. If this option is enabled, it is possible to customize the welcome message. There are also two variables that can be used in the welcome text that will be replaced. These are: %LOCALDOMAIN% - this will be replaced with the SMTP domain from the SMTP options %TIME% - this will be replaced with the current time on the server</td>
</tr>
<tr>
<td>Restrict the number of recipients per email</td>
<td>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.</td>
</tr>
<tr>
<td>Limit number of recipients per hour to</td>
<td>This setting sets how many messages can be sent on a hourly basis.</td>
</tr>
<tr>
<td>Address Spoofing:</td>
<td><strong>Authenticated senders can impersonate:</strong> If this is selected, users who are authenticating to send email do need to use a valid email address when sending via an email client. <strong>Authenticated senders cannot impersonate:</strong> If this is selected, users who are authenticating to send email must configure their email client with a valid email address that is assigned to the mailbox they are using to send on. This option is useful to force clients to use a legitimate email address, thereby reducing the possibility of spam. <strong>Privileged IP addresses can impersonate:</strong> If this option is selected it will allow any privileged IP address within the SMTP privileged IP’s list to impersonate when using an invalid email address. This option is useful for web pages that send via the MailEnable SMTP service using an email address that does not reside within MailEnable.</td>
</tr>
<tr>
<td>Drop a connection when the failed number of commands or recipients reaches</td>
<td>Most email clients will recognize error codes returned by the mail server for an invalid recipient or similar. But some spammers and bulk email utilities may not recognize these errors and keep trying to send. By enabling this option, MailEnable will drop the client connection. It is recommended not to use a low value (5 for example), as some valid web scripts will not check the return codes either - but these will only produce a small number of failed commands.</td>
</tr>
<tr>
<td>Add to denied IP addresses if this number is reached</td>
<td>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.</td>
</tr>
</tbody>
</table>

**6.2.3.7 SMTP - Advanced SMTP**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable alternate catch-all header</td>
<td>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.</td>
</tr>
<tr>
<td>Add required headers for authenticated senders if needed</td>
<td>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.</td>
</tr>
<tr>
<td>Inbound Authentication:</td>
<td><strong>Do not require authentication:</strong>  &lt;br&gt;This setting will enforce that no inbound authentication is required for remote senders that send to locally hosted MailEnable addresses.</td>
</tr>
<tr>
<td></td>
<td><strong>Require authentication for all connections:</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td></td>
<td><strong>Authentication determined by postoffice:</strong>  &lt;br&gt;This setting will set the inbound authentication setting to be determined by the postoffice restriction settings. Please see the postoffice restrictions ('Postoffice - Restrictions' in the on-line documentation) setting Any emails to this postoffice must come from authenticated connections for more information.</td>
</tr>
<tr>
<td>Allowed SMTP Commands</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

### 6.2.3.8 SMTP - Delivery

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

Delivery failure notifications can be customized for the SMTP service. Templates can be used for either a post office (if the message which fails can be attributed to a post office) or for the server.

The template files for a post office need to be configured in the following folder:
Mail Enable\Config\Postoffices\[postoffice]

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

MailEnable provides two template files for non-delivery reports:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP-NDR-FAILEDRECIPIENTS.TXT</td>
<td>Non-Delivery Message that has a list of failed recipients (ie: one or more recipients were refused by the server)</td>
</tr>
<tr>
<td>SMTP-NDR.TXT</td>
<td>Non-Delivery Message that has no failed recipients (ie: transmission errors, system errors)</td>
</tr>
</tbody>
</table>

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

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

6.2.3.10 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Log</td>
<td>Enables the Activity Log.</td>
</tr>
<tr>
<td>Include Debug information in the Activity log</td>
<td>Merges the debug logging information within the activity log file</td>
</tr>
<tr>
<td>Debug Log</td>
<td>Enables the Debug Log.</td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Enables W3C logging for the SMTP service. W3C logging can specify which fields are logged and the rollover frequency. The directory can also be specified.</td>
</tr>
</tbody>
</table>

### 6.2.3.11 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

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

**6.2.3.12 SMTP - White list**

Whitelisted IP addresses are not checked for reverse DNS blacklisting, PTR records, Greylisting, or SPF and will not be auto-banned.
**White list IP addresses** are those that are not checked for reverse DNS blacklisting or SPF and are not automatically blocked by the SMTP security options.

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

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

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

### 6.2.3.13 SMTP - Sender Policy Framework (SPF)

SPF is an acronym for Sender Policy Framework. It describes a method of verifying whether a sender is valid when accepting mail from a remote mail server or email client. An SPF check involves verifying the email address the sender is using to send from, and the IP address they connect to the SMTP service with. SPF uses the sender’s domain to retrieve a TXT DNS record (basically a small text snippet) that describes which IP addresses the domain sends on. The retrieved record is then compared against the connecting IP address and if it matches then the sender is determined to be valid; otherwise it indicates that the sender is impersonating the sending domain.
In basic terms, Sender Policy Framework (SPF) is a method of detecting when an email sender is forging their sender address. It does this by confirming with the senders alleged domain (via DNS lookups) as to whether the connecting IP address, or other details, are valid. For example, if a spammer was sending emails as greatdeals@aol.com, a lookup is done for SPF details against the AOL.com domain. Information returned from this lookup could determine that since the IP address of the spammer is not an AOL IP address then it is likely to be spam. Email can then be marked as likely spam, or not accepted. An SPF record can also be more complicated than just a list of IP addresses, in order to give more flexibility. For details on SPF, see the following website: http://spf.pobox.com

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SPF</td>
<td>Enables SPF detection.</td>
</tr>
<tr>
<td>Reject failures</td>
<td>If an incoming connection returns a SPF fail, then the email message will not be accepted by the SMTP service.</td>
</tr>
<tr>
<td>Add Received-SPF header for unauthenticated senders</td>
<td>Adds the Received-SPF header to all unauthenticated emails arriving via SMTP.</td>
</tr>
<tr>
<td>Pass local IP addresses (no)</td>
<td>If an IP address is determined to be local, then an SPF check is not done.</td>
</tr>
</tbody>
</table>
checking will be 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 7.4.2).

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

6.2.3.14 SMTP - Reverse DNS blacklisting

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

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

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

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

Action when detected

- **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. If enabled the message will be delivered to the Junk E-mail folder within the email client. For further information on the Mark Message as Spam action please review Feature selection in the Message store section (‘Postoffice - Message store’ in the on-line documentation).

Enable DNS Blacklisting

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 whether it is spam.

Action when detected

- **Don’t accept the email** - this will prevent connection by the remote server and respond accordingly. This is the best option for reducing server load.
- **Mark the message as spam** - by adding a line to the email header indicating it is spam. This will allow locally delivered messages to be delivered to the Junk E-mail folder. For further information on the Mark Message as Spam action please review the Feature selection section (‘Postoffice - Feature selection’ in the on-line documentation).

The “Replace the link” option will remove the failed link URL of the message and replace it with “Link is removed”.

Configure Blacklists Button

Opens a screen to allow blacklists to be created or added.
<table>
<thead>
<tr>
<th>Lookup type</th>
<th>The lookup type that will be used for the blacklist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Server</td>
<td>The name of the DNS Zone or the IP Address of the DNS host that should be queried.</td>
</tr>
<tr>
<td>Record Type to check for</td>
<td>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.</td>
</tr>
<tr>
<td>Response</td>
<td>The response that can be sent to the client when a message has been rejected.</td>
</tr>
</tbody>
</table>

**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.

### 6.2.3.15 SMTP - Greylisting

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

Greylisting can be enabled for the SMTP service and the message retry initial delay time and the time the IP and sender/recipient is remembered for can be configured here.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| 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 (on-line documentation) 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 remembered for | 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. |

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.

### 6.2.3.16 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.

6.2.4 Post Office Connector

6.2.4.1 Post office connector

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

6.2.4.2 Post office connector - General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When mailbox has reached quota</td>
<td>Specify what occurs when a mailbox’s quota is exceeded. Determine whether the user is notified of the quota issue and whether the message is returned to the sender, or, sent to the postmaster for that post office.</td>
</tr>
<tr>
<td></td>
<td>Send notifications only: Will send a notification message and not the entire message.</td>
</tr>
<tr>
<td>Notifications when quota is reached</td>
<td>Configure what notifications are sent when a quota is reached, such options such as, notify Sender only, notify sender and mailbox and send no notifications.</td>
</tr>
<tr>
<td>Quota enumeration</td>
<td>When a mailbox is at its quota, it can be calculated in two different ways. 1. Only Inbox folder counts towards quota 2. All users mail folders counts towards quota (Example: Sent Items, Drafts, Inbox)</td>
</tr>
<tr>
<td>Auto</td>
<td>When this setting is enabled there are two selections;</td>
</tr>
</tbody>
</table>
1. The default setting to “Always respond to the sender”

2. Send one response per sender per day can help reduce the problem of spammers generating unnecessary mail. Also if a sender needs to send to a MailEnable mailbox that has an auto responder configured, then they will not receive more than one auto-responder per day.

If the check box is cleared then the auto responder feature is disabled. This can aid in the diagnosis of mail loops or any possible auto responder issues.

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

Redirection handling 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.

6.2.4.3 Post office connector - Logging

Advanced Logging

- **Activity Log**
  - Path: `C:\PROGRAM--MAIL\LOGGI`
  - **Browse**

- **Debug Log**
  - Path: `C:\PROGRAM--MAIL\LOGGI`
  - **Browse**

[Image of the Postoffice Properties window]
6.3 Services

6.3.1 Management Service

6.3.1.1 Management Service

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

6.3.1.2 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

6.3.1.2.1 Management Logging
### 6.3.1.3 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

### 6.3.1.4 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

6.3.2 Web Administration

6.3.2.1 Web administration

The Web Administration interface 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.

Some of the many features are:
- Works with IIS4.0 and greater, allowing easy integration
- Manage domain related information
- Manage the creation of email addresses
- Manage email lists and groups
- Custom skins, leveraging skins from web mail

6.3.2.2 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.**

![WebAdmin Properties](image)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure...</td>
<td>Opens the Site configuration window. Please see How to add the Web Administration interface to web sites within IIS (Section 6.3.2.5)</td>
</tr>
<tr>
<td>Default base</td>
<td>Is the default base folder for the Web administration interface if one has not been specifically assigned to a website.</td>
</tr>
</tbody>
</table>

6.3.2.3 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.

![WebAdmin Properties](image)
6.3.2.4 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.

![Web Admin Configuration]

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 5.3.6) 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.
### Mailbox Properties

**Mailbox Name:**
- Test

**Username for mail clients:**
- Test@MailEnable

**Password:**
- [Input field]

**Mailbox Type:**
- ADMIN

- **Mailbox has a size limit**
  - **Mailbox quota:** Unlimited kilobytes (KB)

- **Prevent user from authenticating**
- **Mailbox is Disabled**

**Mailbox Size:**
- 7 kilobytes (7 KB)

**Delete Messages...**

---

**Service Selection**

<table>
<thead>
<tr>
<th>Service</th>
<th>Restrictions</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>POP Retrieval</td>
<td>Filters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web Mail</td>
</tr>
</tbody>
</table>

---

**General**

<table>
<thead>
<tr>
<th>Addresses</th>
<th>Redirection</th>
<th>Actions</th>
<th>Messages</th>
</tr>
</thead>
</table>

---

**OK** **Cancel** **Apply** **Help**
6.3.2.5 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

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

### 6.3.2.6 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 MailEnable web admin web site within IIS the following URL can be used to access the interface:

Example: http://exampledomain

6.3.3 IMAP Service

6.3.3.1 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 can store messages on a local machine or on a server.

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

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

6.3.3.2 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 > IMAP. Right click on the IMAP icon and select Properties. The General tab options are explained below:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Concurrent connections (threads)</td>
<td>The number of threads that will be used by the IMAP service to handle client requests.</td>
</tr>
<tr>
<td>IMAP port</td>
<td>Port for listening on. Default is 143.</td>
</tr>
<tr>
<td>IMAP Enable SSL (Default Port)</td>
<td>This will enable SSL certificate encryption for the default port that IMAP is running on. Place a tick in this box to enable the service. This also has to be enabled at a server level in the MailEnable Administration program under Server &gt; Localhost Properties &gt; SSL tab.</td>
</tr>
<tr>
<td>Also listen on alternate port</td>
<td>An alternate port can be selected.</td>
</tr>
<tr>
<td>IMAP Enable SSL (Alternate Port)</td>
<td>This will enable SSL certificate encryption for the alternate port that IMAP is running on. The default port number is 993. Place a tick in this box to enable. The service also has to be enabled at a server level in the MailEnable Administration program &gt; Server &gt; Localhost Properties &gt; SSL tab.</td>
</tr>
<tr>
<td>Client Connections</td>
<td>Select either an unlimited number of client connections, or specify a maximum number of concurrent connections. Specifying a maximum number of connections may reduce server load by limiting the threads that IMAP can use.</td>
</tr>
<tr>
<td>Enable NTLM authentication</td>
<td>If enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled use this secure authentication. For example, in Outlook the feature is called SPA - Secure Password Authentication. More information on NTLM can be found in the Overview of NTLM authentication (Section 11.2).</td>
</tr>
<tr>
<td>Enable CRAM-MD5 authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Timeout for idle connections</td>
<td>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.</td>
</tr>
<tr>
<td>IP Addresses to bind to</td>
<td>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</td>
</tr>
</tbody>
</table>
6.3.3.3 IMAP - Logging

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

6.3.4 POP Service

6.3.4.1 POP service

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

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

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

Right click on the POP icon and select Properties.

6.3.4.2 POP - General

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum concurrent connections</td>
<td>The number of concurrent connections from email clients that the service will allow.</td>
</tr>
<tr>
<td>Alternate @ characters</td>
<td>Some older mail clients don’t allow the use of @ in the username section. Since the MailEnable usernames are formatted in mailboxname@postoffice format, this may cause problems. To solve this, MailEnable can specify the characters that can be used as a substitute. Just enter</td>
</tr>
</tbody>
</table>
the list of characters such as #$%. This will allow users to log on using mailboxname@postoffice, mailboxname#postoffice, mailboxname$postoffice and mailboxname%postoffice.

<table>
<thead>
<tr>
<th>POP Port</th>
<th>The port MailEnable will allow client POP connections on. The default is 110.</th>
</tr>
</thead>
<tbody>
<tr>
<td>POP Enable SSL (Default Port)</td>
<td>Enables SSL encryption for the default port that POP is running on. When enabling SSL make sure a valid SSL certificate has been selected in the MailEnable Administration &gt; Server &gt; Localhost Properties &gt; SSL tab</td>
</tr>
<tr>
<td>Also listen on alternate port</td>
<td>Allows the POP service to listen on an alternate port. Usually this is done to cater for clients who may be on connections where their outbound port 110 has been blocked.</td>
</tr>
<tr>
<td>POP Enable SSL (Alternate Port)</td>
<td>Enables SSL certificate encryption for the alternate port that POP is running on. The default port number is 995. When enabling SSL make sure that a valid SSL certificate has been selected in the MailEnable Administration &gt; Server &gt; Localhost Properties &gt; SSL tab.</td>
</tr>
<tr>
<td>Enable APOP authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Enable NTLM authentication</td>
<td>If this feature is enabled then secure authentication between the server and the supported client is enabled. This will allow the server to accept requests from the client to use secure transmissions for the authentication method. The client also has to be enabled to use this secure authentication. For example, in Outlook the feature is called SPA - Secure Password Authentication. More information on NTLM can be found in the Overview of NTLM Authentication section (Section 11.2).</td>
</tr>
<tr>
<td>Enable CRAM-MD5 authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Timeout for idle connections</td>
<td>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.</td>
</tr>
</tbody>
</table>

| 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. |

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

### 6.3.4.4 POP - Logging

The **POP Properties** dialog allows you to configure the POP service settings.

**General** tab:
- **Enable Logging:** Check this box to enable logging.
- **Active Log Type:** Choose the log type.
- **Logging Options:**
  - **Activity Log:** Check this box to log activity.
  - **Debug Log:** Check this box to log debug information.
  - **Path:** Select the log file path.
  - **Browse:** Click to browse for the log file path.

**Advanced** tab:
- Additional settings for advanced users.

**Logging** tab:
- Additional logging settings.

©2011 MailEnable Pty Ltd. All Rights Reserved.
6.3.5 Web Mail

6.3.5.1 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 6.3.5.3.2)

6.3.5.2 Web Mail - Properties

6.3.5.2.1 Web Mail - General

![WebMail Properties](image)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users can configure POP Retrieval items</td>
<td>When disabled the POP Retrieval option under the Advanced branch within the Web Mail Options page will no longer be available.</td>
</tr>
<tr>
<td>Users can add a redirection</td>
<td>When disabled the Redirections option under the Mail branch within the Web Mail Options page will no longer be available.</td>
</tr>
<tr>
<td>User can configure autoresponders</td>
<td>When disabled the Auto response option under the Mail branch within the Web Mail Options page will no longer be available.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable calendaring</td>
<td>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.</td>
</tr>
<tr>
<td>Enable tasks</td>
<td>Enables or disables the use of tasks for all web mail users</td>
</tr>
<tr>
<td>Users can change their spam protection level</td>
<td>When disabled the Spam protection option under the Advanced branch within the Web Mail Options page will no longer be available.</td>
</tr>
<tr>
<td>User can set their display name</td>
<td>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.</td>
</tr>
<tr>
<td>User can change their passwords</td>
<td>This gives a mailbox user the ability to change their password in the options of the web mail.</td>
</tr>
<tr>
<td>Create URL and email hyperlinks for plain text messages</td>
<td>Enables the underlining and HTML link creation for emails and URLs in a message formatted in plain text format.</td>
</tr>
<tr>
<td>Display HTML mails in preview window</td>
<td>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.</td>
</tr>
<tr>
<td>Users can publish resources</td>
<td>When disabled the Calendar Publishing option under the Calendar branch within the Web Mail Options window will no longer be available.</td>
</tr>
<tr>
<td>Enable help</td>
<td>Enables help links within the web mail interface</td>
</tr>
<tr>
<td>Show branded logos</td>
<td>Enables/Disables company logos within Web Mail displayed in the top left hand corner of the interface.</td>
</tr>
<tr>
<td>Don’t add client IP addresses to headers</td>
<td>Enabling this option will hide the clients IP address within the message RECEIVED header line when sent from Web Mail.</td>
</tr>
<tr>
<td>Users can access activity view</td>
<td>When disabled the user will no longer be able to view statistics in Web Mail.</td>
</tr>
<tr>
<td>Users can edit their Whitelist</td>
<td>When disabled the Whitelist option under the Mail branch within the Web Mail Options page will no longer be available.</td>
</tr>
<tr>
<td>Users can edit their Blacklist</td>
<td>When disabled the Blacklist option under the Mail branch within the Web Mail Options page will no longer be available.</td>
</tr>
<tr>
<td>Show YouTube Previews</td>
<td>Will render YouTube video links in messages so that the videos can be viewed within the message.</td>
</tr>
<tr>
<td>Enable Media Player</td>
<td>Enables MP3 media player so that MP3 files can be streamed from within a message attachment or within MyFiles storage files.</td>
</tr>
<tr>
<td>File Storage is enabled</td>
<td>When disabled the MyFiles folder branch will no longer be visible within Web Mail.</td>
</tr>
<tr>
<td>Default Character Set</td>
<td>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</td>
</tr>
</tbody>
</table>
mail and are missing extended characters or they are displayed incorrectly, it could mean that the user has not set their character set.

### Default time zone

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

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

### Site Configuration

If the Configure... button is selected the Site Configuration screen is displayed. The screen will list all the web sites that are published under IIS. Web mail can then be installed or removed for each of these sites. See the Publishing via host headers of virtual directories section (Section 6.3.5.3.2) for more details.

## 6.3.5.2.2 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:

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

![WebMail Properties window](image)
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.

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

6.3.5.2.3 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.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging status</td>
<td>The logging status can be set to either ‘Disabled’, ‘Log to Debug log’ or “Log to Windows Event log’. The sliding bar sets the level of logging from low to high. Low level logging includes only logins, high level logging includes listing messages, folders, sending, receiving, actions, and retrieval.</td>
</tr>
</tbody>
</table>

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

6.3.5.3 Configuring Web Mail

6.3.5.3.1 Configuring web mail Overview

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

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

6.3.5.3.2 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.

---

**Site Configuration**

Below are the current web sites configured under Microsoft IIS (Internet Information Services). This screen will allow you to configure the MailEnable mailbox for any of these sites. If you wish to add more websites you will need to do this through IIS.

<table>
<thead>
<tr>
<th>Site</th>
<th>ID</th>
<th>State</th>
<th>Webmail</th>
<th>Base</th>
<th>Skin</th>
<th>Postoffice</th>
<th>Lang</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Web Site</td>
<td>1</td>
<td>Running</td>
<td>Installed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MailEnable Mobile</td>
<td>3</td>
<td>Running</td>
<td></td>
<td></td>
<td></td>
<td>Mondo</td>
<td></td>
</tr>
</tbody>
</table>

---

118 Professional Manual
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 (on-line documentation) 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.

### 6.3.5.4 Browser compatibility

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

<table>
<thead>
<tr>
<th>Browser</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 5.5 +</td>
<td>Windows</td>
</tr>
<tr>
<td>Firefox</td>
<td>Windows, Linux, Unix, Mac</td>
</tr>
<tr>
<td>Mozilla 1.7+</td>
<td>Windows, Linux, Unix, Mac</td>
</tr>
<tr>
<td>Netscape 7.1+</td>
<td>Windows, Linux, Unix, Mac</td>
</tr>
</tbody>
</table>
6.3.5.5 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**

**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**

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

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

D. Download file from File storage to local machine

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

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 the web

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.

### 6.3.6 Synchronization Service

#### 6.3.6.1 Synchronization - General

The Synchronization Service provides extensions that allow clients to access and synchronize messaging data over an array of protocols.
### 6.3.6.2 Synchronization - CalDAV

MailEnable’s Synchronization Service provides CalDAV services. CalDAV allows leading E-Mail clients and mobile devices (including the Apple iPhone), to access MailEnable mailbox calendars. CalDAV is ideal for mobile users who wish to access and update their calendar in real time. To configure CalDAV, the client is configured with a URL to point to the server calendar. It is also possible to configure CalDAV to access another user’s calendar by specifying their calendar address in the URL.

#### How to Enable CalDAV

1. Navigate to the following location within the administration console: servers > localhost > Services > Synchronization
2. Right click on Synchronization and select properties.
3. Navigate to the CalDAV tab
4. Tick the option Enable CalDAV support and iCalendar hosting
6.3.6.2.1 Published Calendars

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 an overview, and you should see specific documentation for each email client for correct usage.

<table>
<thead>
<tr>
<th>URL</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://host:port/calendars/mailbox@postoffice/calendar1.ics">http://host:port/calendars/mailbox@postoffice/calendar1.ics</a></td>
<td>Connects to a specific iCalendar file in a user's mailbox. In this case the file is calendar1.ics.</td>
</tr>
<tr>
<td><a href="http://host:port/calendars">http://host:port/calendars</a></td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

6.3.6.2.2 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.

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. ie: If you make changes to a calendar via CalDAV, only 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:

<table>
<thead>
<tr>
<th>URL</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://server:port/calendar">http://server:port/calendar</a></td>
<td>Connects to a mailbox calendar via CalDAV. You will need to supply a username and password of the mailbox being accessed.</td>
</tr>
<tr>
<td><a href="http://server:port/calendar/mailbox@postoffice/calendar">http://server:port/calendar/mailbox@postoffice/calendar</a></td>
<td>Connects to a specific mailbox calendar via CalDAV. Authentication may not be needed depending on the permissions the mailbox user has set.</td>
</tr>
</tbody>
</table>

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.

6.3.6.2.3 iCal and CalDav configuration

The Apple iCAL client is particular about connecting to CalDAV and CardDAV servers (in that it typically requires the correct configuration of DNS infrastructure). It often does not give meaningful errors when it is unable to connect to backend CalDAV servers.

To avoid connectivity issues, it is important that you have correctly configured SRV DNS records for the domains offering these services.

This document explains how to configure DNS and then configure an iCAL client.

CONFIGURING DNS INFRASTRUCTURE

When deploying CalDAV and CardDAV services, it is strongly recommended that you configure DNS records to allow clients to locate and connect to these services. This involves creating specific SRV DNS records so that they are published to clients.

For CalDAV you should configure the following SRV records:

Example: service record for server without transport layer security

```
_cal dav._ tcp  SRV 0 1 8008 example.com.
```

Example: service record for server with transport layer security

```
_cal dav s. _ tcp  SRV 0 1 8443 example.com.
```

Note: In the above example, you should also have a DNS A (Host) record created that equates "example.com" to an IP address.

More information can be found at:


Important: The Apple iCAL client will use Port 8443 by default. If you are having issues connecting from an iCAL client, it is suggested that you consider running the server on port 8443 for SSL and 8008 for Non-SSL. You should not use the port number for _caldav as and _caldav.

CONFIGURING AN iCAL CLIENT

To set up a iCAL to connect via CalDAV, please follow these steps.

1. Launch the iCAL application
2. Under the iCAL menu, select Preferences..
3. Click Accounts
4. Click + to add a new account
5. Set the Account type as CalDAV
6. Specify the username and password
7. Enter the server address as the domain name that is hosts the SRV records for calDAV (see earlier section on configuring DNS infrastructure). In the case of the example provided, this would be “example.com”.
8. You should then click the Create button. Once this is clicked, the iCAL client will query DNS for example.com and identify the appropriate SRV record. It will use this record to identify the host and port number that is will then connect to.

MANUALLY CONFIGURING AN iCAL CLIENT

If your initial connection fails, then you can continue and enter manual settings under “Calendar Server Options”, following these steps:

1. From the account template, select “iCal Server”
2. Re-enter your username and password as desired.
3. For the server address, specify the IP address or hostname of the server running CalDAV.
4. Leave the Server path as /calendar (for versions post MailEnable 5.10 you can leave the path as /principals/users/[username]/)
5. Specify the desired port Number (eg: 8443) and tick whether or not SSL is configured for this port (uncheck Kerberos Authentication).
6. Click Create to attempt to connect with the CalDAV server.

More information can be found at:


Apple also provides the following article:


6.3.6.3 Synchronization - SyncML

6.3.6.3.1 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 (such as the Funambol Microsoft Outlook Plugin) may communicate via plain text XML.

6.3.6.3.2 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 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.

6.3.6.3.3 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.
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.

6.3.6.4 Synchronization - HTTPMail

HTTP is the protocol that handles web traffic. It defines how web pages are formatted and the way they are delivered over the Internet. It also includes any information about the objects that are needed by proxy servers or a user’s web browser. HTTPMail is a relatively new protocol for the server hosted messaging services. HTTPMail provides an alternative to using POP and SMTP, with the added benefit of allowing messages to be hosted on the server (rather than downloaded onto the client). Further to this, using HTTPMail, messages can be moved between the server and local stores as required.
HTTPMail utilizes WebDAV HTTP Extensions to provide remote access to server hosted mail folders using standard HTTP communication. This service allows mail messages to be hosted on the server and provides tight integration with Outlook 2002 (and later) and Outlook Express, although subfolders are not supported in HTTPMail. Unlike IMAP, it does not require SMTP to send messages. HTTPMail posts messages into the post office where they are either locally delivered or dispatched through the SMTP Connector.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable public folders for post offices</td>
<td>Public Folders allow one or more mailboxes under the post office to share data (messages in a folder that is seen by all mailboxes in the post office.) Anything placed in this folder (Program Files\MailEnable\Post Offices[Post Office Name]\Pubroot) will become visible to all other mailboxes in the post office. This feature must be enabled for the post office in Post Office Properties. Please see Postoffice - Message Store (on-line documentation)</td>
</tr>
</tbody>
</table>

### 6.3.6.4.1 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 6.3.6.1)). 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 Outlook Express or Outlook 2002 as a mail client, select the mail protocol as HTTP and enter in the following details:

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

  http:// Your Server: 8080/MEHTTPMail

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

### 6.3.6.5 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 6.3.6.1))
- Username: mailboxname@postofficename
- Password: *****

### 6.4 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

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttachmentFilename</td>
<td>The name of the file that to add as an attachment.</td>
</tr>
<tr>
<td>AttachmentName</td>
<td>The name to call the attachment.</td>
</tr>
<tr>
<td>AuthenticationMode</td>
<td>Allows use of SMTP authentication.</td>
</tr>
<tr>
<td><strong>Method</strong></td>
<td><strong>Explanation</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>AddHeader</strong></td>
<td>Adds a custom header to the email. Be careful when using this function, as incorrectly formed headers could prevent the mail from being sent.</td>
</tr>
</tbody>
</table>
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 sends 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\mail enable\mail enable\Components\MEMail
```

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

### 6.4.1 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.
6.4.2 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

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttachmentFilename</td>
<td>The name of the file that to add as an attachment.</td>
</tr>
<tr>
<td>AttachmentName</td>
<td>The name to call the attachment.</td>
</tr>
<tr>
<td>AuthenticationMode</td>
<td>Allows use of SMTP authentication.</td>
</tr>
<tr>
<td></td>
<td>0 = No SMTP authentication</td>
</tr>
<tr>
<td></td>
<td>1 = SMTP authentication. You must populate the Username and Password properties in order to authenticate</td>
</tr>
<tr>
<td>ContentType</td>
<td>The ContentType of the email you are trying to send. For instance, if you wish to send a HTML email, use this property to set the content type to “text/html”.</td>
</tr>
<tr>
<td>ErrorString</td>
<td>This contains the full English language description of the last error. If you encounter an error, you can check this string for a more detailed error.</td>
</tr>
<tr>
<td>MailBCC</td>
<td>This is list of email addresses to BCC the email to. When using multiple email addresses, separate them with a semi-colon “;”.</td>
</tr>
<tr>
<td>MailCC</td>
<td>This is list of email addresses to CC the email to. When using multiple email addresses, separate them with a semi-colon “;”.</td>
</tr>
<tr>
<td>MailCCDisplayName</td>
<td>This is list of email addresses that are the display name corresponding to the email address set in MailCC. This list is optional. When using multiple email addresses, separate them with a semi-colon “;”.</td>
</tr>
<tr>
<td>MailFrom</td>
<td>This is the email address of the sender.</td>
</tr>
<tr>
<td>MailFromDisplayName</td>
<td>The display name of the MailFrom email address. This is the friendly name that the end user will see instead of the email address. For example, you may place the full name of the sender, or the department from which the email is coming from.</td>
</tr>
<tr>
<td>MailTo</td>
<td>The email address to send the email to. To send to multiple email addresses, separate the emails with a semi-colon “;”.</td>
</tr>
<tr>
<td>Property</td>
<td>Explanation</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MailToDisplayName</td>
<td>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”)</td>
</tr>
<tr>
<td>Messagebody</td>
<td>The message contents.</td>
</tr>
<tr>
<td>MessageBodyText</td>
<td>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 text/plain version of the message from the HTML content supplied (assuming the ContentType is set as text/html).</td>
</tr>
<tr>
<td>Password</td>
<td>Password to be used for SMTP authentication.</td>
</tr>
<tr>
<td>Postoffice</td>
<td>The post office name for the user</td>
</tr>
<tr>
<td>Server</td>
<td>The email server to connect to. If none is supplied, it will try to connect to the local machine.</td>
</tr>
<tr>
<td>ServerPort</td>
<td>The port to connect to. The default is 25.</td>
</tr>
<tr>
<td>Subject</td>
<td>The subject of the email message.</td>
</tr>
<tr>
<td>Username</td>
<td>Username to be used for SMTP authentication.</td>
</tr>
</tbody>
</table>

### Methods

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

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

### Advanced settings

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

The values are located under the following registry branch:

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

<table>
<thead>
<tr>
<th>Value</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
</table>

©2011 MailEnable Pty Ltd. All Rights Reserved.
### 6.4.3 Examples

#### Sending an HTML email from an ASP page

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

#### Sending an email with an attachment

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

7.1 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

![Extension Properties](image)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the processing of system filters for this server</td>
<td>Enables server wide level message content filtering</td>
</tr>
<tr>
<td>Junk E-mail Processing</td>
<td>Messages are moved to Inbox:</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Messages are moved to the Junk E-mail folder:</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>
7.2 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:

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

7.3 Spam Protection

Spam protection within MailEnable is what we refer to as a super script which 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 Management > 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 values depending on the score of points compared to the threshold you set in the spam protection values will be added:

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:
http://www.mailenable.com/kb?ID=ME020493

7.4 Global Filtering

7.4.1 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

7.4.2 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 7.5.1.1)

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 Message Body contains specific words

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

Where the To header line contains specific words

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

Enter email addresses here and then click the Add button. If multiple addresses are to be filtered, it is possible to add multiple addresses separated by a semi column - ensuring that no character spaces are
Where the Cc header line contains specific words

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

Where the To or Cc header line contains specific words

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

Where the From header line contains specific words

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

Where the message is marked as priority

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

Where the message size is more than the limit

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

Where the message 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.

Bayesian filter spam probability

Filter to set the threshold for spam probability of Bayesian filtering e.g., define the filter to mark messages as junk if they have over 96.5% spam probability. See Bayesian filtering section (Section 7.7.1.1) 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 7.4.1) 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 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.

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. This filter is useful to reduce the load on the SMTP service if many URL blacklists have been configured to perform lookups. The filter allows the MTA agent to perform the URL lookup after the message is routed from the SMTP inbound queue allowing the SMTP service to free resources quicker to accept messages.

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 DomainKey verification return results matching

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

7.4.3 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 bad mail folder. The message will still be delivered to the destination mailbox as well. To send to bad mail, and not deliver to the mailbox, create a Delete Message action to occur after the Copy to BadMail.
Copy to quarantine

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

Delete message

Deletes the message.

Notify sender

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

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

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

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

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

Notify address

This will send a notification message to a specified address.

Forward to address

This filter action forwards the email to an email address.

Execute application

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

Add header

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

Mark as spam

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

Add Subject Prefix

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

Stop processing filters

This action stops the processing of any more filter actions.

7.4.4 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
7.5 Scripted Filtering

7.5.1 Overview

7.5.1.1 Scripted Filtering

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

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

7.5.1.2 Literal values

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

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

Literal enumeration example

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

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

<table>
<thead>
<tr>
<th>Token</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%IPADDRESS%</td>
<td>The TCP/IP address of the originating message</td>
</tr>
<tr>
<td>%POSTOFFICE%</td>
<td>The post office that can reasonably be assigned to the message.</td>
</tr>
</tbody>
</table>
The sender of the message in Internal format of [CONNECTOR:Address]. E.g. [SMTP:xjz@mailenable.com]

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

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

7.5.1.3 Enumerations requiring the CriteriaMet syntax

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

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

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

7.5.2 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.

7.5.3 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.

<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
<th>Message ID</th>
<th>Connector</th>
<th>Filter</th>
<th>Result</th>
<th>Account</th>
<th>Sender</th>
<th>IP Address</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/21/06</td>
<td>Start</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>08/21/06</td>
<td>Exec</td>
<td>A.MAI</td>
<td>SMTP</td>
<td>Scripted</td>
<td>ADD_HEADER, NOTIFY_SENDER</td>
<td>[SMTP:<a href="mailto:user@mailenable.com">user@mailenable.com</a>]</td>
<td>127.0.0.1</td>
<td>Subject matched ABC</td>
<td></td>
</tr>
<tr>
<td>08/21/06</td>
<td>Exec</td>
<td>B.MAI</td>
<td>SMTP</td>
<td>Basic</td>
<td>ADD_HEADER, NOTIFY_SENDER</td>
<td>[SMTP:<a href="mailto:user@mailenable.com">user@mailenable.com</a>]</td>
<td>127.0.0.1</td>
<td>CRITERIA=SUBJECT, DATA=&lt;MF-W&gt;AB*/MF-W&gt;</td>
<td></td>
</tr>
</tbody>
</table>

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).

### 7.6 Antivirus filtering

#### 7.6.1 ClamAV Antivirus Filtering

**ClamAV Antivirus Filtering**

MailEnable now 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\MailEnable\Agents\MTA\Filters\MEAVCLM - (32Bit Windows) HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable\MailEnable\Agents\MTA\Filters\MEAVCLM
3. Downloads the latest ClamAV antivirus database definitions by calling the the ClamAV freshclam.exe service.

- **Note:** The ClamAV virus definitions need to be updated manually after the installation. Please visit the following MailEnable forum post on how to go about creating a Windows scheduled task for ClamAV updates. Please also refer to the ClamAV documentation for more information.

MailEnable recommends the use of ClamAV as it has been thoroughly tested and proven to be reliable and does not require any further manual configuration settings after the install. Although other Antivirus solutions can be used with MailEnable we strongly recommend using ClamAV. More information about using other Antivirus solutions can be found below:

http://www.mailenable.com/kb/Content/Article.asp?ID=me020144

- F-Prot
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 11.1.3) for more information on this.

Creating an antivirus filter

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

To create an antivirus filter:

1. Open the MailEnable Administration Program
2. Right click on the Messaging Manager > Filters branch and create a new filter.
3. 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

7.6.3 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:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Path</td>
<td>The path to the virus checker application. Only select the command line scanner for the antivirus application (the presets in MailEnable will point to the correct application).</td>
</tr>
<tr>
<td>Command line arguments</td>
<td>The command line arguments that are used to run the antivirus scanner. There should be no need to change these options unless adding your own antivirus scanner (i.e. not a preset).</td>
</tr>
<tr>
<td>Command line arguments will delete attachment</td>
<td>Selecting this will require that the command line scanner to delete any infected attachment. Some virus scanners cannot remove zip files that are infected with viruses using this option.</td>
</tr>
<tr>
<td>Return code will be checked against this list</td>
<td>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)</td>
</tr>
<tr>
<td>Return code check</td>
<td>Choose to detect the attachment as a virus if the return code is a number other than those in the list.</td>
</tr>
</tbody>
</table>

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

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

### 7.6.4 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](http://www.eicar.com). To perform more advanced testing and debugging, follow the details in this article - [http://www.mailenable.com/kb/viewarticle.asp?aid=85](http://www.mailenable.com/kb/viewarticle.asp?aid=85)

### 7.7 Bayesian filtering

#### 7.7.1 Configuring Bayesian Filtering

##### 7.7.1.1 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 7.7.4).

### 7.7.1.2 Step 1: Set up auto-training for the filter

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto-training</td>
<td>Check this box to enable auto-training. While the Bayesian Filter is in auto training mode, the functions to manually update the dictionary using the “mespamcmd.exe” command utility (as mentioned in the Spam Training Utility section (Section 7.7.5)) do not function. This is because when the auto-training is running, new additions to the dictionary are stored in memory, and not written to the hard drive until the MTA service is stopped. A global filter with the ‘Bayesian filter spam probability’ criteria must be configured for auto-training to work. This is described in Step 4. If a filter is not configured with a Bayesian criteria, then no auto-training will occur.</td>
</tr>
<tr>
<td>Options (Process HTML content in Messages)</td>
<td>If this option is selected and the message contains HTML, then the HTML is parsed as well as the message plain/text boundary. Tokens will therefore also include data from the HTML messages. It makes the filter more likely to detect HTML as spam because the tokens/patterns of the HTML of bad messages can be used to calculate the probability of spam.</td>
</tr>
<tr>
<td>Spam Honeypot Email Addresses (Edit address list)</td>
<td>Define email addresses that do not receive valid mail for sampling. This is described in Step 2.</td>
</tr>
<tr>
<td>Ham Addresses (Edit address list)</td>
<td>Define ‘ham’ or legitimate email addresses for sampling. This is described in Step 3.</td>
</tr>
</tbody>
</table>

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

### 7.7.1.3 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.

7.7.1.4 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.

7.7.1.5 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”.

7.7.1.6 Step 5: Testing the Bayesian filter

To ensure Bayesian filtering is working correctly (i.e. the Bayesian filter is using the dictionary and the designated actions are completed when messages are delivered to the system) requires testing. There are a few ways to determine if messages are being checked against the dictionary:

- METray (see the System Tray Utility section (Section 10.1)) shows instances where the Bayesian filter has scanned and detected spam. When the METray display window is open, enable the “View statistics since services were restarted”. The section that details how many “Bayesian Scans” have completed along with “Bayesian Detections” will display how many emails were checked and how many have been detected as spam since the MTA service was last started.
- Filter logs will also display any Bayesian detections. The logs are accessed via: MailEnable Administration program > Servers > Localhost > Filters > MailEnable Message Filter > Logs > Filters. If any messages have been detected and actioned by the Bayesian filter then a line in the logs will be displayed similar to the following:
  
  [Date-Time] [Message ID] SMTP Bayesian COPY_TO_QUARANTINE,DELETE
  [SMTP:sender@remotedomain.com] [IP_Address of sender]

- Messages passing through the Bayesian filter will have a header line added indicated the spam probability that was calculated. The header item is: X-ME-Bayesian: 0.000000

7.7.2 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.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>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 7.7.3).</td>
</tr>
<tr>
<td>Options (Process HTML content in Messages)</td>
<td>If this option is selected and the message contains HTML, then the HTML is parsed as well as the message plain/text boundary. Tokens will therefore also include data from the HTML messages. It makes the filter more likely to detect HTML as spam because the tokens/patterns of the HTML of bad messages can be used to calculate the probability of spam.</td>
</tr>
</tbody>
</table>
| 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
7.7.3 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.

7.7.4 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\*.mai"
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\*.mai"
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 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\*.mai"

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

7.7.5 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.

<table>
<thead>
<tr>
<th>MESPAMCMD [-options] [dictionary, paths]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[c] = Create Dictionary</td>
</tr>
<tr>
<td>[v] = Verify messages in the specified folder against the nominated Dictionary</td>
</tr>
<tr>
<td>[s] = Score a single message against the nominated Dictionary</td>
</tr>
<tr>
<td>[m] = Merge Spam and NoSpam folders into nominated Dictionary</td>
</tr>
<tr>
<td>[r] = Notifies the spam filter to reload the dictionary</td>
</tr>
</tbody>
</table>
[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
```

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.
8  Configuration of Email Clients

8.1 Configuring Email Clients

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

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

8.2 Netscape Messenger

To configure for Netscape Messenger:

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

8.3 Microsoft Outlook Express

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

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

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

8.4 Microsoft Outlook 2000

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

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

8.5 Microsoft Outlook 2002/2003

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

8.6 Microsoft Outlook 2007

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

8.7 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.

8.8 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:

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

8.9 Configuring clients for HTTPMail

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

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

Example

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

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

6. The wizard has now completed; please select Next.

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

8.10 Enabling logging for Microsoft Outlook

Microsoft Outlook Express

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

Microsoft Outlook

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

C:\Documents and Settings\[user]\Local Settings\Temp\Outlook Logging\[account]
9 Operational Procedures

9.1 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: [http://www.mailenable.com/kb/Content/Article.asp?ID=me020024](http://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 article: [http://www.mailenable.com/kb/viewarticle.asp?SS=backup&File=me020114.htm](http://www.mailenable.com/kb/viewarticle.asp?SS=backup&File=me020114.htm)

9.2 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 3 logs for each service. They are called W3C, Activity and Debug logs.

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

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

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


9.3 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: --4.1 ready at 08/28/09 14:04:45

Type the word QUIT and then press enter.

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

nslookup -type=MX aol.com

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

This is outlined as follows:

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

2. At the command prompt, enter the following:  telnet mail.mailenable.com 25

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

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

3. Type the following and press Enter: HELO YourDomainName

   The server should reply with a line similar to:

   250 Requested mail action okay, completed

4. Type the following and press Enter. Senderaddress is the email address you are sending from:

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: --4.1 ready at 08/20/09 23:49:40
EHLO test.mydomain.com.au
250-mailenable.com [192.168.1.1], this server offers 4 extensions
250-AUTH LOGIN CRAM-MD5
250-SIZE 10120000
250-HELP
250 AUTH=LOGIN
MAIL FROM:<senderaddress>
250 Requested mail action okay, completed
RCPT TO:<recipientaddress>
250 Requested mail action okay, completed
DATA
354 Start mail input; end with [CRLF].[CRLF]
Subject: Test Message
250 Requested mail action okay, completed
QUIT
221 Service closing transmission channel

Connection to host lost.

9.4 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:
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.

9.5 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: http://www.mailenable.com/kb/viewarticle.asp?aid=19

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

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

9.6 Licensing

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

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

For computers not connected to the Internet

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

Registration key retrieval method

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

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

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

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

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

This is to personalize the registration key code.

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

When using the Registration Wizard, follow these steps:

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

10.1 System Tray Utility (METray)

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open System Overview...</td>
<td>Opens the METray System overview diagram window</td>
</tr>
<tr>
<td>Open Real Time Activity Monitoring...</td>
<td>Opens the Real time monitoring window.</td>
</tr>
<tr>
<td>Open Message Tracker...</td>
<td>Opens the MailEnable Message tracking utility. Please see Message tracking (Section 10.5)</td>
</tr>
<tr>
<td>Diagnostic Utility...</td>
<td>Runs the MailEnable diagnostic report. Please see MailEnable Diagnostic Utility (Section 4.4.1)</td>
</tr>
<tr>
<td>Exit</td>
<td>Closes the METray utility</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Statistics:</td>
<td>Since services were restarted:</td>
</tr>
<tr>
<td></td>
<td>This option will display System Summary information since the last time the MailEnable services were restarted.</td>
</tr>
<tr>
<td>For this session:</td>
<td>This option will only display System Summary information from the time the METray utility has been opened.</td>
</tr>
</tbody>
</table>

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.
### SMTP Outbound
Displays real time monitoring information for SMTP outbound connections.

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

### SMTP Inbound
Displays real time monitoring information for SMTP inbound connections.

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

### IMAP
Displays real time monitoring information for IMAP connections.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection time</td>
<td>Indicates how long a connection has been active</td>
</tr>
<tr>
<td>Socket</td>
<td>Indicates the socket ID number for the active connection</td>
</tr>
</tbody>
</table>
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.

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

**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 server's SMTP service
8. Enter the authentication details that will be used for relaying the notification alert for the server
9. Click test to send a test message

**10.2 Activity Monitor**

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

**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](http://www.mailenable.com/utilities/addons/meactivitymonitor.zip)

10.3 MEInstaller

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

---

**MailEnable System Configuration Utility**

This utility allows you to install/re-apply installation steps that are performed by MailEnable's installation procedure.

- **Actions:**
  1. Common Installation File Permissions
  2. WebMail Installation / Reconfiguration (File Perms, User Rights, COM+, IIS Proxy User, etc)
  3. WebAdmin Installation / Reconfiguration (File Perms, User Rights, COM+, IIS Proxy User, etc)
  4. File Register Administration (MMC Components)
  5. Set IIS Application Isolation Levels [Low -> In Process]
  6. Set IIS Application Isolation Levels [Medium -> Pooled]
  7. Set IIS Application Isolation Levels [High -> Isolated] (Recommended)
  8. Clear System Blocking Files (removes any blk files remaining from system failure)
  9. Repair Configuration Files (Hosting Controller User's Only)
  10. Apply Strict Server Security Policy (Advanced Configuration Only)
  11. Apply Registry Permissions for IME_ADMIN, IME_USER, and IME_SYSTEM
  12. Reset IIS Virtual Directory Configuration settings for ASP/ASPX Platform

Sets the file permissions on the entire MailEnable message store and ensures that MailEnable accounts have access to such resources.

---

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.

### 10.4 Command Line Send Utility (MESend)

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

**Syntax**

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

**Example**

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

*Note: At least one recipient must be supplied.*

### 10.5 Message Tracking

The message routing trace utility provides an interface to track messages through MailEnable. It is a useful tool to determine whether a message was accepted by the server and as to where it was directed to.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date (mandatory)</td>
<td>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 accepted by the MailEnable server. Eg: postoffice connector logs &gt; MTA agent logs &gt; SMTP connector logs</td>
</tr>
<tr>
<td>Sender (optional)</td>
<td>Enter the sender’s email address.</td>
</tr>
<tr>
<td>Recipient (optional)</td>
<td>Enter the recipient’s email address</td>
</tr>
<tr>
<td>Backtrace Message from Outgoing Queue to Origin</td>
<td>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.</td>
</tr>
<tr>
<td>Cancel Search…</td>
<td>Cancels the search process</td>
</tr>
<tr>
<td>Show Transaction…</td>
<td>Displays the SMTP transaction only</td>
</tr>
<tr>
<td>Trace Message…</td>
<td>Will trace through all MailEnable log files from the SMTP transaction to mailbox delivery.</td>
</tr>
</tbody>
</table>

Information on how to track messages as they pass through the MailEnable services can be found within the following knowledgebase article: [http://www.mailenable.com/kb/Content/Article.asp?ID=me020252](http://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: [http://www.mailenable.com/utilities/addons/MEMSGTRK.zip](http://www.mailenable.com/utilities/addons/MEMSGTRK.zip)

### 10.6 Backup utility

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

This utility allows you to either backup or restore MailEnable data to local disk. If you wish to backup MailEnable, please enter a descriptive name for the backup and click the Backup button. To restore an existing backup, select the backup set name and click the restore button. If you are using a database for your configuration store, then you will need to use your database backup procedures for the configuration data.

![MailEnable Backup and Restore Utility - V1.5](http://www.mailenable.com/utilities/addons/MEMSGTRK.zip)
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup</strong></td>
<td>To backup MailEnable, select a descriptive name for the backup and select “Backup”.</td>
</tr>
<tr>
<td><strong>Restore</strong></td>
<td>To restore an existing backup, select the back up set name from the drop down box and select “Restore”.</td>
</tr>
<tr>
<td><strong>Calculate size</strong></td>
<td>Calculates the maximum storage size required in the backup location to successfully backup the complete configuration.</td>
</tr>
</tbody>
</table>

### 10.7 Queue overview

The Queue overview lists the number of messages in the outbound SMTP queue by the destination domain name. The utility will iterate 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:*

Appendix

11.1 Antivirus Configuration

11.1.1 Using your own antivirus scanner

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

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

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

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

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

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

The respective settings are:

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

"Exit Codes": eg: 1 2 9: space delimited string containing application exit codes

"Exit Codes Error Inclusive": 0/1 - on/off: used to configure whether the "Exit Codes" indicate errors or successes

A sample registry import file is outlined below:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Mail Enable\Mail Enable\Agents\MTA\Filters\Custom]

"Status"=dword:00000000

"Antivirus Notification Message"=">

"Antivirus Scratch Directory"="C:\\Program Files\\Mail Enable\\Scratch"

"Antivirus Parameters"=""[AGENT]" \\[FILENAME]\" -s - nb -nc"

"Antivirus Agent"="C:\\Program Files\\Virus Scanner\\CUSTOM.EXE"

"Provider DLL"="MEAVGEN.DLL"

"Program Name"="Custom"

"Program Info"="This is a template for new virus scanners."

"Exit Code Enabled"=dword:00000000

"Exit Codes Error Inclusive"=dword:00000001

"Exit Codes"=\"1\"

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

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

**F-Prot**

Company: Frisk International  
**Product Name:** F-Prot for Windows [http://www.f-prot.com/](http://www.f-prot.com/)

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

**Sophos**

Company: Sophos  
**Product Name:** Sophos Antivirus [http://www.sophos.com/](http://www.sophos.com/)

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

**Norman Antivirus**

Company: Norman  
**Product Name:** Norman Virus Control (NVC)

**Configuration Guidelines:** MailEnable Knowledge Base [http://www.mailenable.com/kb/Content/Article.asp?ID=me020290](http://www.mailenable.com/kb/Content/Article.asp?ID=me020290)

**Panda**

Company: Panda Software  
**Product Name:** Panda Command Line [http://www.symantec.com/index.htm](http://www.symantec.com/index.htm)

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

**Symantec Norton Antivirus**

Company: Symantec  
**Product Name:** Norton Antivirus (Corporate Edition) [http://www.symantec.com/index.htm](http://www.symantec.com/index.htm)

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

**McAfee Virus Scan**

Company: McAfee  
**Product Name:** McAfee Virus Scan [http://www.mcafee.com/](http://www.mcafee.com/)

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

**Grisoft AVG**

Company: Grisoft  
**Product Name:** AVG [http://www.grisoft.com](http://www.grisoft.com)
11.1.3 Real time protection

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

<table>
<thead>
<tr>
<th>Vendor/Product</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norton Antivirus Corporate Edition</td>
<td>Can exclude directories and file types.</td>
</tr>
<tr>
<td>McAfee Virus Scan</td>
<td>Can exclude directories and file types.</td>
</tr>
<tr>
<td>Panda</td>
<td>Can exclude specific folders.</td>
</tr>
<tr>
<td>AVG</td>
<td>Can exclude directories and file types.</td>
</tr>
<tr>
<td>Norman</td>
<td>Can exclude directories and file types.</td>
</tr>
<tr>
<td>F-Prot</td>
<td>Can exclude directories and file types.</td>
</tr>
</tbody>
</table>

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

11.2 Overview of NTLM authentication

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

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

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

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

This authentication mechanism, is well suited in environments where single sign-on is required or desirable. Using NTLM, once the user has logged into 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.

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

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

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](image)

11.3 Accessing web mail for automatic sign-on

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

**Syntax:**

```plaintext
```

**Example:**

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

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:**

```plaintext
http://127.0.0.1/MEWebMail/hoodoo/lang/EN/login.asp?LanguageID=EN&UserID=James@MailEnable&Password=password&Method=Auto&skin=hoodoo&offset=-600
```
This will pass a time offset of 10 hours for the client to use against the message header when displaying the list of messages.

### 11.4 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.

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

### 11.5 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.

<table>
<thead>
<tr>
<th>Error</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x800CCCFC4</td>
<td>HTTPMail</td>
<td>Outlook settings may be invalid or a firewall is preventing connection to the remote MailEnable Server.</td>
</tr>
<tr>
<td>0x800CCC79</td>
<td>SMTP</td>
<td>SMTP Relay settings are preventing the sending of messages to MailEnable. Ensure</td>
</tr>
</tbody>
</table>
that SMTP Authentication is enabled.

<table>
<thead>
<tr>
<th>Code</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x80042109</td>
<td>SMTP</td>
<td>Outlook is unable to connect to the outgoing (SMTP) e-mail server.</td>
</tr>
<tr>
<td>0x8004210A</td>
<td>POP</td>
<td>The operation timed out waiting for a response from the receiving (POP) server. Establish whether it is possible to telnet to port 110 of the mail server.</td>
</tr>
<tr>
<td>0x800CCC0F</td>
<td>POP</td>
<td>The mail client is unable to contact the MailEnable Server, most likely because a firewall is preventing access or the supplied IP Address is incorrect.</td>
</tr>
<tr>
<td>0x8004210B</td>
<td>POP</td>
<td>Verify that the service pack for Microsoft Office XP is installed.</td>
</tr>
<tr>
<td>0x800CCC0D</td>
<td>POP</td>
<td>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.</td>
</tr>
<tr>
<td>0x800CCC0E</td>
<td>SMTP</td>
<td>This error means that the mail client is connecting to the server via POP, but the SMTP Service is either not running or is configured incorrectly. Verify if the SMTP service is running by using the telnet utility to telnet to port 25 of the mail server. If the server responds, then the issue is most likely that mail client settings are invalid.</td>
</tr>
</tbody>
</table>

### 11.6 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:

```bash
telnet mail.mailenable.com 25
```

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

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

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

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

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

3. Type the following and press Enter: `HELO YourDomainName`

   The server should reply with a line similar to:
250 Requested mail action okay, completed

4. Type the following and press Enter. Senderaddress is the email address you are sending from:

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: --4.1 ready at 08/20/09 23:49:40
EHLO test.mydomain.com.au
250-mailenable.com [192.168.1.1], this server offers 4 extensions
250-AUTH LOGIN CRAM-MD5
250-SIZE 10120000
250-HELP
250 AUTH=LOGIN
MAIL FROM:<senderaddress>
250 Requested mail action okay, completed
RCPT TO:<recipientaddress>
250 Requested mail action okay, completed
DATA
354 Start mail input; end with [CRLF],[CRLF]
Subject: Test Message
250 Requested mail action okay, completed
11.7 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 shown in the square brackets in the box labeled Significant Event Instances. This gives a good indication of the severity of the event.

11.8 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: http://www.mailenable.com/kb/viewarticle.asp?aid=19

The above-mentioned approach is used if the backup mail servers are distributed in different geographic or logical locations.
A second alternative is to host all of the mail servers on the same local network and cluster the servers. This allows MailEnable to be installed on multiple servers and have them all use the same store for their messages and post office data. Any of these servers can then be used to access the mail. This requires that one of the servers share the mail data and configuration directories and that the others access them.

### 11.9 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:

```xml
<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.


### 11.10 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 of 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.
12 Glossary

A

Address Map
An address map is used to define source and target mail exchanges between Connectors by the Mail Transfer Agent. For example, mail sent to the SMTP address [SMTP:Jones@mailenable.com] is likely to have an address map to the post office address [SF:MailEnable/JONES].

Agents
Agents run to 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.

**Recipient**
The address to where the email is destined.

**Services**
Services expose MailEnable functionality to external agents or programs. An example of a service is the POP3 service. This service allows mail clients to access mail from their post office. MailEnable employs standard Windows Services that make it compatible with Windows NT/2000/2003.
13 Warranty

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

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

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

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

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

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

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

://, 105-106

Accessing web mail for automatic sign-on, 177-178

Activity Monitor, 168-169

Administration

Administration, 31
Advertising and Campaign Management, 64
Delete messages, 41
Domain - Blacklists, 43-44
Domain - DKIM (DomainKeys), 44-47
Domain - General, 42-43
Domain configuration, 42
Edit default message, 42
Email users (all), 41
Email users (individual), 41
Export users, 40-41
Group - General, 54-55
Group configuration, 53
How to add a group member, 53-54
How to create a domain, 42
How to create a group, 53
How to create a list, 55
How to create a mailbox, 47
How to create a Post Office, 35-36
How to enable Advertising banners in web mail, 65
How to enable campaign management, 64-65
How to import group members, 54
Import users, 41
Import Windows users, 41
Importing list members, 59
List commands, 59
Lists - General, 55-56
Lists - Headers and Footers, 58-59
Lists - Options, 56-58
Lists, 55
Localhost - Auditing, 63-64
Localhost - General, 59-60
Localhost - Policies, 61-62
Localhost - Secure Sockets Layer (SSL) encryption, 62-63
Mailbox - Actions, 50-51
Mailbox - Addresses, 48-49
Mailbox - General, 47-48
Mailbox - Messages, 51-52
Mailbox - POP Retrieval, 52-53
Mailbox - Redirection, 49-50
Mailbox Overview, 47

188 Professional Manual
Management Logging, 96-97
Management properties, 96
Messaging Manager - Administration, 32-33
Messaging Manager - Footers, 34-35
Messaging Manager - General, 32
Messaging Manager - Security, 33-34
Messaging Manager, 31-32
Option Files, 65-66
Post office - General, 36-37
Post office actions, 40
Post office configuration, 35
Postoffice - Footers, 37-38
Postoffice - Quota, 38-39
Postoffice - Web admin, 39-40
Set quota, 41-42
Administration, 14-15, 31
Advanced Script Example, 145-146
Advertising and Campaign Management, 64
Appendix
Accessing web mail for automatic sign-on, 177-178
Configuring redundant or backup (MX) mail servers, 164
Diagnosing Outlook/Outlook Express error codes, 178-179
DNS error codes and descriptions, 178
Increasing 10000kb upload limit for Webmail, 182
Log analyser, 181
Logical architecture and message flow, 182-184
Manually testing if MailEnable can send mail to remote servers, 161-163
Overview of NTLM authentication, 176-177
Real time protection, 176
Selecting an antivirus application, 174-176
Using your own antivirus scanner, 174
Backing up and restoring data, 161
Backup utility, 172-173
Basic Script Example, 145
Bayesian filter general settings, 151-153
Browser compatibility, 119-120
Check and configure DNS settings, 29-30
Check mail services, 30
ClamAV Antivirus Filtering, 146-147
Command Line Send Utility (MESend), 171
Configuration of connectors, services and agents
  Browser compatibility, 119-120
  Configuration, 128-129
  Configuring the server, 131
  Configuring web mail Overview, 117
Connectors, 69
Examples, 134
File Storage, 120-121
Greylist Cleanup agent, 97
How to access the Web Administration interface, 105-106
How to add the Web Administration interface to web sites within IIS, 104-105
How to enable the Web Administration interface, 101-104
iCal and CalDav configuration, 124-125
IMAP - General, 106-108
IMAP - Logging, 108
IMAP Service, 106
Integrated Mailbox Calendar, 123-124
List Server Connector, 70-71
Log Archive agent, 97-99
Management Service, 96
MTA - Archiving, 68-69
MTA - General, 67-68
MTA Overview, 67
POP - Advanced, 110-111
POP - General, 109-110
POP - Logging, 111-112
POP Retrieval Connector, 69-70
POP service, 108-109
Post office connector - General, 94-95
Post office connector - Logging, 95-96
Post office connector, 93-94
Published Calendars, 123
Publishing via host headers or virtual directories, 117-119
Services, 96
SMTP - Advanced SMTP, 79-81
SMTP - Blocked addresses, 84-85
SMTP - Delivery, 81-83
SMTP - General, 71-73
SMTP - Greylisting, 91-92
SMTP - Inbound, 73-74
SMTP - IP Blocking, 92-93
SMTP - Logging, 83-84
SMTP - Outbound, 74-76
SMTP - Relay, 76-77
SMTP - Reverse DNS blacklisting, 88-91
SMTP - Security, 77-79
SMTP - Sender Policy Framework (SPF), 86-88
SMTP - Smart host, 83
SMTP - White list, 85-86
SMTP Connector, 71
Synchronization - CalDAV, 122-123
Synchronization - General, 121-122
Synchronization - HTTPMail, 127-128
Synchronization WebDAV, 129
SyncML Protocol, 125
SyncML Synchronization Data, 126-127
Using SyncML, 125-126
Using the COM component, 129-131
Web administration, 99-100
Web Mail - General, 113-115
Web Mail - Logging, 116-117
Web Mail - Properties, 113
Web Mail - Spam, 115-116
Web Mail, 112-113
WebAdmin - Features settings, 100-101
WebAdmin - General settings, 100
Configuration repository location, 26
Configuration, 128-129
Configuring clients for HTTPMail, 159-160
Configuring Email Clients
  Configuring clients for HTTPMail, 159-160
  Configuring Email Clients, 157
  Enabling logging for Microsoft Outlook, 160
  Microsoft Outlook 2000, 157-158
  Microsoft Outlook 2002/2003, 158
  Microsoft Outlook 2007, 158
  Microsoft Outlook 2010, 158-159
  Microsoft Outlook Express, 157
  Mozilla Thunderbird, 159
  Netscape Messenger, 157
Configuring Email Clients, 157
Configuring redundant or backup (MX) mail servers, 164
Configuring the antivirus filter, 148-149
Configuring the server, 131
Configuring web mail Overview, 117
Connectors, 69
Delete messages, 41
Diagnosing Outlook/Outlook Express error codes, 178-179
DNS error codes and descriptions, 178
Domain - Blacklists, 43-44
Domain - DKIM (DomainKeys), 44-47
Domain - General, 42-43
Domain configuration, 42
Edit default message, 42
Email Delivery Flow, 15-16
Email users (all), 41
Email users (individual), 41
Enabling logging for Microsoft Outlook, 160
Enumerations requiring the CriteriaMet syntax, 144-145
Examples, 134
Export users, 40-41
File Storage, 120-121
Filter actions, 140-142
Filter Criteria, 137-140
Glossary, 185-186
Greylist Cleanup agent, 97
Group - General, 54-55
Group configuration, 53
How Internet Email Works, 10-11
How to access the Web Administration interface, 105-106
How to add a group member, 53-54
How to add the Web Administration interface to web sites within IIS, 104-105
How to create a domain, 42
How to create a Global Filter, 137
How to create a group, 53
How to create a list, 55
How to create a mailbox, 47
How to create a Post Office, 35-36
How to enable Advertising banners in web mail, 65
How to enable campaign management, 64-65
How to enable Message Filtering, 135
How to enable the Web Administration interface, 101-104
How to implement antivirus filtering, 147-148
How to import group members, 54
iCal and CalDav configuration, 124-125
IMAP - General, 106-108
IMAP - Logging, 108
IMAP Service, 106
Import users, 41
Import Windows users, 41
Importing list members, 59
Increasing 10000kb upload limit for Webmail, 182
Inspecting log files, 161
Installation and Upgrading
  Check and configure DNS settings, 29-30
  Check mail services, 30
  Configuration repository location, 26
  Installation Overview, 17
  Installation, 17-25
  MailEnable Diagnostic Utility, 27-29
  Replace configuration files, 26-27
  To set up PTR records under Microsoft's DNS Server, 30
  Upgrading an existing web mail installation, 25-26
  Upgrading, 25
Installation Overview, 17
Installation, 17-25
Integrated Mailbox Calendar, 123-124
Introduction
MailEnable Message Filter Properties, 135-136
Manual training, 153-154
Setting up auto-training Bayesian filtering, 149-150
Spam Protection, 136-137
Spam Training Utility, 154-156
Step 1: Set up auto-training for the filter, 150
Step 2: Collecting spam for auto-training, 150-151
Step 3: Collecting ham for auto-training, 151
Step 4: Create a global Bayesian filter, 151
Step 5: Testing the Bayesian filter, 151
Testing Antivirus Configuration, 149
Token Substitutions, 142-143
Message Tracking, 171-172
Messaging Manager - Administration, 32-33
Messaging Manager - Footers, 34-35
Messaging Manager - General, 32
Messaging Manager - Security, 33-34
Messaging Manager, 31-32
Microsoft Outlook 2000, 157-158
Microsoft Outlook 2002/2003, 158
Microsoft Outlook 2007, 158
Microsoft Outlook 2010, 158-159
Microsoft Outlook Express, 157
Mozilla Thunderbird, 159
MTA - Archiving, 68-69
MTA - General, 67-68
MTA Overview, 67
Netscape Messenger, 157
Operational procedures
  Backing up and restoring data, 161
  Inspecting log files, 161
  Licensing, 164-165
  Troubleshooting SMTP connectivity issues and analysing log files, 163-164
Option Files, 65-66
Overview
  Administration, 14-15
  Email Delivery Flow, 15-16
  Overview, 13
  Structure of MailEnable, 13-14
Overview of NTLM authentication, 176-177
Overview, 13
POP - Advanced, 110-111
POP - General, 109-110
POP - Logging, 111-112
POP Retrieval Connector, 69-70
POP service, 108-109
Post office - General, 36-37
Post office actions, 40
Post office configuration, 35
Post office connector - General, 94-95
Post office connector - Logging, 95-96
Post office connector, 93-94
Postoffice - Footers, 37-38
Postoffice - Quota, 38-39
Postoffice - Web admin, 39-40
Prerequisites, 9-10
Published Calendars, 123
Publishing via host headers or virtual directories, 117-119
Queue overview, 173
Real time protection, 176
Replace configuration files, 26-27
Scripted Filtering
   Advanced Script Example, 145-146
   Basic Script Example, 145
   Enumerations requiring the CriteriaMet syntax, 144-145
   Literal values, 143-144
   Scripted Filtering, 143
   Scripted Filtering, 143
Selecting an antivirus application, 174-176
Services, 96
Set quota, 41-42
Setting up auto-training Bayesian filtering, 149-150
SMTP - Advanced SMTP, 79-81
SMTP - Blocked addresses, 84-85
SMTP - Delivery, 81-83
SMTP - General, 71-73
SMTP - Greylisting, 91-92
SMTP - Inbound, 73-74
SMTP - IP Blocking, 92-93
SMTP - Logging, 83-84
SMTP - Outbound, 74-76
SMTP - Relay, 76-77
SMTP - Reverse DNS blacklisting, 88-91
SMTP - Security, 77-79
SMTP - Sender Policy Framework (SPF), 86-88
SMTP - Smart host, 83
SMTP - White list, 85-86
SMTP Connector, 71
Spam Protection, 136-137
Spam Training Utility, 154-156
Step 1: Set up auto-training for the filter, 150
Step 2: Collecting spam for auto-training, 150-151
Step 3: Collecting ham for auto-training, 151
Step 4: Create a global Bayesian filter, 151
<table>
<thead>
<tr>
<th>Step 5: Testing the Bayesian filter</th>
<th>151</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure of MailEnable</td>
<td>13-14</td>
</tr>
<tr>
<td>Synchronization - CalDAV</td>
<td>122-123</td>
</tr>
<tr>
<td>Synchronization - General</td>
<td>121-122</td>
</tr>
<tr>
<td>Synchronization - HTTPMail</td>
<td>127-128</td>
</tr>
<tr>
<td>Synchronization WebDAV</td>
<td>129</td>
</tr>
<tr>
<td>SyncML Protocol</td>
<td>125</td>
</tr>
<tr>
<td>SyncML Synchronization Data</td>
<td>126-127</td>
</tr>
<tr>
<td>System Tray Utility (METray)</td>
<td>166-168</td>
</tr>
<tr>
<td>System Utilities</td>
<td></td>
</tr>
<tr>
<td>Activity Monitor</td>
<td>168-169</td>
</tr>
<tr>
<td>Backup utility</td>
<td>172-173</td>
</tr>
<tr>
<td>Command Line Send Utility (MESend)</td>
<td>171</td>
</tr>
<tr>
<td>MEInstaller</td>
<td>169-171</td>
</tr>
<tr>
<td>Message Tracking</td>
<td>171-172</td>
</tr>
<tr>
<td>Queue overview</td>
<td>173</td>
</tr>
<tr>
<td>System Tray Utility (METray)</td>
<td>166-168</td>
</tr>
<tr>
<td>Testing Antivirus Configuration</td>
<td>149</td>
</tr>
<tr>
<td>To set up PTR records under</td>
<td>30</td>
</tr>
<tr>
<td>Microsoft's DNS Server</td>
<td></td>
</tr>
<tr>
<td>Token Substitutions</td>
<td>142-143</td>
</tr>
<tr>
<td>Troubleshooting SMTP connectivity</td>
<td>163-164</td>
</tr>
<tr>
<td>issues and analysing log files</td>
<td></td>
</tr>
<tr>
<td>Upgrading an existing web mail</td>
<td>25-26</td>
</tr>
<tr>
<td>installation</td>
<td></td>
</tr>
<tr>
<td>Upgrading</td>
<td>25</td>
</tr>
<tr>
<td>Using SyncML</td>
<td>125-126</td>
</tr>
<tr>
<td>Using the COM component</td>
<td>129-131</td>
</tr>
<tr>
<td>Using your own antivirus scanner</td>
<td>174</td>
</tr>
<tr>
<td>Warranty</td>
<td>187</td>
</tr>
<tr>
<td>Web administration</td>
<td>99-100</td>
</tr>
<tr>
<td>Web Mail - General</td>
<td>113-115</td>
</tr>
<tr>
<td>Web Mail - Logging</td>
<td>116-117</td>
</tr>
<tr>
<td>Web Mail - Properties</td>
<td>113</td>
</tr>
<tr>
<td>Web Mail - Spam</td>
<td>115-116</td>
</tr>
<tr>
<td>Web Mail</td>
<td>112-113</td>
</tr>
<tr>
<td>WebAdmin - Features settings</td>
<td>100-101</td>
</tr>
<tr>
<td>WebAdmin - General settings</td>
<td>100</td>
</tr>
<tr>
<td>What’s New in Version 7</td>
<td>11-12</td>
</tr>
</tbody>
</table>