Administrator's Manual

A highly scalable, open architecture, internet messaging system running on Windows and Linux platforms.

ISBN: **962-8137-43-3**
Document ID: **IEMS7ADMMAN002**
Date of Publication: **September, 2003**

Portions of this product are based on software developed by the following universities/organizations:

CGI script Copyright © 1997 by Eugene Kim (eekim@eekim.com). DiamondBase Copyright © 1993 by Darren Platt, Andrew Davison, Kevin Lentin of the Monash University Melbourne, Australia.

IMAPD Copyright © 1999 by Mark Crispin of the University of Washington (MRC@CAC.Washington.EDU).

LDAP support is based on software developed by the University of Michigan and its contributors.

SSLeay Copyright © 1995-1998 by Eric Young (eay@cryptsoft.com).

CONTENTS

PREFACE

This is the Internet Exchange Messaging Server (IEMS) version 7.1 Administrator Manual that comes along with your software. IEMS runs on Microsoft Windows platforms and most popular Linux distributions. As such, this Manual has been authored to help you configure, use and administer IEMS on your Linux or Windows machines.

This manual is but one part of the entire IEMS 7 documentation set. It is assumed the reader of this manual understands the concepts presented in the **Internet Exchange Messaging Server 7 Principles of Operations**, and that the software has already been successfully installed. The IEMS 7 documentation set is made up of the following volumes:

- Internet Exchange Messaging Server 7 Principles of Operations
- Internet Exchange Messaging Server 7 Site Planning Guide
- Internet Exchange Messaging Server 7 Installation Guide
- Internet Exchange Messaging Server 7 Administrator's Manual
- Internet Exchange Messaging Server 7 cc:Mail Connector
- Internet Exchange Messaging Server 7 Lotus Notes Connector
- Internet Exchange Messaging Server 7 User's Guide
- Internet Exchange Messaging Server 7 Programmer's Manual

All IEMS documentation can be found either on the IEMS 7 CDROM, or downloaded from the IMA web site (*http://www.ima.com/documents/*).

Each chapter in this manual provides an module overview, and then detailed information regarding the configuration and operation of each module. The manual is organized into the following chapters:

Chapter 1, *Introduction*
Chapter 2, *IEMS Server*
Chapter 3, *Message Transfer Agent*
Chapter 4, *Message Store*
Chapter 5, *Directory Services*
Chapter 6, *SMTP*
Chapter 7, *Domain Administration*
Chapter 8, *Distribution Lists*
Chapter 9, *Web Mail Client*
Chapter 10, *Troubleshooting and Error Handling*

Conventions Used In This Manual

The conventions used in this manual are designed to help you learn IEMS 6 easily and efficiently.

Directory Path (e.g. ***c:\IMACert.imc)*** are printed in italic, arial font.

File names (e.g. **Setup.exe**) are printed in bold, arial font.

Menu choices (drop-down or pull-down list, links, columns, parameters, fields) are presented in bold, arial black font (e.g. **Host Table filename**).

Button commands (e.g. **Add**) are presented in bold, italic, arial font.

Screen Page (e.g. **User Details page**) are put in quote.

Keyboard Keys are presented in this manner: **ENTER; DELETE**

Anything you are asked to type are presented in courier new font (e.g. ***jdoe@ima.com***).

CHAPTER 1

Introduction

Before configuring, you must start the Internet Exchange Messaging Server (IEMS). Please see "Running IEMS" in the **Internet Exchange Messaging Server 7 Installation Guide**. Once the main "Web Administration" page is displayed, click the ***System Administration*** button. A dialog box asking for the administrator's username and password appears. Enter the corresponding username and password in the text boxes provided. The default username created by the software installer is *administrator* and the default password is *system*. Both the username and password are case sensitive and should be typed in lower case. After entering the username and the password, click the OK button. The "System Administration" interface appears, allowing the system administrator to navigate all the components on a distributed system, manage, configure, and monitor the server from anywhere on the Internet.

The system administrator may change the default username and password. To do this, follow the steps below:

For Linux:

1. Open a root shell. Once the # prompt appears, type:

   ```
   htpasswd -c /etc/httpd/user.iems.administrator
   ```

2. Specify the administrator name for IEMS

3. Enter the administrator password

For Windows:

1. Go to C:*Program Files\IMA\IEMS 7\Apache\bin*

2. Run the program **htpasswd.exe** to change the password for the "administrator" account

3. After starting the **htpasswd.exe** program, it will bring up a window asking to enter a new password for "administrator". Enter the new password in the requested fields. This creates the file:

   C:\Program FIles\IMA\IEMS 7\Apache\bin\users

   which is used to store user/password names. Then copy the file "users" to the directory C:\Program Files\IMA\IEMS 7\Apache.

4. To change the name of the "administrator" account, simply edit the above mentioned "users" file and change the name "administrator" to a new name.

Spam Detection and Handling

Spam Filtering Overview

IEMS 7 introduces a new integrated Anti-Spam approach to message reception and delivery. The MTA Pass-Through technology employed by IEMS 7 allows end users (message store accounts), individual distribution list maintainers, and connector modules to define their own security profiles independent of the rest of the system. At the same time the messaging system administrator can still define an overall global security policy, where some anti-spam measures will be handled directly by the MTA (such as reliable DNS-BL identified traffic). Other measures which may be desired by part of the user community, such as DNS-BL's with known high false positive rates can then be passed through to the users for consultation on a case by case basis.

In most conventional messaging systems, security measures are employed on a system wide basis, making the choice of tools, such as DNS-BL's, critical. IEMS MTA Pass-Through technology changes this by allowing the administrator to be able to use many more countermeasures, enabling only those that have been proven to be universally effective at the MTA, or global level, and letting users pick and choose what additional measures they may or may not wish to apply to their individual message traffic.

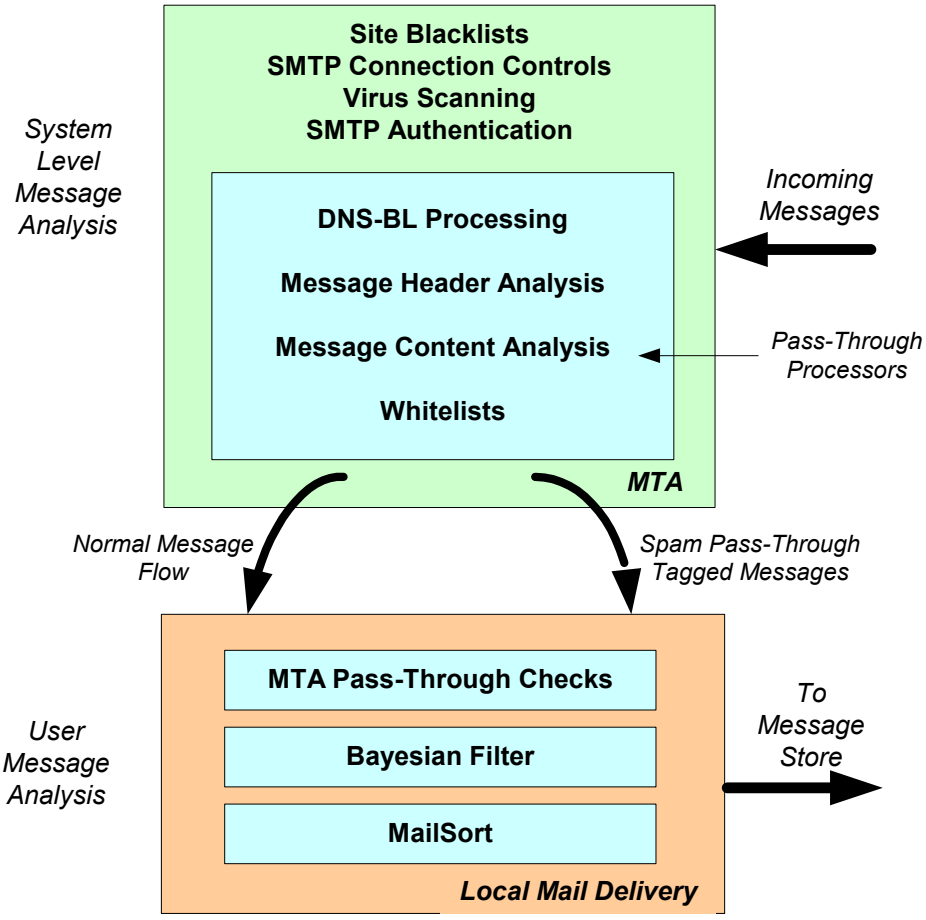

Figure 1: IEMS Pass-Through Architecture

System administrators are often caught in the middle of conflicting sets of requirements. On one hand, it is their responsibility to protect their organization and systems from outside (and sometimes inside) attacks from virus infected messages as well as spam. At the same time, they serve the users of these systems.

Traditional spam fighting techniques are performed by the MTA based upon policies set by the administrator. These global policies normally are set to ensure the maximum protection for the organization with minimal impact on the end user. In the case of spam detection and handling, the definition of what constitutes spam can vary widely from community to community, as well as from user to user within a single organization. Sales and marketing related messages may be very welcome in a sales group, while not being tolerated in a nearby engineering group. Advertisements pitching lower mortgage rates may be undesirable by most but a small group of people looking to purchase a new home. Viagra advertisements and other personal enhancement types of advertisements may not be at home for any users, especially if the site caters to the young or corporate users.

To assist the IEMS administrator in providing for both system security as well as keeping the collateral damage associated with improper spam detection and handling to an absolute minimum, several new tools can be applied. These can be applied on a system wide basis (global) and/or on an individual basis. Some tools such as virus scanning, certain SMTP connection controls, site-wide blacklists, and SMTP Authentication affect an entire site and are global in scope.

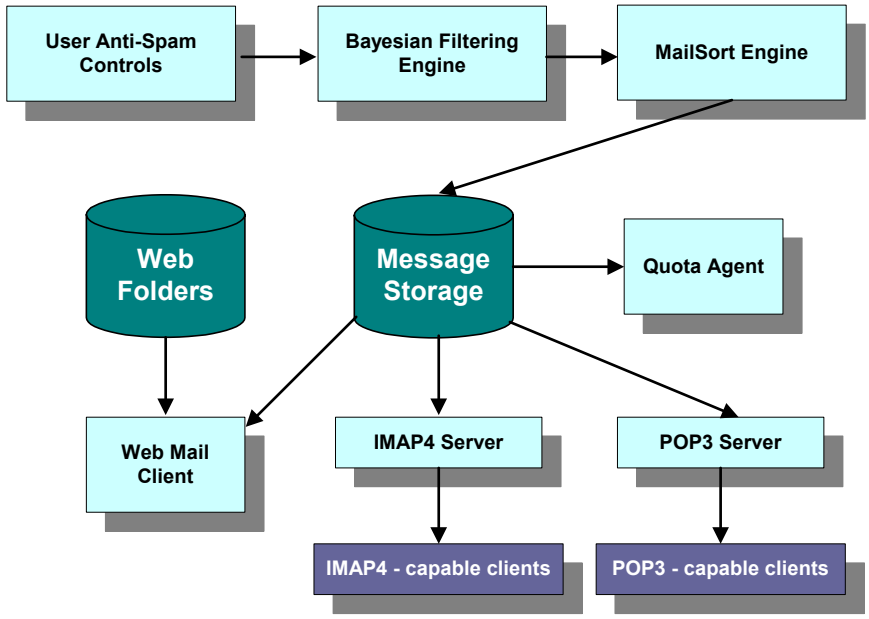

Figure 2: Local Mail Services

Others such as Bayesian Filtering and mail sorting based upon pattern matching are tools end users can apply. Other tools such as DNS Blacklists (DNS-BL), header analysis, and message content analysis occur within the MTA, however can be acted upon either as directed by a system security pol-

icy, or end user security policy. The ability for end users to be able to set security policies on actions normally only associated with system activities is made possible by the IEMS MTA Pass-Through features. These allow for the optional tagging of suspect messages by the MTA. The local mail delivery agent (working on behalf of the user) can then act upon these tagged messages later. This allows for both much more aggressive checking at the MTA level, as well as far more control of what messages are rejected at the user level (see Figure 1 above).

MTA Pass-Through

IEMS 7 Pass-Through technology allows the system administrator to be able to perform MTA level checks on messages, and then to optionally defer any action until being handled by an agent controlled by the end user. These agents are typically output channel processors, such as the Local Mail Delivery Agent, the Distribution List Processor, and others. As not all output channels are capable of handling deferred actions (such as the cc:Mail and Notes connector modules), the administrator can define default actions to be performed on a channel by channel basis, which will then be carried out by the preprocessor.

Local Services

Local services make up the modules and services not associated with message transport across the Internet (SMTP) or MTA switching. These include Distribution Lists, Message Storage and retrieval, user directed Anti-Spam measures, Web folders (storage), private address books, and Microsoft Outlook compatible calendaring / scheduling features. Messages are delivered into the local environment through the Distribution List manager and the Local Mail Delivery Agent (LMDA)

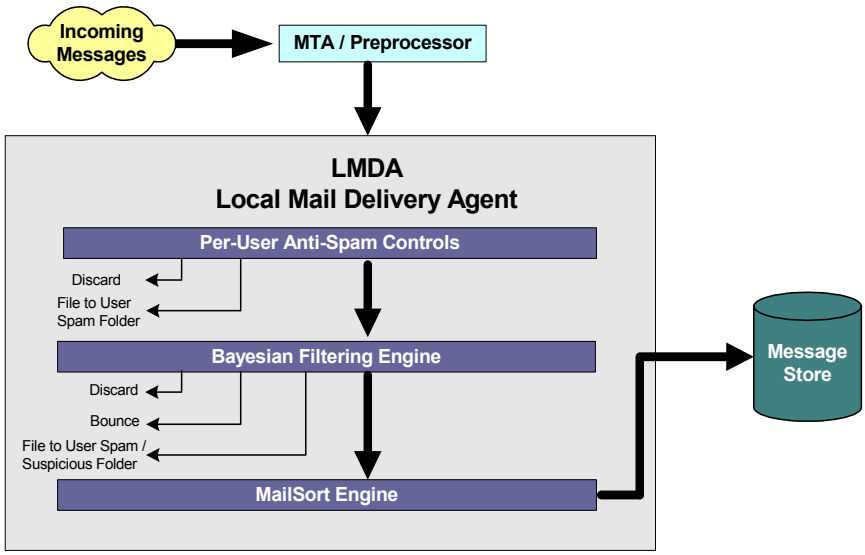

Figure 3: LMDA Architecture

The Local Mail Delivery Agent (LMDA) and the Distribution List Engine perform actions on behalf of their respective users (Message Store, and Distribution Lists). Both of these channel processors can be configured on a per DNS-BL basis as to what actions to perform. The LMDA components are shown in Figure 3. In addition to MTA Pass-Through processing, the LMDA can configured to perform Bayesian messaging filtering on behalf of the user. This filtering technique utilizes per-user message databases made up of user identified spam as the basis for its message blocking. Users, using either the Web Mail Client, or any IMAP client can place received SPAM into a special folder where the system can later process and update the individual Bayesian Filter databases. After an initial learning phase, accuracy rates for Bayesian filters can exceed 98%.

The combination of SMTP controls, Content Filters, Bayesian Filters, DNS-BL's, and the extension of these controls to the end users allows for an extremely flexible protection system, designed to block the maximum number of problem messages.

CHAPTER 2

IEMS Server

Overview

The Internet Exchange Messaging Server (IEMS) is made up of several different modules working together. These modules include the *Message Transfer Agent* (MTA), *Distribution List Manager*, *Message Store*, *Directory Server*, and others. IEMS modules are controlled (starting, stopping, monitoring) by the main server process, the *responder*. Messages are received by IEMS *Input Channels*, and delivered to the *Message Transfer Agent* (MTA). Messages are sent out of IEMS through IEMS *Output Channels*.

The *Message Transfer Agent* (MTA) is responsible for routing received messages to the intended recipients. Upon receiving a message, the MTA temporarily stores the message locally in a Shared Message Queue while analyzing the recipient's address through a directory look up in the Directory Services. The messages are further preprocessed by the Preprocessor Unit. The MTA's output channels will then route the message to the recipient's local address or forward the mail to another MTA.

The MTA features an innovative shared queuing strategy that enables the messaging server to handle large numbers of messages bound for different channels without experiencing bottlenecks common in messaging systems. It makes use of a number of input channels in receiving messages from the Internet or other messaging systems. This increases throughput considerably and enables organizations to send and receive timely information that may be critical to business success.

The MTA is composed of the following components: Input Channel, Output Channel, Preprocessor Unit and Shared Message Queue. Its key components include the MC (Monitor Control) Responder and the Dialup Scheduler.

Input Channels

A channel is a path through which messages flow. It makes use of a specific protocol to format and transfer messages. The MTA makes use of a number of input channels in receiving messages from the Internet or other messaging systems, like cc:Mail and Lotus Notes. These include:

- **LOCALOUT** - used by Local Mail Delivery Agent (LMDA) when forwarding messages via Mailsort
- **SMTPD** - for messages received from the Internet via SMTP
- **BSMTPIN** - for messages received via POP3 connection
- **CCOUT** - for messages received from the cc:Mail environment

- **NOTESOUT** - for messages received from the Notes environment

Note: *CCOUT and NOTESOUT export messages from the cc:Mail or Notes environment and input them into the MTA.*

- **DL**- for messages sent to a distribution list.

- **WEB MAIL CLIENT**- web-based user agent connecting users to the local Message Store

When messages from the Internet are received by the input channels, they are temporarily stored in the Input Queue after which they shall be fetched by the Preprocessor for further processing.

The following contains the list of input channels (see Figure 4 on page 16) together with their corresponding connectors. The connectors are used to associate several identifiers with the different channels. For the cc:Mail and Notes channels, their corresponding connectors can be optionally installed.

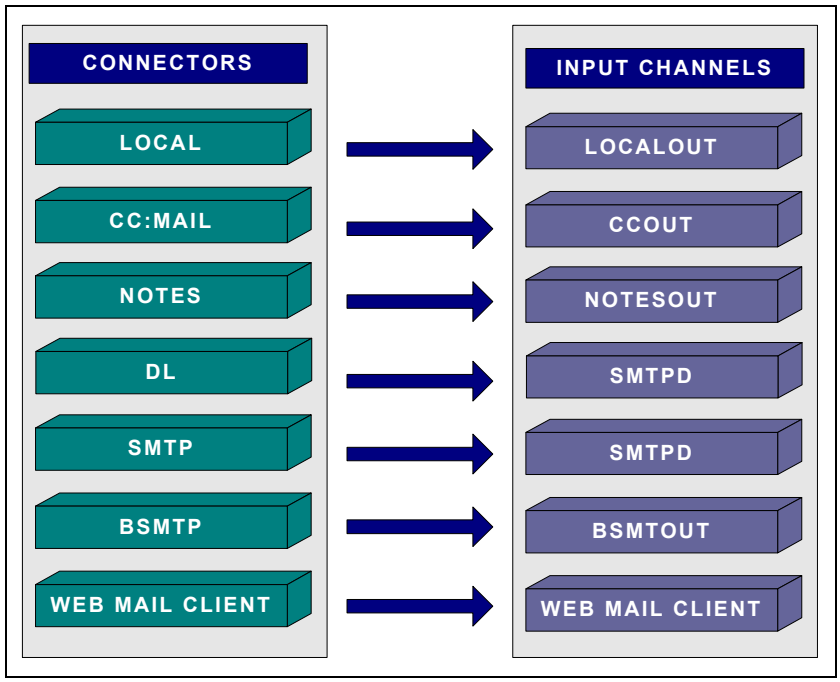

Figure 4: MTA Input Channels/Connectors

Output Channels

IEMS also makes use of a number of output channels in routing messages to the Internet or other messaging systems, such as cc:Mail and Lotus Notes. These are:

- **SMTPC** - sends messages to intended recipients over the Internet using SMTP.

- **BSMTPOUT** - sends messages to the intended recipients on the

other end of the BSMTP Tunnel with a POP3 account.

- **DL** - sends messages to intended distribution list members.
- **LOCAL** - delivers messages to local Message Store users.
- **CCIN** - delivers messages to the cc:Mail environment.
- **NOTESIN** - delivers messages to the Notes environment.

These channel processors are responsible for fetching messages from the MTA Shared Message Queue and sending them to their intended recipients.

The following contains the list of output channels (see Figure 5 on page 17) together with their corresponding connectors. The connectors are used to associate several identifiers with the different channels. For the cc:Mail and Notes channels, their corresponding connectors can be optionally installed.

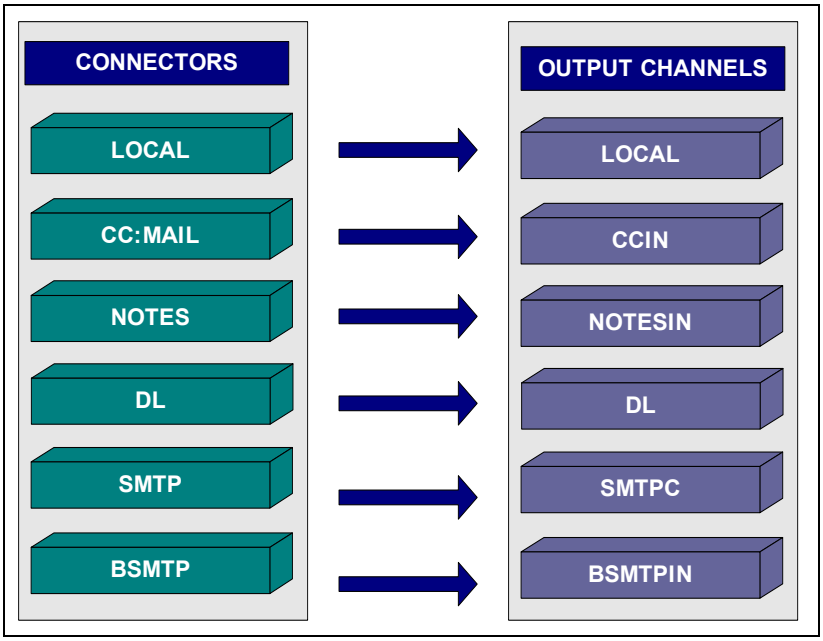

Figure 5: MTA Output Channels/Connectors

Preprocessor

Once messages are received by the MTA, the Preprocessor uses information provided by the Directory to determine proper routing. Once determined, the proper output channels associated with each recipient of a message is marked in the interim MTA message envelope. At this time, the Preprocessor may perform virus scanning, spam control and automatic disclaimer insertion, and other functions based upon how the preprocessor modules have been configured on each message.

The Preprocessor engine consists of the following modules: AntiVirus, SpamArchive, SpamDelete, SpamBounce, Attachment Removal, Loop Detection, TNEFExpansion and AutoInsertion. Each module has its own Channel Action Matrix, which defines all the possible input/output channel

combinations to perform a specific action (e.g. virus scanning) on messages that flow through the system.

MTA Shared Message Queue

After the Preprocessor processes the messages, the messages are temporarily stored in the MTA Shared Message Queue before they are delivered by the different input/output channels to their intended recipients.

MC Responder

The MC Responder allows the system administrator to monitor and control the status of various IEMS components. The system administrator can start or stop the Responder, thereby starting or stopping individual or all installed modules all at the same time. In a multisystem IEMS environment, the MC Responder is extremely useful in the monitoring and controlling of components across multiple machines.

The administrator may also activate certain options, such as the Auto Start, Auto Restart and Auto Stop for a specific component. The administrator may also define the Wait Time, which is the amount of time the MC Responder has to wait upon startup before running a given component. In addition, the web interface can be used to change the status of components from Stop to Running or vise-versa.

Dialup Scheduler (Windows versions only)

Having a dedicated Internet connection is ideal, however, in certain cases, it may be impossible or impractical to maintain a permanent Internet connection. In these cases, it is desirable to use a dial-up mechanism, which will establish a connection to an ISP (Internet Service Provider) at a particular time to download and upload messages to and from the Internet.

The MTA utilizes a RAS (Remote Access Service) dial-up mechanism. RAS is the service by which the Windows Operating System allows the local system to dial and connect to another peer over the Internet. The MTA initiates RAS through the Dialup Scheduler. The following functions are supported:

- Provides a user interface to enable the system administrator to configure dial-up schedules and other RAS connection-related information.
- Performs RAS dial up at the scheduled dial-up time.
- Performs RAS connection hang up at the scheduled hang-up time.

Server Configuration

To configure the IEMS main Server Configuration parameters, click the **Server Controls** link on the top menu frame. This action displays the "Server Controls" screen (see Figure 6 on page 19).

Figure 6: Server Controls

The system administrator needs to configure the main server parameters in order to properly send and/or receive messages from the Internet to the mailbox of the intended recipients. Server Controls define the Internet host names, Internet domains, message queue directories, log directories and logging level used by IEMS. These options determine how the messages will be routed and handled until they are delivered to the intended recipient's mailboxes. To configure the main server parameters, click on the *Configuration* button (see Figure 7 on page 20).

Local Internet host name
The Internet host name of the machine that runs the IEMS MTA. For example, if the FQDN is *mail.ima.com*, the local Internet host name would be *mail*.

Local Internet domain
The Internet domain name of the machine that runs the IEMS MTA. For example, if the FQDN is *mail.ima.com*, the local Internet domain is *ima.com*.

Queue directory
The directory where the MTA message queues reside. This includes the Shared Message Queue and the separate SMTP queues.

Temporary directory
The location of the IEMS temporary directory. The Notes connector, for example, uses this to write temporary files during message conversion process.

Log directory
The location of the IEMS log files directory. The log file IEMTA.LOG is written to this directory. You can set this directory to be a shared directory in the network so that you can read the file remotely on a user station. Doing so, however, may degrade the performance of the software as writing data via a network is generally slower than writing data directly to the local hard disk.

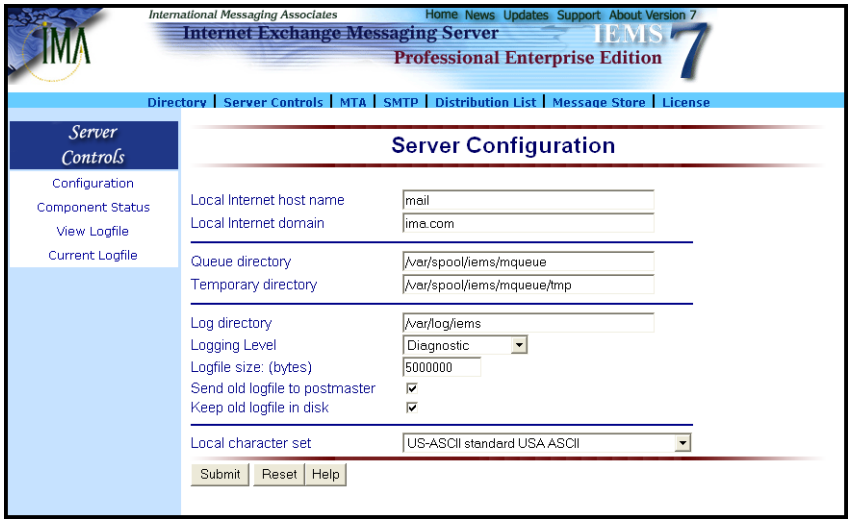

Figure 7: Server Configuration

Logging level

IEMS provides six levels of debugging:

- **Errors only**
  The minimum logging detail. An event is written to the log whenever an error condition occurs. An instance is when a connection attempt to a client or another server fails.

- **Message logging**
  Logs the information about the delivery of all messages.

- **SMTP session**
  All SMTP conversations are logged in this level. SMTP session logging is responsible for recording each incoming and outgoing SMTP command.

- **Diagnostic**
  The most verbose logging. Useful only for debugging purposes. Events are written to the log at individual steps within each process or task to pinpoint problems. It logs additional diagnostic data, including information concerning core operations. Be sure to disable diagnostic level logging after debugging, as the heavy disk activity can reduce system performance.

- **Warning**
  An event is written to the log whenever a warning condition occurs. An instance is when the server cannot understand a communication sent to it by a client.

- **Informational**
  An event is written to the log with every significant action that takes place. An instance is when a user successfully logs on or off or creates or renames a mailbox.

Logfile size
The largest logfile size permitted before it is saved in another name and a new log is started. The default limit is 500,000 bytes. Acceptable values range between 10,240 bytes (10KB) to 2,000,000,000 bytes (roughly 2GB). The default value of zero indicates no limit.

Send old log file to postmaster
This option causes old logfiles to be automatically mailed to the postmaster.

Keep old log files in disk
Prevents deletion of old log files. Storage of such files, however, uses up disk space very rapidly and the administrator should deal with them regularly.

Local character set
Allows a character set identifier to be tagged to all outgoing mail. For recipients in most Anglo-Saxon countries, US-ASCII should be used. Those in other countries, meanwhile, will have to choose a different ISO character set. For Japanese users, ISO-2022-JP should be used.

Component Status

The Responder allows the system administrator to monitor and control IEMS components. The system administrator can **Start** or **Stop** the Responder, which thereby starts or stops all the installed modules together. The administrator may also activate certain options, such as the **Auto Start**, **Auto Restart** and **Auto Stop** for a specific component. There is also a field where the user can define the **Wait Time**, which is the amount of time the MC Responder has to wait before running the component.

The Responder aims to provide simplified management tools and centralized control to monitor all the IEMS components in a distributed system through a web interface. The system administrator may stop or start the Responder remotely using any machine on the network.

To monitor and control the status of various IEMS components, click the ***Component Status*** button on the left menu frame. This action displays the host name location and the Responder's status.

The **Location** field displays the TCP/IP (Transmission Control Protocol/ Internet Protocol) host name of the machine running the IEMS components.

The **Responder Status** field displays the current status returned by the IEMS components (see Figure 8 on page 22).

An established RPC connection to the Responder module displays the Responder Status as **Running**. However, if the RPC connection is unavailable, the Responder module is shown as **Not Running**.

Note: *The Responder will not be able to retrieve the IEMS host name if the Directory Server is not running.*

When the system administrator clicks the ***Stop Responder*** button, an RPC command will signal the Responder to quit. The remote Responder then carries out the normal termination procedure and stops all the local modules that

are automatically enabled on the machine. Clicking the ***Show Details*** button will list all the IEMS modules located within the machine with their corresponding status (see Figure 9 on page 22). This allows the system administrator to modify the **Auto Start**, **Auto Restart**, **Auto Stop** and **Wait Time** value for any module controlled by the Responder. If the component is already running, a **Stop** button is displayed in the **Status** column. If the component is not running, a ***Start*** button is displayed in the **Status** column.

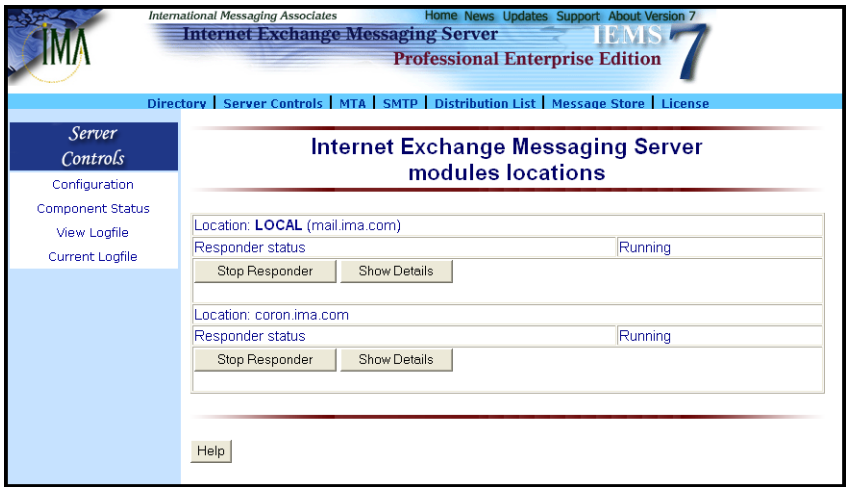

Figure 8: Component Status

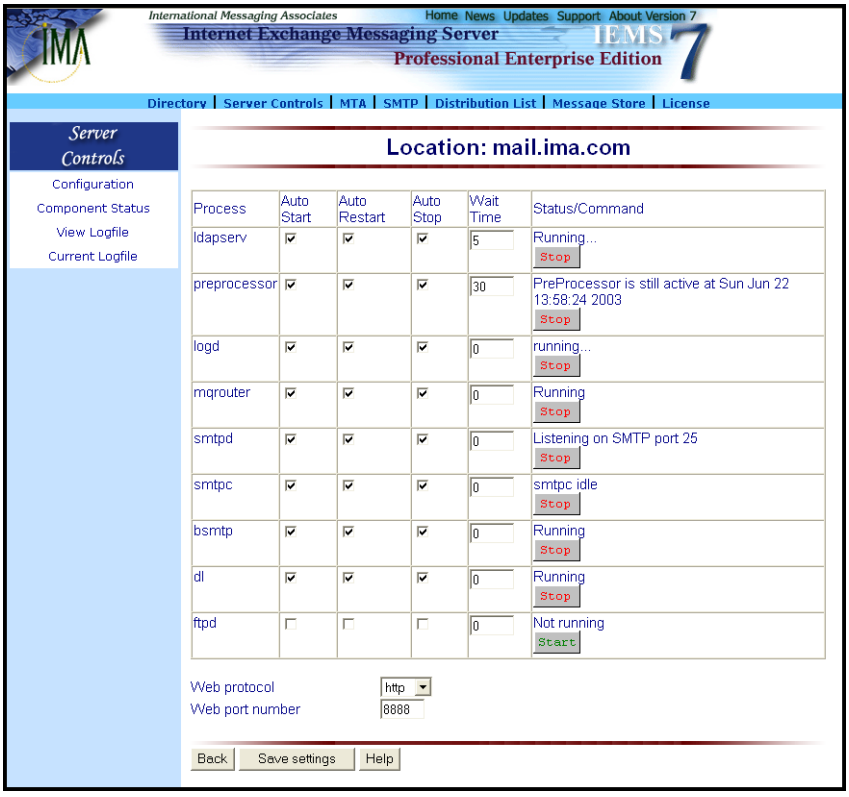

Figure 9: Responder

Log Files

Viewing Old Log Files

IEMS logs the transactions for each operation that have been carried out. An archive of the old log files can be viewed by clicking the ***View Logfile*** button. This action displays the “View Log File” screen (see Figure 10 on page 23). Select the log file from the list then, click the ***Submit*** button.

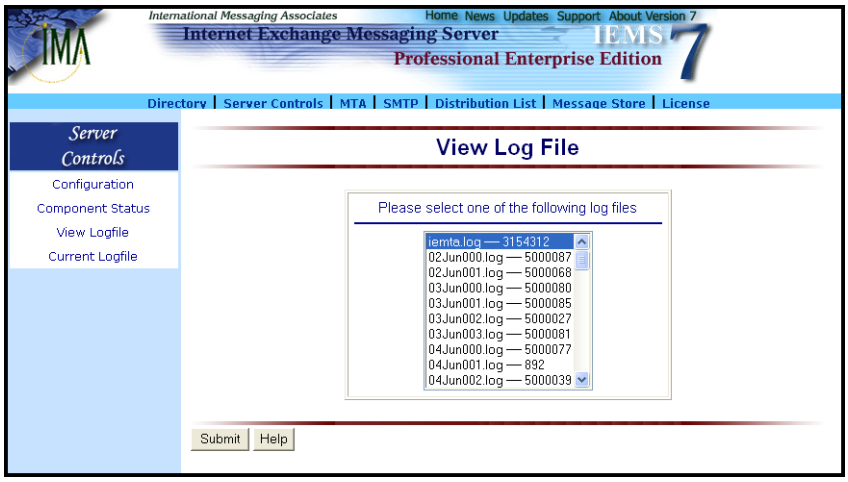

Figure 10: Viewing Old Log Files

Viewing Current Log File

To view the current log file, click the ***Current Logfile*** button on the left menu frame. This action displays the screen (see Figure 11 on page 23) that allows the system administrator to view the transactions for each operation that has been carried out recently.

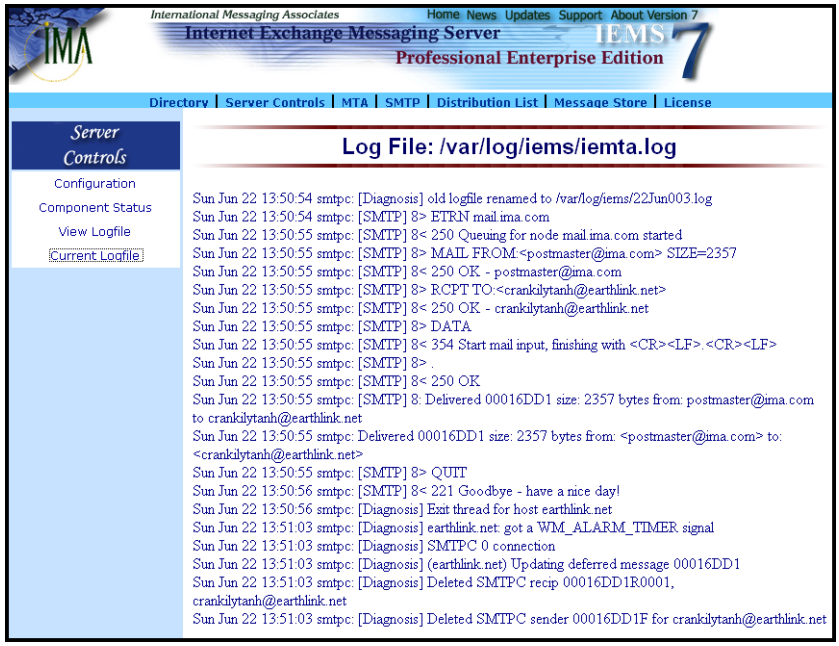

Figure 11: Viewing Current Log File

Dialup Scheduler (Windows)

The IEMS server utilizes a RAS (Remote Access Service) dial-up mechanism. RAS is the service by which the Windows Operating System allows the local system to dial and connect to another peer over the Internet. The MTA initiates RAS through the Dialup Scheduler that supports the following functions:

- provides a user interface to enable the system administrator to configure dial-up schedules and other RAS connection-related information.
- performs RAS dial up at the scheduled dial-up time
- performs RAS connection hang up at the scheduled hang-up time

Note: *This feature is available only on Windows platforms. Before configuring the Dialup Scheduler, the Windows system must be configured for the appropriate dial-up mechanism. For Windows 98 and Windows NT 4.0 platforms, go to Programs/Accessories/ Communications/Dial-Up Networking and Programs/ Accessories/Dial-Up Networking, respectively.*

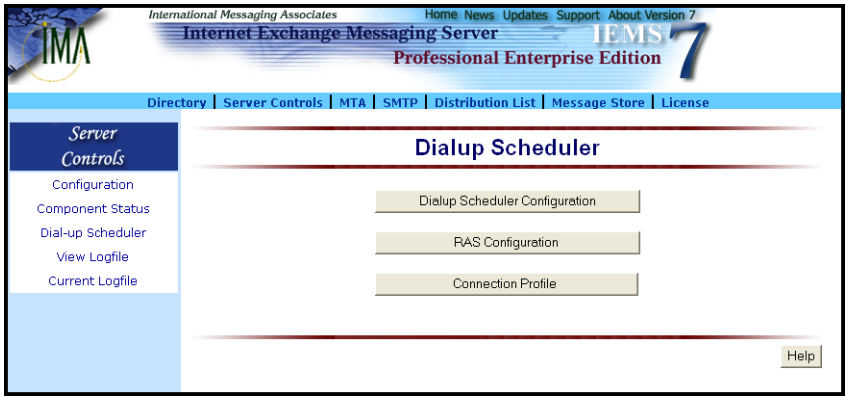

Figure 12: Dialup Scheduler

Setting The Periodic Schedule

To configure the Dialup Scheduler, click the Dialup Scheduler button on the left menu frame. This action displays the “Dialup Scheduler” screen (see Figure 13 on page 25). Click the *Dialup Scheduler Configuration* button. A new screen displaying the periodic scheduling option appears.

If periodic scheduling is enabled, the Dialup Scheduler is configured to perform periodic dial-up operations on every scheduled day.

Sun - Sat
Specifies the day(s) when the Dialup Scheduler should run. This indicates the days when the Dialup Scheduler will be executed from Sunday to Saturday.

Every
Refers to periodic dial-up schedules, with the period specified by the hour and the minute settings.

Start at/Stop at
Specifies the start time and the end time of the periodic dial-up schedule. Periodic dial-ups will be allowed within this time interval.

Only if mail queued
Tells the Dialup Scheduler to check if there are mail queued in the SMTPOUT channel before establishing a dial-up connection. If there are no mail in the queue, the Dialup Scheduler will not attempt to dial.

Automatic RAS Dialup and Hangup
Activating the Automatic RAS dial-up and hang-up option enable RAS support. With this function enabled, IEMS automatically starts a RAS connection during startup and terminates automatically when the system shuts down.

Modules to Start
The Dialup Scheduler will start the selected modules when performing dial-up connections.

Hang-up Time
Specifies the time (in minutes) the Dialup Scheduler waits for a dial-up connection to be established. If the dial-up connection fails, the Dialup Scheduler will re-dial automatically until the time-out value is reached.

Use different schedule on weekends
When enabled, specifies that a different dial-up schedule is to be used for the weekends (i.e., Saturdays and Sundays). The schedule for the weekends can be configured by clicking the Weekend Schedule button.

Whole Day
Configures the periodic dial-up schedule to remain active throughout the whole day.

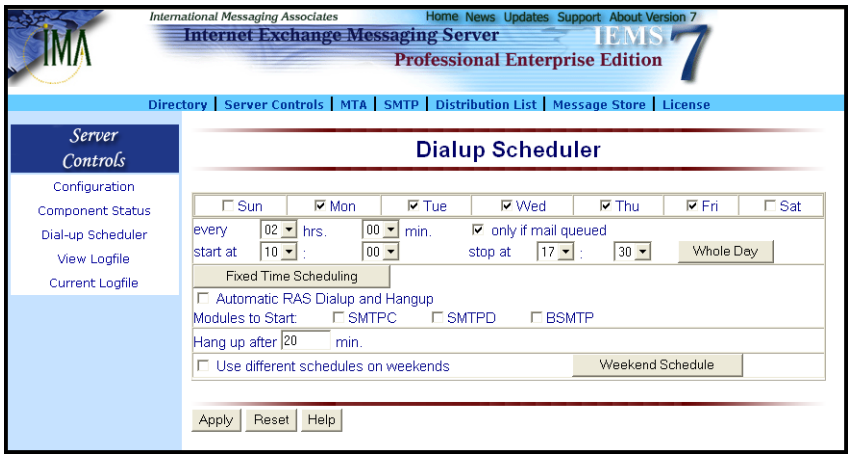

Figure 13: Setting The Periodic Schedule

NOTE: *Clicking the **Fixed Time Scheduling** button displays another screen where you can configure the fixed time scheduling option.*

Setting The Fixed Time Schedule

The system administrator can configure the Dialup Scheduler to perform only one dial-up session on every fixed scheduled day. To configure the fixed time scheduling, click the ***Fixed Time Scheduling*** button on the "Periodic Scheduling" screen (see Figure 14 on page 26). Provide information on the following fields:

Sun - Sat
Specifies the day(s) when the Dialup Scheduler should run. This indicates the days when the Dialup Scheduler will be executed from Sunday to Saturday.

at
Refers to fixed period specified by the hour and the minute settings that the Dialup Scheduler will run.

Automatic RAS Dialup and Hangup
Activating the Automatic RAS dial-up and hang-up option enable RAS support. With this function enabled, IEMS automatically starts a RAS connection during startup and terminates automatically when the system shuts down.

Modules to Start
The Dialup Scheduler will start the selected modules (SMTPC, SMTPD, BSMTP) when performing dial-up connections.

Hang-up Time
Specifies the time (in minutes) the Dialup Scheduler waits for a dial-up connection to be established. If the dial-up connection fails, the Dialup Scheduler will re-dial automatically until the time-out value is reached.

Use different schedule on weekends
This option, when enabled, specifies that a different dial-up schedule is to be used for the weekends (i.e., Saturdays and Sundays). The schedule for the weekends can be configured by clicking the ***Weekend Schedule*** button.

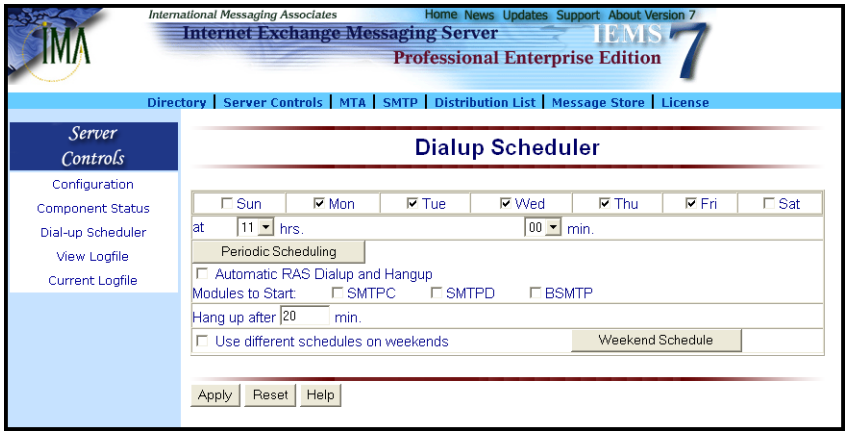

Figure 14: Setting The Fixed Time Schedule

Note: *Clicking the **Periodic Scheduling** button displays another screen where you can configure the periodic scheduling option.*

Setting The Weekend Schedule

The system administrator may specify a different dial-up schedule for the weekends by marking the check box beside **Use different schedule on weekends**. Click the ***Weekend Schedule*** button either on the "Fixed Time Scheduling" or "Periodic Scheduling" screen (see Figure 15 on page 27). Provide information for the following fields:

Every
Refers to periodic dial-up schedules, with the period specified by the hour and the minute settings.

Start at/Stop at
Specifies the start time and the end time of the periodic dial-up schedule. Periodic dial-ups will be allowed within this time interval.

Hang-up Time
Specifies the time (in minutes) the Dialup Scheduler waits for a dial-up connection to be established. If the dial-up connection fails, the Dialup Scheduler will re-dial automatically until the time-out value is reached.

Only if mail queued
This option is only valid for the periodic dial-up schedule.

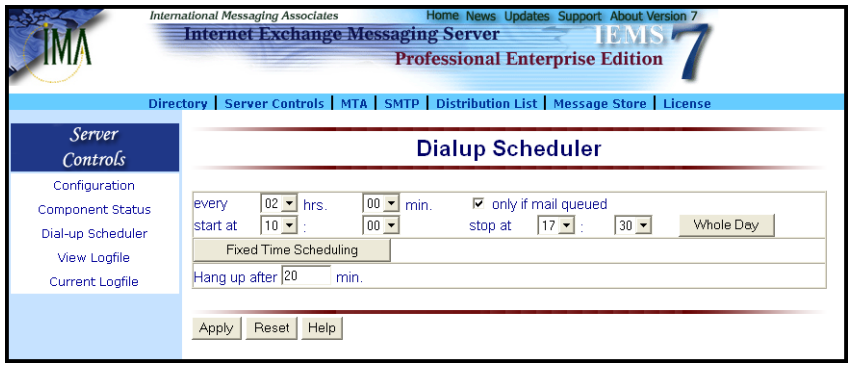

Figure 15: Setting The Weekend Schedule

RAS Configuration

Clicking the ***RAS Configuration*** button on the "Dialup Scheduler" screen (see Figure 16 on page 28) allows the system administrator to configure the RAS settings.

Phonebook
The first RAS Configuration entry, Phonebook, allows the administrator to specify the phone book entry to be used by for RAS connection. Use the ***Browse*** button to search through the file system for other phonebooks (files with the .PBK extension).

Phonebook entry selected
The Phonebook entry selected refers to the RAS profile name to be used. IEMS uses this RAS profile name for making a RAS connection during start-up.

Phonebook entries
Displays the first number to be tried during dial-ups. The phonebook contains several entries, which are tried by the Dialup Scheduler, based on their order in the phonebook.

Timeout after
Specifies the time-out value (in minutes). The Dialup Scheduler waits for a RAS dial-up connection to be established. If the RAS dial-up connection fails, the Dialup Scheduler will re-dial automatically until the time-out value is reached.

Figure 16: RAS Configuration

NOTE: *More than one phonebook can be chosen under Windows NT.*

Disabling ETRN Support

Clicking the ***Connection Profile*** button on the “Dialup Scheduler” screen enables the system administrator to configure the different aspects of the RAS connection and ETRN support. ETRN support specifies that the machine’s FQDN will be conveyed to all remote SMTP hosts when SMTPC is sending out mail to enable a remote queue run. The screen (see Figure 17 on page 29) displays the different “Connection Profile” parameters.

Send keep alive packets
Sends periodic data to the discard port of the remote system to keep the link active (typically used on PPP or some ISDN connections). Some TCP/IP stacks can be configured to time out and automatically disconnect after a predetermined period of zero network activity. Under this condition, it is necessary for the system to keep the stack active if SMTPD is to continue receiving incoming mail. This option enables SMTPD to keep sending alive packets to maintain the dial-up connection.

Run a program when connection is established
Allows the administrator to define the path of the program to be run after the connection is made.

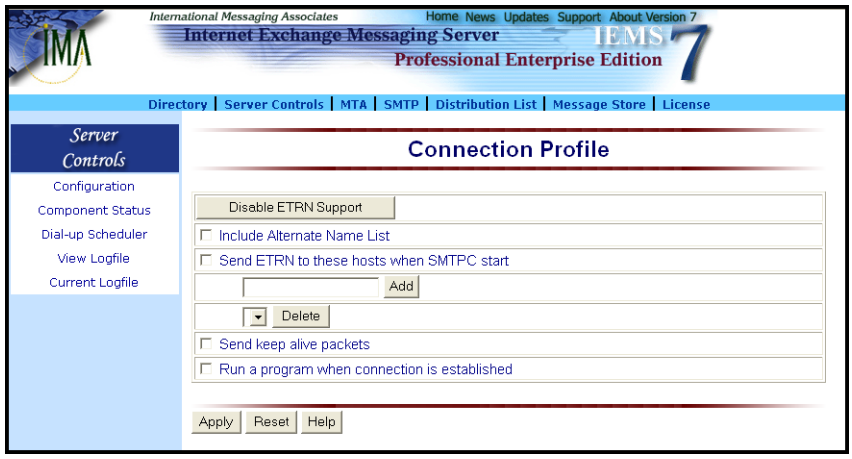

Figure 17: Disabling ETRN Support

Enabling ETRN Support

On the “Disabling ETRN Support” screen (see Figure 18 on page 29), click the ***Enable ETRN Support*** button. This action enables the ETRN Support. The screen displays the following parameters:

Include Alternate Name List
Used to send ETRN requests to alternate remote SMTP hosts.

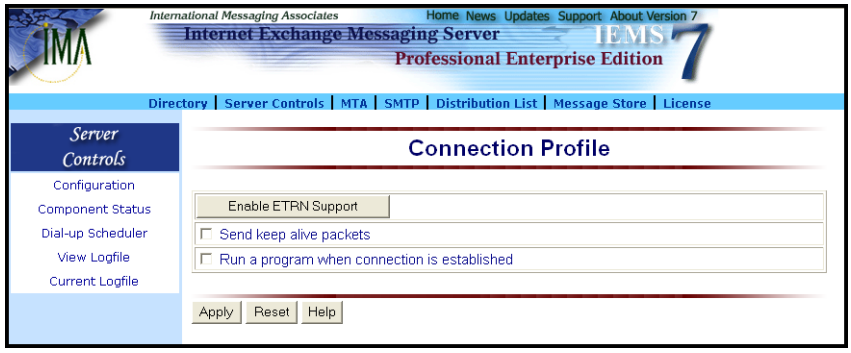

Figure 18: Enabling ETRN Support

Send ETRN to these hosts when SMTPC start
Used to enable sending an ETRN request only to a specific host, even if there is no currently queued outbound mail. This ensures that even though there is no outbound mail to that host when SMTPC runs, the host still receives ETRN requests. An option to add or delete host names is also available.

For **Send keep alive packets** and **Run a program when connection is established**, please refer to page 28.

Secure Web Access

To enable SSL access to your IEMS server, a server certificate / key pair must be obtained and installed. Then the Apache configuration needs to be updated to include SSL support. Procedures for accomplishing these tasks can be found in **Appendix C**.

After enabling SSL support in Apache, IEMS can be configured to support https through the responder configuration page (MTA Component Status -> Show Details). Both the protocol (http/https) and port number can be configured and set at the bottom of this page.

CHAPTER 3

Message Transfer Agent

Overview

The *Message Transfer Agent* (MTA) is a message switch responsible for routing received messages to the intended recipients. Upon receiving a message, the MTA temporarily stores the message locally in its Shared Message Queue. The recipient' addresses are then looked up using local Directory Services. Various other checks are then performed by the Preprocessor before handing the message off to one of the IEMS Output Channels. The output channels will then send the message to the recipient's local address or forward the mail to another MTA.

The MTA is composed of the following components: Input Channel, Output Channel, Preprocessor Unit and Shared Message Queue. The Preprocessor Unit is an integrated subsystem of the MTA that queries the local Directory Server to determine the proper channels/connectors to route messages to. It performs virus scanning, spam control and automatic disclaimer insertion. It can also decode TNEF (Transport Neutral Encapsulation Format) attachments properly.

Anti-Virus Module

The anti-virus plug-in module (see Figure 19 on page 32) is an integral part of the Preprocessor which decodes message attachments and invokes a third-party anti-virus program chosen and defined by the system administrator. The Preprocessor is capable of creating multiple threads for fast and reliable virus scanning. Once the anti-virus module detects a virus, it will bounce the mail, archive the mail to a predefined quarantine location/folder or delete the mail, depending on the configuration set by the system administrator.

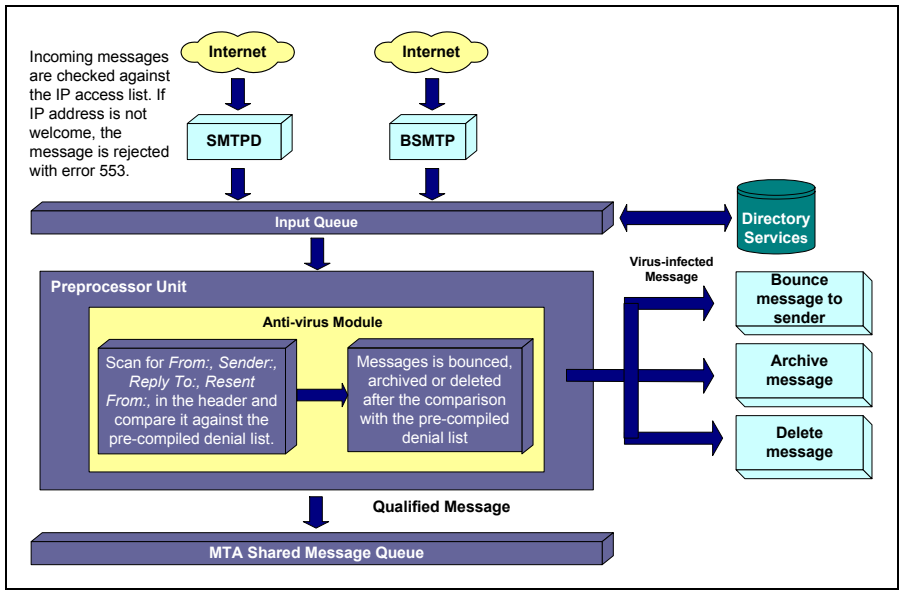

Figure 19: Virus Detection Process

The first step undertaken by the anti-virus module after receiving an email message is message attachment decoding. It makes use of decoding procedures that are based on the encoding methods applied in the attachment. The anti-virus module is capable of decoding and performing simultaneous virus scanning on MIME and non-MIME attachments. The anti-virus module supports the following encoding methods:

- BASE64
- Quoted-Printable
- 7bit
- 8bit
- UUENCODE
- BinHex
- AppleSingle
- AppleDouble
- Non-MIME encoded UUENCODE/Binhex
- Embedded UUENCODE/Binhex in MIME text item.

After decoding the attachment, the anti-virus module can invoke third-party anti-virus software. The anti-virus module has an open interface, which enables it to support multiple anti-virus packages. This feature enables the system administrator to use more than one anti-virus package thus, increasing the virus detection capability of the system. The Preprocessor anti-virus module supports the following anti-virus packages:

- ***McAfee VirusScan***
  This software supports the following platforms:DOS, Windows 95, Windows 98 and Windows NT.

- ***Sophos Sweep for Linux***
  This application has the capability to automatically eliminate common viruses and can easily be installed. It can be updated monthly with the latest anti-virus technology via the World Wide Web or via a CD or floppy disk.

- ***Sophos Anti-Virus for Windows 98***
  This application has the capability to automatically eliminate common viruses and can easily be installed. It can be updated monthly with the latest anti-virus technology via the World Wide Web or via a CD or floppy disk.

- ***Sophos for Windows NT***
  This application is specifically designed for the Windows NT platform and has the same features found in Sophos Anti-Virus for Windows 98. IEMS currently supports two types of Sophos anti-virus format: Sophos Anti-Virus Interface (SAVI.DLL) and Sophos Anti-Virus for Windows NT (SAVI.EXE).

- ***F-PROT Professional Anti-Virus Package***
  This is specifically designed to support Windows 95, Windows 98 and Windows NT 4.0 (Server/Workstation).

- ***F-Secure Anti-Virus***
  Available for both Windows (98/NT/ME) and Linux.

The anti-virus module can be run independently on a remote machine in a distributed environment via a RPC (Remote Procedure Call) mechanism. This feature is useful on a high traffic system where it is more desirable to run the anti-virus module on a dedicated remote machine, reducing CPU (Central Processing Unit) and file Input/Output loading on the Preprocessor system.

For more up to date information on anti-virus solutions supported by IEMS, check out the Anti-Virus Solution page at:

http://www.ima.com/solutions/avirus

Anti-Spam Module

The anti-spam module (see Figure 20 on page 35) is designed to form the first and second lines of defense against undesired email (spam). The last line of defense is made up of user filters and user directed Bayesian Filters invoked by the LMDA and DL Manager.

The first line of defenses consist of various SMTP connection controls, such as site and Internet wide blacklists. Second line defenses consist of MTA level message content analysis. These two lines of defense working together with IMA's MTA Pass-Through technology allow the administrator to define a spam security policy fully taking into consideration the needs of both the system as well as individual users.

Connection Controls

The anti-spam module enables the system administrator to create a list of banned or unwelcome IP addresses using a configurable GUI (Graphical User Interface). It is also capable of verifying the corresponding name of an IP address during the initial stage of the SMTP session using reverse DNS (Domain Name System) lookup to filter out forged names, blocking out potential spammers even before they can enter the system. The module has the ability to reject spam messages using SMTP error codes. The anti-spam module supports DNS based blacklists (DNS-BL's) for additional anti-spam protection.

Many Internet based DNS Blacklists exist, with providers coming and going all the time. One good source of information on different options is the Google summary found at *http://directory.google.com/Top/Computers/Internet/Abuse/Spam/Blacklists/*.

A few of the more well known lists include:

- MAPS-RBL (Mail Abuse Prevention System's Real-time Blackhole List - mail-abuse.org/rbl/)
- MAPS-DUL (Mail Abuse Prevention System's Dial-up User List - mail-abuse.org/dul/)
- Distributed Server Boycott List (dsbl.org)
- Open Relay Database (www.ordb.org)
- Spamhaus Block List (www.spamhaus.org/sbl)
- SpamCop (www.spamcop.net)

When choosing blacklists, it is important to know how each one determines who makes it on their list. Some, like the MAPS lists, tend to be pretty conservative and their false positive rates reasonably low. Others such as SpamCop and other take a more aggressive approach to listing, many times including entire ISP address blocks in an attempt to go after a single subscriber. In situations such as this the collateral damage associated with using these lists can be quite high. Several cases have been documented on the various spam related lists, including at *http://groups.yahoo.com/group/i_did_not_get_my_email/*.

If MTA Pass-Through is enabled, it is possible to determine on a per DNS-BL basis how connections are to be handled. For very reliable blacklists, the administrator may want to reject the mail directly at the SMTP session level. For lists which have high false-positive rates, he may want to pass these through to the user for them to determine how to apply the DNS-BL recommendations.

MTA Content Analysis

Messages that make it though the connection controls can optionally be analyzed for potential spam content. IEMS supports connection to the SpamAssassin filter (*http://www.spamassassin.org*), which can perform header and content analysis of messages based upon a local configuration. For messages that have been tagged by SpamAssassin as potential spam, the system can either immediately delete the message, or pass-through to the user for action.

Once a message has been detected and tagged as spam by the Preprocessor anti-spam module, any of the following actions can be applied:

- Archive the mail
- Delete the mail
- Bounce the mail to the sender
- Send the message on to the appropriate output channel

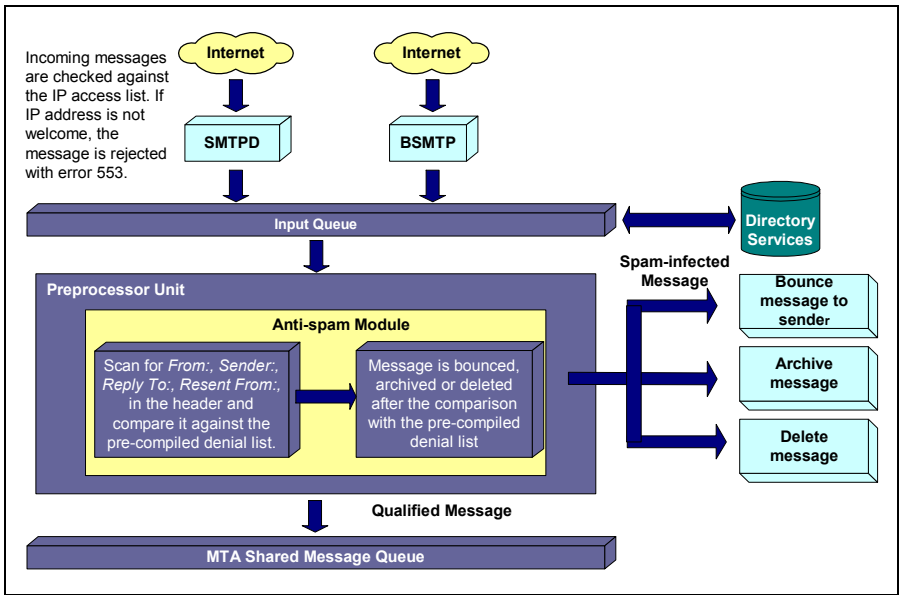

Figure 20: Detecting spam messages

Attachment Removal Filter

The attachment filter module allows for the automatic removal of configured attachment types as they flow through the system. Messages can be of either MIME or non-MIME types. This module supports filtering of mail attachments based upon the content type, filename, or a combination of both. When a message is encountered requiring attachment removal, the message may be bounced back to the sender, or silently forwarded (minus the attachment) to the intended recipient. Optionally, the postmaster can be notified on all messages that require filtering.

The attachment filter module is an important tool in the securing of the local messaging environment. With many viruses being transmitted as Visual Basic (VBS) or Windows PIF files, these and others can now easily be removed without having to rely on the latest anti-virus definition files.

Auto Text Insertion

The auto text insertion engine provides the capability to insert disclaimer messages into mail that passes through the MTA. Using this feature, messages created by the users will automatically include inserted disclaimer in messages passing through the MTA. This inserted message may state the confidentiality of the message in an attempt to limit the liability of the company that maintains the mail system. It may also state anything else the site

may wish to convey for messages passing through the system. The system administrator can add different messages based on the message source channel. It is possible for instance, for messages generated within the cc:Mail environment to have a different disclaimer from those that come from the Lotus Notes environment. The engine, which currently supports insertion into MIME and non-MIME message structures types, allows the system administrator to use a plain text file and/or a HTML file for the insertion process. The Preprocessor module invokes the auto text insertion engine based on the configuration in the Channel Action Matrix.

Channel Action Matrix

The Preprocessor engine consists of several filter modules. Each module has its own specific Channel Action Matrix, defining all possible input and output channel combinations where messages can flow. The system administrator may select from these modules which ones the Preprocessor should run for a particular message and exactly under what conditions it should run. After a specific Preprocessor module has been selected, the different channels and connectors in the Channel Action Matrix will run the specific Preprocessor module for the messages to be routed in the MTA. For example, the system administrator may want to run the anti-virus module and scan the messages coming from the Internet destined to the local Message Store. Another scenario would be, the system administrator would like his spam messages coming from the Web Mail Client and destined to the Internet to be deleted. The Channel Action Matrix's configurable GUI contains a table of all the input and output channels where the system administrator can select the proper channels and connectors to run the anti-virus module.

TNEF Expander

The TNEF Expander is a Preprocessor plug-in responsible for handling TNEF attachments. TNEF is a proprietary format used by the Microsoft Exchange and Outlook email clients when sending messages in RTF (Rich Text Format). Although TNEF attachments can effectively contain Word documents, Excel spreadsheets, video clips and programs, among others, only Microsoft mail products can properly recognize and read it. Most non-Microsoft email clients cannot translate TNEF blocks. Thus, whenever a TNEF-encoded message is received using a non-Microsoft email client, the TNEF part appears as a long sequence of hexadecimal digits either in the message itself or as an attached file (usually named WINMAIL.DAT).

The TNEF expander can extract TNEF attachments as early as the preprocessing phase and resubmits them again in a separate message to the original recipient. This means that when you retrieve your message with TNEF attachments, you will receive two messages. The first message will contain the original message, while the second message will contain the extracted attachments.

MTA Queue Management

An enhanced Queue Management utility is provided to view pending messages that have not yet been processed by the corresponding channel (DL, BSMTPOUT, Notes, cc:Mail, Local, SMTPC).

Pending messages may be sorted for a particular channel according to any of the following criteria: Priority, Sender and Size. The messages can also be searched according to the sender's address or recipient's address. When the sorting or searching criteria is specified, the queue management utility searches all the messages for the specified criteria. The results are displayed on a new page, which shows all the messages that matched the criteria. The system administrator may view the headers of the message, delete the message, bounce the message or reset the message queue.

A similar functionality is available for the Internet Post Office queue (cc:Mail) and the Notes SMTP.BOX queue. The queued messages are displayed for both the queues from where the end user can either delete the messages or bounce the messages.

Domain Forwarding

At times when it is necessary to catch all mail destined for a particular domain or sub-domain, and effect specific routing of messages, IEMS allows the system administrator to perform routing functions on a domain wide basis rather than specifying all email addresses for a domain. Domain forwarding allows the administrator to map all addresses within a domain to a specific channel. This mapping implements static routing between the defined domain and the corresponding channel. In addition to providing the mapping between a domain name and channel, an optional Channel Identifier can be specified depending upon the channel chosen. Examples are given below for use with various Output Channels (BSMTP, SMTP, CCMAIL/NOTES, DL/LOCAL).

BSMTP
When forwarding an entire domain's traffic through a BSMTP Tunnel, it is necessary to specify the remote address of the BSMTP Decoder or message repository where BSMTP messages are held. This is done through the specification of the remote address in the BSMTP Channel Identifier field. All messages received for the specified domain are then placed in the BSMTPOUT queue for later encoding and message routing.

SMTPC
When using SMTPC as the destination channel for Domain Forwarding, the Channel Identifier is not used. Instead all mail for the specified domain is immediately placed in the SMTPC output channel. This can be useful in situations when name resolution uses the local host table as a primary lookup. The domain selected can then be handled through the use of a custom entry in the local host table.

CCMAIL/NOTES
For domains which are handled by either the cc:Mail or Notes connectors, it is possible to explicitly route messages into these environments. The information provided in the Channel Identifier is then passed on to the appropriate connector module for routing within either the cc:Mail or Notes environments.

In the case of cc:Mail, this can be a cc:Mail user address, and for Notes, a Notes user address.

DL/LOCAL
Use of the DL or LOCAL channels for domain forwarding simply route the message for the domain to these channels in case there is no specific mapping for the user in the local directory.

Loop Detection

The loop detection feature enables the system administrator to configure how many times a message is allowed to pass through the system before being rejected. The system administrator may specify the maximum number of received lines that show the FQDN of the MTA machine allowed in an incoming message. Only lines containing the MTA FQDN are counted. If this number is exceeded, the message will be bounced. If the Looping Items To Postmaster option is set, any looping messages will be bounced to the local postmaster instead of being returned to the remote sender.

Alias Table

An alias is like a second identity for a user. You can create your mail alias in the “Directory Services” configuration page using a different email address. Let us say your original email address is *Bart_Simpson@ima.com* and your alias name is *Homer_Simpson@ima.com*. When a message is sent to *Homer_Simpson@ima.com*, the Preprocessor will route the message to *Bart_Simpson@ima.com*. The Preprocessor module maintains an internal database that holds all of the email aliases available in the directory. This database is used to reroute messages sent to aliases.

Queue Status

To configure the different Message Transfer Agent controls, click the **MTA** link on the top menu frame. This action displays the “Message Transfer Agent Controls” screen.

Figure 21: Message Transfer Agent Controls

IEMS uses a number of input and output channels. Input channels include: LOCALOUT, SMTPD, BSMTPIN, CCOUT, NOTESOUT, DL, WEB MAIL CLIENT. These channels are responsible for receiving messages from the Internet and other messaging systems, like cc:Mail and Notes Mail. Output channels include: SMTPC, BSMTPOUT, DL, LOCAL, CCIN and NOTESIN. These channel processors are responsible for fetching messages from the MTA Shared Message Queue and delivering them to their intended recipients.

The system administrator may view the number of pending messages on each channel by clicking the ***Queue Status*** button on the left menu frame. The “Queue Status List” screen (see Figure 22 on page 39) displays the different input and output channels with corresponding pending messages.

The **Queue Name** column contains Input queue and a number of output channels, which are listed in the file **queue.cfg**. These channels are created when the system is installed. All of the messages in these channels are listed in the status page as one entry.

The **# of Pending Message(s)** column displays the total number of pending messages in a specific channel.

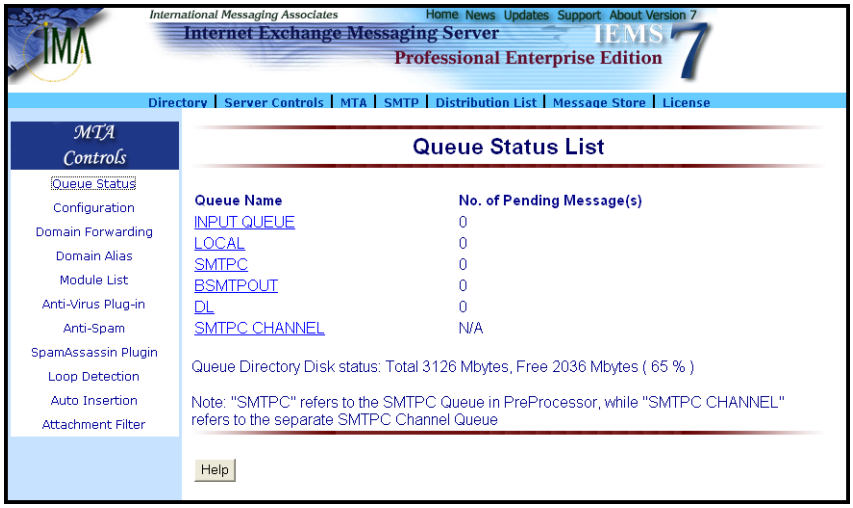

Figure 22: Viewing Queue Status

The system administrator may select a specific output channel (e.g. LOCAL) to view its details. Once a specific channel is selected, a new screen (see Figure 23 on page 40) displays the sender’s domain and the number of pending messages.

Figure 23: Viewing Individual Queue Contents

To read the messages of the particular domain, select the check box message. Choose from the pull-down menu the sorting criteria: **Priority**, **Sender** or **Size**. Click the ***Show Messages*** button.

Note: *The SMTPC subsystem uses its own queuing independent of the Preprocessor. Messages passing through the Preprocessor for the SMTPC Channel are placed into the Processor SMTPC Queue (labeled SMTPC here). The SMTPC Channel queue points to the SMTPC queue managed by the SMTPC subsystem.*

The system administrator may also search for a particular message using the **Sender's Address** or **Recipient's Address**. To search according to Sender's Address or Recipient's Address, enter the recipient or sender's address of the particular message and click the ***Search*** button.

Configuration

The administrator can define the different domains, default and Internet delivery channels, shared message queues and notification messages when performing the preprocessing of messages. These can be done by clicking the ***Configuration*** button on the left menu frame. This action displays the different Preprocessor parameters (see Figure 24 on page 41).

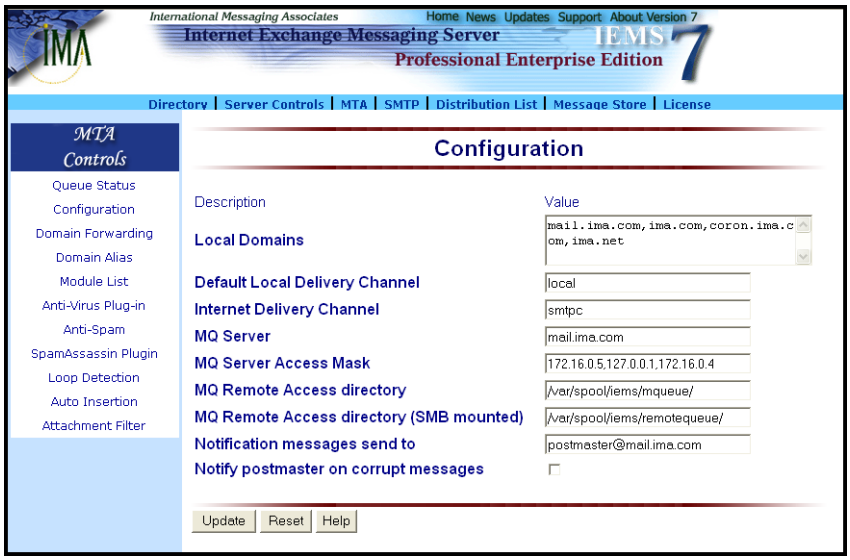

Figure 24: MTA Configuration

Local Domains
These are the Internet domain names recognized by IEMS as local. Local refers to the recipient's domain name that is listed in the local domain listing under the Preprocessor settings.

The MTA performs Directory lookups on all recipients to find out if they are local. If the domain name does not exist in the domain listing, the MTA will route the message to the default non-local channel, which is initially set to be the SMTPC, to complete the routing. Local domains refer to domains that the MTA takes responsibility for handling their messages. The MTA will either do the final delivery to the recipient or bounce the message if the message is undeliverable.

A domain name may begin with an asterisk (*) to denote all sub-domains, not including the main domain. For example, the entry **.ima.com* matches entries that are sub-domains of *ima.com* (e.g. *music.ima.com*). The MTA will accept the mail for all domains listed even if the recipient may not have an entry in the Directory. To configure the system to accept all mail for the primary domain plus all sub-domains, two entries are required (i.e., *ima.com* and **.ima.com*).

Default Local Delivery Channel
Defines the channel processor that will handle non-resolvable local recipients. If the MTA receives a message for a local recipient who does not have an entry in the Directory, the MTA will deliver the message to the default local delivery channel. If the recipient has an entry in the Directory, but does not have any connectors defined, the MTA will deliver the message to the default

local delivery channel. Example: *johndoe@ima.com* is local because *ima.com* is defined in the local domains list. If *johndoe@ima.com* does not have an entry in the Directory, the Preprocessor will route the message to the default local delivery channel, which can be LOCAL, cc:Mail or Notes. If the recipient address is not valid for the default channel, the message will be bounced.

At present, only Notes, cc:Mail and SMTPC connectors can process messages for recipients who do not have entries in the Directory. For the Notes and cc:Mail connectors, it is necessary to have the "unlimited user" license to enable the default mapping functionality.

Internet Delivery Channel
The channel used by the MTA to deliver a message to the Internet. Although the entry is configurable, IEMS is initially setup to make use of the SMTPC channel as the default Internet delivery channel. It is recommended not to change the default setting.

Message Queue Server
The NetBIOS (for Windows) or SMB (for Linux) name of the machine where the MQ (Message Queue) is located. The MQ Server can reside on any NetBIOS compatible host, but the entry should correspond to the NetBIOS name of this server. The NetBIOS name must be the same as the Internet host name. It is possible to configure Microsoft Windows to have two different names for NetBIOS and the Internet name, but this will not work for the system designated as the MQ Server.

Message Queue Server Access Mask
A list of IP addresses describing the systems which are permitted to access the Preprocessor queues. Each entry can either consist of a single dotted IP address (e.g. 192.55.89.10), a range of IP addresses (e.g. 192.55.89.10-192.55.89.12), or an IP address with a mask (e.g. 192.55.89.00/28). The Preprocessor will log an error in the system log file, without listing the IP address, if an application tries to access the channels.

Message Queue Local Directory
The directory path (e.g. *c:\Program Files\IMA\IEMS 7\MsgQueue* for Windows and */var/spool/iems/msqueue* for Linux) where the MQ databases and the sub-directories for the message files are installed. This directory is used by all connectors running on the same system.

Message Queue Remote Access Directory
The directory path (e.g. \\Station1\msqueue for Windows and */var/spool/iems/remotequeue/* for Linux) where the MQ can be accessed remotely. This directory is used by all connectors not running on the same system as the MQ Server. Example: If the MQ Server was running on a machine named Station1, a connector on machine named Station 2 could access the queued messages using this directory prefix.

The system will not operate correctly across a network if the entries MQ Local Directory and MQ Remote Access Directory are not pointing to the same directory. If all the connectors, Preprocessor and the MQ Server are running on the same system, this directory will not be used.

Message Queue Server Account Name (Windows only)
The account name (e.g. Account Name) used to access the MQ Server. It also serves as the authentication information to be able to access the MQ Remote Access Directory. If the remote connector cannot access the MQ Remote Access Directory, then the entry provided is not properly stored in the MQ databases. If this entry is not specified, the connector will use the credentials as previously configured on the current system to access the remote directory.

Message Queue Server Password (Windows only)
The password used for the MQ Server account name. The password must be at least four characters long. The password will appear as a row of asterisks (****) for security purposes.

Notification Messages Sent To
The email address of the person who will receive notification messages. Notify Postmaster on Corrupt Messages Provides the system administrator an option whether he would like to receive notification messages (mark the check box) on corrupted messages or not (leave the check box blank).

Click the ***Update*** button to change the current settings.

Domain Forwarding

Domain forwarding allows the administrator to map all addresses within a domain to a specific channel. This mapping implements static routing between the defined domain and the corresponding channel. In addition to providing the mapping between a domain name and channel, an optional Channel Identifier can be specified, depending upon the channel chosen. Examples are given below for use with various Output Channels (BSMTP, SMTPC, CCMAIL, NOTES, DL/ LOCAL).

BSMTP

When forwarding an entire domain's traffic through a BSMTP Tunnel, it is necessary to specify the remote address of the BSMTP Decoder or message repository where BSMTP messages are held. This is done through the specification of the remote address in the BSMTP Channel Identifier field. All messages received for the specified domain are then placed in the BSMTPOUT queue for later encoding and message routing.

For example, if the MTA *xyz.com* is performing forwarding on behalf of *abc.net*, it could set up domain forwarding as follows:

DOMAIN NAME	QUEUE SELECTION	CHANNEL IDENTIFIER
abc.net	BSMTPOUT	abc@xyz.com

The Channel Identifier address *abc@xyz.com* is used as the address of the remote BSMTP Decoder or mailbox used for later BSMTP downloading, using the POP3 Client/BSMTP Decoder. If a local Message Store account is used, then this will be the Internet email address of that mailbox. Once deliv-

ered back to the MTA, the Preprocessor will perform a lookup on this address, recognize it as local, and deliver accordingly. If the address is not local, but another address on the Internet (perhaps at a remote ISP for example), once received by the MTA, the Preprocessor will detect that the address is not local, and route via SMTPC for further delivery.

SMTPC

When using SMTPC as the destination channel for Domain Forwarding, the Channel Identifier is not used. Instead all mail for the specified domain is immediately placed in the SMTPC output channel. This can be useful in situations when name resolution uses the local host table as a primary lookup. The domain selected can then be handled through the use of a custom entry in the local host table.

For example, if the MTA *xyz.com* is performing forwarding on behalf of "abc.net", the setup might look like:

DOMAIN NAME	QUEUE SELECTION
abc.net	SMTPC

No Channel Identifier is used here, as it is not currently recognized by the SMTPC connector. Once in the SMTPC Queue, assuming the local host table is used as the first lookup option, the IP address of the host you wish to route all *abc.net* traffic to could be associated with *abc.net*, regardless of its real name. This will work fine as long as the host you are relaying *abc.net* traffic to is setup to handle such forwarding properly.

CCMAIL/NOTES

For domains, which are handled by either the cc:Mail or Notes connectors, it is possible to explicitly route messages into these environments. The information provided in the Channel Identifier is then passed on to the appropriate connector module for routing within either the cc:Mail or Notes environments. In the case of cc:Mail, this can be a cc:Mail user, and for Notes, a Notes user address.

For example, if we wish for forward all mail for the sales group with "Jade Corporation" through to cc:Mail, we might use an entry that looks like:

DOMAIN NAME	QUEUE SELECTION	CHANNEL IDENTIFIER
jade.net	CCMAIL	user@sales_post_office

DL/LOCAL

Use of the DL or LOCAL channels for domain forwarding simply route messages from the domain to these channels in case there is no specific mapping for the user in the local directory.

Domain Aliasing

Domain aliasing provides a one way name mapping between domain names for incoming messages. As an example, if *jade.net* is aliased to *ima.com*, and *bart@ima.com* is a valid message store account, mail addressed to *bart@jade.net* will be recognized as a valid email address and delivered to *bart@ima.com*. On the other hand, if there exists a message store account *homer@jade.net* but no equivalent *ima.com* account, messages sent to *homer@ima.com* will go undelivered. If homer has message store accounts on both ima.com and jade.net, messages will get delivered to the actual message store account to which they were addressed.

To establish a domain alias, click on the ***Domain Alias*** button in the main menu area. This brings up the “Domain Alias” page (see Figure 25).

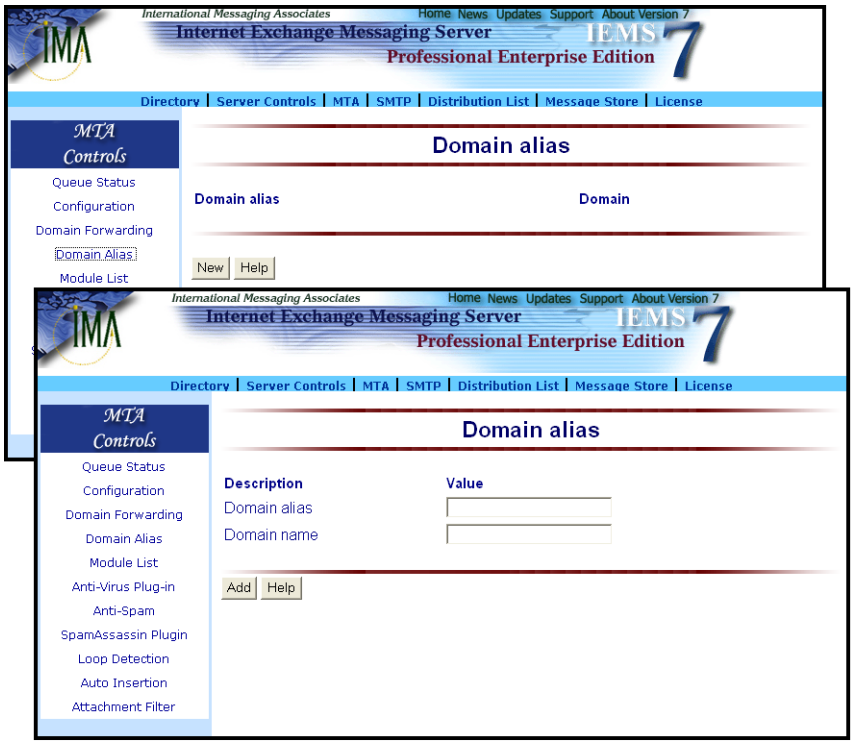

Figure 25: Domain Alias Configuration

This page allows you to create, view, update or delete domain alias entries. Once the main Domain Alias page is shown, click on the ***New*** button to create a new domain alias. The next page will then be displayed allowing you to enter the name mapping.

This page allows you to add or edit an existing domain alias entry. To add a new domain alias entry, perform the following:

- Enter the new alias name for the domain (e.g. *jade.net*) in the Domain alias field.
- Enter the domain name (e.g. *ima.com*) for the alias in the Domain name field.
- Click the ***Add*** button to save the new entry in the domain table.

To update a new domain alias entry, perform the following:

- Enter the new domain name (e.g. ima.com) for the alias in the Domain name field.
- Click the ***Update*** button to save the new entry in the domain table.
- To delete a domain alias entry, do the following:
- Click the ***Delete*** button to remove an entry from the domain table.

Module Lists

Clicking the ***Module List*** button on the left menu frame displays the different modules being run by the Preprocessor, such as the AntiVirus, Spam Archive, SpamDelete, SpamBounce, LoopDetection and AutoInsertion. This page also displays the full pathname of the module, version number and brief description of each module. Each module name is linked to its corresponding Channel Action Matrix (see Figure 26 on page 46).

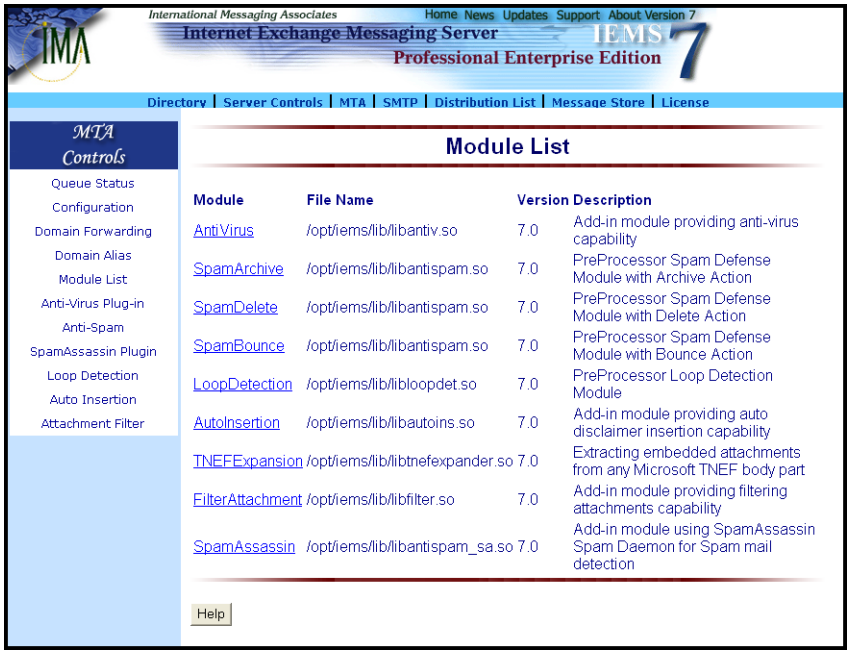

Figure 26: Module List Summary

Channel Action Matrix

Each module in the MTA uses a Channel Action Matrix for determining which combination of input and output channels will run a particular module for a message.

To configure the Channel Action Matrix for each module, click a specific module name from the “Module List” screen (see Figure 26 on page 46). A new screen displays the Channel Action Matrix for that module in table format (see below). The table lists the names of the input channels (i.e., LOCALOUT, SMTPD, BSMTPIN, DLOUT, WEBCLIENT) on the left-hand side, and the names of all the output channels (i.e., LOCAL, SMTPC, BSMTPOUT, DL) on the top. cc:Mail and Notes are also included if they are configured into the system.

Mark the check box of the corresponding entry in the Channel Action Matrix for each combination of input/output channels you wish the module to be applied to. A check mark indicates that the Preprocessor module will execute the specific function. In the example shown below (see Figure 27 on page 47), the anti-virus module will scan the messages coming from the Web Mail Client destined for local Message Store for possible viruses.

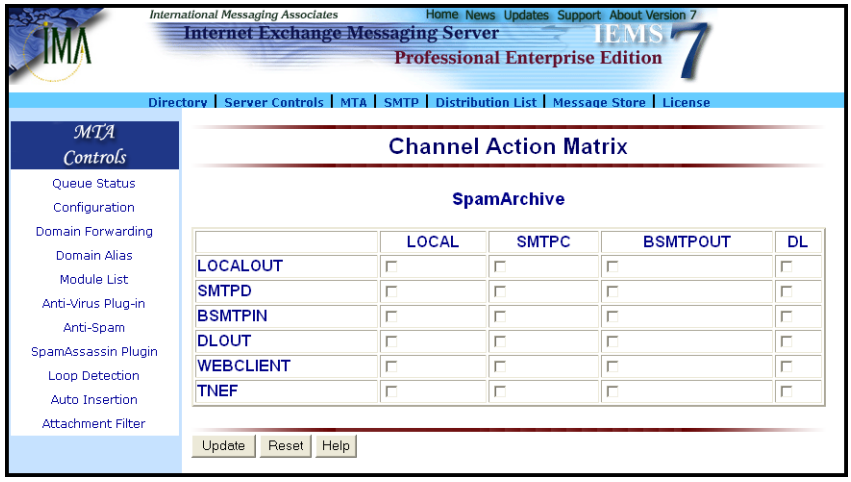

Figure 27: Channel Action Matrix Configuration

Anti-Virus Plug-In

The anti-virus module performs virus scanning on messages that enter the messaging server. The Preprocessor Unit is capable of creating multiple threads for speedy virus scanning. This module is highly configurable and provides the system administrator with several options in detecting and processing virus-infected messages. Such messages can either be bounced back to the sender, deleted or archived to a predefined location or folder.

The anti-virus module provides an open interface for the system administrator to choose their preferred anti-virus software to work with IEMS. Whenever the anti-virus module receives a message, it checks the Channel Action Matrix whether it should invoke a third party anti-virus package configured to run on the machine.

Creating Anti-Virus Profiles

To create a new profile, click the ***Configure Anti-Virus Plug-In*** button on the left menu frame. The “Available profile(s)” screen (see Figure 28 on page 48) appears. Click the New button. The “New profile” screen appears where the system administrator is required to provide information on the following fields:

Virus scanner type
The type of anti-virus software installed on the machine. For scanners that are invoked from the command line, select ***EXE***. For scanners that have an IEMS library interface, select ***DLL***.

Program path
This is the full path name of the directory or folder where the anti-virus software’s executable file resides.

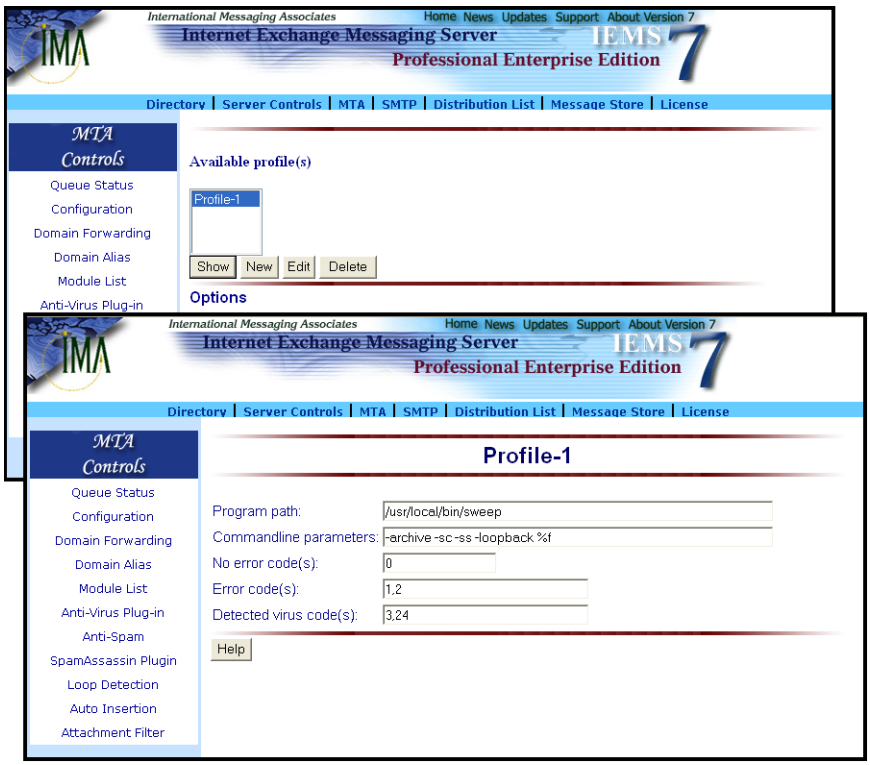

Figure 28: Anti-Virus Profile Creation

Command line parameters
The required and optional parameters that prompts the anti-virus module to substitute a temporary filename to that of the virus scanner. The required parameter, “%f”, is used to substitute for the temporary filename. No error code(s) indicates virus-free conditions.

Error code(s)
Indicates that scanning errors have occurred.

Detected virus code(s)
Indicates that a virus has been detected.
Click the ***Add*** button to install the new anti-virus profile.

In the example given in Figure 28, it is assumed that an anti-virus software package called “Sweep” from Sophos is installed on /usr/local/ bin, which is a command line driven virus scanner for Linux. On the program path entry, put the path and the name of the executable, which in this case is /usr/local/bin/sweep. Depending on the selected anti-virus software, put the proper command line parameters in the configuration. A special symbol “%f” is used for telling the anti-virus plug-in to pass the temporary file name to the selected anti-virus software.

Three sets of numbers may be returned by the selected anti-virus software. These three sets of number tell the anti-virus plug-in whether the attachment is clean (no virus infection), suspicious (error condition) or is infected by a known virus. If there are more than 1 possible values for any of these categories, use a comma to separate each of them. Or, use the symbols “>” (greater than), “<“ (smaller than) or (a range of) to define a number range. Please consult the antivirus manual for all the possible values returned by the software.

The following are the IEMS 7 anti-virus plug-in profile configuration values:

McAfee Viruscan
Program type: EXE
Program path: C:\Neta\scan\scan.exe (or the location where VirusScan is installed.)
Command line parameters: /ALL /ANALYZE /NOBEEP /NOBREAK /NOMEM /UNZIP %f
No error codes: 0
Error codes: 2, 6, 8, 15, 20, 102
Detected virus codes: 10, 13

Sophos Sweep for Linux (command line interface)
Program path: /usr/local/bin/sweep
Command line parameters: -archive %f
No error codes: 0
Error codes: 1, 2
Detected virus codes: 3

Sophos Sweep for Linux (SAVI API)
Program type: DLL
Program path: /usr/local/lib/libsavi.so.3
Command line parameters: *Not Required*
No error codes: *Not Required*
Error codes: *Not Required*
Detected virus codes: *Not Required*

Sophos for Windows 98
Program type: EXE
Program path: C:\Program files\SWEEP\SWEEP.EXE (or the location where your Sophos anti-virus software is installed.)
Command line parameters: NOT REQUIRED

No error codes: NOT REQUIRED
Error codes: NOT REQUIRED
Detected virus codes: NOT REQUIRED

Sophos SAVI
Program type: DLL
Program path: C:\Program files\Sophos SWEEP for NT (or the location your Sophos is installed.)
Command line parameters: NOT REQUIRED
No error codes: NOT REQUIRED
Error codes: NOT REQUIRED
Detected virus codes: NOT REQUIRED

Sophos for NT
Program type: EXE
Program path: C:\Program files\Sophos SWEEP for NT\SAV32CLI.EXE (or the location your Sophos is installed.)
Command line parameters: -Archive %f
No error codes: 0
Error codes: 1, 2
Detected virus codes: 3

F-PROT Professional Anti-Virus
Virus scanner type: EXE
Program Path: C:\F-prot\f-prot.exe
Command line parameters: /ARCHIVE /DUMB /NOBOOT /NOBREAK /NOMEM /PACKED /SILENT %f
No error codes: 0
Error codes: 1, 2, 5, 7, 8
Detected virus codes: 3, 4, 6

F-Secure Anti-Virus
Windows
Virus scanner type: EXE
Program Path: C:\Program Files\F-Secure\Anti-Virus\fsav.exe
Commandline parameters: /noboot /archive %f
No error code(s): 0
Error code(s):
Detected virus code(s): 23

Linux
Program Path: /usr/local/fsav/fsav
Commandline parameters: --archive %f
No error code(s): 0
Error code(s): 1,2,8
Detected virus code(s): 3

The table below summarizes the different anti-virus error codes:

IEMS Anti Virus Module Error Code	No error code(s)	Error code(s)	Detected Virus Code
McAfee VirusScan	0 - No errors occurred; no viruses were found	2 - Driver Integrity check failed 6 - General problem 8 - Could not find driver 15 - Viruscan self-check failed; it maybe infected or damaged 20 - Scanning prevented due to the FREQUENCY switch	10 - A virus was found in memory 13 - One or more viruses or hostile objects were found
McAffee		102 - User quit via ESC-X, ^C or Exit button. This can be disabled with INNOBREAK command-line option	
Sophos Sweep	0 - No error are or encountered	1 - If the user interrupts the execution by pressing the ESC key 2 - If some error preventing further execution is	3 - If viruses or virus fragments are discovered

Table 1: Anti-Virus Error Codes

IEMS Anti Virus Module Error Code	No error code(s)	Error code(s)	Detected Virus Code
F-FROT	0 - Normal exit: nothing found	1 - Abnormal termination -infection unrecoverable. This can mean any of the following: -internal error in the program -DOS version prior to 3.0 was used -ENGLISH.TXO, SIGN.DEF corrupted or not present 2 - Self-test failed -program has been modified 5 - Program terminated with ^C or ESC 6 - A virus was removed 7 - Insufficient memory to run the program 8 - At least one suspicious files was found; but no infections.	3 - A Boot/File 4-Virus Found

Table 1: Anti-Virus Error Codes

IEMS Anti Virus Module Error Code	No error code(s)	Error code(s)	Detected Virus Code
F-FROT	0 - Normal exit: nothing found	1 - Abnormal termination -infection unrecoverable. This can mean any of the following: -internal error in the program -DOS version prior to 3.0 was used -ENGLISH.TXO, SIGN.DEF corrupted or not present 2 - Self-test failed -program has been modified 5 - Program terminated with ^C or ESC 6 - A virus was removed 7 - Insufficient memory to run the program 8 - At least one suspicious files was found; but no infections.	3 - A Boot/File 4-Virus Found

Table 1: Anti-Virus Error Codes

The “Available profile(s)” screen (see Figure 28 on page 48) presents several options on what to do with the infected mail.

Action on infected mail messages
The necessary action to be taken on infected messages. This enables the system administrator to determine what to do with virus-infected messages. Such messages may be deleted, bounced to the sender, or archived.

Action on suspicious mail messages
The anti-virus module can either delete, bounce to the sender, or archive the messages that are suspected to be virus-infected.

Send notification to Postmaster
If enabled, the anti-virus module will notify the postmaster whenever messages are bounced, deleted, or archived by the anti-virus module as configured by the system administrator.

Send notification to sender
If enabled, the anti-virus module will notify the sender whenever messages are bounced, deleted, or archived by the anti-virus module as configured by the system administrator.

Save the settings by clicking the ***Save Options*** button

Note: *The anti-virus plug-in allows the system administrator to utilize more than one anti-virus software at the same time. This increases the virus detection capability of your system as some of the latest viruses cannot be detected by just one anti-virus package.*

Viewing Anti-Virus Profiles

The system administrator can view the existing anti-virus profiles. To view the profile, click the ***Configure Anti-Virus Plug-in*** button. This displays the "Available Profile(s)" screen (see Figure 28 on page 48). Select a particular anti-virus profile and click the ***Show*** button.

Editing Anti-Virus Profiles

After creating the anti-virus profile, the system administrator may edit the different attributes. To edit, select an existing anti-virus profile on the "Available Profile(s)" screen (see Figure 28 on page 48) and click the ***Edit*** button. This displays a screen for modifying the attributes of the profile. Please see "Anti-Virus Plug-In" on page 47.

Click the ***Save*** button to store the new settings.

Deleting Anti-Virus Profiles

The system administrator can delete existing anti-virus profiles. This will remove the profile from the list of anti-virus software used when performing virus scanning.

On the "Available Profile(s)" screen (see Figure 28 on page 48), select a particular anti-virus profile. Click the ***Delete*** button.

Anti-Spam

The anti-spam module within the MTA provides the system administrator with options to control the reception of unwanted messages. It also provides control on what sites can use IEMS as a mail relay.

To activate the MTA anti-spam capabilities, select the ***Anti-Spam*** button. This action displays the “Anti-Spam Configuration” screen (see Figure 29 on page 55).

The anti-spam configuration is presented in a two-column table. The left column contains the Spammer Address/Domain Restriction parameters, while the right column contains the IP Address Access Control parameters.

Spammer Address/Domain Restriction

MAIL FROM during SMTP connection
If enabled, SMTPD will scan for known/configured address or domains during the “MAIL FROM” SMTP command; and will return a 553 error (terminating the transaction) to the remote host if a match is found.

From
Scans addresses and domains in the From header.

Reply-To
Scans addresses and domains in the Reply-to header.

Resent from
Scans addresses and domains in the Resent-from header.

Sender
Scans addresses and domains in the Sender header.

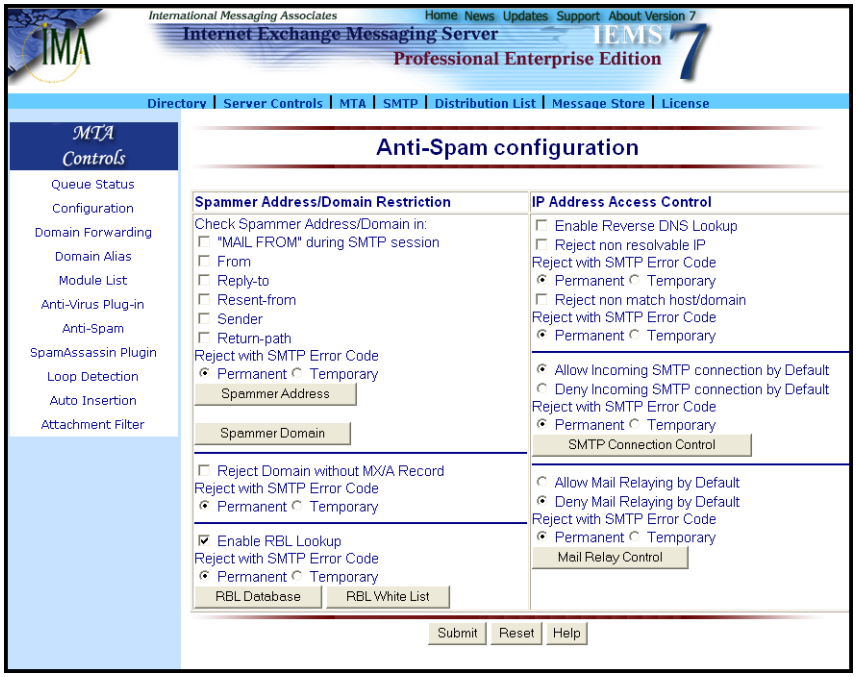

Figure 29: Anti-Spam Configuration

Return-path
Scans addresses and domains in the **Return-path** header.

Reject Domain without MX/A Record
If enabled, SMTPD rejects the connection if there is no MX or A record defined in the DNS for the sender's domain. This can be useful in stopping spammers who are masquerading behind invalid email addresses.

Enable RBL Lookup
SMTPD will try to find and match IP addresses of remote sites against network databases of known spammers. These databases consists of lists of IP addresses that are known to send spam mail, be friendly to spammers, and/or totally open to mail relaying. If this option is enabled, the anti-spam module will have additional spam mail detection capabilities.

Before using any DNS-BL databases, make sure you understand how they gather their information, and how accurate it is. Many DNS-BL databases tend to be overly aggressive, and as a result have a tendency to list sites that are not really spam related, but who ended up in the list anyway. When this happens, the chances of rejecting valid email are high.

Reject with SMTP Error Code
The anti-spam module also allows the system administrator to specify whether to reject spam messages with a Permanent or Temporary *SMTP Error Code*. If the Permanent radio button is selected, the messages will be rejected by SMTPD with a Permanent SMTP error code, and will usually be bounced back to the original sender by the peer MTA. On the other hand, if the **Temporary** radio button is selected, the messages will be rejected by SMTPD with a Temporary SMTP error code and will usually be queued up and retried by the peer MTA later.

Adding and Deleting Spammer Addresses

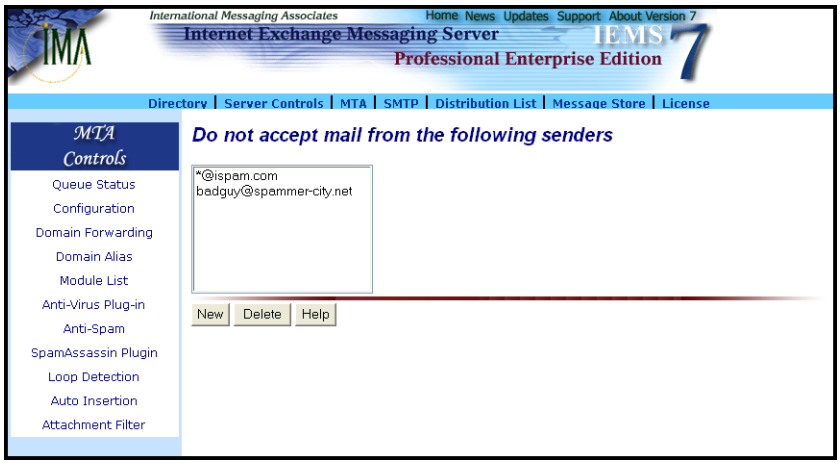

Figure 30: Adding and Deleting Spammer Addresses

The ***Spammer Address*** button as shown in Figure 29, once clicked, enables the system administrator to add, delete email addresses of potential spammers.

To add an email address to the list, click the ***New*** button. A new screen for adding spammer addresses (see Figure 30 on page 57) appears. Enter the email address of the spammer on the blank field and click the ***Add*** button.

To delete an email address from the list, select that particular address and click the ***Delete*** button.

Peer Domain Configuration

IEMS regularly communicates with Internet hosts that possess different capabilities, particularly with regards to email formats.

A peer is defined as a remote host or domain name. In the case of a domain, the scope of a particular peer definition includes the peer domain name as well as all names and sub-domains of that peer. Peer definitions are processed from the most specific to the most general. A peer definition for the sub-domain of a previously defined domain will take precedence over the more general definition. This means that a peer is a remote host or domain that requires encoding rules or send/receive permissions different from the default specified for the system. It is useful when dealing with remote companies or organizations that are still running pre-MIME software and are unable to effectively deal with MIME attachments. It can also be used to restrict email access in one or both directions to/from specific remote sites, to set limits on inbound and outbound message sizes, and set the default attachment types that a remote host is able to handle.

As an example, let us say you want to configure the mail encoding for a company called “XYZ Corp” with a domain name of *xyz.org*. Most of the users in this company are still running pre-MIME software and prefer to receive non-MIME encoded messages. One group however, the engineering group, is

running MIME compliant software. If the engineering group creates their own sub-domain, say *engr.xyz.org*, then you can setup two peer definitions for "XYZ Corp".

The first peer definition will define how you want to encode mail for everyone except the Engineering group. You do this by defining a peer *xyz.org*, and specifying non-MIME encoding for this domain. Then, setup a second peer for *engr.xyz.org*, where you specify MIME-compatible encodings. This has the effect of sending MIME messages to the "Engineering Department" within "XYZ Corp" while at the same time sending non-MIME messages to everyone else within the organization.

Hierarchical peer definitions can be added without limit, producing any combination desired. Peer definitions do not have to be associated with domains as in the above example either. The remote peer can be a machine or system name, providing configurability all the way down to the individual host level.

The peer domain profile contains a list of peers for which certain capabilities apply. These capabilities apply to a specific domain and all its sub-domains.

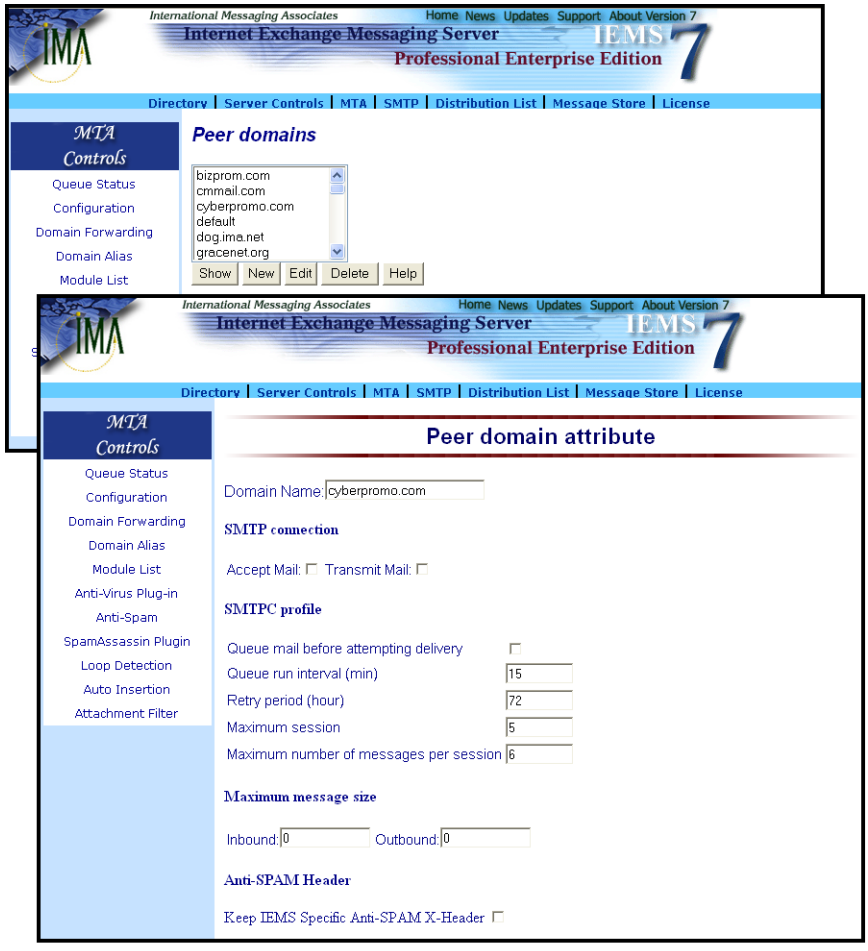

Figure 31: Adding, Editing and Deleting Peer Domains

The ***Spammer Domain*** button (see Figure 30 on page 57), once clicked, enables the system administrator to add, edit and delete peer domain attributes. The front end of the interface lists all the domain names stored in the database. A special entry called "`default`" is added when the database file is being initialized by the system (see Figure 31 on page 58). This entry cannot be removed from the database.

To add a spammer domain, click the ***New*** button on the "Peer domains" screen (see Figure 31 on page 58). A "Peer domain attribute" screen for creating a peer domain and configuring its various options appears.

Peer Domain Attributes

Domain Name
The domain or sub-domain that has the specified capabilities.

SMTP Connection

Accept Mail
If IEMS is not allowed to receive mail from a remote host, SMTPD rejects a HELO/EHLO command from that host with the following response:

550 host sales.xyz.org is not authorized to connect to iegate.jade.net

The default value is Yes. For peers that are known spammers, select **No** here.

Transmit Mail
If IEMS is not allowed to transmit mail to a remote site, CCOUT/NOTESOUT will bounce any messages destined for that host back to the original cc:Mail/Notes sender. The default value is Yes.

SMTPC Profile

Queue mail before attempting delivery
When this option is set to ON, all outgoing messages for this domain will be queued first, i.e., placed in the SMTPC deferred queue, and they will then be processed together at the queue run for this domain. This makes use of the overall system resource more efficient.

For dial-up connected ETRN hosts/domains, it is suggested to queue mail first before any delivery attempt, until an ETRN request is received or the queue run time of its domain arrived. When this option is OFF, all outgoing messages will be attempted first and will be queued if the attempt fails. This is suitable for those domains that require immediate delivery. The default is OFF.

Queue run interval (in minutes)
Determines how long the SMTPC should actively start a new Deferred Queue Processor to process the deferred messages for this domain. For those ETRN hosts, it is suggested to have a longer queue run interval (e.g. 1 day), as the queue run for the ETRN host will be triggered by the ETRN command once the ETRN host is connected. The default is 15 minutes.

Retry period (in hours)
Determines how long SMTPC should keep retrying the deferred messages for this domain. When it expires, SMTPC will bounce the messages to the sender. The default is 72 hours (3 days).

Maximum sessions
The maximum number of simultaneous outbound SMTP connections can be established for this domain. The default is 5.

Maximum number of messages per session
The highest number of messages that can be sent using a single SMTP connection. When this number is increased, more messages can be sent to a remote SMTP server per connection. The default is 6. Maximum Message Size The largest message size, in bytes, that can be sent to and received from the selected domain. The smallest size allowed is 8,192 bytes (8K). A value of zero indicates no limit.

Maximum Message Size

Inbound
If the Inbound message size exceeds this limit, SMTPD will reject the mail during SMTP session. The default is 0 (i.e., no limit).

Outbound
If the Outbound message size exceeds this limit, CCIN/NOTESIN will bounce the message back to the original sender. The default is 0 (i.e., no limit).

Anti-SPAM Header

Keep IEMS Specific Anti-SPAM X-Header
Normally when messages are sent via SMTP to another MTA, any internal MTA Pass-Through information is stripped from the message before sending. In some cases however this may not be desired. If you are running multiple IEMS machines with Pass-Through capabilities, this information can be retained across MTA's. Situations where this may be desirable include DNS-BL checking and message content checking on a firewall MTA. In this case, the downstream MTA needs to be defined as a peer domain, with this option enabled.

Outbound Attachment Option

Convert non-MAC file to MAC format
When enabled, converts all non-Apple attachments to Apple format by adding a header and an empty resource fork and encoding the attachments using the Apple encoding method specified below. This option is useful when IEMS is communicating primarily with a network of Macintosh computers.

Convert MAC file to non-MAC format
When enabled, strips all Apple attachments of their headers and resource fork, allowing non-Macintosh sites to access the information easily.

Generate non-MIME mail message
When activated, ensures that no MIME messages are generated for this peer. This is useful when communicating with older email systems that do not understand MIME. In this case, either UUENCODE or BinHex 4.0 is used to encode binary attachments; if the peer does not contain any Macintosh recipients, it is advisable to select UUENCODE encoding.

Send encapsulated NotesMail as file attachment
Attaches the native Lotus Notes.NSF to the message as well as the message text and the attachments (if any). This is only useful if the recipient is also a Lotus Notes user. If the remote Internet recipients are also using IEMS Lotus Notes connectors, this option can be used to set up a "Virtual Intranet" Notes network via Internet Exchange. This option is used only by the Notes Connector.

Native Attachment Encoding

MIME
Specifies that non-Apple attachments are to be encoded using the MIME standard.

UUENCODE
Specifies that non-Apple attachments are to be encoded using the older UUENCODE format.

Apple Attachment Encoding

MAC MIME AppleSingle
Specifies that outgoing Macintosh attachments are to be encoded using the MAC MIME AppleSingle standard.

MAC MIME DoubleSingle
Specifies that outgoing Macintosh attachments are to be encoded using the MAC MIME DoubleSingle standard.

MAC MIME Binhex
Specifies that outgoing Macintosh attachments are to be encoded using the BinHex 4.0 standard.

UUEncode AppleSingle
Specifies that outgoing Macintosh attachments are to be encoded using the AppleSingle standard via UUENCODE instead of MAC MIME.

Base64 MAC Binary II
Encodes MAC Binary II attachments using the base-64 encoding scheme. This option is not used by the cc:Mail connectors. If this is selected, CCOUT uses MAC MIME AppleSingle instead.

UUENcode MAC Binary II
Encodes MAC Binary II attachments with UNIX-style x-uue Content-Transfer-Encoding. This option is used only by the Notes Connector. If this is selected, CCOUT uses MAC MIME AppleSingle instead.

Note: *Outbound Attachment Option, Native Attachment Option, and Attachment Option are only used by the cc:Mail/Notes connector modules.*

After configuring all the parameters, click the Add button. To edit an existing peer domain, select an entry from the list box. Click the ***Edit*** button. A screen for modifying the peer domain's various options appears (see Figure 31 on page 58).

To delete an existing peer domain, select an entry from the list box and click the ***Delete*** button.

To view an existing peer domain, select an entry from the list box. Click the ***Show*** button. A new screen for modifying the peer domain's various attributes appears.

DNS-BL Access

Several databases accessible to the public exist on the Internet that contain lists of hosts or machines that are friendly to spammers in one way or another. IEMS can be configured to consult with any number of these databases, as long as they conform to the access methods first proposed by the MAPS RBL list.

The MAPS RBL list was the first widely used database containing a list of known sites friendly to spammers. The database is configured as a special DNS zone, and accessed the same way as any other normal DNS server would be. When an SMTP connection is established to SMTPD, the IP address of the connecting site will be used as the basis of a DNS lookup. The octets that make up the connecting machines IP address in its dotted-quad form are reversed and the DNS zone of the DNS-BL is appended. A DNS query is then made to search for an Address (A) record of the constructed name. If an address record is discovered, the connecting host is considered to be listed in the database, and appropriate action can be taken. In the case of IEMS, any successful lookups will result in the denial of SMTP access for the remote host.

Assuming we have received an SMTP connection from the address 192.168.39.5, and we are using the DNS-BL database, the address below will be used as the basis of a DNS Address record lookup:

5.39.168.192.blackholes.mail-abuse.org

If an Address record exists, then a positive match is obtained. If MTA Pass-Through is enabled, the connection is either dropped or message accepted depending on the policy for each DNS-BL. If MTA Pass-Through is not available (Standard Enterprise Edition and Free 3-User), the connection is dropped on a positive match.

Adding or Deleting an DNS-BL Database

The ***RBL Database*** button as shown in Figure 32, once clicked, enables the system administrator to add and delete list of databases used to match the IP addresses of potential spammers. Each database in the list contains blacklisted IP addresses (see Figure 32 on page 63). If MTA Pass-Through is available, additional fields are present to indicate if Pass-Through should be enabled for a given DNS-BL, and what the default action should be.

To add an DNS-BL database file to the list, click the New button. Enter the new DNS-BL zone to be added. If MTA Pass-Through is available, then two additional fields are present. If you wish to enable Pass-Through, select this field. If the message should be discarded with no Pass-Through, select *Discard* as the *Default Action*.

Note: *Only two combinations have meaning: Enable Pass-Through / Ignore, and Disable Pass-Through and Discard. In future releases these will be replaced by simple radio buttons.*

When through entering new DNS-BL information click the ***Add*** button. The new DNS-BL zone will now be supported by the anti-spam module .

To delete any of the DNS-BL database files from the list, select that particular database file and click the ***Delete*** button.

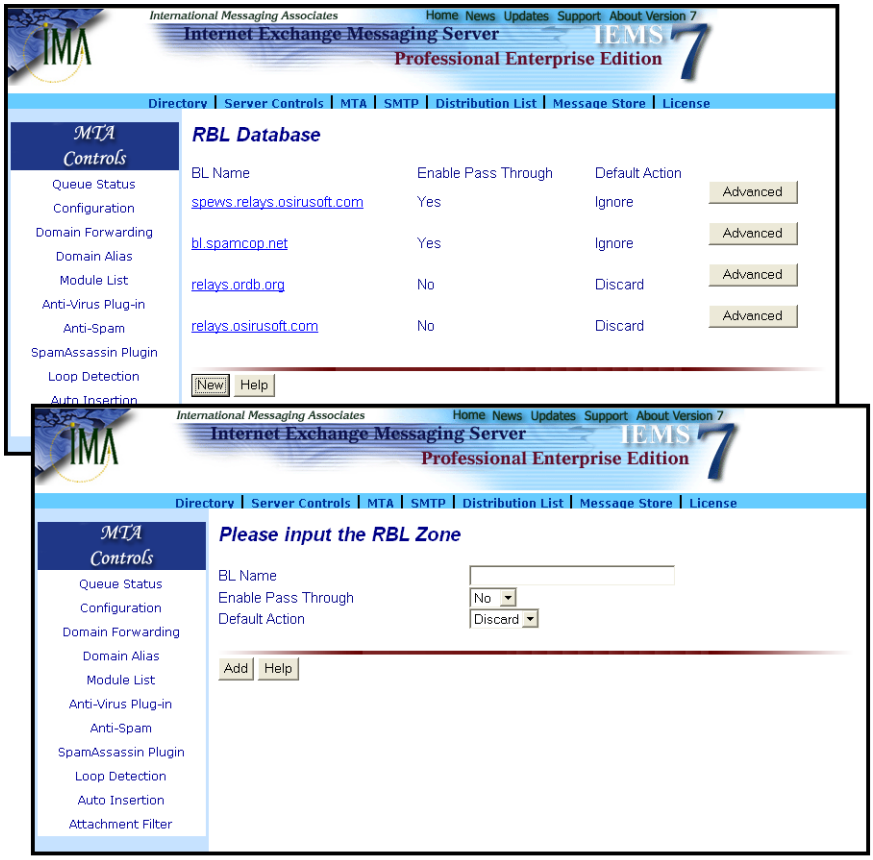

Figure 32: Adding and Deleting DNS-BL Databases

Once a new DNS-BL has been entered to the system, it is possible for the administrator to specify the default actions taken by each of the output channel processors. For channel processors such as the Local Mail Delivery Agent and the Distribution List Processor, this indicates what action to take if per-user or per-list actions have not been specified. For other channel processors, such as the cc:Mail and Notes connector modules - these processors do not have the ability to make decisions on a per decision basis, so the choices here will affect all users for these channels. For situations where it is chosen to discard messages for a particular output channel processor of this type, the action will be taken by a Preprocessor filter module.

To modify the output channel settings, select the ***Advanced*** button next to the DNS-BL to change (see Figure 33).

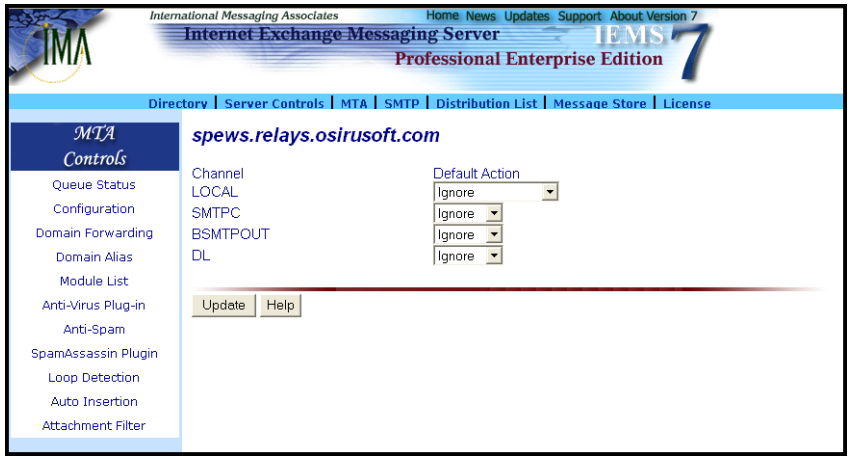

Figure 33: DNS-BL Output Channel Configuration

In the above figure, each output channel defaults can be configured according to their capabilities. In this example, *SMTPC* and *BSMTPOUT* can only have the choices of *Ignore* / *Discard*. This is because it is not possible to make any determination about user preferences for these channels.

DNS-BL Whitelists

While the use of DNS-BL lists can be beneficial many times, it is also true that for some, the number of generated false-positives can be high. In some cases, it may happen that related company or trading partner gets blacklisted. This is not necessarily bad - almost all major companies have been blacklisted at one time or another, as the accuracy of many lists is at best suspect.

For situations where a site you wish to communicate with has been blacklisted, but you still wish to use the configured DNS-BL's, it is possible to include the remote MTA or network in a DNS-BL whitelist.

To enter a DNS-BL Whitelist, simply select the ***RBL White List*** button on the main Anti-Spam configuration page (see Figure 29 on page 55). This brings up the DNS-BL Whitelist Configuration page (see Figure 34).

Figure 34: DNS-BL Whitelist Configuration

To add a new whitelist entry, simply select the ***New*** button and then on the next page enter the IP address or IP address range of the network that you wish to whitelist. When done select ***Add***.

SMTP Connection Control

Incoming SMTPD connections can be controlled through several SMTPD options (see Figure 29 on page 55).

IP Address Access Control
All the parameters in the IP Address Access Control column can be configured by also marking the check box of the following:

Enable Reverse DNS lookup
By activating this option, reverse DNS lookup is performed during the SMTP session. During the HELO/EHLO session, the SMTPC identifies itself to the SMTP server (SMTPD) through the HELO/EHLO parameter. The SMTP server verifies if the domain name corresponds to the IP address of the SMTP client host by performing reverse DNS lookup.

Reject Non-Resolvable IP
When enabled, SMTPD rejects the connection if the incoming IP address is non-resolvable, which means that there is no DNS (PTR) record for

this address.

Reject Non-Match Host/Domain
When enabled, SMTPD matches the resolved domain name with the one declared by the remote SMTPC. If the two do not match, the connection is denied. It is also used to compare the reverse address lookup values, but does not continue to check for possible CNAME entries.

Allow/Deny Incoming SMTP connection by default
If the “Allow Incoming” option is selected, SMTPD accepts every IP address except for those mentioned in the Deny IP address list. On the other hand, if “Deny Incoming” option is selected, every IP address except for those mentioned in the Allow IP address list is rejected.

Allow/Deny Mail Relaying by default
If the *Allow Mail Relaying* option is selected, SMTP allows mail relaying for all IP addresses except for those mentioned in the Deny IP address list. On the other hand, if *Deny Mail Relaying* is selected, every IP address except for those mentioned in the Allow IP address list is prohibited for mail relaying.

Adding and Deleting Banned IP Addresses

The ***SMTP Connection Control*** button (see Figure 29 on page 55), once selected, allows the system administrator to add or delete lists of IP address ranges of potential spammers (see Figure on page 66). Potential spammers are prevented from establishing SMTP connection with IEMS.

To add an IP address, click the ***New*** button. A new screen appears. Enter the IP address range and click the ***Add*** button.

To remove an existing entry, select a particular entry and click the ***Delete*** button.

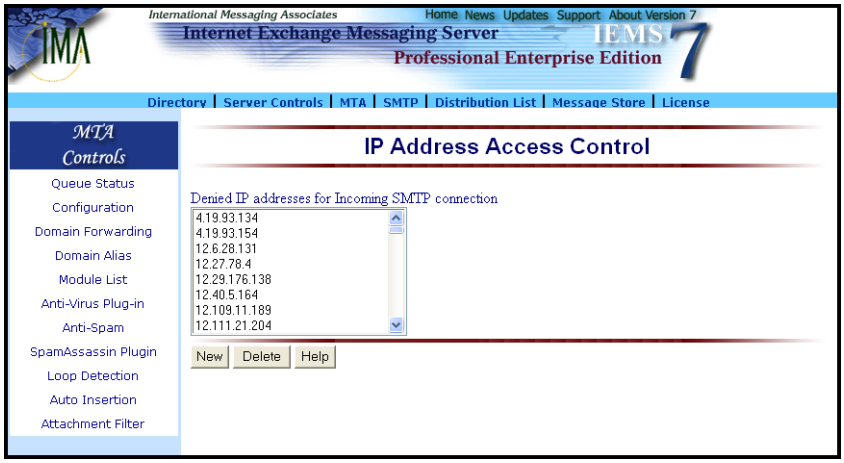

Figure 35:Adding and Deleting Banned IP Addresses

Listing Denied or Blocked IP Addresses for Mail Relaying

The ***Mail Relay Control*** button (see Figure 29 on page 55), once clicked, enables the system administrator to list down the banned or blocked IP address(es). This way, IEMS can block or deny these IP addresses when performing mail relay (see Figure 36 on page 67).

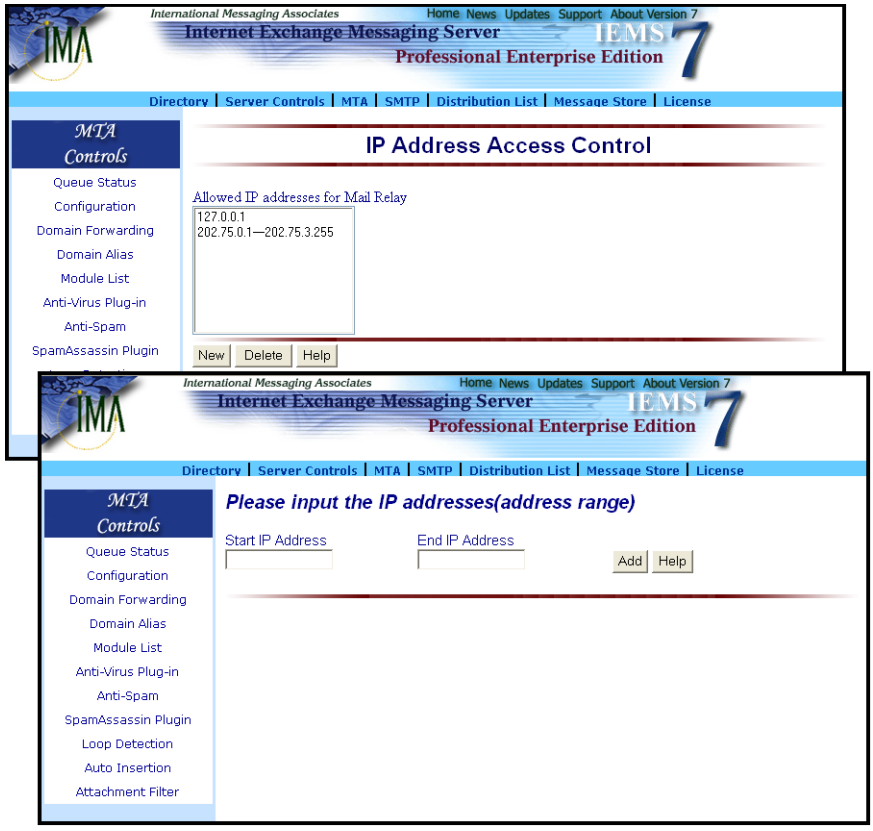

Figure 36: Listing Denied or Blocked IP Addresses

SpamAssassin Plugin

IEMS supports connection to the SpamAssassin mail filter for recommendations related to message content analysis. SpamAssassin is an open source content analysis filter that runs primarily on Linux/Unix machines (see *http://www.spamassassin.org* for more details). The IEMS SpamAssassin Plugin library uses the libspamc library to communicate with SpamAssassin Daemon (spamd) to consult about the probability of a given received message being spam. SpamAssassin needs to be installed and the spamd daemon run before enabling the SpamAssassin Plugin for IEMS. For details on how to install and configure SpamAssassin, please consult the: SpamAassassin Documentation found at their web site

To configure the IEMS SpamAssassin Plugin, click on the ***SpamAssassin Plugin*** button in the main menu area. The “SpamAssassin Plug-In Configuration” will then be displayed (see Figure 37).

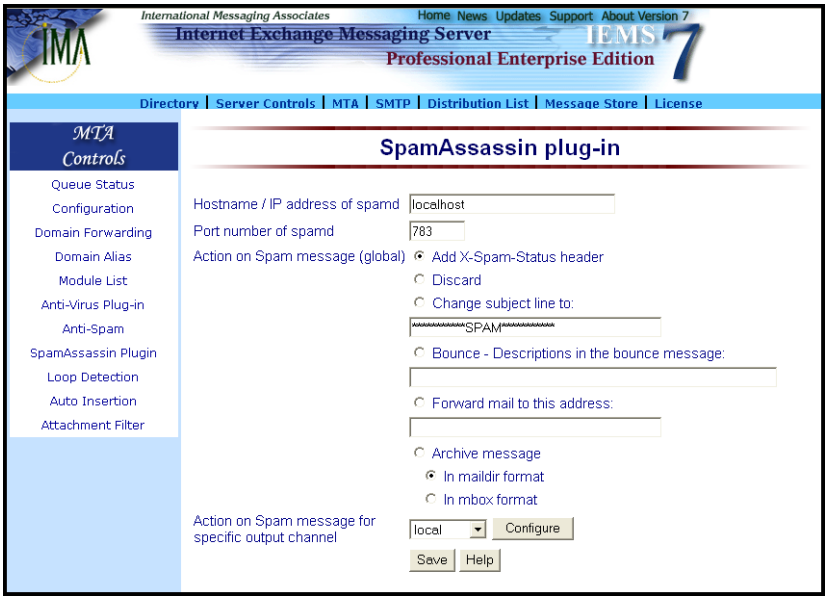

Figure 37: SpamAssassin Plug-In Configuration

To enable the SpamAssassin plugin, you need to define the hostname and the port number of your spamd server. The system assumes spamd is installed on the same server where Internet Exchange is running. The default port number used by spamd is 783. For performance reasons, you may want to consider installing spamd on a separate machine to reduce the loading on the IEMS system.

When a spam Message is Detected
When spamd reports a spam mail has been received, you can configure the SpamAssassin plugin to perform one of the following actions:

Add X-Spam-Status header
An extra "X-Spam-Status: YES" header will be added to the original message. This extra header can be recognized by the Local Mail Delivery module and the Distribution List manager for further processing.

Discard
Select this option to stop the spam mail message being delivered to the final recipient.

Change Subject line
Change the Subject line to a predefined string. It is useful when dealing with mail clients that are not capable of filtering based upon X- header information.

Bounce the message
Bounce the message to the original sender with a predefined sentence in the return mail.

Forward mail to this address
You can select this option to forward the message to another user for human

inspection.

Archive the message

Select this option if you want to keep a copy of the spam message. The message will not be delivered to the intended recipient. The message can be archived in maildir (each message is stored as separate file) or mbox (mail message are saved in a single file) format.

For the Windows version of IEMS, the message will be saved under the "*spam-sa*" directory under the Internet Exchange Messaging Server QUEUE directory. For Linux versions, the message will be saved under the */var/spool/iems/mqueue/spam-sa* directory.

Define action for different channel

You can define separate action for each different output channel in IEMS. For example, you can configure the SpamAssassin plugin to add the "X-Spam-Status" header for your Local MessageStore user (the LOCAL channel) but to discard the message for your ccMail/Notes connector user. To configure the action against different channels, select the output channel name from the list and select the ***Configure*** button to bring up the “SpamAssassin Plug-In Channel Configuration” page (see Figure 38).

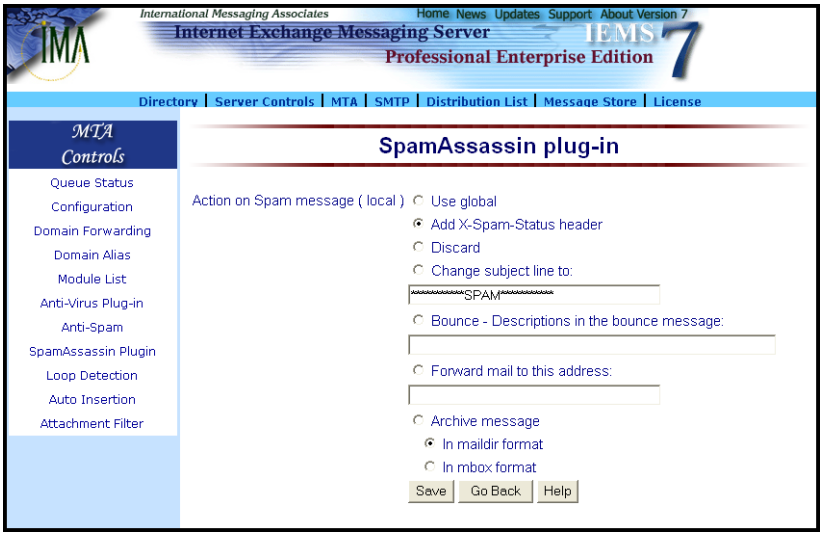

Figure 38: SpamAssassin Plug-In Channel Configuration

Attachment Filter

The Attachment Removal Module allows the system to automatically detect and remove questionable content from messages that pass through the MTA. This provides yet another powerful tool for the administrator to combat virus and other undesirable content from entering the system.

This module supports the filtering of both MIME and non-MIME message types. It can filter attachments based upon content-type and/or attachment file names. For more information on MIME types, please see the IMA White-paper **MIME - Technical Overview**, available at *http://www.ima.com/pdf/*

mimeovr.pdf.

Figure 39: Filter Mail Attachments

To configure this module, select the ***Attachment Filter*** button in the main menu area. This brings up the main FIlter Mail Attachment screen (see Figure 39 on page 70). Attachments filtered through this module are automatically removed from the message. A separate message is then sent to the recipient and optionally to the postmaster, informing them of removal. Attachments can be filtered based upon any of the following criteria:

- Content-Type
- Attachment File Name
- Content-Type + File Name
- All Attachments

Filtering Based on Content-Type
Select the **Configure** button to determine the Content-Type. See the next section for details on this configuration. When done, click on **Add** to register the new filter.

Filtering Based on Attachment File Name
Select the "-(Unknown Content-type)" entry in the *Content-Type* field and enter the desired file name in the *Filename* field. This field can contain "*" wildcards. Thus, if you want to automatically remove for instance all Visual Basic attachments, specify **.vbs* in this field. When done, click on **Add** to register the new filter.

Filtering Based on Content-Type + Attachment File Name
For filtering an attachment given a specific Content-Type and a filename, select any option from the *Content-Type* field other than the "*/* (Filter All)" and "-(Unknown Content-type)" options. Then enter the desired file name in the *Filename* field. Wildcard characters ("*") are accepted. When done, click on **Add** to register the new filter.

Filtering All Attachments

For filtering all attachments, select the "*/* (Filter All)" option from the *Content-Type* field list box. When done, click on **Add** to register the new filter.

Note: *There is no need to enter a filename in the Filename field, as it will be ignored.*

Filter Attachment Options

To specify a MIME Content-Type, select the **Configure** option (see Figure 39 on page 70). This brings up the Content-Type Configuration screen (see Figure 40 on page 71). This screen allow the administrator to configure new MIME Content-Types that the system will recognize when scanning messages.

To add a new Content-Type, first select the radio button of the specific type, i.e, "Text". Next, select a subtype from the subtype list box for the desired type. You may select either "*" to indicate that all subytpes are included, or a specific subtype. Finally, click the **Submit** button, and the Content-Type list box on the main configuration page will be updated.

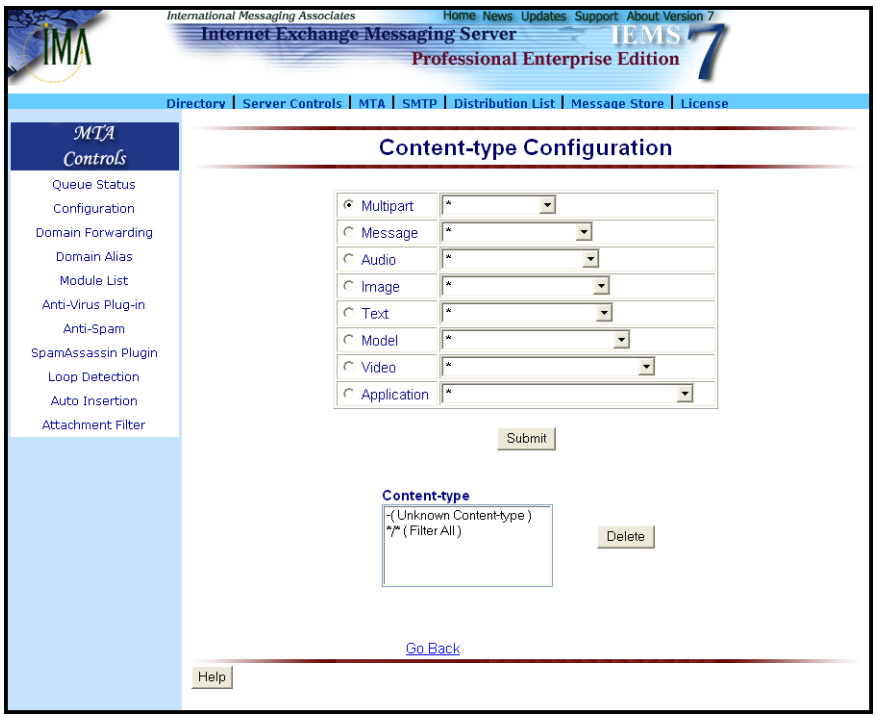

Figure 40: Content-Type Configuration

Note: *If the Content-Type to add is "Type/*", where Type represents the type itself (e.g. "Text"), any existing Content-Type entries of the same type (e.g. "Text/richtext") will be deleted and the Content-Type "Type/*" will be added in the Content-Type list box. If "Type/*" is already configured, trying to add other "Type/whatever" entries will not be added to the list, and an error message "All subtypes are already included!" will be displayed.*

Deleting an Existing Content-Type
To delete an existing Content-Type, simply select the Content-Type to be deleted from the Content-Type list box and depress the **Delete** button. Please note that the "-(Unknown Content-type)" and "*/* (Filter All)" entries are special and cannot be deleted.

When the configuration of the Content-Type is complete, click on "Go Back to FilterAttachment Page" to continue.

Options
Normally when questionable content is detected by the system, it will be quietly removed, and the modified message sent to the intended recipient. If on the other hand, it is desirable to not modify and resend to the end recipient, the *Action on suspicious mail attachment(s)* field can be configured to *Bounce*. When configured in this manner, messages with attachments matching the filtering rules will be bounced back to the sender rather than modified and sent to the recipient. The normal mode of operation is *Ignore*, where filtering takes place and cleansed messages sent onward to the desired recipient(s).

If the administrator needs to monitor filtering activity, the *Send notification to postmaster* field can be selected, where messages will be sent to postmaster whenever a message is cleansed.

Loop Detection

The system administrator may configure the different rules for handling message loops. To configure the loop detection feature, click the ***Configure Loop Detection*** button on the left menu frame. This displays the "Loop Detection Configuration" screen (see Figure 41 on page 72).

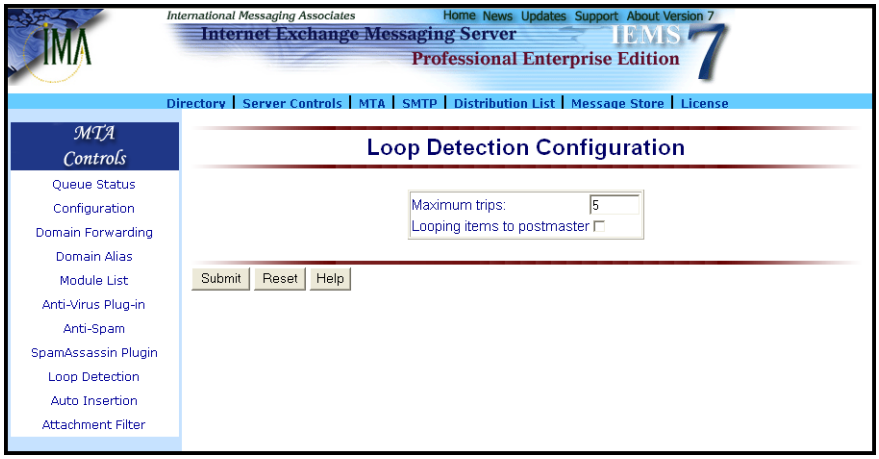

Figure 41: Loop Detection Configuration

Maximum trips
For every message that passes through the MTA, a received header line with the MTA's FQDN is added to the message header. This option specifies the maximum number of received lines (that show the FQDN of the MTA

machine) allowed in an incoming message. Only lines containing the MTA FQDN are counted. If this number is reached, the message will be either bounced to the sender or postmaster. This prevents mail looping.

Looping items to postmaster
When set looping messages are sent back to the local postmaster instead of being returned to the remote sender.

Click the ***Submit*** button to store the new settings.

Auto Text Insertion

The auto insertion engine provides the capability to insert text into messages that pass through the MTA. Using this feature, messages created by users can automatically include insertion text defined by the system administrator. Possible text may state the confidentiality of the message which may limit the liability of the company that maintains the mail server where the message originated.

The administrator can add different disclaimer messages based on the message source. He may use either simple text and/or HTML format messages for the process. The auto insertion engine supports MIME and non-MIME message structures.

To configure this feature, click the ***Configure Auto Insertion*** button on the left menu frame. A new screen (see Figure 42 on page 73) appears. Click the ***New*** button and provide information on the following fields:

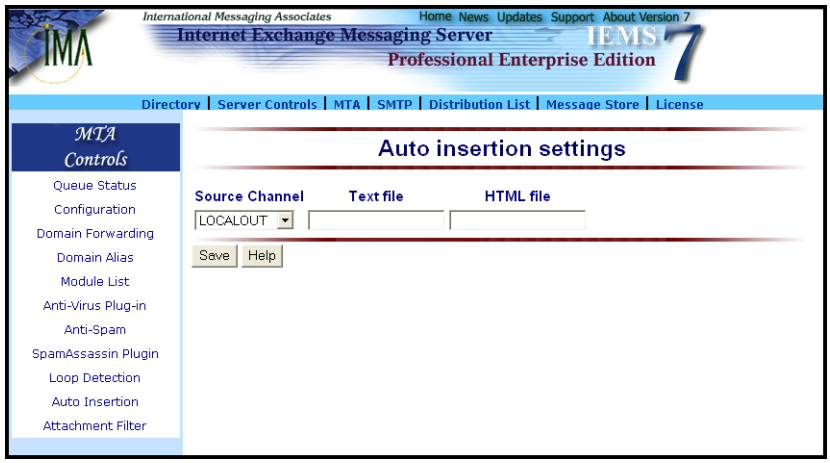

Figure 42: Auto Text Insertion Configuration

Source Channel
The specified text will automatically be attached by the auto insertion engine to messages coming from this channel.

Text file
The path of the text file that contains the text to be inserted to outgoing messages.

HTML file
The path of the HTML file that contains the text to be attached to outgoing messages. The system administrator is provided with the option to use an HTML file as a inserted text for outgoing messages.

Click the ***Save*** button to store the auto insertion files.

The ***Edit contents*** button allows the system administrator to enter corrections, while the Delete button disposes of a file.

CHAPTER 4

Message Store

Overview

The Message Store is more than just a dedicated mail repository for remotely storing, retrieving and manipulating messages (see Figure 43 on page 76). It allows the system administrator to limit the amount of storage space allocated to the user, preventing the user from consuming all the available disk space in the server. Its mail filtering utility enables the system administrator to define rules so that the LMDA (Local Mail Delivery Agent) can direct messages to pre-selected mailboxes or folders other than the user's Inbox.

The Message Store also provides shared mailbox support allowing the system administrator to create mailboxes that can be shared by two or more users. Support for shared mailboxes allow users to have both personal and shared mailboxes, which can be accessed using a single account. This feature makes management of email for a group of people fairly easy since there is no need to create a group login name. The process of creating multiple copies of a single message to be sent to different people is eliminated. It also allows many users to efficiently access the system concurrently.

Unlike other IMAP4-based servers, IEMS handles large mailbox sizes efficiently. Using the shared mailbox system, the system can manage users, groups and other shared data with a single mail account. As a flexible tool, it lets users access their mail using any IMAP4- or POP-capable client, such as Microsoft Outlook, Eudora Mail, Pegasus Mail, among others. The same Message Store can also be accessed remotely using any web browser via the Web Mail Client.

The Message Store makes use of the following databases:

- Message Status Database
- Message Envelope Database
- Message Body Database

IMAP4-related attributes and RFC-822 header information are stored in the Message Status Database and Message Envelope Database, respectively. The Message Body Database stores the body structure of all messages in a given mailbox. Access to the different databases in the Message Store is carried out via the Message Store API.

The Message Store also includes both the IMAP4 and POP3 servers as well as the Web Mail Client. Each of these servers is capable of creating multiple threads to support simultaneous access to the Message Store and the retrieval of multiple messages.

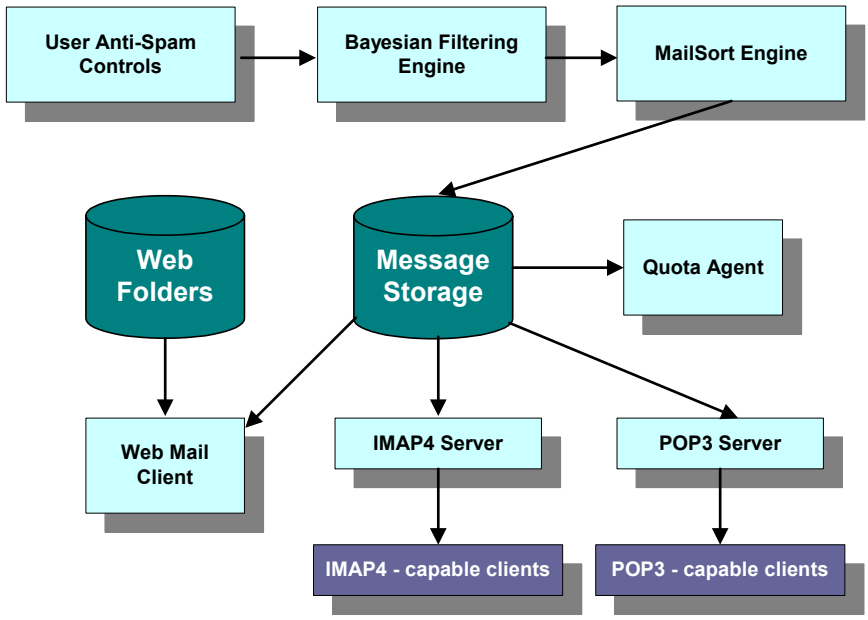

Figure 43: Message Store system architecture

Local Mail Delivery Agent (LMDA)

The Local Mail Delivery Agent (LMDA) is responsible for the delivery of messages from the MTA Shared Message Queue to the Message Store. After the messages have been retrieved from the Shared Message Queue, the LMDA performs several pre-delivery operations on behalf of the recipient. These include optional handling of MTA Pass-Through tagged messages (DNS-BL and content filtering), as well as Bayesian filtering and mail sorting. The LMDA Architecture can be seen in Figure 44.

Bayesian Filtering Engine

Bayesian Filtering is used to apply user specific rules against incoming messages. The Bayesian filter can be trained by the user to understand the types of messages that are undesirable on an individual basis.

The Bayesian filter works by compiling characteristics of messages that each user tells it is spam. When mail is received that is not desired, the user needs to move this to the spam learning folder. This can be done manually when using IMAP configured mail clients, or by selecting ***Mark this as a spam message*** from within the IEMS Web Mail Client view message screen. The system will periodically check the contents of this folder for new messages and update the user Bayesian filter database.

When messages are received, the Bayesian filter consults the user Bayesian filter database and compares the incoming message against information stored in the database. The filter uses a statistical process to determine the probability that an incoming message should be considered spam for a particular user. Messages identified as spam are acted upon based upon the users Bayesian Filter configuration.

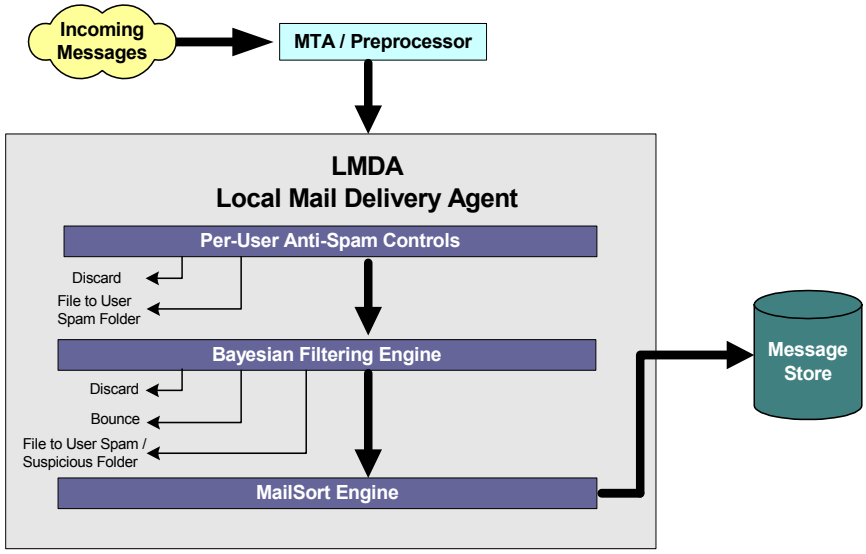

Figure 44: LMDA Architecture

Mailsort

The Mailsort module of the Message Store makes use of user specified rules so that the LMDA can copy or move messages to pre-selected mailboxes other than the Inbox. It can also selectively forward messages to other addresses and generate automatic replies to incoming messages based on predefined criteria.

This feature enables users to sort incoming mail based on attributes, such as the message sender, recipient and subject without having to go through all the messages. Mailsort can also reject mail coming from predefined email addresses.

Individual users of the Message Store can configure their own filtering mechanism. All of the authenticated users can use the Web Mail Client interface for configuring the Mailsort engine.

Mailsort is divided into two modules, the engine and the web configuration interface. The engine is used by the LMDA to determine the destination of messages whose recipients maintain filtering information in their respective Message Store directories. The web interface allows the users to create and edit filter files used by the engine to inform the LMDA of the destination of the messages.

The Mailsort module provides users with a utility for preprocessing incoming mail on a per user and per message basis. Incoming messages delivered to the Message Store through the LMDA are sorted according to the rules set by the user. The engine will read the filter file (**filter.txt**), and perform a very simple recursive-decent parsing to speed up the interpretation of the filter file.

Vacation Utility

The vacation utility is included allowing users to send automatic replies to incoming messages. This feature is useful when you are on leave or when you are unable to reply to your messages for an extended period of time.

When the Mailsort filter matches the received messages, it will send a vacation message to the sender. Only one vacation message will be sent to the sender within seven days even if the sender sends multiple messages.

Vacation messages will not be generated for some types of messages such as standard formatted distribution list messages or bounced messages from the Mailer Daemon like messages from *postmaster@ima.com*. Mailsort will check for these keywords in the message header. When a match is found, it will not generate a vacation message to the sender of this message.

Quota Agent

The Message Store Quota Agent limits the amount of storage space allocated to the individual users, preventing them from consuming all of the available disk space on the server. It also allows the system administrator to monitor the total number of registered users and determine the users who have exceeded their disk quotas. The Quota Agent has two scheduling options -- Daily and Weekly -- in checking the disk space utilization of the Message Store.

The Quota Agent generates reports in HTML and text file formats, which the system administrator uses to check and verify the Message Store performance and disk usage. The reports in HTML format are available through the Message Store web interface, while text file reports are sent to the system administrator as file attachments.

Web Mail Client

The integration of the Web Mail Client in the Message Store allows users to access their mailboxes from the Message Store using any web browser.

IMAP4 Server

The Message Store includes an IMAP4 server, allowing remote clients to access the Message Store using the Internet Mail Access Protocol Version 4 (IMAP4) protocol. Most modern email clients, such as Outlook Express, Eudora, Netscape Communicator, and many more support this standard.

IMAP4 offers users added flexibility in managing their mail over other post office access protocols, such as POP3. With IMAP4 support, users can manipulate their mailboxes/folders on the server without having to download them to a local hard disk. End users can also create multilevel mailboxes on the server that can be easily renamed or deleted by them (with the proper authorization from the system administrator), as well as shared mailboxes which can be viewed concurrently in real time from multiple platforms. Another advantage is that users have the option to search for messages on the server based on various attributes such as message size, headers, and

message sender, and to separate attached files from the text and header portions of a message, with the searches being performed by the back-end Message Store.

The IMAP4 server operates both in online and off-line access modes, allowing client email programs to access and manipulate email messages on a server. It permits manipulation of remote message folders, on the server without having to download them to a local hard disk, saving precious bandwidth resources. For example, messages stored on an IMAP server can be manipulated from a desktop computer at home, a workstation in the office and a notebook computer while travelling without the need to transfer messages or files back and forth between these computers.

The IMAP4 server supports nesting of mailboxes. With this feature, users may create a sub-folder (e.g. Bart_Simpson) of an existing folder (e.g. Cartoon_Characters). Having this feature gives Message Store users added flexibility in managing their messages since they can easily organize their folders in such a way that they can group their mail and file them in different sub-folders.

POP3 Server

The POP3 server provides POP3-capable clients with another means of accessing their incoming mailboxes. Using POP3, users can retrieve messages from the Message Store Inbox and store them in a local hard disk so they can be read in an off-line or disconnected state. The POP3 server also supports multi-threading for fast message retrieval.

User Accounts

Creating User Accounts

To configure the Message Store, select the **Message Store** link on the top menu frame. This action displays the “Message Store” screen (see Figure 45 on page 80).

User accounts contain the user’s personal and mailbox information. The system administrator may also define user disk quota limits to control disk space usage for individual Message Store users as well as web folder permissions. Selecting the ***Add User*** button on the left menu frame displays the “Add User” screen (see Figure 46 on page 80).

Email Address
The email address of the new user. The email address of a new user needs to be registered to serve as reference to their personal mailboxes. The senders, on the other hand, will use this email address to reach the new user’s mailbox.

First Name
The first name of the new user to be added to the Message Store and Directory Services

Figure 45: Message Store

Last Name
The last name of the new user to be added to the Message Store and Directory Server.

Password/Confirm Password
The security password is used to gain access to the user's personal email. To make sure that it is typed correctly, the password needs to be entered a second time in the **Confirm Password** text box. The password appears on screen as a row of asterisks for security purposes.

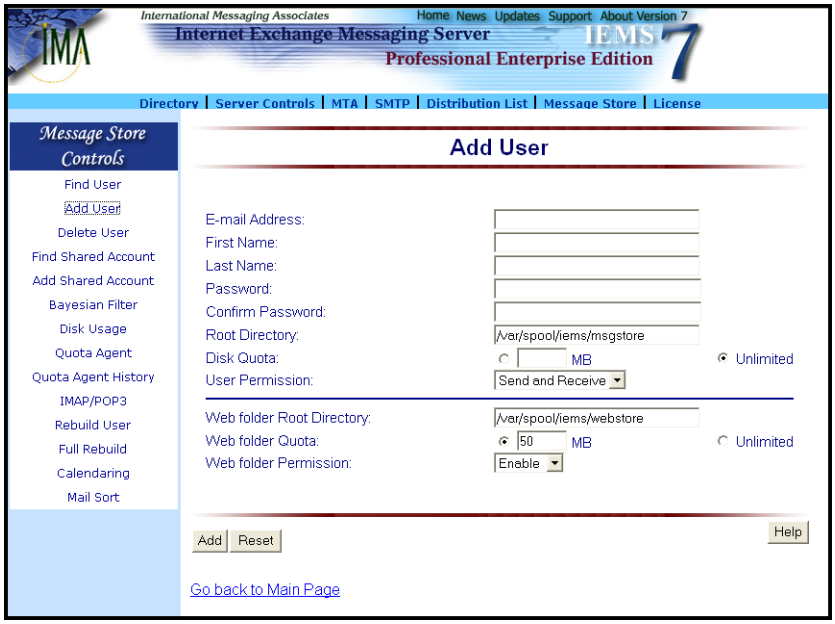

Figure 46: Creating User Accounts

Root Directory
The physical location of the user's mailboxes and messages. The default system root directory path is initially displayed in the form. The system administrator can easily change the home directory of the user by altering the default value.

Disk Quota
The disk quota limit to prevent Message Store users from consuming all the available space in the server. Assigning an "unlimited" quota allows the user to have an infinite size and number of messages inside the folder of his home directory in the Message Store.

User Permission
Send and Receive allows Message Store users to send and receive messages. The **Send Only** permission allows the user to only send messages.

Web Folder Root Directory
The physical location of the user's web folders. The default system root directory path is initial displayed in the form. The system administrator can easily change the web folder home directory of the user by altering the default value.

Web Folder Quota
The disk quota limit for the new user's web folder storage area. Assigning an "unlimited" quota allows the user to have an infinite size and number of files and directories inside their web folders.

Web folder Permission
Used to ***Enable*** or ***Disable*** user access to web folders.

Deleting User Accounts

The system administrator may delete users from the local Message Store by clicking the Delete User button on the left menu frame. This action displays the “Delete User” screen (see Figure 47 on page 82). Highlight the user or users to be deleted in the Users to Delete list box and click the Delete button. A confirmation screen appears. Click the Delete button.

Note: *Deleting a Message Store account will remove the Message Store connector (LOCAL) from the user’s directory entry, but not the entire directory entry. If the entry in the directory is also to be removed, this must be done separately through the Directory Services interface.*

Figure 47: Deleting User Accounts

Finding Users

The system administrator may view a list of existing users by selecting the ***Find User*** button in the left menu frame. This action displays the "Find Users" screen (see Figure 48 on page 83). Type either the first name, last name or email address of the Message Store user.

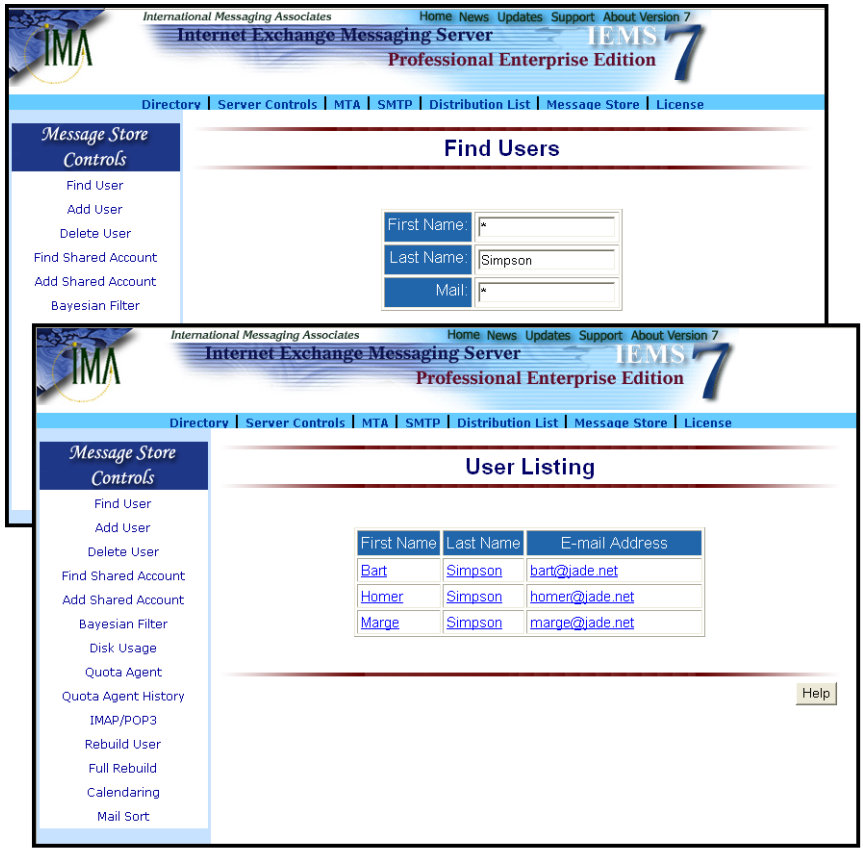

Figure 48: User Listing

Note: *A specific search criteria may be entered to display a subset listing of users. For example, typing R* on the* **First Name** *field will list all usernames that start with the letter "R" Use of wildcards (*) lists all the users within the local Message Store.*

The "User Listing" screen appears after clicking the ***Submit*** button.

Viewing User Profiles

The system administrator may view profile and mailbox information for a particular user by clicking on a user link from the "User Listing" screen (see Figure 48 on page 83). A table of the user's information will then appear (see Figure 49 on page 84).

Editing User Profiles

The system administrator may modify user mailbox information. He may assign a new directory to store the mailbox of the user, specify new disk quotas or permission levels when sending and receiving messages.

Figure 49: User Information

On the “User Information” screen, click the Edit button (see Figure 49 on page 84). This action displays the “Edit User Profile” screen (see Figure 50 on page 85). Please see “Creating User Accounts” on page 80 for information on each field.

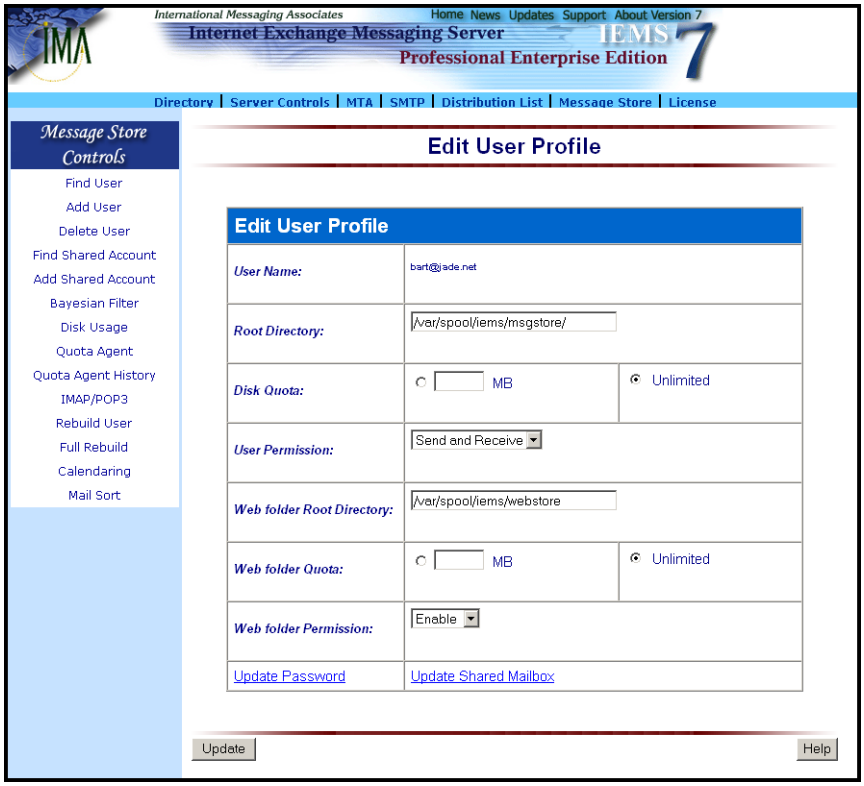

Figure 50: Editing User Profiles

Updating User Password

User passwords can be updated by selecting the Update Password link on the “Edit User Profile” screen (see Figure 50 on page 85). This displays the “Update Password” screen (see Figure 51 on page 86). The new password must be entered in the New Password and the Confirm Password text boxes. Then, click the ***Update*** button.

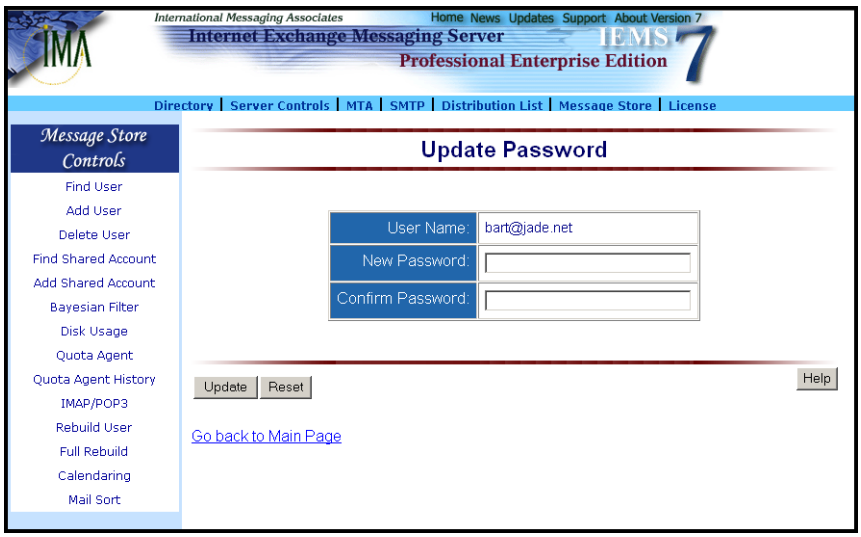

Figure 51: Updating User Password

Note: *Updating password provides a more secure environment for the system administrator and user to prevent unauthorized persons from accessing their mailboxes. End users can update their passwords via the controls found in the Web Mail Client interface.*

Bayesian Filter

The Internet Exchanging Messaging Server provides an interface for system administrator to hook a "Bayesian filter" into the Local Mail Delivery Module (LMDA). Bayesian filters are statistical processes used to identify a spam mail message. For details about the operating principals of the Bayesian filter, please consult the article **A Plan For Spam** written by Paul Graham (*http://www.paulgraham.com/spam.html*), and **Better Bayesian Filtering** (*http://www.paulgraham.com/better.html*).

IEMS 7 bundles the open source **bogofilter** version 0.11.2 Bayesian filter. Details about bogofilter can be found at *http://sourceforge.net/projects/bogofilter/*. IMA's changes and enhancements to **bogofilter** can be freely downloaded at *http://www.ima.com/dist/pd/iems_bogofilter.tgz* and *http://www.ima.com/dist/pd/iems_bogofilter.zip.*

Bayesian Filter Learning Engine

Bayesian filtering is a statistical process that requires some training in order to obtain accurate results on spam message detection. In IEMS a program named "*bayesianlearn*" is provided for this purpose. This *bayesianlearn* program is a command line utility that looks at the spam and good messages under a predefined mailbox folder by each message store user. Each message will be submitted to the underlying Bayesian filter training engine. If you wish to supply your own Bayesian filter training engine, it must support the following features:

- Ability to add a message to the good mail database
- Ability to remove a message from the good mail database
- Ability to add a message to the spam mail database
- Ability to remove a message from the spam mail database

When the *bayesianlearn* program starts, it performs the following tasks for each message store user:

- For each message in the good message folder it calls the Bayesian filter training engine to remove the message from the spam mail database and then adds it to the good mail database.
- For each message in the spam message folder it calls the Bayesian filter training engine to remove the message from the good mail database and then adds it to the spam mail database.

Message Reception

Messages that make it as far as the Bayesian filtering stage, and that pass the initial Bayesian filtering check are assumed by the system to be good, and non-spam. When this happens, the message is submitted to the training engine and added to the good database before being handed off to MailSort for final delivery. The word and frequency values in the good database are updated to reflect another good message received. If the message was determined to be spam, the message is submitted to the learning engine and the spam databases updated accordingly.

This system is designed to learn over time what a particular user considers good and what they consider spam. The good and spam databases will differ from user to user as their opinion of what is appropriate and not differs. When IEMS is first installed, there will be no record of good or bad messages, hence the system will treat all messages as being good in the absence of data to the contrary (the spam database).

When a user finds that a spam mail ends up in the inbox, he should move the message to the spam learning folder. The same applies for false positives (if any) that go incorrectly to the "my-spam" folder. When *bayesianlearn* starts up, it processes each message in the spam learn folder. For each message, it first removes it from the good database and adds the signature to the spam database. For good learn folder, it does the reverse.

To train the engine properly, ***ALL*** spam messages must be moved to the spam learning folder. The reason for this is that the system has already assumed that the received messages are good and updated the frequency count accordingly. If multiple identical spam messages are received, then the frequency count will be adjusted taking this into consideration. In order to correct this, each message must be subtracted from the good database in addition to addition to the spam database. For example a user receives two spam message (A and B) that appear similar. He only moves one of them (Say B) to the spam learning folder. When *bayesianlearn* runs, it removes only B from the good database and adds it to the spam database.

Now, when message C which is the variant of A and B arrives, both good and spam database contain similar information of this spam pattern. Therefore, due to the bayesian design, the message C will be classified as good and added to the good database again. Thus, the engine is not properly trained.

For this case, we need to make sure that all spam messages, no matter if they look similar or not, are moved to the spam learn folder such that the message patterns are properly removed from the good database. It is also important to realize that the training of the bayesian engine takes time to learn. The accuracy rates are extremely high (in excess of 98% for properly trained databases), however it can take time to get enough spam data into the user databases.

One approach that can be used to offset spam in the inbox while undergoing initial Bayesian training, is to enable MTA Pass-Through on the DNS-BL and content filtering, and redirect these messages to the users system spam folder. These messages will not go through the Bayesian learning, however messages that are determined to be spam in the system spam folder (already pre-sorted by the system) can be added to the Bayesian learning folder for training.

Configure Bayesian Filter

Before the LMDA module can use the Bayesian filtering features, you need to enable it. To bring up the Bayesian Filter configuration, click the ***Bayesian Filter*** link in the main menu area. The “Bayesian Filter Configuration” screen will now be displayed (see Figure 52).

Bayesian filter modules can be attached either as command line utilities (**EXE**), or library functions (**DLL**). The **bogofilter** module as shipped by IMA is a library function, and the default settings (as shown n the figure below) should not be changed). Check the **Enable** check box to enable Bayesian Filtering and then select to use either a **DLL** or **EXE** type Bayesian filter.

Configuring DLL Type Filters

When IEMS is installed, the library version of **bogofilter** is automatically installed. It is installed as *libbogo.dll* under the Internet Exchange Messaging Server install directory for Windows installations. Under Linux it is installed as */opt/iems/lib/libbogo.so*.

The library function call needs to expose a function that can be called by the LMDA module. The function name provided by *libbogo* library is "iems_bogofilter".

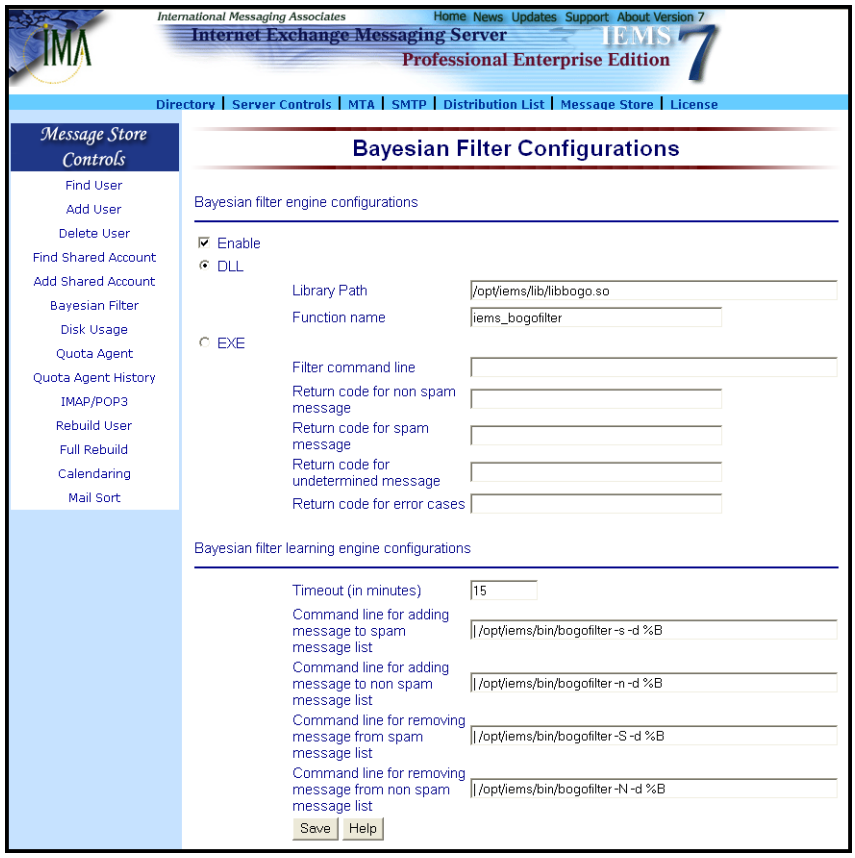

Figure 52: Bayesian Filter Configuration

Configuring EXE Type Filters

If you are using a command line type Bayesian filter (**EXE**), you need to provide the command line argument and the return code provided by the filter to indicate the filtering result. The following directives are supported in the filter command line:

- **| - Pipe the message to STDOUT**
  This tells the LMDA module to dump the message content to STDOUT so that the selected Bayesian filter can read the message content via STDIN. Note, if this is used, you MUST put the "|" symbol at the beginning of the command line.

- **%B - The location of the ".bayesian" directory**
  Each Bayesian filter implementation uses database files to store the statistical information for good and spam message. In Internet Exchange Messaging Server, a special directory called ".bayesian" is created for individual message store user to store the Bayesian filter's database files. This ".bayesian" directory is located under each message store user's HOME directory. For example, the HOME directory for user "john@company.com" is /var/spool/iems/msgstore/john@company.com, the %B directive will be expanded to:

  /var/spool/iems/msgstore/john@company.com/.bayesian

%M - The message file
If your Bayesian filter cannot read the message content via STDIN but expect the message file name in the command line parameters, you can use the %M directive.

- **%F - The message envelope sender**
  The email address of the mail message envelope sender will be substituted.

- **%R - The recipient email address**
  The email address of the current message recipient (ie. the email address of the message store user) will be substituted.

Example 1:

```
| /usr/local/bin/myfilter -d %B
```

Expands to:

```
| /usr/local/bin/myfilter -d /var/spool/iems/msgstore/john@company.com/.bayesian
```

Example 2:

```
/usr/local/bin/myfilter -d %B -I %M
```

Expands to:

```
/usr/local/bin/myfilter -d /var/spool/iems/msgstore/john@company.com/.bayesian -I /var/spool/iems/mqueue/01/1.msg
```

Beside the filter command line, the return code that the Bayesian filter uses to indicate different conditions must be defined. The return codes are integer number various from 0 to 255. If your filter returns different return code values for the same condition, use a COMMA to separate each of them. The 4 conditions are:

- Detected non Spam message
- Detected Spam message
- Undetermined message
- Error condition

You filter must provide return code for the first two conditions.

Bayesian Learning Engine Configuration

When messages need to be added or removed from the users Bayesian databases, the learning engine must be called and the message supplied. The command line arguments of your Bayesian filter training engine must be properly configured for IEMS to work properly with it. The following directives are provided in the IEMS interface:

- **| - Pipe the message to STDOUT**
  This tells the *bayesianlearn* utility to dump the message content to STDOUT so that the selected Bayesian filter training engine can read the message content via STDIN. Note, if this is used, you **MUST** put the "|" symbol at the beginning of the command line.

- **%B - The location of the ".bayesian" directory**
  Each Bayesian filter implementation uses database files to store the statistical information for good and spam message. In IEMS, a special directory called ".bayesian" is created for each individual message store user to store the Bayesian filter's database files. This ".bayesian" directory is located under each message store user's HOME directory. For example, if the HOME directory for the user "john@company.com" is /var/spool/iems/msgstore/john@company.com, the %B directive will be expanded to:

  /var/spool/iems/msgstore/john@company.com/.bayesian

- **%M - The message file**
  If your Bayesian filter training program cannot read the message content via STDIN but expect the message file name in the command line parameters, you can use the %M directive.

There is a locking mechanism between the LMDA module and the bayesianlearn program. If the LMDA fails to acquire the lock, it will keep on retrying until it reaches the TIMEOUT (default is 15 minutes). When the LMDA reaches the timeout, it will send a notification to the system postmaster account and terminate. If you receive such notification, you should check if there are any problems that might cause the *bayesianlearn* program to fail to release the lock. You may need to terminate the *bayesianlearn* program manually and remove the "bayesain.lock" file under each of the message store user's HOME directory. Restart the LMDA afterward.

Shared Accounts

Creating a Shared Mailbox

The system administrator may create mailboxes that can be shared by two or more users. Shared mailbox support allows users to have both personal and shared mailboxes, which can be accessed using a single account. This feature makes the management of email for a group of people fairly simple since there is no need to create a group login name. In addition, the process of creating multiple copies of a single message to be sent to different people is eliminated.

To create a shared mailbox, click the ***Add Shared Account*** button on the left menu frame. This action displays the “Add Shared Account” screen (see Figure 53 on page 93). Provide information for the following fields:

Email Address
The email address of the new shared account needs to be registered to serve as the reference of the shared mailboxes. This email address will also be used by the IMAP4-capable clients, such as Outlook Express and Netscape, in accessing shared messages on the IMAP4 server. Senders use this email address to reach the recipients of the shared mailbox.

User Name
The name of the new shared mailbox to be created in the Message Store and Directory.

Root Directory
The physical location of the shared account’s mailboxes and messages. The system default root directory is displayed in the form. The system administrator can easily change the home directory of the user by altering the default value.

Members
Select the members of the shared account. These will be the initial local Message Store users that will have access to the shared account. The system administrator can choose from a list box that contains all the registered users of the Message Store. At least one user must be selected for a shared account. To select the members of a shared account, highlight the names of the users.

Click the ***Add*** button to include members for the shared account.

Note: *A notification screen appears once a user has been successfully added.*

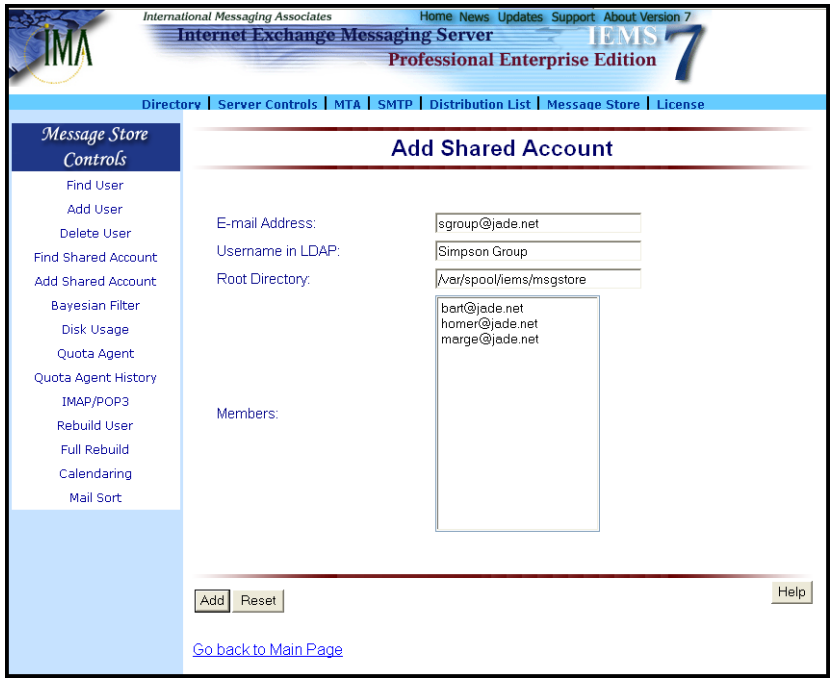

Figure 53: Creating A Shared Mailbox

Updating Shared Mailbox

The system administrator may update a Shared Mailbox account of a user by subscribing to or unsubscribing from a shared account. Once a user is subscribed to a shared account, he will receive messages destined for the shared account. Users may also send messages to the shared account. These messages will be received by the members of the shared account.

To update a shared mailbox account, click the **Update Shared Mailbox** link on the "Edit User Profile" screen (see Figure 50 on page 85). This action displays the shared account mailbox. Update the stored mailbox by removing or adding mailbox subscribers (see Figure on page 94).

To remove or add a mailbox, select the mailbox to be removed or to be added from the **Remove** or **Add** drop-down list. Click the Remove or Add button, respectively.

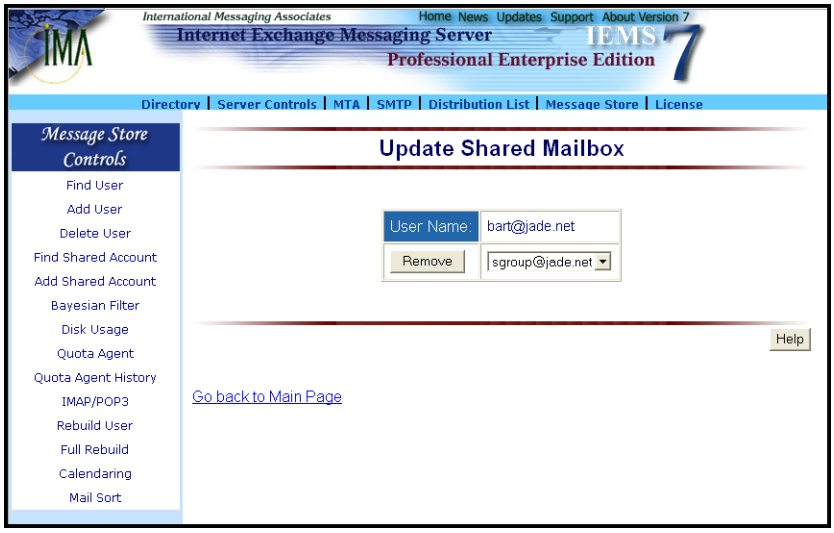

Figure 54:Updating Shared Mailbox

Displaying Shared Account Profiles

The system administrator may browse the list of existing shared accounts by clicking the ***Find Shared Account*** button on the left menu frame. This action displays the “Find Shared Account” screen (see Figure 55 on page 95). Search for shared account by typing either the Shared Name or email address (**Mail**) and clicking the ***Submit*** button. A subset listing of shared mailboxes in the Message Store will appear.

Note: *A specific search criteria may be entered to display a subset listing of users. For example, typing R* on the* ***Shared Name*** *field will list all shared mailboxes with names that start with the letter “R”. Use of wild cards (*) lists all of the shared accounts in the Message Store.*

Details of a particular shared account can be viewed by clicking either the **Shared Account Name** or the **Email Address** from the list. This action displays a table of the shared account information in the “Shared Mailbox Information” screen (see Figure 56 on page 96). The administrator is provided with the option to delete the shared account profile from the Message Store database.

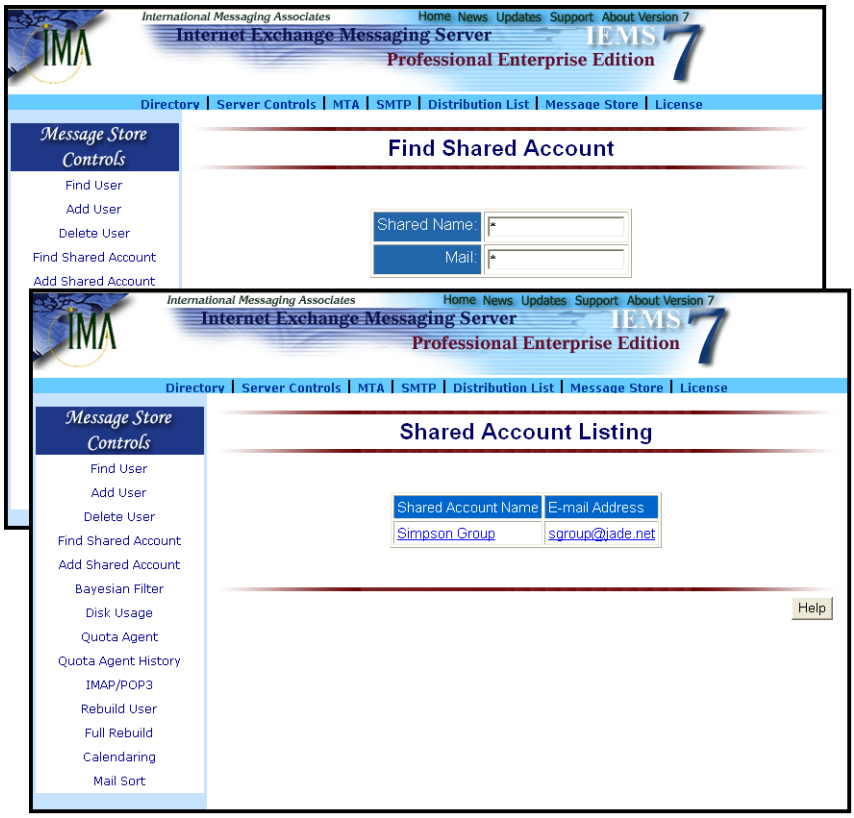

Figure 55: Listing Shared User Accounts

Deleting A Shared Account

The system administrator may delete a shared account via the “Shared Mailbox Information” screen (see Figure 56 on page 96). To delete, click the ***Delete*** button. A confirmation screen appears. Click the Delete button to remove the shared account.

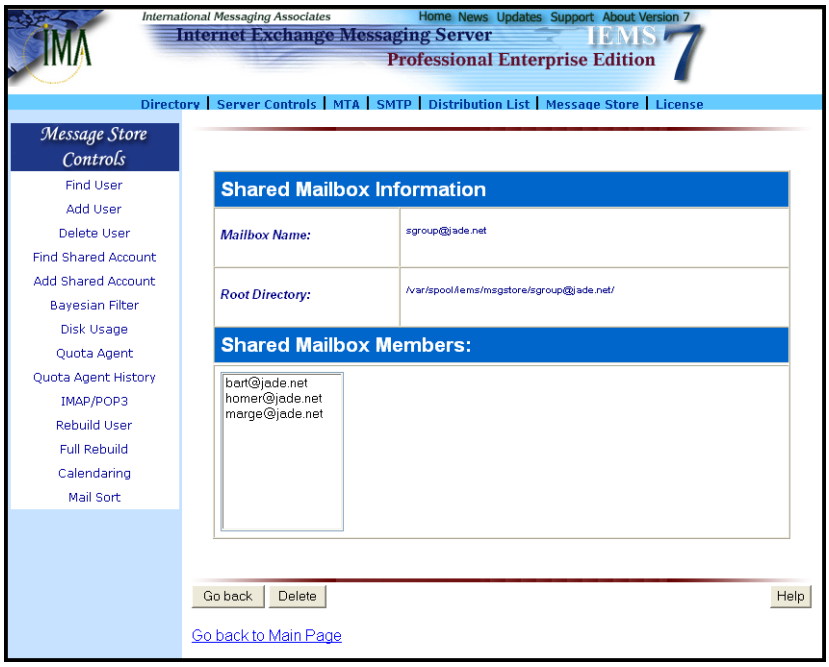

Figure 56: Displaying Shared Mailbox Information

Note: *Deleting the shared mailbox will also delete its home directory in the Message Store home directory and corresponding local connector in the Directory.*

Quota Agent

The Quota Agent allows a system administrator to set and enforce disk usage quotas on Message Store accounts. This feature limits the amount of resources allocated to individual users, preventing them from consuming all available disk space in the local Message Store.

Clicking the ***Configure Quota Agent*** button on the left menu frame displays the “Quota Agent Settings” screen (see Figure 57 on page 97). This interface allows the system administrator to set a **Default Size of User Account** (e.g. Unlimited) for the succeeding Message Store users. This means that the system administrator need not set the disk quota every time he creates a new user. Setting the default quota via this interface will not affect the disk quota limit of the existing Message Store users.

The **Warning Level** refers to the Threshold Setting of the Message Store Quota Agent. The default value for this attribute is 90%. This means that when the user’s disk space usage reaches 90% of the disk space allotted to his account, a warning message will be sent to that particular user stating that he is given a grace period from the date of notification to reduce his disk space usage below the allotted quota.

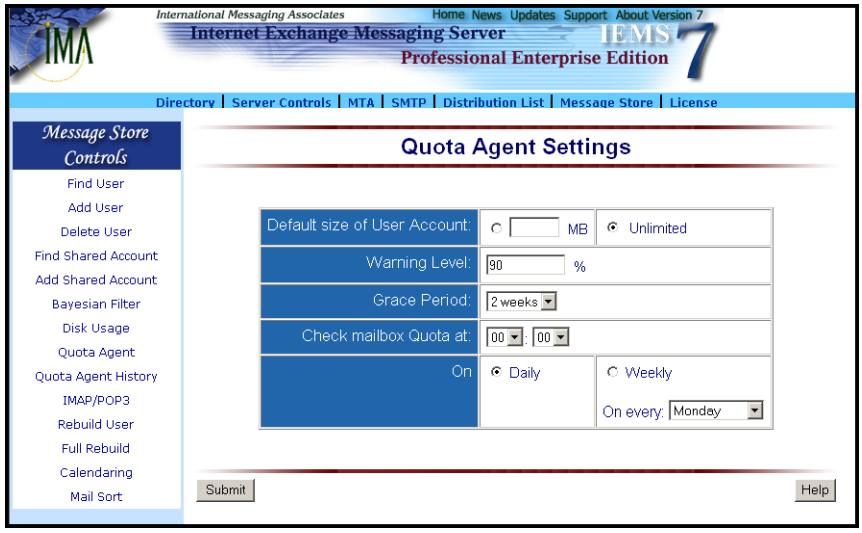

Figure 57: Configuring Quota Agent

Say, the user has a disk quota of 20MB, he will receive a warning message when his disk usage is already 18MB. The system administrator may change the default value.

A Grace Period is given to a user who has exceeded his disk quota. It tells the user to reduce his disk usage before this given time is over. The value for the grace period will either be one week or two weeks upon receipt of the notification message.

The notification message includes the date and the quota assigned to the user. The date is determined depending on the grace period. If the grace period is set for two weeks, the current date will be adjusted to two weeks ahead of time. This will be the grace period for the user to reduce his disk consumption below the allotted disk quota. The same applies if the grace period is set to one week.The quota will also be displayed.

When the grace period has expired and the user account still exceeds the disk quota, a notification message will be sent to the user stating that the account has been disabled. For tracking purposes, the system administrator will also receive a copy of the notification message sent to the Message Store user.

The system administrator may specify the time when the Quota Agent should start traversing and retrieving the disk quota and disk consumption of all the Message Store user in the **Check Mailbox Quota at:**. The system administrator should also set scheduling options either Daily and Weekly.

After specifying values for each parameters, click the Submit button. A confirmation screen indicates a successful operation.

Changing Quota Agent Settings

The system administrator may update the settings of the Quota Agent by clicking the ***Change Setting*** button on the "Quota Agent Settings" screen (see Figure 58 on page 98).

A new screen listing all the attributes found in the configuration page of the Quota Agent appears. In changing the setting, please refer to "Quota Agent" on page 96.

After the preferred values have been set, click the ***Update*** button for the changes to be implemented. A confirmation screen indicates a successful operation.

Note: *The* **Next Run Time** *specifies the schedule when the Quota Agent will start computing the disk space usage of all the Message Store users.*

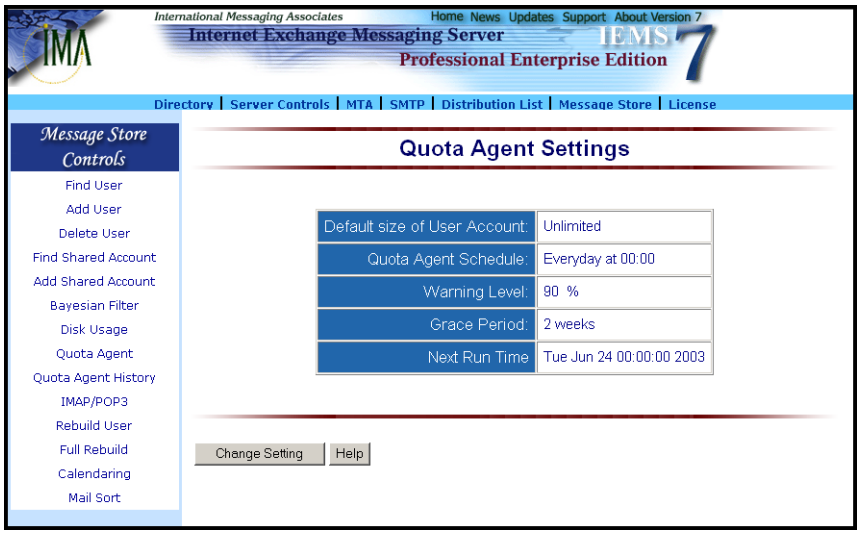

Figure 58: Changing Quota Agent Settings

Disk Usage

The Quota Agent can also generate reports in plain text or HTML formats. The plain text report is sent as a file attachment to the system administrator. The HTML format reports can be viewed via the "Disk Usage" web interface. These system reports enable the system administrator to monitor the total number of registered users and determine the users who have exceeded their disk quotas.

Clicking the ***Disk Usage*** button on the left menu frame enables the system administrator to generate the HTML report, which sorts all the users by their FQDN.

If the Quota Agent has been configured to compute for the disk usage, it displays the "Computing Disk Usage" screen (see Figure 59 on page 99).

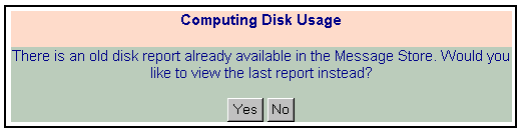

Figure 59: Computing Message Store Disk Usage

Since computing disk usage can be very time consuming especially for those who are managing thousands of Message Store accounts, the Quota Agent has been designed to let users choose to view previous Quota Agent Report. To view a previous report, click the ***Yes*** button. A screen indicating the last run time and run date of the Quota Agent appears (see Figure 60 on page 99).

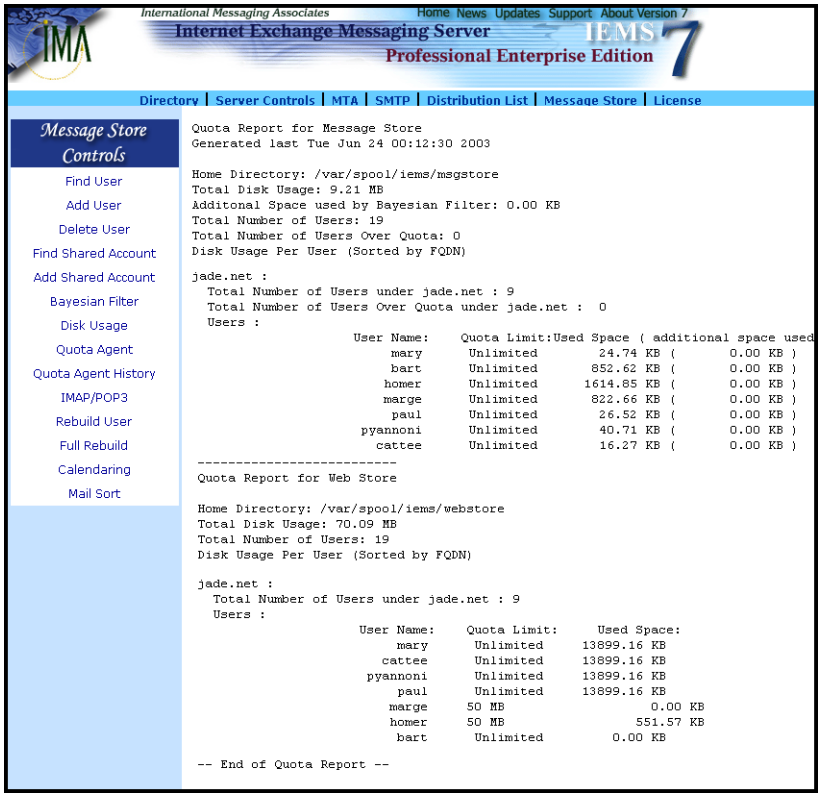

Figure 60: Viewing Previous Quota Agent Report

To compute for the latest disk usage, click the ***No*** button. The Quota Agent will start computing the disk usage for all Message Store users.

The “System Report for Message Store” screen (see Figure 61 on page 100) summarizes the Quota Status of the Message Store. The table displays the **Home Directory**, **Total Disk Usage**, **Total Number of Users and Total Number of Users Over Quota**. The program also sorts all the users by their FQDN. To display the profiles of the entire Message Store users with their respective disk usage, click the button from the field list.

Figure 61: Viewing Disk Usage

Viewing Quota Agent History Reports

The system administrator may view previous reports generated by the Quota Agent by clicking the ***Quota Agent History*** button. This action displays the "Quota Agent History Report" screen (see Figure 62 on page 101).

The history report includes the run time date of the Quota Agent engine. Each run time date is linked to a generated text file report. The run time date includes three attributes that summarizes the Quota Report. These attributes are: **Used Space**, **Total Number of Users** and **Total Number of Users Over Quota**.

Deleting Quota Reports

The system administrator may delete old quota report by marking the check box beside the **Run Time Date** and clicking the Delete button (see Figure 62 on page 101).

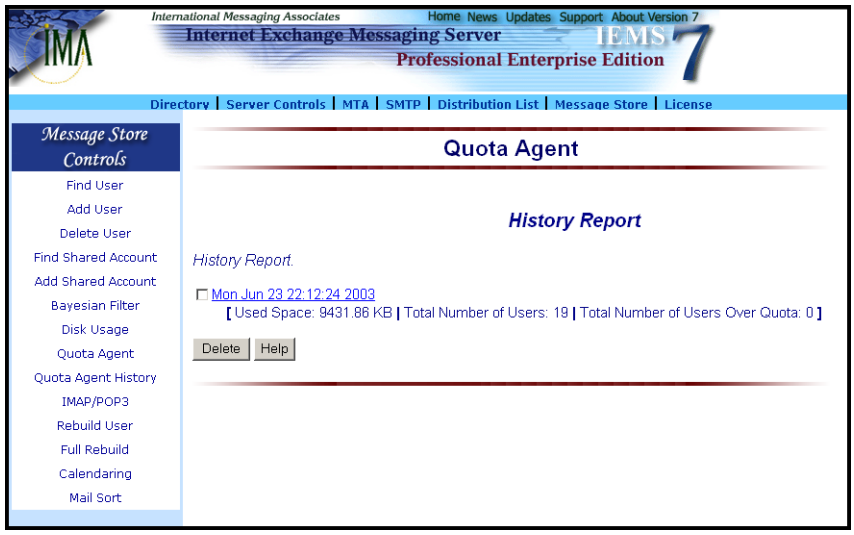

Figure 62: Quota Agent History Archives

Mailbox Maintenance

Under normal conditions, maintenance is not required for the Message Store accounts. However from time to time mailbox databases can become corrupted, resulting in mail delivery and/or remote access errors. This can happen for instance, when the system is not shut down properly. To resolve this problem, suspect mail folders, including the INBOX need to have the internal database files rebuilt.

IEMS stores uses separate databases for each folder and account configured into the system. By utilizing separate databases for these purposes, it is possible to keep individual database size small, as well as providing quick access time. The Message Store databases store pre-parsed information related to message content and folder hierarchy. The rebuild process recreates this information from the messages and folders present in the Message Store. Message Store databases may be rebuilt on a per-folder, per-user, or system-wide basis.

Rebuilding User and Folder Databases

To rebuild selected user accounts or individual folders, select the ***Rebuild*** button (see Figure 45 on page 80). This brings up the main **Rebuild Utility** screen.

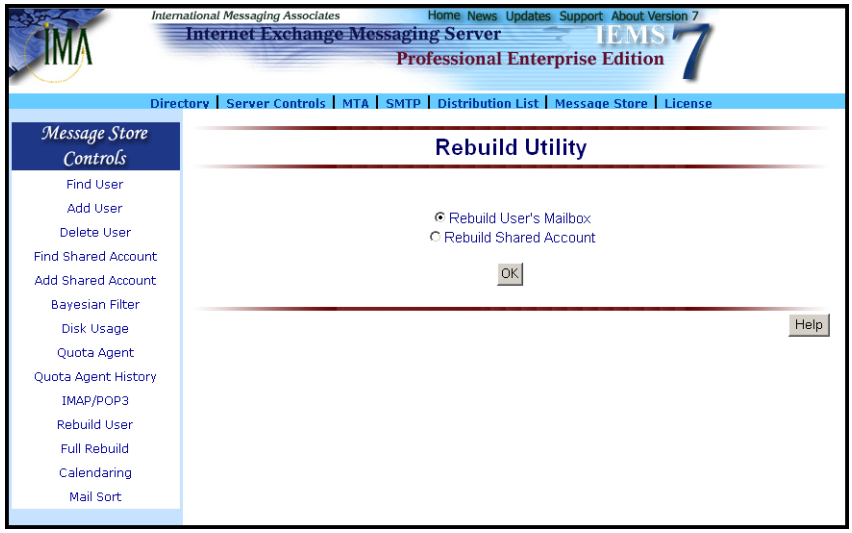

Figure 63: Rebuild Utility

To rebuild a shared account, select the Shared Account button, otherwise select the User's Mailbox button for normal User account maintenance. Once selected, click on **OK** to continue. This brings up the Rebuild Users screen (see Figure 64 on page 102).

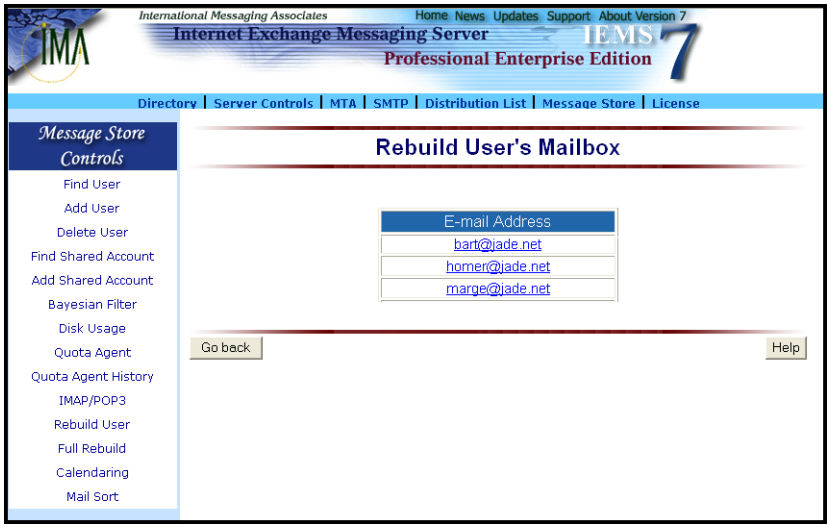

Figure 64: Rebuild Users Mailbox

From the Rebuild Users screen, the administrator can select the account which needs to be rebuilt. Simply click on the email address of the desired account for rebuilding, and the Rebuild Account screen will be displayed (see Figure 65 on page 103).

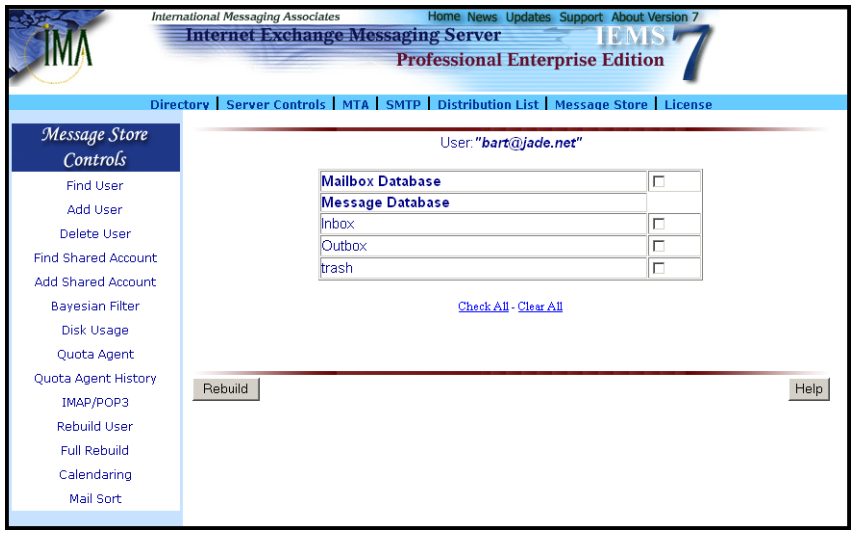

Figure 65: Rebuild Account

From the Rebuild Account screen, the administrator may select which database files are to be rebuilt. A single *Mailbox Database* is present for each folder, including the INBOX. It contains folder data. Information relating to each message in a folder are contained in the *Message Databases*. After selecting which databases to rebuild, click on the ***Rebuild*** button to continue. Upon completion of the selected database rebuild(s), the Rebuild Confirmation screen will be displayed (see Figure 66 on page 103).

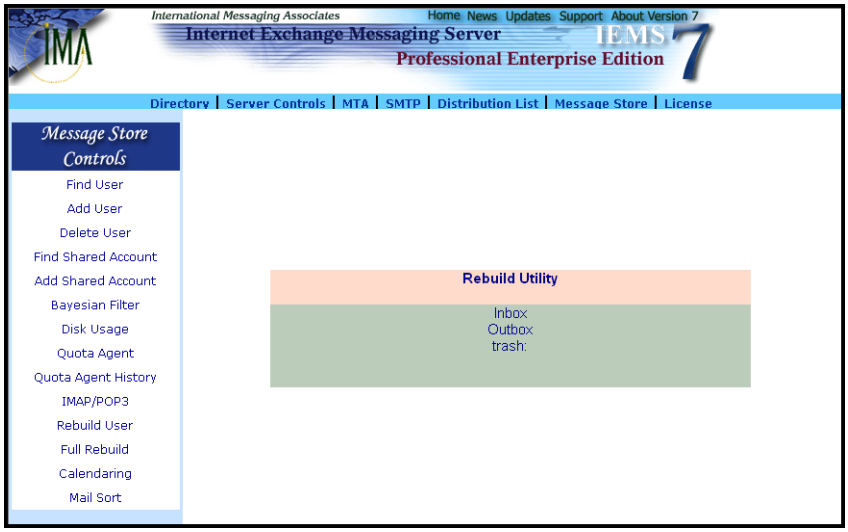

Figure 66: Rebuild Confirmation

Full Message Store Rebuild

Another option rather than having to select individual account and/or folders to rebuild, the administrator may elect to rebuild all the entire Message Store databases. To rebuild everything, select the ***Full Rebuild*** button (see Figure 45 on page 80). This will bring up the Full Rebuild screen (see Figure 67 on page 104).

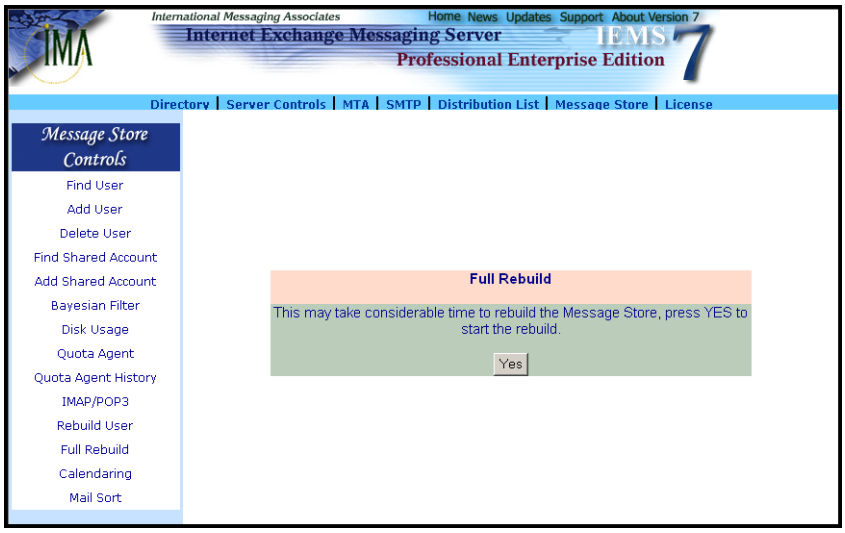

Figure 67: Full Rebuild

For large Message Stores, it may take a considerable amount of time to perform a full rebuild. The Full Rebuild screen requests confirmation for this potentially long operation. To continue, click the ***Yes*** button. This starts the full Message Store rebuild. After completion, the Full Rebuild Confirmation Rebuild screen is displayed (see Figure 68 on page 104). A list of each account and folder that is rebuilt is displayed here.

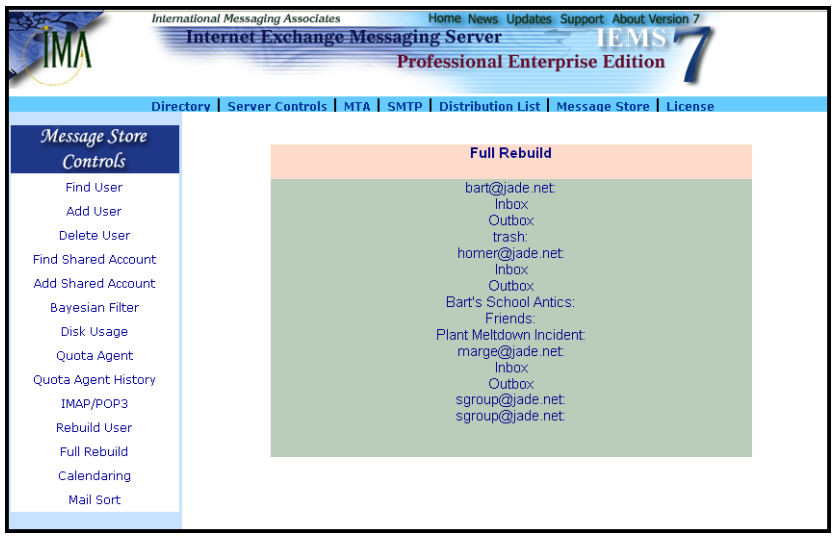

Figure 68: Full Rebuild Confirmation

Mailsort

The Mailsort filtering utility enables the system administrator and users to define rules so that incoming messages can be directed to pre-selected mailboxes or folders other than a user's Inbox, or selectively forward messages to other addresses. Mailsort process incoming mail at message delivery time based on user defined attributes (i.e., message sender, recipient or subject), reject messages or send automatic replies to incoming messages based on a predefined criteria.

To configure the Mailsort filter and vacation utility, click the **Mail Sort** link in the left menu frame. This action displays the "Mail Sort" screen (see Figure 69 on page 105).

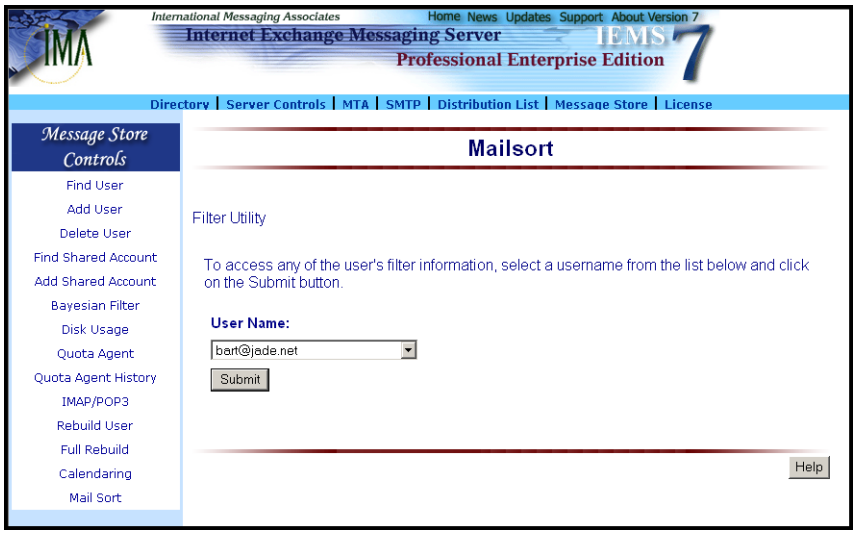

Figure 69: Mailsort

Note: *The system administrator needs to create a user account in the local Message Store before he can create a Mailsort filter file. He must also create a shared account in the local Message Store if he wants the user's messages to be delivered to a shared account.*

In configuring this module, the system administrator should refer to the **Internet Exchange Messaging Server 7 User's Guide**.

IMAP / POP Server Configuration

IEMS provides support for the reconfiguration of the IMAP and/or POP server ports that are used by the respective servers. In addition, if the site has an appropriate SSL server certificate, IEMS can be configured to communicate with remote mail clients using the secure version of IMAP (IMAPS) and/or secure POP3 (POP3S). Message store access via IMAP / POP3 as well as the Web Mail Client can also be configured to only permit clients from acceptable networks access.

IMAP 4 Port Reconfiguration

Clicking the ***IMAP/POP3 Configuration*** button on the left menu frame displays the "IMAP/POP3 Server Configuration" screen (see Figure 70 on page 106). To reconfigure the standard port for the IMAP server, simply enter the new port number in the field *IMAP Server Port Number*, and click on *Submit*. The default port for IMAP Version 4 is 143.

POP3 Port Reconfiguration

To reconfigure the standard port used by the POP 3 server, enter the new port number in the *POP3 Server Port Number* field and click on *Submit*. The default port for POP 3 is 110.

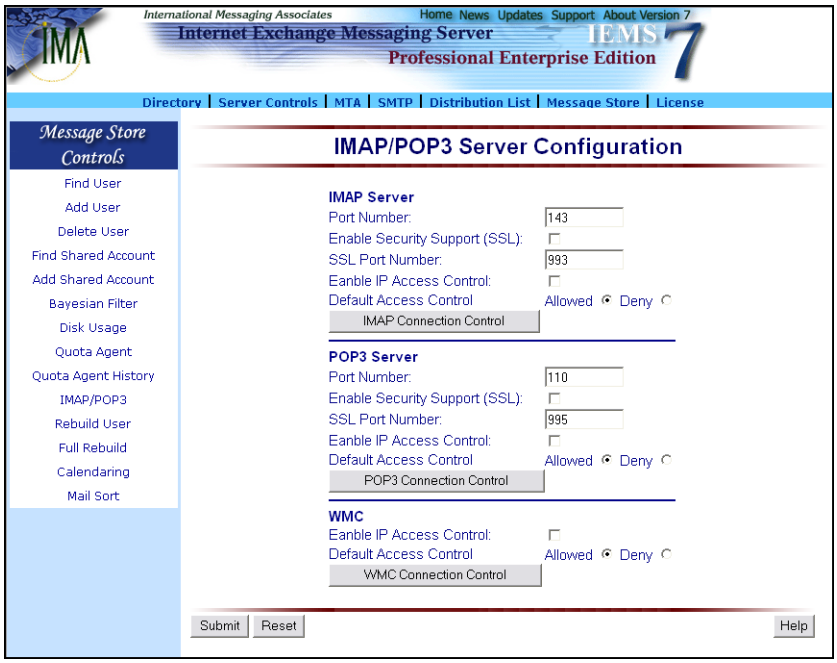

Figure 70: Configuring IMAP-4 / POP-3 Services

SSL Support For IMAP/POP

SSL (**S**ecure **S**ocket **L**ayer) is an industry standard, utilizing public key cryptography. It has been widely deployed in web applications by SSL-enabled web clients and servers. Originally designed by Netscape, it has undergone IETF standardization and is also known as TLS (**T**ransport **L**ayer **S**ecurity).

SSL provides three fundamental security services at the network transport layer - message privacy, message integrity, and mutual authentication.

IEMS includes a distribution of the public domain **stunnel** (Universal SSL Tunnel) and **OpenSSL** packages. Stunnel is a universal SSL enabler for networked applications. IEMS uses the daemon mode of stunnel, which accepts SSL connections for IMAP/POP3 and then connects to the IEMS IMAP/POP server running locally.

Note: *Due to patent protection, IDEA and RC5 algorithms have not been built into the IEMS distributed versions of either **stunnel** or the **openssl library**.*

Additional information about **stunnel** and **OpenSSL** can be found at:

http://www.stunnel.org
http://www.openssl.org

Before enabling SSL support for either the IMAP or POP servers, a server certificate must be installed on the IEMS machine. For details on how to obtain or generate a server certificate, please see Appendix C.

Configuring SSL Support for IMAP/POP Services

Once a site certificate has been obtained and installed, SSL support can be enabled for either the IMAP and/or POP servers. To enable SSL support, simply select the *Enable Security Support (SSL)* box of the appropriate server and then depress the *Submit* button. If alternate port numbers are needed for either IMAPS or POP3S these can be entered into the appropriate *SSL Port Number* fields. The standard ports used by IMAPS and POP3S are 993 and 995 respectively.

POP3 / IMAP / Web Mail Client Access Control

For each way that the Message Store can be accessed (POP3, IMAP and the Web Mail Client), the administrator can set IP access control lists for. Each access method has an associated ***Connection Control*** button associated with it (see Figure 70 on page 106). Once clicked, the system administrator can list the banned or blocked IP addresses for each access method (see Figure 71 on page 108).

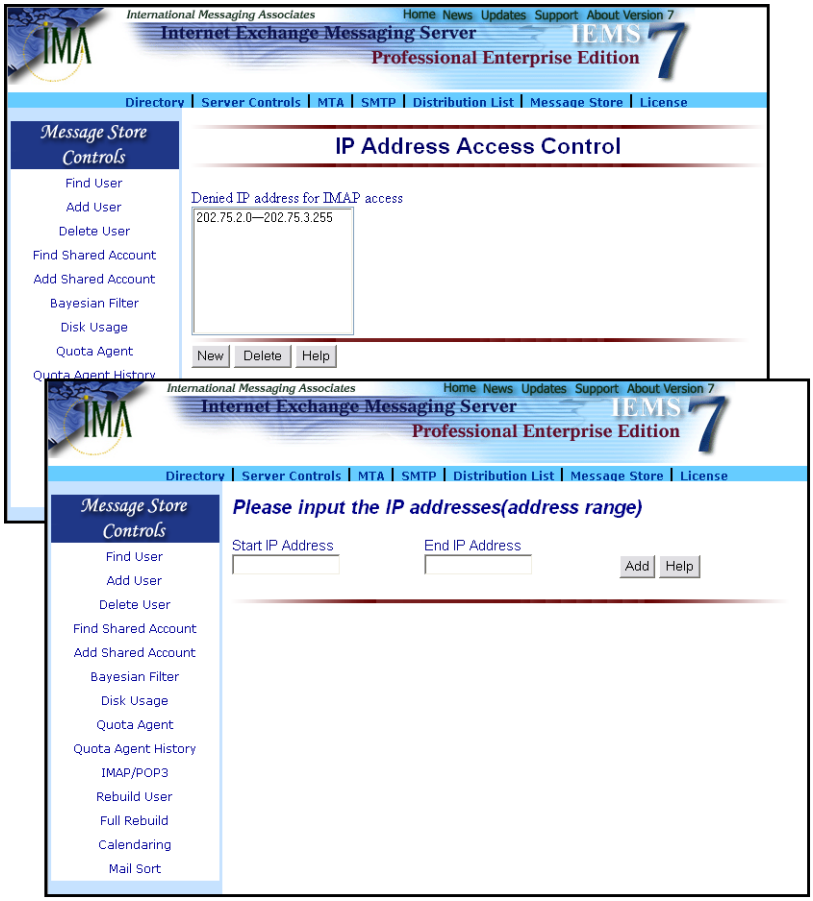

Figure 71: Message Store Access Control Selection

Calendaring and Scheduling

The Professional Enterprise Edition of IEMS provides backend server support for the Microsoft Outlook 98 / 2000 calendaring and scheduling features. In particular, IEMS provides a public file server for the publishing of Internet Free/Busy (IFO) information. Outlook users can share calendaring information between themselves, and schedule meetings via Internet email.

Microsoft Outlook Internet Free / Busy Feature

The Internet Free/Busy (IFO) feature of Outlook 98 / 2000 (Internet Mail Only mode) allows users to see when others are free or busy in order to efficiently schedule meetings. Users publish their busy/free information to an IEMS shared file server. Each user's schedule information is published at a unique URL specific to the individual. Users can then share the information at this location with all users, or any specific users determined by each user. Access to busy/free information is controlled through the configuration information supplied by each user to the IEMS file server.

IEMS Free/Busy Server

Individual Free/Busy information is published from Outlook to an IEMS Free/Busy Server. This server is implemented as a specialized FTP server residing on the IEMS host. All access to information on the IEMS server must be authenticated by providing login information (done through the individual Outlook configurations). This login information is authenticated against account information stored in the IEMS Directory. Once authenticated, users can update their schedules, or access other's schedules, provided they have appropriate access rights.

Users control access rights to their free/busy schedules through the IEMS Web Mail Client. Using this simple interface, users can easily create and maintain access control lists of users permitted to view the free/busy schedule information.

Internet Free / Busy Access Control

Each user can control which users have access to their free/busy information. In addition, the system administrator can access and configure any access control list for each IEMS user. To configure the free/busy access control for a given user, click the ***Calendaring and Scheduling*** button (see Figure 72 on page 109). Select a user from the pull down menu and click the *View* button to display or edit the user's access control list.

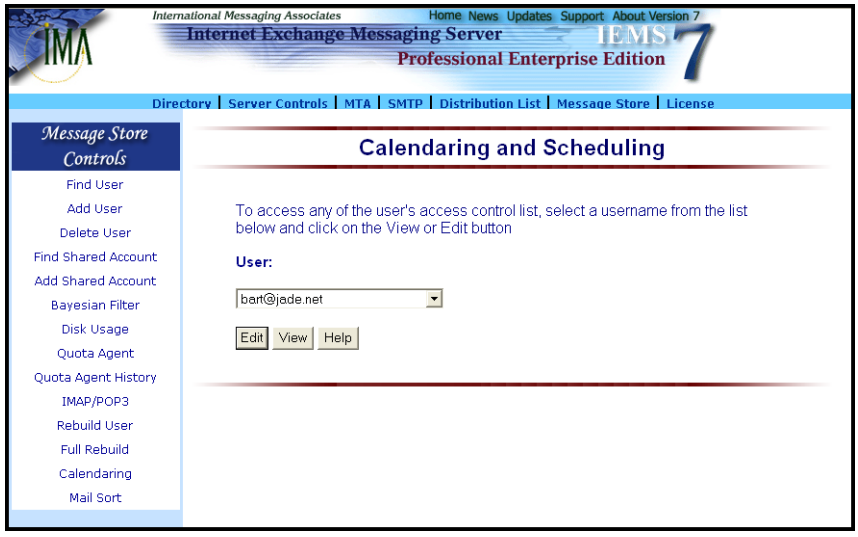

Figure 72: Calendaring and Scheduling User Selection

Once a user has been selected, the following screen will be displayed showing users allowed to access the selected user's free/busy information:

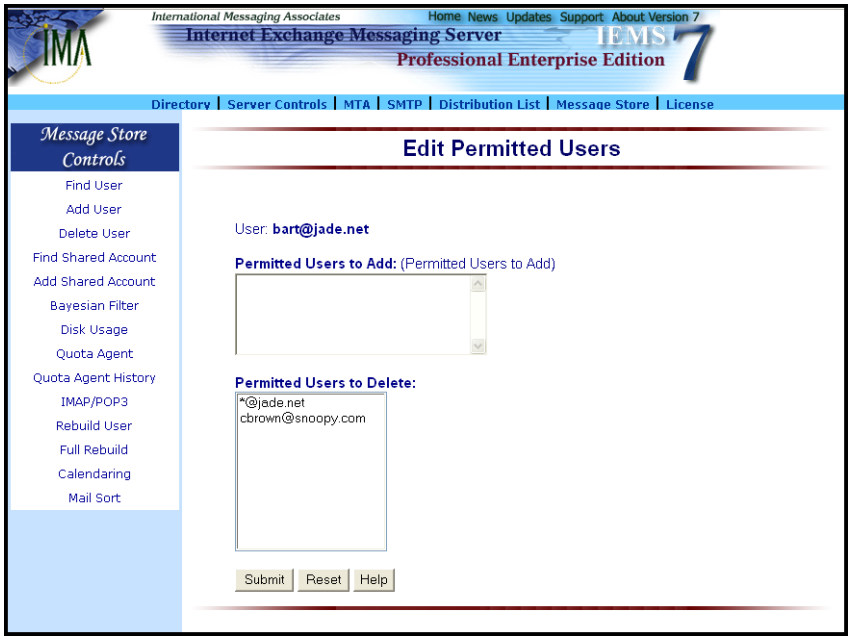

Figure 73:Edit Permitted Users

In this screen you can add the permitted users in the upper text box. The wildcard characters "*" and "?" representing multiple and single character matching respectively are supported. If the permitted user is a distribution list, all members of that list, including sub-lists will be permitted access to the user's free/busy schedule.

REBUILD

Rebuild is a command line utility used rebuild internal Message Store databases.

NAME

rebuild - Internet Exchange Messaging Server - Message Store rebuild utility

SYNOPSIS

rebuild [-f] | [user [mailbox]]

DESCRIPTION

The **rebuild** utility is used to rebuild the internal databases that Message Store applications use to speed up access to mail data. Recover is used to recover from almost all forms of database corruption in the Message Store.

To use the **rebuild** utility, it is recommended that all Message Store applications are first terminated as listed below:

IMAPD
POP3D
Message Store Server
Locmail Server
LMDA

Shutting down the above modules will enable the **rebuild** utility to rebuild users databases faster because no other modules will be competing with it for the locking and access to the databases.

OPTIONS

Rebuild may be run in one of three different modes:

-f Rebuild the entire message store. **Rebuild** will traverse all accounts and rebuild all related database files in all folders and sub-folders. This may take some time, and should not be interrupted.

user@domain.com
Rebuild of a single user account, user@domain.com. **Rebuild** will rebuild all the folders and sub-folders for the specified user.

user@domain.com folder-name
Rebuild of a single folder. **Rebuild** will rebuild only the given folder - no other folders will be rebuilt. It is usually better however to rebuild an entire user account, as this will update the folder databases as well as the message databases.

EXAMPLES

rebuild -f
Rebuilds the entire message store.

rebuild user@domain.com
Rebuilds all the folders and sub-folders for the user user@domain.com in the local Message Store.

rebuild user@domain.com inbox
Rebuilds the inbox folder for the user user@domain.com in the local Message Store.

FILES

/opt/iems/bin/rebuild
Default location for the rebuild utility

/var/spool/iems/msgstore
Default location of the Message Store

IEMSUSER

Iemsuser is a command line utility used to create, delete, and list IEMS Message Store accounts.

NAME

iemsuser - create / delete / list IEMS Message Store accounts

SYNOPSIS

iemsuser [options]

DESCRIPTION

The **iemsuser** program is a command line utility used to allow IEMS administrators to manipulate user accounts directly, rather than through the standard IEMS web interface. This utility can be used from a script to create a batch of IEMS users automatically. This utility is enabled only with the Professional Enterprise Edition of IEMS.

OPTIONS

-C Create a new IEMS user account.

-D Delete an existing IEMS user account.

-L List all IEMS user accounts.

-a ADDR

Specify address for -C or -D options. ADDR is the full email address of the IEMS user.

-p PASSWD

Specify password for -C option. PASSWD is the password to set for the IEMS user. This must contain at least 6 characters.

-l LNAME

Users Last Name for -C option. LNAME is the Last Name to set for the IEMS user.

-f FNAME

Users First Name for -C option. FNAME is the First Name to set for the IEMS user.

-h HDIR

Users home directory for -C option (optional). HDIR is the pathname to the IEMS user mailbox.

-r PERM

Send / Receive permission (optional). Enabled by default. Possible values for PERM are send, receive, and send+receive.

-q QUOTA

Message store quota (optional). When creating a new account, this defaults to Unlimited. Values are in MB.

-w WEBFOLDER

Users home web folder directory for -C option (optional). WEB-FOLDER is the pathname to the IEMS user web folder.

-m WPERM

Enable / Disable permission for web folders (optional). Disabled by default. Possible values for WPERM are enable and disable.

-t WQUOTA

Web Folder quota (optional). Values are in MB.

EXAMPLES

To create an IEMS account for Bart Simpson with an email address of bart@jade.net, Message Store quota 100M, and Web Folder quota 50M:

```
iemsuser -C -a bart@jade.net -p password -f Bart -l Simpson -q 100  -t 50
```

CHAPTER 5

Directory Services

Overview

The Directory Server is used as the central database for user profiles, mail routing and module configuration parameters. It also allows clients to issue multiple requests concurrently. The Directory Server also provides an authentication service, restricting access to sensitive information, such as passwords and confidential user profiles. Operations are provided for adding and deleting an entry from the directory, modifying an existing entry and searching for a particular entry. The search operation allows some portion of the directory to be searched for entries that match the criteria specified by the search filter.

IEMS Directory Services are based on a client/server architecture that uses LDAP (Lightweight Directory Access Protocol). LDAP is an open directory access protocol. The IEMS Directory is designed for managing information about users, groups, mailing lists, aliases processing and mail routing.

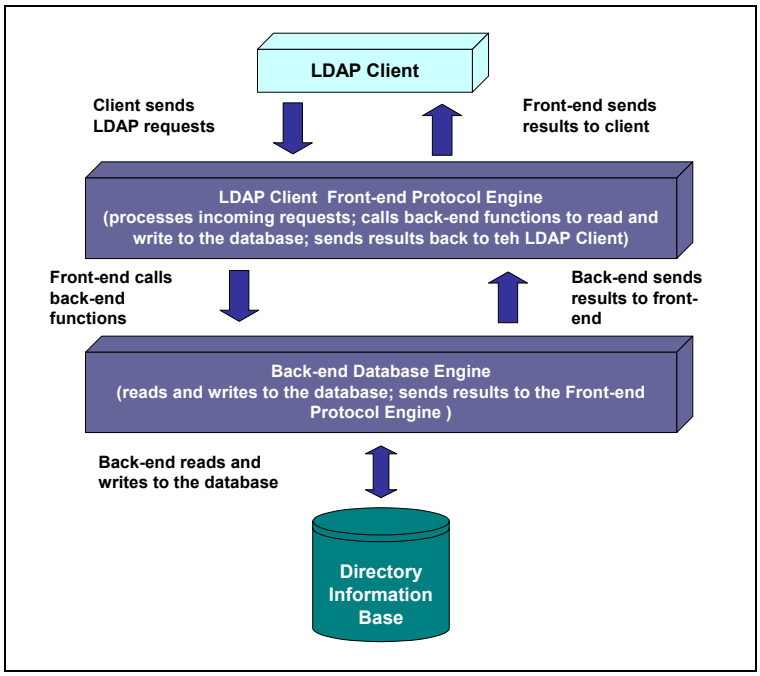

Figure 74: Directory Services system architecture

Note: Starting with release 7.1, the Linux release of IEMS uses the supplied OpenLDAP directory shipped with most Linux distributions.

IEMS Directory Services (see Figure 74 on page 115) consists of two major subsystems: the front-end protocol engine and the back-end database engine. The front-end protocol engine receives requests from the client and processes these requests by invoking read-and-write functions in the back-end database engine. Among the operations performed by the front-end protocol engine are bind, unbind, search, modify, modify RDN (Relative Distinguished Name), delete and abandon operations. The back-end database engine searches for information in the directory and modifies it based on commands from the protocol engine.

The IEMS Directory Server allows clients to issue multiple requests at once. If a client searches the directory and multiple matching entries are found, each of the entries are sent to the client. The Directory Server provides an authentication mechanism, restricting access to sensitive information, such as passwords and confidential user profiles. Operations are provided for adding and deleting entries from the directory, modifying an existing entry and searching for a particular entry. The search operation allows some portion of the directory to be searched for entries that match some criteria specified by a search filter. Information can be requested from each entry that matches the criteria.

Directory Data Storage

IEMS uses a default directory schema for email applications. The directory data includes information about user accounts, groups, and mail routing. The user account information consists of the unique user id (email address), user password, and other user-related profiles. The group information consists of data about the users that have the same access right to the same directory General information, like email addresses and usernames, can be accessed by the LDAP client. Access to sensitive information, such as password and confidential user profiles, is restricted by an authentication mechanism.

Directory Information Tree

Directory entries are organized using a DIT (Directory Information Tree). The root of the DIT is represented by a special entry whose DN (Distinguished Name) is called the Directory Suffix. The IEMS design is based on RFC-2377 which recommends the LDAP directory structure to be based on the domain part of a user's email address. IEMS uses the "mail" and "dc" components to construct the directory tree.

User Records

To configure Directory Services, click the **Directory** link on the top menu frame. This action displays the “Directory Services” screen (see Figure 75 on page 117).

Figure 75: Directory Services

Creating New User Records

In configuring Directory Services for the first time, it is necessary to create at least one user before being able to configure the rest of the parameters. To create a user, click the ***Add Users*** button on the left menu frame. This action displays the “New User” screen (see Figure 76 on page 118). Type the first name, last name, telephone numbers, address, and email address of the user to be added in their respective fields. After entering all the required information, click the ***Create User*** button. The “User Details” screen confirming that you have successfully created a new user appears.

Editing Existing User Records

The system administrator may modify or edit a user profile whenever changes occur regarding personal or mailbox information. The system administrator may update user profile entry by supplying the correct information in the text boxes provided.

On the “User Details” screen (see Figure 76 on page 118), click the ***Edit*** button. This action displays the “Edit User” screen (see Figure 77 on page 118) where user attributes can be modified. Change either the first name, last name, telephone number, address and/or the email address of the user.

After making the necessary changes, click the ***Update*** button.

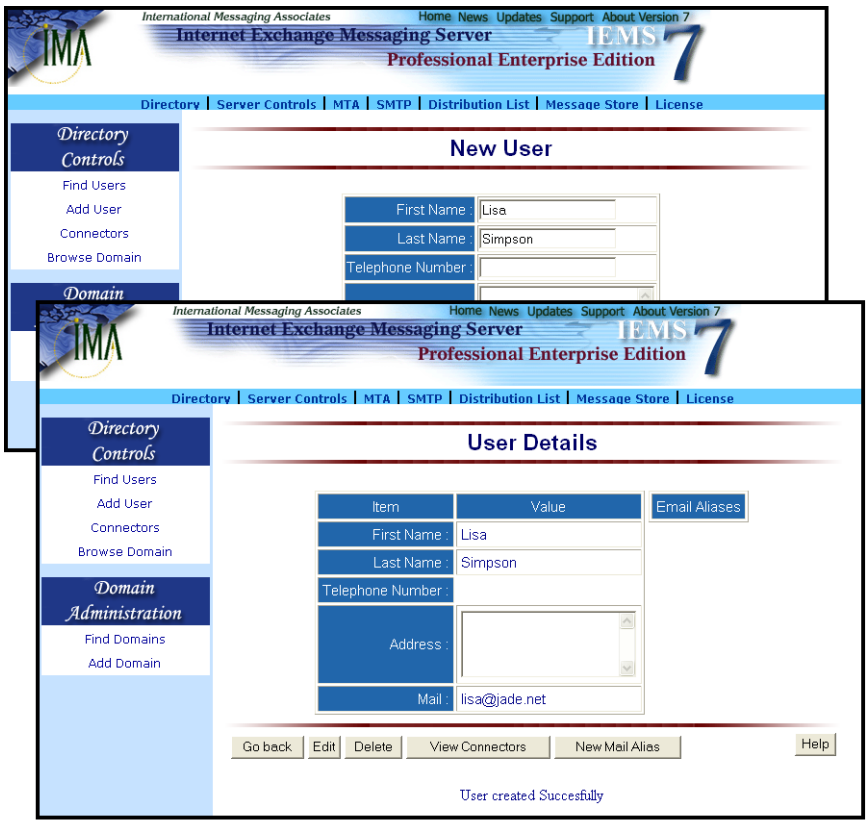

Figure 76: Creating Or Adding A User

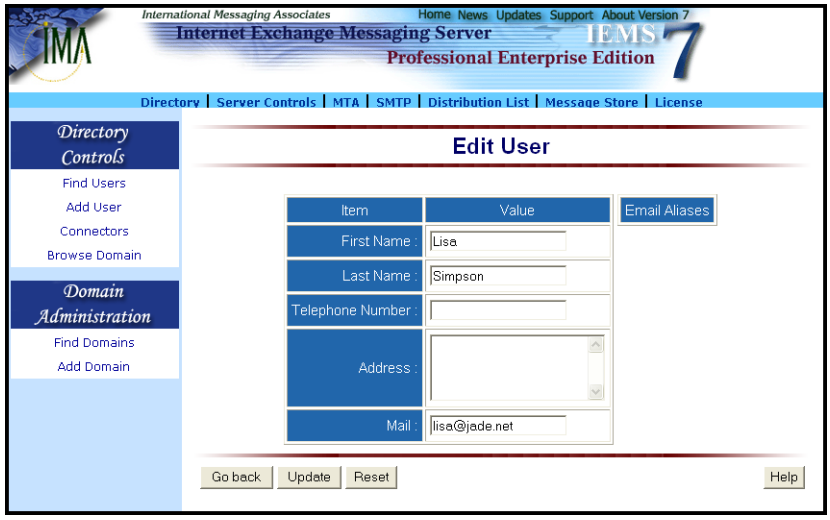

Figure 77: Editing User Information

Deleting Existing User Records

The system administrator may also delete user profiles from Directory Services. On the “User Details” screen (see Figure 76 on page 118), click the ***Delete*** button. This action displays the “Delete User” screen. Click the ***Confirm*** button to delete the user from the directory.

Finding Users

The system administrator may search or view the list of users or mailing lists defined in the Directory. To do this, click the Find Users button on the left menu frame. A subset listing of the search results will be displayed containing the different attributes of the users and mailing lists on the “Find User Menu” screen (see Figure 78 on page 119).

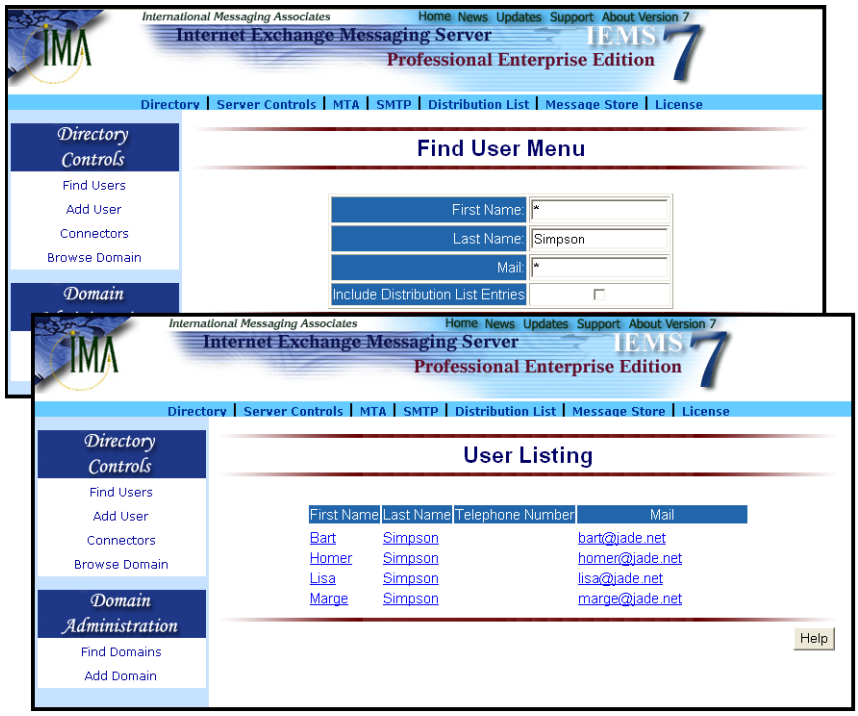

Figure 78: Finding A User

Type the first name, last name, and email address of the user to be found. Mark the **Include Distribution List Entries** check box if you wish to include distribution list entries recorded in the Directory Services.

Note: *The system administrator may also use wildcards (asterisks*) in any and/or all of the text fields. Use of asterisks in all fields displays all the entries recorded in the database.*

After entering all the parameters required, click the ***Find*** button. If Directory Services finds a user whose attributes match those entered by the system administrator, a new screen displaying the list of user(s) appears.

To view the attributes of the user, click the **Last Name**, **First Name** or **Mail** link. A screen displaying the user’s details appears.

Connectors

IEMS uses connectors to associate directory entries with delivery or routing information. Connector information is used by the preprocessor for determining how messages are to be handled for a given address (record) once received by the system. IEMS connectors include the following default channels: LOCAL, SMTPC, BSMTPOUT, DL, NOTES and CC:MAIL.

Each connector is identified by its name, the identifier for that connector, and the permission level. The permission level can be configured for each connector. However, IEMS for Windows only applies this option for the cc:Mail and Notes connector modules.

To create connector(s) for a user, click the ***View Connectors*** button on the User Details. screen (see Figure 76 on page 118). This action displays the "View Connector" screen (see Figure 79 on page 120) where you must click the New button. A screen for creating a connector appears.

Note: *If you already have created a connector for the existing user/identifier, this screen displays the existing connector(s) under the* **Connector** *column.*

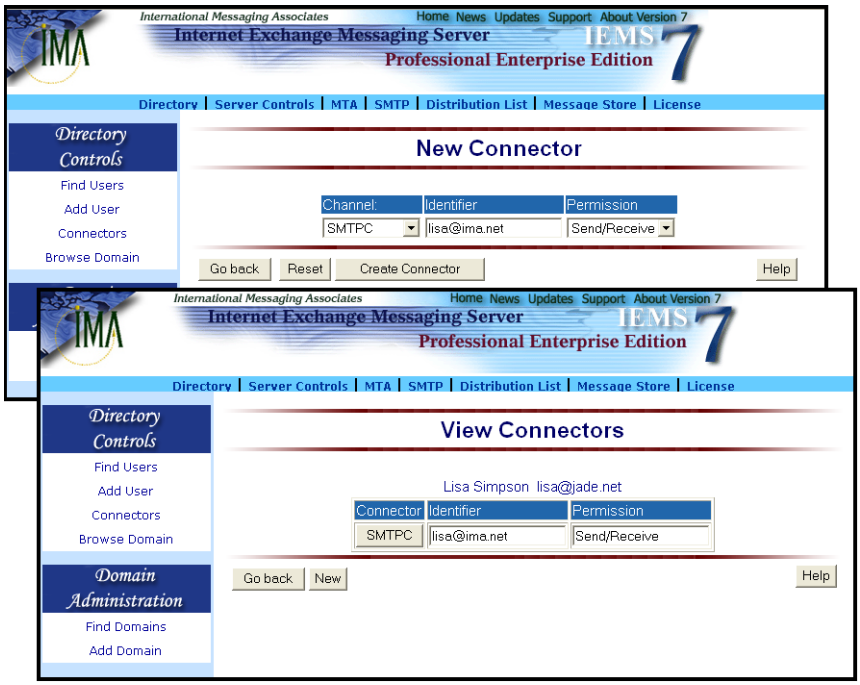

Figure 79: Creating Or Adding A Connector

Select the channel (e.g. LOCAL) to be added from the pull-down menu and type the corresponding identifier (e.g. *john@music.ima.com*). The identifier enables the Directory Services to identify the recipient to which a specific connector is assigned.
The identifier to be used should be either an Internet email address, cc:Mail address, Notes address, or local Message Store user.

Select the permission level **None**, **Send**, **Receive** and **Send/Receive** from the pull-down menu. Selecting **None** does not allow the user to receive and

send messages. The **Send** permission allows the user to send messages, but is not allowed to receive messages. The **Receive** permission allows the user to receive messages, but is not allowed to send messages. The **Send/ Receive** permission allows the user to send and receive messages.

Note: *The Send and Receive Permissions are allowed only for the cc:Mail and Notes connectors. For the Message Store, only None and Receive Permissions are allowed. Permission is not applied to other channels such as DL, SMTPC, and BSMTP.*

After selecting a connector for the user and specifying the connector's attributes, click the ***Create Connector*** button.

Note: *You may delete the connector by clicking the* ***Delete*** *button below the Connector column. A connector information screen where you can either edit or delete the entry from the database appears.*

Listing Connectors

The system administrator may view the list of available connectors by clicking the ***Connectors*** button on the left frame menu. This action displays the "List Connector" screen (see Figure 80 on page 121).

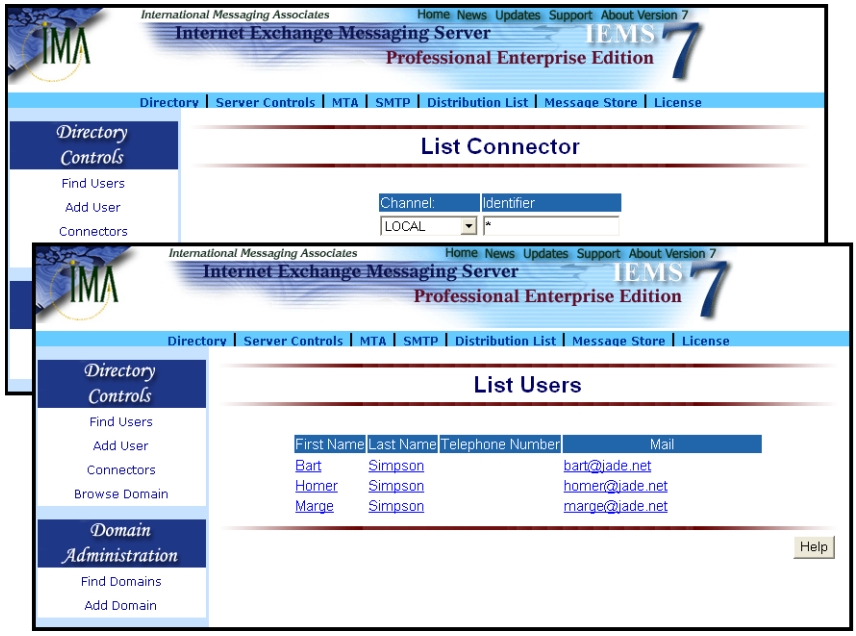

Figure 80: List of Users For A Specified Connector

Select a connector from the pull-down menu. Type the identifier for the particular connector. Click the ***List*** button. This action displays the user(s) for that connector.

The administrator may also view the attributes of the users by clicking either the **Last Name**, **First Name** or **Mail** link on the "List Users" screen.

Mail Aliases

Directory Services allows the system administrator to create mail aliases for individual users enabling them to maintain several email addresses. When a mail alias is defined for a particular user, the messages sent to his alias address will be treated the same as if addressed to the primary address.

On the “User Details” screen (see Figure 76 on page 118), select the ***New Mail Alias*** button. This action displays the “New Alias” screen (see Figure 81 on page 122).

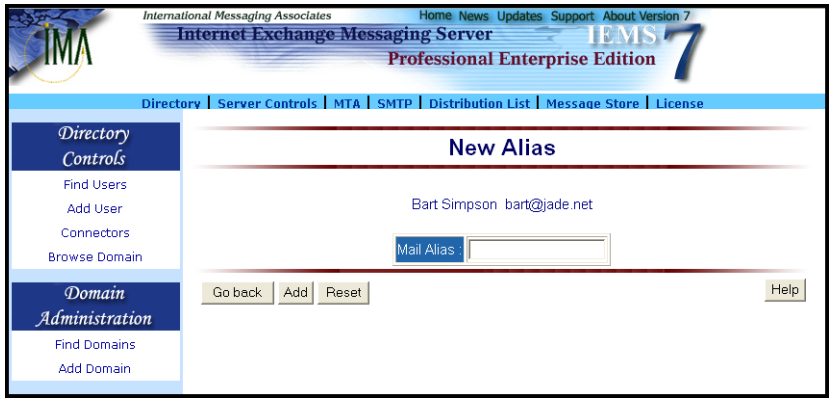

Figure 81: Creating An Alias

Type the new mail alias (e.g. *john@ima.com*) for the entry selected. Click the Add button. This will serve as an alias address for the user who uses *jdoe@ima.com* as his email address.

If you already have an alias for a particular user, the **Email Aliases** column displays the alias for that user. You may edit or delete the alias by selecting its link.

Note: *After creating an email alias, the system will automatically check every few minutes to see if it is necessary to rebuild the alias database. The administrator can also manually rebuild the alias table in the Preprocessor configuration web interface at any time.*

Browse Domains

The ***Browse Domain*** button allows the system administrator to browse the locally configured domains. A sub-domain of the local domains will appear after displaying the local domain. The system administrator may also view the list of users for the selected domain or sub-domain.

In the example shown in Figure 82 on page 123, the domain used is *com*. A sub-domain of this domain will appear after clicking the **com** link (e.g. the domain is *com* and the sub-domain is *ima.com*). If you are using the *ima.com* domain, for instance, click the ***Find users in ima.com*** button to show the *ima.com* user(s).

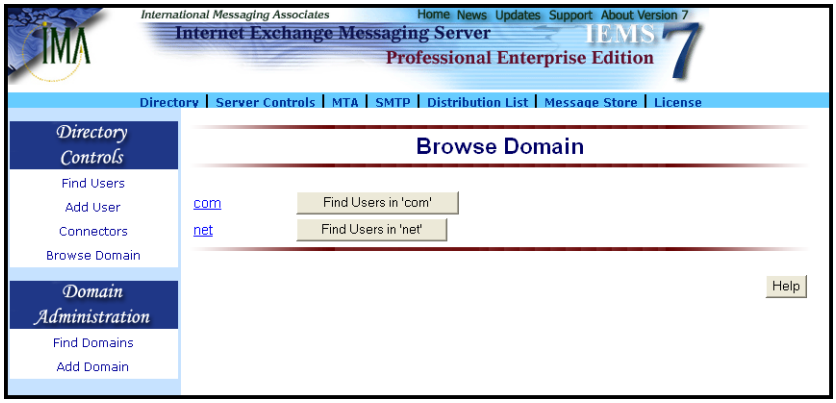

Figure 82: Browsing Domain

CHAPTER 6

SMTP

Overview

The Internet Exchange Messaging Server (IEMS) communicates with mail hosts on the Internet using the **S**imple **M**ail **T**ransfer **P**rotocol (SMTP). This protocol is used for the submission as well as the reception of mail messages. IEMS implements SMTP as two separate modules. A client program (SMTPC) sends messages from the gateway to the Internet, and a server program (SMTPD) receives messages from the Internet bound for the local environment.

While most Internet email is directly transported via SMTP (Simple Mail Transfer Protocol), there are times when other forms of message transports are more desirable. IEMS also supports a Batch version of SMTP (BSMTP) for these situations. This alternative transport method is useful in situations where:

- A dedicated IP (Internet Protocol) address is not available
- Low message volume
- Higher costs associated with dedicated Internet connections
- Internet connection is available only on a dial-up basis

Simple Mail Transfer Protocol Client (SMTPC)

SMTPC (Simple Mail Transfer Protocol Client) is the component responsible for delivering messages to the Internet. It regularly polls for messages queued in the SMTPOUT channel. When messages are found, it establishes the required number of connections with external SMTP servers and transfers the messages to the appropriate Internet mail hosts. SMTPC like SMTPD also has a multi-threaded architecture (see Figure 83 on page 126) that assures high scalability and performance. It consists of a Queue Router and Queue Manager. The *Queue Router*, which retrieves outgoing messages from the Input Queue, determines whether the message should be routed to the Pending Queue or Deferred Queue. The *Queue Manager* controls and synchronizes the Pending Queue and the Deferred Queue.

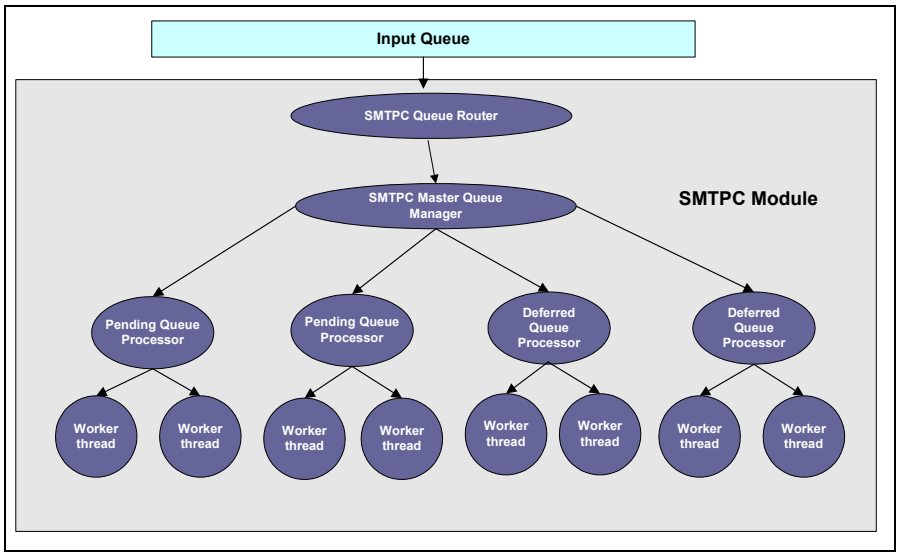

Figure 83: SMTPC system architecture

SMTPC features a hierarchical multi-threaded architecture, which assures high scalability and performance. The pending queue temporarily stores messages that are to be sent out immediately. Messages which previous delivery attempts have failed or intended for later delivery are stored in the deferred queue.

SMTPC features a mechanism for message priority handling that guarantees not only high throughput, but also the orderly handling of messages with different priorities. It uses several criteria when routing Internet messages.

Pending Queue

Newly arrived messages that must be sent out immediately are placed in the Pending Queue. These messages are processed by the Pending Queue Processors, which attempt delivery via SMTP. If the delivery of a message in the Pending Queue is unsuccessful, it is transferred to the Deferred Queue so that it can be delivered at a later time. Messages destined for intermittently connected hosts with ETRN (Extended Turn) support do not go through the Pending Queue; those messages are sent directly to the Deferred Queue.

The system administrator can configure the queue run interval for each Pending Queue Processor by defining the maximum number of Pending Queue Processors that will run concurrently and the number of messages to be processed by each processor during each queue run. The number of pending messages will be displayed for each SMTP channel. Each Pending Queue Processor is capable of creating multiple threads for handling multiple SMTP sessions at the same time.

Deferred Queue

Messages intentionally deferred or whose previous delivery attempts have failed are placed in the Deferred Queue. These messages are further grouped into different SMTP domain channels using the recipient address information. This allows server-side ETRN support and prevents deferred messages from delaying the processing of urgent messages. A message is placed in the Deferred Queue if any of the following reasons is encountered:

- The option queue mail before attempting delivery is enabled. This causes messages to be placed in the deferred queue and not to be delivered immediately. This is particularly useful if the destination domain is an ETRN SMTP domain.
- There is a temporary DNS error during the domain name resolution process.
- A destination host is found, but an SMTP connection cannot be established.
- The destination SMTP server issues a temporary SMTP response code.
- The SMTP connection is aborted prematurely due to network problems.
- The destination SMTP server did not reply within the configured time.

The number of deferred messages, deferred reason and next queue retry time are displayed for each SMTP channel. Messages in the Deferred Queue are processed by the Deferred Queue Processors on a per channel basis. During each scheduled queue run time, one or more Deferred Queue Processors are created for every SMTPC domain channel by the SMTPC component to handle deferred outgoing messages. Messages for each SMTPC domain channel are processed according to their message priority weight.

SMTPC will attempt to deliver the first message for each SMTP Domain Channel. If the delivery attempt is successful, the Queue Processor will create another SMTPC thread to deliver subsequent messages. Otherwise, all subsequent messages in the entire channel will remain queued. This approach greatly improves the overall efficiency of resource usage by eliminating unnecessary message delivery attempts.

It is advisable to queue all the messages for a particular domain (such as ETRN domains) before attempting delivery. When an ETRN host is connected, it makes an ETRN request to SMTPD, which notifies SMTPC. SMTPC then instructs a Deferred Queue Processor to deliver all queued messages for this domain immediately. Since messages for this domain are already grouped, this approach ensures less processing time and fast delivery.

Shared Message Queue Structure

A shared message queue structure is designed for both Pending Queue and Deferred Queue to achieve efficient usage of system memory. Each queue can have one or more queue processors active at a time, each of which will further create multiple SMTPC worker threads to process multiple outbound messages simultaneously and send them to their next destination across the Internet.

SMTPC also supports the following ESMTP service extensions: DSN, SIZE, ETRN remote queue start up (primarily for offline or disconnected access) and 8-bit MIME transports.

ETRN Support

ETRN is an SMTP command issued by SMTPC when connecting to a remote SMTP server. With ETRN support, SMTP hosts can notify the SMTP server when to deliver messages. The ETRN command, which includes the FQDN of the IEMS machine, requests for the remote SMTP server to start processing messages in the mail queues that are addressed to the machine's FQDN. If such messages are at the server, the server creates a new SMTP session and sends the messages at that time. Support for ETRN requests ensures that even though there is no outbound mail to the SMTPC host, the host can still issue ETRN requests.

Message Priority Handling

SMTPC also provides a mechanism for message priority handling by assigning a priority weight for each message based on three factors, namely:

- the predefined message precedence
- the message size
- the total deferred time (for messages in the Deferred Queue)

The message priority weight is calculated using the following formula:

Priority Weight = (precedence * *Mp*)
+ (size * *Ms*)
- (deferred_time * *Md*)

Mp refers to the *precedence multiplier* which specifies the multiplier value for the precedence factor. *Ms* refers to the *size multiplier* which specifies the multiplier value for the size factor. *Md* refers to the *time multiplier* which specifies the multiplier value for the time factor.

The multiplier values specify how important a factor is relative to the other factors. It is an integer value and has a default value of 0, which means that the factor will not be taken into account in prioritizing a message.

The multiplier values are arbitrary. That is, if the system administrator thinks that size is twice more important than deferred time in prioritizing messages, then he can assign 2 to "size multiplier" and 1 to "time multiplier".

Priority weight is also dependent on size and time boundaries where messages are given classification. How messages are classified and how the priority weights are assigned to each range in the classification is totally up to the system administrator.

To illustrate, *Size Boundaries*, expressed in *K bytes*, classify messages into different ranges based on size property. The defined ranges are then assigned different priority weights.

For example, the boundaries can cover four ranges of sizes:

- sizes less than 10K (<10)
- sizes between 10K and 1,000K (10, 1000)
- sizes between 1,000K and 10,000K (1000, 10000)
- sizes larger than 10,000K (>10000)

These size ranges can then be given priority weights (0, 2, 4, 10), such as:

- Assign 0 to (<10) range
- Assign 2 to (10, 1000) range
- Assign 4 to (1000, 10000) range
- Assign 10 to (>10000) range

Similarly, *Time Boundaries*, which are expressed in hours and classify messages into different ranges based on the deferred time attributes, can also be assigned different priority weights.

For example, the boundaries can cover four ranges of deferred time (1, 6,12):

- deferred time shorter than 1 hour (<1)
- deferred time between 1 hour and 6 hours (1, 6)
- deferred time between 6 hours and 12 hours (6, 12)
- deferred time longer than 12 hours (>12)

These time ranges can then be given corresponding priority weights (1, 4, 6, 20), such as:

- Assign 1 to (<1) range
- Assign 4 to (1, 6) range
- Assign 6 to (6, 12) range
- Assign 20 to (>12) range

A priority weight that has a low value produces a higher priority level and the message is processed sooner. The message precedence and size multiplier are configurable parameters that can be defined by the system administrator. The total deferred time is system-generated since it denotes how long the message has been stored in the Deferred Queue. A message with a longer total deferred time is given a higher priority level than those that arrived recently.

Mail Routing Handling

SMTPC is capable of routing Internet messages based on several criteria. The routing options are:

- **DNS name lookup**
  Mail routing via DNS is the preferred method of routing mail in the Internet. The DNS is an Internet network service that stores and retrieves the information associated with domain names, such as address mapping and mail routing information.

- **Host table lookup of destination host**
  If the SMTPC is configured to use host table lookup, the internal host table, usually a text file determines the IP address of the recipient host. The exact format and path name of the host table depends upon the TCP implementation. The location of the host table is specified when IEMS is installed.

- **DNS followed by host table lookup**
  If a mail relay host is not being used, consult the DNS first and then the local host table. The local host may be used in the event of a failure to resolve a name with the DNS. If the name still cannot be resolved using either of the above methods, IEMS will use the defined mail relay host.

- **Host table followed by DNS lookup**
  The system administrator may also perform the reverse method when not using a mail relay host to resolve a name with the DNS. A host table followed by the DNS lookup can be used. In any event, if the name cannot be resolved using either of the above methods, SMTPC will use a defined mail relay host.

- **Delivery to default mail relay host**
  All messages will be sent to a primary mail forwarder for further routing, when configured to use a default mail relay host. If this mail forwarder cannot be contacted for any reason, and a secondary mail relay host is defined, the machine will use the secondary mail relay host. SMTPC will occasionally check to see if and when it is possible to switch back to use the primary relay host.

In the context of Internet mail, the DNS records being used by IEMS are the MX (Mail Exchanger) records and A (Address) records.

MX records contain mail forwarder information for hosts registered on the Internet. These records include the name of the host or domain and a list of one or more mail forwarding hosts and the preference values associated with these hosts. SMTPC uses preference values to determine the order in which to attempt delivery, in case more than one mail forwarder is identified. MX records are essential for the proper routing of mail, especially in situations where the destination host is not physically connected to the Internet and has to rely upon a mail forwarder for mail delivery.

A records, on the other hand, store the IP address information of hosts. SMTPC obtains the MX record of the destination host, when is configured to use the DNS. If an MX record is found, the list of mail forwarding hosts is used during SMTP connection. If no MX record is found, SMTPC searches for an A record. If an A record is found, then this address is used to establish the SMTP connection.

Simple Mail Transfer Protocol Daemon (SMTPD)

SMTPD (Simple Mail Transfer Protocol Daemon) is the server component that listens for incoming messages from the Internet. It creates a worker thread whenever a new connection request for incoming mail is detected. SMTPD supports the ESMTP (Extended SMTP) service extension, DSN (Delivery Status Notification), 8-bit MIME transport, SIZE (Message Size Declaration) extensions, as well as ETRN for downstream dial-up connected sites.

The multi-threaded architecture (see Figure 84 on page 131) enables SMTPD to create multiple threads that can handle many SMTP connections. It consists of the Master Thread Manager and the Worker Thread. The Master Thread Manager listens to the SMTP port for incoming connection requests from other messaging servers. Once a connection request is received, the Master Thread Manager creates a new worker thread to establish a new connection. The Worker Thread manages the connection and the transfer of messages between the IEMS and the external SMTP servers. Once the worker thread receives a message, it submits the message to the IEMS MTA Shared Message Queue.

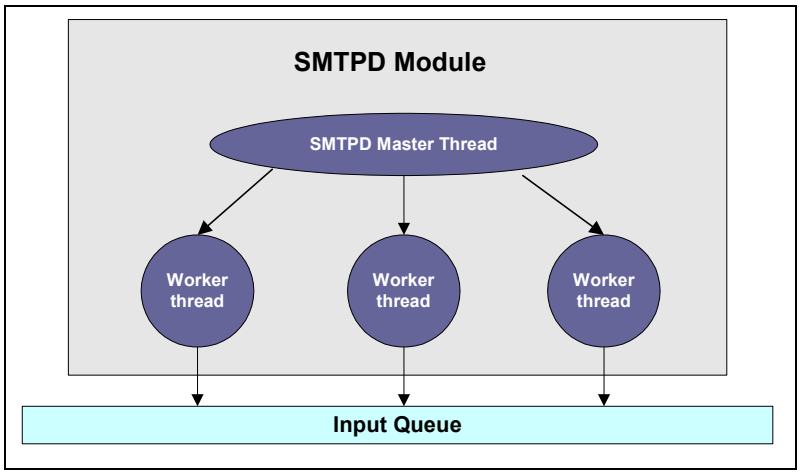

Figure 84: SMTPD system architecture

SMTP Connection Controls

SMTPD performs anti-spam checks on messages before routing them to the MTA Shared Message Queue. With this feature, SMTPD detects and acts upon junk messages even before they enter the system. Currently, the SMTPD module implements the following connection-based detection methods:

- **Site/Network Blacklisting**
  This feature allows a system administrator to control what sites are authorized to connect to SMTPD. If the default permission is to allow unlimited access, then a separate list of blacklisted sites can be used to identify the few sites not allowed to connect. Conversely, if the default permission is for no sites to be able to connect, a whitelist can be created listing just those sites permitted to connect to SMTPD.

- **DNS-BL Blacklisting**
  Internet blacklists based using the Domain Name System (DNS) as a transport can also be consulted. An arbitrary number of DNS-BL's can be configured for consultation. When MTA Pass-Through is enabled, each DNS-BL can be configured so that when connections resulting in DNS-BL matching occur, the SMTP connection can either be dropped before transmission of messages, or the message can be accepted and tagged for later potential action by the appropriate output channel processor. When not utilizing MTA Pass-Through, SMTP sessions for all remote MTA's that are identified by the configured DNS-BL's will be dropped.

- **Third-party relay prevention**
  The SMTPD Mail Relaying configuration permits a system administrator to be able to control what sites can relay mail through SMTP. If the default permission is to disallow all sites the ability to relay through the local MTA, and a whitelist can be created listing just those sites who are allowed relaying capability. Conversely, if the default permission is for all sites to be able to relay traffic (a dangerous and not recommended configuration), a blacklist can be created listing those sites which are not allowed to relay traffic. For roaming users, or those using dynamically allocated IP addresses, SMTP Authentication can be used to selectively enable mail relaying.

- **Remote Name Verification**
  During the SMTP dialog start up, SMTPD identifies the remote machine that sent a connection request. Via the SMTP-HELO command, the remote machine sends its FQDN (Fully Qualified Domain Name). SMTPD uses the supplied FQDN, to perform a reverse DNS lookup to verify the name. The DNS lookup is based upon the known network address of the sending site. If the supplied name and verified name do not match, SMTPD may terminate the connection.

Batch SMTP Overview

While most Internet email is directly transported via SMTP (Simple Mail Transfer Protocol), there are times when other forms of message transports are more desirable.

The following are some situations where an alternative transport method is useful:

- A dedicated IP (Internet Protocol) address is not available
- Low message volume
- Higher costs associated with dedicated Internet connections
- Internet connection is available only on a dial-up basis

Why BSMTP?

When a user composes a message, he uses an email client, such as Microsoft Outlook Express, Netscape Communicator, among others. The email client presents an interface which prompts the user to provide addressing information (**To:**, **Cc:** and **Bcc:**) and a **Subject:** field as minimum requirements. After supplying the addressing and labeling information for the message, the user then composes a message.

Once the user has completed composing his message, an instruction is given to the email client to send the message (see Figure 85 on page 133). At this point, the mail client constructs a message file and an envelope. The message file contains what is known as the message header, consisting of the original **To:**, **Cc:** and **Subject:** fields (but not the **Bcc:** information), as well as the return address of the sender and the time (**Date:** field) when the message was composed. After the message header, the message file then contains the message body as composed by the sender. The envelope is now also constructed. It initially contains the list of recipients specified by the sender in the **To:**, **Cc:** and **Bcc:** fields of the original message.

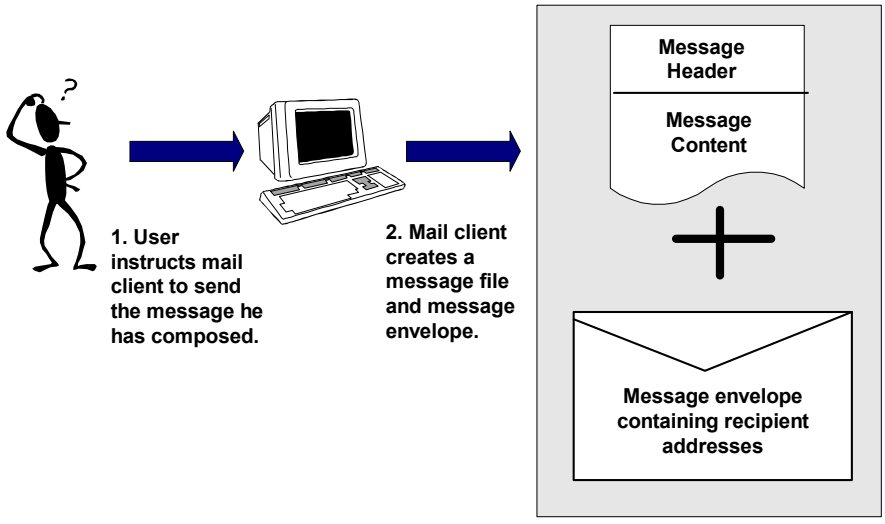

Figure 85: Message Processing

After the construction of the message file and envelope, the message is sent separately to a local MTA, which transfers the message across the Internet to the intended recipients. It is important to note that with the exception of trace information recorded in the message header, the message file remains unchanged during transit. In particular, the addresses present in the **To:** and **Cc:** fields of the message remain as they were when the user first composed the message. However, for the message envelope, the list of recipient addresses are changed during transit because address expansions are done when mail aliases, user forwarding, or distribution lists are encountered.

When the message reaches its final recipient destination, the last MTA in the chain sends the message to the LMDA (Local Mail Delivery Agent) which then deposits the message file in the appropriate repository or mailbox. Now that final delivery has been performed, the envelope information is discarded. By this time, the message viewed by the recipient indicates the original recipient addresses as specified in the **To:** and **Cc:** fields.

The separation of the original message file from the envelope information is the basic principle behind the transfer of email messages on the Internet. This allows not only the proper routing and re-routing of messages from one system to another. It also preserves the original labeling of messages as composed by the sender.

So, why is all of this important in the discussion of BSMTP and the use of mail repository, like POP3 accounts, as message transport holding areas? The answer lies in the fact that when messages are delivered to a POP3 account, the envelope information is usually lost. When this message is retrieved for later delivery, the recipient information has to be derived from the message header present in the message file since the envelope has already been discarded. If the POP3 repository is used as a holding area for more than one recipient, such as an entire organization or a group of people, it will be impossible to guarantee the accuracy of the regenerated envelope. The message recipients that were **Bcc:** in the original message will not show up in the message header, nor will any changes in the envelope that result from alias expansion; user forwarding or distribution list expansion which occurred after the original message was sent. There is simply no reliable way to reconstruct the list of recipients to whom the message was intended once the envelope information has been discarded. The solution to this problem lies in the creation of an email tunnel, where messages can be sent across non-SMTP transports and then re-injected (de-tunneled) into the message transport system on the other side. This is precisely what the IEMS BSMTP Tunnel modules provide. The diagram in Figure 86 (borrowed from RFC-2442 which describes the BSMTP Media Type) describes in detail how the BSMTP Tunnel works:

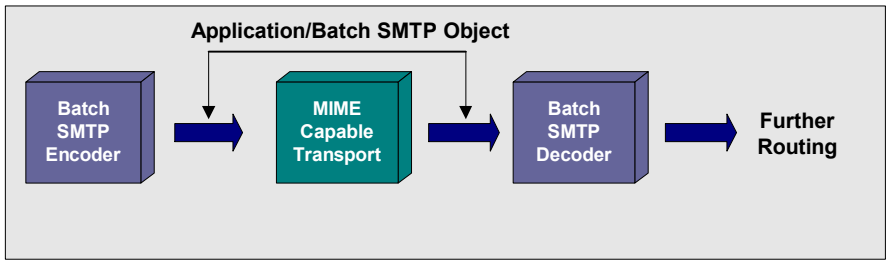

Figure 86: Message Tunneling

When a message arrives at the BSMTP Encoder, both the message file and the envelope information is encapsulated into a new message. This new message is addressed to a remote BSMTP Decoder, which de-tunnels the encapsulated message and then routes the message.

In the case of IEMS, the tunneled message is delivered to the MTA Input Queue where it is routed to any BSMTP Decoder with an email address accessible either on the Internet or any other IEMS local channels.

When a BSMTP tunneled message is delivered to a message repository, like a POP3 account, even though the accompanying envelope is discarded, the original envelope remains intact within the tunneled message. The Internet Exchange BSMTP Decoder first retrieves messages of this type via POP3, before de-tunneling and submitting the original message file and envelope to the MTA Input Queue for further routing.

IEMS BSMTP

IEMS includes a built-in BSMTP (Batch Simple Mail Transfer Protocol) module supporting the tunneling of email across non-SMTP transports. This is an ideal solution for sites that prefer to use POP3 (Post Office Protocol version 3) as their message retrieval protocol rather than SMTP. It preserves the original message envelope while passing through POP3, ensuring the proper routing of messages.

The BSMTP module is comprised of the BSMTP Encoder, Decoder, and a specialized POP3 client used to download BSMTP encoded messages from remote Message Stores. The POP3 client supports UIDL (Unique ID Listing) and provides an option for the system administrator to specify the maximum number of messages per POP3 session.

The Encoder encapsulates messages into BSMTP format before routing them to their destination address. This destination address can be within IEMS or any other server with a mail repository (mailbox) that can be accessed by an RFC-2442 compliant decoder. The Decoder breaks apart BSMTP encoded messages into their original envelope and message components, and then submits them into the Input Queue for further routing. Once the messages are received in the Input Queue, they are treated the same as if they were received directly via SMTP.

Message Forwarding

The routing of messages through a BSMTP Tunnel involves four (4) steps:

- Identification of messages by a receiving MTA (Message Transfer Agent)
- BSMTP encoding
- Transmission of the BSMTP encoded message
- Delivery of the BSMTP encoded message to either a remote decoder or a message repository where the message can be later retrieved by a cooperating BMSTP Decoder

Message Identification

Messages arrive at the MTA through any of the available input channels (LOCALOUT, BSMTPIN, SMTPD, CCOUT, NOTESOUT, DL, WEBMAIL). Each of these messages contain recipient address information in the message envelope that is used as the basis for further routing. The MTA can be configured to identify recipient addresses, either by a specific address, or an entire domain or specific routing (BSMTP in this case). See “Domain Forwarding” on page 43 for specific information on how to configure per user and domain-based forwarding rules. Once an address is identified for forwarding through a BSMTP Tunnel, it is sent to the BSMTP Encoder for encapsulation.

BSTMP Encoding

The BSMTP Encoder encapsulates messages into a BSMTP format before delivering the messages to the destination address. The destination address can be within the local domain or any other messaging server capable of decoding BSMTP encoded messages. The encoder consists of a tunneling mechanism that wraps or encapsulates messages retrieved from the Input Queue into Application/BSMTP messages. It encodes the original message into a BSMTP formatted message that contains the original message and envelope information. These messages are then re-injected into the Input Queue for forwarding to the specified account.

Message Transmission

When a BSMTP message arrives in the Input Queue, a new message envelope is created for the routing of the encapsulated message through the BSMTP Tunnel. This envelope information contains the recipient address for the end of the BSMTP Tunnel. The original message, including its original message content and envelope have been encapsulated in the new message content to be expanded again at the other end of the tunnel.

The MTA at this point will treat a BSMTP injected message the same as any other message submitted to the Input Queue. This allows BSMTP encoded messages to be delivered to any valid Internet email address, either within the local IEMS environment or elsewhere.

Delivery of BSMTP Encoded Messages

The normal use of BSMTP within an IEMS environment is to use a Message Store mailbox (local or remote) as an intermediate holding area. Messages held in these mailboxes can later be retrieved by the BSMTP POP3 client, which then submits them to the BSMTP Decoder for further non-BSMTP routing. This is very useful for sites without permanent Internet connections as they can tunnel all of a sites traffic through a single remote mailbox.

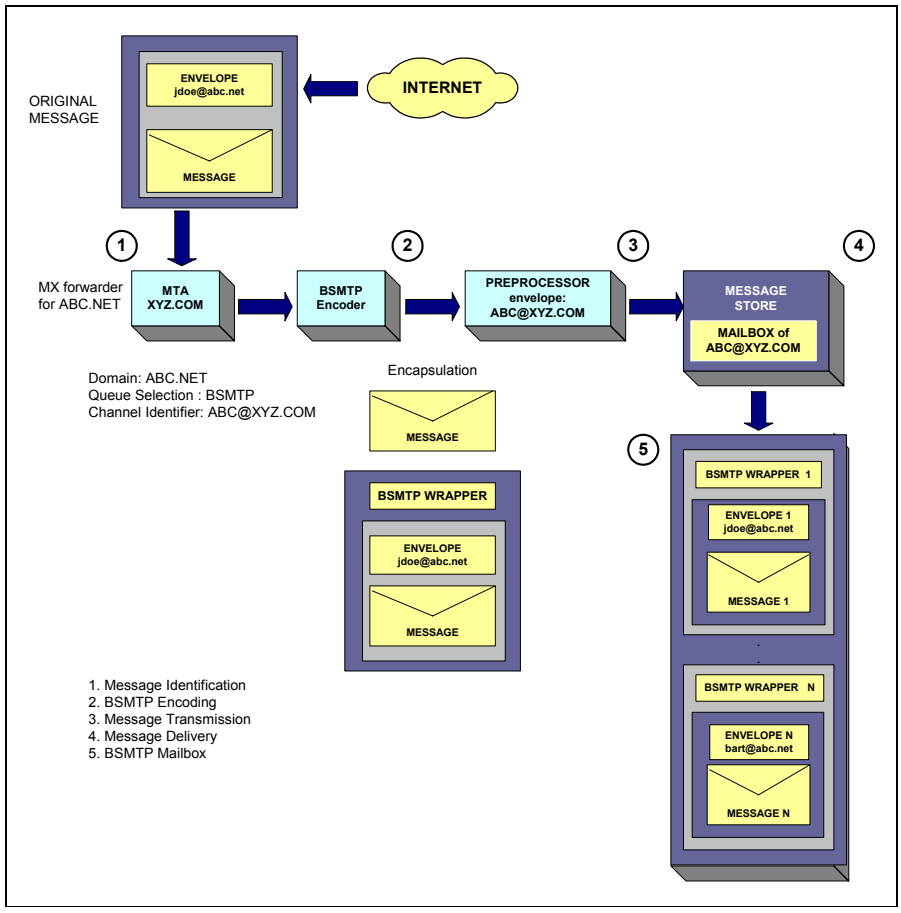

Figure 87: Creating a domain forwarding entry

Figure 87 above describes the routing of messages through a BSMTP Tunnel. In the diagram, *abc@xyz.com* is used as the basis for routing messages for *abc.net*. The BSMTP Encoder encapsulates the messages together with their envelope information into a new BSMTP formatted message and sends the encapsulated message to the Input Queue for further routing. If the channel identifier associated with the message exists, the message will be forwarded to the mailbox corresponding to the address defined in the channel identifier *abc@xyz.com*.

Message Reception

The reception of messages through a BSMTP Tunnel involves three (3) steps:

- Message Retrieval from a remote mailbox
- BSMTP Decoding
- Delivery of BSMTP Decoded Message to the local MTA Input Queue

Message Retrieval Using the POP3 Client
Messages can be held in either a Message Store account or any other mailbox (an ISP account for instance) as long as the message content is unaltered and accessible using POP3. The POP3 client module picks up remote messages and then hands them off to the BSMTP Decoder for further processing.

BSMTP Decoding
The BSMTP Decoder breaks apart an encoded message into its original message envelope and content.

Delivery of BSMTP Decoded Messages
The BSMTP Decoder submits de-tunneled messages to the Input Queue. Once in this queue, they are treated the same as messages received by any of the other input channels (LOCALOUT, BSMTPIN, SMTPD, CCOUT, NOTESOUT, DL, WEBMAIL).

On the receiving end, the BSMTP client uses POP3 to download the BSMTP formatted message from the mailbox of if *abc@xyz.com*. After download, the BSMTP Decoder decodes the message back to its original message format and envelope information. It then submits the message to the Input Queue for further routing. Once the message is submitted to the Input Queue, it will be treated the same as if they were received directly via SMTP. The messages will be preprocessed and submitted to the MTA Shared Message Queue. The different channel processors fetch the message to the mailbox of their intended recipients.

Message Flow

Messages received through either the SMTPD (Simple Mail Transfer Protocol Daemon) or BSMTP Decoder modules are submitted to the Input Queue. The Input Queue delivers the messages to the Preprocessor module. If the preprocessor determines that a message is destined to a recipient on the other end of a BSMTP Tunnel, the BSMTP Encoder encapsulates the message together with its envelope information into a new BSMTP format message. Then, the BSMTP Encoder sends the message to the Input Queue for further routing (see Figure 87 on page 137). From the Input Queue, the message will be delivered to the Preprocessor, which performs preprocessing tasks on the messages before submitting them to the MTA Shared Message Queue, where the messages will be fetched by their respective output channels (LOCAL, BSMTPOUT, CCIN, NOTESIN, DL, SMTPC). The output channels will eventually deliver the messages to the mailboxes of the intended recipients.

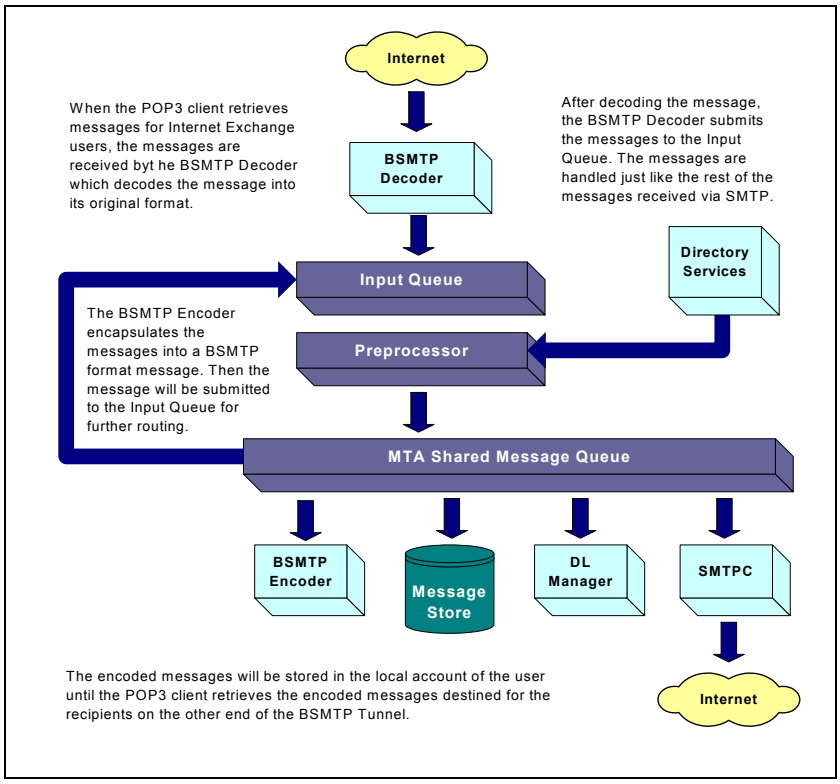

Figure 88: Encoding and decoding process

On the receiving side, when the POP3 client downloads BSMTP-decoded messages destined for IEMS users, the BSMTP Tunnel Decoder decodes the message back to its original message file format and envelope information. After decoding the message, the BSMTP Tunnel Decoder submits the message to the Input Queue for further routing (see Figure 88 on page 139). When the message is submitted to the Input Queue, it is treated just like any other message that was received via SMTP. The appropriate preprocessing and message routing tasks are performed by the IEMS MTA before the messages are delivered to the mailboxes of the intended users.

SMTP Parameters

To configure SMTP parameters, click the SMTP link on the top menu frame. This displays the “SMTP” screen (see Figure 89 on page 140).

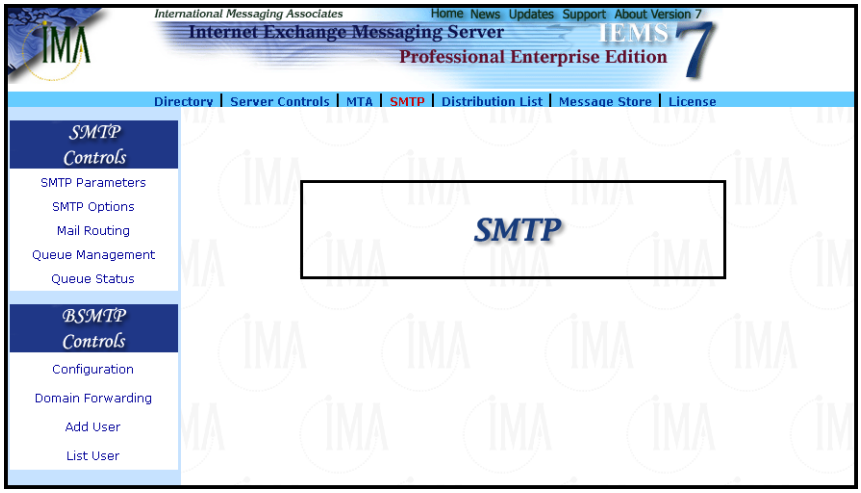

Figure 89: SMTPC Module

The SMTPC module shares a number of common parameters with SMTPD (Simple Mail Transfer Protocol Daemon). The SMTPC and SMTPD components include several ESMTP options, and options for handling delayed messages and SMTP Timeout Tunings. These parameters define how the SMTPC module will deliver the messages to the intended recipients.

To configure the different SMTPC parameters, click the ***SMTPC Parameters*** button on the left menu frame. This action displays the “SMTP Parameters” screen (see Figure 90 on page 141). Enter the desired values in the text boxes provided.

SMTPC Port
The TCP port number to be used by SMTPC when delivering messages across the Internet. This is useful when running SMTPC behind a firewall or any other non-standard setup. The default value is 25.

SMTPD Port
The TCP port number to be used by SMTPD. This is useful when running SMTPD behind a firewall or any other non-standard setup. The default value is 25.

Enable ESMTP
When this option is enabled, SMTPC/SMTPD will support ESMTP. SMTPD will accept the ESMTP command “EHLO” and SMTPC will issue “EHLO” to the peer host. By default, it is enabled. Other ESMTP extensions will be supported after “Enable ESMTP” is enabled. These extensions include “SIZE”, “DSN”, “ETRN”, and “8-bit MIME”. It is recommended to always enable this option.

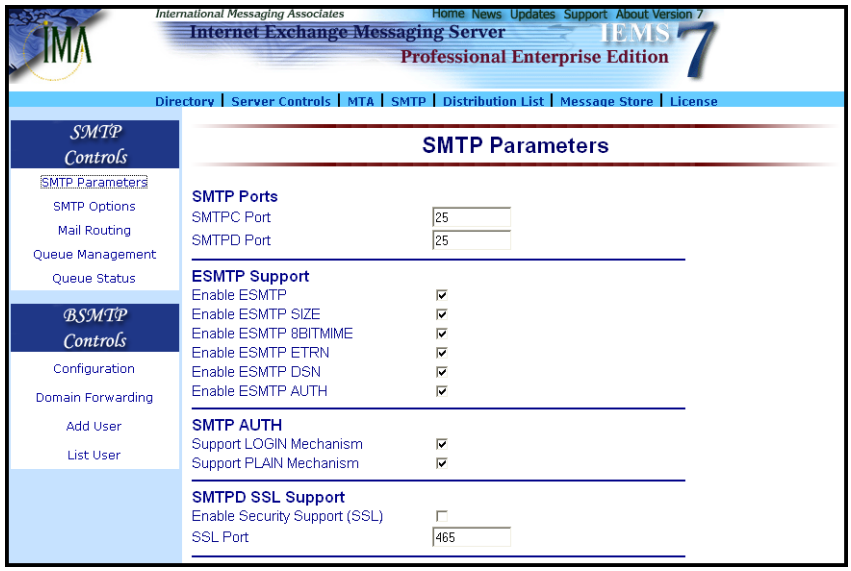

Figure 90: Configuring SMTPC Parameters (a)

Enable ESMTP SIZE
Activating this option allows SMTPC and SMTPD to use the SIZE extension service. If this option is enabled, SMTPD will advertise the keyword SIZE in response to EHLO command. The administrator can configure the maximum inbound message size for each peer domain as well as the default maximum size under the “Peer Configuration” section.

The optional parameter for the keyword SIZE, which is used to specify the fixed maximum size, can be determined from the “Peer Configuration” by taking the maximum value of the size limit for all the peer domains. The default is enabled.

Enable ESMTP 8-bit MIME
When this option is enabled, SMTPD announces support for 8-bit MIME. The default is enabled.

Enable ESMTP ETRN
Prompts SMTPD to announce its support for ETRN and accept ETRN requests. Once an ETRN request is received, SMTPD signals the SMTPC module to start a new queue processor for the requested ETRN host. The default is enabled.

Enable ESMTP DSN
Prompts the SMTPD to announce its support for DSN and accept DSN request during MAIL FROM and/or RCPT TO commands. SMTPC also generates a DSN message when reporting the delivery status. The default is enabled.

Enable ESMTP AUTH
When enabled, SMTPD will accept an AUTH request and perform the user authentication. SMTP sessions authenticated using this method will be allowed to relay mail through the MTA. This option is enabled by default.

SMTP Auth

SMTP Auth is an optional SMTP Authentication mechanism used to validate the identity of remote SMTP users. Once authenticated, mail relaying is enabled for the remote user. This is often used for roaming users. Remote users can use any account login/password that is currently enabled for the system.

Support LOGIN Mechanism
When enabled, the SMTP AUTH LOGIN authentication mechanism will be supported. This option is enabled by default.

Support PLAIN Mechanism
When enabled, the SMTP AUTH PLAIN authentication mechanism will be supported. This option is enabled by default.

SMTP Auth - Client Support

At times it may be necessary to communicate with an upstream mail relay that requires SMTP Authentication. IEMS allows the configuration of both the primary and secondary configured mail relay hosts to use SMTP Authentication. Currently there are no web controls for configuring SMTPC to use SMTPC Authentication, so the IEMS configuration file must be manually edited. All SMTPC Authentication information is configured under the *[Routing]* section. The variables that can be set are as follows:

```
[Routing]
# to enable client side support of SMTP Auth
# valid values: YES / NO
EnabledSMTCPAUTH=Yes

# primary relay host auth account and password names,
# e.g. smtpauth@relay1.isp.com
PMR-AuthUser=relay1.isp.com
PMR-AuthPwd=relay1password

# secondary relay host auth account and password names,
# e.g. smtpauth@relay2.isp.com
PMR-AuthUser=relay2.isp.com
PMR-AuthPwd=relay2password
```

After configuring it is necessary to shut down SMTPC and restart.

SMTPD SSL Support

Enable Security Support (SSL)
When the option is checked, SSL support for SMTPD server will be enabled. By default, it is not enabled.

SSL Port Number
To specify the port number to be used for the SSL enabled SMTPD Server. The default value is 465.

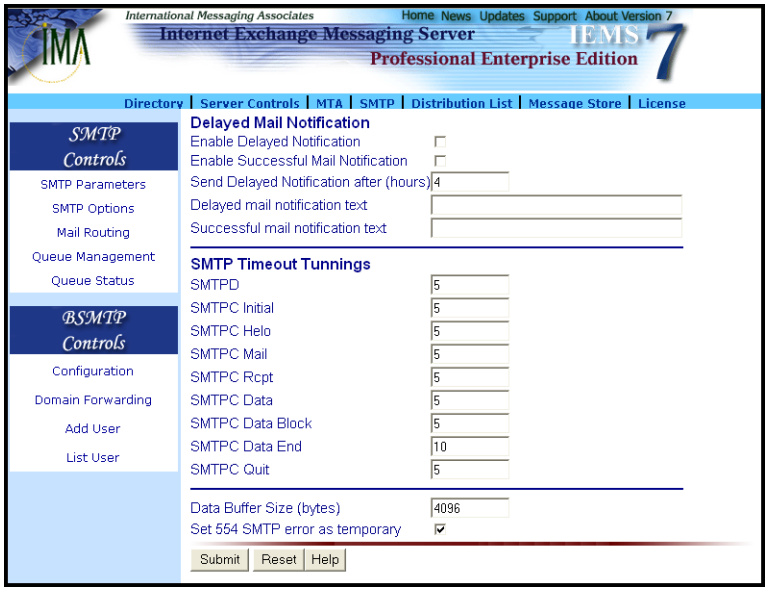

Figure 91: Configuring SMTPC Parameters (b)

Delayed Mail Notification

Enable delayed mail notification
Prompts SMTPC to send a delayed notification message to the sender when an ESMTP DSN is NOT enabled or a DSN request does not specify NOTIFY-NEVER. The default is disabled.

Enable successful mail notification
When this option is enabled, IEMS notifies the sender when a delayed message has been successfully sent. The default is disabled.

Send delayed mail notification after (hours)
SMTPC sends the delayed message notification after the specified amount of time. The default value is 4 hours.

Delayed mail notification text
The path name of the file containing the message to be used to notify the user of a delayed message delivery. If no filename is specified or no file is found at the specified path, an appropriate default warning message is used.

Successful mail delivery text
The path name of the file containing the message that will be sent to the Postmaster when the machine, after having sent at least one delayed message notification, eventually delivers a message. If none is specified, or if no file is found at that path, an appropriate default warning message is sent.

SMTP Timeout Tunings

SMTPD
The timeout value (in minutes) that SMTPD waits for an open socket. The default value, which is 5 minutes, should not be changed. However, if unusual delays are experienced, the default value can be adjusted to stop SMTPD from timing out.

SMTPC Initial
The period (in minutes) that SMTPC waits for the initial contact of a remote host to be completed. The default value is 5 minutes.

SMTPC Helo
The period (in minutes) that SMTPC waits for the remote system to respond to the HELO command. The default value is 5 minutes.

SMTPC Mail
The period (in minutes) that SMTPC waits for the remote system to respond to the MAIL FROM command. The default value is 5 minutes.

SMTPC Rcpt
The period (in minutes) that SMTPC waits for the remote system to respond to the RCPT TO command. The default value is 5 minutes.

SMTPC Data
The period (in minutes) that SMTPC waits for the remote system to respond to the DATA command. The default value is 5 minutes.

SMTPC Data Block
The period (in minutes) that SMTPC waits for the remote system to respond to acknowledge an individual buffer transmission of message data. It can also be defined as the length of time wherein SMTPC waits between writes to the TCP stack before it considers the remote system “dead”. The default value is 5 minutes.

SMTPC Data End
The period (in minutes) that SMTPC waits for the remote system to respond to the DATA phase wrap up represented by the dot (.) command. The default value is 10 minutes.

SMTPC Quit
The period (in minutes) that SMTPC waits for the remote system to respond to the QUIT command. The default value is 5 minutes.

Data Buffer size
The size, in bytes, of the data buffer used by the SMTP programs to read data from the Internet. If the machine uses disk caching, set this option to the size of the read ahead buffer. The default value is 4096 (4K); the maximum buffer size is 32768 (32K).

Set 554 SMTP error temporary
RFC821 on SMTP is not clear as to whether “error 554 transaction failed during the DATA phase” should be regarded as a permanent error. Usually 5xx errors are permanent, but some SMTP servers return 554 errors for tempo-

rary errors. IEMS takes the conservative approach and retries such message later. If this option is set to No, then such messages will be bounced instead or resend to their intended recipients. The default is Yes.

After entering the desired values, click the ***Submit*** button to store the settings.

Mail Routing Options

IEMS provides several options for routing mail over the Internet. The system administrator may define how the messages will be routed by specifying the preferred values in the text boxes provided.

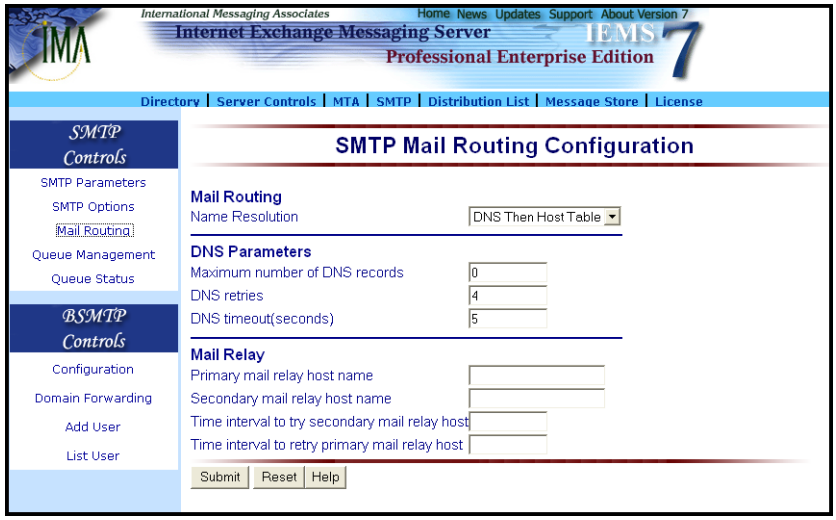

Figure 92: Configuring Mail Routing Options

Note: *For Windows, the "Host table filename", "DNS server address" and "Current DNS server" options are displayed in the "SMTP Mail Configuration" screen. However for Linux, as shown in the figure above, these options are not listed because these values are predefined by the system.*

The administrator has the option to use the DNS or host table when performing a destination host lookup. Click the ***Mail Routing*** button on the left menu frame to configure the various mail routing options (see Figure 92 on page 145).

Mail Routing Parameters

Name resolution

There are several name resolution options, namely: DNSonly, DNSThenHostTable, HostTableThenDNS, HostTableOnly, and MailRelayHost. Any combination of DNS or host table lookup can be used regardless of the order. When the mail relay host only routing option is disabled, it is recommended that DNS be used if possible, as this usually results in the most reliable routing.

Host table filename
Stores the location of the Internet host table for address resolution. Even if the DNS is used for name resolution, it is necessary to configure a host table that contains at least the name and address for the local machine as well as for the default mail relay host. This will allow SMTPC to send the message to the default mail relay host for further routing in case the machine encounters problems when communicating with the name server(s).

DNS server address
SMTPC contacts the list of configured DNS servers to resolve remote machine names. Each address must be of the form a.b.c.d, where each number is between 0 and 255. SMTPC can be configured to contact a list of DNS servers and/or consult the local host table when resolving host names.

Operation without access to DNS servers can be achieved on an Internet connected site only when the outgoing mail is routed through a mail relay host. In this case, the name and address of the mail relay host(s) must appear in the local host table.

DNS Parameters

Maximum number of DNS records
The maximum number of DNS records cached in the database on the local disk. The DNS cache greatly improves the throughput of IEMS, particularly when the DNS server(s) are not on a local LAN. The default value is 1,000,000, which balances throughput against greater disk space used for the cache. A value of zero disables DNS caching.

DNS retries
The number of times a DNS query is retried after the operation has timed out. The default value is 4.

DNS timeout (seconds)
The length of time in seconds before a DNS request timeout is registered. The default value is 5 seconds.

Mail Relay Parameters

Primary mail relay host name
A mail relay host is another host capable of forwarding mail to third parties. Many Internet hosts have this capability, but before using them it is polite to ask for permission from the local administrator. Mail relay hosts used for delivery of outbound traffic are not necessarily the same one used as MX forwarders for incoming traffic, although in some configurations they may coincide. The administrator can define a number of strategies to deliver mail, some of which involve using a mail relay hosts as a primary or last-resource mail router.

If SMTPC is unable to resolve a host name by either DNS or host table lookup, it routes messages to the primary mail relay host for forwarding. This option is also used if routing is configured to mail relay host only.

Secondary mail relay host name
A secondary mail relay host can be defined to be used when the primary relay host is unavailable. When enabled, a secondary mail relay is configured for use when the primary mail relay host is unavailable.

Time interval to try secondary mail relay host
The length of time in minutes that the primary mail relay host is unavailable, after which it is considered offline and the message is routed to the secondary mail relay, if the latter is enabled.
Time interval to retry primary mail relay host
The number of minutes before the machine attempts to revert to the primary mail relay host after the previous attempt has failed.

SMTP Queue Management

SMTPC uses an efficient queue management system that ensures messages are delivered in a timely manner. The Queue Management facility of allows the system administrators to schedule the delivery of messages on a per domain basis. For example, all outgoing mail for a specified domain can be queued for later delivery. Queuing mail before attempting delivery enables SMTPC to process messages efficiently by utilizing the system resources only when needed. The queue run interval determines how long the pending queue processors should check for pending messages.

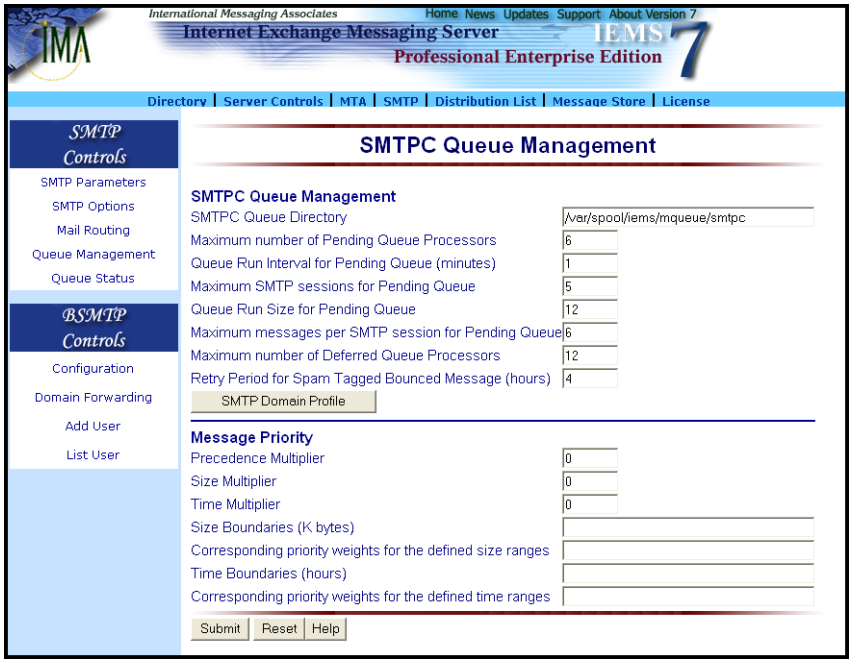

Figure 93: Configuring SMTPC Queue Management

To configure the different queue handling options, click the SMTP Queue Management button on the left menu frame. A screen for configuring queue management options appears (see Figure 93 on page 147). Enter the directory for the SMTPC queue and the desired values for the various queue management parameters in the appropriate text boxes.

SMTPC Queue Management Parameters

SMTPC Queue Directory
The queue directory that SMTPC will use to store outgoing messages.

Maximum number of Pending Queue Processors
The maximum number of Pending Queue Processors that will run concurrently. Pending Queue Processors are responsible for processing messages in the Pending Queue. Each queue processor handles messages independently. The default is 6.

Queue Run Interval for Pending Queue (in minutes)
Determines how often the Pending Queue Processor should check for pending messages in minutes. If pending messages exist, they will be processed immediately. The default value is 1.

Maximum SMTP sessions for Pending Queue
Each Pending Queue Processor is capable of establishing multiple concurrent SMTP sessions. This option specifies the maximum number of SMTP session for each processor. The default value is 5.

Queue Run Size for Pending Queue
At each queue run, each Pending Queue Processor will process messages simultaneously. The queue run size specifies the number of message for each queue run. The default value is 12.

Maximum messages per SMTP session for Pending Queue
The highest number of messages that can be sent using a single SMTP connection for Pending Queue. When this number is increased, more messages can be sent to a remote SMTP server on each connection. The default value is 6.

Maximum number of Deferred Queue Processors
The maximum number of Deferred Queue Processors that will run concurrently. Each Deferred Queue Processor is responsible for processing the deferred messages for a particular deferred SMTP domain. The default value is 6.

Retry Period for Spam Tagged Bounced Messages (hours)
The retry period for spam tagged bounced messages. It is many times desirable to assign different time to live values for non-delivery notifications related to potential spam than for normal messages. The default period for normal messages to remain in the queues for retries is 3 days, while the default for spam tagged non-delivery notifications is 4 hours.

Message Priority

SMTPC features a mechanism for message priority handling which guarantees not only high throughput but also the orderly handling of messages with different priorities. See “Message Priority Handling” on page 128 for a detailed description.

Precedence Multiplier (Mp)
The multiplier value for the Precedence factor. It is an integer value and is used relative to the other factors, size multiplier, and time multiplier. The default value is 0.

Size Multiplier (Ms)
The multiplier value for the Size factor. It is an integer value and is used relative to other factors, precedence multiplier, and time multiplier. The default value is 0.

Time Multiplier (Md)
The multiplier value for the Time factor. It is an integer value and is used relative to the other factors, size multiplier, and precedence multiplier. The default value is 0.

Size Boundaries (K bytes)
Use to classify messages into different ranges based on size. Different weight will then be assigned for the defined ranges. The weights are used for calculating the total priority weight. *e.g. 10, 1000, 10000* The boundaries define 4 ranges of sizes, sizes less than 1K (>10), sizes between 10K and 1,000K, sizes between 1,000K and 10,000K, and sizes larger than 10,000K (>10,000).

Corresponding priority weights for the defined size ranges (e.g. 0, 2, 4, 10)
The defined weights are assigned to the corresponding size range defined by the Size Boundaries. This will assign the weights to the corresponding size range defined above.

- Assign 0 to (<10) range
- Assign 2 to (10,1000) range
- Assign 4 to (1000,10000) range
- Assign 10 to (>10000) range

Time Boundaries (hours) (e.g. 1, 6, 12)
Use to classify messages into different ranges based on the deferred time. Different weight will then be assigned for the defined ranges. The weights are used for calculating the total priority weight. The boundaries define 4 ranges of deferred time: deferred time shorter than 1 hour (<1), deferred time between 1 hour and 6 hours (1, 6), deferred time between 6 hours and 12 hours (6, 12), and deferred time longer than 12 hours (>12).

Corresponding priority weights for the defined time ranges (e.g. 1, 4, 6, 12)
The defined weighs are assigned to the corresponding time range defined by the Time Boundaries. This will assign the weights to the corresponding time ranges defined above.

- Assign 1 to (<1) range
- Assign 4 to (1, 6) range
- Assign 6 to (6, 12) range
- Assign 20 to (>12) range

Click the ***Submit*** button to store the settings.

Adding, Editing, Deleting, and Viewing Peer Domain

On the “SMTP Queue Management” screen, click the ***SMTP Domain Profile*** button (see Figure 93 on page 147). The front end of the interface lists all the domain profiles stored in the database. A special entry called “`default`” is added when the database file is being initialized by the system. This entry cannot be removed from the database. The system administrator may add, edit, delete and view peer domain profiles via this screen. Please refer to “Peer Domain Configuration” on page 57.

Queue Status

The SMTPC Queue Manager displays messages according to one of the following criteria: Priority Weight, Sender, Deferred Time and Size. When the sorting criteria is specified, SMTPC will search all the deferred messages for the specified criteria. The results will be displayed on a new page showing all the messages that matched the searched criteria.

The SMTPC Queue Status screen (see Figure 94 on page 150) displays the number of deferred messages in the SMTP channel, deferred reason and the next queue run time. The system administrator may search process and view messages via the SMTPC Queue Status.

Pending Queue
The Pending Queue displays the number of newly arrived messages that must be sent out immediately. These messages are processed by the Pending Queue Processors, which attempt delivery via SMTP. If the delivery of a message in the Pending Queue is unsuccessful, it is passed on to the Deferred Queue so it can be delivered at a later time.

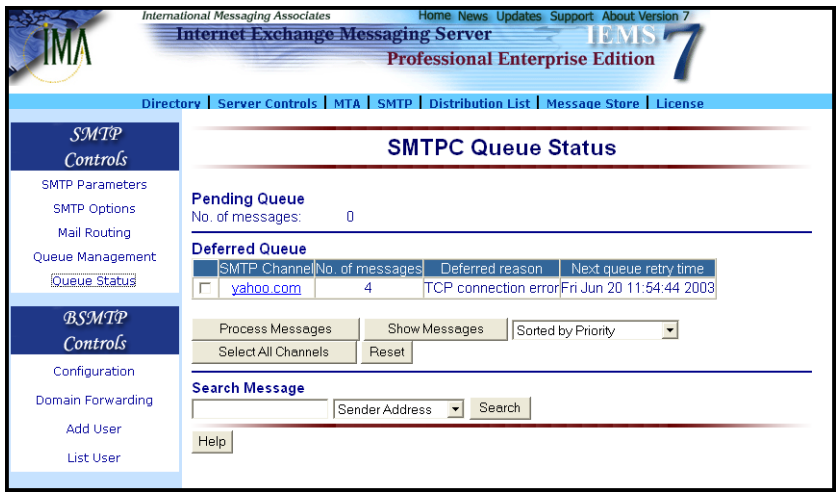

Figure 94: SMTPC Queue Status

Deferred Queue
Messages that are intentionally deferred or whose previous delivery attempt(s) have failed are placed in the Deferred Queue. Messages in the

Deferred Queue are further grouped into different SMTP domain channels using information in the recipient addresses. The number of deferred messages, deferred reason, and next queue retry time are displayed for each SMTP channel. The messages for each SMTPC domain channel are processed according to their message priority weight.

Process Messages
To force SMTPC to process messages, click the *Process Messages* button. This forces SMTPC to start processing the deferred messages in the selected SMTP channels.

Show Messages
To show the deferred messages for the SMTP channels, select the channels and a sorting criteria and click the *Show Messages* button. A new screen displays the deferred messages sorted according to the defined criteria.

Select All Channels
Clicking the *Select All Channels* button will select all the SMTP channels. The selected action will apply to all the SMTP channels.

Search Messages
The search can be based on two search types: sender address or recipient address. When the input address and search type are specified, click the *Search Messages* button. A new screen displays all the messages that matched the searched criteria.

By clicking one of the SMTP channel, two sections of information for SMTP channel are shown. They are the Domain Profile and Queue Status (see Figure 95 on page 152).

The **Domain Profile** displays the profile information defined for this domain. The profile includes the option queue mail before attempting delivery, queue run interval, retry period, maximum session, and maximum number of messages per session.

The **Queue Status** includes the number of deferred message(s), the deferred reason, and next queue run time.

he fields shown include **Message ID**, **Priority Weight**, **Sender**, **Deferred Time**, **Size**, and **Recipients**. The messages are displayed according to the sorting type. The one in the heading that is highlighted, which in this case is the Priority Weight, indicates that the messages are sorted using this field. You may resort the messages by clicking the headers link.

If the number of recipients exceeds three, a **More Recipient** link will be shown. Once clicked, a new page displaying all the recipients for this message will appear.

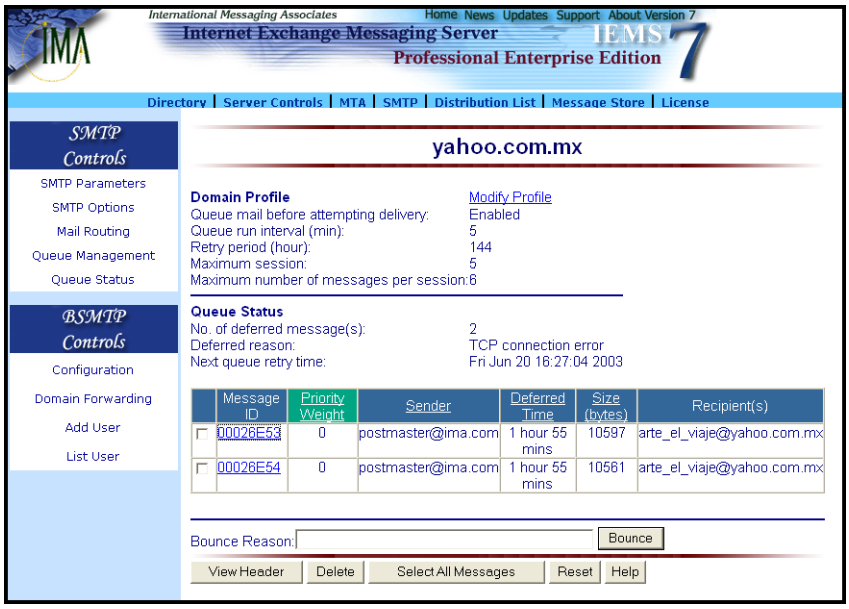

Figure 95: SMTPC Channel Information

The maximum number of messages shown for each SMTP channel on a page view is 100. When the total number of deferred messages in the SMTP channel exceeds this value, a **More Message** link will be shown below the message list. The link points to a new page displaying the next messages.

Bounce
To bounce messages, mark the check box of the messages. Specify the reason in the Bounce Reason edit box. Click the ***Bounce*** button. This bounces the selected message(s) in the SMTP channel.

View Header
To view the message header of the selected message(s) in the SMTP channel, click the ***View Header*** button.

Delete Messages
To delete the selected message(s) in the SMTP channel, click the ***Delete*** button.

Select All Messages
To automatically select all the messages in the SMTP channel, click the ***Select All Messages*** button.

SMTP Options

The system administrator can define how messages from the Internet will be received by SMTPD. To configure the different SMTPD options, click the ***SMTP Options*** button on the left menu frame. This action displays a new screen (see Figure 96 on page 153).

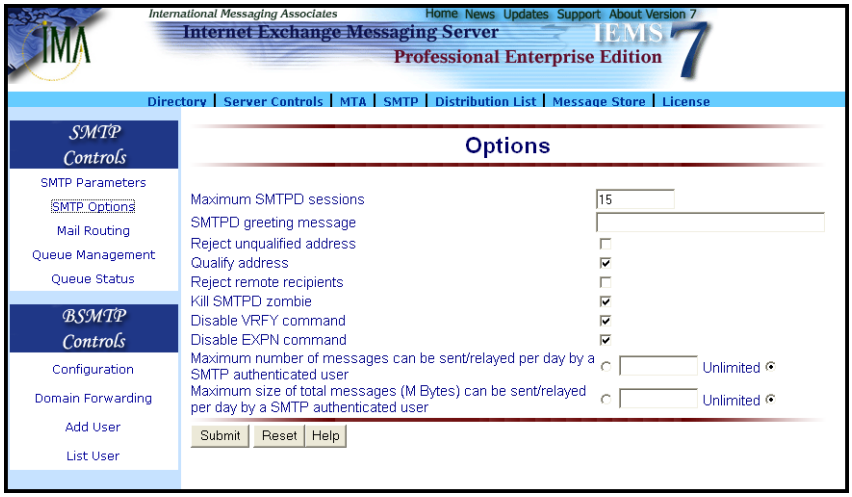

Figure 96: Configuring SMTPD Options

Maximum SMTPD sessions
The maximum number of incoming SMTPD sessions. Some TCP stacks have a limit on the number of concurrent connections. A value of zero indicates that there is no preset maximum value. The default value is 15.

SMTPD Greeting Message
The string test which will be used to customize the SMTPD welcome/greeting message displayed when a SMTPC logs in. This feature is very useful for customizing your company's personal message greeting preference and for security purposes so as not to disclose the mail server product information.

Reject unqualified address
When enabled, SMTPD checks the recipient and sender addresses for a proper domain part, refusing to receive messages where it is absent. For example, *user@ima.com* is accepted, but *user* alone is rejected. This option is useful in encouraging users to use FQDNs every time they send mail to the Internet (as required by the Internet standards). The default is disabled.

Qualify address
When enabled, SMTPD automatically appends the local domain part to an unqualified address. The default is enabled.

Reject remote recipients
When enabled, SMTPD rejects incoming messages for remote Internet recipients. This is to prevent remote sites from trying to spoof messages by rerouting them through the local machine back to the Internet. The default is enabled.

Kill SMTPD zombie
When enabled, SMTPD closes the socket used by SMTPD when it last shut down prematurely. Thus, SMTPD will not get an Address already in use error when restarted. The default is enabled.

Disable VRFY command
For security reasons, the “VRFY” (verify user) command is sometimes considered too intrusive and a security hole. Through this command, a remote host may confirm whether a particular address is valid. Disabling the “VRFY” command causes SMTPD to respond with “252 command disabled” when a remote SMTPC issues this command. The default is disabled.

Disable EXPN command
Through the “EXPN” (expand mailing list) command, a remote host may confirm whether a certain mailing list exists. Disabling the “EXPN” command causes SMTPD to respond with “550 command disabled” when a remote SMTPC issues this command. The default is disabled.

Click the ***Submit*** button to store the new settings.

Maximum number of messages can be sent/relayed per day by a SMTP authenticated user
The maximum number of messages that can be sent/relayed in one day by a SMTP authenticated user. The default is Unlimited.

Maximum size of total messages (M Bytes) can be sent / relayed per day by a SMTP authenticated user
The maximum size of total messages (M Bytes) that can be sent/relayed in one day by a SMTP authenticated user. The default is Unlimited.

BSMTP Encoder / Decoder

Enabling the BSMTP Encoder and Decoder

The system administrator needs to activate the BSMTP Decoder and Encoder components to be able to process the BSMTP formatted messages that pass through IEMS.

The BSMTP Decoder works with the POP3 client module in picking up remote messages using the POP3 protocol. It decodes BSMTP formatted message into their original RFC822 message format. It then de-tunnels the messages by re-injecting them into IEMS.

The BSMTP Encoder consists of a tunneling mechanism that wraps or encapsulate messages retrieved from the Input Queue into Application/ BSMTP messages. It encodes the original message into a BSMTP format message that contains the original message and an envelope information. These messages are then re-injected into the Input Queue for forwarding to a specified account on the other side of the tunnel.

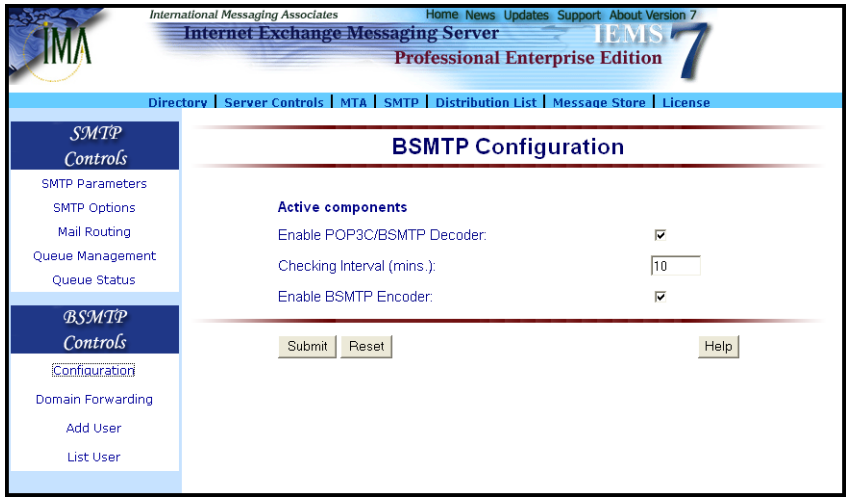

Figure 97: BSMTP Configuration Settings

To enable the BSMTP Encoder and Decoder, click the Configuration Settings button on the left menu frame. This action displays the “BSMTP Configuration” screen (see Figure 97 on page 155). Configure the following:

Enable POP3C/BSMTP Decoder
Set this option to enable the POP3 client/BSMTP decoder.

Checking Interval
The checking interval value will determine in minutes how long the POP3 client will wait before checking a POP3 server for available messages.

Enable BSMTP Encoder
Activate this option to enable the BMSTP Encoder.

Per-Domain Forwarding

Using the Domain Forwarding feature of the Preprocessor, it is possible to simply forward email traffic for an entire domain through a BSMTP Tunnel. For details on Domain Forwarding, see “Domain Forwarding” on page 158.

Per-User Forwarding

It may be desirable at times to forward mail destined for individual addresses through a BSMTP Tunnel. This can be done through the creation of a BSMTP connector in the Directory entry for the desired address(es). Please see See “Connectors” on page 120..

Receiving BSMTP Messages

The POP3 client is used to configure IEMS as the receiving end of a BSMTP Tunnel. The POP3 client connects to a remote POP3 account that holds the queued BSMTP messages. Once received, these BSMTP encoded messages are broken apart into their original message envelope and content and submitted to the MTA Input Queue for further routing.

POP3 Client Profiles

Adding Remote POP3 Client Profiles

The “Add POP3 User Profile Entry” screen (see Figure 98 on page 157) enables the system administrator to add remote POP3 servers that may be accessed by IEMS.

To add a POP3 user, click the ***Add User*** button on the left menu frame. The following parameters need to be supplied with the corresponding users information:

Login Name
The user name of an existing POP3 account on that server.

Password
The user password for the particular user.

Server Name
The POP3 server name (e.g. host1.ima.com) that will be accessed by IEMS. The system administrator can allow a user to access many POP3 servers. A POP3 account may be used to tunnel several user accounts.

Port Number
The port number of the remote POP3 server to be accessed by IEMS. The default is 110.

Timeout
The timeout value in minutes determines how long the POP3 client will wait for the POP3 servers to respond to every POP3 command. The default is 10.

Maximum No. of Messages per Session
The maximum number of messages per POP session. After the POP3 client has downloaded the maximum number of messages from the server, it will issue the ‘QUIT’ command to end the current session. The server will then update and remove those deleted messages from the maildrop. After that, the POP3 client will start a new POP3 session to download the rest of the messages.

The ability to terminate a POP session after N messages have been processed can be critical in situations where the reliability of a given POP session is in question. Due to the design of the POP protocol, servers are not required to remove or update the status of downloaded messages until after receiving a QUIT command. If a connection is dropped or otherwise improperly shut down, previously downloaded messages will not be removed from the server, and will continue to be downloaded until the remote server gets a QUIT command. By specifying at most N messages per POP session, the administrator can reduce the chances of multiple message downloads.

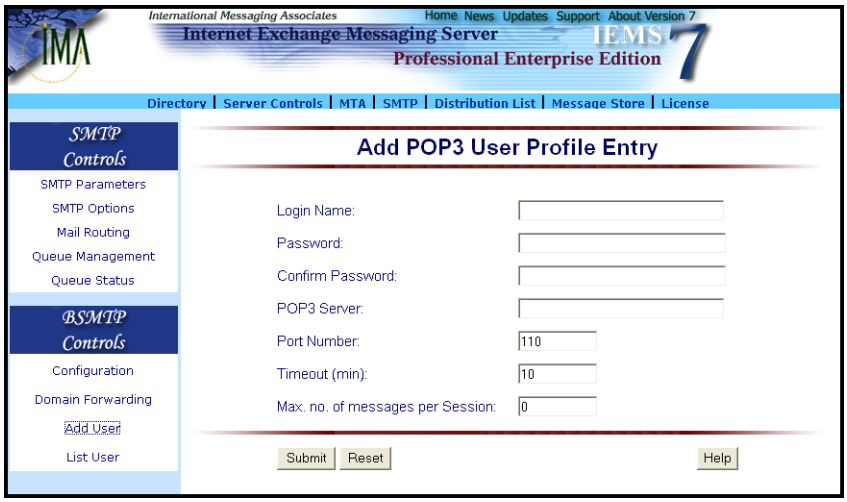

Figure 98: Adding POP3 Clients

Viewing POP3 Client Profiles

The system administrator may view the list of existing POP3 client profiles. To view the existing POP3 profile, click the List Users button on the left menu frame. This action displays the “Profile List” screen (see Figure 99 on page 157).

The **User Name** column contains the list of POP3 client profiles existing on the server.

The **POP3 Server** column contains the POP3 server of the particular POP3 client.

The **Port Number** column contains the port of the remote POP3 server to be accessed.

Figure 99: Viewing POP3 Client Profiles

Deleting a POP3 Profile

The system administrator may delete a POP3 client profile from the list of existing POP3 profiles.

To delete a profile, select the particular profile by marking the check box beside the profile entry (see Figure 99 on page 157). Click the ***Delete Selected*** button.

Note: *Multiple deletion of profiles is allowed.*

Updating POP3 Client Profiles

The system administrator may update a profile by clicking the selected name under the **User Name** column from the “Profile List” screen (see Figure 99 on page 157). When a particular profile has been selected, a table of the profile’s attributes appears (see Figure 100 on page 158). The system administrator may modify the profile by typing new entries in the profile table. See “Adding Remote POP3 Client Profiles” on page 156.

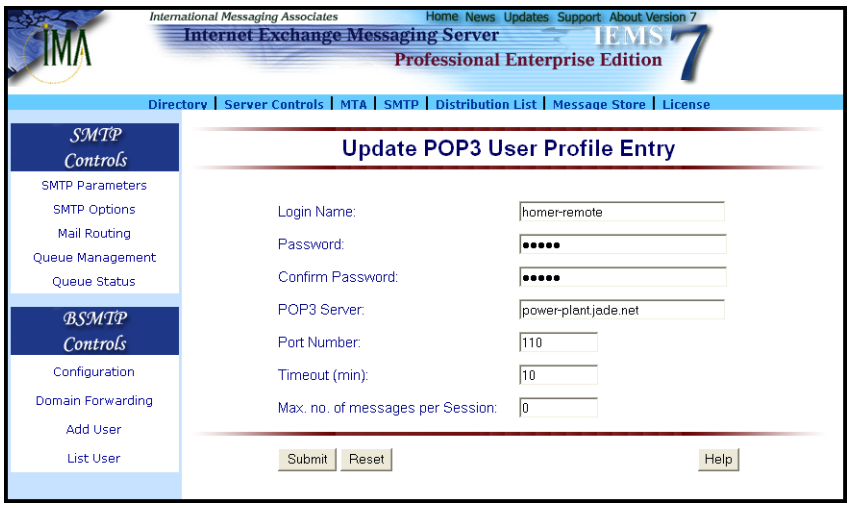

Figure 100: Updating POP3 User Profile

Domain Forwarding

Creating Domain Forwarding Entry

Domain forwarding allows the administrator to map all addresses within a domain to a specific channel. This mapping implements static routing between the defined domain and the corresponding channel. The system administrator may create a domain forwarding entry by clicking the ***Domain Forwarding*** button on the left menu frame. This action displays the “Domain Forwarding” screen.

In creating domains, click the ***New*** button at the bottom of the page (see Figure 101 on page 159). Fill in all the required parameters and then, click the ***Add*** button.

Domain Name
The name of the domain IEMS will do BSMTP forwarding for.

Queue Selection
For BSMTP forwarding, select BSMTPOUT.

Channel Identifier
The address of the remote BSMTP Decoder or mailbox used for later BSMTP downloading.

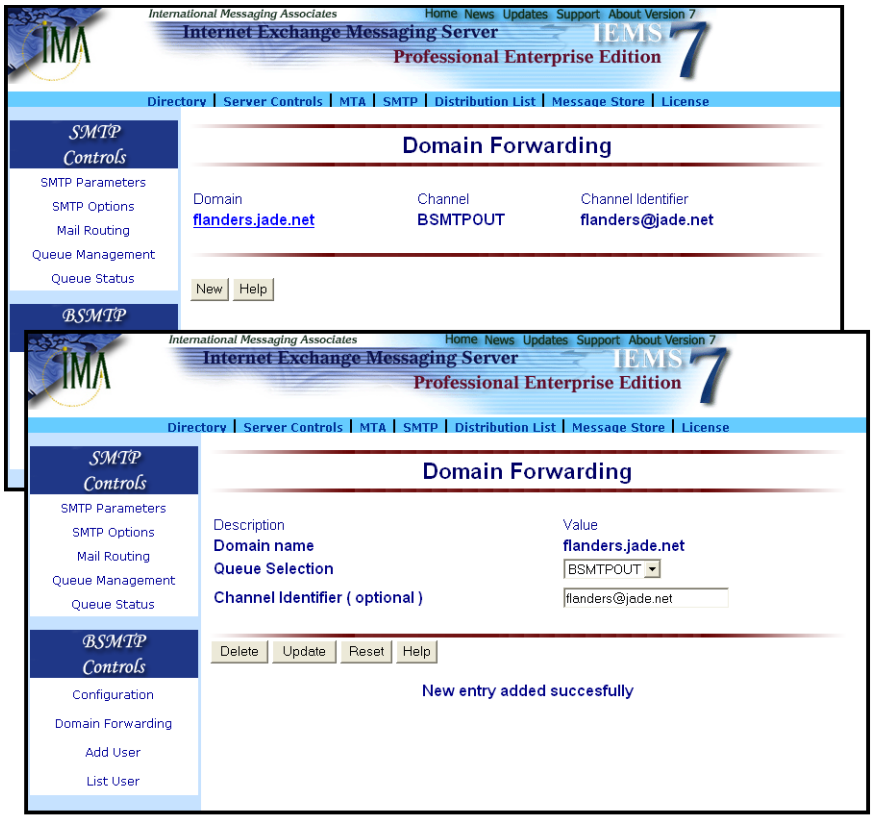

Figure 101: Creating a Domain Forwarding Entry

Note: *A more detailed description of Domain Forwarding, please see “Domain Forwarding” on page 158.*

Updating Domain Forwarding Entries

The system administrator may also update an existing domain forwarding entry.The updated domain forwarding entry will be used when forwarding messages whose domain match the domain forwarding entry.

The system administrator may select any entry on the “Domain Forwarding” screen (see Figure 101 on page 159) for updating. Please see “Domain Forwarding” on page 158.

After accomplishing the above procedures, click the ***Update*** button to save the new domain forwarding entry to the domain forwarding list. A confirmation screen displays that the “entry has been successfully updated”.

Deleting Domain Forwarding Entries

Existing domain forwarding entries may be deleted from the list. This will remove the entry from the database. A selected entry from the “Domain Forwarding” screen can easily be removed using the ***Delete*** button.

SENDMAIL

Sendmail is an IEMS command line utility designed to be a drop in replacement for the BSD sendmail program supplied on most Linux machines.

NAME

sendmail - a mail transport agent for the Internet Exchange Messaging Server

SYNOPSIS

sendmail [flags] [address ...]

DESCRIPTION

Sendmail sends a message to one or more recipients, routing the message via the Internet Exchange Messaging Server.

Sendmail is not intended as a user interface routine; other programs provide user friendly front ends. **Sendmail** is used only to deliver pre-formatted messages.

OPTIONS

Sendmail is intended to be a drop in replacement for the BSD sendmail program for the purposes of submitting message into the Message Transport System. **Sendmail** reads its standard input up to an end-of-file or a line consisting only of a single dot. The message read from standard input is sent to all recipients indicated on the command line.

-fname Sets the name of the ‘‘from’’ person (i.e., the sender of the mail). -f can only be used by ‘‘trusted’’ users (normally root, daemon, and network) or if the person you are trying to become is the same as the person you are.

EXAMPLES

To send the message in the file msg to the recipient jdoe@jade.net:

cat msg | sendmail jdoe@jade.net

To send the same message, setting the envelope sender to be cron@jade.net:

cat msg | sendmail -f cron@jade.net jdoe@jade.net

MAILQ

Mailq is a command line utility used to display IEMS message queue summary information.

NAME

mailq - print the Internet Exchange SMTP mail queue

SYNOPSIS

mailq [-hv] [-s sortOrder] [-q smtpChannel]

DESCRIPTION

mailq prints a summary of the mail messages queued for future delivery.

The first line printed for each message shows the internal identifier used for the destination host for the message, the size of the message in bytes, the date and time the message was accepted into the queue, and the envelope sender of the message. The second line shows the error message that caused the message to be retained in the queue; The following lines show message recipients, one per line.

OPTIONS

The options are as follows:

-h Print help information

-v Verbose mode. This adds the priority field of the message to the information displayed

-s sort_order

Print the messages in the queue according the specified sort order (priority, size, time). By default, the messages are shown in priority order

-q smtpChannel

Print the message for the specified SMTP channel. If the smtpChannel, the messages in the Pending Queue will be printed. By default, all messages in the Pending and Deferred Queues are printed

EXAMPLES

To display the messages in the Pending Queue, sorted by size:

mailq -s size -q ""

To display the messages for the smtp domain jade.net in the Deferred Queue, sorted by time:

mailq -s time -q jade.net

DBUPDATE

Dbupdate is a command line utility used to rebuild possibly corrupted SMTPC databases.

NAME

dbupdate - rebuild Internet Exchange SMTPC databases

SYNOPSIS

dbudpate [-hr]

DESCRIPTION

Dbupdate is used to rebuild possibly corrupted databases used by the Internet Exchange SMTPC Message Queue. Before running **dbupdate**, please shutdown the Internet Exchange Messaging Server.

OPTIONS

-h Print the help information.

-r Rebuild all SMTPC Queue message databases.

EXAMPLES

To rebuild the SMTPC Queue databases:

dbupdate -r

CHAPTER 7

Domain Administration

Overview

The Internet Exchange Messaging Server (IEMS) is a multi-domain messaging solution. A single IEMS machine or IEMS cluster can be setup to satisfy the messaging needs of several domains simultaneously. For larger installations, or those where the persons responsible for the different domains are different, a single administrative interface is not sufficient.

IEMS Domain Administration allows the IEMS administrator (referred in this context as the *super administrator*) to delegate administration of account creation, limits, and distribution lists to a domain administrator. The super administrator sets the overall limits for the domain (disk space, number of lists allowed, etc), and then the domain administrator manages these resources.

Domain Administration can be found together with the *Directory Controls*. To configure Domain Administration, click the **Directory** link on the top menu frame. This brings up the "Directory Services" screen (see Figure 102).

Figure 102: Directory Services / Domain Administration

Note: Existing managed domains can be maintained by going to the following URL: *http://iems-host-fqdn/iems/domain*.

Add Domain

To create a new managed domain account, click on the ***Add Domain*** button in the main menu area. This will bring up the "New Domain Configuration" screen (see Figure 103).

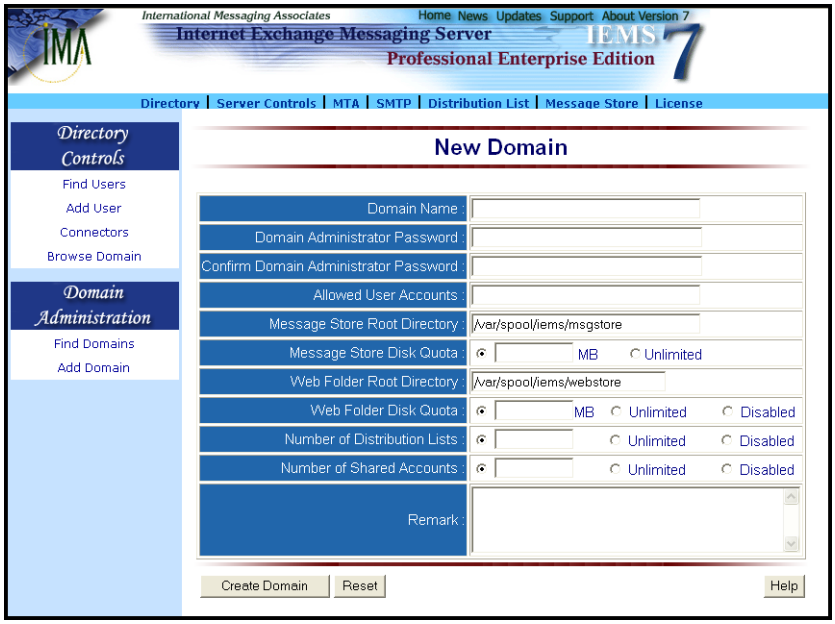

Figure 103: New Domain Configuration

From this page, new domain account can be added to the Directory Server. The attributes associated with a domain account are defined below.

Domain Name
The name of the domain that you want to create (e.g. *jade.net*).

Domain Administrator Password
Confirm Domain Administrator Password
The security password is used to gain access to the domain administration interface. To make sure that it is typed correctly, the password must be entered again in the *Confirm Domain Administrator Password* textbox. The password appears on screen as a row of asterisks for security purposes

Number of User Accounts
The maximum number of Message Store user accounts allowed for the domain

Message Store Root Directory
The physical location of the user's mailboxes and messages for the domain. All new accounts for the new domain will be created under this directory. If disk space becomes a problem, this value can be modified at a later date by the super administrator, and all subsequent account creations will be located in the new location.

Message Store Disk Quota
This determines the maximum Message Store disk space allowed for the domain. To assign an unlimited quota, select the ***Unlimited*** radio button. This allows the domain to have an unlimited disk space that can be allocated for users under the domain. Otherwise, tick the ***MB*** button and enter a value corresponding to the maximum disk quota allowed for the domain.
Please note that this value applies for the sum of all accounts under the managed domain, and not for a single user. For instance if this quota is set for 100MB, and the first account created consumes 50MB, then the rest of the domain has to share the remaining 50MB of allocated space.

Web Folder Root Directory
The physical location of the user's web folder for the domain.

Web Folder Disk Quota
This determines the maximum Web Folder disk space allowed for the domain. If you are to assign an unlimited quota, select the ***Unlimited*** radio button. This allows the domain to have an unlimited disk space that can be allocated for users under the domain. To disable the Web Folder capability for a domain, select the ***Disabled*** button. To enter a numeric amount, select the ***MB*** button and enter a value corresponding to the maximum disk quota allowed for the domain. As with the Message Store quota above, please note that this applies to the sum of all accounts under the managed domain, and not a single account limit.

Number of Distribution Lists
This determines the maximum number of distribution lists allowed for the domain. To assign an unlimited number of distribution lists, select the ***Unlimited*** radio button. To disable the Distribution Lists capability for a domain, select the ***Disabled*** button. To specify a maximum number of lists allowed, select the button next to the textbox and enter a value corresponding to the maximum number of distribution lists allowed for the domain.

Number of Shared Accounts
The maximum number of Message Store Shared Accounts allowed for the domain. To assign an unlimited number of shared accounts, select the ***Unlimited*** radio button. To disable the Shared Account capability for a domain, select the ***Disabled*** button. To enter a numeric value, select the button next to the textbox and enter a value corresponding to the maximum number of shared accounts allowed for the domain.

Remark
This allows you to input and store notes text about the domain. This field is not interpreted by the system, and is present only to simplify domain management.

When done filling in all the fields above, click the ***Create Domain*** button to create the new domain.

Find Domains

Existing managed domain information can be retrieved for display and/or editing using the *Find Domains*. Simple select the ***Find Domains*** link in the main menu area. This will bring up the “Find Domain Menu” (see Figure 104).

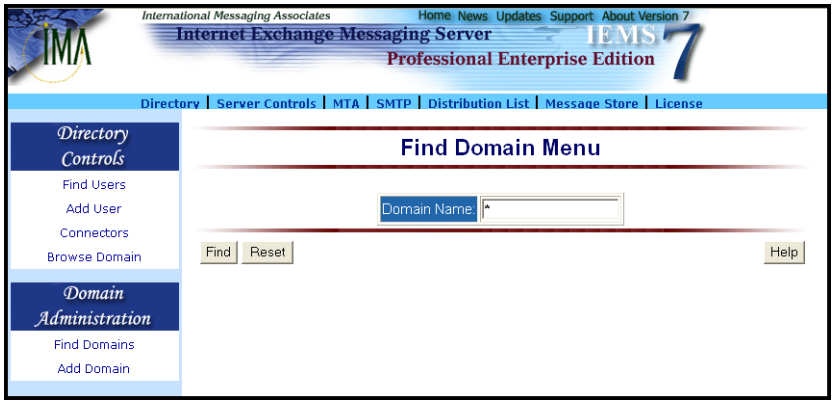

Figure 104: Find Domain Menu

To locate a domain or domains, enter the domain name to be located. Wild-cards (asterisks*) in the text field can also be used to help search for multiple domains. Use of a single asterisk will display the names of all managed domains.

When done, click the ***Find*** button to start the search. A new screen containing the results of the search will be displayed (see Figure 105).

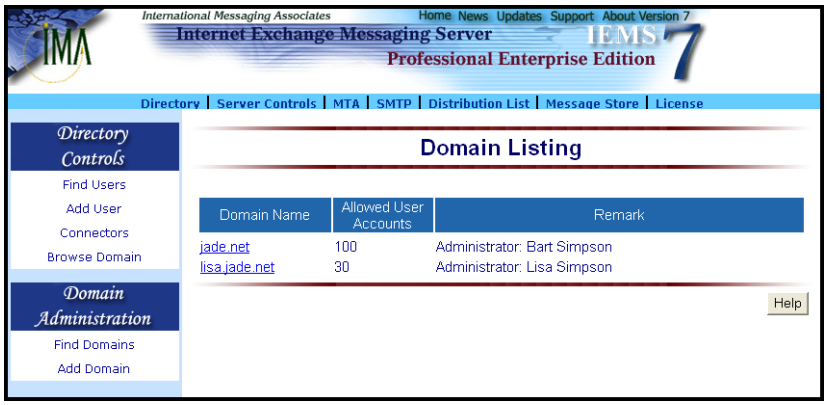

Figure 105: Domain Listing

To display the attributes for any of the listed managed domains, simply click on the appropriate domain name. This will bring up the “Domain Details” screen displaying the current configuration (see Figure 106) for the selected domain.

The following information is presented:

Domain Name
The name of the domain selected (e.g. *jade.net*).

Number of User Accounts (Used / Allowed)
The current and maximum number of allocated Message Store user accounts allowed for the domain

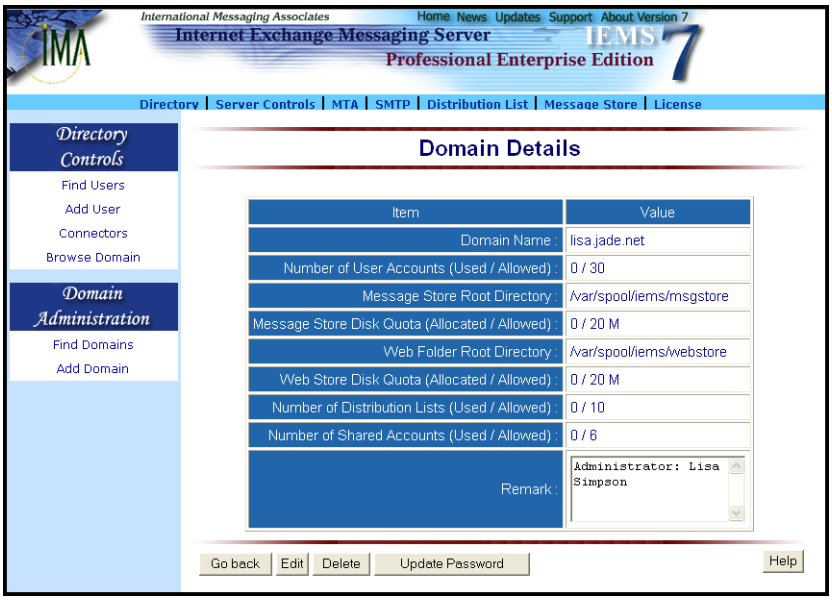

Figure 106: Domain Details

Message Store Root Directory
The physical location of the user's mailboxes and messages for the domain. All new accounts for the new domain will be created under this directory. If disk space becomes a problem, this value can be modified at a later date by the super administrator, and all subsequent account creations will be located in the new location.

Message Store Disk Quota (Allocated / Allowed)
The current allocated and maximum Message Store disk space allowed for the domain.

Please note that this value applies for the sum of all accounts under the managed domain, and not for a single user. For instance if this quota is set for 100MB, and the first account created consumes 50MB, then the rest of the domain has to share the remaining 50MB of allocated space.

Web Folder Root Directory
The physical location of the user's web folder for the domain.

Web Folder Disk Quota (Allocated / Allowed)
The current allocated and maximum Web Folder disk space allowed for the domain. As with the Message Store quota above, please note that this applies to the sum of all accounts under the managed domain, and not a single account limit.

Number of Distribution Lists (Used / Allowed)
The current allocated and maximum number of distribution lists allowed for the domain.

Number of Shared Accounts (Used / Allowed)
The current allocated and maximum number of Message Store Shared Accounts allowed for the domain.

Remark
Notes text about the domain. This field is not interpreted by the system, and is present only to simplify domain management.

Update Password

To change the domain administrator password, simply click on the ***Update Password*** button on the "Domain Details" page (see Figure 106). This brings up the "Update Domain Password" screen (see Figure 107).

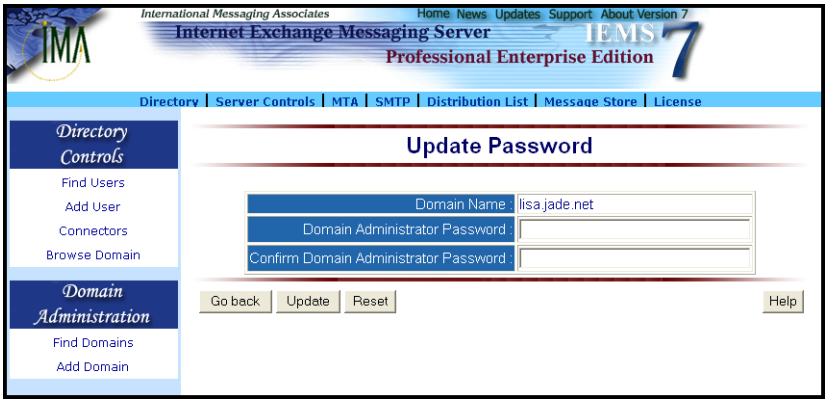

Figure 107: Update Domain Password

To change the domain administrator password for the selected domain, enter the new password in each of the above password text boxes, and then select the ***Update*** button to enter the change.

Edit Domain Details

To change attributes other than the domain administrator password for a managed domain, click on the ***Edit*** button on the "Domain Details" page (see Figure 106). This brings up the "Edit Domain Configuration" page (see Figure 108). From here all other attributes associated with the domain can be modified. For additional information on the meaning of each field, please see the section above on domain account creation.

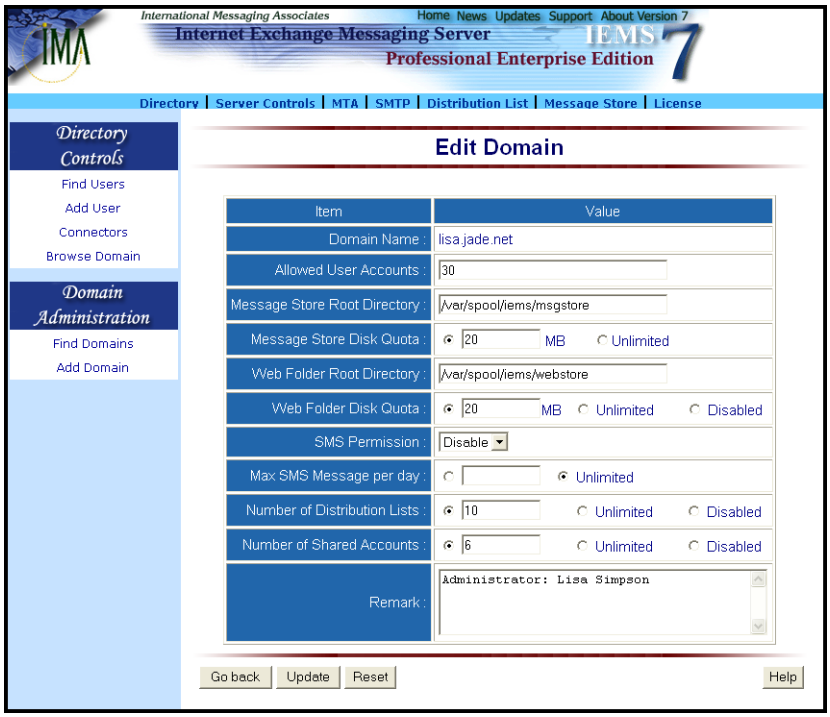

Figure 108: Edit Domain Configuration

Domain Administrator Login

After domain accounts have been setup by the IEMS *Super Administrator*, domain administrators can manage their accounts by logging into Domain Administration. This can be found by going to the following URL: *http://iems-host-fqdn/iems/domain*. The “Domain Administration Login” page will then be shown (see Figure 109).

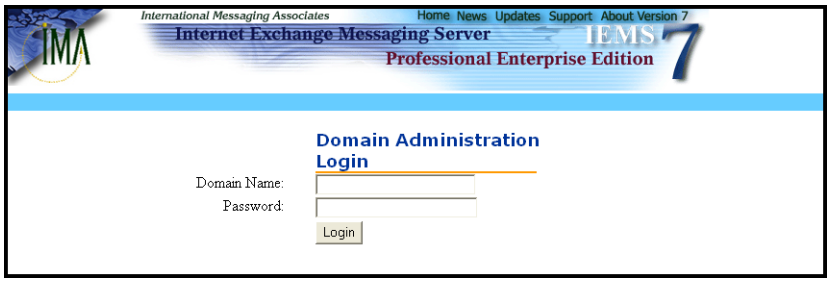

Figure 109: Domain Administration Login

After supplying the name of the managed domain and the appropriate password, the “Domain Management Controls” page will appear (see Figure 110), allowing full domain management.

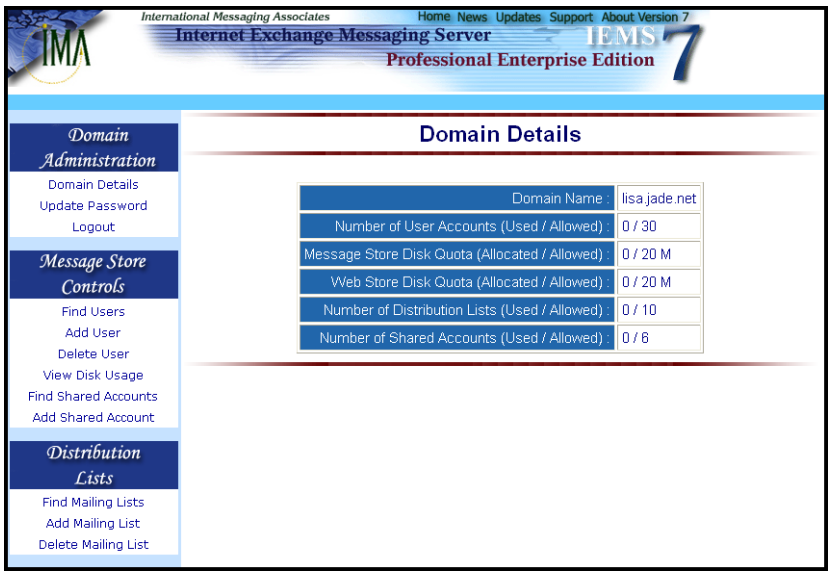

Figure 110: Domain Management Controls

From the main Domain Management Controls page, the domain administrator can manage their domain. This includes updating the domain administrator password, domain Message Store and Distribution List controls. The details of each of these can be found in the relevant section of this manual. The scope of each management area however is limited to the managed domain, rather than the entire system.

IEMSDOMACCT

Iemsdomacct is a command line utility used to create, delete, or list domain accounts.

NAME

iemsdomacct - create / delete / list IEMS domain accounts

SYNOPSIS

iemsdomacct [-C|D|L] [-d domain_name] [-p domain_adm_password] [-u user_number] [-h msgstore_home_directory] [-q msgstore_quota] [-w web-folder_home_directory] [-t webfolder_quota] [-l dl_number] [-s shared_account_number] [-k remark]

INTRODUCTION

Iemsdomacct is used by IEMS administrators to create / delete / list domain accounts via a command line interface.

-C Create a domain account

-D Delete a domain account

-L List all domain accounts

-d domain_name: the name of domain.

-p domain_adm_password: the domain administrator password, maxinum 6 characters

-u user_number: the maxinum number of users that can be created for the domain

-h msgstore_home_directory: optional, if specified, it refers to the Message Store root directory for all all the users under the domain

-q msgstore_quota: the maxinum quota (M Bytes) for the Message Store that can be allocated for all users under the domain

-w webfolder_home_directory: optional, if specified, it refers to the WebFolder root directory for all users under the domain

-t webfolder_quota: the maxinum quota (M Bytes) for Web Folder that can be allocated for all the users under the domain

-l dl_number: the maxinum number of Distribution Lists that can be created for the domain, 0 means disabled

-s shared_account_number: the maxinum number of shared accounts that can be created for the domain, 0 means disabled

-k remark: optional, refers to the remark text for the domain

EXAMPLES

To add a domain account jade.net with 10 users, 1000M Message Store quota, 500M WebFolder quota, 5 Distribution Lists, and no Shared Message Store accounts:

iemsdomacct -C -d jade.net -p password -u 10 -q 1000 -t 500 -l 5 -s 0

CHAPTER 8

Distribution Lists

Overview

The DL (Distribution List) Manager allows messages sent to a single address (the distribution list) to be sent automatically to all of the list's subscribers. It enables the system administrator to create an electronic mailing list that supports the following features: mail blocking, adding subscribers, removing subscribers and setting the preferred delivery options (see Figure 111 on page 173).

By utilizing Distribution Lists rather than the use of aliases or addresses with multiple connectors, non-delivery notifications and other administrative type messages can automatically be sent to the list administrator rather than message originators. This is important since problems with the distribution of messages of this type typically can only be fixed by the list maintainer.

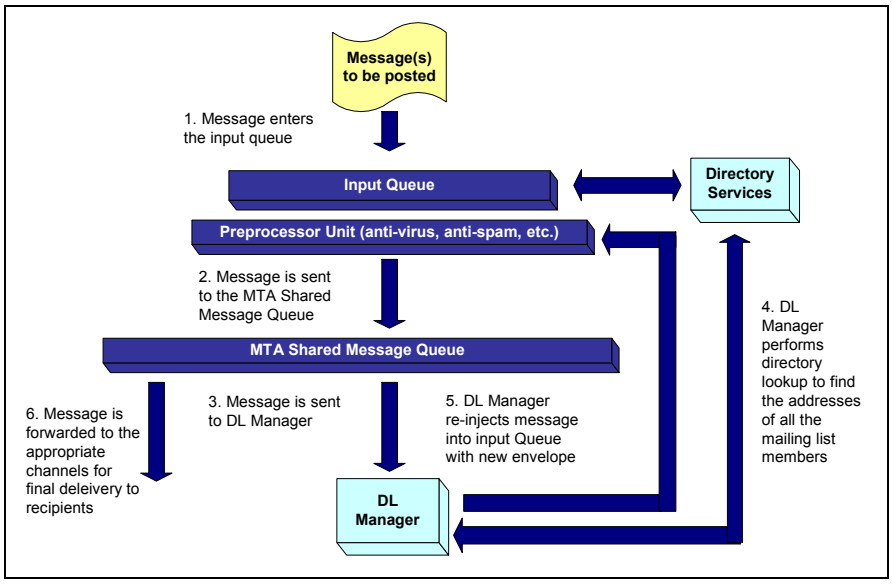

Figure 111: Distribution List Manager system architecture

Types of Distribution Lists

There are four primary types of distribution lists that are commonly used in the Internet. They are based upon two modes of operations, each of which can be configured in either an open or closed configuration. The *subscription mode* of a distribution list controls how new subscribers are to join a list. The *posting mode* of a list controls who can and cannot post to a given list.

Subscription Modes
The subscription mode of a list determines how new subscribers are to join a given list. *Open subscription lists* allow potential subscribers to directly subscribe to a list without requiring list owner intervention. The entire process is automated, with list membership open to everyone after passing a basic authentication check. Many public lists are run in this manner, as membership control is either not necessary or undesirable.

Closed subscription lists on the other hand do not allow for automated subscription, as the membership needs to be monitored or controlled by the list maintainer. Examples of such list are company staff distribution lists, where it would not be wise for arbitrary people outside the organization to be able to join in discussions which may be company confidential.

Posting Modes
The posting mode of a list determines who is allowed to post messages to a given list. *Open posting lists* allow both members as well as non-list members to post messages to the list. Many public lists still operate in this mode as it is desirable to have as many people contribute as possible. This type of list however is not as popular as it once was due to spam attacks on these type of lists by outside parties.

Closed posting lists on the other hand only allow list subscribers to post to the list. This allows much better control over who has access. For the staff list example above, the closed posting mode is also a good choice, so that outside parties, such a recruiters, or other undesirables (in the eyes of the corporation) are not permitted to easily reach all the list's members.

Distribution List Addressing Conventions

When IEMS creates a new distribution list, in addition to the primary distribution address (*list@domain.com*), two additional addresses are established. By convention, the *-request* address (*list-request@domain.com*) is used to send administrative requests, such as subscription and unsubscription requests to. In addition, a *-owner* address (*list-owner@domain.com*) is established. When messages are sent from the Distribution List Manager, they are sent with an envelope sender set to the *-owner* address. This way, if any errors or problems are encountered during transit or delivery of DL processed messages, the notification will be sent back to the list maintainer rather than the original message originator.

Subscription Process

Potential subscribers request membership to a distribution list by submitting a subscription request to the Distribution List Manager. These requests can be either submitted through the IEMS Web Interface (*Mailing List Subscription* button on the main login page) or by sending an message to the *-request* address, i.e. *list-request@domain.com*, with the first line of the message being: *Subscribe*.

Before submitting the subscription request to the system administrator or list owner, the DL Manager will verify the authenticity of the request by sending an email to the potential subscriber. The mail will indicate that the request has been received and that it must be returned to the DL Manager before the subscribe's address can be added to the mailing list (see Figure 112 on page 175). This feature is very useful in managing public mailing lists since some of those applying for subscription may be using forged identities.

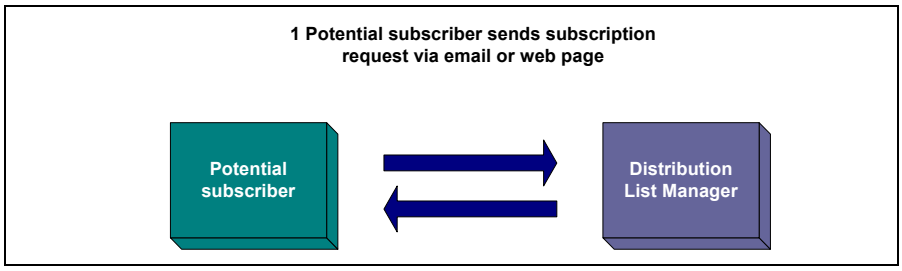

Figure 112: Step 1 of the subscription process

When the potential subscriber replies to the email, the DL Manager will act upon it depending upon the subscription mode of the list. If the list is configured in an open subscription mode, the subscriber will automatically be added to the list without any further action. If the list is in a closed subscription mode, the DL Manager forwards the request to the list owner and waits for the latter's reply (see Figure 113 on page 175). If the DL Manager encounters the word "deny" in the Subject header of the message sent by the system administrator, it will reject the application of the attempting subscriber. Otherwise, the potential subscriber's address will be added to the mailing list (see Figure 114 on page 176).

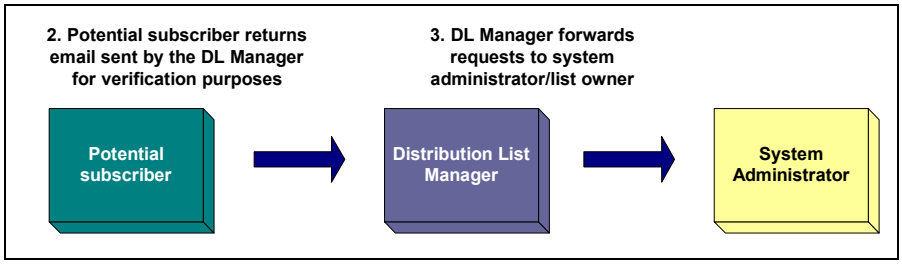

Figure 113: Step 2 of the subscription process

Each distribution list can be separately managed by different list maintainers. They do not need to have system administrator access to the system to run a given list. Each list manager has the capability to add or remove subscribers to lists manually at any time.

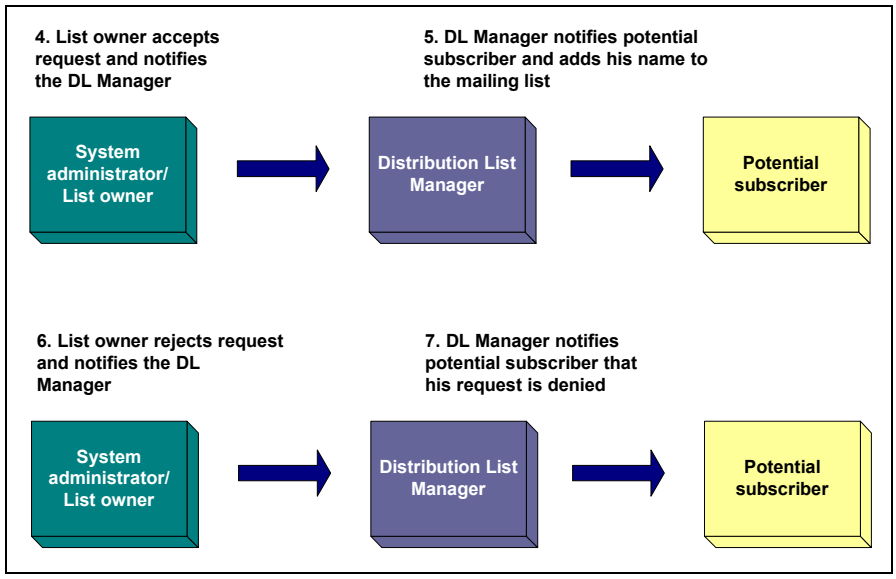

Figure 114: Step 3 of the subscription process

Unsubscription Process

List members may unsubscribe from mailing lists either by requesting to unsubscribe using the IEMS User Tools, or by sending a message to the *list-request* address with the first line of the body of the message of *unsubscribe*. When using the web interface, the DL Manager handles unsubscription requests by automatically removing the member from the mailing list.

For messages that are sent to the DL Manager requesting unsubscription, It first checks if the sender is a registered member of the mailing list. If not, the DL Manager logs an error indicating that the sender is not a member of the mailing list. If the DL Manager verifies that the sender is a registered list member, a confirmation message is sent back to the sender to verify the request. Upon receipt of the confirmation, the sender is automatically removed from that list.

Mail Blocking

Mail blocking is particularly useful for managing open distribution lists. It allows the list owner or system administrator to prevent specific users from sending mail to the list. Upon receiving a message, the DL Manager performs a directory look up to determine whether the address of the sender is included in the list of blocked addresses. If a match is found, the message is bounced back to the sender. Otherwise, the DL Manager processes the message and sends it to the lists' members.

A list owner or system administrator has the right to prevent specific list members from posting messages if his messages only serve as a nuisance to the group. By invoking the mail blocking feature, the member's privilege to post messages can be revoked, although he can still receive messages posted by other members or access the list's archives. Another option for dealing with such situations, although somewhat drastic, is to remove the offending subscriber from the list.

Delivery Modes

The DL Manager offers two modes of delivery: immediate and digest. In *immediate mode*, when messages are posted to a mailing list, the DL Manager sends them immediately to the mailing lists' subscribers. The immediate mode is the default setting. If a subscriber wants his account to be in the digest mode, he must send a request to the list owner or system administrator.

In *digest mode*, posted messages are allowed to accumulate and are sent to the subscriber based on a predetermined schedule set by the list owner or system administrator as requested by the subscriber. The delivery schedule is based on several parameters configured by the list owner or system administrator, such as the day and time of delivery and the maximum number of messages that can be stored as configured in the archive. A web-based user interface is provided to enable the list owner or system administrator to set the option preferred by each subscriber.

DL Manager Engine

The DL Manager Engine monitors the delivery of messages to designated lists. It is also responsible for the delivery of messages to members regardless of the mode of delivery; and for performing automatic subscriptions or unsubscriptions, which would normally be the list owner's responsibilities. The DL Manager engine runs continuously, checking the appropriate channels for new mail and ensuring minimum delay in mail delivery.

Archiving

The DL Manager engine also performs archiving. The engine can optionally keep copies of messages received by distribution lists. The archived messages are stored under the home directory of the DL Manager in a list specific directory. Every archived message contains important information, such as the message headers (i.e., From:, To:, Date: and Subject:) and message body. Each mailing list has its own archive directory where all the archived messages are stored.

DL Archive

A web-based DL archive client is provided allowing users to view messages posted to lists using any web browser. The DL Archive allows both mailing list members and non-members to access the open subscription mode list archives, but limits the access of the closed subscription mode mailing list archives to its members (either local or remote users) only.

Local users are those users defined in the Directory. Remote users, on the other hand, are those users not defined in the Directory, but are members of the closed mailing list.

All closed subscription mode mailing list members are required to go through the DL authentication procedure before they can access the list archives. The authentication procedure requires the mailing list members to enter his username and password as defined in the Directory.

However, remote users must first undergo registration procedure before the authentication. To register, remote users must enter their username and password in the DL Archive registration page. This process verifies if the email address entered is a member of the list. Once verified, an email will be sent to the list member confirming his request. The user must reply to the confirmation email before he will be registered.

The DL Archive sorts messages based on any of the following sorting criteria: Date, Author or Thread. *Archive by Date* sorts all messages on a daily basis. Messages that were sent on the same day will be grouped together. *Archive by Author* sorts all messages by author based on the **From** field of the archived message. Archive by Thread sorts all messages by subject based on the **Subject** field of the archived message. A subject thread is created whenever a message generates one or more reply messages.

The archiving utility also provides the system administrator with a configuration page for the indexing time, allowing the system administrator to select a specific time when the DL engine will start generating index pages of the archive. This can be done via the system administrator “Distribution List” web interface.

Creating a New List

To configure the DL Manager, click the **DL Manager** link on the top menu frame. This action displays the “DL Manager” screen (see Figure 115 on page 178).

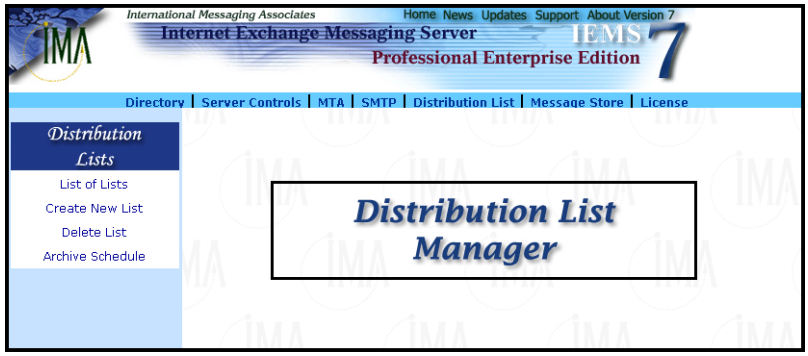

Figure 115: Distribution List Manager

To create a new list, select the ***Create New List*** button on the left menu frame. A screen (see Figure 116 on page 180) for creating a list appears. Provide information on the following fields:

Mailing List Name
The email address of the electronic mailing list to be created. This address must be fully qualified. In other words, if the local mailing list name is *music-people* and it is run from the domain *ima.com*, the mailing list name would be *music-people@ima.com*.

Mailing List Owner
The email address of the person who will maintain or manage the new mailing list. This address must be fully qualified (*jdoe@ima.com*).

Descriptions
A brief description of the mailing list to be created.

Enable Archiving
Set the archiving option either Yes or No. The default is Yes.

Selecting **Yes** will save the messages in the archive folder under the DLMgr sub-directory. Messages will not be saved in the archive folder under the DLMgr sub-directory if the option is set to **No.**

When receiving invalid posting
Choose from the pull-down menu the action to be taken - **bounce to the original sender**, **forward to the list owner**, **bounce and forward**, or **discard** when there is an invalid posting to the list. The default is bounce to the original sender.

Bounce to the original sender
Will send the message back to the original sender when there is an invalid posting to a list. **Forward to the list owner** will pass the message to the list owner of the particular mailing list. **Bounce and Forward** will send the message back to the original sender and at the same time forward the message to the list owner of the particular mailing list. The **Discard** option will delete the message.

Allow posting from non-list member
Selecting **Yes** will allow posting from non-list members. This is usually used for open lists where anyone can post at any time. In recent years this has been problematic in many public lists, as they have become targets for spammers. Selecting **No** will restrict posting to list members only. The default is **Yes**.

Figure 116: Creating A Mailing List

Enable Auto Subscription
When the DL Manager receives a subscription request, it first checks the **Enable Auto Subscription** attribute of the list the sender is trying to subscribe to. If set to **Yes**, the DL Manager activates automatic subscription. A confirmation message is then sent to the prospective subscriber informing him that he must reply to the confirmation message with the word "OK" before he is successfully added to the mailing list.

If set to **No**, the DL Manager passes the subscription request to the list owner. The list owner will then decide if he will add the potential subscriber to the list or not. The default is **Yes**.

Default Posting Permission
The **Allow** permission allows the list member to post messages to the list. The **Block** permission prohibits the list member to post messages to the list to which he is a member. The default is **Allow**.

Remove the Return-Receipt-To Header
Messages that are sent through a distribution list may have a return receipt or delivery notification request attached. If these go through the distribution list and make it to the subscribers of the list, return notifications may be sent back to the original sender. If the list is closed, or if the identities of the subscribers are sensitive or confidential, then allowing these requests through to the subscribers of a distribution list creates a security risk.

Set the header option either Yes or No. The default is Yes. Setting this value to ***Yes*** will remove all Return Receipt and/or DSN requests before they reach the list subscribers.

Use MIME Digest
Distribution lists that generate digests (a collection of list messages compiled into a single message) have the option of using MIME or non-MIME digest formats. MIME formatted digests attach each submitted message as a separate message type attachment, while non-MIME digests append the content of each message as plain text in the digest.

For lists where recipients are using older non-MIME compliant readers, or if the nature of the list is entirely text based, non-MIME digests can be used. For all other applications, especially where structured messages, including HTML and other rich text formats are used, or if attachments are common, the MIME digest type is recommended.

Set the MIME digest either Yes or No. The default is Yes.

Maximum Message Digest Size
The maximum size of the message digest. The default value is 0, which means no limit. If the message digest size is given a value other than zero and it exceeds the limit, the message will be divided into several smaller messages, each of which are equal to or smaller than the specified maximum message size.

Digest Generation at
Set the digest generation options **Daily**, **Weekly**, and **Monthly** to generate digest message. The system administrator can also specify the day, hour, and minute when the message digest shall be generated.

After setting all the required information, click the Next button. This action displays the default auto text locations screen (see Figure 117 on page 182), allowing the system administrator to modify or change the directory path of each text or HTML files.

Spam Filter Configurations
If MTA Pass-Through has been enabled (Professional Enterprise Edition), each distribution list can define its own policy for handling messages tagged by the system as potential spam. The settings here are basic settings that are initially applied to all MTA Pass-Through tagged messages. Choices are to *Ignore*, *Discard*, or *Bounce* spam tagged messages. Finer control is available where actions can be defined on a per DNS-BL basis in addition to the *SpamAssassin* identified messages. Per-DL whitelisting is also possible. For more information, see “Modify Spam Filter Settings” on page 185.

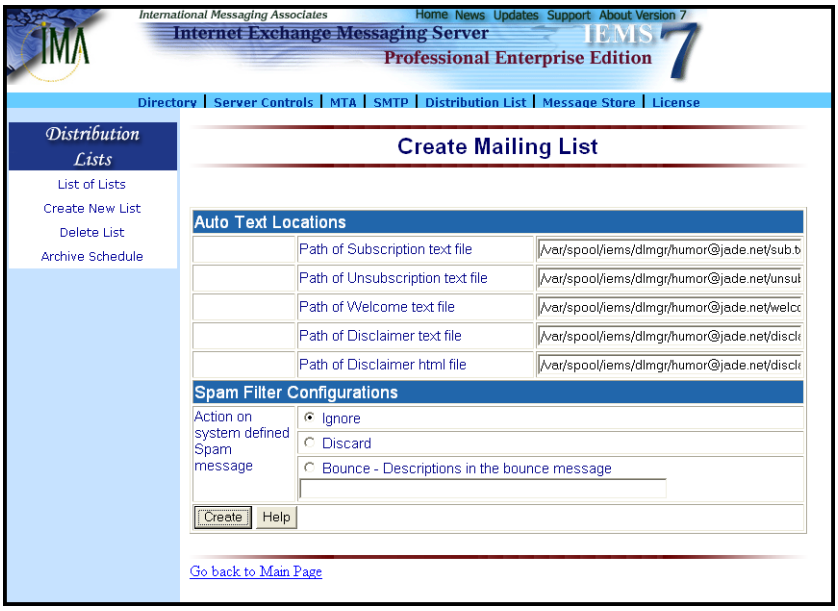

Figure 117: Creating A Mailing List (2)

After selecting the locations for the auto-insertion files and spam filter settings, click the ***Create*** button to store the new list in the database.

The system administrator may delete a mailing list and its subscribers from the distribution lists. Deleting a mailing list will also remove the corresponding entry and connector information in the Directory.

Creating Descriptive Information

The system administrator is allowed to provide a short or long description of the mailing list by clicking the **Descriptive Information** link from the “List of Mailing Lists” screen (see Figure 118 on page 183). He may also create a welcome or farewell message for the mailing list members. The welcome message is sent to those members who were automatically added via automatic subscriptions. The farewell message is sent to those members who were removed from the mailing list via automatic unsubscriptions. Click the ***Save*** button to save the settings.

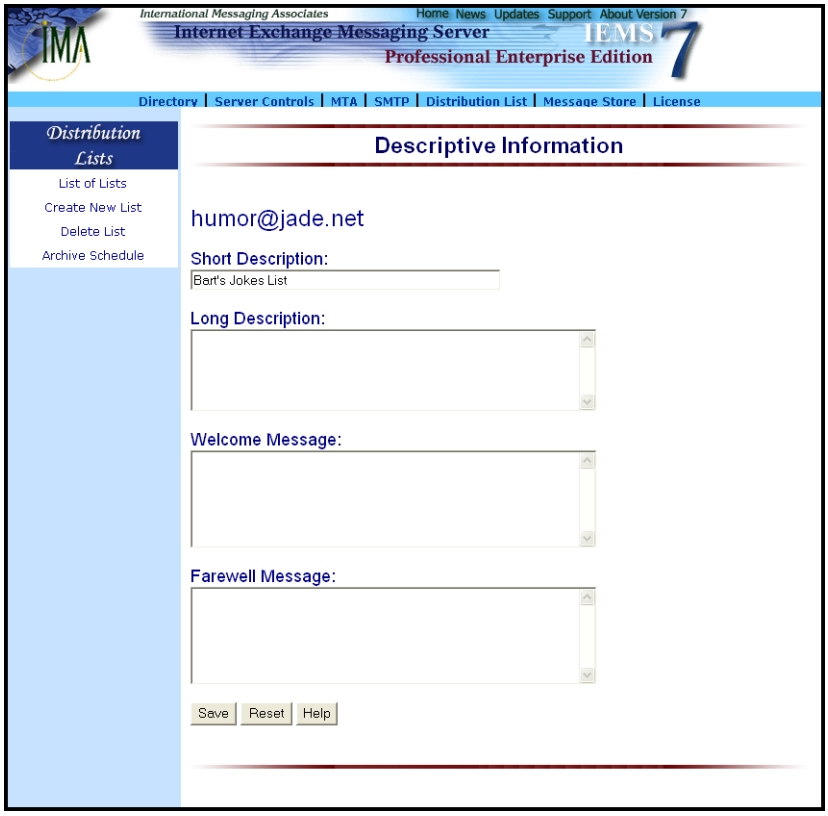

Figure 118: Creating Descriptive Information

Modifying List Settings

Mailing list settings can be modified by entering the correct values for the different mailing list attributes. To do this, click the **Modify List Settings** link from the “List of Mailing Lists” screen (see Figure 126 on page 190). This action displays the “Modify Mailing List Settings” screen (see Figure 119 on page 184). Please see “Creating A Mailing List” on page 180 for more information on each field.

After modifying or updating the mailing list attributes, click the ***Update*** button to save the changes.

Figure 119: Modifying Mailing List Entries

Modify Spam Filter Settings

For systems with MTA Pass-Through enabled, distribution lists can also utilize this information on a list by list basis. All spam pass-through controls made available to local mail users, with the exception of auto-filing to predefined folders, is supported for distribution lists.

To configure the spam settings for the current distribution list, click on the ***Modify Spam filter settings*** button in the *List of Mailing Lists* listing. The *Spam Filter Configurations* screen will be displayed (see Figure 120).

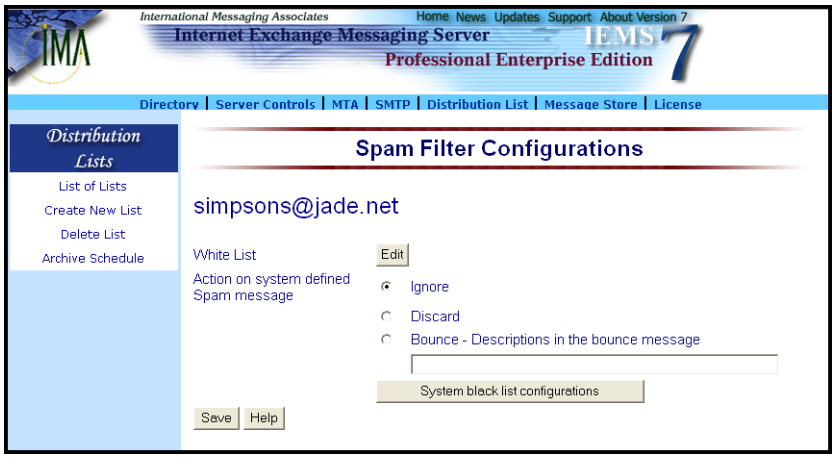

Figure 120: Spam Filter Configurations

The screen is laid out in two sections - DL whitelists and MTA Pass-Through handling.

DL Whitelists

There can be times where it is not desirable to apply spam filtering to messages. Examples include messages from friends, family, and close business associates. Messages from trusted sources such as these are usually desirable regardless of content. IEMS allows for the configuration of DL whitelists, containing the email addresses of trusted senders where normal anti-spam filtering should not be applied. To configure DL whitelists, click on the ***Edit*** button next to the *White List* tag on the top of the screen. The following screen will be displayed:

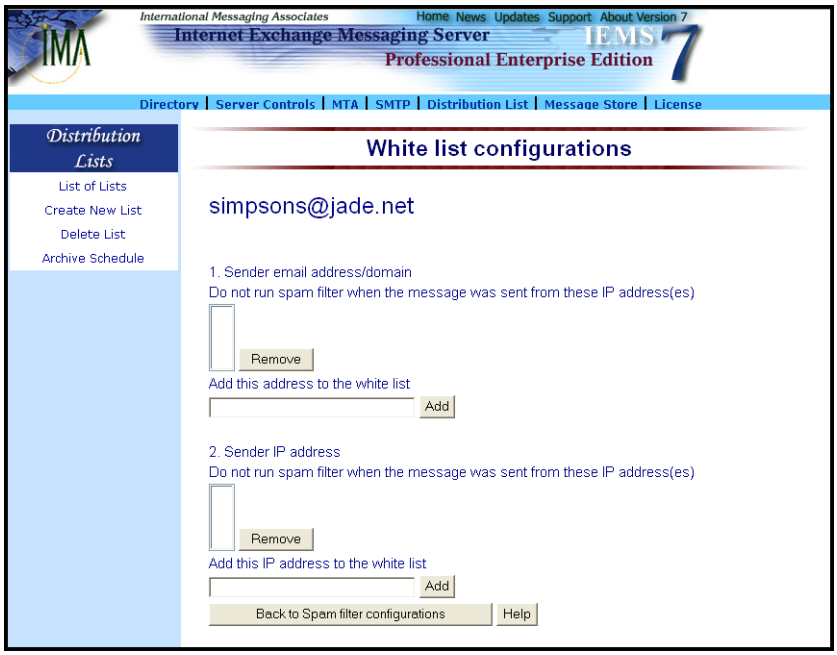

Figure 121: DL White List Configuration

The White List Configuration is presented in two sections - *Sender Email Address Configuration*, and *Sender IP Address Configuration***.** Both can be used and configured independently of the other.

To add the sender email address to the list of allowed senders, type the address under the *Add this address to whitelist* entry and then click the ***Add*** button. If you want to specify a domain, you can use the wildcard "*" character when entering the address. For example:

**@company.com*

will white list all sender from the domain *company.com*.

To remove a sender, select the address from the address list and click the ***Remove*** button.

To add the sender IP (network) address, type the IP address under the *Add this IP address to whitelist* entry and then click the ***Add*** button. If you want to specify a range of IP address, you can use dash "-" character. For example:

192.168.0.0-192.168.0.255

will white list all IP address from 192.168.0.0 to 192.168.0.255.

To remove a sender IP, select the IP address from the address list and click the ***Remove*** button.

MTA Pass-Through Handling

Spam detection procedures that are applied within the MTA can optionally have action deferred until such time as an agent for the user (Distribution List Manager) has control of the message. These MTA Pass-Through actions are defined in the second section of the Spam Filter configuration page. This section is identified by the label *Action on system defined Spam message* (See Figure 122).

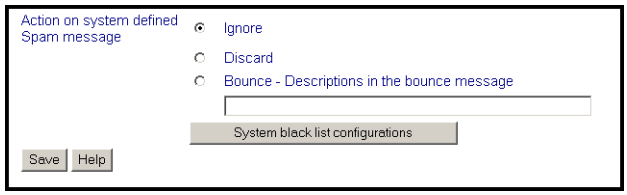

Figure 122: DL MTA Pass-Through Configuration

A message can be marked as Spam by the Internet Exchange Message Server SpamAssassin plugin module, or reported by the DNS-BL lookups at SMTP connection time. When such a spam tagged message is received, you can configure the list profile to perform one of the following actions:

Ignore - Ignore the spam message and continue normal delivery.

Discard - Discard the message such that your mailing list member will not receive this message.

Bounce - Bounce the message back to the sender.

When bouncing a message, the text of the message sent back to the sender can be configured in the box below the ***Bounce*** selection.

When there is one or more DNS-BL host defined in the system, the ***System black list configurations*** button will be displayed. Click this button to configure specific actions to perform on a per DNS-BL tagged message basis (see Figure 123). In this page, you can define action against spam message marked by certain DNS-BL host.

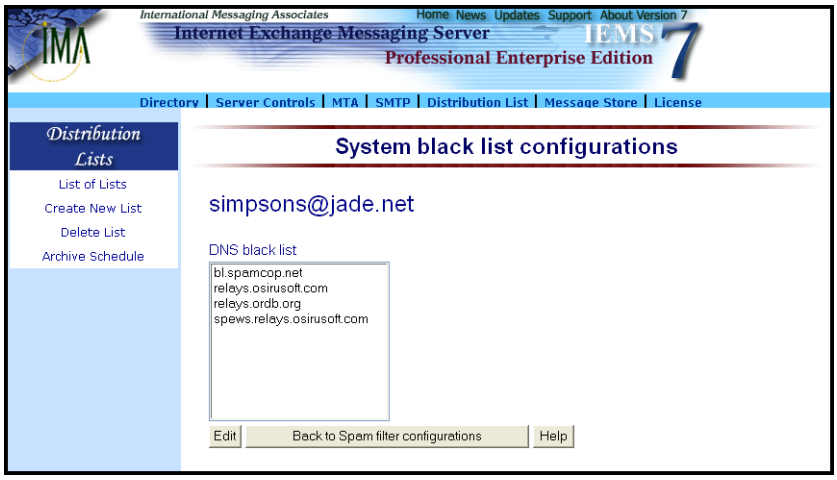

Figure 123: DL DNS Black List Configuration

When there is one or more DNS-BL host defined in the system, this configuration page will be available. You can different actions against each DNS-BL host in your server to refine your spam filter behavior. To configure, first select a DNS-BL host name and then click the ***Edit*** button. The Black List Configuration page (see Figure 124) will be displayed.

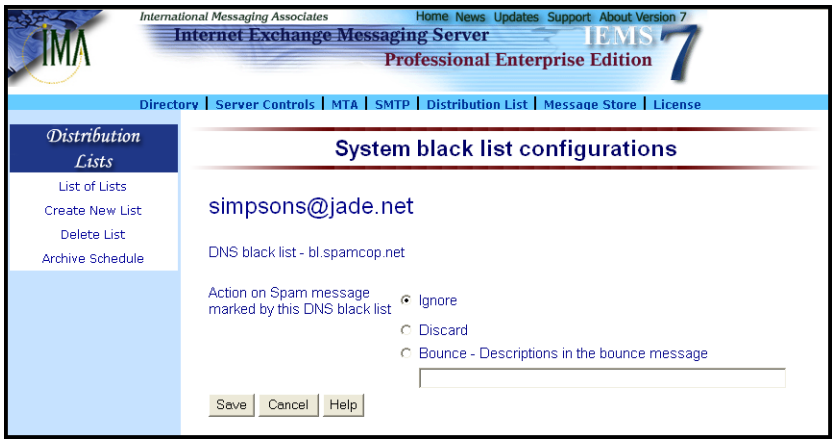

Figure 124: DL DNS Black List Configuration (2)

For each DNS-BL host, you can select one of the following actions:

Ignore - Ignore the spam message and continue normal delivery.

Discard - Discard the message such that your mailing list member will not receive this message.

Bounce - Bounce the message back to the sender.

When bouncing a message, the text of the message sent back to the sender can be configured in the box below the ***Bounce*** selection.

Removing Lists

To delete a mailing list and its subscribers, click the ***Delete List*** button on the left menu frame (see Figure 125 on page 189). The “Delete Mailing Lists” screen appears. Select the name of the mailing list to be deleted from the pull-down menu. Click the ***Delete*** button.

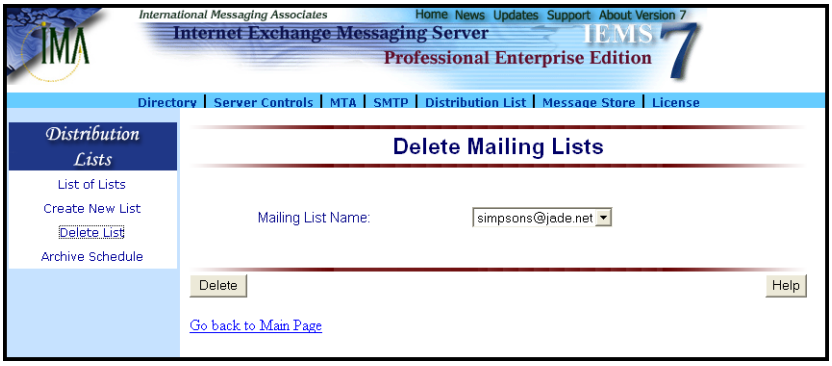

Figure 125: Deleting A Mailing List

Searching For Lists

The system administrator may search for a particular mailing list that is serviced by the DL Manager without displaying the complete list of mailing lists. The system administrator is also allowed to perform other mailing list-related operations, such as editing subscriber lists, creating a descriptive information and modifying list settings.

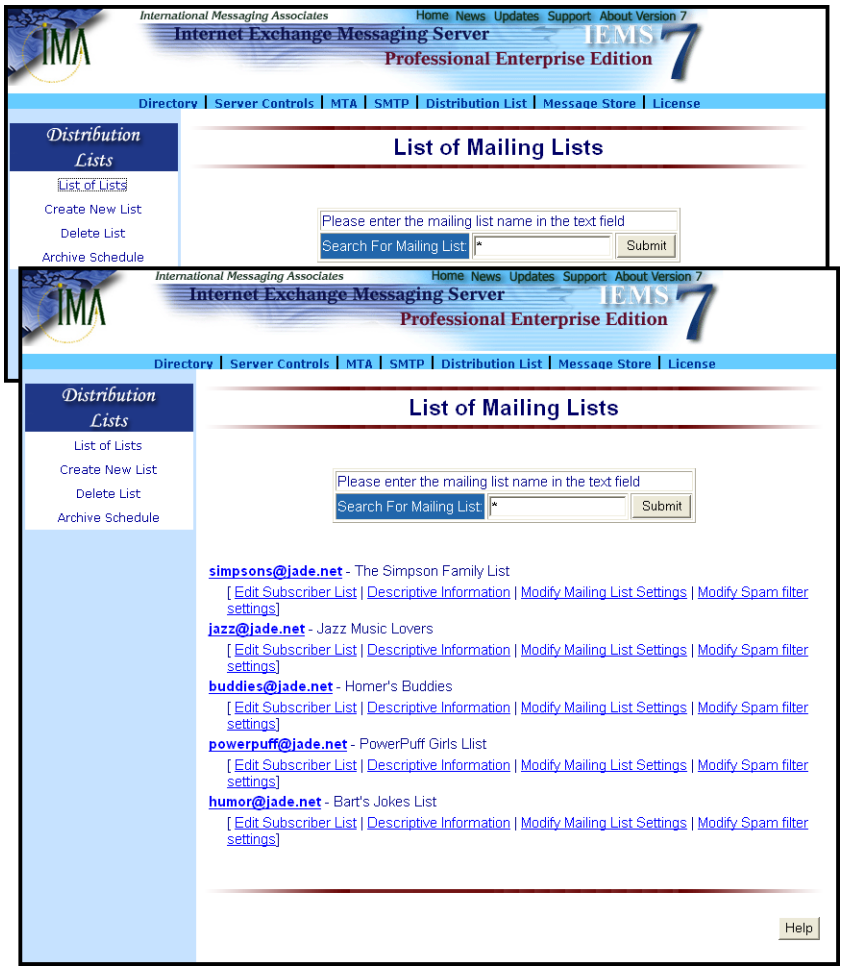

Figure 126: Searching For Mailing Lists

To search for a mailing list, click the ***List of Lists*** button on the left menu frame. This action displays the “List of Mailing Lists” screen (see Figure 126 on page 190). Type the mailing list name in the **Search for Mailing List** field. Click the ***Submit*** button.

Note: *Use of wildcards (*) displays all the available mailing lists.*

Mailing List Profiles

The “List of Mailing Lists” screen displays the primary address and the short description of the searched mailing lists. Each mailing list address is linked to a “Mailing List Profile”. Click the mailing list address to view the list’s attributes (see Figure 127 on page 191).

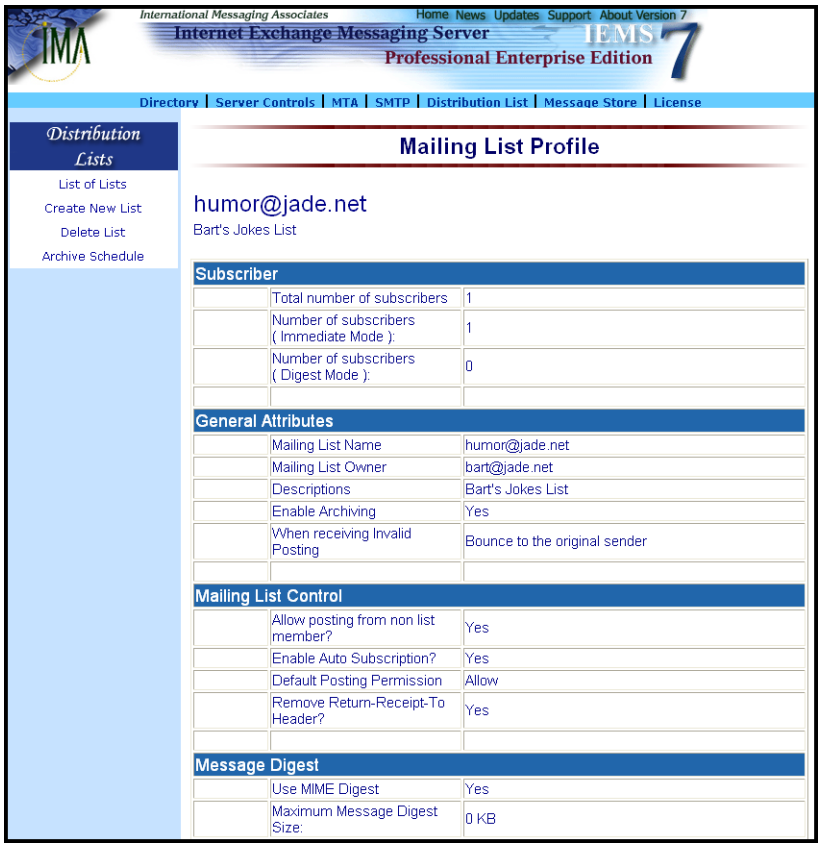

Figure 127: Displaying Mailing List Profile

Adding Or Removing Subscribers

The system administrator may add or delete members from any list by selecting the **Editing Subscriber List** link from the “List of Mailing Lists” screen. This action displays the “List of Subscribers” screen (see Figure 128 on page 192).

Adding Subscribers

To add subscriber(s), type the email address of the subscriber(s) in the **Subscribers to Add** list box. Select a delivery method by ticking the **Immediate** or **Digest** radio button.

In immediate mode, when messages are posted to a mailing list, the DL Manager sends them immediately to the mailing list’s subscribers. The immediate mode is the default setting.

If a subscriber configured for immediate mode delivery wants his account to be digest mode, he must send a request to the list owner or system administrator.

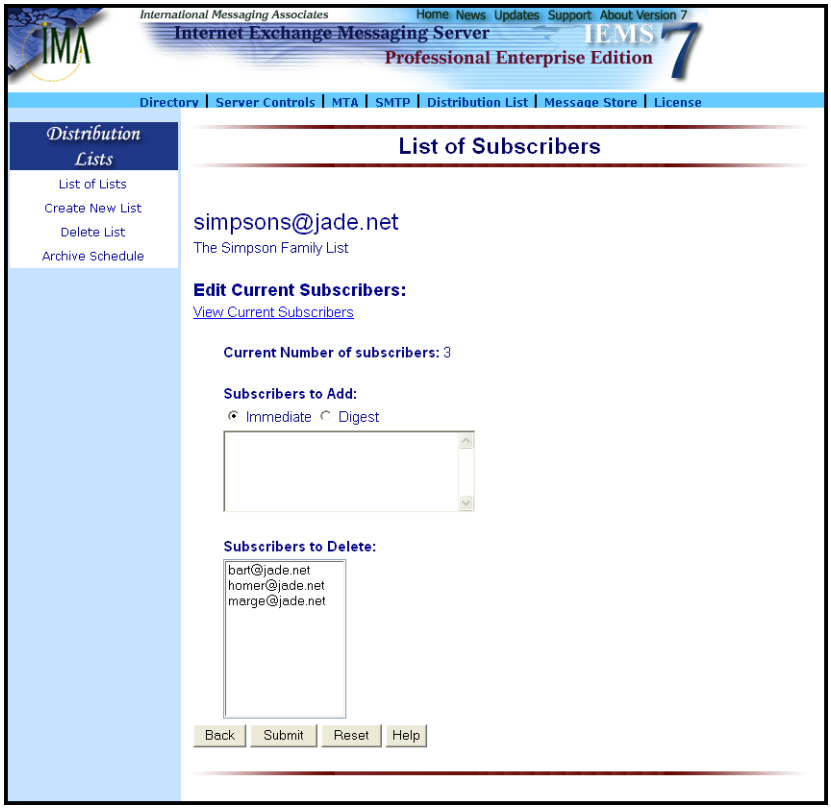

Figure 128: Adding or Deleting Mailing List Subscribers

In the digest mode, posted messages are allowed to accumulate in the local archive of the member(s) who selected this mode and are sent to the subscriber based on a predetermined schedule set by the list owner or system administrator. The delivery schedule is based on several parameters configured by the list owner or system administrator, such as the day and time of delivery and the maximum number of messages that can be stored as configured in the archive.

Deleting Subscribers

The system administrator may delete members from mailing lists to remove their subscription. The members who were removed will not be able to receive message postings from the other members of the mailing list.

To delete subscribers, select the email address of the subscribers in the **Subscribers to Delete** list box and click the ***Submit*** button.

Note: *Multiple deletion or addition of members is allowed. To delete or add multiple members, enter the email address to be deleted separated by a comma, semicolon, or space after each mailing addresses.*

Viewing Current Subscribers

To view the list of current subscriber(s), click the **View Current Subscribers** link on the “List of Subscribers” screen (see (see Figure 128 on page 192)). This action displays the list of current subscribers (see Figure 129 on page 193).

Figure 129: List of Current Subscribers

Links that corresponds to the posting permission of the user are given on this screen. The system administrator may either block or unblock the posting permission of the subscriber(s). Clicking the **Block** link beside the **Delivery Mode** column marks the subscriber as blocked. This means that the subscriber is not allowed to post messages to the list. Clicking the **Unblock** link removes the blocked setting of the subscriber. This means the subscriber is allowed to post messages to the list.

Each mailing list address is linked to the “Mailing List Member” screen. Click the mailing list address under the Subscriber column to edit the profile (email address and delivery mode) of the subscriber.

Updating List Owner Password

The distribution list owner or system administrator may update his password to secure the mailing list settings.

The DL Manager allows the list owner of the mailing list to update its password. To do this, click the **Update List Owner Password** link at the bottom of the “Modify Mailing List Settings” screen. The “Update Password” screen (see Figure 130 on page 194) appears.

Indicate the new password in the **New Password** and **Confirm Password** fields. Click the ***Update*** button to save the new list owner password.

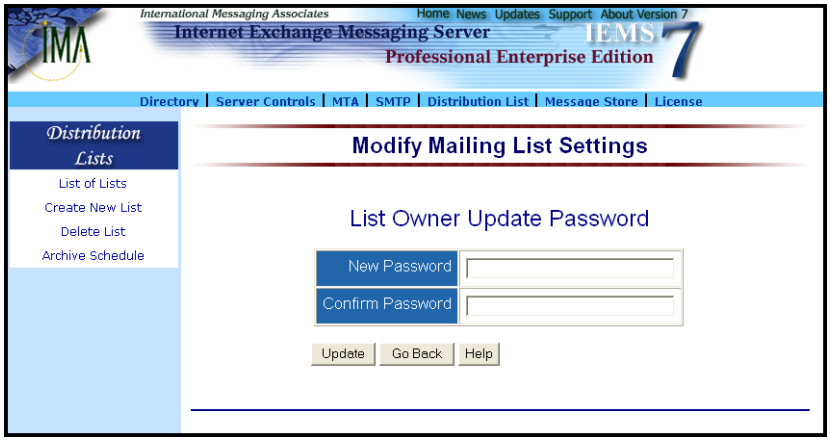

Figure 130: Updating List Owner Password

Archive Scheduling

Setting The DL Archive Schedule

Before users can access list archives, the system administrator must run the Archive Rebuild Utility (arcrebuild), a command line program that converts the archived messages into database format. This utility enables the archiving feature of the Distribution List Archives. To run the arcrebuild, open the MS-DOS Prompt (for Windows) or UNIX shell (for Linux). Go to the directory where the IEMS is installed (*e.g. C:\Program Files\Ima\IEMS 7* (Windows) or */opt/iems/bin* (Linux) and run the arcrebuild utility.

Options:

-l - This will list all the registered mailing lists that has an Enable Archiving attribute that is set to Yes.

-f - This will rebuild the archive database of all the mailing lists that has an Enable Archiving attribute that is set to Yes.

mailinglist - Rebuilds the archive database of a specific mailing list that has an Enable Archiving attribute that is set to Yes.

For example:

To perform full rebuild, type:

```
arcrebuild –f
```

To list all registered mailing lists, type:

```
arcrebuild -l
```

To rebuild the archive database of a specific mailing list, type:

```
arcrebuild jazz@ima.com
```

to rebuild the *jazz@ima.com* list.

Note: *Before running the arcrebuild utility, make sure that the Directory Server is running.*

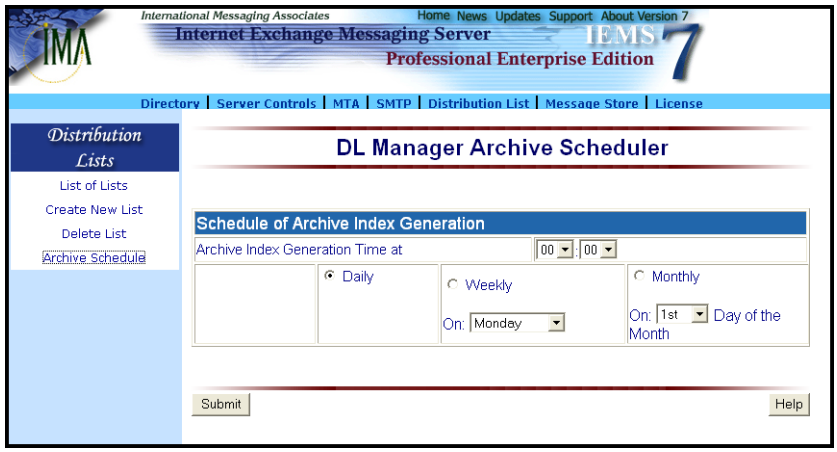

Figure 131: Archive Scheduler

The **Indexing Time** of the Archiving Utility must also be configured. Configuring the Index Time means that you do not have to run the arcrebuild utility manually. This is the automated process of rebuilding the DL Archive.

The Indexing Time is the time when the DL engine will start generating the index pages of the archive. To configure the **Indexing Time** of the DL Archive, click the ***Archive Schedule*** button. This action displays the “DL Manager Archive Scheduler” screen (see Figure 131 on page 195).

Choose from three options “Daily, Weekly or Monthly” to update the index pages of all mailing lists. **Daily** means the index pages will be updated on a daily basis at the time specified. **Weekly** means that the index pages will be updated once a week at the day and time specified. Specify the day (Monday, Tuesday, etc.) during the week when the DL Archive engine will run. **Monthly** means that the index pages will be updated once a month at the day and time specified. Specify the day of the month (1st, 2nd, etc.) when the DL Archive engine will run then click the ***Submit*** button to save the changes.

IEMSDLMBR

Iemsdlmbr is a command line utility used to create, delete, or list distribution list members.

NAME

iemsdlmbr - manipulate IEMS Distribution List Members

SYNOPSIS

iemsdlmbr [-A|D|L] [-l list_name] [-m member_name] [-d delivery_mode] ...

INTRODUCTION

Iemsdlmbr allows the IEMS administrator to add/delete/list Distribution List members using a command line interface.

-A Add a new member to an existing Distribution List

-D Delete a member from an existing Distribution List

-L List all members of an existing Distribution List

-l list_name is the name of the Distribution List to be managed

-m member_name is the email address of the target Distribution List member

-d delivery_mode (optional) is the delivery mode for the member. Possible values are **Digest** and **Immediate**. The default is **Immediate**

EXAMPLES

To add peter@jade.net, to the DL engr@jade.net and set the delivery mode to Digest:

```
iemsdlmbr -A -l engr@jade.net -m peter@jade.net -d Digest
```

ARCREBUILD

Arcrebuild is a command line utility used to rebuild distribution list archives.

NAME

arcrebuild - Distribution List Manager archive rebuild utility for Internet Exchange Messaging Server

SYNOPSIS

arcrebuild [l] | [-f] | [mailinglist]

DESCRIPTION

The archive rebuild utility is used to rebuild archive databases used by the distribution list module. This utility can be used to recover from almost any form of data corruption in the Distribution List archive databases.

To use the arcrebuild utility, it is recommended that the Distribution List module first be shut down. Doing this will enable the arcrebuild utility to rebuild the archive databases faster because no other module will be competing with it for the locking of the databases.

OPTIONS

The **arcrebuild** may be run in one of three different modes:

-l Displays all the registered mailing lists that has the Enabled Archiving attribute set to YES.

-f Rebuild all distribution list archive databases. **Arcrebuild** will traverse all distribution list accounts and rebuild all archive database files. This may take some time, and should not be interrupted.

mailinglist

Rebuild the archive databases for a single Distribution List account. Arcrebuild will rebuild only the given Distribution List account.

EXAMPLES

To rebuild all Distribution List account databases:

arcrebuild -f

To list all Distribution Lists with archiving enabled:

arcrebuild -l

To rebuild the single Distribution List outdoors@domain.com:

arcrebuild outdoors@domain.com

FILES

/var/spool/iems/dlmgr

Default location for Internet Exchange Distribution List

CHAPTER 9

Web Mail Client

Overview

The Web Mail Client is a collection of CGI (Common Gateway Interface) programs that allows users to read, send or forward their messages from the local Message Store using any web browser anytime, anywhere.

The CGI programs use the Message Store API (Application Programming Interface) to interface with the Message Store. The Web Mail Client is composed of the following CGI programs:

- **LOGIN**
  Validates the username and password when a user logs in the Web Mail Client.
- **MENU**
  Displays the Menu Frame together with the different Menu hyperlinks in the Web Mail Client.
- **VFOLDER**
  Presents a summary information of the different folders. It also allows users to copy, move or delete a particular folder.
- **VIEWMSG**
  Allows users to view and manipulate their mail messages.
- **GETFILE**
  Displays the file attachments contained in mail messages.
- **DELMAIL**
  Deletes unwanted messages in the file folders of users for mail maintenance and management.
- **NEWMAIL**
  Lets users compose mail messages; reply to mail messages; or forward mail messages to other recipients.
- **FOLDER**
  Provides the functionality to let users manage their folders.

The Web Mail Client user interface can be customized to suit the look and feel of your organization. System administrators may insert the company logo, banner, CGI scripts or animated files in the headers and footers of the Web Mail Client interface to fit the company's image. In customizing the Web Mail Client interface, the system administrators may edit the HTML source code of the login page; modify the style sheets of the different Web Mail Client screens; edit the **IEMTA.INI** (Windows) or **IEMS.CONF** (Linux) file to modify the headers and footers of the screens.

Note: *The steps in viewing the message list in the Inbox, Outbox and user-defined folders; opening and reading messages; viewing message attachments via the Web Mail Client can be found in the* ***Internet Exchange Messaging Server 7 User's Guide.***

Web Mail Login Page

To customize the Web Mail Client Login page, build an HTML script with a FORM component pointing to */iems/scripts/login.cgi* (Linux) or */iems/scripts/login.exe* (Windows).

To view the default HTML source code, click the **View** menu on the web browser and select **Source** from the pull-down list.

To edit the source code, start IEMS and go to web administration. The main IEMS web interface should appear. Click the ***Web Mail Login*** button to display the main login screen of the Web Mail Client. Click the **View** menu and select **Source** from the list of commands. This displays the HTML source code of the "Web MailLogin" screen. Modify the source code according to the image and standards of your organization. After editing the source, save the file as **login.htm** in *C:\Program Files\IMA\IEMS 7\Apache\HTDocs\IEMS* (Windows) or */opt/iems/htdocs/iems* (Linux) folder. Open your web browser and type:

http://machinename.domain.com/iems/login.htm

in the address field. The new "Web Mail Login" screen will appear.

The HTML source of a sample customized login page of the Web Mail Client (Linux) is given below. For the source below to run with a Windows IEMS backend, simply change the reference to *login.cgi* to *login.exe*.

```
<html>
<head>
<title>Jade Web Mail Login</title>
</head>
<body>
   <form action="http://mail.jade.net/iems/scripts/login.cgi" method="POST">
   <input type="hidden" name="domainname" value="jade.net">

<table border="0" cellpadding="5" width="300">
     <tr><td bgcolor="#336699">
     <p align="center"><font color="#FFFFFF" face="arial, helvetica">
     <strong>Jade Web Mail Login</strong></font></p>

    <table border="0">
      <tr><td><font color="#FFFFFF" face="arial, helvetica">
      Username: <br>
      Password: 
      </font></td>

      <td><font color="#FFFFFF" face="arial, helvetica">
      <input type="text" size="20" maxlength="255" name="name"><br>
```

```
    <input type="password" size="20" maxlength="255" name="password">
    </font></td></tr>
  </table>

  <p align="center">
  <input type="submit" name="Command" value="Login"> </p>
  </td></tr>
  </table>
</form>
</body>
</html>
```

The output of the HTML sample is given below (see Figure 132 on page 201).

Figure 132: Sample New Web Login Page

In the example given above, note the use of form fields. The fields used in this example include:

domainname: when present indicates the domain name to use with the login name. This allows users to enter only the local part of the email address. In our Bart Simpson example, instead of entering a login name of *bart@jade.net*, he would only have to enter *bart*. This example sets *domainname* as a hidden variable.

name: the account name of the user

password: the password associated with the supplied account name

Web Mail Client Login Using Multiple Domains

The system administrator may also customize the “Web Mail Login” screen to support multiple domains of the users.This allows the users to easily log in using the different local domains you created within IEMS. In the source below, the *domainname* value that was hidden in the above example is brought out into a selection box in the form so that the user can determine what domain name to login under. As with the example above, this is coded for a Linux IEMS backend, and a simple change of the reference to *login.cgi* to *login.exe* is all that is required to support a Windows IEMS backend.

```
<html>
<head>
<title>Multi-System Web Mail Login</title>
</head>
<body>
  <form action="http://mail.jade.net/iems/scripts/login.cgi" method="POST">

  <table border="0" cellpadding="5" width="300">
   <tr><td bgcolor="#336699">
   <p align="center"><font color="#FFFFFF" face="arial, helvetica">
   <strong>Multi-System Web Mail Login</strong></font></p>

  <table border="0">
    <tr><td><font color="#FFFFFF" face="arial, helvetica">
    Username: <br>
    Password: 
    </font></td>

    <td><font color="#FFFFFF" face="arial, helvetica">
    <input type="text" size="20" maxlength="255" name="name"><br>
    <input type="password" size="20" maxlength="255" name="password">
    </font></td>

    <td>  </td>

    <td valign="top"><font color="#FFFFFF" face="arial, helvetica">
    <select name="domainname" size="1">
    <option value="ima.com">ima.com</option>
    <option value="jade.net">jade.net</option>
    </select>
    </font></td></tr>
  </table>

  <p align="center">
  <input type="submit" name="Command" value="Login"> </p>
  </td></tr>
  </table>
</form>
</body>
</html>
```

The output of the HTML sample above is given in Figure 133 below.

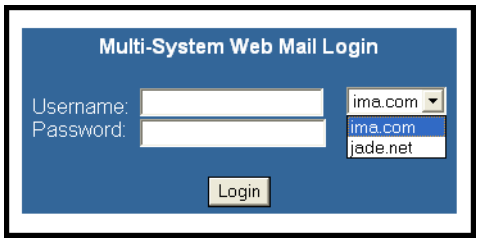

Figure 133: Web Mail Client Login Supporting Multiple Domains

To create a link between the main “IEMS’ web interface and the “Web Mail Login” screen, go to *C:\Program Files\IMA\IEMS 7\Apache\HTDocs\IEMS* (Windows) or */opt/iems/htdocs/iems* (Linux) directory. Open the **index-start.htm** file and edit the source code of the **login.exe** command. Type the name of the new HTML file, then save the file. See HTML script below:

```
<p align=”center” ><a href=”/iems/login.htm?Command=ShowLogin”
target=”_top”>Web mail login</a></p>
```

Now, go to the C:\Windows (Windows) or /etc (Linux) directory. Open the IEMTA.INI (Windows) or IEMS.CONF (Linux) file. In the [WebClient] setting, type the following entries below:

```
[WebClient]
LoginURL-domainname=
```

For example:

```
[WebClient]
LoginURL-domainname=/iems/login.htm
```

Save the file then, go to the main “Internet Exchange” web interface. Click the Refresh button. Click the ‘Web Mail Login’’ button to display the new “Web Mail Login’ screen.

Domain Based Style Sheets

The Web Mail Client uses cascading style sheets (CSS) for customizing the color, font size and font style of the “Web Mail Client” screens. CSS is a mechanism for controlling the style(s) (e.g. fonts, colors, spacing) of a web document. With cascading style sheets, the system administrator can decide how headings will appear by entering that information once in the style sheet. Page linked to this style sheet will have the same heading.

Note: *The style sheet may differ in browser compatibility. This means that some commands may not be applicable for some browsers or the actual output may differ for some web browsers. A browser compatibility chart can be found at http://www.webreview.com/style/css1/charts/mastergrid.shtml. It displays a comprehensive chart for comparing browser support.*

The system administrator can configure the style sheets by modifying the different configurable items of the Web Mail Client’s CGI components found on page 4-104. He may edit the font size, font style, font color and background of the different “Web Mail Client” screens.

The Web Mail Client also allows the system administrator to set up different style sheets based on the domain names of the local Message Store users. This means that the system administrator may customize the Web Mail Client interface for every domain name. A different design or color can be applied to the “Web Mail Client” screens of a different domain.

By default, the Web Mail Client reads the style sheet information of the ieclientstylesheet.css file from the *C:\Program Files\IEMS 7\Apache\HTDocs\IEMS\STYLE\WMC* (Windows) or */opt/iems/htdocs/iems/style/wmc* (Linux) directory for the default domain.

If the mail system supports more than one domain, it is possible to implement different style sheets based on individual domains. This means that a separate style sheets can be implemented by creating a sub-directory for each domain. For example the default domain is “ima.com”. The sub-directory to be created is “jade.net”. To create a sub-directory, go to the *C:\Program Files\IMA\IEMS 7\Apache\HTDocs\IEMS\ STYLE\WMC* (Windows) or */opt/iems/htdocs/iems/style/wmc* (Linux) directory. Click the **File** menu and select **New** then, **Folder**. Type the sub-directory name (i.e., jade.net). Copy the default **ieclientstylesheet.css** file to the “jade.net” folder.

Note: *There should be one style sheet for the default directory and one for the sub-directory. The new style sheet will only be used after creating a new domain directory and copying the default* **ieclientstylesheet.css** file to the sub-directory.

To access the style sheet, go to the *C:\Program Files\IMA\IEMS 7\Apache\HTDocs\IEMS\STYLE\WMC* (Windows) or /opt/iems/htdocs/iems/style/wmc (Linux) directory, right click on the “**ieclientstylesheet.cs**” file and click the open command. Any text editor that supports ASCII text (i.e., “Notepad” for Windows or “text editor” for Linux) can be used to open the style sheet.

To modify the attributes of the style sheet based on your preferences, edit the font size, font style or font color of the specific attribute. Save the style sheet file when you are done. Go back to the “Web Mail Client” interface and click the ***Refresh*** or ***Reload*** button to view the new style.

The following page contains a list of the different screens within the Web Mail Client with a table of all the style sheet item class and item names in the “**ieclientstylesheet.css**” file. It also contains a list of the controllable areas of the different item class and item names. The item class refers to the style of the section of the “Web Mail Client” screen where the style sheet applies. The item name refers to the particular area of the item class that the style sheet applies to.

For example, the “Login” class pertains to the style of the “Login” screen. This is also the HTML tag used in the HTML source code. The item name “Body” of item class “Login” pertains to the default background color, margin, font family, font color and font size of the “Login” screen. If the administrator defines another background color for this attribute, the background color of the “Login” screen will also be changed. The circled numbers refer to the position of the item class names listed in the table on the next page. A brief explanation of the item names used in the tables for customizing the associated screens is also displayed. The format used by the different attributes in the style sheet is given on the next page.

Body.login(1)

Where:

Body - refers to the item name; HTML tag.
Login - refers to the item class ID or the associated CGI.
(1) - refers to the circled number on the screen.

Login Page Style Sheets

Figure 134: Customizing The Login Screen

```
/*              Style for the Login CGI */

 BODY.login {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
  background-image: url(/iems/module-pictures/fadingblue_left.gif);
 }

 TR.login { color: black }
 TD.login { color: black }
 H3.login { color: black; font-size: 16pt;}
 HR.login { color: yellow }
/*****************************************/
```

Item Name	Description
BodyLogin (1)	Configures the attributes of the “LOGIN” screen, such as the margin, font-family, line-height, background and background color.
TD.Login(2)	Configures the font color style of the username and password as presented in the TABLE.

Item Name	Description
H3.Login(3)	Configures the font color, font style and font size of the heading “Web Mail Login” of the “LOGIN” screen.
HR.Login(4)	Configures the color style of the horizontal line in the “LOGIN” screen.

Main Menu Page Style Sheets

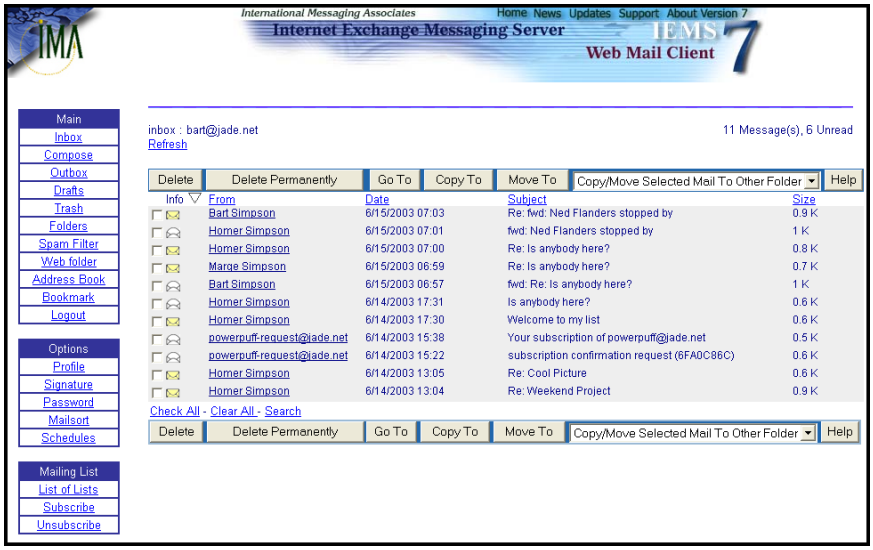

Figure 135: Customizing The Main Menu Screen

```
/*******************************************/
/* Style for MENU CGI */
  BODY.menu {
    margin: 1em;
    font-family: sans-serif;
    background: #FFFFFF;
    color: #000288;
    font-size: 10pt;
   }
A.menu {font-size: 10pt}
A.menu:link {color: blue}            /* unvisited link */
A.menu:visited { color: white}       /* visited links   */
A.menu:active { color: white}        /* active links   */
A.menu:hover {color: yellow}
/*******************************************/
```

Item Name	Description
Body.menu(2)	Configures the attributes of the “MENU” screen, such as the margin, font-family, background color and font size.
A.menu A.menu:link A.menu:visited A.menu:active A. menu:hover(1)	Configures the of the Inbox, Compose, Outbox, Folders and Login hyperlinks. You may change the color of the link when visited, active or hovered.

Folders Page Style Sheets

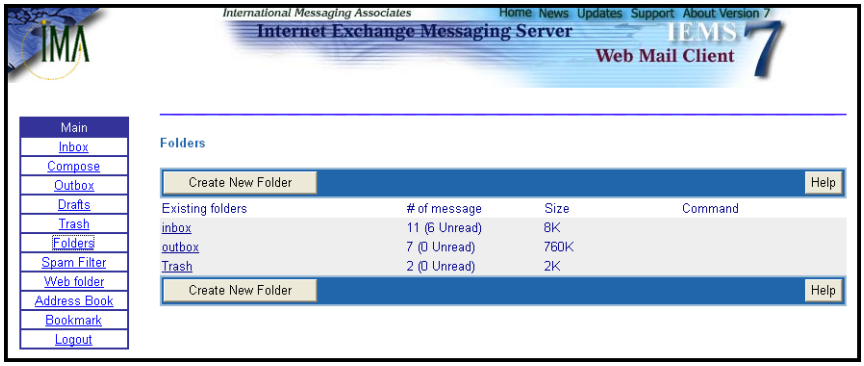

Figure 136: Customizing The Folders Screen

```
/*********************************************/
/* Style for VFOLDER CGI */
  BODY.vfolder {
    margin: 1em;
    font-family: Arial, Helvetica, sans-serif;
    line-height: 1;
 background-image: url(/iems/module-pictures/fadingblue_left.gif);
    font-size: 10pt;
  }
 H3.vfolder {font-family: sans-serif; display: block; font-size: 12pt; font-style:
normal;
color: #2166ab}
  A.vfolder:link { color: red}          /* unvisited link */
  A.vfolder:visited { color: #000288}       /* visited links */
  A.vfolder:active { color: red}        /* active links */
  A.vfolder:hover {color: #2166ab}
  TR.vfolderheader { color: white;
              background-color: #eeeeee;
              font-family: Arial, Helvetica, sans-serif;}
  TR.vfolder { color:#000288;
```

```
            background-color:#eeeeee;
            font-family: Arial, Helvetica, sans-serif; }
   TD.vfolderheader { color: white;
            background-color:#eeeeee;
            font-family: Arial, Helvetica, sans-serif; }
   TD.vfolder { color:#000288;
            background-color:#eeeeee;
            font-family: Arial, Helvetica, sans-serif; }
   TR.vfolderaction { color:#000288;
        background: white;
                font-family: sans-serif; }
   TD.vfolderaction { color:#000288;
  //            background: lightyellow;
                font-family: sans-serif; }
```

Item Name	Description
BODY.vfolder(8)	Configures the margin, font-family, line-height, background color and font size of the main “Folder” or “Inbox” screen.
H3.vfolder(1)	Configures the font family, font-display, font-size, font-style, and font-color of the “XXX for YYY” label (i.e. “Inbox for john@ima.com”).
H4.vfoldersummary (2)	Configures the font family, font display, font-size, font-style and font color of the “X Message(s), Y Unread” label (i.e., “3 Message(s), 1 Unread”).
A.vfolder:link A.vfolder:visited A.vfolder:active A.vfolder;hover (6)	Configures the font color of the visited, active and hover hyperlink under the From filed of each message.
TD.vfolderheader(3)	Configures the font color, background color, font family and font size of the header items (Info, Date, Subject and Size) of the message summary table.
TD.vfolder(4)	Configures the font color, background color, font family, font size of the message summary items.
TD.vfolderaction (5)	Configure the font color, background color, font-family and font-size of the table cells containing the ***Select All Messages***, ***Copy To, Move To***, ***Delete*** button and the folder selection box.

Message Content, Header and Source Page Style Sheets

Figure 137: Customizing The Message Content Screen

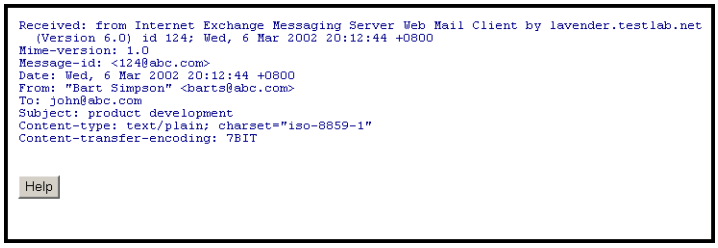

Figure 138: Customizing The Message Header Screen

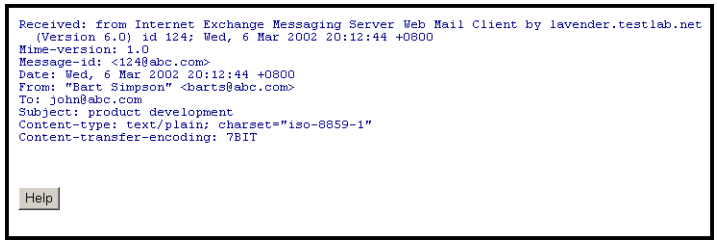

Figure 139: Customizing The Message Source Screen

```
/* Style for VIEWMSG CGI
*/
  BODY.viewmsg {
    margin: 1em;
    font-family: Arial, Helvetica, sans-serif;
    line-height: 1;
    background-color: #ffffff;
//    background-image: url(/iems/module-pictures/fadingblue_left.gif);
```

```
}
BODY.viewmsgheader {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
  background-image: url(/iems/module-pictures/fadingblue_left.gif);
  color: darkblue;
  font-size: 10pt;
}
BODY.viewmsgsource {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
 background-image: url(/iems/module-pictures/fadingblue_left.gif);
  color: darkblue;
}
TR.viewmsg {
  color: darkblue;
  background-color: #eeeeee;
  font-family: Arial, Helvetica, sans-serif;
}
TD.viewmsg {
  color: darkblue;
  background-color: #eeeeee;
  font-family: Arial, Helvetica, sans-serif;
}
A.viewmsgsource:link { color: #2166ab}          /* unvisited link */
A.viewmsgsource:visited { color: #2166ab}       /* visited links */
A.viewmsgsource:active { color: #2166ab}        /* active links */
A.viewmsgsource:hover {color: darkblue}
A.viewmsg:link { color: white}                  /* unvisited link */
A.viewmsg:visited { color: white}               /* visited links */
A.viewmsg:active { color: white}                /* active links */
A.viewmsg:hover {color: yellow}
TR.viewmsgheader {
  color: darkblue;
  background-color: #2166ab;
  font-family: Arial, Helvetica, sans-serif;
  font-size: 10pt;
}
TD.viewmsgheader {
  color: darkblue;
  background-color: #2166ab;
  font-family: Arial, Helvetica, sans-serif;
  font-size: 10pt;
}
TR.viewmsgtrailer {
  color: darkblue;
  background-color: #2166ab;
  font-family: Arial, Helvetica, sans-serif;
  font-size: 10pt;
}
TD.viewmsgtrailer {
  color: darkblue;
```

```
    background-color: #2166ab;
    font-family: Arial, Helvetica, sans-serif;
    font-size: 10pt;
  }
  TR.viewmsgtrailer {
    color: darkblue;
    background-color: #2166ab;
font-family: Arial, Helvetica, sans-serif;
   font-size: 10pt;
  }
  TR.viewmsgname {
    color: black;
      font-family: Arial, Helvetica, sans-serif;
    font-size: 10pt;
  }
  TD.viewmsgname {
    color: darkblue;
    background-color: #eeeeee;
    font-family: Arial, Helvetica, sans-serif;
    font-size: 10pt;
  }
  TR.viewmsgvalue {
     color: black;
     background-color: #eeeeee;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  TD.viewmsgvalue {
     color: darkblue;
     background-color: #eeeeee;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  H3.viewmsg {font-family: sans-serif; display: block; font-size: 10pt;
  font-style: normal; color: #2166ab}
  TD.viewmsgbody {
     color: black;
     background-color: white;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  TR.viewmsgbody {
     color: black;
     background-color: white;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  TD.viewmsg822 {
     color: darkblue;
     background-color: white;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  TR.viewmsg822 {
```

```
    color: darkblue;
    background-color: white;
    font-family: Arial, Helvetica, sans-serif;
    font-size: 10pt;
  }
  TD.viewmsg822name {
    color: darkblue;
    background-color: #eeeeee;
    font-family: Arial, Helvetica, sans-serif;
    font-size: 10pt;
 TR.viewmsg822name {
    color: darkblue;
    background-color: #eeeeee;
    font-family: Arial, Helvetica, sans-serif;
    font-size: 10pt;
  }
  TD.viewmsg822value {
     color: darkblue;
     background-color: #eeeeee;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  TR.viewmsg822value {
     color: darkblue;
     background-color: white;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  TD.viewmsgattach {
     color: darkblue;
     background-color: white;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  TR.viewmsgattach {
     color: darkblue;
     background-color: #eeeeee;
     font-family: Arial, Helvetica, sans-serif;
     font-size: 10pt;
  }
  A.viewmsgattach:link { color: red}          /* unvisited link */
  A.viewmsgattach:visited { color: red}       /* visited links */
  A.viewmsgattach:active { color: red}        /* active links */
  A.viewmsgattach:hover {color: #2166ab}
```

Item Name	Description
BODY.viewmsg(1)	Configures the margin, font family, line-height, background color and font-size of the “Message Content” screen.

BODY.viewmsgheader (1A)	Configures the margin, font-family, line height, background color, font color and font size of the “Message Headers” screen.
BODY.viewmsg-source(1B)	Configures the margin, font family, line-height, background color and font-size of the “Message Source” screen.
TD.viewmsgheader(2)	Configures the font color, background color, font family and font-size of the table cell containing the ***Reply***, ***Reply All***, ***Forward***, ***Delete***, ***Previous*** and ***Next*** hyperlink at the top of the “Message Contents” screen.
TD.viewmsgtrailer(3)	Configures the font color, background color, font family and font-size of the table cell containing the ***Reply***, ***Reply All***, ***Forward***, ***Delete***, ***Previous*** and ***Next*** hyperlink at the bottom of the “Message Contents” screen.
TD.viewmsgname(4)	Configures the font color, background color, font-family and font-size of the table cell containing the ***From***, ***To***, ***Cc***, ***Date*** and ***Subject*** message header fields.
TD.viewmsgvalue(5)	Configures the font color, background color, font-family and font-size of the table cell containing the ***From***, ***To***, ***Cc***, ***Date*** and ***Subject*** value header fields.
TD.viewmsgbody(6)	Configures the font color, background color, font family, and font-size of the table cell containing the message contents.
TD.viewmsg822(7)	Configures the font color, background color, font family and font size of the table cell containing the embedded RFC-822 message contents.
TD.viewmsg822name(8)	Configures the font color, background color, font- family and font-size of the table cell containing the From, To, Cc, Date and Subject message header fields label of the embedded RFC-822 message.
TD.viewmsg822value(9)	Configures the font color, background color, font family and font-size of the table cell containing the ***From***, ***To***, ***Cc***, ***Date*** and ***Subject*** message header fields of the embedded RFC-822 message.

TD.viewmsgattach(10)	Configures the font color, background color, font family and font-size of the table cell containing a hyperlink for downloading attachments.

Item Name	Description
A.viewmsgattach:link A.viewmsgattach:visited A.viewmsgattach:active A.viewmsgattach:hover(11)	Configures the font color of the visited, active and hover hyperlinks for downloading attachments.
A.viewmsgsuorce:link A.viewmsgsource:visited A.viewmsgsource:active A.viewmsg-source:hover(12)	Configures the font color of the ***View Message Headers*** and ***View Message Source*** hyperlinks.
A.viewmsg:link A.viewmsg:visited A.viewmsg:active A.viewmsg:hover(13)	Configures the font color of the ***Reply***, ***Reply To All***, ***Forward, Delete***, ***Previous***, ***Next*** and ***Go Back*** hyperlinks.
H3.viewmsg (14)	Configures the font-family, display, font-size, font-style, and font-color of the “Folder XXXX” label (i.e., Folder:Inbox).

New Message, Reply, Forward, Attach File and Confirmation Page Style Sheets

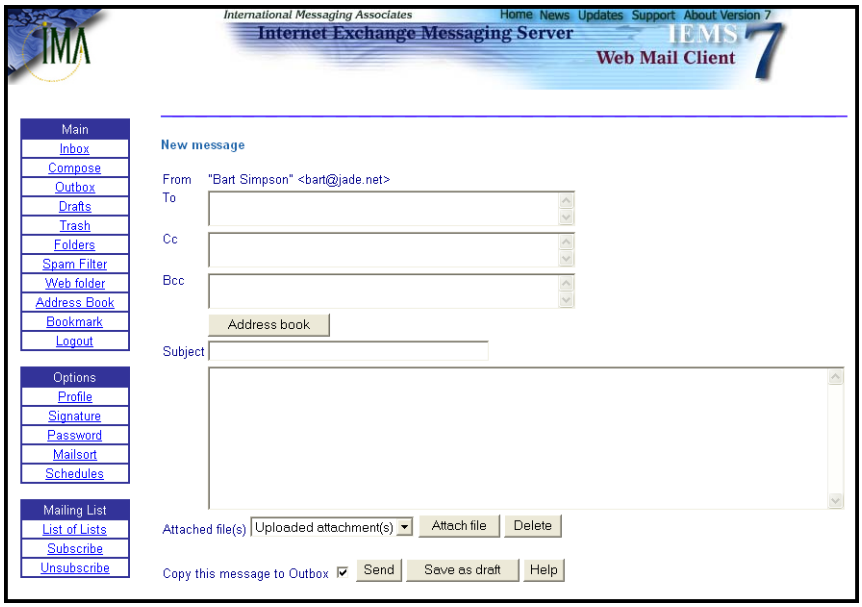

Figure 140: Customizing The New Message Screen

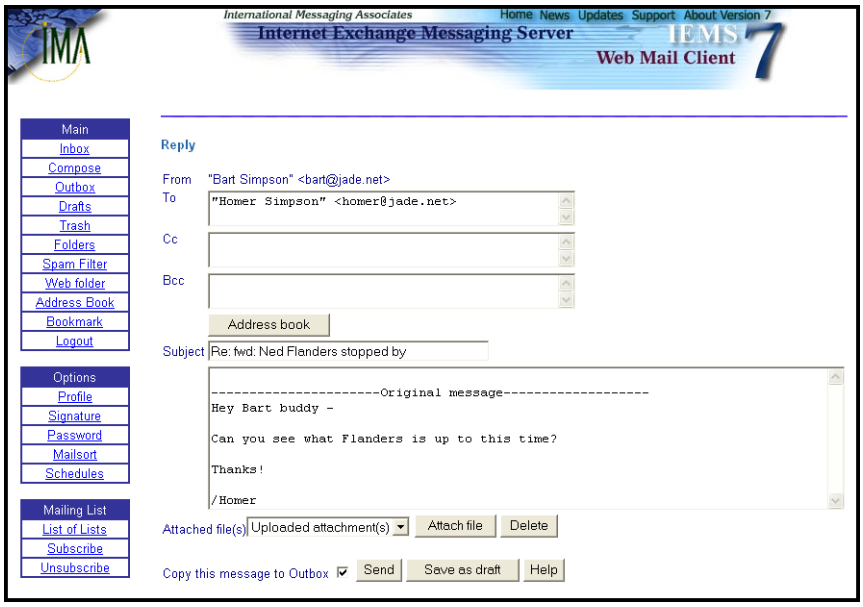

Figure 141: Customizing The Reply Message Page

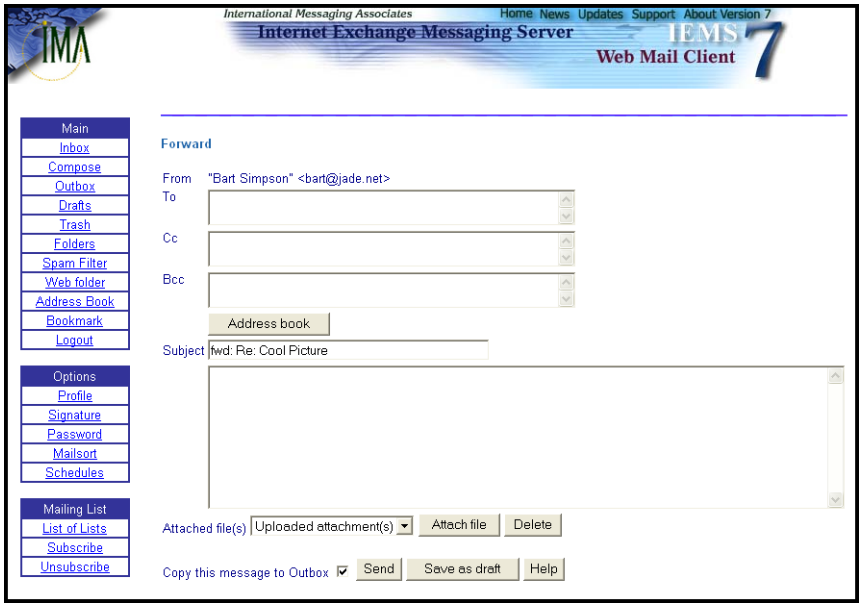

Figure 142: Customizing The Forward Message Page

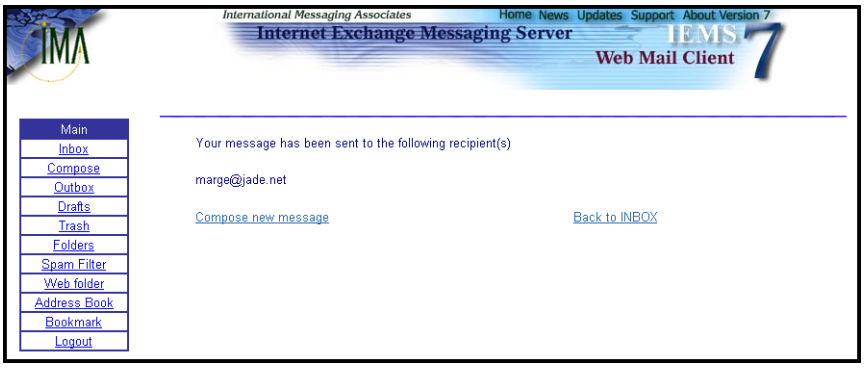

Figure 143: Customizing The Confirmation Page

```
/* Style for NEWMAIL CGI */

BODY.newmail {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
  background-image: url(/iems/module-pictures/fadingblue_left.gif);
  font-size: 10pt;
}

TR.newmail {
        color: black;
        font-family: sans-serif;
        font-size: 10pt
}
```

```
TD.newmail {
        color: darkblue;
        font-family: sans-serif;
        font-size: 10pt
}

TR.newmailtag {
        color: black;
        font-family: sans-serif;
        font-size: 10pt
}

TD.newmailtag {
        color: darkblue;
        font-family: sans-serif;
        font-size: 10pt
}

TR.newmailvalue {
        color: black;
        font-family: sans-serif;
        font-size: 10pt
}

TD.newmailvalue {
        color: darkblue;
        font-family: sans-serif;
        font-size: 10pt
}

H2.newmail {font-family: Arial, Helvetica, sans-serif; display: block;
 font-size: 12pt; font-style: normal; color: #2166ab}
BODY.replymail {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
  background-image: url(/iems/module-pictures/fadingblue_left.gif);
  font-size: 10pt;
}

TR.replymail {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

TD.replymail {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}
TR.replymailtag {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
```

```
        font-size: 10pt
}

TD.replymailtag {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

TR.replymailvalue {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

TD.replymailvalue {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

H2.replymail {font-family: Arial, Helvetica, sans-serif; display: block;
 font-size: 12pt; font-style: normal; color: #2166ab}
BODY.forwardmail {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
  background-image: url(/iems/module-pictures/fadingblue_left.gif);
  font-size: 10pt;
}

TR.forwardmail {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

TD.forwardmail {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

TR.forwardmailtag {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}
TD.forwardmailtag {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
 }
```

```
TR.forwardmailvalue {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}
TD.forwardmailvalue {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

H2.forwardmail {font-family: Arial, Helvetica, sans-serif; display: block; font-size: 10pt; font-style: normal; color: #2166ab}

BODY.newmailattach {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
  background-image: url(/iems/module-pictures/fadingblue_left.gif);
  font-size: 10pt;
}

H3.newmailattach {font-family: Arial, Helvetica, sans-serif; display: block; font-size: 10pt; font-style: normal; color: #2166ab}

BODY.sendmail {
  margin: 1em;
  font-family: Arial, Helvetica, sans-serif;
  line-height: 1;
  background-image: url(/iems/module-pictures/fadingblue_left.gif);
  font-size: 10pt;
}

TR.sendmail {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}

TD.sendmail {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}
TR.sendmailrecip {
        color: black;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}
TD.sendmailrecip {
        color: darkblue;
        font-family: Arial, Helvetica, sans-serif;
        font-size: 10pt
}
```

```
A.sendmail:link { color: #2166ab}          /* unvisited link */
A.sendmail:visited { color: #2166ab}       /* visited links */
A.sendmail:active { color: #2166ab}        /* active links */
A.sendmail:hover {color: darkblue}
```

Table 5 explains the “New Message”, “Reply”, “Forward”, “Attach file” and Confirmation page style sheets.

Item Name	Description
BODY.newmail(A1)	Configures the style of the New Mail screen such as the margin, font family, line-height, background color and font size when composing new messages.
TD.newmail(2)	Configures the font color, background color, font family and font-size when composing new messages.
TD.newmailtag(A3)	Configures the font color, background color, font family and font-size of the page containing the ***From***, ***To***, ***Cc***, ***Bcc*** and ***Subject*** fields boxes when composing a new messages.
TD.newmailvalue(A4)	Configures the font color, background color, font family and font-size of the page containing the ***From***, ***To***, ***Cc***, ***Bcc*** and ***Subject*** fields boxes when composing a new messages.
H2.newmail (A5)	Configures the font family, display, font-size, font style, and font color of the ***New Message*** and ***Attach file(s)*** label.
BODY.replymail(B1)	Configures the margin, font-family, line-height, background color and font-size of the Reply Mail Message page
TD.replymail(B2)	Configures the font-color, background color, font family and font-size of the “Reply Mail” screen.
TD.replymailtag(B3)	Configures the font color, background color, font-family and font-size of the ***From***, ***To***, ***Cc***, ***Bcc*** and ***Subject*** field labels on the “Reply Mail” screen.
TD.replymailvalue (B4)	Configures the font color, background color, font-family and font-size of the ***From***, ***To***, ***Cc***, ***Bcc*** and ***Subject*** text boxes on the “Reply Mail” screen.

Item Name	Description
H2.replymail(B5)	Configures the font-family, display, font-size, font-style, and font color of the ***Reply*** and ***Attached File(s)*** label.
BODY.forwardmail(C1)	Configures the font color, background color, font family and font-size of the “Forward Mail” screen.
TD.forwardmail(C2)	Configures the font color, background color, font family and font size of the message screen in the “Forward Mail” screen.
TD. forwardmailtag(C3)	Configures the font color, background color, font-family and font-size of the ***From***, ***To***, ***Cc***, ***Bcc*** and ***Subject*** field labels on the “Forward Mail” screen.
TD.forwardmail-value(C4)	Configures the font color, background color, font-family and font-size of the ***From***, ***To***, ***Cc***, ***Bcc*** and ***Subject*** text boxes on the “Forward Mail” screen.
H2.forwardmail(C5)	Configures the font-family, display, font-size, font style and font color of the “Forward” and “Attached file(s)” label.
H3.newmailattach(6)	Configures the font-family, display, font-size, font style and font color of the “Attach file” and “File Upload” screens.
BODY.newmail-attach(7)	Configures the margin, font family, line-height background color and font-size of the “ File Upload” screen.
BODY.sendmail(8)	Configures the margin, font family, line-height background color and font-size of the “ Sent Mail Summary” screen.
TD.sendmail(9)	Configures the margin, font family, line-height background color and font-size of the screen on the “ Sent Mail Summary” screen.
TD.sendmailrecip(10)	Configures the font color, background color, font family and font size of the screen containing the recipient’s addresses on the “Sent Mail Summary” screen.
A.sendmail:link A.sendmail:visited A.sendmail:active A.sendmail:hover(11)	Configure the font color of the visited, active and hover hyperlinks for the Compose New Message and Back to Inbox links on the “Sent Mail Summary” screen.

Customizing the Domain-Based Headers and Footers

The headers and footers of the “Web Mail Client” screens can be customized to display the company logo or banner using static HTML, plain text files or by running an executable files (i.e., CGI scripts or animated banners). The headers and footers can also be further defined to handle multiple domains. This means that the headers and footers will appear on the “Web Mail Client” screens even if you are using multiple domains (e.g. ima.com, jade.net). These headers and footers are applicable to both the menu and body frames of the “Web Mail Client” interface. To modify the header or footer, the system administrator must edit the settings in the **IEMTA.INI** (Windows) or **IEMS.CONF** (Linux) file under the [WebClient] section.

```
[WebClient]
HeaderHTML=#C:\Program Files\IMA\IEMS 7\Apache\HTDocs\iems\module-
pictures\banner1.html
```

To define the headers and footers, open the **IEMTA.INI** (Windows) or **IEMS.CONF2** (Linux) file in the *C:\WINDOWS* (Windows) or /etc (Linux) directory. In the [WebClient] setting, type the following entries below:

```
[WebClient]
HeaderHTML=
FooterHTML=
HeaderEXE=
FooterEXE=
```

Body Headers and Footers

Type the correct directory path of the HTML or executable file after the parameter setting. Use HTML or plain text files for the **HeaderHTML=** and **FooterHTML=**parameters. Use executable files (i.e., CGI scripts or animated banners) for the **HeaderEXE=** and **FooterEXE=** parameters. This allows ISPs (Internet Service Providers) to display their banners on the “Web Mail Client” interface.

Note: *These headers and footers are only applicable for the body part of the Web Mail Client interface in a single domain environment.*

For example:

(Windows)

```
[WebClient]
HeaderHTML=C:Program Files\IMA\IEMS 7\banner.htm
FooterHTML=C:Program Files\IMA\IEMS 7\footer.htm
HeaderEXE=C:Program Files\IMA\IEMS 7\banner.exe
FooterEXE=C:Program Files\IMA\IEMS 7\footer.exe
```

(Linux)

[WebClient]

HeaderHTML=/opt/iems/bin/banner.htm
FooterHTML=/opt/iems/bin/footer.htm
HeaderEXE=/opt/iems/bin/banner.cgi
FooterEXE=/opt/iems/bin/footer.cgi

If an executable file was used, the Web Mail Client will pass the currently logged in user name, which refers to the users e-mail address, as the "command line" argument to that executable file. For example:

HeaderEXE=c:\wmc\banner.exe (Windows)

or

HeaderEXE=/opt/iems/bin/banner.cgi (Linux)

The Web Mail Client will launch the executable file via:

system ("c:\wmc\banner.exe user@domain.com") (Windows)

or

system ("/opt/iems/bin/banner.cgi user@domain.com") (Linux)

Using this example, the currently logged in user is "user@ima.com". It should be noted that only this one parameter is passed to the external executable file.

After defining the headers and footers, save the new settings of the **IEMTA.INI** (Windows) or **IEMS.CONF** (Linux) file. Go back to the "Web Mail Client" interface. And click the ***Refresh*** or ***Reload*** button. This updates the web interface.

Menu Headers and Footers

To define headers and footers for the menu side of the Web Mail Client in a single domain configuration, the following entries need to be defined in the IEMTA.INI (Windows) or IEMS.CONF (Linux) file:

[WebClient] MenuHeaderHTML=
MenuFooterHTML=
MenuHeaderEXE=
MenuFooterEXE=

You may also insert HTML or executable files on the menu page by defining your preferred links for the following entries:

```
[WebClient]
MenuHeaderHTML-domainname=
MenuFooterHTML-domainname=
MenuHeaderEXE-domainname=
MenuFooterEXE-domainname=
```

Similarly, to define headers and footers for the body side of the Web Mail Client in a multiple domain configuration, the following entries are to be defined in the **IEMTA.INI** (Windows) or **IEMS.CONF** (Linux) file:

```
[WebClient]
HeaderHTML-domain.com=
FooterHTML-domain.com=
HeaderEXEdomain.com=
FooterEXE-domain.com=
```

Note: *In the above example, "domain.com" is the domain name used. In case you failed to define the domain in the header and the footer settings and you are using multiple domains, the default settings are to be used.*

To specify the headers and footers for the menu side of the "Web Mail Client" interface in a multiple domain environment, the following entries are to be defined in the **IEMTA.INI** (Windows) or **IEMS.CONF** (Linux) file:

```
[WebClient]
MenuHeaderHTML-domain.com=
MenuFooterHTML-domain.com=
MenuHeaderEXE-domain.com=
MenuFooterEXE-domain.com=
```

In the above settings, you can use HTML or plain text files for the **MenuHeaderHTML-domain.com=** and **MenuFooterHTML-domain.com=** parameters. You may use executable files for the **MenuHeaderEXEdomain.com=** and **MenuFooterEXE-domain.com=** parameters.

User Style Sheet Configuration

User selectable styles accessable from the Web Mail Client can also be configured by the IEMS administrator. IEMS ships with 12 standard styles, including the system default configuration. The styles are configured in the IEMS configuration file in the following section:

```
[WebClient]
NumberOfStylesheets=<N>
Style-1=<stylesheetname>,en-us=<display-name>,img=<file1>,
    bigimg=<file2>
:
:
Style-N=<stylesheetname>,en-us=<display-name>,img=<file1>,
   bigimg=<file2>
```

The files specified in <stylesheetname>, <img>, and <bigimg> should be put under the directory */opt/iems/htdocs/iems/style/wmc/en-us* for Linux, and *<InstallDirectory>\apache\htdocs\iems\style\wmc\en-us* for Windows.

Example:

[WebClient}
NumberOfStylesheets=2
Style-1=style-1.css,en-us=Party Time,img=style1-small.jpg,bigimg=style1-big.jpg
Style-2=style-2.css,en-us=At Work,img=style2-small.jpg,bigimg=style2-big.jpg

The names *Party Time* and *At Work* above will appear next to the images of the style in the Web Mail Client. By default these are not set, however can be set to any values the administrator wishes.

The file referenced by <img> is the small JPG image displayed in the Web Mail Client style selection page. If set, the <bigimg> points to a larger version of this screen shot which is displayed if the user clicks on the smaller version on the selection page. While these images can be created with any dimensions, it is recommended to stay with the IMA standard of 852x721 and 213x180 for the large and small images respectively for best rendering.

CHAPTER 10

Troubleshooting and Error Handling

This chapter guides the system administrator on how to troubleshoot some of the common problems that may arise while running, configuring and administering Internet Exchange Messaging Server (IEMS) 7 for Linux and Windows. An error handling section is also included.

Most problems can be identified by checking the log files. To understand the log files, the first section of this chapter describes the types and structures of the log files created by IEMS; and how to analyze the different log files.

Understanding Log Files

Log files record events related to the transmission of messages and to other processes employed by the server. By examining the log files, you can monitor many aspects of the server's operation and identify the sequence of events that brought the problem.

IEMS logs the most recent transactions in the log file called **iemta.log** located in the log file directory *(C:\Program Files\IMA\IEMS 7\Log* for Windows or */var/log/iems* for Linux).

Levels of Logging

The level or priority of logging defines how detailed the logging activity is. A higher priority level means less detail; it means that only events of high priority are logged. A lower level means greater detail; it means that more kinds of events are recorded in the log file (see Figure 144 on page 228).

Logging Level	Description
Errors Only	The minimum logging detail. An event is written to the log whenever an error condition occurs. An instance is when a connection attempt to a client or another server fails.
Warning	An event is written to the log whenever a warning condition occurs. An instance is when the server cannot understand a communication sent to it by a client.
Messsage Logging	Logs the information about the delivery of all messages.
SMTP session	All SMTP conversations are logged in this level. SMTP session logging is responsible for recording each incoming and outgoing SMTP command.
Informational	An event is written to the log with every significant action that takes place. An instance is when a user successfully logs on or off or creates or renames a mailbox.
Diagnostic	The most verbose logging. Useful only for debugging purposes. Events are written to the log at individual steps within each process or task to pinpoint problems. It logs additional diagnostic data including information concerning core operations.

Figure 144: IEMS Logging Levels

Note: *The more detailed the logging you specify, the more disk space your log files will occupy; and the slower the system will run. When you select a particular logging level, events corresponding to that level and to all higher (less detailed) levels are logged. The default level of logging is "Message Logging".*

Filename Conventions

All log files use identical naming conventions. Each log file has a filename of the form:

Date Sequence Number ------ log file size

where:

Date - A large integer that specifies the date that the file was created (e.g. *27nov*).

Sequence Number - An integer that specifies the order of creation of this log file compared to others in the log file directory. Log files with higher sequence numbers are more recent than those with lower numbers. Sequence numbers do not roll over; they increase monotonically for the life of the server (beginning at server installation) (e.g. 003).

Log file size - This corresponds to the largest log file size permitted before it is saved to another name and a new log is started. The default limit is 50,000 bytes, allowing the Windows Notepad application to read the file. The acceptable values range between 10,240 bytes (10KB) and 2,000,000,000 (about 2GB). The default value of zero indicates no limit.

For example, a log file named 13dec123----50109 would be the 23rd log file created in the directory of log files, created on December 13 of the current year with a file size of 50,109 bytes.

Content Format

All log files have identical content formats. Log files are multi-line text files; each line describes one logged event. All event descriptions, for each of the supported services, have the general format:

date time component [logging level]: transaction message

where:

date time - The date and time the event was logged; expressed in Day month hh:mm:ss format (e.g. Mon Dec13 13:16:32).

component - The name of the IEMS component performing the transaction or operation. IEMS is composed of the following components: SMTPC, SMTPD, Directory Services, BSMTP, Message Store, Preprocessor, DL Manager, Mailsort, LMDA, Quota Agent, Web Mail Client, MQ Router.

logging level -The level of logging that the event represents (e.g.diagnostic).

transaction message - An event-specific explanatory message that may be of any length (e.g. old logfile renamed to 27Dec002.log).

Below are three examples of logged events:

a. Wed Dec 27 13:51:47 PreProcessor: [Informational] Application "QUOTA" installed

b. Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Try loading all list members for mailing list writers@music.com
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Archive mode is on
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Mail posting is allowed to new mailing member by default.
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Auto subscription is enabled for closed list
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Invalid posting will be bounced to the sender.
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Message digest will be sent in multipart/digest format
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] This is an open list
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Message digest will be sent at 0:0
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Message digest will be sent every day
Wed Dec 27 11:42:17 DL Manager: [Diagnosis] Return-receipt-to header will be removed

c. Mon Dec 11 16:15:35 Local Mail Delivery Agent: [Error] Could not initialize message queue

Debugging Under Linux

Unable to Apply Certificate Files

When installing licenses, the License Manager needs to have the appropriate access rights to the certificate file. By default, the certificate file (IMACert.imc) must be owned by user "iems" to be able to update the license. See log file below.

```
Tue Dec 26 20:31:02 LDAP Server: [Informational] conn=60 fd=4 connection from
    unknown (192.168.1.1)
Tue Dec 26 20:31:02 LDAP Server: [Informational] conn=60 op=0 BIND dn="root"
    method=128
Tue Dec 26 20:31:03 LDAP Server: [Informational] conn=60 op=-1 fd=20 closed
    errno=Success
Tue Dec 26 20:31:07 Lupdate: [Error] Error creating temporary files.
Tue Dec 26 20:31:08 LDAP Server: [Informational] conn=61 fd=4 connection from
    unknown (192.168.1.1)
Tue Dec 26 20:31:08 LDAP Server: [Informational] conn=61 op=0 BIND dn="root"
    method=128
Tue Dec 26 20:31:08 LDAP Server: [Informational] conn=61 op=-1 fd=20 closed
    errno=Success
```

The system administrator must apply the necessary rights for the directory where the certificate file (**IMACert.imc**) is located. For example, if the IMACert.imc file is located under /CERT. Use the following command directory:

```
chown -R iems:iems /CERT
```

Debugging Under Windows

The VIM32.DLL in Your System Path is Not Usable by The Notes PAB Converter

The Notes migration utility makes use of the VIM32.dll file located in the Notes installation directory (C:\Lotus\Notes). Without this file, migration will not continue. During the migration, the Notes migration tool locates the VIM32.dll file included with the Lotus VIM 6.30 files installed in the C:\Winnt\System32 instead of the **VIM32.dll** file in the Notes installation directory. The located file is incompatible with the Notes migration tool that is why an error message was generated.

You may notice the cc:Mail **VIM32** file under C:\Winnt\ directory is **VIM32.dll** with a size of 181KB. The Lotus Notes' VIM file, **VIM32.dll**, is under the C:\Lotus\Notes\ with a size of 92KB.

To solve this problem, perform these steps:

1. Shut down IEMS.
2. Rename the **VIM32** file located at C:\Winnt\ (e.g. VIM32.dll to VIM32CCMAIL.dll).
3. Copy the **VIM32.dll** from C:\Lotus\Notes\ directory to C:\Winnt.
4. Restart IEMS.
5. Proceed with the migration.

6. After migration, be sure to delete the Lotus Notes' **VIM32** file under C:\Winnt.

7. Rename the VIM32CCMAIL.dll back to **VIM32.dll**.

Note: *Both Notes mailbox migration and cc:Mail user migration make use of the VIM32 file.*

NOTES Server is Down or Inaccessible

In the Notes Connector control menu, clicking the SMTP.BOX monitor will give you an error message that says "Unable to open SMTP.BOX". Even if you try to start or stop the responder or shut down IEMS, the problem will still exist. To solve the problem, perform the following:

1. Make sure your Lotus Notes Server is online.

2. If the problem is persistent, there may be something wrong with the installation of IEMS. Try to reinstall IEMS with the Lotus Notes Server (online) to validate the Notes user.

NOTESOUT Terminates When Processing Outgoing Messages Coming From Notes Users

The NotesOut module is responsible for exporting messages from the Notes server's "SMTP.BOX". To be able to process outgoing messages, NotesOut needs to have a "manager level" access and permission to delete documents. Otherwise, NotesOut will terminate. See log file below.

```
Wed Dec 27 11:26:02 NotesOut: [Diagnosis] Will connect to hostname/lapis!!smtp.box
for mail export
Wed Dec 27 11:26:02 NotesOut: [Diagnosis] Notes build version 4.X
Wed Dec 27 11:26:02 NotesOut: [Error] Current UserKey doesn't have Manager level
access or cannot delete notes from the database: hostname/lapis!!smtp.box
Wed Dec 27 11:26:02 NotesOut: [Diagnosis] terminating...
Wed Dec 27 11:26:02 NotesOut: [Diagnosis] Btrieve database engine is terminated
successfully.
Wed Dec 27 11:26:02 NotesOut: [Diagnosis] Terminating
Wed Dec 27 11:26:02 PreProcessor: [Informational] MQResponder; Closed connection
from "lapis"/"NotesOut", served 0 requests
```

The system administrator must configure IEMS to run with Lotus Domino version 5 to solve this problem. See *http://www.ima.com/pdf/notes5config.pdf* for configuration procedures.

NOTESIN Terminates When Processing Incoming Messages Destined for Notes Users

The NotesIn module is responsible for importing messages from the IEMS Message Queue to the Notes server. To process incoming messages, NotesIn needs to have a "manager level" access and permission to delete documents. Otherwise, NotesIn will terminate. See the following log file.

```
Wed Dec 27 11:28:58 NotesIn: [Diagnosis] Connecting to hostname/lapis!!mail.box for
mail delivery
Wed Dec 27 11:28:58 NotesIn: [Diagnosis] Notes build version 4.X
Wed Dec 27 11:28:58 NotesIn: [Error] Current UserKey doesn't have Manager level
access or cannot delete notes from the database: hostname/lapis!!mail.box
Wed Dec 27 11:28:58 NotesIn: [Diagnosis] terminating...
Wed Dec 27 11:28:58 NotesIn: [Diagnosis] Btrieve database engine is terminated
successfully.
Wed Dec 27 11:28:58 NotesIn: [Diagnosis] Terminating
Wed Dec 27 11:28:59 PreProcessor: [Informational] MQResponder; Closed connection
from "hostname"/"NotesIn", served 0 requests
```

The system administrator must configure IEMS to run with Lotus Domino Server to solve this problem. See http://www.ima.com/pdf/notes5config.pdf for configuration procedures.

NOTESOUT Unable to Bounce Messages to Notes Users

If the Notes connector is running on a Notes workstation, the MAIL.BOX database must be created in the Notes workstation to process bounced messages for Notes users. See log file below.

```
Wed Dec 13 10:06:05 NotesOut: Rejected 15206 size: 2248 bytes: unauthorized local
sender: <CN=John Doe Jade/OU=IMA/O=IMA@UST>
Wed Dec 13 10:06:05 NotesOut: [Error] BounceNotesMail: NSFDbOpen failed (local
MAIL.BOX).
Wed Dec 13 10:06:05 NotesOut: [Error] [Reason]: File does not exist
```

The system administrator must configure IEMS to run with Lotus Domino Server to solve this problem. See *http://www.ima.com/pdf/notes5config.pdf* for configuration procedures.

CCOUT Terminates When Processing Outgoing Messages From the cc:Mail PO

The CCOUT module is responsible for exporting messages from the cc:Mail Post Office. The following log file shows the CCOUT module terminating when it processes outgoing messages.

```
Wed Dec 27 14:25:06 ccOut: [Error] VIMOpenSession failed: 5/0
Wed Dec 27 14:25:06 ccOut: [Error] VIM error message: An invalid parameter was
specified.
Wed Dec 27 14:25:06 ccOut: [Error] VIM extended message: No error
Wed Dec 27 14:25:06 PreProcessor: [Informational] MQResponder; Connection from
192.168.100.14 is "lapis", Application is "ccout"
Wed Dec 27 14:25:06 ccout: [Informational] The current License Key type is Permanent.
Wed Dec 27 14:25:06 ccout: [Informational] The current Serial Number is 88888.
Wed Dec 27 14:25:06 ccout: [Informational] The user limit for the current software is
unlimited.
Wed Dec 27 14:25:06 ccout: [Informational] License settings checked on : Wed Dec 27
14:25:06 2000
Wed Dec 27 14:25:06 ccout: [Informational] The current License Key type is Permanent.
Wed Dec 27 14:25:06 ccout: [Informational] The current Serial Number is 88888.
Wed Dec 27 14:25:06 ccout: [Informational] The user limit for the current software is
unlimited.
Wed Dec 27 14:25:06 ccout: [Informational] License settings checked on : Wed Dec 27
14:25:06 2000
Wed Dec 27 14:25:06 ccOut: [Error] startVim failed
```

To solve the problem, make sure that the cc:Mail VIM files are properly installed and included in the search path.

CCIN Terminates When Processing Messages Destined to cc:Mail Users

The CCIN module is responsible for importing messages from IEMS to the cc:Mail Post Office. The following log file shows the CCIN module terminating when it processes incoming messages.

```
Wed Dec 27 14:23:11 ccIn: [Error] VIMOpenSession failed: 5/0
Wed Dec 27 14:23:11 ccIn: [Error] VIM error message: An invalid parameter was specified.
Wed Dec 27 14:23:11 ccIn: [Error] VIM extended message: No error
Wed Dec 27 14:23:11 ccIn: [Diagnosis] Btrieve engine is terminated
Wed Dec 27 14:23:11 ccIn: [Diagnosis] Terminating
```

To solve the problem, make sure that the cc:Mail VIM files are properly installed and included in the search path.

Corrupted cc:Mail Internet PO Queue Monitor Counter Displays Invalid Number of Outgoing Messages

When the cc:Mail Internet Post Office Queue monitor displays a value in the **Number of unread message(s)** found field, but there are no messages listed in the screen, it is possible that the cc:Mail Post Office is corrupted. To solve the problem, perform the following steps:

1. Open the MS-DOS command prompt.
2. Go the ccadmin directory (e.g. c:\ccmail\ccadmin).
3. Run the cc:Mail Post Office maintenance utilities (i.e., reclaim and chkstat) by typing:

   reclaim.exe/NPO_name/Ppassword/Dccmail_data_directory

4. Press the ENTER key.

If the problem still persists, do the following:

1. Go the cc:Mail main web administration interface by clicking the cc:Mail link from the top menu.
2. Click the cc:Mail Post Office button from the left menu frame.
3. Recreate a new Internet Post Office by removing the corrupted Internet Post Office and creating a new Internet Post Office.

Unable to Apply The License

IEMS cannot validate the license if you do not have the appropriate license keys. An error message "`Generated license key could not be validated`" will appear on the screen. The system administrator must check if the license is valid from the “License Manager” screen, if not, perform the steps in “Unable to Update License” on page 234.

1. Check the FQDN (Fully Qualified Domain Name), (e.g. hostname.domainname) of your machine under the TCP/IP Network properties of Windows. Make sure the FQDN specified on the DNS Configuration matches with the FQDN registered in the certificate file.

2. To apply the license, run the certificate installer in C:\Program Files\IMA\IEMS 7\certinst.exe.

3. Select the modules you wish to updated and INSTALL licenses.

Debugging Under Linux and Windows

Unable to Update License

When doing a license update (i.e., Evaluation to Interim license, Interim to Permanent license or from 100 user license to 250, 400 or 1000 user license), make sure that the license key is using the filename **IMACert.imc**.

1. Start the Apache web server.

2. Open a web browser (e.g. Internet Explorer, Netscape) and type the URL that points to the “License Update” web page (e.g. hostname.domainname/ iems/sysad/lupdate/index.htm).

3. Click the ***License Manager*** button on the left side of the screen. A new screen for installing/updating the license of the IEMS software components you installed on your machine will appear.

4. Check if the Certificate path is pointing to the directory where the certificate file you received from IMA is located.

Note: *For IEMS for Linux, make sure the certificate file is owned by the user “iems”.*

5. Tick the check boxes of the components you wish to license.

6. Click the ***Update*** button to apply the new license. For the license to take effect immediately, you need to shut down IEMS and then restart all the components.

Note: *If other components (i.e., Message Store) terminate after updating the new license, check if the number of users coincide with the new license key's number of users. You may also delete some of the users that you have in the local Message Store to meet the required maximum number of licensed users.*

SMTPD Unable to Process Incoming Mail

The log file below shows that the SMTPD module cannot process incoming mail from the Internet.

```
Thu Dec 7 08:23:33 smtpd: [Diagnosis] SMTPD 1 connection
Thu Dec 7 08:23:33 smtpd: [SMTP] 14< MAIL From:<john@domain.com >
SIZE=2191
Thu Dec 7 08:23:33 smtpd: [SMTP] 14> 250 OK - john@domain.com
Thu Dec 7 08:23:33 smtpd: [SMTP] 14< RCPT To:<doe@domain.com>
Thu Dec 7 08:23:33 smtpd: [Diagnosis] hostname/domain matches - domain is
 local: domain.com
Thu Dec 7 08:23:33 smtpd: [SMTP] 14> 250 OK - doe@domain.com
Thu Dec 7 08:23:33 smtpd: [SMTP] 14< DATA
Thu Dec 7 08:23:33 host.domain.com-smtpd-MQAPI: [Error] CreateMQEntry; Could
 not get a unique QID, Range Error.
Thu Dec 7 08:23:33 smtpd: [Error] CreateMQEntry failed.
Thu Dec 7 08:23:33 smtpd: [Error] 14: GetNewQueueId failed
Thu Dec 7 08:23:33 smtpd: [SMTP] 14> 421 Error - internal error
Thu Dec 7 08:23:33 smtpd: [SMTP] 14< QUIT
 Thu Dec 7 08:23:33 smtpd: [SMTP] 14> 221 Goodbye - have a wonderful day!
```

By default, if the Preprocessor detects that the */var/spool/iems/mqueue* (Linux) or *C:\Program Files\IMA\IEMS 7\MsgQueue* (Windows) directory's free space is less than 50MB, the Preprocessor will refuse to assign a new queue ID to the input processor like SMTPD. This is why the SMTPD module cannot receive incoming mail from the Internet.

The solution is to increase the hard disk's free space or change the default-value, 50MB, to a lower value (e.g. 10MB). To change the default value of 50MB to 10MB, add the value below in the **iems.conf** (Linux) or **iemta.ini** (Windows) file:

```
[PreProcessor]
DriveMin=10
```

DL Manager Unable to Insert Disclaimer Messages

The log file below shows that the DL Manager cannot insert disclaimer messages to the message contents

```
Tue Dec 26 17:56:48 DL Manager: [Diagnosis] Processing message (160)
Tue Dec 26 17:56:48 DL Manager: [Informational] Processing recipient:
mailing.list@hostname.domain.com
Tue Dec 26 17:56:48 lapis-DL Manager-MQAPI: [Diagnosis] CreateMQEntry;
Creating QID=161
Tue Dec 26 17:56:48 DL Manager: [Diagnosis] Mailing list message (QID=161, full
path: C:\PROGRA~1\IMA\INTERN~1.0\MsgQueue\06\161.msg, size: 332 bytes)
has been modified successfully.
Tue Dec 26 17:56:48 DL Manager: [Informational] Processing archive message ID
<161>
Tue Dec 26 17:56:48 AutoInsert: [Diagnosis] Parsing message (QID=161), full path:
C:\PROGRA~1\IMA\INTERN~1.0\MsgQueue\06\161.msg, size: 332 bytes
Tue Dec 26 17:56:48 AutoInsert: [Error] C:\Program Files\IMA\Internet Exchange
Messaging Server 5.0\DLMgr\ mailing.list@hostname.domain.com is missing, no
AutoText will be inserted
Tue Dec 26 17:56:48 AutoInsert: [Error] Unable to insert auto text message 161
(non-MIME), message contents unchanged
Tue Dec 26 17:56:48 DL Manager: Delivered 160 size: 332 bytes from:
<mailing.list@hostname.domain.com> to postmaster@hostname.domain.com
```

To provide a solution, the system administrator must create the disclaimer messages using any text editor (e.g. Notepad) and save it as a **disclaimer.txt** file under *C:\Program Files\IMA\IEMS 7\DLMgr\mailing.list@hostname.ima.com* (Windows) and */var/spool/iems/DL Mgr/mailinglist@hostname.ima.com* (Linux). To support HTML formatted messages, the system administrator must create a separate HTML formatted disclaimer message and save it as **disclaimer.htm** under the same directory.

Error in MQ Credentials

If you encounter an error when changing the value of the default local delivery channel with the following transactions displayed in the log file:

```
Tue Mar 07 18:39:28 AntiX Web: [Informational] Internet Domains recognized by the
 PreProcessor:ccmail.ima.com,notes.ima.com,ima.com,lapis.ima.com,ccmail.ima.com,notes.ima.com
Tue Mar 07 18:39:28 AntiX Web: [Error] Could not get LDAP option
 mqapi:MQCredentials
 Tue Mar 07 18:39:28 PreProcessor: [Informational] MQResponder; Closed
 connection from "lapis"/"AntiXcgi", served 0 requests
```

This means that some configuration options, such as the MQ Server account name and password, have not been configured properly. You need to configure these parameters by performing the following:

1. Go to the Preprocessor web interface by clicking the Preprocessor link on the top menu frame.

2. Click the Configuration button from the left menu frame.

3. Enter the correct values for the MQ Server Account Name, MQ ServerPassword, MQ Server Password (repeat), Notification messages sent to and Notify postmaster on corrupt messages parameters.

4. Click the ***Update*** button.

Preprocessor Anti-Virus Error In Log

Every time the Preprocessor is restarted, it will verify if an anti-virus profile has been configured. It displays an informational message indicating that you have to run the Preprocessor's anti-virus configuration to create one.

```
Wed Dec 27 11:20:41 PreProcessor: [Informational] Initializing IMA Common library
Wed Dec 27 11:20:41 lapis-PreProcessor-MQAPI: [Informational] Calling MQInit.....
Wed Dec 27 11:20:41 PreProcessor: [Informational] Loading Preprocessor modules
Wed Dec 27 11:20:41 Anti-virus: [Informational] Loading virus scan profile(s)
Wed Dec 27 11:20:41 Anti-virus: [Error] No active virus scan engine profile has been
loaded.
Wed Dec 27 11:20:41 Anti-virus: [Error] Please run AntiVirus configuration
Wed Dec 27 11:20:41 PreProcessor: [Informational] Loaded Module AntiVirus, version
5.0, "Add-in module providing anti-virus capability"
```

To get rid of the error, do the following:

1. Go to Preprocessor anti-virus configuration by clicking the **Preprocessor** link on the top menu frame and selecting the ***Anti-virus plug-in configuration*** button from the left menu frame.

2. Click the ***New*** button. The "New Profile" screen will appear, but with blank fields. Supply the necessary values for the different parameters to create an anti-virus profile. See “Creating Anti-Virus Profiles” on page 48.

Preprocessor Terminates After Changing The Machine’s IP Address

If you change the machine's IP address after installing IEMS, the new settings will not automatically be reflected in the Preprocessor configuration. This terminates the Preprocessor.

```
Wed Dec 27 11:18:12 PreProcessor: [Informational] Free space monitor thread
started
Wed Dec 27 11:18:12 lapis-unknown-MQAPI: [Informational] System hostname:
hostname
Wed Dec 27 11:18:12 PreProcessor: [Informational] MQResponder; Rejected
connection from 192.168.1.1, IP address not included in "MQ Server Access
Addresses"
Wed Dec 27 11:18:12 lapis-PreProcessor-MQAPI: [Error] MQInit; Could not
Authenticate to PreProcessor on server lapis
Wed Dec 27 11:18:12 PreProcessor: [Error] MQinit Failed, exiting
Wed Dec 27 11:18:13 PreProcessor: [Informational] MQResponder; Received
Termination request
Wed Dec 27 11:18:13 PreProcessor: [Informational] MQResponder; Listening
thread terminated
```

To solve this problem, update the Preprocessor's MQ Server Access Mask by performing the following steps:

1. Go to Preprocessor anti-virus configuration by clicking the Preprocessor link on the top menu frame and selecting the ***Configuratio***n button from the left menu frame.

2. Input the correct IP address of the machine in the MQ Server Access Mask field.

3. Click the ***Update*** button.

Local User Mailbox is Corrupted

In case a local user's mailbox is corrupted or is inaccessible, you may use the Message Store rebuild utility (REBUILD.EXE) to recover the user's mailbox. The REBUILD utility is command-line driven.

The following options are available for this utility:

-f Rebuild all user/shared mailboxes under Message Store home directory (e.g. rebuild -f)

user Rebuild mailbox(es) of the user (e.g. rebuild *john@ima.com*)

user mailbox Rebuild specified mailbox of the user (e.g. rebuild *john@ima.com* inbox)

To run the rebuild utility, follow the steps below:

1. Go the */opt/iems/bin* (Linux) or the installation directory of IEMS *(C:\Program Files\IMA\IEMS 7*) in the MS-DOS command prompt for Windows.

2. Type:

```
rebuild [-f] [user [mailbox]]
```

(e.g. rebuild -f john@ima.com inbox).

3. Press the ENTER key to restore the user's mailbox in the local Message Store.

Note: *Before running the utility, you must make sure that the account is existing in the local Message Store. Copy the backup files (user's directory in the Message Store) to the new directory before running the rebuild utility.*

IMAPD and POP3D Modules Will Not Start

IMAPD and POP3D will not start if the IMAPD and POP3D ports are being used by another Daemon. See log file below.

```
Wed Dec 27 13:53:27 IMAPD: [Error] Unable to bind connection socket!
Wed Dec 27 13:53:27 topaz.testlab.net-unknown-MQAPI: [Informational] System
hostname: topaz.testlab.net
Wed Dec 27 13:53:27 LDAP Server: [Informational] conn=15 op=-1 fd=16 closed
errno=Success
Wed Dec 27 13:53:27 IMAPD: [Diagnosis] Server shutting down....
Wed Dec 27 13:53:27 IMAPD: [Diagnosis] Waiting for clients to disconnect....
Wed Dec 27 13:53:27 smtpc: [Diagnosis] created the signal worker thread successfully
Wed Dec 27 13:53:27 smtpc: [Diagnosis] Started SignalWorker thread
Wed Dec 27 13:53:27 smtpc: [Informational] The current License Key type is Permanent.
Wed Dec 27 13:53:27 smtpc: [Informational] The current Serial Number is 88888.
Wed Dec 27 13:53:27 smtpc: [Informational] The user limit for the current software is
unlimited.
Wed Dec 27 13:53:27 smtpc: [Informational] License settings checked on : Wed Dec
27 13:53:27 2000
Wed Dec 27 13:53:27 POP3D: [Error] Unable to bind connection socket!
Wed Dec 27 13:53:27 POP3D: [Diagnosis] Server shutting down....
Wed Dec 27 13:53:27 POP3D: [Diagnosis] Waiting for clients to disconnect..
```

The system administrator must check if there is another IMAPD or POP3D server running on the machine. This can happen when another messaging server is running at the same time as IEMS.

For RedHat 6.2, perform the following:

1. Stop IEMS by executing:

```
# /etc/rc.d/init.d/responder stop
```

2. Disable the Sendmail daemon by editing the **/etc/sysconfig/sendmail** configuration file using any text editor. The edited file should read:

```
DAEMON=no
QUEUE=1h
```

3. Restart sendmail by executing the command:

```
#  /etc/rc.d/init.d/sendmail stop
```

4. Edit the **/etc/inetd.conf** file. The edited file should read,

```
# pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d
# imap stream tcp nowait root /usr/sbin/tcpd imapd
```

Note: *The change is indicated by a # character in the first column - this converts the line to a comment*.

5. Restart inet services by issuing the command:

```
#  /etc/rc.d/init.d/inet restart
```

6. Restart the IEMS by executing:

```
#  /etc/rc.d/init.d/responder start
```

For Redhat 7.0/7.1, and other Linux systems running xinetd, perform the following:

1. Stop IEMS by executing:

```
#  /etc/rc.d/init.d/responder stop
```

2. To disable the IMAP, edit the **/etc/xinetd.d/imap** file. The edited file should read:

```
service imap
{
  disable              = yes
  socket_type          = stream
  wait                 = no
  user                 = root
  server               = /usr/sbin/imapd
  log_on_success    += DURATION USERID
  log_on_failure    += USERID
}
```

3. Disable the POP3 server by editing the **/etc/xinetd.d/ipop3** file. The edited file should read:

```
service pop3
{
  disable             = yes
  socket_type         = stream
  wait                = no
  user                = root
  server              = /usr/sbin/ipop3d
  log_on_success   += USERID
  log_on_failure   += USERID
```

```
}
```

4. Restart inet services by issuing the command:

```
# /etc/rc.d/init.d/xinetd restart
```

5. Restart the IEMS by executing:

```
# /etc/rc.d/init.d/responder start
```

For Windows, perform the following:

1. Make sure that IEMS is not running.

2. Perform a telnet session to the machine using port 110 (i.e., POP3) and then on port 143 (i.e., IMAP4) using the telnet utility.

3. Check for the existence of a POP3 server by typing:

   ```
   telnet machinename 110
   ```

   from the MS-DOS command prompt. If another POP3 server is running on the your machine, it will respond with a message.

4. Check for the existence of an IMAP4 server by typing:

   ```
   telnet machinename 143
   ```

   from the MS-DOS command prompt. In case you have another IMAP4 server running on the your machine, it will also respond with a message.

The above mentioned procedures can help in finding out the existence of IMAP/ POP3 servers other than IEMS. If you discover that there is another IMAP/ POP3 server running, make sure you delete, uninstall or disable that mail server software before starting IEMS.

Messages Are Piling up in The SMTPC Queue Status Directory

This problem is due to a corrupted message in the SMTPC queue. This corrupted message must be deleted first before the rest of the messages in the queue can be processed. SMTPC's queueing strategy processes the first message in the queue. Check the messages in the queue by going to the "Queue Status" page of the SMTPC module. To be able to send the messages in the SMTPC queue, perform the steps in “Cannot Send Messages Even After Deleting Suspected Corrupted Files” on page 241.

1. Shut down all IEMS modules.

2. Start the LDAP Server manually.

3. Open MS-DOS prompt and type *C:\Program Files\IMA\Internet Exchange 6.x* (Windows) *or /opt/iems/bin* (Linux).

4. From the *C:\Program Files\IMA\IEMS 7* or */opt/iems/bin*, run:

```
dbupdate -r
```

5. Restart IEMS.

Note: *Remember the message sequence number that has to be deleted.*

If there are still stuck messages in the SMTPC Queue folder after performing the procedures mentioned above, you may have to manually force the delivery of the stuck messages by doing the following:

1. Click the SMTPC link on the top menu of the IEMS main web interface. This action displays the “SMTPC” screen.

2. On the left-hand side of the screen, click the ***Queue Status*** button to display the "SMTPC Queue Status" screen.

3. Select all the messages and click the ***Process Messages*** button.

Cannot Send Messages Even After Deleting Suspected Corrupted Files

This can be due to network or configuration problems. It is possible that message delivery to the Internet fails due to mail routing problem. A possible cause can be the wrong configuration of the MX records in the DNS or host table (if host table or mail relay host is used).

For "DNS only" mail routing, it is very important that MX record setting of the recipient domain is correct for mail to be delivered properly. To verify that the DNS has the correct MX record, use a DNS analysis tool, such as the "nslookup" utility. On any Unix or Linux machine, run performing the following:

- Type **nslookup**

- This gives you a greater than prompt (>).
  To get the MX record, type:

```
> set query=mx
> ima.com (to check records for ima.com)
```

For mail relay host routing, it is important for the mail relay host IP address to be properly entered in the host file (*/etc/hosts*) together with its aliases.

For host file routing, you must enter the correct IP address of all the machines that needs to communicate with the mail server.

Our Mail Server is Being Utilized by a Spammer

To solve this problem you can disable the mail relaying capability of the mail server by performing the following steps:

1. Click the Preprocessor link on the top menu of the IEMS main web interface.

2. Click the ***Configure anti-spam*** button on the left menu frame.

3. Select the option Deny mail relaying by default. If this option is enabled, every IP address except for those mentioned in the Allow IP address list is prohibited for mail relaying.

Note: *It is strongly recommended that mail relaying on Internet connected servers be disabled in order to protect the site from unauthorized use by spammers.*

Database Corruption Within Directory Services

The system administrator can troubleshoot Directory Services by studying the sequence of messages or errors written by the LDAP server. In the case of database corruption, you can either use the LDIF2LDBM tool or the LDBMCAT tool. Both are located under LDAPDB installation directory of IEMS. The LDIF2LDBM tool imports LDAP entries defined in an LDIF file to the LDAP database. The LDBMCAT tool on the other hand, exports the LDAP entries from the LDAP database to a text-based file in LDIF format. It will recursively increment the file name extension if a file with the same name already exists (e.g. ldif.0, ldif.1). The main database that is used for export is the **id2entry.dbb** file.

To use the LDIF2LDBM tool, perform the following:

1. Open MS-DOS prompt and go to the installation directory of IEMS (C:\Program Files\IMA\Internet Exchange Messaging Server 5.1 for Windows or /opt/iems/bin/ for Linux).

2. Type:

   ldif2ldbm ldif_file conf_file (Windows)

   or

   `ldif2ldbm/opt/iems/ldapdb/ldif/opt/iems/slapd.conf` (Linux)

   The first argument (ldif_file) is the path of the LDIF file and the second one (conf_file) is the configuration file of LDAP, slapd.conf, that comes with IEMS.

3. Press the ENTER key.

Note: *Please be cautious while running the import tool because it will overwrite your existing LDAP database. Always make a backup of the existing database before running this tool.*

To use the **LDBMCAT** tool, perform the following:

1. Open MS-DOS prompt and go to the installation directory of IEMS (*c:\Program Files\IMA\IEMS 7 for Windows or /opt/iems/bin/ directory* for Linux).

2. Type:

   ldbmcat c:\Programs Files\IEMS 7\ldapdb\id2entry.dbb (Windows)

   or

   /opt/iems/bin/ ldbmcat (Linux)

3. Press the ENTER key.

You will be prompted with the result of the conversion process, which also indicates the name of the LDIF file containing the exported data, as shown below.

```
C:> ldbmcat LDAP database

C:\LDAPDB\id2entry.dbb has been successfully exported to LDIF file
c:\LDAPDB\ldif.3
```

Inconsistent Deletion of Message Store Users Within The Directory

When a user account is created using the Message Store interface, you are asked to supply the proper values for the following parameters:

- Email Address
- First Name
- Last Name
- Password

When you select the user listing from the Directory Services interface, you will see a local connector that has the same attribute of the email address that you have used when adding the user, and a mail attribute which is also the same as the definition in the local connector.

When the user is deleted via the Message Store administrative interface, the user account is deleted in the Message Store, but still exists in the Directory Services database. This time, the local connector is already deleted and does not exist anymore. To delete the user account completely, go to the Directory Services and delete the user account (directory entry) in order to remove all of his account information.

Messages Are Note Delivered To The User's Mailbox

A possible reason why messages of an existing account of the Message Store, e.g. *john@ima.com*, is being delivered to another account, e.g. *john.doe@ima.com* would be a mail alias was defined for the particular Message Store account. The system administrator may verify from the Directory Services if an alias was defined for *john@ima.com*. Make sure that the alias defined is unique.

Unable to Insert a Disclaimer in The Auto Text Insertion Engine

If the logfile indicates that the auto insertion engine was not able to read the disclaimer text or HTML file (i.e., disclaimer.txt or disclaimer.html), check:

For Windows:

1. If the said files exist and are readable on the system.
2. If the files are stored in a network share, make sure that the system has the proper read permission to that network share.

For Linux:

1. If the said files exist and are readable on the system.

2. Check the ownership of the disclaimer text or HTML file. The disclaimer file must be owned by the user "iems". To change the ownership, run this command:

   chown iems: iems disclaimer.txt
   or
   chown iems: iems disclaimer.html

3. If the files are stored in a network share, make sure that the system has the proper read permission to that network share.

Error Handling Under Linux

Failed Dependencies - libdcerpc.so or lidcethresad.so Is Needed By IEMS

This error means that you are trying to install IEMS without installing the DCE-RPC package first. This package provides support for developing DCE-RPC and Microsoft RPC applications on Linux. The source code and binaries are distributed freely provided you maintain the copyright notice of the source components. This package can be ported to other platforms as well, as long as you can implement the semantics of DCE Exceptions and DCE Threads on the target platforms' thread layer. The DCE RPC development kit for Linux relies on GNU Libc 2.x and LinuxThreads Pthreads. DCE Threads and DCE Exceptions are emulated using LinuxThreads, allowing for multi-threaded RPC client and server applications to co-exist with other threaded and non-threaded library components in the Linux development environment. You have to install the **dce-rpc** package that is provided by IMA or found on your RedHat installation CDs.

Cannot Open Package Index Using DB3 - Permission Denied (3)

RPM database cannot be opened in DB3 format. If you have upgraded the RPM package, you need to convert your database format by running "rpm --rebuilddb" as the root. An error message, "Cannot open packages database in /var/lib/rpm"

For security reasons, restrictions are given to ordinary users trying to install a package. Normally, no other user except root has the write access on the system's rpm database. So if you try to install any package and you do not have a root permission, you will encounter this kind of problem.

Httpd: Cannot Determine Local Hostname

"Use the servername directive to set it manually [FAILED]"

This error means that the http daemon was not able to resolve the local hostname. You can solve this by adding the IP address and FQDN of the local machine in the */etc/hosts* file. The file */etc/hosts* contains a list of IP addresses and the corresponding hostnames (and aliases). Another way of solving the error is to perform the following steps:

1. Edit the /etc/httpd/conf/httpd.conf file.

2. Uncomment option for Server Name.

3. Add the local FQDN
   (e.g.

   #ServerName localhost

   To Read:

   ServerName hostname.domainname

4. Restart HTTP Daemon by executing:

   # /etc/rc.d/init.d/httpd restart

5. HTTPD will now load the new settings and automatically determine the FQDN of the Apache web server every time the Apache is started.

config.c Could Not Open File

This error occurs if the configure file cannot be opened, does not exist or you have no access right to open the file. To solve this problem, make sure that all the configure files (slapd.conf, slapd.at.conf and slapd.oc.conf) are located in the install directory and have read permission.

Application [Error] Failed To Open The UIDL Database, 20

If you encounter this error, it means that the Btrieve engine is not active or running. You must perform the following:

1. Bring up the ***Task Manager*** and click on ***Process***.
2. Stop the **w32mkde.exe** program.
3. Restart IEMS. This will automatically restart the Btrieve engine.

Could Not Authenticate to Preprocessor on Server

IEMS cannot authenticate the Preprocessor due to IP address mismatch. The IP address assigned to your mail server is different from the one set in the Preprocessor. The Preprocessor probably is not updated and still uses the old IP address which conflicts with the newly acquired IP address of the mail server, thus causing the Preprocessor to terminate.

To solve this problem:

1. Shut down all IEMS components.
2. Manually start the Directory Services.
3. Go to the Preprocessor configuration screen and enter the new IP address of the mail server in the MQ Server Access Mask field.
4. Restart the MTA.

daemon.c Binding to Address Failed

This error appears if the port used by the LDAP server (default is 389) is used by another program. The system administrator must shut down the IEMS and the other program utilizing the LDAP port (389). Then, restart IEMS.

LDAP Server: ch_malloc.c Memory Allocation Error

This error means that the LDAP server cannot allocate enough memory. To solve this problem, make sure that the system has enough memory available. You may be able to add system memory by closing the applications that are not being used. If problems still persist, do the following:

1. Shut down all IEMS components.
2. Restart the whole system.

main.c Could Not Open NEXTID

This error means that the database files does exist or is corrupted. You will need to rebuild the LDAP database by using the LDAP database recovery tools "LDIF2LDBM" or "LDBMCAT". Please refer to “Database Corruption Within Directory Services” on page 242 for more information on using the"LDIF2LDBM" or "LDBMCAT" tools.

main.c Creating New Backend Database Files (Including NEXTID)

This error means that LDAP cannot find the database files and cannot create new files. Another possible reason is the corruption of database files. It is recommended to rebuild the database by using the LDAP database recover procedure. Please refer to “Database Corruption Within Directory Services” on page 242.

VIMSendMessage failed: 2/1

“VIM error message: A fatal error occurred; VIM extended message: WIN.INI; VIM extended message: WIN.INI.”

The two log messages, "A fatal error occurred" and "WIN.INI", are the corresponding text for the VIM error 2/1. These two strings are returned from the VIM DLL. Lotus does not offer that much information on the VIM API explaining the cause of this error. Past experiences told us that these error messages are related to cc:Mail database problems. Running the post office maintenance utility "reclaim" resolves this problem most of the time.

Error 2

Error '2' means file not found. This might be caused by the MESG.BTR in the CCIN sub-directory being out of sync with the message queue. To solve the problem, perform the following steps:

1. Shut down all IEMS components except the Apache web server.
2. Go to *C:\Program Files\IMA\IEMS 7\MsgQueue\ccIn* and delete the file "MESG.BTR" (if the system does not allow you to delete the file, wait for at least 2 minutes, then try again).
3. Delete all files with extension ***.ccmail** under the *\MsgQueue\01* up to 10 directories.
4. Restart IEMS.

pwdhook.dll Not Properly Installed, Please Run Setup Again

This problem usually happens when you do not move the **NOTES.INI** file to the *C:\Winnt* directory and reboot before proceeding with the installation. To solve this problem, perform the steps below:

1. Manually modify the **NOTES.INI** file by adding the setting '[Notes] ExtMgr_AddIns=pwdhook' to the last line.
2. Rerun the **notesetup.exe** procedure again.

Error Handling Under Linux and Windows

daemon.c Exceeded Maximum Number of Sockets Allowed

The system administrator must change the maximum number of sockets by modifying the sockets attribute in the **slapd.conf** file.

Under Linux, perform the following:

1. Open the Unix shell and go to the /opt/iems/bin.
2. Edit the file `slapd.conf`.
3. Locate the parameter sockets in the file.
4. Edit the value for the sockets by changing the value to a higher value.
5. Save the file.
6. Restart IEMS.

Under Windows, perform the following:

1. Open the MS-DOS prompt and go to the *C:\Program Files\IMA\IEMS 7*.
2. Locate the slapd.conf file and open it using any text editor (i.e., Notepad.exe)
3. Edit the value for the sockets by changing the value to a higher value. By default, the number of sockets for IEMS 6 is 250.
4. Save the file.
5. Restart IEMS.

SMTPC Message Database is Not in The New (5) Format

"Please run DBUPDATE.EXE to update the database."

This error is generated when the current SMTPC cannot access the SMTPC message database in the system because of incompatibility in database format. This leads to SMTPC's inability to send messages to the Internet, which further results in message pile up in the SMTPC Queue.

To solve this problem, you have to convert the current SMTPC message database to the format recognized by the SMTPC module of IEMS. To do so, follow these steps:

1. Shut down IEMS.
2. Open MS-DOS command prompt or the Unix shell.
3. Go to the IEMS Directory *(C:\Program Files\IMA\IEMS 7* for Windows and */opt/iems/bin* for Linux) and type:

dbupdate -u

4. Press the ENTER key. This command updates the format of the SMPTC queue message database.

The SMTPC message database stores the envelope information and status of the messages in the SMTPC Queue. The SMTPC accesses this database to get information necessary for sending messages to the Internet. If the SMTPC fails to do this, it cannot send the messages to the Internet.

The SMTPC message database of previous versions of IEMS cannot be accessed by the SMTPC module of IEMS. This is why the envelope and status information of the new messages entering the SMTPC Queue are not added to the SMTPC message database, which results in the SMTPC Queue and the SMTPC message database to be unsynchronized. To synchronize the SMTPC Queue and SMTPC message database, type `dbupdate -r` in the IEMS directory. This rebuilds the SMTPC queue message database to include the envelope information of all the messages in the SMTPC Queue.

APPENDIX A

License Agreement

THANK YOU FOR PURCHASING RIGHTS TO USE THIS SOFTWARE OWNED BY INTERNATIONAL MESSAGING ASSOCIATES CORPORATION (IMA). THIS LIMITED USER LICENSE AGREEMENT STATES THE TERMS AND CONDITIONS UNDER WHICH YOU ARE PERMITTED TO USE THE SOFTWARE. INSTALLATION OF THE SOFTWARE **INDICATES YOUR ACCEPTANCE OF THE FOLLOWING TERMS AND CONDITIONS. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU CAN NOT PROCEED FURTHER WITH THE INSTALLATION.**

AS FURTHER DESCRIBED IN THE INFORMATION ACCOMPANYING THE SOFTWARE, THIS SOFTWARE CAN ONLY BE USED WITH AN ENABLING LICENSE KEY. IMA WILL PROVIDE YOU WITH AN AUTHORIZATION KEY WHICH WILL ALLOW THE APPROPRIATE SOFTWARE TO FUNCTION WITHOUT LIMITATION ONCE YOU HAVE MADE FULL PAYMENT TO IMA OR ONE OF ITS AUTHORIZED VENDORS.

LIMITED USE OF SOFTWARE LICENSE

LICENSE: This software contains multiple IMA products. IMA grants you a non-exclusive, nontransferable limited use of licensed software product and accompanying documentation that has been purchased according to the following terms and conditions:

For the software you may:

physically transfer the software from one computer to another, provided that each software product is installed in only one computer or distributed system at a time;

(1.1) A distributed system is defined as one or more computers running a single copy of the software in tandem. With the exception of the responder, no more than one instance of each of the software modules may be running at one time amongst the computers making up the distributed system;

make one copy of the software solely for backup purposes, provided you reproduce and include the copyright notice on the back-up copy.

You may not or will not permit others to do any of the following:

use the software on more than one computer or distributed system at a time (see section 1.1 above);

modify, translate, reverse engineer, decompile, disassemble, prepare derivative works of the software, or copy the software or accompanying documentation;

share, rent, lease, sublicense, or transfer your right to use the software or otherwise grant any right to use the software, or accompanying documentation in any form to another party without the prior written consent of IMA, or provide access to the software on a local area network, wide area network, or any other multiple user computer hardware or software arrangement, to a person who is not a member or employee of your firm, agency or company; or

remove any proprietary notices, labels, or marks on the software and accompanying documentation.

RIGHTS OF IMA: You acknowledge that title and any rights to the software, accompanying documentation and any copy made by you remain the sole and exclusive property of IMA. Any unauthorized reproduction, publication, disclosure or distribution of the software or accompanying documentation is strictly prohibited. Any breach or other failure to comply with the terms and conditions herein will entitle IMA to terminate this license and seek all other appropriate legal remedies.

LIMITED WARRANTY: For a period of 45 days from the date when you pay the license fee for the software, IMA warrants that the medium upon which the software resides will be free of defects that prevent you from loading it onto your computer. IMA.s sole obligation under this warranty is to replace any defective media, provided you have given IMA notice of the defect within that 45-day period. This IMA software is licensed to you “as is” and neither IMA nor its vendor’s warrant, it will be uninterrupted or error free. **THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ALL SUCH WARRANTIES ARE EXPRESSLY AND SPECIFICALLY DISCLAIMED.**

LIMITATION OF LIABILITY: IN NO EVENT WILL IMA OR ITS VENDORS BE LIABLE FOR ANY DAMAGE OR LOSS OF ANY KIND ARISING FROM OR RESULTING FROM YOUR POSSESSION OR USE OF THE SOFTWARE, INCLUDING LOSS OF DATA OR CORRUPTION THEREOF, REGARDLESS OF WHETHER THAT LIABILITY IS BASED IN TORT, CONTRACT OR OTHERWISE. IF THE FOREGOING LIMITATION IS HELD TO BE UNENFORCEABLE, OR IN ANY OTHER CASE, YOU ACKNOWLEDGE THAT THE LICENSE FEE REFLECTS THE ALLOCATION OF RISK AND AGREE THAT IMA.S MAXIMUM LIABILITY TO YOU SHALL NOT EXCEED THE AMOUNT OF THE LICENSE FEE YOU PAID. IMA SHALL IN NO EVENT BE LIABLE FOR ANY LOST PROFITS, COST OF COVER, OR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGE, EVEN IF IMA OR ITS VENDORS HAVE BEEN ADVISED OF SUCH DAMAGE OR POSSIBILITY THEREOF. BECAUSE SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF IMPLIED WARRANTIES OR LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SOME OF THE LIMITATIONS OR EXCLUSIONS DESCRIBED ABOVE MAY NOT APPLY TO YOU.

GOVERNMENT RESTRICTED RIGHTS LEGEND (Applicable to U.S. Government End-Users Only)
Use, duplication or disclosure by the United States Government is subject to restrictions of Restricted Rights for computer software developed at private expense as set forth in FAR Sec. 52.227-19 or DOD FAR Supplement Sec. 252,227-7013(c)(1)(ii), and successor thereof, as applicable.

MISCELLANEOUS: This agreement will be governed and construed in accordance with the substantive laws of the State where delivery of the software occurred. If such delivery did not occur within a State or Territory of the United States, then this agreement shall be governed by the substantive laws of Hong Kong, and will in either case be without application of conflict or law principles.This agreement is the entire agreement and supersedes any other communications or advertising with respect to the software and accompanying documentation. Any modification of this agreement must be in writing and signed by an officer of IMA. If any provision of this agreement is held invalid, the remainder of this agreement will continue in full force and effect. *If you have any questions, please write us in this address:* **IMA Services Limited, 203 Keen Hung Commercial Building, 80 Queen's Road East, Wan Chai, Hong Kong.**

APPENDIX B

System Requirements

For optimum performance, it is recommended that Internet Exchange Messaging Server (IEMS) version 7 and its components be installed using the following minimum configurations:

For Windows 98 (Anti-Virus Processing Only)
- Pentium or higher
- Minimum recommended RAM: 64MB
- Minimum recommended hard disk space for applications: 200MB

For Windows XP, 2000 and Windows NT 4.0 with SP4
- Pentium or higher
- Minimum recommended RAM: 96MB
- Minimum recommended hard disk space for applications: 200MB
- Minimum recommended hard disk space for message store: 1GB or dependent on the number of users

For Linux
- Pentium or higher
- Minimum recommended RAM: 64MB
- Minimum recommended hard disk space for applications: 200MB
- Minimum recommended hard disk space for message store: 1GB or dependent on the number of users

IEMS supports the following Linux distributions:
- RedHat 6.2 - 9.0
- Mandrake 8.2 - 9.1
- SCO Linux Server 4.0 (United Linux 1.0)
- RedFlag
- Cosix (CS&S)

TCP Port Usage
The Internet Exchange Messaging Server makes use of the following TCP ports:

21	FTP (Calendaring / Scheduling backend server)
25	SMTP
110	POP3
143	IMAP4
389	LDAP (Directory Server)
1234	Responder
1235	Message Queue Server
1236	Preprocessor Alias Update listener
1240	Antivirus Server (when AV configured in distributed mode)
4000	Locmail Server
4001	Message Store Server

Note: *The above mentioned system requirements are applicable for both single machine and distributed system installations.*

The base hardware/software configuration is only for running the machine's OS (Operating System) and other software needed to install IEMS properly. To determine the total minimum memory requirement needed by your machine to install the OS and IEMS, you must add the memory requirements of the IEMS components to the base hardware configuration. To compute the minimum memory requirements for your machine, please refer to the **Internet Exchange Messaging Server 7 - Site Planning Guide** for a detailed description.

For example, if you have a machine running Windows 98, you need a minimum of 64MB of RAM to run the OS. If you wish to install IEMS on that machine, then you will have to install additional RAM of 6MB for SMTPD, 4MB for SMTPC, 2MB for the MQ Router, 4MB for the Directory Services, 4MB for the DL Manager, 8MB for the Preprocessor, 4MB for the Btrieve Database Engine, 4MB for the Anti-virus, 2MB for the Responder, 2MB for the Apache Web Server, 2MB for the Auto-loop detection DLL (Dynamic Link Library), 2MB for the Anti-spam, and 8MB for the Administration Tools. Thus, the machine needs at least 118MB of RAM in order for the IEMS to run smoothly.

Before installing the software either on a single machine or on a distributed system, make sure that you have installed the certificate file issued to you by IMA on your local disk drive. The certificate file will be used to activate the modules to be installed on your machine. Please take note of the directory path of the certificate file. You will be prompted to verify this directory path when you reach the licensing stage. Without this certificate file, you will not be able to run the software.

Note: Those with * are available only on Windows platforms.

APPENDIX C

SSL System Configuration

SSL (**S**ecure **S**ocket **L**ayer) is an industry standard, utilizing public key cryptography. It has been widely deployed in web applications by SSL-enabled web clients and servers. Originally designed by Netscape, it has undergone IETF standardization and is also known as TLS (**T**ransport **L**ayer **S**ecurity). SSL provides three fundamental security services at the network transport layer - message privacy, message integrity, and mutual authentication.

IEMS includes a distribution of the public domain **stunnel** (Universal SSL Tunnel) and **OpenSSL** packages. Stunnel is a universal SSL enabler for networked applications. IEMS uses the daemon mode of stunnel, which accepts SSL connections for IMAP/POP3 and then connects to the IEMS IMAP/POP server running locally.

Note: *Due to patent protection, IDEA and RC5 algorithms have not been built into the IEMS distributed versions of either* ***stunnel*** *or the* ***openssl library****.*

Additional information about **stunnel** and **OpenSSL** can be found at:

http://www.stunnel.org
http://www.openssl.org

Certificates

Before enabling SSL support, a server certificate must be installed on the IEMS machine. A certificate (or public key certificate) is a digital document that binds entities (people, servers, others) via a public key. In addition to containing a public key and a name, it also contains an expiration date, the name of the certification authority (CA) that issued the certificate, a serial number, and other information. Most importantly, it contains the digital signature of the certificate issuer. The Certification Authority (CA) represents the trusted third party that issues keys and certificates to end users and manages their life cycle including generation, revocation, expiration, and updates.

To implement either the SSL-enabled web server, IMAP-4 and/or POP-3 servers, a server SSL certificate is used during the SSL handshake process. The IEMS service (web, IMAP, POP) presents its certificate to the client to authenticate the server's identity.

Once authentication has been accomplished, the remote client and IEMS server will negotiate a secret key for encrypting all subsequent communication data. The public key contained in the certificate will be used to encrypt the secret for secure key exchange.

Certificates for use with SSL can be obtained from either an authorized Certificate Authority (CA) or generated by the local system administrator. Certificates issued by an authorized Certificate Authority have an advantage that they are trusted by most clients, while there is no implied guarantee to the authenticity of a non-CA issued certificate.

Generating Your Own SSL Certificate

The **OpenSSL** library toolkit is installed with IEMS 7. Depending on the installation, it is installed in the following locations:

- **Windows:** *C:\iems 7\openssl\bin\openssl.exe*
- **Linux:** */opt/iems/bin/openssl*

The OpenSSL utility is used to create a self-signed SSL server certificate, and the server key, both in PEM format. Both the certificate and server keys are output to the file **stunnel.pem**. Please note that the server key is not password protected, and in the example below is valid for only 365 days.

To generate your key, perform the following steps:

- Change to the IEMS installation directory (defaults are given above).
- Generate the **stunnel.pem** file by issuing the following command:

```
./openssl req -new -x509 -days 365 -nodes -config ./stunnel.cnf
              -out ./stunnel.pem -keyout ./stunnel.pem
```

- You will then be asked to enter a Distinguished Name (DN), made up of the following: *Country Name*, *State*, *Locality Name*, *Organization Name*, *Organization Unit Name*, *and Common Name* (FQDN of your server).

The content of the **stunnel.pem** file should look similar to the following:

```
-----BEGIN CERTIFICATE-----
MIICOTCCAaKgAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGEwJQTDET
MBEGA1UECBMKU29tZS1TdGF0ZTEfMB0GA1UEChMWU3R1bm5lbCBEZXZlbG9wZXJz
IEx0ZDESMBAGA1UEAxMJbG9jYWxob3N0MB4XDTAxMDgxOTA2MjMyMFoXDTAyMDgx
OTA2MjMyMFowVzELMAkGA1UEBhMCUEwxEzARBgNVBAgTClNvbWUtU3RhdGUxHzAd
BgNVBAoTFlN0dW5uZWwgRGV2ZWxvcGVycyBMdGQxEjAQBgNVBAMTCWxvY2FsaG9z
dDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAsxwZcTe1eMbRQt5VeDZX6EDT
vp/yzQL743P1TE5eCCt288oUQ7JehthLs3rqVpAMkwpXBmePvvgHzOJclU08bjel
dae7BwV3jQpPV/qh9VbYdNJLVcv47DMUH6EIFFSWavcREK9cU0PnH+9+dEGt5KVU
pH9nYHsOAPdU60wFkW0CAwEAAaMVMBMwEQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqG
SIb3DQEBBAUAA4GBADHICl7XDurBHkLiC4RL8AsYmzPkfYyi+Ky7lCAEl56j9EEY
aZEWTA3jAtIANdDHerHzqQk8J2Fo5CRWUPj5iIBCLFv+eS5y5D6oy8hkdn5Lg3o3
BPOAErL16Y9LaFTNYEXG1WMYxR0kGzEUL8oqku1KECadKRCDtgPu/o6aNyNC
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCzHBlxN7V4xtFC3lV4NlfoQNO+n/LNAvvjc/VMTl4IK3bzyhRD
sl6G2EuzeupWkAyTClcGZ4+++AfM4lyVTTxuN6V1p7sHBXeNCk9X+qH1VthO0ktV
y/jsMxQfoQgUVJZq9xEQr1xTQ+cf735OQa3kpVSkf2dgew4A91TrTAWRbQIDAQAB
AoGBAK2yHmpRoEeUZ/P1MeX2raGq3K4M56Yxsp2OIuDxTveVTzJ1Utmj7U/QCvnv
xbpU0Bz49hRb8mc8mjPzgd24nVSVRXbnvnOjfBBnW+RvaIKer21qHbyeX/Pifyue
```

```
jPVBtaQuhxTDtqyvs5JWxsTWysU3sVwrqj6p4emnAJVjyhhxAkEA53cFmf2s3Xgm
kEKWs9TRMBa8PL3AZBeYohvyJi7yJHwLm7T/KOOja/sX9fgePY2CYKaqNF/opd20
O4NmcfBXHwJBAMYYYUY42faRY7lV73zqvxoBCjdiFkBOrx6gwOOdXBEXoDjiJOmo
CaYitM/3OBKYsMFC9r6OlpLSan2mEFy8QfMCQGfx7GMOJ65Bgdfw/2p83QBihWAl
upt4eUP7ltAM7xLxXekr7BePCaQ5W7ZLGZF81hr/XZoto/Wwzb7a2Iu8afMCQQC4
xLS2kwB6g1HI5ObkVPC6iI3G6q5mfP3KS5jVOEi3iJnhdM/AXAPj+is8b6CcN99l
49fSFZ1MhQbe+633UYERAkBsERtYYtQm1TDa8bRejOFHqqZTFj2+HhIOla0FhM3F
GITd8c9W9CnGnkPH/371DtQkesSZtXOBhjrk7IcmvdMi
-----END RSA PRIVATE KEY-----
```

The data between the line "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" is the server certificate content. The data between the line "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----" is the server key content.

To check to make sure the certificate file has been correctly generated, issue the following command:

```
./openssl x509 -subject -fingerprint -noout -in ./stunnel.pem
```

If the generated certificate file is in the correct format, the output of the command above should contain the subject and MD5 fingerprint of the certificate, similar to:

```
subject=/C=US/ST=California/L=Oakland/O=IMA/OU=Sales/
CN=bart.ima.com/CN=localhost
MD5 Fingerprint=6C:96:19:74:0A:D8:BB:5E:DC:7B:3D:2B:44:C1:3D:26
```

Enabling SSL Support for IMAP/POP3

To install the server certificate for IEMS use (IMAP/POP3), the **stunnel.pem** file needs to be installed in the IEMS installation directory. Under Windows the default location is *C:\iems\stunnel\stunnel.pem*. Under Linux, the default is */opt/iems/stunnel.pem*. For Linux installations, after copying the **stunnel.pem** file, be sure to change the owner and group id's to iems/iems.

After the **stunnel.pem** file has been installed and ownership rights properly setup, the IMAP/POP3 security settings can be enabled through the administrator's interface.

Enabling SSL Support for Apache

The Apache web server requires the certificate and the server key to be placed in separate files. The certificate file is called **server.crt**, while the server key file is **server.key**. For our sample **stunnel.pem** file content above, the two files should contain content similar to the following:

server.crt file

```
-----BEGIN CERTIFICATE-----
MIICOTCCAaKgAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGEwJQTDET
MBEGA1UECBMKU29tZS1TdGF0ZTEfMB0GA1UEChMWU3R1bm5lbCBEZXZlbG9wZXJz
IEx0ZDESMBAGA1UEAxMJbG9jYWxob3N0MB4XDTAxMDgxOTA2MjMyMFoXDTAyMDgx
OTA2MjMyMFowVzELMAkGA1UEBhMCUEwxEzARBgNVBAgTClNvbWUtU3RhdGUxHzAd
BgNVBAoTFlN0dW5uZWwgRGV2ZWxvcGVycyBMdGQxEjAQBgNVBAMTCWxvY2FsaG9z
dDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAsxwZcTe1eMbRQt5VeDZX6EDT
vp/yzQL743P1TE5eCCt288oUQ7JehthLs3rqVpAMkwpXBmePvvgHzOJclU08bjel
```

```
dae7BwV3jQpPV/qh9VbYdNJLVcv47DMUH6EIFFSWavcREK9cU0PnH+9+dEGt5KVU
pH9nYHsOAPdU60wFkW0CAwEAAaMVMBMwEQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqG
SIb3DQEBBAUAA4GBADHICl7XDurBHkLiC4RL8AsYmzPkfYyi+Ky7lCAEl56j9EEY
aZEWTA3jAtIANdDHerHzqQk8J2Fo5CRWUPj5iIBCLFv+eS5y5D6oy8hkdn5Lg3o3
BPOAErL16Y9LaFTNYEXG1WMYxR0kGzEUL8oqku1KECadKRCDtgPu/o6aNyNC
-----END CERTIFICATE-----
```

server.key file:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCzHBlxN7V4xtFC3lV4NlfoQNO+n/LNAvvjc/VMTl4IK3bzyhRD
sl6G2EuzeupWkAyTClcGZ4+++AfM4lyVTTxuN6V1p7sHBXeNCk9X+qH1Vth00ktV
y/jsMxQfoQgUVJZq9xEQr1xTQ+cf735OQa3kpVSkf2dgew4A91TrTAWRbQIDAQAB
AoGBAK2yHmpRoEeUZ/P1MeX2raGq3K4M56Yxsp2OIuDxTveVTzJ1Utmj7U/QCvnv
xbpU0Bz49hRb8mc8mjPzgd24nVSVRXbnvnOjfBBnW+RvaIKer21qHbyeX/PifyUe
jPVBtaQuhxTDtqyvs5JWxsTWysU3sVwrqj6p4emnAJVjyhhxAkEA53cFmf2s3Xgm
kEKWs9TRMBa8PL3AZBeYohvyJi7yJHwLm7T/KOOja/sX9fgePY2CYKaqNF/opd2O
O4NmcfBXHWJBAMYYYUY42faRY7lV73zqvxoBCjdiFkBOrx6gwOOdXBEXoDjiJOmo
CaYitM/3OBKYsMFC9r6OlpLSan2mEFy8QfMCQGfx7GMOJ65Bgdfw/2p83QBihWAl
upt4eUP7ltAM7xLxXekr7BePCaQ5W7ZLGZF81hr/XZoto/Wwzb7a2Iu8afMCQQC4
xLS2kwB6g1HI5ObkVPC6iI3G6q5mfP3KS5jV0Ei3iJnhdM/AXAPj+is8b6CcN99l
49fSFZ1MhQbe+633UYERAkBsERtYYtQm1TDa8bRejOFHqqZTFj2+HhIOlaOFhM3F
GITd8c9W9CnGnkPH/371DtQkesSZtXOBhjrk7IcmvdMi
-----END RSA PRIVATE KEY-----
```

Installing the Apache Server Certificate and Key

Both the server key and certificate files generated above must be installed in the Apache configuration area. If a default installation was done, the location of the installed files should be as follows:

Windows

C:\iems 7\apache\conf\ssl.crt\server.crt
C:\iems 7\apache\conf\ssl.key\server.key

Linux

/etc/httpd/conf/ssl.crt/server.crt
/etc/httpd/conf/ssl.key/server.key

Apache Configuration File Changes

After copying the certificate and key files, the Apache configuration file needs to be modified for SSL support. The standard way of including IEMS support for Apache is to simply include the IEMS configuration fragment from the installed IEMS files. This is done through an *include* directive in the configuration file. The standard IEMS *iems.httpd.conf* file supports both standard as well as SSL configurations. See the supplied file for specific configuration details. After making the necessary site specific changes perform the following:

Windows:

Stop the Apache server, and start it again using the following command to enable SSL support:

C:\iems 7\apache\Apache -D SSL

Your IEMS server can now be contacted by using the following URL:

https://FQDN/iems

where FQDN is the Fully Qualified Domain Name of the IEMS server.

Linux:
Stop the Apache server, and start it again using the following command to enable SSL support:

/etc/rc.d/init.d/httpd restart

Your IEMS server can now be contacted by using the following URL:

https://FQDN/iems

where FQDN is the Fully Qualified Domain Name of the IEMS server.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W